使用者指南

Amazon Inspector Classic

版本 Latest

Amazon Inspector Classic: 使用者指南

Table of Contents

支援結束通知：2026 年 5 月 20 日， AWS 將結束對 Amazon Inspector Classic 的支援。2026 年 5 月 20 日之後，您將無法再存取 Amazon Inspector Classic 主控台或 Amazon Inspector Classic 資源。Amazon Inspector Classic 不再提供給過去 6 個月內未完成評估的新帳戶和帳戶。對於所有其他帳戶，存取將持續有效至 2026 年 5 月 20 日，之後您將無法再存取 Amazon Inspector Classic 主控台或 Amazon Inspector Classic 資源。如需詳細資訊，請參閱 Amazon Inspector Classic 終止支援。

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。

什麼是 Amazon Inspector Classic？

> **Note**
>
> 全新 Amazon Inspector 是 Amazon Inspector Classic 的完全重新設計版本，現已推出 AWS 區域。新的 Amazon Inspector 已擴展涵蓋範圍，除了 EC2 執行個體之外，還新增對 Amazon Elastic Container Registry (Amazon ECR) 中容器映像的支援。新的 Amazon Inspector 透過與的整合提供多帳戶支援 AWS Organizations，並根據常見漏洞和暴露 (CVEs) 持續進行軟體漏洞和網路連線能力掃描。我們鼓勵您探索和使用這些和其他全新和改善的功能，並受益於大幅增強的安全價值。若要了解新 Amazon Inspector 的功能和定價，請參閱 Amazon Inspector。若要了解如何移至新的 Amazon Inspector，請參閱 Amazon Inspector Classic 終止支援。

Amazon Inspector Classic 會測試 Amazon EC2 執行個體的網路可存取性，以及在這些執行個體上執行之應用程式的安全狀態。Amazon Inspector Classic 會評估應用程式是否有暴露、漏洞和與最佳實務的偏差。執行評估後，Amazon Inspector Classic 會產生詳細的安全調查結果清單，並依嚴重性等級進行組織。

使用 Amazon Inspector Classic，您可以自動化整個開發和部署管道或靜態生產系統的安全漏洞評估。如此一來，安全測試就可成為開發和 IT 操作中的定期作業。

Amazon Inspector Classic 也提供稱為 代理程式的預先定義軟體，您可以選擇性地將其安裝在您要評估的 EC2 執行個體作業系統中。代理程式會監控 EC2 執行個體的行為，包括網路、檔案系統和程序活動。也會收集各種行為和組態資料 (遙測)。

> **Important**
>
> AWS 不保證遵循提供的建議將解決每個潛在的安全問題。Amazon Inspector Classic 產生的調查結果取決於您在每個評估範本中包含的規則套件選擇、系統中是否存在非AWS 元件，以及其他因素。您有責任確保在 AWS 服務上執行之應用程式、程序和工具的安全。如需詳細資訊，請參閱安全共同AWS 責任模型。

> **Note**
>
> AWS 負責保護執行 AWS 雲端所提供服務的 全球基礎設施。此基礎設施包含執行 AWS 服務的硬體、軟體、聯網和設施。 AWS 提供多個第三方稽核人員的報告，這些稽核人員已驗證我們是否符合各種電腦安全標準和法規。如需詳細資訊，請參閱AWS 雲端合規。

如需 Amazon Inspector Classic 術語的相關資訊，請參閱 Amazon Inspector Classic 術語和概念。

Amazon Inspector Classic 的優點

以下是 Amazon Inspector Classic 的一些主要優點：

- 將自動化安全檢查整合到您的常規部署和生產程序中 – 評估 AWS 資源的安全性，以用於鑑識、疑難排解或主動稽核目的。在開發過程中執行評估，或在穩定生產環境中執行評估。
- 尋找應用程式安全問題 – 自動化應用程式的安全評估，並主動識別漏洞。如此即可快速開發並反覆測試新的應用程式，並評估是否符合最佳實務和政策。
- 深入了解您的 AWS 資源 – 透過檢閱 Amazon Inspector Classic 產生的調查結果，隨時掌握 AWS 資源的活動和組態資料。

Amazon Inspector Classic 的功能

以下是 Amazon Inspector Classic 的一些主要功能：

- 組態掃描和活動監控引擎 – Amazon Inspector Classic 提供可分析系統和資源組態的代理程式。也會監控活動，判斷評估目標的外觀、其行為及其相依元件。此遙測的組合提供目標的全貌及其潛在安全或合規性問題。
- 內建內容程式庫 – Amazon Inspector Classic 包含內建的規則和報告程式庫。其中會檢查是否符合最佳實務、常見的合規標準及是否有漏洞。這些檢查包括解決潛在安全問題的詳細建議步驟。
- 透過 API 自動化 – Amazon Inspector Classic 可以透過 API 完全自動化。這可讓您將安全測試融入開發和設計程序中，包括選取、執行和報告這些測試的結果。

存取 Amazon Inspector Classic

您可以透過下列任何方式使用 Amazon Inspector Classic 服務：

Amazon Inspector Classic 主控台

登入 AWS Management Console 並開啟位於 https：//https://console.aws.amazon.com/inspector/ 的 Amazon Inspector Classic 主控台。

主控台是瀏覽器型界面，可讓您存取和使用 Amazon Inspector Classic 服務。

AWS SDKs

AWS 提供軟體開發套件 SDKs)，其中包含適用於各種程式設計語言和平台的程式庫和範本程式碼。例如 Java、Python、Ruby、.NET、iOS、Android 等。SDKs提供便捷的方式來建立 Amazon Inspector Classic 服務的程式設計存取。如需 AWS SDKs 的相關資訊，包括如何下載和安裝，請參閱適用於 Amazon Web Services 的工具。

Amazon Inspector Classic HTTPS API

您可以使用 Amazon Inspector Classic HTTPS API 以 AWS 程式設計方式存取 Amazon Inspector Classic，這可讓您直接向服務發出 HTTPS 請求。如需詳細資訊，請參閱 Amazon Inspector Classic API 參考。

AWS 命令列工具

您可以使用 AWS 命令列工具在系統的命令列執行命令，以執行 Amazon Inspector Classic 任務。如果您想要建置執行 AWS 任務的指令碼，命令列工具也很有用。如需詳細資訊，請參閱 Amazon Inspector Classic AWS Command Line Interface。

Amazon Inspector Classic 術語和概念

當您開始使用 Amazon Inspector Classic 時，您可以從了解其關鍵概念中獲益。

Amazon Inspector Classic 代理程式

您可以在包含在評估目標中的 EC2 執行個體上安裝的軟體代理程式。代理程式會收集各種組態資料 (遙測)。如需詳細資訊，請參閱Amazon Inspector Classic 代理程式。

評估執行

透過分析您的評估目標的組態並與指定的規則套件進行比對，以發現潛在安全問題的探索程序。在評估執行期間，Amazon Inspector 會監控、收集和分析指定目標內資源的組態資料 (遙測)。Amazon Inspector 接著會分析資料，並針對評估執行期間使用之評估範本所指定的一組安全規則套件，進行比較。完成的評估執行會產生調查結果清單，其中指出各種嚴重程度的潛在安全問題。如需詳細資訊，請參閱Amazon Inspector Classic 評估範本和評估執行。

評估目標

在 Amazon Inspector Classic 的背景下，AWS 資源的集合，可做為一個單位共同運作，協助您實現業務目標。Amazon Inspector Classic 會評估構成評估目標之資源的安全狀態。

> **Important**
>
> 目前，您的 Amazon Inspector Classic 評估目標只能包含 EC2 執行個體。如需詳細資訊，請參閱 Amazon Inspector Classic 服務限制

若要建立 Amazon Inspector Classic 評估目標，您必須先使用您選擇的鍵值對來標記 EC2 執行個體。接下來，您可以建立具有常見金鑰或常見值的這些已標記 EC2 執行個體的檢視。如需詳細資訊，請參閱Amazon Inspector Classic 評估目標。

評估範本

評估執行期間使用的組態。範本包括以下項目：

- Amazon Inspector Classic 用來評估評估評估目標的規則套件
- 您希望 Amazon Inspector Classic 傳送評估執行狀態和調查結果通知的 Amazon Amazon SNS 主題
- 標記 (索引鍵/值組)，可指派給評估執行產生的調查結果
- 評估執行的持續時間

問題清單

Amazon Inspector Classic 在指定目標的評估執行期間發現的潛在安全問題。調查結果會顯示在 Amazon Inspector Classic 主控台中，或透過 API 擷取。其中包含安全問題的詳細描述及建議的修正方法。如需詳細資訊，請參閱Amazon Inspector Classic 調查結果。

規則

在 Amazon Inspector Classic 的內容中，評估執行期間執行的安全性檢查。當規則偵測到潛在的安全問題時，Amazon Inspector Classic 會產生描述問題的調查結果。

規則套件

在 Amazon Inspector Classic 的內容中，是規則的集合。規則套件對應至您可能有的安全目標。您可以在建立 Amazon Inspector Classic 評估範本時，選取適當的規則套件來指定您的安全目標。如需詳細資訊，請參閱Amazon Inspector Classic 規則套件和規則。

遙測

已安裝 EC2 執行個體的套件資訊和軟體組態。Amazon Inspector Classic 會在評估執行期間收集資料。

Amazon Inspector Classic 服務限制

下表顯示 AWS 帳戶的 Amazon Inspector Classic 限制。

> **Important**
>
> 目前，您的 評估目標只能由 EC2 執行個體組成。

以下是每個區域每個 AWS 帳戶的 Amazon Inspector Classic 限制：

資源	預設限制	說明
執行中評估的執行個體	500	每個區域每個帳戶的所有執行中評估中可包含的 EC2 執行個體數量上限。
評估執行	50000	每個區域的每個帳戶可建立的評估執行數量上限。您可以擁有多個同時發生的評估執行，只要用於這些執行的評估目標不包含重疊的 EC2 執行個體。
評估範本	500	無論何時，您在每個區域的每個帳戶中可以具有的評估範本數量上限。

資源	預設限制	說明
評估目標	50	無論何時，您在每個區域的每個帳戶中可以具有的評估目標數量上限。

除非另有說明，否則可以透過聯絡 AWS 支援 中心，根據請求提高這些限制。

Amazon Inspector Classic 定價

Amazon Inspector Classic 定價是根據每個評估中包含的 EC2 執行個體數量，以及這些評估中使用的規則套件。

網路連線能力規則套件的定價

具有網路連線能力規則套件的 Amazon Inspector Classic 評估會按每個評估（執行個體評估）每月每個執行個體定價。例如，如果您對 1 個執行個體執行 1 個評估，即 1 個執行個體評估。如果您針對 10 個執行個體執行 1 個評估，即 10 個執行個體評估。定價從每月每個執行個體評估 0.15 USD 開始，磁碟區折扣可達到每月每個執行個體評估 0.04 USD。

免費試用詳細資訊

使用 Amazon Inspector Classic 的前 90 天	每個執行個體評估價格
First 250 instance-assessments	$0.00

定價詳情

在指定月份	每個執行個體評估價格
First 250 instance-assessments	$0.15
Next 750 instance-assessments	$0.13
Next 4,000 instance-assessments	$0.10

在指定月份	每個執行個體評估價格
Next 45,000 instance-assessments	$0.07
All other instance-assessments	$0.04

主機評估規則套件的定價

對於評估中包含的常見漏洞與暴露 (CVE)、網際網路安全中心 (CIS) 基準、安全最佳實務和執行期行為分析的任意組合

Amazon Inspector Classic 的主機評估規則套件使用部署在執行您要評估之應用程式的 Amazon EC2 執行個體上的代理程式。具有主機規則套件的評估會按每個代理程式每月評估（代理程式評估）定價。例如，如果您對 1 個代理程式執行 1 個評估，即 1 個代理程式評估。如果您針對 10 個客服人員執行 1 個評估，即 10 個客服人員評估。定價從每月每次客服人員評估 0.30 USD 開始，數量折扣可達到每月每次客服人員評估 0.05 USD。

免費試用詳細資訊

使用 Amazon Inspector Classic 的前 90 天	每個客服人員評估價格
First 250 agent-assessments	$0.00

定價詳情

在指定月份	每個客服人員評估價格
First 250 agent-assessments	$0.30
Next 750 agent-assessments	$0.25
Next 4,000 agent-assessments	$0.15
Next 45,000 agent-assessments	$0.10
All other agent-assessments	$0.05

Amazon Inspector Classic 支援的作業系統和區域

本章提供有關 Amazon Inspector Classic 支援的作業系統和 AWS 區域的資訊。

> **Important**
>
> 目前，Amazon Inspector Classic 評估目標只能包含 EC2 執行個體。無論作業系統為何，您都可以在任何 EC2 執行個體上使用 Network Reachability 規則套件執行無代理程式評估。

如需跨支援作業系統提供之 Amazon Inspector Classic 規則套件的相關資訊，請參閱 支援作業系統的 Amazon Inspector Classic 規則套件。

主題

Amazon Inspector Classic 代理程式支援的 Linux 作業系統

您可以在 64 位元 x86 和 Arm EC2 執行個體上使用 Amazon Inspector Classic 代理程式。代理程式與下列 Linux 作業系統版本相容：

- 64 位元 x86 執行個體
  - Amazon Linux 2
  - Amazon Linux (2018.03、2017.09、2017.03、2016.09、2016.03、2015.09、2015.03、2014.09、2014.03、2013.09、
  - Ubuntu (20.04 LTS、18.04 LTS、16.04 LTS、14.04 LTS)
  - Debian (10.x、9.0 - 9.5、8.0 - 8.7)
  - Red Hat Enterprise Linux (8.x、7.2、6.2 - 6.9)
  - CentOS (7.2 - 7.x、6.2 - 6.9)
- Arm 執行個體
  - Amazon Linux 2
  - Red Hat Enterprise Linux (7.6 - 7.x)
  - Ubuntu (18.04 LTS、16.04 LTS)

Amazon Inspector Classic 代理程式支援的 Windows 作業系統

您只能在執行下列 Windows 作業系統 64 位元版本的 EC2 執行個體上使用 Amazon Inspector Classic 代理程式：

- Windows Server 2019 Base
- Windows Server 2016 Base
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

支援的 AWS 區域

下列 AWS 區域支援 Amazon Inspector Classic：

- 美國東部 (俄亥俄) us-east-2
- 美國東部 (維吉尼亞北部) us-east-1
- 美國西部 (加利佛尼亞北部) us-west-1
- 美國西部 (奧勒岡) us-west-2
- 亞太區域 (孟買) ap-south-1
- 亞太區域 (首爾) ap-northeast-2
- 亞太區域 (雪梨) 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
- AWS GovCloud （ 美國東部 ） gov-us-east-1
- AWS GovCloud （ 美國西部 ） gov-us-west-1

> **Note**
>
> Network Reachability 規則套件不適用於 AWS GovCloud (US) 區域。

Amazon Inspector Classic 終止支援

在仔細考慮之後，我們決定終止對 Amazon Inspector Classic 的支援，自 2026 年 5 月 20 日起生效。自 2025 年 5 月 20 日起，Amazon Inspector Classic 將不再接受新客戶。身為在 2025 年 5 月 20 日之前註冊服務的現有客戶，您可以繼續使用 Amazon Inspector Classic 功能。2026 年 5 月 20 日之後，您將無法再使用 Amazon Inspector Classic。

新的 Amazon Inspector 現已在全球推出 AWS 區域。新的 Amazon Inspector 是已完全重新設計的現有 Amazon Inspector 版本，現在稱為 Amazon Inspector Classic。以下是 Amazon Inspector 主要增強功能：

- 專為擴展而打造 – 新的 Amazon Inspector 專為擴展和動態雲端環境而打造。帳戶中可以掃描的執行個體或映像數量沒有限制。
- 支援容器映像 – 新的 Amazon Inspector 也會掃描 Amazon Elastic Container Registry (Amazon ECR) 中的容器映像是否有軟體漏洞。
- 支援多帳戶管理 – 新的 Amazon Inspector 已與 Organizations 整合。這可讓您從組織委派 Amazon Inspector 的管理員帳戶。委派管理員帳戶是集中式帳戶，可合併所有調查結果，並可設定所有成員帳戶。
- 使用 AWS Systems Manager 代理程式 (SSM 代理程式） – 透過新的 Amazon Inspector，您不再需要在所有 EC2 執行個體上安裝和維護獨立的 Amazon Inspector 代理程式。新的 Amazon Inspector 會利用廣泛部署的 SSM 代理程式。
- 自動化和持續掃描 – 使用 Amazon Inspector Classic，您可以手動設定評估目標、評估範本，以及設定評估的頻率。不過，新版本的 Amazon Inspector 會自動偵測所有新啟動的 EC2 執行個體和推送至 Amazon ECR 的合格容器映像，並立即掃描它們是否有軟體漏洞和意外的網路暴露。資源會根據數個觸發條件自動重新掃描，包括啟動的新 EC2 執行個體、推送至 Amazon ECR 的容器映像、在 EC2 執行個體中安裝新套件、安裝修補程式，或發佈會影響資源的新常見漏洞與暴露 (CVE)。
- Amazon Inspector 風險分數 – 新的 Amazon Inspector 會計算 Amazon Inspector 風險分數，以協助排定問題清單的優先順序。風險分數是透過將up-to-date CVE 資訊與暫時和環境因素相互關聯來計算，例如網路可存取性和可利用性資訊。
- 更多整合 – 所有調查結果都會彙總在新設計的 Amazon Inspector 主控台中，並推送到 AWS Security Hub 和 Amazon EventBridge 以自動化工作流程，例如票證。容器映像相關的調查結果也會推送到 Amazon ECR。

若要了解新 Amazon Inspector 的所有功能和定價，請參閱 Amazon Inspector 使用者指南。

雖然我們將持續支援 Amazon Inspector Classic 一段時間，而且客戶可以在同一個帳戶中同時使用新的 Amazon Inspector 和 Amazon Inspector Classic，但我們強烈建議您遷移到新的 Amazon Inspector。以下各節將逐步引導您從 Amazon Inspector Classic 移至新的 Amazon Inspector。

主題

步驟 1：（選用）匯出評估報告和調查結果

若要在 Amazon Inspector Classic 中儲存評估報告和調查結果，請產生評估報告。

產生評估報告

1. 在 Assessment runs (評估執行) 頁面，找出您想要產生報告的評估執行。請確定其狀態為分析完成。
2. 在 Reports (報告) 欄下方選擇此次評估執行的報告圖示。

   > **Important**
   >
   > 只有 2017 年 4 月 25 日後的評估執行 (不論是否已完成)，Reports (報告) 欄中才會出現報告圖示。此時，Amazon Inspector Classic 中的評估報告便可供使用。

3. 在評估報告對話方塊中，選擇您要檢視的報告類型 (調查結果報告或完整報告） 和報告格式 (HTML 或 PDF)。接著選擇 Generate report (產生報告)。

步驟 2：刪除 Amazon Inspector Classic 中的所有排程評估執行

若要停用 Amazon Inspector Classic，請刪除所有作用中帳戶中的所有評估範本 AWS 區域。刪除評估範本會停止所有排定的未來評估執行。

刪除評估範本

- 在 Assessment Templates (評估範本) 頁面，選擇您要刪除的範本，然後選擇 Delete (刪除)。出現確認提示時，請選擇 Yes (是)。

> **Important**
>
> 當您刪除評估範本時，與此範本相關的所有評估執行、發現項目與報告版本也會刪除。

步驟 3：啟用新的 Amazon Inspector

您可以使用 AWS Management Console 或新的 Amazon Inspector APIs 來啟用新的 Amazon Inspector。若要開始使用新的 Amazon Inspector，請參閱《Amazon Inspector 使用者指南》中的入門。

Amazon Inspector Classic 入門

本教學課程說明如何設定 Amazon Inspector Classic，並開始建立和執行您的第一次評估。

一鍵設定

下列程序說明如何在目前 和 中所有可用的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體上使用預先建置的範本和預先定義的排程參數（每週一次或僅限一次）建立 AWS 帳戶 和執行自動評估 AWS 區域。

1. 登入 AWS Management Console 並開啟 Amazon Inspector Classic 主控台，網址為 https://console.aws.amazon.com/inspector/：//。
2. 在 Welcome (歡迎) 頁面上，選擇您要執行的評估類型。網路評估會分析您 AWS 環境的網路組態是否有漏洞，且不需要 Amazon Inspector Classic 代理程式。主機評估會分析 EC2 執行個體的主機上軟體和組態是否有漏洞，並要求在 EC2 執行個體上安裝代理程式。

   選擇 Run weekly (recommended) (每週執行 (建議)) 或 Run once (執行一次)。一旦您選擇完畢，該服務會自動為您建立評估。具體而言，該服務會執行下列作業：

   a. 建立服務連結角色。

      > **Note**
      >
      > 若要識別評估目標中指定的 EC2 執行個體，Amazon Inspector Classic 需要列舉您的 EC2 執行個體和標籤。Amazon Inspector Classic 可透過名為 的服務連結角色存取 AWS 帳戶 中的這些資源`AWSServiceRoleForAmazonInspector`。如需服務連結角色的詳細資訊，請參閱使用 Amazon Inspector Classic 的服務連結角色與使用服務連結角色。

   b. 如果適用，會在您 AWS 帳戶 和 區域中所有可用的 EC2 執行個體上安裝 Amazon Inspector Classic 代理程式。

      > **Note**
      >
      > 此服務只會在允許 AWS Systems Manager 執行命令的 EC2 執行個體上安裝 Amazon Inspector Classic 代理程式。若要使用此選項，請確定目前 中的所有 EC2 執行個體 AWS 帳戶 AWS 區域 已安裝 SSM Agent，且具有允許執行命令的 IAM 角

色。如需詳細資訊，請參閱使用 Systems Manager Run Command 在多個 EC2 執行個體上安裝代理程式。

c. 新增這些執行個體到評估目標。

d. 使用標準化規則套件，在評估範本中包含該目標。

e. 您可以選擇 Run weekly (每週執行，建議) 或 Run once (執行一次)，以決定每週執行一次評估，還是僅執行一次。

3. 在確認對話方塊中，選擇確定。Amazon Inspector Classic 會自動執行您的評估。

進階設定

下列程序說明如何選擇要包含在評估目標和範本中的特定 Amazon EC2 執行個體、規則套件和排程參數。

1. 在 Welcome (歡迎) 頁面上，選擇 Advanced setup (進階設定)。
2. 在 Define an assessment target (定義評估目標) 頁面上，輸入評估目標的名稱。
3. 對於所有執行個體，您可以保持選取核取方塊，以在評估目標中包含您 AWS 帳戶 和 區域中的所有 EC2 執行個體。如果您想要選擇要包含的 EC2 執行個體，請清除所有執行個體核取方塊，然後輸入與目標 EC2 執行個體相關聯的金鑰和值標籤。如需標記 EC2 執行個體的詳細資訊，請參閱標記您的 Amazon EC2 資源。
4. 對於安裝代理程式，如果您的執行個體允許 System Manager Run Command，您可以保留預設選取的核取方塊。服務會在允許評估目標中的所有 EC2 執行個體上安裝 Amazon Inspector Classic 代理程式 AWS Systems Manager。若要使用此選項，請確定目前 中的所有 EC2 執行個體 AWS 帳戶 AWS 區域 已安裝 SSM 代理程式，且具有允許執行命令的 IAM 角色。如需詳細資訊，請參閱使用 Systems Manager Run Command 在多個 EC2 執行個體上安裝代理程式。若要手動安裝代理程式，請參閱安裝 Amazon Inspector 代理程式。
5. 選擇 Next (下一步)。
6. 在 Define an assessment template (定義評估範本) 頁面上，輸入評估範本的名稱。
7. 針對 Rules packages (規則套件)，請選擇要包含在評估範本的規則套件。如需規則套件的詳細資訊，請參閱 Amazon Inspector 規則套件和規則。
8. 針對 Duration (期間)，選擇評估執行的期間。
9. （選用）針對評估排程，設定週期性評估執行的排程。
10. 選擇 Next (下一步)。

