使用者指南

Amazon Inspector

Amazon Inspector: 使用者指南

Table of Contents

什麼是 Amazon Inspector？

Amazon Inspector 是一種弱點管理服務，可持續掃描您的 AWS 工作負載，找出軟體弱點和意外的網路暴露。Amazon Inspector 會自動探索和掃描執行中的 Amazon EC2 執行個體、Amazon Elastic Container Registry (Amazon ECR) 中的容器映像，以及針對已知軟體漏洞和意外網路暴露的 AWS Lambda 功能。

當 Amazon Inspector 發現軟體弱點或網路組態問題時，就會建立一個發現。發現項目會描述弱點、識別受影響的資源、評估弱點的嚴重性，並提供修正指引。您可以使用 Amazon Inspector 主控台分析發現項目，或透過其他主控台檢視和處理您的發現項目 AWS 服務。如需詳細資訊，請參閱 了解 Amazon Inspector 中的發現。

主題

Amazon Inspector 的功能

集中管理多個 Amazon Inspector 帳戶

如果您的 AWS 環境有多個帳戶，您可以使用 Organ AWS izations 透過單一帳戶集中管理您的環境。使用此方法，您可以將帳戶指定為 Amazon Inspector 的委派管理員帳戶。

只需單擊一下，即可為整個組織激活 Amazon Inspector。此外，您可以在 future 的成員加入組織時自動啟用服務。Amazon Inspector 委派的管理員帳戶可以管理組織成員的發現項目資料和特定設定。這包括檢視所有成員帳號的彙總發現項目詳細資料、啟用或停用成員帳號的掃描，以及檢閱 AWS 組織內已掃描的資源。

持續掃描環境中的弱點和網路暴露

使用 Amazon Inspector，您不需要手動排程或設定評估掃描。Amazon Inspector 會自動探索並開始掃描您符合資格的資源。Amazon Inspector 會自動重新掃描資源以回應可能導致新弱點的變更，例如：在 EC2 執行個體中安裝新套件、安裝修補程式，以及發佈影響資源的新常見漏洞和曝光 (CVE)，藉此持續評估您的環境。與傳統的安全掃描軟體不同，Amazon Inspector 對叢集效能的影響最小。

當發現漏洞或開放的網路路徑時，Amazon Inspector 會產生一個您可以調查的發現項目。此發現項目包含有關弱點、受影響資源和修復建議的完整詳細資訊。如果您適當地修復發現項目，Amazon Inspector 會自動偵測修復並關閉發現項目。

使用 Amazon Inspector 風險評分準確評估漏洞

當 Amazon Inspector 透過掃描收集有關您環境的資訊時，它會提供專為您的環境量身打造的嚴重性分數。Amazon Inspector 會檢查構成國家弱點資料庫 (NVD) 基本分數的安全指標是否存在弱點，並根據您的運算環境進行調整。例如，如果該弱點可透過網路遭到利用，但執行個體沒有開放網路路徑可用，則該服務可能會降低 Amazon EC2 執行個體發現項目的 Amazon Inspector 分數。此分數採用 CVSS 格式，且會修改 NVD 提供的基本通用弱點評分系統 (CVSS) 分數。

使用 Amazon Inspector 儀表板識別高影響力的發現

Amazon Inspector 儀表板可提供您環境中各個發現項目的高階檢視。從儀表板中，您可以存取發現項目的精細詳細資料。儀表板包含有關您環境中掃描涵蓋範圍、最重要的發現項目，以及哪些資源的發現項目最多的簡化資訊。Amazon Inspector 儀表板中的風險型修復面板會顯示影響最多執行個體和映像數量的發現結果。此面板可讓您更輕鬆地識別對環境造成最大影響的發現項目、檢閱尋找詳細資料，以及檢閱建議的解決方案。

使用可自訂的檢視來管理發現

除了儀表板之外，Amazon Inspector 主控台還提供「發現項目」檢視。此頁面會列出您環境的所有發現項目，並提供個別發現項目的詳細資訊。您可以檢視依類別或弱點類型分組的發現項目。在每個檢視中，您都可以使用篩選條件進一步自訂結果。您也可以使用篩選器來建立隱藏不需要的發現項目的隱藏規則。

您可以使用篩選條件與隱藏規則來產生搜尋結果報告，以顯示所有發現項目或自訂的發現項目選項。您可以使用 CSV 或 JSON 格式產生報告。

監控和處理與其他服務和系統的發現

為了支援與其他服務和系統的整合，Amazon Inspector 會將調查結果發佈給 Amazon EventBridge 作為尋找事件。 EventBridge 是一種無伺服器事件匯流排服務，可將發現項目資料路由到 AWS Lambda 功能和 Amazon Simple Notification Service (Amazon SNS) 主題等目標。有了 EventBridge，您可以近乎即時地監控和處理發現項目，作為現有安全性和合規性工作流程的一部分。

如果您已啟用 AWS Security Hub，則 Amazon Inspector 也會將調查結果發佈到 Security Hub。Security Hub 是一項服務，可提供您 AWS 環境中安全性狀態的全面檢視，並協助您根據安全性產業標準和最佳做法來檢查環境。使用 Security Hub，您可以更輕鬆地監視和處理發現項目，作為對組織中的安全性狀態進行更廣泛分析的一部分 AWS。

訪問 Amazon Inspector

Amazon Inspector 是在大多數可用 AWS 區域. 如需目前提供 Amazon Inspector 的區域清單，請參閱亞馬遜網路服務一般參考中的 Amazon Inspector 端點和配額。若要進一步了解 AWS 區域，請參閱 Amazon Web Services 一般參考 AWS 區域中的管理。在每個區域中，您可以透過下列方式使用 Amazon Inspector。

AWS 管理主控台

這 AWS Management Console 是一個基於瀏覽器的介面，您可以使用它來建立和管理 AWS 資源。作為該主控台的一部分，Amazon Inspector 主控台可讓您存取 Amazon Inspector 帳戶和資源。您可以從 Amazon Inspector 控制台執行 Amazon Inspector 任務。

AWS 命令行工具

使用 AWS 命令列工具，您可以在系統的命令列發出命令以執行 Amazon Inspector 任務。使用命令行可以比使用控制台更快，更方便。若您想要建構執行 任務的指令碼，命令列工具也非常實用。

AWS 提供兩組指令行工具： AWS Command Line Interface (AWS CLI) 和 AWS Tools for PowerShell. 若要取得有關安裝和使用的資訊 AWS CLI，請參閱《指AWS 令行介面使用者指南》。若要取得有關安裝和使用的「工具」的資訊 PowerShell，請參閱《使AWS Tools for PowerShell 用指南》。

AWS 開發套件

AWS 提供包含程式庫和範例程式碼的開發套件，適用於各種程式設計語言和平台，包括 Java、Go、Python、C++ 和 .NET。開發套件提供方便、程式化的 Amazon Inspector 和其他存取。AWS 服務他們還處理諸如密碼編譯簽名請求，管理錯誤以及自動重試請求等任務。如需有關安裝和使用 AWS SDK 的詳細資訊，請參閱建置在其上 AWS的工具。

Amazon Inspector 休息 API

Amazon Inspector REST API 可讓您以程式設計方式全面地存取您的 Amazon Inspector 帳戶和資源。使用此 API，您可以將 HTTPS 請求直接傳送至 Amazon Inspector。但是，與 AWS 命令行工具和 SDK 不同，使用此 API 需要您的應用程序處理低級別的詳細信息，例如生成散列以簽署請求。

開始使用 Amazon Inspector

本教學提供 Amazon Inspector 的實際操作簡介。

步驟 1 涵蓋在多帳戶環境中啟用獨立帳戶的 Amazon Inspector 掃描，或以 Amazon Inspector 委派 AWS Organizations 的管理員身分啟用。

步驟 2 涵蓋了解主控台中的 Amazon Inspector 發現項目。

> **Note**
>
> 在本自學課程中，您將完成目前的工作 AWS 區域。若要在其他區域設定 Amazon Inspector，您必須在這些區域中完成這些步驟。

主題

開始之前

Amazon Inspector 是一種弱點管理服務，可持續掃描您的 Amazon EC2 執行個體、Amazon ECR 容器映像，以及軟體弱點和意外網路暴露的 AWS Lambda 功能。

啟動 Amazon Inspector 之前，請注意以下事項：

- Amazon Inspector 是一項區域服務，而資料會儲存 AWS 區域 在您使用該服務的位置。您在本教學中完成的任何組態程序都必須在您要使用 Amazon Inspector 監控 AWS 區域 的每個設定程序中重複執行。
- Amazon Inspector 器為您提供啟動 Amazon EC2 執行個體、亞馬遜 ECR 容器映像和 AWS Lambda 功能掃描的靈活性。您可以從 Amazon Inspector 主控台的帳戶管理頁面或使用 Amazon Inspector API 來管理掃描類型。
- 只有在已安裝並啟動 Amazon EC2 系統管理員 (SSM) 代理程式後，Amazon Inspector 才能為您的 EC2 執行個體提供常見漏洞和入侵 (CVE) 資料。此代理程式已預先安裝在許多 EC2 執行個體上，但您可能需要手動啟用它。無論 SSM 代理程式狀態為何，都會掃描所有 EC2 執行個體是否有網路

暴露問題。如需設定 Amazon EC2 掃描的詳細資訊，請參閱掃描 Amazon EC2 實例。Amazon ECR 和 AWS Lambda 功能掃描不需要使用代理程式。

- 具有管理員許可的 IAM 使用者身分 AWS 帳戶 可以啟用 Amazon Inspector。基於資料保護目的，我們建議您保護您的登入資料，並使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 設定個別使用者。如此一來，每個使用者都只會獲得管理 Amazon Inspector 所需的許可。如需啟用 Amazon Inspector 查器所需許可的相關資訊，請參閱AWS 受管理的策略：AmazonInspector2FullAccess。
- 當您第一次在任何區域啟用 Amazon Inspector 時，它會在全球為您呼叫`AWSServiceRoleForAmazonInspector2`的帳戶建立服務連結角色。此角色包括許可和信任政策，可讓 Amazon Inspector 收集軟體套件詳細資料並分析 Amazon VPC 組態，以產生漏洞發現的結果。如需詳細資訊，請參閱 使用 Amazon Inspector 的服務連結角色。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。

第 1 步：激活 Amazon Inspector

使用 Amazon Inspector 的第一步是激活它為您的 AWS 帳戶. 啟用任何 Amazon Inspector 掃描類型後，Amazon Inspector 會立即開始探索並掃描所有符合資格的資源。

如果您想要透過集中式管理員帳戶管理組織內多個帳戶的 Amazon Inspector，則必須為 Amazon Inspector 指派委派管理員。選擇下列其中一個選項，以了解如何為您的環境啟用 Amazon Inspector。

Standalone account environment

1. 在 https://console.aws.amazon.com/inspector/v2/home 打開 Amazon Inspector 控制台。
2. 選擇開始使用。
3. 選擇激活 Amazon Inspector.

當您在獨立帳戶中啟用 Amazon Inspector 時，預設會啟用所有掃描類型。您可以從 Amazon Inspector 主控台內的帳戶管理頁面或使用 Amazon Inspector API 來管理已啟動的掃描類型。啟用 Amazon Inspector 之後，它會自動探索並開始掃描所有符合資格的資源。檢閱下列掃描類型資訊，以瞭解哪些資源預設符合資格：

Amazon EC2 掃描

為了提供 EC2 執行個體的常見弱點和入侵 (CVE) 資料，Amazon Inspector 要求安裝並啟用 AWS Systems Manager (SSM) 代理程式。此代理程式已預先安裝在許多 EC2 執行個體上，但您可能需要手動啟用它。無論 SSM 代理程式狀態為何，都會掃描所有 EC2 執行個體是否有網

路暴露問題。如需設定 Amazon EC2 掃描的詳細資訊，請參閱用亞馬遜檢查器掃描亞馬遜 EC2 實例。

Amazon ECR 掃描

當您啟用 Amazon ECR 掃描時，Amazon Inspector 會將私有登錄中針對 Amazon ECR 提供的預設基本掃描設定的所有容器儲存庫轉換為持續掃描的增強型掃描。您也可以選擇將此設定設定為僅在推送時掃描，或透過包含規則掃描選取的儲存庫。過去 30 天內推送的所有影像都排定為終身掃描，此 Amazon ECR 掃描設定可隨時變更。如需設定 Amazon ECR 掃描的詳細資訊，請參閱使用 Amazon 檢查器掃描亞馬遜 ECR 容器映像。

AWS Lambda 功能掃描

當您啟用 AWS Lambda 函數掃描時，Amazon Inspector 會探索您帳戶中的 Lambda 函數，並立即開始掃描它們是否有漏洞。Amazon Inspector 會在部署新的 Lambda 函數和層時進行掃描，並在更新或發佈新的常見弱點和曝光 (CVE) 時重新掃描這些函數和層。Amazon Inspector 提供兩種不同級別的 Lambda 函數掃描。根據預設，當您第一次啟用 Amazon Inspector 時，Lambda 標準掃描會啟動，以掃描函數中的套件相依性。您可以另外啟用 Lambda 程式碼掃描，掃描函數中的開發人員程式碼是否存在程式碼弱點。如需設定 Lambda 函數掃描的詳細資訊，請參閱Amazon Inspector 掃描 AWS Lambda 功能。

Multi-account environment

> **Important**
>
> 若要完成這些步驟，您必須與要管理的所有帳戶位於同一個組織中，並且可以存取 AWS Organizations 管理帳戶，才能在組織內委派 Amazon Inspector 的管理員。可能需要其他權限才能委派管理員。如需詳細資訊，請參閱 指定委派管理員所需的許可。
>
> > **Note**
> >
> > 要以編程方式為多個區域中的多個帳戶啟用 Amazon Inspector，您可以使用 Amazon Inspector 開發的 shell 腳本。如需有關使用此指令碼的詳細資訊，請參閱檢查器 2-enablement-with-cli 上的。 GitHub

委派 Amazon Inspector 員的管理員

1. 登入 AWS Organizations 管理帳戶。

2. 在 https://console.aws.amazon.com/inspector/v2/home 打開 Amazon Inspector 控制台。
3. 在「委派管理員」窗格中，輸入您要指定為組織之 Amazon Inspector 委派管理員的十二位數 ID。 AWS 帳戶 然後選擇「委派」。然後，在確認視窗中，再次選擇「委派」。

> **Note**
>
> 當您委派管理員時，系統會為您的帳戶啟用 Amazon Inspector。

新增會員帳戶

身為委派管理員，您可以針對與 Organizations 管理帳戶相關聯的任何成員啟動掃描。此工作流程會啟動所有成員帳戶的所有掃描類型。不過，成員也可以為自己的帳戶啟用 Amazon Inspector，或者委派的管理員可以選擇性地啟動服務掃描。如需詳細資訊，請參閱 管理多個 帳戶。

1. 登入委派的系統管理員帳戶。
2. 在 https://console.aws.amazon.com/inspector/v2/home 打開 Amazon Inspector 控制台。
3. 在功能窗格中，選擇 [帳戶管理]。「帳戶」表格會顯示與「Organizations」管理帳戶相關聯的所有成員帳戶。
4. 在 [帳戶管理] 頁面中，您可以從頂端橫幅選擇 [啟動所有帳戶的掃描]，以啟用 EC2 執行個體、ECR 容器映像，以及組織中所有帳戶的 AWS Lambda 功能掃描。或者，您可以在「帳戶」表中選取要新增為成員的帳戶，以選擇這些帳戶。然後從「啟用」功能表中選取「所有掃描」。
5. (選擇性) 開啟自動啟用新成員帳戶的 Inspector 功能，然後選取要包含的掃描類型，以針對新增至組織的任何新成員帳戶啟動這些掃描。

Amazon Inspector 器目前提供 EC2 執行個體、ECR 容器映像和 AWS Lambda 功能的掃描。啟用 Amazon Inspector 之後，它會自動開始探索和掃描所有符合資格的資源。檢閱下列掃描類型資訊，以瞭解哪些資源預設符合資格：

Amazon EC2 掃描

為了提供 EC2 執行個體的 CVE 弱點資料，Amazon Inspector 要求安裝並啟用 AWS Systems Manager (SSM) 代理程式。此代理程式已預先安裝在許多 EC2 執行個體上，但您可能需要手動啟用它。無論 SSM 代理程式狀態為何，都會掃描所有 EC2 執行個體是否有網路暴露問題。如需設定 Amazon EC2 掃描的詳細資訊，請參閱用亞馬遜檢查器掃描亞馬遜 EC2 實例。

Amazon ECR 掃描

當您啟用 Amazon ECR 掃描時，Amazon Inspector 會將私有登錄中針對 Amazon ECR 提供的預設基本掃描設定的所有容器儲存庫轉換為使用持續掃描的增強型掃描。您也可以選擇將此設定設定為僅在推送時掃描，或透過包含規則掃描選取的儲存庫。過去 30 天內推送的所有影像都會排程進行終身掃描。委派的管理員可以隨時變更此 Amazon ECR 掃描設定。如需設定 Amazon ECR 掃描的詳細資訊，請參閱使用 Amazon 檢查器掃描亞馬遜 ECR 容器映像。

AWS Lambda 功能掃描

當您啟用 AWS Lambda 函數掃描時，Amazon Inspector 會探索您帳戶中的 Lambda 函數，並立即開始掃描它們是否有漏洞。Amazon Inspector 會在部署新的 Lambda 函數和層時進行掃描，並在更新或發佈新的常見弱點和曝光 (CVE) 時重新掃描這些函數和層。如需設定 Lambda 函數掃描的詳細資訊，請參閱Amazon Inspector 掃描 AWS Lambda 功能。

步驟 2：查看 Amazon Inspector 發現

您可以在 Amazon Inspector 主控台或透過 API 檢視環境的發現結果。所有發現也被推送到 Amazon EventBridge 和 AWS Security Hub （如果激活）。此外，容器映像發現的結果也會推送至 Amazon ECR。

Amazon Inspector 主控台為您的發現項目提供數種不同的檢視格式。Amazon Inspector 儀表板為您提供環境風險的高階概觀，而「發現項目」表則可讓您檢視特定發現項目的詳細資訊。

在此步驟中，您可以使用「發現項目」表格與「發現項目」儀表板來探索發現項目的詳細 如需 Amazon Inspector 儀表板的相關資訊，請參閱了解儀表板。

若要在 Amazon Inspector 主控台中檢視您環境的發現項目詳細資訊：

1. 在 https://console.aws.amazon.com/inspector/v2/home 打開 Amazon Inspector 控制台。
2. 在導覽窗格中，選取 [儀表板]。您可以選取儀表板中的任何連結，以瀏覽 Amazon Inspector 主控台中的某個頁面，其中包含有關該項目的詳細資訊。
3. 從導覽窗格中，選取「發現項目」。
4. 預設情況下，您會看到 [所有發現項目] 索引標籤，其中顯示所有 EC2 執行個體、ECR 容器映像、您環境的 AWS Lambda 函數發現項目。
5. 在「發現項目」清單中，選擇「標題」欄位中的搜尋結果名稱，以開啟該發現項目的明細窗格。所有發現項目都有「搜尋結果詳細資訊 您可以透過下列方式與「尋找項目詳細資料」標籤互動：

   - 如需有關此弱點的詳細資訊，請按照弱點詳細資訊一節中的連結，開啟此資訊安全風險的文件。

- 若要進一步調查您的資源，請按照 [資源受影響] 區段中的 [資源 ID] 連結，開啟受影響資源的服務主控台。

P@@ ackage 弱點類型發現項目還具有 In spector 分數和弱點情報索引標籤，說明如何計算該發現項目的 Amazon Inspector 分數，並提供與發現項目相關聯的常見弱點和漏洞攻擊 (CVE) 的資訊。如需尋找類型的詳細資訊，請參閱在 Amazon Inspector 中查找類型。

了解 Amazon Inspector 儀表板

Amazon Inspector 儀表板提供目前 AWS 區域中資 AWS 源彙總統計資料的快照。這些統計資料包括資源涵蓋範圍和主動弱點的關鍵指標。儀表板也會顯示您帳戶的彙總發現資料群組，例如 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體、Amazon Elastic Container Registry (Amazon ECR)，以及具有最重要發現項目的 AWS Lambda 功能。若要執行更深入的分析，您可以檢視儀表板項目的支援資料。

如果您的帳戶是組織的 Amazon Inspector 委派管理員帳戶，則儀表板會包含組織中所有帳戶 (包括您自己的帳戶) 的帳戶涵蓋範圍、彙總統計資料和發現項目資料。

顯示儀表板

儀表板會顯示環境涵蓋範圍和重要發現項目的概觀。

若要顯示管控面板：

1. 打開 Amazon Inspector 控制台 https://console.aws.amazon.com/inspector/v2/home。
2. 在導覽窗格中，選擇 Dashboard (儀表板)。
3. 您可以透過下列方式與儀表板互動：

   - 儀表板會每五分鐘自動重新整理一次。不過，您可以選取頁面右上角的重新整理圖示來手動重新整理資料。
   - 若要在儀表板上檢視項目的支援資料，請選擇該項目。
   - 如果您以 Amazon Inspector 委派的管理員身分透過 AWS 組織管理多個帳戶，儀表板會顯示成員帳戶的彙總統計資料。若要篩選儀表板並僅顯示特定帳戶的資料，請在 [帳戶] 方塊中輸入帳號 ID。

瞭解儀表板元件和解譯資料

Amazon Inspector 儀表板的每個區段都提供關鍵指標或使用中發現項目資料的深入解析，協助您瞭解目前 AWS 資源的弱點狀態 AWS 區域。

環境覆蓋

「環境涵蓋範圍」區段提供 Amazon Inspector 掃描資源的相關統計資料。在本節中，您可以看到 Amazon Amazon Inspector 查器掃描的 Amazon EC2 實例，亞馬遜 ECR 映像和 AWS Lambda 功

能的計數和百分比。如果您以 Amazon Inspector 委派的 AWS Organizations 管理員身分管理多個帳戶，您也會看到組織帳戶總數、啟用 Amazon Inspector 的數量，以及組織產生的涵蓋範圍百分比。您也可以使用本節來判斷哪些資源未涵蓋 Amazon Inspector。這些資源可能包含可能被利用來使您的組織面臨風險的漏洞。如需詳細資訊，請參閱評估您 AWS 環境的 Amazon Inspector 覆蓋率。

選擇涵蓋範圍群組會帶您前往所選群組的「帳戶管理」頁面。帳戶管理頁面會顯示 Amazon Amazon Inspector spector 涵蓋哪些帳戶、Amazon EC2 執行個體和 Amazon ECR 儲存庫的詳細資訊。

以下是可用的承保群組：

- 帳戶
- 執行個體
- 容器儲存庫
- 容器映像
- Lambda

重大發現

「嚴重發現項目」區段提供您環境中的嚴重弱點計數，以及您環境中所有發現項目的總數。在本節中，將顯示每個資源和評估類型的計數。如需關鍵發現項目以及 Amazon Inspector 如何判斷重要性的詳細資訊，請參閱。了解 Amazon Inspector 中的發現

選擇重要發現項目群組會帶您前往「所有發現項目」頁面，並自動套用篩選，以顯示符合您選取之群組的所有重要發現項目。

下列是可用的重要發現項目群組：

- ECR 容器映像發現項目
- Amazon EC2 發現
- 網路可達性發現
- AWS Lambda 函數發現

以風險為基礎的補救

風險型補救區段會顯示影響您環境中大部分資源的嚴重弱點的前五個軟體套件。修復這些套件可以大幅減少環境中的重大風險數目。選擇軟體套件名稱，以查看相關的弱點詳細資訊和受影響的資源。

具有最重要發現項目的帳戶

「具有最重要發現項目的 AWS 帳戶」區段會顯示您環境中最重要發現項目的前 5 個帳戶，以及該帳戶的發現項目總數。只有 AWS Organizations當 Amazon Inspector 設定為使用多帳戶掃描時，才能從委派的管理員帳戶檢視本節。此檢視可協助委派系統管理員瞭解哪些帳戶在組織內可能面臨最大的風險。

選擇 [帳戶 ID] 以查看有關受影響成員帳戶的詳細資訊。

具有最重要發現結果的 Amazon ECR 儲存庫

具有最重要發現項目的彈性容器登錄 (ECR) 儲存庫區段會顯示環境中排名前五位的 Amazon ECR 儲存庫，其中包含最重要的容器映像發現項目。該視圖顯示存儲庫名稱， AWS 帳戶標識符，存儲庫創建日期，關鍵漏洞數量以及漏洞總數。此檢視可協助您識別哪些儲存庫可能面臨最大的風險。

選擇「存放庫名稱」以查看有關受影響存放庫的詳細資訊

包含最重要發現項目的容器映

「具有最重要發現項目的容器映像」區段會顯示您環境中前五個容器映像，其中包含最重要的發現項目。該視圖顯示圖像標籤數據，存儲庫名稱，圖像摘要， AWS 帳戶標識符，關鍵漏洞數量和漏洞總數。此檢視可協助應用程式擁有者識別哪些容器映像可能需要重建和重新啟動。

選擇容器映像檔，查看有關受影響容器映像檔的詳細資訊。

具有最重要發現項目的執

具有最重要發現項目的執行個體部分顯示前五個 Amazon EC2 執行個體，其中包含最重要的發現結果。此檢視會顯示執行個體識別碼、 AWS 帳戶識別碼、Amazon Machine Image (AMI) 識別碼、重大弱點數目，以及弱點總數。此檢視可協助基礎結構擁有者識別哪些執行處理需要修正

選擇執行個體 ID 以查看有關受影響 Amazon EC2 執行個體的詳細資訊。

具有最關鍵發現的 Amazon 機器映像（AMI）

具有最重要發現項目的 Amazon 機器映像 (AMI) 區段會顯示您環境中的前五個 AMI，其中包含最重要的發現結果。檢視會顯示 AMI 識別碼、 AWS 帳戶識別碼、環境中執行的受影響 EC2 執行個體數量、AMI 建立日期、AMI 的作業系統平台、嚴重弱點的數量以及弱點總數。此檢視可協助基礎結構擁有者識別可能需要重建的 AMI。

選擇受影響的執行個體，查看從受影響 AMI 啟動之執行個體的詳細資訊。

AWS Lambda 具有最關鍵發現的功能

具有最重要發現項目的AWS Lambda 函數區段會顯示環境中前五個 Lambda 函數，其中包含最重要的發現項目。此檢視會顯示 Lambda 函數名稱、 AWS 帳戶識別碼、執行階段環境、嚴重弱點數目、高弱點數目，以及弱點總數。此檢視可協助基礎設施擁有者識別可能需要修復的 Lambda 函數

選擇 [函數名稱] 以查看有關受影響 AWS Lambda 函數的詳細資訊。

了解 Amazon Inspector 中的發現

發現項目是關於會影響您其中一個 AWS 資源的弱點的詳細報告。發現項目會以偵測到的弱點命名，並提供嚴重性等級、受影響資源的相關資訊，以及說明如何修復已回報弱點的詳細資訊。

Amazon Inspector 只要偵測到 Amazon EC2 執行個體中的漏洞、Amazon ECR 儲存庫中的容器映像檔或 AWS Lambda 函數，就會產生一個發現項目。Amazon Inspector 會持續掃描您的運算環境，並儲存所有使用中的發現項目，直到您進行修復為止。

當您修復發現項目時，該發現項目會自動關閉，而 Amazon Inspector 會在 7 天後刪除該發現項目。刪除資源時，Amazon Inspector 會在 30 天後刪除與資源相關聯的任何發現項目。

如果您停用 Amazon Inspector，則發現項目會在 24 小時後移除。如果您的帳戶 AWS 遭到停權，則發現項目會在 90 天後移除。

發現項目會以下列其中一種狀態分類：

Active (作用中)

Amazon Inspector 會識別尚未修復為「作用中」的發現項目。

抑制

Amazon Inspector 會將受到一或多個抑制規則約束的發現項目識別為「抑制」。您可以在隱藏的發現項目清單中找到隱藏的發現項目 如需詳細資訊，請參閱 使用抑制規則抑制 Amazon Inspector 發現。

Closed (封閉式)

修復弱點後，Amazon Inspector 會自動偵測到這一點，並將發現的狀態變更為「已關閉」。已關閉的發現項目會在 7 天後刪除。

主題

- 在 Amazon Inspector 中查找類型
- 查找和查看亞馬遜檢查器發現
- Amazon Inspector 找到細節
- Amazon Inspector 評分和漏洞情報
- Amazon Inspector 發現的嚴重程度

在 Amazon Inspector 中查找類型

Amazon Inspector 產生 Amazon 彈性運算雲端 (Amazon EC2) 執行個體、亞馬遜彈性容器登錄 (亞馬遜 ECR) 儲存庫中的容器映像，以及 AWS Lambda 功能的調查結果。Amazon Inspector 可以產生下列類型的發現項目。

Package 漏洞

套件弱點發現項目可識別您 AWS 環境中暴露於常見弱點和暴露 (CVE) 的軟體套件。攻擊者可以利用這些未修補的漏洞破壞數據的機密性，完整性或可用性，或訪問其他系統。CVE 系統是公開已知資訊安全漏洞和暴露的參考方法。如需詳細資訊，請參閱 https://www.cve.org/。

供應商安全建議在發行後的 24 小時內，Linux 適用的 CVE 偵測會新增至 Amazon Inspector。適用於 Windows 的 CVE 偵測會在 Microsoft 發佈後 48 小時內新增至 Amazon Inspector。您可以使用Amazon Inspector 漏洞數據庫來查看是否支援 CVE 偵測。

Amazon Inspector 可以針對 EC2 執行個體、ECR 容器映像和 Lambda 函數產生套件漏洞發現項目。Package 弱點發現項目具有此發現項目類型獨有的其他詳細資料，包括 Inspector 評分和弱點情報。

程式碼漏洞

程式碼弱點發現項目可識別攻擊者可利用的程式碼行。程式碼弱點包括插入瑕疵、資料洩漏、弱式密碼編譯或程式碼遺漏加密。

Amazon Inspector 會使用自動推理和機器學習來評估您的 Lambda 函數應用程式程式碼，分析您的應用程式程式碼是否符合 它會根據與 Amazon CodeGuru 合作開發的內部偵測器，識別違反政策和漏洞。如需可能偵測的清單，請參閱偵測CodeGuru 器程式庫。

> **Important**
>
> Amazon Inspector 程式碼掃描可擷取程式碼片段，以突顯偵測到的 這些片段可能會以明文顯示硬式編碼的憑證或其他敏感資料。

如果您已Amazon Inspector Lambda 代碼啟動，Amazon Inspector 可以產生 Lambda 函數的程式碼弱點發現項目。

CodeGuru 服務會儲存偵測到與程式碼弱點相關的程式碼片段。依預設，會使用由 CodeGuru 控制的AWS 擁有金鑰來加密您的程式碼，不過，您可以使用自己的客戶受管金鑰透過 Amazon Inspector API 進行加密。如需更多資訊，請參閱針對發現項目中的程式碼進行靜態加密。

網路連線能力

網路連線能力發現指出您的環境中有開放的 Amazon EC2 執行個體的網路路徑。當您可以從 VPC 邊緣存取 TCP 和 UDP 連接埠時，例如網際網路閘道 (包括應用程式負載平衡器或傳統負載平衡器後面的執行個體)、VPC 對等連線或透過虛擬閘道的 VPN，就會出現這些發現項目。這些發現結果強調了可能過於寬鬆的網路組態，例如管理不當的安全性群組、存取控制清單或網際網路閘道，或可能允許潛在惡意存取的網路組態。

Amazon Inspector 只會產生 Amazon EC2 執行個體的網路連接性發現項目。Amazon Inspector 每隔 24 小時執行一次掃描，以查找網路可達性發現項目。

Amazon Inspector 會在掃描網路路徑時評估下列組態：

- Amazon EC2 執行個體
- AWS Lambda 函數
- Application Load Balancer
- Direct Connect
- Elastic Load Balancer
- 彈性網路界面
- 網際網路閘道 (Internet Gateway)
- 網路存取控制清單
- 路由表
- 安全群組
- 子網
- 虛擬私有雲
- 虛擬私有閘道
- VPC 端點
- VPC 閘道端點
- VPC 對等連接
- VPN 連線

查找和查看亞馬遜檢查器發現

本節中的程序說明如何透過 Amazon Inspector 主控台和 API 在 Amazon Inspector 中尋找和檢視發現項目。尋找詳細資訊會因尋找項目類型、弱點類型和受影響的資源而異。如需詳細資訊，請參閱 Amazon Inspector 找到細節。

Console

若要在主控台中檢視發現項目

1. 在 https://console.aws.amazon.com/inspector/v2/home 打開 Amazon Inspector 控制台。
2. 從導覽窗格中選擇「發現項目」。系統會將您導向至「發現項目」畫面，您可以在其中檢視所有發現項目。在「發現項目」表格中，您可以選取「標題」欄下的發現項目名稱，以選擇發現項目。
3. (選擇性) 您也可以檢視依類別分組的發現項目。從導覽窗格中選擇「發現項目」，然後選擇下列其中一個類別：
   - 依漏洞
   - 依執行個體

     > **Note**
     > 依執行個體分組的發現項目不包含網路可用性的相關資訊。

   - 按容器映像
   - 按容器存儲庫
   - 由 Lambda 函數

API

執行 ListFindingsAPI 作業。在請求中，您可`filterCriteria`以指定返回特定的發現。

Amazon Inspector 找到細節

在 Amazon Inspector 主控台中，您可以檢視每個發現項目的詳細資料。尋找詳細資料會因尋找類型而有所不同

若要檢視發現項目的詳細資訊

1. 打開 Amazon Inspector 控制台 https://console.aws.amazon.com/inspector/v2/home
2. 選取要在其中檢視搜尋結果的區域。
3. 在瀏覽窗格中，選擇「發現項目」以顯示發現項目清單
4. (選擇性) 使用篩選列來選取特定發現項目。如需詳細資訊，請參閱 過濾 Amazon Inspector 發現。
5. 選擇發現項目以檢視其詳細資料面板。

「發現項目詳細資料」面板包含發現項目的基本識別功能。這包括發現項目的標題，以及所識別的弱點的基本說明、修復建議和嚴重性分數。如需有關評分的資訊，請參閱Amazon Inspector 發現的嚴重程度。

可用於搜尋結果的詳細資料會因尋找項目類型和受影響的資源而有所不同。

所有發現項目都包含識別發現項目的 AWS 帳戶 ID 號碼、嚴重性、發現項目類型、建立發現項目的日期，以及包含該資源詳細資訊的受影響資源區段。

發現項目類型會決定發現項目可用的補救和弱點情報資訊。根據尋找項目類型，可以使用不同的尋找項目詳細資訊。

Package 漏洞

Package 漏洞發現項目適用於 EC2 執行個體、ECR 容器映像和 Lambda 函數。如需更多詳細資訊，請參閱 Package 漏洞。

Package 漏洞發現還包括Amazon Inspector 評分和漏洞情報.

此尋找項目類型具有下列詳細資訊：

- 修正可用 — 指出該弱點是否已在較新版本的受影響套件中修正。具有下列其中一個值：
  - YES，這表示所有受影響的套件都有固定版本。
  - NO，這表示沒有受影響的套件具有固定版本。
  - PARTIAL，也就是說，一或多個 (但不是全部) 受影響的套件都有固定版本。
- 可用的惡意利用 — 表示該弱點具有已知的攻擊。
  - YES也就是說，在您的環境中發現的弱點具有已知的漏洞。Amazon Inspector 無法掌握環境中漏洞利用的使用情況。
  - NO，這表示此弱點沒有已知的惡意利用。
- 受影響的套件 — 列出發現項目中識別為易受攻擊的每個套件，以及每個套件的詳細資訊：

- 檔案路徑 — EBS 磁碟區 ID 和與發現項目相關聯的分割區號碼。針對使用掃描的 EC2 執行個體的發現項目，此欄位顯示在無代理程式掃描.
- 已@@ 安裝的版本/固定版本 — 偵測到弱點之目前安裝的套件版本號碼。將已安裝的版本號碼與斜線 (/) 之後的值進行比較。第二個值是修正偵測到之弱點的套件版本號碼，這些弱點是「一般弱點和入侵程式」(CVE) 或與發現項目相關聯的公告所提供。如果已在多個版本中修正此弱點，此欄位會列出包含此修正程式的最新版本。如果無法使用修正程式，則此值為`None available`。

  > **Note**
  >
  > 如果在 Amazon Inspector 開始在發現項目中包含此欄位之前偵測到發現項目，則此欄位的值為空白。但是，可能有修復程序。

- Package 管理員 — 用來配置此套件的套件管理員。
- 修正 — 如果可透過更新的套件或程式設計程式庫取得修正程式，則本節包含您可以執行以進行更新的命令。您可以複製提供的命令並在您的環境中運行它。

  > **Note**
  >
  > 修復指令由廠商資料饋送提供，可能會因您的系統組態而有所不同。檢閱尋找參考資料或作業系統文件，以取得更具體的指引

- 弱點詳細資訊 — 為發現項目中識別的 CVE 提供 Amazon Inspector 偏好來源的連結，例如國家弱點資料庫 (NVD)、REDHAT 或其他作業系統廠商。此外，您還可以找到發現項目的嚴重性分數。如需嚴重性評分的詳細資訊，例如，請參閱Amazon Inspector 發現的嚴重程度。包括以下分數，包括每個分數的評分向量：
  - EPSS 得分
  - Inspector 得分
  - Amazon CVE 的 CVE
  - 來自 NVD 的 CVSS 3.1
  - 來自 NVD 的 CVSS 2.0（如適用，適用於較舊的 CVE）
- 相關弱點 — 指定與發現項目相關的其他弱點。一般而言，這些是影響相同套件版本的其他 CVE，或與發現項目 CVE 相同群組內的其他 CVE (由廠商決定)。

程式碼漏洞

程式碼弱點發現項目僅適用於 Lambda 函數。如需更多詳細資訊，請參閱 程式碼漏洞。此尋找項目類型具有下列詳細資訊：

- 修復可用-對於代碼漏洞，此值始終是YES。
- 偵測器名稱 — 用來偵測程式碼弱點的偵測 CodeGuru 器名稱。如需可能偵測的清單，請參閱偵測CodeGuru 器程式庫。
- 檢測器標籤 — 與檢測器關聯的 CodeGuru標籤 CodeGuru 使用標籤對檢測進行分類。
- 相關 CWE — 與程式碼弱點相關聯的常見弱點列舉 (CWE) 識別碼。
- 檔案路徑 — 程式碼弱點的檔案位置。
- 弱點位置 — 對於 Lambda 程式碼掃描程式碼弱點，此欄位會顯示 Amazon Inspector 發現該弱點的確切程式碼行。
- 建議的修正 — 這會建議如何編輯程式碼以修正發現項目。

網路連線能力

網路可達性發現項目僅適用於 EC2 執行個體。如需更多詳細資訊，請參閱 網路連線能力。此尋找項目類型具有下列詳細資訊：

- 開放連接埠範圍 — 可存取 EC2 執行個體的連接埠範圍。
- 開放網路路徑 — 顯示 EC2 執行個體的開放存取路徑。如需詳細資訊，請選取路徑上的項目。
- 修正 — 建議關閉開放網路路徑的方法。

Amazon Inspector 評分和漏洞情報

在 Amazon Inspector 主控台中，當您選取發現項目時，您可以檢視 Inspector 評分和弱點情報索引標籤，顯示發現套件漏洞的評分詳細資訊，以及弱點情報詳細資訊。這些詳細資料僅適用於Package 漏洞發現項目。

Amazon Inspector 得分

Amazon Inspector 分數是亞馬 Amazon Inspector 為每個 EC2 實例發現創建的情境化分數。Amazon Inspector 分數是透過將基本 CVSS v3.1 分數資訊與掃描期間從運算環境收集的資訊 (例如網路連接性結果和可利用性資料) 相互關聯來決定。例如，如果該弱點可透過網路惡意利用，則發現項目的 Amazon Inspector 分數可能會低於基本分數，但 Amazon Inspector 判斷網際網路上沒有可用到易受攻擊執行個體的開放網路路徑。

發現項目的基本分數是廠商提供的 CVSS v3.1 基本分數。對於其他廠商或廠商未提供分數的情況，Amazon Inspector 使用國家漏洞資料庫 (NVD) 的基本分數，則支援 RHEL、Debian 或亞馬遜廠商的基本分數。Amazon Inspector 使用常見漏洞評分系統 3.1 版計算器來計算分數。您可以在弱點詳細資料下的發現項目詳細資料中查看個別發現項目的基本分數來源，做為弱點來源 (或packageVulnerabilityDetails.source在發現的 JSON 中)

> **Note**
>
> Amazon Inspector 分數不適用於執行 Ubuntu 的 Linux 執行個體。這是因為 Ubuntu 定義了自己的弱點嚴重性，可能與相關的 CVE 嚴重性不同。

Amazon Inspector 得分詳情

當您開啟發現項目的詳細資料頁面時，您可以選取 [Inspector 評分] 和 [弱點情報] 索引標籤。此面板顯示基本分數和 Inspector 分數之間的差異。本節說明 Amazon Inspector 如何根據 Amazon Inspector 分數和軟體套件廠商分數的組合，指派嚴重性等級。如果分數不同，則此面板會顯示原因的說明。

在 CVSS 分數量度區段中，您可以看到包含 CVSS 基本分數量度和 Inspector 查員分數之間比較的表格。比較的指標是由first.org維護的 CVSS 規格文件中定義的基本指標。以下是基本測量結果的摘要：

攻擊向量

漏洞可被利用的內容。對於 Amazon Inspector 發現，這可以是網絡，鄰近網絡或本地。

攻擊複雜性

這描述了攻擊者在利用此弱點時將面臨的困難程度。低分數表示攻擊者需要滿足很少或完全不需要額外的條件才能利用此弱點。高分表示攻擊者需要投入大量精力，才能透過此弱點執行成功的攻擊。

所需權限

這說明攻擊者利用弱點所需的權限等級。

使用者互動

此指標指出使用此弱點的成功攻擊是否需要人類使用者 (而非攻擊者)。

Scope (範圍)

這表明某個易受攻擊元件中的漏洞是否會影響超出弱點元件安全範圍之元件中的資源。如果此值為「未變更」，則受影響的資源與受影響的資源相同。如果此值被更改，則易受攻擊的組件可被利用來影響由不同安全機構管理的資源。

保密

這會測量資訊安全風險遭到利用時，對資源內資料機密性的影響程度。其範圍從「無」(不會遺失機密性) 到「高」(High)，資源中的所有資訊都會洩漏，或是洩漏密碼或加密金鑰等機密資訊。

誠信

如果漏洞遭到利用，這會測量受影響資源中資料完整性的影響程度。當攻擊者修改受影響資源中的檔案時，完整性會面臨風險。分數範圍從「無」(此漏洞不允許攻擊者修改任何資訊) 到「高」(High)，如果遭到惡意利用，此弱點將允許攻擊者修改任何或所有檔案，或者可能修改的檔案會造成嚴重後果。

可用性

這會測量受影響資源在利用弱點時對可用性的影響程度。分數範圍從「無」(當弱點完全不影響可用性時) 到「高」(High)，如果遭到惡意利用，攻擊者可完全拒絕資源的可用性，或造成服務無法使用。

弱點情報

本節總結了來自 Amazon 的 CVE 的可用情報，以及業界標準安全情報來源，例如「記錄的未來」和「網路安全與基礎設施安全機構」(CISA)。

> **Note**
>
> 來自 CISA，Amazon 或記錄的未來英特爾將不適用於所有 CVE。

您可以在主控台或使用 BatchGetFindingDetailsAPI 來檢視弱點情報詳細資訊。主控台提供下列詳細資訊：

攻擊 & CK

本節顯示與 CVE 相關聯的 MITRE 策略、技術和程序 (TTP)。相關的 TTP 會顯示出來，如果有兩個以上的適用 TTP，您可以選取連結以查看完整清單。選擇一種策略或技術可以在 MITRE 網站上打開有關它的信息。

中鋼協

本節涵蓋與弱點相關的相關日期。網絡安全和基礎設施安全機構（CISA）根據積極利用的證據將該漏洞添加到已知的漏洞目錄中的日期，以及 CISA 預計將系統修補的截止日期。這些信息來自中鋼協.

