Amazon GuardDuty 用戶指南

Amazon GuardDuty

Amazon GuardDuty: Amazon GuardDuty 用戶指南

Table of Contents

什麼是 Amazon GuardDuty？

Amazon GuardDuty 是一種威脅偵測服務，可持續監控您的 AWS 環境是否存在潛在的安全風險。GuardDuty 分析和處理基礎資料來源，例如 AWS CloudTrail 管理事 AWS CloudTrail 件、事件日誌、VPC 流程日誌 (來自 Amazon EC2 執行個體) 和 DNS 日誌。 GuardDuty 還提供來自其他 AWS 服務的監控日誌和事件。這些來源包括 EKS 稽核日誌、RDS 登入活動、S3 日誌、EBS 磁碟區、執行階段監控和 Lambda 網路活動日誌。 GuardDuty將這些記錄檔和事件來源合併為「功能」一詞。

GuardDuty 使用威脅情報摘要，例如惡意 IP 位址和網域清單，以及機器學習 (ML) 模型來識別您 AWS 環境中的未預期、潛在未經授權和惡意活動。這包括權限提升、使用暴露的登入資料或與惡意 IP 地址的通訊、網域、Amazon EC2 執行個體和容器工作負載上存在惡意軟體，或發現資料庫上異常登入事件模式等問題。

例如， GuardDuty 可以偵測可能遭到入侵的 EC2 執行個體和提供惡意軟體或挖掘比特幣的容器工作負載 它也會監控 AWS 帳戶存取行為是否有潛在入侵的跡象，例如未經授權的基礎結構部署 (部署在以前未使用過的區域中的執行個體或不尋常的 API 呼叫) 密碼政策已變更以降低密碼強度。

啟用時，可 GuardDuty 讓您看到 AWS 環境的安全狀態。當它識別出潛在的安全風險時，它會產生一個發現項目並提供更多詳細資訊。您也可以 EventBridge 將 Amazon 設定為在 GuardDuty 產生搜尋結果時接收通知。 GuardDuty 也會建議步驟，以修正您環境中的指示性安全性問題。

您可以將產生的發現結果匯出到 Amazon Simple Storage Service (Amazon S3) 儲存貯體。GuardDuty 還可與其他 AWS 安全相關服務 (例如 AWS Security Hub 和 Amazon Detective) 整合，這些服務可進一步協助您分析和調查環境中的安全趨勢。

使用 GuardDuty

您可以透過下 GuardDuty 列任何一種方式使用：

GuardDuty 控制台

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

控制台是一個基於瀏覽器的界面，用於訪問和使用 GuardDuty。主 GuardDuty 控台可讓您存取您的 GuardDuty 帳戶、資料和資源。

AWS 命令行工具

使用 AWS 命令行工具，您可以在系統的命令行中發出命令以執行 GuardDuty 任務和 AWS 任務。若您想要建構執行任務的指令碼，命令列工具非常實用。

若要取得有關安裝和使用的資訊 AWS CLI，請參閱AWS Command Line Interface 使用指南。若要檢視的可用命 AWS CLI 令 GuardDuty，請參閱 CLI 命令參考。

GuardDuty HTTPS API

您可以使用 GuardDuty HTTPS API 以 AWS 程式設計方式存取 GuardDuty 和以程式設計方式，該 API 可讓您直接向服務發出 HTTPS 要求。如需詳細資訊，請參閱 GuardDuty API 參考資料。

AWS 開發套件

AWS 提供軟體開發套件 (SDK)，其中包含各種程式設計語言和平台 (Java、Python、Ruby、.NET、iOS、安卓系統等) 的程式庫和範例程式碼。SDK 提供了一種方便的方式來創建程序化訪問. GuardDuty 如需 AWS 開發套件的其他資訊 (包括如何下載並安裝開發套件)，請參閱 Amazon Web Services 工具。

定價 GuardDuty

首次使 GuardDuty 用時，每個 AWS 區域的每個 AWS 帳戶都有 30 天的免費試用期。如需詳細資訊，請參閱 定價。

支援的 AWS 地區

如需可啟用之 AWS 區域的相關資訊 GuardDuty，請參閱區域與端點。

開始使用 GuardDuty

本教學課程提供的實際操作簡介 GuardDuty。以獨立帳戶或 GuardDuty 管理員身分啟用 GuardDuty 的最低需求，請參閱步驟 1。 AWS Organizations 步驟 2 到 5 涵蓋了使用建議的其他功能， GuardDuty 以充分利用您的發現。

主題

開始之前

GuardDuty 是一基礎資料來源種威脅偵測服務，用於監控 AWS CloudTrail 事件日誌、 AWS CloudTrail 管理事件、Amazon VPC 流程日誌和 DNS 日誌。 GuardDuty 只有在個別啟用時，才會分析與其保護類型相關聯的功能。這些功能包括 Kubernetes 稽核日誌、RDS 登入活動、S3 日誌、EBS 磁碟區、執行期監控和 Lambda 網路活動日誌。使用這些資料來源和功能 (如果已啟用)，為您的帳戶 GuardDuty 產生安全性發現項目。

啟用之後 GuardDuty，它會開始監視您的環境。您可以隨 GuardDuty 時停用任何地區的任何帳號。這將停 GuardDuty 止處理基礎資料來源和任何個別啟用的功能。

您不需要明確啟用任何基礎資料來源。Amazon 直接從這些服務中 GuardDuty 提取獨立的資料串流。對於新 GuardDuty 帳戶，預設會啟用中支援的所有可用 AWS 區域 保護類型，並包含在 30 天免費試用期內。您可以選擇不啟用任何或所有保護類型。如果您是現有 GuardDuty 客戶，則可以選擇啟用您的任何或所有可用的保護計劃 AWS 區域。如需詳細資訊，請參閱中與每個保護類型相關聯的功能 GuardDuty。

啟用時 GuardDuty，請考慮下列項目：

- GuardDuty 是區域服務，表示您在此頁面上遵循的任何組態程序都必須在您要監視的每個區域中重複執行 GuardDuty。

我們強烈建議您 GuardDuty 在所有支援的 AWS 區域中啟用。這可讓 GuardDuty 您產生關於未經授權或不尋常活動的發現，即使在您未主動使用的區域中也是如此。這也可 GuardDuty 以監控全球 AWS 服務 (例如 IAM) 的 AWS CloudTrail 事件。如果 GuardDuty 未在所有支援的區域中啟用，則會降低偵測涉及全域服務的活動的能力。如需可用區域的完整清 GuardDuty 單，請參閱區域與端點。

- 任何在 AWS 帳戶中具有管理員權限的使用者都可以啟用 GuardDuty，但是，遵循最低權限的安全性最佳實務，建議您建立 IAM 角色、使用者或群組來 GuardDuty 專門管理。如需啟用所需權限的詳細資訊， GuardDuty 請參閱啟用 GuardDuty 的必要許可。
- 當您第一 GuardDuty 次在任何時間啟用時 AWS 區域，依預設，它也會啟用該區域支援的所有可用防護類型，包括惡意程式碼防護。 GuardDuty 為您的帳戶建立服務連結角色。`AWSServiceRoleForAmazonGuardDuty`此角色包括權限和信任原則，可讓 GuardDuty 您直接從中使用和分析事件，基礎資料來源以產生安全性發現項目。惡意軟體防護會為您的帳戶建立另一個名為 `AWSServiceRoleForAmazonGuardDutyMalwareProtection` 的服務連結角色。此角色包括允許惡意程式碼防護執行無代理程式掃描以偵測帳戶中的惡意程式碼的 GuardDuty 權限和信任策略。它 GuardDuty 允許在您的帳戶中創建 EBS 磁碟區快照，並與 GuardDuty 服務帳戶共享該快照。如需詳細資訊，請參閱 服務連結角色權限 GuardDuty。如需有關服務連結角色的詳細資訊，請參閱使用服務連結角色。

- 當您在任何地區首次啟用 GuardDuty 時，您的 AWS 帳戶將自動註冊該區域的 30 天 GuardDuty 免費試用。

第 1 步：啟用 Amazon GuardDuty

使用的第一步 GuardDuty 是在您的帳戶中啟用它。啟用後， GuardDuty將立即開始監控當前區域中的安全威脅。

如果您想要以管理員 GuardDuty 身分管理組織內其他帳戶的 GuardDuty 發現項目，您必須新增成員帳戶並 GuardDuty 為其啟用。選擇一個選項以了解如何 GuardDuty 為您的環境啟用。

Standalone account environment

1. 請在以下位置開啟 GuardDuty 主控台 https://console.aws.amazon.com/guardduty/
2. 選擇開始使用。
3. 選擇「啟用」 GuardDuty。

Multi-account environment

> **Important**
>
> 作為此程序的先決條件，您必須與您要管理的所有帳戶位於同一個組織中，並具有 AWS Organizations 管理帳戶的存取權，才能在組織 GuardDuty 內委派管理員。委派管理員時可能需要其他許可，如需詳細資訊，請參閱指定委派 GuardDuty 管理員帳戶所需的權限。

若要指定委派的 GuardDuty 管理員帳戶

1. 使用管理帳戶開啟 AWS Organizations 主控台，網址為 https://console.aws.amazon.com/organizations/。
2. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/

   您的帳戶 GuardDuty 已啟用？

   - 如果尚 GuardDuty 未啟用，您可以選取 [開始使用]，然後在 [歡迎使用] GuardDuty 頁面上指定 GuardDuty 委派的管理員。
   - 如果啟 GuardDuty 用，您可以在「設定」 頁面上指定 GuardDuty 委派管理員。
3. 輸入您要指定為組織 GuardDuty 委派管理員之帳戶的十二位數 AWS 帳號 ID，然後選擇 [委派]。

   > **Note**
   >
   > 如果尚 GuardDuty 未啟用，則指定委派管理員將 GuardDuty 為您目前區域中的該帳戶啟用。

新增成員帳戶

此程序涵蓋透過將成員帳戶新增至 GuardDuty 委派管理員帳戶 AWS Organizations。此外，也有透過邀請新增成員的選項。若要進一步瞭解關聯成員的兩種方法 GuardDuty，請參閱在 Amazon 管理多個帳戶 GuardDuty。

1. 登入委派管理員帳戶
2. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/
3. 在導覽窗格中，選擇設定，然後選擇帳戶。

帳戶資料表會顯示組織中的所有帳戶。

4. 選取帳戶 ID 旁邊的方塊，以選擇您要新增為成員的帳戶。然後從動作選單中選取新增成員。

> **Tip**
>
> 您可以開啟自動啟用功能，自動將新帳戶新增為成員；不過，這僅適用於在啟用該功能之後加入組織的帳戶。

步驟 2：產生範例調查結果並探索基本操作

當 GuardDuty 發現安全問題時，它會產生一個發現。發 GuardDuty 現項目是包含與該唯一安全性問題相關詳細資料的資料集。調查結果的詳細資訊可用來協助您調查問題。

GuardDuty 支援使用預留位置值產生範例發現項目，這些預留位置值可用來測試 GuardDuty 功能並熟悉發現項目，然後再需要回應由發現的真實安全性問題。 GuardDuty請遵循下列指南，針對中可用的每個發現項目類型產生搜尋結果範例 GuardDuty，以取得產生搜尋結果範例的其他方式，包括在您的帳戶中產生模擬安全性事件，請參閱範例問題清單。

建立和探索範例調查結果

1. 在導覽窗格中，選擇設定。
2. 在設定頁面的調查結果範例下，選擇產生調查結果範例。
3. 在瀏覽窗格中，選擇 [摘要] 以檢視 AWS 環境中產生之發現項目的相關見解。如需有關「摘要」儀表板中元件的詳細資訊，請參閱「摘要」儀表板。
4. 在導覽窗格中，選擇調查結果。此調查結果範例會顯示在目前調查結果頁面上，並有字首 [SAMPLE]。
5. 從清單中選取一個調查結果，以顯示該調查結果的詳細資訊。

    - 您可以檢閱調查結果詳細資訊窗格中的不同資訊欄位。不同類型的調查結果可以有不同的欄位。如需有關所有調查結果類型中可用欄位的詳細資訊，請參閱調查結果詳細資訊。您可以從詳細資訊窗格執行下列動作：

        - 選取窗格頂端的調查結果 ID，以開啟調查結果的完整 JSON 詳細資訊。您也可以從此面板下載完整的 JSON 檔案。JSON 包含一些未納入主控台檢視中的其他資訊，也是其他工具和服務可擷取的格式。

- 檢視受影響的資源區段。根據真正的發現，此處的資訊將協助您識別帳戶中應進行調查的資源，並包含 AWS Management Console 適當資源的連結。
- 選取 + 或 - 鏡子圖示，為該詳細資訊建立包含或排除篩選條件。如需有關調查結果篩選條件的詳細資訊，請參閱篩選問題清單。

6. 封存您的所有範例調查結果

   a. 選取清單頂端的核取方塊，以選取所有調查結果。

   b. 取消選取要保留的任何調查結果。

   c. 選取動作選單，然後選取封存以隱藏範例調查結果。

> **Note**
>
> 若要檢視已封存的調查結果，請依次選取目前與已封存，以切換調查結果檢視。

步驟 3：設定將 GuardDuty 發現結果匯出至 Amazon S3 儲存貯體

GuardDuty 建議您設定設定以匯出發現項目，因為它可讓您將發現項目匯出到 S3 儲存貯體，以便在 GuardDuty 90 天保留期之後進行無限期儲存。這可讓您保留發現項目的記錄，或追蹤 AWS 環境中一段時間內的問題。此處概述的程序會逐步引導您設定新的 S3 儲存貯體，並建立新的 KMS 金鑰，以便從主控台內加密調查結果。如需相關詳細資訊，包括如何使用自己現有的儲存貯體或其他帳戶中的儲存貯體，請參閱匯出調查結果。

設定 S3 匯出調查結果選項

1. 若要加密發現項目，您需要具有允許 GuardDuty 使用該金鑰進行加密的原則的 KMS 金鑰。下列步驟將協助您建立新的 KMS 金鑰。如果您使用其他帳戶的 KMS 金鑰，則需要登入擁有 AWS 帳戶 該金鑰的金鑰來套用金鑰原則。KMS 金鑰和 S3 儲存貯體必須位於同一區域。不過，您可以針對要匯出調查結果的每個區域，使用此相同的儲存貯體和金鑰對。

   a. 請在以下位置開啟 AWS KMS 主控台。 https://console.aws.amazon.com/kms

   b. 若要變更 AWS 區域，請使用頁面右上角的「地區」選取器。

   c. 在導覽窗格中，選擇 Customer managed keys (客戶受管金鑰)。

   d. 選擇建立金鑰。

   e. 在金鑰類型下選擇對稱，然後選擇下一步。

> **Note**
>
> 如需有關建立 KMS 金鑰的詳細步驟，請參閱《AWS Key Management Service 開發人員指南》中的 Creating keys。

f. 提供金鑰的別名，然後選擇下一步。

g. 選擇下一步，然後再次選擇下一步以接受預設的管理和使用許可。

h. 檢閱組態後，選擇完成來建立金鑰。

i. 在客戶自管金鑰頁面上，選擇您的金鑰別名。

j. 在金鑰政策索引標籤中，選擇切換為政策檢視。

k. 選擇 [編輯]，然後將下列金鑰原則新增至您的 KMS 金鑰，以授與金鑰的 GuardDuty 存取權。此陳述式只 GuardDuty 允許使用您新增此原則的索引鍵。編輯金鑰政策時，請確定 JSON 語法有效。如果您在最終陳述式之前新增陳述式，則必須在右括號後加上逗號。

```
{
    "Sid": "AllowGuardDutyKey",
    "Effect": "Allow",
    "Principal": {
        "Service": "guardduty.amazonaws.com"
    },
    "Action": "kms:GenerateDataKey",
    "Resource": "arn:aws:kms:Region1:444455556666:key/KMSKeyId",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "111122223333",
            "aws:SourceArn":
 "arn:aws:guardduty:Region2:111122223333:detector/SourceDetectorID"
        }
    }
}
```

使用您的 KMS 金鑰的區域取代 *Region1*。將 *444455556666* 取代為擁有 KMS 金鑰的 AWS 帳戶 。將 *KMS* 取代為您選擇KeyId用於加密的 KMS 金鑰的金鑰識別碼。若要識別所有這些值 (區域和金鑰識別碼)，請檢視 KMS 金鑰的 ARN。 AWS 帳戶若要找出金鑰 ARN，請參閱 Finding the key ID and ARN。

同樣地，請使用該帳戶取代 *111122223333*。 AWS 帳戶 GuardDuty 將「區*# 2*」取代為帳戶的「區域」 GuardDuty 。將 *SourceDetectorID* 取代為*##* 2 GuardDuty 帳戶的偵測器 ID。

要查找您`detectorId`的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

l. 選擇儲存。

2. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/
3. 在導覽窗格中，選擇設定。
4. 在調查結果匯出選項下，選擇立即設定。
5. 選擇新儲存貯體。提供 S3 儲存貯體的唯一名稱。
6. (選用) 您可以透過產生範例調查結果來測試新的匯出設定。在導覽窗格中，選擇設定。
7. 在範例調查結果下，選擇產生範例調查結果。新的範例發現項目會在最多五分鐘內顯示為 S3 儲存貯體 GuardDuty 中建立的項目。

步驟 4：設定透過 SNS GuardDuty 尋找警示

GuardDuty 與 Amazon 整合 EventBridge，可用於將發現結果資料傳送到其他應用程式和服務以進行處理。透過將尋找事件連接到 AWS Lambda 功能、Amazon EC2 系統管理員自動化、Amazon Simple Notification Service (SNS) 等目標，您可以使 GuardDuty 用發現結果啟動自動回應。 EventBridge

在此範例中，您將建立 SNS 主題作為 EventBridge 規則的目標，然後使用 EventBridge 建立從中擷取發現項目資料的規則 GuardDuty。產生的規則會將調查結果詳細資訊轉寄至某個電子郵件地址。若要了解如何將調查結果傳送至 Slack 或 Amazon Chime，以及如何修改傳送的調查結果提醒類型，請參閱設定 Amazon SNS 主題和端點。

建立調查結果提醒的 SNS 主題

1. 在 https://console.aws.amazon.com/sns/v3/home 開啟 Amazon SNS 主控台。
2. 在導覽窗格中，選擇主題。
3. 選擇建立主題。
4. 針對類型，選取標準。
5. 對於名稱，輸入 **`GuardDuty`**。
6. 選擇建立主題。新主題的主題詳細資訊隨即開啟。

7. 在訂閱區段中，選擇建立訂閱。
8. 對於通訊協定，選擇電子郵件。
9. 對於端點，輸入將通知傳送到的收件電子郵件地址。
10. 選擇建立訂閱。

    建立訂閱後，您必須透過電子郵件確認訂閱。
11. 若要檢查訂閱訊息，請前往您的電子郵件收件匣，然後在訂閱訊息中選擇確認訂閱。

> **Note**
>
> 若要檢查電子郵件確認狀態，請前往 SNS 主控台並選擇訂閱。

若要建立 EventBridge 規則以擷取 GuardDuty 發現項目並設定其格式

1. 請在以下位置開啟 EventBridge 主控台。 https://console.aws.amazon.com/events/
2. 在導覽窗格中，選擇規則。
3. 選擇建立規則。
4. 輸入規則的名稱和描述。

    在同一個區域和同一個事件匯流排上，規則不能與另一個規則同名。
5. 針對事件匯流排選擇預設值。
6. 針對規則類型選擇具有事件模式的規則。
7. 選擇下一步。
8. 在事件來源，選擇 AWS 事件。
9. 針對事件模式，選擇事件模式表單。
10. 在事件來源欄位中，選擇 AWS 服務。
11. 在AWS 服務中選擇 GuardDuty。
12. 對於「事件型態」，請選擇「GuardDuty搜尋
13. 選擇下一步。
14. 在目標類型欄位中，選擇 AWS 服務。
15. 針對選取目標，選擇 SNS 主題，然後針對主題，選擇您先前建立之 SNS 主題的名稱。
16. 在其他設定區段中，針對設定目標輸入，選擇輸入轉換器。

新增輸入轉換器會 GuardDuty 將從傳送的 JSON 尋找資料格式化為人類可讀的訊息。

17. 選擇設定輸入轉換器。
18. 在目標輸入轉換器區段中，針對輸入路徑，貼上下列程式碼：

```
{
  "severity": "$.detail.severity",
  "Finding_ID": "$.detail.id",
  "Finding_Type": "$.detail.type",
  "region": "$.region",
  "Finding_description": "$.detail.description"
}
```

19. 若要格式化電子郵件，對於範本，貼上下列程式碼，並確定以紅色取代為適合您地區的值的文字：

```
"You have a severity severity GuardDuty finding type Finding_Type in
 the Region_Name Region."
"Finding Description:"
"Finding_Description."
"For more details open the GuardDuty console at https://console.aws.amazon.com/
guardduty/home?region=region#/findings?search=id%3DFinding_ID"
```

20. 選擇確認。
21. 選擇下一步。
22. (選用) 為規則輸入一或多個標籤。如需詳細資訊，請參閱 Amazon EventBridge 使用者指南中的 Amazon EventBridge 標籤。
23. 選擇下一步。
24. 檢閱規則的詳細資訊，然後選擇建立規則。
25. (選用) 使用步驟 2 中的程序產生範例調查結果，以測試新規則。您將收到每個產生的範例調查結果的電子郵件。

後續步驟

當您繼續使用時 GuardDuty，您將瞭解與您的環境相關的發現項目類型。每當收到新調查結果時，您都可以從調查結果詳細資訊窗格中的調查結果說明中，選取進一步了解，或在 調查結果類型 中搜尋調查結果名稱，以尋找資訊，包括有關該調查結果的修復建議。

下列功能可協助您進行調整，以 GuardDuty 便為您的 AWS 環境提供最相關的發現項目：

- 若要根據特定條件 (例如執行個體 ID、帳戶 ID、S3 儲存貯體名稱等) 輕鬆排序發現項目，您可以在中建立並儲存篩選器 GuardDuty。如需詳細資訊，請參閱 篩選問題清單。
- 如果您收到環境中預期行為的調查結果，您可以根據使用隱藏規則定義的條件，自動將調查結果封存。
- 若要防止從受信任 IP 子集產生發現項目，或是讓 GuardDuty 監控 IP 超出正常監控範圍，您可以設定受信任 IP 和威脅清單。

概念和術語

開始使用 Amazon 時 GuardDuty，您可以從學習其關鍵概念中受益。

帳戶

包含您的 AWS 資源的標準 Amazon Web Services（AWS）帳戶。您可以使用您 AWS 的帳戶登錄並啟用 GuardDuty。

您也可以邀請其他帳戶在中啟用 GuardDuty 並與您的 AWS 帳戶建立關聯 GuardDuty。如果您的邀請被接受，您的帳戶將被指定為管理員 GuardDuty 帳戶，而新增的帳戶會成為您的成員帳戶。然後，您可以代表他們查看和管理這些帳戶的 GuardDuty 發現。

管理員帳戶的使用者可 GuardDuty 以設定及檢視和管理自己帳戶及其所有成員帳戶的 GuardDuty發現項目。您最多可以擁有 10,000 個會員帳戶 GuardDuty。

成員帳戶的使用者可以在其帳戶中設定 GuardDuty 及檢視和管理 GuardDuty 發現項目 (透過 GuardDuty 管理主控台或 GuardDuty API)。成員帳戶使用者無法查看或管理其他成員帳戶中的問題清單。

AWS 帳戶不能同時是 GuardDuty 管理員帳戶和成員帳戶。一個帳戶僅能接受一個 AWS 成員邀請。接受成員邀請為選擇性。

如需詳細資訊，請參閱 在 Amazon 管理多個帳戶 GuardDuty。

偵測器

所有 GuardDuty 發現項目都與偵測器相關聯，偵測器是代表 GuardDuty 服務的物件。該檢測器是一個區域實體，並且在其中 GuardDuty 運行的每個檢測器都需要一個唯一 AWS 區域 的檢測器。當您在「區域」 GuardDuty 中啟用時，會在該區域中產生具有唯一 32 個英數字元 detectorId 的新偵測器。detectorId 的格式為 `12abc34d567e8fa901bc2d34e56789f0`。

要查找您`detectorId`的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

> **Note**
>
> 在多個帳戶環境中，成員帳戶的所有調查結果都會匯總到管理員帳戶的偵測器。

某些 GuardDuty 功能是透過偵測器設定的，例如設定 CloudWatch 事件通知頻率，以及啟用或停用 GuardDuty 要處理的選用資料來源。

資料來源

一組資料的原始來源或位置。偵測 AWS 環境中未經授權或未預期的活動。 GuardDuty 分析和處理來自 AWS CloudTrail 事件日誌、 AWS CloudTrail 管理事件、S3 AWS CloudTrail 資料事件、VPC 流程日誌、DNS 日誌、EKS 稽核日誌、RDS 登入活動監控和 EBS 磁碟區的資料。如需詳細資訊，請參閱 基礎資料來源。

功能

針對您的 GuardDuty 保護方案設定的功能物件有助於偵測 AWS 環境中未經授權或未預期的活動。每個 GuardDuty 保護計畫都會規劃對應的圖徵物件，以分析和處理資料。某些功能物件包括 EKS 稽核日誌、RDS 登入活動監控和 EBS 磁碟區。如需詳細資訊，請參閱 功能激活 GuardDuty。

問題清單

GuardDuty 發現的潛在安全問題清單。如需詳細資訊，請參閱 了解 Amazon GuardDuty 發現。

發現項目會顯示在 GuardDuty 主控台中，並包含安全性問題的詳細說明。您也可以呼叫GetFindings和 ListFindingsAPI 作業來擷取產生的發現項目。

您還可以通過 Amazon CloudWatch 事件查看您的 GuardDuty 發現。 GuardDuty CloudWatch 通過 HTTPS 協議將發現結果發送到 Amazon。如需詳細資訊，請參閱 使用 Amazon CloudWatch 活動建立自訂回應的 GuardDuty 發現項目。

掃描選項

啟用 GuardDuty 惡意程式碼防護後，您可以指定要掃描或略過哪些 Amazon EC2 執行個體和 Amazon 彈性區塊存放區 (EBS) 磁碟區。此功能可讓您將與 EC2 執行個體和 EBS 磁碟區相關聯的現有標籤新增至包含標籤清單或排除標籤清單。系統會掃描與您新增至包含標籤清單的標籤相關聯的資源是否含有惡意軟體，不會掃描新增至排除標籤清單的資源。如需詳細資訊，請參閱 具有使用者定義標籤的掃描選項。

快照保留

啟用 GuardDuty 惡意程式碼防護後，它會提供一個選項，讓您在 AWS 帳戶中保留 EBS 磁碟區的快照。 GuardDuty 根據 EBS 磁碟區的快照產生複本 EBS 磁碟區。只有在惡意軟體防護掃描偵測到複本 EBS 磁碟區中的惡意軟體時，才能保留 EBS 磁碟區的快照。如果複本 EBS 磁碟區中未偵測到惡意程式碼，則不論快照保留設定為何，都 GuardDuty 會自動刪除 EBS 磁碟區的快照。如需詳細資訊，請參閱 快照保留。

隱藏規則

隱藏規則可讓您建立非常特定的屬性組合以隱藏問題清單。例如，您可以透過 GuardDuty 篩選器定義規則，以僅Recon:EC2/Portscan從特定 VPC 中的那些執行個體、執行特定 AMI 或使用特定 EC2 標籤自動存檔。此規則會造成符合條件的執行個體連接埠掃描問題清單被自動封存。但是，如果 GuardDuty 檢測到執行其他惡意活動（例如加密貨幣挖掘）的實例，它仍然允許發出警報。

在 GuardDuty 管理員帳戶中定義的隱藏規則適用於 GuardDuty 成員帳戶。 GuardDuty 成員帳戶無法修改隱藏規則。

使用抑制規則， GuardDuty 仍會產生所有發現項目。隱藏規則可抑制問題清單，同時保持所有活動歷史記錄完整不變。

一般來說，隱藏規則是用來隱藏您判定為環境誤判的問題清單，並減少低價值問題清單的雜訊，讓您可以專注於較大的威脅。如需詳細資訊，請參閱 隱藏規則。

信任 IP 清單

信任 IP 位址清單，可與您的 AWS 環境進行高度安全的通訊。 GuardDuty 不會根據信任的 IP 清單產生發現項目。如需詳細資訊，請參閱 使用信任 IP 清單和威脅清單。

威脅 IP 清單

已知惡意 IP 地址的清單。除了由於潛在可疑活動而產生發現項目之外， GuardDuty 還會根據這些安全威脅清單產生發現項目。如需更多詳細資訊，請參閱 使用信任 IP 清單和威脅清單。

功能激活 GuardDuty

當您第一次啟 GuardDuty 用 Amazon 或在中啟用保護類型時 GuardDuty，會 GuardDuty 開始處理 AWS 環境基礎資料來源中對應的。 GuardDuty 使用這些資料來源來處理事件串流，例如 VPC 流程記錄檔、DNS 記錄以及 AWS CloudTrail 事件和管理記錄。然後它會分析這些事件以識別潛在安全威脅，並在您的帳戶中產生調查結果。

除了記錄資料來源之外，還 GuardDuty 可以使用 AWS 環境中其他 AWS 服務的其他資料來監控和分析潛在的安全威脅。

功能啟用

當您新增其他保 GuardDuty 護 (例如 S3 保護、執行階段監控或 EKS 保護) 時，您可以設定與保護類型相對應的 GuardDuty 功能。從歷史上看，在 API `dataSources` 中調用了 GuardDuty 保護措施。不過，2023 年 3 月之後，新的 GuardDuty 防護類型現在會設定為`features`與不`dataSources`設定。GuardDuty 仍然支持配置 2023 年 3 月之前啟動的保護類型，如同`dataSources`通過 API 一樣，但新的保護類型僅提供為`features`.

如果您透過主控台管理 GuardDuty 設定和保護類型，則不會直接受到此變更的影響，也不需要採取任何動作。功能啟動會影響呼叫以啟用 GuardDuty 或保護其中類型的 API 的行為 GuardDuty。如需詳細資訊，請參閱 GuardDuty API 變更。

GuardDuty 二零二三年三月的空氣指數變

GuardDuty API 會設定不屬於的清單的保護功能基礎資料來源。功能物件包含功能詳細資訊，例如功能名稱和狀態，並且可能包含某些功能的其他組態。此遷移會影響 Amazon GuardDuty API 參考中的以下 API：

- CreateDetector
- GetDetector
- UpdateDetector
- GetMemberDetectors
- UpdateMemberDetectors
- DescribeOrganizationConfiguration

- UpdateOrganizationConfiguration
- GetRemainingFreeTrialDays
- GetUsageStatistics

與資料來源相比的功能啟用

從歷史上看，所有 GuardDuty 功能都通過 API 中的dataSources對象傳遞。從 2023 年 3 月開始，GuardDuty 更喜歡features對象而不是 API 中的dataSources對象。所有較早的資料來源都具有對應的功能，但較新的功能可能沒有對應的資料來源。

下列清單顯示了透過 API 傳遞時 dataSources 和 features 物件之間的比較：

- dataSources 物件包含每種保護類型的物件及其狀態。features物件是對應於中每個保護類型的可用功能清單 GuardDuty。

  從 2023 年 3 月開始，功能啟用將是您 AWS 環境中設定新 GuardDuty 功能的唯一方法。
- API 要求或回應中的dataSources結構描述在每個可用 AWS 區域 位置 GuardDuty 都相同。但是，並非每個區域都會提供所有功能。因此，可用的功能名稱可能會因區域而有所不同。

了解功能啟用的運作方式

這些 GuardDuty API 將繼續返回適用的dataSources對象，並且它們還將返回一個包含不同格式的相同信息的features對象。 GuardDuty 2023 年 3 月之前啟動的功能將可透過dataSources物件和features物件使用。 GuardDuty 自 2023 年 3 月以來啟動的功能只能透過features物件使用。您無法在同一 API 請求中建立或更新偵測器，也無法使用 dataSources 和 features 物件標記法來描述 AWS Organizations 。若要啟用 GuardDuty 保護類型，您需要使用現有包含features物件的相同 API，將現有資料來源移轉至features物件。

> **Note**
>
> GuardDuty 在此修改之後，將不會新增資料來源。

GuardDuty 已棄用資料來源的使用。但是仍支援 基礎資料來源。最 GuardDuty 佳做法建議針對已為您的帳戶啟用的任何保護類型使用功能啟用。當您為帳戶啟用新的保護類型時，最佳實務也需要使用功能啟用。

整合功能啟動變更

- 如果您透過 API、SDK 或 AWS CloudFormation 範本管理 GuardDuty 組態，並且想要啟用潛在的新 GuardDuty 功能，則需要分別修改程式碼和範本。如需詳細資訊，請參閱 Amazon GuardDuty API 參考中的更新 API。
- 對於此升級之前設定的 GuardDuty 功能，您可以繼續使用 API、SDK 或 AWS CloudFormation 範本。不過，建議您切換為使用 `feature` 物件。

  所有資料來源均具有對等的功能物件。如需詳細資訊，請參閱 將 dataSources 映射至 features。
- 目前，`features` 物件中的 `additionalConfiguration` 僅適用於某些保護類型。
  - 對於此類保護類型，如果您的功能`AdditionalConfiguration`的`status`已設定為，`ENABLED`但功能的組態`status`未設定為`ENABLED`，則在此情況下 GuardDuty 將不會採取任何動作。
  - 以下 API 受到此影響：
    - UpdateDetector
    - UpdateMemberDetectors
    - UpdateOrganizationConfiguration

將 `dataSources` 映射至 `features`

以下表格顯示保護類型 `dataSources` 和 `features` 的映射。

GuardDuty 保護類型	資料來源名稱 *	特徵名稱
VPC 流量日誌	`flowLogs` (唯讀；無法修改)	`FLOW_LOGS` (唯讀；無法修改)
DNS 日誌	`dnsLogs` (唯讀；無法修改)	`DNS_LOGS` (唯讀；無法修改)
CloudTrail 事件	`cloudLogs` (唯讀；無法修改)	`CLOUD_LOGS` (唯讀；無法修改)
S3	`s3Logs`	`S3_DATA_EVENTS`

GuardDuty 保護類型	資料來源名稱 *	特徵名稱
EKS 稽核日誌監控	kubernetes.auditlogs	EKS_AUDIT_LOGS
惡意軟體防護	malwareProtection.scanEc2InstanceWithFindings.ebsVolumes	EBS_MALWARE_PROTECTION
RDS 登入事件	GuardDuty 僅針對這些防護類型提供功能啟動支援。	RDS_LOGIN_EVENTS
EKS 執行期監控		EKS_RUNTIME_MONITORING
運行時監控		RUNTIME_MONITORING
GuardDuty Amazon EKS 叢集的安全代理程式		EKS_RUNTIME_MONITORING.additionalConfiguration.EKS_ADDON_MANAGEMENT RUNTIME_MONITORING.additionalConfiguration.EKS_ADDON_MANAGEMENT

GuardDuty 保護類型	資料來源名稱 *	特徵名稱
GuardDuty Amazon ECS-Fargate 叢集的安全代理程式		RUNTIME_MONITORING.additionalConfiguration.ECS_FARGATE_AGENT_MANAGEMENT
GuardDuty Amazon EC2 執行個體的安全代理		RUNTIME_MONITORING.additionalConfiguration.EC2_AGENT_MANAGEMENT
Lambda 保護	LAMBDA_NETWORK_LOGS	

* GetUsageStatistics 使用自己的 dataSource 名稱。如需詳細資訊，請參閱 估算成 GuardDuty 本 或 GetUsageStatistics 。

基礎資料來源

GuardDuty 使用基礎資料來源偵測與已知惡意網域和 IP 位址的通訊，並識別異常行為。從這些來源傳輸到時 GuardDuty，所有記錄資料都會加密。 GuardDuty從這些記錄來源擷取各種欄位以進行分析和異常偵測，然後捨棄這些記錄檔。

以下各節說明如何 GuardDuty 使用每個受支援的資料來源。當您 GuardDuty 在中啟用時 AWS 帳戶，GuardDuty 會自動開始監視這些記錄來源。

主題

AWS CloudTrail 事件記錄

AWS CloudTrail 為您的帳戶提供 AWS API 呼叫的歷史記錄，包括使用、 AWS SDK AWS Management Console、命令列工具和特定 AWS 服務進行的 API 呼叫。 CloudTrail 也可協助您識別哪些使用者和帳戶針對支援的服務叫用 AWS API CloudTrail、呼叫呼叫的來源 IP 位址，以及呼叫呼叫的時間。如需詳細資訊，請參閱《AWS CloudTrail 使用者指南》中的 What is AWS CloudTrail。

GuardDuty 也會監控 CloudTrail 管理事件。當您啟用時 GuardDuty，它會開始直接 CloudTrail 透過獨立且重複的事件串流使用 CloudTrail 管理事件，並分析您的 CloudTrail 事件記錄。存取中記錄的事件時不會收 GuardDuty 取額外費用 CloudTrail。

GuardDuty 不會管理您的 CloudTrail 事件，也不會影響您現有的 CloudTrail 組態。同樣地，您的 CloudTrail 配置不會影響 GuardDuty 消耗和處理事件日誌的方式。若要管理 CloudTrail 事件的存取和保留，請使用 CloudTrail 服務主控台或 API。如需詳細資訊，請參閱AWS CloudTrail 使用指南中的檢視具有 CloudTrail 事件歷程記錄的事件

如何 GuardDuty 處理 AWS CloudTrail 全球事件

對於大多數 AWS 服務而言， CloudTrail 事件會記錄 AWS 區域 在建立事件的位置。對於全球服務，例如 AWS Identity and Access Management (IAM)、 AWS Security Token Service (AWS STS)、Amazon 簡單儲存服務 (Amazon S3) CloudFront、Amazon 和亞馬遜路線 53 (Route 53)，事件只會在發生這些事件的區域產生，但它們具有全球意義。

當使用具有安 CloudTrail 全性值的全域服務事件 (例如網路組態或使用者權限) 時，它 GuardDuty 會複寫這些事件，並在您已啟用 GuardDuty的每個區域中處理這些事件。此行為有助於 GuardDuty 維護每個區域中的使用者和角色設定檔，這對於偵測異常事件至關重要。

我們強烈建議您啟 GuardDuty 用所 AWS 區域 有已為您啟用的 AWS 帳戶. 這有助於 GuardDuty 產生有關未經授權或不尋常活動的發現，即使在您可能未主動使用的區域中也是如此。

AWS CloudTrail 管理事件

管理事件也稱為控制平面事件。這些事件可針對您 AWS 帳戶中的資源執行的管理作業提供深入分析。

以下是 GuardDuty監視的 CloudTrail 管理事件範例：

- 設定安全性 (IAM `AttachRolePolicy`API 操作)
- 設定路由資料規則 (Amazon EC2 `CreateSubnet` API 操作)
- 設定記錄 (AWS CloudTrail `CreateTrail`API 作業)

VPC 流量日誌

Amazon VPC 的 VPC 流量日誌功能可擷取環境內連接至 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的網路界面進出 IP 流量的相關資 AWS 訊。

啟用後 GuardDuty，它會立即開始分析帳戶內 Amazon EC2 執行個體的 VPC 流程日誌。它會透獨立且重複的流量日誌串流直接從 VPC 流量日誌功能取用 VPC 流量日誌事件。此程序不會影響任何現有的流量日誌組態。

GuardDuty Lambda 護

Lambda 保護是 Amazon 的可選增強功能 GuardDuty。目前，Lambda 網路活動監控包括來自您帳戶所有 Lambda 函數的 Amazon VPC 流量日誌，甚至包含不使用 VPC 網路的日誌。為了保護 Lambda 函數免受潛在的安全威脅，您需要在 GuardDuty 帳戶中設定 Lambda 保護。如需詳細資訊，請參閱 GuardDuty Lambda 護。

GuardDuty 運行時監控

當您在 EKS 執行個體或 EC2 執行個體的執行階段監控中管理安全代理程式 (無論GuardDuty 是手動或透過 GuardDuty)，且目前部署在 Amazon EC2 執行個體並收集的執行期事件類型從此執行個體接收，則不 GuardDuty 會 AWS 帳戶 針對此 Amazon EC2 執行個體的 VPC 流程日誌分析收費。這有助於 GuardDuty 避免帳戶中的雙重使用成本。

GuardDuty 不會管理您的流量記錄，也無法在您的帳戶中存取它們。若要管理流量日誌的存取和保留，您必須設定 VPC 流量日誌功能。

DNS 日誌

如果您對 Amazon EC2 執行個體使用 AWS DNS 解析器 (預設設定)，則 GuardDuty 可以透過內部 DNS 解析器存取和處理您的請求和回應 AWS DNS 日誌。如果您使用其他 DNS 解析器（例如 OpenDNS 或 GoogleDNS），或者如果您設置了自己的 DNS 解析器，則 GuardDuty 無法訪問和處理來自此數據源的數據。

當您啟用時 GuardDuty，它會立即開始從獨立的資料串流分析您的 DNS 記錄。此資料串流與透過 Route 53 解析器查詢日誌記錄功能提供的資料分開。此特徵的組態不會影響 GuardDuty分析。

> **Note**
>
> GuardDuty 不支援監控啟動之 Amazon EC2 執行個體的 DNS 日誌， AWS Outposts 因為 Amazon Route 53 Resolver 查詢記錄功能在該環境中無法使用。

Amazon 的 EKS 保護 GuardDuty

EKS 稽核日誌監控有助於偵測 Amazon Elastic Kubernetes Service (Amazon EKS) 內 EKS 叢集中的潛在可疑活動。EKS 稽核記錄監控使用 EKS 稽核記錄擷取使用者、使用 Kubernetes API 的應用程式以及控制平面的按時間順序排列的活動。如需詳細資訊，請參閱 EKS 稽核記錄監控。

> **Note**
>
> EKS 運行時監視作為運行時監視的一部分進行管理。如需詳細資訊，請參閱 GuardDuty 運行時監控。

EKS 保護中的功能

EKS 稽核記錄監控

EKS 稽核日誌會擷取 Amazon EKS 叢集中的連續動作，包括來自使用者的活動、使用 Kubernetes API 的應用程式以及控制平面。稽核記錄是所有 Kubernetes 叢集的元件。

如需詳細資訊，請參閱 Kubernetes 文件中的稽核。

Amazon EKS 允許透過 EKS 控制平面記錄功能將 EKS 稽核日誌當作 Amazon CloudWatch 日誌擷取為 Amazon 日誌。 GuardDuty 如果您尚未為 Amazon EKS 啟用 EKS 控制平面記錄，則不會管理您的 Amazon EKS 控制平面記錄，也不會在您的帳戶中存取 EKS 稽核日誌。若要管理 EKS 稽核日誌的存取和保留，您必須設定 Amazon EKS 控制平面記錄功能。如需詳細資訊，請參閱《Amazon EKS 使用者指南》中的啟用和停用控制平面日誌。

如需有關設定 EKS 稽核日誌監控的資訊，請參閱EKS 稽核日誌監控。

EKS 稽核日誌監控

EKS 稽核日誌監控有助於偵測 Amazon Elastic Kubernetes Service 內 EKS 叢集中的潛在可疑活動。啟用 EKS 稽核日誌監控時， GuardDuty 立即開始EKS 稽核記錄監控從 Amazon EKS 叢集進行監控，並對其進行分析是否有潛在的惡意和可疑活動。它會透過獨立且重複的稽核日誌串流，直接從 Amazon EKS 控制平面記錄功能使用 Kubernetes 稽核日誌事件。此程序不需要進行任何額外的設定，也不會影響您可能擁有的任何現有 Amazon EKS 控制平面記錄組態。

停用 EKS 稽核日誌監控時， GuardDuty 立即停止監控和分析 Amazon EKS 資源的 EKS 稽核日誌。

EKS 稽核記錄監控可能無法在所有可用的 AWS 區域 位置使 GuardDuty 用。如需詳細資訊，請參閱區域特定功能的可用性。

30 天免費試用期如何影響 GuardDuty 帳戶

- 首次啟 GuardDuty 用時，EKS 防護中的 EKS 稽核記錄監控已包含在 30 天免費試用期內。
- 現有 GuardDuty 帳戶可以在 30 天的免費試用期內首次啟用 EKS 稽核記錄監控。

設定獨立帳戶的 EKS 稽核日誌監控

選擇您偏好的存取方式，以便為獨立帳戶啟用或停用 EKS 稽核日誌監控。

Console

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/
2. 在導覽窗格中，選擇 EKS 保護。
3. 在組態索引標籤下，您可以檢視 EKS 稽核日誌監控的目前組態狀態。在 EKS 稽核日誌監控區段中，選擇啟用來啟用，或選擇停用來停用 EKS 稽核日誌監控功能。
4. 選擇儲存。

API/CLI

- 使用委派 GuardDuty 管理員帳戶的地區偵測器 ID 執行 updateDetectorAPI 作業，並將`features`物件名稱傳遞為`ENABLED`或`DISABLED`。`EKS_AUDIT_LOGS`

  或者，您也可以啟用或停用執行 AWS CLI 命令的 EKS 稽核記錄監視。下列範例程式碼會啟用 GuardDuty EKS 稽核記錄監視。若要停用，請使用 `DISABLED` 取代 `ENABLED`。

  要查找您`detectorId`的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

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

在多帳戶環境中設定 EKS 稽核日誌監控

在多帳戶環境中，只有委派的 GuardDuty 系統管理員帳戶可以選擇為其組織中的成員帳戶啟用或停用 EKS 稽核記錄監視功能。成 GuardDuty 員帳戶無法從其帳戶修改此設定。委派的管理 GuardDuty 員帳戶會使用來管理其成員帳戶 AWS Organizations。這個委派的 GuardDuty 系統管理員帳戶可以選擇在所有新帳戶加入組織時自動啟用 EKS 稽核記錄監控。如需有關多帳戶環境的詳細資訊，請參閱在 Amazon GuardDuty 中管理多個帳戶。

為委派的 GuardDuty 系統管理員帳戶設定 EKS 稽核記錄監視

選擇您偏好的存取方法，以針對委派的 GuardDuty 系統管理員帳戶設定 EKS 稽核記錄監視。

Console

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/

   確保使用管理帳戶憑證。
2. 在導覽窗格中，選擇「EKS 保護」。
3. 在組態索引標籤下，您可以在相應區段檢視 EKS 稽核日誌監控的目前組態狀態。若要更新委派 GuardDuty 管理員帳戶的組態，請在 [EKS 稽核記錄監視] 窗格中選擇 [編輯]。
4. 執行以下任意一項：

   使用為所有帳戶啟用

   - 選擇為所有帳戶啟用。這將啟用 AWS 組織中所有作用中 GuardDuty 帳戶的保護計劃，包括加入組織的新帳戶。
   - 選擇儲存。

   使用手動設定帳戶

   - 若要僅針對委派的 GuardDuty 系統管理員帳戶啟用保護方案，請選擇 [手動設定帳戶]。
   - 在 [委派 GuardDuty 管理員帳戶 (此帳戶)] 區段下選擇 [啟用]。
   - 選擇儲存。

API/CLI

使用您自己的區域偵測器 ID，並透過將 `name` 設定為 `EKS_AUDIT_LOGS` 及將 `status` 設定為 `ENABLED` 或 `DISABLED` 來傳遞 `features` 物件，從而執行 updateDetector API 操作。

要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

您可以執行下列 AWS CLI 命令來啟用或停用 EKS 稽核記錄監視。確保使用委派 GuardDuty 管理員帳戶的有效*### ID*。

> **Note**
>
> 下列範例程式碼會啟用 EKS 稽核日誌監控。*############################ # 12abc34d56789 f0 ############detector-id GuardDuty* AWS 帳戶 GuardDuty

要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

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

若要停用 EKS 稽核日誌監控，請使用 DISABLED 取代 ENABLED。

為所有成員帳戶自動啟用 EKS 稽核日誌監控

選擇您偏好的存取方式，以便為組織中現有的成員帳戶啟用 EKS 稽核日誌監控。

Console

1. 請登入 AWS Management Console 並開啟 GuardDuty 主控台，網址為 https://console.aws.amazon.com/guardduty/。

   請務必使用委派的 GuardDuty 系統管理員帳戶認證。
2. 執行以下任意一項：

   使用 EKS 保護 頁面

   1. 在導覽窗格中，選擇 EKS 保護。
   2. 在組態索引標籤下，您可以檢視組織中作用中成員帳戶的 EKS 稽核日誌監控目前狀態。

      若要更新 EKS 稽核日誌監控組態，請選擇編輯。

3. 選擇為所有帳戶啟用。此動作會自動為組織中的現有帳戶和新帳戶啟用 EKS 稽核日誌監控。
4. 選擇儲存。

> **Note**
>
> 最多可能需要 24 小時才會更新成員帳戶的組態。

使用帳戶頁面

1. 在導覽窗格中，選擇帳戶。
2. 在帳戶頁面上，選擇自動啟用偏好設定，然後再透過邀請新增帳戶。
3. 在管理自動啟用偏好設定視窗中，選擇 EKS 稽核日誌監控下的為所有帳戶啟用。
4. 選擇儲存。

如果您無法使用為所有帳戶啟用的選項，而且想要為組織中的特定帳戶自訂 EKS 稽核日誌監控組態，請參閱選擇性地為成員帳戶啟用或停用 EKS 稽核日誌監控。

API/CLI

- 若要為您的成員帳戶選擇性地啟用或停用 EKS 稽核日誌監控，請使用您自己的*### ID* 執行 updateMemberDetectors API 操作。
- 以下範例顯示如何為單一成員帳戶啟用 EKS 稽核日誌監控。若要停用，請使用 DISABLED 取代 ENABLED。

  要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

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

> **Note**
>
> 您也可以傳遞以空格分隔的帳戶 ID 清單。

- 當程式碼成功執行時，會返回一個空白 UnprocessedAccounts 清單。如果變更帳戶的偵測器設定時發生任何問題，則會列出該帳戶 ID 以及問題摘要。

為所有現有作用中成員帳戶啟用 EKS 稽核日誌監控

選擇您偏好的存取方式，以便為組織中所有現有作用中成員帳戶啟用 EKS 稽核日誌監控。

Console

1. 請登入 AWS Management Console 並開啟 GuardDuty 主控台，網址為 https://console.aws.amazon.com/guardduty/。

   使用委派的 GuardDuty 系統管理員帳戶認證登入。
2. 在導覽窗格中，選擇 EKS 保護。
3. 在 EKS 防護頁面上，您可以檢視啟動的惡意程式碼GuardDuty掃描組態的目前狀態。在作用中成員帳戶區段下，選擇動作。
4. 從動作下拉式選單中，選擇為所有作用中的成員帳戶啟用。
5. 選擇儲存。

API/CLI

- 若要為您的成員帳戶選擇性地啟用或停用 EKS 稽核日誌監控，請使用您自己的*### ID* 執行 updateMemberDetectors API 操作。
- 以下範例顯示如何為單一成員帳戶啟用 EKS 稽核日誌監控。若要停用，請使用 DISABLED 取代 ENABLED。

  要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

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

> **Note**
>
> 您也可以傳遞以空格分隔的帳戶 ID 清單。

- 當程式碼成功執行時，會返回一個空白 UnprocessedAccounts 清單。如果變更帳戶的偵測器設定時發生任何問題，則會列出該帳戶 ID 以及問題摘要。

為新成員帳戶自動啟用 EKS 稽核日誌監控

新增的成員帳戶必須 GuardDuty 先啟用，才能選取設定啟 GuardDuty動的惡意程式碼掃描。受邀請管理的成員帳戶可以手動為其帳戶配置 GuardDuty啟動的惡意軟件掃描。如需詳細資訊，請參閱 Step 3 - Accept an invitation。

選擇您偏好的存取方式，以便為加入組織的新帳戶啟用 EKS 稽核日誌監控。

Console

委派的 GuardDuty 系統管理員帳戶可以使用 [EKS 稽核記錄監視] 或 [帳戶] 頁面，針對組織中的新成員帳戶啟用 EKS 稽核記錄監視。

為新成員帳戶自動啟用 EKS 稽核日誌監控

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/

   請務必使用委派的 GuardDuty 系統管理員帳戶認證。

2. 執行以下任意一項：
   - 使用 EKS 保護頁面：
     1. 在導覽窗格中，選擇 EKS 保護。
     2. 在 EKS 保護頁面上，選擇 EKS 稽核日誌監控中的編輯。
     3. 選擇手動設定帳戶。
     4. 選取為新成員帳戶自動啟用。此步驟可確保每當有新帳戶加入您的組織時，EKS 稽核日誌監控都會自動為其帳戶啟用。只有組織委派的 GuardDuty 管理員帳戶可以修改此組態。
     5. 選擇儲存。
   - 使用帳戶頁面：
     1. 在導覽窗格中，選擇帳戶。
     2. 在帳戶頁面上，選擇自動啟用偏好設定。
     3. 在管理自動啟用偏好設定視窗中，選擇 EKS 稽核日誌監控下的為新帳戶啟用。
     4. 選擇儲存。

API/CLI

- 若要為新帳戶選擇性地啟用或停用 EKS 稽核日誌監控，請使用您自己的*### ID* 執行 UpdateOrganizationConfigurationAPI 操作。
- 下列範例顯示如何為加入組織的新成員啟用 EKS 稽核日誌監控。您也可以傳遞以空格分隔的帳戶 ID 清單。

  要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

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

選擇性地為成員帳戶啟用或停用 EKS 稽核日誌監控

選擇您偏好的存取方式，以便為組織中的指定成員帳戶啟用或停用 EKS 稽核日誌監控。

Console

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/

   請務必使用委派的 GuardDuty 系統管理員帳戶認證。
2. 在導覽窗格中，選擇帳戶。

   在帳戶頁面上，檢閱 EKS 稽核日誌監控欄位，了解您的成員帳戶狀態。
3. 啟用或停用 EKS 稽核日誌監控

   選取您想要設定進行 EKS 稽核日誌監控的帳戶。您可以一次選取多個帳戶。在編輯保護計畫下拉式選單中，選擇 EKS 稽核日誌監控，然後選擇適當的選項。

API/CLI

若要為您的成員帳戶選擇性地啟用或停用 EKS 稽核日誌監控，請使用您自己的*### ID* 調用 updateMemberDetectors API 操作。

以下範例顯示如何為單一成員帳戶啟用 EKS 稽核日誌監控。若要停用，請使用 DISABLED 取代 ENABLED。您也可以傳遞以空格分隔的帳戶 ID 清單。

要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

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

Amazon 的 Lambda 保護 GuardDuty

當在 AWS 環境中調用 AWS Lambda 函數時，Lambda 保護可協助您識別潛在安全威脅。啟用 Lambda 保護時， GuardDuty 開始監視 Lambda 網路活動日誌，VPC 流量日誌從所有帳戶的 Lambda 函數開始監控，包括那些不使用 VPC 聯網的日誌，並在叫用 Lambda 函數時產生。如果 GuardDuty 識別出表示 Lambda 函數中存在潛在惡意程式碼片段的可疑網路流量， GuardDuty 將會產生發現。

> **Note**
>
> Lambda 網路活動監控不包含 Lambda@Edge 函數的日誌。

您可以隨時為任何帳戶或可用 AWS 區域帳戶設定 Lambda 保護。根據預設，現有 GuardDuty 帳戶可以在 30 天的試用期內啟用 Lambda 保護。對於新 GuardDuty 帳戶，Lambda 保護已啟用，並包含在 30 天試用期內。如需有關用量統計資料的資訊，請參閱估算成本。

GuardDuty 監控叫用 Lambda 函數所產生的網路活動記錄。目前，Lambda 網路活動監控包含來自您帳戶的所有 Lambda 函數的 Amazon VPC 流量日誌，包括那些不使用 VPC 網路且可能會變更的日誌，包括擴展至其他網路活動，例如透過調用 Lambda 函數產生的 DNS 查詢資料。擴展到其他形式的網路活動監控會增加 Lambda 保護處理的資料量。 GuardDuty 這將直接影響 Lambda 保護的用量成本。每當 GuardDuty 開始監視其他網路活動記錄時，都會在發行前至少 30 天向已開啟 Lambda 保護的帳戶提供通知。

Lambda 保護中的功能

Lambda 網路活動監控

啟用 Lambda 保護時，會 GuardDuty 監控呼叫與您帳戶相關聯的 Lambda 函數時所產生的 Lambda 網路活動記錄。這可協助您偵測 Lambda 函數的潛在安全威脅。 GuardDuty 監控來自所有 Lambda 函數的 VPC 流程日誌，包括那些不使用 VPC 網路的函數。對於設定為使用虛擬私人雲端網路的 Lambda 函數，您不需要為 Lambda 為其建立的彈性網路介面 (ENI) 啟用 VPC 流程記錄。 GuardDuty GuardDuty 僅針對已處理的 Lambda 網路活動記錄資料量 (以 GB 為單位) 收取費用，以產生發現項目。 GuardDuty 套用智慧型篩選器，並分析與威脅偵測相關的 Lambda 網路活動記錄子集，以最佳化成本。如需有關定價的資訊，請參閱 Amazon GuardDuty 定價。

GuardDuty 不會管理您的 Lambda 網路活動記錄 (包括 VPC 和非 VPC 流程記錄)，也不會在您的帳戶中存取這些記錄。

設定 Lambda 保護

為獨立帳戶設定 Lambda 保護

對於與相關聯的帳戶 AWS Organizations，您可以透過 GuardDuty主控台或 API 指示自動執行此程序，如下一節所述。

選擇您偏好的存取方式，為獨立帳戶啟用或停用 Lambda 保護。

Console

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/
2. 在導覽窗格中的設定下，選擇 Lambda 保護。
3. Lambda 保護頁面會顯示您帳戶的目前狀態。您可以隨時透過分別選取啟用或停用來啟用或停用此功能。
4. 選擇儲存。

API/CLI

使用您自己的區域偵測器 ID，並透過將 `name` 設定為 `LAMBDA_NETWORK_LOGS` 及將 `status` 設定為 `ENABLED` 或 `DISABLED` 來傳遞 `features` 物件，從而執行 updateDetector API 操作。

您也可以執行下列命令來啟用或停用 Lambda 網路活動監 AWS CLI 控。請務必使用您自己的有效*### ID*。

> **Note**
>
> 下列範例程式碼可啟用 Lambda 網路活動監控。若要停用，請使用 `DISABLED` 取代 `ENABLED`。

要查找您`detectorId`的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

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

在多帳戶環境中設定 Lambda 保護

在多帳戶環境中，只有委派的 GuardDuty 管理員帳戶可以選擇為其組織中的成員帳戶啟用或停用 Lambda 保護。成 GuardDuty 員帳戶無法從其帳戶修改此設定。委派的 GuardDuty 系統管理員帳戶會使用 AWS Organizations。委派的 GuardDuty 管理員帳戶可以選擇在所有新帳戶加入組織時自動啟用 Lambda 網路活動監控。如需有關多帳戶環境的詳細資訊，請參閱在 Amazon GuardDuty 中管理多個帳戶。

為委派 GuardDuty 管理員帳戶設定 Lambda 保護

選擇您偏好的存取方法，以針對委派的 GuardDuty 管理員帳戶啟用或停用 Lambda 網路活動監控。

Console

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/

   確保使用管理帳戶憑證。
2. 在導覽窗格中的設定下，選擇 Lambda 保護。
3. 在 Lambda 保護頁面上，選擇編輯。
4. 執行以下任意一項：

   使用為所有帳戶啟用

   - 選擇為所有帳戶啟用。這將啟用 AWS 組織中所有作用中 GuardDuty 帳戶的保護計劃，包括加入組織的新帳戶。
   - 選擇儲存。

   使用手動設定帳戶

   - 若要僅針對委派的 GuardDuty 系統管理員帳戶啟用保護方案，請選擇 [手動設定帳戶]。
   - 在 [委派 GuardDuty 管理員帳戶 (此帳戶)] 區段下選擇 [啟用]。
   - 選擇儲存。

API/CLI

使用您自己的區域偵測器 ID，並透過將 `name` 設定為 `LAMBDA_NETWORK_LOGS` 及將 `status` 設定為 `ENABLED` 或 `DISABLED` 來傳遞 `features` 物件，從而執行 updateDetector API 操作。

您可以執行下列命令來啟用或停用 Lambda 網路活動監 AWS CLI 控。確保使用委派 GuardDuty 管理員帳戶的有效*### ID*。

> **Note**
>
> 下列範例程式碼可啟用 Lambda 網路活動監控。若要停用，請使用 DISABLED 取代 ENABLED。

要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

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

為所有成員帳戶自動啟用 Lambda 網路活動監控

選擇您偏好的存取方式，為所有成員帳戶啟用 Lambda 網路活動監控功能。這包括現有的成員帳戶和加入組織的新帳戶。

Console

1. 請登入 AWS Management Console 並開啟 GuardDuty 主控台，網址為 https://console.aws.amazon.com/guardduty/。

   請務必使用委派的 GuardDuty 系統管理員帳戶認證。

2. 執行以下任意一項：

   使用 Lambda 保護頁面

   1. 在導覽窗格中，選擇 Lambda 保護。
   2. 選擇為所有帳戶啟用。此動作會自動為組織中的現有帳戶和新帳戶啟用 Lambda 網路活動監控。
   3. 選擇儲存。

> **Note**
>
> 最多可能需要 24 小時才會更新成員帳戶的組態。

使用帳戶頁面

1. 在導覽窗格中，選擇帳戶。
2. 在帳戶頁面上，選擇自動啟用偏好設定，然後再透過邀請新增帳戶。
3. 在管理自動啟用偏好設定視窗中，選擇 Lambda 網路活動監控下的為所有帳戶啟用。

> **Note**
>
> 依預設，此動作會自動開啟自動啟 GuardDuty 用新成員帳戶選項。

4. 選擇儲存。

如果您無法使用為所有帳戶啟用選項，請參閱 選擇性地為成員帳戶啟用或停用 Lambda 網路活動監控。

API/CLI

- 若要為您的成員帳戶選擇性地啟用或停用 Lambda 網路活動監控，請使用您的*### ID* 調用 updateMemberDetectors API 操作。
- 以下範例顯示如何為單一成員帳戶啟用 Lambda 網路活動監控。若要停用成員帳戶，請使用 DISABLED 取代 ENABLED。

  要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

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

  您也可以傳遞以空格分隔的帳戶 ID 清單。

- 當程式碼成功執行時，會返回一個空白 UnprocessedAccounts 清單。如果變更帳戶的偵測器設定時發生任何問題，則會列出該帳戶 ID 以及問題摘要。

為所有現有作用中成員帳戶啟用 Lambda 網路活動監控

選擇您偏好的存取方式，為組織中所有現有作用中成員帳戶啟用 Lambda 網路活動監控。

Console

為所有現有作用中成員帳戶設定 Lambda 網路活動監控

1. 請登入 AWS Management Console 並開啟 GuardDuty 主控台，網址為 https://console.aws.amazon.com/guardduty/。

   使用委派的 GuardDuty 系統管理員帳戶認證登入。
2. 在導覽窗格中，選擇 Lambda 保護。
3. 在 Lambda 保護頁面上，您可以檢視組態的目前狀態。在作用中成員帳戶區段下，選擇動作。
4. 從動作下拉式選單中，選擇為所有作用中的成員帳戶啟用。
5. 選擇確認。

API/CLI

- 若要為您的成員帳戶選擇性地啟用或停用 Lambda 網路活動監控，請使用您的*### ID* 調用 updateMemberDetectors API 操作。
- 以下範例顯示如何為單一成員帳戶啟用 Lambda 網路活動監控。若要停用成員帳戶，請使用 DISABLED 取代 ENABLED。

  要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

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

  您也可以傳遞以空格分隔的帳戶 ID 清單。
- 當程式碼成功執行時，會返回一個空白 UnprocessedAccounts 清單。如果變更帳戶的偵測器設定時發生任何問題，則會列出該帳戶 ID 以及問題摘要。

為新成員帳戶自動啟用 Lambda 網路活動監控

選擇您偏好的存取方式，為加入組織的新帳戶啟用 Lambda 網路活動監控。

Console

委派的 GuardDuty 管理員帳戶可以使用 Lambda 保護或帳戶頁面，為組織中的新成員帳戶啟用 Lambda 網路活動監控。

為新成員帳戶自動啟用 Lambda 網路活動監控

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/

   請務必使用委派的 GuardDuty 系統管理員帳戶認證。

2. 執行以下任意一項：
   - 使用 Lambda 保護頁面：
     1. 在導覽窗格中，選擇 Lambda 保護。
     2. 在 Lambda 保護頁面上，選擇編輯。
     3. 選擇手動設定帳戶。
     4. 選取為新成員帳戶自動啟用。此步驟可確保每當有新帳戶加入您的組織時，即會為該帳戶自動啟用 Lambda 保護。只有組織委派的 GuardDuty 管理員帳戶可以修改此組態。
     5. 選擇儲存。
   - 使用帳戶頁面：
     1. 在導覽窗格中，選擇帳戶。
     2. 在帳戶頁面上，選擇自動啟用偏好設定。
     3. 在管理自動啟用偏好設定視窗中，選取 Lambda 網路活動監控下的為新帳戶啟用。
     4. 選擇儲存。

API/CLI

- 若要為新成員帳戶啟用或停用 Lambda 網路活動監控，請使用您的*### ID* 調用 UpdateOrganizationConfiguration API 操作。
- 以下範例顯示如何為單一成員帳戶啟用 Lambda 網路活動監控。若要停用，請參閱選擇性地為成員帳戶啟用或停用 Lambda 網路活動監控。如果您不想為加入組織的所有新帳戶啟用此功能，請將 `AutoEnable` 設定為 `NONE`。

要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

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

您也可以傳遞以空格分隔的帳戶 ID 清單。

- 當程式碼成功執行時，會返回一個空白 UnprocessedAccounts 清單。如果變更帳戶的偵測器設定時發生任何問題，則會列出該帳戶 ID 以及問題摘要。

選擇性地為成員帳戶啟用或停用 Lambda 網路活動監控

選擇您偏好的存取方式，以便選擇性地為成員帳戶啟用或停用 Lambda 網路活動監控。

Console

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/

   請務必使用委派的 GuardDuty 系統管理員帳戶認證。

2. 在導覽窗格中，於設定下選擇帳戶。

   在帳戶頁面上，檢閱 Lambda 網路活動監控資料欄。這會指示是否已啟用 Lambda 網路活動監控。

3. 選擇您要設定 Lambda 保護的帳戶。您可以一次選擇多個帳戶。
4. 從編輯保護計畫下拉式選單中，選擇 Lambda 網路活動監控，然後選擇適當的動作。

API/CLI

使用您的### *ID* 調用 updateMemberDetectors API。

以下範例顯示如何為單一成員帳戶啟用 Lambda 網路活動監控。若要停用，請使用 DISABLED 取代 ENABLED。

要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

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

您也可以傳遞以空格分隔的帳戶 ID 清單。

當程式碼成功執行時，會返回一個空白 UnprocessedAccounts 清單。如果變更帳戶的偵測器設定時發生任何問題，則會列出該帳戶 ID 以及問題摘要。

Amazon 中的惡意軟件 GuardDuty

惡意軟體防護可透過掃描連接至 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體和容器工作負載的 Amazon Elastic Block Store (Amazon EBS) 磁碟區，協助您偵測潛在的惡意軟體。惡意軟體防護提供掃描選項，讓您決定是否要在掃描時包含或排除特定 Amazon EC2 執行個體和容器工作負載。它還提供了一個選項，可將連接到 Amazon EC2 執行個體或容器工作負載的 Amazon EBS 磁碟區快照保留在您的 GuardDuty 帳戶中。只有在發現惡意軟體並產生惡意軟體防護調查結果時，才會保留快照。

惡意軟體防護提供兩種類型的掃描，以偵測 Amazon EC2 執行個體和容器工作負載中潛在惡意活動 — GuardDuty 啟動的惡意軟體掃描和隨選惡意軟體掃描。下表顯示了兩種掃描類型之間的比較。

Factor	GuardDuty-發起的惡意軟件掃	隨需惡意軟體掃描
如何調用掃描	啟用啟動的惡意軟體掃描後，每當 GuardDuty 產生指出 Amazon EC2 執行個體或容器工作負載中可能存在惡意軟體的 GuardDuty發現時，都會在連接至潛在影響資源的 Amazon EBS 磁碟區上 GuardDuty 自動啟動無代理程式惡意軟體掃描。如需詳細資訊，請參閱 GuardDuty-發起的惡意軟件掃。	您可以透過提供與 Amazon EC2 執行個體或容器工作負載關聯的 Amazon Resource Name (ARN) 來啟動隨需惡意軟體掃描。即使沒有針對您的資源產生任何 GuardDuty 發現，您也可以啟動指定惡意程式碼掃描。如需詳細資訊，請參閱 隨需惡意軟體掃描。
需要的配置	若要使用啟 GuardDuty動的惡意程式碼掃描，您必須為您的帳戶啟用它。如需詳細資訊，請參閱 設定起始 GuardDuty的惡意軟體掃描。	您的帳戶必須已 GuardDuty 啟用。若要使用指定惡意程式碼掃描，功能層級不需要設定。
等待時間初始化新掃描	每當 GuardDuty 產生其中一個時呼叫 GuardDuty起始惡意軟體掃描的發現項目，惡意軟體掃描只會每 24 小時自動啟動一次。	您可以在上一次掃描開始時間起 1 小時後，隨時在相同資源上啟動指定惡意程式碼掃描。

Factor	GuardDuty-發起的惡意軟件掃	隨需惡意軟體掃描
30 天免費試用期的可用性	當您第一次在帳戶中啟用GuardDuty開始的惡意程式碼掃描時，您可以使用 30 天的免費試用期 *。	針對新帳戶或現有 GuardDuty帳戶的隨選惡意軟體掃描，沒有免費試用期 *。
掃描選項	設定好 GuardDuty啟動的惡意程式碼掃描之後，惡意程式碼防護也可協助您選取要掃描或略過的資源。惡意軟體防護不會對您選擇從掃描中排除的資源啟動自動掃描。	按需惡意軟體掃描支援全域標籤 — `GuardDuty Excluded` 。 具有使用者定義標籤的掃描選項不適用於指定惡意軟體掃描，因為您手動提供資源 ARN。

* 建立 EBS 磁碟區快照並保留快照會產生使用費。如需設定帳戶以保留快照的詳細資訊，請參閱快照保留。

惡意程式碼防護是選擇性的增強功能，其設計方式不會影響資源效能。 GuardDuty如需有關「惡意程式碼防護」如何在中運作的資訊 GuardDuty惡意軟體防護的功能，如需有關不同之惡意程式碼防護可用性的資訊 AWS 區域，請參閱區域與端點。

> **Note**
>
> GuardDuty 惡意軟體防護不支援 Amazon EKS 或 Amazon ECS 的 Fargate。

惡意軟體防護的功能

Elastic Block Storage (EBS) 磁碟區

本節說明惡意軟體防護 (包括 GuardDuty啟動的惡意軟體掃描和隨選惡意軟體掃描) 如何掃描與 Amazon EC2 執行個體和容器工作負載關聯的 Amazon EBS 磁碟區。繼續前，請考慮下列自訂內容：

- 掃描選項：惡意軟體防護提供指定標籤的功能，以在掃描程序中包含或排除 Amazon EC2 執行個體和 Amazon EBS 磁碟區。只有 GuardDuty開始的惡意程式碼掃描支援含使用者定義標籤的掃描GuardDuty啟動的惡意程式碼掃描和指定惡意軟體掃描都支援全域`GuardDutyExcluded`標籤。如需詳細資訊，請參閱 具有使用者定義標籤的掃描選項。

- 快照保留 — 惡意軟體防護可讓您選擇在 AWS 帳戶中保留 Amazon EBS 磁碟區的快照。根據預設，此選項為關閉。您可以選擇保留 GuardDuty 已啟動和隨選惡意軟體掃描的快照保留。如需詳細資訊，請參閱 快照保留。

當 GuardDuty 產生指示 Amazon EC2 執行個體或容器工作負載中可能存在惡意軟體的發現，且您已在惡意軟體防護中啟用 GuardDuty 初始掃描類型時，系統可能會根據您的掃描選項叫用 GuardDuty起始的惡意軟體掃描。

若要在與 Amazon EC2 執行個體關聯的 Amazon EBS 磁碟區上啟動隨需惡意軟體掃描，請提供 Amazon EC2 執行個體的 Amazon Resource Name (ARN)。

作為回應隨選惡意程式碼掃描或自動 GuardDuty啟動的惡意軟體掃描， GuardDuty 建立連接至潛在受影響資源的相關 EBS 磁碟區的快照，並與. GuardDuty 服務帳戶 從這些快照集中，在服務帳戶中 GuardDuty 建立加密複本 EBS 磁碟區。

掃描完成後， GuardDuty 刪除 EBS 磁碟區的加密複本和 EBS 磁碟區的快照。如果發現惡意軟體且您已開啟快照保留設定，EBS 磁碟區的快照不會遭到刪除，而且會自動保留在您的 AWS 帳戶中。找不到惡意軟體時，無論快照保留設定為何，EBS 磁碟區的快照都不會保留。依預設，快照保留設定為關閉。如需快照成本及保留的相關資訊，請參閱 Amazon EBS 定價。

GuardDuty 將服務帳戶中的每個複本 EBS 磁碟區保留最多 55 小時。如果 EBS 磁碟區複本及其惡意軟體掃描發生服務中斷或故障， GuardDuty 將保留此類 EBS 磁碟區不超過七天。延長的磁碟區保留期是分類和解決中斷或故障。 GuardDuty 惡意程式碼防護會在解決中斷或故障解決後，或延長保留期限過後，從服務帳戶中刪除複本 EBS 磁碟區。

支援用於惡意軟體掃描的 Amazon EBS 磁碟區

在所有 GuardDuty 支援惡意軟體防護功能的 AWS 區域 地方，您都可以掃描未加密或加密的 Amazon EBS 磁碟區。您可以擁有使用其中一個AWS 受管金鑰或客戶受管金鑰加密的 Amazon EBS 磁碟區。目前，某些 AWS 區域 支援既是加密 Amazon EBS 磁碟區的方式，其他支援則只支援客戶受管金鑰。

如需尚未支援此功能的詳細資訊，請參閱 China Regions

下列清單說明 GuardDuty 使用 Amazon EBS 磁碟區是否已加密的金鑰：

- 使用未加密或加密的 Amazon EBS 磁碟區 AWS 受管金鑰 — GuardDuty 使用其自己的金鑰來加密複本 Amazon EBS 磁碟區。

  如果您的帳戶屬於不支援掃描使用 EBS 預設值加密的 Amazon EBS 磁碟區的帳戶， AWS 受管金鑰請參閱。 AWS 區域 修改 Amazon EBS 磁碟區的預設 AWS KMS 金鑰識別碼

- 使用客戶受管金鑰加密的 Amazon EBS 磁碟區 — GuardDuty 使用相同的金鑰來加密複本 EBS 磁碟區。

惡意軟體防護不支援使用 `productCode` as 掃描 Amazon EC2 執行個體`marketplace`。如果針對此類 Amazon EC2 執行個體啟動惡意軟體掃描，則會略過掃描。如需詳細資訊，請參閱 惡意軟體掃描期間略過資源的原因 中的 `UNSUPPORTED_PRODUCT_CODE_TYPE`。

修改 Amazon EBS 磁碟區的預設 AWS KMS 金鑰識別碼

依預設，在將加密設定為`true`且不指定 KMS 金鑰識別碼的情況下呼叫 CreateVolumeAPI，會建立一個 Amazon EBS 磁碟區，該磁碟區會使用 EBS 加密的預設金 AWS KMS 鑰加密。但是，如果未明確提供加密金鑰，您可以叫用 ModifyEbsDefaultKmsKeyIdAPI 或使用對應的 AWS CLI 命令來修改預設金鑰。

若要修改 EBS 預設金鑰 ID，請將下列必要許可新增至 IAM 政策：`ec2:modifyEbsDefaultKmsKeyId`。任何您選擇加密但未指定關聯 KMS 金鑰識別碼的新建立 Amazon EBS 磁碟區，都會使用預設金鑰識別碼。使用下列其中一種方法來更新 EBS 預設金鑰識別碼：

修改 Amazon EBS 磁碟區的預設 KMS 金鑰 ID

執行以下任意一項：

- 使用 API — 您可以使用 ModifyEbsDefaultKmsKeyIdAPI。如需如何檢視磁碟區加密狀態的相關資訊，請參閱建立 Amazon EBS 磁碟區。
- 使用 AWS CLI 命令 — 下列範例會修改預設 KMS 金鑰識別碼，如果您未提供 KMS 金鑰識別碼，該識別碼將加密 Amazon EBS 磁碟區。確保將區域替換為您 AWS 區域 的 KM 密鑰 ID。

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

以上命令會產生與下列輸出類似的輸出：

```
{
  "KmsKeyId": "arn:aws:kms:us-west-2:444455556666:key/AKIAIOSFODNN7EXAMPLE"
}
```

如需詳細資訊，請參閱 modify-ebs-default-kms-key-id。

惡意軟體防護中的自訂項目

本節說明如何在呼叫惡意軟體掃描時 (隨需或透過啟動) 自訂 Amazon EC2 執行個體或容器工作負載的掃描選項 GuardDuty。

一般設定

快照保留

GuardDuty 為您提供在 AWS 帳戶中保留 EBS 磁碟區快照的選項。依預設，快照保留設定為關閉。只有在掃描開始前開啟此設定時，才會保留快照。

掃描開始時， GuardDuty 會根據 EBS 磁碟區的快照產生複本 EBS 磁碟區。掃描完成且帳戶中的快照保留設定已開啟後，只有在找到惡意軟體並產生 惡意軟體防護調查結果類型 時，EBS 磁碟區的快照才會保留。無論您是否開啟快照保留設定，當未偵測到惡意程式碼時，都 GuardDuty 會自動刪除 EBS 磁碟區的快照。

快照使用費

在惡意軟體掃描期間， GuardDuty 建立 Amazon EBS 磁碟區的快照時，此步驟會產生相關的使用費用。如果您開啟帳戶的快照保留設定，當發現惡意軟體並保留快照時，將會產生相同的使用費。如需有關快照成本及保留的相關資訊，請參閱 Amazon EBS 定價。

選擇您偏好的存取方式，以便開啟快照保留設定。

Console

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/
2. 在導覽窗格的保護計畫下，選擇惡意軟體防護。
3. 選擇主控台底部的一般設定。若要保留快照，請開啟快照保留。

API/CLI

1. 執行UpdateMalwareScanSettings以更新快照保留設定的目前組態。
2. 或者，您也可以執行下列 AWS CLI 命令，在 GuardDuty 惡意程式碼防護產生發現項目時自動保留快照。

   確保使用您自己的有效 `detectorId` 取代 *`detector-id`*。

3. 要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

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

4. 如果您想要關閉快照保留功能，請使用 NO_RETENTION 取代 RETENTION_WITH_FINDING。

具有使用者定義標籤的掃描選項

透過使用 GuardDuty啟動的惡意軟體掃描，您也可以指定標籤，在掃描和威脅偵測程序中包含或排除 Amazon EC2 執行個體和 Amazon EBS 磁碟區。您可以透過編輯包含或排除標籤清單中的標籤來自訂每個 GuardDuty起始的惡意程式碼掃描。每個清單最多可包含 50 個標籤。

如果您還沒有與 EC2 資源相關聯的使用者定義標籤，請參閱《Amazon EC2 Linux 執行個體使用者指南》中的標記您的 Amazon EC2 資源，或在《Amazon EC2 Windows 執行個體使用者指南》中標記您的 Amazon EC2 資源。

> **Note**
>
> 隨需惡意軟體掃描不支援具有使用者定義標籤的掃描選項 支援 全域 GuardDutyExcluded 標籤。

在惡意軟體掃描中排除 EC2 執行個體

如果您想要在掃描過程中排除任何 Amazon EC2 執行個體或 Amazon EBS 磁碟區，可以將任何 Amazon EC2 執行個體或 Amazon EBS 磁碟區的GuardDutyExcluded標籤設定true為，而 GuardDuty 不會進行掃描。如需有關 GuardDutyExcluded 標籤的詳細資訊，請參閱惡意軟體防護的服務連結角色許可。您也可以將 Amazon EC2 執行個體標籤新增至排除清單。如果您在排除標籤清單中新增多個標籤，則包含其中至少一個標籤的任何 Amazon EC2 執行個體都將從惡意軟體掃描過程中排除。

選擇您偏好的存取方法，以便將與 Amazon EC2 執行個體關聯的標籤新增至排除清單。

Console

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/

2. 在導覽窗格的保護計畫下，選擇惡意軟體防護。
3. 展開包含/排除標籤區段。選擇 Add tags (新增標籤)。
4. 選擇排除標籤，然後選擇確認。
5. 指定您要排除的標籤 **Key** 和 **Value** 對。可選擇性提供 **Value**。新增所有標籤後，請選擇儲存。

> **Important**
>
> 標籤金鑰與值皆區分大小寫。如需有關詳細資訊，請參閱《Amazon EC2 Linux 執行個體使用者指南》中的標籤限制或《Amazon EC2 Windows 執行個體使用者指南》中的標籤限制。

如果未提供金鑰的值，且 EC2 執行個體已標記指定的金鑰，則無論標籤的指派值為何，此 EC2 執行個體都會從 GuardDuty啟動的惡意程式碼掃描程序中排除。

API/CLI

- 透過從掃描過程中排除 EC2 執行個體或容器工作負載，以更新惡意軟體掃描設定。

  下列 AWS CLI 範例指令會將新標籤新增至例外標籤清單。確保使用您自己的有效 `detectorId` 取代範例 *`detector-id`*。

  `MapEquals` 是 Key/Value 對的清單。

  要查找您`detectorId`的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

```
aws guardduty update-malware-scan-settings --detector-
id 60b87779336485625 54d637e0e4bb3b2 --scan-resource-criteria '{"Exclude":
 {"EC2_INSTANCE_TAG" : {"MapEquals": [{ "Key": "TestKeyWithValue", "Value":
 "TestValue" }, {"Key":"TestKeyWithoutValue"} ]}}}' --ebs-snapshot-preservation
 "RETENTION_WITH_FINDING"
```

> **Important**
>
> 標籤金鑰與值皆區分大小寫。如需有關詳細資訊，請參閱《Amazon EC2 Linux 執行個體使用者指南》中的標籤限制或《Amazon EC2 Windows 執行個體使用者指南》中的標籤限制。

在惡意軟體掃描中包含 EC2 執行個體

如果要掃描 EC2 執行個體，請將其標籤新增至包含清單。當您將標籤新增至包含標籤清單時，惡意軟體掃描會略過不包含任何新增標籤的 EC2 執行個體。如果您在包含標籤清單中新增多個標籤，則惡意軟體掃描中會包含至少包含其中一個標籤的 EC2 執行個體。有時，在掃描過程中可能會略過 EC2 執行個體。如需詳細資訊，請參閱 惡意軟體掃描期間略過資源的原因。

選擇您偏好的存取方法，以便將與 EC2 執行個體關聯的標籤新增至包含清單。

Console

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/
2. 在導覽窗格的保護計畫下，選擇惡意軟體防護。
3. 展開包含/排除標籤區段。選擇 Add tags (新增標籤)。
4. 選擇包含標籤，然後選擇確認。
5. 選擇新增包含標籤，然後指定您要包含的標籤的 **`Key`** 和 **`Value`** 對。可選擇性提供 **`Value`**。

   新增所有包含標籤之後，請選擇儲存。

   如果未提供鍵值，且 EC2 執行個體已透過指定鍵標記，則無論標籤指派的值為何，此 EC2 執行個體都會包含在惡意軟體掃描程序中。

API/CLI

- 更新惡意軟體掃描設定，以在掃描過程中包含 EC2 執行個體或容器工作負載。

  下列 AWS CLI 範例指令會將新標籤新增至包含標籤清單。確保使用您自己的有效 `detectorId` 取代範例 *`detector-id`*。將範例以*`TestKey`*及*`TestValue`*與 EC2 資源關聯的標籤`Key`和`Value`配對取代。

  `MapEquals` 是 `Key/Value` 對的清單。

要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

```
aws guardduty update-malware-scan-settings --detector-
id 60b87779336485625554d637e0e4bb3b2 --scan-resource-criteria '{"Include":
 {"EC2_INSTANCE_TAG" : {"MapEquals": [{ "Key": "TestKeyWithValue", "Value":
 "TestValue" }, {"Key":"TestKeyWithoutValue"} ]}}}' --ebs-snapshot-preservation
 "RETENTION_WITH_FINDING"
```

> **Important**
>
> 標籤金鑰與值皆區分大小寫。如需有關詳細資訊，請參閱《Amazon EC2 Linux 執行個體使用者指南》中的標籤限制或《Amazon EC2 Windows 執行個體使用者指南》中的標籤限制。

> **Note**
>
> 偵測新標籤最多可能需 GuardDuty 要 5 分鐘的時間。

您可以隨時選擇包含標籤或排除標籤，但不能同時選擇兩者。如果您想要在標籤之間切換，請在新增標籤時從下拉式選單中選擇該標籤，然後確認您的選擇。此動作會清除所有目前的標籤。

全域 GuardDutyExcluded 標籤

依預設，EBS 磁碟區的快照會以 GuardDutyScanId 標籤建立。請勿移除此標籤，因為這樣做會導致GuardDuty無法存取快照。惡意軟體防護中的兩種掃描類型均不會掃描 GuardDutyExcluded 標籤設定為 true 的 Amazon EC2 執行個體或 Amazon EBS 磁碟區。如果針對此類資源進行惡意軟體防護掃描，則將生成掃描 ID，但掃描將由於 EXCLUDED_BY_SCAN_SETTINGS 原因而跳過。如需詳細資訊，請參閱 惡意軟體掃描期間略過資源的原因。

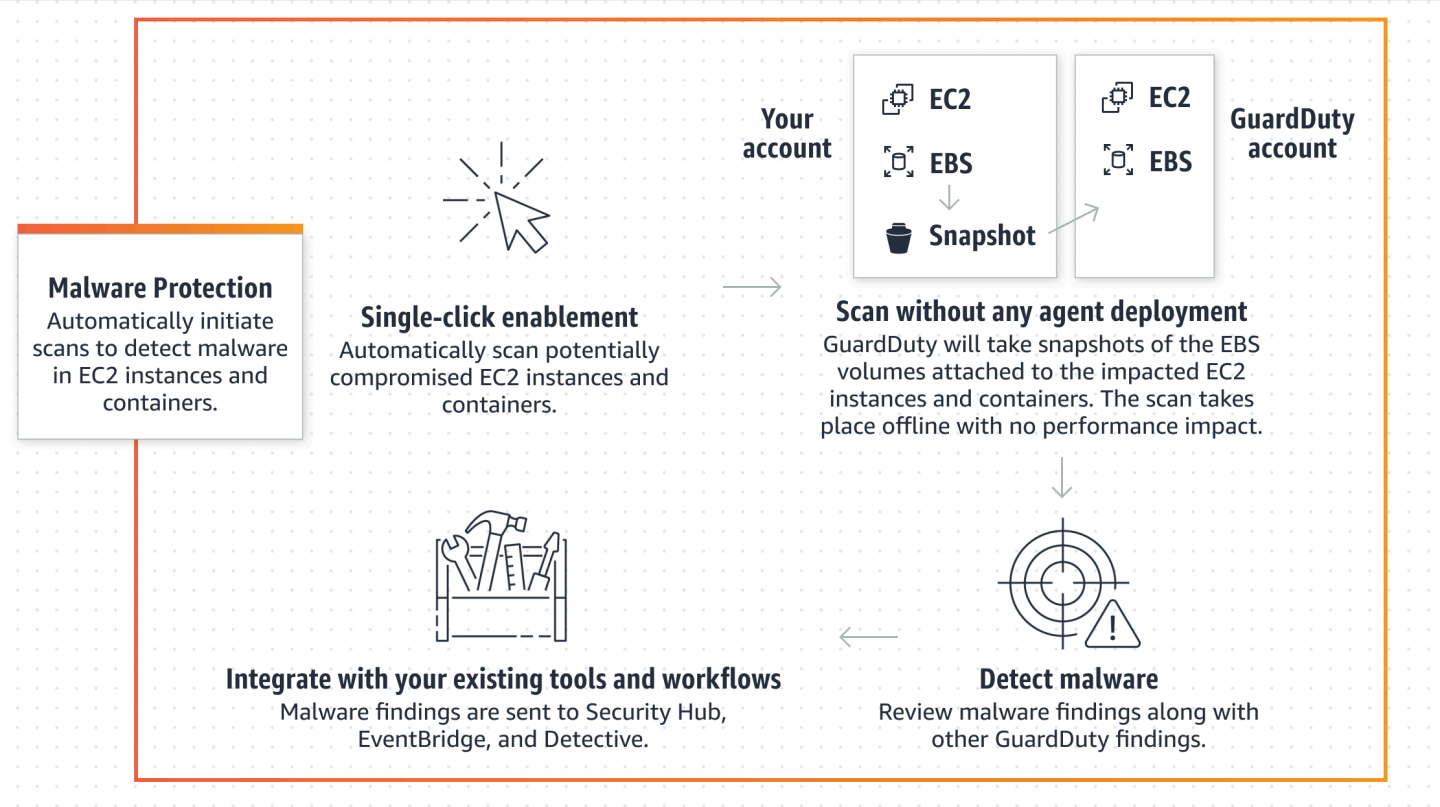
GuardDuty-發起的惡意軟件掃

啟用啟動的惡意軟體掃描後，每當 GuardDuty 偵測到指出 Amazon EC2 執行個體或容器工作負載中潛在存在惡意軟體的惡意活動並 GuardDuty 產生時呼叫 GuardDuty起始惡意軟體掃描的發現項目，都會在附加至潛在受影響的 Amazon Amazon EC2 執行個體或容器工作負載的 Elastic Block

Store (Amazon EBS) 磁碟區上 GuardDuty 自動啟動無代理程式掃描，以偵測是否存在惡意軟體。GuardDuty使用掃描選項，您可以新增與要掃描的資源相關聯的包含標籤，或新增與要從掃描程序略過的資源相關聯的排除標籤。自動掃描啟動始終會考慮您的掃描選項。您也可以選擇開啟快照保留設定，只有在惡意軟體防護偵測到存在惡意軟體時，才保留 EBS 磁碟區的快照。如需詳細資訊，請參閱 惡意軟體防護中的自訂項目。

對於 GuardDuty 產生發現結果的每個 Amazon EC2 執行個體和容器工作負載，每 24 小時會叫用一次自動 GuardDuty啟動的惡意軟體掃描。如需有關如何掃描連接至 Amazon EC2 執行個體或容器工作負載的 Amazon EBS 磁碟區的詳細資訊，請參閱惡意軟體防護的功能。

下圖說明啟動的惡意程式碼 GuardDuty掃描的運作方式。



當發現惡意軟件時， GuardDuty 生成惡意軟體防護調查結果類型。如果 GuardDuty 沒有在同一資源上產生指示惡意軟件的發現，則不會調用 GuardDuty啟動的惡意軟件掃描。您也可以在相同的資源上啟動隨需惡意軟體掃描。如需詳細資訊，請參閱 隨需惡意軟體掃描。

30 天免費試用期如何影響 GuardDuty 帳戶

您可以選擇隨時為任何帳戶或可用 AWS 區域帳戶開 GuardDuty啟或關閉啟動的惡意程式碼掃描功能。

- 當您第一次啟 GuardDuty 用 (新 GuardDuty 帳戶) 時，已開啟啟 GuardDuty動的惡意程式碼掃描，並包含在 30 天的免費試用期內。
- 現有 GuardDuty 帳戶可以在 30 天的免費試用期內首次開 GuardDuty啟啟動的惡意軟體掃描。
- 如果您的現有 GuardDuty 帳戶在隨選惡意軟體掃描正式推出之前一直在使用惡意軟體防護，而且此 GuardDuty 帳戶已使用定價模式 AWS 區域，則無需採取任何動作即可繼續使用 GuardDuty啟動的惡意軟體掃描。

> **Note**
>
> 如果您正處於 30 天的免費試用期內，建立 Amazon EBS 磁碟區快照及其保留的使用費仍然適用。如需詳細資訊，請參閱 Amazon EBS 定價。

如需啟用起始之惡意程式碼 GuardDuty掃描的資訊，請參閱設定起始 GuardDuty的惡意軟體掃描。

設定起始 GuardDuty的惡意軟體掃描

針對獨立 GuardDuty帳戶設定起始的惡意程式碼掃描

對於與相關聯的帳戶 AWS Organizations，您可以透過主控台設定自動執行此程序，如下一節所述。

啟用或停用起始的惡意程式碼 GuardDuty掃描

選擇您偏好的存取方法，以針對獨立帳戶設定 GuardDuty起始的惡意程式碼掃描。

Console

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/
2. 在導覽窗格的保護計畫下，選擇惡意軟體防護。
3. [惡意程式碼防護] 窗格會列出您帳戶所 GuardDuty啟動之惡意程式碼掃描的目前狀態。您可以隨時透過分別選取啟用或停用來啟用或停用它。
4. 選擇儲存。

API/CLI

- 使用您自己的區域偵測器 ID，並透過將 `EbsVolumes` 設定為 `true` 或 `false` 來傳遞 `dataSources` 物件，從而執行 updateDetector API 操作。

您也可以執行下 AWS CLI 列命令，使用 AWS 命令列工具啟用或停用啟 GuardDuty動的惡意程式碼掃描。請務必使用您自己的有效*### ID*。

> **Note**
>
> 下列範例程式碼會啟用 GuardDuty起始的惡意程式碼掃描。若要停用，請使用 `false` 取代 `true`。

要查找您`detectorId`的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

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

在多帳戶 GuardDuty環境中設定啟動的惡意程式碼掃描

在多帳戶環境中，只有 GuardDuty 系統管理員帳戶可以設定起始的惡意程式碼 GuardDuty掃描。GuardDuty 管理員帳戶可以啟用或禁用對其成員帳戶啟用或禁用啟 GuardDuty動的惡意軟件掃描。管理員帳戶為成員帳戶配置 GuardDuty啟動的惡意軟件掃描後，該成員帳戶將遵循管理員帳戶設置，並且無法通過控制台修改這些設置。 GuardDuty 透過 AWS Organizations 支援管理其成員帳戶的管理員帳戶帳戶，可以選擇在組織中的所有現有帳戶和新帳戶上自動啟用啟動的惡意軟體掃描。 GuardDuty 如需詳細資訊，請參閱 管理 GuardDuty 帳戶 AWS Organizations。

建立受信任的存取以啟 GuardDuty動惡意軟體掃描

如果 GuardDuty 委派的系統管理員帳戶與組織中的管理帳戶不同，則管理帳戶必須為其組織啟用 GuardDuty起始的惡意程式碼掃描。如此一來，委派的系統管理員帳戶就可以建立透過管理的 惡意軟體防護的服務連結角色許可 in 成員帳戶 AWS Organizations。

> **Note**
>
> 指定委派的 GuardDuty 管理員帳戶之前，請參閱考量和建議。

選擇您偏好的存取方法，以允許委派的 GuardDuty 系統管理員帳戶針對組織中的成員帳戶啟用 GuardDuty起始的惡意程式碼掃描。

Console

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/

   若要登入，請使用 AWS Organizations 組織的管理帳戶。

2. a. 如果您尚未指定委派 GuardDuty 管理員帳戶，則：

      在 [設定] 頁面的 [委派 GuardDuty 系統管理員帳戶] 下，輸入您**account ID**要指定用來管理組織中 GuardDuty 策略的 12 位數。選擇委派。

   b. i. 如果您已指定與管理帳戶不同的委派 GuardDuty 管理員帳戶，請執行下列動作：

      在設定頁面的委派管理員下，開啟許可設定。此動作將允許委派的 GuardDuty 管理員帳戶將相關權限附加到成員帳戶，並在這些成員帳戶中啟用啟 GuardDuty動的惡意軟體掃描。

      ii. 如果您已經指定了與 GuardDuty 管理帳戶相同的委派管理員帳戶，則可以直接為成員帳戶啟用啟 GuardDuty動的惡意軟體掃描。如需詳細資訊，請參閱 自動啟動所有成 GuardDuty員帳戶的惡意軟體掃描。

   > **Tip**
   >
   > 如果委派的系統管理 GuardDuty 員帳戶與您的管理帳戶不同，您必須提供委派 GuardDuty 系統管理員帳戶的權限，以允許針對成員帳戶啟用 GuardDuty起始的惡意程式碼掃描。

3. 如果您想要允許委派的 GuardDuty 系統管理員帳戶啟用 GuardDuty其他區域中成員帳戶的惡意程式碼掃描，請變更您的 AWS 區域，然後重複上述步驟。

API/CLI

1. 使用您的管理帳戶憑證，執行下列命令：

   ```
   aws organizations enable-aws-service-access --service-principal malware-
   protection.guardduty.amazonaws.com
   ```

2. (選擇性) 若要針對非委派系統管理員帳戶的管理帳戶啟用 GuardDuty-起始的惡意程式碼掃描，管理帳戶會先在其帳戶中惡意軟體防護的服務連結角色許可明確建立，然後從委派的系統管理員帳戶啟用啟 GuardDuty動的惡意程式碼掃描，類似於任何其他成員帳戶。

```
aws iam create-service-linked-role --aws-service-name malware-
protection.guardduty.amazonaws.com
```

3. 您已在目前選取的中指定委派 GuardDuty 管理員帳戶 AWS 區域。如果您已在某個區域中將帳戶指定為委派 GuardDuty 管理員帳戶，則該帳戶必須是您在所有其他區域中委派的 GuardDuty 管理員帳戶。為其他所有區域重複上述步驟。

為委派的 GuardDuty 管理員帳戶設定 GuardDuty啟動的惡意程式碼

選擇您偏好的存取方法，以啟用或停用 GuardDuty委派 GuardDuty 系統管理員帳戶的惡意程式碼掃描。

Console

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/

   確保使用管理帳戶憑證。
2. 在導覽窗格中，選擇惡意軟體防護。
3. 在 [惡意程式碼防護] 頁面上，選擇 [起GuardDuty始惡意程式碼掃描] 旁邊的 [
4. 執行以下任意一項：

   使用為所有帳戶啟用

   - 選擇為所有帳戶啟用。這將啟用 AWS 組織中所有作用中 GuardDuty 帳戶的保護計劃，包括加入組織的新帳戶。
   - 選擇儲存。

   使用手動設定帳戶

   - 若要僅針對委派的 GuardDuty 系統管理員帳戶啟用保護方案，請選擇 [手動設定帳戶]。
   - 在 [委派 GuardDuty 管理員帳戶 (此帳戶)] 區段下選擇 [啟用]。
   - 選擇儲存。

API/CLI

使用您自己的區域偵測器 ID，並透過將 `name` 設定為 `EBS_MALWARE_PROTECTION` 及將 `status` 設定為 `ENABLED` 或 `DISABLED` 來傳遞 `features` 物件，從而執行 updateDetector API 操作。

您可以通過運行以下 AWS CLI 命令啟用或禁用啟 GuardDuty動的惡意軟件掃描。確保使用委派 GuardDuty 管理員帳戶的有效*### ID*。

> **Note**
>
> 下列範例程式碼會啟用 GuardDuty起始的惡意程式碼掃描。若要停用，請使用 DISABLED 取代 ENABLED。

要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 /
              --account-ids 555555555555 /
              --features '[{"Name": "EBS_MALWARE_PROTECTION", "Status": "ENABLED"}]'
```

自動啟動所有成 GuardDuty員帳戶的惡意軟體掃描

選擇您偏好的存取方法，為所有成員帳戶啟用 GuardDuty起始的惡意軟體掃描功能。這包括現有的成員帳戶和加入組織的新帳戶。

Console

1. 請登入 AWS Management Console 並開啟 GuardDuty 主控台，網址為 https://console.aws.amazon.com/guardduty/。

   請務必使用委派的 GuardDuty 系統管理員帳戶認證。

2. 執行以下任意一項：

   使用惡意軟體防護頁面

   1. 在導覽窗格中，選擇惡意軟體防護。
   2. 在 [惡意程式碼防護] 頁面上，選擇啟動的惡意程式碼GuardDuty掃描區段中的 [編輯
   3. 選擇為所有帳戶啟用。此動作會自動 GuardDuty啟用組織中現有和新帳戶的惡意程式碼掃描。
   4. 選擇儲存。

> **Note**
>
> 最多可能需要 24 小時才會更新成員帳戶的組態。

使用帳戶頁面

1. 在導覽窗格中，選擇帳戶。
2. 在帳戶頁面上，選擇自動啟用偏好設定，然後再透過邀請新增帳戶。
3. 在 [管理自動啟用喜好設定] 視窗中，選擇 [啟動的惡意程式碼掃描] 下的所有帳戶GuardDuty啟用
4. 在 [惡意程式碼防護] 頁面上，選擇啟動的惡意程式碼GuardDuty掃描區段中的 [編輯
5. 選擇為所有帳戶啟用。此動作會自動 GuardDuty啟用組織中現有和新帳戶的惡意程式碼掃描。
6. 選擇儲存。

> **Note**
>
> 最多可能需要 24 小時才會更新成員帳戶的組態。

使用帳戶頁面

1. 在導覽窗格中，選擇帳戶。
2. 在帳戶頁面上，選擇自動啟用偏好設定，然後再透過邀請新增帳戶。
3. 在 [管理自動啟用喜好設定] 視窗中，選擇 [啟動的惡意程式碼掃描] 下的所有帳戶GuardDuty啟用
4. 選擇儲存。

如果您無法使用為所有帳戶啟用選項，請參閱 選擇性地啟用或停用成員 GuardDuty帳戶的惡意程式碼掃描。

API/CLI

- 要選擇性地為您的成員帳戶啟用或禁用啟 GuardDuty動的惡意軟件掃描，請使用您自己的*### ID* 調用 updateMemberDetectorsAPI 操作。
- 下列範例顯示如何針對單一成員帳戶啟用 GuardDuty起始的惡意程式碼掃描。若要停用成員帳戶，請使用 DISABLED 取代 ENABLED。

  要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

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

  您也可以傳遞以空格分隔的帳戶 ID 清單。
- 當程式碼成功執行時，會返回一個空白 UnprocessedAccounts 清單。如果變更帳戶的偵測器設定時發生任何問題，則會列出該帳戶 ID 以及問題摘要。

啟用 GuardDuty所有現有活躍成員帳戶的惡意軟件掃描

選擇您偏好的存取方法，以啟用 GuardDuty組織中所有現有作用中成員帳戶的惡意程式碼掃描。

為所有現有作用中成員帳戶設定 GuardDuty啟動的惡意程式碼掃描

1. 請登入 AWS Management Console 並開啟 GuardDuty 主控台，網址為 https://console.aws.amazon.com/guardduty/。

   使用委派的 GuardDuty 系統管理員帳戶認證登入。
2. 在導覽窗格中，選擇惡意軟體防護。
3. 在 [惡意程式碼防護] 上，您可以檢視啟動之惡意程式碼GuardDuty掃描組態的目前狀態。在作用中成員帳戶區段下，選擇動作。
4. 從動作下拉式選單中，選擇為所有作用中的成員帳戶啟用。
5. 選擇儲存。

自動啟動新 GuardDuty成員帳戶的惡意軟體掃描

新增的成員帳戶必須 GuardDuty 先啟用，才能選取設定啟 GuardDuty動的惡意程式碼掃描。受邀請管理的成員帳戶可以手動為其帳戶配置 GuardDuty啟動的惡意軟件掃描。如需詳細資訊，請參閱 Step 3 - Accept an invitation。

選擇您偏好的存取方法，以針對加入組織的新帳戶啟用 GuardDuty開始的惡意程式碼掃描。

Console

委派的 GuardDuty 系統管理員帳戶可以使用 [惡意程式碼防護] 或 [帳戶] 頁面，針對組織中的新成員帳戶啟用 GuardDuty起始的惡意程式碼掃描。

自動啟用新成 GuardDuty員帳戶的惡意程式碼掃描

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/

   請務必使用委派的 GuardDuty 系統管理員帳戶認證。

2. 執行以下任意一項：

   - 使用惡意軟體防護頁面：

     1. 在導覽窗格中，選擇惡意軟體防護。
     2. 在 [惡意程式碼防護] 頁面上，在啟動的惡意程式碼GuardDuty掃描中選擇 [編輯
     3. 選擇手動設定帳戶。
     4. 選取為新成員帳戶自動啟用。此步驟可確保每當有新帳戶加入您的組織時， GuardDuty 系統都會自動為其帳戶啟用啟動的惡意軟體掃描。只有組織委派的 GuardDuty 管理員帳戶可以修改此組態。
     5. 選擇儲存。

   - 使用帳戶頁面：

     1. 在導覽窗格中，選擇帳戶。
     2. 在帳戶頁面上，選擇自動啟用偏好設定。
     3. 在 [管理自動啟用喜好設定] 視窗中，選取 [開始的惡意程式碼GuardDuty掃描] 下的 [針對新帳號
     4. 選擇儲存。

API/CLI

- 若要為新成員帳戶啟用或停用啟 GuardDuty動的惡意程式碼掃描，請使用您自己的*### ID* 呼叫 UpdateOrganizationConfigurationAPI 作業。
- 下列範例顯示如何針對單一成員帳戶啟用 GuardDuty起始的惡意程式碼掃描。若要停用，請參閱選擇性地啟用或停用成員 GuardDuty帳戶的惡意程式碼掃描。如果您不想為加入組織的所有新帳戶啟用此功能，請將 AutoEnable 設定為 NONE。

  要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

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

  您也可以傳遞以空格分隔的帳戶 ID 清單。
- 當程式碼成功執行時，會返回一個空白 UnprocessedAccounts 清單。如果變更帳戶的偵測器設定時發生任何問題，則會列出該帳戶 ID 以及問題摘要。

選擇性地啟用或停用成員 GuardDuty帳戶的惡意程式碼掃描

選擇您偏好的存取方法，選擇性地為成員帳戶設定 GuardDuty啟動的惡意程式碼掃描。

Console

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/
2. 在導覽窗格中，選擇帳戶。
3. 在 [帳戶] 頁面上，檢閱GuardDuty啟動的惡意軟體掃描欄，瞭解您的成員帳戶的狀態。
4. 選取您要設定 GuardDuty起始惡意程式碼掃描的帳戶。您可以一次選取多個帳戶。
5. 從 [編輯防護方案] 功能表中，為起始的惡意程式碼GuardDuty掃描選擇適當的選項。

API/CLI

要選擇性地為您的成員帳戶啟用或禁用啟 GuardDuty動的惡意軟件掃描，請使用您自己的*### ID* 調用 updateMemberDetectorsAPI 操作。

下列範例顯示如何針對單一成員帳戶啟用 GuardDuty起始的惡意程式碼掃描。若要停用，請使用 DISABLED 取代 ENABLED。

要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

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

> **Note**
>
> 您也可以傳遞以空格分隔的帳戶 ID 清單。

當程式碼成功執行時，會返回一個空白 UnprocessedAccounts 清單。如果變更帳戶的偵測器設定時發生任何問題，則會列出該帳戶 ID 以及問題摘要。

要選擇性地為您的成員帳戶啟用或禁用啟 GuardDuty動的惡意軟件掃描，請使用您自己的### *ID* 運行 updateMemberDetectorsAPI 操作。下列範例顯示如何針對單一成員帳戶啟用 GuardDuty起始的惡意程式碼掃描。若要停用，請使用 `false` 取代 `true`。

要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

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

> **Note**
>
> 您也可以傳遞以空格分隔的帳戶 ID 清單。

當程式碼成功執行時，會返回一個空白 UnprocessedAccounts 清單。如果變更帳戶的偵測器設定時發生任何問題，則會列出該帳戶 ID 以及問題摘要。

針對透過邀請管理的組織中的現有帳戶啟用 GuardDuty開始的惡意程式碼掃描

必須在成員帳戶中建立 GuardDuty 惡意程式碼防護服務連結角色 (SLR)。管理員帳戶無法在不受管理的成員帳戶中啟用啟 GuardDuty動的惡意軟體掃描功能。 AWS Organizations

目前，您可以通過 https://console.aws.amazon.com/guardduty/ 的 GuardDuty 控制台執行以下步驟，以啟 GuardDuty用現有成員帳戶的惡意軟件掃描。

Console

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/

   使用您的系統管理員帳戶認證登入。
2. 在導覽窗格中，選擇帳戶。
3. 選取您要啟用 GuardDuty起始惡意程式碼掃描的成員帳戶。您可以一次選取多個帳戶。
4. 選擇動作。
5. 選擇取消關聯成員。
6. 在成員帳戶中，在導覽窗格的保護計畫下，選擇惡意軟體防護。
7. 選擇啟 GuardDuty動啟動的惡意程式碼掃描。 GuardDuty 將為會員帳戶建立單鏡反光相機。如需有關 SLR 的詳細資訊，請參閱惡意軟體防護的服務連結角色許可。
8. 在您的系統管理員帳戶中，選擇功能窗格上的 [帳戶]。
9. 選擇需要新增回組織的成員帳戶。
10. 選擇動作，然後選擇新增成員。

API/CLI

1. 使用管理員帳戶在要啟 GuardDuty用惡意軟件掃描的成員帳戶上運行 DisassociateMembersAPI。
2. 使用您的會員帳戶調用以啟UpdateDetector用啟 GuardDuty動的惡意軟件掃描。

   要查找您`detectorId`的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

   ```
   aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0
    --data-sources '{"MalwareProtection":{"ScanEc2InstanceWithFindings":
   {"EbsVolumes":true}}}'
   ```
3. 使用系統管理員帳戶執行 CreateMembersAPI，將成員新增回組織。

呼叫 GuardDuty起始惡意軟體掃描的發現項目

在 Amazon EC2 執行個體或容器工作負載上 GuardDuty 偵測到指示惡意程式碼的可疑行為時，便會叫用 GuardDuty啟動的惡意程式碼掃描。

- Backdoor:EC2/C&CActivity.B
- Backdoor:EC2/C&CActivity.B!DNS
- Backdoor:EC2/DenialOfService.Dns
- Backdoor:EC2/DenialOfService.Tcp
- Backdoor:EC2/DenialOfService.Udp
- Backdoor:EC2/DenialOfService.UdpOnTcpPorts
- Backdoor:EC2/DenialOfService.UnusualProtocol
- Backdoor:EC2/Spambot
- CryptoCurrency:EC2/BitcoinTool.B
- CryptoCurrency:EC2/BitcoinTool.B!DNS
- Impact:EC2/AbusedDomainRequest.Reputation
- Impact:EC2/BitcoinDomainRequest.Reputation
- Impact:EC2/MaliciousDomainRequest.Reputation
- Impact:EC2/PortSweep
- Impact:EC2/SuspiciousDomainRequest.Reputation
- Impact:EC2/WinRMBruteForce (僅限傳出)
- Recon:EC2/Portscan
- Trojan:EC2/BlackholeTraffic
- Trojan:EC2/BlackholeTraffic!DNS
- Trojan:EC2/DGADomainRequest.B
- Trojan:EC2/DGADomainRequest.C!DNS
- Trojan:EC2/DNSDataExfiltration
- Trojan:EC2/DriveBySourceTraffic!DNS
- Trojan:EC2/DropPoint
- Trojan:EC2/DropPoint!DNS
- Trojan:EC2/PhishingDomainRequest!DNS

- UnauthorizedAccess:EC2/RDPBruteForce (僅限傳出)
- UnauthorizedAccess:EC2/SSHBruteForce (僅限傳出)
- UnauthorizedAccess:EC2/TorClient
- UnauthorizedAccess:EC2/TorRelay
- Backdoor:Runtime/C&CActivity.B
- Backdoor:Runtime/C&CActivity.B!DNS
- CryptoCurrency:Runtime/BitcoinTool.B
- CryptoCurrency:Runtime/BitcoinTool.B!DNS
- Execution:Runtime/NewBinaryExecuted
- Execution:Runtime/NewLibraryLoaded
- Execution:Runtime/ReverseShell
- Impact:Runtime/AbusedDomainRequest.Reputation
- Impact:Runtime/BitcoinDomainRequest.Reputation
- Impact:Runtime/CryptoMinerExecuted
- Impact:Runtime/MaliciousDomainRequest.Reputation
- Impact:Runtime/SuspiciousDomainRequest.Reputation
- PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified
- PrivilegeEscalation:Runtime/ContainerMountsHostDirectory
- PrivilegeEscalation:Runtime/DockerSocketAccessed
- PrivilegeEscalation:Runtime/RuncContainerEscape
- PrivilegeEscalation:Runtime/UserfaultfdUsage
- Trojan:Runtime/BlackholeTraffic
- Trojan:Runtime/BlackholeTraffic!DNS
- Trojan:Runtime/DropPoint
- Trojan:Runtime/DropPoint!DNS
- Trojan:Runtime/DGADomainRequest.C!DNS
- Trojan:Runtime/DriveBySourceTraffic!DNS
- Trojan:Runtime/PhishingDomainRequest!DNS
- UnauthorizedAccess:Runtime/MetadataDNSRebind

隨需惡意軟體掃描

隨需惡意軟體掃描可協助您偵測連接到 Amazon EC2 執行個體之 Amazon Elastic Block Store (Amazon EBS) 磁碟區的惡意軟體。無需設定，即可透過提供要掃描之 Amazon EC2 執行個體的 Amazon Resource Name (ARN) 來啟動隨需惡意軟體掃描。您可以透過 GuardDuty 主控台或 API 啟動指定惡意程式碼掃描。在啟動隨需惡意軟體掃描之前，您可以設定偏好的 快照保留 設定。下列案例可協助您識別何時搭配使用隨選惡意程式碼掃描類型 GuardDuty：

- 您想要偵測 Amazon EC2 執行個體中是否存在惡意軟體，而不需啟用啟 GuardDuty動的惡意軟體掃描。
- 您已啟用啟 GuardDuty動的惡意程式碼掃描，而且已自動啟動掃描。遵循針對產生的惡意軟體防護調查結果類型所建議的補救措施後，如果您想要在相同資源上啟動掃描，可以在從上一個掃描開始時間過 1 小時後啟動隨需惡意軟體掃描。

  使用隨需惡意軟體掃描不需要在上一次惡意軟體掃描啟動之後等待 24 小時。在相同資源上啟動隨需惡意軟體掃描之前，應等候一小時。若要避免在同一 EC2 執行個體上重複惡意軟體掃描，請參閱重新掃描相同的 Amazon EC2 執行個體。

> **Note**
>
> 隨選惡意軟體掃描不包含在使用的 30 天免費試用期內 GuardDuty。使用費適用於每次惡意軟體掃描過程所掃描的 Amazon EBS 磁碟區總數。如需詳細資訊，請參閱 Amazon GuardDuty 定價。如需有關建立 Amazon EBS 磁碟區快照的成本及保留的相關資訊，請參閱 Amazon EBS 定價。

隨需惡意軟體掃描的運作方式

透過隨需惡意軟體掃描，您可以針對 Amazon EC2 執行個體啟動惡意軟體掃描請求，即使該執行個體目前正在使用中也可以。啟動隨需惡意軟體掃描後， GuardDuty 建立 Amazon EBS 磁碟區的快照，連接至已為掃描提供 Amazon 資源名稱 (ARN) 的 Amazon EC2 執行個體。接下來， GuardDuty 將這些快照與GuardDuty 服務帳戶. GuardDuty 從 GuardDuty 服務帳戶中的那些快照建立加密複本 EBS 磁碟區。如需有關如何掃描 Amazon EBS 磁碟區的詳細資訊，請參閱Elastic Block Storage (EBS) 磁碟區。

> **Note**
>
> GuardDuty 當您啟動隨選惡意軟體掃描 point-in-time 時，會建立已寫入 Amazon EBS 磁碟區的資料快照。

如果發現惡意軟體，且您已啟用快照保留設定，EBS 磁碟區的快照會自動保留在您的 AWS 帳戶中。隨需惡意軟體掃描會產生惡意軟體防護調查結果類型。如果找不到惡意軟體，則無論快照保留設定為何，都會刪除 EBS 磁碟區的快照。

依預設，EBS 磁碟區的快照會以 `GuardDutyScanId` 標籤建立。請勿移除此標籤，因為這樣做會導致GuardDuty無法存取快照。惡意軟體防護中的兩種掃描類型均不會掃描 `GuardDutyExcluded` 標籤設定為 `true` 的 Amazon EC2 執行個體或 Amazon EBS 磁碟區。如果針對此類資源進行惡意軟體防護掃描，則將生成掃描 ID，但掃描將由於 `EXCLUDED_BY_SCAN_SETTINGS` 原因而跳過。如需詳細資訊，請參閱 惡意軟體掃描期間略過資源的原因。

AWS Organizations 服務控制策略 — 拒絕訪問

委派的 GuardDuty 管理員帳戶可以使用中的服務控制政策 (SCP) 來限制許可並拒絕動作 AWS Organizations，例如針對您帳戶擁有的 Amazon EC2 執行個體啟動隨選惡意軟體掃描。

身為 GuardDuty 會員帳戶，當您為 Amazon EC2 執行個體啟動隨選惡意軟體掃描時，可能會收到錯誤訊息。您可以與管理帳戶連線，以了解為何為您的成員帳戶設定 SCP。如需詳細資訊，請參閱 SCP 對許可的影響。

開始使用隨需惡意軟體掃描

GuardDuty 身為系統管理員帳戶，您可以代表已在其帳戶中設定下列必要條件的作用中成員帳戶啟動隨選惡意程式碼掃描。中的獨立帳戶和作用中成員帳戶也 GuardDuty 可以針對自己的 Amazon EC2 執行個體啟動隨選惡意軟體掃描。

必要條件

- GuardDuty 必須在您要啟動指定惡意軟體掃描的 AWS 區域 位置啟用。
- 確保 AWS 受管理的策略：AmazonGuardDutyFullAccess 已連接至 IAM 使用者或 IAM 角色。您將需要與 IAM 使用者或 IAM 角色相關聯的存取金鑰和私密金鑰。
- 身為委派的 GuardDuty 系統管理員帳戶，您可以選擇代表作用中的成員帳戶啟動隨選惡意軟體掃描。

- 如果您是沒有 惡意軟體防護的服務連結角色許可 的成員帳戶，當針對屬於您帳戶的 Amazon EC2 執行個體啟動隨需惡意軟體掃描時，將會自動建立用於惡意軟體防護的 SLR。

> **Important**
>
> 確保沒有人刪除惡意軟體防護的 SLR 權限，無論是 GuardDuty啟動的還是隨選掃描仍在進行中。這樣做會阻礙掃描成功完成和提供明確的掃描結果。

在您啟動隨需惡意軟體掃描之前，請確定過去 1 小時內未對相同資源啟動掃描；否則，系統會取消重複動作。如需詳細資訊，請參閱 重新掃描相同的資源。

啟動隨需惡意軟體掃描

選擇您偏好的存取方法，以便啟動隨需惡意軟體掃描。

Console

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/
2. 使用下列選項之一開始掃描：
   a. 使用惡意軟體防護頁面：
      i. 在導覽窗格的保護計畫下，選擇惡意軟體防護。
      ii. 在惡意軟體防護頁面上，提供您要啟動掃描的 Amazon EC2 執行個體 ARN [1]。
   b. 使用惡意軟體掃描頁面：
      i. 在導覽窗格中，選擇惡意軟體掃描。
      ii. 選擇開始隨需掃描，並提供要啟動掃描的 Amazon EC2 執行個體 ARN [1]。
      iii. 如果這是重新掃描，請在惡意軟體掃描頁面上選取 Amazon EC2 執行個體 ID。

      展開開始隨需掃描下拉式選單，然後選擇重新掃描選取的執行個體。
3. 使用任一方法成功啟動掃描後，就會產生掃描 ID。您可以使用此掃描 ID 來追蹤掃描進度。如需詳細資訊，請參閱 監控惡意軟體掃描狀態和結果。

API/CLI

接StartMalwareScan受您想要啟動隨選惡意軟體掃描resourceArn之 Amazon EC2 執行個體 [1] 的呼叫。

```
aws guardduty start-malware-scan --resource-arn "arn:aws:ec2:us-
east-1:555555555555:instance/i-b188560f"
```

成功起始掃描之後，StartMalwareScan 會傳回 scanId。呼叫會DescribeMalwareScans監視開始掃描的進度。

[1] 如需有關 Amazon EC2 執行個體 ARN 格式的詳細資訊，請參閱 Amazon Resource Name (ARN)。針對 Amazon EC2 執行個體，您可以使用下列範例 ARN 格式，方法是取代分區、區域、 AWS 帳戶 ID 和 Amazon EC2 執行個體 ID 的值。如需有關執行個體 ID 長度的詳細資訊，請參閱資源 ID。

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

重新掃描相同的 Amazon EC2 執行個體

無論是啟動掃描還是 GuardDuty隨需掃描，您都可以在上一次惡意軟體掃描開始後 1 小時後，在相同 EC2 執行個體上啟動新的隨選惡意軟體掃描。如果在先前的惡意軟體掃描啟動後 1 小時內啟動新的惡意軟體掃描，您的要求將導致下列錯誤，並且不會針對此請求產生任何掃描 ID。

```
A scan was initiated on this resource recently. You can request a scan on
the same resource one hour after the previous scan start time.
```

如需有關如何在相同資源上啟動新掃描的詳細資訊，請參閱啟動隨需惡意軟體掃描。

若要追蹤惡意軟體掃描的狀態，請參閱在 GuardDuty 惡意軟體防護中監控掃描狀態和結果。

在 GuardDuty 惡意軟體防護中監控掃描狀態和結果

您可以監視每個 GuardDuty 惡意程式碼防護掃描的掃描狀態。掃描狀態的可能值為 Completed、Running、Skipped 和 Failed。

掃描完成後，系統會針對狀態為 Completed 的掃描填入掃描結果。掃描結果的可能值為 Clean 和 Infected。使用掃描類型，您可以識別惡意軟體掃描是否為 GuardDuty initiated 或 On demand。

每種惡意軟體掃描的掃描結果的保留期為 90 天。選擇您偏好的存取方式，以便追蹤惡意軟體掃描狀態。

Console

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/
2. 在導覽窗格中，選擇惡意軟體掃描。
3. 您可以依據篩選條件中提供的下列屬性來篩選惡意軟體掃描。

   - 掃描 ID
   - 帳戶 ID
   - EC2 執行個體 ARN
   - 掃描類型
   - 掃描狀態

   如需有關用於篩選條件的屬性的詳細資訊，請參閱調查結果詳細資訊。

API/CLI

- 惡意軟體掃描有掃描結果後，您可以根據 `EC2_INSTANCE_ARN`、`SCAN_ID`、`ACCOUNT_ID`、`SCAN_TYPE`、`GUARDDUTY_FINDING_ID`、`SCAN_S` 和 `SCAN_START_TIME` 篩選惡意軟體掃描。

  GuardDuty 啟動時，即可使用`GUARDDUTY_FINDING_ID`篩選條件。`SCAN_TYPE`如需有關任何篩選條件的詳細資訊，請參閱調查結果詳細資訊。
- 您可以在下面的命令中更改示例`####`。目前，您可以一次篩選一個 `CriterionKey`。`CriterionKey` 的選項包括 `EC2_INSTANCE_ARN`、`SCAN_ID`、`ACCOUNT_ID`、`SCAN_TYPE`、`GUARDDUTY_FINDING_ID`、`SCAN_S` 和 `SCAN_START_TIME`。

  如果您使用與下面相同的 `CriterionKey`，請確保用您自己的有效 AWS *`scan-id`* 取代範例 `EqualsValue`。

  使用您自己的有效 *`detector-id`* 取代範例 `detector-id`。您可以更改`####` (最多 50 個) 和`####`。`AttributeName` 是必要選項，必須是 `scanStartTime`。

```
aws guardduty describe-malware-scans --detector-
id 60b87779336485625554d637e0e4bb3b2 --max-results 1 --sort-criteria
 '{"AttributeName": "scanStartTime", "OrderBy": "DESC"}' --filter-criteria
 '{"FilterCriterion":[{"CriterionKey":"SCAN_ID", "FilterCondition":
{"EqualsValue":"123456789012"}}] }'
```

- 此命令的回應最多會顯示一個結果，其中包含有關受影響資源和惡意軟體調查結果的詳細資訊 (如果是 Infected)。

GuardDuty 服務帳戶依據 AWS 區域

建立快照集並與 GuardDuty 服務帳戶共用時，會在 CloudTrail 記錄檔中建立新事件。此事件會指定對應的snapshotId和 userId (該GuardDuty 服務帳戶 AWS 區域)。如需詳細資訊，請參閱 惡意軟體防護的功能。

下列範例是 CloudTrail 事件中的程式碼片段，其中顯示要求的ModifySnapshotAttribute要求主體：