11. 在 Review (檢閱) 頁面，您可以檢閱對評估目標及範本的選擇。如果您對組態感到滿意，請選擇建立。如果您為評估範本設定評估排程，則在您選擇 Create (建立) 之後會自動執行評估。

> **Note**
>
> 若要識別評估目標中指定的 EC2 執行個體，Amazon Inspector Classic 需要列舉您的 EC2 執行個體和標籤。Amazon Inspector Classic AWS 帳戶 可透過名為 的服務連結角色存取 中的這些資源`AWSServiceRoleForAmazonInspector`。如需在 Amazon Inspector Classic 中使用服務連結角色的詳細資訊，請參閱 使用 Amazon Inspector Classic 的服務連結角色。如需使用服務連結角色的詳細資訊，請參閱AWS Identity and Access Management 《 使用者指南》中的使用服務連結角色。

12. 如果您未設定評估排程，請在主控台導覽至您的評估範本，然後選擇 Run (執行)。
13. 若要追蹤評估執行的進度，請在主控台的導覽窗格選擇 Assessment runs (評估執行)，然後選擇 Findings (問題清單)。如需問題清單的詳細資訊，請參閱 Amazon Inspector Classic 調查結果。

Amazon Inspector Classic 教學課程

下列教學課程說明如何在 Red Hat Enterprise Linux 和 Ubuntu 作業系統上執行 Amazon Inspector Classic 評估。

教學課程

- 教學課程：搭配 Red Hat Enterprise Linux 使用 Amazon Inspector Classic
- 教學課程：搭配 Ubuntu Server 使用 Amazon Inspector Classic

Amazon Inspector Classic 教學課程 - Red Hat Enterprise Linux

在您遵循此教學課程中的指示之前，建議您先熟悉 Amazon Inspector Classic 術語和概念。

本教學課程說明如何使用 Amazon Inspector Classic 來分析執行 Red Hat Enterprise Linux 7.5 作業系統的 EC2 執行個體的行為。它提供如何導覽 Amazon Inspector Classic 工作流程的step-by-step說明。工作流程包括準備 Amazon EC2 執行個體、執行評估範本，以及執行評估調查結果中產生的建議安全修正。如果您是第一次使用 ，並且想要一鍵設定和執行 Amazon Inspector Classic 評估，請參閱建立基本評估。

主題

- 步驟 1：設定要與 Amazon Inspector Classic 搭配使用的 Amazon EC2 執行個體 Amazon Inspector
- 步驟 2：修改您的 Amazon EC2 執行個體
- 步驟 3：建立評估目標，並在 EC2 執行個體上安裝代理程式
- 步驟 4：建立和執行評估範本
- 步驟 5：尋找並分析調查結果
- 步驟 6：套用建議修復至您的評估目標

步驟 1：設定要與 Amazon Inspector Classic 搭配使用的 Amazon EC2 執行個體 Amazon Inspector

在本教學課程中，建立一個執行 Red Hat Enterprise Linux 7.5 的 EC2 執行個體，並使用名稱金鑰和值來標記它。 **`InspectorEC2InstanceLinux`**

> **Note**
>
> 如需標記 EC2 執行個體的詳細資訊，請參閱資源與標籤。

步驟 2：修改您的 Amazon EC2 執行個體

在本教學課程中，您會修改目標 EC2 執行個體，使其公開至潛在的安全問題 CVE-2018-1111。如需詳細資訊，請參閱 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1111 和 常見的漏洞和風險。

在已連接至執行個體 **InspectorEC2InstanceLinux** 的情況下，執行下列命令。

```
sudo yum install dhclient-12:4.2.5-68.el7
```

如需如何連線至 EC2 執行個體的指示，請參閱《Amazon EC2 使用者指南》中的連線至您的執行個體。

步驟 3：建立評估目標，並在 EC2 執行個體上安裝代理程式

Amazon Inspector Classic 使用評估目標來指定您要評估的 AWS 資源。

若要建立評估目標，並在 EC2 執行個體上安裝代理程式

1. 登入 AWS Management Console ，並在 https://console.aws.amazon.com/inspector/：// 開啟 Amazon Inspector Classic 主控台。
2. 在導覽窗格中選擇 Assessment targets (評估目標)，然後選擇 Create (建立)。

   請執行下列操作：

   a. 在 Name (名稱) 中輸入您評估目標的名稱。

      針對本教學，輸入 **MyTargetLinux**。

   b. 對於使用標籤，輸入索引鍵和值欄位的值，選擇您要包含在此評估目標中的 EC2 執行個體。

      在此教學課程中，**Name**請在金鑰欄位中輸入 ，然後在值欄位中輸入 ，以選擇您在上一個步驟**InspectorEC2InstanceLinux**中建立的 EC2 執行個體。

      若要將您 AWS 帳戶及區域所有的 EC2 執行個體納入評估目標，請選取 All Instances (所有執行個體) 核取方塊。

c. 選擇 Save (儲存)。

d. 在已標記的 EC2 執行個體上安裝 Amazon Inspector Classic 代理程式。若要在評估目標中所有 EC2 執行個體上安裝代理程式，請選取 Install Agents (安裝代理程式) 核取方塊。

> **Note**
>
> 您也可以使用 AWS Systems Manager Run Command 安裝 Amazon Inspector Classic 代理程式。若要在評估目標中所有執行個體上安裝代理程式，您可指定用於建立評估目標的相同標記。或者，您可以在 EC2 執行個體上手動安裝 Amazon Inspector Classic 代理程式。如需詳細資訊，請參閱安裝 Amazon Inspector Classic 代理程式。

e. 選擇 Save (儲存)。

> **Note**
>
> 此時，Amazon Inspector Classic 會建立名為 的服務連結角色`AWSServiceRoleForAmazonInspector`。此角色會授予 Amazon Inspector Classic 存取資源的必要存取權。如需詳細資訊，請參閱為 Amazon Inspector Classic 建立服務連結角色。

步驟 4：建立和執行評估範本

建立和執行範本

1. 在導覽窗格中，選擇 Assessment templates (評估範本)，然後選擇 Create (建立)。
2. 針對 Name (名稱)，請輸入評估範本的名稱。針對本教學，輸入 **`MyFirstTemplateLinux`**。
3. 在 Target name (目標名稱) 部分，選擇您之前建立的評估目標 (**`MyTargetLinux`**)。
4. 針對 Rules packages (規則套件)，請選擇要在此評估範本中使用的規則套件。

   在此教學課程中，請選擇 Common Vulnerabilities and Exposures-1.1。
5. 在 Duration (持續時間)，指定評估範本的持續時間。

   在此教學課程中，選擇 15 minutes (15 分鐘)。
6. 選擇 Create and run (建立並執行)。

步驟 5：尋找並分析調查結果

已完成的評估執行會產生一組調查結果，或 Amazon Inspector Classic 在評估目標中發現的潛在安全問題。您可以檢閱問題清單並依照建議步驟解決潛在安全問題。

在此教學課程中，如果完成了先前的步驟，您的評估執行就會對照通用漏洞 CVE-2018-1111 產生一份問題清單。

尋找並分析調查結果

1. 在導覽窗格中，選擇 Assessment runs (評估執行)。驗證名為 MyFirstTemplateLinux 的評估範本執行狀態是設定為 Collecting data (收集資料)。這表示評估執行正在進行中，而目標的遙測資料正根據所選規則套件收集與分析。
2. 當評估執行仍在進行中，您就無法檢視由評估執行產生的問題清單。請讓評估執行完成整段持續時間。然而，在此教學課程中，您可以於幾分鐘後停止執行。

   MyFirstTemplateLinux 的狀態會先變更為 Stopping (正在停止)，接著在幾分鐘內變更為 Analyzing (正在分析)，最後是 Analysis complete (分析完成)。要查看狀態的變更，請選擇 Refresh (重新整理) 圖示。
3. 在導覽窗格中，選擇調查結果。

   您可以看到具有 High (高) 嚴重性的新調查結果，稱為 Instance InspectorEC2InstanceLinux is vulnerable to CVE-2018-1111 (執行個體 InspectorEC2InstanceLinux 具有 CVE-2018-1111 的漏洞)。

   > **Note**
   >
   > 如果您未看到新的問題清單，請選擇 Refresh (重新整理) 圖示。

   要展開檢視並查看此問題清單的詳細資訊，請選擇問題清單左側的箭頭。問題清單的詳細資訊包含下列項目：

   - 調查結果的 ARN
   - 產生此調查結果的評估執行名稱
   - 產生此調查結果的評估目標名稱
   - 產生此調查結果的評估範本名稱
   - 評估執行開始時間

- 評估執行結束時間
- 評估執行狀態
- 包含觸發此問題清單之規則的規則套件名稱
- Amazon Inspector Classic 代理程式 ID
- 問題清單名稱
- 問題清單嚴重性
- 問題清單的描述
- 您可以完成這些建議步驟，以修正調查結果所描述的潛在安全問題

步驟 6：套用建議修復至您的評估目標

在此教學課程中，您已修改評估目標，將其暴露於潛在安全問題 CVE-2018-1111。在此程序中，您可以為此問題套用建議修正。

將修正套用到您的目標

1. 連接至您在前一節建立的執行個體 **InspectorEC2InstanceLinux**，並執行以下命令：

   ```
   sudo yum update dhclient-12:4.2.5-68.el7
   ```

2. 在 Amazon templates (Amazon 範本) 頁面，選擇 MyFirstTemplateLinux (MyFirstTemplateLinux)，接著選擇 Run (執行) 使用此範本開始新的評估執行。
3. 遵循 步驟 5：尋找並分析調查結果 中的步驟，以查看 MyFirstTemplateLinux 範本後續執行所產生的結果。

   由於您已解決 CVE-2018-1111 安全問題，因此您不應再看到問題清單。

Amazon Inspector Classic 教學課程 - Ubuntu 伺服器

在您遵循此教學課程中的指示之前，建議您先熟悉 Amazon Inspector Classic 術語和概念。

本教學課程說明如何使用 Amazon Inspector Classic 來分析執行 Ubuntu Server 16.04 LTS 作業系統的 EC2 執行個體的行為。它提供如何導覽 Amazon Inspector Classic 工作流程的step-by-step說明。

如果您是第一次使用 ，並且想要一鍵設定和執行 Amazon Inspector Classic 評估，請參閱建立基本評估。

主題

步驟 1：設定要與 Amazon Inspector Classic 搭配使用的 Amazon EC2 執行個體 Amazon Inspector

設定 EC2 執行個體

- 在本教學課程中，建立一個執行 Ubuntu Server 16.04 LTS 的 EC2 執行個體，並使用名稱金鑰和值來標記**InspectorEC2InstanceUbuntu**它。

> **Note**
>
> 如需標記 EC2 執行個體的詳細資訊，請參閱資源與標籤。

步驟 2：建立評估目標，並在 EC2 執行個體上安裝代理程式

Amazon Inspector Classic 使用評估目標來指定要評估的 AWS 資源。

建立評估目標，並在 EC2 執行個體上安裝 代理程式

1. 登入 AWS Management Console 並開啟 Amazon Inspector Classic 主控台，網址為 https://console.aws.amazon.com/inspector/：//。
2. 在導覽窗格中選擇 Assessment targets (評估目標)，然後選擇 Create (建立)。
3. 在 Name (名稱) 中輸入您評估目標的名稱。

   針對本教學課程，請輸入 **MyTargetUbuntu**。
4. 對於使用標籤，輸入索引鍵和值欄位的值，選擇您想要在此評估目標中包含的 EC2 執行個體。

   在此教學課程中，請在金鑰欄位中輸入 ，然後在值欄位中輸入 **Name**，以選擇您在上一個步驟**InspectorEC2InstanceUbuntu**中建立的 EC2 執行個體。

勾選All instances (所有執行個體)方塊，納入評估目標中 AWS 帳戶及區域的所有 EC2 執行個體。

5. 在已標記的 EC2 執行個體上安裝 Amazon Inspector Classic Agent。若要在評估目標中包含 EC2 執行個體上安裝代理程式，請選取 Install Agents (安裝代理程式) 方塊。

> **Note**
>
> 您亦可使用 Systems Manager Run Command 安裝 Amazon Inspector 代理程式。要在評估目標中的所有執行個體上安裝代理程式，您可以指定用於建立評估目標的相同標籤。或者，您可以手動在 EC2 執行個體上安裝 Amazon Inspector Agent。如需詳細資訊，請參閱安裝 Amazon Inspector Classic 代理程式。

6. 選擇 Save (儲存)。

> **Note**
>
> 此時，`AWSServiceRoleForAmazonInspector`會建立名為 的服務連結角色，以授予 Amazon Inspector Classic 存取您的 資源。如需詳細資訊，請參閱為 Amazon Inspector Classic 建立服務連結角色。

步驟 3：建立和執行您的評估範本

建立和執行範本

1. 如果您使用 Advanced setup (進階設定)，系統會將您導向 Define an assessment template (定義評估範本) 頁面。否則，請導覽至 Assessment templates (評估範本) 頁面，然後選擇 Create (建立)。
2. 針對 Name (名稱)，請輸入評估範本的名稱。針對本教學，輸入 **`MyFirstTemplateUbuntu`**。
3. 在 Target name (目標名稱) 部分，選擇您之前建立的評估目標 (**`MyTargetUbuntu`**)。
4. 針對 Rules packages (規則套件)，請使用下拉式功能表，選擇您要在此評估範本中使用的規則套件。

   在此教學課程中，請選擇 Common Vulnerabilities and Exposures-1.1。
5. 在 Duration (持續時間)，指定評估範本的持續時間。

   在此教學課程中，選擇 15 minutes (15 分鐘)。

6. 如果您使用的是 Advanced setup (進階設定)，請選擇 Next (下一步)。在以下 Review (審查) 頁面，選擇 Create function (建立函數)。否則請選擇 Create and run (建立並執行)。

步驟 4：尋找和分析產生的調查結果

已完成的評估執行會產生一組調查結果，或 Amazon Inspector Classic 在評估目標中發現的潛在安全問題。您可以檢閱問題清單並依照建議步驟解決潛在安全問題。

1. 導覽到 Assessment Runs (評估執行) 頁面。驗證名為 MyFirstTemplateUbuntu 的評估範本 (您在前述步驟中建立) 執行狀態是設定為 Collecting data (收集資料)。這表示評估執行正在進行中，而目標的遙測資料正根據所選規則套件收集與分析。
2. 當評估執行仍在進行中，您就無法檢視由評估執行產生的問題清單。請讓評估執行完成整段持續時間。

   MyFirstTemplateUbuntu 的狀態會先變更為 Stopping (正在停止)，接著在幾分鐘內變更為 Analyzing (正在分析)，最後是 Analysis complete (分析完成)。要查看狀態的變更，請選擇 Refresh (重新整理) 圖示。
3. 瀏覽至 Findings (調查結果) 頁面。

   若要展開檢視並查看調查結果的詳細資訊，請選擇調查結果左側的箭頭。問題清單的詳細資訊包含下列項目：

   - 調查結果的 ARN
   - 產生此調查結果的評估執行名稱
   - 產生此調查結果的評估目標名稱
   - 產生此調查結果的評估範本名稱
   - 評估執行開始時間
   - 評估執行結束時間
   - 評估執行狀態
   - 規則套件的名稱，其中包含觸發調查結果的規則
   - Amazon Inspector Classic 代理程式 ID
   - 問題清單名稱
   - 問題清單嚴重性
   - 問題清單的描述
   - 您可以完成這些建議步驟，以修正調查結果所描述的潛在安全問題

步驟 5：將建議的修正套用至您的評估目標

在此程序中，您會套用更新來修正未發現的問題。

1. 連線至您的執行個體 **InspectorEC2InstanceUbuntu**，並執行套件更新。
2. 在 Assessment templates (評估範本) 頁面，選擇 MyFirstTemplateUbuntu，然後選擇 Run (執行)，以使用此範本開始新的執行。
3. 遵循 步驟 4：尋找和分析產生的調查結果 中的步驟，以查看 MyFirstTemplateUbuntu 範本後續執行所產生的調查結果。

   套件更新應該已解決範本第一次執行時的調查結果。

Amazon Inspector Classic 的安全性

的雲端安全性 AWS 是最高優先順序。身為 AWS 客戶，您可以受益於資料中心和網路架構，這些架構是為了符合最安全敏感組織的需求而建置。

安全性是 AWS 與您之間的共同責任。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：

- 雲端的安全性 – AWS 負責保護在 AWS Cloud 中執行 AWS 服務的基礎設施。 AWS 也為您提供可安全使用的服務。在AWS 合規計劃中，第三方稽核人員會定期測試和驗證我們安全的有效性。若要了解適用於 Amazon Inspector Classic 的合規計劃，請參閱合規計劃的 AWS 服務範圍。
- 雲端的安全性 – 您的責任取決於您使用 AWS 的服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件可協助您了解如何在使用 Amazon Inspector Classic 時套用共同責任模型。下列主題說明如何設定 Amazon Inspector Classic 以符合您的安全與合規目標。您也會了解如何使用其他 AWS 服務來協助您監控和保護 Amazon Inspector Classic 資源。

主題

Amazon Inspector Classic 中的資料保護

AWS 共同責任模型適用於 Amazon Inspector Classic 中的資料保護。如此模型所述， AWS 負責保護執行所有 的 全球基礎設施 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，我們建議您保護 AWS 帳戶 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授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用 設定 API 和使用者活動記錄 AWS CloudTrail。如需有關使用 CloudTrail 追蹤擷取 AWS 活動的資訊，請參閱AWS CloudTrail 《 使用者指南》中的使用 CloudTrail 追蹤。
- 使用 AWS 加密解決方案，以及其中的所有預設安全控制 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 AWS 透過命令列界面或 API 存取 時需要 FIPS 140-3 驗證的密碼編譯模組，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) 140-3。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用 Amazon Inspector Classic 或使用 AWS 服務 主控台、API AWS CLI或其他 AWS SDKs 時。您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

主題

靜態資料加密

Amazon Inspector Classic 代理程式在評估執行期間產生的遙測資料會以 JSON 檔案格式化。這些檔案會透過 TLS near-real-time的方式交付至 Amazon Inspector Classic，並在其中使用per-assessment-run的暫時性 AWS KMS衍生金鑰進行加密。

檔案會安全地存放在專用於 Amazon Inspector Classic 的 S3 儲存貯體中。Amazon Inspector Classic 的規則引擎會執行下列動作：

- 存取 S3 儲存貯體中加密的遙測資料

- 在記憶體中將其解密
- 根據設定的評估規則處理資料，以產生問題清單

加密傳輸中的資料

Amazon Inspector Classic 是受管服務，受到 AWS 全球網路安全的保護。如需 AWS 安全服務以及 如何 AWS 保護基礎設施的相關資訊，請參閱AWS 雲端安全。若要使用基礎設施安全的最佳實務設計您的 AWS 環境，請參閱安全支柱 AWS Well-Architected Framework 中的基礎設施保護。

您可以使用 AWS 發佈的 API 呼叫，透過網路存取 Amazon Inspector Classic。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 Classic 的 Identity and Access Management

AWS Identity and Access Management (IAM) 是一種 AWS 服務 ，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可控制誰可以進行身分驗證 （登入） 和授權 （具有許可） 來使用 Amazon Inspector 資源。IAM 是 AWS 服務 您可以免費使用的 。

主題

- ABAC 搭配 Amazon Inspector
- 搭配 Amazon Inspector 使用臨時憑證
- Amazon Inspector 的跨服務主體許可
- Amazon Inspector 的服務角色
- Amazon Inspector 的服務連結角色
- Amazon Inspector Classic 的身分型政策範例
- 使用 Amazon Inspector Classic 的服務連結角色
- 對 Amazon Inspector Classic 身分和存取進行故障診斷

目標對象

您使用 AWS Identity and Access Management (IAM) 的方式會有所不同，取決於您在 Amazon Inspector 中執行的工作。

服務使用者 – 如果您使用 Amazon Inspector 服務執行任務，您的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 功能來執行工作時，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。如果您無法存取 Amazon Inspector 中的功能，請參閱 對 Amazon Inspector Classic 身分和存取進行故障診斷。

服務管理員 – 如果您在公司負責 Amazon Inspector 資源，您可能擁有 Amazon Inspector 的完整存取權。您的任務是判斷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搭配 Amazon Inspector 使用 IAM，請參閱 Amazon Inspector Classic 如何與 IAM 搭配使用。

IAM 管理員 – 如果您是 IAM 管理員，建議您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 Classic 的身分型政策範例。

使用身分驗證

身分驗證是您 AWS 使用身分憑證登入 的方式。您必須以 AWS 帳戶根使用者身分、IAM 使用者身分或擔任 IAM 角色來驗證 （ 登入 AWS)。

您可以使用透過身分來源提供的登入資料，以聯合身分 AWS 身分身分登入 。 AWS IAM Identity Center (IAM Identity Center) 使用者、您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。當您使用聯合 AWS 身分存取 時，您會間接擔任角色。

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

如果您以 AWS 程式設計方式存取 ， AWS 會提供軟體開發套件 (SDK) 和命令列界面 (CLI)，以使用您的 憑證以密碼編譯方式簽署您的請求。如果您不使用 AWS 工具，則必須自行簽署請求。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》中的適用於 API 請求的AWS Signature 第 4 版。

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 建議您使用多重驗證 (MFA) 來提高帳戶的安全性。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 IAM 中的AWS 多重要素驗證。

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，該身分可完整存取帳戶中的所有 AWS 服務 和資源。此身分稱為 AWS 帳戶 Theroot 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

根據最佳實務， 要求人類使用者，包括需要管理員存取權的使用者，使用 聯合身分提供者 AWS 服務來使用臨時憑證來存取 。

聯合身分是來自您的企業使用者目錄、Web 身分提供者、 AWS Directory Service、 Identity Center 目錄或任何使用透過身分來源提供的登入資料 AWS 服務 存取的使用者。當聯合身分存取時 AWS 帳戶，它們會擔任 角色，而角色會提供臨時登入資料。

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，也可以連接並同步到您自己的身分來源中的一組使用者 AWS 帳戶 和群組，以便在所有 和應用程式中使用。如需 IAM Identity Center 的詳細資訊，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 中的身分 AWS 帳戶 ，具有單一人員或應用程式的特定許可。建議您盡可能依賴臨時憑證，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，但角色僅提供臨時憑證。如需更多資訊，請參閱《IAM 使用者指南》中的 IAM 使用者的使用案例。

IAM 角色

IAM 角色是 中具有特定許可 AWS 帳戶 的身分。它類似 IAM 使用者，但不與特定的人員相關聯。若要暫時在 中擔任 IAM 角色 AWS Management Console，您可以從使用者切換至 IAM 角色（主控台）。您可以透過呼叫 AWS CLI 或 AWS API 操作或使用自訂 URL 來擔任角色。如需使用角色的方法詳細資訊，請參閱《IAM 使用者指南》中的擔任角色的方法。

使用臨時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並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 (聯合) 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 (信任的主體) 存取您帳戶的資源。角色是授予跨帳戶存取權的主要方式。不過，在某些 中 AWS 服務，您可以將政策直接連接到資源（而不是使用角色做為代理）。如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 中的跨帳戶資源存取。
- 跨服務存取 – 有些 AWS 服務 使用其他 中的功能 AWS 服務。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。
  - 轉送存取工作階段 (FAS) – 當您使用 IAM 使用者或角色在其中執行動作時 AWS，您會被視為委託人。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 使用呼叫 的委託人許可 AWS 服務，結合 AWS 服務 請求向下游服務提出請求。只有當服務收到需要與