已知的惡意

本節列出利用此弱點的已知漏洞利用套件和工具。

证据

本節總結了與此弱點相關的最嚴重安全事件。如果超過 3 個事件具有相同的重要性等級，則會顯示前三個最近的事件。

上次報告時間

本節顯示此弱點的上次已知公開利用日期。

Amazon Inspector 發現的嚴重程度

Amazon Inspector 產生弱點發現項目時，會自動為發現項目指派嚴重性。發現項目的嚴重性會反映發現項目的主要特徵，因此可協助您評估發現項目並排定其優先順序。發現項目的嚴重性並不暗示或以其他方式表示受影響資源對您的組織可能具有的重要性或重要性。

發現項目的嚴重性等級是由與下列其中一個嚴重性層級相對應的數值分數所驅動：資訊性、低、中、高或嚴重。

Amazon Inspector 判斷嚴重性的方法會根據尋找項目類型而有所不同。請參閱以下各節，進一步了解 Amazon Inspector 如何判斷每個發現項目類型的嚴重性等級。

軟體套件弱點嚴重性

Amazon Inspector 使用 NVD/CVSS 分數作為軟體套件弱點嚴重性評分的基礎。NVD/CVSS 分數是由 NVD 公佈且由 CVSS 定義的弱點嚴重性分數。NVD/CVSS 分數是安全指標的組成，例如攻擊複雜度、漏洞利用程式碼成熟度和所需權限。Amazon Inspector 會產生從 1 到 10 的數字分數，反映弱點的嚴重性。Amazon Inspector 將其歸類為基本分數，因為它會根據弱點的內在特徵反映弱點的嚴重程度，而這些特徵會隨著時間的推移而保持不變。此分數也會假設在不同部署環境中產生合理的最差情況影響。CVSS v3 標準會將 CVSS 分數對應至下列嚴重性等級。

得分	評分
0	資訊
0.1—3.9	低
4.0—6.9	中
7.0—8.9	高
9.0—10.0	嚴重

Package 弱點發現項目的嚴重性也可能為「未分類」。這表示廠商尚未針對偵測到的弱點設定弱點評分。在這種情況下，我們建議使用參考 URL 進行發現，以研究該漏洞並作出相應的回應。

Package 件弱點發現項目包含下列分數和相關評分向量，作為其發現詳細資料的一部分：

- EPSS 得分
- Inspector 得分
- Amazon CVE 的 CVE
- 來自 NVD 的 CVSS 3.1
- 來自 NVD 的保障制度 2.0（如適用）

代碼漏洞嚴重性

針對程式碼弱點發現項目，Amazon Inspector 會使用產生該發現項目之 Amazon CodeGuru 偵測器所定義的嚴重性等級。使用 CVSS v3 評分系統為每個偵測器分配嚴重性。如需嚴重性 CodeGuru 使用的說明，請參閱 CodeGuru 指南中的嚴重性定義。如需嚴重性的偵測器清單，請從下列支援的程式設計語言中進行選取：

- 按嚴重性分類的 Python 探測器
- 依嚴重性分類的 Java 偵測器

網路連線能力嚴重性

Amazon Inspector 會根據公開的服務、連接埠和通訊協定以及開放路徑類型，判斷網路連接性弱點的嚴重性。下表定義了這些嚴重性等級。「開放路徑分級」欄中的值代表來自虛擬閘道、對等 VPC 和 AWS Direct Connect 網路的開放路徑。所有其他公開的服務、連接埠和通訊協定都有資訊嚴重性等級。

服務	通訊埠	UDP 連接埠	互聯網路徑分級	開放路徑評等
DHCP	67、68、546、547	67、68、546、547	中	資訊
Elasticsearch	9300、9200	NA	中	資訊
FTP	21	21	高	中

通用類別目錄 LDAP	3268	NA	中	資訊
透過 TLS 的通用類別目錄 LDAP	3269	NA	中	資訊
HTTP	80	80	低	資訊
HTTPS	443	443	低	資訊
Kerberos	88、464、543、544、749、751	88、464、749、750、751、752	中	資訊
LDAP	389	389	中	資訊
透過 TLS 的 LDAP	636	NA	中	資訊
MongoDB	27017、27018、27019、28017	NA	中	資訊
MySQL	3306	NA	中	資訊
NetBIOS	137、139	137、138	中	資訊
NFS	111、2049、4045、1110	111、2049、4045、1110	中	資訊
Oracle	1521、1630	NA	中	資訊
PostgreSQL	5432	NA	中	資訊
列印服務	515	NA	高	中
RDP	3389	3389	中	低
RPC	111、135、530	111、135、530	中	資訊
SMB	445	445	中	資訊

SSH	22	22	中	低
SQL Server	1433	1434	中	資訊
Syslog	601	514	中	資訊
Telnet	23	23	高	中
WINS	1512、42	1512、42	中	資訊

管理 Amazon Inspector 中的發現

Amazon Inspector 提供數種方式來排序、分組和管理您的發現項目。這些功能可協助您針對環境量身打造發現項目、依不同檢視彙總發現項目，並專注於特定 AWS 環境的弱點。

發現項目會根據其狀態顯示在不同的檢視中：作用中、隱抑或已關閉。依預設，每個檢視只會顯示作用中的發現項目。使用中的發現項目代表 Amazon Inspector 偵測到的潛在安全問題，表示存在弱點或潛在威脅。隱藏的發現項目是您已使用抑制規則排除的作用中發現項目。Amazon Inspector 偵測到發現項目已修復時，會自動將發現項目的狀態設定為已關閉。您不要手動關閉發現項目。

您也可以在中檢視發現項目 AWS Security Hub，這項服務可提供您 AWS 環境中安全性狀態的全面檢視。如需詳細資訊，請參閱 Amazon Inspector 與集成 AWS Security Hub。Amazon ECR 主控台也提供容器映像發現項目，您可以使用 AWS Command Line Interface (AWS CLI) 或 API 檢視所有資源的發現項目。

主題

查看亞馬遜檢查器的

Amazon Inspector 主控台會根據相關分組，以索引標籤式檢視顯示發現項目。每個檢視都包含可協助您分析特定弱點、識別最易受攻擊的資源，以及評估環境中弱點的整體影響的資訊。您可以選擇「發現項目」導覽側面板下的選項，以切換作業選項至其他搜尋結果檢視表。您也可以在每個檢視中建立篩選器，以便專注於特定類型的發現項目。如需如何使用篩選條件的詳細資訊，請參閱過濾 Amazon Inspector 發現。

發現項目可以依下列參數分組：

- 依弱點 — 列出在您的環境中偵測到的最嚴重弱點。從此檢視中選擇弱點標題，即可開啟包含其他資訊的詳細資料窗格。
- 依帳戶 — 列出您的帳戶、Amazon Inspector 掃描每個帳戶的涵蓋範圍百分比，以及每個帳戶的嚴重性和高嚴重性發現項目總數。此群組僅適用於委派的系統管理員。

- 依執行個體 — 列出環境中最脆弱的 Amazon EC2 執行個體。
- 依容器映像 — 列出您環境中最脆弱的 Amazon ECR 容器映像。
- 依容器存放庫 — 顯示具有最多弱點的存放庫。
- 依 Lambda 函數 — 顯示具有最多弱點的 Lambda 函數。
- 所有發現項目 — 顯示您環境的完整發現項目清單。這是當您切換作業選項至「發現項目」頁面時的預設檢視表。在此檢視中，您可以依作用中、隱藏及已關閉的發現項目進行篩選。

您可以根據篩選建立隱藏規則，以將發現項目從發現項目檢視中排除。如需詳細資訊，請參閱 使用抑制規則抑制 Amazon Inspector 發現。

過濾 Amazon Inspector 發現

發現項目篩選可讓您僅檢視符合指定條件的發現項目。不符合篩選條件的發現項目會從您的檢視中排除。您可以使用 Amazon Inspector 主控台建立尋找篩選器。若要使用這些篩選器來自動隱藏現有和 future 的發現項目，請參閱使用抑制規則抑制 Amazon Inspector 發現。

在 Amazon Inspector 器控制台創建過濾器

在每個發現項目檢視中，您可以使用篩選功能來尋找具有特定特性的發現項目。當您移至不同的索引標籤式檢視時，篩選器會被移除。

篩選器由篩選條件組成，篩選條件由與篩選器值配對的篩選器屬性組成。不符合篩選條件的發現項目會從發現項目清單中排除。例如，若要查看與管理員帳戶相關聯的所有發現項目，您可以選擇 AWS 帳號 ID 屬性，並將其與十二位數 AWS 帳號 ID 的值配對。

某些篩選條件適用於所有發現項目，而其他篩選條件則僅適用於特定資源類型或尋找項目類型。

若要將篩選套用至發現項目檢視

1. 打開 Amazon Inspector 控制台 https://console.aws.amazon.com/inspector/v2/home.
2. 在導覽窗格中，選擇調查結果。預設檢視會顯示所有狀態為「作用中」的發現項目。
3. 若要依條件篩選發現項目，請選取 [新增篩選列]，以查看該檢視表所有適用篩選條件的清單。不同的檢視中提供不同的篩選條件。
4. 從清單中選擇您要篩選依據的條件。
5. 在準則輸入窗格中，輸入所需的篩選值以定義該條件。

6. 選擇「套用」，將該篩選條件套用至您目前的結果。您可以再次選取篩選器輸入列來繼續新增其他篩選條件。
7. (選擇性) 若要檢視隱藏或已關閉的發現項目，請在篩選列中選擇作用中，然後選擇隱藏或已關閉。選擇全部顯示，即可在相同檢視中查看作用中、隱藏及已關閉的發現項目。

使用抑制規則抑制 Amazon Inspector 發現

使用隱藏規則排除符合條件的發現項目。例如，您可以建立一個規則來隱藏弱點分數較低的所有發現項目，因此您只能專注於最重要的發現項目。

> **Note**
>
> 抑制規則僅用於篩選您的發現項目清單，不會對發現項目造成任何影響，或防止 Amazon Inspector 產生發現項目。

如果 Amazon Inspector 產生符合抑制規則的發現項目，則發現項目會設定為「抑制」。根據預設，符合抑制規則的發現項目不會顯示在清單中。

Amazon Inspector 會儲存抑制的發現，直到它們得到補救為止 Amazon Inspector 可偵測已修復的鰭。當 Amazon Inspector 偵測到已修正的發現時，會將尋找項目設定為「已關閉」，並將其存放 7 天。

抑制的發現會以事件 AWS Security Hub 的形式發佈 EventBridge 至 Amazon。您可以使用 EventBridge 規則變更發現項目的狀態，自動隱藏 Security Hub 中不需要的發現項目。如需詳細資訊，請參閱如何在 AWS Security Hub中建立自動抑制規則。

您無法建立關閉或修正搜尋結果的隱藏規則。您只能建立隱藏規則來篩選出現在清單中的發現項目。您可以隨時在 Amazon Inspector 主控台中檢視隱藏的發現項目。

> **Note**
>
> 組織中的成員帳戶無法建立或管理隱藏規則。

建立抑制規則

您可以建立隱藏規則來篩選依預設顯示的發現項目清單。您可以使用 CreateFilterAPI 並指定SUPRESS為的值，以程式設計方式建立抑制規則`action`。

> **Note**
>
> 只有獨立帳戶，而 Amazon Inspector 委派的管理員才能建立和管理抑制規則。組織中的成員不會在導覽窗格中看到隱藏規則的選項。

建立抑制規則 (主控台)

1. 打開 Amazon Inspector 控制台 https://console.aws.amazon.com/inspector/v2/home.
2. 在導覽窗格中，選擇 [隱藏規則]。然後，選擇 Create role (建立角色)。
3. 針對每個準則，執行下列動作：
   - 選取篩選列以查看可新增至隱藏規則的篩選準則清單。
   - 選取隱藏規則的篩選準則。
4. 完成新增條件後，請輸入規則的名稱和選擇性描述。
5. 選擇 [儲存規則]。Amazon Inspector 會立即套用新的抑制規則，並隱藏符合條件的任何發現項目。

檢視隱藏的發現

依預設，Amazon Inspector 不會在亞馬 Amazon Inspector 查器主控台中顯示抑制的發現項目。不過，您可以檢視特定規則所抑制的發現項目。

檢視隱藏的發現項目

1. 打開 Amazon Inspector 控制台 https://console.aws.amazon.com/inspector/v2/home.
2. 在導覽窗格中，選取隱藏規則。
3. 在隱藏規則清單中，選取規則的標題。

變更抑制規則

您可以隨時變更抑制規則。

修改抑制規則

1. 打開 Amazon Inspector 控制台 https://console.aws.amazon.com/inspector/v2/home
2. 在導覽窗格中，選取隱藏規則。

3. 選取您要修改的隱藏規則的標題。
4. 進行預期的變更，然後選擇「儲存」以更新規則。

刪除抑制規則

您可以刪除抑制規則。如果您刪除抑制規則，Amazon Inspector 會停止隱藏符合規則準則且未受其他規則抑制的新發現項目和現有發現項目。

刪除抑制規則後，符合規則條件的發現項目的新出現次數和現有出現項目的狀態為「作用中」。這意味著它們默認顯示在 Amazon Inspector 控制台上。此外，Amazon Inspector 將這些發現 EventBridge 作為事件發佈到 AWS Security Hub 和 Amazon。

刪除抑制規則

1. 打開 Amazon Inspector 控制台 https://console.aws.amazon.com/inspector/v2/home.
2. 在導覽窗格中，選取隱藏規則。
3. 選取您要刪除的隱藏規則標題旁邊的核取方塊。
4. 選擇 [刪除]，然後確認您的選擇永久刪除規則。

從 Amazon Inspector 匯出發現報告

除了將發現結果傳送給 Amazon 之外 EventBridge AWS Security Hub，您還可以選擇將發現結果匯出到 Amazon Simple Storage Service (Amazon S3) 儲存貯體，做為發現報告。發現項目報告是 CSV 或 JSON 檔案，其中包含您選擇包含在報告中的發現項目詳細資訊。它會在特定時間點提供發現項目的詳細快照。對於每個發現項目，檔案都包含受影響資源的 Amazon 資源名稱 (ARN)、建立發現項目的日期和時間、相關的常見弱點和曝光 (CVE) ID，以及發現項目的嚴重性、狀態以及 Amazon Inspector 和 CVSS 分數。

設定發現項目報告時，首先要指定要包含在報告中的發現項目。根據預設，Amazon Inspector 會包含目前 AWS 區域 狀態為「作用中」狀態之所有發現項目的資料。如果您是某個組織委派的 Amazon Inspector 管理員，這包括組織中所有成員帳戶的發現項目資料。

您可以選擇性地篩選資料來自訂報告。使用篩選器，您可以包含或排除具有特定特性之發現項目的資料，例如，在特定時間範圍內建立的所有嚴重發現項目、特定資源的所有作用中發現項目，或特定類型的所有「嚴重」發現項目。如果您是某個組織的 Amazon Inspector 管理員，則可以使用篩選器建立報告，其中包含組織 AWS 帳戶 中特定項目的發現項目 — 例如，帳戶的所有狀態為「作用中」且可用修正程式的重要發現項目。然後，您可以與帳戶擁有者共用報告以進行修正。

> **Note**
>
> 當您使用 CreateFindingsReportAPI 匯出發現項目報告時，預設只會看到作用中的發現項目。若要查看隱藏或已關閉的發現項目，您必須指定SUPPRESSED或CLOSED作為 FindingStatus 篩選條件的值。

當您匯出發現項目報告時，Amazon Inspector 會使用您指定的 AWS Key Management Service (AWS KMS) 金鑰加密資料，並將報告新增至您也指定的 S3 儲存貯體。加密金鑰必須是客戶管理的 AWS Key Management Service (AWS KMS) 目前 AWS 區域對稱加密金鑰。此外，金鑰政策必須允許 Amazon Inspector 使用金鑰。S3 儲存貯體也必須位於目前的區域，且儲存貯體的政策必須允許 Amazon Inspector 將物件新增至儲存貯體。

Amazon Inspector 完成報告的加密和存放後，您可以從指定的 S3 儲存貯體下載報告，或將報告移至其他位置。或者，您可以將報告保留在相同的 S3 儲存貯體中，並將該儲存貯體用作隨後匯出之發現項目報告的存放庫。

本主題會引導您完成使用匯出發現項目報告的程序。 AWS Management Console 此程序包括確認您具有所需的權限、設定所需的資源，然後設定和匯出報告。

> **Note**
>
> 您一次只能匯出一個發現項目報告。如果匯出目前正在進行中，請等到匯出完成，然後再嘗試匯出其他報告。

任務

- 步驟 1：驗證您的權限
- 步驟 2：設定 S3 儲存貯體
- 步驟 3：設定 AWS KMS key
- 步驟 4：設定及匯出發現項目報告
- 排解匯出錯誤

第一次匯出發現項目報告之後，步驟 1 到 3 可以是選擇性的。這主要取決於您是否要使用相同的 S3 儲存貯體以及 AWS KMS key 後續報告。

如果您偏好在步驟 1 到 3 之後以程式設計方式匯出報表，請使用 Amazon Inspector API 的CreateFindingsReport操作。

步驟 1：驗證您的權限

從 Amazon Inspector 匯出發現項目報告之前，請確認您具有匯出發現項目報告和設定資源以加密和存放報告所需的許可。若要驗證您的許可，請使用 AWS Identity and Access Management (IAM) 檢閱附加到 IAM 身分的 IAM 政策。然後將這些策略中的資訊與下列您必須允許執行的動作清單進行比較，才能匯出發現項目報告。

Amazon Inspector

對於 Amazon Inspector，請確認您是否允許執行下列動作：

- `inspector2:ListFindings`
- `inspector2:CreateFindingsReport`

這些動作可讓您擷取帳戶的發現項目資料，並將該資料匯出到發現項目報告中。

如果您打算以程式設計方式匯出大型報表，您也可以確認您是否允許執行下列動作：`inspector2:GetFindingsReportStatus`、檢查報表的狀態`inspector2:CancelFindingsReport`，以及取消進行中的匯出。

AWS KMS

對於 AWS KMS，請確認您是否被允許執行下列動作：

- `kms:GetKeyPolicy`
- `kms:PutKeyPolicy`

這些動作可讓您擷取和更新您希望 Amazon Inspector 用來加密報告的金鑰政策。 AWS KMS key

若要使用 Amazon Inspector 主控台匯出報告，請確認您是否可以執行下列 AWS KMS 動作：

- `kms:DescribeKey`
- `kms:ListAliases`

這些動作可讓您擷取和顯示您帳戶 AWS KMS keys 的相關資訊。然後，您可以選擇其中一個金鑰來加密報表。

如果您打算建立新的 KMS 金鑰來加密報表，您也需要被允許執行`kms:CreateKey`動作。

Amazon Simple Storage Service (Amazon S3)

對於 Amazon S3，請確認您是否允許執行下列動作：

- s3:CreateBucket
- s3:DeleteObject
- s3:PutBucketAcl
- s3:PutBucketPolicy
- s3:PutBucketPublicAccessBlock
- s3:PutObject
- s3:PutObjectAcl

這些動作可讓您建立和設定您希望 Amazon Inspector 存放報表的 S3 儲存貯體。它們也可讓您從值區新增和刪除物件。

如果您打算使用 Amazon Inspector 主控台匯出報告，請確認您是否可以執行s3:ListAllMyBuckets和s3:GetBucketLocation動作。這些動作可讓您擷取和顯示帳戶 S3 儲存貯體的相關資訊。然後，您可以選擇其中一個值區來儲存報表。

如果您無法執行一或多個必要動作，請在繼續執行下一個步驟之前，向 AWS 管理員尋求協助。

步驟 2：設定 S3 儲存貯體

驗證許可後，您就可以設定要在其中存放發現結果報告的 S3 儲存貯體。它可以是您自己帳戶的現有值區，也可以是另一個帳戶所擁有 AWS 帳戶 且您可以存取的現有值區。如果您想要將報告儲存在新值區中，請先建立值區，然後再繼續。

S3 儲存貯體必須與 AWS 區域 您要匯出的發現項目資料相同。例如，如果您在美國東部 (維吉尼亞北部) 區域使用 Amazon Inspector，並且想要匯出該區域的發現項目資料，則該值區也必須位於美國東部 (維吉尼亞北部) 區域。

此外，儲存貯體的政策必須允許 Amazon Inspector 將物件新增至儲存貯體。本主題說明如何更新值區政策，並提供要新增至政策的陳述式範例。如需新增和更新儲存貯體政策的詳細資訊，請參閱 Amazon 簡單儲存服務使用者指南中的使用儲存貯體政策。

如果您想要將報告存放在另一個帳戶擁有的 S3 儲存貯體中，請與儲存貯體的擁有者合作更新儲存貯體的政策。同時取得值區的 URI。匯出報表時，您必須輸入此 URI。

若要更新值區政策

1. 在以下位置打開 Amazon S3 控制台 https://console.aws.amazon.com/s3。

2. 在導覽窗格中，選擇 儲存貯體。
3. 選擇您要存放發現結果報告的 S3 儲存貯體。
4. 選擇許可索引標籤標籤。
5. 在儲存貯體政策區段中，選擇編輯。
6. 將下列範例陳述式複製到剪貼簿：

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "allow-inspector",
   "Effect": "Allow",
   "Principal": {
    "Service": "inspector2.amazonaws.com"
   },
   "Action": [
    "s3:PutObject",
    "s3:PutObjectAcl",
    "s3:AbortMultipartUpload"
   ],
   "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*",
   "Condition": {
    "StringEquals": {
     "aws:SourceAccount": "111122223333"
    },
    "ArnLike": {
     "aws:SourceArn": "arn:aws:inspector2:Region:111122223333:report/*"
    }
   }
  }
 ]
}
```

7. 在 Amazon S3 主控台的儲存貯體政策編輯器中，將前述陳述式貼到政策中，以將其新增至政策。

   當您新增陳述式時，請確定語法有效。儲存貯體政策使用 JSON 格式。這表示您需要在陳述式之前或之後新增逗號，視您將陳述式新增至原則的位置而定。如果您將陳述式新增為最後一個陳述式，請在前述陳述式的右括號後加上逗號。如果您將它新增為第一個陳述式或兩個現有陳述式之間，請在陳述式的右括號後加上逗號。
8. 使用適用於您環境的正確值更新陳述式，其中：

- *#########*的名稱。
- *111122223333* 是您的帳戶識別碼。 AWS 帳戶
- *##*是您正 AWS 區域 在使用 Amazon Inspector，並希望允許 Amazon Inspector 向存儲桶添加報告。例如，us-east-1針對美國東部 (維吉尼亞北部) 區域。

> **Note**
>
> 如果您在手動啟用的情況下使用 Amazon Inspector AWS 區域，請同時將適當的區域代碼新增至Service欄位的值。此欄位指定 Amazon Inspector 服務主體。
> 例如，如果您在具有區域代碼的中東 (巴林) 區域中使用 Amazon Inspectorme-south-1，請inspector2.me-south-1.amazonaws.com在陳述式中取inspector2.amazonaws.com代。

請注意，範例陳述式定義了使用兩個 IAM 全域條件金鑰的條件：

- aws：SourceAccount-這種情況允許 Amazon Inspector 僅為您的帳戶將報告添加到存儲桶中。它可以防止 Amazon Inspector 向其他帳戶的存儲桶添加報告。更具體地說，條件會指定哪個帳戶可以針對條aws:SourceArn件指定的資源和動作使用值區。

  若要將其他帳戶的報告儲存在值區中，請將每個額外帳戶的帳戶 ID 新增至此條件。例如：

  ```
  "aws:SourceAccount": [111122223333,444455556666,123456789012]
  ```

- aws：SourceArn— 此條件會根據要添加到存儲桶的對象的來源限制對存儲桶的訪問。它可以防 AWS 服務 止其他人將對象添加到存儲桶。這也可以防止 Amazon Inspector 在為您的帳戶執行其他動作時，將物件新增至儲存貯體。更具體地說，該條件允許 Amazon Inspector 只有在物件為發現項目報告時，才能將物件新增至儲存貯體，且僅當這些報表是由帳戶建立並在條件中指定的區域中時。

  若要允許 Amazon Inspector 針對其他帳戶執行指定的動作，請將每個額外帳戶的 Amazon 資源名稱 (ARN) 新增至此情況。例如：

  ```
  "aws:SourceArn": [
      "arn:aws:inspector2:Region:111122223333:report/*",
      "arn:aws:inspector2:Region:444455556666:report/*",
      "arn:aws:inspector2:Region:123456789012:report/*"
  ```

```
]
```

`aws:SourceAccount`和`aws:SourceArn`條件所指定的帳戶應該符合。

這兩種情況都有助於防止 Amazon Inspector 在與 Amazon S3 進行交易時被用作混淆的副手。雖然我們不建議這樣做，但您可以從值區政策中移除這些條件。

9. 完成值區政策更新後，請選擇 [儲存變更]。

步驟 3：設定 AWS KMS key

驗證許可並設定 S3 儲存貯體後，請確定 AWS KMS key 您希望 Amazon Inspector 用來加密發現結果報告的內容。金鑰必須是客戶管理的對稱式加密 KMS 金鑰。此外，金鑰必須與 AWS 區域 您設定用來存放報表的 S3 儲存貯體位於相同。

金鑰可以是您自己帳戶中的現有 KMS 金鑰，也可以是其他帳戶擁有的現有 KMS 金鑰。如果您想要使用新的 KMS 金鑰，請先建立金鑰，然後再繼續。如果您想要使用其他帳戶擁有的現有金鑰，請取得該金鑰的 Amazon 資源名稱 (ARN)。當您從 Amazon Inspector 導出報告時，您需要輸入此 ARN。如需建立和檢閱 KMS 金鑰設定的詳細資訊，請參閱AWS Key Management Service 開發人員指南中的管理金鑰。

決定要使用的 KMS 金鑰之後，請授與 Amazon Inspector 使用金鑰的權限。否則，Amazon Inspector 將無法加密和導出報告。若要授予 Amazon Inspector 使用金鑰的權限，請更新金鑰的金鑰政策。如需有關金鑰原則和管理 KMS 金鑰存取權的詳細資訊，請參閱AWS Key Management Service 開發人員指南 AWS KMS中的金鑰政策。

若要更新金鑰原則

> **Note**
>
> 下列程序適用於更新現有金鑰以允許 Amazon Inspector 使用該金鑰。如果您還沒有現有的金鑰，請參閱以https://docs.aws.amazon.com/kms/latest/developerguide/create-keys.html取得建立金鑰的指引。

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

4. 選擇您要用來加密報表的 KMS 金鑰。金鑰必須是對稱加密 (對稱加密) 金鑰。
5. 在金鑰原則索引標籤上，選擇編輯。如果您看不到含 [編輯] 按鈕的金鑰原則，您必須先選取 [切換至原則檢視]。
6. 將下列範例陳述式複製到剪貼簿：

```
{
    "Sid": "Allow Amazon Inspector to use the key",
    "Effect": "Allow",
    "Principal": {
        "Service": "inspector2.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "111122223333"
        },
        "ArnLike": {
            "aws:SourceArn": "arn:aws:inspector2:Region:111122223333:report/*"
        }
    }
}
```

7. 在 AWS KMS 主控台的金鑰原則編輯器中，將前述陳述式貼到金鑰原則中，以將其新增至原則。

   當您新增陳述式時，請確定語法有效。金鑰政策使用 JSON 格式。這表示您需要在陳述式之前或之後新增逗號，視您將陳述式新增至原則的位置而定。如果您將陳述式新增為最後一個陳述式，請在前述陳述式的右括號後加上逗號。如果您將它新增為第一個陳述式或兩個現有陳述式之間，請在陳述式的右括號後加上逗號。
8. 使用適用於您環境的正確值更新陳述式，其中：

   - *111122223333* 是您的帳戶識別碼。 AWS 帳戶
   - *##*是您要允許 Amazon Inspector 使用金鑰加密報告的 AWS 區域 位置。例如，`us-east-1`針對美國東部 (維吉尼亞北部) 區域。

> **Note**
>
> 如果您在手動啟用的情況下使用 Amazon Inspector AWS 區域，請同時將適當的區域代碼新增至`Service`欄位的值。例如，如果您在中東 (巴林) 區域使用 Amazon Inspector，請取代`inspector2.amazonaws.com`為`inspector2.me-south-1.amazonaws.com`.

如同前一步驟中儲存貯體政策的範例陳述式，此範例中的`Condition`欄位使用兩個 IAM 全域條件金鑰：

- aws：SourceAccount— 這種情況允許 Amazon Inspector 僅為您的帳戶執行指定的操作。更具體地說，它決定哪個帳戶可以針對`aws:SourceArn`條件指定的資源和動作執行指定的動作。

  若要允許 Amazon Inspector 針對其他帳戶執行指定的動作，請將每個額外帳戶的帳戶 ID 新增至此情況。例如：

  ```
  "aws:SourceAccount": [111122223333,444455556666,123456789012]
  ```

- aws：SourceArn-此條件可防 AWS 服務 止其他人執行指定的操作。這也可以防止 Amazon Inspector 在為您的帳戶執行其他動作時使用金鑰。換句話說，它允許 Amazon Inspector 僅在物件為發現項目報告時使用金鑰加密 S3 物件，且僅當這些報告是由帳戶建立並在條件中指定的區域中建立時。

  若要允許 Amazon Inspector 針對其他帳戶執行指定的動作，請為每個額外的帳戶新增 ARN 至此條件。例如：

  ```
  "aws:SourceArn": [
      "arn:aws:inspector2:us-east-1:111122223333:report/*",
      "arn:aws:inspector2:us-east-1:444455556666:report/*",
      "arn:aws:inspector2:us-east-1:123456789012:report/*"
  ]
  ```

  `aws:SourceAccount`和`aws:SourceArn`條件所指定的帳戶應該符合。

這些條件有助於防止 Amazon Inspector 在與交易期間被用作混淆的副手 AWS KMS。雖然我們不建議這樣做，但您可以從陳述式中移除這些條件。

9. 完成金鑰原則更新後，請選擇 [儲存變更]。

步驟 4：設定及匯出發現項目報告

驗證您的權限並設定資源以加密和儲存發現項目報告之後，您就可以設定和匯出報告了。

若要設定及匯出發現項目報告

1. 打開 Amazon Inspector 控制台 https://console.aws.amazon.com/inspector/v2/home.
2. 在瀏覽窗格的「發現項目」下，選擇「所有發現項目」。
3. (選擇性) 使用「發現項目」表格上方的篩選列，新增篩選條件，以指定要包含在報告中的發現項目。當您新增條件時，Amazon Inspector 會更新表格，以僅包含符合條件的發現項目。此表格提供報表將包含之資料的預覽。

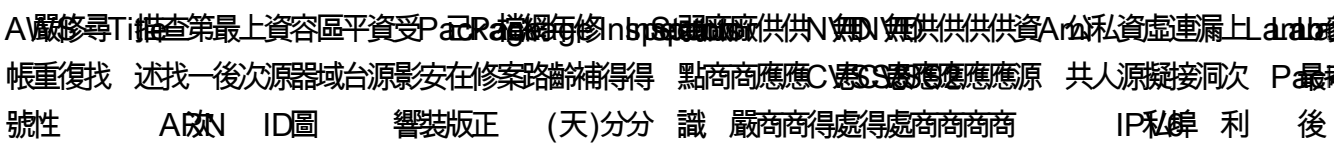
   > **Note**
   >
   > 我們建議您新增篩選條件。如果不 AWS 區域 這樣做，報告會包含目前狀態為「作用中」之所有發現項目的資料。如果您是某個組織的 Amazon Inspector 管理員，這包括組織中所有成員帳戶的發現項目資料。
   > 如果報告包含所有或多個發現項目的資料，產生和匯出報告可能需要很長時間，而且您一次只能匯出一個報告。

4. 選擇匯出搜尋結果。
5. 在「匯出設定」區段中，對於「匯出檔案類型」，指定報告的檔案格式：

   - 若要建立包含資料的 JavaScript 物件標記法 (.json) 檔案，請選擇 [JSON]。

     如果您選擇 JSON 選項，報告將包含每個發現項目的所有欄位。如需可能的 JSON 欄位清單，請參閱 Amazon Inspector API 參考資料中的尋找資料類型。
   - 若要建立包含資料的逗號分隔值 (.csv) 檔案，請選擇 [CSV]。

     如果您選擇 CSV 選項，則報告只會包含每個發現項目的一部分欄位，大約 45 個報告發現項目關鍵屬性的欄位。欄位包括：「尋找項目類型」、「標題」、「嚴重性」、「狀態」、「描述」、「第一次上線」、「上次上線時間」、「可用的修正程式」、「 AWS 帳號 ID」、「資源 ID」 這些欄位除了可擷取每個發現項目的評分詳細資料和參考 URL 的欄位之外。以下是發現項目報告中 CSV 標頭的範例：

識別碼 可類用型 看上更到線新 像標籤 標套籤件 版本中修正 路路徑徑 向量 別碼 重諮性詢 公分出版 CV 量圖形 S 量分圖形 資源 資源 人範資圍源 可用用於 類更型新 網址於

6. 在「匯出位置」下，對於 S3 URI，指定要存放報表的 S3 儲存貯體：

   - 若要將報表存放在您帳戶擁有的儲存貯體中，請選擇瀏覽 S3。Amazon Inspector 會為您的帳戶顯示 S3 儲存貯體的表格。選取您要的時段資料列，然後選擇「選擇」。

     > **Tip**
     >
     > 若要同時為報表指定 Amazon S3 路徑前置詞，請在 S3 URI 方塊中的值附加斜線 (/) 和前置詞。然後，Amazon Inspector 會在將報告新增至儲存貯體時包含前置詞，而 Amazon S3 會產生由前置詞指定的路徑。
     > 例如，如果您想要使用您的 AWS 帳戶 識別碼做為前置詞，而您的帳戶識別碼是 111122223333，請附加**/111122223333**至 S3 URI 方塊中的值。
     > 前綴類似於 S3 存儲桶中的目錄路徑。它允許您將類似的對象組合在一個存儲桶中，就像您可以將類似的文件一起存儲在文件系統上的文件夾中。如需詳細資訊，請參閱 Amazon 簡單儲存服務使用者指南中的使用資料夾組織 Amazon S3 主控台中的物件。

   - 若要將報表儲存在其他帳戶擁有的值區中，請輸入儲存貯體的 URI — 例如，**s3://DOC-EXAMPLE_BUCKET**其中 DOC/EXAMPLE _BUCKET 是值區的名稱。值區擁有者可以在值區的屬性中找到此資訊。

7. 對於 KMS 金鑰，請指 AWS KMS key 定您要用來加密報表的金鑰：

   - 若要使用您自己帳戶中的金鑰，請從清單中選擇金鑰。此清單會顯示您帳戶的客戶管理、對稱加密 KMS 金鑰。
   - 若要使用其他帳戶擁有的金鑰，請輸入該金鑰的 Amazon 資源名稱 (ARN)。金鑰擁有者可以在金鑰的屬性中找到此資訊。如需詳細資訊，請參閱AWS Key Management Service 開發人員指南中的尋找金鑰 ID 和金鑰 ARN。

8. 選擇 Export (匯出)。

Amazon Inspector 會產生發現項目報告，使用您指定的 KMS 金鑰加密該報告，然後將其新增至您指定的 S3 儲存貯體。視您選擇包含在報告中的發現項目數量而定，此程序可能需要數分鐘或數小時。匯

出完成後，Amazon Inspector 會顯示一則訊息，指出您的發現項目報告已成功匯出。選擇性地選擇訊息中的「檢視報告」以導覽至 Amazon S3 中的報告。

請注意，您一次只能匯出一份報告。如果匯出目前正在進行中，請等到匯出完成，然後再嘗試匯出其他報告。

排解匯出錯誤

如果您嘗試匯出發現項目報告時發生錯誤，Amazon Inspector 會顯示說明錯誤的訊息。您可以使用本主題中的資訊做為指南，以識別錯誤的可能原因和解決方案。

例如，確認 S3 儲存貯體是否在目前儲存貯體中， AWS 區域 而儲存貯體的政策允許 Amazon Inspector 將物件新增至儲存貯體。此外，請確認目前區域中已啟用，並確保金鑰政策允許 Amazon Inspector 使用金鑰。 AWS KMS key

解決錯誤後，請嘗試再次匯出報告。

無法有多個報告錯誤

如果您嘗試建立報告，但 Amazon Inspector 已經產生報告，您會收到錯誤訊息，說明原因：無法有多個正在進行中的報告。因為 Amazon Inspector 一次只能為一個帳戶產生一份報告，就會發生這個錯誤。

若要解決此錯誤，您可以等待其他報告完成或取消，然後再要求新的報告。

您可以使用作業來檢查報表的狀態，此GetFindingsReportStatus作業會傳回目前正在產生之任何報表的報告 ID。

如有需要，您可以使用作業指定的報告 ID，使用`GetFindingsReportStatus`作業取消目前正在進行的CancelFindingsReport匯出。

使用 Amazon 創建對 Amazon Inspector 發現的自定義 EventBridge

Amazon Inspector 會為 Amazon 建立新產生 EventBridge的發現項目、新彙總的發現項目以及發現項目狀態變更的事件。除了變更`updatedAt`和`lastObservedAt`欄位以外的任何項目都會發佈新事件。這表示當您採取動作 (例如重新啟動資源或變更與資源相關聯的標籤) 時，會產生尋找項目的新事件。不過，`id`欄位中的尋找項目 ID 會保持不變。盡可能發出事件。

> **Note**
>
> 如果您的帳戶是 Amazon Inspector 委派的管理員，除了將事件 EventBridge 發佈到您的帳戶，還會將事件發佈到您的帳戶中。

當您將 EventBridge 事件與 Amazon Inspector 搭配使用時，您可以自動化任務以協助您回應 Amazon Inspector 發現項目所顯示的安全問題。

Amazon Inspector 會將事件發送到相同區域中的預設事件匯流排。這表示您必須為執行 Amazon Inspector 的每個區域設定事件規則，才能查看該區域的事件。

若要根據 EventBridge 事件接收有關 Amazon Inspector 發現項目的通知，您必須為 Amazon Inspector 建立 EventBridge 規則和目標。此規則允許 EventBridge 針對 Amazon Inspector 產生的發現項目傳送通知到規則中指定的目標。如需詳細資訊，請參閱 Amazon EventBridge 使用者指南中的 Amazon EventBridge 規則。

事件模式

以下是 EC2 尋找事件的 Amazon Inspector 事件格式範例。如需其他尋找項目類型和事件類型的綱要範例，請參閱EventBridge 架構。

```
{
    "version": "0",
    "id": "66a7a279-5f92-971c-6d3e-c92da0950992",
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-19T22:46:15Z",
    "region": "us-east-1",
    "resources": ["i-0c2a343f1948d5205"],
    "detail": {
        "awsAccountId": "111122223333",
        "description": "\n It was discovered that the sound subsystem in the Linux
 kernel contained a\n race condition in some situations. A local attacker could use
 this to cause\n a denial of service (system crash).",
        "exploitAvailable": "YES",
        "exploitabilityDetails": {
            "lastKnownExploitAt": "Oct 24, 2022, 11:08:59 PM"
        },
        "findingArn": "arn:aws:inspector2:us-east-1:111122223333:finding/FINDING_ID",
```

```
        "firstObservedAt": "Jan 19, 2023, 10:46:15 PM",
        "fixAvailable": "YES",
        "lastObservedAt": "Jan 19, 2023, 10:46:15 PM",
        "packageVulnerabilityDetails": {
            "cvss": [{
                "baseScore": 4.7,
                "scoringVector": "CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H",
                "source": "NVD",
                "version": "3.1"
            }],
            "referenceUrls": ["https://lore.kernel.org/all/
CAFcO6XN7JDM4xSXGhtusQfS2mSBcx50VJKwQpCq=WeLt57aaZA@mail.gmail.com/", "https://
ubuntu.com/security/notices/USN-5792-1", "https://ubuntu.com/security/notices/
USN-5791-2", "https://ubuntu.com/security/notices/USN-5791-1", "https://ubuntu.com/
security/notices/USN-5793-2", "https://git.kernel.org/pub/scm/linux/kernel/git/
torvalds/linux.git/commit/?id=8423f0b6d513b259fdab9c9bf4aaa6188d054c2d", "https://
ubuntu.com/security/notices/USN-5793-1", "https://ubuntu.com/security/notices/
USN-5792-2", "https://ubuntu.com/security/notices/USN-5791-3", "https://ubuntu.com/
security/notices/USN-5793-4", "https://ubuntu.com/security/notices/USN-5793-3",
 "https://git.kernel.org/linus/8423f0b6d513b259fdab9c9bf4aaa6188d054c2d(6.0-rc5)",
 "https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3303"],
            "relatedVulnerabilities": [],
            "source": "UBUNTU_CVE",
            "sourceUrl": "https://people.canonical.com/~ubuntu-security/cve/2022/
CVE-2022-3303.html",
            "vendorCreatedAt": "Sep 27, 2022, 11:15:00 PM",
            "vendorSeverity": "medium",
            "vulnerabilityId": "CVE-2022-3303",
            "vulnerablePackages": [{
                "arch": "X86_64",
                "epoch": 0,
                "fixedInVersion": "0:5.15.0.1027.31~20.04.16",
                "name": "linux-image-aws",
                "packageManager": "OS",
                "remediation": "apt update && apt install --only-upgrade linux-image-
aws",
                "version": "5.15.0.1026.30~20.04.16"
            }]
        },
        "remediation": {
            "recommendation": {
                "text": "None Provided"
            }
        },
```

```
        "resources": [{
            "details": {
                "awsEc2Instance": {
                    "iamInstanceProfileArn": "arn:aws:iam::111122223333:instance-
profile/AmazonSSMRoleForInstancesQuickSetup",
                    "imageId": "ami-0b7ff1a8d69f1bb35",
                    "ipV4Addresses": ["172.31.85.212", "44.203.45.27"],
                    "ipV6Addresses": [],
                    "launchedAt": "Jan 19, 2023, 7:53:14 PM",
                    "platform": "UBUNTU_20_04",
                    "subnetId": "subnet-8213f2a3",
                    "type": "t2.micro",
                    "vpcId": "vpc-ab6650d1"
                }
            },
            "id": "i-0c2a343f1948d5205",
            "partition": "aws",
            "region": "us-east-1",
            "type": "AWS_EC2_INSTANCE"
        }],
        "severity": "MEDIUM",
        "status": "ACTIVE",
        "title": "CVE-2022-3303 - linux-image-aws",
        "type": "PACKAGE_VULNERABILITY",
        "updatedAt": "Jan 19, 2023, 10:46:15 PM"
    }
}
```


建立 EventBridge 規則以通知您 Amazon Inspector 發現

若要提高 Amazon Inspector 發現項目的可見度，您可 EventBridge 以使用設定傳送至簡訊中樞的自動尋找提醒。本主題說明如何將發現的警示CRITICAL和HIGH嚴重性發現項目傳送至電子郵件、Slack 或 Amazon Chime。您將學習如何設定 Amazon 簡單通知服務主題，然後將該主題連接到 EventBridge 事件規則。

步驟 1. 設定 Amazon SNS 主題和端點

若要設定自動提醒，您必須先在 Amazon 簡單通知服務中設定主題，然後新增端點。如需詳細資訊，請參閱 SNS 指南。

此程序會建立您要傳送 Amazon Inspector 發現項目資料的位置。在建立 EventBridge 事件規則期間或之後，可將 SNS 主題新增至事件規則。

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. 從導覽窗格中，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**`Inspector_to_Email`**。其他詳細資料是選擇性的。
4. 選擇建立主題。這將打開一個新面板，其中包含新主題的詳細信息。
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，輸入您要接收通知的電子郵件地址。

   > **Note**
   >
   > 創建訂閱後，您將需要通過電子郵件客戶端確認您的訂閱。

   c. 選擇建立訂閱。
7. 在收件匣中尋找訂閱訊息，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. 從導覽窗格中，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**`Inspector_to_Slack`**。其他詳細資料是選擇性的。選擇「建立主題」以完成端點建立。

設定用 AWS Chatbot 戶端

1. 瀏覽至 AWS Chatbot 主控台，位於https://console.aws.amazon.com/chatbot/。
2. 在「設定的用戶端」窗格中，選取「設定新用戶端」
3. 選擇「鬆弛」，然後選擇「設定」以確認。

> **Note**
>
> 選擇 Slack 時，您必須選取 [允許] AWS Chatbot 以確認存取頻道的權限。

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，請選擇您要使用的頻道。
   c. 在 Slack 中，以滑鼠右鍵按一下頻道名稱並選取「複製連結」，以複製私人通道的通道 ID。
   d. 在 AWS Chatbot 視窗中 AWS Management Console，將您從 Slack 複製的通道 ID 貼到「私人通道 ID」欄位中。
   e. 在許可中，如果您還沒有角色，請選擇使用範本建立 IAM 角色。
   f. 針對策略範本，請選擇 [通知權限]。這是的 IAM 政策範本 AWS Chatbot。此政策為 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. 對於頻道護欄策略，請選擇 AmazonInspector 2。ReadOnlyAccess
   h. 選擇您先前建立 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。

Amazon 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. 從導覽窗格中選取 [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**`Inspector_to_Chime`**。其他詳細資料是選擇性的。選擇 [建立主題] 以完成。

設定用 AWS Chatbot 戶端

1. 瀏覽至 AWS Chatbot 主控台，位於https://console.aws.amazon.com/chatbot/。
2. 從設定的用戶端面板中，選取設定新用戶端。
3. 選擇「鈴聲」，然後選擇「設定」以確認。

4. 在組態詳細資訊窗格中，輸入頻道的名稱。
5. 在 Amazon 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 Chatbot 視窗中 AWS Management Console，將您複製的網址貼到「Webhook 網址」欄位中。
7. 在許可中，如果您還沒有角色，請選擇使用範本建立 IAM 角色。
8. 針對策略範本，請選擇 [通知權限]。這是的 IAM 政策範本 AWS Chatbot。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，將通知傳送到 Amazon Chime 會議室。
10. 選取設定。

步驟 2. 為 Amazon Inspector 發現創建 EventBridge 規則

1. 在以下位置打開 Amazon EventBridge 控制台 https://console.aws.amazon.com/events/。
2. 從導覽窗格中選取 [規則]，然後選取 [建立規則]。
3. 輸入規則的名稱和選擇性說明。
4. 選取具有事件模式的規則，然後選取下一步。
5. 在 [事件模式] 窗格中，選擇 [自訂模式 (JSON 編輯器)]。
6. 將以下 JSON 貼至編輯器中。

```
{
  "source": ["aws.inspector2"],
  "detail-type": ["Inspector2 Finding"],
  "detail": {
    "severity": ["HIGH", "CRITICAL"],
    "status": ["ACTIVE"]
  }
}
```

> **Note**
>
> 此模式會針對 Amazon Inspector 偵測到的任何使用中`CRITICAL`或`HIGH`嚴重性發現傳送通知。

完成輸入事件模式後，請選取 [下一步]。

7. 在「選取目標」 頁面上，選擇AWS 服務。然後，針對 [選取目標類型] 選擇 [SNS 主題]。
8. 針對「主題」，選取您在步驟 1 中建立的 SNS 主題名稱。然後選擇下一步。
9. 視需要新增可選標籤，然後選擇「下一步」
10. 檢閱規則，然後選擇 [建立規則]。

EventBridge 適用於 Amazon Inspector 多帳戶環境

如果您是 Amazon Inspector 委派的管理員， EventBridge 則會根據您會員帳戶中的適用發現項目，在您的帳戶中顯示規則。如果您透過 EventBridge 管理員帳戶設定發現項目通知 (如上一節所述)，您將會收到有關多個帳戶的通知。換句話說，除了您自己的帳戶生成的發現和事件之外，還會通知您會員帳戶產生的發現和事件。

您可以使用`accountId`來自發現項目的 JSON 詳細資料來識別 Amazon Inspector 尋找來源的成員帳戶。

使用 Amazon Inspector 匯出 sBOM

您可以使用 Amazon Inspector 主控台或 API 為您的資源產生軟體材料清單 (SBOM)。SBOM 是程式碼庫中所有開放原始碼和協力廠商軟體元件的巢狀清查。Amazon Inspector 為您環境中的個別資源提供 SBOM。從 Amazon Inspector 匯出的 sBOM 可協助您瞭解軟體供應的相關資訊，例如最常用的套件，以及組織中相關的弱點。

您可以針對 Amazon Inspector 主動監控的所有受支援資源匯出 SBOM。您可以透過以下方式檢閱資源的狀態評估您 AWS 環境的 Amazon Inspector 覆蓋率。

> **Note**
>
> Amazon Inspector 不支援匯出適用於 Windows EC2 執行個體的 SBOM。

Amazon Inspector 格式

Amazon Inspector 支持以循環 1.4 和 SPDX 2.3 兼容格式導出 SBOM。Amazon Inspector 將 SBOM 作為JSON文件導出到您選擇的 Amazon S3 存儲桶。

> **Note**
>
> 來自 Amazon Inspector 的 SPDX 格式導出與使用 SPDX 2.3 的系統兼容，但它們不包含創用共享零（CC0）字段。這是因為包含此字段將允許用戶重新分發或編輯材料。

來自 Amazon Inspector 的循環式 1.4 SBOM 格式的示例

```
                {
"bomFormat": "CycloneDX",
"specVersion": "1.4",
"version": 1,
"metadata": {
  "timestamp": "2023-06-02T01:17:46Z",
  "component": null,
  "properties": [
    {
      "name": "imageId",
```

```
        "value":
 "sha256:c8ee97f7052776ef223080741f61fcdf6a3a9107810ea9649f904aa4269fdac6"
      },
      {
        "name": "architecture",
        "value": "arm64"
      },
      {
        "name": "accountId",
        "value": "111122223333"
      },
      {
        "name": "resourceType",
        "value": "AWS_ECR_CONTAINER_IMAGE"
      }
    ]
  },
  "components": [
    {
      "type": "library",
      "name": "pip",
      "purl": "pkg:pypi/pip@22.0.4?path=usr/local/lib/python3.8/site-packages/
pip-22.0.4.dist-info/METADATA",
      "bom-ref": "98dc550d1e9a0b24161daaa0d535c699"
    },
    {
      "type": "application",
      "name": "libss2",
      "purl": "pkg:dpkg/libss2@1.44.5-1+deb10u3?
arch=ARM64&epoch=0&upstream=libss2-1.44.5-1+deb10u3.src.dpkg",
      "bom-ref": "2f4d199d4ef9e2ae639b4f8d04a813a2"
    },
    {
      "type": "application",
      "name": "liblz4-1",
      "purl": "pkg:dpkg/liblz4-1@1.8.3-1+deb10u1?
arch=ARM64&epoch=0&upstream=liblz4-1-1.8.3-1+deb10u1.src.dpkg",
      "bom-ref": "9a6be8907ead891b070e60f5a7b7aa9a"
    },
    {
      "type": "application",
      "name": "mawk",
      "purl": "pkg:dpkg/mawk@1.3.3-17+b3?
arch=ARM64&epoch=0&upstream=mawk-1.3.3-17+b3.src.dpkg",
```

```
      "bom-ref": "c2015852a729f97fde924e62a16f78a5"
    },
    {
      "type": "application",
      "name": "libgmp10",
      "purl": "pkg:dpkg/libgmp10@6.1.2+dfsg-4+deb10u1?
arch=ARM64&epoch=2&upstream=libgmp10-6.1.2+dfsg-4+deb10u1.src.dpkg",
      "bom-ref": "52907290f5beef00dff8da77901b1085"
    },
    {
      "type": "application",
      "name": "ncurses-bin",
      "purl": "pkg:dpkg/ncurses-bin@6.1+20181013-2+deb10u3?
arch=ARM64&epoch=0&upstream=ncurses-bin-6.1+20181013-2+deb10u3.src.dpkg",
      "bom-ref": "cd20cfb9ebeeadba3809764376f43bce"
    }
  ],
  "vulnerabilities": [
    {
      "id": "CVE-2022-40897",
      "affects": [
        {
          "ref": "a74a4862cc654a2520ec56da0c81cdb3"
        },
        {
          "ref": "0119eb286405d780dc437e7dbf2f9d9d"
        }
      ]
    }
  ]
}
```

從 Amazon Inspector SPDX 2.3 SBOM 格式的示例

```
{
 "name": "409870544328/EC2/i-022fba820db137c64/ami-074ea14c08effb2d8",
 "spdxVersion": "SPDX-2.3",
 "creationInfo": {
  "created": "2023-06-02T21:19:22Z",
  "creators": [
   "Organization: 409870544328",
```

```
    "Tool: Amazon Inspector SBOM Generator"
   ]
  },
  "documentNamespace": "EC2://i-022fba820db137c64/AMAZON_LINUX_2/null/x86_64",
  "comment": "",
  "packages": [{
    "name": "elfutils-libelf",
    "versionInfo": "0.176-2.amzn2",
    "downloadLocation": "NOASSERTION",
    "sourceInfo": "/var/lib/rpm/Packages",
    "filesAnalyzed": false,
    "externalRefs": [{
     "referenceCategory": "PACKAGE-MANAGER",
     "referenceType": "purl",
     "referenceLocator": "pkg:rpm/elfutils-libelf@0.176-2.amzn2?
arch=X86_64&epoch=0&upstream=elfutils-libelf-0.176-2.amzn2.src.rpm"
    }],
    "SPDXID": "SPDXRef-Package-rpm-elfutils-libelf-ddf56a513c0e76ab2ae3246d9a91c463"
   },
   {
    "name": "libcurl",
    "versionInfo": "7.79.1-1.amzn2.0.1",
    "downloadLocation": "NOASSERTION",
    "sourceInfo": "/var/lib/rpm/Packages",
    "filesAnalyzed": false,
    "externalRefs": [{
      "referenceCategory": "PACKAGE-MANAGER",
      "referenceType": "purl",
      "referenceLocator": "pkg:rpm/libcurl@7.79.1-1.amzn2.0.1?
arch=X86_64&epoch=0&upstream=libcurl-7.79.1-1.amzn2.0.1.src.rpm"
     },
     {
      "referenceCategory": "SECURITY",
      "referenceType": "vulnerability",
      "referenceLocator": "CVE-2022-32205"
     }
    ],
    "SPDXID": "SPDXRef-Package-rpm-libcurl-710fb33829bc5106559bcd380cddb7d5"
   },
   {
    "name": "hunspell-en-US",
    "versionInfo": "0.20121024-6.amzn2.0.1",
    "downloadLocation": "NOASSERTION",
    "sourceInfo": "/var/lib/rpm/Packages",
```