```
"requestParameters": {
        "snapshotId": "snap-1234567890abcdef0",
        "createVolumePermission": {
            "add": {
                "items": [
                    {
                        "userId": "111122223333"
                    }
                ]
            }
        },
        "attributeType": "CREATE_VOLUME_PERMISSION"
    }
```

下表顯示每個區域的 GuardDuty 服務帳戶。userId是 GuardDuty 服務帳戶，視選取的區域而定。

AWS 區域	區域代碼	GuardDuty 服務帳戶識別碼 (**userId**)
美國東部 (維吉尼亞北部)	us-east-1	652050842985
美國東部 (俄亥俄)	us-east-2	178123968615

AWS 區域	區域代碼	GuardDuty 服務帳戶識別碼 (**`userId`**)
美國西部 (加利佛尼亞北部)	us-west-1	669213148797
美國西部 (奧勒岡)	us-west-2	447226417196
亞太區域 (孟買)	ap-south-1	913179291432
亞太區域 (大阪)	ap-northeast-3	089661699081
亞太區域 (首爾)	ap-northeast-2	039163547507
亞太區域 (東京)	ap-northeast-1	874749492622
亞太區域 (新加坡)	ap-southeast-1	247460962669
亞太區域 (悉尼)	ap-southeast-2	124839743349
加拿大 (中部)	ca-central-1	175877067165
加拿大西部 (卡加利)	ca-west-1	894794104037
歐洲 (法蘭克福)	eu-central-1	002294850712
歐洲 (愛爾蘭)	eu-west-1	283769539786
歐洲 (倫敦)	eu-west-2	310125036783
Europe (Paris)	eu-west-3	866607715269
歐洲 (斯德哥爾摩)	eu-north-1	693780578038
中國 (北京)	cn-north-1	448721096076
中國 (寧夏)	cn-northwest-1	480864352451
南美洲 (聖保羅)	sa-east-1	546914126324
亞太區域 (海德拉巴) (選擇加入)	ap-south-2	682251015962

AWS 區域	區域代碼	GuardDuty 服務帳戶識別碼 (**`userId`**)
亞太區域 (墨爾本) (選擇加入)	ap-southeast-4	353488359550
歐洲 (西班牙) (選擇加入)	eu-south-2	936182149045
歐洲 (蘇黎世) (選擇加入)	eu-central-2	867642063380
以色列 (特拉維夫) (選擇加入)	il-central-1	619233833001
歐洲 (米蘭) (選擇加入)	eu-south-1	977238331021
亞太區域 (香港) (選擇加入)	ap-east-1	249472122084
中東 (巴林) (選擇加入)	me-south-1	404001805210
非洲 (開普敦) (選擇加入)	af-south-1	957664736811
亞太區域 (雅加達) (選擇加入)	ap-southeast-3	452118225523
中東 (阿拉伯聯合大公國) (選擇加入)	me-central-1	828603743433

惡意軟體防護配額

惡意軟體防護對該功能使用的各種資源具有下列預設可用性。

範圍	預設	說明
擷取和分析壓縮或封存檔案中的資料	5	封存檔案允許的巢狀層級數上限。
封存檔案中的檔案數	1000	封存內可掃描的最大檔案數量。此計數是從封存中擷取的

範圍	預設	說明
		檔案數，以及從所有巢狀封存中擷取的檔案數的總和。
安全威脅數量	32	您可以在發現項目面板中檢視的安全威脅數目上限。GuardDuty 惡意程式碼防護可能偵測到更多威脅名稱。如果偵測到的安全威脅名稱數目大於預設值，您可以在 GuardDuty 主控台的詳細資料面板中，選取發現項目名稱下的尋找項目 ID，以檢視 JSON 詳細資料。
每個偵測到的安全威脅的檔案數量	5	每個偵測到的安全威脅所識別的檔案數量上限。例如，如果 GuardDuty 偵測到 10 個與單一安全威脅相關聯的檔案，則安全威脅最多會顯示 5 個檔案。
每個執行個體每次掃描的 EBS 磁碟區	11	每個 EC2 執行個體 GuardDuty 可掃描的 EBS 磁碟區數目上限。如果需要掃描 11 個以上的 EBS 磁碟區， GuardDuty 惡意程式碼防護會`deviceName` 依字母順序排序，並選取前 11 個 EBS 磁碟區。
EBS 磁碟區大小	英國	GuardDuty 惡意軟體防護與 Amazon EC2 執行個體和容器工作負載相關聯，可掃描大小高達 2048 GB 的每個 Amazon EBS 磁碟區。此配額適用於提供惡意軟體防護支援的每個 AWS 區域 位置。

範圍	預設	說明
支援的檔案系統類型	GuardDuty 惡意程式碼防護可掃描下列檔案系統類型： • New Technology File System (NTFS) • X File System (XFS) • 第二代擴充 (ext2) 檔案系統 • 第四代擴充 (ext4) 檔案系統 • 檔案配置表 (FAT) 檔案系統 • 虛擬檔案配置表 (VFAT) 檔案系統	無
掃描選項標籤	50	您可新增用來自訂惡意軟體掃描選項設定的最大資源標籤數。如需詳細資訊，請參閱 具有使用者定義標籤的掃描選項。
尋找保留期間	90	GuardDuty 保留發現項目的最大天數。如需最新資訊，請參閱Amazon 的配額 GuardDuty。
惡意軟體掃描保留期	90	「GuardDuty 惡意程式碼防護」會保留掃描歷程記錄的天數上限。如需有關檢視最近惡意軟體掃描的詳細資訊，請參閱在 GuardDuty 惡意軟體防護中監控掃描狀態和結果。
隨需惡意軟體掃描的每秒交易數 (TPS)	1	每個區域中每秒可啟動的隨需惡意軟體掃描請求數量。
隨需惡意軟體掃描的高載限制	1	每個區域中每秒可啟動的並行隨需惡意軟體掃描請求數量。

GuardDuty 遠端防護

Amazon 的 RDS 防護會 GuardDuty 分析 RDS 登入活動，並分析對您的 Amazon Aurora 資料庫（Amazon Aurora MySQL 相容版本和 Aurora PostgreSQL 相容版本）的潛在存取威脅。此功能可讓您識別潛在的可疑登入行為。RDS 保護不需要額外的基礎設施；專門為不影響資料庫執行個體的效能而設計。

當 RDS Protection 偵測到可能可疑或異常的登入嘗試表明資料庫有威脅時， GuardDuty 會產生新的發現項目，其中包含可能遭到入侵的資料庫的詳細資料。

您可以隨時在 Amazon GuardDuty 內部提供此功能的任 AWS 區域 何帳戶啟用或停用 RDS 保護功能。現有 GuardDuty 帳戶可以在 30 天的試用期內啟用 RDS 防護。對於新 GuardDuty 帳戶，RDS 防護已啟用，並包含在 30 天免費試用期內。如需詳細資訊，請參閱 估算成本。

> **Note**
>
> 未啟用 RDS 防護功能時， GuardDuty 既不會收集您的 RDS 登入活動，也不會偵測異常或可疑的登入行為。

如需尚 GuardDuty 未支援 RDS 防護之 AWS 區域 位置的相關資訊，請參閱區域特定功能的可用性。

支援的 Amazon Aurora 資料庫

下表顯示支援的 Aurora 資料庫版本。

Amazon Aurora 資料庫引擎	支援的引擎版本
Aurora MySQL	• 2.10.2 或更新版本 • 3.02.1 或更新版本
Aurora PostgreSQL	• 10.17 或更新版本 • 11.12 或更新版本 • 12.7 或更新版本 • 13.3 或更新版本 • 14.3 或更新版本

Amazon Aurora 資料庫引擎	支援的引擎版本
	• 15.2 或更高版本 • 16.1 或更高版本

RDS 保護如何使用 RDS 登入活動監控

Amazon 的 RDS 防護可 GuardDuty 協助您保護帳戶中受支援的 Amazon Aurora (Aurora) 資料庫。啟用 RDS 防護功能之後， GuardDuty 立即開始從您帳戶中的 Aurora 資料庫監視 RDS 登入活動。GuardDuty 持續監控並分析 RDS 登入活動中是否有可疑活動，例如，未經授權存取您帳戶中的 Aurora 資料庫，從先前看不見的外部參與者。當您第一次啟用 RDS 保護或您有新建立的資料庫執行個體時，需要一段學習期以將一般行為基準化。基於這個原因，新啟用或新建立的資料庫執行個體，在長達兩週的時間內可能沒有相關的異常登入調查結果。如需詳細資訊，請參閱 RDS 登入活動監控。

當 RDS Protection 偵測到潛在安全威脅時，例如一系列成功、失敗或不完整登入嘗試中的異常病毒碼， GuardDuty 會產生新的發現項目，其中包含可能遭到入侵的資料庫執行個體的詳細資料。如需詳細資訊，請參閱 RDS 保護調查結果類型。如果停用 RDS 防護，請 GuardDuty 立即停止監控 RDS 登入活動，且無法偵測到支援的資料庫執行個體的任何潛在威脅。

> **Note**
>
> GuardDuty 不會管理您的支援的資料庫或 RDS 登入活動，也不會讓您使用 RDS 登入活動。

為獨立帳戶設定 RDS 保護

Console

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/
2. 在導覽窗格中，選擇 RDS 保護。
3. RDS 保護頁面會顯示您帳戶的目前狀態。您可以隨時透過分別選取啟用或停用來啟用或停用此功能。確認您的選擇。

API/CLI

使用您自己的區域偵測器 ID，並透過將 `name` 設定為 `RDS_LOGIN_EVENTS` 及將 `status` 設定為 `ENABLED` 或 `DISABLED` 來傳遞 `features` 物件，從而執行 updateDetector API 操作。

您也可以執行下列 AWS CLI 命令來啟用或停用 RDS 防護。請務必使用您自己的有效*### ID*。

> **Note**
>
> 下列範例程式碼會啟用 RDS 保護。若要停用，請使用 DISABLED 取代 ENABLED。

要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

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

在多帳戶環境中設定 RDS 保護

在多帳戶環境中，只有委派的 GuardDuty 系統管理員帳戶可以選擇為其組織中的成員帳戶啟用或停用 RDS 保護功能。成 GuardDuty員帳戶無法從其帳戶修改此設定。委派的管理 GuardDuty 員帳戶會使用來管理其成員帳戶 AWS Organizations。這個委派的 GuardDuty 系統管理員帳戶可以選擇在所有新帳戶加入組織時自動啟用 RDS 登入活動監控功能。如需有關多帳戶環境的詳細資訊，請參閱在 Amazon GuardDuty 中管理多個帳戶。

針對委派的 GuardDuty 管理員帳戶設定 RDS 保護

選擇您偏好的存取方法，以針對委派的 GuardDuty 系統管理員帳戶設定 RDS 登入活動監視。

Console

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/

   確保使用管理帳戶憑證。
2. 在導覽窗格中，選擇 RDS 保護。
3. 在 RDS 保護頁面上，選擇編輯。
4. 執行以下任意一項：

   使用為所有帳戶啟用

   - 選擇為所有帳戶啟用。這將啟用 AWS 組織中所有作用中 GuardDuty 帳戶的保護計劃，包括加入組織的新帳戶。

- 選擇儲存。

使用手動設定帳戶

- 若要僅針對委派的 GuardDuty 系統管理員帳戶啟用保護方案，請選擇 [手動設定帳戶]。
- 在 [委派 GuardDuty 管理員帳戶 (此帳戶)] 區段下選擇 [啟用]。
- 選擇儲存。

API/CLI

使用您自己的區域偵測器 ID，並透過將 `name` 設定為 `RDS_LOGIN_EVENTS` 及將 `status` 設定為 `ENABLED` 或 `DISABLED` 來傳遞 `features` 物件，從而執行 updateDetector API 操作。

您可以執行下列 AWS CLI 命令來啟用或停用 RDS 防護。確保使用委派 GuardDuty 管理員帳戶的有效*### ID*。

> **Note**
>
> 下列範例程式碼會啟用 RDS 保護。若要停用，請使用 `DISABLED` 取代 `ENABLED`。

要查找您`detectorId`的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

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

為所有成員帳戶自動啟用 RDS 保護

選擇您偏好的存取方法，以便為所有成員帳戶啟用 RDS 保護功能。這包括現有的成員帳戶和加入組織的新帳戶。

Console

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/

   請務必使用委派的 GuardDuty 系統管理員帳戶認證。

2. 執行以下任意一項：

   使用 RDS 保護頁面

   1. 在導覽窗格中，選擇 RDS 保護。
   2. 選擇為所有帳戶啟用。此動作會自動為組織中的現有帳戶和新帳戶啟用 RDS 保護。
   3. 選擇儲存。

   > **Note**
   >
   > 最多可能需要 24 小時才會更新成員帳戶的組態。

   使用帳戶頁面

   1. 在導覽窗格中，選擇帳戶。
   2. 在帳戶頁面上，選擇自動啟用偏好設定，然後再透過邀請新增帳戶。
   3. 在管理自動啟用偏好設定視窗中，選擇 RDS 登入活動監控下的為所有帳戶啟用。
   4. 選擇儲存。

   如果您無法使用為所有帳戶啟用選項，請參閱 選擇性地為成員帳戶啟用或停用 RDS 保護。

API/CLI

- 若要為您的成員帳戶選擇性地啟用或停用 RDS 保護，請使用您自己的*### ID* 調用 updateMemberDetectors API 操作。
- 以下範例顯示如何為單一成員帳戶啟用 RDS 保護。若要停用，請使用 DISABLED 取代 ENABLED。

  要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

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

> **Note**
>
> 您也可以傳遞以空格分隔的帳戶 ID 清單。

- 當程式碼成功執行時，會返回一個空白 `UnprocessedAccounts` 清單。如果變更帳戶的偵測器設定時發生任何問題，則會列出該帳戶 ID 以及問題摘要。

為所有現有作用中成員帳戶啟用 RDS 保護

選擇您偏好的存取方法，以便為組織中的所有現有作用中成員帳戶啟用 RDS 保護。

Console

為所有現有作用中成員帳戶設定 RDS 保護

1. 請登入 AWS Management Console 並開啟 GuardDuty 主控台，網址為 https://console.aws.amazon.com/guardduty/。

   使用委派的 GuardDuty 系統管理員帳戶認證登入。
2. 在導覽窗格中，選擇 RDS 保護。
3. 在 RDS 保護頁面上，您可以檢視組態的目前狀態。在作用中成員帳戶區段下，選擇動作。
4. 從動作下拉式選單中，選擇為所有作用中的成員帳戶啟用。
5. 選擇確認。

API/CLI

- 若要為您的成員帳戶選擇性地啟用或停用 RDS 保護，請使用您自己的*### ID* 調用 updateMemberDetectors API 操作。
- 以下範例顯示如何為單一成員帳戶啟用 RDS 保護。若要停用，請使用 `DISABLED` 取代 `ENABLED`。

  要查找您`detectorId`的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

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

> **Note**
>
> 您也可以傳遞以空格分隔的帳戶 ID 清單。

- 當程式碼成功執行時，會返回一個空白 `UnprocessedAccounts` 清單。如果變更帳戶的偵測器設定時發生任何問題，則會列出該帳戶 ID 以及問題摘要。

為新成員帳戶自動啟用 RDS 保護

選擇您偏好的存取方法，以便為新加入組織的新帳戶啟用 RDS 登入活動監控。

Console

委派的 GuardDuty 系統管理員帳戶可以使用 RDS 防護或帳號頁面，透過主控台為組織中的新成員帳戶啟用。

為新成員帳戶自動啟用 RDS 保護

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/

   請務必使用委派的 GuardDuty 系統管理員帳戶認證。

2. 執行以下任意一項：
   - 使用 RDS 保護頁面：
     1. 在導覽窗格中，選擇 RDS 保護。
     2. 在 RDS 保護頁面上，選擇編輯。
     3. 選擇手動設定帳戶。
     4. 選取為新成員帳戶自動啟用。此步驟可確保每當有新帳戶加入您的組織時，RDS 保護都會自動為其帳戶啟用。只有組織委派的 GuardDuty 管理員帳戶可以修改此組態。
     5. 選擇儲存。
   - 使用帳戶頁面：
     1. 在導覽窗格中，選擇帳戶。
     2. 在帳戶頁面上，選擇自動啟用偏好設定。
     3. 在管理自動啟用偏好設定視窗中，選取 RDS 登入活動監控下的為新帳戶啟用。
     4. 選擇儲存。

API/CLI

- 若要為您的成員帳戶選擇性地啟用或停用 RDS 保護，請使用您自己的*### ID* 調用 UpdateOrganizationConfiguration API 操作。
- 以下範例顯示如何為單一成員帳戶啟用 RDS 保護。若要停用，請參閱選擇性地為成員帳戶啟用或停用 RDS 保護。如果您不想為加入組織的所有新帳戶啟用此功能，請將 `autoEnable` 設定為 `NONE`。

  要查找您`detectorId`的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

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

  > **Note**
  >
  > 您也可以傳遞以空格分隔的帳戶 ID 清單。

- 當程式碼成功執行時，會返回一個空白 `UnprocessedAccounts` 清單。如果變更帳戶的偵測器設定時發生任何問題，則會列出該帳戶 ID 以及問題摘要。

選擇性地為成員帳戶啟用或停用 RDS 保護

選擇您偏好的存取方式，以便選擇性地為成員帳戶啟用或停用 RDS 登入活動監控。

Console

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/

   請務必使用委派的 GuardDuty 系統管理員帳戶認證。
2. 在導覽窗格中，選擇帳戶。

   在帳戶頁面上，檢閱 RDS 登入活動欄位，了解您的成員帳戶狀態。
3. 選擇性地啟用或停用 RDS 登入活動

   選取您要設定 RDS 保護的帳戶。您可以一次選取多個帳戶。在編輯保護計畫下拉式選單中，選擇 RDS 登入活動，然後選擇適當的選項。

API/CLI

若要為您的成員帳戶選擇性地啟用或停用 RDS 保護，請使用您自己的*### ID* 調用 updateMemberDetectors API 操作。

以下範例顯示如何為單一成員帳戶啟用 RDS 保護。若要停用，請使用 DISABLED 取代 ENABLED。

要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

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

> **Note**
>
> 您也可以傳遞以空格分隔的帳戶 ID 清單。

當程式碼成功執行時，會返回一個空白 UnprocessedAccounts 清單。如果變更帳戶的偵測器設定時發生任何問題，則會列出該帳戶 ID 以及問題摘要。

RDS 保護中的功能

RDS 登入活動監控

RDS 登入活動會擷取您 AWS 環境中針對 支援的 Amazon Aurora 資料庫 的成功和失敗登入嘗試。為了協助您保護資料庫， GuardDuty RDS Protection 會持續監控登入活動是否存在可疑的登入嘗試。例如，對手可能會透過猜測資料庫的密碼來嘗試暴力破解存取 Amazon Aurora 資料庫。

當您啟用 RDS 防護功能時， GuardDuty 會自動開始直接從 Aurora 服務監視資料庫的 RDS 登入活動。如果有異常登入行為的指示， GuardDuty 會產生一個包含可能遭到入侵之資料庫的詳細資料的發現項目。當您第一次啟用 RDS 保護或您有新建立的資料庫執行個體時，需要一段學習期以將一般行為基準化。基於這個原因，新啟用或新建立的資料庫執行個體，在長達兩週的時間內可能沒有相關的異常登入調查結果。

RDS 防護功能不需要任何額外的設定；它不會影響您現有的 Amazon Aurora 資料庫組態。 GuardDuty 不會管理支援的資料庫或 RDS 登入活動，或讓您可以使用 RDS 登入活動。

如果您選擇在新成員帳戶加入組織時自動啟用 RDS 防護功能，則這些新成員帳戶會自動啟 GuardDuty 用此動作。如需有關將 RDS 登入活動監控設定為功能的詳細資訊，請參閱GuardDuty 遠端防護。

GuardDuty 運行時監控

執行階段監控會觀察並分析作業系統層級、網路和檔案事件，協助您偵測環境中特定 AWS 工作負載中的潛在威脅。

GuardDuty 最初發布的運行時監控僅支持 Amazon Elastic Kubernetes Service（Amazon EKS）資源。不過，現在您也可以使用執行階段監控功能，為您的 Amazon Elastic Container Service (AWS Fargate Amazon ECS) 和亞馬遜彈性運算雲端 (Amazon EC2) 資源提供威脅偵測。

在本文件以及其他與執行階段監控相關的章節中， GuardDuty 使用資源類型術語來參考 Amazon EKS、Fargate 亞馬遜 ECS 和 Amazon EC2 資源。

執行階段監控會使用 GuardDuty 安全性代理程式來增加執行階段行為的可見度，例如檔案存取、程序執行、命令列引數和網路連線。針對您要監控潛在威脅的每種資源類型，您可以自動或手動管理該特定資源類型的安全代理程式 (Fargate (僅限 Amazon ECS) 除外)。自動管理安全代理程式表示您 GuardDuty 允許代表您安裝和更新安全代理程式。另一方面，當您手動管理資源的安全代理程式時，您必須視需要負責安裝和更新安全代理程式。

透過此擴充功能， GuardDuty 可協助您識別並回應可能針對個別工作負載和執行個體中執行之應用程式和資料的潛在威脅。例如，威脅可能從破壞運行易受攻擊 Web 應用程序的單個容器開始。此 Web 應用程式可能具有基礎容器和工作負載的存取權限。在這個案例中，設定不正確的認證可能會導致對帳戶及其中儲存的資料有更廣泛的存取權。

透過分析個別容器和工作負載的執行階段事件， GuardDuty 可能會在初始階段識別容器和相關 AWS 認證的入侵情況，並偵測嘗試提升權限、可疑的 API 要求，以及對環境中資料的惡意存取權限的嘗試。

目錄

- 使用收集的執行階段事 GuardDuty 件類型
- Amazon ECR 儲存庫託管代 GuardDuty 理
- GuardDuty 代理程式發行歷
- 停用及清理資源的影響

運作方式

若要使用執行階段監視，您必須啟用執行階段監視，然後管理 GuardDuty 安全代理程式。下列清單說明此兩個步驟的程序：

1. 為您的帳戶啟用執行階段監控， GuardDuty 以便接受從 Amazon EC2 執行個體、Amazon ECS 叢集和 Amazon EKS 工作負載接收到的執行階段事件。
2. 針對您要監視其執行階段行為的個別資源管理 GuardDuty 代理程式。根據資源類型，您可以選擇手動部署 GuardDuty Security Agent，或允許 GuardDuty 代表您管理它，稱為自動化代理程式組態。

   GuardDuty 使用針對每個資源類型驗證安全代理程式的執行個體身分識別角色，將相關的執行階段事件傳送至 VPC 端點。

> **Note**
>
> GuardDuty 不會使您可以訪問運行時事件。

當您在 EKS 執行個體或 EC2 執行個體的執行階段監控中管理安全代理程式 (無論GuardDuty 是手動或透過 GuardDuty)，且目前部署在 Amazon EC2 執行個體並收集的執行期事件類型從此執行個體接收，則不 GuardDuty 會 AWS 帳戶 針對此 Amazon EC2 執行個體的 VPC 流程日誌分析收費。這有助於 GuardDuty 避免帳戶中的雙重使用成本。

下列主題說明啟用執行階段監視和管理 GuardDuty Security Agent 對每種資源類型的運作方式不同。

目錄

- 執行階段監控如何與 Amazon EC2 執行個體搭配
- 運行時監控如何與 Fargate 一起工作（僅限 Amazon ECS）
- 執行階段監控如何與 Amazon EKS 叢集搭配使用
- 執行時間後監視組態

執行階段監控如何與 Amazon EC2 執行個體搭配

Amazon EC2 執行個體可以在您的 AWS 環境中執行多種類型的應用程式和工作負載。啟用執行階段監控並管理 GuardDuty 安全代理程式時，可 GuardDuty 協助您偵測現有 Amazon EC2 執行個體中的威脅，以及可能是新執行個體中的威脅。此功能也支援 Amazon ECS 受管 Amazon EC2 執行個體。

啟用執行時期監控 GuardDuty 可以使用 Amazon EC2 執行個體中目前執行中和新程序的執行時間事件。 GuardDuty 需要安全代理程式才能將執行階段事件從 EC2 執行個體傳送到 GuardDuty.

對於 Amazon EC2 執行個體， GuardDuty 安全代理程式會在執行個體層級運作。您可以決定是要監控帳戶中的所有 Amazon EC2 執行個體還是選擇性的 Amazon EC2 執行個體。如果您想要管理選擇性執行個體，只有這些執行個體才需要安全性代理程式。

GuardDuty 也可以從 Amazon ECS 叢集內的 Amazon EC2 執行個體中執行的新任務和現有任務中使用執行時期事件。

若要安裝安 GuardDuty 全性代理程式，執行階段監控提供下列兩個選項：

- 使用自動化代理程式組態 (建議)，或
- 手動管理安全代理

透過使用自動化代理程式組態 GuardDuty (建議)

使用允許 GuardDuty 您在 Amazon EC2 執行個體上安裝安全代理程式的自動化代理程式組態。 GuardDuty 也會管理安全代理程式的更新。

根據預設， GuardDuty 會在您帳戶中的所有執行個體上安裝安全代理程式。如果您只想 GuardDuty 為所選 EC2 執行個體安裝和管理安全代理程式，請視需要為 EC2 執行個體新增包含或排除標籤。

有時候，您可能不想監控屬於您帳戶的所有 Amazon EC2 執行個體的執行階段事件。如果您想要監視有限數量執行個體的執行階段事件，請將包含標籤新增為`GuardDutyManaged:true`至這些選取的執行個體。從 Amazon EC2 提供自動化代理程式組態開始，如果您的 EC2 執行個體具有包含標籤 (`GuardDutyManaged:true`)，即使您未明確啟用自動化代理程式組態，仍 GuardDuty會為所選執行個體顯示標籤並管理安全代理程式。

另一方面，如果您不想監視執行階段事件的 EC2 執行個體數量有限，請在這些選取的執行個體中新增排除標記 (`GuardDutyManaged:false`)。 GuardDuty 將通過既不安裝或管理這些 EC2 資源的安全代理程序來遵循排除標籤。

影響

當您在 AWS 帳戶 或組織中使用自動化代理程式設定時，您 GuardDuty 允許代表您採取下列步驟：

- GuardDuty 為所有受 SSM 管理的 Amazon EC2 執行個體建立一個 SSM 關聯，並顯示在 https://console.aws.amazon.com/systems-manager/ 主控台的叢集管理員下方。
- 在停用自動化代理程式組態的情況下使用包含標籤 — 啟用執行時期監控之後，當您未啟用自動化代理程式組態，但在 Amazon EC2 執行個體新增包含標籤時，表示您 GuardDuty 允許代表您管理安全代理程式。然後，SSM 關聯會在每個具有包含標記 (`GuardDutyManaged:true`) 的執行個體中安裝安全性代理程式。
- 如果您啟用自動化代理程式組態 — SSM 關聯會接著會在屬於您帳戶的所有 EC2 執行個體中安裝安全代理程式。
- 使用具有自動化代理程式組態的排除標籤 — 啟用自動化代理程式組態之前，當您將排除標籤新增至 Amazon EC2 執行個體時，表示您允許禁止 GuardDuty 為此選定執行個體安裝和管理安全代理程式。

  現在，當您啟用自動化代理程式組態時，SSM 關聯將在所有 EC2 執行個體中安裝和管理安全代理程式，但標有排除標籤的執行個體除外。
- GuardDuty 只要該 VPC 中至少有一個 Linux EC2 執行個體不處於終止或往返執行個體狀態，即可在所有 VPC (包括共用 VPC) 中建立 VPC 端點。有關不同執行個體狀態的資訊，請參閱 Amazon EC2 Linux 執行個體使用者指南中的執行個體生命週期。

  GuardDuty 也支持搭配自動化安全代理程式使用共用 VPC。當您的組織考慮所有必要條件時 AWS 帳戶， GuardDuty 將使用共用 VPC 來接收執行階段事件。

> **Note**
>
> 使用 GuardDuty 建立的 VPC 端點無需額外費用。

手動管理安全代理

有兩種方式可以手動管理 Amazon EC2 的安全代理程式：

- 使用中的 GuardDuty 受管文件，在 AWS Systems Manager 已經受 SSM 管理的 Amazon EC2 執行個體上安裝安全代理程式。

  每當您啟動新的 Amazon EC2 執行個體時，請確保該執行個體已啟用 SSM。

- 使用 RPM 套件管理員 (RPM) 指令碼在 Amazon EC2 執行個體上安裝安全代理程式，無論這些執行個體是否為 SSM 管理。

下一步驟

若要開始使用執行階段監控組態來監控 Amazon EC2 執行個體，請參閱Amazon EC2 執行個體支援的先決條件。

運行時監控如何與 Fargate 一起工作（僅限 Amazon ECS）

當您啟用執行階段監視時， GuardDuty 就可以使用工作的執行階段事件。這些任務會在 Amazon ECS 叢集內執行，然後在執行個體上 AWS Fargate (Fargate) 執行。若 GuardDuty 要接收這些執行階段事件，您必須使用完全管理的專用安全性代理程式。

目前，運行時監視不支持啟動的任務。 AWS CodePipeline

目前，執行階段監控僅支援透過管理 Amazon ECS 叢集的安全代理程式 (AWS Fargate)。 GuardDuty 不支援在 Amazon ECS 叢集上手動管理安全代理程式。

您可以 GuardDuty 允許代表您管理 GuardDuty 安全性代理程式，方法是為 AWS 帳戶或組織使用自動化代理程式設定。 GuardDuty 將開始將安全代理程式部署到 Amazon ECS 叢集中啟動的新 Fargate 任務。下列清單指定啟用 GuardDuty 安全代理程式時應預期的情況。

啟用 GuardDuty 安全代理程式的影響

GuardDuty 建立虛擬私有雲端 (VPC) 端點

當您部署 GuardDuty 安全性代理程式時， GuardDuty 將建立 VPC 端點，安全代理程式會透過該端點將執行階段事件傳送至 GuardDuty該端點。

> **Note**
>
> 使用 GuardDuty 建立的 VPC 端點無需額外費用。

GuardDuty 增加了一個邊車容器

對於開始執行的新 Fargate 任務或服務， GuardDuty 容器 (邊車) 會將自己附加到 Amazon ECS Fargate 任務中的每個容器上。 GuardDuty 安全性代理程式會在連接的 GuardDuty 容器內執行。這有助 GuardDuty 於收集在這些任務中運行的每個容器的運行時事件。

當您啟動 Fargate 任務時，如果 GuardDuty 容器（附屬）無法以健康狀態啟動，則運行時監視旨在不阻止任務運行。

默認情況下，Fargate 任務是不可變的。 GuardDuty 當工作已經處於執行中狀態時，將不會部署並行。如果您想要監視已在執行中的工作中的容器，您可以停止工作並重新啟動它。

執行階段監控如何與 Amazon EKS 叢集搭配使用

執行階段監視使用 EKS 附加元件 `aws-guardduty-agent`，也稱為 GuardDuty 安全性代理程式。在您的 EKS 叢集上部署 GuardDuty安全代理程式之後， GuardDuty 就能夠接收這些 EKS 叢集的執行階段事件。

您可以在帳戶或叢集層級監控 Amazon EKS 叢集的執行階段事件。您只能針對要監控威脅偵測的 Amazon EKS 叢集管理 GuardDuty 安全代理程式。您可以手動管理 GuardDuty 安全代理程式，也可以使用自動化代理程式組態 GuardDuty 來代表您管理安全代理程式。

當您使用自動化代理程式組態方法 GuardDuty 允許代表您管理安全代理程式的部署時，它會自動建立 Amazon Virtual Private Cloud 端 (Amazon VPC) 端點。安全代理程式使用此 Amazon VPC 端點將 GuardDuty 執行階段事件傳遞給。

> **Note**
>
> 使用 GuardDuty 建立的 VPC 端點無需額外費用。

目前， GuardDuty 支持在 Amazon EC2 實例上運行的亞馬遜 EKS 集群。 GuardDuty 不支援在 AWS Fargate上執行的 Amazon EKS 叢集。

執行時間後監視組態

評估運行時覆蓋

啟用執行階段監控並部署 GuardDuty Security Agent 之後，我們建議您持續 [1] 評估已部署 Security Agent 之資源的涵蓋範圍狀態。承保狀態可能是「健康」或「不健康」。狀態良好的涵蓋範圍狀態表示 GuardDuty 當有作業系統層級活動時，正從對應資源接收執行階段事件。

當資源的涵蓋範圍狀態變為 [正常] 時， GuardDuty 就可以接收執行階段事件並分析它們以進行威脅偵測。當在容器工作負載和執行個體中執行的工作或應用程式中 GuardDuty 偵測到潛在的安全威脅時， GuardDuty 會產生一或多個執行階段監控尋找類型。

[1] 您也可以設定 Amazon EventBridge (EventBridge)，以便在保固狀態從「不良」變更為「狀況良好」等狀態時接收通知。

如需詳細資訊，請參閱 評估資源的執行階段涵蓋範圍。

GuardDuty 偵測潛在威脅

當 GuardDuty 開始接收資源的執行階段事件時，它會開始分析這些事件。當 GuardDuty 偵測到任何 Amazon EC2 執行個體、Amazon ECS 叢集或 Amazon EKS 叢集中存在潛在的安全威脅時，就會產生一個或多個。執行階段監視尋找項您可以存取尋找項目詳細資訊以檢視受影響的資源詳細資訊。

30 天免費試用如何在運行時監控中工作

30 天免費試用期對於新 GuardDuty 帳戶和已啟用 EKS 執行階段監控的現有帳戶而言，在執行階段監控功能擴展到 Amazon EC2 執行個體和 AWS Fargate (僅限 Amazon ECS) 之前，其運作方式有所不同。

我正在使用 GuardDuty 試用期，或者我從未啟用 EKS 運行時監視

下列清單說明如果您使用的是 30 天試用期或從未啟用 EKS 執行階段監控， GuardDuty 30 天免費試用期的運作方式：

- 第一次啟 GuardDuty 用時，依預設不會啟用執行階段監視和 EKS 執行階段監視。

  當您為帳戶或組織啟用「執行階段監控」時，請務必同時針對您要監控威脅偵測的資源設定 GuardDuty 安全代理程式。例如，如果您想要為 Amazon EC2 執行個體使用執行階段監控，則在啟用執行階段監控之後，您還必須設定 Amazon EC2 的安全代理程式。您可以選擇手動執行此操作或通過自動執行此操作 GuardDuty。
- 執行階段監控保護計畫會在帳戶層級啟用。30 天免費試用期在資源層級運作。將 GuardDuty Security Agent 部署至特定資源類型後，30 天免費試用會在 GuardDuty 收到與此資源類型相關聯的第一個執行階段事件時開始。例如，您已在資源層級部署 GuardDuty 代理程式 (適用於 Amazon EC2 執行個體、Amazon ECS 叢集和 Amazon EKS 叢集)。當 GuardDuty 收到 Amazon EC2 執行個體的第一個執行階段事件時，只會針對 Amazon EC2 開始 30 天免費試用。
- 當您只想啟用 EKS 執行階段監視時 — 第一次啟 GuardDuty 用時，預設不會啟用 EKS 執行階段監視 (在發行執行時間監視之後)。您將需要啟用 EKS 運行時監視。若要以最佳方式使用，請確定您要手動管理 GuardDuty Security Agent，或啟用自動化代理程式組態，以便代表您 GuardDuty 管理代理程式。EKS 執行階段監控的 30 天免費試用期會在 GuardDuty 收到 Amazon EKS 資源的第一個執行時間事件時開始。

我在啟動運行時監視之前啟用了 EKS 運行時監視

- 對於已啟用 EKS 執行階段監視保護計畫並使用 GuardDuty 主控台體驗使用此保護計畫的現有 GuardDuty 帳戶 — 隨著執行階段監視的宣告，EKS 執行階段監視主控台體驗現在已整合到執行階段監視中。您現有的 EKS 執行階段監視組態會保持不變。您可以繼續使用 API/CLI 支援來執行與 EKS 執行階段監視相關聯的作業。
- 要使用 EKS 運行時監視作為運行時監視的一部分，您需要為您的帳戶或組織配置運行時監視。若要保留執行階段監視的相同組態，請參閱從 EKS 執行階段監視移轉至執行階段監視。但是，這不會影響您的 30 天免費試用 Amazon EKS 資源。
- 執行階段監控保護計畫會在每個區域的帳戶層級啟用。 GuardDuty 安全代理程式部署到其中一個指定的資源類型 (Amazon EC2 執行個體和 Amazon ECS 叢集) 後，30 天免費試用會在 GuardDuty 收到與資源相關聯的第一個執行時間事件時開始。每種資源類型都有 30 天的免費試用期。

  例如，啟用執行時期監控之後，您選擇僅在 Amazon EC2 執行個體上部署 GuardDuty 代理程式，此資源的 30 天免費試用只會在 GuardDuty 收到 Amazon EC2 執行個體的第一個執行時間事件時開始。稍後，當您為 Fargate 部署 GuardDuty 代理程式 (僅限 Amazon ECS) 時，此資源的 30 天免費試用僅在 GuardDuty收到 Amazon ECS 叢集的第一個執行階段事件時才會開始。考慮到您的帳戶已啟用 EKS 執行階段監控， GuardDuty 不會重設 Amazon EKS 資源的 30 天免費試用期。

關鍵概念-管理 GuardDuty 安全代理程式的方法

請考慮可協助您在 Amazon EKS 叢集和 Amazon ECS 叢集上管理安全代理程式的關鍵概念。

目錄

Fargate (僅限 Amazon ECS) 資源-管理安全代理 GuardDuty 程式的方法

執行階段監控可讓您選擇偵測帳戶中所有 Amazon ECS 叢集 (帳戶層級) 或選擇性叢集 (叢集層級) 上的潛在安全威脅。當您為將執行的每個 Amazon ECS Fargate 任務啟用自動化代理程式組態時，GuardDuty 會為該任務中的每個容器工作負載新增一個附屬容器。 GuardDuty 安全代理程式被部署到這個附屬容器。這就是瞭解 GuardDuty Amazon ECS 任務內容器的執行階段行為的方式。

目前，執行階段監控僅支援透過管理 Amazon ECS 叢集的安全代理程式 (AWS Fargate)。 GuardDuty 不支援在 Amazon ECS 叢集上手動管理安全代理程式。

在設定帳戶之前，請先評估您要如何管理 GuardDuty 安全代理程式，並可能監控屬於 Amazon ECS 任務之容器的執行階段行為。請考慮下列方法。

主題

管理所有 Amazon ECS 叢集的 GuardDuty 安全代理程式

這種方法將幫助您在帳戶級別檢測潛在的安全威脅。當您想要 GuardDuty 偵測屬於您帳戶的所有 Amazon ECS 叢集的潛在安全威脅時，請使用此方法。

管理大部分 Amazon ECS 叢集的 GuardDuty 安全代理程式，但排除部分 Amazon ECS 叢集

當您想 GuardDuty 要偵測 AWS 環境中大部分 Amazon ECS 叢集的潛在安全威脅，但排除部分叢集時，請使用此方法。此方法可協助您在叢集層級監控 Amazon ECS 任務中容器的執行階段行為。例如，屬於您帳戶的 Amazon ECS 叢集數量為 1000 個。不過，您只想監控 930 個 Amazon ECS 叢集。

此方法要求您將預先定義的 GuardDuty 標籤新增至不想監控的 Amazon ECS 叢集。如需詳細資訊，請參閱 管理 Fargate 的自動化安全代理程式 (僅限 Amazon ECS)。

管理選擇性 Amazon ECS 叢集的 GuardDuty 安全代理程式

當您想要 GuardDuty 偵測某些 Amazon ECS 叢集的潛在安全威脅時，請使用此方法。此方法可協助您在叢集層級監控 Amazon ECS 任務中容器的執行階段行為。例如，屬於您帳戶的 Amazon ECS 叢集數量為 1000 個。不過，您只想要監視 230 個叢集。

此方法要求您將預先定義的 GuardDuty 標籤新增至要監控的 Amazon ECS 叢集。如需詳細資訊，請參閱 管理 Fargate 的自動化安全代理程式 (僅限 Amazon ECS)。

Amazon EKS 叢集-管理 GuardDuty 安全代理程式的方法

GuardDuty 若要在帳戶層級或叢集層級使用 EKS 叢集中的執行階段事件，必須管理對應叢集的 GuardDuty 安全性代理程式。

管理 GuardDuty安全代理程式的方法

在 2023 年 9 月 13 日之前，您可以設定 GuardDuty 為在帳戶層級管理安全代理程式。此行為指出，依預設， GuardDuty 將管理屬於. AWS 帳戶現在， GuardDuty 提供精細的功能，協助您選擇要管理安全代理程式 GuardDuty 的 EKS 叢集。

選擇 手動管理 GuardDuty 安全代理 時，您仍可選取要監控的 EKS 叢集。但是，若要手動管理代理程式，則須事先為 AWS 帳戶 建立一個 Amazon VPC 端點。

> **Note**
>
> 無論您使用哪種方法來管理 GuardDuty 安全性代理程式，EKS 執行階段監視一律會在帳戶層級啟用。

主題

- 管理安全代理程式 GuardDuty
- 手動管理 GuardDuty 安全代理

管理安全代理程式 GuardDuty

GuardDuty 代表您部署和管理安全代理程式。您可以在任何時間點使用下列其中一種方法來監控帳戶中的 EKS 叢集。

主題

- 監控所有 EKS 叢集
- 監控所有 EKS 叢集並排除選定 EKS 叢集
- 監控選定 EKS 叢集

監控所有 EKS 叢集

- 使用此方法的時機 — 當您想 GuardDuty 要部署和管理帳戶中所有 EKS 叢集的安全性代理程式時，請使用此方法。依預設，也 GuardDuty 會在您帳戶中建立的可能新 EKS 叢集上部署安全性代理程式。
- 使用此方法帶來的影響：

  - GuardDuty 建立 Amazon Virtual Private Cloud 端 (Amazon VPC) 端點， GuardDuty 安全代理程式可透過該端點將執行時間事件傳遞至 GuardDuty該端點。透 GuardDuty過管理安全代理程式時，建立 Amazon VPC 端點無需額外費用。
  - 您的工作者節點必須具有通往作用中 `guardduty-data` VPC 端點的有效網路路徑。 GuardDuty 在您的 EKS 叢集上部署安全代理程式。Amazon Elastic Kubernetes Service (Amazon EKS) 將協調在 EKS 叢集中的節點上部署安全代理程式。
  - 在 IP 可用性的基礎上， GuardDuty 選取子網路以建立 VPC 端點。如果使用進階網路拓撲，則須驗證是否可以連線。
- 考量事項：目前使用此選項時，EKS 執行期監控不會建立共用 VPC。

監控所有 EKS 叢集並排除選定 EKS 叢集

- 何時使用此方法 — 當您想要 GuardDuty 管理帳戶中所有 EKS 叢集的安全性代理程式，但排除選擇性 EKS 叢集時，請使用此方法。此方法使用標籤型[1]方法，其中您可以標記不要接收執行期事件的 EKS 叢集。預先定義的標籤必須具有 `GuardDutyManaged-false` 作為鍵值對。
- 使用此方法帶來的影響：
  - 此方法要求您僅在將標籤新增至要從監視中排除的 EKS 叢集之後啟用 GuardDuty 代理程式自動管理。

    因此，當您 管理安全代理程式 GuardDuty 時，此影響也適用於此方法。在啟用 GuardDuty 代理程式自動管理之前新增標籤時， GuardDuty 將不會部署或管理從監視中排除的 EKS 叢集的安全代理程式。
- 考量：
  - 在啟用自動化代理程式組態之前，您必須將標籤鍵值配對新增為`GuardDutyManaged`：對`false`於選擇性 EKS 叢集，否則， GuardDuty 安全性代理程式將部署在所有 EKS 叢集上，直到您使用該標籤為止。
  - 您必須防止標籤遭到修改 (僅允許可信身分進行修改)。

    > **Important**
    >
    > 使用服務控制政策或 IAM 政策來管理修改 EKS 叢集的 `GuardDutyManaged` 標籤值的許可。如需詳細資訊，請參閱使用指南中的服務控制政策 (SCP) 或 IAM AWS Organizations 使用者指南中的控制對 AWS 資源的存取。

- 對於不想要監控的潛在新 EKS 叢集，請確定在建立此 EKS 叢集時新增 `GuardDutyManaged-false` 鍵值對。
- 此方法的考量事項與 監控所有 EKS 叢集 的考量事項相同。

監控選定 EKS 叢集

- 使用此方法的時機 — 當您想 GuardDuty 要僅針對帳戶中的選擇性 EKS 叢集部署和管理安全代理程式的更新時，請使用此方法。此方法使用標籤型[1]方法，其中您可以標記要接收執行期事件的 EKS 叢集。
- 使用此方法帶來的影響：
  - 透過使用包含標記， GuardDuty 將僅針對標記為 `GuardDutyManaged-`的選擇性 EKS 叢集自動部署和管理安全代理程式`true`作為鍵值配對。
  - 使用此方法所帶來的影響與 監控所有 EKS 叢集 的相同。
- 考量事項：
  - 如果 `GuardDutyManaged` 標籤的值未設定為 `true`，包含標籤將不會如預期般運作，而且這可能會對 EKS 叢集的監控帶來影響。
  - 若要確保您的選定 EKS 叢集受到監控，則需要防止標籤遭到修改 (僅允許可信身分進行修改)。

    > **Important**
    >
    > 使用服務控制政策或 IAM 政策來管理修改 EKS 叢集的 `GuardDutyManaged` 標籤值的許可。如需詳細資訊，請參閱使用指南中的服務控制政策 (SCP) 或 IAM AWS Organizations 使用者指南中的控制對 AWS 資源的存取。

  - 對於不想要監控的潛在新 EKS 叢集，請確定在建立此 EKS 叢集時新增 `GuardDutyManaged-false` 鍵值對。
  - 此方法的考量事項與 監控所有 EKS 叢集 的考量事項相同。

[1]如需有關標記選定 EKS 叢集的詳細資訊，請參閱《Amazon EKS 使用者指南》中的為您的 Amazon EKS 資源加上標籤。

手動管理 GuardDuty 安全代理

- 何時使用此方法 — 當您想要在所有 EKS 叢集上手動部署和管理 GuardDuty 安全性代理程式時，請使用此方法。確保您的帳戶已啟用 EKS 執行期監控。如果您未啟用 EKS 執行階段監視，GuardDuty安全性代理程式可能無法如預期般運作。
- 使用此方法的影響 — 您將需要協調 EKS 叢集中所有帳戶的 GuardDuty 安全性代理程式軟體部署，以及可使用此功能的 AWS 區域 地方。
- 考量事項：在持續部署新叢集和工作負載時，必須支援安全資料流程，同時監控和解決涵蓋範圍差距。

啟用 GuardDuty 執行期監視

在您的帳戶中啟用執行階段監視之前，請確定您要監視執行階段事件的資源類型支援平台需求。如需詳細資訊，請參閱 必要條件。

如果您在啟動執行階段監視之前一直使用 EKS 執行階段監視，您可以使用 API 來檢查和更新 EKS 執行階段監視的現有組態。您也可以將現有的配置從 EKS 運行時監視遷移到運行時監視。如需詳細資訊，請參閱 從 EKS 執行階段監視移轉至執行階段監視。

> **Note**
>
> 目前，本文檔提供了僅通過控制台為您的帳戶和組織啟用運行時監視的步驟。您也可以使用 API 動作或AWS CLI 來啟用執行階段監視 GuardDuty。

您可以使用下列主題中的步驟來設定「程式實際執行監視」。

目錄

啟用程式實際執行監視的

若要啟用「執行階段監控」並管理 GuardDuty Security Agent，您必須符合每個要監控安全威脅偵測之資源類型的必要條件。

目錄

Amazon EC2 執行個體支援的先決條件

讓 EC2 執行個體 SSM 受管理

您要 GuardDuty 監控執行階段事件的 Amazon EC2 執行個體必須受管理 AWS Systems Manager (SSM)。無論您是使用自動管理安全代理程式還是手動管理安全代理程式（除外方法 2-使用 RPM 安裝程序檔），都可 GuardDuty 以這樣做。

若要使用管理 Amazon EC2 執行個體 AWS Systems Manager，請參閱AWS Systems Manager 使用者指南中的為 Amazon EC2 執行個體設定 Systems Manager。

驗證架構需求

作業系統發行版的架構可能會影響 GuardDuty 安全性代理程式的行為方式。在 Amazon EC2 執行個體使用執行階段監控之前，您必須符合下列要求：

- 目前，Amazon EC2 的運行時監控支持僅適用於 Linux 版本。儘管目前無法使用對 Ubuntu 的支持，但它將在不久的將 future 進行。若要接收有關此頁面更新的通知，請訂閱 RSS 摘要。

  下表顯示已驗證可支援 Amazon EC2 執行個體 GuardDuty 安全代理程式的作業系統分佈。

作業系統發行版本	核心版本	核心支援	CPU 架構	
			x64 (AMD64)	Graviton (ARM64)
AL2 和 AL2023	5.4、5.10、5.15、6.1 * -	eBPF、Tracepoints、Kprobe	支援	支援

- 附加要求-僅當您有 Amazon EC/ 亞 Amazon EC2 時

  對於 Amazon EC/Amazon EC2，我們建議您使用最新的 Amazon ECS 優化 AMI (日期為 2023 年 9 月 29 日或更新版本)，或使用 Amazon ECS 代理程式 v1.77.0 版。

- * 目前，使用核心版本`6.1`， GuardDuty無法產執行階段監視尋找項生與. DNS 事件

驗證您的組織服務控制政策

如果您已設定服務控制原則 (SCP) 來管理組織中的權限，請確定該原則不會拒絕該權`guardduty:SendSecurityTelemetry`限。需要跨不同資源類型支援執行階段監視。 GuardDuty

如果您是成員帳戶，請與相關聯的委派管理員連線。如需管理組織的 SCP 的相關資訊，請參閱服務控制原則 (SCP)。

使用自動代理程式組態時

若要使用自動化代理程式組態 (建議)，您 AWS 帳戶 必須符合下列先決條件：

- 搭配自動化代理程式設定使用包含標籤時， GuardDuty 若要建立新執行個體的 SSM 關聯，請確定新執行個體已受 SSM 管理，並顯示在 https://console.aws.amazon.com/systems-manager/ 主控台的叢集管理員下方。
- 搭配自動化代理程式組態使用例外標記時：
  - 在為您的帳戶設定 GuardDuty 自動化代理程式之前，請先新增`GuardDutyManaged:false`標籤。

    確保在啟動 Amazon EC2 執行個體之前，先將排除標籤新增至 Amazon EC2 執行個體。啟用 Amazon EC2 的自動代理程式組態後，任何在沒有排除標籤的情況下啟動的 EC2 執行個體都會涵蓋在 GuardDuty 自動化代理程式組態下。
  - 若要讓排除標記正常運作，請更新執行個體組態，讓執行個體身分識別文件可在執行個體中繼資料服務 (IMDS) 中使用。執行此步驟的程序已經是您帳戶啟用執行期監視的一部分。

GuardDuty 代理程式的 CPU 和記憶體限制

CPU 限制

與 Amazon EC2 執行個體相關聯的 GuardDuty 安全代理程式的最大 CPU 限制為 vCPU 核心總數的 10%。例如，如果您的 EC2 執行個體具有 4 個 vCPU 核心，則安全性代理程式最多可以使用 40% 的可用百分之四十。

Memory limit (記憶體限制)

從與 Amazon EC2 執行個體相關聯的記憶體中， GuardDuty 安全性代理程式可以使用的記憶體有限。

下表顯示記憶體限制。

亞馬遜 EC2 執行個體的記憶體	GuardDuty 代理程式記憶體上限
少於 8 GB	128 MB
少於 32 GB	256 MB
大於或等於 32 GB	1 GB

下一步驟

下一步是設定執行階段監控，並管理安全代理程式 (自動或手動)。

AWS Fargate (僅限 Amazon ECS) 支援的先決條件

驗證架構需求

您使用的平台可能會影響 GuardDuty 安全代理程式 GuardDuty 在從 Amazon ECS 叢集接收執行時期事件時支援的方式。您必須確認您使用的是經過驗證的平台之一。

初始考慮因素：

您的 Amazon ECS 叢集的 AWS Fargate (Fargate) 平台必須是 Linux。對應的平台版本必須至少`1.4.0`為或`LATEST`。如需有關平台版本的詳細資訊，請參閱 Amazon 彈性容器服務開發人員指南中的 Linux 平台版本。

目前尚不支援視窗平台版本。

已驗證的平台

作業系統發佈和 CPU 架構會影響 GuardDuty安全性代理程式提供的支援。下表顯示用於部署 GuardDuty安全代理程式和設定「執行時期監控」的已驗證組態。

作業系統發行版本	核心支援	CPU 架構

		x64 (AMD64)	Graviton (ARM64)
Linux	eBPF、Trac epoints、Kprobe	支援	支援

提供 ECR 權限和子網路詳細資料

啟用執行階段監視之前，您必須提供下列詳細資訊：

提供具有權限的工作執行角色

任務執行角色要求您具有某些 Amazon Elastic Container Registry (Amazon ECR) 許可。您可以使用 AmazonECs TaskExecutionRolePolicy 託管策略，也可以將以下權限添加到您的策略中：`TaskExecutionRole`

```
...
      "ecr:GetAuthorizationToken",
      "ecr:BatchCheckLayerAvailability",
      "ecr:GetDownloadUrlForLayer",
      "ecr:BatchGetImage",
...
```

若要進一步限制 Amazon ECR 許可，您可以新增託管 GuardDuty 安全代理程式的 Amazon ECR 儲存庫 URI AWS Fargate (僅限 Amazon ECS)。如需詳細資訊，請參閱 用於 GuardDuty 代理程式的儲存庫 AWS Fargate (僅限 Amazon ECS)。

在任務定義中提供子網路詳細

您可以在任務定義中提供公有子網路做為輸入，也可以建立 Amazon ECR VPC 端點。

- 使用任務定義選項 — 在 Amazon 彈性容器服務 API 參考中執行CreateService和 UpdateServiceAPI 時，您必須傳遞子網路資訊。如需詳細資訊，請參閱 Amazon 彈性容器服務開發人員指南中的 Amazon ECS 任務定義。
- 使用 Amazon ECR VPC 端點選項 — 提供 Amazon ECR 的網路路徑-確保託管 GuardDuty 安全代理程式的 Amazon ECR 儲存庫 URI 可以存取網路。如果您的 Fargate 任務將在私有子網中運行，則 Fargate 將需要網絡路徑才能下載容器 GuardDuty 。

  如需啟用 Fargate 下載容器的相關資訊，請參閱 Amazon 彈性 GuardDuty 容器服務開發人員指南中的將 Amazon ECR 與 Amazon ECS 搭配使用。

驗證您的組織服務控制政策

如果您已設定服務控制原則 (SCP) 來管理組織中的權限，請確定該原則不會拒絕該權`guardduty:SendSecurityTelemetry`限。需要跨不同資源類型支援執行階段監視。 GuardDuty

如果您是成員帳戶，請與相關聯的委派管理員連線。如需管理組織的 SCP 的相關資訊，請參閱服務控制原則 (SCP)。

CPU 和記憶體限制

在 Fargate 工作定義中，您必須在工作層級指定 CPU 和記憶體值。下表顯示工作層級 CPU 和記憶體值的有效組合，以及容器的對應 GuardDuty 安全代理程式最大記憶體限制。 GuardDuty

CPU 數值	記憶體數值	GuardDuty 代理程式記憶體上限
256 (.25 vCPU)	512 千 MiB 位，1 GB，二 GB	128 MB
512 (.5 vCPU)	1 GB、2 GB、3 GB、4 GB	
1024 (1 vCPU)	2 GB，3 GB，4 GB	
	5 GB，6 GB，7 GB，8 GB	
2048 (2 vCPU)	介於 4 GB 與 16 GB 之間，以 1 GB 為單位遞增	
4096 (4 vCPU)	介於 8 GB 到 20 GB 之間，以 1 GB 為單位遞增	
8192 (8 vCPU)	介於 16 GB 到 28 GB 之間，以 4 GB 為單位遞增	256 MB
	介於 32 GB 到 60 GB 之間，以 4 GB 為單位遞增	512 MB
16384 (16 vCPU)	介於 32 GB 與 120 GB 之間，以 8 GB 為單位遞增	1 GB

啟用執行階段監視並評估叢集的涵蓋範圍狀態為 [狀況良好] 之後，您可以設定並檢視容器洞察指標。如需更多詳細資訊，在 Amazon ECS 叢集上設定監控。

下一步是設定執行階段監視，並設定安全代理程式。

Amazon EKS 叢集支援的先決條件

驗證架構需求

您使用的平台可能會影響 GuardDuty Security Agent 從 EKS 叢集接收執行階段事件時支援 GuardDuty 的方式。您必須確認您使用的是經過驗證的平台之一。如果您要手動管理 GuardDuty 代理程式，請確定 Kubernetes 版本支援目前使用中的 GuardDuty 代理程式版本。

已驗證的平台

作業系統發行版本、核心版本和 CPU 架構會影響 GuardDuty 安全性代理程式提供的支援。下表顯示部署 GuardDuty 安全代理程式和設定 EKS 執行階段監視的已驗證組態。

作業系統發行版本	核心版本	核心支援	CPU 架構		支援的 Kubernetes 版本
			x64 (AMD64)	Graviton (ARM64)（重力 2 及以上）[1]	
Ubuntu AL2 AL2023 [3]	5.4、5.10、5.15、6.1 [2]	eBPF 追蹤點、科普羅	支援	支援	V1.21-
Bottlerocket					V1.23-

1. Amazon EKS 叢集的執行階段監控不支援第一代 Graviton 執行個體，例如 A1 執行個體類型。
2. 目前，使用內核版本6.1， GuardDuty無法執行階段監視尋找項生成DNS 事件與.
3.

「執行階段監視」支援 AL2023，並發行 GuardDuty 安全性代理程式 v1.6.0 及更新版本。如需詳細資訊，請參閱 GuardDuty Amazon EKS 叢集的安全代理程式。

安全性代理程式支援的 Kubernetes 版本 GuardDuty

下表顯示安全性代理程式支援之 EKS 叢集的 Kubernetes 版本。 GuardDuty

Kubernetes 版本	Amazon EKS 附加 GuardDuty 安全代理版本									
	v1.6.1	v1.6.0	V1.5.0	v1.4.1	V1.4.0	v1.3.1	v1.3.0	v1.2.0	v1.1.0	v1.0.0
1.29	支援	支援	支援	支援	支援	不支援	不支援	不支援	不支援	不支援
1.28						支援	支援			
1.27								支援		
1.26									支援	
1.25										支援
1.24										
1.23										
1.22										
1.21										

部分 GuardDuty 安全代理程式版本將會結束標準支援。如需代理程式發行版本的相關資訊，請參閱GuardDuty Amazon EKS 叢集的安全代理程式。

CPU 和記憶體限制

下表顯示 GuardDuty (`aws-guardduty-agent`) 的 Amazon EKS 附加元件的 CPU 和記憶體限制。

參數	下限	上限
CPU	200 m	1000 m
記憶體	256 Mi	1024 Mi

當您使用 Amazon EKS 附加元件 1.5.0 版或更新版本時， GuardDuty 提供針對 CPU 和記憶體值設定附加元件架構的功能。如需有關可配置範圍的資訊，請參閱可配置的參數和值。

啟用 EKS 執行期監控並評估 EKS 叢集的涵蓋範圍狀態後，您可以設定和檢視 Container Insights 指標。如需詳細資訊，請參閱 設定 CPU 和記憶體監控。

下一步驟

下一步是配置運行時監視，並通過手動或自動管理安全代理程序 GuardDuty。

啟用獨立帳戶的執行階段監視

Console

1. 請登入 AWS Management Console 並開啟 GuardDuty 主控台，網址為 https://console.aws.amazon.com/guardduty/。
2. 在功能窗格中，選擇 [執行階段監視]。
3. 在 [組態] 索引標籤下，選擇 [啟用]，為您的帳戶啟用執行階段監控
4. 若 GuardDuty 要從一或多個資源類型 (Amazon EC2 執行個體、Amazon ECS 叢集或 Amazon EKS 叢集) 接收執行階段事件，請使用下列選項來管理這些資源的安全代理程式：

   啟用 GuardDuty 安全代理程式

   - 管理 Amazon EC2 執行個體的自動安全代理程式
   - 手動管理 Amazon EC2 執行個體的安全代理程式
   - 管理 Fargate 的自動化安全代理程式 (僅限 Amazon ECS)
   - 自動管理 Amazon EKS 叢集的安全代理程式
   - 手動管理 Amazon EKS 叢集的安全代理程式

啟用多帳戶環境的執行階段監控

在多帳號環境中，只有委派的系統管理 GuardDuty 員帳戶可以啟用或停用成員帳號的執行階段監視，以及管理屬於其組織中成員帳號之資源類型的自動化代理程式組態。成 GuardDuty 員帳戶無法從其帳戶修改此設定。委派的 GuardDuty 系統管理員帳戶會使用來管理其成員帳戶 AWS Organizations。如需有關多帳戶環境的詳細資訊，請參閱 Managing multiple accounts。

對於委派 GuardDuty 管理員帳戶

啟用委派 GuardDuty 管理員帳戶的執行階段監視

1. 請登入 AWS Management Console 並開啟 GuardDuty 主控台，網址為 https://console.aws.amazon.com/guardduty/。
2. 在功能窗格中，選擇 [執行階段監視]。
3. 在「組態」索引標籤下，選擇「執行時期監督」組態區段中的編輯
4. 使用為所有帳戶啟用

   如果您要針對屬於組織的所有帳戶 (包括委派的 GuardDuty 管理員帳戶) 啟用「執行階段監視」，請選擇 [啟用所有帳戶]。
5. 使用手動設定帳戶

   如果您要個別為每個成員帳戶啟用執行階段監控，請選擇「手動設定帳戶」。

   - 在委派管理員 (此帳戶) 區段下選擇啟用。
6. 若 GuardDuty 要從一或多個資源類型 (Amazon EC2 執行個體、Amazon ECS 叢集或 Amazon EKS 叢集) 接收執行階段事件，請使用下列選項來管理這些資源的安全代理程式：

   啟用 GuardDuty 安全代理程式

   - 管理 Amazon EC2 執行個體的自動安全代理程式
   - 手動管理 Amazon EC2 執行個體的安全代理程式
   - 管理 Fargate 的自動化安全代理程式 (僅限 Amazon ECS)
   - 自動管理 Amazon EKS 叢集的安全代理程式
   - 手動管理 Amazon EKS 叢集的安全代理程式

所有會員帳戶

若要為組織中的所有成員帳戶啟用執行階段監視

1. 請登入 AWS Management Console 並開啟 GuardDuty 主控台，網址為 https://console.aws.amazon.com/guardduty/。

   使用委派的 GuardDuty 系統管理員帳戶登入。
2. 在功能窗格中，選擇 [執行階段監視]。
3. 在「程式實際執行監督」頁面的「組態」頁籤下，選擇「程式實際執行監督」組態段落中的編
4. 選擇為所有帳戶啟用。
5. 若 GuardDuty 要從一或多個資源類型 (Amazon EC2 執行個體、Amazon ECS 叢集或 Amazon EKS 叢集) 接收執行階段事件，請使用下列選項來管理這些資源的安全代理程式：

   啟用 GuardDuty 安全代理程式

   - 管理 Amazon EC2 執行個體的自動安全代理程式
   - 手動管理 Amazon EC2 執行個體的安全代理程式
   - 管理 Fargate 的自動化安全代理程式 (僅限 Amazon ECS)
   - 自動管理 Amazon EKS 叢集的安全代理程式
   - 手動管理 Amazon EKS 叢集的安全代理程式

所有現有活躍會員帳戶

若要啟用組織中現有成員帳戶的執行階段監視

1. 請登入 AWS Management Console 並開啟 GuardDuty 主控台，網址為 https://console.aws.amazon.com/guardduty/。

   使用組織的委派 GuardDuty 系統管理員帳戶登入。
2. 在功能窗格中，選擇 [執行階段監視]。
3. 您可以在「程式實際執行監督」頁面的「組態」頁籤底下，檢視「程式實際執行監督」組態的目前狀態。
4. 在 [執行階段監視] 窗格的 [作用中成員帳戶] 區段下，選擇 [動作]。
5. 從動作下拉式選單中，選擇為所有作用中的成員帳戶啟用。
6. 選擇確認。

7. 若 GuardDuty 要從一或多個資源類型 (Amazon EC2 執行個體、Amazon ECS 叢集或 Amazon EKS 叢集) 接收執行階段事件，請使用下列選項來管理這些資源的安全代理程式：

   啟用 GuardDuty 安全代理程式

   - 管理 Amazon EC2 執行個體的自動安全代理程式
   - 手動管理 Amazon EC2 執行個體的安全代理程式
   - 管理 Fargate 的自動化安全代理程式 (僅限 Amazon ECS)
   - 自動管理 Amazon EKS 叢集的安全代理程式
   - 手動管理 Amazon EKS 叢集的安全代理程式

> **Note**
>
> 最多可能需要 24 小時才會更新成員帳戶的組態。

僅對新成員帳戶啟用運行時監控

為組織中的新成員帳戶啟用執行階段監視

1. 請登入 AWS Management Console 並開啟 GuardDuty 主控台，網址為 https://console.aws.amazon.com/guardduty/。

   使用組織的指定委派 GuardDuty 管理員帳戶登入。
2. 在功能窗格中，選擇 [執行階段監視]
3. 在「組態」索引標籤下，選擇「執行時期監督」組態區段中的編輯
4. 選擇手動設定帳戶。
5. 選取為新成員帳戶自動啟用。
6. 若 GuardDuty 要從一或多個資源類型 (Amazon EC2 執行個體、Amazon ECS 叢集或 Amazon EKS 叢集) 接收執行階段事件，請使用下列選項來管理這些資源的安全代理程式：

   啟用 GuardDuty 安全代理程式

   - 管理 Amazon EC2 執行個體的自動安全代理程式
   - 手動管理 Amazon EC2 執行個體的安全代理程式
   - 管理 Fargate 的自動化安全代理程式 (僅限 Amazon ECS)

- 自動管理 Amazon EKS 叢集的安全代理程式
- 手動管理 Amazon EKS 叢集的安全代理程式

僅適用於選擇性活躍會員帳戶

啟用個別作用中成員帳戶的執行階段監視

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/

   使用委派的 GuardDuty 系統管理員帳戶認證登入。
2. 在導覽窗格中，選擇帳戶。
3. 在 [帳戶] 頁面上，檢閱 [執行階段監視] 和 [自動管理代理程式] 欄中的值。這些值指出對應帳戶的「啟用執行時期監視」和「 GuardDuty 代理程式管理」是否已啟用或未啟用。
4. 從「帳戶」表中，選取您要啟用執行階段監視的帳戶。您可以一次選擇多個帳戶。
5. 選擇確認。
6. 選擇編輯保護計畫。選擇適當動作。
7. 選擇確認。
8. 若 GuardDuty 要從一或多個資源類型 (Amazon EC2 執行個體、Amazon ECS 叢集或 Amazon EKS 叢集) 接收執行階段事件，請使用下列選項來管理這些資源的安全代理程式：

   啟用 GuardDuty 安全代理程式

   - 管理 Amazon EC2 執行個體的自動安全代理程式
   - 手動管理 Amazon EC2 執行個體的安全代理程式
   - 管理 Fargate 的自動化安全代理程式 (僅限 Amazon ECS)
   - 自動管理 Amazon EKS 叢集的安全代理程式
   - 手動管理 Amazon EKS 叢集的安全代理程式

管理 GuardDuty 安全代理

您可以針對要監視的資源管理 GuardDuty 安全代理程式。如果您要監視多種資源類型，請務必管理該資源的 GuardDuty 代理程式。

> **Important**
>
> 使用 Amazon EC2 執行個體的安 GuardDuty 全代理程式時，您可以在 Amazon EKS 叢集內的基礎主機上安裝和使用代理程式。如果您已在該 EKS 叢集上部署安全性代理程式，則相同主機可能會同時在其上執行兩個安全代理程式。如需此案例中如何 GuardDuty 運作的相關資訊，請參閱處理雙安全代理程式。

下列主題將協助您進行管理安全代理程式的後續步驟。

目錄

搭配自動化安全代理程式使用共用 VPC

當您選擇 GuardDuty 自動管理安全性代理程式時，執行階段監視支援針對屬於中 AWS Organizations 的 AWS 帳戶 相同組織使用共用 VPC。您 GuardDuty 可以代表您根據與組織的共用 VPC 相關聯的詳細資料設定 Amazon VPC 端點政策。

在此版本之前，只有當您選擇手動管理 GuardDuty 安全代理程式時，才 GuardDuty 支援使用共用 VPC。

目錄

運作方式

當共用 VPC 的擁有者帳戶為任何資源 (Amazon EKS 或 AWS Fargate (僅限 Amazon ECS)) 啟用執行階段監控和自動代理程式組態時，所有共用 VPC 都有資格自動安裝共用的 Amazon VPC 端點和共用 VPC 擁有者帳戶中關聯的安全群組。 GuardDuty 擷取與共用 Amazon VPC 相關聯的組織識別碼。

現在，屬於與共用 Amazon VPC 擁有者帳戶相同組織的組織也可以共用相同的 Amazon VPC 端點。AWS 帳戶 GuardDuty 當共用 VPC 擁有者帳戶或參與帳戶需要 Amazon VPC 端點時，會建立共用 VPC。需要 Amazon VPC 端點的範例包括啟用 GuardDuty、執行階段監控、EKS 執行階段監控，或啟動新的 Amazon ECS-Fargate 任務。當這些帳戶為任何資源類型啟用執行時期監控和自動代理程式組態時， GuardDuty 會建立 Amazon VPC 端點，並使用與共用 VPC 擁有者帳戶相同的組織 ID 設定端點政策。 GuardDuty `true`為 GuardDuty 建立的 Amazon VPC 端點新增`GuardDutyManaged`標籤並將其設定為。如果共用 Amazon VPC 擁有者帳戶尚未為任何資源啟用執行時期監控或自動代理程式組態，則不 GuardDuty 會設定 Amazon VPC 端點政策。如需在共用 VPC 擁有者帳戶中設定執行階段監視和自動管理安全代理程式的相關資訊，請參閱啟用 GuardDuty 執行期監視。

使用相同 Amazon VPC 端點政策的每個帳戶都會被稱為相關聯共用 Amazon VPC 的參與者 AWS 帳戶。

以下範例顯示共用 VPC 擁有者帳戶和參與者帳戶的預設 VPC 端點策略。`aws:PrincipalOrgID`會顯示與共用 VPC 資源相關聯的組織 ID。此策略的使用僅限於擁有者帳戶組織中存在的參與者帳戶。

Example

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Action": "*",
            "Resource": "*",
            "Effect": "Allow",
            "Principal": "*"
        },
        {
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalOrgID": "o-abcdef0123"
                }
            },
            "Action": "*",
            "Resource": "*",
            "Effect": "Deny",
            "Principal": "*"
```

```
        }
    ]
}
```

使用共用 VPC 的先決條件

初始設定的先決條件

執行您要成為共用 VPC 擁有者的下列步驟： AWS 帳戶

1. 建立組織 — 按照《AWS Organizations 使用指南》中的〈建立及管理組織〉中的步驟來建立組織。

   如需新增或移除成員帳戶的相關資訊，請參閱 AWS 帳戶 在組織中管理。
2. 建立共用 VPC 資源 — 您可以從擁有者帳號建立共用 VPC 資源。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的與其他帳戶共享 VPC。

GuardDuty程式實際執行監視特定的

下列清單提供下列特定的先決條件 GuardDuty：

- 共用 VPC 的擁有者帳戶和參與帳戶可以來自中 GuardDuty的不同組織。但是，它們必須屬於中的相同組織 AWS Organizations。 GuardDuty 若要為共用虛擬私人雲端建立 Amazon VPC 端點和安全群組，這是必要的。如需共用 VPC 如何運作的相關資訊，請參閱 Amazon VPC 使用者指南中的與其他帳戶共用您的 VPC。
- 為共用 VPC 擁有者帳戶和參與者帳戶中的任何資源啟用執行階段監視或 EKS 執行階段監控，以及 GuardDuty 自動化代理程式設定。如需詳細資訊，請參閱 啟用執行期監視。

  如果您已完成這些組態，請繼續下一個步驟。
- 使用 Amazon EKS 或 Amazon ECS (AWS Fargate 僅限) 任務時，請務必選擇與擁有者帳戶相關聯的共用 VPC 資源，並選取其子網路。

常見問答集 (FAQ)

下列清單提供在執行階段監視中啟用 GuardDuty 自動化代理程式組態的共用 VPC 資源時，常見問題的疑難排解步驟：

我已經在使用運行時監視（或 EKS 運行時監視）。如何啟用共用 VPC？

如需建立共用 VPC 先決條件的相關資訊，請參閱必要條件。

當共用 VPC 擁有者帳戶和參與者帳戶都符合先決條件時， GuardDuty 將嘗試自動設定 Amazon VPC 端點政策。

如果在此版本之前，您 AWS 帳戶 遇到有關共用 VPC 不受支援的涵蓋範圍問題，請遵循先決條件。當您的資源類型 (Amazon EKS 或 Amazon ECS (AWS Fargate 僅限) 任務) 叫用共用 VPC 端點的需求時， GuardDuty 將嘗試設定新的 VPC 端點政策。

身為共用 VPC 擁有者帳戶，我希望將共用的 VPC 端點原則限制為組織中的參與者帳戶子集。我怎麼能做到這一點？

如果您有與端點關聯的`GuardDutyManaged:true`標籤，請將其移除。這可防止 GuardDuty 嘗試修改或覆寫共用 VPC 的 VPC 端點原則。

如需詳細資訊，請參閱使用端點策略控制對 VPC 端點的存取。

為什麼共用 VPC 端點會從修改**`aws:PrincipalAccount`**為**`aws:PrincipalOrgId`**？ 我怎樣才能防止這種情況？

當 GuardDuty 偵測到中相同組織的多個帳戶共用 VPC 時 AWS Organizations，會 GuardDuty 嘗試修改策略以指定組織 ID。

若要防止這種情況發生，請從共用 VPC 端點移除`GuardDutyManaged:true`標籤。這可防止 GuardDuty 嘗試修改或覆寫共用 VPC 的 VPC 端點原則。

當共享 VPC 所有者帳戶或其中一個參與者帳戶禁用或運行時監視（ GuardDuty 或 EKS 運行時監視）時會發生什麼情況？

當共用 VPC 擁有者帳戶停用 GuardDuty 或執行階段監視 (或 EKS Runtime Monitoring) 時，請GuardDuty檢查屬於參與者帳戶的任何資源類型是否已使用共用 VPC 端點，或是任何參與者帳戶是否已針對任何資源類型啟用 GuardDuty 代理程式管理。如果是，則 GuardDuty 不會刪除 VPC 端點和安全群組。

如果共用 VPC 參與者帳戶停用 GuardDuty 或執行階段監視 (或 EKS 執行階段監視)，則對共用 VPC 擁有者帳戶沒有影響，且擁有者帳戶也不會刪除共用 VPC 資源和安全性群組。

如何刪除共用的 VPC 資源？ 它會有什麼影響？

身為共用 VPC 擁有者帳戶，您可以刪除共用的 VPC 資源，即使您的帳戶或執行階段監控中的任何參與帳戶正在使用共用的 VPC 資源。如需刪除共用 VPC 及其影響的相關資訊，請參閱To delete a VPC endpoint。

處理主機上安裝的雙重安全性代理程式

Amazon EC2 執行個體可支援多種類型的工作負載。當您在 Amazon EC2 執行個體上設定自動安全代理程式時，相同的 EC2 執行個體可能會有另一個透過 EKS 的安全代理程式。

概觀

請考慮您已啟用執行階段監視的案例。現在，您可以透 GuardDuty過啟用 Amazon EKS 的自動化代理程式。您也已為 Amazon EC2 啟用自動化代理程式。可能發生在同一個基礎主機上安裝了兩個安全代理程式-一個用於 Amazon EKS，另一個用於 Amazon EC2。這可導致兩個安全性代理程式在相同主機內執行，收集執行階段事件並將其傳送至 GuardDuty，並可能產生重複的發現項目。

影響

- 當同一台主機上執行多個安全性代理程式時，您的帳戶可能會遇到兩倍的 CPU 和記憶體處理需求。如需有關每種資源類型的 CPU 和記憶體限制的資訊，請必要條件參閱該資源。
- GuardDuty 已設計執行階段監視功能的方式，即使有兩個安全性代理程式從相同的基礎主機收集執行階段事件的重疊，您的帳戶只會針對一個執行階段事件串流收取費用。

如何 GuardDuty 處理多個代理

GuardDuty 偵測兩個安全代理程式在同一台主機上執行時，並僅將其中一個安全代理程式指定為主動收集執行階段事件的安全性代理程式。第二個代理程式會消耗最少的系統資源，以防止對應用程式效能造成任何影響。

GuardDuty 會考慮下列案例：

- 當 EC2 執行個體同時屬於 Amazon EKS 和 Amazon EC2 安全代理程式的範圍時，EKS 安全代理程式會優先考慮。只有當您在 Amazon EC2 上使用安全代理程式 v1.1.0 或以上版本時，才適用此選項。較舊的代理程式版本將繼續執行並收集執行階段事件，因為舊版代理程式版本不受優先順序排列的影響
- 當 Amazon EKS 和 Amazon EC2 都有 GuardDuty 受管安全代理程式，而您的 Amazon EC2 執行個體也受到 SSM 管理時，這兩個安全代理程式都會在主機層級安裝。安裝代理程式之後， GuardDuty 決定哪個安全性代理程式將繼續執行。當兩個安全代理程式都在執行時，最終只有其中一個會收集執行階段事件。
- 當與 EC2 和 EKS 相關聯的安全代理程式同時執行時， GuardDuty 可能只在重疊期間產生重複的發現項目。

  這可能發生在以下情況：

- EC2 和 EKS 的安全代理程式可透過 GuardDuty (自動) 設定，或
- 您的 Amazon EKS 資源具有自動化安全代理程式。

- 當 EKS 安全代理程式已在執行中時，如果您在相同的基礎主機上手動部署 EC2 安全代理程式並符合所有必要條件，則 GuardDuty 可能不會安裝第二個安全代理程式。

管理 Amazon EC2 執行個體的自動安全代理程式

> **Note**
>
> 在繼續之前，請確保遵循所有Amazon EC2 執行個體支援的先決條件.

從 Amazon EC2 手動代理程式遷移至自動化代理程式

AWS 帳戶 如果您之前是手動管理 Security Agent，現在想要使用自動 GuardDuty 化代理程式組態，則此區段適用於您的。如果這不適用於您，請繼續為您的帳戶設定安全性代理程式。

當您啟用 GuardDuty 自動化代理程式時，請代表您 GuardDuty 管理安全代理程式。如 GuardDuty 需執行哪些步驟的相關資訊，請參閱使用自動化代理程式組態 (建議)。

清除資源

刪除 SSM 關聯

- 刪除您手動管理 Amazon EC2 安全代理程式時可能已建立的任何 SSM 關聯。如需詳細資訊，請參閱刪除關聯。
- 這樣做是為了 GuardDuty 能夠接管 SSM 動作的管理，無論您是在帳戶層級還是執行個體層級使用自動化代理程式 (使用包含或排除標記)。如需 SSM 動作可以 GuardDuty 採取的詳細資訊，請參閱服務連結角色權限 GuardDuty。
- 當您刪除先前為手動管理安全性代理程式而建 GuardDuty 立的 SSM 關聯時，建立用於自動管理安全性代理程式的 SSM 關聯時，可能會有短暫的重疊期間。在此期間，您可能會遇到以 SSM 排程為基礎的衝突。如需詳細資訊，請參閱 Amazon EC2 SSM 排程。

管理 Amazon EC2 執行個體的包含和排除標籤

- 包含標籤 — 當您未啟用 GuardDuty 自動化代理程式組態，但使用包含標籤 (`GuardDutyManaged:true`) 標記任何 Amazon EC2 執行個體時，會 GuardDuty 建立 SSM 關聯，以便在所選 EC2 執行個體上安裝和管理安全代理程式。這是預期的行為，可協助您僅管理所選 EC2 執行個體上的安全代理程式。如需詳細資訊，請參閱 執行階段監控如何與 Amazon EC2 執行個體搭配。

若要防 GuardDuty 止安裝和管理安全代理程式，請從這些 EC2 執行個體移除包含標籤。如需詳細資訊，請參閱 Amazon EC2 Linux 執行個體使用者指南中的新增和刪除標籤。

- 排除標籤 — 當您想要為帳戶中的所有 EC2 執行個體啟用 GuardDuty 自動化代理程式組態時，請確定沒有 EC2 執行個體標記為排除標籤 (`GuardDutyManaged:false`)。

設定獨立帳號的 GuardDuty 代理程式

Configure for all instances

為獨立帳戶中的所有執行個體設定執行階段監控

1. 請登入 AWS Management Console 並開啟 GuardDuty 主控台，網址為 https://console.aws.amazon.com/guardduty/。
2. 在功能窗格中，選擇 [執行階段監視]。
3. 在組態索引標籤下，選擇編輯。
4. 在 EC2 區段中，選擇啟用。
5. 選擇儲存。
6. 您可以確認 GuardDuty 建立的 SSM 關聯將在屬於您帳戶的所有 EC2 資源上安裝和管理安全代理程式。

   a. 開啟主 AWS Systems Manager 控台，網址為 https://console.aws.amazon.com/systems-manager/。

   b. 開啟 SSM 關聯的「目標」索引標籤 (`GuardDutyRuntimeMonitoring-do-not-delete`)。請注意，標籤鍵顯示為InstanceIds。

Using inclusion tag in selected instances

為選取的 Amazon EC2 執行個體設定 GuardDuty 安全代理程式

1. 登入 AWS Management Console 並開啟 Amazon EC2 主控台，網址為 https://console.aws.amazon.com/ec2/。
2. 將`GuardDutyManaged:true`標籤新增至您要 GuardDuty 監控和偵測潛在威脅的執行個體。如需新增此標籤的詳細資訊，請參閱將標籤新增至個別資源。
3. 您可以確認所 GuardDuty 建立的 SSM 關聯只會在使用包含標籤標記的 EC2 資源上安裝和管理安全代理程式。

開啟主 AWS Systems Manager 控台，網址為 https://console.aws.amazon.com/systems-manager/。

- 開啟建立之 SSM 關聯的 [目標] 索引標籤 (`GuardDutyRuntimeMonitoring-do-not-delete`)。標籤鍵會顯示為標籤:GuardDutyManaged。

Using exclusion tag in selected instances

> **Note**
>
> 確保在啟動 Amazon EC2 執行個體之前，先將排除標籤新增至 Amazon EC2 執行個體。啟用 Amazon EC2 的自動代理程式組態後，任何在沒有排除標籤的情況下啟動的 EC2 執行個體都會涵蓋在 GuardDuty 自動化代理程式組態下。

為選取的 Amazon EC2 執行個體設定 GuardDuty 安全代理程式

1. 登入 AWS Management Console 並開啟 Amazon EC2 主控台，網址為 https://console.aws.amazon.com/ec2/。
2. 將`GuardDutyManaged:標false`籤新增至您不想 GuardDuty 監控和偵測潛在威脅的執行個體。如需新增此標籤的詳細資訊，請參閱將標籤新增至個別資源。
3. 若要在執行個體中繼資料中使用排除標記，請執行下列步驟：
   a. 在執行個體的 [詳細資料] 索引標籤下，檢視執行個體中繼資料中允許標記的狀態。

      如果目前為「已停用」，請使用下列步驟將狀態變更為「已啟用」。否則，請跳過這個步驟。
   b. 選取您要允許其標籤的例證。
   c. 在 [動作] 功能表下，選擇 [例項設定]。
   d. 選擇「允許在執行個體中繼資料中
   e. 在執行個體中繼資料中的標籤存取權下，選取允許。
   f. 選擇儲存。
4. 新增排除標籤之後，請執行與 [設定所有執行個體] 索引標籤中指定的相同步驟。

您現在可以評估執行階段Amazon EC2 實例的覆蓋範圍。

在多帳戶環境中設定 GuardDuty 代理程式

對於委派 GuardDuty 管理員帳戶

Configure for all instances

如果您選擇啟用執行階段監視的所有帳戶，請為委派的 GuardDuty 系統管理員帳戶選擇下列其中一個選項：

- 選項 1

  在「自動化代理程式組態」下的 EC2 區段中，選取「為所有帳戶啟用」。
- 選項 2
  - 在「自動化代理程式組態」下的 EC2 區段中，選取「手動設定帳戶」。
  - 在 [委派管理員 (此帳戶)] 下，選擇 [啟用]。
- 選擇儲存。

如果您選擇「手動設定帳戶」進行「執行階段監視」，請執行下列步驟：

- 在「自動化代理程式組態」下的 EC2 區段中，選取「手動設定帳戶」。
- 在 [委派管理員 (此帳戶)] 下，選擇 [啟用]。
- 選擇儲存。

無論您選擇哪個選項來啟用委派管理 GuardDuty 員帳戶的自動化代理程式組態，您都可以確認 GuardDuty 建立的 SSM 關聯將在屬於此帳戶的所有 EC2 資源上安裝和管理安全代理程式。

1. 開啟主 AWS Systems Manager 控台，網址為 https://console.aws.amazon.com/systems-manager/。
2. 開啟 SSM 關聯的「目標」索引標籤 (`GuardDutyRuntimeMonitoring-do-not-delete`)。請注意，標籤鍵顯示為InstanceIds。

Using inclusion tag in selected instances

為選取的 Amazon EC2 執行個體設定 GuardDuty 代理程式

1. 登入 AWS Management Console 並開啟 Amazon EC2 主控台，網址為 https://console.aws.amazon.com/ec2/。

2. 將GuardDutyManaged:標true籤新增至您要 GuardDuty 監控和偵測潛在威脅的執行個體。如需新增此標籤的詳細資訊，請參閱將標籤新增至個別資源。

   新增此標籤將允許 GuardDuty 為這些選取的 EC2 執行個體安裝和管理安全代理程式。您不需要明確啟用自動化代理程式設定。

3. 您可以確認所 GuardDuty 建立的 SSM 關聯只會在使用包含標籤標記的 EC2 資源上安裝和管理安全代理程式。

   開啟主 AWS Systems Manager 控台，網址為 https://console.aws.amazon.com/systems-manager/。

   - 開啟建立之 SSM 關聯的 [目標] 索引標籤 (GuardDutyRuntimeMonitoring-do-not-delete)。標籤鍵會顯示為標籤:GuardDutyManaged。

Using exclusion tag in selected instances

> **Note**
>
> 確保在啟動 Amazon EC2 執行個體之前，先將排除標籤新增至 Amazon EC2 執行個體。啟用 Amazon EC2 的自動代理程式組態後，任何在沒有排除標籤的情況下啟動的 EC2 執行個體都會涵蓋在 GuardDuty 自動化代理程式組態下。

為選取的 Amazon EC2 執行個體設定 GuardDuty 代理程式

1. 登入 AWS Management Console 並開啟 Amazon EC2 主控台，網址為 https://console.aws.amazon.com/ec2/。
2. 將GuardDutyManaged:標false籤新增至您不想 GuardDuty 監控和偵測潛在威脅的執行個體。如需新增此標籤的詳細資訊，請參閱將標籤新增至個別資源。
3. 若要在執行個體中繼資料中使用排除標記，請執行下列步驟：

   a. 在執行個體的 [詳細資料] 索引標籤下，檢視執行個體中繼資料中允許標記的狀態。

      如果目前為「已停用」，請使用下列步驟將狀態變更為「已啟用」。否則，請跳過這個步驟。

   b. 在 [動作] 功能表下，選擇 [例項設定]。

   c. 選擇「允許在執行個體中繼資料中

4. 新增排除標籤之後，請執行與 [設定所有執行個體] 索引標籤中指定的相同步驟。

您現在可以評估執行階段Amazon EC2 實例的覆蓋範圍。

自動啟用所有會員帳戶

> **Note**
>
> 最多可能需要 24 小時才會更新成員帳戶的組態。

Configure for all instances

下列步驟假設您在「執行時期監視」區段中選擇了針對所有帳戶啟用：

1. 在 Amazon EC2 的「自動化代理程式組態」區段中，為所有帳戶選擇啟用。
2. 您可以確認 GuardDuty 建立 (`GuardDutyRuntimeMonitoring-do-not-delete`) 的 SSM 關聯將在屬於此帳戶的所有 EC2 資源上安裝和管理安全代理程式。

   a. 開啟主 AWS Systems Manager 控台，網址為 https://console.aws.amazon.com/systems-manager/。
   b. 開啟 SSM 關聯的「目標」索引標籤。請注意，標籤鍵顯示為InstanceIds。

Using inclusion tag in selected instances

為選取的 Amazon EC2 執行個體設定 GuardDuty 代理程式

1. 登入 AWS Management Console 並開啟 Amazon EC2 主控台，網址為 https://console.aws.amazon.com/ec2/。
2. 將`GuardDutyManaged:true`標籤新增至您要 GuardDuty 監控和偵測潛在威脅的 EC2 執行個體。如需新增此標籤的詳細資訊，請參閱將標籤新增至個別資源。

   新增此標籤將允許 GuardDuty 為這些選取的 EC2 執行個體安裝和管理安全代理程式。您不需要明確啟用自動化代理程式設定。
3. 您可以確認 GuardDuty 建立的 SSM 關聯將在屬於您帳戶的所有 EC2 資源上安裝和管理安全代理程式。

   a. 開啟主 AWS Systems Manager 控台，網址為 https://console.aws.amazon.com/systems-manager/。
   b. 開啟 SSM 關聯的「目標」索引標籤 (`GuardDutyRuntimeMonitoring-do-not-delete`)。請注意，標籤鍵顯示為InstanceIds。

Using exclusion tag in selected instances

> **Note**
>
> 確保在啟動 Amazon EC2 執行個體之前，先將排除標籤新增至 Amazon EC2 執行個體。啟用 Amazon EC2 的自動代理程式組態後，任何在沒有排除標籤的情況下啟動的 EC2 執行個體都會涵蓋在 GuardDuty 自動化代理程式組態下。

為選取的 Amazon EC2 執行個體設定 GuardDuty 安全代理程式

1. 登入 AWS Management Console 並開啟 Amazon EC2 主控台，網址為 https://console.aws.amazon.com/ec2/。
2. 將`GuardDutyManaged:false`標籤新增至您不想 GuardDuty 監控和偵測潛在威脅的執行個體。如需新增此標籤的詳細資訊，請參閱將標籤新增至個別資源。
3. 若要在執行個體中繼資料中使用排除標記，請執行下列步驟：
   a. 在執行個體的 [詳細資料] 索引標籤下，檢視執行個體中繼資料中允許標記的狀態。

      如果目前為「已停用」，請使用下列步驟將狀態變更為「已啟用」。否則，請跳過這個步驟。
   b. 在 [動作] 功能表下，選擇 [例項設定]。
   c. 選擇「允許在執行個體中繼資料中
4. 新增排除標籤之後，請執行與 [設定所有執行個體] 索引標籤中指定的相同步驟。

您現在可以評估執行階段Amazon EC2 實例的覆蓋範圍。

僅對新會員帳戶自動啟用

委派的 GuardDuty 管理員帳戶可以為 Amazon EC2 資源設定自動代理程式組態，以便在新成員帳戶加入組織時自動啟用。

Configure for all instances

下列步驟假設您已在「執行階段監視」區段下選取「為新成員帳戶啟用自動啟用」：

1. 在功能窗格中，選擇 [執行階段監視]。
2. 在「程式實際執行監督」頁面上，選擇編輯

3. 選取為新成員帳戶自動啟用。此步驟可確保每當有新帳戶加入組織時，Amazon EC2 的自動代理程式組態都會自動為其帳戶啟用。只有組織的委派 GuardDuty 管理員帳戶可以修改此選項。
4. 選擇儲存。

當新成員帳戶加入組織時，會自動為他們啟用此組態。 GuardDuty 要管理屬於此新成員帳戶的 Amazon EC2 執行個體的安全代理程式，請確保符合所對於 EC2 執行個體有先決條件。

建立 SSM 關聯時 (`GuardDutyRuntimeMonitoring-do-not-delete`)，您可以確認 SSM 關聯將在屬於新成員帳戶的所有 EC2 執行個體上安裝和管理安全代理程式。

- 開啟主 AWS Systems Manager 控台，網址為 https://console.aws.amazon.com/systems-manager/。
- 開啟 SSM 關聯的「目標」索引標籤。請注意，標籤鍵顯示為InstanceIds。

Using inclusion tag in selected instances

為您帳戶中選取的執行個體設定 GuardDuty 安全代理程式

1. 登入 AWS Management Console 並開啟 Amazon EC2 主控台，網址為 https://console.aws.amazon.com/ec2/。
2. 將`GuardDutyManaged`:標`true`籤新增至您要 GuardDuty 監控和偵測潛在威脅的執行個體。如需新增此標籤的詳細資訊，請參閱將標籤新增至個別資源。

   新增此標籤將允許 GuardDuty 為這些選取的執行個體安裝和管理安全代理程式。您不需要明確啟用自動化代理程式設定。
3. 您可以確認所 GuardDuty 建立的 SSM 關聯只會在使用包含標籤標記的 EC2 資源上安裝和管理安全代理程式。

   a. 請在以下位置開啟 AWS Systems Manager 主控台。 https://console.aws.amazon.com/systems-manager/

   b. 開啟所建立之 SSM 關聯的 [目標] 索引標籤。標籤鍵會顯示為標籤:GuardDutyManaged。

Using exclusion tag in selected instances

> **Note**
>
> 確保在啟動 Amazon EC2 執行個體之前，先將排除標籤新增至 Amazon EC2 執行個體。啟用 Amazon EC2 的自動代理程式組態後，任何在沒有排除標籤的情況下啟動的 EC2 執行個體都會涵蓋在 GuardDuty 自動化代理程式組態下。

為獨立帳戶中的特定執行個體設定 GuardDuty 安全性代理程式

1. 登入 AWS Management Console 並開啟 Amazon EC2 主控台，網址為 https://console.aws.amazon.com/ec2/。
2. 將`GuardDutyManaged:false`標籤新增至您不想 GuardDuty 監控和偵測潛在威脅的執行個體。如需新增此標籤的詳細資訊，請參閱將標籤新增至個別資源。
3. 若要在執行個體中繼資料中使用排除標記，請執行下列步驟：
   a. 在執行個體的 [詳細資料] 索引標籤下，檢視執行個體中繼資料中允許標記的狀態。

      如果目前為「已停用」，請使用下列步驟將狀態變更為「已啟用」。否則，請跳過這個步驟。
   b. 在 [動作] 功能表下，選擇 [例項設定]。
   c. 選擇「允許在執行個體中繼資料中
4. 新增排除標籤之後，請執行與 [設定所有執行個體] 索引標籤中指定的相同步驟。

您現在可以評估執行階段Amazon EC2 實例的覆蓋範圍。

僅限選擇性成員帳戶

Configure for all instances

1. 在 [帳戶] 頁面上，選取要啟用執行時間監控-自動化代理程式組態 (Amazon EC2) 的一或多個帳戶。請確定您在此步驟中選取的帳戶已啟用「執行階段監視」。
2. 從編輯保護計劃中，選擇適當的選項以啟用執行時期監控-自動化代理程式組態 (Amazon EC2)。
3. 選擇確認。

Using inclusion tag in selected instances

設定所選執行個體的 GuardDuty 安全代理程式

1. 登入 AWS Management Console 並開啟 Amazon EC2 主控台，網址為 https://console.aws.amazon.com/ec2/。
2. 將`GuardDutyManaged:標true`籤新增至您要 GuardDuty 監控和偵測潛在威脅的執行個體。如需新增此標籤的詳細資訊，請參閱將標籤新增至個別資源。

   新增此標籤將 GuardDuty 允許管理標記 Amazon EC2 執行個體的安全代理程式。您不需要明確啟用自動化代理程式組態 (執行階段監控-自動化代理程式組態 (EC2)。

Using exclusion tag in selected instances

> **Note**
>
> 確保在啟動 Amazon EC2 執行個體之前，先將排除標籤新增至 Amazon EC2 執行個體。啟用 Amazon EC2 的自動代理程式組態後，任何在沒有排除標籤的情況下啟動的 EC2 執行個體都會涵蓋在 GuardDuty 自動化代理程式組態下。

設定所選執行個體的 GuardDuty 安全代理程式

1. 登入 AWS Management Console 並開啟 Amazon EC2 主控台，網址為 https://console.aws.amazon.com/ec2/。
2. 將`GuardDutyManaged:標false`籤新增至您不想 GuardDuty 監控或偵測潛在威脅的 EC2 執行個體。如需新增此標籤的詳細資訊，請參閱將標籤新增至個別資源。
3. 若要在執行個體中繼資料中使用排除標記，請執行下列步驟：

   a. 在執行個體的 [詳細資料] 索引標籤下，檢視執行個體中繼資料中允許標記的狀態。

      如果目前為「已停用」，請使用下列步驟將狀態變更為「已啟用」。否則，請跳過這個步驟。

   b. 在 [動作] 功能表下，選擇 [例項設定]。

   c. 選擇「允許在執行個體中繼資料中

4. 新增排除標籤之後，請執行與 [設定所有執行個體] 索引標籤中指定的相同步驟。

您現在可以評估Amazon EC2 實例的覆蓋範圍。

手動管理 Amazon EC2 執行個體的安全代理程式

啟用執行階段監控之後，您將需要手動安裝安 GuardDuty 全代理程式。透過安裝代理程式，GuardDuty 將會從 Amazon EC2 執行個體接收執行階段事件。

若要管理 GuardDuty 安全代理程式，您必須建立 Amazon VPC 端點，然後按照步驟手動安裝安全代理程式。

手動建立 Amazon VPC 端點

您必須先建立 Amazon 虛擬私有雲端 (Amazon VPC) 端點，才能安裝安 GuardDuty 全代理程式。這將有助於 GuardDuty 接收 Amazon EC2 執行個體的執行階段事件。

> **Note**
>
> 使用 VPC 端點不會產生額外費用。

若要建立 Amazon VPC 端點

1. 登入 AWS Management Console 並開啟 Amazon VPC 主控台，網址為 https://console.aws.amazon.com/vpc/。
2. 在導覽窗格的 VPC 私有雲下，選擇 [端點]。
3. 選擇建立端點。
4. 在建立端點頁面上，為服務類別選擇其他端點服務。
5. 對於服務名稱，輸入 **`com.amazonaws.`*`us-east-1`*`.guardduty-data`**。

   確保將 *`us-east-1`* 替換為您的. AWS 區域這個區域必須與屬於您 AWS 帳戶 ID 的 Amazon EC2 執行個體所在的區域相同。
6. 選擇驗證服務。
7. 成功驗證服務名稱後，請選擇執行個體所在的 VPC。新增下列政策，將 Amazon VPC 端點僅限於指定帳戶的使用量。您可以透過本政策下方提供的組織 `Condition`，更新下列政策以限制對端點的存取權限。若要為組織中的特定帳戶 ID 提供 Amazon VPC 端點支援，請參閱Organization condition to restrict access to your endpoint。

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

```
 "Statement": [
  {
   "Action": "*",
   "Resource": "*",
   "Effect": "Allow",
   "Principal": "*"
  },
  {
   "Condition": {
    "StringNotEquals": {
     "aws:PrincipalAccount": "111122223333"
    }
   },
   "Action": "*",
   "Resource": "*",
   "Effect": "Deny",
   "Principal": "*"
  }
 ]
}
```

aws:PrincipalAccount 帳戶 ID 必須符合包含 VPC 和 VPC 端點的帳戶。下列清單顯示如何與其他 AWS 帳號 ID 共用 VPC 端點：

- 若要指定多個帳戶以存取 VPC 端點，請以下列區塊取代"aws:PrincipalAccount: "111122223333"：

  ```
  "aws:PrincipalAccount": [
            "666666666666",
            "555555555555"
       ]
  ```

  請務必將 AWS 帳號 ID 取代為需要存取 VPC 端點之帳戶的帳戶 ID。

- 若要允許組織中的所有成員存取 VPC 端點，請以下列行取代"aws:PrincipalAccount: "111122223333"：

  ```
  "aws:PrincipalOrgID": "o-abcdef0123"
  ```

  請務必使用您的組織識別碼取代組織 *o-abcdef0123*。

- 若要透過組織 ID 限制存取資源，請將您的資源新增`ResourceOrgID`至策略。如需詳細資訊，請參閱《IAM 使用者指南》中的 `aws:ResourceOrgID`。

```
"aws:ResourceOrgID": "o-abcdef0123"
```

8. 在其他設定下方，選擇啟用 DNS 名稱。
9. 在「子網路」下，選擇執行個體所在的子網路。
10. 在安全群組下，選擇已從 VPC (或 Amazon EC2 執行個體) 啟用連接埠 443 的安全群組。如果您尚未啟用連結連接埠 443 的安全群組，請參閱 Amazon EC2 Linux 執行個體使用者指南中的建立安全群組。

    如果在限制 VPC (或執行個體) 的上傳權限時發生問題，請從任何 IP 位址提供對內繫結 443 連接埠的支援。(`0.0.0.0/0`)

手動安裝安全代理程式

GuardDuty 提供下列兩種在 Amazon EC2 執行個體上 GuardDuty 安裝安全代理程式的方法：

- 方法 1-使用 AWS Systems Manager — 此方法需要 AWS Systems Manager 管理您的 Amazon EC2 執行個體。
- 方法 2-使用 RPM 安裝指令碼 — 無論您的 Amazon EC2 執行個體是否 AWS Systems Manager 受管，都可以使用此方法。

方法 1-通過使用 AWS Systems Manager

若要使用此方法，請確定您的 Amazon EC2 執行個體已受 AWS Systems Manager 管理，然後再安裝代理程式。

AWS Systems Manager 受管亞馬遜 EC2 執行個

使用下列步驟讓您的 Amazon EC2 執行個體 AWS Systems Manager 受到管理。

- AWS Systems Manager協助您管理 AWS 應用程式和資源， end-to-end 並實現大規模的安全作業。

  若要使用管理 Amazon EC2 執行個體 AWS Systems Manager，請參閱AWS Systems Manager 使用者指南中的為 Amazon EC2 執行個體設定 Systems Manager。
- 下表顯示新的 GuardDuty 受管理 AWS Systems Manager 文件：

文件名稱	文件類型	用途
AmazonGuardDuty-RuntimeMonitoringSsmPlugin	Distributor	封裝 GuardDuty 安全代理程式。
AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin	Command	執行安裝/解除安裝指令碼以安裝 Security Agent。GuardDuty

如需有關的詳細資訊 AWS Systems Manager，請參閱AWS Systems Manager 使用者指南中的 Amazon EC2 Systems Manager 文件。

若要使用安裝亞馬遜 EC2 執行個體的 GuardDuty 代理程式 AWS Systems Manager

1. 請在以下位置開啟 AWS Systems Manager 主控台。 https://console.aws.amazon.com/systems-manager/
2. 在功能窗格中，選擇 [文件]
3. 在 Amazon 擁有, 選擇AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin.
4. 選擇 Run Command (執行命令)。
5. 輸入以下運行命令參數
   - 動作：選擇 [安裝]。
   - 安裝類型：選擇安裝或解除安裝。
   - 名稱：AmazonGuardDuty-RuntimeMonitoringSsmPlugin
   - 版本：如果這仍然是空的，您將獲得最新版本的 GuardDuty 安全代理程式。如需有關發行版本的詳細資訊，請參閱GuardDuty Amazon EC2 執行個體的安全代理。
6. 選取目標亞馬遜 EC2 執行個體。您可以選取一或多個 Amazon EC2 執行個體。若要取得更多資訊，請參閱《使用指南》中的〈從主控台AWS Systems Manager 執行AWS Systems Manager 指令
7. 驗證 GuardDuty 代理程式安裝是否正常。如需詳細資訊，請參閱 驗證安 GuardDuty 全代理程式安裝狀態。

方法 2-使用 RPM 安裝程序檔

> **Important**
>
> 強烈建議您先驗證 GuardDuty 安全代理程式 RPM 簽章，然後再將其安裝到您的電腦上。

1. 驗證 GuardDuty 安全性代理程式 RPM 簽章

   a. 下載適當的公開金鑰、x86_64 RPM 的簽章、arm64 RPM 的簽章，以及存取 Amazon S3 儲存貯體中託管之 RPM 指令碼的對應存取連結

      您可以使用下列範本來形成公開金鑰、x86_64 RPM 的簽章、arm64 RPM 簽章，以及 RPM 指令碼的對應存取連結。取代 AWS 區域、 AWS 帳號識別碼和 GuardDuty 代理程式版本的值，以存取 RPM 指令碼。

      - 公開金鑰：

        ```
        s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/publickey.pem
        ```

      - GuardDuty 安全代理程式 RPM 簽章：

        64 轉速的簽名

        ```
        s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/x86_64/
        amazon-guardduty-agent-1.1.0.x86_64.sig
        ```

        臂 64 轉速簽名

        ```
        s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/arm64/
        amazon-guardduty-agent-1.1.0.arm64.sig
        ```

      - 存取 Amazon S3 儲存貯體中 RPM 指令碼的連結：

        存取 64 轉速的連結

        ```
        s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/x86_64/
        amazon-guardduty-agent-1.1.0.x86_64.rpm
        ```

ARM64 轉速的存取連結

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/arm64/
amazon-guardduty-agent-1.1.0.arm64.rpm
```

在下列命令中下載適當的公開金鑰、x86_64 RPM 的簽章、arm64 RPM 簽章，以及 Amazon S3 儲存貯體中託管之 RPM 指令碼的對應存取連結，請務必將帳戶 ID 替換為適當 AWS 帳戶的 ID，並將該區域取代為您目前的區域。

```
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/
x86_64/amazon-guardduty-agent-1.1.0.x86_64.rpm ./amazon-guardduty-
agent-1.1.0.x86_64.rpm
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/
x86_64/amazon-guardduty-agent-1.1.0.x86_64.sig ./amazon-guardduty-
agent-1.1.0.x86_64.sig
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/
publickey.pem ./publickey.pem
```

AWS 區域	區域名稱	AWS 帳號識別碼
eu-west-1	歐洲 (愛爾蘭)	694911143906
us-east-1	美國東部 (維吉尼亞北部)	593207742271
us-west-2	美國西部 (奧勒岡)	733349766148
eu-west-3	Europe (Paris)	665651866788
us-east-2	美國東部 (俄亥俄)	307168627858
eu-central-1	歐洲 (法蘭克福)	323658145986
ap-northeast-2	亞太區域 (首爾)	914738172881
eu-north-1	歐洲 (斯德哥爾摩)	591436053604
ap-east-1	亞太區域 (香港)	258348409381
me-south-1	Middle East (Bahrain)	536382113932

eu-west-2	歐洲 (倫敦)	892757235363
ap-northeast-1	亞太區域 (東京)	533107202818
ap-southeast-1	亞太區域 (新加坡)	174946120834
ap-south-1	亞太區域 (孟買)	251508486986
ap-southeast-3	亞太區域 (雅加達)	510637619217
sa-east-1	南美洲 (聖保羅)	758426053663
ap-northeast-3	亞太區域 (大阪)	273192626886
eu-south-1	歐洲 (米蘭)	266869475730
af-south-1	非洲 (開普敦)	197869348890
ap-southeast-2	亞太區域 (悉尼)	005257825471
me-central-1	中東 (阿拉伯聯合大公國)	000014521398
us-west-1	美國西部 (加利佛尼亞北部)	684579721401
ca-central-1	加拿大 (中部)	354763396469
ap-south-2	亞太區域 (海德拉巴)	950823858135
eu-south-2	歐洲 (西班牙)	919611009337
eu-central-2	歐洲 (蘇黎世)	529164026651
ap-southeast-4	亞太區域 (墨爾本)	251357961535
il-central-1	以色列 (特拉維夫)	870907303882

b. 將公鑰導入數據庫

```
gpg --import publickey.pem
```

gpg 顯示匯入成功

```
gpg: key 093FF49D: public key "AwsGuardDuty" imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
```

c. 驗證簽名

```
gpg --verify amazon-guardduty-agent-1.1.0.x86_64.sig amazon-guardduty-
agent-1.1.0.x86_64.rpm
```

如果驗證通過，您將看到類似以下結果的消息。您現在可以繼續使用 RPM 來 GuardDuty 安裝安全代理程式。

輸出範例：

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: Good signature from "AwsGuardDuty"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 7478 91EF 5378 1334 4456  7603 06C9 06A7 093F F49D
```

如果驗證失敗，表示 RPM 上的簽章可能遭到竄改。您必須從資料庫移除公開金鑰，然後重試驗證程序。

範例：

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: BAD signature from "AwsGuardDuty"
```

d. 從資料庫中移除公開金鑰。

```
gpg --delete-keys AwsGuardDuty
```

2. 透過安全殼層從 Linux 或 macOS 系統 Connec t 線。
3. 使用下列命令安裝安 GuardDuty 全代理程式：

```
sudo rpm -ivh amazon-guardduty-agent-1.1.0.x86_64.rpm
```

4. 驗證 GuardDuty 代理程式安裝是否正常。若要取得有關步驟的更多資訊，請參閱驗證安 GuardDuty 全代理程式安裝狀態。

5. (選擇性) 使用下列命令移除 GuardDuty 安全代理程式：

```
sudo rpm -ev amazon-guardduty-agent
```

記憶體不足錯誤

如果手動安裝或更新 Amazon EC2 的安 GuardDuty 全代理程式時`out-of-memory`發生錯誤，請參閱疑難排解記憶體不足錯誤。

驗證安 GuardDuty 全代理程式安裝狀態

驗證 GuardDuty 安全性代理程式是否健全

1. 透過安全殼層從 Linux 或 macOS 系統 Connec t 線。
2. 執行下列命令以檢查 GuardDuty 安全代理程式的狀態：

```
sudo systemctl status amazon-guardduty-agent
```

如果您要檢視 Security Agent 安裝記錄檔，可在下找到這些記錄檔`/var/log/amzn-guardduty-agent/`。

要查看日誌，請執行`sudo journalctl -u amazon-guardduty-agent`。

手動更新 GuardDuty 安全代理程式

您可以使用 [執行] 命令來更新 GuardDuty 安全性代理程式。您可以遵循與安裝安 GuardDuty 全代理程式相同的步驟。

手動解除安全性代理

本節提供從 Amazon EC2 資源解除 GuardDuty 安全代理程式解除安裝的方法。如果您進一步計劃停用執行階段監視，請參閱禁用的影響。

方法 1-通過使用運行命令

使用 [執行] 命令解除 GuardDuty 安裝安全性代理程式

1. 您可以依照《AWS Systems Manager 使用者指南》中的AWS Systems Manager 執行命令中指定的步驟，解除安裝 GuardDuty Security Agent。使用參數中的「解除安裝」動作可解除安裝 GuardDuty Security Agent。

在「目標」區段中，請確定影響只對您要從中解除安全代理程式解除安裝的 Amazon EC2 執行個體。

使用以下 GuardDuty 文件和分銷商：

- 文件名稱：`AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin`
- 經銷商:`AmazonGuardDuty-RuntimeMonitoringSsmPlugin`

2. 提供所有詳細資料後，當您選擇執行時，會移除其在目標 Amazon EC2 執行個體上部署的安全代理程式。

   若要移除 Amazon VPC 端點組態，您必須同時停用執行階段監控和 Amazon EKS 執行階段監控。

方法 2-使用 RPM 指令碼

使用 rpm 解除 GuardDuty 安裝安全代理程式

1. 透過安全殼層從 Linux 或 macOS 系統 Connec t 線。
2. 下列命令會從您連線的 Amazon EC2 執行個體解除 GuardDuty 安全代理程式：

   ```
   sudo rpm -e amazon-guardduty-agent
   ```

   您也可以檢查與此命令相關聯的日誌。

刪除 Amazon VPC 端點

當您要停用執行階段監控或解除 GuardDuty 安裝帳戶的安全代理程式時，也可以選擇刪除手動建立的 Amazon VPC 端點 (手動建立 Amazon VPC 端點)。

使用主控台刪除 Amazon VPC 端點

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中選擇 Endpoints (端點)。
3. 選取啟用「執行時期監視」時手動建立的端點。
4. 選擇 Actions (動作)、Delete VPC endpoints (刪除 VPC 端點)。
5. 出現確認提示時，請按一下 **`delete`**。

6. 選擇刪除。

若要使用刪除 Amazon VPC 端點 AWS CLI

- delete-vpc-endpoints (AWS Command Line Interface)
- Remove-EC2VpcEndpoint指令程式 (視窗 PowerShell工具)

管理 Fargate 的自動化安全代理程式 (僅限 Amazon ECS)

設定獨立帳號的 GuardDuty 代理程式

目前，執行階段監控僅支援透過管理 Amazon ECS 叢集的安全代理程式 (AWS Fargate)。 GuardDuty 不支援在 Amazon ECS 叢集上手動管理安全代理程式。

Console

1. 請登入 AWS Management Console 並開啟 GuardDuty 主控台，網址為 https://console.aws.amazon.com/guardduty/。
2. 在功能窗格中，選擇 [執行階段監視]。
3. 在組態索引標籤下：

   a. 管理所有 Amazon ECS 叢集 (帳戶層級) 的自動化代理程式組態

      在的 AWS Fargate (僅限 ECS) 的「自動化代理程式組態」區段中選擇「啟用」。當新的 Fargate Amazon ECS 任務啟動時， GuardDuty 將管理安全代理程式的部署。

      - 選擇儲存。

   b. 透過排除部分 Amazon ECS 叢集 (叢集層級) 來管理自動化代理程式組態

      i. 將標籤新增至您要排除所有任務的 Amazon ECS 叢集。鍵值對必須是 `GuardDutyManaged-false`。

      ii. 防止修改這些標籤，但受信任的實體除外。除了AWS Organizations 使用者指南中的授權原則外，「防止標籤被修改」中提供的原則已修改為適用於此處。

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

```
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
```

```
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

iii. 在「組態」索引標籤下，選擇「自動化代理程式組態」區段中的啟

> **Note**
>
> 在為您的帳戶啟用 GuardDuty 代理程式自動管理之前，請務必將排除標籤新增至 Amazon ECS 叢集；否則，安全代理程式將部署到對應 Amazon ECS 叢集中啟動的所有任務中。

對於尚未排除的 Amazon ECS 叢集， GuardDuty 將管理附屬容器中安全代理程式的部署。

iv. 選擇儲存。

c. 透過包含部分 Amazon ECS 叢集 (叢集層級) 來管理自動化代理程式組態

i. 將標籤新增至您要包含所有任務的 Amazon ECS 叢集。鍵值對必須是 `GuardDutyManaged-true`。

ii. 防止修改這些標籤，但受信任的實體除外。除了AWS Organizations 使用者指南中的授權原則外，「防止標籤被修改」中提供的原則已修改為適用於此處。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
```

```
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

設定多帳戶環境的 GuardDuty 代理程式

在多帳戶環境中，只有委派的管理 GuardDuty 員帳戶可以為成員帳戶啟用或停用自動化代理程式組態，以及管理屬於其組織中成員帳戶之 Amazon ECS 叢集的自動代理程式組態。成 GuardDuty員帳戶無法修改此設定。委派的管理 GuardDuty 員帳戶會使用來管理其成員帳戶 AWS Organizations。如需有關多帳戶環境的詳細資訊，請參閱在 GuardDuty中管理多個帳戶。

為委派的管理 GuardDuty 員帳戶啟用自動代理程式

Manage for all Amazon ECS clusters (account level)

如果您選擇為執行階段監視的所有帳戶啟用，則有下列選項：

- 在 [自動代理程式組態] 區段中選擇 [啟用所有帳戶]。 GuardDuty 將針對啟動的所有 Amazon ECS 任務部署和管理安全代理程式。
- 選擇手動設定帳戶。

如果您在「執行階段監視」區段中選擇「手動設定帳戶」，請執行下列動作：

1. 在「自動化代理程式組態」區段中選擇「手動設定帳
2. 在委派的 GuardDuty 系統管理員帳戶 (此帳戶) 區段中選擇 [啟用]。

選擇儲存。

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. 將標籤新增至此 Amazon ECS 叢集，其鍵值對為 `GuardDutyManaged-。false`
2. 防止對標籤進行修改，但受信任的實體除外。除了AWS Organizations 使用者指南中的授權原則外，「防止標籤被修改」中提供的原則已修改為適用於此處。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
```

```
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
```

```
        }
    ]
}
```

3. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/
4. 在功能窗格中，選擇 [執行階段監視]。
5.

> **Note**
>
> 在為您的帳戶啟用自動化代理程式組態之前，請務必將排除標籤新增至 Amazon ECS 叢集；否則， GuardDuty 附屬容器將附加到 Amazon ECS 任務中啟動的所有容器。

   在組態索引標籤下，選擇自動化代理程式組態中的啟用。

   對於尚未排除的 Amazon ECS 叢集， GuardDuty 將管理附屬容器中安全代理程式的部署。
6. 選擇儲存。

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. 將標籤新增至您要包含所有任務的 Amazon ECS 叢集。鍵值對必須是 `GuardDutyManaged-true`。
2. 防止修改這些標籤，但受信任的實體除外。除了AWS Organizations 使用者指南中的授權原則外，「防止標籤被修改」中提供的原則已修改為適用於此處。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
```

```
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
```

```
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> 在 Amazon ECS 叢集使用包含標籤時，您不需要明確透過自動化 GuardDuty 代理程式調整啟用代理程式。

自動啟用所有會員帳戶

Manage for all Amazon ECS clusters (account level)

下列步驟假設您在「執行時期監視」區段中選擇了針對所有帳戶啟用。

1. 在 [自動代理程式組態] 區段中選擇 [啟用所有帳戶]。 GuardDuty 將針對啟動的所有 Amazon ECS 任務部署和管理安全代理程式。
2. 選擇儲存。

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. 將標籤新增至此 Amazon ECS 叢集，其鍵值對為 `GuardDutyManaged-。false`
2. 防止對標籤進行修改，但受信任的實體除外。除了AWS Organizations 使用者指南中的授權原則外，「防止標籤被修改」中提供的原則已修改為適用於此處。

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

```
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
```

```
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/
4. 在功能窗格中，選擇 [執行階段監視]。
5.

> **Note**
>
> 在為您的帳戶啟用自動化代理程式組態之前，請務必將排除標籤新增至 Amazon ECS 叢集；否則， GuardDuty 附屬容器將附加到 Amazon ECS 任務中啟動的所有容器。

   在組態索引標籤下，選擇編輯。
6. 在自動化代理程式組態段落中選擇啟用所有帳號

   對於尚未排除的 Amazon ECS 叢集， GuardDuty 將管理附屬容器中安全代理程式的部署。
7. 選擇儲存。

Manage for selective (inclusion-only) Amazon ECS clusters (cluster level)

無論您選擇以何種方式啟用執行階段監控，下列步驟都可協助您監控組織中所有成員帳戶的選擇性 Amazon ECS Fargate 任務。

1. 請勿啟用 [自動化代理程式組態] 區段中的任何組態。保持「程式實際執行監督」組態與您在上一個步驟中選取的相同。
2. 選擇儲存。
3. 防止修改這些標籤，但受信任的實體除外。除了AWS Organizations 使用者指南中的授權原則外，「防止標籤被修改」中提供的原則已修改為適用於此處。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
```

```
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> 在 Amazon ECS 叢集使用包含標籤時，不需要明確啟用代理GuardDuty 程式自動管理。

啟用現有作用中成員帳戶的自動化代理程式

Manage for all Amazon ECS clusters (account level)

1. 您可以在「程式實際執行監督」頁面的「組態」頁籤底下，檢視自動化代理程式組態的目前狀態。
2. 在 [自動化代理程式組態] 窗格的 [作用中成員帳戶] 區段下，選擇 [動作]。
3. 從動作中選擇為所有現有作用中成員帳戶啟用。
4. 選擇確認。

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. 將標籤新增至此 Amazon ECS 叢集，其鍵值對為 `GuardDutyManaged-`。`false`
2. 防止對標籤進行修改，但受信任的實體除外。除了AWS Organizations 使用者指南中的授權原則外，「防止標籤被修改」中提供的原則已修改為適用於此處。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
```

```
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
```

```
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/
4. 在功能窗格中，選擇 [執行階段監視]。
5.

> **Note**
>
> 在為您的帳戶啟用自動化代理程式組態之前，請務必將排除標籤新增至 Amazon ECS 叢集；否則， GuardDuty 附屬容器將附加到 Amazon ECS 任務中啟動的所有容器。

   在 [組態] 索引標籤下的 [自動化代理程式組態] 區段的 [作用中成員帳戶] 下，選擇 [動作
6. 從動作中選擇為所有作用中成員帳戶啟用。

   對於尚未排除的 Amazon ECS 叢集， GuardDuty 將管理附屬容器中安全代理程式的部署。
7. 選擇確認。

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. 將標籤新增至您要包含所有任務的 Amazon ECS 叢集。鍵值對必須是 `GuardDutyManaged-true`。
2. 防止修改這些標籤，但受信任的實體除外。除了AWS Organizations 使用者指南中的授權原則外，「防止標籤被修改」中提供的原則已修改為適用於此處。

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

```
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
```

```
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> 在 Amazon ECS 叢集使用包含標籤時，不需要明確啟用自動化代理程式組態。

自動啟用新成員的自動代理程式組態

Manage for all Amazon ECS clusters (account level)

1. 在「程式實際執行監督」頁面上，選擇編輯來更新現有的組態。
2. 在「自動代理程式組態」區段中，選取「為新成員帳戶自動啟用」。
3. 選擇儲存。

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. 將標籤新增至此 Amazon ECS 叢集，其鍵值對為 `GuardDutyManaged-`。`false`

2. 防止對標籤進行修改，但受信任的實體除外。除了AWS Organizations 使用者指南中的授權原則外，「防止標籤被修改」中提供的原則已修改為適用於此處。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
```

```
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/
4. 在功能窗格中，選擇 [執行階段監視]。
5.

> **Note**
>
> 在為您的帳戶啟用自動化代理程式組態之前，請務必將排除標籤新增至 Amazon ECS 叢集；否則， GuardDuty 附屬容器將附加到 Amazon ECS 任務中啟動的所有容器。

在 [組態] 索引標籤下，選取 [自動化代理程式組態] 區段中的新成員帳戶自動啟用。

對於尚未排除的 Amazon ECS 叢集，GuardDuty 將管理附屬容器中安全代理程式的部署。

6. 選擇儲存。

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. 將標籤新增至您要包含所有任務的 Amazon ECS 叢集。鍵值對必須是 `GuardDutyManaged-true`。
2. 防止修改這些標籤，但受信任的實體除外。除了AWS Organizations 使用者指南中的[授權原則外，「防止標籤被修改」中提供的原則](#)已修改為適用於此處。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
```

```
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> 在 Amazon ECS 叢集使用包含標籤時，不需要明確啟用自動化代理程式組態。

選擇性地為作用中成員帳戶啟用自動化代理

Manage for all Amazon ECS (account level)

1. 在 [帳戶] 頁面上，選取您要啟用執行階段監視-自動代理程式組態 (ECS-Fargate) 的帳戶。您可以選擇多個帳戶。請確定您在此步驟中選取的帳戶已透過「執行階段監視」啟用。
2. 從 [編輯保護計畫] 中，選擇適當的選項以啟用執行階段監視-自動化代理程式組態 (EC S-Fargate)。
3. 選擇確認。

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. 將標籤新增至此 Amazon ECS 叢集，其鍵值對為 `GuardDutyManaged-。false`
2. 防止對標籤進行修改，但受信任的實體除外。除了AWS Organizations 使用者指南中的授權原則外，「防止標籤被修改」中提供的原則已修改為適用於此處。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
```

```
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
```

```
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/
4. 在功能窗格中，選擇 [執行階段監視]。
5.

> **Note**
>
> 在為您的帳戶啟用 GuardDuty 代理程式自動管理之前，請務必將排除標籤新增至 Amazon ECS 叢集；否則， GuardDuty附屬容器將附加到 Amazon ECS 任務中啟動的所有容器。

   在 [帳戶] 頁面上，選取您要啟用執行階段監視-自動代理程式組態 (ECS-Fargate) 的帳戶。您可以選擇多個帳戶。請確定您在此步驟中選取的帳戶已透過「執行階段監視」啟用。

   對於尚未排除的 Amazon ECS 叢集， GuardDuty 將管理附屬容器中安全代理程式的部署。
6. 從 [編輯保護計畫] 中，選擇適當的選項以啟用執行階段監視-自動化代理程式組態 (EC S-Fargate)。
7. 選擇儲存。

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. 請確定您沒有為擁有要監控之 Amazon ECS 叢集的所選帳戶啟用自動化代理程式組態 (或執行時期監控-自動代理程式組態 (ECS-Fargate))。
2. 將標籤新增至您要包含所有任務的 Amazon ECS 叢集。鍵值對必須是 `GuardDutyManaged-true`。
3. 防止修改這些標籤，但受信任的實體除外。除了AWS Organizations 使用者指南中的授權原則外，「防止標籤被修改」中提供的原則已修改為適用於此處。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
```

```
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> 在 Amazon ECS 叢集使用包含標籤時，不需要明確啟用自動化代理程式組態。

自動管理 Amazon EKS 叢集的安全代理程式

設定獨立帳戶的自動代理程式

1. 請登入 AWS Management Console 並開啟 GuardDuty 主控台，網址為 https://console.aws.amazon.com/guardduty/。
2. 在功能窗格中，選擇 [執行階段監視]。
3. 在 [組態] 索引標籤下，選擇 [啟用]，為您的帳戶啟用自動代理程式設定

部署 GuardDuty 安全代理程式的偏好方法	步驟
管理安全代理程式 GuardDuty (監控所有 EKS 叢集)	1. 在「自動化代理程式組態」段落中選擇啟用 GuardDuty 將管理您帳戶中所有現有和潛在新 EKS 叢集的安全代理程式的部署和更新。 2. 選擇儲存。

部署 GuardDuty 安全代理程式的偏好方法	步驟
監控所有 EKS 叢集，但排除其中一些叢集 (使用排除標籤)	請從下列程序中選擇其中一個適用於您的案例。 當尚未在此叢集上部署 GuardDuty 安全代理程式時，將 EKS 叢集排除在監視範圍之外 1. 為此 EKS 叢集加上標籤，且索引鍵為 `GuardDutyManaged` ，值為 `false`。 如需有關標記 Amazon EKS 叢集的詳細資訊，請參閱《Amazon EKS 使用者指南》中的透過主控台使用標籤。 2. 若要防止修改標籤 (僅允許信任的實體進行修改)，請使用《AWS Organizations 使用者指南》中防止標籤被授權主體以外的人員修改中提供的政策。在此政策中，請取代下列詳細資訊： • 將 *ec2#CreateTags* 替換為`eks:TagResource` 。 • 將 *ec2#DeleteTags* 替換為`eks:UntagResource` 。 • 使用 `GuardDutyManaged` 取代 *access-project* • 將 *AWS ## 123456789012* 取代為受信任實體的識別碼。 當不只有一個信任的實體時，使用下列範例來新增多個 `PrincipalArn` ： `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

部署 GuardDuty 安全代理程式的偏好方法	步驟
	3. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/ 4. 在功能窗格中，選擇 [執行階段監視]。 **Note** 在為您的帳戶啟用 GuardDuty 代理程式自動管理之前，請務必將排除標記新增至您的 EKS 叢集；否則， GuardDuty 安全性代理程式將部署到您帳戶中的所有 EKS 叢集上。 5. 在組態索引標籤下，選擇GuardDuty 代理程式管理區段中的啟用。 對於尚未從監視中排除的 EKS 叢集， GuardDuty 將管理 GuardDuty 安全代理程式的部署和更新。 6. 選擇儲存。 在 GuardDuty 安全性代理程式已部署到此叢集後，將 EKS 叢集排除在監視之外 1. 為此 EKS 叢集加上標籤，且索引鍵為 `GuardDuty Managed` ，值為 `false`。 如需有關標記 Amazon EKS 叢集的詳細資訊，請參閱《Amazon EKS 使用者指南》中的透過主控台使用標籤。 完成此步驟後， GuardDuty 將不會更新此叢集的安全性代理程式。不過，安全性代理程式將保持部署狀態，並 GuardDuty 繼續從此 EKS 叢集接收執行階段事件。這可能會影響您的用量統計資料。 2. 若要防止修改標籤 (僅允許信任的實體進行修改)，請使用《AWS Organizations 使用者指南》中防止標籤

部署 GuardDuty 安全代理程式的偏好方法	步驟
	被授權主體以外的人員修改中提供的政策。在此政策中，請取代下列詳細資訊： • 將 *ec2#CreateTags* 替換為eks:TagResource . • 將 *ec2#DeleteTags* 替換為eks:UntagResource . • 使用 GuardDutyManaged 取代 *access-project* • 將 *AWS ## 123456789012* 取代為受信任實體的識別碼。 當不只有一個信任的實體時，使用下列範例來新增多個 PrincipalArn ： `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. 若要停止接收此叢集的執行期事件，您必須從此 EKS 叢集中移除部署的安全代理程式。如需有關移除部署的安全代理程式的詳細資訊，請參閱停用及清理資源的影響。

部署 GuardDuty 安全代理程式的偏好方法	步驟
使用包含標籤監控選定 EKS 叢集	1. 請務必選擇 [自動化代理程式組態] 區段中的 [停用]。保持啟用執行階段監視。 2. 選擇儲存 3. 為此 EKS 叢集加上標籤，且索引鍵為 `GuardDuty Managed` ，值為 `true`。 如需有關標記 Amazon EKS 叢集的詳細資訊，請參閱《Amazon EKS 使用者指南》中的透過主控台使用標籤。 GuardDuty 將針對您要監視的選擇性 EKS 叢集，管理安全代理程式的部署和更新。 4. 若要防止修改標籤 (僅允許信任的實體進行修改)，請使用《AWS Organizations 使用者指南》中防止標籤被授權主體以外的人員修改中提供的政策。在此政策中，請取代下列詳細資訊： • 將 *ec2#CreateTags* 替換為`eks:TagResource` 。 • 將 *ec2#DeleteTags* 替換為`eks:UntagResource` 。 • 使用 `GuardDutyManaged` 取代 *access-project* • 將 *AWS ## 123456789012* 取代為受信任實體的識別碼。 當不只有一個信任的實體時，使用下列範例來新增多個 `PrincipalArn` ： `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:`

部署 GuardDuty 安全代理程式的偏好方法	步驟
	`iam::123456789012:role/org-admins/iam-admin"]`
手動管理代理程式	1. 請務必選擇 [自動化代理程式組態] 區段中的 [停用]。保持啟用執行階段監視。 2. 選擇儲存。 3. 若要管理安全代理程式，請參閱手動管理 Amazon EKS 叢集的安全代理程式。

為多帳戶環境設定自動化代理程式

在多帳戶環境中，只有委派的系統管理 GuardDuty 員帳戶可以啟用或停用成員帳戶的自動化代理程式組態，以及管理屬於其組織中成員帳戶的 EKS 叢集的自動化代理程式。成 GuardDuty 員帳戶無法從其帳戶修改此設定。委派的 GuardDuty 系統管理員帳戶會使用來管理其成員帳戶 AWS Organizations。如需有關多帳戶環境的詳細資訊，請參閱 Managing multiple accounts。

設定委派 GuardDuty 管理員帳戶的自動化代理程式

管理 GuardDuty安全代理程式的偏好方法	步驟
管理安全代理程式 GuardDuty (監控所有 EKS 叢集)	如果您在「執行階段監視」區段中選擇「針對所有帳戶啟用」，則有下列選項： • 在 [自動代理程式組態] 區段中選擇 [啟用所有帳戶]。 GuardDuty 將針對屬於委派 GuardDuty 系統管理員帳戶的所有 EKS 叢集，以及屬於組織中所有現有和可能新成員帳戶的所有 EKS 叢集部署和管理安全性代理程式。 • 選擇手動設定帳戶。 如果您在「執行階段監視」區段中選擇「手動設定帳戶」，請執行下列動作： 1. 在「自動化代理程式組態」區段中選擇「手動設定帳

管理 GuardDuty安全代理程式的偏好方法	步驟
	2. 在委派的 GuardDuty 系統管理員帳戶 (此帳戶) 區段中選擇 [啟用]。 選擇儲存。

管理 GuardDuty安全代理程式的偏好方法	步驟
監控所有 EKS 叢集，但排除其中一些叢集 (使用排除標籤)	請從下列程序中選擇其中一個適用於您的案例。 當尚未在此叢集上部署 GuardDuty安全代理程式時，將 EKS 叢集排除在監視範圍之外 1. 為此 EKS 叢集加上標籤，且索引鍵為 `GuardDutyManaged` ，值為 `false`。 如需有關標記 Amazon EKS 叢集的詳細資訊，請參閱《Amazon EKS 使用者指南》中的透過主控台使用標籤。 2. 若要防止修改標籤 (僅允許信任的實體進行修改)，請使用《AWS Organizations 使用者指南》中防止標籤被授權主體以外的人員修改中提供的政策。在此政策中，請取代下列詳細資訊： • 將 *ec2#CreateTags* 替換為`eks:TagResource` 。 • 將 *ec2#DeleteTags* 替換為`eks:UntagResource` 。 • 使用 `GuardDutyManaged` 取代 *access-project* • 將 *AWS ## 123456789012* 取代為受信任實體的識別碼。 當不只有一個信任的實體時，使用下列範例來新增多個 `PrincipalArn` ： `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/ 4. 在功能窗格中，選擇 [執行階段監視]。 **Note** 在為您的帳戶啟用 GuardDuty 代理程式自動管理之前，請務必將排除標記新增至您的 EKS 叢集；否則，

管理 GuardDuty安全代理程式的偏好方法	步驟
	GuardDuty 安全性代理程式將部署到您帳戶中的所有 EKS 叢集上。 5. 在組態索引標籤下，選擇GuardDuty 代理程式管理區段中的啟用。 對於尚未從監視中排除的 EKS 叢集， GuardDuty 將管理 GuardDuty 安全代理程式的部署和更新。 6. 選擇儲存。 將 EKS 叢集排除在此叢集上部署 GuardDuty安全代理程式時進行監視 1. 為此 EKS 叢集加上標籤，且索引鍵為 `GuardDutyManaged` ，值為 `false`。 如需有關標記 Amazon EKS 叢集的詳細資訊，請參閱《Amazon EKS 使用者指南》中的透過主控台使用標籤。 2. 若要防止修改標籤 (僅允許信任的實體進行修改)，請使用《AWS Organizations 使用者指南》中防止標籤被授權主體以外的人員修改中提供的政策。在此政策中，請取代下列詳細資訊： • 將 *ec2#CreateTags* 替換為`eks:TagResource` . • 將 *ec2#DeleteTags* 替換為`eks:UntagResource` . • 使用 `GuardDutyManaged` 取代 *access-project* • 將 *AWS ## 123456789012* 取代為受信任實體的識別碼。 當不只有一個信任的實體時，使用下列範例來新增多個 `PrincipalArn` ： `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

管理 GuardDuty安全代理程式的偏好方法	步驟
	3. 如果您已為此 EKS 叢集啟用自動化代理程式，則在此步驟之後，GuardDuty 將不會更新此叢集的安全性代理程式。不過，安全性代理程式將保持部署狀態，並 GuardDuty 繼續從此 EKS 叢集接收執行階段事件。這可能會影響您的用量統計資料。 若要停止接收此叢集的執行期事件，您必須從此 EKS 叢集中移除部署的安全代理程式。如需有關移除部署的安全代理程式的詳細資訊，請參閱停用及清理資源的影響 4. 如果您手動管理此 EKS 叢集的 GuardDuty 安全性代理程式，請參閱停用及清理資源的影響。

管理 GuardDuty安全代理程式的偏好方法	步驟
使用包含標籤監控選定 EKS 叢集	無論您選擇以何種方式啟用執行階段監視，下列步驟都能協助您監視帳戶中的選擇性 EKS 叢集： 1. 請務必在 [自動化代 GuardDuty 理程式組態] 區段中選擇 [停用委派的系統管理員帳戶 (此帳戶)]。保持「執行時期監視」組態與上一個步驟中所設定的相同。 2. 選擇儲存。 3. 為您的 EKS 叢集加上標籤，且索引鍵為 `GuardDuty Managed` ，值為 `true`。 如需有關標記 Amazon EKS 叢集的詳細資訊，請參閱《Amazon EKS 使用者指南》中的透過主控台使用標籤。 GuardDuty 將針對您要監視的選擇性 EKS 叢集，管理安全代理程式的部署和更新。 4. 若要防止修改標籤 (僅允許信任的實體進行修改)，請使用《AWS Organizations 使用者指南》中防止標籤被授權主體以外的人員修改中提供的政策。在此政策中，請取代下列詳細資訊： • 將 *ec2#CreateTags* 替換為`eks:TagResource` . • 將 *ec2#DeleteTags* 替換為`eks:UntagResource` . • 使用 `GuardDutyManaged` 取代 *access-project* • 將 *AWS ## 123456789012* 取代為受信任實體的識別碼。 當不只有一個信任的實體時，使用下列範例來新增多個 `PrincipalArn` ： `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

管理 GuardDuty安全代理程式的偏好方法	步驟
手動管理 GuardDuty 安全代理程式	無論您選擇如何啟用執行階段監視，都可以手動管理 EKS 叢集的安全性代理程式。 1. 請務必在 [自動化代 GuardDuty 理程式組態] 區段中選擇 [停用委派的系統管理員帳戶 (此帳戶)]。保持「執行時期監視」組態與上一個步驟中所設定的相同。 2. 選擇儲存。 3. 若要管理安全代理程式，請參閱手動管理 Amazon EKS 叢集的安全代理程式。

自動啟用所有成員帳戶的自動代理

> **Note**
>
> 最多可能需要 24 小時才會更新成員帳戶的組態。

管理 GuardDuty安全代理程式的偏好方法	步驟
管理安全代理程式 GuardDuty (監控所有 EKS 叢集)	本主題是為所有成員帳戶啟用執行階段監視，因此，下列步驟假設您必須在 [執行時期監視] 區段中選擇 [啟用所有帳戶]。 1. 在 [自動代理程式組態] 區段中選擇 [啟用所有帳戶]。 GuardDuty 將針對屬於委派 GuardDuty 系統管理員帳戶的所有 EKS 叢集，以及屬於組織中所有現有和可能新成員帳戶的所有 EKS 叢集部署和管理安全性代理程式。 2. 選擇儲存。
監控所有 EKS 叢集，但排除其中一些叢集 (使用排除標籤)	請從下列程序中選擇其中一個適用於您的案例。

管理 GuardDuty安全代理程式的偏好方法	步驟
	當尚未在此叢集上部署 GuardDuty安全代理程式時，將 EKS 叢集排除在監視範圍之外 1. 為此 EKS 叢集加上標籤，且索引鍵為 `GuardDutyManaged` ，值為 `false`。 如需有關標記 Amazon EKS 叢集的詳細資訊，請參閱《Amazon EKS 使用者指南》中的透過主控台使用標籤。 2. 若要防止修改標籤 (僅允許信任的實體進行修改)，請使用《AWS Organizations 使用者指南》中防止標籤被授權主體以外的人員修改中提供的政策。在此政策中，請取代下列詳細資訊： • 將 *ec2#CreateTags* 替換為`eks:TagResource` . • 將 *ec2#DeleteTags* 替換為`eks:UntagResource` . • 使用 `GuardDutyManaged` 取代 *access-project* • 將 *AWS ## 123456789012* 取代為受信任實體的識別碼。 當不只有一個信任的實體時，使用下列範例來新增多個 `PrincipalArn` ： `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/ 4. 在功能窗格中，選擇 [執行階段監視]。 **Note** 在為您的帳戶啟用自動化代理程式之前，請務必將排除標記新增至您的 EKS 叢集；否則， GuardDuty 安全性代理程式將部署到您帳戶中的所有 EKS 叢集上。

管理 GuardDuty安全代理程式的偏好方法	步驟
	5. 在「組態」索引標籤下，選擇「執行時期監督」組態區段中的編輯 6. 在 [自動代理程式組態] 區段中選擇 [啟用所有帳戶]。對於尚未從監視中排除的 EKS 叢集， GuardDuty 將管理 GuardDuty 安全代理程式的部署和更新。 7. 選擇儲存。 將 EKS 叢集排除在此叢集上部署 GuardDuty安全代理程式時進行監視 1. 為此 EKS 叢集加上標籤，且索引鍵為 `GuardDutyManaged` ，值為 `false`。 如需有關標記 Amazon EKS 叢集的詳細資訊，請參閱《Amazon EKS 使用者指南》中的透過主控台使用標籤。 2. 如果您已為此 EKS 叢集啟用自動化代理程式組態，則在此步驟之後， GuardDuty 將不會更新此叢集的安全性代理程式。不過，安全性代理程式將保持部署狀態，並 GuardDuty 繼續從此 EKS 叢集接收執行階段事件。這可能會影響您的用量統計資料。 若要停止接收此叢集的執行期事件，您必須從此 EKS 叢集中移除部署的安全代理程式。如需有關移除部署的安全代理程式的詳細資訊，請參閱停用及清理資源的影響 3. 若要防止修改標籤 (僅允許信任的實體進行修改)，請使用《AWS Organizations 使用者指南》中防止標籤被授權主體以外的人員修改中提供的政策。在此政策中，請取代下列詳細資訊： • 將 *`ec2#CreateTags`* 替換為`eks:TagResource` . • 將 *`ec2#DeleteTags`* 替換為`eks:UntagResource` . • 使用 `GuardDutyManaged` 取代 *`access-project`* • 將 *`AWS ## 123456789012`* 取代為受信任實體的識別碼。 當不只有一個信任的實體時，使用下列範例來新增多個 `PrincipalArn` ：

管理 GuardDuty安全代理程式的偏好方法	步驟

	<pre>"aws:PrincipalArn":["arn:aws:iam::12345678901
	2:role/org-admins/iam-admin", "arn:aws:iam::1234
	56789012:role/org-admins/iam-admin", "arn:aws:
	iam::123456789012:role/org-admins/iam-admin"]</pre>
	4. 如果您手動管理此 EKS 叢集的 GuardDuty 安全性代理程式，請參閱停用及清理資源的影響。

管理 GuardDuty安全代理程式的偏好方法	步驟
使用包含標籤監控選定 EKS 叢集	無論您選擇如何啟用執行階段監視，下列步驟都可協助您監視組織中所有成員帳戶的選擇性 EKS 叢集： 1. 請勿啟用 [自動化代理程式組態] 區段中的任何組態。保持「執行時期監視」組態與上一個步驟中所設定的相同。 2. 選擇儲存。 3. 為您的 EKS 叢集加上標籤，且索引鍵為 `GuardDuty Managed` ，值為 `true`。 如需有關標記 Amazon EKS 叢集的詳細資訊，請參閱《Amazon EKS 使用者指南》中的透過主控台使用標籤。 GuardDuty 將針對您要監視的選擇性 EKS 叢集，管理安全代理程式的部署和更新。 4. 若要防止修改標籤 (僅允許信任的實體進行修改)，請使用《AWS Organizations 使用者指南》中防止標籤被授權主體以外的人員修改中提供的政策。在此政策中，請取代下列詳細資訊： • 將 *ec2#CreateTags* 替換為`eks:TagResource` 。 • 將 *ec2#DeleteTags* 替換為`eks:UntagResource` 。 • 使用 `GuardDutyManaged` 取代 *access-project* • 將 *AWS ## 123456789012* 取代為受信任實體的識別碼。 當不只有一個信任的實體時，使用下列範例來新增多個 `PrincipalArn` ： `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

管理 GuardDuty安全代理程式的偏好方法	步驟
手動管理 GuardDuty 安全代理程式	無論您選擇如何啟用執行階段監視，都可以手動管理 EKS 叢集的安全性代理程式。 1. 請勿啟用 [自動化代理程式組態] 區段中的任何組態。保持「執行時期監視」組態與上一個步驟中所設定的相同。 2. 選擇儲存。 3. 若要管理安全代理程式，請參閱手動管理 Amazon EKS 叢集的安全代理程式。

為所有現有活躍成員帳戶啟用自動代理

> **Note**
>
> 最多可能需要 24 小時才會更新成員帳戶的組態。

管理組織中現有作用中成員帳戶的 GuardDuty 安全性代理程式

- GuardDuty 若要從屬於組織中現有作用中成員帳戶的 EKS 叢集接收執行階段事件，您必須選擇偏好的方法來管理這些 EKS 叢集的 GuardDuty 安全性代理程式。如需有關各方法的詳細資訊，請參閱管理 GuardDuty安全代理程式的方法。

管理 GuardDuty 安全代理程式的偏好方法	步驟
管理安全代理程式 GuardDuty (監控所有 EKS 叢集)	監控所有現有作用中成員帳戶的所有 EKS 叢集 1. 您可以在「程式實際執行監督」頁面的「組態」頁籤底下，檢視自動化代理程式組態的目前狀態。 2. 在 [自動化代理程式組態] 窗格的 [作用中成員帳戶] 區段下，選擇 [動作]。 3. 從動作中選擇為所有現有作用中成員帳戶啟用。 4. 選擇確認。

管理 GuardDuty 安全代理程式的偏好方法	步驟
監控所有 EKS 叢集，但排除其中一些叢集 (使用排除標籤)	請從下列程序中選擇其中一個適用於您的案例。 當尚未在此叢集上部署 GuardDuty 安全代理程式時，將 EKS 叢集排除在監視範圍之外 1. 為此 EKS 叢集加上標籤，且索引鍵為 `GuardDutyManaged` ，值為 `false`。 如需有關標記 Amazon EKS 叢集的詳細資訊，請參閱《Amazon EKS 使用者指南》中的透過主控台使用標籤。 2. 若要防止修改標籤 (僅允許信任的實體進行修改)，請使用《AWS Organizations 使用者指南》中防止標籤被授權主體以外的人員修改中提供的政策。在此政策中，請取代下列詳細資訊： • 將 *ec2#CreateTags* 替換為`eks:TagResource` 。 • 將 *ec2#DeleteTags* 替換為`eks:UntagResource` 。 • 使用 `GuardDutyManaged` 取代 *access-project* • 將 *AWS ## 123456789012* 取代為受信任實體的識別碼。 當不只有一個信任的實體時，使用下列範例來新增多個 `PrincipalArn` ： `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

管理 GuardDuty 安全代理程式的偏好方法	步驟
	3. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/ 4. 在功能窗格中，選擇 [執行階段監視]。 **Note** 在為您的帳戶啟用自動化代理程式組態之前，請務必將排除標記新增至您的 EKS 叢集；否則， GuardDuty 安全性代理程式將部署到您帳戶中的所有 EKS 叢集上。 5. 在 [組態] 索引標籤下的 [自動化代理程式組態] 窗格的 [作用中成員帳戶] 下，選擇 [動作 6. 從動作中選擇為所有作用中成員帳戶啟用。 7. 選擇確認。 在 GuardDuty 安全性代理程式已部署到此叢集後，將 EKS 叢集排除在監視之外 1. 為此 EKS 叢集加上標籤，且索引鍵為 `GuardDuty Managed` ，值為 `false`。 如需有關標記 Amazon EKS 叢集的詳細資訊，請參閱《Amazon EKS 使用者指南》中的透過主控台使用標籤。 完成此步驟後， GuardDuty 將不會更新此叢集的安全性代理程式。不過，安全性代理程式將保持部署狀態，並 GuardDuty 繼續從此 EKS 叢集接收執行階段事件。這可能會影響您的用量統計資料。 2. 若要防止修改標籤 (僅允許信任的實體進行修改)，請使用《AWS Organizations 使用者指南》中防止標籤被授權主體以外的人員修改中提供的政策。在此政策中，請取代下列詳細資訊：

管理 GuardDuty 安全代理程式的偏好方法	步驟
	• 將 *ec2#CreateTags* 替換為eks:TagResource 。 • 將 *ec2#DeleteTags* 替換為eks:UntagResource 。 • 使用 GuardDutyManaged 取代 *access-project* • 將 *AWS ## 123456789012* 取代為受信任實體的識別碼。 當不只有一個信任的實體時，使用下列範例來新增多個 PrincipalArn ： `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. 無論您是透過 GuardDuty 或手動管理安全代理程式的方式，若要停止從此叢集接收執行階段事件，您必須從此 EKS 叢集移除已部署的安全代理程式。如需有關移除部署的安全代理程式的詳細資訊，請參閱停用及清理資源的影響。

管理 GuardDuty 安全代理程式的偏好方法	步驟
使用包含標籤監控選定 EKS 叢集	1. 在 [帳戶] 頁面上，啟用 [執行階段監視] 之後，請勿啟用執行階段監視-自動化代理程式組態。 2. 將標籤新增至屬於您要監控之所選帳戶的 EKS 叢集。標籤的鍵值對必須是 `GuardDutyManaged -true`。 如需有關標記 Amazon EKS 叢集的詳細資訊，請參閱《Amazon EKS 使用者指南》中的透過主控台使用標籤。 GuardDuty 將針對您要監視的選擇性 EKS 叢集，管理安全代理程式的部署和更新。 3. 若要防止修改標籤 (僅允許信任的實體進行修改)，請使用《AWS Organizations 使用者指南》中防止標籤被授權主體以外的人員修改中提供的政策。在此政策中，請取代下列詳細資訊： • 將 *ec2#CreateTags* 替換為`eks:TagResource`。 • 將 *ec2#DeleteTags* 替換為`eks:UntagResource`。 • 使用 `GuardDutyManaged` 取代 *access-project* • 將 *AWS ## 123456789012* 取代為受信任實體的識別碼。 當不只有一個信任的實體時，使用下列範例來新增多個 `PrincipalArn`： `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

管理 GuardDuty 安全代理程式的偏好方法	步驟
手動管理 GuardDuty 安全代理程式	1. 請確定您未在 [自動化代理程式設定] 區段中選擇 [啟用]。保持啟用執行階段監視。 2. 選擇儲存。 3. 若要管理安全代理程式，請參閱手動管理 Amazon EKS 叢集的安全代理程式。

為新成員自動啟用自動代理程式組態

管理 GuardDuty安全代理程式的偏好方法	步驟
管理安全代理程式 GuardDuty (監控所有 EKS 叢集)	1. 在「程式實際執行監督」頁面上，選擇編輯來更新現有的組態。 2. 在「自動代理程式組態」區段中，選取「為新成員帳戶自動啟用」。 3. 選擇儲存。
監控所有 EKS 叢集，但排除其中一些叢集 (使用排除標籤)	請從下列程序中選擇其中一個適用於您的案例。 當尚未在此叢集上部署 GuardDuty安全代理程式時，將 EKS 叢集排除在監視範圍之外 1. 為此 EKS 叢集加上標籤，且索引鍵為 `GuardDuty Managed` ，值為 `false`。 如需有關標記 Amazon EKS 叢集的詳細資訊，請參閱《Amazon EKS 使用者指南》中的透過主控台使用標籤。 2. 若要防止修改標籤 (僅允許信任的實體進行修改)，請使用《AWS Organizations 使用者指南》中防止標籤被授權主體以外的人員修改中提供的政策。在此政策中，請取代下列詳細資訊： • 將 *ec2#CreateTags* 替換為`eks:TagResource` .

管理 GuardDuty安全代理程式的偏好方法	步驟
	• 將 *ec2#DeleteTags* 替換為eks:Untag Resource 。 • 使用 GuardDutyManaged 取代 *access-project* • 將 *AWS ## 123456789012* 取代為受信任實體的識別碼。 當不只有一個信任的實體時，使用下列範例來新增多個 PrincipalArn ： `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/ 4. 在功能窗格中，選擇 [執行階段監視]。 **Note** 在為您的帳戶啟用自動化代理程式組態之前，請務必將排除標記新增至您的 EKS 叢集；否則，GuardDuty 安全性代理程式將部署到您帳戶中的所有 EKS 叢集上。 5. 在 [組態] 索引標籤下，選取 [GuardDuty 代理程式管理] 區段中的新成員帳戶自動啟用。 對於尚未從監視中排除的 EKS 叢集， GuardDuty 將管理 GuardDuty 安全代理程式的部署和更新。 6. 選擇儲存。

管理 GuardDuty安全代理程式的偏好方法	步驟
	將 EKS 叢集排除在此叢集上部署 GuardDuty安全代理程式時進行監視 1. 無論您是透過 GuardDuty 還是手動管理 GuardDuty 安全代理程式，請在此 EKS 叢集中新增標籤，其金鑰為`GuardDutyManaged` ，其值為`false`。 如需有關標記 Amazon EKS 叢集的詳細資訊，請參閱《Amazon EKS 使用者指南》中的透過主控台使用標籤。 如果您已為此 EKS 叢集啟用自動化代理程式，則在此步驟之後， GuardDuty 將不會更新此叢集的安全性代理程式。不過，安全性代理程式將保持部署狀態，並 GuardDuty 繼續從此 EKS 叢集接收執行階段事件。這可能會影響您的用量統計資料。 若要停止接收此叢集的執行期事件，您必須從此 EKS 叢集中移除部署的安全代理程式。如需有關移除部署的安全代理程式的詳細資訊，請參閱停用及清理資源的影響 2. 若要防止修改標籤 (僅允許信任的實體進行修改)，請使用《AWS Organizations 使用者指南》中防止標籤被授權主體以外的人員修改中提供的政策。在此政策中，請取代下列詳細資訊： • 將 *ec2#CreateTags* 替換為`eks:TagResource` . • 將 *ec2#DeleteTags* 替換為`eks:Untag Resource` . • 使用 `GuardDutyManaged` 取代 *access-project* • 將 *AWS ## 123456789012* 取代為受信任實體的識別碼。 當不只有一個信任的實體時，使用下列範例來新增多個 `PrincipalArn` ：

管理 GuardDuty安全代理程式的偏好方法	步驟
	<pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> 3. 如果您手動管理此 EKS 叢集的 GuardDuty 安全性代理程式，請參閱停用及清理資源的影響。

管理 GuardDuty安全代理程式的偏好方法	步驟
使用包含標籤監控選定 EKS 叢集	無論您選擇以何種方式啟用執行階段監視，下列步驟都可協助您監控組織中新成員帳戶的選擇性 EKS 叢集。 1. 請務必清除 [自動化代理程式設定] 區段中的 [為新成員帳戶自動啟用]。保持「執行時期監視」組態與上一個步驟中所設定的相同。 2. 選擇儲存。 3. 為您的 EKS 叢集加上標籤，且索引鍵為 `GuardDuty Managed` ，值為 `true`。 如需有關標記 Amazon EKS 叢集的詳細資訊，請參閱《Amazon EKS 使用者指南》中的透過主控台使用標籤。 GuardDuty 將針對您要監視的選擇性 EKS 叢集，管理安全代理程式的部署和更新。 4. 若要防止修改標籤 (僅允許信任的實體進行修改)，請使用《AWS Organizations 使用者指南》中防止標籤被授權主體以外的人員修改中提供的政策。在此政策中，請取代下列詳細資訊： • 將 *ec2#CreateTags* 替換為`eks:TagResource` 。 • 將 *ec2#DeleteTags* 替換為`eks:UntagResource` 。 • 使用 `GuardDutyManaged` 取代 *access-project* • 將 *AWS ## 123456789012* 取代為受信任實體的識別碼。 當不只有一個信任的實體時，使用下列範例來新增多個 `PrincipalArn` ： `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin`

管理 GuardDuty安全代理程式的偏好方法	步驟
	", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]
手動管理 GuardDuty 安全代理程式	無論您選擇如何啟用執行階段監視，都可以手動管理 EKS 叢集的安全性代理程式。 1. 請務必在 [自動化代理程式設定] 區段中清除 [為新成員帳戶自動啟用] 核取方塊。保持「執行時期監視」組態與上一個步驟中所設定的相同。 2. 選擇儲存。 3. 若要管理安全代理程式，請參閱手動管理 Amazon EKS 叢集的安全代理程式。

選擇性地為作用中成員帳戶設定自動化

管理 GuardDuty安全代理程式的偏好方法	步驟
管理安全代理程式 GuardDuty (監控所有 EKS 叢集)	1. 在 [帳戶] 頁面上，選取要啟用自動化代理程式組態的帳戶。您可以一次選擇多個帳戶。請確定您在此步驟中選擇的帳戶已啟用 EKS 執行期監控。 2. 從編輯保護方案中選擇適當的選項以啟用執行階段監視-自動化代理程式組態。 3. 選擇確認。
監控所有 EKS 叢集，但排除其中一些叢集 (使用排除標籤)	請從下列程序中選擇其中一個適用於您的案例。 當尚未在此叢集上部署 GuardDuty安全代理程式時，將 EKS 叢集排除在監視範圍之外 1. 為此 EKS 叢集加上標籤，且索引鍵為 `GuardDutyManaged` ，值為 `false`。

管理 GuardDuty安全代理程式的偏好方法	步驟
	如需有關標記 Amazon EKS 叢集的詳細資訊，請參閱《Amazon EKS 使用者指南》中的透過主控台使用標籤。 2. 若要防止修改標籤 (僅允許信任的實體進行修改)，請使用《AWS Organizations 使用者指南》中防止標籤被授權主體以外的人員修改中提供的政策。在此政策中，請取代下列詳細資訊： • 將 *ec2#CreateTags* 替換為eks:TagResource . • 將 *ec2#DeleteTags* 替換為eks:UntagResource . • 使用 GuardDutyManaged 取代 *access-project* • 將 *AWS ## 123456789012* 取代為受信任實體的識別碼。 當不只有一個信任的實體時，使用下列範例來新增多個 PrincipalArn ： `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/ **Note** 在為您的帳戶啟用自動化代理程式組態之前，請務必將排除標記新增至您的 EKS 叢集；否則， GuardDuty 安全性代理程式將部署到您帳戶中的所有 EKS 叢集上。 4. 在「帳戶」頁面上，選擇您要啟用自動管理代理程式的帳戶。您可以一次選擇多個帳戶。 5. 從 [編輯保護方案] 中，選擇適當的選項，以針對所選帳戶啟用 [執行階段監視-自動代理程式組態] 對於尚未從監視中排除的 EKS 叢集， GuardDuty 將管理 GuardDuty 安全代理程式的部署和更新。

管理 GuardDuty安全代理程式的偏好方法	步驟
	6. 選擇儲存。 將 EKS 叢集排除在此叢集上部署 GuardDuty安全代理程式時進行監視 1. 為此 EKS 叢集加上標籤，且索引鍵為 `GuardDutyManaged` ，值為 `false`。 如需有關標記 Amazon EKS 叢集的詳細資訊，請參閱《Amazon EKS 使用者指南》中的透過主控台使用標籤。 如果您先前已為此 EKS 叢集啟用自動化代理程式組態，則在此步驟之後， GuardDuty 將不會更新此叢集的安全性代理程式。不過，安全性代理程式將保持部署狀態，並 GuardDuty 繼續從此 EKS 叢集接收執行階段事件。這可能會影響您的用量統計資料。 若要停止接收此叢集的執行期事件，您必須從此 EKS 叢集中移除部署的安全代理程式。如需有關移除部署的安全代理程式的詳細資訊，請參閱停用及清理資源的影響 2. 若要防止修改標籤 (僅允許信任的實體進行修改)，請使用《AWS Organizations 使用者指南》中防止標籤被授權主體以外的人員修改中提供的政策。在此政策中，請取代下列詳細資訊： • 將 *ec2#CreateTags* 替換為`eks:TagResource` 。 • 將 *ec2#DeleteTags* 替換為`eks:UntagResource` 。 • 使用 `GuardDutyManaged` 取代 *access-project* • 將 *AWS ## 123456789012* 取代為受信任實體的識別碼。 當不只有一個信任的實體時，使用下列範例來新增多個 `PrincipalArn` ： `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

管理 GuardDuty安全代理程式的偏好方法	步驟
	3. 如果您要手動管理此 EKS 叢集的 GuardDuty 安全性代理程式，則必須將其移除。如需詳細資訊，請參閱 停用及清理資源的影響。
使用包含標籤監控選定 EKS 叢集	無論您選擇以何種方式啟用執行階段監視，下列步驟都可協助您監視屬於所選帳戶的選擇性 EKS 叢集： 1. 請確定您未針對具有要監視之 EKS 叢集的所選帳戶啟用「執行時期監視-自動化代理程式」組態。 2. 為您的 EKS 叢集加上標籤，且索引鍵為 `GuardDuty Managed` ，值為 `true`。 如需有關標記 Amazon EKS 叢集的詳細資訊，請參閱《Amazon EKS 使用者指南》中的透過主控台使用標籤。 新增標籤之後， GuardDuty 將管理您要監視之選擇性 EKS 叢集的安全代理程式部署和更新。 3. 若要防止修改標籤 (僅允許信任的實體進行修改)，請使用《AWS Organizations 使用者指南》中防止標籤被授權主體以外的人員修改中提供的政策。在此政策中，請取代下列詳細資訊： • 將 *ec2#CreateTags* 替換為`eks:TagResource` . • 將 *ec2#DeleteTags* 替換為`eks:UntagResource` . • 使用 `GuardDutyManaged` 取代 *access-project* • 將 *AWS ## 123456789012* 取代為受信任實體的識別碼。 當不只有一個信任的實體時，使用下列範例來新增多個 `PrincipalArn` ： `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

管理 GuardDuty安全代理程式的偏好方法	步驟
手動管理 GuardDuty 安全代理程式	1. 保持「執行時期監視」組態與上一個步驟中所設定的相同。請確定您未針對任何選取的帳戶啟用執行階段監控-自動化代理程式組態。 2. 選擇確認。 3. 若要管理安全代理程式，請參閱手動管理 Amazon EKS 叢集的安全代理程式。

手動管理 Amazon EKS 叢集的安全代理程式

本節說明啟用執行階段監控後，如何管理 Amazon EKS 附加元件GuardDuty 代理程式 (代理程式)。若要使用執行階段監控，您必須啟用執行階段監控並設定 Amazon EKS 附加元件。`aws-guardduty-agent`僅執行這兩個步驟之一，將無法協助 GuardDuty 偵測潛在威脅或產生發現項目。

部署 GuardDuty 安全代理程式的必要

本節說明手動為 EKS 叢集部署 GuardDuty 安全性代理程式的必要條件。在繼續之前，請確保您已經為您的帳戶配置了運行時監控。如果您未設定執行階段監視， GuardDuty 安全性代理程式 (EKS 附加元件) 將無法運作。如需詳細資訊，請參閱 啟用 GuardDuty 執行期監視。完成下列步驟之後，請參閱部署 GuardDuty 安全代理。

選擇您偏好的存取方法以建立 Amazon VPC 端點。

Console

建立 VPC 端點

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中的虛擬私有雲端下，選擇端點。
3. 選擇建立端點。
4. 在建立端點頁面上，為服務類別選擇其他端點服務。
5. 對於服務名稱，輸入 **`com.amazonaws.`*`us-east-1`*`.guardduty-data`**。

   請務必使用正確的區域取代 *`us-east-1`*。這必須與屬於您 AWS 帳戶 ID 的 EKS 叢集所在的區域相同。

6. 選擇驗證服務。
7. 成功驗證服務名稱後，選擇叢集所在的 VPC。新增下列策略，以將 VPC 端點用量限制為僅限指定帳戶。您可以透過本政策下方提供的組織 Condition，更新下列政策以限制對端點的存取權限。若要為組織中的特定帳戶 ID 提供 VPC 端點支援，請參閱Organization condition to restrict access to your endpoint。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Action": "*",
   "Resource": "*",
   "Effect": "Allow",
   "Principal": "*"
  },
  {
   "Condition": {
    "StringNotEquals": {
     "aws:PrincipalAccount": "111122223333"
    }
   },
   "Action": "*",
   "Resource": "*",
   "Effect": "Deny",
   "Principal": "*"
  }
 ]
}
```

aws:PrincipalAccount 帳戶 ID 必須符合包含 VPC 和 VPC 端點的帳戶。下列清單顯示如何與其他 AWS 帳戶 ID 共用 VPC 端點：

