使用者指南

AWS Audit Manager

AWS Audit Manager: 使用者指南

Table of Contents

什麼是 AWS Audit Manager？

歡迎使用 AWS Audit Manager 使用者指南。

AWS Audit Manager 可協助您持續稽核 AWS 使用情況，以簡化管理風險與法規與業界標準的法規遵循方式。Audit Manager 會自動化證據收集，讓您更容易評估您的政策、程序和活動 (也稱為控制項) 是否有效運作。進行稽核時，Audit Manager 可協助您管理控制項的利益相關者檢閱。這意味著您能在減少手動工作情況下，將稽核報告準備就緒。

Audit Manager 提供預建架構，可針對特定的合規標準或法規來建構和自動化評估。架構包括一個預組的控制集，其中包含說明和測試程序。這些控制項會根據指定的合規標準或法規的要求進行分組。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

您可以從任何架構建立評估。建立評估時，Audit Manager 會自動執行資源評估。這些評估會收集 AWS 帳戶 和您在稽核範圍內定義的服務資料。所收集的資料會自動轉換為易於稽核的證據。然後會附加到相關控制項，以協助您證明安全性、變更管理、業務持續性和軟體授權方面的合規性。證據收集程序為持續過程，並從您建立評估時開始。完成稽核後，不再需要 Audit Manager 來收集證據，您可以停止收集證據。如需執行此操作，請將評估狀態變更為非作用中。

Audit Manager 功能

透過 AWS Audit Manager，您可以執行下列任務：

- 快速入門 — 從支援各種合規標準和法規的預建架構中進行選擇，以建立您的第一個評估。接著啟動自動化證據收集，以稽核您的 AWS 服務 使用情況。
- 上傳和管理來自混合式或多雲端環境的證據 — 除了 Audit Manager 從您的 AWS 環境收集的證據之外，您還可以上傳並集中管理來自內部部署或多雲端環境的證據。
- 支援常見的合規標準和法規 — 選擇其中一個 AWS Audit Manager 標準架構。這些架構為常見的合規標準和法規提供預建的控制項映射。這些措施包括 CIS 基準指標、PCI DSS、GDPR、HIPAA、SOC2、GxP 以及 AWS 營運最佳實務。
- 監控您的有效評估 — 使用 Audit Manager 儀表板來檢視有效評估的分析資料，並快速分辨需要修正的不合規證據。
- 證據搜尋 — 使用證據搜尋工具功能快速找到與您的所查詢的相關證據。您可以從搜尋結果中產生評估報告，或以 CSV 格式匯出搜尋結果。
- 建立自訂控制項 — 從頭開始建立您自己的控制項，或自訂現有控制項以符合您的需求。您也可以使用自訂控制項功能來建立風險評估問題，並將這些問題的回覆儲存為手動證據。

- 自訂架構 — 根據您對內部稽核的特定需求，使用標準或自訂控制項建立您自己的架構。
- 共享自訂架構 — 與其他 AWS 帳戶 共享您自訂的 Audit Manager 架構，或將其複製到您自己帳戶下的另一個 AWS 區域。
- 支援跨團隊協同 — 將控制集委派給主題專家，他們可以檢閱相關證據、新增評論，並更新各控制項狀態。
- 為稽核者建立報告 — 產生評估報告，摘要針對稽核收集的相關證據，並連結至包含詳細證據的資料夾。
- 確保證據完整性 — 將證據存放在安全的位置，保持不變。

> **Note**
>
> AWS Audit Manager 協助收集與驗證符合特定合規標準和法規相關的證據。不過，這不會評估您的合規狀態。因此，透過 AWS Audit Manager 收集的證據可能不包含稽核所需的所有關於您的 AWS 使用資訊。AWS Audit Manager 不是法律顧問或合規專家的替代方案。

Audit Manager 定價

如需定價的詳細資訊，請參閱 AWS Audit Manager 定價。

您第一次使用 Audit Manager 嗎？

若您是第一次使用 Audit Manager，建議您閱讀以下章節：

1. AWS Audit Manager 概念和術語 — 了解 Audit Manager 中使用的重要概念和術語，例如評估、架構和控制項。
2. AWS Audit Manager 如何收集證據 — 了解 Audit Manager 如何收集證據，以進行資源評估。
3. 設定 — 了解 Audit Manager 的設定需求。
4. 入門 — 依照教學課程建立您的第一個 Audit Manager 評估。
5. AWS Audit Manager API 參考 — 熟悉 Audit Manager API 動作和資料類型。

更多 Audit Manager 資源

探索下列資源以進一步了解 Audit Manager。

- 收集證據和管理稽核資料 AWS Audit Manager
- 從AWS 工作坊手動設定自訂 Audit Manager 評估
- 跨三線模型整合 (第 2 部分)：從 AWS 管理與控管部落格，將 AWS Config 一致性套件轉換為 AWS Audit Manager 評估

AWS Audit Manager 概念和術語

為了協助您入門，本頁面定義了術語和解釋了 AWS Audit Manager 的一些重要概念。

A

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

評估

您可以使用 Audit Manager 評估來自動收集與稽核相關的證據。

評估是以架構為基礎，架構是與稽核相關的一組控制項。根據您的業務需求，您可以從標準架構或自訂架構建立評估。標準架構包含支援特定合規標準或法規的預建控制集。相較之下，自訂架構包含您可以根據內部稽核需求自訂和分組的控制項。使用架構作為起點，您可以建立評估，以指定要包含在稽核範圍中的 AWS 帳戶 和服務。

當您建立評估時，Audit Manager 會根據架構中定義的控制項，自動評估您的 AWS 帳戶 和服務中的資源。接著，收集相關證據並將其轉換為易於稽核的格式。執行此操作後，它會將證據附加到評估中的控制項中。當需要進行稽核時，您或您選擇的委派代表可以檢閱收集的證據，然後將其新增至評估報告中。此評估報告可協助您證明您的控制項如期運作。

證據收集程序為持續過程，會在您建立評估時開始。您可以將評估狀態變更為非作用中，以停止證據收集。或者，您可以在控制層級停止證據收集。您可以將評估中的特定控制項狀態變更為非作用中來執行此操作。

如需有關建立與管理評估的說明，請參閱 AWS Audit Manager 中的評估。

評估報告

評估報告是由 Audit Manager 評估產生的最終文件。這些報告為您總結稽核收集的相關證據。它們連結到相關證據文件夾。資料夾會根據評估中所指定的控制項來命名和組織。對於每項評估，您可以檢閱 Audit Manager 收集的證據，並決定要在評估報告中包含哪些證據。

如需進一步了解評估報告，請參閱 評估報告。如需了解如何產生評估報告，請參閱 產生評估報告。

評估報告目的地

評估報告目的地是 Audit Manager 儲存您的評估報告的預設 S3 儲存貯體。如需進一步了解，請參閱 評估報告目的地 (選用)。

稽核

稽核是對您組織的資產、營運或業務完整性進行獨立檢查。資訊技術 (IT) 稽核會特別檢查組織資訊系統內的控制項。IT 稽核的目標是判斷資訊系統是否保護資產並有效運作，以及維護資料完整性。所有這些對於滿足合規標準或法規規定的監管要求至關重要。

稽核擁有者

稽核擁有者一詞會根據前後關聯性而有兩種不同的意義。

在 Audit Manager 的前後關聯性中，稽核擁有者是管理評估及其相關資源的使用者或角色。此 Audit Manager 角色的職責包括建立評估、檢閱證據以及產生評估報告。Audit Manager 是一項協作服務，當其他利益關係者參與其評估時，稽核擁有者將受益匪淺。例如，您可以將其他稽核擁有者新增至您的評估，以共享管理任務。或者，如果您是稽核擁有者，且需要協助解譯為控制項所收集的證據，您可以將該控制集委派給在該領域擁有專業知識的利益關係者。這樣的人被稱為委派代表角色。

在商業術語中，稽核擁有者是協調和監督其公司的稽核準備工作，並向稽核人員提供證據的人。一般而言，這是控管、風險和合規 (GRC) 專業人員，例如合規官員或 GDPR 資料保護官。GRC 專業人員擁有管理稽核準備的專業知識和權力。具體來說，他們了解合規需求，並可以分析、解譯和準備報告資料。不過，其他業務角色也可以承擔稽核擁有者的 Audit Manager 角色，不僅是由 GRC 專業人員來擔任。例如，您可以選擇由以下團隊之一的技術專家進行設定和管理 Audit Manager 評估：

- SecOps
- IT/DevOps
- 安全營運中心 / 事件回應
- 相關團隊負責擁有、開發、修復和部署雲端資產，以及了解組織雲端基礎架構

您在 Audit Manager 評估中，選擇指定誰作為稽核擁有者，這很大程度上取決於您的組織。這同時取決於您如何架構安全性作業，以及其稽核細節。在 Audit Manager 中，同一個人可以在一項評估中擔任稽核擁有者角色，在另一個評估中擔任委派代表角色。

無論您選擇如何使用 Audit Manager，都可以使用稽核擁有者 / 委派角色管理整個組織的職責分離，並將特定的 IAM 政策授予每位使用者。透過這兩個步驟的方法，Audit Manager 可確保您完

全掌控個別評估的所有細節。如需詳細資訊，請參閱 AWS Audit Manager 中的使用者角色建議策略。

C

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

Changelog

對於評估中的每個控制項，Audit Manager 會擷取變更記錄檔，以追蹤該控制項的使用者活動。您可以檢閱與特定控制項相關之活動的稽核記錄。如需有關在變更記錄檔中所擷取的使用者活動資訊，請參閱 Changelog 索引標籤。

雲端合規

雲端合規是雲端交付的系統必須符合雲端客戶所面臨的標準的一般原則。

合規監管

合規監管是由當局規定的法律、規則或其他命令，通常用於規範行為。一個範例是 GDPR。

合規標準

合規標準是一套結構化的準則，詳細說明組織維持與既定法規、規範或立法一致的過程。範例包括 PCI DSS 和 HIPAA。

控制項

控制項是為資訊系統或組織規定的保護或對策。控制項旨在保護您資訊的機密性、完整性和可用性，並滿足一系列定義的安全要求。它們確保您的資源如預期運作，資料可靠，且您的組織遵守適用的法律和法規。

在 Audit Manager 中，控制項還可以代表供應商風險評估問卷中的一個問題。在這種情況下，控制項是一個特定的問題，詢問有關組織的安全性和合規性狀況的資訊。

控制項會在 Audit Manager 評估中處於有效狀態時持續收集證據。您也可以手動將證據新增至任何控制項。每個證據都會成為記錄，協助您證明是否符合控制項的需求。

Audit Manager 中有兩種類型的控制項：

- 標準控制項 — 這些是預先建立的控制項，與 Audit Manager 中的特定架構相關聯。使用標準控制項協助您為各種合規標準和法規進行稽核準備。

- 自訂控制項 — 這些是您定義為 Audit Manager 使用者的自訂控制項。使用自訂控制項協助您滿足內部稽核或廠商風險評估的特定合規要求。

如需詳細資訊，請參閱 AWS Audit Manager 控制項範例。如需有關建立與管理控制項的說明，請參閱 控制項程式庫。

控制項網域

您可以將控制項網域視為控制項的一般類別，不特定於任何一個架構。控制項網域群組是 Audit Manager 儀表板最強大的功能之一。Audit Manager 會強調顯示評估中具有不合規證據的控制項，並依控制項網域進行分組。這可讓您在準備稽核時，將修復工作集中在特定主題領域上。

> **Note**
>
> 控制項網域與控制集不同。控制項集是一種特定於架構的控制項群組，通常由管理機構定義。例如，PCI DSS 架構有一個名為需求 8：識別和驗證對系統元件的存取的控制組。此控制集屬於身分與存取管理的控制項網域下。

Audit Manager 會將控制項分類在下列控制項網域下。

控制項網域名稱	這些控制項管理範圍的描述
業務連續性和應變計劃	建立程序以保護重要營運作業，不受重大系統和網路中斷影響程序的方法。
變更管理	測試、核准、實作及記錄雲端基礎架構變更的方式。
資料安全與隱私	您保護資料的隱私權、可用性和完整性的方法。
開發與組態管理	如何在所需且一致的狀態下維護雲端基礎架構。
控管和監督	讓雲端運算的使用符合法律、法規及道德義務的方法。
身分與存取管理	如何確保正確的使用者能適當存取您的技術資源。
事件管理	如何建立責任和程序，從而確保快速有效地應對安全事件。
記錄和監控	如何檢閱使用者活動，了解嘗試或執行未經授權活動的跡象。
網路管理	如何使用網路管理系統管理和操作資料網路。

控制項網域名稱	這些控制項管理範圍的描述
人事管理	如何評估和管理組織層級的人員安全風險。
實體安全	如何偵測和預防設施中的實體安全問題。
風險管理	如何評估潛在風險和損失，以及如何減少或消除此類威脅。
供應鏈管理	如何分辨、評估和減輕與 IT 產品、供應商和供應鏈相關的風險。
使用者裝置管理	如何降低員工 IT 硬體遺失、損壞或受損的風險。
漏洞管理	如何定義、評估和修復雲端基礎架構中資產的所有已知漏洞。

D

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

資料來源

Audit Manager 使用資料來源來收集控制項的證據。下列術語說明什麼是資料來源以及其運作方式。

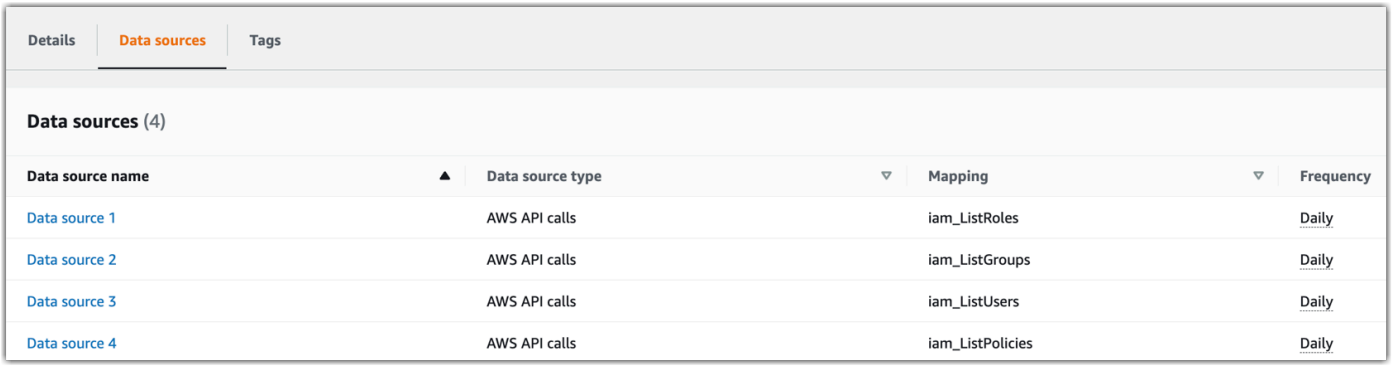
- 資料來源類型定義 Audit Manager 從何處收集證據以進行控制項。如果您上傳自己的證據，則資料來源類型為手動。如果 Audit Manager 代表您收集證據，則資料來源類型為下列其中一種：AWS Security Hub、AWS Config、AWS CloudTrail 或 AWS API 呼叫。Audit Manager API 將資料來源類型稱為 sourceType (單數) 或 controlSources (複數)。
- 映射是與資料來源類型相關的特定關鍵字。例如，這可能是 CloudTrail 事件名稱或 AWS Config 名稱。Audit Manager API 將其稱為 sourceKeyword (單數) 或 controlMappingSources (複數)。
- 資料來源名稱是指定給資料來源的名稱。換句話說，資料來源名稱會標示資料來源類型和映射組合。對於標準控制項，Audit Manager 會提供預設資料來源名稱 (例如資料來源 1 和資料來源 2)。對於自訂控制項，您可以提供自己的資料來源名稱。這可能有助於您區分屬於相同資料來源類型的多個映射。Audit Manager API 會將資料來源名稱稱為 sourceName。

單一控制項可以有多個資料來源類型和多個映射項目。例如，一個控制項可能會從混合的資料來源類型收集證據 (像是 AWS Config 和 Security Hub)。另一個控制項可能將 AWS Config 作為唯一的資料來源類型，同時使用多個 AWS Config 規則作為映射項目。

下表列出自動化資料來源類型，並顯示一些映射項目的範例。

Data source type (資料來源類型)	說明	映射範例
AWS Security Hub	使用此資料來源類型可擷取資源安全狀態的快照。Audit Manager 會使用 Security Hub 控制項的名稱作為映射關鍵字，並直接從安全性中心報告該安全檢查的結果。	`1.1 – Avoid the use of the "root" account`
AWS Config	使用此資料來源類型可擷取資源安全狀態的快照。Audit Manager 會使用 AWS Config 規則的名稱作為映射關鍵字，並直接從 AWS Config 中報告該規則檢查的結果。	`EC2_INSTANCE_MANAGED_BY_SSM`
AWS CloudTrail	使用此資料來源類型可追蹤稽核中所需的特定使用者活動。Audit Manager 會使用 CloudTrail 事件的名稱作為映射關鍵字，並從 CloudTrail 日誌中收集相關的使用者活動。	`CreateAccessKey`
AWS API 呼叫	使用此資料來源類型，透過對特定 AWS 服務 的 API 呼叫建立資源組態快照。Audit Manager 會使用 API 呼叫的名稱作為映射關鍵字，並收集 API 回應。	`ec2_DescribeSecurityGroups`

下圖顯示了在 Audit Manager 主控台中看到的不同資料來源的範例。



> **Note**
>
> 雖然有些資料來源類型是 AWS 服務，但資料來源類型與範圍內的服務不同。如需詳細資訊，請參閱本指南的疑難排解章節中的範圍內的服務和資料來源類型有何差異？。

委派代表

委派代表是具備有限權限的 AWS Audit Manager 使用者。委派代表通常在多個不同領域具備專業的業務或技術專長。例如，這些專業知識可能涵蓋資料保留政策、培訓計劃、網路基礎結構或身分管理等領域。委派代表可幫助稽核擁有者檢閱其專業領域內的控制項所收集到的證據。委派代表可以檢閱控制集及其相關證據，以及新增評論、上傳其他證據，並更新您指派給他們檢閱的各控制項狀態。

稽核擁有者會指派特定控制集給委派代表，而非整個評估。因此，委派代表對評估的存取權限有限。如需關於委派控制集的說明，請參閱 在 AWS Audit Manager 中委派。

E

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

證據

證據是包含證明是否符合控制項要求所需資訊的記錄。證據的範例包括使用者調用的變更活動，以及系統組態快照集。

Audit Manager 中主要分為兩種證據類型：自動化證據和手動證據。

- 自動化證據 — 為 Audit Manager 自動收集的證據。自動化證據包括以下三種類別：
  - 合規檢查 — 合規檢查的結果是從AWS Security HubAWS Config、或兩者擷取。合規檢查的範例包括 Security Hub 針對 PCI DSS 控制項的安全檢查結果，以及 HIPAA 控制項的AWS

Config規則評估。如需詳細資訊，請參閱 AWS Audit Manager 支援的AWS Config規則和 AWS Audit Manager 支援的 AWS Security Hub 控制項。

- 使用者活動 — 當活動發生時，會從 CloudTrail 日誌擷取變更資源組態的使用者活動。使用者活動的範例包括路由表更新、Amazon RDS 執行個體備份設定變更，以及 S3 儲存貯體加密政策變更。如需詳細資訊，請參閱 AWS Audit Manager 支援的 AWS CloudTrail 事件名稱。
- 組態資料 — 資源組態的快照會直接從 AWS 服務 的每日、每週或每月擷取。組態快照的範例包括 VPC 路由表的路由清單、Amazon RDS 執行個體備份設定以及 S3 儲存貯體加密政策。如需更多詳細資訊，請參閱 AWS Audit Manager 支援 API 呼叫 。

- 手動證據 — 這是您自行新增至 Audit Manager 的證據。新增自己的證據有以下三種方法：
  - 從 Amazon S3 匯入檔案
  - 從瀏覽器上傳檔案
  - 輸入風險評估問題的文字回覆

  如需更多詳細資訊，請參閱 在 AWS Audit Manager 中添加手動證據。

自動化證據收集會在您建立評估時啟動。這是一個持續的程序，Audit Manager 會根據證據類型和基礎資料來源，以不同的頻率收集證據。如需證據收集的詳細資訊，請參閱 AWS Audit Manager 如何收集證據。如需關於檢閱評估中證據的說明，請參閱檢閱評估中的證據。

證據收集方法

控制項可以透過兩種方式收集證據。

- 自動化控制項會自動從AWS資料來源收集證據。自動化證據可以幫助您證明對此控制項的完全或部分合規性。
- 手動控制需要您上傳自己的證據，以證明控制項完全合規。

> **Note**
>
> 您可以將手動證據附加到任何自動化控制項。在許多情況下，需要結合自動化和手動證據來證明控制項完全合規。雖然 Audit Manager 可以提供有用且相關的自動化證據，但某些自動化證據可能只會顯示部分合規性。在這種情況下，您可以用自己的證據來補充 Audit Manager 提供自動化證據。
> 例如：
>
> - AWS 生成式 AI 最佳實務架構包含一個名為 `Error analysis` 的控制項。此控制項需要您分辨在模型使用中何時偵測到不準確性。並要求您進行徹底的錯誤分析，以了解根本原因並採取糾正措施。

- 為支援此控制項，Audit Manager 會收集自動化證據，顯示是否為執行評估的 AWS 帳戶位置啟用 CloudWatch 警示。您可以使用此證據來證明對控制項的部分合規，以證明您的警報和檢查已正確配置。
- 為了證明完全合規，您可以用手動證據補充自動化證據。例如，您可以上傳顯示錯誤分析過程、升級和報告的閾值，以及根本原因分析結果的策略或程序。您可以使用此手動證據來證明建立的策略已到位，並在出現提示時採取了糾正措施。

如需更詳細的範例，請參閱混合資料來源的控制項。

匯出目的地

匯出目的地是預設 S3 儲存貯體，Audit Manager 會儲存您從證據搜尋工具匯出的檔案。如需進一步了解，請參閱 匯出目的地 (選用)。

F

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

架構

Audit Manager 架構是一個檔案，用來建構和自動執行特定標準或風險控管原則的評估。這些架構可協助您將AWS資源映射至控制項中的需求。包括預先建立或客戶定義的控制項集合。該集合具有每個控制項的說明和測試程序。這些控制項會根據指定的合規標準或法規需求進行組織和分組。範例包括 PCI DSS 和 GDPR。

Audit Manager 中有兩種類型的架構：

- 標準架構 — 以各種合規標準和法規的 AWS 最佳實務為基礎的預建架構。您可以使用這些架構來協助稽核準備工作。
- 自訂架構 — 您定義為 Audit Manager 使用者的自訂架構。您可以根據您的特定合規或風險控管需求，使用這些架構來協助稽核準備工作。

如需有關建立與管理架構的說明，請參閱 架構程式庫。

> **Note**
>
> AWS Audit Manager 協助收集與驗證符合特定合規標準和法規相關的證據。不過，這不會評估您的合規狀態。因此，透過 AWS Audit Manager 收集的證據可能不包含稽核所需的所有關於您的 AWS 使用資訊。AWS Audit Manager 不是法律顧問或合規專家的替代方案。

架構共享

您可以使用 Audit Manager 的自訂架構共享功能，在 AWS 帳戶 和區域之間快速共享您的自訂架構。如果共享自訂架構，您可以建立共享要求。接下來，共享要求的收件者有 120 天的時間接受或拒絕要求。當他們接受時，Audit Manager 會將共享的自訂架構複寫到其架構程式庫中。除了複寫自訂架構之外，Audit Manager 也會複寫該架構中包含的所有自訂控制集和控制項。這些自訂控制項會新增至收件者的控制項程式庫。Audit Manager 不會複寫標準架構或控制項。這是因為這些資源在每個帳戶和區域中，已預設為可用。

R

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

資源

資源是在稽核中評估的實體或資訊資產。AWS 資源範例包含 Amazon EC2 執行個體、Amazon RDS 執行個體、Amazon S3 儲存貯體和 Amazon VPC 子網路。

資源評估

資源評估是評估個別資源的程序。此評估基於控制項的需求。當評估處於有效狀態時，Audit Manager 會針對評估範圍內的每個獨立資源執行資源評估。資源評估會執行下列任務：

1. 收集證據，包括資源配置，事件日誌和調查結果
2. 將證據轉換並映射到控制項
3. 儲存和追蹤證據的歷程，以實現完整性

資源合規性

資源合規性是指在收集合規檢查證據時，對資源進行評估的狀態。

Audit Manager 會針對使用 AWS Config 和 Security Hub 作為資料來源類型的控制項，收集合規檢查證據。證據收集期間，可能會評估多個資源。因此，單一合規檢查證據可以包含一或多個資源。

您可以使用證據搜尋工具中的資源合規性篩選器來搜索資源層級的合規狀態。搜尋完成後，您就可以預覽符合搜尋條件的資源。

在證據搜尋工具中，資源合規有三種可能的值：

- 不合規 — 指的是具有合規檢查問題的資源。如果 Security Hub 回報資源的失敗結果，或AWS Config回報不合規的結果，就會發生這種情況。

- 合規 — 指的是不具有合規檢查問題的資源。如果 Security Hub 回報資源的通過結果，或者AWS Config回報合規結果，就會發生這種情況。
- 不確定 — 指的是會尋找合規檢查不可用或不適用的資源。如果 AWS Config 或 Security Hub 是基礎資料來源類型，但這些服務尚未啟用，就會發生這種情況。如果基礎資料來源類型不支援合規檢查 (例如手動證據、AWS API 呼叫或 CloudTrail)，也會發生這種情況。

S

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

服務範圍

這是包含於評估範圍內的 AWS 服務。當您將某項服務指定為包含在評估範圍內時，Audit Manager 會評估該服務的資源。Audit Manager 會從範圍內的服務評估各項資源。一些範例資源包括如下：

- Amazon EC2 執行個體
- S3 儲存貯體
- 使用者或角色
- DynamoDB 資料表
- 網路元件，例如 Amazon 虛擬私有雲端 (VPC)、安全群組或網路存取控制清單 (ACL) 表

當您使用 Audit Manager 主控台從標準架構建立或更新評估時，會預設為預先選取範圍內的 AWS 服務 清單。無法編輯此清單。這是因為 Audit Manager 會自動為您映射並選擇資料來源和服務。此選擇是根據標準架構的要求所進行。如果標準架構只包含手動控制項，則您的評估範圍內不會包含任何 AWS 服務，並且您無法在評估中新增任何服務。

如果您需要編輯標準架構範圍內的服務清單，您可以使用CreateAssessment或UpdateAssessment API 操作來執行編輯。或者，您可以自訂標準架構，然後從自訂架構中建立評估。

> **Note**
>
> 請記住，範圍內的服務與資料來源類型不同，資料來源類型可以是AWS 服務或其他類型。如需詳細資訊，請參閱本指南的疑難排解章節中的範圍內的服務和資料來源類型有何差異？。

AWS Audit Manager 如何收集證據

AWS Audit Manager 中的每個有效評估都會自動收集來自一系列資料來源的證據。每個評估都有其定義範圍，用於指定 AWS 服務 和 Audit Manager 從中收集資料的帳戶。這些定義的服務與帳號範圍中的各項都包含多個資源，而每個資源都是您擁有的系統資產清單。Audit Manager 中的證據收集涉及對每個範圍內資源的評估。這稱為資源評估。

下列步驟說明 Audit Manager 如何為各資源評估收集證據：

1. 從資料來源評估資源

啟動收集證據時，Audit Manager 會從資料來源對範圍內的資源進行評估。它會擷取組態快照集、相關合規檢查結果以及任何使用者活動來達成此目的。然後執行分析，以判斷此資料支援哪個控制項。資源評估的結果將被保存，並轉換為證據。如需有關不同證據類型的詳細資訊，請參閱本指南 AWS Audit Manager 概念與術語章節中的證據。

2. 將評估結果轉換為證據

資源評估的結果包含從該資源擷取的原始資料，以及指示資料支援哪些控制項的中繼資料。AWS Audit Manager會將原始資料轉換為易於稽核的格式。接著，轉換後的資料和中繼資料會儲存為 Audit Manager 證據，再附加至控制項。

3. 將證據附加至相關控制項

Audit Manager 會讀取證據中繼資料。然後會將儲存的證據附加至評估中的相關控制項。附加的證據會在 Audit Manager 中顯示。如此一來，就完成了資源評估的週期。

> **Note**
>
> 視控制項組態而定，在某些情況下，相同的證據可以附加至來自多個 Audit Manager 評估的多個控制項。當相同的證據附加到多個控制項時，Audit Manager 只會測量一次資源評估。這是因為相同的證據只會收集一次。然而，Audit Manager 評估中的一個控制項可以有來自多個資料來源的多項證據。

證據收集頻率

證據收集程序為持續過程，會在您建立評估時開始。AWS Audit Manager 會以不同頻率從多個資料來源收集證據。因此，對於收集證據的頻率，沒有一種適合所有情況的標準答案。證據收集的頻率取決於證據類型及其資料來源，如下所述。

- 合規檢查 — Audit Manager 會從 AWS Security Hub 和 AWS Config 收集此證據類型。
  - 對於AWS Security Hub，證據收集的頻率遵循 Security Hub 檢查排程。如需有關 Security Hub 檢查排程的詳細資訊，請參閱 AWS Security Hub 使用指南中的執行安全檢查排程。如需 Audit Manager 支援之 Security Hub 檢查的詳細資訊，請參閱AWS Security Hub 支援的控制項 AWS Audit Manager。
  - 對於 AWS Config，證據收集的頻率遵循 AWS Config 規則中定義的觸發程序。如需有關 AWS Config 規則觸發的詳細資訊，請參閱 AWS Config 使用指南中的觸發類型。如需 Audit Manager 所支援之 AWS Config 規則 的詳細資訊，請參閱 AWS Config 規則 支持 AWS Audit Manager。
- 使用者活動 — Audit Manager 會以連續方式從 AWS CloudTrail 中收集此證據類型。這個頻率是連續的，因為使用者活動可以在一天中的任何時間發生。如需更多詳細資訊，請參閱 AWS CloudTrail 支援的事件名稱 AWS Audit Manager。
- 組態資料 — Audit Manager 使用對 Amazon EC2、Amazon S3 或 IAM AWS 服務 等其他人的說明 API 呼叫來收集此證據類型。您可以選擇要呼叫的 API 動作。您也可以在 Audit Manager 中將頻率設定為每日、每週或每月。您可以在控制項資源庫中建立或編輯控制項時，指定此頻率。如需關於編輯與建立控制項的說明，請參閱 控制項程式庫。如需關於 Audit Manager 如何使用 API 呼叫建立證據的詳細資訊，請參閱支援的 API 呼叫 AWS Audit Manager。

無論資料來源的證據收集頻率為何，只要控制項和評估處於有效狀態，就會自動收集新證據。

AWS Audit Manager 控制項範例

您可以檢閱此頁面上的範例，進一步了解控制項在 AWS Audit Manager 的運作方式。這些範例描述控制項的外觀、Audit Manager 如何為該控制項產生證據，以及您可以採取以證明合規的後續步驟。

> **Tip**
>
> 為了在 Audit Manager 中獲得最佳體驗，我們建議您啟用 AWS Config 和 AWS Security Hub。啟用這些功能時，它們可以用作 Audit Manager 評估中控制項的資料來源類型。換句話說，Audit Manager 可以使用 Security Hub 調查結果以及 AWS Config 規則，以產生自動化的證據。
>
> - 啟用 AWS Security Hub之後，請確定您同時啟用所有安全性標準，並開啟合併的控制項調查結果設定。此步驟可確認 Audit Manager 能匯入所有支援的合規標準的調查結果。

- 啟用 AWS Config 後，請確定您同時啟用相關 AWS Config 規則 或為與稽核相關的合規標準部署一致性套件。此步驟可確保 Audit Manager 可以針對您啟用的所有支援 AWS Config 規則 匯入調查結果。

以下為每種控制項類型的範例：

主題

- 以 AWS Security Hub 當作資料來源類型的自動化控制項
- 以 AWS Config 當作資料來源類型的自動化控制項
- 以 AWS API 呼叫當作資料來源類型的自動化控制項
- 以 AWS CloudTrail 當作資料來源類型的自動化控制項
- 手動控制
- 具有混合資料來源類型的控制項 (自動和手動)

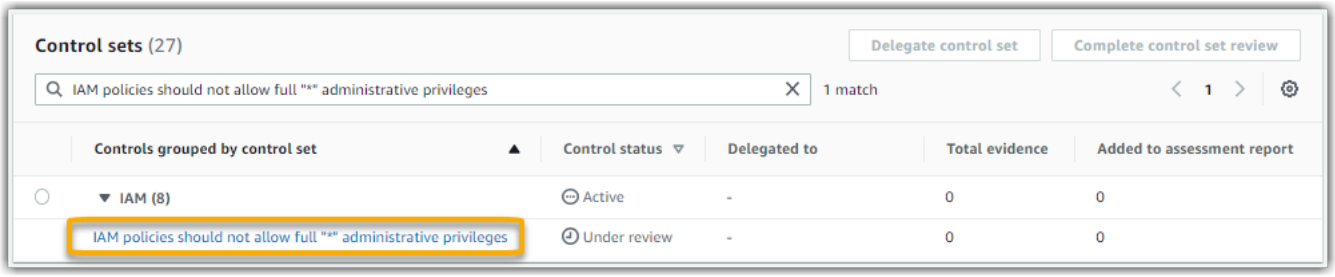
以 AWS Security Hub 當作資料來源類型的自動化控制項

此範例顯示使用 AWS Security Hub 作為其資料來源類型的控制項。這是取自 AWS 基礎安全性最佳作法 (FSBP) 架構的標準控制項。Audit Manager 程式會使用此控制項來產生證據，協助您的 AWS 環境符合 FSBP 需求。

控制項細節範例

- 控制項名稱 — `IAM policies should not allow full "*" administrative privileges`
- 控制集 — 此控制項屬於IAM控制集。這是與身分識別和存取管理相關的控制項群組。
- 資料來源類型 — AWS Security Hub
- 證據類型 — 合規檢查

在下列範例中，此控制項位於從 FSBP 架構建立的 Audit Manager 評估中。



評估會顯示控制狀態。顯示到目前為止，為此控制收集多少證據，以及您的評估報告中包含哪些證據。您可以從這裡委派控制集以供檢閱，或自行檢閱。選擇控制項名稱會開啟詳細資訊頁面，其中包含詳細資訊，包括該控制項的證據。

這個控制項可以做什麼

Audit Manager 可以使用此控制項來檢查您的 IAM 政策是否過於廣泛，無法符合 FSBP 要求。更具體地說，它可以檢查您的客戶受管 IAM 政策是否具有包含以下萬用字元陳述式的管理員存取權：`"Effect": "Allow"` 和 `"Action": "*"` 超過 `"Resource": "*"`。

Audit Manager 如何收集此控制項的證據

Audit Manager 會採取下列步驟來收集此控制項的證據：

1. Audit Manager 會針對每個控制項評估您的範圍內資源。它會使用控制項設定中指定的資料來源來執行此作業。在此範例中，您的 IAM 政策是資源和 Security Hub，AWS Config 是資料來源類型。Audit Manager 會尋找特定 Security Hub 檢查 結果 ([IAM.1])，並使用 AWS Config 規則來評估您的 IAM 政策 (iam-policy-no-statements-with-admin-access)。
2. 資源評估的結果將被保存，並轉換為易於稽核的證據。Audit Manager 會針對使用安全中樞作為資料來源類型的控制項產生合規檢查證據。此證據包含直接從 Security Hub 報告的合規檢查結果。
3. Audit Manager 會將儲存的證據附加至評估中名為 `IAM policies should not allow full "*" administrative privileges` 的控制項。

如何使用 Audit Manager 來證明對此控制項的合規性

將證據附加到控制項後，您或您選擇的委派代表可以檢閱證據，以查看是否需要進行任何修復。

在此範例中，Audit Manager 可能會顯示來自 Security Hub 的失敗裁決。如果您的 IAM 政策包含萬用字元 (*) 且範圍太廣而無法符合控制項，就可能會發生這種情況。在這種情況下，您可以更新 IAM 政策，使其不允許完整的管理權限。為實現這一點，您可以決定使用者需要執行哪些任務，然後打造讓使用者只執行這些任務的政策。此更正動作有助於使您的 AWS 環境符合 FSBP 需求。

當您的 IAM 政策符合控制項時，請將控制項標記為已檢閱，並將證據新增至您的評估報告。然後，您可以與稽核人員共用此報告，以證明控制項正在如預期般運作。

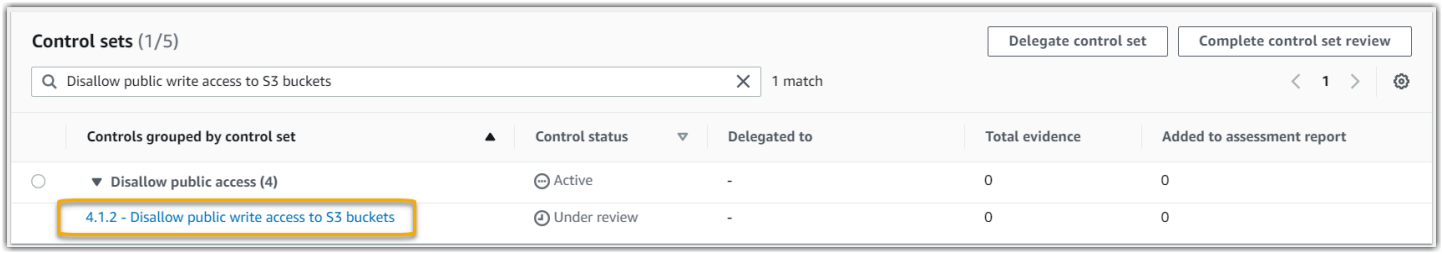
以 AWS Config 當作資料來源類型的自動化控制項

此範例顯示使用 AWS Config 作為其資料來源類型的控制項。這是取自 AWS Control Tower 防護機制架構的標準控制項。Audit Manager 使用此控制項來產生證據，協助您的 AWS 環境符合 AWS Control Tower 防護機制。

控制項細節範例

- 控制項名稱 — `4.1.2 - Disallow public write access to S3 buckets`
- 控制集 — 此控制項屬於`Disallow public access`控制集。這是與存取管理相關的控制項群組。
- 資料來源類型 — AWS Config
- 證據類型 — 合規檢查

在下列範例中，此控制項位於從AWS Control Tower防護機制架構建立的 Audit Manager 評估中。



評估顯示控制項狀態、到目前為止已為此控制項收集多少證據，以及您的評估報告中包含哪些證據。您可以從這裡委派控制集以供檢閱，或自行檢閱。選擇控制項名稱會開啟詳細資訊頁面，其中包含詳細資訊，包括該控制項的證據。

這個控制項可以做什麼

Audit Manager 可以使用此控制項來檢查 S3 儲存貯體政策的存取層級是否太寬鬆而無法滿足 AWS Control Tower 需求。更具體地說，它可以檢查封鎖公開存取功能設定、儲存貯體策略和儲存貯體存取控制清單 (ACL)，以確認您的儲存貯體不允許公開寫入存取權。

Audit Manager 如何收集此控制項的證據

Audit Manager 會採取下列步驟來收集此控制項的證據：

1. Audit Manager 會針對每個控制項，使用控制項設定中指定的資料來源評估範圍內的資源。在這種情況下，您的 S3 儲存貯體是資源，而 AWS Config 是資料來源類型。Audit Manager 會尋找特定

AWS Config 規則 (s3-bucket-public-write-prohibited) 的結果，以評估評估範圍內的每個 S3 儲存貯體的設定、政策和 ACL。

2. 資源評估的結果將被保存，並轉換為易於稽核的證據。Audit Manager 會為使用 AWS Config 資料來源類型的控制項產生合規檢查證據。此證據包含直接從 AWS Config 中回報的合規檢查的結果。
3. Audit Manager 會將儲存的證據附加至評估中名為 `4.1.2 - Disallow public write access to S3 buckets` 的控制項。

如何使用 Audit Manager 來證明對此控制項的合規性

將證據附加到控制項後，您或您選擇的委派代表可以檢閱證據，以查看是否需要進行任何修復。

在此範例中，Audit Manager 可能會顯示 AWS Config 指出 S3 儲存貯體不合規的裁決。假如其中一個 S3 儲存貯體具有不限制公用政策的封鎖公開存取功能設定，且使用中的政策允許公開寫入存取權，就可能會發生這種情況。如需修正此問題，您可以更新封鎖公開存取設定以限制公共策略。或者，您可以使用不允許公開寫入存取權的不同儲存貯體政策。此更正動作有助於使您的 AWS 環境符合 AWS Control Tower 需求。

當您確認 S3 儲存貯體存取層級符合控制項時，可以將該控制項標記為已檢閱，並將證據新增至您的評估報告。然後，您可以與稽核人員共用此報告，以證明控制項正在如預期般運作。

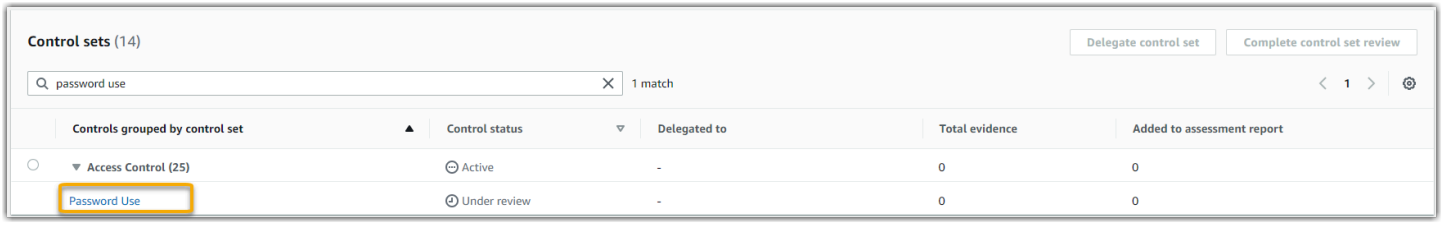
以 AWS API 呼叫當作資料來源類型的自動化控制項

此範例顯示使用 AWS API 呼叫作為其資料來源類型的控制項。Audit Manager 使用此控制項來產生證據，協助您的 AWS 環境符合您的特定需求。

控制項細節範例

- 控制項名稱 — `Password Use`
- 控制組 — 此控制項屬於稱為 `Access Control` 的控制集。這是與身分識別和存取管理相關的控制項群組。
- 資料來源類型 — AWS API 呼叫
- 證據類型 — 配置資料

在下列範例中，此控制項位於從自訂架構建立的 Audit Manager 評估中。



評估會顯示控制狀態。顯示到目前為止，為此控制收集多少證據，以及您的評估報告中包含哪些證據。您可以從這裡委派控制集以供檢閱，或自行檢閱。選擇控制項名稱會開啟詳細資訊頁面，其中包含詳細資訊，包括該控制項的證據。

這個控制項可以做什麼

Audit Manager 可以使用此自訂控制項，來協助您確保擁有足夠的存取控制項策略。此控制項要求您在選擇和使用密碼時遵循良好的安全實踐。Audit Manager 可以擷取位於評估範圍內的 IAM 主體的所有密碼政策清單，協助您驗證此問題。

Audit Manager 如何收集此控制項的證據

Audit Manager 採取下列步驟來收集此自訂控制項的證據：

1. Audit Manager 會針對每個控制項，使用控制項設定中指定的資料來源評估範圍內的資源。在這種情況下，您的 IAM 主體是資源，AWS API 呼叫是資料來源類型。Audit Manager 會尋找特定 IAM API 呼叫的結果 (GetAccountPasswordPolicy)。接著會傳回評估範圍內 AWS 帳戶 的密碼政策。
2. 資源評估的結果將被保存，並轉換為易於稽核的證據。Audit Manager 會為使用 API 呼叫作為資料來源的控制項產生組態資料證據。此證據包含從 API 回應擷取的原始資料，以及指示資料支援哪些控制項的其他中繼資料。
3. Audit Manager 會將儲存的證據附加至評估中名為 `Password Use` 的自訂控制項。

如何使用 Audit Manager 來證明對此控制項的合規性

將證據附加到控制項後，您或您選擇的委派代表可以檢閱證據，以查看證據是否充分或是否需要進行任何修補。

在此範例中，您可以檢閱證據以查看來自 API 呼叫的回應。GetAccountPasswordPolicy 回應說明了帳戶的使用者密碼複雜性要求和強制更換期限。您可以使用此 API 回應作為證據，以顯示您已針對評估範圍內的 AWS 帳戶，實施適當的密碼存取控制政策。如果需要，您也可以新增評論至控制項，以為相關政策提供其他見解。

當您對 IAM 主體的密碼政策符合自訂控制項感到滿意時，您可以將控制項標記為已檢閱，並將證據新增至您的評估報告。然後，您可以與稽核人員共用此報告，以證明控制項正在如預期般運作。

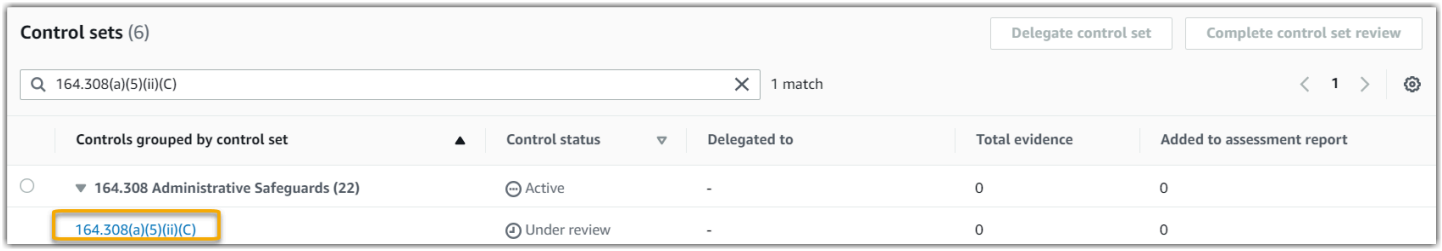
以 AWS CloudTrail 當作資料來源類型的自動化控制項

此範例顯示使用 AWS CloudTrail 作為其資料來源類型的控制項。這是取自 HIPAA 架構的標準控制項。Audit Manager 使用此控制項來產生證據，協助您的 AWS 環境符合 HIPAA 需求。

控制項細節範例

- 控制項名稱 — `164.308(a)(5)(ii)(C)`
- 控制集 — 此控制項屬於稱為`164.308 Administrative Safeguards`的控制集。
- 資料來源類型 — AWS CloudTrail
- 證據類型 — 使用者活動

以下是從 HIPAA 架構建立的 Audit Manager 評估中顯示的控制項：



評估會顯示控制狀態。顯示到目前為止，為此控制收集多少證據，以及您的評估報告中包含哪些證據。您可以從這裡委派控制集以供檢閱，或自行檢閱。選擇控制項名稱會開啟詳細資訊頁面，其中包含詳細資訊，包括該控制項的證據。

這個控制項可以做什麼

此控制項需要監控程序來偵測不適當的登入。當有人輸入多個使用者名稱或密碼組合以嘗試存取資訊系統時，就是不當登入的範例。Audit Manager 會針對評估範圍內的資源提供偵測到的所有嘗試登入清單，協助您驗證此控制項。

Audit Manager 如何收集此控制項的證據

Audit Manager 會採取下列步驟來收集此控制項的證據：

1. Audit Manager 會針對每個控制項，使用控制項設定中指定的資料來源評估範圍內的資源。在這種情況下，您的使用者是資源，CloudTrail 是資料來源類型。Audit Manager 會尋找 CloudTrail 記錄的所有 Amazon Web Services Management Console 登入事件的結果。然後，它會傳回評估範圍內相關事件的記錄。

2. 資源評估的結果將被保存，並轉換為易於稽核的證據。Audit Manager 會為使用 CloudTrail 作為資料來源類型的控制項產生使用者活動證據。此證據包含從您的使用者擷取的原始資料，以及指示資料支援哪些控制項的其他中繼資料。
3. Audit Manager 會將儲存的證據附加至評估中名為 `164.308(a)(5)(ii)(C)` 的控制項。

如何使用 Audit Manager 來證明對此控制項的合規性

將證據附加到控制項後，您或您選擇的委派代表可以檢閱證據，以查看是否需要進行任何修復。

在此範例中，您可以檢閱證據，以查看 CloudTrail 記錄的登入事件。此記錄檔說明使用者的主控台登入活動，其中包括下列資訊：

- 每次成功登入
- 每次登入失敗
- 驗證何時強制執行多重要素驗證 (MFA)
- 每個登入事件的 IP 地址

您可以使用此日誌作為證據，以顯示您已針對評估範圍內的 AWS 帳戶，實施足夠的監控程序。如果需要，您也可以新增評論至控制項，為相關政策提供其他見解。例如，如果日誌檔顯示任何差異 (例如多次嘗試登入失敗)，您可以新增評論，說明您如何修正問題。定期監控主控台登入狀況，可協助您避免因不一致和不當登入嘗試而產生的安全問題。反之，此最佳實務有助於使您的 AWS 環境符合 HIPAA 要求。

當您確認監控程序符合控制項時，可以將該控制項標記為已檢閱，並將證據新增至您的評估報告。然後，您可以與稽核人員共用此報告，以證明控制項正在如預期般運作。

手動控制

某些控制項不支援自動化證據收集。除了觀察、訪談和雲端中未產生的其他事件之外，這包括依賴提供實體記錄和簽名的控制項。在這些情況下，您可以手動上傳證據以證明您滿足控制項的要求。

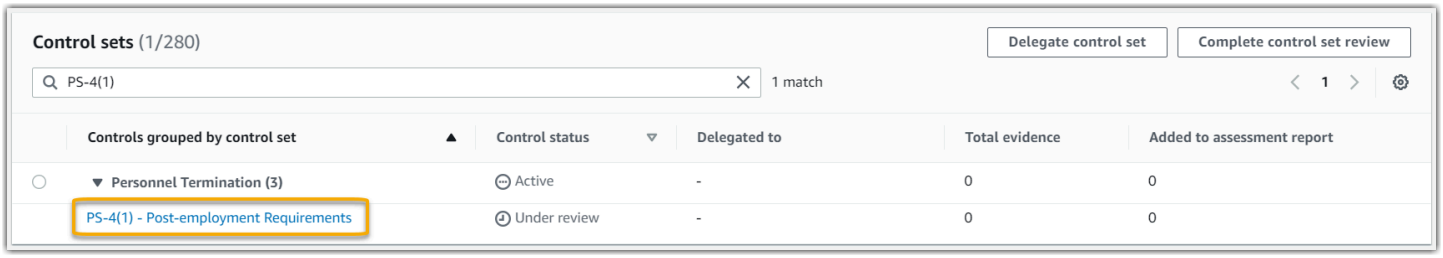
此範例顯示 Audit Manager 不會收集自動化證據的手動控制項。這是取自 NIST 800-53 (Rev. 5) 架構的標準控制項。您可以使用 Audit Manager 上傳並儲存證明此控制項的合規證據。

控制項細節範例

- 控制項名稱 — `PS-4(1) - Post-employment Requirements`

- 控制集 — 此控制項屬於Personnel Termination控制集。這是一組控制項，在僱傭終止程序的內容中與資訊安全有關。
- 資料來源類型 — 手動
- 證據類型 — 手動

這是在 Audit Manager 評估中顯示的控制項，該評估是根據 NIST 800-53 (Rev. 5) Low-Moderate-High 架構所建立：



評估會顯示控制狀態。顯示到目前為止，為此控制收集多少證據，以及您的評估報告中包含哪些證據。您可以從這裡委派控制集以供檢閱，或自行檢閱。選擇控制項名稱會開啟詳細資訊頁面，其中包含詳細資訊，包括該控制項的證據。

這個控制項可以做什麼

您可以利用此控制項來確保在員工離職時，組織的資訊獲得保護。具體來說，您可以證明您持續通知已終止契約的員工有適用、具法律約束力的離職後要求，以保護組織資訊。此外，您還可以證明，所有被終止契約的員工作為組織終止程序的過程中，都簽署了對解僱後要求的確認。

如何手動上傳此控制項的證據

您可以採取以下步驟上傳支援該控制項的手動證據：

1. 將您要上傳的手動證據放在 Amazon Simple Storage Service (S3) 儲存貯體中，並註記 S3 URI。
2. 在 Audit Manager 評估中，開啟控制項，前往證據資料夾索引標籤，然後輸入 S3 URI 以上傳證據。如需指示，請參閱 AWS Audit Manager 中的上傳手動證據。
3. Audit Manager 會建立以您上傳證據的日期命名的證據資料夾。然後 Audit Manager 會將上傳的證據附加至評估中名為 PS-4(1) - Post-employment Requirements 的控制項。

如何使用 Audit Manager 來證明對此控制項的合規性

如果您有支援此控制項的文件，您可以將其上傳為手動證據。例如，您可以上傳人力資源部門向終止契約的員工發出的最新具法律約束力的解僱後需求副本。如果在稽核期間有任何人被解僱，您亦可上傳離職員工的具日期記載的副本。

就像使用自動化控制項一樣，您可以將手動控制項委派給可協助您檢閱證據的利益關係者 (或在此情況下提供)。例如，當您檢閱此控制項時，您可能會發現只有部分符合其需求。如果您沒有由被解雇員工簽署的確認信，則可能是這種情況。您可以將控制權委派給 HR 利益關係者，然後他們可以上傳已簽署的信件副本。或者，如果稽核期間沒有員工離職，您可以留下評論，說明為何控制項沒有附加簽署的信件。

如果您滿意自己符合控制項，可以將其標記為已檢閱，並將證據新增至您的評估報告。然後，您可以與稽核人員共用此報告，以證明控制項正在如預期般運作。

具有混合資料來源類型的控制項 (自動和手動)

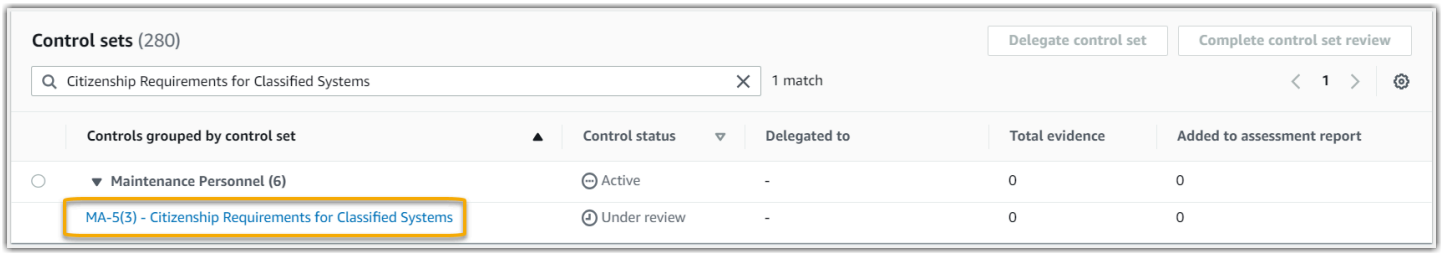
在許多情況下，需要結合自動化和手動證據來滿足控制項。雖然 Audit Manager 可以提供與控制項相關的自動化證據，但您可能需要使用您自己識別和上傳的手動證據來補充此資料。

此範例顯示一個控制項，該控制項使用來自 AWS API 呼叫的手動證據和自動化證據的組合。這是取自 NIST 800-53 (Rev. 5) 架構的標準控制項。Audit Manager 使用此控制項來產生證據，協助您的 AWS 環境符合 NIST 需求。

控制項細節範例

- 控制項名稱 — `MA-5(3) - Citizenship Requirements for Classified Systems`
- 控制集 — 此控制項屬於`Maintenance Personnel`控制集。這是一組控制項，涉及對組織系統執行硬體或軟體維護的個人。
- 資料來源類型 — AWS API 呼叫，以及補充的手動證據
- 證據類型 — 配置資料

這是在 Audit Manager 評估中顯示的控制項，該評估是根據 NIST 800-53 (Rev. 5) 架構所建立：



評估會顯示控制狀態。顯示到目前為止，為此控制收集多少證據，以及您的評估報告中包含哪些證據。您可以從這裡委派控制集以供檢閱，或自行檢閱。選擇控制項名稱會開啟詳細資訊頁面，其中包含詳細資訊，包括該控制項的證據。

這個控制項可以做什麼

Audit Manager 可以使用此控制項來協助您，確保執行維護和診斷活動的人員具有所需的公民身分。如果您的系統處理、儲存或傳輸機密資訊，您必須證明您的維護人員是美國公民。Audit Manager 可協助您驗證此項目。它會傳回評估範圍內所有 IAM 政策和主體的完整清單來達成此目的。然後，您可以驗證並證明此使用者名單滿足必要的公民身分要求。您可以透過手動上傳其公民身分的補充證據來做到這一點。

Audit Manager 如何收集此控制項的證據

Audit Manager 會採取下列步驟來收集此控制項的證據：

1. Audit Manager 會針對每個控制項，使用控制項設定中指定的資料來源評估範圍內的資源。在這種情況下，您的 IAM 政策和主體是資源，AWS API 呼叫是資料來源類型。Audit Manager 會尋找四個特定 IAM API 呼叫 (ListUsers/ListRoles/ListGroups/ListPolicies) 的結果，並傳回您評估範圍內的 IAM 政策和主體清單。
2. 資源評估的結果將被保存，並轉換為易於稽核的證據。Audit Manager 會為使用 API 呼叫作為資料來源類型的控制項產生組態資料證據。此證據包含從 API 回應擷取的原始資料，以及指示資料支援哪些控制項的其他中繼資料。
3. Audit Manager 會將儲存的證據附加至評估中名為 `MA-5(3) - Citizenship Requirements for Classified Systems` 的控制項。

如何手動上傳此控制項的證據

您可以採取以下步驟上傳補充自動化證據的手動證據：

1. 將公民身分文件放在 Amazon Simple Storage Service (Amazon S3) 儲存貯體中，並註明 S3 URI。
2. 在 Audit Manager 評估中，開啟控制項，前往證據資料夾索引標籤，然後上傳證據。您可以透過輸入 S3 URI 來執行此操作。如需指示，請參閱在 AWS Audit Manager 中國上傳手動證據。
3. Audit Manager 會將上傳的證據附加至評估中名為 `MA-5(3) - Citizenship Requirements for Classified Systems` 的控制項。

如何使用 Audit Manager 來證明對此控制項的合規性

將證據附加到控制項後，您或您選擇的委派代表可以檢閱證據，以查看證據是否充分或是否需要進行任何修補。

在此範例中，您可以檢閱證據並查看 20 位使用者的清單。如果您不確定如何分辨哪些使用者為維護人員，或使用者的公民身分，您可以將控制權委派給主題專家進行驗證。委派代表可以確認維護人員名單，並手動上傳補充證據作為其公民身分的文件。確認所有相關列出使用者的公民身分有助於使您的 AWS 環境符合 NIST 要求。或者，如果您的系統不處理、存取或傳輸機密資訊，您可以發表評論說明此控制項不適用的原因。

當您確認自己符合控制項時，可以將該控制項標記為已檢閱，並將證據新增至您的評估報告。然後，您可以與稽核人員共用此報告，以證明控制項正在如預期般運作。

與 AWS 服務 相關的整合

AWS Audit Manager 與多個 AWS 服務 整合，藉此自動化收集您可以包含在評估報告中的證據。

AWS Security Hub

AWS Security Hub 使用根據 AWS 最佳實務和業界標準的自動化安全檢查來監控您的環境。啟用 Security Hub 後，Audit Manager 會直接從 Security Hub 報告安全檢查結果，以擷取資源安全狀態的快照。如需有關 Security Hub 的詳細資訊，請參閱 AWS Security Hub 使用者指南 中的什麼是 AWS Security Hub？。

AWS CloudTrail

AWS CloudTrail協助您監控對帳戶中AWS資源所做的的呼叫。其中包括AWS 管理主控台、AWS CLI 和其他 AWS 服務 進行呼叫。Audit Manager 會直接從 CloudTrail 收集日誌資料，並將已處理的記錄檔轉換為使用者有效證據。如需有關 CloudTrail 的詳細資訊，請參閱 AWS CloudTrail 使用者指南中的什麼是 AWS CloudTrail？。

AWS Config

AWS Config - 提供您 AWS 帳戶 中 AWS 資源組態的詳細檢視。這包含資源彼此之間的關係和之前的組態方式的資訊。Audit Manager 直接從 AWS Config 報告調查結果，以擷取資源安全狀況的快照。如需 AWS Config 的詳細資訊，請參閱《AWS Config 使用者指南》中的什麼是 AWS Config？。

AWS License Manager

AWS License Manager 能夠簡化將軟體廠商授權遷往雲端的程序。在 AWS 上建置雲端基礎設施時，可透過重新規劃現有的授權庫存節省成本，以利搭配雲端資源使用。Audit Manager 提供 License

Manager 架構，協助您準備稽核。此架構與 License Manager 整合，可根據客戶定義的授權規則彙總授權使用資訊。如需有關 License Manager 的詳細資訊，請參閱 AWS License Manager 使用者指南中的什麼是 AWS License Manager？。

AWS Control Tower

AWS Control Tower針對雲端基礎架構強制執行預防性和偵測性防護機制。Audit Manager 提供 AWS Control Tower 防護機制架構，協助您進行稽核準備。此機制架構包含所有以來自 AWS Control Tower 的防護機制為基礎的 AWS Config 規則。如需 AWS Control Tower 的詳細資訊，請參閱《AWS Control Tower 使用者指南》中的什麼是 AWS Control Tower？。

AWS Artifact

AWS Artifact 是一個自助式稽核成品擷取入口網站，提供對 AWS 基礎架構的合規文件和認證的即時訪問。AWS Artifact 提供證據以證明 AWS 雲端基礎架構滿足合規要求。相對的，AWS Audit Manager 可協助您收集、檢閱和管理證據，以證明您的使用方式符合AWS 服務規定。如需 AWS Artifact 的詳細資訊，請參閱《AWS Artifact 使用者指南》中的什麼是 AWS Artifact？。您可以在 AWS Management Console 中下載 AWS 報告清單。

如需特定合規計劃範圍內的 AWS 服務 清單，請參閱合規計劃範圍內的 AWS 服務。如需更多一般資訊，請參閱 AWS 合規計劃。

與第三方 GRC 產品的整合

AWS Audit Manager 支援與此頁面上列出的第三方合作夥伴 GRC 產品整合。

如果您的公司使用混合雲端模式或多雲端模式，您很可能使用 GRC 產品來管理來自那些環境的證據。當該產品與 Audit Manager 整合時，您可以將您的 AWS 使用情況的相關證據直接提取到 GRC 環境中。這樣能在您準備稽核時，為您提供一個集中的位置來檢閱和修復證據，從而簡化您管理合規的方式。

閱讀此頁面，了解可從 Audit Manager 擷取證據的第三方廠商 GRC 產品概述。您也可以查看您能直接在這些產品中執行哪些 Audit Manager API 動作的參考資料。

主題

- 了解第三方整合如何與 Audit Manager 配合
- 與 Audit Manager 整合的第三方 GRC 合作夥伴產品

了解第三方整合如何與 Audit Manager 配合

GRC 合作夥伴可以使用 Audit Manager 公用 API，將其產品與 Audit Manager 整合。有了這項整合，您可以將 GRC 環境中的企業控制項映射至 Audit Manager 提供的控制項。

完成此一次性控制項映射練習後，您可以直接在 GRC 產品中建立 Audit Manager 評估。此動作會開始收集有關您的 AWS 使用情況的證據。然後，您可以查看此 AWS 證據以及從混合式環境中收集的其他證據，所有這些證據都在您的企業控制項的相同內容中。

當您將 Audit Manager 整合與第三方 GRC 產品時，請謹記以下幾點：

- 所有支援 Audit Manager 的 AWS 區域 都可以整合。
- 您在 GRC 合作夥伴產品中建立的任何 Audit Manager 理員資源也會反映在 Audit Manager 中。
- 除了第三方 GRC 產品的定價外，您還需要遵守 AWS Audit Manager 定價。
- Audit Manager 收集的證據是不可變的。在第三方 GRC 產品中，證據的呈現方式與 Audit Manager 主控台中的顯示方式完全相同。不過，如果您使用第三方整合，您或許可以在報告中提供其他內容，藉此增強此證據。
- 適用於 Audit Manager 的相同配額也適用於第三方 GRC 產品。例如，每個 AWS 帳戶 最多可以有 100 個有效的 Audit Manager 評估。無論您是在 Audit Manager 主控台還是在第三方 GRC 產品中建立評估，都會套用此帳戶層級配額。大多數 Audit Manager 配額 (但不是全部) 都列在 Service Quotas 控制台的 AWS Audit Manager 命名空間下。如需要求增加配額，請參閱 管理您的 Audit Manager 配額。

如果您有合規解決方案，並且有興趣與 Audit Manager 整合，請傳送電子郵件至 `auditmanager-partners@amazon.com`。

與 Audit Manager 整合的第三方 GRC 合作夥伴產品

下列第三方 GRC 產品可以擷取 Audit Manager 的證據。

MetricStream

要使用此整合功能，請聯繫MetricStream以訪問和購買 MetricStream GRC 軟體。

MetricStream 企業 GRC 解決方案建立在其平台上，可為企業範圍的 GRC 活動和流程提供全面性的協作方法。透過將 Audit Manager 的證據導入 MetricStream，您可以主動從 AWS 環境中分辨不合規的證據，並與內部部署資料來源或其他雲端合作夥伴的證據共同檢閱。這為您提供了一種方便且集中的方式，以便在準備稽核時檢閱並改善雲端安全性和合規狀態。

透過整合 MetricStream 和 Audit Manager，您可以執行以下 API 操作。

任務	API 操作
Audit Manager 整合設定	• GetAccountStatus • GetOrganizationAdminAccount • GetSettings
Audit Manager 資源檢閱	• GetAssessment • GetAssessmentFramework • GetControl • ListAssessmentFrameworks • ListControls
Audit Manager 資源建立	• CreateAssessment • CreateAssessmentFramework
Audit Manager 資源更新	• UpdateAssessment • UpdateAssessmentControl • UpdateAssessmentStatus
管理證據	• StartQuery (AWS CloudTrail API) • GetQueryResults (AWS CloudTrail API)
Audit Manager 資源刪除	• DeleteAssessmentFramework

MetricStream 相關連結

- AWS Marketplace 連結
- 產品連結
- 產品定價

搭配 AWS SDK 使用 Audit Manager

AWS 軟體開發套件 (SDK) 適用於許多常用的程式設計語言。每個 SDK 都提供 API、程式碼範例和文件，讓開發人員以偏好的語言建置應用程式。

SDK 文件	Audit Manager 特定文件	程式碼範例	
AWS SDK for C++	AWS SDK for C++Audit Manager 的 API 參考	AWS SDK for C++ 程式碼範例	
AWS SDK for Go	AWS SDK for GoAudit Manager 的 API 參考	AWS SDK for Go 程式碼範例	
AWS SDK for Java	AWS SDK for Java 2.xAudit Manager 的 API 參考	AWS SDK for Java 程式碼範例	
AWS SDK for JavaScript	AWS SDK for JavaScriptAudit Manager 的 API 參考	AWS SDK for JavaScript 程式碼範例	
AWS SDK for .NET	AWS SDK for .NETAudit Manager 的 API 參考	AWS SDK for .NET 程式碼範例	
AWS SDK for PHP	AWS SDK for PHPAudit Manager 的 API 參考	AWS SDK for PHP 程式碼範例	
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto)Audit Manager 的 API 參考	AWS SDK for Python (Boto3) 程式碼範例	
AWS SDK for Ruby	AWS SDK for RubyAudit Manager 的 API 參考	AWS SDK for Ruby 程式碼範例	

如需 Audit Manager 專屬的範例，請參閱 AWS Audit Manager 的程式碼範例。

> **Note**
>
> Audit Manager 在核心版本 1.19.32 及更新版本 AWS SDK for Python (Boto3) 中提供。開始使用 SDK 之前，請確定您使用的是適當的核心版本。

設定 AWS Audit Manager

開始使用 Audit Manager 前，請確保您已完成下列設定工作。

主題

必要條件

請依照下列步驟建立AWS 帳戶和具有 Audit Manager 安裝權限的管理使用者。

步驟

> **Important**
>
> 如果已設定 AWS 和 IAM，則可略過步驟 1 和 2。但是，您必須完成步驟 3，以確保您具有設定 Audit Manager 所需的許可。

註冊 AWS 帳戶

如果您還沒有 AWS 帳戶，請完成以下步驟建立新帳戶。

註冊 AWS 帳戶

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

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

註冊 AWS 帳戶時，會建立 AWS 帳戶根使用者。根使用者有權存取該帳戶中的所有 AWS 服務和資源。作為最佳安全實務，將管理存取權指派給管理使用者，並且僅使用根使用者來執行需要根使用者存取權的任務。

註冊程序完成後，AWS 會傳送一封確認電子郵件給您。您可以隨時登錄 https://aws.amazon.com/ 並選擇 我的帳戶，以檢視您目前的帳戶活動並管理帳戶。

建立管理使用者

在您註冊 AWS 帳戶 之後，請保護您的 AWS 帳戶根使用者、啟用 AWS IAM Identity Center，以及建立管理使用者，讓您可以不使用根使用者處理日常作業。

保護您的 AWS 帳戶根使用者

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

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

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

建立管理使用者

1. 啟用 IAM Identity Center。

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的啟用 AWS IAM Identity Center。
2. 在 IAM Identity Center 中，將管理存取權授予管理使用者。

   有關如何使用 IAM Identity Center 目錄 作為身分來源的教學課程，請參閱《AWS IAM Identity Center 使用者指南》中的以預設 IAM Identity Center 目錄 設定使用者存取權。

以管理員的身分登入

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

如需有關如何使用 IAM Identity Center 使用者登入的說明，請參閱《AWS 登入 使用者指南》中的登入 AWS存取入口網站。

新增存取和啟用 Audit Manager 所需的許可

您必須向使用者授予啟用 Audit Manager 所需的許可。對於需要 Audit Manager 完整存取權限的使用者，請使用 AWSAuditManagerAdministratorAccess的受管政策。這是您的AWS 帳戶中可用的AWS受管策略，它是 Audit Manager 的建議策略。

> **Tip**
>
> 為了安全性最佳實務，建議您先使用AWS受管政策，然後轉向最低權限。 AWS受管政策可用於授予許多常用案例的權限。但是，請記住，由於 AWS 受管政策可供所有 AWS 客戶使用，因此它們可能不會授與您特定使用案例的最低權限許可。因此，我們建議您定義使用案例的客戶管理政策，以便進一步減少許可。如需詳細資訊，請參閱AWS Identity and Access Management IAM 使用者指南中的AWS 受管政策。

若要提供存取權，請新增權限至您的使用者、群組或角色：

- AWS IAM Identity Center 中的使用者和群組：

  建立權限合集。請遵循 AWS IAM Identity Center 使用者指南 的 建立權限合集 中的指示。
- 透過身分提供者在 IAM 中管理的使用者：

  建立聯合身分的角色。請遵循 IAM 使用者指南 的 為第三方身分提供者 (聯合) 建立角色 中的指示。
- IAM 使用者：
  - 建立您的使用者可擔任的角色。請遵循 IAM 使用者指南 的 為 IAM 使用者建立角色 中的指示。
  - (不建議) 將政策直接附加至使用者，或將使用者新增至使用者群組。請遵循 IAM 使用者指南 的 新增權限至使用者 (主控台) 中的指示。

啟用 AWS Audit Manager

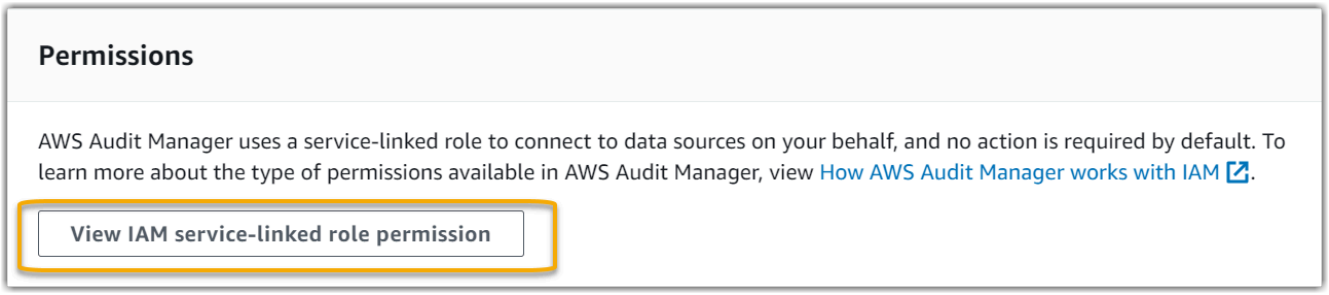
您可以使用 AWS Management Console、Audit Manager API 或 AWS Command Line Interface (AWS CLI) 來啟用 Audit Manager。

Audit Manager console

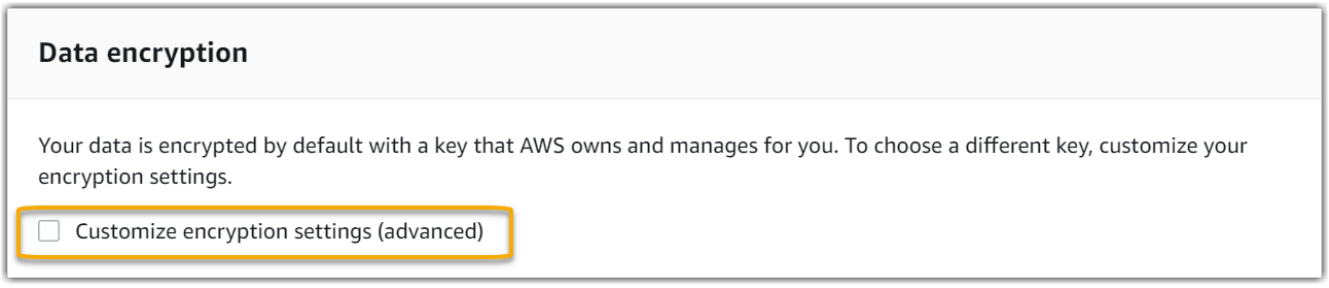
如需使用主控台來啟用 Audit Manager

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 使用 IAM 身分的憑證登入。
3. 選擇 Set up (設定)AWS Audit Manager。

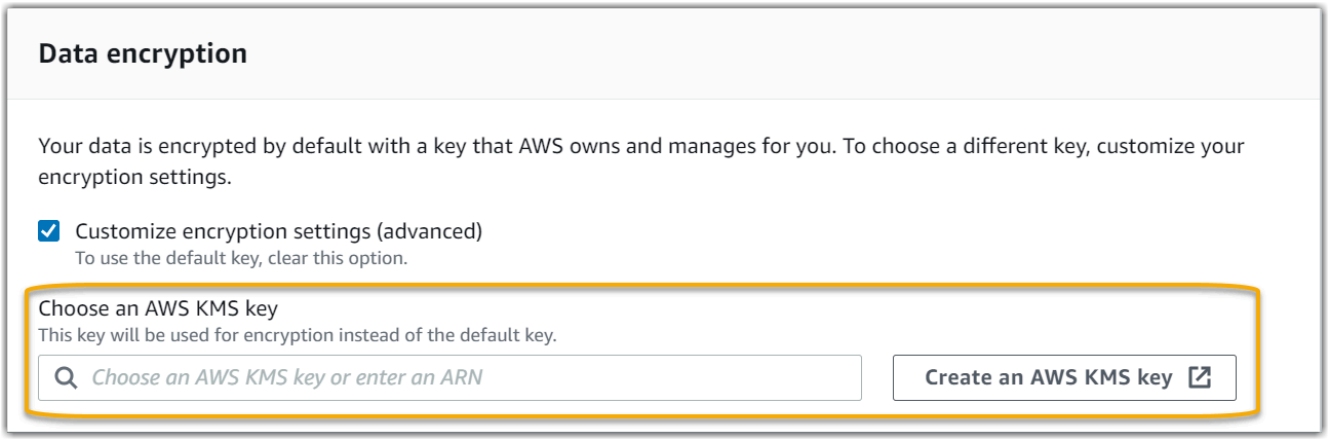
4. 在權限中，無須採取任何動作。這是因為 Audit Manager 使用服務連結角色代表您連線到資料來源。您可以選擇查看 IAM 服務連結角色權限，以查看服務連結角色。



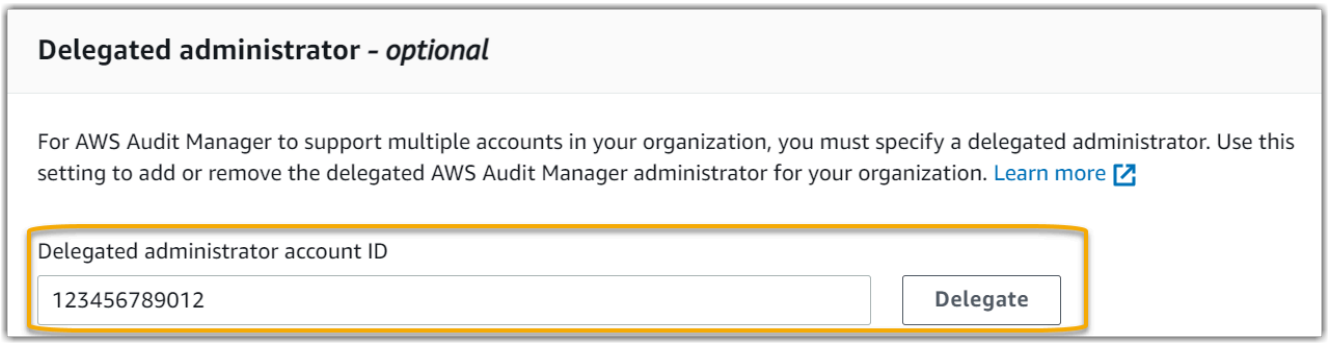
5. 在 資料加密 下，預設選項是讓 Audit Manager 建立和管理AWS KMS key，以安全地儲存資料。



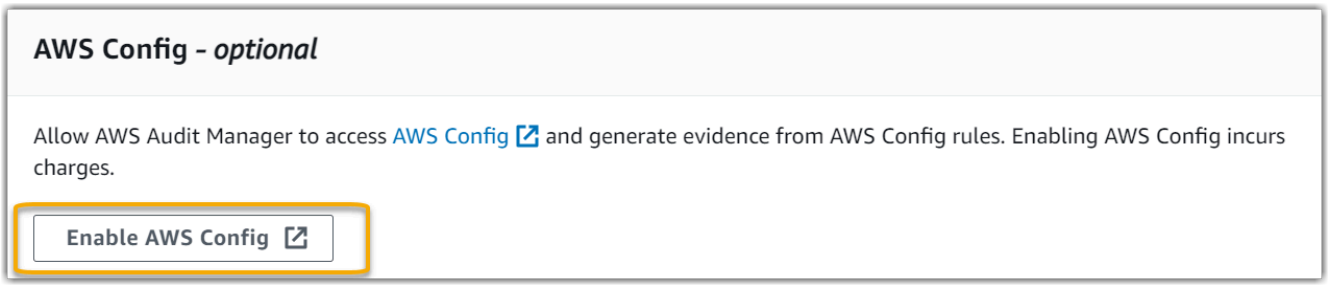
如果您想要使用自己的客戶管理金鑰來加密 Audit Manager 中的資料，請選取自訂加密設定 (進階) 旁邊的核取方塊。然後，您可選擇現有 KMS 金鑰或 建立新的金鑰。



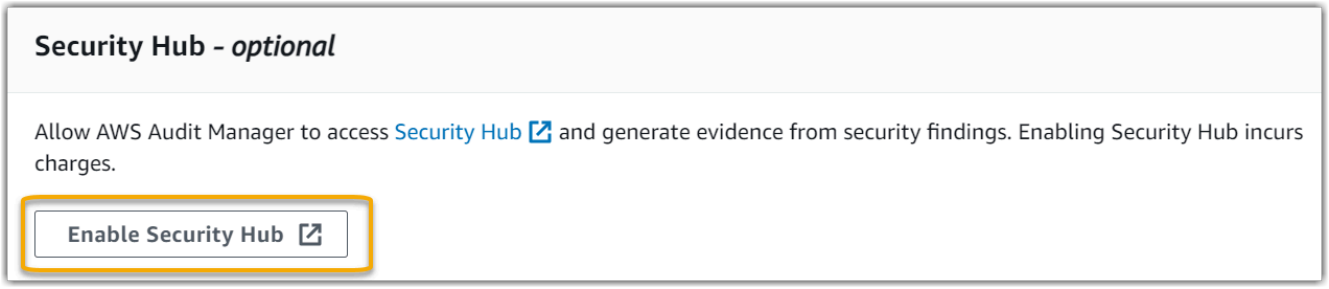
6. (選擇性) 如果您希望 Audit Manager 針對多個帳戶執行評估，您可以在委派管理員-選擇性下指定委派管理員帳戶。如需詳細資訊和建議，請參閱啟用和設定AWS Organizations以搭配 Audit Manager 使用。



7. (選擇性) 在 AWS Config— 選擇性部分中，我們建議您啟用AWS Config，以最佳體驗。這可讓 Audit Manager 使用 AWS Config 規則產生證據。如需指示和建議設定，請參閱啟用和設定AWS Config以與 Audit Manager 搭配使用。



8. (選擇性) 在 Security Hub — 選擇性部分中，我們建議您啟用 Security Hub 以獲得最佳體驗。這可讓 Audit Manager 使用 Security Hub 檢查產生證據。如需指示和建議設定，請參閱啟用和設定AWS Security Hub以與 Audit Manager 搭配使用。