```
   "filesAnalyzed": false,
   "externalRefs": [{
    "referenceCategory": "PACKAGE-MANAGER",
    "referenceType": "purl",
    "referenceLocator": "pkg:rpm/hunspell-en-US@0.20121024-6.amzn2.0.1?
arch=NOARCH&epoch=0&upstream=hunspell-en-US-0.20121024-6.amzn2.0.1.src.rpm"
   }],
   "SPDXID": "SPDXRef-Package-rpm-hunspell-en-US-de19ae0883973d6cea5e7e079d544fe5"
  },
  {
   "name": "grub2-tools-minimal",
   "versionInfo": "2.06-2.amzn2.0.6",
   "downloadLocation": "NOASSERTION",
   "sourceInfo": "/var/lib/rpm/Packages",
   "filesAnalyzed": false,
   "externalRefs": [{
     "referenceCategory": "PACKAGE-MANAGER",
     "referenceType": "purl",
     "referenceLocator": "pkg:rpm/grub2-tools-minimal@2.06-2.amzn2.0.6?
arch=X86_64&epoch=1&upstream=grub2-tools-minimal-2.06-2.amzn2.0.6.src.rpm"
    },
    {
     "referenceCategory": "SECURITY",
     "referenceType": "vulnerability",
     "referenceLocator": "CVE-2021-3981"
    }
   ],
   "SPDXID": "SPDXRef-Package-rpm-grub2-tools-minimal-c56b7ea76e5a28ab8f232ef6d7564636"
  },
  {
   "name": "unixODBC-devel",
   "versionInfo": "2.3.1-14.amzn2",
   "downloadLocation": "NOASSERTION",
   "sourceInfo": "/var/lib/rpm/Packages",
   "filesAnalyzed": false,
   "externalRefs": [{
    "referenceCategory": "PACKAGE-MANAGER",
    "referenceType": "purl",
    "referenceLocator": "pkg:rpm/unixODBC-devel@2.3.1-14.amzn2?
arch=X86_64&epoch=0&upstream=unixODBC-devel-2.3.1-14.amzn2.src.rpm"
   }],
   "SPDXID": "SPDXRef-Package-rpm-unixODBC-devel-1bb35add92978df021a13fc9f81237d2"
  }
 ],
```

```
 "relationships": [{
   "spdxElementId": "SPDXRef-DOCUMENT",
   "relatedSpdxElement": "SPDXRef-Package-rpm-elfutils-libelf-
ddf56a513c0e76ab2ae3246d9a91c463",
   "relationshipType": "DESCRIBES"
  },
  {
   "spdxElementId": "SPDXRef-DOCUMENT",
   "relatedSpdxElement": "SPDXRef-Package-rpm-yajl-8476ce2db98b28cfab2b4484f84f1903",
   "relationshipType": "DESCRIBES"
  },
  {
   "spdxElementId": "SPDXRef-DOCUMENT",
   "relatedSpdxElement": "SPDXRef-Package-rpm-unixODBC-
devel-1bb35add92978df021a13fc9f81237d2",
   "relationshipType": "DESCRIBES"
  }
 ],
 "SPDXID": "SPDXRef-DOCUMENT"
}
```

適用於 sBOM 的篩選器

匯出 sBOM 時，您可以包含篩選器，以針對特定資源子集建立報告。如果您未提供篩選器，則會匯出所有作用中的 sBOM，則會匯出支援的資源。如果您是委派的系統管理員，也會包含所有成員的資源。可用的篩選條件如下：

- AccountID — 此篩選器可用來匯出與特定帳號 ID 相關聯之任何資源的 sBOM。
- EC2 執行個體標籤 — 此篩選器可用於匯出具有特定標籤之 EC2 執行個體的 sBOM。
- 函數名稱 — 此篩選器可用來匯出特定 Lambda 函數的 sBOM。
- 影像標籤 — 此篩選器可用來匯出具有特定標籤之容器映像的 sBOM。
- Lambda 函數標籤 — 此篩選器可用來匯出具有特定標籤之 Lambda 函數的 SBOM。
- 資源類型 — 此篩選器可用來篩選資源類型：EC2/ECR/Lambda。
- 資源 ID — 此篩選器可用來匯出特定資源的 SBOM。
- 存放庫名稱 — 此篩選器可用來為特定儲存庫中的容器映像產生 sBOM。

配置及匯出 SBOM

若要匯出 sBOM，您必須先設定 Amazon S3 儲存貯體和允許 Amazon Inspector 使用的 AWS KMS 金鑰。您可以使用篩選器來匯出資源之特定子集的 SBOM。若要匯出 AWS 組織中多個帳戶的 SBOM，請在以 Amazon Inspector 委派的管理員身分登入時遵循下列步驟。

必要條件

- 支援的資源正由 Amazon Inspector 主動監控。
- Amazon S3 儲存貯體設定了允許 Amazon Inspector 將物件新增至的政策。如需有關設定原則的資訊，請參閱設定匯出權限。
- 使用政策設定的 AWS KMS 金鑰，可讓 Amazon Inspector 用來加密您的報告。如需設定原則的相關資訊，請參閱設定匯出 AWS KMS 金鑰。

> **Note**
>
> 如果您先前已設定 Amazon S3 儲存貯體和發現項目匯出的 AWS KMS 金鑰，則可以使用相同的儲存貯體和金鑰進行 SBOM 匯出。

選擇您偏好的存取方法以匯出 SBOM。

Console

1. 在 https://console.aws.amazon.com/inspector/v2/home 打開 Amazon Inspector 控制台。
2. 使用頁面右上角的選取 AWS 區域 器，選取包含您要匯出 SBOM 的資源的「區域」。
3. 在導覽窗格中，選擇「匯出 SBOM」。
4. (選擇性) 在 [匯出 sBOM] 頁面中，使用 [新增篩選器] 功能表選取要建立報表的資源子集。如果沒有提供過濾器，Amazon Inspector 將導出所有活動資源的報告。如果您是委派管理員，則會包含組織中的所有使用中資源。
5. 在「匯出設定」下，選取您要用於 SBOM 的格式。
6. 輸入 Amazon S3 URI，或選擇瀏覽 Amazon S3 以選擇用於存放 SBOM 的 Amazon S3 位置。
7. 輸入為 Amazon Inspector 設定的AWS KMS 金鑰，以用來加密您的報告。

API

- 若要以程式設計方式匯出資源的 SBOM，請使用 Amazon Inspector API 的CreateSbomExport作業。

  在您的請求中，使用reportFormat參數來指定 SBOM 輸出格式，然後選擇CYCLONEDX_1_4或SPDX_2_3。此s3Destination參數為必要參數，您必須指定一個 S3 儲存貯體，其政策可讓 Amazon Inspector 寫入該儲存貯體。選擇性地使用resourceFilterCriteria參數，將報表的範圍限制為特定資源。

AWS CLI

- 若要使用 AWS Command Line Interface 執行下列命令匯出資源的 SBOM：

  ```
  aws inspector2 create-sbom-export --report-format
  FORMAT --s3-destination bucketName=DOC-EXAMPLE-
  BUCKET1,keyPrefix=PREFIX,kmsKeyArn=arn:aws:kms:Region:111122223333:key/123
  ```

  在您的請求中，將 *FORMA* T 替換為您選擇的格式，CYCLONEDX_1_4或SPDX_2_3。然後，將 s3 目標的名稱取代*user input placeholders*為要匯出目的地的 S3 儲存貯體名稱、用於 S3 輸出的前置詞，以及用於加密報告的 KMS 金鑰的 ARN。

Amazon Inspector 漏洞數據庫

您可以在 Amazon Inspector 弱點資料庫中搜尋漏洞和暴露 (CVE)。Amazon Inspector 會使用弱點資料庫中的資訊產生與 CVE ID 相關的詳細資訊。您可以在 CVE 詳細資訊頁面中存取這些詳細資料。

本主題說明如何使用 CVE ID 搜尋 Amazon Inspector 易受攻擊性資料庫，以及如何互動 CVE 詳細資料頁面。如需發現項目的資訊，請參閱Amazon Inspector 找到細節。

> **Note**
>
> Amazon Inspector 會追蹤並產生資料庫中其他軟體弱點的發現項目。不過，Amazon Inspector 僅支援 CVE 詳細資料頁面之 [偵測平台] 區段中所列平台的 CVE。目前 CVE 搜尋不支援 Microsoft Windows。

搜尋弱點資料庫

本節說明如何在主控台和 Amazon Inspector API 中搜尋弱點資料庫。

> **Note**
>
> 您必須先啟用目 AWS 區域 前的 Amazon Inspector，才能搜尋弱點資料庫。

Console

1. 打開 Amazon Inspector 控制台 https://console.aws.amazon.com/inspector/
2. 在瀏覽窗格中，選擇弱點資料庫搜尋。
3. 在搜尋列中，輸入 CVE ID，然後選擇「搜尋」。

API

執行 Amazon Inspector SearchVulnerabilitiesAPI，並提供單一 CVE ID，如`filterCriteria`下列格式所示：`CVE-<year>-<ID>`

瞭解 CVE 詳細資料

本節說明如何互動 CVE 詳細資料頁面。

CVE 詳細資料

CVE 詳細資料區段包含下列資訊：

- CVE 說明和識別碼
- CVE 嚴重性
- 常見漏洞評分系統（CVSS）和漏洞利用預測評分系統（EPSS）分數
- 偵測平台

> **Note**
>
> 如果此欄位為空白，Amazon Inspector 不支援偵測您的 CVE ID。

- 常見弱點枚舉 (CWE)
- 供應商建立與更新日期

弱點情報

弱點情報區段提供威脅情報資料，例如攻擊目標和上次已知的公開攻擊日期。

它也提供來自網路安全與基礎架構安全機構 (CISA) 的資料，其中包括修復動作、將 CVE 新增至已知惡意利用弱點目錄的日期，以及 CISA 預期聯邦機構修復 CVE 的日期。

參考

參照區段提供資源連結，以取得有關 CVE 的詳細資訊。

Amazon EventBridge 事件模式 Amazon Inspector 事件

為了支援與其他應用程式、服務和系統 (例如監控或事件管理系統) 的整合，Amazon Inspector 會自動將發現結果 EventBridge 作為事件發佈到 Amazon。 EventBridge是一種無伺服器事件匯流排服務，可將來自應用程式和其他應用程式的即時資料串流傳遞 AWS 服務 至 AWS Lambda 功能、Amazon 簡單通知服務主題和 Amazon Kinesis Data Streams 等目標。若要進一步了解 EventBridge 和 EventBridge 活動，請參閱 Amazon EventBridge 使用者指南。

Amazon Inspector 會發佈有關發現項目、資源涵蓋範圍變更以及個別資源初始掃描的事件。每個事件都是符合事件結構 EventBridge 描述的 JSON 物件。 AWS 由於資料結構為 EventBridge 事件，因此您可以使用其他應用程式、服務和工具，更輕鬆地監控、處理發現項目和支援的 Amazon Inspector 事件並採取行動。

主題

Amazon 檢查器的亞馬遜 EventBridge 基本模

以下是 Amazon Inspector EventBridge 事件的基本結構描述範例。活動詳細資訊會根據事件類型而有所不同。

```
{
    "version": "0",
    "id": "Event ID",
    "detail-type": "Inspector2 *event type*",
    "source": "aws.inspector2",
    "account": "AWS ## ID (string)",
    "time": "event timestamp (string)",
    "region": "AWS ## (string)",
    "resources": [
        *IDs or ARNs of the resources involved in the event*
    ],
    "detail": {
        *Details of an Amazon Inspector event type*
    }
```

```
}
```

Amazon Inspector 發現事件模式示例

以下是 Amazon Inspector 發現項目 EventBridge 事件的結構描述範例。當 Amazon Inspector 在您的其中一個資源中發現軟體弱點或網路問題時，就會建立尋找事件。如需建立通知以回應此類事件的指南，請參閱使用 Amazon 創建對 Amazon Inspector 發現的自定義 EventBridge。

下列欄位可識別搜尋結果事件：

- `detail-type`欄位設定為`Inspector2 Finding`。
- `detail`物件描述發現項目。

從選項中選取，以查看尋找不同資源的事件綱要和尋找類型。

Amazon EC2 package vulnerability finding

```
{
    "version": "0",
    "id": "66a7a279-5f92-971c-6d3e-c92da0950992",
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-19T22:46:15Z",
    "region": "us-east-1",
    "resources": ["i-0c2a343f1948d5205"],
    "detail": {
        "awsAccountId": "111122223333",
        "description": "\n It was discovered that the sound subsystem in the Linux
 kernel contained a\n race condition in some situations. A local attacker could use
 this to cause\n a denial of service (system crash).",
        "exploitAvailable": "YES",
        "exploitabilityDetails": {
            "lastKnownExploitAt": "Oct 24, 2022, 11:08:59 PM"
        },
        "findingArn": "arn:aws:inspector2:us-east-1:111122223333:finding/
FINDING_ID",
        "firstObservedAt": "Jan 19, 2023, 10:46:15 PM",
        "fixAvailable": "YES",
        "lastObservedAt": "Jan 19, 2023, 10:46:15 PM",
```

```
        "packageVulnerabilityDetails": {
            "cvss": [{
                "baseScore": 4.7,
                "scoringVector": "CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H",
                "source": "NVD",
                "version": "3.1"
            }],
            "referenceUrls": ["https://lore.kernel.org/all/
CAFcO6XN7JDM4xSXGhtusQfS2mSBcx50VJKwQpCq=WeLt57aaZA@mail.gmail.com/", "https://
ubuntu.com/security/notices/USN-5792-1", "https://ubuntu.com/security/notices/
USN-5791-2", "https://ubuntu.com/security/notices/USN-5791-1", "https://ubuntu.com/
security/notices/USN-5793-2", "https://git.kernel.org/pub/scm/linux/kernel/git/
torvalds/linux.git/commit/?id=8423f0b6d513b259fdab9c9bf4aaa6188d054c2d", "https://
ubuntu.com/security/notices/USN-5793-1", "https://ubuntu.com/security/notices/
USN-5792-2", "https://ubuntu.com/security/notices/USN-5791-3", "https://ubuntu.com/
security/notices/USN-5793-4", "https://ubuntu.com/security/notices/USN-5793-3",
 "https://git.kernel.org/linus/8423f0b6d513b259fdab9c9bf4aaa6188d054c2d(6.0-rc5)",
 "https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3303"],
            "relatedVulnerabilities": [],
            "source": "UBUNTU_CVE",
            "sourceUrl": "https://people.canonical.com/~ubuntu-security/cve/2022/
CVE-2022-3303.html",
            "vendorCreatedAt": "Sep 27, 2022, 11:15:00 PM",
            "vendorSeverity": "medium",
            "vulnerabilityId": "CVE-2022-3303",
            "vulnerablePackages": [{
                "arch": "X86_64",
                "epoch": 0,
                "fixedInVersion": "0:5.15.0.1027.31~20.04.16",
                "name": "linux-image-aws",
                "packageManager": "OS",
                "remediation": "apt update && apt install --only-upgrade linux-
image-aws",
                "version": "5.15.0.1026.30~20.04.16"
            }]
        },
        "remediation": {
            "recommendation": {
                "text": "None Provided"
            }
        },
        "resources": [{
            "details": {
                "awsEc2Instance": {
```

```
                    "iamInstanceProfileArn": "arn:aws:iam::111122223333:instance-
profile/AmazonSSMRoleForInstancesQuickSetup",
                    "imageId": "ami-0b7ff1a8d69f1bb35",
                    "ipV4Addresses": ["172.31.85.212", "44.203.45.27"],
                    "ipV6Addresses": [],
                    "launchedAt": "Jan 19, 2023, 7:53:14 PM",
                    "platform": "UBUNTU_20_04",
                    "subnetId": "subnet-8213f2a3",
                    "type": "t2.micro",
                    "vpcId": "vpc-ab6650d1"
                }
            },
            "id": "i-0c2a343f1948d5205",
            "partition": "aws",
            "region": "us-east-1",
            "type": "AWS_EC2_INSTANCE"
        }],
        "severity": "MEDIUM",
        "status": "ACTIVE",
        "title": "CVE-2022-3303 - linux-image-aws",
        "type": "PACKAGE_VULNERABILITY",
        "updatedAt": "Jan 19, 2023, 10:46:15 PM"
    }
}
```

Amazon EC2 network reachability finding

```
{
    "version": "0",
    "id": "d0384f63-1621-1b75-d014-a5e45628ef3e",
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-20T09:17:57Z",
    "region": "us-east-1",
    "resources": ["i-0a96278c2206a8e4b"],
    "detail": {
        "awsAccountId": "111122223333",
        "description": "On the instance i-0a96278c2206a8e4b, the port range
 22-22 is reachable from the InternetGateway igw-72069c09 from an attached ENI
 eni-0976efe678170408f.",
```

```
        "findingArn": "arn:aws:inspector2:us-east-1:111122223333:finding/
FINDING_ID",
        "firstObservedAt": "Jan 20, 2023, 9:17:57 AM",
        "lastObservedAt": "Jan 20, 2023, 9:17:57 AM",
        "networkReachabilityDetails": {
            "networkPath": {
                "steps": [{
                    "componentId": "igw-72069c09",
                    "componentType": "AWS::EC2::InternetGateway"
                }, {
                    "componentId": "acl-91d74eec",
                    "componentType": "AWS::EC2::NetworkAcl"
                }, {
                    "componentId": "sg-0aaed0af450bd0165",
                    "componentType": "AWS::EC2::SecurityGroup"
                }, {
                    "componentId": "eni-0976efe678170408f",
                    "componentType": "AWS::EC2::NetworkInterface"
                }, {
                    "componentId": "i-0a96278c2206a8e4b",
                    "componentType": "AWS::EC2::Instance"
                }]
            },
            "openPortRange": {
                "begin": 22,
                "end": 22
            },
            "protocol": "TCP"
        },
        "remediation": {
            "recommendation": {
                "text": "You can restrict access to your instance by modifying the
 Security Groups or ACLs in the network path."
            }
        },
        "resources": [{
            "details": {
                "awsEc2Instance": {
                    "iamInstanceProfileArn": "arn:aws:iam::111122223333:instance-
profile/AmazonSSMRoleForInstancesQuickSetup",
                    "imageId": "ami-0b5eea76982371e91",
                    "ipV4Addresses": ["3.89.90.19", "172.31.93.57"],
                    "ipV6Addresses": [],
                    "keyName": "example-inspector-test",
```

```
                    "launchedAt": "Jan 19, 2023, 7:25:02 PM",
                    "platform": "AMAZON_LINUX_2",
                    "subnetId": "subnet-8213f2a3",
                    "type": "t2.micro",
                    "vpcId": "vpc-ab6650d1"
                }
            },
            "id": "i-0a96278c2206a8e4b",
            "partition": "aws",
            "region": "us-east-1",
            "type": "AWS_EC2_INSTANCE"
        }],
        "severity": "MEDIUM",
        "status": "ACTIVE",
        "title": "Port 22 is reachable from an Internet Gateway",
        "type": "NETWORK_REACHABILITY",
        "updatedAt": "Jan 20, 2023, 9:17:57 AM"
    }
}
```

Amazon ECR package vulnerability finding

```
{
    "version": "0",
    "id": "5b52952e-26df-3a51-6d14-4dbe737e58ec",
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-19T21:59:00Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ecr:us-east-1:111122223333:repository/inspector2/
sha256:98f0304b3a3b7c12ce641177a99d1f3be56f532473a528fda38d53d519cafb13"
    ],
    "detail": {
        "awsAccountId": "111122223333",
        "description": "libcurl would reuse a previously created connection even
 when a TLS or SSHrelated option had been changed that should have prohibited
 reuse.libcurl keeps previously used connections in a connection pool for
 subsequenttransfers to reuse if one of them matches the setup. However, several TLS
```

```
 andSSH settings were left out from the configuration match checks, making themmatch
 too easily.",
        "exploitAvailable": "NO",
        "findingArn": "arn:aws:inspector2:us-east-1:111122223333:finding/
FINDING_ID",
        "firstObservedAt": "Jan 19, 2023, 9:59:00 PM",
        "fixAvailable": "YES",
        "inspectorScore": 7.5,
        "inspectorScoreDetails": {
            "adjustedCvss": {
                "adjustments": [],
                "cvssSource": "NVD",
                "score": 7.5,
                "scoreSource": "NVD",
                "scoringVector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N",
                "version": "3.1"
            }
        },
        "lastObservedAt": "Jan 19, 2023, 9:59:00 PM",
        "packageVulnerabilityDetails": {
            "cvss": [
                {
                    "baseScore": 5,
                    "scoringVector": "AV:N/AC:L/Au:N/C:N/I:P/A:N",
                    "source": "NVD",
                    "version": "2.0"
                },
                {
                    "baseScore": 7.5,
                    "scoringVector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N",
                    "source": "NVD",
                    "version": "3.1"
                }
            ],
            "referenceUrls": [
                "https://hackerone.com/reports/1555796",
                "https://security.gentoo.org/glsa/202212-01",
                "https://lists.debian.org/debian-lts-announce/2022/08/
msg00017.html",
                "https://www.debian.org/security/2022/dsa-5197"
            ],
            "relatedVulnerabilities": [],
            "source": "NVD",
            "sourceUrl": "https://nvd.nist.gov/vuln/detail/CVE-2022-27782",
```

```
            "vendorCreatedAt": "Jun 2, 2022, 2:15:00 PM",
            "vendorSeverity": "HIGH",
            "vendorUpdatedAt": "Jan 5, 2023, 5:51:00 PM",
            "vulnerabilityId": "CVE-2022-27782",
            "vulnerablePackages": [
                {
                    "arch": "X86_64",
                    "epoch": 0,
                    "fixedInVersion": "0:7.61.1-22.el8_6.3",
                    "name": "libcurl",
                    "packageManager": "OS",
                    "release": "22.el8",
                    "remediation": "yum update libcurl",
                    "sourceLayerHash":
"sha256:38a980f2cc8accf69c23deae6743d42a87eb34a54f02396f3fcfd7c2d06e2c5b",
                    "version": "7.61.1"
                },
                {
                    "arch": "X86_64",
                    "epoch": 0,
                    "fixedInVersion": "0:7.61.1-22.el8_6.3",
                    "name": "curl",
                    "packageManager": "OS",
                    "release": "22.el8",
                    "remediation": "yum update curl",
                    "sourceLayerHash":
"sha256:38a980f2cc8accf69c23deae6743d42a87eb34a54f02396f3fcfd7c2d06e2c5b",
                    "version": "7.61.1"
                }
            ]
        },
        "remediation": {
            "recommendation": {
                "text": "None Provided"
            }
        },
        "resources": [
            {
                "details": {
                    "awsEcrContainerImage": {
                        "architecture": "amd64",
                        "imageHash":
"sha256:98f0304b3a3b7c12ce641177a99d1f3be56f532473a528fda38d53d519cafb13",
                        "imageTags": [
```

```
                            "o3"
                        ],
                        "platform": "ORACLE_LINUX_8",
                        "pushedAt": "Jan 19, 2023, 7:38:39 PM",
                        "registry": "111122223333",
                        "repositoryName": "inspector2"
                    }
                },
                "id": "arn:aws:ecr:us-east-1:111122223333:repository/inspector2/
sha256:98f0304b3a3b7c12ce641177a99d1f3be56f532473a528fda38d53d519cafb13",
                "partition": "aws",
                "region": "us-east-1",
                "type": "AWS_ECR_CONTAINER_IMAGE"
            }
        ],
        "severity": "HIGH",
        "status": "ACTIVE",
        "title": "CVE-2022-27782 - libcurl, curl",
        "type": "PACKAGE_VULNERABILITY",
        "updatedAt": "Jan 19, 2023, 9:59:00 PM"
    }
}
```

Lambda package vulnerability finding

```
{
    "version": "0",
    "id": "040bb590-3a12-353f-ecb1-05e54b0fbea7",
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-19T19:20:25Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:lambda:us-east-1:111122223333:function:ExampleFunction:$LATEST"
    ],
    "detail": {
        "awsAccountId": "111122223333",
        "description": "Those using Woodstox to parse XML data may be vulnerable to
 Denial of Service attacks (DOS) if DTD support is enabled. If the parser is running
```

```
 on user supplied input, an attacker may supply content that causes the parser to
 crash by stackoverflow. This effect may support a denial of service attack.",
        "exploitAvailable": "NO",
        "findingArn": "arn:aws:inspector2:us-east-1:111122223333:finding/
FINDING_ID",
        "firstObservedAt": "Jan 19, 2023, 7:20:25 PM",
        "fixAvailable": "YES",
        "inspectorScore": 7.5,
        "inspectorScoreDetails": {
            "adjustedCvss": {
                "cvssSource": "NVD",
                "score": 7.5,
                "scoreSource": "NVD",
                "scoringVector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H",
                "version": "3.1"
            }
        },
        "lastObservedAt": "Jan 19, 2023, 7:20:25 PM",
        "packageVulnerabilityDetails": {
            "cvss": [
                {
                    "baseScore": 7.5,
                    "scoringVector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H",
                    "source": "NVD",
                    "version": "3.1"
                }
            ],
            "referenceUrls": [
                "https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=47434"
            ],
            "relatedVulnerabilities": [],
            "source": "NVD",
            "sourceUrl": "https://nvd.nist.gov/vuln/detail/CVE-2022-40152",
            "vendorCreatedAt": "Sep 16, 2022, 10:15:00 AM",
            "vendorSeverity": "HIGH",
            "vendorUpdatedAt": "Nov 25, 2022, 11:15:00 AM",
            "vulnerabilityId": "CVE-2022-40152",
            "vulnerablePackages": [
                {
                    "epoch": 0,
                    "filePath": "lib/woodstox-core-6.2.7.jar",
                    "fixedInVersion": "6.4.0",
                    "name": "com.fasterxml.woodstox:woodstox-core",
                    "packageManager": "JAR",
```

```
                    "remediation": "Update woodstox-core to 6.4.0",
                    "version": "6.2.7"
                }
            ]
        },
        "remediation": {
            "recommendation": {
                "text": "None Provided"
            }
        },
        "resources": [
            {
                "details": {
                    "awsLambdaFunction": {
                        "architectures": [
                            "X86_64"
                        ],
                        "codeSha256": "+EwrOrht2um4fdVCD73gj
+O7HJIAUvUxi8AD0eKHSkc=",
                        "executionRoleArn": "arn:aws:iam::111122223333:role/
ExampleFunction-ExecutionRole",
                        "functionName": "Example-function",
                        "lastModifiedAt": "Nov 7, 2022, 8:29:27 PM",
                        "packageType": "ZIP",
                        "runtime": "JAVA_11",
                        "version": "$LATEST"
                    }
                },
                "id": "arn:aws:lambda:us-
east-1:111122223333:function:ExampleFunction:$LATEST",
                "partition": "aws",
                "region": "us-east-1",
                "tags": {
                    "TargetAlias": "DeploymentStack",
                    "SoftwareType": "Infrastructure"
                },
                "type": "AWS_LAMBDA_FUNCTION"
            }
        ],
        "severity": "HIGH",
        "status": "ACTIVE",
        "title": "CVE-2022-40152 - com.fasterxml.woodstox:woodstox-core",
        "type": "PACKAGE_VULNERABILITY",
        "updatedAt": "Jan 19, 2023, 7:20:25 PM"
```

```
    }
}
```

Lambda code vulnerability finding

```
{
   "version":"0",
   "id":"9df01cb1-df24-bc46-5650-085a4087e7aa",
   "detail-type":"Inspector2 Finding",
   "source":"aws.inspector2",
   "account":"111122223333",
   "time":"2023-12-07T22:14:45Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:lambda:us-east-1:111122223333:function:code-finding:$LATEST"
   ],
   "detail":{
      "awsAccountId":"111122223333",
      "codeVulnerabilityDetails":{
         "detectorId":"python/lambda-override-reserved@v1.0",
         "detectorName":"Override of reserved variable names in a Lambda function",
         "detectorTags":[
            "availability",
            "aws-python-sdk",
            "aws-lambda",
            "data-integrity",
            "maintainability",
            "security",
            "security-context",
            "python"
         ],
         "filePath":{
            "endLine":6,
            "fileName":"lambda_function.py",
            "filePath":"lambda_function.py",
            "startLine":6
         },
         "ruleId":"Rule-434311"
      },
      "description":"Overriding environment variables that are reserved by AWS
 Lambda might lead to unexpected behavior or failure of the Lambda function.",
```

```
      "findingArn":"arn:aws:inspector2:us-east-1:111122223333:finding/FINDING_ID",
      "firstObservedAt":"Aug 8, 2023, 7:33:58 PM",
      "lastObservedAt":"Dec 7, 2023, 10:14:45 PM",
      "remediation":{
         "recommendation":{
            "text":"Your code attempts to override an environment variable that is
 reserved by the Lambda runtime environment. This can lead to unexpected behavior
 and might break the execution of your Lambda function.\n\n[Learn more](https://
docs.aws.amazon.com/lambda/latest/dg/configuration-envvars.html#configuration-
envvars-runtime)"
         }
      },
      "resources":[
         {
            "details":{
               "awsLambdaFunction":{
                  "architectures":[
                     "X86_64"
                  ],
                  "codeSha256":"2mtfH+CgubesG6NYpb2zEqBja5WN6FfbH4AAYDuF8RE=",
                  "executionRoleArn":"arn:aws:iam::193043430472:role/service-role/
code-finding-role-7jgg3wan",
                  "functionName":"code-finding",
                  "lastModifiedAt":"Dec 7, 2023, 10:12:48 PM",
                  "packageType":"ZIP",
                  "runtime":"PYTHON_3_7",
                  "version":"$LATEST"
               }
            },
            "id":"arn:aws:lambda:us-east-1:193043430472:function:code-finding:
$LATEST",
            "partition":"aws",
            "region":"us-east-1",
            "type":"AWS_LAMBDA_FUNCTION"
         }
      ],
      "severity":"HIGH",
      "status":"ACTIVE",
      "title":"Overriding environment variables that are reserved by AWS Lambda
 might lead to unexpected behavior.",
      "type":"CODE_VULNERABILITY",
      "updatedAt":"Dec 7, 2023, 10:14:45 PM"
   }
}
```

> **Note**
>
> 詳細資料值會以物件形式傳回單一發現項目的 JSON 詳細資訊。它不會傳回整個發現項目回應語法，它支援陣列中的多個發現項目。

Amazon Inspector 初始掃描完成事件架構示例

以下是完成初始掃描之 EventBridge Amazon Inspector 事件的事件結構描述範例。當 Amazon Inspector 完成對您其中一個資源的初始掃描時，就會建立此事件。

下列欄位可識別初始掃描完成事件：

- `detail-type`欄位設定為`Inspector2 Scan`。
- `detail`物件包含一個`finding-severity-counts`物件，其中詳細說明適用嚴重性類別中發現項目的數目`CRITICAL`，例如`HIGH`、和`MEDIUM`。

從選項中選取，依資源類型查看不同的初始掃描事件結構描述。

Amazon EC2 instance initial scan

```
{
    "version": "0",
    "id": "28a46762-6ac8-6cc4-4f55-bc9ab99af928",
    "detail-type": "Inspector2 Scan",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-20T22:52:35Z",
    "region": "us-east-1",
    "resources": [
        "i-087d63509b8c97098"
    ],
    "detail": {
        "scan-status": "INITIAL_SCAN_COMPLETE",
        "finding-severity-counts": {
            "CRITICAL": 0,
```

```
            "HIGH": 0,
            "MEDIUM": 0,
            "TOTAL": 0
        },
        "instance-id": "i-087d63509b8c97098",
        "version": "1.0"
    }
}
```

Amazon ECR image initial scan

```
{
    "version": "0",
    "id": "fdaa751a-984c-a709-44f9-9a9da9cd3606",
    "detail-type": "Inspector2 Scan",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-20T23:15:18Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ecr:us-east-1:111122223333:repository/inspector2"
    ],
    "detail": {
        "scan-status": "INITIAL_SCAN_COMPLETE",
        "repository-name": "arn:aws:ecr:us-east-1:111122223333:repository/
inspector2",
        "finding-severity-counts": {
            "CRITICAL": 0,
            "HIGH": 0,
            "MEDIUM": 0,
            "TOTAL": 0
        },
        "image-digest":
 "sha256:965fbcae990b0467ed5657caceaec165018ef44a4d2d46c7cdea80a9dff0d1ea",
        "image-tags": [
            "ubuntu22"
        ],
        "version": "1.0"
    }
}
```

Lambda function initial scan

```
{
  "version": "0",
  "id": "4f290a7c-361b-c442-03c8-a629f6f20d6c",
  "detail-type": "Inspector2 Scan",
  "source": "aws.inspector2",
  "account": "111122223333",
  "time": "2023-02-23T18:06:03Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:lambda:us-west-2:111122223333:function:lambda-example:$LATEST"
  ],
  "detail": {
    "scan-status": "INITIAL_SCAN_COMPLETE",
    "finding-severity-counts": {
      "CRITICAL": 0,
      "HIGH": 0,
      "MEDIUM": 0,
      "TOTAL": 0
    },
    "version": "1.0"
  }
}
```

Amazon Inspector 覆蓋事件架構示例

以下是涵蓋範圍之 Amazon Inspector EventBridge 事件的事件結構描述範例。變更資源的 Amazon Inspector 掃描涵蓋範圍時，就會建立此事件。下列欄位可識別涵蓋範圍事件：

- `detail-type`欄位設定為`Inspector2 Coverage`。
- `detail`物件包含一個`scanStatus`物件，指出資源的新掃描狀態。

```
{
```

```
    "version": "0",
    "id": "000adda5-0fbf-913e-bc0e-10f0376412aa",
    "detail-type": "Inspector2 Coverage",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-20T22:51:39Z",
    "region": "us-east-1",
    "resources": [
        "i-087d63509b8c97098"
    ],
    "detail": {
        "scanStatus": {
            "reason": "UNMANAGED_EC2_INSTANCE",
            "statusCodeValue": "INACTIVE"
        },
        "scanType": "PACKAGE",
        "eventTimestamp": "2023-01-20T22:51:35.665501Z",
        "version": "1.0"
    }
}
```

將亞馬Amazon Inspector 查器掃描整合到您的CI/CD 管道

您可以將 Amazon Inspector 容器映像掃描直接整合到 CI/CD 管道中，以掃描軟體漏洞並在組建結束時提供報告。Amazon Inspector 產生的弱點報告可讓您在部署之前調查和補救風險。

Amazon Inspector 器 CI/CD 整合利用 Amazon Inspector 器 SBOM 生成器和亞 Amazon Inspector 器掃描 API 的組合來為您的容器映像生成漏洞報告。Amazon Inspector SBOM 產生器會從提供的容器映像建立軟體物料清單 (SBOM)，然後，Amazon Inspector 掃描 API 會掃描該 SBOM，並建立報告，其中包含偵測到的任何弱點的詳細資訊。

您可以透過專為個別 CI/CD 解決方案建置的 Amazon Inspector 外掛程式，並在其市場上使用，或者您可以建立自己的自訂掃描整合，與亞馬遜 Inspector 達成 CI/CD 整合。

主題

插件集成

Amazon Inspector 為支持的 CI/CD 解決方案提供插件。您可以從各自的市集安裝這些外掛程式，然後使用它們將 Amazon Inspector 掃描新增為管道中的建置步驟。外掛程式建置步驟會在您提供的映像上執行 Amazon Inspector SBOM 產生器，然後在產生的 SBOM 上執行 Amazon Inspector 器掃描 API。

以下是 Amazon Inspector CI/CD 集成如何通過插件工作的概述：

1. 您可以設定 AWS 帳戶 為允許存取 Amazon Inspector 掃描 API。如需說明，請參閱設置一個 AWS 帳戶以使用 Amazon Inspector CI/CD 集成。
2. 您可以從市場上安裝 Amazon Inspector 插件。

3. 您安裝和設定 Amazon Inspector SBOM 產生器二進位檔。如需說明，請參閱Amazon Inspector 器 SBOM 發生器。
4. 您可以在 CI/CD 管道中新增 Amazon Inspector 掃描做為建置步驟，並設定掃描。
5. 當您執行組建時，外掛程式會將您的容器映像檔做為輸入，然後在映像上執行 Amazon Inspector SBOM 產生器，以產生CycloneDX相容的 SBOM。
6. 此外掛程式會將產生的 SBOM 傳送至 Amazon Inspector 掃描 API 端點，該端點會評估每個 SBOM 元件是否存在弱點。
7. Amazon Inspector 掃描 API 回應已轉換為 CSV、SBOM JSON 和 HTML 格式的漏洞報告。該報告包含 Amazon Inspector 發現的任何漏洞的詳細信息。

支援的 CI/CD 解決方案

Amazon Inspector 目前支援下列 CI/CD 解決方案。如需使用外掛程式設定 CI/CD 整合的完整說明，請選取 CI/CD 解決方案的外掛程式：

- 詹金斯插件
- TeamCity 外掛程式

自訂整合

如果 Amazon Inspector 沒有為您的 CI/CD 解決方案提供外掛程式，您可以使用亞馬遜檢查器 SBOM 產生器和 Amazon Inspector 器掃描 API 的組合來建立自己的自訂 CI/CD 整合。您也可以使用自訂整合，使用 Amazon Inspector SBOM 產生器提供的選項來微調掃描。

以下是自訂 Amazon Inspector CI/CD 整合運作方式的概觀：

1. 您可以設定 AWS 帳戶 為允許存取 Amazon Inspector 掃描 API。如需說明，請參閱設置一個 AWS 帳戶以使用 Amazon Inspector CI/CD 集成。
2. 您安裝和設定 Amazon Inspector SBOM 產生器二進位檔。如需說明，請參閱Amazon Inspector 器 SBOM 發生器。
3. 您可以使用 Amazon Inspector 器 SBOM 產生器為您的CycloneDX容器映像產生相容的 SBOM。
4. 您可以在產生的 SBOM 上使用 Amazon Inspector 掃描 API 來產生弱點報告。

如需設定自訂整合的指示，請參閱使用 Amazon Inspector 掃描建立您自己的自訂 CI/CD 管道整合。

設置一個 AWS 帳戶以使用 Amazon Inspector CI/CD 集成

您必須註冊才 AWS 帳戶 能使用 Amazon Inspector CI/CD 整合。 AWS 帳戶 必須具有 IAM 角色，該角色可授予您對 Amazon Inspector 掃描 API 的存取權限。

完成下列主題中的工作以註冊 AWS 帳戶、建立管理員使用者，以及設定用於 CI/CD 整合的 IAM 角色。

> **Note**
>
> 如果您已經註冊了 AWS 帳戶，則可以跳到設定用來進行CI/CD 整合的 IAM 角色。

主題

註冊一個 AWS 帳戶

如果您沒有 AWS 帳戶，請完成以下步驟來建立一個。

若要註冊成為 AWS 帳戶

1. 開啟 https://portal.aws.amazon.com/billing/signup。
2. 請遵循線上指示進行。

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

   當您註冊一個時 AWS 帳戶，將創建AWS 帳戶根使用者一個。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。作為安全最佳實務，將管理存取權指派給管理使用者，並且僅使用根使用者來執行 需要根使用者存取權的任務。

AWS 註冊過程完成後，會向您發送確認電子郵件。您可以隨時登錄 https://aws.amazon.com/ 並選擇我的帳戶，以檢視您目前的帳戶活動並管理帳戶。

建立管理使用者

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

保護您的 AWS 帳戶根使用者

1. 選擇 Root 使用者並輸入您的 AWS 帳戶 電子郵件地址，以帳戶擁有者身分登入。AWS Management Console在下一頁中，輸入您的密碼。

   如需使用根使用者登入的說明，請參閱 AWS 登入 使用者指南中的以根使用者身分登入。
2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

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

建立管理使用者

1. 啟用 IAM Identity Center。

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

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

以管理員的身分簽署

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

  如需使用 IAM 身分中心使用者登入的說明，請參閱使用AWS 登入 者指南中的登入 AWS 存取入口網站。

設定用來進行CI/CD 整合的 IAM 角色

若要將 Amazon Inspector 掃描整合到您的 CI/CD 管道中，您需要建立 IAM 政策以允許存取 Amazon Inspector 掃描 API 以掃描軟體物料清單 (SBOM)。然後，您可以將該政策附加到 IAM 角色，您的帳戶可以假設該角色執行 Amazon Inspector 掃描 API。

1. 登入 AWS Management Console 並開啟身分與存取權管理主控台，網址為 https://console.aws.amazon.com/iam/。
2. 在 IAM 主控台的導覽窗格中，選擇 [政策]，然後選擇 [建立政策]。
3. 在 [原則編輯器] 中，選取 JSON 並貼上下列陳述式：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "inspector-scan:ScanSbom",
            "Resource": "*"
        }
    ]
}
```

4. 選擇下一步。
5. 例如，為策略命名`InspectorCICDscan-policy`，並新增選擇性描述，然後選擇「建立策略」。此原則將附加至您將在後續步驟中建立的角色。
6. 在 IAM 主控台的導覽窗格中，選取 [角色]，然後選取 [建立新角色]。
7. 對於信任的實體類型，請選擇 [自訂信任原則] 並貼上下列原則：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::{ACCOUNT_ID}:root"
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```

8. 選擇下一步。

9. 在 [新增權限] 中，搜尋並選取您先前建立的原則，然後選擇 [下一步]。
10. 例如，為角色指定名稱InspectorCICDscan-role，並新增選擇性描述，然後選擇Create Role。

Amazon Inspector 器 SBOM 發生器

Amazon Inspector 器 SBOM 生成器（Sbomgen）是一種二進制工具，可為容器映像生成軟件材料清單（SBOM）。SBOM 是系統上安裝之軟體的收集清查。

Sbomgen通過掃描已知包含有關已安裝軟件包信息的文件來工作。如果找到其中一個檔案，工具會擷取套件名稱、版本和其他中繼資料。然後，此套件中繼資料會轉換為 CycloneDX SBOM。

Sbomgen可作為獨立工具來提供 CycloneDX SBOM 作為檔案或標準輸出。它也可作為 Amazon Inspector CI/CD 整合的一部分使用，該整合會自動掃描容器映像，做為部署管道的一部分。如需詳細資訊，請參閱 將亞馬Amazon Inspector 查器掃描整合到您的CI/CD 管道。

支持的軟件包和圖像格式

此時，Sbomgen可以收集下列包裹類型的庫存：

- Alpine APK
- Debian / Ubuntu DPKG
- Red Hat RPM
- Go套件透過go.mod和 go mod cache
- Java透過套件 pom.properties
- Node.js包通過package.json文件裡面 node_modules
- C# 包通過 Nuget 文件（.deps.json, csprojPackages.config, 打包 .json）
- PHP 通過installed.json和 composer.lock
- Python透過requirements.txt、Pipfile.lock、poetry.lock和egg/wheel檔案的封裝
- Ruby透過Gemfile.lock.gemspec、及全球安裝的 gem 封裝
- Rust套件透過Cargo.lock和 Cargo.toml

Sbomgen支援下列影像的容器映像資訊清單格式：

- OCI 映像資訊清單

- Docker圖像清單版本 2，架構 2
- Docker圖像清單版本 2，架構 1
- Docker圖像清單版本 1

> **Important**
>
> Sbomgen如果容器映像大小超過 5 GB、層數超過 60 個，或安裝的套件超過 2,000 個，則無法掃描容器映像。

安裝 Amazon Inspector SBOM 發生器（ ）Sbomgen

Sbomgen僅適用於 Linux 作業系統。如果您要使用它來分析容器映像檔，則必須安裝容器服務 Docker，例如 Podman、或containerd。

為了獲得最佳性能，我們建議使用以下最低硬件規格從系統運行二進製文件：

- 4 倍核心 CPU
- 8 GB RAM

安裝 Sbomgen

1. 從適用於您的架構的正確 URL 下載 Sbomgen zip 文件：

   AMD64

   https://amazon-inspector-sbomgen.s3.amazonaws.com/latest/linux/amd64/inspector-sbomgen.zip

   ARM64

   https://amazon-inspector-sbomgen.s3.amazonaws.com/latest/linux/arm64/inspector-sbomgen.zip
2. 使用以下命令解壓縮下載：

   ```
   unzip inspector-sbomgen.zip
   ```
3. 檢查歸檔中是否有下列檔案：

- `inspector-sbomgen`— 這是您將執行以產生 SBOM 的二進位檔案。
- `README.txt`-這是使用的文檔Sbomgen。
- `LICENSE.txt`— 此檔案包含的軟體授權Sbomgen。
- `licenses`— 此資料夾包含使用的協力廠商套件的授權資訊Sbomgen。
- `checksums.txt`-此文件提供了Sbomgen二進製文件的哈希值。
- `sbom.json`-這是Sbomgen二進位檔的 CycloneDX SBOM。

4. (選擇性) 使用下列指令驗證二進位檔的真實性與完整性：

   ```
   sha256sum < inspector-sbomgen
   ```

   - 將結果與`checksums.txt`檔案的內容進行比較。

5. 使用以下命令將可執行權限授予二進製文件：

   ```
   chmod +x inspector-sbomgen
   ```

6. 使用Sbomgen下列命令確認已成功安裝：

   ```
   ./inspector-sbomgen --version
   ```

   您應該會看到類似下列內容的輸出：

   ```
   Version: 1.X.X
   ```

使用 Sbomgen

您可以使用Sbomgen來產生容器映像的 SBOM。

您也可以透過選項 (例如排除特定檔案，或定義工具掃描的封裝) 來自訂 SBOM 產生的結果。如需這些使用案例及其他使用案例的範例，請執行下列命令：

```
./inspector-sbomgen list-examples
```

產生容器映像的 SBOM 並將結果輸出至檔案

在此範例中，請*`image:tag`*以影像的 ID 取代，以及*`output_path.json`*將輸出儲存至的路徑取代：

```
./inspector-sbomgen container --image image:tag -o output_path.json
```

使用以下方式對私人登錄進行驗證 Sbomgen

您可以透過提供私人登錄驗證認證，從私人登錄中託管的容器產生 SBOM。您可以透過多種方式提供認證；透過快取認證、透過互動式方法，或透過非互動式方法，在執行Sbomgen之前，您的認證會作為環境變數提供。

使用快取的認證進行驗證 (建議)

1. Sbomgen將嘗試使用緩存憑據（如果您的代理程序上可用）。對於此方法，請先向您的容器登錄進行驗證。例如，如果您正在使用Docker，則可以使用以下Dockerlogin命令向註冊表進行身份驗證：

   ```
   docker login
   ```

2. 然後，在成功對私人註冊表進行身份驗證後，您可以在該註冊表中的容器映像Sbomgen上使用。若要使用下列範例，請*image:tag*以要掃描的影像名稱取代：

   ```
   ./inspector-sbomgen container --image image:tag
   ```

使用互動式方法進行驗證

- 對於這種方法，您提供您的用戶名作為參數，並Sbomgen在需要時提示您輸入安全密碼。若要使用下列範例，請取代*image:tag*為要掃描的影像名稱，以及*your_username*可存取該影像的使用者名稱：

  ```
  ./inspector-sbomgen container --image image:tag --username
  your_username
  ```

使用非互動式方法進行驗證

- 要使用此方法，您應該將密碼或註冊表令牌存儲在只有當前用戶可讀的 .txt 文件中。文本文件應該只包含您的密碼或令牌在一行。若要使用下列範例，請以您*your_username*的使用者名稱取代，取代*password.txt*包含您的密碼或權杖的檔案，然後以要掃描的影像名稱取*image:tag*代：

  ```
  INSPECTOR_SBOMGEN_USERNAME=your_username\
  INSPECTOR_SBOMGEN_PASSWORD=`cat password.txt` \
  ./inspector-sbomgen container --image image:tag
  ```