限制端點存取的組織條件

- 若要指定可存取 VPC 端點的多個帳戶，請使用下列項目取代 "aws:PrincipalAccount": "111122223333"：

```
"aws:PrincipalAccount": [
          "666666666666",
          "555555555555"
    ]
```

- 若要允許組織中的所有成員存取 VPC 端點，請使用下列項目取代 `"aws:PrincipalAccount": "111122223333"`：

```
"aws:PrincipalOrgID": "o-abcdef0123"
```

- 若要限制存取組織 ID 的資源，請將您的 `ResourceOrgID` 新增至該政策。

  如需詳細資訊，請參閱 ResourceOrgID。

```
"aws:ResourceOrgID": "o-abcdef0123"
```

8. 在其他設定下方，選擇啟用 DNS 名稱。
9. 在子網路下方，選擇叢集所在的子網路。
10. 在安全群組下方，選擇擁有從您的 VPC (或 EKS 叢集) 啟用之輸入連接埠 443 的安全群組。如果您尚未擁有已啟用輸入連接埠 443 的安全群組，則建立安全群組。

    如果在限制 VPC (或叢集) 的輸入許可時發生問題，請為來自任何 IP 地址 (`0.0.0.0/0`) 的輸入 443 連接埠提供支援。

API/CLI

- 調用CreateVpcEndpoint。
- 使用下列值做為參數：
  - 對於服務名稱，輸入 **com.amazonaws.*us-east-1*.guardduty-data**。

    請務必使用正確的區域取代 *us-east-1*。這必須與屬於您 AWS 帳戶 ID 的 EKS 叢集所在的區域相同。
  - 對於 DNSOptions，請將它設定為 `true`，以啟用私有 DNS 選項。
- 對於 AWS Command Line Interface，請參閱create-vpc-endpoint。

設定 Amazon EKS 的 GuardDuty 安全代理程式 (附加元件) 參數

您可以為 Amazon EKS 設定 GuardDuty 安全代理程式的特定參數。此支援適用於 GuardDuty 安全代理程式版本 1.5.0 及更新版本。如需最新附加元件版本的資訊，請參閱GuardDuty Amazon EKS 叢集的安全代理程式。

為什麼要更新安全代理程式設定結構描述

Amazon EKS 叢集中所有容器的 GuardDuty 安全代理程式組態結構描述相同。如果預設值與相關聯的工作負載和執行個體大小不一致，請考慮設定 CPU 設定、記憶體設定和`dnsPolicy`設定。`PriorityClass`無論您如何管理 Amazon EKS 叢集的 GuardDuty 代理程式，都可以設定或更新這些參數的現有組態。

使用已設定參數的自動化代理程式

代表您 GuardDuty 管理安全性代理程式 (EKS 附加元件) 時，會視需要更新附加元件。 GuardDuty 會將可配置參數的值設定為預設值。但是，您仍然可以將參數更新為所需的值。如果這會導致衝突，解決衝突的預設選項為。None

可配置的參數和值

如需設定附加元件參數之步驟的相關資訊，請參閱：

- 部署 GuardDuty 安全代理 或
- 手動更新安全代理

下表提供可用於手動部署 Amazon EKS 附加元件或更新現有附加元件設定的範圍和值。

CPU 設定

參數	預設值	可配置範圍
請求	200 m	二百米至一萬米之間，均包括在內
限制	1000 m	

記憶體設定

參數	預設值	可配置範圍
請求	二百六海	256 米至 200 英里之間，均包括在內
限制	一百二十米	

`PriorityClass` 設定

為您 GuardDuty 創建一個 Amazon EKS 附加組件時，分配的`PriorityClass`是`aws-guardduty-agent.priorityclass`。這表示不會根據代理程式網繭的優先順序採取任何動作。您可以選擇下列其中一個選`PriorityClass`項來設定此附加元件參數：

可配置 **PriorityClass**	**preemptionPolicy** 值	**preemptionPolicy** 描述	網繭值
`aws-guardduty-agent.priorityclass`	`Never`	無動作	1000000
`aws-guardduty-agent.priorityclass-high`	`PreemptLowerPriority`	指派此值將會預佔優先順序值低於代理程式網繭值的網繭。	100000000
`system-cluster-critical` [1]	`PreemptLowerPriority`		2000000000
`system-node-critical` [1]	`PreemptLowerPriority`		2000001000

[1] 庫伯尼特提供這兩個`PriorityClass`選項 — 和. `system-cluster-critical` `system-node-critical` 如需詳細資訊，請參閱 Kubernetes 文件PriorityClass中的。

`dnsPolicy` 設定

選擇下列其中一個支援的 DNS 原則選項。如果未指定任何組態，`ClusterFirst`則會用作預設值。

- `ClusterFirst`
- `ClusterFirstWithHostNet`
- `Default`

如需這些原則的相關資訊，請參閱 Kubernetes 說明文件中的網繭的 DNS 原則。

部署 GuardDuty 安全代理

本節說明如何首次為特定 EKS 叢集部署 GuardDuty 安全代理程式。在繼續執行本節之前，請確定您已設定必要條件並為您的帳戶啟用「執行階段監視」。如果您未啟用執行階段監視， GuardDuty安全性代理程式 (EKS 附加元件) 將無法運作。

選擇您偏好的存取方法，以首次部署 GuardDuty Security Agent。

Console

1. 在以下網址開啟 Amazon EKS 主控台：https://console.aws.amazon.com/eks/home#/clusters。
2. 選擇您的叢集名稱。
3. 選擇附加元件索引標籤。
4. 選擇取得更多附加元件。
5. 在 [選取附加元件] 頁面上，選擇 Amazon GuardDuty 執行階段監控。
6. 在設定選取的附加元件設定頁面上，使用預設設定。如果 EKS 附加元件的 [狀態] 為 [需要啟用]，請選擇 [啟用 GuardDuty]。這個動作會開啟 GuardDuty 主控台，為您的帳戶設定執行階段監控。
7. 為帳戶設定執行階段監控之後，請切換回 Amazon EKS 主控台。EKS 附加元件的狀態應已變更為可立即安裝。
8. (選擇性) 提供 EKS 附加元件組態結構描述

   對於附加版本，如果您選擇 v1.5.0 及更高版本，執行階段監控支援設定代理程式的特定參數。GuardDuty 如需有關參數範圍的資訊，請參閱設定 EKS 附加元件參數。

   a. 展開選擇性組態設定以檢視可設定的參數及其預期值和格式。
   b. 設定參數。這些值必須在中提供的範圍內設定 EKS 附加元件參數。
   c. 選擇 [儲存變更]，根據進階設定建立附加元件。
   d. 對於衝突解決方法，當您將參數值更新為非預設值時，將使用您選擇的選項來解決衝突。如需有關所列選項的詳細資訊，請參閱 Amazon E KS API 參考中的解決衝突。
9. 選擇下一步。
10. 在檢閱和建立頁面上，確認所有詳細資訊，然後選擇建立。
11. 導覽回叢集詳細資訊，然後選擇資源索引標籤。
12. 您可以使用前置詞檢視新網繭aws-guardduty-agent。

API/CLI

您可以使用下列任一選項來設定 Amazon EKS 附加元件代理程式 (aws-guardduty-agent)：

- CreateAddon為您的帳戶運行。
-

> **Note**
>
> 對於附加元件version，如果您選擇 v1.5.0 及更新版本，執行階段監視支援設定代理程式的特定參數。 GuardDuty 如需詳細資訊，請參閱 設定 EKS 附加元件參數。

使用下列值作為請求參數：

- 針對 addonName，請輸入 aws-guardduty-agent。

  當使用附加元件 v1.5.0 及更新版本支援的可設定值時，您可以使用下列 AWS CLI 範例。請務必取代以紅色反白顯示的預留位置值，以及Example.json與設定值相關聯的預留位置值。

```
aws eks create-addon --region us-east-1 --cluster-name myClusterName --addon-
name aws-guardduty-agent --addon-version v1.5.0-eksbuild.1 --configuration-
values 'file://example.json'
```

  Example 示例

```
{
 "priorityClassName": "aws-guardduty-agent.priorityclass-high",
 "dnsPolicy": "Default",
 "resources": {
  "requests": {
   "cpu": "237m",
   "memory": "512Mi"
  },
  "limits": {
   "cpu": "2000m",
   "memory": "2048Mi"
  }
 }
}
```

- 如需有關支援的 addonVersion 的資訊，請參閱安全性代理程式支援的 Kubernetes 版本 GuardDuty 。

- 或者，您可以使用 AWS CLI. 如需詳細資訊，請參閱建立附加元件。

手動更新安全代理

當您手動管理 GuardDuty 安全代理程式時，您有責任為您的帳戶更新安全代理程式。如需有關新代理程式版本的通知，您可以訂閱 RSS 摘要GuardDuty 代理程式發行歷。

您可以將安全代理程式更新為最新版本，以便從新增的支援和改進中獲益。如果您目前的代理程式版本已到達標準支援的終止，則若要繼續使用執行階段監視 (或 EKS 執行階段監控)，您必須更新目前的代理程式版本。如需有關發行版本的資訊，請參閱GuardDuty Amazon EKS 叢集的安全代理程式。

必要條件

在您更新安全性代理程式版本之前，請確定您目前打算使用的代理程式版本與您的 Kubernetes 版本相容。如需詳細資訊，請參閱 安全性代理程式支援的 Kubernetes 版本 GuardDuty 。

Console

1. 在以下網址開啟 Amazon EKS 主控台：https://console.aws.amazon.com/eks/home#/clusters。
2. 選擇您的叢集名稱。
3. 選擇附加元件。
4. 在附加元件下，選取GuardDuty執行階段監控
5. 選擇編輯以更新代理程式詳細資訊。
6. 在「設定 GuardDuty 執行階段監視」頁面上，更新詳細資料。
7. (選擇性) 更新附加元件組態參數

   如果您的 EKS 附加元件版本為 1.5.0 或更新版本，您也可以更新附加元件組態設定。

   a. 展開選擇性組態設定以檢視組態結構描述。
   b. 根據中提供的範圍更新參數值設定 EKS 附加元件參數。
   c. 選擇儲存變更以開始更新。
   d. 對於衝突解決方法，當您將參數值更新為非預設值時，將使用您選擇的選項來解決衝突。如需有關所列選項的詳細資訊，請參閱 Amazon E KS API 參考中的解決衝突。

API/CLI

若要更新 Amazon EKS 叢集的 GuardDuty 安全代理程式，請參閱更新附加元件。

> **Note**
>
> 對於附加元件version，如果您選擇 v1.5.0 及更新版本，執行階段監視支援設定代理程式的特定參數。 GuardDuty 如需有關參數範圍的資訊，請參閱設定 EKS 附加元件參數。

當使用附加元件 v1.5.0 及更新版本支援的可設定值時，您可以使用下列 AWS CLI 範例。請務必取代以紅色反白顯示的預留位置值，以及Example.json與設定值相關聯的預留位置值。

```
aws eks update-addon --region us-east-1 --cluster-name myClusterName --addon-
name aws-guardduty-agent --addon-version v1.5.0-eksbuild.1 --configuration-
values 'file://example.json'
```

Example 示例

```
{
 "priorityClassName": "aws-guardduty-agent.priorityclass-high",
 "dnsPolicy": "Default",
 "resources": {
  "requests": {
   "cpu": "237m",
   "memory": "512Mi"
  },
  "limits": {
   "cpu": "2000m",
   "memory": "2048Mi"
  }
 }
}
```

如果 Amazon EKS 附加元件版本為 1.5.0 或更新版本，且您已設定附加元件結構描述，則可以驗證叢集的值是否正確顯示。如需詳細資訊，請參閱 驗證組態架構更新。

驗證組態架構更新

設定完參數之後，請執行下列步驟來確認組態結構描述是否已更新：

1. 在以下網址開啟 Amazon EKS 主控台：https://console.aws.amazon.com/eks/home#/clusters。
2. 在導覽窗格中，選擇叢集。
3. 在 [叢集] 頁面上，選取您要驗證更新的叢集名稱。
4. 選擇 Resources (資源) 標籤。
5. 從 [資源類型] 窗格的 [工作負載] 下，選擇DaemonSets。
6. 選取 aws-guardduty-agent。
7. 在aws-guardduty-agent頁面上，選擇 [原始檢視] 以檢視未格式化的 JSON 回應。確認可配置參數是否顯示您提供的值。

確認之後，請切換至主 GuardDuty 控台。選取對應的， AWS 區域 然後檢視 Amazon EKS 叢集的涵蓋範圍狀態。如需詳細資訊，請參閱 Amazon EKS 叢集的涵蓋範圍。

設定 EKS 執行階段監控 (僅限 API)

在帳戶中設定 EKS 執行期監控前，請確定您正在使用已驗證平台之一，且該平台支援目前正在使用的 Kubernetes 版本。如需更多資訊，請參閱 驗證架構需求。

設定獨立帳戶的 EKS 執行期監控

如果是與 AWS Organizations 相關聯的帳戶，請參閱設定多帳戶環境的 EKS 執行期監控。

選擇您偏好的存取方式，以啟用您帳戶的 EKS 執行期監控。

API/CLI

根據 管理 GuardDuty安全代理程式的方法，您可以選擇偏好的方法，並依照下表所述的步驟進行。

管理 GuardDuty 安全代理程式的偏好方法	步驟
透過管理安全代理程式 GuardDuty (監視所有 EKS 叢集)	1. 使用您的區域偵測器 ID，並將 `features` 物件名稱作為 `EKS_RUNTIME_MONITORING` 來以 `ENABLED` 狀態傳遞，進而執行 updateDetector API。 將 `EKS_ADDON_MANAGEMENT` 的狀態設定為 `ENABLED`。

管理 GuardDuty 安全代理程式的偏好方法	步驟
	GuardDuty 將管理您帳戶中所有 Amazon EKS 叢集的安全代理程式部署和更新。 2. 或者，您可以使用自己的區域檢測器 ID 來使用該 AWS CLI 命令。要查找您`detectorId` 的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。 下列範例會啟用 `EKS_RUNTIME_MONITORING` 和 `EKS_ADDON_MANAGEMENT` ： `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'`

管理 GuardDuty 安全代理程式的偏好方法	步驟
監控所有 EKS 叢集，但排除其中一些叢集 (使用排除標籤)	1. 為您要排除監控的 EKS 叢集加上標籤。鍵值對為 `GuardDutyManaged -false`。如需有關新增標籤的詳細資訊，請參閱《Amazon EKS 使用者指南》中的透過 CLI、API 或 eksctl 使用標籤。 2. 若要防止修改標籤 (僅允許信任的實體進行修改)，請使用《AWS Organizations 使用者指南》中防止標籤被授權主體以外的人員修改中提供的政策。在此政策中，請取代下列詳細資訊： • 將 *ec2#CreateTags* 替換為`eks:TagResource` . • 將 *ec2#DeleteTags* 替換為`eks:UntagResource` . • 使用 `GuardDutyManaged` 取代 *access-project* • 將 *AWS ## 123456789012* 取代為受信任實體的識別碼。 當不只有一個信任的實體時，使用下列範例來新增多個 `PrincipalArn` ： `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. **Note** 在將的設定為之前，請務必將排除標籤新增`EKS_RUNTIME_MONITORING` 至您的 `STATUS` EKS 叢集`ENABLED`；否則，GuardDuty 安全性代理程式將部署到您帳戶中的所有 EKS 叢集上。

管理 GuardDuty 安全代理程式的偏好方法	步驟
	使用您的區域偵測器 ID，並將 `features` 物件名稱作為 `EKS_RUNTIME_MONITORING` 來以 `ENABLED` 狀態傳遞，進而執行 updateDetector API。 將 `EKS_ADDON_MANAGEMENT` 的狀態設定為 `ENABLED`。 GuardDuty 將管理尚未排除在受監控之外的所有 Amazon EKS 叢集的安全代理程式部署和更新。 或者，您可以使用自己的區域檢測器 ID 來使用該 AWS CLI 命令。要查找您`detectorId` 的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。 下列範例會啟用 `EKS_RUNTIME_MONITORING` 和 `EKS_ADDON_MANAGEMENT` ： `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'`

管理 GuardDuty 安全代理程式的偏好方法	步驟
監控選定 EKS 叢集 (使用包含標籤)	1. 為您要排除監控的 EKS 叢集加上標籤。鍵值對為 GuardDutyManaged -true。如需有關新增標籤的詳細資訊，請參閱《Amazon EKS 使用者指南》中的透過 CLI、API 或 eksctl 使用標籤。 2. 若要防止修改標籤 (僅允許信任的實體進行修改)，請使用《AWS Organizations 使用者指南》中防止標籤被授權主體以外的人員修改中提供的政策。在此政策中，請取代下列詳細資訊： • 將 *ec2#CreateTags* 替換為eks:TagResource . • 將 *ec2#DeleteTags* 替換為eks:UntagResource . • 使用 GuardDutyManaged 取代 *access-project* • 將 *AWS ## 123456789012* 取代為受信任實體的識別碼。 當不只有一個信任的實體時，使用下列範例來新增多個 PrincipalArn ： `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. 使用您的區域偵測器 ID，並將 features 物件名稱作為 EKS_RUNTIME_MONITORING 來以 ENABLED 狀態傳遞，進而執行 updateDetector API。 將 EKS_ADDON_MANAGEMENT 的狀態設定為 DISABLED。

管理 GuardDuty 安全代理程式的偏好方法	步驟
	GuardDuty 將管理已標記為 GuardDuty Managed -true 對之所有 Amazon EKS 叢集的安全代理程式的部署和更新。 或者，您可以使用自己的區域檢測器 ID 來使用該 AWS CLI 命令。要查找您detectorId 的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。 下列範例會啟用 EKS_RUNTIME_MONITORING 並停用 EKS_ADDON_MANAGEMENT ： `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'`

管理 GuardDuty 安全代理程式的偏好方法	步驟
手動管理安全代理程式	1. 使用您的區域偵測器 ID，並將 `features` 物件名稱作為 `EKS_RUNTIME_MONITORING` 來以 `ENABLED` 狀態傳遞，進而執行 updateDetector API。 將 `EKS_ADDON_MANAGEMENT` 的狀態設定為 `DISABLED`。 或者，您可以使用自己的區域檢測器 ID 來使用該 AWS CLI 命令。要查找您`detectorId` 的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。 下列範例會啟用 `EKS_RUNTIME_MONITORING` 並停用 `EKS_ADDON_MANAGEMENT` ： `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'` 2. 若要管理安全代理程式，請參閱手動管理 Amazon EKS 叢集的安全代理程式。

設定多帳戶環境的 EKS 執行期監控

在多帳戶環境中，只有委派的系統管理 GuardDuty 員帳戶可以啟用或停用成員帳戶的 EKS 執行階段監視，以及管 GuardDuty 理屬於其組織中成員帳戶的 EKS 叢集的代理程式管理。成 GuardDuty 員帳戶無法從其帳戶修改此設定。委派的 GuardDuty 系統管理員帳戶會使用來管理其成員帳戶 AWS Organizations。如需有關多帳戶環境的詳細資訊，請參閱 Managing multiple accounts。

為委派的 GuardDuty 管理員帳戶設定 EKS 執行階段監視

選擇您偏好的存取方法，以啟用 EKS 執行階段監視，並管理屬於委派 GuardDuty 系統管理員帳戶之 EKS 叢集的 GuardDuty安全性代理程式。

API/CLI

根據 管理 GuardDuty安全代理程式的方法，您可以選擇偏好的方法，並依照下表所述的步驟進行。

管理 GuardDuty 安全代理程式的偏好方法	步驟
透過管理安全代理程式 GuardDuty (監視所有 EKS 叢集)	使用您的區域偵測器 ID，並將 `features` 物件名稱作為 `EKS_RUNTIME_MONITORING` 來以 `ENABLED` 狀態傳遞，進而執行 updateDetector API。 將 `EKS_ADDON_MANAGEMENT` 的狀態設定為 `ENABLED`。 GuardDuty 將管理您帳戶中所有 Amazon EKS 叢集的安全代理程式部署和更新。 或者，您可以使用自己的區域檢測器 ID 來使用該 AWS CLI 命令。要查找您`detectorId` 的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。 下列範例會啟用 `EKS_RUNTIME_MONITORING` 和 `EKS_ADDON_MANAGEMENT` ： `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] ]'`
監控所有 EKS 叢集，但排除其中一些叢集 (使用排除標籤)	1. 為您要排除監控的 EKS 叢集加上標籤。鍵值對為 `GuardDutyManaged -false`。如需有關新增標籤的詳細資訊，請參閱《Amazon EKS 使用者指南》中的透過 CLI、API 或 eksctl 使用標籤。 2. 若要防止修改標籤 (僅允許信任的實體進行修改)，請使用《AWS Organizations 使用者指南》中防止標籤

管理 GuardDuty 安全代理程式的偏好方法	步驟
	被授權主體以外的人員修改中提供的政策。在此政策中，請取代下列詳細資訊： • 將 *ec2#CreateTags* 替換為eks:TagResource . • 將 *ec2#DeleteTags* 替換為eks:UntagResource . • 使用 GuardDutyManaged 取代 *access-project* • 將 *AWS ## 123456789012* 取代為受信任實體的識別碼。 當不只有一個信任的實體時，使用下列範例來新增多個 PrincipalArn ： `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. **Note** 在將的設定為之前，請務必將排除標籤新增EKS_RUNTIME_MONITORING 至您的 STATUS EKS 叢集ENABLED；否則，GuardDuty 安全性代理程式將部署到您帳戶中的所有 EKS 叢集上。 使用您的區域偵測器 ID，並將 features 物件名稱作為 EKS_RUNTIME_MONITORING 來以 ENABLED 狀態傳遞，進而執行 updateDetector API。

管理 GuardDuty 安全代理程式的偏好方法	步驟
	將 EKS_ADDON_MANAGEMENT 的狀態設定為 ENABLED。 GuardDuty 將管理尚未排除在受監控之外的所有 Amazon EKS 叢集的安全代理程式部署和更新。 或者，您可以使用自己的區域檢測器 ID 來使用該 AWS CLI 命令。要查找您detectorId 的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。 下列範例會啟用 EKS_RUNTIME_MONITORING 和 EKS_ADDON_MANAGEMENT ： `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'`

管理 GuardDuty 安全代理程式的偏好方法	步驟
監控選定 EKS 叢集 (使用包含標籤)	1. 為您要排除監控的 EKS 叢集加上標籤。鍵值對為 GuardDutyManaged -true。如需有關新增標籤的詳細資訊，請參閱《Amazon EKS 使用者指南》中的透過 CLI、API 或 eksctl 使用標籤。 2. 若要防止修改標籤 (僅允許信任的實體進行修改)，請使用《AWS Organizations 使用者指南》中防止標籤被授權主體以外的人員修改中提供的政策。在此政策中，請取代下列詳細資訊： • 將 *ec2#CreateTags* 替換為eks:TagResource . • 將 *ec2#DeleteTags* 替換為eks:UntagResource . • 使用 GuardDutyManaged 取代 *access-project* • 將 *AWS ## 123456789012* 取代為受信任實體的識別碼。 當不只有一個信任的實體時，使用下列範例來新增多個 PrincipalArn ： `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. 使用您的區域偵測器 ID，並將 features 物件名稱作為 EKS_RUNTIME_MONITORING 來以 ENABLED 狀態傳遞，進而執行 updateDetector API。 將 EKS_ADDON_MANAGEMENT 的狀態設定為 DISABLED。

管理 GuardDuty 安全代理程式的偏好方法	步驟
	GuardDuty 將管理已標記為 GuardDuty Managed -true 對之所有 Amazon EKS 叢集的安全代理程式的部署和更新。 或者，您可以使用自己的區域檢測器 ID 來使用該 AWS CLI 命令。要查找您detectorId 的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。 下列範例會啟用 EKS_RUNTIME_MONITORING 並停用 EKS_ADDON_MANAGEMENT ： `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'`

管理 GuardDuty 安全代理程式的偏好方法	步驟
手動管理安全代理程式	1. 使用您的區域偵測器 ID，並將 `features` 物件名稱作為 `EKS_RUNTIME_MONITORING` 來以 `ENABLED` 狀態傳遞，進而執行 updateDetector API。 將 `EKS_ADDON_MANAGEMENT` 的狀態設定為 `DISABLED`。 或者，您可以使用自己的區域檢測器 ID 來使用該 AWS CLI 命令。要查找您`detectorId` 的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。 下列範例會啟用 `EKS_RUNTIME_MONITORING` 並停用 `EKS_ADDON_MANAGEMENT` ： `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] }]'` 2. 若要管理安全代理程式，請參閱手動管理 Amazon EKS 叢集的安全代理程式。

為所有成員帳戶自動啟用 EKS 執行期監控

選擇您偏好的存取方式，為所有成員帳戶啟用 EKS 執行期監控。這包括委派的 GuardDuty 系統管理員帳戶、現有成員帳戶，以及加入組織的新帳戶。選擇您偏好的方法來管理屬於這些成員帳戶的 EKS 叢集的 GuardDuty 安全性代理程式。

API/CLI

根據 管理 GuardDuty安全代理程式的方法，您可以選擇偏好的方法，並依照下表所述的步驟進行。

管理 GuardDuty 安全代理程式的偏好方法	步驟
透過管理安全代理程式 GuardDuty (監視所有 EKS 叢集)	若要為您的成員帳戶選擇性地啟用 EKS 執行期監控，請使用您自己的### *ID* 執行 updateMemberDetectors API 操作。 將 EKS_ADDON_MANAGEMENT 的狀態設定為 ENABLED。 GuardDuty 將管理您帳戶中所有 Amazon EKS 叢集的安全代理程式部署和更新。 或者，您可以使用自己的區域檢測器 ID 來使用該 AWS CLI 命令。要查找您detectorId 的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。 下列範例會啟用 EKS_RUNTIME_MONITORING 和 EKS_ADDON_MANAGEMENT ： `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] ]'` **Note** 您也可以傳遞以空格分隔的帳戶 ID 清單。 當程式碼成功執行時，會返回一個空白 UnprocessedAccounts 清單。如果變更帳戶的偵測器設定時發生任何問題，則會列出該帳戶 ID 以及問題摘要。
監控所有 EKS 叢集，但排除其中一些叢集 (使用排除標籤)	1. 為您要排除監控的 EKS 叢集加上標籤。鍵值對為 GuardDutyManaged -false。如需有關新增標籤的詳細資訊，請參閱《Amazon EKS 使用者指南》中的透過 CLI、API 或 eksctl 使用標籤。

管理 GuardDuty 安全代理程式的偏好方法	步驟
	2. 若要防止修改標籤 (僅允許信任的實體進行修改)，請使用《AWS Organizations 使用者指南》中防止標籤被授權主體以外的人員修改中提供的政策。在此政策中，請取代下列詳細資訊： • 將 *ec2#CreateTags* 替換為eks:TagResource . • 將 *ec2#DeleteTags* 替換為eks:UntagResource . • 使用 GuardDutyManaged 取代 *access-project* • 將 *AWS ## 123456789012* 取代為受信任實體的識別碼。 當不只有一個信任的實體時，使用下列範例來新增多個 PrincipalArn ： `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. **Note** 在將的設定為之前，請務必將排除標籤新增EKS_RUNTIME_MONITORING 至您的 STATUS EKS 叢集ENABLED；否則， GuardDuty 安全性代理程式將部署到您帳戶中的所有 EKS 叢集上。 使用您的區域偵測器 ID，並將 features 物件名稱作為 EKS_RUNTIME_MONITORING 來以 ENABLED 狀態傳遞，進而執行 updateDetector API。 將 EKS_ADDON_MANAGEMENT 的狀態設定為 ENABLED。 GuardDuty 將管理尚未排除在受監控之外的所有 Amazon EKS 叢集的安全代理程式部署和更新。

管理 GuardDuty 安全代理程式的偏好方法	步驟
	或者，您可以使用自己的區域檢測器 ID 來使用該 AWS CLI 命令。要查找您detectorId 的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。 下列範例會啟用 EKS_RUNTIME_MONITORING 和 EKS_ADDON_MANAGEMENT ： `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'` **Note** 您也可以傳遞以空格分隔的帳戶 ID 清單。 當程式碼成功執行時，會返回一個空白 UnprocessedAccounts 清單。如果變更帳戶的偵測器設定時發生任何問題，則會列出該帳戶 ID 以及問題摘要。

管理 GuardDuty 安全代理程式的偏好方法	步驟
監控選定 EKS 叢集 (使用包含標籤)	1. 為您要排除監控的 EKS 叢集加上標籤。鍵值對為 GuardDutyManaged -true。如需有關新增標籤的詳細資訊，請參閱《Amazon EKS 使用者指南》中的透過 CLI、API 或 eksctl 使用標籤。 2. 若要防止修改標籤 (僅允許信任的實體進行修改)，請使用《AWS Organizations 使用者指南》中防止標籤被授權主體以外的人員修改中提供的政策。在此政策中，請取代下列詳細資訊： • 將 *ec2#CreateTags* 替換為eks:TagResource . • 將 *ec2#DeleteTags* 替換為eks:UntagResource . • 使用 GuardDutyManaged 取代 *access-project* • 將 *AWS ## 123456789012* 取代為受信任實體的識別碼。 當不只有一個信任的實體時，使用下列範例來新增多個 PrincipalArn ： `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. 使用您的區域偵測器 ID，並將 features 物件名稱作為 EKS_RUNTIME_MONITORING 來以 ENABLED 狀態傳遞，進而執行 updateDetector API。 將 EKS_ADDON_MANAGEMENT 的狀態設定為 DISABLED。 GuardDuty 將管理已標記為 GuardDutyManaged -true 對之所有 Amazon EKS 叢集的安全代理程式的部署和更新。 或者，您可以使用自己的區域檢測器 ID 來使用該 AWS CLI 命令。要查找您detectorId 的帳戶和當前區域的，請參閱

管理 GuardDuty 安全代理程式的偏好方法	步驟
	https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。 下列範例會啟用 EKS_RUNTIME_MONITORING 並停用 EKS_ADDON_MANAGEMENT : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'` **Note** 您也可以傳遞以空格分隔的帳戶 ID 清單。 當程式碼成功執行時，會返回一個空白 UnprocessedAccounts 清單。如果變更帳戶的偵測器設定時發生任何問題，則會列出該帳戶 ID 以及問題摘要。

管理 GuardDuty 安全代理程式的偏好方法	步驟
手動管理安全代理程式	1. 使用您的區域偵測器 ID，並將 `features` 物件名稱作為 `EKS_RUNTIME_MONITORING` 來以 `ENABLED` 狀態傳遞，進而執行 updateDetector API。 將 `EKS_ADDON_MANAGEMENT` 的狀態設定為 `DISABLED`。 或者，您可以使用自己的區域檢測器 ID 來使用該 AWS CLI 命令。要查找您`detectorId` 的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。 下列範例會啟用 `EKS_RUNTIME_MONITORING` 並停用 `EKS_ADDON_MANAGEMENT` ： `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] } ]'` 2. 若要管理安全代理程式，請參閱手動管理 Amazon EKS 叢集的安全代理程式。

為所有現有作用中成員帳戶設定 EKS 執行期監控

選擇您偏好的存取方法，以啟用 EKS 執行階段監控，並管理組織中現有作用中成員帳戶的 GuardDuty 安全性代理程式。

API/CLI

根據 管理 GuardDuty安全代理程式的方法，您可以選擇偏好的方法，並依照下表所述的步驟進行。

管理 GuardDuty 安全代理程式的偏好方法	步驟
透過管理安全代理程式 GuardDuty (監視所有 EKS 叢集)	若要為您的成員帳戶選擇性地啟用 EKS 執行期監控，請使用您自己的### *ID* 執行 updateMemberDetectors API 操作。 將 EKS_ADDON_MANAGEMENT 的狀態設定為 ENABLED。 GuardDuty 將管理您帳戶中所有 Amazon EKS 叢集的安全代理程式部署和更新。 或者，您可以使用自己的區域檢測器 ID 來使用該 AWS CLI 命令。要查找您detectorId 的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。 下列範例會啟用 EKS_RUNTIME_MONITORING 和 EKS_ADDON_MANAGEMENT ： `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] ]'` **Note** 您也可以傳遞以空格分隔的帳戶 ID 清單。 當程式碼成功執行時，會返回一個空白 UnprocessedAccounts 清單。如果變更帳戶的偵測器設定時發生任何問題，則會列出該帳戶 ID 以及問題摘要。
監控所有 EKS 叢集，但排除其中一些叢集 (使用排除標籤)	1. 為您要排除監控的 EKS 叢集加上標籤。鍵值對為 GuardDutyManaged -false。如需有關新增標籤的詳細資訊，請參閱《Amazon EKS 使用者指南》中的透過 CLI、API 或 eksctl 使用標籤。

管理 GuardDuty 安全代理程式的偏好方法	步驟
	2. 若要防止修改標籤 (僅允許信任的實體進行修改)，請使用《AWS Organizations 使用者指南》中防止標籤被授權主體以外的人員修改中提供的政策。在此政策中，請取代下列詳細資訊： • 將 *ec2#CreateTags* 替換為eks:TagResource 。 • 將 *ec2#DeleteTags* 替換為eks:UntagResource 。 • 使用 GuardDutyManaged 取代 *access-project* • 將 *AWS ## 123456789012* 取代為受信任實體的識別碼。 當不只有一個信任的實體時，使用下列範例來新增多個 PrincipalArn ： `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. **Note** 在將的設定為之前，請務必將排除標籤新增EKS_RUNTIME_MONITORING 至您的 STATUS EKS 叢集ENABLED；否則， GuardDuty 安全性代理程式將部署到您帳戶中的所有 EKS 叢集上。 若要為您的成員帳戶選擇性地啟用 EKS 執行期監控，請使用您自己的*### ID* 執行 updateMemberDetectors API 操作。 將 EKS_ADDON_MANAGEMENT 的狀態設定為 ENABLED。 GuardDuty 將管理尚未排除在受監控之外的所有 Amazon EKS 叢集的安全代理程式部署和更新。

管理 GuardDuty 安全代理程式的偏好方法	步驟
	或者，您可以使用自己的區域檢測器 ID 來使用該 AWS CLI 命令。要查找您detectorId 的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。 下列範例會啟用 EKS_RUNTIME_MONITORING 和 EKS_ADDON_MANAGEMENT ： `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'` **Note** 您也可以傳遞以空格分隔的帳戶 ID 清單。 當程式碼成功執行時，會返回一個空白 UnprocessedAccounts 清單。如果變更帳戶的偵測器設定時發生任何問題，則會列出該帳戶 ID 以及問題摘要。

管理 GuardDuty 安全代理程式的偏好方法	步驟
監控選定 EKS 叢集 (使用包含標籤)	1. 為您要排除監控的 EKS 叢集加上標籤。鍵值對為 GuardDuty Managed -true。如需有關新增標籤的詳細資訊，請參閱《Amazon EKS 使用者指南》中的透過 CLI、API 或 eksctl 使用標籤。 2. 若要防止修改標籤 (僅允許信任的實體進行修改)，請使用《AWS Organizations 使用者指南》中防止標籤被授權主體以外的人員修改中提供的政策。在此政策中，請取代下列詳細資訊： • 將 *ec2#CreateTags* 替換為eks:TagResource . • 將 *ec2#DeleteTags* 替換為eks:UntagResource . • 使用 GuardDutyManaged 取代 *access-project* • 將 *AWS ## 123456789012* 取代為受信任實體的識別碼。 當不只有一個信任的實體時，使用下列範例來新增多個 PrincipalArn ： `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. 若要為您的成員帳戶選擇性地啟用 EKS 執行期監控，請使用您自己的*### ID* 執行 updateMemberDetectors API 操作。 將 EKS_ADDON_MANAGEMENT 的狀態設定為 DISABLED。 GuardDuty 將管理已標記為 GuardDutyManaged -true 對之所有 Amazon EKS 叢集的安全代理程式的部署和更新。 或者，您可以使用自己的區域檢測器 ID 來使用該 AWS CLI 命令。要查找您detectorId 的帳戶和當前區域的，請參閱

管理 GuardDuty 安全代理程式的偏好方法	步驟
	https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。 下列範例會啟用 EKS_RUNTIME_MONITORING 並停用 EKS_ADDON_MANAGEMENT : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'` **Note** 您也可以傳遞以空格分隔的帳戶 ID 清單。 當程式碼成功執行時，會返回一個空白 UnprocessedAccounts 清單。如果變更帳戶的偵測器設定時發生任何問題，則會列出該帳戶 ID 以及問題摘要。

管理 GuardDuty 安全代理程式的偏好方法	步驟
手動管理安全代理程式	1. 若要為您的成員帳戶選擇性地啟用 EKS 執行期監控，請使用您自己的### *ID* 執行 updateMemberDetectors API 操作。 將 EKS_ADDON_MANAGEMENT 的狀態設定為 DISABLED。 或者，您可以使用自己的區域檢測器 ID 來使用該 AWS CLI 命令。要查找您detectorId 的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。 下列範例會啟用 EKS_RUNTIME_MONITORING 並停用 EKS_ADDON_MANAGEMENT ： `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] } ]'` 2. 若要管理安全代理程式，請參閱手動管理 Amazon EKS 叢集的安全代理程式。

為新成員自動啟用 EKS 執行期監控

委派的系統管理 GuardDuty 員帳戶可以自動啟用 EKS 執行階段監控，並選擇如何管理加入組織之新帳戶的 GuardDuty 安全性代理程式的方法。

API/CLI

根據 管理 GuardDuty安全代理程式的方法，您可以選擇偏好的方法，並依照下表所述的步驟進行。

管理 GuardDuty 安全代理程式的偏好方法	步驟
透過管理安全代理程式 GuardDuty (監視所有 EKS 叢集)	若要為您的新帳戶選擇性地啟用 EKS 執行期監控，請使用您自己的*### ID* 調用 UpdateOrganizationConfiguration API 操作。 將 EKS_ADDON_MANAGEMENT 的狀態設定為 ENABLED。 GuardDuty 將管理您帳戶中所有 Amazon EKS 叢集的安全代理程式部署和更新。 或者，您可以使用自己的區域檢測器 ID 來使用該 AWS CLI 命令。要查找您detectorId 的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。 下列範例會為單一帳戶啟用 EKS_ADDON_MANAGEMENT 和 EKS_RUNTIME_MONITORING 。您也可以傳遞以空格分隔的帳戶 ID 清單。 要查找您detectorId 的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。 `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] ]'` 當程式碼成功執行時，會返回一個空白 UnprocessedAccounts 清單。如果變更帳戶的偵測器設定時發生任何問題，則會列出該帳戶 ID 以及問題摘要。

管理 GuardDuty 安全代理程式的偏好方法	步驟
監控所有 EKS 叢集，但排除其中一些叢集 (使用排除標籤)	1. 為您要排除監控的 EKS 叢集加上標籤。鍵值對為 `GuardDutyManaged -false`。如需有關新增標籤的詳細資訊，請參閱《Amazon EKS 使用者指南》中的透過 CLI、API 或 eksctl 使用標籤。 2. 若要防止修改標籤 (僅允許信任的實體進行修改)，請使用《AWS Organizations 使用者指南》中防止標籤被授權主體以外的人員修改中提供的政策。在此政策中，請取代下列詳細資訊： • 將 *ec2#CreateTags* 替換為`eks:TagResource` 。 • 將 *ec2#DeleteTags* 替換為`eks:UntagResource` 。 • 使用 `GuardDutyManaged` 取代 *access-project* • 將 *AWS ## 123456789012* 取代為受信任實體的識別碼。 當不只有一個信任的實體時，使用下列範例來新增多個 `PrincipalArn` ： `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. **Note** 在將的設定為之前，請務必將排除標籤新增`EKS_RUNTIME_MONITORING` 至您的 `STATUS` EKS 叢集`ENABLED`；否則，GuardDuty 安全性代理程式將部署到您帳戶中的所有 EKS 叢集上。

管理 GuardDuty 安全代理程式的偏好方法	步驟
	若要為您的新帳戶選擇性地啟用 EKS 執行期監控，請使用您自己的*### ID* 調用 UpdateOrganizationConfiguration API 操作。 將 EKS_ADDON_MANAGEMENT 的狀態設定為 ENABLED。 GuardDuty 將管理尚未排除在受監控之外的所有 Amazon EKS 叢集的安全代理程式部署和更新。 或者，您可以使用自己的區域檢測器 ID 來使用該 AWS CLI 命令。要查找您detectorId 的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。 下列範例會為單一帳戶啟用 EKS_ADDON_MANAGEMENT 和 EKS_RUNTIME_MONITORING 。您也可以傳遞以空格分隔的帳戶 ID 清單。 要查找您detectorId 的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。 `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] ]'` 當程式碼成功執行時，會返回一個空白 UnprocessedAccounts 清單。如果變更帳戶的偵測器設定時發生任何問題，則會列出該帳戶 ID 以及問題摘要。

管理 GuardDuty 安全代理程式的偏好方法	步驟
監控選定 EKS 叢集 (使用包含標籤)	1. 為您要排除監控的 EKS 叢集加上標籤。鍵值對為 GuardDutyManaged -true。如需有關新增標籤的詳細資訊，請參閱《Amazon EKS 使用者指南》中的透過 CLI、API 或 eksctl 使用標籤。 2. 若要防止修改標籤 (僅允許信任的實體進行修改)，請使用《AWS Organizations 使用者指南》中防止標籤被授權主體以外的人員修改中提供的政策。在此政策中，請取代下列詳細資訊： • 將 *ec2#CreateTags* 替換為eks:TagResource . • 將 *ec2#DeleteTags* 替換為eks:UntagResource . • 使用 GuardDutyManaged 取代 *access-project* • 將 *AWS ## 123456789012* 取代為受信任實體的識別碼。 當不只有一個信任的實體時，使用下列範例來新增多個 PrincipalArn ： `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. 若要為您的新帳戶選擇性地啟用 EKS 執行期監控，請使用您自己的*### ID* 調用 UpdateOrganizationConfiguration API 操作。 將 EKS_ADDON_MANAGEMENT 的狀態設定為 DISABLED。

管理 GuardDuty 安全代理程式的偏好方法	步驟
	GuardDuty 將管理已標記為 GuardDuty Managed -true 對之所有 Amazon EKS 叢集的安全代理程式的部署和更新。 或者，您可以使用自己的區域檢測器 ID 來使用該 AWS CLI 命令。要查找您detectorId 的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。 下列範例會為單一帳戶啟用 EKS_ADDON_MANAGEMENT 和停用 EKS_RUNTIME_MONITORING 。您也可以傳遞以空格分隔的帳戶 ID 清單。 要查找您detectorId 的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。 `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] ]'` 當程式碼成功執行時，會返回一個空白 UnprocessedAccounts 清單。如果變更帳戶的偵測器設定時發生任何問題，則會列出該帳戶 ID 以及問題摘要。

管理 GuardDuty 安全代理程式的偏好方法	步驟
手動管理安全代理程式	1. 若要為您的新帳戶選擇性地啟用 EKS 執行期監控，請使用您自己的### *ID* 調用 UpdateOrganizationConfiguration API 操作。 將 EKS_ADDON_MANAGEMENT 的狀態設定為 DISABLED。 或者，您可以使用自己的區域檢測器 ID 來使用該 AWS CLI 命令。要查找您detectorId 的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。 下列範例會為單一帳戶啟用 EKS_ADDON_MANAGEMENT 和停用 EKS_RUNTIME_MONITORING 。您也可以傳遞以空格分隔的帳戶 ID 清單。 要查找您detectorId 的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。 `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] ]'` 當程式碼成功執行時，會返回一個空白 UnprocessedAccounts 清單。如果變更帳戶的偵測器設定時發生任何問題，則會列出該帳戶 ID 以及問題摘要。 2. 若要管理安全代理程式，請參閱手動管理 Amazon EKS 叢集的安全代理程式。

為個別作用中成員帳戶啟用 EKS 執行期監控

API/CLI

根據 管理 GuardDuty安全代理程式的方法，您可以選擇偏好的方法，並依照下表所述的步驟進行。

管理 GuardDuty 安全代理程式的偏好方法	步驟
透過管理安全代理程式 GuardDuty (監視所有 EKS 叢集)	若要為您的成員帳戶選擇性地啟用 EKS 執行期監控，請使用您自己的*### ID* 執行 updateMemberDetectors API 操作。 將 EKS_ADDON_MANAGEMENT 的狀態設定為 ENABLED。 GuardDuty 將管理您帳戶中所有 Amazon EKS 叢集的安全代理程式部署和更新。 或者，您可以使用自己的區域檢測器 ID 來使用該 AWS CLI 命令。要查找您detectorId 的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。 下列範例會啟用 EKS_RUNTIME_MONITORING 和 EKS_ADDON_MANAGEMENT ： `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] ]'` **Note** 您也可以傳遞以空格分隔的帳戶 ID 清單。

管理 GuardDuty 安全代理程式的偏好方法	步驟
	當程式碼成功執行時，會返回一個空白 UnprocessedAccounts 清單。如果變更帳戶的偵測器設定時發生任何問題，則會列出該帳戶 ID 以及問題摘要。

管理 GuardDuty 安全代理程式的偏好方法	步驟
監控所有 EKS 叢集，但排除其中一些叢集 (使用排除標籤)	1. 為您要排除監控的 EKS 叢集加上標籤。鍵值對為 `GuardDutyManaged -false`。如需有關新增標籤的詳細資訊，請參閱《Amazon EKS 使用者指南》中的透過 CLI、API 或 eksctl 使用標籤。 2. 若要防止修改標籤 (僅允許信任的實體進行修改)，請使用《AWS Organizations 使用者指南》中防止標籤被授權主體以外的人員修改中提供的政策。在此政策中，請取代下列詳細資訊： • 將 *ec2#CreateTags* 替換為`eks:TagResource` . • 將 *ec2#DeleteTags* 替換為`eks:UntagResource` . • 使用 `GuardDutyManaged` 取代 *access-project* • 將 *AWS ## 123456789012* 取代為受信任實體的識別碼。 當不只有一個信任的實體時，使用下列範例來新增多個 `PrincipalArn` ： `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. **Note** 在將的設定為之前，請務必將排除標籤新增`EKS_RUNTIME_MONITORING` 至您的 `STATUS` EKS 叢集`ENABLED`；否則，GuardDuty 安全性代理程式將部署到您帳戶中的所有 EKS 叢集上。

管理 GuardDuty 安全代理程式的偏好方法	步驟
	若要為您的成員帳戶選擇性地啟用 EKS 執行期監控，請使用您自己的*### ID* 執行 updateMemberDetectors API 操作。 將 EKS_ADDON_MANAGEMENT 的狀態設定為 ENABLED。 GuardDuty 將管理尚未排除在受監控之外的所有 Amazon EKS 叢集的安全代理程式部署和更新。 或者，您可以使用自己的區域檢測器 ID 來使用該 AWS CLI 命令。要查找您detectorId 的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。 下列範例會啟用 EKS_RUNTIME_MONITORING 和 EKS_ADDON_MANAGEMENT ： `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'` **Note** 您也可以傳遞以空格分隔的帳戶 ID 清單。 當程式碼成功執行時，會返回一個空白 UnprocessedAccounts 清單。如果變更帳戶的偵測器設定時發生任何問題，則會列出該帳戶 ID 以及問題摘要。

管理 GuardDuty 安全代理程式的偏好方法	步驟
監控選定 EKS 叢集 (使用包含標籤)	1. 為您要排除監控的 EKS 叢集加上標籤。鍵值對為 GuardDutyManaged -true。如需有關新增標籤的詳細資訊，請參閱《Amazon EKS 使用者指南》中的透過 CLI、API 或 eksctl 使用標籤。 2. 若要防止修改標籤 (僅允許信任的實體進行修改)，請使用《AWS Organizations 使用者指南》中防止標籤被授權主體以外的人員修改中提供的政策。在此政策中，請取代下列詳細資訊： • 將 *ec2#CreateTags* 替換為eks:TagResource . • 將 *ec2#DeleteTags* 替換為eks:UntagResource . • 使用 GuardDutyManaged 取代 *access-project* • 將 *AWS ## 123456789012* 取代為受信任實體的識別碼。 當不只有一個信任的實體時，使用下列範例來新增多個 PrincipalArn ： `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. 若要為您的成員帳戶選擇性地啟用 EKS 執行期監控，請使用您自己的*### ID* 執行 updateMemberDetectors API 操作。 將 EKS_ADDON_MANAGEMENT 的狀態設定為 DISABLED。

管理 GuardDuty 安全代理程式的偏好方法	步驟
	GuardDuty 將管理已標記為 GuardDuty Managed -true 對之所有 Amazon EKS 叢集的安全代理程式的部署和更新。 或者，您可以使用自己的區域檢測器 ID 來使用該 AWS CLI 命令。要查找您detectorId 的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。 下列範例會啟用 EKS_RUNTIME_MONITORING 並停用 EKS_ADDON_MANAGEMENT ： `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'` **Note** 您也可以傳遞以空格分隔的帳戶 ID 清單。 當程式碼成功執行時，會返回一個空白 UnprocessedAccounts 清單。如果變更帳戶的偵測器設定時發生任何問題，則會列出該帳戶 ID 以及問題摘要。

管理 GuardDuty 安全代理程式的偏好方法	步驟
手動管理安全代理程式	1. 若要為您的成員帳戶選擇性地啟用 EKS 執行期監控，請使用您自己的*### ID* 執行 updateMemberDetectors API 操作。 將 EKS_ADDON_MANAGEMENT 的狀態設定為 DISABLED。 或者，您可以使用自己的區域檢測器 ID 來使用該 AWS CLI 命令。要查找您detectorId 的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。 下列範例會啟用 EKS_RUNTIME_MONITORING 並停用 EKS_ADDON_MANAGEMENT ： `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] } ]'` 2. 若要管理安全代理程式，請參閱手動管理 Amazon EKS 叢集的安全代理程式。

從 EKS 執行階段監視移轉至執行階段監視

隨著 GuardDuty 運行時監控的推出，威脅偵測涵蓋範圍已擴展到 Amazon ECS 容器和 Amazon EC2 執行個體。EKS 執行階段監視現在已整合到執行階段監視中。您可以針對要監控執行階段行為的每種資源類型 (Amazon EC2 執行個體、Amazon ECS 叢集和 Amazon EKS 叢集) 啟用執行階段監控，並管理個別 GuardDuty 安全代理程式。

EKS 運行時監視沒有單獨的 GuardDuty 控制台體驗。若要繼續使用 EKS 執行階段監視，您需要使用 API 或. AWS Command Line Interface

從 EKS 執行階段監視移轉至執行階段監視

1. GuardDuty 控制台支持 EKS 運行時監視作為運行時監視的一部分。

   您可以依檢查 EKS 執行階段監視組態狀態組織和帳戶開始使用執行階段監視。

   啟用執行階段監視之前，請確定不要停用 EKS 執行階段監視。如果停用 EKS 執行階段監控，Amazon EKS 附加元件管理也會停用。依照列出的順序繼續執行下列步驟。
2. 確保你滿足所有啟用程式實際執行監視的.
3. 針對「執行階段監視」複製與 EKS 執行階段監視相同的組織組態設定，以啟用「執行時期監視」。如需詳細資訊，請參閱 啟用執行期監視。
   - 如果您有獨立帳戶，則需要啟用運行時監視。

     如果您的 GuardDuty Security Agent 已部署，則會自動複製對應的設定，您不需要再次進行設定。
   - 如果您的組織具有自動啟用設定，請務必針對「執行階段監視」複製相同的自動啟用設定。
   - 如果您的組織具有針對現有作用中成員帳戶個別設定的設定，請務必啟用執行階段監控，並個別為這些成員設定 GuardDuty 安全代理程式。
4. 確定執行階段監視和 GuardDuty 安全性代理程式設定正確無誤之後，請使用 API 或命令停用 EKS 執行階段監視。 AWS CLI
5. (選擇性) 如果您要清除與 GuardDuty Security Agent 相關聯的任何資源，請參閱停用及清理資源的影響。

如果您想要繼續使用 EKS 執行階段監視而不啟用執行階段監視，請參閱設定 EKS 執行階段監控 (僅限 API)。

檢查 EKS 執行階段監視組態狀態

使用下列 API 或 AWS CLI 命令來檢查 EKS 執行階段監視的現有組態狀態。

檢查帳戶中現有的 EKS 執行階段監控組態狀態

- 運行GetDetector以檢查您自己帳戶的配置狀態。
- 或者，您可以使用以下命令來執行 AWS CLI：

```
aws guardduty get-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
region us-east-1
```

確保更換您和當前區域 AWS 帳戶 的檢測器 ID。要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

若要檢查組織的現有 EKS 執行階段監視組態狀態 (僅限委派的 GuardDuty 系統管理員帳戶)

- 執行DescribeOrganizationConfiguration以檢查組織的組態狀態。

  或者，您可以使用以下命令來執行下列命令 AWS CLI：

  ```
  aws guardduty describe-organization-configuration --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --region us-east-1
  ```

  確保將檢測器 ID 替換為委託 GuardDuty 管理員帳戶的檢測器 ID，並將該地區替換為您當前區域的檢測器 ID。要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

移轉至執行階段監視之後停用 EKS 執行階段監視

確定帳戶或組織的現有設定已複製到執行階段監視之後，您可以停用 EKS 執行階段監視。

停用 EKS 執行階段監視

- 在您自己的帳戶中停用 EKS 執行階段監控

  使用您自己的區域### ID ## *UpdateDetector*API。

  或者，您可以使用以下 AWS CLI 命令。############### 12abc34e56789f0#

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

- 若要停用組織中成員帳戶的 EKS 執行階段監視

  使用組織委派 GuardDuty 管理員帳戶的區域######執行 UpdateMemberDetectorsAPI。

  或者，您可以使用以下 AWS CLI 命令。# 12abc34d567e8fa1bc2d34e56789f0 ########## ################ 1111222 23333 ################### GuardDuty AWS 帳戶

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

- 更新組織的 EKS 執行階段監視自動啟用設定

  僅當您已將 EKS 執行階段監視自動啟用設定設定設定設定設定設定設定為組織中的新 (NEW) 或全部 (ALL) 成員帳戶時，才執行下列步驟。如果您已將其配置為NONE，則可以跳過此步驟。

  > **Note**
  >
  > 將 EKS 執行階段監視自動啟用組態設定，NONE表示不會針對任何現有成員帳戶或新成員帳戶加入組織時自動啟用 EKS 執行階段監視。

  使用組織委派 GuardDuty 管理員帳戶的區域######執行 UpdateOrganizationConfigurationAPI。

  或者，您可以使用以下 AWS CLI 命令。*# 12abc34d567e8fa901bc2d34e56789 f0 ###### ##################* GuardDuty 將############態，以便自動啟用。 GuardDuty

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members EXISTING_VALUE
 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NONE"}]'
```

評估資源的執行階段涵蓋範圍

啟用執行階段監視並將 GuardDuty Security Agent 部署到您的資源後，會針對屬於您帳戶的資源 GuardDuty提供對應資源類型的涵蓋範圍統計資料，以及個別涵蓋範圍狀態的統計資料。涵蓋範圍狀態的決定方式是確定您已啟用執行時期監控、已建立 Amazon VPC 端點，以及對應資源的 GuardDuty 安全代理程式已部署。狀態良好的涵蓋範圍狀態表示當有與資源相關的執行時期事件時， GuardDuty 能夠透過 Amazon VPC 端點接收上述執行階段事件，並監控行為。如果在設定執行階段監控、建立 Amazon VPC 端點或部署 GuardDuty安全代理程式時發生問題，則涵蓋範圍狀態會顯示為「狀況不良」。當涵蓋範圍狀態不良時， GuardDuty 將無法接收或監視對應資源的執行階段行為，也無法產生任何「執行時期監控」發現項目。

下列主題將協助您檢閱涵蓋範圍統計資料、設定 EventBridge 通知，以及疑難排解特定資源類型的涵蓋範圍問題。

目錄

Amazon EC2 實例的覆蓋範圍

對於 Amazon EC2 資源，執行階段涵蓋範圍會在執行個體層級進行評估。您的 Amazon EC2 執行個體可以在您的 AWS 環境中執行多種類型的應用程式和工作負載。此功能也支援 Amazon ECS 受管的 Amazon EC2 執行個體，如果您的 Amazon ECS 叢集在 Amazon EC2 執行個體上執行，則執行個體層級的涵蓋範圍問題將會顯示在 Amazon EC2 執行階段涵蓋範圍下。

主題

檢閱涵蓋範圍統計資料

與您自己帳戶或成員帳戶關聯之 Amazon EC2 執行個體的涵蓋範圍統計資料是所選 EC2 執行個體中運作狀態良好的 EC2 執行個體的百分比 AWS 區域。可以用下列方程式將此表示為：

(狀態良好的執行個體/所有執行個體) *100

如果您也為 Amazon ECS 叢集部署 GuardDuty 安全代理程式，則與在 Amazon EC2 執行個體上執行的 Amazon ECS 叢集相關的任何執行個體層級涵蓋範圍問題都會顯示為 Amazon EC2 執行個體執行階段涵蓋範圍問題。

選擇其中一種存取方法來檢閱您帳戶的涵蓋範圍統計資料。

Console

- 請登入 AWS Management Console 並開啟 GuardDuty 主控台，網址為 https://console.aws.amazon.com/guardduty/。
- 在功能窗格中，選擇 [執行階段監視]。

- 選擇「執行時間範圍」標籤。
- 在 EC2 執行個體執行階段涵蓋範圍索引標籤下，您可以檢視依執行個體清單表格中可用之每個 Amazon EC2 執行個體的涵蓋範圍狀態彙總的涵蓋範圍統計資料。
  - 您可以依下列欄篩選「例證」清單表格：
    - 帳戶 ID
    - 代理程式管理類型
    - 代理版本
    - 涵蓋範圍狀態
    - 實例識別碼
    - 集群 ARN
- 如果您的任何 EC2 執行個體的涵蓋範圍狀態為「不良狀態」，「問題」欄會包含有關狀態不良原因的其他資訊。

API/CLI

- 使用您自己的有效偵測器 ID、目前區域和服務端點執行 ListCoverageAPI。您可以使用此 API 篩選和排序執行個體清單。
  - 您可以使用 `CriterionKey` 的下列選項之一變更範例 `filter-criteria`：
    - `ACCOUNT_ID`
    - `RESOURCE_TYPE`
    - `COVERAGE_STATUS`
    - `AGENT_VERSION`
    - `MANAGEMENT_TYPE`
    - `INSTANCE_ID`
    - `CLUSTER_ARN`
  - 當`filter-criteria`包含`RESOURCE_TYPE`為 EC2 時，運行時監控不支持使用問題作為`AttributeName`. 如果使用它，API 響應將導致`InvalidInputException`。

    您可以使用下列選項變更 `sort-criteria` 中的範例 `AttributeName`：
    - `ACCOUNT_ID`
    - `COVERAGE_STATUS`
    - `INSTANCE_ID`

    - UPDATED_AT
  - 您可以變更 *max-results* (最多 50 個)。
  - 要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

```
aws guardduty --region us-east-1 list-coverage --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName":
 "EKS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria
 '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":
{"EqualsValue":"111122223333"}}] }'  --max-results 5
```

- 執行 GetCoverageStatisticsAPI 以擷取涵蓋範圍彙總統計資料statisticsType。
  - 您可以將範例 statisticsType 變更成下列選項之一：
    - COUNT_BY_COVERAGE_STATUS：表示依涵蓋範圍狀態彙總的 EKS 叢集涵蓋範圍統計資料。
    - COUNT_BY_RESOURCE_TYPE— 根據列表中的 AWS 資源類型匯總覆蓋率統計信息。
    - 您可以在命令中變更範例 filter-criteria。您可將下列選項用於 CriterionKey：
      - ACCOUNT_ID
      - RESOURCE_TYPE
      - COVERAGE_STATUS
      - AGENT_VERSION
      - MANAGEMENT_TYPE
      - INSTANCE_ID
      - CLUSTER_ARN
  - 要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS
 --filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID",
 "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

如果 EC2 執行個體的涵蓋範圍狀態為「狀態不良」，請參閱對涵蓋範圍問題進行疑難排解。

設定涵蓋範圍狀態變更通知

您的 Amazon EC2 執行個體的涵蓋範圍狀態可能會顯示為「狀態不良」。若要知道保險狀態變更的時間，我們建議您定期監控保險狀態，並進行疑難排解狀態是否變為「不健康」。或者，您可以建立 Amazon EventBridge 規則，以便在涵蓋範圍狀態從「不良狀態」變更為「狀況良好」或其他狀態時接收通知。默認情況下，將其 GuardDuty 發佈在EventBridge 公共汽車中為您的帳戶。

範例通知結構描述

在 EventBridge 規則中，您可以使用預先定義的範例事件和事件模式來接收涵蓋範圍狀態通知。如需有關建立 EventBridge 規則的詳細資訊，請參閱 Amazon EventBridge 使用者指南中的建立規則。

此外，您可以使用下列範例通知結構描述來建立自訂事件模式。請務必替換您帳戶的值。若要在 Amazon EC2 執行個體的涵蓋範圍狀態從變更為時收Healthy到通知Unhealthy，`detail-type`應為執*GuardDuty #########*。若要在涵蓋範圍狀態從變更為時收到通知Healthy，Unhealthy請`detail-type`使用 [*GuardDuty ########*] 取代的值。

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "AWS ## ID",
  "time": "event timestamp (string)",
  "region": "AWS ##",
  "resources": [
      ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
        "resourceType": "EC2",
        "ec2InstanceDetails": {
          "instanceId":"",
          "instanceType":"",
          "clusterArn": "",
          "agentDetails": {
            "version":""
          },
          "managementType":""
        }
```

```
    },
    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}
```

對涵蓋範圍問題進行疑難排解

如果 Amazon EC2 執行個體的涵蓋範圍狀態為「狀態不良」，您可以在「問題」欄下檢視原因。

如果您的 EC2 執行個體與 EKS 叢集相關聯，而 EKS 的安全代理程式是手動或透過自動化代理程式組態安裝，則若要疑難排解涵蓋範圍問題，請參閱。Amazon EKS 叢集的涵蓋範圍

下表列出問題類型和對應的疑難排解步驟。

問題類型	問題訊息	疑難排解步驟
無代理報告	正在等待 SSM 通知	請確定亞馬遜 EC2 執行個體已經受到 SSM 管理。接收 SSM 通知可能需要幾分鐘的時間。
	（故意為空）	如果您要手動管理 GuardDuty 安全代理程式，請確定您已按照下方的步驟進行手動管理 Amazon EC2 執行個體的安全代理程式。
		如果您已啟用自動化代理程式設定： • 您的 EC2 執行個體受到 SSM 管理。 • 定期檢視安全代理程式的狀態。如需詳細資訊，請參閱驗證安 GuardDuty 全代理程式安裝狀態。
		如果您的組織有服務控制原則 (SCP)，請確定它不會拒絕`guardduty:SendSecurityTelemetry` 權限。如需詳細資訊，請參閱 驗證您的組織服務控制政策。
	代理已中斷	• 檢視安全代理程式的狀態。如需詳細資訊，請參閱 驗證安 GuardDuty 全代理程式安裝狀態。 • 檢視安全代理程式記錄檔，以識別潛在的根本原因。記錄檔提供詳細的錯誤，您可以用來自行疑難排解問題。記錄檔可在下找到`/var/log/amzn-guardduty-agent/` 。

問題類型	問題訊息	疑難排解步驟
		做`sudo journalctl -u amazon-guardduty-agent` 。
建立 SSM 關聯失敗	GuardDuty SSM 關聯已存在於您的帳戶	1. 手動刪除現有的關聯。如需詳細資訊，請參閱《使用指南》中的AWS Systems Manager 〈刪除關聯〉。 2. 刪除關聯後，請停用 Amazon EC2 的 GuardDuty 自動化代理程式組態，然後重新啟用。
	您的帳戶有太多 SSM 關聯	選擇下列兩個選項之一： • 刪除任何未使用的 SSM 關聯。如需詳細資訊，請參閱《使用指南》中的AWS Systems Manager 〈刪除關聯〉。 • 檢查您的帳戶是否符合增加配額的資格。如需詳細資訊，請參閱 AWS 一般參考.
SSM 關聯更新失敗	GuardDuty 您的帳戶中不存在 SSM 關聯	GuardDuty SSM 關聯不存在於您的帳戶中。停用執行階段監視，然後再重新啟用。
SSM 關聯刪除失敗	GuardDuty 您的帳戶中不存在 SSM 關聯	SSM 關聯不存在於您的帳戶中。如果有意刪除 SSM 關聯，則不需要採取任何動作。

問題類型	問題訊息	疑難排解步驟
SSM 執行個體關聯執行失敗	不符合架構需求或其他先決條件。	如需有關已驗證作業系統發行版的資訊，請參閱 Amazon EC2 執行個體支援的先決條件 如果您仍然遇到這個問題，下列步驟將協助您識別並解決問題： 1. 請在以下位置開啟 AWS Systems Manager 主控台。 https://console.aws.amazon.com/systems-manager/ 2. 在功能窗格的 [節點管理] 下，選取 [狀態管理員]。 3. 依「文件名稱」內容篩選並輸入AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin。 4. 選取對應的關聯 ID 並檢視其執行歷史記錄。 5. 使用執行歷史記錄，查看失敗，識別潛在的根本原因，然後嘗試解決它。
VPC 端點建立失敗	共用 VPC *vpcId* 不支援建立 VPC 端點	執行階段監視支援在組織內使用共用 VPC。如需詳細資訊，請參閱 搭配自動化安全代理程式使用共用 VPC。
	僅當使用具有自動代理程式組態的共用 VPC 共用 VPC *vpcId* 的擁有者帳戶識別碼 *111122223333* 未啟用執行階段監視、自動化代理程式組態，或兩者皆未啟用	共用 VPC 擁有者帳戶必須為至少一種資源類型 (Amazon EKS 或 Amazon ECS (AWS Fargate)) 啟用執行時期監控和自動化代理程式組態。如需詳細資訊，請參閱 GuardDuty程式實際執行監視特定的。

問題類型	問題訊息	疑難排解步驟
	啟用私有 DNS 需要 enableDnsSupport 和 enableDnsHostnames VPC 屬性針對 *vpcId* 設定為 true (服務：Ec2、狀態碼：400，請求 ID：*a1b2c3d4-5678-90ab-cdef-EXAMPLE11111*)。	請確保將下列 VPC 屬性設定為 true：enableDnsSupport 和 enableDnsHostnames。如需詳細資訊，請參閱 VPC 中的 DNS 屬性。 如果您造訪 https://console.aws.amazon.com/vpc/ 以使用 Amazon VPC 主控台建立 Amazon VPC，請務必選擇啟用 DNS 主機名稱和啟用 DNS 解析。如需詳細資訊，請參閱 VPC 組態選項。
共用 VPC 端點刪除失敗	*##### 111122223333 ###### ### vPCID# ######## 55555555 ########## ##*	潛在步驟： • 停用共用 VPC 參與者帳戶的執行階段監視狀態不會影響共用 VPC 端點原則和擁有者帳戶中存在的安全性群組。 若要刪除共用 VPC 端點和安全群組，您必須停用共用 VPC 擁有者帳戶中的執行階段監控或自動代理程式設定狀態。 • 共用 VPC 參與者帳戶無法刪除共用 VPC 擁有者帳戶中託管的共用 VPC 端點和安全群組。
代理程式未報告	（故意為空）	問題類型已終止支援。如果您持續遇到此問題，但尚未發生此問題，請為 Amazon EC2 啟用 GuardDuty 自動化代理程式。 如果問題仍然存在，請考慮禁用運行時監視幾分鐘，然後再次啟用它。

Amazon ECS 叢集的涵蓋範圍

Amazon ECS 叢集的執行階段涵蓋範圍包括在 Amazon ECS 容器執行個 AWS Fargate (Fargate) 體上執行的任務。[1]

對於在 Fargate 上執行的 Amazon ECS 叢集，會在任務層級評估執行階段涵蓋範圍。ECS 叢集執行階段涵蓋範圍包括在您為 Fargate 啟用執行階段監視和自動化代理程式組態 (僅限 ECS) 之後開始執行的 Fargate 工作。默認情況下，Fargate 任務是不可變的。 GuardDuty 將無法安裝安全代理程式來監視已在執行中工作上的容器。要包含這樣的 Fargate 任務，您必須停止並重新啟動任務。確保檢查是否支持關聯的服務。

目前，運行時監視不支持啟動的任務。 AWS CodePipeline

如需 Amazon ECS 容器的相關資訊，請參閱容量建立。

目錄

檢閱涵蓋範圍統計資料

與您自己的帳戶或您的會員帳戶相關聯之 Amazon ECS 資源的涵蓋範圍統計資料是所選 Amazon ECS 叢集中運作良好的 Amazon ECS 叢集的百分比。 AWS 區域這包括與 Fargate 和 Amazon EC2 執行個體相關聯的亞馬遜 ECS 叢集的涵蓋範圍。可以用下列方程式將此表示為：

(運作狀態良好的叢集/所有叢集) * 100

考量事項

- ECS 叢集的涵蓋範圍統計資料包括與該 ECS 叢集相關聯的 Fargate 工作或 ECS 容器執行個體的涵蓋範圍狀態。Fargate 工作的涵蓋範圍狀態包括處於執行中狀態或最近已完成執行的工作。
- 在 ECS 叢集執行階段涵蓋範圍索引標籤中，容器執行個體涵蓋欄位會指出與 Amazon ECS 叢集相關聯之容器執行個體的涵蓋範圍狀態。

  如果您的 Amazon ECS 叢集僅包含 Fargate 任務，則計數會顯示為 0/0。
- 如果您的 Amazon ECS 叢集與沒有安全代理程式的 Amazon EC2 執行個體相關聯，Amazon ECS 叢集也會呈現狀態不良的涵蓋狀態。

若要識別相關 Amazon EC2 執行個體的涵蓋範圍問題並進行疑難排解，請參閱 對涵蓋範圍問題進行疑難排解 Amazon EC2 執行個體相關資訊。

選擇其中一種存取方法來檢閱您帳戶的涵蓋範圍統計資料。

Console

- 請登入 AWS Management Console 並開啟 GuardDuty 主控台，網址為 https://console.aws.amazon.com/guardduty/。
- 在功能窗格中，選擇 [執行階段監視]。
- 選擇「執行時間範圍」標籤。
- 在 ECS 叢集執行時期涵蓋範圍索引標籤下，您可以檢視「叢集」清單表格中可用之每個 Amazon ECS 叢集的涵蓋範圍狀態彙總的涵蓋範圍統計資料。
  - 您可以依下列資料欄篩選「叢集」清單表格：
    - 帳戶 ID
    - 叢集名稱
    - 代理程式管理類型
    - 涵蓋範圍狀態
- 如果您的任何 Amazon ECS 叢集的「涵蓋範圍」狀態為「不良狀態」，「問題」欄會包含有關狀態不良原因的其他資訊。

  如果 Amazon ECS 叢集與 Amazon EC2 執行個體相關聯，請導覽至 EC2 執行個體執行個體執行階段涵蓋範圍索引標籤，並按叢集名稱欄位進行篩選，以檢視相關問題。

API/CLI

- 使用您自己的有效偵測器 ID、目前區域和服務端點執行 ListCoverageAPI。您可以使用此 API 篩選和排序執行個體清單。
  - 您可以使用 `CriterionKey` 的下列選項之一變更範例 `filter-criteria`：
    - `ACCOUNT_ID`
    - `ECS_CLUSTER_NAME`
    - `COVERAGE_STATUS`
    - `MANAGEMENT_TYPE`

- 您可以使用下列選項變更 sort-criteria 中的範例 AttributeName：
  - ACCOUNT_ID
  - COVERAGE_STATUS
  - ISSUE
  - ECS_CLUSTER_NAME
  - UPDATED_AT

    只有在關聯的 Amazon ECS 叢集中建立新任務，或對應的涵蓋範圍狀態發生變更時，此欄位才會更新。
- 您可以變更 *max-results* (最多 50 個)。
- 要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

```
aws guardduty --region us-east-1 list-coverage --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName":
 "ECS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria
 '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":
{"EqualsValue":"111122223333"}}] }'  --max-results 5
```

- 執行 GetCoverageStatisticsAPI 以擷取涵蓋範圍彙總統計資料statisticsType。
  - 您可以將範例 statisticsType 變更成下列選項之一：
    - COUNT_BY_COVERAGE_STATUS— 表示按涵蓋範圍狀態彙總的 ECS 叢集涵蓋率統計資料。
    - COUNT_BY_RESOURCE_TYPE— 根據列表中的 AWS 資源類型匯總覆蓋率統計信息。
    - 您可以在命令中變更範例 filter-criteria。您可將下列選項用於 CriterionKey：
      - ACCOUNT_ID
      - ECS_CLUSTER_NAME
      - COVERAGE_STATUS
      - MANAGEMENT_TYPE
      - INSTANCE_ID
  - 要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS
```

```
--filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID",
"FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

如需涵蓋範圍問題的詳細資訊，請參閱對涵蓋範圍問題進行疑難排解。

設定涵蓋範圍狀態變更通知

Amazon ECS 叢集的涵蓋範圍狀態可能會顯示為「狀況不良」。若要知道保險狀態變更的時間，我們建議您定期監控保險狀態，並進行疑難排解狀態是否變為「不健康」。或者，您可以建立 Amazon EventBridge 規則，以便在涵蓋範圍狀態從「不良狀態」變更為「狀況良好」或其他狀態時接收通知。默認情況下，將其 GuardDuty 發佈在EventBridge 公共汽車中為您的帳戶。

範例通知結構描述

在 EventBridge 規則中，您可以使用預先定義的範例事件和事件模式來接收涵蓋範圍狀態通知。如需有關建立 EventBridge 規則的詳細資訊，請參閱 Amazon EventBridge 使用者指南中的建立規則。

此外，您可以使用下列範例通知結構描述來建立自訂事件模式。請務必替換您帳戶的值。若要在 Amazon ECS 叢集的涵蓋範圍狀態從變更Healthy為時收到通知Unhealthy，detail-type應為*GuardDuty #########*良。若要在涵蓋範圍狀態從變更為時收到通知Healthy，Unhealthy請detail-type使用 [*GuardDuty ########*] 取代的值。

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "AWS ## ID",
  "time": "event timestamp (string)",
  "region": "AWS ##",
  "resources": [
       ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
        "resourceType": "ECS",
        "ecsClusterDetails": {
          "clusterName":"",
          "fargateDetails":{
```

```
            "issues":[],
            "managementType":""
          },
          "containerInstanceDetails":{
            "coveredContainerInstances":int,
            "compatibleContainerInstances":int
          }
        }
    },
    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}
```

對涵蓋範圍問題進行疑難排解

如果 Amazon ECS 叢集的涵蓋範圍狀態為「狀況不良」，您可以在「問題」欄下檢視原因。

下表提供 Fargate (僅限 Amazon ECS) 問題的建議疑難排解步驟。如需 Amazon EC2 執行個體涵蓋範圍問題的相關資訊，請參閱 對涵蓋範圍問題進行疑難排解 Amazon EC2 執行個體相關資訊

問題類型	額外資訊	建議的疑難排解步驟
代理程式未報告	代理程式未針對中的工作報告 TaskDefinition - ' *TASK_DEFINITION* '	驗證您的 VPC 端點組態是否正確。 如果您的組織有服務控制原則 (SCP)，請確定它不會拒絕guardduty:SendSecurityTelemetry 權限。如需詳細資訊，請參閱 驗證您的組織服務控制政策。
	VPC_ISSUE ; for task in TaskDefinition - ' *TASK_DEFINITION* '	在額外資訊中檢視 VPC 問題詳細資訊。
代理程式已退出	ExitCode：EXIT_CODE 針對工作 TaskDefinition - ' *TASK_DEFINITION* '	在額外資訊中檢視問題詳細資訊。

問題類型	額外資訊	建議的疑難排解步驟
	原####### TaskDefinition - ' *TASK_DEFINITION* '	
	ExitCode：EXIT_CODE 有原因：用於任務的「####」TaskDefinition - ' *TASK_DEFINITION* '	

	代理退出:原因:CannotPullContainerError：拉圖像清單已被重試...	任務執行角色必須具有以下亞馬遜彈性容器登錄 (Amazon ECR) 許可：
		`...`
		`"ecr:GetAuthorizationToken",`
		`"ecr:BatchCheckLayerAvailability",`
		`"ecr:GetDownloadUrlForLayer",`
		`"ecr:BatchGetImage",`
		`...`
		如需詳細資訊，請參閱 提供 ECR 權限和子網路詳細資料。
		新增 Amazon ECR 許可後，您必須重新啟動任務。
		如果問題仍然存在，請參閱我的 AWS Step Functions 工作流程意外失敗。

問題類型	額外資訊	建議的疑難排解步驟
未佈建的其他或代理程式	無法辨識的問題, 針對工作 TaskDefinition - '*TASK_DEFINITION* '	請使用下列問題找出問題的根本原因： • 在啟用執行階段監視之前，工作是否已啟動？ 在 Amazon ECS 中，任務是不可變的。若要評估執行中 Fargate 工作的執行階段行為，請確定已啟用執行階段監控，然後重新啟動工作 GuardDuty 以新增容器附屬。 • 該任務是由不支持的服務啟動的嗎？ 目前，運行時監視不支持啟動的任務。 AWS CodePipeline • 這項工作是在您啟用執行階段監視之前啟動的服務部署的一部分嗎？ 如果是，您可以使用更新服務中的步驟`forceNewDeployment` 來重新啟動服務或更新服務。 您也可以使用UpdateService或AWS CLI。 • 從執行階段監視排除 ECS 叢集後，工作是否啟動？ 當您將預先定義的 GuardDuty 標籤從 `GuardDutyManaged` -變更`true`為 `GuardDutyManaged` -時`false`，GuardDuty 將不會接收 ECS 叢集的執行階段事件。 • 您的任務缺少了`TaskExecutionRole` 嗎？ 您必須新增一個，`TaskExecutionRole` 因為 GuardDuty 需要從

問題類型	額外資訊	建議的疑難排解步驟
		ECR 存放庫下載 GuardDuty 容器的權限。如需詳細資訊，請參閱 提供 ECR 權限和子網路詳細資料。 • 您的服務是否包含具有舊格式的任務`taskArn`？ GuardDuty 運行時監視不支持具有舊格式的任務的覆蓋範圍`taskArn`。 如需 Amazon ECS 資源的 Amazon 資源名稱 (ARN) 的相關資訊，請參閱 Amazon 資源名稱 (ARN) 和 ID。

Amazon EKS 叢集的涵蓋範圍

手動或透過自動化代理程式組態啟用執行階段監控並安裝 EKS 的安 GuardDuty 全代理程式 (附加元件) 之後，您就可以開始評估 EKS 叢集的涵蓋範圍。

目錄

檢閱涵蓋範圍統計資料

與您帳戶或您的成員帳戶相關聯的 EKS 叢集涵蓋範圍統計資料，是指運作狀態良好的 EKS 叢集在所選 AWS 區域的所有 EKS 叢集中所佔百分比。可以用下列方程式將此表示為：

(運作狀態良好的叢集/所有叢集) * 100

選擇其中一種存取方法來檢閱您帳戶的涵蓋範圍統計資料。

Console

- 請登入 AWS Management Console 並開啟 GuardDuty 主控台，網址為 https://console.aws.amazon.com/guardduty/。

- 在功能窗格中，選擇 [執行階段監視]。
- 選擇 EKS 叢集執行期涵蓋範圍索引標籤。
- 在 EKS 叢集執行期涵蓋範圍索引標籤下，您可以檢視依叢集清單表格中可用的涵蓋範圍狀態彙總的涵蓋範圍統計資料。
  - 您可以依下列資料欄篩選叢集清單表格：
    - 叢集名稱
    - 帳戶 ID
    - 代理程式管理類型
    - 涵蓋範圍狀態
    - 附加元件版本
- 如果您的任何 EKS 叢集擁有運作狀態不良的涵蓋範圍狀態，問題資料欄可能會包含有關運作狀態不良狀態的原因的其他資訊。

API/CLI

- 使用您自己的有效偵測器 ID、區域和服務端點執行 ListCoverageAPI。您可以使用此 API 篩選和排序叢集清單。
  - 您可以使用 `CriterionKey` 的下列選項之一變更範例 `filter-criteria`：
    - `ACCOUNT_ID`
    - `CLUSTER_NAME`
    - `RESOURCE_TYPE`
    - `COVERAGE_STATUS`
    - `ADDON_VERSION`
    - `MANAGEMENT_TYPE`
  - 您可以使用下列選項變更 `sort-criteria` 中的範例 `AttributeName`：
    - `ACCOUNT_ID`
    - `CLUSTER_NAME`
    - `COVERAGE_STATUS`
    - `ISSUE`
    - `ADDON_VERSION`
    - `UPDATED_AT`
  - 您可以變更 *`max-results`* (最多 50 個)。

- 要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

```
aws guardduty --region us-east-1 list-coverage --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName":
 "EKS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria
 '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":
{"EqualsValue":"111122223333"}}] }'  --max-results 5
```

- 執行 GetCoverageStatisticsAPI 以擷取涵蓋範圍彙總統計資料statisticsType。
  - 您可以將範例 statisticsType 變更成下列選項之一：
    - COUNT_BY_COVERAGE_STATUS：表示依涵蓋範圍狀態彙總的 EKS 叢集涵蓋範圍統計資料。
    - COUNT_BY_RESOURCE_TYPE— 根據列表中的 AWS 資源類型匯總覆蓋率統計信息。
    - 您可以在命令中變更範例 filter-criteria。您可將下列選項用於 CriterionKey：
      - ACCOUNT_ID
      - CLUSTER_NAME
      - RESOURCE_TYPE
      - COVERAGE_STATUS
      - ADDON_VERSION
      - MANAGEMENT_TYPE
  - 要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS
 --filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID",
 "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

如果 EKS 叢集的涵蓋範圍狀態為運作狀態不良，請參閱EKS 涵蓋問題疑難排解。

設定涵蓋範圍狀態變更通知

您帳戶中 EKS 叢集的涵蓋範圍狀態可能會顯示為運作狀態不良。若要偵測涵蓋範圍狀態何時變成運作狀態不良，建議您定期監控涵蓋範圍狀態，並在狀態為運作狀態不良時進行疑難排解。或者，您也可以

建立 Amazon EventBridge 規則，以便在涵蓋範圍狀態從變更Unhealthy為Healthy或以其他方式通知您。默認情況下，將其 GuardDuty 發佈在EventBridge公共汽車中為您的帳戶。

範例通知結構描述

在 EventBridge 規則中，您可以使用預先定義的範例事件和事件模式來接收涵蓋範圍狀態通知。如需有關建立 EventBridge 規則的詳細資訊，請參閱 Amazon EventBridge 使用者指南中的建立規則。

此外，您可以使用下列範例通知結構描述來建立自訂事件模式。請務必替換您帳戶的值。若要在 Amazon EKS 叢集的涵蓋範圍狀態從變更Healthy為時收到通知Unhealthy，detail-type應為*GuardDuty #########*良。若要在涵蓋範圍狀態從變更為時收到通知Healthy，Unhealthy請detail-type使用 [*GuardDuty ########*] 取代的值。

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "AWS ## ID",
  "time": "event timestamp (string)",
  "region": "AWS ##",
  "resources": [
       ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
        "resourceType": "EKS",
        "eksClusterDetails": {
            "clusterName": "string",
            "availableNodes": "string",
             "desiredNodes": "string",
             "addonVersion": "string"
         }
    },
    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}
```

EKS 涵蓋問題疑難排解

如果 EKS 叢集的涵蓋範圍狀態為Unhealthy，您可以在 GuardDuty 主控台的 [問題] 欄下方或使用CoverageResource資料類型來檢視對應的錯誤。

使用包含或排除標籤選擇性地監控 EKS 叢集時，標籤可能需要一些時間才能同步。這可能會影響相關聯 EKS 叢集的涵蓋範圍狀態。您可以嘗試再次移除和新增對應的標籤 (包含或排除)。如需詳細資訊，請參閱《Amazon ECS 使用者指南》中的為您的 Amazon EKS 資源加上標籤。

涵蓋範圍問題的結構是 `Issue type:Extra information`。這些問題一般會有選用的額外資訊，其中可能包含特定的用戶端例外狀況或與問題相關的描述。根據額外資訊，下表提供針對 EKS 叢集疑難排解涵蓋範圍問題的建議步驟。

問題類型 (字首)	額外資訊	建議的疑難排解步驟
附加元件建立失敗	附加元件`aws-guardduty-agent` 與目前叢集版本的叢集*`ClusterName`* 集不相容。不支援指定的附加元件。	請確保您使用的是支援 `aws-guardduty-agent` EKS 附加元件部署的其中一個 Kubernetes 版本。如需詳細資訊，請參閱 安全性代理程式支援的 Kubernetes 版本 GuardDuty 。如需有關更新您的 Kubernetes 版本的資訊，請參閱 更新 Amazon EKS 叢集 Kubernetes 版本。
附加元件建立失敗 附加元件更新失敗 插件狀態不健康	EKS 附加元件問題 - `AddonIssueCode` ：`AddonIssueMessage`	如需特定附加元件問題程式碼之建議步驟的詳細資訊，請參閱Troubleshooting steps for Addon creation/updatation error with Addon issue code。 如需您在此問題中可能遇到的附加問題代碼清單，請參閱AddonIssue。

問題類型 (字首)	額外資訊	建議的疑難排解步驟
VPC 端點建立失敗	*######## vPCID ##### #########*	執行階段監視現在支援在組織內使用共用 VPC。確保您的帳戶符合所有先決條件。如需詳細資訊，請參閱 使用共用 VPC 的先決條件。
	僅當使用具有自動代理程式組態的共用 VPC 共用 VPC *vpcId* 的擁有者帳戶識別碼 *111122223333* 未啟用執行階段監視、自動化代理程式組態或兩者皆啟用。	共用 VPC 擁有者帳戶必須為至少一種資源類型 (Amazon EKS 或 Amazon ECS (AWS Fargate)) 啟用執行時期監控和自動化代理程式組態。如需詳細資訊，請參閱 GuardDuty 程式實際執行監視特定的。
	啟用私有 DNS 需要 `enableDnsSupport` 和 `enableDnsHostnames` VPC 屬性針對 *vpcId* 設定為 `true` (服務：Ec2、狀態碼：400，請求 ID：*a1b2c3d4-5678-90ab-cdef-EXAMPLE11111*)。	請確保將下列 VPC 屬性設定為 `true`：`enableDnsSupport` 和 `enableDnsHostnames` 。如需詳細資訊，請參閱 VPC 中的 DNS 屬性。 如果您造訪 https://console.aws.amazon.com/vpc/ 以使用 Amazon VPC 主控台建立 Amazon VPC，請務必選擇啟用 DNS 主機名稱和啟用 DNS 解析。如需詳細資訊，請參閱 VPC 組態選項。

問題類型 (字首)	額外資訊	建議的疑難排解步驟
共用 VPC 端點刪除失敗	*##### 111122223333 ######### vPCID######### 55555555 ######### #######*	潛在步驟： • 停用共用 VPC 參與者帳戶的執行階段監視狀態不會影響共用 VPC 端點原則和擁有者帳戶中存在的安全性群組。 若要刪除共用 VPC 端點和安全群組，您必須停用共用 VPC 擁有者帳戶中的執行階段監控或自動代理程式設定狀態。 • 共用 VPC 參與者帳戶無法刪除共用 VPC 擁有者帳戶中託管的共用 VPC 端點和安全群組。
本機 EKS 叢集	本機 Outpost 叢集不支援 EKS 附加元件。	不可行。 如需詳細資訊，請參閱 AWS Outpost 上的 Amazon EKS。
未授予 EKS 執行期監控啟用許可	（可能會或可能不會顯示額外信息）	1. 如果此問題有額外資訊可用，請修正根本原因，然後依照下一個步驟進行。 2. 切換 EKS 執行期監控以關閉此功能，然後再重新開啟。確保 GuardDuty 代理程式也會自動透過 GuardDuty 或手動部署。

問題類型 (字首)	額外資訊	建議的疑難排解步驟
EKS 執行期監控啟用資源佈建進行中	（可能會或可能不會顯示額外信息）	不可行。 啟用 EKS 執行期監控之後，在資源佈建步驟完成之前，涵蓋範圍狀態可能保持為 `Unhealthy` 。涵蓋範圍狀態會得到定期監控和更新。
其他（任何其他問題）	由於授權失敗而發生錯誤	切換 EKS 執行期監控以關閉此功能，然後再重新開啟。確定 GuardDuty 代理程式也會透過自動 GuardDuty 或手動部署。

插件創建或更新錯誤	疑難排解步驟
EKS 附加元件問題-`InsufficientNumberOfReplicas` ：附加元件不健康，因為它沒有所需的複本數量。	您可以使用問題訊息識別並修正根本原因。您可以從描述您的叢集開始。例如，用`kubectl describe pods`於識別網繭失敗的根本原因。 修正根本原因之後，請重試該步驟 (建立或更新附加元件)。
EKS 插件問題-`AdmissionRequestDenied` ：入場 webhook `"validate.kyverno.svc-fail"` 拒絕了請求：資源違規策略`DaemonSet/amazon-guardduty/aws-guardduty-agent` :: restrict-image-registries... `autogen-validate-registries`	1. Amazon EKS 叢集或安全管理員必須檢閱封鎖附加元件更新的安全政策。 2. 您必須停用控制器 (webhook) 或讓控制器接受來自 Amazon EKS 的請求。

插件創建或更新錯誤	疑難排解步驟
EKS 插件問題-ConfigurationConflict ：嘗試申請時發現衝突。由於解決衝突模式，將無法繼續。 Conflicts: DaemonSet.apps aws-guardduty-agent - .spec.template.spec.containers[name="aws-guardduty-agent"].image	建立或更新附加元件時，請提供OVERWRITE 解決衝突旗標。這可能會覆寫使用 Kubernetes API 直接對 Kubernetes 中相關資源所做的任何變更。 您可以先刪除插件，然後重新安裝。

EKS 插件問題-AccessDenied: priorityclasses.scheduling.k8s.io "aws-guardduty-agent.priorityclass" is forbidden: User "eks:addon-manager" cannot patch resource "priorityclasses" in API group "scheduling.k8s.io" at the cluster scope	您必須eks:addon-cluster-admin ClusterRoleBinding 手動將缺少的權限新增至。將下列項目新增yaml至eks:addon-cluster-admin ：
	
	`---`
	`kind: ClusterRoleBinding`
	`apiVersion: rbac.authorization.k8s.io/v1`
	`metadata:`
	`  name: eks:addon-cluster-admin`
	`subjects:`
	`- kind: User`
	`  name: eks:addon-manager`
	`  apiGroup: rbac.authorization.k8s.io`
	`roleRef:`
	`  kind: ClusterRole`
	`  name: cluster-admin`
	`  apiGroup: rbac.authorization.k8s.io`
	`---`
	
	現在，您可以使用下列命令yaml將其套用到 Amazon EKS 叢集：
	
	`kubectl apply -f eks-addon-cluster-admin.yaml`

插件創建或更新錯誤	疑難排解步驟
EKS 插件問題-AccessDenied: admission webhook "validation.gatekeeper.sh" denied the request: [all-namespace-must-have-label-owner] All namespaces must have an `owner` label	您必須停用控制器，或讓控制器接受來自 Amazon EKS 叢集的請求。 在建立或更新附加元件之前，您也可以建立 GuardDuty 命名空間並將其標示為owner。

常見問答集 (FAQ)

目錄

為什麼**Unhealthy**即使在啟用執行階段監控、部署 GuardDuty 安全性代理程式並符合所有先決條件之後，我的資源仍會出現涵蓋範圍狀態？

如果您剛部署 GuardDuty 安全代理程式 (透過自動化代理程式設定或手動方式)，或依照建議的步驟來疑難排解涵蓋範圍問題，可能需要幾分鐘的時間才能讓涵蓋範圍狀態變得正常。您可以定期檢查涵蓋範圍狀態，也可以設定 Amazon EventBridge (EventBridge) 以在涵蓋範圍狀態變更時收到通知。

誰可以查看屬於我的資源的運行時覆蓋率狀態 AWS 帳戶？

身為會員帳戶或獨立帳戶，您可以檢視與您自己帳戶相關聯之資源的涵蓋範圍統計資料。身為組織的委派 GuardDuty 系統管理員帳戶，您可以檢視與您帳戶相關聯之資源的涵蓋範圍統計資料，以及屬於您組織的成員帳戶。

設定 CPU 和記憶體監控

啟用「執行階段監視」並評估叢集的涵蓋範圍狀態為「狀況良好」之後，您可以設定並檢視洞察指標。

下列主題可協助您評估已部署的代理程式如何根據 GuardDuty 代理程式的 CPU 和記憶體限制執行。

在 Amazon ECS 叢集上設定監控

Amazon CloudWatch 使用者指南中的以下步驟可協助您評估部署的代理程式如何根據代理程式的 CPU 和記憶體限制執行： GuardDuty

1. 在 Amazon ECS 上設定叢集和服務層級指標的容器洞見
2. Amazon ECS 容器洞察指標

在 Amazon EKS 集群上設置監控

部署 GuardDuty 安全性代理程式並評估叢集的涵蓋範圍狀態為 [狀況良好] 之後，您可以設定並檢視容器洞察指標。

評估安全代理程式的效能

1. 在 Amazon 用戶指南中設置有關 Amazon EKS 和 Kubernetes 的容器洞察 CloudWatch
2. Amazon 用戶指南中的 Amazon EKS 和 Kubernetes 容器洞察指標 CloudWatch

使用安全代理程式 v1.5.0 及更新版本管理效能

透過 Security Agent v1.5.0 及更新版本，當深入解析指出關聯的 GuardDuty 代理程式達到指派的限制時，您可以設定特定參數。如需詳細資訊，請參閱 設定 EKS 附加元件參數。

使用收集的執行階段事 GuardDuty 件類型

Sec GuardDuty urity Agent 會收集下列事件類型，並將它們傳送至後 GuardDuty端進行威脅偵測和分析。 GuardDuty 不會使您可以訪問這些事件。如果 GuardDuty 偵測到潛在威脅並產生「執行階段監控」發現項目，您可以檢視對應的發現項目詳細資料 如需如何 GuardDuty 使用所收集事件類型的詳細資訊，請參閱選擇不使用您的資料以改善服務。

程序事件

欄位名稱	描述
程序名稱	觀察到的程序名稱。
程序路徑	程序可執行檔的絕對路徑。
程序 ID	由作業系統指派給程序的 ID。

欄位名稱	描述
命名空間 PID	主機層級 PID 命名空間以外的次要 PID 命名空間中程序的程序 ID。對於容器內的程序，它是容器內觀察到的程序 ID。
程序使用者 ID	執行程序的使用者 ID。
程序 UUID	由指派給程序的唯一識別碼 GuardDuty。
程序 GID	程序群組的程序 ID。
程序 EGID	程序群組的有效群組 ID。
程序 EUID	程序的有效使用者 ID。
程序使用者名稱	執行程序的使用者名稱。
程序開始時間	程序的建立時間。此欄位是 UTC 日期字串格式 (`2023-03-22T19:37:20.168Z`)。
程序可執行檔 SHA-256	程序可執行檔的 SHA256 雜湊。
程序指令碼路徑	指令碼檔案的執行路徑。
程序環境變數	可供程序使用的環境變數。只會收集 `LD_PRELOAD` 和 `LD_LIBRARY_PATH` 。
程序目前的工作目錄 (PWD)	程序目前的工作目錄。
父程序	父程序的程序詳細資訊。父程序是建立觀察到的程序的程序。

欄位名稱	描述
命令行參數 目前，此欄位僅限於與資源類型對應的特定代理程式版本： • Fargate（僅限 Amazon ECS），具有 1.0.0 版及更高版本的 GuardDuty 安全代理程式。 • 具有 1.0.0 版及以上版本的 GuardDuty 安全代理程式的 Amazon EC2 執行個體。 • 具有安全代理程式 v1.4.0 及以上版本的 Amazon EKS 叢集。 如需詳細資訊，請參閱 GuardDuty 代理程式發行歷。	在進程執行時提供的命令行參數。此欄位可能包含敏感的客戶資料。

容器事件

欄位名稱	描述
容器名稱	容器的名稱。 如果可用，此欄位會顯示標籤 `io.kubenetes.container.name` 的值。
容器 UID	容器執行期所指派容器的唯一 ID。
容器執行期	用於執行容器的容器執行期 (例如 `docker` 或 `containerd`)。
容器映像 ID	容器映像的 ID。
容器映像名稱	容器映像的名稱。

AWS Fargate (僅限 Amazon ECS) 任務事件

欄位名稱	描述
Amazon 任務資源名稱 (ARN)	任務的 ARN。
叢集名稱	Amazon ECS 叢集的名稱。
族群名稱	任務定義的姓氏。作`family`為用來啟動任務之任務定義的名稱使用。
服務名稱	Amazon ECS 服務的名稱 (如果任務是作為服務的一部分啟動)。
啟動類型	您的工作執行所在的基礎結構。對於資源類型為的運行時監視`ECSCluster` ，啟動類型可以是`EC2`或`FARGATE`。
CPU	作業使用的 CPU 單位數目 (如作業定義中所表示)。

Kubernetes Pod 事件

欄位名稱	描述
Pod ID	Kubernetes Pod 的 ID。
Pod 名稱	Kubernetes Pod 的名稱。
Pod 命名空間	Kubernetes 工作負載所屬 Kubernetes 命名空間的名稱。
Kubernetes 叢集名稱	Kubernetes 叢集的名稱。

DNS 事件

欄位名稱	描述
通訊端類型	指出通訊語意的通訊端類型。例如 `SOCK_RAW`。

欄位名稱	描述
地址系列	代表與地址相關聯的通訊協定。例如，地址系列 AF_INET 用於 IP v4 通訊協定。
方向 ID	連線方向的 ID。
通訊協定編號	Layer 4 通訊協定編號，例如 UDP 是 17，TCP 是 6。
DNS 遠端端點 IP	連線的遠端 IP。
DNS 遠端端點連接埠	連線的連接埠號碼。
DNS 本機端點 IP	連線的本機 IP。
DNS 本機端點連接埠	連線的連接埠號碼。
DNS 承載	包含 DNS 查詢和回應的 DNS 封包承載。

開放事件

欄位名稱	描述
檔案路徑	在此事件中開啟的檔案路徑。
旗標	描述檔案存取模式，例如唯讀、唯寫和讀寫。

載入模組事件

欄位名稱	描述
模組名稱	載入核心之模組的名稱。

Mprotect 事件

欄位名稱	描述
地址範圍	修改存取保護的地址範圍。
記憶體區域	指定程序的地址空間區域，如堆疊和堆積。
旗標	代表控制此事件行為的選項。

掛載事件

欄位名稱	描述
掛載目標	掛載來源所在的路徑。
掛載來源	掛載於掛載目標之主機上的路徑。
檔案系統類型	代表掛載的檔案系統的類型。
旗標	代表控制此事件行為的選項。

連結事件

欄位名稱	描述
連結路徑	建立硬連結的路徑。
目標路徑	硬連結指向的檔案路徑。

符號連結事件

欄位名稱	描述
連結路徑	建立符號連結的路徑。

欄位名稱	描述
目標路徑	符號連結指向的檔案路徑。

Dup 事件

欄位名稱	描述
舊檔案描述項	代表開放檔案物件的檔案描述項。
新檔案描述項	新檔案描述項，是舊檔案描述項的重複項。舊的和新的檔案描述項代表相同的開放檔案物件。
Dup 遠端端點 IP	舊檔案描述項所代表網路通訊端的遠端 IP 地址。僅在舊檔案描述項代表網絡通訊端時適用。
Dup 遠端端點連接埠	舊檔案描述項所代表網路通訊端的遠端連接埠。僅在舊檔案描述項代表網絡通訊端時適用。
Dup 本機端點 IP	舊檔案描述項所代表網路通訊端的本機 IP 地址。僅在舊檔案描述項代表網絡通訊端時適用。
Dup 本機端點連接埠	舊檔案描述項所代表網路通訊端的本機連接埠。僅在舊檔案描述項代表網絡通訊端時適用。

記憶體映射事件

欄位名稱	描述
檔案路徑	記憶體所映射至的檔案路徑。

通訊端事件

欄位名稱	描述
地址系列	代表與地址相關聯的通訊協定。例如，地址系列 AF_INET 用於 4 通訊協定的 IP 版本。
通訊端類型	指出通訊語意的通訊端類型。例如 SOCK_RAW。
通訊協定號碼	指定地址系列中的特定通訊協定。通常在地址系列中有單一通訊協定。例如，地址系列 AF_INET 只有 IP 通訊協定。

連接事件

欄位名稱	描述
地址系列	代表與地址相關聯的通訊協定。例如，地址系列 AF_INET 用於 IP v4 通訊協定。
通訊端類型	指出通訊語意的通訊端類型。例如 SOCK_RAW。
通訊協定編號	指定地址系列中的特定通訊協定。通常在地址系列中有單一通訊協定。例如，地址系列 AF_INET 只有 IP 通訊協定。
檔案路徑	如果地址系列是 AF_UNIX，則為通訊端檔案的路徑。
遠端端點 IP	連線的遠端 IP。
遠端端點連接埠	連線的連接埠號碼。
本機端點 IP	連線的本機 IP。
本機端點連接埠	連線的連接埠號碼。

程序 VM Readv 事件

欄位名稱	描述
旗標	代表控制此事件行為的選項。
目標 PID	正在讀取記憶體之程序的程序 ID。
目標程序 UUID	目標程序的唯一 ID。
目標可執行檔路徑	目標程序可執行檔的絕對路徑。

程序 VM Writev 事件

欄位名稱	描述
旗標	代表控制此事件行為的選項。
目標 PID	正在寫入記憶體之程序的程序 ID。
目標程序 UUID	目標程序的唯一 ID。
目標可執行檔路徑	目標程序可執行檔的絕對路徑。

Ptrace 事件

欄位名稱	描述
目標 PID	目標程序的程序 ID。
目標程序 UUID	目標程序的唯一 ID。
目標可執行檔路徑	目標程序可執行檔的絕對路徑。
旗標	代表控制此事件行為的選項。

繫結事件

欄位名稱	描述
地址系列	代表與地址相關聯的通訊協定。例如，地址系列 AF_INET 用於 IP v4 通訊協定。
插座類型	指出通訊語意的通訊端類型。例如 SOCK_RAW。
通訊協定號碼	Layer 4 通訊協定編號，例如 UDP 是 17，TCP 是 6。
本機端點 IP	連線的本機 IP。
本機端點連接埠	連線的連接埠號碼。

聆聽事件

欄位名稱	描述
地址系列	代表與地址相關聯的通訊協定。例如，地址系列 AF_INET 用於 IP v4 通訊協定。
插座類型	指出通訊語意的通訊端類型。例如 SOCK_RAW。
通訊協定號碼	Layer 4 通訊協定編號，例如 UDP 是 17，TCP 是 6。
本機端點 IP	連線的本機 IP。
本機端點連接埠	連線的連接埠號碼。

重命名事件

欄位名稱	描述
檔案路徑	重新命名檔案的路徑。
目標	檔案的新路徑。

設定 UID 事件

欄位名稱	描述
新 EUID	該過程的新有效用戶 ID。
新使用者識別碼	該進程的新用戶 ID。

文件模式活動

欄位名稱	描述
檔案路徑	呼叫此事件的檔案路徑。
檔案模式	關聯檔案的更新存取權限。

Amazon ECR 儲存庫託管代 GuardDuty 理

以下各節列出 Amazon Elastic Container Registry (Amazon ECR) 儲存庫，其中 GuardDuty 託管部署在 Amazon EKS 和 Amazon ECS 叢集上的安全代理程式。

目錄

EKS 代理程式 1.6.0 版或更新版本的儲存庫

下表顯示託管 Amazon EKS 附加代理程式版本 (`aws-guardduty-agent`) 1.6.0 及更新版本的 Amazon ECR 儲存庫，每個儲存庫均適用。 AWS 區域

AWS 區域	Amazon ECR 儲存庫 URI
美國西部 (奧勒岡)	`602401143452.dkr.ecr.us-west-2.amazonaws.com`

AWS 區域	Amazon ECR 儲存庫 URI
Europe (Paris)	602401143452.dkr.ecr.eu-west-3.amazonaws.com
亞太區域 (孟買)	602401143452.dkr.ecr.ap-south-1.amazonaws.com
亞太區域 (海德拉巴)	900889452093.dkr.ecr.ap-south-2.amazonaws.com
加拿大 (中部)	602401143452.dkr.ecr.ca-central-1.amazonaws.com
加拿大西部 (卡加利)	761377655185.dkr.ecr.ca-west-1.amazonaws.com
中東 (阿拉伯聯合大公國)	759879836304.dkr.ecr.me-central-1.amazonaws.com
歐洲 (倫敦)	602401143452.dkr.ecr.eu-west-2.amazonaws.com
歐洲 (愛爾蘭)	602401143452.dkr.ecr.us-west-1.amazonaws.com
美國東部 (維吉尼亞北部)	602401143452.dkr.ecr.us-east-1.amazonaws.com
美國東部 (俄亥俄)	602401143452.dkr.ecr.us-east-2.amazonaws.com
歐洲 (愛爾蘭)	602401143452.dkr.ecr.eu-west-1.amazonaws.com
南美洲 (聖保羅)	602401143452.dkr.ecr.sa-east-1.amazonaws.com
歐洲 (斯德哥爾摩)	602401143452.dkr.ecr.eu-north-1.amazonaws.com
歐洲 (法蘭克福)	602401143452.dkr.ecr.eu-central-1.amazonaws.com
歐洲 (蘇黎世)	900612956339.dkr.ecr.eu-central-2.amazonaws.com
亞太區域 (新加坡)	602401143452.dkr.ecr.ap-southeast-1.amazonaws.com

AWS 區域	Amazon ECR 儲存庫 URI
亞太區域 (悉尼)	602401143452.dkr.ecr.ap-southeast-2.amazonaws.com
亞太區域 (雅加達)	296578399912.dkr.ecr.ap-southeast-3.amazonaws.com
亞太區域 (東京)	602401143452.dkr.ecr.ap-northeast-1.amazonaws.com
亞太區域 (首爾)	602401143452.dkr.ecr.ap-northeast-2.amazonaws.com
亞太區域 (大阪)	602401143452.dkr.ecr.ap-northeast-3.amazonaws.com
亞太區域 (香港)	800184023465.dkr.ecr.ap-east-1.amazonaws.com
Middle East (Bahrain)	759879836304.dkr.ecr.me-south-1.amazonaws.com
歐洲 (米蘭)	590381155156.dkr.ecr.eu-south-1.amazonaws.com
歐洲 (西班牙)	455263428931.dkr.ecr.eu-south-2.amazonaws.com
非洲 (開普敦)	877085696533.dkr.ecr.af-south-1.amazonaws.com
亞太區域 (墨爾本)	491585149902.dkr.ecr.ap-southeast-4.amazonaws.com
以色列 (特拉維夫)	066635153087.dkr.ecr.il-central-1.amazonaws.com

EKS 代理程式 1.5.0 版及更早版本的儲存庫

下表顯示託管 Amazon EKS 附加元件代理程式版本 (aws-guardduty-agent) 1.5.0 及更早版本的 Amazon ECR 儲存庫。 AWS 區域

AWS 區域	Amazon ECR 儲存庫 URI
美國西部 (奧勒岡)	039403964562.dkr.ecr.us-west-2.amazonaws.com

AWS 區域	Amazon ECR 儲存庫 URI
Europe (Paris)	113643092156.dkr.ecr.eu-west-3.amazonaws.com
亞太區域 (孟買)	610108029387.dkr.ecr.ap-south-1.amazonaws.com
亞太區域 (海德拉巴)	618745550137.dkr.ecr.ap-south-2.amazonaws.com
加拿大 (中部)	001188825231.dkr.ecr.ca-central-1.amazonaws.com
中東 (阿拉伯聯合大公國)	601769779514.dkr.ecr.me-central-1.amazonaws.com
歐洲 (倫敦)	109118265657.dkr.ecr.eu-west-2.amazonaws.com
歐洲 (愛爾蘭)	373421517865.dkr.ecr.us-west-1.amazonaws.com
美國東部 (維吉尼亞北部)	031903291036.dkr.ecr.us-east-1.amazonaws.com
美國東部 (俄亥俄)	591382732059.dkr.ecr.us-east-2.amazonaws.com
歐洲 (愛爾蘭)	673884943994.dkr.ecr.eu-west-1.amazonaws.com
南美洲 (聖保羅)	941219317354.dkr.ecr.sa-east-1.amazonaws.com
歐洲 (斯德哥爾摩)	366771026645.dkr.ecr.eu-north-1.amazonaws.com
歐洲 (法蘭克福)	409493279830.dkr.ecr.eu-central-1.amazonaws.com
歐洲 (蘇黎世)	718440343717.dkr.ecr.eu-central-2.amazonaws.com
亞太區域 (新加坡)	584580519942.dkr.ecr.ap-southeast-1.amazonaws.com
亞太區域 (悉尼)	011662287384.dkr.ecr.ap-southeast-2.amazonaws.com

AWS 區域	Amazon ECR 儲存庫 URI
亞太區域 (雅加達)	617474730032.dkr.ecr.ap-southeast-3.amazonaws.com
亞太區域 (東京)	781592569369.dkr.ecr.ap-northeast-1.amazonaws.com
亞太區域 (首爾)	732248494576.dkr.ecr.ap-northeast-2.amazonaws.com
亞太區域 (大阪)	810724417379.dkr.ecr.ap-northeast-3.amazonaws.com
亞太區域 (香港)	790429075973.dkr.ecr.ap-east-1.amazonaws.com
Middle East (Bahrain)	541829937850.dkr.ecr.me-south-1.amazonaws.com
歐洲 (米蘭)	528450769569.dkr.ecr.eu-south-1.amazonaws.com
歐洲 (西班牙)	531047660167.dkr.ecr.eu-south-2.amazonaws.com
非洲 (開普敦)	379032919888.dkr.ecr.af-south-1.amazonaws.com
亞太區域 (墨爾本)	750462861327.dkr.ecr.ap-southeast-4.amazonaws.com
以色列 (特拉維夫)	292660727137.dkr.ecr.il-central-1.amazonaws.com

用於 GuardDuty 代理程式的儲存庫 AWS Fargate (僅限 Amazon ECS)

下表顯示 GuardDuty 代理程式託管每個儲存庫 AWS Fargate (僅限 Amazon ECS) 的 Amazon ECR 儲存庫。 AWS 區域

AWS 區域	Amazon ECR 儲存庫 URI
美國西部 (奧勒岡)	733349766148.dkr.ecr.us-west-2.amazonaws.com/aws-guardduty-agent-fargate

AWS 區域	Amazon ECR 儲存庫 URI
Europe (Paris)	665651866788.dkr.ecr.eu-west-3.amazonaws.com/aws-guardduty-agent-fargate
亞太區域 (孟買)	251508486986.dkr.ecr.ap-south-1.amazonaws.com/aws-guardduty-agent-fargate
亞太區域 (海德拉巴)	950823858135.dkr.ecr.ap-south-2.amazonaws.com/aws-guardduty-agent-fargate
加拿大 (中部)	354763396469.dkr.ecr.ca-central-1.amazonaws.com/aws-guardduty-agent-fargate
中東 (阿拉伯聯合大公國)	000014521398.dkr.ecr.me-central-1.amazonaws.com/aws-guardduty-agent-fargate
歐洲 (倫敦)	892757235363.dkr.ecr.eu-west-2.amazonaws.com/aws-guardduty-agent-fargate
歐洲 (愛爾蘭)	684579721401.dkr.ecr.us-west-1.amazonaws.com/aws-guardduty-agent-fargate
美國東部 (維吉尼亞北部)	593207742271.dkr.ecr.us-east-1.amazonaws.com/aws-guardduty-agent-fargate
美國東部 (俄亥俄)	307168627858.dkr.ecr.us-east-2.amazonaws.com/aws-guardduty-agent-fargate
歐洲 (愛爾蘭)	694911143906.dkr.ecr.eu-west-1.amazonaws.com/aws-guardduty-agent-fargate
南美洲 (聖保羅)	758426053663.dkr.ecr.sa-east-1.amazonaws.com/aws-guardduty-agent-fargate
歐洲 (斯德哥爾摩)	591436053604.dkr.ecr.eu-north-1.amazonaws.com/aws-guardduty-agent-fargate
歐洲 (法蘭克福)	323658145986.dkr.ecr.eu-central-1.amazonaws.com/aws-guardduty-agent-fargate

AWS 區域	Amazon ECR 儲存庫 URI
歐洲 (蘇黎世)	529164026651.dkr.ecr.eu-central-2.amazonaws.com/aws-guardduty-agent-fargate
亞太區域 (新加坡)	174946120834.dkr.ecr.ap-southeast-1.amazonaws.com/aws-guardduty-agent-fargate
亞太區域 (悉尼)	005257825471.dkr.ecr.ap-southeast-2.amazonaws.com/aws-guardduty-agent-fargate
亞太區域 (雅加達)	510637619217.dkr.ecr.ap-southeast-3.amazonaws.com/aws-guardduty-agent-fargate
亞太區域 (東京)	533107202818.dkr.ecr.ap-northeast-1.amazonaws.com/aws-guardduty-agent-fargate
亞太區域 (首爾)	914738172881.dkr.ecr.ap-northeast-2.amazonaws.com/aws-guardduty-agent-fargate
亞太區域 (大阪)	273192626886.dkr.ecr.ap-northeast-3.amazonaws.com/aws-guardduty-agent-fargate
亞太區域 (香港)	258348409381.dkr.ecr.ap-east-1.amazonaws.com/aws-guardduty-agent-fargate
Middle East (Bahrain)	536382113932.dkr.ecr.me-south-1.amazonaws.com/aws-guardduty-agent-fargate
歐洲 (米蘭)	266869475730.dkr.ecr.eu-south-1.amazonaws.com/aws-guardduty-agent-fargate
歐洲 (西班牙)	919611009337.dkr.ecr.eu-south-2.amazonaws.com/aws-guardduty-agent-fargate
非洲 (開普敦)	197869348890.dkr.ecr.af-south-1.amazonaws.com/aws-guardduty-agent-fargate
亞太區域 (墨爾本)	251357961535.dkr.ecr.ap-southeast-4.amazonaws.com/aws-guardduty-agent-fargate

AWS 區域	Amazon ECR 儲存庫 URI
以色列 (特拉維夫)	`870907303882.dkr.ecr.il-central-1.amazonaws.com/aws-guardduty-agent-fargate`

GuardDuty 代理程式發行歷

以下各節提供部署在 Amazon EC2 執行個體、Amazon ECS 叢集和 Amazon EKS 叢集上的 GuardDuty 代理程式的發行版本

GuardDuty Amazon EC2 執行個體的安全代理

代理程式版本	版本備註	可用日期
v1.1.0	在 Amazon EC2 執行個體的執行階段監控中支援 GuardDuty 自動代理程式組態 支援宣布 EC2 執行個體執行時期監控正式推出的新安全訊號和發現項目。 一般性能改善。	2024年3月26日
V1.0.2	支援最新的 Amazon ECS AMI。	2024年2月2日
V1.0.1	一般效能調整和增強功能 在 1.0.2 版之前發行的代理程式版本與 2024 年 1 月 31 日之後推出的 Amazon ECS AMI 不相容。	2024 年 1 月 23 日
v1.0.0	RPM 安裝的初始發行版本。 在 1.0.2 版之前發行的代理程式版本與 2024 年 1 月 31 日之	2023 年 11 月 26 日