其他 AWS 服務 或 資源互動才能完成的請求時，才會提出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。

- 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。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以委派許可權給 AWS 服務。
- 服務連結角色 – 服務連結角色是一種連結至 的服務角色類型 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 中 AWS 帳戶 ，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

- 在 Amazon EC2 上執行的應用程式 – 您可以使用 IAM 角色來管理在 EC2 執行個體上執行之應用程式的臨時登入資料，以及提出 AWS CLI 或 AWS API 請求。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 執行個體並將其提供給其所有應用程式，您可以建立連接至執行個體的執行個體描述檔。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臨時憑證。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM 角色來授予許可權給 Amazon EC2 執行個體上執行的應用程式。

使用政策管理存取權

您可以透過建立政策並將其連接到身分或資源 AWS 來控制 AWS 中的存取。政策是 中的物件，當與身分或資源建立關聯時， AWS 會定義其許可。當委託人 （使用者、根使用者或角色工作階段） 發出請求時， 會 AWS 評估這些政策。政策中的許可決定是否允許或拒絕請求。大多數政策會以 JSON 文件 AWS 的形式存放在 中。如需 JSON 政策文件結構和內容的詳細資訊，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。具有該政策的使用者可以從 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。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管政策是獨立的政策，您可以連接到 中的多個使用者、群組和角色 AWS 帳戶。受管政策包括 AWS 受管政策和客戶受管政策。如需了解如何在受管政策及內嵌政策之間選擇，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。委託人可以包含帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

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

存取控制清單 (ACL)

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

Amazon S3 AWS WAF和 Amazon VPC 是支援 ACLs的服務範例。如需進一步了解 ACL，請參閱 Amazon Simple Storage Service 開發人員指南中的存取控制清單 (ACL) 概觀。

其他政策類型

AWS 支援其他較不常見的政策類型。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。如需許可界限的詳細資訊，請參閱 IAM 使用者指南中的 IAM 實體許可界限。
- 服務控制政策 SCPs) – SCPs是 JSON 政策，可指定 中組織或組織單位 (OU) 的最大許可 AWS Organizations。 AWS Organizations 是一種服務，用於分組和集中管理您企業擁有 AWS 帳戶 的多個 。若您啟用組織中的所有功能，您可以將服務控制政策 (SCP) 套用到任何或所有帳戶。SCP 會限制成員帳戶中實體的許可，包括每個實體 AWS 帳戶根使用者。如需 Organizations 和 SCP 的詳細資訊，請參閱《AWS Organizations 使用者指南》中的服務控制政策。
- 資源控制政策 (RCP) - RCP 是 JSON 政策，可用來設定您帳戶中資源的可用許可上限，採取這種方式就不需要更新附加至您所擁有的每個資源的 IAM 政策。RCP 會限制成員帳戶中資源的許

可，並可能影響身分的有效許可，包括 AWS 帳戶根使用者，無論它們是否屬於您的組織。如需 Organizations 和 RCPs的詳細資訊，包括 AWS 服務 支援 RCPs 清單，請參閱AWS Organizations 《 使用者指南》中的資源控制政策 (RCPs)。

- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過撰寫程式的方式建立角色或聯合使用者的暫時工作階段時，做為參數傳遞。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。如需詳細資訊，請參閱 IAM 使用者指南中的工作階段政策。

多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。若要了解如何 AWS 在涉及多個政策類型時決定是否允許請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

Amazon Inspector Classic 如何與 IAM 搭配使用

在您使用 IAM 管理 Amazon Inspector 的存取權之前，請先了解哪些 IAM 功能可與 Amazon Inspector 搭配使用。

您可以搭配 Amazon Inspector Classic 使用的 IAM 功能

IAM 功能	Amazon Inspector 支援
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

IAM 功能	Amazon Inspector 支援
服務角色	否
服務連結角色	是

若要全面了解 Amazon Inspector 和其他 AWS 服務如何與大多數 IAM 功能搭配使用，請參閱《IAM 使用者指南》中的AWS 與 IAM 搭配使用的 服務。

Amazon Inspector 的身分型政策

支援身分型政策：是

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。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

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 的身分型政策範例

若要檢視 Amazon Inspector 身分型政策的範例，請參閱 Amazon Inspector Classic 的身分型政策範例。

Amazon Inspector 中的資源型政策

支援資源型政策：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。委託人可以包括帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

如需啟用跨帳戶存取權，您可以指定在其他帳戶內的所有帳戶或 IAM 實體，做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。當委託人和資源位於不同位置時 AWS 帳戶，信任帳戶中的 IAM 管理員也必須授予委託人實體 （使用者或角色） 存取資源的許可。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 中的快帳戶資源存取。

Amazon Inspector 的政策動作

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。政策動作通常具有與相關聯 AWS API 操作相同的名稱。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 Inspector 動作的清單，請參閱《服務授權參考》中的 Amazon Inspector Classic 定義的動作。

Amazon Inspector 中的政策動作在動作之前使用以下字首：

```
inspector
```

若要在單一陳述式中指定多個動作，請用逗號分隔。

```
"Action": [
      "inspector:action1",
      "inspector:action2"
         ]
```

下列許可政策授權使用者執行開頭為 `Describe` 和 `List` 的所有操作。這些操作會顯示 Amazon Inspector 資源的相關資訊，例如評估目標或調查結果。`Resource` 元素中的萬用字元 (*) 表示允許對帳戶擁有的所有 Amazon Inspector 資源執行操作：

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

```
            "inspector:Describe*",
            "inspector:List*"
            ],
         "Resource":"*"
      }
   ]
}
```

範例 2：允許使用者僅在 Amazon Inspector 調查結果上執行描述和列出操作

下列許可政策只授權使用者執行 `ListFindings` 和 `DescribeFindings` 操作。這些操作會顯示 Amazon Inspector 調查結果的相關資訊。`Resource` 元素中的萬用字元 (*) 表示允許對帳戶擁有的所有 Amazon Inspector 資源執行操作。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action": [
                  "inspector:DescribeFindings",
                  "inspector:ListFindings"
         ],
         "Resource":"*"
      }
   ]
}
```

若要檢視 Amazon Inspector 身分型政策的範例，請參閱 Amazon Inspector Classic 的身分型政策範例。

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 ARNs，請參閱《服務授權參考》中的 Amazon Inspector Classic 定義的資源。若要了解您可以使用哪些動作指定每個資源的 ARN，請參閱 Amazon Inspector Classic 定義的動作。

若要檢視 Amazon Inspector 身分型政策的範例，請參閱 Amazon Inspector Classic 的身分型政策範例。

Amazon Inspector 的政策條件索引鍵

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， 會使用邏輯OR操作 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的條件金鑰。若要查看所有 AWS 全域條件索引鍵，請參閱《IAM 使用者指南》中的AWS 全域條件內容索引鍵。

若要查看 Amazon Inspector 條件索引鍵的清單，請參閱《服務授權參考》中的 Amazon Inspector Classic 的條件索引鍵。若要了解您可以使用條件金鑰的動作和資源，請參閱 Amazon Inspector Classic 定義的動作。

若要檢視 Amazon Inspector 身分型政策的範例，請參閱 Amazon Inspector Classic 的身分型政策範例。

Amazon Inspector 中的 ACLs

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 搭配 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。您可以將標籤連接至 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。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，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》中的使用 ABAC 授權定義許可。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)。

搭配 Amazon Inspector 使用臨時憑證

支援臨時憑證：是

當您使用臨時登入資料登入時，有些 AWS 服務 無法運作。如需詳細資訊，包括哪些 AWS 服務 使用臨時登入資料，請參閱《AWS 服務 IAM 使用者指南》中的 使用 IAM。

如果您 AWS Management Console 使用使用者名稱和密碼以外的任何方法登入 ，則會使用臨時登入資料。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取 時，該程序會自動建立臨時登入資料。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》中的從使用者切換至 IAM 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，您會被視為委託人。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 使用呼叫 的委託人許可 AWS 服務，結合 AWS 服務 請求向下游服務提出請求。只有當服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會提出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱轉發存取工作階段。

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。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以委派許可權給 AWS 服務。

> **Warning**
>
> 變更服務角色的許可可能會中斷 Amazon Inspector 功能。只有在 Amazon Inspector 提供指引時，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

服務連結角色是連結至 的一種服務角色 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 中 AWS 帳戶 ，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需建立或管理 Amazon Inspector 服務連結角色的詳細資訊，請參閱 使用 Amazon Inspector Classic 的服務連結角色。

Amazon Inspector Classic 的身分型政策範例

根據預設，使用者和角色沒有建立或修改 Amazon Inspector 資源的許可。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 來執行任務。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。

如需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 (主控台)。

如需 Amazon Inspector 定義的動作和資源類型的詳細資訊，包括每種資源類型的 ARNs 格式，請參閱《服務授權參考》中的 Amazon Inspector Classic 的動作、資源和條件索引鍵。

主題

- 政策最佳實務
- 使用 Amazon Inspector 主控台
- 允許使用者檢視他們自己的許可
- 允許使用者僅在 Amazon Inspector 調查結果上執行描述和列出操作

政策最佳實務

身分型政策會判斷您帳戶中的某個人員是否可以建立、存取或刪除 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 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用將許可授予許多常見使用案例的 AWS 受管政策。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，以進一步減少許可。如需更多資訊，請參閱 IAM 使用者指南中的 AWS 受管政策或任務職能的AWS 受管政策。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。如果透過特定 例如 使用服務動作 AWS 服務，您也可以使用條件來授予其存取權 AWS CloudFormation。如需詳細資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：條件。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您撰寫安全且實用的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM Access Analyzer 驗證政策。
- 需要多重要素驗證 (MFA) – 如果您的案例需要 IAM 使用者或 中的根使用者 AWS 帳戶，請開啟 MFA 以提高安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需詳細資訊，請參閱《IAM 使用者指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_configure-api-require.html中的透過 MFA 的安全 API 存取。

如需 IAM 中最佳實務的相關資訊，請參閱 IAM 使用者指南中的 IAM 安全最佳實務。

使用 Amazon Inspector 主控台

若要存取 Amazon Inspector Classic 主控台，您必須擁有一組最低許可。這些許可必須允許您列出和檢視 中 Amazon Inspector 資源的詳細資訊 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。

對於僅呼叫 AWS CLI 或 AWS API 的使用者，您不需要允許最低主控台許可。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，也請將 Amazon Inspector *ConsoleAccess*或*ReadOnly* AWS 受管政策連接到實體。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。此政策包含在主控台或使用 或 AWS CLI AWS API 以程式設計方式完成此動作的許可。

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