範例輸出 Sbomgen

以下是使用清查之容器映像的 SBOM 範例。Sbomgen

容器映像檔


```
{
  "bomFormat": "CycloneDX",
  "specVersion": "1.5",
  "serialNumber": "urn:uuid:828875ef-8c32-4777-b688-0af96f3cf619",
  "version": 1,
  "metadata": {
    "timestamp": "2023-11-17T21:36:38Z",
    "tools": [
      {
        "vendor": "Amazon Web Services, Inc. (AWS)",
        "name": "Amazon Inspector SBOM Generator",
        "version": "1.0.0",
        "hashes": [
          {
            "alg": "SHA-256",
            "content":
 "10ab669cfc99774786301a745165b5957c92ed9562d19972fbf344d4393b5eb1"
          }
        ]
      }
    ],
    "component": {
      "bom-ref": "comp-1",
      "type": "container",
      "name": "fedora:latest",
      "properties": [
        {
          "name": "amazon:inspector:sbom_generator:image_id",
          "value":
 "sha256:c81c8ae4dda7dedc0711daefe4076d33a88a69a28c398688090c1141eff17e50"
        },
        {
          "name": "amazon:inspector:sbom_generator:layer_diff_id",
          "value":
 "sha256:eddd0d48c295dc168d0710f70364581bd84b1dda6bb386c4a4de0b61de2f2119"
        }
      ]
```

```
    }
  },
  "components": [
    {
      "bom-ref": "comp-2",
      "type": "library",
      "name": "dnf",
      "version": "4.18.0",
      "purl": "pkg:pypi/dnf@4.18.0",
      "properties": [
        {
          "name": "amazon:inspector:sbom_generator:source_file_scanner",
          "value": "python-pkg"
        },
        {
          "name": "amazon:inspector:sbom_generator:source_package_collector",
          "value": "python-pkg"
        },
        {
          "name": "amazon:inspector:sbom_generator:source_path",
          "value": "/usr/lib/python3.12/site-packages/dnf-4.18.0.dist-info/METADATA"
        },
        {
          "name": "amazon:inspector:sbom_generator:is_duplicate_package",
          "value": "true"
        },
        {
          "name": "amazon:inspector:sbom_generator:duplicate_purl",
          "value": "pkg:rpm/fedora/python3-dnf@4.18.0-2.fc39?
arch=noarch&distro=39&epoch=0"
        }
      ]
    },
    {
      "bom-ref": "comp-3",
      "type": "library",
      "name": "libcomps",
      "version": "0.1.20",
      "purl": "pkg:pypi/libcomps@0.1.20",
      "properties": [
        {
          "name": "amazon:inspector:sbom_generator:source_file_scanner",
          "value": "python-pkg"
        },
```

```
        {
          "name": "amazon:inspector:sbom_generator:source_package_collector",
          "value": "python-pkg"
        },
        {
          "name": "amazon:inspector:sbom_generator:source_path",
          "value": "/usr/lib64/python3.12/site-packages/libcomps-0.1.20-py3.12.egg-
info/PKG-INFO"
        },
        {
          "name": "amazon:inspector:sbom_generator:is_duplicate_package",
          "value": "true"
        },
        {
          "name": "amazon:inspector:sbom_generator:duplicate_purl",
          "value": "pkg:rpm/fedora/python3-libcomps@0.1.20-1.fc39?
arch=x86_64&distro=39&epoch=0"
        }
      ]
    }
  ]
}
```

使用 Amazon Inspector 掃描建立您自己的自訂 CI/CD 管道整合

我們建議您使用 Amazon Inspector CI/CD 插件，如果它們在您的 CI/CD 市場可用。如需可用外掛程式的清單，請參閱支援的 CI/CD 解決方案。

如果 Amazon Inspector 沒有為您的 CI/CD 解決方案提供外掛程式，您可以使用亞馬遜檢查器 SBOM 產生器和 Amazon Inspector 器掃描 API 的組合來建立自己的自訂 CI/CD 整合。您也可以使用自訂整合，透過 Amazon Inspector SBOM 產生器中可用的選項微調掃描。

若要設定您自己的自訂整合

1. 設定 AWS 帳戶 以允許存取 Amazon Inspector 掃描 API。如需說明，請參閱設置一個 AWS 帳戶以使用 Amazon Inspector CI/CD 集成。
2. 安裝和設定 Amazon Inspector SBOM 產生器二進位檔。如需說明，請參閱安裝 Amazon Inspector SBOM 發生器（ ）Sbomgen。
3. 使用 SBOM 產生器為您要掃描的容器映像建立 SBOM 檔案。若要使用下列範例，請取代*image:id*為要掃描的影像名稱，*sbom_path.json*以及儲存 SBOM 輸出的位置：

```
./inspector-sbomgen container –image image:id -o sbom_path.json
```

4. 呼叫 inspector-scan API 以掃描產生的 SBOM 並提供弱點報告。若要使用下列範例，請以有效的 CyclonedX 相容 *SBOM ######### sbom_path.json#*然後將*##*取代為 AWS 區域 您目前已驗證的 API 端點，並以對應的*##*取代 REGION。如Amazon Inspector 掃描 API 的端點需區域和端點的完整清單，請參閱。

```
aws inspector-scan scan-sbom --sbom file://sbom_path.json --endpoint
"ENDPOINT" --region REGION
```

API 輸出格式

Amazon Inspector 掃描 API 可以輸出 CycloneDX 1.5 格式的漏洞報告或 Amazon Inspector 找 JSON。您可以使用--output-format旗標變更預設值。

CycloneDX1.5 格式輸出的示例


```
{
  "status": "SBOM parsed successfully, 1 vulnerabilities found",
  "sbom": {
    "bomFormat": "CycloneDX",
    "specVersion": "1.5",
    "serialNumber": "urn:uuid:0077b45b-ff1e-4dbb-8950-ded11d8242b1",
    "metadata": {
      "properties": [
        {
          "name": "amazon:inspector:sbom_scanner:critical_vulnerabilities",
          "value": "1"
        },
        {
          "name": "amazon:inspector:sbom_scanner:high_vulnerabilities",
          "value": "0"
        },
        {
          "name": "amazon:inspector:sbom_scanner:medium_vulnerabilities",
          "value": "0"
        },
        {
          "name": "amazon:inspector:sbom_scanner:low_vulnerabilities",
          "value": "0"
        }
```

```
      ],
      "tools": [
        {
          "name": "CycloneDX SBOM API",
          "vendor": "Amazon Inspector",
          "version": "empty:083c9b00:083c9b00:083c9b00"
        }
      ],
      "timestamp": "2023-06-28T14:15:53.760Z"
    },
    "components": [
      {
        "bom-ref": "comp-1",
        "type": "library",
        "name": "log4j-core",
        "purl": "pkg:maven/org.apache.logging.log4j/log4j-core@2.12.1",
        "properties": [
          {
            "name": "amazon:inspector:sbom_scanner:path",
            "value": "/home/dev/foo.jar"
          }
        ]
      }
    ],
    "vulnerabilities": [
      {
        "bom-ref": "vuln-1",
        "id": "CVE-2021-44228",
        "source": {
          "name": "NVD",
          "url": "https://nvd.nist.gov/vuln/detail/CVE-2021-44228"
        },
        "references": [
          {
            "id": "SNYK-JAVA-ORGAPACHELOGGINGLOG4J-2314720",
            "source": {
              "name": "SNYK",
              "url": "https://security.snyk.io/vuln/SNYK-JAVA-
ORGAPACHELOGGINGLOG4J-2314720"
            }
          },
          {
            "id": "GHSA-jfh8-c2jp-5v3q",
            "source": {
```

```
              "name": "GITHUB",
              "url": "https://github.com/advisories/GHSA-jfh8-c2jp-5v3q"
            }
          }
        ],
        "ratings": [
          {
            "source": {
              "name": "NVD",
              "url": "https://www.first.org/cvss/v3-1/"
            },
            "score": 10.0,
            "severity": "critical",
            "method": "CVSSv31",
            "vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H"
          },
          {
            "source": {
              "name": "NVD",
              "url": "https://www.first.org/cvss/v2/"
            },
            "score": 9.3,
            "severity": "critical",
            "method": "CVSSv2",
            "vector": "AC:M/Au:N/C:C/I:C/A:C"
          },
          {
            "source": {
              "name": "EPSS",
              "url": "https://www.first.org/epss/"
            },
            "score": 0.97565,
            "severity": "none",
            "method": "other",
            "vector": "model:v2023.03.01,date:2023-06-27T00:00:00+0000"
          },
          {
            "source": {
              "name": "SNYK",
              "url": "https://security.snyk.io/vuln/SNYK-JAVA-
ORGAPACHELOGGINGLOG4J-2314720"
            },
            "score": 10.0,
            "severity": "critical",
```

```
            "method": "CVSSv31",
            "vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:H"
          },
          {
            "source": {
              "name": "GITHUB",
              "url": "https://github.com/advisories/GHSA-jfh8-c2jp-5v3q"
            },
            "score": 10.0,
            "severity": "critical",
            "method": "CVSSv31",
            "vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H"
          }
        ],
        "cwes": [
          400,
          20,
          502
        ],
        "description": "Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security
 releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages,
 and parameters do not protect against attacker controlled LDAP and other JNDI related
 endpoints. An attacker who can control log messages or log message parameters can
 execute arbitrary code loaded from LDAP servers when message lookup substitution is
 enabled. From log4j 2.15.0, this behavior has been disabled by default. From version
 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely
 removed. Note that this vulnerability is specific to log4j-core and does not affect
 log4net, log4cxx, or other Apache Logging Services projects.",
        "advisories": [
          {
            "url": "https://www.intel.com/content/www/us/en/security-center/advisory/
intel-sa-00646.html"
          },
          {
            "url": "https://support.apple.com/kb/HT213189"
          },
          {
            "url": "https://msrc-blog.microsoft.com/2021/12/11/microsofts-response-to-
cve-2021-44228-apache-log4j2/"
          },
          {
            "url": "https://logging.apache.org/log4j/2.x/security.html"
          },
          {
```

```
            "url": "https://www.debian.org/security/2021/dsa-5020"
          },
          {
            "url": "https://cert-portal.siemens.com/productcert/pdf/ssa-479842.pdf"
          },
          {
            "url": "https://www.oracle.com/security-alerts/alert-cve-2021-44228.html"
          },
          {
            "url": "https://www.oracle.com/security-alerts/cpujan2022.html"
          },
          {
            "url": "https://cert-portal.siemens.com/productcert/pdf/ssa-714170.pdf"
          },
          {
            "url": "https://lists.fedoraproject.org/archives/list/package-
announce@lists.fedoraproject.org/message/M5CSVUNV4HWZZXGOKNSK6L7RPM7BOKIB/"
          },
          {
            "url": "https://cert-portal.siemens.com/productcert/pdf/ssa-397453.pdf"
          },
          {
            "url": "https://cert-portal.siemens.com/productcert/pdf/ssa-661247.pdf"
          },
          {
            "url": "https://lists.fedoraproject.org/archives/list/package-
announce@lists.fedoraproject.org/message/VU57UJDCFIASIO35GC55JMKSRXJMCDFM/"
          },
          {
            "url": "https://www.oracle.com/security-alerts/cpuapr2022.html"
          },
          {
            "url": "https://twitter.com/kurtseifried/status/1469345530182455296"
          },
          {
            "url": "https://tools.cisco.com/security/center/content/
CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd"
          },
          {
            "url": "https://lists.debian.org/debian-lts-announce/2021/12/msg00007.html"
          },
          {
            "url": "https://www.kb.cert.org/vuls/id/930724"
          }
```

```
        ],
        "created": "2021-12-10T10:15:00Z",
        "updated": "2023-04-03T20:15:00Z",
        "affects": [
          {
            "ref": "comp-1"
          }
        ],
        "properties": [
          {
            "name": "amazon:inspector:sbom_scanner:exploit_available",
            "value": "true"
          },
          {
            "name": "amazon:inspector:sbom_scanner:exploit_last_seen_in_public",
            "value": "2023-03-06T00:00:00Z"
          },
          {
            "name": "amazon:inspector:sbom_scanner:cisa_kev_date_added",
            "value": "2021-12-10T00:00:00Z"
          },
          {
            "name": "amazon:inspector:sbom_scanner:cisa_kev_date_due",
            "value": "2021-12-24T00:00:00Z"
          },
          {
            "name": "amazon:inspector:sbom_scanner:fixed_version:comp-1",
            "value": "2.15.0"
          }
        ]
      }
    ]
  }
}
```

Inspector 格式輸出示例

```
                        {
  "status": "SBOM parsed successfully, 1 vulnerability found",
  "inspector": {
    "messages": [
      {
```

```
        "name": "foo",
        "purl": "pkg:maven/foo@1.0.0", // Will not exist in output if missing in sbom
        "info": "Component skipped: no rules found."
      }
    ],
    "vulnerability_count": {
      "critical": 1,
      "high": 0,
      "medium": 0,
      "low": 0
    },
    "vulnerabilities": [
      {
        "id": "CVE-2021-44228",
        "severity": "critical",
        "source": "https://nvd.nist.gov/vuln/detail/CVE-2021-44228",
        "related": [
          "SNYK-JAVA-ORGAPACHELOGGINGLOG4J-2314720",
          "GHSA-jfh8-c2jp-5v3q"
        ],
        "description": "Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security
 releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages,
 and parameters do not protect against attacker controlled LDAP and other JNDI related
 endpoints. An attacker who can control log messages or log message parameters can
 execute arbitrary code loaded from LDAP servers when message lookup substitution is
 enabled. From log4j 2.15.0, this behavior has been disabled by default. From version
 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely
 removed. Note that this vulnerability is specific to log4j-core and does not affect
 log4net, log4cxx, or other Apache Logging Services projects.",
        "references": [
          "https://www.intel.com/content/www/us/en/security-center/advisory/intel-
sa-00646.html",
          "https://support.apple.com/kb/HT213189",
          "https://msrc-blog.microsoft.com/2021/12/11/microsofts-response-to-
cve-2021-44228-apache-log4j2/",
          "https://logging.apache.org/log4j/2.x/security.html",
          "https://www.debian.org/security/2021/dsa-5020",
          "https://cert-portal.siemens.com/productcert/pdf/ssa-479842.pdf",
          "https://www.oracle.com/security-alerts/alert-cve-2021-44228.html",
          "https://www.oracle.com/security-alerts/cpujan2022.html",
          "https://cert-portal.siemens.com/productcert/pdf/ssa-714170.pdf",
          "https://lists.fedoraproject.org/archives/list/package-
announce@lists.fedoraproject.org/message/M5CSVUNV4HWZZXGOKNSK6L7RPM7BOKIB/",
          "https://cert-portal.siemens.com/productcert/pdf/ssa-397453.pdf",
```

```
          "https://cert-portal.siemens.com/productcert/pdf/ssa-661247.pdf",
          "https://lists.fedoraproject.org/archives/list/package-
announce@lists.fedoraproject.org/message/VU57UJDCFIASIO35GC55JMKSRXJMCDFM/",
          "https://www.oracle.com/security-alerts/cpuapr2022.html",
          "https://twitter.com/kurtseifried/status/1469345530182455296",
          "https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-
sa-apache-log4j-qRuKNEbd",
          "https://lists.debian.org/debian-lts-announce/2021/12/msg00007.html",
          "https://www.kb.cert.org/vuls/id/930724"
        ],
        "created": "2021-12-10T10:15:00Z",
        "updated": "2023-04-03T20:15:00Z",
        "properties": {
          "cisa_kev_date_added": "2021-12-10T00:00:00Z",
          "cisa_kev_date_due": "2021-12-24T00:00:00Z",
          "cwes": [
            400,
            20,
            502
          ],
          "cvss": [
            {
              "source": "NVD",
              "severity": "critical",
              "cvss3_base_score": 10.0,
              "cvss3_base_vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H",
              "cvss2_base_score": 9.3,
              "cvss2_base_vector": "AC:M/Au:N/C:C/I:C/A:C"
            },
            {
              "source": "SNYK",
              "severity": "critical",
              "cvss3_base_score": 10.0,
              "cvss3_base_vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:H"
            },
            {
              "source": "GITHUB",
              "severity": "critical",
              "cvss3_base_score": 10.0,
              "cvss3_base_vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H"
            }
          ],
          "epss": 0.97565,
          "exploit_available": true,
```

```
          "exploit_last_seen_in_public": "2023-03-06T00:00:00Z"
        },
        "affects": [
          {
            "installed_version": "pkg:maven/org.apache.logging.log4j/log4j-
core@2.12.1",
            "fixed_version": "2.15.0",
            "path": "/home/dev/foo.jar"
          }
        ]
      }
    ]
  }
}
```

使用 Amazon Inspector Jenkins 插件

此Jenkins外掛程式利用 Amazon Inspector SBOM 產生器二進位檔和 Amazon Inspector 掃描 API，在建置結束時產生詳細的報告，讓您可以在部署之前調查並修復風險。

Amazon Inspector 是一項弱點管理服務，可掃描容器映像中的作業系統，以及以 CVE 為基礎的程式設計語言套件弱點。

使用 Amazon Inspector Jenkins 外掛程式，您可以將 Amazon Inspector 漏洞掃描添加到您的Jenkins管道。

> **Note**
>
> Amazon Inspector 弱點掃描可設定為根據偵測到的弱點數量和嚴重性來通過或失敗管道執行。

您可以在Jenkins市場上查看該Jenkins插件的最新版本 https://plugins.jenkins.io/amazon-inspector-image-scanner/.

下列步驟說明如何設定 Amazon Inspector Jenkins 外掛程式。

> **Important**
>
> 在完成下列步驟之前，您必須將 Jenkins 升級至 2.387.3 版或更高版本，才能執行外掛程式。

步驟 1. 設置一個 AWS 帳戶

使 AWS 帳戶 用 IAM 角色進行設定，以允許存取 Amazon Inspector 掃描 API。如需說明，請參閱設置一個 AWS 帳戶以使用 Amazon Inspector CI/CD 集成。

步驟 2. 安裝 Amazon Inspector 詹金斯插件

下面的過程描述了如何從Jenkins儀表板安裝 Amazon Inspector 詹金斯插件。

1. 從詹金斯儀表板，選擇管理詹金斯，然後選擇管理插件。
2. 選擇 [可用]。
3. 在「可用」索引標籤中搜尋 Amazon Inspector 掃描，然後安裝外掛程式。

(選擇性) 步驟 3。將 docker 認證添加到 Jenkins

> **Note**
>
> 如果 docker 映像位於私有存儲庫中，則僅添加 docker 憑據。否則，請跳過這個步驟。

下列程序說明如何從Jenkins儀表板將 docker 認證新增Jenkins至。

1. 從詹金斯儀表板，選擇管理詹金斯，憑據，然後系統。
2. 選擇全域認證，然後選擇新增認證。
3. 對於種類，選取使用者名稱與密碼。
4. 對於範圍，選擇全局（詹金斯，節點，項目，所有子項目等）。
5. 輸入您的詳細資訊，然後選擇 [確定]。

(選擇性) 步驟 4。新增 AWS 認證

> **Note**
>
> 如果您想要根據 IAM 使用者進行驗證，請僅新增 AWS 登入資料。否則，請跳過這個步驟。

下列程序說明如何從Jenkins儀表板新增 AWS 認證。

1. 從詹金斯儀表板，選擇管理詹金斯，憑據，然後系統。
2. 選擇全域認證，然後選擇新增認證。
3. 對於種類，選取 AWS 登入資料。
4. 輸入您的詳細資訊，包括您的存取金鑰 ID 和秘密存取金鑰，然後選擇 [確定]。

步驟 5. 在Jenkins腳本中添加 CSS 支持

下列程序說明如何在Jenkikns指令碼中新增 CSS 支援。

1. 重新啟動 Jenkins。
2. 從儀表板中，選擇管理 Jenkins、節點、內建節點，然後選擇指令碼主控台。
3. 在文字方塊中，新增該行`System.setProperty("hudson.model.DirectoryBrowserSupport.CSP", "")`，然後選擇 [執行]。

步驟 6. 添加 Amazon Inspector 掃描到您的構建

您可以在專案中新增建置步驟或使用Jenkins宣告式管道，將 Amazon Inspector Scan 新增至您的組建。

Amazon Inspector 掃描到您的構建，在您的項目中添加一個構建步驟

1. 在 [設定] 頁面上，向下捲動至 [建置步驟]，然後選擇 [新增建置步驟]。然後選擇 Amazon Inspector 掃描。
2. 在兩種檢測器-sbomgen 安裝方式之間進行選擇：自動或手動。

   a. (選項 1) 選擇自動下載最新版本的檢測器-sbomgen. 如果您選擇此方法，請務必選取與執行外掛程式之系統相符的 CPU 架構。

   b. (選項 2) 如果要設定用於掃描的 Amazon Inspector 器 SBOM 產生器二進位檔，請選擇手動。如果您選擇此方法，請確保提供檢查器-sbomgen 先前下載版本的完整路徑。

   有關更多信息，請參閱 Amazon Inspector 查器 SBOM 生成器（安裝）Amazon Inspector 查器 SBOM 生成器。
3. 完成以下步驟以完成 Amazon Inspector 掃描建置步驟的設定：

a. 輸入您的圖像 ID。影像可以是本機、遠端或封存影像。影像名稱應遵循Docker命名慣例。如果要分析匯出的影像，請提供預期 tar 檔案的路徑。請參閱下列範例影像 ID 路徑：

   i. 對於本機或遠端容器：`NAME[:TAG|@DIGEST]`

   ii. 對於 tar 文件：`/path/to/image.tar`

b. 選取AWS 區域要透過傳送掃描要求。

c. (選擇性) 對於 Docker 認證，請選取您的Docker使用者名稱。只有當您的容器映像位於私有存儲庫中時，才執行此操作。

d. (選擇性) 您可以提供下列支援的 AWS 驗證方法：

   i. （可選）對於 IAM 角色，請提供角色 ARN（AR: aw:iam::: 角色/）。*AccountNumberRoleName*

   ii. (選擇性) 對於 AWS 登入資料，請選取要根據 IAM 使用者進行身份驗證的 ID。

   iii. (選擇性) 對於AWS 設定檔名稱，請提供要使用設定檔名稱進行驗證的設定檔名稱。

e. (選擇性) 指定每個嚴重性的弱點閾值。如果在掃描期間超過您指定的數目，映像建立將會失敗。如果值為全部`0`，則無論是否發現任何漏洞，組建都會成功。

4. 選擇儲存。

使用Jenkins宣告式管道將 Amazon Inspector 掃描新增至您的組建

您可以使用 Jenkins 宣告式管道自動或手動將 Amazon Inspector 掃描新增至您的組建。

若要自動下載 SBOmgen 宣告式管線

- 若要將 Amazon Inspector 掃描新增至組建，請使用下列範例語法。根據您首選的操作系統架構 Amazon Inspector 器 SBOM 生成器下載, 替換 *SBOMGEN_ #*與 Linux 64 或 將 *IMAGE_PATH* 取代為映像檔的路徑 (例如 *Alpine: latest*)、將 *IAM_ROLE ####### 1 #### IAM ##*的 ARN；如果您使用的是私有存放庫，則以您的身分Docker證明*###*取代 IMAGE_PATH。您可以選擇性地啟動弱點閾值，並指定每個嚴重性的值。

```
pipeline {
   agent any
   stages {
       stage('amazon-inspector-image-scanner') {
           steps {
               script {
```

```
                step([
                $class:
'com.amazon.inspector.jenkins.amazoninspectorbuildstep.AmazonInspectorBuilder',
                sbomgenSource: 'SBOMGEN_SOURCE', // this can be linuxAmd64 or linuxArm64
                archivePath: 'IMAGE_PATH',
                awsRegion: 'REGION',
                iamRole: 'IAM ROLE',
                credentialId: 'Id', // provide empty string if image not in private
repositories
                awsCredentialId: ''AWS ID;',
                awsProfileName: 'Profile Name',
                isThresholdEnabled: false,
                countCritical: 0,
                countHigh: 0,
                countLow: 10,
                countMedium: 5,
               ])
            }
          }
        }
    }
}
```

若要手動下載 SBOmGen 宣告式管線

- 若要將 Amazon Inspector 掃描新增至組建，請使用下列範例語法。*# SBOMGEN_PATH #### ### 3 #### Amazon Inspector # SBOM ######## IMAGE_PATH ######### (## Alpine: latest)## IAM_ROLE ####### 1 #### IAM ### ARN################ IAM_ROLE ####### 1 #### IAM ### ARN########## ID ID ###* Docker您可以選擇性地啟動弱點閾值，並指定每個嚴重性的值。

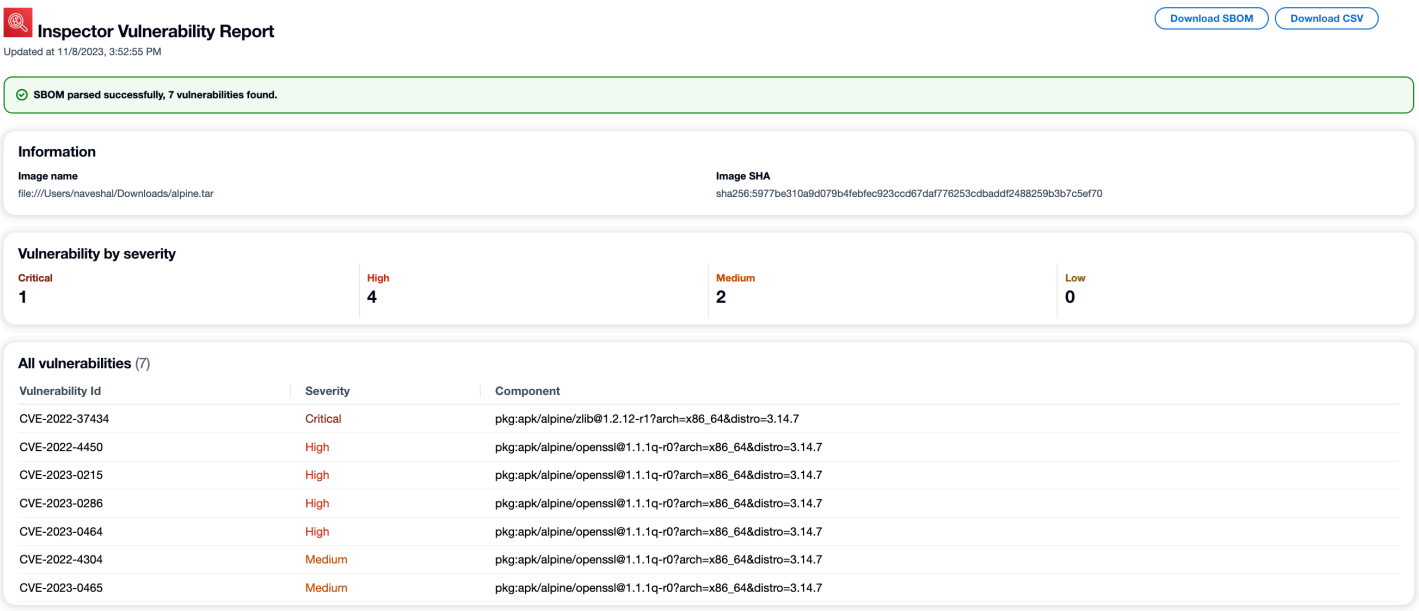
> **Note**
>
> 放置Sbomgen在詹金斯目錄中，並在插件中提供詹金斯目錄的路徑（如/選擇/文件夾/arm64/檢查器-sbomgen）。

```
pipeline {
    agent any
    stages {
```

```
        stage('amazon-inspector-image-scanner') {
            steps {
                script {
                step([
                $class:
'com.amazon.inspector.jenkins.amazoninspectorbuildstep.AmazonInspectorBuilder',
                sbomgenPath: 'SBOMGEN_PATH',
                archivePath: 'IMAGE_PATH',
                awsRegion: 'REGION',
                iamRole: 'IAM ROLE',
                awsCredentialId: ''AWS ID;',
                credentialId: 'Id;', // provide empty string if image not in private
repositories
                awsProfileName: 'Profile Name',
                isThresholdEnabled: false,
                countCritical: 0,
                countHigh: 0,
                countLow: 10,
                countMedium: 5,
               ])
            }
          }
        }
    }
 }
```

步驟 7. 查看您的 Amazon Inspector 漏洞報告

1. 完成專案的新組建。
2. 建置完成後，請從結果中選取輸出格式。如果您選取 HTML，您可以選擇下載報告的 JSON SBOM 或 CSV 版本。以下是 HTML 報告的範例：



故障診斷

以下是您在使用 Amazon Inspector 掃描外掛程式時可能會遇到的常見錯誤Jenkins。

無法載入認證或 sts 例外狀況錯誤

錯誤：

```
InstanceProfileCredentialsProvider(): Failed to load credentials or sts exception.
```

重新排序

獲取`aws_access_key_id`並`aws_secret_access_key`為您的 AWS 帳戶。設定`aws_access_key_id`並`aws_secret_access_key`在中`~/.aws/credentials`。

Inspector-檢查器路徑錯誤

錯誤：

```
Exception:com.amazon.inspector.jenkins.amazoninspectorbuildstep.exception.Sbomge
There was an issue running inspector-sbomgen, is /opt/inspector/inspector-sbomgen the correct path?
```

解決方法：

請完成下列程序來解決問題。

1. 在Jenkins目錄中放置正確的作業系統架構檢測器-sbomgen 如需詳細資訊，請參閱亞馬遜 Inspector 查器 SBOM 產生器。
2. 使用以下命令將可執行權限授予二進製文件：`chmod +x inspector-sbomgen`。
3. 在插件中提供正確的Jenkins機器路徑，例如`/opt/folder/arm64/inspector-sbomgen`。
4. 儲存設定並執行Jenkins工作。

使用 Amazon Inspector TeamCity 插件

Amazon Inspector TeamCity 插件使您能夠將 Amazon Inspector 漏洞掃描添加到您的TeamCity管道。此外掛程式利用 Amazon Inspector SBOM 產生器二進位檔和 Amazon Inspector 掃描 API，在組建結束時產生詳細的報告，讓您可以在部署之前調查並修復風險。也可以根據偵測到的弱點數目和嚴重性，將掃描設定為通過或失敗管道執行。

Amazon Inspector 是一項弱點管理服務，可針對 AWS 以 CVE 為基礎的作業系統和程式設計語言套件弱點掃描容器映像檔。如需 Amazon Inspector CI/CD 整合的詳細資訊，請參閱。將亞馬Amazon Inspector 查器掃描整合到您的CI/CD 管道

如需套件和容器映像格式的清單，請參閱 Amazon Inspector 外掛程式支援的支持的軟件包和圖像格式。

您可以在以下位置查看該插件的最TeamCity新版本：https://plugins.jetbrains.com/plugin/23236-amazon-inspector-scanner。或者，請依照本文件各節中的步驟設定 Amazon Inspector 外 TeamCity掛程式：

1. 設定 AWS 帳戶.
   - 使 AWS 帳戶 用 IAM 角色進行設定，以允許存取 Amazon Inspector 掃描 API。如需說明，請參閱設置一個 AWS 帳戶以使用 Amazon Inspector CI/CD 集成。
2. 安裝 Amazon Inspector TeamCity 插件。
   a. 從儀表板前往管理 > 外掛程式。
   b. 搜索 Amazon Inspector 掃描。
   c. 安裝 外掛程式。
3. 安裝 Amazon Inspector 器 SBOM 發生器。
   - 在您的 Teamcity 伺服器目錄中安裝 Amazon Inspector SBOM 產生器二進位檔。如需說明，請參閱安裝 Amazon Inspector SBOM 發生器（ ）Sbomgen。

4. 將 Amazon Inspector 掃描構建步驟添加到您的項目中。

   a. 在設定頁面上，向下捲動至建置步驟，選擇 [新增建置步驟]，然後選取 [Amazon Inspector 掃描]。

   b. 填寫下列詳細資料以設定 Amazon Inspector 掃描建置步驟：

      - 新增步驟名稱。
      - 在兩種 Amazon Inspector 器 SBOM 生成器安裝方法之間進行選擇：自動或手動。
        - 根據您的系統和 CPU 架構，自動下載最新版本的 Amazon Inspector 器 SBOM 生成器。
        - 手冊要求您提供先前下載版本的 Amazon Inspector 器 SBOM 生成器的完整路徑。

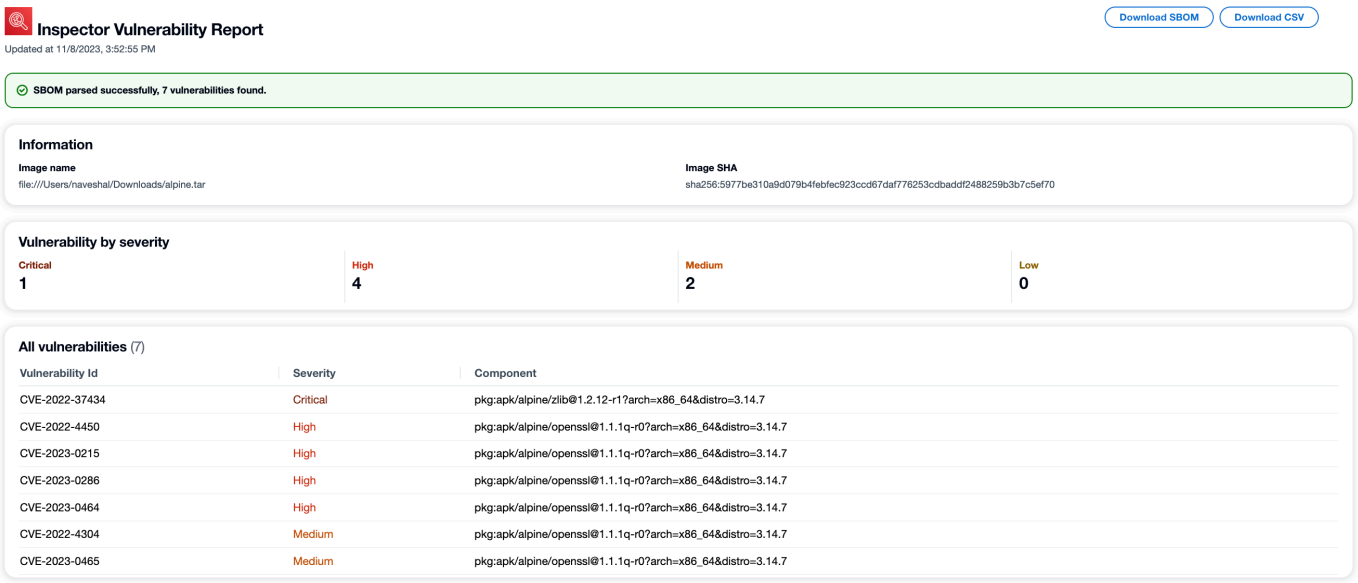
        有關更多信息，請參閱 Amazon Inspector SBOM 發生器安裝 (安裝) Amazon Inspector SBOM 發生器.
      - 輸入您的圖像 ID。您的映像檔可以是本機、遠端或封存。影像名稱應遵循Docker命名慣例。如果要分析匯出的影像，請提供預期 tar 檔案的路徑。請參閱下列範例影像 ID 路徑：
        - 對於本機或遠端容器：`NAME[:TAG|@DIGEST]`
        - 對於 tar 文件：`/path/to/image.tar`
      - 針對 IAM 角色，輸入您在步驟 1 中設定之角色的 ARN。
      - 選取AWS 區域要透過傳送掃描要求。
      - （可選）對於 Docker 身份驗證，請輸入您的 Docker 用戶名和碼頭密碼。只有當您的容器映像位於私有存儲庫中時，才執行此操作。
      - (選擇性) 對於AWS 驗證，請輸入您的 AWS 存取金鑰 ID 和 AWS 秘密金鑰。只有當您要根據 AWS 認證進行驗證時，才執行此操作。
      - (選擇性) 指定每個嚴重性的弱點閾值。如果在掃描期間超過您指定的數目，映像建立將會失敗。如果值為所0有，則無論發現的漏洞數量如何，構建都將成功。

   c. 選取 Save (儲存)。

5. 查看您的 Amazon Inspector 漏洞報告。

   a. 完成專案的新組建。

   b. 建置完成時，請從結果中選取輸出格式。當您選取 HTML 時，您可以選擇下載報告的 JSON SBOM 或 CSV 版本。以下是 HTML 報告的範例：



Amazon Inspector CycloneDX 命名空間

Amazon Inspector 器已保留CycloneDX命名空間和屬性名稱，以與亞馬遜檢查器 SBOM 生成器和 Amazon Inspector 器掃描 API 生成的 sBOM 一起使用。本頁記錄所有可能新增至使用 Amazon Inspector 工具建立之 CycloneDX sBOM 元件的自訂索引鍵/值屬性。有關CycloneDX財產分類的更多信息，請參閱官方文檔。

`amazon:inspector:sbom_scanner`命名空間分類

該`amazon:inspector:sbom_scanner`命名空間由 Amazon Inspector 掃描 API 使用。它具有下列屬性：

屬性	Description
`amazon:inspector:sbom_scanner:critical_vulnerabilities`	在 SBOM 中發現的嚴重性嚴重性弱點總數計數。
`amazon:inspector:sbom_scanner:high_vulnerabilities`	在 SBOM 中發現的高嚴重性弱點總數計數。
`amazon:inspector:sbom_scanner:medium_vulnerabilities`	在 SBOM 中發現的中等嚴重程度弱點總數計數。

屬性	Description
amazon:inspector:sbom_scanner:low_vulnerabilities	在 SBOM 中發現的低嚴重性弱點總數計數。
amazon:inspector:sbom_scanner:info	提供指定元件的掃描內容，例如：「已掃描的元件：找不到弱點」。
amazon:inspector:sbom_scanner:warning	提供未掃描給定元件的原因的上下文，例如：「略過的元件：未提供清除」。
amazon:inspector:sbom_scanner:fixed_version: *component_bom_ref*	針對指定的弱點提供指定元件的修正版本。
amazon:inspector:sbom_scanner:exploit_available	指出指定弱點是否有惡意利用。
amazon:inspector:sbom_scanner:exploit_last_seen_in_public	指出上次針對特定弱點在公開中發現的惡意利用的時間。
amazon:inspector:sbom_scanner:cisa_kev_date_added	指出此弱點新增至 CISA 已知的惡意利用弱點目錄的時間。
amazon:inspector:sbom_scanner:cisa_kev_date_due	根據 CISA 已知的惡意利用弱點目錄指出弱點修正的時間。
amazon:inspector:sbom_scanner:path	產生主旨套件資訊之檔案的路徑。

amazon:inspector:sbom_generator命名空間分類

該amazon:inspector:sbom_generator命名空間是由 Amazon Inspector SBOM 生成器使用。它具有下列屬性：

屬性	Description
amazon:inspector:sbom_generator:os_hostname	要清查之系統的主機名稱。
amazon:inspector:sbom_generator:kernel_name	要清查之系統的核心名稱。
amazon:inspector:sbom_generator:kernel_version	要清查之系統的核心版本。
amazon:inspector:sbom_generator:cpu_architecture	正在清查之系統的 CPU 架構，例如 x86_64。
amazon:inspector:sbom_generator:image_id	容器映像檔設定檔的雜湊值，也稱為映像 ID。
amazon:inspector:sbom_generator:layer_diff_id	未壓縮容器映像層的雜湊值。
amazon:inspector:sbom_generator:source_file_scanner	找到包含套件資訊的檔案的掃描器，例如：/var/lib/dpkg/status 。
amazon:inspector:sbom_generator:source_package_collector	從特定檔案中擷取封裝名稱和版本的收集器。
amazon:inspector:sbom_generator:source_path	從中擷取主旨套件資訊的檔案路徑。
amazon:inspector:sbom_generator:is_duplicate_package	表示主旨套件已被多個檔案掃描器找到。
amazon:inspector:sbom_generator:go_toolchain	表示用來產生 Go 可執行檔的Go編譯器或工具鏈版本。
amazon:inspector:sbom_generator:expires_before	SSL 憑證有效之前的日期。

屬性	Description
amazon:inspector:sbom_generator:expires_after	SSL 憑證無效的日期。
amazon:inspector:sbom_generator:is_expired	布林值，指出 SSL 憑證是否已過期。

使用 Amazon Inspector 自動化資源

亞馬遜 Amazon EC2 的亞馬遜檢查器無代理程式掃描正在預覽版本中。您使用無代理程式的 Amazon EC2 掃描功能須遵守AWS 服務條款第 2 節 (以下稱「試用版和預覽版」)。

Amazon Inspector 使用自己的專用掃描引擎。此引擎會監控您的資源，找出軟體弱點或開放網路路徑，這些路徑可能會導致工作負載入侵、惡意使用資源或未經授權存取您的資料。當 Amazon Inspector 測到漏洞時，它會創建一個發現。發現項目包括與偵測相關聯的詳細資訊，可協助您修復弱點。您可以在亞馬遜檢查器主控台上檢閱發現的結果，並使用 Amazon Inspector API。如需詳細資訊，請參閱 管理 Amazon Inspector 中的發現。

啟用後，Amazon Inspector 會自動探索所有符合資格的資源，並開始持續掃描這些資源。Amazon Inspector 會掃描軟體弱點和意外的網路暴露。Amazon Inspector 也會執行掃描以回應事件，例如安裝新應用程式或修補程式。

當您第一次啟用 Amazon Inspector 時，您的帳戶會自動註冊所有掃描類型。下列主題涵蓋 Amazon Inspector 提供的掃描類型的特定詳細資料。Amazon Inspector 會根據受弱點影響的資源類型，對掃描類型進行分類。下列主題涵蓋 Amazon Inspector 掃描哪些資源、針對這些資源起始新掃描的原因，以及如何針對每種資源類型設定掃描。

主題

- Amazon Inspector 掃描類型概觀
- 啟動掃瞄類型
- 用亞馬遜檢查器掃描亞馬遜 EC2 實例
- 使用 Amazon 檢查器掃描亞馬遜 ECR 容器映像
- Amazon Inspector 掃描 AWS Lambda 功能
- 停用掃瞄類型

當您第一次啟用 Amazon Inspector 時，您的帳戶會自動註冊下列掃描類型：Amazon EC2 掃描、Amazon ECR 掃描、Lambda 標準掃描。Lambda 程式碼掃描是選用的 Lambda 函數掃描層，您可以隨時啟動它。

Amazon Inspector 掃描類型概觀

Amazon Inspector 提供各種不同的掃描類型，專注於您 AWS 環境中的特定資源類型。

Amazon EC2 掃描

當您啟用 Amazon EC2 掃描時，Amazon Inspector 會掃描您的 Amazon EC2 執行個體，找出作業系統套件和程式設計語言套件漏洞，以及網路連線能力。Amazon Inspector 會掃描您的 EC2 執行個體，找出常見漏洞和入侵程式 (CVE) 和網路暴露問題。Amazon Inspector 會使用您執行個體上安裝的 SSM 代理程式，或透過 Amazon EBS 執行個體快照執行個體來執行掃描。如需 Amazon EC2 掃描的詳細資訊，請參閱用亞馬遜檢查器掃描亞馬遜 EC2 實例。

Amazon ECR 掃描

當您啟用 Amazon ECR 掃描時，Amazon Inspector 會將私有登錄中的所有基本掃描容器儲存庫轉換為持續掃描的增強型掃描。您也可以選擇將此設定設定為僅在推送時掃描，或透過包含規則掃描選取的儲存庫。一開始掃描過去 30 天內推送或過去 90 天內提取的所有影像。根據預設，Amazon Inspector 會持續監控影像 90 天，此設定可隨時變更。如需 Amazon ECR 掃描的詳細資訊，請參閱使用 Amazon 檢查器掃描亞馬遜 ECR 容器映像。

Lambda 準掃描

當您啟用 Lambda 標準掃描時，Amazon Inspector 會探索您帳戶中的 Lambda 函數，並立即開始掃描它們是否有漏洞。Amazon Inspector 會在部署新的 Lambda 函數和層時進行掃描，並在更新或發佈新的常見弱點和曝光 (CVE) 時重新掃描這些函數和層。如需 Lambda 函數掃描的詳細資訊，請參閱Amazon Inspector 掃描 AWS Lambda 功能。

Lambda 準掃描 + 程 Lambda 碼掃描

此可選項將 Lambda 標準掃描與 Lambda 程式碼掃描相結合。啟動 Lambda 程式碼掃描後，Amazon Inspector 會探索您帳戶中的 Lambda 函數和層，並掃描應用程式套件相依性的程式碼弱點。Lambda 程式碼掃描會掃描 Lambda 函數中的自訂應用程式程式碼，找出程式碼 這兩種掃瞄類型必須同時啟動。如需更多資訊，請參閱Amazon Inspector Lambda 代碼。

啟動掃瞄類型

您可以隨時啟用新的 Amazon Inspector 掃描類型。啟用掃描類型後，Amazon Inspector 將立即開始掃描該掃描類型的合格資源。如需可用掃瞄類型的概觀，請參閱Amazon Inspector 掃描類型概觀。以下說明首次啟動每種掃瞄類型時會發生什麼情況：

- Amazon EC2 掃描 — 當您為帳戶啟用 Amazon Inspector Amazon EC2 掃描時，Amazon Inspector 會掃描您帳戶中所有符合資格的執行個體，找出套件漏洞和網路連線問題。Amazon Inspector SSM 外掛程式已安裝在您所有受 SS Windows M 管理的主機上。如需詳細資訊，請參閱 掃描Windows實例。此外，Amazon Inspector 會在您的帳戶中建立下列 SSM 關聯：
  - `InspectorDistributor-do-not-delete`
  - `InspectorInventoryCollection-do-not-delete`
  - `InspectorLinuxDistributor-do-not-delete`
  - `InvokeInspectorLinuxSsmPlugin-do-not-delete`
  - `InvokeInspectorSsmPlugin-do-not-delete`.
- Amazon ECR 掃描 — 當您為帳戶啟用 Amazon ECR 容器映像掃描時，該帳戶中私有儲存庫的 Amazon ECR 掃描類型會從使用 Amazon ECR 的基本掃描變更為使用 Amazon Inspector 進行增強型掃描。然後掃描過去 30 天內推送或在過去 90 天內提取的所有合格 Amazon ECR 容器映像，以查看是否存在套件漏洞。此外，針對影像推送和提取日期，Amazon ECR 重新掃描持續時間設定為 90 天。
- Lambda 標準掃描 — 當您在帳戶中啟用 Lambda 標準掃描時，會掃描您帳戶中過去 90 天內叫用或更新的所有 Lambda 函數是否存在套件漏洞。此外，系統會在您的帳戶中建立 CloudTrail服務連結頻道。
- Lambda 標準掃描 + Lambda 程式碼掃描 — 這些 Lambda 函數掃描類型會一起啟動。當您在帳戶中啟用 Lambda 程式碼掃描時，會掃描帳戶中過去 90 天內叫用或更新的所有 Lambda 函數是否存在程式碼弱點。

啟動掃描

如果您是 AWS 組織中 Amazon Inspector 的委派管理員，則可以使用 Amazon Inspector 檢查器 2-enablement-with-cli 開發的殼層指令碼，自動為多個區域中的多個帳戶啟用各種 Amazon Inspector 掃描類型。 GitHub否則，若要透過主控台針對多帳戶環境完成此程序，請在以 Amazon Inspector 委派管理員身分登入時完成以下步驟。

Console

啟動掃描

1. 打開 Amazon Inspector 控制台 https://console.aws.amazon.com/inspector/v2/home.
2. 使用頁面右上角的選取 AWS 區域 器，選取您要啟動新掃描類型的區域。
3. 在功能窗格中，選擇 [帳戶管理]。

4. 在 [帳戶管理] 頁面上，選取您要啟動掃描類型的帳戶。
5. 選擇激活，然後選擇要激活的掃描類型。
6. (建議) 在您要啟動該掃描類型 AWS 區域 的每個步驟中重複這些步驟。

API

執行啟用 API 作業。在請求中，提供您要啟動掃描的帳戶 ID，以及冪等權杖，以及一個或多個`EC2`、`ECR`、`LAMBDA`、或`LAMBDA_CODE`以啟動該類型掃描的帳戶 ID。`resourceTypes`

用亞馬遜檢查器掃描亞馬遜 EC2 實例

亞馬遜 Amazon EC2 的亞馬遜檢查器無代理程式掃描正在預覽版本中。您使用無代理程式的 Amazon EC2 掃描功能須遵守AWS 服務條款第 2 節 (以下稱「試用版和預覽版」)。

Amazon Inspector EC2 掃描會從 EC2 執行個體擷取中繼資料，然後將此中繼資料與從安全建議收集的規則進行比較，以產生發現結果。Amazon Inspector 會掃描執行個體，找出套件漏洞和網路連線性問題。如需針對這些問題所產生之發現項目類型的資訊，請參閱在 Amazon Inspector 中查找類型。

Amazon Inspector 每 24 小時執行一次網路連線掃描，而套件弱點掃描則會根據與執行個體相關聯的掃描方法，以可變步頻率執行。

掃瞄方法

Package 弱點掃瞄可以使用代理程式或無代理程式掃瞄方法執行。這些掃描方法決定 Amazon Inspector 如何以及何時從 EC2 執行個體收集軟體庫存以進行套件漏洞掃描。以代理程式為基礎的方法依賴 SSM 代理程式來收集軟體清查，而無代理程式方法則使用 Amazon EBS 快照而非代理程式。

Amazon Inspector 使用的掃描方法取決於您帳戶的掃描模式設定。如需詳細資訊，請參閱，管理掃描模式。

若要啟用 Amazon EC2 掃描，請參閱啟動掃瞄類型。

代理程式型掃描

代理程式型掃描會在所有合格的執行個體上使用 SSM 代理程式持續執行。對於以代理程式為基礎的掃描，Amazon Inspector 會使用 SSM 關聯和透過這些關聯安裝的外掛程式，從您的執行個體收集軟體

庫存。除了針對作業系統套件進行封裝弱點掃描之外，Amazon Inspector 代理程式掃描還可以透過以 Linux 為基礎的執行個體中的應用程式程式設計語言套件偵測套件漏洞。Amazon Inspector 深度檢查 Amazon EC2 Linux 實例

下列程序說明 Amazon Inspector 如何使用 SSM 來收集庫存並執行代理程式型掃描：

1. Amazon Inspector 會在您的帳戶中建立 SSM 關聯，以便從您的執行個體收集庫存。對於某些執行個體類型 (Windows 和 Linux)，這些關聯會在個別執行個體上安裝外掛程式以收集庫存。
2. Amazon Inspector 會使用 SSM 從執行個體擷取套件庫存。
3. Amazon Inspector 會評估擷取的庫存，並針對任何偵測到的弱點產生發現。

合格的實例

如果執行個體符合下列條件，Amazon Inspector 將使用以代理程式為基礎的方法掃描執行個體：

- 執行個體具有支援的作業系統。如需支援的作業系統清單，請參閱的代理程式型掃描支援欄。the section called “支援 Amazon EC2 掃描的作業系統”
- Amazon Inspector EC2 排除標籤不會從掃描中排除執行個體。
- 執行個體受 SSM 管理。如需驗證和設定代理程式的指示，請參閱設定 SSM 代理程式。