代理程式版本	版本備註	可用日期
	後推出的 Amazon ECS AMI 不相容。	

公開金鑰、x86_64 RPM 的簽章、arm64 RPM 的簽章，以及 Amazon S3 儲存貯體中託管之 RPM 指令碼的對應存取連結，都可以從下列範本形成。取代 AWS 區域、 AWS 帳號識別碼和 GuardDuty 代理程式版本的值，以存取 RPM 指令碼。下列範本包含適用於 Amazon EC2 執行個體的最新代理程式版本。

- 公開金鑰：

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/publickey.pem
```

- GuardDuty 安全代理程式 RPM 簽章：

  64 轉速的簽名

  ```
  s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/x86_64/amazon-guardduty-agent-1.1.0.x86_64.sig
  ```

  臂 64 轉速簽名

  ```
  s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/arm64/amazon-guardduty-agent-1.1.0.arm64.sig
  ```

- 存取 Amazon S3 儲存貯體中 RPM 指令碼的連結：

  存取 64 轉速的連結

  ```
  s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/x86_64/amazon-guardduty-agent-1.1.0.x86_64.rpm
  ```

  ARM64 轉速的存取連結

  ```
  s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/arm64/amazon-guardduty-agent-1.1.0.arm64.rpm
  ```

AWS 區域	區域名稱	AWS 帳號識別碼
eu-west-1	歐洲 (愛爾蘭)	694911143906
us-east-1	美國東部 (維吉尼亞北部)	593207742271
us-east-2	美國東部 (俄亥俄)	733349766148
eu-west-3	Europe (Paris)	665651866788
us-east-2	美國東部 (俄亥俄)	307168627858
eu-central-1	歐洲 (法蘭克福)	323658145986
ap-northeast-2	亞太區域 (首爾)	914738172881
eu-north-1	歐洲 (斯德哥爾摩)	591436053604
ap-east-1	亞太區域 (香港)	258348409381
me-south-1	Middle East (Bahrain)	536382113932
eu-west-2	歐洲 (倫敦)	892757235363
ap-northeast-1	亞太區域 (東京)	533107202818
ap-southeast-1	亞太區域 (新加坡)	174946120834
ap-south-1	亞太區域 (孟買)	251508486986
ap-southeast-3	亞太區域 (雅加達)	510637619217
sa-east-1	南美洲 (聖保羅)	758426053663
ap-northeast-3	亞太區域 (大阪)	273192626886
eu-south-1	歐洲 (米蘭)	266869475730
af-south-1	非洲 (開普敦)	197869348890
ap-southeast-2	亞太區域 (悉尼)	005257825471

me-central-1	中東 (阿拉伯聯合大公國)	000014521398
us-west-1	美國西部 (加利佛尼亞北部)	684579721401
ca-central-1	加拿大 (中部)	354763396469
ap-south-2	亞太區域 (海德拉巴)	950823858135
eu-south-2	歐洲 (西班牙)	919611009337
eu-central-2	歐洲 (蘇黎世)	529164026651
ap-southeast-4	亞太區域 (墨爾本)	251357961535
il-central-1	以色列 (特拉維夫)	870907303882

GuardDuty 適用的安全代理程式 AWS Fargate (僅限 Amazon ECS)

下表顯示 Fargate GuardDuty 安全代理程式的發行版本歷史記錄 (僅限 Amazon ECS)。

代理程式版本	容器映像	版本備註	可用日期
v1.2.0	x86_64 (AMD64)：sha256:1dbad20ac2dc66d52d00bb28dde4281fe0d3c5f261b1649b247c2369d9e26b93 Graviton (ARM64): sha256:91930f8446f5f95b93b8ccb18773992affa401eb3f42da89d68077a56bafa6cd	一般效能調整和增強功能	2024年5月31 日
v1.1.0	x86_64 (AMD64)：sha256:83ce3cf2ef85a349ed1797a8cf30a008ac5d8c	支援新的安全訊號和發現 一般效能調整和增強功能	2024年5月01 日

代理程式版本	容器映像	版本備註	可用日期
	9f673f2835823957e9dcf71657 Graviton (ARM64): sha256:0d4b61648d7bdeab8ab8d94684f805498927c7d437d318204dcccfe8c9383dc7		
V1.0.1	x86_64 (AMD64)：sha256:9f8cd438fb66f62d09bfc641286439f7ed5177988a314a6021ef4ff880642e68 Graviton (ARM64): sha256:82c66bb615bd0d1e96db77b1f1fb51dc03220caa593b1962249571bf7147d1b7	一般效能調整和增強功能	2024年1月26日
v1.0.0	x86_64 (AMD64)：sha256:359b8b014e5076c625daa1056090e522631587a7afa3b2e055edda6bd1141017 Graviton (ARM64): sha256:b9438690fa8a86067180a11658bec0f4f838ae3fbd225d04b9306250648b3984	初始版本的 GuardDuty 安全代理程式 AWS Fargate (僅適用於 Amazon ECS)。	2023 年 11 月 26 日

GuardDuty Amazon EKS 叢集的安全代理程式

下表顯示 Amazon EKS 附加元件 GuardDuty 代理程式的發行版本歷史記錄。

代理程式版本	容器映像	版本備註	可用日期	標準支援結束[1]
v1.6.1	x86_64 (AMD64)：sha256:30650708a6601f6d6b9046f54b30f5fd65af296b1e40b8c24426b9bdb07c3ab1 Graviton (ARM64): sha256:5f637c42ffb306b20f776d9d83e1e0b4be40ce245be44afcf43a8902b4d71019	一般性能調整和增強功能。	2024 年 5 月 14 日	–
v1.6.0	x86_64 (AMD64)：sha256:7dabcbee30d8b053676752fbc19e89f77272d9a6a53cc93731f5872180ef9010 Graviton (ARM64): sha256:9710f53afccdf4f22b265a1a6fc27f1469403af1f7d5d08c4869a7269cdd2650	• 支援 EKS/EC2 資源的 GuardDuty 自動化代理程式組態。 • 支持新的安全信號和發現。如需詳細資訊，請參閱 使用收集的執行階段事 GuardDuty 件類型 及 執行階段監視尋找項。 • 一般性能調整和增強功能。	2024年4月29日	–

代理程式版本	容器映像	版本備註	可用日期	標準支援結束[1]
V1.5.0	x86_64 (AMD64)：sha256:e09a4e70af4058a212f172cc8eb3fc23ad9bed547ed609faa2bb82cf7cc5532d Graviton (ARM64): sha256:afc9a3f8f17ae12499d76069efcf1b46271a5a4b2b3f6ba5de54637b8f55d5c6	• 一般性能調整和增強功能。 • 安全增強功能，包括下的新事件類型收集的執行期事件類型。 • CPU 使用率的效能增強功能。	2024年3月7日	–
v1.4.1	x86_64 (AMD64)：sha256:66d491927763742660faa87cc2c39bb97b7873039157ae8b90bc999cb73d0b9c Graviton (ARM64): sha256:537a330b2dd82357024fb6daeb8761034b7defd43b10dffe0792c9e6d0778b40	一般性能調整和增強功能。	2024年1月16日	–

代理程式版本	容器映像	版本備註	可用日期	標準支援結束[1]
V1.4.0	x86_64 (AMD64)：sha256:848ce13d9430bad554ac23d4699551505326ada2a88e1a721fe9f86b56b52c0f Graviton (ARM64): sha256:0c650aeafeeb5f2bcb8b989ac849bedc1fae1a4de1cf6306ffdd9c6aebe67f8e	清單掛載點支持更好的數據收集 AppArmor 清單中的配置 收集命令行參數 一般效能調整和增強功能	2023 年 12 月 21 日	–
v1.3.1	x86_64 (AMD64)：sha256:55578fcb7b73097ade5c8404390ef16cf76a7b568490abaae01ac75992b3ea29 Graviton (ARM64): sha256:e3ce8d66ac2121f8d476eb58f8bc50ab51336647615eb7cf514c21421cb818fd	重要的安全修補程式和更新。	2023 年 10 月 23 日	–

代理程式版本	容器映像	版本備註	可用日期	標準支援結束[1]
v1.3.0	x86_64 (AMD64)：sha256:6dace2337dfbb7609811be89fb4b23ae0b865f1027ad78fbe69530bfbd46c694 Graviton (ARM64): sha256:4928a7c6ef40e77c8ec95841323bb9a110db31f12c0ee7ab965e08b43efd01bb	支援 Ubuntu 平台 支援 Kubernetes 1.28 版 一般效能增強功能和穩定性改進。	2023 年 10 月 5 日	–
v1.2.0	x86_64 (AMD64)：sha256:d610413d662ec042057f05d6942496d7f2c08e9f5a077ea307ffdb5d3f11bcc3 Graviton (ARM64): sha256:174d7ab28b2f95e5309da80d95b88ad26f602dfe72c2b351a0ef9297a1412bfa	除了以 AMD64 為基礎的執行個體之外，v1.2.0 現在也支援以 ARM64 為基礎的執行個體。新增並驗證了對 Bottlerocket 的支援 支援 Kubernetes 1.27 版 一般性能增強功能和穩定性改進。	2023 年 6 月 16 日	–

代理程式版本	容器映像	版本備註	可用日期	標準支援結束 [1]
v1.1.0	sha256:b19ba3a3c1a508d153263ae2fda891a7928b5ca9b3a5692db6c101829303281c	除了 安全性代理程式支援的 Kubernetes 版本 GuardDuty 之外，此代理程式版本也支援 Kubernetes 1.26 版。 一般性能增強功能和穩定性改進。	2023 年 5 月 2 日	2024 年 5 月 14 日
v1.0.0	sha256:e38bdd2b1323e89113f1a31bd4bc8e5a8098525dd98e6981a28b9906b1e4411e	Amazon EKS 附加元件代理程式的初始版本。	2023 年 3 月 30 日	2024 年 5 月 14 日

- [1] 如需更新接近標準支援結束之目前代理程式版本的相關資訊，請參閱手動更新安全代理。

停用及清理資源的影響

AWS 帳戶 如果您選擇停用「執行階段監視」，或僅停用某個資源類型的 GuardDuty 自動代理程式組態，則此區段適用於您的。

停用 GuardDuty 自動化代理程式

GuardDuty 不會移除資源上部署的安全性代理程式。不過， GuardDuty 將停止管理安全性代理程式的更新。

GuardDuty 繼續從您的資源類型接收運行時事件。若要避免影響您的使用統計資料，請務必從資源中移除 GuardDuty Security Agent。

無論是否 AWS 帳戶 使用共用 VPC 端點，都不 GuardDuty 會刪除 VPC 端點。如果需要，您將需要手動刪除 VPC 端點。

停用執行階段監視和 EKS 執行階段監視

在下列情況下，本節適用於您：

- 您從未單獨啟用 EKS 運行時監視，現在您禁用了運行時監視。
- 您正在禁用運行時監視和 EKS 運行時監視。如果您不確定 EKS 執行階段監視的組態狀態，請參閱檢查 EKS 執行階段監視組態狀態。

如果先前列出的案例適用於您，則 GuardDuty 會在您的帳戶中採取下列動作：

- GuardDuty 刪除具有`GuardDutyManaged:true`標籤的 VPC。這是為 GuardDuty 了管理自動安全代理程式而建立的 VPC。
- GuardDuty 刪除標記為`GuardDutyManaged`：的安全性群組`true`。
- 對於至少一個參與者帳戶使用的共用 VPC，則 GuardDuty 不會刪除 VPC 端點和與共用 VPC 資源相關聯的安全性群組。
- 對於 Amazon EKS 資源，請 GuardDuty 刪除安全代理程式。這與手動管理還是通過管理無關 GuardDuty。

  對於 Amazon ECS 資源，因為 ECS 任務是不可變的，因此 GuardDuty 無法從該資源解除安裝安全代理程式。這與您透過手動或自動管理安全代理程式的方式無關 GuardDuty。停用執行階段監控之後，當新的 ECS 工作開始執行時， GuardDuty 將不會附加附加附加容器。如需使用 Fargate 端 ECS 工作的相關資訊，請參閱。運行時監控如何與 Fargate 一起工作（僅限 Amazon ECS）

  對於 Amazon EC2 資源，只有在符合下列條件時，才從所有 Systems Manager (SSM) 受管的 Amazon EC2 執行個體 GuardDuty 解除安裝安全代理程式：

  - 您的資源未標記為`GuardDutyManaged:false`排除標籤。
  - GuardDuty 必須具有存取執行個體中繼資料中標籤的權限。對於此 EC2 資源，執行個體中繼資料中的標籤存取設定為 [允許]。

當您停止手動管理安全代理程式時

無論您使用哪種方法來部署和管理 GuardDuty 安全代理程式，若要停止監視資源中的執行階段事件，您都必須移除 GuardDuty 安全代理程式。當您想要停止監控帳戶中資源類型的執行階段事件時，也可以刪除 Amazon VPC 端點。

清理安全代理程式資源的程序

刪除 Amazon VPC 端點

- 如果沒有共用 VPC — 如果您不想再監控帳戶中的資源，請考慮刪除 Amazon VPC 端點。
- 使用共用 VPC — 當共用 VPC 擁有者帳戶刪除仍在使用中的共用 VPC 資源時，共用 VPC 擁有者帳戶和參與帳戶中資源的執行階段監視 (以及適用時，EKS Runtime Monitoring) 涵蓋範圍狀態可能會變得不健康。如需涵蓋範圍狀態的資訊，請參閱評估資源的執行階段涵蓋範圍。

如需詳細資訊，請參閱建立介面端點。

若要刪除安全性群組

- 沒有共用 VPC — 如果您不想再監控帳戶中的資源類型，請考慮刪除與 Amazon VPC 關聯的安全群組。
- 使用共用 VPC — 當共用 VPC 擁有者帳戶刪除安全性群組時，目前正在使用與共用 VPC 關聯之安全性群組的任何參與者帳戶，共用 VPC 擁有者帳戶中資源的執行階段監視涵蓋範圍狀態可能會變得不健康。如需詳細資訊，請參閱 評估資源的執行階段涵蓋範圍。

如需詳細資訊，請參閱刪除安全性群組。

從 EKS 叢集移除 GuardDuty 安全代理程式

若要從您不想再監視的 EKS 叢集中移除安全性代理程式，請參閱刪除附加元件。

移除 EKS 附加元件代理程式並不會從 EKS 叢集中移除 `amazon-guardduty` 命名空間。若要刪除 `amazon-guardduty` 命名空間，請刪除命名空間。

若要刪除命**`amazon-guardduty`**名空間 (EKS 叢集)

停用自動化代理程式組態並不會自動從 EKS 叢集移除`amazon-guardduty`命名空間。若要刪除 `amazon-guardduty` 命名空間，請刪除命名空間。

Amazon S3 保護在 Amazon GuardDuty

S3 保護可協助 Amazon GuardDuty 監控 Amazon Simple Storage Service (Amazon S3) 的 AWS CloudTrail 資料事件，其中包括物件層級 API 操作，以識別 Amazon S3 儲存貯體中資料的潛在安全風險。

GuardDuty 同時監控 AWS CloudTrail 管理事件和 AWS CloudTrail S3 資料事件，以識別 Amazon S3 資源中的潛在威脅。這兩個資料來源會監控不同類型的活動。S3 的 CloudTrail 管理事件範例包括列出或設定 Amazon S3 儲存貯體的操作`ListBuckets`，例如`DeleteBuckets`、和`PutBucketReplication`。S3 的 CloudTrail 資料事件範例包括物件層級 API 操作，例如`GetObjectListObjects`、`DeleteObject`、和`PutObject`。

當您啟用 Amazon GuardDuty 的時候 AWS 帳戶， GuardDuty 開始監視 CloudTrail 管理事件。您不需要手動啟用或設定 S3 資料事件登入 AWS CloudTrail。您可以隨時針對 Amazon GuardDuty 內部提供此功能的任何帳戶啟用 S3 保護功能 (用於監控 S3 的 CloudTrail 資料事件)。 AWS 區域 AWS 帳戶 已啟用的 GuardDuty，可以在 30 天免費試用期內首次啟用 S3 保護。對於首次啟 AWS 帳戶 GuardDuty 用的，S3 保護已啟用並包含在此 30 天免費試用中。如需詳細資訊，請參閱 估算成 GuardDuty 本。

我們建議您在中啟用 S3 保護 GuardDuty。如果未啟用此功能， GuardDuty 將無法完全監控 Amazon S3 儲存貯體，或產生存放在 S3 儲存貯體中資料的可疑存取的發現結果。

如何 GuardDuty 使用 S3 資料事件

啟用 S3 資料事件 (S3 防護) 時，會 GuardDuty 開始分析所有 S3 儲存貯體中的 S3 資料事件，並監控它們是否有惡意和可疑活動。如需詳細資訊，請參閱 AWS CloudTrail S3 的資料事件。

當未經驗證的使用者存取 S3 物件時，表示 S3 物件可公開存取。因此， GuardDuty不會處理此類要求。 GuardDuty 使用有效的 IAM (AWS Identity and Access Management) 或 AWS STS () 登入資料處理對 S3 物件發出的請求。AWS Security Token Service

當根據 S3 資料事件監控 GuardDuty 偵測到潛在威脅時，會產生安全性發現。如需 GuardDuty 可針對 Amazon S3 儲存貯體產生之發現項目類型的相關資訊，請參閱GuardDuty S3 尋找項目類型。

如果停用 S3 保護，請 GuardDuty 停止對 S3 儲存貯體中存放的資料進行 S3 資料事件監控。

為獨立帳戶設定 S3 保護

對於與之關聯的帳戶 AWS Organizations，可透過主控台設定自動執行此程序。如需詳細資訊，請參閱在多帳戶環境中設定 S3 保護。

啟用或停用 S3 保護

選擇您偏好的存取方式，為獨立帳戶設定 S3 保護。

Console

1. 請登入 AWS Management Console 並開啟 GuardDuty 主控台，網址為 https://console.aws.amazon.com/guardduty/。
2. 在導覽窗格中，選擇 S3 保護。
3. S3 保護頁面為您的帳戶提供 S3 保護的目前狀態。選擇啟用或停用可隨時啟用或停用 S3 保護。
4. 選擇確認以確認您選取的項目。

API/CLI

1. 使用目前區域的有效偵測器 ID，並將 `features` 物件 `name` 以 `S3_DATA_EVENTS` 設定為 `ENABLED` 或 `DISABLED` 來傳遞，進而執行 updateDetector，以分別啟用或停用 S3 保護。

   > **Note**
   >
   > 要查找您`detectorId`的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

2. 或者，您可以使用 AWS Command Line Interface. 若要啟用 S3 保護，請執行下列命令，並確保使用您自己的有效偵測器 ID。

   ```
   aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
   features '[{"Name" : "S3_DATA_EVENTS", "Status" : "ENABLED"}]'
   ```

   若要停用 S3 保護，請使用 `DISABLED` 取代範例中的 `ENABLED`。

在多帳戶環境中設定 S3 保護

在多帳戶環境中，只有委派的 GuardDuty 管理員帳戶可以選擇為其 AWS 組織中的成員帳戶設定 (啟用或停用) S3 Protection。成 GuardDuty 員帳戶無法從其帳戶修改此設定。委派的管理 GuardDuty 員帳戶會使用來管理其成員帳戶 AWS Organizations。委派的 GuardDuty 管理員帳戶可以選擇在所有帳戶

上自動啟用 S3 Protection，只有新帳戶或組織中不啟用任何帳戶。如需詳細資訊，請參閱 透過 AWS Organizations管理帳戶。

為委派的 GuardDuty 管理員帳戶設定 S3 保護

選擇您偏好的存取方法，為委派的 GuardDuty 管理員帳戶設定 S3 保護。

Console

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/

   確保使用管理帳戶憑證。
2. 在導覽窗格中，選擇 S3 保護。
3. 在 S3 保護頁面上，選擇編輯。
4. 執行以下任意一項：

   使用為所有帳戶啟用

   - 選擇為所有帳戶啟用。這將啟用 AWS 組織中所有作用中 GuardDuty 帳戶的保護計劃，包括加入組織的新帳戶。
   - 選擇儲存。

   使用手動設定帳戶

   - 若要僅針對委派的 GuardDuty 系統管理員帳戶啟用保護方案，請選擇 [手動設定帳戶]。
   - 在 [委派 GuardDuty 管理員帳戶 (此帳戶)] 區段下選擇 [啟用]。
   - 選擇儲存。

API/CLI

updateDetector透過針對目前區域使用委派 GuardDuty 管理員帳戶的偵測器 ID 執行，並name以S3_DATA_EVENTSENABLED或傳遞features物件的方status式執行DISABLED。

或者，您可以使用 AWS Command Line Interface. *########## 12abc34d567e8fa901bc2d34e56789f0 ########################## 555555555555 ################ GuardDuty* AWS 帳戶 GuardDuty

要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

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

為組織中的所有成員帳戶自動啟用 S3 保護

Console

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/

   使用您的系統管理員帳戶登入。

2. 執行以下任意一項：

   使用 S3 保護頁面

   1. 在導覽窗格中，選擇 S3 保護。
   2. 選擇為所有帳戶啟用。此動作會自動為組織中的現有帳戶和新帳戶啟用 S3 保護。
   3. 選擇儲存。

   > **Note**
   >
   > 最多可能需要 24 小時才會更新成員帳戶的組態。

   使用帳戶頁面

   1. 在導覽窗格中，選擇帳戶。
   2. 在帳戶頁面上，選擇自動啟用偏好設定，然後再透過邀請新增帳戶。
   3. 在管理自動啟用偏好設定視窗中，選擇 S3 保護下的為所有帳戶啟用。
   4. 選擇儲存。

   如果您無法使用為所有帳戶啟用選項，請參閱 選擇性地啟用或停用成員帳戶中的 S3 保護。

API/CLI

- 若要為您的成員帳戶選擇性地啟用或停用 S3 保護，請使用您自己的*### ID* 調用 updateMemberDetectors API 操作。
- 以下範例顯示如何為單一成員帳戶啟用 S3 保護。*################## 111122223 333 # ##detector-id GuardDuty* 若要停用 S3 保護，請使用 DISABLED 取代 ENABLED。

  要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"name": "S3_DATA_EVENTS", "status": "ENABLED"}]'
  ```

  > **Note**
  >
  > 您也可以傳遞以空格分隔的帳戶 ID 清單。

- 當程式碼成功執行時，會返回一個空白 UnprocessedAccounts 清單。如果變更帳戶的偵測器設定時發生任何問題，則會列出該帳戶 ID 以及問題摘要。

為所有現有作用中成員帳戶啟用 S3 保護

選擇您偏好的存取方式，為組織中的所有現有作用中成員帳戶啟用 S3 保護。

Console

1. 請登入 AWS Management Console 並開啟 GuardDuty 主控台，網址為 https://console.aws.amazon.com/guardduty/。

   使用委派的 GuardDuty 系統管理員帳戶認證登入。
2. 在導覽窗格中，選擇 S3 保護。
3. 在 S3 保護頁面上，您可以檢視組態的目前狀態。在作用中成員帳戶區段下，選擇動作。
4. 從動作下拉式選單中，選擇為所有作用中的成員帳戶啟用。
5. 選擇確認。

API/CLI

- 若要為您的成員帳戶選擇性地啟用或停用 S3 保護，請使用您自己的*### ID* 調用 updateMemberDetectors API 操作。
- 以下範例顯示如何為單一成員帳戶啟用 S3 保護。*################## 111122223 333 # ##detector-id GuardDuty* 若要停用 S3 保護，請使用 DISABLED 取代 ENABLED。

  要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"name": "S3_DATA_EVENTS", "status": "ENABLED"}]'
  ```

  > **Note**
  >
  > 您也可以傳遞以空格分隔的帳戶 ID 清單。

- 當程式碼成功執行時，會返回一個空白 UnprocessedAccounts 清單。如果變更帳戶的偵測器設定時發生任何問題，則會列出該帳戶 ID 以及問題摘要。

為新成員帳戶自動啟用 S3 保護

選擇您偏好的存取方式，為加入組織的新帳戶啟用 S3 保護。

Console

委派的 GuardDuty 管理員帳戶可以使用 S3 Protection 或帳戶頁面，透過主控台為組織中的新成員帳戶啟用。

為新成員帳戶自動啟用 S3 保護

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/

   請務必使用委派的 GuardDuty 系統管理員帳戶認證。
2. 執行以下任意一項：
   - 使用 S3 保護頁面：

     1. 在導覽窗格中，選擇 S3 保護。

2. 在 S3 保護頁面上，選擇編輯。
3. 選擇手動設定帳戶。
4. 選取為新成員帳戶自動啟用。此步驟可確保每當有新帳戶加入您的組織時，S3 保護都會自動為其帳戶啟用。只有組織委派的 GuardDuty 管理員帳戶可以修改此組態。
5. 選擇儲存。

- 使用帳戶頁面：

1. 在導覽窗格中，選擇帳戶。
2. 在帳戶頁面上，選擇自動啟用偏好設定。
3. 在管理自動啟用偏好設定視窗中，選擇 S3 保護下的為新帳戶啟用。
4. 選擇儲存。

API/CLI

- 若要為您的成員帳戶選擇性地啟用或停用 S3 保護，請使用您自己的*### ID* 調用 UpdateOrganizationConfiguration API 操作。
- 以下範例顯示如何為單一成員帳戶啟用 S3 保護。若要停用，請參閱選擇性地為成員帳戶啟用或停用 RDS 保護。設定偏好設定，以在該區域中為加入組織的新帳戶 (NEW)、所有帳戶 (ALL) 或非組織帳戶 (NONE) 自動啟用或停用保護計畫。如需詳細資訊，請參閱autoEnableOrganization成員。根據您的偏好設定，您可能需要使用 ALL 或 NONE 取代 NEW。

  要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name":
 "S3_DATA_EVENTS", "autoEnable": "NEW"}]'
```

> **Note**
>
> 您也可以傳遞以空格分隔的帳戶 ID 清單。

- 當程式碼成功執行時，會返回一個空白 UnprocessedAccounts 清單。如果變更帳戶的偵測器設定時發生任何問題，則會列出該帳戶 ID 以及問題摘要。

選擇性地啟用或停用成員帳戶中的 S3 保護

選擇您偏好的存取方式，選擇性地為成員帳戶啟用或停用 S3 保護。

Console

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/

   請務必使用委派的 GuardDuty 系統管理員帳戶認證。

2. 在導覽窗格中，選擇帳戶。

   在帳戶頁面上，檢閱 S3 保護資料欄，了解您的成員帳戶的狀態。

3. 選擇性地啟用或停用 S3 保護

   選取您要設定 S3 保護的帳戶。您可以一次選取多個帳戶。在編輯保護計畫下拉式選單中，選擇 S3Pro，然後選擇適當的選項。

API/CLI

若要為您的成員帳戶選擇性地啟用或停用 S3 保護，請使用您自己的偵測器 ID 執行 updateMemberDetectors API 操作。以下範例顯示如何為單一成員帳戶啟用 S3 保護。若要停用，請使用 `false` 取代 `true`。

要查找您`detectorId`的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

```
 aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 123456789012 --features
 '[{"Name" : "S3_DATA_EVENTS", "Status" : "ENABLED"}]'
```

> **Note**
>
> 您也可以傳遞以空格分隔的帳戶 ID 清單。

當程式碼成功執行時，會返回一個空白 `UnprocessedAccounts` 清單。如果變更帳戶的偵測器設定時發生任何問題，則會列出該帳戶 ID 以及問題摘要。

> **Note**
>
> 如果您使用指令碼建立新帳戶，並且想要在新帳戶中停用 S3 保護，則可以使用選用的 `dataSources` 物件修改 createDetector API 操作，如本主題所述。

自動停用新 GuardDuty 帳戶的 S3 保護

> **Important**
>
> 根據預設，第一次會自動為 AWS 帳戶 該聯結 GuardDuty 啟用 S3 保護。

如果您是第一次在新帳戶上啟 GuardDuty 用的 GuardDuty 管理員帳戶，並且不希望預設啟用 S3 Protection，則可以透過使用選用`features`物件修改 createDetectorAPI 操作來停用它。下列範例使用啟 AWS CLI 用停用 S3 保護的新 GuardDuty 偵測器。

```
aws guardduty create-detector --enable --features '[{"Name" : "S3_DATA_EVENTS",
"Status" : "DISABLED"}]'
```

S3 保護中的功能

AWS CloudTrail S3 的資料事件

資料事件 (也稱為資料平面操作) 可讓您深入了解對資源執行的或在資源中執行的資源操作。它們通常是大量資料的活動。

以下是 S3 GuardDuty 可監控的 CloudTrail 資料事件範例：

- `GetObject` API 作業
- `PutObject` API 作業
- `ListObjects` API 作業
- `DeleteObject` API 作業

首次啟 GuardDuty 用時，S3 保護預設為啟用，並包含在 30 天免費試用期內。但是，這是選用的功能，您可以隨時為任何帳戶或區域選擇啟用或停用此功能。如需有關將 Amazon S3 設定為功能的詳細資訊，請參閱GuardDuty S3 保護。

了解 Amazon GuardDuty 發現

發 GuardDuty 現項目代表在您的網路中偵測到的潛在安全性問題。 GuardDuty每當偵測到您 AWS 環境中的未預期和潛在惡意活動時，就會產生發現結果。

您可以在 GuardDuty 主控台的 [GuardDuty 發現項目] 頁面上檢視及管理發現項目，或使用 AWS CLI 或 API 作業。如需可用於管理調查結果的方法概觀，請參閱管理 Amazon GuardDuty 發現。

主題：

調查結果詳細資訊

瞭解 GuardDuty 發現項目中可用的資料類型。

範例問題清單

瞭解如何產生範例發現項目以進行測試或進一步瞭解 GuardDuty。

GuardDuty 調查結果格式

瞭解 GuardDuty 尋找類型的格式，以及追蹤的不同威脅目的 GuardDuty。

調查結果類型

依類型檢視和搜尋所有可用的搜 GuardDuty 尋結果。每個調查結果類型項目都包含該調查結果的說明，以及修復的秘訣和建議。

調查結果詳細資訊

在 Amazon 主 GuardDuty 控台中，您可以在「尋找摘要」區段中檢視尋找詳細資訊。調查結果的詳細資訊會根據調查結果類型而有所不同。

有兩項主要詳細資訊會決定哪些資訊類型可供任何調查結果使用。第一項是資源類型，可能是 `Instance`、`AccessKey`、`S3Bucket`、`Kubernetes cluster`、`ECS cluster`、`Container`、`RDSDBInstance` 或 `Lambda`。決定調查結果資訊的第二項詳細資訊是資源角色。資源角色可以是用於存取金鑰的 `Target`，這意味資源是可疑活動的目標。對於調查結果執行個體類型，資源角色也可以是 `Actor`，這意味著您的資源是執行可疑活動的執行者。本主題說明調查結果的一些常用詳細資訊。

調查結果概觀

調查結果的概觀區段包含調查結果最基本的識別特徵，包括下列資訊：

- 帳號 ID — 發生活動時提示 GuardDuty 產生此發現項 AWS 目的帳戶 ID。
- 計數 — GuardDuty 已將符合此模式的活動彙總至此發現項目 ID 的次數。
- 建立日期：第一次建立此調查結果的時間和日期。如果此值與更新時間不同，則表示活動已發生多次，而且是持續發生的問題。

> **Note**
>
> GuardDuty 主控台中發現項目的時間戳記會以您的當地時區顯示，而 JSON 匯出和 CLI 輸出則以 UTC 顯示時間戳記。

- 調查結果 ID：此調查結果類型和參數組的唯一識別符。符合此模式的活動新出現次數將會彙總至同一個 ID。
- 尋找類型：代表觸發調查結果之活動類型的格式化字串。如需詳細資訊，請參閱 GuardDuty 調查結果格式。
- 「區 AWS 域」— 產生搜尋結果的「區域」。如需支援區域的詳細資訊，請參閱 區域與端點
- 資源 ID — 提示 GuardDuty 產生此發現項目的活動所針對的 AWS 資源 ID。
- 掃描 ID — 適用於啟用 GuardDuty 惡意軟體防護時的發現項目，這是在連接到可能受損 EC2 執行個體或容器工作負載的 EBS 磁碟區上執行的惡意軟體掃描的識別碼。如需詳細資訊，請參閱 惡意軟體保護調查結果詳細資訊。
- 嚴重性：調查結果的指定嚴重性等級，分高、中或低。如需詳細資訊，請參閱 GuardDuty 發現項目的嚴重程度。
- 更新時間 — 上次使用符合提示產生此發現項目之模式的新活動更新此發現 GuardDuty項目的時間。

資源

受影響的資源會提供有關啟動活動鎖定之 AWS 資源的詳細資訊。可用資訊會根據資源類型和動作類型而有所不同。

資源角色 — 起始尋找項目的 AWS 資源角色。此值可以是 TARGET 或 ACTOR，而且表示資源是否為可疑活動的目標或執行可疑活動的執行者。

資源類型：受影響的資源類型。如果涉及多個資源，則一個調查結果可以包含多種資源類型。資源類型為「執行個體」、「S3 儲存貯體」AccessKey、「集群」、「容器」KubernetesCluster、「資料庫執行個體」和「L ambda」。根據資源類型，會提供不同的調查結果詳細資訊。選取資源選項索引標籤，以了解該資源可用的詳細資訊。

Instance

執行個體詳細資訊：

> **Note**
>
> 如果執行個體已終止，或在進行跨區域 API 呼叫時基礎 API 調用來自不同區域中的 EC2 執行個體，則可能會遺失一些執行個體詳細資訊。

- 執行個體 ID — 與提示 GuardDuty 產生發現項目的活動相關的 EC2 執行個體 ID。
- 執行個體類型：調查結果所涉及的 EC2 執行個體類型。
- 啟動時間：執行個體啟動的時間與日期。
- 前哨 ARN — Amazon 資源名稱 (ARN) 的. AWS Outposts僅適用於 AWS Outposts 實例。如需詳細資訊，請參閱什麼是 AWS Outposts？
- 安全群組名稱：連接到涉及之執行個體的安全群組名稱。
- 安全群組 ID：連接到涉及之執行個體的安全群組ID。
- 執行個體狀態：鎖定目標之執行個體的目前狀態。
- 可用區域：相關執行個體所在 AWS 區域的可用區域。
- 影像 ID：用來建置活動所涉及之執行個體的 Amazon Machine Image ID。
- 影像描述：用來建置活動所涉及之執行個體的 Amazon Machine Image ID 描述。
- 標籤：連接到此資源的標籤清單 (以 `key:value` 格式列出)。

AccessKey

存取金鑰詳細資訊：

- 存取金鑰 ID — 參與提示產生發現項目之活動的使用者存 GuardDuty 取金鑰 ID。
- 主參與者 ID — 參與提示產生發現項目之活動的使 GuardDuty用者主體 ID。
- 使用者類型 — 參與提示 GuardDuty 產生尋找項目之活動的使用者類型。如需詳細資訊，請參閱 CloudTrail userIdentity 元素。
- 使用者名稱 — 參與提示 GuardDuty 產生尋找項目之活動的使用者名稱。

S3Bucket

Amazon S3 儲存貯體詳細資訊：

- 名稱：調查結果所涉及的儲存貯體名稱。
- ARN：調查結果所包含之儲存貯體 ARN。
- 擁有者：擁有此調查結果所涉及之儲存貯體使用者的正式使用者 ID。如需正式使用者 ID 的詳細資訊，請參閱 AWS account identifiers。
- 類型：儲存貯體調查結果類型，可為目的地或來源。
- 預設伺服器端加密：儲存貯體的加密詳細資訊。
- 儲存貯體標籤：連接到此資源的標籤清單 (以 `key:value` 的格式列出)。
- 有效許可：儲存貯體上的所有有效許可和政策的評估，表示涉及的儲存貯體是否已公開。值可以是公有，也可以是非公有。

EKSCluster

Kubernetes 叢集詳細資訊：

- 名稱：Kubernetes 叢集的名稱。
- ARN：識別叢集的 ARN。
- 建立日期：建立此叢集的時間和日期。

> **Note**
>
> GuardDuty 主控台中發現項目的時間戳記會以您的當地時區顯示，而 JSON 匯出和 CLI 輸出則以 UTC 顯示時間戳記。

- VPC ID：與您的叢集關聯的 VPC ID。
- 狀態：提取叢集的目前狀態。
- 標籤：您套用到叢集以協助您分類和組織的中繼資料。每個標籤皆包含索引鍵與選用值，以 `key:value` 的格式列出。您可以定義索引鍵和值。

  叢集標籤不會傳播到與叢集相關聯的任何其他資源。

Kubernetes 工作負載詳細資訊：

- 類型：Kubernetes 工作負載的類型，例如 Pod、部署和工作。
- 名稱：Kubernetes 工作負載的名稱。
- Uid：Kubernetes 工作負載的唯一識別碼。

- 建立時間：建立此工作負載的時間和日期。
- 標籤：連接到 Kubernetes 工作負載的索引鍵/值組。
- 容器：作為 Kubernetes 工作負載一部分執行之容器的詳細資訊。
- 命名空間：工作負載屬於此 Kubernetes 命名空間。
- 磁碟區：Kubernetes 工作負載使用的磁碟區。
  - 主機路徑：代表磁碟區映射至的主機機器上預先存在的檔案或目錄。
  - 名稱：磁碟區名稱。
- Pod 安全性內容：定義 Pod 中所有容器的權限和存取控制設定。
- 主機網路：設定為 `true` 是否將 Pod 包含在 Kubernetes 工作負載中。

Kubernetes 使用者詳細資訊：

- 群組：與產生調查結果之活動相關之使用者的 Kubernetes RBAC (角色存取型的控制) 群組。
- ID：Kubernetes 使用者的唯一識別碼。
- 使用者名稱：參與產生調查結果之活動的 Kubernetes 使用者名稱。
- 工作階段名稱：擔任具有 Kubernetes RBAC 許可的 IAM 角色之實體。

ECSCluster

ECS 叢集詳細資訊：

- ARN：識別叢集的 ARN。
- 名稱：叢集的名稱。
- 狀態：提取叢集的目前狀態。
- 作用中服務計數：在叢集上執行處於某種 `ACTIVE` 狀態的服務數目。您可以查看這些服務 ListServices
- 已註冊的容器執行個體計數：在叢集中註冊的容器執行個體數目。這包括 `ACTIVE` 和 `DRAINING` 狀態的容器執行個體。
- 執行中工作計數：叢集中處於 `RUNNING` 狀態的任務數目。
- 標籤：您套用到叢集以協助您分類和組織的中繼資料。每個標籤皆包含索引鍵與選用值，以 `key:value` 的格式列出。您可以定義索引鍵和值。
- 容器：與任務相關聯之容器的詳細資訊：

    - 容器名稱：容器的名稱。
    - 容器映像：容器的映像。
- 任務詳細資訊：叢集中任務的詳細資訊。
    - ARN：任務的 Amazon Resource Name (ARN)。
    - 定義 ARN：建立任務的任務定義 Amazon Resource Name (ARN)。
    - 版本：任務的版本計數器。
    - 任務建立時間：建立任務時的 Unix 時間戳記。
    - 任務開始時間：任務開始時的 Unix 時間戳記。
    - 任務開始者：任務啟動時指定的標籤。

Container

容器詳細資訊：

- 容器執行期：用來執行容器的容器執行期 (例如 `docker` 或 `containerd`)。
- ID：容器執行個體 ID 或容器執行個體的完整 ARN 項目。
- 名稱：容器的名稱。

  如果可用，此欄位會顯示標籤 `io.kubenetes.container.name` 的值。
- 映像：容器執行個體的映像。
- 磁碟區掛載：容器磁碟區掛載的清單。容器可以在其檔案系統下掛載磁碟區。
- 安全性內容：容器安全性內容定義容器的權限和存取控制設定。
- 程序詳細資訊：描述與調查結果相關聯之程序的詳細資訊。

RDSDBInstance

RDSDBInstance 詳細資訊：

> **Note**
>
> 此資源可在與資料庫執行個體相關的 RDS 保護調查結果中找到。

- 資料庫執行處理 ID — 與 GuardDuty 發現項目相關的資料庫執行處理相關聯的 ID。

- 引擎：調查結果所涉及的資料庫執行個體的資料庫引擎名稱。可能的值是 Aurora MySQL 相容或 Aurora PostgreSQL 相容。
- 引擎版本 — 發 GuardDuty現項目所涉及的資料庫引擎版本。
- 資料庫叢集 ID — 資料庫叢集的 ID，包含與 GuardDuty 發現項目相關的資料庫執行處理 ID。
- 資料庫執行處理 ARN — 識別發現項目所涉及之資料庫執行處理的 ARN。 GuardDuty

Lambda

Lambda 函數詳細資訊

- 函數名稱：調查結果所涉及的 Lambda 函數名稱。
- 函數版本：調查結果所涉及的 Lambda 函數版本。
- 函數說明：調查結果所涉及的 Lambda 函數的說明。
- 函數 ARN：調查結果中涉及的 Lambda 函數的 Amazon Resource Name (ARN)。
- 修訂識別碼：Lambda 函數版本的修訂識別碼。
- 角色：調查結果中涉及的 Lambda 函數的執行角色。
- VPC 組態：Amazon VPC 組態，包括與 Lambda 函數相關聯的 VPC ID、安全群組和子網路 ID。
- VPC ID：與調查結果中涉及的 Lambda 函數相關聯的 Amazon VPC ID。
- 子網路 ID：與 Lambda 函數相關聯之子網路的 ID。
- 安全群組：連接到涉及 Lambda 函數的安全群組。這包括安全群組名稱和群組 ID。
- 標籤：連接到此資源的標籤清單 (以 `key:value` 對格式列出)。

RDS 資料庫 (DB) 使用者詳細資訊

> **Note**
>
> 本節適用於您在中啟用 RDS 防護功能時的發現項目 GuardDuty。如需詳細資訊，請參閱 GuardDuty 遠端防護。

此發 GuardDuty 現項目提供下列可能遭到入侵之資料庫的使用者和驗證詳細資料。

- 使用者：用來進行異常登入嘗試的使用者名稱。

- 應用程式：用來進行異常登入嘗試的應用程式名稱。
- 資料庫：異常登入嘗試所涉及的資料庫執行個體名稱。
- SSL：用於網路的 Secure Socket Layer (SSL) 版本。
- 驗證方法：與調查結果中涉及的使用者使用的驗證方法。

執行階段監視尋找詳

> **Note**
>
> 只有在 GuardDuty 產生其中一個時，才能使用這些詳細資訊執行階段監視尋找項。

本區段包含執行期詳細資訊，例如程序詳細資訊和任何必要的內容。處理程序詳細資訊描述觀察到的程序之相關資訊，而執行期內容則描述有關潛在可疑活動的其他資訊。

程序詳細資訊

- 名稱：程序的名稱。
- 可執行路徑：處理程序可執行檔的絕對路徑。
- 可執行 SHA-256：處理程序可執行的 SHA256 雜湊值。
- 命名空間 PID：主機層級 PID 命名空間以外的次要 PID 命名空間中的程序之程序 ID。對於容器內的程序，它是容器內觀察到的程序 ID。
- 目前的工作目錄：程序的目前工作目錄。
- 程序 ID：由作業系統指派給程序的 ID。
- startTime：程序開始的時間。這是 UTC 日期字串格式 (`2023-03-22T19:37:20.168Z`)。
- UUID — 由指派給程序的唯一識別碼。 GuardDuty
- 父系 UUID：父系程序的唯一識別碼。此 ID 由指派給父流程 GuardDuty。
- 使用者：執行程序的使用者。
- 使用者 ID：執行程序的使用者 ID。
- 有效使用者 ID：事件發生時程序的有效使用者 ID。
- 世系：程序上階的相關資訊。
  - 程序 ID：由作業系統指派給程序的 ID。

- UUID — 由指派給程序的唯一識別碼。 GuardDuty
- 可執行路徑：處理程序可執行檔的絕對路徑。
- 有效使用者 ID：事件發生時程序的有效使用者 ID。
- 父系 UUID：父系程序的唯一識別碼。此 ID 由指派給父流程 GuardDuty。
- 開始時間：程序開始的時間。
- 命名空間 PID：主機層級 PID 命名空間以外的次要 PID 命名空間中的程序之程序 ID。對於容器內的程序，它是容器內觀察到的程序 ID。
- 使用者 ID：執行程序的使用者的使用者 ID。
- 名稱：程序的名稱。

執行期內容

從下列欄位中，產生的調查結果可能只包含與調查結果類型相關的欄位。

- 掛載來源：由容器掛載的主機路徑。
- 掛載目標：對應至主機目錄之容器中的路徑。
- 檔案系統類型：代表已掛載檔案系統的類型。
- 旗標：代表控制此調查結果所涉及之事件行為的選項。
- 修改程序：在執行期的容器內建立或修改二進位、指令碼或程式庫之程序的相關資訊。
- 修改時間：程序在執行期建立或修改二進位、指令碼或程式庫的時間戳記。此欄位是 UTC 日期字串格式 (`2023-03-22T19:37:20.168Z`)。
- 程式庫路徑：已載入之新程式庫的路徑。
- LD 載入前的值：`LD_PRELOAD` 環境變數的值。
- 通訊端路徑：存取 Docker 通訊端的路徑。
- Runc 二進位路徑：`runc` 二進位的路徑。
- 代理程式版本路徑：`cgroup` 發行代理程式檔案的路徑。
- 命令列範例 — 涉及潛在可疑活動的命令列範例。
- 工具類別 — 工具所屬的類別。一些例子是後門工具，Pentest 工具，網絡掃描儀和網絡嗅探器。
- 工具名稱 — 潛在可疑工具的名稱。
- 命令檔路徑 — 產生發現項目之已執行命令檔的路徑。
- 威脅檔案路徑 — 找到威脅情報詳細資訊的可疑路徑。

- 服務名稱 — 已停用的安全性服務名稱。

EBS 磁碟區掃描詳細資訊

> **Note**
>
> 本節適用於在GuardDuty 惡意程式碼中開 GuardDuty啟啟動的惡意程式碼掃描時發現的項目。

EBS 磁碟區掃描提供有關連接至可能洩露 EC2 執行個體或容器工作負載的 EBS 磁碟區之詳細資訊。

- 掃描 ID：惡意程式碼掃描的識別碼。
- 掃描開始時間：惡意程式碼掃描開始的日期和時間。
- 掃描完成時間：惡意程式碼掃描完成的日期和時間。
- 觸發發現項目 ID — 起始此惡意程式碼掃描之 GuardDuty 發現項目的發現項目 ID。
- 來源：可能的值為 `Bitdefender` 和 `AWS`。
- 掃描偵測：每個惡意程式碼掃描的詳細資訊和結果的完整檢視。
  - 掃描項目計數：已掃描檔案的總數。它提供了詳細資訊，例如 `totalGb`、`files`，和 `volumes`。
  - 偵測到的威脅項目計數：掃描期間 `files` 偵測到的惡意程式總數。
  - 最高嚴重性威脅詳細資訊：掃描期間偵測到的最高嚴重性威脅之詳細資訊，以及惡意檔案數目。它提供了詳細資訊，例如 `severity`、`threatName`，和 `count`。
  - 依名稱偵測到的威脅：容器元素會將所有嚴重性等級的威脅分組。它提供了詳細資訊，例如 `itemCount`、`uniqueThreatNameCount`、`shortened` 和 `threatNames`。

惡意軟體保護調查結果詳細資訊

> **Note**
>
> 本節適用於在GuardDuty 惡意程式碼中開 GuardDuty啟啟動的惡意程式碼掃描時發現的項目。

當惡意軟體防護掃描偵測到惡意軟體時，您可以在 https://console.aws.amazon.com/guardduty/ 主控台的調查結果頁面上選取對應的調查結果，以檢視掃描詳細資訊。您的惡意軟件防護發現的嚴重性取決於 GuardDuty發現的嚴重性。

> **Note**
>
> `GuardDutyFindingDetected` 標記指定快照包含惡意軟體。

下列資訊可在詳細資訊面板的偵測到的威脅區段下取得。

- 名稱：透過偵測將檔案分組而取得的威脅名稱。
- 嚴重性：偵測到的威脅嚴重性。
- 雜湊：檔案的 SHA-256。
- 檔案路徑：惡意檔案在 EBS 磁碟區中的位置。
- 檔案名稱：偵測到威脅的檔案名稱。
- 磁碟區 ARN：已掃描的 EBS 磁碟區的 ARN。

下列資訊可在詳細資訊面板的惡意軟體掃描詳細資訊區段下取得。

- 掃描 ID：惡意軟體掃描的掃描 ID。
- 掃描開始時間：掃描開始的日期和時間。
- 掃描完成時間：掃描完成的日期和時間。
- 掃描的檔案：已掃描檔案和目錄的總數。
- 已掃描的 GB 總數：程序期間掃描的儲存空間量。
- 觸發發現項目 ID — 起始此惡意程式碼掃描之 GuardDuty 發現項目的發現項目 ID。
- 下列資訊可在詳細資訊面板的磁碟區詳細資訊區段下取得。
  - 磁碟區 ARN：磁碟區的 Amazon Resource Name (ARN)。
  - SnapshotARN：EBS 磁碟區快照的 ARN。
  - 狀態：磁碟區的掃描狀態，例如 `Running`、`Skipped` 和 `Completed`。
  - 加密類型：用來加密磁碟區的加密類型。例如 `CMCMK`。
  - 裝置名稱：裝置的名稱。例如 `/dev/xvda`。

動作

調查結果的動作提供觸發此調查結果之活動類型的相關詳細資訊。可用資訊會根據動作類型而有所不同。

動作類型：調查結果活動類型。這個值可以是NETWORK_CONNECTION、PORT_PROBE、DNS_REQUEST、AWS_API_CALL 或 RDS_LOGIN_ATTEMPT。可用資訊會根據動作類型而有所不同：

- NETWORK_CONNECTION：表示已識別的 EC2 執行個體和遠端主機之間的網路流量已進行交換。此動作類型具有以下其他資訊：
  - 連線方向 — 在提示 GuardDuty 產生發現項目的活動中觀察到的網路連線方向。這些值可為下列其中一項：
    - INBOUND：表示遠端主機已啟動本機連接埠的連線，該本機連接埠位於您帳戶中的已識別 EC2 執行個體。
    - OUTBOUND：表示識別的 EC2 執行個體已啟動到遠端主機的連線。
    - 未知 — 表示 GuardDuty 無法確定連接的方向。
  - 通訊協定 — 在提示 GuardDuty 產生發現項目的活動中觀察到的網路連線通訊協定。
  - 本機 IP：觸發調查結果之流量的原始來源 IP 地址。此資訊可以用來區分流量流經之中繼層的 IP 地址，以及觸發調查結果之流量的原始來源 IP 地址。例如，EKS Pod 的 IP 地址，而不是 EKS Pod 執行所在之執行個體的 IP 地址。
  - 已封鎖：表示目標通訊埠是否已封鎖。
- PORT_PROBE：表示遠端主機在多個開放連接埠上探測了已識別的 EC2 執行個體。此動作類型具有以下其他資訊：
  - 本機 IP：觸發調查結果之流量的原始來源 IP 地址。此資訊可以用來區分流量流經之中繼層的 IP 地址，以及觸發調查結果之流量的原始來源 IP 地址。例如，EKS Pod 的 IP 地址，而不是 EKS Pod 執行所在之執行個體的 IP 地址。
  - 已封鎖：表示目標通訊埠是否已封鎖。
- DNS_REQUEST：表示識別的 EC2 執行個體已查詢網域名稱。此動作類型具有以下其他資訊：
  - 通訊協定 — 在提示 GuardDuty 產生發現項目的活動中觀察到的網路連線通訊協定。
  - 已封鎖：表示目標通訊埠是否已封鎖。
- AWS_API_CALL：表示已呼叫 AWS API。此動作類型具有以下其他資訊：
  - API — 叫用並因此提示 GuardDuty 產生此發現項目的 API 作業名稱。

> **Note**
>
> 這些操作也可以包含 AWS CloudTrail擷取的非 API 活動。如需詳細資訊，請參閱由 CloudTrail.

  - 使用者代理程式：發出 API 請求的使用者代理程式。此值告訴您呼叫是從 AWS Management Console、 AWS 服務、 AWS SDK 或. AWS CLI
  - 錯誤代碼：如果調查結果是由失敗的 API 呼叫觸發，則會顯示該呼叫的錯誤代碼。
  - 服務名稱：試圖發出觸發此調查結果之 API 呼叫的服務的 DNS 名稱。
- RDS_LOGIN_ATTEMPT：表示嘗試從遠端 IP 地址登入可能遭到洩露的資料庫。
  - IP 地址：用來進行潛在可疑登入嘗試的遠端 IP 地址。

執行者或目標

如果資源角色是 TARGET，則調查結果具有執行者區段。這表示可疑活動已將目標鎖定在您的資源，而且執行者區段包含了將目標鎖定在執行個體之實體的相關詳細資訊。

如果資源角色是 ACTOR，則調查結果具有目標區段。這表示針對遠端主機之可疑活動涉及了您的資源，而且此區段包含 IP 或資源已鎖定目標之網域的相關資訊。

執行者或目標區段中的可用資訊可包含下列項目：

- 附屬 — 有關遠程 API 調用者的 AWS 帳戶是否與您的 GuardDuty 環境相關的詳細信息。如果此值為 `true`，則 API 呼叫者會以某種方式與您的帳戶相關聯；如果為 `false`，API 呼叫者來自您的環境之外。
- 遠端帳號 ID — 擁有輸出 IP 位址的帳號 ID，該位址用於存取最終網路上的資源。
- IP 位址 — 活動中涉及提示產生發現項目 GuardDuty 的 IP 位址。
- 位置 — 與提示產生尋找項目的活動相關 IP 位址 GuardDuty 的位置資訊。
- 組織 — 與提示 GuardDuty 產生發現項目之活動相關 IP 位址的 ISP 組織資訊。
- 連接埠 — 活動中涉及的連接埠號碼， GuardDuty 提示產生尋找項目。
- 網域 — 參與提示 GuardDuty 產生尋找項目之活動的網域。
- 具有尾碼的網域 — 參與可能提示產生發現項目之活動的第二 GuardDuty 個和頂層網域。如需頂層和第二層網域的清單，請參閱公用尾碼清單。

其他資訊

所有調查結果的其他資訊區段可包含以下資訊：

- 威脅清單名稱 — 安全威脅清單的名稱，其中包含 IP 位址或與提示產生發現項目的活動相關 GuardDuty 的網域名稱。

- 範例：表示此是否為調查結果範本的 true 或 false 值。
- 已封存：表示此調查結果是否已封存的 true 或 false 值。
- 異常：在歷史中未觀察到的活動詳細資訊。這些可能包括不尋常 (以前未觀察到) 的使用者、位置、時間、儲存貯體、登入行為或 ASN Org。
- 異常通訊協定 — 提示 GuardDuty 產生發現項目的活動中涉及的網路連線通訊協定。
- 代理程式詳細資訊：目前部署在 AWS 帳戶的 EKS 叢集上的安全代理程式的詳細資訊。這僅適用於 EKS 執行期監控調查結果類型。
  - 代理程式版本 — GuardDuty 安全代理程式的版本。
  - 代理程式 ID — GuardDuty 安全性代理程式的唯一識別碼。

證據

根據威脅情報的調查結果具有證據區段，其中包含下列資訊：

- 威脅情報詳細資訊 — `Threat name` 顯示已辨識的威脅清單名稱。
- 威脅名稱 — 惡意程式碼系列的名稱或與威脅相關聯的其他識別碼。
- 安全威脅檔案 SHA256 — 產生發現項目的檔案的 SHA256。

異常行為

結尾為的發現項目類型AnomalousBehavior表示發現項目是由 GuardDuty 異常偵測機器學習 (ML) 模型所產生。ML 模型會評估帳戶中的所有 API 請求，並識別與對手使用的策略相關聯的異常事件。ML 模型會追蹤 API 請求的各種因素，例如發出請求的使用者、發出請求的位置，以及請求的特定 API。

有關哪些 API 請求因素對於調用請求的 CloudTrail 用戶身份不尋常的詳細信息可以在發現項目詳細信息中找到。識別是由 CloudTrail userIdentity 別元素所定義，可能的值為：`Root`、`IAMUser`、`AssumedRole`、`FederatedUser`、`AWSAccount`、或`AWSService`。

除了可用於所有與 API 活動相關聯之 GuardDuty 發現項目的詳細資料之外，AnomalousBehavior發現項目還有下一節概述的其他詳細資料。您可以在主控台中檢視這些詳細資訊，也可以在調查結果的 JSON 中找到。

- 異常 API：由與調查結果相關聯的主要 API 請求附近的使用者身分調用的 API 請求清單。此窗格會透過下列方式進一步細分 API 事件的詳細資訊。

- 列出的第一個 API 是主要 API，這是與觀察到的最高風險活動相關聯的 API 請求。這是觸發調查結果並與調查結果類型的攻擊階段相關的 API。這也是在主控台的動作區段下，以及調查結果的 JSON 中詳細說明的 API。
- 列出的任何其他 API 都是在主要 API 附近觀察到的所列使用者身分的其他異常 API。如果清單上只有一個 API，ML 模型就不會將來自該使用者身分的任何其他 API 請求識別為異常。
- API 清單會根據是否成功呼叫 API，或是否呼叫 API 失敗而劃分，表示收到錯誤回應。收到的錯誤回應類型列在每個未成功呼叫 API 的上面。可能的錯誤回應類型為：`access denied`、`access denied exception`、`auth failure`、`instance limit exceeded`、`invalid permission - duplicate`、`invalid permission - not found` 和 `operation not permitted`。
- API 按其關聯的服務進行分類。

> **Note**
>
> 如需更多內容，請選擇歷史 API 以檢視有關頂端 API 的詳細資訊，最多 20 個，通常針對使用者身分和帳戶內的所有使用者顯示。這些 API 被標記為極少 (每月少於一次)、不常 (每月幾次)或經常 (每天到每週)，具體取決於它們在您的帳戶中使用頻率。

- 異常行為 (帳戶)：本節提供有關帳戶已分析行為的其他詳細資訊。此面板中追蹤的資訊包括：
  - ASN Org：發出異常 API 呼叫的 ASN Org。
  - 使用者名稱：進行異常 API 呼叫的使用者名稱。
  - 使用者代理程式：用來進行異常 API 呼叫的使用者代理程式。使用者代理程式是用來進行呼叫的方法，例如 `aws-cli` 或 `Botocore`。
  - 使用者類型：進行異常 API 呼叫的使用者類型。可能值為 `AWS_SERVICE`、`ASSUMED_ROLE`、`IAM_USER`、 或 `ROLE`。
  - 儲存貯體：要存取的 S3 儲存貯體名稱。
- 異常行為 (使用者身分)：本節提供調查結果所涉及使用者身分之已分析行為的其他詳細資訊。當行為未被識別為歷史時，這表示 GuardDuty ML 模型先前沒有看到此使用者身分在訓練期間以這種方式進行此 API 呼叫。下列有關使用者身分的其他詳細資訊：
  - ASN Org：發出異常 API 呼叫的 ASN Org。
  - 使用者代理程式：用來進行異常 API 呼叫的使用者代理程式。使用者代理程式是用來進行呼叫的方法，例如 `aws-cli` 或 `Botocore`。
  - 儲存貯體：要存取的 S3 儲存貯體名稱。

- 異常行為 (儲存貯體)：本區段提供與調查結果相關聯之 S3 儲存貯體已分析行為的其他詳細資訊。當行為未識別為歷史行為時，這表示 GuardDuty ML 模型先前沒有看到在訓練期間以這種方式對此值區進行的 API 呼叫。本區段追蹤的資訊包括：
  - ASN Org：發出異常 API 呼叫的 ASN Org。
  - 使用者名稱：進行異常 API 呼叫的使用者名稱。
  - 使用者代理程式：用來進行異常 API 呼叫的使用者代理程式。使用者代理程式是用來進行呼叫的方法，例如 `aws-cli` 或 `Botocore`。
  - 使用者類型：進行異常 API 呼叫的使用者類型。可能值為 `AWS_SERVICE`、`ASSUMED_ROLE`、`IAM_USER`、 或 `ROLE`。

  > **Note**
  >
  > 如需有關歷史行為的詳細內容，請在異常行為 (帳戶)、使用者 ID或儲存貯體區段中選擇歷史行為，以檢視您帳戶中每個類別預期行為的詳細資訊：極少 (每月少於一次)、不常 (每月幾次) 或經常 (每天到每週)，具體取決於它們在您的帳戶中使用頻率。

- 異常行為 (資料庫)：此區段提供與調查結果相關聯之資料庫執行個體已分析行為的其他詳細資訊。如果行為未識別為歷史記錄，則表示 GuardDuty ML 模型先前並未在訓練期間看到以這種方式對此資料庫執行個體進行的登入嘗試。在調查結果面板中針對此區段所追蹤的資訊包括：
  - 使用者名稱：用來進行異常登入嘗試的使用者名稱。
  - ASN Org：發出異常登入嘗試的 ASN Org。
  - 應用程式名稱：用來進行異常登入嘗試的應用程式名稱。
  - 資料庫名稱：異常登入嘗試所涉及的資料庫執行個體名稱。

  > **Note**
  >
  > 歷史行為區段提供有關之前觀察到的使用者名稱、ASN Org、應用程式名稱和相關聯資料庫的資料庫名稱的詳細內容。每個唯一值都有一個相關聯的計數，代表在成功登入事件中觀察到此值的次數。

- 異常行為 (帳戶 Kubernetes 叢集、Kubernetes 命名空間和 Kubernetes 使用者名稱)：本區段提供有關 Kubernetes 叢集的已分析行為的其他詳細資訊，以及與調查結果相關聯的命名空間。當行為未識別為歷史時，表示 GuardDuty ML 模型先前未以這種方式觀察到此帳戶、叢集、命名空間或使用者名稱。在調查結果面板中針對此區段所追蹤的資訊包括：
  - 使用者名稱：呼叫與調查結果相關聯之 Kubernetes API 的使用者。

- 模擬使用者名稱：被 `username` 模擬的使用者。
- 命名空間：產生動作的 Amazon EKS 叢集內的 Kubernetes 命名空間。
- 使用者代理程式：與 Kubernetes API 呼叫相關聯的使用者代理程式。使用者代理程式是用來進行呼叫的方法，例如 `kubectl`。
- API：由 Amazon EKS 叢集內 `username` 呼叫的 Kubernetes API。
- ASN 資訊：與進行此呼叫之使用者 IP 地址相關聯的 ASN 資訊，例如組織和 ISP。
- 週幾：進行 Kubernetes API 呼叫時是週幾。
- 許可[1]：正在檢查是否有存取權的 Kubernetes 動詞和資源，以指出 `username` 是否可以使用 Kubernetes API。
- 服務帳戶名稱[1]：與 Kubernetes 工作負載相關聯的服務帳戶，可為工作負載提供身分。
- 登錄[1]：與 Kubernetes 工作負載中部署的容器映像相關聯的容器登錄。
- 映像[1]：部署在 Kubernetes 工作負載中的容器映像，不含相關標籤和摘要。
- 映像字首組態[1]：啟用容器和工作負載安全性組態的映像字首，例如使用映像的容器的 `hostNetwork` 或 `privileged`。
- 主旨名稱[1]：在 `RoleBinding` 或 `ClusterRoleBinding` 中綁定到參考角色的主旨，例如 `user`、`group` 或 `serviceAccountName`。
- 角色名稱[1]：涉及建立或修改角色或 `roleBinding` API 的角色名稱。

S3 磁碟區型異常

本區段詳細說明 S3 磁碟區型異常的關聯式資訊。磁碟區型調查結果 (Exfiltration:S3/AnomalousBehavior) 會監控使用者對 S3 儲存貯體進行的不尋常 S3 API 呼叫次數，以表示可能的資料外洩。下列 S3 API 呼叫會受到監控，以進行磁碟區型的異常偵測。

- `GetObject`
- `CopyObject.Read`
- `SelectObjectContent`

當 IAM 儲存貯體存取 S3 儲存貯體時，以下指標有助於建立常見行為的基準。為了偵測資料外洩，磁碟區型異常偵測調查結果會根據通常的行為基準來評估所有活動。在異常行為 (使用者身分)、觀察到的磁碟區 (使用者身分)和觀察到的磁碟區 (儲存貯體)區段中選擇歷史行為，分別檢視下列指標。

- 過去 24 小時內，IAM 使用者或 IAM 角色調用的 `s3-api-name` API 呼叫次數 (取決於發出哪一個)與受影響的 S3 儲存貯體相關聯。

- 過去 24 小時內，IAM 使用者或 IAM 角色調用的 s3-api-name API 呼叫次數 (取決於發出哪一個) 與所有 S3 儲存貯體相關聯。
- 過去 24 小時內，在各個 IAM 使用者或 IAM 角色中的 s3-api-name API 呼叫次數 (取決於發出哪一個) 與受影響的 S3 儲存貯體相關聯。

RDS 登入活動型異常

本區段詳細說明了不尋常執行者執行的登入嘗試次數，並按登入嘗試的結果進行分組。RDS 保護調查結果類型 透過監控 successfulLoginCount、failedLoginCount 和 incompleteConnectionCount 異常模式的登入事件來識別異常行為。

- successfulLoginCount— 此計數器代表不尋常的 actor 對資料庫執行處理建立的成功連線 (正確的登入屬性組合) 的總和。登入屬性包括使用者名稱、密碼和資料庫名稱。
- failedLoginCount— 此計數器代表為建立資料庫執行個體連線而嘗試登入失敗 (失敗) 的總和。這表示登入組合一個或多個屬性，例如使用者名稱、密碼或資料庫名稱不正確。
- incompleteConnectionCount— 此計數器代表無法分類為成功或失敗的連線嘗試次數。這些連接在資料庫提供回應之前關閉。例如，連接埠掃描，其中資料庫連接埠已連接，但沒有任何資訊發送到資料庫，或在成功或失敗的嘗試中登入完成之前連線已中止。

GuardDuty 調查結果格式

當 GuardDuty 在您的 AWS 環境中偵測到可疑或意外行為時，便會產生調查結果。調查結果是包含 GuardDuty 所發現潛在安全問題相關詳細資訊的通知。調查結果詳細資訊包含發生情況、哪些 AWS 資源涉及可疑活動、活動發生的時間等資訊與其他資訊。

在問題清單詳細資訊中，最有用的資訊之一是問題清單類型。問題清單類型的目的，是提供潛在安全問題精簡易讀的描述。例如，GuardDuty Recon:EC2/PortProbeUnprotectedPort 調查結果類型會迅速通知您，在 AWS 環境中的某處，有潛在攻擊者正在探測 EC2 執行個體未受保護的連接埠。

GuardDuty 會使用以下格式命名其產生的各種調查結果類型：

ThreatPurpose:ResourceTypeAffected/ThreatFamilyName.DetectionMechanism!Artifact

此格式的每個部分都代表調查結果類型的一個層面。這些層面具有以下解釋：

- ThreatPurpose - 描述威脅、攻擊類型或潛在攻擊階段的主要目的。如需 GuardDuty 威脅目的完整清單，請參閱下一節。

- ResourceTypeAffected - 描述此調查結果中識別為對手潛在目標的 AWS 資源。目前，GuardDuty 可以產生 EC2、S3、IAM 和 EKS 資源的調查結果。
- ThreatFamilyName - 描述 GuardDuty 偵測到的整體威脅或潛在惡意活動。例如，NetworkPortUnusual 的值指出在 GuardDuty 調查結果中識別的 EC2 執行個體在調查結果中識別之特定遠端連接埠上沒有之前的通訊歷程記錄。
- DetectionMechanism - 描述 GuardDuty 檢測到調查結果的方法。這可用來指出常見調查結果類型的變化，或 GuardDuty 使用特定機制加以偵測的調查結果。例如，Backdoor:EC2/DenialOfService.Tcp 表示透過 TCP 偵測到拒絕服務 (DoS)。UDP 變體為 Backdoor:EC2/DenialOfService.Udp。

  .Custom 的值表示 GuardDuty 根據您的自訂威脅清單偵測到調查結果，而 .Reputation 則表示 GuardDuty 使用網域信譽評分模型偵測到調查結果。
- 成品 - 描述在惡意活動中使用的工具所擁有的特定資源。例如，調查結果類型 CryptoCurrency:EC2/BitcoinTool.B!DNS 中的 DNS 表示 EC2 執行個體正在與已知的比特幣相關網域進行通訊。

威脅目的

在 GuardDuty 中，威脅目的描述威脅、攻擊類型或潛在攻擊階段的主要目的。例如，某些威脅目的 (例如後門) 表示攻擊類型。然而，某些威脅目的 (例如影響) 與 MITRE ATT&CK 策略保持一致。MITRE ATT&CK 測略指出對手的攻擊週期中不同的階段。在目前的 GuardDuty 版本中，ThreatPurpose 可以有以下值：

Backdoor (後門)

此值表示對手已入侵 AWS 資源並更改該資源，是以可聯絡其主要命令和控制 (C&C) 伺服器，接收惡意活動的進一步指示。

行為

此值表示 GuardDuty 已偵測與涉及之 AWS 資源的既有基準不同的活動或活動模式。

CredentialAccess

此值表示 GuardDuty 偵測到對手可能用來從您的環境竊取憑證 (例如帳戶 ID 或密碼) 的活動模式。此威脅目的是基於 MITRE ATT&CK 策略

加密貨幣

此值表示 GuardDuty 偵測到您環境中的AWS 資源正在託管與加密貨幣相關聯的軟體 (例如，比特幣)。

DefenseEvasion

此值表示 GuardDuty 偵測到對手可能在滲透您的環境時用於避免偵測的活動或活動模式。此威脅目的是基於 MITRE ATT&CK 策略

探索

此值表示 GuardDuty 偵測到對手可能會用來擴展他們對系統和內部網路之知識的活動或活動模式。此威脅目的是基於 MITRE ATT&CK 策略。

執行

此值表示 GuardDuty 偵測到對手可能會嘗試執行惡意程式碼來探索網路或竊取資料。此威脅目的是基於 MITRE ATT&CK 策略 。

外流

此值表示 GuardDuty 偵測到對手嘗試從您的網路竊取資料時可能使用的活動或活動模式。此威脅目的是基於 MITRE ATT&CK 策略。

影響

此值表示 GuardDuty 偵測到活動或活動模式，表明對手正嘗試操縱、中斷或銷毀您的系統和資料。此威脅目的是基於 MITRE ATT&CK 策略

InitialAccess

此威脅目的是基於 MITRE ATT&CK 策略

滲透測試

有時 AWS 資源擁有者或其授權代表會故意針對 AWS 應用程式進行測試以尋找漏洞，例如開放式安全群組，或是過度寬鬆的存取金鑰。這些滲透測試，是要試圖在攻擊者發現易受攻擊資源之前識別並鎖定易受攻擊資源。不過，某些已授權的滲透測試者使用的工具其實是無償提供的，因此能讓未經授權的使用者或對手用於執行探測測試。雖然 GuardDuty 無法識別該活動背後的真正目的，但滲透測試值會表示 GuardDuty 正在偵測此類活動 (此類活動和已知的滲透測試工具所產生活動相似)，並且可能表示對您的網路進行惡意探測。

Persistence (持續)

此值表示 GuardDuty 已偵測到即使對手的初始存取路由中斷，對手也可能使用的活動或活動模式，以嘗試與維持對您的系統之存取權限。例如，這可能包括在透過現有使用者遭入侵的憑證取得存取權限後，建立新的 IAM 使用者。刪除現有使用者的憑證後，對手將保留新使用者 (未偵測為原始事件一部分的新使用者) 的存取權限。此威脅目的是基於 MITRE ATT&CK 策略。

政策

此值表示您的 AWS 帳戶 正在展現違反建議之安全最佳實務的行為。

PrivilegeEscalation

此值會通知您，AWS 環境中涉及的主體正在展現對手可能用來取得較高層級網路許可的行為。此威脅目的是基於 MITRE ATT&CK 策略。

Recon (偵察)

此值表示 GuardDuty 偵測到對手在偵察您的網路時可能會使用的活動或活動模式，以判斷他們如何擴大他們的存取權限或利用您的資源。例如，此活動可能會透過探測連接埠、列出使用者、資料庫資料表等，來找出 AWS 環境中的漏洞。

Stealth (隱匿)

此值表示對手正在積極嘗試隱藏其動作。例如，他們可能使用匿名代理服務器，因此非常難以衡量活動的真實本質。

Trojan (木馬程式)

此值表示攻擊正在使用木馬程式，以隱匿方式進行惡意活動。有時候這些軟體會隱藏在合法程式之中。有時使用者會意外的執行此軟體。其他時候這些軟體可能會利用漏洞自動執行。

UnauthorizedAccess (未授權的存取)

此值表示 GuardDuty 偵測到了非授權人員的可疑活動或可疑活動模式。

產生範例發現項目 GuardDuty

您可以使用 Amazon 產生範例發現項目， GuardDuty 以協助您視覺化並瞭解 GuardDuty 可產生的各種尋找類型。當您產生發現項目範例時，會針對每個支援的尋找項目類型， GuardDuty填入目前發現項目清單中的一個搜尋結果

產生的範例是使用預留位置填入的近似值。這些範例看起來可能與您環境的實際發現項目不同，但您可以使用它們來測試各種組態 GuardDuty，例如 CloudWatch 事件或篩選器。調查結果類型的可用值清單列在 調查結果類型 資料表中。

若要根據環境中的模擬活動產生一些常見的問題清單，請參閱下方自動產生常見的 GuardDuty發現。

透過 GuardDuty 主控台或 API 產生範例發現項目

選擇您偏好的存取方法，以便產生調查結果範例。

> **Note**
>
> 主控台方法會產生每個調查結果類型的其中一種。您只能透過 API 產生單一調查結果範例。

Console

請使用下列程序來產生問題清單範本。此程序會為每個尋找項目類型產生一個範例 GuardDuty 尋找項目

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/
2. 在導覽窗格中，選擇設定。
3. 在設定頁面的調查結果範例下，選擇產生調查結果範例。
4. 在導覽窗格中，選擇調查結果。此調查結果範例會顯示在目前調查結果頁面上，並有字首 [SAMPLE]。

API/CLI

您可以通過 CreateSampleFindingsAPI 生成匹配任何發 GuardDuty 現項目類型的單個示例查找項目，查找類型的可用值列在調查結果類型表中。

這對於測試 CloudWatch 事件規則或根據發現項目的自動化非常有用。以下範例顯示如何使用 AWS CLI來產生 `Backdoor:EC2/DenialOfService.Tcp` 類型的單一調查結果範例。

要查找您`detectorId`的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

```
aws guardduty create-sample-findings --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --finding-types Backdoor:EC2/DenialOfService.Tcp
```

透過這些方法產生的調查結果範例標題一律以主控台中的 [SAMPLE] 為開頭。在調查結果 JSON 詳細資訊的 additionalInfo 區段中，調查結果範例的值為 `"sample": true`。

自動產生常見的 GuardDuty發現

您可以使用下列指令碼自動產生數個常見 GuardDuty 發現項目。防護測試器 .template 使用 AWS CloudFormation 建立隔離的環境，其中包含防禦主機、可透過 SSH 存取的測試人員 Amazon EC2 執

行個體，以及兩個目標 EC2 執行個體。然後，您可以執行 guardduty_tester.sh 以啟動測試儀 EC2 執行個體、目標 Windows EC2 執行個體和目標 Linux EC2 執行個體之間的互動，以模擬五種類型的常見攻擊，這些攻擊 GuardDuty 可以偵測並通知您產生的發現項目。

1. 先決條件是，您必須 GuardDuty 在帳戶和區域中啟用您要執行保安測試員 .template 和 guardduty_tester.sh。如需啟用的詳細資訊 GuardDuty，請參閱開始使用 GuardDuty。

   您也必須在要執行這些指令碼的每個區域中，產生新的 EC2 金鑰對或使用現有的 EC2 金鑰對。這個 EC2 key pair 在您用來建立新堆疊的保護測試器 .template 指令碼中做為參數使用。CloudFormation 如需有關產生金鑰對的詳細資訊，請參閱 Amazon EC2 金鑰對。

2. 使用防護測試員 .template 建立新 CloudFormation 堆疊。如需有關建立堆疊的詳細指示，請參閱建立堆疊。在您執行 guardduty-tester.template 前，請以下列參數值對其進行修改：用以識別新堆疊的 Stack Name (堆疊名稱)，您想執行堆疊的區域 Availability Zone (可用區域)，以及您要用來啟動 EC2 執行個體的 Key Pair (金鑰對)。接著，您即可使用對應的私有金鑰，透過 SSH 存取 EC2 執行個體。

   guardduty-tester.template 需約 10 分鐘執行並完成。其將建立您的環境，並複製 guardduty_tester.sh 到您的 EC2 執行個體測試程式上。

3. 在 AWS CloudFormation 主控台中，選擇新執行中 AWS CloudFormation 堆疊旁邊的核取方塊。在顯示的一組標籤中，選取 Output (輸出) 標籤。請注意，IP 地址已指派給堡壘主機和 EC2 執行個體測試程式。您需要這兩種 IP 地址，以透過 SSH 存取測試程式 EC2 執行個體。

4. 在 ~/.ssh/config 檔案中建立下列項目，以透過堡壘主機登入至執行個體。

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

   現在您可以呼叫 $ ssh 測試程式以登入目標 EC2 執行個體。如需透過防禦主機設定和連線 EC2 執行個體的詳細資訊，請參閱 https://aws.amazon.com/blogs/security/ securely-connect-to-linux-instances-running-in-a-private-amazon-vpc/。

5. 連接到測試儀 EC2 實例後，運行 guardduty_tester.sh 以啟動測試人員和目標 EC2 實例之間的交互，模擬攻擊並生成 GuardDuty發現結果。

GuardDuty 發現項目的嚴重程度

每個 GuardDuty 發現項目都有指定的嚴重性等級和價值，這些值會反映發現項目可能對您的網路造成的潛在風險，由我們的安全工程師決定。嚴重性值可能落在 1.0 到 8.9 範圍內的任何位置，值越高，表示安全風險越大。為了協助您判斷發現項目所反白的潛在安全性問題的回應，請將此範圍劃 GuardDuty 分為「高」、「中」和「低」嚴重性層級。

> **Note**
>
> 值 0 和介於 9.0 到 10.0 目前預留供日後使用。

以下是 GuardDuty發現項目目前定義的嚴重性層級和值，以及各項的一般建議：

嚴重性等級	值範圍
高	7.0-8.9
「高」嚴重性等級表示有問題的資源 (EC2 執行個體或一組 IAM 使用者登入憑證) 遭到入侵，且目前正用於未經授權的用途。 建議您將任何「高」嚴重性的調查結果安全問題視為優先處理，並立即採取修復步驟，以防止進一步未經授權使用您的資源。例如，清除您的 EC2 執行個體或將其終止，或輪換 IAM 憑證。如需詳細資訊，請參閱修復步驟。	
中性	4.0
「中」嚴重性等級表示與正常觀察到的行為不同的可疑活動，視您的使用案例而定，可能表示資源遭受入侵。 我們建議您儘早調查相關資源。修復步驟會因資源和「調查結果」系列而有所不同，但一般來說，您應該要確認活動已獲授權，且符合您的使用案例。如果您無法確定原因或無法確認活動是否已獲授權，則應該將資源視為已遭到入侵，並遵循修復步驟來保護資源的安全。 以下是審查「中」嚴重性等級調查結果的一些注意事項：	

嚴重性等級	值範圍
• 檢查授權使用者是否安裝了變更資源行為的新軟體 (例如，允許高於正常流量，或啟用了新連接埠上的通訊)。 • 檢查授權使用者是否已變更控制面板設定，例如，修改安全群組設定。 • 在相關資源上執行防毒掃描，以偵測未經授權的軟體。 • 驗證連接至相關 IAM 角色、使用者、群組或憑證組的許可。這些可能需要變更或輪換。	
低	1.0 - 3.9
「低」嚴重性等級表示嘗試進行的可疑活動未危及您的網路，例如連接埠掃描或入侵嘗試失敗。 沒有立即建議採取的動作，但這項資訊值得注意，因為這可能表示有人正在尋找您網路中的弱點。	

GuardDuty 尋找彙總

所有發現項目都是動態的，這意味著，如果 GuardDuty 偵測到與相同安全性問題相關的新活動，它將以新資訊更新原始發現項目，而不是產生新的發現項目。此行為可讓您確定持續發生的問題，而不需要查看多份類似的報告，並減少您已注意到的安全問題所帶來的整體雜訊。

例如，對於 `UnauthorizedAccess:EC2/SSHBruteForce` 調查結果，對您的執行個體的多次存取嘗試將彙總到同一個調查結果 ID，這會增加調查結果詳細資訊中的計數。這是因為調查結果代表執行個體的單一安全問題，表示執行個體上的 SSH 連接埠未針對此類活動進行適當地保護。不過，如果 GuardDuty偵測到針對您環境中新執行個體的 SSH 存取活動，則會建立具有唯一尋找 ID 的新發現項目，以提醒您新資源存在安全性問題的事實。

彙總調查結果時，系統會使用該活動最近一次出現的資訊來進行更新。這表示在上述範例中，如果您的執行個體是新執行者嘗試執行暴力密碼破解的目標，將會更新調查結果詳細資訊，以反映最新來源的遠端 IP，而且將取代舊的資訊。有關個別活動嘗試的完整資訊仍會顯示在您的 CloudTrail或 VPC 流程記錄中。

警 GuardDuty 示產生新搜尋結果而非彙總現有發現項目的條件，取決於搜尋結果型態。每種調查結果類型的彙總條件由我們的安全工程師決定，為您提供帳戶內不同安全問題的最佳概觀。

尋找和分析 GuardDuty發現項目

使用下列程序來檢視和分析您的 GuardDuty 發現項目。

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/
2. 選擇調查結果，然後選取特定的調查結果以檢視其詳細資訊。

   根據調查結果類型、涉及的資源以及活動性質，每個調查結果的詳細資訊都會有所不同。如需可用調查結果欄位的詳細資訊，請參閱 調查結果詳細資訊。
3. (選用) 若要封存或下載調查結果，請從您的調查結果清單中選取對應調查結果，然後選擇動作選單。然後選擇 封存。

   從目前下拉式清單中選擇已封存，即可檢視已封存的調查結果。

   目前在 GuardDuty 成員帳戶中的 GuardDuty 使用者無法封存發現項目。

   > **Important**
   >
   > 如果您使用了上述程序手動封存了調查結果，則所有後續出現的此調查結果 (在封存完成後產生的) 將新增到目前的調查結果清單中。若之後不想在目前清單中再看到此調查結果，您可以將其設為自動封存。如需詳細資訊，請參閱 隱藏規則。
4. (選用) 若要下載調查結果，請從清單中選取調查結果，然後選擇動作功能表。然後選擇 匯出。當您匯出 調查結果時，您可以查看其完整的 JSON 文件。

   > **Note**
   >
   > 在某些情況下 GuardDuty ，意識到某些發現是誤報後，他們已經產生。 GuardDuty 在發現項目的 JSON 中提供 [信賴度] 欄位，並將其值設定為零。這種方式可以 GuardDuty 讓您知道您可以安全地忽略此類發現。

調查結果類型

如需 GuardDuty 發現項目類型的重要變更 (包括新增或已淘汰的尋找項目類型) 的相關資訊，請參閱Amazon 的文檔歷史 GuardDuty。

如需有關尋找現已淘汰之調查結果類型類型的詳細資訊，請參閱已淘汰的調查結果類型。

GuardDuty EC2 尋找類型

以下調查結果專用於 Amazon EC2 資源，而且一律具有 `Instance` 的資源類型。調查結果的嚴重性和詳細資訊會根據資源角色而有所不同，資源角色會指出 EC2 資源是可疑活動的目標，還是執行活動的執行者。

此處列出的調查結果包括用來產生該調查結果類型的資料來源和模型。如需有關資料來源和模型的詳細資訊，請參閱基礎資料來源。

> **Note**
>
> 如果執行個體已經終止，或者基礎 API 呼叫是來自不同區域中 EC2 執行個體的跨區域 API 呼叫的一部分，則某些 EC2 調查結果可能會遺失執行個體詳細資訊。

對於所有 EC2 調查結果，建議您檢查有問題的資源，以確定它是否以預期的方式運行。如果活動獲得授權，您可以使用隱藏規則或受信任的 IP 清單來防止該資源的誤判通知。如果活動是非預期的，安全最佳實務是假設執行個體已遭入侵，並採取修復可能遭到入侵的 Amazon EC2 執行個體中詳述的動作。

主題

- Backdoor:EC2/C&CActivity.B
- Backdoor:EC2/C&CActivity.B!DNS
- Backdoor:EC2/DenialOfService.Dns
- Backdoor:EC2/DenialOfService.Tcp
- Backdoor:EC2/DenialOfService.Udp
- Backdoor:EC2/DenialOfService.UdpOnTcpPorts
- Backdoor:EC2/DenialOfService.UnusualProtocol
- Backdoor:EC2/Spambot

- Behavior:EC2/NetworkPortUnusual
- Behavior:EC2/TrafficVolumeUnusual
- CryptoCurrency:EC2/BitcoinTool.B
- CryptoCurrency:EC2/BitcoinTool.B!DNS
- DefenseEvasion:EC2/UnusualDNSResolver
- DefenseEvasion:EC2/UnusualDoHActivity
- DefenseEvasion:EC2/UnusualDoTActivity
- Impact:EC2/AbusedDomainRequest.Reputation
- Impact:EC2/BitcoinDomainRequest.Reputation
- Impact:EC2/MaliciousDomainRequest.Reputation
- Impact:EC2/PortSweep
- Impact:EC2/SuspiciousDomainRequest.Reputation
- Impact:EC2/WinRMBruteForce
- Recon:EC2/PortProbeEMRUnprotectedPort
- Recon:EC2/PortProbeUnprotectedPort
- Recon:EC2/Portscan
- Trojan:EC2/BlackholeTraffic
- Trojan:EC2/BlackholeTraffic!DNS
- Trojan:EC2/DGADomainRequest.B
- Trojan:EC2/DGADomainRequest.C!DNS
- Trojan:EC2/DNSDataExfiltration
- Trojan:EC2/DriveBySourceTraffic!DNS
- Trojan:EC2/DropPoint
- Trojan:EC2/DropPoint!DNS
- Trojan:EC2/PhishingDomainRequest!DNS
- UnauthorizedAccess:EC2/MaliciousIPCaller.Custom
- UnauthorizedAccess:EC2/MetadataDNSRebind
- UnauthorizedAccess:EC2/RDPBruteForce
- UnauthorizedAccess:EC2/SSHBruteForce
- UnauthorizedAccess:EC2/TorClient

- UnauthorizedAccess:EC2/TorRelay

Backdoor:EC2/C&CActivity.B

EC2 執行個體正在查詢與已知為命令和控管伺服器相關聯的 IP。

預設嚴重性：高

- 資料來源：VPC 流量日誌

此調查結果會通知您，列出的 AWS 環境中的執行個體正在查詢與已知為命令和控管 (C&C) 伺服器相關聯的 IP。列出的執行個體可能遭到入侵。命令和控管伺服器是對殭屍網路的成員發出命令的電腦。

殭屍網路是一種透過常見惡意軟體感染和控制的網際網路連線裝置集合，可能包括 PC、伺服器、行動裝置及物聯網裝置。殭屍網路經常用來散佈惡意軟體和收集不當資訊，像是信用卡號碼。根據殭屍網路的用途和結構而定，C&C 伺服器也可能發出命令來展開分散式阻斷服務 (DDoS) 攻擊。

> **Note**
>
> 如果查詢的 IP 與 log4J 相關，則相關調查結果的欄位將包含下列值：
>
> - 服務。附加信息。 threatListName = Amazon
> - service.additionalInfo.threatName = Log4j Related

修復建議：

如果此活動為非預期活動，即代表您的執行個體可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到入侵的 Amazon EC2 執行個體。

Backdoor:EC2/C&CActivity.B!DNS

EC2 執行個體正在查詢與已知為命令和控管伺服器相關聯的網域名稱。

預設嚴重性：高

- 資料來源：DNS 日誌

此調查結果會通知您，列出的 AWS 環境中的執行個體正在查詢與已知為命令和控管 (C&C) 伺服器相關聯的網域名稱。列出的執行個體可能遭到入侵。命令和控管伺服器是對殭屍網路的成員發出命令的電腦。

殭屍網路是一種透過常見惡意軟體感染和控制的網際網路連線裝置集合，可能包括 PC、伺服器、行動裝置及物聯網裝置。殭屍網路經常用來散佈惡意軟體和收集不當資訊，像是信用卡號碼。根據殭屍網路的用途和結構而定，C&C 伺服器也可能發出命令來展開分散式阻斷服務 (DDoS) 攻擊。

> **Note**
>
> 如果查詢的網域名稱與 log4J 相關，則相關調查結果的欄位將包含下列值：
>
> - 服務。附加信息。 threatListName = Amazon
> - service.additionalInfo.threatName = Log4j Related

> **Note**
>
> 若要測試如何 GuardDuty 產生此尋找項目類型，您可以針對測試網域從執行個體 (使用 `dig` Linux 或 `nslookup` Windows) 發出 DNS 要求`guarddutyc2activityb.com`。

修復建議：

如果此活動為非預期活動，即代表您的執行個體可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到入侵的 Amazon EC2 執行個體。

Backdoor:EC2/DenialOfService.Dns

EC2 執行個體的表現方式，可能表示它被用來執行利用 DNS 通訊協定的阻斷服務 (DoS) 攻擊。

預設嚴重性：高

- 資料來源：VPC 流量日誌

此調查結果會通知您，列出的 AWS 環境中的 EC2 執行個體正在產生大量的傳出 DNS 流量。這可能表示列出的執行個體遭到入侵，並且正在使用 DNS 通訊協定執行 denial-of-service (DoS) 攻擊。

> **Note**
>
> 此調查結果偵測僅針對可公開路由 IP 地址 (DoS 攻擊的主要目標) 的 DoS 攻擊。

修復建議：

如果此活動為非預期活動，即代表您的執行個體可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到入侵的 Amazon EC2 執行個體。

Backdoor:EC2/DenialOfService.Tcp

EC2 執行個體的表現方式，表示它正用來執行利用 TCP 通訊協定的阻斷服務 (DoS) 攻擊。

預設嚴重性：高

- 資料來源：VPC 流量日誌

此調查結果會通知您，列出的 AWS 環境中的 EC2 執行個體正在產生大量的傳出 TCP 流量。這可能表示執行個體遭到入侵，並使用 TCP 通訊協定執行 denial-of-service (DoS) 攻擊。

> **Note**
>
> 此調查結果偵測僅針對可公開路由 IP 地址 (DoS 攻擊的主要目標) 的 DoS 攻擊。

修復建議：

如果此活動為非預期活動，即代表您的執行個體可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到入侵的 Amazon EC2 執行個體。

Backdoor:EC2/DenialOfService.Udp

EC2 執行個體的表現方式，表示它正用來執行利用 UDP 通訊協定的阻斷服務 (DoS) 攻擊。

預設嚴重性：高

- 資料來源：VPC 流量日誌

此調查結果會通知您，列出的 AWS 環境中的 EC2 執行個體正在產生大量的傳出 UDP 流量。這可能表示列出的執行個體遭到入侵，並且正在使用 UDP 通訊協定執行 denial-of-service (DoS) 攻擊。

> **Note**
>
> 此調查結果偵測僅針對可公開路由 IP 地址 (DoS 攻擊的主要目標) 的 DoS 攻擊。

修復建議：

如果此活動為非預期活動，即代表您的執行個體可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到入侵的 Amazon EC2 執行個體。

Backdoor:EC2/DenialOfService.UdpOnTcpPorts

EC2 執行個體的表現方式，可能表示它被用來執行在 TCP 連接埠上利用 UDP 通訊協定的阻斷服務 (DoS) 攻擊。

預設嚴重性：高

- 資料來源：VPC 流量日誌

此調查結果會通知您，列出的 AWS 環境中的 EC2 執行個體正產生大量的傳出 UDP 流量，而這些流量是以 TCP 通訊常用的連接埠為目標。這可能表示列出的執行個體遭到入侵，並且正在使用 TCP 連接埠上的 UDP 通訊協定執行 denial-of-service (DoS) 攻擊。

> **Note**
>
> 此調查結果偵測僅針對可公開路由 IP 地址 (DoS 攻擊的主要目標) 的 DoS 攻擊。

修復建議：

如果此活動為非預期活動，即代表您的執行個體可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到入侵的 Amazon EC2 執行個體。

Backdoor:EC2/DenialOfService.UnusualProtocol

EC2 執行個體的表現方式，可能表示它被用來執行利用不常見通訊協定的阻斷服務 (DoS) 攻擊。

預設嚴重性：高

- 資料來源：VPC 流量日誌

此調查結果會通知您，列出的 AWS 環境中的 EC2 執行個體正從不常見的通訊協定類型產生傳出大量流量，EC2 執行個體通常不會使用該通訊協定 (例如，網際網路組管理協定)。這可能表示執行個體遭到入侵，而且正在使用不尋常的通訊協定執行 denial-of-service (DoS) 攻擊。此調查結果偵測僅針對可公開路由 IP 地址 (DoS 攻擊的主要目標) 的 DoS 攻擊。

修復建議：

如果此活動為非預期活動，即代表您的執行個體可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到入侵的 Amazon EC2 執行個體。

Backdoor:EC2/Spambot

EC2 執行個體正在連接埠 25 上與遠端主機通訊，此舉展現出不尋常的行為。

預設嚴重性：中

- 資料來源：VPC 流量日誌

此調查結果會通知您，列出的 AWS 環境中的 EC2 執行個體正在與連接埠 25 上的遠端主機進行通訊。此行為並不尋常，因為此 EC2 執行個體先前並沒有在連接埠 25 上通訊的歷程記錄。連接埠 25 以往是郵件伺服器進行 SMTP 通訊時使用。此調查結果表示您的 EC2 執行個體可能已遭受入侵，無法用於傳送垃圾郵件。

修復建議：

如果此活動為非預期活動，即代表您的執行個體可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到入侵的 Amazon EC2 執行個體。

Behavior:EC2/NetworkPortUnusual

EC2 執行個體正在不尋常的伺服器連接埠上與遠端主機通訊。

預設嚴重性：中

- 資料來源：VPC 流量日誌

此調查結果會通知您，列出的 AWS 環境中的 EC2 執行個體正在進行與既有基準不同的行為。此 EC2 執行個體先前並沒有在此遠端連接埠上通訊的歷程記錄。

> **Note**
>
> 如果 EC2 執行個體在連接埠 389 或連接埠 1389 上通訊，則相關聯的調查結果嚴重性會修改為「高」，而調查結果欄位將包含下列值：
>
> - service.additionalInfo.context = Possible log4j callback

修復建議：

如果此活動為非預期活動，即代表您的執行個體可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到入侵的 Amazon EC2 執行個體。

Behavior:EC2/TrafficVolumeUnusual

EC2 執行個體與遠端主機之間產生異常大量的網路流量。

預設嚴重性：中

- 資料來源：VPC 流量日誌

此調查結果會通知您，列出的 AWS 環境中的 EC2 執行個體正在進行與既有基準不同的行為。此 EC2 執行個體先前並沒有傳送如此大流量至此遠端主機的歷程記錄。

修復建議：

如果此活動為非預期活動，即代表您的執行個體可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到入侵的 Amazon EC2 執行個體。

CryptoCurrency:EC2/BitcoinTool.B

EC2 執行個體正在查詢與加密貨幣活動有關聯的 IP 地址。

預設嚴重性：高

- 資料來源：VPC 流量日誌

此調查結果會通知您，列出的 AWS 環境中的 EC2 執行個體正在查詢與比特幣或其他加密貨幣活動有關聯的 IP 地址。比特幣是一種全球性的加密貨幣和數位支付系統，可以用來兌換其他貨幣，產品和服務。比特幣是比特幣開採的獎勵，受到威脅參與者的高度追捧。

修復建議：

如果您使用此 EC2 執行個體來開採或管理加密貨幣，或者此執行個體以其他方式參與區塊鏈活動，則此調查結果可能是您環境的預期活動。如果您的 AWS 環境是這種情況，建議您為此調查結果設定隱藏規則。隱藏規則應包含兩個篩選準則。第一個條件應該使用調查結果類型屬性，其值為 `CryptoCurrency:EC2/BitcoinTool.B`。第二個篩選條件應該是區塊鏈活動中涉及之執行個體的 Instance ID (執行個體 ID)。若要進一步了解如何建立隱藏規則，請參閱隱藏規則。

如果此活動非預期，表示您的執行個體可能遭到破壞，請參閱修復可能遭到入侵的 Amazon EC2 執行個體。

CryptoCurrency:EC2/BitcoinTool.B!DNS

EC2 執行個體正在查詢與加密貨幣活動有關聯的網域名稱。

預設嚴重性：高

- 資料來源：DNS 日誌

此調查結果會通知您，列出的 AWS 環境中的 EC2 執行個體正在查詢與比特幣或其他加密貨幣活動有關聯的網域名稱。比特幣是一種全球性的加密貨幣和數位支付系統，可以用來兌換其他貨幣，產品和服務。比特幣是比特幣開採的獎勵，受到威脅參與者的高度追捧。

修復建議：

如果您使用此 EC2 執行個體來開採或管理加密貨幣，或者此執行個體以其他方式參與區塊鏈活動，則此調查結果可能是您環境的預期活動。如果您的 AWS 環境是這種情況，建議您為此調查結果

設定隱藏規則。隱藏規則應包含兩個篩選準則。第一個條件應該使用調查結果類型屬性，其值為 `CryptoCurrency:EC2/BitcoinTool.B!DNS`。第二個篩選條件應該是區塊鏈活動中涉及之執行個體的 Instance ID (執行個體 ID)。若要進一步了解如何建立隱藏規則，請參閱隱藏規則。

如果此活動非預期，表示您的執行個體可能遭到破壞，請參閱修復可能遭到入侵的 Amazon EC2 執行個體。

DefenseEvasion:EC2/UnusualDNSResolver

Amazon EC2 執行個體正在與一個不尋常的公有 DNS 解析程式進行通訊。

預設嚴重性：中

- 資料來源：VPC 流量日誌

此調查結果會通知您，列出的 AWS 環境中的 Amazon EC2 執行個體正在進行與既有基準行為不同的行為。此 EC2 執行個體最近沒有與此公有 DNS 解析程式通訊的歷史記錄。 GuardDuty 主控台中「尋找項目詳細資料」面板中的「異常」欄位可提供查詢 DNS 解析程式的相關資訊。

修復建議：

如果此活動為非預期活動，即代表您的執行個體可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到入侵的 Amazon EC2 執行個體。

DefenseEvasion:EC2/UnusualDoHActivity

Amazon EC2 執行個體正在通過 HTTPS (DoH) 通訊執行不尋常的 DNS。

預設嚴重性：中

- 資料來源：VPC 流量日誌

此調查結果會通知您，列出的 AWS 環境中的 Amazon EC2 執行個體正在進行與既有基準不同的行為。此 EC2 執行個體沒有任何最近透過 HTTPS (DoH) 與此公有 DoH 伺服器通訊的 DNS 歷史記錄。調查結果詳細資訊中的不尋常欄位可提供有關查詢 DoH 伺服器的資訊。

修復建議：

如果此活動為非預期活動，即代表您的執行個體可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到入侵的 Amazon EC2 執行個體。

DefenseEvasion:EC2/UnusualDoTActivity

Amazon EC2 執行個體正在通過 TLS (DoT) 通訊執行不尋常的 DNS。

預設嚴重性：中

- 資料來源：VPC 流量日誌

此調查結果會通知您，列出的 AWS 環境中的 EC2 執行個體正在進行與既有基準不同的行為。此 EC2 執行個體沒有任何最近透過 TLS (DoT) 與此公有 DoT 伺服器通訊的 DNS 歷史記錄。調查結果詳細資訊中的不尋常欄位面板可提供有關查詢 DoT 伺服器的資訊。

修復建議：

如果此活動為非預期活動，即代表您的執行個體可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到入侵的 Amazon EC2 執行個體。

Impact:EC2/AbusedDomainRequest.Reputation

EC2 執行個體正在查詢與已知濫用網域相關聯的低信譽網域名稱。

預設嚴重性：中

- 資料來源：DNS 日誌

此調查結果會通知您，列出的 AWS 環境中的 Amazon EC2 執行個體正在查詢與已知濫用網域或 IP 地址相關聯的低信譽網域名稱。濫用網域的範例包括頂層網域名稱 (TLD) 和第二層網域名稱 (2LD)，提供免費的子網域註冊，以及動態 DNS 提供者。威脅執行者傾向於使用這些服務免費或低成本註冊網域。此類別中的低信譽網域也可能是解析為註冊機構停駐 IP 地址的過期網域，因此可能不再處於作用中狀態。停駐 IP 是註冊機構為尚未連結到任何服務的網域引導流量的地方。列出的 Amazon EC2 執行個體可能已遭入侵，因為威脅參與者通常使用這些註冊機構或服務進行 C&C 和惡意軟體分發。

低信譽網域以信譽評分模型為基礎。此模型會評估網域的特徵並對其進行排名，以判斷其為惡意的可能性。

修復建議：

如果此活動為非預期活動，即代表您的執行個體可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到入侵的 Amazon EC2 執行個體。

Impact:EC2/BitcoinDomainRequest.Reputation

EC2 執行個體正在查詢與加密貨幣活動有關聯的低信譽網域名稱。

預設嚴重性：高

- 資料來源：DNS 日誌

此調查結果會通知您，列出的 AWS 環境中的 Amazon EC2 執行個體正在查詢與比特幣或其他加密貨幣活動有關聯的低信譽網域名稱。比特幣是一種全球性的加密貨幣和數位支付系統，可以用來兌換其他貨幣，產品和服務。比特幣是比特幣開採的獎勵，受到威脅參與者的高度追捧。

低信譽網域以信譽評分模型為基礎。此模型會評估網域的特徵並對其進行排名，以判斷其為惡意的可能性。

修復建議：

如果您使用此 EC2 執行個體來開採或管理加密貨幣，或者此執行個體以其他方式參與區塊鏈活動，則此調查結果可能代表您環境的預期活動。如果您的 AWS 環境是這種情況，建議您為此調查結果設定隱藏規則。隱藏規則應包含兩個篩選準則。第一個條件應該使用調查結果類型屬性，其值為 `Impact:EC2/BitcoinDomainRequest.Reputation`。第二個篩選條件應該是區塊鏈活動中涉及之執行個體的 Instance ID (執行個體 ID)。若要進一步了解如何建立隱藏規則，請參閱隱藏規則。

如果此活動非預期，表示您的執行個體可能遭到破壞，請參閱修復可能遭到入侵的 Amazon EC2 執行個體。

Impact:EC2/MaliciousDomainRequest.Reputation

EC2 執行個體正在查詢與已知惡意網域相關聯的低信譽網域。

預設嚴重性：高

- 資料來源：DNS 日誌

此調查結果會通知您，列出的 AWS 環境中的 Amazon EC2 執行個體正在查詢與已知惡意網域或 IP 地址相關聯的低信譽網域名稱。例如，網域可能與已知的沉洞 IP 地址相關聯。沉洞網域是先前由威脅執行者控制的網域，對其提出的請求可能表示執行個體已遭到入侵。這些網域也可能與已知的惡意活動或網域產生演算法相關。

低信譽網域以信譽評分模型為基礎。此模型會評估網域的特徵並對其進行排名，以判斷其為惡意的可能性。

修復建議：

如果此活動為非預期活動，即代表您的執行個體可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到入侵的 Amazon EC2 執行個體。

Impact:EC2/PortSweep

EC2 執行個體正在探查大量 IP 地址上的連接埠。

預設嚴重性：高

- 資料來源：VPC 流量日誌

此調查結果會通知您，列出的 AWS 環境中的 EC2 執行個體正在探查大量公開路由 IP 地址上的連接埠。這種類型的活動通常用於尋找易受攻擊的主機來利用。在 GuardDuty 主機的尋找詳細資料面板中，只會顯示最新的遠端 IP 位址

修復建議：

如果此活動為非預期活動，即代表您的執行個體可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到入侵的 Amazon EC2 執行個體。

Impact:EC2/SuspiciousDomainRequest.Reputation

EC2 執行個體正在查詢低信譽的網域名稱，該網域名稱本質上因其使用期限或低受歡迎程度而可疑。

預設嚴重性：低

- 資料來源：DNS 日誌

此調查結果會通知您，列出的 AWS 環境中的 Amazon EC2 執行個體正在查詢疑似惡意的低信譽網域名稱。注意到該網域的特徵與先前觀察到的惡意網域一致，但是，我們的聲譽模型無法明確地將其與已知威脅聯繫起來。這些網域通常是新觀察到的，或接收少量的流量。

低信譽網域以信譽評分模型為基礎。此模型會評估網域的特徵並對其進行排名，以判斷其為惡意的可能性。

修復建議：

如果此活動為非預期活動，即代表您的執行個體可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到入侵的 Amazon EC2 執行個體。

Impact:EC2/WinRMBruteForce

EC2 執行個體正在執行傳出 Windows 遠端管理暴力破解攻擊。

預設嚴重性：低*

> **Note**
>
> 如果您的 EC2 執行個體是暴力密碼破解攻擊的目標，則此調查結果的嚴重性為「低」。如果您的 EC2 執行個體是用來執行暴力密碼破解攻擊的執行者，則此調查結果嚴重性為「高」。

- 資料來源：VPC 流量日誌

此調查結果項目會通知您，列出的 AWS 環境中的 EC2 執行個體正在執行 Windows 遠端管理 (WinRM) 暴力攻擊，旨在取得 Windows 系統上對 Windows 遠端管理服務的存取權。

修復建議：

如果此活動為非預期活動，即代表您的執行個體可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到入侵的 Amazon EC2 執行個體。

Recon:EC2/PortProbeEMRUnprotectedPort

EC2 執行個體有一個未受保護的 EMR 相關連接埠，正由已知的惡意主機探測。

預設嚴重性：高

- 資料來源：VPC 流量日誌

此發現項目會通知您，屬於您AWS環境中叢集一部分的所列 EC2 執行個體上的 EMR 相關敏感連接埠，不會受到安全群組、存取控制清單 (ACL) 或主機上防火牆 (例如 Linux IPTabes) 所封鎖。此發現項目也會通知網際網路上已知的掃描程式正在主動探查此連接埠。觸發此調查結果的連接埠 (如連接埠 8088 (YARN Web UI 連接埠))，可能會被用來遠端執行程式碼。

修復建議：

您應該封鎖從網際網路開放存取叢集上的連接埠，並限制只有需要存取這些連接埠的特定 IP 地址才能存取。如需詳細資訊，請參閱 EMR 叢集的安全群組。

Recon:EC2/PortProbeUnprotectedPort

EC2 執行個體有一個未受保護的連接埠，正由已知的惡意主機探測。

預設嚴重性：低*

> **Note**
>
> 此調查結果的預設嚴重性為「低」。不過，如果正在探查的連接埠是由彈性搜尋 (9200 或 9300) 使用，則發現項目的嚴重性為「高」。

- 資料來源：VPC 流量日誌

此調查結果項目會通知您，列出的 AWS 環境中的 EC2 執行個體上的連接埠未由安全群組、存取控制清單 (ACL) 或主機上的防火牆 (例如 Linux IPTables) 以及網際網路上的已知掃描程式封鎖，且正在被積極的探測。

如果已識別的未受保護連接埠是 22 或 3389，且您正在使用這些連接埠連線到您的執行個體，您仍然可以透過僅允許來自公司的網路 IP 地址空間的 IP 地址，來存取這些連接埠以限制曝光。若要在 Linux 上限制存取連接埠 22，請參閱授權 Linux 執行個體的傳入流量。若要在 Windows 上限制存取連接埠 3389，請參閱授權 Windows 執行個體的傳入流量。

GuardDuty 不會針對連接埠 443 和 80 產生此發現項目。

修復建議：

在某些情況下，可能會刻意暴露執行個體，例如，若是託管在 Web 伺服器上。如果您的 AWS 環境是這種情況，建議您為此調查結果設定隱藏規則。隱藏規則應包含兩個篩選準則。第一個條件應該使用調查結果類型屬性，其值為 Recon:EC2/PortProbeUnprotectedPort。第二個篩選條件應該找出執行個體或做為堡壘主機的執行個體。您可以使用執行個體映像 ID 屬性或標籤值屬性，視主控這些工具的執行個體可識別的準則而定。如需有關建立隱藏規則的詳細資訊，請參閱隱藏規則。

如果此活動非預期，表示您的執行個體可能遭到破壞，請參閱修復可能遭到入侵的 Amazon EC2 執行個體。

Recon:EC2/Portscan

EC2 執行個體正在對遠端主機執行傳出連接埠掃描。

預設嚴重性：中

- 資料來源：VPC 流量日誌

此調查結果項目會通知您，列出的 AWS 環境中的 EC2 執行個體已遭受可能的連接埠掃描攻擊，因為它正試圖在短時間內連接到多個連接埠。連接埠掃描攻擊的目的是找出開放連接埠，以探索該機器正在執行的服務並識別其作業系統。

修復建議：

當漏洞評定應用程式部署在環境中的 EC2 執行個體上時，此調查結果可能是誤判，因為這些應用程式會執行連接埠掃描，以警告您開放連接埠設定不當。如果您的 AWS 環境是這種情況，建議您為此調查結果設定隱藏規則。隱藏規則應包含兩個篩選準則。第一個條件應該使用調查結果類型屬性，其值為 Recon:EC2/Portscan。第二個篩選條件應該找出主控這些漏洞評定工具的執行個體。您可以使用執行個體映像 ID 屬性或標籤值屬性，視主控這些工具的執行個體可識別的條件而定。如需有關建立隱藏規則的詳細資訊，請參閱隱藏規則。

如果此活動非預期，表示您的執行個體可能遭到破壞，請參閱修復可能遭到入侵的 Amazon EC2 執行個體。

Trojan:EC2/BlackholeTraffic

EC2 執行個體正在嘗試與已知黑洞的遠端主機 IP 地址進行通訊。

預設嚴重性：中

- 資料來源：VPC 流量日誌

此調查結果會通知您，列出的 AWS 環境中的 EC2 執行個體可能會遭入侵，因為它正在試圖與黑洞 (或漏洞) 的 IP 地址進行通訊。黑洞是在網路上某些傳入或傳出流量會被無聲無息丟棄的地方，且資料來源也不會收到資料未傳送至收件人的通知。黑洞的 IP 地址會指定為未執行的主機，或未分配主機的地址。

修復建議：

如果此活動為非預期活動，即代表您的執行個體可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到入侵的 Amazon EC2 執行個體。

Trojan:EC2/BlackholeTraffic!DNS

EC2 執行個體正在查詢重新導向到黑洞 IP 地址的網域名稱。

預設嚴重性：中

- 資料來源：DNS 日誌

此調查結果會通知您，列出的 AWS 環境中的 EC2 執行個體可能會遭入侵，因為它正在查詢被重新導向至黑洞 IP 地址的網域名稱。黑洞是在網路上某些傳入或傳出流量會被無聲無息丟棄的地方，且資料來源也不會收到資料未傳送至收件人的通知。

修復建議：

如果此活動為非預期活動，即代表您的執行個體可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到入侵的 Amazon EC2 執行個體。

Trojan:EC2/DGADomainRequest.B

EC2 執行個體正在查詢演算法產生的網域。這種網域常遭惡意軟體利用，且可以做為 EC2 執行個體已被盜用的跡象。

預設嚴重性：高

- 資料來源：DNS 日誌

此調查結果會通知您，列出的 AWS 環境中的 EC2 執行個體正在嘗試查詢網域產生演算法 (DGA) 網域。您的 EC2 執行個體可能遭到盜用。

DGA 可用來定期產生大量網域名稱，這些名稱可做為他們的命令與控制 (C&C) 伺服器的會合點。命令和控管伺服器是對殭屍網路的成員發出命令的電腦，這是一種透過常見惡意軟體感染和控制的網際網路連線裝置集合。大量潛在的會合點會造成難以有效地關閉殭屍網路，因為受感染的電腦每天都會嘗試聯繫其中一些網域名稱以接收更新或命令。

> **Note**
>
> 此調查結果是根據使用進階啟發式網域名稱分析，且可以識別威脅情報饋送中不存在的新 DGA 域。

修復建議：

如果此活動為非預期活動，即代表您的執行個體可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到入侵的 Amazon EC2 執行個體。

Trojan:EC2/DGADomainRequest.C!DNS

EC2 執行個體正在查詢演算法產生的網域。這種網域常遭惡意軟體利用，且可以做為 EC2 執行個體已被盜用的跡象。

預設嚴重性：高

- 資料來源：DNS 日誌

此調查結果會通知您，列出的 AWS 環境中的 EC2 執行個體正在嘗試查詢網域產生演算法 (DGA) 網域。您的 EC2 執行個體可能遭到盜用。

DGA 可用來定期產生大量網域名稱，這些名稱可做為他們的命令與控制 (C&C) 伺服器的會合點。命令和控管伺服器是對殭屍網路的成員發出命令的電腦，這是一種透過常見惡意軟體感染和控制的網際網路

連線裝置集合。大量潛在的會合點會造成難以有效地關閉殭屍網路，因為受感染的電腦每天都會嘗試聯繫其中一些網域名稱以接收更新或命令。

> **Note**
>
> 此發現項目是以威脅情報摘要中已知 GuardDuty的 DGA 網域為基礎。

修復建議：

如果此活動為非預期活動，即代表您的執行個體可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到入侵的 Amazon EC2 執行個體。

Trojan:EC2/DNSDataExfiltration

EC2 執行個體是透過 DNS 查詢移植資料的。

預設嚴重性：高

- 資料來源：DNS 日誌

此調查結果會通知您，列出的 AWS 環境中的 EC2 執行個體正在執行使用 DNS 查詢的惡意軟體，進行對外資料傳輸。這種類型的資料傳輸表示執行個體遭到入侵，可能導致資料外洩。DNS 流量通常不會被防火牆阻擋。例如，遭侵入 EC2 執行個體中的惡意軟體可以將資料 (例如，您的信用卡號) 編碼到 DNS 查詢中，並將它傳送到攻擊者所控制的遠端 DNS 伺服器。

修復建議：

如果此活動為非預期活動，即代表您的執行個體可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到入侵的 Amazon EC2 執行個體。

Trojan:EC2/DriveBySourceTraffic!DNS

EC2 執行個體正在查詢已知為 Drive-By (路過式) 下載攻擊來源的遠端主機網域名稱。

預設嚴重性：高

- 資料來源：DNS 日誌

此調查結果會通知您，列出的 AWS 環境中的 EC2 執行個體可能會遭入侵，因為它正在查詢已知為 Drive-By (路過式) 下載攻擊來源的遠端主機網域名稱。這些是從網際網路上意外下載的電腦軟體，它們可以觸發病毒、間諜軟體或惡意軟體的自動安裝。

修復建議：

如果此活動為非預期活動，即代表您的執行個體可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到入侵的 Amazon EC2 執行個體。

Trojan:EC2/DropPoint

EC2 執行個體正在嘗試與遠端主機的 IP 地址進行通信，該主機已知會保存由惡意軟體擷取的登入資料和其他遭竊資料。

預設嚴重性：中

- 資料來源：VPC 流量日誌

此調查結果會通知您，AWS 環境中的 EC2 執行個體正在嘗試與遠端主機 IP 地址進行通訊，該主機已知存放了惡意軟體擷取的憑證和其他遭竊資料。

修復建議：

如果此活動為非預期活動，即代表您的執行個體可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到入侵的 Amazon EC2 執行個體。

Trojan:EC2/DropPoint!DNS

EC2 執行個體正在查詢遠端主機的網域名稱，該主機已知會保存由惡意軟體擷取的登入資料和其他遭竊資料。

預設嚴重性：中

- 資料來源：DNS 日誌

此調查結果會通知您，AWS 環境中的 EC2 執行個體正在查詢已知存放登入資料和惡意軟體擷取的其他遭竊資料的遠端主機網域名稱。

修復建議：

如果此活動為非預期活動，即代表您的執行個體可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到入侵的 Amazon EC2 執行個體。

Trojan:EC2/PhishingDomainRequest!DNS

EC2 執行個體正在查詢遭釣魚攻擊的網域。您的 EC2 執行個體可能遭到盜用。

預設嚴重性：高

- 資料來源：DNS 日誌

此調查結果會通知您，在 AWS 環境中有一個 EC2 執行個體正在嘗試查詢遭釣魚攻擊的網域。釣魚網域是由冒充合法機構的人所建立，以誘使個人提供敏感資料，如個人身分資訊、銀行和信用卡詳細資訊以及密碼。您的 EC2 執行個體可能試圖擷取儲存在釣魚網站上的敏感資料，或者嘗試設定網路釣魚網站。您的 EC2 執行個體可能遭到盜用。

修復建議：

如果此活動為非預期活動，即代表您的執行個體可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到入侵的 Amazon EC2 執行個體。

UnauthorizedAccess:EC2/MaliciousIPCaller.Custom

EC2 執行個體正在連線到自訂威脅清單上的 IP 地址。

預設嚴重性：中

- 資料來源：VPC 流量日誌

此調查結果通知您，AWS 環境中的 EC2 執行個體正在與您上傳的威脅清單上所包含的 IP 地址進行通訊。在 GuardDuty 中，威脅清單是由已知的惡意 IP 地址所組成。 GuardDuty 會根據上傳的威脅清單產生問題清單。用於產生此調查結果的威脅清單會列在調查結果詳細資訊中。

修復建議：

如果此活動為非預期活動，即代表您的執行個體可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到入侵的 Amazon EC2 執行個體。

UnauthorizedAccess:EC2/MetadataDNSRebind

EC2 執行個體正在執行 DNS 查詢，以解析執行個體中繼資料服務。

預設嚴重性：高

- 資料來源：DNS 日誌

此調查結果會通知您，AWS 環境中的 EC2 執行個體正在查詢解析為 EC2 中繼資料 IP 地址 (169.254.169.254) 的網域。這種類型的 DNS 查詢可能表示執行個體是 DNS 重新繫結技術的目標。此技術可用於從 EC2 執行個體獲取中繼資料，包含與執行個體相關聯的 IAM 憑證。

DNS 重新繫結涉及誘使在 EC2 執行個體上執行的應用程式從 URL 載入傳回資料，URL 中的網域名稱解析為 EC2 中繼資料的 IP 地址 (169.254.169.254)。這會導致應用程式存取 EC2 中繼資料，並可能讓攻擊者能夠使用。

只有在 EC2 執行個體執行的具漏洞應用程式允許注入 URL，或有人在 EC2 執行個體上執行的 Web 瀏覽器存取 URL 時，才可能使用 DNS 重新繫結存取 EC2 中繼資料。

修復建議：

為了回應此調查結果，您應該評估是否有在 EC2 執行個體上執行的具漏洞應用程式，或是有人使用瀏覽器存取調查結果中所識別的網域。如果根本原因是具漏洞的應用程式，您應該修復該漏洞。如果有人瀏覽已識別的網域，您應該封鎖該網域或防止使用者存取該網域。如果您判斷此調查結果與上述任一案例有關，請撤銷與 EC2 執行個體相關聯的工作階段。

有些 AWS 客戶會刻意將中繼資料 IP 地址對應至其授權 DNS 伺服器上的網域名稱。如果您的 環境是這種情況，建議您為此調查結果設定隱藏規則。隱藏規則應包含兩個篩選準則。第一個條件應該使用調查結果類型屬性，其值為 `UnauthorizedAccess:EC2/MetaDataDNSRebind`。第二個篩選條件應該是 DNS request domain (DNS 請求網域)，而且值應該符合您對應至中繼資料 IP 地址 (169.254.169.254) 的網域。如需建立隱藏規則的詳細資訊，請參閱隱藏規則。

UnauthorizedAccess:EC2/RDPBruteForce

EC2 執行個體已遭受 RDP 暴力密碼破解攻擊。

預設嚴重性：低*

> **Note**
>
> 如果您的 EC2 執行個體是暴力密碼破解攻擊的目標，則此調查結果的嚴重性為「低」。如果您的 EC2 執行個體是用來執行暴力密碼破解攻擊的執行者，則此調查結果嚴重性為「高」。

- 資料來源：VPC 流量日誌

此調查結果會通知您，AWS 環境中的 EC2 執行個體正遭受暴力破解攻擊，此攻擊目標在獲取以 Windows 為基礎系統上的 RDP 服務密碼。這可能表示您的 AWS 資源有未經授權的存取。

修復建議：

如果您執行個體的資源角色是 `ACTOR`，這表示您的執行個體已用於執行 RDP 暴力密碼破解攻擊。除非該執行個體有正當理由連線列為 `Target` 的 IP 地址，否則建議假設您的執行個體已遭受入侵，並採取修復可能遭到入侵的 Amazon EC2 執行個體 中所列的動作。

如果執行個體的資源角色 為 `TARGET`，可透過安全群組、ACL 或防火牆，僅針對可信任 IP 保護您的 SSH 連接埠，從而修復此調查結果。如需詳細資訊，請參閱 Tips for securing your EC2 instances (Linux)。

UnauthorizedAccess:EC2/SSHBruteForce

EC2 執行個體已遭受 SSH 暴力密碼破解攻擊。

預設嚴重性：低*

> **Note**
>
> 如果暴力攻擊法的目標是您的其中一個 EC2 執行個體，則此調查結果的嚴重性為低。如果您的 EC2 執行個體被用來執行暴力攻擊法，則此調查結果嚴重性為高。

- 資料來源：VPC 流量日誌

此調查結果會通知您，AWS 環境中的 EC2 執行個體正遭受暴力破解攻擊，此攻擊目標在獲取以 Linux 為基礎系統上的 SSH 服務密碼。這可能表示您的 AWS 資源有未經授權的存取。

> **Note**
>
> 此調查結果只會透過連接埠 22 上的監控流量來產生。如果您的 SSH 服務已設定為使用其他連接埠，則此調查結果將不會產生。

修復建議：

如果暴力密碼破解嘗試的目標是堡壘主機，這可能代表 AWS 環境的預期行為。如果是這種情況，我們建議您為此調查結果設定隱藏規則。隱藏規則應包含兩個篩選準則。第一個條件應該使用調查結果類型屬性，其值為 `UnauthorizedAccess:EC2/SSHBruteForce`。第二個篩選條件應該找出執行個體或做為堡壘主機的執行個體。您可以使用執行個體映像 ID 屬性或標籤值屬性，視主控這些工具的執行個體可識別的條件而定。如需有關建立隱藏規則的詳細資訊，請參閱隱藏規則。

如果預計您的環境不會有這項活動，而且執行個體的 Resource Role (資源角色) 為 `TARGET`，可透過安全群組、ACL 或防火牆，僅針對可信任 IP 保護您的 SSH 連接埠，從而修復此調查結果。如需詳細資訊，請參閱 Tips for securing your EC2 instances (Linux)。

如果您執行個體的資源角色 是 `ACTOR`，這表示執行個體已用於執行 SSH 暴力密碼破解攻擊。除非該執行個體有正當理由連線列為 `Target` 的 IP 地址，否則建議假設您的執行個體已遭受入侵，並採取 修復可能遭到入侵的 Amazon EC2 執行個體 中所列的動作。

UnauthorizedAccess:EC2/TorClient

您的 EC2 執行個體正在連線至 Tor Guard 或 Authority 節點。

預設嚴重性：高

- 資料來源：VPC 流量日誌

此調查結果通知您，AWS 環境中的 EC2 執行個體正在連線至 Tor Guard 或 Authority 節點。Tor 是一種啟用匿名通訊的軟體。Tor Guards 和 Authority 節點為進入 Tor 網路的初始閘道。此流量表示此 EC2 執行個體已洩露且做為 Tor 網路的用戶端。此調查結果可能表示您的 AWS 資源有未經授權的存取，目的是隱藏攻擊者的真實身分。

修復建議：

如果此活動為非預期活動，即代表您的執行個體可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到入侵的 Amazon EC2 執行個體。

UnauthorizedAccess:EC2/TorRelay

您的 EC2 執行個體正在連線至 Tor 網路，且連線方式為顯示為代表 Tor 轉送。

預設嚴重性：高

- 資料來源：VPC 流量日誌

此調查結果會通知您，AWS 環境中的 EC2 執行個體正在與 Tor 網路進行連線，其連線方式表明它正在作為 Tor 轉送。Tor 是一種啟用匿名通訊的軟體。Tor 增加匿名通訊，做法是從一個 Tor 轉送轉寄使用者端潛在非法流量至另一個 Tor 轉送。

修復建議：

如果此活動為非預期活動，即代表您的執行個體可能已遭入侵。如需更多詳細資訊，請參閱 修復可能遭到入侵的 Amazon EC2 執行個體。

GuardDuty IAM 尋找項目類型

以下調查結果專用於 IAM 實體和存取金鑰，而且一律具有 `AccessKey` 的資源類型。調查結果的嚴重性和詳細資訊依據調查結果類型而有所不同。

此處列出的調查結果包括用來產生該調查結果類型的資料來源和模型。如需詳細資訊，請參閱 基礎資料來源。

對於所有與 IAM 相關的調查結果，我們建議您檢查有問題的實體，並確保其許可依循最低權限的最佳實務。如果此活動為非預期活動，即代表憑證可能已遭入侵。如需有關修復調查結果的詳細資訊，請參閱修復可能遭到破壞 AWS 的認證。

主題

- CredentialAccess:IAMUser/AnomalousBehavior
- DefenseEvasion:IAMUser/AnomalousBehavior

- Discovery:IAMUser/AnomalousBehavior
- Exfiltration:IAMUser/AnomalousBehavior
- Impact:IAMUser/AnomalousBehavior
- InitialAccess:IAMUser/AnomalousBehavior
- PenTest:IAMUser/KaliLinux
- PenTest:IAMUser/ParrotLinux
- PenTest:IAMUser/PentooLinux
- Persistence:IAMUser/AnomalousBehavior
- Policy:IAMUser/RootCredentialUsage
- PrivilegeEscalation:IAMUser/AnomalousBehavior
- Recon:IAMUser/MaliciousIPCaller
- Recon:IAMUser/MaliciousIPCaller.Custom
- Recon:IAMUser/TorIPCaller
- Stealth:IAMUser/CloudTrailLoggingDisabled
- Stealth:IAMUser/PasswordPolicyChange
- UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B
- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS
- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS
- UnauthorizedAccess:IAMUser/MaliciousIPCaller
- UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom
- UnauthorizedAccess:IAMUser/TorIPCaller

CredentialAccess:IAMUser/AnomalousBehavior

以異常方式叫用來取得 AWS 環境存取權的 API。

預設嚴重性：中

- 資料來源：CloudTrail 管理事件

此調查結果會通知您，在您的帳戶中觀察到異常的 API 請求。此調查結果可能包含由單一使用者身分在鄰近提出的單一 API 或一系列相關 API 請求。當對手嘗試收集您的環境之密碼、使用

者名稱和存取金鑰時，觀察到的 API 通常與攻擊的憑證存取階段相關聯。此類別中的 API 為 `GetPasswordData`、`GetSecretValue` 和 `GenerateDbAuthToken`。

透 GuardDuty過異常偵測機器學習 (ML) 模型，將此 API 要求識別為異常狀況。ML 模型會評估帳戶中的所有 API 請求，並識別與對手使用的技術相關聯的異常事件。ML 模型會追蹤 API 要求的各種因素，例如發出請求的使用者、發出請求的位置，以及請求的特定 API。有關對於調用要求的使用者身份而言，哪些是不常見 API 請求的詳細資訊，請參閱調查結果詳細資訊。

修復建議：

如果此活動為非預期活動，即代表您的憑證可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到破壞 AWS 的認證。

DefenseEvasion:IAMUser/AnomalousBehavior

用於逃避防禦措施的 API 調用方式異常。

預設嚴重性：中

- 資料來源：CloudTrail 管理事件

此調查結果會通知您，在您的帳戶中觀察到異常的 API 請求。此調查結果可能包含由單一使用者身分在鄰近提出的單一 API 或一系列相關 API 請求。觀察到的 API 通常與防禦逃稅策略有關，其中對手嘗試掩蓋其追蹤與避免檢測。此類別中的 API 通常是刪除、停用或停止操作，例如 `DeleteFlowLogs`、`DisableAlarmActions` 或 `StopLogging`。

透 GuardDuty過異常偵測機器學習 (ML) 模型，將此 API 要求識別為異常狀況。ML 模型會評估帳戶中的所有 API 請求，並識別與對手使用的技術相關聯的異常事件。ML 模型會追蹤 API 要求的各種因素，例如發出請求的使用者、發出請求的位置，以及請求的特定 API。有關對於調用要求的使用者身份而言，哪些是不常見 API 請求的詳細資訊，請參閱調查結果詳細資訊。

修復建議：

如果此活動為非預期活動，即代表您的憑證可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到破壞 AWS 的認證。

Discovery:IAMUser/AnomalousBehavior

常用來探索資源的 API 調用方式異常。

預設嚴重性：低

- 資料來源：CloudTrail 管理事件

此調查結果會通知您，在您的帳戶中觀察到異常的 API 請求。此調查結果可能包含由單一使用者身分在鄰近提出的單一 API 或一系列相關 API 請求。當對手收集資訊以判斷您的 AWS 環境是否容易受到更廣泛的攻擊時，觀察到的 API 通常與攻擊的發現階段相關聯。此類別中的 API 通常是取得、描述或列出操作，例如 `DescribeInstances`、`GetRolePolicy` 或 `ListAccessKeys`。

透 GuardDuty過異常偵測機器學習 (ML) 模型，將此 API 要求識別為異常狀況。ML 模型會評估帳戶中的所有 API 請求，並識別與對手使用的技術相關聯的異常事件。ML 模型會追蹤 API 要求的各種因素，例如發出請求的使用者、發出請求的位置，以及請求的特定 API。有關對於調用要求的使用者身份而言，哪些是不常見 API 請求的詳細資訊，請參閱調查結果詳細資訊。

修復建議：

如果此活動為非預期活動，即代表您的憑證可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到破壞 AWS 的認證。

Exfiltration:IAMUser/AnomalousBehavior

常用來從 AWS 環境收集資料的 API 以異常的方式叫用。

預設嚴重性：高

- 資料來源：CloudTrail 管理事件

此調查結果會通知您，在您的帳戶中觀察到異常的 API 請求。此調查結果可能包含由單一使用者身分在鄰近提出的單一 API 或一系列相關 API 請求。觀察到的 API 通常與外流策略有關，其中對手試圖使用封裝和加密，從您的網路收集資料以避免偵測。此調查結果類型的 API 僅為管理 (控制平面) 操作，通常與 S3、快照和資料庫相關，例如 `PutBucketReplication`、`CreateSnapshot` 或 `RestoreDBInstanceFromDBSnapshot`。

透 GuardDuty過異常偵測機器學習 (ML) 模型，將此 API 要求識別為異常狀況。ML 模型會評估帳戶中的所有 API 請求，並識別與對手使用的技術相關聯的異常事件。ML 模型會追蹤 API 要求的各種因素，例如發出請求的使用者、發出請求的位置，以及請求的特定 API。有關對於調用要求的使用者身份而言，哪些是不常見 API 請求的詳細資訊，請參閱調查結果詳細資訊。

修復建議：

如果此活動為非預期活動，即代表您的憑證可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到破壞 AWS 的認證。

Impact:IAMUser/AnomalousBehavior

以異常方式叫用常用來竄改 AWS 環境中的資料或程序的 API。

預設嚴重性：高

- 資料來源：CloudTrail 管理事件

此調查結果會通知您，在您的帳戶中觀察到異常的 API 請求。此調查結果可能包含由單一使用者身分在鄰近提出的單一 API 或一系列相關 API 請求。觀察到的 API 通常與影響策略相關聯，其中對手嘗試中斷操作與操縱、中斷或銷毀帳戶中的資料。此調查結果類型的 API 通常為刪除、更新或 PUT 操作，例如 `DeleteSecurityGroup`、`UpdateUser` 或 `PutBucketPolicy`。

透 GuardDuty過異常偵測機器學習 (ML) 模型，將此 API 要求識別為異常狀況。ML 模型會評估帳戶中的所有 API 請求，並識別與對手使用的技術相關聯的異常事件。ML 模型會追蹤 API 要求的各種因素，例如發出請求的使用者、發出請求的位置，以及請求的特定 API。有關對於調用要求的使用者身份而言，哪些是不常見 API 請求的詳細資訊，請參閱調查結果詳細資訊。

修復建議：

如果此活動為非預期活動，即代表您的憑證可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到破壞 AWS 的認證。

InitialAccess:IAMUser/AnomalousBehavior

常用來取得未經授權存取 AWS 環境的 API 會以異常的方式叫用。

預設嚴重性：中

- 資料來源：CloudTrail 管理事件

此調查結果會通知您，在您的帳戶中觀察到異常的 API 請求。此調查結果可能包含由單一使用者身分在鄰近提出的單一 API 或一系列相關 API 請求。當對手嘗試建置對您環境的存取權限時，觀察到

的 API 通常與攻擊的初始存取階段相關聯。此類別中的 API 通常是取得權杖或工作階段操作，例如 `GetFederationToken`、`StartSession` 或 `GetAuthorizationToken`。

透 GuardDuty過異常偵測機器學習 (ML) 模型，將此 API 要求識別為異常狀況。ML 模型會評估帳戶中的所有 API 請求，並識別與對手使用的技術相關聯的異常事件。ML 模型會追蹤 API 要求的各種因素，例如發出請求的使用者、發出請求的位置，以及請求的特定 API。有關對於調用要求的使用者身份而言，哪些是不常見 API 請求的詳細資訊，請參閱調查結果詳細資訊。

修復建議：

如果此活動為非預期活動，即代表您的憑證可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到破壞 AWS 的認證。

PenTest:IAMUser/KaliLinux

一個 API 是從卡利 Linux 機器調用的。

預設嚴重性：中

- 資料來源：CloudTrail 管理事件

此發現會通知您執行 Kali Linux 的機器正在使用屬於您環境中所列 AWS 帳戶的認證進行 API 呼叫。Kali Linux 是一種安全專業人員所使用的熱門滲透測試工具，以在需要修補的 EC2 執行個體中找出弱點。攻擊者也會使用此工具找出 EC2 組態弱點，並取得您 AWS 環境的未經授權存取權。

修復建議：

如果此活動為非預期活動，即代表您的憑證可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到破壞 AWS 的認證。

PenTest:IAMUser/ParrotLinux

已從 Parrot Security Linux 機器調用一個 API。

預設嚴重性：中

- 資料來源：CloudTrail 管理事件

此發現會通知您執行 Parrot Security Linux 的電腦正在使用屬於您環境中所列 AWS 帳戶的認證進行 API 呼叫。Parrot Security Linux 是一種安全專業人員所使用的熱門滲透測試工具，以在需要修補的 EC2 執行個體中找出弱點。攻擊者也會使用此工具找出 EC2 組態弱點，並取得您 AWS 環境的未經授權存取權。

修復建議：

如果此活動為非預期活動，即代表您的憑證可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到破壞 AWS 的認證。

