aws

管理指南

Amazon Detective

Amazon Detective: 管理指南

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數據。此資料可透過一組視覺化取得，視覺化可顯示已選取時間範圍內活動類型和數目的變化。Detective 將此類變更連結至 GuardDuty 調查結果。如需 Detective 中來源資料的詳細資訊，請參閱 行為圖表中使用的來源資料。

Detective 如何運作？

Detective 會自動擷取時間型事件，例如登入嘗試、API 呼叫和來自 AWS CloudTrail 的網路流量以及 Amazon VPC 流程日誌。它還會擷取 GuardDuty 偵測到的調查結果。

透過此類事件，Detective 使用機器學習和視覺化來建立資源行為的統一互動式檢視，以及它們之間在一段時間後的互動。您可以探索此行為圖表，以檢查潛在的惡意動作，例如失敗的登入嘗試或可疑的 API 呼叫。您也可以查看此類動作如何影響 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 也與 AWS Organizations 一起集成。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。

如需有關 Detective 如何使用行為圖表帳戶中的來源資料的資訊，請參閱 行為圖表中使用的來源資料。

如需有關管理員帳戶如何管理行為圖表的資訊，請參閱 管理帳戶。如需有關成員帳戶如何管理其行為圖表邀請和成員資格的資訊，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化，用於調查 AWS 資源和 GuardDuty 調查結果。使用 GuardDuty 和 AWS Security Hub 的 Detective 整合，您可以從此類服務中的 GuardDuty 調查結果直接錨定到 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。

Amazon Detective 術語和概念

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

擁有行為圖表且使用行為圖表進行調查的 AWS 帳戶。

管理員帳戶會邀請成員帳戶將其資料提供至行為圖表。如需更多詳細資訊，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。如需更多詳細資訊，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。如需更多詳細資訊，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 (ASO)

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

行為圖表

從傳入來源資料產生的連結資料集，該資料與一個或多個 AWS 帳戶 相關聯。

每個行為圖表都使用相同的調查結果、實體和關係。

委派管理員帳戶 (AWS Organizations)

在組織中，服務的委派管理員帳戶能夠管理組織服務的使用情況。

在 Detective 中，Detective 管理員帳戶也是委派的管理員帳戶，除非 Detective 管理員帳戶是組織管理帳戶。組織管理帳戶無法成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。如需更多詳細資訊，請參閱 the section called “指定 Detective 管理員帳戶”。

Detective 建議組織管理帳戶選擇其帳戶以外的帳戶。

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

Detective 來源資料

來自以下摘要類型的已處理、結構化資訊版本：

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

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

實體

從擷取資料中擷取的項目。

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

實體可以是您管理的 AWS 資源，也可以是與資源互動的外部 IP 地址。

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

問題清單

Amazon GuardDuty 偵測到的安全問題。

調查結果群組

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

Detective 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。

調查結果概觀

提供調查結果資訊摘要的單一頁面。

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

調查結果概觀也包含含有調查結果屬性的詳細資訊面板。

大量實體

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

當目前的範圍時間包含大量的時間間隔時，Detective 會通知使用者。

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

調查

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

成員帳戶

管理員帳戶邀請將資料提供至行為圖表的受邀 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。如需更多詳細資訊，請參閱 the section called “針對成員帳戶：管理邀請和成員資格”。

組織帳戶無法在組織行為圖表中變更其成員資格。

所有成員帳戶也可以在提供資料的行為圖表中檢視其帳戶的用量資訊。

他們沒有對行為圖表的其他存取。

組織行為圖表

Detective 管理員帳戶所擁有的行為圖表。組織管理帳戶會指定 Detective 管理員帳戶。如需更多詳細資訊，請參閱 the section called “指定 Detective 管理員帳戶”。

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

Detective 管理員帳戶也可以邀請其他帳戶加入組織行為圖表。

設定檔

提供與實體活動相關資料視覺化集合的單一頁面。

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

檔案提供資訊以支援對某項調查結果進行調查，或用於常規尋找可疑活動。

設定檔面板

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

設定檔面板可以包含鍵值對、資料表、時間軸、長條圖或地理位置圖。

關係

個別實體之間發生的活動。也會從引入來源資料中擷取關係。

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

範圍名稱

用於設定檔上顯示資料範圍的時間範圍。

調查結果的預設範圍時間會反映觀察到可疑活動的首次和末次時間。

實體設定檔的預設範圍時間為前 24 小時。

Amazon Detective 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 可用的 AWS 區域 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。

設定 Amazon Detective

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 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"。

目錄

Amazon Detective 的先決條件和建議

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。作為最佳安全實務，將管理存取權指派給管理使用者，並且僅使用根使用者來執行需要根使用者存取權的任務。

AWS 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。

建立管理使用者

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)。

建立管理使用者

1. 啟用 IAM Identity Center。

   如需指示，請參閱 AWS IAM Identity Center 使用者指南中的啟用 AWS IAM Identity Center。
2. 在 IAM Identity Center 中，將管理權限授予管理使用者。

   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」。

以管理員的身分登入

- 若要使用您的 IAM 身分中心使用者登入，請使用建立 IAM 身分中心使用者時傳送至您電子郵件地址的登入 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。

您也必須注意以下要求和建議。

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。

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。

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

當您啟用 Detective 時，您可以指定 Detective 管理員帳戶，並邀請其他帳戶成為會員帳戶。當潛在成員帳戶接受邀請時，就會建立管理員與成員關係。如需詳細資訊，請參閱管理帳戶。

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。有關如何管理 Detective 管理員帳戶的詳細資訊，請參閱指定組織的 Detective 管理員帳戶。

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。然後開啟 Detective 主控台，網址為 https://console.aws.amazon.com/detective/。
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. 透過附加 IAM 政策 按鈕，您會直接導向至 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詳細資訊，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，請參閱使用Amazon Detective Python 指令碼。

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。

對於初始萃取，資料通常會在 2 小時內在行為圖中提供。

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. 開啟位於 https://console.aws.amazon.com/detective/ 的 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數據並擷取到您的行為圖表中。

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。有關如何跟踪 Detective 活動，監控用量並查看預計成本的更多資訊，請參閱 追蹤 Amazon Detective 的動作和用量。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”。