代理程式型掃瞄行為

使用以代理程式為基礎的掃描方法時，Amazon Inspector 會在下列情況下啟動 EC2 執行個體的新弱點掃描：

- 當您啟動新的 EC2 執行個體時。
- 當您在現有 EC2 執行個體 (Linux 和 Mac) 上安裝新軟體時。
- 當 Amazon Inspector 將新的常見漏洞和暴露 (CVE) 項目添加到其資料庫時，並且 CVE 與您的 EC2 執行個體 (Linux 和 Mac) 相關。

當初始掃描完成時，Amazon Inspector 會更新 EC2 執行個體的「上次掃描」欄位。此後，當 Amazon Inspector 評估 SSM 庫存時 (依預設每 30 分鐘)，或是因為影響該執行個體的新 CVE 已新增至 Amazon Inspector 資料庫而重新掃描執行個體時，就會更新「上次掃描」欄位。

您可以從帳戶管理頁面上的 [執行個體] 索引標籤或使用ListCoverage指令，檢查 EC2 執行個體上次掃描是否有漏洞的時間。

設定 SSM 代理程式

為了讓 Amazon Inspector 能夠使用以代理程式為基礎的掃描方法偵測 Amazon EC2 執行個體的軟體漏洞，該執行個體必須是 Amazon EC2 系統管理員 (SSM) 中的受管執行個體。SSM 代管執行個體已安裝並執行 SSM 代理程式，且 SSM 具有管理執行個體的權限。如果您已經使用 SSM 來管理執行個體，則代理程式型掃描不需要其他步驟。

SSM 代理程式預設會安裝在從某些 Amazon 機器映像 (AMI) 建立的 EC2 執行個體上。如需詳細資訊，請參閱AWS Systems Manager 使用指南中的關於 SSM 代理程式。不過，即使已安裝，您也可能需要手動啟動 SSM 代理程式，並授與 SSM 權限來管理您的執行個體。

下列程序說明如何使用 IAM 執行個體設定檔將 Amazon EC2 執行個體設定為受管執行個體。該程序還提供了《AWS Systems Manager 使用指南》中更詳細資訊的連結。

AmazonSSMManagedInstanceCore是附加執行個體設定檔時所要使用的建議政策。此政策具有 Amazon Inspector EC2 掃描所需的所有許可。

> **Note**
>
> 您也可以使用 SSM 預設主機管理組態，將所有 EC2 執行個體的 SSM 管理自動化，而無需使用 IAM 執行個體設定檔。如需詳細資訊，請參閱預設主機管理組態。

為 Amazon EC2 執行個體設定 SSM

1. 如果您的作業系統廠商尚未安裝，請安裝 SSM 代理程式。如需詳細資訊，請參閱使用 SSM 代理程式。
2. 使用 AWS CLI 來確認 SSM 代理程式是否正在執行。如需詳細資訊，請參閱檢查 SSM 代理程式狀態和啟動代理程式。
3. 授予 SSM 管理執行個體的權限。您可以透過建立 IAM 執行個體設定檔並將其附加到執行個體來授予權限。我們建議您使用此AmazonSSMManagedInstanceCore政策，因為此政策具有 Amazon Inspector 掃描所需的「SSM 代理商」、「SSM 庫存」和「SSM 狀態管理員」的許可。如需使用這些權限建立執行個體設定檔並附加執行個體的指示，請參閱為 Systems Manager 設定執行個體權限。
4. (選擇性) 啟動 SSM 代理程式的自動更新。如需詳細資訊，請參閱自動更新 SSM 代理程式。
5. (選擇性) 將 Systems Manager 設定為使用 Amazon Virtual Private Cloud 端 (Amazon VPC) 端點。如需詳細資訊，請參閱建立 Amazon VPC 端點。

> **Important**
>
> Amazon Inspector 需要您帳戶中的 Systems Manager 理員狀態管理員關聯，才能收集軟體應用程式庫存。`InspectorInventoryCollection-do-not-delete`如果尚未存在，Amazon Inspector 會自動創建一個稱為的關聯。
> Amazon Inspector 還需要資源資料同步，`InspectorResourceDataSync-do-not-delete`如果尚未存在，則會自動建立呼叫的資料同步。如需詳細資訊，請參閱AWS Systems Manager 使用指南中的設定詳細目錄的資源資料同步。每個帳號可以對每個區域進行一定數量的資源資料同步。如需詳細資訊，請參閱 SSM 端點和配額中的資源資料同步處理數目上限 (AWS 帳戶 每個區域)。如果您已達到此上限，則需要刪除資源資料同步，請參閱管理資源資料同步。

為掃描建立的 SSM 資源

Amazon Inspector 需要您帳戶中的許多 SSM 資源才能執行 Amazon EC2 掃描。當您第一次啟用 Amazon Inspector EC2 掃描時，會建立下列資源：

> **Note**
>
> 如果在您的帳戶啟用 Amazon Inspector Amazon EC2 掃描時刪除這些 SSM 資源中的任何一個，Amazon Inspector 會在下一次掃描間隔時嘗試重新建立這些資源。

`InspectorInventoryCollection-do-not-delete`

這是一個 Systems Manager 狀態管理員 (SSM) 關聯，Amazon Inspector 用來從您的 Amazon EC2 執行個體收集軟體應用程式庫存。如果您的帳戶已經有用於收集庫存的 SSM 關聯`InstanceIds*`，Amazon Inspector 將使用該關聯，而不是建立自己的關聯。

`InspectorResourceDataSync-do-not-delete`

這是一種資源資料同步，Amazon Inspector 用來將收集的庫存資料從您的 Amazon EC2 執行個體傳送到 Amazon S3 儲存貯體所擁有的 Amazon Inspector S3 儲存貯體。如需詳細資訊，請參閱AWS Systems Manager 使用指南中的設定詳細目錄的資源資料同步。

`InspectorDistributor-do-not-delete`

這是 Amazon Inspector 用於掃描 Windows 執行個體的 SSM 關聯。此關聯會在您的 Windows 執行個體上安裝 Amazon Inspector SSM 外掛程式。如果無意中刪除了外掛程式檔案，則此關聯會在下一個關聯間隔時重新安裝該檔案。

`InvokeInspectorSsmPlugin-do-not-delete`

這是 Amazon Inspector 用於掃描 Windows 執行個體的 SSM 關聯。此關聯允許 Amazon Inspector 使用該外掛程式啟動掃描，您也可以使用它來設定 Windows 執行個體掃描的自訂間隔。如需詳細資訊，請參閱 設定Windows執行個體掃描的自訂排程。

`InspectorLinuxDistributor-do-not-delete`

這是亞馬遜檢查器用於亞馬 Amazon EC2 Linux 深度檢查的 SSM 關聯。此關聯會在您的 Linux 執行個體上安裝 Amazon Inspector SSM 外掛程式。

`InvokeInspectorLinuxSsmPlugin-do-not-delete`

這是亞馬遜檢查器用於亞馬 Amazon EC2 Linux 深度檢查的 SSM 關聯。此關聯可讓 Amazon Inspector 使用外掛程式啟動掃描。

> **Note**
>
> 當您停用 Amazon Inspector 亞馬遜 EC2 掃描或深度檢查時，所有 SSM 資源都會自動從對應的 Linux 主機解除安裝。

無代理程式掃描

當您的帳戶處於混合掃描模式 (包括以代理程式為基礎和無代理程式掃描) 時，Amazon Inspector 會在合格的執行個體上使用無代理程式掃描方法。對於無代理程式掃描，Amazon Inspector 會使用 EBS 快照從您的執行個體收集軟體庫存。使用無代理程式方法掃描的執行個體會同時掃描作業系統套件和應用程式設計語言套件弱點。

> **Note**
>
> 掃描 Linux 執行個體是否有應用程式設計語言套件弱點時，無代理程式方法會掃描所有可用的路徑，而代理程式型掃描只會掃描您指定為其中一部分的預設路徑和其他路徑。Amazon Inspector 深度檢查 Amazon EC2 Linux 實例這可能會導致相同的執行個體具有不同的發現項目，具體取決於是使用代理程式型方法還是無代理程式方法進行掃描。

下列程序說明 Amazon Inspector 如何使用 EBS 快照來收集庫存並執行無代理程式掃描：

1. Amazon Inspector 會針對連接至執行個體的所有磁碟區建立 EBS 快照。使用 Amazon Inspector 時，快照會儲存在您的帳戶中，並以標記`InspectorScan`為標籤金鑰，以及唯一的掃描 ID 做為標籤值。
2. Amazon Inspector 使用 EBS 直接 API 從快照擷取資料，並評估這些資料是否存在漏洞。針對任何偵測到的弱點產生發現項目。
3. Amazon Inspector 會刪除它在您的帳戶中建立的 EBS 快照。

合格的實例

如果執行個體符合下列條件，Amazon Inspector 將使用無代理程式方法掃描執行個體：

- 執行個體具有支援的作業系統。如需支援的作業系統清單，請參閱的代理程式型掃描支援欄。the section called “支援 Amazon EC2 掃描的作業系統”
- Amazon Inspector EC2 排除標籤不會從掃描中排除執行個體。
- 執行個體的狀態為`Unmanaged EC2 instance`、`Stale inventory`或`No inventory`。
- 執行個體為 EBS 支援，並具有下列其中一種檔案系統格式：
  - `ext3`
  - `ext4`
  - `xfs`

無代理程式掃瞄行為

當您的帳戶設定為混合式掃描時，Amazon Inspector 會每 24 小時在合格的執行個體上執行一次無代理程式掃描。Amazon Inspector 每小時偵測並掃描新符合資格的執行個體，其中包括沒有 SSM 代理程式的新執行個體，或狀態已變更為的預先存在執行個體。`SSM_UNMANAGED`

每當 Amazon EC2 執行個體在無代理程式掃描後掃描從執行個體擷取的快照時，Amazon Inspector 就會更新上次掃描的欄位。

您可以從帳戶管理頁面上的 [執行個體] 索引標籤或使用ListCoverage指令，檢查 EC2 執行個體上次掃描是否有漏洞的時間。

管理掃描模式

您的 EC2 掃描模式會決定 Amazon Inspector 在您的帳戶中執行 EC2 掃描時會使用哪些掃描方法。您可以從 [一般設定] 下的 [EC2 掃描設定] 頁面檢視帳戶的掃描模式。獨立帳戶或 Amazon Inspector 委

派的管理員可以變更掃描模式。當您將掃描模式設定為 Amazon Inspector 委派管理員時，系統會為組織中的所有成員帳戶設定掃描模式。Amazon Inspector 具有以下掃描模式：

代理程式型掃描 — 在此掃描模式下，Amazon Inspector 在掃描套件弱點時將專門使用以代理程式為基礎的掃描方法。此掃描模式只會掃描您帳戶中的 SSM 代管執行個體，但具有提供持續掃描以回應新 CVE 或執行個體變更的好處。以代理程式為基礎的掃描也為合格的執行個體提供 Amazon Inspector 深這是新啟動帳號的預設掃描模式。

混合式掃描 — 在此掃描模式中，Amazon Inspector 使用代理程式和無代理程式方法的組合來掃描套件漏洞。對於已安裝和設定 SSM 代理程式的合格 EC2 執行個體，Amazon Inspector 會使用以代理程式為基礎的方法。對於非 SSM 受管的合格執行個體，Amazon Inspector 會針對符合資格的 EBS 支援執行個體使用無代理程式方法。

變更掃描模式

1. 打開 Amazon Inspector 控制台 https://console.aws.amazon.com/inspector/v2/home.
2. 使用頁面右上角的選取 AWS 區域 器，選取要變更 EC2 掃描模式的區域。
3. 從側邊導覽面板的 [一般設定] 下，選取 [EC2 掃描設定]。
4. 在掃描模式下，選取編輯。
5. 選擇掃描模式，然後選取 [儲存變更]。

將執行個體排除在 Amazon Inspector

您可以標記特定執行個體，將其排除在 Amazon Inspector 掃描之外。從掃描中排除執行個體有助於防止無法執行的警示。排除的執行個體不會向您收費。

若要從掃描中排除 EC2 執行個體，請使用下列金鑰標記該執行個體：

- `InspectorEc2Exclusion`

值是可選的。

如需新增標籤的詳細資訊，請參閱標記您的 Amazon EC2 資源。

此外，您可以將加密的 EBS 磁碟區排除在無代理程式掃描之外，方法是使用標籤來加密該磁碟區的 AWS KMS 金鑰。`InspectorEc2Exclusion`如需詳細資訊，請參閱標記金鑰

支援的作業系統

Amazon Inspector 會掃描支援的 Mac、視窗和 Linux EC2 執行個體，找出作業系統套件中的漏洞。對於 Linux 執行個體，Amazon Inspector 可以使用Amazon Inspector 深度檢查 Amazon EC2 Linux 實例. 對於 Mac 和 Windows 執行個體，只會掃描作業系統套件。

如需有關支援作業系統的資訊，包括哪些作業系統可在沒有 SSM 代理程式的情況下進行掃描，請參閱支援 Amazon EC2 掃描的作業系統。

Amazon Inspector 深度檢查 Amazon EC2 Linux 實例

Amazon Inspector 擴大其 Amazon EC2 掃描範圍，包括深度檢查。透過深入檢查，Amazon Inspector 可以偵測 Linux 型 Amazon EC2 執行個體中應用程式設計語言套件的套件漏洞。

Amazon Inspector 掃描程式設計語言套件程式庫的預設路徑。除了預設路徑之外，您還可以規劃自訂路徑。如需詳細資訊，請參閱 Amazon Inspector 深度檢查的自訂路徑。

亞馬遜檢查器會使用透過 Amazon Inspector SSM 外掛程式收集的資料執行深度檢查掃描。若要管理外掛程式並針對 Linux 執行深度檢查，Amazon Inspector 會在您的帳戶`InvokeInspectorLinuxSsmPlugin-do-not-delete`中自動建立下列 SSM 關聯。這發生在 Amazon Inspector 激活深度檢查時。

Amazon Inspector 每 6 小時會從執行個體收集更新的應用程式庫存以進行深度檢

如需 Amazon Inspector 支援深度檢查的程式設計語言清單，請參閱支援的程式設計語言：Amazon EC2 深度檢查。

> **Note**
>
> Windows 或 Mac 執行個體不支援深度檢查。

啟動或停用深度檢查

> **Note**
>
> 對於在 2023 年 4 月 17 日之後啟用亞馬遜檢查器的帳戶，深度檢查會在 Amazon EC2 掃描中自動啟用。

您可以從「帳戶管理」頁面上的 Amazon EC2 掃描欄，檢查 Amazon Inspector 主控台中某個帳戶的深度檢查是否有效。如果未啟用深度檢驗，此欄會顯示「已啟動」(深度檢查已停用)。若要以程式設計方式檢查啟用狀態，請使用 GetEc2DeepInspectionConfigurationAPI。或者，對於多個帳戶，請使用 BatchGetMemberEc2DeepInspectionStatusAPI。

如果您在 2023 年 4 月 17 日之前啟動了 Amazon Inspector，則可以透過主控台橫幅或 UpdateEc2DeepInspectionConfigurationAPI 啟用深度檢查。如果您是 Amazon Inspector 中某個組織的委派管理員，則可以使用 BatchUpdateMemberEc2DeepInspectionStatusAPI 為您自己和您的成員帳戶啟用它。

您可以透過 UpdateEc2DeepInspectionConfigurationAPI 停用深度檢查。組織中的成員帳戶無法停用深度檢查。而是必須由其委派的系統管理員使用 BatchUpdateMemberEc2DeepInspectionStatusAPI 停用成員帳戶。

關於 Amazon Inspector SSM 外掛程式

Amazon Inspector 使用 Amazon Inspector SSM 外掛程式來執行 Linux 執行個體的深度檢查。Amazon Inspector SSM 外掛程式會自動安裝在您的 Linux 執行個體上，位於下列目錄中：`/opt/aws/inspector/bin`可執行檔的名稱是`inspectorssmplugin`。

> **Note**
>
> Amazon Inspector 使用系統管理器代理商在您的 Amazon EC2 執行個體中部署外掛程式。「系統管理員代理商」支援「系統管理員」指南中列為支援套件平台和架構的作業系統。您的 Amazon EC2 執行個體作業系統必須由系統管理員代理商和 Amazon Inspector 支援，才能執行深度檢查掃描。

Amazon Inspector 會建立下列檔案目錄，以管理 Amazon Inspector SSM 外掛程式所收集以進行深度檢查的資料：

- `/opt/aws/inspector/var/input`
- `/opt/aws/inspector/var/output`
  - 此目錄`packages.txt`中的儲存深度檢查所發現之封裝的完整路徑。如果 Amazon Inspector 在您的執行個體上多次偵測到相同的套件，則此檔案會列出找到該套件的每個位置。

Amazon Inspector 將外掛程式的日誌存放在`/var/log/amazon/inspector`目錄中。

卸載 Amazon Inspector SSM 插件

如果無意中刪除`inspectorssmplugin`檔案，`InspectorLinuxDistributor-do-not-delete`SSM 關聯會嘗試在下次掃描間隔時重新安裝外掛程式。

如果您停用 Amazon EC2 掃描，該外掛程式將自動從所有 Linux 主機解除安裝。

Amazon Inspector 深度檢查的自訂路徑

您可以為 Amazon Inspector 設定自訂路徑，以便在對 Linux Amazon EC2 執行個體執行深度檢查時進行搜尋。當您新增自訂路徑時，Amazon Inspector 會掃描該目錄中的套件及其中的所有子目錄。

所有帳戶最多可為其個別帳戶定義 5 個自訂路徑。如果您是組織的委派系統管理員，則可以定義 5 個將套用至整個組織的其他路徑。組織中每個帳戶最多可掃描 10 個自訂路徑。

除了針對所有帳戶掃描的下列預設路徑外，Amazon Inspector 還會掃描所有自訂路徑：

- `/usr/lib`
- `/usr/lib64`
- `/usr/local/lib`
- `/usr/local/lib64`

> **Note**
>
> 自訂路徑必須是本機路徑。Amazon Inspector 不會掃描對應的網路路徑，例如網路檔案系統 (NFS) 掛載或 Amazon S3 檔案系統掛載。

自訂路徑的格式

以下是自訂路徑的格式範例：`/home/usr1/project01`

您的自訂路徑長度不得超過 256 個字元。

每個執行個體有 5,000 個套件限制，套件庫存收集時間上限為 15 分鐘。我們建議您嘗試選擇自訂路徑，以協助您避免這些限制。

在控制台中設置自定義路徑

Console

以 Amazon Inspector 委派的管理員身分登入，然後按照以下步驟為您的組織新增自訂路徑。

1. 打開 Amazon Inspector 控制台 https://console.aws.amazon.com/inspector/v2/home.
2. 使用頁面右上角的選 AWS 區域 擇器，選取您要啟用 Lambda 標準掃描的區域。
3. 從側邊導覽面板的 [一般設定] 下，選取 [EC2 掃描設定]。
4. 在您自己帳戶的自訂路徑下，選取 [編輯] 以新增個別帳戶的路徑。如果您是委派管理員，則可以在組織的 [自訂路徑] 窗格中選擇 [編輯]，為組織內的所有帳戶新增自訂路徑。
5. 在文字方塊中輸入您的自訂路徑。
6. 選擇「儲存」以儲存您的自訂路徑。Amazon Inspector 將在下一次深度檢查中包含這些路徑。

API

執行 UpdateEc2DeepInspectionConfiguration 命令。用於`packagePaths`指定要掃描的路徑陣列。

支援的程式設計語言

對於 Linux 執行個體，除了作業系統套件中的弱點之外，Amazon Inspector 深度檢查還可產生應用程式設計語言套件的發現結果。對於 Mac 和 Windows 執行個體，只會掃描作業系統套件。

如需支援之程式設計語言的資訊，請參閱支援 Amazon Inspector 深度檢查的程式設計。

使用 Amazon Inspector 掃描 Windows EC2 實例

> **Note**
>
> 2022 年 8 月 31 日，Amazon Inspector 擴大了其 Amazon EC2 掃描範圍，以包括執行中的 EC2 執行個體Windows。

Amazon Inspector 會自動探索所有受支援的Windows執行個體，並將它們包含在連續掃描中，無需執行任何 如需支援哪些執行個體的資訊，請參閱支援 Amazon EC2 掃描的作業系統。

與掃描 Linux 執行個體不同，Amazon Inspector 會定期執行Windows掃描。 Windows執行個體一開始會在探索時掃描，然後每 6 小時掃描一次。不過，預設的 6 小時掃描間隔是可調整的。如需詳細資訊，請參閱 設定Windows執行個體掃描的自訂排程。以下是 Amazon Inspector 如何掃描Windows執行個體的概觀：

1. 啟動 Amazon EC2 掃描後，Amazon Inspector 會為您的Windows資源建立新的 SSM 關聯：`InspectorDistributor-do-not-delete`、`InspectorInventoryCollection-do-not-delete`、和`InvokeInspectorSsmPlugin-do-not-delete`。
2. `InspectorDistributor-do-not-delete`SSM 關聯會使用 SSM 文件和 `AWS-ConfigureAWSPackage`、`AmazonInspector2-InspectorSsmPlugin`SSM 代理商套件，在您的執行個體上安裝 Amazon Inspector SSM 外掛程式。Windows如需詳細資訊，請參閱關於 Amazon Inspector SSM 插件 Windows。
3. `InvokeInspectorSsmPlugin-do-not-delete`SSM 關聯會定期執行 Amazon Inspector SSM 外掛程式，以收集執行個體資料並產生 Amazon Inspector 發現項目。依預設，間隔為每 6 小時一次。不過，您可以使用 SSM 為關聯設定 cron 運算式或速率運算式來自訂此項目。如需詳細資訊，請參閱《AWS Systems Manager 使用指南》中的參考：Systems Manager 的 Cron 和速率運算式。

> **Note**
>
> Amazon Inspector 將更新的開放漏洞和評估語言 (OVAL) 定義檔案暫存到 S3 儲存貯體`inspector2-oval-prod-`*`REGION`*。此 S3 儲存貯體包含掃描中使用的 OVAL 定義，不應該進行修改。變更此設定可防止 Amazon Inspector 在新 CVE 發行時掃描新 CVE。

Windows執行個體的 Amazon Inspector 掃描

若要掃描Windows執行個體，Amazon Inspector 要求執行個體必須符合下列條件：

- 執行個體是 SSM 代管執行個體。如需設定執行個體進行掃描的指示，請參閱設定 SSM 代理程式。
- 執行個體作業系統是支援的Windows作業系統之一。如需支援作業系統的完整清單，請參閱支援 Amazon EC2 掃描的作業系統。
- 執行個體已安裝 Amazon Inspector SSM 外掛程式。Amazon Inspector 會在探索時自動為受管執行個體安裝 Amazon Inspector SSM 外掛程式。有關插件的詳細信息，請參見下一個主題。

> **Note**
>
> 如果您的主機在沒有外送網際網路存取權的 Amazon VPC 中執行，則Windows掃描需要您的主機必須能夠存取區域性 Amazon S3 端點。若要了解如何設定 Amazon S3 Amazon VPC 端點，請參閱 Amazon 虛擬私有雲使用者指南中的建立閘道端點。如果您的 Amazon VPC 端點政策限制了對外部 S3 儲存貯體的存取，您必須特別允許存取 Amazon Inspector 所維護的儲存貯體，以存 AWS 區域 放用於評估執行個體的 OVAL 定義。此值區的格式如下：`inspector2-oval-prod-REGION`。

關於 Amazon Inspector SSM 插件 Windows

Amazon Inspector SSM 外掛程式需要 Amazon Inspector 掃描您的Windows執行個體。Amazon Inspector SSM 外掛程式會自動安裝在您的執行Windows個體上`C:\Program Files\Amazon\Inspector`，而可執行的二進位檔案會命名為`InspectorSsmPlugin.exe`。

系統會建立下列檔案位置來儲存 Amazon Inspector SSM 外掛程式收集的資料：

- `C:\ProgramData\Amazon\Inspector\Input`
- `C:\ProgramData\Amazon\Inspector\Output`
- `C:\ProgramData\Amazon\Inspector\Logs`

> **Note**
>
> 默認情況下，Amazon Inspector SSM 插件以低於正常優先級運行。

卸載 Amazon Inspector SSM 插件

如果無意中刪除`InspectorSsmPlugin.exe`檔案，`InspectorDistributor-do-not-delete`SSM 關聯會在下次掃描間隔Windows時重新安裝外掛程式。如果您想要解除安裝 Amazon Inspector SSM 外掛程式，可以在`AmazonInspector2-ConfigureInspectorSsmPlugin`文件上使用「解除安裝」動作。

此外，如果您停用 Amazon EC2 掃描，Amazon Inspector SSM 外掛程式也會自動從所有Windows主機解除安裝。

> **Note**
>
> 如果您在停用 Amazon Inspector 之前解除安裝 SSM 代理程式，Amazon Inspector SSM 外掛程式將保留在Windows主機上，但不會再將資料傳送到 Amazon Inspector SSM 外掛程式。如需詳細資訊，請參閱 停用 Amazon Inspector。

設定Windows執行個體掃描的自訂排程

您可以使用 SSM 為`InvokeInspectorSsmPlugin-do-not-delete`關聯設定 cron 運算式或費率運算式，自訂 Windows Amazon EC2 執行個體掃描之間的時間。如需詳細資訊，請參閱使用指南中的參考：Systems Manager 的 Cron 和速率運算式，或使用下列指示。AWS Systems Manager

從下列程式碼範例中選取，以使用速率運算式或 cron 運算式，將Windows執行個體的掃描頻率從預設 6 小時變更為 12 小時。

下列範例會要求您使用名AssociationId為的關聯`InvokeInspectorSsmPlugin-do-not-delete`。您可以AssociationId通過運行以下 AWS CLI 命令來檢索您的：

```
$ aws ssm list-associations --association-filter-list
 "key=AssociationName,value=InvokeInspectorSsmPlugin-do-not-delete" --region us-east-1
```

> **Note**
>
> AssociationId是地區，因此您必須先擷取每個 ID 的唯一 ID AWS 區域。然後，您可以執行指令來變更要為執行個Windows體設定自訂掃描排程的每個區域中的掃描頻率。

Example rate expression

```
$ aws ssm update-association \
--association-id "YourAssociationId" \
--association-name "InvokeInspectorSsmPlugin-do-not-delete" \
--schedule-expression "rate(12 hours)"
```

Example cron expression

```
$ aws ssm update-association \
```

```
--association-id "YourAssociationId" \
--association-name "InvokeInspectorSsmPlugin-do-not-delete" \
--schedule-expression "cron(0 0/12 * * ? *)"
```

使用 Amazon 檢查器掃描亞馬遜 ECR 容器映像

Amazon Inspector 會掃描存放在 Amazon ECR 中的容器映像中，找出軟體弱點，以產生 Pack age 件漏洞的發現。如需針對這些問題所產生之發現項目類型的資訊，請參閱在 Amazon Inspector 中查找類型。

當您啟用 Amazon ECR 的亞馬遜檢查器掃描時，您將 Amazon Inspector 設置為您的私有註冊表首選掃描服務。這會以增強型掃描取代 Amazon ECR 免費提供的預設基本掃描，這是透過 Amazon Inspector 提供和計費的增強型掃描。

Amazon Inspector 提供的增強型掃描可讓您在登錄層級針對作業系統和程式設計語言套件進行弱點掃描的好處。您可以在 Amazon ECR 主控台上，針對影像的每一層，在映像層級使用增強型掃描來檢閱發現的發現項目。此外，您可以在其他不適用於基本掃描發現項目 (包括和 Amazon) 的服務中檢閱 AWS Security Hub 和處理這些發現項目 EventBridge。您可以在 Amazon Inspector 主控台上檢視由掃描所發現的發現項目，網址為 https://console.aws.amazon.com/inspector/v2/home。如需有關使用發現項目的資訊，請參閱管理 Amazon Inspector 中的發現。

如需啟用 Amazon ECR 掃描的指示，請參閱啟動掃瞄類型。

Amazon ECR 掃描的掃描行為

當您第一次啟動 ECR 掃描並將儲存庫設定為連續掃描時，Amazon Inspector 會偵測您在 30 天內推送或過去 90 天內提取的所有合格映像。然後，Amazon Inspector 會掃描偵測到的影像，並將其掃描狀態設定為`active`。只要在過去 90 天內 (依預設) 或在您設定的 ECR 重新掃描持續時間內推送或拉出影像，Amazon Inspector 就會持續監控影像。如需詳細資訊，請參閱 設定 ECR 重新掃描持續時間。

對於持續掃描，Amazon Inspector 會在下列情況下啟動容器映像的新弱點掃描：

- 每當一個新的容器映像被推送。
- 每當 Amazon Inspector 在其資料庫中新增一個新的常見漏洞和曝光 (CVE) 項目時，並且 CVE 與該容器映像相關 (僅限連續掃描)。

如果您在推送掃描時設定儲存庫，則只有在您推送影像時才會掃描影像。

您可以從 [帳戶管理] 頁面上的 [容器映像] 索引標籤或使用 ListCoverageAPI，檢查上次檢查容器映像檔是否有漏洞的時間。Amazon Inspector 會更新 Amazon ECR 影像的「上次掃描時間」欄位，以回應下列事件：

- 當 Amazon Inspector 器完成容器映像的初始掃描時。
- 當 Amazon Inspector 重新掃描容器映像時，因為影響該容器映像的新常見漏洞和曝光 (CVE) 項目已新增至 Amazon Inspector 資料庫。

支援的作業系統和媒體類型

如需有關支援作業系統的資訊，請參閱支援 Amazon ECR 掃描的作業系統。

Amazon ECR 儲存庫的 Amazon Inspector 掃描涵蓋下列支援的媒體類型：

- `"application/vnd.docker.distribution.manifest.v1+json"`
- `"application/vnd.docker.distribution.manifest.v1+prettyjws"`
- `"application/vnd.oci.image.manifest.v1+json"`
- `"application/vnd.docker.distribution.manifest.v2+json"`

> **Note**
>
> 不支援刮擦`DockerV2ListMediaType`影像和影像。

為 Amazon ECR 儲存庫設定增強型掃描

當您針對 Amazon ECR 容器映像啟用 Amazon Inspector 掃描時，您可以變更私有登錄的掃描組態設定。登錄的掃描類型會從基本掃描變更為 Amazon Inspector 提供的增強型掃描。如需詳細資訊，請參閱 Amazon ECR 使用者指南中的影像掃描。

您可以在 ECR 的儲存庫層級管理增強型掃描的設定。您可以為存放庫選擇持續掃描或推送掃描。連續掃描包括推送掃描和自動重新掃描。推送掃描僅在您最初推送影像時進行掃描。對於這兩個選項，您都可以透過包含篩選器調整掃描範圍。根據預設，當您第一次啟用增強型掃描時，您的設定會設定為持續掃描所有儲存庫。

設定您的增強型掃描設定

1. 在 https://console.aws.amazon.com/ecr/ 開啟 Amazon ECR 主控台。

2. 在頁面右上角的選取 AWS 區域 器中，選取具有您要掃描之儲存庫的區域。
3. 在功能窗格中，選擇 [私人登錄]，然後選擇 [掃描]。
4. 在 [掃描類型] 下，確定已選取 [增強型掃描]。如果不是，請選取 [增強型掃描]。

   依預設，會選取「持續掃描所有儲存庫」選項，以開啟所有儲存庫的完整 Amazon Inspector 掃描涵蓋範圍。
5. 取消選取持續掃描所有儲存庫，以篩選要連續掃描或推送時掃描的儲存庫。

如需設定增強型掃描的詳細資訊，請參閱 Amazon ECR 使用者指南中的使用增強型掃描。

設定 ECR 重新掃描持續時間

ECR 重新掃描持續時間設定可決定 Amazon Inspector 持續監控儲存庫中容器映像的時間長度。您可以設定影像推送日期和影像提取日期的重新掃描持續時間。新帳戶 (包括新增至組織的新帳戶) 的預設掃描持續時間為 90 天。

影像推送日期持續期

映像推送日期持續時間可決定 Amazon Inspector 在最新提取日期之後將影像推送至儲存庫之後持續監控影像的時間長度。下列選項可作為重新掃描持續時間使用：

- 14 天
- 30 天
- 六十天
- 90 天 (預設值)
- 180 天
- 生命週期

影像拉取日期持續時

影像提取日期持續時間決定 Amazon Inspector 在最近提取日期之後持續監控影像的時間長度。下列選項可作為重新掃描持續時間使用：

- 14 天
- 30 天
- 六十天

- 90 天 (預設值)
- 180 天

只要在設定的推送和拉出日期內推送或拉出影像，Amazon Inspector 就會繼續監控和重新掃描影像。如果映像尚未在設定的推送和提取日期內推送或提取，Amazon Inspector 會停止監控該影像。

> **Note**
>
> 當 Amazon Inspector 停止監控影像時，會將影像掃描狀態碼設定為，`inactive`並將程式碼原因為`expired`。然後，它會將所有關聯的影像發現項目排程為關閉。

設定最適合您環境的重新掃描持續時間。例如，如果您經常建立影像，請選擇較短的掃描持續時間。同樣地，如果長時間使用影像，請選擇較長的掃描持續時間。

當您從委派的管理員帳戶設定重新掃描持續時間時，Amazon Inspector 會將該設定套用至組織中的所有成員帳戶。

設定 ECR 重新掃描持續時間

1. 打開 Amazon Inspector 控制台 https://console.aws.amazon.com/inspector/v2/home.
2. 在瀏覽窗格中，選擇 [一般設定]，然後選擇 [ECR 掃描設定]。
3. 在 ECR 掃描設定上，在 ECR 重新掃描持續時間下，選擇要設定的影像推送日期持續時間和影像提取日期持續時間。
4. 選擇儲存。系統會立即套用您的新設定。

> **Note**
>
> 如果您增加推送日期持續時間，Amazon Inspector 會將變更套用至針對持續掃描而設定的儲存庫中的所有主動掃描影像。但是，即使您在新的持續時間內推送非作用中影像，仍會保持非作用中的影像。

Amazon Inspector 掃描 AWS Lambda 功能

Amazon Inspector 對 AWS Lambda 功能的支援可為 Lambda 函數和層提供持續、自動化的安全漏洞評估。Amazon Inspector 提供兩種類型的 Lambda 掃描。這些掃描類型會尋找不同類型的弱點。

Amazon Inspector Lambda 標準

這是預設的 Lambda 掃描類型。Lambda 標準掃描會掃描 Lambda 函數及其層中的應用程式相依性，找出套件漏洞。如需詳細資訊，請參閱 Lambda 準掃描。

Amazon Inspector Lambda 代碼

此掃描類型會掃描函數和層中的自訂應用程式程式碼，以找出程式碼弱點。您可以啟動 Lambda 標準掃描，或同時啟動 Lambda 標準掃描和 Lambda 程式碼掃描。如需詳細資訊，請參閱 Amazon Inspector Lambda 代碼。

當您啟用 Lambda 掃描時，Amazon Inspector 會在您的帳戶中建立下列 AWS CloudTrail 服務連結通道：

- `cloudtrail:CreateServiceLinkedChannel`
- `cloudtrail:DeleteServiceLinkedChannel`

Amazon Inspector 會管理這些通道，並使用這些通道監控您的 CloudTrail 事件以進行掃描。如需有關服務連結通道的詳細資訊，請參閱使用 CLI 檢視的服務連結 CloudTrail 通道。 AWS

> **Note**
>
> Amazon Inspector 建立的服務連結管道可讓您查看帳戶中的 CloudTrail 事件，就像有 CloudTrail 追蹤一樣，不過，我們建議您建立自己的管道 CloudTrail 來管理帳戶的事件。

如需啟用 Lambda 函數掃描的指示，請參閱啟動掃瞄類型。

Lambda 函數掃描的掃描行為

啟用後，Amazon Inspector 會掃描您帳戶中過去 90 天內叫用或更新的所有 Lambda 函數。在下列情況下，Amazon Inspector 會啟動 Lambda 函數的弱點掃描：

- 一旦 Amazon Inspector 發現現有的 Lambda 函數。
- 當您將新的 Lambda 函數部署到 Lambda 服務時。
- 當您對現有的 Lambda 函數或其層的應用程式程式碼或相依性部署更新時。
- 每當 Amazon Inspector 新增一個常見漏洞和暴露 (CVE) 項目到其資料庫，而該 CVE 與您的函數相關時。

Amazon Inspector 會在整個使用期間監控每個 Lambda 函數，直到將其刪除或從掃描中排除為止。

您可以從帳戶管理頁面上的 Lambda 函數索引標籤或使用 ListCoverageAPI 來檢查 Lambda 函數是否有漏洞的最後一次檢查時間。Amazon Inspector 會更新 Lambda 函數的「上次掃描時間」欄位，以回應下列事件：

- 當 Amazon Inspector 完成 Lambda 函數的初始掃描時。
- 當一個 Lambda 函數被更新。
- 當 Amazon Inspector 重新掃描 Lambda 函數時，因為影響該函數的新 CVE 項目已添加到 Amazon Inspector 數據庫中。

支援的執行階段和合格函數

Amazon Inspector 支援 Lambda 標準掃描和 Lambda 程式碼掃描的不同執行階段 如需每種掃瞄類型支援的執行階段清單，請參閱支援的執行階段：Amazon Inspector Lambda 標準和支援的執行階段：Amazon Inspector Lambda 程式。

除了具有受支援的執行階段之外，Lambda 函數還需要符合下列條件，才能符合 Amazon Inspector 掃描的資格：

- 該函數在過去 90 天內已被調用或更新。
- 該功能被標記$LATEST。
- 該功能不會從標籤的掃描中排除。

> **Note**
>
> 過去 90 天內未叫用或修改的 Lambda 函數會自動從掃描中排除。如果再次呼叫自動排除的函數，或對 Lambda 函數程式碼進行變更，Amazon Inspector 將繼續掃描該函數。

Amazon Inspector Lambda 標準

Amazon Inspector Lambda 標準掃描可識別您新增至 Lambda 函數程式碼和層的應用程式套件相依性中的軟體弱點。例如，如果您的 Lambda 函數使用具有已知漏洞的`python-jwt`套件版本，則 Lambda 標準掃描將為該函數產生一個發現項目。

如果 Amazon Inspector 在您的 Lambda 函數應用程式 Package 相依性中偵測到漏洞，Amazon Inspector 會產生詳細的套件漏洞類型發現。

如需啟動掃瞄類型的指示，請參閱啟動掃瞄類型。

> **Note**
>
> Lambda 標準掃描不會掃描預設安裝在 Lambda 執行階段環境中的 AWS SDK 相依性。Amazon Inspector 只會掃描使用函數程式碼上傳或從圖層繼承而來的相依性。

> **Note**
>
> 停用 Amazon Inspector Lambda 標準掃描也會停用 Amazon Inspector Lambda 代碼掃描。

從 Lambda 標準掃描中排除函數

您可以標記某些函數，將它們排除在 Amazon Inspector Lambda 標準掃描之外。從掃描中排除功能有助於防止無法執行的警示。

若要從 Lambda 標準掃描中排除 Lambda 函數，請使用下列索引鍵值組標記函數：

- 關鍵字：`InspectorExclusion`
- 值：`LambdaStandardScanning`

若要從 Lambda 標準掃描中排除函數

1. 開啟 Lambda 主控台，網址為 https://console.aws.amazon.com/lambda/。
2. 選取函數。
3. 從函數表格中，選取您要從 Amazon Inspector Lambda 標準掃描中排除的函數名稱。
4. 選擇配置，然後從菜單中選擇標籤。
5. 選取管理標籤，然後選取新增標籤。
6. 在「機碼」欄位中輸入`InspectorExclusion`，然後在「值」欄位中輸入`LambdaStandardScanning`。
7. 選取儲存以新增標籤，並從 Amazon Inspector Lambda 標準掃描中排除您的函數。

如需在 Lambda 中新增標籤的詳細資訊，請參閱在 L ambda 函數上使用標籤。

Amazon Inspector Lambda 代碼

> **Important**
>
> 程式碼掃描會從 Lambda 函數擷取程式碼片段，以反白顯示偵測 這些片段可能會以明文顯示硬式編碼的憑證或其他敏感資料。

Amazon Inspector Lambda 程式碼掃描會根據 AWS 安全最佳實務，掃描 Lambda 函數中的自訂應用程式程式碼，找出程式碼弱 Lambda 程式碼掃描可以偵測程式碼中的插入瑕疵、資料外洩、弱式密碼編譯或遺漏的加密。如需有關可用區域的資訊，請參閱區域特定功能的可用性。

Lambda 標準掃描是評估函數中常見漏洞和暴露 (CVE) 所使用之應用程式套件相依性的功能。您可以使用 Lambda 標準掃描來啟動 Lambda 程式碼掃描。

Amazon Inspector 會使用自動推理和機器學習來評估您的 Lambda 函數應用程式程式碼，以分析您的應用程式程式碼以達到整體 它會根據與 Amazon CodeGuru 合作開發的內部偵測器，識別違反政策和漏洞。如需可能偵測的清單，請參閱偵測CodeGuru 器程式庫。

如果 Amazon Inspector 在您的 Lambda 函數應用程式程式碼中偵測到漏洞，Amazon Inspector 會產生詳細的程式碼弱點類型發現 此發現項目類型包含問題在程式碼中的確切位置、顯示問題的程式碼片段，以及建議的補救措施。建議的補救措施包括可用來取 plug-and-play 代易受攻擊的程式碼行的程式碼區塊。除了該發現項目的一般程式碼修正指引之外，還提供這些建議的程式碼修正。

> **Important**
>
> 程式碼修正建議是由自動推理和生成人工智慧服務提供支援，因此可能無法如預期般運作。您必須對所採用的程式碼修正建議負責。在採用之前，請務必檢閱程式碼修正建議。您可能需要編輯程式碼修正建議，以確保程式碼能如預期般執行。請參閱負責任的 AI 政策。

在發現程式碼漏洞中加密您的程式碼

CodeGuru 服務會儲存與使用 Lambda 程式碼掃描發現的程式碼弱點相關的程式碼片段。依預設，會使用由 CodeGuru 控制的AWS 擁有金鑰來加密您的程式碼，不過，您可以使用自己的客戶受管金鑰透過 Amazon Inspector API 進行加密。如需詳細資訊，請參閱 針對發現項目中的程式碼進行靜態加密

Lambda 程式碼掃描可與 Lambda 標準掃描一起啟動。如需啟動掃瞄類型的指示，請參閱啟動掃瞄類型。

從 Lambda 程式碼掃描排除函數

您可以標記某些函數，將它們排除在 Amazon Inspector Lambda 程式碼掃描之外。從掃描中排除功能有助於防止無法執行的警示。

若要從 Amazon Inspector 中排除 Lambda 函數，Lambda 程式碼會掃描使用下列索引鍵值組來標記函數：

- 關鍵字：`InspectorCodeExclusion`
- 值：`LambdaCodeScanning`

若要從 Lambda 程式碼掃描中排除函數

1. 登入 Lambda 主控台，網址為 https://console.aws.amazon.com/lambda/。
2. 選取函數。
3. 從函數表格中，選取您要從 Amazon Inspector Lambda 程式碼掃描中排除的函數名稱。
4. 選擇配置，然後從菜單中選擇標籤。
5. 選取管理標籤，然後選取新增標籤。
6. 在「機碼」欄位中輸入`InspectorCodeExclusion`，然後在「值」欄位中輸入`LambdaCodeScanning`。
7. 選取儲存以新增標籤，並從 Amazon Inspector Lambda 程式碼掃描中排除您的函數。

如需在 Lambda 中新增標籤的詳細資訊，請參閱在 L ambda 函數上使用標籤。

停用掃瞄類型

您可以隨時停用新的 Amazon Inspector 掃描類型。停用掃描類型時，您將無法存取該掃描類型產生的任何現有發現項目。如果您重新啟用掃描類型，則會掃描符合資格的資源，Amazon Inspector 會產生新的發現項目。若要保留發現項目資料的記錄，您可以在停用之前匯出發現項目。如需詳細資訊，請參閱 從 Amazon Inspector 匯出發現報告。

停用掃描類型時，該 AWS 帳戶可能會發生某些變更，具體取決於停用的掃描類型。以下是停用這些掃瞄類型時將發生的變更：

- Amazon EC2 掃描 — 當您停用 Amazon Inspector 亞馬遜 EC2 掃描帳戶時，亞 Amazon Inspector 使用的以下 SSM 關聯將被刪除：
  - `InspectorDistributor-do-not-delete`
  - `InspectorInventoryCollection-do-not-delete`
  - `InspectorLinuxDistributor-do-not-delete`
  - `InvokeInspectorLinuxSsmPlugin-do-not-delete`
  - `InvokeInspectorSsmPlugin-do-not-delete`。 此外，透過此關聯安裝的 Amazon Inspector SSM 外掛程式也會從所有Windows主機中移除。如需詳細資訊，請參閱 掃描Windows實例。
- 亞馬遜 ECR 掃描 — 當您停用某個帳戶的 Amazon ECR 容器映像掃描時，該帳戶的 Amazon ECR 掃描類型會從使用 Amazon Inspector 進行增強掃描變更為使用 Amazon ECR 進行基本掃描。
- Lambda 標準掃描 — 當您停用帳戶中的 Lambda 標準掃描時，如果程式碼掃描也處於作用中狀態，則會停用 Lambda 程式碼掃描。此外，掃描啟用時建立的 CloudTrail 服務連結通道也會被刪除。

停用掃描

停用某個帳戶的所有掃描類型會停用該帳戶的 Amazon Inspector。 AWS 區域如需詳細資訊，請參閱停用 Amazon Inspector。

若要針對多帳戶環境完成此程序，請在以 Amazon Inspector 委派管理員身分登入時遵循下列步驟。

Console

停用掃描

1. 打開 Amazon Inspector 控制台 https://console.aws.amazon.com/inspector/v2/home.
2. 使用頁面右上角的選取 AWS 區域 器，選取您要停用掃描的區域。
3. 在功能窗格中，選擇 [帳戶管理]。
4. 選擇帳戶標籤以顯示帳戶的掃描狀態。
5. 選取您要停用掃描之每個帳戶的核取方塊。
6. 選擇 [動作]，然後從 [停用] 選項中選取您要停用的掃描類型。
7. (建議) 在每個 AWS 區域 您要停用該掃描類型的步驟中重複這些步驟。

API

執行停用 API 作業。在要求中，提供您要停用掃描的帳號 ID，並resourceTypes提供一或多個EC2、ECRLAMBDA、或停LAMBDA_CODE用掃描。

EC2 執行個體的網際網路安全中心 (CIS) 掃描

當您為帳戶啟用 Amazon Inspector EC2 掃描時，您可以讓 Amazon Inspector 執行或排程獨聯體掃描。Amazon Inspector CIS 會掃描 Amazon EC2 執行個體的作業系統基準測試，以查看它們是否已根據網際網路安全中心建立的最佳實務建議進行設定。CIS 安全性基準測試計畫提供業界標準組態基準，以及安全設定系統的最佳做法。如需詳細資訊，請參閱什麼是 CIS 基準測試？

Amazon Inspector 會根據您在掃描組態中定義的執行個體標籤和掃描排程，在目標 Amazon EC2 執行個體上執行獨聯體掃描。對於每個目標執行個體，Amazon Inspector 會對執行個體執行一系列檢查。每次檢查都會評估您的系統配置是否符合特定的 CIS Benchmark 建議。每個檢查都有一個 CIS 檢查 ID 和標題，這些 ID 和標題直接與該平台的 CIS 基準建議相關。掃描完成後，您可以檢視結果，並查看執行個體針對該系統通過、失敗或略過的哪些檢查。

Amazon Inspector CIS 掃描 EC2 執行個體需求

若要在執行個體上執行獨聯體掃描，Amazon Inspector 要求執行個體符合下列條件：

- 執行個體作業系統是 CIS 掃描支援的作業系統之一。如需支援作業系統的完整清單，請參閱支持的操作系統：CIS 掃描。
- 執行個體是 Amazon EC2 Systems Manager (SSM) 受管執行個體。如需詳細資訊，請參閱使用 SSM 代理程式。
- 執行個體已安裝 Amazon Inspector SSM 外掛程式。Amazon Inspector 會自動為 SSM 受管執行個體安裝此外掛程式。
- 執行個體擁有一個執行個體設定檔，可授予 SSM 管理執行個體的許可，而 Amazon Inspector 則可執行該執行個體的 CIS 掃描。要授予這些許可，請將 AmazonInspector2 FullAccess、AmazonSSM ManagedInstanceCore 和 AmazonInspector2 個ManagedCispolicy政策附加到 IAM 角色，並將該角色作為執行個體設定檔附加到您的執行個體。如需建立和附加執行個體設定檔的指示，請參閱 Amazon EC2 使用者指南中的使用 IAM 角色。

> **Note**
>
> 在執行個體上執行獨聯體掃描時，不再需要啟用 Amazon Inspector 深度檢查。如果停用深度檢查，Amazon Inspector 仍會繼續安裝 SSM 代理程式，但不會再叫用外掛程式來執行深度檢查。這意味著您的帳戶中將存在以下關聯：`InspectorLinuxDistributor-do-not-delete`。