PenTest:IAMUser/PentooLinux

已從 Pentoo Linux 機器調用一個 API。

預設嚴重性：中

- 資料來源：CloudTrail 管理事件

此發現項目會通知您執行 Pentoo Linux 的電腦正在使用屬於您環境中所列 AWS 帳戶的認證進行 API 呼叫。Pentoo Linux 是一種安全專業人員所使用的熱門滲透測試工具，以在需要修補的 EC2 執行個體中找出弱點。攻擊者也會使用此工具找出 EC2 組態弱點，並取得您 AWS 環境的未經授權存取權。

修復建議：

如果此活動為非預期活動，即代表您的憑證可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到破壞 AWS 的認證。

Persistence:IAMUser/AnomalousBehavior

常用來維護 AWS 環境未經授權存取的 API 會以異常的方式叫用。

預設嚴重性：中

- 資料來源：CloudTrail 管理事件

此調查結果會通知您，在您的帳戶中觀察到異常的 API 請求。此調查結果可能包含由單一使用者身分在鄰近提出的單一 API 或一系列相關 API 請求。觀察到的 API 通常與持續性策略相關聯，其中對

手已取得您的環境的存取權限，並嘗試維護該存取權限。此類別中的 API 通常是建立、匯入或修改操作，例如 `CreateAccessKey`、`ImportKeyPair` 或 `ModifyInstanceAttribute`。

透 GuardDuty過異常偵測機器學習 (ML) 模型，將此 API 要求識別為異常狀況。ML 模型會評估帳戶中的所有 API 請求，並識別與對手使用的技術相關聯的異常事件。ML 模型會追蹤 API 要求的各種因素，例如發出請求的使用者、發出請求的位置，以及請求的特定 API。有關對於調用要求的使用者身份而言，哪些是不常見 API 請求的詳細資訊，請參閱調查結果詳細資訊。

修復建議：

如果此活動為非預期活動，即代表您的憑證可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到破壞 AWS 的認證。

Policy:IAMUser/RootCredentialUsage

使用根使用者登入憑證調用 API。

預設嚴重性：低

- 資料來源：CloudTrail 管理事件或 CloudTrail 資料事件

這個調查結果會通知您，列出的環境中的 AWS 帳戶 的根使用者登入憑證正用於向 AWS 服務提出請求。建議使用者永遠不要使用 root 使用者登入認證來存取 AWS 服務。相反地，應該使用 AWS Security Token Service (STS) 的最低權限臨時登入資料來存取 AWS 服務。對於不支援 AWS STS 的情況，建議使用 IAM 使用者憑證。如需詳細資訊，請參閱 IAM 最佳實務。

> **Note**
>
> 如果為帳戶啟用 S3 威脅偵測，則可能會產生此調查結果，以回應嘗試使用 AWS 帳戶的根使用者登入憑證在 S3 資源上執行 S3 資料平面操作的嘗試。使用的 API 呼叫會列示在調查結果詳細資訊中。如果未啟用 S3 威脅偵測，則此調查結果只能由事件日誌 API 觸發。如需有關 S3 威脅偵測的資訊，請參閱 S3 保護。

修復建議：

如果此活動為非預期活動，即代表您的憑證可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到破壞 AWS 的認證。

PrivilegeEscalation:IAMUser/AnomalousBehavior

常用來取得 AWS 環境的高階權限的 API 會以異常的方式叫用。

預設嚴重性：中

- 資料來源：CloudTrail 管理事件

此調查結果會通知您，在您的帳戶中觀察到異常的 API 請求。此調查結果可能包含由單一使用者身分在鄰近提出的單一 API 或一系列相關 API 請求。觀察到的 API 通常與權限提升策略相關聯，其中對手嘗試取得環境的較更高層級許可。此類別中的 API 通常涉及變更 IAM 政策、角色和使用者的操作，例如 `AssociateIamInstanceProfile`、`AddUserToGroup` 或 `PutUserPolicy`。

透 GuardDuty過異常偵測機器學習 (ML) 模型，將此 API 要求識別為異常狀況。ML 模型會評估帳戶中的所有 API 請求，並識別與對手使用的技術相關聯的異常事件。ML 模型會追蹤 API 要求的各種因素，例如發出請求的使用者、發出請求的位置，以及請求的特定 API。有關對於調用要求的使用者身份而言，哪些是不常見 API 請求的詳細資訊，請參閱調查結果詳細資訊。

修復建議：

如果此活動為非預期活動，即代表您的憑證可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到破壞 AWS 的認證。

Recon:IAMUser/MaliciousIPCaller

從已知惡意 IP 地址呼叫的 API。

預設嚴重性：中

- 資料來源：CloudTrail 管理事件

此調查結果會通知您，可列出或描述在您的環境內之帳戶中 AWS 資源的 API 操作，已從威脅清單中包含的 IP 地址被調用。攻擊者可能會使用竊取的認證來執行這種類型的 AWS 資源偵察，以尋找更有價值的認證或判斷其已擁有的認證的功能。

修復建議：

如果此活動為非預期活動，即代表您的憑證可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到破壞 AWS 的認證。

Recon:IAMUser/MaliciousIPCaller.Custom

從已知惡意 IP 地址呼叫的 API。

預設嚴重性：中

- 資料來源：CloudTrail 管理事件

此調查結果會通知您，可列出或描述在您的環境內之帳戶中 AWS 資源的 API 操作，已從自訂威脅清單中包含的 IP 地址被調用。使用的威脅清單會列在問題清單詳細資訊中。攻擊者可能會使用遭竊的認證來執行這種類型的 AWS 資源偵察，以尋找更有價值的認證或判斷其已擁有的認證的功能。

修復建議：

如果此活動為非預期活動，即代表您的憑證可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到破壞 AWS 的認證。

Recon:IAMUser/TorIPCaller

從 Tor 退出節點的 IP 地址呼叫 API。

預設嚴重性：中

- 資料來源：CloudTrail 管理事件

此調查結果會通知您，可列出或描述在您的環境內之帳戶中 AWS 資源的 API 操作，已從 Tor 退出節點 IP 地址被調用。Tor 是一種啟用匿名通訊的軟體。它會透過一系列網路節點之間的中繼來加密並隨機反彈通訊。最後的 Tor 節點稱為退出節點。攻擊者會使用 Tor 遮罩他們的真實身分。

修復建議：

如果此活動為非預期活動，即代表您的憑證可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到破壞 AWS 的認證。

Stealth:IAMUser/CloudTrailLoggingDisabled

AWS CloudTrail 記錄已停用。

預設嚴重性：低

- 資料來源：CloudTrail 管理事件

此發現項目會通知您 AWS 環境中的 CloudTrail 追蹤已停用。這可能是攻擊者嘗試停用日誌，以透過消除對其活動的任何追蹤進而掩蓋其蹤跡，同時為了惡意目的而取得對您的 AWS 資源之存取權限。可以透過成功刪除或更新線索來觸發此問題清單。成功刪除 S3 儲存貯體會從與之相關聯的追蹤中儲存日誌的 S3 儲存貯體觸發此發現 GuardDuty。

修復建議：

如果此活動為非預期活動，即代表您的憑證可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到破壞 AWS 的認證。

Stealth:IAMUser/PasswordPolicyChange

帳戶密碼政策已減弱。

預設嚴重性：低*

> **Note**
>
> 根據密碼政策變更的嚴重性，此問題清單的嚴重性可以是「低」、「中」或「高」。

- 資料來源：CloudTrail 管理事件

在您的 AWS 環境中列出的 AWS 帳戶上，帳戶密碼策略已被削弱。例如，它已被刪除或更新為要求較少的字元、不需要符號和數字，或要求延長密碼過期時段。嘗試更新或刪除您的 AWS 帳戶密碼政策也可以觸發此發現。 AWS 帳戶密碼政策會定義規則，以管理可為 IAM 使用者設定哪些類型的密碼。較弱的密碼政策將允許建立易於記憶且可能更容易猜測的密碼，從而產生安全風險。

修復建議：

如果此活動為非預期活動，即代表您的憑證可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到破壞 AWS 的認證。

UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B

已觀察到多個全球主控台成功登入。

預設嚴重性：中

- 資料來源：CloudTrail 管理事件

此問題清單會通知您在不同的地理位置、同一時間觀察到同一個 IAM 使用者的多個成功控制台登入。這種異常和有風險的存取位置模式表明，可能會在未經授權的情況下存取 AWS 您

修復建議：

如果此活動為非預期活動，即代表您的憑證可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到破壞 AWS 的認證。

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS

透過執行個體啟動角色專為 EC2 執行個體建立的憑證，正在從 AWS內的其他帳戶中使用。

預設嚴重性：高*

> **Note**
>
> 此調查結果的預設嚴重性為「高」。但是，如果 API 是由與您的 AWS 環境相關聯的帳戶調用，則嚴重性為「中」。

- 資料來源：CloudTrail 管理事件或 S3 資料事件

此發現項目會通知您何時使用 EC2 執行個體登入資料從與執行關聯 EC2 執行個體所在 AWS 帳戶不同的 IP 地址叫用 API。

AWS 不建議將臨時登入資料重新分配到建立這些登入資料的實體之外 (例如， AWS 應用程式、EC2 或 Lambda)。但是，授權的使用者可以從其 EC2 執行個體匯出登入資料以進行合法的 API 呼叫。如果

該remoteAccountDetails.Affiliated字段是True從與您的 AWS 環境關聯的帳戶調用 API。如要排除潛在攻擊並驗證活動的合法性，請與指派這些登入資料的 IAM 使用者聯繫。

> **Note**
>
> 如果從遠端帳戶 GuardDuty 觀察持續的活動，其機器學習 (ML) 模型會將其識別為預期的行為。因此， GuardDuty 將停止針對該遠端帳戶的活動產生此發現項目。 GuardDuty 將繼續從其他遠端帳戶產生新行為的發現結果，並會隨著行為隨著時間的推移而重新評估已學習的遠端帳戶。

修復建議：

針對此調查結果，您可以使用下列工作流程來決定動作方案：

1. 從 service.action.awsApiCallAction.remoteAccountDetails.accountId 欄位識別涉及的遠端帳戶。
2. 接下來從service.action.awsApiCallAction.remoteAccountDetails.affiliated現場確定該帳戶是否與您的 GuardDuty環境相關聯。
3. 如果帳戶是附屬帳戶，請聯絡遠端帳戶擁有者和 EC2 執行個體憑證的擁有者以進行調查。
4. 如果該帳戶不是關聯帳戶，首先評估該帳戶與您的組織相關聯，但不是 GuardDuty多帳戶設定的一部分，或者尚 GuardDuty 未在帳戶中啟用。否則，請聯絡 EC2 憑證的擁有者，以確定是否有遠端帳戶使用這些憑證的使用案例。
5. 如果憑證的擁有者無法辨識遠端帳戶，則憑證可能已遭到在 AWS內運作的威脅執行者入侵。您應該採取 修復可能遭到入侵的 Amazon EC2 執行個體 中建議的步驟來保護您的環境。此外，您可以向 AWS 信任與安全團隊提交濫用報告，以開始對遠端帳戶進行調查。向 AWS 信任與安全提交您的報告時，請包括該調查結果的完整 JSON 詳細資訊。

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS

透過執行個體啟動角色且專為 EC2 執行個體建立的登入資料，正在從外部 IP 地址使用。

預設嚴重性：高

- 資料來源：CloudTrail 管理事件或 S3 資料事件

此發現項目會通知您，以外的主機 AWS 已嘗試使用在 AWS 環境中 EC2 執行個體上建立的臨時 AWS 登入資料執行 AWS API 作業。列出的 EC2 執行個體可能已遭到入侵，而且此執行個體的臨時登入資料可能已洩漏至其他地方的遠端主機。 AWS AWS 不建議將臨時登入資料重新分配到建立這些登入資料的實體之外 (例如， AWS 應用程式、EC2 或 Lambda)。但是，授權的使用者可以從其 EC2 執行個體匯出登入資料以進行合法的 API 呼叫。若要排除潛在攻擊並驗證活動的合法性，請驗證是否需要在調查結果中使用來自遠端 IP 的執行個體憑證。

> **Note**
>
> 如果從遠端帳戶 GuardDuty 觀察持續的活動，其機器學習 (ML) 模型會將其識別為預期的行為。因此， GuardDuty 將停止針對該遠端帳戶的活動產生此發現項目。 GuardDuty 將繼續從其他遠端帳戶產生新行為的發現結果，並會隨著行為隨著時間的推移而重新評估已學習的遠端帳戶。

修復建議：

當將網路設定為路由網際網路流量，使其從內部部署閘道而不是從 VPC 網際網路閘道 (IGW) 輸出時，就會產生此調查結果。一般組態 (例如使用 AWS Outposts 或 VPC VPN 連接) 可能會導致流量以這種方式路由。如果這是預期的行為，我們建議您使用抑制規則，並建立包含兩個篩選條件準則的規則。第一個條件是 finding type (問題清單類型)，應該是 `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS`。第二個篩選條件是具有內部部署網際網路閘道 IP 地址或 CIDR 範圍的 API 呼叫者 IPv4 地址。若要進一步了解如何建立隱藏規則，請參閱隱藏規則。

> **Note**
>
> 如果 GuardDuty 觀察到來自外部來源的持續活動，則其機器學習模型會將其識別為預期行為，並停止針對該來源的活動產生此發現項目。 GuardDuty 將繼續從其他來源產生新行為的發現結果，並會隨著行為隨著時間的推移而重新評估已學到的來源。

如果此活動非預期，即代表您的登入資料可能已遭入侵，請參閱修復可能遭到破壞 AWS 的認證。

UnauthorizedAccess:IAMUser/MaliciousIPCaller

從已知惡意 IP 地址呼叫的 API。

預設嚴重性：中

- 資料來源：CloudTrail 管理事件

此發現項目會通知您 API 作業 (例如，嘗試啟動 EC2 執行個體、建立新的 IAM 使用者或修改您的 AWS 權限) 已從已知的惡意 IP 位址叫用。這可能表示未經授權存取您環境中的 AWS 資源。

修復建議：

如果此活動為非預期活動，即代表您的憑證可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到破壞 AWS 的認證。

UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom

從自訂威脅清單上的 IP 地址呼叫的 API。

預設嚴重性：中

- 資料來源：CloudTrail 管理事件

此發現項目會通知您，API 作業 (例如，嘗試啟動 EC2 執行個體、建立新的 IAM 使用者或修改 AWS 權限) 是從您上傳的威脅清單中包含的 IP 位址叫用的。在 ，威脅清單包含已知的惡意 IP 地址。這可能表示未經授權存取您環境中的 AWS 資源。

修復建議：

如果此活動為非預期活動，即代表您的憑證可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到破壞 AWS 的認證。

UnauthorizedAccess:IAMUser/TorIPCaller

從 Tor 退出節點的 IP 地址呼叫 API。

預設嚴重性：中

- 資料來源：CloudTrail 管理事件

此調查結果會通知您，API 操作 (例如，嘗試啟動 EC2 執行個體、建立新的 IAM 使用者，或修改 AWS 權限) 已從 Tor 退出節點 IP 地址被調用。Tor 是一種啟用匿名通訊的軟體。它會透過一系列網路節點之間的中繼來加密並隨機反彈通訊。最後的 Tor 節點稱為退出節點。這可能表示您的 AWS 資源有未經授權的存取，目的是隱藏攻擊者的真實身分。

修復建議：

如果此活動為非預期活動，即代表您的憑證可能已遭入侵。如需更多詳細資訊，請參閱 修復可能遭到破壞 AWS 的認證。

EKS 稽核記錄尋找類型

以下調查結果專用於 Kubernetes 資源，而且具有 `EKSCluster` 的 resource_type。調查結果的嚴重性和詳細資訊依據調查結果類型而有所不同。

對於所有 Kubernetes 類型調查結果，我們建議您檢查有問題的資源，以確定該活動是預期還是潛在的惡意活動。如需修正發現項目所識別之遭入侵 Kubernetes 資源的指引，請參閱。 GuardDuty 修復 EKS 稽核日誌監控調查結果

> **Note**
>
> 如果預期有此活動 (因其產生這些調查結果)，請考慮新增 隱藏規則 以防止未來出現警報。

主題

- CredentialAccess:Kubernetes/MaliciousIPCaller
- CredentialAccess:Kubernetes/MaliciousIPCaller.Custom
- CredentialAccess:Kubernetes/SuccessfulAnonymousAccess
- CredentialAccess:Kubernetes/TorIPCaller
- DefenseEvasion:Kubernetes/MaliciousIPCaller
- DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom
- DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess
- DefenseEvasion:Kubernetes/TorIPCaller
- Discovery:Kubernetes/MaliciousIPCaller
- Discovery:Kubernetes/MaliciousIPCaller.Custom

- Discovery:Kubernetes/SuccessfulAnonymousAccess
- Discovery:Kubernetes/TorIPCaller
- Execution:Kubernetes/ExecInKubeSystemPod
- Impact:Kubernetes/MaliciousIPCaller
- Impact:Kubernetes/MaliciousIPCaller.Custom
- Impact:Kubernetes/SuccessfulAnonymousAccess
- Impact:Kubernetes/TorIPCaller
- Persistence:Kubernetes/ContainerWithSensitiveMount
- Persistence:Kubernetes/MaliciousIPCaller
- Persistence:Kubernetes/MaliciousIPCaller.Custom
- Persistence:Kubernetes/SuccessfulAnonymousAccess
- Persistence:Kubernetes/TorIPCaller
- Policy:Kubernetes/AdminAccessToDefaultServiceAccount
- Policy:Kubernetes/AnonymousAccessGranted
- Policy:Kubernetes/ExposedDashboard
- Policy:Kubernetes/KubeflowDashboardExposed
- PrivilegeEscalation:Kubernetes/PrivilegedContainer
- CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated
- Execution:Kubernetes/AnomalousBehavior.ExecInPod
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer
- Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount
- Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated
- Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

> **Note**
>
> 在 Kubernetes 版本 1.14 之前，依預設，`system:unauthenticated`群組已與 () 相關聯。`system:discovery` `system:basic-user` ClusterRoles此關聯可能會允許匿名使用者的非預期存取。叢集更新不會撤銷這些許可。即使您將叢集更新至 1.14 或更高版本，仍可能會

啟用這些權限。建議您取消這些許可與 `system:unauthenticated` 群組的關聯。如需撤銷這些許可的指引，請參閱 Amazon EKS 使用者指南中的 Amazon EKS 安全性最佳實務。

CredentialAccess:Kubernetes/MaliciousIPCaller

從已知的惡意 IP 地址調用了 Kubernetes 叢集中常用來存取憑證或秘密的 API。

預設嚴重性：高

- 功能：EKS 稽核記錄

此調查結果會通知您，從與已知惡意活動關聯的 IP 地址調用了 API 操作。觀察到的 API 通常與對手嘗試為 Kubernetes 叢集收集密碼、使用者名稱和存取金鑰的憑證存取策略相關聯。

修復建議：

如果本`KubernetesUserDetails`節下發現項目中報告的使用者是`system:anonymous`，請按照 Amazon EKS 使用者指南中 Amazon EKS 安全性最佳實務中的指示，調查為何允許匿名使用者叫用 API 並撤銷許可 (如有需要)。如果使用者是經過驗證的使用者，請調查以確定該活動是否為合法或惡意的活動。如果活動是惡意的，請撤銷使用者的存取權限，並還原對手對您的叢集所做的任何變更。如需詳細資訊，請參閱 修復 EKS 稽核日誌監控調查結果。

CredentialAccess:Kubernetes/MaliciousIPCaller.Custom

從自訂威脅清單上的 IP 地址調用了常用來存取 Kubernetes 叢集中之憑證或秘密的 API。

預設嚴重性：高

- 功能：EKS 稽核記錄

此調查結果會通知您，從您上傳的威脅清單上所包含的 IP 地址調用了 API 操作。與此調查結果相關聯的威脅清單會列在調查結果詳細資訊的其他資訊區段中。觀察到的 API 通常與對手嘗試為 Kubernetes 叢集收集密碼、使用者名稱和存取金鑰的憑證存取策略相關聯。

修復建議：

如果本KubernetesUserDetails節下發現項目中報告的使用者是system:anonymous，請依照 Amazon EKS 使用者指南中 Amazon EKS 安全性最佳實務中的指示，調查為何允許匿名使用者叫用 API，並視需要撤銷許可。如果使用者是經過驗證的使用者，請調查以確定該活動是否為合法或惡意的活動。如果活動是惡意的，請撤銷使用者的存取權限，並還原對手對您的叢集所做的任何變更。如需詳細資訊，請參閱 修復 EKS 稽核日誌監控調查結果。

CredentialAccess:Kubernetes/SuccessfulAnonymousAccess

未經驗證的使用者調用 Kubernetes 叢集中常用來存取憑證或秘密的 API。

預設嚴重性：高

- 功能：EKS 稽核記錄

此調查結果會通知您，system:anonymous 使用者已成功調用 API 操作。由 system:anonymous 進行的 API 呼叫未經驗證。觀察到的 API 通常與對手嘗試為 Kubernetes 叢集收集密碼、使用者名稱和存取金鑰的憑證存取策略相關聯。此活動表示在調查結果中報告的 API 動作允許匿名或未經驗證的存取，並且可能在其他動作上允許匿名或未經驗證的存取。如果未預期出現這種行為，則可能表示組態錯誤或您的憑證遭到入侵。

修復建議：

您應該檢查已向叢集上 system:anonymous 使用者授與的許可，並確保所有許可都是必要的。如果錯誤或惡意地授與許可，您應該撤銷使用者的存取權限，並還原對手對叢集所做的任何變更。如需詳細資訊，請參閱 Amazon EKS 使用者指南中的 Amazon EKS 安全性最佳實務。

如需詳細資訊，請參閱 修復 EKS 稽核日誌監控調查結果。

CredentialAccess:Kubernetes/TorIPCaller

從 Tor 退出節點 IP 地址調用一個常用來存取 Kubernetes 叢集中之憑證或秘密的 API。

預設嚴重性：高

- 功能：EKS 稽核記錄

此調查結果會通知您，已從 Tor 退出節點 IP 地址調用 API。觀察到的 API 通常與對手嘗試為 Kubernetes 叢集收集密碼、使用者名稱和存取金鑰的憑證存取策略相關聯。Tor 是一種啟用匿名通

訊的軟體。它會透過一系列網路節點之間的中繼來加密並隨機反彈通訊。最後的 Tor 節點稱為退出節點。這可能表示您的 Kubernetes 叢集資源有未經授權的存取，目的是隱藏攻擊者的真實身分。

修復建議：

如果本KubernetesUserDetails節下發現項目中報告的使用者是system:anonymous，請按照 Amazon EKS 使用者指南中 Amazon EKS 安全性最佳實務中的指示，調查為何允許匿名使用者叫用 API 並撤銷許可 (如有需要)。如果使用者是經過驗證的使用者，請調查以確定該活動是否為合法或惡意的活動。如果活動是惡意的，請撤銷使用者的存取權限，並還原對手對您的叢集所做的任何變更。如需詳細資訊，請參閱 修復 EKS 稽核日誌監控調查結果。

DefenseEvasion:Kubernetes/MaliciousIPCaller

從已知的惡意 IP 地址調用的常用來逃避防禦措施的 API。

預設嚴重性：高

- 功能：EKS 稽核記錄

此調查結果會通知您，從與已知惡意活動關聯的 IP 地址調用了 API 操作。觀察到的 API 通常與防禦逃稅策略有關，其中對手嘗試隱藏其行動以避免檢測。

修復建議：

如果本KubernetesUserDetails節下發現項目中報告的使用者是system:anonymous，請按照 Amazon EKS 使用者指南中 Amazon EKS 安全性最佳實務中的指示，調查為何允許匿名使用者叫用 API 並撤銷許可 (如有需要)。如果使用者是經過驗證的使用者，請調查以確定該活動是否為合法或惡意的活動。如果活動是惡意的，請撤銷使用者的存取權限，並還原對手對您的叢集所做的任何變更。如需詳細資訊，請參閱 修復 EKS 稽核日誌監控調查結果。

DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom

從自訂威脅清單上的 IP 地址調用常用來逃避防禦措施的 API。

預設嚴重性：高

- 功能：EKS 稽核記錄

此調查結果會通知您，從您上傳的威脅清單上所包含的 IP 地址調用了 API 操作。與此調查結果相關聯的威脅清單會列在調查結果詳細資訊的其他資訊區段中。觀察到的 API 通常與防禦逃稅策略有關，其中對手嘗試隱藏其行動以避免檢測。

修復建議：

如果本KubernetesUserDetails節下發現項目中報告的使用者是system:anonymous，請按照 Amazon EKS 使用者指南中 Amazon EKS 安全性最佳實務中的指示，調查為何允許匿名使用者叫用 API 並撤銷許可 (如有需要)。如果使用者是經過驗證的使用者，請調查以確定該活動是否為合法或惡意的活動。如果活動是惡意的，請撤銷使用者的存取權限，並還原對手對您的叢集所做的任何變更。如需詳細資訊，請參閱 修復 EKS 稽核日誌監控調查結果。

DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess

由經驗證使用者調用常用來逃避防禦措施的 API。

預設嚴重性：高

- 功能：EKS 稽核記錄

此調查結果會通知您，system:anonymous 使用者已成功調用 API 操作。由 system:anonymous 進行的 API 呼叫未經驗證。觀察到的 API 通常與防禦逃稅策略有關，其中對手嘗試隱藏其行動以避免檢測。此活動表示在調查結果中報告的 API 動作允許匿名或未經驗證的存取，並且可能在其他動作上允許匿名或未經驗證的存取。如果未預期出現這種行為，則可能表示組態錯誤或您的憑證遭到入侵。

修復建議：

您應該檢查已向叢集上 system:anonymous 使用者授與的許可，並確保所有許可都是必要的。如果錯誤或惡意地授與許可，您應該撤銷使用者的存取權限，並還原對手對叢集所做的任何變更。如需詳細資訊，請參閱 Amazon EKS 使用者指南中的 Amazon EKS 安全性最佳實務。

如需詳細資訊，請參閱 修復 EKS 稽核日誌監控調查結果。

DefenseEvasion:Kubernetes/TorIPCaller

從 Tor 退出節點 IP 地址調用的常用來逃避防禦措施的 API。

預設嚴重性：高

- 功能：EKS 稽核記錄

此調查結果會通知您，已從 Tor 退出節點 IP 地址調用 API。觀察到的 API 通常與防禦逃稅策略有關，其中對手嘗試隱藏其行動以避免檢測。Tor 是一種啟用匿名通訊的軟體。它會透過一系列網路節點之間的中繼來加密並隨機反彈通訊。最後的 Tor 節點稱為退出節點。這可能表示您的 Kubernetes 叢集有未經授權的存取，目的是隱藏對手的真實身分。

修復建議：

如果本`KubernetesUserDetails`節下發現項目中報告的使用者是`system:anonymous`，請按照 Amazon EKS 使用者指南中 Amazon EKS 安全性最佳實務中的指示，調查為何允許匿名使用者叫用 API 並撤銷許可 (如有需要)。如果使用者是經過驗證的使用者，請調查以確定該活動是否為合法或惡意的活動。如果活動是惡意的，請撤銷使用者的存取權限，並還原對手對您的叢集所做的任何變更。如需詳細資訊，請參閱 修復 EKS 稽核日誌監控調查結果。

Discovery:Kubernetes/MaliciousIPCaller

從 IP 地址調用常用來探索在 Kubernetes 叢集中之資源的 API。

預設嚴重性：中

- 功能：EKS 稽核記錄

此調查結果會通知您，從與已知惡意活動關聯的 IP 地址調用了 API 操作。觀察到的 API 常與攻擊的探索階段搭配使用，其中攻擊者正在收集資訊以確定您的 Kubernetes 叢集是否容易受到更廣泛的攻擊。

修復建議：

如果本`KubernetesUserDetails`節下發現項目中報告的使用者是`system:anonymous`，請按照 Amazon EKS 使用者指南中 Amazon EKS 安全性最佳實務中的指示，調查為何允許匿名使用者叫用 API 並撤銷許可 (如有需要)。如果使用者是經過驗證的使用者，請調查以確定該活動是否為合法或惡意的活動。如果活動是惡意的，請撤銷使用者的存取權限，並還原對手對您的叢集所做的任何變更。如需詳細資訊，請參閱 修復 EKS 稽核日誌監控調查結果。

Discovery:Kubernetes/MaliciousIPCaller.Custom

從自訂威脅清單上的 IP 地址調用常用來探索在 Kubernetes 叢集中之資源的 API。

預設嚴重性：中

- 功能：EKS 稽核記錄

此調查結果會通知您，已從您上傳的威脅清單上所包含的 IP 地址調用 API。與此調查結果相關聯的威脅清單會列在調查結果詳細資訊的其他資訊區段中。觀察到的 API 常與攻擊的探索階段搭配使用，其中攻擊者正在收集資訊以確定您的 Kubernetes 叢集是否容易受到更廣泛的攻擊。

修復建議：

如果本`KubernetesUserDetails`節下發現項目中報告的使用者是`system:anonymous`，請按照 Amazon EKS 使用者指南中 Amazon EKS 安全性最佳實務中的指示，調查為何允許匿名使用者叫用 API 並撤銷許可 (如有需要)。如果使用者是經過驗證的使用者，請調查以確定該活動是否為合法或惡意的活動。如果活動是惡意的，請撤銷使用者的存取權限，並還原對手對您的叢集所做的任何變更。如需詳細資訊，請參閱 修復 EKS 稽核日誌監控調查結果。

Discovery:Kubernetes/SuccessfulAnonymousAccess

未經驗證的使用者調用 Kubernetes 叢集中常用來探索資源的 API。

預設嚴重性：中

- 功能：EKS 稽核記錄

此調查結果會通知您，`system:anonymous` 使用者已成功調用 API 操作。由 `system:anonymous` 進行的 API 呼叫未經驗證。當對手在您的 Kubernetes 叢集上收集資訊時，觀察到的 API 通常與攻擊的探索階段相關聯。此活動表示在調查結果中報告的 API 動作允許匿名或未經驗證的存取，並且可能在其他動作上允許匿名或未經驗證的存取。如果未預期出現這種行為，則可能表示組態錯誤或您的憑證遭到入侵。

修復建議：

您應該檢查已向叢集上 `system:anonymous` 使用者授與的許可，並確保所有許可都是必要的。如果錯誤或惡意地授與許可，您應該撤銷使用者的存取權限，並還原對手對叢集所做的任何變更。如需詳細資訊，請參閱 Amazon EKS 使用者指南中的 Amazon EKS 安全性最佳實務。

如需詳細資訊，請參閱 修復 EKS 稽核日誌監控調查結果。

Discovery:Kubernetes/TorIPCaller

從 Tor 退出節點 IP 地址調用常用來探索在 Kubernetes 叢集中之資源的 API。

預設嚴重性：中

- 功能：EKS 稽核記錄

此調查結果會通知您，已從 Tor 退出節點 IP 地址調用 API。觀察到的 API 常與攻擊的探索階段搭配使用，其中攻擊者正在收集資訊以確定您的 Kubernetes 叢集是否容易受到更廣泛的攻擊。Tor 是一種啟用匿名通訊的軟體。它會透過一系列網路節點之間的中繼來加密並隨機反彈通訊。最後的 Tor 節點稱為退出節點。這可能表示您的 Kubernetes 叢集有未經授權的存取，目的是隱藏對手的真實身分。

修復建議：

如果本*KubernetesUserDetails*節下發現項目中報告的使用者是*system:anonymous*，請依照 Amazon EKS 使用者指南中 Amazon EKS 安全性最佳實務中的指示，調查為何允許匿名使用者叫用 API 並視需要撤銷許可。如果使用者是經過驗證的使用者，請調查以確定該活動是否為合法或惡意的活動。如果活動是惡意的，請撤銷使用者的存取權限，並還原對手對您的叢集所做的任何變更。如需詳細資訊，請參閱 修復 EKS 稽核日誌監控調查結果。

Execution:Kubernetes/ExecInKubeSystemPod

命令已在 **kube-system** 命名空間中的 Pod 內執行

預設嚴重性：中

- 功能：EKS 稽核記錄

此調查結果會通知您使用 Kubernetes exec API 在 kube-system 命名空間內的 Pod 中執行的命令。kube-system 命名空間為預設的命名空間，主要用於系統層級元件，例如 kube-dns 和 kube-proxy。在 kube-system 命名空間下的 Pod 或容器內執行命令的情控非常罕見，並且可能表示可疑活動。

修復建議：

如果未預期執行此命令，用於執行命令的使用者身分憑證可能已遭入侵。請撤銷使用者的存取權限，並還原對手對您的叢集所做的任何變更。如需詳細資訊，請參閱 修復 EKS 稽核日誌監控調查結果。

Impact:Kubernetes/MaliciousIPCaller

從已知的惡意 IP 地址調用了 Kubernetes 叢集中常用來竄改資源的 API。

預設嚴重性：高

- 功能：EKS 稽核記錄

此調查結果會通知您，從與已知惡意活動關聯的 IP 地址調用了 API 操作。觀察到的 API 通常與對手試圖操縱，中斷或銷毀環境中的數據的影響策略相關聯 AWS 。

修復建議：

如果本`KubernetesUserDetails`節下發現項目中報告的使用者是`system:anonymous`，請按照 Amazon EKS 使用者指南中 Amazon EKS 安全性最佳實務中的指示，調查為何允許匿名使用者叫用 API 並撤銷許可 (如有需要)。如果使用者是經過驗證的使用者，請調查以確定該活動是否為合法或惡意的活動。如果活動是惡意的，請撤銷使用者的存取權限，並還原對手對您的叢集所做的任何變更。如需詳細資訊，請參閱 修復 EKS 稽核日誌監控調查結果。

Impact:Kubernetes/MaliciousIPCaller.Custom

從自訂威脅清單上的 IP 地址調用常用來竄改在 Kubernetes 叢集中之資源的 API。

預設嚴重性：高

- 功能：EKS 稽核記錄

此調查結果會通知您，從您上傳的威脅清單上所包含的 IP 地址調用了 API 操作。與此調查結果相關聯的威脅清單會列在調查結果詳細資訊的其他資訊區段中。觀察到的 API 通常與對手試圖操縱，中斷或銷毀環境中的數據的影響策略相關聯 AWS 。

修復建議：

如果本`KubernetesUserDetails`節下發現項目中報告的使用者是`system:anonymous`，請按照 Amazon EKS 使用者指南中 Amazon EKS 安全性最佳實務中的指示，調查為何允許匿名使用者叫用 API 並撤銷許可 (如有需要)。如果使用者是經過驗證的使用者，請調查以確定該活動是否為合法或惡意的活動。如果活動是惡意的，請撤銷使用者的存取權限，並還原對手對您的叢集所做的任何變更。如需詳細資訊，請參閱 修復 EKS 稽核日誌監控調查結果。

Impact:Kubernetes/SuccessfulAnonymousAccess

未經驗證的使用者調用 Kubernetes 叢集中常用來竄改資源的 API。

預設嚴重性：高

- 功能：EKS 稽核記錄

此調查結果會通知您，system:anonymous 使用者已成功調用 API 操作。由 system:anonymous 進行的 API 呼叫未經驗證。當對手竄改叢集中的資源時，觀察到的 API 通常與攻擊的影響階段相關聯。此活動表示在調查結果中報告的 API 動作允許匿名或未經驗證的存取，並且可能在其他動作上允許匿名或未經驗證的存取。如果未預期出現這種行為，則可能表示組態錯誤或您的憑證遭到入侵。

修復建議：

您應該檢查已向叢集上 system:anonymous 使用者授與的許可，並確保所有許可都是必要的。如果錯誤或惡意地授與許可，您應該撤銷使用者的存取權限，並還原對手對叢集所做的任何變更。如需詳細資訊，請參閱 Amazon EKS 使用者指南中的 Amazon EKS 安全性最佳實務。

如需詳細資訊，請參閱 修復 EKS 稽核日誌監控調查結果。

Impact:Kubernetes/TorIPCaller

從 Tor 退出節點 IP 地址調用常用來竄改在 Kubernetes 叢集中之資源的 API。

預設嚴重性：高

- 功能：EKS 稽核記錄

此調查結果會通知您，已從 Tor 退出節點 IP 地址調用 API。觀察到的 API 通常與影響策略相關聯，其中對手嘗試操縱、中斷或銷毀 AWS 環境中的資料。Tor 是一種啟用匿名通訊的軟體。它會透過一系列網路節點之間的中繼來加密並隨機反彈通訊。最後的 Tor 節點稱為退出節點。這可能表示您的 Kubernetes 叢集有未經授權的存取，目的是隱藏對手的真實身分。

修復建議：

如果本KubernetesUserDetails節下發現項目中報告的使用者是system:anonymous，請按照 Amazon EKS 使用者指南中 Amazon EKS 安全性最佳實務中的指示，調查為何允許匿名使用者叫用

API 並撤銷許可 (如有需要)。如果使用者是經過驗證的使用者，請調查以確定該活動是否為合法或惡意的活動。如果活動是惡意的，請撤銷使用者的存取權限，並還原對手對您的叢集所做的任何變更。如需詳細資訊，請參閱 修復 EKS 稽核日誌監控調查結果。

Persistence:Kubernetes/ContainerWithSensitiveMount

啟動了一個容器，其中掛載了敏感的外部主機路徑。

預設嚴重性：中

- 功能：EKS 稽核記錄

此調查結果會通知您已啟動容器，其組態包含在 `volumeMounts` 區段中具有寫入存取權限的敏感主機路徑。這使得敏感的主機路徑可從容器內部存取和寫入。這種技術通常被對手用來存取主機的檔案系統。

修復建議：

如果此容器啟動並非預期的結果，用於啟動容器的使用者身分憑證可能已遭入侵。請撤銷使用者的存取權限，並還原對手對您的叢集所做的任何變更。如需詳細資訊，請參閱 修復 EKS 稽核日誌監控調查結果。

如果此容器啟動為預期的結果，建議您根據 `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix` 欄位使用篩選條件準則組成的抑制規則。在篩選條件準則中，`imagePrefix` 欄位應與調查結果中指定的 `imagePrefix` 相同。若要進一步了解有關建立隱藏規則的資訊，請參閱隱藏規則。

Persistence:Kubernetes/MaliciousIPCaller

從已知的惡意 IP 地址調用常用來取得 Kubernetes 叢集持續存取權限的 API。

預設嚴重性：中

- 功能：EKS 稽核記錄

此調查結果會通知您，從與已知惡意活動關聯的 IP 地址調用了 API 操作。觀察到的 API 通常與持續性策略相關聯，其中對手已取得您的 Kubernetes 叢集的存取權限，並嘗試維護該存取權限。

修復建議：

如果本KubernetesUserDetails節下發現項目中報告的使用者是system:anonymous，請按照 Amazon EKS 使用者指南中 Amazon EKS 安全性最佳實務中的指示，調查為何允許匿名使用者叫用 API 並撤銷許可 (如有需要)。如果使用者是經過驗證的使用者，請調查以確定該活動是否為合法或惡意的活動。如果活動是惡意的，請撤銷使用者的存取權限，並還原對手對您的叢集所做的任何變更。如需詳細資訊，請參閱 修復 EKS 稽核日誌監控調查結果。

Persistence:Kubernetes/MaliciousIPCaller.Custom

從自訂威脅清單上的 IP 地址調用常用來取得 Kubernetes 叢集持續存取權限的 API。

預設嚴重性：中

- 功能：EKS 稽核記錄

此調查結果會通知您，從您上傳的威脅清單上所包含的 IP 地址調用了 API 操作。與此調查結果相關聯的威脅清單會列在調查結果詳細資訊的其他資訊區段中。觀察到的 API 通常與持續性策略相關聯，其中對手已取得您的 Kubernetes 叢集的存取權限，並嘗試維護該存取權限。

修復建議：

如果本KubernetesUserDetails節下發現項目中報告的使用者是system:anonymous，請按照 Amazon EKS 使用者指南中 Amazon EKS 安全性最佳實務中的指示，調查為何允許匿名使用者叫用 API 並撤銷許可 (如有需要)。如果使用者是經過驗證的使用者，請調查以確定該活動是否為合法或惡意的活動。如果活動是惡意的，請撤銷使用者的存取權限，並還原對手對您的叢集所做的任何變更。如需詳細資訊，請參閱 修復 EKS 稽核日誌監控調查結果。

Persistence:Kubernetes/SuccessfulAnonymousAccess

未經驗證的使用者調用常用來取得 Kubernetes 叢集之高層級許可的 API。

預設嚴重性：高

- 功能：EKS 稽核記錄

此調查結果會通知您，system:anonymous 使用者已成功調用 API 操作。由 system:anonymous 進行的 API 呼叫未經驗證。觀察到的 API 通常與持續性策略相關聯，其中對手已取得您的叢集之存

取權限，並嘗試維護該存取權限。此活動表示在調查結果中報告的 API 動作允許匿名或未經驗證的存取，並且可能在其他動作上允許匿名或未經驗證的存取。如果未預期出現這種行為，則可能表示組態錯誤或您的憑證遭到入侵。

修復建議：

您應該檢查已向叢集上 `system:anonymous` 使用者授與的許可，並確保所有許可都是必要的。如果錯誤或惡意地授與許可，您應該撤銷使用者的存取權限，並還原對手對叢集所做的任何變更。如需詳細資訊，請參閱 Amazon EKS 使用者指南中的 Amazon EKS 安全性最佳實務。

如需詳細資訊，請參閱 修復 EKS 稽核日誌監控調查結果。

Persistence:Kubernetes/TorIPCaller

從 Tor 退出節點 IP 地址調用常用來取得 Kubernetes 叢集持續存取權限的 API。

預設嚴重性：中

- 功能：EKS 稽核記錄

此調查結果會通知您，已從 Tor 退出節點 IP 地址調用 API。觀察到的 API 通常與持續性策略相關聯，其中對手已取得您的 Kubernetes 叢集的存取權限，並嘗試維護該存取權限。Tor 是一種啟用匿名通訊的軟體。它會透過一系列網路節點之間的中繼來加密並隨機反彈通訊。最後的 Tor 節點稱為退出節點。這可能表示未經授權存取您的 AWS 資源，意圖隱藏攻擊者的真實身分。

修復建議：

如果本`KubernetesUserDetails`節下發現項目中報告的使用者是`system:anonymous`，請按照 Amazon EKS 使用者指南中 Amazon EKS 安全性最佳實務中的指示，調查為何允許匿名使用者叫用 API 並撤銷許可 (如有需要)。如果使用者是經過驗證的使用者，請調查以確定該活動是否為合法或惡意的活動。如果活動是惡意的，請撤銷使用者的存取權限，並還原對手對您的叢集所做的任何變更。如需詳細資訊，請參閱 修復 EKS 稽核日誌監控調查結果。

Policy:Kubernetes/AdminAccessToDefaultServiceAccount

預設服務帳戶已被授與 Kubernetes 叢集上的管理員權限。

預設嚴重性：高

- 功能：EKS 稽核記錄

此調查結果會通知您，Kubernetes 叢集中命名空間的預設服務帳戶已被授與管理員權限。Kubernetes 會為叢集中的所有命名空間建立預設服務帳戶。它會自動將預設服務帳戶以身分的形式指派給尚未明確關聯至另一個服務帳戶的 Pod。如果預設服務帳戶具有管理員權限，可能會導致意外地以管理員權限啟動 Pod。如果未預期出現這種行為，則可能表示組態錯誤或您的憑證遭到入侵。

修復建議：

您不應使用預設服務帳戶對 Pod 授與許可。相反地，您應該為每個工作負載建立專用服務帳戶，並根據需要對該帳戶授與許可。若要修正此問題，您應該為所有 Pod 和工作負載建立專用服務帳戶，並更新 Pod 和工作負載，以便從預設服務帳戶遷移至其專用帳戶。然後，您應該從預設服務帳戶中移除管理員權限。如需詳細資訊，請參閱 修復 EKS 稽核日誌監控調查結果。

Policy:Kubernetes/AnonymousAccessGranted

`system:anonymous` 使用者已被授與 Kubernetes 叢集上的 API 許可。

預設嚴重性：高

- 功能：EKS 稽核記錄

此調查結果會通知您，Kubernetes 叢集上的使用者已成功建立 `ClusterRoleBinding` 或 `RoleBinding`，以將使用者 `system:anonymous` 繫結至角色。這會啟用角色所允許之 API 操作的未經驗證存取權限。如果未預期出現這種行為，則可能表示組態錯誤或您的憑證遭到入侵

修復建議：

您應該檢查已授與叢集上 `system:anonymous` 使用者或 `system:unauthenticated` 群組的許可，並撤銷不必要的匿名存取權限。如需詳細資訊，請參閱 Amazon EKS 使用者指南中的 Amazon EKS 安全性最佳實務。如果惡意地授與許可，您應該撤銷已授與許可之使用者的存取權限，並還原對手對叢集所做的任何變更。如需詳細資訊，請參閱 修復 EKS 稽核日誌監控調查結果。

Policy:Kubernetes/ExposedDashboard

Kubernetes 叢集的儀表板已公開至網際網路

預設嚴重性：中

- 功能：EKS 稽核記錄

此調查結果會通知您，叢集的 Kubernetes 儀表板已由負載平衡器服務公開至網際網路。公開的儀表板使叢集的管理界面可從網際網路存取，並允許對手利用任何可能存在的驗證和存取控制差距。

修復建議：

您應該確保在 Kubernetes 儀表板上強制執行強式驗證和授權。您也應該實作網路存取控制，以限制從特定 IP 地址存取儀表板。

如需詳細資訊，請參閱 修復 EKS 稽核日誌監控調查結果。

Policy:Kubernetes/KubeflowDashboardExposed

Kubernetes 叢集的 Kubeflow 儀表板已向網際網路公開

預設嚴重性：中

- 功能：EKS 稽核記錄

此調查結果會通知您，叢集的 Kubeflow 儀表板已由負載平衡器服務公開至網際網路。公開的 Kubeflow 儀表板使 Kubeflow 環境的管理界面可從網際網路存取，並允許對手利用任何可能存在的驗證和存取控制差距。

修復建議：

您應該確保在 Kubeflow 儀表板上強制執行強式驗證和授權。您也應該實作網路存取控制，以限制從特定 IP 地址存取儀表板。

如需詳細資訊，請參閱 修復 EKS 稽核日誌監控調查結果。

PrivilegeEscalation:Kubernetes/PrivilegedContainer

在您的 Kubernetes 叢集上啟動具有根層級存取權限的具有權限容器。

預設嚴重性：中

- 功能：EKS 稽核記錄

此調查結果會通知您，在 Kubernetes 叢集上使用映像啟動具有權限容器，以前從未被用來啟動叢集中具有權限的容器。具有權限容器有主機的根層級存取權限。對手可以啟動具有特權容器作為特權提升策略，以取得主機的存取權限，然後入侵主機。

修復建議：

如果此容器啟動並非預期的結果，用於啟動容器的使用者身分憑證可能已遭入侵。請撤銷使用者的存取權限，並還原對手對您的叢集所做的任何變更。如需詳細資訊，請參閱 修復 EKS 稽核日誌監控調查結果。

CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed

常用來存取秘密的 Kubernetes API 調用方式異常。

預設嚴重性：中

- 功能：EKS 稽核記錄

此調查結果會通知您，叢集中的 Kubernetes 使用者調用擷取敏感叢集秘密的異常 API 操作。觀察到的 API 通常與可能導致具有特權提升並在您的叢集中進一步存取的憑證存取策略相關聯。如果沒有預期出現這種行為，可能表示配置錯誤或您的 AWS 憑證遭到入侵。

異常偵測機器學習 (ML) 模型將觀察到的 API 識別為 GuardDuty 異常。ML 模型會評估 EKS 叢集中的所有使用者 API 活動，並識別與未經授權使用者使用的技術相關聯的異常事件。ML 模型追蹤 API 操作的多個因素，例如提出請求的使用者、提出請求的位置、使用的使用者代理程式，和使用者操作的命名空間。您可以在控制台的查找詳細信息面板中找到異常 API 請求的詳細信 GuardDuty 息。

修復建議：

檢查授與叢集中 Kubernetes 使用者的許可並確保需要這所有許可。如果錯誤或惡意地授與許可，則撤銷使用者的存取權限，並還原未經授權使用者對叢集所做的任何變更。如需詳細資訊，請參閱 修復 EKS 稽核日誌監控調查結果。

如果您的 AWS 憑證遭到入侵，請參閱修復可能遭到破壞 AWS 的認證。

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated

已在 Kubernetes 叢集中建立 RoleBinding 或 ClusterRoleBinding 修改或過於寬鬆的角色或敏感命名空間。

預設嚴重性：中*

> **Note**
>
> 此調查結果的預設嚴重性為「中」。但是，如果 RoleBinding或 ClusterRoleBinding 涉及 ClusterRoles `admin`或`cluster-admin`，則嚴重性為「高」。

- 功能：EKS 稽核記錄

此調查結果會通知您，Kubernetes 叢集中的使用者已建立 `RoleBinding` 或 `ClusterRoleBinding`，將使用者繫結至具有管理員許可或敏感命名空間的角色。如果沒有預期出現這種行為，可能表示配置錯誤或您的 AWS 憑證遭到入侵。

異常偵測機器學習 (ML) 模型將觀察到的 API 識別為 GuardDuty 異常。ML 模型會評估 EKS 叢集中的所有使用者 API 活動。此 ML 模型也會識別與未經授權使用者所使用之技術相關聯的異常事件。ML 模型也會追蹤 API 操作的多個因素，例如提出請求的使用者、提出請求的位置、使用的使用者代理程式，和使用者操作的命名空間。您可以在控制台的查找詳細信息面板中找到異常 API 請求的詳細信 GuardDuty 息。

修復建議：

檢查授與 Kubernetes 使用者的許可。這些許可以 `RoleBinding` 和 `ClusterRoleBinding` 中涉及的角色和主體予以定義。如果錯誤或惡意地授與許可，則撤銷使用者的存取權限，並還原未經授權使用者對叢集所做的任何變更。如需詳細資訊，請參閱 修復 EKS 稽核日誌監控調查結果。

如果您的 AWS 憑證遭到入侵，請參閱修復可能遭到破壞 AWS 的認證。

Execution:Kubernetes/AnomalousBehavior.ExecInPod

Pod 內命令的執行方式異常。

預設嚴重性：中

- 功能：EKS 稽核記錄

此調查結果會通知您使用 Kubernetes exec API 在 Pod 中執行命令。Kubernetes exec API 允許在 Pod 中執行任意命令。如果使用者、命名空間或網繭未預期出現此行為，則可能表示組態錯誤或您的 AWS 認證遭到入侵。

異常偵測機器學習 (ML) 模型將觀察到的 API 識別為 GuardDuty 異常。ML 模型會評估 EKS 叢集中的所有使用者 API 活動。此 ML 模型也會識別與未經授權使用者所使用之技術相關聯的異常事件。ML 模型也會追蹤 API 操作的多個因素，例如提出請求的使用者、提出請求的位置、使用的使用者代理程式，和使用者操作的命名空間。您可以在控制台的查找詳細信息面板中找到異常 API 請求的詳細信 GuardDuty 息。

修復建議：

如果未預期執行此命令，用於執行命令的使用者身分憑證可能已遭到入侵。撤銷使用者存取權限，並還原未經授權使用者對叢集所做的任何變更。如需詳細資訊，請參閱 修復 EKS 稽核日誌監控調查結果。

如果您的 AWS 憑證遭到入侵，請參閱修復可能遭到破壞 AWS 的認證。

PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer

使用具有特權容器，啟動工作負載的方式異常。

預設嚴重性：高

- 功能：EKS 稽核記錄

此調查結果會通知您，在您的 Amazon EKS 叢集中使用具有特權容器啟動工作負載。具有權限容器有主機的根層級存取權限。未經授權使用者可以啟動具有特權容器作為特權提升策略，先取得主機的存取權限，然後入侵主機。

異常偵測機器學習 (ML) 模型將觀察到的容器建立或修改識別為 GuardDuty 異常狀況。ML 模型會評估 EKS 叢集中的所有使用者 API 和容器映像活動。此 ML 模型也會識別與未經授權使用者所使用之技術相關聯的異常事件。ML 模型也會追蹤 API 操作的多個因素，例如提出請求的使用者、提出請求的位置、使用的使用者代理程式、在您的帳戶中觀察到的容器映像，和使用者操作的命名空間。您可以在控制台的查找詳細信息面板中找到異常 API 請求的詳細信 GuardDuty 息。

修復建議：

如果此容器啟動並非預期的結果，用於啟動容器的使用者身分憑證可能已遭到入侵。撤銷使用者存取權限，並還原未經授權使用者對叢集所做的任何變更。如需詳細資訊，請參閱 修復 EKS 稽核日誌監控調查結果。

如果您的 AWS 憑證遭到入侵，請參閱修復可能遭到破壞 AWS 的認證。

如果此容器啟動為預期的結果，建議您根據 `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix` 欄位使用具有篩選條件準則的抑制規則。在篩選條件準則中，`imagePrefix` 欄位必須具有與調查結果中指定的 `imagePrefix` 欄位相同的值。如需詳細資訊，請參閱 隱藏規則。

Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount

部署工作負載的方式異常，並在工作負載內部裝載了敏感的主機路徑。

預設嚴重性：高

- 功能：EKS 稽核記錄

此調查結果會通知您，已透過 `volumeMounts` 區段中包含敏感主機路徑的容器啟動工作負載。這可能使得敏感的主機路徑可從容器內部存取和寫入。這種技術通常被未經授權使用者用來存取主機的檔案系統。

異常偵測機器學習 (ML) 模型將觀察到的容器建立或修改識別為 GuardDuty 異常狀況。ML 模型會評估 EKS 叢集中的所有使用者 API 和容器映像活動。此 ML 模型也會識別與未經授權使用者所使用之技術相關聯的異常事件。ML 模型也會追蹤 API 操作的多個因素，例如提出請求的使用者、提出請求的位置、使用的使用者代理程式、在您的帳戶中觀察到的容器映像，和使用者操作的命名空間。您可以在控制台的查找詳細信息面板中找到異常 API 請求的詳細信 GuardDuty 息。

修復建議：

如果此容器啟動並非預期的結果，用於啟動容器的使用者身分憑證可能已遭到入侵。撤銷使用者存取權限，並還原未經授權使用者對叢集所做的任何變更。如需詳細資訊，請參閱 修復 EKS 稽核日誌監控調查結果。

如果您的 AWS 憑證遭到入侵，請參閱修復可能遭到破壞 AWS 的認證。

如果此容器啟動為預期的結果，建議您根據 `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix` 欄位使用具有篩選條件準則的抑制規則。在篩選條件準則中，`imagePrefix` 欄位必須具有與調查結果中指定的 `imagePrefix` 欄位相同的值。如需詳細資訊，請參閱 隱藏規則。

Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed

啟動工作負載的方式異常。

預設嚴重性：低*

> **Note**
>
> 預設嚴重性為低。不過，如果工作負載包含潛在可疑的映像名稱 (例如已知的滲透測試工具)，或是在啟動時執行潛在可疑命令的容器 (例如反向 Shell 命令)，則此調查結果類型的嚴重性將被視為「中」。

- 功能：EKS 稽核記錄

此調查結果會通知您建立或修改 Kubernetes 工作負載的方式異常，例如 Amazon EKS 叢集中的 API 活動、新容器映像或有風險的工作負載組態。未經授權使用者可以啟動容器作為執行任意程式碼的策略，先取得主機的存取權限，然後入侵主機。

異常偵測機器學習 (ML) 模型將觀察到的容器建立或修改識別為 GuardDuty 異常狀況。ML 模型會評估 EKS 叢集中的所有使用者 API 和容器映像活動。此 ML 模型也會識別與未經授權使用者所使用之技術相關聯的異常事件。ML 模型也會追蹤 API 操作的多個因素，例如提出請求的使用者、提出請求的位置、使用的使用者代理程式、在您的帳戶中觀察到的容器映像，和使用者操作的命名空間。您可以在控制台的查找詳細信息面板中找到異常 API 請求的詳細信 GuardDuty 息。

修復建議：

如果此容器啟動並非預期的結果，用於啟動容器的使用者身分憑證可能已遭到入侵。撤銷使用者存取權限，並還原未經授權使用者對叢集所做的任何變更。如需詳細資訊，請參閱 修復 EKS 稽核日誌監控調查結果。

如果您的 AWS 憑證遭到入侵，請參閱修復可能遭到破壞 AWS 的認證。

如果此容器啟動為預期的結果，建議您根據 `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix` 欄位使用具有篩選條件準則的抑制規則。在篩選條件準則中，`imagePrefix` 欄位必須具有與調查結果中指定的 `imagePrefix` 欄位相同的值。如需詳細資訊，請參閱 隱藏規則。

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated

高度寬鬆的角色，或 ClusterRole 以異常方式創建或修改。

預設嚴重性：低

- 功能：EKS 稽核記錄

此調查結果會通知您，Amazon EKS 叢集中的 Kubernetes 使用者呼叫建立具有過多許可之 `Role` 或 `ClusterRole` 的異常 API 操作。行動者可以使用具有強大許可的角色建立，以避免使用內建管理員式角色並避免偵測。過多的許可，可能會導致具有特權提升、遠端程式碼執行，以及可能控制命名空間或叢集。如果未預期出現這種行為，則可能表示組態錯誤或您的憑證遭到入侵。

異常偵測機器學習 (ML) 模型將觀察到的 API 識別為 GuardDuty 異常。ML 模型會評估 Amazon EKS 叢集中的所有使用者 API 活動，並識別與未經授權使用者使用的技術相關聯的異常事件。ML 模型也會追蹤 API 操作的多個因素，例如提出請求的使用者、提出請求的位置、使用的使用者代理程式、在您的帳戶中觀察到的容器映像，和使用者操作的命名空間。您可以在控制台的查找詳細信息面板中找到異常 API 請求的詳細信 GuardDuty 息。

修復建議：

檢查 `Role` 或 `ClusterRole` 中定義的權限，以確保需要所有權限，並遵循最低權限政策。如果錯誤或惡意地授與許可，則撤銷使用者的存取權限，並還原未經授權使用者對叢集所做的任何變更。如需詳細資訊，請參閱 修復 EKS 稽核日誌監控調查結果。

如果您的 AWS 憑證遭到入侵，請參閱修復可能遭到破壞 AWS 的認證。

Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

使用者檢查其存取許可的方式異常。

預設嚴重性：低

- 功能：EKS 稽核記錄

此調查結果會通知您，Kubernetes 叢集中的使用者已成功檢查是否允許可導致具有權限提升和遠端程式碼執行的已知強大許可。例如，用來檢查使用者許可的常用命令為 `kubectl auth can-i`。如果未預期出現這種行為，則可能表示組態錯誤或您的憑證遭到入侵。

異常偵測機器學習 (ML) 模型將觀察到的 API 識別為 GuardDuty 異常。ML 模型會評估 Amazon EKS 叢集中的所有使用者 API 活動，並識別與未經授權使用者使用的技術相關聯的異常事件。ML 模型也會追蹤 API 操作的多個因素，例如提出請求的使用者、提出請求的位置、檢查的許可，和使用者操作的命名空間。您可以在控制台的查找詳細信息面板中找到異常 API 請求的詳細信 GuardDuty 息。

修復建議：

檢查授與 Kubernetes 使用者的許可，以確保需要所有許可。如果錯誤或惡意地授與許可，則撤銷使用者的存取權限，並還原未經授權使用者對叢集所做的任何變更。如需詳細資訊，請參閱 修復 EKS 稽核日誌監控調查結果。

如果您的 AWS 憑證遭到入侵，請參閱修復可能遭到破壞 AWS 的認證。

Lambda 保護調查結果類型

本節說明 AWS Lambda 資源特有且將 `resourceType` 列為 `Lambda` 的調查結果類型。對於所有 Lambda 調查結果，我們建議您檢查有問題的資源，並判斷該資源是否以預期的方式運作。如果活動獲得授權，您可以使用隱藏規則或受信任的 IP 和威脅清單，來防止該資源的誤判通知。

如果活動是非預期的結果，安全性最佳實務是假設 Lambda 可能遭到破壞，並遵循修復建議。

主題

- Backdoor:Lambda/C&CActivity.B
- CryptoCurrency:Lambda/BitcoinTool.B
- Trojan:Lambda/BlackholeTraffic
- Trojan:Lambda/DropPoint
- UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom
- UnauthorizedAccess:Lambda/TorClient
- UnauthorizedAccess:Lambda/TorRelay

Backdoor:Lambda/C&CActivity.B

Lambda 函數正在查詢與已知命令和控管伺服器相關聯的 IP 地址。

預設嚴重性：高

- 功能：Lambda 網路活動監控

此調查結果會通知您，在 AWS 環境中的 Lambda 函數正在查詢與已知命令和控管 (C&C) 伺服器相關聯的 IP 地址。與產生的調查結果相關聯的 Lambda 函數可能遭到破壞。C&C 伺服器是對殭屍網路的成員發出命令的電腦。

殭屍網路是一種透過感染和常見惡意軟體控制的網際網路連線裝置集合，可能包括 PC、伺服器、行動裝置及物聯網裝置。殭屍網路經常用來散佈惡意軟體和收集不當資訊，像是信用卡號碼。根據殭屍網路的用途和結構而定，C&C 伺服器也可能發出命令，來展開分散式阻斷服務。

修復建議：

如果此活動為非預期活動，即代表 Lambda 函數可能已遭入侵。如需詳細資訊，請參閱修復可能受損的 Lambda 函數。

CryptoCurrency:Lambda/BitcoinTool.B

Lambda 函數正在查詢與加密貨幣相關活動有關聯的 IP 地址。

預設嚴重性：高

- 功能：Lambda 網路活動監控

此調查結果會通知您，在 AWS 環境中所列的 Lambda 函數正在查詢與比特幣或其他加密貨幣相關活動有關聯的 IP 地址。威脅參與者可能會尋求 Lambda 函數的控制權，目的是惡意地重新利用這些函數進行未經授權的加密貨幣挖掘。

修復建議：

如果您使用此 Lambda 函數來挖掘或管理加密貨幣，或者此函數以其他方式參與區塊鏈活動，則此函數可能是您環境的預期活動。如果您的 AWS 環境是這種情況，建議您為此調查結果設定隱藏規則。隱藏規則應包含兩個篩選準則。第一個條件應該使用調查結果類型屬性，其值為 CryptoCurrency:Lambda/BitcoinTool.B。第二個篩選條件應是參與區塊鏈活動之函數的 Lambda 函數名稱。如需有關建立隱藏規則的詳細資訊，請參閱隱藏規則。

如果此活動是非預期的結果，則 Lambda 函數可能會遭到破壞。如需詳細資訊，請參閱修復可能受損的 Lambda 函數。

Trojan:Lambda/BlackholeTraffic

Lambda 函數正在嘗試與已知黑洞的遠端主機 IP 地址進行通訊。

預設嚴重性：中

- 功能：Lambda 網路活動監控

此調查結果會通知您，AWS 環境中的 Lambda 函數正在嘗試與黑洞 (或漏洞) 的 IP 地址進行通訊。黑洞是在網路上某些傳入或傳出流量會被無聲無息丟棄的地方，且資料來源也不會收到資料未傳送至收件人的通知。黑洞的 IP 地址會指定為未執行的主機，或未分配主機的地址。列出的 Lambda 函數可能遭到破壞。

修復建議：

如果此活動為非預期活動，即代表 Lambda 函數可能已遭入侵。如需詳細資訊，請參閱修復可能受損的 Lambda 函數。

Trojan:Lambda/DropPoint

Lambda 函數正在嘗試與遠端主機的 IP 地址進行通信，該主機已知會保存由惡意軟體擷取的憑證和其他遭竊資料。

預設嚴重性：中

- 功能：Lambda 網路活動監控

此調查結果會通知您，AWS 環境中所列的 Lambda 函數正在嘗試與已知存放憑證和惡意軟體擷取之其他遭竊資料的遠端主機 IP 地址進行通訊。

修復建議：

如果此活動為非預期活動，即代表 Lambda 函數可能已遭入侵。如需詳細資訊，請參閱修復可能受損的 Lambda 函數。

UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom

Lambda 函數正在連線至自訂威脅清單上的 IP 地址。

預設嚴重性：中

- 功能：Lambda 網路活動監控

此調查結果通知您，AWS 環境中的 Lambda 函數正在與您上傳的威脅清單上所包含的 IP 地址進行通訊。在 GuardDuty 中，威脅清單包含已知的惡意 IP 地址。GuardDuty 會根據上傳的威脅清單產生調查結果。您可以在 GuardDuty 主控台的調查結果詳細資訊中檢視威脅清單的詳細資訊。

修復建議：

如果此活動為非預期活動，即代表 Lambda 函數可能已遭入侵。如需詳細資訊，請參閱修復可能受損的 Lambda 函數。

UnauthorizedAccess:Lambda/TorClient

Lambda 函數正在連線至 Tor Guard 或 Authority 節點。

預設嚴重性：高

- 功能：Lambda 網路活動監控

此調查結果通知您，AWS 環境中的 Lambda 函數正在連線至 Tor Guard 或 Authority 節點。Tor 是一種啟用匿名通訊的軟體。Tor Guards 和 Authority 節點為進入 Tor 網路的初始閘道。此流量可能表示此 Lambda 函數已可能遭到破壞。其現在作為 Tor 網路上的用戶端。

修復建議：

如果此活動為非預期活動，即代表 Lambda 函數可能已遭入侵。如需詳細資訊，請參閱修復可能受損的 Lambda 函數。

UnauthorizedAccess:Lambda/TorRelay

Lambda 函數正在連線至 Tor 網路，且連線方式為顯示為代表 Tor 轉送。

預設嚴重性：高

- 功能：Lambda 網路活動監控

此調查結果通知您，AWS 環境中的 Lambda 函數正在連線至 Tor 網路，其連線方式表明它正在作為 Tor 轉送。Tor 是一種啟用匿名通訊的軟體。Tor 允許匿名通訊，做法是從某個 Tor 轉送將用戶端潛在非法流量轉寄至另一個 Tor 轉送。

修復建議：

如果此活動為非預期活動，即代表 Lambda 函數可能已遭入侵。如需詳細資訊，請參閱修復可能受損的 Lambda 函數。

惡意軟體防護調查結果類型

GuardDuty 惡意軟體防護針對 EC2 執行個體或容器工作負載掃描期間偵測到的所有威脅，提供單一惡意軟體防護發現。此調查結果包括掃描期間所執行的偵測總數，並根據嚴重性，提供其偵測到的前 32 個安全威脅的詳細資訊。與其他 GuardDuty 發現結果不同，再次掃描相同 EC2 執行個體或容器工作負載時，不會更新惡意軟體防護發現項目。

每次偵測到惡意軟體的掃描都會產生新的惡意軟體防護調查結果。惡意程式碼防護發現項目包括產生發現項目之對應掃描的相關資訊，以及起始此掃描的發 GuardDuty現項目。這樣可以更輕鬆地將可疑行為與偵測到的惡意程式建立關聯。

> **Note**
>
> GuardDuty 偵測到容器工作負載上的惡意活動時，惡意程式碼防護不會產生 EC2 層級的發現。

下列發現項目特定於 GuardDuty 惡意程式碼防護。

主題

- Execution:EC2/MaliciousFile
- Execution:ECS/MaliciousFile
- Execution:Kubernetes/MaliciousFile
- Execution:Container/MaliciousFile
- Execution:EC2/SuspiciousFile
- Execution:ECS/SuspiciousFile
- Execution:Kubernetes/SuspiciousFile
- Execution:Container/SuspiciousFile

Execution:EC2/MaliciousFile

在 EC2 執行個體上偵測到惡意檔案。

預設嚴重性：視偵測到的安全威脅而有所不同。

- 功能：EBS 惡意軟件防護

此發現指出惡意 GuardDuty 軟體防護掃描已偵測到您 AWS 環境中所列 EC2 執行個體上的一或多個惡意檔案。EC2 執行個體可能已遭入侵。如需詳細資訊，請參閱調查結果詳細資訊中的偵測到的威脅區段。

修復建議：

如果此活動為非預期活動，即代表您的執行個體可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到入侵的 Amazon EC2 執行個體。

Execution:ECS/MaliciousFile

在 ECS 叢集上偵測到惡意檔案。

預設嚴重性：視偵測到的安全威脅而有所不同。

- 功能：EBS 惡意軟件防護

此發現項目表示惡意程式 GuardDuty 碼防護掃描已偵測到屬於 ECS 叢集之容器工作負載上的一或多個惡意檔案。如需詳細資訊，請參閱調查結果詳細資訊中的偵測到的威脅區段。

修復建議：

如果此活動為非預期活動，即代表屬於 ECS 叢集的容器可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到入侵的 ECS 叢集。

Execution:Kubernetes/MaliciousFile

在 Kubernetes 叢集上偵測到惡意檔案。

預設嚴重性：視偵測到的安全威脅而有所不同。

- 功能：EBS 惡意軟件防護

此發現項目表示惡意程式 GuardDuty 碼防護掃描已在屬於 Kubernetes 叢集的容器工作負載上偵測到一或多個惡意檔案。如果這是 EKS 受管叢集，則調查結果詳細資訊將提供有關受影響 EKS 資源的其他資訊。如需詳細資訊，請參閱調查結果詳細資訊中的偵測到的威脅區段。

修復建議：

如果此活動為非預期活動，即代表您的容器工作負載可能已遭入侵。如需詳細資訊，請參閱 修復 EKS 稽核日誌監控調查結果。

Execution:Container/MaliciousFile

在獨立容器上偵測到惡意檔案。

預設嚴重性：視偵測到的安全威脅而有所不同。

- 功能：EBS 惡意軟件防護

此發現項目表示惡意程式 GuardDuty 碼防護掃描已偵測到容器工作負載上的一或多個惡意檔案，且未識別任何叢集資訊。如需詳細資訊，請參閱調查結果詳細資訊中的偵測到的威脅區段。

修復建議：

如果此活動為非預期活動，即代表您的容器工作負載可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到入侵的獨立容器。

Execution:EC2/SuspiciousFile

在 EC2 執行個體上偵測到可疑檔案。

預設嚴重性：視偵測到的安全威脅而有所不同。

- 功能：EBS 惡意軟件防護

此發現表明 GuardDuty 惡意軟體防護掃描已偵測到 EC2 執行個體上的一或多個可疑檔案。如需詳細資訊，請參閱調查結果詳細資訊中的偵測到的威脅區段。

SuspiciousFile 類型偵測表示受影響的資源上存在可能有害的程式，例如廣告軟體、間諜軟體或雙重使用工具。這些程式可能會對您的資源產生負面影響，或被攻擊者以惡意目的使用。例如，對手可以合法或惡意地使用網路工具作為駭客工具來嘗試入侵資源。

偵測到可疑檔案時，請評估您是否希望在 AWS 環境中看到偵測到的檔案。如果檔案不在預期中，請遵循下一節提供的修補建議。

修復建議：

如果此活動為非預期活動，即代表您的執行個體可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到入侵的 Amazon EC2 執行個體。

Execution:ECS/SuspiciousFile

在 ECS 叢集上偵測到可疑檔案。

預設嚴重性：視偵測到的安全威脅而有所不同。

- 功能：EBS 惡意軟件防護

此發現項目表示 GuardDuty 惡意程式碼防護掃描已偵測到屬於 ECS 叢集之容器上的一或多個可疑檔案。如需詳細資訊，請參閱調查結果詳細資訊中的偵測到的威脅區段。

SuspiciousFile 類型偵測表示受影響的資源上存在可能有害的程式，例如廣告軟體、間諜軟體或雙重使用工具。這些程式可能會對您的資源產生負面影響，或被攻擊者以惡意目的使用。例如，對手可以合法或惡意地使用網路工具作為駭客工具來嘗試入侵資源。

偵測到可疑檔案時，請評估您是否希望在 AWS 環境中看到偵測到的檔案。如果檔案不在預期中，請遵循下一節提供的修補建議。

修復建議：

如果此活動為非預期活動，即代表屬於 ECS 叢集的容器可能已遭入侵。如需詳細資訊，請參閱 修復可能遭到入侵的 ECS 叢集。

Execution:Kubernetes/SuspiciousFile

在 Kubernetes 叢集上偵測到可疑檔案。

預設嚴重性：視偵測到的安全威脅而有所不同。

- 功能：EBS 惡意軟件防護

此發現項目表示 GuardDuty 惡意程式碼防護掃描已在屬於 Kubernetes 叢集的容器上偵測到一或多個可疑檔案。如果這是 EKS 受管叢集，則調查結果詳細資訊將提供有關受影響 EKS 的其他資訊。如需詳細資訊，請參閱調查結果詳細資訊中的偵測到的威脅區段。

SuspiciousFile 類型偵測表示受影響的資源上存在可能有害的程式，例如廣告軟體、間諜軟體或雙重使用工具。這些程式可能會對您的資源產生負面影響，或被攻擊者以惡意目的使用。例如，對手可以合法或惡意地使用網路工具作為駭客工具來嘗試入侵資源。

偵測到可疑檔案時，請評估您是否希望在 AWS 環境中看到偵測到的檔案。如果檔案不在預期中，請遵循下一節提供的修補建議。

修復建議：

如果此活動為非預期活動，即代表您的容器工作負載可能已遭入侵。如需詳細資訊，請參閱 修復 EKS 稽核日誌監控調查結果。

Execution:Container/SuspiciousFile

在獨立容器上偵測到可疑檔案。

預設嚴重性：視偵測到的安全威脅而有所不同。

- 功能：EBS 惡意軟件防護

此發現項目表示 GuardDuty 惡意程式碼防護掃描在沒有叢集資訊的容器上偵測到一或多個可疑檔案。如需詳細資訊，請參閱調查結果詳細資訊中的偵測到的威脅區段。

SuspiciousFile 類型偵測表示受影響的資源上存在可能有害的程式，例如廣告軟體、間諜軟體或雙重使用工具。這些程式可能會對您的資源產生負面影響，或被攻擊者以惡意目的使用。例如，對手可以合法或惡意地使用網路工具作為駭客工具來嘗試入侵資源。

偵測到可疑檔案時，請評估您是否希望在 AWS 環境中看到偵測到的檔案。如果檔案不在預期中，請遵循下一節提供的修補建議。

修復建議：

如果此活動為非預期活動，即代表您的容器工作負載可能已遭入侵。如需更多詳細資訊，請參閱 修復可能遭到入侵的獨立容器。

GuardDuty RDS 保護調查結果類型

GuardDuty RDS 保護可偵測資料庫執行個體上的異常登入行為。以下調查結果專用於 支援的 Amazon Aurora 資料庫，而且資源類型為 RDSDBInstance。調查結果的嚴重性和詳細資訊依調查結果類型而有所不同。

主題

- CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin
- CredentialAccess:RDS/AnomalousBehavior.FailedLogin
- CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce
- CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin
- CredentialAccess:RDS/MaliciousIPCaller.FailedLogin
- Discovery:RDS/MaliciousIPCaller
- CredentialAccess:RDS/TorIPCaller.SuccessfulLogin
- CredentialAccess:RDS/TorIPCaller.FailedLogin
- Discovery:RDS/TorIPCaller

CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin

使用者以異常方式在您的帳戶中成功登入 RDS 資料庫。

預設嚴重性：變數

> **Note**
>
> 根據與此調查結果相關聯的異常行為，預設嚴重性可以是「低」、「中」和「高」。
>
> - 低：如果與此調查結果相關聯的使用者名稱從與私有網路相關聯的 IP 地址登入。
> - 中：如果與此調查結果相關聯的使用者名稱從公有 IP 地址登入。
> - 高：如果公有 IP 地址存在一致的失敗登入嘗試模式，表示存在過於寬鬆的存取政策。

- 功能：RDS 登入活動監控

此調查結果會通知您，在 AWS 環境中 RDS 資料庫上發現異常的成功登入。這可能表示先前未出現的使用者是第一次登入 RDS 資料庫。常見的案例是內部使用者登入資料庫，該資料庫是由應用程式以程式設計方式存取，而不是由個別使用者存取。

GuardDuty 異常偵測機器學習 (ML) 模型將此成功登入識別為異常狀況。ML 模型會評估 支援的 Amazon Aurora 資料庫 中的所有資料庫登入事件，並識別與對手使用的技術相關聯的異常事件。ML 模型會追蹤 RDS 登入活動的各種因素，例如發出請求的使用者、發出請求的位置，以及使用的特定資料庫連線詳細資訊。如需有關可能異常之登入事件的詳細資訊，請參閱RDS 登入活動型異常。

修復建議：

如果此活動對於關聯的資料庫為非預期活動，建議您變更關聯資料庫使用者的密碼，並檢閱異常使用者執行活動的可用稽核日誌。中等嚴重性和高嚴重性調查結果可能表示資料庫存在過於寬鬆的存取政策，而且使用者憑證可能已公開或遭到入侵。建議將資料庫放置在私有 VPC 中，並將安全群組規則限制為僅允許來自必要來源的流量。如需詳細資訊，請參閱修復可能遭到入侵且含有成功登入事件的資料庫。

CredentialAccess:RDS/AnomalousBehavior.FailedLogin

在您帳戶中的 RDS 資料庫上發現一次或多次異常登入失敗嘗試。

預設嚴重性：低

- 功能：RDS 登入活動監控

此調查結果會通知您，在 AWS 環境中 RDS 資料庫上發現一次或多次異常登入失敗嘗試。從公有 IP 地址嘗試登入失敗，可能表示您帳戶中的 RDS 資料庫已遭受潛在惡意執行者嘗試的暴力攻擊。

GuardDuty 異常偵測機器學習 (ML) 模型會將這些失敗的登入識別為異常。ML 模型會評估 支援的 Amazon Aurora 資料庫 中的所有資料庫登入事件，並識別與對手使用的技術相關聯的異常事件。ML 模型會追蹤 RDS 登入活動的各種因素，例如發出請求的使用者、發出請求的位置，以及使用的特定資料庫連線詳細資訊。如需有關可能異常之 RDS 登入活動的詳細資訊，請參閱RDS 登入活動型異常。

修復建議：

如果此活動對於關聯的資料庫為非預期活動，則可能表示資料庫已公開，或是資料庫存在過於寬鬆的存取政策。建議將資料庫放置在私有 VPC 中，並將安全群組規則限制為僅允許來自必要來源的流量。如需詳細資訊，請參閱修復可能遭到入侵且含有失敗登入事件的資料庫。

CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce

在一致的異常失敗登錄嘗試模式之後，使用者以異常方式從公有 IP 地址成功登入您帳戶中的 RDS 資料庫。

預設嚴重性：高

- 功能：RDS 登入活動監控

此調查結果會通知您，在 AWS 環境中 RDS 資料庫上發現表示成功暴力破解的異常登入。在異常成功登入之前，發現一致的異常失敗登錄嘗試模式。這表示您帳戶中與 RDS 資料庫相關聯的使用者和密碼可能已遭到入侵，而且 RDS 資料庫可能已被潛在惡意執行者存取。

GuardDuty 異常偵測機器學習 (ML) 模型將這次成功的暴力破解登入識別為異常狀況。ML 模型會評估支援的 Amazon Aurora 資料庫 中的所有資料庫登入事件，並識別與對手使用的技術相關聯的異常事件。ML 模型會追蹤 RDS 登入活動的各種因素，例如發出請求的使用者、發出請求的位置，以及使用的特定資料庫連線詳細資訊。如需有關可能異常之 RDS 登入活動的詳細資訊，請參閱RDS 登入活動型異常。

修復建議：

此活動表示資料庫憑證可能已公開或洩露。建議您變更關聯資料庫使用者的密碼，並檢閱可用的稽核日誌，以查看可能遭到入侵的使用者所執行的活動。一致的異常失敗登錄嘗試模式表示資料庫存在過於寬鬆的存取政策，或者資料庫也可能已公開。建議將資料庫放置在私有 VPC 中，並將安全群組規則限制為僅允許來自必要來源的流量。如需詳細資訊，請參閱修復可能遭到入侵且含有成功登入事件的資料庫。

CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin

使用者從已知惡意 IP 地址成功登入您帳戶中的 RDS 資料庫。

預設嚴重性：高

- 功能：RDS 登入活動監控

此調查結果會通知您，從與 AWS 環境中的已知惡意活動相關聯的 IP 地址發生了成功的 RDS 登入活動。這表示您帳戶中與 RDS 資料庫相關聯的使用者和密碼可能已遭到入侵，而且 RDS 資料庫可能已被潛在惡意執行者存取。

修復建議：

如果此活動對於關聯的資料庫為非預期活動，則可能表示使用者憑證可能已公開或遭到入侵。建議您變更關聯資料庫使用者的密碼，並檢閱可用的稽核日誌，以查看遭盜用的使用者所執行的活動。此活動也可能表示資料庫存在過於寬鬆的存取政策，或資料庫已公開。建議將資料庫放置在私有 VPC 中，並將安全群組規則限制為僅允許來自必要來源的流量。如需詳細資訊，請參閱修復可能遭到入侵且含有成功登入事件的資料庫。

CredentialAccess:RDS/MaliciousIPCaller.FailedLogin

與已知惡意活動相關聯的IP 地址未成功嘗試登入帳戶中的 RDS 資料庫。

預設嚴重性：中

- 功能：RDS 登入活動監控

此調查結果會通知您，與已知惡意活動相關聯的 IP 地址嘗試登入 AWS 環境中的 RDS 資料庫，但無法提供正確的使用者名稱或密碼。這表示潛在惡意的參與者可能正在嘗試入侵您帳戶中的 RDS 資料庫。

修復建議：

如果此活動對於關聯的資料庫為非預期活動，則可能表示資料庫存在過於寬鬆的存取政策，或資料庫已公開。建議將資料庫放置在私有 VPC 中，並將安全群組規則限制為僅允許來自必要來源的流量。如需詳細資訊，請參閱修復可能遭到入侵且含有失敗登入事件的資料庫。

Discovery:RDS/MaliciousIPCaller

與已知惡意活動相關聯的IP 地址探查了您帳戶中的 RDS 資料庫；未嘗試進行身分驗證。

預設嚴重性：中

- 功能：RDS 登入活動監控

此調查結果會通知您，與已知惡意活動相關聯的 IP 地址探查了 AWS 環境中的 RDS 資料庫，但未嘗試登入。這可能表示潛在惡意執行者正在嘗試掃描可公開存取的基礎設施。

修復建議：

如果此活動對於關聯的資料庫為非預期活動，則可能表示資料庫存在過於寬鬆的存取政策，或資料庫已公開。建議將資料庫放置在私有 VPC 中，並將安全群組規則限制為僅允許來自必要來源的流量。如需詳細資訊，請參閱修復可能遭到入侵且含有失敗登入事件的資料庫。

CredentialAccess:RDS/TorIPCaller.SuccessfulLogin

使用者從 Tor 退出節點 IP 地址成功登入您帳戶中的 RDS 資料庫。

預設嚴重性：高

- 功能：RDS 登入活動監控

此調查結果會通知您，使用者從 Tor 退出節點 IP 地址成功登入 AWS 環境中的 RDS 資料庫。Tor 是一種啟用匿名通訊的軟體。它會透過一系列網路節點之間的中繼來加密並隨機反彈通訊。最後的 Tor 節點稱為退出節點。這可能表明您帳戶中的 RDS 資源有未經授權的存取，目的是隱藏匿名使用者的真實身分。

修復建議：

如果此活動對於關聯的資料庫為非預期活動，則可能表示使用者憑證可能已公開或遭到入侵。建議您變更關聯資料庫使用者的密碼，並檢閱可用的稽核日誌，以查看遭盜用的使用者所執行的活動。此活動也可能表示資料庫存在過於寬鬆的存取政策，或資料庫已公開。建議將資料庫放置在私有 VPC 中，並將安全群組規則限制為僅允許來自必要來源的流量。如需詳細資訊，請參閱修復可能遭到入侵且含有成功登入事件的資料庫。

CredentialAccess:RDS/TorIPCaller.FailedLogin

Tor IP 地址嘗試登入您帳戶中的 RDS 資料庫失敗。

預設嚴重性：中

- 功能：RDS 登入活動監控

此調查結果會通知您，Tor 退出節點 IP 地址嘗試登入 AWS 環境中的 RDS 資料庫，但無法提供正確的使用者名稱或密碼。Tor 是一種啟用匿名通訊的軟體。它會透過一系列網路節點之間的中繼來加密並隨

機反彈通訊。最後的 Tor 節點稱為退出節點。這可能表明您帳戶中的 RDS 資源有未經授權的存取，目的是隱藏匿名使用者的真實身分。

修復建議：

如果此活動對於關聯的資料庫為非預期活動，則可能表示資料庫存在過於寬鬆的存取政策，或資料庫已公開。建議將資料庫放置在私有 VPC 中，並將安全群組規則限制為僅允許來自必要來源的流量。如需詳細資訊，請參閱修復可能遭到入侵且含有失敗登入事件的資料庫。

Discovery:RDS/TorIPCaller

Tor 退出節點 IP 地址探查到您帳戶中的 RDS 資料庫，但未嘗試進行身分驗證。

預設嚴重性：中

- 功能：RDS 登入活動監控

此調查結果會通知您，Tor 退出節點 IP 地址探查了 AWS 環境中的 RDS 資料庫，但未嘗試登入。這可能表示潛在惡意執行者正在嘗試掃描可公開存取的基礎設施。Tor 是一種啟用匿名通訊的軟體。它會透過一系列網路節點之間的傳送來加密並隨機反彈通訊。最後的 Tor 節點稱為退出節點。這可能表明您帳戶中的 RDS 資源有未經授權的存取，目的是隱藏潛在惡意執行者的真實身分。

修復建議：

如果此活動對於關聯的資料庫為非預期活動，則可能表示資料庫存在過於寬鬆的存取政策，或資料庫已公開。建議將資料庫放置在私有 VPC 中，並將安全群組規則限制為僅允許來自必要來源的流量。如需詳細資訊，請參閱修復可能遭到入侵且含有失敗登入事件的資料庫。

執行階段監視尋找項

Amazon GuardDuty 會產生下列執行階段監控調查結果，以根據 Amazon EKS 叢集、Fargate 和 Amazon ECS 工作負載以及 Amazon EC2 執行個體中 Amazon EC2 主機和容器的作業系統層級行為指出潛在威脅。

> **Note**
>
> 執行期監控調查結果類型以從主機收集的執行期記錄為基礎。日誌包含可能由惡意執行者控制的檔案路徑等欄位。這些欄位也包含在 GuardDuty 發現項目中，以提供執行階段內容。在

GuardDuty 主控台外部處理「執行時期監視」發現項目時，您必須清理尋找項目欄位。例如，在網頁上顯示調查結果欄位時，您可以進行 HTML 編碼。

主題

- CryptoCurrency:Runtime/BitcoinTool.B
- Backdoor:Runtime/C&CActivity.B
- UnauthorizedAccess:Runtime/TorRelay
- UnauthorizedAccess:Runtime/TorClient
- Trojan:Runtime/BlackholeTraffic
- Trojan:Runtime/DropPoint
- CryptoCurrency:Runtime/BitcoinTool.B!DNS
- Backdoor:Runtime/C&CActivity.B!DNS
- Trojan:Runtime/BlackholeTraffic!DNS
- Trojan:Runtime/DropPoint!DNS
- Trojan:Runtime/DGADomainRequest.C!DNS
- Trojan:Runtime/DriveBySourceTraffic!DNS
- Trojan:Runtime/PhishingDomainRequest!DNS
- Impact:Runtime/AbusedDomainRequest.Reputation
- Impact:Runtime/BitcoinDomainRequest.Reputation
- Impact:Runtime/MaliciousDomainRequest.Reputation
- Impact:Runtime/SuspiciousDomainRequest.Reputation
- UnauthorizedAccess:Runtime/MetadataDNSRebind
- Execution:Runtime/NewBinaryExecuted
- PrivilegeEscalation:Runtime/DockerSocketAccessed
- PrivilegeEscalation:Runtime/RuncContainerEscape
- PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified
- DefenseEvasion:Runtime/ProcessInjection.Proc
- DefenseEvasion:Runtime/ProcessInjection.Ptrace
- DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite

- Execution:Runtime/ReverseShell
- DefenseEvasion:Runtime/FilelessExecution
- Impact:Runtime/CryptoMinerExecuted
- Execution:Runtime/NewLibraryLoaded
- PrivilegeEscalation:Runtime/ContainerMountsHostDirectory
- PrivilegeEscalation:Runtime/UserfaultfdUsage
- Execution:Runtime/SuspiciousTool
- Execution:Runtime/SuspiciousCommand
- DefenseEvasion:Runtime/SuspiciousCommand
- DefenseEvasion:Runtime/PtraceAntiDebugging
- Execution:Runtime/MaliciousFileExecuted

CryptoCurrency:Runtime/BitcoinTool.B

Amazon EC2 執行個體或容器正在查詢與加密貨幣相關活動有關聯的 IP 地址。

預設嚴重性：高

- 功能：執行期監控

此調查結果會通知您，列出的 AWS 環境中的 EC2 執行個體或容器正在查詢與加密貨幣相關活動有關聯的 IP 地址。威脅執行者可能試圖控制計算資源，以惡意重新利用它們進行未經授權的加密貨幣挖掘。

執行期代理程式會監控多種資源類型的事件。若要識別可能遭到入侵的資源，請在 GuardDuty 主控台的「發現項目」面板中檢視資源類型。

修復建議：

如果您使用此 EC2 執行個體或容器來挖掘或管理加密貨幣，或者進行兩者中以其他方式參與區塊鏈活動的行為，則此 CryptoCurrency:Runtime/BitcoinTool.B 調查結果可能代表您環境的預期活動。如果您的 AWS 環境是這種情況，建議您為此發現項目設定抑制規則。隱藏規則應包含兩個篩選準則。第一個篩選條件應該使用調查結果類型屬性，其值為 `CryptoCurrency:Runtime/BitcoinTool.B`。第二個篩選條件應該是涉及加密貨幣或區塊鏈相關活動的執行個體的執行個體 ID 或相關容器的容器映像 ID。如需詳細資訊，請參閱隱藏規則。

如果此活動不在預期中，即代表您的資源可能已遭入侵。如需詳細資訊，請參閱 修正執行時期監視發現項。

Backdoor:Runtime/C&CActivity.B

Amazon EC2 執行個體或容器正在查詢與已知命令和控管伺服器相關聯的 IP。

預設嚴重性：高

- 功能：執行期監控

此調查結果會通知您，列出的 AWS 環境中的 EC2 執行個體或容器正在查詢與已知命令和控管 (C&C) 伺服器相關聯的 IP。列出的執行個體或容器可能已遭入侵。命令和控管伺服器是對殭屍網路的成員發出命令的電腦。

殭屍網路是一種透過常見惡意軟體感染和控制的網際網路連線裝置集合，可能包括 PC、伺服器、行動裝置及物聯網裝置。殭屍網路經常用來散佈惡意軟體和收集不當資訊，像是信用卡號碼。根據殭屍網路的用途和結構而定，C&C 伺服器也可能發出命令來展開分散式阻斷服務 (DDoS) 攻擊。

> **Note**
>
> 如果查詢的 IP 與 log4J 相關，則相關調查結果的欄位將包含下列值：
>
> - `service.additionalInfo.threatListName = Amazon`
> - `service.additionalInfo.threatName = Log4j Related`

執行期代理程式會監控多種資源類型的事件。若要識別可能遭到入侵的資源，請在 GuardDuty主控台的發現項目面板中檢視資源類型。

修復建議：

如果此活動不在預期中，即代表您的資源可能已遭入侵。如需詳細資訊，請參閱 修正執行時期監視發現項。

UnauthorizedAccess:Runtime/TorRelay

您的 Amazon EC2 執行個體或容器正在連線至 Tor 網路作為 Tor 轉送。

預設嚴重性：高

- 功能：執行期監控

這項發現會通知您 AWS 環境中的 EC2 執行個體或容器正在連線到 Tor 網路，表明它充當 Tor 中繼。Tor 是一種啟用匿名通訊的軟體。Tor 增加匿名通訊，做法是從一個 Tor 轉送轉寄使用者端潛在非法流量至另一個 Tor 轉送。

執行期代理程式會監控多種資源類型的事件。若要識別可能遭到入侵的資源，請在 GuardDuty 主控台的「發現項目」面板中檢視資源類型。

執行期代理程式會監控多種資源類型的事件。若要識別可能遭到入侵的資源，請在 GuardDuty 主控台的「發現項目」面板中檢視資源類型。

修復建議：

如果此活動不在預期中，即代表您的資源可能已遭入侵。如需詳細資訊，請參閱 修正執行時期監視發現項。

UnauthorizedAccess:Runtime/TorClient

您的 Amazon EC2 執行個體或容器正在連線到 Tor Guard 或 Authority 節點。

預設嚴重性：高

- 功能：執行期監控

此發現會通知您 AWS 環境中的 EC2 執行個體或容器正在連線到 Tor Guard 或授權節點。Tor 是一種啟用匿名通訊的軟體。Tor Guards 和 Authority 節點為進入 Tor 網路的初始閘道。此流量表示此 EC2 執行個體或容器可能已遭入侵，且作為 Tor 網路中的用戶端。此發現可能表示未經授權存取您的 AWS 資源，意圖隱藏攻擊者的真實身分。

執行期代理程式會監控多種資源類型的事件。若要識別可能遭到入侵的資源，請在 GuardDuty 主控台的「發現項目」面板中檢視資源類型。

執行期代理程式會監控多種資源類型的事件。若要識別可能遭到入侵的資源，請在 GuardDuty 主控台的「發現項目」面板中檢視資源類型。

修復建議：

如果此活動不在預期中，即代表您的資源可能已遭入侵。如需詳細資訊，請參閱 修正執行時期監視發現項。

Trojan:Runtime/BlackholeTraffic

Amazon EC2 執行個體或容器正在嘗試與已知是黑洞的遠端主機 IP 地址進行通訊。

預設嚴重性：中

- 功能：執行期監控

此發現項目會通知您 AWS 環境中列出的 EC2 執行個體或容器可能遭到入侵，因為它試圖與黑洞 (或接收孔) 的 IP 位址進行通訊。黑洞是在網路上某些傳入或傳出流量會被無聲無息丟棄的地方，且資料來源也不會收到資料未傳送至收件人的通知。黑洞的 IP 地址會指定為未執行的主機，或未分配主機的地址。

執行期代理程式會監控多種資源類型的事件。若要識別可能遭到入侵的資源，請在 GuardDuty 主控台的「發現項目」面板中檢視資源類型。

修復建議：

如果此活動不在預期中，即代表您的資源可能已遭入侵。如需詳細資訊，請參閱 修正執行時期監視發現項。

Trojan:Runtime/DropPoint

Amazon EC2 執行個體或容器正在嘗試與遠端主機的 IP 地址進行通訊，該主機已知存放了惡意軟體擷取的憑證和其他遭竊資料。

預設嚴重性：中

- 功能：執行期監控

此發現項目會通知您 AWS 環境中的 EC2 執行個體或容器正在嘗試與遠端主機的 IP 位址進行通訊，該 IP 位址已知會保留登入資料以及惡意軟體擷取的其他遭竊資料。

執行期代理程式會監控多種資源類型的事件。若要識別可能遭到入侵的資源，請在 GuardDuty 主控台的「發現項目」面板中檢視資源類型。

修復建議：

如果此活動不在預期中，即代表您的資源可能已遭入侵。如需詳細資訊，請參閱 修正執行時期監視發現項。

CryptoCurrency:Runtime/BitcoinTool.B!DNS

Amazon EC2 執行個體或容器正在查詢與加密貨幣活動有關聯的網域名稱。

預設嚴重性：高

- 功能：執行期監控

此調查結果會通知您，列出的 AWS 環境中的 EC2 執行個體或容器正在查詢與比特幣或其他加密貨幣相關活動有關聯的網域名稱。威脅執行者可能試圖控制計算資源，以惡意重新利用它們進行未經授權的加密貨幣挖掘。

執行期代理程式會監控多種資源類型的事件。若要識別可能遭到入侵的資源，請在 GuardDuty 主控台的「發現項目」面板中檢視資源類型。

修復建議：

如果您使用此 EC2 執行個體或容器來挖掘或管理加密貨幣，或者進行兩者中以其他方式參與區塊鏈活動的行為，則此 CryptoCurrency:Runtime/BitcoinTool.B!DNS 調查結果可能是您環境的預期活動。如果您的 AWS 環境是這種情況，建議您為此發現項目設定抑制規則。隱藏規則應包含兩個篩選準則。第一個條件應該使用調查結果類型屬性，其值為 `CryptoCurrency:Runtime/BitcoinTool.B!DNS`。第二個篩選條件應該是加密貨幣或區塊鏈活動的執行個體的執行個體 ID 或相關容器的容器映像 ID。如需詳細資訊，請參閱隱藏規則。

如果此活動不在預期中，即代表您的資源可能已遭入侵。如需詳細資訊，請參閱 修正執行時期監視發現項。

Backdoor:Runtime/C&CActivity.B!DNS

Amazon EC2 執行個體或容器正在查詢與已知命令和控管伺服器相關聯的網域名稱。

預設嚴重性：高

- 功能：執行期監控

此調查結果會通知您，列出的 AWS 環境中的 EC2 執行個體或容器正在查詢與已知命令和控管 (C&C) 伺服器相關聯的網域名稱。列出的 EC2 執行個體或容器可能已遭入侵。命令和控管伺服器是對殭屍網路的成員發出命令的電腦。

殭屍網路是一種透過常見惡意軟體感染和控制的網際網路連線裝置集合，可能包括 PC、伺服器、行動裝置及物聯網裝置。殭屍網路經常用來散佈惡意軟體和收集不當資訊，像是信用卡號碼。根據殭屍網路的用途和結構而定，C&C 伺服器也可能發出命令來展開分散式阻斷服務 (DDoS) 攻擊。

> **Note**
>
> 如果查詢的網域名稱與 log4J 相關，則相關調查結果的欄位將包含下列值：
>
> - `service.additionalInfo.threatListName = Amazon`
> - `service.additionalInfo.threatName = Log4j Related`

> **Note**
>
> 若要測試如何 GuardDuty 產生此尋找項目類型，您可以針對測試網域從執行個體 (使用 `dig` Linux 或 `nslookup` Windows) 發出 DNS 要求`guarddutyc2activityb.com`。

執行期代理程式會監控多種資源類型的事件。若要識別可能遭到入侵的資源，請在 GuardDuty 主控台的「發現項目」面板中檢視資源類型。

修復建議：

如果此活動不在預期中，即代表您的資源可能已遭入侵。如需詳細資訊，請參閱 修正執行時期監視發現項。

Trojan:Runtime/BlackholeTraffic!DNS

Amazon EC2 執行個體或容器正在查詢重新導向到黑洞 IP 地址的網域名稱。

預設嚴重性：中

- 功能：執行期監控

此調查結果會通知您，列出的 AWS 環境中的 EC2 執行個體或容器可能已遭入侵，因為它正在查詢被重新導向至黑洞 IP 地址的網域名稱。黑洞是在網路上某些傳入或傳出流量會被無聲無息丟棄的地方，且資料來源也不會收到資料未傳送至收件人的通知。

執行期代理程式會監控多種資源類型的事件。若要識別可能遭到入侵的資源，請在 GuardDuty 主控台的「發現項目」面板中檢視資源類型。

如果此活動不在預期中，即代表您的資源可能已遭入侵。如需詳細資訊，請參閱 修正執行時期監視發現項。

Trojan:Runtime/DropPoint!DNS

Amazon EC2 執行個體或容器正在查詢遠端主機的網域名稱，該主機已知存放了惡意軟體擷取的憑證和其他遭竊資料。

預設嚴重性：中

- 功能：執行期監控

此發現項目會通知您 AWS 環境中的 EC2 執行個體或容器正在查詢遠端主機的網域名稱，該遠端主機的網域名稱已知會保留登入資料以及惡意軟體擷取的其他遭竊資料。

執行期代理程式會監控多種資源類型的事件。若要識別可能遭到入侵的資源，請在 GuardDuty 主控台的「發現項目」面板中檢視資源類型。

修復建議：

如果此活動不在預期中，即代表您的資源可能已遭入侵。如需詳細資訊，請參閱 修正執行時期監視發現項。

Trojan:Runtime/DGADomainRequest.C!DNS

Amazon EC2 執行個體或容器正在查詢演算法產生的網域。惡意軟體常用這種網域，且這可以視為 EC2 執行個體或容器已遭入侵的跡象。

預設嚴重性：高

- 功能：執行期監控

此調查結果會通知您，列出的 AWS 環境中的 EC2 執行個體或容器正在嘗試查詢網域產生演算法 (DGA) 網域。您的資源可能已遭入侵。

DGA 可用來定期產生大量網域名稱，這些名稱可做為他們的命令與控制 (C&C) 伺服器的會合點。命令和控管伺服器是對殭屍網路的成員發出命令的電腦，這是一種透過常見惡意軟體感染和控制的網際網路連線裝置集合。大量潛在的會合點會造成難以有效地關閉殭屍網路，因為受感染的電腦每天都會嘗試聯繫其中一些網域名稱以接收更新或命令。

> **Note**
>
> 此發現項目是以 GuardDuty 威脅情報摘要中已知的 DGA 網域為基礎。

執行期代理程式會監控多種資源類型的事件。若要識別可能遭到入侵的資源，請在 GuardDuty 主控台的「發現項目」面板中檢視資源類型。

修復建議：

如果此活動不在預期中，即代表您的資源可能已遭入侵。如需詳細資訊，請參閱 修正執行時期監視發現項。

Trojan:Runtime/DriveBySourceTraffic!DNS

Amazon EC2 執行個體或容器正在查詢已知是 Drive-By (路過式) 下載攻擊來源的遠端主機網域名稱。

預設嚴重性：高

- 功能：執行期監控

此調查結果會通知您，列出的 AWS 環境中的 EC2 執行個體或容器可能已遭入侵，因為它正在查詢已知是 Drive-By (路過式) 下載攻擊來源的遠端主機網域名稱。這些是從網際網路上意外下載的電腦軟體，它們可以啟動病毒、間諜軟體或惡意軟體的自動安裝。

執行期代理程式會監控多種資源類型的事件。若要識別可能遭到入侵的資源，請在 GuardDuty 主控台的「發現項目」面板中檢視資源類型。

修復建議：

如果此活動不在預期中，即代表您的資源可能已遭入侵。如需詳細資訊，請參閱 修正執行時期監視發現項。

Trojan:Runtime/PhishingDomainRequest!DNS

Amazon EC2 執行個體或容器正在查詢遭釣魚攻擊的網域。

預設嚴重性：高

- 功能：執行期監控

此調查結果會通知您，在 AWS 環境中有一個 EC2 執行個體或容器正在嘗試查詢遭釣魚攻擊的網域。釣魚網域是由冒充合法機構的人所建立，以誘使個人提供敏感資料，如個人身分資訊、銀行和信用卡詳細資訊以及密碼。您的 EC2 執行個體或容器可能試圖擷取儲存在釣魚網站上的敏感資料，或者嘗試設定網路釣魚網站。您的 EC2 執行個體或容器可能已遭入侵。

執行期代理程式會監控多種資源類型的事件。若要識別可能遭到入侵的資源，請在 GuardDuty 主控台的「發現項目」面板中檢視資源類型。

修復建議：

如果此活動不在預期中，即代表您的資源可能已遭入侵。如需詳細資訊，請參閱 修正執行時期監視發現項。

Impact:Runtime/AbusedDomainRequest.Reputation

Amazon EC2 執行個體或容器正在查詢與已知的濫用網域相關聯的低信譽網域名稱。

預設嚴重性：中

- 功能：執行期監控

此調查結果會通知您，列出的 AWS 環境中的 EC2 執行個體或容器正在查詢與已知的濫用網域或 IP 地址相關聯的低信譽網域名稱。濫用網域的範例包括頂層網域名稱 (TLD) 和第二層網域名稱 (2LD)，提供

免費的子網域註冊，以及動態 DNS 提供者。威脅執行者傾向於使用這些服務免費或低成本註冊網域。此類別中的低信譽網域也可能是解析為註冊機構停駐 IP 地址的過期網域，因此可能不再處於作用中狀態。停駐 IP 是註冊機構為尚未連結到任何服務的網域引導流量的地方。列出的 Amazon EC2 執行個體或容器可能已遭入侵，因為威脅執行者通常使用這些註冊機構或服務進行 C&C 和惡意軟體分發。

低信譽網域以信譽評分模型為基礎。此模型會評估網域的特徵並對其進行排名，以判斷其為惡意的可能性。

執行期代理程式會監控多種資源類型的事件。若要識別可能遭到入侵的資源，請在 GuardDuty 主控台的「發現項目」面板中檢視資源類型。

修復建議：

如果此活動不在預期中，即代表您的資源可能已遭入侵。如需詳細資訊，請參閱 修正執行時期監視發現項。

Impact:Runtime/BitcoinDomainRequest.Reputation

Amazon EC2 執行個體或容器正在查詢與加密貨幣相關活動有關聯的低信譽網域名稱。

預設嚴重性：高

- 功能：執行期監控

此調查結果會通知您，列出的 AWS 環境中的 EC2 執行個體或容器正在查詢與比特幣或其他加密貨幣相關活動有關聯的低信譽網域名稱。威脅執行者可能試圖控制計算資源，以惡意重新利用它們進行未經授權的加密貨幣挖掘。

低信譽網域以信譽評分模型為基礎。此模型會評估網域的特徵並對其進行排名，以判斷其為惡意的可能性。

執行期代理程式會監控多種資源類型的事件。若要識別可能遭到入侵的資源，請在 GuardDuty 主控台的「發現項目」面板中檢視資源類型。

修復建議：

如果您使用此 EC2 執行個體或容器來挖掘或管理加密貨幣，或者如果這些資源以其他方式參與區塊鏈活動的行為，則此調查結果可能代表您環境的預期活動。如果您的 AWS 環境是這種情況，建議您為此

發現項目設定抑制規則。隱藏規則應包含兩個篩選準則。第一個篩選條件應該使用調查結果類型屬性，其值為 `Impact:Runtime/BitcoinDomainRequest.Reputation`。第二個篩選條件應該是涉及加密貨幣或區塊鏈相關活動的執行個體的執行個體 ID 或相關容器的容器映像 ID。如需詳細資訊，請參閱隱藏規則。

如果此活動不在預期中，即代表您的資源可能已遭入侵。如需詳細資訊，請參閱 修正執行時期監視發現項。

Impact:Runtime/MaliciousDomainRequest.Reputation

Amazon EC2 執行個體或容器正在查詢與已知惡意網域相關聯的低信譽網域名稱。

預設嚴重性：高

- 功能：執行期監控

此調查結果會通知您，列出的 AWS 環境中的 EC2 執行個體或容器正在查詢與已知惡意網域或 IP 地址相關聯的低信譽網域名稱。例如，網域可能與已知的沉洞 IP 地址相關聯。沉洞網域是先前由威脅執行者控制的網域，對其提出的請求可能表示執行個體已遭到入侵。這些網域也可能與已知的惡意活動或網域產生演算法相關。

低信譽網域以信譽評分模型為基礎。此模型會評估網域的特徵並對其進行排名，以判斷其為惡意的可能性。

執行期代理程式會監控多種資源類型的事件。若要識別可能遭到入侵的資源，請在 GuardDuty 主控台的「發現項目」面板中檢視資源類型。

修復建議：

如果此活動不在預期中，即代表您的資源可能已遭入侵。如需詳細資訊，請參閱 修正執行時期監視發現項。

Impact:Runtime/SuspiciousDomainRequest.Reputation

Amazon EC2 執行個體或容器正在查詢低信譽的網域名稱，該網域名稱本質上因其使用期限或低熱門程度而可疑。

預設嚴重性：低

- 功能：執行期監控

此調查結果會通知您，列出的 AWS 環境中的 EC2 執行個體或容器正在查詢疑似惡意的低信譽網域名稱。注意到該網域的特徵與先前發現的惡意網域一致，但是，我們的信譽模型無法明確地將其與已知威脅聯繫起來。這些網域通常是新觀察到的，或接收少量的流量。

低信譽網域以信譽評分模型為基礎。此模型會評估網域的特徵並對其進行排名，以判斷其為惡意的可能性。

執行期代理程式會監控多種資源類型的事件。若要識別可能遭到入侵的資源，請在 GuardDuty 主控台的「發現項目」面板中檢視資源類型。

修復建議：

如果此活動不在預期中，即代表您的資源可能已遭入侵。如需詳細資訊，請參閱 修正執行時期監視發現項。

UnauthorizedAccess:Runtime/MetadataDNSRebind

Amazon EC2 執行個體或容器正在執行解析為執行個體中繼資料服務的 DNS 查詢。

預設嚴重性：高

- 功能：執行期監控

> **Note**
>
> 目前，此查找類型僅支持 AMD64 架構。

此發現項目會通知您 AWS 環境中的 EC2 執行個體或容器正在查詢解析為 EC2 中繼資料 IP 位址的網域 (169.254.169.254)。這種類型的 DNS 查詢可能表示執行個體是 DNS 重新繫結技術的目標。此技術可用於從 EC2 執行個體獲取中繼資料，包含與執行個體相關聯的 IAM 憑證。

DNS 重新繫結涉及誘使在 EC2 執行個體上執行的應用程式從 URL 載入傳回資料，其中，URL 中的網域名稱解析為 EC2 中繼資料的 IP 地址 (169.254.169.254)。這會導致應用程式存取 EC2 中繼資料，並可能讓攻擊者能夠使用。

只有在 EC2 執行個體執行的具漏洞應用程式允許注入 URL，或有人在 EC2 執行個體上執行的 Web 瀏覽器存取 URL 時，才可能使用 DNS 重新繫結存取 EC2 中繼資料。

執行期代理程式會監控多種資源類型的事件。若要識別可能遭到入侵的資源，請在 GuardDuty 主控台的「發現項目」面板中檢視資源類型。

修復建議：

為了回應此調查結果，您應該評估是否有在 EC2 執行個體或容器上執行的易受攻擊的應用程式，或是是否有人使用瀏覽器存取調查結果中識別的網域。如果根本原因是易受攻擊的應用程式，請修復該漏洞。如果有人瀏覽已識別的網域，請封鎖該網域或防止使用者存取該網域。如果您判斷此調查結果與上述任一案例有關，請撤銷與 EC2 執行個體相關聯的工作階段。

有些 AWS 客戶故意將中繼資料 IP 位址對應至其授權 DNS 伺服器上的網域名稱。如果您的 環境是這種情況，建議您為此調查結果設定隱藏規則。隱藏規則應包含兩個篩選準則。第一個篩選條件應該使用調查結果類型屬性，其值為 `UnauthorizedAccess:Runtime/MetaDataDNSRebind`。第二個篩選條件應該是 DNS 請求網域或容器的容器映像 ID。DNS 請求網域值應該符合您映射到中繼資料 IP 地址 (`169.254.169.254`) 的網域。如需有關建立隱藏規則的詳細資訊，請參閱隱藏規則。

如果此活動不在預期中，即代表您的資源可能已遭入侵。如需詳細資訊，請參閱 修正執行時期監視發現項。

Execution:Runtime/NewBinaryExecuted

已執行容器中新建立或最近修改的二進位檔案。

預設嚴重性：中

- 功能：執行期監控

此調查結果會通知您，系統已執行容器中新建立或最近修改的二進位檔案。最佳實務是讓容器在執行期不可變，而且不應在容器的生命週期內建立或修改二進位檔案、指令碼或程式庫。此行為表示已取得容器存取權、下載並執行惡意程式碼或其他軟體，作為潛在入侵的一部分的惡意行為者。雖然這種類型的活動可能是一種折衷的指示，但它也是一種常見的使用模式。因此，會 GuardDuty 使用機制來識別此活動的可疑執行個體，並僅針對可疑執行個體產生此尋找類型。

執行期代理程式會監控多種資源類型的事件。若要識別可能遭到入侵的資源，請在 GuardDuty 主控台的「發現項目」面板中檢視資源類型。

修復建議：

如果此活動不在預期中，即代表您的資源可能已遭入侵。如需詳細資訊，請參閱 修正執行時期監視發現項。

PrivilegeEscalation:Runtime/DockerSocketAccessed

容器內的程序正在使用 Docker 通訊端與 Docker 常駐程式進行通訊。

預設嚴重性：中

- 功能：執行期監控

Docker 通訊端是 Docker 常駐程式 (`dockerd`) 用於與用戶端進行通訊的 Unix 網域通訊端。用戶端可以執行各種操作，例如通過 Docker 通訊端與 Docker 常駐程式進行通訊來建立容器。容器程序存取 Docker 通訊端是可疑行為。容器程序可以透過與 Docket 通訊端通訊並建立特權容器來逸出容器並獲得主機層級存取許可。

執行期代理程式會監控多種資源類型的事件。若要識別可能遭到入侵的資源，請在 GuardDuty 主控台的發現項目面板中檢視資源類型。

修復建議：

如果此活動不在預期中，即代表您的資源可能已遭入侵。如需詳細資訊，請參閱 修正執行時期監視發現項。

PrivilegeEscalation:Runtime/RuncContainerEscape

偵測到透過 runC 的容器逸出嘗試。

預設嚴重性：高

- 功能：執行期監控

runC 是高階容器執行階段 (例如 Docker 和 Containerd) 用來產生和執行容器的低階容器執行階段。runC 始終以 root 權限執行，因為它需要執行創建容器的低級任務。威脅執行者可透過修改或利用 RunC 二進位檔案中的弱點來取得主機層級的存取權。

此發現項目會偵測到對 runC 二進位檔案的修改，以及可能嘗試惡意利用下列 RunC 弱點：

- CVE-2019-5736— 利用CVE-2019-5736涉及從容器內覆寫 runC 二進位檔。當容器內的處理序修改 runC 二進位檔時，就會叫用此發現項目。
- CVE-2024-21626-利用CVE-2024-21626涉及將當前工作目錄（CWD）或容器設置為打開的文件描述符。`/proc/self/fd/`*`FileDescriptor`*當偵測到具有下目前工作目錄的容器處理序時，`/proc/self/fd/`就會叫用此發現項目，例如，`/proc/self/fd/7`。

此發現可能表示惡意行為者嘗試在下列其中一種類型的容器中執行惡意利用：

- 具有攻擊者控制的映像的新容器。
- 具有主機層級 RunC 二進位檔寫入權限的演員可存取的現有容器。

執行期代理程式會監控多種資源類型的事件。若要識別可能遭到入侵的資源，請在 GuardDuty 主控台的發現項目面板中檢視資源類型。

修復建議：

如果此活動不在預期中，即代表您的資源可能已遭入侵。如需詳細資訊，請參閱 修正執行時期監視發現項。

PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified

偵測到透過 cGroups 發行代理程式進行的容器逸出嘗試。

預設嚴重性：高

- 功能：執行期監控

此調查結果會通知您，偵測到嘗試修改控制群組 (cgroup) 發行代理程式檔案的行為。Linux 使用控制群組 (cgroup) 來限制、說明和隔離處理程序集合的資源使用情況。每個 cgroup 都有一個發行代理程式檔案 (`release_agent`)，這是一個指令碼，當 cgroup 內的任何程序終止時，Linux 會執行該命令碼。發行代理程式檔案一律會在主機層級執行。容器內的安全威脅執行者可將任意命令寫入屬於 cgroup 的發行代理程式檔案，藉此逸出至主機。當 cgroup 中的一個程序終止時，該執行者編寫的命令將被執行。

執行期代理程式會監控多種資源類型的事件。若要識別可能遭到入侵的資源，請在 GuardDuty 主控台的發現項目面板中檢視資源類型。

修復建議：

如果此活動不在預期中，即代表您的資源可能已遭入侵。如需詳細資訊，請參閱 修正執行時期監視發現項。

DefenseEvasion:Runtime/ProcessInjection.Proc

在容器或 Amazon EC2 執行個體中偵測到使用 proc 檔案系統的程序注入。

預設嚴重性：高

- 功能：執行期監控

程序注入是威脅執行者用來將程式碼插入程序中的一種技術，以逃避防禦並可能提升許可。proc 檔案系統 (procfs) 是 Linux 中的一種特殊的檔案系統，會將程序的虛擬記憶體作為檔案顯示。該檔案的路徑是 `/proc/PID/mem`，其中 `PID` 是程序的唯一 ID。威脅執行者可以寫入此檔案，將程式碼插入程序。此調查結果可識別寫入此檔案的潛在嘗試。

執行期代理程式會監控多種資源類型的事件。若要識別可能遭到入侵的資源，請在 GuardDuty 主控台的發現項目面板中檢視資源類型。

修復建議：

如果此活動不在預期中，即代表您的資源類型可能已遭入侵。如需詳細資訊，請參閱 修正執行時期監視發現項。

DefenseEvasion:Runtime/ProcessInjection.Ptrace

在容器或 Amazon EC2 執行個體中偵測到使用 ptrace 系統呼叫的程序注入。

預設嚴重性：中

- 功能：執行期監控

程序注入是威脅執行者用來將程式碼插入程序中的一種技術，以逃避防禦並可能提升許可。一個程序可以使用 ptrace 系統呼叫將程式碼注入到另一個程序中。此調查結果可識別使用 ptrace 系統呼叫將程式碼插入程序的潛在嘗試。

執行期代理程式會監控多種資源類型的事件。若要識別可能遭到入侵的資源，請在 GuardDuty 主控台的發現項目面板中檢視資源類型。

修復建議：

如果此活動不在預期中，即代表您的資源類型可能已遭入侵。如需詳細資訊，請參閱 修正執行時期監視發現項。

DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite

在容器或 Amazon EC2 執行個體中偵測到透過直接寫入虛擬記憶體的程序注入。

預設嚴重性：高

- 功能：執行期監控

程序注入是威脅執行者用來將程式碼插入程序中的一種技術，以逃避防禦並可能提升許可。一個程序可以使用系統呼叫 (例如 `process_vm_writev`) 直接將程式碼插入另一個程序的虛擬記憶體中。此調查結果可識別使用系統呼叫寫入處理程序虛擬記憶體，從而將程式碼插入程序的潛在嘗試。

執行期代理程式會監控多種資源類型的事件。若要識別可能遭到入侵的資源，請在 GuardDuty 主控台的發現項目面板中檢視資源類型。

修復建議：

如果此活動不在預期中，即代表您的資源類型可能已遭入侵。如需詳細資訊，請參閱 修正執行時期監視發現項。

Execution:Runtime/ReverseShell

容器或 Amazon EC2 執行個體中的程序已建立反向 Shell。

預設嚴重性：高

- 功能：執行期監控

反向 Shell 是在從目標主機啟動至執行者主機的連線上建立的 Shell 工作階段。正常 Shell 是從執行者的主機啟動到目標主機，反向 Shell 則與之相反。威脅執行者會建立反向 Shell，在取得對目標的初始存取許可後，在目標上執行命令。此調查結果可識別建立反向 Shell 的潛在嘗試。

修復建議：

如果此活動不在預期中，即代表您的資源類型可能已遭入侵。

DefenseEvasion:Runtime/FilelessExecution

容器或 Amazon EC2 執行個體中的程序正在從記憶體執行程式碼。

預設嚴重性：中

- 功能：執行期監控

當使用磁碟上的記憶體內可執行檔執行程序時，此調查結果會通知您。這是一種常見的防禦逃避技術，可避免將惡意可執行檔案寫入磁碟，以逃避基於掃描的檔案系統的檢測。儘管惡意軟體會使用此技術，但也有一些合法的用例。其中一個例子是一個 just-in-time （JIT）編譯器，它將編譯後的代碼寫入內存並從內存中執行它。

執行期代理程式會監控多種資源類型的事件。若要識別可能遭到入侵的資源，請在 GuardDuty 主控台的發現項目面板中檢視資源類型。

修復建議：

如果此活動不在預期中，即代表您的資源可能已遭入侵。如需詳細資訊，請參閱 修正執行時期監視發現項。

Impact:Runtime/CryptoMinerExecuted

容器或 Amazon EC2 執行個體正在執行與加密貨幣挖掘活動相關聯的二進位檔案。

預設嚴重性：高

- 功能：執行期監控

此發現項目會通知您 AWS 環境中的容器或 EC2 執行個體正在執行與加密貨幣採礦活動相關聯的二進位檔案。威脅執行者可能試圖控制計算資源，以惡意重新利用它們進行未經授權的加密貨幣挖掘。

執行期代理程式會監控多種資源類型的事件。若要識別可能遭到入侵的資源，請在 GuardDuty 主控台的發現項目面板中檢視資源類型。

修復建議：

執行期代理程式會監控多個資源的事件。若要識別受影響的資源，請在 GuardDuty 主控台的發現項目詳細資料中檢視資源類型，然後參閱修正執行時期監視發現項。

Execution:Runtime/NewLibraryLoaded

新建立或最近修改的程式庫由容器內的程序載入。

預設嚴重性：中

- 功能：執行期監控

此調查結果會通知您，程式庫是在執行期在容器內建立或修改的，並由容器內執行的程序載入。最佳實務是讓容器在執行期不可變，而且不應在容器的生命週期內建立或修改二進位檔案、指令碼或程式庫。在容器中載入新建立或修改的程式庫可能表示存在可疑活動。此行為表示惡意執行者可能獲得對容器的存取許可，且已經下載並執行惡意軟體或其他軟體作為潛在入侵的一部分。雖然這種類型的活動可能是一種折衷的指示，但它也是一種常見的使用模式。因此，會 GuardDuty 使用機制來識別此活動的可疑執行個體，並僅針對可疑執行個體產生此尋找類型。

執行期代理程式會監控多個資源的事件。若要識別受影響的資源，請在 GuardDuty主控台的發現項目詳細資料中檢視資源類型。

修復建議：

如果此活動不在預期中，即代表您的資源可能已遭入侵。如需詳細資訊，請參閱 修正執行時期監視發現項。

PrivilegeEscalation:Runtime/ContainerMountsHostDirectory

容器內的程序在執行期掛載了主機檔案系統。

預設嚴重性：中

- 功能：執行期監控

多種容器逸出技術涉及在執行期在容器中安裝主機檔案系統。此調查結果會通知您，容器內的程序可能嘗試掛載主機檔案系統，這可能表示存在嘗試逸出到主機的行為。

執行期代理程式會監控多個資源的事件。若要識別受影響的資源，請在 GuardDuty主控台的發現項目詳細資料中檢視資源類型。

修復建議：

如果此活動不在預期中，即代表您的資源可能已遭入侵。如需詳細資訊，請參閱 修正執行時期監視發現項。

PrivilegeEscalation:Runtime/UserfaultfdUsage

程序使用 **userfaultfd** 系統呼叫來處理使用者空間中的頁面錯誤。

預設嚴重性：中

- 功能：執行期監控

通常，頁面錯誤由核心空間中的核心處理。但是，userfaultfd 系統呼叫允許程序在使用者空間中處理檔案系統上的頁面錯誤。這個有用的功能可以實現使用者空間檔案系統的實作。另一方面，潛在惡意程序也可以利用它來中斷使用者空間的核心。使用 userfaultfd 系統呼叫中斷核心是在利用核心競爭條件期間延伸競爭視窗的常見利用技術。使用 userfaultfd 可能表示 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體上存在可疑活動。

執行期代理程式會監控多個資源的事件。若要識別受影響的資源，請在 GuardDuty主控台的發現項目詳細資料中檢視資源類型。

修復建議：

如果此活動不在預期中，即代表您的資源可能已遭入侵。如需詳細資訊，請參閱 修正執行時期監視發現項。

Execution:Runtime/SuspiciousTool

容器或 Amazon EC2 執行個體正在執行二進位檔案或指令碼，這些檔案或指令碼經常用於冒犯性的安全案例 (例如滲透測試參與)。

預設嚴重性：變數

此發現的嚴重程度可以是高還是低，具體取決於檢測到的可疑工具是否被認為是雙重使用還是專門用於冒犯性用途。

- 功能：執行期監控

此發現項目會通知您 AWS 環境中的 EC2 執行個體或容器上已執行可疑工具。這包括用於執行測試的工具，也稱為後門工具，網絡掃描器和網絡嗅探器。所有這些工具都可以在良性環境中使用，但有惡意意圖的威脅行為者也經常使用。觀察攻擊性的安全工具可能表明相關的 EC2 實例或容器已遭到入侵。

GuardDuty 檢查相關的執行階段活動和前後關聯，以便僅在關聯的活動和前後關聯可能可疑時才產生此發現項目。

執行期代理程式會監控多個資源的事件。若要識別受影響的資源，請在 GuardDuty主控台的發現項目詳細資料中檢視資源類型。

修復建議：

如果此活動不在預期中，即代表您的資源可能已遭入侵。如需詳細資訊，請參閱 修正執行時期監視發現項。

Execution:Runtime/SuspiciousCommand

已在 Amazon EC2 執行個體或容器上執行可疑命令，表示遭到妥協。

預設嚴重性：變數

根據觀察到的惡意病毒碼的影響，此發現項目類型的嚴重性可能是低、中或高。

- 功能：執行期監控

此發現項目會通知您已執行可疑命令，並指出您 AWS 環境中的 Amazon EC2 執行個體或容器已遭到入侵。這表示檔案可能是從可疑來源下載後再執行，或執行中的處理程序會在其命令列中顯示已知的惡意病毒碼。這進一步表明惡意軟件正在系統上運行。

GuardDuty 檢查相關的執行階段活動和前後關聯，以便僅在關聯的活動和前後關聯可能可疑時才產生此發現項目。

執行期代理程式會監控多個資源的事件。若要識別受影響的資源，請在 GuardDuty主控台的發現項目詳細資料中檢視資源類型。

修復建議：

如果此活動不在預期中，即代表您的資源可能已遭入侵。如需詳細資訊，請參閱 修正執行時期監視發現項。

DefenseEvasion:Runtime/SuspiciousCommand

指令已在列出的 Amazon EC2 執行個體或容器上執行，它會嘗試修改或停用 Linux 防禦機制，例如防火牆或基本系統服務。

預設嚴重性：變數

視已修改或停用的防禦機制而定，此發現項目類型的嚴重性可以是「高」、「中」或「低」。

- 功能：執行期監控

此發現項目會通知您已執行嘗試隱藏來自本機系統安全性服務之攻擊的命令。這包括停用 Unix 防火牆、修改本機 IP 資料表、移除crontab項目、停用本機服務或接管LDPreload功能等動作。任何修改都是高度可疑的，並且是潛在的妥協指標。因此，這些機制會偵測或防止系統的進一步危害。

GuardDuty 檢查相關的執行階段活動和前後關聯，以便僅在關聯的活動和前後關聯可能可疑時才產生此發現項目。

執行期代理程式會監控多個資源的事件。若要識別可能遭到入侵的資源，請在 GuardDuty主控台的發現項目詳細資料中檢視資源類型。

修復建議：

如果此活動不在預期中，即代表您的資源可能已遭入侵。如需詳細資訊，請參閱 修正執行時期監視發現項。

DefenseEvasion:Runtime/PtraceAntiDebugging

容器或 Amazon EC2 執行個體中的程序已使用 ptrace 系統呼叫執行反偵錯措施。

預設嚴重性：低

- 功能：執行期監控

此發現顯示，在 Amazon EC2 執行個體或 AWS 環境中的容器上執行的程序已使用 ptrace 系統呼叫搭配選PTRACE_TRACEME項。此活動將導致連接的調試器從正在運行的進程中分離。如果沒有附加調試器，它沒有任何效果。但是，該活動本身引起了懷疑。這可能表示惡意軟體正在系統上執行。惡意軟件經常使用反調試技術來逃避分析，並且可以在運行時檢測到這些技術。

GuardDuty 檢查相關的執行階段活動和前後關聯，以便僅在關聯的活動和前後關聯可能可疑時才產生此發現項目。

執行期代理程式會監控多個資源的事件。若要識別受影響的資源，請在 GuardDuty主控台的發現項目詳細資料中檢視資源類型。

修復建議：

如果此活動不在預期中，即代表您的資源可能已遭入侵。如需詳細資訊，請參閱 修正執行時期監視發現項。

Execution:Runtime/MaliciousFileExecuted

已知的惡意可執行檔案已在 Amazon EC2 執行個體或容器上執行。

預設嚴重性：高

- 功能：執行期監控

此發現項目會通知您已知的惡意可執行檔已在 Amazon EC2 執行個體或 AWS 環境中的容器上執行。這是一個有力的指標，表明實例或容器已被破壞，並且惡意軟件已被執行。

惡意軟件經常使用反調試技術來逃避分析，並且可以在運行時檢測到這些技術。

GuardDuty 檢查相關的執行階段活動和前後關聯，以便僅在關聯的活動和前後關聯可能可疑時才產生此發現項目。

執行期代理程式會監控多個資源的事件。若要識別受影響的資源，請在 GuardDuty主控台的發現項目詳細資料中檢視資源類型。

修復建議：

如果此活動不在預期中，即代表您的資源可能已遭入侵。如需更多詳細資訊，請參閱 修正執行時期監視發現項。

GuardDuty S3 尋找項目類型

以下發現項目特定於 Amazon S3 資源，**S3Bucket**如果資料來源是 S3 的資料事件，或資CloudTrail料來源是CloudTrail 管理事件，**AccessKey**則資源類型將為。問題清單的嚴重性和詳細資訊，依問題清單類型以及與該儲存貯體相關聯的許可而有所不同。

此處列出的調查結果包括用來產生該調查結果類型的資料來源和模型。如需有關資料來源和模型的詳細資訊，請參閱基礎資料來源。

> **Important**
>
> 只有在啟用 S3 保護的情況下，才會產生具有 S3 CloudTrail 資料事件資料來源的發現項目 GuardDuty。在 2020 年 7 月 31 日之後建立的所有帳戶中，預設會啟用 S3 保護。如需有關如何啟用或停用 S3 保護的詳細資訊，請參閱Amazon S3 保護在 Amazon GuardDuty

對於所有 S3Bucket 類型的調查結果，建議您檢查有問題儲存貯體的許可，以及與調查結果涉及之任何使用者的許可，如果活動是非預期的結果，請參閱修復可能遭到入侵的 S3 儲存貯體中詳細說明的修復建議。

主題

- Discovery:S3/AnomalousBehavior
- Discovery:S3/MaliciousIPCaller
- Discovery:S3/MaliciousIPCaller.Custom
- Discovery:S3/TorIPCaller
- Exfiltration:S3/AnomalousBehavior
- Exfiltration:S3/MaliciousIPCaller
- Impact:S3/AnomalousBehavior.Delete
- Impact:S3/AnomalousBehavior.Permission
- Impact:S3/AnomalousBehavior.Write
- Impact:S3/MaliciousIPCaller
- PenTest:S3/KaliLinux
- PenTest:S3/ParrotLinux
- PenTest:S3/PentooLinux
- Policy:S3/AccountBlockPublicAccessDisabled

- Policy:S3/BucketAnonymousAccessGranted
- Policy:S3/BucketBlockPublicAccessDisabled
- Policy:S3/BucketPublicAccessGranted
- Stealth:S3/ServerAccessLoggingDisabled
- UnauthorizedAccess:S3/MaliciousIPCaller.Custom
- UnauthorizedAccess:S3/TorIPCaller

Discovery:S3/AnomalousBehavior

以異常方式調用通常用來探索 S3 物件的 API。

預設嚴重性：低

- 資料來源：S3 的CloudTrail 資料事件

此調查結果會通知您，IAM 實體已調用 S3 API，來探索環境中的 S3 儲存貯體，例如 `ListObjects`。此類活動與攻擊的探索階段相關聯，攻擊者會收集資訊，判斷您的 AWS 環境是否容易受到更廣泛的攻擊。此活動非常可疑，因為 IAM 實體調用 API 的方式並不尋常。例如，沒有先前歷史記錄的 IAM 實體會調用 S3 API，或者 IAM 實體會從不尋常的位置調用 S3 API。

此 API 透過 GuardDuty異常偵測機器學習 (ML) 模型識別為異常狀況。ML 模型會評估帳戶中的所有 API 請求，並識別與對手使用之技術相關聯的異常事件。ML 模型會追蹤 API 請求的各種因素，例如提出請求的使用者、發出請求的位置、請求的特定 API、請求的儲存貯體，以及發出的 API 呼叫次數。對於調用請求的使用者身分而言，如需哪些是不尋常之 API 請求的詳細資訊，請參閱調查結果詳細資訊。

修復建議：

如果此活動對於關聯的主體是非預期的結果，則可能表示憑證已暴露或 S3 許可的限制不夠嚴格。如需詳細資訊，請參閱 修復可能遭到入侵的 S3 儲存貯體。

Discovery:S3/MaliciousIPCaller

常用來探索 AWS 環境中資源的 S3 API 是從已知惡意 IP 位址叫用的。

預設嚴重性：高

- 資料來源：S3 的CloudTrail 資料事件

此調查結果會通知您，已從與已知惡意活動關聯的 IP 地址調用 S3 API 操作。當對手收集有關您環境的資訊時，觀察到的 API 通常與攻擊的發現階段相關聯 AWS 。範例包括 `GetObjectAcl` 和 `ListObjects`。

修復建議：

如果此活動對於關聯的主體是非預期的結果，則可能表示憑證已暴露或 S3 許可的限制不夠嚴格。如需詳細資訊，請參閱 修復可能遭到入侵的 S3 儲存貯體。

Discovery:S3/MaliciousIPCaller.Custom

從自訂威脅清單上的 IP 地址調用的 S3 API。

預設嚴重性：高

- 資料來源：S3 的CloudTrail 資料事件

此調查結果會通知您，已從您上傳的威脅清單上所包含的 IP 地址調用 S3 API (例如 `GetObjectAcl` 或 `ListObjects`)。與此調查結果相關聯的威脅清單會列在調查結果詳細資訊的其他資訊區段中。這類活動與攻擊的探索階段相關聯，攻擊者會在此階段收集資訊，以判斷 AWS 環境是否容易受到更廣泛的攻擊。

修復建議：

如果此活動對於關聯的主體是非預期的結果，則可能表示憑證已暴露或 S3 許可的限制不夠嚴格。如需詳細資訊，請參閱 修復可能遭到入侵的 S3 儲存貯體。

Discovery:S3/TorIPCaller

從 Tor 退出節點的 IP 地址調用 S3 API。

預設嚴重性：中

- 資料來源：S3 的CloudTrail 資料事件

此調查結果會通知您，已從 Tor 退出節點 IP 地址調用 S3 API (例如 `GetObjectAcl` 或 `ListObjects`)。這種類型的活動與攻擊的發現階段相關聯，其中攻擊者正在收集信息以確定您的 AWS 環境是否容易受到更廣泛的攻擊。Tor 是一種啟用匿名通訊的軟體。它會透過一系列網路節點之間的中繼來加密並隨機反彈通訊。最後的 Tor 節點稱為退出節點。這可能表示未經授權存取您的 AWS 資源，意圖隱藏攻擊者的真實身分。