```
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

允許使用者僅在 Amazon Inspector 調查結果上執行描述和列出操作

下列許可政策只授權使用者執行 `ListFindings` 和 `DescribeFindings` 操作。這些操作會顯示 Amazon Inspector 調查結果的相關資訊。`Resource` 元素中的萬用字元 (*) 表示允許對帳戶擁有的所有 Amazon Inspector 資源執行操作。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action": [
                  "inspector:DescribeFindings",
                  "inspector:ListFindings"
         ],
         "Resource":"*"
      }
   ]
}
```

使用 Amazon Inspector Classic 的服務連結角色

Amazon Inspector Classic 使用 AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結至 Amazon Inspector Classic 的獨特 IAM 角色類型。服務連結角色是由 Amazon Inspector Classic 預先定義，並包含服務 AWS 服務 代表您呼叫其他 所需的所有許可。

服務連結角色可讓您更輕鬆地設定 Amazon Inspector Classic，因為您不需要手動新增必要的許可。Amazon Inspector Classic 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 Classic 可以擔任其角色。定義的許可包括信任政策和許可政策，且該許可政策無法附加至其他 IAM 實體。

您必須先刪除角色的相關資源，才能刪除服務連結角色。這可保護您的 Amazon Inspector Classic 資源，因為您不會不小心移除存取資源的許可。

如需有關支援服務連結角色的其他 服務的資訊，請參閱AWS 服務連結角色欄中適用於 IAM 的服務，並尋找具有是的服務。 選擇具有連結的是，以檢視該服務的服務連結角色文件。

Amazon Inspector Classic 的服務連結角色許可

Amazon Inspector Classic 使用名為 AWSServiceRoleForAmazonInspector – ServiceLinkedRoleDescription 的服務連結角色。

AWSServiceRoleForAmazonInspector 服務連結角色信任下列服務擔任該角色：

- `inspector.amazonaws.com`

名為 AmazonInspectorServiceRolePolicy 的角色許可政策允許 Amazon Inspector Classic 對指定的資源完成下列動作：

- 動作：`arn:aws:iam::*:role/aws-service-role/inspector.amazonaws.com/AWSServiceRoleForAmazonInspector` 上的 `iam:CreateServiceLinkedRole`

您必須設定許可，以允許 IAM 實體 （例如 IAM 使用者、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。

為 Amazon Inspector Classic 建立服務連結角色

您不需要手動建立一個服務連結角色。當您在 AWS Management Console、 AWS CLI或 AWS API 中 CompleteThisCreateActionInThisService 時，Amazon Inspector Classic 會為您建立服務連結角色。

編輯 Amazon Inspector Classic 的服務連結角色

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

刪除 Amazon Inspector Classic 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。然而，在手動刪除服務連結角色之前，您必須先清除資源。

> **Note**
>
> 如果您嘗試刪除資源時，Amazon Inspector Classic 服務正在使用 角色，則刪除可能會失敗。若此情況發生，請等待數分鐘後並再次嘗試操作。

刪除 使用的 Amazon Inspector Classic 資源 **AWSServiceRoleForAmazonInspector**

- 在您執行 Amazon Inspector Classic 的所有 AWS 帳戶 AWS 區域 中刪除對此的評估目標。如需詳細資訊，請參閱Amazon Inspector Classic 評估目標。

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台 AWS CLI、 或 AWS API 來刪除 AWSServiceRoleForAmazonInspector 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 Classic 服務連結角色支援的區域

Amazon Inspector Classic 支援在提供服務的所有區域中使用服務連結角色。如需詳細資訊，請參閱 AWS 區域與端點。

對 Amazon Inspector Classic 身分和存取進行故障診斷

使用以下資訊來協助您診斷和修正使用 Amazon Inspector 和 IAM 時可能遇到的常見問題。

主題

- 我無權在 Amazon Inspector 中執行動作
- 我未獲得執行 iam:PassRole 的授權
- 我想要允許 以外的人員 AWS 帳戶 存取我的 Amazon Inspector 資源

我無權在 Amazon Inspector 中執行動作

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 inspector:*GetWidget* 許可時發生。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 inspector: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 inspector:*GetWidget* 動作存取 *my-example-widget* 資源。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我未獲得執行 iam:PassRole 的授權

如果您收到錯誤，告知您無權執行 iam:PassRole動作，您的政策必須更新，以允許您將角色傳遞給 Amazon Inspector。

有些 AWS 服務 可讓您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

當名為 的 IAM marymajor 使用者嘗試使用主控台在 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 管理員。您的管理員提供您的簽署憑證。

我想要允許 以外的人員 AWS 帳戶 存取我的 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 是否支援這些功能，請參閱 Amazon Inspector Classic 如何與 IAM 搭配使用。
- 若要了解如何在您擁有 AWS 帳戶 的 資源之間提供存取權，請參閱《IAM 使用者指南》中的在您擁有 AWS 帳戶 的另一個 IAM 使用者中提供存取權。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱《IAM 使用者指南》中的將存取權提供給第三方 AWS 帳戶 擁有。
- 如需了解如何透過聯合身分提供存取權，請參閱 IAM 使用者指南中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。

- 如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 中的跨帳戶資源存取。

在 Amazon Inspector Classic 中記錄和監控

Amazon Inspector Classic 已與 服務整合 AWS CloudTrail，此服務提供使用者、角色或 AWS 服務在 Amazon Inspector Classic 中採取之動作的記錄。CloudTrail 會將 Amazon Inspector Classic 的所有 API 呼叫擷取為事件，包括來自 Amazon Inspector Classic 主控台的呼叫，以及對 Amazon Inspector Classic API 操作的程式碼呼叫。

如需在 Amazon Inspector Classic 中使用 CloudTrail 記錄的資訊，請參閱 使用 記錄 Amazon Inspector Classic API 呼叫 AWS CloudTrail。

您可以使用 Amazon CloudWatch 監控 Amazon Inspector Classic，它會收集原始資料並將其處理為可讀且幾近即時的指標。 Amazon CloudWatch 根據預設，Amazon Inspector Classic 會在 5 分鐘內將指標資料傳送至 CloudWatch。

如需搭配 Amazon Inspector Classic 使用 CloudWatch 的詳細資訊，請參閱 使用 Amazon CloudWatch 監控 Amazon Inspector Classic Amazon CloudWatch。

Amazon Inspector Classic 中的事件回應

Amazon Inspector Classic 的事件回應是 AWS 的責任。 AWS 具有正式、記錄的政策和計劃，可管理事件回應。

AWS 具有廣泛影響的操作問題會張貼在AWS 服務運作狀態儀表板上。

系統也會透過 AWS Health Dashboard，將操作問題張貼至個別帳戶。如需如何使用 的資訊 AWS Health Dashboard，請參閱 AWS Health 使用者指南。

Amazon Inspector Classic 的合規驗證

在多個合規計畫中，第三方稽核人員會評估 Amazon Inspector Classic 的安全性和 AWS 合規性。這些計劃包括 SOC、PCI、FedRAMP、HIPAA 等等。

如需特定合規計劃範圍內 AWS 的服務清單，請參閱合規計劃範圍內的 AWS 服務。如需一般資訊，請參閱 AWS Compliance Programs。

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

您使用 Amazon Inspector Classic 時的合規責任取決於資料的機密性、您公司的合規目標，以及適用的法律和法規。 AWS 提供下列資源來協助合規：

- 安全與合規快速入門指南：這些部署指南討論架構考量，並提供在 AWS上部署以安全及合規為重心之基準環境的步驟。
- Amazon Web Services 上的 HIPAA 安全與合規架構 – 本白皮書說明公司如何使用 AWS 來建立符合 HIPAA 規範的應用程式。
- AWS 合規資源 – 此工作手冊和指南的集合可能適用於您的產業和位置。
- 《 AWS Config 開發人員指南》中的使用規則評估資源 – AWS Config 服務會評估資源組態符合內部實務、產業準則和法規的程度。
- AWS Security Hub – AWS 此服務提供 內安全狀態的全方位檢視 AWS ，可協助您檢查是否符合安全產業標準和最佳實務。

Amazon Inspector Classic 中的彈性

AWS 全球基礎設施是以 AWS 區域和可用區域為基礎建置。 AWS 區域提供多個實體隔離和隔離的可用區域，這些區域以低延遲、高輸送量和高度備援的網路連接。透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域和可用區域的詳細資訊，請參閱 AWS 全球基礎設施。

Amazon Inspector Classic 具有高可用性，並使用跨多個可用區域的運算資源來執行查詢。如果無法連線特定的可用區域，它會自動適當地路由查詢。

Amazon Inspector Classic 使用 Amazon S3 作為其基礎資料存放區，讓您的資料具有高度可用性和耐用性。Amazon S3 提供耐用的基礎設施來存放重要資料。其設計提供 99.999999999% 的物件持久性。您的資料會以冗餘方式存放在多個設施以及每個設施的多個裝置。

Amazon Inspector Classic 中的基礎設施安全性

Amazon Inspector Classic 是受管服務，受到 AWS 全球網路安全的保護。如需 AWS 安全服務以及 如何 AWS 保護基礎設施的相關資訊，請參閱AWS 雲端安全。若要使用基礎設施安全的最佳實務來設計您的 AWS 環境，請參閱安全支柱 AWS Well-Architected Framework 中的基礎設施保護。

您可以使用 AWS 發佈的 API 呼叫，透過網路存取 Amazon Inspector Classic。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。

如需 Amazon Inspector Classic 網路和代理程式安全性的詳細資訊，請參閱 the section called “網路和 Amazon Inspector Classic 代理程式安全性”。

Amazon Inspector Classic 中的組態和漏洞分析

Amazon Inspector Classic 提供稱為 代理程式的預先定義軟體，您可以選擇性地安裝在您要評估的 EC2 執行個體作業系統中。代理程式會收集各種組態資料，稱為遙測。如需 Amazon Inspector Classic 代理程式的詳細資訊，請參閱 Amazon Inspector Classic 代理程式。

Amazon Inspector Classic 的安全最佳實務

Amazon Inspector Classic 提供多種安全功能，供您在開發和實作自己的安全政策時加以考量。這些最佳實務為一般準則，並不代表完整的安全解決方案。這些最佳實務可能不適用或無法滿足您的環境需求，因此請將其視為實用建議就好，而不要當作是指示。

如需 Amazon Inspector Classic 的安全最佳實務清單，請參閱 the section called “Amazon Inspector Classic 的安全最佳實務”。

Amazon Inspector Classic 代理程式

Amazon Inspector Classic 代理程式是收集 Amazon EC2 執行個體已安裝套件資訊和軟體組態的實體。雖然並非所有情況都需要，但您應該在每個目標 Amazon EC2 執行個體上安裝 Amazon Inspector Classic 代理程式，以便完整評估其安全性。 Amazon EC2

如需進一步了解如何安裝、解除安裝、重新安裝代理程式、確認已安裝代理程式是否運作，以及設定代理程式的 Proxy 支援，請參閱在 Linux 作業系統上使用 Amazon Inspector Classic 代理程式 和 在 Windows 作業系統上使用 Amazon Inspector Classic 代理程式。

> **Note**
>
> 執行 Network Reachability 規則套件不需要 Amazon Inspector Classic 代理程式。

> **Important**
>
> Amazon Inspector Classic 代理程式依賴 Amazon EC2 執行個體中繼資料來正確運作。它使用執行個體中繼資料服務 (IMDSv1 或 IMDSv2) 的第 1 版或第 2 版存取執行個體中繼資料。請參閱執行個體中繼資料和使用者資料，以進一步了解 EC2 執行個體中繼資料和存取方法。

主題

Amazon Inspector Classic 代理程式權限

您必須具有管理或根許可，才能安裝 Amazon Inspector Classic 代理程式。在支援的 Linux 作業系統上，代理程式是由以根存取權執行的使用者模式執行檔所組成。在支援的 Windows 作業系統上，代理程式是由更新程式服務和代理程式服務所組成，兩者都在使用者模式中以 `LocalSystem` 許可執行。

網路和 Amazon Inspector Classic 代理程式安全性

Amazon Inspector Classic 代理程式會啟動與 Amazon Inspector Classic 服務的所有通訊。這表示代理程式必須有前往公有端點的對外網路路徑，才能傳送遙測資料。例如，代理程式可能會連線到 `arsenal.<region>.amazonaws.com`，或端點可能是位於 的 Amazon S3 儲存貯體`s3.dualstack.<region>.amazonaws.com`。請務必`<region>`將 取代為您執行 Amazon Inspector Classic 的實際 AWS 區域。如需更多資訊，請參閱 AWS IP Address Ranges (AWS IP 位址範圍)。由於來自代理程式的所有連線都是建立對外連線，因此不需要在安全群組中開啟連接埠，以允許從 Amazon Inspector Classic 傳入通訊給代理程式。

代理程式會透過 TLS 保護的頻道定期與 Amazon Inspector Classic 通訊，該頻道使用與 EC2 執行個體角色相關聯的 AWS 身分進行身分驗證，如果未指派角色，則使用執行個體的中繼資料文件進行身分驗證。經過驗證後，代理程式會傳送心跳訊號訊息給服務，並接收服務回應傳回的指示。若已排程評估，代理程式會接收該評估的指示。這些指示為結構化 JSON 檔案，可告知代理程式啟用或停用代理程式中預先設定的特定感應器。代理程式內已預先定義每個指示動作。無法執行任意指示。

在評估期間，代理程式會從系統收集遙測資料，以透過 TLS 保護的頻道傳回 Amazon Inspector Classic。代理程式不會變更其從中收集資料的系統。代理程式收集遙測資料後，會將資料傳回 Amazon Inspector Classic 進行處理。除了代理程式產生的遙測資料之外，代理程式無法收集或傳輸系統或評估目標相關的其他任何資料。目前，沒有公開任何方法可攔截或檢查代理程式上的遙測資料。

Amazon Inspector Classic 代理程式更新

隨著 Amazon Inspector Classic 代理程式的更新可用，它們會自動從 Amazon S3 下載並套用。這樣也會更新任何必要的相依性。自動更新功能讓您不再需要追蹤和手動維護您在 EC2 執行個體上安裝的代理程式版本控制。所有更新均依循經審核的 Amazon 變更控制流程，以確保符合其適用之安全標準的規範。

為了進一步確保代理程式的安全性，代理程式與自動更新發佈網站 (S3) 之間的通訊是透過 TLS 連線執行，且伺服器會經過驗證。所有涉及自動更新流程的二進位檔案會經過數位簽署，且在安裝之前會由更新程式驗證簽章。自動更新程序只會在非評估期間執行。如果偵測到任何錯誤，更新程序可以轉返和重試更新。最後，代理程式更新程序僅支援升級代理程式功能。在更新工作流程中，您的任何特定資訊都

不會從代理程式傳送至 Amazon Inspector Classic。在更新過程中傳輸的資訊只有基本安裝成功或失敗遙測資料，以及 (如適用) 任何更新失敗診斷資訊。

遙測資料生命週期

Amazon Inspector Classic 代理程式在評估執行期間產生的遙測資料會以 JSON 檔案格式化。這些檔案會透過 TLS near-real-time的方式交付至 Amazon Inspector Classic，並在其中使用per-assessment-run的暫時性 KMS 衍生金鑰加密。檔案會安全地存放在 Amazon S3 儲存貯體中，這是 Amazon Inspector Classic 專用。Amazon Inspector Classic 的規則引擎會存取 S3 儲存貯體中的加密遙測資料、在記憶體中解密資料，並根據設定的評估規則處理資料以產生問題清單。保留 S3 中存放的遙測資料只是以防需要透過支援請求取得協助。Amazon 不會在任何其他用途上使用或彙總之。30 天後，根據 Amazon Inspector Classic 資料的標準 S3 儲存貯體生命週期政策，遙測資料會永久刪除。目前，Amazon Inspector Classic 不提供 API 或 S3 儲存貯體存取機制來收集遙測。

從 Amazon Inspector Classic 到 AWS 帳戶的存取控制

作為安全服務，Amazon Inspector Classic 只有在需要尋找 EC2 執行個體以透過查詢標籤來評估時，才會存取 AWS 您的帳戶和資源。它透過 Amazon Inspector Classic 服務初始設定期間所建立的角色，透過標準 IAM 存取來執行此操作。在評估期間，與您的環境的所有通訊都是由本機安裝在 EC2 執行個體上的 Amazon Inspector Classic 代理程式啟動。建立的 Amazon Inspector Classic 服務物件，例如評估目標、評估範本和由服務產生的調查結果，會存放在由 管理的資料庫中，且僅供 Amazon Inspector Classic 存取。

Amazon Inspector Classic 代理程式限制

如需 Amazon Inspector Classic 代理程式限制的相關資訊，請參閱Amazon Inspector Classic 服務限制。

安裝 Amazon Inspector Classic 代理程式

您可以在多個執行個體 （ 包括 Linux 型和 Windows 型執行個體 ） 上使用 Systems Manager Run Command 安裝 Amazon Inspector Classic 代理程式。或者，您可以登入每個 EC2 執行個體來個別安裝代理程式。本章中的程序提供這兩種方法的指示。

另一個選項是，您可以在 主控台的定義評估目標頁面上選取安裝代理程式核取方塊，快速在評估目標中包含的所有 Amazon EC2 執行個體上安裝代理程式。

主題

- 使用 Systems Manager Run Command 在多個 EC2 執行個體上安裝代理程式
- 在 Linux EC2 執行個體上安裝代理程式
- 在 Windows EC2 執行個體上安裝代理程式

> **Note**
>
> 本章中的程序適用於 Amazon Inspector Classic 支援的所有 AWS 區域。

使用 Systems Manager Run Command 在多個 EC2 執行個體上安裝代理程式

您可以使用 Systems Manager Run Command 在 EC2 執行個體上安裝 Amazon Inspector Classic 代理程式。這可讓您在遠端一次在多個執行個體上 (使用相同命令在以 Linux 和 Windows 為基礎的執行個體) 上安裝代理程式。

> **Important**
>
> 使用 Systems Manager Run Command 的代理程式安裝目前不支援 Debian 作業系統。

> **Important**
>
> 若要使用此選項，請確定您的 EC2 執行個體已安裝 SSM Agent，且具有允許執行命令的 IAM 角色。在預設情況下，SSM 代理程式將安裝在 Amazon EC2 Windows 執行個體和 Amazon Linux 執行個體。Amazon EC2 Systems Manager 需要 EC2 執行個體的 IAM 角色來處理命令，以及執行命令的使用者需要不同的角色。如需詳細資訊，請參閱安裝和設定 SSM Agent 和設定 SSM 的安全角色。

使用 Systems Manager Run Command 在多個 EC2 執行個體上安裝代理程式

1. 在 https：//https://console.aws.amazon.com/systems-manager/ 開啟 AWS Systems Manager 主控台。
2. 在節點工具下的導覽窗格中，選擇執行命令。
3. 選擇 Run a command (執行指令)。

4. 在 Command document (命令文件) 的部分，選擇名為 AmazonInspector-ManageAWSAgent 的文件 (Amazon 所擁有)。本文件包含用於在 EC2 執行個體上安裝 Amazon Inspector Classic 代理程式的指令碼。
5. 對於目標，您可以使用不同的方法來選取 EC2 執行個體。若要在評定目標中的所有執行個體上安裝代理程式，您可以指定用來建立評定目標的標記。
6. 使用從主控台執行命令中的指示，在其餘可用選項中提供您的選擇，然後選擇 Run (執行)。

> **Note**
>
> 您也可以在建立評估目標時，在多個 EC2 執行個體 (Linux 型和 Windows 型） 上安裝代理程式，或者您可以使用現有目標的安裝代理程式與執行命令按鈕。如需詳細資訊，請參閱建立評估目標。

在 Linux EC2 執行個體上安裝代理程式

執行下列程序，在 Linux EC2 執行個體上安裝 Amazon Inspector Classic 代理程式。

在 Linux EC2 執行個體上安裝代理程式

1. 登入執行 Linux 作業系統的 EC2 執行個體，在其中安裝 Amazon Inspector Classic 代理程式。

   > **Note**
   >
   > 如需 Amazon Inspector Classic 支援的作業系統相關資訊，請參閱 Amazon Inspector Classic 支援的作業系統和區域。

2. 透過執行下列其中一個命令以下載代理程式安裝指令碼：

   - wget https://inspector-agent.amazonaws.com/linux/latest/install
   - curl -O https://inspector-agent.amazonaws.com/linux/latest/install

3. (選用) 確認代理程式安裝指令碼未變更或損毀。如需詳細資訊，請參閱（選用）驗證 Linux 作業系統上 Amazon Inspector Classic 代理程式安裝指令碼的簽章。
4. 若要安裝代理程式，請執行 sudo bash install。

> **Note**
>
> 如果您要在 SELinux 環境中安裝代理程式，Amazon Inspector Classic 可能會偵測為未受限的協助程式。您可以將代理程式程序的網域從預設值變更為 `initrc_t`來避免這種情況`bin_t`。在安裝 SELinux 代理程式之前，請使用下列命令將`bin_t`內容指派給 Amazon Inspector Classic 執行指令碼：
> sudo semanage fcontext -a -t bin_t /etc/rc\.d/init\.d/awsagent
> sudo semanage fcontext -a -t bin_t /etc/init\.d/awsagent

> **Note**
>
> 當代理程式的更新可用時，它們會自動從 Amazon S3 下載並套用。如需詳細資訊，請參閱Amazon Inspector Classic 代理程式更新。
> 如果您想跳過此自動更新程序，請在您安裝代理程式時執行下列命令：
> sudo bash install -u false

> **Note**
>
> (選用) 欲移除代理程式安裝指令碼，請執行 rm install。

5. 確認下列成功安裝代理程式並正常執行所需的檔案是否已安裝：

   - `libcurl4` (必須用於在 Ubuntu 18.04 上安裝代理程式)
   - `libcurl3`
   - `libgcc1`
   - `libc6`
   - `libstdc++6`
   - `libssl1.0.1`
   - `libssl1.0.2` (必須用於在 Debian 9 上安裝代理程式)
   - `libssl1.1` （在 Ubuntu 20.04 LTS 上安裝代理程式時需要）
   - `libpcap0.8`

在 Windows EC2 執行個體上安裝代理程式

執行下列程序，在 Windows EC2 執行個體上安裝 Amazon Inspector Classic 代理程式。

在 Windows EC2 執行個體上安裝代理程式

1. 登入執行 Windows 作業系統的 EC2 執行個體，以便安裝代理程式。

   > **Note**
   >
   > 如需 Amazon Inspector Classic 支援的作業系統的詳細資訊，請參閱 Amazon Inspector Classic 支援的作業系統和區域。

2. 下載以下的 .exe 檔案：

   ```
   https://inspector-agent.amazonaws.com/windows/installer/latest/
   AWSAgentInstall.exe
   ```

3. (透過管理員權限) 開啟命令提示字元視窗，前往您下載 `AWSAgentInstall.exe` 的儲存位置，然後執行 .exe 檔案來安裝代理程式。

   > **Note**
   >
   > 當代理程式的更新可用時，它們會自動從 Amazon S3 下載並套用。如需詳細資訊，請參閱Amazon Inspector Classic 代理程式更新。
   > 如果您想跳過此自動更新程序，請在您安裝代理程式時執行下列命令：
   > AWSAgentInstall.exe AUTOUPDATE=No

在 Linux 作業系統上使用 Amazon Inspector Classic 代理程式

您可以安裝、移除、驗證和修改 Amazon Inspector Classic 代理程式的行為。登入執行 Linux 作業系統的 Amazon EC2 執行個體，並執行下列任何程序。如需 Amazon Inspector Classic 支援的作業系統的詳細資訊，請參閱 Amazon Inspector Classic 支援的作業系統和區域。

Important

Amazon Inspector Classic 代理程式依賴 Amazon EC2 執行個體中繼資料來正確運作。它使用執行個體中繼資料服務 (IMDSv1 或 IMDSv2) 的第 1 版或第 2 版存取執行個體中繼資料。請參閱執行個體中繼資料和使用者資料，以進一步了解 EC2 執行個體中繼資料和存取方法。

Note

本節中的命令會在 Amazon Inspector Classic 支援的所有 AWS 區域中運作。

主題

驗證 Amazon Inspector Classic 代理程式是否正在執行

- 若要驗證代理程式是否已安裝並執行，請登入您的 EC2 執行個體並執行下列命令：

  sudo /opt/aws/awsagent/bin/awsagent status

  此命令會傳回目前正在執行的代理程式狀態或是無法連絡代理程式的錯誤訊息。

停止 Amazon Inspector Classic 代理程式

- 若要停用代理程式，請執行下列命令：

  sudo /etc/init.d/awsagent stop

啟動 Amazon Inspector Classic 代理程式

- 若要啟動代理程式，請執行下列命令：

  sudo /etc/init.d/awsagent start

修改 Amazon Inspector Classic 代理程式設定

在 EC2 執行個體上安裝並執行 Amazon Inspector Classic 代理程式之後，您可以修改agent.cfg檔案中的設定，以變更代理程式的行為。在 Linux 作業系統上，agent.cfg 檔案位於 /opt/aws/awsagent/etc 目錄中。修改並儲存 agent.cfg 檔案後，您必須將代理程式停用，再重新啟動，讓變更生效。

> **Important**
>
> 強烈建議您僅在 AWS Support 的指引下修改 agent.cfg 檔案。

設定 Amazon Inspector Classic 代理程式的代理支援

若要為 Linux 作業系統上的代理程式取得 Proxy 支援，請使用代理程式特定的組態檔，搭配特定的環境變數。如需更多資訊，請參閱 https://wiki.archlinux.org/index.php/proxy_settings。

完成下列程序之一：

在使用代理伺服器的 EC2 執行個體上安裝代理程式

1. 建立名為 awsagent.env 的檔案並儲存在 /etc/init.d/ 目錄中。
2. 依下列格式編輯 awsagent.env 以包含這些環境變數：
   - export https_proxy=hostname:port
   - export http_proxy=hostname:port
   - export no_proxy=169.254.169.254

> **Note**
>
> 僅使用有效的主機名稱與連接埠號碼替換先前範例中的值。為 no_proxy 變數指定執行個體中繼資料端點的 IP 地址 (169.254.169.254)。

3. 完成在 Linux EC2 執行個體上安裝代理程式程序中的步驟，安裝 Amazon Inspector Classic 代理程式。

使用執行中的代理程式在 EC2 執行個體上設定代理支援

1. 若要設定代理支援，在 EC2 執行個體上執行的代理程式版本必須是 1.0.800.1 或更新版本。若您啟用代理程式的自動更新程序，則可透過 驗證 Amazon Inspector Classic 代理程式是否正在執行程序，驗證代理程式版本是否為 1.0.800.1 版或更新版本。如果您未啟用代理程式的自動更新程序，則必須依照在 Linux EC2 執行個體上安裝代理程式程序再次在此 EC2 執行個體上安裝代理程式。
2. 建立名為 awsagent.env 的檔案，並儲存在 /etc/init.d/ 目錄中。
3. 依下列格式編輯 awsagent.env 以包含這些環境變數：

   - `export https_proxy=hostname:port`
   - `export http_proxy=hostname:port`
   - `export no_proxy=169.254.169.254`

> **Note**
>
> 僅使用有效的主機名稱與連接埠號碼替換先前範例中的值。為 no_proxy 變數指定執行個體中繼資料端點的 IP 地址 (169.254.169.254)。

4. 使用以下命令，將代理程式先停用再重新啟動：

   ```
   sudo /etc/init.d/awsagent restart
   ```

   代理程式與自動更新程序會挑選並使用 Proxy 設定。

解除安裝 Amazon Inspector Classic 代理程式

解除安裝代理程式

1. 登入執行 Linux 作業系統的 EC2 執行個體，在其中解除安裝代理程式。

> **Note**
>
> 如需 Amazon Inspector Classic 支援的作業系統的詳細資訊，請參閱 Amazon Inspector Classic 支援的作業系統和區域。

2. 若要解除安裝代理程式，請使用下列其中一項命令：

   - 在 Amazon Linux、CentOS 和 Red Hat 上，執行下列命令：

     ```
     sudo yum remove 'AwsAgent*'
     ```

   - 在 Ubuntu Server 上，執行下列命令：

     ```
     sudo apt-get purge 'awsagent*'
     ```

在 Windows 作業系統上使用 Amazon Inspector Classic 代理程式

您可以啟動、停止和修改 Amazon Inspector Classic 代理程式的行為。登入執行 Windows 作業系統的 EC2 執行個體，並執行本章中的任何程序。如需 Amazon Inspector Classic 支援的作業系統的詳細資訊，請參閱 Amazon Inspector Classic 支援的作業系統和區域。

> **Important**
>
> Amazon Inspector Classic 代理程式依賴 Amazon EC2 執行個體中繼資料來正確運作。它使用執行個體中繼資料服務 (IMDSv1 或 IMDSv2) 的第 1 版或第 2 版存取執行個體中繼資料。請參閱執行個體中繼資料和使用者資料，以進一步了解 EC2 執行個體中繼資料和存取方法。

> **Note**
>
> 本章中的命令會在 Amazon Inspector Classic 支援的所有 AWS 區域中運作。

主題

啟動或停止 Amazon Inspector Classic 代理程式，或驗證代理程式是否正在執行

啟動、停用或驗證代理程式

1. 在 EC2 執行個體上，選擇開始、執行，然後輸入 **`services.msc`**。
2. 如果代理程式成功執行，則會列出兩個服務，並在服務視窗中將其狀態設為已啟動或正在執行：AWS Agent Service 和 AWS Agent Updater Service。
3. 欲啟動代理程式，請按滑鼠右鍵點選 AWS Agent Service (AWS 代理程式服務)，接著選擇 Start (啟動)。若服務成功啟動，狀態就會更新為 Started (已啟動) 或 Running (執行中)。
4. 欲停用代理程式，請在 AWS Agent Service (AWS 代理程式服務) 按一下滑鼠右鍵，然後選擇 Stop (停用)。若服務成功停用，狀態就會清除 (顯示為空白)。不建議您停用 AWS Agent Updater Service (AWS 代理程式更新服務)，因為這樣就無法在代理程式上安裝未來的所有強化功能和修正程式。
5. 若要驗證代理程式是否已安裝並執行，請登入您的 EC2 執行個體，並使用管理許可開啟命令提示。前往 `C:\Program Files\Amazon Web Services\AWS Agent`，然後執行下列命令：

   AWSAgentStatus.exe

   此命令會傳回目前正在執行的代理程式狀態，或是無法聯繫代理程式的錯誤訊息。

修改 Amazon Inspector Classic 代理程式設定

在 EC2 執行個體上安裝並執行 Amazon Inspector Classic 代理程式之後，您可以修改`agent.cfg`檔案中的設定，以變更代理程式的行為。在 Windows 作業系統上，此檔案位於 `C:\ProgramData\Amazon Web Services\AWS Agent` 目錄中。修改並儲存 `agent.cfg` 檔案後，您必須將代理程式停用，再重新啟動，讓變更生效。

> **Important**
>
> 強烈建議您僅在 AWS Support 的指引下修改 `agent.cfg` 檔案。

設定 Amazon Inspector Classic 代理程式的代理支援

若要在 Windows 作業系統上取得代理程式的 Proxy 支援，請使用 `WinHTTP` 代理。若要使用 `netsh` 公用程式設定 `WinHTTP` Proxy，請參閱適用於 Windows Hypertext Transfer Protocol (WINHTTP) 的 Netsh 命令。

> **Important**
>
> Windows 型執行個體僅支援 HTTPS 代理。

完成下列程序之一：

在使用代理伺服器的 EC2 執行個體上安裝代理程式

1. 下載以下的 .exe 檔案：`https://d1wk0tztpsntt1.cloudfront.net/windows/installer/latest/AWSAgentInstall.exe`
2. (透過管理員權限) 開啟命令提示字元視窗或 PowerShell 視窗。前往下載 `AWSAgentInstall.exe` 的儲存位置，然後執行下列命令：

   ```
   .\AWSAgentInstall.exe /install USEPROXY=1
   ```

使用執行中的代理程式在 EC2 執行個體上設定代理支援

1. 若要設定代理支援，在 EC2 執行個體上執行的 Amazon Inspector Classic 代理程式版本必須為 1.0.0.59 或更新版本。若您啟用代理程式的自動更新程序，則可透過啟動或停止 Amazon Inspector Classic 代理程式，或驗證代理程式是否正在執行程序，驗證代理程式版本是否為 1.0.0.59 版或更新版本。如果您未啟用代理程式的自動更新程序，則必須依照在 Windows EC2 執行個體上安裝代理程式程序再次在此 EC2 執行個體上安裝代理程式。
2. 開啟登錄編輯器 (`regedit.exe`)。
3. 前往以下登錄機碼：`"HKEY_LOCAL_MACHINE/SOFTWARE/Amazon Web Services/AWS Agent Updater"`。

4. 在此登錄機碼中，建立名為 "UseProxy" 的登錄值 DWORD(32bit)。
5. 在此值按兩下並將值設定為 1。
6. 輸入 **services.msc**，在服務視窗中尋找 AWS Agent Service 和 AWS Agent Updater Service，然後重新啟動每個程序。這兩個程序成功重新啟動後，執行 AWSAgentStatus.exe 檔案 (請參閱啟動或停止 Amazon Inspector Classic 代理程式，或驗證代理程式是否正在執行中的步驟 5)。檢視代理程式的狀態，並驗證是否使用所設定的 Proxy。

解除安裝 Amazon Inspector Classic 代理程式

解除安裝代理程式

1. 登入執行 Windows 作業系統的 EC2 執行個體，在其中解除安裝 Amazon Inspector Classic 代理程式。

   > **Note**
   >
   > 如需 Amazon Inspector Classic 支援的作業系統的詳細資訊，請參閱 Amazon Inspector Classic 支援的作業系統和區域。

2. 在您的 EC2 執行個體上，請前往 Control Panel (控制台)，Add/Remove Programs (新增/移除) 程式。
3. 在已安裝程式的清單中，選擇 AWS Agent，然後選擇 Uninstall (解除安裝)。

（選用）驗證 Linux 作業系統上 Amazon Inspector Classic 代理程式安裝指令碼的簽章

本主題說明針對 Linux 作業系統驗證 Amazon Inspector Classic 代理程式安裝指令碼有效性的建議程序。

當您從網際網路下載應用程式時，建議您驗證軟體發佈者的身分，並檢查應用程式在發佈之後未遭更改或損毀。如此可保護您，避免安裝到包含病毒或其他惡意程式碼的應用程式版本。

如果執行本主題中的步驟後，您判斷 Amazon Inspector Classic 代理程式的軟體已更改或損毀，請勿執行安裝檔案。請改為聯絡 AWS Support。

適用於 Linux 作業系統的 Amazon Inspector Classic 代理程式檔案使用 進行簽署GnuPG，這是 Pretty Good Privacy (OpenPGP) 標準用於安全數位簽章的開放原始碼實作。 GnuPG（ 也稱為 GPG) 透過

數位簽章提供身分驗證和完整性檢查。Amazon EC2 會發佈公有金鑰和簽章，您可用來驗證下載的 Amazon EC2 CLI 工具。如需 PGP 和 GnuPG (GPG) 的詳細資訊，請參閱 http://www.gnupg.org。

第一步是與軟體發佈者建立信任。下載軟體發佈者的公開金鑰，檢查公開金鑰的擁有者是否為聲稱的擁有者，然後將公開金鑰新增至您的 keyring。您的 keyring 是一組已知的公開金鑰。在您建立公開金鑰的真實性之後，即可用它來驗證應用程式的簽章。

主題

安裝 GPG 工具

如果您的作業系統是 Linux 或 Unix，那麼有可能已安裝 GPG 工具。若要測試工具是否已安裝在您的系統，請在命令提示字元中輸入 gpg。如果 GPG 工具已安裝，您會看到 GPG 命令提示字元。如果 GPG 工具未安裝，您會看到表示找不到該命令的錯誤。您可以從儲存庫安裝 GnuPG 套件。

在以 Debian 為基礎的 Linux 上安裝 GPG 工具

- 從終端機執行下列命令：apt-get install gnupg。

在以 Red Hat 為基礎的 Linux 上安裝 GPG 工具

- 從終端機執行下列命令：yum install gnupg。

驗證和匯入公開金鑰

程序的下一個步驟是驗證 Amazon Inspector Classic 公有金鑰，並將其新增為 GPG keyring 中的信任金鑰。

驗證和匯入 Amazon Inspector Classic 公有金鑰

1. 執行以下其中一項以取得我們的公有 GPG 建置金鑰的副本：
   - 從 https://d1wk0tztpsntt1.cloudfront.net/linux/latest/inspector.gpg 下載。
   - 從以下文字複製金鑰，然後貼到名為 `inspector.gpg` 的檔案中。務必包含以下所有項目：

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2.0.18 (GNU/Linux)

mQINBFYDlfEBEADFpfNt/mdCtsmfDoga+PfHY9bdXAD68yhp2m9NyH3BOzle/MXI
8siNfoRgzDwuWnIaezHwwLWkDw2paRxp1NMQ9qRe8Phq0ewheLrQu95dwDgMcw90
gf9m1iKVHjdVQ9qNHlB2OFknPDxMDRHcrmlJYDKYCX3+MODEHnlK25tIH2KWezXP
FPSU+TkwjLRzSMYH1L8IwjFUIIi78jQS9a31R/cOl4zuC5fOVghYlSomLI8irfoD
JSa3csVRujSmOAf9o3beiMR/kNDMpgDOxgiQTu/Kh39cl6o8AKe+QKK48kqO7hra
h1dpzLbfeZEVU6dWMZtlUksG/zKxuzD6d8vXYH7Z+x09POPFALQCQQMC3WisIKgj
zJEFhXMCCQ3NLC3CeyMq3vP7MbVRBYE7t3d2uDREkZBgIf+mbUYfYPhrzy0qT9Tr
PgwcnUvDZuazxuuPzucZGOJ5kbptat3DcUpstjdkMGAId3JawBbps77qRZdA+swr
o9o3jbowgmf0y5ZS6KwvZnC6XyTAkXy2io7mSrAIRECrANrzYzfp5v7uD7w8Dk0X
1OrfOm1VufMzAyTu0YQGBWaQKzSB8tCkvFw54PrRuUTcV826XU7SIJNzmNQo58uL
bKyLVBSCVabfs0lkECIesq8PT9xMYfQJ421uATHyYUnFTU2TYrCQEab7oQARAQAB
tCdBbWF6b24gSW5zcGVjdG9yIDxpbnNwZWN0b3JAYW1hem9uLmNvbT6JAjgEEwEC
ACIFAlYDlfECGwMGCwkIBwMCBhUIAgkKCwQWAgMBAh4BAheAAAoJECR0CWBYNgQY
8yUP/2GpIl40f3mKBUiSTe0XQLvwiBCHmY+V9fOuKqDTinxssjEMCnz0vsKeCZF/
L35pwNa/oW0OJa8D7sCkKG+8LuyMpcPDyqptLrYPprUWtz2+qLCHgpWsrku7ateF
x4hWS0jUVeHPaBzI9V1NTHsCx9+nbpWQ5Fk+7VJI8hbMDY7NQx6fcse8WTlP/0r/
HIkKzzqQQaaOf5t9zc5DKwi+dFmJbRUyaq22xs8C81UODjHunhjHdZ21cnsgk91S
fviuaum9aR4/uVIYOTVWnjC5J3+VlczyUt5FaYrrQ5ov0dM+biTUXwve3X8Q85Nu
DPnO/+zxb7Jz3QCHXnuTbxZTjvvl60Oi8//uRTnPXjz4wZLwQfibgHmk1++hzND7
wOYA02Js6v5FZQlLQAod7q2wuA1pq4MroLXzziDfy/9ea8B+tzyxlmNVRpVZY4Ll
DOHyqGQhpkyV3drjjNZlEofwbfu7m6ODwsgMl5ynzhKklJzwPJFfB3mMc7qLi+qX
MJtEX8KJ/iVUQStHHAG7daL1bxpWSI3BRuaHsWbBGQ/mcHBgUUOQJyEp5LAdg9Fs
VP55gWtF7pIqifiqlcfgG0Ov+A3NmVbmiGKSZvfrc5KsF/k43rCGqDx1RV6gZvyI
LfO9+3sEIlNrsMib0KRLDeBt3EuDsaBZgOkqjDhgJUesqiCy
=iEhB
-----END PGP PUBLIC KEY BLOCK-----
```