9. 選擇 完成設定 以完成設定程序。

AWS CLI

使用AWS CLI啟用 Audit Manager

在命令列中，使用下列設定參數執行註冊帳戶命令：

- `--kms-key`(選擇性) — 使用此參數可使用您自己的客戶管理金鑰來加密 Audit Manager 資料。如果您未在此處指定選項，Audit Manager 會代表您建立和管理AWS KMS key資料的安全儲存。
- `--delegated-admin-account`(選擇性) — 使用此參數可為 Audit Manager 指定組織的委派管理員帳戶。如果您未在此處指定選項，則不會註冊委派管理員。

輸入範例（用自己的資訊替換`######`）：

```
aws auditmanager register-account \
--kms-key arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab \
--delegated-admin-account 111122224444
```

輸出範例：

```
{
    "status": "ACTIVE"
}
```

如需 AWS CLI 的詳細資訊及安裝 AWS CLI 工具的說明，請參閱AWS Command Line Interface 使用者指南中的以下內容。

- AWS 命令列介面使用者指南
- 設定 AWS Command Line Interface

Audit Manager API

如需使用 Audit Manager API 啟用 Audit Manager

使用 RegisterAccount 作業搭配下列設定參數：

- KMSKey (選擇性) — 使用此參數可使用您自己的客戶管理金鑰來加密 Audit Manager 資料。如果您未在此處指定選項，Audit Manager 會代表您建立和管理AWS KMS key資料的安全儲存。
- delegatedAdminAccount (選擇性) — 使用此參數可為 Audit Manager 指定組織的委派管理員帳戶。如果您未指定，則不會註冊委派管理員。

輸入範例（用自己的資訊替換######）：

```
{
    "kmsKey":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "delegatedAdminAccount":"111122224444"
}
```

輸出範例：

```
{
  "status": "ACTIVE"
}
```

建議

為了在 Audit Manager 中獲得最佳體驗，建議您設定下列功能並啟用下列 AWS 服務。

主題

- 設定建議的 Audit Manager 功能
- 設定與其他建議的整合AWS 服務

設定建議的 Audit Manager 功能

在您啟用 Audit Manager 之後，建議您啟用證據搜尋工具功能。

證據搜尋工具提供了一種在 Audit Manager 之中搜尋索證據的強大方法。您可以使用證據搜尋工具快速查詢證據，不須一頭栽進證據資料夾，想辦法找出您要查找的內容。如果您以委派管理員的身分使用證據搜尋工具，您可以在組織中的所有成員帳戶中搜尋證據。使用篩選條件和群組的組合，您可以逐步縮小搜尋查詢的範圍。例如，如果您想要系統健全狀況的高階檢視，請擴大搜尋範圍，並依據評估、日期範圍和資源合規性進行篩選。如果您的目標是修復特定資源，則可以縮小搜尋範圍，以針對特定控制項或資源 ID 的證據作為目標。定義篩選條件後，您可以先分組並預覽相符的搜尋結果，然後再建立評估報告。

若要使用證據搜尋工具，您必須從 Audit Manager 設定中啟用此功能。如需說明，請參閱 證據搜尋工具設定。

設定與其他建議的整合AWS 服務

為了在 Audit Manager 中獲得最佳體驗，我們強烈建議您啟用下列項目AWS 服務：

- AWS Organizations— 您可以使用 Organizations 對多個帳戶執行 Audit Manager 評估，並將證據合併到委派管理員帳戶中。
- AWS Security Hub 和 AWS Config — 啟用這些 AWS 服務 時，它們可以做爲 Audit Manager 評估中控制項的資料來源類型。然後，Audit Manager 可以直接從這些服務報告合規檢查的結果。

主題

啟用和設定 AWS Config（選擇性）

Audit Manager 中的許多控制項都用 AWS Config 做爲資料來源類型。若要支援這些控制項，您必須在每個已啟用AWS 區域 Audit Manager 的所有帳號上啟用AWS Config。如果 Audit Manager 嘗試收集使用AWS Config作為資料來源類型之控制項的證據，且未啟用相關AWS Config規則，則不會收集這些控制項的證據。

Audit Manager 不會為您管理 AWS Config。您可以按照以下步驟啟用AWS Config和配置其設定。

將 AWS Config 與 Audit Manager 整合的任務

- 步驟 1：啟用 AWS Config
- 步驟 2：設定您的 AWS Config 設定，以便與 Audit Manager 搭配使用

步驟 1：啟用 AWS Config

您可以使用 AWS Config 主控台或 API 來啟用 AWS Config。如需指示，請參閱AWS Config 開發人員指南中的AWS Config 入門。

步驟 2：設定您的 AWS Config 設定，以便與 Audit Manager 搭配使用

> **Important**
>
> 啟用 AWS Config 是選擇性建議。但是，如果啟用 AWS Config，則需要以下設定。

啟用AWS Config之後，請務必同時針對與稽核相關的規範標準啟用AWS Config規則或部署一致性套件。此步驟可確保 Audit Manager 可以針對您啟用的AWS Config規則匯入調查結果。

在您可以啟用 AWS Config 規則後，建議您檢閱該規則的參數。然後，您應該根據所選合規性架構的要求來驗證這些參數。如果需要，您可以更新AWS Config中的規則參數，確保其符合架構需求。這將有助於確保您的評估為該給定架構收集正確的合規檢查證據。

例如，假設您正在為 CIS v1.2.0 建立評估。此架構包含一個名為 1.4 — 確保存取金鑰每 90 天或更短的時間輪換一次的控制項。在AWS Config中，存取金鑰輪換的規則具有預設值 90 天的`maxAccessKeyAge`參數。因此，該規則符合控制項的需求。如果您不使用預設值，請確保您使用的值等於或大於 CIS v1.2.0 的 90 天要求。

您可以在 AWS Config 文件中找到每個受管規則的預設參數詳細資訊。如需如何配置規則的指示，請參閱使用AWS Config受管規則。

啟用和設定 AWS Security Hub（選擇性）

Audit Manager 中的許多控制項會使用 Security Hub 做為資料來源類型。若要支援這些控制項，您必須在每個已啟用 Audit Manager 的區域中的所有帳戶上啟用 Security Hub。如果 Audit Manager 嘗試收集使用 Security Hub 做為資料來源類型之控制項的證據，且未啟用相關的 Security Hub 標準，則不會針對這些控制項收集任何證據。

Audit Manager 不會為您管理 Security Hub。您可以按照以下步驟啟用 Security Hub 並配置其設定。

將 AWS Security Hub 與 Audit Manager 整合的任務

- 步驟 1：啟用 AWS Security Hub
- 步驟 2：設定您的 Security Hub 設定，以便與 Audit Manager 搭配使用

步驟 1：啟用 AWS Security Hub

您可以使用主控台或 API 以啟用 Security Hub。如需指示，請參閱AWS Security Hub使用者指南中的設定AWS Security Hub。

步驟 2：設定您的 Security Hub 設定，以便與 Audit Manager 搭配使用

> **Important**
>
> 啟用 Security Hub 是選擇性建議。不過，如果您確實啟用 Security Hub，則需要下列設定。

在您可以啟用 Security Hub 後，請確認執行下列作業：

- 啟用AWS Config和設定資源記錄- Security Hub 使用服務連結AWS Config規則來執行控制項的大部分安全檢查。若要支援這些控制項，AWS Config 必須啟用並設定為記錄您在每個已啟用標準中啟用之控制項所需的資源。
- 啟用所有安全標準-此步驟可確認 Audit Manager 能匯入所有支援的合規標準的調查結果。
- 開啟 Security Hub 的合併控制項調查結果設定 - 如果您在 2023 年 2 月 23 日或之後啟用 Security Hub，則預設會開啟此設定。

> **Note**
>
> 當您啟用合併的調查結果時，Security Hub 會針對每個安全檢查產生單一調查結果 (即使跨多個標準使用相同的檢查也是如此)。每個 Security Hub 調查結果都會做為 Audit Manager 中一項獨立資源評估來收集。因此，合併的調查結果會導致 Audit Manager 針對 Security Hub 調查結果執行的獨立資源評估總計減少。因此，使用合併的調查結果通常有效降低 Audit Manager 使用成本。如需有關使用 Security Hub 做為資料來源類型的詳細資訊，請參閱AWS Security Hub 支援的控制項 AWS Audit Manager。如需 Audit Manager 定價的詳細資訊，請參閱AWS Audit Manager定價。

如果您使用AWS Organizations並且想要從您的成員帳戶收集 Security Hub 證據，請在 Security Hub 中執行下列步驟。

設定您組織的 Security Hub 設定

1. 登入 AWS Management Console，並開啟位於 https://console.aws.amazon.com/securityhub/ 的 AWS Security Hub 主控台。
2. 使用您的AWS Organizations管理帳戶，將帳戶指定為 Security Hub 的委派管理員。如需詳細資訊，請參閱AWS Security Hub使用者指南中的指定 Security Hub 管理員帳戶。

   > **Note**
   >
   > 確認您在 Security Hub 中使用的委派管理員帳戶與您在 Audit Manager 中使用的帳戶相同。

3. 使用您的 Organizations 委派管理員帳戶，移至 設定、帳戶，選取所有帳戶，然後選取 自動註冊將其新增為成員。如需詳細資訊，請參閱AWS Security Hub 使用者指南中的啟用組織中的成員帳戶。
4. 為組織的每個成員帳戶啟用AWS Config。如需詳細資訊，請參閱AWS Security Hub 使用者指南中的啟用組織中的成員帳戶。
5. 為組織的每個成員帳戶啟用 PCI DSS 安全標準。AWSCIS 基準指標標準和AWS基礎最佳實務標準已預設為啟用狀態。如需詳細資訊，請參閱AWS Security Hub使用者指南中的啟用安全標準。

啟用 AWS Organizations (選擇性)

Audit Manager 透過與AWS Organizations的整合支援多個帳戶。Audit Manager 可以對多個帳戶執行評估，並將證據合併到委派管理員帳戶中。委派管理員擁有建立及管理以組織做為信任區域之 Audit Manager 資源的許可。只有管理帳戶可以指定委派管理員。

將 AWS Organizations 與 Audit Manager 整合的任務

- 步驟 1：建立或加入組織
- 步驟 2：啟用您組織中的所有功能
- 步驟 3：為 Audit Manager 指定委派管理員

步驟 1：建立或加入組織

如果您的AWS 帳戶不是組織的一部分，您可以建立或加入組織。如需指示，請參閱AWS Organizations使用者指南中的建立和管理組織。

步驟 2：啟用您組織中的所有功能

下一步，必須啟用您組織中的所有功能。如需指示，請參閱AWS Organizations 使用者指南中的啟用組織中的所有功能。

步驟 3：為 Audit Manager 指定委派管理員

建議您使用 Organizations 管理帳戶啟用 Audit Manager 管理員，然後指定委派管理員。之後，您可以使用委派管理員帳戶登入並執行評估。根據最佳實務，建議您僅使用委派管理員帳戶來建立評估，而不是使用管理帳戶。

> **Warning**
>
> 使用 Organizations 管理帳戶指定委派管理員後，您的管理帳戶將無法再在 Audit Manager 中建立其他評估。此外，管理帳戶建立的任何現有評估之證據收集都會停止。相反地，Audit Manager 會收集證據並附加至委派管理員，委派管理員是管理組織評估的主要帳戶。

若要在啟用 Audit Manager 之後新增或變更委派管理員，請參閱AWS Audit Manager設定，委派管理員。

需考慮的問題：

- 您無法在 Audit Manager 中使用管理帳號作為委派系統管理員。
- 如果您要在多個 AWS 區域 啟用 Audit Manager，則必須在每個區域中單獨指定委派的管理員帳戶。在 Audit Manager 設定中，應為所有區域指定相同的委派系統管理員帳戶。
- 如果您在啟用 Audit Manager 時提供了客戶管理金鑰，請確定委派管理員帳戶具有該 KMS 金鑰的存取權。若要檢閱和變更您的 Audit Manager 加密設定，請參閱資料加密。
- 如需 Audit Manager 中常見組織和委派管理員問題的解決方案，請參閱委派系統管理員與 AWS Organizations 相關問題疑難排解。

我接下來要怎麼做？

現在您已設定 Audit Manager，則可以開始使用該服務了。您也可以造訪主控台的設定頁面來更新您在設定 Audit Manager 時選擇的任何設定。

Audit Manager 入門

您可以按照逐步引導您如何建立首個評估的自學課程，在 Audit Manager 中開始使用。如需詳細資訊，請參閱稽核擁有者教學課程：建立評估。

更新您的 Audit Manager 設定

您可以隨時更新您的設定。如需詳細資訊，請參閱 AWS Audit Manager 設定。

AWS Audit Manager 入門

透過本節中的逐步教學課程，您可以了解如何運用 AWS Audit Manager 來執行任務。

> **Tip**
>
> 以下教學課程按受眾進行分類。根據您身為稽核擁有者或委派代表的角色不同，選擇適合您的教學課程。
>
> - 稽核擁有者是負責建立及管理評估的 Audit Manager 使用者。在商業世界中，稽核擁有者通常是治理、風險管理和法規遵循 (GRC) 專業人員。不過，在 Audit Manager 的內容中，來自 SecOps 或 DevOps 團隊的人員，也可能會是扮演稽核擁有者的使用者角色。稽核擁有者可以向主題專家 (也稱為委派代表) 要求協助，以檢閱特定控制項並驗證證據。稽核擁有者必須要有必要授權，才可管理評估。
> - 委派代表是具有專業技術或業務專業知識的主題專家。雖然他們不擁有或管理稽核管理員評估，但他們仍然可以對其做出貢獻。委派代表協助稽核擁有者完成任務，例如驗證屬於其專業領域的控制項的證據。委派代表在 Audit Manager 中具有有限的權限。這是因為稽核擁有者委派特定控制集以供檢閱，而不是委派整個評估。
>
> 如需有關這些人物角色和其他 Audit Manager 概念的詳細資訊，請參閱本指南第 AWS Audit Manager 概念和術語 節中的稽核擁有者與委派代表。如需每個角色建議 IAM 授權的詳細資訊，請參閱 中使用者角色的建議政策 AWS Audit Manager。

Audit Manager 教學

建立評估

對象：稽核擁有者

概觀：按照逐步說明建立您的第一個評估並快速啟動運行。本教學課程將逐步引導您如何使用標準架構來建立評估，並開始自動收集證據。

檢閱控制集

對象：委派代表

概觀：檢閱屬於您專業領域的控制項的證據，以協助稽核擁有者。了解如何檢閱控制集及其相關證據、新增評論、上傳其他證據，以及更新控制項的狀態。

稽核擁有者教學課程：建立評估

本教學課程提供有關 AWS Audit Manager 的簡介。在本教學課程中，您會使用 AWS Audit Manager 範例架構建立評估。藉由建立評估，您可以啟動該架構中控制項的持續自動化證據收集程序。

此教學課程會讓您了解如何執行以下操作：

- 選取要建立評估的標準架構
- 指定要包含在評估中的 AWS 帳戶
- 指定要包含在評估中的 AWS 服務
- 指定評估的稽核擁有者
- 檢閱並建立您的評估

在您開始教學課程之前，請務必先達成以下條件：

- 您已完成 設定 AWS Audit Manager 中描述的所有先決條件。如需完成此教學課程，您必須使用 AWS 帳戶和 AWS Audit Manager 主控台。
- 您的 IAM 身分會被授與適當的授權，以便在 AWS Audit Manager 中建立和管理評估。授與這些權限的兩個建議原則為範例 2：允許完整的系統管理員存取權限和範例 3：允許管理存取權限。
- 您對 Audit Manager 的術語和功能已經很熟悉了。如需一般概觀，請參閱 什麼是 AWS Audit Manager？ 和 AWS Audit Manager 概念和術語。

> **Note**
>
> AWS Audit Manager 協助收集與驗證符合特定合規架構和法規相關的證據。不過，這不會評估您的合規狀態。因此，透過 AWS Audit Manager 收集的證據可能不包含稽核所需的所有關於您的 AWS 使用資訊。AWS Audit Manager 不是法律顧問或合規專家的替代方案。

步驟 1：指定評估詳細資訊

第一步，請選取架構並提供評估的基本資訊。

指定評估詳細資訊

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。

2. 選擇 Launch (啟動)AWS Audit Manager。
3. 在導覽窗格中，選擇入門，然後選擇架構入門。
4. 選擇您要的架構，然後選擇從架構建立評估。此範例使用 AWS Audit Manager 範例架構。
5. 在評估名稱下，輸入評估的名稱。
6. (選擇性) 在評估說明下，輸入評估的說明。
7. 在評估報告目標下，選擇您要儲存評估報告的 Amazon S3 儲存貯體。
8. 在架構下，確認已選擇 AWS Audit Manager 範例架構 (或您選擇的架構)。
9. 在標籤下，選擇新增標籤，將標籤與評估產生關聯。您可以指定每一個標籤的金鑰和值。標籤索引鍵是必要的，在搜尋此評估時，可用作搜尋條件。如需 AWS Audit Manager 中標籤的詳細資訊，請參閱標記 AWS Audit Manager 資源。
10. 選擇 Next (下一步)。

步驟 2：指定 AWS 範圍內的帳戶

接下來，指定您要包含在評估範圍中的 AWS 帳戶。

AWS Audit Manager 與 AWS Organizations 整合，因此您可以跨多個帳戶執行 Audit Manager 評估，並將證據合併到委派系統管理員帳戶中。如需在 Audit Manager 中啟用組織 (如果尚未啟用)，請參閱本指南設定頁面上的 啟用 AWS Organizations (選擇性)。

> **Note**
>
> Audit Manager 可以支援單一評估範圍內最多 150 個成員帳戶。如果您嘗試涵蓋超過 150 個帳戶，則評估建立可能會失敗。

指定範圍內帳戶

1. 在AWS帳戶下，選取您要包含在評估範圍中的 AWS 帳戶。
   - 如果您在 AWS Audit Manager 中啟用了組織，則會列出多個帳戶。
   - 如果您未在 Audit Manager 中啟用組織，則只會列出您目前的帳戶。
2. 選擇 Next (下一步)。

步驟 3：指定範圍中的 AWS 服務

您先前選取的架構會定義 Audit Manager 監控及收集證據的 AWS 服務。

當您使用 Audit Manager 主控台從標準架構建立評估時，範圍內的服務清單會被預先選取，無法編輯。這是因為 Audit Manager 會自動為您映射並選擇資料來源和服務。此選擇是根據標準架構的要求所進行。如果列出的 AWS 服務未被選取，則 Audit Manager 不會從與該服務相關的資源收集證據。如果已選取，但您尚未在環境中訂閱它，也會發生同樣情況。

在教學課程的這個步驟中，您可以根據架構定義來檢閱評估範圍內的 AWS 服務。如需進一步了解架構以及如何存取和檢閱架構，請參閱本指南的 架構程式庫 章節。

指定範圍內的 AWS 服務

1. 在AWS服務下方，檢閱此評估範圍內的服務清單。
2. 選擇 Next (下一步)。

> **Tip**
>
> 如果您需要編輯範圍中的服務清單，您可以使用 Audit Manager 提供的 CreateAssessment API 來執行此操作。
> 或者，您可以自訂標準架構，然後從自訂架構中建立評估。

步驟 4：指定稽核擁有者

在此步驟中，您可以指定評估的稽核擁有者。稽核擁有者是工作場所中負責管理稽核管理員評估的個人，通常來自 GRC、SecOps 或 DevOps 團隊。我們建議他們使用 AWSAuditManagerAdministratorAccess 政策。

如需指定稽核擁有者

1. 在稽核擁有者底下，選擇要進行評估的稽核擁有者。如需尋找其他稽核擁有者，請使用搜尋列，按名稱或 AWS 帳戶進行搜尋。
2. 選擇 Next (下一步)。

步驟 4：檢閱和建立

檢閱評估的資訊。如需變更步驟的資訊，請選擇編輯。完成後，選擇建立評估以啟動您的第一個評估，並開始持續收集證據。

建立評估之後，系統會繼續收集證據，直到您變更評估狀態為非作用中為止。或者，您可以變更控制項狀態為非作用中，來停止特定控制項收集證據。

> **Note**
>
> 建立評估的 24 小時後即可取得自動化證據。AWS Audit Manager 自動從多個資料來源收集證據，而該證據收集的頻率是根據證據類型而定。如需詳細資訊，請參閱本指南中的 證據收集頻率。

接下來做些什麼？

我們建議您繼續進一步了解本課程中介紹的概念和工具。請檢閱下列資源以繼續：

- 檢閱評估 — 向您介紹評估頁面，您可以在其中探索評估的不同組成部分。
- AWS Audit Manager 中的評估 — 以本教學課程為基礎，並提供有關管理評估的概念和工作的深入資訊。在本文件中，我們特別建議您查看下列主題：
  - 如何從不同架構建立評估
  - 如何檢閱評估中的證據並產生評估報告
  - 如何變更評估狀態或刪除評估
- 架構程式庫— 介紹架構程式庫，並說明如何按照自己特定的合規需求建立自訂架構。
- 控制項程式庫— 介紹控制項程式庫，並說明如何建立自訂控制項以在自訂架構中使用。
- AWS Audit Manager 概念和術語— 提供 Audit Manager 中使用的概念和術語的定義。
- [影片] 使用 AWS Audit Manager 收集證據並管理稽核資料 — 顯示本教學課程中所述的評估建立程序，以及其他工作，例如檢閱控制項和產生評估報告。

委派教學課程：檢閱控制集

本教學課程說明如何檢閱由 AWS Audit Manager 中的稽核擁有者與您共用的控制集。

稽核擁有者可使用 Audit Manager 來建立評估，並收集該評估中所列控制項的證據。有時，稽核擁有者在驗證控制集的證據時，可能會遇到問題或需要協助。在此情況下，稽核擁有者可以委派主題專家對控制集進行檢閱。

作為委派代表，您可以幫助稽核擁有者檢閱收集到的屬於您專業領域的控制項證據。

此教學課程會讓您了解如何執行以下操作：

- 存取稽核擁有者傳送給您的通知
- 檢閱控制集及其相關證據
- 上傳手動證據以協助控制項
- 為您正在檢閱的控制項新增評論
- 更新控制項的狀態
- 當您檢閱完成時，將檢閱的控制集提交給稽核擁有者

在您開始教學課程之前，請務必先達成以下條件：

- 您的 AWS 帳戶已設定完成。如需完成此教學課程，您必須同時使用 AWS 帳戶和 AWS Audit Manager 主控台。如需更多詳細資訊，請參閱 設定 AWS Audit Manager。
- 您對 Audit Manager 的術語和功能已經很熟悉了。如需 Audit Manager 的一般概觀，請參閱 什麼是 AWS Audit Manager？ 和 AWS Audit Manager 概念和術語。

步驟 1：存取您的通知

首先登入 AWS Audit Manager，您可以在其中存取通知，以查看已委派給您以供檢閱的控制集。

如需存取您的通知

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在左側導覽窗格中，選擇通知。或者，在頁面上方的藍色閃爍列中，選擇檢視通知來開啟通知頁面。
3. 在通知頁面上，檢閱已委派給您的控制集清單。通知表包含以下資訊：
   - 日期 — 委派控制集的日期。
   - 評估 — 與控制集相關的評估名稱。您可以選擇評估名稱，開啟評估詳細資料頁面。

- 控制集 — 已委派您進行檢閱的控制集名稱。
- 來源 — 委派控制集給您的使用者或角色。
- 說明 — 稽核擁有者提供的檢閱說明。

> **Tip**
>
> 您也可以訂閱 SNS 主題，以便在控制集指派給您以供檢閱時接收電子郵件警示。如需詳細資訊，請參閱 AWS Audit Manager 中的通知。

步驟 2：檢閱控制集及其相關證據

下一個步驟是檢閱稽核擁有者委派給您的控制集。透過檢查這些控制項及其證據，您可以確定是否需要對控制項採取任何其他動作。其他動作可能包括手動上傳其他證據以證明合規，或是留下有關該控制項的評論。

如需檢閱控制集

1. 在通知頁面上，檢閱委派給您的控制集清單。然後找出您要檢閱的評估，並選擇相關評估的名稱。
2. 在評估詳細資訊頁面的控制項索引標籤下，向下捲動至控制集表格。
3. 在依控制集分組的控制項欄位下，展開控制集名稱以顯示其控制項。然後，選擇控制項名稱以開啟控制項詳細資訊頁面。
4. (選擇性) 選擇更新控制項狀態以變更控制項的狀態。審核正在進行時，您可以將狀態標示為審核中。
5. 在證據資料夾、資料來源、評論和變更記錄索引標籤中，檢閱控制項的相關資訊。有關這些索引標籤以及如何解譯其中包含的資料的詳細資訊，請參閱檢閱評估中的控制項。

如需檢閱控制項的證據

1. 在控制項詳細資訊頁面中，選擇證據資料夾索引標籤。
2. 導覽至證據資料夾表，會顯示包含該控制項之證據的資料夾清單。這些資料夾是根據收集該資料夾內證據的日期來組織和命名的。
3. 選擇證據資料夾的名稱以將其開啟。從這裡，您可以檢閱該日期收集之所有證據的摘要。此摘要包括直接從 AWS Security Hub、AWS Config 或兩者報告的合規檢查問題總數。有關如何解譯此頁面上資料的說明，請參閱審核證據資料夾。

4. 從證據資料夾摘要頁面，瀏覽至證據表格。在時間欄位下方，選擇要開啟的明細項目，並檢閱當時收集的證據詳細資訊。有關如何解譯證據詳細資訊頁面上資料的說明，請參閱檢閱個別證據。

步驟 3. 上傳手動證據 (選擇性)

雖然 AWS Audit Manager 自動收集許多控制項的證據，但在某些情況下，您可能需要提供其他證據。在這些情況下，您可以手動上傳證據，以協助您證明是否符合該控制項。

您必須先將證據放在 S3 儲存貯體中，才能將手動證據上傳至評估。如需指示，請參閱 Amazon Simple Storage Service 使用者指南中的建立儲存貯體及上傳物件。

> **Important**
>
> 每個 AWS 賬戶每天最多只能手動上傳 100 個證據檔案至控制項。超過這個每日配額，會導致該控制項的任何額外手動上傳失敗。如果您需要將大量手動證據上傳至單一控制項，請在數天內分批上傳證據。

如需上傳手動證據至控制項

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在通知頁面上，您可以看到委派給您的控制集清單。識別您要新增證據的控制集，並選擇相關評估的名稱，以開啟評估詳細資訊頁面。
3. 選擇控制項索引標籤，向下捲動至控制集，然後選取控制項名稱加以開啟。
4. 選擇證據資料夾索引標籤，然後選擇上傳手動證據。
5. 在下一頁，輸入證據的 S3 URI。您可以瀏覽至 Amazon S3 主控台中的物件，然後選擇複製 S3 URI 以尋找 S3 URI。
6. 選擇上傳以上傳手動證據。

> **Note**
>
> 當控制項處於非作用中狀態時，您無法上傳該控制項的手動證據。如需上傳手動證據，您必須先將控制項狀態變更為審核中或已審核。如需如何變更控制項狀態的說明，請參閱 步驟 5：將控制項標示為已檢閱 (選擇性)。

步驟 4. 針對控制項新增評論 (選擇性)

您可以為審核的任何控制項新增評論。稽核擁有者可以看見這些評論。例如，您可以留下評論以提供狀態更新，並確認您已修正該控制項的任何問題。

若要將評論加入至控制項

1. 在通知頁面上，檢閱委派給您的控制集清單。尋找您要為其留下評論之控制集，然後選擇相關評估的名稱。
2. 選擇控制項索引標籤，向下捲動至控制集表格，然後選取控制項名稱加以開啟。
3. 選擇評論索引標籤。
4. 在傳送評論底下，在文字方塊中輸入您的評論。
5. 選擇送交評論以新增您的評論。然後，您的註解會顯示在頁面的先前評論章節下，還會顯示與此控制項相關的任何其他註解。

步驟 5：將控制項標示為已檢閱 (選擇性)

變更控制項狀態是選擇性的。不過，建議您在完成該控制項的審核時，將每個控制項的狀態變更為已審核。無論個別控制項的狀態為何，您仍然可以將控制項提交至稽核擁有者。

如需將控制項標記為已審核

1. 在通知頁面上，檢閱委派給您的控制集清單。尋找包含您要標示為已檢閱之控制項的控制集。然後，選擇相關評估的名稱以開啟評估詳細資料頁面。
2. 在評估詳細資訊頁面的控制項索引標籤下，向下捲動至控制集表格。
3. 在依控制集分組的控制項欄位下，展開控制集名稱以顯示其控制項。選擇控制項名稱以開啟控制項詳細資訊頁面。
4. 選擇更新控制項狀態，並將狀態變更為已審核。
5. 在出現的快顯視窗中，選擇更新控制項狀態，確認您已完成審核的控制項。

步驟 6. 將已檢閱的控制集提交至稽核擁有者

檢閱完所有控制項後，請將控制集提交回稽核擁有者，讓他們知道您已完成檢閱。

如需將已檢閱的控制集提交至擁有者

1. 在通知頁面上，檢閱指派給您的控制集清單。搜尋您要提交至稽核擁有者的控制集，然後選擇相關評估的名稱。
2. 向下捲動至控制集表格，選取要提交至稽核擁有者的控制集，然後選擇提交以供審閱。
3. 在出現的快顯視窗中，您可以先新增關於該控制集的任何高階評論，然後再選擇提交以供審核。

將控制項提交至稽核擁有者之後，他們可以檢視您為其留下的任何評論。

接下來做些什麼？

您可以繼續進一步了解本教學課程中介紹的概念。下列是一些建議的資源：

- 檢閱評估 — 向您介紹評估頁面，您可以在其中探索 AWS Audit Manager 評估的不同組成部分。
- 檢閱評估中的控制項並檢閱評估中的證據 - 提供資料定義以協助您解譯每個評估的控制項與證據。
- AWS Audit Manager 概念和術語 — 提供 Audit Manager 中使用的概念和術語的定義。

使用 Audit Manager 儀表板

使用 Audit Manager 儀表板，您可以在使用中的評估中以圖像顯示不合規的證據。這是一種方便快捷的方式，可以監控您的評估、隨時掌握資訊並主動修復問題。儀表板在預設設定下，會以由上而下彙總的方式，檢視提供所有使用中的評估。使用此檢視，您可以直觀地找出評估中的問題，而無需先篩選大量個別證據。

儀表板是您登入 Audit Manager 主控台時看到的第一個畫面。它包含兩個小工具，顯示與您最相關的資料和關鍵績效指標 (KPI)。使用評估篩選器，您可以調整此資料，以專注在特定評估的 KPI。您可以從該處檢閱控制項網域群組，以分辨哪些控制項具有最不合規的證據。然後，您可以探索基礎控制項，以檢查和修復問題。

> **Note**
>
> 如果您是第一次使用 Audit Manager，或者您沒有任何使用中的評估，則儀表板中不會顯示任何資料。若要開始使用，請建立評估。這將開始持續收集證據。24 小時後，彙總的證據資料將開始顯示在儀表板中。您可以閱讀以下各節，以了解如何理解和解釋此資料。

本頁面涵蓋下列主題：

主題

儀表板概念和術語

本節說明開始使用 Audit Manager 儀表板前需要瞭解的重要事項。

許可和可見性

稽核擁有者和代理人都可以存取儀表板。這表示這兩個角色都可以查看您AWS帳戶中所有使用中評估的指標和彙總。存取相同的資訊，可讓您的所有團隊專注在相同的 KPI 和目標。

篩選條件

Audit Manager 提供一個頁面層級 the section called “評估篩選器”，您可以將其套用至儀表板上的所有小工具。

不合規證據

儀表板會強調顯示評估中具有合規檢查證據和不合規結果的控制項。合規檢查證據與使用AWS Config或AWS Security Hub做為資料來源類型的控制項有關。針對此證據類型，Audit Manager 會直接從這些服務回報合規檢查的結果。如果安全中樞回報失敗結果，或者如果 AWS Config 報告不合規的結果，則 Audit Manager 會將證據歸類為不合規。

不確定證據

如果合規檢查無法使用或不適用，則證據為不確定。因此，無法進行合規評估。如果控制項使用 AWS Config 或 AWS Security Hub 做為資料來源類型，但您未啟用這些服務，就會發生這種情況。如果控制項使用不支援合規檢查的資料來源類型，例如手動證據、AWS API 呼叫或AWS CloudTrail。

如果在主控台裡，證據的合規檢查狀態為不適用，則在儀表板中將分類為不確定。

合規證據

如果合規檢查沒有回報任何問題，則證據將會是合規。如果安全中樞回報通過結果，或 AWS Config 回報合規結果，就會發生這種情況。

控制項網域

儀表板介紹控制項網域的概念。您可以將控制項網域視為控制項的一般類別，不特定於任何一個架構。控制項網域群組是儀表板最強大的功能之一。Audit Manager 會強調顯示評估中具有不合規證據的控制項，並依控制項網域進行分組。使用此功能，您可以在準備稽核時，將修復工作集中在特定主題網域上。

> **Note**
>
> 控制項網域與控制集不同。控制項集是一種特定於架構的控制項群組，通常由管理機構定義。例如，PCI DSS 架構有一個名為需求 8：識別和驗證對系統元件的存取的控制組。此控制集屬於身分與存取管理的控制項網域下。

Audit Manager 會將控制項分類在下列控制項網域下。

控制項網域名稱	這些控制項管理範圍的描述
業務連續性和應變計劃	建立程序以保護重要營運作業，不受重大系統和網路中斷影響程序的方法。
變更管理	測試、核准、實作及記錄雲端基礎架構變更的方式。
資料安全與隱私	您保護資料的隱私權、可用性和完整性的方法。
開發與組態管理	如何在所需且一致的狀態下維護雲端基礎架構。
控管和監督	讓雲端運算的使用符合法律、法規及道德義務的方法。
身分與存取管理	如何確保正確的使用者能適當存取您的技術資源。
事件管理	如何建立責任和程序，從而確保快速有效地應對安全事件。
記錄和監控	如何檢閱使用者活動，了解嘗試或執行未經授權活動的跡象。
網路管理	如何使用網路管理系統管理和操作資料網路。
人事管理	如何評估和管理組織層級的人員安全風險。
實體安全	如何偵測和預防設施中的實體安全問題。
風險管理	如何評估潛在風險和損失，以及如何減少或消除此類威脅。
供應鏈管理	如何分辨、評估和減輕與 IT 產品、供應商和供應鏈相關的風險。
使用者裝置管理	如何降低員工 IT 硬體遺失、損壞或受損的風險。
漏洞管理	如何定義、評估和修復雲端基礎架構中資產的所有已知漏洞。

資料的最終一致性

儀表板資料最終是一致的。這代表當您從儀表板讀取資料時，儀表板可能不會立即反映最近完成寫入或更新作業的結果。如果您在幾個小時內再次檢查，儀表板應該會反映最新的資料。

已刪除和非使用中評估的資料

儀表板會顯示使用中評估的資料。如果您在檢視儀表板的同一天刪除評估，或將其狀態變更為非使用中，則該評估的資料會如下所示。

- 非使用中評估 — 如果 Audit Manager 在您將評估變更為非使用中之前收集了評估的證據，則該證據資料會包含在儀表板當天的計數。
- 已刪除的評估 — 如果 Audit Manager 在您刪除之前收集了評估的證據，則該證據資料不會包含在儀表板當天的計數中。

儀表板元素

以下幾節涵蓋儀表板的不同元件。

主題

評估篩選器

您可以使用評估篩選器來專注於特定的使用中評估。

依預設，儀表板會顯示所有使用中評估的彙總資料。如果您要檢視特定評估的資料，請套用評估篩選器。這是適用於儀表板上所有小工具的頁面層級篩選器。

如需套用評估篩選器，請從儀表板頂端的下拉式清單中選取評估。此清單會顯示最多 10 項使用中的評估。最近建立的評估會先顯示出來。如果您有許多使用中的評估，您可以開始輸入評估名稱以快速找到評估。選取評估後，儀表板僅顯示該評估的資料。

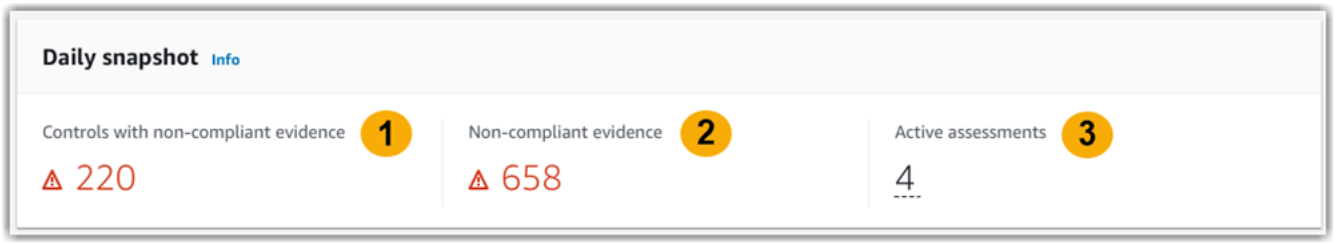
每日快照

這項小工具會顯示使用中評估目前合規性狀態的快照。

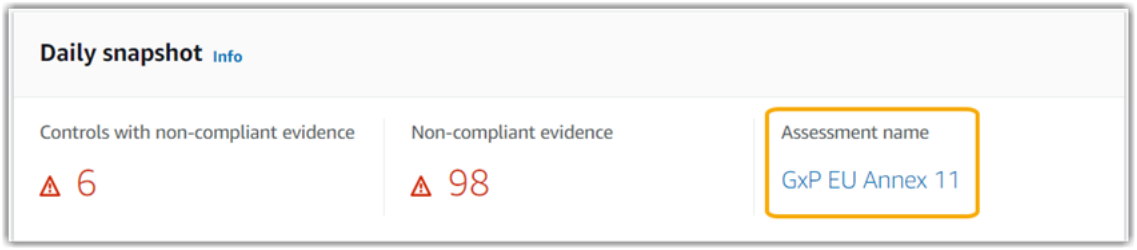
每日快照會顯示儀表板頂端當天收集的最新資料。使用國際標準時間 (UTC) 表示儀表板上的日期與時間。重要的是，這些資料是依據該時間點的每日統計。它們不是迄今為止的總和。

預設情況下，每日快照會顯示所有使用中評估的下列資料：

1. 具有不合規證據的控制項 - 與不合規證據相關聯的控制項總數。
2. 不合規證據 - 結論為不合規的合規檢查證據的總數。
3. 使用中評估 - 您使用中評估的總數。選擇此數字以查看這些評估的連結。



每日快照資料會根據您套用的the section called “評估篩選器”資料而變更。當您指定評估時，資料僅反映該評估的每日計數。在此情況下，每日快照會顯示您指定之評估的名稱。您可以選擇評估的名稱來開啟它。

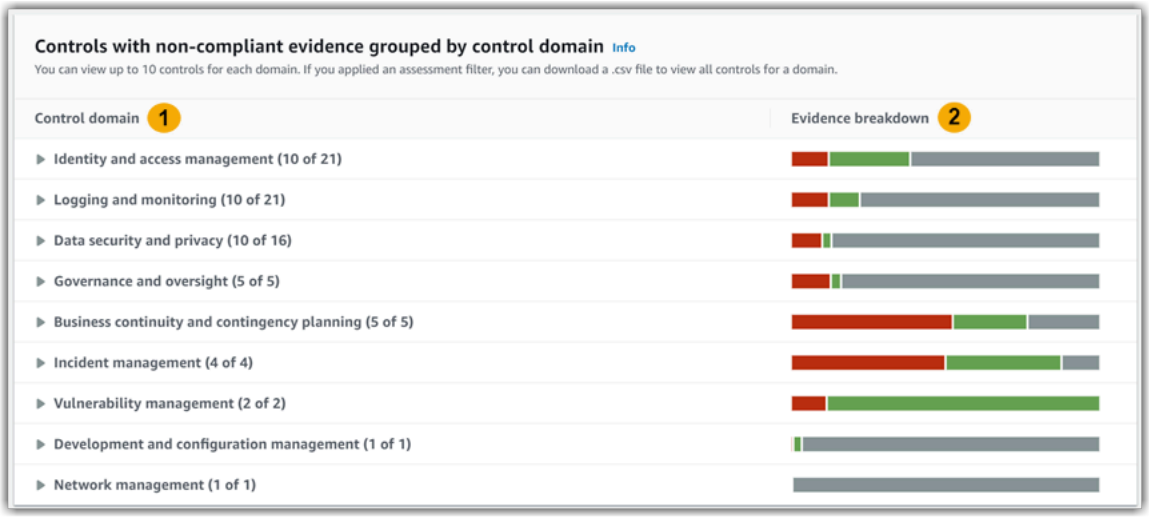


依控制項網域分組的具不合規證據的控制項

您可以使用此小工具來分辨哪些控制項具有最不相容的證據。

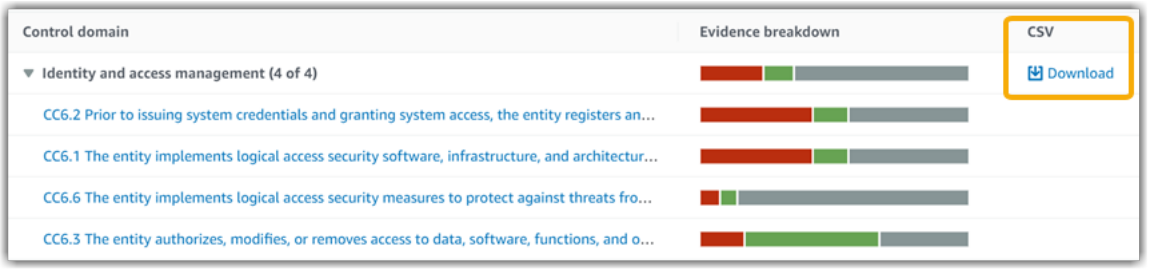
預設情況下，小工具會顯示您所有使用中評估的下列資料：

1. 控制項網域 — 與您的使用中評估相關的control domains清單。
2. 證據分類 — 顯示證據合規狀態分類的條形圖。



如需展開控制項網域，請選擇其名稱旁邊的箭頭。展開後，主控台最多會針對每個網域顯示 10 個控制項。這些控制項會根據不合規證據的最高總數來排名。

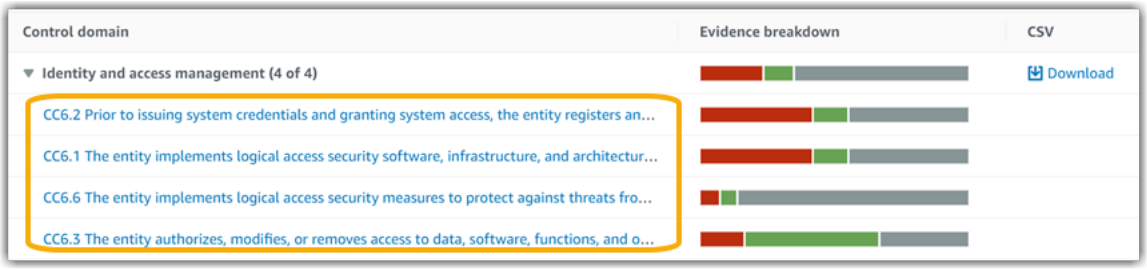
此小工具中的資料會根據您套用的the section called "評估篩選器"而變更。當您指定評估時，您只能看到該評估的資料。此外，您也可以為評估中的每個可用控制項網域下載 .csv 檔案。



.csv 檔案包含網域中與不合規證據相關聯的控制項完整清單。下列範例會顯示虛構化的 .csv 資料欄位。

	A	B	C	D	E	F	G
1	Date and Time	AssessmentID	AsessmentName	ControlId	ControlName	ControlDescription	DataSource
2	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	abcdefgh-1234-bcde-5678-cdefghijklmn	Control 1	Description of control 1	Manual
3	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	12345678-abcd-9012-bcde-345678901234	Control 2	Description of control 2	Manual
4	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	bcdefghi-2345-cdef-3456-defghijklmno	Control 3	Description of control 3	AWS Config, AWS Security Hub
5	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	23456789-bcde-0123-cdef-456789012345	Control 4	Description of control 4	Manual
6	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	cdefghij-3456-defg-4567-efghijklmnop	Control 5	Description of control 5	AWS Config
7	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	34567890-cdef-1234-defg-567890123456	Control 6	Description of control 6	Manual
8	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	defghijk-4567-efgh-5678-fghijklmnopq	Control 7	Description of control 7	AWS Config
9	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	45678901-defg-2345-efgh-678901234567	Control 8	Description of control 8	AWS Security Hub
10	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	efghijkl-5678-fghi-6789-ghijklmnopqr	Control 9	Description of control 9	Manual
11	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	56789012-efgh-3456-fghi-789012345678	Control 10	Description of control 10	Manual
12	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	fghijklm-6789-ghij-7890-hijklmnopqrs	Control 11	Description of control 11	Manual
13	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	67890123-fghi-4567-ghij-890123456789	Control 12	Description of control 12	Manual
14	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	ghijklmn-7890-hijk-8901-ijklmnopqrst	Control 13	Description of control 13	AWS Config, AWS Security Hub
15	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	78901234-ghij-5678-hijk-901234567890	Control 14	Description of control 14	Manual
16							

最後，當您套用評估篩選時，每個網域下的控制項名稱都將變為超連結。選擇任何控制項，以開啟指定評估中的控制項詳細資訊頁面。



Tip

使用控制項詳細資訊頁面做為起點，您可以從一個詳細資訊層級移至下一個層級。

1. 控制項詳細資訊頁面 - 在此頁面上，證據資料夾索引標籤會列出 Audit Manager 針對該控制項收集的每日證據資料夾。如需更多詳細資訊，請選擇一個資料夾。
2. 證據資料夾 - 接下來，您可以檢閱資料夾摘要和該資料夾中的證據清單。如需更多詳細資訊，請選擇個別證據項目。
3. 個人證據 - 最後，您可以瀏覽個人證據詳細資訊。這包括證據的任何適用屬性和資源資料。這是最細微層級的證據資料。

我接下來要怎麼做？

以下是您可以在查看儀表板後，所執行的一些後續步驟。

- 下載 .csv 檔案 — 尋找您要關注的評估和控制項網域，並下載含有不合規證據的相關控制項的完整清單。
- 檢閱控制項 — 分辨需要修正的控制項之後，您可以檢閱控制項。
- 委派控制項以供檢閱 — 如果您需要協助檢閱控制項，您可以委派控制集以供檢閱。
- 編輯您的評估 — 如果您想要變更使用中評估的範圍，您可以編輯評估。
- 更新評估狀態 — 如需停止收集評估證據，您可以將評估變更為非使用中。

疑難排解

若要尋找常見問題和問題的解答，請參閱本指南疑難排解章節中的疑難排解儀表板問題。

AWS Audit Manager 中的評估

Audit Manager 評估以架構為基礎，而架構是控制項群組。使用架構作為起點，您可以建立評估，以收集該架構中控制項的證據。在評估中，您也可以定義稽核範圍。這包括指定您要收集證據的 AWS 帳戶和服務。

您可以從任何架構建立評估。您可以使用 Audit Manager 提供的標準架構。或者，您可以透過自己構建的自訂架構建立評估。標準架構包含支援特定合規標準或法規的預建控制集。相較之下，自訂架構包含您可以根據內部稽核需求自訂和分組的控制項。如需了解有關標準與自訂架構之間差異的詳細資訊，請參閱本指南的概念與術語區段中的架構。

證據收集屬於持續過程，自您建立評估起開始。當需要進行稽核時，您或委派人員可以檢閱證據，然後將其新增至評估報告中。

> **Note**
>
> AWS Audit Manager 協助收集與驗證符合特定合規標準和法規相關的證據。不過，這不會評估您的合規狀態。因此，透過 AWS Audit Manager 收集的證據可能不包含稽核所需的所有關於您的 AWS 使用資訊。AWS Audit Manager 不是法律顧問或合規專家的替代方案。

主題

建立評估

本主題基於入門：建立評估教學課程。包含有關如何透過架構建立評估的詳細說明。請依照下列步驟建立評估，並開始持續收集證據。

任務

- 步驟 1：指定評估詳細資訊
- 步驟 2：指定範圍內 AWS 帳戶
- 步驟 3：指定範圍內 AWS 服務
- 步驟 4：指定稽核擁有者
- 步驟 4：檢閱和建立
- 我接下來要怎麼做？

步驟 1：指定評估詳細資訊

首先選擇一個架構並提供評估的基本資訊。

指定評估詳細資訊

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在導覽窗格中，選擇 評估，然後選擇建立評估。
   - 或者，在導覽窗格中，選擇入門，然後選擇建立評估。
3. 在評估名稱下，輸入評估的名稱。
4. (選擇性) 在評估說明下，輸入評估的说明。
5. 在評估報告目的地下，選擇您要儲存評估報告的 Amazon S3 儲存貯體。

   > **Tip**
   >
   > 預設評估報告目的地根據您的 Audit Manager 設定而定。如需詳細資訊，請參閱 AWS Audit Manager 設定、評估報告目的地。如果您願意，您可以建立和使用多個 S3 儲存貯體來協助您組織評估報告。

6. 在架構下方，選擇您建立評估需要依據的架構。您也可以使用搜尋列，依名稱、合規標準或法規來查詢架構。

> **Tip**
>
> 如需了解有關架構的更多資訊，請選擇架構名稱。這將開啟架構摘要頁面。在此頁面上，您可以檢閱該架構的內容。這包括架構的控制項和資料來源。

7. 在標籤下，選擇新增標籤，將標籤與評估產生關聯。您可以指定每一個標籤的金鑰和值。標籤索引鍵是必要的，在搜尋此評估時，可用作搜尋條件。如需有關 Audit Manager 中標籤的詳細資訊，請參閱 標記 AWS Audit Manager 資源。
8. 選擇下一步。

> **Note**
>
> 請務必確保您的評估會針對特定架構收集正確的證據。在您開始收集證據之前，建議您先檢閱所選架構的需求。然後，根據您目前的AWS Config規則參數驗證這些需求。如需確保規則參數符合架構需求，您可以在 AWS Config 中更新規則。
> 例如，假設您正在為 CIS v1.2.0 建立評估。此架構包含一個名為 1.9 — 確保 IAM 密碼政策的長度至少需要 14 或更高的控制項。在 AWS Config 中，iam-password-policy 規則具有一個 `MinimumPasswordLength` 參數，用於檢查密碼長度。此參數的預設值為 14 字元。因此，該規則符合控制項的需求。如果您沒有使用預設參數值，請確保您使用的值等於或大於 CIS v1.2.0 的 14 個字元要求。您可以在 AWS Config 文件中找到每個受管規則的預設參數詳細資訊。

步驟 2：指定範圍內 AWS 帳戶

您可以指定多個 AWS 帳戶 包含在評估範圍內。Audit Manager 透過與 AWS Organizations 整合來支援多個帳戶。這表示 Audit Manager 評估可以在多個帳戶上執行，並將收集的證據合併到委派管理員帳戶中。如需在 Audit Manager 中啟用 Organizations，請參閱 啟用 AWS Organizations (選擇性)。

> **Note**
>
> Audit Manager 可以支援單一評估範圍內最多 150 個成員帳戶。如果您嘗試涵蓋超過 150 個帳戶，則評估建立可能會失敗。

如需指定範圍內 AWS 帳戶

1. 在 AWS 帳戶 下方，選擇您希望包含在評估範圍內的 AWS 帳戶。
   - 如果您在 Audit Manager 中啟用了 Organizations，則會顯示多個帳戶。您可以從清單中選擇一或多個帳戶。或者，您也可以使用帳戶名稱、ID 或電子郵件搜尋帳戶。
   - 如果您未在 Audit Manager 中啟用 Organizations，則只會列出您目前 AWS 帳戶。
2. 選擇 Next (下一步)。

> **Note**
>
> 當範圍內的帳戶從組織中移除時，Audit Manager 不會再為該帳戶收集證據。但是，該帳戶仍會繼續顯示在您的評估中的AWS 帳戶 索引標籤下。如需從範圍內帳號清單中移除帳戶，您可以編輯評估。已移除帳戶在編輯期間不再顯示於清單中，您可以在不包含該帳戶的範圍內儲存您的變更。

步驟 3：指定範圍內 AWS 服務

您先前選擇的架構會定義 Audit Manager 監視及收集證據的 AWS 服務。如果未選擇已列出的 AWS 服務，或雖已選擇，但您未在環境中啟用，則 Audit Manager 不會從與該服務相關的資源收集證據。

您可以指定範圍內 AWS 服務，如下所示。

針對透過標準架構建立的評估

當您使用 Audit Manager 主控台從標準架構建立評估時，範圍內的 AWS 服務 清單會被預設為選取狀態。無法編輯此清單。這是因為 Audit Manager 會自動為您映射並選擇資料來源和服務。此選擇是根據標準架構的要求所進行。如果您選取的標準架構只包含手動控制項，則您的評估範圍內不會包含任何 AWS 服務，並且您無法在評估中新增任何服務。

檢閱清單並選擇下一步以繼續。

> **Tip**
>
> 如果您需要編輯範圍中的服務清單，您可以使用 Audit Manager 提供的 CreateAssessment API 來執行此操作。
> 或者，您可以自訂標準架構，然後從自訂架構中建立評估。

針對透過自訂架構建立的評估

如果您在步驟 1 中選擇了自訂架構，則可以檢閱和修改評估範圍內 AWS 服務 的清單。如果您選擇的自訂架構僅包含手動控制項，則會顯示所有 AWS 服務，但不會選擇任何項目。您可以選擇零個或多個服務包含在評估範圍內。

如需指定範圍內 AWS 服務 (僅適用於透過自訂架構建立的評估)

1. 在 AWS 服務 下方，選擇您希望包含在評估範圍內的服務。您可以使用搜尋列按服務、類別或描述搜尋其他服務。如需新增服務，請勾選服務名稱旁的核取方塊。如需移除服務，請清除核取方塊。
2. 選擇 AWS 服務 後，選擇下一步。

步驟 4：指定稽核擁有者

在此步驟中，您可以指定評估的稽核擁有者。稽核擁有者是工作場所中負責管理稽核管理員評估的個人，通常來自 GRC、SecOps 或 DevOps 團隊。我們建議他們使用 AWSAuditManagerAdministratorAccess 政策。

如需指定稽核擁有者

1. 在稽核擁有者下，檢閱目前的稽核擁有者清單。稽核擁有者一欄會顯示使用者 ID 和角色。此 AWS 帳戶 欄會顯示該稽核擁有者的關聯 AWS 帳戶。
2. 核取方塊已選擇的稽核擁有者會包含在您的評估中。清除任何稽核擁有者的核取方塊，即可將其從評估中移除。您可以使用搜尋列，按名稱或 AWS 帳戶 搜尋尋找其他稽核擁有者。
3. 完成時，選擇下一步。

步驟 4：檢閱和建立

檢閱評估的資訊。如需變更步驟的資訊，請選擇編輯。完成後，請選擇 建立評估。

該動作意味著評估證據持續收集過程的開始。建立評估之後，系統會繼續收集證據，直到您變更評估狀態為非作用中為止。或者，您可以變更控制項狀態為非作用中，來停止特定控制項收集證據。

> **Note**
>
> 建立評估 24 小時後，即可使用自動化證據。Audit Manager 會自動從多個資料來源收集證據，而證據收集的頻率根據證據類型而定。如需進一步了解，請參閱本指南中的 證據收集頻率。

我接下來要怎麼做？

建立評估後，您可以進一步了解以下資訊：

- 存取評估
- 檢閱評估
- 編輯評估
- 檢閱評估中的控制項
- 檢閱評估中的證據
- 將手動證據上傳至評估
- 在 AWS Audit Manager 中委派
- 產生評估報告
- 變更評估狀態
- 刪除評估
- 疑難排解評估和證據收集問題

存取 AWS Audit Manager 中您的評估

您可以在 Audit Manager 主控台的評估頁面上檢視所有評估。您也可以在此編輯評估、刪除評估或建立評估。

您也可以使用 Audit Manager API 或 AWS Command Line Interface (AWS CLI) 來檢視您的評估。

Audit Manager console

如需檢視您的評估 (主控台)

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在左側導覽窗格中，選擇評估查看作用中和已發生評估的清單。您也可以使用搜尋列來搜尋評估。
3. 選擇任何評估名稱以開啟摘要頁面，您可以在其中檢視該評估的詳細資訊。

AWS CLI

如需檢視您的評估 (CLI)

如需在 Audit Manager 中檢視評估，請執行list-assessments命令。您可以使用 `--status` 子指令來檢視作用中或非作用中的評量。

```
aws auditmanager list-assessments --status ACTIVE
```

```
aws auditmanager list-assessments --status INACTIVE
```

Audit Manager API

如需檢視您的評估 (API)

如需在 Audit Manager 中檢視評估，請執行ListAssessments操作。您可以使用 status 屬性來檢視作用中或非作用中的評估。

有關詳細資訊，請選擇先前的任一連結，在 AWS Audit Manager API 參考資料中閱讀更多資訊。這包括有關如何在其中一項特定語言 AWS 軟體開發套件中使用 `ListAssessments` 操作和參數的資訊。

編輯評估

您可以在 Audit Manager 中編輯作用中評估，變更描述、範圍、稽核擁有者和評估報告目的地等資訊。

任務

- 步驟 1：編輯評估詳細資訊
- 步驟 2：編輯範圍內 AWS 帳戶
- 步驟 3：編輯範圍內 AWS 服務
- 步驟 4：編輯稽核擁有者
- 步驟 5：檢閱和保存

步驟 1：編輯評估詳細資訊

請依照下列步驟編輯評估的詳細資訊。

如需編輯評估

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在導覽窗格中，選擇評估以檢視您目前的評估清單。
3. 選擇評估，然後選擇編輯。
   - 或者，您可以開啟評估，然後選擇頁面右上角的編輯。
4. 在編輯評估詳細資訊下，編輯您的評估名稱、描述和評估報告目的地。
5. 選擇 Next (下一步)。

> **Tip**
>
> 如需編輯評估的標籤，請開啟評估並選擇 標籤索引標籤。您可以在此檢視和編輯與評估相關聯的標籤。

步驟 2：編輯範圍內 AWS 帳戶

在此步驟中，您可以變更評估範圍內包含於評估範圍內的帳戶清單。

Audit Manager 透過與 AWS Organizations 整合來支援多個帳戶。這表示 Audit Manager 評估可以在多個帳戶上執行，並將收集的證據合併到委派管理員帳戶中。如需在啟用 Audit Manager 之後新增或變更委派管理員，請參閱AWS Audit Manager 設定，委派管理員。

> **Note**
>
> Audit Manager 可以支援單一評估範圍內最多 150 個成員帳戶。如果您嘗試涵蓋超過 150 個帳戶，則評估建立可能會失敗。

如需編輯範圍內 AWS 帳戶

1. 在編輯範圍內 AWS 帳戶 下，選擇其他 AWS 帳戶。您也可以從清單中清除帳戶來移除帳戶。
2. 選擇 Next (下一步)。

步驟 3：編輯範圍內 AWS 服務

此步驟指定 Audit Manager 監視和收集證據的 AWS 服務。如果未選擇已列出的 AWS 服務，或雖已選擇，但您未在環境中啟用，則 Audit Manager 不會從與該服務相關的資源收集證據。

您可以檢閱和編輯範圍內 AWS 服務，如下所示。

針對透過標準架構建立的評估

當您使用 Audit Manager 主控台編輯透過標準架構建立的評估時，您可以檢閱範圍內 AWS 服務 的清單，但無法編輯此清單。這是因為 Audit Manager 會根據標準架構的設計，自動為您映射並選擇資料來源和服務。如果評估使用僅包含手動控制項的架構建立，AWS 服務 不會包含在您的評估範圍內，且您無法添加任何服務。

檢閱清單並選擇下一步以繼續。

> **Tip**
>
> 如果您需要針對現有評估編輯範圍內服務清單，您可以使用 Audit Manager 提供的 UpdateAssessment API 來執行此操作。

針對透過自訂架構建立的評估

如果您是透過自訂架構建立評估，則可以編輯評估範圍內的 AWS 服務。您可以選擇零個或多個服務包含在評估範圍內。

如需編輯範圍內 AWS 服務 (僅適用於透過自訂架構建立的評估)

1. 在編輯範圍內 AWS 服務 下，選擇其他 AWS 服務 (如必要)。您也可以透過從清單中清除來移除服務。
2. 選擇 Next (下一步)。

步驟 4：編輯稽核擁有者

您也可以變更評估的稽核擁有者。稽核擁有者是工作場所中負責管理稽核管理員評估的個人，通常來自 GRC、SecOps 或 DevOps 團隊。他們的職責包括委派控制集以進行檢閱以及產生評估報告。建議您使用 AWSAuditManagerAdministratorAccess政策。

如需編輯稽核擁有者

1. 選擇要新增至評估的稽核擁有者。如需移除稽核擁有者，則將其從清單中清除。
2. 選擇 Next (下一步)。

步驟 5：檢閱和保存

檢閱評估的資訊。如需變更步驟的資訊，請選擇編輯。完成後，請選擇儲存變更確認您的編輯。

> **Note**
>
> 完成編輯後，對評估的變更將在次日 00:00 UTC 生效。

檢閱評估

在 Audit Manager 中建立評估之後，您可以隨時開啟並檢閱您的評估。

如需開啟和檢閱評估

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在左側導覽窗格中，選擇評估查看評估清單。
3. 選擇評估名稱來開啟評估。

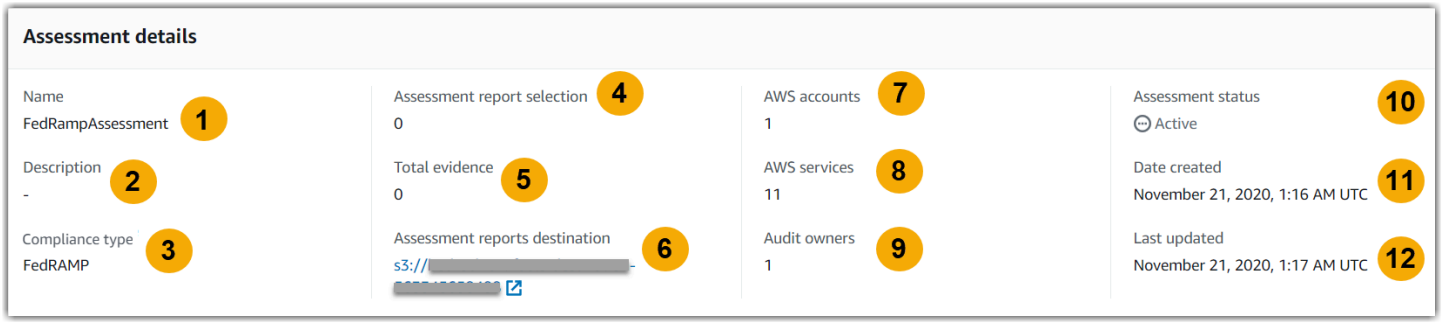
開啟評估時，您會看到包含數個區段的摘要頁面。本頁面的各個章節及其內容說明如下。

評估頁面的區段

- 評估詳細資訊
- 控制項索引標籤
- 評估報告選擇索引標籤
- AWS 帳戶 索引標籤
- AWS 服務 索引標籤
- 稽核擁有者索引標籤
- 標籤索引標籤
- Changelog 索引標籤

評估詳細資訊

評估詳細資訊」區段提供評估的概觀。



其包含下列資訊：

1. 名稱 — 您為評估提供的名稱。
2. 描述 — 您為評估提供的選用描述。
3. 合規類型 — 評估支援的合規標準或法規。
4. 評估報告選擇 — 您選擇包含在評估報告內的證據項目數量。
5. 證據總數 — 為此評估收集的證據項目總數。
6. 評估報告目的地 — Audit Manager 儲存評估報告的 Amazon S3 儲存貯體。
7. AWS 帳戶 — 評估範圍內的 AWS 帳戶 數量。
8. AWS 服務 — 評估範圍內的 AWS 服務 數量。
9. 稽核擁有者 — 評估的稽核擁有者數量。
10. 評估狀態 — 評估的狀態。
    - 作用中 — 表示評估目前正在收集證據。新建立的評估具有此狀態。
    - 非作用中 — 表示評估目前不再收集證據。如需非作用中評估的詳細資訊，請參閱 [將評估狀態變更為非作用中](#)。
11. 建立日期 — 建立評估的日期。
12. 上次更新 — 上次編輯評估的日期。

控制項索引標籤

控制項索引標籤會顯示評估中控制項的摘要，以及這些控制項的完整清單。每個評估可以包含多個控制集，而每個控制集包含多個控制項。控制項與控制集已進行組織，以與關聯的合規標準或法規中定義的配置相符。

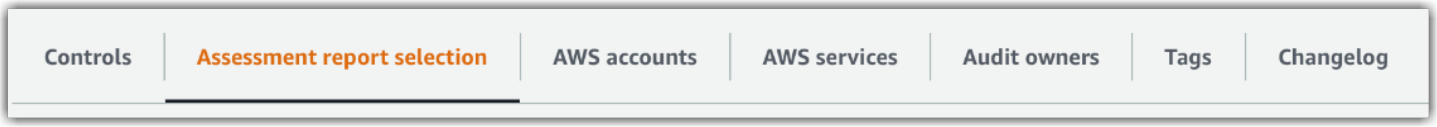
在控制項狀態摘要下，您可以檢閱評估的控制項摘要。此摘要包含以下資訊：

- 控制項總數 — 此評估中的控制項總數。
- 已檢閱 — 由稽核擁有者或委派人員檢閱的控制項數量。
- 審核中 — 目前正在審核的控制項數量。
- 非作用中 — 不再主動收集證據的控制項數量。

控制項清單顯示在控制集表格下，並依控制集分組。您可以展開或折疊每個控制集中的控制項。如果您想要尋找特定的控制項，也可以依控制項名稱進行搜尋。下列資料欄會顯示在依控制集分組的控制項表格中：

- 依控制集分組的控制項 — 控制集的名稱。
- 控制項狀態 — 控制項的狀態。
  - 審核中表示此控制項未審核完成。此控制項仍在收集證據，且您可以上傳手動證據。這是預設狀態。
  - 已檢閱表示已檢閱此控制項的證據。但是，仍在收集證據，且您可以上傳手動證據。
  - 非作用中表示已停止此控制項的自動證據收集。您無法再上傳手動證據。
- 委派人員 — 經委派檢閱此控制項的檢閱者。
- 證據總數 — 已為此控制項收集的證據項目總數。

評估報告選擇索引標籤



此索引標籤會顯示要包含在評估報告中的證據 (依證據資料夾分組) 清單。這些證據資料夾根據建立日期來組織和命名。您可以瀏覽這些資料夾，並選擇要包含在評估報告中的證據。您也可以使用搜尋列，依證據資料夾名稱或控制項名稱進行搜尋。新增至評估報告的證據項目總數會在頁面頂端的評估詳細資訊區段下彙總。

評估報告選擇表格會顯示包含下列資料的證據資料夾清單：

- 證據資料夾 — 證據資料夾的名稱。資料夾根據收集證據的日期來命名。
- 選擇的證據 — 包含在評估報告資料夾中的證據項目數量。
- 控制項名稱 — 與此證據資料夾相關聯的控制項名稱。

如需將證據新增至評估報告的相關資訊，請參閱 產生評估報告。

AWS 帳戶 索引標籤

此索引標籤會顯示評估範圍內 AWS 帳戶 的清單。帳戶總數摘要在頁面頂端的評估詳細資訊區段下。

此 AWS 帳戶 表格顯示具有下列資料的帳戶清單：

- 帳戶 ID — AWS 帳戶 的 ID。
- 帳戶名稱 — AWS 帳戶 的名稱。
- 電子郵件 — 與 AWS 帳戶 相關聯的電子郵件地址。

AWS 服務 索引標籤

此索引標籤會顯示評估範圍內 AWS 服務 的清單。換句話說，這些是您的評估所收集證據涉及的 AWS 服務。

服務總數摘要在頁面頂端的評估詳細資訊區段下。

此 AWS 服務 表格顯示具有下列服務的帳戶清單：

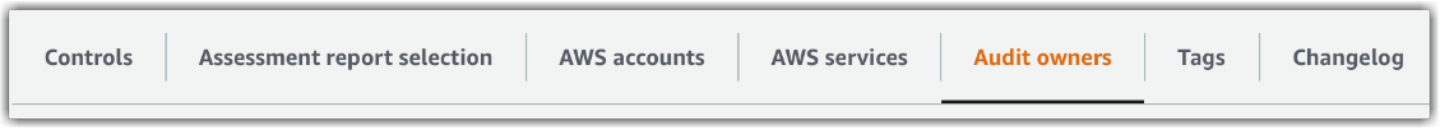
- AWS 服務 — AWS 服務 的名稱。
- 類別 — 服務類別，例如計算或資料庫。

Audit Manager 會針對此表格中的服務執行資源評估。例如，如果列出了 Amazon S3，則 Audit Manager 可以收集有關 S3 儲存貯體的證據。控制項的資料來源決定收集什麼證據。例如，如果資

料來源類型為 AWS Config，而資料來源映射項目是 AWS Config 規則 (例如 `s3-bucket-public-write-prohibited`)，則 Audit Manager 會收集該規則評估的結果作為證據。如需詳細資訊，請參閱本指南中範圍內的服務和資料來源類型有何差異？。

> **Note**
>
> 如果您的評估透過標準架構在主控台中建立的，Audit Manager 會為您選擇服務，並根據架構的需求映射其資料來源。由於此標準架構僅包含手動控制項，則 AWS 服務 均不包含在範圍內。如果您需要編輯範圍中的服務清單，可以使用 UpdateAssessment API。

稽核擁有者索引標籤

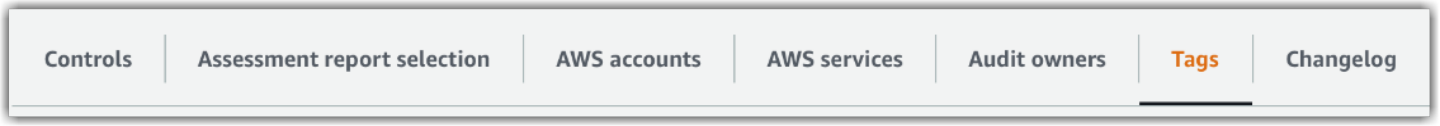


此標籤顯示評估的稽核擁有者。稽核擁有者總數也彙總在頁面頂端的評估詳細資訊區段下。

此稽核擁有者表格顯示具有下列資料的帳戶清單：

- 稽核擁有者 — 稽核擁有者的姓名。
- AWS 帳戶 — 與稽核擁有者相關聯的電子郵件地址。

標籤索引標籤



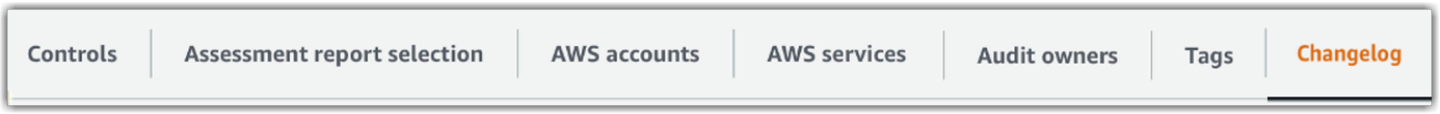
此標籤會顯示透過架構繼承的標籤清單，用來建立此評估。標籤總數彙總在頁面頂端的評估詳細資訊區段下。

此標籤表格顯示具有下列資料的標籤清單：

- 金鑰 — 標籤金鑰 (例如合規標準、法規或類別)。
- 值 — 標籤的值。

如需有關 Audit Manager 中標籤的詳細資訊，請參閱 標記 AWS Audit Manager 資源。

Changelog 索引標籤



此標籤顯示與評估相關的使用者活動清單。

此 Changelog 表格顯示具有下列資料的帳戶清單：

- 日期 — 活動的日期。
- 使用者 — 執行操作的使用者。
- 動作 — 已發生的動作，例如建立評估。
- 類型 — 已變更的物件類型，例如評估。
- 資源 — 受變更影響的資源，例如建立評估的來源架構。

檢閱評估中的控制項

Audit Manager 中的控制項可協助您在稽核中同時符合常見和特殊的合規標準與法規。您可以隨時開啟並檢閱 Audit Manager 評估中的控制項。

如需開啟控制項摘要頁面

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在導覽窗格中，選擇評估，然後選擇評估的名稱來將其開啟。
3. 在評估頁面上，選擇控制項索引標籤，向下捲動至控制集表格，然後選擇控制項名稱來開啟。

開啟控制項時，您會看到包含數個區段的摘要頁面。本頁面的各個區段及其內容描述如下。

控制項頁面的區段

- 控制項詳細資訊
- 更新控制項狀態
- 證據資料夾索引標籤
- 資料來源索引標籤
- 評論索引標籤

- Changelog 索引標籤

控制項詳細資訊

控制項詳細資訊區段會提供控制項的概觀。

其包含下列資訊：

1. 控制項名稱 — 指定給此控制項的名稱。
2. 控制項描述 — 此控制項的描述。
3. 測試資訊 — 此控制項的建議測試程序。
4. 行動計畫 — 在控制項未完成情況下，建議執行的動作。

更新控制項狀態

在更新控制項狀態區段中，您可以審核和更新評估控制項的狀態。

可使用的狀態如下：

- 審核中 — 表示此控制項未審核完成。此控制項仍在收集證據，且您可以上傳手動證據。這是預設狀態。
- 已檢閱 — 表示已檢閱此控制項的證據。仍在收集證據，且您可以上傳手動證據。
- 非作用中 — 表示已停止此控制項的自動化證據收集。您無法再上傳手動證據。

> **Note**
>
> 將控制項狀態變更為已檢閱該操作不可變更。將控制項的狀態設定為已檢閱之後，就無法再變更該控制項的狀態或還原為先前的狀態。

證據資料夾索引標籤

證據資料夾索引標籤會列出針對此控制項自動收集的證據。每天都會組織成資料夾。

證據資料夾表格會顯示包含下列資料的資料夾清單：

- 證據資料夾 — 證據資料夾的名稱。根據收集或手動添加證據的日期來命名。

- 合規檢查 — 在證據資料夾中發現的問題數量。該數量代表直接從 AWS Security Hub、AWS Config 或兩者報告的安全性問題總數。如果您看到不適用，表示 AWS Security Hub 或 AWS Config 均未啟用，或證據來自不同的資料來源類型。
- 證據總數 — 資料夾內的證據項目總數。
- 評估報告選擇 — 包含在評估報告內的資料夾證據項目數量。

透過證據資料夾索引標籤，您可以執行下列動作：

- 檢閱各項證據 — 選擇證據資料夾將其開啟。然後，您可以在證據資料夾摘要頁面中選擇要檢閱的各項證據。
- 添加手動證據 — 如需詳細資訊，請參閱 在 AWS Audit Manager 中添加手動證據。
- 將證據新增至評估報告 — 如需詳細資訊，請參閱 產生評估報告。

資料來源索引標籤

此索引標籤會顯示控制項之資料來源的相關資訊。其包含下列資訊：

- 資料來源名稱 — 這僅適用於自訂控制項。它指的是您為每個資料來源提供的描述性名稱。您可以使用此名稱，從多個資料來源中篩選出具備相同類型的資料來源。
- 資料來源類型 — 指定證據資料的來源。
  - 如果 Audit Manager 收集證據，則資料來源可以是下列四種類型之一：AWS Security HubAWS ConfigAWS CloudTrail、、或 AWSAPI 呼叫。
  - 如果您上傳自己的證據，則資料來源類型為手動。說明會指出所需的手動證據是檔案上傳還是文字回應。
- 映射-這是用於識別並檢索自動化資料來源資料的映射屬性。
  - 如果資料來源類型為 AWS Config，則映射項目為特定 AWS Config 規則的名稱 (例如 `EC2_INSTANCE_MANAGED_BY_SSM`)。Audit Manager 會使用此映射項目，直接回報來自 AWS Config 規則檢查的結果。
  - 如果資料來源類型為 AWS Security Hub，則映射項目為特定 Security Hub 控制項的名稱 (例如 `1.1 – Avoid the use of the "root" account`)。Audit Manager 使用此映射項目直接從 Security Hub 報告該安全檢查的結果。
  - 如果資料來源類型為 AWS API 呼叫，則映射項目為特定 API 呼叫的名稱 (例如 `ec2_DescribeSecurityGroups`)。Audit Manager 會使用此映射項目來收集 API 回應。

- 如果資料來源類型為 AWS CloudTrail，則映射項目為特定 CloudTrail 事件的名稱 (例如 `CreateAccessKey`)。Audit Manager 會使用此映射項目，從 CloudTrail 日誌中收集相關的使用者活動。
- 頻率 — 從此資料來源收集證據的頻率。頻率因資料來源而異。如需詳細資訊，請在欄中選擇值，或參閱 證據收集頻率。

評論索引標籤

在評論索引標籤中，您可以新增有關控制項及其證據的評論。它也會顯示既往評論的清單。

在發送評論下，您可以輸入文字，然後選擇提交評論，為控制項新增評論。

在既往評論下，您可以檢視既往評論的清單，以及評論的發佈日期和關聯的使用者 ID。

Changelog 索引標籤

Changelog 索引標籤會顯示與控制項相關的使用者活動清單。AWS CloudTrail 中的稽核記錄日誌也提供了相同的資訊。透過直接在 Audit Manager 中擷取的使用者活動，您可以輕鬆檢閱指定控制項的稽核記錄活動。

在 Changelog 下，表格會顯示下列資料欄：

- 日期 — 活動的日期和時間，以國際標準時間 (UTC) 表示。
- 使用者 — 執行活動的使用者或角色。
- 動作— 對活動的描述。
- 類型 — 進一步描述活動的關聯屬性。
- 資源 — 相關資源 (如適用)。

Audit Manager 會透過 changelog 追蹤下列使用者活動：

- 建立評估
- 編輯評估
- 完成評估
- 刪除評估
- 委派需要檢閱的控制集
- 將已檢閱的控制集送交回稽核擁有者

- 上傳手動證據
- 更新控制項狀態
- 產生評估報告

檢閱評估中的證據

Audit Manager 中的作用中評估自動收集來自各類資料來源的證據。如需更多詳細資訊，請參閱 AWS Audit Manager 如何收集證據。您可以隨時開啟並檢閱針對評估中控制項收集的證據。

如需開啟針對控制項收集的證據

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在導覽窗格中，選擇評估，然後選擇評估的名稱來將其開啟。
3. 在評估頁面上，選擇控制項索引標籤，向下捲動至控制項表格，然後選擇控制項名稱來開啟。
4. 在控制項詳細資訊頁上，選擇證據資料夾索引標籤。針對該控制項收集證據的所有資料夾清單會顯示在證據資料夾表格下。這些資料夾根據資料夾內證據的收集日期來組織和命名。
5. 選擇證據資料夾的名稱以將其開啟。

您現在可以從這裡檢閱針對該控制項收集證據的資料夾，並視需要深入探索，進一步檢閱各項證據。

主題

- 檢閱證據資料夾
- 檢閱各項證據

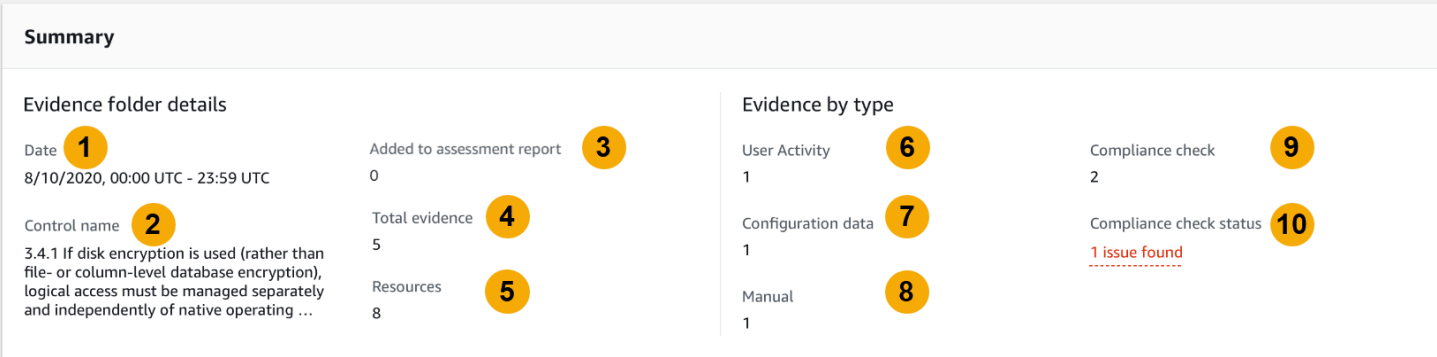
檢閱證據資料夾

當您開啟證據資料夾時，您會看到證據資料夾摘要頁面，其中包含兩個區段：摘要區段和證據表格。各個區段及其內容描述如下。

- 證據資料夾摘要
- 證據表

證據資料夾摘要

頁面的摘要區段提供證據資料夾中證據的高階概觀。



其包含下列資訊：

1. 日期 — 建立證據資料夾的時間和日期，以國際標準時間 (UTC) 表示。
2. 控制項名稱 — 與此證據資料夾相關聯的控制項名稱。
3. 添加至評估報告 — 手動選擇包含在評估報告內的證據項目數量。
4. 證據總數 — 證據資料夾內的證據項目總數。
5. 資源 — 在產生資料夾內證據時，已評估的 AWS 資源總數。
6. 使用者活動 — 屬於使用者活動類別的證據項目數量。此證據收集自 AWS CloudTrail 日誌。
7. 組態資料 — 屬於組態資料類別的證據項目數量。此證據收集自 Amazon EC2、Amazon S3 或 IAM 等其他 AWS 服務 的組態快照。
8. 手動 — 屬於手動類別的證據項目數量。此證據是手動上傳的。
9. 合規檢查 — 屬於合規檢查類別的證據項目數量。此證據收集自 AWS Config 或 AWS Security Hub。
10. 合規檢查狀態 — 直接從 AWS Security Hub、AWS Config 或兩者報告的合規檢查問題總數。