可選資料來源的免費試用

Detective 還為可選資料來源提供 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。

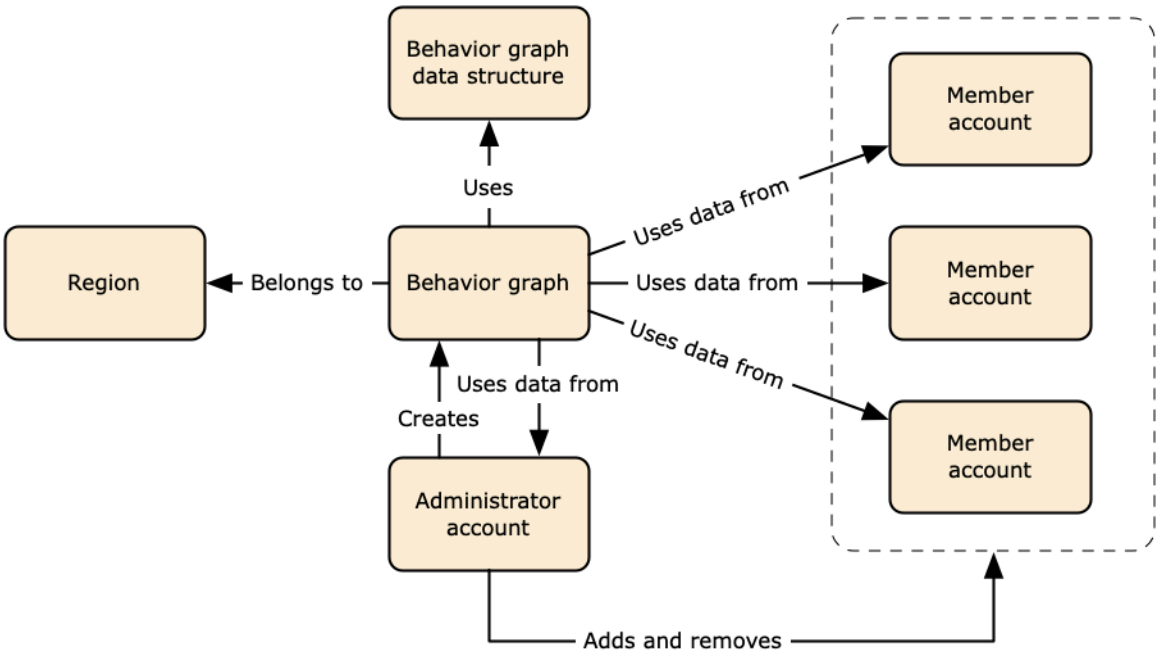
> **Note**
>
> 如果客戶在啟用選用的資料來源套件後 7 天內停用選用資料來源套件，則 Detective 會對該資料來源套件執行一次性自動重設免費試用 (如果再次啟用)。

若要啟用或停用選用的資料來源，請參閱 Detective 中可選資料來源的類型。

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數據。此資料可透過一組視覺化取得，視覺化可顯示已選取時間範圍內活動類型和數目的變化。Detective 將此類變更連結至 GuardDuty 調查結果。



如需有關行為圖表資料結構的詳細資訊，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 會從以下類型的 AWS 記錄擷取資料：

- AWS CloudTrail 日誌
- Amazon Virtual Private Cloud (Amazon VPC) 流程日誌
- 針對已註冊加入 GuardDuty 的帳戶，Detective 也會擷取 GuardDuty 的調查結果。

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

Detective 中可選資料來源的類型

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

Detective 為每個區域的所有核心和可選來源套件提供 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。如需詳細資訊，請參閱 針對 Detective 的 Amazon EKS 審核日誌。
- AWS 安全調查結果

  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 安全調查結果。

啟動或停止選用的資料來源：

1. 打開 Detective 主控台，網址為 https://console.aws.amazon.com/detective/。
2. 在導覽窗格中，於設定下選擇一般。
3. 在可選來源套件下，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 可選資料來源的免費試用。

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

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

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

新增或移除 Amazon EKS 稽核日誌作為選用資料來源：

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

AWS 安全調查結果

AWS 安全調查結果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 可選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 安全調查結果作為選用資料來源：

> **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 安全調查結果資料來源。針對 2023 年 5 月 16 日之前建立的行為圖表，必須手動啟用。

1. 打開 Detective 主控台，網址為 https://console.aws.amazon.com/detective/。
2. 在導覽窗格中，於設定下選擇一般。
3. 在來源套件下，選取 AWS 安全調查結果以啟用此資料來源。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 AWS 擁有的服務中擷取 Security Hub 中的所有 ASFF 調查結果。

- 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。
- 系統不會對合規狀態未設爲 `FAILED` 的 AWS 服務調查結果和跨區域彙總調查結果進行擷取。

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數據進行調查。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，讓資料量低於配額。此舉可以簡化重新啟用行為圖表的資料擷取程序。

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。如需在行為圖表中追蹤每個帳戶資料量的資訊，請參閱 the section called “管理員帳戶用量和費用”。

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 來管理帳戶，則組織管理帳戶會為該組織指定 Detective 管理員帳戶。該 Detective 管理員帳戶會成為組織行為圖表的管理員帳戶。

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

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

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

將管理員帳戶與 Security Hub 和 GuardDuty 對齊

為了確保與 AWS Security Hub 和 Amazon GuardDuty 的整合能夠順利進行，我們建議所有此類服務中的管理員帳戶使用相同帳戶。

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

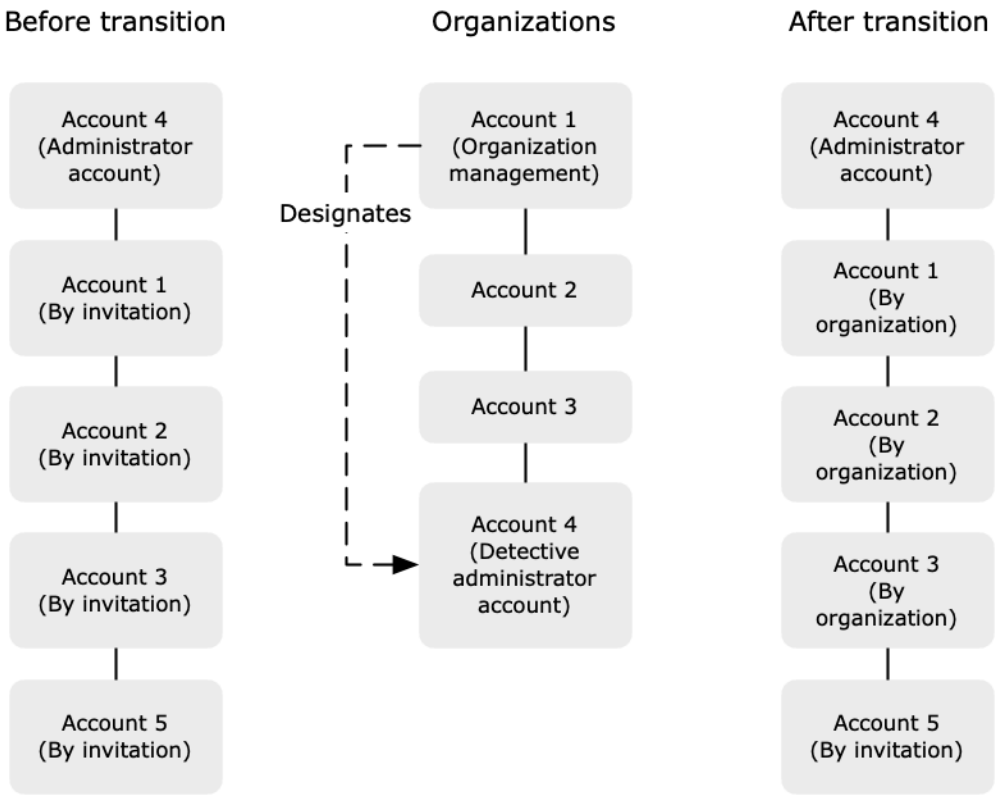
您可能具有現有行為圖表，其中包含接受手動邀請的成員帳戶。如果您已註冊 AWS Organizations，請使用以下步驟來使用組織來啟用和管理成員帳戶，不必使用手動邀請程序：

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。

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。
- 本人：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。

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	本人 (檢視管理員帳戶)	本人 (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	–	Self
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	Self	Self	–	–
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	–	–

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

組織管理帳戶會為各 AWS 區域 中的組織指定 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 的委派管理員帳戶是 Detective 在 AWS Organizations 中的管理員帳戶。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。