修復建議：

如果此活動對於關聯的主體是非預期的結果，則可能表示憑證已暴露或 S3 許可的限制不夠嚴格。如需詳細資訊，請參閱 修復可能遭到入侵的 S3 儲存貯體。

Exfiltration:S3/AnomalousBehavior

IAM 實體以可疑的方式調用 S3 API。

預設嚴重性：高

- 資料來源：S3 的CloudTrail 資料事件

此調查結果會通知您，IAM 實體正在發出涉及 S3 儲存貯體的 API 呼叫，且此活動與該實體建立的基準不同。此活動中使用的 API 呼叫與攻擊的洩漏階段相關聯，攻擊者會在此階段嘗試收集資料。此活動非常可疑，因為 IAM 實體調用 API 的方式並不尋常。例如，沒有先前歷史記錄的 IAM 實體會調用 S3 API，或者 IAM 實體會從不尋常的位置調用 S3 API。

此 API 透過 GuardDuty異常偵測機器學習 (ML) 模型識別為異常狀況。ML 模型會評估帳戶中的所有 API 請求，並識別與對手使用之技術相關聯的異常事件。ML 模型會追蹤 API 請求的各種因素，例如提出請求的使用者、發出請求的位置、請求的特定 API、請求的儲存貯體，以及發出的 API 呼叫次數。對於調用請求的使用者身分而言，如需哪些是不尋常之 API 請求的詳細資訊，請參閱調查結果詳細資訊。

修復建議：

如果此活動對於關聯的主體是非預期的結果，則可能表示憑證已暴露或 S3 許可的限制不夠嚴格。如需詳細資訊，請參閱 修復可能遭到入侵的 S3 儲存貯體。

Exfiltration:S3/MaliciousIPCaller

常用來從 AWS 環境收集資料的 S3 API 是從已知的惡意 IP 位址叫用的。

預設嚴重性：高

- 資料來源：S3 的CloudTrail 資料事件

此調查結果會通知您，已從與已知惡意活動關聯的 IP 地址調用 S3 API 操作。觀察到的 API 通常與外洩策略有關，其中對手試圖從您的網路收集資料。範例包括 `GetObject` 和 `CopyObject`。

修復建議：

如果此活動對於關聯的主體是非預期的結果，則可能表示憑證已暴露或 S3 許可的限制不夠嚴格。如需詳細資訊，請參閱 修復可能遭到入侵的 S3 儲存貯體。

Impact:S3/AnomalousBehavior.Delete

IAM 實體調用了嘗試以可疑方式刪除資料的 S3 API。

預設嚴重性：高

- 資料來源：S3 的CloudTrail 資料事件

此發現項目會通知您 AWS 環境中的 IAM 實體正在進行涉及 S3 儲存貯體的 API 呼叫，而且此行為與該實體建立的基準不同。此活動中使用的 API 呼叫與嘗試刪除資料的攻擊相關聯。此活動非常可疑，因為 IAM 實體調用 API 的方式並不尋常。例如，沒有先前歷史記錄的 IAM 實體會調用 S3 API，或者 IAM 實體會從不尋常的位置調用 S3 API。

此 API 透過 GuardDuty異常偵測機器學習 (ML) 模型識別為異常狀況。ML 模型會評估帳戶中的所有 API 請求，並識別與對手使用之技術相關聯的異常事件。ML 模型會追蹤 API 請求的各種因素，例如提出請求的使用者、發出請求的位置、請求的特定 API、請求的儲存貯體，以及發出的 API 呼叫次數。對於調用請求的使用者身分而言，如需哪些是不尋常之 API 請求的詳細資訊，請參閱調查結果詳細資訊。

修復建議：

如果此活動對於關聯的主體是非預期的結果，則可能表示憑證已暴露或 S3 許可的限制不夠嚴格。如需詳細資訊，請參閱 修復可能遭到入侵的 S3 儲存貯體。

我們建議您稽核 S3 儲存貯體的內容，以判斷您是否可以還原先前的物件版本。

Impact:S3/AnomalousBehavior.Permission

以異常方式調用通常在設定存取控制清單 (ACL) 許可所用的 API。

預設嚴重性：高

- 資料來源：S3 的CloudTrail 資料事件

此發現項目會通知您 AWS 環境中的 IAM 實體已變更所列 S3 儲存貯體上的儲存貯體政策或 ACL。此變更可能會將您的 S3 儲存貯體公開給所有已驗證的 AWS 使用者。

此 API 透過 GuardDuty異常偵測機器學習 (ML) 模型識別為異常狀況。ML 模型會評估帳戶中的所有 API 請求，並識別與對手使用之技術相關聯的異常事件。ML 模型會追蹤 API 請求的各種因素，例如提出請求的使用者、發出請求的位置、請求的特定 API、請求的儲存貯體，以及發出的 API 呼叫次數。對於調用請求的使用者身分而言，如需哪些是不尋常之 API 請求的詳細資訊，請參閱調查結果詳細資訊。

修復建議：

如果此活動對於關聯的主體是非預期的結果，則可能表示憑證已暴露或 S3 許可的限制不夠嚴格。如需詳細資訊，請參閱 修復可能遭到入侵的 S3 儲存貯體。

我們建議您稽核 S3 儲存貯體的內容，以確保不會以非預期的方式允許公開存取所有物件。

Impact:S3/AnomalousBehavior.Write

IAM 實體調用了嘗試以可疑方式寫入資料的 S3 API。

預設嚴重性：中

- 資料來源：S3 的CloudTrail 資料事件

此發現項目會通知您 AWS 環境中的 IAM 實體正在進行涉及 S3 儲存貯體的 API 呼叫，而且此行為與該實體建立的基準不同。此活動中使用的 API 呼叫與嘗試寫入資料的攻擊相關聯。此活動非常可疑，因為 IAM 實體調用 API 的方式並不尋常。例如，沒有先前歷史記錄的 IAM 實體會調用 S3 API，或者 IAM 實體會從不尋常的位置調用 S3 API。

此 API 透過 GuardDuty異常偵測機器學習 (ML) 模型識別為異常狀況。ML 模型會評估帳戶中的所有 API 請求，並識別與對手使用之技術相關聯的異常事件。ML 模型會追蹤 API 請求的各種因素，例如提

出請求的使用者、發出請求的位置、請求的特定 API、請求的儲存貯體，以及發出的 API 呼叫次數。對於調用請求的使用者身分而言，如需哪些是不尋常之 API 請求的詳細資訊，請參閱調查結果詳細資訊。

修復建議：

如果此活動對於關聯的主體是非預期的結果，則可能表示憑證已暴露或 S3 許可的限制不夠嚴格。如需詳細資訊，請參閱 修復可能遭到入侵的 S3 儲存貯體。

我們建議您稽核 S3 儲存貯體的內容，以確保此 API 呼叫不會寫入惡意或未經授權的資料。

Impact:S3/MaliciousIPCaller

從已知的惡意 IP 位址叫用通常用來竄改 AWS 環境中的資料或程序的 S3 API。

預設嚴重性：高

- 資料來源：S3 的CloudTrail 資料事件

此調查結果會通知您，已從與已知惡意活動關聯的 IP 地址調用 S3 API 操作。觀察到的 API 通常與對手嘗試操縱，中斷或銷毀環境中的數據的影響策略相關聯 AWS 。範例包括 `PutObject` 和 `PutObjectAcl`。

修復建議：

如果此活動對於關聯的主體是非預期的結果，則可能表示憑證已暴露或 S3 許可的限制不夠嚴格。如需詳細資訊，請參閱 修復可能遭到入侵的 S3 儲存貯體。

PenTest:S3/KaliLinux

已從 Kali Linux 機器調用 S3 API。

預設嚴重性：中

- 資料來源：S3 的CloudTrail 資料事件

此發現會通知您執行 Kali Linux 的機器正在使用屬於您 AWS 帳戶的登入資料進行 S3 API 呼叫。您的登入資料可能已被盜用。Kali Linux 是一種安全專業人員所使用的熱門滲透測試工具，以在需要修補的

EC2 執行個體中找出弱點。攻擊者也會使用此工具找出 EC2 組態弱點，並取得您 AWS 環境的未經授權存取權。

修復建議：

如果此活動對於關聯的主體是非預期的結果，則可能表示憑證已暴露或 S3 許可的限制不夠嚴格。如需詳細資訊，請參閱 修復可能遭到入侵的 S3 儲存貯體。

PenTest:S3/ParrotLinux

已從 Parrot Security Linux 機器調用 S3 API。

預設嚴重性：中

- 資料來源：S3 的CloudTrail 資料事件

此發現會通知您執行鸚鵡安全 Linux 的機器正在使用屬於您 AWS 帳戶的憑據進行 S3 API 呼叫。您的登入資料可能已被盜用。Parrot Security Linux 是一種安全專業人員所使用的熱門滲透測試工具，以在需要修補的 EC2 執行個體中找出弱點。攻擊者也會使用此工具來尋找 EC2 組態的弱點，並以未授權的方式存取您的 AWS 環境。

修復建議：

如果此活動對於關聯的主體是非預期的結果，則可能表示憑證已暴露或 S3 許可的限制不夠嚴格。如需詳細資訊，請參閱 修復可能遭到入侵的 S3 儲存貯體。

PenTest:S3/PentooLinux

已從 Pentoo Linux 機器調用 S3 API。

預設嚴重性：中

- 資料來源：S3 的CloudTrail 資料事件

這項發現會通知您執行 Pentoo Linux 的機器正在使用屬於您 AWS 帳戶的登入資料進行 S3 API 呼叫。您的登入資料可能已被盜用。Pentoo Linux 是一種安全專業人員所使用的熱門滲透測試工具，以在需要修補的 EC2 執行個體中找出弱點。攻擊者也會使用此工具找出 EC2 組態弱點，並取得您 AWS 環境的未經授權存取權。

修復建議：

如果此活動對於關聯的主體是非預期的結果，則可能表示憑證已暴露或 S3 許可的限制不夠嚴格。如需詳細資訊，請參閱 修復可能遭到入侵的 S3 儲存貯體。

Policy:S3/AccountBlockPublicAccessDisabled

IAM 實體調用的 API，會用於停用帳戶上的 S3 封鎖公開存取。

預設嚴重性：低

- 資料來源：CloudTrail 管理事件

此調查結果會通知您，Amazon S3 封鎖公開存取已在帳戶層級停用。啟用 S3 封鎖公開存取時，可將其設定為篩選儲存貯體上的政策或存取控制清單 (ACL) 作為安全措施，以防止資料不慎公開曝光。

一般而言，帳戶中的 S3 封鎖公開存取會關閉，以允許公開存取儲存貯體或儲存貯體中的物件。當帳戶停用 S3 封鎖公開存取時，對儲存貯體的存取將由套用至個別儲存貯體的政策、ACL 或儲存貯體層級封鎖公開存取設定所控制。這並不表示儲存貯體是公開共用的，但您應該稽核向儲存貯體套用的政策和 ACL，以確認其提供的是適當的許可層級。

修復建議：

如果此活動對於關聯的主體是非預期的結果，則可能表示憑證已暴露或 S3 許可的限制不夠嚴格。如需詳細資訊，請參閱 修復可能遭到入侵的 S3 儲存貯體。

Policy:S3/BucketAnonymousAccessGranted

IAM 主體已透過變更儲存貯體政策或 ACL，授予 S3 儲存貯體網際網路的存取權限。

預設嚴重性：高

- 資料來源：CloudTrail 管理事件

此調查結果會通知您，列出的 S3 儲存貯體已在網際網路上設為可供公開存取，因為 IAM 實體已變更該儲存貯體上的儲存貯體政策或 ACL。偵測到政策或 ACL 變更後，會使用 Zelkova 支援的自動推理，來判斷儲存貯體是否可公開存取。

> **Note**
>
> 如果儲存貯體的 ACL 或儲存貯體政策設定為明確拒絕或全部拒絕，則此調查結果可能不會反映儲存貯體目前的狀態。此調查結果不會反映可能已為 S3 儲存貯體啟用的任何 S3 封鎖公開存取設定。在這種情況下，調查結果中的 `effectivePermission` 值將標記為 `UNKNOWN`。

修復建議：

如果此活動對於關聯的主體是非預期的結果，則可能表示憑證已暴露或 S3 許可的限制不夠嚴格。如需詳細資訊，請參閱 修復可能遭到入侵的 S3 儲存貯體。

Policy:S3/BucketBlockPublicAccessDisabled

IAM 主體調用的 API，會用於停用儲存貯體上的 S3 封鎖公開存取。

預設嚴重性：低

- 資料來源：CloudTrail 管理事件

此調查結果會通知您，已針對列出的 S3 儲存貯體停用封鎖公開存取。啟用時，S3 封鎖公開存取設定可用於篩選向儲存貯體套用的政策或存取控制清單 (ACL) 作為安全措施，以防止資料不慎公開曝光。

一般而言，儲存貯體上的 S3 封鎖公開存取會關閉，以允許公開存取儲存貯體或儲存貯體中的物件。由於儲存貯體的 S3 封鎖公開存取現已停用，因此套用至此儲存貯體的任何政策或 ACL 都會控制對此儲存貯體的存取。這並不表示儲存貯體是公開共用的，但您應該稽核套用到儲存貯體的政策和 ACL，以確認套用適當的許可。

修復建議：

如果此活動對於關聯的主體是非預期的結果，則可能表示憑證已暴露或 S3 許可的限制不夠嚴格。如需詳細資訊，請參閱 修復可能遭到入侵的 S3 儲存貯體。

Policy:S3/BucketPublicAccessGranted

IAM 主體透過變更儲存貯體政策或 ACL，將 S3 儲存貯體的公 AWS 用存取權授予所有使用者。

預設嚴重性：高

- 資料來源：CloudTrail 管理事件

此發現項目會通知您列出的 S3 儲存貯體已公開給所有已驗證的 AWS 使用者，因為 IAM 實體已變更該 S3 儲存貯體上的儲存貯體政策或 ACL。偵測到政策或 ACL 變更後，會使用 Zelkova 支援的自動推理，來判斷儲存貯體是否可公開存取。

> **Note**
>
> 如果儲存貯體的 ACL 或儲存貯體政策設定為明確拒絕或全部拒絕，則此調查結果可能不會反映儲存貯體目前的狀態。此調查結果不會反映可能已為 S3 儲存貯體啟用的任何 S3 封鎖公開存取設定。在這種情況下，調查結果中的 `effectivePermission` 值將標記為 `UNKNOWN`。

修復建議：

如果此活動對於關聯的主體是非預期的結果，則可能表示憑證已暴露或 S3 許可的限制不夠嚴格。如需詳細資訊，請參閱 修復可能遭到入侵的 S3 儲存貯體。

Stealth:S3/ServerAccessLoggingDisabled

儲存貯體的 S3 伺服器存取記錄已停用。

預設嚴重性：低

- 資料來源：CloudTrail 管理事件

此發現項目會通知您 AWS 環境中儲存貯體的 S3 伺服器存取記錄已停用。如果停用，則不會為任何嘗試存取已識別的 S3 儲存貯體建立 Web 請求日誌，但仍會追蹤儲存貯體的 S3 管理 API 呼叫 DeleteBucket，例如。如果透過 CloudTrail 此儲存貯體啟用 S3 資料事件記錄，則仍會追蹤儲存貯體內物件的 Web 請求。停用記錄是未經授權的使用者用來逃避偵測的技術。若要進一步了解 S3 日誌，請參閱 S3 伺服器存取記錄和 S3 記錄選項。

修復建議：

如果此活動對於關聯的主體是非預期的結果，則可能表示憑證已暴露或 S3 許可的限制不夠嚴格。如需詳細資訊，請參閱 修復可能遭到入侵的 S3 儲存貯體。

UnauthorizedAccess:S3/MaliciousIPCaller.Custom

從自訂威脅清單上的 IP 地址調用的 S3 API。

預設嚴重性：高

- 資料來源：S3 的CloudTrail 資料事件

此調查結果會通知您，已從您上傳的威脅清單上所包含的 IP 地址調用 S3 API 操作 (例如 `PutObject` 或 `PutObjectAcl`)。與此調查結果相關聯的威脅清單會列在調查結果詳細資訊的其他資訊區段中。

修復建議：

如果此活動對於關聯的主體是非預期的結果，則可能表示憑證已暴露或 S3 許可的限制不夠嚴格。如需詳細資訊，請參閱 修復可能遭到入侵的 S3 儲存貯體。

UnauthorizedAccess:S3/TorIPCaller

從 Tor 退出節點的 IP 地址調用 S3 API。

預設嚴重性：高

- 資料來源：S3 的CloudTrail 資料事件

此調查結果會通知您，已從 Tor 退出節點 IP 地址調用 S3 API 操作 (例如 `PutObject` 或 `PutObjectAcl`)。Tor 是一種啟用匿名通訊的軟體。它會透過一系列網路節點之間的中繼來加密並隨機反彈通訊。最後的 Tor 節點稱為退出節點。此發現可表示未經授權存取您的 AWS 資源，意圖隱藏攻擊者的真實身分。

修復建議：

如果此活動對於關聯的主體是非預期的結果，則可能表示憑證已暴露或 S3 許可的限制不夠嚴格。如需更多詳細資訊，請參閱 修復可能遭到入侵的 S3 儲存貯體。

已淘汰的調查結果類型

調查結果是一種包含 GuardDuty 所發現潛在安全問題詳細資訊的通知。如需有關 GuardDuty 調查結果類型重要變更的詳細資訊，包括新增或淘汰的調查結果類型，請參閱Amazon 的文檔歷史 GuardDuty。

下列調查結果類型已淘汰，GuardDuty 不再產生這類調查結果。

> **Important**
>
> 您無法重新啟動已淘汰的 GuardDuty 調查結果類型。

主題

Exfiltration:S3/ObjectRead.Unusual

IAM 實體以可疑的方式調用 S3 API。

預設嚴重性：中*

> **Note**
>
> 此調查結果的預設嚴重性為「中」。不過，如果使用在執行個體上建立的臨時 AWS 憑證來調用 API，則調查結果的嚴重性為「高」。

- 資料來源：適用於 S3 的 CloudTrail 資料事件

此調查結果會通知您，AWS 環境中的 IAM 實體正在發出涉及 S3 儲存貯體的 API 呼叫，且與該實體建立的基準不同。此活動中使用的 API 呼叫與攻擊的洩漏階段相關聯，攻擊者會在此階段嘗試收集資料。此活動非常可疑，因為 IAM 實體調用 API 的方式並不尋常。例如，此 IAM 實體先前沒有調用此類 API 的歷史記錄，或者 API 的調用是從不尋常的位置進行。

修復建議：

如果此活動對於關聯的主體是非預期的結果，則可能表示憑證已暴露或 S3 許可的限制不夠嚴格。如需詳細資訊，請參閱修復可能遭到入侵的 S3 儲存貯體。

Impact:S3/PermissionsModification.Unusual

IAM 實體調用 API 來修改一或多個 S3 資源的許可。

預設嚴重性：中*

> **Note**
>
> 此調查結果的預設嚴重性為「中」。不過，如果使用在執行個體上建立的臨時 AWS 憑證來調用 API，則調查結果的嚴重性為「高」。

此調查結果會通知您，IAM 實體正在進行 API 呼叫，這類呼叫旨在修改 AWS 環境中一個或多個儲存貯體或物件的許可。攻擊者可能會執行此動作，以允許在帳戶外共用資訊。此活動非常可疑，因為 IAM 實體調用 API 的方式並不尋常。例如，此 IAM 實體先前沒有調用此類 API 的歷史記錄，或者 API 的調用是從不尋常的位置進行。

修復建議：

如果此活動對於關聯的主體是非預期的結果，則可能表示憑證已暴露或 S3 許可的限制不夠嚴格。如需詳細資訊，請參閱修復可能遭到入侵的 S3 儲存貯體。

Impact:S3/ObjectDelete.Unusual

IAM 實體調用的是刪除 S3 儲存貯體中資料所用的 API。

預設嚴重性：中*

> **Note**
>
> 此調查結果的預設嚴重性為「中」。不過，如果使用在執行個體上建立的臨時 AWS 憑證來調用 API，則調查結果的嚴重性為「高」。

此調查結果會通知您，AWS 環境中的特定 IAM 實體正在進行 API 呼叫，此類呼叫旨在透過刪除儲存貯體本身來刪除所列 S3 儲存貯體中的資料。此活動非常可疑，因為 IAM 實體調用 API 的方式並不尋常。例如，此 IAM 實體先前沒有調用此類 API 的歷史記錄，或者 API 的調用是從不尋常的位置進行。

修復建議：

如果此活動對於關聯的主體是非預期的結果，則可能表示憑證已暴露或 S3 許可的限制不夠嚴格。如需詳細資訊，請參閱修復可能遭到入侵的 S3 儲存貯體。

Discovery:S3/BucketEnumeration.Unusual

IAM 實體調用探索網路中 S3 儲存貯體所用的 S3 API。

預設嚴重性：中*

> **Note**
>
> 此調查結果的預設嚴重性為「中」。不過，如果使用在執行個體上建立的臨時 AWS 憑證來調用 API，則調查結果的嚴重性為「高」。

此調查結果會通知您，IAM 實體已調用 S3 API，來探索環境中的 S3 儲存貯體，例如 `ListBuckets`。這類活動與攻擊的探索階段相關聯，攻擊者會在此階段收集資訊，以判斷 AWS 環境是否容易受到更廣泛的攻擊。此活動非常可疑，因為 IAM 實體調用 API 的方式並不尋常。例如，此 IAM 實體先前沒有調用此類 API 的歷史記錄，或者 API 的調用是從不尋常的位置進行。

修復建議：

如果此活動對於關聯的主體是非預期的結果，則可能表示憑證已暴露或 S3 許可的限制不夠嚴格。如需詳細資訊，請參閱修復可能遭到入侵的 S3 儲存貯體。

Persistence:IAMUser/NetworkPermissions

IAM 實體調用常用的 API，以變更 AWS 帳戶中的安全群組、路由和 ACL 的網路存取許可。

預設嚴重性：中*

> **Note**
>
> 此調查結果的預設嚴重性為「中」。不過，如果使用在執行個體上建立的臨時 AWS 憑證來調用 API，則調查結果的嚴重性為「高」。

此調查結果表示 AWS 環境中的特定主體 (AWS 帳戶根使用者、IAM 角色或使用者) 正在展現與既有基準不同的行為。此委託人之前沒有呼叫此 API 的歷程記錄。

在可疑情況下變更網路組態設定時，例如主體調用 `CreateSecurityGroup` API，但先前沒有這樣做的歷史記錄時，就會觸發此調查結果。攻擊者通常會嘗試變更安全群組，並在各種連接埠上允許特定傳入流量，以改進他們存取 EC2 執行個體的能力。

修復建議：

如果此活動為非預期活動，即代表您的憑證可能已遭入侵。如需詳細資訊，請參閱修復可能遭到破壞 AWS 的認證。

Persistence:IAMUser/ResourcePermissions

主體調用的 API，通常用於變更 AWS 帳戶 中各種資源的安全性存取政策。

預設嚴重性：中*

> **Note**
>
> 此調查結果的預設嚴重性為「中」。不過，如果使用在執行個體上建立的臨時 AWS 憑證來調用 API，則調查結果的嚴重性為「高」。

此調查結果表示 AWS 環境中的特定主體 (AWS 帳戶根使用者、IAM 角色或使用者) 正在展現與既有基準不同的行為。此委託人之前沒有呼叫此 API 的歷程記錄。

當偵測到連接至 AWS 資源的政策或許可有變更時，例如 AWS 環境中的主體調用 `PutBucketPolicy` API，但先前沒有這樣做的歷史記錄時，就會觸發此調查結果。有些服務 (例如 Amazon S3) 可支援授予一個或以上的主體存取資源的資源連接許可。攻擊者可以透過竊取的憑證，變更連接到資源的政策，以獲得對該資源的存取權限。

修復建議：

如果此活動為非預期活動，即代表您的憑證可能已遭入侵。如需詳細資訊，請參閱修復可能遭到破壞 AWS 的認證。

Persistence:IAMUser/UserPermissions

主體調用的 API，通常用於新增、修改或刪除 AWS 帳戶中的 IAM 使用者、群組或政策。

預設嚴重性：中*

> **Note**
>
> 此調查結果的預設嚴重性為「中」。不過，如果使用在執行個體上建立的臨時 AWS 憑證來調用 API，則調查結果的嚴重性為「高」。

此調查結果表示 AWS 環境中的特定主體 (AWS 帳戶根使用者、IAM 角色或使用者) 正在展現與既有基準不同的行為。此委託人之前沒有呼叫此 API 的歷程記錄。

此調查結果是由 AWS 環境中與使用者相關許可的可疑變更所觸發，例如當 AWS 環境中的主體調用 `AttachUserPolicy` API，但先前沒有這樣做的歷史記錄時。攻擊者可能會使用竊取的憑證來新建使用者、為現有使用者新增存取政策，或建立存取金鑰以最大限度地提高其對帳戶的存取權限，即使原始

存取點關閉也是如此。例如，帳戶擁有者可能會注意到特定 IAM 使用者或密碼遭竊，並將其從帳戶中刪除。不過，他們可能不會刪除以詐欺手段建立之管理員主體所建立的其他使用者，而導致攻擊者仍可以存取其 AWS 帳戶。

修復建議：

如果此活動為非預期活動，即代表您的憑證可能已遭入侵。如需詳細資訊，請參閱修復可能遭到破壞 AWS 的認證。

PrivilegeEscalation:IAMUser/AdministrativePermissions

委託人嘗試將非常寬鬆的政策指派給自己。

預設嚴重性：低*

> **Note**
>
> 如果嘗試權限提升失敗，此調查結果的嚴重性為「低」，如果嘗試提升權限成功，則為嚴重性為「中」。

此調查結果指出 AWS 環境中特定 IAM 實體所展現的行為很可能是權限提升攻擊。當 IAM 使用者或角色嘗試將非常寬鬆的政策指派給自己時，將會觸發此調查結果。如果有爭議的使用者或角色不應取得管理權限，表示使用者的登入資料遭竊，或未正確設定該角色的許可。

攻擊者將會使用竊取的憑證來新建使用者、為現有使用者新增存取政策，或建立存取金鑰以最大限度地提高其對帳戶的存取權限，即使原始存取點關閉也是如此。例如，該帳戶的擁有者可能會注意到特定 IAM 使用者登入憑證遭竊，並將其從帳戶中刪除，但可能不會刪除以詐欺手段建立之管理員主體所建立的其他使用者，因而導致攻擊者仍可存取其 AWS 帳戶。

修復建議：

如果此活動為非預期活動，即代表您的憑證可能已遭入侵。如需詳細資訊，請參閱修復可能遭到破壞 AWS 的認證。

Recon:IAMUser/NetworkPermissions

主體調用常用的 API，以變更 AWS 帳戶中的安全群組、路由和 ACL 的網路存取許可。

預設嚴重性：中*

> **Note**
>
> 此調查結果的預設嚴重性為「中」。不過，如果使用在執行個體上建立的臨時 AWS 憑證來調用 API，則調查結果的嚴重性為「高」。

此調查結果表示 AWS 環境中的特定主體 (AWS 帳戶根使用者、IAM 角色或使用者) 正在展現與既有基準不同的行為。此委託人之前沒有呼叫此 API 的歷程記錄。

此調查結果會在可疑情況下探測 AWS 帳戶中的資源存取許可時被觸發。例如，如果主體在調用 `DescribeInstances` API 時先前沒有這樣做的歷史記錄。攻擊者可能會使用遭竊的憑證，以對 AWS 資源進行此類型的偵察，以便找出更有價值的憑證或判斷其已擁有憑證的功能。

修復建議：

如果此活動為非預期活動，即代表您的憑證可能已遭入侵。如需詳細資訊，請參閱修復可能遭到破壞 AWS 的認證。

Recon:IAMUser/ResourcePermissions

主體調用的 API，通常用於變更 AWS 帳戶中各種資源的安全性存取政策。

預設嚴重性：中*

> **Note**
>
> 此調查結果的預設嚴重性為「中」。不過，如果使用在執行個體上建立的臨時 AWS 憑證來調用 API，則調查結果的嚴重性為「高」。

此調查結果表示 AWS 環境中的特定主體 (AWS 帳戶根使用者、IAM 角色或使用者) 正在展現與既有基準不同的行為。此委託人之前沒有呼叫此 API 的歷程記錄。

此調查結果會在可疑情況下探測 AWS 帳戶中的資源存取許可時被觸發。例如，如果主體在調用 `DescribeInstances` API 時先前沒有這樣做的歷史記錄。攻擊者可能會使用遭竊的憑證，以對 AWS 資源進行此類型的偵察，以便找出更有價值的憑證或判斷其已擁有憑證的功能。

修復建議：

如果此活動為非預期活動，即代表您的憑證可能已遭入侵。如需詳細資訊，請參閱修復可能遭到破壞 AWS 的認證。

Recon:IAMUser/UserPermissions

主體調用的 API，通常用於新增、修改或刪除 AWS 帳戶中的 IAM 使用者、群組或政策。

預設嚴重性：中*

> **Note**
>
> 此調查結果的預設嚴重性為「中」。不過，如果使用在執行個體上建立的臨時 AWS 憑證來調用 API，則調查結果的嚴重性為「高」。

此調查結果會在可疑情況下探測 AWS 環境中的使用者許可時被觸發。例如，如果主體 (AWS 帳戶根使用者、IAM 角色或 IAM 使用者) 在調用 `ListInstanceProfilesForRole` API 時先前沒有這樣做的歷史記錄。攻擊者可能會使用遭竊的憑證，以對 AWS 資源進行此類型的偵察，以便找出更有價值的憑證或判斷其已擁有憑證的功能。

此調查結果表示 AWS 環境中的特定主體正在展現與既有基準不同的行為。此委託人之前沒有使用此方法叫用 API 的歷程記錄。

修復建議：

如果此活動為非預期活動，即代表您的憑證可能已遭入侵。如需詳細資訊，請參閱修復可能遭到破壞 AWS 的認證。

ResourceConsumption:IAMUser/ComputeResources

委託人叫用常用於啟動運算資源 (例如 EC2 執行個體) 的 API。

預設嚴重性：中*

> **Note**
>
> 此調查結果的預設嚴重性為「中」。不過，如果使用在執行個體上建立的臨時 AWS 憑證來調用 API，則調查結果的嚴重性為「高」。

此調查結果會在可疑情況下啟動 AWS 環境中所列帳戶中的 EC2 執行個體時被觸發。此調查結果表示 AWS 環境中的特定主體所呈現的行為與建立的基準不同；例如，如果主體 (AWS 帳戶根使用者、IAM 角色或 IAM 使用者) 在調用 `RunInstances` API 時先前沒有這樣做的歷史記錄。這可能表示攻擊者使用了遭竊的登入資料來竊取運算時間 (可能用於加密貨幣採礦或密碼破解)。其也可以表示攻擊者在 AWS 環境中使用了 EC2 執行個體及其憑證，來維持對您帳戶的存取權限。

修復建議：

如果此活動為非預期活動，即代表您的憑證可能已遭入侵。如需詳細資訊，請參閱修復可能遭到破壞 AWS 的認證。

Stealth:IAMUser/LoggingConfigurationModified

主體調用的 API，常用於停止 CloudTrail 記錄、刪除現有日誌，以及以其他方式消除 AWS 帳戶中的活動追蹤。

預設嚴重性：中*

> **Note**
>
> 此調查結果的預設嚴重性為「中」。不過，如果使用在執行個體上建立的臨時 AWS 憑證來調用 API，則調查結果的嚴重性為「高」。

此調查結果會在可疑情況下修改您環境中所列 AWS 帳戶中的記錄組態時被觸發。此調查結果會通知您，AWS 環境中的特定主體所呈現的行為與建立的基準不同；例如，如果主體 (AWS 帳戶根使用者、IAM 角色或 IAM 使用者) 在調用 `StopLogging` API 時先前沒有這樣做的歷史記錄。這可能表示攻擊者正試圖透過消除他們的任何活動痕跡來掩蓋其踪跡。

修復建議：

如果此活動為非預期活動，即代表您的憑證可能已遭入侵。如需詳細資訊，請參閱修復可能遭到破壞 AWS 的認證。

UnauthorizedAccess:IAMUser/ConsoleLogin

已在 AWS 帳戶中觀察到主體在進行不尋常的主控台登入。

預設嚴重性：中*

> **Note**
>
> 此調查結果的預設嚴重性為「中」。不過，如果使用在執行個體上建立的臨時 AWS 憑證來調用 API，則調查結果的嚴重性為「高」。

在可疑情況下偵測到主控台登入時都會觸發此問題清單。例如，如果一個委託人沒有之前的歷程記錄，則會從一個從未使用過的用戶端或不尋常的位置呼叫 ConsoleLogin API。這可能表示用於存取 AWS 帳戶的憑證已遭竊，或者某個有效使用者正在以無效或較不安全的方式存取該帳戶 (例如，未透過批准的 VPN 進行存取)。

此調查結果會通知您，AWS 環境中的特定主體正在展現與既有基準不同的行為。此委託人之前沒有從此特定位置使用此用戶端應用程式登入活動的歷程記錄。

修復建議：

如果此活動為非預期活動，即代表您的憑證可能已遭入侵。如需詳細資訊，請參閱修復可能遭到破壞 AWS 的認證。

UnauthorizedAccess:EC2/TorIPCaller

您的 EC2 執行個體正在從一個 Tor 退出節點接收傳入連線。

預設嚴重性：中

此調查結果會通知您，AWS 環境中的 EC2 執行個體正在接收從 Tor 退出節點傳入的連線。Tor 是一種啟用匿名通訊的軟體。它會透過一系列網路節點之間的中繼來加密並隨機反彈通訊。最後的 Tor 節點稱為退出節點。此調查結果可能表示您的 AWS 資源有未經授權的存取，目的是隱藏攻擊者的真實身分。

修復建議：

如果此活動為非預期活動，即代表您的執行個體可能已遭入侵。如需詳細資訊，請參閱修復可能遭到入侵的 Amazon EC2 執行個體。

Backdoor:EC2/XORDDOS

EC2 執行個體嘗試與 XOR DDoS 惡意軟體相關聯的 IP 地址進行通訊。

預設嚴重性：高

此調查結果會通知您，AWS 環境中的 EC2 執行個體正嘗試與 XOR DDoS 惡意軟體相關聯的 IP 地址進行通訊。此 EC2 執行個體可能已遭到盜用。XOR DDoS 是 Trojan (木馬程式) 惡意軟體，會劫持 Linux 系統。為了取得系統存取權限，它會啟動暴力破解攻擊，以找出 Linux 上 Secure Shell (SSH) 服務的密碼。取得 SSH 憑證並成功登入後，其會利用根使用者權限執行指令碼，來下載和安裝 XOR DDoS。接著此惡意軟體就會成為殭屍網路的一部分，用來對其他目標發動分散式阻斷服務 (DDoS) 攻擊。

修復建議：

如果此活動為非預期活動，即代表您的執行個體可能已遭入侵。如需詳細資訊，請參閱修復可能遭到入侵的 Amazon EC2 執行個體。

Behavior:IAMUser/InstanceLaunchUnusual

使用者啟動了不尋常的 EC2 執行個體類型。

預設嚴重性：高

此調查結果會通知您，AWS 環境中的特定使用者正在展現與既有基準不同的行為。此使用者沒有啟動此 EC2 執行個體類型的歷史記錄。登入憑證可能已遭盜用。

修復建議：

如果此活動為非預期活動，即代表您的憑證可能已遭入侵。如需詳細資訊，請參閱修復可能遭到破壞 AWS 的認證。

CryptoCurrency:EC2/BitcoinTool.A

EC2 執行個體正在與 Bitcoin (比特幣) 採礦區通訊。

預設嚴重性：高

此調查結果會通知您，AWS 環境中的 EC2 執行個體正在與 Bitcoin (比特幣) 採礦區通訊。在加密貨幣採礦的領域中，採礦池是礦工透過網路分享處理能力來匯集資源的集區，並根據他們解決區塊時貢獻的工作量來分割獎勵。除非您使用此 EC2 執行個體來挖掘 Bitcoin (比特幣)，否則您的 EC2 執行個體可能會被入侵。

修復建議：

如果此活動為非預期活動，即代表您的執行個體可能已遭入侵。如需詳細資訊，請參閱修復可能遭到入侵的 Amazon EC2 執行個體。

UnauthorizedAccess:IAMUser/UnusualASNCaller

API 已被一個不尋常網路的 IP 地址呼叫。

預設嚴重性：高

此問題清單會通知您不尋常網路中的 IP 地址已呼叫了特定活動。在所描述使用者的 AWS 使用歷史記錄中從未觀察到該網路。此活動可以包括主控台登入、嘗試啟動 EC2 執行個體、新建 IAM 使用者、修改 AWS 權限等。這可能表示您的 AWS 資源有未經授權的存取。

修復建議：

如果此活動為非預期活動，即代表您的憑證可能已遭入侵。如需詳細資訊，請參閱修復可能遭到破壞 AWS 的認證。

依資源類型分類的調查結果

下列頁面會依與 GuardDuty 搜尋結果相關聯的資源類型分類：

- EC2 調查結果類型
- 執行階段監視尋找項
- IAM 調查結果類型
- EKS 稽核記錄尋找類型
- Lambda 保護調查結果類型
- 惡意軟體防護調查結果類型
- RDS 保護調查結果類型
- S3 調查結果類型

調查結果表

下表展示了依基礎資料來源或功能 (如適用) 排序的所有作用中調查結果類型。下列某些調查結果類型可能具有變數嚴重性，以星號 (*) 表示。如需有關調查結果類型之變數嚴重性的詳細資訊，請檢視該調查結果類型的詳細說明。

調查結果類型	資源類型	基礎資料來源/功能	調查結果的嚴重性
Discovery:S3/AnomalousBehavior	Amazon S3	CloudTrail S3 的資料事件	低
Discovery:S3/MaliciousIPCaller	Amazon S3	CloudTrail S3 的資料事件	高
Discovery:S3/MaliciousIPCaller.Custom	Amazon S3	CloudTrail S3 的資料事件	高
Discovery:S3/TorIPCaller	Amazon S3	CloudTrail S3 的資料事件	中
Exfiltration:S3/AnomalousBehavior	Amazon S3	CloudTrail S3 的資料事件	高
Exfiltration:S3/MaliciousIPCaller	Amazon S3	CloudTrail S3 的資料事件	高
Impact:S3/AnomalousBehavior.Delete	Amazon S3	CloudTrail S3 的資料事件	高
Impact:S3/AnomalousBehavior.Permission	Amazon S3	CloudTrail S3 的資料事件	高
Impact:S3/Anomalou	Amazon S3	CloudTrail S3 的資料事件	中

調查結果類型	資源類型	基礎資料來源/功能	調查結果的嚴重性
sBehavior.Write			
Impact:S3/MaliciousIPCaller	Amazon S3	CloudTrail S3 的資料事件	高
PenTest:S3/KaliLinux	Amazon S3	CloudTrail S3 的資料事件	中
PenTest:S3/ParrotLinux	Amazon S3	CloudTrail S3 的資料事件	中
PenTest:S3/PentooLinux	Amazon S3	CloudTrail S3 的資料事件	中
UnauthorizedAccess:S3/TorIPCaller	Amazon S3	CloudTrail S3 的資料事件	高
UnauthorizedAccess:S3/MaliciousIPCaller.Custom	Amazon S3	CloudTrail S3 的資料事件	高
CredentialAccess:IAMUser/AnomalousBehavior	IAM	CloudTrail 管理事件	中
DefenseEvasion:IAMUser/AnomalousBehavior	IAM	CloudTrail 管理事件	中

調查結果類型	資源類型	基礎資料來源/功能	調查結果的嚴重性
Discovery:IAMUser/AnomalousBehavior	IAM	CloudTrail 管理事件	低
Exfiltration:IAMUser/AnomalousBehavior	IAM	CloudTrail 管理事件	高
Impact:IAMUser/AnomalousBehavior	IAM	CloudTrail 管理事件	高
InitialAccess:IAMUser/AnomalousBehavior	IAM	CloudTrail 管理事件	中
PenTest:IAMUser/KaliLinux	IAM	CloudTrail 管理事件	中
PenTest:IAMUser/ParrotLinux	IAM	CloudTrail 管理事件	中
PenTest:IAMUser/PentooLinux	IAM	CloudTrail 管理事件	中

調查結果類型	資源類型	基礎資料來源/功能	調查結果的嚴重性
Persistence:IAMUser/AnomalousBehavior	IAM	CloudTrail 管理事件	中
Stealth:IAMUser/PasswordPolicyChange	IAM	CloudTrail 管理事件	低*
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS	IAM	CloudTrail 管理事件	高*
Policy:S3/AccountBlockPublicAccessDisabled	Amazon S3	CloudTrail 管理事件	低
Policy:S3/BucketAnonymousAccessGranted	Amazon S3	CloudTrail 管理事件	高
Policy:S3/BucketBlockPublicAccessDisabled	Amazon S3	CloudTrail 管理事件	低

調查結果類型	資源類型	基礎資料來源/功能	調查結果的嚴重性
Policy:S3/BucketPublicAccessGranted	Amazon S3	CloudTrail 管理事件	高
PrivilegeEscalation:IAMUser/AnomalousBehavior	IAM	CloudTrail 管理事件	中
Recon:IAMUser/MaliciousIPCaller	IAM	CloudTrail 管理事件	中
Recon:IAMUser/MaliciousIPCaller.Custom	IAM	CloudTrail 管理事件	中
Recon:IAMUser/TorIPCaller	IAM	CloudTrail 管理事件	中
Stealth:IAMUser/CloudTrailLoggingDisabled	IAM	CloudTrail 管理事件	低
Stealth:S3/ServerAccessLoggingDisabled	Amazon S3	CloudTrail 管理事件	低

調查結果類型	資源類型	基礎資料來源/功能	調查結果的嚴重性
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	IAM	CloudTrail 管理事件	中
UnauthorizedAccess:IAMUser/MaliciousIPCaller	IAM	CloudTrail 管理事件	中
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	IAM	CloudTrail 管理事件	中
UnauthorizedAccess:IAMUser/TorIPCaller	IAM	CloudTrail 管理事件	中
Policy:IAMUser/RootCredentialUsage	IAM	CloudTrail S3 的管理事件或 CloudTrail 資料事件	低

調查結果類型	資源類型	基礎資料來源/功能	調查結果的嚴重性
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	IAM	CloudTrail S3 的管理事件或 CloudTrail 資料事件	高
Backdoor:EC2/C&CActivity.B!DNS	Amazon EC2	DNS 日誌	高
CryptoCurrency:EC2/BitcoinTool.B!DNS	Amazon EC2	DNS 日誌	高
Impact:EC2/AbusedDomainRequest.Reputation	Amazon EC2	DNS 日誌	中
Impact:EC2/BitcoinDomainRequest.Reputation	Amazon EC2	DNS 日誌	高
Impact:EC2/MaliciousDomainRequest.Reputation	Amazon EC2	DNS 日誌	高

調查結果類型	資源類型	基礎資料來源/功能	調查結果的嚴重性
Impact:EC2/SuspiciousDomainRequest.Reputation	Amazon EC2	DNS 日誌	低
Trojan:EC2/BlackholeTraffic!DNS	Amazon EC2	DNS 日誌	中
Trojan:EC2/DGADomainRequest.B	Amazon EC2	DNS 日誌	高
Trojan:EC2/DGADomainRequest.C!DNS	Amazon EC2	DNS 日誌	高
Trojan:EC2/DNSDataExfiltration	Amazon EC2	DNS 日誌	高
Trojan:EC2/DriveBySourceTraffic!DNS	Amazon EC2	DNS 日誌	高
Trojan:EC2/DropPoint!DNS	Amazon EC2	DNS 日誌	中
Trojan:EC2/PhishingDomainRequest!DNS	Amazon EC2	DNS 日誌	高

調查結果類型	資源類型	基礎資料來源/功能	調查結果的嚴重性
UnauthorizedAccess:EC2/MetadataDNSRebind	Amazon EC2	DNS 日誌	高
Execution:Container/MaliciousFile	容器	EBS 惡意軟體防護	根據偵測到的安全威脅而異
Execution:Container/SuspiciousFile	容器	EBS 惡意軟體防護	根據偵測到的安全威脅而異
Execution:EC2/MaliciousFile	EC2	EBS 惡意軟體防護	根據偵測到的安全威脅而異
Execution:EC2/SuspiciousFile	EC2	EBS 惡意軟體防護	根據偵測到的安全威脅而異
Execution:ECS/MaliciousFile	ECS	EBS 惡意軟體防護	根據偵測到的安全威脅而異
Execution:ECS/SuspiciousFile	ECS	EBS 惡意軟體防護	根據偵測到的安全威脅而異
Execution:Kubernetes/MaliciousFile	Kubernetes	EBS 惡意軟體防護	根據偵測到的安全威脅而異
Execution:Kubernetes/SuspiciousFile	Kubernetes	EBS 惡意軟體防護	根據偵測到的安全威脅而異

調查結果類型	資源類型	基礎資料來源/功能	調查結果的嚴重性
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed	Kubernetes	EKS 稽核日誌	中
CredentialAccess:Kubernetes/MaliciousIPCaller	Kubernetes	EKS 稽核日誌	高
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKS 稽核日誌	高
CredentialAccess:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKS 稽核日誌	高
CredentialAccess:Kubernetes/TorIPCaller	Kubernetes	EKS 稽核日誌	高

調查結果類型	資源類型	基礎資料來源/功能	調查結果的嚴重性
DefenseEvasion:Kubernetes/MaliciousIPCaller	Kubernetes	EKS 稽核日誌	高
DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKS 稽核日誌	高
DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKS 稽核日誌	高
DefenseEvasion:Kubernetes/TorIPCaller	Kubernetes	EKS 稽核日誌	高
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	Kubernetes	EKS 稽核日誌	低
Discovery:Kubernetes/MaliciousIPCaller	Kubernetes	EKS 稽核日誌	中

調查結果類型	資源類型	基礎資料來源/功能	調查結果的嚴重性
Discovery:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKS 稽核日誌	中
Discovery:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKS 稽核日誌	中
Discovery:Kubernetes/TorIPCaller	Kubernetes	EKS 稽核日誌	中
Execution:Kubernetes/ExecInKubeSystemPod	Kubernetes	EKS 稽核日誌	中
Execution:Kubernetes/AnomalousBehavior.ExecInPod	Kubernetes	EKS 稽核日誌	中
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	Kubernetes	EKS 稽核日誌	低

調查結果類型	資源類型	基礎資料來源/功能	調查結果的嚴重性
Impact:Kubernetes/MaliciousIPCaller	Kubernetes	EKS 稽核日誌	高
Impact:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKS 稽核日誌	高
Impact:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKS 稽核日誌	高
Impact:Kubernetes/TorIPCaller	Kubernetes	EKS 稽核日誌	高
Persistence:Kubernetes/ContainerWithSensitiveMount	Kubernetes	EKS 稽核日誌	中
Persistence:Kubernetes/MaliciousIPCaller	Kubernetes	EKS 稽核日誌	中
Persistence:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKS 稽核日誌	中

調查結果類型	資源類型	基礎資料來源/功能	調查結果的嚴重性
Persistence:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKS 稽核日誌	高
Persistence:Kubernetes/TorIPCaller	Kubernetes	EKS 稽核日誌	中
Policy:Kubernetes/AdminAccessToDefaultServiceAccount	Kubernetes	EKS 稽核日誌	高
Policy:Kubernetes/AnonymousAccessGranted	Kubernetes	EKS 稽核日誌	高
Policy:Kubernetes/KubeflowDashboardExposed	Kubernetes	EKS 稽核日誌	中
Policy:Kubernetes/ExposedDashboard	Kubernetes	EKS 稽核日誌	中

調查結果類型	資源類型	基礎資料來源/功能	調查結果的嚴重性
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated	Kubernetes	EKS 稽核日誌	中*
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	Kubernetes	EKS 稽核日誌	低
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount	Kubernetes	EKS 稽核日誌	高

調查結果類型	資源類型	基礎資料來源/功能	調查結果的嚴重性
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer	Kubernetes	EKS 稽核日誌	高
PrivilegeEscalation:Kubernetes/PrivilegedContainer	Kubernetes	EKS 稽核日誌	中
Backdoor:Lambda/C&CActivity.B	Lambda	Lambda 網路活動監控	高
CryptoCurrency:Lambda/BitcoinTool.B	Lambda	Lambda 網路活動監控	高
Trojan:Lambda/BlackholeTraffic	Lambda	Lambda 網路活動監控	中
Trojan:Lambda/DropPoint	Lambda	Lambda 網路活動監控	中

調查結果類型	資源類型	基礎資料來源/功能	調查結果的嚴重性
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom	Lambda	Lambda 網路活動監控	中
UnauthorizedAccess:Lambda/TorClient	Lambda	Lambda 網路活動監控	高
UnauthorizedAccess:Lambda/TorRelay	Lambda	Lambda 網路活動監控	高
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	支援的 Amazon Aurora 資料庫	RDS 登入活動監控	低
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	支援的 Amazon Aurora 資料庫	RDS 登入活動監控	高

調查結果類型	資源類型	基礎資料來源/功能	調查結果的嚴重性
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	支援的 Amazon Aurora 資料庫	RDS 登入活動監控	變數*
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	支援的 Amazon Aurora 資料庫	RDS 登入活動監控	中
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	支援的 Amazon Aurora 資料庫	RDS 登入活動監控	高
CredentialAccess:RDS/TorIPCaller.FailedLogin	支援的 Amazon Aurora 資料庫	RDS 登入活動監控	中
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	支援的 Amazon Aurora 資料庫	RDS 登入活動監控	高
Discovery:RDS/MaliciousIPCaller	支援的 Amazon Aurora 資料庫	RDS 登入活動監控	中

調查結果類型	資源類型	基礎資料來源/功能	調查結果的嚴重性
Discovery:RDS/TorIPCaller	支援的 Amazon Aurora 資料庫	RDS 登入活動監控	中
Backdoor:Runtime/C&CActivity.B	執行個體、EKS 叢集、ECS 叢集或容器	執行期監控	高
Backdoor:Runtime/C&CActivity.B!DNS	執行個體、EKS 叢集、ECS 叢集或容器	執行期監控	高
CryptoCurrency:Runtime/BitcoinTool.B	執行個體、EKS 叢集、ECS 叢集或容器	執行期監控	高
CryptoCurrency:Runtime/BitcoinTool.B!DNS	執行個體、EKS 叢集、ECS 叢集或容器	執行期監控	高
DefenseEvasion:Runtime/FilelessExecution	執行個體、EKS 叢集、ECS 叢集或容器	執行期監控	中
DefenseEvasion:Runtime/ProcessInjection.Proc	執行個體、EKS 叢集、ECS 叢集或容器	執行期監控	高

調查結果類型	資源類型	基礎資料來源/功能	調查結果的嚴重性
DefenseEvasion:Runtime/ProcessInjection.Ptrace	執行個體、EKS 叢集、ECS 叢集或容器	執行期監控	中
DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite	執行個體、EKS 叢集、ECS 叢集或容器	執行期監控	高
DefenseEvasion:Runtime/PtraceAntiDebugging	執行個體、EKS 叢集、ECS 叢集或容器	執行期監控	低
DefenseEvasion:Runtime/SuspiciousCommand	執行個體、EKS 叢集、ECS 叢集或容器	執行期監控	高
Execution:Runtime/MaliciousFileExecuted	執行個體、EKS 叢集、ECS 叢集或容器	執行期監控	高
Execution:Runtime/NewBinaryExecuted	執行個體、EKS 叢集、ECS 叢集或容器	執行期監控	中
Execution:Runtime/NewLibraryLoaded	執行個體、EKS 叢集、ECS 叢集或容器	執行期監控	中

調查結果類型	資源類型	基礎資料來源/功能	調查結果的嚴重性
Execution:Runtime/SuspiciousCommand	執行個體、EKS 叢集、ECS 叢集或容器	執行期監控	變數
Execution:Runtime/SuspiciousTool	執行個體、EKS 叢集、ECS 叢集或容器	執行期監控	變數
Execution:Runtime/ReverseShell	執行個體、EKS 叢集、ECS 叢集或容器	執行期監控	高
Impact:Runtime/AbusedDomainRequest.Reputation	執行個體、EKS 叢集、ECS 叢集或容器	執行期監控	中
Impact:Runtime/BitcoinDomainRequest.Reputation	執行個體、EKS 叢集、ECS 叢集或容器	執行期監控	高
Impact:Runtime/CryptoMinerExecuted	執行個體、EKS 叢集、ECS 叢集或容器	執行期監控	高
Impact:Runtime/MaliciousDomainRequest.Reputation	執行個體、EKS 叢集、ECS 叢集或容器	執行期監控	中

調查結果類型	資源類型	基礎資料來源/功能	調查結果的嚴重性
Impact:Runtime/SuspiciousDomainRequest.Reputation	執行個體、EKS 叢集、ECS 叢集或容器	執行期監控	低
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	執行個體、EKS 叢集、ECS 叢集或容器	執行期監控	高
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory	執行個體、EKS 叢集、ECS 叢集或容器	執行期監控	中
PrivilegeEscalation:Runtime/DockerSocketAccessed	執行個體、EKS 叢集、ECS 叢集或容器	執行期監控	中
PrivilegeEscalation:Runtime/RuncContainerEscape	執行個體、EKS 叢集、ECS 叢集或容器	執行期監控	高

調查結果類型	資源類型	基礎資料來源/功能	調查結果的嚴重性
PrivilegeEscalation:Runtime/UserfaultfdUsage	執行個體、EKS 叢集、ECS 叢集或容器	執行期監控	中
Trojan:Runtime/BlackholeTraffic	執行個體、EKS 叢集、ECS 叢集或容器	執行期監控	中
Trojan:Runtime/BlackholeTraffic!DNS	執行個體、EKS 叢集、ECS 叢集或容器	執行期監控	中
Trojan:Runtime/DropPoint	執行個體、EKS 叢集、ECS 叢集或容器	執行期監控	中
Trojan:Runtime/DGADomainRequest.C!DNS	執行個體、EKS 叢集、ECS 叢集或容器	執行期監控	高
Trojan:Runtime/DriveBySourceTraffic!DNS	執行個體、EKS 叢集、ECS 叢集或容器	執行期監控	高
Trojan:Runtime/DropPoint!DNS	執行個體、EKS 叢集、ECS 叢集或容器	執行期監控	中

調查結果類型	資源類型	基礎資料來源/功能	調查結果的嚴重性
Trojan:Runtime/PhishingDomainRequest!DNS	執行個體、EKS 叢集、ECS 叢集或容器	執行期監控	高
UnauthorizedAccess:Runtime/MetadataDNSRebind	執行個體、EKS 叢集、ECS 叢集或容器	執行期監控	高
UnauthorizedAccess:Runtime/TorClient	執行個體、EKS 叢集、ECS 叢集或容器	執行期監控	高
UnauthorizedAccess:Runtime/TorRelay	執行個體、EKS 叢集、ECS 叢集或容器	執行期監控	高
Backdoor:EC2/C&CActivity.B	EC2	VPC 流量日誌	高
Backdoor:EC2/DenialOfService.Dns	EC2	VPC 流量日誌	高
Backdoor:EC2/DenialOfService.Tcp	EC2	VPC 流量日誌	高
Backdoor:EC2/DenialOfService.Udp	EC2	VPC 流量日誌	高

調查結果類型	資源類型	基礎資料來源/功能	調查結果的嚴重性
Backdoor:EC2/DenialOfService.UdpOnTcpPorts	EC2	VPC 流量日誌	高
Backdoor:EC2/DenialOfService.UnusualProtocol	EC2	VPC 流量日誌	高
Backdoor:EC2/Spambot	EC2	VPC 流量日誌	中
Behavior:EC2/NetworkPortUnusual	EC2	VPC 流量日誌	中
Behavior:EC2/TrafficVolumeUnusual	EC2	VPC 流量日誌	中
CryptoCurrency:EC2/BitcoinTool.B	EC2	VPC 流量日誌	高
DefenseEvasion:EC2/UnusualDNSResolver	EC2	VPC 流量日誌	中
DefenseEvasion:EC2/UnusualDoHActivity	EC2	VPC 流量日誌	中

調查結果類型	資源類型	基礎資料來源/功能	調查結果的嚴重性
DefenseEvasion:EC2/UnusualDoTActivity	EC2	VPC 流量日誌	中
Impact:EC2/PortSweep	EC2	VPC 流量日誌	高
Impact:EC2/WinRMBruteForce	EC2	VPC 流量日誌	低*
Recon:EC2/PortProbeEMRUnprotectedPort	EC2	VPC 流量日誌	高
Recon:EC2/PortProbeUnprotectedPort	EC2	VPC 流量日誌	低*
Recon:EC2/Portscan	EC2	VPC 流量日誌	中
Trojan:EC2/BlackholeTraffic	EC2	VPC 流量日誌	中
Trojan:EC2/DropPoint	EC2	VPC 流量日誌	中

調查結果類型	資源類型	基礎資料來源/功能	調查結果的嚴重性
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	EC2	VPC 流量日誌	中
UnauthorizedAccess:EC2/RDPBruteForce	EC2	VPC 流量日誌	低*
UnauthorizedAccess:EC2/SSHBruteForce	EC2	VPC 流量日誌	低*
UnauthorizedAccess:EC2/TorClient	EC2	VPC 流量日誌	高
UnauthorizedAccess:EC2/TorRelay	EC2	VPC 流量日誌	高

管理 Amazon GuardDuty 發現

GuardDuty 提供數項重要功能，協助您排序、儲存和管理發現項目。這些功能可幫助您根據具體環境以量身打造調查結果，讓您減少來自低價值調查結果的雜訊，以便專注於 AWS 環境的特定威脅。檢閱此頁面上的主題，瞭解如何使用這些功能來增加發現項目 GuardDuty的價值。

主題：

「摘要」儀表板

「摘要」控制面板提供您 AWS 帳戶 在目前「區域」中產生之 GuardDuty 發現項目的彙總檢視。目前，該儀表板最多支援 5,000 個調查結果。不過，您可以使用 GuardDuty 主控台上的「發現項目」頁面，GetFindings或者，檢視所有發現項目的詳細資訊ListFindings。

> **Note**
>
> 發現項目摘要只能透過 https://console.aws.amazon.com/guardduty/ 的 GuardDuty 主控台取得。

下列各節將協助您存取該儀表板並了解其元件。

目錄

存取「摘要」儀表板

在 GuardDuty 主控台上，[摘要] 儀表板會顯示目前「區域」中產生的最近 5,000 個 GuardDuty 發現項目的合併檢視。

存取「摘要」儀表板

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/
2. 在導覽窗格中，選擇摘要。開啟主控台時，會 GuardDuty 顯示 [摘要] 控制面板。
3. 依預設，系統會顯示當日 (今天) 的摘要。主 GuardDuty控台提供檢視「過去 2 天」、「過去 7 天」和「過去 30 天」摘要的選項。若要變更預設時間範圍，請選擇概觀窗格上方下拉式清單中的其中一個選項。
4. 篩選資料
   - 具有最多調查結果的帳戶、具有最多調查結果的資源以及最不常見的調查結果小工具可協助您根據調查結果的嚴重性等級篩選資料。
   - 具有最多調查結果的資源小工具也可協助您根據可能受影響的資源類型篩選資料。

成員帳戶可以檢視屬於自己帳戶之可能受影響資源的詳細資訊。如果您是 GuardDuty 管理員帳戶，並且想要檢視可能受影響資源的詳細資料，請使用相關聯成員帳戶的認證開啟 GuardDuty 主控台。

5. 保障計劃承保

   保護方案涵蓋範圍提供組織 GuardDuty 中已啟用的成員帳戶計數。只有委派的 GuardDuty 管理員才能看到統計資料。

了解「摘要」儀表板

摘要儀表板會在下列各節中顯示彙總資料。在繼續檢視和了解摘要之前，請務必從主控台頂端的「區域」選取器中選擇所需 AWS 區域 。另外，請確保從概觀窗格上方提供的下拉式清單中選擇所需時間範圍。如果沒有針對所選參數產生任何調查結果，則所有小工具都不會提供任何資料。

在最多 5,000 個發 GuardDuty 現項目的數量中，具有最多發現項目的帳戶的摘要儀表板、具有最多發現項目的資源以及發現次數最少的發現項目會顯示以前 5 個結果為基礎的資料。如需更深入的分析，請參閱 GuardDuty 主控台中的「發現項目」頁面。

概觀

本節提供下列資料：

- 調查結果總計：表示在目前區域中，帳戶中產生的調查結果總數。
- 高嚴重性發現項目：指出目前「區域」中嚴重性層級較高的 GuardDuty發現項目數目。
- 具有調查結果的資源：表示與調查結果相關聯且可能遭到入侵的資源數量。
- 具有調查結果的帳戶：表示至少產生了一個調查結果的帳戶數量。如果您是獨立帳戶，則此欄位中的值為 1。

對於過去 7 天和過去 30 天的時間範圍，概觀窗格可分別顯示逐週產生的調查結果 (WoW) 或逐月 (MoM) 產生的調查結果百分比差值。如果在前一週或前一個月沒有產生任何調查結果，則由於沒有可比較的資料，可能無法獲得百分比差值。

如果您是 GuardDuty 系統管理員帳戶，則所有這些欄位都會提供組織中所有成員帳戶的摘要資料。

依嚴重性劃分的調查結果

本節會顯示長條圖，其中包含所選時間範圍內的調查結果總數。您可以檢視在所選時間範圍內的特定日期所產生之低、中或高嚴重性的調查結果數量。

最常見的調查結果類型

本節提供從目前「區域」產生的最後 5,000 個發現項目數量中觀察到的前五個常見 GuardDuty 發現項目類型的圓餅圖圖例。當滑鼠懸停在每個磁區上時，此圓餅圖會顯示以下資料：

- 調查結果計數：表示在所選時間範圍內產生此調查結果的次數。
- 嚴重性：表示調查結果的嚴重性等級，例如「中」和「高」。
- 百分比：表示此調查結果類型在圓餅圖中的占有率。
- 上次產生：表示自上次產生此調查結果類型以來已經過了多長時間。

具有最多調查結果的帳戶

本節提供下列資料：

- 科目：指出產生搜尋結果的 AWS 帳戶 識別碼。
- 調查結果計數：表示針對此帳戶 ID 產生調查結果的次數。
- 上次產生：表示自上次針對此帳戶 ID 產生調查結果類型以來已經過了多長時間。
- 高嚴重性：依預設，系統會針對高嚴重性調查結果類型顯示資料。此欄位的可能選項為高嚴重性、中等嚴重性和所有嚴重性。

具有調查結果的資源

本節提供下列資料：

- 資源：表示可能受影響的資源類型，如果此資源屬於您的帳戶，您可以存取快速連結以檢視資源詳細資訊。如果您是 GuardDuty 系統管理員帳號，則可以使用此資源所屬成員帳號的認證存取 GuardDuty 主控台，以檢視可能受影響資源的詳細資訊。
- 帳號：表示此資源所屬的 AWS 帳戶 ID。
- 調查結果計數：表示此資源與調查結果相關聯的次數。
- 上次產生：表示自上次產生與此資源相關聯的調查結果類型以來已經過了多長時間。
- 所有資源類型：依預設，系統會顯示所有資源類型的資料。透過使用下拉式清單，您可以檢視特定資源類型的資料，例如執行個體AccessKey、Lambda 等。
- 高嚴重性：依預設，系統會針對高嚴重性調查結果類型顯示資料。透過使用下拉式清單，您可以檢視其他嚴重性等級的資料。可能的選項為高嚴重性、中等嚴重性和所有嚴重性。

最不常見的調查結果

本節提供您 AWS 環境中不常產生之尋找項目類型的詳細資訊。此洞察可協助您調查環境中的緊急威脅模式並採取對應行動。表格顯示了以下資料：

- 調查結果類型：表示調查結果類型名稱。
- 調查結果計數：表示在所選時間範圍內產生此調查結果類型的次數。
- 上次產生：表示自上次產生此調查結果類型以來已經過了多長時間。
- 高嚴重性：依預設，系統會針對高嚴重性調查結果類型顯示資料。此欄位的可能選項為高嚴重性、中等嚴重性和所有嚴重性。

保障計劃承保

本節提供屬於您組織的作用中成員帳戶數目，並已在目前啟用一或多個功能和其他功能 (如果適用) 組態 AWS 區域。

只有委派的 GuardDuty 管理員可以檢視其組織內成員帳戶的統計資料。如果未設定功能，請在「動作」 欄下選擇「設定」。

建立新 AWS 組織時，最多可能需要 24 小時才能產生整個組織的統計資料。

在「摘要」儀表板上提供意見回饋

GuardDuty 鼓勵您針對「摘要」控制面板的可用性、功能和效能提供意見反應。這有助於我們改進儀表板。

在「摘要」儀表板上提供意見回饋

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/
2. 在導覽窗格中，選擇摘要。當您開啟 GuardDuty主控台時，它會顯示 [摘要] 控制面板。
3. 選擇儀表板右上角的意見回饋。這將開啟一個表單。提供意見回饋後，請選擇提交。

篩選問題清單

調查結果篩選條件可讓您檢視符合您指定準則的調查結果，並篩選出任何不相符的調查結果。您可以使用 Amazon GuardDuty 主控台輕鬆建立尋找篩選器，也可以使用 JSON 使用 CreateFilterAPI 建立篩選器。請檢閱下列各節，以了解如何在主控台中建立篩選條件。若要使用這些篩選條件自動封存傳入的調查結果，請參閱 隱藏規則。

在 GuardDuty 控制台中創建過濾器

查找過濾器可以創建並通過 GuardDuty 控制台進行測試。您可儲存透過主控台建立的篩選條件，以便用於抑制規則或未來的篩選條件操作。篩選條件由至少一個篩選條件準則組成，其中包含一個與至少一個值配對的篩選條件屬性。

當您建立新的篩選條件時，請注意下列事項：

- 篩選條件不接受萬用字元。
- 您可以指定最少一個屬性或最多 50 個屬性，作為特定篩選條件的準則。
- 使用等於或不等於條件篩選屬性值 (例如帳戶 ID) 時，您最多可以指定 50 個值。
- 每個篩選條件準則屬性都會作為 AND 運算子予以評估。相同屬性的多個值會作為 AND/OR 予以評估。

篩選問題清單 (主控台)

1. 選擇顯示 GuardDuty 發現項目清單上方的新增篩選條件。
2. 在展開的屬性清單中，選取您要指定作為準則的屬性，例如帳戶 ID或動作類型。

   > **Note**
   >
   > 如需可用來建立篩選條件準則的屬性清單，請參閱此頁面中的篩選條件屬性資料表。

3. 在顯示的文字欄位中，指定每個選取屬性的值，然後選擇套用。

   > **Note**
   >
   > 套用篩選條件後，您可以透過選擇篩選條件名稱左側的黑點，將篩選條件轉換為排除符合篩選條件的調查結果。這樣可有效為選取的屬性建立「不等於」篩選條件。

4. 若要儲存指定的屬性和值 (篩選條件) 以做為篩選條件，請選擇 Save (儲存)。輸入篩選條件名稱和說明，然後選擇完成。

篩選條件屬性

當您使用 API 操作建立篩選條件或排序調查結果時，您必須在 JSON 中指定篩選條件準則。這些篩選條件準則與調查結果的詳細資訊 JSON 相關聯。下表包含篩選條件屬性及其對等 JSON 欄位名稱的主控台顯示名稱清單。

主控台欄位名稱	JSON 欄位名稱
帳戶 ID	accountId
問題清單 ID	id
區域	region
嚴重性	severity 如果您`severity`與 API AWS CLI、或搭配使用 AWS CloudFormation，它將具有數值。如需詳細資訊，請參閱 findingCriteria。
調查結果類型	type
更新時間	updatedAt
存取金鑰 ID	資源。 accessKeyDetails。 accessKeyId
委託人 ID	資源。 accessKeyDetails. principalId
使用者名稱	資源。 accessKeyDetails. 用 userName
使用者類型	資源。 accessKeyDetails. 使用者類型
IAM 執行個體描述檔 ID	資源。實例詳細信息。 iamInstanceProfile.id
執行個體 ID	resource.instanceDetails.instanceId
執行個體影像 ID	resource.instanceDetails.imageId
執行個體標籤索引鍵	resource.instanceDetails.tags.key
執行個體標籤值	resource.instanceDetails.tags.value

主控台欄位名稱	JSON 欄位名稱
IPv6 地址	resource.instanceDetails.networkInterfaces.ipv6Addresses
私有 IPv4 地址	實例詳細信息。網絡接口。 privateIpAddresses 。 privateIpAddress
公有 DNS 名稱	實例詳細信息。網絡接口。 publicDnsName
公有 IP	resource.instanceDetails.networkInterfaces.publicIp
安全群組 ID	resource.instanceDetails.networkInterfaces.securityGroups.groupId
安全群組名稱	resource.instanceDetails.networkInterfaces.securityGroups.groupName
子網路 ID	resource.instanceDetails.networkInterfaces.subnetId
VPC ID	resource.instanceDetails.networkInterfaces.vpcId
Outpost ARN	resource.instanceDetails.outpostARN
資源類型	resource.resourceType
儲存貯體許可	資源 .s3. 公共訪BucketDetails問.
儲存貯體名稱	資源 .s3. BucketDetails 名稱
儲存貯體標籤金鑰	資源 .s3。標籤BucketDetails密鑰
儲存貯體標籤值	資源 .s3. BucketDetails 標籤值
儲存貯體類型	資源 .s3. 類型 BucketDetails
動作類型	service.action.actionType

主控台欄位名稱	JSON 欄位名稱
已發出 API 呼叫	服務行動。 awsApiCall動作
API 發起人類型	服務行動。 awsApiCall動作. 呼叫器類型
API 錯誤碼	服務行動。 awsApiCall動作. 錯誤碼
API 發起人城市	服務行動。 awsApiCall動作。 remoteIpDetails. 城市. 城市名稱
API 發起人國家/地區	服務行動。 awsApiCall動作。 remoteIpDetails. 國家. 國家名稱
API 發起人 IPv4 地址	服務行動。 awsApiCall動作。 remoteIpD etails.IP 地址 4
API 呼叫者 IPv6 位址	服務行動。 awsApiCall動作。 remoteIpD etails.IP 地址 6
API 發起人 ASN ID	服務行動。 awsApiCall動作。 remoteIpDetails. 組織.
API 發起人 ASN 名稱	服務行動。 awsApiCall動作。 remoteIpDetails. 組織. 阿斯諾格
API 發起人服務名稱	服務行動。 awsApiCall動作. 服務名稱
DNS 請求網域	服務行動。 dnsRequestAction. 網域名稱
DNS 要求網域尾碼	服務行動。 dnsRequestAction。 domainWit hSuffix
已封鎖網路連線	服務行動。 networkConnectionAction. 封鎖。
網路連線方向	服務行動。 networkConnectionAction連接方向 。
網路連線本機連接埠	服務行動。 networkConnectionAction。 localPortDetails. 端口。

主控台欄位名稱	JSON 欄位名稱
網路連線通訊協定	服務行動。 networkConnectionAction. 協議。
網路連線城市	服務行動。 networkConnectionAction。 remoteIpDetails. 城市. 城市名稱
網路連線國家/地區	服務行動。 networkConnectionAction。 remoteIpDetails. 國家. 國家名稱
網路連線遠端 IPv4 地址	服務行動。 networkConnectionAction。 remoteIpDetails.IP 地址 4
網路連線遠端 IPv6 位址	服務行動。 networkConnectionAction。 remoteIpDetails.IP 地址 6
網路連線遠端 IP ASN ID	服務行動。 networkConnectionAction。 remoteIpDetails. 組織.
網路連線遠端 IP ASN 名稱	服務行動。 networkConnectionAction。 remoteIpDetails. 組織. 阿斯諾格
網路連線遠端連接埠	服務行動。 networkConnectionAction。 remotePortDetails. 端口。
附屬的遠端帳戶	服務行動。 awsApiCall動作。 remoteAcc ountDetails. 附屬。
Kubernetes API 呼叫者 IPv4 地址	服務行動。 kubernetesApiCall動作。 remoteIpDetails.IP 地址 4
庫伯內特斯 API 呼叫者 IPv6 地址	服務行動。 kubernetesApiCall動作。 remoteIpDetails.IP 地址 6
Kubernetes 命名空間	服務行動。 kubernetesApiCall動作. 命名空間
Kubernetes API 呼叫者 ASN ID	服務行動。 kubernetesApiCall動作。 remoteIpDetails. 組織.
Kubernetes API 呼叫請求 URI	服務行動。 kubernetesApiCall動作請求

主控台欄位名稱	JSON 欄位名稱
Kubernetes API 狀態碼	服務行動。 kubernetesApiCall動作. 狀態碼
網路連線本機 IPv4 地址	服務行動。 networkConnectionAction。 localIpDetails.IP 地址 4
網路連線本機 IPv6 位址	服務行動。 networkConnectionAction。 localIpDetails.IP 地址 6
通訊協定	服務行動。 networkConnectionAction. 協議。
API 呼叫服務名稱	服務行動。 awsApiCall動作. 服務名稱
API 呼叫者帳戶 ID	服務行動。 awsApiCall動作。 remoteAcc ountDetails. accountId
威脅清單名稱	服務。附加信息。 threatListName
資源角色	service.resourceRole
EKS 叢集名稱	資源。 eksClusterDetails. 名稱。
Kubernetes 工作負載名稱	資源。庫伯特詳細信息。 kubernetesWorkload Details. 名稱。
Kubernetes 工作負載命名空間	資源。庫伯特詳細信息。 kubernetesWorkload Details. 命名空間
Kubernetes 使用者名稱	資源。庫伯特詳細信息。 kubernetesUserDeta ils. 用戶名
Kubernetes 容器映像	資源。庫伯特詳細信息。 kubernetesWorkload Details. 容器.
Kubernetes 容器映像前綴	資源。庫伯特詳細信息。 kubernetesWorkload Details. 容器. 圖像前綴
掃描 ID	服務。 ebsVolumeScan詳細資訊. 掃描

主控台欄位名稱	JSON 欄位名稱
EBS 磁碟區掃瞄威脅名稱	服務。 ebsVolumeScan詳細資料。掃描偵測。threatDetectedBy名稱. 威脅名稱. 名稱
威脅嚴重性	服務。 ebsVolumeScan詳細資料。掃描偵測。threatDetectedBy名稱. 威脅名稱. 嚴重性
SHA 檔案	服務。 ebsVolumeScan詳細資料。掃描偵測。threatDetectedBy名稱. 威脅名稱. 檔案路徑. 雜湊
ECS 叢集名稱	資源。 ecsClusterDetails. 名稱。
ECS 容器映像	資源。 ecsClusterDetails任務詳細信息. 容器.
ECS 任務定義 ARN	資源。 ecsClusterDetails工作詳細資訊. 定義
獨立容器映像	resource.containerDetails.image
資料庫執行個體 ID	資源。 rdsDbInstance詳細資訊。 dbInstanceIdentifier
資料庫叢集 ID	資源。 rdsDbInstance詳細資訊。 dbClusterIdentifier
資料庫引擎	資源。 rdsDbInstance詳情引擎
資料庫使用者	資源。 rdsDbUser詳情. 用戶
資料庫執行個體標籤索引鍵	資源。 rdsDbInstance詳細信息標籤
資料庫執行個體標籤值	資源。 rdsDbInstance詳細資料. 標籤.
可執行 SHA-256	service.runtimeDetails.process.executableSha256
程序名稱	service.runtimeDetails.process.name
可執行路徑	service.runtimeDetails.process.executablePath

主控台欄位名稱	JSON 欄位名稱
Lambda 功能名稱	resource.lambdaDetails.functionName
Lambda 函數 ARN	resource.lambdaDetails.functionArn
Lambda 函數標籤索引鍵	resource.lambdaDetails.tags.key
Lambda 函數標籤值	resource.lambdaDetails.tags.value
DNS 請求網域	服務行動。 dnsRequestAction。 domainWithSuffix

隱藏規則

隱藏規則是一組條件 (由與值配對的篩選屬性組成)，用於自動封存符合指定條件的新調查結果來篩選調查結果。隱藏規則可用來篩選低價值的問題清單、誤判問題清單，或您不打算採取行動的威脅，以便更容易辨識對環境影響最大的安全威脅。

建立隱藏規則後，只要有隱藏規則，就會自動封存符合規則中定義之條件的新問題清單。您可以使用既有的篩選條件來建立隱藏規則，或從定義的新篩選條件中建立隱藏規則。您可以設定隱藏規則以隱藏整個問題清單類型，或定義更細微的篩選條件，而僅隱藏特定問題清單類型的特定例項。您可以隨時編輯抑制規則。

隱藏的發現不會傳送至 AWS Security Hub Amazon 簡易儲存服務、Amazon Detective 或 Amazon，如果您透過 Security Hub EventBridge、第三方 SIEM 或其他警示和票務應用程式消耗發 GuardDuty 現結果，可降低發現雜訊等級。如果您已啟用GuardDuty 惡意程式碼，則抑制的 GuardDuty 發現項目將不會起始惡意軟體掃描。

GuardDuty 即使發現項目符合您的抑制規則，仍會繼續產生搜尋結果，不過，這些發現項目會自動標示為已封存。封存的發現項目會儲存 90 天，並可在 GuardDuty 該期間的任何時間進行檢視。您可以在 GuardDuty 主控台中檢視隱藏的發現項目，方法是從發現項目表格中選取「已封存」，或透過 GuardDuty API 使用`findingCriteria`準則`service.archived`等於 true 的 ListFindingsAPI 來檢視隱藏的發現項目。

> **Note**
>
> 在多帳戶環境中，只有 GuardDuty 管理員可以建立抑制規則。

隱藏規則的常用案例和範例

下列調查結果類型有套用隱藏規則的常見使用案例、選取調查結果名稱以深入了解該調查結果的相關資訊，或檢閱資訊，以便從主控台為該調查結果類型建立隱藏規則。

> **Important**
>
> GuardDuty 建議您以動態方式建立抑制規則，並且僅針對您重複識別出誤判的發現項目。

- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS：使用隱藏規則，以自動封存將 VPC 聯網設為路由網際網路流量，使其從內部部署閘道 (而非 VPC 網際網路閘道) 輸出時所產生的調查結果。

  當將網路設定為路由網際網路流量，使其從內部部署閘道而不是從 VPC 網際網路閘道 (IGW) 輸出時，就會產生此調查結果。一般組態 (例如使用 AWS Outposts 或 VPC VPN 連接) 可能會導致流量以這種方式路由。如果這是預期的行為，建議您使用 中的隱藏規則，並建立包含兩個篩選條件的規則。第一個條件是 finding type (問題清單類型)，應該是 `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS`。第二個篩選條件是具有內部部署網際網路閘道 IP 地址或 CIDR 範圍的 API 呼叫者 IPv4 地址。下面的範例表示您將用於根據 API 呼叫者 IP 地址隱藏此調查結果類型的篩選條件。

  ```
  Finding type: UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS
   API caller IPv4 address: 198.51.100.6
  ```

  > **Note**
  >
  > 若要包含多個 API 呼叫者 IP，您可以為每個 IP 新增新的 API 呼叫者 IPv4 地址篩選條件。

- Recon:EC2/Portscan：使用漏洞評估應用程式時，使用隱藏規則以自動封存調查結果。

  隱藏規則應包含兩個篩選準則。第一個條件應該使用調查結果類型屬性，其值為 `Recon:EC2/Portscan`。第二個篩選條件應該找出主控這些漏洞評定工具的執行個體。您可以使用執行個體映像 ID 屬性或標籤值屬性，視主控這些工具的執行個體可識別的條件而定。下面的範例表示您根據具有特定 AMI 的執行個體隱藏此調查結果類型所用的篩選條件。

  ```
  Finding type: Recon:EC2/Portscan Instance image ID: ami-999999999
  ```

- UnauthorizedAccess:EC2/SSHBruteForce：使用隱藏規則，在調查結果目標為堡壘執行個體時，自動封存調查結果。

  如果蠻力嘗試的目標是堡壘主機，這可能代表您 AWS 環境的預期行為。如果是這種情況，我們建議您為此調查結果設定隱藏規則。隱藏規則應包含兩個篩選準則。第一個條件應該使用調查結果類型屬性，其值為 `UnauthorizedAccess:EC2/SSHBruteForce`。第二個篩選條件應該找出執行個體或做為堡壘主機的執行個體。您可以使用執行個體映像 ID 屬性或標籤值屬性，視主控這些工具的執行個體可識別的條件而定。下面的範例表示您根據具有特定執行個體標籤值的執行個體，隱藏此調查結果類型所用的篩選條件。

  ```
  Finding type: UnauthorizedAccess:EC2/SSHBruteForce Instance tag value: devops
  ```

- Recon:EC2/PortProbeUnprotectedPort：使用隱藏規則，在調查結果目標為刻意公開的執行個體時，自動封存調查結果。

  在某些情況下，可能會刻意暴露執行個體，例如，若是託管在 Web 伺服器上。如果您的 AWS 環境是這種情況，建議您為此發現項目設定抑制規則。隱藏規則應包含兩個篩選準則。第一個條件應該使用調查結果類型屬性，其值為 `Recon:EC2/PortProbeUnprotectedPort`。第二個篩選條件應該找出執行個體或做為堡壘主機的執行個體。您可以使用執行個體映像 ID 屬性或標籤值屬性，視主控這些工具的執行個體可識別的準則而定。下面的範例表示您根據具有主控台中特定執行個體標籤值的執行個體，隱藏此調查結果類型所用的篩選條件。

  ```
  Finding type: Recon:EC2/PortProbeUnprotectedPort Instance tag key: prod
  ```

執行階段監視發現項目的建議抑制

- 當容器內的程序與 Docker 通訊端通訊時便會產生 PrivilegeEscalation:Runtime/DockerSocketAccessed。由於正當原因，環境中存在可能需要存取 Docker 通訊端的容器。從這類容器存取將產生 PrivilegeEscalation:Runtime/DockerSocketAccessed 調查結果。如果您的 AWS 環境是這種情況，建議您為此尋找項目類型設定隱藏規則。第一個條件應該使用調查結果類型欄位，其值等於 `PrivilegeEscalation:Runtime/DockerSocketAccessed`。第二個篩選條件是可執行檔路徑欄位，其值等於產生的調查結果中程序的 `executablePath`。或者，第二個篩選條件可以使用可執行檔 SHA-256 欄位，其值等於產生的調查結果中程序的 `executableSha256`。
- Kubernetes 叢集會以 pod 的形式執行自己的 DNS 伺服器，例如 `coredns`。因此，對於來自網繭的每個 DNS 查閱，都會 GuardDuty 擷取兩個 DNS 事件 — 一個來自網繭，另一個來自伺服器網繭。這可能會產生下列 DNS 調查結果的重複項目：
  - Backdoor:Runtime/C&CActivity.B!DNS

- CryptoCurrency:Runtime/BitcoinTool.B!DNS
- Impact:Runtime/AbusedDomainRequest.Reputation
- Impact:Runtime/BitcoinDomainRequest.Reputation
- Impact:Runtime/MaliciousDomainRequest.Reputation
- Impact:Runtime/SuspiciousDomainRequest.Reputation
- Trojan:Runtime/BlackholeTraffic!DNS
- Trojan:Runtime/DGADomainRequest.C!DNS
- Trojan:Runtime/DriveBySourceTraffic!DNS
- Trojan:Runtime/DropPoint!DNS
- Trojan:Runtime/PhishingDomainRequest!DNS

重複的調查結果將包括與 DNS 伺服器 pod 對應的 pod、容器和程序詳細資訊。您可以使用這些欄位設定隱藏規則，以隱藏這些重複的調查結果。第一個篩選條件應使用調查結果類型欄位，其值等於本節稍早提供的調查結果清單中的 DNS 調查結果類型。第二個篩選條件可以是值等於 DNS 伺服器 `executablePath` 的可執行檔路徑，或值等於 DNS 伺服器 `executableSHA256` 在產生的調查結果中的可執行檔 SHA-256。作為選用的第三個篩選條件，您可以使用 Kubernetes 容器映像欄位，其值等於產生的調查結果中 DNS 伺服器 pod 的容器映像。

建立抑制規則

選擇您偏好的存取方式，以建立 GuardDuty 搜尋型態的隱藏規則。

Console

您可以使用 GuardDuty 主控台視覺化、建立和管理隱藏規則。隱藏規則的產生方式與篩選條件相同，且您現有儲存的篩選條件可用作隱藏規則。如需建立篩選條件的詳細資訊，請參閱篩選問題清單。

若要使用主控台建立隱藏規則：

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/
2. 在調查結果頁面上，選擇隱藏調查結果以開啟隱藏規則面板。
3. 若要開啟篩選條件選單，請在新增篩選條件中輸入 **`filter criteria`**。您可以從清單中選擇條件。輸入所選條件的有效值。

> **Note**
>
> 若要判斷值是否有效，請檢視調查結果資料表，並選擇您要隱藏的調查結果。在調查結果面板中檢閱其詳細資訊。

您可以新增多個篩選條件，並確保資料表中僅顯示您要隱藏的那些調查結果。

4. 輸入隱藏規則的名稱和說明。有效的字元包括英數字元、句號 (.)、破折號 (-)、底線 (_) 和空格。
5. 選擇儲存。

您也可以從現有儲存的篩選條件建立隱藏規則。如需建立篩選條件的詳細資訊，請參閱篩選問題清單。

若要從已儲存的篩選條件建立隱藏規則：

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/
2. 在調查結果頁面上，選擇隱藏調查結果以開啟隱藏規則面板。
3. 從已儲存的規則下拉式清單中，選擇儲存的篩選條件。
4. 您也可以新增篩選條件。如果您不需要其他篩選條件，請略過此步驟。

   若要開啟篩選條件選單，請在新增篩選條件中輸入 **`filter criteria`**。您可以從清單中選擇條件。輸入所選條件的有效值。

   > **Note**
   >
   > 若要判斷值是否有效，請檢視調查結果資料表，並選擇您要隱藏的調查結果。在調查結果面板中檢閱其詳細資訊。

5. 輸入隱藏規則的名稱和說明。有效的字元包括英數字元、句號 (.)、破折號 (-)、底線 (_) 和空格。
6. 選擇儲存。

API/CLI

使用 API 建立隱藏規則：

1. 您也可以透過 CreateFilter API 建立隱藏規則。若要這麼做，請依照下面詳述的範例格式，在 JSON 檔案中指定篩選條件。下列範例會隱藏任何對 test.example.com 網域具有 DNS 請求的嚴重程度低的未封存調查結果。對於中等嚴重程度的調查結果，輸入清單會是 ["4", "5", "7"]。對於高嚴重程度的調查結果，輸入清單會是 ["6", "7", "8"]。您也可以根據清單中的任何一個值進行篩選。

```
{
    "Criterion": {
        "service.archived": {
            "Eq": [
                "false"
            ]
        },
        "service.action.dnsRequestAction.domain": {
            "Eq": [
                "test.example.com"
            ]
        },
        "severity": {
            "Eq": [
                "1",
                "2",
                "3"
            ]
        }
    }
}
```

如需 JSON 欄位名稱及其主控台對等值的清單，請參閱篩選條件屬性。

若要測試篩選條件，請在 ListFindings API 中使用相同的 JSON 條件，並確認選取的是正確的調查結果。要使用您自己的檢測器 ID 和 .json 文件， AWS CLI 請按照示例測試您的過濾器條件。

要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

```
aws guardduty list-findings --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
finding-criteria file://criteria.json
```

2. 使用 CreateFilter API，或藉由使用 AWS CLI，依照下列範例，使用您自己的偵測器 ID、隱藏規則的名稱，以及 .json 檔案，上傳篩選條件以作為隱藏規則。

   要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

   ```
   aws guardduty create-filter --action ARCHIVE --detector-
   id 12abc34d567e8fa901bc2d34e56789f0 --name yourfiltername --finding-criteria
    file://criteria.json
   ```

您可以使用 ListFilter API，以程式設計方式檢視篩選條件清單。您可以透過向 GetFilter API 提供篩選條件名稱，來檢視個別篩選條件的詳細資訊。使用 UpdateFilter 更新篩選條件，或使用 DeleteFilter API 將其刪除。

刪除抑制規則

選擇您偏好的存取方式，以刪除 GuardDuty 搜尋型態的隱藏規則。

Console

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/
2. 在調查結果頁面上，選擇隱藏調查結果以開啟隱藏規則面板。
3. 從已儲存的規則下拉式清單中，選擇儲存的篩選條件。
4. 選擇 Delete rule (刪除規則)。

API/CLI

執行 DeleteFilter API。指定特定區域的篩選器名稱和相關聯的偵測器 ID。

或者，您可以透過取代以##格式化的值來使用下列 AWS CLI 範例：

```
aws guardduty delete-filter --region us-east-1 --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --filter-name filterName
```

要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

使用信任 IP 清單和威脅清單

Amazon 透過分析和處理 VPC 人雲端流程日誌、 AWS CloudTrail 事件日誌和 DNS 日誌來 GuardDuty 監控您 AWS 環境的安全。您可以設定 GuardDuty 為停止受信任 IP 清單中受信任 IP 的警示，並從您自己的威脅清單對已知惡意 IP 發出警示，以自訂此監控範圍。

信任 IP 清單和威脅清單僅適用於以公共可路由的 IP 地址為目的地的流量。清單的效果適用於所有 VPC 流程記錄檔和 CloudTrail 發現項目，但不適用於 DNS 發現項目。

GuardDuty 可以配置為使用以下類型的列表。

信任 IP 清單

受信任的 IP 清單包含您信任的 IP 位址，以便與 AWS 基礎結構和應用程式進行安全通訊。GuardDuty 不會針對受信任 IP 清單上的 IP 位址產生 VPC 流程記錄檔或 CloudTrail 發現項目。您最多可以在單一信任 IP 清單中包含 2000 個 IP 地址和 CIDR 範圍。在任何指定的時間，您在每個區域的每個 AWS 帳戶中，僅能上傳一份信任 IP 清單。

威脅 IP 清單

威脅清單包含已知的惡意 IP 地址。此清單可由第三方威脅情報提供，也可以專門為您的組織建立。除了由於潛在可疑活動而產生發現項目之外， GuardDuty 還會根據這些安全威脅清單產生發現項目。您最多可以在單一威脅清單中包含 250,000 個 IP 位址和 CIDR 範圍。 GuardDuty 只會根據威脅清單中涉及 IP 位址和 CIDR 範圍的活動產生發現項目；發現項目不會根據網域名稱產生。在任何特定時間點， AWS 帳戶 每個區域最多可以有六個上傳的威脅清單。

> **Note**
>
> 如果您同時在信任 IP 清單和威脅清單中包含相同的 IP，則信任 IP 清單會先處理該 IP，而且不會產生調查結果。

在多帳戶環境中，只有管理 GuardDuty 員帳號的使用者才能新增和管理信任的 IP 清單和威脅清單。由管理員帳戶帳戶上傳的受信任 IP 清單和威脅清單會強加在其成員帳戶中的 GuardDuty 功能上。換句話說，在成員帳 GuardDuty 戶中，會根據涉及管理員帳戶安全威脅清單中已知惡意 IP 位址的活動產生發

現項目，並且不會根據涉及管理員帳戶信任 IP 清單中 IP 位址的活動產生發現項目。如需詳細資訊，請參閱 在 Amazon 管理多個帳戶 GuardDuty。

清單格式

GuardDuty 接受下列格式的清單。

託管信任 IP 清單或威脅 IP 清單的每個檔案的大小上限為 35 MB。在信任 IP 清單和威脅 IP 清單中，IP 地址和 CIDR 範圍必須各自顯示為一行。僅接受 IPv4 地址。

- 純文字 (TXT)

  此格式同時支援 CIDR 區塊和個別 IP 地址。下列範例清單使用純文字 (TXT) 格式。

```
192.0.2.0/24
198.51.100.1
203.0.113.1
```

- 結構化威脅資訊運算式 (STIX)

  此格式同時支援 CIDR 區塊和個別 IP 地址。下列範例清單使用 STIX 格式。

```
<?xml version="1.0" encoding="UTF-8"?>
<stix:STIX_Package
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:stix="http://stix.mitre.org/stix-1"
    xmlns:stixCommon="http://stix.mitre.org/common-1"
    xmlns:ttp="http://stix.mitre.org/TTP-1"
    xmlns:cybox="http://cybox.mitre.org/cybox-2"
    xmlns:AddressObject="http://cybox.mitre.org/objects#AddressObject-2"
    xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
    xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
    xmlns:example="http://example.com/"
    xsi:schemaLocation="
    http://stix.mitre.org/stix-1 http://stix.mitre.org/XMLSchema/core/1.2/
stix_core.xsd
    http://stix.mitre.org/Campaign-1 http://stix.mitre.org/XMLSchema/campaign/1.2/
campaign.xsd
    http://stix.mitre.org/Indicator-2 http://stix.mitre.org/XMLSchema/indicator/2.2/
indicator.xsd
    http://stix.mitre.org/TTP-2 http://stix.mitre.org/XMLSchema/ttp/1.2/ttp.xsd
    http://stix.mitre.org/default_vocabularies-1 http://stix.mitre.org/XMLSchema/
default_vocabularies/1.2.0/stix_default_vocabularies.xsd
```

```
    http://cybox.mitre.org/objects#AddressObject-2 http://cybox.mitre.org/XMLSchema/
objects/Address/2.1/Address_Object.xsd"
    id="example:STIXPackage-a78fc4e3-df94-42dd-a074-6de62babfe16"
    version="1.2">
    <stix:Observables cybox_major_version="1" cybox_minor_version="1">
        <cybox:Observable id="example:observable-80b26f43-
dc41-43ff-861d-19aff31e0236">
            <cybox:Object id="example:object-161a5438-1c26-4275-ba44-a35ba963c245">
                <cybox:Properties xsi:type="AddressObject:AddressObjectType"
 category="ipv4-addr">

 <AddressObject:Address_Valuecondition="InclusiveBetween">192.0.2.0##comma##192.0.2.255</
AddressObject:Address_Value>
                </cybox:Properties>
            </cybox:Object>
        </cybox:Observable>
        <cybox:Observable id="example:observable-b442b399-aea4-436f-bb34-
b9ef6c5ed8ab">
            <cybox:Object id="example:object-b422417f-bf78-4b34-ba2d-de4b09590a6d">
                <cybox:Properties xsi:type="AddressObject:AddressObjectType"
 category="ipv4-addr">
                    <AddressObject:Address_Value>198.51.100.1</
AddressObject:Address_Value>
                </cybox:Properties>
            </cybox:Object>
        </cybox:Observable>
        <cybox:Observable
 id="example:observable-1742fa06-8b5e-4449-9d89-6f9f32595784">
            <cybox:Object id="example:object-dc73b749-8a31-46be-803f-71df77565391">
                <cybox:Properties xsi:type="AddressObject:AddressObjectType"
 category="ipv4-addr">
                    <AddressObject:Address_Value>203.0.113.1</
AddressObject:Address_Value>
                </cybox:Properties>
            </cybox:Object>
        </cybox:Observable>
    </stix:Observables>
</stix:STIX_Package>
```

- 開放式威脅交換 (OTX)™ CSV

  此格式同時支援 CIDR 區塊和個別 IP 地址。下列範例清單使用 OTX™ CSV 格式。

```
Indicator type, Indicator, Description
```

```
CIDR, 192.0.2.0/24, example
IPv4, 198.51.100.1, example
IPv4, 203.0.113.1, example
```

- FireEye威脅情報

  此格式同時支援 CIDR 區塊和個別 IP 地址。下列範例清單使用 FireEye™ CSV 格式。

```
reportId, title, threatScape, audience, intelligenceType, publishDate, reportLink,
 webLink, emailIdentifier, senderAddress, senderName, sourceDomain, sourceIp,
 subject, recipient, emailLanguage, fileName, fileSize, fuzzyHash, fileIdentifier,
 md5, sha1, sha256, description, fileType, packer, userAgent, registry,
 fileCompilationDateTime, filePath, asn, cidr, domain, domainTimeOfLookup,
 networkIdentifier, ip, port, protocol, registrantEmail, registrantName, networkType,
 url, malwareFamily, malwareFamilyId, actor, actorId, observationTime

01-00000001, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000001, https://www.example.com/
report/01-00000001, , , , , , , , , , , , , , , , , , , , , , , , , , , , , 192.0.2.0/24, , ,
 Related, , , , , , network, , Ursnif, 21a14673-0d94-46d3-89ab-8281a0466099, , ,
 1494944400

01-00000002, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000002, https://www.example.com/
report/01-00000002, , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , Related,
 198.51.100.1, , , , , network, , Ursnif,
 12ab7bc4-62ed-49fa-99e3-14b92afc41bf, , ,1494944400

01-00000003, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000003, https://www.example.com/
report/01-00000003, , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , Related,
 203.0.113.1, , , , , network, , Ursnif, 8a78c3db-7bcb-40bc-a080-75bd35a2572d, , ,
 1494944400
```

- Proofpoint™ ET 情報饋送 CSV

  此格式僅支援個別 IP 地址。下列範例清單使用 Proofpoint CSV 格式。ports 為選用參數。如果跳過連接埠，請務必在結尾留下尾隨逗號 (,)。

```
ip, category, score, first_seen, last_seen, ports (|)
198.51.100.1, 1, 100, 2000-01-01, 2000-01-01,
203.0.113.1, 1, 100, 2000-01-01, 2000-01-01, 80
```

- AlienVault™ 信譽摘要

  此格式僅支援個別 IP 地址。下列範例清單使用 AlienVault 格式。

```
198.51.100.1#4#2#Malicious Host#US##0.0,0.0#3
203.0.113.1#4#2#Malicious Host#US##0.0,0.0#3
```

上傳信任 IP 清單和威脅清單所需的許可

各種 IAM 身分都需要特殊許可才能與中的受信任 IP 清單和威脅清單搭配使用 GuardDuty。具有連接的 AmazonGuardDutyFullAccess 受管政策的身分，只能重新命名和停用上傳的信任 IP 清單和威脅清單。

若要授予各種身分使用信任 IP 清單和威脅清單 (除了重新命名和停用，還包括新增、啟用、刪除和更新清單的位置或名稱) 的完整存取權限，請確認以下動作存在於連接至使用者、群組或角色的許可政策中：

```
{
    "Effect": "Allow",
    "Action": [
        "iam:PutRolePolicy",
        "iam:DeleteRolePolicy"
    ],
    "Resource": "arn:aws:iam::555555555555:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
}
```

> **Important**
>
> 這些動作不包含在 AmazonGuardDutyFullAccess 受管政策中。

對信任 IP 清單和威脅清單使用伺服器端加密

GuardDuty 支援下列清單的加密類型：SSE-AES256 和 SSE-KMS。不支援 SSE-C。如需有關 S3 的加密類型的詳細資訊，請參閱使用伺服器端加密保護資料。

如果您的清單使用伺服器端加密 SSE-KMS 加密，您必須授與 GuardDuty 服務連結角色的AWSServiceRoleForAmazonGuardDuty權限，才能解密檔案，才能啟用清單。將下列陳述式新增至 KMS 金鑰政策，並使用您的帳戶 ID 取代其中的帳戶 ID：

```
{
    "Sid": "AllowGuardDutyServiceRole",
    "Effect": "Allow",
    "Principal": {
    "AWS": "arn:aws:iam::123456789123:role/aws-service-role/guardduty.amazonaws.com/
AWSServiceRoleForAmazonGuardDuty"
    },
    "Action": "kms:Decrypt*",
    "Resource": "*"
}
```

新增和啟用信任 IP 清單或威脅 IP 清單

選擇下列其中一種存取方法，以新增並啟用信任 IP 清單或威脅 IP 清單。

Console

(選用) 步驟 1：擷取清單的位置 URL

1. 前往 https://console.aws.amazon.com/s3/ 開啟的 Amazon Simple Storage Service (Amazon S3) 主控台。
2. 在導覽窗格中，選擇 儲存貯體。
3. 選擇 Amazon S3 儲存貯體名稱，其中包含您要新增的特定清單。
4. 選擇物件 (清單) 名稱以檢視其詳細資訊。
5. 在屬性索引標籤下，複製此物件的 S3 URI。

步驟 2：新增信任 IP 清單或威脅清單

> **Important**
>
> 依預設，在任何指定的時間點，您只能擁有一個信任 IP 清單。同樣地，您可以有最多六個威脅清單。

1. 開啟主 GuardDuty 控台，網址為 https://console.aws.amazon.com/guardduty/。

2. 在導覽窗格中，選擇清單。
3. 在清單管理頁面上，選擇新增信任 IP 清單或新增威脅清單。
4. 根據您的選擇，將出現一個對話框。執行以下步驟：

   a. 針對清單名稱，輸入清單的名稱。

      清單命名條件約束 — 清單名稱可包括小寫字母、大寫字母、數字、破折號 (-) 和底線 (_)。

   b. 針對位置，提供您上傳清單的位置。如果您尚未擁有位置，請參閱Step 1: Fetching location URL of your list。

      位置 URL 的格式

      - https://s3.amazonaws.com/bucket.name/file.txt
      - https://s3-aws-region.amazonaws.com/bucket.name/file.txt
      - http://bucket.s3.amazonaws.com/file.txt
      - http://bucket.s3-aws-region.amazonaws.com/file.txt
      - s3://bucket.name/file.txt

   c. 選取我同意核取方塊。

   d. 選擇新增清單。依預設，新增清單的狀態為非作用中。若要使清單生效，您必須啟用清單。

步驟 3：啟用信任 IP 清單或威脅清單

1. 開啟主 GuardDuty 控台，網址為 https://console.aws.amazon.com/guardduty/。
2. 在導覽窗格中，選擇清單。
3. 在清單管理頁面上，選取您要啟用的清單。
4. 選擇動作，然後選擇啟用。最多可能需要 15 分鐘的時間才能生效。

API/CLI

針對信任 IP 清單

- 執行 CreateIPSet。請務必提供您要為其建立此信任 IP 清單之成員帳戶的 `detectorId`。

  清單命名條件約束 — 清單名稱可包括小寫字母、大寫字母、數字、破折號 (-) 和底線 (_)。

- 或者，您可以執行下列 AWS Command Line Interface 命令來完成此操作，並務必使用您要更新信任 IP 清單之成員帳戶的偵測器 ID 來取代 `detector-id`。

```
aws guardduty create-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --name AnyOrganization List --format Plaintext --location https://
s3.amazonaws.com/DOC-EXAMPLE-BUCKET2/DOC-EXAMPLE-SOURCE-FILE.format --
activate
```

針對威脅清單

- 執行 CreateThreatIntelSet。請務必提供您要為其建立此威脅清單之成員帳戶的 `detectorId`。
  - 或者，您也可以執行下列 AWS Command Line Interface 命令來執行此操作。請務必提供您要為其建立威脅清單之成員帳戶的 `detectorId`。

```
aws guardduty create-threat-intel-set --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --name AnyOrganization List --
format Plaintext --location https://s3.amazonaws.com/DOC-EXAMPLE-BUCKET2/
DOC-EXAMPLE-SOURCE-FILE.format --activate
```

> **Note**
>
> 啟用或更新任何 IP 清單後，最多 GuardDuty 可能需要 15 分鐘才能同步處理清單。

更新信任 IP 清單和威脅清單

您可以更新清單的名稱，或更新已新增並啟用之清單的新增 IP 地址。如果您更新清單，您必須再次啟動清單， GuardDuty 才能使用最新版本的清單。

選擇其中一種存取方法來更新信任 IP 清單或威脅清單。

Console

1. 開啟主 GuardDuty 控台，網址為 https://console.aws.amazon.com/guardduty/。
2. 在導覽窗格中，選擇清單。
3. 在清單管理頁面上，選取您要更新的信任 IP 集或威脅清單。

4. 選擇動作，然後選擇編輯。
5. 在更新清單對話方塊中，視需要更新資訊。

   清單命名條件約束 — 清單名稱可包括小寫字母、大寫字母、數字、破折號 (-) 和底線 (_)。
6. 選中我同意核取方塊，然後選擇更新清單。狀態資料欄中的值將變更為非作用中。
7. 重新啟用更新後的清單

   a. 在清單管理頁面上，選取您要再次啟用的清單。

   b. 選擇動作，然後選擇啟用。

API/CLI

1. 執行 UpdateIPSet 以更新信任 IP 清單。
   - 或者，您可以執行下列 AWS CLI 命令來更新信任 IP 清單，並務必使用更新信任 IP 清單之成員帳戶的偵測器 ID 取代 `detector-id`。

   ```
   aws guardduty update-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0
    --name AnyOrganization List --ip-set-id d4b94fc952d6912b8f3060768example --
   activate
   ```
2. 執行 UpdateThreatIntelSet 以更新威脅清單
   - 或者，您可以執行下列 AWS CLI 命令來更新威脅清單，並務必使用更新威脅清單之成員帳戶的偵測器 ID 取代 `detector-id`。

   ```
   aws guardduty update-threatintel-set --detector-
   id 12abc34d567e8fa901bc2d34e56789f0 --name AnyOrganization List --threat-
   intel-set-id d4b94fc952d6912b8f3060768example --activate
   ```

停用或刪除信任 IP 清單或威脅清單

選擇其中一種存取方法，以刪除 (使用主控台) 或停用 (使用 API/CLI) 信任 IP 清單或威脅清單。

Console

1. 開啟主 GuardDuty 控台，網址為 https://console.aws.amazon.com/guardduty/。
2. 在導覽窗格中，選擇清單。
3. 在清單管理頁面上，選取您要刪除的清單。

4. 選擇動作，然後選擇刪除。
5. 確認動作，然後選擇刪除。特定清單將不再可用於表格中。

API/CLI

1. 針對信任 IP 清單

   執行 UpdateIPSet 以更新信任 IP 清單。

   - 或者，您可以執行下列 AWS CLI 命令來更新信任 IP 清單，並務必使用更新信任 IP 清單之成員帳戶的偵測器 ID 取代 `detector-id`。

     要查找您`detectorId`的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

     ```
     aws guardduty update-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0
      --name AnyOrganization List --ip-set-id d4b94fc952d6912b8f3060768example --
     no-activate
     ```

2. 針對威脅清單

   執行 UpdateThreatIntelSet 以更新威脅清單

   - 或者，您可以執行下列 AWS CLI 命令來更新信任 IP 清單，並務必使用更新威脅清單之成員帳戶的偵測器 ID 取代 `detector-id`。

     ```
     aws guardduty update-threatintel-set --detector-
     id 12abc34d567e8fa901bc2d34e56789f0 --name AnyOrganization List --threat-
     intel-set-id d4b94fc952d6912b8f3060768example --no-activate
     ```

匯出調查結果

GuardDuty 保留產生的發現項目為期 90 天。 GuardDuty 將活動發現導出到 Amazon EventBridge（ EventBridge ）。您可以選擇將產生的發現結果匯出到 Amazon Simple Storage Service (Amazon S3) 儲存貯體。這可協助您追蹤帳戶中潛在可疑活動的歷史資料，並評估建議的補救步驟是否成功。

GuardDuty 產生的任何新作用中發現項目會在產生搜尋結果後約 5 分鐘內自動匯出。您可以設定匯出使用中發現項目的更新頻率 EventBridge。您選取的頻率適用於將現有發現項目的新發現項目匯出至 EventBridge、S3 儲存貯體 (設定時) 和 Detective (整合時)。如需如何 GuardDuty 彙總多個現有發現項目的相關資訊，請參閱GuardDuty 尋找彙總。

當您設定設定以將發現項目匯出到 Amazon S3 儲存貯體時，請 GuardDuty 使用 AWS Key Management Service (AWS KMS) 來加密 S3 儲存貯體中的發現項目資料。這需要您將許可新增到 S3 儲存貯體和 AWS KMS 金鑰， GuardDuty 以便使用它們匯出帳戶中的發現項目。

目錄

考量事項

繼續匯出發現項目的先決條件和步驟之前，請考慮下列主要概念：

- 匯出設定為區域性 — 您必須在使用的每個區域中設定匯出選項 GuardDuty。
- 將發現項目匯出到不同 AWS 區域 (跨區域) 的 Amazon S3 儲存貯體 — GuardDuty 支援下列匯出設定：
  - 您的 Amazon S3 儲存貯體或物件和 AWS KMS 金鑰必須屬於同一個儲存貯體或物件 AWS 區域。
  - 對於在商業區域產生的發現項目，您可以選擇將這些發現項目匯出到任何商業區域的 S3 儲存貯體。但是，您無法將這些發現項目匯出到選擇加入區域中的 S3 儲存貯體。
  - 對於在選擇加入區域中產生的發現項目，您可以選擇將這些搜尋結果匯出至產生這些搜尋結果的相同選擇加入區域或任何商業區域。但是，您無法將搜尋結果從一個選擇加入的區域匯出到另一個選擇加入區域。
- 匯出發現項目的權限 — 若要設定匯出作用中發現項目的設定，S3 儲存貯體必須具有允許 GuardDuty 上傳物件的許可。您也必須擁有 GuardDuty 可用來加密發現項目的 AWS KMS 金鑰。
- 不會匯出已封存的發現項目 — 預設行為是不會匯出已封存的發現項目 (包括隱藏發現項目的新例項)。

  若要匯出已封存的搜尋結果，您必須將其取消封存。這會將其狀態變更為「作用中」。根據匯出頻率，發現項目將匯出到設定的 S3 儲存貯體。
- GuardDuty 管理員帳戶可以匯出關聯成員帳戶中產生的發現項目 — 當您在管理員帳戶中設定匯出發現項目時，在相同區域中產生的關聯成員帳戶中的所有發現項目也會匯出至您為管理員帳戶設定的相同位置。如需詳細資訊，請參閱 了解管理員帳戶和成 GuardDuty 員帳戶之間的關係。

步驟 1 — 匯出發現項目所需的權限

設定匯出發現項目的設定時，您可以選取 Amazon S3 儲存貯體，您可以在其中存放發現項目和用於資料加密的 AWS KMS 金鑰。除了 GuardDuty 動作的權限之外，您還必須擁有下列動作的權限，才能成功設定匯出發現項目的設定：

- S3：GetBucketLocation
- S3：PutObject

步驟 2 — 將政策附加到您的 KMS 金鑰

GuardDuty 使 AWS Key Management Service用加密值區中的發現項目資料。若要成功設定，您必須先授與使用 KMS 金鑰的 GuardDuty 權限。您可以透過將政策連接至 KMS 金鑰來授予許可。

當您使用其他帳戶的 KMS 金鑰時，您需要登入擁有 AWS 帳戶 該金鑰的金鑰來套用金鑰原則。當您設定匯出發現項目的設定時，您也需要擁有金鑰的帳戶中的金鑰 ARN。

修改用 GuardDuty 於加密匯出發現項目的 KMS 金鑰原則

1. 請在以下位置開啟 AWS KMS 主控台。 https://console.aws.amazon.com/kms
2. 若要變更 AWS 區域，請使用頁面右上角的「地區」選取器。
3. 在AWS Key Management Service 開發人員指南中選取現有的 KMS 金鑰或執行步驟以建立新金鑰，您將使用該金鑰來加密匯出的發現項目。

   > **Note**
   >
   > 您 AWS 區域 的 KMS 金鑰和 Amazon S3 儲存貯體必須相同。

   您可以使用相同的 S3 儲存貯體和 KMS key pair，從任何適用的區域匯出發現項目。如需詳細資訊，請參閱跨區域匯考量事項出發現項目的資訊。
4. 在 Key policy (金鑰政策) 區段中，選擇 Edit (編輯)。

   如果顯示 [切換至原則檢視]，請選擇它來顯示 [金鑰] 原則，然後選擇 [編輯]。
5. 將下列原則區塊複製到您的 KMS 金鑰原則，以授與使用金鑰的 GuardDuty 權限。

```
{
    "Sid": "AllowGuardDutyKey",
```

```
    "Effect": "Allow",
    "Principal": {
        "Service": "guardduty.amazonaws.com"
    },
    "Action": "kms:GenerateDataKey",
    "Resource": "KMS key ARN",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "123456789012",
            "aws:SourceArn":
 "arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"
        }
    }
}
```

6. 透過取代下列在策略範例中以##格式化的值來編輯策略：

   1. 將 *KMS ## ARN* 取代為 KMS 金鑰的 Amazon 資源名稱 (ARN)。若要找出金鑰 ARN，請參閱AWS Key Management Service 開發人員指南中的尋找金鑰 ID 和 ARN。
   2. 將 *123456789012* 取代為擁有匯出發現項目之 AWS 帳戶 帳戶的識別碼。 GuardDuty
   3. 將 *Region 2* 取代為產生 GuardDuty 發現項目的 AWS 區域 位置。
   4. 將 *SourceDetectorID* 取代為產生發現項目之特定區域中 GuardDuty 帳戶detectorID的 ID。

      要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

   > **Note**
   >
   > 如果您 GuardDuty 在選擇加入的區域中使用，請將「服務」的值替換為該區域的區域端點。例如，如果您 GuardDuty 在中東（巴林）（me-south-1）區域中使用，請替換"Service": "guardduty.amazonaws.com"為. "Service": "guardduty.me-south-1.amazonaws.com" 如需每個選擇加入區域之端點的相關資訊，請參閱GuardDuty 端點和配額。

7. 如果您在最終陳述式之前加入政策陳述式，請在新增此陳述式之前加上逗號。請確定 KMS 金鑰原則的 JSON 語法有效。

   選擇儲存。

8. (選擇性) 將金鑰 ARN 複製到記事本，以便在稍後的步驟中使用。

步驟 3 — 將政策附加到 Amazon S3 存儲桶

將許可新增至要匯出發現項目的 Amazon S3 儲存貯體， GuardDuty 以便將物件上傳到此 S3 儲存貯體。與使用屬於您帳戶或其他帳戶的 Amazon S3 儲存貯體無關 AWS 帳戶，您必須新增這些許可。

如果您決定在任何時間點將發現項目匯出到不同的 S3 儲存貯體，則若要繼續匯出發現項目，您必須將許可新增至該 S3 儲存貯體，然後再次設定匯出發現項目設定。

如果您還沒有要匯出這些發現項目的 Amazon S3 儲存貯體，請參閱 Amazon S3 使用者指南中的建立儲存貯體。

將許可附加到 S3 儲存貯體政策

1. 執行 Amazon S3 使用者指南中建立或編輯儲存貯體政策下的步驟，直到出現「編輯儲存貯體政策」頁面為止。
2. 範例政策顯示如何 GuardDuty 授與將發現結果匯出到 Amazon S3 儲存貯體的權限。如果您在設定匯出發現項目之後變更路徑，則必須修改原則以授與新位置的權限。

   複製下列範例政策，並將其貼到值區政策編輯器中。

   如果您在最終陳述式之前加入政策陳述式，請在新增此陳述式之前加上逗號。請確定 KMS 金鑰原則的 JSON 語法有效。

   S3 儲存貯體範例政策

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowGuardDutygetBucketLocation",
            "Effect": "Allow",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:GetBucketLocation",
            "Resource": "Amazon S3 bucket ARN",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012",
```

```
                    "aws:SourceArn":
"arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"

                }
            }
        },
        {
            "Sid": "AllowGuardDutyPutObject",
            "Effect": "Allow",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012",
                    "aws:SourceArn":
"arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"

                }
            }
        },
        {
            "Sid": "DenyUnencryptedUploadsThis is optional",
            "Effect": "Deny",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-server-side-encryption": "aws:kms"
                }
            }
        },
        {
            "Sid": "DenyIncorrectHeaderThis is optional",
            "Effect": "Deny",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
```

```
            "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-server-side-encryption-aws-kms-key-id": "KMS key ARN"
                }
            }
        },
        {
            "Sid": "DenyNon-HTTPS",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            }
        }
    ]
}
```

3. 透過取代下列在策略範例中以##格式化的值來編輯策略：

    1. 將 *Amazon S3 #### ARN* 取代為 Amazon S3 儲存貯體的亞馬遜資源名稱 (ARN)。您可以在 https://console.aws.amazon.com/s3/ 主控台的 「編輯值區政策」頁面上找到「儲存貯體 ARN」。
    2. 將 *123456789012* 取代為擁有匯出發現項目之 AWS 帳戶 帳戶的識別碼。 GuardDuty
    3. 將 *Region 2* 取代為產生 GuardDuty 發現項目的 AWS 區域 位置。
    4. 將 *SourceDetectorID* 取代為產生發現項目之特定區域中 GuardDuty 帳戶`detectorID`的 ID。

        要查找您`detectorId`的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。
    5. 將 *S3 #### ARN/ [####] ###### [####]* 部分取代為您要匯出發現項目的選用資料夾位置。如需有關使用前置詞的詳細資訊，請參閱 Amazon S3 使用者指南中的使用前置詞組織物件。

當您提供不存在的選用資料夾位置時，只有在與 S3 儲存貯體關聯的帳戶與匯出發現項目的帳戶相同時，才 GuardDuty會建立該位置。當您將發現項目匯出到屬於另一個帳戶的 S3 儲存貯體時，資料夾位置必須已經存在。

6. 將 *KMS ## ARN* 取代為與匯出至 S3 儲存貯體的發現項目加密相關聯的 KMS 金鑰的 Amazon 資源名稱 (ARN)。若要找出金鑰 ARN，請參閱AWS Key Management Service 開發人員指南中的尋找金鑰 ID 和 ARN。

> **Note**
>
> 如果您 GuardDuty 在選擇加入的區域中使用，請將「服務」的值替換為該區域的區域端點。例如，如果您 GuardDuty 在中東（巴林）（me-south-1）區域中使用，請替換`"Service": "guardduty.amazonaws.com"`為. `"Service": "guardduty.me-south-1.amazonaws.com"` 如需每個選擇加入區域之端點的相關資訊，請參閱GuardDuty 端點和配額。

4. 選擇儲存。

步驟 4-將發現結果導出到 S3 存儲桶（控制台）

GuardDuty 允許您將發現結果匯出至另一個儲存貯體中的現有值區 AWS 帳戶。

在您的帳戶中建立新的 S3 儲存貯體或選擇現有儲存貯體時，您可以新增選用的前置詞。設定匯出發現項目時，請在 S3 儲存貯體中為您的發現項目 GuardDuty 建立新資料夾。字首將附加至建立的預設資料 GuardDuty 夾結構。例如，可選前綴的格式`/AWSLogs/`*`123456789012`*`/GuardDuty/`*`Region`*。

S3 物件的整個路徑將是*`DOC-EXAMPLE-BUCKET`*`/`*`prefix-name`*`/UUID`*`.jsonl.gz`*。UUID是隨機產生的，不代表偵測器 ID 或尋找 ID。

> **Important**
>
> KMS 金鑰和 S3 儲存貯體必須位於同一區域。

在完成這些步驟之前，請確定已將個別政策附加到 KMS 金鑰和現有 S3 儲存貯體。

設定匯出發現項目

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/
2. 在導覽窗格中，選擇設定。
3. 在 [設定] 頁面的 [發現項目匯出選項] 下，對於 S3 儲存貯體，選擇 [立即設定] (或視需要編輯)。
4. 對於 S3 儲存貯體 ARN，請輸入**bucket ARN**. 若要尋找儲存貯體 ARN，請參閱 Amazon S3 使用者指南中的檢視 S3 儲存貯體的屬性。在 https://console.aws.amazon.com/guardduty/ 主控台中相關值區「內容」頁面的「權限」索引標籤中。
5. 對於 KMS 金鑰 ARN，請輸入 **key ARN**. 若要找出金鑰 ARN，請參閱AWS Key Management Service 開發人員指南中的尋找金鑰 ID 和 ARN。
6. 附加策略
   - 執行附加 S3 儲存貯體政策的步驟。如需詳細資訊，請參閱 步驟 3 — 將政策附加到 Amazon S3 存儲桶。
   - 執行附加 KMS 金鑰原則的步驟。如需詳細資訊，請參閱 步驟 2 — 將政策附加到您的 KMS 金鑰。
7. 選擇 Save (儲存)。

步驟 5 — 設定匯出更新的使用中發現項目的頻率

視您的環境設定匯出更新作用中發現項目的頻率。根據預設，每 6 小時匯出更新的問題清單。這表示任何在最近一次匯出之後更新的問題清單都會包含在下一個的匯出中。如果每 6 小時匯出更新的問題清單，且匯出在 12:00 進行，則您在 12:00 之後更新的任何問題清單都會在 18:00 匯出。

設定頻率

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/
2. 選擇設定。
3. 在調查結果匯出選項區段中，選擇更新後的調查結果的頻率。這會設定將更新的作用中發現項目匯出至 EventBridge 和 Amazon S3 的頻率。您可以選擇下列項目：
   - 每 15 分鐘更新一次 EventBridge 和 S3
   - 每 1 小時更新一次 EventBridge 和 S3
   - Update CWE and S3 every 6 hours (default) (每 6 小時更新 CWE 和 S3 (預設值))

4. 選擇儲存變更。

使用 Amazon CloudWatch 活動建立自訂回應的 GuardDuty 發現項目

GuardDuty 當發現項目發生任何變更時，會為 Amazon CloudWatch 活動建立事件。尋找將建立 CloudWatch 事件的變更包括新產生的發現項目或新彙總的發現項目。盡可能發出事件。

每個 GuardDuty 發現項目都會指派一個尋找 ID。 GuardDuty 使用唯 CloudWatch 一的尋找項目 ID 為每個尋找項目建立事件。所有後續出現的現有調查結果都會彙總至原始調查結果。如需詳細資訊，請參閱 GuardDuty 尋找彙總。

> **Note**
>
> 如果您的帳戶是 GuardDuty 委派的系統管理員，則會將 CloudWatch 事件發佈到您的帳戶以及產生發現項目的成員帳戶。

透過搭配使用 CloudWatch 事件 GuardDuty，您可以自動化工作，以協助您回應 GuardDuty 發現項目所揭露的安全性問題。

若要接收根據「 CloudWatch 事件」 GuardDuty 發現項目的相關通知，您必須建立「 CloudWatch 事件」規則和目標 GuardDuty。此規則可 CloudWatch 讓您將 GuardDuty 產生之發現項目的通知傳送至規則中指定的目標。如需詳細資訊，請參閱 為 GuardDuty (CLI) 建立 CloudWatch 事件規則和目標。

主題

- CloudWatch 事件通知頻率 GuardDuty
- CloudWatch 事件格式 GuardDuty
- 建立 CloudWatch 事件規則以通知您 GuardDuty 發現項目 (主控台)
- 為 GuardDuty (CLI) 建立 CloudWatch 事件規則和目標
- CloudWatch 適用於 GuardDuty 多帳戶環境的活動

CloudWatch 事件通知頻率 GuardDuty

針對具有唯一調查結果 ID 的新產生調查結果的通知

GuardDuty 在發現後的 5 分鐘內根據其 CloudWatch 事件發送通知。由於產生了此具有唯一 ID 的調查結果，此事件 (以及此通知) 也包括在前 5 分鐘內所有後續出現的此調查結果。

> **Note**
>
> 依預設，新產生調查結果的通知頻率為 5 分鐘。此頻率無法更新。

後續出現的調查結果的通知

根據預設，對於具有唯一尋找項目 ID 的每個發現項目，都會將 6 小時間隔內發生之特定尋找項目類型的所有後續發生項目 GuardDuty 彙總為單一事件。 GuardDuty 然後根據此事件發送有關這些後續事件的通知。依預設，對於現有發現項目的後續發生項目，每 6 小時會根據 CloudWatch 事件 GuardDuty 傳送通知。

只有管理員帳戶帳戶可以自訂傳送有關事件後續發現 CloudWatch 事件發生次數的通知預設頻率。成員帳戶的使用者無法自訂此頻率。系統管理員帳戶在其自己帳戶中設定的頻率值會強加在其所有成員帳戶的 GuardDuty功能上。如果來自管理員帳戶帳戶的使用者將此頻率值設定為 1 小時，則所有成員帳戶也會以 1 小時的頻率接收有關後續發現項目的通知。如需詳細資訊，請參閱 在 Amazon 管理多個帳戶 GuardDuty。

> **Note**
>
> 身為管理員帳戶，您可以自訂有關後續發現事件的預設通知頻率。可能的值有 15 分鐘、1 小時或預設的 6 小時。如需有關設定這些通知頻率的資訊，請參閱步驟 5 — 設定匯出更新的使用中發現項目的頻率。

使用事件監視封存的 GuardDuty CloudWatch 發現

針對手動封存的發現項目，這些發現項目的初始與後續發現項目 (在封存完成之後產生) 都會傳送至上述每個頻率的 CloudWatch 事件。

對於自動存檔的發現項目，這些發現項目的初始和所有後續發現項目 (在封存完成之後產生) 都不會傳送至 CloudWatch 事件。

CloudWatch 事件格式 GuardDuty

的 CloudWatch 事件 GuardDuty 具有下列格式。

```
{
 "version": "0",
 "id": "cd2d702e-ab31-411b-9344-793ce56b1bc7",
 "detail-type": "GuardDuty Finding",
 "source": "aws.guardduty",
 "account": "111122223333",
 "time": "1970-01-01T00:00:00Z",
 "region": "us-east-1",
 "resources": [],
 "detail": {GUARDDUTY_FINDING_JSON_OBJECT}
}
```

> **Note**
>
> 詳細資訊值作為物件返回單一調查結果的 JSON 詳細資訊，而不是返回可支援陣列中多個調查結果的「調查結果」值。

如需包含在 GUARDDUTY_FINDING_JSON_OBJECT 中全部參數的完整清單，請參閱 GetFindings。在 GUARDDUTY_FINDING_JSON_OBJECT 中出現的 id 參數，即為之前描述的調查結果 ID。

建立 CloudWatch 事件規則以通知您 GuardDuty 發現項目 (主控台)

您可以 GuardDuty 將 CloudWatch 事件與搭配使用，藉由將尋找事件傳送至訊息中樞來設定自動 GuardDuty尋找警示，以協助提高發 GuardDuty 現項目的可見度。本主題說明如何透過設定 SNS 主題，然後將該主題連接至事件事件規則，將發現項目警示傳送至電子郵 CloudWatch 件、Slack 或 Amazon Chime。

設定 Amazon SNS 主題和端點

首先，您必須先在 Amazon Simple Notification Service 中設定主題並新增端點。如需詳細資訊，請參閱《Amazon Simple Notification Service 開發人員指南》中的入門。

此程序會建立您要傳送 GuardDuty 尋找資料的位置。在建立 CloudWatch 事件規則期間或之後，可將 SNS 主題新增至「事件事件」規則。

Email setup

建立 SNS 主題

1. 登入 Amazon SNS 主控台，網址為 https://console.aws.amazon.com/sns/v3/home。
2. 從瀏覽窗格選取主題，然後選取 建立主題。
3. 在「建立主題」區段中，選取標準。接下來，輸入主題名稱 (例如 **GuardDuty_to_Email**)。其他詳細資料是選擇性的。
4. 選擇建立主題。新主題的主題詳細資料隨即開啟。
5. 在訂閱區段中，選取建立訂閱
6. a. 從通訊協定功能表中，選取電子郵件。
   b. 在端點欄位中，新增您想要接收通知的電子郵件地址。

   > **Note**
   >
   > 建立後，您需要透過您的電子郵件使用者端確認訂閱。

   c. 選擇建立訂閱
7. 查看收件匣中的訂閱郵件，然後選擇確認訂閱

Slack setup

建立 SNS 主題

1. 登入 Amazon SNS 主控台，網址為 https://console.aws.amazon.com/sns/v3/home。
2. 從瀏覽窗格選取主題，然後選取 建立主題。
3. 在「建立主題」區段中，選取標準。接下來，輸入主題名稱 (例如 **GuardDuty_to_Slack**)。其他詳細資料是選擇性的。選擇建立主題以完成。

設定 AWS Chatbot 用戶端

1. 導覽至 AWS Chatbot 主控台
2. 從設定的用戶端面板中，選取設定新用戶端。
3. 選擇 Slack 並按「設定」進行確認。

> **Note**
>
> 選擇 Slack 時，您必須透過選取「允許」來確認 AWS Chatbot 存取頻道的許可。

4. 選取設定新頻道以開啟組態詳細資訊窗格。
   a. 輸入頻道的名稱。
   b. 對於 Slack 頻道，選擇要使用的頻道。若要搭配 AWS Chatbot 使用私有 Slack 頻道，請選擇「私有頻道」。
   c. 在 Slack 中，以滑鼠右鍵按一下頻道名稱並選取「複製連結」，以複製私有頻道的頻道 ID。
   d. 在 AWS 管理主控台的 AWS Chatbot 視窗中，將您從 Slack 複製的 ID 貼到「私有頻道 ID」欄位中。
   e. 在許可中，如果您還沒有角色，則選擇使用範本建立 IAM 角色。
   f. 在政策範本中，選擇「通知許可」。這是 AWS Chatbot 的 IAM 政策範本。它為 CloudWatch 警示、事件和日誌以及 Amazon SNS 主題提供必要的讀取和列出許可。
   g. 選擇您先前在其中建立 SNS 主題的區域，然後選取您建立的 Amazon SNS 主題，將通知傳送至 Slack 頻道。
5. 選取設定。

Chime setup

建立 SNS 主題

1. 登入 Amazon SNS 主控台，網址為 https://console.aws.amazon.com/sns/v3/home。
2. 從瀏覽窗格選取主題，然後選取 建立主題。
3. 在「建立主題」區段中，選取標準。接下來，輸入主題名稱 (例如 **`GuardDuty_to_Chime`**)。其他詳細資料是選擇性的。選擇建立主題以完成。

設定 AWS Chatbot 用戶端

1. 導覽至 AWS Chatbot 主控台
2. 從設定的用戶端面板中，選取設定新用戶端。
3. 選擇 Chime 並按「設定」進行確認。

4. 在組態詳細資訊窗格中，輸入頻道的名稱。
5. 在 Chime 中開啟所需的聊天室

   a. 選擇右上角的齒輪圖示，然後選擇管理 Webhook 和機器人。

   b. 選取複製 URL，將 Webhook URL 複製到剪貼簿。
6. 在 AWS 管理主控台的 AWS Chatbot 視窗中，將您複製的 URL 貼到 Webhook URL 欄位中。
7. 在許可中，如果您還沒有角色，則選擇使用範本建立 IAM 角色。
8. 在政策範本中，選擇「通知許可」。這是 AWS Chatbot 的 IAM 政策範本。它為 CloudWatch 警示、事件和日誌以及 Amazon SNS 主題提供必要的讀取和列出許可。
9. 選擇您先前在其中建立 SNS 主題的區域，然後選取您建立的 Amazon SNS 主題，將通知傳送至 Chime 聊天室。
10. 選取設定。

設定發 GuardDuty現項目的 CloudWatch 事件

1. 請在以下位置開啟 CloudWatch 主控台。 https://console.aws.amazon.com/cloudwatch/
2. 從導覽窗格選取規則，然後選取建立規則。
3. 從「服務名稱」功能表中選擇GuardDuty。
4. 從「事件型態」功能表選擇「GuardDuty搜尋結果」。
5. 在事件模式預覽中，選擇編輯。
6. 將下面的 JSON 程式碼貼到事件模式預覽中，然後選擇儲存

```
{
  "source": [
    "aws.guardduty"
  ],
  "detail-type": [
    "GuardDuty Finding"
  ],
  "detail": {
    "severity": [
      4,
      4.0,
      4.1,
      4.2,
      4.3,
      4.4,
```

```
        4.5,
        4.6,
        4.7,
        4.8,
        4.9,
        5,
        5.0,
        5.1,
        5.2,
        5.3,
        5.4,
        5.5,
        5.6,
        5.7,
        5.8,
        5.9,
        6,
        6.0,
        6.1,
        6.2,
        6.3,
        6.4,
        6.5,
        6.6,
        6.7,
        6.8,
        6.9,
        7,
        7.0,
        7.1,
        7.2,
        7.3,
        7.4,
        7.5,
        7.6,
        7.7,
        7.8,
        7.9,
        8,
        8.0,
        8.1,
        8.2,
        8.3,
        8.4,
```

```
      8.5,
      8.6,
      8.7,
      8.8,
      8.9
    ]
  }
}
```

> **Note**
>
> 上面的程式碼會提醒任何「中」至「高」調查結果。

7. 在目標區段中，按一下新增目標。
8. 從選取目標功能表中，選擇 SNS 主題。
9. 針對選取主題，請選取您在步驟 1 中建立的 SNS 主題名稱。
10. 設定事件的輸入。

    - 如果您要設定 Chime 或 Slack 的通知，請跳至步驟 11，輸入類型預設為符合的事件。
    - 如果您要透過 SNS 設定電子郵件通知，請遵循下列步驟，使用下列步驟自訂傳送至收件匣的郵件：

    a. 展開設定輸入，然後選擇輸入轉換器。

    b. 複製下列程式碼並貼到輸入路徑欄位中。

```
{
    "severity": "$.detail.severity",
    "Account_ID": "$.detail.accountId",
    "Finding_ID": "$.detail.id",
    "Finding_Type": "$.detail.type",
    "region": "$.region",
    "Finding_description": "$.detail.description"
}
```

    c. 複製下列程式碼並貼到 輸入範本欄位，以格式化電子郵件。