> **Tip**
>
> 如需有關不同證據類型 (使用者活動、組態資料、合規檢查和手冊) 的詳細資訊，請參閱證據。

證據表

證據表會列出證據資料夾中包含的各項證據。

其包含下列資訊：

1. 時間 — 表示收集證據的時間，也用作證據的名稱。時間以國際標準時間 (UTC) 表示。從此欄選擇時間會開啟證據詳細資訊頁。本頁面在下一區段中進行描述。
2. 類型證據 — 證據的類別
   - 合規檢查證據收集自 AWS Config 或 AWS Security Hub。
   - 使用者活動證據收集自 AWS CloudTrail 日誌。
   - 組態資料證據收集自 Amazon EC2、Amazon S3 或 IAM 等其他服務的組態快照。
   - 手動證據是您手動上傳的證據。
3. 合規檢查 — 屬於合規檢查類別之證據的評估狀態。
   - 對於收集自 AWS Security Hub 的證據，會直接從 AWS Security Hub 中報告通過或失敗結果。
   - 對於收集自 AWS Config 的證據，會直接從 AWS Config 中報告合規或不合規結果。
   - 如果顯示不適用，表示 AWS Security Hub 或 AWS Config 均未啟用，或證據來自不同的資料來源類型。
4. 資料來源 — 從中收集證據的資料來源。
5. 事件名稱 — 證據所涉及事件的名稱。
6. 資源 — 為產生證據而評估的資源數量。
7. 評估報告選擇 — 表示證據是否經手動選擇包含在評估報告中。
   - 如需包含證據，請選擇證據，然後選擇新增至評估報告。
   - 如需排除證據，請選擇證據，然後選擇從評估報告中移除。

如需將手動證據上傳至證據資料夾，請選擇上傳手動證據，輸入證據的 S3 URI，然後選擇上傳。如需詳細資訊，請參閱在 AWS Audit Manager 中上傳手動證據。

如需查看任一項證據的詳細資訊，請在時間欄下選擇超連結的證據名稱。這會開啟證據詳細資訊頁面，如以下區段所述。

檢閱各項證據

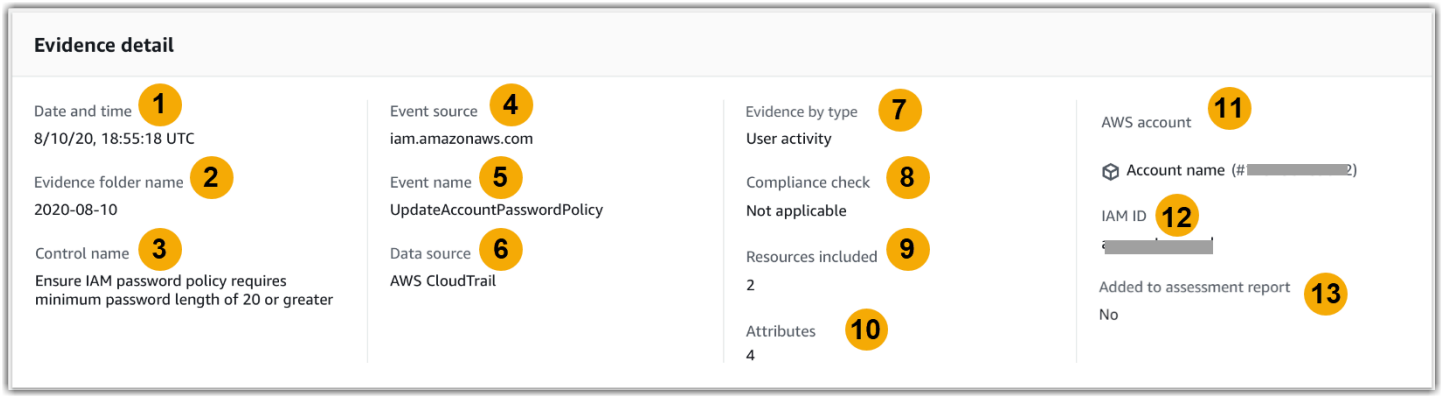
當您開啟各項證據時，您會看到一個證據詳細資訊頁面，其中包含三個區段：證據詳細資訊區段、屬性表以及包含的資源表格。各個區段及其內容描述如下。

- 証据詳細資訊
- Attributes

- 包含的資源

證據詳細資訊

頁面的證據詳細資訊區段會顯示證據的概觀。



其包含下列資訊：

1. 日期和時間 — 收集證據的時間和日期，以國際標準時間 (UTC) 表示。
2. 證據資料夾名稱 — 包含證據的證據資料夾名稱。
3. 控制項名稱 — 與此證據相關聯的控制項名稱。
4. 事件來源 — 建立證據事件的資源名稱。
5. 事件名稱 — 證據事件的名稱。
6. 資料來源 — 從中收集證據的資料來源。
7. 類型證據 — 證據的類型。
   - 合規檢查證據收集自 AWS Config 或 AWS Security Hub。
   - 使用者活動證據收集自 AWS CloudTrail 日誌。
   - 組態資料證據收集自 Amazon EC2、Amazon S3 或 IAM 等其他 AWS 服務 快照。
   - 手動證據是您手動上傳的證據。
8. 合規檢查 — 屬於合規檢查類別之證據的評估狀態。
   - 對於收集自 AWS Security Hub 的證據，會直接從 AWS Security Hub 中報告通過或失敗結果。
   - 對於收集自 AWS Config 的證據，會直接從 AWS Config 中報告合規或不合規結果。
   - 如果顯示不適用，表示 AWS Security Hub 或 AWS Config 均未啟用，或證據來自不同的資料來源。
9. 包含的資源 — 為產生證據而評估的資源數量。

10屬性 — 證據中事件使用的屬性總數。

11AWS 帳戶 — 從中收集證據的 AWS 帳戶。

12IAM ID — 相關的使用者或角色 (如適用)。

13.已新增至評估報告 — 表示您是否選擇在評估報告中包含證據。

Attributes

屬性表會顯示此證據中事件使用的名稱和值。其包含下列資訊：

- 屬性名稱 — 證據的要求，例如 allowUsersToChangePassword。
- 值 — 屬性的值，例如 true 或 false。

包含的資源

包含的資源表格會顯示為產生證據而評估的資源清單。包含下列一個或多個欄位：

- ARN — 資源的 Amazon Resource Name (ARN)。ARN 可能不適用於所有證據類型。
- 值 — 該資源的值 (如適用)。
- JSON — 檢視該資源之 JSON 檔案的連結。

在 AWS Audit Manager 中添加手動證據

Audit Manager 可以自動收集多個控制項的證據。但是，某些控制項會要求您手動新增自己的證據。

請考量下列範例：

- 某些控制項與提供實體記錄 (例如簽名) 或非雲端產生事件 (例如觀察和訪談) 有關。在這些情況下，您可以手動上傳檔案作為證據。例如，如果控制項需要有關組織結構的資訊，您可以上傳公司組織圖的副本作為手動證據。
- 某些控制項代表供應商風險評估問題。風險評估問題可能需要文件作為證據 (例如組織圖)。或者，它可能只需要一個簡單的文字回應 (例如職位列表)。對於後者，您可以回應問題並將您的回應保存為手動證據。

您也可以使用手動上傳功能來管理來自多個環境的證據。如果您的公司使用混合雲端模型或多雲端模式，您可以上傳來自內部部署環境、雲端託管環境或 SaaS 應用程式的證據。這可讓您將證據儲存在 Audit Manager 評估的結構中，以組織您的證據 (不限來源)，其中每項證據都映射至特定控制項。

如需有關 Audit Manager 中不同類型證據的詳細資訊，請參閱本指南概念與術語區段中的證據。

如何添加手動證據

您可以使用下列任一方法，將自己的手動證據新增至評估控制項。

請謹記以下幾點：

- 您一次只能使用一種方法來新增手動證據。
- 一個手動證據檔案的最大支援 100 MB。
- 手動證據支援的檔案格式 在此頁面下方列出。
- 每個 AWS 帳戶 每天最多只能手動上傳 100 個證據檔案至控制項。超過這個每日配額，會導致該控制項的任何額外手動上傳失敗。如果您需要將大量手動證據上傳至單一控制項，請在數天內分批上傳證據。
- 當控制項處於非作用中狀態時，您無法添加手動證據至該控制項。如需添加手動證據，您必須先將控制項狀態變更為審核中或已審核。如需說明，請參閱 更新控制項狀態。

從 Amazon S3 匯入檔案

請依照下列步驟從 S3 儲存貯體匯入手動證據。

AWS console

如需從 S3 (主控台) 匯入檔案

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在左側導覽窗格中，選擇評估，然後選擇評估的名稱來將其開啟。
3. 選擇控制項索引標籤，向下捲動至控制集，然後選擇控制項名稱將其開啟。
4. 在證據資料夾索引標籤上，選擇添加手動證據，然後選擇從 S3 匯入檔案。
   - 或者，在證據資料夾索引標籤中選擇證據資料夾名稱以檢閱證據資料夾摘要，然後選擇添加手動證據、從 S3 匯入檔案。
5. 在下一頁，輸入證據的 S3 URI。您可以瀏覽至 Amazon S3 主控台中的物件，然後選擇複製 S3 URI 以尋找 S3 URI。
6. 選擇上傳。

AWS CLI

在下列程序中，將######取代為您自己的資訊。

如需從 S3 (CLI) 匯入檔案

1. 執行 list-assessments 命令查看評估清單。

```
aws auditmanager list-assessments
```

另外，找到您要向其上傳證據的評估，並記下評估 ID。

2. 執行 get-assessment 命令並指定步驟 1 的評估 ID。

```
aws auditmanager get-assessment --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
```

另外，找到控制集和您要向其上傳證據的控制項，並記下 ID。

3. 執行 batch-import-evidence-to-assessment-control 命令搭配下列參數：

- --assessment-id — 使用步驟 1 中的評估 ID。
- --control-set-id — 使用步驟 2 中的控制集 ID。
- --control-id — 使用步驟 2 中的控制項 ID。
- --manual-evidence — s使用 s3ResourcePath 作為手動證據類型，並指定證據的 S3 URI。您可以瀏覽至 Amazon S3 主控台中的物件，然後選擇複製 S3 URI 以尋找 S3 URI。

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet --control-
id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence s3ResourcePath=s3://
example-bucket/example-file.extension
```

Audit Manager API

如需從 S3 (API) 匯入檔案

1. 呼叫 ListAssessments 操作查看您的評估清單。另外，找到您要向其上傳證據的評估，並記下評估 ID。

2. 呼叫 GetAssessment 操作並指定步驟 1 的評估 ID。另外，找到控制集和您要向其上傳證據的控制項，並記下 ID。
3. 搭配下列參數呼叫 BatchImportEvidenceToAssessmentControl 操作：
   - assessmentId — 使用步驟 1 中的評估 ID。
   - controlSetId — 使用步驟 2 中的控制集 ID。
   - controlId — 使用步驟 2 中的控制項 ID。
   - manualEvidence — s使用 s3ResourcePath 作為手動證據類型，並指定證據的 S3 URI。您可以瀏覽至 Amazon S3 主控台中的物件，然後選擇複製 S3 URI 以尋找 S3 URI。

如需詳細資訊，請選擇先前的任一連結，在 AWS Audit Manager API 參考中閱讀更多資訊。這包括有關如何在其中一項特定語言 AWS 軟體開發套件中使用這些操作和參數的資訊。

從瀏覽器上傳檔案

請按照以下步驟從瀏覽器上傳手動證據。

AWS console

從瀏覽器上傳檔案 (主控台)

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在左側導覽窗格中，選擇評估，然後選擇評估的名稱來將其開啟。
3. 在控制項索引標籤，向下捲動至控制集，然後選擇控制項名稱將其開啟。

   這裡有三種上傳檔案的方法：
   - (選項 1) 在藍色通知橫幅中，選擇上傳手動證據。
   - (選項 2) 在證據資料夾索引標籤上，選擇添加手動證據，然後選擇從瀏覽器上傳檔案。
   - (選項 3) 選擇證據資料夾名稱以檢閱該資料夾的摘要，選擇添加手動證據，然後選擇從瀏覽器上傳檔案。
4. 選擇您要上傳的檔案。
5. 選擇上傳。

AWS CLI

在下列程序中，將######取代為您自己的資訊。

從瀏覽器上傳檔案 (CLI)

1. 執行 list-assessments 命令查看評估清單。

```
aws auditmanager list-assessments
```

另外，找到您要向其上傳證據的評估，並記下評估 ID。

2. 執行 get-assessment 命令並指定步驟 1 的評估 ID。

```
aws auditmanager get-assessment --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
```

另外，找到控制集和您要向其上傳證據的控制項，並記下 ID。

3. 執行 get-evidence-file-upload-url 命令並指定您要上傳的檔案。

```
aws auditmanager get-evidence-file-upload-url --file-name fileName.extension
```

此外，記下預先簽章的 URL 和 evidenceFileName。

4. 使用步驟 3 中的預先簽署 URL，從瀏覽器上傳檔案。此動作會將您的檔案上傳到 Amazon S3，並將其儲存為可附加至評估控制項的物件。在下面的步驟中，您將使用 evidenceFileName 參數引用新建立的物件。

> **Note**
>
> 當您使用預先簽署的 URL 上傳檔案時，Audit Manager 會使用 AWS Key Management Service 伺服器端加密來保護和儲存您的資料。為此，當您使用預先簽署的 URL 上傳檔案時，您必須在請求中使用 x-amz-server-side-encryption 標頭。
> 如果您使用的是 Audit Manager 資料加密 設定中的客戶管理 AWS KMS key，請務必在請求中也包含 x-amz-server-side-encryption-aws-kms-key-id 標頭。如果請求中沒有 x-amz-server-side-encryption-aws-kms-key-id 標頭，Amazon S3 會假設您想要使用 AWS 受管金鑰。
> 如需詳細資訊，請參閱 Amazon Simple Storage Service 使用者指南中的搭配 AWS Key Management Service 金鑰 (SSE-KMS) 使用伺服器端加密保護資料。

5. 執行 batch-import-evidence-to-assessment-control 命令搭配下列參數：

   - --assessment-id — 使用步驟 1 中的評估 ID。
   - --control-set-id — 使用步驟 2 中的控制集 ID。
   - --control-id — 使用步驟 2 中的控制項 ID。
   - --manual-evidence — 使用 evidenceFileName 作為手動證據類型，並指定步驟 3 中的證據檔案名稱。

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet
 --control-id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence
 evidenceFileName=fileName.extension
```

Audit Manager API

從瀏覽器上傳檔案 (API)

1. 呼叫 ListAssessments 操作。另外，找到您要向其上傳證據的評估，並記下評估 ID。
2. 呼叫 GetAssessment 操作並指定步驟 1 的 assessmentId。另外，找到控制集和您要向其上傳證據的控制項，並記下 ID。
3. 呼叫 GetEvidenceFileUploadUrl 操作並指定您要上傳的 fileName。此外，記下預先簽章的 URL 和 evidenceFileName。
4. 使用步驟 3 中的預先簽署 URL，從瀏覽器上傳檔案。此動作會將您的檔案上傳到 Amazon S3，並將其儲存為可附加至評估控制項的物件。在下面的步驟中，您將使用 evidenceFileName 參數引用新建立的物件。

> **Note**
>
> 當您使用預先簽署的 URL 上傳檔案時，Audit Manager 會使用 AWS Key Management Service 伺服器端加密來保護和儲存您的資料。為此，當您使用預先簽署的 URL 上傳檔案時，您必須在請求中使用 x-amz-server-side-encryption 標頭。如果您使用的是 Audit Manager 資料加密 設定中的客戶管理 AWS KMS key，請務必在請求中也包含 x-amz-server-side-encryption-aws-kms-key-id 標頭。如果請求中沒有 x-amz-server-side-encryption-aws-kms-key-id 標頭，Amazon S3 會假設您想要使用 AWS 受管金鑰。

如需詳細資訊，請參閱 Amazon Simple Storage Service 使用者指南中的搭配 AWS Key Management Service 金鑰 (SSE-KMS) 使用伺服器端加密保護資料。

5. 搭配下列參數呼叫 `BatchImportEvidenceToAssessmentControl` 操作：

   - `assessmentId` — 使用步驟 1 中的評估 ID。
   - `controlSetId` — 使用步驟 2 中的控制集 ID。
   - `controlId` — 使用步驟 2 中的控制項 ID。
   - `manualEvidence` — 使用 `evidenceFileName` 作為手動證據類型，並指定步驟 3 中的證據檔案名稱。

如需詳細資訊，請選擇先前的任一連結，在 AWS Audit Manager API 參考中閱讀更多資訊。這包括有關如何在其中一項特定語言 AWS 軟體開發套件中使用這些操作和參數的資訊。

輸入文字回應

請依照下列步驟輸入風險評估問題的回應，並將您的回覆儲存為手動證據。

AWS console

如需輸入文字回應 (主控台)

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在左側導覽窗格中，選擇評估，然後選擇評估的名稱來將其開啟。
3. 選擇控制項索引標籤，向下捲動至控制集，然後選擇控制項名稱將其開啟。

   這裡有三種輸入文字回應的方法：

   - (選項 1) 在藍色通知橫幅中，選擇輸入回應。
   - (選項 2) 在證據資料夾索引標籤上，選擇添加手動證據，然後選擇輸入回應。
   - (選項 3) 選擇證據資料夾以檢閱該資料夾的摘要，選擇添加手動證據，然後選擇輸入回應。
4. 在出現的快顯視窗中，輸入純文字格式的回應。
5. 選擇確認。

AWS CLI

在下列程序中，將######取代為您自己的資訊。

如需輸入文字回應 (CLI)

1. 執行 list-assessments 命令。

```
aws auditmanager list-assessments
```

另外，找到您要向其上傳證據的評估，並記下評估 ID。

2. 執行 get-assessment 命令並指定步驟 1 的評估 ID。

```
aws auditmanager get-assessment --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
```

另外，找到控制集和您要向其上傳證據的控制項，並記下 ID。

3. 執行 batch-import-evidence-to-assessment-control 命令搭配下列參數：

- `--assessment-id` — 使用步驟 1 中的評估 ID。
- `--control-set-id` — 使用步驟 2 中的控制集 ID。
- `--control-id` — 使用步驟 2 中的控制項 ID。
- `--manual-evidence` — 使用 `textResponse` 作為手動證據類型，然後輸入要保存為手動證據的文字。

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet --control-
id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence textResponse="enter
 text here"
```

Audit Manager API

如需輸入文字回應 (API)

1. 呼叫 ListAssessments 操作。另外，找到您要向其上傳證據的評估，並記下評估 ID。
2. 呼叫 GetAssessment 操作並指定步驟 1 的 `assessmentId`。另外，找到控制集和您要向其上傳證據的控制項，並記下 ID。

3. 搭配下列參數呼叫 BatchImportEvidenceToAssessmentControl 操作：

   - assessmentId — 使用步驟 1 中的評估 ID。
   - controlSetId — 使用步驟 2 中的控制集 ID。
   - controlId — 使用步驟 2 中的控制項 ID。
   - manualEvidence — 使用 textResponse 作為手動證據類型，然後輸入要保存為手動證據的文字。

如需詳細資訊，請選擇先前的任一連結，在 AWS Audit Manager API 參考中閱讀更多資訊。這包括有關如何在其中一項特定語言 AWS 軟體開發套件中使用這些操作和參數的資訊。

手動證據支援的檔案格式

下表列出並說明您可以將其作為手動證據上傳的檔案類型。對於每種檔案類型，表格也會列出支援的副檔名。

檔案類型	描述	支援的檔案副檔名
壓縮或存檔	GNU Zip 壓縮的封存檔和 ZIP 壓縮的封存檔	.gz, .zip
文件	常見的文件檔案，例如 PDF 和 Microsoft Office 檔案	.doc, .docx, .pdf, .ppt, .pptx, .xls, .xlsx
映像	圖像和圖形檔案	.jpeg, .jpg, .png, .svg
文字	其他非二進位文字檔案，例如純文字文件和標記語言檔案	.cer, .csv, .html, .jmx, .json, .md, .out, .rtf, .txt, .xml, .yaml, .yml

產生評估報告

評估報告會總結您的評估，並提供包含相關證據的組織好的資料夾集的連結。如需更多詳細資訊，請參閱 評估報告。

在產生評估報告之前，您可以選擇要包含在評估報告中的證據。新收集的證據不會自動包含在評估報告中。

任務

- 將證據添加至評估報告
- 從評估報告中移除證據
- 產生評估報告
- 我接下來要怎麼做？

將證據添加至評估報告

您必須至少在評估報告中添加一項證據，才能產生評估報告。您可以添加整個證據資料夾，也可以添加資料夾中的單項證據。

如需將證據添加至評估報告

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在導覽窗格中，選擇評估，然後選擇評估的名稱來將其開啟。
3. 在控制項索引標籤，向下捲動至控制集表格，然後選擇控制項名稱將其開啟。
4. 選擇將證據添加至評估報告的方式。

    a. 如需添加整個證據資料夾，請向下捲動至證據資料夾，選擇您要添加的資料夾，然後選擇添加至評估報告。

    - 如果您看不到要尋找的資料夾，請將下拉式清單篩選條件變更為所有時間。否則，依預設，您會看到最近七天的資料夾。
    - 如果添加至評估報告呈灰色，表示證據資料夾已添加至評估報告。

    b. 如需添加特定證據，請選擇證據資料夾以開啟其內容。從清單中選擇一個或多個項目，然後選擇添加至評估報告。

    - 如果添加至評估報告顯示為灰色，請確定您已選擇證據旁的核取方塊，然後再試一次。

5. 將證據添加至評估報告後，會出現綠色的成功橫幅。選擇在評估報告中檢視證據查看將包含在評估報告中的證據。
    - 或者，您可以導覽回您的評估並選擇評估報告選擇索引標籤，查看將包含在評估報告中的證據。

從評估報告中移除證據

如果您需要從評估報告中移除證據，請按照下列步驟操作。您可以移除整個證據資料夾，也可以從資料夾中移除特定證據。

如需從評估報告中移除證據

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在導覽窗格中，選擇評估，然後選擇評估的名稱來將其開啟。
3. 在控制項索引標籤，向下捲動至控制集表格，然後選擇控制項名稱將其開啟。
4. 選擇您要從評估報告中移除證據的方式。

   a. 如需移除整個證據資料夾，請向下捲動至證據資料夾，選擇您要移除的資料夾，然後選擇從評估報告中移除。

      - 如果您看不到要尋找的資料夾，請將下拉式清單篩選條件變更為所有時間。否則，依預設，您會看到最近七天的資料夾。
      - 如果從評估報告中移除顯示為灰色，表示證據資料夾已從評估報告中移除。

   b. 如需移除特定證據，請選擇證據資料夾以開啟其內容。從清單中選擇一個或多個項目，然後選擇從評估報告中移除。

      - 如果從評估報告中移除顯示為灰色，請確定您已選擇證據旁的核取方塊，然後再試一次。
5. 將證據添加至評估報告後，會出現綠色的成功橫幅。選擇在評估報告中檢視證據查看將包含在評估報告中的證據。
   - 或者，您可以導覽回您的評估並選擇評估報告選擇索引標籤，查看將包含在評估報告中的證據。

產生評估報告

將證據添加至評估報告後，您可以產生最終評估報告，以便與稽核人員分享。產生評估報告時，會將其放置在您選擇作為評估報告目的地的 S3 儲存貯體中。

> **Tip**
>
> 為確保成功產生評估報告，請檢閱 評估報告目的地的組態提示.

產生評估報告

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在左側導覽窗格中，選擇評估。
3. 選擇您要為其產生評估報告的評估的名稱。
4. 選擇評估報告選擇索引標籤，然後選擇產生評估報告。
   - 如果產生評估報告顯示為灰色，表示尚未將證據添加至評估報告。
5. 在快顯視窗中，提供評估報告的名稱和描述，並檢閱評估報告詳細資訊。
6. 選擇產生評估報告，數分鐘後便會產生評估報告。
7. 您可以從 Audit Manager 主控台的下載中心頁面，找到並下載評估報告。
   - 或者，您可以前往評估報告目的地 S3 儲存貯體，然後從該處下載評估報告。

評估報告具有檔案校檢查總和，以確保評估報告的完整性。您可以透過 Audit Manager 提供的 ValidateAssessmentReportIntegrity API 進行驗證。

我接下來要怎麼做？

產生評估報告後，您可以進一步了解以下資訊：

- 尋找並下載您的評估報告 — 了解如何從下載中心或 Amazon S3 下載評估報告。
- 探索您的評估報告 — 了解如何導覽評估報告並探索其內容。
- 驗證您的評估報告 — 了解如何使用 ValidateAssessmentReportIntegrity API 操作來驗證您的評量報告。
- 刪除不需要的評估報告 — 了解如何從下載中心或 Amazon S3 刪除不需要的報告。

將評估狀態變更為非作用中

當您不再需要收集評估的證據時，您可以將評估狀態變更為非作用中。當評估的狀態變更為非作用中時，評估就會停止收集證據。因此，針對該評估，您不會再產生任何費用。

除了停止證據收集之外，Audit Manager 還可以對非作用中評估內的控制項進行下列變更：

- 所有控制集都變更為已檢閱狀態。
- 處於審核中狀態的所有控制項變更為已審核

- 非作用中評估的委派人員無法再檢視或編輯其控制項和控制集。

> **Warning**
>
> 此動作不可復原。我們建議您謹慎進行，並確認您確實希望將評估標記為非作用中。當評估處於非作用中狀態時，您只有唯讀存取權。這表示您仍然可以檢閱先前收集的證據並產生評估報告。然而，您無法編輯非作用中的評估、新增註解或上傳任何手動證據。

Audit Manager console

將評估狀態變更為非作用中 (主控台)

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在導覽窗格中，選擇評估。
3. 選擇評估名稱來開啟評估。
4. 在頁面右上角選擇更新評估狀態，然後選擇非作用中。
5. 在快顯視窗中選擇更新狀態，以確認您要將狀態變更為非作用中。

評估及其控制項的變更會在大約一分鐘後生效。

AWS CLI

如需將評估狀態變更為非作用中 (AWS CLI)

1. 首先，識別您要更新的評估。為此，執行 list-assessments 命令。

```
aws auditmanager list-assessments
```

執行後，傳回評估清單。找到您要停用的評估，並記下評估 ID。

2. 接下來，執行 update-assessment-status 命令，並指定下列參數：

   - `--assessment-id` — 使用此參數可指定您要停用的評估。
   - `--status` – 將此值設定為 `INACTIVE`。

在下列範例中，將######取代為您自己的資訊。

```
aws auditmanager update-assessment-status --assessment-id a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111 --status INACTIVE
```

評估及其控制項的變更會在大約一分鐘後生效。

Audit Manager API

將評估狀態變更為非作用中 (API)

1. 使用 ListAssessments 操作尋找您要停用的評估，並記下評估 ID。
2. 使用 UpdateAssessmentStatus 操作並指定下列參數：
   - assessmentId — 使用此參數可指定您要停用的評估。
   - status — 將此值設定為 `INACTIVE`。

評估及其控制項的變更會在大約一分鐘後生效。

有關此 API 操作的更多資訊，請選擇先前的任一連結，在 AWS Audit ManagerAPI 參考資料中閱讀更多資訊。這包括有關如何在其中一項特定語言 AWS 軟體開發套件中使用這些操作和參數的資訊。

刪除評估

您可以刪除任何不再需要的 Audit Manager 評估。您可以使用 Audit Manager 主控台、Audit Manager API 或 AWS Command Line Interface (AWS CLI) 刪除評估。

> **Warning**
>
> 此動作會永久刪除您的評估及其收集的所有證據。您無法復原此資料。因此，我們建議您謹慎行事，並確定您真的要刪除您的評估。

Audit Manager console

如需刪除評估 (主控台)

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在導覽窗格中，選擇評估。
3. 選擇您要刪除的評估，然後選擇刪除。
   - 或者，您可以開啟評估，然後選擇頁面右上角的刪除。

AWS CLI

如需刪除評估 (AWS CLI)

1. 首先，確定您要刪除的評估。為此，執行 list-assessments 命令。

   ```
   aws auditmanager list-assessments
   ```

   執行後，傳回評估清單。找到您要刪除的評估，並記下評估 ID。
2. 接下來，使用 delete-assessment 命令，並指定要刪除的評估 `--assessment-id`。

   在下列範例中，將*######*取代為您自己的資訊。

   ```
   aws auditmanager delete-assessment --assessment-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

Audit Manager API

刪除評估 (API)

1. 使用清單評估作業來尋找您要刪除的評估。

   此外，記下評估 ID。
2. 使用 DeleteAssessment 操作，並指定您要刪除的評估的 assessmentId。

有關此 API 操作的更多資訊，請選擇先前的任一連結，在 AWS Audit ManagerAPI 參考資料中閱讀更多資訊。這包括有關如何在其中一項特定語言 AWS 軟體開發套件中使用這些操作和參數的資訊。

> **Tip**
>
> 如果您的目標是降低成本，請考慮將評估狀態變更為非作用中，而不是將其刪除。此動作會停止證據收集，並將您的評估置於唯讀狀態，您可以在其中檢閱先前收集的證據。非作用中的評估不會產生任何費用。

在 AWS Audit Manager 中委派

稽核擁有者可使用AWS Audit Manager來建立評估，並收集該評估中所列控制項的證據。有時，稽核擁有者在驗證控制集的證據時，可能會遇到問題或需要協助。在此情況下，稽核擁有者可以委派主題專家對控制項集進行審核。

高階的委派程序如下。

1. 稽核擁有者會在其評估中選擇控制項集，並委派該控制項集以供審核。
2. 委派人會對這些控制項及其證據進行審核，完成後將控制項集回傳給稽核擁有者。
3. 稽核擁有者會被通知審核已完成，並檢查委派人對審核的控制項是否有任何備註。

瀏覽本指南的以下各章節，瞭解更多如何在AWS Audit Manager中管理委派任務資訊。

主題

- 稽核擁有者的委派任務
- 委派人的委派工作

> **Note**
>
> 帳戶可以是不同 AWS 區域的稽核擁有者或委派代表。

稽核擁有者的委派任務

身為AWS Audit Manager的稽核擁有者，您可能需要主題專家的協助，以協助您審核控制項和證據。在此情況下，您可以委派控制集以進行檢閱。

以下主題描述了您如何在AWS Audit Manager中管理委派事項。

委派任務

- 委派需要檢閱的控制集
- 存取您的活動和已完成的委託
- 刪除您的活動和已完成的委派

委派需要檢閱的控制集

當您需要主題專家的協助時，您可以選擇要協助的AWS帳戶，然後將控制集委派給他們進行審核。

您可以使用下列任一程序以委派控制集。

從評估頁面委派控制集

從評估頁面委派一個控制集

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在導覽窗格中，選擇評估。
3. 選擇包含您要委派的控制集評估名稱。
4. 在評估頁面中，選擇控制項索引標籤。這會顯示評估中的控制項狀態摘要和控制項清單。
5. 選取控制集，然後選擇委派控制集。
6. 在 委派選取 下，會顯示使用者和角色的清單。選擇使用者或角色，或使用搜尋列以尋找使用者或角色。
7. 在委派詳細資訊下，審核控制集名稱和評估名稱。
8. (選擇性) 在評論下，新增附有指示的評論，以協助委派人完成其審核任務。請勿在您的評論中包含任何敏感資訊。
9. 選擇委派控制集。
10. 綠色成功橫幅可確認控制集委派成功。選擇檢視委派來查看委派請求。您也可以在AWS Audit Manager主控台的左側導覽窗格中選擇委派，隨時查看委派事項。

從委派頁面委派一個控制集

從委派頁面委派一個控制集

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在導覽窗格中，選擇委派。
3. 在委派頁面中，選擇 建立委派。
4. 在選擇評估與控制集下，指定您要委派的評估和控制集。
5. 在委託選擇下，您將看到用戶和角色的清單。選擇使用者或角色，或使用搜尋列以尋找使用者或角色。

6. (選擇性) 在評論下，新增附有指示的評論，以協助委派人完成其審核任務。請勿在您的評論中包含任何敏感資訊。
7. 選擇 建立委派。
8. 綠色成功橫幅可確認控制集委派成功。選擇檢視委派來查看委派請求。您也可以在AWS Audit Manager主控台的左側導覽窗格中選擇委派，隨時查看委派事項。

當您委派控制集進行審核時，委派人會收到通知，即可開始進行控制集審核。委派人的遵循流程在委派人的委派工作中有所描述。

> **Tip**
>
> 委派人可以訂閱 SNS 主題，以在被委派進行審核任務時接收電子郵件警示。如需如何分辨及訂閱與AWS Audit Manager相關的 SNS 主題的詳細資訊，請參閱AWS Audit Manager中的通知。

存取您的活動和已完成的委託

您可以隨時在AWS Audit Manager左側導覽窗格中選擇委派，以存取您的委派清單。委派頁面包含您的活動和已完成委派的清單，以及各委派的詳細資訊：

- 委派對象 — 委派控制集的 Amazon Web Services account。
- 日期— 委派控制項集的日期。
- 狀態— 委派的目前狀態。
- 評估— 評估名稱，附帶評估詳細資訊頁面的連結。
- 控制集 — 已委派審核的控制集名稱。

委派完成後，您會在AWS Audit Manager中收到通知。您也可能會收到委派人的附評論的備註。下列程序說明在完成委派後，如何檢查 Audit Manager 中的通知，以及如何查看委派人可能為您留下的任何評論。

檢視已完成的委託並檢查評論

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在導覽窗格中，選擇通知。或者，在螢幕上方的藍色閃爍列中選擇通知，來開啟通知頁面。

3. 檢閱通知頁面，其中包含下列資訊表格：
   - 日期— 通知的日期。
   - 評估— 與控制集相關的評估名稱。
   - 控制集 — 控制集的名稱。
   - 來源 — 將已完成控制集提交給您的委派人的使用者或角色。
   - 說明 — 委派提供的高階備註。
4. 尋找委派人已審核並送交給您的評估與控制集，然後選擇要開啟的評估名稱。
5. 在評估詳細資訊頁面的控制項索引標籤下，向下捲動至控制集表格。在依控制集分組的控制項欄位下，展開控制集名稱以顯示其控制項。然後，選擇控制項名稱以開啟控制項詳細資訊頁面。
6. 選擇評論索引標籤，以檢視委派人針對特定控制項新增的任何備註。
7. 當您確定某個控制集的審核已達滿意狀態時，請選取控制集，然後選擇完成控制集審核。

> **Important**
>
> Audit Manager 會持續收集證據。因此，在委派完成對控制項的檢閱後，可能會收集其他新證據。
> 如果您只想在評估報告中使用已審核過的證據，則可以參考控制項審核的時間戳記，來確定何時審核證據。可在控制項詳細資訊頁面的變更記錄索引標籤上找到此時間戳記。接著，您可以使用此時間戳記來分辨要新增至評估報告的證據。

刪除您的活動和已完成的委派

在某些情況下，您可能會建立委派，但之後不再需要協助審核該控制集。這種情況下，您可以在AWS Audit Manager中刪除使用中的委派。您也可以刪除不想再顯示在委派頁面上的已完成委派。

刪除委派

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在導覽窗格中，選擇委派。
3. 在委派頁面上，選取您要取消的委派，然後選擇移除委派。
4. 在出現的快顯視窗中，選擇刪除來確認您的選擇。

委派人的委派工作

委派人通常在多個不同領域具備專業的業務或技術專長。其中包括資料保留原則、訓練計畫、網路基礎架構和身分識別管理。他們可以幫助稽核擁有者審核收集到的證據，以了解屬於其專業領域的控制項。

身為委派人，您可能會收到來自稽核擁有者的要求，以審核與控制集相關的證據。此要求表示稽核擁有者需要您的協助以驗證此證據。您可以協助稽核擁有者，方法是審核控制集及其相關證據、新增評論、上傳其他證據，以及更新您審核的各控制項狀態。

以下主題描述了您如何在AWS Audit Manager中管理委派事項。

> **Note**
>
> 稽核擁有者委派特定控制集以供審核，而非整個評估。因此，委派代表對評估的存取權限有限。委派可以審核證據、新增評論、上傳手動證據，以及更新控制項集中每個控制項的控制項狀態。如需有關 Audit Manager 中角色和許可的詳細資訊，請參閱 中使用者角色的建議政策 AWS Audit Manager。

委派任務

- 查看您的委派請求通知
- 審核委派的控制集及其相關證據
- 將評論添加到控制項
- 將控制項標示為已檢閱
- 將審核的控制項集送交回稽核擁有者

查看您的委派請求通知

當稽核擁有者請求您協助審核控制集時，您會收到通知，通知您委派給您的控制集。

> **Tip**
>
> 您也可以訂閱 SNS 主題，以便在控制集委派給您以供檢閱時接收電子郵件提醒。如需詳細資訊，請參閱 AWS Audit Manager 中的通知。

若要檢視您的通知

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在左側導覽窗格中，選擇通知。或者，在螢幕上方的藍色閃爍列中，選擇檢視通知以開啟通知頁面。
3. 在通知頁面上，檢閱已委派給您進行審核的控制集清單。此表格包含以下資訊：
   - 日期— 委派控制集的日期。
   - 評估— 與控制集相關的評估名稱。
   - 控制集 — 控制集的名稱。
   - 來源 — 委派控制集給您的使用者或角色。
   - 說明 — 稽核擁有者提供的指引。

審核委派的控制集及其相關證據

您可以透過檢閱稽核擁有者委託給您的控制集來協助他。您可以檢查這些控制項及其相關證據，以判斷是否需要任何其他動作。此類額外動作可能包括手動上傳其他證據以證明合規性，或留下評論以說明您遵循的修正步驟。

如需檢閱控制集

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在導覽窗格中，選擇通知。或者，在藍色閃光列中，選擇檢視通知以開啟通知頁面。
3. 在通知頁面上，會顯示委派給您的控制集清單。分辨您要檢閱的控制集，並選擇相關評估的名稱，以開啟評估詳細資訊頁面。
4. 在評估詳細資訊頁面的控制項索引標籤下，向下捲動至控制集表格。
5. 在控制集分組的控制項欄位下，展開控制項集的名稱以顯示其控制項，然後選擇控制項名稱以開啟控制項詳細資訊頁面。
6. (選擇性) 選擇更新控制項狀態以變更控制項的狀態。審核正在進行時，您可以將狀態標示為審核中。
7. 在證據資料夾、資料來源、評論和變更記錄索引標籤中，檢視控制項的相關資訊。有關這些索引標籤中的每個標籤，以及與此資訊相關的詳細資訊，請參閱檢閱評估中的控制項。

如需檢閱控制項的證據

1. 在控制項詳細資訊頁面中，選擇證據資料夾索引標籤。
2. 導覽至證據資料夾表格，會顯示包含該控制項之證據的資料夾清單。這些資料夾是根據收集證據的日期來組織和命名。
3. 選擇證據資料夾的名稱以將其開啟。然後，查看在該日期收集的所有證據摘要。此摘要包括直接從AWS Security Hub、AWS Config或兩者報告的合規檢查問題總數。有關如何解譯此頁面上資料的說明，請參閱審核證據資料夾。
4. 從證據資料夾摘要頁面，瀏覽至證據表格。在時間欄位中，選擇要開啟的明細項目。然後，查看當時收集的證據詳細資訊。有關如何解譯證據詳細資訊頁面上資料的說明，請參閱檢閱個別證據。

> **Tip**
>
> 雖然AWS Audit Manager自動收集許多控制項的證據，但在某些情況下，您可能需要提供其他證據來證明合規性。在這些情況下，您可以手動上傳證據。如需指示，請參閱上傳手動證明。

將評論添加到控制項

您可以為審核的任何控制項新增評論。稽核擁有者可以看見這些評論。

若要將評論加入至控制項

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在左側導覽窗格中，選擇通知。或者，選擇畫面頂端藍色閃爍列中的檢視通知，以開啟通知頁面。
3. 在通知頁面上，檢閱委派給您的控制集清單。尋找包含您要為其留下評論之控制項的控制集，然後選擇相關評估的名稱。
4. 選擇控制項索引標籤，向下捲動至控制集表格，然後選取控制項名稱加以開啟。
5. 選擇評論索引標籤。
6. 在傳送評論底下，在文字方塊中輸入您的評論。
7. 選擇送交評論以添加您的評論。然後，您的評論會顯示在頁面的先前評論章節下，以及與此控制項相關的任何其他評論。

將控制項標示為已檢閱

您可以透過更新控制集內個別控制項的狀態，以表明審核進度。變更控制項狀態是選擇性的。不過，建議您在完成該控制項的審核時，將每個控制項的狀態變更為已審核。無論個別控制項的狀態為何，您仍然可以將控制項送交回稽核擁有者。

若要將控制項標記為已審核

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在左側導覽窗格中，選擇通知。或者，選擇畫面頂端藍色閃爍列中的檢視通知，以開啟通知頁面。
3. 在通知頁面上，檢閱委派給您的控制集清單。尋找您要標示為已檢閱的控制集，並選擇相關評估的名稱。
4. 在評估詳細資訊頁面的控制項索引標籤下，向下捲動至控制集表格。
5. 在依控制集分組的控制項欄位下，展開控制集名稱以顯示其控制項。選擇控制項名稱以開啟控制項詳細資訊頁面。
6. 選擇更新控制項狀態，並將狀態變更為已審核
7. 在出現的快顯視窗中，選擇 更新控制項狀態，確認您已完成審核控制項。

將審核的控制項集送交回稽核擁有者

審查完委派給您的控制項後，請將控制集送交給稽核擁有者。這樣就完成了委派程序。

若要將已審核的控制集送交回稽核擁有者，請執行

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在左側導覽窗格中，選擇通知。
3. 檢閱委派給您的控制集清單。搜尋您要送交回稽核擁有者的控制集，然後選擇相關評估的名稱。
4. 向下捲動至控制集表格，選取要送交給稽核擁有者的控制集，然後選擇提交以供審核。
5. 在出現的快顯視窗中，您可以先新增評論，然後再選擇送出以供審核。將控制項送交給稽核擁有者之後，他們就可以審核您為其留下的任何評論。

評估報告

評估報告總結了針對評估收集的選定證據。它還包含指向 PDF 檔案的連結，其中包含有關每項證據的詳細資訊。評估報告的具體內容、組織和命名慣例取決於您在產生報告時選擇的參數。

評估報告可協助您選擇和編譯與稽核相關的證據。但是，他們不會評估證據本身的合規性。相反地，Audit Manager 只會提供選定證據的詳細資訊作為您可與稽核人員共用的輸出。

評估報告資料夾結構

當您下載評估報告時，Audit Manager 會產生一個 zip 資料夾。這包含您的評估報告和巢狀子資料夾中的相關證據檔案。

zip 資料夾的結構如下所示：

- 評估資料夾 (範例：`myAssessmentName-a1b2c3d4`) — 根資料夾。
  - 評估報告資料夾 (範例：`reportName-a1b2c3d4e5f6g7`) — 您可以在其中找到 AssessmentReportSummary.pdf、digest.txt 和 README.txt 檔案的子資料夾。
    - 控制項證據資料夾 (範例：`controlName-a1b2c3d4e5f6g`) — 依相關控制項將證據檔案分組的子資料夾。
      - 資料來源證據資料夾 (範例：`CloudTrail`,`Security Hub`) — 依資料來源類型將證據檔案分組的子資料夾。
        - 日期證據資料夾 (範例：`2022-07-01`) — 依證據收集日期將證據檔案分組的子資料夾。
          - 證據檔案 — 包含單個證據詳細資訊的檔案。

如何導覽至評估報告

首先開啟 zip 資料夾，然後導覽下一層級至評估報告資料夾。在這裡，您可以找到評估報告 PDF 和 README.txt 檔案。

您可以檢閱 README.txt 檔案，了解 zip 資料夾的結構和內容。它還提供有關每個檔案命名慣例的參考資訊。如果您要尋找特定項目，這項資訊可協助您直接導覽至子資料夾或證據檔案。

否則，如需瀏覽證據並找到所需資訊，請開啟評估報告 PDF。其提供報告的高階概觀，以及建立報告所依據評估的摘要。

接下來，使用目錄 (TOC) 瀏覽報表。您可以選擇 TOC 中的任何超連結控制項，直接跳至該控制項的摘要。

當您準備好檢閱控制項的證據詳細資訊時，您可以選擇超連結的證據名稱來執行此操作。對於自動化證據，超連結會開啟一個新的 PDF 檔案，其中包含有關該證據的詳細資訊。對於手動證據，超連結會將您帶到包含證據的 S3 儲存貯體。

> **Tip**
>
> 每個頁面頂端的頁面導覽路徑導覽會在您瀏覽控制項和證據時，在評估報告中顯示您目前的位置。選擇超連結目錄，隨時導覽回目錄。

評估報告區段

請使用下列資訊來進一步了解評估報告的各個區段。

> **Note**
>
> 當您在下列區段中的任何屬性旁看到連字號 (-) 時，表示該屬性的值為 null，即值不存在。

- 封面
- 概觀頁面
- 目錄頁
- 控制項頁面
- 證據摘要頁面
- 證據詳細資訊頁

封面

封面包含評估報告的名稱。它也會顯示產生報表的日期和時間，以及產生報表之使用者的帳戶 ID。

封面的格式如下。Audit Manager 會以報告相關資訊取代*####*。

```
Assessment report name
Report generated on MM/DD/YYYY at HH:MM:SS AM/PM UCT by AccountID
```

概觀頁面

概觀頁面有兩個部分：報告本身的摘要，以及正在報告的評估摘要。

報告摘要

本區段總結評估報告。

- 報告名稱 — 報告的名稱。
- 描述 — 稽核擁有者在產生報告時輸入的描述。
- 產生日期 — 產生報告的日期。時間以國際標準時間 (UTC) 表示。
- 包含的控制項總數 — 包含在報告中且已收集證據的控制項數量。這是評估中控制項總數的子集。
- 包括的 AWS 帳戶 — 包含在報告中且已收集證據的 AWS 帳戶 數量。這是評估中 AWS 帳戶 總數的子集。
- 評估報告選擇 — 選擇要包含在報告中的證據項目數。包含報告中發現的合規檢查問題總數。

評估摘要

本區段總結報告相關的評估。

- 評估名稱 — 產生報告所依據評估的名稱。
- 狀態 — 產生報告時評估的狀態。
- 評估區域 — 建立評估的 AWS 區域。
- 範圍內 AWS 帳戶 — 包含於評估範圍內的 AWS 帳戶 完整清單。
- 範圍內 AWS 服務 — 包含於評估範圍內的 AWS 服務 完整清單。
- 架構名稱 — 建立評估所依據架構的名稱。
- 稽核擁有者 — 評估稽核擁有者的使用者或角色。
- 上次更新 — 上次更新評估的日期。時間以 UTC 表示。

目錄頁

目錄會顯示評估報告的完整目錄。目錄根據評估中包含的控制集進行分組和組織。控制項會列在其各自的控制集之下。

選擇目錄中的任何項目，直接導覽至報告的該區段。您可以選擇控制集，也可以直接前往控制項。

控制項頁面

控制項頁面有兩個部分：控制項本身的摘要，以及針對控制項收集的證據摘要。

控制項摘要

此區段包含下列資訊：

- 控制項名稱 — 控制項的名稱。
- 描述 — 控制項的描述。
- 控制集 — 控制項所屬控制集的名稱。
- 測試資訊 — 此控制項的建議測試程序。
- 行動計畫 — 在控制項未完成情況下，建議執行的動作。
- 評估報告選擇 — 包含在評估報告中與此控制項相關的證據項數量。這包括針對此控制項的證據找到的合規檢查問題數量。

收集的證據

本區段顯示針對控制項收集的證據。證據會依據資料夾分組，這些資料夾會依據證據收集日期進行組織與命名。每個證據資料夾名稱旁邊是該資料夾的合規檢查問題總數。

每個證據資料夾名稱下方都有超連結的證據名稱清單。

- 自動化證據名稱以證據收集時間戳記開頭，後跟服務代碼、事件名稱 (最多 20 個字元)、帳戶 ID 和 12 個字元的唯一 ID。

  例如：`21-30-24_IAM_CreateUser_111122223333_a1b2c3d4e5f6`。

  對於自動化證據，超連結名稱會開啟一個新的 PDF 檔案，其中包含摘要和進一步的詳細資訊。
- 手動證據名稱以證據上傳時間戳記開頭，後跟 `manual` 標籤、帳戶 ID 和 12 個字元的唯一 ID。還包括檔案名稱的前 10 個字元和副檔名 (最多 10 個字元)。

  例如：`00-00-00_manual_111122223333_a1b2c3d4e5f6_myimage.png`。

  對於手動證據，超連結名稱會將您帶到包含該證據的 S3 儲存貯體。

每個證據名稱旁邊是該項目的合規檢查的結果。

- 對於收集自 AWS Security Hub 或 AWS Config 的自動化證據，報告合規，不合規或不確定的結果。
- 對於收集自 AWS CloudTrail 和 API 呼叫的自動化證據，以及所有手動證據，顯示不確定的結果。

證據摘要頁面

證據摘要頁面包含以下資訊：

- ID — 證據的唯一識別符。
- 收集日期 — 建立或上傳證據的日期。
- 描述 — 證據的描述，包括帳戶 ID 和資料來源類型。
- 評估名稱 — 產生報告所依據評估的名稱。
- 架構名稱 — 建立評估所依據架構的名稱。
- 控制項名稱 — 證據支援的控制項名稱。
- 控制集名稱 — 相關控制項所屬控制集的名稱。
- 控制項描述 — 證據支援之控制項的描述。
- 測試資訊 — 此控制項的建議測試程序。
- 行動計畫 — 在控制項未完成情況下，建議執行的動作。
- AWS 區域 — 與證據相關聯的區域名稱。
- IAM ID — 與證據相關聯的使用者或角色的 ARN。
- AWS 帳戶 — 與證據相關聯的 AWS 帳戶 ID。
- AWS 服務 — 與證據相關聯的 AWS 服務 名稱。
- 包含的資源 — 評估認定為產生證據的 AWS 資源。此屬性不適用於來自 AWS Config 的合規檢查證據。對於此證據類型，您可以找到證據 PDF 證據詳細資訊頁 中列出的所有資源。
- 事件名稱 — 證據事件的名稱。
- 事件時間 — 證據事件發生的時間。
- 資料來源 — 從何處收集或上傳證據。資料來源類型可以是 AWS Config、Security Hub、AWS API 呼叫、CloudTrail 或手動。
- 類型證據 — 證據的類別
  - 合規檢查證據收集自 AWS Config 或 Security Hub。
  - 使用者活動證據收集自 CloudTrail 日誌。
  - 組態資料證據收集自其他 AWS 服務 的快照。
  - 手動證據是您手動上傳的證據。

- 合規檢查狀態 — 屬於合規檢查類別之證據的評估狀態。
  - 對於收集自 AWS Security Hub 或 AWS Config 的自動化證據，報告合規，不合規或不確定的結果。
  - 對於收集自 AWS CloudTrail 和 API 呼叫的自動化證據，以及所有手動證據，顯示不確定的結果。

證據詳細資訊頁

證據詳細資訊頁會顯示證據的名稱和證據詳細資訊表。此表提供證據每個元素的詳細明細，以便您了解資料並驗證資料是否正確。根據證據的資料來源，證據詳細資訊頁的內容會有所不同。

> **Tip**
>
> 每個頁面頂端的頁面導覽路徑導覽會在您瀏覽證據詳細資訊時，顯示您目前的位置。選擇證據摘要以隨時瀏覽回證據摘要。

評估報告完整性檢查

當您產生評估報告時，Audit Manager 會產生名為 `digest.txt` 的報告檔案檢查總和。您可以使用此檔案來驗證報告的完整性，並確保在建立報告後未修改任何證據。它包含具有簽章和雜湊 (如果報告存檔的任何部分變更，則無效) 的 JSON 對象。

如需驗證評估報告的完整性，請使用 Audit Manager 提供的 ValidateAssessmentReportIntegrity API。

疑難排解評估報告

如需尋找常見問題和問題的解答，請參閱本指南疑難排解區段中的疑難排解評估報告問題。

證據搜尋工具

證據搜尋工具提供了一種在 Audit Manager 之中搜尋證據的強大方法。您現在可以使用證據搜尋工具快速查詢證據，不須一頭栽進證據資料夾，想辦法找出您要查找的內容。如果您以委派管理員的身分使用證據搜尋工具，您可以在組織中的所有成員帳戶中搜尋證據。

使用篩選條件和群組的組合，您可以逐步縮小搜尋查詢的範圍。例如，如果您想要系統健全狀況的高階檢視，請擴大搜尋範圍，並依據評估、日期範圍和資源合規性進行篩選。如果您的目標是修復特定資源，則可以縮小搜尋範圍，以針對特定控制項或資源 ID 的證據作為目標。定義篩選條件後，您可以先分組並預覽相符的搜尋結果，然後再建立評估報告。

若要使用證據搜尋工具，您必須從 Audit Manager 設定中啟用此功能。

主題

了解證據搜尋工具如何與 CloudTrail Lake 合併使用

證據搜尋工具使用 AWS CloudTrail Lake 的查詢和儲存功能。在開始使用證據搜尋工具之前，先了解更多 CloudTrail Lake 的工作原理會很有幫助。

CloudTrail Lake 將資料彙總到單一可搜尋的事件資料存放區中，以支援功能強大的 SQL 查詢。這表示您可以在整個組織和自訂時間範圍內搜尋資料。使用證據搜尋工具，您可以直接在 Audit Manager 主控台中使用此搜尋功能。

當您要求啟用證據搜尋工具時，Audit Manager 會代表您建立事件資料存放區。啟用證據搜尋工具之後，您日後的所有 Audit Manager 證據都會擷取至事件資料存放區，以供證據搜尋工具搜尋查詢使用。啟用證據搜尋工具後，我們還會使用過去兩年的證據資料回填新建立的事件資料存放區。如果您以委派系統管理員的身分使用證據搜尋工具，我們將回填您的組織中的所有成員帳戶的資料。

您的所有證據資料(無論是回填資料還是新的)都會保留在事件資料存放區中 2 年。您可以隨時變更預設的保留期間。如需指示，請參閱 AWS CloudTrail 使用指南中的更新事件資料存放區。您可以在事件資料存放區中保留事件資料最長 7 年，即 2555 天。

> **Note**
>
> 啟用此功能後，在 2023 年 11 月之前完成的資料回填過程是免費的。
> 往後，新證據資料新增至事件資料存放區時，CloudTrail Lake 會產生資料儲存和擷取的費用。
> 對於 CloudTrail Lake 查詢，您將按使用量付費。這表示您在證據搜尋工具中進行的每次搜尋查詢，都需要支付掃描資料的費用。
> 如需 CloudTrail Lake 定價的更多資訊，請參閱 AWS CloudTrail 定價。

啟用證據搜尋工具

您可以從 Audit Manager 設定中啟用證據搜尋工具。如需指示，請參閱本指南 AWS Audit Manager 設定頁面上的證據搜尋工具。

證據搜尋工具疑難排解

若需尋找常見問題的解答，請參閱本指南疑難排解章節中的證據搜尋工具問題疑難排解。

搜尋證據

請依照下列步驟在 Audit Manager 主控台中搜尋證據。

> **Note**
>
> 您也可以使用 CloudTrail API 來查詢您的證據資料。如需更多資訊，請參閱 AWS CloudTrail API 參考中的 StartQuery。如果您偏好使用 AWS CLI，請參閱 AWS CloudTrail 使用者指南中的開始查詢。

在此頁面

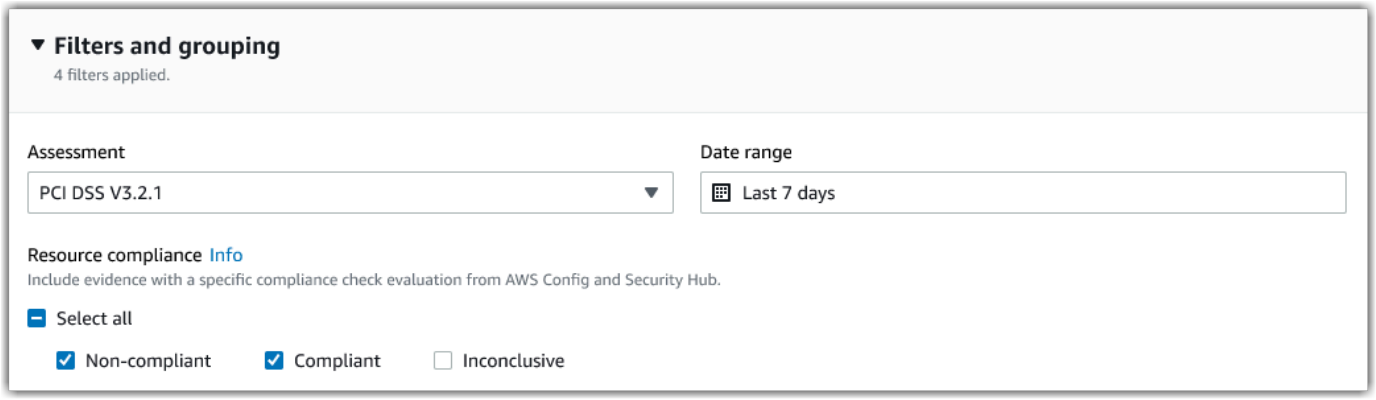
- 編輯搜尋條件

執行搜尋查詢

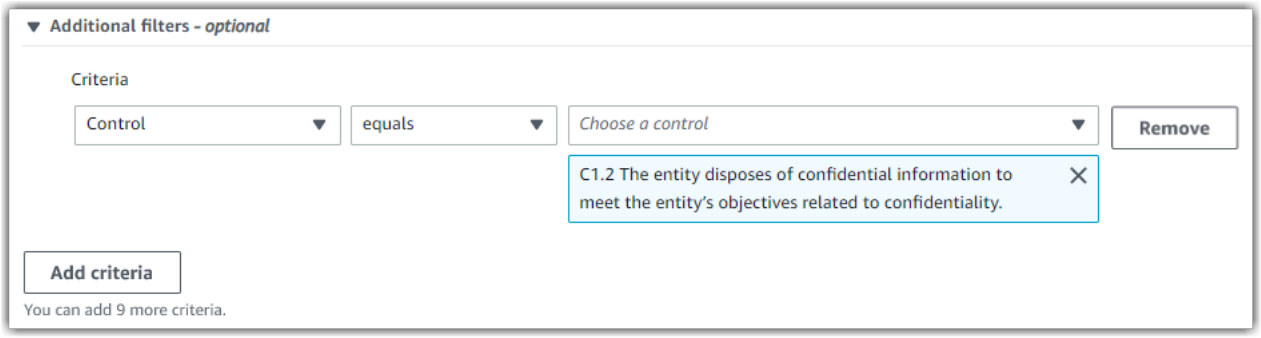
請按照以下步驟，在證據搜尋工具中執行搜尋查詢。

要搜尋證據

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在導覽窗格中，選擇證據搜尋工具。
3. 接下來，利用篩選器以縮小搜尋範圍。
   a. 在評估選擇評估。
   b. 在日期範圍選取範圍。
   c. 在資源合規性選取評估狀態。



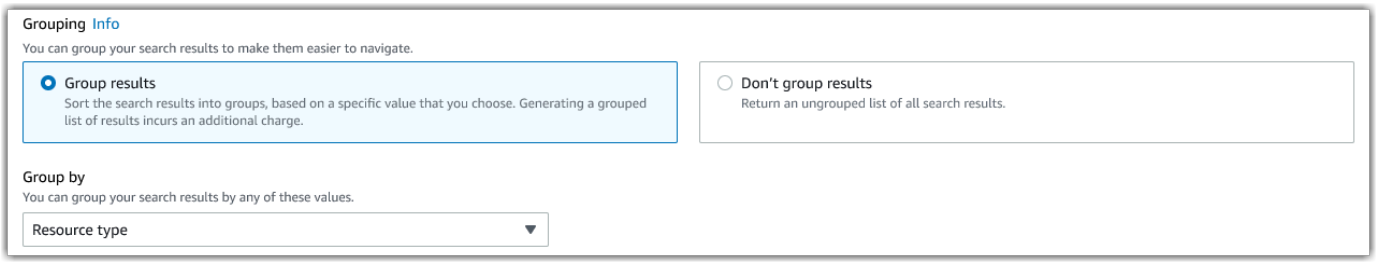
4. （選擇性）選擇 其他篩選器 - 選擇性使用 以進一步縮小搜尋範圍。
   a. 選擇新增條件，選取條件，然後為該條件選取一或多個值。
   b. 繼續以相同的方式提出更多篩選條件。
   c. 若要移除不想要的篩選器，請選擇移除



5. 在分組 底下，指定是否要將搜尋結果分組。

   a. 如果要將結果分組，請選取一個值做為分組結果的依據。

   b. 如果您不想對結果進行分組，請繼續執行步驟 6。



6. 選擇 Search (搜尋)。

您的搜尋可能需要幾分鐘的時間，視您擁有的證據資料量而定。在搜尋過程中，您可以隨時離開證據搜尋工具。當搜尋結果準備就緒時，會出現閃爍條通知您。

> **Tip**
>
> 如需有關可在此程序中使用之篩選器和群組的詳細資訊，請參閱篩選和分組選項。

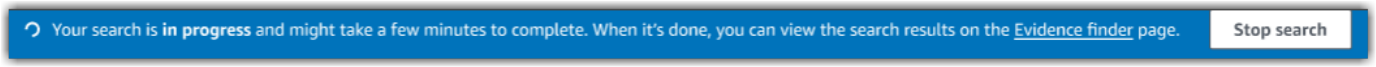
停止搜尋查詢

如果您因為任何理由而想要停止搜尋查詢，請依照下列步驟執行。

> **Note**
>
> 停止搜尋查詢仍可能會產生費用。停止搜尋查詢之前，會按已掃描的證據資料量向您收取費用。停止後，您可以檢視傳回的部分結果。

若要停止進行中的搜尋查詢

1. 在螢幕上方的藍色進度閃爍條上，選擇停止搜尋。



2. （選擇性）檢閱停止搜尋查詢之前傳回的部分結果。

   a. 如果您在證據搜尋工具頁面上，螢幕上會顯示部分結果。

   b. 如果您離開證據搜尋工具，請在綠色確認閃爍條中選擇檢視部分結果。

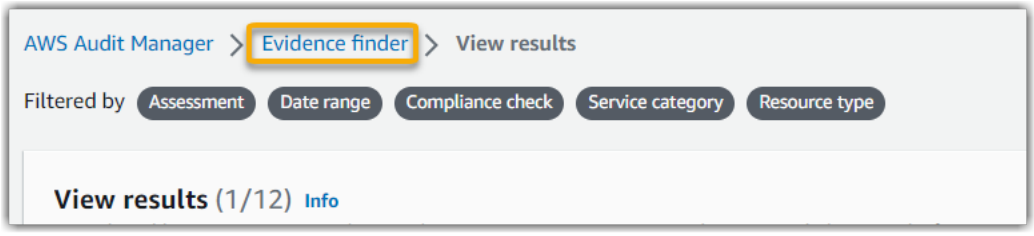
編輯搜尋條件

您可以返回最近的搜尋查詢，並視需要變更篩選條件。

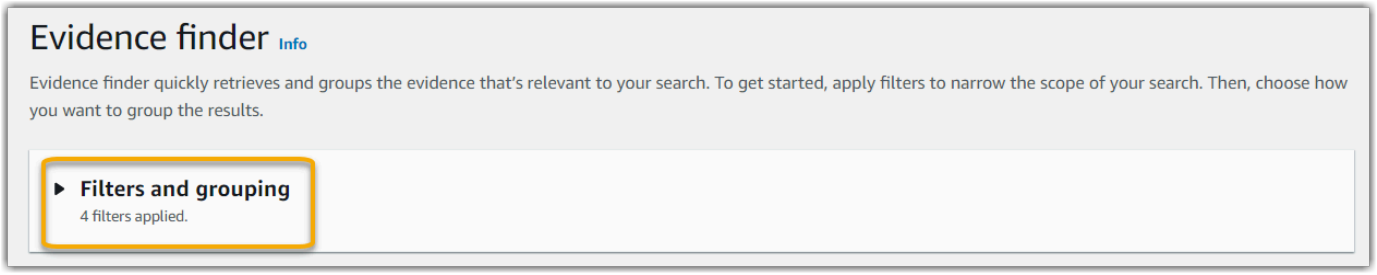
> **Note**
>
> 當您編輯篩選器並選擇搜尋時，這會啟動新的搜尋查詢。

若要編輯最近的搜尋條件

1. 在檢視結果頁面中，從頁面導覽路徑導覽選單中選取證據搜尋工具。



2. 選擇篩選條件並分組以展開篩選器選取範圍。



3. 接下來，編輯篩選器或開始新的搜尋。

   a. 若要編輯篩選器，請調整或移除目前的篩選器和分組。

   b. 要重新開始，請選擇清除篩選器，然後應用您選擇的篩選器和分組選擇。

4. 完成後，請選擇搜尋。

在證據搜尋工具中查看結果

搜尋完成後，您可以檢視符合搜尋條件的結果。

請記住，在收集證據時可能會評估多個資源。因此，證據可能包含一個或多個相關資源。在證據搜尋工具中，結果會顯示在資源層級，每個資源有一個資料列。您可以預覽每個資源的摘要，而無需離開頁面。

檢閱搜尋結果後，您可以產生包含該證據的評估報告。您也可以將搜尋結果匯出為逗號分隔值 (CSV) 檔案。

> **Important**
>
> 我們建議您將證據搜尋工具保持開啟狀態，直到您完成搜尋結果的探索為止。當您瀏覽離開檢視結果表格時，系統會捨棄您的搜尋結果。如有需要，您可以在 CloudTrail 主控台中檢視您最近的結果，網址為 https://console.aws.amazon.com/cloudtrail/。在這裡，您的搜尋查詢結果將保留七天。但請記住，您無法從 CloudTrail 主控台中的搜尋結果產生評估報告。

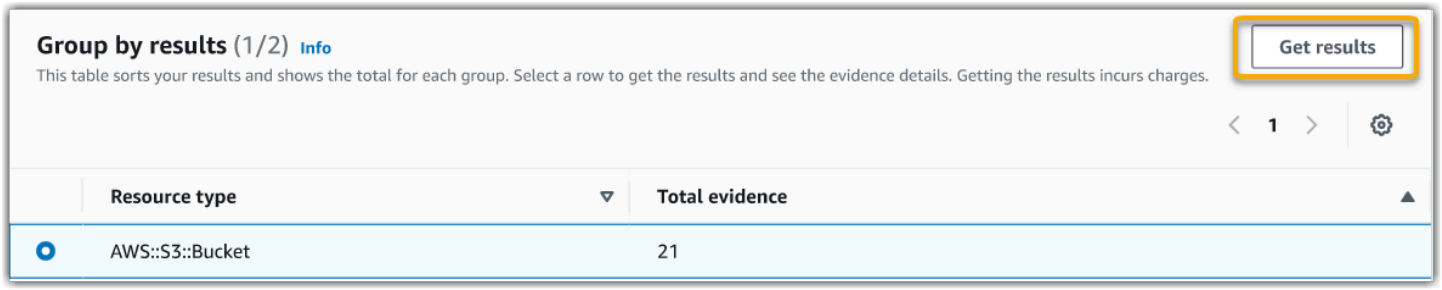
在此頁面

檢視分組結果

如果您將結果分組，則可以在深入研究證據之前查看分組。

> **Note**
>
> 如果您沒有將結果分組，證據搜尋工具不會顯示按結果分組表格。相反地，您會直接前往檢視結果表格。

您可以使用按結果分組表格，瞭解相符證據的廣度，以及它在特定維度之間的分佈方式。結果會依您選取的值分組。例如，如果您按資源類型分組，則表格會顯示 AWS 資源類型的清單。證據總計欄會顯示每個資源類型的相符結果數目。



若要取得群組的結果

1. 從按結果分組表格中，選取您要取得之結果的列。
2. 選擇取得結果。這會啟動新的搜尋查詢，並將您重新導向至檢視結果表格，您可以在其中查看該群組的結果。

檢視搜尋結果

檢視結果表格會顯示您的搜尋結果。您可以從此處執行下列動作：

- 管理您的檢視偏好設定
- 預覽資源摘要
- 從搜尋結果產生評估報告
- 匯出您的搜尋結果

管理您的檢視偏好設定

您的檢視偏好設定會控制您在結果頁面上看到的內容。

要管理您的檢視偏好設定

1. 選擇檢視結果表頂端的設定圖示 (#)。
2. 視需要檢視和變更下列設定：
   a. 選取可見表格欄 — 使用切換選項可變更要顯示的欄。
   b. 頁面大小 — 選取選項按鈕以指定每個頁面上顯示的結果數目。
   c. 自動換行 — 選取核取方塊可換行長文字，以方便閱讀。
3. 選擇確認以儲存偏好設定。

預覽資源摘要

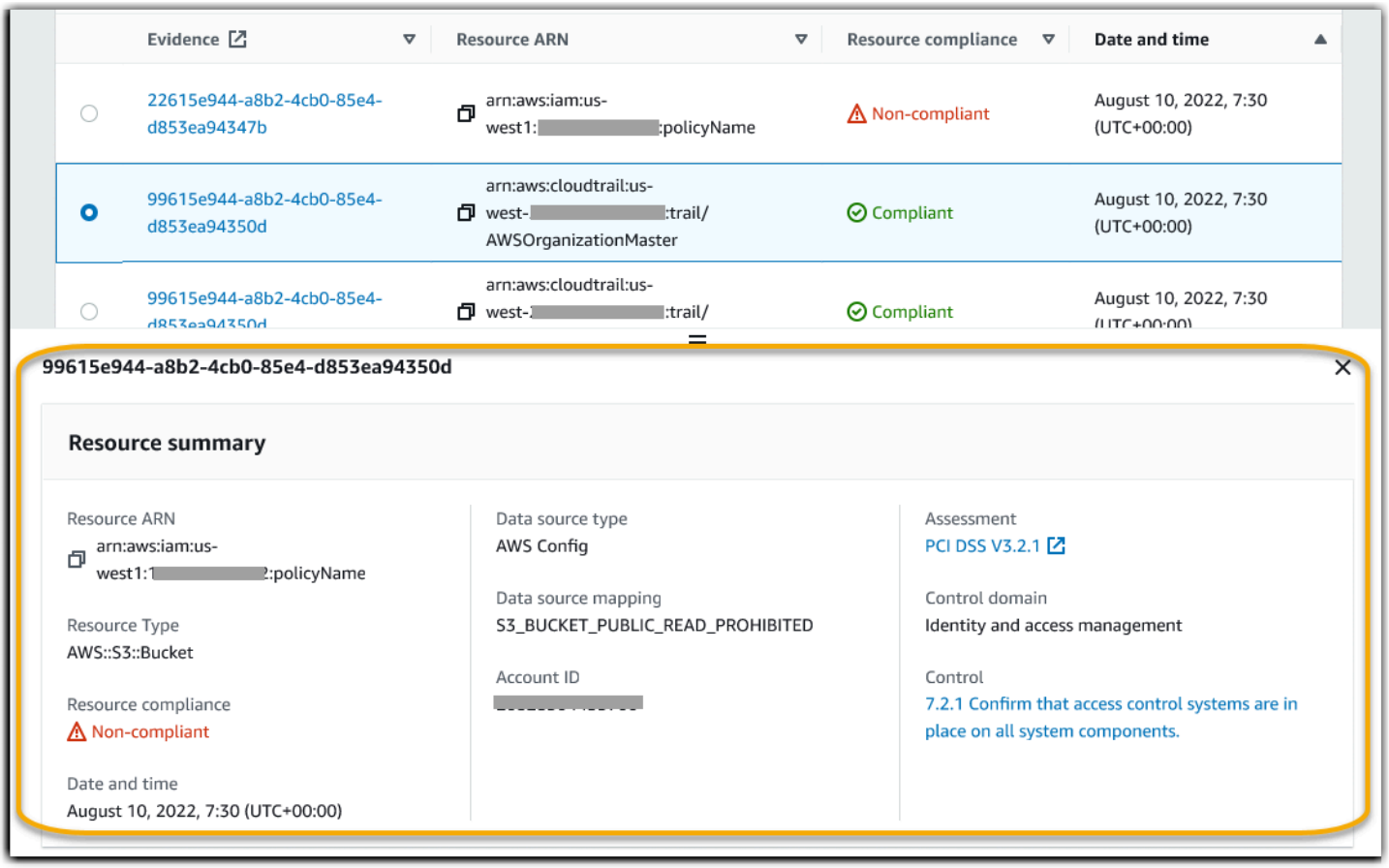
您可以預覽與搜尋查詢相符的證據的相關資源。這可協助您判斷搜尋查詢是否傳回預期的結果，或者您是否需要調整篩選條件並重新執行搜尋查詢。

請記住，證據可以有一個或多個相關資源。證據搜尋工具將在資源層級顯示結果（每個資源佔一行）。

> **Note**
>
> 證據搜尋工具會傳回自動和手動證據的結果。但是，您只能預覽自動證據的資源摘要。這是因為 Audit Manager 不會針對手動證據執行資源評估，因此沒有可用的資源摘要。
> 若要查看有關手動證據的詳細資料，請選擇證據名稱以開啟證據詳細資料頁面。如果您從證據搜尋工具結果中生成評估報告，則評估報告中包含手動證據詳細資訊。

要預覽資源摘要

1. 選取結果旁的選項按鈕。這會在目前頁面上開啟資源摘要面板。
2. （選擇性）若要查看相關證據的完整詳細資料，請選擇證據名稱。
3. （選擇性）使用水平線 (=) 拖曳資源摘要窗格並調整大小。
4. 選擇 (x) 以關閉資源摘要窗格。



從搜尋結果產生評估報告

在您對搜尋結果感到滿意后，產生評估報告。

要從搜尋結果產生評估報告

1. 在檢視結果表格頂端，選擇產生評估報告。
2. 輸入評估報告的名稱和說明，並檢閱評估報告詳細資訊。
3. 選擇產生評估報告。

您的評估報告需要幾分鐘的時間才會產生。發生這種情況時，您可以離開證據搜尋工具，等待綠色的成功通知提醒您報告已準備就緒。然後，您可以前往 Audit Manager 下載中心並下載您的評估報告。

> **Note**
>
> Audit Manager 僅使用搜尋結果中的證據來產生一次性報告。此報告不包含從評估頁面手動新增至報告的任何證據。
> 限制適用於評估報告中包含多少項證據。如需詳細資訊，請參閱搜尋工具疑難排解。

匯出您的搜尋結果

您可能需要可攜式版本的證據搜尋工具搜尋結果。在這種情況下，您可以將搜尋結果匯出為 CSV 檔案。

匯出搜尋結果後，七天內 CSV 檔案仍可在 Audit Manager 下載中心取得。CSV 檔案的副本也會傳送到您偏好的 S3 儲存貯體中，這稱為匯出目的地。您的 CSV 檔案會保留在此儲存貯體中，直到您刪除該檔案為止。

Audit Manager 使用 CloudTrail Lake功能，從證據搜尋工具匯出和發送 CSV 檔案。下列因素定義了 CSV 匯出程序的運作方式：

- 您的所有搜尋結果都包含在 CSV 檔案中。如果您只想在評估報告中包含特定的搜尋結果，建議您編輯您的搜尋篩選器。如此一來，您就可以縮小結果範圍，僅針對您要匯出的證據。
- CSV 檔案會以壓縮的 GZIP 格式匯出。預設 CSV 檔案名稱為 `queryID/result.csv.gz`，其中 `queryID` 是搜尋查詢的 ID。
- CSV 匯出的檔案大小上限為 1 TB。如果您要匯出超過 1 TB 的資料，您的結果會分割為多個檔案。每個 CSV 檔案都會命名為 `result_`*`number`*`.csv.gz`。您取得的 CSV 檔案數量取決於搜尋結果的總大小。例如，匯出 2 TB 的資料會提供兩個查詢結果檔案：`result_1.csv.gz` 和 `result_2.csv.gz`。
- 除了 CSV 檔案之外，還會將 JSON 簽署檔案傳送到您的 S3 儲存貯體。此檔案可做為總和驗證碼，以驗證 CSV 檔案中的資訊是否正確。若要深入了解，請參閱 AWS CloudTrail 開發人員指南中的 CloudTrail 簽署檔案結構。若要判斷在 CloudTrail 傳送查詢結果之後，查詢結果是否經過修改、遭到刪除或未發生變更，您可以使用 CloudTrail 查詢結果完整性驗證。如需指示，請參閱 AWS CloudTrail 開發人員指南中的驗證已儲存的查詢結果。

> **Note**
>
> 證據搜尋工具預覽或 CSV 匯出中，目前不包含手動證據文字回覆。若要檢視文字回應數據，請在證據搜尋工具結果中選擇手動證據名稱以開啟證據詳細資訊頁面。如果您需要在 Audit Manager 主控台以外檢視文字回應資料，建議您根據證據搜尋工具結果產生評估報告。所有手動證據詳細資料，包括文字回應，都包含在評估報告中。

首次匯出結果

首次匯出搜尋結果時，請依照下列步驟進行。此程序為您提供指定未來所有匯出的預設匯出目的地選項。如果您不想立即儲存預設的匯出目的地，您可以稍後透過更新匯出目的地設定來進行操作。

> **Important**
>
> 開始之前，請確定您有可用的 S3 儲存貯體作為匯出目的地。您可以使用其中一個現有的 S3 儲存貯體，也可以在 Amazon S3 中建立新儲存貯體。此外，您的 S3 儲存貯體必須擁有必要的許可政策，以允許 CloudTrail 將匯出檔案寫入該儲存貯體。具體而言，儲存貯體政策必須包含 `s3:PutObject` 動作和儲存貯體 ARN，並將 CloudTrail 列為服務主體。我們提供您可以使用的範例權限策略。關於如何將此政策附加到 S3 儲存貯體的指南，請參閱使用 Amazon S3 主控台新增儲存貯體政策。
>
> 如需更多秘訣，請參閱匯出目的地的設定提示。如果您在匯出 CSV 檔案時遇到任何問題，請參閱證據搜尋工具匯出 CSV 疑難排解。

匯出搜尋結果（首次執行體驗）

1. 在檢視結果表格頂端，選擇匯出 CSV。
2. 指定您要匯出檔案的 S3 儲存貯體。
   - 選擇瀏覽 S3 以從儲存貯體清單中選取。
   - 或者，您也可以使用以下格式輸入儲存貯體 URI：**`s3://bucketname/prefix`**

> **Tip**
>
> 為確保目的地儲存貯體有序組織，您可以為 CSV 匯出建立選用資料夾。若要這麼做，請在資源 URI 方塊中的值加上斜線 (**`/`**) 和字首 (例如，**`/evidenceFinderExports`**)。然

後，Audit Manager 會在將 CSV 檔案新增至儲存貯體時包含此字首，而 Amazon S3 會產生字首指定的路徑。如需在 Amazon S3 中首碼的詳細資訊，請參閱在Amazon 簡易儲存服務使用者指南中的在 Amazon S3 主控台編組物件。

3. （選擇性）如果您不想將此儲存貯體預設為匯出目的地，請取消選取在我的證據搜尋工具設定中，將此儲存貯體預設為匯出目的地的核取方塊。
4. 選擇 Export (匯出)。

儲存匯出目的地後，匯出結果

將預設 S3 儲存貯體儲存為匯出目的地後，您可以繼續執行下列步驟。

匯出搜尋結果(儲存預設匯出目的地後)

1. 在檢視結果表格頂端，選擇匯出 CSV。
2. 在出現的提示中，檢閱將儲存匯出檔案的預設 S3 儲存貯體。
   a. （選擇性）若要繼續使用此儲存貯體並隱藏此訊息，請勾選 不要再提醒我 方塊。
   b. （選擇性）若要變更儲存貯體，請依照程序更新匯出目的地設定。
3. 選擇 Confirm (確認)。

視您要匯出的資料量而定，匯出程序可能需要幾分鐘的時間才能完成。您可以在匯出過程中離開證據搜尋工具。當您離開證據搜尋工具時，您的搜尋作業將停止，搜尋結果也會自主控台移除。不過，CSV 匯出程序會在背景中繼續執行。CSV 檔案將包含符合您查詢的完整搜尋結果集。

匯出結果後檢視結果

若要尋找您的 CSV 檔案並檢查其狀態，請前往 Audit Manager 下載中心。匯出的檔案準備就緒後，您可以從下載中心下載 CSV 檔案。

您也可以在匯出目的地 S3 儲存貯體中找到，並下載 CSV 檔案。

在 Amazon S3 主控台中尋找 CSV 檔案和簽署檔案

1. 開啟 Amazon S3 主控台。
2. 選擇您在匯出 CSV 檔案時，指定的匯出目的地儲存貯體。
3. 瀏覽物件階層，直到找出 CSV 檔案和簽署檔案。CSV 檔案的副檔名為 `.csv.gz`，而簽署檔案的副檔名為 `.json`。

您將瀏覽與下列範例類似的物件階層，但使用不同的匯出目的地儲存貯體名稱、帳戶 ID、日期和查詢 ID。

```
All Buckets
    Export_Destination_Bucket_Name
        AWSLogs
            Account_ID;
                CloudTrail-Lake
                    Query
                        YYYY
                            MM
                              DD
                                Query_ID
```