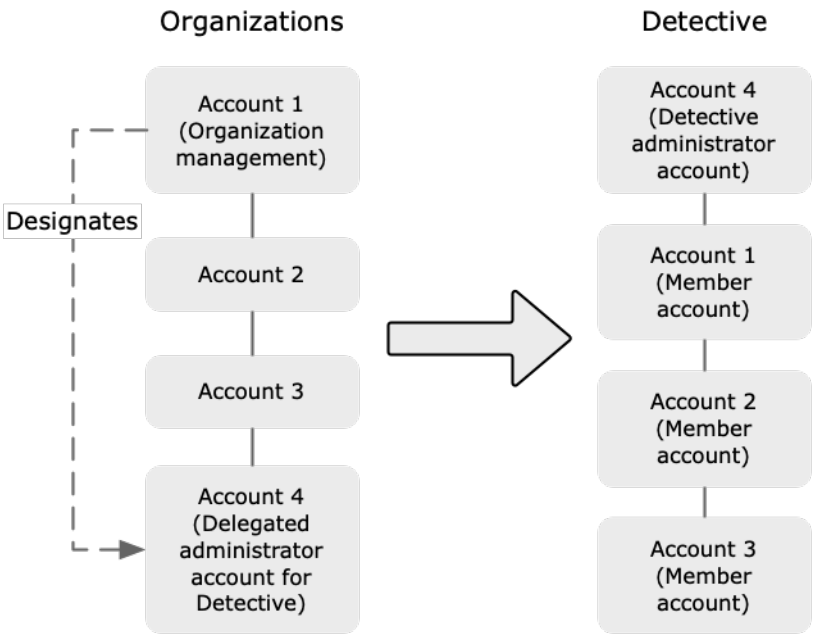
在組織中設定委派的管理員帳戶之後，組織管理帳戶只能選擇委派的管理員帳戶或他們自己的帳戶作為 Detective 管理員帳戶。我們建議您在所有區域中選擇委派的管理員帳戶。

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受管政策附加到您的 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. 開啟位於 https://console.aws.amazon.com/detective/ 的 Amazon Detective 主控台。
2. 選擇 Get started (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、Amazon Macie 或 AWS Security Hub 的組織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. 開啟位於 https://console.aws.amazon.com/detective/ 的 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、Amazon Macie 或 AWS Security Hub 的組織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. 開啟位於 https://console.aws.amazon.com/detective/ 的 Amazon Detective 主控台。
2. 選擇 Get started (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. 開啟位於 https://console.aws.amazon.com/detective/ 的 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 管理員帳戶 (Detective API，AWS CLI)

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

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

> **Important**
>
> 移除 Detective 管理員帳戶不會影響組織中委派的管理員帳戶。

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

- Detective API：使用 `DisableOrganizationAdminAccount` 操作。

  當您使用 Detective API 移除 Detective 管理員帳戶時，只會在發出 API 呼叫或指令的區域中移除該帳戶。
- AWS CLI：在命令列中執行 `disable-organization-admin-account` 命令。