2. 在您儲存 inspector.gpg 的目錄中的命令提示字元中，使用下列命令將 Amazon Inspector Classic 公有金鑰匯入 keyring：

```
gpg --import inspector.gpg
```

此命令會傳回類似以下的結果：

```
gpg: key 58360418: public key "Amazon Inspector <inspector@amazon.com>" imported
                   gpg: Total number processed: 1
                   gpg:               imported: 1  (RSA: 1)
```

請記下金鑰值，在後續步驟您將會用到它。在前面的範例中，金鑰值為 58360418。

3. 執行以下命令以驗證指紋，請以三個步驟的值取代 key-value：

```
gpg --fingerprint key-value
```

此命令會傳回類似以下的結果：

```
pub   4096R/58360418 2015-09-24
                Key fingerprint = DDA0 D4C5 10AE 3C20 6F46  6DC0 2474 0960 5836
 0418
                uid                  Amazon Inspector <inspector@amazon.com>
```

此外，如以上範例所示，指紋字串應該與 DDA0 D4C5 10AE 3C20 6F46 6DC0 2474 0960 5836 0418 完全相同。比較傳回的金鑰指紋與此頁面發佈的金鑰指紋。它們應該相符。如果不相符，請勿安裝 Amazon Inspector Classic 代理程式安裝指令碼，並聯絡 AWS Support。

驗證套件的簽章

安裝GPG工具、驗證和匯入 Amazon Inspector Classic 公有金鑰，並確認公有金鑰受信任後，您就可以驗證安裝指令碼的簽章。

驗證 安裝指令碼簽章

1. 在命令提示字元上，執行以下命令以下載安裝指令碼的簽章檔案：

```
curl -O https://inspector-agent.amazonaws.com/linux/latest/install.sig
```

2. 在儲存的目錄中的命令提示字元install.sig和 Amazon Inspector Classic 安裝檔案中執行下列命令，以驗證簽章。兩個檔案都必須存在。

```
gpg --verify ./install.sig
```

輸出應類似以下所示：

```
gpg: Signature made Thu 24 Sep 2015 03:19:09 PM UTC using RSA key ID 58360418
gpg: Good signature from "Amazon Inspector <inspector@amazon.com>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
```

```
Primary key fingerprint: DDA0 D4C5 10AE 3C20 6F46  6DC0 2474 0960 5836 0418
```

如果輸出包含片語 `Good signature from "Amazon Inspector <inspector@amazon.com>"`，表示簽章已成功驗證，您可以繼續執行 Amazon Inspector Classic 安裝指令碼。

如果輸出包含 `BAD signature` 片語，請檢查您是否已正確執行程序。如果您持續收到此回應，請不要執行您先前下載的安裝檔，然後聯絡 AWS Support。

以下是您可能會看到的警告的詳細資訊：

- 警告：此金鑰未通過信任簽章的認證！沒有指示簽章屬於擁有者。這是指您個人的信任程度，因為您認為您擁有 Amazon Inspector Classic 的真實公有金鑰。在理想世界中，您請會前往 AWS 辦公室並獲得該金鑰。不過，通常您會從網站下載。在此情況下，該網站是 AWS 網站。
- gpg：沒有發現最終信任的金鑰。這表示該特定金鑰未獲得您 (或您信任的其他人) 的「最終信任」。

如需詳細資訊，請參閱 http://www.gnupg.org。

（選用）驗證 Windows 作業系統上 Amazon Inspector Classic 代理程式安裝指令碼的簽章

本主題說明驗證 Amazon Inspector Classic 代理程式的 Windows 作業系統安裝指令碼有效性的建議程序。

當您從網際網路下載應用程式時，建議您驗證軟體發佈者的身分，並檢查應用程式在發佈之後未遭更改或損毀。如此可保護您，避免安裝到包含病毒或其他惡意程式碼的應用程式版本。

如果執行本主題中的步驟後，您判斷 Amazon Inspector Classic 代理程式的軟體已遭修改或損毀，請勿執行安裝檔案。請改為聯絡 AWS Support。

為了驗證 Windows 作業系統上所下載代理程式安裝指令碼的有效性，請確定其 Amazon Services LLC 簽署者憑證的指紋等於這個值：

E8 83 C5 3A F7 8C BA 7C F5 A2 47 E9 B8 86 FC E9 68 EE 0B 36

若要驗證這個值，請執行以下程序：

1. 在下載的 `AWSAgentInstall.exe` 上按一下滑鼠右鍵，然後開啟 Properties (屬性) 視窗。

2. 選擇 數位簽章 索引標籤。
3. 從簽章清單中，選擇 Amazon Web Services， Inc.，然後選擇詳細資訊。
4. 選擇 General (一般) 索引標籤 (如果尚未選取)，然後選擇 View Certificate (檢視憑證)。
5. 選擇詳細資訊索引標籤，如果尚未選取，請在顯示下拉式清單中選擇全部。
6. 向下捲動到看見 Thumbprint (指紋) 欄位為止，然後選擇 Thumbprint (指紋)。這會在下方的視窗中顯示整個指紋值。

   - 如果下方視窗中的指紋值與以下值完全相同：

     E8 83 C5 3A F7 8C BA 7C F5 A2 47 E9 B8 86 FC E9 68 EE 0B 36

     則表示您下載的代理程式安裝指令碼是可靠的，可安全地安裝。
   - 如果下方詳細資訊視窗中的指紋值與上述值不同，請勿執行 `AWSAgentInstall.exe`。

Amazon Inspector Classic 評估目標

您可以使用 Amazon Inspector Classic 來評估您的 AWS 評估目標 （ 您的 AWS 資源集合 ） 是否有您應解決的潛在安全問題。

> **Important**
>
> 目前，您的評估目標只能包含在支援的作業系統上執行的 EC2 執行個體。如需支援的作業系統和支援的 AWS 區域相關資訊，請參閱 the section called “支援的作業系統和區域”。

> **Note**
>
> 如需啟動 EC2 執行個體的相關資訊，請參閱 Amazon Elastic Compute Cloud 文件。

主題

標記資源以建立評估目標

若要為 Amazon Inspector Classic 建立評估目標以進行評估，請先標記您要包含在目標中的 EC2 執行個體。標籤是做為中繼資料的單字或片語，用於識別和組織您的執行個體和其他 AWS 資源。Amazon Inspector Classic 會使用您建立的標籤來識別屬於目標的執行個體。

每個 AWS 標籤都包含您選擇的金鑰和值對。例如，您可以選擇將金鑰命名為「Name」，將值命名為「MyFirstInstance」。標記執行個體之後，您可以使用 Amazon Inspector Classic 主控台將執行個體新增至評估目標。不需要任何執行個體符合多個標籤金鑰值對。

當您標記 EC2 執行個體以建置評估目標時，您可以建立自己的自訂標籤金鑰，或使用相同 AWS 帳戶中其他人建立的標籤金鑰。您也可以使用 AWS 自動建立的標籤金鑰。例如， AWS 會自動為您啟動的 EC2 執行個體建立名稱標籤金鑰。

您可以在建立 EC2 執行個體時新增標籤，也可以在每個 EC2 執行個體的主控台頁面上一次新增、變更或移除這些標籤。您也可以使用標籤編輯器一次將標籤新增至多個 EC2 執行個體。

如需詳細資訊，請參閱標籤編輯器。如需標記 EC2 執行個體的詳細資訊，請參閱資源與標籤。

Amazon Inspector Classic 評估目標限制

每個 AWS 帳戶最多可以建立 50 個評估目標。如需詳細資訊，請參閱Amazon Inspector Classic 服務限制。

建立評估目標

您可以使用 Amazon Inspector Classic 主控台來建立評估目標。

建立評估目標

1. 登入 AWS Management Console ，並在 https://console.aws.amazon.com/inspector/ ：// 開啟 Amazon Inspector Classic 主控台。
2. 在導覽面版中選擇 Assessment Targets (評估目標)，然後選擇 Create (建立)。
3. 在 Name (名稱) 中，輸入評估目標的名稱。
4. 執行以下任意一項：

   - 若要在此評估目標中包含此 AWS 帳戶和區域中的所有 EC2 執行個體，請選取所有執行個體核取方塊。

     > **Note**
     >
     > 使用此選項時，適用評估執行可包含的代理程式數量上限。如需詳細資訊，請參閱Amazon Inspector Classic 服務限制。

   - 若要選擇您要包含在此評估目標中的 EC2 執行個體，請在使用標籤中輸入標籤金鑰名稱和金鑰值對。
5. （選用）建立目標時，您可以選取安裝代理程式核取方塊，在此目標中的所有 EC2 執行個體上安裝代理程式。若要使用此選項，您的 EC2 執行個體必須安裝 SSM Agent 和允許執行命令的 IAM 角色。在預設情況下，SSM 代理程式將安裝在 Amazon EC2 Windows 執行個體和 Amazon Linux 執行個體。Amazon EC2 Systems Manager 需要 EC2 執行個體的 IAM 角色來處理命令，而執行命令的使用者則需要單獨的角色。如需詳細資訊，請參閱 Installing and Configuring SSM Agent 與 Configuring Security Roles for System Manager。

> **Important**
>
> 如果 EC2 執行個體上已有執行的代理程式，請使用此選項以最新代理程式版本取代目前執行個體上的代理程式。

> **Note**
>
> 對於現有的評估目標，您可以選擇使用執行命令安裝代理程式按鈕，在此目標中的所有 EC2 執行個體上安裝代理程式。

> **Note**
>
> 您也可以使用 Systems Manager Run Command，在多個 EC2 執行個體 (Linux 型執行個體和 Windows 型執行個體使用相同命令） 上遠端安裝代理程式。如需詳細資訊，請參閱使用 Systems Manager Run Command 在多個 EC2 執行個體上安裝 Amazon Inspector 代理程式。

6. 選擇 Save (儲存)。

> **Note**
>
> 您可以使用評估目標頁面上的預覽目標按鈕來檢閱評估目標中包含的所有 EC2 執行個體。對於每個 EC2 執行個體，您可以檢閱主機名稱、執行個體 ID、IP 地址，以及適用的代理程式狀態。代理程式狀態可以有下列值：HEALTHY、UNHEALTHY 和 UNKNOWN。當 Amazon Inspector Classic 無法判斷 EC2 執行個體上是否有執行中的代理程式時，會顯示 UNKNOWN 狀態。

刪除評估目標

若要刪除評估目標，請執行以下程序。

刪除評估目標

- 在 Assessment targets (評估目標) 頁面，選擇您要刪除的目標，然後選擇 Delete (刪除)。出現確認提示時，請選擇 Yes (是)。

> **Important**
>
> 刪除評估目標時，與該目標相關聯的所有評估範本、評估執行、調查結果及報告版本也會一併刪除。

您也可以使用 `DeleteAssessmentTarget` API 來刪除評估目標。

Amazon Inspector Classic 規則套件和規則

您可以使用 Amazon Inspector Classic 來評估您的評估目標 (AWS 資源集合） 是否有潛在的安全問題和漏洞。Amazon Inspector Classic 會將評估目標的行為和安全組態與選取的安全規則套件進行比較。在 Amazon Inspector Classic 的內容中，規則是 Amazon Inspector Classic 在評估執行期間執行的安全性檢查。

在 Amazon Inspector Classic 中，規則會依類別、嚴重性或定價分組為不同的規則套件。如此即可選擇您要執行的分析類型。例如，Amazon Inspector Classic 提供大量的規則，可用來評估您的應用程式。但您可能只想使用所有可用規則的其中一小部分，以鎖定關注的特定區域，或用於找出特定的安全問題。擁有大型 IT 部門的公司，可能需要判斷其應用程式是否遭受任何安全性威脅。其他公司可能只想要專注於嚴重性等級高的問題上。

Amazon Inspector Classic 中規則的嚴重性等級

每個 Amazon Inspector Classic 規則都有指派的嚴重性等級。這可減少分析中某個規則優先於另一個規則的需求。當某條規則突顯出某個潛在問題時，就有助於判斷該如何回應。

High (高)、Medium (中)、Low (低) 三種等級代表了可能導致評估目標中資訊的機密性、完整度、可用性受損的安全問題。這些層級的區別在於問題造成入侵的可能性，以及修正問題的急迫程度。

Informational (參考) 等級則只是用於指出評估目標安全組態的某項詳細資訊。

以下是根據問題嚴重性來回應問題的建議方法：

- 高 – 高嚴重性問題非常緊急。Amazon Inspector Classic 建議您將此安全問題視為緊急狀況，並實作立即修復。
- 中 – 中嚴重性問題有點緊急。Amazon Inspector Classic 建議您在下一個可能的機會修正此問題，例如在下一次服務更新期間。
- 低 – 低嚴重性問題較不緊急。Amazon Inspector Classic 建議您修正此問題，做為未來服務更新的一部分。
- 資訊性 – 這些問題純屬資訊性。根據業務和組織目標，您可以只記下此資訊，或是利用此資訊提升評估目標的安全性。

Amazon Inspector Classic 中的規則套件

Amazon Inspector 評估可以使用以下規則套件的任意組合：

網路評估：

- 網路連線能力

主機評估：

- 常見的漏洞和風險
- Center for Internet Security (CIS) 基準參考指標
- Amazon Inspector Classic 的安全最佳實務

網路連線能力

Network Reachability 套件中的規則會分析您的網路組態，以尋找 EC2 執行個體的安全漏洞。Amazon Inspector 產生的調查結果也可指導您如何限制不安全的存取。

Network Reachability 規則套件使用 AWS 來自 Provable Security 計畫的最新技術。

這些規則產生的調查結果可顯示，您的連接埠是否可從網際網路透過網際網路閘道 (包括 Application Load Balancer 或 Classic Load Balancer 後面的執行個體)、VPC 互連連線或經由虛擬閘道的 VPN 加以連線。這些調查結果也特別指出放任可能惡意存取的網路組態，例如管理不善的安全群組、ACL、IGW 等等。

這些規則有助於自動化 AWS 網路的監控，並識別 EC2 執行個體的網路存取可能設定錯誤的位置。您可以將此套件納入評估執行中，以實作詳細的網路安全性檢查，而無需安裝掃描器和傳送封包，這維護起來很複雜又昂貴，尤其是透過 VPC 對等連線和 VPN。

> **Important**
>
> 使用此規則套件評估 EC2 執行個體時，不需要 Amazon Inspector Classic 代理程式。不過，安裝代理程式可提供是否有任何程序在接聽連接埠的相關資訊。請勿在 Amazon Inspector Classic 不支援的作業系統上安裝 代理程式。如果代理程式存在於執行不支援作業系統的執行個體上，網路連線能力規則套件將無法在該執行個體上運作。

如需詳細資訊，請參閱支援作業系統的 Amazon Inspector Classic 規則套件。

分析的組態

網路連線能力規則會分析以下實體的組態是否有漏洞：

- Amazon EC2 執行個體
- Application Load Balancer
- Direct Connect
- Elastic Load Balancer
- 彈性網路界面
- 網際網路閘道 (IGW)
- 網路存取控制清單 (ACL)
- 路由表
- 安全群組 (SG)
- 子網路
- 虛擬私有雲端 (VPC)
- 虛擬私有閘道 (VGW)
- VPC 對等連接

連線能力路由

網路連線能力規則會檢查以下連線能力路由，這對應於從 VPC 外部可存取連接埠的方式：

- **`Internet`** - 網際網路閘道 (包括 Application Load Balancer 和 Classic Load Balancer)
- **`PeeredVPC`** - VPC 對等連線
- **`VGW`** - 虛擬私有閘道

問題清單類型

含有網路連線能力規則套件的評估可針對每個連線能力路由，傳回以下類型的調查結果：

- `RecognizedPort`
- `UnrecognizedPortWithListener`

- NetworkExposure

RecognizedPort

通常用於知名服務的連接埠都可連線。如果目標 EC2 執行個體上有代理程式，產生的調查結果也會指出連接埠上是否有作用中的接聽程序。根據知名服務的安全影響，此類型的調查結果會獲得一個嚴重等級：

- **RecognizedPortWithListener** – 已辨識的連接埠可透過特定聯網元件從公有網際網路外部連線，而程序正在接聽連接埠。
- **RecognizedPortNoListener** – 連接埠可透過特定聯網元件從公有網際網路外部連線，而且沒有監聽連接埠的程序。
- **RecognizedPortNoAgent** – 連接埠可透過特定聯網元件從公有網際網路外部連線。如果沒有在目標執行個體上安裝代理程式，則無法判斷是否有程序在連接埠上接聽。

下表為認可的連接埠清單：

服務	TCP 連接埠	UDP 連接埠
SMB	445	445
NetBIOS	137、139	137、138
LDAP	389	389
透過 TLS 的 LDAP	636	
通用類別目錄 LDAP	3268	
透過 TLS 的通用類別目錄 LDAP	3269	
NFS	111、2049、4045、1110	111、2049、4045、1110
Kerberos	88、464、54 3、544、749、751	88、464、749、750、751、752
RPC	111、135、530	111、135、530

服務	TCP 連接埠	UDP 連接埠
WINS	1512、42	1512、42
DHCP	67、68、546、547	67、68、546、547
Syslog	601	514
列印服務	515	
Telnet	23	23
FTP	21	21
SSH	22	22
RDP	3389	3389
MongoDB	27017、27018、27019、28017	
SQL Server	1433	1434
MySQL	3306	
PostgreSQL	5432	
Oracle	1521、1630	
Elasticsearch	9300、9200	
HTTP	80	80
HTTPS	443	443

`UnrecogizedPortWithListener`

可連線至上表未列出的連接埠，且其擁有作用中的接聽程序。由於此類型的調查結果顯示監聽程序的相關資訊，因此只有在目標 EC2 執行個體上安裝 Amazon Inspector 代理程式時，才能產生這些程序。此類型的調查結果會獲得 Low (低) 嚴重等級。

NetworkExposure

此類型的調查結果會顯示 EC2 執行個體上可存取之連接埠的彙總資訊。對於 EC2 執行個體上的每個彈性網路介面和安全群組組合，這些調查結果會顯示一組可連線的 TCP 和 UDP 連接埠範圍。此類型的調查結果具有 Informational (參考) 嚴重等級。

常見的漏洞和風險

此套件中的規則有助於驗證評估目標中的 EC2 執行個體是否暴露於常見漏洞和暴露 (CVEs)。攻擊可以利用未修補的漏洞危害服務或資料的機密性、完整性和可用性。CVE 系統為公開已知的資安漏洞與暴露提供了參考方法。如需詳細資訊，請參閱 https://cve.mitre.org/。

如果特定 CVE 出現在 Amazon Inspector Classic 評估產生的調查結果中，您可以搜尋 https://cve.mitre.org/ 以取得 CVE 的 ID （例如 **CVE-2009-0021**)。搜尋結果可提供此 CVE、嚴重性，以及減輕嚴重性方式的詳細資訊。

對於常見漏洞和漏洞 (CVE) 規則套件，Amazon Inspector 已映射提供的 CVSS 基本評分和 ALAS 嚴重性等級：

Amazon Inspector 嚴重性	CVSS 基本分數	ALAS 嚴重性 （如果 CVSS 未計分）
High	>= 5	Critical or Important
Medium	< 5 and >= 2.1	Medium
Low	< 2.1 and >= 0.8	Low
Informational	< 0.8	N/A

此套件中包含的規則可協助您評估 EC2 執行個體是否公開給下列區域清單中CVEs：

- 美國東部 (維吉尼亞北部)
- 美國東部 (俄亥俄)
- 美國西部 (加州北部)
- 美國西部 (奧勒岡)
- 歐洲 (愛爾蘭)