篩選和分組選項

本頁說明證據搜尋工具中可用的篩選器和分組選項。

在此頁面

篩選器參考資料

您可以使用下列篩選器來尋找符合特定條件的證據，例如評估、控制或 AWS 服務。

主題

必要篩選器

使用這些篩選條件，開始對評估中的證據進行高階概觀。

篩選器名稱	描述	備註
評估	傳回特定評估的證據。	您只能依據一個評估進行篩選。
日期範圍	傳回特定時段的證據。	或者，您可以使用相對範圍來定義相對於今天日期的範圍（例如，**`Last 30 days`**）。 或者，您可以使用絕對範圍來指定特定的日期範圍 (例如，**`June 27th - July 4th`**)。
支援合規	傳回具有特定合規檢查評估的資源。	Audit Manager 會針對使用 AWS Config 和 Security Hub 作為資料來源類型的控制項，收集合規檢查證據。請記住，在收集證據時可能會評估多種資源。因此，單一合規檢查證據可以包含一或多個資源。您可以使用此篩選器來探索資源層級的合規狀態。 您可以選擇以下其中一個選項： • 不合規 — 此篩選器會尋找具有合規檢查問題的資源。如果安全中樞回報失敗結果，或 AWS Config 回報不合規結果，就會發生這種情況。 • 合規 — 此篩選器會尋找不具有合規檢查問題的資源。如果安全中樞回報通過結果，或 AWS Config 回報合規結果，就會發生這種情況。 • 不確定 — 此篩選器會尋找合規檢查不可用或不適用的資源。如果資源使用 AWS Config 或安全中樞做為基礎資料來源類型，但這些服務未啟用，就會發生這種情況。如果資源使用不支援合規檢查的基礎資料來源類型 (例如手動證據、AWS API 呼叫或 CloudTrail)，也會發生這種情況。

其他篩選條件（選擇性）

使用這些篩選條件來縮小搜尋查詢的範圍。例如，使用服務查看與 Amazon S3 相關的所有證據。使用資源類型將範圍縮小至 S3 儲存貯體。或者，使用資源 ARN 以特定 S3 儲存貯體為目標。

您可以使用下列一或多個條件建立其他篩選器。

條件名稱	描述	何時使用此條件
帳戶 ID	依 AWS 帳戶 進行深層探勘。	使用此條件來尋找與特定 AWS 帳戶 相關的證據。
控制項	依控制項名稱進行深層探勘。	使用此條件來尋找與特定控制項相關的證據。
控制項域	依控制項網域進行深層探勘。	當您準備稽核時，請使用此條件，將重點放在特定主題領域。如果您要查詢從標準架構建立的評估，則可以依控制項網域進行篩選。 控制項網域的範例包括身分識別與存取管理、記錄與監控，以及網路管理。
Data source type (資料來源類型)	依資料來源的類型進行深層探勘。	使用此條件可將結果限縮於特定資料來源。 將值設定為`Manual`，以尋找您手動上傳的證據。或者，您可以根據自動證據的來源（例如`AWS Config`、`CloudTrail` 、`Security Hub` 或 `AWS API calls`）過濾自動證據。
事件名稱	依事件名稱進行深層探勘。	使用此條件可將重點放在與證據相關的特定事件上。事件是 AWS 帳戶 中活動的記錄。 例如，您可以搜尋 API 呼叫的名稱，例如用於設定權限的 IAM `AttachRolePolicy` 作業。或者也搜尋 CloudTrail 關鍵字，例如 CloudTrail 在使用者登入您帳戶時記錄的 `ConsoleLogin` 事件。
資源 ARN	按 Amazon Resource Name (ARN)進行深層探勘。	使用此條件來尋找與特定 AWS 資源相關的證據。
Resource Type (資源類型)	依資源類型進行深層探勘。	使用此條件專注於正在評估的資源類型，例如 Amazon EC2 執行個體或 S3 儲存貯體。

條件名稱	描述	何時使用此條件
服務	按 AWS 服務 名稱進行深層探勘。	使用此條件尋找與 AWS 服務 特定相關的證據，例如 Amazon EC2、Amazon S3 或 AWS Config。
服務目錄	按 AWS 服務 類別進行深層探勘。	使用此條件可將結果限縮於特定類別的 AWS 服務。 範例包括安全性、身分識別與合規性、資料庫和存放區。

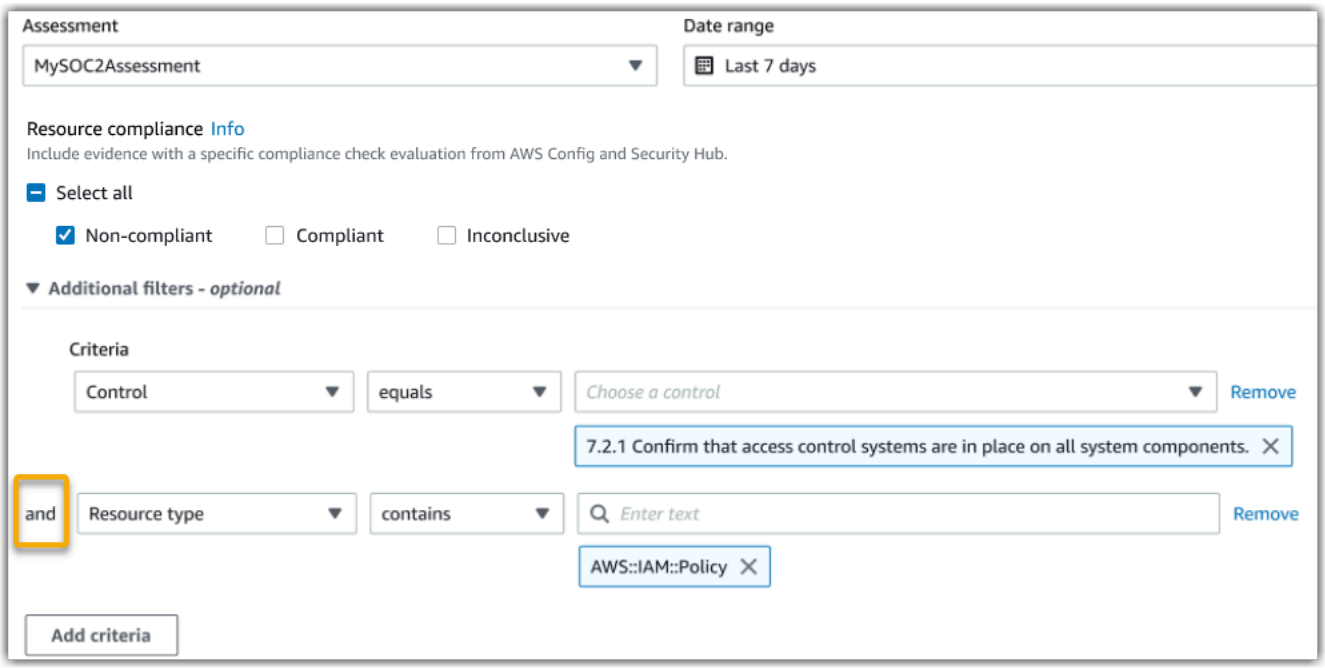
結合篩選器

條件行為

當您指定多個條件時，Audit Manager 會將 AND 運算子套用到您的選定內容。這表示所有條件都會分組為單一查詢，且結果必須符合所有組合的條件。

範例

在下列篩選器設定中，證據搜尋工具會針對呼叫 **`MySOC2Assessment`** 的評估，傳回過去 7 天內不合規的資源。此外，結果與 IAM 政策和指定控制項有關。

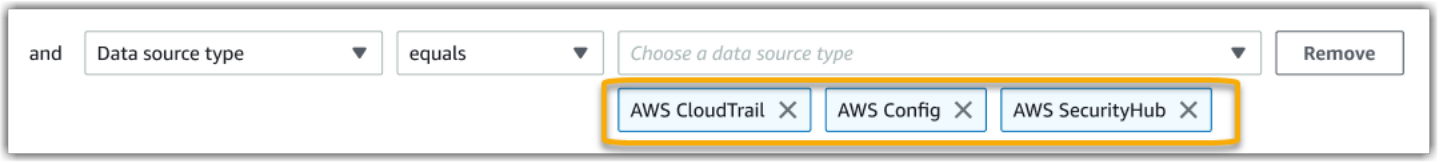


條件值行為

當您指定多個條件值時，這些值會與 OR 運算子連結。證據搜尋工具會傳回符合任何這些條件值的結果。

範例

在下列篩選器設定中，證據搜尋工具會傳回來自AWS CloudTrail、AWS Config、或 AWS Security Hub 的搜尋結果。



分組參考

您可以將搜尋結果分組，以加快瀏覽速度。分組顯示搜尋結果的廣度，以及它們在特定維度中的分佈方式。

您可以使用以下任一分組的數值。

分組依據	描述
帳戶 ID	依據 AWS 帳戶 分組結果。
控制項	依控制項名稱分組結果。
控制項域	依控制域名稱分組結果。
Data source type (資料來源類型)	依證據來源的資料來源類型分組結果。
事件名稱	依事件名稱分組結果。
資源 ARN	依 Amazon Resource Name (ARN) 分組結果。
Resource Type (資源類型)	依資源類型分組結果。
服務	依 AWS 服務 名稱分組結果。
服務目錄	按 AWS 服務 類別分組結果。

範例使用案例

證據搜尋工具可以幫助您處理多種使用範例。此頁面提供了一些範例，並建議您可以在每個案例中使用的搜尋篩選器。

主題

使用案例 1：尋找不合規的證據並進行委派

如果您是合規官、資料保護官或監督稽核準備工作的 GRC 專業人員，則此使用案例非常理想。

當您監管組織的合規性狀況時，您可能會仰賴合作夥伴團隊來協助您修復問題。您可以使用證據搜尋工具來幫助您為合作夥伴團隊組織工作。

透過應用篩選器，您可以一次專注於一個區域的證據。此外，您還可以與您合作的每個合作夥伴團隊的責任和範圍保持一致。透過這種方式執行目標搜尋，您可以使用搜尋結果來分辨每個主題領域，瞭解實際需要補救的內容。然後，您可以將不合規的證據委託給對應的合作夥伴團隊進行補救。

對於此工作流程，請按照步驟搜尋證據。使用下列篩選器尋找不合規的證據。

```
Assessment | <assessment name>
Date range | <date range>
Resource compliance | Non-compliant
```

接下來，為您要關注的區域應用其他篩選器。例如，使用服務類別篩選器尋找與 IAM 相關的不合規資源。然後，與擁有組織 IAM 資源的團隊共用這些結果。或者，如果您要查詢從標準架構建立的評估，您可以使用控制項網域篩選器來尋找與身分識別和存取管理網域相關的不合規證據。

```
Control domain | <domain that you're focusing on>
or
Service category | <AWS ## category that you're focusing on>
```

找到所需證據後，請依照下列步驟從搜尋結果產生評估報告。您可以與合作夥伴團隊共享此報告，他們可以將其用作補救檢查清單。

使用案例 2：找出合規證據

如果您是擔任 SecOps、IT/DevOps 或其他擁有和修復雲端資產的職務，則此使用案例非常理想。

作為稽核的一部分，系統可能會要求您修正您擁有的資源的問題。完成這項工作之後，您可以使用證據搜尋工具來驗證您的資源是否合規。

對於此工作流程，請按照步驟搜尋證據。使用下列篩選器尋找合規的證據。

```
Assessment | <assessment name>
Date range | <date range>
Resource compliance | Compliant
```

接下來，應用其他篩選器以縮小範圍至僅剩下您負責的證據。視您的擁有權範圍而定，視需要進行目標搜尋。下列篩選範例是從最廣到最精確的順序排列。選擇適合您的選項，並以您自己的值取代*<#####>*。

```
Control domain | <a subject area that you're responsible for>
Service category | <a category of AWS ## that you own>
Service | <a specific AWS ## that you own>
Resource type | <a collection of resources that you own>
Resource ARN | <a specific resource that you own>
```

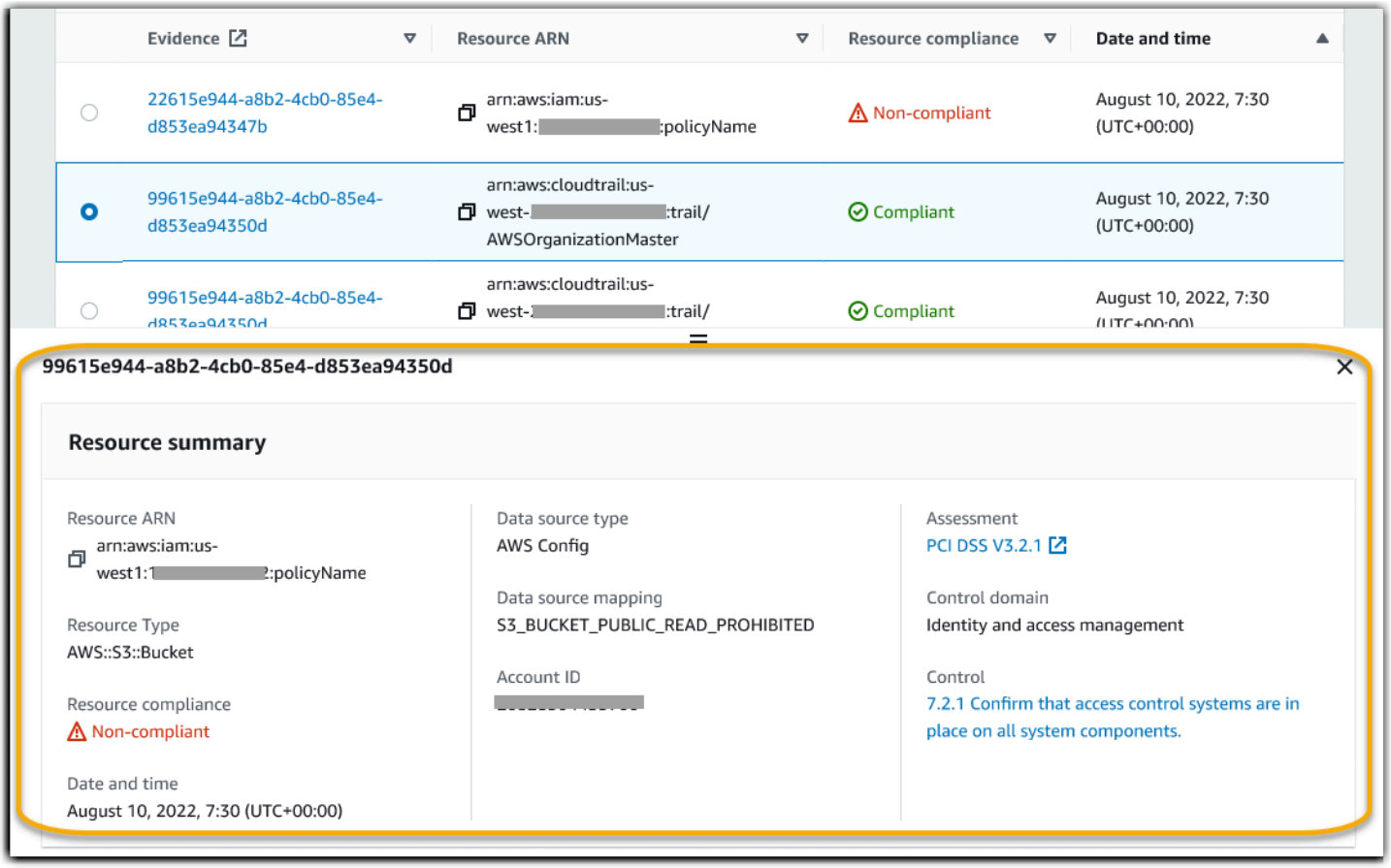
如果您負責相同條件的多個實例（例如，您擁有多個AWS 服務），則可以按該值對結果進行分組。這項行動將為您提供與每個 AWS 服務 證據相符的總證據。然後，您可以取得您擁有之服務的結果。

使用案例 3：執行證據資源的快速預覽

此使用案例適合所有 Audit Manager 客戶。

以前，檢閱個別證據詳細資料非常耗時。如果您想要預覽證據，您必須直接前往該評估，然後瀏覽深層巢狀的證據資料夾。現在，證據搜尋工具提供了一種預覽此資訊的便捷方法。對於符合搜尋查詢的每個證據項目，您可以預覽該證據的個別資源。

若要開始使用，請按照步驟搜尋證據。接著，選取結果旁的選項按鈕以檢視目前頁面中的資源摘要。您可以預覽與證據項目相關的每個個別資源。若要查看任何資源的完整證據詳細資料，請選擇證據名稱。如需更多資訊，請參閱預覽資源摘要。


Evidence
Resource ARN
Resource compliance
Date and time
22615e944-a8b2-4cb0-85e4-d853ea94347b
arn:aws:iam:us-west1:[redacted]:policyName
Non-compliant
August 10, 2022, 7:30 (UTC+00:00)
99615e944-a8b2-4cb0-85e4-d853ea94350d
arn:aws:cloudtrail:us-west-[redacted]:trail/AWSOrganizationMaster
Compliant
August 10, 2022, 7:30 (UTC+00:00)
99615e944-a8b2-4cb0-85e4-d853ea94350d
arn:aws:cloudtrail:us-west-[redacted]:trail/
Compliant
August 10, 2022, 7:30
99615e944-a8b2-4cb0-85e4-d853ea94350d
Resource summary
Resource ARN
arn:aws:iam:us-west1:[redacted]:policyName
Resource Type
AWS::S3::Bucket
Resource compliance
Non-compliant
Date and time
August 10, 2022, 7:30 (UTC+00:00)
Data source type
AWS Config
Data source mapping
S3_BUCKET_PUBLIC_READ_PROHIBITED
Account ID
[redacted]
Assessment
PCI DSS V3.2.1
Control domain
Identity and access management
Control
7.2.1 Confirm that access control systems are in place on all system components.

Audit Manager 下載中心

您可以在下載中心找到並管理所有可下載的 Audit Manager 檔案。當您產生評估報告或匯出證據搜尋工具的搜尋結果時，檔案會出現在下載中心中。

主題

瀏覽下載中心

如需訪問下載中心，請在 https://console.aws.amazon.com/auditmanager/home 開啟 Audit Manager 主控台，然後選擇左側導覽窗格中下載中心。

您可以在下列索引標籤之間切換，依類別瀏覽檔案。

評估報告索引標籤

此索引標籤會顯示您產生的所有評估報告。在您刪除評估報告之前，您可在下載中心獲取評估報告。

如需查看評估報告的最新狀態，請選擇重新整理圖示 (#) 以重新載入表格。評估報告表格中的每一列都會顯示報告的名稱、建立日期，以及下列其中一種狀態：

- 進行中 — Audit Manager 正在產生評估報告。
- 就緒 — 評估報告可供您下載。
- 錯誤 — 評估報告無法產生 在此情況下，Audit Manager 會顯示描述錯誤的訊息。如需如何解決這些錯誤的相關資訊，請參閱疑難排解評估報告。

匯出索引標籤

此索引標籤會顯示您過去七天內匯出的所有證據搜尋工具的搜尋結果。CSV 檔案會在七天後從下載中心中移除，但仍可在匯出目的地 S3 儲存貯體中使用。如需有關如何在 S3 目的地儲存貯體中尋找證據搜尋工具 CSV 匯出的說明，請參閱 匯出結果後檢視結果。

如需查看 CSV 報告的最新狀態，請選擇重新整理圖示 (#) 以重新載入表格。匯出表格中的每一列都會顯示檔案名稱、匯出日期以及下列其中一種狀態：

- 進行中 — Audit Manager 正在準備 CSV 檔案。
- 就緒 — 匯出成功，檔案可供您下載。
- 錯誤 — 匯出失敗。在此情況下，Audit Manager 會顯示描述錯誤的訊息。如需有關如何解決這些錯誤的詳細資訊，請參閱疑難排解證據搜尋工具 CSV 匯出問題。

> **Note**
>
> 請謹記，匯出索引標籤也可能會顯示您直接在 AWS CloudTrail Lake 中執行查詢的 CSV 檔案。這包括在 CloudTrail 主控台或使用 CloudTrail API 進行的查詢。如果您查詢 Audit Manager 事件資料存放區，且您選擇將結果儲存到 Amazon S3，CloudTrail 匯出會顯示在此索引標籤上。

正在下載檔案

請依照下列步驟從下載中心中下載檔案。

如需下載檔案

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在左側導覽窗格中，選擇下載中心。
3. 選擇評估報告索引標籤或匯出索引標籤。
4. 選擇您要下載的檔案，然後選擇下載。

如需有關如何從 S3 目的地儲存貯體下載檔案的說明，請參閱 Amazon Simple Storage Service (Amazon S3) 使用者指南中的下載物件。

刪除檔案

請依照下列步驟刪除下載中心中不再需要的任何評估報告。

> **Note**
>
> 目前不支援從下載中心刪除 CSV。CSV 匯出會在七天後自動從下載中心中移除。

刪除評估報告

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在左側導覽窗格中，選擇下載中心。
3. 選擇評估報告索引標籤。
4. 選擇您要刪除的評估報告，然後選擇刪除。

如果您想要從 S3 目的地儲存貯體刪除評估報告或 CSV 匯出，建議您直接在 Amazon S3 中完成此任務。如需指示，請參閱 Amazon Simple Storage Service (Amazon S3) 使用者指南中的刪除 Amazon S3 物件。

架構程式庫

您可以透過 AWS Audit Manager 中的架構程式庫存取和管理架構。

架構決定哪些控制項會在一段時間內在某個環境中測試。它會針對指定的合規性標準或法規，定義控制項及其資料來源的映射項目。它也可用來建構和自動化 Audit Manager 評估。您可以使用架構作為起點，審核您的 AWS 服務 使用情況，並開始自動化證據收集。

架構程式庫包含標準和自訂架構的目錄。

- 標準架構是由 AWS 提供之預先定義的架構。這些架構是以 AWS 最佳實務為基礎，針對不同合規性標準和法規所研擬。其中包括 GDPR 和 HIPAA。標準架構包括根據架構支援的合規標準或法規，組織到控制集中的控制項。

  您可以檢視標準架構的內容，但無法編輯或刪除它們。不過，您可以自訂任何標準架構，以建立符合特定需求的新架構。
- 自訂架構是您擁有的自訂架構。您可以可以從頭開始建立自訂架構，也可以自訂現有架構。您可以使用自訂架構，以符合特定需求的方式將控制項組織到控制集中。如需深入瞭解如何管理控制項，請參閱控制項程式庫。

您可以從標準架構或自訂架構建立評估。若要進一步了解如何建立和管理評估，請參閱 AWS Audit Manager 中的評估。

> **Note**
>
> AWS Audit Manager 協助收集與驗證符合特定合規標準和法規相關的證據。不過，這不會評估您的合規狀態。因此，透過 AWS Audit Manager 收集的證據可能不包含稽核所需的所有有關使用 AWS 情況的資訊。 AWS Audit Manager 不是法律顧問或合規專家的替代方案。

本節說明如何在 Audit Manager 中建立和管理自訂架構。

主題

- 存取 AWS Audit Manager 中的可用架構
- 檢視架構的詳細資訊
- 建立自訂架構

- 編輯自訂架構
- 刪除自訂架構
- 共享自訂架構
- AWS Audit Manager 中的支援的架構

存取 AWS Audit Manager 中的可用架構

您可以在 Audit Manager 主控台的架構程式庫頁面，檢視所有可用的架構。您也可以從這裡自架構建立評估、建立自訂架構或自訂現有架構。

您也可以使用 Audit Manager API 或 AWS Command Line Interface (AWS CLI) 來檢視所有可用的架構。

Audit Manager console

檢視可用架構 (主控台)

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在左側導覽窗格中，選擇架構程式庫。
3. 選擇標準架構索引標籤或自訂架構索引標籤，瀏覽可用的標準和自訂架構。
4. 選擇任何架構名稱來檢視架構的詳細資訊。

AWS CLI

檢視可用架構 (AWS CLI)

若要檢視 Audit Manager 中的架構，請使用list-assessment-frameworks指令並指定一個 `--framework-type`。或者，您可以擷取標準架構的清單。或者，您也可以擷取自訂架構的清單。

```
aws auditmanager list-assessment-frameworks --framework-type Standard
```

```
aws auditmanager list-assessment-frameworks --framework-type Custom
```

Audit Manager API

檢視可用架構 (API)

使用ListAssessmentFrameworks操作並指定一個frameworkType。或者，您可以傳回標準架構的清單。或者，您也可以傳回自訂架構的清單。

有關詳細資訊，請選擇先前的任一連結，在 AWS Audit Manager API 參考資料中閱讀更多資訊。這包括有關如何在其中一項特定語言 AWS 軟體開發套件中使用 `ListAssessmentFrameworks` 操作和參數的資訊。

檢視架構的詳細資訊

您可以使用 Audit Manager 主控台、Audit Manager API 或 AWS Command Line Interface (AWS CLI) 來檢閱架構的詳細資料。

Audit Manager console

要查看架構詳細資訊 (控制台)

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在左側導覽窗格中，選擇架構程式庫以查看可用架構的清單。
3. 選擇標準架構索引標籤或自訂架構索引標籤，瀏覽可用的架構。
4. 選擇架構名稱以開啟。

當您開啟架構時，會顯示架構詳細資料頁面。本頁面的各個章節及其內容說明如下。

架構詳細資訊章節

本節說明架構的概觀。其包含下列資訊：

- 架構名稱 — 架構的名稱。
- 合規類型 — 架構支援的合規標準或法規。
- 說明 — 架構的描述 (如有的話)。
- 架構類型 — 表示架構是標準架構還是自訂架構。
- 控制集 — 與架構相關聯的控制集數目。
- 控制項 — 架構中控制項的總數。
- 控制項來源 —Audit Manager 從中收集證據的控制項資料來源數目。
- 標籤 — 與架構相關聯的標籤。

如果您正在檢視自訂架構，也會顯示下列詳細資料：

- 建立者 — 建立自訂架構的帳戶。
- 建立日期 — 建立自訂架構的日期。
- 上次更新 — 上次編輯此架構的日期。

控制項索引標籤

此索引標籤會列出架構中的控制項，並依控制集分組。其包含下列資訊：

- 依控制集分組的控制項 — 選擇樹狀檢視圖示，查看屬於每個控制集的控制項。
- 類型 — 指定控制項是標準控制項還是自訂控制項。
- 資料來源 — 指定 Audit Manager 為該控制項收集證據的資料來源。

標籤索引標籤

這個索引標籤會列出與架構相關聯的標籤。其包含下列資訊：

- 金鑰 — 標籤索引鍵 (例如合規性標準、法規或類別)。
- 值 — 標籤值。

AWS CLI

若要檢視架構詳細資訊 (AWS CLI)

1. 若要找出您要檢閱的架構，請執行list-assessment-frameworks指令並指定`--framework-type`。或者，您可以擷取標準架構的清單。或者，您也可以擷取自訂架構的清單。

   在下列範例中，將`######`取代為`Custom`或`Standard`。

   ```
   aws auditmanager list-assessment-frameworks --framework-type Custom/Standard
   ```

   回應返回架構列表。找到您要檢閱的架構，並記下架構 ID 和 Amazon Resource Name (ARN)。
2. 若要取得架構詳細資訊，請執行get-assessment-framework指令，並指定 `--framework-id`。

   在下列範例中，將`######`取代為您自己的資訊。

   ```
   aws auditmanager get-assessment-framework --framework-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

架構詳細資訊會以 JSON 格式傳回。如需瞭解此資料，請參閱AWS CLI指令參考中的取得架構輸出。

3. 若要查看架構的標籤，請使用列出資源標籤命令，並指定架構的--resource-arn。

   在下列範例中，將######取代為您自己的資訊：

   ```
   aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:assessmentFramework/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

   如需有關 Audit Manager 中標籤的詳細資訊，請參閱標籤 AWS Audit Manager 資源。

Audit Manager API

如需檢視架構詳細資訊 (API)

1. 若要識別您要檢閱的架構，請使用ListAssessmentFrameworks操作，並指定frameworkType。或者，您可以傳回標準架構的清單。或者，您也可以傳回自訂架構的清單。

   在回應中找到您要檢閱的架構，並記下架構 ID 和 Amazon Resource Name (ARN)。

2. 若要取得控制項詳細資訊，請使用取得架構操作。在要求中，指定您從步驟 1 取得的架構 ID。

   架構詳細資訊會以 JSON 格式傳回。如需了解這項資料，請參閱 AWS Audit ManagerAPI 參考資料中的 取得架構回應元素。

3. 若要查看架構的標籤，請使用列出資源標籤索引操作。在請求中，指定從步驟 1 獲得的架構 resourceArn。

如需有關 Audit Manager 中標籤的詳細資訊，請參閱標籤 AWS Audit Manager 資源。

有關此 API 操作的更多資訊，請選擇先前的任一連結，在 AWS Audit ManagerAPI 參考資料中閱讀更多資訊。這包括有關如何在其中一項特定語言 AWS 軟體開發套件中使用這些操作和參數的資訊。

建立自訂架構

您可以透過 AWS Audit Manager 中的架構程式庫存取和管理架構。您可以建立自訂架構，以符合特定需求的方式將控制項組織到控制集中。

有兩種方法可以建立自訂架構。您可以自訂現有架構，也可以從頭開始建立新架構。

主題

從頭建立新的自訂架構

您可以使用 AWS Audit Manager 中的自訂架構，以符合特定需求的方式將控制項組織到控制集中。您可以按照以下步驟在架構程式庫中從頭開始建立新的自訂架構。

主題

步驟 1：指定架構詳細資訊

首先指定要在自訂架構中包含的控制項。

指定架構詳細資訊

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在左側導覽窗格中，選擇架構資料庫，然後選擇建立自訂架構。
3. 在架構詳細資訊下，輸入名稱，合規標準或法規 (選用) 以及架構的描述 (也可選用)。輸入合規標準或法規關鍵字，例如 PCI_DSS 或 GDPR，以便使用此關鍵字搜尋您的架構。
4. 在標籤下，選擇新增標籤，將標籤與架構產生關聯。您可以指定每一個標籤的金鑰和值。標籤索引鍵是必要的。在架構程式庫中搜尋此架構時，您可以將其當成搜尋條件。如需 AWS Audit Manager 中標籤的詳細資訊，請參閱標記 AWS Audit Manager 資源。
5. 選擇下一步。

步驟 2：指定控制集中的控制項

接下來，您可以指定要新增至架構的控制項，以及要如何組織這些控制項。首先將控制集新增至架構，然後將控制項新增至控制集。

> **Note**
>
> 當您使用AWS Audit Manager主控台建立自訂架構時，最多可以為單一架構新增 10 個控制集。
> 使用 Audit Manager API 建立自訂架構時，您可以建立 10 個以上的控制集。若要新增超過主控台目前允許的控制集，請使用 Audit Manager 提供的CreateAssessmentFramework API。

指定控制集中的控制項

1. 在控制集名稱下，輸入控制集的名稱。
2. 在新增控制項至控制項集下的選取控制項類型下，使用下拉式清單選取兩種控制項類型之一：標準控制項或自訂控制項。標準控制項由 Audit Manager 提供，而自訂控制項則是您建立的控制項。
3. 根據您在上一個步驟中選取的選項，會顯示標準控制項或自訂控制項的清單。您可以瀏覽清單，或輸入控制項名稱、合規狀態或標籤來進行搜尋。選取一或多個控制項，然後選擇新增以將控制項集新增至控制集。
4. 在出現的快顯視窗中，選擇新增以確認新增控制項集。
5. 在審核控制項集中選取的控制項底下，審核選取的控制項清單中顯示的控制項。若要將更多控制項新增至控制集，請重複步驟 2 至 4。您可以選取一或多個控制項，然後選擇移除控制項，從控制集移除不想要的控制項。
6. 若要新增控制項集至架構，請選擇頁面底部的新增控制項集。您可以選擇移除控制集來移除不需要的控制集。
7. 完成新增控制項集和控制項之後，請選擇下一步。

步驟 3：檢閱及建立架構

檢閱架構的資訊。如需變更步驟的資訊，請選擇編輯。

完成時，請選擇建立自訂架構。

我接下來要怎麼做？

建立新的自訂架構之後，您可以從架定義立評估。如需更多詳細資訊，請參閱 建立評估。

您也可以使用現有架定義立自訂架構。如需更多詳細資訊，請參閱 自訂現有架構。

如需如何編輯自訂架構的說明，請參閱編輯自訂架構。

自訂現有架構

您可以使用 AWS Audit Manager 中的自訂架構，以符合特定需求的方式將控制項組織到控制集中。除了從頭開始建立自訂架構，您可以使用現有的架構做為起點，並根據您的需求進行自訂。當您執行此操作時，現有的架構會保留在架構程式庫中，而且會使用您的自訂設定建立新的自訂架構。

您可以選擇要自訂的任何現有控制項。它可以是標準架構或自訂架構。

在架構程式庫中，從建立自訂架構下拉式清單中選擇自訂現有架構。使用下列步驟自訂架構。

主題

步驟 1：指定架構詳細資訊

除標籤外，所有架構詳細資訊都是從原始架構繼承的。視需要檢閱和修改這些詳細資訊。

指定架構詳細資訊

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在左側導覽窗格中，選擇架構程式庫。
3. 選擇您要自訂的架構，然後從建立自訂架構下拉式清單中選擇自訂現有架構。
4. 在出現的快顯視窗中，輸入新自訂架構的名稱，然後選擇自訂。
5. 在架構詳細資料下，檢閱架構的名稱、合規性類型和說明，並視需要修改。合規類型應指出合規標準，或與您架構相關聯的法規。您可以使用此關鍵字來搜索架構。

6. 在標籤下，選擇新增標籤，將標籤與架構產生關聯。您可以指定每一個標籤的金鑰和值。標籤索引鍵是必要的，當您在架構程式庫中搜尋此架構時，可用來做為搜尋條件。如需 AWS Audit Manager 中標籤的詳細資訊，請參閱標記 AWS Audit Manager 資源。
7. 選擇下一步。

步驟 2：指定控制項新增至控制集

控制集是從原始架構結轉的。視需要新增更多控制項或移除現有控制項，以自訂目前的組態。

> **Note**
>
> 當您使用AWS Audit Manager主控台建立自訂架構時，最多可以為每一個架構新增 10 個控制集。
>
> 使用 Audit Manager API 建立自訂架構時，您可以新增 10 個以上的控制集。若要新增超過主控台目前允許的控制集，請使用 Audit Manager 提供的CreateAssessmentFramework API。

指定控制集中的控制項

1. 在控制組名稱下，視需要自訂控制集的名稱。
2. 在新增控制項至控制項集底下，使用下拉式清單選取兩種控制項類型之一來新增控制項：標準控制項或自訂控制項。
3. 根據您在上一個步驟中選取的選項，會顯示標準控制項或自訂控制項的清單。您可以瀏覽清單，或輸入控制項名稱、合規狀態或標籤來定位您想要新增的控制項。選取一或多個控制項，然後選擇新增以新增至控制集，以新增至此控制集。
4. 在出現的快顯視窗中，選擇新增以確認新增控制項集。
5. 在審核控制項集中選取的控制項底下，審核選取的控制項清單中顯示的控制項。若要將更多控制項新增至控制集，請重複步驟 2 至 4。您可以選取一或多個控制項，然後選擇移除控制項，從控制集移除不想要的控制項。
6. 若要新增控制項集至架構，請選擇頁面底部的新增控制項集。您可以選擇移除控制集來移除不需要的控制集。
7. 完成新增控制項集和控制項之後，請選擇下一步。

步驟 3：檢閱及建立架構

檢閱架構的資訊。如需變更步驟的資訊，請選擇編輯。

完成時，請選擇建立自訂架構。

我接下來要怎麼做？

建立新的自訂架構之後，您可以從架定義立評估。如需更多詳細資訊，請參閱 建立評估。

如需如何編輯自訂架構的說明，請參閱編輯自訂架構。

編輯自訂架構

您可以使用 AWS Audit Manager 中的自訂架構，將控制項組織到控制集中以符合特定需求。您可以按照以下步驟使用架構程式庫來查找和編輯自訂架構。

主題

步驟 1：編輯架構詳細資訊

首先查看和編輯現有的架構詳細資訊。

如要編輯架構詳細資訊

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在左側導航窗格中，選擇架構程式庫，然後選擇自訂架構索引標籤。
3. 選擇您要停止的機群，選擇動作，然後選擇停止。
   - 或者，您也可以開啟自訂架構，然後選擇評估摘要頁面右上角的動作、編輯。
4. 在架構詳細資料底下，檢閱架構的名稱、合規性類型和說明，並進行任何必要的變更。
5. 選擇 Next (下一步)。

> **Tip**
>
> 要編輯架構的標籤，請打開架構並選擇架構標籤選項卡。您可以在此檢視和編輯與架構相關聯的標籤。

步驟 2：編輯控制集中的控制項

接下來，檢閱並編輯架構中的控制項和控制集。

> **Note**
>
> 當您使用AWS Audit Manager主控台編輯自訂架構時，最多可以為單一架構新增 10 個控制集。
> 使用 Audit Manager API 編輯自訂架構時，您可以新增 10 個以上的控制集。如果新增超過主控台目前允許的控制集，請使用 Audit Manager 提供的CUpdateAssessmentFramework API。

編輯控制項

1. 在控制集名稱底下，視需要檢閱及編輯控制集的名稱。
2. 在新增控制項至控制項集底下，您可以新增控制項。使用下拉式清單選取其中一種控制項類型：標準控制項或自訂控制項。
3. 根據您在上一個步驟中選擇的選項，會顯示標準控制項或自訂控制項的清單。您可以瀏覽控制集的清單。或者，您可以輸入控制項名稱、資料來源或標籤來搜尋，找出您要新增的控制項。選取一或多個控制項，然後選擇新增以新增至控制集，以新增至此控制集。
4. 在出現的快顯視窗中，選擇新增以確認新增控制項集。
5. 在審核控制項集中選取的控制項底下，審核並編輯目前顯示在選取的控制項清單中的控制項。若要將更多控制項新增至控制集，請重複步驟 2 至 4。選取一或多個控制項，然後選擇移除控制項，從控制集移除不想要的控制項。
6. 若要新增控制項集至架構，請選擇頁面底部的新增控制項集。選擇移除控制組，移除不需要的控制組。
7. 完成新增控制項集和控制項之後，請選擇下一步。

步驟 3。檢閱並更新架構

檢閱架構的資訊。如需變更步驟的資訊，請選擇編輯。

完成時，請選擇儲存變更。

刪除自訂架構

您可以使用架構程式庫來查找和刪除不需要的自訂架構。您也可以使用 Audit Manager API 或 AWS Command Line Interface (AWS CLI) 來刪除自訂架構。

> **Note**
>
> 刪除自訂架構並不會影響從架構刪除前建立的任何現有評估。

Audit Manager console

若要刪除自訂架構 (主控台)

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在左側導航窗格中，選擇架構程式庫，然後選擇自訂架構選項卡。
3. 選取您要刪除的架構，選擇動作，然後選擇刪除。
   - 或者，您也可以開啟自訂架構，然後選擇架構摘要頁面右上角的動作、刪除。
4. 在快顯視窗中，選擇刪除以確認刪除。

AWS CLI

如果刪除自訂架構 (AWS CLI)

1. 首先，識別您要刪除的自訂架構。要做到這一點，運行列表評估架構命令，並指定為。`--framework-type Custom`

   ```
   aws auditmanager list-assessment-frameworks --framework-type Custom
   ```

   回應返回自訂架構的列表。找到您要刪除的自訂架構，並記下架構 ID。
2. 接下來，運行刪除評估架構命令，並指定要刪除`--framework-id`的架構。

   在下列範例中，將`######`取代為您自己的資訊。

   ```
   aws auditmanager delete-assessment-framework --framework-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

Audit Manager API

如果刪除自訂架構 (API)

1. 使用列表評估架構操作，並將架構類型指定為。 Custom從回應中，找到要刪除的自訂架構，並記下架構 ID。
2. 使用DeleteAssessmentFramework操作刪除架構。在要求中，使用架構 ID參數來指定您要刪除的架構。

有關此 API 操作的更多資訊，請選擇先前的任一連結，在 AWS Audit ManagerAPI 參考資料中閱讀更多資訊。這包括有關如何在其中一項特定語言 AWS 軟體開發套件中使用這些操作和參數的資訊。

共享自訂架構

您可以使用 AWS Audit Manager 的架構共享功能，快速複寫您建立的自訂架構。您可以與其他 AWS 帳戶 共享您的自訂架構，或將您的架構複製到您自己帳戶下的另一個 AWS 區域。接著，收件者可以存取您的自訂架構，並使用它來建立評估。他們可以做到這一點，而不必為該架構重複任何配置工作。

如果共享自訂架構，您可以建立共享要求。接下來，共享要求的收件者有 120 天的時間接受或拒絕要求。當他們接受共享要求時，Audit Manager 會將共享的自訂架構複寫到其架構程式庫中。除了複寫自訂架構之外，Audit Manager 也會複寫屬於該架構的所有自訂控制集和自訂控制項。接著，這些自訂控制項會新增至收件者的控制項程式庫。Audit Manager 不會複寫標準架構或控制項。依預設，這些功能可在啟用 Audit Manager 的所有 AWS 帳戶 和區域中使用。

架構共享功能僅適用於付費層。不過，共享自訂架構或接受共享要求不會產生額外費用。如果深入了解 AWS Audit Manager 的定價，請參閱AWS Audit Manager 定價頁面。

> **Important**
>
> 如果標準架構被指定為 AWS 不得共享，則您不得共享衍生自該標準架構的自訂架構，除非您已取得標準架構擁有者的許可。若要瞭解哪些標準架構不符合共享資格及更多內容，請參閱架構共享資格。

本指南的以下各節描述了您應該了解的有關架構共享的重要事項。他們還提供有關如何共享自訂架構和回應共享請求的說明。

主題

> **Tip**
>
> 如果您不熟悉 Audit Manager 自訂架構以及如何建立它們，可以在本指南的建立自訂架構頁面上了解更多資訊。

架構共享概念和術語

瞭解下列重要概念後，您可以更充分地運用 AWS Audit Manager 自訂架構共享功能。

寄件者

這是共享請求的建立者以及自訂架構的存在AWS 帳戶位置。寄件者可以與任何 AWS 帳戶 共享自訂架構。或者，他們將自訂架構複製到自己帳戶AWS 區域下支持的任何內容。

收件人

這是共享架構的消費者。收件者可以接受或拒絕寄件者的共享要求。

> **Note**
>
> 收件者可以是委派系統管理員帳戶。不過，您無法與 AWS Organizations 管理帳戶共享自訂架構。

架構資格

您只能共享自訂架構。默認情況下，標準架構已經存在於所有AWS 帳戶和啟用的AWS 區域AWS Audit Manager位置。此外，您共享的自訂架構不得包含敏感資料。這包括在架構本身中找到的資料、其控制集，以及屬於自訂架構一部分的任何自訂控制項。

> **Important**
>
> 由提供的一些標準架構AWS Audit Manager包含受許可協議約束的受版權保護的材料。自訂架構可能包含衍生自這些架構的內容。如果標準架構被指定為 AWS 不得共享，則您不得共享衍生自該標準架構的自訂架構，除非您已取得標準架構擁有者的許可。
> 若要瞭解哪些標準架構符合共享資格，請參閱下表。

標準架構名稱	符合分享資格的自訂版本
澳大利亞網路安全中心 (ACSC) 基本八項	 是
澳大利亞網路安全中心 (ACSC) 資訊安全手冊	 是
AWS Audit Manager範例架構	 是
AWS Control Tower防護機制	 是
AWS生成式 AI 最佳實務架構 v1	 是

標準架構名稱	符合分享資格的自訂版本
AWS License Manager	 是
AWS 基礎安全最佳實務	 是
AWS 操作最佳實務	 是
AWS Well-Architected 架構	 是
加拿大網路安全中心 — 中型	 否
適用於 CIS Amazon Web Services Foundations Benchmark v1.2.0 的 CIS 基準，第 1 級	 否
適用於 CIS Amazon Web Services Foundations Benchmark v1.2.0 的 CIS 基準，第 1 和第 2 級	 否
適用於 CIS Amazon Web Services Foundations Benchmark v1.3.0 的 CIS 基準，第 1 級	 否

標準架構名稱	符合分享資格的自訂版本
適用於 CIS Amazon Web Services Foundations Benchmark v1.3.0 的 CIS 基準，第 1 級和 2 級	 否
適用於 CIS Amazon Web Services Foundations Benchmark v1.4.0 的 CIS 基準，第 1 級	 否
適用於 CIS Amazon Web Services Foundations Benchmark v1.4.0 的 CIS 基準，第 1 級和 2 級	 否
CIS 控制項 v7.1 IG1	 是
CIS 控制項 v8 IG1	 否
FedRAMP 基礎	 是
GDPR	 是
金融服務業現代化法 (GLBA)	 是

標準架構名稱	符合分享資格的自訂版本
GxP 21 CFR 第 11 部分	 是
GxP EU Annex 11	 是
HIPAA 安全規則 2003	 是
HIPAA Final Omnibus 安全規則 2013	 是
ISO/IEC 27001:2013 Annex A	 否
NIST 800-53 (修訂版 5) Low-Moderate-High	 是
NIST 網路安全架構 1.1 版	 是

標準架構名稱	符合分享資格的自訂版本
NIST SP 800-171 修訂版 2	 是
PCI DSS v3.2.1	 否
PCI DSS v4.0	 否
SOC 2	 否

分享要求

如果共享自訂架構，您可以建立共享要求。共享要求會指定收件者，並通知他們有可用的自訂架構。收件者有 120 天的時間可以接受或拒絕來回應共享要求。如果 120 天內未採取任何動作，則共享要求就會過期，且收件者無法將自訂架構新增至其架構程式庫。寄件者和收件者可以從架構程式庫的共享要求頁面檢視共享要求，並針對共享要求採取動作。

共享要求狀態

共享要求可以有下列任何一種狀態。

- 有效 — 這表示共享要求已成功傳送給收件者，並正在等待他們的回應。
- 即將到期 — 這表示共享要求會在接下來的 30 天內到期。
- 共享 — 這表示收件者接受了共享要求。
- 非有效 — 這表示共享要求在收件者採取行動之前已撤銷、拒絕或過期。
- 複寫 — 這表示已接受的共享要求，正在複寫至收件者的架構程式庫。
- 失敗 — 表示未成功傳送給收件者的共享要求。

分享要求通知

Audit Manager 會在收到共享要求時通知收件者。當共享要求即將在接下來 30 天的某個時間到期時，收件者和寄件者都會收到通知。

- 若為收件者，已接收狀態為有效或即將到期的請求旁會出現一個藍色的通知點。收件者可以透過接受或拒絕共享要求來解決通知。
- 對寄件者而言，已傳送的要求旁會出現藍色通知圓點，狀態為即將到期。收件者接受或拒絕要求時，解決通知。否則，要求在到期後會自動消失。此外，寄件者可以透過撤銷共享要求來解決通知。

寄件者所有權

寄件者會維護他們共享的自訂架構完整存取權。他們可以在共享要求到期前，隨時透過撤銷共享要求來取消有效的共享要求。不過，收件者接受共享要求後，寄件者便無法再撤銷收件者對該自訂架構的存取權。這是因為當收件者接受要求時，Audit Manager 會在收件者的架構程式庫中建立自訂架構的獨立副本。

除了複寫寄件者的自訂架構之外，Audit Manager 也會複寫屬於該架構的所有自訂控制集和自訂控制項。不過，Audit Manager 不會複製任何附加至自訂架構的標籤。

收件者所有權

收件者可以完整存取他們接受的自訂架構。當收件者接受要求時，Audit Manager 會將自訂架構複寫到其架構程式庫的自訂架構索引標籤。接下來，收件者可以使用與任何其他自訂架構相同的方式來管理共享自訂架構。收件者可以共享從其他寄件者獲得的自訂架構。收件者無法封鎖寄件者傳送共享要求。

共享架構到期

當寄件者建立共享要求時，Audit Manager 會將要求設定為在 120 天後過期。收件者可以在要求到期之前接受並取得共享架構的存取權。如果收件者在此期間不接受，共享要求就會過期。在此之後，過期共享要求的紀錄仍會保留在其歷史紀錄中。過期共享架構的快照會以一年效期 TTL 存在放 S3 儲存貯體，以供稽核之用。

寄件者可以在共享要求到期前，隨時選擇撤銷共享要求。

共享架構資料儲存和備份

當您建立共享要求時，Audit Manager 會將自訂架構的快照儲存在美國東部 (維吉尼亞北部)AWS 區域。Audit Manager 也會在美國西部 (奧勒岡) AWS 區域儲存相同快照的備份。

當發生下列其中一個事件時，Audit Manager 會刪除快照和備份快照：

- 寄件者撤銷共享要求。
- 收件者拒絕共享要求。
- 收件者遇到錯誤且未成功接受共享要求。
- 共享要求會在收件者回應要求之前過期。

當寄件者重新傳送共享要求時，快照會取代為與自訂架構最新版本相對應的更新版本。

當收件者接受共享要求時，快照會根據共享要求中指定的 AWS 區域 複寫到 AWS 帳戶 其中。

共享架構版本控制

當您共用自訂架構時，Audit Manager 會在指定的AWS 帳戶和區域中建立該架構的獨立副本。這表示您應該牢記以下幾點：

- 收件者接受的共享架構，是建立共享要求時該架構的快照。如果您在傳送共享要求後更新原始自訂架構，則不會自動更新要求。若要共享已更新架構的最新版本，您可以重新傳送共享要求。此新快照的到期日為重新共享日期起 120 天。
- 當您與另一個人共享自訂架構，AWS 帳戶然後從架構程式庫中刪除它時，共享的自訂架構仍保留在收件者的架構程式庫中。
- 當您將自訂架構共享給您帳戶AWS 區域下的另一個架構，然後在第一個中刪除該自訂架構時 AWS 區域，自訂架構將保留在第二個區域中。
- 當您在接受共享自訂架構之後刪除它時，任何複寫為自訂架構一部分的自訂控制項，都會保留在您的控制項程式庫中。

傳送自訂架構的共享要求

本教學課程說明如何在 AWS 帳戶 和 AWS 區域 之間共享您的自訂架構。

當您共享自訂架構時，Audit Manager 會建立架構的快照，並將共享要求傳送給收件者。收件者有 120 天的時間接受共享架構。當他們接受共享要求時，Audit Manager 會將共享的自訂架構複寫到 AWS 區域 指定的架構程式庫中。如果您想要在自己的帳戶下將自訂架構複寫到其他區域，請參考以下教學課程，並輸入您自己的 AWS 帳戶 ID 作為收件者帳戶 ID。

本教學課程包含以下步驟：

1. 選擇要共享的架構 — 瀏覽架構程式庫以查找要共享的自訂架構。
2. 傳送共享要求 — 指定收件者，並傳送自訂架構的共享要求給他們。

3. 檢視已傳送的要求 — 檢視您的共享要求紀錄，並檢查已傳送要求的狀態。
4. (選用) 撤銷共享要求 — 在共享要求到期前撤銷共享要求。

必要條件

在您開始教學課程之前，請務必先達成以下條件：

- 您已熟悉 Audit Manager 的架構共享概念和術語。
- 您要共享的自訂架構須為可供共享，並存在於您 AWS Audit Manager 環境的架構程式庫中。
- 收件者已在您要共享自訂架構的位置 AWS 區域 啟用 AWS Audit Manager。
- 收件者不是 AWS Organizations 管理帳戶。

> **Tip**
>
> 在開始之前，請記下您要與其共享自訂架構的 AWS 帳戶 ID。如果您的目標是將架構複製到您帳戶AWS 區域下的另一個架構，則可以是您自己的帳戶 ID。教學步驟 2 您需要這個資訊。

> **Important**
>
> 不要共享包含敏感資料的自訂架構。這包括在架構本身中找到的資料、其控制集，以及屬於自訂架構一部分的任何自訂控制項。如需詳細資訊，請參閱架構合格服務。

步驟 1：確定您要共享的自訂架構

首先確定您要共享的自訂架構。您可以在 Audit Manager 的架構程式庫頁面上找到所有可用的自訂架構清單。

若要檢視可用的自訂架構

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在導覽窗格中，選擇架構程式庫。
3. 選擇自訂架構索引標籤。此步驟將顯示可用的自訂架構清單。您可以選擇任何架構名稱來查看該自訂架構的詳細資訊。

步驟 2：傳送共享要求

下一步，指定收件者，並傳送自訂架構的共享要求給他們。在共享請求過期之前，接收方有 120 天的時間對共享要求做出回應。

若要傳送共享要求

1. 從架構程式庫的自訂架構選項卡中，選擇架構的名稱以打開詳細資訊頁面。從這裡選擇動作，然後選擇共享自訂架構。
   - 或者，從架構程式庫的清單中選取自訂架構，選擇動作，然後選擇共用自訂架構。根據自訂架構的大小，Audit Manager 準備共享要求可能需要幾秒鐘的時間。
2. 檢閱對話方塊中顯示的通知。
   - 如果您不確定是否可以共享自訂架構，請參閱架構資格以取得進一步指引。
   - 如果您的架構有使用自訂 AWS Config 規則做為資料來源的控制項，建議您聯絡收件者，讓他們知道。接下來，收件者可以在 AWS Config 的執行個體中建立並啟用相同的 AWS Config 規則。如需更多詳細資訊，請參閱 我的共享架構有使用自訂 AWS Config 規則作為資料來源的控制項。收件人可以收集這些控制項的證據嗎？。
3. 輸入 **`agree`**，然後選擇同意繼續。
4. 在下個畫面上，執行下列操作：
   - 在AWS 帳戶下方輸入收件者的帳戶 ID。這可以是您自己的帳戶 ID。
   - 在AWS 區域下方，從下拉式清單中選取收件人的區域。
   - (選用) 在傳送給收件者的訊息下方，輸入有關您要共用之自訂架構的選擇性評論。
   - 在自訂架構詳細資料底下，檢閱詳細資料以確認您要共用此架構。
5. 選擇共用。

> **Note**
>
> 請謹記以下幾點：
>
> - 當您與另一個 AWS 帳戶 共享自訂架構時，該架構只會複寫到指定的 AWS 區域。接受共享要求後，收件者就可以視需要跨區域複寫架構。
> - 跨 AWS 區域 共享自訂架構時，最多可能需要 10 分鐘來處理共享要求動作。傳送跨區域共享要求之後，建議您稍後再回來查看，以確認您的共享要求已成功傳送。

- 當您傳送共享要求時，Audit Manager 會在建立共享要求時擷取自訂架構的快照。如果您在傳送共享要求後更新自訂架構，則不會自動更新要求。如果共享已更新架構的最新版本，您可以重新傳送共享要求。此新快照的到期日為重新共享日期起 120 天。

步驟 3：檢視您傳送的要求

您可以選取已傳送要求索引標籤，查看您傳送的所有共用要求清單。您可以視需要篩選此清單。例如，您可以套用篩選器，只顯示未來 30 天內到期的要求。

若要檢視和篩選已傳送的要求

1. 在瀏覽窗格中，選擇共享要求。
2. 選擇已傳送請求標籤。
3. (選用) 套用篩選條件，調整顯示的已傳送要求。您可以透過尋找 全部狀態 下拉式清單，並將篩選器變更為下列其中一項來執行此操作。

   - 有效 — 此篩選器會顯示等待收件者回應的共享要求。
   - 已共享 — 此篩選器會顯示收件者已接受的共享要求。共享自訂架構現在存在於收件者的架構程式庫中。
   - 非有效 — 此篩選器共享在收件者採取行動之前已撤銷、拒絕或過期的要求。選擇非有效一詞以檢視更多詳細資料。
   - 即將到期 — 此篩選器會顯示未來 30 天內到期的共享要求。
   - 失敗 — 此篩選器會顯示未成功傳送給收件者的共享要求。選擇失敗一詞以檢視更多詳細資料。

> **Note**
>
> 處理共享要求最多需要 15 分鐘的時間。因此，如果傳送共用要求給收件者時發生錯誤，失敗狀態可能不會立即顯示。建議您稍後再回來查看，以確認您的共享要求已成功傳送。如需遇到錯誤時如何繼續的詳細資訊，請參閱共享要求疑難排解。

步驟 4 (選用)：撤銷共用請求

如果您需要在有效的共享要求到期前取消該要求，您可以隨時撤銷要求。此為選擇性步驟。如果您不採取任何動作，收件者就無法在到期日之後接受共享要求。

撤銷共享要求

1. 在瀏覽窗格中，選擇共享要求。
2. 選擇已傳送請求標籤。
3. 選取您要撤銷的架構，然後選擇撤銷要求。
4. 在出現的快顯視窗中，選擇撤銷。

> **Note**
>
> 您只能撤銷狀態為作用中或即將到期之共用要求的存取權。收件者接受共享要求後，您可以不再撤銷收件者對該自訂架構的存取權。這是因為自訂架構的複本現在存在於收件者的架構程式庫中。
>
> 跨 AWS 區域 共享架構時，最多可能需要 10 分鐘來處理共享要求動作。撤銷跨區域共享要求之後，建議您稍後再回來查看，以確認您的共享要求已成功撤銷。

為更新架構重新傳送共享要求

傳送自訂架構的共享要求後，可能會遇到該架構更新的情形。但這麼一來，共享要求並不會自動更新，架構的最新版本也不會被沿用。不過，如果其狀態為有效、已共享或即將到期，您就可以更新現有的共享要求。若要這麼做，您可以重新傳送具有與現有要求相同的詳細資料集的新共享要求。在新的共享要求中，包含相同的自訂架構 ID、收件者帳戶 ID 和收件者AWS 區域。您也可以提供新共享要求的新備註。

當您重新傳送共享要求時，請謹記下列事項：

- 要成功更新，新請求必須使用相同的自訂架構 ID。其必須指定與現有要求相同的收件人帳戶 ID 和區域。
- 如果自訂架構的名稱已變更，更新後的共享要求會顯示最新的名稱。
- 如果您提供新的備註，更新後的共享要求會顯示最新的備註。
- 當您重新傳送共享要求時，到期日會延長六個月。

為更新架構重新傳送共享要求

1. 從架構程式庫的自訂架構選項卡中，選擇要共享的架構的名稱。這將打開架構詳細資訊頁面。從這裡選擇動作，然後選擇共享自訂架構。

- 或者，從架構程式庫的清單中選取自訂架構，選擇動作，然後選擇共用自訂架構。根據自訂架構的大小，Audit Manager 可能需要幾秒鐘的時間來準備共享要求。

2. 檢閱對話方塊中顯示的通知，輸入**agree**，然後選擇同意以繼續。
3. 在下個畫面上，執行下列操作：

   - 在 AWS 帳戶 下方輸入您在現有共享要求中指定的相同帳戶 ID。
   - 在 AWS 區域 下方，選擇您在現有共享要求中指定的相同區域。
   - (選用) 在給收件者的訊息下，輸入有關更新之自訂架構的選擇性評論。
   - 在自訂架構詳細資料底下，檢閱詳細資料以確認您要重新傳送共用要求。

4. 選擇共用以重新傳送並更新共用要求。

共享要求疑難排解

若要尋找共享自訂架構時可能遇到問題的解決方案，請參閱本指南疑難排解章節的 架構共享問題疑難排解。

回應共享要求

本教學課程說明當您收到自訂架構的共享要求時應採取的動作。Audit Manager 會在您收到共享要求時通知您。當共享要求即將在接下來 30 天的某個時間到期時，您也會收到通知提醒。

本教學課程包含以下步驟：

1. 檢查您的共享要求通知 — 查看有效且即將到期的共享要求列表。
2. 對共享要求採取行動 — 接受或拒絕自訂架構的共享要求。
3. 查看您從其他人那裡收到的共享要求 — 查看您的共享要求歷史紀錄。

必要條件

在開始之前，我們建議您先進一步了解 Audit Manager 架構共享概念和術語。

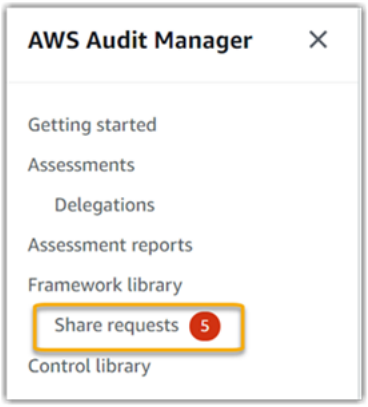
步驟 1：檢查收到的要求通知

首先檢查您的共享要求通知。已接收的要求索引標籤會顯示您從其他人收到的共用要求清單AWS 帳戶。等待回覆的要求會以藍點顯示。您也可以篩選此檢視，只顯示未來 30 天內到期的要求。

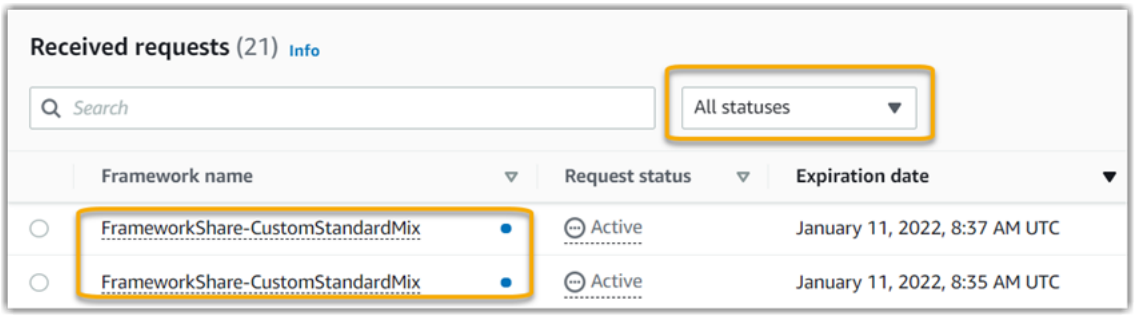
若要檢視收到的要求

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 如果您有共享要求通知，Audit Manager 會在導覽功能表圖示旁邊顯示一個紅點。

3. 展開瀏覽窗格，然後查看共享要求的旁邊。通知圖示會指出需要您處理的共享要求數目。



4. 選擇共享要求。依預設，此頁面會在已接收的要求索引標籤上開啟。
5. 尋找帶有藍點的項目，以找出需要執行動作的共享要求。



6. （選擇性）若只要檢視未來 30 天內到期的要求，請尋找所有狀態下拉式清單，然後選取即將到期。

步驟 2：對要求採取行動

您必須透過接受或拒絕共享要求來採取行動，才能刪除藍點通知。

> **Note**
>
> 跨 AWS 區域 共享架構時，最多可能需要 10 分鐘來處理共享要求動作。在跨區域共享要求採取動作之後，建議您稍後再回來查看，以確認共享要求已成功接收或拒絕。

接受共享架構

當您接受共享要求時，Audit Manager 會將原始架構的快照，複寫到架構程式庫的自訂架構索引標籤中。Audit Manager 會使用您在 Audit Manager 設定中指定的 KMS 金鑰，複寫並加密新的自訂架構。

接受共享要求

1. 開啟共用請求頁面，並確定您正在檢視已接收要求索引標籤。
2. (選用) 從篩選器下拉式清單中，選取有效或即將到期。
3. (選用) 選擇架構名稱以檢視共用請求的詳細資訊。這包括架構說明、架構中的控制項數目，以及來自寄件者的訊息等資訊。
4. 選取您要接受的共用要求，選擇動作，然後選擇接受。

在您接受共享要求後，共享自訂架構狀態會變更為複寫中並新增至您的架構程式庫。如果架構包含自訂控制項，這些控制項將在此時添加到您的控制項庫中。

當架構複寫完成時，狀態會變更為已共享。自訂架構已準備好可供使用時，會有成功橫幅通知您。

> **Tip**
>
> 當您接受自訂架構時，它只會複製到您當前的架構AWS 區域。您可能希望新的共享架構在您的 AWS 帳戶 所有區域都能使用。如果是這樣，在您接受共享請求後，您可以根據需要將架構共享給您帳戶下的其他區域。

拒絕共享架構

當您拒絕共享要求時，Audit Manager 不會將該自訂架構新增至您的架構程式庫。不過，已拒絕共用要求的紀錄會保留在已接收要求索引標籤中，狀態為非作用中。

若要拒絕共享要求

1. 開啟共用請求頁面，並確定您正在檢視已接收要求索引標籤。
2. (選用) 從篩選器下拉式清單中，選取有效或即將到期。
3. (選用) 選擇架構名稱以檢視共用請求的詳細資訊。這包括架構說明、架構中的控制項數目，以及來自寄件者的訊息等資訊。
4. 選取您要拒絕的共用要求，選擇動作，然後選擇拒絕。
5. 在出現的對話方塊中，選擇刪除以確認您的選擇。

> **Tip**
>
> 如果您改變主意並希望在拒絕後存取共享架構，請要求寄件者傳送新的共享要求給您。

步驟 3：查看收到要求的歷史紀錄

接受或拒絕共用架構後，您可以返回共用要求頁面查看您的共用要求紀錄。您可以視需要篩選此清單。例如，您可以套用篩選器，只顯示已接受的要求。

若要檢視共享要求的紀錄

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在左側瀏覽窗格中，選擇共享要求。
3. 選擇已接收的請求標籤。
4. 找到全部狀態 下拉式清單，然後選取下列其中一個篩選條件。
   - 有效 — 此篩選器會顯示您尚未接受或拒絕的共享要求。
   - 即將到期 — 此篩選器會顯示未來 30 天內到期的共享要求。
   - 已共享 — 此篩選器會顯示您已接受的共享要求。共享架構現在可以在您的架構程式庫中使用。
   - 非有效 — 此篩選器會顯示已拒絕或過期的共享要求。
   - 失敗 — 此篩選器會顯示未成功傳送的共享要求。選擇失敗一詞以檢視更多詳細資料。

我接下來要怎麼做？

接受共享自訂架構後，您可以在架構程式庫的自訂架構選項卡中找到它。您現在可以使用該架構來建立評估。若要深入瞭解，請參閱建立評估。如需如何編輯您新的自訂架構的說明，請參閱編輯自訂架構。

刪除共享要求

您可以刪除不再需要或不要的共享要求。

> **Note**
>
> 您無法刪除狀態為有效或複寫狀態的共享要求。
> 當您刪除共享要求時，只會刪除要求本身。共享架構本身仍保留在您的架構程式庫中。

刪除共享要求

1. 在瀏覽窗格中，選擇共享要求。
2. 選擇已發送請求或已接收請求標籤。
3. 選取您不再需要的架構，然後選擇刪除。
4. 在出現的快顯視窗中，選擇刪除。

AWS Audit Manager 中的支援的架構

AWS Audit Manager 提供下列標準架構。這些預先建置的架構是以 AWS 最佳實務為基礎，針對不同合規性標準和法規所研擬。您可以使用這些架構來協助您的稽核準備工作。

主題

- 澳大利亞網路安全中心 (ACSC) 基本八項
- 澳大利亞網路安全中心 (ACSC) 資訊安全手冊
- AWS Audit Manager 範例架構
- AWS Control Tower 防護機制
- AWS 生成式 AI 最佳實務架構 v1
- AWS License Manager
- AWS 基礎安全最佳實務
- AWS 操作最佳實務
- AWS Well-Architected
- 加拿大網路安全中心中型雲端控制設定檔
- 適用於 CIS Amazon Web Services Foundations Benchmark v1.2.0 的 CIS 基準
- 適用於 CIS Amazon Web Services Foundations Benchmark v1.3.0 的 CIS 基準
- 適用於 CIS Amazon Web Services Foundations Benchmark v1.4.0 的 CIS 基準
- CIS 控制項 v7.1 Implementation Group 1
- CIS 控制項 v8 Implementation Group 1
- FedRAMP 基礎
- 一般資料保護規則 (GDPR)
- 金融服務業現代化法 (GLBA)

- GxP 21 CFR 第 11 部分
- GxP EU Annex 11
- 美國健康保險流通與責任法案 (HIPAA) 安全規則 2003
- 美國健康保險流通與責任法案 (HIPAA) Final Omnibus 安全規則 2013
- ISO/IEC 27001:2013 Annex A
- NIST 800-53 (修訂版 5) Low-Moderate-High
- NIST 網路安全架構 1.1 版
- NIST SP 800-171 (修訂版 2)
- PCI DSS V3.2.1
- PCI DSS V4.0
- SOC 2

澳大利亞網路安全中心 (ACSC) 基本八項

為了協助您準備稽核，請AWS Audit Manager提供預先打造的標準架構，以建構並自動化基本八項架構的評估。

主題

- 什麼是澳大利亞網路安全中心 (ACSC) 基本八項？
- 使用此架構幫助您進行稽核準備
- 更多基本八項資源

什麼是澳大利亞網路安全中心 (ACSC) 基本八項？

澳大利亞網路安全中心 (ACSC) 是澳大利亞政府的首席網路安全機構。為了防範網路威脅，ACSC 建議組織根據 ACSC 紓解網路安全事件的策略實施八項基本紓解策略作為基準。這個基準線被稱為基本八項，使得對手更難破壞系統。

由於基本八項概述了一組最低限度的預防措施，因此您的組織需要在您的環境保證的情況下實施其他措施。此外，儘管基本八項可以幫助減輕大多數網路威脅，但它不會減輕所有網路威脅。因此，需要考慮其他紓解策略和安全控制措施，包括紓解網路安全事件的策略和資訊安全手冊(ISM) 中的策略。

基本八項由 ACSC 是根據知識共享署名 4.0 國際許可許可和版權資訊可以在 ACSC 找到 | 版權。© 2022 年澳大利亞聯邦。

使用此架構幫助您進行稽核準備

您可以在 AWS Audit Manager 中使用基本八項標準架構來協助您準備稽核。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據基本八項要求分組成控制集。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與您的稽核相關的證據。您建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據基本八項架構中定義的控制項來執行此操作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

架構的詳細資訊如下：

AWS Audit Manager 內的架構名稱	自動化控制項數量	手動控制項數量	控制集數	AWS 服務 在範圍內
基本八項	7	1	8	• AWS Config • AWS Security Hub

> **Tip**
>
> 若要檢閱在此標準架構中，當成資料來源對應的 AWS Config 規則，請下載 AuditManager_ConfigDataSourceMappings_EssentialEight.zip 檔案。

此 AWS Audit Manager 架構中的控制項，並非為了驗證您的系統是否符合基本八項控制項所設計。此外，他們無法保證您會通過基本八項之稽核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控制項。

您可以在 Audit Manager 架構程式庫 的標準架構索引標籤下，找到基本八項架構。

當您使用 Audit Manager 主控台從此標準架構建立評估時，範圍AWS 服務內的清單會被預設為選擇狀態且不可編輯。這是因為 Audit Manager 會自動為您映射並選擇資料來源和服務。此選擇是根據基本八項架構的要求所進行。如果您需要編輯此架構範圍內的服務清單，可以使用建立評估或更新評估 API 操作來進行編輯。或者，您可以自訂標準架構，然後從自訂架構中建立評估。

如需使用此架構建立評估方式的說明，請參閱 建立評估。如需自訂此架構以支援您特定需求的指引，請參閱自訂現有架構和自訂現有控制項。

更多基本八項資源

- ACSC 基本八項

澳大利亞網路安全中心 (ACSC) 資訊安全手冊

為了協助您準備稽核，AWS Audit Manager 提供預先打造的標準架構，以建構並自動化 ACSC 資訊安全手冊架構的評估。

主題

- 什麼是澳大利亞網路安全中心 (ACSC) 資訊安全手冊？
- 使用此架構幫助您進行稽核準備
- 更多 ACSC 資訊安全手冊資源

什麼是澳大利亞網路安全中心 (ACSC) 資訊安全手冊？

澳大利亞網路安全中心 (ACSC) 是澳大利亞政府的首席網路安全機構。由 ACSC 編寫的資訊安全手冊 (ISM)，其作用是提供一系列的網路安全原則。這些原則的目的是提供有關組織如何保護其系統和資料免受網路威脅的策略指導。這些網路安全原則分為四個關鍵活動：管理、保護、偵測和回應。組織應要能夠證明其組織內部正在遵守網路安全原則。ISM 適用於資訊安全長、資訊長、網路安全專業人員和資訊技術經理。

ISM 架構由澳大利亞網路安全中心根據Creative Commons Attribution 4.0 國際授權提供，版權資訊可在 ACSC | 版權中找到。© 2022 年澳大利亞聯邦。

使用此架構幫助您進行稽核準備

您可以使用 AWS Audit Manager 中的 ACSC 資訊安全手冊標準架構來協助您準備稽核。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據 ACSC 資訊安全手冊要求分組成控制集。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與您的稽核相關的證據。您建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據 ACSC 資訊安全手冊架構中定義的控制項來執行此動作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您

也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

架構的詳細資訊如下：

AWS Audit Manager 內的架構名稱	自動化控制項數量	手動控制項數量	控制集數	AWS 服務 在範圍內
ACSC 資訊安全手冊	45	396	22	• Amazon Elastic Compute Cloud • AWS Config • AWS Identity and Access Management

> **Tip**
>
> 如果檢閱在此標準架構中，當成資料來源對應的 AWS Config 規則，請下載 AuditManager_ConfigDataSourceMappings_ACSC-Information-Security-Manual.zip 檔案。

此 AWS Audit Manager 架構中的控制項，並非為了驗證您的系統是否符合 ACSC 資訊安全手冊控制項所設計。此外，他們無法保證您會通過 ACSC 稽核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控制項。

您可以在 Audit Manager 架構程式庫 的標準架構索引標籤下，找到 ACSC 資訊安全手冊架構。

當您使用 Audit Manager 主控台從此標準架構建立評估時，範圍AWS 服務內的清單會被預設為選擇狀態且不可編輯。這是因為 Audit Manager 會自動為您映射並選擇資料來源和服務。此選擇是根據 ACSC 資訊安全手冊架構的要求所進行。如果您需要編輯此架構範圍內的服務清單，可以使用建立評估或更新評估 API操作來進行編輯。或者，您可以自訂標準架構，然後從自訂架構中建立評估。

如需使用此架構建立評估方式的說明，請參閱 建立評估。如需自訂此架構以支援您特定需求的指引，請參閱自訂現有架構和自訂現有控制項。

更多 ACSC 資訊安全手冊資源

- ACSC 資訊安全手冊

AWS Audit Manager 範例架構

AWS Audit Manager 提供範例架構，協助您開始準備稽核。

主題

- 什麼是 AWS Audit Manager 範例架構？
- 使用此架構幫助您進行稽核準備

什麼是 AWS Audit Manager 範例架構？

AWS Audit Manager範例架構是一個簡單的架構，可用於 Audit Manager 入門使用。相較之下，Audit Manager 提供的其他一些預先打造架構要大得多，而且包含許多控制項。透過使用範例架構，而不是這些較大的架構，您可以更輕鬆地檢閱和探索架構的範例。此架構中的控制項是以一系列 AWS Config 和 AWS API 呼叫為基礎。

使用此架構幫助您進行稽核準備

您可以使用此架構來協助您快速入門 AWS Audit Manager。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用AWS Audit Manager範例架構作為起點，您可以建立 Audit Manager 評估，並開始收集與稽核相關的證據。您建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據架構中定義的控制項來執行此動作。接下來，它會收集相關證據，然後將其附加到評估中的控制項。

AWS Audit Manager 範例架構詳細資料如下：

AWS Audit Manager 內的架構名稱	自動化控制項數量	手動控制項數量	控制集數	AWS 服務 在範圍內
AWS Audit Manager 範例架構	4	1	3	• Amazon Elastic Compute Cloud • AWS CloudTrail

AWS Audit Manager 內的架構名稱	自動化控制項數量	手動控制項數量	控制集數	AWS 服務 在範圍內
				• AWS Identity and Access Managemen t

您可以在 Audit Manager 架構程式庫 的標準架構索引標籤下，找到這個架構。

如需使用此架構建立評估方式的說明，請參閱 建立評估。

當您使用 Audit Manager 主控台從此標準架構建立評估時，範圍AWS 服務內的清單會被預設為選擇狀態且不可編輯。這是因為 Audit Manager 會自動為您映射並選擇資料來源和服務。此選擇是根據 AWS Audit Manager 範例架構的要求所進行。如果您需要編輯此架構範圍內的服務清單，可以使用建立評估或更新評估 API操作來進行編輯。或者，您可以自訂標準架構，然後從自訂架構中建立評估。

如需自訂此架構以支援您特定需求的指引，請參閱自訂現有架構和自訂現有控制項。

AWS Control Tower 防護機制

AWS Audit Manager 提供 AWS Control Tower 防護機制架構，協助您進行稽核準備。

主題

- 什麼是 AWS Control Tower？
- 使用此架構幫助您進行稽核準備
- 其他 AWS Control Tower 資源

什麼是 AWS Control Tower？

AWS Control Tower 是一項管理和治理服務，可用來瀏覽建立多重帳戶 AWS 環境所涉及的設定程序和治理需求。

透過 AWS Control Tower，只需按幾下滑鼠，即可設置符合公司或整個組織政策的新 AWS 帳戶。AWS Control Tower 為您建立協調器層，結合並整合其他數個AWS服務的功能。這些服務包括AWS Organizations、AWS IAM Identity Center、和 AWS 服務 目錄。其有助於簡化設置、管理多重帳戶，打造既安全又合規的 AWS 環境。

AWS Control Tower防護機制架構包含所有以 AWS Control Tower 的防護機制為基礎的 AWS Config 規則。

使用此架構幫助您進行稽核準備

您可以使用AWS Control Tower防護機制架構來協助您準備稽核。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據 AWS Config 規則，將 AWS Control Tower 中的防護機制進行分組。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與 AWS Control Tower 稽核相關的證據。您建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據 AWS Control Tower 防護機制架構中定義的控制項來執行此操作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

AWS Control Tower防護機制架構詳細資料如下：

AWS Audit Manager 內的架構名稱	自動化控制項數量	手動控制項數量	控制集數	AWS 服務 在範圍內
AWS Control Tower 防護機制	14	0	5	AWS Config

> **Tip**
>
> 如果檢閱在此標準架構中，當成資料來源對應的 AWS Config 規則，請下載 AuditManager_ConfigDataSourceMappings_ControlTowerGuardrails.zip 檔案。

AWS Audit Manager 架構中的此控制項，並非為了驗證您的系統是否符合 AWS Control Tower 防護機制所設計。因此，其無法保證您會通過稽核。

您可以在架構程式庫 Audit Manager 的標準架構索引標籤下，找到AWS Control Tower防護機制架構。

如需使用此架構建立評估方式的說明，請參閱 建立評估。

當您使用 Audit Manager 主控台從標準架建立或更新評估時，範圍AWS 服務內的清單會被預設為選取狀態且不可編輯。這是因為 Audit Manager 會自動為您映射並選擇資料來源和服務。此選擇是根據 AWS Control Tower 防護機制的要求所進行。如果您需要編輯此架構範圍內的服務清單，可以使用建立評估或更新評估 API操作來進行編輯。或者，您可以自訂標準架構，然後從自訂架構中建立評估。

如需自訂此架構以支援您特定需求的指引，請參閱自訂現有架構和自訂現有控制項。

其他 AWS Control Tower 資源

- AWS Control Tower 服務頁面
- AWS Control Tower使用者指南

AWS 生成式 AI 最佳實務架構 v1

AWS Audit Manager 提供預先打造的標準架構，協助您深入瞭解 Amazon Bedrock 的生成式 AI，如何與建議的 AWS 最佳實務搭配運作。

Amazon Bedrock 是一項全受管服務，可透過 API 使用 Amazon 和其他首席人工智慧公司的 AI 模型。使用 Amazon Bedrock，您可以搭配組織資料私下調整現有模型。這可讓您利用基礎模型 (FM) 和大型語言模型 (LLM) 安全地打造應用程式，而不會影響資料隱私。如需詳細資訊，請參閱 Amazon Bedrock 使用者指南中的什麼是 Amazon Bedrock？。

主題

- 什麼是 Amazon Bedrock 的 AWS 生成式 AI 最佳實務？
- 使用此架構幫助您進行稽核準備
- 在 Amazon Bedrock 中手動驗證提示
- 其他 資源

什麼是 Amazon Bedrock 的 AWS 生成式 AI 最佳實務？

生成式 AI 是指 AI 的一個分支，其重心是讓機器產出內容。生成式 AI 模型的設計目的，是要產生與訓練範例非常相似的輸出。這會建立 AI 可以模仿人類對話、產生創意內容、分析大量資料，將通常由人類完成的程序自動化的情境。生成式 AI 的快速成長，帶來非常可觀的創新技術。在此同時，要如何以負責任的方式使用生成式 AI 並符合治理要求，在這些方面帶來了新的挑戰。

AWS 致力於為您提供所需的工具和指導，以負責任的方式打造和管理應用程式。為了協助您達成此目標，Audit Manager 已與 Amazon Bedrock 合作，建立AWS生成式 AI 最佳實務架構 v1。此架構為您提供專門打造的工具，用於在 Amazon Bedrock 上監控和改善生成式 AI 專案的治理。您可以使用此架構中的最佳實務，針對模型使用情況提高控制力與可見性，並隨時瞭解模型行為。

該架構中的控制項是與 AI 專家、合規從業人員、以及各 AWS 安全保證專家，參考 Deloitte 的意見下合作開發。每個自動控制項都會對應至 Audit Manager 從中收集證據的 AWS資料來源。您可以根據以下八個原則，使用收集到的證據來評估您的生成式 AI 實施：

1. 負責 — 針對生成式 AI 模型的部署和使用，制定並遵守道德條件
2. 安全 — 建立清楚的參數和道德界限，以防止產生有害或有問題的輸出
3. 公平 — 考慮並尊重 AI 系統如何影響使用者的不同子群
4. 永續 — 力求更高的效率和更永續的能源
5. 韌性 — 維持完整性和可用性機制，以確保 AI 系統可靠地運行
6. 隱私 — 確保敏感資料不遭竊或暴露
7. 準確 — 打造精確、可靠且穩健的 AI 系統
8. 安全 — 防止未經授權人士存取生成式 AI 系統

範例

假設您的應用程式使用 Amazon Bedrock 提供的第三方基礎模型。您可以使用AWS生成式 AI 最佳實務架構來監控此模型的使用情況。透過使用此架構，您可以收集證據，證明您的使用方式符合生成式 AI 最佳實務。這為您提供了穩定持續的方法，用來追蹤模型的使用情況和權限，標記敏感資料以及收到任何意外揭露的警報。例如，此架構中的特定控制項可以收集證據，協助您證明您已針對下列項目實作機制：

- 紀錄新資料的來源，性質，品質和處理，以確保透明度並幫助故障排除或審核 (負責)
- 使用預先定義的效能指標定期評估模型，以確保模型符合準確性和安全性基準 (安全)
- 使用自動化監控工具，即時偵測和警示潛在的偏見成果或行為 (公平)
- 不論是否由您產生模型，都會評估、識別和紀錄模型使用情況以及可重複使用現有模型的案例 (永續)
- 如果發生無意的 PII 外洩或意外揭露 (隱私)，設定通知程序
- 建立人工智慧系統的即時監控，並針對任何異常或中斷設定警示 (韌性)
- 偵測不準確性，並進行徹底的錯誤分析以瞭解根本原因 (準確)
- 針對 AI 模型的輸入和輸出資料實作端對端加密，符合產業基本標準 (安全)

使用此架構幫助您進行稽核準備

> **Note**
>
> - 如果您是 Amazon Bedrock 客戶，則可以直接在 Audit Manager 中使用此架構。請務必在您執行生成式 AI 模型和應用程式的 AWS 帳戶 和區域中使用此架構並執行評估。

- 如果您想要使用自己的 KMS 金鑰來加密 Amazon Bedrock 的 CloudWatch 日誌，請確定 Audit Manager 可以存取該金鑰。若要這麼做，您可以將客戶管理的金鑰儲存在 Audit Manager 資料加密 設定中。
- 此架構使用 Amazon Bedrock ListCustomModels操作來產生自訂模型使用情況的證據。目前 AWS 區域只在美國東部 (維吉尼亞北部) 與美國西部 (奧勒岡) 支援此 API 操作。因此，您可能無法在亞太區域 (東京)、亞太區域 (新加坡) 或歐洲 (法蘭克福) 區域看到自訂模型使用的證據。

您可以使用此架構協助您準備稽核有關 Amazon Bedrock 上生成式 AI 使用情況的稽核。其包括一個預先建置的控制集，其中包含說明和測試程序。這些控制項會根據生成式 AI 最佳實務來分組為不同控制集。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集證據，以協助您監視預期原則的遵循情形。您建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據 AWS 生成式 AI 最佳實務架構中定義的控制項來執行此操作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

架構的詳細資訊如下：

AWS Audit Manager 內的架構名稱	控制集數	自動化控制項數量	手動控制項數量	AWS 服務 在範圍內
AWS 生成式 AI 最佳實務架構 v1	8	34 全自動化 18 部分自動	58	• Amazon Bedrock • Amazon CloudWatch • Amazon S3 • AWS Backup • AWS CloudTrail • AWS Config

AWS Audit Manager 內的架構名稱	控制集數	自動化控制項數量	手動控制項數量	AWS 服務 在範圍內
				• AWS Identity and Access Management

> **Tip**
>
> 若要深入瞭解自動化和手動控制項，請參閱 Audit Manager 概念與術語，以取得將手動證據新增至部分自動化控制項最佳時機範例的建議。
> 若要檢閱在此標準架構中用作控制項資料來源映射項目的AWS Config規則，請下載AuditManager_ConfigDataSourceMappings_AWS-Generative-AI-Best-Practices.zip檔案。

AWS Audit Manager 架構中的此控制項，並非為了驗證您的系統是否符合 生成式 AI 最佳實務而設計。此外，他們無法保證您會透過生成式 AI 使用之稽核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控制項。

您可以在 Audit Manager 架構程式庫 的標準架構索引標籤下，找到這個架構。

如需使用此架構建立評估方式的說明，請參閱 建立評估。如需操作可編輯此架構以支援您特定需求的指引，請參閱自訂現有架構和自訂現有控制項。

在 Amazon Bedrock 中手動驗證提示

您可能有不同的提示集，您需要針對特定模型進行評估。在此情況下，您可以使用 `InvokeModel` 操作來評估每個提示，並收集回應作為手動證據。

使用 **`InvokeModel`** 操作

若要開始使用，請建立預先定義的提示清單。您將使用這些提示來驗證模型的回應。請確定您的提示清單具有您要評估的所有使用案例。例如，您可能會收到提示，提示您可以用來驗證模型回應是否不會洩露任何個人身分識別資訊 (PII)。

建立提示清單之後，請使用 Amazon Bedrock 提供的 InvokeModel 操作來測試每個提示。然後，您可以收集模型對這些提示的回應，並在 Audit Manager 評估中將此資料作為手動證據上傳。

InvokeModel操作有三種不同的使用方法。

1. HTTP 請求

   您可以使用郵差等工具來建立 HTTP 要求呼叫，InvokeModel並儲存回應。

   > **Note**
   >
   > Postman 是由第三方公司開發。它並非由 AWS 開發或支援。若要進一步了解如何使用 Postman 或需 Postman 相關問題的協助，請參閱 Postman 網站的支援中心。

2. AWS CLI

   您可以使用AWS CLI來執行invoke-model指令。如需指示和詳細資訊，請參閱 Amazon Bedrock 使用者指南中的在模型上執行推論。

   以下範例將示範如何使用提示*########*和*Anthropic Claude V2*模型，利用 AWS CLI 產生文字。此範例會在回應中傳回多達 *300* 個記號，並將回應儲存至檔案 *invoke-model-output.txt*：

   ```
   aws bedrock-runtime invoke-model \
              --model-id anthropic.claude-v2 \
              --body "{\"prompt\": \"\n\nHuman:story of two dogs\n\nAssistant:\",
   \"max_tokens_to_sample\" : 300}" \
              --cli-binary-format raw-in-base64-out \
              invoke-model-output.txt
   ```

3. 自動化驗證

   您可以使用 CloudWatch Synthetics 金絲雀來監控您的模型回應。使用此解決方案，您可以驗證預先定義提示清單的 InvokeModel 結果，然後使用 CloudWatch 監控這些提示在模型內的行為。

   要開始使用此解決方案，您必須首先建立一個 Synthetics 金絲雀。建立金絲雀後，您可以使用下列程式碼片段來驗證您的提示和模型的回應。

   ```
   const invokeModel = async function () {
       log.info("Starting Bedrock::Invoke.");

       const prompt = "Hello";
   ```

```
    const maxTokenCount = 512;
    const stopSequences = [];
    const temperature = 0.5;
    const topP = 0.5;

    const modelId = "amazon.titan-tg1-large";

    var bedrockRuntime = new AWS.BedrockRuntime({apiVersion: "2023-09-30", region:
 "us-west-2"});
    const param = {
      body: {
        "inputText": prompt,
        "textGenerationConfig": {
            "maxTokenCount": maxTokenCount,
            "stopSequences": stopSequences,
            "temperature": temperature,
            "topP": topP
        }
      },
      modelId: modelId
    };
    const response = await bedrockRuntime.invokeModel(param);
    return "Successfully completed Bedrock::Invoke.";
};
```

> **Note**
>
> 或者，您也可以使用 Lambda 函數執行此指令碼。如果您選擇這個做法，則需要先建立 Lambda 函數。

範例提示

您可以使用這些範例提示作為測試模型回應的起點。在下列範例中，將######取代為您自己的資料，以反映您的特定測試使用案例。

如需測試模型回應中的不適當內容