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

移除委派的管理員帳戶 (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
```

檢視帳戶清單

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

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

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

正在進行中的驗證

針對受邀帳戶，Detective 會在傳送邀請之前驗證帳戶電子郵件地址。

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

驗證失敗

驗證失敗。邀請未傳送，或組織帳戶未啟用為成員。

已邀請

針對受邀帳戶。邀請已傳送，但成員帳戶尚未回應。

非成員

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

已啟用

針對受邀帳戶，成員帳戶接受邀請，並將資料提供至行為圖表。

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

未啟用

針對受邀帳戶，成員帳戶已接受邀請，但無法啟用。

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

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

Detective 會檢查您的資料量是否在 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。如果行為圖資料量的目前擷取量超過每天 10 TB 的限制，則 Detective 將不允許您新增其他成員帳戶。

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。開啟 Detective 主控台，網址為 https://console.aws.amazon.com/detective/。
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
- 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. 若要移除篩選器，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。

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

Detective 會檢查您的資料量是否在 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。如果目前擷取的磁碟區超過每天 10 TB 的限制，您就無法新增更多帳號，Detective 將停用進一步擷取資料。

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. 開啟位於 https://console.aws.amazon.com/detective/ 的 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。帳戶不會將資料提供至行為圖表。

一旦成員帳戶得以啟用，Detective 會自動將成員帳戶狀態變更為已啟用。例如，如果管理員帳戶移除其他成員帳戶以為帳戶騰出空間，則成員帳戶狀態會變更為 [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. 開啟位於 https://console.aws.amazon.com/detective/ 的 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. 開啟位於 https://console.aws.amazon.com/detective/ 的 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。如果帳戶資訊有效，Detective 會將邀請傳送至成員帳戶。

   Detective 不會執行此驗證，也不會傳送電子郵件邀請至下列區域的會員帳戶：

   - AWS GovCloud (美國東部) 區域

- AWS GovCloud (美國西部) 區域

對於其他地區，您可以`DisableEmailNotification`使用 Detective API 的CreateMembers操作。如果設置`DisableEmailNotification`為 true，則 Detective 不會向會員帳戶發送邀請。對於集中管理的帳戶而言，這是一個有用的設定。

3. 成員帳戶將接受或拒絕邀請。

   即使管理員帳戶未發送邀請電子郵件，成員帳戶仍然必須回應邀請。

4. 成員帳戶接受邀請後，Detective 會開始將成員帳戶中的資料擷取到行為圖表中。
5. 一旦成員帳戶符合啟用資格，Detective 會自動將成員帳戶狀態變更為已啟用。

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

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

   管理員帳戶也可以手動啟用帳戶，而不必等待自動程序。例如，管理員帳戶可能想要選取要啟用的帳戶。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. 開啟位於 https://console.aws.amazon.com/detective/ 的 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. 開啟位於 https://console.aws.amazon.com/detective/ 的 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，請參閱使用Amazon Detective Python 指令碼。

啟用未啟用的成員帳戶

會員帳戶接受邀請後，Amazon Detective 會檢查會員帳戶的數量。行為圖表中成員帳戶的數目上限為 1,200。如果行為圖表已包含 1,200 個成員帳戶，則無法啟用新帳戶。如果 Detective 無法啟用成員帳戶，則會將成員帳戶狀態設定為未啟用。

未啟用的成員帳戶不會將資料提供至行為圖表。

Detective 會自動啟用帳戶，因為行為圖表可以容納帳戶。

您也可以嘗試手動啟用未啟用成員帳戶的成員帳戶。例如，您可以移除現有的成員帳戶以減少資料量。您可以嘗試啟用未啟用成員帳戶，不必等待啟用帳戶的自動程序。

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. 開啟位於 https://console.aws.amazon.com/detective/ 的 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. 開啟位於 https://console.aws.amazon.com/detective/ 的 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，請參閱使用Amazon Detective Python 指令碼。

針對成員帳戶：管理行為圖表邀請和成員資格

Amazon Detective 會針對每個成員帳戶所提供的每個行為圖表，收取擷取的資料費用。

透過帳戶管理頁面，成員帳戶可以查看其所屬行為圖表的管理員帳戶。

受邀加入行為圖表的成員帳戶可以檢視並回應其邀請。他們也可以將自己的帳戶從行為圖表中移除。

針對組織行為圖表，組織帳戶不會控制其帳戶是否為成員帳戶。Detective 管理員帳戶會選擇要作為成員帳戶啟用或停用的組織帳戶。

目錄

成員帳戶所需的 IAM 政策

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。開啟 Detective 主控台，網址為 https://console.aws.amazon.com/detective/。
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。

  如果您的帳號不會導致行為圖表超出 Detective 配額，Detective 會將您的帳號狀態更新為 [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

在您接受邀請後，Detective 會檢查會員帳號的數量。行為圖表中成員帳戶的數目上限為 1,200。如果行為圖表已包含 1,200 個成員帳戶，則無法啟用新帳戶。

接受邀請後，您的帳戶就會啟用 Detective 功能。Detective 會檢查您的資料量是否在 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。如果目前擷取的磁碟區超過每天 10 TB 的限制，您就無法新增更多帳號，Detective 將停用進一步擷取資料。Detective 主控台會顯示通知，指出資料磁碟區太大且狀態仍維持「未啟用」狀態。

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. 開啟位於 https://console.aws.amazon.com/detective/ 的 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。

若要接受行為圖形邀請 (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. 開啟位於 https://console.aws.amazon.com/detective/ 的 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 帳戶遭到暫停

當管理員帳戶在 AWS 中暫停時，帳戶會失去檢視 Detective 中行為圖表的許可。Detective 停止將資料擷取至行為圖表中。

當某個成員帳戶在 AWS 暫停時，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 帳戶關閉

當 AWS 帳戶關閉時，Detective 對關閉作出如下回應。

- 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 會將帳戶的政策資料保留 90 天，自您管理員帳戶關閉生效日起算。在 90 天期結束時，AWS 會永久刪除帳戶的所有政策資料。

- 若要保留問題清單超過 90 天，您可以封存政策。您也可以將自訂動作與 EventBridge 規則搭配使用，將問題清單存放在 S3 儲存貯體中。
- 只要 AWS 會保留政策資料，當您重新開啟已關閉的帳戶時，AWS 會將帳戶重新指派為服務管理員，並復原帳戶的服務政策資料。
- 如需詳細資訊，請參閱關閉帳戶。

> **Important**
>
> 對於 AWS GovCloud (US) 區域的客戶：
>
> - 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。

追蹤 Amazon Detective 的動作和用量

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 還支援 AWS CloudTrail 記錄。

目錄

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。然後開啟 Detective 主控台，網址為 https://console.aws.amazon.com/detective/。
2. 在 Detective 導覽窗格中的設定下，選擇用量。
3. 選擇標籤以依資料來源或依帳戶選取檢視用量。

為每個帳戶擷取的資料量

依成員帳戶擷取的資料量會在行為圖表中列出作用中帳戶。它不會列出已移除的成員帳戶。

針對每個帳戶，擷取的資料量清單會提供以下資訊。

- AWS 帳戶識別符和根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 日誌、VPC 流程日誌和 GuardDuty 調查結果) 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。然後開啟 Detective 主控台，網址為 https://console.aws.amazon.com/detective/。
2. 在 Detective 導覽窗格中的設定下，選擇用量。

每個行為圖表的擷取量

此帳戶的擷取量會列出成員帳戶提供的行為圖表。它不包括您放棄的成員資格或管理員帳戶移除的成員資格。

針對每個行為圖表，清單包含以下資訊：

- 管理員帳戶的帳號
- 過去 30 天內從成員帳戶擷取的資料量。總計包括所有來源類型。
- 成員帳戶啟用行為圖表的日期。

跨行為圖表的預計成本

此帳戶的預計成本會在其提供的所有行為圖表中，顯示成員帳戶 30 天資料的預計成本。預計成本根據成員帳戶的每日平均值而定。

> **Important**
>
> 此金額僅為預計成本。它會預測管理員帳戶資料在 30 天期間內的總常規成本。它基於前 30 天的用量。請參閱 the section called “Detective 如何計算預計成本”。

Amazon Detective 如何計算預計成本

若要計算它顯示在用量頁面上顯示的預計成本值，Detective 會執行以下動作。

1. 若要在行為圖表中取得個別帳戶的預計成本，Detective 會執行以下動作。
   a. 計算每天的平均值。它會在所有作用中日期中新增資料量，然後除以帳戶處於作用中狀態的天數。

      如果帳戶在 30 天前已啟用，則天數為 30 天。如果帳戶的啟用時間短於 30 天，則天數為該帳戶自接受日期以來的天數。

      例如，如果帳戶在 12 天前啟用，則 Detective 會新增 12 天內所擷取的資料量，然後將其除以 12。
   b. 將帳戶的每日平均值乘以 30。所得即爲帳戶的預計 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 AWS CloudTrail 記錄 Amazon Detective API 呼叫

Detective 已與 AWS CloudTrail 整合，該服務提供由使用者、角色或 Detective 中的 AWS 服務所採取動作的記錄。CloudTrail 會將 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。

- 若您建立追蹤，便可將 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 Detective 的事件。
- 即使您未設定追蹤，依然可以透過 CloudTrail 主控台中的事件歷史記錄檢視最新事件。

您可以使用 CloudTrail 收集的資訊來判斷以下項目：

- 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《AWS CloudTrail 使用者指南》。

CloudTrail 中的 Detective 資訊

當您建立帳戶時，系統即會在 AWS 帳戶中啟用 CloudTrail。當 Detective 中發生活動時，該活動會記錄在 CloudTrail 事件中，其他 AWS 服務事件則記錄於事件歷史記錄中。您可以檢視、搜尋和下載 AWS 帳戶的最新事件。如需詳細資訊，請參閱使用 CloudTrail 事件歷史記錄檢視事件。

如需 AWS 帳戶中正在進行事件的記錄 (包含 Detective 的事件)，請建立追蹤。追蹤能讓 CloudTrail 將日誌檔交付至 Amazon S3 儲存貯體。

根據預設，當您在主控台建立線索時，線索會套用到所有 AWS 區域。該追蹤會記錄來自 AWS 分割區中所有區域的事件，並將日誌檔案交付到您指定的 Amazon S3 儲存貯體。您還可設定其他 AWS 服務，以進一步分析和處理 CloudTrail 記錄中所收集的事件資料。

如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務和整合
- 設定 CloudTrail 的 Amazon SNS 通知
- 從多個區域接收 CloudTrail 日誌檔案，以及從多個帳戶接收 CloudTrail 日誌檔案

CloudTrail 會記錄所有 Detective 操作，此類作業記錄在 Detective API 參考資料中。

例如，對 `CreateMembers`、`AcceptInvitation` 和 `DeleteMembers` 操作的呼叫都會在 CloudTrail 日誌檔案中產生項目。

每一筆事件或日誌項目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：

- 該請求是否使用根或 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
- 該請求是否由另一項 AWS 服務提出

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

了解 Detective 日誌檔案項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一個或多個日誌項目。

事件代表來自任何來源的單一請求。事件包含請求的動作、動作的日期和時間、請求參數等相關資訊。CloudTrail 日誌檔並非依公有 API 呼叫的堆疊追蹤排序，因此項目不會以任何特定順序出現。

以下範例顯示的是展示 `AcceptInvitation` 動作的 CloudTrail 日誌項目。

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

```
            "CloudTrailEvent": "{\"eventVersion\":\"1.05\",\"userIdentity\":
{\"type\":\"AssumedRole\",\"principalId\":\"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": []
        },
```

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，您可以在 AWS Cost Explorer 中搜尋該標籤，以查看此類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. 開啟位於 https://console.aws.amazon.com/detective/ 的 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 取得行為圖表的標籤清單。

要取得行為圖表的標籤清單 (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表 (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表。

若要將標籤新增至行為圖表 (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 AWS CLI，從行為圖表中移除標籤值。

若要從行為圖表 (Detective APIAWS CLI) 中移除標籤

- 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"
```