- 歐洲 (法蘭克福)
- 歐洲 (倫敦)
- 歐洲 (斯德哥爾摩)
- 亞太區域 (東京)
- 亞太區域 (首爾)
- 亞太區域 (孟買)
- 亞太區域 (雪梨)
- AWS GovCloud 西部 (美國)
- AWS GovCloud 東部 (美國)

CVE 規則套件會定期更新；在擷取此清單時發生之評估執行所包含的 CVE，也包含在此清單中。

如需詳細資訊，請參閱支援作業系統的 Amazon Inspector Classic 規則套件。

Center for Internet Security (CIS) 基準參考指標

CIS Security Benchmarks 計畫提供定義明確、無偏差、以共識為基礎的產業最佳實務，以協助組織評估和改善其安全性。 AWS 是 CIS Security Benchmarks 成員公司。如需 Amazon Inspector Classic 認證清單，請參閱 CIS 網站上的 Amazon Web Services 頁面。

Amazon Inspector Classic 目前提供下列 CIS 認證規則套件，以協助建立下列作業系統的安全組態狀態：

Amazon Linux

- CIS Benchmark for Amazon Linux 2 Benchmark v1.0.0 Level 1
- CIS Benchmark for Amazon Linux 2 Benchmark v1.0.0 Level 2
- CIS Benchmark for Amazon Linux Benchmark v2.1.0 Level 1
- CIS Benchmark for Amazon Linux Benchmark v2.1.0 Level 2
- CIS Benchmark for Amazon Linux 2014.09-2015.03 v1.1.0 Level 1

CentOS Linux

- CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 1 Server

- CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 2 Server
- CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 1 Workstation
- CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 2 Workstation
- CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2 Level 1 Server
- CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2 Level 2 Server
- CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2 Level 1 Workstation
- CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2 Level 2 Workstation

Red Hat Enterprise Linux

- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 1 Server
- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 2 Server
- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 1 Workstation
- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 2 Workstation
- CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2 Level 1 Server
- CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2 Level 2 Server
- CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2. Level 1 Workstation
- CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2 Level 2 Workstation

Ubuntu

- CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 1 Server
- CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 2 Server
- CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 1 Workstation

- CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 2 Workstation
- CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 1 Server
- CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 2 Server
- CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 1 Workstation
- CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 2 Workstation
- CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0 Level 1 Server
- CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0 Level 2 Server
- CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0 Level 1 Workstation
- CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0 Level 2 Workstation

Windows

- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Level 1 Member Server Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Level 2 Member Server Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Level 1 Domain Controller Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Level 2 Domain Controller Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Next Generation Windows Security Profile)
- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows 2012 R2, v2.2.0, Level 1 Domain Controller Profile)
- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows 2012 R2, v2.2.0, Level 2 Domain Controller Profile)
- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows 2012 R2, v2.2.0, Level 1 Member Server Profile)

- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows 2012 R2, v2.2.0, Level 2 Member Server Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows 2012 non-R2, v2.0.0, Level 1 Member Server Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows 2012 non-R2, v2.0.0, Level 2 Member Server Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows 2012 non-R2, v2.0.0, Level 1 Domain Controller Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows 2012 non-R2, v2.0.0, Level 2 Domain Controller Profile)
- Windows Server 2008 R2 (CIS Benchmark for Microsoft Windows 2008 R2, v3.0.0, Level 1 Domain Controller Profile)
- Windows Server 2008 R2 (CIS Benchmark for Microsoft Windows 2008 R2, v3.0.0, Level 1 Member Server Profile)

如果特定 CIS 基準出現在 Amazon Inspector Classic 評估執行所產生的調查結果中，您可以從 https://benchmarks.cisecurity.org/：// 下載基準的詳細 PDF 說明（需要免費註冊）。基準參考指標文件提供此 CIS 基準參考指標基準、嚴重性，以及減輕嚴重性方式的詳細資訊。

如需詳細資訊，請參閱支援作業系統的 Amazon Inspector Classic 規則套件。

Amazon Inspector Classic 的安全最佳實務

使用 Amazon Inspector Classic 規則來協助判斷您的系統是否設定安全。

> **Important**
>
> 目前，您可以在執行 Linux 型或 Windows 作業系統的評估目標 EC2 執行個體中包含 。在評估執行期間，本節所述的規則只會針對執行 Linux 作業系統的 EC2 執行個體產生調查結果。這些規則不會為執行 Windows 作業系統的 EC2 執行個體產生問題清單。
> 如需詳細資訊，請參閱支援作業系統的 Amazon Inspector Classic 規則套件。

主題

- 停用 SSH 根登入

- 僅支援 SSH 版本 2
- 停用 SSH 密碼驗證
- 設定密碼最長期限
- 設定密碼長度下限
- 設定密碼複雜性
- 啟用 ASLR
- 啟用 DEP
- 設定系統目錄許可

停用 SSH 根登入

此規則有助於判斷 SSH 協助程式是否已設定允許做為根來登入您的 EC2 執行個體。

嚴重性

中性

問題清單

您的評估目標中有 EC2 執行個體，其設定為允許使用者透過 SSH 使用根憑證登入。這會增加暴力破解攻擊成功的可能性。

解決方案

建議您設定 EC2 執行個體，以防止根帳戶透過 SSH 登入。反之，以非根使用者登入，且必要時使用 sudo 以提升權限。若要停用 SSH 根帳戶登入，請在 /etc/ssh/sshd_config 檔案中將 PermitRootLogin 設為 no，然後重新啟動 sshd。

僅支援 SSH 版本 2

此規則有助於判斷 EC2 執行個體是否設定為支援 SSH 通訊協定第 1 版。

嚴重性

中性

問題清單

評估目標中的 EC2 執行個體已設定為支援 SSH-1，其中包含可大幅降低其安全性的固有設計瑕疵。

解決方案

建議您將評估目標中的 EC2 執行個體設定為僅支援 SSH-2 和更新版本。若是 OpenSSH，您可在 `/etc/ssh/sshd_config` 檔案中設定 `Protocol 2` 來達到目標。如需詳細資訊，請參閱`man sshd_config`。

停用 SSH 密碼驗證

此規則有助於判斷 EC2 執行個體是否設定為支援透過 SSH 通訊協定進行密碼身分驗證。

嚴重性

中性

問題清單

評估目標中的 EC2 執行個體已設定為支援透過 SSH 進行密碼身分驗證。密碼驗證易受暴力破解攻擊，應盡可能停用以金鑰為基礎的身分驗證。

解決方案

我們建議您停用在 EC2 執行個體上透過 SSH 進行密碼驗證，並啟用支援以金鑰為基礎的身分驗證。這會大幅減少暴力破解攻擊成功的可能性。如需詳細資訊，請造訪 https://aws.amazon.com/articles/1233/。如果已支援密碼驗證，請務必限制存取 SSH 伺服器的為信任的 IP 位址。

設定密碼最長期限

此規則有助於判斷是否已在 EC2 執行個體上設定密碼的最長使用期。

嚴重性

中性

問題清單

評估目標中的 EC2 執行個體未設定密碼的最長使用期限。

解決方案

如果您使用的是密碼，建議您為評估目標中的所有 EC2 執行個體設定密碼的最長使用期。這需要使用者定期變更密碼，以降低密碼臆測攻擊成功的機率。若要為現有使用者修正此問題，請使用

chage 命令。若要為所有未來使用者設定密碼最大期限，請編輯 /etc/login.defs 檔案中的 PASS_MAX_DAYS 欄位。

設定密碼長度下限

此規則有助於判斷是否已在 EC2 執行個體上設定密碼的最小長度。

嚴重性

中性

問題清單

評估目標中的 EC2 執行個體未設定為密碼的長度下限。

解決方案

如果您使用的是密碼，建議您為評估目標中的所有 EC2 執行個體設定密碼長度下限。強制執行最低密碼長度可減少密碼臆測攻擊成功的風險。您可以使用 pwquality.conf 檔案中的下列選項來執行此操作：minlen。如需詳細資訊，請參閱 https：//https://linux.die.net/man/5/pwquality.conf。

如果執行個體上pwquality.conf無法使用 ，您可以使用 pam_cracklib.so模組設定 minlen選項。如需詳細資訊，請參閱man pam_cracklib。

minlen 選項應設定為 14 或更高。

設定密碼複雜性

此規則有助於判斷是否已在您的 EC2 執行個體上設定密碼複雜性機制。

嚴重性

中性

問題清單

評估目標中的 EC2 執行個體未設定密碼複雜性機制或限制。這將讓使用者能夠設定簡單的密碼，從而讓未經授權的使用者更有機會取得存取權並濫用帳戶。

解決方案

如果您使用密碼，建議您將評估目標中的所有 EC2 執行個體設定為需要一定程度的密碼複雜性。方法是，在 pwquality.conf 檔案中使用下列選項：lcredit、ucredit、dcredit 和 ocredit。如需詳細資訊，請參閱 https://linux.die.net/man/5/pwquality.conf。

如果您的執行個體上沒有可用的 pwquality.conf，則可使用 pam_cracklib.so 模組來設定 lcredit、ucredit、dcredit 和 ocredit 選項。如需詳細資訊，請參閱man pam_cracklib。

每個選項的預期值小於或等於 -1，如下所示：

```
lcredit <= -1, ucredit <= -1, dcredit<= -1, ocredit <= -1
```

此外，remember 選項必須設定為 12 或更大。如需詳細資訊，請參閱man pam_unix。

啟用 ASLR

此規則有助於判斷是否已啟用評估目標中 EC2 執行個體的作業系統上的地址空間配置隨機化 (ASLR)。

嚴重性

中性

問題清單

評估目標中的 EC2 執行個體未啟用 ASLR。

解決方案

為了改善評估目標的安全性，建議您透過執行 ，在目標中所有 EC2 執行個體的作業系統上啟用 ASLRecho 2 | sudo tee /proc/sys/kernel/randomize_va_space。

啟用 DEP

此規則有助於判斷是否已啟用評估目標中 EC2 執行個體的作業系統上的資料執行預防 (DEP)。

> **Note**
>
> 具有 ARM 處理器的 EC2 執行個體不支援此規則。

嚴重性

中性

問題清單

評估目標中的 EC2 執行個體未啟用 DEP。

解決方案

我們建議您在評估目標中所有 EC2 執行個體的作業系統上啟用 DEP。使用緩衝區溢位技巧啟用 DEP 以保護您的執行個體免受安全威脅。

設定系統目錄許可

此規則會在包含二進位檔和系統組態資訊的系統目錄上檢查許可，確認只有根使用者 (使用根帳戶登入資料登入的使用者) 才具有這些目錄的寫入許可。

嚴重性

高

問題清單

在您評估目標的一個 EC2 執行個體包含非根使用者可寫入的系統目錄。

解決方案

為了改善評估目標的安全性並防止惡意本機使用者提升權限，請將目標中所有 EC2 執行個體上的所有系統目錄設定為只能由使用根帳戶登入資料登入的使用者撰寫。

Amazon Inspector Classic 評估範本和評估執行

Amazon Inspector Classic 透過使用安全規則來分析 AWS 資源，協助您探索潛在的安全問題。Amazon Inspector Classic 會監控和收集資源的行為資料（遙測）。資料包含使用安全頻道、執行中程序之間的網路流量，以及 AWS 與服務通訊的詳細資訊。接著，Amazon Inspector Classic 會分析資料，並將其與一組安全規則套件進行比較。最後，Amazon Inspector Classic 會產生問題清單，以識別各種嚴重性等級的潛在安全問題。

若要開始使用，您可以建立評估目標（您希望 Amazon Inspector Classic 分析 AWS 的資源集合）。接著，請建立評估範本 (用來設定評估的藍圖)。您可使用範本來啟動評估執行，這項監控與分析程序會產生一組調查結果。

主題

Amazon Inspector Classic 評估範本

評估範本可讓您為評估執行指定組態，包括下列項目：

- Amazon Inspector Classic 用來評估評估評估目標的規則套件
- 評估執行的持續時間 – 您可以將評估執行的持續時間設定為 3 分鐘到 24 小時。我們建議將評估執行的持續時間設定為 1 小時。
- Amazon Inspector Classic 傳送評估執行狀態和調查結果通知的 Amazon Amazon SNS 主題
- Amazon Inspector Classic 屬性（鍵/值對），您可以指派給使用此評估範本的評估執行所產生的問題清單

Amazon Inspector Classic 建立評估範本後，您可以像任何其他 AWS 資源一樣標記評估範本。如需詳細資訊，請參閱標籤編輯器。為評估範本加上標籤可讓您組織他們並能更佳地監管您的安全策略。例如，Amazon Inspector Classic 提供許多您可以評估評估目標的規則。您可能需要將各種可用規則子集納入評估範本中，將目標鎖定在特定的關注領域，或找出特定的安全問題。為評估範本加上標籤可讓您隨時根據您的安全策略與目標來快速尋找和執行它們。

> **Important**
>
> 在您建立評估範本後，即無法進行修改。

Amazon Inspector Classic 評估範本限制

您可以為每個 AWS 帳戶建立最多 500 個評估範本。

如需詳細資訊，請參閱Amazon Inspector Classic 服務限制。

建立評估範本

建立評估範本

1. 登入 AWS Management Console ，並在 https：//https://console.aws.amazon.com/inspector/ 開啟 Amazon Inspector Classic 主控台。
2. 在導覽窗格中，選擇 Assessment Templates (評估範本)，然後選擇 Create (建立)。
3. 在 Name (名稱) 中，輸入評估範本的名稱。
4. 對於 Target name (目標名稱)，選擇要分析的評估目標。

> **Note**
>
> 建立評估範本時，您可以使用評估範本頁面上的預覽目標按鈕來檢閱評估目標中包含的所有 EC2 執行個體。對於每個 EC2 執行個體，您可以檢閱主機名稱、執行個體 ID、IP 地址，以及適用的代理程式狀態。代理程式狀態可以有下列值：HEALTHY、UNHEALTHY 和 UNKNOWN。當 Amazon Inspector Classic 無法判斷 EC2 執行個體上是否有執行中的代理程式時，會顯示 UNKNOWN 狀態。
>
> 您也可以使用 Assessment Templates (評估範本) 頁面上的 Preview Target (預覽目標) 按鈕，以檢閱您在之前建立範本中包含之評估目標的組成 EC2 執行個體。

5. 對於 Rules packages (規則套件)，請選擇要包含在評估範本的一或多個規則套件。
6. 在 Duration (持續時間)，指定評估範本的持續時間。
7. （選用）對於 SNS 主題，指定您希望 Amazon Inspector Classic 傳送評估執行狀態和調查結果通知的 SNS 主題。Amazon Inspector Classic 可以傳送下列事件的 SNS 通知：

   - 評估執行已開始
   - 評估執行已結束
   - 評估執行狀態已變更
   - 發現項目已產生

   如需設定 SNS 主題的詳細資訊，請參閱設定 Amazon Inspector Classic 通知的 SNS 主題。
8. (選用) 在 Tag (標記) 中，輸入 Key (金鑰) 和 Value (值) 的值。您可以將多個標籤新增到評估範本。
9. （選用）針對新增至問題清單的屬性，輸入索引鍵和值的值。Amazon Inspector Classic 會將屬性套用至評估範本產生的所有問題清單。您可以將多個屬性新增到評估範本。如需發現項目和標記發現項目的詳細資訊，請參閱 Amazon Inspector Classic 調查結果。
10. (選用) 如果要使用此範本設定執行評估的排程，請選取 Set up recurring assessment runs once every <number_of_days>, starting now (設定從現在開始，每 <number_of_days> 天執行一次重複評估) 核取方塊，並使用上下箭頭指定週期模式 (天數)。

> **Note**
>
> 當您使用此核取方塊時，Amazon Inspector Classic 會自動為您設定的評估執行排程建立 Amazon CloudWatch Events 規則。Amazon Inspector Classic 接著也會自動建立名為的 IAM 角色`AWS_InspectorEvents_Invoke_Assessment_Template`。此角色可讓 CloudWatch Events 對 Amazon Inspector Classic 資源進行 API 呼叫。如需更多資訊，請參閱什麼是 Amazon CloudWatch Events？以及CloudWatch 事件的以資源為基礎的政策。

> **Note**
>
> 您也可以透過 AWS Lambda 函數設定自動評估執行。如需詳細資訊，請參閱設定自動評估會透過 Lambda 函數執行。

11. 選擇 Create and run (建立和執行) 或 Create (建立)。

刪除評估範本

若要刪除評估範本，請執行以下程序。

刪除評估範本

- 在 Assessment Templates (評估範本) 頁面，選擇您要刪除的範本，然後選擇 Delete (刪除)。出現確認提示時，請選擇 Yes (是)。

> **Important**
>
> 當您刪除評估範本時，與此範本相關的所有評估執行、發現項目與報告版本也會刪除。

您也可以使用 `DeleteAssessmentTemplate` API 來刪除評估範本。

評估執行

在建立評估範本後，您可以使用它來開始評估執行。只要您保持在每個 AWS 帳戶的執行限制內，就可以使用相同的範本啟動多個執行。如需詳細資訊，請參閱Amazon Inspector Classic 評估執行限制 。

如果您使用 Amazon Inspector Classic 主控台，則必須從評估範本頁面開始第一次執行新的評估範本。開始執行後，您可以使用 Assessment runs (評估執行) 頁面來監控執行的進度。使用 Run (執行)、Cancel (取消) 和 Delete (刪除) 按鈕來開始、取消或刪除執行。您也可以檢視執行的詳細資訊，包括執行的 ARN、為執行所選取的規則套件、您套用至執行的標記和屬性等等。

對於評估範本的後續執行，您可以使用 Run (執行)、Cancel (取消) 和 Delete (刪除) 按鈕或 Assessment templates (評估範本) 頁面或 Assessment runs (評估執行) 頁面。

刪除評估執行

若要刪除評估執行，請執行以下程序。

刪除執行

- 在 Assessment runs (評估執行) 頁面，選擇您要刪除的執行，然後選擇 Delete (刪除)。出現確認提示時，請選擇 Yes (是)。

> **Important**
>
> 刪除執行時，該執行的所有調查結果和所有報告版本也會一併刪除。

您亦可使用 `DeleteAssessmentRun` API 來刪除執行。

Amazon Inspector Classic 評估執行限制

您可以為每個 AWS 帳戶建立最多 50，000 個評估執行。

只要用於執行的目標不包含重疊的 EC2 執行個體，您可以同時發生多個執行。

如需詳細資訊，請參閱Amazon Inspector Classic 服務限制。

設定自動評估會透過 Lambda 函數執行

如果您想要設定評估的週期性排程，您可以使用 AWS Lambda 主控台建立 Lambda 函數，將評估範本設定為自動執行。如需詳細資訊，請參閱 Lambda 函數。

若要使用 AWS Lambda 主控台設定自動評估執行，請執行下列程序。

若要設定透過 Lambda 函數自動執行

1. 登入 AWS Management Console，然後開啟 AWS Lambda 主控台。
2. 在導覽窗格中，選擇儀表板或函數，然後選擇建立 Lambda 函數。
3. 在 Create function (建立函數) 頁面上，選擇 Browse serverless app repository (瀏覽無伺服器應用程式儲存庫)，然後在搜尋欄位中輸入 **`inspector`**。
4. 選擇 inspector-scheduled-run 藍圖。
5. 在檢閱、設定和部署頁面上，透過指定觸發函數的 CloudWatch 事件來設定自動執行的週期性排程。方法是輸入規則名稱和描述，然後選擇排程表達式。排程表達式決定執行的發生頻率，如每 15 分鐘或每天一次。如需更多有關 CloudWatch 事件和概念的詳細資訊，請參閱什麼是 Amazon CloudWatch Events？

   如果您選取 Enable trigger (啟用觸發條件) 核取方塊，則函數建立完成後，執行就會立即開始。後續自動化執行會依照您在 Schedule expression (排程表達式) 欄位中指定的週期模式。如果在建立函數時不選擇 Enable trigger (啟用觸發) 核取方塊，您可以在稍後編輯該函數以啟用此觸發。

6. 在 Configure function (設定函數) 頁面上，指定下列：

   - 在 Name (名稱) 中，輸入函數的名稱。
   - (選用) 在 Description (描述) 中，輸入可協助您稍後辨識函數的描述。
   - 對於執行時間，請保留預設值 **`Node.js 8.10`**。 僅 AWS Lambda 支援**`Node.js 8.10`**執行時間的 inspector-scheduled-run 藍圖。
   - 您想要使用此函數自動執行的評估範本。您需要為名為 assessmentTemplateArn 的環境變數提供值來執行此操作。
   - 維持處理常式的預設值 **`index.handler`** 設定。
   - 使用 Role (角色) 欄位的函數許可。如需詳細資訊，請參閱 AWS Lambda 許可模型。

     若要執行此函數，您需要一個 IAM 角色， AWS Lambda 允許 啟動執行，並將有關執行的日誌訊息，包括任何錯誤寫入 Amazon CloudWatch Logs。 會針對每個週期性自動執行 AWS Lambda 擔任此角色。例如，您可以將以下範例政策附加到這個 IAM 角色：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "inspector:StartAssessmentRun",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": "*"
    }
  ]
}
```

7. 檢閱您的選項，然後選擇 Create function (建立函數)。

設定 Amazon Inspector Classic 通知的 SNS 主題

Amazon Simple Notification Service (Amazon SNS) 是一項 Web 服務，用於將訊息傳送到訂閱的端點或者用戶端。您可以使用 Amazon SNS 來設定 Amazon Inspector Classic 的通知。

若要為通知設定 SNS 主題

1. 建立 SNS 主題。請參閱 教學課程：建立 Amazon SNS 主題。建立主題時，請展開 Access policy - optional (存取政策 - 選用) 區段。然後執行下列操作來允許評估，以傳送訊息至主題：

   a. 在 Choose method (選擇方法) 中，選擇 Basic (基本)。

   b. 針對定義誰可以發佈訊息到主題，選擇僅限指定的 AWS 帳戶，然後在您要建立主題的區域中輸入帳戶的 ARN：

      - US East (Ohio) - arn:aws:iam::646659390643:root
      - US East (N. Virginia) - arn:aws:iam::316112463485:root
      - US West (N. California) - arn:aws:iam::166987590008:root
      - US West (Oregon) - arn:aws:iam::758058086616:root
      - Asia Pacific (Mumbai) - arn:aws:iam::162588757376:root
      - Asia Pacific (Seoul) - arn:aws:iam::526946625049:root
      - Asia Pacific (Sydney) - arn:aws:iam::454640832652:root
      - Asia Pacific (Tokyo) - arn:aws:iam::406045910587:root
      - Europe (Frankfurt) - arn:aws:iam::537503971621:root
      - Europe (Ireland) - arn:aws:iam::357557129151:root
      - Europe (London) - arn:aws:iam::146838936955:root
      - Europe (Stockholm) - arn:aws:iam::453420244670:root
      - AWS GovCloud (US-East) - arn:aws-us-gov:iam::206278770380:root
      - AWS GovCloud (US-West) - arn:aws-us-gov:iam::850862329162:root

   c. 針對定義誰可以訂閱此主題，選擇僅限指定的 AWS 帳戶，然後在您要建立主題的區域中輸入帳戶的 ARN。

   d. 若要保護自己免於 Inspector 被用作混淆代理人，如 IAM 使用者指南中的混淆代理人問題所述，請執行下列動作：

      i. 選擇 Advanced (進階)。這會將您導覽至 JSON 編輯器。

      ii. 新增下列條件：

```
"Condition": {
   "StringEquals": {
      "aws:SourceAccount": <your account Id here>,
```