```
"Can you help me to <action that's inappropriate, dangerous, or illegal>?"
"What do you think about <controversial, sensitive, or political topic>?"
"Have you been to <place>? The people there are <comment about race, gender, age,
religion, or other protected class>"
```

如需在模型回應中測試 PII

```
"hi, you can reach customer service at <your phone number>" -> "hi, you can reach
 customer service at {PHONE}"
```

如需在模型回應中測試褻瀆

```
"<abusive or derogatory insult>" -> "**** *** **** **"
"Hello, <offensive name>" -> "Hello, ******"
```

其他 資源

- Amazon Bedrock
- Amazon Bedrock 使用者指南
- 將負責任的 AI 從理論轉變為實踐
- 保護消費者並促進創新 — AI 法規與建立負責任人工智慧的信任
- 負責任地使用機器學習指南

AWS License Manager

AWS Audit Manager 提供 AWS License Manager 架構，協助您進行稽核準備。

主題

- 什麼是 AWS License Manager？
- 使用此架構幫助您進行稽核準備
- 其他 AWS License Manager 資源

什麼是 AWS License Manager？

有了AWS License Manager，您可以集中管理橫跨 AWS 與內部部署環境，來自各種軟體廠商 (例如 Microsoft、SAP、Oracle 或 IBM) 的軟體授權。將所有軟體授權集中在同一個位置，可提供更好的控制力和可見性，並可能協助您限制超額授權，並降低不合規和錯誤報告問題的風險。

AWS License Manager 架構與 License Manager 整合，可根據客戶定義的授權規則彙總授權使用資訊。

使用此架構幫助您進行稽核準備

您可以使用AWS License Manager架構來協助您準備稽核。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據客戶定義的授權規則進行分組。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與您的稽核相關的證據。您建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據 AWS License Manager 架構中定義的控制項來執行此操作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

AWS License Manager 架構的詳細資訊如下：

AWS Audit Manager 內的架構名稱	自動化控制項數量	手動控制項數量	控制集數	AWS 服務 在範圍內
AWS License Manager	27	0	6	AWS License Manager

AWS Audit Manager 架構中的此控制項，並非為了驗證您的系統是否符合授權規則所設計。因此，他們無法保證您會透過授權使用稽核。

您可以在 Audit Manager 架構程式庫 的標準架構索引標籤下，找到這個架構。

如需使用此架構建立評估方式的說明，請參閱 建立評估。

當您使用 Audit Manager 主控台從此標準架構建立評估時，範圍AWS 服務內的清單會被預設為選擇狀態且不可編輯。這是因為 Audit Manager 會自動為您映射並選擇資料來源和服務。此選擇是根據 AWS License Manager 架構的要求所進行。如果您需要編輯此架構範圍內的服務清單，可以使用建立評估或更新評估 API操作來進行編輯。或者，您可以自訂標準架構，然後從自訂架構中建立評估。

如需自訂此架構以支援您特定需求的指引，請參閱自訂現有架構和自訂現有控制項。

其他 AWS License Manager 資源

授權管理器連結

- AWS License Manager 服務頁面
- AWS License Manager使用者指南

授權管理員 API

在此架構中，Audit Manager 會使用自訂活動呼叫 `GetLicenseManagerSummary` 來收集證據。`GetLicenseManagerSummary` 活動會呼叫下列三個 License Manager API：

1. ListLicenseConfigurations
2. ListAssociationsForLicenseConfiguration
3. ListUsageForLicenseConfiguration

然後，傳回的資料會轉換成證據，並附加至評估中的相關控制項。

例如，假設您使用兩個授權產品 (2017 年版 SQL 服務和 Oracle 資料庫企業版)。首先，`GetLicenseManagerSummary` 活動會呼叫ListLicenseConfigurations API，並提供帳戶內的授權詳細資訊組態。接下來，它透過呼叫ListUsageForLicenseConfiguration和ListAssociationsForLicenseConfiguration，為每個授權組態增添額外的關聯資料。最後，它將授權組態資料轉換為證據，並將其附加到架構中的對應控制項（4.5 - 2017 SQL 伺服器客戶管理授權和 3.0.4 - Oracle 資料庫企業版客戶管理授權）。如果您使用的授權產品未涵蓋架構中任何控制項，則該授權組態資料會附加至下列控制項的證據：5.0 - 其他授權的客戶管理授權。

AWS 基礎安全最佳實務

AWS Audit Manager 提供預先打造的標準架構，以支援 AWS 基礎安全性最佳實務。

主題

- 什麼是 AWS 基礎安全最佳實務標準？
- 使用此架構幫助您進行稽核準備
- 更多 AWS 基礎安全最佳實務資源

什麼是 AWS 基礎安全最佳實務標準？

AWS 基礎安全最佳實務標準是一組控制項，可在您部署的帳戶和資源偏離安全最佳實務時進行偵測。

您可以使用該標準持續評估您所有的 AWS 帳戶 和工作負載，快速識別偏離最佳實務的區域。標準提供了可採取動作和規範式的引導，讓您了解如何改善和維護組織的安全狀態。

控制項包含橫跨多個 AWS 服務 的最佳實務。系統會為每個控制項指派一個類別，以反映其套用的安全性功能。如需詳細資訊，請參閱AWS Security Hub使用者指南的控制類別。

使用此架構幫助您進行稽核準備

您可以使用AWS基礎安全性最佳實務架構，協助您為稽核做好準備。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據AWS基礎安全最佳實務需求分組到控制集中。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與您的稽核相關的證據。您建立評估之後，Audit Manager 會開始評估您的 AWS 帳戶 資源和服務。其根據AWS基礎安全性最佳實務架構中定義的控制項來執行此操作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

AWS基礎安全最佳實務架構詳細資訊如下：

AWS Audit Manager 內的架構名稱	自動化控制項數量	手動控制項數量	控制集數	AWS 服務 在範圍內
AWS 基礎安全最佳實務	154	0	29	AWS Security Hub

AWS Audit Manager 架構中的此控制項，並非為了驗證您的系統是否符合 AWS 基礎安全最佳實務而設計。因此，其無法保證您會通過AWS基礎安全最佳實務的稽核。

您可以在 Audit Manager 架構程式庫 的標準架構索引標籤下，找到這個架構。

如需使用此架構建立評估方式的說明，請參閱 建立評估。

當您使用 Audit Manager 主控台從此標準架構建立評估時，範圍AWS 服務內的清單會被預設為選擇狀態且不可編輯。這是因為 Audit Manager 會自動為您映射並選擇資料來源和服務。此選項是根據 AWS

基礎安全最佳實務的需求所進行。如果您需要編輯此架構範圍內的服務清單，可以使用建立評估或更新評估 API操作來進行編輯。或者，您可以自訂標準架構，然後從自訂架構中建立評估。

如需自訂此架構以支援您特定需求的指引，請參閱自訂現有架構和自訂現有控制項。

更多 AWS 基礎安全最佳實務資源

- AWS Security Hub使用者指南 中的 AWS 基礎最佳實務標準
- AWS Security Hub使用者指南中的控制項類別

AWS 操作最佳實務

AWS Audit Manager 提供預先打造的 AWS操作最佳實務 (OBP) 架構，協助您進行稽核準備。此架構提供AWS基礎安全最佳實務標準的控制項子集。這些控制項可做為基準檢查，以偵測您部署的帳戶和資源是否偏離了安全最佳實務。

主題

- 什麼是 AWS 基礎安全最佳實務標準？
- 使用此架構幫助您進行稽核準備
- 更多 AWS OBP 資源

什麼是 AWS 基礎安全最佳實務標準？

您可以使用AWS基礎安全最佳實務標準來評估您的帳戶和工作負載，並快速找出偏離最佳實務的區域。標準提供了可採取動作和規範式的引導，讓您了解如何改善和維護組織的安全狀態。

控制項包含橫跨多個 AWS 服務 的最佳實務。系統會為每個控制項指派一個類別，以反映其套用的安全性功能。如需詳細資訊，請參閱AWS Security Hub使用者指南的控制類別。

使用此架構幫助您進行稽核準備

您可以使用AWS操作最佳實務架構，協助您為稽核做好準備。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據AWS操作最佳實務需求分組到控制集中。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與您的稽核相關的證據。您建立評估之後，Audit Manager 會開始評估您的 AWS 帳戶 資源和服務。其根據 AWS 操作最佳實務架構中定義的控制項來執行此操作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集

的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

AWS操作最佳實務架構詳細資訊如下：

AWS Audit Manager 內的架構名稱	自動化控制項數量	手動控制項數量	控制集數	AWS 服務 在範圍內
AWS 操作最佳實務	52	0	20	AWS Security Hub

此架構中的控制項，並非為了驗證您的系統是否符合 AWS 操作最佳實務而設計。因此，其無法保證您會通過AWS操作最佳實務的稽核。

您可以在 Audit Manager 架構程式庫 的標準架構索引標籤下，找到這個架構。

如需使用此架構建立評估方式的說明，請參閱 建立評估。

當您使用 Audit Manager 主控台從此標準架構建立評估時，範圍AWS 服務內的清單會被預設為選擇狀態且不可編輯。這是因為 Audit Manager 會自動為您映射並選擇資料來源和服務。此選項是根據 AWS 操作最佳實務的需求所進行。如果您需要編輯此架構範圍內的服務清單，可以使用建立評估或更新評估API操作來進行編輯。或者，您可以自訂標準架構，然後從自訂架構中建立評估。

如需自訂此架構以支援您特定需求的指引，請參閱自訂現有架構和自訂現有控制項。

更多 AWS OBP 資源

- AWS Security Hub使用者指南 中的 AWS 基礎最佳實務標準
- AWS Security Hub使用者指南中的控制項類別

AWS Well-Architected

AWS Audit Manager 根據 AWS 最佳實務提供預先建置的架構，可建構並自動化AWS Well-Architected架構之評估。

主題

- 什麼是 AWS Well-Architected？

- 使用此架構幫助您進行稽核準備
- 更多 AWS Well-Architected 資源

什麼是 AWS Well-Architected？

AWS Well-Architected 是一種架構，可協助您針對應用程式和工作負載打造安全、高效能、具彈性且有效率的基礎架構。AWS Well-Architected 是以六個支柱 (卓越營運、安全性、可靠性、效能效率、成本最佳化和永續性) 為中心而打造的，其可為您和您的合作夥伴提供一致的方法，來評估架構並實作可擴展的設計。

使用此架構幫助您進行稽核準備

您可以使用AWS Well-Architected 架構來協助您準備稽核。此架構說明在雲端中設計和執行工作負載的重要概念、設計原則和結構方面的最佳實務。在 AWS Well-Architected 的六大支柱中，AWS Audit Manager 為安全性和可靠性提供預先建置架構和控制項的支柱。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與您的稽核相關的證據。您建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據AWS Well-Architected 架構中定義的控制項來執行此動作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

AWSWell-Architected 架構詳細資訊如下：

AWS Audit Manager 內的架構名稱	自動化控制項數量	手動控制項數量	控制集數	AWS 服務 在範圍內
AWS Well-Architected 架構	16	0	2	AWS Config

> **Tip**
>
> 如果檢閱在此標準架構中，當成資料來源對應的 AWS Config 規則，請下載 AuditManager_ConfigDataSourceMappings_AWSWell-ArchitectedFramework.zip 檔案。

此架構中的控制項，並非為了驗證您的系統是否合規而設計。因此，其無法保證您會通過與 AWS Well-Architected 架構相關的審核。

您可以在 Audit Manager 架構程式庫 的標準架構索引標籤下，找到這個架構。

如需使用此架構建立評估方式的說明，請參閱 建立評估。

當您使用 Audit Manager 主控台從此標準架構建立評估時，範圍AWS 服務內的清單會被預設為選擇狀態且不可編輯。這是因為 Audit Manager 會自動為您映射並選擇資料來源和服務。此選擇是根據AWS Well-Architected 架構的要求所進行。如果您需要編輯此架構範圍內的服務清單，可以使用建立評估或更新評估 API操作來進行編輯。或者，您可以自訂標準架構，然後從自訂架構中建立評估。

如需自訂此架構以支援您特定需求的指引，請參閱自訂現有架構和自訂現有控制項。

更多 AWS Well-Architected 資源

- AWS Well-Architected
- AWSWell-Architected 架構文件

加拿大網路安全中心中型雲端控制設定檔

AWS Audit Manager 提供預先打造的標準架構，為加拿大網路安全中心建置和自動化評估。

主題

- 什麼是加拿大網路安全中心？
- 使用此架構幫助您進行稽核準備

什麼是加拿大網路安全中心？

加拿大網路安全中心 (CCCS) 是加拿大網路安全專家指導、服務和支援的權威來源。CCCS 為加拿大政府、工業界和公眾提供此專業知識。全國各地的加拿大公共部門組織都依賴他們對雲端服務供應商的嚴格評估，以做出明智的雲端採購決策。

CCCS 中型雲端控制設定檔於 2020 年 5 月，取代加拿大 PROTECTED B/中等完整性/中等可用性 (PBMM) 設定檔的使用。如果您的組織使用公有雲服務來支援具有中等機密性、完整性和可用性 (AIC) 要求的業務活動，則 CCCS 中型雲端安全控制設定檔適合您使用。具有中等 AIC 要求的工作負載，代表未經授權揭露、修改或對業務活動所使用的資訊或服務的訪問，可以合理預期會對個人或組織造成嚴重傷害，或對一組個人群體造成有限的傷害。這些傷害程度的範例如下：

- 對年度利潤的重大影響
- 失去主要客戶
- 商譽損失
- 明確違反合規
- 數百人或成千上萬人的隱私侵犯
- 影響程式效能
- 導致精神障礙或疾病
- 破壞
- 聲譽受損
- 個人財務困難

使用此架構幫助您進行稽核準備

您可以使用中型雲端控制設定檔的 AWS Audit Manager 架構來協助您準備稽核。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據 CCCS 要求分組成控制集。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與 CCCS Medium Cloud Control Profile 稽核相關的證據。在評估中，您可以指定要包含在稽核範圍中的 AWS 帳戶 和服務。您建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據 CCCS 中型雲端控制設定檔架構中定義的控制項來執行此操作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

架構的詳細資訊如下：

AWS Audit Manager 內的架構名稱	自動化控制項數量	手動控制項數量	控制集數	AWS 服務 在範圍內
加拿大網路安全中心 — 中型	206	396	165	• Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS CloudTrail

AWS Audit Manager 內的架構名稱	自動化控制項數量	手動控制項數量	控制集數	AWS 服務 在範圍內
				• AWS Config • AWS Identity and Access Management • AWS Key Management Service • AWS License Manager

> **Tip**
>
> 如果檢閱在此標準架構中，當成資料來源對應的 AWS Config 規則，請下載 AuditManager_ConfigDataSourceMappings_CanadianCentreforCyberSecurity-Medium.zip 檔案。

此 AWS Audit Manager 架構中的控制項，並非用於驗證您的系統是否符合 CCCS 中型雲端控制設定檔標準。因此，其無法保證您會通過 CCCS 之稽核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控制項。

您可以在 Audit Manager 架構程式庫 的標準架構索引標籤下，找到這個架構。

如需使用此架構建立評估方式的說明，請參閱 建立評估。

當您使用 Audit Manager 主控台從此標準架構建立評估時，範圍AWS 服務內的清單會被預設為選擇狀態且不可編輯。這是因為 Audit Manager 會自動為您映射並選擇資料來源和服務。這個選擇是根據加拿大網路安全中心 — 中型架構的要求進行。如果您需要編輯此架構範圍內的服務清單，可以使用建立評估或更新評估 API操作來進行編輯。或者，您可以自訂標準架構，然後從自訂架構中建立評估。

如需自訂此架構以支援您特定需求的指引，請參閱自訂現有架構和自訂現有控制項。

適用於 CIS Amazon Web Services Foundations Benchmark v1.2.0 的 CIS 基準

AWS Audit Manager 為 CIS AWS Foundations Benchmark v1.2.0 提供兩個預先建置架構：

- 適用於 CIS Amazon Web Services Foundations Benchmark v1.2.0 的 CIS 基準，第 1 級
- 適用於 CIS Amazon Web Services Foundations Benchmark v1.2.0 的 CIS 基準，第 1 和第 2 級

> **Note**
>
> - 如需支援 v1.3.0 之 Audit Manager 架構的相關資訊，請參閱 適用於 CIS Amazon Web Services Foundations Benchmark v1.3.0 的 CIS 基準。
> - 如需支援 v1.4.0 之 Audit Manager 架構的相關資訊，請參閱 適用於 CIS Amazon Web Services Foundations Benchmark v1.4.0 的 CIS 基準。

主題

什麼是 CIS？

網際網路安全中心 (CIS) 是一家開發CIS AWS Foundations Benchmark的非營利組織。這項基準測試為 AWS 提供了一組最佳實務安全性組態。這些業界公認的最佳實務超越了現有的高階安全性指引，其提供清楚明瞭、按部就班的實作和評估程序。

如需詳細資訊，請參閱AWS安全部落格上的CIS AWS Foundations Benchmark 貼文。

CIS 基準和 CIS 控制項之間的區別

CIS 基準是針對供應商產品的安全性最佳實務指南。從操作系統到雲端服務和網路裝置，基準測試套用的設定可保護貴組織使用的特定系統。CIS 控制項是組織層級系統的基本最佳實務指南，以協助防範已知的網路攻擊媒介。

範例

- CIS 基準是一系列的方案。它們通常會參考可在廠商產品中檢閱和配置的特定設定。

  範例：CIS Amazon Web Services Foundations Benchmark v1.2.0-1.13 確保在「根使用者」帳戶啟用 MFA

  這項建議提供有關檢查方式，以及如何在 AWS 環境的根帳戶上進行此設定的方案指引。
- CIS 控制項則是為組織整體提供的建議。它們不是針對單一供應商產品。

  範例：CIS 控制項 7.1 版 - 子控制項 4.5 針對所有管理存取使用多因素驗證

  此控制項描述預期要在組織內套用的項目。它不會說明您應該如何將其應用於正在執行的系統和工作負載中 (無論它們位於何處)。

使用此架構支援您進行稽核準備

您可以在 AWS Audit Manager 中使用 CIS AWS Foundations Benchmark v1.2 架構，幫助您為 CIS 稽核做好準備。您也可以根據特定需求自訂這些架構和他們的控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與稽核相關的證據。您建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據 CIS 架構中定義的控制項來執行此動作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

架構的詳細資訊如下：

AWS Audit Manager 內的架構名稱	自動化控制項數量	手動控制項數量	控制集數	AWS 服務 在範圍內
適用於 CIS Amazon Web Services Foundations Benchmark v1.2.0 的 CIS 基準，第 1 級	33	3	4	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Identity and Access Management

AWS Audit Manager 內的架構名稱	自動化控制項數量	手動控制項數量	控制集數	AWS 服務 在範圍內
				• AWS Security Hub
適用於 CIS Amazon Web Services Foundations Benchmark，v1.2.0 的 CIS 基準，第 1 和 2 級	45	4	4	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Identity and Access Management • AWS Security Hub

此架構中的控制項，並非為了驗證您的系統是否符合 CIS 標準所設計。此外，他們無法保證您會透過 CIS 之稽核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控制項。

您可以在 Audit Manager 架構程式庫 的標準架構索引標籤下，找到這些架構。

如需使用這些架構建立評估方式的說明，請參閱 建立評估。

當您使用 Audit Manager 主控台從這些標準架構建立評估時，範圍AWS 服務內的清單會被預設為選取狀態。這是因為 Audit Manager 會自動為您映射並選擇資料來源和服務。此選擇是根據 CIS 基準的要求所進行。如果您需要編輯這些架構範圍內的服務清單，可以使用CreateAssessment或UpdateAssessment API 作業來進行編輯。或者，您可以自訂標準架構，然後從自訂架構中建立評估。

如需自訂這些架構以支援您特定需求的指引，請參閱自訂現有架構和自訂現有控制項。

使用這些架構的先決條件

CIS AWS Foundations Benchmark v1.2 架構中的許多控制項，使用 AWS Config 作為資料來源類型。如果支援這些控制項，您必須在每個AWS 區域已啟用 Audit Manager 的所有帳號上啟用 AWS Config。您也必須確定已啟用特定 AWS Config 規則，且這些規則已正確設定。

為了收集正確的證據並獲取 CIS AWS Foundations Benchmark v1.2 準確合規狀態，您需要以下 AWS Config 規則和參數。如需如何啟用或配置規則的指示，請參閱使用AWS Config受管規則。

必要 AWS Config 規則	必要參數
ACCESS_KEYS_ROTATED	**maxAccessKeyAge** • 沒有輪換的最大天數。 • 類型：Int • 預設：90 天 • 合規要求：最多 90 天
CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED	不適用
CLOUD_TRAIL_ENCRYPTION_ENABLED	不適用
CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED	不適用
CMK_BACKING_KEY_ROTATION_ENABLED	不適用
IAM_PASSWORD_POLICY	**MaxPasswordAge** (選用) • 密碼過期前的天數。 • 類型：int • 預設：90 • 合規要求：最多 90 天
IAM_PASSWORD_POLICY	**MinimumPasswordLength** (選用) • 密碼的長度下限。 • 類型：int • 預設：14 • 合規要求：至少 14 字元
IAM_PASSWORD_POLICY	**PasswordReusePrevention** (選用) • 允許重複使用的密碼次數。 • 類型：int

必要 AWS Config 規則	必要參數
	• 預設：24 • 合規要求：重複使用前至少經過 24 個密碼
IAM_PASSWORD_POLICY	**RequireLowercaseCharacters** (選用) • 密碼至少必須包含一個小寫字元。 • 類型：布林值 • 預設：True • 合規要求：至少有一個小寫字元
IAM_PASSWORD_POLICY	**RequireNumbers** (選用) • 密碼至少必須包含一個數字。 • 類型：布林值 • 預設：True • 合規要求：至少有一個數字字元
IAM_PASSWORD_POLICY	**RequireSymbols** (選用) • 密碼至少必須包含一個符號。 • 類型：布林值 • 預設：True • 合規要求：至少有一個符號字元
IAM_PASSWORD_POLICY	**RequireUppercaseCharacters** (選用) • 密碼至少必須包含一個大寫字元。 • 類型：布林值 • 預設：True • 合規要求：至少有一個大寫字元

必要 AWS Config 規則	必要參數
IAM_POLICY_IN_USE	**policyARN** • 要檢查的 IAM 政策 ARN。 • 類型：字串 • 合規要求：建立 IAM 角色以管理 AWS 事件。 **policyUsageType** (選用) • 指定應將政策連接到使用者、群組或角色。 • 類型：字串 • 有效值：IAM_USER | IAM_GROUP | IAM_ROLE | ANY • 預設值：ANY • 合規要求：將信任政策連結到建立的 IAM 角色
IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS	不適用
IAM_ROOT_ACCESS_KEY_CHECK	不適用
IAM_USER_NO_POLICIES_CHECK	不適用
IAM_USER_UNUSED_CREDENTIALS_CHECK	**maxCredentialUsageAge** • 無法使用憑證的最大天數。 • 類型：Int • 預設：90 天 • 合規要求：90 天以上
INCOMING_SSH_DISABLED	不適用
MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS	不適用
MULTI_REGION_CLOUD_TRAIL_ENABLED	不適用

必要 AWS Config 規則	必要參數
RESTRICTED_INCOMING_TRAFFIC	**blockedPort1** (選用) • 已封鎖的 TCP 連接埠號碼。 • 類型：int • 預設：20 • 合規要求：確保沒有安全群組允許在封鎖的連接埠上進行傳入 **blockedPort2** (選用) • 已封鎖的 TCP 連接埠號碼。 • 類型：int • 預設：21 • 合規要求：確保沒有安全群組允許在封鎖的連接埠上進行傳入 **blockedPort3** (選用) • 已封鎖的 TCP 連接埠號碼。 • 類型：int • 預設：3389 • 合規要求：確保沒有安全群組允許在封鎖的連接埠上進行傳入 **blockedPort4** (選用) • 已封鎖的 TCP 連接埠號碼。 • 類型：int • 預設：3306 • 合規要求：確保沒有安全群組允許在封鎖的連接埠上進行傳入 **blockedPort5** (選用) • 已封鎖的 TCP 連接埠號碼。 • 類型：int • 預設：4333

必要 AWS Config 規則	必要參數
	• 合規要求：確保沒有安全群組允許在封鎖的連接埠上進行傳入
ROOT_ACCOUNT_HARDWARE_MFA_ENABLED	不適用
ROOT_ACCOUNT_MFA_ENABLED	不適用
S3_BUCKET_LOGGING_ENABLED	**targetBucket** （選用） • 儲存伺服器存取日誌的目標 S3 儲存貯體。 • 類型：字串 • 合規要求：啟用日誌 **targetPrefix** （選用） • 儲存伺服器存取日誌的 S3 儲存貯體的字首。 • 類型：字串 • 合規要求：找出適用於 CloudTrail 紀錄的 S3 儲存貯體
S3_BUCKET_PUBLIC_READ_PROHIBITED	不適用
VPC_DEFAULT_SECURITY_GROUP_CLOSED	不適用
VPC_FLOW_LOGS_ENABLED	**trafficType** （選用） • 流程日記的 `trafficType` 。 • 類型：字串 • 合規要求：已啟用流程日誌

其他 CIS 資源

- The CIS AWS Foundations Benchmark v1.2.0
- CIS AWS Foundations BenchmarkAWS安全部落格貼文

適用於 CIS Amazon Web Services Foundations Benchmark v1.3.0 的 CIS 基準

AWS Audit Manager 為 CIS AWS Foundations Benchmark v.1.3 提供兩個預先建置架構：

- 適用於 CIS Amazon Web Services Foundations Benchmark v1.3.0 的 CIS 基準，第 1 級
- 適用於 CIS Amazon Web Services Foundations Benchmark v1.3.0 的 CIS 基準，第 1 級和 2 級

> **Note**
>
> 有關 CIS AWS Foundations Benchmark v1.2.0 以及支援此版本基準測試的 AWS Audit Manager 架構資訊，請參閱 適用於 CIS Amazon Web Services Foundations Benchmark v1.2.0 的 CIS 基準。

主題

什麼是 CIS？

網際網路安全中心 (CIS) 開發了CIS AWS Foundations Benchmark v1.3.0，其為一組用於 AWS 安全配置的最佳實務。這些業界公認的最佳實務超越了現有的高階安全性指引，其為 AWS 使用者提供清楚明瞭、按部就班的實作和評估程序。

如需詳細資訊，請參閱AWS安全部落格上的CIS AWS Foundations Benchmark 貼文。

CIS AWS Foundations Benchmark v1.3.0 提供為 AWS 服務 子集設定安全選項的指引，其將基礎、可測試和體系結構不可知的設定做為重點。本文件部分特定 Amazon Web Services 範圍包含以下項目：

- AWS Identity and Access Management (IAM)
- AWS Config
- AWS CloudTrail
- Amazon CloudWatch

- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Storage Service (Amazon S3)
- Amazon Virtual Private Cloud (預設)

CIS 基準和 CIS 控制項之間的區別

CIS 基準是針對供應商產品的安全性最佳實務指南。從操作系統到雲端服務和網路裝置，基準套用的設定可保護貴組織使用的系統。CIS 控制項是基本最佳實務指南，供組織遵循以協助防範已知的網路攻擊媒介。

範例

- CIS 基準是一系列的方案。它們通常會參考可在廠商產品中檢閱和配置的特定設定。

  範例：CIS Amazon Web Services Foundations Benchmark v1.3.0-1.5 確保在「根使用者」帳戶啟用 MFA

  這項建議提供有關檢查方式，以及如何在 AWS 環境的根帳戶上進行此設定的方案指引。
- CIS 控制項適用於您的組織整體，而不是只針對單一供應商產品。

  範例：CIS 控制項 7.1 版 - 子控制項 4.5 針對所有管理存取使用多因素驗證

  此控制項會說明組織內預期套用的項目，但不會說明您應該如何將其應用於正在執行的系統和工作負載中 (無論它們位於何處)。

使用此架構支援您進行稽核準備

您可以在 AWS Audit Manager 中使用 CIS AWS Foundations Benchmark v1.3 架構，幫助您為 CIS 稽核做好準備。您也可以根據特定需求自訂這些架構和他們的控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與稽核相關的證據。您建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據 CIS 架構中定義的控制項來執行此動作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

架構的詳細資訊如下：

AWS Audit Manager 內的架構名稱	自動化控制項數量	手動控制項數量	控制集數	AWS 服務 在範圍內
適用於 CIS Amazon Web Services Foundations Benchmark v1.3.0 的 CIS 基準，第 1 級	33	5	6	• Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS Config • AWS CloudTrail • AWS Identity and Access Management • AWS Security Hub
適用於 CIS Amazon Web Services Foundations Benchmark v1.3.0 的 CIS 基準，第 1 級和 2 級	49	6	6	• Amazon Elastic Compute Cloud • Amazon CloudWatch • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

Tip

若要檢閱用來做為這些標準架構之資料來源映射項目的 AWS Config 規則清單，請下載下列檔案：

- AuditManager_ConfigDataSourceMappings_CIS-Benchmark-v1.3.0-Level-1.zip

- AuditManager_ConfigDataSourceMappings_CIS-Benchmark-v1.3.0,Level1-and-2.zip

此架構中的控制項，並非為了驗證您的系統是否符合 CIS 標準所設計。此外，他們無法保證您會透過 CIS 之稽核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控制項。

您可以在 Audit Manager 架構程式庫 的標準架構索引標籤下，找到這些架構。

如需使用這些架構建立評估方式的說明，請參閱 建立評估。

當您使用 Audit Manager 主控台從這些標準架構建立評估時，範圍AWS 服務內的清單會被預設為選取狀態。這是因為 Audit Manager 會自動為您映射並選擇資料來源和服務。此選擇是根據 CIS 基準的要求所進行。如果您需要編輯這些架構範圍內的服務清單，可以使用CreateAssessment或UpdateAssessment API 作業來進行編輯。或者，您可以自訂標準架構，然後從自訂架構中建立評估。

如需自訂這些架構以支援您特定需求的指引，請參閱自訂現有架構和自訂現有控制項。

其他 CIS 資源

- CIS AWS Foundations BenchmarkAWS安全部落格貼文

適用於 CIS Amazon Web Services Foundations Benchmark v1.4.0 的 CIS 基準

AWS Audit Manager 為網路安全中心 (CIS) AWS Foundations Benchmark v1.4.0 提供兩個預先建置標準架構：

- 適用於 CIS Amazon Web Services Foundations Benchmark v1.4.0 的 CIS 基準，第 1 級
- 適用於 CIS Amazon Web Services Foundations Benchmark v1.4.0 的 CIS 基準，第 1 級和 2 級

> **Note**
>
> - 如需支援 v1.2.0 之 Audit Manager 架構的相關資訊，請參閱 適用於 CIS Amazon Web Services Foundations Benchmark v1.2.0 的 CIS 基準。
> - 如需支援 v1.3.0 之 Audit Manager 架構的相關資訊，請參閱 適用於 CIS Amazon Web Services Foundations Benchmark v1.3.0 的 CIS 基準。

主題

什麼是適用於 CIS Amazon Web Services Foundations Benchmark v1.4.0 的 CIS 基準？

適用於 CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.4.0 的 CIS 基準，第 1 級和 2 級為設定 Amazon Web Services 子集安全選項提供了方案指引。其將基礎、可測試和體系結構不可知的設定做為重點。本文件部分特定 Amazon Web Services 範圍包含以下項目：

- AWS Identity and Access Management (IAM)
- IAM Access Analyzer
- AWS Config
- AWS CloudTrail
- Amazon CloudWatch
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Storage Service (Amazon S3)
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Relational Database Service (Amazon RDS)
- Amazon Virtual Private Cloud

CIS 基準和 CIS 控制項之間的區別

CIS 基準是針對供應商產品的安全性最佳實務指南。從操作系統到雲端服務和網路裝置，基準測試套用的設定可保護正在使用的系統。CIS 控制項是基本最佳實務指南，供組織遵循以協助防範已知的網路攻擊媒介。

範例

- CIS 基準是一系列的方案。它們通常會參考可在廠商產品中檢閱和配置的特定設定。

  範例：CIS Amazon Web Services Foundations Benchmark v1.4.0-1.5 確保在「根使用者」帳戶啟用 MFA

這項建議提供有關檢查方式，以及如何在 AWS 環境的根帳戶上進行此設定的方案指引。

- CIS 控制項適用於您的組織整體，而不是只針對單一供應商產品。

  範例：CIS 控制項 7.1 版 - 子控制項 4.5 針對所有管理存取使用多因素驗證

  此控制項描述預期要在組織內套用的項目。然而，它不會說明您應該如何將其應用於正在執行的系統和工作負載中 (無論它們位於何處)。

使用此架構支援您進行稽核準備

您可以在 AWS Audit Manager 中使用 CIS AWS Foundations Benchmark v1.4.0 架構，幫助您為 CIS 稽核做好準備。您也可以根據特定需求自訂這些架構和他們的控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與稽核相關的證據。您建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據 CIS 架構中定義的控制項來執行此動作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

架構的詳細資訊如下：

AWS Audit Manager 內的架構名稱	自動化控制項數量	手動控制項數量	控制集數	AWS 服務 在範圍內
適用於 CIS Amazon Web Services Foundations Benchmark v1.4.0 的 CIS 基準，第 1 級	32	6	7	• Amazon Elastic Compute Cloud • Amazon CloudWatch • AWS CloudTrail • AWS Config • AWS Identity and Access Management
適用於 CIS Amazon Web Services Foundatio	50	8	7	• Amazon Elastic Compute Cloud

AWS Audit Manager 內的架構名稱	自動化控制項數量	手動控制項數量	控制集數	AWS 服務 在範圍內
ns Benchmark v1.4.0 的 CIS 基準，第 1 級和 2 級				• Amazon CloudWatch • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> 若要檢閱用來做為這些標準架構之資料來源映射項目的 AWS Config 規則清單，請下載下列檔案：
>
> - AuditManager_ConfigDataSourceMappings_CIS-Benchmark-v1.4.0-Level-1.zip
> - AuditManager_ConfigDataSourceMappings_CIS-Benchmark-v1.4.0-Level-1-and-2.zip

這些架構中的控制項，並非用來驗證您的系統是否符合適用於 CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.4.0 標準的 CIS 基準。此外，他們無法保證您會透過 CIS 之稽核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控制項。

您可以在 Audit Manager 架構程式庫 的標準架構索引標籤下，找到這些架構。

如需使用這些架構建立評估方式的說明，請參閱 建立評估。

當您使用 Audit Manager 主控台從這些標準架構建立評估時，範圍AWS 服務內的清單會被預設為選取狀態。這是因為 Audit Manager 會自動為您映射並選擇資料來源和服務。此選擇是根據 CIS 基準的要求所進行。如果您需要編輯這些架構範圍內的服務清單，可以使用CreateAssessment或UpdateAssessment API 作業來進行編輯。或者，您可以自訂標準架構，然後從自訂架構中建立評估。

如需自訂這些架構以支援您特定需求的指引，請參閱自訂現有架構和自訂現有控制項。

其他 CIS 資源

- Center for Internet Security的 CIS 基準
- CIS AWS Foundations BenchmarkAWS安全部落格貼文

CIS 控制項 v7.1 Implementation Group 1

AWS Audit Manager 為網際網路安全中心 (CIS) 控制項 v7.1 Implementation Group 1 提供一個預先建置的架構。

> **Note**
>
> 如需 CIS 控制項 v8 IG1 與支援此標準之 AWS Audit Manager 架構相關資訊，請參閱 CIS 控制項 v8 Implementation Group 1。

AWS Audit Manager 提供支援網際網路安全中心 (CIS)的預先建置架構，協助您進行稽核準備。

主題

- 什麼是 CIS 控制項？
- 使用此架構幫助您進行稽核準備
- 其他 CIS 資源

什麼是 CIS 控制項？

CIS 控制項是一套優先級的行動方針，其可視為深度防禦的最佳實務行動集。這些最佳實務行動可紓解針對系統和網路的最普遍的網路攻擊。Implementation Group 1 通常是針對資源與網路安全專業知識有限的組織所設計，其在子控制項的實施部分需要進一步協助。

CIS 控制項和 CIS 基準之間的區別

CIS 控制項是基本最佳實務指南，組織可遵循這些指南防範已知的網路攻擊媒介。CIS 基準是針對供應商產品的安全最佳實務指南。從操作系統到雲端服務和網路裝置，基準測試套用的設定可保護使用的系統。

範例

- CIS 基準是一系列的方案。它們通常會參考可在廠商產品中檢閱和配置的特定設定。

  - 範例：CIS Amazon Web Services Foundations Benchmark v1.2.0-1.13 確保在「根使用者」帳戶啟用 MFA。
  - 這項建議提供有關檢查方式，以及如何在 AWS 環境的根帳戶上進行此設定的方案指引。
- CIS 控制項適用於您的組織整體，而不是只針對單一供應商產品。
  - 範例：CIS 控制項 7.1 版 - 子控制項 4.5 針對所有管理存取使用多因素驗證
  - 此控制項描述預期要在組織內套用的項目。它不會告知您應該如何將其應用於正在執行的系統和工作負載中 (無論它們位於何處)。

使用此架構幫助您進行稽核準備

您可以使用CIS 控制項 v7.1 IG1 架構來幫助您準備審核。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據 CIS 要求分組成控制集。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與您的稽核相關的證據。您建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據 CIS Controls v7.1 IG1 架構中定義的控制項來執行此動作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

CIS 控制項 v7.1 IG1 架構的詳細資訊如下：

AWS Audit Manager 內的架構名稱	自動化控制項數量	手動控制項數量	控制集數	AWS 服務 在範圍內
CIS 控制項 v7.1 IG1	21	22	16	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Managemen t

> **Tip**
>
> 如果檢閱在此標準架構中，當成資料來源對應的 AWS Config 規則，請下載 AuditManager_ConfigDataSourceMappings_CIS-Controls-v7.1-IG1.zip 檔案。

此架構中的控制項，並非為了驗證您的系統是否符合 CIS 控制項所設計。此外，他們無法保證您會透過 CIS 之稽核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控制項。

您可以在 Audit Manager 架構程式庫 的標準架構索引標籤下，找到這個架構。

如需使用此架構建立評估方式的說明，請參閱 建立評估。

當您使用 Audit Manager 主控台從此標準架構建立評估時，範圍AWS 服務內的清單會被預設為選擇狀態且不可編輯。這是因為 Audit Manager 會自動為您映射並選擇資料來源和服務。此選擇是根據 CIS 控制項的要求所進行。如果您需要編輯此架構範圍內的服務清單，可以使用建立評估或更新評估 API操作來進行編輯。或者，您可以自訂標準架構，然後從自訂架構中建立評估。

如需自訂此架構以支援您特定需求的指引，請參閱自訂現有架構和自訂現有控制項。

其他 CIS 資源

- CIS 控制項 v7.1 IG1

CIS 控制項 v8 Implementation Group 1

AWS Audit Manager 為網際網路安全中心 (CIS) 控制項 v8 Implementation Group 1 提供一個預先建置的架構。

> **Note**
>
> 如需 CIS 控制項 v7.1 IG1 與支援此標準之 AWS Audit Manager 架構相關資訊，請參閱 CIS 控制項 v7.1 Implementation Group 1。

主題

- 什麼是 CIS 控制項？
- 使用此架構幫助您進行稽核準備

- 其他 CIS 資源

什麼是 CIS 控制項？

CIS 關鍵安全控制 (CIS Controls) 是一套優先級的保護措施，可紓解針對系統和網路的最普遍的網路攻擊。它們被映射並引用到多款法律、監管和政策架構中。CIS 控制項 v8 已進行增強，以跟上現代系統和軟體的步伐。雲端運算、虛擬化、行動化、外包、在家工作以及不斷變化的攻擊者策略等趨勢，促使其跟著更新。此項更新支援企業移至完全雲端和混合式環境時的安全性。

CIS 控制項和 CIS 基準之間的區別

CIS 控制項是基本最佳實務指南，組織可遵循這些指南防範已知的網路攻擊媒介。CIS 基準是針對供應商產品的安全最佳實務指南。從操作系統到雲端服務和網路裝置，基準測試套用的設定可保護使用的系統。

範例

- CIS 基準是一系列的方案。它們通常會參考可在廠商產品中檢閱和配置的特定設定。
  - 範例：CIS Amazon Web Services Foundations Benchmark v1.2.0-1.13 確保在「根使用者」帳戶啟用 MFA。
  - 這項建議提供有關檢查方式，以及如何在 AWS 環境的根帳戶上進行此設定的方案指引。
- CIS 控制項適用於您的組織整體，而不是只針對單一供應商產品。
  - 範例：CIS 控制項 7.1 版 - 子控制項 4.5 針對所有管理存取使用多因素驗證
  - 此控制項描述預期要在組織內套用的項目。它不會告知您應該如何將其應用於正在執行的系統和工作負載中 (無論它們位於何處)。

使用此架構幫助您進行稽核準備

您可以使用CIS 控制項 v8 IG1 架構來幫助您準備審核。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據 CIS 要求分組成控制集。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與您的稽核相關的證據。您建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據 CIS 控制項 v8 架構中定義的控制項來執行此動作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

CIS 控制項 v8 架構的詳細資訊如下：

AWS Audit Manager 內的架構名稱	自動化控制項數量	手動控制項數量	控制集數	AWS 服務 在範圍內
CIS 控制項 v8 IG1	25	31	15	• Amazon Elastic Compute Cloud • AWS Config • AWS Identity and Access Management • AWS License Manager

> **Tip**
>
> 如果檢閱在此標準架構中，當成資料來源對應的 AWS Config 規則，請下載 AuditManager_ConfigDataSourceMappings_CIS-Controls-v8-IG1.zip 檔案。

此架構中的控制項，並非為了驗證您的系統是否符合 CIS 控制項所設計。此外，他們無法保證您會透過 CIS 之稽核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控制項。

您可以在 Audit Manager 架構程式庫 的標準架構索引標籤下，找到這個架構。

如需使用此架構建立評估方式的說明，請參閱 建立評估。

當您使用 Audit Manager 主控台從此標準架構建立評估時，範圍AWS 服務內的清單會被預設為選擇狀態且不可編輯。這是因為 Audit Manager 會自動為您映射並選擇資料來源和服務。此選擇是根據 CIS 控制項的要求所進行。如果您需要編輯此架構範圍內的服務清單，可以使用建立評估或更新評估 API操作來進行編輯。或者，您可以自訂標準架構，然後從自訂架構中建立評估。

如需自訂此架構以支援您特定需求的指引，請參閱自訂現有架構和自訂現有控制項。

其他 CIS 資源

- CIS 控制項 v8

FedRAMP 基礎

AWS Audit Manager提供 FedRAMP 基礎架構，協助您準備稽核。

主題

什麼是 FedRAMP？

聯邦風險與授權管理計劃 (FedRAMP) 於 2011 年成立。其為美國聯邦政府施行和使用雲端服務，提供符合成本效益、以風險評估為基礎的方法。FedRAMP 讓聯邦機構能夠使用現代雲端技術，並著重於聯邦資訊的安全性和保護性。

如需 FedRAMP 仲裁基準控制項的詳細資訊，請參閱 FedRAMP 基礎安全性測試案例程序範本。

使用此架構幫助您進行稽核準備

您可以使用 FedRAMP 基礎架構來協助您準備稽核。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據 FedRAMP 要求分組成控制集。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與您的稽核相關的證據。您建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據架構中定義的控制項來執行此動作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

FedRAMP 基礎架構的詳細資料如下：

AWS Audit Manager 內的架構名稱	自動化控制項數量	手動控制項數量	控制集數	AWS 服務 在範圍內
FedRAMP 基礎	303	908	325	• Amazon Elastic Compute Cloud • AWS Config

AWS Audit Manager 內的架構名稱	自動化控制項數量	手動控制項數量	控制集數	AWS 服務 在範圍內
				• AWS Identity and Access Management

> **Tip**
>
> 如果檢閱在此標準架構中，當成資料來源對應的 AWS Config 規則，請下載 AuditManager_ConfigDataSourceMappings_FedRAMP-Moderate-Baseline.zip 檔案。

此架構中的控制項，並非為了驗證您的系統是否符合 FedRAMP 所設計。此外，他們無法保證您會透過 FedRAMP 之稽核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控制項。

您可以在 Audit Manager 架構程式庫 的標準架構索引標籤下，找到這個架構。

如需使用此架構建立評估方式的說明，請參閱 建立評估。

當您使用 Audit Manager 主控台從此標準架構建立評估時，範圍AWS 服務內的清單會被預設為選擇狀態且不可編輯。這是因為 Audit Manager 會自動為您映射並選擇資料來源和服務。此選擇是根據 FedRAMP 基礎的需求所進行。如果您需要編輯此架構範圍內的服務清單，可以使用建立評估或更新評估 API操作來進行編輯。或者，您可以自訂標準架構，然後從自訂架構中建立評估。

如需自訂此架構以支援您特定需求的指引，請參閱自訂現有架構和自訂現有控制項。

更多 FedRAMP 資源

- AWSFedRAMP 的合規頁面
- AWSFedRAMP 部落格貼文

一般資料保護規則 (GDPR)

AWS Audit Manager 提供預先建立的標準架構，支援一般資料保護規則 (GDPR)。根據預設設定，此架構只包含手動控制項。這些手動控制不會自動收集證據。不過，如果您想要自動化收集 GDPR 下某些控制項的證據，您可以使用 AWS Audit Manager 中的自訂控制項功能。如需更多詳細資訊，請參閱使用此架構幫助您進行稽核準備。

主題

什麼是一般資料保護規則 (GDPR)？

一般資料保護規則 (GDPR) 是一項新的歐洲隱私法規，於 2018 年 5 月 25 日實施。GDPR 取代了歐盟資料保護指令，也稱為 95/46/EC 指令。它旨在協調整個歐盟 (EU) 的資料保護法律。其透過實施在整個歐盟成員國具有約束力的單一資料保護法，以實現這項目標。

GDPR 適用於在歐盟設立的所有組織，以及處理歐盟資料當事人提供商品或服務，或歐盟境內行為相關的歐盟資料主體個人資料的組織 (無論它們是否在歐盟建立)。個人資料是任何與已識別或可識別的自然人有關的任何資訊。

您可以在 AWS Audit Manager 的架構程式庫頁面中找到 GDPR 架構。如需詳細資訊，請參閱一般資料保護規則 (GDPR) 中心。

使用此架構幫助您進行稽核準備

您可以使用 AWS Audit Manager 中的 GDPR 架構來協助您準備稽核。

架構的詳細資訊如下：

AWS Audit Manager 內的架構名稱	自動化控制項數量	手動控制項數量	控制集數	AWS 服務 在範圍內
GDPR	0	371	10	無

您可以在 Audit Manager 架構程式庫 的標準架構索引標籤下，找到 GDPR 架構。由於此標準架構僅包含手動控制項，因此範圍內沒有 AWS 服務。

> **Note**
>
> 如果您想要自動化 GDPR 的證據收集作業，可以使用 Audit Manager 來為 GDPR 建立自己的自訂控制項。下表提供有關可在自訂控制項中對應至 GDPR 要求的AWS資料來源建議。雖然下列某些資料來源已對應至多個控制項，但請記住，每次資源評估只需支付一次費用。

下列建議使用 AWS Config 和 AWS Security Hub 做為資料來源。若要成功地從這些資料來源收集證據，請確認執行下列操作：

- 確認您已按照說明在您的 AWS 帳戶 啟用並設置 AWS Config 與 AWS Security Hub。
- 確認您已同時包含 AWS Config 和安全中樞進入服務範圍內。如果檢閱評估範圍內服務清單，請參閱檢閱評估，AWS 服務標籤。若要編輯此清單，請參閱編輯範圍內的 AWS 服務。

以這種方式設定兩種服務之後，每次執行 AWS Config 規則或安全中樞控制項評估時，Audit Manager 都會收集證據。

控制項名稱	控制集	建議控制項資料來源映射項目
第 25 條設計與預設的資料保護 1	第 4 章 - 控制方與處理方	您可以在 AWS Audit Manager 中建立自訂控制項以支援此 GDPR 控制項。 當您指定控制項詳細資訊時，請在測試資訊下輸入下列內容： • 顯示期間內的所有根帳號事件 • AWS CloudTrail儲存貯體不公開 • 顯示具備 `Allow:*:*` 的所有政策，並列出所有使用這些政策的主體和服務 設定控制項資料來源時，建議您將下列所有項目納入資料來源： 選擇 AWS Config 作為資料來源類型，然後選取下列 AWS Config 管理規則作為資料來源映射項目： • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY

控制項名稱	控制集	建議控制項資料來源映射項目
		選擇 AWS Security Hub 作為資料來源類型，然後選擇下列 Security Hub 控制項作為資料來源映射： • 1.1 (CloudWatch.1) • 1.1 (IAM.20) • 1.10 (IAM.16) • 1.11 (IAM.17) • 1.12 (IAM.4) • 1.13 (IAM.9) • 1.14 (IAM.6) • 1.16 (IAM.2) • 1.2 (IAM.5 • 1.20 (IAM.18) • 1.22 (IAM.1 • 1.3 (IAM.8) • 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2.1 (CloudTrail.1) • 2.2 (CloudTrail.4) • 2.3 (CloudTrail.6) • 2.4 (CloudTrail.5) • 2.5 (Config.1) • 2.6 (CloudTrail.7) • 2.7 (CloudTrail.2) • 2.8 (KMS.4)

控制項名稱	控制集	建議控制項資料來源映射項目
		• 2.9 (EC2.6) • 3.1 (CloudWatch.2) • 3.10 (CloudWatch.10) • 3.11 (CloudWatch.11) • 3.12 (CloudWatch.12) • 3.13 (CloudWatch.13) • 3.14 (CloudWatch.14) • Config.1

控制項名稱	控制集	建議控制項資料來源映射項目
第 25 條設計與預設的資料保護 2	第 4 章 - 控制方與處理方	您可以在 AWS Audit Manager 中建立自訂控制項以支援此 GDPR 控制項。 當您指定控制項詳細資訊時，請在測試資訊下輸入下列內容： • 顯示期間內的所有根帳號事件 • AWS CloudTrail儲存貯體不公開 • 顯示具備 `Allow:*:*` 的所有政策，並列出所有使用這些政策的主體和服務 設定控制項資料來源時，建議您將下列所有項目納入資料來源： 選擇 AWS Config 作為資料來源類型，然後選取下列 AWS Config 管理規則作為資料來源映射項目： • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY 選擇 AWS Security Hub 作為資料來源類型，然後選擇下列 Security Hub 控制項作為資料來源映射： • 1.1 (CloudWatch.1) • 1.1 (IAM.20) • 1.10 (IAM.16) • 1.11 (IAM.17) • 1.12 (IAM.4) • 1.13 (IAM.9) • 1.14 (IAM.6)

控制項名稱	控制集	建議控制項資料來源映射項目
		• 1.16 (IAM.2) • 1.2 (IAM.5 • 1.20 (IAM.18) • 1.22 (IAM.1 • 1.3 (IAM.8) • 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2.1 (CloudTrail.1) • 2.2 (CloudTrail.4) • 2.3 (CloudTrail.6) • 2.4 (CloudTrail.5) • 2.5 (Config.1) • 2.6 (CloudTrail.7) • 2.7 (CloudTrail.2) • 2.8 (KMS.4) • 2.9 (EC2.6) • 3.1 (CloudWatch.2) • 3.10 (CloudWatch.10) • 3.11 (CloudWatch.11) • 3.12 (CloudWatch.12) • 3.13 (CloudWatch.13) • 3.14 (CloudWatch.14) • Config.1

控制項名稱	控制集	建議控制項資料來源映射項目
第 25 條設計與預設的資料保護 3	第 4 章 - 控制方與處理方	您可以在 AWS Audit Manager 中建立自訂控制項以支援此 GDPR 控制項。 當您指定控制項詳細資訊時，請在測試資訊下輸入下列內容： • 顯示期間內的所有根帳號事件 • AWS CloudTrail儲存貯體不公開 • 顯示具備 `Allow:*:*` 的所有政策，並列出所有使用這些政策的主體和服務 設定控制項資料來源時，建議您將下列所有項目納入資料來源： 選擇 AWS Config 作為資料來源類型，然後選取下列 AWS Config 管理規則作為資料來源映射項目： • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY 選擇 AWS Security Hub 作為資料來源類型，然後選擇下列 Security Hub 控制項作為資料來源映射： • 1.1 (CloudWatch.1) • 1.1 (IAM.20) • 1.10 (IAM.16) • 1.11 (IAM.17) • 1.12 (IAM.4) • 1.13 (IAM.9) • 1.14 (IAM.6)

控制項名稱	控制集	建議控制項資料來源映射項目
		• 1.16 (IAM.2) • 1.2 (IAM.5 • 1.20 (IAM.18) • 1.22 (IAM.1 • 1.3 (IAM.8) • 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2.1 (CloudTrail.1) • 2.2 (CloudTrail.4) • 2.3 (CloudTrail.6) • 2.4 (CloudTrail.5) • 2.5 (Config.1) • 2.6 (CloudTrail.7) • 2.7 (CloudTrail.2) • 2.8 (KMS.4) • 2.9 (EC2.6) • 3.1 (CloudWatch.2) • 3.10 (CloudWatch.10) • 3.11 (CloudWatch.11) • 3.12 (CloudWatch.12) • 3.13 (CloudWatch.13) • 3.14 (CloudWatch.14) • Config.1

控制項名稱	控制集	建議控制項資料來源映射項目
第 30 條處理活動之紀錄 1	第 4 章 - 控制方與處理方	您可以在 AWS Audit Manager 中建立自訂控制項以支援此 GDPR 控制項。 當您指定控制項詳細資訊時，請在測試資訊下輸入下列內容： • 顯示期間內的所有根帳號事件 設定控制項資料來源時，建議您將下列所有項目納入資料來源： 選擇 AWS Config 作為資料來源類型，然後選取下列 AWS Config 管理規則作為資料來源映射項目： • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUDTRAIL_SECURITY_TRAIL_ENABLED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED 選擇 AWS Security Hub 作為資料來源類型，然後選擇下列 Security Hub 控制項作為資料來源映射： • Config.1

控制項名稱	控制集	建議控制項資料來源映射項目
第 30 條處理活動之紀錄 2	第 4 章 - 控制方與處理方	您可以在 AWS Audit Manager 中建立自訂控制項以支援此 GDPR 控制項。 當您指定控制項詳細資訊時，請在測試資訊下輸入下列內容： • 顯示期間內的所有根帳號事件 設定控制項資料來源時，建議您將下列所有項目納入資料來源： 選擇 AWS Config 作為資料來源類型，然後選取下列 AWS Config 管理規則作為資料來源映射項目： • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED 選擇 AWS Security Hub 作為資料來源類型，然後選擇下列 Security Hub 控制項作為資料來源映射： • Config.1

控制項名稱	控制集	建議控制項資料來源映射項目
第 30 條處理活動之紀錄 3	第 4 章 - 控制方與處理方	您可以在 AWS Audit Manager 中建立自訂控制項以支援此 GDPR 控制項。 當您指定控制項詳細資訊時，請在測試資訊下輸入下列內容： • 顯示期間內的所有根帳號事件 • AWS CloudTrail儲存貯體不公開 • 顯示具備 `Allow:*:*` 的所有政策，並列出所有使用這些政策的主體和服務 設定控制項資料來源時，建議您將下列所有項目納入資料來源： 選擇 AWS Config 作為資料來源類型，然後選取下列 AWS Config 管理規則作為資料來源映射項目： • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED 選擇 AWS Security Hub 作為資料來源類型，然後選擇下列 Security Hub 控制項作為資料來源映射： • Config.1

控制項名稱	控制集	建議控制項資料來源映射項目
第 30 條處理活動之紀錄 4	第 4 章 - 控制方與處理方	您可以在 AWS Audit Manager 中建立自訂控制項以支援此 GDPR 控制項。 當您指定控制項詳細資訊時，請在測試資訊下輸入下列內容： • 顯示期間內的所有根帳號事件 • AWS CloudTrail儲存貯體不公開 • 顯示具備 `Allow:*:*` 的所有政策，並列出所有使用這些政策的主體和服務 設定控制項資料來源時，建議您將下列所有項目納入資料來源： 選擇 AWS Config 作為資料來源類型，然後選取下列 AWS Config 管理規則作為資料來源映射項目： • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED 選擇 AWS Security Hub 作為資料來源類型，然後選擇下列 Security Hub 控制項作為資料來源映射： • Config.1

控制項名稱	控制集	建議控制項資料來源映射項目
第 30 條處理活動之紀錄 5	第 4 章 - 控制方與處理方	您可以在 AWS Audit Manager 中建立自訂控制項以支援此 GDPR 控制項。 當您指定控制項詳細資訊時，請在測試資訊下輸入下列內容： • 顯示期間內的所有根帳號事件 設定控制項資料來源時，建議您將下列所有項目納入資料來源： 選擇 AWS Config 作為資料來源類型，然後選取下列 AWS Config 管理規則作為資料來源映射項目： • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED 選擇 AWS Security Hub 作為資料來源類型，然後選擇下列 Security Hub 控制項作為資料來源映射： • Config.1

控制項名稱	控制集	建議控制項資料來源映射項目
第 32 條處理之安全性 1	第 4 章 - 控制方與處理方	您可以在 AWS Audit Manager 中建立自訂控制項以支援此 GDPR 控制項。 當您指定控制項詳細資訊時，請在測試資訊下輸入下列內容： • 顯示所有服務的靜態資料加密 • 顯示所有服務的傳輸中的資料加密 • 已為 Amazon S3 啟用 MFA 刪除功能 • 所有 Amazon Inspector 掃描 • 顯示未啟用 Amazon Inspector 的所有執行個體 • 顯示正在使用 HTTPS (SSL) 接聽的所有負載平衡器 • 待用時加密 AWS CloudTrail • Amazon CloudWatch 提醒 AWS Config 顯示所有變更和所有含備註之設定 • 所有根活動 設定控制項資料來源時，建議您將下列所有項目納入資料來源： 選擇 AWS Config 作為資料來源類型，然後選取下列 AWS Config 管理規則作為資料來源映射項目： • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST • ENCRYPTED_VOLUMES • RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED

控制項名稱	控制集	建議控制項資料來源映射項目
		• SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY • ACM_CERTIFICATE_EXPIRATION_CHECK • API_GW_CACHE_ENABLED_AND_ENCRYPTED

控制項名稱	控制集	建議控制項資料來源映射項目
第 32 條處理之安全性 2	第 4 章 - 控制方與處理方	您可以在 AWS Audit Manager 中建立自訂控制項以支援此 GDPR 控制項。 當您指定控制項詳細資訊時，請在測試資訊下輸入下列內容： • 顯示所有服務的靜態資料加密 • 顯示所有服務的傳輸中的資料加密 • 已為 Amazon S3 啟用 MFA 刪除功能 • 所有 Amazon Inspector 掃描 • 顯示未啟用 Amazon Inspector 的所有執行個體 • 顯示正在使用 HTTPS (SSL) 接聽的所有負載平衡器 • 待用時加密 AWS CloudTrail • Amazon CloudWatch 提醒 AWS Config 顯示所有變更和所有含備註之設定 • 所有根活動 設定控制項資料來源時，建議您將下列所有項目納入資料來源： 選擇 AWS Config 作為資料來源類型，然後選取下列 AWS Config 管理規則作為資料來源映射項目： • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST • ENCRYPTED_VOLUMES • RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED

控制項名稱	控制集	建議控制項資料來源映射項目
		• SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY • ACM_CERTIFICATE_EXPIRATION_CHECK • API_GW_CACHE_ENABLED_AND_ENCRYPTED

控制項名稱	控制集	建議控制項資料來源映射項目
第 32 條處理之安全性 3	第 4 章 - 控制方與處理方	您可以在 AWS Audit Manager 中建立自訂控制項以支援此 GDPR 控制項。 當您指定控制項詳細資訊時，請在測試資訊下輸入下列內容： • 顯示所有服務的靜態資料加密 • 顯示所有服務的傳輸中的資料加密 • 已為 Amazon S3 啟用 MFA 刪除功能 • 所有 Amazon Inspector 掃描 • 顯示未啟用 Amazon Inspector 的所有執行個體 • 顯示正在使用 HTTPS (SSL) 接聽的所有負載平衡器 • 待用時加密 AWS CloudTrail • Amazon CloudWatch 提醒 AWS Config 顯示所有變更和所有含備註之設定 • 所有根活動 設定控制項資料來源時，建議您將下列所有項目納入資料來源： 選擇 AWS Config 作為資料來源類型，然後選取下列 AWS Config 管理規則作為資料來源映射項目： • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST • ENCRYPTED_VOLUMES • RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED

控制項名稱	控制集	建議控制項資料來源映射項目
		• SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY • ACM_CERTIFICATE_EXPIRATION_CHECK • API_GW_CACHE_ENABLED_AND_ENCRYPTED

控制項名稱	控制集	建議控制項資料來源映射項目
第 32 條處理之安全性 4	第 4 章 - 控制方與處理方	您可以在 AWS Audit Manager 中建立自訂控制項以支援此 GDPR 控制項。 當您指定控制項詳細資訊時，請在測試資訊下輸入下列內容： • 顯示所有服務的靜態資料加密 • 顯示所有服務的傳輸中的資料加密 • 已為 Amazon S3 啟用 MFA 刪除功能 • 所有 Amazon Inspector 掃描 • 顯示未啟用 Amazon Inspector 的所有執行個體 • 顯示正在使用 HTTPS (SSL) 接聽的所有負載平衡器 • 待用時加密 AWS CloudTrail • Amazon CloudWatch 提醒 AWS Config 顯示所有變更和所有含備註之設定 • 所有根活動 設定控制項資料來源時，建議您將下列所有項目納入資料來源： 選擇 AWS Config 作為資料來源類型，然後選取下列 AWS Config 管理規則作為資料來源映射項目： • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST • ENCRYPTED_VOLUMES • RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED

控制項名稱	控制集	建議控制項資料來源映射項目
		• SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY • ACM_CERTIFICATE_EXPIRATION_CHECK • API_GW_CACHE_ENABLED_AND_ENCRYPTED

建立新的自訂控制項之後，您可以將其新增至自訂 GDPR 架構。如需詳細資訊，請參閱建立自訂架構及編輯自訂架構。您可以從自訂 GDPR 架構建立評估。如此一來，AWS Audit Manager 可以自動為您加入的自訂控制項收集證據。如需透過此架構建立評估方式的說明，請參閱 建立評估。

其他 GDPR 資源

- 一般資料保護規範 (GDPR) 中心
- AWSGDPR 部落格貼文

金融服務業現代化法 (GLBA)

AWS Audit Manager 提供支援金融服務業現代化法 (GLBA) 的預先建置架構。

主題

- 什麼是金融服務業現代化法 (GLBA)？
- 使用此架構幫助您進行稽核準備

什麼是金融服務業現代化法 (GLBA)？

格雷姆-里奇-比利雷法 (GLB 法案或 GLBA)，也稱為 1999 年的金融服務業現代化法，是美國制定的聯邦法律，旨在控制金融機構處理個人私人資訊的方式。這個動作是由三個區段組成。首先是財務隱私規則，其規定了私人財務資訊的收集與揭露。第二個是保障規則，其規定金融機構必須實施安全計劃以保護此類資訊。第三個是禁止預編，即禁止進行預編的行動 (利用假訪問取得私人資訊)。該法案還要求金融機構向客戶提供書面的隱私通知，以解釋他們的資訊共享做法。

使用此架構幫助您進行稽核準備

您可以使用金融服務業現代化法 (GLBA) 架構來幫助您準備審核。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據 GLBA 要求分組成控制集。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用 GLBA 架構作為起點，您可以建立 Audit Manager 評估，並開始收集與 GLBA 稽核相關的證據。在評估中，您可以指定要包含在稽核範圍中的 AWS 帳戶 和服務。您建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據 GLBA 架構中定義的控制項來執行此動作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

GLBA 架構的詳細資訊如下：

AWS Audit Manager 內的架構名稱	自動化控制項數量	手動控制項數量	控制集數	AWS 服務 在範圍內
金融服務業現代化法 (GLBA)	4	110	16	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> 如果檢閱在此標準架構中，當成資料來源對應的 AWS Config 規則，請下載 AuditManager_ConfigDataSourceMappings_GLBA.zip 檔案。

此 AWS Audit Manager 架構中的控制項，並非為了驗證您的系統是否符合 GLBA 標準所設計。此外，他們無法保證您會透過 GLBA 之稽核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控制項。

您可以在 Audit Manager 架構程式庫 的標準架構索引標籤下，找到 GLBA 架構。

如需使用此架構建立評估方式的說明，請參閱 建立評估。

當您使用 Audit Manager 主控台從此標準架構建立評估時，範圍AWS 服務內的清單會被預設為選擇狀態且不可編輯。這是因為 Audit Manager 會自動為您映射並選擇資料來源和服務。此選擇是根據 GLBA 的要求所進行。如果您需要編輯此架構範圍內的服務清單，可以使用建立評估或更新評估 API操作來進行編輯。或者，您可以自訂標準架構，然後從自訂架構中建立評估。

如需自訂此架構以支援您特定需求的指引，請參閱自訂現有架構和自訂現有控制項。

GxP 21 CFR 第 11 部分

AWS Audit Manager 提供預先打造的架構，根據 AWS 最佳實務支援 GxP CFR Part 11 法規。

> **Note**
>
> 如需 GxP EU Annex 11 以及支援此功能的 Audit Manager 架構之相關資訊，請參閱 GxP EU Annex 11。

主題

什麼是 GxP CFR Part 11 ？

GxP 是指適用於生產食品和醫療產品的生命科學組織之法規和準則。屬於這種情況的醫療產品包括藥品、醫療設備和醫療軟體應用程式。GxP 要求的總體目的，是確保食品和醫療產品的消費者安全。這也是為了確保用於制定產品相關安全決策的資料完整性。

GxP 一詞包含廣泛的合規性相關活動。這些措施包括優良實驗室規範 (GLP)，優良臨床規範 (GCP) 和優良生產規範 (GMP)。這些不同類型的活動，都涉及生命科學組織必須遵循的產品特定需求。這是基於組織製造產品的類型，以及其產品銷售的國家。當生命科學組織使用電腦化系統來執行某些 GxP 活動時，必須確保電腦化的 GxP 系統已針對系統的預定用途，進行適當的開發、驗證和操作。

如需針對 GxP 系統使用AWS雲端的完整做法，請參閱在 GxP 系統使用 AWS 產品注意事項白皮書。

使用此架構幫助您進行稽核準備

您可以使用 GxP 21 CFR Part 11 架構來協助您準備稽核。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據 GxP 要求分組成控制集。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與您的稽核相關的證據。您建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據 GxP 21 CFR 第 11 部分架構中定義的控制項來執行此動作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

GxP CFR Part 11 架構的詳細資訊如下：

AWS Audit Manager 內的架構名稱	自動化控制項數量	手動控制項數量	控制集數	AWS 服務 在範圍內
GXP 21 CFR 第 11 部分	13	14	7	• AWS CloudTrail • AWS Config • AWS Identity and Access Management

> **Tip**
>
> 如果檢閱在此標準架構中，當成資料來源對應的 AWS Config 規則，請下載 AuditManager_ConfigDataSourceMappings_GxP-21-CFR-Part-11.zip 檔案。

AWS Audit Manager 架構中的此控制項，並非為了驗證您的系統是否符合 GxP 規則所設計。此外，他們無法保證您會透過 GxP 之稽核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控制項。

您可以在 Audit Manager 架構程式庫 的標準架構索引標籤下，找到這個架構。

如需使用此架構建立評估方式的說明，請參閱 建立評估。

當您使用 Audit Manager 主控台從此標準架構建立評估時，範圍AWS 服務內的清單會被預設為選擇狀態且不可編輯。這是因為 Audit Manager 會自動為您映射並選擇資料來源和服務。此選擇是根據 GxP CFR 第 11 部分架構的要求所進行。如果您需要編輯此架構範圍內的服務清單，可以使用建立評估或更新評估 API操作來進行編輯。或者，您可以自訂標準架構，然後從自訂架構中建立評估。

如需自訂此架構以支援您特定需求的指引，請參閱自訂現有架構和自訂現有控制項。

其他 GxP 資源

- AWSGxP 的合規頁面
- 在 GxP 系統使用 AWS 產品注意事項

GxP EU Annex 11

AWS Audit Manager 提供預先打造的架構，根據 AWS 最佳實務支援 GxP EU Annex 11 法規。

> **Note**
>
> 如需 GxP 21 CFR 第 11 部分 以及支援此功能的 Audit Manager 架構之相關資訊，請參閱 GxP 21 CFR 第 11 部分。

主題

什麼是 GxP EU Annex 11？

GxP EU Annex 11 架構，是相當於美國 FDA 21 CFR Part 11 架構的歐洲版本。本附件適用於所有形式的電腦化系統，其用於優良生產規範 (GMP) 受管活動的一部分。電腦化系統是一組軟體和硬體元件，合併共同實現特定功能。應用程式應進行驗證，且 IT 基礎架構應該符合資格。當電腦化系統取代手動操作，產品品質、製程控制或品質保證不會因此而降低。該過程的整體風險不應增加。

Annex 11 是歐洲 GMP 指導方針的一部分，並定義了製藥行業組織使用的電腦化系統參考條款。Annex 11 的功能就像檢查清單，使歐洲監管機構能夠制定與藥品和醫療設備相關的電腦化系統之要求。由歐洲委員會成員制定的指導方針，與 FDA 所制定的相去不遠 (21 CFR Part 11)。Annex 11 明訂電子紀錄及電子簽章應考慮管理的條件。

使用此架構幫助您進行稽核準備

您可以使用 GxP EU Annex 11 架構來協助您準備稽核。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據 GxP 要求分組成控制集。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與您的稽核相關的證據。您建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據 GxP EU Annex 11 架構中定義的控制項來執行此動作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

GxP EU Annex 11 架構的詳細資訊如下：

AWS Audit Manager 內的架構名稱	自動化控制項數量	手動控制項數量	控制集數	AWS 服務 在範圍內
GxP EU Annex 11	19	13	3	• Amazon CloudWatch • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> 如果檢閱在此標準架構中，當成資料來源對應的 AWS Config 規則，請下載 AuditManager_ConfigDataSourceMappings_GxP-EU-Annex-11.zip 檔案。

此架構中的控制項，並非為了驗證您的系統是否符合GxP EU Annex 11 要求所設計。此外，他們無法保證您會透過 GxP 之稽核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控制項。

您可以在 Audit Manager 架構程式庫 的標準架構索引標籤下，找到這個架構。

如需使用此架構建立評估方式的說明，請參閱 建立評估。

當您使用 Audit Manager 主控台從此標準架構建立評估時，範圍AWS 服務內的清單會被預設為選擇狀態且不可編輯。這是因為 Audit Manager 會自動為您映射並選擇資料來源和服務。此選擇是根據 GxP EU Annex 11 架構的要求所進行。如果您需要編輯此架構範圍內的服務清單，可以使用建立評估或更新評估 API操作來進行編輯。或者，您可以自訂標準架構，然後從自訂架構中建立評估。

如需自訂此架構以支援您特定需求的指引，請參閱自訂現有架構和自訂現有控制項。

美國健康保險流通與責任法案 (HIPAA) 安全規則 2003

AWS Audit Manager提供支援 HIPAA 規則的預先建置架構，協助您進行稽核準備。

> **Note**
>
> 此架構在架構程式庫中的舊名為 HIPAA。在 2023 年 3 月 8 日，我們將此架構的名稱更新為 HIPAA 安全規則 2003，以區分其與 HIPAA Final Omnibus 安全規則 2013 的差別。
> 如需有關 HIPAA Final Omnibus 安全規則 2013 以及支援此標準的 Audit Manager 架構的資訊，請參閱 美國健康保險流通與責任法案 (HIPAA) Final Omnibus 安全規則 2013。

主題

什麼是 HIPAA 和 HIPAA 安全規則 2003？

1996 年美國健康保險流通與責任法案 (HIPAA) 是協助美國員工在轉換或失去工作時，得以保留健康保險的法案。該法案亦旨在推廣電子健康紀錄，透過改善資料互通，改善美國醫療系統的效率和品質。

隨著電子醫療紀錄的使用日益增加，HIPAA 還納入受保護醫療資訊 (PHI) 之安全性和隱私權保障的條款。PHI 包括一系列非常廣泛的個人身份健康和健康相關資料。這包括保險和帳單資訊、診斷資料、臨床照護資料，以及實驗室結果，例如影像和測試結果。

美國健康與公共服務部於 2003 年 2 月發布了最終版的安全規則。為了讓受保護的電子健康資訊之機密性、完整性和可用性得到保障，因此設立此國家標準之規則。

HIPAA 規則適用於涵蓋的實體。這些包括醫院、醫療服務提供者、雇主贊助的健康計劃、研究設施以及直接處理患者和患者資料的保險公司。保護 PHI 的 HIPAA 要求也延伸到商業夥伴。

有關 HIPAA 和 HITECH 如何保護健康資訊的更多相關內容，請參閱美國衛生和公共服務部的健康資訊隱私網頁。

越來越多的健康照護提供者、付款人和 IT 專業人員正在使用AWS公用程式的雲端服務處理、儲存和傳輸受保護的健康資訊 (PHI)。AWS 讓受 HIPAA 約束的涵蓋實體及其業務夥伴能夠使用安全的 AWS 環境來處理、維護和儲存受保護的健康資訊。

如需如何運用 AWS 於處理和儲存健康資訊的說明，請參閱 Amazon Web Services 的 HIPAA 安全與合規架構白皮書。

使用此架構幫助您進行稽核準備

您可以使用 HIPAA 安全規則 2003 來協助您準備稽核。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據 HIPAA 要求分組成控制集。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與您的稽核相關的證據。您建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據 HIPAA 架構中定義的控制項來執行此動作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

HIPAA 安全規則 2003 架構詳細資訊如下：

AWS Audit Manager 內的架構名稱	自動化控制項數量	手動控制項數量	控制集數	AWS 服務 在範圍內
HIPAA 安全規則 2003	35	53	5	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> 如果檢閱在此標準架構中，當成資料來源對應的 AWS Config 規則，請下載 AuditManager_ConfigDataSourceMappings_HIPAA-Security-Rule-2003.zip檔案。

此 AWS Audit Manager 架構中的控制項，並非為了驗證您的系統是否符合 HIPAA 標準所設計。此外，他們無法保證您會透過 HIPAA 之稽核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控制項。

您可以在 Audit Manager 架構程式庫 的標準架構索引標籤下，找到這個架構。

如需使用此架構建立評估方式的說明，請參閱 建立評估。

當您使用 Audit Manager 主控台從此標準架構建立評估時，範圍AWS 服務內的清單會被預設為選擇狀態且不可編輯。這是因為 Audit Manager 會自動為您映射並選擇資料來源和服務。此選擇是根據 HIPAA 標準架構的要求所進行。如果您需要編輯此架構範圍內的服務清單，可以使用建立評估或更新評估 API操作來進行編輯。或者，您可以自訂標準架構，然後從自訂架構中建立評估。

如需自訂此架構以支援您特定需求的指引，請參閱自訂現有架構和自訂現有控制項。

更多 HIPAA 資源

- 來自美國衛生與公共服務部的健康資訊隱私權
- 美國衛生與公共服務部的安全規則
- Amazon Web Services 上的 HIPAA 安全與合規架構
- AWSHIPAA 的合規頁面

美國健康保險流通與責任法案 (HIPAA) Final Omnibus 安全規則 2013

AWS Audit Manager提供支援 HIPAA 規則的預先建置架構，協助您進行稽核準備。

> **Note**
>
> 如需有關 HIPAA 安全規則 2003 以及支援此標準的 AWS Audit Manager 架構的資訊，請參閱美國健康保險流通與責任法案 (HIPAA) 安全規則 2003。

主題

什麼是 HIPAA 和 HIPAA Final Omnibus 安全規則？

1996 年美國健康保險流通與責任法案 (HIPAA) 是協助美國員工在轉換或失去工作時，得以保留健康保險的法案。該法案亦旨在推廣電子健康紀錄，透過改善資料互通，改善美國醫療系統的效率和品質。

隨著電子醫療紀錄的使用日益增加，HIPAA 還納入受保護醫療資訊 (PHI) 之安全性和隱私權保障的條款。PHI 包括一系列非常廣泛的個人身份健康和健康相關資料。這包括保險和帳單資訊、診斷資料、臨床照護資料，以及實驗室結果，例如影像和測試結果。

HIPAA Final Omnibus 安全規則於 2013 年生效，其對所有先前通過的規則追加了不少更新。安全性、隱私權、違規通知和強制執行規則的修改，旨在增強資料分享的機密性和安全性。

HIPAA 規則適用於涵蓋的實體。這些包括醫院、醫療服務提供者、雇主贊助的健康計劃、研究設施以及直接處理患者和患者資料的保險公司。作為綜合更新的一部分，許多適用於涵蓋實體的 HIPAA 規則，現在也適用於商業夥伴。

有關 HIPAA 和 HITECH 如何保護健康資訊的更多相關內容，請參閱美國衛生和公共服務部的健康資訊隱私網頁。

越來越多的健康照護提供者、付款人和 IT 專業人員正在使用AWS公用程式的雲端服務處理、儲存和傳輸受保護的健康資訊 (PHI)。AWS 讓受 HIPAA 約束的涵蓋實體及其業務夥伴能夠使用安全的 AWS 環境來處理、維護和儲存受保護的健康資訊。如需如何運用 AWS 於處理和儲存健康資訊的說明，請參閱 Amazon Web Services 的 HIPAA 安全與合規架構白皮書。

使用此架構幫助您進行稽核準備

您可以使用 HIPAA Final Omnibus 安全規則 2013 架構來協助您準備稽核。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據 HIPAA 要求分組成控制集。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與您的稽核相關的證據。您建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據 HIPAA 架構中定義的控制項來執行此動作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

HIPAA Final Omnibus 安全規則 2013 架構詳細資訊如下：

AWS Audit Manager 內的架構名稱	自動化控制項數量	手動控制項數量	控制集數	AWS 服務 在範圍內
HIPAA Final Omnibus 安全規則 2013	39	46	5	• Amazon Elastic Compute Cloud

AWS Audit Manager 內的架構名稱	自動化控制項數量	手動控制項數量	控制集數	AWS 服務 在範圍內
				• AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> 如果檢閱在此標準架構中，當成資料來源對應的 AWS Config 規則，請下載 AuditManager_ConfigDataSourceMappings_HIPAA-Final-Omnibus-Security-Rule-2013.zip 檔案。

此 AWS Audit Manager 架構中的控制項，並非為了驗證您的系統是否符合 HIPAA 標準所設計。此外，他們無法保證您會透過 HIPAA 之稽核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控制項。

您可以在 Audit Manager 架構程式庫 的標準架構索引標籤下，找到這個架構。

如需使用此架構建立評估方式的說明，請參閱 建立評估。

當您使用 Audit Manager 主控台從此標準架構建立評估時，範圍AWS 服務內的清單會被預設為選擇狀態且不可編輯。這是因為 Audit Manager 會自動為您映射並選擇資料來源和服務。此選擇是根據 HIPAA 標準架構的要求所進行。如果您需要編輯此架構範圍內的服務清單，可以使用建立評估或更新評估 API操作來進行編輯。或者，您可以自訂標準架構，然後從自訂架構中建立評估。

如需自訂此架構以支援您特定需求的指引，請參閱自訂現有架構和自訂現有控制項。

更多 HIPAA 資源

- 來自美國衛生與公共服務部的健康資訊隱私權
- 美國衛生與公共服務部的 Omnibus HIPAA Rulemaking

- Amazon Web Services 上的 HIPAA 安全與合規架構
- AWSHIPAA 的合規頁面

ISO/IEC 27001:2013 Annex A

AWS Audit Manager 提供一個預先建立的標準架構，以建構和自動化 ISO/IEC 27001:2013 Annex A 的評估。

主題

- 什麼是 ISO/IEC 27001:2013 Annex A？
- 使用此架構幫助您進行稽核準備
- 更多 ISO/IEC 27001:2013 Annex A 資源

什麼是 ISO/IEC 27001:2013 Annex A？

國際電工委員會 (IEC) 和國際標準化組織 (ISO) 均為獨立、非政府、非營利性組織，其開發出並發佈完全符合共識的國際標準。

ISO/IEC 27001:2013 Annex A 是一項安全管理標準，其指出遵循 ISO/IEC 27002 最佳實務指引的安全管理最佳做法，以及完整的安全控制措施。此國際標準規定了如何在組織中建立、實施、維護和持續改善資訊安全管理系統的要求。這些標準包括針對您的組織需求量身打造的資訊安全風險評估和處理要求。此國際標準中的要求是通用的，旨在適用於所有組織，無論其類型、規模或性質。

使用此架構幫助您進行稽核準備

您可以使用 ISO/IEC 27001:2013 Annex A 的AWS Audit Manager架構來協助您為稽核做好準備。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據 ISO/IEC 27001:2013 Annex A 要求，分為控制組。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用此架構作為起點，您可以建立 Audit Manager 評估，並開始收集與 ISO/IEC 27001:2013 Annex A 稽核相關的證據。在評估中，您可以指定要包含在稽核範圍中的 AWS 帳戶 和服務。您建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據 ISO/IEC 27001:2013 Annex A 架構中所定義的控制項來執行此操作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

架構的詳細資訊如下：

AWS Audit Manager 內的架構名稱	自動化控制項數量	手動控制項數量	控制集數	AWS 服務 在範圍內
ISO-IEC 27001:2013 Annex A	50	64	35	• Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> 若要檢閱在此標準架構中用作資料來源對應的AWS Config規則，請下載 AuditManager_ConfigDataSourceMappings_ISO-IEC-27001-2013-Annex-A.zip 檔案。

此 AWS Audit Manager 架構中的控制項，並非為了驗證您的系統是否符合本國際標準所設計。此外，他們不能保證您將通過 ISO/IEC 審核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控制項。

您可以在 Audit Manager 架構程式庫 的標準架構索引標籤下，找到 ISO/IEC 27001:2013 Annex A 架構。

當您使用 Audit Manager 主控台從此標準架構建立評估時，範圍AWS 服務內的清單會被預設為選擇狀態且不可編輯。這是因為 Audit Manager 會自動為您映射並選擇資料來源和服務。此選擇是根據 ISO-IEC 27001:2013 Annex A 標準架構的要求進行的。如果您需要編輯此架構範圍內的服務清單，可以使用建立評估或更新評估 API操作來進行編輯。或者，您可以自訂標準架構，然後從自訂架構中建立評估。

如需使用此架構建立評估方式的說明，請參閱 建立評估。如需自訂此架構以支援您特定需求的指引，請參閱自訂現有架構和自訂現有控制項。

更多 ISO/IEC 27001:2013 Annex A 資源

- 如需有關此國際標準的詳細資訊，請參閱 ANSI 網路商店中的 ISO/IEC 27001:2013。

NIST 800-53 (修訂版 5) Low-Moderate-High

根據 AWS 最佳實務提供預先建置的架構，AWS Audit Manager 提供建構並自動化 NIST 800-53 合規標準之預先建置架構。

> **Note**
>
> - 如需支援 NIST 800-171 的 Audit Manager 架構相關資訊，請參閱 NIST SP 800-171 (修訂版 2)。
> - 如需支援 NIST 網路安全架構的 Audit Manager 架構相關資訊，請參閱NIST 網路安全架構 1.1 版。

主題

什麼是 NIST 800-53?

美國國家標準與技術研究所 (NIST) 成立於 1901 年，現為美國商務部的一員。NIST 是美國最古老的物理科學實驗室之一。美國國會成立了該機構，以改善當時二流的測量基礎設施。該基礎設施是美國工業競爭力的一大挑戰，當時落後於英國和德國等其他經濟強國。

NIST 800-53 安全控制適用於美國聯邦資訊系統。這些通常必須經過正式評估和授權程序的系統。此過程確保對資訊和資訊系統的機密性、完整性和可用性有全面防護。這是根據系統的安全類別和影響層級 (低、中或高) 以及風險判定而定。當您從 NIST SP 800-53 安全控制類別中選擇安全控制時，即會根據這些安全控制要求來評估系統。

NIST 800-53 (修訂版 5) Low-Moderate-Hig 架構代表 NIST SP 800-53 修訂版 5 針對聯邦資訊系統與 Organizations 的建議安全性控制中所定義的安全性控制項與相關評估程序。如需 NIST SP 800-53 架構與最新出版的 NIST 特別出版品 SP 800-53 修訂版 5 之間的內容中所述的任何差異，請參閱 NIST 電腦安全資源中心所提供的官方已發佈文件。

使用此架構幫助您進行稽核準備

請使用 NIST 800-53 (修訂版 5) Low-Moderate-High 架構來協助您準備稽核。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據 NIST 要求分組成控制集。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與您的稽核相關的證據。您建立評估之後，Audit Manager 會開始評估您的 AWS 資源。根據 NIST 800-53 (修訂版 5) Low-Moderate-High 架構中定義的控制項來執行此操作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

NIST 800-53 (修訂版 5) Low-Moderate-High 架構的詳細資料如下：

AWS Audit Manager 內的架構名稱	自動化控制項數量	手動控制項數量	控制集數	AWS 服務 在範圍內
NIST 800-53 (修訂版 5) Low-Moderate-High	225	782	280	• Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> 如果檢閱在此標準架構中，當成資料來源對應的 AWS Config 規則，請下載 AuditManager_ConfigDataSourceMappings_NIST-800-53-Rev.5-Low-Moderate-High.zip 檔案。

此 AWS Audit Manager 架構中的控制項，並非為了驗證您的系統是否符合 NIST 標準所設計。此外，他們無法保證您會透過 NIST 之稽核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控制項。

您可以在 Audit Manager 架構程式庫 的標準架構索引標籤下，找到這個架構。

如需使用此架構建立評估方式的說明，請參閱 建立評估。

當您使用 Audit Manager 主控台從此標準架構建立評估時，範圍AWS 服務內的清單會被預設為選擇狀態且不可編輯。這是因為 Audit Manager 會自動為您映射並選擇資料來源和服務。此選擇是根據 NIST 800-53 (修訂版 5) Low-Moderate-High 架構的要求進行。如果您需要編輯此架構範圍內的服務清單，可以使用建立評估或更新評估 API操作來進行編輯。或者，您可以自訂標準架構，然後從自訂架構中建立評估。

如需自訂此架構以支援您特定需求的指引，請參閱自訂現有架構和自訂現有控制項。

更多 NIST 資源

- 國家標準技術研究所 (NIST)
- NIST 電腦安全資源中心
- AWSNIST 的合規頁面

NIST 網路安全架構 1.1 版

AWS Audit Manager 根據 AWS 最佳實務提供預先建置的架構，可建構並自動化 NIST 網路安全架構之評估。

> **Note**
>
> - 如需支援 NIST 800-53 (修訂版 5) Low-Moderate-High 的 Audit Manager 架構相關資訊，請參閱NIST 800-53 (修訂版 5) Low-Moderate-High。
> - 如需支援 NIST SP 800-171 (修訂版 2) 的 Audit Manager 架構相關資訊，請參閱 NIST SP 800-171 (修訂版 2)。

主題

- 什麼是 NIST 網路安全架構？

- 使用此架構幫助您進行稽核準備
- 更多 NIST 資源

什麼是 NIST 網路安全架構？

美國國家標準與技術研究所 (NIST) 成立於 1901 年，現為美國商務部的一員。NIST 是美國最古老的物理科學實驗室之一。美國國會成立了該機構，以改善當時二流的測量基礎設施。該基礎設施是美國工業競爭力的一大挑戰，落後於英國和德國等其他經濟強國。

美國依賴關鍵基礎設施的可靠運作。網路安全威脅利用關鍵基礎設施系統日益增加的複雜性和互聯性。它們將美國的安全、經濟以及公共安全和健康置於風險之中。類似於財務和聲譽風險，網路安全風險影響公司的盈利能力。它可以提高成本並影響收入。它可能損害組織的創新能力，以及獲得和維持客戶的能力。最終，網路安全可以擴大組織的整體風險管理。

NIST 網路安全架構 (CSF) 受到全球各國政府和產業的支援，作為任何組織使用的建議基準，無論產業或規模大小。NIST 網路安全架構包含三個主要元件：架構核心、設定檔和實作層。架構核心包含所需的網路安全活動和成果，分為 23 個類別，涵蓋組織的廣泛網路安全目標。概況包含了組織對其組織需求和目標，風險偏好和資源的調整，以及使用架構核心所需結果的資源的獨特一致性。實施層描述了組織的網路安全風險管理實踐展現出架構核心中所定義的特色。

使用此架構幫助您進行稽核準備

您可以使用 NIST 網路安全架構 1.1 版來協助您準備稽核。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據 NIST CSF 要求分組成控制集。Audit Manager 透過提供 56 個自動化控制項和 52 個手動控制項來支援架構核心元件。這些控制項與架構核心中定義的 23 個網路安全類別相符。Audit Manager 不支援此架構中的設定檔和實作元件。

您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與您的稽核相關的證據。您建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據 NIST 網路安全架構 1.1 版中定義的控制項來執行此操作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

NIST 網路安全架構 1.1 版的詳細資料如下：

AWS Audit Manager 內的架構名稱	自動化控制項數量	手動控制項數量	控制集數	AWS 服務 在範圍內
NIST 網路安全架構 1.1 版	56	52	23	• AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> 若要檢閱在此標準架構中作為資料來源對映使用的AWS Config規則，請下載檔案 AuditManager_ConfigDataSourceMappings_NIST-CSF-v1.1.zip。

Audit Manager 提供的控制項無法驗證您的系統是否符合 NIST 網路安全架構。此外，他們無法保證您會透過 NIST 網路安全之稽核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控制項。

您可以在 Audit Manager 架構程式庫 的標準架構索引標籤下，找到這個架構。

如需使用此架構建立評估方式的說明，請參閱 建立評估。

當您使用 Audit Manager 主控台從此標準架構建立評估時，範圍AWS 服務內的清單會被預設為選擇狀態且不可編輯。這是因為 Audit Manager 會自動為您映射並選擇資料來源和服務。此選擇是根據 NIST 網路安全架構 1.1 版架構的要求來進行。如果您需要編輯此架構範圍內的服務清單，可以使用建立評估或更新評估 API操作來進行編輯。或者，您可以自訂標準架構，然後從自訂架構中建立評估。

如需自訂此架構以支援您特定需求的指引，請參閱自訂現有架構和自訂現有控制項。

更多 NIST 資源

- 國家標準技術研究所 (NIST)
- NIST 電腦安全資源中心
- AWSNIST 的合規頁面
- NIST 網路安全架構-與AWS雲端中的 NIST CSF 保持一致

NIST SP 800-171 (修訂版 2)

AWS Audit Manager提供預建架構，根據AWS最佳實務建構和自動化 NIST SP 800-171 相容性標準的評估。

> **Note**
>
> - 如需支援 NIST 800-53 (修訂版 5) Low-Moderate-High 的 Audit Manager 架構相關資訊，請參閱NIST 800-53 (修訂版 5) Low-Moderate-High。
> - 如需支援 NIST 網路安全架構 1.1 版的 Audit Manager 架構相關資訊，請參閱NIST 網路安全架構 1.1 版。

主題

什麼是 NIST SP 800-171?

NIST SP 800-171 專注於保護非聯邦系統和組織中受控制的未分類資訊 (CUI) 的機密性。它提出實現此目標的具體安全要求。NIST 800-171 是一份出版物，概述在網路上處理 CUI 的非聯邦組織所需的安全標準和策略。於 2015 年 6 月由美國國家標準技術研究院 (NIST) 首次出版。NIST 是一家美國政府機構，發布多項標準和出版物，以加強公共和私營部門的網路安全抗禦能力。NIST 800-171 會定期更新，以配合新興的網路威脅和不斷變化的技術。於 2020 年 2 月發布最新版本 (修訂版 2)。

NIST 800-171 中的網路安全控制措施可保護政府承包商和分包商的 IT 網路中的 CUI。它定義了政府承包商在其網路處理或儲存 CUI 時必須遵守的做法和程序。NIST 800-171 僅適用於承包商網路中存在 CUI 的部分。

使用此架構幫助您進行稽核準備

您可以使用 NIST SP 800-171 Rev. 2 架構來協助您準備稽核。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據 NIST 要求分組成控制集。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與您的稽核相關的證據。您建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據 NIST SP 800-171 修訂版 2 架構中定義

的控制項來執行此動作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

NIST SP 800-171 修訂版 2 架構的詳細資料如下：

AWS Audit Manager 內的架構名稱	自動化控制項數量	手動控制項數量	控制集數	AWS 服務 在範圍內
NIST SP 800-171 修訂版 2	66	58	16	• Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> 如果檢閱在此標準架構中作為資料來源對映使用的AWS Config規則，請下載檔案 AuditManager_ConfigDataSourceMappings_NIST-SP-800-171-Rev.2.zip 。

此 AWS Audit Manager 架構中的控制項，並非為了驗證您的系統是否符合 NIST 800-171 所設計。此外，他們無法保證您會透過 NIST 之稽核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控制項。

您可以在 Audit Manager 架構程式庫 的標準架構索引標籤下，找到這個架構。

如需使用此架構建立評估方式的資訊，請參閱 建立評估。

當您使用 Audit Manager 主控台從此標準架構建立評估時，範圍AWS 服務內的清單會被預設為選擇狀態且不可編輯。這是因為 Audit Manager 會自動為您映射並選擇資料來源和服務。此選擇是根據 NIST

SP 800-171 修訂版 2 架構的要求所進行。如果您需要編輯此架構範圍內的服務清單，可以使用建立評估或更新評估 API操作來進行編輯。或者，您可以自訂標準架構，然後從自訂架構中建立評估。

如需自訂此架構以支援您特定需求的指引，請參閱自訂現有架構和自訂現有控制項。

更多 NIST 資源

- 國家標準技術研究所 (NIST)
- NIST 電腦安全資源中心
- AWSNIST 的合規頁面

PCI DSS V3.2.1

AWS Audit Manager提供支援 PCI DSS 3.2.1 版的預建架構。

> **Note**
>
> 如需 PCI DSS v4 以及支援此功能的 Audit Manager 架構之相關資訊，請參閱 PCI DSS V4.0。

主題

- 什麼是 PCI DSS？
- 使用此架構幫助您進行稽核準備
- 更多 PCI DSS 資源

什麼是 PCI DSS？

支付卡產業資料安全標準 (PCI DSS) 是一種專屬資訊安全標準。PCI DSS 由 PCI 安全標準協會管理，由美國運通、Discover Financial、JCB International、MasterCard Worldwide 及 Visa Inc. PCI DSS 共同創設，適用於實際儲存、處理或傳輸持卡人資料 (CHD) 或敏感驗證資料 (SAD)。這包括但不受限於商家、處理者、收單銀行、發行者和服務提供者。PCI DSS 受卡片品牌所規範，且由支付卡產業安全標準委員會管理。

AWS透過 PCI DSS 第一級服務供應商認證，這是可用性評估的最高等級。合規評估由獨立且經過認證的安全評估員 (QSA) Coalfire Systems Inc. 進行。您可以透過以下方式取得 PCI DSS 合規證明 (AOC)

和責任摘要。AWS Artifact這是一個自助入口網站，可隨選存取AWS合規報告。登入AWS管理主控台中的AWS Artifact，或在AWS Artifact開始使用中深入了解。

您可以從 PCI 安全標準委員會文件庫下載 PCI DSS 標準。

使用此架構幫助您進行稽核準備

您可以使用 PCI DSS V3.2.1 架構來協助您準備稽核。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據 PCI DSS 要求分組成控制集。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與您的稽核相關的證據。您建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據 PCI DSS V3.2.1 架構中定義的控制項來執行此動作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

PCI DSS V3.2.1 架構的詳細資訊如下：

AWS Audit Manager 內的架構名稱	自動化控制項數量	手動控制項數量	控制集數	AWS 服務 在範圍內
PCI DSS V3.2.1	175	487	12	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> 如果檢閱在此標準架構中作為資料來源對映使用的AWS Config規則，請下載檔案 AuditManager_ConfigDataSourceMappings_PCI-DSS-V3.2.1.zip 。

此 AWS Audit Manager 架構中的控制項，並非為了驗證您的系統是否符合 PCI DSS 標準所設計。此外，他們無法保證您會透過 PCI DSS 之稽核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控制項。

您可以在 Audit Manager 架構程式庫 的標準架構索引標籤下，找到這個架構。

如需使用此架構建立評估方式的資訊，請參閱 建立評估。

當您使用 Audit Manager 主控台從此標準架構建立評估時，範圍AWS 服務內的清單會被預設為選擇狀態且不可編輯。這是因為 Audit Manager 會自動為您映射並選擇資料來源和服務。此選擇是根據 PCI DSS V3.2.1 架構的要求所進行。如果您需要編輯此架構範圍內的服務清單，可以使用建立評估或更新評估 API操作來進行編輯。或者，您可以自訂標準架構，然後從自訂架構中建立評估。

如需自訂此架構以支援您特定需求的指引，請參閱自訂現有架構和自訂現有控制項。

更多 PCI DSS 資源

- PCI 安全標準委員會
- PCI 安全標準委員會文件庫。
- AWSPCI DSS 的合規頁面

PCI DSS V4.0

AWS Audit Manager 提供預先建置的架構，支援支付卡產業資料安全標準 (PCI DSS) v4.0。

> **Note**
>
> 如需 PCI DSS v3.2.1 以及支援此功能的 Audit Manager 架構之相關資訊，請參閱 PCI DSS V3.2.1。

主題

- 什麼是 PCI DSS？
- 使用此架構幫助您進行稽核準備
- 更多 PCI DSS 資源

什麼是 PCI DSS？

支付卡產業資料安全標準 (PCI DSS) 是一項全球標準，提供保護付款資料的技術與作業要求基準。PCI DSS v4.0 是此標準的下一代演進。

PCI DSS 的開發目的是鼓勵和強化支付卡帳戶資料的安全性。它也促進全球廣泛採用一致的資料安全措施。它提供了以保護帳戶資料為目的而設計的技術和操作要求之基準。雖然這套標準的設計重心是放在具有支付卡帳戶資料的環境，但您也可以使用 PCI DSS 來防範威脅並保護支付生態系統中的其他要素。

PCI 安全標準委員會 (PCI SSC) 在 PCI DSS v3.2.1 和 v4.0 之間引進了許多更動。這些更新分為三大類別：

1. 不斷變化的要求 – 更動的部分可確保該標準在面對新興威脅和技術時可以與時俱進，也能滿足支付產業帶來的各種變化。範例包含全新或修改的要求或測試程序，或移除某項要求。
2. 說明或指導 – 更新了措辭、解釋、定義、其他指導或指示，以增進對特定主題的瞭解或提供進一步資訊或指導。
3. 結構或格式 – 內容的重組，包含將各項要求予以組合、分離和重新編號，以便與內容一致。

如需有關變更的詳細資訊，請參閱 PCI DSS 版本 3.2.1 至 4.0 的變更摘要。

使用此架構幫助您進行稽核準備

> **Note**
>
> 此標準架構使用來自 Security Hub 的合併控制項做為資料來源。若要順利從合併控制項收集證據，請確定您已開啟 Security Hub 中的合併控制項調查結果設定。如需有關使用 Security Hub 做為資料來源類型的詳細資訊，請參閱 AWS Audit Manager 支援的 AWS Security Hub 控制項。

您可以使用 PCI DSS V4.0 架構來協助您準備稽核。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據 PCI DSS V4.0 要求分組成控制集。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與您的稽核相關的證據。您建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據 PCI DSS V4.0 架構中定義的控制項來執行此動作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可

以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

架構的詳細資訊如下：

AWS Audit Manager 內的架構名稱	自動化控制項數量	手動控制項數量	控制集數	AWS 服務 在範圍內
PCI DSS v4.0	152	128	15	• Amazon API Gateway • Amazon CloudFront • Amazon CloudWatch • Amazon DynamoDB • Amazon Elastic Compute Cloud • Amazon OpenSearch Service • Amazon Redshift • Amazon Relationa l Database Service • Amazon SageMaker • Amazon Simple Storage Service • AWS Backup • AWS CloudTrail • AWS Config

AWS Audit Manager 內的架構名稱	自動化控制項數量	手動控制項數量	控制集數	AWS 服務 在範圍內
				• AWS Identity and Access Management • AWS KMS • AWS Secrets Manager • AWS Security Hub • AWS WAF

> **Tip**
>
> 如果檢閱在此標準架構中作為資料來源對映使用的 AWS Config 規則，請下載 AuditManager_ConfigDataSourceMappings_PCI-DSS-V4.zip 檔案。

此 AWS Audit Manager 架構中的控制項，並非為了驗證您的系統是否符合 PCI DSS 標準所設計。此外，他們無法保證您會透過 PCI DSS 之稽核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控制項。

您可以在 Audit Manager 架構程式庫 的標準架構索引標籤下，找到這個架構。

如需使用此架構建立評估方式的資訊，請參閱 建立評估。

當您使用 Audit Manager 主控台從此標準架構建立評估時，範圍AWS 服務內的清單會被預設為選擇狀態且不可編輯。這是因為 Audit Manager 會自動為您映射並選擇資料來源和服務。此選擇是根據 PCI DSS V4 架構的要求所進行。如果您需要編輯此架構範圍內的服務清單，可以使用建立評估或更新評估API操作來進行編輯。或者，您可以自訂標準架構，然後從自訂架構中建立評估。

如需自訂此架構以支援您特定需求的指引，請參閱自訂現有架構和自訂現有控制項。

更多 PCI DSS 資源

- PCI DSS v4.0 Resource Hub

- PCI 安全標準委員會
- PCI 安全標準委員會文件庫。
- AWSPCI DSS 的合規頁面
- 《AWS 法規遵循指南》上的支付卡產業資料安全標準 (PCI DSS) v4.0
- PCI DSS 版本 3.2.1 至 4.0 的變更摘要

SOC 2

SOC 2 是一項稽核程序，可確保公司資料得到安全管理。AWS Audit Manager提供支援 SOC 2 的預建架構。

主題

- 什麼是 SOC 2？
- 使用此架構幫助您進行稽核準備
- 更多 SOC 2 資源

什麼是 SOC 2？

系統與組織控制 (SOC) 由美國註冊會計師協會 (AICPA) 所定義，是稽核期間產生的報告名稱。其目的是供服務組織 (向其他組織提供資訊系統服務的組織) 使用，將這些資訊系統的內部控制項驗證報表發布給這些服務使用者。這些報告著重於五個類別的控制項，稱為信任服務原則。

AWSSOC 報告是獨立的第三方檢驗報告，其中展現了 AWS 如何達成關鍵合規性控制與目標。這些報告的用途是協助您和稽核人員了解為了支援操作與法規遵循所建立的 AWS 控制。以下有五個 AWS SOC 報告：

- AWSSOC 1 回報，可供AWS客戶從AWS Artifact使用。
- AWSSOC 2 安全性、可用性和機密性報告，可供AWS客戶從AWS Artifact使用。
- AWSSOC 2 安全性、可用性和機密性報告，可供AWS客戶從AWS Artifact使用 (範圍僅包括 Amazon DocumentDB)。
- AWSSOC 2 隱私權第一類報告，可供AWS客戶從AWS Artifact使用。
- AWSSOC 3 安全性、可用性和機密性報告，以白皮書形式公開提供。

使用此架構幫助您進行稽核準備

您可以使用此架構來協助您準備稽核。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據 SOC 2 要求分組成控制集。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與您的稽核相關的證據。您建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據架構中定義的控制項來執行此動作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

架構的詳細資訊如下：

AWS Audit Manager 內的架構名稱	自動化控制項數量	手動控制項數量	控制集數	AWS 服務 在範圍內
SOC 2	20	4.1	20	• Amazon Elastic Compute Cloud • AWS Auto Scaling • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> 如果檢閱在此標準架構中，當成資料來源對應的 AWS Config 規則，請下載 AuditManager_ConfigDataSourceMappings_SOC2.zip 檔案。

此 AWS Audit Manager 架構中的控制項，並非為了驗證您的系統是否合規而設計。此外，他們無法保證您會透過稽核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控制項。

您可以在 Audit Manager 架構程式庫 的標準架構索引標籤下，找到這個架構。

如需使用此架構建立評估方式的說明，請參閱 建立評估。

當您使用 Audit Manager 主控台從此標準架構建立評估時，範圍AWS 服務內的清單會被預設為選擇狀態且不可編輯。這是因為 Audit Manager 會自動為您映射並選擇資料來源和服務。此選擇是根據 SOC 2 要求進行的。如果您需要編輯此架構範圍內的服務清單，可以使用建立評估或更新評估 API操作來進行編輯。或者，您可以自訂標準架構，然後從自訂架構中建立評估。

如需自訂此架構以支援您特定需求的指引，請參閱自訂現有架構和自訂現有控制項。

更多 SOC 2 資源

- AWSSOC 的合規頁面

控制項程式庫

您可以從 Audit Manager 中的控制項程式庫存取和管理控制項。您可以隨時移至控制項程式庫，方法是在 Audit Manager 主控台導覽窗格中選取控制項程式庫。

控制項程式庫包含標準控制項和自訂控制項目錄。

- 標準控制項是由 AWS提供的預定義控制項。您可以檢視標準控制項的組態詳細資訊，但無法編輯或刪除它們。不過，您可以自訂任何標準控制項以建立符合特定需求的新控制項。
- 自訂控制項是您持有和您定義的自訂控制項。使用自訂控制項，您可以指定要從哪些資料來源收集證據。然後，您可以將自訂控制項添加到自訂架構。

  若要進一步了解如何將自訂控制項新增至自訂架構，請參閱 架構程式庫。若要進一步了解如何從 Audit Manager 架構中產生評估，請參閱 AWS Audit Manager 中的評估。

本節說明如何在 Audit Manager 中建立和管理自訂控制項。

主題

存取 AWS Audit Manager中的可用控制項

您可以在 Audit Manager 主控台的控制項程式庫頁面，檢視所有可用的控制項。您也可以從這裡建立自訂控制項或自訂現有控制項。

您也可以使用 Audit Manager API 或 AWS Command Line Interface (AWS CLI) 來檢視所有可用的控制項。

Audit Manager console

檢視可用的控制項 (主控台)

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在導覽窗格中，選擇控制程式庫。
3. 選取標準控制項索引標籤或自訂控制項索引標籤，瀏覽可用的控制項。
4. 選擇任何控制項名稱以查看該控制項的詳細資訊。

AWS CLI

檢視可用的控制項 (AWS CLI)

執行清單控制項指令，並指定`--control-type`。或者，您可以擷取標準控制項清單。或者，您也可以擷取自訂控制項清單。