Amazon Detective 中的安全

雲端安全是 AWS 最重視的一環。身為 AWS 客戶的您，將能從資料中心和網路架構的建置中獲益，以滿足組織最為敏感的安全要求。

安全是 AWS 與您共同的責任。共同的責任模型 將此描述為雲端 本身 的安全和雲端內部的安全：

- 雲端本身的安全 – AWS 負責保護在 AWS Cloud 中執行 AWS 服務的基礎設施。AWS 也提供您可安全使用的服務。

  在 AWS 合規計畫中，第三方稽核員會定期測試並驗證我們的安全功效。

  若要了解適用於 Amazon Detective 的合規計劃，請參閱《合規計劃範圍內的 AWS 服務》。
- 雲端內部的安全 – 您的責任取決於所使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您公司的請求和適用法律和法規。

本文件有助於您了解如何在使用 Detective 時套用共同責任模型。以下主題說明如何將 Detective 設定為達到您的安全及法規遵循目標。您也會了解如何使用其他 AWS 服務來協助監控並保護 Detective 資源。

目錄

Amazon Detective 中的資料保護

AWS 共同的責任模型適用於 Amazon Detective 中的資料保護。如此模型所述，AWS 負責保護執行所有 AWS 雲端 的全球基礎設施。您負責維護在此基礎設施上託管內容的控制權。您也必須負責您所使

用 AWS 服務 的安全組態和管理任務。如需有關資料隱私權的更多相關資訊，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，建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 憑證，並設定個人使用者。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 資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用 AWS CloudTrail 設定 API 和使用者活動日誌記錄。
- 使用 AWS 加密解決方案，以及 AWS 服務 內的所有預設安全控制項。
- 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 AWS 時，需要 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 Name (名稱) 欄位。這包括當您使用主控台、API、AWS CLI 或 AWS 開發套件操作 Detective 或其他 AWS 服務 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《AWS Key Management Service 開發人員指南》中對 AWS 擁有的金鑰的說明。

此類型的 KMS 金鑰每年 (大約 365 天) 會自動輪換。請參閱《AWS Key Management Service 開發人員指南》中對金鑰輪換的說明。

Amazon Detective 的身分和存取管理

AWS Identity and Access Management (IAM) 是一種 AWS 服務，讓管理員能夠安全地控制對 AWS 資源的存取權。IAM 管理員可以控制完成身分驗證 (已登入) 和獲得授權 (具有許可) 而得以使用 Detective 資源的對象。IAM 是一種您可以免費使用的 AWS 服務。

目錄

對象

AWS Identity and Access Management (IAM) 的使用方式會有所不同，取決於您在 Detective 中所執行的工作。

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 中的某項特徵，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

身分驗證是使用身分憑證登入 AWS 的方式。您必須以 AWS 帳戶根使用者、IAM 使用者身分，或擔任 IAM 角色進行 驗證（登入至 AWS）。

您可以使用透過身分來源 AWS IAM Identity Center 提供的憑證，以聯合身分登入 AWS。(IAM Identity Center) 使用者、貴公司的單一登入身分驗證和您的 Google 或 Facebook 憑證都是聯合身分的範例。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。您 AWS 藉由使用聯合進行存取時，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。如需有關登入至 AWS 的更多相關資訊，請參閱《AWS 登入 使用者指南》中的如何登入您的 AWS 帳戶。

如果您是以程式設計的方式存取 AWS，AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以便使用您的憑證透過密碼編譯方式簽署您的請求。如果您不使用 AWS 工具，您必須自行簽署請求。如需使用建議的方法自行簽署請求的更多相關資訊，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) 以提高帳戶的安全。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

如果是建立 AWS 帳戶，您會先有一個登入身分，可以完整存取帳戶中所有 AWS 服務 與資源。此身分稱為 AWS 帳戶 根使用者，使用建立帳戶時所使用的電子郵件地址和密碼即可登入並存取。強烈建議您不要以根使用者處理日常作業。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 AWS 帳戶 中的一種身分，具備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。您無法以群組身分登入。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過程變得更為容易。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 中的一種身分，具備特定許可。它類似 IAM 使用者，但不與特定的人員相關聯。您可以在 AWS Management Console 中透過切換角色來暫時取得 IAM 角色。您可以透過呼叫 AWS CLI 或 AWS API 操作，或是使用自訂 URL 來取得角色。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 — 如需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，並取得由角色定義的許可。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。
- 跨帳户存取權 – 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。角色是授予跨帳户存取權的主要方式。但是，針對某些 AWS 服務，您可以將政策直接連接到資源（而非使用角色作為代理）。若要了解跨帳户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。
- 跨服務存取 – 有些 AWS 服務 會使用其他 AWS 服務 中的功能。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。
  - 轉發存取工作階段 (FAS)：當您使用 IAM 使用者或角色在 AWS 中執行動作時，系統會將您視為主體。當您使用某些服務時，您可能會執行一個動作，而該動作之後會在不同的服務中啟動另一個動作。FAS 使用主體的許可呼叫 AWS 服務，搭配請求 AWS 服務 以向下游服務發出請求。只有在服務收到需要與其他 AWS 服務 或資源互動才能完成的請求之後，才會提出 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》https://docs.aws.amazon.com/IAM/latest/UserGuide/access_forward_access_sessions.html。
  - 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。
  - 服務連結角色 – 服務連結角色是一種連結到 AWS 服務 的服務角色類型。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 AWS 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。

- 在 Amazon EC2 上執行的應用程式 – 針對在 EC2 執行個體上執行並提出 AWS CLI 和 AWS API 請求的應用程式，您可以使用 IAM 角色來管理暫時憑證。這是在 EC2 執行個體內儲存存取金鑰的較好方式。如需指派 AWS 角色給 EC2 執行個體並提供其所有應用程式使用，您可以建立連接到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

您可以透過建立政策並將其連接到 AWS 身分或資源，在 AWS 中控制存取。政策是 AWS 中的一個物件，當其和身分或資源建立關聯時，便可定義其許可。AWS 會在主體（使用者、根使用者或角色工作階段）發出請求時評估這些政策。政策中的許可決定是否允許或拒絕請求。大部分政策以 JSON 文件形式儲存在 AWS 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。若要授與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。具備該政策的使用者便可以從 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。受管政策則是獨立的政策，您可以將這些政策連接到 AWS 帳戶 中的多個使用者、群組和角色。受管政策包含 AWS 管理政策和客戶管理政策。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。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。主體可以包括帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

資源型政策是位於該服務中的內嵌政策。您無法在資源型政策中使用來自 IAM 的 AWS 受管政策。

存取控制清單 (ACL)

存取控制清單 (ACL) 可控制哪些委託人（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 Simple Storage Service (Amazon S3)、AWS WAF 和 Amazon VPC 是支援 ACL 的服務範例。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 支援其他較少見的政策類型。這些政策類型可設定較常見政策類型授與您的最大許可。

- 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。
- 服務控制政策 (SCP) – SCP 是 JSON 政策，可指定 AWS Organizations 中組織或組織單位 (OU) 的最大許可。AWS Organizations 服務可用來分組和集中管理您企業所擁有的多個 AWS 帳戶。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 會限制成員帳戶中實體的許可，包括每個 AWS 帳戶根使用者。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。若要了解 AWS 在涉及多種政策類型時如何判斷是否允許一項請求，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，IAM 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 執行任務。IAM 管理員必須建立 AWS Identity and Access Management (IAM) 政策，授予 IAM 使用者和角色在所需指定資源上執行特定 API 操作的所需許可。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。他們也會使用行為圖表來分類和調查與此類帳戶相關聯的調查結果和資源。