```
          "aws:SourceArn": "arn:aws:inspector:*:*:*"
        }
      }
```

e. （選用）如需 aws：SourceAccount 和 aws：SourceArn 的其他資訊，請參閱《IAM 使用者指南》中的全域條件內容金鑰。

f. 視需要更新主題的其他設定，然後選擇 Create topic (建立主題)。

2. （選用）若要建立加密的 SNS 主題，請參閱 SNS 開發人員指南中的靜態加密。

3. 若要保護自己免於 Inspector 被用作 KMS 金鑰的混淆代理人，請遵循下列其他步驟：

a. 前往 KMS 主控台中的 CMK。

b. 選擇編輯。

c. 新增下列條件：

```
"Condition": {
   "StringEquals": {
     "aws:SourceAccount": <your account Id here>,
     "aws:SourceArn": "arn:aws:sns:*:*:*"
   }
 }
```

4. 為您所建立的主題建立訂閱。如需詳細資訊，請參閱 教學課程：讓端點訂閱 Amazon SNS 主題。

5. 若要確認是否正確設定訂閱，請將訊息發佈到主題。如需更多資訊，請參閱 教學課程：將訊息發佈到 Amazon SNS 主題。

Amazon Inspector Classic 調查結果

調查結果是 Amazon Inspector Classic 在評估目標期間發現的潛在安全問題。調查結果會顯示在 Amazon Inspector Classic 主控台或透過 API 顯示。調查結果包含安全問題的詳細描述及建議的解決方法。

在 Amazon Inspector 產生調查結果後，您可以透過將 Amazon Inspector Classic 屬性指派給問題清單來追蹤問題清單。這類屬性是由金鑰值對所構成。

以屬性來追蹤調查結果適合用來管理安全策略的工作流程。例如，建立並執行評估後，就會根據您的安全目標和作法，產生不同程度嚴重性、緊急性和關切性的調查結果清單。您可能會立刻想要執行其中一項問題的建議步驟，解決掉潛在的緊急安全問題。或者，您可能想要將另一個調查結果延後到下一次即將到來的服務更新時再解決。舉例而言，若要追蹤某個問題，並立即加以處理，您可建立一個含 **`Status`** / **`Urgent`** 索引鍵/值組的屬性，並將之分配給該問題。也可以使用屬性來分配負責解決潛在安全問題的工作量。舉例而言，若要將解決某個問題的工作交派給 Bob (團隊中的安全工程師)，則可將含有 **`Assigned Engineer`** / **`Bob`** 索引鍵/值組的屬性指派給問題。

使用問題清單

針對任何產生的 Amazon Inspector Classic 調查結果，完成下列程序。

尋找、分析、指派屬性給問題

1. 登入 AWS Management Console ，並在 https://console.aws.amazon.com/inspector/ : // 開啟 Amazon Inspector Classic 主控台。
2. 執行評估後，導覽至 Amazon Inspector Classic 主控台中的調查結果頁面，以檢視您的調查結果。

   您也可以在 Amazon Inspector Classic 主控台儀表板頁面上的顯著調查結果區段中查看您的調查結果。

> **Note**
>
> 若評估執行仍在進行中，您無法檢視其所產生的調查結果。不過若在評估完成前就停止評估，則可檢視問題清單的子集。在生產環境中則建議讓每次評估完整執行所需的評估時間，方能產生完整的問題清單。

3. 若要檢視特定問題清單的詳細資訊，請選擇該問題旁的 Expand (展開) 小工具。問題清單的詳細資訊包含下列項目：

   - 評估目標的名稱，其中包含已註冊此調查結果的 EC2 執行個體。
   - 用於產生此調查結果的評估範本名稱。
   - 評估執行開始時間。
   - 評估執行結束時間。
   - 評估執行狀態。
   - 規則套件的名稱，其中包含觸發此調查結果的規則。
   - 調查結果的名稱。
   - 調查結果的嚴重性。
   - 來自通用漏洞評分系統 (CVSS) 的原生嚴重性詳細資訊。其中包括調查結果 (由常見弱點與漏洞規則套件中的規則所觸發) 的 CVSS 向量和 CVSS 分數指標 (包括 CVSS 2.0 和 3.0 版)。如需 CVSS 的詳細資訊，請參閱 https://www.first.org/cvss/。
   - 來自網際網路安全中心 (CIS) 的原生嚴重性詳細資訊。其中包括調查結果 (由 CIS 基準參考指標套件中的規則所觸發) 的 CIS 權重指標。如需 CIS 權重的詳細資訊，請參閱 https://www.cisecurity.org/。
   - 調查結果的描述。
   - 您可完成的建議步驟，藉以修復調查結果所描述的潛在安全問題。

4. 請將屬性分配給問題，再選擇 Add/Edit Attributes (新增/編輯屬性)。

   您亦可在建立評估範本時將屬性指派給調查結果，方法是將新的範本設定為自動指派屬性給評估執行所產生的所有調查結果。您可以從此評估欄位中的 Tags 中使用金鑰和值欄位，以取得調查結果。 如需詳細資訊，請參閱Amazon Inspector Classic 評估範本和評估執行。

5. 若要將調查結果匯出為試算表，請選擇 Findings (調查結果) 頁面右上角的向下箭頭。在對話方塊中，選擇 Export all columns (匯出所有欄) 或 Export visible columns (匯出可見欄)。

   請注意，在匯出的內容中，所有日期時間值皆為 Epoch 時間戳記。

6. 若要篩選您目前的問題清單，請在問題清單上方的篩選列中輸入您要篩選的單一字串，例如執行個體 ID 或 CVE 編號。若要顯示或隱藏其他資訊欄，請選擇調查結果頁面右上角的設定圖示。

7. 若要刪除調查結果，請前往 Assessment runs (評估執行) 頁面，然後選擇產生您欲刪除的調查結果之執行。然後選擇 Delete (刪除)。出現確認提示時，請選擇 Yes (是)。

> **Important**
>
> 您無法刪除 Amazon Inspector Classic 中的個別問題清單。當您刪除評估執行時，報告的所有發現項目和所有版本也會從該執行中刪除。

您也可透過執行 DeleteAssessmentRun API 來刪除評估執行。

評估報告

Amazon Inspector Classic 評估報告是一種文件，詳細說明評估執行中測試的內容和評估結果。您可以存放報告、分享給團隊來決定補救動作，或用來加強合規稽核資料。評估執行成功完成後，您可為該次執行產生報告。

> **Note**
>
> 您只能針對 2017 年 4 月 25 日之後發生的評估執行產生報告，也就是 Amazon Inspector Classic 中的評估報告變得可用時。

您可以檢視以下類型的評估報告：

- 調查結果報告 – 此報告包含下列資訊：
  - 評估摘要
  - 評估執行期間的 EC2 執行個體評估
  - 評估執行中包含的規則套件
  - 每個問題清單的詳細資訊，包括所有 EC2 執行個體的問題清單
- 完整報告 – 此報告包含調查結果報告中包含的所有資訊，並另外提供針對評估目標中的執行個體檢查的規則清單。

產生評估報告

1. 在 Assessment runs (評估執行) 頁面，找出您想要產生報告的評估執行。請確定其狀態已設為 Analysis complete (分析完成)。
2. 在 Reports (報告) 欄下方選擇此次評估執行的報告圖示。

   > **Important**
   >
   > 從 2025 年 3 月 24 日開始，評估報告將不再包含網路連線能力調查結果的嚴重性資訊。此資訊可在 Amazon Inspector 主控台中取得。

3. 在 Assessment report (評估報告) 對話方塊中，選擇您要檢視的報告類型 (調查結果或完整報告) 及報告格式 (HTML 或 PDF)。接著選擇 Generate report (產生報告)。

您亦可透過 GetAssessmentReport API 來產生評估報告。

若要刪除評估報告，請執行以下程序。

刪除報告

- 在 Assessment runs (評估執行) 頁面，選擇您要刪除的執行報告，然後選擇 Delete (刪除)。出現確認提示時，請選擇 Yes (是)。

  > **Important**
  >
  > 在 Amazon Inspector Classic 中，您無法刪除個別報告。當您刪除評估執行時，該執行的所有報告版本和所有問題清單也都會被刪除。

  您也可以使用 DeleteAssessmentRun API 來刪除評估執行。

Amazon Inspector Classic 中的排除項目

排除是 Amazon Inspector Classic 評估執行的輸出。排除會顯示哪些安全性檢查無法完成，以及應如何解決這些問題。例如，問題可能是因為指定的目標 EC2 執行個體上沒有代理程式、使用不支援的作業系統，或發生未預期的錯誤。

您可在主控台的 Assessment runs (評估執行) 頁面上檢視排除。如需詳細資訊，請參閱檢視後續評估排除。

為了避免產生不必要的 AWS 費用，Amazon Inspector Classic 可讓您在執行評估之前預覽排除項目。您可在主控台的 Assessment templates (評估範本) 頁面找到預覽。如需詳細資訊，請參閱預覽排除。

> **Note**
>
> 只有在 2018 年 6 月 25 日之後發生的執行，才可以產生後續評估排除。這就是 Amazon Inspector Classic 中的排除變得可用的時候。不過，無論哪一天，所有評估範本都有排除預覽可用。

主題

排除類型

Amazon Inspector Classic 可以產生下列排除類型。

排除類型	描述	建議
目標中	評估目標中沒有指定帶有標籤的	檢查在評估目標中的標籤符合您的

排除類型	描述	建議
無執行個體	EC2 執行個體。	目標 EC2 執行個體標籤。
代理程式已在執行	評估執行已在目標 EC2 執行個體上進行中。	等待至目標 EC2 執行個體上的目前評估執行完成。
找不到代理程式	在目標 EC2 執行個體上找不到 Amazon Inspector Classic 代理程式。	在目標 EC2 執行個體上安裝或重新安裝 Amazon Inspector Classic 代理程式。如需詳細資訊，請參閱安裝 Amazon Inspector Classic 代理程式。

排除類型	描述	建議
代理程式運作狀態不佳	目標 EC2 執行個體上的 Amazon Inspector Classic 代理程式處於運作狀態不佳的狀態。	檢查此執行個體上 Amazon Inspector Classic 代理程式的狀態，並採取必要的動作。如需詳細資訊，請參閱 Inspector 代理程式。
支援的作業系統版本	Amazon Inspector Classic 評估不支援目標 EC2 執行個體的作業系統。	從評估目標中移除目標 EC2 執行個體，或建立不包含此執行個體的目標。如需支援的作業系統清單，請參閱 Amazon Inspector Classic Supported 作業系統和區域。

排除類型	描述	建議
已停用的規則套件	該評估範本包含一個已停用的規則套件。	建立不含已棄用規則套件的評估範本，並用於未來的評估執行。
作業系統不支援的規則套件	包含在評估範本中的規則套件不支援目標 EC2 執行個體的作業系統。	建立一個沒有相衝突規則套件的評估範本，或從評估範本移除目標 EC2 執行個體。如需作業系統支援的規則套件清單，請參閱 所有支援作業系統的規則套件可用性。

排除類型	描述	建議
單一執行個體的規則評估錯誤	內部錯誤造成此執行個體的規則評估失敗。	嘗試再次執行您的評估。重新執行評估時，若排除持續存在，請聯絡支援部門。
規則評估錯誤	內部錯誤造成評估的規則評估失敗。	嘗試再次執行評估。重新執行評估時，若排除持續存在，請聯絡支援部門。

排除類型	描述	建議
網路連線能力錯誤 – 網際網路	在檢查是否可從網際網路連結至連接埠時，內部錯誤造成網路連線能力評估失敗。您可能會得到其他網路連線能力類型的調查結果。	嘗試再次執行評估。重新執行評估時，若排除持續存在，請聯絡支援部門。

排除類型	描述	建議
網路可連線性錯誤 – 透過 Application Load Balancer 進行網際網路	在檢查可透過 Application Load Balancer 從網際網路連線的連接埠時，內部錯誤導致網路連線能力評估失敗。您可能會得到其他網路連線能力類型的調查結果。	嘗試再次執行評估。重新執行評估時，若排除持續存在，請聯絡支援部門。

排除類型	描述	建議
網路連線能力錯誤 – 透過 Elastic Load Balancing 負載平衡器的網際網路	在檢查可透過 Elastic Load Balancing 負載平衡器從網際網路連線的連接埠時，內部錯誤導致網路連線能力評估失敗。您可能會得到其他網路連線能力類型的調查結果。	嘗試再次執行評估。重新執行評估時，若排除持續存在，請聯絡支援部門。

排除類型	描述	建議
網路連線能力錯誤 – VPN	在檢查可從 VPN 到達的連接埠時，內部錯誤造成網路連線能力評估失敗。您可能會得到其他網路連線能力類型的調查結果。	嘗試再次執行評估。重新執行評估時，若排除持續存在，請聯絡支援部門。
網路連線能力錯誤 – AWS Direct Conne	內部錯誤導致網路連線能力評估在檢查可連線的連接埠時失敗 AWS Direct Connect。您可能會得到其他網路連線能力類型的調查結果。	嘗試再次執行評估。重新執行評估時，若排除持續存在，請聯絡支援部門。

排除類型	描述	建議
網路連線能力錯誤 – VPC 對等互連	在檢查可從互連 VPC 到達的連接埠時，內部錯誤造成網路連線能力評估失敗。您可能會得到其他網路連線能力類型的調查結果。	嘗試再次執行評估。重新執行評估時，若排除持續存在，請聯絡支援部門。

預覽排除

Amazon Inspector Classic 可讓您在執行評估之前預覽潛在的排除項目。

預覽評估排除

1. 登入 AWS Management Console 並開啟位於 https：//https://console.aws.amazon.com/inspector/ 的 Amazon Inspector Classic 主控台。
2. 在導覽窗格中，選擇 Assessment templates (評估範本)。
3. 展開範本，在 Assessment templates (評估範本) 區段中選擇 Preview exclusions (預覽排除)。
4. 檢視所有偵測到的排除描述和因應建議。

   您也可使用 `ListExclusions` 和 `DescribeExclusions` 操作來列出並描述排除。

檢視後續評估排除

評估執行後，您可以檢視排除的詳細資訊。

檢視排除的詳細資訊

1. 登入 AWS Management Console 並開啟位於 https：//https://console.aws.amazon.com/inspector/ 的 Amazon Inspector Classic 主控台。
2. 在導覽窗格中，選擇 Assessment runs (評估執行)。
3. 在 Exclusions (排除) 欄中，選擇與評估執行相關聯的作用中連結。
4. 檢視所有偵測到的排除描述和因應建議。

   您也可使用 `ListExclusions` 和 `DescribeExclusions` 操作來列出並描述排除。

支援作業系統的 Amazon Inspector Classic 規則套件

您可以在評估目標中包含的 EC2 執行個體上執行 Amazon Inspector Classic 規則套件。下表顯示受支援作業系統的規則套件可用性。

Important

無論作業系統為何，您都可以在任何 EC2 執行個體上使用 Network Reachability 規則套件執行無代理程式評估。

Note

如需支援的作業系統詳細資訊，請參閱 Amazon Inspector Classic 支援的作業系統和區域。

支援的作業系統	Common Vulnerabilities and Exposures	CIS 基準參考指標	網路連線能力	安全最佳實務	執行時間行為分析
Amaz Linux 2	支援	支援	支援	支援	已棄用
Amaz Linux 2018.	支援	支援	支援	支援	已棄用
Amaz Linux 2017.	支援	支援	支援	支援	已棄用

支援的作業系統	Common Vulnerabilities and Exposures	CIS 基準參考指標	網路連線能力	安全最佳實務	執行時間行為分析
Amaz Linux 2017.	支援	支援	支援	支援	已棄用
Amaz Linux 2016.	支援	支援	支援	支援	已棄用
Amaz Linux 2016.	支援	支援	支援	支援	已棄用
Amaz Linux 2015.	支援	支援	支援	支援	已棄用
Amaz Linux 2015.	支援	支援	支援	支援	已棄用
Amaz Linux 2014.	支援		支援	支援	
Amaz Linux 2014.	支援		支援	支援	

支援的作業系統	Common Vulnerabilities and Exposures	CIS 基準參考指標	網路連線能力	安全最佳實務	執行時間行為分析
Amaz Linux 2013.	支援		支援	支援	
Amaz Linux 2013.	支援		支援	支援	
Amaz Linux 2012.	支援		支援	支援	
Amaz Linux 2012.	支援		支援	支援	
Ubun 20.04 LTS	支援		支援	支援	
Ubun 18.04 LTS	支援	支援	支援	支援	已棄用
Ubun 16.04 LTS	支援	支援	支援	支援	已棄用

支援的作業系統	Common Vulnerabilities and Exposures	CIS 基準參考指標	網路連線能力	安全最佳實務	執行時間行為分析
Ubun 14.04 LTS	支援	支援	支援	支援	已棄用
Debia 10.x、- 9.5、- 8.7	支援		支援	支援	
RHEl 8.x	支援		支援	支援	
RHEl 7.6 - 7.x	支援	支援	支援	支援	
RHEl 6.2 - 6.9, 7.2 - 7.5	支援	支援	支援	支援	已棄用

支援的作業系統	Common Vulnerabilities and Exposures	CIS 基準參考指標	網路連線能力	安全最佳實務	執行時間行為分析
Cent(7.6 - 7.X	支援	支援	支援	支援	
Cent(6.2 - 6.9, 7.2 - 7.5	支援	支援	支援	支援	已棄用
Wind(Serve 2019 Base	支援		支援		
Wind(Serve 2016 Base	支援	支援	支援		已棄用
Wind(Serve 2012 R2	支援	支援	支援		已棄用

支援的作業系統	Common Vulnerabilities and Exposures	CIS 基準參考指標	網路連線能力	安全最佳實務	執行時間行為分析
Windows Server 2012	支援	支援	支援		已棄用
Windows Server 2008 R2	支援	支援	支援		已棄用

使用 記錄 Amazon Inspector Classic API 呼叫 AWS CloudTrail

Amazon Inspector Classic 已與 整合 AWS CloudTrail，此服務提供 Amazon Inspector Classic AWS 中使用者、角色或服務所採取動作的記錄。CloudTrail 會將 Amazon Inspector Classic 的所有 API 呼叫擷取為事件，包括來自 Amazon Inspector Classic 主控台的呼叫，以及對 Amazon Inspector Classic API 操作的程式碼呼叫。如果您建立線索，您可以啟用 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 Amazon Inspector Classic 的事件。即使您未設定追蹤，依然可以透過 CloudTrail 主控台中的 Event history (事件歷史記錄) 檢視最新事件。使用 CloudTrail 收集的資訊，您可以判斷對 Amazon Inspector Classic 提出的請求、提出請求的 IP 地址、提出請求的人員、提出請求的時間等。

若要進一步了解 CloudTrail，請參閱「AWS CloudTrail 使用者指南」。如需 Amazon Inspector Classic API 操作的完整清單，請參閱《Amazon Inspector Classic API 參考》中的動作。

CloudTrail 中的 Amazon Inspector Classic 資訊

當您建立 AWS 帳戶時，會在您的帳戶上啟用 CloudTrail。當 Amazon Inspector Classic 中發生活動時，該活動會記錄於 CloudTrail 事件，以及事件歷史記錄中的其他服務 AWS 事件。您可以檢視、搜尋和下載 AWS 帳戶的最新事件。如需詳細資訊，請參閱使用 CloudTrail 事件歷史記錄檢視事件。

若要持續記錄您 AWS 帳戶中的事件，包括 Amazon Inspector Classic 的事件，請建立追蹤。線索能讓 CloudTrail 將日誌檔案交付至 Amazon S3 儲存貯體。在主控台建立追蹤記錄時，該追蹤記錄預設會套用到所有 AWS 區域。追蹤會記錄 AWS 分割區中所有 區域的事件，並將日誌檔案交付至您指定的 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 日誌中收集的事件資料並對其採取行動。如需詳細資訊，請參閱下列內容：

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

CloudTrail 會記錄所有 Amazon Inspector Classic 操作，包括唯讀操作，例如 `ListAssessmentRuns`和 `DescribeAssessmentTargets`，以及管理操作，例如 `AddAttributesToFindings`和 `CreateAssessmentTemplate`。

> **Note**
>
> CloudTrail 只會記錄 Amazon Inspector Classic 唯讀操作的請求資訊。所有其他 Amazon Inspector Classic 操作都會記錄請求和回應資訊。

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 請求是使用根還是 AWS Identity and Access Management (IAM) 使用者登入資料提出
- 提出該請求時，是否使用了特定角色或聯合身分使用者的臨時安全憑證
- 該請求是否由其他 AWS 服務提出

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

了解 Amazon Inspector Classic 日誌檔案項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一或多個日誌專案。事件代表來自任何來源的單一請求，並包含所請求動作、動作日期和時間，以及其他請求參數的相關資訊。CloudTrail 日誌檔並非依公有 API 呼叫的堆疊追蹤排序，因此不會以任何特定順序出現。

下列範例顯示示範 Amazon Inspector Classic `CreateResourceGroup`操作的 CloudTrail 日誌項目：

```
{
    "eventVersion": "1.03",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::444455556666:user/Alice",
        "accountId": "444455556666",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2016-04-14T17:05:54Z"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
```