```
"AWS <Account_ID> has a severity <severity> GuardDuty finding type
 <Finding_Type> in the <region> region."
"Finding Description:"
"<Finding_description>. "
"For more details open the GuardDuty console at https://console.aws.amazon.com/
guardduty/home?region=<region>#/findings?search=id%3D<Finding_ID>"
```

11. 按一下設定詳細資料。
12. 在設定規則詳細資訊頁面上，輸入規則的名稱和描述，然後選擇建立規則。

為 GuardDuty (CLI) 建立 CloudWatch 事件規則和目標

下列程序顯示如何使用AWS CLI命令建立 CloudWatch 事件規則和目標 GuardDuty。具體而言，此程序會示範如何建立規則，以 CloudWatch 便傳送所有發現項目的事件，這些發現項目 GuardDuty 會產生並將AWS Lambda函數新增為規則的目標。

> **Note**
>
> 除了 Lambda 函數之外 GuardDuty ，還 CloudWatch 支援下列目標類型：Amazon EC2 執行個體、Amazon Kinesis 串流、Amazon ECS 任務、AWS Step Functions狀態機器、run命令和內建目標。

您也可以 GuardDuty 透過「 CloudWatch 事件」主控台建立「 CloudWatch 事件」規則和目標。如需詳細資訊和詳細步驟，請參閱建立在 CloudWatch 事件上觸發的事件規則。在事件來源區段中，為服務名稱選取 **GuardDuty** 並為事件類型選取 **GuardDuty Finding**。

建立規則和目標

1. 若要為 GuardDuty產生的所有發現項目建立可 CloudWatch 傳送事件的規則，請執行下列 CloudWatch CLI 命令。

   ```
   AWS events put-rule --name Test --event-pattern "{\"source\":
   [\"aws.guardduty\"]}"
   ```

> **Important**
>
> 您可以進一步自訂規則，以便僅針對 GuardDuty產生的發現項目的子集傳送事件。CloudWatch 此部分項目是根據調查結果屬性或規則中指定的屬性而定。例如，使用下列 CLI 命令建立只能 CloudWatch 傳送嚴重性為 5 或 8 之發 GuardDuty 現項目事件的規則：
>
> ```
> AWS events put-rule --name Test --event-pattern "{\"source\":
> [\"aws.guardduty\"],\"detail-type\":[\"GuardDuty Finding\"],
> \"detail\":{\"severity\":[5,8]}}"
> ```
>
> 為此，您可以使用 JSON 中提供的任何屬性值來進行發 GuardDuty 現項目。

2. 若要將 Lambda 函數附加為您在步驟 1 中建立之規則的目標，請執行下列 CloudWatch CLI 命令。

   ```
   AWS events put-targets --rule Test --targets
   Id=1,Arn=arn:aws:lambda:us-east-1:111122223333:function:<your_function>
   ```

   > **Note**
   >
   > 確保在<your_function>上面的命令中用 GuardDuty 事件的實際 Lambda 函數替換。

3. 若要新增調用目標所需的許可，請執行以下 Lambda CLI 命令。

   ```
   AWS lambda add-permission --function-name <your_function> --statement-
   id 1 --action 'lambda:InvokeFunction' --principal events.amazonaws.com
   ```

   > **Note**
   >
   > 確保在<your_function>上面的命令中用 GuardDuty 事件的實際 Lambda 函數替換。

   > **Note**
   >
   > 在上述程序中，我們使用 Lambda 函數做為觸發 CloudWatch 事件之規則的目標。您也可以將其他AWS資源配置為觸發 CloudWatch 事件的目標。如需詳細資訊，請參閱 PutTargets。

CloudWatch 適用於 GuardDuty 多帳戶環境的活動

GuardDuty 身為管理員，您帳戶中的 CloudWatch 事件規則將根據您會員帳戶中的適用發現項目觸發。這表示，如果您透過系統管理員帳戶中的 CloudWatch 事件設定尋找通知 (如上一節所述)，則除了您自己的成員帳戶之外，還會收到通知您的成員帳戶所產生的高度和中等嚴重性發現項目。

您可以使用 GuardDuty 發現項目的 JSON 詳細資料`accountId`欄位來識別發現項目來源的成員帳戶。

若要開始在主控台中為環境中的特定成員帳戶撰寫自訂事件規則，請建立新規則並將下列範本貼到「事件模式預覽」中，然後新增要觸發事件之成員帳戶的帳戶 ID。

```
{
  "source": [
    "aws.guardduty"
  ],
  "detail-type": [
    "GuardDuty Finding"
  ],
  "detail": {
    "accountId": [
      "123456789012"
    ]
  }
}
```

> **Note**
>
> 此範例會在所列帳戶 ID 的任何調查結果上觸發。您可以新增多個 ID，並以遵循 JSON 語法的逗號分隔。

瞭解 CloudWatch 記錄檔和在惡意程式碼防護掃描期間略過資源的

GuardDuty 惡意軟體防護會將事件發佈到您的 Amazon CloudWatch 日誌群組 /aws/guardduty/malware-scan-events。對於與惡意軟體掃描相關的每個事件，您可以監控受影響資源的狀態和掃描結果。在惡意軟體防護掃描期間，某些 Amazon EC2 資源和 Amazon EBS 磁碟區可能已被略過。

GuardDuty 惡意程式碼防護中的 CloudWatch 稽核

/aws/guardduty/ malware-scan-events CloudWatch 記錄群組支援三種類型的掃描事件。

惡意軟體防護掃描事件名稱	說明
EC2_SCAN_STARTED	在 GuardDuty 惡意程式碼防護起始惡意程式碼掃描程序時建立，例如準備擷取 EBS 磁碟區的快照。
EC2_SCAN_COMPLETED	在受影響資源的至少一個 EBS 磁碟區的 GuardDuty 惡意程式碼防護掃描完成時建立。此事件也包括屬於已掃描 EBS 磁碟區的 snapshotId 。掃描完成後，掃描結果將為 CLEAN、THREATS_FOUND 或 NOT_SCANNED 。
EC2_SCAN_SKIPPED	當 GuardDuty 惡意軟體防護掃描略過受影響資源的所有 EBS 磁碟區時建立。若要識別略過原因，請選取對應的事件，然後檢視詳細資訊。如需有關略過原因的詳細資訊，請參閱以下惡意軟體掃描期間略過資源的原因。

> **Note**
>
> 如果您使用的是 AWS Organizations，則來自組 Organizations 中成員帳戶的 CloudWatch 記錄事件會發佈到系統管理員帳戶和成員帳戶的記錄群組。

選擇您偏好的存取方式來檢視和查詢 CloudWatch 事件。

Console

1. 請登入 AWS Management Console 並開啟 CloudWatch 主控台，網址為 https://console.aws.amazon.com/cloudwatch/。
2. 在導覽窗格中，選擇日誌下方的日誌群組。選擇 /aws/guardduty/ malware-scan-events 記錄群組，以檢視惡意程式碼防護的掃描事件。 GuardDuty

若要執行查詢，請選擇 Log Insights。

如需執行查詢的相關資訊，請參閱 Amazon CloudWatch 使用者指南中的使用 CloudWatch 日誌洞察分析日誌資料。

3. 選擇掃描 ID 以監控受影響資源和惡意軟體調查結果的詳細資訊。例如，您可以使用執行下列查詢來篩選 CloudWatch 記錄事件`scanId`。請務必使用您自己的有效 *`scan-id`*。

```
fields @timestamp, @message, scanRequestDetails.scanId as scanId
| filter scanId like "77a6f6115da4bd95f4e4ca398492bcc0"
| sort @timestamp asc
```

API/CLI

- 若要使用日誌群組，請參閱 Amazon 使用 CloudWatch 者指南 AWS CLI中的使用搜尋日誌項目。

  選擇 /aws/guardduty/ malware-scan-events 記錄群組，以檢視惡意程式碼防護的掃描事件。GuardDuty
- 若要檢視和篩選日誌事件 GetLogEventsFilterLogEvents，請分別參閱 Amazon CloudWatch API 參考中的和。

GuardDuty 惡意程式碼防護記錄

/aws/guardduty/ 記錄群組的預設malware-scan-events記錄保留期間為 90 天，之後會自動刪除記錄事件。若要變更記錄群組的記 CloudWatch 錄保留原則，請參閱變更 CloudWatch 記錄檔資料保留或PutRetentionPolicy。

惡意軟體掃描期間略過資源的原因

在與惡意軟體掃描相關的事件中，掃描程序期間可能略過某些 EC2 資源和 EBS 磁碟區。下表列出 GuardDuty 惡意程式碼防護可能無法掃描資源的原因。如果適用，請使用建議的步驟來解決這些問題，並在下次 GuardDuty 惡意軟體防護啟動惡意程式碼掃描時掃描這些資源。其他問題用於通知您有關事件的進展情況，並且不可採取動作。

略過的原因	說明	建議步驟	
RESOURCE_NOT_FOUND	在您的 AWS 環境中找不到resourceArn 提供給啟動隨選惡意軟體掃描的。	驗證 Amazon EC2 執行個體或容器工作負載的 resourceArn ，然後再試一次。	
ACCOUNT_INELIGIBLE	您嘗試啟動指定惡意程式碼掃描的 AWS 帳戶 ID 尚未啟用 GuardDuty。	確認 GuardDuty 此 AWS 帳戶已啟用。 當您以新的方 GuardDuty 式啟用時 AWS 區域 ，最多可能需要 20 分鐘才能同步處理。	
UNSUPPORTED_KEY_ENCRYPTION	GuardDuty 惡意程式碼防護支援未加密和使用客戶管理金鑰加密的磁碟區。其不支援掃描使用 Amazon EBS 加密進行加密的 EBS 磁碟區。 目前，這種跳過原因不適用於區域存在差異。如需這些項目的詳細資訊 AWS 區域，請參閱區域特定功能的可用性。	使用客戶自管金鑰取代您的加密金鑰。如需 GuardDuty 支援之加密類型的詳細資訊，請參閱支援用於惡意軟體掃描的 Amazon EBS 磁碟區。	
EXCLUDED_BY_SCAN_SETTINGS	在惡意軟體掃描期間，EC2 執行個體或 EBS 磁碟區已排除。有兩種可能性：標籤已新增至包含清單，但資源未與此標籤相關聯；標籤已新	更新掃描選項或與 Amazon EC2 資源相關聯的標籤。如需詳細資訊，請參閱 具有使用者定義標籤的掃描選項。	

略過的原因	說明	建議步驟	
	增至排除清單，且資源與此標籤相關聯；或 GuardDuty Excluded 標籤針對此資源設定為 true。		
UNSUPPORTED_VOLUME_SIZE	該磁碟區大於 2048 GB。	不可行。	
NO_VOLUMES_ATTACHED	GuardDuty 惡意軟體防護在您的帳戶中找到執行個體，但沒有 EBS 磁碟區連接至此執行個體以繼續掃描。	不可行。	
UNABLE_TO_SCAN	這是內部服務錯誤。	不可行。	
SNAPSHOT_NOT_FOUND	找不到從 EBS 磁碟區建立並與服務帳戶共用的快照集，而且 GuardDuty 惡意程式碼防護無法繼續進行掃描。	檢查 CloudTrail 以確保快照未被刻意移除。	
SNAPSHOT_QUOTA_REACHED	您已達到每個區域允許的最大快照量。這不僅會阻止保留，還會阻止建立新快照。	您可以移除舊快照或請求提高配額。您可以在《AWS 一般參考指南》中的 Service Quotas 下檢視每個區域快照的預設限制，以及如何請求提高配額。	

略過的原因	說明	建議步驟	
MAX_NUMBER_OF_ATTACHED_VOLUMES_REACHED	超過 11 個 EBS 磁碟區已連接至 EC2 執行個體。 GuardDuty 惡意軟體防護會掃描前 11 個 EBS 磁碟區，並deviceName 依字母順序排序取得。	不可行。	
UNSUPPORTED_PRODUCT_CODE_TYPE	GuardDuty 不支援使用 as 掃描執行個productCode 體marketplace 。如需詳細資訊，請參閱《Amazon EC2 Linux 執行個體使用者指南》中的已支付 AMI。 如需有關 productCode 的資訊，請參閱《Amazon EC2 API 參考》中的 ProductCode。	不可行。	

報告 GuardDuty 惡意軟體防護中的誤報

GuardDuty 惡意軟體防護掃描可能會將 Amazon EC2 執行個體或容器工作負載中的無害檔案識別為惡意或有害檔案。為改善您使用惡意軟體防護和 GuardDuty 服務的體驗，如果您認為在掃描期間識別為惡意或有害的檔案實際上並未包含惡意軟體，則可以報告誤報結果。

誤報檔案提交

1. 登入主控台，網址為 https://console.aws.amazon.com/guardduty/。
2. 當您發現疑似誤報結果時，請聯絡 AWS Support 以啟動誤報檔案提交程序。

3. 選擇惡意軟體掃描。
4. 選擇一項掃描以檢視其調查結果 ID。
5. 提供調查結果 ID。您也必須提供檔案的 SHA-256 雜湊。這是確保 GuardDuty 惡意軟體防護已收到正確檔案的必要條件。
6. AWS Support 團隊將為您提供一個 Amazon Simple Storage Service (S3) URL，您可以用於上傳檔案和 SHA-256 雜湊。成功上傳檔案後，請通知 AWS Support 團隊。

> **Warning**
>
> 請勿將檔案或 SHA-256 雜湊直接提供給 AWS Support。您應該只透過提供的 URL 將檔案和雜湊上傳至 Amazon S3。如果您在收到 URL 後 7 天內未能上傳檔案和雜湊，則該 URL 將失效。如果 URL 失效，您必須聯絡 AWS Support 才能接收新的 URL。

GuardDuty 保留檔案的時間不超過 30 天。GuardDuty 團隊成員將分析您提交的內容，並採取適當的步驟來改善您使用惡意軟體防護和 GuardDuty 服務的體驗。

補救發現的安全性問題 GuardDuty

Amazon GuardDuty 產生指出潛在安全問題的發現結果。在此版本中 GuardDuty，潛在的安全問題表示您 AWS 環境中遭到入侵的 EC2 執行個體或容器工作負載，或是一組遭到入侵的登入資料。以下各節說明這些情況下的建議修復步驟。如果有其他修復案例，則會在該特定調查結果類型的項目中加以說明。您可以從作用中調查結果類型表格中選取調查結果類型，以存取該類型的相關完整資訊。

目錄

修復可能遭到入侵的 Amazon EC2 執行個體

請遵循下列建議步驟，修復 AWS 環境中可能遭到入侵的 EC2 執行個體：

1. 識別可能遭到入侵的 Amazon EC2 執行個體

   調查可能遭盜用的執行個體是否受惡意軟體攻擊，並移除任何發現的惡意軟體。您可以使用 隨需惡意軟體掃描 來識別可能遭到入侵的 EC2 執行個體中的惡意軟體，或檢查 AWS Marketplace 是否有實用的合作夥伴產品來識別和移除惡意軟體。

2. 隔離可能遭到入侵的 Amazon EC2 執行個體

   如果可能，請使用下列步驟隔離可能遭到入侵的執行個體：

   1. 建立專用的隔離安全性群組。
   2. 為輸出規則中`0.0.0.0/0 (0-65535)`的所有流量建立單一規則。

套用此規則時，會將所有現有 (和新的) 輸出流量轉換為未追蹤，並封鎖任何已建立的輸出工作階段。如需詳細資訊，請參閱未追蹤的連線。

3. 從可能遭到入侵的執行個體移除所有目前的安全性群組關聯。
4. 將隔離安全性群組與此執行個體建立關聯。

   建立關聯之後，從隔離安全性群組的輸出規則中刪除所有流量的規則。`0.0.0.0/0 (0-65535)`

3. 識別可疑活動的來源

   如果偵測到惡意軟體，請根據您帳戶中的調查結果類型，識別並停止 EC2 執行個體上可能未經授權的活動。這可能需要採取動作，例如關閉任何開啟的連接埠、變更存取政策，以及升級應用程式以修正漏洞。

   如果您無法識別並停止潛在受損 EC2 執行個體上的未經授權活動，建議您終止受感染的 EC2 執行個體，並視需要將其替換為新的執行個體。以下是保護您 EC2 執行個體的其他資源：

   - Amazon EC2 最佳實務中的「安全和網路」一節
   - 適用於 Linux 執行個體的 Amazon EC2 安全群組和適用於 Windows 執行個體的 Amazon EC2 安全群組
   - Amazon EC2 中的安全性
   - 保護您 EC2 執行個體安全的要訣 (Linux)。
   - AWS 安全性最佳做法
   - 基礎結構網域事件 AWS

4. 瀏覽 AWS re:Post

   瀏覽以AWS re:Post尋求進一步協助。

5. 提交技術支援請求

   如果您是付費支援套件訂閱用戶，則可以提交技術支援請求。

修復可能遭到入侵的 S3 儲存貯體

請遵循下列建議步驟，修復 AWS 環境中可能遭到入侵的 Amazon S3 儲存貯體：

1. 識別可能遭到入侵的 S3 資源。

S3 的發現將在 GuardDuty 查找詳細信息中列出關聯的 S3 存儲桶，其 Amazon 資源名稱（ARN）及其所有者。

2. 識別可疑活動的來源和使用的 API 呼叫。

   使用的 API 呼叫會在調查結果詳細資訊中列為 API。來源將是 IAM 主體 (IAM 角色、使用者或帳戶)，而識別詳細資訊將列在調查結果中。視來源類型而定，遠端 IP 地址或來源網域資訊將可供使用，並可協助您評估來源是否已獲得授權。如果發現涉及來自 Amazon EC2 執行個體的登入資料，該資源的詳細資訊也會包含在內。

3. 判斷呼叫來源是否已獲得授權可存取已識別的資源。

   如需範例，請考慮以下內容：

   - 如果涉及 IAM 使用者，他們的登入資料是否有可能遭到破壞？ 如需詳細資訊，請參閱 修復可能遭到破壞 AWS 的認證。
   - 如果從先前沒有調用此類型 API 之歷史記錄的主體調用 API，此來源是否需要此操作的存取權限？ 是否可以進一步限制儲存貯體許可？
   - 如果從使用者類型為 AWSAccount 的使用者名稱 ANONYMOUS_PRINCIPAL 中看到存取，則表示該儲存貯體為公有且已存取。這個儲存貯體是否應該為公有？ 如果不是，請檢閱以下安全建議，了解共用 S3 資源的替代解決方案。
   - 如果是從使用者類型為 AWSAccount 的使用者名稱 ANONYMOUS_PRINCIPAL 中看到成功 PreflightRequest 呼叫因而進行的存取，則表示儲存貯體已設定跨來源資源共用 (CORS) 政策。這個儲存貯體是否應該有 CORS 政策？ 如果不是，請確保儲存貯體不會意外公開，並檢閱以下安全建議，了解共用 S3 資源的替代解決方案。如需有關 CORS 的詳細資訊，請參閱《S3 使用者指南》中的使用跨來源資源共用 (CORS)。

4. 判斷 S3 儲存貯體是否包含敏感資料。

   使用 Amazon Macie 判斷 S3 儲存貯體是否包含敏感資料，例如個人身分識別資訊 (PII)、財務資料或憑證。如果您的 Macie 帳戶啟用了自動化敏感資料探索，請檢閱 S3 儲存貯體的詳細資訊，以更深入了解 S3 儲存貯體的內容。如果您的 Macie 帳戶已停用此功能，建議您將其開啟以加速評估。或者，您可以建立並執行敏感資料探索任務，以檢查 S3 儲存貯體的物件是否存在敏感資料。如需詳細資訊，請參閱 Discovering sensitive data with Macie。

如已授權存取，您可以忽略該調查結果。https://console.aws.amazon.com/guardduty/ 控制台允許您設定規則以完全隱藏單個調查結果，使其不再顯示。如需詳細資訊，請參閱 隱藏規則。

如果您判斷您的 S3 資料已被未經授權的一方公開或存取，請檢閱下列 S3 安全建議，以收緊許可並限制存取。適當的修復解決方案取決於特定環境的需求。

根據特定 S3 儲存貯體存取需求提供建議

下列清單根據特定 Amazon S3 儲存貯體存取需求提供建議：

- 如需限制公開存取 S3 資料使用的集中方式，S3 封鎖公用存取。透過四種不同的設定，可針對存取點、儲存貯體和 AWS 帳戶啟用封鎖公用存取設定，以控制存取的精細度。如需詳細資訊，請參閱 S3 封鎖公有存取設定。
- AWS 存取政策可用來控制 IAM 使用者如何存取您的資源，或存取值區的方式。如需詳細資訊，請參閱使用儲存貯體政策與使用者政策。

  此外，您可以將虛擬私有雲端 (VPC) 端點與 S3 儲存貯體政策搭配使用，以限制對特定 VPC 端點的存取。如需詳細資訊，請參閱 Amazon S3 VPC 端點的儲存貯體政策範例
- 若要暫時允許信任的實體存取您的 S3 物件，您可以透過 S3 建立預先簽章的 URL。此存取權限使用您的帳戶憑證建立而成，並根據使用的憑證可以持續 6 小時到 7 天。如需詳細資訊，請參閱 Generating presigned URLs with S3。
- 對於需要在不同來源之間共用 S3 物件的使用案例，您可以使用 S3 存取點建立許可集，以限制只存取私有網路中的物件。如需詳細資訊，請參閱使用 Amazon S3 Access Points 管理資料存取。
- 若要安全地將 S3 資源的存取權授予其他 AWS 帳戶，您可以使用存取控制清單 (ACL)，如需詳細資訊，請參閱使用 ACL 管理 S3 存取。

如需 S3 安全性選項的詳細資訊，請參閱 S3 安全性最佳實務。

修復可能遭到入侵的 ECS 叢集

請遵循下列建議步驟來修復環境中可能受到危害的 AWS Amazon ECS 叢集：

1. 識別可能受到危害的 ECS 叢集。

   ECS 的 GuardDuty 惡意程式碼防護發現項目會在發現項目的詳細資料面板中提供 ECS 叢集詳細資料。
2. 評估惡意軟體的來源

   評估偵測到的惡意軟體是否在容器映像中。如果映像中有惡意軟體，請識別使用此映像執行的所有其他任務。如需執行中工作的相關資訊，請參閱ListTasks。
3. 隔離可能受影響的工作

拒絕任務的所有輸入和輸出流量，以隔離受影響的任務。拒絕所有流量規則可透過切斷與工作的所有連線，協助您阻止已在進行的攻擊。

如已授權存取，您可以忽略該調查結果。https://console.aws.amazon.com/guardduty/ 控制台允許您設定規則以完全隱藏單個調查結果，使其不再顯示。如需詳細資訊，請參閱 隱藏規則。

修復可能遭到破壞 AWS 的認證

請依照下列建議步驟修復 AWS 環境中可能遭到入侵的認證：

1. 識別可能遭到入侵的 IAM 實體和所使用的 API 呼叫。

   使用的 API 呼叫會在調查結果詳細資訊中列為 API。IAM 實體 (IAM 角色或使用者) 及其識別資訊將列在發現項目詳細資料的「資源」區段中。涉及的 IAM 實體類型可由使用者類型欄位決定，IAM 實體名稱將位於使用者名稱 欄位中。調查結果中涉及的 IAM 實體類型也可由使用的存取金鑰 ID 決定。

   對於以 AKIA 開頭的金鑰：

   此類金鑰是與 IAM 使用者或 AWS 帳戶根使用者相關聯的長期客戶自管憑證。如需有關管理 IAM 使用者存取金鑰的資訊，請參閱管理 IAM 使用者的存取金鑰。

   對於以 ASIA 開頭的金鑰：

   此類金鑰是 AWS Security Token Service產生的短期臨時登入資料。這些金鑰只存在很短的時間，無法在 AWS 管理主控台中檢視或管理。IAM 角色一律會使用 AWS STS 登入資料，但也可以為 IAM 使用者產生登入資料，如需有關 IAM：臨時安全登入資料的 AWS STS 詳細資訊。

   如果已使用角色，使用者名稱欄位將顯示所使用角色的名稱。您可以 AWS CloudTrail 透過檢查 CloudTrail 日誌項目的sessionIssuer元素來判斷金鑰的要求方式，如需詳細資訊，請參閱 IAM 和中的 AWS STS 資訊 CloudTrail。
2. 檢閱 IAM 實體的許可。

   開啟 IAM 主控台。根據所使用實體的類型，選擇 [使用者] 或 [角色] 索引標籤，然後在搜尋欄位中輸入識別的名稱來尋找受影響的實體。使用許可和存取顧問索引標籤，以檢閱該實體的有效許可。
3. 判斷是否合法使用 IAM 實體登入資料。

   請聯絡該登入資料的使用者，以判斷活動是否為刻意。

例如，查出使用者是否進行了以下動作：

- 叫用 GuardDuty 發現項目中列出的 API 作業
- 在 GuardDuty發現項目中列出的時間叫用 API 作業
- 從 GuardDuty 發現項目中列出的 IP 位址叫用 API 作業

如果此活動是 AWS 認證的合法用途，您可以忽略此 GuardDuty 發現項目。https://console.aws.amazon.com/guardduty/ 控制台允許您設定規則以完全隱藏單個調查結果，使其不再顯示。如需詳細資訊，請參閱 隱藏規則。

如果您無法確認此活動是否為合法用途，則可能是因為對特定存取金鑰 (IAM 使用者的登入憑證，或可能是整個存取金鑰) 遭到入侵的結果 AWS 帳戶。如果您懷疑自己的認證已遭入侵，請檢閱「我的 AWS 帳戶 可能遭到入侵」文章中的資訊，以修正此問題。

修復可能遭到入侵的獨立容器

1. 隔離可能遭到入侵的容器

   下列步驟可協助您識別潛在惡意的容器工作負載：

   - 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/
   - 在「發現項目」頁面上，選擇對應的發現項目，以檢視發現項目面板。
   - 在調查結果面板的受影響資源區段下，您可以檢視容器的 ID 和名稱。

   將此容器與其他容器工作負載隔離。

2. 暫停容器

   暫停容器中的所有程序。

   如需凍結容器的相關資訊，請參閱暫停容器。

   停止容器

   如果上述步驟失敗，且容器沒有暫停，請停止執行容器。如果您已啟用此快照保留功能，GuardDuty 將保留包含惡意軟體之 EBS 磁碟區的快照。

   如需停止容器的相關資訊，請參閱停止容器。

3. 評估惡意軟體的存在

評估容器映像中是否有惡意軟體。

如已授權存取，您可以忽略該調查結果。https://console.aws.amazon.com/guardduty/ 控制台允許您設定規則以完全隱藏單個調查結果，使其不再顯示。主 GuardDuty 控台可讓您設定規則以完全隱藏個別發現項目，使其不再顯示。如需更多詳細資訊，請參閱 隱藏規則。

修復 EKS 稽核日誌監控調查結果

當您的帳戶啟用 EKS 稽核日誌監控時，Amazon GuardDuty 會產生指出潛在 Kubernetes 安全問題的發現結果。如需詳細資訊，請參閱 EKS 稽核日誌監控。以下各節說明這些情況下的建議修復步驟。特定修復動作會在該特定調查結果類型的項目中說明。您可以從作用中調查結果類型表格中選取調查結果類型，以存取該類型的相關完整資訊。

如果任何 EKS 稽核日誌監控調查結果類型已如預期產生，您可以考慮新增 隱藏規則 以防止將來出現提醒。

不同類型的攻擊和設定問題可能會觸發 GuardDuty Kubernetes 發現項目。本指南可協助您針對叢集識別 GuardDuty 發現項目的根本原因，並概述適當的修復指引。以下是導致 GuardDuty Kubernetes 發現項目的主要根本原因：

- 潛在的組態問題
- 修復可能遭到入侵的 Kubernetes 使用者
- 修復可能遭到入侵的 Kubernetes 網繭
- 修復可能遭到入侵的 Kubernetes 節點
- 修復可能遭到破壞的容器映像

> **Note**
>
> 在 Kubernetes 版本 1.14 之前，依預設，`system:unauthenticated`群組已與 () 相關聯。`system:discovery` `system:basic-user` ClusterRoles這可能會允許匿名使用者的意外存取。叢集更新不會撤銷這些許可，這表示即使您已將叢集更新至 1.14 版或更新版本，這些許可也許仍然存在。建議您取消這些許可與 `system:unauthenticated` 群組的關聯。如需移除這些許可的詳細資訊，請參閱 Amazon EKS 使用者指南中的 Amazon EKS 安全最佳實務。

潛在的組態問題

如果調查結果指出組態問題，請參閱該調查結果的「修復」區段，以取得有關解決該特定問題的指引。如需詳細資訊，請參閱下列指出組態問題的調查結果類型：

- Policy:Kubernetes/AnonymousAccessGranted
- Policy:Kubernetes/ExposedDashboard
- Policy:Kubernetes/AdminAccessToDefaultServiceAccount
- Policy:Kubernetes/KubeflowDashboardExposed
- 任何結束的發現 SuccessfulAnonymousAccess

修復可能遭到入侵的 Kubernetes 使用者

當發 GuardDuty 現項目中識別的使用者執行非預期的 API 動作時，發現項目可能表示遭到入侵的 Kubernetes 使用者。您可以在主控台中調查結果詳細資訊的 Kubernetes 使用者詳細資訊區段中，或在調查結果 JSON 的 `resources.eksClusterDetails.kubernetesDetails.kubernetesUserDetails` 中識別使用者。這些使用者詳細資訊包括 `user name`、`uid` 和使用者所屬的 Kubernetes 群組。

如果使用者使用 IAM 實體存取工作負載，您可以使用 `Access Key details` 區段來識別 IAM 角色或使用者的詳細資訊。請參閱下列使用者類型及其修復指引。

> **Note**
>
> 您可以使用 Amazon Detective 進一步調查調查結果中識別的 IAM 角色或使用者。在 GuardDuty 主控台中檢視發現項目詳細資料時，選擇 [Detective 中調查]。然後從列出的項目中選擇 AWS 用戶或角色以在「Detective」中對其進行調查。

內建的 Kubernetes 管理員：Amazon EKS 指派給建立叢集的 IAM 身分的預設使用者。此使用者類型由使用者名稱 `kubernetes-admin` 識別。

若要撤銷內建的 Kubernetes 管理員的存取權限：

- 識別 `Access Key details` 區段中的 `userType`。
  - 如果 `userType` 是角色且角色屬於 EC2 執行個體角色：

- 識別該執行個體，然後按照 修復可能遭到入侵的 Amazon EC2 執行個體 中的說明進行操作。
- 如果 userType 是使用者，或是使用者擔任的角色：
  1. 輪換該使用者的存取金鑰。
  2. 輪換使用者可存取的任何秘密。
  3. 查看「我的 AWS 帳戶」中的資訊可能會遭到入侵，以取得更多詳細

OIDC 驗證的使用者：透過 OIDC 提供者經授予存取權限的使用者。OIDC 使用者通常會以電子郵件地址作為使用者名稱。您可用下列命令檢查您的叢集是否使用 OIDC：`aws eks list-identity-provider-configs --cluster-name your-cluster-name`

撤銷 OIDC 驗證使用者的存取權限：

1. 在 OIDC 提供者中輪換該使用者的憑證。
2. 輪換使用者可存取的任何秘密。

AWS-身份驗證 ConfigMap 定義的用戶 — 通過 AWS- ConfigMap auth 授予訪問權限的 IAM 用戶。如需詳細資訊，請參閱《EKS 使用者指南》中的管理叢集的使用者或 IAM 角色。您可以使用以下命令檢視其許可：`kubectl edit configmaps aws-auth --namespace kube-system`

若要撤銷使 AWS ConfigMap用者的存取權：

1. 使用下列指令來開啟 ConfigMap。

```
kubectl edit configmaps aws-auth --namespace kube-system
```

2. 使用與發現項目的 Kubernetes 使用者詳細資料區段中報告的使用者名稱相同的使用者名稱，識別「Map Rles」或「對應使用者」區段下的角色或使用者項目。 GuardDuty 請參閱下列範例，其中已在調查結果中識別管理員使用者。

```
apiVersion: v1
data:
  mapRoles: |
    - rolearn: arn:aws:iam::444455556666:role/eksctl-my-cluster-nodegroup-
standard-wo-NodeInstanceRole-1WP3NUE3O6UCF
      user name: system:node:EC2_PrivateDNSName
      groups:
        - system:bootstrappers
        - system:nodes
  mapUsers: |
```

```
    - userarn: arn:aws:iam::123456789012:user/admin
      username: admin
      groups:
        - system:masters
    - userarn: arn:aws:iam::111122223333:user/ops-user
      username: ops-user
      groups:
        - system:masters
```

3. 從中移除該使用者 ConfigMap。請參閱下列範例，其中已移除管理員使用者。

```
apiVersion: v1
data:
  mapRoles: |
    - rolearn: arn:aws:iam::111122223333:role/eksctl-my-cluster-nodegroup-
standard-wo-NodeInstanceRole-1WP3NUE3O6UCF
      username: system:node:{{EC2PrivateDNSName}}
      groups:
        - system:bootstrappers
        - system:nodes
  mapUsers: |
    - userarn: arn:aws:iam::111122223333:user/ops-user
      username: ops-user
      groups:
        - system:masters
```

4. 如果 userType 是使用者，或是使用者擔任的角色：

   a. 輪換該使用者的存取金鑰。

   b. 輪換使用者可存取的任何秘密。

   c. 查看「我的 AWS 帳戶」中的資訊可能會遭到入侵，以取得更多詳細

如果調查結果沒有 resource.accessKeyDetails 區段，則使用者是 Kubernetes 服務帳戶。

服務帳戶：服務帳戶提供 Pod 的身分，並可使用下列格式的使用者名稱進行識別：system:serviceaccount:*namespace*:*service_account_name*。

撤銷對服務帳戶的存取權限：

1. 輪換服務帳戶憑證。
2. 檢閱下一節中有關 Pod 入侵的指引。

修復可能遭到入侵的 Kubernetes 網繭

在`resource.kubernetesDetails.kubernetesWorkloadDetails`區段內 GuardDuty 指定網繭或工作負載資源的詳細資料時，該網繭或工作負載資源已可能遭到入侵。 GuardDuty 發現可能表示單一網繭已遭入侵，或是多個網繭已透過較高層級的資源遭到入侵。如需有關如何識別遭到入侵的 Pod 的指引，請參閱下列入侵情況。

單一 Pod 入侵

如果 `resource.kubernetesDetails.kubernetesWorkloadDetails` 區段內的 `type` 欄位是 Pod，則調查結果會識別單一 Pod。名稱欄位是 Pod 的 `name`，而 `namespace` 欄位則是其命名空間。

如需識別執行網繭之工作者節點的相關資訊，請參閱識別有問題的網繭和 Worker 節點。

Pod 透過工作負載資源遭到入侵

如果 `resource.kubernetesDetails.kubernetesWorkloadDetails` 區段內的 `type` 欄位識別出工作負載資源 (例如 `Deployment`)，則該工作負載資源中的所有 Pod 很可能都已遭到入侵。

如需識別工作負載資源的所有網繭及其執行所在節點的相關資訊，請參閱使用工作負載名稱識別有問題的網繭和 Worker 節點。

透過服務帳戶入侵的 Pod

如果發現項目在`resource.kubernetesDetails.kubernetesUserDetails`區段中識別了服務帳戶，則使用已識別服務帳戶的網繭很可能遭 GuardDuty 到入侵。如果調查結果報告的使用者名稱具有以下格式，則該使用者名稱是服務帳戶：`system:serviceaccount:`*`namespace`*`:`*`service_account_name`*。

如需使用服務帳戶及其執行所在節點識別所有網繭的相關資訊，請參閱使用服務帳戶名稱識別有問題的網繭和 Worker 節點。

識別出所有遭入侵的網繭及其執行所在的節點之後，請參閱 Amazon EKS 最佳實務指南，瞭解隔離網繭、輪換其登入資料，以及收集資料以進行鑑識分析。

若要修復可能遭到入侵的網繭：

1. 識別入侵 Pod 的漏洞。
2. 實作該漏洞的修正程式，並啟動新的替換 Pod。

3. 刪除易遭受攻擊的 Pod。

   如需詳細資訊，請參閱重新部署受損的網繭或工作負載資源。

如果已指派工作者節點的 IAM 角色可讓 Pod 取得其他 AWS 資源的存取權，請從執行個體中移除這些角色，以避免遭受進一步的攻擊損害。同樣地，如果已為 Pod 指派 IAM 角色，請評估您是否可以安全地從該角色中移除 IAM 政策，而不會影響其他工作負載。

修復可能遭到破壞的容器映像

當發 GuardDuty 現項目指出網繭入侵時，用來啟動網繭的映像可能是惡意或遭到入侵。 GuardDuty 發現項目會識別`resource.kubernetesDetails.kubernetesWorkloadDetails.containers.image`欄位內的容器映像。您可以掃描映像是否含有惡意軟體，判斷該映像是否為惡意的。

若要修復可能遭到入侵的容器映像檔：

1. 立即停止使用該映像，並將其從映像儲存庫中移除。
2. 使用可能遭到入侵的映像識別所有網繭。

   如需詳細資訊，請參閱識別具有可能易受攻擊或遭入侵之容器映像的網繭和背景工作

3. 隔離可能遭到入侵的 Pod、輪換憑證，並收集資料以進行分析。如需詳細資訊，請參閱 Amazon EKS 最佳實務指南。
4. 使用可能遭到入侵的映像刪除所有網繭。

修復可能遭到入侵的 Kubernetes 節點

如果發 GuardDuty 現項目中識別的使用者代表節點識別碼，或發現項目指出使用授權的容器，則發現項目可表示節點遭到入侵。

如果使用者名稱欄位具有以下格式，則使用者身分為工作節點：`system:node:node name`。例如 `system:node:ip-192-168-3-201.ec2.internal`。這表示對手已取得節點的存取權，而且正在使用節點的憑證與 Kubernetes API 端點通訊。

如果調查結果中列出的一個或多個容器的 `resource.kubernetesDetails.kubernetesWorkloadDetails.containers.securityContext.` 調查結果欄位設定為 `True`，則該調查結果表示使用了有權限的容器。

若要修復可能遭到入侵的節點：

1. 隔離網繭、旋轉其認證，並收集資料以進行鑑識分析。

   如需詳細資訊，請參閱 Amazon EKS 最佳實務指南。
2. 識別可能遭到入侵的節點上執行的所有網繭所使用的服務帳戶。檢閱其許可，並視需要輪換服務帳戶。
3. 終止可能遭到入侵的節點。

修正執行時期監視發現項

當您為帳戶啟用執行階段監控時，Amazon GuardDuty 可能會產生執行階段監視尋找項指出 AWS 環境中潛在的安全問題。潛在的安全問題表示您 AWS 環境中的 Amazon EC2 執行個體遭到入侵、容器工作負載、Amazon EKS 叢集或一組遭到入侵的登入資料。安全代理程式監視來自多個資源類型的執行階段事件 若要識別可能遭到入侵的資源，請在 GuardDuty主控台中產生的尋找項目詳細資料中檢視資源類型。下節說明各種資源類型的建議修復步驟。

Instance

如果調查結果詳細資訊中的資源類型是執行個體，則表示 EC2 執行個體或 EKS 節點可能遭到入侵。

- 若要修復遭到入侵的 EKS 節點，請參閱修復可能遭到入侵的 Kubernetes 節點。
- 若要修復遭到入侵的 EC2 執行個體，請參閱修復可能遭到入侵的 Amazon EC2 執行個體。

EKSCluster

如果調查結果詳細資訊中的資源類型為 EKSCluster，則表示 EKS 叢集內的 Pod 或容器可能遭到入侵。

- 若要修復遭到入侵的 Pod，請參閱修復可能遭到入侵的 Kubernetes 網繭。
- 若要修復遭到入侵的容器映像，請參閱修復可能遭到破壞的容器映像。

ECSCluster

如果發現項目詳細資料中的資源類型是 ECSCluster，則表示 ECS 工作或 ECS 工作內的容器可能遭到危害。

1. 識別受影響的 ECS 叢集

   「GuardDuty 執行階段監視」發現項目會在發現項目的詳細資料面板或尋找到的 JSON `resource.ecsClusterDetails` 區段中提供 ECS 叢集詳細資料。

2. 識別受影響的 ECS 任務

   「GuardDuty 執行階段監視」發現項目會在發現項目的詳細資料面板或尋找 JSON 的`resource.ecsClusterDetails.taskDetails`區段中提供 ECS 工作詳細資訊。

3. 隔離受影響的工作

   拒絕任務的所有入口和輸出流量，以隔離受影響的任務。拒絕所有流量規則可透過切斷與任務的所有連線，協助阻止已在進行的攻擊。

4. 修復遭到入侵的工作

   a. 找出危及工作的弱點。

   b. 實作該弱點的修正程式，並開始新的替換工作。

   c. 停止易受攻擊的任務。

Container

如果調查結果詳細資訊中的資源類型為容器，則表示獨立容器可能遭到入侵。

- 若要修復，請參閱修復可能遭到入侵的獨立容器。
- 如果使用相同容器映像跨多個容器產生調查結果，請參閱修復可能遭到破壞的容器映像。
- 如果容器已存取基礎 EC2 主機，則其關聯的執行個體憑證可能已遭到入侵。如需詳細資訊，請參閱 修復可能遭到破壞 AWS 的認證。
- 如果潛在惡意執行者存取了基礎 EKS 節點或 EC2 執行個體，請參閱 EKSCluster 和執行個體索引標籤下建議的修復措施。

修復遭到入侵的容器映像

當發 GuardDuty 現項目指出工作遭到入侵時，用來啟動工作的映像可能是惡意的或遭到入侵。GuardDuty 發現項目會識別`resource.ecsClusterDetails.taskDetails.containers.image`欄位內的容器映像。您可以掃描影像是否有惡意程式，判斷影像是否為惡意程式碼。

修復遭到入侵的容器映像

1. 立即停止使用該映像，並將其從映像儲存庫中移除。
2. 識別使用此映像檔的所有工作。
3. 停止所有正在使用受感染映像的任務。更新他們的任務定義，以便他們停止使用受感染的圖像。

修復可能遭到入侵的資料庫

GuardDuty 在您啟GuardDuty 遠端防護用支援的資料庫之後RDS 保護調查結果類型，會產生指出您的潛在可疑和異常登入行為。使用 RDS 登入活動，透過識別登入嘗試中的異常模式來 GuardDuty 分析和分析威脅。

> **Note**
>
> 您可以從 調查結果表 中選取調查結果類型，以存取該類型的完整資訊。

請遵循這些建議的步驟，修復 AWS 環境中可能遭到入侵的 Amazon Aurora 資料庫。

主題

- 修復可能遭到入侵且含有成功登入事件的資料庫
- 修復可能遭到入侵且含有失敗登入事件的資料庫
- 修復可能遭到入侵的憑證
- 限制網路存取權限

修復可能遭到入侵且含有成功登入事件的資料庫

下列建議步驟可協助您修復可能遭到入侵的 Aurora 資料庫，且該資料庫會出現與成功登入事件相關的異常行為。

1. 識別受影響的資料庫和使用者。

   產生的 GuardDuty 發現項目會提供受影響資料庫的名稱以及對應的使用者詳細資訊。如需詳細資訊，請參閱 調查結果詳細資訊。

2. 確認此行為是預期還是意外的行為。

下列清單指定可能導致產生發現項目 GuardDuty 的潛在案例：

- 使用者在很長一段時間後登入其資料庫。
- 使用者偶爾登入資料庫，例如財務分析師每個季度登入。
- 參與成功登入嘗試的潛在可疑執行者可能會入侵資料庫。

3. 如果是意外行為，請開始此步驟。

    1. 限制資料庫存取權限

        限制可疑帳戶的資料庫存取權限，以及此登入活動的來源。如需詳細資訊，請參閱 修復可能遭到入侵的憑證 及 限制網路存取權限。

    2. 評估影響並確定存取了哪些資訊。
        - 如果可用，請檢閱稽核日誌以識別可能已存取的資訊片段。如需詳細資訊，請參閱《Amazon Aurora 使用者指南》中的在 Amazon Aurora 資料庫叢集中監控事件、日誌和串流。
        - 判斷是否存取或修改了任何敏感或受保護的資訊。

修復可能遭到入侵且含有失敗登入事件的資料庫

下列建議步驟可協助您修復可能遭到入侵的 Aurora 資料庫，且該資料庫會出現與失敗登入事件相關的異常行為。

1. 識別受影響的資料庫和使用者。

    產生的 GuardDuty 發現項目會提供受影響資料庫的名稱以及對應的使用者詳細資訊。如需詳細資訊，請參閱 調查結果詳細資訊。

2. 識別失敗登入嘗試的來源。

    產生的 GuardDuty 發現項目會在發現項目面板的 Actor 區段下提供 IP 位址和 ASN 組織 (如果是公用連線)。

    自治系統 (AS) 是由一個或多個網路業者執行的一個或多個 IP 字首 (可在網路上存取的 IP 地址清單) 的群組，而這些網路業者維護單一且明確定義的路由政策。網路業者需要自治系統編號 (ASN) 來控制其網路內的路由，並與其他網際網路服務供應商 (ISP) 交換路由資訊。

3. 確認此行為是意外行為。

    檢查此活動是否表示嘗試獲得對資料庫的其他未經授權的存取權限，如下所示：

    - 如果來源是內部來源，請檢查應用程式是否設定錯誤，並重複嘗試連線。

- 如果這是外部執行者，請檢查對應的資料庫是否設定為公有或設定錯誤，進而允許潛在惡意動作者暴力破解常見使用者名稱。

4. 如果是意外行為，請開始此步驟。

   1. 限制資料庫存取權限

      限制可疑帳戶的資料庫存取權限，以及此登入活動的來源。如需詳細資訊，請參閱 修復可能遭到入侵的憑證 及 限制網路存取權限。

   2. 執行根本原因分析，並確定可能導致此活動的步驟。

      設定提醒以在活動修改網路政策並建立不安全狀態時收到通知。如需詳細資訊，請參閱 AWS Network Firewall Developer Guide 中的 Firewall policies in AWS Network Firewall。

修復可能遭到入侵的憑證

發 GuardDuty 現項目可能表示當發現項目中識別的使用者執行非預期的資料庫作業時，受影響資料庫的使用者證明資料已遭入侵。您可以在主控台的調查結果面板內的 RDS DB 使用者詳細資訊區段中，或在調查結果 JSON 的 `resource.rdsDbUserDetails` 內識別使用者。這些使用者詳細資訊包括使用者名稱、使用的應用程式、存取的資料庫、SSL 版本和身分驗證方法。

- 若要撤銷與調查結果有關的特定使用者的存取權限或輪換密碼，請參閱《Amazon Aurora 使用者指南》中的 Amazon Aurora MySQL 的安全性或 Amazon Aurora PostgreSQL 的安全性。
- 用 AWS Secrets Manager 於安全地存放和自動輪換 Amazon 關聯式資料庫服務 (RDS) 資料庫的密碼。如需詳細資訊，請參閱《AWS Secrets Manager 使用者指南》中的 AWS Secrets Manager 教學課程。
- 使用 IAM 資料庫身分驗證來管理資料庫使用者的存取權限，而不需要密碼。如需詳細資訊，請參閱《Amazon Aurora 使用者指南》中的 IAM 資料庫身分驗證。

  如需詳細資訊，請參閱《Amazon RDS 使用者指南》中的 Amazon Relational Database Service 的安全最佳實務。

限制網路存取權限

GuardDuty 發現可能表示您的應用程式或 Virtual Private Cloud (VPC) (VPC) 之外，還可以存取資料庫。如果調查結果中的遠端 IP 地址是非預期的連線來源，請稽核安全群組。連接至資料庫的安全群組清單位於 https://console.aws.amazon.com/rds/ 主控台的安全群組下，或調查結果 JSON 的

`resource.rdsDbInstanceDetails.dbSecurityGroups` 中。如需有關設定安全群組的詳細資訊，請參閱《Amazon RDS 使用者指南》中的使用安全群組控制存取權限。

如果您使用防火牆，請重新設定網路存取控制清單 (NACL) 以限制對資料庫的網路存取權限。如需詳細資訊，請參閱 AWS Network Firewall Developer Guide 中的 Firewalls in AWS Network Firewall。

修復可能受損的 Lambda 函數

當 GuardDuty 產生 Lambda 保護發現並且活動出現意外時，您的 Lambda 函數可能會受到損害。我們建議您完成下列步驟，以修復遭到入侵的 Lambda 函數。

修復 Lambda 保護調查結果

1. 識別可能受到損害的 Lambda 函數版本。

   Lambda 保護的 GuardDuty 發現提供名稱、Amazon 資源名稱 (ARN)、函數版本，以及與發現項目詳細資料中列出的 Lambda 函數相關聯的修訂 ID。
2. 識別潛在可疑活動的來源。

   a. 檢閱與調查結果相關的 Lambda 函數版本相關聯的程式碼。
   b. 檢閱與調查結果相關之 Lambda 函數版本的匯入程式庫和層。
   c. 如果您已透過 Amazon Inspector 啟用掃描 AWS Lambda 功能，請檢閱與發現項目相關的 Lambda 函數相關聯的 Amazon Inspector 發現項目。
   d. 檢閱記 AWS CloudTrail 錄檔以識別造成函數更新的主體，並確定活動已獲得授權或預期。
3. 修復可能受損的 Lambda 函數。

   a. 停用與調查結果相關之 Lambda 函數的執行觸發程序。如需詳細資訊，請參閱DeleteFunctionEventInvokeConfig。
   b. 檢閱 Lambda 程式碼並更新程式庫匯入和 Lambda 函數層，以移除潛在可疑的程式庫和層。
   c. 緩解與調查結果中涉及的 Lambda 函數相關的 Amazon Inspector 調查結果。

在 Amazon 管理多個帳戶 GuardDuty

當您的 AWS 環境有多個帳戶時，您可以將一個帳戶指定為您的管理員 AWS 帳戶來管理這些帳戶。然後，您可以將其他 AWS 帳戶與此管理員帳戶關聯為其成員帳戶。這個指定的 GuardDuty 系統管理員帳戶可以設定 GuardDuty 保護方案以下兩種方式可將帳戶與系統管理員帳戶建立關聯：使用 AWS Organizations 管理員帳戶和一或多個成員帳戶都屬於此組織，或透過傳送邀請至 AWS 帳戶 GuardDuty。

GuardDuty 建議使用該 AWS Organizations 方法。如需有關設定組織的詳細資訊，請參閱《AWS Organizations 使用者指南》中的建立組織。

管理多個帳戶 AWS Organizations

如果您要指定為 GuardDuty 管理員帳戶的帳戶是中組織的一部分 AWS Organizations，則您可以將該帳戶指定為組織的委派管理員 GuardDuty。註冊為委派系統管理員的帳戶會自動成為系 GuardDuty 統管理員帳戶。

當您將該帳戶新增為成員帳戶時，您可以使用此系統管理 GuardDuty 員帳戶來啟用和管理組織 AWS 帳戶 中的任何人。

如果您已經透過邀請擁有 GuardDuty 管理員帳戶與關聯成員帳戶，您可以將該帳戶註冊為組織的 GuardDuty 委派管理員。當您這麼做時，所有目前關聯的成員帳戶都會保留成員，讓您充分利用管理 GuardDuty帳戶的新增功能 AWS Organizations。

如需透過組織支援多個帳戶 GuardDuty 的詳細資訊，請參閱管理 GuardDuty 帳戶 AWS Organizations。

應邀管理多個帳戶

如果您要建立關聯的帳戶不是組織的一部分，您可以在中指定管理員帳戶， GuardDuty 然後使用管理員帳戶邀請其他人成 AWS 帳戶 為成員帳戶。當受邀帳戶接受邀請時，該帳戶就會成為與管理 GuardDuty 員帳戶相關聯的成員帳戶。

如需有關透過邀請支援多個帳戶的詳細資訊，請 GuardDuty 參閱透過邀請管理 GuardDuty 帳戶。

了解管理員帳戶和成 GuardDuty 員帳戶之間的關係

當您 GuardDuty 在多帳戶環境中使用時，管理員帳戶可以代表成員帳戶管理某些層面。 GuardDuty 管理員帳戶可以執行的主要功能如下：

- 新增和移除相關聯的成員帳戶。執行這項操作的程序會根據帳戶是否透過組織或邀請建立關聯而有所不同。
- 管理關聯成員帳戶 GuardDuty 內的狀態，包括啟用和暫停 GuardDuty。

> **Note**
>
> 管理的委派管理員帳戶會 GuardDuty 在新增為成員的帳戶中 AWS Organizations 自動啟用。

- 透過建立和管理抑制規則、信任 IP 清單和安全威脅清單，自訂 GuardDuty 網路中的發現項目。成員帳戶無法在多個帳戶環境中存取這些功能。

下表詳細說明管理員帳戶與成 GuardDuty 員帳戶之間的關係。

在此資料表中：

- 自我 — 帳戶只能針對自己的帳戶執行列出的動作。
- 任何 — 帳號可針對任何關聯帳號執行列出的動作。
- 全部 — 帳號可以執行列出的動作，並套用至所有相關聯的帳號。通常，採取此動作的帳戶是指定的 GuardDuty 管理員帳戶

帶有破折號 (—) 的表格儲存格表示帳戶無法執行列出的動作。

Action	通過 AWS Organizations		通過邀請	
	委派 GuardDuty 管理員帳戶	關聯會員帳戶	委派 GuardDuty 管理員帳戶	關聯會員帳戶
Enable GuardDuty	Any	–	Self	Self
Enable GuardDuty automatically for the entire organization (ALL, #, NONE)	All	–	–	–

View all Organizations member accounts regardless of GuardDuty status	Any	–	–	–
Generate sample findings	Self	Self	Self	Self
View all GuardDuty findings	Any	Self	Any	Self
Archive GuardDuty findings	Any	–	Any	–
Apply suppression rules	All	–	All	–
Create trusted IP list or threat lists	All	–	All	–
Update trusted IP list or threat lists	All	–	All	–
Delete trusted IP list or threat lists	All	–	All	–
Set EventBridge notification frequency	All	–	All	Self

Set Amazon S3 location for exporting findings	All	–	All	Self
Enable one or more optional protection plans for the entire organization (`ALL`, `#`, `NONE`)	All	–	–	–
Enable any GuardDuty protection plan for individual accounts	Any	–	Any	Self
Disassociate a member account	Any	–	Any	–
Disassociate from an administrator account account	–	Self[#]	–	Self
Delete a disassociated member account	Any	–	Any	–
Suspend GuardDuty	Any[*]	–	Any[*]	–
Disable GuardDuty	Any[*]	–	Any[*]	–

- # 表示只有在委派 GuardDuty 管理員帳戶尚未設定組織成員的自動啟用偏好設定時，帳戶才能採`ALL`取此動作。

- * 表示必須先對所有關聯帳戶採取此動作，才能為此帳號採取。取消這些帳戶的關聯後，您必須刪除它們。如需有關在組織中執行這些工作的詳細資訊，請參閱維護您的組織 GuardDuty。

管理 GuardDuty 帳戶 AWS Organizations

當您與組織 GuardDuty 搭配使用時，該 AWS 組織的管理帳戶可以將組織內的任何帳戶指定為委派的管理 GuardDuty 員帳戶。對於此管理員帳戶， GuardDuty只會在指定的中自動啟用 AWS 區域。此帳戶也具有 GuardDuty 針對該區域內組織中所有帳戶啟用和管理的權限。管理員帳戶可以檢視此組織的成員，並將成員新增至此 AWS 組織。

如果您已透過邀請設定具有相關聯成員帳戶的 GuardDuty 管理員帳戶，且成員帳戶屬於同一組織，則當您為組織設定委派的管理員帳戶時，成 GuardDuty 員帳戶的「類型」會從「依邀請」變更為「透過組織」。如果委派的 GuardDuty 管理員帳戶先前透過邀請新增不屬於同一組織的成員，則其「類型」會保留「依邀請」。在這兩種情況下，先前新增的帳戶都是與組織委派 GuardDuty 管理員帳戶相關聯的成員帳戶。

您可以繼續將帳戶新增為成員，即使帳戶在您的組織外。如需詳細資訊，請參閱 應邀新增並管理帳戶 或 使用主控台指定委派 GuardDuty 的 GuardDuty 管理員帳戶並管理成員。

目錄

指定委派 GuardDuty 管理員帳戶時的考量事項與建議

下列考量事項與建議可協助您瞭解委派 GuardDuty 系統管理員帳戶的運作方式 GuardDuty：

委派的 GuardDuty 系統管理員帳戶最多可管理 50,000 名成員。

> 每個委派的管理員帳戶上限為 50,000 個成 GuardDuty 員帳戶。這包括透過新增的成員帳戶， AWS Organizations 或是接受 GuardDuty 管理員帳戶加入其組織邀請的成員帳戶。但是，您的 AWS 組織中可能有 50,000 個以上的帳戶。

如果您超過 50,000 個成員帳戶限制，您將會收到來自 CloudWatch AWS Health Dashboard、和指定委派 GuardDuty 管理員帳戶的電子郵件通知。

委派的 GuardDuty 管理員帳戶為「地區」。

不同的 GuardDuty 是 AWS Organizations，是一個區域服務。委派的 GuardDuty 管理員帳戶及其成員帳戶必須 AWS Organizations 在您已 GuardDuty 啟用的每個所需區域中新增。如果組織管理帳戶僅在美國東部 (維吉尼亞北部) 指定委派的管理 GuardDuty 員帳戶，則委派的管理 GuardDuty 員帳戶只會管理新增至該區域中組織的成員帳戶。如需有關可用區域中特徵同位檢查的 GuardDuty 更多資訊，請參閱區域與端點。

選擇加入地區的特殊情況

- 當委派的 GuardDuty 系統管理員帳戶選擇退出選擇加入區域時，即使您的組織將 GuardDuty 自動啟用組態設定為僅限新成員帳戶 (NEW) 或所有成員帳戶 (ALL)，也 GuardDuty無法針對目前已停用的組織中的任何成員帳戶啟用。 GuardDuty 如需成員帳戶設定的相關資訊，請在GuardDuty主控台導覽窗格中開啟 [帳戶]，或使用 ListMembersAPI。
- 使 GuardDuty 用自動啟用組態集時NEW，請確定符合下列順序：

  1. 會員帳戶選擇加入選擇加入區域。
  2. 將成員帳戶新增至中的組織 AWS Organizations。

  如果您變更這些步驟的順序， GuardDuty 自動啟用設定NEW將無法在特定的選擇加入區域中運作，因為該成員帳戶不再是組織的新成員。 GuardDuty 提供兩種替代解決方案：

  - 將 GuardDuty 自動啟用組態設定為ALL，其中包括新的和現有的成員帳戶。在這種情況下，這些步驟的順序是不相關的。
  - 如果成員帳戶已經是組織的一部分，請使用 GuardDuty 控制台或 API 在特定選擇加入區域中個別管理此帳戶的 GuardDuty 配置。

建議組 AWS 織在所有組織中擁有相同的委派 GuardDuty 管理員帳戶 AWS 區域。

我們建議您 AWS 區域 在所有已啟用的位置指定相同的委派 GuardDuty 管理員帳戶給您的組織 GuardDuty。如果您將帳戶指定為某個區域中的委派 GuardDuty 管理員帳戶，建議您在所有其他區域中使用與委派 GuardDuty 管理員帳戶相同的帳戶。

您可以隨時指定新的委派 GuardDuty 管理員帳戶。如需移除現有委派 GuardDuty 系統管理員帳戶的詳細資訊，請參閱變更委派的 GuardDuty 管理員帳戶。

不建議將組織的管理帳戶設定為委派的系統管理 GuardDuty 員帳戶。

您組織的管理帳戶可以是委派的系統管理 GuardDuty 員帳戶。不過， AWS 安全性最佳實務遵循最低權限原則，不建議使用此組態。

變更委派的 GuardDuty 系統管理員帳戶並不會停 GuardDuty 用成員帳戶。

如果您移除委派的 GuardDuty 系統管理員帳戶，則會 GuardDuty 移除與此委派 GuardDuty 管理員帳戶相關聯的所有成員帳戶。 GuardDuty 所有這些成員帳戶仍保持啟用狀態。

指定委派 GuardDuty 管理員帳戶所需的權限

委派委派的 GuardDuty 系統管理員帳戶時，您必須擁有啟用權限 GuardDuty 以及特定 AWS Organizations API 動作。您可以在某個 IAM 政策的結尾新增下列陳述式，以授予這些許可：

```
{
    "Sid": "PermissionsForGuardDutyAdmin",
    "Effect": "Allow",
    "Action": [
        "guardduty:EnableOrganizationAdminAccount",
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
    ],
    "Resource": "*"
}
```

此外，如果您想要將 AWS Organizations 管理帳戶指定為 GuardDuty委派的系統管理 GuardDuty 員帳戶，該實體將需要初始化`CreateServiceLinkedRole`權限 GuardDuty。若要這麼做，請將下列陳述式新增至 IAM 政策，並以組織管理 AWS 帳戶 帳戶的識別碼取代 *111122223333*：

```
{
 "Sid": "PermissionsToEnableGuardDuty"
 "Effect": "Allow",
 "Action": [
  "iam:CreateServiceLinkedRole"
 ],
 "Resource": "arn:aws:iam::111122223333:role/aws-service-role/guardduty.amazonaws.com/
AWSServiceRoleForAmazonGuardDuty",
 "Condition": {
  "StringLike": {
```

```
    "iam:AWSServiceName": "guardduty.amazonaws.com"
   }
  }
 }
```

使用主控台指定委派 GuardDuty 的 GuardDuty 管理員帳戶並管理成員

目錄

步驟 1 — 指定組織的委派 GuardDuty 系統管理員帳戶

1. 開啟主 GuardDuty 控台，網址為 https://console.aws.amazon.com/guardduty/。

   若要登入，使用 AWS Organizations 組織的管理帳戶憑證。
2. 如果您已啟 GuardDuty 用管理帳戶，請略過此步驟，並依照下一個步驟執行。

   如果 GuardDuty 尚未啟用，請選取 [開始使用]，然後在 [歡迎使用] GuardDuty 頁面上指定委派的 GuardDuty 系統管理員帳戶。

   > **Note**
   >
   > 管理帳戶必須具有 GuardDuty 服務連結角色 (SLR)，如此委派的系統管理 GuardDuty 員帳戶才能在該帳戶 GuardDuty 中啟用和管理。在管理帳戶的區域 GuardDuty 中啟用後，系統就會自動建立此單鏡反光相機。
3. 啟用 GuardDuty 管理帳戶後，請執行此步驟。在 GuardDuty 主控台的功能窗格中，選擇 [設定]。在 [設定] 頁面上，輸入您要指定為組織委派 GuardDuty 管理員帳戶之帳戶的 12 位數 AWS 帳戶 ID。

   請務必 GuardDuty 為新指定的委派 GuardDuty 管理員帳戶啟用，否則將無法採取任何動作。
4. 選擇委派。
5. (建議) 重複上一個步驟，以在每個您已 GuardDuty 啟用的 AWS 區域 位置指定委派 GuardDuty 管理員帳戶。

步驟 2 — 設定組織的自動啟用偏好設定

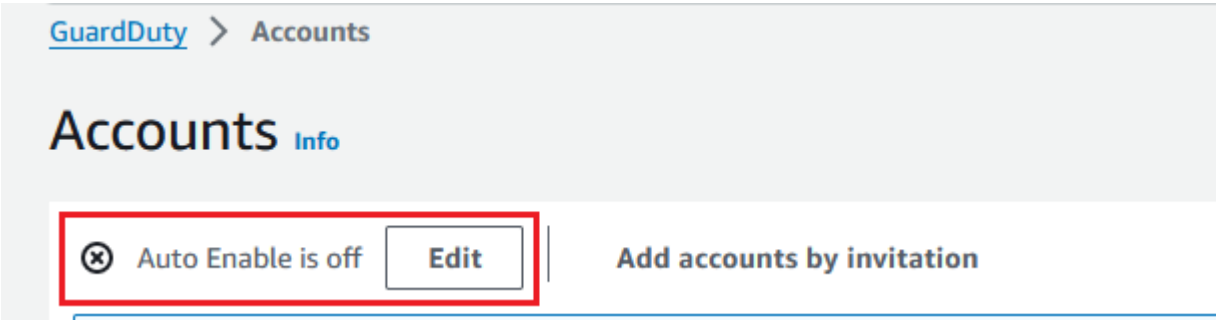
1. 開啟主 GuardDuty 控台，網址為 https://console.aws.amazon.com/guardduty/。

   若要登入，請使用 GuardDuty 系統管理員帳戶認證。

2. 在導覽窗格中，選擇帳戶。

   [帳戶] 頁面為 GuardDuty 系統管理員帳戶提供 [自動啟用] 的組態選項，以 GuardDuty 及代表屬於組織的成員帳戶的選擇性保護計劃。

3. 若要更新現有的自動啟用設定，請選擇 「編輯」。



   您可以使用此支援來設定 GuardDuty 和所有支援的選用保護方案 AWS 區域。您可以代表您的成員帳戶選取 GuardDuty 下列其中一個組態選項：

   - 針對所有帳號啟用 (**ALL**) — 選取此選項可為組織中所有帳號啟用對應的選項。這包括加入組織的新帳戶，以及可能已暫停或從組織中移除的帳戶。這也包括委派的 GuardDuty 管理員帳戶。

     > **Note**
     >
     > 更新所有成員帳戶的設定最多可能需要 24 小時。

   - 自動啟用新帳號 (**NEW**) — 選取此選項可在新成員帳戶加入組織時自動啟用 GuardDuty 或選用的保護方案。
   - 不要啟用 (**NONE**) — 選取此選項可防止針對組織中的新帳號啟用對應的選項。在這種情況下，管理 GuardDuty 員帳戶將單獨管理每個帳戶。

     當您NEW將自動啟用設定從ALL或更新為時NONE，此動作不會停用現有帳戶的對應選項。此設定將套用至加入組織的新帳戶。更新自動啟用設定後，沒有新帳戶的對應選項已啟用。

> **Note**
>
> 當委派的 GuardDuty 系統管理員帳戶選擇退出選擇加入區域時，即使您的組織將 GuardDuty 自動啟用組態設定為僅限新成員帳戶 (NEW) 或所有成員帳戶 (ALL)，也 GuardDuty無法針對目前已停用的組織中的任何成員帳戶啟用。 GuardDuty 如需成員帳戶設定的相關資訊，請在GuardDuty 主控台導覽窗格中開啟 [帳戶]，或使用 ListMembersAPI。

4. 選擇儲存變更。
5. (選擇性) 如果您想在每個「地區」中使用相同的偏好設定，請分別更新每個支援地區的偏好設定。

   某些可選的保護計劃可能不適用於所有可用 GuardDuty 的 AWS 區域 地方。如需詳細資訊，請參閱 區域與端點。

步驟 3：將帳戶作為成員新增至組織

1. 開啟主 GuardDuty 控台，網址為 https://console.aws.amazon.com/guardduty/。

   若要登入，請使用委派的 GuardDuty 系統管理員帳戶認證。
2. 在導覽窗格中，選擇帳戶。

   帳戶表格會顯示透過組織 (AWS Organizations) 或透過邀請新增的所有帳戶。如果成員帳戶與組織的 GuardDuty 管理員帳戶沒有關聯，則此成員帳戶的「狀態」 不是成員。
3. 選擇您要新增為成員的一個或多個帳戶 ID。這些帳戶 ID 必須具有透過組織的類型。

   透過邀請新增的帳戶不屬於您組織的一部分。您可以單獨管理此類帳戶。如需詳細資訊，請參閱應邀管理帳戶。
4. 選擇動作下拉式清單，然後選擇新增成員。將此帳戶新增為成員後，將套用自動啟用 GuardDuty 設定。根據中的設定the section called “步驟 1 — 指定組織的委派 GuardDuty 系統管理員帳戶”，這些帳戶的 GuardDuty組態可能會變更。
5. 您可以選取 [狀態] 欄的向下箭頭，依 [非成員] 狀態對帳戶進行排序，然後選擇目前 [區域] 中未 GuardDuty 啟用的每個帳戶。

   如果帳號表格中列出的帳戶尚未新增為成員，您可以在目前區域 GuardDuty 中為所有組織帳戶啟用。在頁面頂端的橫幅中選擇啟用。此動作會自動開啟自動啟用組 GuardDuty 態，以便 GuardDuty 為加入組織的任何新帳戶啟用。

6. 選擇確認以將帳戶新增為成員。此動作也會針 GuardDuty 對所有選取的帳號啟用。這些帳戶的狀態將變更為已啟用。
7. (建議) 在每個步驟中重複這些步驟 AWS 區域。如此可確保委派的系統管理 GuardDuty 員帳戶可以管理您已啟用之所有區域中成員帳戶的發現項目和其他組 GuardDuty 態。

   自動啟用功能可 GuardDuty 供組織的所有 future 成員使用。這可讓您的委派 GuardDuty 管理員帳戶管理在組織內建立或新增至組織的任何新成員。當成員帳戶數量達到 50,000 個上限時，自動啟用功能將自動關閉。如果您移除成員帳戶，且成員總數減少至少於 50,000，則自動啟用功能會重新開啟。

(選擇性) 步驟 4 — 設定個別帳戶的保護方案

您可以透過帳戶頁面設定個別帳戶的保護計畫。

1. 開啟主 GuardDuty 控台，網址為 https://console.aws.amazon.com/guardduty/。

   使用委派的 GuardDuty 系統管理員帳戶認證。
2. 在導覽窗格中，選擇帳戶。
3. 選擇您要設定保護計畫的一個或多個帳戶。針對您想要設定的每個保護計畫，重複下列步驟：

   a. 選擇編輯保護計畫。

   b. 從保護計畫清單中，選擇一個您想要設定的保護計畫。

   c. 選擇您要針對此保護計畫執行的其中一個動作，然後選擇確認。

   d. 對於選取的帳戶，與設定的保護計畫對應的資料欄會將更新後的組態顯示為已啟用或未啟用。

使用 API 指定委 GuardDuty 派 GuardDuty 的管理員帳戶並管理成員

目錄

步驟 1 — 指定 AWS 組織的委派 GuardDuty 系統管理員帳戶

1. enableOrganizationAdminAccount使用組織管理帳戶 AWS 帳戶 的認證執行。

- 或者，您可以使用 AWS Command Line Interface 來執行此操作。下列 AWS CLI 命令僅會指定您目前區域的委派 GuardDuty 管理員帳戶。執行下列 AWS CLI 命令，並確定將 *111111111111* 取代為您要指定為委派系統管理員帳戶的帳戶 AWS 帳戶 識別碼：GuardDuty

```
aws guardduty enable-organization-admin-account --admin-account-id 111111111111
```

若要指定其他區域的委派 GuardDuty 管理員帳戶，請在 AWS CLI 命令中指定 Region。下列範例示範如何在美國西部 (奧勒岡) 啟用委派的 GuardDuty 系統管理員帳戶。請務必將 *us-west-2* 取代為您要指 GuardDuty 派委派管理員 GuardDuty 帳戶的地區。

```
aws guardduty enable-organization-admin-account --admin-account-id 111111111111
 --region us-west-2
```

如需有關「可用 AWS 區域 位置 GuardDuty 」的資訊，請參閱區域與端點。

如果 GuardDuty 您委派的 GuardDuty 系統管理員帳戶未啟用，則無法採取任何動作。如果尚未這麼做，請確定 GuardDuty 為新指定的委派 GuardDuty 管理員帳戶啟用。

2. (建議) 重複上一個步驟，以在每個您已 GuardDuty 啟用的 AWS 區域 位置指定委派 GuardDuty 管理員帳戶。

步驟 2：設定組織的自動啟用偏好設定

1. 1. 使UpdateOrganizationConfiguration用委派 GuardDuty 系統管理員帳戶的認證來執行，為您的組織自動在該區域中設定 GuardDuty 和選擇性的保護方案

   要查找您`detectorId`的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

   > **Note**
   >
   > 如需各種自動啟用組態的相關資訊，請參閱autoEnableOrganization成員。

2. 若要為您區域中任何支援的選用保護計畫設定自動啟用偏好設定，請依照每個保護計畫對應文件章節中提供的步驟進行。
3. 您可以驗證目前區域中組織的偏好設定。執行 describeOrganizationConfiguration。確保指定委派 GuardDuty 管理員帳戶的偵測器 ID。

> **Note**
>
> 最多可能需要 24 小時才會更新所有成員帳戶的組態。

- 1. 或者，執行下列 AWS CLI 命令將偏好設定設定設定為 GuardDuty 在該區域中針對加入組織的新帳號 (NEW)、所有帳號 () 或組織中不使用任何帳號 (ALL)，自動啟用或停用該區域中的偏好設定。NONE如需詳細資訊，請參閱autoEnableOrganization成員。根據您的偏好設定，您可能需要使用 ALL 或 NONE 取代 NEW。如果您使用設定保護方案ALL，則委派的 GuardDuty 系統管理員帳戶也會啟用保護方案。請務必指定管理組織組態之委派管理 GuardDuty 員帳戶的偵測器識別碼。

  要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

  ```
  aws guardduty update-organization-configuration --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members=NEW
  ```

  2. 您可以驗證目前區域中組織的偏好設定。使用委派 GuardDuty 系統管理員帳戶的偵測器識別碼執行下列 AWS CLI 命令。

  ```
  aws guardduty describe-organization-configuration --detector-
  id 12abc34d567e8fa901bc2d34e56789f0
  ```

2. (建議) 使用委派的 GuardDuty 系統管理員帳戶偵測器 ID，在每個區域中重複上述步驟。

> **Note**
>
> 當委派的 GuardDuty 系統管理員帳戶選擇退出選擇加入區域時，即使您的組織將 GuardDuty 自動啟用組態設定為僅限新成員帳戶 (NEW) 或所有成員帳戶 (ALL)，也GuardDuty無法針對目前已停用的組織中的任何成員帳戶啟用。 GuardDuty 如需成員帳戶設定的相關資訊，請在GuardDuty 主控台導覽窗格中開啟 [帳戶]，或使用ListMembersAPI。

步驟 3：將帳戶作為成員新增至組織

- 使CreateMembers用在上一個步驟中指定之委派 GuardDuty 管理員帳戶的認證來執行。

您必須指定委派 GuardDuty 管理員帳戶的地區偵測器 ID，以及要新增為 GuardDuty 成員之帳戶的帳戶詳細資料 (AWS 帳戶 ID 和對應的電子郵件地址)。您可以使用此 API 操作建立一個或多個成員。

當您CreateMembers在組織中執行時，新成員的自動啟用偏好設定會在新成員帳戶加入組織時套用。當您CreateMembers使用現有的成員帳戶執行時，組織組態也會套用至現有的成員。這可能會變更現有成員帳戶的目前設定。

ListAccounts在 AWS Organizations API 參考中執行，以檢視 AWS 組織中的所有帳戶。

> **Important**
>
> 當您將帳戶添加為會 GuardDuty 員時，該帳戶將自動在該區域中 GuardDuty 啟用。組織管理帳戶有例外狀況。管理帳戶帳戶新增為 GuardDuty 成員之前，必須先 GuardDuty 啟用該帳戶。

- 或者，您可以使用 AWS Command Line Interface. 執行下列 AWS CLI 命令，並確保使用您的有效偵測器 ID、 AWS 帳戶 ID 以及與帳戶 ID 相關聯的電子郵件地址。

  要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

  ```
  aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
  account-details AccountId=111122223333,Email=guardduty-member-name@amazon.com
  ```

  您可以執行下列 AWS CLI 命令來檢視所有組織成員的清單：

  ```
  aws organizations list-accounts
  ```

將此帳戶新增為成員後，將套用自動啟用 GuardDuty設定。

維護您的組織 GuardDuty

身為委派的 GuardDuty 系統管理員帳戶，您必須負責維護組織中每個受支援帳戶的組態 GuardDuty 及其選擇性保護方案 AWS 區域。下列各節提供有關維護 GuardDuty 或其任何選擇性保護計劃之組態狀態的選項：

若要維護每個區域中整個組織的組態狀態

- 使用 GuardDuty 主控台設定整個組織的自動啟 GuardDuty用偏好設定 — 您可以為組織中的所有成員或加入組織的新成員 (NEW) 自動啟用，或選擇不 (NONE) 自動啟用組織中的任何成員。ALL

  您也可以為中的任何保護方案設定相同或不同的設定 GuardDuty。

  最多可能需要 24 小時才能更新組織中所有成員帳戶的組態。
- 使用 API 更新自動啟用偏好設定 — 執行UpdateOrganizationConfiguration以自動設定組織GuardDuty及其選用的保護計畫。當您執行CreateMembers以在組織中新增成員帳戶時，已設定的設定將自動套用。當您CreateMembers使用現有的成員帳戶執行時，組織組態也會套用至現有的成員。這可能會變更現有成員帳戶的目前設定。

  若要檢視組織中的所有帳戶，請ListAccounts在 AWS Organizations API 參考中執行。

在每個區域中個別維護成員帳戶的組態狀態

- 若要檢視組織中的所有帳戶，請ListAccounts在 AWS Organizations API 參考中執行。
- 當您希望選擇性成員帳戶具有不同的組態狀態時，請分別UpdateMemberDetectors針對每個成員帳戶執行。

  您可以瀏覽至 GuardDuty 主控台中的 [帳戶] 頁面，使用 GuardDuty 主控台來執行相同的工作。

  如需使用主控台或 API 為個別帳戶啟用保護方案的相關資訊，請參閱對應保護方案的設定頁面。

變更委派的 GuardDuty 管理員帳戶

您可以在每個區域中變更組織的委派 GuardDuty 管理員帳戶，然後在每個區域中委派新的管理員。若要維護區域中組織成員帳戶的安全性狀態，您必須在該區域中擁有委派的 GuardDuty 管理員帳戶。

移除現有委派 GuardDuty 管理員帳戶

步驟 1-移除每個區域中現有的委派 GuardDuty 管理員帳戶

1. 作為現有委派 GuardDuty 管理員帳戶，列出與您的管理員帳戶相關聯的所有成員帳戶。運行ListMembers與`OnlyAssociated=false`.
2. 如果將 GuardDuty 或任何選用保護方案的自動啟用喜好設定設為`ALL`，則執行UpdateOrganizationConfiguration以將組織組態更新為`NEW`或`NONE`。當您在下一個步驟中取消關聯所有成員帳戶時，此動作將防止發生錯誤。
3. 執行DisassociateMembers以取消與管理員帳戶相關聯的所有成員帳戶的關聯。
4. 執行DeleteMembers以刪除管理員帳戶與成員帳戶之間的關聯。
5. 做為組織管理帳戶，執行DisableOrganizationAdminAccount以移除現有的委派管理 GuardDuty 員帳戶。
6. 在您擁有此委派 GuardDuty 管理員帳戶 AWS 區域 的每個位置重複這些步驟。

步驟 2-要取消註冊現有委託 GuardDuty 管理員帳戶 AWS Organizations （一次性全局操作）

- 在 AWS Organizations API 參考DeregisterDelegatedAdministrator中執行，以取消註冊中的現有委派 GuardDuty 管理員帳戶。 AWS Organizations

  或者，您也可以執行下列 AWS CLI 命令：

  ```
  aws organizations deregister-delegated-administrator --account-id 111122223333 --
  service-principal guardduty.amazonaws.com
  ```

  請務必將 *111122223333* 取代為現有的委派系統管理員帳戶。 GuardDuty

  取消註冊舊的委派 GuardDuty 管理員帳戶後，您可以將其作為成員帳戶新增至新的委派 GuardDuty 管理員帳戶。

在每個區域中指定新的委派 GuardDuty 管理員帳戶

1. 使用下列其中一種存取方法，在每個區域中指定新的委派 GuardDuty 管理員帳戶：
   - 使用 GuardDuty 控制台-步驟 1 — 指定組織的委派 GuardDuty 系統管理員帳戶。
   - 使用 GuardDuty API —步驟 1 — 指定 AWS 組織的委派 GuardDuty 系統管理員帳戶.
2. 執行DescribeOrganizationConfiguration以檢視組織目前的自動啟用組態。

> **Important**
>
> 在將任何成員新增至新委派的 GuardDuty 管理員帳戶之前，您必須先驗證組織的自動啟用組態。此設定僅適用於新委派的 GuardDuty 系統管理員帳戶和選取的區域，與 AWS Organizations。當您在新委派的系統管理員帳戶下新增 (新的或現有的) 組織成 GuardDuty 員帳戶時，新委派系統 GuardDuty 管理員帳戶的自動啟用組態會在啟用時套用， GuardDuty 或套用其任何選用的保護方案。

若要變更新委派 GuardDuty 管理員帳戶的此組織組態，請使用下列其中一種存取方法：

- 使用 GuardDuty 控制台-步驟 2 — 設定組織的自動啟用偏好設定。
- 使用 GuardDuty API —步驟 2：設定組織的自動啟用偏好設定.

透過邀請管理 GuardDuty 帳戶

若要管理組織外部的帳戶，您可以使用傳統邀請方法。使用此方法時，在另一個帳戶接受您的邀請成為成員帳戶後，您的帳戶便會指定為管理員帳戶。

如果您的帳戶不是管理員帳戶，您可以接受其他帳戶的邀請。當您接受時，您的帳戶會成為成員帳戶。AWS 帳戶不能同時是 GuardDuty 管理員帳戶和成員帳戶。

當您接受來自某個帳戶的邀請時，您無法接受其他帳戶的邀請。若要接受來自其他帳戶的邀請，您必須先取消帳戶與現有管理員帳戶的關聯。或者，管理員帳戶也可以從組織中取消關聯和移除您帳戶的關聯。

透過邀請關聯的帳戶與所關聯的帳戶具有相同的整體管理員 account-to-member 關係 AWS Organizations，如中所述了解管理員帳戶和成 GuardDuty 員帳戶之間的關係。但是，邀請管理員帳戶使用者無法代表 GuardDuty 關聯的成員帳戶啟用，或檢視其 AWS Organizations 組織內的其他非成員帳戶。

> **Important**
>
> 使用此方法 GuardDuty 建立會員帳戶時，可能會發生跨區域資料傳輸。為了驗證會員帳戶的電子郵件地址，請 GuardDuty 使用僅在美國東部 (維吉尼亞北部) 區域運作的電子郵件驗證服務。

應邀新增並管理帳戶

選擇其中一種存取方法，以管理員帳戶的身分新增和邀請帳戶成為 GuardDuty 會 GuardDuty 員帳戶。

Console

步驟 1：新增帳戶

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/
2. 在導覽窗格中，選擇帳戶。
3. 選擇頂端窗格中的透過邀請新增帳戶。
4. 在 [新增成員帳戶] 頁面的 [輸入帳戶詳細資訊] 底下，輸入與您要新增之帳戶相關聯的 AWS 帳戶 ID 和電子郵件地址。
5. 若要新增其他資料列以一次輸入帳戶詳細資訊，請選擇新增其他帳戶。您也可以選擇上傳包含帳戶詳細資訊的 .csv 檔案以大量新增帳戶。

   > **Important**
   >
   > 您的 csv 檔案第一行應包含標頭，如以下範例所示：`Account ID,Email`。後續每一行都必須包含單一有效 AWS 帳戶 ID 及其相關聯的電子郵件地址。如果列的格式只包含一個 AWS 帳戶 ID 和相關聯的電子郵件地址 (以逗號分隔)，則該列的格式有效。
   >
   > ```
   > Account ID,Email
   > 555555555555,user@example.com
   > ```

6. 新增所有帳戶的詳細資訊後，請選擇下一步。您可以在「帳戶」表格中檢視新增的帳戶。這些帳戶的狀態將為未傳送邀請。如需有關傳送邀請至一個或多個新增帳戶的資訊，請參閱Step 2 - Invite an account。

步驟 2：邀請帳戶

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/
2. 在導覽窗格中，選擇帳戶。
3. 選擇您要邀請到 Amazon 的一個或多個帳戶 GuardDuty。
4. 選擇動作下拉式選單，然後選擇邀請。
5. 在「邀請函 GuardDuty」對話方塊中，輸入 (選用) 邀請訊息。

如果受邀帳戶無法存取電子郵件，請選取同時傳送電子郵件通知給受邀者之 AWS 帳戶 上的根使用者，並在受邀者的 AWS Health Dashboard中產生提醒核取方塊。

6. 選擇傳送邀請。如果受邀者可以存取指定的電子郵件地址，他們可以在 https://console.aws.amazon.com/guardduty/ 開啟 GuardDuty主控台來檢視邀請。
7. 當受邀者接受邀請時，狀態資料欄中的值會變更為已受邀。如需有關接受邀請的資訊，請參閱Step 3 - Accept an invitation。

步驟 3：接受邀請

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/

> **Important**
>
> 您必須 GuardDuty 先啟用，才能檢視或接受會員邀請。

2. 只有在 GuardDuty 尚未啟用時才執行下列動作；否則，您可以略過此步驟並繼續下一個步驟。

   如果您尚未啟用 GuardDuty，請在 Amazon GuardDuty 頁面上選擇「開始使用」。

   在 [歡迎使用 GuardDuty] 頁面上，選擇 [啟用] GuardDuty。
3. 為帳戶啟 GuardDuty 用後，請按照下列步驟接受會員邀請：

   a. 在導覽窗格中，選擇設定。
   b. 選擇帳戶。
   c. 在帳戶上，務必驗證您接受邀請之帳戶所有者的身分。開啟接受以接受成員資格邀請。
4. 接受邀請後，您的帳戶就 GuardDuty 會成為會員帳戶。擁有者傳送邀請函的帳戶會成為 GuardDuty 管理員帳戶。管理員帳戶將知道您已接受邀請。他們帳戶中的「 GuardDuty 帳戶」表格將會更新。與您的會員帳戶 ID 對應的「狀態」欄中的值將變更為「已啟用」。系統管理員帳戶擁有者現在可以代表您的帳戶檢視 GuardDuty 和管理和保護方案組態。管理員帳戶還可以查看和管理為您的成員帳戶生成的 GuardDuty 發現項目。

API/CLI

您可以指定 GuardDuty 管理員帳戶，並透過 API 作業的邀請來建立或新增 GuardDuty 成員帳戶。執行下列 GuardDuty API 作業，以便在中指定管理員帳戶和成員帳戶 GuardDuty。

使用您要指定為 GuardDuty 管理員帳戶的 AWS 帳戶 認證，完成下列程序。

建立或新增成員帳戶

1. 使用已 GuardDuty 啟用 AWS 帳戶的認證執行 CreateMembersAPI 作業。這是您要成為管理員帳戶的 GuardDuty 帳戶。

   您必須指定當前 AWS 帳戶的檢測器 ID 以及要成為 GuardDuty 會員的帳戶的帳戶 ID 和電子郵件地址。您可以使用此 API 操作建立一個或多個成員。

   您也可以透過執行下列 CLI AWS 命令，使用命令列工具來指定管理員帳戶。請務必使用您自己的有效偵測器 ID、帳戶 ID 和電子郵件。

   要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

   ```
   aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
   account-details AccountId=111122223333,Email=guardduty-member@organization.com
   ```

2. 使InviteMembers用已 GuardDuty 啟用 AWS 帳戶的認證來執行。這是您要成為管理員帳戶的 GuardDuty 帳戶。

   您必須指定目前 AWS 帳戶的偵測器 ID，以及要成為成 GuardDuty 員之帳戶的帳戶 ID。您可以使用此 API 操作邀請一個或多個成員。

   > **Note**
   >
   > 您也可以透過使用 message 請求參數指定選用的邀請訊息。

   您也可以透過執行下列命令 AWS Command Line Interface 來指定成員帳戶。請務必為您要邀請的帳戶使用自己的有效偵測器 ID 和有效的帳戶 ID。

   要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

   ```
   aws guardduty invite-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
   account-ids 111122223333
   ```

接受邀請

使用您要指定為成員帳戶的每個 AWS 帳戶的認證，完 GuardDuty 成下列程序。

1. 針對受邀成為 GuardDuty 會員 AWS 帳戶且您想要接受邀請的每個帳戶執行 CreateDetectorAPI 操作。

   您必須指定是否要使用 GuardDuty服務啟用偵測器資源。必須建立並啟用偵測器，才能正常 GuardDuty 運作。您必須先啟用 GuardDuty 才能接受邀請。

   您也可以使用以下 CLI AWS 命令使用命令行工具來執行此操作。

   ```
   aws guardduty create-detector --enable
   ```

2. 使用該 AWS 帳戶的認證，針對您要接受成員資格邀請的每個帳戶執行 AcceptAdministratorInvitationAPI 作業。

   您必須為成員帳戶指定此 AWS 帳戶的偵測器 ID、傳送邀請的系統管理員帳戶的帳戶 ID，以及您接受之邀請的邀請 ID。您可以在邀請電子郵件中或使用 API 的 ListInvitations 操作來尋找管理員帳戶的帳戶 ID。

   您也可以執行下列 CLI AWS 命令，使用命令列工具接受邀請。請務必使用有效的偵測器 ID、管理員帳戶 ID 和邀請 ID。

   要查找您`detectorId`的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

   ```
   aws guardduty accept-invitation --detector-id 12abc34d567e8fa901bc2d34e56789f0
    --administrator-id 444455556666 --invitation-
   id 84b097800250d17d1872b34c4daadcf5
   ```

將 GuardDuty 管理員帳戶合併到單一組織委派的 GuardDuty 管理員帳戶下

GuardDuty 建議使用關聯 AWS Organizations 至來管理委派管理員帳戶下的成 GuardDuty 員帳戶。您可以使用下面概述的範例程序，在單一 GuardDuty委派管理員帳戶下，合併組織中透過邀請關聯的 GuardDuty 管理員帳戶和成員。

> **Note**
>
> 已由委派系統管理員帳戶所管理的帳戶，或與委派 GuardDuty 系統管理員帳戶相關聯的作用中成 GuardDuty 員帳戶無法新增至不同的委派 GuardDuty 系統管理員帳戶。每個組織每個區域只能有一個委派 GuardDuty 管理員帳戶，而每個成員帳戶只能有一個委派的 GuardDuty 管理員帳戶。

選擇其中一種存取方法，將 GuardDuty 管理員帳戶合併到單一委派的 GuardDuty 管理員帳戶下。

Console

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/

   若要登入，請使用組織管理帳戶的憑證。

2. 您要管理的所有帳戶都 GuardDuty 必須是組織的一部分。如需將帳戶新增至組織的相關資訊，請參閱邀請 AWS 帳戶 加入您的組織。

3. 確定所有成員帳戶都與您要指定為單一委派 GuardDuty 管理員帳戶的帳戶相關聯。取消仍與預先存在的管理員帳戶相關聯的任何成員帳戶的關聯。

   下列步驟可協助您取消成員帳戶與預先存在的管理員帳戶之間的關聯：

   a. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/

   b. 若要登入，請使用預先存在的管理員帳戶的憑證。

   c. 在導覽窗格中，選擇帳戶。

   d. 在帳戶頁面上，選取一個或多個您要取消與管理員帳戶關聯的帳戶。

   e. 選擇動作，然後選擇取消帳戶關聯。

   f. 選擇確認以完成該步驟。

4. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/

   若要登入，請使用管理帳戶憑證。

5. 在導覽窗格中，選擇設定。在 [設定] 頁面上，指定組織的委派 GuardDuty 管理員帳戶。

6. 登入指定的委派 GuardDuty 管理員帳戶。

7. 從組織新增成員。如需詳細資訊，請參閱 管理 GuardDuty 帳戶 AWS Organizations。

API/CLI

1. 您要管理的所有帳戶都 GuardDuty 必須是組織的一部分。如需將帳戶新增至組織的相關資訊，請參閱邀請 AWS 帳戶 加入您的組織。
2. 確定所有成員帳戶都與您要指定為單一委派 GuardDuty 管理員帳戶的帳戶相關聯。

   a. 執行DisassociateMembers以取消與現有管理員帳戶相關聯的任何成員帳戶的關聯。

   b. 或者，您可以使用 AWS Command Line Interface 來運行以下命令，並將 *777777777777* 替換為要取消與成員帳戶關聯的預先存在管理員帳戶的檢測器 ID。使用您要取消關聯的成員帳戶的 AWS 帳戶 ID 取代 *666666666666*。

   ```
   aws guardduty disassociate-members --detector-id 777777777777 --account-ids 666666666666
   ```

3. 執行EnableOrganizationAdminAccount以委派 GuardDuty 管理員帳戶的身分委派。 AWS 帳戶

   或者，您也可以使用 AWS Command Line Interface 來執行下列命令來委派委派的 GuardDuty 系統管理員帳戶：

   ```
   aws guardduty enable-organization-admin-account --admin-account-id 777777777777
   ```

4. 從組織新增成員。如需詳細資訊，請參閱 Create or add member member accounts using API。

> **Important**
>
> 為了最大限度地發揮區域服務的 GuardDuty有效性，我們建議您指定委派的 GuardDuty 管理員帳戶，並在每個區域中新增所有成員帳戶。

同時 GuardDuty 在多個帳戶中啟用

使用以下方法同時 GuardDuty 在多個帳戶中啟用。

使用 Python 腳本同時 GuardDuty 在多個帳戶中啟用

您可以使用 Amazon 多帳戶指令碼範例儲存庫中的指令碼，自動啟用或停用 GuardDuty 多個帳戶。GuardDuty 使用本節中的程序來啟 GuardDuty 用使用 Amazon EC2 的成員帳戶清單。如需使用停用指令碼或在本機設定指令碼的相關資訊，請參閱分享連結中的指示。

該enableguardduty.py腳本啟用 GuardDuty，從管理員帳戶發送邀請，並接受所有成員帳戶中的邀請。結果是系統管理員 GuardDuty 帳戶，其中包含所有成員帳戶的所有安全性發現項目。由於由「區域」隔離，因 GuardDuty 此每個成員帳戶的發現項目會累計至管理員帳戶中對應的「區域」。例如，管理員帳戶中的 us-east-1 區域包含所有相關聯成 GuardDuty 員帳戶中所有 us-east-1 發現項目的安全性發現項目。

這些指令碼在共用 IAM 角色上具有與受管政策 AWS 受管理的策略：AmazonGuardDutyFullAccess 的相依性。此原則提供實體存取權限， GuardDuty 且必須出現在系統管理員帳戶以及您要啟用的每個帳戶中 GuardDuty。

依預設，下列程序會 GuardDuty 在所有可用的區域中啟用。您只能使用選擇性--enabled_regions引數並提供區域的逗號分隔清單，才能 GuardDuty 在指定的區域中啟用。您也可以選擇開啟 enableguardduty.py 和編輯 gd_invite_message 字串，來自訂傳送至成員帳戶的邀請訊息。

1. 在 GuardDuty 管理員帳戶中建立 IAM 角色，並附加要啟用的AWS 受管理的策略：AmazonGuardDutyFullAccess政策 GuardDuty。
2. 在您 GuardDuty 希望由管理員帳戶管理的每個成員帳戶中建立 IAM 角色。此角色的名稱必須與步驟 1 中建立的角色相同，它應該允許系統管理員帳戶做為受信任的實體，而且它應該具有與先前所述相同的 AmazonGuardDutyFullAccess 受管理原則。
3. 啟動具有下列信任關係之連接角色的新 Amazon Linux 執行個體，以允許執行個體擔任服務角色。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

4. 登入新的執行個體，然後執行下列命令進行設定。

```
sudo yum install git python
sudo yum install python-pip
pip install boto3
```

```
aws configure
git clone https://github.com/aws-samples/amazon-guardduty-multiaccount-scripts.git
cd amazon-guardduty-multiaccount-scripts
sudo chmod +x disableguardduty.py enableguardduty.py
```

5. 建立 CSV 檔案，在當中包含您在步驟 2 中新增角色的成員帳戶 ID 清單和電子郵件。帳戶必須每行出現一個，而且帳戶 ID 與電子郵件地址必須以逗號分隔，如下所示。

```
111122223333,guardduty-member@organization.com
```

> **Note**
>
> CSV 檔案必須位於與 `enableguardduty.py` 指令碼相同的位置。您可以使用下列方法將現有 CSV 檔案從 Amazon S3 複製到目前的目錄。
>
> ```
> aws s3 cp s3://my-bucket/my_key_name example.csv
> ```

6. 執行 Python 指令碼。請務必提供您的 GuardDuty 系統管理員帳戶 ID、在第一個步驟中建立的角色名稱，以及 CSV 檔案的名稱做為引數。

```
python enableguardduty.py --master_account 444455556666 --assume_role
 roleName accountID.csv
```

估算成 GuardDuty 本

您可以使用 GuardDuty 主控台或 API 作業估算的每日平均使用成本 GuardDuty。在 30 天免費試用期內，成本估算可推算您在試用期後的預估成本。如果您在多帳戶環境中操作，您的 GuardDuty 管理員帳戶可以監控所有成員帳戶的成本指標。

您可以根據下列指標檢視成本估算：

- 帳號 ID — 列出您帳戶的預估費用，如果您是以管理員帳戶帳戶操作，則列出您的會 GuardDuty 員帳戶的預估費用。
- 資料來源 — 針對下列資料來源類型列出指定資 GuardDuty 料來源的預估成本：VPC 流程記錄、CloudTrail 管理記錄、 CloudTrail 資料事件或 DNS 記錄。
- 功能 — 列出下列 GuardDuty 功能的指定資料來源預估成本：S3 的 CloudTrail 資料事件、EKS 稽核記錄監控、EBS 磁碟區資料、RDS 登入活動、EKS 執行階段監控、Fargate 執行階段監控、EC2 執行階段監控或 Lambda 網路活動監控。
- S3 儲存貯體：列出在環境中帳戶的指定儲存貯體或最昂貴儲存貯體上 S3 資料事件的預估成本。

> **Note**
>
> 只有在帳戶啟用 S3 保護時，才能使用 S3 儲存貯體統計資料。如需詳細資訊，請參閱 Amazon S3 保護在 Amazon GuardDuty。

瞭解 GuardDuty 計算使用成本的方式

主機中顯示的預估值可能與 GuardDuty 主機上的 AWS Billing and Cost Management 預估值略有不同。下列清單說明 GuardDuty 估計使用成本的方式：

- GuardDuty 使用量估計僅適用於目前的區域。
- GuardDuty 使用費用是根據最近 30 天的使用量而定。
- 試用用量成本預估值包括目前在試用期內的基礎資料來源和功能的預估值。中的每個圖徵和資料來源都 GuardDuty 有其自己的試用期，但可能會與的試用期 GuardDuty或同時啟用的其他功能重疊。
- GuardDuty 使用 GuardDuty 量估算包含每個區域的批量定價折扣，詳情請參閱 Amazon GuardDuty 定價頁面，但僅適用於滿足大量定價層級的個別帳戶。大量定價折扣不包括在組織內帳戶之間合併總用量的預估值中。如需有關合併用量大量折扣定價的資訊，請參閱 AWS 帳單：大量折扣。

- 組織 AWS 帳戶 中每個使用費用的總和可能不一定與所選資料來源的最近 30 天預估費用相同。定價層可能會隨著 GuardDuty 處理更多事件或資料而變更。如需詳細資訊，請參閱AWS Billing 使用指南中的定價層。

執行階段監控 — EC2 執行個體的 VPC 流程日誌如何影響使用成本

當您在 EKS 執行個體或 EC2 執行個體的執行階段監控中管理安全代理程式 (無論GuardDuty 是手動或透過 GuardDuty)，且目前部署在 Amazon EC2 執行個體並收集的執行期事件類型從此執行個體接收，則不 GuardDuty 會 AWS 帳戶 針對此 Amazon EC2 執行個體的 VPC 流程日誌分析收費。這有助於 GuardDuty 避免帳戶中的雙重使用成本。

如何 GuardDuty 估計 CloudTrail 事件的使用成本

啟用時 GuardDuty，它會自動開始使用所選帳戶中記錄的 AWS CloudTrail 事件日誌 AWS 區域。GuardDuty 複寫全域服務事件記錄檔，然後在您 GuardDuty 已啟用的每個區域中獨立處理這些事件。這有助於 GuardDuty 維護每個區域中的使用者和角色設定檔，以識別異常情況。

您的 CloudTrail 配置不會影響 GuardDuty 使用成本或 GuardDuty 處理事件日誌的方式。您的 GuardDuty 使用費用會受到您使用記錄的 AWS API 的影響 CloudTrail。如需詳細資訊，請參閱 AWS CloudTrail 事件記錄。

檢視 GuardDuty 使用量統計

選擇您偏好的存取方式，以檢視您 GuardDuty帳戶的使用統計資料。如果您是 GuardDuty 管理員帳戶，以下方法將幫助您查看所有成員的使用統計信息。

Console

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/

   確保使用 GuardDuty 管理員帳戶帳戶。
2. 在導覽窗格中，選擇用量。
3. 在 [使用量] 頁面上，具有成員帳戶的 GuardDuty 管理員帳戶可以檢視過去 30 天的預估組織成本。這是您組織的估計總使用費用。
4. GuardDuty 擁有成員的管理員帳戶可以依資料來源或帳戶檢視使用成本明細。個別或獨立帳戶可以依資料來源檢視劃分。

   如果您有成員帳戶，則可以在「帳戶」表格中選取該帳戶，以檢視個別帳戶的統計資料。

在 [依資料來源] 索引標籤下，當您選取具有相關使用費用的資料來源時，帳戶層級的相應成本細目總和可能不一定相同。

API/CLI

使用 GuardDuty 管理員帳戶帳戶的憑據運行 GetUsageStatisticsAPI 操作。提供下列資訊以執行命令：

- (必要) 提供您要擷取其統計資料之帳戶的區域 GuardDuty 偵測器 ID。
- (必要) 提供要擷取的統計資料類型之一：SUM_BY_ACCOUNT | SUM_BY_DATA_SOURCE | SUM_BY_RESOURCE | SUM_BY_FEATURE | TOP_ACCOUNTS_BY_FEATURE。

  目前TOP_ACCOUNTS_BY_FEATURE不支援擷取的使用狀況統計資料RDS_LOGIN_EVENTS。
- (必要) 提供一或多個資料來源或功能，以查詢您的使用情況統計資料。
- (選用) 提供您要擷取用量統計資料的帳戶 ID 清單。

您也可以使用 AWS Command Line Interface。以下命令是關於擷取由帳戶計算的所有資料來源和圖徵的使用統計資料的範例。確保使用您的有效偵測器 ID 取代 detector-id。若為獨立帳戶，此命令僅會傳回過去 30 天內帳戶的用量成本。如果您是擁有成 GuardDuty 員帳戶的管理員帳戶，您會看到所有成員依帳戶列出的費用。

要查找您detectorId的帳戶和當前區域的，請參閱 https://console.aws.amazon.com/guardduty/ 主控台中的 「設置」 頁面。

以您要計算使用量統計資料的類型來取SUM_BY_ACCOUNT代。

僅監視資料來源的成本

```
aws guardduty get-usage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --usage-statistic-type SUM_BY_ACCOUNT --usage-criteria '{"DataSources":
["FLOW_LOGS", "CLOUD_TRAIL", "DNS_LOGS", "S3_LOGS", "KUBERNETES_AUDIT_LOGS",
 "EC2_MALWARE_SCAN"]}'
```

若要監視功能的成本

```
aws guardduty get-usage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --usage-statistic-type SUM_BY_ACCOUNT --usage-criteria '{"Features":
["FLOW_LOGS", "CLOUD_TRAIL", "DNS_LOGS", "S3_DATA_EVENTS", "EKS_AUDIT_LOGS",
```

```
"EBS_MALWARE_PROTECTION", "RDS_LOGIN_EVENTS", "LAMBDA_NETWORK_LOGS",
"EKS_RUNTIME_MONITORING", "FARGATE_RUNTIME_MONITORING", "EC2_RUNTIME_MONITORING"]}'
```

Amazon GuardDuty 中的安全性

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 與您共同肩負的責任。共同責任模式將其描述為雲端的安全性和雲端中的安全性：

- 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。第三方稽核人員會定期測試和驗證我們安全性的有效性，做為 AWS 合規計劃的一部分。若要了解適用於 GuardDuty 的合規計畫，請參閱 AWS 的合規計畫服務範圍。
- 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、您公司的要求和適用法律和法規。

本文件有助於您了解如何在使用 GuardDuty 時套用共同責任模式。其中會示範如何設定 GuardDuty 以符合您的安全與合規目標。您也會了解如何使用其他 AWS 服務來協助監控並保護 GuardDuty 資源。

目錄

Amazon 的數據保護 GuardDuty

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

基於資料保護目的，我們建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 登入資料並設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。

- 使用 SSL/TLS 與 AWS 資源進行通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用設定 API 和使用者活動記錄 AWS CloudTrail。
- 使用 AWS 加密解決方案以及其中的所有默認安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在透過命令列介面或 API 存取時需要經 AWS 過 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-2 概觀。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用主控台、API GuardDuty 或 AWS SDK 時 AWS 服務 使用或其他使用時。 AWS CLI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。

靜態加密

所有 GuardDuty 客戶數據均使用加密解決方案進行靜 AWS 態加密。

GuardDuty 資料 (例如發現項目) 會使用 AWS Key Management Service (AWS KMS) 使用 AWS 擁有的客戶管理金鑰進行靜態加密。

傳輸中加密

GuardDuty 分析來自其他服務的記錄資料。這會使用 HTTPS 和 KMS 加密來自這些服務的所有傳輸中的資料。一旦 GuardDuty 從日誌中提取所需的信息，它們將被丟棄。如需有關如何 GuardDuty 使用其他服務資訊的詳細資訊，請參閱資GuardDuty 料來源。

GuardDuty 資料在服務之間傳輸過程中會加密。

選擇不使用您的資料以改善服務

您可以使用退出政策選擇 AWS Organizations 退出使用您的數據來開發 GuardDuty 和改進以及其他 AWS 安全服務。即使目前 GuardDuty 沒有收集任何此類數據，您也可以選擇退出。如需有關如何選擇退出的詳細資訊，請參閱《AWS Organizations 使用者指南》中的 AI 服務選擇退出政策。

> **Note**
>
> 若要使用退出政策，您的 AWS 帳戶必須由集中管理 AWS Organizations。如果您尚未為 AWS 帳戶建立組織，請參閱AWS Organizations 使用者指南中的建立和管理組織。

選擇退出具有以下影響：

- GuardDuty 在您選擇退出之前，將刪除其為改進服務目的而收集和存儲的數據（如果有的話）。
- 選擇退出後， GuardDuty 將不再收集或儲存這些資料以改善服務目的。

下列主題說明中 GuardDuty 的每個功能如何處理您的資料以改善服務。

目錄

GuardDuty 運行時監控

GuardDuty 執行階段監控可為您環境中的 Amazon Elastic Kubernetes Service (Amazon EKS) 叢集、僅限 Amazon 彈性容器服務 (AWS Fargate (Fargate) Amazon ECS) 和亞馬遜彈性運算雲端 (Amazon EC2) 執行個體提供執行時期威脅偵測。 AWS 啟用執行階段監視並部署資源的 GuardDuty 安全代理程式之後， GuardDuty 開始監視和分析與資源相關聯的執行階段事件。這些執行階段事件類型包括處理序事件、容器事件、DNS 事件等。如需詳細資訊，請參閱 使用收集的執行階段事 GuardDuty 件類型。

雖然 GuardDuty 現在會收集您可以直接指向工作負載的命令列引數，但它目前並未將這些引數用於服務改善目的 (future 可能會這樣做)。我們已經開始收集命令列引數，以期待即將發佈的新威脅偵測規則和發現項目。您的信任、隱私和內容的安全性是我們最重視的，我們也會確保我們的使用符合我們對您的承諾。如需詳細資訊，請參閱資料隱私權常見問答集。

GuardDuty 惡意程式碼

GuardDuty 惡意軟體防護會掃描並偵測 EBS 磁碟區中包含的惡意程式碼，連接至可能受到危害的 Amazon EC2 執行個體和容器工 當 GuardDuty 惡意程式碼防護將 EBS 磁碟區檔案識別為惡意或有害時， GuardDuty 惡意程式碼防護會收集並儲存此檔案，以開發並改善其惡意程式碼偵測和服務。 GuardDuty 該文件也可以用於開發和改進其他 AWS 安全服務。您的信任、隱私和內容的安全性是我們最重視的，我們也會確保我們的使用符合我們對您的承諾。如需詳細資訊，請參閱資料隱私權常見問答集。

記錄 Amazon GuardDuty API 呼叫 AWS CloudTrail

Amazon GuardDuty 與服務整合在一起AWS CloudTrail，可提供中使用者、角色或服務所採取的動作記錄的AWS服務 GuardDuty。 CloudTrail 擷取 GuardDuty 做為事件的所有 API 呼叫，包括來自

GuardDuty 主控台的呼叫，以及從 API 的程 GuardDuty 式碼呼叫。如果您建立追蹤，您可以啟用持續交付 CloudTrail 事件到 Amazon Simple Storage Service (Amazon S3) 儲存貯體，包括 GuardDuty. 如果您未設定追蹤，您仍然可以在 [事件歷程記錄] 中檢視 CloudTrail 主控台中最近的事件。使用收集的資訊 CloudTrail，您可以判斷提出要求 GuardDuty、提出要求的 IP 位址、提出要求的人員、提出要求的時間，以及其他詳細資訊。

若要取得有關的更多資訊 CloudTrail，包括如何設定和啟用它，請參閱《AWS CloudTrail使用者指南》。

GuardDuty 中的資訊 CloudTrail

CloudTrail 在您創建AWS帳戶時，您的帳戶已啟用。當受支援的事件活動發生在中時 GuardDuty，該活動會與 CloudTrail 事件歷史記錄中的其他AWS服務事件一起記錄在事件中。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 事件歷程記錄檢視事件。

如需AWS帳戶中持續記錄事件 (包括的事件) GuardDuty，請建立追蹤。追蹤可 CloudTrail 將日誌檔交付到 Amazon S3 儲存貯體。根據預設，當您在主控台建立追蹤記錄時，追蹤記錄會套用到所有區域。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。此外，您還可以設定其他AWS服務，以進一步分析 CloudTrail 記錄中收集的事件資料並採取行動。如需詳細資訊，請參閱：

- 建立追蹤的概觀
- CloudTrail 支援的服務和整合
- 設定 Amazon SNS 通知 CloudTrail
- 從多個區域接收 CloudTrail 日誌文件並從多個帳戶接收 CloudTrail 日誌文件

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：

- 是否使用根使用者或 IAM 使用者登入憑證提出該請求
- 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。

GuardDuty 控制平面事件 CloudTrail

依預設，會將 Amazon GuardDuty API 參考中提供的所有 GuardDuty API 操作 CloudTrail 記錄為 CloudTrail 檔案中的事件。

GuardDuty 資料事件 CloudTrail

GuardDuty 運行時監控使用部署到 Amazon 彈性 Kubernetes 服務 (Amazon EKS) 叢集、Amazon 彈性運算雲端 (Amazon EC2) 執行個體和 (僅限 Amazon 彈性容器服務 AWS Fargate (Amazon ECS)) 任務的 GuardDuty 安全代理程式來收集收集的執行期事件類型為您的AWS工作負載收集的附加元件 (`aws-guardduty-agent`)，然後將它們傳送至 GuardDuty 威脅偵測和分析。

記錄和監控資料事件

您可以選擇性地設定AWS CloudTrail記錄檔，以檢視 GuardDuty Security Agent 的資料事件。

若要建立和配置 CloudTrail，請參閱《AWS CloudTrail使用指南》中的資料事件，並遵循中使用進階事件選取器記錄資料事件的指示。AWS Management Console在記錄追蹤時，請務必進行下列變更：

- 針對 [資料] 事件類型，選擇GuardDuty 偵測器。
- 對於日誌選取器範本，選擇記錄所有事件。
- 展開組態的 JSON 檢視。它應類似於以下 JSON：

```
[
  {
    "name": "",
    "fieldSelectors": [
      {
        "field": "eventCategory",
        "equals": [
          "Data"
        ]
      },
      {
        "field": "resources.type",
        "equals": [
          "AWS::GuardDuty::Detector"
        ]
      }
    ]
  }
]
```

啟用追蹤的選取器後，請瀏覽至 Amazon S3 主控台 https://console.aws.amazon.com/s3/。您可以從設定 CloudTrail 日誌時選擇的 S3 儲存貯體下載資料事件。

範例： GuardDuty 記錄檔項目

追蹤是一種組態，可讓事件以日誌檔的形式傳遞到您指定的 Amazon S3 儲存貯體。 CloudTrail 記錄檔包含一或多個記錄項目。事件代表來自任何來源的單一請求，包括有關請求的操作，動作的日期和時間，請求參數等信息。 CloudTrail 日誌文件不是公共 API 調用的有序堆棧跟踪，因此它們不會以任何特定順序顯示。

下列範例顯示示範資料平面事件的 CloudTrail 記錄項目。


```
{
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "111122223333:aws:ec2-instance:i-123412341234example",
            "arn": "arn:aws:sts::111122223333:assumed-role/aws:ec2-
instance/i-123412341234example",
            "accountId": "111122223333",
            "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "111122223333:aws:ec2-instance",
                    "arn": "arn:aws:iam::111122223333:role/aws:ec2-instance",
                    "accountId": "111122223333",
                    "userName": "aws:ec2-instance"
                },
                "attributes": {
                    "creationDate": "2023-03-05T04:00:21Z",
                    "mfaAuthenticated": "false"
                },
                "ec2RoleDelivery": "2.0"
            }
        },
        "eventTime": "2023-03-05T06:03:49Z",
        "eventSource": "guardduty.amazonaws.com",
        "eventName": "SendSecurityTelemetry",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "54.240.230.177",
        "userAgent": "aws-sdk-rust/0.54.1 os/linux lang/rust/1.66.0",
        "requestParameters": null,
        "responseElements": null,
        "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbb",
```

```
        "readOnly": false,
        "resources": [{
            "accountId": "111122223333",
            "type": "AWS::GuardDuty::Detector",
            "ARN": "arn:aws:guardduty:us-
west-2:111122223333:detector/12abc34d567e8fa901bc2d34e56789f0"
        }],
        "eventType": "AwsApiCall",
        "managementEvent": false,
        "recipientAccountId": "111122223333",
        "eventCategory": "Data",
        "tlsDetails": {
            "tlsVersion": "TLSv1.2",
            "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
            "clientProvidedHostHeader": "guardduty-data.us-east-1.amazonaws.com"
        }
    }
```

下列範例顯示示範`CreateIPThreatIntelSet`動作 (控制平面事件) 的 CloudTrail 記錄項目。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::444455556666:user/Alice",
        "accountId": "444455556666",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-06-14T22:54:20Z"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::444455556666:user/Alice",
                "accountId": "444455556666",
                "userName": "Alice"
            }
        }
    },
    "eventTime": "2018-06-14T22:57:56Z",
```

```
    "eventSource": "guardduty.amazonaws.com",
    "eventName": "CreateThreatIntelSet",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "54.240.230.177",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "detectorId": "12abc34d567e8fa901bc2d34e56789f0",
        "name": "Example",
        "format": "TXT",
        "activate": false,
        "location": "https://s3.amazonaws.com/bucket.name/file.txt"
    },
    "responseElements": {
        "threatIntelSetId": "1ab200428351c99d859bf61992460d24"
    },
    "requestID": "5f6bf981-7026-11e8-a9fc-5b37d2684c5c",
    "eventID": "81337b11-e5c8-4f91-b141-deb405625bc9",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "444455556666"
}
```


從這個事件資訊可以判斷出，這是在 GuardDuty 中建立威脅清單 `Example` 的請求。您也可看到，該請求是由名為 Alice 的使用者於 2018 年 6 月 14 日發出。

Amazon Identity and Access Management GuardDuty

AWS Identity and Access Management (IAM) 可協助系統管理員安全地控制 AWS 資源存取權。 AWS 服務 IAM 管理員控制哪些人可以通過身份驗證 (登入) 和授權 (具有權限) 來使用 GuardDuty 資源。IAM 是您可以使用的 AWS 服務 ，無需額外付費。

主題

- 物件
- 使用身分驗證
- 使用政策管理存取權
- Amazon 如何與 IAM 合 GuardDuty 作
- Amazon 的基於身份的政策示例 GuardDuty
- 在 Amazon 使用服務連結角色 GuardDuty

- AWS Amazon 的受管政策 GuardDuty
- 疑難排解 Amazon GuardDuty 身分和存取

物件

您使用 AWS Identity and Access Management (IAM) 的方式會有所不同，具體取決於您在進行的工作 GuardDuty。

服務使用者 — 如果您使用 GuardDuty 服務執行工作，則管理員會為您提供所需的認證和權限。當您使用更多 GuardDuty 功能來完成工作時，您可能需要其他權限。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果無法存取中的圖徵 GuardDuty，請參閱疑難排解 Amazon GuardDuty 身分和存取。

服務管理員 — 如果您負責公司的 GuardDuty 資源，您可能擁有完整的存取權 GuardDuty。決定您的服務使用者應該存取哪些 GuardDuty 功能和資源是您的工作。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。若要進一步瞭解貴公司如何搭配使用 IAM GuardDuty，請參閱Amazon 如何與 IAM 合 GuardDuty 作。

IAM 管理員 — 如果您是 IAM 管理員，您可能想要瞭解如何撰寫政策來管理存取權限的詳細資訊 GuardDuty。若要檢視可在 IAM 中使用的 GuardDuty 基於身分的政策範例，請參閱。Amazon 的基於身份的政策示例 GuardDuty

使用身分驗證

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

您可以使用透過 AWS 身分識別來源提供的認證，以聯合身分識別身分登入。 AWS IAM Identity Center (IAM 身分中心) 使用者、貴公司的單一登入身分驗證，以及您的 Google 或 Facebook 登入資料都是聯合身分識別的範例。您以聯合身分登入時，您的管理員先前已設定使用 IAM 角色的聯合身分。當您使 AWS 用同盟存取時，您會間接擔任角色。

根據您的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需有關登入的詳細資訊 AWS，請參閱《AWS 登入 使用指南》 AWS 帳戶中的如何登入您的。

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

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

AWS 帳戶 根使用者

當您建立時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取該帳戶中的所有資源 AWS 服務和資源。此身分稱為 AWS 帳戶 root 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需這些任務的完整清單，了解需以根使用者登入的任務，請參閱 IAM 使用者指南中的需要根使用者憑證的任務。

聯合身分

最佳作法是要求人類使用者 (包括需要系統管理員存取權的使用者) 使用與身分識別提供者的同盟，才能使用臨時登入資料進行存取 AWS 服務 。

聯合身分識別是來自企業使用者目錄的使用者、Web 身分識別提供者、Identi ty Center 目錄，或使用透過身分識別來源提供的認證進行存取 AWS 服務 的任何使用者。 AWS Directory Service同盟身分存取時 AWS 帳戶，他們會假設角色，而角色則提供臨時認證。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，也可以連線並同步到自己身分識別來源中的一組使用者和群組，以便在所有應用程式 AWS 帳戶 和應用程式中使用。如需 IAM Identity Center 的相關資訊，請參閱 AWS IAM Identity Center 使用者指南中的什麼是 IAM Identity Center？。

IAM 使用者和群組

IAM 使用者是您內部的身分，具 AWS 帳戶 有單一人員或應用程式的特定許可。建議您盡可能依賴暫時憑證，而不是擁有建立長期憑證 (例如密碼和存取金鑰) 的 IAM 使用者。但是如果特定使用案例需要擁有長期憑證的 IAM 使用者，建議您輪換存取金鑰。如需更多資訊，請參閱 IAM 使用者指南中的為需要長期憑證的使用案例定期輪換存取金鑰。

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

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

IAM 角色

IAM 角色是您 AWS 帳戶 內部具有特定許可的身分。它類似 IAM 使用者，但不與特定的人員相關聯。您可以切換角色，在中暫時擔任 IAM 角色。 AWS Management Console 您可以透過呼叫 AWS CLI 或 AWS API 作業或使用自訂 URL 來擔任角色。如需使用角色的方法更多相關資訊，請參閱 IAM 使用者指南中的使用 IAM 角色。

使用暫時憑證的 IAM 角色在下列情況中非常有用：

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

的執行個體設定檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得暫時憑證。如需更多資訊，請參閱 IAM 使用者指南中的利用 IAM 角色來授予許可給 Amazon EC2 執行個體上執行的應用程式。

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

使用政策管理存取權

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

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

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

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

身分型政策

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

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

資源型政策

資源型政策是連接到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源

的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

資源型政策是位於該服務中的內嵌政策。您無法在以資源為基礎的政策中使用 IAM 的 AWS 受管政策。

存取控制清單 (ACL)

存取控制清單 (ACL) 可控制哪些委託人 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

Amazon S3 和 Amazon VPC 是支援 ACL 的服務範例。 AWS WAF若要進一步了解 ACL，請參閱 Amazon Simple Storage Service 開發人員指南中的存取控制清單 (ACL) 概觀。

其他政策類型

AWS 支援其他較不常見的原則類型。這些政策類型可設定較常見政策類型授予您的最大許可。

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

多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。要了解如何在涉及多個政策類型時 AWS 確定是否允許請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

Amazon 如何與 IAM 合 GuardDuty 作

在您使用 IAM 管理存取權限之前 GuardDuty，請先了解哪些 IAM 功能可搭配使用 GuardDuty。

您可以與 Amazon 搭配使用的 IAM 功能 GuardDuty

IAM 功能	GuardDuty 支持
身分型政策	是
資源型政策	否
政策動作	是
政策資源	是
政策條件索引鍵	是
ACL	否
ABAC(政策中的標籤)	部分
臨時憑證	是
主體許可	是
服務角色	是
服務連結角色	是

若要深入瞭解如何以 GuardDuty 及其他 AWS 服務如何使用大多數 IAM 功能，請參閱 IAM 使用者指南中的搭配 IAM 使用的AWS 服務。

以身分識別為基礎的原則 GuardDuty

支援身分型政策	是

身分型政策是可以連接到身分 (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。

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。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。如要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素參考。

以身分識別為基礎的原則範例 GuardDuty

若要檢視以 GuardDuty 身分為基礎的原則範例，請參閱。Amazon 的基於身份的政策示例 GuardDuty

以資源為基礎的政策 GuardDuty

支援以資源基礎的政策	否

資源型政策是附加到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

若要啟用跨帳戶存取，您可以指定在其他帳戶內的所有帳戶或 IAM 實體，作為資源型政策的主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主體和資源位於不同時 AWS 帳戶，受信任帳戶中的 IAM 管理員也必須授與主體實體 (使用者或角色) 權限，才能存取資源。其透過將身分型政策連接到實體來授與許可。不過，如果資源型政策會為相同帳戶中的主體授予存取，這時就不需要額外的身分型政策。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 角色與資源型政策有何差異。

的政策動作 GuardDuty

支援政策動作	是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON 政策的 Action 元素描述您可以用來允許或拒絕政策中存取的動作。原則動作通常與關聯的 AWS API 作業具有相同的名稱。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

若要查看 GuardDuty 動作清單，請參閱服務授權參考 GuardDuty中 Amazon 定義的動作。

中的策略動作在動作之前 GuardDuty 使用下列前置詞：

```
guardduty
```

若要在單一陳述式中指定多個動作，請用逗號分隔。

```
"Action": [
      "guardduty:action1",
      "guardduty:action2"
         ]
```

若要檢視以 GuardDuty 身分為基礎的原則範例，請參閱。Amazon 的基於身份的政策示例 GuardDuty

的政策資源 GuardDuty

支援政策資源	是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Resource JSON 政策元素可指定要套用動作的物件。陳述式必須包含 Resource 或 NotResource 元素。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

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

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

要查看 GuardDuty 資源類型及其 ARN 的列表，請參閱服務授權參考 GuardDuty中由 Amazon 定義的資源。若要了解可以使用哪些動作指定每個資源的 ARN，請參閱 Amazon GuardDuty 定義的動作。

若要檢視以 GuardDuty 身分為基礎的原則範例，請參閱。Amazon 的基於身份的政策示例 GuardDuty

的政策條件索引鍵 GuardDuty

支援服務特定政策條件金鑰	是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

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

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

AWS 支援全域條件金鑰和服務特定條件金鑰。若要查看所有 AWS 全域條件金鑰，請參閱《IAM 使用者指南》中的AWS 全域條件內容金鑰。

若要查看 GuardDuty 條件金鑰清單，請參閱服務授權參考 GuardDuty中的 Amazon 條件金鑰。若要了解您可以使用條件金鑰的動作和資源，請參閱 Amazon 定義的動作 GuardDuty。

若要檢視以 GuardDuty 身分為基礎的原則範例，請參閱。Amazon 的基於身份的政策示例 GuardDuty

GuardDuty 中的存取控制清單 (ACL)

支援 ACL	否

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

以屬性為基礎的存取控制 (ABAC) 搭配 GuardDuty

支援 ABAC (政策中的標籤)	部分

屬性型存取控制 (ABAC) 是一種授權策略，可根據屬性來定義許可。在中 AWS，這些屬性稱為標籤。您可以將標籤附加到 IAM 實體 (使用者或角色) 和許多 AWS 資源。為實體和資源加上標籤是 ABAC 的第一步。您接著要設計 ABAC 政策，允許在主體的標籤與其嘗試存取的資源標籤相符時操作。

ABAC 在成長快速的環境中相當有幫助，並能在政策管理變得繁瑣時提供協助。

若要根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件金鑰，在政策的條件元素中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需 ABAC 的詳細資訊，請參閱《IAM 使用者指南》中的什麼是 ABAC?。如要查看含有設定 ABAC 步驟的教學課程，請參閱《IAM 使用者指南》中的使用屬性型存取控制 (ABAC)。

使用臨時登入資料 GuardDuty

支援臨時憑證	是

當您使用臨時憑據登錄時，某些 AWS 服務 不起作用。如需其他資訊，包括哪些 AWS 服務 與臨時登入資料搭配AWS 服務 使用，請參閱 IAM 使用者指南中的 IAM。

如果您使用除了使用者名稱和密碼以外的任何方法登入，則您正在 AWS Management Console 使用臨時認證。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取時，該程序會自動建立暫時認證。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需切換角色的詳細資訊，請參閱《IAM 使用者指南》中的切換至角色 (主控台)。

您可以使用 AWS CLI 或 AWS API 手動建立臨時登入資料。然後，您可以使用這些臨時登入資料來存取 AWS。 AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱 IAM 中的暫時性安全憑證。

的跨服務主體權限 GuardDuty

支援轉寄存取工作階段 (FAS)	是

當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。

GuardDuty 的服務角色

支援服務角色	是

服務角色是服務擔任的 IAM 角色，可代您執行動作。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。

> **Warning**
>
> 變更服務角色的權限可能會中斷 GuardDuty 功能。只有在 GuardDuty 提供指引時才編輯服務角色。

服務連結角色 GuardDuty

支援服務連結角色	是

服務連結角色是一種連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需有關建立或管理 GuardDuty 服務連結角色的詳細資訊，請參閱在 Amazon 使用服務連結角色 GuardDuty。

如需建立或管理服務連結角色的詳細資訊，請參閱可搭配 IAM 運作的AWS 服務。在表格中尋找服務，其中包含服務連結角色欄中的 Yes。選擇是連結，以檢視該服務的服務連結角色文件。

Amazon 的基於身份的政策示例 GuardDuty

依預設，使用者和角色沒有建立或修改 GuardDuty資源的權限。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 來執行工作。若要授予使用者對其

所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

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》中的建立 IAM 政策。

有關由定義的動作和資源類型的詳細資訊 GuardDuty，包括每種資源類型的 ARN 格式，請參閱服務授權參考 GuardDuty中適用於 Amazon 的動作、資源和條件金鑰。

主題

- 政策最佳實務
- 使用 GuardDuty 主控台
- 啟用 GuardDuty 的必要許可
- 允許使用者檢視他們自己的許可
- 用於授予唯讀存取權的自訂 IAM 政策 GuardDuty
- 拒絕存取 GuardDuty 發現項目
- 使用自訂 IAM 政策限制對 GuardDuty 資源的存取

政策最佳實務

以身分識別為基礎的政策會決定某人是否可以建立、存取或刪除您帳戶中的 GuardDuty 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管原則並邁向最低權限權限 — 若要開始授與使用者和工作負載的權限，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們在您的 AWS 帳戶. 建議您透過定義特定於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。如需更多資訊，請參閱 IAM 使用者指南中的 AWS 受管政策或任務職能的AWS 受管政策。
- 套用最低許可許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的權限。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。您也可以使用條件來授與對服務動作的存取權 (如透過特定) 使用這些動作 AWS 服務，例如 AWS CloudFormation。如需更多資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：條件。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access

Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您編寫安全且實用的政策。如需更多資訊，請參閱 IAM 使用者指南中的 IAM Access Analyzer 政策驗證。

- 需要多因素身份驗證 (MFA) — 如果您的案例需要 IAM 使用者或根使用者 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。若要在呼叫 API 作業時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，請參閱 IAM 使用者指南中的設定 MFA 保護的 API 存取。

如需 IAM 中最佳實務的相關資訊，請參閱 IAM 使用者指南中的 IAM 安全最佳實務。

使用 GuardDuty 主控台

若要存取 Amazon GuardDuty 主控台，您必須擁有最少一組許可。這些權限必須允許您列出和檢視有關 AWS 帳戶. GuardDuty 如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

您不需要為僅對 AWS CLI 或 AWS API 進行呼叫的使用者允許最低主控台權限。反之，只需允許存取符合他們嘗試執行之 API 操作的動作就可以了。

若要確保使用者和角色仍可使用 GuardDuty 主控台，請同時將 GuardDuty `ConsoleAccess`或受`ReadOnly` AWS 管理的原則附加至實體。如需詳細資訊，請參閱《IAM 使用者指南》中的新增許可到使用者。

啟用 GuardDuty 的必要許可

若要授與各種 IAM 身分 (使用者、群組和角色) 必須具有的許可，請附加要啟用的必要AWS 受管理的策略：AmazonGuardDutyFullAccess政策 GuardDuty。

允許使用者檢視他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視附加到他們使用者身分的內嵌及受管政策。此原則包含在主控台上或以程式設計方式使用 AWS CLI 或 AWS API 完成此動作的權限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
```

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

用於授予唯讀存取權的自訂 IAM 政策 GuardDuty

若要授與唯讀存取權限， GuardDuty 您可以使用受AmazonGuardDutyReadOnlyAccess管理的策略。

若要建立授與 IAM 角色、使用者或群組唯讀存取權的自訂政策 GuardDuty，您可以使用下列陳述式：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:ListMembers",
                "guardduty:GetMembers",
                "guardduty:ListInvitations",
                "guardduty:ListDetectors",
                "guardduty:GetDetector",
                "guardduty:ListFindings",
                "guardduty:GetFindings",
```

```
                "guardduty:ListIPSets",
                "guardduty:GetIPSet",
                "guardduty:ListThreatIntelSets",
                "guardduty:GetThreatIntelSet",
                "guardduty:GetMasterAccount",
                "guardduty:GetInvitationsCount",
                "guardduty:GetFindingsStatistics",
                "guardduty:DescribeMalwareScans",
                "guardduty:UpdateMalwareScanSettings",
                "guardduty:GetMalwareScanSettings"
            ],
            "Resource": "*"
        }
    ]
}
```

拒絕存取 GuardDuty 發現項目

您可以使用下列政策拒絕 IAM 角色、使用者或群組存取 GuardDuty 發現項目。使用者無法檢視發現項目或有關發現項目的詳細資料，但可以存取所有其他 GuardDuty 作業：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:CreateDetector",
                "guardduty:DeleteDetector",
                "guardduty:UpdateDetector",
                "guardduty:GetDetector",
                "guardduty:ListDetectors",
                "guardduty:CreateIPSet",
                "guardduty:DeleteIPSet",
                "guardduty:UpdateIPSet",
                "guardduty:GetIPSet",
                "guardduty:ListIPSets",
                "guardduty:CreateThreatIntelSet",
                "guardduty:DeleteThreatIntelSet",
                "guardduty:UpdateThreatIntelSet",
                "guardduty:GetThreatIntelSet",
                "guardduty:ListThreatIntelSets",
                "guardduty:ArchiveFindings",
```

```
                "guardduty:UnarchiveFindings",
                "guardduty:CreateSampleFindings",
                "guardduty:CreateMembers",
                "guardduty:InviteMembers",
                "guardduty:GetMembers",
                "guardduty:DeleteMembers",
                "guardduty:DisassociateMembers",
                "guardduty:StartMonitoringMembers",
                "guardduty:StopMonitoringMembers",
                "guardduty:ListMembers",
                "guardduty:GetMasterAccount",
                "guardduty:DisassociateFromMasterAccount",
                "guardduty:AcceptAdministratorInvitation",
                "guardduty:ListInvitations",
                "guardduty:GetInvitationsCount",
                "guardduty:DeclineInvitations",
                "guardduty:DeleteInvitations"
            ],
            "Resource": "*"
        },
         {
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "guardduty.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PutRolePolicy",
                "iam:DeleteRolePolicy"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
        }
    ]
```

```
}
```

使用自訂 IAM 政策限制對 GuardDuty 資源的存取

若要 GuardDuty 根據偵測器 ID 定義使用者的存取權限，您可以在自訂 IAM 政策中使用所有 GuardDutyAPI 動作，但下列操作除外：

- `guardduty:CreateDetector`
- `guardduty:DeclineInvitations`
- `guardduty:DeleteInvitations`
- `guardduty:GetInvitationsCount`
- `guardduty:ListDetectors`
- `guardduty:ListInvitations`

使用 IAM 政策中的下列操作， GuardDuty根據 IPSet ID 和 ThreatIntelSet ID 定義使用者的存取權限：

- `guardduty:DeleteIPSet`
- `guardduty:DeleteThreatIntelSet`
- `guardduty:GetIPSet`
- `guardduty:GetThreatIntelSet`
- `guardduty:UpdateIPSet`
- `guardduty:UpdateThreatIntelSet`

以下範例說明如何使用一些上述操作來建立政策：

- 此政策可讓使用者執行 `guardduty:UpdateDetector` 操作，並在 us-east-1 區域中使用偵測器 ID 1234567：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "guardduty:UpdateDetector",
             ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567"
```

```
        }
    ]
}
```

- 此政策可讓使用者執行 guardduty:UpdateIPSet 操作，並在 us-east-1 區域中使用偵測器 ID 1234567 和 IPSet ID 000000：

> **Note**
>
> 請確定使用者具有存取中受信任 IP 清單和安全威脅清單所需的權限 GuardDuty。如需詳細資訊，請參閱 上傳信任 IP 清單和威脅清單所需的許可。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "guardduty:UpdateIPSet",
             ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567/
ipset/000000"
        }
    ]
}
```

- 此政策可讓使用者執行 guardduty:UpdateIPSet 操作，並在 us-east-1 區域中使用任何偵測器 ID 和 IPSet ID 000000：

> **Note**
>
> 請確定使用者具有存取中受信任 IP 清單和安全威脅清單所需的權限 GuardDuty。如需詳細資訊，請參閱 上傳信任 IP 清單和威脅清單所需的許可。

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

```
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:UpdateIPSet",
             ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/*/
ipset/000000"
        }
    ]
}
```

- 此政策可讓使用者執行 guardduty:UpdateIPSet 操作，並在 us-east-1 區域中使用其偵測器 ID 和任何 IPSet ID：

> **Note**
>
> 請確定使用者具有存取中受信任 IP 清單和安全威脅清單所需的權限 GuardDuty。如需詳細資訊，請參閱 上傳信任 IP 清單和威脅清單所需的許可。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:UpdateIPSet",
             ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567/
ipset/*"
        }
    ]
}
```

在 Amazon 使用服務連結角色 GuardDuty

Amazon GuardDuty 使用 AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色 (SLR) 是直接連結到的唯一 IAM 角色類型。 GuardDuty服務連結角色由預先定義， GuardDuty 並包含代表您呼叫其他 AWS 服務所 GuardDuty 需的所有權限。

透過服務連結角色，您可以在不手動新增必要權限的 GuardDuty 情況下進行設定。 GuardDuty 定義其服務連結角色的權限，除非另有定義權限，否則只 GuardDuty 能擔任該角色。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。

GuardDuty 支援在所有可用的區域中使用服務連結角色。 GuardDuty 如需詳細資訊，請參閱 區域與端點。

只有 GuardDuty 在啟用 GuardDuty 服務連結的所有區域中首次停用服務連結角色之後，您才可以刪除該角色。這樣可以保護您的 GuardDuty 資源，因為您無法不小心移除存取資源的權限。

如需有關支援服務連結角色的其他服務的資訊，請參閱《IAM 使用者指南》中的可搭配 IAM 運作的 AWS 服務，並尋找在服務連結角色資料欄中顯示為是的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