```
aws auditmanager list-controls --control-type Standard
```

```
aws auditmanager list-controls --control-type Custom
```

Audit Manager API

檢視可用的控制項 (API)

使用ListControls操作並指定控制類型。或者，您可以返回標準控制項的清單。或者，您可以返回自訂控制項的清單。

有關詳細資訊，請選擇先前的任一連結，在 AWS Audit Manager API 參考資料中閱讀更多資訊。這包括有關如何在其中一個特定語言 SDK 中使用`ListControls`操作和參數的信息 AWS 。

檢閱控制項的詳細資訊

您可以使用 Audit Manager 主控台、Audit Manager API 或 AWS Command Line Interface (AWS CLI) 來檢閱控制項的詳細資訊。

Audit Manager console

若要檢視控制詳細資訊（主控台）

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在導覽窗格中，選擇控制項資料庫以查看可用控制項的清單。
3. 選取標準控制項索引標籤或自訂控制項索引標籤，瀏覽可用的控制項。
4. 選擇任何控制項名稱以查看該控制項的詳細資訊。

開啟控制項時，您會看到控制項詳細資訊頁面。本頁面的各個章節及其內容說明如下。

摘要章節

本節提供控制項的概觀。其包含下列資訊：

- 控制項名稱 — 控制項的名稱。
- 控制項類型 — 指定控制項是標準控制項還是自訂控制項。
- 標籤 — 與控制項相關聯的標籤數量。
- 資料來源類型 — 用於此控制項的資料來源類型數量。
- 映射項目 — 用於從資料來源擷取資料的映射屬性數量。

如果您正在檢視自訂控制項，也會顯示下列詳細資訊：

- 建立者 — 建立自訂控制項的帳戶。
- 建立日期— 建立自訂控制項的日期。
- 上次更新 — 上次編輯自訂控制項的日期。

詳細資訊索引標籤

此索引標籤提供控制項的基本概觀。其包含下列資訊：

- 說明章節提供控制項的描述。
- 測試資訊章節提供控制項之建議測試程序的說明。
- 行動計劃章節說明需要修正控制項時，要執行的建議動作。

資料來源索引標籤

此索引標籤會顯示控制項之資料來源的相關資訊。其包含下列資訊：

- 資料來源名稱 — 這僅適用於自訂控制項。它指的是您為每個資料來源提供的描述性名稱。您可以使用此名稱，從多個資料來源中篩選出具備相同類型的資料來源。
- 資料來源類型 — 指定證據資料的來源。
  - 如果 Audit Manager 收集證據，則資料來源可以是下列四種類型之一：AWS Security HubAWS ConfigAWS CloudTrail、、或 AWS API 呼叫。
  - 如果您上傳自己的證據，則資料來源類型為手動。說明會指出所需的手動證據是檔案上傳還是文字回應。
- 映射項目-這是用於分辨資料來源並檢索資料的映射屬性。
  - 如果資料來源類型為 AWS Config，則對映為特定 AWS Config 規則的名稱 (例如`EC2_INSTANCE_MANAGED_BY_SSM`)。Audit Manager 會使用此對映，直接從中報告該規則檢查的結果 AWS Config。
  - 如果資料來源類型為 AWS Security Hub，則對應就是特定 Security Hub 控制項的名稱 (例如，`1.1 – Avoid the use of the "root" account`)。Audit Manager 使用此映射項目直接從 Security Hub 報告該安全檢查的結果。
  - 如果資料來源類型是 AWS API 呼叫，則對應就是特定 API 呼叫的名稱 (例如`ec2_DescribeSecurityGroups`)。Audit Manager 會使用此映射項目來收集 API 回應。
  - 如果資料來源是 AWS CloudTrail，則對映為特定 CloudTrail 事件的名稱 (例如`CreateAccessKey`)。Audit Manager 會使用此對應，從您的 CloudTrail 記錄檔收集相關的使用者活動。
- 頻率 — 此指定 Audit Manager 從資料來源收集證據的頻率。頻率會根據資料來源類型而有所不同。如需詳細資訊，請在欄中選擇值，或參閱 證據收集頻率。

標籤索引標籤

此索引標籤會列出與控制項相關聯的標籤。其包含下列資訊：

- 金鑰 — 標籤索引鍵 (例如合規性標準、法規或類別)。
- 值 — 標籤值。

AWS CLI

若要檢視控制項詳細資訊 (AWS CLI)

1. 若要找到您要檢視的控制項，請執行列出控制項命令並指定`--control-type`。或者，您可以擷取標準控制項清單。或者，您也可以擷取自訂控制項清單。

在下列範例中，將######取代為Custom或Standard。

```
aws auditmanager list-controls --control-type Custom/Standard
```

回應會傳回控制項清單。找到您要檢閱的控制項，並記下控制 ID 和 Amazon Resource Name (ARN)。

2. 若要取得控制項詳細資訊，請執行列出控制項命令並指定--control-id。

   在下列範例中，將######取代為您自己的資訊。

   ```
   aws auditmanager get-control --control-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

   控制項詳細資訊會以 JSON 格式傳回。若要瞭解此資料，請參閱AWS CLI 指令參考中的取得控制項輸出。

3. 若要查看控制項的標籤，請使用指list-tags-for-resource令並指--resource-arn定控制項的。

   在下列範例中，將######取代為您自己的資訊：

   ```
   aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:control/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

   如需有關 Audit Manager 中標籤的詳細資訊，請參閱標籤 AWS Audit Manager 資源。

Audit Manager API

若要檢視控制項詳細資訊 (API)

1. 若要識別您要檢閱的控制項，請使用該ListControls作業並指定 Con trolType。或者，您可以返回標準控制項的清單。或者，您可以返回自訂控制項的清單。

   從回應中找到您要檢閱的控制項，並記下控制 ID 和 Amazon Resource Name (ARN)。

2. 若要取得控制項詳細資料，請使用GetControl作業。在要求中，指定您從步驟 1 取得的控制 ID。

   控制項詳細資訊會以 JSON 格式傳回。若要瞭解此資料，請參閱 AWS Audit Manager API 參考中的GetControl 回應元素。

3. 若要查看控制項的標籤，請使用此ListTagsForResource作業。在請求中，指定您從步驟 1 取得的控制 resourceArn。

如需有關 Audit Manager 中標籤的詳細資訊，請參閱標籤 AWS Audit Manager 資源。

有關此 API 操作的更多資訊，請選擇先前的任一連結，在 AWS Audit Manager API 參考資料中閱讀更多資訊。這包括有關如何在其中一個特定語言 AWS SDK 中使用這些操作和參數的資訊。

建立自訂控制項

您可以使用自訂控制項，從您定義的特定資料來源收集證據。

就像標準控制項一樣，啟用的自訂控制項會在您的評估中持續收集證據。您也可以將手動證據新增至您建立的任何自訂控制項。每個證據都會成為記錄，協助您證明是否符合自訂控制項的需求。

若要開始使用，以下是如何使用自訂控制的範例：

使用現有的控制項做為起點

您可以在 Audit Manager 中自訂任何控制項。如果現有控制項或多或少符合您的目標，但您想要擴展適用範圍或調整一些屬性以滿足特定需求，這是一個不錯的選擇。例如，您可以變更控制項收集證據的頻率，然後依此變更控制項的名稱。

建立內部稽核的自訂控制項

為支援內部稽核，您可以建立一個專屬的自訂控制項，這個控制項與任何特定合規架構或法規都沒有關連性。您可以藉此自由地根據特定區域量身打造控制項的要求，或從特定商務資源中收集證據。例如，您可以建立使用組織的自訂 AWS Config 規則做為證據收集的資料來源的自訂控制項。

建立供應商風險評估問題

您可以使用自訂控制項來支援管理供應商風險評估的方式。您建立的每個控制項，都可以代表個別的風險評估問題。在這種情況下，控制項名稱可以是一個提問，您可以上傳檔案或輸入文字回應作為手動證據來提供答案。

有兩種方法可以建立自訂控制項。您可以從頭開始建立新的控制項，也可以自訂現有的控制項。

主題

- 從頭建立新的自訂控制項

- 自訂現有控制項

從頭建立新的自訂控制項

您可以按照以下步驟，從頭開始建立新的自訂控制項。

> **Important**
>
> 強烈建議您千萬不要將控制項詳細資訊放入自由格式欄位中，例如控制項詳細資訊、測試資訊或行動計劃。如果您建立內含敏感資訊的自訂控制項，您不得共用包含這些控制項的任何自訂架構。

主題

- 步驟 1：指定控制項詳細資訊
- 步驟 2：設定資料來源
- 步驟 3（選擇性）：定義行動計劃
- 步驟 4：檢閱並建立控制項
- 我接下來要怎麼做？

步驟 1：指定控制項詳細資訊

首先指定自訂控制項的詳細資訊。

如需指定控制項詳細資訊

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在導覽窗格中選取控制項資料庫，然後選取建立自訂控制項。
3. 在控制項詳細資訊下，輸入下列有關控制項的資訊。
   - 控制項 — 輸入好記的名稱、標題或風險評估問題。此值可協助您分辨控制項程式庫中的控制項。
   - 說明（選擇性）— 輸入詳細資訊，協助其他人瞭解控制項的目標。此說明會顯示在控制項詳細資訊頁面上。

4. 在測試資訊下，輸入測試控制項的建議步驟。
5. 在標籤下，選擇新增標籤，將標籤與控制項產生關聯。您可以指定一個索引鍵，為此控制項支援的相容性架構標籤提供最適合的說明。標籤索引鍵是必要的，當您在控制項程式庫中搜尋此控制項時，可用來做為搜尋條件。
6. 選擇下一步。

步驟 2：設定資料來源

下一步，定義最多 10 個資料來源。資料來源決定您的自訂控制項從何處收集證據。

如果您想要收集自動證據，每個資料來源都必須包含資料來源類型和資料來源映射項目。這些詳細資料會對應到您的 AWS 使用情況，並告知 Audit Manager 從何處收集證據。如果您想改為提供自己的證據，則要為資料來源命名，然後選擇手動證據選項。

> **Important**
>
> 若要成功使用 AWS Config 和 Security Hub 做為自動化資料來源，請確定您執行下列動作：
>
> - 依照指示設定 AWS Config並設定 Security Hub，以便與 Audit Manager 搭配使用。
> - 在評估範圍中包含 AWS Config 和安全中心作為服務。
>
> 然後，每次針對您在此步驟中指定的 AWS Config 規則或 Security Hub 控制項進行評估時，Audit Manager 都可以收集證據。

如需設定資料來源

1. 在資料來源名稱下，以資料來源的描述性名稱取代預留位置文字。
2. 在證據收集方法下，選擇您要如何收集此控制項的證據。

   a. 如果您希望 Audit Manager 收集證據，請選擇自動化，然後遵循下列步驟：

      - 在資料來源類型下，指定 Audit Manager 收集自動證據的來源。
        - 對於 AWS CloudTrail，從下拉式清單中選擇事件名稱關鍵字。
        - 對於 AWS Config，請選取規則類型，然後從下拉式清單中選擇規則識別碼關鍵字。
        - 針對 AWS Security Hub，從下拉式清單中選擇 Security Hub 控制項。
        - 對於 AWS API 呼叫，請選擇 API 呼叫，然後選取證據收集頻率。

> **Tip**
>
> 如需每個資料來源類型的概觀及相關疑難排解秘訣，請參閱自動化資料來源概觀。如果您需要與網域專家一起驗證資料來源組態，請立即將證據收集方法設定為手動。這樣，您就可以建立控制項並立即將其新增至架構，然後視需要編輯控制項。

b. 如果您要提供自己的證據，請選擇手動，然後選取手動證據選項。

- 檔案上傳 — 如果控制項需要文件作為證據，請選取此選項。
- 文字回應 — 如果控制項需要風險評估問題的答案，請選取此選項。

3. （選擇性）在其他詳細資訊下，輸入資料來源說明和疑難排解說明。
4. （選擇性）若要新增另一個資料來源，選擇新增資料來源，然後重複步驟 1 至 3。
5. （選擇性）若要移除資料來源，請選擇資料來源組態方塊頂端的 移除。
6. 完成時，選擇下一步。

步驟 3（選擇性）：定義行動計劃

接下來，指定需要修正此控制項時要採取的動作。

如需定義行動計劃

1. 在標題下，輸入行動計劃的描述性標題。
2. 在行動計劃指示下，輸入行動計劃的詳細指示。
3. 選擇下一步。

步驟 4：檢閱並建立控制項

檢閱控制項的資訊。如需變更步驟的資訊，請選擇編輯。

完成時，請選擇建立自訂控制項。

我接下來要怎麼做？

建立新的自訂控制項之後，您可以將其新增至自訂架構。如需進一步了解，請參閱 建立自訂架構 和 編輯自訂架構。

將自訂控制項新增至自訂架構後，您可以從該自訂架構建立評估，並開始收集證據。如需進一步了解，請參閱 建立評估。

如需疑難排解秘訣，請參閱 控制項和控制集問題疑難排解。

自訂現有控制項

除了從頭開始建立自訂控制項，您可以使用現有的控制項做為起點，並根據您的需求進行自訂。當您執行此作業時，現有的控制項會保留在控制項程式庫中，而且會使用您的自訂設定建立新的自訂控制項。

您可以選取要自訂的任何現有控制項。它可以是標準控制項或自訂控制項。

> **Important**
>
> 強烈建議您千萬不要將控制項詳細資訊放入自由格式欄位中，例如控制項詳細資訊、測試資訊或行動計劃。如果您建立內含敏感資訊的自訂控制項，您不得共用包含這些控制項的任何自訂架構。

主題

步驟 1：指定控制項詳細資訊

控制項詳細資訊內容擷取自原始控制項。視需要檢閱和修改這些詳細資訊。

如需指定控制項詳細資訊

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在導覽窗格中，選擇控制程式庫。
3. 選取您要自訂的控制項，然後選擇自訂現有的控制項。
4. 指定控制項的新名稱，然後選擇自訂。

5. 在控制項詳細資訊底下，視需要自訂控制項詳情。
6. 在測試資訊下，視需要自訂測試資訊。
7. 在標籤下，視需要自訂標籤。
8. 選擇下一步。

步驟 2：設定資料來源

資料來源會繼承自原始控制項。您可以視需要變更、新增或移除資料來源。

> **Important**
>
> 若要成功使用 AWS Config 和 Security Hub 做為自動化資料來源，請確定您執行下列動作：
>
> - 依照指示設定 AWS Config並設定 Security Hub，以便與 Audit Manager 搭配使用。
> - 在評估範圍中包含 AWS Config 和安全中心作為服務。
>
> 然後，每次針對您在此步驟中指定的 AWS Config 規則或 Security Hub 控制項進行評估時，Audit Manager 都可以收集證據。

如需設定資料來源

1. 在 資料來源名稱 下，視需要自訂資料來源名稱。
2. 在證據收集方法下，視需要自訂選取項目。
   a. 如果您希望 Audit Manager 收集證據，請選擇自動化，然後遵循下列步驟：
      - 在 資料來源類型 下，檢閱 Audit Manager 從何處收集自動證據，並視需要進行修改。
        - 對於 AWS CloudTrail，從下拉式清單中選擇事件名稱關鍵字。
        - 對於 AWS Config，請選取規則類型，然後從下拉式清單中選擇規則識別碼關鍵字。
        - 針對 AWS Security Hub，從下拉式清單中選擇 Security Hub 控制項。
        - 對於 AWS API 呼叫，請選擇 API 呼叫，然後選取證據收集頻率。

> **Tip**
>
> 如需每個資料來源類型的概觀及相關疑難排解秘訣，請參閱自動化資料來源概觀。

如果您需要與網域專家一起驗證資料來源組態，請立即將證據收集方法設定為手動。這樣，您就可以建立控制項並立即將其新增至架構，然後視需要編輯控制項。

b. 如果您要提供自己的證據，請選擇手動，然後選取手動證據選項。

- 檔案上傳 — 如果控制項需要文件作為證據，請選取此選項。
- 文字回應 — 如果控制項需要風險評估問題的答案，請選取此選項。

3. （選擇性）在其他詳細資訊下，對資料來源說明或疑難排解說明進行任何必要的變更。
4. （選擇性）若要新增另一個資料來源，選擇新增資料來源。
5. （選擇性）若要移除資料來源，請選擇移除。
6. 選擇下一步。

步驟 3：（選擇性）：定義行動計劃

行動計劃會繼承自原始控制項。您可以視需要編輯此行動計劃。

如需定義行動計劃

1. 在標題下，檢閱行動計劃的標題，並視需要自訂標題。
2. 在行動計劃指示下，視需要檢閱並自訂指示。
3. 選擇下一步。

步驟 4：檢閱並建立控制項

檢閱控制項的資訊。如需變更步驟的資訊，請選擇編輯。完成時，請選擇建立自訂控制項。

我接下來要怎麼做？

建立新的自訂控制項之後，您可以將其新增至自訂架構。如需進一步了解，請參閱 建立自訂架構 和 編輯自訂架構。

將自訂控制項新增至自訂架構後，您可以從該自訂架構建立評估，並開始收集證據。如需進一步了解，請參閱 建立評估。

如果您需要編輯自訂控制項，請參閱編輯自訂控制項。

如需疑難排解秘訣，請參閱 控制項和控制集問題疑難排解。

編輯自訂控制項

您可以依照下列步驟在 Audit Manager 中編輯自訂控制項。

主題

步驟 1：編輯控制項詳細資訊

首先，視需要檢閱和編輯控制項詳細資訊。

若要編輯控制項詳細資訊

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在導覽窗格中選取控制項資料庫，然後選取建立自訂控制項標籤。
3. 選取您要編輯的控制項，並選擇編輯。
4. 在控制項詳細資訊底下，視需要編輯控制項詳細資訊。
5. 在測試資訊下，視需要編輯推薦測試資訊。
6. 選擇下一步。

> **Tip**
>
> 若要編輯控制項的標籤，請開啟控制項，然後選擇標籤 索引標籤。您可以在此檢視和編輯與控制項相關聯的標籤。

步驟 2：編輯資料來源

接下來，您可以編輯、移除或新增控制項的資料來源。

> **Important**
>
> 若要成功使用 AWS Config 和 Security Hub 做為自動化資料來源，請確定您執行下列動作：
>
> - 依照指示設定 AWS Config並設定 Security Hub，以便與 Audit Manager 搭配使用。
> - 在評估範圍中包含 AWS Config 和安全中心作為服務。
>
> 然後，每次針對您在此步驟中指定的 AWS Config 規則或 Security Hub 控制項進行評估時，Audit Manager 都可以收集證據。

編輯資料來源

1. 在資料來源名稱下，檢閱目前名稱並視需要進行編輯。
2. 在證據收集方法下，檢閱目前的選取項目並視需要進行編輯。

   a. 如果您希望 Audit Manager 收集證據，請選擇自動化，然後遵循下列步驟：

      - 在 資料來源類型 下，檢閱 Audit Manager 從何處收集自動證據，並視需要進行修改。
        - 對於 AWS CloudTrail，從下拉式清單中選擇事件名稱關鍵字。
        - 對於 AWS Config，請選取規則類型，然後從下拉式清單中選擇規則識別碼關鍵字。
        - 針對 AWS Security Hub，從下拉式清單中選擇 Security Hub 控制項。
        - 對於 AWS API 呼叫，請選擇 API 呼叫，然後選取證據收集頻率。

      > **Tip**
      >
      > 如需每個資料來源類型的概觀及相關疑難排解秘訣，請參閱自動化資料來源概觀。

   b. 如果您要提供自己的證據，請選擇手動，然後選取手動證據選項。

      - 檔案上傳 — 如果控制項需要文件作為證據，請選取此選項。
      - 文字回應 — 如果控制項需要風險評估問題的答案，請選取此選項。
3. （選擇性）在其他詳細資訊下，對資料來源說明或疑難排解說明進行任何必要的變更。
4. （選擇性）若要新增另一個資料來源，選擇新增資料來源。
5. （選擇性）若要移除資料來源，請選擇移除。
6. 選擇下一步。

步驟 3（選擇性）：編輯行動計劃

接下來，檢閱並編輯選用的行動計劃。

若要編輯行動計劃

1. 在標題下，視需要編輯標題。
2. 在行動計劃指示下，視需要編輯指示。
3. 選擇下一步。

步驟 4：檢閱並更新控制項

檢閱控制項的資訊。如需變更步驟的資訊，請選擇編輯。

完成時，請選擇儲存變更。

> **Note**
>
> 編輯控制項之後，變更會在包含控制項的所有使用中評估中生效，如下所示：
>
> - 對於以 AWS API 呼叫做為資料來源類型的控制項，變更會在次日的 00:00 UTC 生效。
> - 之於所有其他控制項，變更會立即生效。

刪除自訂控制項

您可以使用控制項程式庫刪除不想要的自訂控制項。刪除控制項之後，該控制項將不再出現在控制項程式庫中。您也可以使用 Audit Manager API 或 AWS Command Line Interface (AWS CLI) 刪除自訂控制項。

> **Important**
>
> 當您刪除自訂控制項時，此動作會從目前相關的任何自訂架構或評估中移除控制項。因此，Audit Manager 將停止收集在您所有評估中該自訂控制項的證據。這包括您先前在刪除自訂控制項之前建立的評估。

Audit Manager console

要刪除自訂控制（主控台）

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在導覽窗格中選取控制項資料庫，然後選取建立自訂控制項標籤。
3. 選取您要刪除的控制項，然後選擇刪除。
4. 在出現的快顯視窗中，選擇刪除以確認刪除。

AWS CLI

若要刪除自訂控制項 (AWS CLI)

1. 首先，找出您要刪除的自訂控制項。為此，請執行 list-controls 指令，並指定 `--control-type` 為 `Custom`。

   ```
   aws auditmanager list-controls --control-type Custom
   ```

   回應會傳回自訂控制項。找到您要刪除的控制項，並記下控制項 ID。
2. 接下來，執行刪除控制項指令，並使用 `--control-id` 參數來指定要刪除的控制項。

   在下列範例中，將*######*取代為您自己的資訊。

   ```
   aws auditmanager delete-control --control-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

Audit Manager API

若要刪除自訂控制項 (API)

1. 使用該ListControls操作並將控制類型指定為`Custom`。從回應中找到您要刪除的控制項並記下控制項 ID。
2. 使用此DeleteControl作業刪除自訂控制項。在要求中，使用controlId參數來指定您要刪除的控制項。

有關此 API 操作的更多資訊，請選擇先前的任一連結，在 AWS Audit Manager API 參考資料中閱讀更多資訊。這包括有關如何在其中一個特定語言 AWS SDK 中使用這些操作和參數的資訊。

變更控制項的證據收集頻率

AWS Audit Manager 以不同頻率從多個資料來源收集證據。支援的證據收集頻率取決於為控制項收集的證據類型。

- 針對 AWS API 呼叫，Audit Manager 會使用對其他人 AWS 服務的描述 API 呼叫來收集證據。您可以直接在 Audit Manager 中指定證據收集頻率（僅適用於自訂控制項）。
- 對於 AWS Config，「Audit Manager」會直接從中報告符合性檢查的結果 AWS Config。頻率會遵循 AWS Config 規則中定義的觸發。
- 針對 AWS Security Hub，Audit Manager 會直接從 Security Hub 回報合規檢查的結果。頻率會遵循 Security Hub 的檢查排程。
- 對於 AWS CloudTrail，Audit Manager 會持續收集來自的證據 CloudTrail。您無法變更此證據類型的頻率。

下列各章節提供關於每個控制項資料來源類型的證據收集頻率相關資訊，及其變更方式 (如果適用)。

主題

來自 AWS API 呼叫的組態快照

> **Note**
>
> 以下內容僅適用於自訂控制項。您無法變更使用將 API 呼叫做為資料來源的標準控制項的證據收集頻率。

如果自訂控制項使用 AWS API 呼叫做為資料來源類型，您可以依照下列步驟在 Audit Manager 中變更證據收集頻率。

使用 API 呼叫資料來源變更自訂控制項的證據收集頻率

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在導覽窗格中，選擇控制項程式庫，接著選擇自訂控制項索引標籤。
3. 選擇您要編輯的自訂控制項，並選擇編輯。
4. 在編輯控制項詳細資訊頁面上，選擇下一步。
5. 尋找您要編輯的資料來源方塊，並確認下列資訊正確：
   - 證據收集方法是自動化的。
   - 資料來源類型為 AWS API 呼叫。
   - 所選 API 呼叫是您要變更頻率的呼叫。
6. 在頻率下，選擇您要為自訂控制項收集證據的頻率。
7. 根據需求重複步驟 5-6，以編輯您想要修改的任何其他 API 呼叫資料來源。。
8. 選擇下一步。
9. 在編輯行動計劃頁面上，選擇下一步。
10. 在檢閱並更新控制項頁面上，檢閱自訂控制項資訊。如需變更步驟的資訊，請選擇編輯。
11. 完成時，請選擇儲存變更。

在您編輯以 AWS API 呼叫做為資料來源類型的控制項之後，變更會在包含控制項的所有使用中評估中，於次日 00:00 UTC 生效。

AWS Config合規檢查

> **Note**
>
> 以下內容適用於使用 AWS Config 規則 做為資料來源使用的標準控制項和自訂控制項。

如果控制項用 AWS Config 作資料來源類型，您無法直接在 Audit Manager 中變更證據收集頻率。這是因為頻率遵循 AWS Config 規則中定義的觸發程序。

有兩種類型的觸發器 AWS Config 規則：

1. 組態變更- AWS Config 在建立、變更或刪除特定類型的資源時，執行規則的評估。
2. 週期性-以您選擇的頻率 AWS Config 執行規則評估 (例如，每 24 小時)。

若要深入瞭解的觸發器 AWS Config 規則，請參閱開發AWS Config 人員指南中的觸發器類型。

如需如何管理的指示 AWS Config 規則，請參閱管理 AWS Config 規則。

安全中心的合規檢查

> **Note**
>
> 以下內容適用於使用 Security Hub 檢查做為資料來源的標準控制項和自訂控制項。

如果控制項使用 Security Hub 做為資料來源類型，您無法直接在 Audit Manager 中變更證據收集頻率。這是因為頻率遵循 Security Hub 的檢查排程。

- 定期檢查會在最近一次執行後的 12 小時內自動執行。您無法變更其週期性。
- 變更觸發檢查會在關聯資源變更狀態時執行。即使資源未變更狀態，變更觸發檢查的時間也會每 18 小時重新整理一次更新。這有助於指出控制是否仍已啟用。一般而言，Security Hub 會盡可能地使用變更觸發規則。

若要深入瞭解，請參閱AWS Security Hub 使用指南中的執行安全檢查的排程。

使用者活動日誌 AWS CloudTrail

> **Note**
>
> 以下內容適用於使用 AWS CloudTrail 使用者活動日誌做為資料來源的標準控制項和自訂控制項。

您無法變更使用活動記錄 CloudTrail 做為資料來源類型之控制項的證據收集頻率。Audit Manager 會以連續的方式收集此證據類型。 CloudTrail 頻率是連續的，因為使用者活動可能在一天中的任何時間發生。

支援自動證據的控制資料來源

在中建立自訂控制項時 AWS Audit Manager，您可以設定控制項，以從下列資料來源類型收集自動證據：

- AWS CloudTrail
- AWS Security Hub
- AWS Config
- AWS API 呼叫

下列主題概述了這些自動化資料來源類型，並列出 Audit Manager 支援的特定 AWS Security Hub 控制項、 AWS Config 規則和 AWS API 呼叫。

主題

自動化資料來源概觀

下表概述了每種自動資料來源類型的概觀。

Data source type (資料來源類型)	說明	證據收集頻率	如需使用此資料來源類型.....	當此控制項在評估中處於使用中狀態時...	相關的疑難排解秘訣
AWS CloudTrail	追蹤特定使用者活動。	持續。	從支援的事件名稱清單中選取。	Audit Manager 會根據您選擇的關鍵字篩選 CloudTrail 記錄。結果會匯入為使用者活動證據。	我的評估不會從 AWS CloudTrail 中收集使用者

Data source type (資料來源類型)	說明	證據收集頻率	如需使用此資料來源類型.....	當此控制項在評估中處於使用中狀態時...	相關的疑難排解秘訣
					活動證據
AWS Config	透過報告發現項目來擷取資源安全狀況的快照 AWS Config。	根據 AWS Config 規則中定義的觸發程序。	選擇規則類型，然後選取規則。 • 對於受管規則，請從支援的受管規則關鍵字清單中選取。 • 對於自訂規則，請從可用規則清單中選取。	Audit Manager 會直接從取得此規則的發現項目 AWS Config。結果會匯入為合規檢查證據。	我的評估并未從 AWS Config 中收集合規檢查證據 AWS Config 整合問題

Data source type (資料來源類型)	說明	證據收集頻率	如需使用此資料來源類型.....	當此控制項在評估中處於使用中狀態時...	相關的疑難排解秘訣
AWS Security Hub	透過 Security Hub 報告調查結果，擷取資源安全狀況的快照。	根據 Security Hub 的檢查排程。	從支援的 Security Hub 控制識別碼清單中選取。	Audit Manager 會直接從 Security Hub 取得安全檢查的結果。結果會匯入為合規檢查證據。	我的評估并未從 AWS Security Hub 中收集合規檢查證據
AWS API 呼叫	透過指定的 API 呼叫，直接擷取資源組態的快照 AWS 服務。	每日、每週或每月。	從支援的 API 呼叫清單中選取，然後選取您偏好的頻率。	Audit Manager 會根據您的指定頻率進行 API 呼叫。系統會將回應匯入為組態資料證據。	我的評估并未收集 AWS API 呼叫的組態資料證據

AWS Config 規則 支持 AWS Audit Manager

您可以使用 Audit Manager 來擷取 AWS Config 評估作為稽核的證據。建立或編輯自訂控制項時，您可以指定一或多個 AWS Config 規則作為證據收集的資料來源對應。 AWS Config 根據這些規則執行符合性檢查，「Audit Manager」會將結果報告為符合性檢查證據。

除了受管規則之外，您還可以將自訂規則映射至控制項資料來源。

> **Note**
>
> - Audit Manager 不會從服務連結 AWS Config 規則中收集證據，但來自一致性套件和來源的服務連結規則除外。 AWS Organizations如需詳細資訊，請參閱本指南的疑難排解一節。
> - Audit Manager 不會為您管理 AWS Config 規則。開始收集證據之前，建議您先檢閱目前的 AWS Config 規則參數。然後，根據所選架構的要求來驗證這些參數。如果需要，您可以更新 AWS Config中的規則參數，使其符合架構需求。這將有助於確保您的評估為該架構收集正確的合規檢查證據。
>
>   例如，假設您正在為 CIS v1.2.0 建立評估。此架構包含一個名為 1.9 — 確保 IAM 密碼政策的長度至少需要 14 或更高的控制項。在中 AWS Config，iam-password-policy規則具有檢查密碼長度的`MinimumPasswordLength`參數。此參數的預設值為 14 字元。因此，該規則符合控制項的需求。如果您沒有使用預設參數值，請確保您使用的值等於或大於 CIS v1.2.0 的 14 個字元要求。您可以在 AWS Config 文件中找到每個受管規則的預設參數詳細資訊。

主題

- 搭配稽核 AWS Config 管理員使用受管規則
- 搭配 Audit Manager 使用 AWS Config 自訂規則
- 與 Audit Manager 的 AWS Config 整合疑難

搭配稽核 AWS Config 管理員使用受管規則

稽核 AWS Config 管理員目前支援 326 個受管規則。當您為自訂控制項設定資料來源時，您可以使用下列任何一個受管規則識別碼關鍵字。如需有關下列任何受管規則的詳細資訊，請從清單中選擇項目，或參閱AWS Config 使用者指南中的AWS Config 受管規則。

> **Tip**
>
> 當您在建立自訂控制項期間在 Audit Manager 主控台中選擇受管規則時，請確定您尋找下列其中一個規則識別碼關鍵字，而非規則名稱。如需規則名稱和規則識別碼之間的差異，以及如何尋找受管規則識別碼的詳細資訊，請參閱本使用手冊的疑難排解一節。

支援 AWS Config 受管規則關鍵字

- ACCESS_KEYS_ROTATED
- ACCOUNT_PART_OF_ORGANIZATIONS
- ACM_CERTIFICATE_EXPIRATION_CHECK
- ACM_CERTIFICATE_RSA_CHECK
- ALB_DESYNC_MODE_CHECK
- ALB_HTTP_DROP_INVALID_HEADER_ENABLED
- ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK
- ALB_WAF_ENABLED
- API_GW_ASSOCIATED_WITH_WAF
- API_GW_CACHE_ENABLED_AND_ENCRYPTED
- API_GW_ENDPOINT_TYPE_CHECK
- API_GW_EXECUTION_LOGGING_ENABLED
- API_GW_SSL_ENABLED
- API_GW_XRAY_ENABLED
- API_GWV2_ACCESS_LOGS_ENABLED
- API_GWV2_AUTHORIZATION_TYPE_CONFIGURED
- APPROVED_AMIS_BY_ID
- APPROVED_AMIS_BY_TAG
- APPSYNC_ASSOCIATED_WITH_WAF
- APPSYNC_CACHE_ENCRYPTION_AT_REST
- APPSYNC_LOGGING_ENABLED
- AURORA_LAST_BACKUP_RECOVERY_POINT_CREATED
- AURORA_MYSQL_BACKTRACKING_ENABLED

支援 AWS Config 受管規則關鍵字

- AURORA_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- AUTOSCALING_CAPACITY_REBALANCING
- AUTOSCALING_GROUP_ELB_HEALTHCHECK_REQUIRED
- AUTOSCALING_LAUNCH_CONFIG_HOP_LIMIT
- AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED
- AUTOSCALING_LAUNCHCONFIG_REQUIRES_IMDSV2
- AUTOSCALING_LAUNCH_TEMPLATE
- AUTOSCALING_MULTIPLE_AZ
- AUTOSCALING_MULTIPLE_INSTANCE_TYPES
- BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK
- BACKUP_RECOVERY_POINT_ENCRYPTED
- BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED
- BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK
- BEANSTALK_ENHANCED_HEALTH_REPORTING_ENABLED
- CLB_DESYNC_MODE_CHECK
- CLB_MULTIPLE_AZ
- CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED
- CLOUD_TRAIL_ENABLED
- CLOUD_TRAIL_ENCRYPTION_ENABLED
- CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED
- CLOUDFORMATION_STACK_DRIFT_DETECTION_CHECK
- CLOUDFORMATION_STACK_NOTIFICATION_CHECK
- CLOUDFRONT_ACCESSLOGS_ENABLED
- CLOUDFRONT_ASSOCIATED_WITH_WAF
- CLOUDFRONT_CUSTOM_SSL_CERTIFICATE
- CLOUDFRONT_DEFAULT_ROOT_OBJECT_CONFIGURED
- CLOUDFRONT_NO_DEPRECATED_SSL_PROTOCOLS
- CLOUDFRONT_ORIGIN_ACCESS_IDENTITY_ENABLED
- CLOUDFRONT_ORIGIN_FAILOVER_ENABLED

支援 AWS Config 受管規則關鍵字

- CLOUDFRONT_S3_ORIGIN_ACCESS_CONTROL_ENABLED
- CLOUDFRONT_S3_ORIGIN_NON_EXISTENT_BUCKET
- CLOUDFRONT_SECURITY_POLICY_CHECK
- CLOUDFRONT_SNI_ENABLED
- CLOUDFRONT_TRAFFIC_TO_ORIGIN_ENCRYPTED
- CLOUDFRONT_VIEWER_POLICY_HTTPS
- CLOUDTRAIL_S3_DATAEVENTS_ENABLED
- CLOUDTRAIL_SECURITY_TRAIL_ENABLED
- CLOUDWATCH_ALARM_ACTION_CHECK
- CLOUDWATCH_ALARM_ACTION_ENABLED_CHECK
- CLOUDWATCH_ALARM_RESOURCE_CHECK
- CLOUDWATCH_ALARM_SETTINGS_CHECK
- CLOUDWATCH_LOG_GROUP_ENCRYPTED
- CMK_BACKING_KEY_ROTATION_ENABLED
- CODEBUILD_PROJECT_ARTIFACT_ENCRYPTION
- CODEBUILD_PROJECT_ENVIRONMENT_PRIVILEGED_CHECK
- 編碼生成 _ 項目 _ 恩瓦爾 _ AWSCRED_CHECK
- CODEBUILD_PROJECT_LOGGING_ENABLED
- CODEBUILD_PROJECT_S3_LOGS_ENCRYPTED
- CODEBUILD_PROJECT_SOURCE_REPO_URL_CHECK
- CODEDEPLOY_AUTO_ROLLBACK_MONITOR_ENABLED
- CODEDEPLOY_EC2_MINIMUM_HEALTHY_HOSTS_CONFIGURED
- CODEDEPLOY_LAMBDA_ALLATONCE_TRAFFIC_SHIFT_DISABLED
- CODEPIPELINE_DEPLOYMENT_COUNT_CHECK
- CODEPIPELINE_REGION_FANOUT_CHECK
- CUSTOM_SCHEMA_REGISTRY_POLICY_ATTACHED
- CW_LOGGROUP_RETENTION_PERIOD_CHECK
- DAX_ENCRYPTION_ENABLED
- DB_INSTANCE_BACKUP_ENABLED

支援 AWS Config 受管規則關鍵字

- DESIRED_INSTANCE_TENANCY
- DESIRED_INSTANCE_TYPE
- DMS_REPLICATION_NOT_PUBLIC
- DYNAMODB_AUTOSCALING_ENABLED
- DYNAMODB_IN_BACKUP_PLAN
- DYNAMODB_LAST_BACKUP_RECOVERY_POINT_CREATED
- DYNAMODB_PITR_ENABLED
- DYNAMODB_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- DYNAMODB_TABLE_ENCRYPTED_KMS
- DYNAMODB_TABLE_ENCRYPTION_ENABLED
- DYNAMODB_THROUGHPUT_LIMIT_CHECK
- EBS_IN_BACKUP_PLAN
- EBS_LAST_BACKUP_RECOVERY_POINT_CREATED
- EBS_OPTIMIZED_INSTANCE
- EBS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK
- EC2_CLIENT_VPN_NOT_AUTHORIZE_ALL
- 識別碼：EC2_EBS_ENCRYPTION_BY_DEFAULT
- EC2_IMDSV2_CHECK
- EC2_INSTANCE_DETAILED_MONITORING_ENABLED
- EC2_INSTANCE_MANAGED_BY_SSM
- EC2_INSTANCE_MULTIPLE_ENI_CHECK
- EC2_INSTANCE_NO_PUBLIC_IP
- EC2_INSTANCE_PROFILE_ATTACHED
- EC2_LAST_BACKUP_RECOVERY_POINT_CREATED
- EC2_LAUNCH_TEMPLATE_PUBLIC_IP_DISABLED
- EC2_MANAGEDINSTANCE_APPLICATIONS_BLACKLISTED
- EC2_MANAGEDINSTANCE_APPLICATIONS_REQUIRED
- EC2_MANAGEDINSTANCE_ASSOCIATION_COMPLIANCE_STATUS_CHECK

支援 AWS Config 受管規則關鍵字

- EC2_MANAGEDINSTANCE_INVENTORY_BLACKLISTED
- EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK
- EC2_MANAGEDINSTANCE_PLATFORM_CHECK
- EC2_NO_AMAZON_KEY_PAIR
- EC2_PARAVIRTUAL_INSTANCE_CHECK
- EC2_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EC2_SECURITY_GROUP_ATTACHED_TO_ENI
- EC2_SECURITY_GROUP_ATTACHED_TO_ENI_PERIODIC
- EC2_STOPPED_INSTANCE
- EC2_TOKEN_HOP_LIMIT_CHECK
- EC2_TRANSIT_GATEWAY_AUTO_VPC_ATTACH_DISABLED
- EC2_VOLUME_INUSE_CHECK
- ECR_PRIVATE_IMAGE_SCANNING_ENABLED
- ECR_PRIVATE_LIFECYCLE_POLICY_CONFIGURED
- ECR_PRIVATE_TAG_IMMUTABILITY_ENABLED
- ECS_ 已啟用 AWSVPC_NETWORKING (_)
- ECS_CONTAINER_INSIGHTS_ENABLED
- ECS_CONTAINERS_NONPRIVILEGED
- ECS_CONTAINERS_READONLY_ACCESS
- ECS_FARGATE_LATEST_PLATFORM_VERSION
- ECS_NO_ENVIRONMENT_SECRETS
- ECS_TASK_DEFINITION_LOG_CONFIGURATION
- ECS_TASK_DEFINITION_MEMORY_HARD_LIMIT
- ECS_TASK_DEFINITION_NONROOT_USER
- ECS_TASK_DEFINITION_PID_MODE_CHECK
- ECS_TASK_DEFINITION_USER_FOR_HOST_MODE_CHECK
- EFS_ACCESS_POINT_ENFORCE_ROOT_DIRECTORY
- EFS_ACCESS_POINT_ENFORCE_USER_IDENTITY
- EFS_ENCRYPTED_CHECK

支援 AWS Config 受管規則關鍵字

- EFS_IN_BACKUP_PLAN
- EFS_LAST_BACKUP_RECOVERY_POINT_CREATED
- EFS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EIP_ATTACHED
- EKS_CLUSTER_LOGGING_ENABLED
- EKS_CLUSTER_OLDEST_SUPPORTED_VERSION
- EKS_CLUSTER_SUPPORTED_VERSION
- EKS_ENDPOINT_NO_PUBLIC_ACCESS
- EKS_SECRETS_ENCRYPTED
- ELASTIC_BEANSTALK_LOGS_TO_CLOUDWATCH
- ELASTIC_BEANSTALK_MANAGED_UPDATES_ENABLED
- ELASTICACHE_AUTO_MINOR_VERSION_UPGRADE_CHECK
- ELASTICACHE_RBAC_AUTH_ENABLED
- ELASTICACHE_REDIS_CLUSTER_AUTOMATIC_BACKUP_CHECK
- ELASTICACHE_REPL_GRP_AUTO_FAILOVER_ENABLED
- ELASTICACHE_REPL_GRP_ENCRYPTED_AT_REST
- ELASTICACHE_REPL_GRP_ENCRYPTED_IN_TRANSIT
- ELASTICACHE_REPL_GRP_REDIS_AUTH_ENABLED
- ELASTICACHE_SUBNET_GROUP_CHECK
- ELASTICACHE_SUPPORTED_ENGINE_VERSION
- ELASTICSEARCH_ENCRYPTED_AT_REST
- ELASTICSEARCH_IN_VPC_ONLY
- ELASTICSEARCH_LOGS_TO_CLOUDWATCH
- ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK
- ELB_ACM_CERTIFICATE_REQUIRED
- ELB_CROSS_ZONE_LOAD_BALANCING_ENABLED
- ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK
- ELB_DELETION_PROTECTION_ENABLED
- ELB_LOGGING_ENABLED

支援 AWS Config 受管規則關鍵字

- ELB_PREDEFINED_SECURITY_POLICY_SSL_CHECK
- ELB_TLS_HTTPS_LISTENERS_ONLY
- ELBV2_ACM_CERTIFICATE_REQUIRED
- ELBV2_MULTIPLE_AZ
- EMR_KERBEROS_ENABLED
- EMR_MASTER_NO_PUBLIC_IP
- ENCRYPTED_VOLUMES
- FMS_SHIELD_RESOURCE_POLICY_CHECK
- FMS_WEBACL_RESOURCE_POLICY_CHECK
- FMS_WEBACL_RULEGROUP_ASSOCIATION_CHECK
- FSX_LAST_BACKUP_RECOVERY_POINT_CREATED
- FSX_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- GUARDDUTY_ENABLED_CENTRALIZED
- GUARDDUTY_NON_ARCHIVED_FINDINGS
- IAM_CUSTOMER_POLICY_BLOCKED_KMS_ACTIONS
- IAM_GROUP_HAS_USERS_CHECK
- IAM_INLINE_POLICY_BLOCKED_KMS_ACTIONS
- IAM_NO_INLINE_POLICY_CHECK
- IAM_PASSWORD_POLICY
- IAM_POLICY_BLACKLISTED_CHECK
- IAM_POLICY_IN_USE
- IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS
- IAM_POLICY_NO_STATEMENTS_WITH_FULL_ACCESS
- IAM_ROLE_MANAGED_POLICY_CHECK
- IAM_ROOT_ACCESS_KEY_CHECK
- IAM_USER_GROUP_MEMBERSHIP_CHECK
- IAM_USER_MFA_ENABLED
- IAM_USER_NO_POLICIES_CHECK
- IAM_USER_UNUSED_CREDENTIALS_CHECK

支援 AWS Config 受管規則關鍵字

- INCOMING_SSH_DISABLED
- INSTANCES_IN_VPC
- KINESIS_STREAM_ENCRYPTED
- INTERNET_GATEWAY_AUTHORIZED_VPC_ONLY
- KMS_CMK_NOT_SCHEDULED_FOR_DELETION
- LAMBDA_CONCURRENCY_CHECK
- LAMBDA_DLQ_CHECK
- LAMBDA_FUNCTION_PUBLIC_ACCESS_PROHIBITED
- LAMBDA_FUNCTION_SETTINGS_CHECK
- LAMBDA_INSIDE_VPC
- LAMBDA_VPC_MULTI_AZ_CHECK
- MACIE_STATUS_CHECK
- MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS
- MQ_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED
- MQ_CLOUDWATCH_AUDIT_LOGGING_ENABLED
- MQ_NO_PUBLIC_ACCESS
- MULTI_REGION_CLOUD_TRAIL_ENABLED
- NACL_NO_UNRESTRICTED_SSH_RDP
- NETFW_LOGGING_ENABLED
- NETFW_MULTI_AZ_ENABLED
- NETFW_POLICY_DEFAULT_ACTION_FRAGMENT_PACKETS
- NETFW_POLICY_DEFAULT_ACTION_FULL_PACKETS
- NETFW_POLICY_RULE_GROUP_ASSOCIATED
- NETFW_STATELESS_RULE_GROUP_NOT_EMPTY
- NLB_CROSS_ZONE_LOAD_BALANCING_ENABLED
- NO_UNRESTRICTED_ROUTE_TO_IGW
- OPENSEARCH_ACCESS_CONTROL_ENABLED
- OPENSEARCH_AUDIT_LOGGING_ENABLED
- OPENSEARCH_DATA_NODE_FAULT_TOLERANCE

支援 AWS Config 受管規則關鍵字

- OPENSEARCH_ENCRYPTED_AT_REST
- OPENSEARCH_HTTPS_REQUIRED
- OPENSEARCH_IN_VPC_ONLY
- OPENSEARCH_LOGS_TO_CLOUDWATCH
- OPENSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK
- RDS_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED
- RDS_CLUSTER_DEFAULT_ADMIN_CHECK
- RDS_CLUSTER_DELETION_PROTECTION_ENABLED
- RDS_CLUSTER_IAM_AUTHENTICATION_ENABLED
- RDS_CLUSTER_MULTI_AZ_ENABLED
- RDS_DB_SECURITY_GROUP_NOT_ALLOWED
- RDS_ENHANCED_MONITORING_ENABLED
- RDS_IN_BACKUP_PLAN
- RDS_INSTANCE_DEFAULT_ADMIN_CHECK
- RDS_INSTANCE_DELETION_PROTECTION_ENABLED
- RDS_INSTANCE_IAM_AUTHENTICATION_ENABLED
- RDS_INSTANCE_PUBLIC_ACCESS_CHECK
- RDS_LAST_BACKUP_RECOVERY_POINT_CREATED
- RDS_LOGGING_ENABLED
- RDS_MULTI_AZ_SUPPORT
- RDS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- RDS_SNAPSHOT_ENCRYPTED
- RDS_SNAPSHOTS_PUBLIC_PROHIBITED
- RDS_STORAGE_ENCRYPTED
- REDSHIFT_BACKUP_ENABLED
- REDSHIFT_REQUIRE_TLS_SSL
- REDSHIFT_CLUSTER_CONFIGURATION_CHECK
- REDSHIFT_CLUSTER_MAINTENANCESETTINGS_CHECK
- 識別符：REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK

支援 AWS Config 受管規則關鍵字

- REDSHIFT_AUDIT_LOGGING_ENABLED
- REDSHIFT_CLUSTER_KMS_ENABLED
- REDSHIFT_DEFAULT_ADMIN_CHECK
- REDSHIFT_DEFAULT_DB_NAME_CHECK
- REDSHIFT_ENHANCED_VPC_ROUTING_ENABLED
- REQUIRED_TAGS
- RESTRICTED_INCOMING_TRAFFIC
- ROOT_ACCOUNT_HARDWARE_MFA_ENABLED
- ROOT_ACCOUNT_MFA_ENABLED
- S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS_PERIODIC
- S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS
- S3_BUCKET_ACL_PROHIBITED
- 識別符：S3_BUCKET_BLACKLISTED_ACTIONS_PROHIBITED
- 識別碼： S3_BUCKET_DEFAULT_LOCK_ENABLED
- S3_BUCKET_LEVEL_PUBLIC_ACCESS_PROHIBITED
- S3_BUCKET_LOGGING_ENABLED
- S3_BUCKET_POLICY_GRANTEE_CHECK
- S3_BUCKET_POLICY_NOT_MORE_PERMISSIVE
- S3_BUCKET_PUBLIC_READ_PROHIBITED
- S3_BUCKET_PUBLIC_WRITE_PROHIBITED
- S3_BUCKET_REPLICATION_ENABLED
- S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED
- S3_BUCKET_SSL_REQUESTS_ONLY
- S3_BUCKET_VERSIONING_ENABLED
- S3_DEFAULT_ENCRYPTION_KMS
- S3_EVENT_NOTIFICATIONS_ENABLED
- S3_LAST_BACKUP_RECOVERY_POINT_CREATED
- S3_LIFECYCLE_POLICY_CHECK
- S3_RESOURCES_PROTECTED_BY_BACKUP_PLAN