執行獨聯體掃描

您可以按需執行一次 CIS 掃描，也可以作為排程週期性掃描執行。若要執行掃描，請先建立掃描組態。

建立掃描組態時，您可以指定用於鎖定執行個體的標籤鍵值配對。如果您是某個組織的 Amazon Inspector 委派管理員，則可以在掃描組態中指定多個帳戶，Amazon Inspector 會在每個帳戶中尋找具有指定標記的執行個體。您可以選擇 CIS 基準測試級別進行掃描。對於每個基準，CIS 支援 1 級和 2 級設定檔，其設計目的是針對不同環境可能需要的不同層級的安全性提供基準。

- 層級 1 — 建議可在任何系統上設定的基本安全性設定。實施這些設置應該很少或不會導致服務中斷。這些建議的目標是減少系統的進入點數量，從而降低整體網路安全風險。
- 層級 2 — 針對高安全性環境建議使用更進階的安全性設定。實作這些設定需要進行規劃和協調，以將業務影響的風險降到最低。這些建議的目標是幫助您實現法規遵循。

樓層 2 延伸樓層 1。當您選擇第 2 級時，Amazon Inspector 會檢查第 1 級和第 2 級建議的所有組態。

定義掃描的參數之後，您可以選擇是以一次性掃描的形式執行 (在您完成設定後執行)，還是執行週期性掃描。週期性掃描可以在您選擇的時間每天、每週或每月執行。

> **Tip**
>
> 我們建議您選擇在掃描執行時影響系統最不可能的日期和時間。

若要建立 CIS 掃描組態

1. 在 https://console.aws.amazon.com/inspector/v2/home 打開 Amazon Inspector 控制台。
2. 使用頁面右上角的選取 AWS 區域 器，選取您 AWS 區域 要執行 CIS 掃描的位置。
3. 從導覽面板的 [指定掃描] 下，選取 [CIS 掃描]。
4. 選擇 [建立新掃描]。
    a. 輸入掃描組態名稱。
    b. 針對 Target 資源，輸入您要掃描之執行個體上之標籤的金鑰和對應值。您總共可以指定 25 個要包含在掃描中的標籤，對於每個金鑰，您最多可以指定五個不同的值。
    c. 選擇一個獨聯體基準水平。您可以選取層級 1 做為基本安全性組態，或選取層級 2 做為進階安全性組態。

5. 對於 Target 帳戶，指定要包含在掃描中的帳戶。組織中的獨立帳戶或成員可以選取 [自我]，為其帳戶建立掃描組態。Amazon Inspector 委派管理員可以選取「所有帳戶」以鎖定組織內的所有帳戶，或選取「指定帳戶」並指定要鎖定目標的成員帳戶子集。委派的系統管理員可以輸入SELF而非帳號 ID，為自己的帳戶建立掃描組態。如需更多資訊，請參閱在 AWS 組織中管理 Amazon Inspector CIS 掃描的注意事項。
6. 選擇掃描的排程。選擇 [一次性掃描] (在您完成建立掃描組態後立即執行) 或 [週期性掃描]，這些掃描會在您選擇的排程時間執行，直到刪除為止。
7. 選擇 [建立] 以完成建立掃描組態。

檢視和編輯 CIS 掃描組態

您可以隨時檢視或編輯先前排程的掃描。

檢視或編輯 CIS 掃描組態

1. 在 https://console.aws.amazon.com/inspector/v2/home 打開 Amazon Inspector 控制台。
2. 使用頁面右上角的選取 AWS 區域 器，選取您建立 CIS 掃描組態的 AWS 區域 位置。
3. 從導覽面板的 [指定掃描] 下，選取 [CIS 掃描]。
4. 選擇「預約」以檢視預約掃瞄組態。
5. 從掃描組態名稱欄中選取項目，以開啟該掃描組態的詳細資料。
6. (選擇性) 選擇編輯以變更此掃描的參數。

檢視 CIS 掃描的結果

Amazon Inspector 會在每次掃描組態執行時建立掃描任務，並以唯一的掃描 ID 收集掃描結果。

掃描結果在掃描完成後 90 天內可用。您可以檢視依檢查或目標資源彙總的掃描結果。

按檢查彙總的掃描結果

掃描結果會依掃描期間執行的每個個別檢查來分組。對於每次檢查，您都會收到通過、失敗或略過的資源數量的報告。

依資源彙總的掃描結果

掃描結果會依掃描組態目標的每個資源分組。對於每個資源，您都會收到一份報告，其中檢查該資源的已通過、失敗或已跳過的資源。

若要檢視掃描結果

1. 在 https://console.aws.amazon.com/inspector/v2/home 打開 Amazon Inspector 控制台。
2. 使用頁面右上角的選取 AWS 區域 器，選取您 AWS 區域 要檢視掃描結果的位置。
3. 從導覽面板的 [指定掃描] 下，選取 [CIS 掃描]。
4. 從「掃描 ID」欄中選取您要檢視結果的掃描 ID。
5. 選擇如何檢視掃描結果：
   - 選取 [檢查] 索引標籤以檢視依檢查彙總的掃描結果。
     - 對於列出的檢查，請在 [資源狀態] 欄中從 [已通過]、[已略過] 或 [失敗] 中選取一個數字，以開啟依該狀態和該檢查篩選的資源檢視。
   - 選取 [已掃描的資源] 索引標籤以檢視依資源彙總的掃描結果。
     - 選取資源以開啟詳細資料面板，其中列出資源已通過、失敗或略過的檢查。
6. (選擇性) 在任一檢視中使用篩選列來縮小結果。

您可以使用控制台或 API 下載 CIS 掃描的結果。

下載掃描結果

1. 在 https://console.aws.amazon.com/inspector/v2/home 打開 Amazon Inspector 控制台。
2. 使用頁面右上角的選取 AWS 區域 器，選取您 AWS 區域 要檢視掃描結果的位置。
3. 從導覽面板的 [指定掃描] 下，選取 [CIS 掃描]。
4. 從「掃描 ID」欄中選取您要檢視結果的掃描 ID。
5. 選擇 Download (下載)。如果您是委派管理員，則可以選擇下載特定會員帳戶的結果。

在 AWS 組織中管理 Amazon Inspector CIS 掃描的注意事項

在組織內執行 CIS 掃描時，會員帳戶和 Amazon Inspector 委派的管理員會與 CIS 掃描組態互動，並以不同的方式掃描結果。

當委派的系統管理員為所有帳戶建立 CIS 掃描組態時，或是組織擁有該掃描組態的成員帳號 ID 清單。無論目前委派的管理員帳戶為何，都可以管理組織擁有的掃描組態，即使是不同的帳戶建立掃描組態也是如此。該組織擁有的 CIS 掃描配置將具有 ARN，該 ARN 將組織 ID 列為所有者，遵循以下模式：`arn:aws:inspector2:`*`Region`*`:`*`111122223333`*`:owner/`*`OrganizationId`*`/cis-configuration/`*`scanId`*。帳戶 ID 將是 Organizations 管理帳戶的 ID。

> **Important**
>
> 您無法將標籤新增至組織擁有的 CIS 掃描組態。

委派的系統管理員建立掃描組態並指定SELF為目標帳戶時，其帳戶會擁有該掃描組態。即使他們離開組織，他們仍然可以管理該掃描配置。

> **Note**
>
> 委派的系統管理員無法變更目標之掃描組態的目標SELF。

由成員帳戶、獨立帳戶或委派管理員建立的掃描組態，以SELF做為目標的掃描組態，由建立這些組態的帳戶所擁有。這些 CIS 掃描配置有一個 ARN，它將該帳戶列為遵循該模式的所有者：`arn:aws:inspector2:`*`Region`*`:`*`111122223333`*`:owner/`*`111122223333`*`/cis-configuration/`*`scanId`*。帳號 ID 將是建立掃描的帳戶。

組織中的成員帳戶可以為自己的帳戶建立掃描組態。委派的系統管理員可以檢視成員建立的掃描組態，但無法編輯或刪除它們。如果成員帳戶離開組織，委派的系統管理員將無法再看到該帳戶建立的掃描組態。

委派的系統管理員可以檢視組織中任何帳號的掃描結果，包括成員排程的掃描結果。會員帳戶可以檢視其帳戶中資源的任何 CIS 掃描結果，包括委派管理員排程的資源。

Amazon Inspector 擁有 Amazon S3 存儲桶用於 Amazon Inspector CIS 掃描

Amazon Inspector 階段進行 CIS 掃描所需的更新開放弱點和評估語言 (OVAL) 定義檔案。下表列出 Amazon Inspector 擁有的所有 Amazon S3 儲存貯體，其中包含每個支援 AWS 區域的獨聯體掃描使用的橢圓形定義。如有必要，應允許在 VPC 中列出存儲桶。

> **Note**
>
> 以下每個 Amazon Inspector 擁有的 Amazon S3 儲存貯體的詳細資料都不會變更。但是，該列表可能會更新以反映新的支持 AWS 區域。您無法將這些儲存貯體用於其他 Amazon S3 作業或您自己的 Amazon S3 儲存貯體中。

独联体斗	AWS 區域
cis-datasets-prod-arn-5908f6f	歐洲 (斯德哥爾摩)
cis-datasets-prod-bah-8f88801	Middle East (Bahrain)
cis-datasets-prod-bjs-0f40506	中國 (北京)
cis-datasets-prod-bom-435a167	亞太區域 (孟買)
cis-datasets-prod-cdg-f3a9c58	Europe (Paris)
cis-datasets-prod-cgk-09eb12f	亞太區域 (雅加達)
cis-datasets-prod-cmh-63030b9	美國東部 (俄亥俄)
cis-datasets-prod-cpt-02c5c6f	非洲 (開普敦)
cis-datasets-prod-dub-984936f	歐洲 (愛爾蘭)
cis-datasets-prod-fra-6eb96eb	歐洲 (法蘭克福)
cis-datasets-prod-gru-de69f99	南美洲 (聖保羅)
cis-datasets-prod-hkg-8e30800	亞太區域 (香港)
cis-datasets-prod-iad-8438411	美國東部 (維吉尼亞北部)
cis-datasets-prod-icn-f4eff1c	亞太區域 (首爾)
cis-datasets-prod-kix-5743b21	亞太區域 (大阪)
cis-datasets-prod-lhr-8b1fbd0	歐洲 (倫敦)
cis-datasets-prod-mxp-7b1bbce	歐洲 (米蘭)
cis-datasets-prod-nrt-464f684	亞太區域 (東京)
cis-datasets-prod-osu-5bead6f	AWS GovCloud (美國東部)
cis-datasets-prod-pdt-adadf9c	AWS GovCloud (美國西部)

独联体斗	AWS 區域
cis-datasets-prod-pdx-acfb052	美國西部 (奧勒岡)
cis-datasets-prod-sfo-1515ba8	美國西部 (加利佛尼亞北部)
cis-datasets-prod-sin-309725b	亞太區域 (新加坡)
cis-datasets-prod-syd-f349107	亞太區域 (悉尼)
cis-datasets-prod-yul-5e0c95e	加拿大 (中部)
cis-datasets-prod-zhy-5a8eacb	中國 (寧夏)
cis-datasets-prod-zrh-67e0e3d	歐洲 (蘇黎世)

評估您 AWS 環境的 Amazon Inspector 覆蓋率

為了協助您評估和解譯 AWS 環境的 Amazon Inspector 涵蓋範圍，Amazon Inspector 主控台上的帳戶管理頁面提供有關您帳戶和資源之 Amazon Inspector 掃描狀態的統計資料和詳細資料。使用此頁面，您可以檢閱資源的彙總統計資料和其他資料。您也可以針對個別資源執行 Amazon Inspector 涵蓋範圍的深入分析，並深入檢閱特定資源的發現結果。如果您是某個組織委派的 Amazon Inspector 管理員，資料會包含組織中所有帳戶的統計資料和詳細資料。

評估您 AWS 環境的 Amazon Inspector 涵蓋範圍

1. 打開 Amazon Inspector 控制台 https://console.aws.amazon.com/inspector/v2/home.
2. 在功能窗格中，選擇 [帳戶管理]。
3. 在 [帳戶管理] 頁面上，選擇五種不同涵蓋範圍檢視之一的索引標籤：
   - 帳戶，用於帳戶層級涵蓋範圍。
   - 執行個體，用於亞馬遜彈性運算雲端 (Amazon EC2) 執行個體的涵蓋範圍。
   - 儲存庫，用於亞馬遜彈性容器登錄 (Amazon ECR) 儲存庫的涵蓋範圍。
   - 圖片，用於 Amazon ECR 容器映像的覆蓋範圍。
   - Lambda，用於覆蓋 Lambda 函數。

本節中的主題說明每個索引標籤提供的資訊，包括個別資源可具有的掃描狀態。

主題

評估帳戶層級涵蓋範圍

如果您的帳戶不是組織的一部分，或者不是組織委派的 Amazon Inspector 管理員帳戶，則 [帳戶] 索引標籤會提供有關您帳戶和帳戶資源掃描狀態的資訊。在此索引標籤上，您可以針對您帳戶的所有或僅針對特定類型的資源啟用或停用掃描。如需詳細資訊，請參閱 使用 Amazon Inspector 自動化資源。

如果您的帳戶是組織委派的 Amazon Inspector 管理員帳戶，則 [帳戶] 索引標籤會為組織中的帳戶提供自動啟用設定，並列出組織中的所有帳戶。對於每個帳戶，清單會指出帳戶是否已啟用 Amazon Inspector，以及為該帳戶啟動的資源掃描類型 (如果啟用)。身為委派的系統管理員，您可以使用此索引標籤來變更組織的自動啟用設定。您也可以針對個別成員帳號啟動或停用特定類型的資源掃描。如需詳細資訊，請參閱 激活 Amazon Inspector 掃描成員帳戶。

評估 Amazon EC2 執行個體的涵蓋範圍

執行個體索引標籤會顯示您 AWS 環境中的 Amazon EC2 執行個體。這些清單會在下列索引標籤上組織成群組：

- 全部 — 顯示環境中的所有執行個體。「狀態」欄會指出執行個體目前的掃瞄狀態。
- 掃描 — 顯示 Amazon Inspector 在您的環境中主動監控和掃描的所有執行個體。
- 未掃描 — 顯示所有 Amazon Inspector 未在您的環境中監控和掃描的執行個體。「原因」欄會指出 Amazon Inspector 未監控和掃描執行個體的原因。

  EC2 執行個體可能會出現在不掃描索引標籤上的任何一個原因。Amazon Inspector 使用 AWS Systems Manager (SSM) 和 SSM 代理程式來自動監控和掃描 EC2 執行個體是否有漏洞。如果執行個體沒有執行 SSM 代理程式、沒有支援 Systems Manager 的 AWS Identity and Access Management (IAM) 角色，或者沒有執行受支援的作業系統或架構，Amazon Inspector 將無法監控和掃描執行個體。如需詳細資訊，請參閱 掃描 Amazon EC2 實例。

在每個索引標籤上，[帳戶] 欄會指 AWS 帳戶 定擁有執行個體的。

EC2 執行個體標籤 — 此欄會顯示與執行個體相關聯的標籤，並可用來判斷您的執行個體是否已透過標籤掃描排除。

作業系統 — 此資料欄會顯示作業系統類型`WINDOWS`，可以是`MACLINUX`、、或`UNKNOWN`。

監控方式 — 此欄會顯示 Amazon Inspector 在此執行個體上使用以代理程式為基礎的掃描方法還是無代理程式掃描方法。

上次掃描 — 此欄會顯示 Amazon Inspector 上次檢查該資源是否存在弱點的時間。Amazon Inspector 執行掃描的頻率取決於它用來掃描執行個體的掃描方法。

若要檢閱 EC2 執行個體的其他詳細資訊，請選擇 EC2 執行個體欄中的連結。然後，Amazon Inspector 會顯示執行個體和執行個體目前發現項目的詳細資訊。若要檢閱發現項目的詳細資訊，請選擇「標題」欄中的連結。如需這些詳細資訊，請參閱Amazon Inspector 找到細節。

掃描 Amazon EC2 執行個體的狀態值

對於亞馬遜彈性運算雲端 (Amazon EC2) 執行個體，可能的狀態值為：

- 主動監控 — Amazon Inspector 會持續監控和掃描執行個體。
- EC2 執行個體已停止 — Amazon Inspector 已暫停掃描執行個體，因為執行個體處於停止狀態。任何現有發現項目都會持續存在，直到執行個體終止 如果執行個體重新啟動，Amazon Inspector 會自動繼續掃描執行個體。
- 內部錯誤 — 當 Amazon Inspector 嘗試掃描執行個體時，就會發生內部錯誤。Amazon Inspector 將自動解決錯誤並儘快恢復掃描。
- 沒有庫存 — Amazon Inspector 找不到要掃描執行個體的軟體應用程式庫存。執行個體的 Amazon Inspector 關聯可能已被刪除，或者它們可能無法執行。

  若要修正此問題，請使用 AWS Systems Manager 來確保`InspectorInventoryCollection-do-not-delete`關聯存在且關聯狀態成功。此外，請使用 AWS Systems Manager 叢集管理員來驗證執行個體的軟體應用程式清查。
- 擱置停用 — Amazon Inspector 已停止掃描執行個體。執行個體正在停用，待完成清理工作。
- 擱置初始掃描 — Amazon Inspector 已將執行個體排入佇列以進行初始掃描。
- 資源終止 — 執行個體已終止。Amazon Inspector 目前正在清理執行個體的現有發現項目和涵蓋範圍資料。
- 過時的庫存 — Amazon Inspector 無法收集在過去 7 天內為執行個體擷取的更新軟體應用程式庫存。

  若要修復此問題，請使用確 AWS Systems Manager 保所需的 Amazon Inspector 關聯存在且正在執行該執行個體。此外，請使用 AWS Systems Manager 叢集管理員來驗證執行個體的軟體應用程式清查。
- 非受管 EC2 執行個體 — Amazon Inspector 不會監控或掃描執行個體。執行個體不受管理 AWS Systems Manager。

  若要修正此問題，您可以使用 AWS Systems Manager 自動化AWSSupport-TroubleshootManagedInstance runbook提供的。設定 AWS Systems Manager 為管理執行個體後，Amazon Inspector 將自動開始持續監控和掃描執行個體。
- 不支援的作業系統 — Amazon Inspector 不會監控或掃描執行個體。執行個體使用 Amazon Inspector 不支援的作業系統或架構。如需 Amazon Inspector 支援的作業系統清單，請參閱支援 Amazon EC2 掃描的作業系統。
- 主動監控並發生部分錯誤 — 此狀態表示 EC2 掃描處於活動狀態，但存在與相關的錯誤Amazon Inspector 深度檢查 Amazon EC2 Linux 實例。可能出現的深度檢查錯誤為：

- 超過深度檢查套件收集限制 — 執行個體已超過 Amazon Inspector 深度檢查的 5000 個套件限制。若要繼續對此執行個體進行深度檢查，您可以嘗試調整與帳戶相關聯的自訂路徑。
- 超過深度檢查每日 ssm 庫存限制 — SSM 代理程式無法將庫存傳送至 Amazon Inspector，因為這個執行個體已達到每日每個執行個體收集的庫存資料的 SSM 配額。如需詳細資訊，請參閱 Amazon EC2 Systems Manager 端點和配額。
- 超過深度檢驗收集時間限制 — Amazon Inspector 無法擷取包裹庫存，因為包裹收集時間超過 15 分鐘的最大門檻。
- 深度檢查沒有庫存 — Amazon Inspector SSM 外掛程式尚未能收集此執行個體的套件庫存。這通常是待處理掃描的結果，但是，如果此狀態在 6 小時後仍然存在，請使用 Amazon EC2 Systems Manager 器確保所需的 Amazon Inspector 關聯存在並且正在執行該執行個體。

如需設定 EC2 執行個體掃描設定的詳細資訊，請參閱掃描 Amazon EC2 實例。

評估 Amazon ECR 儲存庫的涵蓋範圍

儲存庫索引標籤會顯示您 AWS 環境中的 Amazon ECR 儲存庫。這些清單會在下列索引標籤上組織成群組：

- 全部 — 顯示您環境中的所有儲存庫。狀態欄會指出存放庫目前的掃描狀態。
- 已啟動 — 顯示 Amazon Inspector 設定為在您的環境中監控和掃描的所有儲存庫。狀態欄會指出存放庫目前的掃描狀態。
- 未啟動 — 顯示 Amazon Inspector 未在您的環境中監控和掃描的所有儲存庫。「原因」欄會指出 Amazon Inspector 未監控和掃描儲存庫的原因。

在每個索引標籤上，[帳戶] 欄會指 AWS 帳戶 定擁有儲存庫的。

若要檢閱有關儲存區域的其他詳細資訊，請選擇儲存庫的名稱。然後，Amazon Inspector 會在儲存庫中顯示容器映像清單，以及每個映像的詳細資料。詳細資料包括影像標籤、影像摘要和掃描狀態。它們還包括關鍵發現項目統計資料，例如影像的嚴重發現項目數目。若要向下展開並檢閱尋找統計資料的支援資料，請選擇影像的影像標記。

掃描 Amazon ECR 儲存庫的狀態值

對於 Amazon Elastic Container Registry (Amazon ECR) 存儲庫，可能的狀態值為：

- 已啟動 (連續) — 對於儲存庫，Amazon Inspector 會持續監控此儲存庫中的影像。儲存庫的增強掃描設定已設定為連續掃描。Amazon Inspector 會在推送新映像時進行掃描，並在發佈與該映像相關的

新 CVE 時重新掃描影像。在您設定的 ECR 掃描持續時間內，Amazon Inspector 將繼續監控此儲存庫中的映像。

- 啟動 (推送時) — 推送新映像時，Amazon Inspector 會自動掃描儲存庫中的個別容器映像。已針對儲存庫啟動增強型掃描，並設定為推送時掃描。
- 拒絕存取 — Amazon Inspector 不允許存取儲存庫或儲存庫中的任何容器映像。

  若要修復此問題，請確保儲存庫的 AWS Identity and Access Management (IAM) 政策允許 Amazon Inspector 存取儲存庫。
- 停用 (手動) — Amazon Inspector 不會監控或掃描儲存庫中的任何容器映像。存放庫的 Amazon ECR 掃描設定設定為基本的手動掃描。

  若要開始使用 Amazon Inspector 掃描儲存庫中的影像，請將存放庫的掃描設定變更為增強型掃描，然後選擇要連續掃描影像，還是僅在推送新映像時掃描影像。
- 啟動 (推送時) — 推送新映像時，Amazon Inspector 會自動掃描儲存庫中的個別容器映像。儲存庫的增強型掃描設定已設定為推送時掃描。
- 內部錯誤 — 當 Amazon Inspector 嘗試掃描存放庫時，就會發生內部錯誤。Amazon Inspector 將自動解決錯誤並儘快恢復掃描。

如需設定儲存庫掃描設定的詳細資訊掃描 Amazon ECR 容器映像。

評估 Amazon ECR 容器映像的覆蓋範圍

[映像] 索引標籤會顯示您 AWS 環境中的 Amazon ECR 容器映像。這些清單會在下列索引標籤上組織成群組：

- 全部 — 顯示環境中的所有容器映像。狀態欄指示影像目前的掃描狀態。
- 掃描 — 顯示 Amazon Inspector 設定為在您的環境中監控和掃描的所有容器映像。狀態欄指示影像目前的掃描狀態。
- 未掃描 — 顯示 Amazon Inspector 未在您的環境中監控和掃描的所有容器映像。「原因」欄會指出 Amazon Inspector 未監控和掃描影像的原因。

  由於以下任何原因，容器映像檔可能會出現在 [未啟動] 索引標籤上。映像檔可能會儲存在未啟動 Amazon Inspector 掃描的儲存庫中，或者 Amazon ECR 篩選規則會阻止掃描該儲存庫。或者，在您針對 ECR 重新掃描持續時間設定的天數內，映像尚未推送或提取。如需詳細資訊，請參閱 設定 ECR 重新掃描持續時間。

在每個索引標籤上，「存放庫名稱」欄會指定儲存容器映像檔的存放庫名稱。「帳戶」欄指定擁 AWS 帳戶 有存放庫的。上次掃描的欄會顯示 Amazon Inspector 上次檢查該資源是否存在弱點的時間。這可能包括檢查是否有尋找中繼資料的更新、資源的應用程式詳細目錄有更新，或是針對新 CVE 進行重新掃描時進行檢查。如需詳細資訊，請參閱 Amazon ECR 掃描的掃描行為。

若要檢閱容器映像檔的其他詳細資訊，請選擇 ECR 容器映像資料欄中的連結。然後，Amazon Inspector 會顯示有關影像的詳細資料以及影像的目前發現項目。若要檢閱發現項目的詳細資訊，請選擇「標題」欄中的連結。如需這些詳細資訊，請參閱Amazon Inspector 找到細節。

掃描 Amazon ECR 容器映像的狀態值

對於 Amazon 彈性容器登錄容器映像，可能的狀態值為：

- 主動監控 (連續) — 每當發佈新的相關 CVE 時，Amazon Inspector 會持續監控影像和新掃描，並在其上執行影像和新掃描。每當推送或拉出影像時，Amazon ECR 重新掃描影像的持續時間都會重新整理。已針對儲存影像的存放庫啟用增強型掃描，並將存放庫的增強掃描設定設定設定為連續掃描。
- 啟動 (推送時) — Amazon Inspector 會在每次推送新影像時自動掃描影像。針對儲存影像的存放庫啟動增強型掃描，並將存放庫的增強掃描設定設定設定設定為推送時掃描。
- 內部錯誤 — 當 Amazon Inspector 嘗試掃描容器映像時，就會發生內部錯誤。Amazon Inspector 將自動解決錯誤並儘快恢復掃描。
- 擱置初始掃描 — Amazon Inspector 已將映像排入佇列以進行初始掃描。
- 掃描資格已過期 (連續) — Amazon Inspector 暫停掃描影像。在您為儲存庫中的影像自動重新掃描指定的持續時間內，影像尚未更新。您可以推或拉影像以繼續掃描。
- 掃描資格已過期 (推送時) — Amazon Inspector 暫停掃描影像。在您為儲存庫中的影像自動重新掃描指定的持續時間內，影像尚未更新。您可以推送影像以繼續掃描。
- 掃描頻率手冊 (手動) — Amazon Inspector 器不掃描 Amazon ECR 容器映像。儲存映像的儲存庫的 Amazon ECR 掃描設定設定為基本的手動掃描。若要開始使用 Amazon Inspector 自動掃描影像，請將儲存庫設定變更為增強型掃描，然後選擇要連續掃描影像，還是僅在推送新映像時掃描影像。
- 不支援的作業系統 — Amazon Inspector 不監控或掃描影像。此映像檔是以 Amazon Inspector 不支援的作業系統為基礎，或是使用 Amazon Inspector 不支援的媒體類型。

  如需 Amazon Inspector 支援的作業系統清單，請參閱支援 Amazon ECR 掃描的作業系統。如需 Amazon Inspector 支援的媒體類型清單，請參閱支援的媒體類型。

如需有關設定儲存庫和映像的掃描設定的詳細資訊，請參閱掃描 Amazon ECR 容器映像。

評估 AWS Lambda 功能的涵蓋範圍

Lambda 索引標籤會顯示 AWS 環境中的 Lambda 函數。此頁面的兩個表格，一個顯示 Lambda 標準掃描的函數涵蓋範圍詳細資料，另一個用於 Lambda 程式碼掃描 您可以根據下列標籤來分組函數：

- 全部 — 顯示環境中的所有 Lambda 函數。狀態欄會指出 Lambda 函數目前的掃描狀態。
- 掃描 — 顯示 Amazon Inspector 設定為掃描的 Lambda 函數。狀態欄會指出每個 Lambda 函數的目前掃描狀態。
- 不掃描 — 顯示 Amazon Inspector 未配置為掃描的 Lambda 函數。「原因」欄會指出 Amazon Inspector 未監控和掃描功能的原因。

  Lambda 函數可能會出現在非掃描索引標籤上的原因有幾個。Lambda 函數可能屬於尚未新增至 Amazon Inspector 的帳戶，或篩選規則會阻止掃描此函數。如需詳細資訊，請參閱 掃描 AWS Lambda 功能。

在每個索引標籤上，[函數名稱] 資料行會指定 Lambda 函數的名稱。[帳戶] 資料行指 AWS 帳戶 定擁有函數的。運行時指定函數的運行時。狀態欄會指出每個 Lambda 函數的目前掃描狀態。資源標籤顯示已套用至函數的標籤。上次掃描的欄會顯示 Amazon Inspector 上次檢查該資源是否存在弱點的時間。這可能包括檢查是否有尋找中繼資料的更新、資源的應用程式詳細目錄有更新，或是針對新 CVE 進行重新掃描時進行檢查。如需詳細資訊，請參閱 Lambda 函數掃描的掃描行為。

掃描 AWS Lambda 功能的狀態值

對於 Lambda 函數，可能的狀態值為：

- 主動監控 — Amazon Inspector 持續監控和掃描 Lambda 函數。連續掃描包括將新功能推送到存放庫時對其進行初始掃描，並在更新或發布新的常見漏洞和曝光（CVE）時自動重新掃描函數。
- 依標籤排除 — Amazon Inspector 不會掃描此功能，因為該功能已從依標籤的掃描中排除。
- 掃描資格已過期 — Amazon Inspector 未監控此功能，因為該功能自上次呼叫或更新之後已經過了 90 天或更長時間。
- 內部錯誤 — 當 Amazon Inspector 嘗試掃描該功能時，發生內部錯誤。Amazon Inspector 將自動解決錯誤並儘快恢復掃描。
- 擱置初始掃描 — Amazon Inspector 已將函數排入佇列以進行初始掃描。
- 不支援 — Lambda 函數具有不支援的執行階段。

使用 Organizations 織管理 Amazon Inspector 中的多個帳戶

您可以使用 Amazon Inspector 來管理透過 Organ AWS izations 關聯的多個帳戶。若要管理多個 Amazon Inspector 帳戶，組 Organizations 管理帳戶會將組織內的帳戶指定為 Amazon Inspector 的委派管理員帳戶。委派的管理員會管理組織的 Amazon Inspector，並獲得特殊權限，以代表您的組織執行任務。這些工作包括啟動或停用成員帳戶的掃描、檢視整個組織的彙總尋找資料，以及建立和管理隱藏規則。

> **Note**
>
> 若要以程式設計方式為多個帳戶啟用多個帳戶的 Amazon Inspector AWS 區域，您可以使用 Amazon Inspector 開發的殼層指令碼。有關使用此腳本的更多信息，請參見檢查器 2-enablement-with-cli 在網站上 GitHub 。

主題

了解管理員和 Amazon Inspector 中的成員帳戶之間的關係

當您在多帳戶環境中使用 Amazon Inspector 時，Amazon Inspector 委派的管理員帳戶可以存取特定中繼資料。此中繼資料包括 Amazon EC2 和 Amazon ECR 組態資料，以及會員帳戶的安全性尋找結果。管理員帳戶也可以建立套用至成員帳戶的尋找抑制規則。如需詳細資訊，請參閱 使用抑制規則抑制 Amazon Inspector 發現。

委派管理員動作

一般而言，委派的系統管理員將設定套用至其帳戶時，這些設定會套用至組織中的所有其他帳戶。委派的管理員也可以檢視和擷取其自己帳戶和任何關聯成員的資訊。Amazon Inspector 委派的管理員帳戶可以執行下列動作：

- 檢視和管理相關帳戶的 Amazon Inspector 狀態，包括啟用和停用 Amazon Inspector。
- 啟用或停用組織中所有成員帳戶的掃描類型。
- 檢視整個組織的彙總搜尋結果資料，並尋找組織內所有成員帳戶的詳細資訊。
- 建立及管理適用於組織中所有帳號之發現項目的抑制規則。

- 為組織的所有成員啟用 Amazon ECR 增強型掃描。
- 檢視整個組織的資源涵蓋範圍。
- 定義自動重新掃描組織中所有成員帳戶的 ECR 容器映像的持續時間。委派管理員的掃描持續時間設定會覆寫成員帳戶先前設定的任何設定。組織中的所有帳戶共用委派管理員的 Amazon ECR 自動重新掃描持續時間。您無法為個別帳戶設定不同的重新掃描持續時間。
- 為 Amazon EC2 的 Amazon Inspector 深度檢查指定五個自訂路徑，這些路徑將用於組織中的所有帳戶。這是委派管理員可為其個別帳戶設定的五個自訂路徑之外的補充。如需有關設定深度檢查自訂路徑的更多資訊，請參閱Amazon Inspector 深度檢查的自訂路徑。
- 激活和停用 Amazon Inspector 查器會員帳戶的深度檢查。
- 匯出組織中任何成員帳戶的 sBOM。
- 為組織中的所有成員帳戶設定 Amazon EC2 掃描模式。如需詳細資訊，請參閱 管理掃描模式。
- 為組織中的所有帳戶建立和管理 CIS 掃描組態，但會員帳戶建立的任何掃描組態除外。

> **Note**
>
> 如果成員帳戶離開組織，委派的系統管理員將無法再看到該帳戶排程的掃描組態。

- 檢視組織中所有帳戶的 CIS 掃描結果。

會員帳號動作

成員帳戶可以在 Amazon Inspector 中檢視和擷取其帳戶的相關資訊，而其帳戶的設定則由委派的管理員管理。組織內的成員帳戶可以在 Amazon Inspector 中執行下列動作：

- 為自己的帳戶激活 Amazon Inspector。
- 檢視自己帳號的資源涵蓋範圍。
- 檢視其帳戶的發現項目詳細資料。
- 檢視自己帳戶的 ECR 容器映像自動重新掃描持續時間設定。
- 為 EC2 的 Amazon Inspector 深度檢查指定五個自訂路徑，這些路徑將用於其個別帳戶。除了委派管理員為組織指定的任何自訂路徑外，還會掃描這些路徑。如需設定深度檢驗路徑的詳細資訊，請參閱〈〉Amazon Inspector 深度檢查的自訂路徑。
- 檢視委派管理員為 Amazon Inspector 深度檢查設定的自訂路徑。
- 匯出與其帳戶相關聯之任何資源的 sBOM。
- 檢視其帳戶的掃描模式。

- 為其帳戶建立和管理 CIS 掃描組態。
- 檢視其帳戶中資源的任何 CIS 掃描結果，包括委派系統管理員排定的資源。

> **Note**
>
> 啟用後，只有委派的管理員帳戶才能停用 Amazon Inspector。

指定 Amazon Inspector 的委派管理員

委派管理員的重要考量

請注意下列定義委派管理員在 Amazon Inspector 中操作方式的因素：

委派的系統管理員最多可管理 5,000 名成員。

每個 Amazon Inspector 委派的管理員都有 5,000 個成員帳戶的配額。但是，您的組織可能包含 5,000 多個帳戶。如果您超過 5,000 個會員帳戶，您將透過 Amazon Pers CloudWatch onal Health Dashboard 收到通知，並傳送給委派管理員帳戶的電子郵件。

委派管理員為區域性。

不同的是 AWS Organizations，Amazon Inspector 是一個區域服務。這表示您必須指定委派的管理員、新增成員帳戶，以及啟用每個想 AWS 區域 要使用 Amazon Inspector 的掃描類型。

一個組織只能有一個委派管理員。

對於一個組織，您只能有一個委派給 Amazon Inspector 的管理員。如果您已將帳戶指定為某個區域中的委派管理員，則該帳戶必須是您在所有其他區域中的委派管理員。

變更委派的管理員不會停用會員帳戶的 Amazon Inspector。

如果您移除委派的管理員，則不會停用這些帳戶中的 Amazon Inspector，而且掃描設定也不會受到影響。

您的 AWS 組織必須啟用所有功能。

這是的預設設定 AWS Organizations。如果尚未啟用，請參閱啟用組織中的所有功能。

指定委派管理員所需的許可

您必須有權限才能啟用 Amazon Inspector，並指定 Amazon Inspector 員委派的管理員。

在 IAM 政策的末尾新增以下陳述式，以授予這些許可。

```
{
    "Sid": "PermissionsForInspectorAdmin",
    "Effect": "Allow",
    "Action": [
        "inspector2:EnableDelegatedAdminAccount",
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization"
    ],
    "Resource": "*"
}
```

為您的組織指定委派的 AWS 管理員

下列程序說明如何為 AWS 組織指定委派管理員。完成此指定後，Organizations 管理帳戶和選擇的委派管理員帳戶都會啟用 Amazon Inspector。

> **Note**
>
> 只有「Organizations」管理帳戶可以指定委派的管理員。

第一次啟用 Amazon Inspector 會建立帳戶的服務連結角色 (SLR) `AWSServiceRoleForAmazonInspector`。如需 Amazon Inspector 如何使用服務連結角色的詳細資訊，請參閱使用 Amazon Inspector 的服務連結角色。如需有關服務連結角色的一般資訊，請參閱 IAM 使用者指南中的使用服務連結角色。

若要指定 Amazon Inspector 員的委派管理員

Console

在主控台中指定委派的管理員

1. AWS Management Console 使用 AWS Organizations 管理帳戶登入。

2. 在 https://console.aws.amazon.com/inspector/v2/home 開啟 Amazon Inspector 主控台，然後使用右上角的 AWS 區域 選取器來指定您要在其中指定管理員的區域。
3. 在「委派管理員」窗格中，輸入您要指定為組織 AWS 帳戶 之 Amazon Inspector 委派管理員的十二位數帳戶 ID。然後選擇 [委派管理]。
4. (建議) 針對每個步驟重複上述步驟 AWS 區域。

API

使用 API 指定委派的管理員

- 使用 Organizations 管理帳戶 AWS 帳戶 的認證來執行 EnableDelegatedAdminAccountAPI 作業。您也可以使用執 AWS Command Line Interface 行下列 CLI 命令來執行此操作：`aws inspector2 enable-delegated-admin-account --delegated-admin-account-id 11111111111`。

> **Note**
>
> 請務必指定您要設為 Amazon Inspector 委派管理員之帳戶的帳戶 ID。

指定委派管理員之後，您只能使用 AWS Organizations 管理帳戶來變更或移除委派的管理員帳戶。

激活 Amazon Inspector 掃描成員帳戶

身為組織的委派管理員，您可以針對與 AWS Organizations 管理帳戶關聯的任何成員啟用 Amazon EC2 掃描、Amazon ECR 掃描或兩者。當您啟用成員帳戶的掃描時，該帳戶會與委派的管理員建立關聯，Amazon Inspector 會自動啟用，並立即開始所選類型的掃描。如需有關可掃描哪些資源以及如何設定掃描的資訊，請參閱使用 Amazon Inspector 自動化資源。

Amazon Inspector 提供多個選項，可用來管理和啟用成員帳戶的掃描，包括允許成員帳戶啟用 Amazon Inspector。使用下列其中一個選項開始掃描您的會員帳戶。

自動啟動掃描所有會員帳戶

1. 登入委派的系統管理員帳戶。
2. 在 https://console.aws.amazon.com/inspector/v2/home 打開 Amazon Inspector 控制台。然後使用右上角的 AWS 區域 選擇器來指定您要啟動掃描所有成員帳戶的區域。

3. 在功能窗格的 [設定] 底下，選擇 [帳戶管理]。帳戶表格會顯示與 AWS Organizations 管理帳戶相關聯的所有成員帳戶。
4. 選取表格頂端的核取方塊，以選取此頁面上的所有帳戶。然後選擇激活並從菜單中選擇您首選的掃描類型選項。

> **Note**
>
> 只會選取頁面上目前可見的帳號。如果您有多個頁面的帳戶，則必須在每個頁面上重複此過程。若要變更頁面上顯示的帳號數目，請選取齒輪圖示。

5. 開啟 [為新成員帳戶自動啟用 Inspector] 設定，然後選取掃描類型以啟動新增至組織的任何新成員。
6. （建議）在您要掃描成員帳戶的每個區域中重複這些步驟。

[自動啟用新成員帳戶的檢查器] 設定會為組織的所有 future 成員啟用 Amazon Inspector。這可讓 Amazon Inspector 委派的管理員管理員管理新增至組織的任何新成員。當成員帳戶數量達到 5,000 個配額時，此設定會自動關閉。如果移除帳戶且成員總數減少至少於 5,000，則會自動重新啟用該設定。

選擇性地啟動會員帳戶

1. 登入委派的系統管理員帳戶。
2. 在 https://console.aws.amazon.com/inspector/v2/home 開啟 Amazon Inspector 主控台，然後使用右上角的 AWS 區域 選擇器來指定您要啟用掃描特定成員帳戶的區域。
3. 在功能窗格的 [設定] 底下，選擇 [帳戶管理]。帳戶表格會顯示與 AWS Organizations 管理帳戶相關聯的所有成員帳戶。
4. 在 [帳戶管理] 頁面上，選取您要啟動掃描的每個成員帳戶的核取方塊。
5. 選取 [啟用]。
6. 從「啟動」功能表中，選擇要為所選帳戶啟動的掃描類型。您可以從下列掃描選項中選擇：
   - 所有掃描 — 啟動所有掃描類型。
   - EC2 掃描 — 啟動 Amazon EC2 執行個體的掃描。
   - ECR 容器掃描 — 啟動 ECR 容器映像的掃描。
   - AWS Lambda 標準掃描 — 啟動 Lambda 函數的掃描。
7. (建議使用) 在每個您要啟動掃描的區域中，重複這些步驟。

如果您的 AWS Organizations 管理帳戶已委派 Amazon Inspector 的管理員，您可以將自己的帳戶啟用為成員，並檢視自己帳戶的掃描詳細資料。

啟動掃描成為會員帳號

1. 登錄到您的帳戶。
2. 在 https://console.aws.amazon.com/inspector/v2/home 開啟 Amazon Inspector 主控台，然後使用右上角的 AWS 區域 選擇器指定要在其中啟用掃描的區域。
3. 在功能窗格的 [設定] 底下，選擇 [帳戶管理]。
4. 在 [帳戶管理] 頁面上，選取您帳戶的核取方塊。
5. 從「啟動」功能表中，選擇要啟動的掃描類型。您可以從下列掃描選項中選擇：
   - 所有掃描 — 啟動所有掃描類型。
   - EC2 掃描 — 啟動 Amazon EC2 執行個體的掃描。
   - ECR 容器掃描 — 啟動 ECR 容器映像的掃描。
   - AWS Lambda 標準掃描 — 啟動 Lambda 函數的掃描。
6. （建議）在您要啟動掃描的每個區域中重複這些步驟。

在 Amazon Inspector 中取消關聯會員帳戶

下列程序說明如何取消成員帳戶的關聯。取消關聯的成員帳戶會以獨立的 Amazon Inspector 帳戶形式保留在 AWS Organizations 組織中。Amazon Inspector 委派的管理員不再具有啟動和管理這些帳戶的 Amazon Inspector 的權限。您可以稍後再次將取消關聯的帳戶新增為成員。

> **Note**
> 取消關聯帳戶並不會停用該帳戶的 Amazon Inspector 掃描。

Console

使用主控台取消成員帳戶的關聯

1. 登入委派的系統管理員帳戶。
2. 在 https://console.aws.amazon.com/inspector/v2/home 開啟 Amazon Inspector 主控台，然後使用右上角的 AWS 區域 選擇器來指定要取消關聯一或多個成員帳戶的區域。

3. 在功能窗格的 [設定] 底下，選擇 [帳戶管理]。
4. 在 [帳戶管理] 頁面上，選取要取消關聯之每個帳戶的核取方塊。
5. 從 [動作] 功能表中，選擇 [取消帳號關聯]。
6. (建議) 在您要取消帳戶關聯的每個區域中重複這些步驟。

API

使用 API 取消成員帳戶的關聯

執行 DisassociateMember API 作業。在要求中，提供您要取消關聯的帳戶 ID。

移除 Amazon Inspector 委派的管理員

如果您必須指派新的 Amazon Inspector 委派管理員，您可以移除現有的委派管理員做為 AWS Organizations 管理帳戶。

移除委派的管理員時，不會停用該帳戶或任何組織成員帳戶中的 Amazon Inspector。組織內的帳戶會轉換為獨立帳戶，並保留其在由委派系統管理員管理之前所擁有的掃描設定。

若要移除委派的管理員

1. AWS Management Console 使用 AWS Organizations 管理帳戶登入。
2. 在 https://console.aws.amazon.com/inspector/v2/home 開啟 Amazon Inspector 主控台，然後使用右上角的 AWS 區域 選取器來指定您要移除委派管理員的區域。
3. 在功能窗格的 [設定] 底下，選擇 [帳戶管理]。
4. 在「委派管理員」區段中，選擇「移除」，然後確認您的動作。
5. 在您註冊此委派管理員的每個區域中重複這些步驟。

新增 Amazon Inspector 委派的管理員時，必須手動將組織成員與新的管理員帳戶建立關聯。請遵循下列步驟，將組織成員與新的管理員帳戶建立關聯。

建立成員與新委派管理員的關聯

1. AWS Management Console 使用委派的系統管理員帳戶登入。
2. 在 https://console.aws.amazon.com/inspector/v2/home 開啟 Amazon Inspector 主控台，然後使用右上角的 AWS 區域 選取器來指定您要在其中將成員與新委派管理員建立關聯的區域。

3. 在功能窗格的 [設定] 底下，選擇 [帳戶管理]。
4. 使用頂端的核取方塊，選取組織中列出的所有帳戶。
5. 從「動作」功能表中選擇「新增成員」。
6. 在您要將成員與中的新委派管理員建立關聯的每個區域中重複這些步驟。

在 Amazon Inspector 中監控用量和成本

您可以使用 Amazon Inspector 主控台和 API 操作來預測在您的環境中使用 Amazon Inspector 的每月成本。如果您是多帳戶環境的 Amazon Inspector 管理員，則可以檢視整個環境的總成本和每個成員帳戶的成本指標。

使用使用主控台

您可以從主控台評估 Amazon Inspector 的用量和預估成本。

存取使用統計資料

1. 在 https://console.aws.amazon.com/inspector/v2/home 打開 Amazon Inspector 控制台。
2. 使用頁面右上角的選取 AWS 區域 器，選取您要監控成本的區域。
3. 在導覽窗格中，選擇用量。

在「按帳戶」選項卡中，您將看到根據帳戶使用情況下列出的 30 天期限的預計總成本。在「預計成本」欄下的表格中，選取一個值，以查看該帳戶的掃描類型的使用情況明細。在此詳細資料窗格中，您還可以查看哪些掃描類型對該帳戶有效的免費試用版。

如果您是組織的委派管理員，您會在表格中看到組織內每個帳戶的一列。如果您組織中的帳戶取消關聯，主控台會將其預估成本顯示為 -。

在 [依掃描類型] 索引標籤中，您可以查看目前 30 天期間目前為止的實際使用量細分 (依掃描類型)。這是用來計算「依帳戶」頁標中預估成本的資訊。

如果您是組織的委派管理員，則可以查看組織中每個帳戶的使用情況。

在此索引標籤中，您可以展開下列任何使用狀況統計資料窗格：

Amazon EC2 掃描

Amazon Inspector 使用主控台會針對以代理程式為基礎的掃描和無代理程式掃描追蹤下列指標：

- 執行個體 (平均) — Amazon Inspector 會使用涵蓋時數來計算 EC2 執行個體掃描的平均資源數。平均值是總保險時數除以 720 小時（即 30 天內的小時數）。
- 涵蓋時數 — 對於 Amazon EC2 掃描，這是 Amazon Amazon Inspector 為帳戶中每個 EC2 執行個體提供有效涵蓋範圍的最近 30 天內總小時數總和。對於 EC2 執行個體，涵蓋範圍小時是指從

Amazon Inspector 探索執行個體到終止或停止執行個體，或從標籤掃描中排除為止的小時數。(當您重新啟動已停止的執行個體或移除排除標記時，Amazon Inspector 會恢復該執行個體的涵蓋範圍，並繼續累積涵蓋時數)。

CIS 執行個體掃描 — 針對帳戶中執行個體執行的 CIS 掃描總數。

Amazon ECR 掃描

初始掃描 — 過去 30 天內首次掃描帳戶中影像的總和。

重新掃描 — 過去 30 天內帳戶中重新掃描影像的總和。重新掃描是在 Amazon Inspector 先前掃描過的 ECR 影像上完成的任何掃描。如果您已將 ECR 儲存庫設定為持續掃描，則當 Amazon Inspector 將新的常見弱點和入侵程式 (CVE) 新增至其資料庫時，會自動進行重新掃描。

Lambda 掃描

Amazon Inspector 使用主控台會追蹤 Lambda 標準掃描和 Lambda 程式碼掃描的下列指標：

- Lambda 函數的數量 (平均值) — Amazon Inspector 會使用涵蓋時數來計算 Lambda 函數掃描的平均函數數目。「平均」是指總保險時數除以 720 小時 (即 30 天內的小時數) 。
- 涵蓋時數 — 對於 Lambda 函數掃描，這是 Amazon Amazon Inspector 為帳戶中每個 Lambda 函數提供有效涵蓋範圍的最近 30 天內總小時數總和。對於 AWS Lambda 功能，涵蓋時數是從 Amazon Inspector 發現函數的時間開始計算，直到將其刪除或從掃描中排除為止。如果再次包含排除的功能，則該功能的承保時數將繼續累積。