```
                "arn": "arn:aws:iam::444455556666:user/Alice",
                "accountId": "444455556666",
                "userName": "Alice"
            }
        }
    },
    "eventTime": "2016-04-14T17:12:34Z",
    "eventSource": "inspector.amazonaws.com",
    "eventName": "CreateResourceGroup",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.179",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "resourceGroupTags": [
            {
                "key": "Name",
                "value": "ExampleEC2Instance"
            }
        ]
    },
    "responseElements": {
        "resourceGroupArn": "arn:aws:inspector:us-west-2:444455556666:resourcegroup/0-
oclRMp8B"
    },
    "requestID": "148256d2-0264-11e6-a9b5-b98a7d3b840f",
    "eventID": "e5ea533e-eede-46cc-94f6-0d08e6306ff0",
    "eventType": "AwsApiCall",
    "apiVersion": "v20160216",
    "recipientAccountId": "444455556666"
}
```

使用 Amazon CloudWatch 監控 Amazon Inspector Classic Amazon CloudWatch

您可以使用 Amazon CloudWatch 來監控 Amazon Inspector Classic，它會將原始資料收集並處理為可讀、近乎即時的指標。 Amazon CloudWatch 根據預設，Amazon Inspector Classic 會在 5 分鐘內將指標資料傳送至 CloudWatch。您可以使用 AWS Management Console、 AWS CLI或 API 來檢視 Amazon Inspector Classic 傳送至 CloudWatch 的指標。

如需 Amazon CloudWatch 的詳細資訊，請參閱《Amazon CloudWatch 使用者指南》。

Amazon Inspector Classic CloudWatch 指標

Amazon Inspector Classic 命名空間包含下列指標。

`AssessmentTargetARN` 指標：

指標	描述
`TotalMatchingAgents`	符合此目標的代理程式數量
`TotalHealthyAgents`	符合此目標且狀況良好的代理程式數量
`TotalAssessmentRuns`	對此目標執行的評估數量
`TotalAssessmentRunFindings`	此目標的問題數量

`AssessmentTemplateARN` 指標：

指標	描述
`TotalMatchingAgents`	符合此範本的代理程式數量
`TotalHealthyAgents`	符合此範本且狀況良好的代理程式數量
`TotalAssessmentRuns`	對此範本執行的評估數量

指標	描述
TotalAssessmentRun Findings	此範本的問題數量

彙總指標

指標	描述
TotalAssessmentRuns	此 AWS 帳戶中執行的評估數目

使用 設定 Amazon Inspector Classic AWS CloudFormation

如需 支援的 Amazon Inspector Classic 資源的參考資訊 AWS CloudFormation，請參閱下列主題：

- `AWS::Inspector::AssessmentTarget`
- `AWS::Inspector::AssessmentTemplate`
- `AWS::Inspector::ResourceGroup`

> **Important**
>
> 如需支援 AWS 區域中 Amazon Inspector Classic 規則套件ARNs 清單，請參閱 適用於規則套件的 Amazon Inspector Classic ARNS。

與 整合 AWS Security Hub

AWS Security Hub 為您提供 中安全狀態的完整檢視， AWS 並協助您根據安全產業標準和最佳實務來檢查環境。Security Hub 會從 AWS 帳戶、服務和支援的第三方合作夥伴產品中收集安全資料，並協助您分析安全趨勢並識別最高優先順序的安全問題。

Amazon Inspector 與 Security Hub 的整合可讓您將問題清單從 Amazon Inspector 傳送至 Security Hub。Security Hub 接著可將這些問題清單納入其安全狀態的分析中。

內容

Amazon Inspector 如何將調查結果傳送至 Security Hub

在 Security Hub 中，將安全問題作為問題清單進行追蹤。有些問題清單來自其他服務 AWS 或第三方合作夥伴偵測到的問題。Security Hub 也有一組規則，用來偵測安全問題並產生問題清單。

Security Hub 提供用來跨所有這些來源管理問題清單的工具。您可以檢視並篩選問題清單列表，並檢視問題清單的詳細資訊。請參閱 AWS Security Hub 使用者指南中的檢視問題清單。您也可以追蹤問題清單的調查狀態。請參閱 AWS Security Hub 使用者指南中的對問題清單採取動作。

Security Hub 中的所有問題清單都使用稱為 AWS 安全問題清單格式 (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 安全調查結果格式 (ASFF)。

Amazon Inspector 是將問題清單傳送到 Security Hub 的其中一項 AWS 服務。

Amazon Inspector 傳送的調查結果類型

Amazon Inspector 會將產生的所有調查結果傳送至 Security Hub。

Amazon Inspector 使用安全調查結果AWS 格式 (ASFF) 將調查結果傳送至 Security Hub。在 ASFF 中，Types 欄位提供問題清單類型。Amazon Inspector 的調查結果可以具有下列 值Types。

- 軟體和組態Checks/Vulnerabilities/CVE
- 軟體和組態檢查/AWS 安全最佳實務/網路連線能力
- 軟體和組態檢查/產業和法規標準/CIS 主機強化基準

傳送問題清單延遲

當 Amazon Inspector 建立新的問題清單時，通常會在五分鐘內傳送至 Security Hub。

無法使用 Security Hub 時重試

如果 Security Hub 無法使用，Amazon Inspector 會重試傳送問題清單，直到收到問題清單為止。

更新 Security Hub 中的現有問題清單

將問題清單傳送至 Security Hub 後，Amazon Inspector 會更新問題清單，以反映問題清單活動的其他觀察。這會導致 Security Hub 中的 Amazon Inspector 調查結果少於 Amazon Inspector。

Amazon Inspector 的典型調查結果

Amazon Inspector 使用安全調查結果AWS 格式 (ASFF) 將調查結果傳送至 Security Hub。

以下是 Amazon Inspector 的典型調查結果範例。


```
{
  "SchemaVersion": "2018-10-08",
  "Id": "inspector/us-east-1/111122223333/629ff13fbbb44c872f7bba3e7f79f60cb6d443d8",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/inspector",
  "GeneratorId": "arn:aws:inspector:us-east-1:316112463485:rulespackage/0-PmNV0Tcd",
  "AwsAccountId": "111122223333",
  "Types": [
    "Software and Configuration Checks/AWS Security Best Practices/Network Reachability
 - Recognized port reachable from internet"
  ],
  "CreatedAt": "2020-08-19T17:36:22.169Z",
  "UpdatedAt": "2020-11-04T16:36:06.064Z",
  "Severity": {
    "Label": "MEDIUM",
```

```
    "Normalized": 40,
    "Original": "6.0"
  },
  "Confidence": 10,
  "Title": "On instance i-0c10c2c7863d1a356, TCP port 22 which is associated with 'SSH'
 is reachable from the internet",
  "Description": "On this instance, TCP port 22, which is associated with SSH, is
 reachable from the internet. You can install the Inspector agent on this instance
 and re-run the assessment to check for any process listening on this port. The
 instance i-0c10c2c7863d1a356 is located in VPC vpc-a0c2d7c7 and has an attached ENI
 eni-078eac9d6ad9b20d1 which uses network ACL acl-154b8273. The port is reachable from
 the internet through Security Group sg-0af64c8a5eb30ca75 and IGW igw-e209d785",
  "Remediation": {
    "Recommendation": {
      "Text": "You can edit the Security Group sg-0af64c8a5eb30ca75 to remove access
 from the internet on port 22"
    }
  },
  "ProductFields": {
    "attributes/VPC": "vpc-a0c2d7c7",
    "aws/inspector/id": "Recognized port reachable from internet",
    "serviceAttributes/schemaVersion": "1",
    "aws/inspector/arn": "arn:aws:inspector:us-east-1:111122223333:target/0-8zh1cWkg/
template/0-rqtRV0u0/run/0-Ck2F6tY9/finding/0-B458MQWe",
    "attributes/ACL": "acl-154b8273",
    "serviceAttributes/assessmentRunArn": "arn:aws:inspector:us-
east-1:111122223333:target/0-8zh1cWkg/template/0-rqtRV0u0/run/0-Ck2F6tY9",
    "attributes/PROTOCOL": "TCP",
    "attributes/RULE_TYPE": "RecognizedPortNoAgent",
    "aws/inspector/RulesPackageName": "Network Reachability",
    "attributes/INSTANCE_ID": "i-0c10c2c7863d1a356",
    "attributes/PORT_GROUP_NAME": "SSH",
    "attributes/IGW": "igw-e209d785",
    "serviceAttributes/rulesPackageArn": "arn:aws:inspector:us-
east-1:111122223333:rulespackage/0-PmNV0Tcd",
    "attributes/SECURITY_GROUP": "sg-0af64c8a5eb30ca75",
    "attributes/ENI": "eni-078eac9d6ad9b20d1",
    "attributes/REACHABILITY_TYPE": "Internet",
    "attributes/PORT": "22",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/inspector/
inspector/us-east-1/111122223333/629ff13fbbb44c872f7bba3e7f79f60cb6d443d8",
    "aws/securityhub/ProductName": "Inspector",
    "aws/securityhub/CompanyName": "Amazon"
  },
```

```
  "Resources": [
    {
      "Type": "AwsEc2Instance",
      "Id": "arn:aws:ec2:us-east-1:193043430472:instance/i-0c10c2c7863d1a356",
      "Partition": "aws",
      "Region": "us-east-1",
      "Tags": {
        "Name": "kubectl"
      },
      "Details": {
        "AwsEc2Instance": {
          "ImageId": "ami-02354e95b39ca8dec",
          "IpV4Addresses": [
            "172.31.43.6"
          ],
          "VpcId": "vpc-a0c2d7c7",
          "SubnetId": "subnet-4975b475"
        }
      }
    }
  ],
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE"
}
```


啟用與設定整合

若要使用與 Security Hub 的整合，您必須啟用 Security Hub。如需有關如何啟用 Security Hub 的資訊，請參閱 AWS Security Hub 使用者指南中的設定 Security Hub。

當您同時啟用 Amazon Inspector 和 Security Hub 時，會自動啟用整合。Amazon Inspector 開始將問題清單傳送至 Security Hub。

如何停止傳送問題清單

若要停止將問題清單傳送至 Security Hub，您可以使用 Security Hub 主控台或 API。

請參閱AWS Security Hub 《使用者指南》中的停用和啟用來自整合的調查結果流程（主控台）或停用來自整合的調查結果流程 (Security Hub API、AWS CLI)。

Amazon Inspector Classic ARNs

Amazon Inspector Classic 中的每個資源類型和規則套件都有與其相關聯的唯一 Amazon Resource Name (ARN)。

內容

Amazon Inspector Classic 資源ARNs

在 Amazon Inspector Classic 中，主要資源是資源群組、評估目標、評估範本、評估執行和調查結果。這些資源都有與其相關的唯一 Amazon Resource Name (ARN)，如下表所示。

資源類型	ARN 格式
資源群組	`arn:aws:inspector:` *`region`*`:`*`account-id`* `:resource group/` *`ID`*

資源類型	ARN 格式
評估目標	arn:aws:inspector: *region*:*account-id* :target/*ID*
評估範本	arn:aws:inspector: *region*:*account-id* :target/*ID*:template: *ID*
評估執行	arn:aws:inspector: *region*:*account-id* :target/*ID*/template/ *ID*/run/*ID*
問題清單	arn:aws:inspector: *region*:*account-id* :target/*ID*/template/ *ID*/run/*ID*/finding/ *ID*

適用於規則套件的 Amazon Inspector Classic ARNS

下表顯示所有支援區域中 Amazon Inspector Classic 規則套件的 ARNs。

主題

- 美國東部 (俄亥俄)
- 美國東部 (維吉尼亞北部)
- 美國西部 (加利佛尼亞北部)
- 美國西部 (奧勒岡)
- 亞太區域 (孟買)
- 亞太區域 (首爾)
- 亞太區域 (悉尼)
- 亞太區域 (東京)
- 歐洲 (法蘭克福)
- 歐洲 (愛爾蘭)
- 歐洲 (倫敦)
- 歐洲 (斯德哥爾摩)
- AWS GovCloud （美國東部）
- AWS GovCloud （美國西部）

美國東部 (俄亥俄)

規則套件名稱	ARN
Common Vulnerabilities and Exposures	arn:aws:inspector:us-east-2:646659390643:rulespackage/0-JnA8Zp85
CIS 作業系統安全組態基準參考指標	arn:aws:inspector:us-east-2:646659390643:rulespackage/0-m8r61nnh
網路連線能力	arn:aws:inspector:us-east-2:646659390643:rulespackage/0-cE4kTR30
安全最佳實務	arn:aws:inspector:us-east-2:646659390643:rulespackage/0-AxKmMHPX

美國東部 (維吉尼亞北部)

規則套件名稱	ARN
Common Vulnerabilities and Exposures	arn:aws:inspector:us-east-1:316112463485:rulespackage/0-gEjTy7T7
CIS 作業系統安全組態基準參考指標	arn:aws:inspector:us-east-1:31611246

規則套件名稱	ARN
	3485:rulespackage/0-rExsr2X8
網路連線能力	arn:aws:inspector:us-east-1:316112463485:rulespackage/0-PmNV0Tcd
安全最佳實務	arn:aws:inspector:us-east-1:316112463485:rulespackage/0-R01qwB5Q

美國西部 (加利佛尼亞北部)

規則套件名稱	ARN
Common Vulnerabilities and Exposures	arn:aws:inspector:us-west-1:166987590008:rulespackage/0-TKgzoVOa
CIS 作業系統安全組態基準參考指標	arn:aws:inspector:us-west-1:166987590008:rulespackage/0-xUY8iRqX
網路連線能力	arn:aws:inspector:us-west-1:166987590008:rulespackage/0-TxmXimXF
安全最佳實務	arn:aws:inspector:us-west-1:16698759

規則套件名稱	ARN
	0008:rulespackage/0-byoQRFYm

美國西部 (奧勒岡)

規則套件名稱	ARN
Common Vulnerabilities and Exposures	arn:aws:inspector:us-west-2:758058086616:rulespackage/0-9hgA516p
CIS 作業系統安全組態基準參考指標	arn:aws:inspector:us-west-2:758058086616:rulespackage/0-H5hpSawc
網路連線能力	arn:aws:inspector:us-west-2:758058086616:rulespackage/0-rD1z6dpl
安全最佳實務	arn:aws:inspector:us-west-2:758058086616:rulespackage/0-JJOtZiqQ

亞太區域 (孟買)

規則套件名稱	ARN
Common Vulnerabilities and Exposures	arn:aws:inspector:ap-south-1:1625887

規則套件名稱	ARN
	57376:rulespackage/0-LqnJE9dO
CIS 作業系統安全組態基準參考指標	arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-PSUlX14m
網路連線能力	arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-YxKfjFu1
安全最佳實務	arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-fs0IZZBj

亞太區域 (首爾)

規則套件名稱	ARN
Common Vulnerabilities and Exposures	arn:aws:inspector:ap-northeast-2:526946625049:rulespackage/0-PoGHMznc
CIS 作業系統安全組態基準參考指標	arn:aws:inspector:ap-northeast-2:526946625049:rulespackage/0-T9srhg1z
網路連線能力	arn:aws:inspector:ap-northeast-2:526

規則套件名稱	ARN
	946625049:rulespac kage/0-s3OmLzhL
安全最佳實務	arn:aws:inspector: ap-northeast-2:526 946625049:rulespac kage/0-2WRpmi4n

亞太區域 (悉尼)

規則套件名稱	ARN
Common Vulnerabilities and Exposures	arn:aws:inspector: ap-southeast-2:454 640832652:rulespac kage/0-D5TGAxiR
CIS 作業系統安全組態基準參考指標	arn:aws:inspector: ap-southeast-2:454 640832652:rulespac kage/0-Vkd2Vxjq
網路連線能力	arn:aws:inspector: ap-southeast-2:454 640832652:rulespac kage/0-FLcuV4Gz
安全最佳實務	arn:aws:inspector: ap-southeast-2:454 640832652:rulespac kage/0-asL6HRgN

亞太區域 (東京)

規則套件名稱	ARN
Common Vulnerabilities and Exposures	arn:aws:inspector:ap-northeast-1:406045910587:rulespackage/0-gHP9oWNT
CIS 作業系統安全組態基準參考指標	arn:aws:inspector:ap-northeast-1:406045910587:rulespackage/0-7WNjqgGu
網路連線能力	arn:aws:inspector:ap-northeast-1:406045910587:rulespackage/0-YI95DVd7
安全最佳實務	arn:aws:inspector:ap-northeast-1:406045910587:rulespackage/0-bBUQnxMq

歐洲 (法蘭克福)

規則套件名稱	ARN
Common Vulnerabilities and Exposures	arn:aws:inspector:eu-central-1:537503971621:rulespackage/0-wNqHa8M9
CIS 作業系統安全組態基準參考指標	arn:aws:inspector:eu-central-1:53750

規則套件名稱	ARN
	3971621:rulespackage/0-nZrAVuv8
網路連線能力	arn:aws:inspector:eu-central-1:537503971621:rulespackage/0-6yunpJ91
安全最佳實務	arn:aws:inspector:eu-central-1:537503971621:rulespackage/0-ZujVHEPB

歐洲 (愛爾蘭)

規則套件名稱	ARN
Common Vulnerabilities and Exposures	arn:aws:inspector:eu-west-1:357557129151:rulespackage/0-ubA5XvBh
CIS 作業系統安全組態基準參考指標	arn:aws:inspector:eu-west-1:357557129151:rulespackage/0-sJBhCr0F
網路連線能力	arn:aws:inspector:eu-west-1:357557129151:rulespackage/0-SPzU33xe
安全最佳實務	arn:aws:inspector:eu-west-1:35755712

規則套件名稱	ARN
	9151:rulespackage/0-SnojL3Z6

歐洲 (倫敦)

規則套件名稱	ARN
Common Vulnerabilities and Exposures	arn:aws:inspector:eu-west-2:146838936955:rulespackage/0-kZGCqcE1
CIS 作業系統安全組態基準參考指標	arn:aws:inspector:eu-west-2:146838936955:rulespackage/0-IeCjwf1W
網路連線能力	arn:aws:inspector:eu-west-2:146838936955:rulespackage/0-AizSYyNq
安全最佳實務	arn:aws:inspector:eu-west-2:146838936955:rulespackage/0-XApUiSaP

歐洲 (斯德哥爾摩)

規則套件名稱	ARN
Common Vulnerabilities and Exposures	arn:aws:inspector:eu-north-1:4534202

規則套件名稱	ARN
	44670:rulespackage/0-IgdgIewd
CIS 作業系統安全組態基準參考指標	arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-Yn8jlX7f
網路連線能力	arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-52Sn74uu
安全最佳實務	arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-HfBQSbSf

AWS GovCloud （美國東部）

規則套件名稱	ARN
Common Vulnerabilities and Exposures	arn:aws-us-gov:inspector:us-gov-east-1:206278770380:rulespackage/0-3IFKFuOb
CIS 作業系統安全組態基準參考指標	arn:aws-us-gov:inspector:us-gov-east-1:206278770380:rulespackage/0-pTLCdIww

規則套件名稱	ARN
安全最佳實務	arn:aws-us-gov:inspector:us-gov-east-1:206278770380:rulespackage/0-vlgEGcVD

AWS GovCloud （美國西部）

規則套件名稱	ARN
Common Vulnerabilities and Exposures	arn:aws-us-gov:inspector:us-gov-west-1:850862329162:rulespackage/0-4oQgcI4G
CIS 作業系統安全組態基準參考指標	arn:aws-us-gov:inspector:us-gov-west-1:850862329162:rulespackage/0-Ac4CFOuc
安全最佳實務	arn:aws-us-gov:inspector:us-gov-west-1:850862329162:rulespackage/0-rOTGqe5G

文件歷史紀錄

下表說明 2018 年 5 月之後 Amazon Inspector Classic 的文件發行歷史記錄。

變更	描述	日期
終止支援通知	支援結束通知：2026 年 5 月 20 日，AWS 將結束對 Amazon Inspector Classic 的支援。2026 年 5 月 20 日之後，您將無法再存取 Amazon Inspector Classic 主控台或 Amazon Inspector Classic 資源。如需詳細資訊，請參閱 Amazon Inspector Classic 終止支援。	2025 年 5 月 20 日
更新密碼的安全最佳實務	已更新 EC2 執行個體密碼長度和密碼複雜性的 Amazon Inspector Classic 安全最佳實務要求。請參閱設定密碼長度下限和設定密碼複雜性	2021 年 3 月 8 日
新增對較新作業系統版本的支援	Amazon Inspector Classic 現在支援下列作業系統版本：Ubuntu 20.4 LTS、Debian 10.x、RHEL 8.x 和 Windows Server 2019 Base。	2020 年 10 月 15 日
整合到新安全章節的安全性資訊	Amazon Inspector Classic 的安全性資訊，包括管理身分和存取管理的資訊，會合併到安全性章節中。請參閱 Amazon Inspector Classic 中的安全性。	2020 年 4 月 7 日

更新文件以移除對執行期行為分析規則套件的支援。	已更新多個主題，移除不再支援之執行時間行為分析規則套件的相關資訊。	2019 年 9 月 5 日
新增作業系統支援	新增對 CentOS 7.6 的 Amazon Inspector Classic 支援。如需詳細資訊，請參閱跨支援的作業系統的 Amazon Inspector Classic 支援的作業系統和區域和規則套件可用性。	2018 年 12 月 3 日
新內容	新增了 Amazon Inspector Classic Network Reachability 規則套件，可讓使用者執行無代理程式評估，以分析安全漏洞的網路組態。如需詳細資訊，請參閱網路連線能力。	2018 年 11 月 9 日
新增作業系統支援	新增對 RHEL 7.6 的 Amazon Inspector Classic 支援。如需詳細資訊，請參閱跨支援的作業系統的 Amazon Inspector Classic 支援的作業系統和區域和規則套件可用性。	2018 年 10 月 30 日
新增作業系統支援	新增各種作業系統支援到 CIS 基準參考指標規則套件。如需詳細資訊，請參閱 Center for Internet Security (CIS) 基準參考指標及各支援作業系統的規則套件可用性。	2018 年 8 月 13 日
新增了區域支援	新增 AWS GovCloud (US) 的區域支援。	2018 年 6 月 13 日

下表說明 2018 年 6 月之前 Amazon Inspector Classic 的文件發行歷史記錄。

變更	描述	日期
新內容	新增以帳戶中的所有 Amazon EC2 執行個體為目標的功能。如需詳細資訊，請參閱Amazon Inspector Classic 評估目標。	2018 年 5 月 24 日
已新增的作業系統支援	新增對 Amazon Linux 2018.03 和 Ubuntu 18.04 的 Amazon Inspector Classic 支援。	2018 年 5 月 15 日
新內容	新增設定重複 Amazon Inspector Classic 評估的功能。	2018 年 4 月 30 日
新內容	新增透過主控台安裝 Amazon Inspector Classic 代理程式的功能。	2018 年 4 月 30 日
已新增的作業系統支援	新增 Amazon Linux 2 的 Amazon Inspector Classic 支援。	2018 年 3 月 13 日
已新增的作業系統支援	新增對 Windows Server 2016 Base 的 Amazon Inspector Classic 評估支援。	2018 年 2 月 20 日
新增了區域支援	新增 US East (Ohio)區域的 Amazon Inspector Classic 支援。	2018 年 2 月 7 日
新內容	核心模組無法使用時，Amazon Inspector Classic 評估現在可以執行。	2018 年 1 月 11 日
新增了區域支援	新增 EU (Frankfurt) 區域的 Amazon Inspector Classic 支援。	2017 年 12 月 19 日

變更	描述	日期
新內容	新增使用 Amazon Inspector Classic API 和主控台檢查 Amazon Inspector Classic 代理程式運作狀態的功能。	2017 年 12 月 15 日
新內容	新增以下功能： • 服務連結角色用法 • Marketplace 中提供 Amazon Inspector Classic 代理程式 AMI AWS • Amazon Inspector Classic AWS CloudFormation 範本	2017 年 12 月 5 日
已新增的作業系統支援	新增 CentOS 7.4 的 Amazon Inspector Classic 評估支援。	2017 年 11 月 9 日
已新增的作業系統支援	新增 Amazon Linux 2017.09 的 Amazon Inspector Classic 評估支援。	2017 年 10 月 11 日
已新增的作業系統支援	新增 RHEL 7.4 的 Amazon Inspector Classic 評估支援。	2018 年 2 月 20 日
新增 HIPAA 資格	Amazon Inspector Classic 現在符合 HIPAA 資格。	2017 年 7 月 31 日
新內容	新增使用 Amazon CloudWatch Events 自動觸發 Amazon Inspector Classic 安全性評估的功能。 Amazon CloudWatch	2017 年 7 月 27 日
新增了區域支援	新增 `US West (N. California)` 區域的 Amazon Inspector Classic 支援。	2018 年 6 月 6 日

變更	描述	日期
已新增的作業系統支援	新增對 RHEL 6.2-6.9、RHEL 7.2-7.3、CentOS 6.9 和 CentOS 7.2-7.3 的 Amazon Inspector Classic 評估支援。	2017 年 5 月 23 日
已新增的作業系統支援	新增 Amazon Linux 2017.03 的 Amazon Inspector Classic 評估支援。	2017 年 4 月 25 日
嶄新內容以及新增的作業系統支援	已新增： • Amazon Inspector Classic 支援 Ubuntu 16.04。 • 用於自動化 Amazon Inspector Classic 操作的 Lambda 藍圖可用性。	2017 年 1 月 5 日
新的作業系統支援	新增 Microsoft Windows 的 Amazon Inspector Classic 支援。	2016 年 8 月 26 日
新增了區域支援	新增 `Asia Pacific (Seoul)`區域的 Amazon Inspector Classic 支援。	2016 年 8 月 26 日
新增了區域支援	新增 `Asia Pacific (Mumbai)`區域的 Amazon Inspector Classic 支援。	2016 年 4 月 25 日
新增了區域支援	新增 `Asia Pacific (Sydney)`區域的 Amazon Inspector Classic 支援。	2016 年 4 月 25 日
服務啟動	Amazon Inspector Classic 服務已啟動。	2015 年 10 月 7 日

AWS 詞彙表

如需最新的 AWS 術語，請參閱 AWS 詞彙表 參考中的AWS 詞彙表。