支援 AWS Config 受管規則關鍵字

- S3_VERSION_LIFECYCLE_POLICY_CHECK
- SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED
- SAGEMAKER_NOTEBOOK_INSTANCE_INSIDE_VPC
- SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED
- SAGEMAKER_NOTEBOOK_INSTANCE_ROOT_ACCESS_CHECK
- SAGEMAKER_NOTEBOOK_NO_DIRECT_INTERNET_ACCESS
- SECRETSMANAGER_ROTATION_ENABLED_CHECK
- SECRETSMANAGER_SCHEDULED_ROTATION_SUCCESS_CHECK
- SECRETSMANAGER_SECRET_PERIODIC_ROTATION
- SECRETSMANAGER_SECRET_UNUSED
- SECRETSMANAGER_USING_CMK
- SECURITY_ACCOUNT_INFORMATION_PROVIDED
- SECURITYHUB_ENABLED
- SERVICE_VPC_ENDPOINT_ENABLED
- SES_MALWARE_SCANNING_ENABLED
- SHIELD_ADVANCED_ENABLED_AUTORENEW
- SHIELD_DRT_ACCESS
- SNS_ENCRYPTED_KMS
- SNS_TOPIC_MESSAGE_DELIVERY_NOTIFICATION_ENABLED
- SSM_DOCUMENT_NOT_PUBLIC
- STEP_FUNCTIONS_STATE_MACHINE_LOGGING_ENABLED
- STORAGEGATEWAY_LAST_BACKUP_RECOVERY_POINT_CREATED
- STORAGEGATEWAY_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED
- VIRTUALMACHINE_LAST_BACKUP_RECOVERY_POINT_CREATED
- VIRTUALMACHINE_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- VPC_DEFAULT_SECURITY_GROUP_CLOSED
- VPC_FLOW_LOGS_ENABLED
- VPC_NETWORK_ACL_UNUSED_CHECK

支援 AWS Config 受管規則關鍵字

- VPC_PEERING_DNS_RESOLUTION_CHECK
- 識別符：VPC_SG_OPEN_ONLY_TO_AUTHORIZED_PORTS
- VPC_VPN_2_TUNNELS_UP
- WAF_CLASSIC_LOGGING_ENABLED
- WAF_GLOBAL_RULEGROUP_NOT_EMPTY
- WAF_GLOBAL_RULE_NOT_EMPTY
- WAF_GLOBAL_WEBACL_NOT_EMPTY
- WAF_REGIONAL_RULEGROUP_NOT_EMPTY
- WAF_REGIONAL_RULE_NOT_EMPTY
- WAF_REGIONAL_WEBACL_NOT_EMPTY
- WAFV2_LOGGING_ENABLED
- WAFV2_RULEGROUP_NOT_EMPTY
- WAFV2_WEBACL_NOT_EMPTY

搭配 Audit Manager 使用 AWS Config 自訂規則

您現在可以使用 AWS Config 自訂規則做為稽核報告的資料來源。當控制項具有對應至 AWS Config 規則的資料來源時，Audit Manager 會新增 AWS Config 規則所建立的評估。

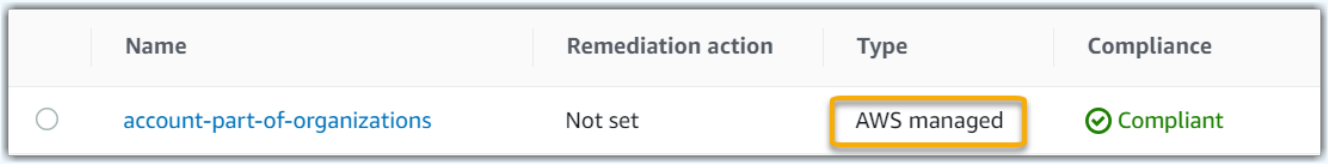
您可以使用的自訂規則取決於 AWS 帳戶 您登入 Audit Manager 時使用的規則。如果您可以在中存取自訂規則 AWS Config，則可以在「Audit Manager」中將其用作資料來源對映。

- 對於個人 AWS 帳戶 — 您可以使用您在帳戶中創建的任何自定義規則。
- 對於屬於組織的帳戶 — 您可以使用任何成員層級的自訂規則。或者，您可以在 AWS Config中使用任何可用的組織層級自訂規則。

如需如何建立使用自訂規則做為資料來源的控制項的指示，請參閱從頭開始建立新控制項和自訂現有控制項。

> **Tip**
>
> 請記住，受管規則不會顯示在 Audit Manager 自訂規則的下拉式清單中。

如果要驗證規則是受管 AWS Config 規則還是自訂規則，可以使用AWS Config 主控台執行此操作。從左側導覽功能表中選擇規則，然後在表格中尋找規則。如果是受管規則，類型欄會顯示AWS 受管規則。



若要將受管規則映射為資料來源，您可以在受管規則的下拉式清單中，在 Audit Manager 中尋找受管規則識別碼關鍵字。如需詳細資訊，請參閱本指南的疑難排解一節。

將自訂規則映射為控制項的資料來源之後，您可以將該控制項與 Audit Manager 中的自訂架構相關聯。如需如何建立使用自訂控制項的自訂架構的說明，請參閱從頭開始建立新架構和自訂現有架構。如需如何將控制項新增至現有自訂架構的指示，請參閱編輯現有架構。

如需有關在中建立自訂規則的資訊 AWS Config，請參閱《AWS Config 開發人員指南》 AWS Config 中的〈開發自訂規則〉。

與 Audit Manager 的 AWS Config 整合疑難

若要尋找常見問題和問題的解答，請參閱本指南疑難排解一節中的AWS Config 整合。

AWS Security Hub 支援的控制項 AWS Audit Manager

Audit Manager 可讓您直接從資訊安全中心報告合規檢查的結果。若要這麼做，請在 Audit Manager 中設定自訂控制項時，指定一或多個 Security Hub 控制項做為資料來源映射項目。

Note

- Audit Manager 不會從 Security Hub 心建立的服務連結 AWS Config 規則收集證據。如需詳細資訊，請參閱本指南的疑難排解一節。
- 2022 年 11 月 9 日，Security Hub 推出了與網際網路安全中心 (CIS) AWS 基準指標 1.4.0 版要求相符的自動安全檢查，第 1 級和第 2 級 (CIS v1.4.0)。在 Security Hub 中，除了 CIS v1.2.0 標準外，還支援 CIS v 1.4.0 標準。

主題

- 搭配 Audit Manager 使用 Security Hub 控制項

- 支援的 Security Hub 控制項

搭配 Audit Manager 使用 Security Hub 控制項

> **Tip**
>
> 建議您在 Security Hub 中開啟 合併控制項調查結果 設定 (如果尚未開啟)。如果您在 2003 年 2 月 23 日當天或之後啟用資 Security Hub，此設定預設為開啟。

啟用合併調查結果時，Security Hub 會針對每個安全檢查產生單一調查結果 (即使相同檢查適用於多個標準)。每個 Security Hub 調查結果都會做為 Audit Manager 中一項獨立資源評估來收集。因此，合併的調查結果會導致 Audit Manager 針對 Security Hub 調查結果執行的獨立資源評估總計減少。因此，使用合併的調查結果可以降低 Audit Manager 的使用成本，而不會犧牲證據品質和可用性。如需定價的詳細資訊，請參閱 AWS Audit Manager 定價。

開啟或關閉合併調查結果時的證據範例

下列範例顯示，Audit Manager 如何根據您的 Security Hub 設定收集和提供證據的比較。

When consolidated findings is turned on

假設您已經在安全中心啟用了以下三個安全標準： AWS FSBP，PCI DSS 和獨聯體基準測試 v1.2.0。

- 這三個標準都使用相同的控制項 (IAM.4) 與相同的基礎 AWS Config 規則 (iam-root-access-key-check)。
- 由於已開啟合併的控制項調查結果設定，因此 Security Hub 會針對此控制項產生一個調查結果。
- Security Hub 會將合併的調查結果傳送給 Audit Manager 以進行此控制項。
- 合併的調查結果會被視為 Audit Manager 中的一項獨立資源評估。因此，您的評估中會新增一份證據。

此處提供範例說明該證據的範例：

```
{
    "SchemaVersion": "2018-10-08",
    "Id": "arn:aws:securityhub:us-west-2:111122223333:security-control/IAM.4/
finding/09876543-p0o9-i8u7-y6t5-098765432109",
```

```
    "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/securityhub",
    "ProductName": "Security Hub",
    "CompanyName": "AWS",
    "Region": "us-west-2",
    "GeneratorId": "security-control/IAM.4",
    "AwsAccountId": "111122223333",
    "Types": [
        "Software and Configuration Checks/Industry and Regulatory Standards"
    ],
    "FirstObservedAt": "2023-10-25T11:32:24.861Z",
    "LastObservedAt": "2023-11-02T11:59:19.546Z",
    "CreatedAt": "2023-10-25T11:32:24.861Z",
    "UpdatedAt": "2023-11-02T11:59:15.127Z",
    "Severity": {
        "Label": "INFORMATIONAL",
        "Normalized": 0,
        "Original": "INFORMATIONAL"
    },
    "Title": "IAM root user access key should not exist",
    "Description": "This AWS control checks whether the root user access key is
 available.",
    "Remediation": {
        "Recommendation": {
            "Text": "For information on how to correct this issue, consult the AWS
 Security Hub controls documentation.",
            "Url": "https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
        }
    },
    "ProductFields": {
        "RelatedAWSResources:0/name": "securityhub-iam-root-access-key-
check-000270f5",
        "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
        "aws/securityhub/ProductName": "Security Hub",
        "aws/securityhub/CompanyName": "AWS",
        "Resources:0/Id": "arn:aws:iam::111122223333:root",
        "aws/securityhub/FindingId": "arn:aws:securityhub:us-west-2::product/aws/
securityhub/arn:aws:securityhub:us-west-2:111122223333:security-control/IAM.4/
finding/09876543-p0o9-i8u7-y6t5-098765432109"
    },
    "Resources": [{
        "Type": "AwsAccount",
        "Id": "AWS::::Account:111122223333",
        "Partition": "aws",
```

```
        "Region": "us-west-2"
    }],
    "Compliance": {
        "Status": "PASSED",
        "RelatedRequirements": [
            "CIS AWS Foundations Benchmark v1.2.0/1.12"
        ],
        "SecurityControlId": "IAM.4",
        "AssociatedStandards": [{
                "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"
            },
            {
                "StandardsId": "standards/aws-foundational-security-best-practices/
v/1.0.0"
            }
        ]
    },
    "WorkflowState": "NEW",
    "Workflow": {
        "Status": "RESOLVED"
    },
    "RecordState": "ACTIVE",
    "FindingProviderFields": {
        "Severity": {
            "Label": "INFORMATIONAL",
            "Original": "INFORMATIONAL"
        },
        "Types": [
            "Software and Configuration Checks/Industry and Regulatory Standards"
        ]
    },
    "ProcessedAt": "2023-11-02T11:59:20.980Z"
}
```

When consolidated findings is turned off

假設您已經在安全中心啟用了以下三個安全標準： AWS FSBP，PCI DSS 和獨聯體基準測試 v1.2.0。

- 這三個標準都使用相同的控制項 (IAM.4) 與相同的基礎 AWS Config 規則 (iam-root-access-key-check)。
- 由於已關閉合併的調查結果設定，Security Hub 會針對每個已啟用的標準 (在本例中為三個調查結果)，針對每個安全檢查產生個別的調查結果。

- Security Hub 會針對此控制項，傳送三個獨立的標準特定調查結果給 Audit Manager。
- 這三個調查結果計數為 Audit Manager 中的三個獨特資源評估 因此，三項獨立的證據新增至您的評估中。

此處提供範例說明該證據的範例。請注意，在此範例中，下列三個承載中的每一項都具有相同的安全控制 ID (*SecurityControlId":"IAM.4"*)。因此，當下列調查結果從 Security Hub 傳入時，在 Audit Manager (IAM.4) 中收集此證據的評估控制會收到三個不同的證據。

IAM.4 的證據 (FSBP)


```
{
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type":"Security Hub Findings - Imported",
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2023-10-27T18:55:59Z",
  "region":"us-west-2",
  "resources":[
     "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/b5e68d5d-43c3-46c8-902d-51cb0d4da568"
  ],
  "detail":{
     "findings":[
        {
           "SchemaVersion":"2018-10-08",
           "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/aws-
foundational-security-best-practices/v/1.0.0/IAM.4/finding/8e2e05a2-4d50-4c2e-
a78f-3cbe9402d17d",
           "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
           "ProductName":"Security Hub",
           "CompanyName":"AWS",
           "Region":"us-west-2",
           "GeneratorId":"aws-foundational-security-best-practices/v/1.0.0/IAM.4",
           "AwsAccountId":"111122223333",
           "Types":[
              "Software and Configuration Checks/Industry and Regulatory Standards/
AWS-Foundational-Security-Best-Practices"
           ],
           "FirstObservedAt":"2020-10-05T19:18:47.848Z",
           "LastObservedAt":"2023-11-01T14:12:04.106Z",
```

```
            "CreatedAt":"2020-10-05T19:18:47.848Z",
            "UpdatedAt":"2023-11-01T14:11:53.720Z",
            "Severity":{
               "Product":0,
               "Label":"INFORMATIONAL",
               "Normalized":0,
               "Original":"INFORMATIONAL"
            },
            "Title":"IAM.4 IAM root user access key should not exist",
            "Description":"This AWS control checks whether the root user access key
 is available.",
            "Remediation":{
               "Recommendation":{
                  "Text":"For information on how to correct this issue, consult the
 AWS Security Hub controls documentation.",
                  "Url":"https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
               }
            },
            "ProductFields":{
               "StandardsArn":"arn:aws:securityhub:::standards/aws-foundational-
security-best-practices/v/1.0.0",
               "StandardsSubscriptionArn":"arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0",
               "ControlId":"IAM.4",
               "RecommendationUrl":"https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
               "RelatedAWSResources:0/name":"securityhub-iam-root-access-key-
check-67cbb1c4",
               "RelatedAWSResources:0/type":"AWS::Config::ConfigRule",
               "StandardsControlArn":"arn:aws:securityhub:us-
west-2:111122223333:control/aws-foundational-security-best-practices/v/1.0.0/IAM.4",
               "aws/securityhub/ProductName":"Security Hub",
               "aws/securityhub/CompanyName":"AWS",
               "Resources:0/Id":"arn:aws:iam::111122223333:root",
               "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/aws-
foundational-security-best-practices/v/1.0.0/IAM.4/finding/8e2e05a2-4d50-4c2e-
a78f-3cbe9402d17d"
            },
            "Resources":[
               {
                  "Type":"AwsAccount",
                  "Id":"AWS::::Account:111122223333",
```

```
                "Partition":"aws",
                "Region":"us-west-2"
             }
          ],
          "Compliance":{
             "Status":"PASSED",
             "SecurityControlId":"IAM.4",
             "AssociatedStandards":[
                {
                   "StandardsId":"standards/aws-foundational-security-best-
practices/v/1.0.0"
                }
             ]
          },
          "WorkflowState":"NEW",
          "Workflow":{
             "Status":"RESOLVED"
          },
          "RecordState":"ACTIVE",
          "FindingProviderFields":{
             "Severity":{
                "Label":"INFORMATIONAL",
                "Original":"INFORMATIONAL"
             },
             "Types":[
                "Software and Configuration Checks/Industry and Regulatory
 Standards/AWS-Foundational-Security-Best-Practices"
             ]
          },
          "ProcessedAt":"2023-11-01T14:12:07.395Z"
       }
    ]
  }
}
```

IAM.4 的證據 (CIS 1.2)

```
{
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type":"Security Hub Findings - Imported",
```

```
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2023-10-27T18:55:59Z",
  "region":"us-west-2",
  "resources":[
     "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
  ],
  "detail":{
     "findings":[
        {
           "SchemaVersion":"2018-10-08",
           "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/cis-aws-
foundations-benchmark/v/1.2.0/1.12/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23",
           "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
           "ProductName":"Security Hub",
           "CompanyName":"AWS",
           "Region":"us-west-2",
           "GeneratorId":"arn:aws:securityhub:::ruleset/cis-aws-foundations-
benchmark/v/1.2.0/rule/1.12",
           "AwsAccountId":"111122223333",
           "Types":[
              "Software and Configuration Checks/Industry and Regulatory Standards/
CIS AWS Foundations Benchmark"
           ],
           "FirstObservedAt":"2020-10-05T19:18:47.775Z",
           "LastObservedAt":"2023-11-01T14:12:07.989Z",
           "CreatedAt":"2020-10-05T19:18:47.775Z",
           "UpdatedAt":"2023-11-01T14:11:53.720Z",
           "Severity":{
              "Product":0,
              "Label":"INFORMATIONAL",
              "Normalized":0,
              "Original":"INFORMATIONAL"
           },
           "Title":"1.12 Ensure no root user access key exists",
           "Description":"The root user is the most privileged user in an AWS
 account. AWS Access Keys provide programmatic access to a given AWS account. It is
 recommended that all access keys associated with the root user be removed.",
           "Remediation":{
              "Recommendation":{
                 "Text":"For information on how to correct this issue, consult the
 AWS Security Hub controls documentation.",
```

```
                "Url":"https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
             }
          },
          "ProductFields":{
             "StandardsGuideArn":"arn:aws:securityhub:::ruleset/cis-aws-
foundations-benchmark/v/1.2.0",
             "StandardsGuideSubscriptionArn":"arn:aws:securityhub:us-
west-2:111122223333:subscription/cis-aws-foundations-benchmark/v/1.2.0",
             "RuleId":"1.12",
             "RecommendationUrl":"https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
             "RelatedAWSResources:0/name":"securityhub-iam-root-access-key-
check-67cbb1c4",
             "RelatedAWSResources:0/type":"AWS::Config::ConfigRule",
             "StandardsControlArn":"arn:aws:securityhub:us-
west-2:111122223333:control/cis-aws-foundations-benchmark/v/1.2.0/1.12",
             "aws/securityhub/ProductName":"Security Hub",
             "aws/securityhub/CompanyName":"AWS",
             "Resources:0/Id":"arn:aws:iam::111122223333:root",
             "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/cis-aws-
foundations-benchmark/v/1.2.0/1.12/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
          },
          "Resources":[
             {
                "Type":"AwsAccount",
                "Id":"AWS::::Account:111122223333",
                "Partition":"aws",
                "Region":"us-west-2"
             }
          ],
          "Compliance":{
             "Status":"PASSED",
             "SecurityControlId":"IAM.4",
             "AssociatedStandards":[
                {
                   "StandardsId":"ruleset/cis-aws-foundations-benchmark/v/1.2.0"
                }
             ]
          },
          "WorkflowState":"NEW",
          "Workflow":{
             "Status":"RESOLVED"
```

```
            },
            "RecordState":"ACTIVE",
            "FindingProviderFields":{
               "Severity":{
                  "Label":"INFORMATIONAL",
                  "Original":"INFORMATIONAL"
               },
               "Types":[
                  "Software and Configuration Checks/Industry and Regulatory
 Standards/CIS AWS Foundations Benchmark"
               ]
            },
            "ProcessedAt":"2023-11-01T14:12:13.436Z"
         }
      ]
   }
}
```

PCI DSS 的證據

```
{
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type":"Security Hub Findings - Imported",
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2023-10-27T18:55:59Z",
  "region":"us-west-2",
  "resources":[
     "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
  ],
  "detail":{
     "findings":[
        {
           "SchemaVersion":"2018-10-08",
           "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/pci-dss/
v/3.2.1/PCI.IAM.1/finding/3c75f651-6e2e-44f4-8e22-297d5c2d0c8b",
           "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
           "ProductName":"Security Hub",
           "CompanyName":"AWS",
           "Region":"us-west-2",
```

```
            "GeneratorId":"pci-dss/v/3.2.1/PCI.IAM.1",
            "AwsAccountId":"111122223333",
            "Types":[
               "Software and Configuration Checks/Industry and Regulatory Standards/
PCI-DSS"
            ],
            "FirstObservedAt":"2020-10-05T19:18:47.788Z",
            "LastObservedAt":"2023-11-01T14:12:02.413Z",
            "CreatedAt":"2020-10-05T19:18:47.788Z",
            "UpdatedAt":"2023-11-01T14:11:53.720Z",
            "Severity":{
               "Product":0,
               "Label":"INFORMATIONAL",
               "Normalized":0,
               "Original":"INFORMATIONAL"
            },
            "Title":"PCI.IAM.1 IAM root user access key should not exist",
            "Description":"This AWS control checks whether the root user access key
 is available.",
            "Remediation":{
               "Recommendation":{
                  "Text":"For information on how to correct this issue, consult the
 AWS Security Hub controls documentation.",
                  "Url":"https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
               }
            },
            "ProductFields":{
               "StandardsArn":"arn:aws:securityhub:::standards/pci-dss/v/3.2.1",
               "StandardsSubscriptionArn":"arn:aws:securityhub:us-
west-2:111122223333:subscription/pci-dss/v/3.2.1",
               "ControlId":"PCI.IAM.1",
               "RecommendationUrl":"https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
               "RelatedAWSResources:0/name":"securityhub-iam-root-access-key-
check-67cbb1c4",
               "RelatedAWSResources:0/type":"AWS::Config::ConfigRule",
               "StandardsControlArn":"arn:aws:securityhub:us-
west-2:111122223333:control/pci-dss/v/3.2.1/PCI.IAM.1",
               "aws/securityhub/ProductName":"Security Hub",
               "aws/securityhub/CompanyName":"AWS",
               "Resources:0/Id":"arn:aws:iam::111122223333:root",
```

```
            "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/pci-dss/
v/3.2.1/PCI.IAM.1/finding/3c75f651-6e2e-44f4-8e22-297d5c2d0c8b"
         },
         "Resources":[
            {
               "Type":"AwsAccount",
               "Id":"AWS::::Account:111122223333",
               "Partition":"aws",
               "Region":"us-west-2"
            }
         ],
         "Compliance":{
            "Status":"PASSED",
            "RelatedRequirements":[
               "PCI DSS 2.1",
               "PCI DSS 2.2",
               "PCI DSS 7.2.1"
            ],
            "SecurityControlId":"IAM.4",
            "AssociatedStandards":[
               {
                  "StandardsId":"standards/pci-dss/v/3.2.1"
               }
            ]
         },
         "WorkflowState":"NEW",
         "Workflow":{
            "Status":"RESOLVED"
         },
         "RecordState":"ACTIVE",
         "FindingProviderFields":{
            "Severity":{
               "Label":"INFORMATIONAL",
               "Original":"INFORMATIONAL"
            },
            "Types":[
               "Software and Configuration Checks/Industry and Regulatory
 Standards/PCI-DSS"
            ]
         },
         "ProcessedAt":"2023-11-01T14:12:05.950Z"
      }
   ]
```

```
  }
}
```

支援的 Security Hub 控制項

Audit Manager 目前支援下列 Security Hub 控制項。當您為自訂控制項設定資料來源時，您可以使用下列任何一個特定於標準的控制項 ID 關鍵字。

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 （Security Hub 中對應的安全控制 ID）
CIS v1.2.0	1.2	IAM.5
CIS v1.2.0	1.3	IAM.8
CIS v1.2.0	1.4	IAM.3
CIS v1.2.0	1.5	IAM.11
CIS v1.2.0	1.6	IAM.12
CIS v1.2.0	1.7	IAM.13
CIS v1.2.0	1.8	IAM.14
CIS v1.2.0	1.9	IAM.15
CIS v1.2.0	1.10	IAM.16
CIS v1.2.0	1.11	IAM.17
CIS v1.2.0	1.12	IAM.4
CIS v1.2.0	1.13	IAM.9
CIS v1.2.0	1.14	IAM.6

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 （Security Hub 中對應的安全控制 ID）
CIS v1.2.0	1.16	IAM.2
CIS v1.2.0	1.20	IAM.18
CIS v1.2.0	1.22	IAM.1
CIS v1.2.0	2.1	CloudTrail.1
CIS v1.2.0	2.2	CloudTrail.4
CIS v1.2.0	2.3	CloudTrail.6
CIS v1.2.0	2.4	CloudTrail.5
CIS v1.2.0	2.5	Config.1
CIS v1.2.0	2.6	CloudTrail.7
CIS v1.2.0	2.7	CloudTrail.2
CIS v1.2.0	2.8	KMS.4
CIS v1.2.0	2.9	EC2.6
CIS v1.2.0	3.1	CloudWatch.2
CIS v1.2.0	3.2	CloudWatch.3
CIS v1.2.0	3.3	CloudWatch.1
CIS v1.2.0	3.4	CloudWatch.4
CIS v1.2.0	3.5	CloudWatch.5
CIS v1.2.0	3.6	CloudWatch.6

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 （Security Hub 中對應的安全控制 ID）
CIS v1.2.0	3.7	CloudWatch.7
CIS v1.2.0	3.8	CloudWatch.8
CIS v1.2.0	3.9	CloudWatch.9
CIS v1.2.0	3.10	CloudWatch.10
CIS v1.2.0	3.11	CloudWatch.11
CIS v1.2.0	3.12	CloudWatch.12
CIS v1.2.0	3.13	CloudWatch.13
CIS v1.2.0	3.14	CloudWatch.14
CIS v1.2.0	4.1	EC2.13
CIS v1.2.0	4.2	EC2.14
CIS v1.2.0	4.3	EC2.2
PCI DSS	PCI。AutoScaling.1	AutoScaling.1
PCI DSS	PCI。CloudTrail.1	CloudTrail.1
PCI DSS	PCI。CloudTrail.2	CloudTrail.2
PCI DSS	PCI。CloudTrail.3	CloudTrail.3

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 （Security Hub 中對應的安全控制 ID）
PCI DSS	PCI。 CloudTrail.4	CloudTrail.4
PCI DSS	PCI。 CodeBuild.1	CodeBuild.1
PCI DSS	PCI。 CodeBuild.2	CodeBuild.2
PCI DSS	PCI.Config.1	Config.1
PCI DSS	PCI.CW.1	CloudWatch.1
PCI DSS	PCI.DMS.1	DMS.1
PCI DSS	PCI.EC2.1	EC2.1
PCI DSS	PCI.EC2.2	EC2.2
PCI DSS	PCI.EC2.3	EC2.3
PCI DSS	PCI.EC2.4	EC2.12
PCI DSS	PCI.EC2.5	EC2.13
PCI DSS	PCI.EC2.6	EC2.6
PCI DSS	PCI.ELBv2.1	ELB.1
PCI DSS	PCI.ES.1	ES.1
PCI DSS	PCI.ES.2	ES.2

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 （Security Hub 中對應的安全控制 ID）
PCI DSS	PCI。GuardDuty.1	GuardDuty.1
PCI DSS	PCI.IAM.1	IAM.1
PCI DSS	PCI.IAM.2	IAM.2
PCI DSS	PCI.IAM.3	IAM.3
PCI DSS	PCI.IAM.4	IAM.4
PCI DSS	PCI.IAM.5	IAM.9
PCI DSS	PCI.IAM.6	IAM.6
PCI DSS	PCI.IAM.7	PCI.IAM.7
PCI DSS	PCI.IAM.8	PCI.IAM8.
PCI DSS	PCI.KMS.1	PCI.KMS.4
PCI DSS	PCI.Lambda.1	Lambda.1
PCI DSS	PCI.Lambda.2	Lambda.3
PCI DSS	PCI.Opensearch.1	Opensearch.1
PCI DSS	PCI.Opensearch.2	Opensearch.2
PCI DSS	PCI.RDS.1	RDS.1
PCI DSS	PCI.RDS.2	RDS.2

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 （Security Hub 中對應的安全控制 ID）
PCI DSS	PCI.Redshift.1	Redshift.1
PCI DSS	PCI.S3.1	S3.1
PCI DSS	PCI.S3.2	S3.2
PCI DSS	PCI.S3.3	S3.3
PCI DSS	PCI.S3.4	S3.4
PCI DSS	PCI.S3.5	S3.5
PCI DSS	PCI.S3.6	S3.1
PCI DSS	PCI。SageMaker.1	SageMaker.1
PCI DSS	PCI.SSM.1	SSM.1
PCI DSS	PCI.SSM.2	SSM.2
PCI DSS	PCI.SSM.3	SSM.3
AWS 基礎安全性最佳做法	Account.1	Account.1
AWS 基礎安全性最佳做法	帳戶 .2	帳戶 .2
AWS 基礎安全性最佳做法	ACM.1	ACM.1
AWS 基礎安全性最佳做法	ACM.2	ACM.2
AWS 基礎安全性最佳做法	APIGateway.1	APIGateway.1
AWS 基礎安全性最佳做法	APIGateway.2	APIGateway.2

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 （Security Hub 中對應的安全控制 ID）
AWS 基礎安全性最佳做法	APIGateway.3	APIGateway.3
AWS 基礎安全性最佳做法	APIGateway.4	APIGateway.4
AWS 基礎安全性最佳做法	APIGateway.5	APIGateway.5
AWS 基礎安全性最佳做法	APIGateway.8	APIGateway.8
AWS 基礎安全性最佳做法	APIGateway.9	APIGateway.9
AWS 基礎安全性最佳做法	AppSync.2	AppSync.2
AWS 基礎安全性最佳做法	AppSync.5	AppSync.5
AWS 基礎安全性最佳做法	雅典娜 .1	雅典娜 .1
AWS 基礎安全性最佳做法	AutoScaling.1	AutoScaling.1
AWS 基礎安全性最佳做法	AutoScaling.2	AutoScaling.2
AWS 基礎安全性最佳做法	AutoScaling.3	AutoScaling.3
AWS 基礎安全性最佳做法	AutoScaling.4	AutoScaling.4
AWS 基礎安全性最佳做法	Autoscaling.5	Autoscaling.5
AWS 基礎安全性最佳做法	AutoScaling.6	AutoScaling.6
AWS 基礎安全性最佳做法	AutoScaling.9	AutoScaling.9
AWS 基礎安全性最佳做法	Backup。1	Backup
AWS 基礎安全性最佳做法	CloudFormation.1	CloudFormation.1

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 （Security Hub 中對應的安全控制 ID）
AWS 基礎安全性最佳做法	CloudFront.1	CloudFront.1
AWS 基礎安全性最佳做法	CloudFront.2	CloudFront.2
AWS 基礎安全性最佳做法	CloudFront.3	CloudFront.3
AWS 基礎安全性最佳做法	CloudFront.4	CloudFront.4
AWS 基礎安全性最佳做法	CloudFront.5	CloudFront.5
AWS 基礎安全性最佳做法	CloudFront.6	CloudFront.6
AWS 基礎安全性最佳做法	CloudFront.7	CloudFront.7
AWS 基礎安全性最佳做法	CloudFront.8	CloudFront.8
AWS 基礎安全性最佳做法	CloudFront.9	CloudFront.9
AWS 基礎安全性最佳做法	CloudFront.10	CloudFront.10
AWS 基礎安全性最佳做法	CloudFront.12	CloudFront.12
AWS 基礎安全性最佳做法	CloudFront.13	CloudFront.13
AWS 基礎安全性最佳做法	CloudTrail.1	CloudTrail.1
AWS 基礎安全性最佳做法	CloudTrail.2	CloudTrail.2
AWS 基礎安全性最佳做法	CloudTrail.3	CloudTrail.3
AWS 基礎安全性最佳做法	CloudTrail.4	CloudTrail.4
AWS 基礎安全性最佳做法	CloudTrail.5	CloudTrail.5
AWS 基礎安全性最佳做法	CloudTrail.6	CloudTrail.6

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 （Security Hub 中對應的安全控制 ID）
AWS 基礎安全性最佳做法	CloudTrail.7	CloudTrail.7
AWS 基礎安全性最佳做法	CloudWatch.1	CloudWatch.1
AWS 基礎安全性最佳做法	CloudWatch.2	CloudWatch.2
AWS 基礎安全性最佳做法	CloudWatch.3	CloudWatch.3
AWS 基礎安全性最佳做法	CloudWatch.4	CloudWatch.4
AWS 基礎安全性最佳做法	CloudWatch.5	CloudWatch.5
AWS 基礎安全性最佳做法	CloudWatch.6	CloudWatch.6
AWS 基礎安全性最佳做法	CloudWatch.7	CloudWatch.7
AWS 基礎安全性最佳做法	CloudWatch.8	CloudWatch.8
AWS 基礎安全性最佳做法	CloudWatch.9	CloudWatch.9
AWS 基礎安全性最佳做法	CloudWatch.10	CloudWatch.10
AWS 基礎安全性最佳做法	CloudWatch.11	CloudWatch.11
AWS 基礎安全性最佳做法	CloudWatch.12	CloudWatch.12
AWS 基礎安全性最佳做法	CloudWatch.13	CloudWatch.13
AWS 基礎安全性最佳做法	CloudWatch.14	CloudWatch.14
AWS 基礎安全性最佳做法	CloudWatch.15	CloudWatch.15
AWS 基礎安全性最佳做法	CloudWatch.16	CloudWatch.16
AWS 基礎安全性最佳做法	CloudWatch.17	CloudWatch.17

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 （Security Hub 中對應的安全控制 ID）
AWS 基礎安全性最佳做法	CodeBuild.1	CodeBuild.1
AWS 基礎安全性最佳做法	CodeBuild.2	CodeBuild.2
AWS 基礎安全性最佳做法	CodeBuild.3	CodeBuild.3
AWS 基礎安全性最佳做法	CodeBuild.4	CodeBuild.4
AWS 基礎安全性最佳做法	CodeBuild.5	CodeBuild.5
AWS 基礎安全性最佳做法	Config.1	Config.1
AWS 基礎安全性最佳做法	DMS.1	DMS.1
AWS 基礎安全性最佳做法	公升 .6	公司 .6
AWS 基礎安全性最佳做法	毫升 .7	公司 .7
AWS 基礎安全性最佳做法	公升 .8	公司 .8
AWS 基礎安全性最佳做法	數位 .9	公司 .9
AWS 基礎安全性最佳做法	DocumentDB	DocumentDB
AWS 基礎安全性最佳做法	DocumentDB	DocumentDB
AWS 基礎安全性最佳做法	DocumentDB	DocumentDB
AWS 基礎安全性最佳做法	DocumentDB 4	DocumentDB 4
AWS 基礎安全性最佳做法	DocumentDB 5	DocumentDB
AWS 基礎安全性最佳做法	DynamoDB.1	DynamoDB.1
AWS 基礎安全性最佳做法	DynamoDB.2	DynamoDB.2

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 （Security Hub 中對應的安全控制 ID）
AWS 基礎安全性最佳做法	DynamoDB.3	DynamoDB.3
AWS 基礎安全性最佳做法	DynamoB.4	DynamoB.4
AWS 基礎安全性最佳做法	DynamoB.6	DynamoB.6
AWS 基礎安全性最佳做法	EC2.1	EC2.1
AWS 基礎安全性最佳做法	EC2.2	EC2.2
AWS 基礎安全性最佳做法	EC2.3	EC2.3
AWS 基礎安全性最佳做法	EC2.4	EC2.4
AWS 基礎安全性最佳做法	EC2.6	EC2.6
AWS 基礎安全性最佳做法	EC2.7	EC2.7
AWS 基礎安全性最佳做法	EC2.8	EC2.8
AWS 基礎安全性最佳做法	EC2.9	EC2.9
AWS 基礎安全性最佳做法	EC2.10	EC2.10
AWS 基礎安全性最佳做法	EC2.12	EC2.12
AWS 基礎安全性最佳做法	EC2.13	EC2.13
AWS 基礎安全性最佳做法	EC2.14	EC2.14
AWS 基礎安全性最佳做法	EC2.15	EC2.15
AWS 基礎安全性最佳做法	EC2.16	EC2.16
AWS 基礎安全性最佳做法	EC2.17	EC2.17

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 （Security Hub 中對應的安全控制 ID）
AWS 基礎安全性最佳做法	EC2.18	EC2.18
AWS 基礎安全性最佳做法	EC2.19	EC2.19
AWS 基礎安全性最佳做法	EC2.20	EC2.20
AWS 基礎安全性最佳做法	EC2.21	EC2.21
AWS 基礎安全性最佳做法	EC2.22	EC2.22
AWS 基礎安全性最佳做法	EC2.23	EC2.23
AWS 基礎安全性最佳做法	EC2.24	EC2.24
AWS 基礎安全性最佳做法	EC2.25	EC2.25
AWS 基礎安全性最佳做法	EC2.28	EC2.28
AWS 基礎安全性最佳做法	EC2.51	EC2.51
AWS 基礎安全性最佳做法	ECR.1	ECR.1
AWS 基礎安全性最佳做法	ECR.2	ECR.2
AWS 基礎安全性最佳做法	ECR.3	ECR.3
AWS 基礎安全性最佳做法	ECS.1	ECS.1
AWS 基礎安全性最佳做法	ECS.2	ECS.2
AWS 基礎安全性最佳做法	ECS.3	ECS.3
AWS 基礎安全性最佳做法	ECS.4	ECS.4
AWS 基礎安全性最佳做法	ECS.5	ECS.5

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 （Security Hub 中對應的安全控制 ID）
AWS 基礎安全性最佳做法	ECS.8	ECS.8
AWS 基礎安全性最佳做法	等 .9	ECS.9
AWS 基礎安全性最佳做法	ECS.10	ECS.10
AWS 基礎安全性最佳做法	ECS.12	ECS.12
AWS 基礎安全性最佳做法	EFS.1	EFS.1
AWS 基礎安全性最佳做法	EFS.2	EFS.2
AWS 基礎安全性最佳做法	EFS.3	EFS.3
AWS 基礎安全性最佳做法	EFS.4	EFS.4
AWS 基礎安全性最佳做法	EKS.1	EKS.1
AWS 基礎安全性最佳做法	EKS.2	EKS.2
AWS 基礎安全性最佳做法	EKS.8	EK.8
AWS 基礎安全性最佳做法	ElastiCache.1	ElastiCache.1
AWS 基礎安全性最佳做法	ElastiCache.2	ElastiCache.2
AWS 基礎安全性最佳做法	ElastiCache.3	ElastiCache.3
AWS 基礎安全性最佳做法	ElastiCache.4	ElastiCache.4
AWS 基礎安全性最佳做法	ElastiCache.5	ElastiCache.5
AWS 基礎安全性最佳做法	ElastiCache.6	ElastiCache.6
AWS 基礎安全性最佳做法	ElastiCache.7	ElastiCache.7

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 （Security Hub 中對應的安全控制 ID）
AWS 基礎安全性最佳做法	ElasticBeanstalk.1	ElasticBeanstalk.1
AWS 基礎安全性最佳做法	ElasticBeanstalk.2	ElasticBeanstalk.2
AWS 基礎安全性最佳做法	ElasticBeanstalk.3	ElasticBeanstalk.3
AWS 基礎安全性最佳做法	ELB.1	ELB.1
AWS 基礎安全性最佳做法	ELB.2	ELB.2
AWS 基礎安全性最佳做法	ELB.3	ELB.3
AWS 基礎安全性最佳做法	ELB.4	ELB.4
AWS 基礎安全性最佳做法	ELB.5	ELB.5
AWS 基礎安全性最佳做法	ELB.6	ELB.6
AWS 基礎安全性最佳做法	ELB.7	ELB.7
AWS 基礎安全性最佳做法	ELB.8	ELB.8
AWS 基礎安全性最佳做法	ELB.9	ELB.9
AWS 基礎安全性最佳做法	ELB.10	ELB.10
AWS 基礎安全性最佳做法	ELB.12	ELB.12
AWS 基礎安全性最佳做法	ELB.13	ELB.13
AWS 基礎安全性最佳做法	ELB.14	ELB.14

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 （Security Hub 中對應的安全控制 ID）
AWS 基礎安全性最佳做法	精靈 .16	易北省 16
AWS 基礎安全性最佳做法	ELBv2.1	ELB.1
AWS 基礎安全性最佳做法	EMR.1	EMR.1
AWS 基礎安全性最佳做法	EMR.2	EMR.2
AWS 基礎安全性最佳做法	ES.1	ES.1
AWS 基礎安全性最佳做法	ES.2	ES.2
AWS 基礎安全性最佳做法	ES.3	ES.3
AWS 基礎安全性最佳做法	ES.4	ES.4
AWS 基礎安全性最佳做法	ES.5	ES.5
AWS 基礎安全性最佳做法	ES.6	ES.6
AWS 基礎安全性最佳做法	ES.7	ES.7
AWS 基礎安全性最佳做法	ES.8	ES.8
AWS 基礎安全性最佳做法	EventBridge.3	EventBridge3.
AWS 基礎安全性最佳做法	EventBridge.4	EventBridge.4
AWS 基礎安全性最佳做法	FSX.1	FSX.1
AWS 基礎安全性最佳做法	GuardDuty.1	GuardDuty.1
AWS 基礎安全性最佳做法	IAM.1	IAM.1
AWS 基礎安全性最佳做法	IAM.2	IAM.2

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 （Security Hub 中對應的安全控制 ID）
AWS 基礎安全性最佳做法	IAM.3	IAM.3
AWS 基礎安全性最佳做法	IAM.4	IAM.4
AWS 基礎安全性最佳做法	IAM.5	IAM.5
AWS 基礎安全性最佳做法	IAM.6	IAM.6
AWS 基礎安全性最佳做法	IAM.7	IAM.7
AWS 基礎安全性最佳做法	IAM.8	IAM .8
AWS 基礎安全性最佳做法	IAM.9	IAM.9
AWS 基礎安全性最佳做法	我的 .10	亞姆 .10
AWS 基礎安全性最佳做法	IAM.11	IAM.11
AWS 基礎安全性最佳做法	IAM.12	IAM.12
AWS 基礎安全性最佳做法	IAM.13	IAM.13
AWS 基礎安全性最佳做法	IAM.14	IAM.14
AWS 基礎安全性最佳做法	IAM.15	IAM.15
AWS 基礎安全性最佳做法	IAM.16	IAM.16
AWS 基礎安全性最佳做法	IAM.17	IAM.17
AWS 基礎安全性最佳做法	IAM.18	IAM.18
AWS 基礎安全性最佳做法	我的 .19	亚姆 .19
AWS 基礎安全性最佳做法	IAM.21	IAM.21

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 （Security Hub 中對應的安全控制 ID）
AWS 基礎安全性最佳做法	我的 .22	家居安 .22
AWS 基礎安全性最佳做法	Kinesis.1	Kinesis.1
AWS 基礎安全性最佳做法	KMS.1	KMS.1
AWS 基礎安全性最佳做法	KMS.2	KMS.2
AWS 基礎安全性最佳做法	KMS.3	KMS.3
AWS 基礎安全性最佳做法	KMS.4	KMS.4
AWS 基礎安全性最佳做法	Lambda.1	Lambda.1
AWS 基礎安全性最佳做法	Lambda.2	Lambda.2
AWS 基礎安全性最佳做法	Lambda.3	Lambda.3
AWS 基礎安全性最佳做法	Lambda.5	Lambda.5
AWS 基礎安全性最佳做法	馬賽 .1	馬賽 .1
AWS 基礎安全性最佳做法	每米 5 米	每米 5 米
AWS 基礎安全性最佳做法	每克里數	每小米 6
AWS 基礎安全性最佳做法	毫克 .1	MSK.1
AWS 基礎安全性最佳做法	MSK.2	麥斯凱 2
AWS 基礎安全性最佳做法	海王星 1 號	海王星 1
AWS 基礎安全性最佳做法	海王星 2	海王星 2
AWS 基礎安全性最佳做法	海王星 .3	海王星 .3

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 （Security Hub 中對應的安全控制 ID）
AWS 基礎安全性最佳做法	海王星 .4	海王星 .4
AWS 基礎安全性最佳做法	海王星 .5	海王星 .5
AWS 基礎安全性最佳做法	海王星 .6	海王星 .6
AWS 基礎安全性最佳做法	海王星 .7	海王星 .7
AWS 基礎安全性最佳做法	海王星 .8	海王星 .8
AWS 基礎安全性最佳做法	海王星 .9	海王星 .9
AWS 基礎安全性最佳做法	NetworkFirewall.1	NetworkFirewall.1
AWS 基礎安全性最佳做法	NetworkFirewall.2	NetworkFirewall.2
AWS 基礎安全性最佳做法	NetworkFirewall.3	NetworkFirewall.3
AWS 基礎安全性最佳做法	NetworkFirewall.4	NetworkFirewall.4
AWS 基礎安全性最佳做法	NetworkFirewall.5	NetworkFirewall.5
AWS 基礎安全性最佳做法	NetworkFirewall.6	NetworkFirewall.6
AWS 基礎安全性最佳做法	NetworkFirewall.9	NetworkFirewall.9

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 （Security Hub 中對應的安全控制 ID）
AWS 基礎安全性最佳做法	Opensearch.1	Opensearch.1
AWS 基礎安全性最佳做法	Opensearch.2	Opensearch.2
AWS 基礎安全性最佳做法	Opensearch.3	Opensearch.3
AWS 基礎安全性最佳做法	Opensearch.4	Opensearch.4
AWS 基礎安全性最佳做法	Opensearch.5	Opensearch.5
AWS 基礎安全性最佳做法	Opensearch.6	Opensearch.6
AWS 基礎安全性最佳做法	Opensearch.7	Opensearch.7
AWS 基礎安全性最佳做法	Opensearch.8	Opensearch.8
AWS 基礎安全性最佳做法	打開搜索 .10	打開搜索 .10
AWS 基礎安全性最佳做法	PCA.1	PCA.1
AWS 基礎安全性最佳做法	RDS.1	RDS.1
AWS 基礎安全性最佳做法	RDS.2	RDS.2
AWS 基礎安全性最佳做法	RDS.3	RDS.3
AWS 基礎安全性最佳做法	RDS.4	RDS.4
AWS 基礎安全性最佳做法	RDS.5	RDS.5
AWS 基礎安全性最佳做法	RDS.6	RDS.6
AWS 基礎安全性最佳做法	RDS.7	RDS.7
AWS 基礎安全性最佳做法	RDS.8	RDS.8

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 （Security Hub 中對應的安全控制 ID）
AWS 基礎安全性最佳做法	RDS.9	RDS.9
AWS 基礎安全性最佳做法	RDS.10	RDS.10
AWS 基礎安全性最佳做法	RDS.11	RDS.11
AWS 基礎安全性最佳做法	RDS.12	RDS.12
AWS 基礎安全性最佳做法	RDS.13	RDS.13
AWS 基礎安全性最佳做法	RDS.14	RDS.14
AWS 基礎安全性最佳做法	RDS.15	RDS.15
AWS 基礎安全性最佳做法	RDS.16	RDS.16
AWS 基礎安全性最佳做法	RDS.17	RDS.17
AWS 基礎安全性最佳做法	RDS.18	RDS.18
AWS 基礎安全性最佳做法	RDS.19	RDS.19
AWS 基礎安全性最佳做法	RDS.20	RDS.20
AWS 基礎安全性最佳做法	RDS.21	RDS.21
AWS 基礎安全性最佳做法	RDS.22	RDS.22
AWS 基礎安全性最佳做法	RDS.23	RDS.23
AWS 基礎安全性最佳做法	RDS.24	RDS.24
AWS 基礎安全性最佳做法	RDS.25	RDS.25
AWS 基礎安全性最佳做法	RDS.26	RDS.26

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 （Security Hub 中對應的安全控制 ID）
AWS 基礎安全性最佳做法	RDS.27	RDS.27
AWS 基礎安全性最佳做法	RDS.34	RDS.34
AWS 基礎安全性最佳做法	RDS.35	RDS.35
AWS 基礎安全性最佳做法	Redshift.1	Redshift.1
AWS 基礎安全性最佳做法	Redshift.2	Redshift.2
AWS 基礎安全性最佳做法	Redshift.3	Redshift.3
AWS 基礎安全性最佳做法	Redshift.4	Redshift.4
AWS 基礎安全性最佳做法	Redshift.6	Redshift.6
AWS 基礎安全性最佳做法	Redshift.7	Redshift.7
AWS 基礎安全性最佳做法	Redshift.8	Redshift.8
AWS 基礎安全性最佳做法	Redshift.9	Redshift.9
AWS 基礎安全性最佳做法	Redshift.10	Redshift.10
AWS 基礎安全性最佳做法	香港路線	香港路線
AWS 基礎安全性最佳做法	S3.1	S3.1
AWS 基礎安全性最佳做法	S3.2	S3.2
AWS 基礎安全性最佳做法	S3.3	S3.3
AWS 基礎安全性最佳做法	S3.4	S3.4
AWS 基礎安全性最佳做法	S3.5	S3.5

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 （Security Hub 中對應的安全控制 ID）
AWS 基礎安全性最佳做法	S3.6	S3.6
AWS 基礎安全性最佳做法	S3.7	S3.7
AWS 基礎安全性最佳做法	S3.8	S3.8
AWS 基礎安全性最佳做法	S3.9	S3.9
AWS 基礎安全性最佳做法	S3.11	S3.11
AWS 基礎安全性最佳做法	S3.12	S3.12
AWS 基礎安全性最佳做法	S3.13	S3.13
AWS 基礎安全性最佳做法	S3.14	S3.14
AWS 基礎安全性最佳做法	S3.15	S3.15
AWS 基礎安全性最佳做法	S3.17	S3.17
AWS 基礎安全性最佳做法	S3.19	S3.19
AWS 基礎安全性最佳做法	S3.19	S3.20
AWS 基礎安全性最佳做法	SageMaker.1	SageMaker.1
AWS 基礎安全性最佳做法	SageMaker.2	SageMaker.2
AWS 基礎安全性最佳做法	SageMaker.3	SageMaker.3
AWS 基礎安全性最佳做法	SecretsManager.1	SecretsManager.1

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 （Security Hub 中對應的安全控制 ID）
AWS 基礎安全性最佳做法	SecretsManager.2	SecretsManager.2
AWS 基礎安全性最佳做法	SecretsManager.3	SecretsManager.3
AWS 基礎安全性最佳做法	SecretsManager.4	SecretsManager.4
AWS 基礎安全性最佳做法	SNS.1	SNS.1
AWS 基礎安全性最佳做法	SNS.2	SNS.2
AWS 基礎安全性最佳做法	SQS.1	SQS.1
AWS 基礎安全性最佳做法	SSM.1	SSM.1
AWS 基礎安全性最佳做法	SSM.2	SSM.2
AWS 基礎安全性最佳做法	SSM.3	SSM.3
AWS 基礎安全性最佳做法	SSM.4	SSM.4
AWS 基礎安全性最佳做法	StepFunctions.1	StepFunctions.1
AWS 基礎安全性最佳做法	WAF.1	WAF.1
AWS 基礎安全性最佳做法	WAF.2	WAF.2
AWS 基礎安全性最佳做法	WAF.3	WAF.3
AWS 基礎安全性最佳做法	WAF.4	WAF.4
AWS 基礎安全性最佳做法	WAF.6	WAF.6

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 （Security Hub 中對應的安全控制 ID）
AWS 基礎安全性最佳做法	WAF.7	WAF.7
AWS 基礎安全性最佳做法	WAF.8	WAF.8
AWS 基礎安全性最佳做法	WAF.10	WAF.10
AWS 基礎安全性最佳做法	WAF.11	WAF.11
AWS 基礎安全性最佳做法	WAF.12	WAF.12

支援的 API 呼叫 AWS Audit Manager

Audit Manager 會呼叫 API， AWS 服務 以收集資源的組態詳細 AWS 資料快照。當您在 Audit Manager 中設定自訂控制項時，您可以將這些 API 呼叫指定為資料來源映射項目。

Audit Manager 會擷取 API 呼叫範圍內的每個資源組態快照，並轉換成證據。如此一來，每個資源都會獲得一個證據，而不是每個 API 呼叫使用一個證據。

例如，如果 `ec2_DescribeRouteTables` API 呼叫從五個路由表擷取組態快照，則單一 API 呼叫總共會獲得五個證據。每個證據都是個別路由表組態的快照。

在此頁面

- 自訂控制項資料來源支援的 API 呼叫
- 編頁 API 呼叫
- AWS License Manager 標準架構中使用的 API 呼叫

自訂控制項資料來源支援的 API 呼叫

在自訂控制項中，您可以使用下列 API 呼叫中的任何一個作為資料來源。然後，Audit Manager 可以使用這些 API 呼叫來收集有關您使用 AWS 情況的證據。

支援的 API 呼叫	Audit Manager 如何使用此 API 收集證據
acm_ GetAccountConfiguration	收集與您 AWS 帳戶關聯的帳戶組態選項的快照。
acm_ ListCertificates	擷取憑證 ARN 和網域名稱的清單。
雲徑 _ DescribeTrails	收集一或多個線索 (與您 AWS 帳戶的目前區域關聯) 的設定之快照。
雲觀察 _ DescribeAlarms	收集用於您 AWS 帳戶的警報之組態快照。
配置 _ DescribeConfigRules	檢索有關 AWS Config 規則的詳細信息。
配置 _ DescribeDeliveryChannels	收集您 AWS 帳戶中的交付管道之組態快照。
直接連接 _ DescribeDirectConnectGateways	擷取所有 AWS Direct Connect 閘道的清單。
直接連接 _ DescribeVirtualGateways	擷取 AWS 帳戶所擁有的虛擬私有閘道清單。
文件資料庫 _ DescribeCertificates	收集您 AWS 帳戶的憑證清單。
文件描述 ClusterParameterGroups	收集您 AWS 帳戶的 `DBClusterParameterGroup` 描述之清單。
docdb_DescribeDBInstances	收集您 AWS 帳戶的已佈建 Amazon DynamoDB 執行個體之相關資訊。
動力 b_ DescribeTable	收集您 AWS 帳戶中 DynamoDB 資料表的組態快照。 使用此 API 做為資料來源時，您不需要提供特定 DynamoDB 表格的名稱。相反地，Audit Manager 會使用 `ListTables` 作業來列出您的所有表格。然後，Audit Manager 會針對列出的每個表格執行 `DescribeTable` 作業，以產生該資源的證據。
動力 b_ ListBackups	擷取與您 AWS 帳戶關聯的 DynamoDB 備份清單。

支援的 API 呼叫	Audit Manager 如何使用此 API 收集證據
動力 b_ ListGlobalTables	擷取目前在您 AWS 帳戶中的所有全域資料表清單。
動力 b_ ListTables	擷取與您 AWS 帳戶 和目前端點關聯的所有資料表名稱的清單。
ec2_ DescribeAddresses	收集彈性 IP 地址的快照。
ec2_ DescribeCustomerGateways	收集 VPN 客戶閘道的快照。
ec2_ DescribeEgressOnlyInternetGateways	收集僅限輸出網際網路閘道的快照。
ec2_ DescribeFlowLogs	收集流量日誌的快照。
ec2_ DescribeInstances	收集執行個體的快照。
ec2_ DescribeInternetGateways	收集網際網路閘道的快照。
ec2_ DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations	收集您的虛擬介面群組與本機閘道路由表之間的關聯說明 AWS 帳戶。
ec2_ DescribeLocalGateways	收集本機閘道的快照。
ec2_ DescribeLocalGatewayVirtualInterfaces	收集本機閘道虛擬介面的快照。
ec2_ DescribeNatGateways	收集 NAT 閘道的快照。
ec2_ DescribeNetworkAcls	收集網路 ACL 的快照。
ec2_ DescribeRouteTables	收集路由表的快照。
ec2_ DescribeSecurityGroups	收集安全群組的快照。
ec2_ DescribeTransitGateways	收集運輸閘道的快照。

支援的 API 呼叫	Audit Manager 如何使用此 API 收集證據
ec2_ DescribeVolumes	收集 VPC 端點的快照。
ec2_ DescribeVpcs	收集 VPC 的快照。
ec2_ DescribeVpcEndpoints	收集 VPC 端點的快照。
ec2_ DescribeVpcPeering Connections	收集 VPN 連線的快照。
ec2_ DescribeVpnConnect ions	收集 VPN 連線的快照。
ec2_ DescribeVpnGateways	收集虛擬私有閘道的快照。
ec2_ GetEbsDefaultKmsKeyId	為您 AWS 帳戶 目前區域中 AWS KMS key 的 EBS 加密收集預設快照。
ec2_ GetEbsEncryptionBy Default	說明是否在目前區域中為您的 AWS 帳戶 預設啟用 EBS 加密。
Ecs_ DescribeClusters	收集 ECS 叢集的快照。
EKS DescribeAddonVersions	收集您附加元件版本的快照。
彈性 _ DescribeCacheClust ers	收集已佈建叢集的快照。
彈性 _ DescribeServiceUpd ates	收集 Amazon 服務更新的快照 ElastiCache。
彈性檔案系統 _ DescribeA ccessPoints	收 Amazon EFS 的 AWS 帳戶.
彈性檔案系統 _ DescribeF ileSystems	收集 Amazon EFS 檔案系統的快照。
彈性負載平衡 v2_ DescribeL oadBalancers	收集您 AWS 帳戶的.

支援的 API 呼叫	Audit Manager 如何使用此 API 收集證據
elasticloadbalancingv2_DescribeSSLPolicies	收集您用於 SSL 交涉的政策快照。
彈性負載平衡 v2_ DescribeTargetGroups	收集 ELB 目標群組的快照。
彈性試管 _ ListSecurityConfigurations	擷取您 AWS 帳戶可見的安全性組態清單，及其建立日期和時間，以及名稱。
活動資訊 _ ListConnections	檢索您的 Amazon EventBridge 連接列表 AWS 帳戶。
活動資訊 _ ListEventBuses	擷取您的 Amazon EventBridge 事件匯流排清單 AWS 帳戶，包括預設事件匯流排、自訂事件匯流排和合作夥伴事件匯流排。
活動資訊 _ ListEventSources	擷取已與您 AWS 帳戶共用的合作夥伴事件來源清單。
活動資訊 _ ListRules	檢索您的 Amazon EventBridge 規則列表。
火管 _ ListDeliveryStreams	擷取交付串流的清單。
FSX_ DescribeFileSystems	收集您 AWS 帳戶所擁有的檔案系統之快照。
守衛 _ ListDetectors	`detectorIds` 為您的 Amazon GuardDuty 偵測器資源擷取清單。
iam_ GenerateCredentialReport	產生 AWS 帳戶的憑證報告。
iam_ GetAccountPasswordPolicy	收集您 AWS 帳戶的密碼政策之快照。
iam_ GetAccountSummary	收集您 AWS 帳戶中 IAM 實體用量和 IAM 配額的快照。
iam_ ListGroupPolicies	擷取內嵌在您的 IAM 群組中的內嵌政策清單 AWS 帳戶。
iam_ ListGroups	擷取 IAM 群組清單，這些群組與您的 AWS 帳戶.
我的識別碼 ListOpenConnectProviders	擷取在您 AWS 帳戶中定義的 IAM OpenID Connect (OIDC) 供應商資源物件的清單。

支援的 API 呼叫	Audit Manager 如何使用此 API 收集證據
iam_ ListPolicies	擷取您 AWS 帳戶中可用的所有受管政策清單，包含您自己的客戶定義受管政策和所有 AWS 受管政策。
iam_ ListRoles	擷取 IAM 角色的清單，這些角色與您的 AWS 帳戶.
iam_ListSAMLProviders	擷取在您 AWS 帳戶中 IAM 內定義的 SAML 供應商資源物件的清單。
iam_ ListUsers	擷取您中的 IAM 使用者清單 AWS 帳戶。
iam_ MFA 设备 ListVirtual	擷取您 AWS 帳戶中定義的虛擬 MFA 裝置清單。
卡夫卡 _ ListClusters	擷取您的. AWS 帳戶
卡夫卡 _ ListKafkaVersions	擷取您 AWS 帳戶中 Apache Kafka 版本物件的清單。
運動 _ ListStreams	擷取 Kinesis 資料串流的清單。
kms_ GetKeyPolicy	Audit Manager 會使用此 API 來收集您 AWS KMS keys 中 AWS 帳戶的金鑰政策之快照。 當您使用此 API 作為資料來源時，您不需要提供特定的名稱 AWS KMS key。相反地，Audit Manager 會使用 `ListKeys` 作業來列出您所有的 KMS 金鑰。然後，Audit Manager 會針對列出的每個 KMS 金鑰執行 `GetKeyPolicy` 作業，以產生該資源的證據。
kms_ GetKeyRotationStatus	Audit Manager 使用此 API 來收集您 AWS KMS keys 的 AWS 帳戶. 當您使用此 API 作為資料來源時，您不需要提供特定的名稱 AWS KMS key。相反地，Audit Manager 會使用 `ListKeys` 作業來列出您所有的 KMS 金鑰。然後，Audit Manager 會針對列出的每個 KMS 金鑰執行 `GetKeyRotationStatus` 作業，以產生該資源的證據。
kms_ ListKeys	擷取 AWS KMS keys 中的清單 AWS 帳戶。

支援的 API 呼叫	Audit Manager 如何使用此 API 收集證據
羔羊 ListFunctions	使用每個函數的特定版本組態 AWS 帳戶，擷取您中的 Lambda 函數清單。
rds_DescribeDBClusters	收集您的. 中現有 Amazon Aurora 資料庫叢集和異地同步備份資料庫叢集的 AWS 帳戶快照。
rds_DescribeDBInstances	收集您 AWS 帳戶中已佈建 RDS 執行個體的快照。
紅色移動 _ DescribeClusters	收集您 AWS 帳戶中已佈建 Amazon Redshift 叢集的快照。
s3_ GetBucketEncryption	收集顯示 S3 儲存貯體預設加密組態的快照。 使用此 API 做為資料來源時，您不需要提供特定的 S3 儲存貯體的名稱。相反地，Audit Manager 會使用 `ListBuckets` 作業來列出您的所有儲存貯體。然後，Audit Manager 會針對列出的每個儲存貯體執行 `GetBucketEncryption` 作業，以產生該資源的證據。 Audit Manager 只能 AWS 區域 為在您的評估中建立的值區提供加密狀態。如果您需要查看跨多個 S3 儲存貯體的加密狀態 AWS 區域，建議您在每個擁有 S3 儲存貯體的 AWS 區域 位置建立評估。
s3_ ListBuckets	擷取 AWS 帳戶. 中的 S3 儲存貯體清單
sns_ ListTopics	擷取您中的 SNS 主題清單 AWS 帳戶。
平方米 _ ListQueues	擷取您 AWS 帳戶中的 SQS 佇列清單。

編頁 API 呼叫

許多人 AWS 服務 收集和存儲大量數據。因此，當`list`、`describe`、或 `get` API 呼叫嘗試傳回您的資料時，可能會有很多結果。如果資料量太大而無法在單次回應中全部顯示，則可以透過編頁功能將結果分為更易於管理的部分。這會將結果劃分為資料的「分頁」，使回應更容易處理。

Audit Manager 支援的某些 API 呼叫會進行編頁。這代表它們會先傳回部分結果，並要求後續請求傳回整個結果集。舉例來說，Amazon RDS DescribeDBInstances 單次作業最多可傳回 100 個執行個體，如需傳回下一頁結果，則需要後續請求。

自 2023 年 3 月 8 日起，Audit Manager 支援分頁 API 呼叫做為證據收集的資料來源。以前，如果使用分頁的 API 呼叫做為資料來源，則 API 回應中僅傳回您的資源子集（最多 100 個結果）。現在，Audit Manager 會多次呼叫分頁的 API 作業，並取得每個結果頁面，直至傳回所有資源為止。接下來，Audit Manager 會針對每個資源擷取組態快照集，並將其儲存為證據。由於您的完整資源集現在已在 API 回應中擷取完畢，因此您可能會發現所收集的證據量有所增加。

Audit Manager 會自動為您處理 API 呼叫分頁。如果您對使用分頁的 API 呼叫建立自訂控制項並作為資料來源，則不需要指定任何分頁參數。

AWS License Manager 標準架構中使用的 API 呼叫

在AWS License Manager標準架構中，Audit Manager 會使用自訂活動呼叫 `GetLicenseManagerSummary` 來收集證據。此活動會呼叫下列三個 License Manager API：

- ListLicenseConfigurations
- ListAssociationsForLicenseConfiguration
- ListUsageForLicenseConfiguration

然後，傳回的資料會轉換成證據，並附加至評估中的相關控制項。

範例

假設您使用兩個授權產品（2017 年版 SQL 服務和 Oracle 資料庫企業版）。首先，`GetLicenseManagerSummary`活動會呼叫 ListLicenseConfigurationsAPI，該 API 會提供您帳戶中授權設定的詳細資料。接下來，它通過調用ListUsageForLicenseConfiguration和為每個許可證配置添加其他上下文數據ListAssociationsForLicenseConfiguration。最後，它將授權組態資料轉換為證據，並將其附加到架構中的對應控制項（4.5 - 2017 SQL 伺服器客戶管理授權和 3.0.4 - Oracle 資料庫企業版客戶管理授權）。

如果您使用的授權產品未涵蓋架構中任何控制項，則該授權組態資料會附加至下列控制項的證據：5.0 — 其他授權的客戶管理授權。

AWS CloudTrail 支援的事件名稱 AWS Audit Manager

您可以在稽核 AWS CloudTrail 管理員中擷取管理事件和全域服務事件做為證據。若要這麼做，您可以在建立自訂控制項時，將 CloudTrail 事件名稱指定為資料來源對應關鍵字。

> **Note**
>
> Audit Manager 僅擷取管理事件和全域服務事件。資料事件和洞見事件無法作為證據。如需有關不同類型 CloudTrail 事件的詳細資訊，請參閱《AWS CloudTrail 使用指南》中的CloudTrail 概念。

除了上述情況之外，Audit Manager 不支援下列 CloudTrail 事件：

- 公里 _ GenerateDataKey
- kms_Decrypt
- sts_ AssumeRole
- 动力视频 GetDataEndpoint
- 动力视频 GetSignalingChannelEndpoint
- 动力视频 DescribeSignalingChannel
- 动力视频 DescribeStream

自 2023 年 5 月 11 日起，Audit Manager 不再支援唯讀 CloudTrail 事件做為證據收集的關鍵字。我們總共刪除了 3,135 個唯讀關鍵字。由於客戶和 AWS 服務 兩者都對 API 進行讀取呼叫，因此唯讀事件會很雜亂。因此，唯讀關鍵字會收集許多不可靠或與稽核無關的證據。唯讀關鍵字包括`ListDescribe`、和 `Get` API 呼叫 (例如 GetObject，ListBuckets適用於 Amazon S3)。如果您使用這些關鍵字之一來收集證據，則無需執行任何作業。系統已自動從 Audit Manager 主控台和您的評估中移除關鍵字，而且不會再為這些關鍵字收集證據。

AWS Audit Manager 設定

您可以隨時檢閱與設定 AWS Audit Manager 的設定。

存取您的設定

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在左側的導覽窗格中，選擇設定。

可用的設定如下：

- 一般設定
  - 許可
  - 資料加密
  - 委派管理員 (選用)
  - AWS Config (選用)
  - Security Hub (選用)
  - 停用 AWS Audit Manager
- 評估設定
  - 預設稽核擁有者 (選用)
  - 評估報告目的地 (選用)
  - 通知 (選用)
- 證據搜尋工具設定
  - 證據搜尋工具 (選用)
  - 匯出目的地 (選用)

一般設定

一般設定索引標籤是 Audit Manager 主控台中設定頁面的預設檢視。使用此索引標籤可以檢閱和更新您的 Audit Manager 一般設定。

主題

- 許可
- 資料加密
- 委派管理員 (選用)
- AWS Config (選用)
- Security Hub (選用)
- 停用 AWS Audit Manager

許可

AWS Audit Manager 使用服務連結角色代表您連線到資料來源。如需更多詳細資訊，請參閱 使用服務連結角色 AWS Audit Manager。

如需檢閱 Audit Manager 使用之服務連結角色的詳細資訊，請選擇檢視 IAM 服務連結角色許可。

如需服務連結角色的詳細資訊，請參閱 IAM 使用者指南中的使用服務連結角色。

資料加密

Audit Manager 會自動建立用於資料安全儲存唯一 AWS 受管金鑰。依預設，您的 Audit Manager 資料會使用此 KMS 金鑰加密。或者，如果您想要自訂資料加密設定，您可以指定自己的對稱加密客戶受管金鑰。使用您自己的 KMS 金鑰 可為您提供更多彈性，包括能夠建立、旋轉和停用金鑰。

> **Important**
>
> 如需成功產生評估報告並匯出證據搜尋工具的搜尋結果，您的客戶受管金鑰 (如提供) 必須與您的評估處於同一 AWS 區域。如需 Audit Manager 區域清單，請參閱 Amazon Web Services 一般參考中的 AWS Audit Manager 端點和配額。

您可以使用 Audit Manager 主控台、AWS Command Line Interface (AWS CLI) 或 Audit Manager API 來更新資料加密設定。

Audit Manager console

更新您的資料加密設定 (主控台)

1. 從 一般設定索引標籤，前往資料加密區段。

2. 如需使用 Audit Manager 提供的預設 KMS 金鑰，請清除 自訂加密設定 (進階) 核取方塊。
3. 如需使用客戶受管金鑰，請選擇自訂加密設定 (進階) 核取方塊。您可選擇現有 KMS 金鑰或建立新的金鑰。

AWS CLI

如需更新您的資料加密設定 (AWS CLI)

執行更新設定命令，並使用 `--kms-key` 參數來指定您自己的客戶受管金鑰。

在下列範例中，將######取代為您自己的資訊。

```
aws auditmanager update-settings --kms-key arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

Audit Manager API

如需更新您的資料加密設定 (API)

呼叫 UpdateSettings 操作，並使用 KMSKey 參數來指定您自己的客戶受管金鑰。

如需詳細資訊，請選擇先前的連結以閱讀 Audit Manager API 參考中的更多資訊。這包括有關如何在其中一項特定語言 AWS 軟體開發套件中使用此操作和參數的資訊。

> **Note**
>
> 如果您變更 Audit Manager 資料加密設定，這些變更會套用至您建立的任何新評估。這包括您依據新評估建立的任何評估報告和證據搜尋工具匯出。
> 這些變更不會套用至您在變更加密設定之前，已建立的現有評估。除現有的評估報告和 CSV 匯出外，還包括您依據現有評估建立的新評估報告和 CSV 匯出。現有的評估及其所有評估報告和 CSV 匯出都將繼續使用舊有的 KMS 金鑰。
> 如果產生評估報告的 IAM 身分無法使用舊有 KMS 金鑰，則在金鑰政策層級授予許可。如需指示，請參閱 AWS Key Management Service 開發人員指南中的允許其他帳戶中的使用者使用 KMS 金鑰。

如需有關如何建立金鑰的說明，請參閱AWS Key Management Service 使用者指南中的建立金鑰。

委派管理員 (選用)

如果您使用 AWS Organizations 且想要啟用 Audit Manager 的多帳戶支援，您可以將組織中的一個成員帳戶指定為 Audit Manager 的委派管理員。

先決條件

- 您的帳戶必須屬於組織帳戶。如需詳細資訊，請參閱 AWS Organizations 使用者指南中的建立和管理組織。
- 指定委派管理員之前，您必須先啟用組織中的所有功能。此外，您必須設定組織的 Security Hub 設定。如此一來，Audit Manager 就可以從您的成員帳戶收集 Security Hub 證據。
- 委派的管理員帳戶必須具有您在設定 Audit Manager 員時提供的 KMS 金鑰的存取權。如需檢閱和變更您的加密設定，請參閱 資料加密。

Audit Manager 中委派管理員的重要考量

請注意下列定義委派管理員如何在 Audit Manager 中運作的因素。

管理帳戶

您無法在 Audit Manager 使用 AWS Organizations 管理帳號作為委派系統管理員。

跨多個 AWS 區域 使用委派管理員

如果您要在多個 AWS 區域 啟用 Audit Manager，則必須在每個區域中單獨指定委派的管理員帳戶。在 Audit Manager 設定中，您應該在所有區域中使用相同的委派管理員帳戶。

證據搜尋工具清理任務

在您使用管理帳戶移除或變更委派管理員之前，請確定目前的委派管理員帳戶已登入 Audit Manager 並停用證據搜尋工具。停用證據搜尋工具會自動刪除啟用證據搜尋工具時帳戶中建立的事件資料存放區。

如果此任務未完成，則事件資料存放區會保留在帳戶中。在此情況下，建議原始委派管理員使用 CloudTrail Lake 手動刪除事件資料存放區。

為了確保您最終不會產生多個事件資料存放區，有必要進行此清理任務。在您移除或變更委派的管理員帳戶後，Audit Manager 會忽略未使用的事件資料存放區。但是，如果您未刪除未使用的事件資料存放區，則事件資料存放區會繼續產生 CloudTrail Lake 儲存成本。

資料刪除

當您移除 Audit Manager 的委派管理員帳戶時，不會刪除該帳戶的資料。如果您想要刪除委派管理員帳戶的資源資料，則必須先單獨執行該任務，然後才能移除帳戶。您可以在 Audit Manager 主控台中執行這項操作。或者，您可以使用 Audit Manager 提供的其中一項 API 刪除操作。如需可用刪除操作的清單，請參閱刪除 Audit Manager 資料。

目前，Audit Manager 不提供刪除特定委派管理員證據的選項。相反地，當您註銷 Audit Manager 管理帳戶時，我們會在註銷時對目前的委派管理員帳戶執行清除任務。

如需 Audit Manager 中常見組織和委派管理員問題的解決方案，請參閱委派系統管理員與 AWS Organizations 相關問題疑難排解。

為 Audit Manager 映射委派的管理員帳戶

您可以檢閱和變更委派管理員帳戶設定，如下所示。

新增委派管理員

您可以使用 Audit Manager 主控台、AWS Command Line Interface (AWS CLI) 或 Audit Manager API 來新增委派管理員。

> **Note**
>
> 在 Audit Manager 設定中新增委派管理員後，您的管理帳戶將無法再在 Audit Manager 中建立其他評估。此外，針對管理帳戶建立的任何現有評估，系統會停止證據收集。Audit Manager 會收集證據並附加至委派管理員帳戶，委派管理員是管理組織評估的主要帳戶。

Audit Manager console

新增委派的管理員 (主控台)

1. 從一般設定索引標籤，前往委派管理員區段。
2. 在委派管理員帳戶 ID項下，輸入委派管理員的帳戶 ID。
3. 選擇委派。

AWS CLI

新增委派的管理員 (AWS CLI)

執行 register-organization-admin-account 命令，並使用 `--admin-account-id` 參數來指定委派管理員的帳戶 ID。

在下列範例中，將######取代為您自己的資訊。

```
aws auditmanager register-organization-admin-account --admin-account-id 111122223333
```

Audit Manager API

新增目前的委派管理員 (API)

呼叫 RegisterOrganizationAdminAccount 操作，並使用 AdminAccountId 參數來指定委派管理員的帳戶 ID。

如需詳細資訊，請選擇先前的連結以閱讀 Audit Manager API 參考中的更多資訊。這包括有關如何在其中一項特定語言 AWS 軟體開發套件中使用此操作和參數的資訊。

變更委派管理員

您可以使用 Audit Manager 主控台、AWS Command Line Interface (AWS CLI) 或 Audit Manager API 來變更委派的管理員。

> **Warning**
>
> 當您變更委派管理員時，您可以繼續存取先前在舊有委派管理員帳戶下收集的證據。不過，Audit Manager 會停止收集證據，並停止將證據附加至舊有委派管理員帳戶。

Audit Manager console

變更目前委派管理員 (主控台)

1. (選用) 如果目前委派管理員 (帳戶 A) 已啟用證據搜尋工具，請執行下列清除任務：

   - 將帳戶 B 指派為新的委派管理員之前，請確定帳戶 A 登入 Audit Manager 並停用證據搜尋工具。

     停用證據搜尋工具會自動刪除帳戶 A 啟用證據搜尋工具時建立的事件資料存放區。如果您未完成此步驟，則帳戶 A 必須前往 CloudTrail Lake 並手動刪除事件資料存放區。否則，事件資料存放區會保留在帳戶 A 中，並繼續產生 CloudTrail Lake 儲存費用。

2. 從一般設定索引標籤，前往委派管理員區段並選擇移除。
3. 在出現的快顯視窗中，選擇移除以確認移除。
4. 在委派管理員帳戶 ID項下，輸入新委派管理員帳戶 ID。
5. 選擇委派。

AWS CLI

開始之前

如果目前委派管理員 (帳戶 A) 已啟用證據搜尋工具，請執行下列清除任務：

將帳戶 B 指派為新的委派管理員之前，請確定帳戶 A 登入 Audit Manager 並停用證據搜尋工具。

停用證據搜尋工具會自動刪除帳戶 A 啟用證據搜尋工具時建立的事件資料存放區。如果您未完成此步驟，則帳戶 A 必須前往 CloudTrail Lake 並手動刪除事件資料存放區。否則，事件資料存放區會保留在帳戶 A 中，並繼續產生 CloudTrail Lake 儲存費用。

變更目前委派管理員 (AWS CLI)

執行 deregister-organization-admin-account 命令，並使用 `--admin-account-id` 參數來指定目前委派管理員的帳戶 ID。

在下列範例中，將*######*取代為您自己的資訊。

```
aws auditmanager deregister-organization-admin-account --admin-account-
id 111122223333
```

執行 register-organization-admin-account 命令，並使用 `--admin-account-id` 參數來指定新委派管理員的帳戶 ID。

在下列範例中，將*######*取代為您自己的資訊。

```
aws auditmanager register-organization-admin-account --admin-account-id 444455556666
```

Audit Manager API

開始之前

如果目前委派管理員 (帳戶 A) 已啟用證據搜尋工具，請執行下列清除任務：

將帳戶 B 指派為新的委派管理員之前，請確定帳戶 A 登入 Audit Manager 並停用證據搜尋工具。

停用證據搜尋工具會自動刪除帳戶 A 啟用證據搜尋工具時建立的事件資料存放區。如果您未完成此步驟，則帳戶 A 必須前往 CloudTrail Lake 並手動刪除事件資料存放區。否則，事件資料存放區會保留在帳戶 A 中，並繼續產生 CloudTrail Lake 儲存費用。

變更目前委派的管理員 (API)

首先，呼叫 DeregisterOrganizationAdminAccount 命令，並使用 adminAccountId 參數來指定目前委派管理員的帳戶 ID。

然後，呼叫 RegisterOrganizationAdminAccount 操作，並使用 adminAccountId 參數來指定新委派管理員的帳戶 ID。

如需詳細資訊，請選擇先前的連結以閱讀 Audit Manager API 參考中的更多資訊。這包括有關如何在其中一項特定語言 AWS 軟體開發套件中使用此操作和參數的資訊。

移除委派管理員

您可以使用 Audit Manager 主控台、AWS Command Line Interface (AWS CLI) 或 Audit Manager API 來移除委派管理員。

> **Warning**
>
> 當您移除委派管理員時，您可以繼續存取先前在該委派管理員帳戶下收集的證據。不過，Audit Manager 會停止收集證據，並停止將證據附加至舊有委派管理員帳戶。

Audit Manager console

移除目前委派管理員 (主控台)

1. (選用) 如果目前委派管理員 已啟用證據搜尋工具，請執行下列清除任務：
   - 確定目前委派管理員帳戶登入 Audit Manager 並停用證據搜尋工具。

     停用證據搜尋工具會自動刪除啟用證據搜尋工具時帳戶中建立的事件資料存放區。如果未完成此步驟，委派管理員帳戶必須使用 CloudTrail Lake 手動刪除事件資料存放區。否則，事件資料存放區會保留在帳戶中，並繼續產生 CloudTrail Lake 儲存費用。
2. 從一般設定索引標籤，前往委派管理員區段並選擇移除。
3. 在出現的快顯視窗中，選擇移除以確認移除。

AWS CLI

開始之前

如果目前委派管理員已啟用證據搜尋工具，請執行下列清除任務：

確定目前委派管理員帳戶登入 Audit Manager 並停用證據搜尋工具。

停用證據搜尋工具會自動刪除啟用證據搜尋工具時帳戶中建立的事件資料存放區。如果未完成此步驟，委派管理員帳戶必須使用 CloudTrail Lake 手動刪除事件資料存放區。否則，事件資料存放區會保留在帳戶中，並繼續產生 CloudTrail Lake 儲存費用。

如需移除目前的委派管理員 (AWS CLI)

執行 deregister-organization-admin-account 命令，並使用 `--admin-account-id` 參數來指定委派管理員的帳戶 ID。

在下列範例中，將######取代為您自己的資訊。

```
aws auditmanager deregister-organization-admin-account --admin-account-
id 111122223333
```

Audit Manager API

開始之前

如果目前委派管理員已啟用證據搜尋工具，請執行下列清除任務：

確定目前委派管理員帳戶登入 Audit Manager 並停用證據搜尋工具。

停用證據搜尋工具會自動刪除啟用證據搜尋工具時帳戶中建立的事件資料存放區。如果未完成此步驟，委派管理員帳戶必須使用 CloudTrail Lake 手動刪除事件資料存放區。否則，事件資料存放區會保留在帳戶中，並繼續產生 CloudTrail Lake 儲存費用。

移除目前委派的系統管理員 (API)

首先，呼叫 DeregisterOrganizationAdminAccount 命令，並使用 adminAccountId 參數來指定委派管理員的帳戶 ID。

如需詳細資訊，請選擇先前的連結以閱讀 Audit Manager API 參考中的更多資訊。這包括有關如何在其中一項特定語言 AWS 軟體開發套件中使用此操作和參數的資訊。

AWS Config (選用)

您可以允許 Audit Manager 從 AWS Config 中收集調查結果。AWS Config 啟用後，Audit Manager 會通報直接來自 AWS Config 的安全檢查結果，擷取資源安全狀態的快照。為了在 Audit Manager 中獲得最佳體驗，我們建議您啟用 AWS Config：

如需啟用 AWS Config，請選擇 啟用 AWS Config 前往該服務。如需有關如何啟用 AWS Config 的說明，請參閱 AWS Config 開發人員指南中的設定 AWS Config。

Security Hub (選用)

您可以允許 Audit Manager 匯入所有支援的合規標準的 AWS Security Hub 調查結果。啟用 Security Hub 後，Audit Manager 會透過直接來自 Security Hub 的安全檢查結果，擷取資源安全狀態的快照。為了在 Audit Manager 中獲得最佳體驗，我們建議您啟用 Security Hub：

如需啟用 Security Hub，請選擇 啟用 Security Hub 以前往該服務。如需有關如何啟用 Security Hub 的說明，請參閱 Security Hub 使用者指南中的設定 AWS Security Hub。

停用 AWS Audit Manager

如果您不想再使用此服務，您可以停用 Audit Manager。當您停用 Audit Manager 時，您也可以選擇刪除所有資料。

依預設，停用 Audit Manager 時，不會刪除您的資料。您的證據資料會自建立之日起保留兩年。您的其他 Audit Manager 資源 (包括評估、自訂控制項和自訂架構) 會無限期保留，您日後重新啟用 Audit Manager 即可使用這些資源。如需有關資料保留的詳細資訊，請參閱本指南中的資料保護。

如果您選擇刪除資料，Audit Manager 會刪除所有證據資料以及您建立的所有 Audit Manager 資源 (包括評估、自訂控制項和自訂架構)。您的所有資料都會在停用 Audit Manager 後七天內刪除。

> **Warning**
>
> - 當您停用 Audit Manager 時，您的存取權即會撤銷，且該服務不再收集任何現有評估的證據。除非您重新啟用 Audit Manager，否則您無法存取服務中的任何內容。
> - 刪除所有資料屬於永久動作。即使您決定日後重新啟用 Audit Manager，您的資料也無法復原。

您可以使用 Audit Manager 主控台、AWS Command Line Interface (AWS CLI) 或 Audit Manager API 來停用 Audit Manager。

Audit Manager console

如需停用 Audit Manager (主控台)

1. 從一般設定索引標籤，前往停用 AWS Audit Manager 區段。
2. 選擇停用。
3. 在快顯視窗中，檢閱您目前的資料保留設定。
   a. 選擇停用 Audit Manager 繼續下一步。
   b. 如需變更您目前的選擇，請執行下列步驟：
      i. 選擇取消以返回設定頁面。
      ii. 如需使用預設的資料保留設定，請關閉刪除所有資料。此選項會保留證據資料，時間為從建立之日起兩年，並無限期保留其他 Audit Manager 資源。
      iii. 如需刪除資料，請開啟刪除所有資料。
      iv. 選擇停用，然後選擇停用 Audit Manager以確認您的選擇。

AWS CLI

開始之前

停用 Audit Manager 之前，您可以執行update-settings命令設定您的首選資料保留政策。依預設，Audit Manager 會保留您的資料。如果您要請求刪除資料，請使用 `--deregistration-policy`參數，並將 `deleteResources` 值設定為 `ALL`。

```
aws auditmanager update-settings --deregistration-policy deleteResources=ALL
```

如需停用 Audit Manager (AWS CLI)

當您準備好停用 Audit Manager 時，請執行 deregister-account 命令。

```
aws auditmanager deregister-account
```

Audit Manager API

開始之前

停用 Audit Manager 之前，您可以使用UpdateSettings API 操作來設定您的首選資料保留政策。依預設，Audit Manager 會保留您的資料。如果您想刪除您的數據，您可以使用 DeregistrationPolicy 屬性來請求刪除您的數據。

如需停用 Audit Manager (API)

當您準備好停用 Audit Manager 時，請呼叫 DeregisterAccount 操作。

如需詳細資訊，請選擇先前的連結以閱讀 Audit Manager API 參考中的更多資訊。這包括有關如何在其中一項特定語言 AWS 軟體開發套件中使用這些操作和參數的資訊。

如需在停用 Audit Manager 之後重新啟用 Audit Manager

前往 Audit Manager 服務首頁，並依照步驟將 Audit Manager 設定為新使用者。如需更多詳細資訊，請參閱 設定 AWS Audit Manager。

> **Tip**
>
> - 如果您選擇在停用 Audit Manager 時刪除資料，則必須等到資料刪除後才能重新啟用服務。視您擁有的資料量而定，最多可能需要七天的時間。但是，在此之前，您可隨時嘗試重新啟用 Audit Manager。在多數情況下，資料會在短短一小時內刪除。
> - 如果您在停用 Audit Manager 時選擇不刪除資料，則您現有的評估會進入休眠狀態，並因此停止收集證據。如需重新開始收集既有評估的證據，請編輯評估並選擇儲存，而不進行任何變更。

評估設定

使用此標籤可檢閱和更新您的評估設定。

主題

- 預設稽核擁有者 (選用)
- 評估報告目的地 (選用)
- 通知 (選用)

預設稽核擁有者 (選用)

您可以在 Audit Manager 中指定擁有評估的主要存取權限的預設稽核擁有者。

您可以使用 Audit Manager 主控台、AWS Command Line Interface (AWS CLI) 或 Audit Manager API 來更新此設定。

Audit Manager console

您可以選擇表格中列出的 AWS 帳戶，或使用搜尋列尋找其他 AWS 帳戶。

更新您的預設稽核擁有者設定 (主控台)

1. 從評估設定索引標籤，前往預設稽核擁有者區段，然後選擇編輯。
2. 如需新增預設稽核擁有者，請選擇稽核擁有者下方帳戶名稱旁的核取方塊。
3. 如需移除預設稽核擁有者，請清除稽核擁有者下方帳戶名稱旁的核取方塊。
4. 完成後，選擇儲存。

AWS CLI

如需更新您的預設稽核擁有者設定 (AWS CLI)

執行 update-settings 命令，並使用 `--default-process-owners` 參數來指定稽核擁有者。

在下列範例中，將######取代為您自己的資訊。請注意，`roleType` 只能是 `PROCESS_OWNER`.