了解 Amazon Inspector 如何計算用量成本

Amazon Inspector 提供的成本是預估成本，而非實際成本，因此可能與 AWS Billing 主控台中的成本不同。

請注意下列有關 Amazon Inspector 如何在「用量」頁面計算成本的相關事項

- 使用成本僅反映目前區域。每種掃描類型的價格因 AWS 區域而異，要查看每個區域的確切價格，請參閱 Amazon Inspector 的定價
- 所有使用預測都會四捨五入至最接近的美元。
- 折扣不包含在預計成本中。
- 預估成本代表每種掃描類型 30 天使用期間的總成本。如果帳戶的使用時間少於 30 天，Amazon Inspector 會在 30 天後預測成本，就好像任何目前涵蓋的資源在 30 天的剩餘時間內仍會保持涵蓋範圍一樣。
- 每種掃描類型的成本是根據下列項目計算：

- EC2 掃描：成本反映過去 30 天內 Amazon Inspector 涵蓋的 EC2 執行個體平均數量。
- ECR 容器掃描：成本反映過去 30 天內初始影像掃描 + 影像重新掃描次數的總和。
- Lambda 標準掃描：成本反映過去 30 天 Amazon Inspector 涵蓋的 Lambda 函數平均數量。
- Lambda 程式碼掃描：成本反映過去 30 天 Amazon Inspector 涵蓋的 Lambda 函數平均數目。

關於 Amazon Inspector 免費試用

當您啟用 Amazon Inspector 掃描類型時，系統會自動為您註冊該掃描類型的 15 天免費試用期。每種掃描類型都有獨立的免費追蹤，包括：EC2 掃描、ECR 掃描、Lambda 標準掃描和 Lambda 程式碼掃描。

> **Note**
>
> 免費試用版不適用於 CIS 掃描。

如果您在免費試用期間停用某種掃描類型，則該掃描類型的免費試用將暫停。如果您重新激活該服務，免費試用將恢復，您將獲得該免費試用的剩餘天數。

Amazon Inspector 中的安全

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，這些架構是為了滿足對安全性最敏感的組織的需求而建置的。

安全是 AWS 與您之間共同承擔的責任。共同責任模型將其描述為雲端的安全性和雲端中的安全性：

- 雲端安全性 — AWS 負責保護中執行 AWS 服務的基礎架構 AWS 雲端。 AWS 還為您提供可以安全使用的服務。若要了解適用於 Amazon Inspector 的合規計劃，請參閱合規計劃AWS 服務範圍內的合規計劃AWS的服務。
- 雲端中的安全性 — 您的責任取決於您使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件可協助您了解如何在使用 Amazon Inspector 時套用共同的責任模型。下列主題說明如何設定 Amazon Inspector 以符合安全性和合規目標。您也會學到如何使用其他可 AWS 協助您監控和保護 Amazon Inspector 資源的服務。

主題

Amazon Inspector 中的數據保護

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

基於資料保護目的，我們建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 登入資料並設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源進行通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用設定 API 和使用者活動記錄 AWS CloudTrail。
- 使用 AWS 加密解決方案以及其中的所有默認安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在透過命令列介面或 API 存取時需要經 AWS 過 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-2 概觀。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用主控台、API 或 AWS 開發套件 AWS 服務 使用 Amazon Inspector 或其他工作時。 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。

主題

靜態加密

Amazon Inspector 預設會使用 AWS 加密解決方案安全地存放您的靜態資料。Amazon Inspector 會加密資料，例如使用 AWS Systems Manager 收集的資源庫存、從 Amazon ECR 映像剖析的資源庫存，以及使用金鑰管理服務中 AWS AWS 擁有的加密金鑰產生的安全發現結果 ()。AWS KMS您無法檢視、管理或使用 AWS 擁有的金鑰，也無法稽核其使用情況。但是，您不必採取任何動作或更改任何程序來保護加密數據的密鑰。有關詳情，請參閱AWS 擁有的金鑰。

如果停用 Amazon Inspector，它會永久刪除它為您存放或維護的所有資源，例如收集的庫存和安全發現項目。

針對發現項目中的程式碼進行靜態加密

對於亞馬遜檢查器 Lambda 代碼掃描，Amazon Inspector 與 CodeGuru 合作掃描您的代碼是否存在漏洞。偵測到弱點時，會 CodeGuru 擷取包含該弱點的程式碼片段，並儲存該程式碼，直到 Amazon Inspector 請求存取為止。依預設 CodeGuru 會使用 AWS 擁有的金鑰來加密擷取的程式碼，不過，您可以設定 Amazon Inspector 使用自己的客戶受管 AWS KMS 金鑰進行加密。

下列工作流程說明 Amazon Inspector 如何使用您設定的金鑰來加密程式碼：

1. 您提供一個 AWS KMS 密鑰 Amazon Inspector 使用 Amazon Inspector UpdateEncryptionKeyAPI。
2. Amazon Inspector 轉發關於你的 AWS KMS 密鑰的信息。 CodeGuru CodeGuru 儲存資訊以供 future 使用。
3. CodeGuru 請求授予您在 Amazon Inspector 中設定的金鑰。 AWS KMS
4. CodeGuru 從您的密鑰創建一個加密的數據密 AWS KMS 鑰並將其存儲。此資料金鑰可用來加密儲存的程式碼資料 CodeGuru。
5. 每當 Amazon Inspector 從程式碼掃描請求資料時， CodeGuru 會使用授權來解密加密的資料金鑰，然後使用該金鑰解密資料以便擷取資料。

停用 Lambda 程式碼掃描時，會 CodeGuru 淘汰授權並刪除相關聯的資料金鑰。

使用客戶管理的金鑰進行程式碼加密的權限

若要使用加密，您必須擁有允許存取 AWS KMS 動作的政策，以及授予 Amazon Inspector 的陳述式，以及透過條件金鑰使用這些動作的 CodeGuru 權限。

如果您要設定、更新或重設帳戶的加密金鑰，則必須使用 Amazon Inspector 管理員政策，例如AWS 受管理的策略：AmazonInspector2FullAccess。您還需要將下列權限授與需要從發現項目或選擇用於加密之金鑰的相關資料擷取程式碼片段的唯讀使用者。

針對 KMS，原則必須允許您執行下列動作：

- `kms:CreateGrant`
- `kms:Decrypt`
- `kms:DescribeKey`
- `kms:GenerateDataKeyWithoutPlainText`
- `kms:Encrypt`
- `kms:RetireGrant`

在確認您的政策中具有正確的 AWS KMS 許可後，您必須附加允許 Amazon Inspector 的陳述式，並使 CodeGuru 用您的金鑰進行加密。附上以下政策聲明：

> **Note**
>
> 將區域取代為您已啟用 Amazon Inspector Lambda 程式碼掃描的 AWS 區域。

```
{
            "Sid": "allow CodeGuru Security to request a grant for a AWS KMS key",
          "Effect": "Allow",
          "Action": "kms:CreateGrant",
          "Resource": "*",
          "Condition": {
           "ForAllValues:StringEquals": {
            "kms:GrantOperations": [
             "GenerateDataKey",
             "GenerateDataKeyWithoutPlaintext",
             "Encrypt",
             "Decrypt",
             "RetireGrant",
             "DescribeKey"
            ]
           },
           "StringEquals": {
            "kms:ViaService": [
             "codeguru-security.Region.amazonaws.com"
            ]
           }
          }
        },
        {
         "Sid": "allow Amazon Inspector and CodeGuru Security to use your AWS KMS key",
         "Effect": "Allow",
         "Action": [
          "kms:Encrypt",
          "kms:Decrypt",
          "kms:RetireGrant",
          "kms:DescribeKey",
          "kms:GenerateDataKeyWithoutPlaintext"
         ],
```

```
        "Resource": "*",
        "Condition": {
         "StringEquals": {
          "kms:ViaService": [
           "inspector2.Region.amazonaws.com",
           "codeguru-security.Region.amazonaws.com"
          ]
         }
        }
       }
```

> **Note**
>
> 當您新增陳述式時，請確定語法有效。策略使用 JSON 格式。這表示您需要在陳述式之前或之後新增逗號，視您將陳述式新增至原則的位置而定。如果您將陳述式新增為最後一個陳述式，請在前述陳述式的右括號後加上逗號。如果您將它新增為第一個陳述式或兩個現有陳述式之間，請在陳述式的右括號後加上逗號。

使用客戶管理的金鑰設定加密

若要使用客戶受管金鑰為您的帳戶設定加密，您必須是 Amazon Inspector 管理員，並具有中所述許可使用客戶管理的金鑰進行程式碼加密的權限。此外，您需要在與發現項目相同的 AWS 區域中使用金 AWS KMS 鑰，或是多區域金鑰。您可以在帳戶中使用現有的對稱金鑰，或使用 AWS 管理主控台或 API 建立對稱的客戶管理金鑰。 AWS KMS 如需詳細資訊，請參閱 AWS KMS 使用指南中的建立對稱加密 AWS KMS 金鑰。

使用 Amazon Inspector API 設定加密

若要設定加密金鑰，請在以亞馬遜檢查器管理員身分登入時執行 Amazon Inspector API 的UpdateEncryptionKey操作。在 API 要求中，使用`kmsKeyId`欄位指定要使用之 AWS KMS 金鑰的 ARN。對於`scanType`輸入`CODE`和`resourceType`輸入`AWS_LAMBDA_FUNCTION`。

您可以使用 UpdateEncryptionKeyAPI 來檢查 Amazon Inspector 查器使用哪個 AWS KMS 金鑰進行加密。

> **Note**
>
> 如果您嘗試在尚未設定客戶管理金鑰`GetEncryptionKey`時使用，則作業會傳回`ResourceNotFoundException`錯誤訊息，表示 AWS 擁有的金鑰正在用於加密。

如果您刪除或密鑰或更改它的政策是拒絕訪問 Amazon Inspector，否則 CodeGuru 您將無法訪問代碼漏洞發現的發現，並且 Lambda 代碼掃描將失敗您的帳戶。

您可以使用 AWS 擁有的金鑰`ResetEncryptionKey`來繼續使用，加密擷取為 Amazon Inspector 發現項目的一部分所擷取的程式碼。

傳輸中加密

AWS 加密 AWS 內部系統與其他 AWS 服務之間傳輸的所有資料。

對於庫存收集，Systems Manager 會從客戶擁有的 EC2 執行個體透 AWS 過受傳輸層安全性 (TLS) 保護的通道收集遙測資料，以進行評估。請參閱 Systems Manager 中的資料保護，瞭解 SSM 如何加密傳輸中的資料。

同樣地，傳送至 Security Hub 的 Amazon ECR 和 AWS Lambda 函數掃描發現項目也會使用受 TLS 保護的通道加密。

Amazon Inspector 的 Identity and Access Management

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 (具有許可) 來使用 Amazon Inspector 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
- 亞馬遜檢查器如何使用 IAM
- Amazon Inspector 基於身份的政策示例

- AWS Amazon Inspector 的受管政策
- 使用 Amazon Inspector 的服務連結角色
- Amazon Inspector 身分和存取疑難

物件

您的使用方式 AWS Identity and Access Management (IAM) 會有所不同，這取決於您在 Amazon Inspector 中所做的工作。

服務使用者 — 如果您使用 Amazon Inspector 服務執行工作，則管理員會為您提供所需的登入資料和許可。當您使用更多 Amazon Inspector 功能來完成工作時，您可能需要額外的許可。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果您無法在 Amazon Inspector 查器中訪問某個功能，請參閱Amazon Inspector 身分和存取疑難。

服務管理員 — 如果您負責公司的 Amazon Inspector 資源，您可能擁有完整的 Amazon Inspector 存取權。您的任務是決定服務使用者應存取哪些 Amazon Inspector 功能和資源。接著，您必須將請求提交給您的 IAM 管理員，來變更您服務使用者的許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。若要進一步了解貴公司如何將 IAM 與 Amazon Inspector 搭配使用，請參閱亞馬遜檢查器如何使用 IAM。

IAM 管理員 — 如果您是 IAM 管理員，您可能想要了解如何撰寫政策以管理 Amazon Inspector 存取權的詳細資訊。若要檢視您可以在 IAM 中使用的 Amazon Inspector 身分型政策範例，請參閱。Amazon Inspector 基於身份的政策示例

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。

亞馬遜檢查器如何使用 IAM

在您使用 IAM 管理 Amazon 檢查器的存取權限之前，請先了解哪些 IAM 功能可與 Amazon Inspector 搭配使用。

您可以搭配 Amazon Inspector 使用的 IAM 功能

IAM 功能	Amazon Inspector 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 (服務特定)	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	否
服務連結角色	是

若要深入瞭解 Amazon Inspector 和其他人如何 AWS 服務 使用大多數 IAM 功能 AWS 服務 ，請參閱 IAM 使用者指南中的 IAM。

Amazon Inspector 基於身份的政策

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。

Amazon Inspector 基於身份的政策示例

若要檢視 Amazon Inspector 以身分識別為基礎的政策範例，請參閱。Amazon Inspector 基於身份的政策示例

Amazon Inspector 內的資源型政策

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。

Amazon Inspector 的政策行動

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，哪個主體在什麼条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 Amazon 檢查器動作清單，請參閱服務授權參考資料中由 Amazon Inspector 定義的動作。

Amazon Inspector 中的政策動作會在動作之前使用下列前置詞：

```
inspector2
```

若要在單一陳述式中指定多個動作，請用逗號分隔。

```
"Action": [
      "inspector2:action1",
      "inspector2:action2"
         ]
```

若要檢視 Amazon Inspector 以身分識別為基礎的政策範例，請參閱。Amazon Inspector 基於身份的政策示例

Amazon Inspector 的政策資源

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": "*"
```

若要查看 Amazon Inspector 資源類型及其 ARN 的清單，請參閱服務授權參考資料中由 Amazon Inspector 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 Inspector 定義的動作。

若要檢視 Amazon Inspector 以身分識別為基礎的政策範例，請參閱。Amazon Inspector 基於身份的政策示例

Amazon Inspector 的政策條件密鑰

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 Amazon 檢查器條件金鑰清單，請參閱服務授權參考資料中的 Amazon Inspector 的條件金鑰。若要了解可以使用條件金鑰的動作和資源，請參閱 Amazon Inspector 定義的動作。

若要檢視 Amazon Inspector 以身分識別為基礎的政策範例，請參閱。Amazon Inspector 基於身份的政策示例

Amazon Inspector 中的 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。

ABAC 與 Amazon Inspector

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)。

使用臨時登入資料搭配 Amazon Inspector

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。

Amazon Inspector 的跨服務主體許可

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》。

Amazon Inspector 的服務角色

支援服務角色	否

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**
>
> 變更服務角色的許可可可可可能會中斷 Amazon Inspector 的功能。只有在 Amazon Inspector 提供指導時，才能編輯服務角色。

Amazon Inspector 的服務連結角色

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。

如需建立或管理服務連結角色的詳細資訊 AWS 服務 ，請參閱使用 IAM。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 Inspector 基於身份的政策示例

依預設，使用者和角色沒有建立或修改 Amazon Inspector 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。

如需 Amazon Inspector 定義的動作和資源類型的詳細資訊，包括每個資源類型的 ARN 格式，請參閱服務授權參考中適用於 Amazon Inspector 的動作、資源和條件金鑰。

主題

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在您的帳戶中建立、存取或刪除 Amazon Inspector 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管原則並邁向最低權限權限 — 若要開始將權限授與使用者和工作負載，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們可用在您的 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 Amazon Inspector 控制台

若要存取 Amazon Inspector 主控台，您必須擁有最少一組許可。這些許可必須允許您列出 Amazon Inspector 視有關 AWS 帳戶. 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。

為了確保使用者和角色仍然可以使用 Amazon Inspector 主控台，請同時將 Amazon Inspector *ConsoleAccess* 或*ReadOnly* AWS 受管政策附加到實體。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。

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": "*"
        }
    ]
}
```

允許所有 Amazon Inspector 資源的唯讀存取

此範例顯示允許對所有 Amazon Inspector 資源進行唯讀存取的政策。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "inspector2:Describe*",
                "inspector2:Get*",
                "inspector2:BatchGet*",
                "inspector2:List*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
```

```
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization"
            ],
            "Resource": "*"
        }
    ]
}
```

允許完整存取所有 Amazon Inspector 資源

此範例顯示允許完整存取所有 Amazon Inspector 資源的政策。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "inspector2:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "inspector2.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:RegisterDelegatedAdministrator",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

AWS Amazon Inspector 的受管政策

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

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

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

如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

AWS 受管理的策略：AmazonInspector2FullAccess

您可將 `AmazonInspector2FullAccess` 政策連接到 IAM 身分。

此政策授予允許完整存取 Amazon Inspector 的管理許可。

許可詳細資訊

此政策包含以下許可。

- `inspector2`— 允許完全訪問 Amazon Inspector 功能.
- `iam`— 允許 Amazon Inspector 創建服務鏈接角色，`AmazonInspector2AgentlessServiceRole`. 這是必要的，Amazon Inspector 才能執行各種操作，例如擷取 Amazon EC2 執行個體和 Amazon ECR 儲存庫和容器映像的相關資訊、分析您的 VPC 網路，以及描述與組織相關聯的帳戶。如需詳細資訊，請參閱 使用 Amazon Inspector 的服務連結角色。

- `organizations`— 允許管理員在中為組織使用 Amazon Inspector AWS Organizations。在中啟用 Amazon Inspector 的受信任存取權之後 AWS Organizations，委派管理員帳戶的成員可以管理設定並檢視其組織中的發現項目。
- `codeguru-security`— 可讓管理員使用 Amazon Inspector 擷取資訊程式碼片段，並針對 CodeGuru 安全性存放的程式碼變更加密設定。如需詳細資訊，請參閱 針對發現項目中的程式碼進行靜態加密。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": "inspector2:*",
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": [
    "codeguru-security:BatchGetFindings",
    "codeguru-security:GetAccountConfiguration",
    "codeguru-security:UpdateAccountConfiguration"
   ],
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": "iam:CreateServiceLinkedRole",
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "iam:AWSServiceName": "inspector2.amazonaws.com"
    }
   }
  },
  {
   "Effect": "Allow",
   "Action": [
    "organizations:EnableAWSServiceAccess",
    "organizations:RegisterDelegatedAdministrator",
    "organizations:ListDelegatedAdministrators",
    "organizations:ListAWSServiceAccessForOrganization",
```

```
    "organizations:DescribeOrganizationalUnit",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization"
   ],
   "Resource": "*"
  }
 ]
}
```

AWS 受管理的策略：AmazonInspector2ReadOnlyAccess

您可將 AmazonInspector2ReadOnlyAccess 政策連接到 IAM 身分。

此政策授予允許對 Amazon Inspector 進行唯讀存取的許可。

許可詳細資訊

此政策包含以下許可。

- inspector2— 允許只讀訪問 Amazon Inspector 功能。
- organizations— 允許檢視中某個組織的 Amazon Inspector 涵蓋範圍 AWS Organizations 的詳細資訊。
- codeguru-security— 允許從 CodeGuru 安全性擷取程式碼片段。也允許檢視儲存在 [CodeGuru 安全性] 中之程式碼的加密設定。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "organizations:ListDelegatedAdministrators",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:DescribeOrganizationalUnit",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "inspector2:BatchGet*",
```

```
    "inspector2:List*",
    "inspector2:Describe*",
    "inspector2:Get*",
    "inspector2:Search*",
    "codeguru-security:BatchGetFindings",
    "codeguru-security:GetAccountConfiguration"
   ],
   "Resource": "*"
  }
 ]
}
```

AWS 受管理的策略：AmazonInspector2ManagedCisPolicy

您可將 AmazonInspector2ManagedCisPolicy 政策附加至 IAM 實體。此政策應附加至授予 Amazon EC2 執行個體許可的角色，以執行執行個體的 CIS 掃描。您可以使用 IAM 角色管理在 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。

許可詳細資訊

此政策包含以下許可。

- inspector2— 允許存取用於執行 CIS 掃描的動作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
            "inspector2:StartCisSession",
            "inspector2:StopCisSession",
            "inspector2:SendCisSessionTelemetry",
            "inspector2:SendCisSessionHealth"
            ],
            "Resource": "*",
        }
```

```
    ]
}
```

AWS 受管理的策略：AmazonInspector2ServiceRolePolicy

您無法將 `AmazonInspector2ServiceRolePolicy` 政策附加至 IAM 實體。此政策附加至服務連結角色，可讓 Amazon Inspector 代表您執行動作。如需詳細資訊，請參閱 使用 Amazon Inspector 的服務連結角色。

AWS 受管理的策略：AmazonInspector2AgentlessServiceRolePolicy

您無法將 `AmazonInspector2AgentlessServiceRolePolicy` 政策附加至 IAM 實體。此政策附加至服務連結角色，可讓 Amazon Inspector 代表您執行動作。如需詳細資訊，請參閱 使用 Amazon Inspector 的服務連結角色。

Amazon Inspector 更新受 AWS 管政策

檢視有關 Amazon Inspector AWS 受管政策更新的詳細資訊，因為此服務開始追蹤這些變更。如需有關此頁面變更的自動警示，請訂閱 Amazon Inspector 文件歷史記錄頁面上的 RSS 摘要。

變更	描述	日期
AmazonInspector2 ManagedCisPolicy — 新政策	Amazon Inspector 新增了一個新的受管政策，您可以將其用作執行個體設定檔的一部分，以允許執行個體上的 CIS 掃描。	2024 年 1 月 23 日
AmazonInspector2 ServiceRolePolicy — 現有政策的更新	Amazon Inspector 添加了新的許可，允許 Amazon Inspector 在目標實例上啟動獨聯體掃描。	2024 年 1 月 23 日
AmazonInspector2 AgentlessServiceRolePolicy — 新政策	Amazon Inspector 已新增服務連結角色政策，以允許無代理程式掃描 EC2 執行個體。	2023 年 11 月 27 日

變更	描述	日期
AmazonInspector2 ReadOnlyAccess — 現有政策的更新	Amazon Inspector 新增了新的許可，可讓唯讀使用者擷取漏洞情報詳細資訊，以便發現套件漏洞。	2023 年 9 月 22 日
AmazonInspector2 ServiceRolePolicy — 現有政策的更新	Amazon Inspector 已新增許可，讓 Amazon Inspector 掃描屬於 Elastic Load Balancing 目標群組一部分之 Amazon EC2 執行個體的網路組態。	2023 年 8 月 31 日
AmazonInspector2 ReadOnlyAccess — 現有政策的更新	Amazon Inspector 新增了新的許可，允許唯讀使用者匯出其資源的軟體材料清單 (SBOM)。	2023 年 6 月 29 日
AmazonInspector2 ReadOnlyAccess — 現有政策的更新	Amazon Inspector 新增了新的許可，可讓唯讀使用者擷取其帳戶的 Lambda 程式碼掃描發現項目的加密設定詳細資料。	2023 年 6 月 13 日
AmazonInspector2 FullAccess — 現有政策的更新	Amazon Inspector 新增了新許可，可讓使用者設定客戶受管 KMS 金鑰，以加密 Lambda 程式碼掃描發現項目中的程式碼。	2023 年 6 月 13 日
AmazonInspector2 ReadOnlyAccess — 現有政策的更新	Amazon Inspector 新增了新的許可，可讓唯讀使用者擷取其帳戶的 Lambda 程式碼掃描狀態和發現項目的詳細資訊。	2023 年 5 月 2 日

變更	描述	日期
AmazonInspector2 ServiceRolePolicy — 現有政策的更新	Amazon Inspector 已新增許可，讓 Amazon Inspector 在您啟用 Lambda 掃描時，在您的帳戶中建立 AWS CloudTrail 服務連結通道。這使 Amazon Inspector 器可以監控您帳戶中的 CloudTrail 事件。	2023年4月30日
AmazonInspector2 FullAccess — 現有政策的更新	Amazon Inspector 新增了新的許可，可讓使用者從 Lambda 程式碼掃描擷取程式碼漏洞發現的詳細資訊。	2023 年 4 月 21 日
AmazonInspector2 ServiceRolePolicy — 現有政策的更新	Amazon Inspector 已新增許可，讓 Amazon Inspector 能夠將客戶為 Amazon EC2 深度檢查所定義的自訂路徑相關資訊傳送至 Amazon EC2 系統管理員。	2023 年 4 月 17 日
AmazonInspector2 ServiceRolePolicy — 現有政策的更新	Amazon Inspector 已新增許可，讓 Amazon Inspector 在您啟用 Lambda 掃描時，在您的帳戶中建立 AWS CloudTrail 服務連結通道。這使 Amazon Inspector 器可以監控您帳戶中的 CloudTrail 事件。	2023年4月30日

變更	描述	日期
AmazonInspector2 ServiceRolePolicy — 現有政策的更新	Amazon Inspector 新增了新的許可，允許 Amazon Inspector 請求掃描 AWS Lambda 功能中的開發人員代碼，並從 Amazon CodeGuru 安全接收掃描數據。此外，Amazon Inspector 已新增審查 IAM 政策的許可。Amazon Inspector 使用此資訊掃描 Lambda 函數是否存在程式碼漏洞	2023 年 2 月 28 日
AmazonInspector2 ServiceRolePolicy — 現有政策的更新	Amazon Inspector 添加了一個新的語句，允許 Amazon Inspector 從有 CloudWatch 關 AWS Lambda 函數的最後一次調用時檢索信息。Amazon Inspector 會使用這項資訊，將掃描重點放在您環境中過去 90 天內處於作用中狀態的 Lambda 函數。	2023 年 2 月 20 日
AmazonInspector2 ServiceRolePolicy — 現有政策的更新	Amazon Inspector 添加了一個新的語句，允許 Amazon Inspector 檢索有關 AWS Lambda 功能的信息，包括與每個功能關聯的每個層版本。Amazon Inspector 使用此資訊掃描 Lambda 函數是否存在安全漏洞。	2022 年 11 月 28 日

變更	描述	日期
AmazonInspector2 ServiceRolePolicy — 現有政策的更新	Amazon Inspector 已經添加了一個新的動作，以允許 Amazon Inspector 描述 SSM 關聯執行。此外，Amazon Inspector 也新增了額外的資源範圍，讓 Amazon Inspector 能夠建立、更新、刪除和啟動具有`AmazonInspector2` 擁有的 SSM 文件的 SSM 關聯。	2022 年 8 月 31 日
AmazonInspector2 現有政策的ServiceRolePolicy更新	Amazon Inspector 已更新政策的資源範圍設定，以允許 Amazon Inspector 收集其他 AWS 分割區中的軟體庫存。	2022 年 8 月 12 日
AmazonInspector2 ServiceRolePolicy — 現有政策的更新	Amazon Inspector 已重新架構動作的資源範圍，讓 Amazon Inspector 能夠建立、刪除和更新 SSM 關聯。	2022 年 8 月 10 日
AmazonInspector2 ReadOnlyAccess — 新政策	Amazon Inspector 添加了一個新的政策，以允許對 Amazon Inspector 功能的只讀	2022 年 1 月 21 日
AmazonInspector2 FullAccess — 新政策	Amazon Inspector 添加了一項新政策，以允許完全訪問 Amazon Inspector 功能。	2021 年 11 月 29 日
AmazonInspector2 ServiceRolePolicy — 新政策	亞馬遜 Inspector 添加了一項新政策，允許 Amazon Inspector 代表您在其他服務中執行操作。	2021 年 11 月 29 日
Amazon Inspector 開始跟踪更改	Amazon Inspector 開始追蹤其 AWS 受管政策的變更。	2021 年 11 月 29 日

使用 Amazon Inspector 的服務連結角色

Amazon Inspector 使用名為AWSServiceRoleForAmazonInspector2的 AWS Identity and Access Management (IAM) 服務連結角色。此服務連結角色是直接連結至 Amazon Inspector 的 IAM 角色。它是由 Amazon Inspector 預先定義的，它包括亞馬遜 Inspector 需要代表您調用其他 AWS 服務 的所有許可。

服務連結角色可讓您輕鬆設定 Amazon Inspector，因為您不必手動新增必要的許可。Amazon Inspector 會定義其服務連結角色的許可，除非另有定義，否則只有 Amazon Inspector 可以擔任該角色。定義的許可包括信任政策和許可政策，且該許可政策無法附加至其他 IAM 實體。

您必須設定許可，以允許 IAM 實體 (例如群組或角色) 建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的服務連結角色許可。只有在刪除服務連結角色的相關資源後，才能刪除該角色。這樣可以保護您的 Amazon Inspector 資源，因為您無法意外移除存取資源的權限。

如需關於支援服務連結角色的其他服務資訊，請參閱《可搭配 IAM 運作的AWS 服務》，尋找服務連結角色欄中顯示為是的服務。選擇具有連結的 [是]，以檢閱該服務的服務連結角色文件。

Amazon Inspector 的服務連結角色許可

Amazon Inspector 使用名為AWSServiceRoleForAmazonInspector2的服務連結角色。此服務連結角色會信任inspector2.amazonaws.com服務擔任該角色。

角色的許可政策 (名AmazonInspector2ServiceRolePolicy為) 可讓 Amazon Inspector 執行以下任務：

- 使用 Amazon Elastic Compute Cloud (Amazon EC2) 動作擷取執行個體和網路路徑的相關資訊。
- 使用 AWS Systems Manager 動作從 Amazon EC2 執行個體擷取庫存，以及從自訂路徑擷取第三方套件的相關資訊。
- 使用此 AWS Systems Manager SendCommand動作可呼叫目標執行個體的 CIS 掃描。
- 使用 Amazon 彈性容器登錄動作擷取容器映像的相關資訊。
- 使用 AWS Lambda 動作擷取有關 Lambda 函數的資訊。
- 使用 AWS Organizations 動作來描述相關聯的帳號。
- 使用 CloudWatch 動作擷取上次呼叫 Lambda 函數的相關資訊。
- 使用選取 IAM 動作擷取 IAM 政策的相關資訊，這些資訊可能會在 Lambda 程式碼中造成安全漏洞。
- 使用 CodeGuru 安全性動作來執行 Lambda 函數中的程式碼掃描。Amazon Inspector 使用下列 CodeGuru 安全動作：

- 程式碼安全性：CreateScan — 授予建立 CodeGuru 安全性掃描的權限。
- 程式碼安全性：GetScan — 授予擷取 CodeGuru 安全性掃描中繼資料的權限。
- 程式碼古魯安全性：ListFindings — 授予擷取安全性產生之發現項目的權限。 CodeGuru
- 程式碼庫安全性：DeleteScansByCategory — 授予 CodeGuru 安全性刪除 Amazon Inspector 所啟動之掃描的權限。
- 程式碼古魯安全性：BatchGetFindings — 授予擷取安全性產生之特定發現項目批次的權限。 CodeGuru

- 使用選取 Elastic Load Balancing 動作，對屬於 Elastic Load Balancing 目標群組的 EC2 執行個體進行網路掃描。

角色設定為下列權限原則。

```
    {
"Version": "2012-10-17",
"Statement": [
 {
  "Sid": "TirosPolicy",
  "Effect": "Allow",
  "Action": [
   "directconnect:DescribeConnections",
   "directconnect:DescribeDirectConnectGatewayAssociations",
   "directconnect:DescribeDirectConnectGatewayAttachments",
   "directconnect:DescribeDirectConnectGateways",
   "directconnect:DescribeVirtualGateways",
   "directconnect:DescribeVirtualInterfaces",
   "ec2:DescribeAvailabilityZones",
   "ec2:DescribeCustomerGateways",
   "ec2:DescribeInstances",
   "ec2:DescribeInternetGateways",
   "ec2:DescribeManagedPrefixLists",
   "ec2:DescribeNatGateways",
   "ec2:DescribeNetworkAcls",
   "ec2:DescribeNetworkInterfaces",
   "ec2:DescribePrefixLists",
   "ec2:DescribeRegions",
   "ec2:DescribeRouteTables",
   "ec2:DescribeSecurityGroups",
   "ec2:DescribeSubnets",
   "ec2:DescribeTransitGatewayAttachments",
```

```
    "ec2:DescribeTransitGatewayConnects",
    "ec2:DescribeTransitGatewayPeeringAttachments",
    "ec2:DescribeTransitGatewayRouteTables",
    "ec2:DescribeTransitGatewayVpcAttachments",
    "ec2:DescribeTransitGateways",
    "ec2:DescribeVpcEndpointServiceConfigurations",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcPeeringConnections",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpnConnections",
    "ec2:DescribeVpnGateways",
    "ec2:GetManagedPrefixListEntries",
    "ec2:GetTransitGatewayRouteTablePropagations",
    "ec2:SearchTransitGatewayRoutes",
    "elasticloadbalancing:DescribeListeners",
    "elasticloadbalancing:DescribeLoadBalancerAttributes",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeRules",
    "elasticloadbalancing:DescribeTags",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTargetGroupAttributes",
    "elasticloadbalancing:DescribeTargetHealth",
    "network-firewall:DescribeFirewall",
    "network-firewall:DescribeFirewallPolicy",
    "network-firewall:DescribeResourcePolicy",
    "network-firewall:DescribeRuleGroup",
    "network-firewall:ListFirewallPolicies",
    "network-firewall:ListFirewalls",
    "network-firewall:ListRuleGroups",
    "tiros:CreateQuery",
    "tiros:GetQueryAnswer"
   ],
   "Resource": [
    "*"
   ]
  },
  {
   "Sid": "PackageVulnerabilityScanning",
   "Effect": "Allow",
   "Action": [
    "ecr:BatchGetImage",
    "ecr:BatchGetRepositoryScanningConfiguration",
    "ecr:DescribeImages",
    "ecr:DescribeRegistry",
```

```
    "ecr:DescribeRepositories",
    "ecr:GetAuthorizationToken",
    "ecr:GetDownloadUrlForLayer",
    "ecr:GetRegistryScanningConfiguration",
    "ecr:ListImages",
    "ecr:PutRegistryScanningConfiguration",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAccounts",
    "ssm:DescribeAssociation",
    "ssm:DescribeAssociationExecutions",
    "ssm:DescribeInstanceInformation",
    "ssm:ListAssociations",
    "ssm:ListResourceDataSync"
   ],
   "Resource": "*"
  },
  {
   "Sid": "LambdaPackageVulnerabilityScanning",
   "Effect": "Allow",
   "Action": [
    "lambda:ListFunctions",
    "lambda:GetFunction",
    "lambda:GetLayerVersion",
    "cloudwatch:GetMetricData"
   ],
   "Resource": "*"
  },
  {
   "Sid": "GatherInventory",
   "Effect": "Allow",
   "Action": [
    "ssm:CreateAssociation",
    "ssm:StartAssociationsOnce",
    "ssm:DeleteAssociation",
    "ssm:UpdateAssociation"
   ],
   "Resource": [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ssm:*:*:document/AmazonInspector2-*",
    "arn:aws:ssm:*:*:document/AWS-GatherSoftwareInventory",
    "arn:aws:ssm:*:*:managed-instance/*",
    "arn:aws:ssm:*:*:association/*"
   ]
```

```
  },
  {
   "Sid": "DataSyncCleanup",
   "Effect": "Allow",
   "Action": [
    "ssm:CreateResourceDataSync",
    "ssm:DeleteResourceDataSync"
   ],
   "Resource": [
    "arn:aws:ssm:*:*:resource-data-sync/InspectorResourceDataSync-do-not-delete"
   ]
  },
  {
   "Sid": "ManagedRules",
   "Effect": "Allow",
   "Action": [
    "events:PutRule",
    "events:DeleteRule",
    "events:DescribeRule",
    "events:ListTargetsByRule",
    "events:PutTargets",
    "events:RemoveTargets"
   ],
   "Resource": [
    "arn:aws:events:*:*:rule/DO-NOT-DELETE-AmazonInspector*ManagedRule"
   ]
  },
  {
   "Sid": "LambdaCodeVulnerabilityScanning",
   "Effect": "Allow",
   "Action": [
    "codeguru-security:CreateScan",
    "codeguru-security:GetAccountConfiguration",
    "codeguru-security:GetFindings",
    "codeguru-security:GetScan",
    "codeguru-security:ListFindings",
    "codeguru-security:BatchGetFindings",
    "codeguru-security:DeleteScansByCategory"
   ],
   "Resource": [
    "*"
   ]
  },
  {
```

```
    "Sid": "CodeGuruCodeVulnerabilityScanning",
    "Effect": "Allow",
    "Action": [
     "iam:GetRole",
     "iam:GetRolePolicy",
     "iam:GetPolicy",
     "iam:GetPolicyVersion",
     "iam:ListAttachedRolePolicies",
     "iam:ListPolicies",
     "iam:ListPolicyVersions",
     "iam:ListRolePolicies",
     "lambda:ListVersionsByFunction"
    ],
    "Resource": [
     "*"
    ],
    "Condition": {
     "ForAnyValue:StringEquals": {
      "aws:CalledVia": [
       "codeguru-security.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "Ec2DeepInspection",
    "Effect": "Allow",
    "Action": [
     "ssm:PutParameter",
     "ssm:GetParameters",
     "ssm:DeleteParameter"
    ],
    "Resource": [
     "arn:aws:ssm:*:*:parameter/inspector-aws/service/inspector-linux-application-paths"
    ],
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   },
   {
    "Sid": "AllowManagementOfServiceLinkedChannel",
    "Effect": "Allow",
```

```
    "Action": [
     "cloudtrail:CreateServiceLinkedChannel",
     "cloudtrail:DeleteServiceLinkedChannel"
    ],
    "Resource": [
     "arn:aws:cloudtrail:*:*:channel/aws-service-channel/inspector2/*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   },
   {
    "Sid": "AllowListServiceLinkedChannels",
    "Effect": "Allow",
    "Action": [
     "cloudtrail:ListServiceLinkedChannels"
    ],
    "Resource": [
     "*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   },
   {
    "Sid": "AllowToRunInvokeCisSpecificDocuments",
    "Effect": "Allow",
    "Action": [
     "ssm:SendCommand",
     "ssm:GetCommandInvocation"
    ],
    "Resource": [
     "arn:aws:ssm:*:*:document/AmazonInspector2-InvokeInspectorSsmPluginCIS"
    ]
   },
   {
    "Sid": "AllowToRunCisCommandsToSpecificResources",
    "Effect": "Allow",
    "Action": [
     "ssm:SendCommand"
```

```
    ],
    "Resource": [
     "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   },
   {
    "Sid": "AllowToPutCloudwatchMetricData",
    "Effect": "Allow",
    "Action": [
     "cloudwatch:PutMetricData"
    ],
    "Resource": [
     "*"
    ],
    "Condition": {
     "StringEquals": {
      "cloudwatch:namespace": "AWS/Inspector2"
     }
    }
   }
  ]
}
```

為 Amazon Inspector 創建服務鏈接角色

您不需要手動建立一個服務連結角色。當您在 AWS Management Console、或 AWS API 中啟用亞馬遜檢查器時 AWS CLI，Amazon Inspector 會為您建立服務連結角色。

編輯 Amazon Inspector 的服務連結角色

Amazon Inspector 不允許您編輯AWSServiceRoleForAmazonInspector2服務連結的角色。建立服務連結角色之後，您無法變更角色的名稱，因為各種實體可能會參照該角色。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 Amazon Inspector 的服務鏈接角色

如果您不再需要使用 Amazon Inspector，建議您刪除AWSServiceRoleForAmazonInspector2服務連結角色。刪除角色之前，您必須先在每個已啟用 Amazon Inspector 的 AWS 區域 位置停用

該角色。當您停用 Amazon Inspector 時，它不會為您刪除角色。因此，如果您再次啟用 Amazon Inspector，它可以使用現有的角色。這樣，您就可以避免擁有未被主動監視或維護的未使用實體。然而，在手動刪除服務連結角色之前，您必須先清除資源。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您啟用 Amazon Inspector 時，Amazon Inspector 會為您重新建立服務連結角色。

> **Note**
>
> 如果您嘗試刪除資源時，Amazon Inspector 服務正在使用該角色，則刪除可能會失敗。如果發生這種情況，請等待幾分鐘，然後再次嘗試該操作。

您可以使用 IAM 主控台 AWS CLI、或 AWS API 刪除`AWSServiceRoleForAmazonInspector2`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。

Amazon Inspector 無代理程式掃描的服務連結角色許可

Amazon Inspector 無代理程式掃描會使用名為的服務連結角色。`AWSServiceRoleForAmazonInspector2Agentless`此單鏡反光相機可讓 Amazon Inspector 在您的帳戶中建立 Amazon EBS 磁碟區快照，然後從該快照存取資料。此服務連結角色會信任`agentless.inspector2.amazonaws.com`服務擔任該角色。

> **Important**
>
> 此服務連結角色中的陳述式可防止 Amazon Inspector 在您使用標籤從掃描中排除的任何 EC2 執行個體上執行無代理程式掃描。`InspectorEc2Exclusion`此外，當用於加密磁碟區的 KMS 金鑰具有`InspectorEc2Exclusion`標籤時，這些陳述式會防止 Amazon Inspector 從磁碟區存取加密的資料。如需詳細資訊，請參閱 將執行個體排除在 Amazon Inspector。

角色的許可政策 (名`AmazonInspector2AgentlessServiceRolePolicy`為) 可讓 Amazon Inspector 執行以下任務：

- 使用 Amazon Elastic Compute Cloud (Amazon EC2) 動作擷取 EC2 執行個體、磁碟區和快照的相關資訊。
  - 使用 Amazon EC2 標記動作，使用標籤金鑰`InspectorScan`標記掃描的快照。
  - 使用 Amazon EC2 快照動作建立快照、使用標籤金鑰`InspectorScan`標記快照，然後刪除已使用標籤金鑰`InspectorScan`標記之 Amazon EBS 磁碟區的快照。

- 使用 Amazon EBS 動作從使用`InspectorScan`標籤金鑰標記的快照擷取資訊。
- 使用選取 AWS KMS 解密動作來解密使用 AWS KMS 客戶管理金鑰加密的快照。當用來加密快照的 KMS 金鑰使用標籤加上`InspectorEc2Exclusion`標籤時，Amazon Inspector 不會解密快照。

角色設定為下列權限原則。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "InstanceIdentification",
   "Effect": "Allow",
   "Action": [
    "ec2:DescribeInstances",
    "ec2:DescribeVolumes",
    "ec2:DescribeSnapshots"
   ],
   "Resource": "*"
  },
  {
   "Sid": "GetSnapshotData",
   "Effect": "Allow",
   "Action": [
    "ebs:ListSnapshotBlocks",
    "ebs:GetSnapshotBlock"
   ],
   "Resource": "arn:aws:ec2:*:*:snapshot/*",
   "Condition": {
    "StringLike": {
     "aws:ResourceTag/InspectorScan": "*"
    }
   }
  },
  {
   "Sid": "CreateSnapshotsAnyInstanceOrVolume",
   "Effect": "Allow",
   "Action": "ec2:CreateSnapshots",
   "Resource": [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:volume/*"
   ]
```

```
  },
  {
   "Sid": "DenyCreateSnapshotsOnExcludedInstances",
   "Effect": "Deny",
   "Action": "ec2:CreateSnapshots",
   "Resource": "arn:aws:ec2:*:*:instance/*",
   "Condition": {
    "StringEquals": {
     "ec2:ResourceTag/InspectorEc2Exclusion": "true"
    }
   }
  },
  {
   "Sid": "CreateSnapshotsOnAnySnapshotOnlyWithTag",
   "Effect": "Allow",
   "Action": "ec2:CreateSnapshots",
   "Resource": "arn:aws:ec2:*:*:snapshot/*",
   "Condition": {
    "Null": {
     "aws:TagKeys": "false"
    },
    "ForAllValues:StringEquals": {
     "aws:TagKeys": "InspectorScan"
    }
   }
  },
  {
   "Sid": "CreateOnlyInspectorScanTagOnlyUsingCreateSnapshots",
   "Effect": "Allow",
   "Action": "ec2:CreateTags",
   "Resource": "arn:aws:ec2:*:*:snapshot/*",
   "Condition": {
    "StringLike": {
     "ec2:CreateAction": "CreateSnapshots"
    },
    "Null": {
     "aws:TagKeys": "false"
    },
    "ForAllValues:StringEquals": {
     "aws:TagKeys": "InspectorScan"
    }
   }
  },
  {
```

```
    "Sid": "DeleteOnlySnapshotsTaggedForScanning",
    "Effect": "Allow",
    "Action": "ec2:DeleteSnapshot",
    "Resource": "arn:aws:ec2:*:*:snapshot/*",
    "Condition": {
     "StringLike": {
      "ec2:ResourceTag/InspectorScan": "*"
     }
    }
   },
   {
    "Sid": "DenyKmsDecryptForExcludedKeys",
    "Effect": "Deny",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:*:*:key/*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceTag/InspectorEc2Exclusion": "true"
     }
    }
   },
   {
    "Sid": "DecryptSnapshotBlocksVolContext",
    "Effect": "Allow",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:*:*:key/*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     },
     "StringLike": {
      "kms:ViaService": "ec2.*.amazonaws.com",
      "kms:EncryptionContext:aws:ebs:id": "vol-*"
     }
    }
   },
   {
    "Sid": "DecryptSnapshotBlocksSnapContext",
    "Effect": "Allow",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:*:*:key/*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
```