  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。

若要取得 Detective 和其他 AWS 服務 如何使用 IAM 的詳細資訊，請參閱《IAM 使用者指南》中的在 JSON 標籤上建立政策。

Detective 身分型政策

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。Detective 支援特定動作、資源和條件金鑰。

若要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的 JSON 政策元素參考。

動作

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。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。政策動作的名稱通常會和相關聯的 AWS API 操作相同。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。也有一些操作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與執行相關聯操作的許可。

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。

如需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"
```

如要查看 ACM 動作的清單，請參閱《服務授權參考》中由 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 (例如列出作業)，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 Resource Name (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 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。

條件金鑰

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。若您為單一條件索引鍵指定多個值，AWS 會使用邏輯 OR 操作評估條件。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與該 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的條件金鑰。若要查看 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 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 帳戶中具備特定許可的實體。

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。您取得暫時安全憑證的方式是透過呼叫 AWS STS API 操作（例如，AssumeRole 或 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 執行任務。

IAM 管理員必須建立 IAM 政策，授予使用者和角色在指定資源上執行特定 API 操作的所需許可。管理員接著必須將此類政策附加至需要此類許可的 IAM 使用者或群組。

若要了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的在 JSON 索引標籤上建立政策。

主題

- 政策最佳實務
- 使用 Detective 主控台
- 允許使用者檢視自己的許可
- 管理員帳戶：在行為圖表中管理成員帳戶
- 管理員帳戶：使用行為圖表進行調查
- 成員帳戶：管理行為圖表邀請和成員資格
- 管理員帳戶：根據標籤值限制存取許可

政策最佳實務

身分型政策會判斷您帳戶中的某個人員是否可以建立、存取或刪除 Detective 資源。這些動作可能會讓您的 AWS 帳戶 產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管政策並朝向最低權限許可的目標邁進：如需開始授予許可給使用者和工作負載，請使用 AWS 受管政策，這些政策會授予許可給許多常用案例。它們可在您的 AWS 帳戶 中使用。我們建議您定義特定於使用案例的 AWS 客戶管理政策，以便進一步減少許可。如需更多資訊，請參閱 IAM 使用者指南中的 AWS 受管政策或任務職能的 AWS 受管政策。
- 套用最低許可許可 – 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予對服務動作的存取權，前提是透過特定 AWS 服務（例如 AWS CloudFormation）使用條件。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。
- 需要多重要素驗證 (MFA)：如果存在需要 AWS 帳戶中 IAM 使用者或根使用者的情況，請開啟 MFA 提供額外的安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，請參閱 IAM 使用者指南中的設定 MFA 保護的 API 存取。

有關 IAM 中最佳實務的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 最佳安全實務。

使用 Detective 主控台

若要使用 Amazon Detective 主控台，使用者或角色必須能夠存取相關動作，此類動作與 API 中的對應動作相符。

若要啟用 Detective 並成為行為圖表的管理員帳戶，必須向使用者或角色授予 `CreateGraph` 動作的許可。

若要使用 Detective 主控台執行任何管理員帳戶動作，必須向使用者或角色授予 `ListGraphs` 動作的許可。這會授予擷取其帳戶為管理員帳戶行為圖表的許可。他們也必須獲得執行特定管理員帳戶動作的許可。

最基本的管理員帳戶動作是檢視行為圖表中的成員帳戶清單，並使用行為圖表進行調查。

- 若要檢視行為圖表中的成員帳戶清單，必須向主體授予 `ListMembers` 動作的許可。
- 若要在行為圖表中進行調查，必須向主體授予 `SearchGraph` 動作的許可。

若要使用 Detective 主控台執行任何成員帳戶動作，必須向使用者或角色授予 `ListInvitations` 動作的許可。這會授予檢視行為圖表邀請的許可。然後，他們可以被授予特定成員帳戶動作的許可。

允許使用者檢視自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視連接到他們使用者身分的內嵌及受管政策。此政策包含在主控台上，或是使用 AWS CLI 或 AWS API 透過編寫程式的方式完成此動作的許可。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

管理員帳戶：在行為圖表中管理成員帳戶

此範例政策適用於僅負責管理行為圖表中使用的成員帳戶的管理員帳戶使用者。透過此政策，使用者也可以檢視用量資訊，並停用 Detective。此政策未授予使用行為圖表進行調查的許可。

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

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 拒絕存取問題或類似困難，請參閱《IAM 使用者指南》中的故障診斷 IAM 主題。

我未獲授權，不得在 Detective 中執行動作

若 AWS Management Console 告知您並未獲得執行動作的授權，您必須聯絡您的管理員以取得協助。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。

我未獲得執行 iam:PassRole 的授權

如果錯誤訊息告知您未獲得授權，無法執行 `iam:PassRole` 動作，您必須更新政策，以允許您將角色傳遞給 Detective。

有些 AWS 服務 允許您傳遞現有的角色至該服務，而無須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，該動作要求服務具備服務角色授與的許可。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。

如需任何協助，請聯絡您的 AWS 管理員。您的管理員提供您的登入憑證。

我想要允許 AWS 帳戶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的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對象取得該角色。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。
- 如需了解如何存取您擁有的所有 AWS 帳戶 所提供的資源，請參閱 IAM 使用者指南中的將存取權提供給您所擁有的另一個 AWS 帳戶 中的 IAM 使用者。
- 如需了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱 IAM 使用者指南中的將存取權提供給第三方擁有的 AWS 帳戶。
- 如需了解如何透過聯合身分提供存取權，請參閱 IAM 使用者指南中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。
- 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。

使用 Detective 的服務連結角色

Amazon Detective 使用 AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結至 Detective 的一種特殊 IAM 角色類型。服務連結角色由 Detective 預先定義，並包含該服務代您呼叫其他 AWS 服務所需的所有許可。

服務連結角色可簡化 Detective 的設定，因為您不必手動新增必要的許可。Detective 定義其服務連結角色的許可，除非另有定義，否則僅有 Detective 可以擔任其角色。定義的許可包括信任政策和許可政策，並且該許可政策不能連接到任何其他 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 會使用名為 AWSServiceRoleForDetective 的服務連結角色，這將允許 Detective 代您存取 AWS Organizations 資訊。

AWSServiceRoleForDetective 服務連結角色信任以下服務可擔任該角色：

- `detective.amazonaws.com`

AWSServiceRoleForDetective 服務連結角色會使用受管政策，即 `AmazonDetectiveServiceLinkedRolePolicy`。

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。當您為 AWS Management Console、AWS CLI 或 AWS API 中的組織指定 Detective 管理員帳戶時，Detective 可為您建立服務連結的角色。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您為組織指定 Detective 管理員帳戶時，Detective 可再次為您建立服務連結角色。

為 Detective 編輯服務連結角色

Detective 不允許您編輯 AWSServiceRoleForDetective 服務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱《IAM 使用者指南》中的編輯服務連結角色。

為 Detective 刪除服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。然而，在手動刪除服務連結角色之前，您必須先清除資源。

> **Note**
>
> 若 Detective 服務在您試圖刪除資源時正在使用該角色，刪除可能會失敗。若此情況發生，請等待數分鐘後，然後再次嘗試操作。

若要刪除 AWSServiceRoleForDetective 所使用的 Detective 資源

1. 移除 Detective 管理員帳戶。請參閱 the section called “指定 Detective 管理員帳戶”。
2. 在您指定 Detective 管理員帳戶的每個區域中重複此程序。