服務連結角色權限 GuardDuty

GuardDuty 使用名為的服務連結角色 (SLR)。AWSServiceRoleForAmazonGuardDutySLR 允許執 GuardDuty 行以下任務。它還允許 GuardDuty 將屬於 EC2 實例的檢索到的元數據包含在 GuardDuty 可能產生的有關潛在威脅的發現項目中。AWSServiceRoleForAmazonGuardDuty 服務連結角色信任 guardduty.amazonaws.com 服務來擔任該角色。

權限原則有助於 GuardDuty 執行下列工作：

- 使用 Amazon EC2 動作來管理和擷取 EC2 執行個體、映像和聯網元件 (例如 VPC、子網路和傳輸閘道) 的相關資訊。
- 使用 Amazon EC2 的自動化代理程式啟用執行時 GuardDuty 間監控時，使用動 AWS Systems Manager 作來管理 Amazon EC2 執行個體上的 SSM 關聯。停用 GuardDuty 自動化代理程式組態時，只 GuardDuty 會考慮具有包含標籤 (GuardDutyManaged:true) 的 EC2 執行個體。
- 使用 AWS Organizations 動作來描述相關聯的帳號和組織 ID。
- 使用 Amazon S3 動作擷取有關 S3 儲存貯體和物件的資訊。
- 使用 AWS Lambda 動作擷取有關 Lambda 函數和標籤的資訊。
- 使用 Amazon EKS 動作來管理和擷取有關 EKS 叢集的資訊，以及管理 EKS 叢集上的 Amazon EKS 附加元件。EKS 動作也會擷取與相關聯之標籤的相關資訊。 GuardDuty
- 在啟用惡意軟體防護之後，使用 IAM 建立 惡意軟體防護的服務連結角色許可。
- 使用 Amazon ECS 動作來管理和擷取有關 Amazon ECS 叢集的資訊，以及使用管理 Amazon ECS 帳戶設定。guarddutyActivate與 Amazon ECS 相關的動作也會擷取與相關聯標籤的相 GuardDuty關資訊。

該角色使用名為 AmazonGuardDutyServiceRolePolicy 的下列 AWS 受管政策進行設定。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GuardDutyGetDescribeListPolicy",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeImages",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcPeeringConnections",
                "ec2:DescribeTransitGatewayAttachments",
                "organizations:ListAccounts",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetEncryptionConfiguration",
                "s3:GetBucketTagging",
                "s3:GetAccountPublicAccessBlock",
                "s3:ListAllMyBuckets",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:GetBucketPolicyStatus",
                "lambda:GetFunctionConfiguration",
                "lambda:ListTags",
                "eks:ListClusters",
                "eks:DescribeCluster",
                "ec2:DescribeVpcEndpointServices",
                "ec2:DescribeSecurityGroups",
                "ecs:ListClusters",
                "ecs:DescribeClusters"
            ],
            "Resource": "*"
        },
        {
            "Sid": "GuardDutyCreateSLRPolicy",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
```

```
                    "iam:AWSServiceName": "malware-protection.guardduty.amazonaws.com"
                }
            }
        },
        {
            "Sid": "GuardDutyCreateVpcEndpointPolicy",
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": "arn:aws:ec2:*:*:vpc-endpoint/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                },
                "StringLike": {
                    "ec2:VpceServiceName": [
                        "com.amazonaws.*.guardduty-data",
                        "com.amazonaws.*.guardduty-data-fips"
                    ]
                }
            }
        },
        {
            "Sid": "GuardDutyModifyDeleteVpcEndpointPolicy",
            "Effect": "Allow",
            "Action": [
                "ec2:ModifyVpcEndpoint",
                "ec2:DeleteVpcEndpoints"
            ],
            "Resource": "arn:aws:ec2:*:*:vpc-endpoint/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "GuardDutyCreateModifyVpcEndpointNetworkPolicy",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateVpcEndpoint",
                "ec2:ModifyVpcEndpoint"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:vpc/*",
```

```
                "arn:aws:ec2:*:*:security-group/*",
                "arn:aws:ec2:*:*:subnet/*"
            ]
        },
        {
             "Sid": "GuardDutyCreateTagsDuringVpcEndpointCreationPolicy",
             "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:vpc-endpoint/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateVpcEndpoint"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                }
            }
        },
        {
            "Sid": "GuardDutySecurityGroupManagementPolicy",
            "Effect": "Allow",
            "Action": [
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:DeleteSecurityGroup"
            ],
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "GuardDutyCreateSecurityGroupPolicy",
            "Effect": "Allow",
            "Action": "ec2:CreateSecurityGroup",
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/GuardDutyManaged": "*"
                }
```

```
            }
        },
        {
            "Sid": "GuardDutyCreateSecurityGroupForVpcPolicy",
            "Effect": "Allow",
            "Action": "ec2:CreateSecurityGroup",
            "Resource": "arn:aws:ec2:*:*:vpc/*"
        },
        {
            "Sid": "GuardDutyCreateTagsDuringSecurityGroupCreationPolicy",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateSecurityGroup"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                }
            }
        },
        {
            "Sid": "GuardDutyCreateEksAddonPolicy",
            "Effect": "Allow",
            "Action": "eks:CreateAddon",
            "Resource": "arn:aws:eks:*:*:cluster/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                }
            }
        },
        {
            "Sid": "GuardDutyEksAddonManagementPolicy",
            "Effect": "Allow",
            "Action": [
                "eks:DeleteAddon",
                "eks:UpdateAddon",
                "eks:DescribeAddon"
            ],
            "Resource": "arn:aws:eks:*:*:addon/*/aws-guardduty-agent/*"
        },
        {
```

```
            "Sid": "GuardDutyEksClusterTagResourcePolicy",
            "Effect": "Allow",
            "Action": "eks:TagResource",
            "Resource": "arn:aws:eks:*:*:cluster/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                }
            }
        },
        {
            "Sid": "GuardDutyEcsPutAccountSettingsDefaultPolicy",
            "Effect": "Allow",
            "Action": "ecs:PutAccountSettingDefault",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ecs:account-setting": [
                        "guardDutyActivate"
                    ]
                 }
            }
        },
        {
            "Sid": "SsmCreateDescribeUpdateDeleteStartAssociationPermission",
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeAssociation",
                "ssm:DeleteAssociation",
                "ssm:UpdateAssociation",
                "ssm:CreateAssociation",
                "ssm:StartAssociationsOnce"
            ],
            "Resource": "arn:aws:ssm:*:*:association/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/GuardDutyManaged": "true"
                }
            }
        },
        {
            "Sid": "SsmAddTagsToResourcePermission",
            "Effect": "Allow",
            "Action": [
```

```
                "ssm:AddTagsToResource"
            ],
            "Resource": "arn:aws:arn:aws:ssm:*:*:association/*",
            "Condition":{
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                },
                "StringEquals": {
                    "aws:ResourceTag/GuardDutyManaged": "true"
                }
            }
        },
        {
            "Sid": "SsmCreateUpdateAssociationInstanceDocumentPermission",
            "Effect": "Allow",
            "Action": [
                "ssm:CreateAssociation",
                "ssm:UpdateAssociation"
            ],
            "Resource": "arn:aws:ssm:*:*:document/AmazonGuardDuty-
ConfigureRuntimeMonitoringSsmPlugin"
        },
        {
            "Sid": "SsmSendCommandPermission",
            "Effect": "Allow",
            "Action": "ssm:SendCommand",
            "Resource": [
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ssm:*:*:document/AmazonGuardDuty-
ConfigureRuntimeMonitoringSsmPlugin"
            ]
        },
        {
            "Sid": "SsmGetCommandStatus",
            "Effect": "Allow",
            "Action": "ssm:GetCommandInvocation",
            "Resource": "*"
        }
    ]
}
```

以下是附加到 AWSServiceRoleForAmazonGuardDuty 服務連結角色的信任政策：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

如需有關AmazonGuardDutyServiceRolePolicy策略更新的詳細資訊，請參閱GuardDuty AWS 受管理策略的更新。如需有關此原則變更的自動警示，請訂閱文件歷史紀錄頁面上的 RSS 摘要。

建立服務連結角色 GuardDuty

當您第一次啟 GuardDuty 用AWSServiceRoleForAmazonGuardDuty服務連結角色，或在先前未啟用的支援地 GuardDuty 區啟用時，就會自動建立服務連結角色。您也可以使用 IAM 主控台、或 IAM API 手動建立服務連結角色。 AWS CLI

> **Important**
>
> 針對 GuardDuty 委派系統管理員帳戶建立的服務連結角色不適用於成員 GuardDuty 帳戶。

您必須設定許可，IAM 主體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。若要成功建立AWSServiceRoleForAmazonGuardDuty服務連結角色，您 GuardDuty 搭配使用的 IAM 主體必須具有必要的許可。如需授與必要的許可，請附加以下政策至此 使用者、群組或角色：

> **Note**
>
> 將下列範例中的範例*## ID* 取代為您的實際 AWS 帳戶 ID。

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

```
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "guardduty.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PutRolePolicy",
                "iam:DeleteRolePolicy"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
        }
    ]
}
```

如需有關手動建立角色的詳細資訊，請參閱《IAM 使用者指南》中的建立服務連結角色。

編輯下列項目的服務連結角色 GuardDuty

GuardDuty 不允許您編輯AWSServiceRoleForAmazonGuardDuty服務連結角色。因為可能有各種實體會參考服務連結角色，所以您無法在建立角色之後變更其名稱。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。

刪除下列項目的服務連結角色 GuardDuty

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。

> **Important**
>
> 如果您已啟用惡意軟體防護，刪除 AWSServiceRoleForAmazonGuardDuty 並不會自動刪除 AWSServiceRoleForAmazonGuardDutyMalwareProtection。如果您要刪除 AWSServiceRoleForAmazonGuardDutyMalwareProtection，請參閱 Deleting a service-linked role for Malware Protection。

您必須先 GuardDuty 在啟用此功能的所有區域中停用，才能刪除AWSServiceRoleForAmazonGuardDuty。如果在嘗試刪除 GuardDuty 服務連結角色時未停用服務，則刪除作業會失敗。如需詳細資訊，請參閱 暫停或停用 GuardDuty。

禁用時 GuardDuty，AWSServiceRoleForAmazonGuardDuty不會自動刪除。如果您 GuardDuty 再次啟用，它將開始使用現有的AWSServiceRoleForAmazonGuardDuty.

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台或 IAM API 刪除AWSServiceRoleForAmazonGuardDuty服務連結角色。 AWS CLI如需詳細資訊，請參閱《IAM 使用者指南》中的刪除服務連結角色。

支援 AWS 區域

Amazon GuardDuty 支持在所有可用的地方使用AWSServiceRoleForAmazonGuardDuty服務鏈接 AWS 區域 GuardDuty 的角色。如需目前可用的區域清 Amazon GuardDuty ，請參閱 Amazon Web Services 一般參考. GuardDuty

惡意軟體防護的服務連結角色許可

惡意軟體防護使用名為 AWSServiceRoleForAmazonGuardDutyMalwareProtection 的服務連結角色 (SLR)。此 SLR 可讓惡意程式碼防護執行無代理程式掃描，以偵測帳戶中的惡意程式碼。GuardDuty 它 GuardDuty 允許在您的帳戶中創建 EBS 磁碟區快照，並與 GuardDuty 服務帳戶共享該快照。 GuardDuty 評估快照後，它會在惡意軟體防護發現項目中包含擷取的 EC2 執行個體和容器工作負載中繼資料。AWSServiceRoleForAmazonGuardDutyMalwareProtection 服務連結角色信任 malware-protection.guardduty.amazonaws.com 服務來擔任該角色。

此角色的權限原則可協助惡意程式碼防護執行下列工作：

- 使用 Amazon Elastic Compute Cloud (Amazon EC2) 動作擷取有關 Amazon EC2 執行個體、磁碟區和快照的資訊。惡意軟體防護也提供存取 Amazon EKS 和 Amazon ECS 叢集中繼資料的許可。

- 為 GuardDutyExcluded 標籤未設定為 true 的 EBS 磁碟區建立快照。依預設，快照會以 GuardDutyScanId 標籤建立。請勿移除此標籤，否則惡意軟體防護將無法存取快照。

> **Important**
>
> 當您將設定GuardDutyExcluded為時true， GuardDuty服務將 future 將無法存取這些快照集。這是因為此服務連結角色中的其他陳述式無 GuardDuty 法對GuardDutyExcluded設定為的快照執行任何動作。true

- 僅當 GuardDutyScanId 標籤存在且 GuardDutyExcluded 標籤未設定為 true 時，才允許共用和刪除快照。

> **Note**
>
> 不允許惡意軟體防護將快照公開。

- 存取客戶受管金鑰 (GuardDutyExcluded標籤設定為的金鑰除外)true，CreateGrant以呼叫從與 GuardDuty 服務帳戶共用的加密快照建立和存取加密的 EBS 磁碟區。如需每個區域的 GuardDuty 服務帳戶清單，請參閱GuardDuty 服務帳戶依據 AWS 區域。
- 訪問客戶的 CloudWatch 日誌以創建惡意軟件防護日誌組，並將惡意軟件掃描事件日誌放在日/aws/guardduty/malware-scan-events誌組下。
- 允許客戶決定是否要將快照保留在偵測到惡意軟體的帳戶中。如果掃描檢測到惡意軟件，則服務鏈接角色允許 GuardDuty 向快照添加兩個標籤-GuardDutyFindingDetected和GuardDutyExcluded。

> **Note**
>
> GuardDutyFindingDetected 標記指定快照包含惡意軟體。

- 判斷磁碟區是否使用 EBS 受管金鑰加密。 GuardDuty 執行DescribeKey動作以判斷您帳戶中 EBS 管理的金鑰。key Id
- 擷取使用加密的 EBS 磁碟區的快照 AWS 受管金鑰， AWS 帳戶 然後將其複製到GuardDuty 服務帳戶. 為此，我們使用權限GetSnapshotBlock和ListSnapshotBlocks. GuardDuty 然後將掃描服務帳戶中的快照。目前，掃描使用加密的 EBS 卷的惡意軟件防護支持 AWS 受管金鑰 可能不適用於所有. AWS 區域如需詳細資訊，請參閱 區域特定功能的可用性。

- 允許 Amazon EC2 代表惡意軟體防護呼叫，以 AWS KMS 對客戶受管金鑰執行多個加密動作。共用使用客戶自管金鑰加密的快照時，需要執行 kms:ReEncryptTo 和 kms:ReEncryptFrom 等動作。僅可存取 GuardDutyExcluded 標籤未設定為 true 的金鑰。

該角色使用名為 AmazonGuardDutyMalwareProtectionServiceRolePolicy 的下列 AWS 受管政策進行設定。

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "DescribeAndListPermissions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeVolumes",
                "ec2:DescribeSnapshots",
                "ecs:ListClusters",
                "ecs:ListContainerInstances",
                "ecs:ListTasks",
                "ecs:DescribeTasks",
                "eks:DescribeCluster"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateSnapshotVolumeConditionalStatement",
            "Effect": "Allow",
            "Action": "ec2:CreateSnapshot",
            "Resource": "arn:aws:ec2:*:*:volume/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/GuardDutyExcluded": "true"
                }
            }
        },
        {
            "Sid": "CreateSnapshotConditionalStatement",
            "Effect": "Allow",
            "Action": "ec2:CreateSnapshot",
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
```

```
                    "aws:TagKeys": "GuardDutyScanId"
                }
            }
        },
        {
            "Sid": "CreateTagsPermission",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:*/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateSnapshot"
                }
            }
        },
        {
            "Sid": "AddTagsToSnapshotPermission",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/GuardDutyScanId": "*"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyExcluded",
                        "GuardDutyFindingDetected"
                    ]
                }
            }
        },
        {
            "Sid": "DeleteAndShareSnapshotPermission",
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteSnapshot",
                "ec2:ModifySnapshotAttribute"
            ],
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/GuardDutyScanId": "*"
                },
```

```
                "Null": {
                    "aws:ResourceTag/GuardDutyExcluded": "true"
                }
            }
        },
        {
            "Sid": "PreventPublicAccessToSnapshotPermission",
            "Effect": "Deny",
            "Action": [
                "ec2:ModifySnapshotAttribute"
            ],
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "StringEquals": {
                    "ec2:Add/group": "all"
                }
            }
        },
        {
            "Sid": "CreateGrantPermission",
            "Effect": "Allow",
            "Action": "kms:CreateGrant",
            "Resource": "arn:aws:kms:*:*:key/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/GuardDutyExcluded": "true"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:ebs:id": "snap-*"
                },
                "ForAllValues:StringEquals": {
                    "kms:GrantOperations": [
                        "Decrypt",
                        "CreateGrant",
                        "GenerateDataKeyWithoutPlaintext",
                        "ReEncryptFrom",
                        "ReEncryptTo",
                        "RetireGrant",
                        "DescribeKey"
                    ]
                },
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                }
```

```
            }
        },
        {
            "Sid": "ShareSnapshotKMSPermission",
            "Effect": "Allow",
            "Action": [
                "kms:ReEncryptTo",
                "kms:ReEncryptFrom"
            ],
            "Resource": "arn:aws:kms:*:*:key/*",
            "Condition": {
                "StringLike": {
                    "kms:ViaService": "ec2.*.amazonaws.com"
                },
                "Null": {
                    "aws:ResourceTag/GuardDutyExcluded": "true"
                }
            }
        },
        {
            "Sid": "DescribeKeyPermission",
            "Effect": "Allow",
            "Action": "kms:DescribeKey",
            "Resource": "arn:aws:kms:*:*:key/*"
        },
        {
            "Sid": "GuardDutyLogGroupPermission",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups",
                "logs:CreateLogGroup",
                "logs:PutRetentionPolicy"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/guardduty/*"
        },
        {
            "Sid": "GuardDutyLogStreamPermission",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:DescribeLogStreams"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/guardduty/*:log-stream:*"
```

```
        },
        {
            "Sid": "EBSDirectAPIPermissions",
            "Effect": "Allow",
            "Action": [
                "ebs:GetSnapshotBlock",
                "ebs:ListSnapshotBlocks"
            ],
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/GuardDutyScanId": "*"
                },
                "Null": {
                    "aws:ResourceTag/GuardDutyExcluded": "true"
                }
            }
        }
    ]
}
```

以下是連接至 AWSServiceRoleForAmazonGuardDutyMalwareProtection 服務連結角色的信任政策：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "malware-protection.guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

為惡意軟體防護建立服務連結角色

當您第一次啟用惡意軟體防護，或在先前未啟用惡意軟體防護的支援區域中啟用時，AWSServiceRoleForAmazonGuardDutyMalwareProtection 服務連

結角色會自動建立。您也可以使用 IAM 主控台、IAM CLI 或 IAM API 來手動建立 `AWSServiceRoleForAmazonGuardDutyMalwareProtection` 服務連結角色。

> **Note**
>
> 預設情況下，如果您是 Amazon 的新手 GuardDuty，則會自動啟用惡意軟體防護。

> **Important**
>
> 針對委派 GuardDuty 系統管理員帳戶建立的服務連結角色不適用於成員 GuardDuty 帳戶。

您必須設定許可，IAM 主體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。若要成功建立`AWSServiceRoleForAmazonGuardDutyMalwareProtection`服務連結角色， GuardDuty 搭配使用的 IAM 身分必須具有必要的許可。如需授與必要的許可，請附加以下政策至此 使用者、群組或角色：

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": "guardduty:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": [
                        "malware-protection.guardduty.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
```

```
                "organizations:RegisterDelegatedAdministrator",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:GetRole",
            "Resource": "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
        }
    ]
}
```

如需有關手動建立角色的詳細資訊，請參閱《IAM 使用者指南》中的建立服務連結角色。

為惡意軟體防護編輯服務連結角色

惡意軟體防護不允許您編輯 AWSServiceRoleForAmazonGuardDutyMalwareProtection 服務連結角色。因為可能有各種實體會參考服務連結角色，所以您無法在建立角色之後變更其名稱。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。

為惡意軟體防護刪除服務連結角色

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。

> **Important**
>
> 您必須先在已啟用惡意軟體防護的所有區域中將其停用，才能刪除 AWSServiceRoleForAmazonGuardDutyMalwareProtection。
> 如果未停用惡意軟體防護，當您嘗試刪除服務連結角色時，刪除就會失敗。如需詳細資訊，請參閱 啟用或停用起始的惡意程式碼 GuardDuty掃描。

當您選擇停用以停止惡意軟體防護服務時，AWSServiceRoleForAmazonGuardDutyMalwareProtection 不會自動刪除。

如果您接著選擇 [啟用] 再次啟動 [惡意程式碼防護] 服務， GuardDuty 將會開始使用現有的`AWSServiceRoleForAmazonGuardDutyMalwareProtection`。

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台、 AWS CLI 或 IAM API 刪除`AWSServiceRoleForAmazonGuardDutyMalwareProtection`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。

支援 AWS 區域

Amazon GuardDuty 支援在所有可用惡意軟體防護的 AWS 區域 地方使用`AWSServiceRoleForAmazonGuardDutyMalwareProtection`服務連結角色。

如需目前可用的區域清 Amazon GuardDuty ，請參閱 Amazon Web Services 一般參考. GuardDuty

> **Note**
>
> 目前 AWS GovCloud (美國東部) 和 AWS GovCloud (美國西部) 無法使用惡意程式碼防護。

AWS Amazon 的受管政策 GuardDuty

若要新增使用者、群組和角色的權限，使用 AWS 受管理的原則比自己撰寫原則更容易。建立 IAM 客戶受管政策需要時間和專業知識，而受管政策可為您的團隊提供其所需的許可。若要快速開始使用，您可以使用我們的 AWS 受管政策。這些政策涵蓋常見的使用案例，並可在您的 AWS 帳戶中使用。如需 AWS 受管政策的詳細資訊，請參閱 IAM 使用者指南中的AWS 受管政策。

AWS 服務會維護和更新 AWS 受管理的策略。您無法變更 AWS 受管理原則中的權限。服務有時會將其他權限新增至受 AWS 管理的策略，以支援新功能。此類型的更新會影響已連接政策的所有身分識別 (使用者、群組和角色)。當新功能啟動或新作業可用時，服務最有可能更新 AWS 受管理的策略。服務不會從 AWS 受管理的政策移除權限，因此政策更新不會破壞您現有的權限。

此外，還 AWS 支援跨多個服務之工作職能的受管理原則。例如，ReadOnlyAccess AWS 受管理的策略提供對所有 AWS 服務和資源的唯讀存取權。當服務啟動新功能時，會為新作業和資源新 AWS 增唯讀權限。如需任務職能政策的清單和說明，請參閱 IAM 使用者指南中有關任務職能的AWS 受管政策。

AWS 受管理的策略：AmazonGuardDutyFullAccess

您可將 `AmazonGuardDutyFullAccess` 政策連接到 IAM 身分。

此原則會授與允許使用者完整存取所有 GuardDuty 動作的管理權限。

許可詳細資訊

此政策包含以下許可。

- `GuardDuty`— 允許使用者完全存取所有 GuardDuty動作。
- `IAM`— 允許使用者建立 GuardDuty 服務連結角色。這可讓 GuardDuty 系統管理員啟 GuardDuty 用成員帳戶。
- `Organizations`— 可讓使用者指定委派的管理員並管理 GuardDuty 組織的成員。

如果帳戶中存在用於惡意軟體防護的服務連結角色 (SLR)，則會建立對 `AWSServiceRoleForAmazonGuardDutyMalwareProtection` 執行 `iam:GetRole` 動作的許可。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonGuardDutyFullAccessSid1",
            "Effect": "Allow",
            "Action": "guardduty:*",
            "Resource": "*"
        },
        {
            "Sid": "CreateServiceLinkedRoleSid1",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": [
                        "guardduty.amazonaws.com",
                        "malware-protection.guardduty.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "ActionsForOrganizationsSid1",
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
```

```
                "organizations:RegisterDelegatedAdministrator",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IamGetRoleSid1",
            "Effect": "Allow",
            "Action": "iam:GetRole",
            "Resource": "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
        }
    ]
}
```

AWS 受管理的策略：AmazonGuardDutyReadOnlyAccess

您可將 AmazonGuardDutyReadOnlyAccess 政策連接到 IAM 身分。

此原則會授與唯讀權限，讓使用者可以檢視 GuardDuty 組織的 GuardDuty 發現項目和詳細資料。

許可詳細資訊

此政策包含以下許可。

- GuardDuty— 可讓使用者檢視 GuardDuty 發現項目，並執行以GetList、或開頭的 API 作業Describe。
- Organizations— 可讓使用者擷取 GuardDuty 組織組態的相關資訊，包括委派管理員帳戶的詳細資訊。

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

```
            "Action": [
                "guardduty:Describe*",
                "guardduty:Get*",
                "guardduty:List*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 受管理的策略：AmazonGuardDutyServiceRolePolicy

您不得將 AmazonGuardDutyServiceRolePolicy 連接到 IAM 實體。此 AWS 受管理策略會附加至服務連結角色，可 GuardDuty 代表您執行動作。如需詳細資訊，請參閱 服務連結角色權限 GuardDuty。

GuardDuty AWS 受管理策略的更新

檢視 GuardDuty 自此服務開始追蹤這些變更以來的 AWS 受管理策略更新詳細資料。如需有關此頁面變更的自動警示，請訂閱「 GuardDuty 文件歷史記錄」頁面上的 RSS 摘要。

變更	描述	日期
AmazonGuardDutyServiceRolePolicy – 更新現有政策。	使用 Amazon EC2 的自動化代理程式啟用執行時 GuardDuty 間監控時，使用動 AWS Systems Manager 作來管理 Amazon EC2 執行	2024年3月26日

變更	描述	日期
	個體上的 SSM 關聯。停用 GuardDuty 自動化代理程式組態時，只 GuardDuty 會考慮具有包含標籤 (GuardDuty Managed :true) 的 EC2 執行個體。	
AmazonGuardDutyServiceRolePolicy – 更新現有政策。	GuardDuty 已新增許可-擷organization:DescribeOrganization 取共用 Amazon VPC 帳戶的組織 ID，並使用組織 ID 設定 Amazon VPC 端點政策。	2024年2月9 日
AmazonGuardDutyMalwareProtectionServiceRolePolicy – 更新現有政策。	惡意軟體防護新增了兩個權限-GetSnapshotBlock 並ListSnapshotBlocks 從您的 EBS 磁碟區擷取快照 (使用加密 AWS 受管金鑰)，AWS 帳戶 並將其複製到 GuardDuty 服務帳戶，然後再開始惡意軟體掃描。	2024年1月25日
AmazonGuardDutyServiceRolePolicy – 更新現有政策	新增許可以新增 guardduty Activate Amazon ECS 帳戶設定，GuardDuty 以及在 Amazon ECS 叢集上執行清單和描述操作。	2023年11月26日
AmazonGuardDutyReadOnlyAccess – 更新現有政策	GuardDuty 已將新政策新增organizations 至ListAccounts 。	2023 年 11 月 16 日
AmazonGuardDutyFullAccess – 更新現有政策	GuardDuty 已將新政策新增organizations 至ListAccounts 。	2023 年 11 月 16 日

變更	描述	日期
AmazonGuardDutyServiceRolePolicy – 更新現有政策	GuardDuty 添加了新的權限，以支持即將推出的 GuardDuty EKS 運行時監視功能。	2023 年 3 月 8 日
AmazonGuardDutyServiceRolePolicy – 更新現有政策	GuardDuty 已新增新權限，以允許 GuardDuty 針對惡意程式碼防護建立服務連結角色。這將有助於 GuardDuty簡化啟用惡意軟件防護的過程。 GuardDuty 現在可以執行下列 IAM 動作： `{ "Effect": "Allow", "Action": "iam:CreateServiceLinkedRole", "Resource": "*", "Condition": { "StringEquals": { "iam:AWSServiceName": "malware-protection.guardduty.amazonaws.com" } } }`	2023 年 2 月 21 日
AmazonGuardDutyFullAccess – 更新現有政策	GuardDuty 將 ARN 更新`iam:GetRole` 為。`*AWSServiceRoleForAmazonGuardDutyMalwareProtection`	2022 年 7 月 26 日

變更	描述	日期
AmazonGuardDutyFullAccess – 更新現有政策	GuardDuty 已新增新功能，AWSServiceName 以允許使iam:CreateServiceLinkedRole 用「GuardDuty 惡意程式碼防護」服務建立服務連結角色。 GuardDuty 現在可以執行iam:GetRole 動作以取得資訊AWSServiceRole 。	2022 年 7 月 26 日
AmazonGuardDutyServiceRolePolicy – 更新現有政策	GuardDuty 增加了新的許可，以 GuardDuty 允許使用 Amazon EC2 聯網操作來改善發現結果。 GuardDuty 現在可以執行下列 EC2 動作，以取得 EC2 執行個體如何通訊的相關資訊。此資訊用於提高調查結果準確度。 • ec2:DescribeVpcEndpoints • ec2:DescribeSubnets • ec2:DescribeVpcPeeringConnections • ec2:DescribeTransitGatewayAttachments	2021 年 8 月 3 日
GuardDuty 開始追蹤變更	GuardDuty 開始追蹤其 AWS 受管理策略的變更。	2021 年 8 月 3 日

疑難排解 Amazon GuardDuty 身分和存取

使用下列資訊可協助您診斷和修正使用和 IAM 時可能會遇到的 GuardDuty 常見問題。

主題

我沒有執行操作的授權 GuardDuty

如果您收到錯誤，告知您未獲授權執行動作，您的政策必須更新，允許您執行動作。

下列範例錯誤會在mateojackson IAM 使用者嘗試使用主控台檢視一個虛構 *my-example-widget* 資源的詳細資訊，但卻無虛構 guardduty:*GetWidget* 許可時發生。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 guardduty:GetWidget on resource: my-example-widget
```

在此情況下，必須更新 mateojackson 使用者的政策，允許使用 guardduty:*GetWidget* 動作存取 *my-example-widget* 資源。

如果您需要協助，請聯絡您的 AWS 系統管理員。您的管理員提供您的簽署憑證。

我沒有授權執行 iam: PassRole。

如果您收到未獲授權執行iam:PassRole動作的錯誤訊息，則必須更新您的原則以允許您將角色傳遞給 GuardDuty。

有些 AWS 服務 允許您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

當名為的 IAM 使用者marymajor嘗試使用主控台執行中的動作時，會發生下列範例錯誤 GuardDuty。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞至該服務的許可。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在這種情況下，Mary 的政策必須更新，允許她執行 `iam:PassRole` 動作。

如果您需要協助，請聯絡您的 AWS 系統管理員。您的管理員提供您的簽署憑證。

我想允許我以外的人訪 AWS 帳戶 問我的 GuardDuty 資源。

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要瞭解是否 GuardDuty 支援這些功能，請參閱Amazon 如何與 IAM 合 GuardDuty 作。
- 若要了解如何提供對您所擁有資源 AWS 帳戶 的存取權，請參閱《IAM 使用者指南》中您擁有的另一 AWS 帳戶 個 IAM 使用者提供存取權限。
- 若要了解如何向第三方提供對資源的存取權 AWS 帳戶，請參閱 IAM 使用者指南中的提供第三方 AWS 帳戶 擁有的存取權。
- 若要了解如何透過聯合身分提供存取權，請參閱 IAM 使用者指南中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。
- 若要了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 角色與資源型政策的差異。

Amazon 的合規驗證 GuardDuty

若要瞭解 AWS 服務 是否屬於特定規範遵循方案的範圍內，請參閱AWS 服務 遵循規範計劃方案中的，並選擇您感興趣的合規方案。如需一般資訊，請參閱AWS 規範計劃AWS。

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

您在使用時的合規責任取決 AWS 服務 於您資料的敏感性、公司的合規目標以及適用的法律和法規。AWS 提供下列資源以協助遵循法規：

- 安全性與合規性快速入門指南 — 這些部署指南討論架構考量，並提供部署以安全性和合規性 AWS 為重點的基準環境的步驟。
- 在 Amazon Web Services 上架構 HIPAA 安全性與合規性 — 本白皮書說明公司如何使用建立符合 HIPAA 資格的應 AWS 用程式。

> **Note**
>
> 並非所有人 AWS 服務 都符合 HIPAA 資格。如需詳細資訊，請參閱 HIPAA 資格服務參照。

- AWS 合規資源AWS — 此工作簿和指南集合可能適用於您的產業和所在地。
- AWS 客戶合規指南 — 透過合規的角度瞭解共同的責任模式。這份指南總結了在多個架構 (包括美國國家標準技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO)) 中，保 AWS 服務 護指引並對應至安全控制的最佳實務。
- 使用AWS Config 開發人員指南中的規則評估資源 — 此 AWS Config 服務會評估您的資源組態符合內部實務、產業準則和法規的程度。
- AWS Security Hub— 這 AWS 服務 提供了內部安全狀態的全面視圖 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 Security Hub controls reference。
- Amazon GuardDuty — 透過監控環境中的 AWS 帳戶可疑和惡意活動，藉此 AWS 服務 偵測您的工作負載、容器和資料的潛在威脅。 GuardDuty 可協助您滿足特定合規性架構所要求的入侵偵測需求，例如 PCI DSS 等各種合規性需求。
- AWS Audit Manager— 這 AWS 服務 有助於您持續稽核您的 AWS 使用情況，以簡化您管理風險的方式，以及遵守法規和業界標準的方式。

Amazon GuardDuty 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。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網路連線相互連結。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 AWS 區域與可用區域的詳細資訊，請參閱 AWS 全球基礎設施。

Amazon GuardDuty 中的基礎設施安全

Amazon GuardDuty 是一項受管服務，受到 AWS 全球網路安全的防護。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 發布的 API 呼叫，透過網路存取 GuardDuty。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。

AWS 與 GuardDuty 的服務整合

GuardDuty 可與其他 AWS 安全服務整合。這些服務可以從 GuardDuty 擷取資料，讓您以新方式檢視調查結果。檢閱以下整合選項，進一步了解如何設定服務，以搭配 GuardDuty 使用。

將 GuardDuty 與 AWS Security Hub 整合

AWS Security Hub 從各個 AWS 帳戶、服務和支援的第三方合作夥伴產品收集安全資料，以根據業界標準和最佳實務評估您環境的安全狀態。除了評估您的安全狀態之外，Security Hub 還會為所有 AWS 整合服務和 AWS 合作夥伴產品的調查結果建立一個集中位置。使用 GuardDuty 啟用 Security Hub 將自動允許 Security Hub 擷取 GuardDuty 調查結果資料。

如需有關將 Security Hub 與 GuardDuty 搭配使用的詳細資訊，請參閱與整合 AWS Security Hub。

將 GuardDuty 與 Amazon Detective 整合

Amazon Detective 會使用來自各個 AWS 帳戶的日誌資料，為與您環境互動的資源和 IP 地址建立資料視覺化效果。Detective 的視覺化效果可協助您快速輕鬆地調查安全問題。啟用這兩項服務後，您可以將 GuardDuty 的調查結果詳細資訊轉換為 Detective 主控台中的資訊。

如需有關將 Detective 與 GuardDuty 搭配使用的詳細資訊，請參閱與 Amazon Detective 整合。

與整合 AWS Security Hub

AWS Security Hub 可讓您全方位地檢視 AWS 中的安全狀態，並可協助您檢查環境是否符合安全業界標準和最佳實務。Security Hub 會從各個 AWS 帳戶、服務和支援的協力廠商合作夥伴產品收集安全性資料，並協助您分析安全性趨勢並找出最優先順序的安全性問題。

Amazon 與 Security Hub 的 GuardDuty 整合可讓您將發現項目從安全中心傳送 GuardDuty 到 Security Hub。Security Hub 接著可將這些問題清單納入其安全狀態的分析中。

內容

Amazon 如何 GuardDuty 將結果發送到 AWS Security Hub

在中 AWS Security Hub，安全性問題會追蹤為發現項目。某些發現項目來自其他 AWS 服務或協力廠商合作夥伴偵測到的問題。Security Hub 也有一組規則，用來偵測安全問題並產生問題清單。

Security Hub 提供用來跨所有這些來源管理問題清單的工具。您可以檢視並篩選問題清單列表，並檢視問題清單的詳細資訊。如需詳細資訊，請參閱《AWS Security Hub 使用者指南》中的檢視問題清單。您也可以追蹤問題清單的調查狀態。如需詳細資訊，請參閱《AWS Security Hub 使用者指南》中的針對問題清單採取動作。

安全性中樞中的所有發現項目都使用稱為 AWS 安全性尋找格式 (ASFF) 的標準 JSON 格式。ASFF 包含問題來源、受影響的資源以及問題清單目前狀態的詳細資訊。請參閱 AWS Security Hub 使用者指南中的 AWS 安全問題清單格式 (ASFF)。

Amazon GuardDuty 是將調查結果發送到 Security Hub 的 AWS 服務之一。

GuardDuty 傳送至 Security Hub 的發現項目類型

一旦您在同一個帳戶中啟用 GuardDuty 和安全中心 AWS 區域， GuardDuty開始將所有生成的發現項目發送到 Security Hub。這些發現項目會使用安全性尋找格式 (ASFF) 傳送至AWS 安全性中樞。在 ASFF 中，Types 欄位提供問題清單類型。

傳送新發現項目的延遲

GuardDuty 建立新的發現項目時，通常會在五分鐘內傳送至 Security Hub。

無法使用 Security Hub 時重試

如果 Security Hub 無法使用，請 GuardDuty 重試傳送發現項目，直到收到它們為止。

更新 Security Hub 中的現有問題清單

將發現項目傳送至 Security Hub 之後， GuardDuty 會傳送更新，以反映對尋找活動的其他觀察結果至 Security Hub。這些發現項目的新觀察會根據您 AWS 帳戶中的步驟 5 — 匯出更新頻率設定傳送至安全中心。

當您封存或取消封存發現項目時， GuardDuty 不會將該發現項目傳送至 Security Hub。任何稍後變為作用中的手動取消封存發現項目， GuardDuty 都不會傳送至 Security Hub。

檢視 GuardDuty 發現項目於 AWS Security Hub

若要在 Security Hub 中檢視您的 GuardDuty 發現項目，請 GuardDuty從摘要頁面選取 Amazon 下的查看發現項目。或者，您可以從導覽面板中選取「發現項目」，然後選取值為的「產品名稱:」欄位來篩選 GuardDuty 發現項目，以僅顯示發現項目GuardDuty。

解譯 GuardDuty 尋找名稱 AWS Security Hub

GuardDuty 使用安全性搜尋結果格式 (ASFF)，將發現項目傳送至AWS 安全性中樞。在 ASFF 中，Types 欄位提供問題清單類型。ASFF 類型使用的命名配置與 GuardDuty類型不同。下表詳細說明所有 GuardDuty 發現項目類型及其 ASFF 對應項目，如同它們出現在 Security Hub 中。

> **Note**
>
> 針對某些 GuardDuty 發現項目類型，Security Hub 會根據發現項目詳細資料的資源角色是 ACTOR 還是 TARGET，指派不同的 ASFF 尋找項目 如需更多資訊，請參閱調查結果詳細資訊。

GuardDuty 尋找類型	ASFF 問題清單類型
Backdoor:EC2/C&CActivity.B	TTPs/Command and Control/Backdoor:EC2-C&CActivity.B
Backdoor:EC2/C&CActivity.B!DNS	TTPs/Command and Control/Backdoor:EC2-C&CActivity.B!DNS
Backdoor:EC2/DenialOfService.Dns	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Dns

GuardDuty 尋找類型	ASFF 問題清單類型
Backdoor:EC2/DenialOfService.Tcp	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Tcp
Backdoor:EC2/DenialOfService.Udp	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Udp
Backdoor:EC2/DenialOfService.UdpOnTcpPorts	TTPs/Command and Control/Backdoor:EC2-DenialOfService.UdpOnTcpPorts
Backdoor:EC2/DenialOfService.UnusualProtocol	TTPs/Command and Control/Backdoor:EC2-DenialOfService.UnusualProtocol
Backdoor:EC2/Spambot	TTPs/Command and Control/Backdoor:EC2-Spambot
Behavior:EC2/NetworkPortUnusual	Unusual Behaviors/VM/Behavior:EC2-NetworkPortUnusual
Behavior:EC2/TrafficVolumeUnusual	Unusual Behaviors/VM/Behavior:EC2-TrafficVolumeUnusual
Backdoor:Lambda/C&CActivity.B	TTPs/Command and Control/Backdoor:Lambda-C&CActivity.B
Backdoor:Runtime/C&CActivity.B	TTPs/Command and Control/Backdoor:Runtime-C&CActivity.B
Backdoor:Runtime/C&CActivity.B!DNS	TTPs/Command and Control/Backdoor:Runtime-C&CActivity.B!DNS
CredentialAccess:IAMUser/AnomalousBehavior	TTPs/Credential Access/IAMUser-AnomalousBehavior
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed	TTPs/AnomalousBehavior/CredentialAccess:Kubernetes-SecretsAccessed
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	TTPs/Credential Access/CredentialAccess:RDS-AnomalousBehavior.FailedLogin

GuardDuty 尋找類型	ASFF 問題清單類型
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	TTPs/Credential Access/RDS-AnomalousBehavior.SuccessfulBruteForce
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	TTPs/Credential Access/RDS-AnomalousBehavior.SuccessfulLogin
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	TTPs/Credential Access/RDS-MaliciousIPCaller.FailedLogin
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	TTPs/Credential Access/RDS-MaliciousIPCaller.SuccessfulLogin
CredentialAccess:RDS/TorIPCaller.FailedLogin	TTPs/Credential Access/RDS-TorIPCaller.FailedLogin
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	TTPs/Credential Access/RDS-TorIPCaller.SuccessfulLogin
CryptoCurrency:EC2/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B
CryptoCurrency:EC2/BitcoinTool.B!DNS	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B!DNS
CryptoCurrency:Lambda/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:Lambda-BitcoinTool.B Effects/Resource Consumption/CryptoCurrency:Lambda-BitcoinTool.B
CryptoCurrency:Runtime/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:Runtime-BitcoinTool.B
CryptoCurrency:Runtime/BitcoinTool.B!DNS	TTPs/Command and Control/CryptoCurrency:Runtime-BitcoinTool.B!DNS
DefenseEvasion:EC2/UnusualDNSResolver	TTPs/DefenseEvasion/EC2:Unusual-DNS-Resolver

GuardDuty 尋找類型	ASFF 問題清單類型
DefenseEvasion:EC2/UnusualDoHActivity	TTPs/DefenseEvasion/EC2:Unusual-DoH-Activity
DefenseEvasion:EC2/UnusualDoTActivity	TTPs/DefenseEvasion/EC2:Unusual-DoT-Activity
DefenseEvasion：用戶/AnomalousBehavior	TTPs/Defense Evasion/IAMUser-AnomalousBehavior
DefenseEvasion:Runtime/FilelessExecution	TTPs/Defense Evasion/DefenseEvasion:Runtime-FilelessExecution
DefenseEvasion:Runtime/PtraceAntiDebugging	TTPs/DefenseEvasion/DefenseEvasion:Runtime-PtraceAntiDebugging
DefenseEvasion:Runtime/SuspiciousCommand	TTPs/DefenseEvasion/DefenseEvasion:Runtime-SuspiciousCommand
發現:在線使用者/AnomalousBehavior	TTPs/Discovery/IAMUser-AnomalousBehavior
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	TTPs/AnomalousBehavior/Discovery:Kubernetes-PermissionChecked
Discovery:RDS/MaliciousIPCaller	TTPs/Discovery/RDS-MaliciousIPCaller
Discovery:RDS/TorIPCaller	TTPs/Discovery/RDS-TorIPCaller
Discovery:S3/AnomalousBehavior	TTPs/Discovery:S3-AnomalousBehavior
Discovery:S3/BucketEnumeration.Unusual	TTPs/Discovery:S3-BucketEnumeration.Unusual
Discovery:S3/MaliciousIPCaller.Custom	TTPs/Discovery:S3-MaliciousIPCaller.Custom
Discovery:S3/TorIPCaller	TTPs/Discovery:S3-TorIPCaller
Discovery:S3/MaliciousIPCaller	TTPs/Discovery:S3-MaliciousIPCaller

GuardDuty 尋找類型	ASFF 問題清單類型
Execution:Kubernetes/AnomalousBehavior.ExecInPod	TTPs/AnomalousBehavior/Execution:Kubernetes-ExecInPod
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	TTPs/AnomalousBehavior/Execution:Kubernetes-WorkloadDeployed
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount	TTPs/AnomalousBehavior/Persistence:Kubernetes-WorkloadDeployed!ContainerWithSensitiveMount
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer	TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-WorkloadDeployed!PrivilegedContainer
Execution:EC2/MaliciousFile	TTPs/Execution/Execution:EC2-MaliciousFile
Execution:ECS/MaliciousFile	TTPs/Execution/Execution:ECS-MaliciousFile
Execution:Kubernetes/MaliciousFile	TTPs/Execution/Execution:Kubernetes-MaliciousFile
Execution:Container/MaliciousFile	TTPs/Execution/Execution:Container-MaliciousFile
Execution:EC2/SuspiciousFile	TTPs/Execution/Execution:EC2-SuspiciousFile
Execution:ECS/SuspiciousFile	TTPs/Execution/Execution:ECS-SuspiciousFile
Execution:Kubernetes/SuspiciousFile	TTPs/Execution/Execution:Kubernetes-SuspiciousFile
Execution:Container/SuspiciousFile	TTPs/Execution/Execution:Container-SuspiciousFile
Execution:Runtime/MaliciousFileExecuted	TTPs/Execution/Execution:Runtime-MaliciousFileExecuted

GuardDuty 尋找類型	ASFF 問題清單類型
Execution:Runtime/NewBinaryExecuted	TTPs/Execution/Execution:Runtime-NewBinaryExecuted
Execution:Runtime/NewLibraryLoaded	TTPs/Execution/Execution:Runtime-NewLibraryLoaded
Execution:Runtime/ReverseShell	TTPs/Execution/Execution:Runtime-ReverseShell
Execution:Runtime/SuspiciousCommand	TTPs/Execution/Execution:Runtime-SuspiciousCommand
Execution:Runtime/SuspiciousTool	TTPs/Execution/Execution:Runtime-SuspiciousTool
Exfiltration:S3/AnomalousBehavior	TTPs/Exfiltration:S3-AnomalousBehavior
Exfiltration:S3/ObjectRead.Unusual	TTPs/Exfiltration:S3-ObjectRead.Unusual
Exfiltration:S3/MaliciousIPCaller	TTPs/Exfiltration:S3-MaliciousIPCaller
Impact:EC2/AbusedDomainRequest.Reputation	TTPs/Impact:EC2-AbusedDomainRequest.Reputation
Impact:EC2/BitcoinDomainRequest.Reputation	TTPs/Impact:EC2-BitcoinDomainRequest.Reputation
Impact:EC2/MaliciousDomainRequest.Reputation	TTPs/Impact:EC2-MaliciousDomainRequest.Reputation
Impact:EC2/PortSweep	TTPs/Impact/Impact:EC2-PortSweep
Impact:EC2/SuspiciousDomainRequest.Reputation	TTPs/Impact:EC2-SuspiciousDomainRequest.Reputation
Impact:EC2/WinRMBruteForce	TTPs/Impact/Impact:EC2-WinRMBruteForce
影響：用戶/AnomalousBehavior	TTPs/Impact/IAMUser-AnomalousBehavior

GuardDuty 尋找類型	ASFF 問題清單類型
Impact:Runtime/AbusedDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-AbusedDomainRequest.Reputation
Impact:Runtime/BitcoinDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-BitcoinDomainRequest.Reputation
Impact:Runtime/CryptoMinerExecuted	TTPs/Impact/Impact:Runtime-CryptoMinerExecuted
Impact:Runtime/MaliciousDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation
Impact:Runtime/SuspiciousDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-SuspiciousDomainRequest.Reputatio
Impact:S3/AnomalousBehavior.Delete	TTPs/Impact:S3-AnomalousBehavior.Delete
Impact:S3/AnomalousBehavior.Permission	TTPs/Impact:S3-AnomalousBehavior.Permission
Impact:S3/AnomalousBehavior.Write	TTPs/Impact:S3-AnomalousBehavior.Write
Impact:S3/ObjectDelete.Unusual	TTPs/Impact:S3-ObjectDelete.Unusual
Impact:S3/PermissionsModification.Unusual	TTPs/Impact:S3-PermissionsModification.Unusual
Impact:S3/MaliciousIPCaller	TTPs/Impact:S3-MaliciousIPCaller
InitialAccess：用戶/AnomalousBehavior	TTPs/Initial Access/IAMUser-AnomalousBehavior
PenTest:IAMUser/KaliLinux	TTPs/PenTest:IAMUser/KaliLinux
PenTest:IAMUser/ParrotLinux	TTPs/PenTest:IAMUser/ParrotLinux
PenTest:IAMUser/PentooLinux	TTPs/PenTest:IAMUser/PentooLinux
PenTest:S3/KaliLinux	TTPs/PenTest:S3-KaliLinux

GuardDuty 尋找類型	ASFF 問題清單類型
PenTest:S3/ParrotLinux	TTPs/PenTest:S3-ParrotLinux
PenTest:S3/PentooLinux	TTPs/PenTest:S3-PentooLinux
持久性：用戶/AnomalousBehavior	TTPs/Persistence/IAMUser-AnomalousBehavior
Persistence:IAMUser/NetworkPermissions	TTPs/Persistence/Persistence:IAMUser-NetworkPermissions
Persistence:IAMUser/ResourcePermissions	TTPs/Persistence/Persistence:IAMUser-ResourcePermissions
Persistence:IAMUser/UserPermissions	TTPs/Persistence/Persistence:IAMUser-UserPermissions
Policy:IAMUser/RootCredentialUsage	TTPs/Policy:IAMUser-RootCredentialUsage
Policy:S3/AccountBlockPublicAccessDisabled	TTPs/Policy:S3-AccountBlockPublicAccessDisabled
Policy:S3/BucketAnonymousAccessGranted	TTPs/Policy:S3-BucketAnonymousAccessGranted
Policy:S3/BucketBlockPublicAccessDisabled	Effects/Data Exposure/Policy:S3-BucketBlockPublicAccessDisabled
Policy:S3/BucketPublicAccessGranted	TTPs/Policy:S3-BucketPublicAccessGranted
PrivilegeEscalation：用戶/AnomalousBehavior	TTPs/Privilege Escalation/IAMUser-AnomalousBehavior
PrivilegeEscalation:IAMUser/AdministrativePermissions	TTPs/Privilege Escalation/PrivilegeEscalation:IAMUser-AdministrativePermissions
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated	TTPs/AnomalousBehavior/PriviledgeEscalation:Kubernetes-RoleBindingCreated

GuardDuty 尋找類型	ASFF 問題清單類型
PriviledgeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	TTPs/AnomalousBehavior/PriviledgeEscalation:Kubernetes-RoleCreated
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-ContainerMountsHostDirectory
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-CGroupsReleaseAgentModified
PrivilegeEscalation:Runtime/DockerSocketAccessed	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-DockerSocketAccessed
PrivilegeEscalation:Runtime/RuncContainerEscape	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-RuncContainerEscape
PrivilegeEscalation:Runtime/UserfaultfdUsage	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-UserfaultfdUsage
Recon:EC2/PortProbeEMRUnprotectedPort	TTPs/Discovery/Recon:EC2-PortProbeEMRUnprotectedPort
Recon:EC2/PortProbeUnprotectedPort	TTPs/Discovery/Recon:EC2-PortProbeUnprotectedPort
Recon:EC2/Portscan	TTPs/Discovery/Recon:EC2-Portscan
Recon:IAMUser/MaliciousIPCaller	TTPs/Discovery/Recon:IAMUser-MaliciousIPCaller
Recon:IAMUser/MaliciousIPCaller.Custom	TTPs/Discovery/Recon:IAMUser-MaliciousIPCaller.Custom
Recon:IAMUser/NetworkPermissions	TTPs/Discovery/Recon:IAMUser-NetworkPermissions
Recon:IAMUser/ResourcePermissions	TTPs/Discovery/Recon:IAMUser-ResourcePermissions

GuardDuty 尋找類型	ASFF 問題清單類型
Recon:IAMUser/TorIPCaller	TTPs/Discovery/Recon:IAMUser-TorIPCaller
Recon:IAMUser/UserPermissions	TTPs/Discovery/Recon:IAMUser-UserPermissions
ResourceConsumption:IAMUser/ComputeResources	Unusual Behaviors/User/ResourceConsumption:IAMUser-ComputeResources
Stealth:IAMUser/CloudTrailLoggingDisabled	TTPs/Defense Evasion/Stealth:IAMUser-CloudTrailLoggingDisabled
Stealth:IAMUser/LoggingConfigurationModified	TTPs/Defense Evasion/Stealth:IAMUser-LoggingConfigurationModified
Stealth:IAMUser/PasswordPolicyChange	TTPs/Defense Evasion/Stealth:IAMUser-PasswordPolicyChange
Stealth:S3/ServerAccessLoggingDisabled	TTPs/Defense Evasion/Stealth:S3-ServerAccessLoggingDisabled
Trojan:EC2/BlackholeTraffic	TTPs/Command and Control/Trojan:EC2-BlackholeTraffic
Trojan:EC2/BlackholeTraffic!DNS	TTPs/Command and Control/Trojan:EC2-BlackholeTraffic!DNS
Trojan:EC2/DGADomainRequest.B	TTPs/Command and Control/Trojan:EC2-DGADomainRequest.B
Trojan:EC2/DGADomainRequest.C!DNS	TTPs/Command and Control/Trojan:EC2-DGADomainRequest.C!DNS
Trojan:EC2/DNSDataExfiltration	TTPs/Command and Control/Trojan:EC2-DNSDataExfiltration
Trojan:EC2/DriveBySourceTraffic!DNS	TTPs/Initial Access/Trojan:EC2-DriveBySourceTraffic!DNS

GuardDuty 尋找類型	ASFF 問題清單類型
Trojan:EC2/DropPoint	Effects/Data Exfiltration/Trojan:EC2-DropPoint
Trojan:EC2/DropPoint!DNS	Effects/Data Exfiltration/Trojan:EC2-DropPoint!DNS
Trojan:EC2/PhishingDomainRequest!DNS	TTPs/Command and Control/Trojan:EC2-PhishingDomainRequest!DNS
Trojan:Lambda/BlackholeTraffic	TTPs/Command and Control/Trojan:Lambda-BlackholeTraffic
Trojan:Lambda/DropPoint	Effects/Data Exfiltration/Trojan:Lambda-DropPoint
Trojan:Runtime/BlackholeTraffic	TTPs/Command and Control/Trojan:Runtime-BlackholeTraffic
Trojan:Runtime/BlackholeTraffic!DNS	TTPs/Command and Control/Trojan:Runtime-BlackholeTraffic!DNS
Trojan:Runtime/DGADomainRequest.C!DNS	TTPs/Command and Control/Trojan:Runtime-DGADomainRequest.C!DNS
Trojan:Runtime/DriveBySourceTraffic!DNS	TTPs/Initial Access/Trojan:Runtime-DriveBySourceTraffic!DNS
Trojan:Runtime/DropPoint	Effects/Data Exfiltration/Trojan:Runtime-DropPoint
Trojan:Runtime/DropPoint!DNS	Effects/Data Exfiltration/Trojan:Runtime-DropPoint!DNS
Trojan:Runtime/PhishingDomainRequest!DNS	TTPs/Command and Control/Trojan:Runtime-PhishingDomainRequest!DNS
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	TTPs/Command and Control/UnauthorizedAccess:EC2-MaliciousIPCaller.Custom

GuardDuty 尋找類型	ASFF 問題清單類型
UnauthorizedAccess:EC2/MetadataDNSRebind	TTPs/UnauthorizedAccess:EC2-MetadataDNSRebind
UnauthorizedAccess:EC2/RDPBruteForce	TTPs/Initial Access/UnauthorizedAccess:EC2-RDPBruteForce
UnauthorizedAccess:EC2/SSHBruteForce	TTPs/Initial Access/UnauthorizedAccess:EC2-SSHBruteForce
UnauthorizedAccess:EC2/TorClient	Effects/Resource Consumption/UnauthorizedAccess:EC2-TorClient
UnauthorizedAccess:EC2/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:EC2-TorRelay
UnauthorizedAccess:IAMUser/ConsoleLogin	Unusual Behaviors/User/UnauthorizedAccess:IAMUser-ConsoleLogin
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	TTPs/UnauthorizedAccess:IAMUser-ConsoleLoginSuccess.B
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-InstanceCredentialExfiltration.InsideAWS
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-InstanceCredentialExfiltration.OutsideAWS
UnauthorizedAccess:IAMUser/MaliciousIPCaller	TTPs/UnauthorizedAccess:IAMUser-MaliciousIPCaller
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	TTPs/UnauthorizedAccess:IAMUser-MaliciousIPCaller.Custom
UnauthorizedAccess:IAMUser/TorIPCaller	TTPs/Command and Control/UnauthorizedAccess:IAMUser-TorIPCaller

GuardDuty 尋找類型	ASFF 問題清單類型
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom	TTPs/Command and Control/UnauthorizedAccess:Lambda-MaliciousIPCaller.Custom
UnauthorizedAccess:Lambda/TorClient	Effects/Resource Consumption/UnauthorizedAccess:Lambda-TorClient
UnauthorizedAccess:Lambda/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:Lambda-TorRelay
UnauthorizedAccess:Runtime/MetadataDNSRebind	TTPs/UnauthorizedAccess:Runtime-MetadataDNSRebind
UnauthorizedAccess:Runtime/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:Runtime-TorRelay
UnauthorizedAccess:Runtime/TorClient	Effects/Resource Consumption/UnauthorizedAccess:Runtime-TorClient
UnauthorizedAccess:S3/MaliciousIPCaller.Custom	TTPs/UnauthorizedAccess:S3-MaliciousIPCaller.Custom
UnauthorizedAccess:S3/TorIPCaller	TTPs/UnauthorizedAccess:S3-TorIPCaller

來自 GuardDuty 的一般問題清單

GuardDuty 使用安全性搜尋結果格式 (ASFF) 將發現項目傳送至AWS 安全性中樞。

這是一個典型的發現的例子 GuardDuty。

```
  {
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws::guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64/finding/46ba0ac2845071e23ccdeb2ae03bfdea",
  "ProductArn": "arn:aws::securityhub:us-east-1:product/aws/guardduty",
  "GeneratorId": "arn:aws::guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64",
  "AwsAccountId": "193043430472",
```

```
  "Types": [
    "TTPs/Initial Access/UnauthorizedAccess:EC2-SSHBruteForce"
  ],
  "FirstObservedAt": "2020-08-22T09:15:57Z",
  "LastObservedAt": "2020-09-30T11:56:49Z",
  "CreatedAt": "2020-08-22T09:34:34.146Z",
  "UpdatedAt": "2020-09-30T12:14:00.206Z",
  "Severity": {
    "Product": 2,
    "Label": "MEDIUM",
    "Normalized": 40
  },
  "Title": "199.241.229.197 is performing SSH brute force attacks against
 i-0c10c2c7863d1a356.",
  "Description": "199.241.229.197 is performing SSH brute force attacks against
 i-0c10c2c7863d1a356. Brute force attacks are used to gain unauthorized access to your
 instance by guessing the SSH password.",
  "SourceUrl": "https://us-east-1.console.aws.amazon.com/guardduty/home?region=us-
east-1#/findings?macros=current&fId=46ba0ac2845071e23ccdeb2ae03bfdea",
  "ProductFields": {
    "aws/guardduty/service/action/networkConnectionAction/remotePortDetails/portName":
 "Unknown",
    "aws/guardduty/service/archived": "false",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
asnOrg": "CENTURYLINK-US-LEGACY-QWEST",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/geoLocation/
lat": "42.5122",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/ipAddressV4":
 "199.241.229.197",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/geoLocation/
lon": "-90.7384",
    "aws/guardduty/service/action/networkConnectionAction/blocked": "false",
    "aws/guardduty/service/action/networkConnectionAction/remotePortDetails/port":
 "46717",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/country/
countryName": "United States",
    "aws/guardduty/service/serviceName": "guardduty",
    "aws/guardduty/service/evidence": "",
    "aws/guardduty/service/action/networkConnectionAction/localIpDetails/ipAddressV4":
 "172.31.43.6",
    "aws/guardduty/service/detectorId": "d4b040365221be2b54a6264dc9a4bc64",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
org": "CenturyLink",
```

```
    "aws/guardduty/service/action/networkConnectionAction/connectionDirection":
 "INBOUND",
    "aws/guardduty/service/eventFirstSeen": "2020-08-22T09:15:57Z",
    "aws/guardduty/service/eventLastSeen": "2020-09-30T11:56:49Z",
    "aws/guardduty/service/action/networkConnectionAction/localPortDetails/portName":
 "SSH",
    "aws/guardduty/service/action/actionType": "NETWORK_CONNECTION",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/city/
cityName": "Dubuque",
    "aws/guardduty/service/additionalInfo": "",
    "aws/guardduty/service/resourceRole": "TARGET",
    "aws/guardduty/service/action/networkConnectionAction/localPortDetails/port": "22",
    "aws/guardduty/service/action/networkConnectionAction/protocol": "TCP",
    "aws/guardduty/service/count": "74",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
asn": "209",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
isp": "CenturyLink",
    "aws/securityhub/FindingId": "arn:aws::securityhub:us-east-1::product/
aws/guardduty/arn:aws::guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64/finding/46ba0ac2845071e23ccdeb2ae03bfdea",
    "aws/securityhub/ProductName": "GuardDuty",
    "aws/securityhub/CompanyName": "Amazon"
  },
  "Resources": [
    {
      "Type": "AwsEc2Instance",
      "Id": "arn:aws::ec2:us-east-1:193043430472:instance/i-0c10c2c7863d1a356",
      "Partition": "aws",
      "Region": "us-east-1",
      "Tags": {
        "Name": "kubectl"
      },
      "Details": {
        "AwsEc2Instance": {
          "Type": "t2.micro",
          "ImageId": "ami-02354e95b39ca8dec",
          "IpV4Addresses": [
            "18.234.130.16",
            "172.31.43.6"
          ],
          "VpcId": "vpc-a0c2d7c7",
          "SubnetId": "subnet-4975b475",
          "LaunchedAt": "2020-08-03T23:21:57Z"
```

```
        }
      }
    }
  ],
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE"
}
```

啟用與設定整合

若要使用與整合 AWS Security Hub，您必須啟用 Security Hub。如需有關如何啟用 Security Hub 的資訊，請參閱 AWS Security Hub 使用者指南中的設定 Security Hub。

當您同時啟用 GuardDuty 和 Security Hub 時，會自動啟用整合。 GuardDuty立即開始將發現發現發送到 Security Hub。

停止將調查結果發布至 Security Hub

若要停止將問題清單傳送至 Security Hub，您可以使用 Security Hub 主控台或 API。

請參閱AWS Security Hub 使用指南中的整合 (主控台) 停用和啟用發現項目流程或停用整合 (Security Hub API、 AWS CLI) 中的發現項目流程。

與 Amazon Detective 整合

Amazon Detective 會透過建立資料視覺化效果，以表示資源在一段時間內的行為和互動方式，協助您快速分析和調查一個或多個 AWS 帳戶的安全事件。Detective 將 GuardDuty 的調查結果建立視覺化效果。

Detective 會擷取所有調查結果類型的調查結果詳細資訊，並提供實體設定檔的存取權，以調查與調查結果有關的不同實體。實體可以是 AWS 帳戶、帳戶內的 AWS 資源，也可以是與您的資源互動的外部 IP 地址。GuardDuty 主控台支援從下列實體樞紐至 Amazon Detective，具體取決於調查結果類型：AWS 帳戶、IAM 角色、使用者或角色工作階段、使用者代理程式、聯合身分使用者、Amazon EC2 執行個體或 IP 地址。

內容

啟用整合

若要將 Amazon Detective 與 GuardDuty 一起使用，您必須首先啟用 Amazon Detective。如需有關如何啟用 Detective 的資訊，請參閱 Amazon Detective Administration Guide 的 Setting up Amazon Detective。

當您同時啟用 GuardDuty 和 Detective 時，會自動啟用整合。啟用後，Detective 將立即擷取 GuardDuty 調查結果資料。

> **Note**
>
> GuardDuty 會根據 GuardDuty 調查結果的匯出頻率，將調查結果傳送給 Detective。根據預設，現有調查結果更新的匯出頻率為 6 小時。為了確保 Detective 能夠收到您調查結果的最新更新，建議您在 Detective 與 GuardDuty 一起使用的每個區域中將匯出頻率變更為 15 分鐘。如需詳細資訊，請參閱步驟 5 — 設定匯出更新的使用中發現項目的頻率。

從 GuardDuty 調查結果樞紐至 Amazon Detective

1. 登入主控台，網址為 https://console.aws.amazon.com/guardduty/。
2. 從調查結果表中選擇單個調查結果。
3. 從調查結果詳細資訊窗格中選擇使用 Detective 來調查。
4. 選擇調查結果的一個方面，以使用 Amazon Detective 來調查。這會針對該調查結果或實體開啟 Detective 主控台。

如果樞紐未如預期般運作，請參閱 Amazon Detective User Guide 中的 Troubleshooting the pivot。

> **Note**
>
> 如果您在 Detective 主控台中封存 GuardDuty 調查結果，該調查結果也會封存在 GuardDuty 主控台中。

使用與 GuardDuty 多帳戶環境的整合

如果您在 GuardDuty 中管理多帳戶環境，則必須將您的成員帳戶新增至 Amazon Detective，才能查看這些帳戶中調查結果和實體的 Detective 資料視覺化效果。

建議您使用與 Detective 的管理員帳戶相同的 GuardDuty 管理員帳戶。如需有關在 Detective 中新增成員帳戶的詳細資訊，請參閱 Inviting member accounts。

> **Note**
>
> Detective 是一項區域性服務，這意味著您必須啟用 Detective，並在要使用整合的每個區域中新增成員帳戶。

暫停或停用 GuardDuty

您可以使用 GuardDuty 主控台暫停或停用 GuardDuty 服務。當服務暫停 GuardDuty 時，您無需支付使用費用。

- 您必須先取消關聯或刪除所有成員帳戶，然後才能暫停或停用 GuardDuty。
- 如果您暫停 GuardDuty，它將不再監視 AWS 環境的安全性或產生新的發現項目。您現有的發現保持完整，不會受到 GuardDuty 暫停的影響。您可以選擇 GuardDuty 稍後重新啟用。
- 當您在帳戶 GuardDuty 中停用時，只會針對目前選取的帳戶停用該帳號 AWS 區域。如果要完全禁用 GuardDuty，則必須在啟用它的每個區域中禁用它。
- 如果停用 GuardDuty，您現有的發現項目和 GuardDuty 設定都會遺失，而且無法復原。如果您要儲存現有的發現項目，您必須先匯出它們，然後再確認停用 GuardDuty。如需有關如何匯出調查結果的資訊，請參閱匯出調查結果。

若要暫停或停用 GuardDuty

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/
2. 在導覽窗格中，選擇設定。
3. 在「暫停 GuardDuty」區段中，選擇「暫停」 GuardDuty 或「停用」 GuardDuty，然後選擇「確認動作」

暫停後重新啟 GuardDuty 用

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/
2. 在導覽窗格中，選擇設定。
3. 選擇重新啟用 GuardDuty。

訂閱 Amazon SNS GuardDuty 公告

本節提供訂閱 Amazon SNS (簡單通知服務) 的相關資訊，以接收有關新發現項目類型的通知、現有發現項目類型的更新，以及其他功能變更的通知。 GuardDuty 所有 Amazon SNS 所支援格式的通知。

GuardDuty SNS 會將有關 GuardDuty 服務更新的公告傳送 AWS 到任何訂閱帳戶。若要接收有關帳戶內調查結果的通知，請參閱使用 Amazon CloudWatch 活動建立自訂回應的 GuardDuty 發現項目。

> **Note**
>
> 您的 IAM 使用者帳戶必須具有 `sns::subscribe` 許可，才能訂閱 SNS。

您可以訂閱此通知主題的 Amazon SQS 佇列，但使用的主題 ARN 必須位於相同的區域。如需詳細資訊，請參閱《Amazon Simple Queue Service 開發人員指南》中的教學課程：Subscribing an Amazon SQS queue to an Amazon SNS topic。

您也可以使用 AWS Lambda 功能在收到通知時觸發事件。如需詳細資訊，請參閱《Amazon Simple Queue Service 開發人員指南》中的 Invoking Lambda functions using Amazon SNS notifications。

每個區域的 Amazon SNS 主題 ARN 如下所示。

AWS 地區	Amazon SNS 主題 ARN
us-east-1	arn:aws:sns:us-east-1:242987662583:GuardDutyAnnouncements
us-east-2	arn:aws:sns:us-east-2:118283430703:GuardDutyAnnouncements
us-west-1	arn:aws:sns:us-west-1:144182107116:GuardDutyAnnouncements

AWS 地區	Amazon SNS 主題 ARN
us-west-2	arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements
ca-central-1	arn:aws:sns:ca-central-1:107430051933:GuardDutyAnnouncements
ca-west-1	arn:aws:sns:ca-west-1:440427180217:GuardDutyAnnouncements
eu-north-1	arn:aws:sns:eu-north-1:973841112453:GuardDutyAnnouncements
eu-west-1	arn:aws:sns:eu-west-1:965013871422:GuardDutyAnnouncements
eu-west-2	arn:aws:sns:eu-west-2:506403581195:GuardDutyAnnouncements
eu-west-3	arn:aws:sns:eu-west-3:436163563069:GuardDutyAnnouncements

AWS 地區	Amazon SNS 主題 ARN
eu-central-1	arn:aws:sns:eu-central-1:378365507264:GuardDutyAnnouncements
eu-central-2	arn:aws:sns:eu-central-2:383009515534:GuardDutyAnnouncements
ap-east-1	arn:aws:sns:ap-east-1:646602203151:GuardDutyAnnouncements
ap-northeast-1	arn:aws:sns:ap-northeast-1:741172661024:GuardDutyAnnouncements
ap-northeast-2	arn:aws:sns:ap-northeast-2:464168911255:GuardDutyAnnouncements
ap-southeast-1	arn:aws:sns:ap-southeast-1:476419727788:GuardDutyAnnouncements
ap-southeast-2	arn:aws:sns:ap-southeast-2:457615622431:GuardDutyAnnouncements

AWS 地區	Amazon SNS 主題 ARN
ap-south-1	arn:aws:sns:ap-south-1:926826061926:GuardDutyAnnouncements
sa-east-1	arn:aws:sns:sa-east-1:955633302743:GuardDutyAnnouncements
us-gov-west-1	arn:aws-us-gov:sns:us-gov-west-1:430639793359:GuardDutyAnnouncements
cn-north-1	arn:aws-cn:sns:cn-north-1:002991280229:GuardDutyAnnouncements
cn-northwest-1	arn:aws-cn:sns:cn-northwest-1:003033775354:GuardDutyAnnouncements
me-south-1	arn:aws:sns:me-south-1:552740612889:GuardDutyAnnouncements
me-central-1	arn:aws:sns:me-central-1:030935290150:GuardDutyAnnouncements

AWS 地區	Amazon SNS 主題 ARN
eu-south-1	arn:aws:sns:eu-south-1:188461706213:GuardDutyAnnouncements
eu-south-2	arn:aws:sns:eu-south-2:445632894446:GuardDutyAnnouncements
us-gov-east-1	arn:aws:sns:us-gov-east-1:143972945659:GuardDutyAnnouncements
ap-northeast-3	arn:aws:sns:ap-northeast-3:129086577509:GuardDutyAnnouncements
ap-southeast-3	arn:aws:sns:ap-southeast-3:225965583551:GuardDutyAnnouncements
ap-south-2	arn:aws:sns:ap-south-2:595653072700:GuardDutyAnnouncements
ap-southeast-4	arn:aws:sns:ap-southeast-4:529900636122:GuardDutyAnnouncements

AWS 地區	Amazon SNS 主題 ARN
il-central-1	arn:aws:sns:il-central-1:847886274986:GuardDutyAnnouncements

若要在中訂閱 GuardDuty 更新通知電子郵件 AWS Management Console

1. 在 https://console.aws.amazon.com/sns/v3/home 開啟 Amazon SNS 主控台。
2. 在區域清單中，選擇與您要訂閱的主題 ARN 相同的區域。此範例使用 us-west-2 區域。
3. 在左側導覽窗格中，選擇訂閱、建立訂閱。
4. 在建立訂閱對話方塊中，針對主題 ARN，貼上主題 ARN：arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements。
5. 對於通訊協定，選擇電子郵件。針對端點，輸入可用於接收通知的電子郵件地址。
6. 選擇建立訂閱。
7. 在您的電子郵件應用程式中，開啟「AWS 通知」中的訊息，然後開啟連結以確認您的訂閱。

   您的 Web 瀏覽器顯示自 Amazon SNS 的確認回覆。

若要使用訂閱 GuardDuty 更新通知電子郵件 AWS CLI

1. 使用 AWS CLI執行下列命令：

```
 aws  sns --region us-west-2 subscribe --topic-arn arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements --protocol email --notification-endpoint your_email@your_domain.com
```

2. 在您的電子郵件應用程式中，開啟「AWS 通知」中的訊息，然後開啟連結以確認您的訂閱。

   您的 Web 瀏覽器顯示自 Amazon SNS 的確認回覆。

Amazon SNS 訊息格式

有關新發現項目的 GuardDuty 更新通知訊息範例如下所示：

```
{
    "Type" : "Notification",
    "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message" : "{\"version\":\"1\",\"type\":\"NEW_FINDINGS\",\"findingDetails
\":[{\"link\":\"https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html\",\"findingType\":\"UnauthorizedAccess:EC2/TorClient\",
\"findingDescription\":\"This finding informs you that an EC2 instance in your AWS
 environment is making connections to a Tor Guard or an Authority node. Tor is software
 for enabling anonymous communication. Tor Guards and Authority nodes act as initial
 gateways into a Tor network. This traffic can indicate that this EC2 instance is
 acting as a client on a Tor network. A common use for a Tor client is to circumvent
 network monitoring and filter for access to unauthorized or illicit content. Tor
 clients can also generate nefarious Internet traffic, including attacking SSH servers.
 This activity can indicate that your EC2 instance is compromised.\"}]}",
    "Timestamp" : "2018-03-09T00:25:43.483Z",
    "SignatureVersion" : "1",
    "Signature" : "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/6ssyrlj1g==",
    "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

已經移除逸出引號的剖析訊息數值會如下所示：

```
{
    "version": "1",
    "type": "NEW_FINDINGS",
    "findingDetails": [{
        "link": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html",
        "findingType": "UnauthorizedAccess:EC2/TorClient",
        "findingDescription": "This finding informs you that an EC2 instance in your
 AWS environment is making connections to a Tor Guard or an Authority node. Tor is
 software for enabling anonymous communication. Tor Guards and Authority nodes act as
 initial gateways into a Tor network. This traffic can indicate that this EC2 instance
```

```
 is acting as a client on a Tor network. A common use for a Tor client is to circumvent
 network monitoring and filter for access to unauthorized or illicit content. Tor
 clients can also generate nefarious Internet traffic, including attacking SSH servers.
 This activity can indicate that your EC2 instance is compromised."
    }]
}
```

關於 GuardDuty 功能 GuardDuty 更新的範例更新通知訊息如下所示：

```
{
    "Type" : "Notification",
    "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message" : "{\"version\":\"1\",\"type\":\"NEW_FEATURES\",\"featureDetails
\":[{\"featureDescription\":\"Customers with high-volumes of global CloudTrail
 events should see a net positive impact on their GuardDuty costs.\",\"featureLink
\":\"https://docs.aws.amazon.com//guardduty/latest/ug/guardduty_data-
sources.html#guardduty_cloudtrail\"}]}",
    "Timestamp" : "2018-03-09T00:25:43.483Z",
    "SignatureVersion" : "1",
    "Signature" : "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/6ssyrlj1g==",
    "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

已經移除逸出引號的剖析訊息數值會如下所示：

```
{
    "version": "1",
    "type": "NEW_FEATURES",
    "featureDetails": [{
        "featureDescription": "Customers with high-volumes of global CloudTrail events
 should see a net positive impact on their GuardDuty costs.",
        "featureLink": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_data-sources.html#guardduty_cloudtrail"
```

```
    }]
}
```

有關 GuardDuty 更新發現項目的更新通知訊息範例如下所示：

```
{
    "Type": "Notification",
    "MessageId": "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn": "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message": "{\"version\":\"1\",\"type\":\"UPDATED_FINDINGS\",
\"findingDetails\":[{\"link\":\"https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html\",\"findingType\":\"UnauthorizedAccess:EC2/TorClient\",
\"description\":\"Increased severity value from 5 to 8.\"}]}",
    "Timestamp": "2018-03-09T00:25:43.483Z",
    "SignatureVersion": "1",
    "Signature": "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/6ssyrlj1g==",
    "SigningCertURL": "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL": "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

已經移除逸出引號的剖析訊息數值會如下所示：

```
{
    "version": "1",
    "type": "UPDATED_FINDINGS",
    "findingDetails": [{
        "link": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html",
        "findingType": "UnauthorizedAccess:EC2/TorClient",
        "description": "Increased severity value from 5 to 8."
    }]
}
```

Amazon 的配額 GuardDuty

您的 AWS 帳戶有每項 AWS 服務的預設配額 (先前稱為限制)。除非另有說明，否則每個配額都是區域特定規定。您可以要求增加某些配額，而其他配額則無法增加。

若要檢視的配額 GuardDuty，請開啟「Service Quotas」主控台。在導覽窗格中，選擇AWS 服務，然後選取 Amazon GuardDuty。

若要請求提高配額，請參閱《Service Quotas 使用者指南》中的請求提高配額。

您的 AWS 帳戶對 GuardDuty 每個區域的 Amazon 配額如下。

> **Note**
>
> 如需 GuardDuty 惡意程式碼防護的特定配額，請參閱惡意軟體防護配額。

資源	預設	說明
偵測器	1	每個區域的每個 AWS 帳戶可建立之偵測器資源的數量上限。 您無法要求提高配額。
篩選條件	100	每個區域每個 AWS 帳戶可儲存的過濾器數目上限。 您無法要求提高配額。
尋找保留期間	90 天	調查結果的保留天數上限。 您無法要求提高配額。

資源	預設	說明
每個受信任 IP 清單的 IP 地址和 CIDR 範圍	2,000	單一受信任 IP 清單可包含的 IP 地址和 CIDR 範圍數量上限。 您無法要求提高配額。
每個威脅清單的 IP 地址和 CIDR 範圍	250,000	威脅清單中可包含的 IP 地址和 CIDR 範圍數量上限。 您無法要求提高配額。
檔案大小上限	35 MB	受信任 IP 清單或威脅清單中，上傳至 IP 地址清單或 CIDR 範圍的檔案大小上限。 您無法要求提高配額。
成員帳戶 (透過邀請)	5000	與管理員帳戶帳戶相關聯的成員帳戶數目上限。 您無法要求提高配額。

資源	預設	說明
成員帳戶	50,000	透過管理員帳戶與管理員帳戶相關聯的成員帳戶數目上限 AWS Organizations。這包括透過邀請新增至組織的成員帳戶。 此預設值取決於您目前在中的成員帳戶配額 AWS Organizations。透過新增的成員帳戶數目不 AWS Organizations 能超過組織中的成員帳戶數目。 GuardDuty 若要取得有關組織 AWS 帳戶 中的數目的資訊，請參閱《AWS Organizations 使用指南》中的〈最大值和最小值〉。
威脅 intel 集	6	每個區域的每個 AWS 帳戶可新增之威脅情報集的數量上限。 您無法要求提高配額。
信任的 IP 集	1	每個區域每個 AWS 帳戶可上傳和啟用的信任 IP 集數目上限。 您無法要求提高配額。

Amazon 故障 GuardDuty

當您收到與執行特定動作相關的問題時 GuardDuty，請參閱本節中的主題。

主題

中的一般問題 GuardDuty

導出發現結果時出 GuardDuty 現訪問錯誤。我該如何解決這個問題？

設定匯出發現項目的設定後，如果 GuardDuty 無法匯出發現項目，它會在 GuardDuty 主控台的 [設定] 頁面上顯示錯誤訊息。當無法再存取目標資源時， GuardDuty 可能會發生這種情況，例如，如果刪除了 Amazon S3 儲存貯體或存取儲存貯體的權限已修改。當 GuardDuty 無法再存取用於加密 Amazon S3 儲存貯體中資料的 AWS KMS 金鑰時，也可能發生這種情況。無 GuardDuty 法匯出時，會傳送通知至與帳戶相關聯的電子郵件，以提供此問題的相關資訊。

若要解決此問題，請確定對應的資源存在，且 GuardDuty 具有存取所需資源的權限。如果您在 90 天尋找保留期完成之前未解決問題 GuardDuty，則不會匯出您的發現項目。 GuardDuty 將禁用在特定區域中查找此帳戶的導出設置。即使在此保留日期之後，您也可以更新組態設定，以重新匯出特定區域中的發現項目。

如需詳細資訊，請參閱 匯出調查結果。

惡意程式碼防護

我正在啟動隨需惡意軟體掃描，但會導致缺少所需許可的錯誤。

如果您收到錯誤，提示您不具備在 Amazon EC2 執行個體上啟動隨需惡意軟體掃描所需的許可，請確認您是否已將 AWS 受管理的策略：AmazonGuardDutyFullAccess 政策連接至您的 IAM 角色。

如果您是 AWS 組織的成員，但仍然收到相同的錯誤訊息，請連線至您的管理帳戶。如需詳細資訊，請參閱 AWS Organizations SCP — 拒絕存取。

我在使用惡意軟體防護時收到 **iam:GetRole** 錯誤。

如果您收到此錯誤 —`Unable to get role: AWSServiceRoleForAmazonGuardDutyMalwareProtection`，則表示您缺少啟用 GuardDuty 起始的惡意軟體掃描或使用指定惡意軟體掃描的權限。確認您是否已將 AWS 受管理的策略：AmazonGuardDutyFullAccess 政策連接至您的 IAM 角色。

我是一個管理 GuardDuty 員帳戶，需要啟用啟 GuardDuty動的惡意軟件掃描，但不使用 AWS 託管策略： AmazonGuardDutyFullAccess進行管理 GuardDuty。

- 設定與您搭配使用的 IAM 角色，以取 GuardDuty 得啟用啟用惡意程式碼 GuardDuty掃描的必要權限。如需有關所需許可的詳細資訊，請參閱 Creating a service-linked role for Malware Protection。
- 將 AWS 受管理的策略：AmazonGuardDutyFullAccess 連接至您的 IAM 角色。這將幫助您為成員帳戶啟用啟 GuardDuty動的惡意軟件掃描。

運行時監視問題

我的 AWS Step Functions 工作流程意外失敗

如果 GuardDuty 容器導致工作流程失敗，請參閱對涵蓋範圍問題進行疑難排解。如果問題仍然存在，請執行下列其中一個步驟，以防止工作流程因為 GuardDuty 容器而失敗：

- 將`GuardDutyManaged`:標`false`籤新增至關聯的 Amazon ECS 叢集。
- 在帳戶層級停用 AWS Fargate (僅限 ECS) 的自動化代理程式組態。將包含標籤`GuardDutyManaged`：新增`true`至您要使用 GuardDuty 自動化代理程式繼續監控的關聯 Amazon ECS 叢集。

執行階段監控中記憶體不足錯誤的疑難排解 (僅限 Amazon EC2 支援)

本節提供當您發生記憶體不足錯誤時，根據手動部署 GuardDuty Security Agent 的疑難排解步驟。CPU 和記憶體限制

如果因為`out-of-memory`問題而`systemd`終止 GuardDuty 代理程式，而您評估為 GuardDuty 代理程式提供更多記憶體是合理的，則可以更新限制。

1. 在根權限下，開啟`/lib/systemd/system/amazon-guardduty-agent.service`。

2. 查找MemoryLimit和MemoryMax更新這兩個值。

```
MemoryLimit=256MB
MemoryMax=256MB
```

3. 更新值之後，請使用下列命令重新啟動 GuardDuty 代理程式：

```
sudo systemctl daemon-reload
sudo systemctl restart amazon-guardduty-agent
```

4. 執行下列命令以檢視狀態：

```
sudo systemctl status amazon-guardduty-agent
```

預期的輸出將顯示新的內存限制：

```
Main PID: 2540 (amazon-guardduty)
Tasks: 16
Memory: 21.9M (limit: 256.0M)
```

管理多個帳戶問題

我想要管理多個帳戶，但沒有必要的 AWS Organizations 管理權限。

如果您收到這個錯誤 —`The request failed because you do not have required AWS Organization master permission.`，這表示您缺少啟用 GuardDuty組織中多個帳戶的惡意軟體掃描的權限。如需有關提供管理帳戶權限的詳細資訊，請參閱建立受信任的存取以啟 GuardDuty動惡意軟體掃描。

其他疑難排解問題

如果找不到適合您問題的案例，請檢視下列疑難排解選項：

- 如需了解存取 https://console.aws.amazon.com/guardduty/ 時的一般 IAM 問題，請參閱疑難排解 Amazon GuardDuty 身分和存取。
- 有關存取時的身份驗證和授權問題 AWS AWS Console Home，請參閱 IAM 疑難排解。

區域與端點

要查看 Amazon AWS 區域 可 GuardDuty 用的地方， GuardDuty 請參閱 Amazon Web Services 一般參考.

我們建議您 GuardDuty 在所有支援中啟用 AWS 區域。這可讓 GuardDuty 您產生關於未經授權或不尋常活動的發現，即使在您未主動使用的區域中也是如此。這也 GuardDuty 允許監視受支持的 AWS CloudTrail 事件 AWS 區域，其檢測涉及全局服務的活動的能力減少。

區域特定功能的可用性

用於指定 GuardDuty 功能可用性的區域差異列表。

ListFindings 和 GetFindingsStatistics API

GetFindingsStatistics和 ListFindingsAPI 有一個臨時`consoleOnly`標誌。當您使用這些 API 中的任何一個或兩個時，該`consoleOnly`標誌意味著 API 可以獲取結果的最大限制為 1000。

GuardDuty 具有區域差距的功能

GuardDuty 惡意程式碼

GuardDuty 支援AWS 專屬 Local Zones 中的惡意程式碼防護功能。

Amazon GuardDuty API 參考中的下列 API 可能會因為先前指定 AWS 區域的某些資料來源或功能無法使用而存在區域差異：

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

Amazon EC2 調查結果類型：DefenseEvasion:EC2/UnusualDoHActivity 和 DefenseEvasion:EC2/UnusualDoTActivity

下表顯示可用的 AWS 區域 GuardDuty 位置，但這兩個 Amazon EC2 尋找類型尚不受支援。

AWS 區域	區域代碼
亞太區域 (首爾)	ap-northeast-2
亞太區域 (大阪)	ap-northeast-3
亞太區域 (雅加達)	ap-southeast-3

AWS GovCloud (US) 地區

如需最新資訊，請參閱AWS GovCloud (US) 使用者指南 GuardDuty中的 Amazon。

中國地區

如需最新資訊，請參閱 Feature availability and implementation differences。

GuardDuty 舊式動作和參數

Amazon GuardDuty 已經棄用了一些 API 操作和參數，但仍然支持它們。最佳實務是使用新的 API 動作和參數來取代舊版選項。以下表格對舊版和新版動作及參數進行了比較。

舊版動作/參數	新版動作/參數	Comparison (比較)
DisassociateFromMasterAccount	DisassociateFromAdministratorAccount	在這兩個動作中使用相同的實作時， GuardDuty 會使用Administrator 中的術語DisassociateFromAdministratorAccount 。
autoEnable 和 DescribeOrganizationConfiguration和中的參數 UpdateOrganizationConfiguration	autoEnableOrganizationMembers	使用時autoEnableOrganizationMembers ，GuardDuty 管理員帳戶可以稽核所有成員帳戶，並強制執行 GuardDuty 其中一個值。使用 API，最多可能需要 24 小時才會更新所有成員帳戶的組態。如需autoEnableOrganizationMembers 欄位可能值的詳細資訊，請參閱autoEnableOrganization成員
GuardDuty 二零二三年三月的空氣指數變 列出的 API 中的 dataSources 參數。	features	從 2023 年 3 月開始，您可以Amazon 中的惡意軟件 GuardDuty GuardDuty 使用features. 2023 年 3 月之前啟動的保護計畫 (包括惡意軟體防護) 仍支援使用 dataSources 進行設定。如果您使用 API 來設定保護計畫，則每個 API 請求可以包含 dataSources 或 features，但不能同時包含兩者。

Amazon 的文檔歷史 GuardDuty

下表說明自上次發行 Amazon GuardDuty 使用者指南以來對文件的重要變更。如需有關此文件更新的通知，您可以訂閱 RSS 訂閱源。

變更	描述	日期
GuardDuty 運行時監控中的更新功能-Fargate (僅限 Amazon ECS)	執行階段監控針對 AWS Fargate (僅限 Amazon ECS) 資源發佈了新的代理程式版本 1.2.0。如需有關版本說明的詳細資訊，請參閱 Fargate-ECs 的GuardDuty 安全性代理程式。	2024年5月31 日
更新的 GuardDuty 惡意軟體防護功能	對於連接到 Amazon EC2 執行個體和容器工作負載的每個 Amazon EBS 磁碟區，GuardDuty 惡意軟體防護已將掃描的 EBS 磁碟區大小增加到最高 2048 GB。如需掃描連接至執行個體的 Amazon EBS 磁碟區的詳細資訊，請參閱GuardDuty 惡意軟體防護。	2024年5月29 日
運行時監視中的更新功能	適用於 Amazon ECS-Fargate 資源的執行階段監控現在可支援偵測由啟動的任務上的潛在威脅。 AWS Batch如需詳細資訊，請參閱執行階段監控如何與 Fargate 搭配使用 (僅限 Amazon ECS)。	2024年5月28日
運行時監視中的更新功能	運行時監控針對 Amazon EKS 資源發布了新的代理程式版本 1.6.1。如需有關版本說明的資	2024 年 5 月 14 日

	訊，請參閱 EKS 附加元件代理程式發行歷程	
擴充執行階段監控的區域支援	GuardDuty 將對運行時監控的支持擴展到加拿大西部（卡爾加里）地區。如需開始使用執行階段監視的相關資訊，請參閱啟用執行階段監視	2024年5月7日
針對 RDS 保護的擴充區域支援	GuardDuty 將 RDS 保護支援擴展到以下內容 AWS 區域： • 加拿大西部 (卡加利) • 亞太區域 (海德拉巴) • 歐洲 (西班牙) • 歐洲 (蘇黎世) • 中東 (阿拉伯聯合大公國) • 以色列 (特拉維夫) • 亞太區域 (墨爾本) 如需啟用此功能的相關資訊，請參閱 RDS 防護。	2024年5月3日
運行時監視中的更新功能	執行階段監控針對 AWS Fargate (僅限 Amazon ECS) 資源發佈了新的代理程式 1.1.0 版。如需有關版本說明的詳細資訊，請參閱 Fargate-ECs 的 GuardDuty 安全性代理程式。	2024年5月1日
運行時監視中的更新功能	運行時監控發布了用於 Amazon EKS 資源的新代理版本 1.6.0。如需有關版本說明的資訊，請參閱 EKS 附加元件代理程式發行歷程	2024年4月29 日

Support IP 位址 6	GuardDuty 已為本地和遠程 IP 詳細信息添加了 IPAddressv6 支持。您可以使用關聯的「篩選器」屬性來篩選 GuardDuty 發現項目或建立隱藏規則。	2024年4月18日
更新主控台體驗以設定匯出發現項	GuardDuty 已更新主控台體驗 AWS 帳戶，將您的發現項目匯出至 Amazon S3 儲存貯體。如需詳細資訊，請參閱匯出 GuardDuty 發現項目。	2024年4月1日
運行時監視中的更新功能	執行階段監控針對 Amazon EC2 資源發佈了新的安全代理程式 1.1.0 版。此版本支援 Amazon EC2 執行個體的執行階段監控中的 GuardDuty 自動代理程式組態。如需有關版本說明的資訊，請參閱 Amazon EC2 執行個體的GuardDuty 安全代理程式。	2024年3月28日

適用於 Amazon EC2 執行個體的執行階段監控一般可	GuardDuty 宣布針對 Amazon EC2 執行個體提供執行時間監控的正式可用性 (GA)。現在，您可以選擇啟用自動化代理程式組態，以 GuardDuty 便代表您安裝和管理 Amazon EC2 執行個體的安全代理程式。透過 GuardDuty 自動化代理程式，您也可以使用包含或排除標籤 GuardDuty 來通知僅在選定的 Amazon EC2 執行個體上安裝和管理安全代理程式。如需詳細資訊，請參閱執行階段監控如何搭配 Amazon EC2 執行個體運作。 與此 GA 一起發布的新發現類型列表 • 執行：執行階段/SuspiciousTool • 執行：執行階段/SuspiciousCommand • DefenseEvasion: 執行時間/SuspiciousCommand • DefenseEvasion: 執行時間/PtraceAntiDebugging • 執行：執行階段/MaliciousFileExecuted	2024年3月28日

Amazon GuardDuty 已經更新了服務鏈接角色（SLR）	使用 Amazon EC2 的自動化代理程式啟用執行時 GuardDuty 間監控時，使用動 AWS Systems Manager 作來管理 Amazon EC2 執行個體上的 SSM 關聯。停用 GuardDuty 自動化代理程式組態時，只 GuardDuty 會考慮具有包含標籤 (GuardDuty Managed :true) 的 EC2 執行個體。 • 下列清單顯示新的權限： `"ssm:DescribeAssociation", "ssm:DeleteAssociation", "ssm:UpdateAssociation", "ssm:CreateAssociation", "ssm:StartAssociationsOnce", "ssm:AddTagsToResource", "ssm:CreateAssociation", "ssm:UpdateAssociation", "ssm:SendCommand", "ssm:GetCommandInvocation"`	2024年3月26日

運行時監視中的更新功能	使用適用於 Amazon EKS 的最新 GuardDuty 安全代理程式 (附加元件) v1.5.0 版本，執行階段監控現在支援設定 GuardDuty 安全代理程式的特定參數，例如 CPU 和記憶體設定、`PriorityClass` 設定和 DNS 政策設定。如需詳細資訊，請參閱設定 GuardDuty安全性代理程式 (EKS 附加元件)參數。	2024年3月7日
運行時監視中的更新功能	運行時監控發布了適用於 Amazon EKS 資源的新代理程式版本 1.5.0。如需有關版本說明的資訊，請參閱 EKS 附加元件代理程式發行歷程	2024年3月7日
Support 加拿大西部（卡加利）	Amazon 現 GuardDuty 已在加拿大西部（卡爾加里）地區提供。此地區 GuardDuty 可能無法使用其中的某些保護計劃。如需最新資訊，請參閱區域和端點。	2024年3月6日
運行時監視中的更新功能	自 2024 年 5 月 14 日起，將不再支援適用於 Amazon EKS 叢集的 GuardDuty 安全代理程式版本 1.0.0 和 1.1.0 版。如需在標準支援結束前可採取哪些步驟的相關資訊，請參閱 Amazon EKS 叢集的GuardDuty 安全代理程式。	2024年2月16日

運行時監視中的更新功能	執行階段監視支援最新的 Kubernetes 1.29 版，以及現有的安全性代理程式版本 1.4.1。自此 Kubernetes 版本推出以來，已提供支援服務。如需支援之 Kubernetes 版本的相關資訊，請參閱安全性代理程式支援的 Kubernetes 版本。GuardDuty	2024年2月16日
執行階段監控中的更新功能-區域可用	GuardDuty 執行階段監控現在支援相同 AWS Organizations版本中的共用 Amazon VPC。GuardDuty 服務連結角色 (SLR) 具有新的權限，`organizations:DescribeOrganization` 可協助擷取共用 Amazon VPC 帳戶的組織 ID 以設定端點政策。如需在執行階段監控中使用共用 Amazon VPC 端點的先決條件的相關資訊，請參閱共用 Amazon VPC 的 Support。此功能適用於所有 GuardDuty 支援執行階段監視的區域。	2024年2月12日

執行階段監控中的更新功能-區域可用	GuardDuty 執行階段監控現在支援相同 AWS Organizations版本中的共用 Amazon VPC。GuardDuty 服務連結角色 (SLR) 具有新的權限，`organizations:DescribeOrganization` 可協助擷取共用 Amazon VPC 帳戶的組織 ID 以設定端點政策。如需在執行階段監控中使用共用 Amazon VPC 端點的先決條件的相關資訊，請參閱共用 Amazon VPC 的 Support。目前，此功能在某些. AWS 區域如需詳細資訊，請參閱區域與端點。	2024年2月9 日
支持新的更新功能 AWS 區域 - 惡意軟件防護	惡意程式碼防護現在支援掃描美國西部 (奧勒岡) 區域 AWS 受管金鑰 中加密的 EBS 磁碟區。	2024年2月6日

支持新的更新功能 AWS 區域 - 惡意軟件防護	惡意程式碼防護現在支援掃描以下內容加密 AWS 受管金鑰的 EBS 磁碟區：AWS 區域 • 亞太區域 (新加坡) (ap-southeast-1) • 歐洲 (法蘭克福) (eu-central-1) • 亞太區域 (大阪) (ap-northeast-3) • 美國東部 (俄亥俄) (us-east-2) • 歐洲 (米蘭) (eu-south-1) • 亞太區域 (東京) (ap-northeast-1) • 亞太區域 (首爾) (ap-northeast-2) • 加拿大 (中部) (ca-central-1) • 歐洲 (愛爾蘭) (eu-west-1) • 美國東部 (維吉尼亞北部) (us-east-1)	2024年2月5 日
運行時監視中的更新功能	GuardDuty 執行階段監控已發佈適用於 Amazon EC2 執行個體的新 GuardDuty 安全代理程式版本 (v1.0.2)。此代理程式版本包含對最新的 Amazon ECS AMI 的支援。如需代理程式發行歷史記錄的詳細資訊，請參閱 Amazon EC2 執行個體的 GuardDuty 安全性代理	2024年2月2日

支持新的更新功能 AWS 區域 - 惡意軟件防護	惡意程式碼防護現在支援掃描使用下列方式加密的 AWS 受管金鑰 Amazon EBS 磁碟區：AWS 區域 • 歐洲 (倫敦) (eu-west-2) • 歐洲 (斯德哥爾摩) (eu-north-1) • 亞太區域 (香港)ap-east-1 • 非洲 (開普敦)af-south-1 • 中東 (巴林) (me-south-1) • 亞太區域 (海德拉巴) (ap-south-2) • 歐洲 (西班牙) (eu-south-2) • 亞太區域 (墨爾本) (ap-southeast-4) • 亞太區域 (雪梨) (ap-southeast-2) • 以色列 (特拉維夫) (il-central-1)	2024 年 1 月 31 日
更新了管理帳戶 AWS Organizations	使 AWS Organizations用「管理帳戶」下重新組織內容。 ，新增了變更委派 GuardDuty 管理員帳戶的步驟，並更新了解系統管理員帳戶與成 GuardDuty 員帳戶之間的關係。	2024年1月30日

更新的功能與新的支持 AWS 區域	惡意程式碼防護現在支援掃描以下內容加密 AWS 受管金鑰的 EBS 磁碟區：AWS 區域 • 亞太區域 (雅加達) (ap-southeast-3) • 美國西部 (加利佛尼亞北部) (us-west-1) • 中東 (阿拉伯聯合大公國) (me-central-1) • 歐洲 (蘇黎世) (eu-central-2) • 亞太區域 (孟買)ap-south-1 • 南美洲 (聖保羅) (sa-east-1)	2024年1月29日
更新的惡意軟體防護功能	惡意軟體防護現在支援掃描使用 AWS 受管金鑰. 惡意程式碼防護服務連結角色 (SLR) 具有兩個新權限 — GetSnapshotBlock 和. ListSnapshotBlocks 這些權限將有助於從您的 EBS 卷（使用加密 AWS 受管金鑰） GuardDuty 獲取快照， AWS 帳戶 並在開始惡意軟件掃描之前將其複製到GuardDuty 服務帳戶。目前，此功能僅適用於歐洲（巴黎）（eu-west-3 ）。如需詳細資訊，請參閱惡意軟體掃描支援的磁碟區。	2024年1月25日

運行時監視中的更新功能	GuardDuty 執行階段監控已發佈新的 GuardDuty 安全代理程式版本 (v1.0.1)，其中包含一般效能調整和增強功能。如需代理程式發行歷史記錄的詳細資訊，請參閱 Amazon EC2 執行個體的GuardDuty 安全性代理	2024 年 1 月 23 日
運行時監視中的更新功能	運行時監控發布了針對 Amazon EKS 資源的新代理程序版本 1.4.1。如需詳細資訊，請參閱 EKS 附加元件代理程式發行歷史記錄。	2024年1月16日
運行時監控為 Amazon EKS 資源發布了新的代理 v1.4.0	運行時監控發布了適用於 Amazon EKS 資源的新代理程式版本 1.4.0。如需詳細資訊，請參閱 EKS 附加元件代理程式發行歷史記錄。	2023 年 12 月 21 日

在歐洲 (蘇黎世)、歐洲 (西班牙)、亞太區域 (海德拉巴)、亞太區域 (墨爾本) 和以色列 (特拉維夫) 新增 S3 和 AWS CloudTrail 機器學習 (ML) 發現項目類型	歐洲 (蘇黎世)、歐洲 (西班牙)、亞太區域 (海德拉巴)、亞太區域 (墨爾本) 和以色列 (特拉維夫) 區域現已提供下列 S3 和 CloudTrail 調查結果，使用異常偵測機器學習 (ML) 模型來識別異常行為： GuardDuty • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior • Exfiltration:IAMUser/AnomalousBehavior • Impact:IAMUser/AnomalousBehavior • CredentialAccess:IAMUser/AnomalousBehavior • DefenseEvasion:IAMUser/AnomalousBehavior • InitialAccess:IAMUser/AnomalousBehavior • Persistence:IAMUser/AnomalousBehavior • PrivilegeEscalation:IAMUser/AnomalousBehavior	2023 年 12 月 21 日

	• Discovery:IAMUser/AnomalousBehavior	
GuardDuty 通過支持 50,000 個會員帳戶 AWS Organizations	委派管理 GuardDuty 員現在最多可透過管理 50,000 個成員帳戶 AWS Organizations。這也包括最多 5000 個成員帳戶，這些帳戶通過邀請與 GuardDuty 管理員帳戶相關聯。	2023 年 12 月 20 日
GuardDuty 執行階段監控支援擴充至 19 AWS 區域	執行階段監控現已在亞太區域 (雅加達)、歐洲 (巴黎)、亞太區域 (大阪)、亞太區域 (首爾)、中東 (巴林)、歐洲 (西班牙)、亞太區域 (海德拉巴)、亞太區域 (墨爾本)、以色列 (特拉維夫)、美國西部 (加利佛尼亞北部)、歐洲 (倫敦)、亞太區域 (香港)、歐洲 (香港)、歐洲 (米蘭)、美國西部 (加利佛尼亞北部)、歐洲 (倫敦)、亞太區域 (香港)、歐洲 (香港)、歐洲 (米蘭)、美國西部 (加利佛尼亞北部) 亞太區域 (孟買)、加拿大 (中部)、非洲 (開普敦)、歐洲 (蘇黎世)。	2023 年 12 月 6 日
GuardDuty 擴展運行時監視功能	除了偵測 Amazon EKS 叢集的威脅外，還 GuardDuty 宣布正式推出執行時間監控以偵測 Amazon ECS 工作負載的威脅，以及預覽版本以偵測 Amazon EC2 執行個體的威脅。如需 AWS 區域 目前支援執行階段監控的詳細資訊，請參閱區域和端點。	2023 年 11 月 26 日

Amazon GuardDuty 已經更新了服務鏈接角色（SLR）	GuardDuty 已新增使用 Amazon ECS 動作來管理和擷取有關 Amazon ECS 叢集的資訊，以及使用管理 Amazon ECS 帳戶設定的新許可。`guarddutyActivate` 與 Amazon ECS 相關的動作也會擷取與相關聯標籤的相 GuardDuty關資訊。 • 下列權限已新增為 GuardDuty 擴充「執行階段監視」功能的一部分： `"ecs:ListClusters", "ecs:DescribeClusters", "ecs:PutAccountSettingDefault"`	2023 年 11 月 26 日
更新了受 AWS 管理的策略	GuardDuty 增加了新的權限，`organizations:ListAccounts` 到AmazonGuardDutyFullAccessPolicy和AmazonGuardDutyReadOnlyAccess。	2023 年 11 月 16 日

GuardDuty 發行使用 EKS 稽核記錄監視的新尋找項目類型。	EKS 稽核記錄監控現在支援亞太區域 (墨爾本) (`ap-southeast-4`) 的下列尋找類型。 • CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated • Execution:Kubernetes/AnomalousBehavior.ExecInPod • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount • Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated • Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	2023年11月11日

GuardDuty 發行使用 EKS 稽核記錄監視的新尋找項目類型。	EKS 稽核記錄監控現在支援亞太區域 (海德拉巴) ()、歐洲 (蘇黎世ap-south-2) () 和歐洲 (西班牙eu-central-2) (eu-south-2) 區域的下列尋找類型。 • CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated • Execution:Kubernetes/AnomalousBehavior.ExecInPod • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount • Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated • Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	2023 年 11 月 10 日

GuardDuty 發行使用 EKS 稽核記錄監視的新尋找項目類型。	EKS 稽核記錄監控現在支援下列尋找類型。亞太區域 (海德拉巴) ()、歐洲 (蘇黎世) (ap-south-2)、歐洲 (西班牙) (eu-central-2) 和亞太區域 (墨爾本) (eu-south-2) 等區域尚未提供這些搜尋結果類型。ap-southeast-4 • CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated • Execution:Kubernetes/AnomalousBehavior.ExecInPod • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount • Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	2023 年 11 月 8 日

	• Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	
EKS 執行期監控發佈了新的代理程式 v1.3.1	EKS 執行階段監控發行了新的代理程式 1.3.1 版，其中包含重要的安全性修補程式和更新。	2023 年 10 月 23 日
用於調查結果的新篩選條件屬性	GuardDuty 已新增條件來篩選產生的發現項目。DNS 要求網域尾碼會提供與提示 GuardDuty 產生發現項目之活動相關的第二個和最上層網域。	2023 年 10 月 17 日
EKS 執行期監控發佈了新的代理程式 v1.3.0，該版本支援 Kubernetes 版本 1.28	EKS 執行階段監控發佈新的代理程式版本 1.3.0，支援 Kubernetes 版本 1.28。新增對 Ubuntu 的支援。如需詳細資訊，請參閱 EKS 附加元件代理程式發行歷史記錄。	2023 年 10 月 5 日

新增以 S3 和 AWS CloudTrail 機器學習 (ML) 為基礎的發現項目類型至亞太區域 (雅加達) 和中東 (阿拉伯聯合大公國) 區域	亞太區域 (雅加達) 和中東 (阿拉伯聯合大公國) 區域現已提供以下 S3 和使用異常偵測機器學習 (ML) 模型識別異常行為的 CloudTrail 研究結果：GuardDuty • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior • Exfiltration:IAMUser/AnomalousBehavior • Impact:IAMUser/AnomalousBehavior • CredentialAccess:IAMUser/AnomalousBehavior • DefenseEvasion:IAMUser/AnomalousBehavior • InitialAccess:IAMUser/AnomalousBehavior • Persistence:IAMUser/AnomalousBehavior • PrivilegeEscalation:IAMUser/AnomalousBehavior • Discovery:IAMUser/AnomalousBehavior	2023 年 9 月 20 日

GuardDuty EKS 運行時監視引入了在集群級別管理 GuardDuty 安全代理	EKS 執行階段監視新增了管理個別 EKS 叢集的 GuardDuty 安全性代理程式的支援，以便僅從這些選擇性叢集監視執行階段事件。EKS 執行期監控擴展了此功能，現在支援標籤。	2023 年 9 月 13 日
GuardDuty 惡意軟體防護將支援擴展到更 AWS 區域	惡意軟體防護現已在亞太區域 (海德拉巴)、亞太區域 (墨爾本)、歐洲 (蘇黎世) 和歐洲 (西班牙) 區域提供。	2023 年 9 月 11 日
GuardDuty 以色列 (特拉維夫) 地區現已推出	將以色列（特拉維夫）區域添加到現在可用的 AWS 區域 列表中。 GuardDuty 下列保護計畫現已在以色列 (特拉維夫) 區域可用： • GuardDuty EKS 防護 包括 EKS 稽核日誌監控和 EKS 執行期監控。 • GuardDuty Lambda 護. • GuardDuty 惡意程式碼. • GuardDuty S3 保護. 如需有關以色列 (特拉維夫) 區域保護計畫可用性的詳細資訊，請參閱區域與端點。	2023 年 8 月 24 日
GuardDuty 在保護計劃級別為您的組織添加了自動啟用配置	更新您區域中保護計畫的組織組態。可能的組態選項包括為組織中的所有帳戶啟用、為組織中的新帳戶自動啟用，或不為組織中的任何帳戶自動啟用。	2023 年 8 月 16 日

使用 GuardDuty異常偵測機器學習 (ML) 模型識別異常行為的 S3 尋找類型現已在亞太區域 (大阪) 推出	下列調查結果類型現已在亞太區域 (大阪) 區域可用： • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior	2023 年 8 月 10 日
EKS 執行期監控現已在亞太區域 (墨爾本) 區域可用	EKS 防護中的 EKS 執行階段監控可 GuardDuty 為環境中的 Amazon EKS 叢集提供執行時期威脅偵測。 AWS 現已在亞太區域 (墨爾本) 區域可用。	2023 年 8 月 8 日
更新了調用 GuardDuty啟動惡意軟件掃描的 GuardDuty 發現項目列表	某些 EKS 執行階段監控尋找GuardDuty項目類型現在可以在您的. AWS 帳戶	2023 年 7 月 19 日
GuardDuty 通過支持 10,000 個會員帳戶 AWS Organizations	管理 GuardDuty 員帳戶現在可以通過管理最多 10,000 個成員帳戶 AWS Organizations。這也包括最多 5000 個成員帳戶，這些帳戶通過邀請與GuardDuty管理員帳戶相關聯。	2023 年 6 月 29 日

EKS 執行期監控推出三種新的調查結果類型。	EKS 執行期監控支援基於程序注入技術的三種新的調查結果類型。新的尋找項目類型為：執行階段/ DefenseEvasion.Proc、:執行階段 /.Ptrace，以及：執行階段/。ProcessInjection DefenseEvasion ProcessInjection DefenseEvasion ProcessInjection VirtualMemoryWrite。	2023 年 6 月 22 日
EKS 執行期監控發佈了新的代理程式 v1.2.0，該版本支援 Kubernetes 版本 1.27	EKS 運行時監控發布了一個新的代理程序版本 1.2.0，該版本還支持基於 ARM64 的實例。新增對 Bottlerocket 的支援。如需詳細資訊，請參閱 EKS 附加元件代理程式發行歷史記錄。	2023 年 6 月 16 日
GuardDuty 主控台提供您發現項目的摘要檢視。	GuardDuty 主控台中的摘要儀表板提供發 GuardDuty現項目的彙總檢視。目前，儀表板通過各種小部件顯示為您的帳戶生成的最近 10,000 個發現項目的數據（如果您是 GuardDuty 管理員帳戶，則為當前區域的成員帳戶）。	2023 年 6 月 12 日
EKS 稽核日誌監控現已在亞太區域 (海德拉巴)、亞太區域 (墨爾本)、歐洲 (蘇黎世) 和歐洲 (西班牙) 區域提供	為您的帳戶啟用 EKS 稽核日誌監控 (在 EKS 防護中)，以監控 Amazon EKS 叢集中的 EKS 稽核日誌，並對其進行分析是否有潛在惡意和可疑活動。	2023 年 6 月 1 日

EKS 稽核日誌監控現已在中東 (阿拉伯聯合大公國) 區域可用	EKS 稽核記錄監控現已在中東 (阿拉伯聯合大公國) 提供。為您的帳戶啟用 EKS 稽核日誌監控，以監控 Amazon EKS 叢集中的 EKS 稽核日誌，並對其進行分析是否有潛在的惡意和可疑活動。	2023 年 5 月 3 日
GuardDuty 惡意軟體防護宣佈依需求掃描	惡意軟體防護可協助您偵測連接至 Amazon EC2 執行個體和容器工作負載的 Amazon EBS 磁碟區中是否存在潛在的惡意軟體。它現在提供兩種類型的掃描- GuardDuty 啟動和按需掃描。 GuardDuty開始的惡意程式碼掃描只會在產生啟動的惡意程式碼掃描的其中一個發現項目時，才 GuardDuty 會在 Amazon EBS 磁碟區中自動啟動無代理程式掃描。GuardDuty您可以透過提供與 Amazon EC2 執行個體關聯的 Amazon Resource Name (ARN) 來對 Amazon EC2 執行個體啟動隨需惡意軟體掃描。如需有關兩種掃描類型差異的詳細資訊，請參閱惡意軟體防護。 • GuardDuty-發起的惡意軟件掃 • 隨需惡意軟體掃描	2023 年 4 月 27 日

GuardDuty 宣佈 Lambda 保護	Lambda 保護可協助您識別 AWS Lambda 函數中潛在的安全威脅。 • Lambda 保護調查結果類型 • 修復可能受損的 Lambda 函數	2023 年 4 月 20 日
GuardDuty 亞太區域 (墨爾本) 區域現已推出	將亞太區域（墨爾本）添加到可用 AWS 區域 GuardDuty 的列表中。如需有關此區域可用哪些功能的詳細資訊，請參閱區域與端點。	2023 年 4 月 19 日
GuardDuty 添加了 3 個新的 EC2 發現類型	GuardDuty 引入新的尋找類型，以偵測外部 DNS 解析器和加密 DNS 技術的使用情況。如需支援這些尋找項目類型之 AWS 區域 位置的相關資訊，請參閱區域和端點。 • DefenseEvasion:EC2/UnusualDNSResolver • DefenseEvasion:EC2/UnusualDoHActivity • DefenseEvasion:EC2/UnusualDoTActivity	2023 年 4 月 5 日

GuardDuty 宣布 EKS 保護中的 EKS 運行時監控	EKS 防護中的 EKS 執行階段監控可為環境中的 Amazon EKS 叢集提供執行時期威脅偵測。 AWS 這使用 Amazon EKS 附加元件代理程式 (`aws-guardduty-agent`)，從您的 EKS 工作負載收集執行期事件。 GuardDuty 收到這些執行階段事件後，它會監控並分析這些事件，以識別潛在的可疑安全威脅。如需詳細資訊，請參閱調查結果詳細資訊和 EKS 執行期監控調查結果類型。	2023 年 3 月 30 日
GuardDuty 增加了一個新的功能-`autoEnableOrganizationMembers`	Amazon 新 GuardDuty 增了一個新的組織組態選項，可協助 GuardDuty 管理員帳戶稽核和強制執行為ALL其組織成員啟用的 (必要時)。 GuardDuty 現在的最佳實務是使用 `autoEnableOrganizationMembers` 取代 `autoEnable` 。`autoEnable` 已棄用，但仍受支援。以下 API 受到此新功能的影響： • DescribeOrganizationConfiguration • UpdateOrganizationConfiguration • DisassociateMembers • DeleteMembers • DisassociateFromAdministratorAccount • StopMonitoringMembers	2023 年 3 月 23 日

Amazon 中的 RDS 保護功能現 GuardDuty 已正式推出	GuardDuty RDS 防護會監控和描述 RDS 登入活動，以識別 Amazon Aurora 資料庫執行個體上的可疑登入行為。如需有關支援 RDS 保護的 AWS 區域的相關資訊，請參閱區域與端點。	2023 年 3 月 16 日
GuardDuty 宣布功能啟動	過去， GuardDuty API 允許設定功能和資料來源，但現在，所有新的 GuardDuty 保護類型都會設定為功能，而不是資料來源。 GuardDuty 仍然支持通過 API 的數據源，但不會添加新的 API。功能啟用會影響用於啟用的 API GuardDuty 或其中的保護類型的行為 GuardDuty。如果您是透過 API、SDK 或 CFN 範本管理 GuardDuty 帳戶，請參閱 2023 年 3 月的 GuardDuty API 變更。	2023 年 3 月 16 日
GuardDuty 中東 (阿拉伯聯合大公國) 區域現已推出惡意軟體防護	中東 (阿拉伯聯合大 GuardDuty 公國) 區域支援中的惡意程式碼防護功能。如需詳細資訊，請參閱區域與端點。	2023 年 3 月 13 日

Amazon GuardDuty 已經更新了服務鏈接角色（SLR）	GuardDuty 添加了以下新權限以支持即將推出的 GuardDuty EKS 運行時監視功能。 • 使用 Amazon EKS 動作來管理和擷取有關 EKS 叢集的資訊，以及管理 EKS 叢集上的 EKS 附加元件。EKS 動作也會擷取與 GuardDuty關聯之標籤的相關資訊。 `"eks:ListClusters", "eks:DescribeCluster", "ec2:DescribeVpcEndpointServices", "ec2:DescribeSecurityGroups"`	2023 年 3 月 8 日
Amazon GuardDuty 已經更新了服務鏈接角色（SLR）	GuardDuty SLR 已更新，允許在啟用惡意程式碼防護之後建立惡意程式碼防護單反相機。	2023 年 2 月 21 日
GuardDuty 需要 TLS 版本 1.2 或更新版本	若要與 AWS 資源通訊，GuardDuty 需要並支援 TLS v1.2 或更新版本。如需詳細資訊，請參閱資料保護和基礎設施安全。	2023 年 2 月 14 日
GuardDuty 亞太區域 (海德拉巴) 區域現已推出	將亞太區域 (海得拉巴) 區域新增至可用 GuardDuty 的 AWS 區域 清單。如需詳細資訊，請參閱區域與端點。	2023 年 2 月 14 日
Amazon GuardDuty 使用者指南符合 IAM 最佳實務	更新了指南以符合 IAM 最佳實務。如需更多詳細資訊，請參閱 IAM 中的安全最佳實務。	2023 年 2 月 10 日

GuardDuty 歐洲 (西班牙) 區域現已推出	將歐洲（西班牙）添加到可用 AWS 區域 GuardDuty 的列表中。如需詳細資訊，請參閱區域與端點。	2023 年 2 月 8 日
GuardDuty 歐洲 (蘇黎世) 區域現已推出	將歐洲（蘇黎世）添加到可用 AWS 區域 GuardDuty 的列表中。如需詳細資訊，請參閱區域與端點。	2022 年 12 月 12 日
新功能的預覽版本 — GuardDuty RDS 保護	GuardDuty RDS 防護會監控和描述 RDS 登入活動，以識別 Amazon Aurora 資料庫執行個體上的可疑登入行為。目前在五個 AWS 區域提供預覽版。如需詳細資訊，請參閱區域與端點。	2022 年 11 月 30 日
GuardDuty 中東 (阿拉伯聯合大公國) 區域目前提供	將中東（阿聯酋）添加到可用 AWS 區域 位置 GuardDuty 的列表中。如需詳細資訊，請參閱區域與端點。	2022 年 10 月 6 日

新功能的新增內容 — GuardDuty 惡意軟體防護	GuardDuty 惡意軟體防護是 Amazon 的選擇性增強功能 GuardDuty。「惡意程式碼防護」會偵測可能是入侵來源的惡意程式碼，同時 GuardDuty 識別處於風險中的資源。啟用惡意程式碼保護後，每當在 Amazon EC2 執行個體或指示惡意軟體的容器工作負載上 GuardDuty 偵測到可疑行為時， GuardDuty 惡意軟體防護就會在連接到受影響 EC2 執行個體或容器工作負載的 EBS 磁碟區上啟動無代理程式掃描，以偵測是否存在惡意軟體。如需惡意程式碼防護如何運作及設定此功能的相關資訊，請參閱GuardDuty 惡意程式碼 • 如需有關惡意軟體防護調查結果的詳細資訊，請參閱調查結果詳細資訊。 • 如需修復受感染的 EC2 執行個體和獨立容器的相關資訊，請參閱補救由發現的安全問題。 GuardDuty • 如需有關惡意程式碼掃描的稽核 CloudWatch 記錄檔，以及在惡意程式碼掃描期間略過資源的原因的詳細資訊，請參閱瞭解 CloudWatch 記錄檔 • 如需偵測誤判安全威脅的相關資訊，請參閱在 GuardDuty 惡意程式碼防護中回報誤判。	2022 年 7 月 26 日

淘汰了一種調查結果類型	Exfiltration:S3/ObjectRead.Unusual 已淘汰。	2022 年 7 月 5 日
新增使用異常偵測機器學習 (ML) 模型識別異常行為 GuardDuty的 S3 尋找類型。	已新增下列新的 S3 調查結果類型。這些調查結果類型可識別 API 請求是否以異常方式調用 IAM 實體。ML 模型會評估帳戶中的所有 API 請求，並識別與對手使用的技術相關聯的異常事件。若要進一步了解這些新調查結果，請參閱 S3 調查結果類型。 • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior	2022 年 7 月 5 日
為以下項目新增 GuardDuty EKS 保護內容 GuardDuty	GuardDuty 現在可以透過監控 EKS 稽核日誌，為您的 Amazon EKS 資源產生發現結果。要了解如何配置此功能，請參閱 Amazon GuardDuty 中的 EKS 保護。如需 GuardDuty 可針對 Amazon EKS 資源產生的發現項目清單，請參閱 Kubernetes 發現項目。在 Kubernetes 調查結果修復指南中新增修復指引，以支援對調查結果的修正。	2022 年 1 月 25 日

新增了 1 個新調查結果	新增了新的調查結果 UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS。此發現項目會在 AWS 環境外的 AWS 帳戶存取您的執行個體認證時通知您。	2022 年 1 月 20 日
更新了調查結果類型，以協助識別與 log4j 相關的問題	Amazon GuardDuty 已經更新了以下發現類型，以幫助識別與 CVE-2021-44228 和 CVE-2021-45046 相關的問題並排定優先順序：後門：EC2 / C&C 活動。B; 後門：EC2 /C＆C 活動。 DNS; 行為:EC2/.NetworkPortUnusual	2021 年 12 月 22 日
調查結果變更	UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration 已變更為 UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS。此經改進的調查結果版本會了解通常使用憑證的位置，以減少透過內部部署網路路由傳送之流量的調查結果。UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	2021 年 9 月 7 日
GuardDuty 單鏡反光相機更新	GuardDuty 單鏡反光相機已經更新了新動作，以提高查找準確性。	2021 年 8 月 3 日
針對每個調查結果類型新增了資料來源資訊。	尋找描述現在包含 GuardDuty 用來產生該發現項目的資料來源的相關資訊。	2021 年 5 月 10 日

淘汰了 13 種調查結果類型。	13 項調查結果已退休，以新 AnomalousBehavoir 發現取代。 Persistence:IAMUser/NetworkPermissions、Persistence:IAMUser/ResourcePermissions、Persistence:IAMUser/UserPermissions、PrivilegeEscalation:IAMUser/AdministrativePermissions、Recon:IAMUser/NetworkPermissions、Recon:IAMUser/ResourcePermissions、Recon:IAMUser/UserPermissions、ResourceConsumption:IAMUser/ComputeResources、Stealth:IAMUser/LoggingConfigurationModified、Discovery:S3/BucketEnumeration.Unusual、Impact:S3/ObjectDelete.Unusual、Impact:S3/PermissionsModification.Unusual。	2021 年 3 月 12 日

為異常行為新增了 8 種新的調查結果類型。	根據 IAM 主體的異常行為，新增 8 種新的 IAMUser 調查結果類型。CredentialAccess:IAMUser/AnomalousBehavior、DefenseEvasion:IAMUser/AnomalousBehavior、Discovery:IAMUser/AnomalousBehavior、Exfiltration:IAMUser/AnomalousBehavior、Impact:IAMUser/AnomalousBehavior、InitialAccess:IAMUser/AnomalousBehavior、Persistence:IAMUser/AnomalousBehavior、PrivilegeEscalation:IAMUser/AnomalousBehavior。	2021 年 3 月 12 日
新增了根據網域評價的 EC2 調查結果。	新增 4 種根據網域評價的 Impact 調查結果類型。Impact:EC2/AbusedDomainRequest.Reputation、Impact:EC2/BitcoinDomainRequest.Reputation、Impact:EC2/MaliciousDomainRequest.Reputation。為 C&C 活動新增了一個新的 EC2 調查結果。Impact:EC2/SuspiciousDomainRequest.Reputation	2021 年 1 月 27 日

新增了 4 種新的調查結果類型。	新增了 3 個新的 S3 MaliciousIPCaller 調查結果。Discovery:S3/MaliciousIPCaller、Exfiltration:S3/MaliciousIPCaller、Impact:S3/MaliciousIPCaller。為 C&C 活動新增了一個新的 EC2 調查結果。Backdoor:EC2/C&CActivity.B	2020 年 12 月 21 日
淘汰了 UnauthorizedAccess:EC2/TorIPCaller 調查結果類型。	UnauthorizedAccess:EC2/TorIPCaller尋找項目類型現在已從中淘汰 GuardDuty。進一步了解。	2020 年 10 月 1 日
新增了 Impact:EC2/WinRmBruteForce 調查結果類型。	新增了新的 Impact 調查結果，Impact:EC2/WinRmBruteForce。進一步了解。	2020 年 9 月 17 日
新增了 Impact:EC2/PortSweep 調查結果類型。	新增了新的 Impact 調查結果，Impact:EC2/PortSweep。進一步了解。	2020 年 9 月 17 日
GuardDuty 現已在非洲 (開普敦) 和歐洲 (米蘭) 地區推出。	將非洲（開普敦）和歐洲（米蘭）添加到可用的 AWS 地區列表中。 GuardDuty 進一步了解	2020 年 7 月 31 日
新增監控 GuardDuty 成本的新使用詳細資料。	您現在可以使用新的指標來查詢 GuardDuty 帳戶和所管理帳戶的使用成本資料。主控台提供有關使用費的全新概觀，網址為：https://console.aws.amazon.com/guardduty/。更詳細的資訊可以通過 API 存取。	2020 年 7 月 31 日

透過中 GuardDuty的 S3 資料事件監控新增涵蓋 S3 保護的內容	GuardDuty S3 保護現在可透過將 S3 資料平面事件作為新的資料來源進行監控。新帳戶將自動啟用此功能。如果您已經在使用，則 GuardDuty 可以為自己或您的成員帳戶啟用新的資料來源。	2020 年 7 月 31 日
新增了 14 個新的 S3 調查結果。	已為 S3 控制平面和資料平面來源新增了 14 個新的 S3 調查結果類型。	2020 年 7 月 31 日
新增了對 S3 調查結果的額外支援，並變更了 2 個現有的調查結果類型名稱。	GuardDuty 發現現在包含涉及 S3 儲存貯體的發現項目的更多詳細 與 S3 活動相關的現有調查結果類型已重新命名：Policy:IAMUser/S3BlockPublicAccessDisabled 已變更為 Policy:S3/BucketBlockPublicAccessDisabled。Stealth:IAMUser/S3ServerAccessLoggingDisabled 已變更為 Stealth:S3/ServerAccessLoggingDisabled。	2020 年 5 月 28 日
新增內容以進行 AWS Organizations 整合。	GuardDuty 現在可與 AWS Organizations 委派的系統管理員整合，讓您管理組織內的 GuardDuty 帳戶。當您將委派管理員設定為管理 GuardDuty 員帳戶時，您可以自動啟 GuardDuty 用讓任何組織成員由委派的管理員帳戶管理。您也可以 GuardDuty 在新 AWS Organizations 成員帳戶中自動啟用。進一步了解。	2020 年 4 月 20 日

新增了匯出調查結果功能的內容。	已新增描述的「匯出發現項目」功能的內容 GuardDuty。	2019 年 11 月 14 日
新增了 UnauthorizedAccess:EC2/MetadataDNSRebind 調查結果類型。	新增了新的 Unauthorized 調查結果，UnauthorizedAccess:EC2/MetadataDNSRebind。進一步了解。	2019 年 10 月 10 日
新增了 Stealth:IAMUser/S3ServerAccessLoggingDisabled 調查結果類型。	新增了一個新的 Stealth 調查結果，Stealth:IAMUser/S3ServerAccessLoggingDisabled。進一步了解。	2019 年 10 月 10 日
新增了 Policy:IAMUser/S3BlockPublicAccessDisabled 調查結果類型。	新增了 Policy 調查結果，Policy:IAMUser/S3BlockPublicAccessDisabled。進一步了解。	2019 年 10 月 10 日
淘汰了 Backdoor:EC2/XORDDOS 調查結果類型。	Backdoor:EC2/XORDDOS尋找項目類型現在已從中淘汰 GuardDuty。 了解更多	2019 年 6 月 12 日
新增了 PrivilegeEscalation 調查結果類型。	PrivilegeEscalation 調查結果類型偵測使用者何時嘗試將更高、更寬鬆的許可指派給他們的帳戶。進一步了解	2019 年 5 月 14 日
GuardDuty 歐洲 (斯德哥爾摩) 區域現已推出。	將歐洲 (斯德哥爾摩) 新增至可用 AWS GuardDuty 區域清單。進一步了解	2019 年 5 月 9 日
新增了新的調查結果類型，Recon:EC2/PortProbeEMRUnprotectedPort。	此調查結果通知您，EC2 執行個體上 EMR 相關的敏感連接埠未封鎖，正被積極探測中。進一步了解	2019 年 5 月 8 日

新增了 5 種新的調查結果類型，其偵測您的 EC2 執行個體是否可能正被用於阻斷服務 (DoS) 攻擊。	這些調查結果通知您，EC2 執行個體在環境中的表現方式可能表示它們被用於執行阻斷服務 (DoS) 攻擊。進一步了解	2019 年 3 月 8 日
新增了調查結果類型：Policy:IAMUser/RootCredentialUsage	Policy:IAMUser/RootCredentialUsage查找類型會通知您您的根用戶登錄憑據 AWS 帳戶正在用於向服務發出程序化請求。 AWS 進一步了解	2019 年 1 月 24 日
UnauthorizedAccess:IAMUser/UnusualASNCaller 調查結果類型已淘汰	UnauthorizedAccess:IAMUser/UnusualASNCaller 調查結果類型已淘汰。您現在會收到有關透過其他使用中尋 GuardDuty 找類型從異常網路叫用的活動的通知。產生的調查結果類型將以從異常網路調用的 API 類型為基礎。進一步了解	2018 年 12 月 21 日
新增了兩種新的調查結果類型：PenTest:IAMUser/ParrotLinux 和 PenTest:IAMUser/PentooLinux	PenTest:IAMUser/ParrotLinux 調查結果類型會通知您，執行 Parrot Security Linux 的電腦正在使用屬於您的 AWS 帳戶的憑證進行 API 呼叫。PenTest:IAMUser/PentooLinux 調查結果類型通知您，執行 PentooLinux 的電腦正在使用屬於您 AWS 帳戶的憑證進行 API 呼叫。進一步了解	2018 年 12 月 21 日

增加了對 Amazon 公 GuardDuty 告 SNS 主題的支持	您現在可以訂閱通 GuardDuty 告 SNS 主題，以接收有關新發行之尋找項目類型、現有發現項目類型的更新以及其他功能變更的通知。所有 Amazon SNS 所支援格式的通知。進一步了解	2018 年 11 月 21 日
新增了兩種新的調查結果類型：UnauthorizedAccess:EC2 /TorClient 和 Unauthori zedAccess:EC2/TorRelay	UnauthorizedAccess:EC2/ TorClient尋找類型會通知您 AWS 環境中的 EC2 執行個體正在連線到 Tor Guard 或授權節點。 UnauthorizedAccess :EC2/TorRelay查找類型會通知您 AWS 環境中的 EC2 實例正在以一種方式與 Tor 網絡進行連接，表明它充當 Tor 中繼。進一步了解	2018 年 11 月 16 日
新增了調查結果類型：CryptoCurrency:EC2/Bitcoin Tool.B	此發現項目會通知您 AWS 環境中的 EC2 執行個體正在查詢與 Bitcoin 相關的網域名稱，或其他與加密貨幣相關的活動。進一步了解	2018 年 11 月 9 日
增加了對更新發送到 CloudWatch 事件的通知頻率的支持	您現在可以更新傳送至「 CloudWatch 事件」的通知頻率，以供後續發現的現有發現項目發生時使用。可能的值有 15 分鐘、1 小時或預設的 6 小時。進一步了解	2018 年 10 月 9 日
新增了區域支援	新增地區支援 AWS GovCloud (美國西部) 深入瞭解	2018 年 7 月 25 日

增加了對 AWS CloudFormation StackSets 中的支持 GuardDuty	您可以使用啟用 Amazon GuardDuty 範本在多個帳戶中 GuardDuty 同時啟用。進一步了解	2018 年 6 月 25 日
增加了對 GuardDuty 自動存檔規則的支持	客戶現在可以建置更精細的自動封存規則，以進行問題清單隱藏。對於符合自動封存規則的發現項目， GuardDuty 會自動將其標示為已封存。這可讓客戶進一步調整 GuardDuty ，只在目前的發現項目表格中保留相關的發現項目。進一步了解	2018 年 5 月 4 日
GuardDuty 適用於歐洲 (巴黎) 地區	GuardDuty 歐洲 (巴黎) 現已推出，讓您能夠在此區域擴展持續的安全監控和威脅偵測。進一步了解	2018 年 3 月 29 日
現在支持通過 AWS CloudFormation 創建 GuardDuty 管理員帳戶和成員帳戶。	如需詳細資訊，請參閱 `AWS::GuardDuty::master` 及 `AWS::GuardDuty::member` 。	2018 年 3 月 6 日
新增九個 CloudTrail基於異常偵測的新功能。	這些新的搜尋結果類型會在所有支援的「區域」 GuardDuty 中自動啟用。 進一步了解	2018 年 2 月 28 日
新增了三項新的威脅智慧偵測 (調查結果類型)。	這些新的搜尋結果類型會在所有支援的「區域」 GuardDuty 中自動啟用。進一步了解	2018 年 2 月 5 日
GuardDuty 會員帳戶的上限增加。	在此版本中，每個帳戶最多可以添加 1000 個 GuardDuty 成員帳 AWS 戶（ GuardDuty 管理員帳戶帳戶）。進一步了解	2018 年 1 月 25 日

管理員帳戶和成員帳戶的受信任 IP 清單和威脅清單的上傳和進一步 GuardDuty 管理變更。	在此版本中，來自管理員 GuardDuty 帳戶的使用者可以上傳和管理受信任的 IP 清單和威脅清單。來自會員 GuardDuty 帳戶的用戶無法上傳和管理列表。由管理員帳戶帳戶上傳的受信任 IP 清單和威脅清單會強加在其成員帳戶中的 GuardDuty 功能上。進一步了解	2018 年 1 月 25 日

舊版更新

變更	描述	日期
初次出版	Amazon GuardDuty 用戶指南的初始發布。	2017 年 11 月 28 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。