```
    },
    "StringLike": {
     "kms:ViaService": "ec2.*.amazonaws.com",
     "kms:EncryptionContext:aws:ebs:id": "snap-*"
    }
   }
  },
  {
   "Sid": "DescribeKeysForEbsOperations",
   "Effect": "Allow",
   "Action": "kms:DescribeKey",
   "Resource": "arn:aws:kms:*:*:key/*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    },
    "StringLike": {
     "kms:ViaService": "ec2.*.amazonaws.com"
    }
   }
  },
  {
   "Sid": "ListKeyResourceTags",
   "Effect": "Allow",
   "Action": "kms:ListResourceTags",
   "Resource": "arn:aws:kms:*:*:key/*"
  }
 ]
}
```

建立無代理程式掃描的服務連結角色

您不需要手動建立一個服務連結角色。當您在 AWS Management Console、或 AWS API 中啟用亞馬遜檢查器時 AWS CLI，Amazon Inspector 會為您建立服務連結角色。

編輯無代理程式掃描的服務連結角色

Amazon Inspector 不允許您編輯AWSServiceRoleForAmazonInspector2Agentless服務連結的角色。建立服務連結角色之後，您無法變更角色的名稱，因為各種實體可能會參照該角色。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。

刪除無代理程式掃描的服務連結角色

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**
>
> 若要刪除AWSServiceRoleForAmazonInspector2Agentless角色，您必須在所有提供無代理程式掃瞄的區域中，將掃描模式設定為以代理程式為基礎。如需詳細資訊，請參閱 [TBD 設定掃描模式連結]。

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台或 AWS API 刪除 AWSServiceRoleForAmazonInspector2Agentless 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。

Amazon Inspector 身分和存取疑難

使用下列資訊可協助您診斷和修正使用 Amazon Inspector 和 IAM 時可能會遇到的常見問題。

主題

- 我沒有授權在 Amazon Inspector 中執行操作
- 我沒有授權執行 iam：PassRole
- 我想允許我以外的人訪問我 AWS 帳戶 的 Amazon Inspector 資源

我沒有授權在 Amazon Inspector 中執行操作

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 inspector2:*GetWidget* 許可時發生。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 inspector2: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 inspector2:*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，則必須更新您的政策以允許您將角色傳遞給 Amazon Inspector。

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`嘗試使用主控台在 Amazon Inspector 中執行動作時，會發生下列範例錯誤。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞至該服務的許可。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在這種情況下，Mary 的政策必須更新，允許她執行 `iam:PassRole` 動作。

如果您需要協助，請聯絡您的 AWS 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問我 AWS 帳戶 的 Amazon Inspector 資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要了解 Amazon Inspector 查器是否支援這些功能，請參閱亞馬遜檢查器如何使用 IAM。
- 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。
- 若要了解如何將資源存取權提供給第三方 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。

監控 Amazon Inspector

監控是維持 Amazon Inspector 和其他 AWS 解決方案的可靠性、可用性和效能的重要組成部分。 AWS 提供監控工具來觀看 Amazon Inspector、在發生錯誤時報告，並在適當時採取自動動作：

- Amazon EventBridge 是一種無伺服器事件匯流排服務，可讓您輕鬆地將應用程式與各種來源的資料連接起來。 EventBridge 從您自己的應用程式、S oftware-as-a 服務 (SaaS) 應用程式以及服務提供即時資料串流，並 AWS 將該資料路由到目標 (例如 Lambda)。這可讓您監視發生在服務中的事件，並建置事件驅動的架構。如需詳細資訊，請參閱 Amazon EventBridge 使用者指南。
- AWS CloudTrail 會擷取來自或代表 AWS 帳戶發出的 API 呼叫和相關事件。 CloudTrail 然後將日誌檔交付到您指定的 Amazon S3 儲存貯體。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。如需詳細資訊，請參閱 AWS CloudTrail 使用者指南。

使用記錄 Amazon Inspector API 調用 AWS CloudTrail

Amazon Inspector 與這項服務整合在一起 AWS CloudTrail，可提供 IAM 使用者或角色或 Amazon Inspector 中所採取的動作記錄的服務。 AWS 服務 CloudTrail 捕獲 Amazon Inspector 的所有 API 調用作為事件。擷取的呼叫包括來自 Amazon Inspector 主控台的呼叫，以及對 Amazon Inspector API 操作的呼叫。如果您建立追蹤，您可以啟用持續交付 CloudTrail 事件到 Amazon S3 儲存貯體，包括 Amazon Inspector 的事件。如果您未設定追蹤，您仍然可以在 [事件歷程記錄] 中檢視 CloudTrail主控台中最近的事件。使用收集的資訊 CloudTrail，您可以判斷：

- 這是向 Amazon Inspector 提出的請求。
- 提出請求的 IP 地址。
- 提出要求的人員。
- 提出請求的時間。

若要進一步了解 CloudTrail，請參閱使AWS CloudTrail 用者指南。

Amazon Inspector 信息 CloudTrail

CloudTrail 在您創建帳戶 AWS 帳戶 時啟用。當活動在 Amazon Inspector 中發生時，該活動會與事件歷史記錄中的其他 CloudTrail AWS 服務 事件一起記錄在事件中。您可以查看，搜索和下載最近的事件 AWS 帳戶。如需詳細資訊，請參閱使用 CloudTrail 事件歷程記錄檢視事件。

若要持續記錄您 AWS 帳戶的事件 (包括 Amazon Inspector 的事件)，請建立追蹤。追蹤可 CloudTrail 將日誌檔交付到 Amazon S3 儲存貯體。依預設，當您在主控台中建立追蹤時，該追蹤會套用至所有的 AWS 區域。該追蹤會記錄來自 AWS 分割區中所有區域的事件，並將日誌檔案交付到您指定的 Amazon S3 儲存貯體。此外，您可以設定其他， AWS 服務 以進一步分析 CloudTrail 記錄中收集的事件資料並採取行動。如需詳細資訊，請參閱下列主題：

- 建立追蹤的概觀
- CloudTrail 支援的服務與整合
- 設定 CloudTrail 的 Amazon SNS 通知
- 從多個帳戶接收 CloudTrail 日誌文件
- 接收來自多個區域的 CloudTrail 記錄檔

所有 Amazon Inspector 操作都由記錄 CloudTrail。Amazon Inspector 可以執行的所有操作都記錄在 Amazon Inspector API 參考中。例如，呼叫`CreateFindingsReportListCoverage`、和`UpdateOrganizationConfiguration`動作會在 CloudTrail 記錄檔中產生項目。

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 是否使用根使用者或 IAM 使用者憑證提出該請求。
- 要求是使用角色或同盟使用者的暫時安全性登入資料來提出。
- 該請求是否由另一項 AWS 服務服務提出。

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

瞭解 Amazon Inspector 日誌檔項目

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。事件包含請求的動作、動作的日期和時間、請求參數等相關資訊。 CloudTrail 日誌文件不是公共 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。

Amazon Inspector 掃描信息 CloudTrail

Amazon Inspector 掃描集成 CloudTrail. 所有 Amazon Inspector 掃描 API 操作都會記錄為管理事件。如需亞馬遜檢查器日誌到的 Amazon Inspector 掃描 API 操作的清單 CloudTrail，請參閱 Amazon Inspector 查器 API 參考中的 Amazon Inspector 查器掃描。

下列範例顯示示範ScanSbom動作的 CloudTrail 記錄項目：


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROA123456789EXAMPLE:akua_mansa",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/akua_mansa",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA123456789EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-10-17T15:22:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-10-17T16:02:34Z",
    "eventSource": "gamma-inspector-scan.amazonaws.com",
    "eventName": "ScanSbom",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "203.0.113.0",
    "userAgent": "aws-sdk-java/2.20.162 Mac_OS_X/13.5.2 OpenJDK_64-
Bit_Server_VM/17.0.8+7-LTS Java/17.0.8 vendor/Amazon.com_Inc. io/sync http/
UrlConnection cfg/retry-mode/legacy",
    "requestParameters": {
        "sbom": {
            "specVersion": "1.5",
            "metadata": {
                "component": {
                    "name": "debian",
                    "type": "operating-system",
                    "version": "9"
                }
            },
```

```
            "components": [
                {
                    "name": "packageOne",
                    "purl": "pkg:deb/debian/packageOne@1.0.0?arch=x86_64&distro=9",
                    "type": "application"
                }
            ],
            "bomFormat": "CycloneDX"
        }
    },
    "responseElements": null,
    "requestID": "f041a27f-f33e-4f70-b09b-5fbc5927282a",
    "eventID": "abc8d1e4-d214-4f07-bc56-8a31be6e36fe",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Amazon Inspector 的合規驗證

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性控制的最佳實務。
- 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。
- 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 Inspector 的彈性

AWS 全球基礎架構是圍繞 AWS 區域 和可用區域建立的。 AWS 區域 提供多個實體分離和隔離的可用區域，這些區域透過低延遲、高輸送量和高度備援的網路連線。透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

Amazon Inspector 的基礎設施

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

您可以使用 AWS 已發佈的 API 呼叫，透過網路存取 Amazon Inspector。使用者端必須支援下列專案：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 具備完美轉送私密(PFS)的密碼套件，例如 DHE (Ephemeral Diffie-Hellman)或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

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

Amazon Inspector 的事件回應

安全性是最高的優先事項 AWS。作為 AWS 雲端共同責任模式的一部分，您可以 AWS 管理符合最敏感安全性組織需求的資料中心、網路和軟體架構。 AWS 負責與 AWS Config 服務本身相關的任何事件響應。此外，身為 AWS 客戶，您有責任維護雲端中的安全性。這表示您可以透過可存取的 AWS 工具和功能來控制選擇實作的安全性，並負責共用責任模型中的事件回應。

透過為雲端中執行的應用程式建立符合目標的安全性基準，您可以偵測可以回應的偏差。由於安全性事件回應可能是一個複雜的主題，因此我們建議您檢閱下列資源，讓您更了解事件回應 (IR) 和您的選擇對公司目標的影響：AWS 安全性事件回應指南、AWS 安全性最佳實務白皮書，以及AWS 雲端採用架構 (CAF) 白皮 paper 的安全性觀點。

Amazon Inspector 整合

Amazon Inspector 與其他 AWS 服務集成。這些服務可以從 Amazon Inspector 擷取資料，讓您以新的方式檢視發現結果。檢閱下列整合選項，進一步了解該服務如何設定為與 Amazon Inspector 搭配使用。

整合 Amazon Inspector 與 Amazon ECR

Amazon Elastic Container Registry (Amazon ECR) 是全受管的 Docker 容器登錄，可讓您輕鬆存放、共用和部署容器映像。Amazon ECR 私有登錄會將您的容器映像託管在高可用性和可擴展的架構中。您可以使用 Amazon Inspector 掃描存放在 Amazon ECR 儲存庫中的容器映像，找出易受攻擊的作業系統套件和程式設計語言套件。

如需將 Amazon ECR 與亞馬 Amazon Inspector 查器搭配使用的詳細資訊，請參閱Amazon Inspector 器與 Amazon Elastic Container Registry (Amazon ECR)。

Amazon Inspector 集成 AWS Security Hub

AWS Security Hub從您的 AWS 帳戶、服務和其他支援產品中收集安全性資料，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 還會為所有整合式 AWS 服務和合 AWS 作夥伴網路產品的發現項目建立中央位置。透過 Amazon Inspector 啟用 Security Hub 會自動允許 Security Hub 擷取 Amazon Inspector 發現項目資料。

如需使用 Security Hub 搭配 Amazon 檢查器的詳細資訊，請參閱Amazon Inspector 與集成 AWS Security Hub。

Amazon Inspector 器與 Amazon Elastic Container Registry (Amazon ECR)

Amazon ECR 是全受管容器登錄，支援碼頭工人和 OCI 映像和成品。 AWS如果您使用 Amazon ECR，可以為登錄啟用增強型掃描，讓 Amazon Inspector 自動偵測您的容器映像，並掃描它們是否有易受攻擊的作業系統套件和程式設計語言套件。

這項整合可讓您在 Amazon ECR 主控台中檢視容器映像的 Amazon Inspector 發現項目。此外，您可以從 Amazon ECR 主控台管理掃描頻率，並透過建立包含篩選器來精簡掃描範圍。

啟動整合

您可以透過 Amazon Inspector 主控台或 API 啟用 Amazon Inspector 掃描，或透過將儲存庫設定為透過 Amazon ECR 主控台或 API 搭配 Amazon Inspector 使用增強型掃描來啟動整合。

如需透過 Amazon Inspector 啟用整合的詳細資訊，請參閱使用 Amazon Inspector 自動化資源。

如需在 Amazon ECR 中啟用和設定增強型掃描的相關資訊，請參閱 Amazon ECR 使用者指南中的增強型掃描。

使用與多帳戶環境的整合

如果您是多帳戶環境中的會員，則可以透過 Amazon ECR 啟用增強型掃描。不過，一旦啟用，就只能由 Amazon Inspector 委派的管理員停用它。如果停用，則會恢復為基本掃描。如需更多詳細資訊，請參閱 停用 Amazon Inspector。

Amazon Inspector 與集成 AWS Security Hub

Security Hub 提供中安全性狀態的全面檢視， AWS 並協助您根據安全性產業標準和最佳做法來檢查您的環境。Security Hub 會從各個 AWS 帳戶、服務和其他支援的產品收集安全性資料。您可以使用它提供的資訊來分析您的安全趨勢，並找出最優先順序的安全性問題。

Amazon Inspector 與 Security Hub 的集成允許您將發現從 Amazon Inspector 發送到 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。

在中 AWS Security Hub，安全性問題會追蹤為發現項目。某些發現項目是由其他 AWS 服務或協力廠商產品偵測到的問題所導致。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。您可以檢視和篩選發現項目清單，並檢視發現項目詳細資訊。如需有關 Security Hub 中發現項目的詳細資訊，請參閱AWS Security Hub 使用者指南中的檢視發現項目。您也可以追蹤問題清單的調查狀態。請參閱 AWS Security Hub 使用者指南中的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)。

一旦 Amazon Inspector 中解決並關閉了這些發現，Security Hub 將存檔 Amazon Inspector 的發現。

查看亞馬遜檢查器發現 AWS Security Hub

Amazon Inspector 經典版和新的 Amazon Inspector 的發現可在安全中心的同一個面板中找到。不過，您可以在篩選列中新增一個來篩選新 Amazon Inspector `"aws/inspector/ProductVersion": "2"` 的發現項目。新增此篩選器會從安全中心儀表板排除 Amazon Inspector 經典版中的發現項目。

從 Amazon Inspector 發現示例


```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:inspector2:us-east-1:123456789012:finding/FINDING_ID",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/inspector",
  "ProductName": "Inspector",
  "CompanyName": "Amazon",
  "Region": "us-east-1",
  "GeneratorId": "AWSInspector",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Vulnerabilities/CVE"
  ],
  "FirstObservedAt": "2023-01-31T20:25:38Z",
  "LastObservedAt": "2023-05-04T18:18:43Z",
  "CreatedAt": "2023-01-31T20:25:38Z",
  "UpdatedAt": "2023-05-04T18:18:43Z",
  "Severity": {
    "Label": "HIGH",
    "Normalized": 70
  },
  "Title": "CVE-2022-34918 - kernel",
  "Description": "An issue was discovered in the Linux kernel through 5.18.9. A type
confusion bug in nft_set_elem_init (leading to a buffer overflow) could be used by a
local attacker to escalate privileges, a different vulnerability than CVE-2022-32250.
(The attacker can obtain root access, but must start with an unprivileged user
namespace to obtain CAP_NET_ADMIN access.) This can be fixed in nft_setelem_parse_data
in net/netfilter/nf_tables_api.c.",
  "Remediation": {
    "Recommendation": {
      "Text": "Remediation is available. Please refer to the Fixed version in the
vulnerability details section above. For detailed remediation guidance for each of the
affected packages, refer to the vulnerabilities section of the detailed finding JSON."
    }
  },
  "ProductFields": {
```

```
    "aws/inspector/FindingStatus": "ACTIVE",
    "aws/inspector/inspectorScore": "7.8",
    "aws/inspector/resources/1/resourceDetails/awsEc2InstanceDetails/platform":
 "AMAZON_LINUX_2",
    "aws/inspector/ProductVersion": "2",
    "aws/inspector/instanceId": "i-0f1ed287081bdf0fb",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/inspector/
arn:aws:inspector2:us-east-1:123456789012:finding/FINDING_ID",
    "aws/securityhub/ProductName": "Inspector",
    "aws/securityhub/CompanyName": "Amazon"
  },
  "Resources": [
    {
      "Type": "AwsEc2Instance",
      "Id": "arn:aws:ec2:us-east-1:123456789012:i-0f1ed287081bdf0fb",
      "Partition": "aws",
      "Region": "us-east-1",
      "Tags": {
        "Patch Group": "SSM",
        "Name": "High-SEv-Test"
      },
      "Details": {
        "AwsEc2Instance": {
          "Type": "t2.micro",
          "ImageId": "ami-0cff7528ff583bf9a",
          "IpV4Addresses": [
            "52.87.229.97",
            "172.31.57.162"
          ],
          "KeyName": "ACloudGuru",
          "IamInstanceProfileArn": "arn:aws:iam::123456789012:instance-profile/
AmazonSSMRoleForInstancesQuickSetup",
          "VpcId": "vpc-a0c2d7c7",
          "SubnetId": "subnet-9c934cb1",
          "LaunchedAt": "2022-07-26T21:49:46Z"
        }
      }
    }
  ],
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
```

```
  "Vulnerabilities": [
    {
      "Id": "CVE-2022-34918",
      "VulnerablePackages": [
        {
          "Name": "kernel",
          "Version": "5.10.118",
          "Epoch": "0",
          "Release": "111.515.amzn2",
          "Architecture": "X86_64",
          "PackageManager": "OS",
          "FixedInVersion": "0:5.10.130-118.517.amzn2",
          "Remediation": "yum update kernel"
        }
      ],
      "Cvss": [
        {
          "Version": "2.0",
          "BaseScore": 7.2,
          "BaseVector": "AV:L/AC:L/Au:N/C:C/I:C/A:C",
          "Source": "NVD"
        },
        {
          "Version": "3.1",
          "BaseScore": 7.8,
          "BaseVector": "CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H",
          "Source": "NVD"
        },
        {
          "Version": "3.1",
          "BaseScore": 7.8,
          "BaseVector": "CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H",
          "Source": "NVD",
          "Adjustments": []
        }
      ],
      "Vendor": {
        "Name": "NVD",
        "Url": "https://nvd.nist.gov/vuln/detail/CVE-2022-34918",
        "VendorSeverity": "HIGH",
        "VendorCreatedAt": "2022-07-04T21:15:00Z",
        "VendorUpdatedAt": "2022-10-26T17:05:00Z"
      },
      "ReferenceUrls": [
```

```
        "https://git.kernel.org/pub/scm/linux/kernel/git/netdev/net.git/commit/?
id=7e6bc1f6cabcd30aba0b11219d8e01b952eacbb6",
        "https://lore.kernel.org/netfilter-devel/cd9428b6-7ffb-dd22-d949-
d86f4869f452@randorisec.fr/T/",
        "https://www.debian.org/security/2022/dsa-5191"
      ],
      "FixAvailable": "YES"
    }
  ],
  "FindingProviderFields": {
    "Severity": {
      "Label": "HIGH"
    },
    "Types": [
      "Software and Configuration Checks/Vulnerabilities/CVE"
    ]
  },
  "ProcessedAt": "2023-05-05T20:28:38.822Z"
}
```


啟用和設定整合

若要使用 Amazon Inspector 整合 AWS Security Hub，您必須啟用 Security Hub。如需有關如何啟動 Security Hub 的資訊，請參閱AWS Security Hub 使用者指南中的設定安全性中樞。

當您同時啟用 Amazon Inspector 和 Security Hub 時，整合會自動啟動，而 Amazon Inspector 會開始將發現項目傳送到 Security Hub。Amazon Inspector 會使用安全尋找格式 (ASFF)，將其產生的所有發現項目傳送至AWS 安全中樞。

停止發現項目的發佈至 AWS Security Hub

如何停止傳送發現項目

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。

請參閱使用指南中的整合 (主控台) 停用和啟動發現項目流程或停AWS Security Hub 用整合中的發現項目流程 (Security Hub API AWS CLI)。

由 Amazon Inspector 支援的作業系統和程式語言

Amazon Inspector 可以掃描安裝在亞馬遜彈性運算雲端 (Amazon EC2) 執行個體上的軟體應用程式、存放在亞馬遜彈性容器登錄 (Amazon ECR) 儲存庫中的容器映像，以及 AWS Lambda 功能。對於 ECR 容器映像檔，Amazon Inspector 可以掃描作業系統和程式設計語言套件的弱點。對於 Lambda 函數，Amazon Inspector 可以掃描程式碼弱點。Amazon Inspector 掃描資源時，它會使用自己專用的掃描引擎，並從 50 多個資料摘要取得，以產生常見弱點和曝光 (CVE) 的發現結果。來源包括供應商安全諮詢、NVD、MITRE、開放原始碼摘要、內部研究和授權資料摘要。

若要讓 Amazon Inspector 掃描資源，資源必須執行支援的作業系統或使用支援的程式設計語言。本節中的主題列出 Amazon Inspector 目前支援不同資源和掃描類型的作業系統、執行階段和程式設計語言。它們還列出了 Amazon Inspector 先前支援的作業系統，但此後已被廠商停產。廠商停止對作業系統的支援後，Amazon Inspector 只能為作業系統提供有限的支援。

主題

支援的作業系統：Amazon EC2 掃描

下表列出 Amazon Inspector 目前支援掃描 Amazon EC2 執行個體的作業系統。它也會列出每個廠商安全性建議的來源，以及該作業系統是否可以使用以代理程式為基礎或無代理程式掃瞄方法進行掃描。如需有關掃瞄方法的詳細資訊，請參閱代理程式型掃描和無代理程式掃描。

> **Note**
>
> Linux 作業系統偵測僅支援預設套件管理員儲存庫，而且不包含第三方應用程式、延伸支援儲存庫 (例如 BYOS RHEL、PAYG RHEL 和 SAP 適用的 RHEL)，以及選用的儲存庫，例如 Red Hat 應用程式串流。

作業系統	版本	供應商安全建議	無代理程式掃描支援	代理程式型掃描支援
AlmaLinux	8	阿爾薩	是	是
AlmaLinux	9	阿爾薩	是	是
Amazon 亞馬遜	AL2	唉	是	是
Amazon Linux 2023 (AL2023)	AL2023	唉	是	是
Bottlerocket	1.7.0 及更新版本	克薩, CVE	否	是
CentOS CentOS 版	7	西薩	是	是
巴斯特伺服器	10	DSA	是	是
伺服器 (靶心)	11	DSA	是	是
書蟲伺服器	12	DSA	是	是
Fedora	38	CVE	是	是
Fedora	39	CVE	是	是
OpenSUSE	15.5	CVE	是	是
甲骨文 Linux (甲骨文)	7	艾爾莎	是	是

作業系統	版本	供應商安全建議	無代理程式掃描支援	代理程式型掃描支援
甲骨文 Linux (甲骨文)	8	艾爾莎	是	是
甲骨文 Linux (甲骨文)	9	艾爾莎	是	是
Red Hat Enterprise Linux (RHEL)	7	RHSA	是	是
Red Hat Enterprise Linux (RHEL)	8	RHSA	是	是
Red Hat Enterprise Linux (RHEL)	9	RHSA	是	是
Rocky Linux	8	RLSA	是	是
Rocky Linux	9	RLSA	是	是
SUSE Linux Enterprise Server (SLES)	12.4	冰雪公司	是	是
SUSE Linux Enterprise Server (SLES)	12.5	冰雪公司	是	是
SUSE Linux Enterprise Server (SLES)	15.3	冰雪公司	是	是

作業系統	版本	供應商安全建議	無代理程式掃描支援	代理程式型掃描支援
SUSE Linux Enterprise Server (SLES)	15.4	冰雪公司	是	是
SUSE Linux Enterprise Server (SLES)	15.5	冰雪公司	是	是
Ubuntu 的（值得信賴）	14.04 (埃斯姆)	USN, UBUNTU 專業版	是	是
异系列	16.04 (埃斯姆)	USN, UBUNTU 專業版	是	是
仿生	18.04 (埃斯姆)	USN, UBUNTU 專業版	是	是
Ubuntu (焦點)	20.04（英文）	USN	是	是
阿布圖（賈米）	22 月 4 日（英文）	USN	是	是
牛头怪	23.10	USN	是	是
Windows Server	2016	MSKB	否	是
Windows Server	2019	MSKB	否	是
Windows Server	2022	MSKB	否	是
macOS (莫哈韋)	10.14	蘋果 SA	否	是
卡塔利娜	10.15	蘋果 SA	否	是
macOS (大蘇爾)	11	蘋果 SA	否	是
macOS 特雷	12	蘋果 SA	否	是

作業系統	版本	供應商安全建議	無代理程式掃描支援	代理程式型掃描支援
macOS (文圖拉)	13	蘋果 SA	否	是

支援的程式設計語言：Amazon EC2 深度檢查

當掃描 Amazon EC2 Linux 執行個體是否有第三方軟體套件中的漏洞時，Amazon Inspector 目前支援下列程式設計語言：

- Java
- JavaScript
- Python

Amazon Inspector 使用系統管理員代理商在 Amazon EC2 執行個體中部署用於深度檢查的外掛程式。「系統管理員代理商」支援「系統管理員」指南中列為支援套件平台和架構的作業系統。您的 Amazon EC2 執行個體作業系統必須由系統管理員代理商和 Amazon Inspector 支援，才能執行深度檢查掃描。

> **Note**
>
> 瓶裝機作業系統不支援深度檢查。

支持的操作系統：CIS 掃描

下表列出 Amazon Inspector 目前支援進行獨聯體掃描的作業系統。該表還包括用於執行該操作系統掃描的 CIS 基準測試版本。

作業系統	版本	獨聯體基準版
Amazon Linux 2	AL2	2.0.0
Amazon Linux 2023	AL2023	1.0.0
Windows Server	2019	2.0.0
Windows Server	2022	2.0.0

支援的作業系統：使用 Amazon 檢查器掃描 Amazon Inspector R

當掃描 Amazon ECR 儲存庫中的容器映像時，Amazon Inspector 目前支援掃描下列作業系統：此表格也會列出每個作業系統之廠商安全性建議的來源。

作業系統	版本	供應商安全建議
Alpine Linux (Alpine)	3.16	Alpine SecDB
Alpine Linux (Alpine)	3.17	Alpine SecDB
Alpine Linux (Alpine)	3.18	Alpine SecDB
Alpine Linux (Alpine)	3.19	Alpine SecDB
AlmaLinux	8	ALSA
AlmaLinux	9	ALSA
Amazon Linux (AL2)	AL2	ALAS
Amazon Linux 2023 (AL2023)	AL2023	ALAS
CentOS Linux (CentOS)	7	CESA
Debian Server (Buster)	10	DSA
Debian Server (Bullseye)	11	DSA
Debian Server (Bookworm)	12	DSA
Fedora	38	CVE
Fedora	39	CVE
OpenSUSE	15.5	CVE
Oracle Linux (Oracle)	7	ELSA
Oracle Linux (Oracle)	8	ELSA

作業系統	版本	供應商安全建議
Oracle Linux (Oracle)	9	ELSA
Photon OS	3	PHSA
Photon OS	4	PHSA
Photon OS	5	PHSA
Red Hat Enterprise Linux (RHEL)	7	RHSA
Red Hat Enterprise Linux (RHEL)	8	RHSA
Red Hat Enterprise Linux (RHEL)	9	RHSA
Rocky Linux	8	RLSA
Rocky Linux	9	RLSA
SUSE Linux Enterprise Server (SLES)	12.4	SUSE CVE
SUSE Linux Enterprise Server (SLES)	12.5	SUSE CVE
SUSE Linux Enterprise Server (SLES)	15.3	SUSE CVE
SUSE Linux Enterprise Server (SLES)	15.4	SUSE CVE
SUSE Linux Enterprise Server (SLES)	15.5	SUSE CVE
Ubuntu (Trusty)	14.04 (ESM)	USN, Ubuntu Pro
Ubuntu (Xenial)	16.04 (ESM)	USN, Ubuntu Pro

作業系統	版本	供應商安全建議
Ubuntu (Bionic)	18.04 (ESM)	USN, Ubuntu Pro
Ubuntu (Focal)	20.04 (LTS)	USN
Ubuntu (Jammy)	22.04 (LTS)	USN
Ubuntu (Mantic Minotaur)	23.10	USN

支援的程式設計語言：Amazon ECR 掃描

當掃描 Amazon ECR 儲存庫中的容器映像時，Amazon Inspector 目前支援下列程式設計語言：

- C#
- Go
- Java
- JavaScript
- PHP
- Python
- Ruby
- Rust

支援的執行階段：Amazon Inspector Lambda 標準

當掃描 Lambda 函數是否存在第三方軟體套件中的漏洞時，Amazon Inspector Lambda 標準掃描目前支援下列程式設

- Java
  - java8
  - java8.al2
  - java11
  - java17
- Node.js

  - nodejs12.x
  - nodejs14.x
  - nodejs16.x
  - nodejs18.x
  - nodejs20.x
- Python
  - python3.7
  - python3.8
  - python3.9
  - python3.10
  - python3.11
- Go
  - go1.x
- Ruby
  - ruby2.7
  - ruby3.2
- .NET
  - .NET 6

支援的執行階段：Amazon Inspector Lambda 程式

當掃描 Lambda 函數中的程式碼漏洞時，Amazon Inspector Lambda 程式碼掃描目前支援下列程式設計語言

- Java
  - java8
  - java8.al2
  - java11
  - java17
- Node.js
  - nodejs12.x

  - nodejs14.x
  - nodejs16.x
  - nodejs18.x
  - nodejs20.x
- Python
  - python3.7
  - python3.8
  - python3.9
  - python3.10
  - python3.11
- Ruby
  - ruby2.7
  - ruby3.2

停產的作業系統

廠商已停止對下表所列之作業系統的標準廠商支援。在表格中，「已停止」欄會指出廠商停止對作業系統的標準支援的時間。

Amazon Inspector 先前已為這些作業系統提供完整支援，並會繼續掃描執行這些作業系統的 Amazon EC2 執行個體和 Amazon ECR 容器映像檔。但是，根據供應商政策，操作系統不再使用修補程序進行更新，並且在許多情況下，不再為其發布新的安全建議。此外，某些廠商會在受影響的作業系統達到標準支援結束時，從其摘要中移除現有的安全性建議和偵測。因此，Amazon Inspector 可能會停止產生已知 CVE 的發現項目。Amazon Inspector 確實針對停止的作業系統產生的任何發現項目，都應該僅用於資訊目的。

作為安全性最佳實務，以及 Amazon Inspector 的持續涵蓋範圍，我們建議您移至目前受支援的作業系統版本。

已停產的作業系統：Amazon EC2 掃描

作業系統	版本	已停產
Amazon 亞馬遜	2012	2021年12月31 日

作業系統	版本	已停產
CentOS CentOS 版	8	2021年12月31 日
Debian 伺服器 (延伸)	9	2022 年 6 月 30 日
Fedora	35	2022 年 12 月 13 日
Fedora	36	2023 年 5 月 16 日
Fedora	37	2023 年 12 月 5 日
OpenSUSE	15.3	2022 年 12 月 1 日
OpenSUSE	15.4	2023 年 12 月 7 日
OpenSUSE 飛躍 (跳躍)	15.2	2021 年 12 月 1 日
甲骨文 Linux (甲骨文)	6	2021 年 3 月 1 日
SUSE Linux Enterprise Server (SLES)	12	2019 年 7 月 1 日
SUSE Linux Enterprise Server (SLES)	12.1	2020年5月31日
SUSE Linux Enterprise Server (SLES)	12.2	2021 年 3 月 31 日
SUSE Linux Enterprise Server (SLES)	12.3	2022 年 6 月 30 日
SUSE Linux Enterprise Server (SLES)	15	2019 年 12 月 31 日
SUSE Linux Enterprise Server (SLES)	15.1	2021年1月31日
SUSE Linux Enterprise Server (SLES)	15.2	2021年12月31 日

作業系統	版本	已停產
乌图坦	20.10	2021 年 7 月 22 日
Ubuntu（毛手）	21.04	2022 年 1 月 20 日
Ubuntu 的（英雄）	21.10	2022 年 7 月 31 日
Ubuntu (Kinetic)	22.10	July 20, 2023
Ubuntu (Lunar Lobster)	23.04	January 25, 2024
Windows Server	2012	2023 年 10 月 10 日
Windows Server	2012 R2	2023 年 10 月 10 日

已停產的作業系統：Amazon ECR 掃描

作業系統	版本	已停產
高山 Linux（高山）	3.12	2022 年 5 月 1 日
高山 Linux（高山）	3.13	2022 年 11 月 1 日
Alpine Linux (Alpine)	3.14	May 1, 2023
Alpine Linux (Alpine)	3.15	November 1, 2023
Amazon 亞馬遜	2012	2021年12月31 日
CentOS CentOS 版	8	2021年12月31 日
Debian 伺服器 (延伸)	9	2022 年 6 月 30 日
Fedora	35	2022 年 12 月 13 日
Fedora	36	2023 年 5 月 16 日
OpenSUSE	15.3	2022 年 12 月 1 日

作業系統	版本	已停產
OpenSUSE	15.4	December 7, 2023
OpenSUSE 飛躍 (跳躍)	15.2	2021 年 12 月 1 日
甲骨文 Linux (甲骨文)	6	2021 年 3 月 1 日
SUSE Linux Enterprise Server (SLES)	12	2019 年 7 月 1 日
SUSE Linux Enterprise Server (SLES)	12.1	2020年5月31日
SUSE Linux Enterprise Server (SLES)	12.2	2021 年 3 月 31 日
SUSE Linux Enterprise Server (SLES)	12.3	2022 年 6 月 30 日
SUSE Linux Enterprise Server (SLES)	15	2019 年 12 月 31 日
SUSE Linux Enterprise Server (SLES)	15.1	2021年1月31日
SUSE Linux Enterprise Server (SLES)	15.2	2021年12月31 日
乌图坦	20.10	2021 年 7 月 22 日
Ubuntu（毛手）	21.04	2022 年 1 月 20 日
Ubuntu 的（英雄）	21.10	2022 年 7 月 31 日
Ubuntu (Kinetic)	22.10	July 20, 2023
Ubuntu (Lunar Lobster)	23.04	January 25, 2024

停用 Amazon Inspector

您可以停用 Amazon Inspector 在任何 AWS 區域 通過使用 Amazon Inspector 控制台或 API。請依照本主題結尾的指示停用 Amazon Inspector。如果您停用所有的 Amazon Inspector 掃描 AWS 帳戶，Amazon Inspector 會自動停用此帳戶。如需停用不同資源的掃描類型的相關資訊，請參閱使用 Amazon Inspector 自動化資源。

停用某個帳戶的 Amazon Inspector 之後，該區域中該帳戶的所有掃描類型都會停用。此外，會刪除該區域中帳戶的所有 Amazon Inspector 掃描設定、抑制規則以及篩選器和發現項目。

您在該區域的帳戶停用時，使用 Amazon Inspector 不會收取任何費用。停用 Amazon Inspector 之後，您可以選擇稍後再重新啟用它。

> **Note**
>
> 停用 Amazon Inspector 之前，我們建議您匯出您的發現項目。如需詳細資訊，請參閱 從 Amazon Inspector 匯出發現報告。

當您停用 Amazon Inspector Amazon EC2 掃描時，亞馬 Amazon Inspector 使用的以下 SSM 關聯將被刪除：

- `InspectorDistributor-do-not-delete`
- `InspectorInventoryCollection-do-not-delete`
- `InvokeInspectorSsmPlugin-do-not-delete`。 此外，透過此關聯安裝的 Amazon Inspector SSM 外掛程式也會從所有Windows主機中移除。如需詳細資訊，請參閱 掃描Windows實例。

先決條件

根據您的帳戶類型，您可能需要採取其他步驟才能停用 Amazon Inspector，如下所示：

- 如果您擁有獨立的 Amazon Inspector 帳戶，您可以隨時將其停用。
- 如果您是 Amazon Inspector 多帳戶環境中的會員帳戶，則無法停用自己的服務。您必須連絡組織的委派管理員才能停用服務。
- 如果您是委派的管理員，您必須先取消所有成員帳戶的關聯，然後才能停用 Amazon Inspector。如需詳細資訊，請參閱 在 Amazon Inspector 中取消關聯會員帳戶。

> **Note**
>
> 取消關聯帳戶並不會停用該帳戶的 Amazon Inspector，而是取消關聯的成員帳戶會變成獨立帳戶。

> **Note**
>
> 當您以委派的管理員身分停用 Amazon Inspector 時，會停用組織的自動啟用功能。

停用 Amazon Inspector

Console

停用 Amazon Inspector

1. 打開 Amazon Inspector 控制台 https://console.aws.amazon.com/inspector/v2/home.
2. 使用頁面右上角的選 AWS 區域 取器，選擇您要停用 Amazon Inspector 的區域。
3. 在導覽窗格中，選擇 [一般設定]。
4. 選擇停用 Inspector。
5. 出現確認提示時，請在文字方塊中輸入停用，然後選擇 [停用 Inspector]。
6. (建議) 在您要停用 Amazon Inspector 的每個區域中重複這些步驟。

API

執行停用 API 作業。在請求中，提供您要停用的帳戶 ID，以及停`EC2`, `ECR`, `LAMBDA`和`resourceTypes`用所有掃描，這將停用該帳戶。

Amazon Inspector 的配額

您的 AWS 帳戶具有以下每個區域的 Amazon Inspector 配額。

資源	預設	說明
隱藏規則	500	每個區域每個 AWS 帳戶可儲存的最大隱藏規則數目。 您無法請求增加配額。
Amazon EC2 網路發現	10,000	每個 AWS 帳戶的 Amazon EC2 網路發現項目數目上限。 您無法請求增加配額。
成員帳戶	10000	與 Amazon Inspector 委派的管理員帳戶相關聯的成員帳戶數目上限。此限制是根據 AWS Organizations，請參閱 AWS Organizations。
CIS 掃描配置	500	CIS 掃描組態的最大數目。 您無法請求增加配額。

如需與 Amazon Inspector 經典版相關聯的配額清單，請參閱 AWS 一般參考.

如需與 Organizations 相關聯的配額清單，請參閱 AWS 一般參考.

區域與端點

亞馬遜 Amazon EC2 的亞馬遜檢查器無代理程式掃描正在預覽版本中。您使用無代理程式的 Amazon EC2 掃描功能須遵守AWS 服務條款第 2 節 (以下稱「試用版和預覽版」)。

若要檢視 Amazon Inspector 查器可用的 AWS 區域 位置，請參閱 Amazon Web Services 一般參考.

Amazon Inspector 掃描 API 的端點

下表顯示呼叫 Amazon Inspector 掃描 API 時可使用的區域端點。使用 API 時，您必須提供端點，並且它是您當前正在驗證的 AWS 區域的對應區域。

Amazon Inspector 掃描端點的命名慣例為`inspector-scan.region.amazonaws.com`。例如，如果您已在中驗證`us-west-2`，則可以使`inspector-scan.us-west-2.amazonaws.com`用端點呼叫 `inspector-scan` API。

區域名稱	區域	端點	通訊協定
美國東部 (俄亥俄)	us-east-2	檢查員掃描東部 2. 亞馬遜 inspector-scan-fips. 美東 2. 亞馬遜	HTTPS
美國東部 (維吉尼亞北部)	us-east-1	檢查員掃描東部-亞馬遜 inspector-scan-fips.us-east-1.amazonaws.com	HTTPS
美國西部 (加利佛尼亞北部)	us-west-1	檢查員掃描-西部-1. 亞馬遜 inspector-scan-fips. 美國西部-1. 亞馬遜	HTTPS

區域名稱	區域	端點	通訊協定
美國西部 (奧勒岡)	us-west-2	檢查員掃描西部 2. 亞馬遜 inspector-scan-fips.us-west-2.amazonaws.com	HTTPS
非洲 (開普敦)	af-south-1	檢查員掃描. AF-南部	HTTPS
亞太區域 (香港)	ap-east-1	檢查員掃描. AP-東-1. 亞馬遜	HTTPS
亞太區域 (雅加達)	ap-southeast-3	檢查員掃描. AP-東南部-3. 亞馬遜	HTTPS
亞太區域 (孟買)	ap-south-1	檢查員掃描南 1. 亞馬遜	HTTPS
亞太區域 (大阪)	ap-northeast-3	檢查員掃描 .pt-東北部-3. 亞馬遜	HTTPS
亞太區域 (首爾)	ap-northeast-2	檢查員掃描 .pt-東北部-2. 亞馬遜	HTTPS
亞太區域 (新加坡)	ap-southeast-1	檢查員掃描. AP-東南部-1. 亞馬遜	HTTPS
亞太區域 (悉尼)	ap-southeast-2	檢查員掃描 .pt-東南部 2. 亞馬遜	HTTPS
亞太區域 (東京)	ap-northeast-1	檢查員掃描 .pt-東北部-1. 亞馬遜	HTTPS
加拿大 (中部)	ca-central-1	檢查員掃描中央 1. 亞馬遜	HTTPS
歐洲 (法蘭克福)	eu-central-1	檢查員掃描歐盟-中央-1. 亞馬遜	HTTPS

區域名稱	區域	端點	通訊協定
歐洲 (愛爾蘭)	eu-west-1	檢查員掃描歐洲西部 -1. 亞馬遜	HTTPS
歐洲 (倫敦)	eu-west-2	檢查員掃描歐洲西部 2. 亞馬遜	HTTPS
歐洲 (米蘭)	eu-south-1	檢查員掃描歐盟南部 1. 亞馬遜	HTTPS
歐洲 (巴黎)	eu-west-3	檢查員掃描歐洲西部 3. 亞馬遜	HTTPS
歐洲 (斯德哥爾摩)	eu-north-1	檢查員掃描歐盟北部 1. 亞馬遜	HTTPS
歐洲 (蘇黎世)	eu-central-2	檢查員掃描歐盟中央 2. 亞馬遜	HTTPS
中東 (巴林)	me-south-1	檢查員掃描我南 1. 亞馬遜	HTTPS
南美洲 (聖保羅)	sa-east-1	檢查員掃描東部-1. 亞馬遜	HTTPS
AWS GovCloud (美國東部)	us-gov-east-1	檢查員掃描。 us-gov-east-1. 亞馬遜 inspector-scan-fips。 us-gov-east-1. 亞馬遜	HTTPS
AWS GovCloud (美國西部)	us-gov-west-1	檢查員掃描。 us-gov-west-1. 亞馬遜 inspector-scan-fips。 us-gov-west-1. 亞馬遜	HTTPS

區域特定功能的可用性

本節說明 Amazon Inspector 功能的可用性 AWS 區域。

適用於亞馬遜 EC2 區域的無代理 Amazon EC2 掃描

下表顯示目前可用於 Amazon EC2 的無代理程式掃描的 AWS 區域 位置。

區域名稱	區域代碼
美國東部 (維吉尼亞北部)	us-east-1
美國西部 (奧勒岡)	us-west-2
歐洲 (愛爾蘭)	eu-west-1

程 Lambda 碼掃描區域

下表顯示 Lambda 程式碼掃描目前可用的 AWS 區域 位置。

區域名稱	區域代碼
美國東部 (維吉尼亞北部)	us-east-1
美國西部 (奧勒岡)	us-west-2
美國東部 (俄亥俄)	us-east-2
亞太區域 (悉尼)	ap-southeast-2
亞太區域 (東京)	ap-northeast-1
歐洲 (法蘭克福)	eu-central-1
歐洲 (愛爾蘭)	eu-west-1
歐洲 (倫敦)	eu-west-2
歐洲 (斯德哥爾摩)	eu-north-1

區域名稱	區域代碼
亞太區域 (新加坡)	ap-southeast-1

AWS GovCloud (US) 地區

如需最新資訊，請參閱AWS GovCloud (US) 使用者指南中的 Amazon Inspector 查器。

Amazon Inspector 用戶指南的文檔歷史記錄

下表說明自上次發行 Amazon Inspector 以來文件的重要變更。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
已更新的功能	Amazon Inspector 將已關閉發現結果的保留期從 30 天更新為 7 天。如需詳細資訊，請參閱了解 Amazon Inspector 中的發現項目。	2024年2月12日
已更新的功能	Amazon Inspector 增加了一個新的聲明的AmazonInspector2ServiceRolePolicy政策。新的陳述式可讓 Amazon Inspector 為您的執行個體啟動獨聯體掃描。	2024 年 1 月 23 日
新政策	Amazon Inspector 新增了一個新的政AmazonInspector2ManagedCisPolicy策，即政策，您可以在執行個體設定檔中用來允許執行個體進行 CIS 掃描。	2024 年 1 月 23 日
新功能	當您提取容器映像時，Amazon Inspector 現在會重新整理容器映像的 ECR 重新掃描持續時間。若要根據推送或提取日期變更重新掃描持續時間，請參閱設定 ECR 重新掃描持續時間。	2024 年 1 月 23 日
新功能	Amazon Inspector 現在可以在 EC2 執行個體上執行網際	2024 年 1 月 23 日

	網路安全中心 (CIS) 掃描。如需詳細資訊，請參閱 Amazon Inspector CIS 掃描。	
新功能	Amazon Inspector 器現在可以掃描 CI/CD 管道中的容器映像。如需詳細資訊，請參閱與 Amazon Inspector 查器的 CI/CD 整合。	2023 年 11 月 30 日
新政策	Amazon Inspector 新增了一項新政策，允許 Amazon Inspector 從您的 EC2 執行個體掃描 Amazon EBS 快照，以進行無代理程式掃描。如需有關策略的詳細資訊，請參閱無代理程式掃描。	2023 年 11 月 27 日
新功能	Amazon Inspector 現在支援透過無代理程式掃描，無需使用 SSM 代理程式掃描支援 Linux Amazon EC2 執行個體 如需詳細資訊，請參閱無代理程式掃描。	2023 年 11 月 27 日
新的支援資源	Amazon Inspector 現在支持 MacOS Amazon EC2 實例的掃描。如需支援的 MacOS 版本，請參閱支援的作業系統：Amazon EC2 掃描。	2023 年 10 月 5 日
新區域	Amazon Inspector 現已在亞太區域 (雅加達)、非洲 (開普敦)、亞太區域 (大阪) 和歐洲 (蘇黎世) 推出。	2023 年 9 月 29 日

新功能	您現在可以使用排除標籤從 Amazon Inspector 掃描中排除 EC2 執行個體。	2023 年 9 月 14 日
新功能	Amazon Inspector 已新增許可，讓 Amazon Inspector 掃描屬於 Elastic Load Balancing 目標群組一部分之 Amazon EC2 執行個體的網路組態。	2023 年 8 月 31 日
新功能	Amazon Inspector 現在針對套件弱點發現的情報提供弱點情報詳細	2023 年 7 月 31 日
已更新的功能	Amazon Inspector 新增了新的許可，允許唯讀使用者匯出其資源的軟體材料清單 (SBOM)。	2023 年 6 月 29 日
新功能	您現在可以匯出 SBOM，以取得由 Amazon Inspector 掃描的資源。	2023 年 6 月 13 日
新功能	Lambda 程式碼掃描現已正式推出。已新增新功能，可讓您加密 Lambda 程式碼掃描發現項目中所識別的程式碼。此外，Lambda 程式碼掃描現在還提供建議的程式碼修正重寫功能。	2023 年 6 月 13 日
已更新的功能	Amazon Inspector 增加了一個新的聲明的AmazonInspector2ReadOnlyAccess政策。新的陳述式可讓唯讀使用者擷取其帳戶的 Lambda 程式碼掃描狀態和發現項目的詳細資訊。	2023 年 5 月 2 日

新功能	Amazon Inspector 查器增加了漏洞數據庫搜索，使您可以檢查 Amazon Inspector 查器是否涵蓋了特定的 CVE。	2023 年 5 月 1 日
已更新的功能	Amazon Inspector 已在AmazonInspector2ServiceRolePolicy政策中新增許可，讓 Amazon Inspector 在您啟用 Lambda 掃描時，在您的帳戶中建立 AWS CloudTrail 服務連結通道。這使 Amazon Inspector 器可以監控您帳戶中的 CloudTrail 事件。	2023年4月30日
已更新的功能	Amazon Inspector 增加了一個新的聲明的AmazonInspector2FullAccess政策。新的陳述式可讓使用者從 Lambda 程式碼掃描擷取發現的程式碼弱點詳細資訊。	2023 年 4 月 17 日
已更新的功能	Amazon Inspector 增加了一個新的聲明的AmazonInspector2ServiceRolePolicy政策。新的聲明允許亞馬遜檢查器將有關您為 Amazon EC2 深度檢查定義的自訂路徑的相關資訊傳送給 Amazon EC2 系統管理器。	2023 年 4 月 17 日
新功能	Amazon Inspector 以 Amazon Inspector 深度檢查的形式新增對 Linux EC2 執行個體的額外支援，可掃描執行個體是否存在應用程式程式設計語言套件中的套件漏洞。	2023 年 4 月 17 日

已更新的功能	Amazon Inspector 增加了一個新的聲明的AmazonInspector2ServiceRolePolicy政策。這些新陳述式可讓 Amazon Inspector 要求掃描 AWS Lambda 函式中的開發人員程式碼，並從 Amazon CodeGuru 安全接收掃描資料。此外，Amazon Inspector 已新增許可以檢閱 IAM 政策。Amazon Inspector 使用此資訊掃描 Lambda 函數是否存在程式碼漏洞	2023 年 2 月 28 日
新功能	Amazon Inspector 以 Lambda 程式碼掃描的形式新增對 Lambda 函數的額外支援，可掃描 Lambda 函數的開發人員程式碼是否存在安全漏洞。	2023 年 2 月 28 日
已更新的功能	Amazon Inspector 增加了一個新的聲明的AmazonInspector2ServiceRolePolicy政策。新陳述式可讓 Amazon Inspector 從上次呼叫 AWS Lambda 函數的時間擷取 CloudWatch 相關資訊。使用此資訊將重點掃描到您環境中過去 90 天內處於作用中狀態的 Lambda 函數。	2023 年 2 月 20 日

已更新的功能	Amazon Inspector 增加了一個新的聲明的AmazonInspector2ServiceRolePolicy政策。新的語句允許 Amazon Inspector 檢索有關您的 AWS Lambda 功能的信息。Amazon Inspector 使用此資訊掃描您的 Lambda 函數是否存在安全漏洞。	2022 年 11 月 28 日
新功能	Amazon Inspector 增加了對掃描 AWS Lambda 功能的支持	2022 年 11 月 28 日
已更新內容	新增將發現結果報告從 Amazon Inspector 匯出到 Amazon Simple Storage Service (Amazon S3) 儲存貯體的程序、政策範例和提示。	2022 年 10 月 14 日
新內容	已新增使用 Amazon Inspector 主控台評估您 AWS 環境的 Amazon Inspector 涵蓋範圍的相關資訊。此資訊包括環境中個別資源之狀態值的描述。	2022 年 10 月 7 日
新功能	Amazon Inspector 現在提供有關如何修復套件弱點的其他詳細資訊。新欄位已新增至尋找詳細資料。新欄位提供有關是否可透過套件更新取得修正程式的前後關聯。如果有可用的修正程式，發現項目的「建議的修正」區段會顯示您可以執行以進行修正的命令。	2022 年 9 月 2 日

已更新的功能	Amazon Inspector 增加了一個新的行動，以AmazonInspector2ServiceRolePolicy政策。這項新動作可讓 Amazon Inspector 描述 SSM 關聯執行。Amazon Inspector 也新增了額外的資源範圍設定，讓 Amazon Inspector 能夠使用`AmazonInspector2` 擁有的 SSM 文件建立、更新、刪除和啟動 SSM 關聯。	2022 年 8 月 31 日
新功能	Amazon Inspector 現在支援掃描Windows執行個體。Amazon Inspector 現在可以掃描執行支援Windows作業系統的 SSM 受管執行個體。Windows主機掃描是由 Amazon Inspector SSM 外掛程式執行，該外掛程式會透過 Amazon Inspector 自動建立的新 SSM 關聯進行安裝和叫用。	2022 年 8 月 31 日
已更新的功能	Amazon Inspector 更新了AmazonInspector2ServiceRolePolicy政策的資源範圍，以允許 Amazon Inspector 收集其他 AWS 分割區中的軟體庫存。	2022 年 8 月 12 日
已更新的功能	在這項AmazonInspector2ServiceRolePolicy政策中，Amazon Inspector 重新架構了動作的資源範圍，讓 Amazon Inspector 能夠建立、刪除和更新 SSM 關聯。	2022 年 8 月 10 日

新功能	Amazon Inspector 現在支援變更您的 ECR 自動重新掃描持續時間設定。Amazon ECR 自動重新掃描持續時間設定可決定 Amazon Inspector 持續監控推入儲存庫之影像的時間長度。當影像超過掃描持續時間時，Amazon Inspector 將不再掃描影像並關閉所有現有的發現項目。所有新帳戶的 ECR 自動重新掃描持續時間都會自動設定為存留期。先前建立的帳戶的 ECR 自動重新掃描持續時間為 30 天，但您現在可以選擇 30 天、180 天或終身期間進行掃描。	2022年6月25日
新功能	Amazon Inspector 新增了一個新的 AWS 受管政策，即該AmazonInspector2ReadOnlyAccess政策，允許對 Amazon Inspector 功能進行唯讀存取。	2022 年 1 月 21 日
一般可用性	這是 Amazon Inspector 使用者指南的初始公開發行版本。	2021 年 11 月 29 日

AWS 詞彙表

有關最新 AWS 術語，請參閱AWS 詞彙表 參考文獻中的AWS 詞彙表。

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。