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台、AWS CLI 或 AWS API 來刪除 AWSServiceRoleForDetective 服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的刪除服務連結角色。

Detective 服務連結角色支援的區域

Detective 支援在所有提供服務的區域中使用服務連結角色。如需詳細資訊，請參閱 AWS 區域與端點。

Amazon Detective 的 AWS 受管政策

AWS 管理的政策是由 AWS 建立和管理的獨立政策。AWS 管理的政策的設計在於為許多常見使用案例提供許可，如此您就可以開始將許可指派給使用者、群組和角色。

請謹記，AWS 管理的政策可能不會授予您特定使用案例的最低權限許可，因為它們可供所有 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。

您無法更改 AWS 管理的政策中定義的許可。如果 AWS 更新 AWS 管理的政策中定義的許可，更新會影響政策連接的所有主體身分 (使用者、群組和角色)。在推出新的 AWS 服務 或有新的 API 操作可供現有服務使用時，AWS 很可能會更新 AWS 管理的政策。

如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

AWS 受管政策：AmazonDetectiveFullAccess

您可將 AmazonDetectiveFullAccess 政策連接到 IAM 身分。

此政策會授予管理許可，允許主體完整存取所有 Amazon Detective 動作。您可以將此政策附加到主體，然後再針對帳戶啟用 Detective。它還必須附加到用於執行 Detective Python 指令碼以建立和管理行為圖表的角色。

具有此類許可的主體可以管理成員帳戶、將標籤新增至其行為圖表，以及使用 Detective 進行調查。他們還可以封存 GuardDuty 調查結果。此政策會提供 Detective 主控台所需許可，以顯示 AWS Organizations 中帳戶的帳戶名稱。

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：允許主體從 Detective 內部取得和封存 GuardDuty 調查結果。
- securityhub：允許主體從 Detective 中取得 Security Hub 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 受管政策：AmazonDetectiveMemberAccess

您可將 AmazonDetectiveMemberAccess 政策附加至 IAM 實體。

此政策會向成員提供 Amazon Detective 的存取，以及主控台的特定範圍存取。

使用此政策，您可以：

- 檢視向 Detective 圖表成員發出的邀請，並接受或拒絕邀請。
- 在用量頁面查看您在 Detective 中的活動如何影響使用此服務的成本。
- 放棄圖表中的成員資格。

此政策授予唯讀許可，允許在一定範圍內存取 Detective 主控台。

許可詳細資訊

此政策包含以下許可：

- `detective`：允許成員存取 Detective。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:AcceptInvitation",
        "detective:BatchGetMembershipDatasources",
        "detective:DisassociateMembership",
        "detective:GetFreeTrialEligibility",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListInvitations",
        "detective:RejectInvitation"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS 受管政策：AmazonDetectiveInvestigatorAccess

您可將 `AmazonDetectiveInvestigatorAccess` 政策附加至 IAM 實體。

此政策向調查人員提供對 Detective 服務的存取，以及 Detective 主控台 UI 相依性的特定範圍存取。此政策授予在 Detective 中對 IAM 使用者和 IAM 角色啟用 Detective 調查的許可。您可以使用調查報告來調查以識別調查結果等入侵指標，該報告提供有關安全指標的分析和見解。該報告按嚴重性進行排名，由 Detective 的行為分析和機器學習決定。您可以使用報告來排定資源修補的優先順序。

許可詳細資訊

此政策包含以下許可：

- `detective`：允許主體調查者存取 Detective 動作，以啟用 Detective 調查，以及啟用調查結果群組摘要。
- `guardduty`：允許主體從 Detective 內部取得和封存 GuardDuty 調查結果。
- `securityhub`：允許主體從 Detective 中取得 Security Hub 調查結果。
- `organizations`：允許主體從 AWS Organizations 中擷取組織中帳戶的相關資訊。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 受管政策：AmazonDetectiveOrganizationsAccess

您可將 AmazonDetectiveOrganizationsAccess 政策附加至 IAM 實體。

此政策授予在組織內啟用和管理 Amazon Detective 的許可。您可以在整個組織中啟用 Detective，並決定 Detective 的委派管理員帳戶。

許可詳細資訊

此政策包含以下許可：

- `detective`：允許主體存取 Detective 動作。
- `iam`：指定在 Detective 呼叫 `EnableOrganizationAdminAccount` 時建立服務連結角色。
- `organizations`：允許主體從 AWS Organizations 中擷取組織中帳戶的相關資訊。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，並允許主體擷取其他安全服務中的委派管理員帳戶，例如 Amazon Detective、Amazon GuardDuty、Amazon Macie 和 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。如需更多詳細資訊，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 受管政策的 Detective 更新

檢視自該服務開始追蹤變更以來的 Detective AWS 受管政策更新的詳細資訊。如需有關此頁面變更的自動提醒，請訂閱文件歷史記錄頁面上的 RSS 摘要。

變更	描述	日期
AmazonDetectiveInvestigatorAccess：現有政策的更新	在 AmazonDetectiveInvestigatorAccess 政策中新增	2023 年 11 月 26 日

變更	描述	日期
	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。	
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。 此政策會向成員提供 Detective 的存取，以及主控台 UI 依存關係的特定範圍存取。	2023 年 1 月 17 日
AmazonDetectiveFullAccess：現有政策的更新	Detective 向 `AmazonDetectiveFullAccess` 政策新增了 GuardDuty `GetFindings` 動作。 透過此類動作，可從 Detective 內部取得 GuardDuty 調查結果。	2023 年 1 月 17 日

變更	描述	日期
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 已開始追蹤其 AWS 受管政策的變更。	2021 年 5 月 10 日

在 Amazon Detective 中記錄和監控

Amazon Detective 已經集成 AWS CloudTrail。CloudTrail 會將 Detective 的所有 API 呼叫擷取為事件。

如需有關針對 Detective 使用 CloudTrail 記錄的詳細資訊，請參閱 the section called “使用 CloudTrail 記錄 API 呼叫”。

Amazon Detective 的合規驗證

Amazon Detective 屬於 AWS 保證計劃範圍之內。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內的 AWS 服務清單，請參閱合規計劃範圍內的 AWS 服務。如需一般資訊，請參閱 AWS 法規遵循方案。

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

AWS 提供下列資源，以協助實現合規性：

- 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。
- 《AWS Config 開發人員指南》中的使用規則評估資源 – AWS Config 服務會評估資源組態在內部實務、業界準則和法規方面的合規程度。
- AWS Security Hub：此 AWS 服務可供您檢視 AWS 中的安全狀態，可助您檢查是否符合安全產業標準和最佳實務。

Amazon Detective 中的彈性

AWS 全球基礎設施是以 AWS 區域與可用區域為中心建置的。AWS區域提供多個分開且隔離的實際可用區域，並以低延遲、高輸送量和高度備援聯網功能相互連結。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、容錯能力和擴充能力，均較單一或多個資料中心的傳統基礎設施還高。

如需有關 AWS 區域與可用區域的詳細資訊，請參閱 AWS 全球基礎設施。

除了 AWS 全球基礎設施外，Detective 還使用 Amazon DynamoDB 和 Amazon Simple Storage Service (Amazon S3) 中內建的彈性功能。

Detective 架構也可以抵禦單一可用區域的故障。彈性內置於 Detective 中，不需要任何組態。

Amazon Detective 的基礎設施安全

Amazon Detective 是一項受管服務，受到 AWS 全球網路安全的保護。如需有關 AWS 安全服務以及 AWS 如何保護基礎設施的詳細資訊，請參閱 AWS 雲端安全。若要使用基礎設施安全性的最佳實務來設計您的 AWS 環境，請參閱安全性支柱 AWS 架構良好的框架中的基礎設施保護。

您可使用 AWS 發佈的 API 呼叫來透過網路存取 Detective。用戶端必須支援下列項目：

- 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，請求必須使用存取索引鍵 ID 和與 IAM 主體相關聯的私密存取索引鍵來簽署。或者，您可以使用 AWS Security Token Service (AWS STS) 來產生暫時安全憑證來簽署請求。

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。

檢查傳送邀請的管理員帳戶的 AWS 帳戶識別符。確認您知道該帳戶的所屬資訊，以及邀請帳戶有合法理由監控您的安全資料。

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。

若要停用 Detective (主控台)

1. 開啟位於 https://console.aws.amazon.com/detective/ 的 Amazon Detective 主控台。
2. 在 Detective 導覽窗格中，於設定下選擇通用。
3. 在一般頁面的停用下，選擇停用。
4. 出現提示時，請輸入 **disable**。
5. 選擇停用。

停用 Detective (Detective API，AWS CLI)

您可以透過 Detective API 或 AWS Command Line Interface 停用 Amazon Detective。若要取得行為圖表的 ARN 以供在請求中使用，請使用 `ListGraphs` 操作。

若要停用 Detective (Detective API，AWS CLI)

- Detective API：使用 `DeleteGraph` 操作。您必須提供圖表 ARN。
- AWS CLI：在命令列中執行 `delete-graph` 命令。

```
aws detective delete-graph --graph-arn <graph ARN>
```

範例：

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

停用跨區域的 Detective (GitHub 上的 Python 指令碼)

Detective 在 GitHub 中提供了開源指令碼，您可以借此在指定的區域清單中停用管理員帳戶的 Detective。

如需有關如何設定和使用 GitHub 指令碼的資訊，請參閱 使用Amazon Detective Python 指令碼。

使用Amazon Detective Python 指令碼

Amazon Detective 在 GitHub 儲存庫 (amazon-detective-multiaccount-scripts) 中提供了一組開放原始 Python 指令碼。此類指令碼需要 Python 3。

您可透過下屬操作執行以下任務：

- 為跨區域的管理員帳戶啟用 Detective。

  啟用 Detective 後，您可以將標籤指派給行為圖表。
- 將成員帳戶新增至管理員帳戶的跨區域行為圖表。
- 可以選擇向成員帳戶發送邀請電子郵件。您還可以將請求設定為不發送邀請電子郵件。
- 將成員帳戶從管理員帳戶的跨區域行為圖表中移除。
- 為跨區域的管理員帳戶停用 Detective。當管理員帳戶停用 Detective 時，系統會停用每個區域中的管理員帳戶行為圖表。

enableDetective.py 指令碼概觀

enableDetective.py 指令碼會執行以下操作：

1. 如果管理員帳戶尚未在該區域中啟用 Detective，則為每個指定區域中的管理員帳戶啟用Detective。

   當您使用指令碼啟用 Detective 後，您可以將標籤指派給行為圖表。
2. 可以選擇將管理員帳戶發送的要求傳送至各行為圖表的指定成員帳戶。

   邀請電子郵件訊息會使用預設訊息內容，且無法自訂。

   您還可以將請求設定為不發送邀請電子郵件。
3. 自動接受成員帳戶的邀請。

   由於指令碼會自動接受邀請，因此成員帳戶可以忽略此類訊息。

   我們建議您直接與成員帳戶聯絡，通知他們邀請已自動接受。

disableDetective.py 指令碼概觀

disableDetective.py 指令碼會從指定區域的管理員帳戶行為圖表中刪除指定的成員帳戶。

它還提供了一個選項，以在跨指定區域中停用管理員帳戶的 Detective。

指令碼的必要許可

此類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：

- detective:CreateGraph
- detective:CreateMembers
- detective:DeleteGraph
- detective:DeleteMembers
- detective:ListGraphs
- detective:ListMembers
- detective:AcceptInvitation

角色信任關係

角色信任關係必須允許您的執行個體或本機憑證擔任該角色。

```
{
  "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。
- 在上方新增必要的許可 (建議) 或選取 AmazonDetective FullAccess 受管政策。
- 如上所述，新增角色信任關係區塊。

您也可以使用 `EnableDetective.yaml` AWS CloudFormation 範本來自動化此程序。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。如需有關如何啟動 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 主控台輕鬆取代或附加 IAM 角色至現有 EC2 執行個體》。
3. 安裝所需的軟體：

   - APT：`sudo apt-get -y install python3-pip python3 git`

- RPM：`sudo yum -y install python3-pip python3 git`
- Boto (最低版本 1.15)：`sudo pip install boto3`

4. 將儲存庫複製到 EC2 執行個體。

```
git clone https://github.com/aws-samples/amazon-detective-multiaccount-scripts.git
```

設定本機電腦以執行指令碼

您也可以從本機電腦中執行指令碼。

設定本機電腦以執行指令碼

1. 請確定您已針對具有呼叫 `AssumeRole` 許可的管理員帳戶設定本機電腦憑證。
2. 安裝所需的軟體：

   - Python 3
   - Boto (最低版本 1.15)
   - GitHub 指令碼

平台	設定說明
Windows	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. 從 GitHub (https://github.com/aws-samples/amazon-detective-multiaccount-scripts) 下載指令碼來源程式碼。
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. 從 GitHub (https://github.com/aws-samples/amazon-detective-multiaccount-scripts) 下載指令碼來源程式碼。

平台	設定說明
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/amazon-detective-multiaccount-scripts 複製指令碼來源程式碼。

建立要新增或移除的成員帳戶 .csv 清單

若要識別要新增至行為圖表或從行為圖表中移除的成員帳戶，您需要提供包含帳戶清單的 .csv 檔案。

在單獨的行上列出各個帳戶。每個成員帳戶項目都包含 AWS 帳戶 ID 和帳戶根使用者電子郵件地址。

請參閱下列範例：

```
111122223333,srodriguez@example.com
444455556666,rroe@example.com
```

執行 enableDetective.py

您可以從 EC2 enableDetective.py 執行個體或本機電腦執行指令碼。

請執行 **enableDetective.py**。

1. 將 .csv 檔案複製到 EC2 執行個體或本機電腦上的 amazon-detective-multiaccount-scripts 目錄。
2. 切換至 amazon-detective-multiaccount-scripts 目錄。
3. 執行 enableDetective.py 指令碼。

```
enableDetective.py --master_account administratorAccountID --assume_role roleName
 --input_file inputFileName --tags tagValueList --enabled_regions regionList  --
disable_email
```

執行指令碼時，請取代以下值：

administratorAccountID

管理員帳戶的 AWS 帳戶 ID。

roleName

管理員帳戶和每個成員帳戶中要承擔的 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

管理員帳戶的 AWS 帳戶 ID。

roleName

管理員帳戶和每個成員帳戶中要承擔的 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。

Detective 管理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 4 月 15 日

變更	描述	日期
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
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
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
已將受管政策資訊新增至安全性章節	在 `AmazonDetectiveInvestigatorAccess` 政策中	2023 年 11 月 26 日

	新增了 Detective 調查和調查結果群組摘要動作。	
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
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
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
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
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

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
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 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
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
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
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
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

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。

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。