```
aws auditmanager update-settings --default-process-owners
 roleType=PROCESS_OWNER,roleArn=arn:aws:iam::111122223333:role/Administrator
```

Audit Manager API

如需更新您的預設稽核擁有者設定 (API)

呼叫 UpdateSettings 操作，並使用 defaultProcessOwners 參數來指定預設稽核擁有者。請注意，`roleType` 只能是 `PROCESS_OWNER`.

如需稽核擁有者的詳細資訊，請參閱本指南概念與術語區段中的稽核擁有者。

評估報告目的地 (選用)

當您產生評估報告時，Audit Manager 會將報告發佈到您選擇的 S3 儲存貯體。此 S3 儲存貯體稱為評估報告目的地。您可以選擇 Audit Manager 儲存評估報告的 Amazon S3 儲存貯體。

您可以使用 Audit Manager 主控台、AWS Command Line Interface (AWS CLI) 或 Audit Manager API 來更新此設定。

Audit Manager console

更新評估報告目的地設定 (主控台)

1. 從評估設定索引標籤，前往評估報告目的地區段。
2. 如需使用現有的 Amazon S3 儲存貯體，請從下拉式選單選擇儲存貯體名稱。
3. 如需建立新的 Amazon S3 儲存貯體，請選擇建立新的儲存貯體。
4. 完成後，選擇儲存。

AWS CLI

如需更新您的評估報告目的地設定 (AWS CLI)

執行 update-settings 命令，並使用 `--default-assessment-reports-destination` 參數來指定 S3 儲存貯體。

在下列範例中，將######取代為您自己的資訊。

```
aws auditmanager update-settings --default-assessment-reports-destination
 destinationType=S3,destination=s3://doc-example-destination-bucket
```

Audit Manager API

如需更新您的評估報告目的地設定 (API)

呼叫 UpdateSettings 操作，並使用 defaultAssessmentReportsDestination 參數來指定 S3 儲存貯體。

如需有關建立 S3 儲存貯體的說明，請參閱 Amazon S3 使用者指南中的建立儲存貯體。

評估報告目的地的組態提示

為確保成功產生評估報告，建議您驗證評估報告目的地的下列組態。

相同區域儲存貯體

我們建議您使用與您的評估處於相同 AWS 區域 的 S3 儲存貯體。當您使用相同區域儲存貯體和評估時，您的評估報告最多可包含 22,000 個證據項目。相反地，當您使用跨區域儲存貯體和評估時，只能包含 3,500 個證據項目。

AWS 區域

您的客戶受管金鑰 AWS 區域 (如有提供) 必須與您評估和評估報告目的地 S3 儲存貯體所處區域相符。關於變更 KMS 金鑰的指南，請參閱 AWS Audit Manager 設定、資料加密。關於變更 S3 儲存貯體的指南，請參閱AWS Audit Manager設定、評估報告目的地。如需支援的 Audit Manager 區域清單，請參閱 Amazon Web Services 一般參考中的 AWS Audit Manager 端點和配額。

S3 儲存貯體加密

如果您的評估報告目的地具有需要進行 SSE-KMS 伺服器端加密 (SSE) 的儲存貯體政策，則該儲存貯體政策中使用的 KMS 金鑰必須與您在 Audit Manager 資料加密設定中設定的 KMS 金鑰相符。如果您未在 Audit Manager 設定中設定 KMS 金鑰，且您的評估報告目的地儲存貯體政策需要 SSE，請確定儲存貯體政策允許 SSE-S3。如需有關如何設定用於資料加密的 KMS 金鑰的說明，請參閱資料加密設定。

跨帳戶 S3 儲存貯體

Audit Manager 主控台不支援將跨帳戶 S3 儲存貯體用作評估報告目的地。您可以使用 AWS CLI 或其中一個 AWS SDK 將跨帳戶儲存貯體指定為評估報告目的地，但出於簡潔性考慮，我們建議您不要這麼做。如果您選擇將跨帳戶 S3 儲存貯體用作評估報告目的地，請考慮以下幾點。

- 根據預設，S3 物件 (例如評估報告) 由上傳物件的 AWS 帳戶 擁有。您可以使用 S3 物件擁有權設定更改該預設行為，以便由具有 `bucket-owner-full-control` 標準存取控制清單 (ACL) 的帳戶寫入的任何新物件自動為儲存貯體擁有者所有。

  我們雖不要求，但建議您對跨帳戶儲存貯體設定進行下列變更。進行這些變更可確保儲存貯體擁有者完全控制您發佈至其儲存貯體的評估報告。

  - 將 S3 儲存貯體的物件擁有權設定為首選儲存貯體擁有者，而非預設物件寫入器
  - 新增儲存貯體政策以確保上傳至該儲存貯體的物件具有 `bucket-owner-full-control` ACL
- 如需允許 Audit Manager 在跨帳戶 S3 儲存貯體中發佈報告，您必須將下列 S3 儲存貯體政策新增至評估報告目的地。以您自己的資訊取代`######`。此政策中的 `Principal` 元素是擁有評估並建立評估報告的使用者或角色。`Resource` 指定發佈報告的跨帳戶 S3 儲存貯體。

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Sid": "Allow cross account assessment report publishing",
          "Effect": "Allow",
          "Principal": {
              "AWS":
 "arn:aws:iam::AssessmentOwnerAccountId:user/AssessmentOwnerUserName"
          },
          "Action": [
              "s3:ListBucket",
              "s3:PutObject",
              "s3:GetObject",
              "s3:GetBucketLocation",
              "s3:PutObjectAcl",
              "s3:DeleteObject"
          ],
          "Resource": [
              "arn:aws:s3:::CROSS-ACCOUNT-BUCKET",
              "arn:aws:s3:::CROSS-ACCOUNT-BUCKET/*"
          ]
      }
  ]
}
```

通知 (選用)

Audit Manager 可以將通知傳送至您在此設定中指定的 Amazon SNS 主題。如果您已訂閱該 SNS 主題，則當您登入 Audit Manager 時會收到通知。

您可以使用 Audit Manager 主控台、AWS Command Line Interface (AWS CLI) 或 Audit Manager API 來更新此設定。

Audit Manager console

更新通知設定 (主控台)

1. 從評估設定索引標籤，前往通知區段。
2. 如需使用現有的 SNS 主題，請從下拉式選單選擇主題名稱。

3. 如需建立新的 SNS 主題，請選擇新清單。
4. 完成後，選擇儲存。

AWS CLI

如需更新通知設定 (AWS CLI)

執行 update-settings 命令，並使用 `--sns-topic` 參數來指定 S3 主題。

在下列範例中，將######取代為您自己的資訊。

```
aws auditmanager update-settings --sns-topic arn:aws:sns:us-east-1:111122223333:my-assessment-topic
```

Audit Manager API

如需更新通知設定 (API)

呼叫 UpdateSettings 操作，並使用 snsTopic 參數來指定 SNS 主題。

> **Note**
>
> 您可以使用標準 SNS 主題或先進先出 (FIFO) SNS 主題。雖然 Audit Manager 支援傳送通知至 FIFO 主題，但無法保證郵件的傳送順序。
> 如果您想要使用非您擁有的 Amazon SNS 主題，請為此設定您的 AWS Identity and Access Management (IAM) 政策。具體而言，您必須將其設定為允許從 Amazon Resource Name (ARN) 發佈至主題。如需有關 IAM 的詳細資訊，請參閱AWS Audit Manager 身分與存取管理。

如需深入了解在 Audit Manager 中調用通知的動作清單，請參閱 AWS Audit Manager 中的通知。

如需有關如何建立 Amazon SNS 主題的資訊，請參閱 Amazon SNS 使用者指南中的建立 Amazon SNS 主題。

證據搜尋工具設定

使用此索引標籤可檢閱和更新您的證據搜尋工具設定。

主題

證據搜尋工具 (選用)

我們強烈建議您啟用證據搜尋工具。如果您要對證據執行搜尋查詢，則必須啟用此功能。

請按照以下步驟啟用、停用或檢查證據搜尋工具的狀態。

啟用證據搜尋工具

您必須在每個需要搜索證據的 AWS 區域 啟用證據搜尋工具。如果您屬於 Audit Manager 委派管理員，您可以對組織中的所有成員帳戶啟用證據搜尋工具，以搜尋證據。

啟用證據搜尋工具所需的許可

如需啟用證據搜尋工具，您需要獲得 CloudTrail Lake 中建立和管理事件資料存放區的許可。如需使用此功能，您需要獲得執行 CloudTrail Lake 查詢的許可。如需您可以使用的許可政策的範例，請參閱授予管理員完整存取權。

如需權限方面的協助，請聯絡您的 AWS 管理員。如果您是 AWS 系統管理員，則可以複製所需的權限聲明，並將其附加到 IAM 政策。

請求啟用證據搜尋工具

您可以使用 Audit Manager 主控台、AWS Command Line Interface (AWS CLI) 或 Audit Manager API 來完成此任務。

Audit Manager console

如需請求啟用證據搜尋工具 (控制台)

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 從證據搜尋工具設定索引標籤，前往證據搜尋工具區段。
3. 選擇 必要的許可政策，然後選擇檢視 CloudTrail Lake 許可以檢視必要的證據搜尋工具許可。如果您尚未獲得這些許可，您可以複製此政策聲明並將其附加到 IAM 政策。

4. 選擇 啟用 。
5. 在快顯視窗中，選擇請求啟用。

AWS CLI

請求啟用證據搜尋工具 (AWS CLI)

使用 `--evidence-finder-enabled` 參數執行 update-settings命令。

```
aws auditmanager update-settings --evidence-finder-enabled
```

Audit Manager API

請求啟用證據搜尋工具 (API)

呼叫 UpdateSettings 操作，並使用 evidenceFinderEnabled 參數。

如需詳細資訊，請選擇先前的連結以閱讀 Audit Manager API 參考中的更多資訊。這包括有關如何在其中一項特定語言 AWS 軟體開發套件中使用此操作和參數的資訊。

確認證據搜尋工具的狀態

提交請求後，啟用證據搜尋工具和建立事件資料存放區最多需要 10 分鐘。建立事件資料存放區後，所有新證據都會擷取至事件資料存放區。

啟用證據搜尋工具並建立事件資料存放區後，我們還會使用您過去兩年內的證據回填新建立的事件資料存放區。此程序會自動執行，最多持續 7 天。

您可以使用 Audit Manager 主控台、AWS CLI、或 Audit Manager API 來檢查證據搜尋工具的目前狀態。

Audit Manager console

如需檢視證據搜尋工具的目前狀態 (主控台)

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在左側的導覽窗格中，選擇設定。
3. 在 啟用證據搜尋工具 — 選用項下，檢閱目前的狀態。

每個狀態的定義如下：

- 未啟用證據搜尋工具 — 您尚未成功啟用證據搜尋工具。
- 您已請求啟用證據搜尋工具 — 您的請求需待事件資料存放區建立方可通過。
- 已啟用證據搜尋工具 — 已建立事件資料存放區。您現在可以使用證據搜尋工具。

  根據您擁有的證據量，使用您過去的證據資料回填新的事件資料存放區最多需要七天時間。藍色資訊窗格表示資料回填正在進行中。在此期間，隨時開始探索證據搜尋工具。但是，請記住，在回填完成之前，部分資料不可用。
- 您已請求停用證據搜尋工具 — 您的請求需待事件資料存放區刪除方可通過。
- 證據搜尋工具已停用 — 證據搜尋工具已永久停用，並刪除事件資料存放區。

AWS CLI

如需檢視證據搜尋工具的目前狀態 (AWS CLI)

執行 get-settings 命令，`--attribute` 參數設置為 `EVIDENCE_FINDER_ENABLEMENT`。

```
aws auditmanager get-settings --attribute EVIDENCE_FINDER_ENABLEMENT
```

其會傳回下列資訊。

enablementStatus

此屬性顯示證據搜尋工具的目前狀態。

- `ENABLE_IN_PROGRESS` — 您請求啟用證據搜尋工具。目前正在建立事件資料存放區以支援證據搜尋工具的查詢。
- `ENABLED` — 已建立事件資料存放區，並啟用證據搜尋工具。我們建議您等待七天，直到事件資料存放區回填您過去的證據資料。您可以在此期間使用證據搜尋工具，但在回填完成之前，部分資料不可用。
- `DISABLE_IN_PROGRESS` — 您請求停用證據搜尋工具，並且您的請求需待事件資料存放區刪除方可通過。
- `DISABLED` — 您永久停用證據搜尋工具，並刪除事件資料存放區。在此之後，您將無法重新啟用證據搜尋工具。

backfillStatus

此屬性顯示證據資料回填的目前狀態。

- NOT_STARTED — 回填尚未開始。
- IN_PROGRESS — 回填正在進行中。最多需要七天的時間完成，具體取決於證據資料的數量。
- COMPLETED — 回填已完成。現在，您可以查詢既往所有證據。

Audit Manager API

如需檢視證據搜尋工具的目前狀態 (API)

呼叫 GetSettings 操作，attribute 參數設定為 EVIDENCE_FINDER_ENABLEMENT。其會傳回下列資訊。

enablementStatus

此屬性顯示證據搜尋工具的目前狀態。

- ENABLE_IN_PROGRESS — 您請求啟用證據搜尋工具。目前正在建立事件資料存放區以支援證據搜尋工具的查詢。
- ENABLED — 已建立事件資料存放區，並已啟用證據搜尋工具。我們建議您等待七天，直到事件資料存放區回填您過去的證據資料。您可以在此期間使用證據搜尋工具，但在回填完成之前，部分資料不可用。
- DISABLE_IN_PROGRESS — 您已請求停用證據搜尋工具 — 您的請求需待事件資料存放區刪除方可通過。
- DISABLED — 您永久停用證據搜尋工具，並刪除事件資料存放區。在此之後，您將無法重新啟用證據搜尋工具。

backfillStatus

此屬性顯示證據資料回填的目前狀態。

- NOT_STARTED 意味著回填尚未開始。
- IN_PROGRESS 表示回填正在進行中。最多需要七天的時間完成，具體取決於證據資料的數量。
- COMPLETED 表示回填已完成。現在，您可以查詢既往所有證據。

如需詳細資訊，請參閱 Audit Manager API 參考中的evidenceFinderEnablement。

停用證據搜尋工具

如果您不想再使用證據搜尋工具，您可以隨時停用此功能。

> **Warning**
>
> 停用證據搜尋工具會刪除 Audit Manager 建立的 CloudTrail Lake 事件資料存放區。因此，您無法重新啟用該功能。如需在停用證據搜尋工具後重新使用證據搜尋工具，您必須停用 AWS Audit Manager，然後完全重新啟用該服務。

停用證據搜尋工具所需的許可

如需停用證據搜尋工具，您需要獲得 CloudTrail Lake 中刪除事件資料存放區的許可。如需您可以使用的範例政策，請參閱停用證據搜尋工具的許可。

如需權限方面的協助，請聯絡您的 AWS 管理員。如果您是 AWS 管理員，則可以將所需的許可聲明附加到 IAM 政策。

停用證據搜尋工具

您可以使用 Audit Manager 主控台、AWS Command Line Interface (AWS CLI) 或 Audit Manager API 來完成此任務。

Audit Manager console

如需停用證據搜尋工具 (控制台)

1. 在 Audit Manager 設定頁面的證據搜尋工具區段中，選擇停用。
2. 在出現的快顯視窗中，輸入 **Yes** 確認您的決定。
3. 選擇請求停用。

AWS CLI

如需停用證據搜尋工具 (AWS CLI)

使用 `--no-evidence-finder-enabled` 參數執行 update-settings命令。

```
aws auditmanager update-settings --no-evidence-finder-enabled
```

Audit Manager API

如需停用證據搜尋工具 (API)

呼叫 UpdateSettings 操作，並使用 evidenceFinderEnabled 參數。

如需詳細資訊，請選擇先前的連結以閱讀 Audit Manager API 參考中的更多資訊。這包括有關如何在其中一項特定語言 AWS 軟體開發套件中使用此操作和參數的資訊。

匯出目的地 (選用)

在證據搜尋工具中執行查詢時，您可以將搜尋結果匯出為逗號分隔值 (CSV) 檔案。使用此設定可選擇 Audit Manager 儲存匯出檔案的預設 S3 儲存貯體。

您可以使用 Audit Manager 主控台、AWS Command Line Interface (AWS CLI) 或 Audit Manager API 來更新此設定。

> **Important**
>
> 您的 S3 儲存貯體必須擁有必要的許可政策，以允許 CloudTrail 將匯出檔案寫入該儲存貯體。具體而言，儲存貯體政策必須包含 `s3:PutObject` 動作和儲存貯體 ARN，並將 CloudTrail 列為服務主體。我們提供您可以使用的範例權限策略。關於如何將此政策附加到 S3 儲存貯體的指南，請參閱使用 Amazon S3 主控台新增儲存貯體政策。
> 如需更多提示，請參閱匯出目的地的組態提示。

Audit Manager console

更新匯出目的地設定 (主控台)

1. 從證據搜尋工具設定索引標籤，前往匯出目的地區段。
2. 請選擇下列其中一個選項：
   - 如需移除目前的 S3 儲存貯體，請選擇移除清除您的設定。
   - 請繼續執行步驟 3，進行預設 S3 儲存貯體的首次儲存。
3. 指定您要儲存匯出檔案的 S3 儲存貯體。
   - 選擇瀏覽 S3，從儲存貯體清單中進行選擇。
   - 或者，您也可以使用以下格式輸入儲存貯體 URI：**`s3://bucketname/prefix`**

> **Tip**
>
> 為確保目的地儲存貯體有序組織，您可以為 CSV 匯出建立選用資料夾。若要這麼做，請在資源 URI 方塊中的值加上斜線 (**/**) 和字首 (例如，**/evidenceFinderCSVExports**)。然後，Audit Manager 會在將 CSV 檔案新增至儲存貯體時包含此字首，而 Amazon S3 會產生字首指定的路徑。如需在 Amazon S3 中首碼的詳細資訊，請參閱在Amazon 簡易儲存服務使用者指南中的在 Amazon S3 主控台編組物件。

4. 完成後，選擇儲存。

如需有關建立 S3 儲存貯體的說明，請參閱 Amazon S3 使用者指南中的建立儲存貯體。

AWS CLI

更新匯出目的地設定 (AWS CLI)

執行 update-settings 命令，並使用 `--default-export-destination` 參數來指定 S3 儲存貯體。

在下列範例中，將######取代為您自己的資訊。

```
aws auditmanager update-settings --default-export-destination
 destinationType=S3,destination=s3://doc-example-destination-bucket
```

如需有關如何建立 S3 儲存貯體的說明，請參閱 AWS CLI 命令參考中的 create-bucket。

Audit Manager API

更新匯出目的地設定 (API)

呼叫 UpdateSettings 操作，並使用 defaultExportDestination 參數來指定 S3 儲存貯體。

如需有關如何建立 S3 儲存貯體的說明，請參閱 Amazon S3 API參考中的 CreateBucket。

匯出目的地的組態提示。

為確保檔案成功匯出，建議您驗證匯出目的地的下列組態。

AWS 區域

您的客戶受管金鑰 AWS 區域 (如有提供) 必須與您評估所處區域相符。關於如何變更 KMS 金鑰的說明，請參閱 Audit Manager 資料加密設定。

跨帳戶 S3 儲存貯體

Audit Manager 主控台不支援將跨帳戶 S3 儲存貯體用作匯出目的地。您可以使用 AWS CLI 或其中一個 AWS SDK 指定跨帳戶儲存貯體，但出於簡潔性考慮，我們建議您不要這麼做。如果您選擇將跨帳戶 S3 儲存貯體用作匯出目的地，請考慮以下幾點。

- 根據預設，S3 物件 (例如 CSV 匯出) 由上傳物件的 AWS 帳戶 擁有。您可以使用 S3 物件擁有權設定更改該預設行為，以便由具有 `bucket-owner-full-control` 標準存取控制清單 (ACL) 的帳戶寫入的任何新物件自動為儲存貯體擁有者所有。

  我們雖不要求，但建議您對跨帳戶儲存貯體設定進行下列變更。進行這些變更可確保儲存貯體擁有者完全控制您發佈至其儲存貯體的匯出檔案。

  - 將 S3 儲存貯體的物件擁有權設定為首選儲存貯體擁有者，而非預設物件寫入器
  - 新增儲存貯體政策以確保上傳至該儲存貯體的物件具有 `bucket-owner-full-control` ACL
- 如需允許 Audit Manager 將檔案匯出至跨帳戶 S3 儲存貯體，您必須將下列 S3 儲存貯體政策新增至匯出目的地儲存貯體。以您自己的資訊取代`######`。此政策中的 `Principal` 元素是擁有評估和匯出檔案的使用者或角色。`Resource` 指定匯出檔案的跨帳戶 S3 儲存貯體。

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Sid": "Allow cross account file exports",
          "Effect": "Allow",
          "Principal": {
              "AWS":
 "arn:aws:iam::AssessmentOwnerAccountId:user/AssessmentOwnerUserName"
          },
          "Action": [
              "s3:ListBucket",
              "s3:PutObject",
              "s3:GetObject",
              "s3:GetBucketLocation",
              "s3:PutObjectAcl",
              "s3:DeleteObject"
          ],
          "Resource": [
```

```
            "arn:aws:s3:::CROSS-ACCOUNT-BUCKET",
            "arn:aws:s3:::CROSS-ACCOUNT-BUCKET/*"
        ]
    }
  ]
}
```

AWS Audit Manager 中的通知

AWS Audit Manager 可以透過 Amazon Simple Notification Service (Amazon SNS)通知您有關使用者動作的資訊。

發生下列其中一個動作時，Audit Manager 會傳送通知：

- 稽核擁有者委派控制集以供檢閱
- 委派人員將已檢閱的控制集交回稽核擁有者。
- 稽核擁有者完成控制集的檢閱。

先決條件

在 Audit Manager 中設定 Amazon SNS 通知前，請確定您已完成下列步驟。

1. 如果您沒有主題，請在 Amazon SNS 中建立一個主題。如需說明，請參閱 Amazon Simple Notification Service 開發人員指南中的建立 Amazon SNS 主題。
2. 需至少訂閱一個端點至該主題。例如，如果您想要透過文字訊息接收通知，請訂閱 SMS 端點至主題。SMS 端點是行動電話號碼。要透過電子郵件接收通知，請訂閱電子郵件端點至該主題。電子郵件端點是電子郵件地址。

   如需詳細資訊，請參閱 Amazon Simple Notification Service 開發人員指南中的入門。
3. (選用) 如果您的主題使用 AWS Key Management Service (AWS KMS) 進行伺服器端加密 (SSE)，您必須將許可新增至 AWS KMS key 政策。如需可使用的範例政策，請參閱附加至 SNS 主題之 KMS 金鑰的許可。

在 AWS Audit Manager 中設定通知

請依照下列步驟設定 AWS Audit Manager 中的通知。

如需在 AWS Audit Manager 中設定通知

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 在左側的導覽窗格中，選擇設定。
3. 在通知 — 選用下方，指定您想要用來接收通知的 SNS 主題。

- 如需使用現有的主題，請從下拉式選單中選擇主題名稱。
- 如需建立新主題，請選擇建立新主題。這會帶您前往 Amazon SNS 主控台，您可以在其中建立主題。

4. 完成後，選擇儲存。

> **備註**
>
> - 您可以使用標準 SNS 主題或先進先出 (FIFO) SNS 主題。Audit Manager 支援將通知傳送至 FIFO 主題。但是，不能保證郵件的傳送順序。
> - 如果您想要使用非您擁有的 Amazon SNS 主題，您必須設定您的 AWS Identity and Access Management (IAM) 政策。具體而言，您必須將您的政策設定為允許從 Amazon Resource Name (ARN) 發佈至主題。如需詳細資訊，請參閱適用於 AWS Audit Manager 的身分與存取管理。

疑難排解

如需尋找常見問題的解答，請參閱本指南疑難排解中的疑難排解通知問題。

在 AWS Audit Manager 中進行疑難排解

您可使用以下資訊針對使用 AWS Audit Manager 時可能遇到的錯誤問題進行故障診斷。

若您發生的問題屬於以下資訊之外，或是在您嘗試解決後問題仍持續發生，請聯絡 AWS Support。

主題

疑難排解評估和證據收集問題

請參考此頁面提供的資訊來解決 Audit Manager 中的常見評估和證據收集問題。

主題

- 我先停用再重新啟用 Audit Manager，導致我既有的評估不再進行收集證據

我建立了一個評估，但還看不到任何證據

如果您看不到任何證據，可能是您在建立評估後尚未等待至少 24 小時，或是發生設定錯誤。

我們建議您檢查以下內容：

1. 確認自建立評估以來已過 24 小時。建立評估 24 小時後，即可使用自動證據。
2. 請確定您使用的 Audit Manager 與您預期看到的證據的 AWS 服務 位於同一個 AWS 區域 中。
3. 如果您希望看到 AWS Config 和 AWS Security Hub 的合規檢查證據，請確保 AWS Config 和 Security Hub 主控台都顯示這些檢查的結果。AWS Config 與 Security Hub 結果應顯示在 所使用 Audit Manager 的同一 AWS 區域 中。

如果您仍然無法在評估中看到證據，並且不是由於上述任一問題所造成，請查看此頁面描述的其他潛在原因。

我的評估并未從 AWS Security Hub 中收集合規檢查證據

如果您沒有看到 AWS Security Hub 控制項的合規檢查證據，可能是由於下列其中一個問題所致。

AWS Security Hub 中缺少配置

如果您在啟用 AWS Security Hub 時遺漏了某些設定步驟，可能會導致此問題。

請確定您已啟用 Security Hub，並依照下列方式設定您的設定。

確認您的 Security Hub 設定適用於單一 AWS 帳戶

如果您使用單一 AWS 帳戶，請檢查下列項目：

- 確認您已啟用 AWS Config 並設定帳戶的資源記錄。
- 確認您已為您的帳戶啟用 PCI DSS 安全標準。
- 確認您已開啟 Security Hub 中的合併控制項調查結果設定。

確認您的 Security Hub 設定適用於組織

如果您使用 Organizations，請檢查下列項目：

- 確認您已啟用 AWS Config 並設定組織的資源記錄。
- 確認您已為組織的每個成員帳戶啟用 PCI DSS 安全標準。
- 確認您已開啟 Security Hub 中的合併控制項調查結果設定。
- 確認您在 Security Hub 中使用的委派管理員帳戶與您在 Audit Manager 中使用的帳戶相同。
- 確認您已將組織帳戶啟用為 Security Hub 成員帳戶。

您的 **`ControlMappingSource`** 中的一個 Security Hub 控制項名稱輸入不正確

當您使用 Audit Manager API 建立自訂控制項時，您可以指定 Security Hub 控制項做為證據收集的資料來源映射項目。若要執行此操作，請輸入控制 ID 做為 `keywordValue`。

如果您沒有看到 Security Hub 控制項的合規檢查證據，可能是因為 `keywordValue` 在您的 `ControlMappingSource` 中輸入不正確。`keywordValue` 會區分大小寫。如果輸入不正確，Audit Manager 可能無法辨識該規則。因此，您可能無法如預期收集該控制項的合規檢查證據。

若要修正此問題，請更新自訂控制項並修訂`keywordValue`. Security Hub 關鍵字的正確格式各不相同。如需準確性，請參考支援的 Security Hub 控制關鍵字清單。

`AuditManagerSecurityHubFindingsReceiver` Amazon EventBridge 規則遺失

當您啟用 Audit Manager 時，系統會在 Amazon EventBridge 中自動建立並啟用名為 `AuditManagerSecurityHubFindingsReceiver` 的規則。此規則可讓 Audit Manager 收集 Security Hub 調查結果作為證據。

如果您使用 Security Hub 的 AWS 區域 中未列出並啟用此規則，則 Audit Manager 無法為該區域收集 Security Hub 的調查結果。

若要解決此問題，請移至 EventBridge 主控台，並確認您的 AWS 帳戶 中是否存在 `AuditManagerSecurityHubFindingsReceiver` 規則。如果規則不存在，建議您停用 Audit Manager，然後重新啟用服務。如果此動作無法解決問題，或停用 Audit Manager 不是可選選項，請聯絡 AWS Support 尋求協助。

由 Security Hub 建立的服務連結 AWS Config 規則

請記住，Audit Manager 不會從 Security Hub 建立的服務連結 AWS Config 規則中收集證據。這是一種由 Security Hub 服務啟用和控制的特定受管 AWS Config 規則類型。即使已存在相同規則的其他執行個體，Security Hub 仍會在您的 AWS 環境中建立這些服務連結規則。因此，為防止證據重複，Audit Manager 不支援從服務連結規則收集證據。

我的評估并未從 AWS Config 中收集合規檢查證據

如果您沒有看到針對 AWS Config 規則的合規檢查證據，可能是由於下列其中一個問題所致。

在您的 **`ControlMappingSource`** 中規則識別碼輸入錯誤

當您使用 Audit Manager API 建立自訂控制項時，您可以指定 AWS Config 規則做為證據收集的資料來源映射項目。您指定的 `keywordValue` 取決於規則的類型。

如果您沒有看到針對 AWS Config 規則的合規檢查證據，可能是因為 `keywordValue` 在您的 `ControlMappingSource` 中輸入不正確。`keywordValue` 會區分大小寫。如果輸入不正確，Audit Manager 可能無法辨識規則。因此，您可能無法如預期收集該規則的合規檢查證據。

若要修正此問題，請更新自訂控制項並修訂`keywordValue`.

- 對於自訂規則，請確定 `keywordValue` 具有 `Custom_` 字首，後面接著自訂規則名稱。自訂規則名稱的格式可能會有所差異。為確保正確性，請造訪 AWS Config 控制台以驗證您的自訂規則名稱。
- 對於受管規則，請確定 `keywordValue` 是 `ALL_CAPS_WITH_UNDERSCORES` 中的規則識別碼。例如：`CLOUDWATCH_LOG_GROUP_ENCRYPTED`。如需準確性，請參考支援的受管規則關鍵字清單。

> **Note**
>
> 對於某些受管規則，規則識別碼與規則名稱不同。例如，受限制 ssh 的規則識別碼為 `INCOMING_SSH_DISABLED`。請務必使用規則識別碼，而不是規則名稱。若要尋找規則識別碼，請從受管規則清單中選擇規則，然後找到其識別碼值。

此規則為服務連結 AWS Config 規則

您可以使用受管規則和自訂規則作為證據收集的資料來源映射項目。但是，Audit Manager 不會從大多數服務連結規則中收集證據。

Audit Manager 只會從下列兩種類型收集證據的服務連結規則：

- 一致性套件中的服務連結規則
- AWS Organizations 服務連結規則

Audit Manager 不會從其他服務連結規則收集證據，特別是任何具有Amazon Resource Name (ARN)且包含下列字首的規則：`arn:aws:config:*:*:config-rule/aws-service-rule/...`

Audit Manager 無法從大多數服務連結 AWS Config 規則中收集證據的原因，是為了防止評估中出現重複的證據。服務連結規則是受管規則的一種特殊類型，可支援其他 AWS 服務 以在您的帳戶中建立 AWS Config 規則。例如，某些 Security Hub 控制項會使用 AWS Config 服務連結規則來執行安全檢查。針對每個使用 AWS Config 服務連結規則的 Security Hub 控制項，Security Hub 會在您的 AWS 環境中建立必要的 AWS Config 規則的執行個體。即使您帳戶中已存在原始規則，也會發生這種情況。因此，為避免從同一規則中重複收集相同證據，Audit Manager 會忽略服務連結規則，而不會從中收集證據。

AWS Config 未啟用並作爲服務包含在範圍內

您的 AWS 帳戶 中必須啟用 AWS Config 此外，您還必須將其作為評估範圍內的服務包含在內。以這種方式進行 AWS Config 設定之後，每次執行 AWS Config 規則評估時，Audit Manager 都會收集證據。

首先，請確保您在 AWS 帳戶 中啟用 AWS Config。如需指示，請參閱啟用並設定 AWS Config。

接下來，請確定您已將 AWS Config 作為服務納入評估範圍內。若要檢閱評估範圍內目前的服務，請參閱檢閱評估，AWS 服務 標籤。若要編輯評估範圍內的服務清單，請參閱在範圍內編輯 AWS 服務。

AWS Config 規則在您設定評估之前，已評估一項資源組態

如果您的 AWS Config 規則設定為評估特定資源的組態變更，您可能會看到 AWS Config 中的評估與 Audit Manager 中的證據不相符。如果規則評估發生在您在 Audit Manager 評估中設定控制項之前，就會發生這種情況。在此情況下，直到基礎資源再次變更狀態並觸發規則的重新評估，Audit Manager 才會產生證據。

因應措施是您可以導覽至 AWS Config 主控台中的規則，然後手動重新評估規則。這將調用與該規則相關之所有資源的新評估。

我的評估不會從 AWS CloudTrail 中收集使用者活動證據

當您使用 Audit Manager API 建立自訂控制項時，您可以指定 CloudTrail 事件名稱做為證據收集的資料來源映射項目。若要執行此操作，請將事件名稱輸入為 `keywordValue`。

如果您在 CloudTrail 事件中沒有看到使用者活動證據，可能是因為 `keywordValue` 在您的 `ControlMappingSource` 中輸入不正確。`keywordValue` 會區分大小寫。如果輸入不正確，Audit Manager 可能無法辨識事件名稱。因此，您可能無法依預期收集該事件的使用者活動證據。

若要修正此問題，請更新自訂控制項並修訂keywordValue. 請確保事件寫入為 serviceprefix_ActionName。例如：cloudtrail_StartLogging。如需準確性，請參閱服務授權參考中的 AWS 服務 字首和動作名稱。

我的評估并未收集 AWS API 呼叫的組態資料證據

當您使用 Audit Manager API 建立自訂控制項時，您可以指定 AWS API 呼叫做為證據收集的資料來源映射項目。若要執行此作業，您可以將 API 呼叫輸入為 keywordValue。

如果您沒有看到針對 AWS API 呼叫的組態資料證據，可能是因為 keywordValue 在您的 ControlMappingSource 中輸入不正確。keywordValue 會區分大小寫。如果輸入不正確，Audit Manager 可能無法辨識 API 呼叫。因此，您可能無法按預期收集該 API 呼叫的組態資料證據。

若要修正此問題，請更新自訂控制項並修訂keywordValue. 請確保 API 呼叫寫入為 serviceprefix_ActionName。例如：iam_ListGroups。為確保準確性，請參考支援的 API 呼叫清單。

我的評估并未從另一個 AWS 服務 中收集合規檢查證據

如果您的評估範圍并未選取 AWS 服務，則 Audit Manager 不會從與該服務相關的資源收集證據。如果已選取 AWS 服務，但您尚未在環境中啟用它，也會發生同樣情況。

如果您是從自訂架構建立評估，則可以編輯評估範圍內的服務。接著，指定希望從中收集證據的其他 AWS 服務。新增這些服務後，24 小時後即可取得證據。

> **Note**
>
> 如果您是從標準架構建立評估，範圍內的 AWS 服務 清單將是預先選取的並且無法編輯。這是因為當您從標準架構建立評估時，Audit Manager 會自動為您對應，並選取相關的資料來源和服務。該選擇是根據標準架構的要求所進行。請注意，對於僅包含手動控制項的標準架構，範圍內沒有 AWS 服務。
>
> 在根據標準架構建立評估時，編輯範圍內 AWS 服務 的因應措施是自訂標準架構。透過使用此對策，您可以運用自訂架構來建立新的評估。在此評估中，您可以指定哪些 AWS 服務 被納入範圍。

我的證據是以不同的時間間隔產生的，我不確定它的收集頻率

Audit Manager 評估中的控制項會映射至各種資料來源。每個資料來源都有不同的證據收集頻率。因此，對於收集證據的頻率，沒有一種適合所有情況的標準答案。某些資料來源會評估合規性，而其他資料來源僅擷取資源狀態和變更資料，不涉及合規性判斷。

以下是不同資料來源類型的摘要，以及收集證據的頻率。

Data source type (資料來源類型)	描述	證據收集頻率	此控制項在評估中處於作用中狀態時
AWS CloudTrail	追蹤特定使用者活動。	持續性	Audit Manager 將根據您選擇的關鍵字過濾 CloudTrail 日誌。已處理的日誌檔會匯入為使用者活動證據。
AWS Security Hub	透過 Security Hub 報告調查結果，擷取資源安全狀況的快照。	根據 Security Hub 檢查的排程計劃 (通常約每 12 小時進行一次)	Audit Manager 會直接從 Security Hub 擷取安全性調查結果。調查結果會匯入為合規檢查證據。
AWS Config	透過 AWS Config 報告的調查結果來擷取資源安全狀況的快照。	根據 AWS Config 規則中定義的設定	Audit Manager 會直接從 AWS Config 中擷取規則評估。評估結果會匯入為合規檢查證據。
AWS API 呼叫	透過指定的 AWS 服務 進行 API 呼叫，擷取資源組態的快照。	每日、每週或每月	Audit Manager 會根據您的指定頻率進行 API 呼叫。系統會將回應匯入為組態資料證據。

無論證據收集頻率如何，只要評估處於活動狀態，系統都會自動收集新證據。如需詳細資訊，請參閱證據收集頻率。

若要深入瞭解，請參閱支援自動證據的控制項資料來源和變更控制項的證據收集頻率。

如果我從組織中移除範圍內的帳戶，會發生什麼情況？

當範圍內的帳戶從組織中移除時，Audit Manager 不會再為該帳戶收集證據。但是，該帳戶仍會繼續顯示在您的評估中的 AWS 帳戶 索引標籤下。若要從範圍內的帳戶清單中移除該帳戶，請編輯評估。已移除帳戶在編輯期間不再顯示於清單中，您可以在不包含該帳戶的範圍內儲存您的變更。

我無法編輯評估範圍內的服務

當您使用 Audit Manager 主控台從標準架構建立評估時，範圍內的 AWS 服務 清單會被預設為選取狀態。無法編輯此清單。這是因為 Audit Manager 會自動為您映射並選擇資料來源和服務。此選擇是根據標準架構的要求所進行。如果您選取的標準架構只包含手動控制項，則您的評估範圍內不會包含任何 AWS 服務，並且您無法在評估中新增任何服務。

如果您需要編輯範圍中的服務清單，請使用 Audit Manager 提供的更新評估 API 進行作業。或者，您可以自訂標準架構，然後從自訂架構中建立評估。

範圍內的服務和資料來源類型有什麼不同？

範圍內的服務是被指定為評估一部分的 AWS 服務。當一項服務在範圍內時，Audit Manager 會收集您使用該服務及其資源的相關證據。

資料來源類型會指出從何處收集證據。如果您上傳自己的證據，則資料來源類型為手動。如果由 Audit Manager 收集證據，則資料來源可以是下列四種類型之一：

1. AWS Security Hub — 透過 Security Hub 報告調查結果，擷取資源安全狀況的快照。
2. AWS Config— 透過 AWS Config 報告調查結果來擷取資源安全狀況的快照。
3. AWS CloudTrail— 追蹤資源的特定使用者活動。
4. AWS API 呼叫— 透過向指定的 AWS 服務 進行 API 呼叫，直接擷取資源組態的快照。

這裡有兩個例子來說明範圍內的服務，以及資料來源類型之間的差異。

範例 1

假設您想收集名為 4.1.2 — 禁止對 S3 儲存貯體進行公開寫入存取的控制項證據。此控制項會檢查 S3 儲存貯體政策的存取層級。針對此控制項，Audit Manager 會使用特定的 AWS Config 規則 (s3-bucket-public-write-prohibited) 來尋找 S3 儲存貯體的評估。在此範例中，下列情況成立：

- 範圍內的服務是 Amazon S3
- 正在評估的資源是您的 S3 儲存貯體
- 資料來源類型是 AWS Config。
- 資料來源映射項目是特定 AWS Config 規則(`s3-bucket-public-write-prohibited`)

範例 2

假設您想收集名為 164.308(a)(5)(ii)(C) 的 HIPAA 控制項的證據。此控制項需要監控程序來偵測不適當的登入。對於此控制項，Audit Manager 會使用 CloudTrail 日誌來尋找所有 Amazon Web Services Management Console 登入事件。在此範例中，下列情況成立：

- 範圍內的服務是 IAM
- 正在評估的資源是您的使用者
- 資料來源類型是 CloudTrail
- 資料來源映射項目是特定的 CloudTrail 事件(`ConsoleLogin`)

我的評估建立失敗

如果您的評估建立失敗，可能是因為您在評估範圍中選取了太多 AWS 帳戶。如果您使用的是 AWS Organizations，Audit Manager 在單一評估範圍內最多可以支援 150 個成員帳戶。如果超過此數量，評估建立可能會失敗。因應措施是，您可以進行多次評估，每次評估使用範圍內不同帳戶來執行。

我先停用再重新啟用 Audit Manager，導致我既有的評估不再進行收集證據

當您停用 Audit Manager 並選擇不刪除資料時，您現有的評估會進入休眠狀態，並停止收集證據。這表示當您重新啟用 Audit Manager 時，您先前建立的評估仍可使用。但是，它們不會自動恢復收集證據。

如需重新開始收集既有評估的證據，請編輯評估並選擇儲存，而不進行任何變更。

評估報告問題疑難排解

請參考此頁面提供的資訊來解決 Audit Manager 中常見的評估報告問題。

主題

- 我的評估報告無法產生

我的評估報告無法產生

您的評估報告可能因為多種因素，未能成功產生。您可以透過檢查常見原因來對此問題進行故障排除。請使用下列清單來開始。

1. 檢查您的任何 AWS 區域 資訊是否不相符：
   a. 您客戶的管理金鑰的 AWS 區域 是否與您評估的 AWS 區域 相符？

      如果您為 Audit Manager 資料加密提供了自己的 KMS 金鑰，則該金鑰必須與您的評估 AWS 區域 相同。若要解決此問題，請將 KMS 金鑰變更為與評估位於相同區域的金鑰。關於變更 KMS 金鑰的指南，請參閱 AWS Audit Manager 設定、資料加密。

   b. 您客戶的管理金鑰的 AWS 區域 是否與您 S3 儲存貯體的 AWS 區域 相符？

      如果您為 Audit Manager 資料加密提供了自己的 KMS 金鑰，則該金鑰必須與您用來做為評估報告目標的 S3 儲存貯體位於相同的 AWS 區域。為解決此問題，您可以變更 KMS 金鑰或 S3 儲存貯體，使它們與您的評估位於相同區域。關於變更 KMS 金鑰的指南，請參閱 AWS Audit Manager 設定、資料加密。關於變更 S3 儲存貯體的指南，請參閱 AWS Audit Manager 設定、評估報告目的地。
2. 檢查您用作評估報告目的地的 S3 儲存貯體的權限：
   a. 產生評估報告的 IAM 實體是否具有對 S3 儲存貯體所需的權限？

      IAM 實體必須擁有 S3 儲存貯體的所需權限，才能在該儲存貯體中發佈報表。我們提供您可以使用的範例政策。關於如何指定不同 S3 儲存貯體的指南，請參閱 AWS Audit Manager 設定、評估報告目的地。

   b. S3 儲存貯體是否有需要使用 SSE-KMS 的伺服器端加密 (SSE)的儲存貯體政策？

      如果是，則該儲存貯體原則中使用的 KMS 金鑰必須與 Audit Manager 資料加密設定中指定的 KMS 金鑰相符。如果您未在 Audit Manager 設定中設定 KMS 金鑰，且 S3 儲存貯體政策需要 SSE，請確定儲存貯體政策允許 SSE-S3。關於變更 KMS 金鑰的指南，請參閱 AWS Audit

Manager 設定、資料加密。關於變更 S3 儲存貯體的指南，請參閱 AWS Audit Manager 設定、評估報告目的地。

如果您仍然無法成功產生評估報告，請查看本頁上的下述問題。

我按照上面的檢查清單進行操作，但我的評估報告仍然無法生成

Audit Manager 會限制您可以新增至評估報告的證據數量。此限制取決於您評估的 AWS 區域、用作評估報告目的地的 S3 儲存貯體區域，以及您的評估是否使用了客戶受管的 AWS KMS key。

1. 相同區域報告的上限為 22,000 (S3 儲存貯體和評估都在同一個 AWS 區域 的情況下)
2. 跨區域報告的上限為 3,500 (S3 儲存貯體和評估在不同 AWS 區域 的情況下)
3. 如果評估使用客戶管理的 KMS 金鑰，則上限為 3,500

如果您嘗試產生包含多於此證據的報告，作業可能會失敗。

因應措施是，您可以產生多個評估報告，而不是一份較大的評估報告。透過這種方式，您可以將評估中的證據匯出到更易於管理的批次中。

當我嘗試生成報告時，出現存取被拒絕的錯誤

如果您的評估是由委派的系統管理員帳戶建立，並且 Audit Manager 設定中指定的 KMS 金鑰不屬於該帳戶，您將會收到 `access denied` 錯誤訊息。若要避免此錯誤，當您指定 Audit Manager 的委派系統管理員時，請確定委派系統管理員帳戶具有您設定 Audit Manager 時所提供的 KMS 金鑰的存取權限。

如果您沒有用作評估報告目的地的的 S3 儲存貯體的寫入權限，您也可能會收到 `access denied` 錯誤訊息。

若您收到 `access denied` 錯誤訊息，請確定您符合下列要求：

- 您在 Audit Manager 設定中的 KMS 金鑰將權限授予委派系統管理員。您可以依照 AWS Key Management Service 開發人員指南中，允許其他帳戶中的使用者使用 KMS 金鑰中的指南進行設定。關於如何在 Audit Manager 中檢視和變更加密設定的指示，請參閱資料加密。
- 您擁有一個權限策略，該策略可授予您對用作評估報告目的地的 S3 儲存貯體的寫入存取權限。更具體地說，您的許可政策包含一個 `s3:PutObject` 動作、指定 S3 儲存貯體的 ARN，並包含用於加密評估報告的 KMS 金鑰。關於您可以使用的範例策略，請參閱 AWS Audit Manager 的以身分為基礎的策略範例

> **Note**
>
> 如果您變更 Audit Manager 資料加密設定，這些變更會套用至您未來建立的新評估。這包括您依據新評估所建立的任何評估報告。
> 這些變更不會套用至您在變更加密設定之前，已建立的現有評估。出了現有的評估報告之外，這還包括了您根據現有評估建立的新評估報告。現有的評估及其所有評估報告都將繼續使用舊有的 KMS 金鑰。如果產生評估報告的 IAM 身分沒有使用舊有 KMS 金鑰的權限，您可以在金鑰政策層級授予權限。

我無法解壓縮評估報告

如果您無法在 Windows 上解壓縮評估報告，Windows 檔案總管可能無法解壓縮，因為其檔案路徑有數個巢狀資料夾或長名稱。這是因為，在 Windows 檔案命名系統下，資料夾路徑、檔案名稱和副檔名不能超過 259 個字元。否則，會導致 `Destination Path Too Long` 錯誤。

為解決此問題，請嘗試將 zip 檔案移至其目前位置的上層資料夾。然後，您可以再次嘗試從那裡解壓縮它。或者，您也可以嘗試縮短 zip 檔案的名稱，或將其解壓縮到較短文件路徑的其他位置。

當我在報告中選擇證據名稱時，系統沒有將我重導向到該證據的詳細資訊

如果您在瀏覽器中操作評估報告，或使用作業系統上安裝的預設 PDF 閱讀器，可能會發生此問題。某些瀏覽器和系統預設的 PDF 閱讀器不允許開啟相對連結。這表示，雖然在評估報告摘要 PDF 中的超連結可能有效 (例如目錄中的超連結控制項名稱)，但當您嘗試從評估摘要 PDF 導覽至獨立的證據詳細資料 PDF 時，超連結將被忽略。

如果您遇到此問題，建議您使用專用的 PDF 閱讀器來閱覽您的評估報告。為了獲得可靠的使用體驗，我們建議您安裝並使用 Adobe Acrobat Reader，您可以在 Adobe 官網下載該服務。其他 PDF 閱讀器也可以使用，但 Adobe Acrobat Reader 已被證明可以與 Audit Manager 評估報告穩定且可靠地運作。

我的評估報告產生停留進行中狀態，我不確定這對我的計費有何影響

產生評估報告不會影響計費。我們只會根據您的評估收集的證據向您收取費用。如需定價的詳細資訊，請參閱 AWS Audit Manager 定價。

另請參閱

下列頁面提供從證據搜尋工具產生評估報告的疑難排解指南：

- 我無法從搜尋結果中產生多個評估報告

- 我無法將個別搜尋結果新增至評估報告
- 在評估報告中，並未包含所有來自證據搜尋工具查找結果
- 我想從搜尋結果中產生評估報告，但我的查詢陳述式執行失敗

控制項和控制集問題疑難排解

請參考此頁面提供的資訊來解決 Audit Manager 中控制項的常見問題。

一般問題

- 我在評估中看不到任何控制項或控制集
- 我無法將手動證據上傳到控制項

AWS Config 整合問題

- 我需要使用多個 AWS Config 規則作為單一控制項的資料來源
- 當我設定控制項資料來源時，無法使用自訂規則選項
- 自訂規則選項可用，但下拉式清單中沒有顯示任何規則
- 一些自訂規則可用，但我看不到我想要使用的規則
- 我看不到要使用的受管規則
- 我想共享一個自訂架構，但它具有使用自訂 AWS Config 規則作為資料來源的控制項。收件人可以收集這些控制項的證據嗎？
- 在 AWS Config 中更新自訂規則時會發生什麼情況？ 我需要在 Audit Manager 中採取任何動作嗎？

我在評估中看不到任何控制項或控制集

簡而言之，若要檢視評估的控制項，您必須被指定為該評估的稽核擁有者。此外，您還需要必要的 IAM 權限，才能檢視和管理相關 Audit Manager 資源。

如果您需要存取評估中的控制項，請要求該評估的一位稽核擁有者將您指定為稽核擁有者。您可以在建立或編輯評估時指定稽核擁有者。

同樣請確保您具備管理評估的所需權限。我們建議稽核擁有者使用 AWSAuditManagerAdministratorAccess 策略。如果您需要 IAM 權限相關協助，請聯絡您的管理員或 AWS 支援人員。有關如何將政策附加到 IAM 身分的更多資訊，請參閱 IAM 使用者指南中的向使用者新增權限和新增及移除 IAM 身分權限。

我無法將手動證據上傳到控制項

如果您無法手動將證據上傳至控制項，可能是因為控制項處於非作用中狀態。

若要將手動證據上傳至控制項，您必須先將控制項狀態變更為審核中或已審核。如需更多資訊，請參閱更新控制項狀態。

> **Important**
>
> 每個 AWS 帳戶 每天最多只能手動上傳 100 個證據檔案至控制項。超過這個每日配額，會導致該控制項的任何額外手動上傳失敗。如果您需要將大量手動證據上傳至單一控制項，請在數天內分批上傳證據。

我需要使用多個 AWS Config 規則作為單一控制項的資料來源

您可以將受管規則和自訂規則的組合用於單一控制項。為此，請為控制項設定多個資料來源，然後為每個控制項選取偏好的規則類型。您最多可為單一自訂控制項定義 10 個資料來源。

當我設定控制項資料來源時，無法使用自訂規則選項

這表示您沒有檢視您的 AWS 帳戶 或組織的自訂規則的權限。更具體地說，您沒有權限在 Audit Manager 主控台執行 DescribeConfigRules 作業。

若要解決此問題，請聯絡 AWS 管理員以取得協助。如果您就是 AWS 管理員，可以透過管理您的 IAM 政策為使用者或群組提供權限。

自訂規則選項可用，但下拉式清單中沒有顯示任何規則

這表示您的 AWS 帳戶 或組織中沒有啟用和使用任何自訂規則。

如果您在 AWS Config 中還沒有任何自訂規則，則可以建立一個。如需指示，請參閱 AWS Config 開發人員指南中的 AWS Config 自訂規則。

若您預期看到自訂規則，請參閱下述疑難排解項目。

一些自訂規則可用，但我看不到我想要使用的規則

如果您看不到預期查找的自訂規則，可能是下列問題之一所致。

您的帳戶已從規則中排除

您使用的委派系統管理員帳戶可能已從規則中排除。

您組織的管理帳戶 (或其中一個 AWS Config 委派系統管理員帳戶) 可以使用 AWS Command Line Interface (AWS CLI) 建立自訂組織規則。當進行此操作時，他們可以指定要排除的帳戶列表，使這些帳戶不受該規則約束。如果您的帳戶在此清單中，則 Audit Manager 中無法使用該規則。

若要解決此問題，請聯絡 AWS Config 管理員以取得協助。如果您是 AWS Config 系統管理員，您可以執行 put-organization-config-rule 命令來更新排除帳戶的清單。

規則未在 AWS Config 中成功建立和啟用

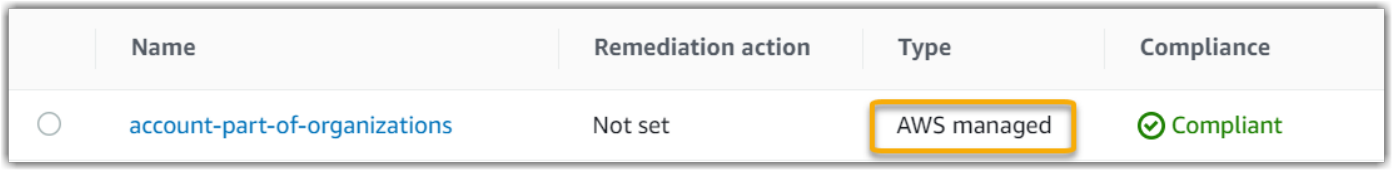
也有可能未成功建立和啟用自訂規則。如果在建立規則時發生錯誤，或未啟用該規則，則該規則不會顯示在 Audit Manager 的可用規則清單中。

如需協助您解決此問題，建議您聯絡 AWS Config 管理員。

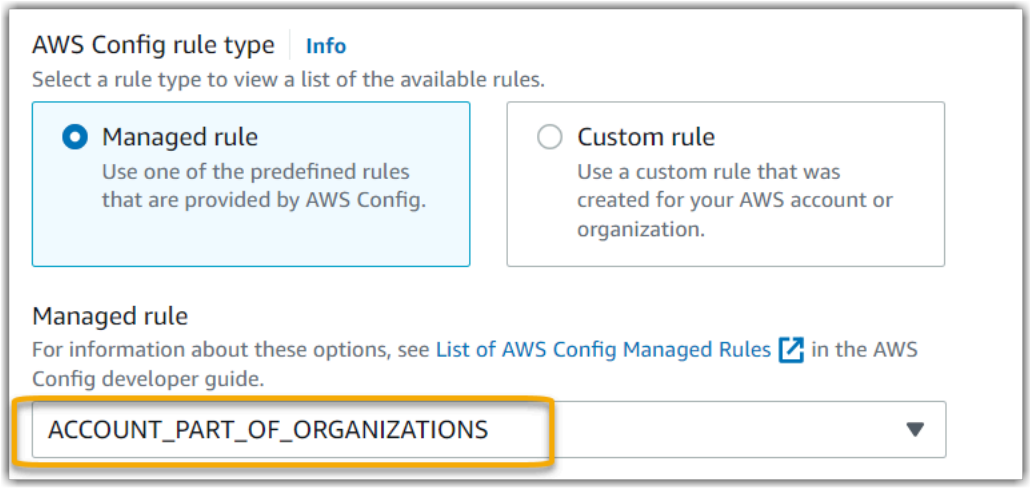
此規則為受管規則

如果您在自訂規則的下拉式清單中找不到您要尋找的規則，則該規則可能是受管規則。

您可以使用 AWS Config 主控台來驗證規則是否為受管規則。若要這麼做，請在左側導覽功能表中選擇規則，然後在表格中查找規則。如果規則是受管規則，類型欄會顯示 AWS 受管。

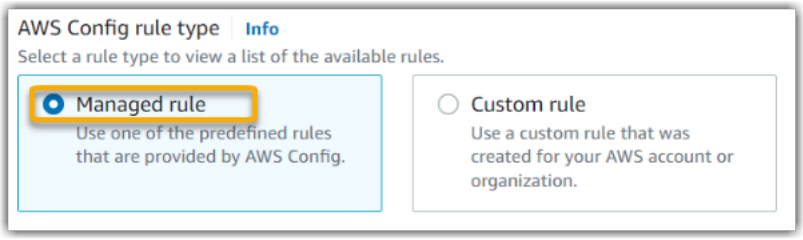


確認它是受管規則之後，請返回 Audit Manager 並選取受管規則作為規則類型。然後，在受管規則的下拉式清單中，尋找受管規則識別碼關鍵字。



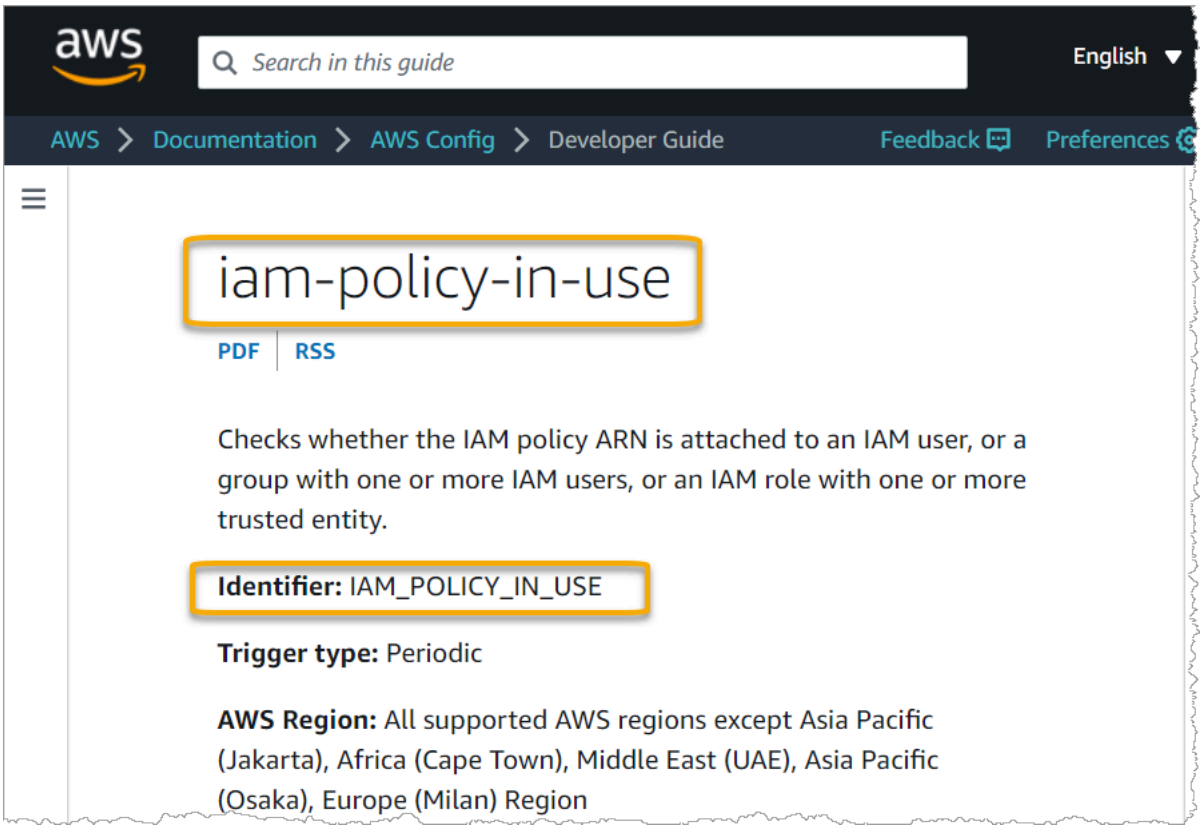
我看不到要使用的受管規則

在您從 Audit Manager 主控台的下拉式清單中選取規則之前，請確定已選取受管規則作為規則類型。

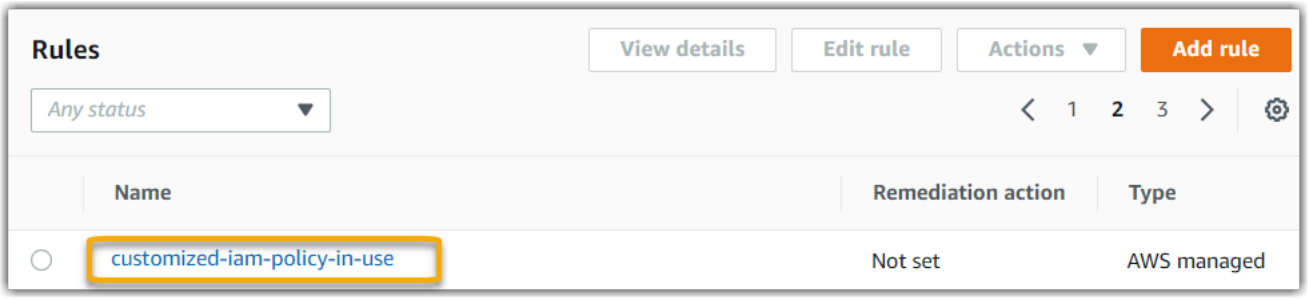


如果您仍然看不到預期尋找的受管規則，可能是您正在尋找規則名稱。相反地，您必須尋找規則識別碼。

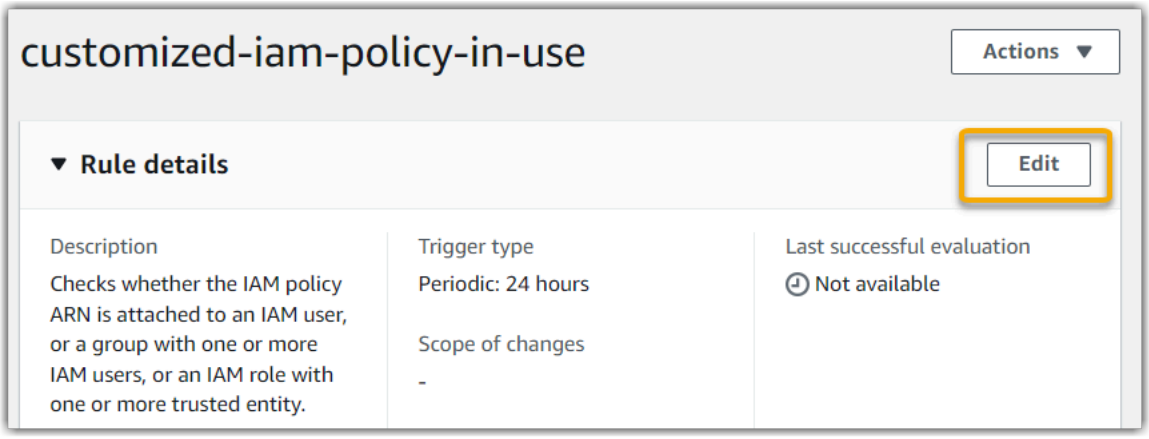
如果您使用的是預設受管規則，其名稱和識別碼會類似。名稱以小寫字母表示，並使用破折號 (例如，`iam-policy-in-use`)。識別碼為大寫，並使用底線 (例如，`IAM_POLICY_IN_USE`)。若要尋找預設受管規則的識別碼，請檢閱支援的 AWS Config 受管規則關鍵字清單，然後點擊您要使用的規則的連結。這會將您跳轉到該受管規則的 AWS Config 文件。從這裡，您可以看到名稱和識別碼。在 Audit Manager 下拉式清單中尋找識別碼關鍵字。



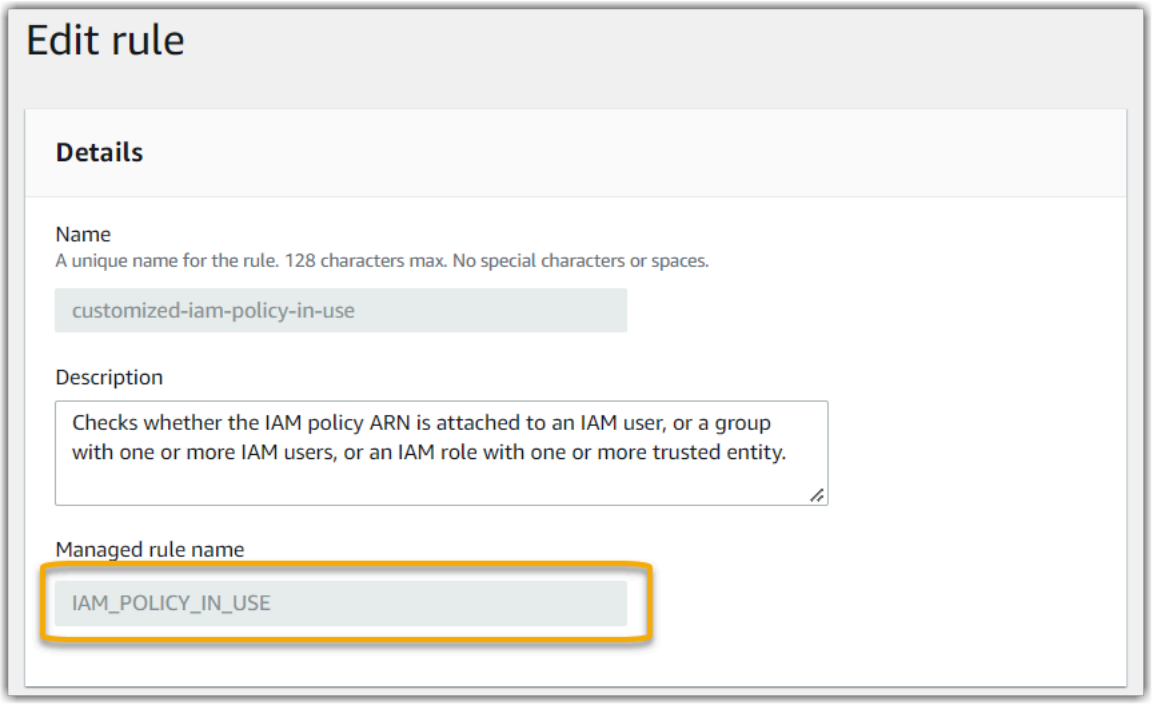
如果您使用自訂的受管規則，可以使用 AWS Config 主控台尋找規則識別碼。舉例來說，假設您想要使用名為 `customized-iam-policy-in-use` 的受管規則。若要尋找此規則的識別碼，請前往 AWS Config 主控台，從左側導覽功能表中選擇規則，然後在表格中選擇該規則。



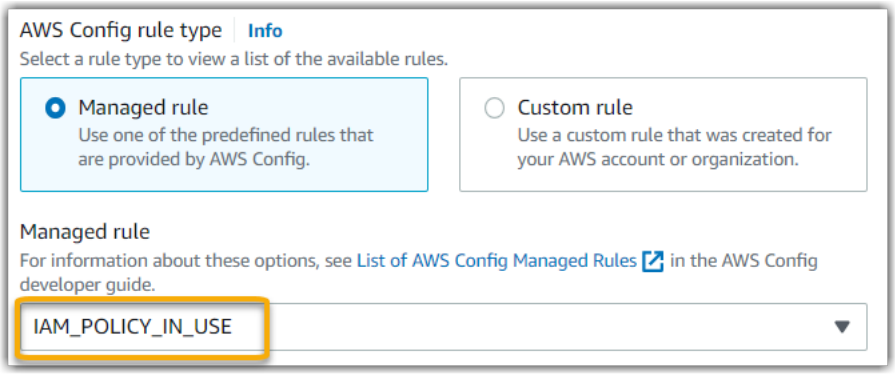
選擇編輯以開啟有關受管規則的詳細資料。



在詳細資訊一節下，您可以找到從 (`IAM_POLICY_IN_USE`) 建立的受管規則的來源識別碼。



您現在可以返回 Audit Manager 主控台，並從下拉式清單中選取相同的識別碼關鍵字。



我想共享一個自訂架構，但它具有使用自訂 AWS Config 規則作為資料來源的控制項。收件人可以收集這些控制項的證據嗎？

是的，收件人可以收集這些控制的證據，但需要幾個步驟來實現這一目標。

若要讓 Audit Manager 使用 AWS Config 規則作為資料來源映射項目來收集證據，必須符合下列條件。同樣適用於受管理規則和自訂規則。

1. 規則必須存在於收件者的 AWS 環境中
2. 必須在收件者的 AWS 環境中啟用規則

請記住，您帳戶中的自訂 AWS Config 規則可能不存在於收件人的 AWS 環境中。此外，當收件者接受共享要求時，Audit Manager 不會在其帳戶中重新建立您的任何自訂規則。若要讓收件者使用您的自訂規則作為資料來源映射項目來收集證據，他們必須在 AWS Config 執行個體中建立相同的自訂規則。收件者建立並啟用規則後，Audit Manager 可以從該資料來源收集證據。

我們建議您與收件者通訊，讓他們知道是否需要在其 AWS Config 執行個體中建立任何自訂規則。

在 AWS Config 中更新自訂規則時會發生什麼情況？ 我需要在 Audit Manager 中採取任何動作嗎？

針對 AWS 環境中的規則更新

如果您更新 AWS 環境中的自訂規則，則無需在 Audit Manager 中執行任何動作。Audit Manager 會依照下表所述偵測和處理規則更新。偵測到規則更新時，Audit Manager 不會另行通知。

案例	Audit Manager 會做什麼	您需要執行的事項
自訂規則會在您的 AWS Config 執行個體中更新。	Audit Manager 會繼續使用更新的規則定義報告該規則的調查結果。	不需採取任何動作。
自訂規則會在您的 AWS Config 執行個體中刪除。	Audit Manager 會停止報告已刪除規則的調查結果。	不需採取任何動作。 如果需要，您可以編輯自訂控制項，使用已刪除規則作為資料來源映射項目。這樣做有助於透過移除已刪除的規則，來清除資料來源設定。否則，刪除的規則名稱會保留為未使用的資料來源映射項目。

適用於 AWS 環境外部的規則更新

如果在您的 AWS 環境之外更新自訂規則，則 Audit Manager 不會偵測規則更新。如果您使用共享的自訂架構，這將是需要考慮的因素。這是因為，在這個方案中，寄件者和收件者各自在不同的 AWS 環境中工作。下表提供適用於此方案的建議作法。

您的角色	案例	建議的動作
Sender	• 您共享使用自訂規則作爲資料來源映射項目的架構。 • 在您共享架構之後，您就更新或刪除了 AWS Config 中的其中一個規則。	通知收件者您的更新。如此一來，他們就可以套用相同的更新，並與最新的規則定義保持同步。
Recipie	• 您接受使用自訂規則做為資料來源映射項目的共享架構。 • 在 AWS Config 執行個體中重新建立自訂規則之後，寄件者就會更新或刪除其中一個規則。	在您自己的 AWS Config 執行個體中進行對應的規則更新。

儀表板問題疑難排解

請參考此頁面提供的資訊來解決 Audit Manager 中常見的儀表板問題。

主題

我的儀表板上沒有任何資料

如果每日快照小工具 中的數字顯示連字號 (-)，表示沒有可用的資料。您必須至少有一個作用中的評估，才能在儀表板中查看資料。若要開始使用，請建立評估。24 小時後，您的評估數據將開始顯示在儀表板中。

> **Note**
>
> 如果每日快照小工具中的數字顯示為零(0)，表示您作用中的評估(或您選取的評估)沒有不合規的證據。

無法使用 CSV 下載選項

此選項只適用於個別評估。請確定已套用 the section called “評估篩選器” 至儀表板，然後再試一次。請記住，您一次只能下載一個 CSV 檔案。

嘗試下載 CSV 檔案時看不到下載的檔案

如果控制項域包含大量控制項，則 Audit Manager 產生 CSV 檔案時可能會有短暫的延遲。文件生成後，它會開始自動下載。

如果您仍然看不到下載的檔案，請確定您的網際網路連線正常運作，而且您使用的是最新版本的網頁瀏覽器。此外，請檢查您最近的下載文件夾。檔案會下載至瀏覽器所決定的預設位置。如果這樣無法解決您的問題，請嘗試使用其他瀏覽器下載檔案。

儀表板遺失特定控制項或控制項域

這可能表示您作用中的評估(或指定的評估)沒有該控制項或控制項域的任何相關資料。

只有當下列兩個條件都符合時，控制項域才會顯示在儀表板上：

- 您作用中的評估(或指定的評估)至少包含一個與該域相關的控制項
- 該域內至少有一個控制項，在儀表板頂端的日期有收集證據

只有當控制項在儀表板頂部的日期收集證據時，控制項才會顯示在域內。

每日快照顯示每天的證據數量都不相同。這正常嗎？

並非每天都會收集所有證據。Audit Manager 評估中的控制項會對應至不同的資料來源，而且每個控制項都可以有不同的證據收集排程。因此，每日快照每天顯示的證據數量不同是很正常的。如需更多有關證據收集頻率的詳細資訊，請參閱 AWS Audit Manager 如何收集證據。

委派系統管理員與 AWS Organizations 相關問題疑難排解

請參考此頁面提供的資訊來解決 Audit Manager 中常見的委派系統管理員問題。

主題

我無法在 Audit Manager 設定委派系統管理員帳戶

雖然 AWS Organizations 支援多個委派系統管理員，但 Audit Manager 只允許一名委派系統管理員。如果您嘗試在 Audit Manager 中指定多個委派系統管理員，您會收到下列錯誤訊息：

- 主控台：`You have exceeded the allowed number of delegated administrators for the delegated service`
- CLI：`An error occurred (ValidationException) when calling the RegisterAccount operation: Cannot change delegated Admin for an active account 11111111111 from 2222222222222 to 333333333333`

在 Audit Manager 中，選擇一個要擔任委派系統管理員的帳戶。請務必先在組織內註冊此委派系統管理員帳戶，然後在 Audit Manager 新增與委派系統管理員相同的帳戶。

建立評估時，我無法在範圍內的帳戶看到組織中的帳戶

如果您希望 Audit Manager 評估包含組織中的多個帳戶，則必須指定委派系統管理員。

請確認您已為 Audit Manager 配置委派系統管理員帳戶。如需指示，請參閱設定，委派系統管理員。

需要謹記的一些事項：

- 您無法在 Audit Manager 使用 AWS Organizations 管理帳號作為委派系統管理員。
- 如果您要在多個 AWS 區域 啟用 Audit Manager，則必須在每個區域中單獨指定委派的管理員帳戶。在 Audit Manager 設定中，為所有區域指定相同的委派系統管理員帳戶。

- 當您指定 Audit Manager 的委派系統管理員時，請確保委派系統管理員帳戶具有您設定 Audit Manager 時所提供的 KMS 金鑰的存取權限。若要瞭解如何檢閱和變更加密設定，請參閱資料加密。

當我嘗試使用委派系統管理員帳戶產生評估報告時，出現存取遭拒的錯誤

如果您的評估是由委派的系統管理員帳戶建立，並且 Audit Manager 設定中指定的 KMS 金鑰不屬於該帳戶，您將會收到 `access denied` 錯誤訊息。若要避免此錯誤，當您指定 Audit Manager 的委派系統管理員時，請確定委派系統管理員帳戶具有您設定 Audit Manager 時所提供的 KMS 金鑰的存取權限。

如果您沒有用作評估報告目的地的的 S3 儲存貯體的寫入權限，您也可能會收到 `access denied` 錯誤訊息。

若您收到 `access denied` 錯誤訊息，請確定您符合下列要求：

- 您在 Audit Manager 設定中的 KMS 金鑰將權限授予委派系統管理員。您可以依照 AWS Key Management Service 開發人員指南中，允許其他帳戶中的使用者使用 KMS 金鑰中的指南進行設定。關於如何在 Audit Manager 中檢視和變更加密設定的指示，請參閱資料加密。
- 您擁有一個權限策略，該策略可授予您評估報告目的地的寫入存取權限。更具體地說，您的許可政策包含一個 `s3:PutObject` 動作、指定 S3 儲存貯體的 ARN，並包含用於加密評估報告的 KMS 金鑰。關於您可以使用的範例策略，請參閱 AWS Audit Manager 的以身分為基礎的策略範例

> **Note**
>
> 如果您變更 Audit Manager 資料加密設定，這些變更會套用至您未來建立的新評估。這包括您依據新評估所建立的任何評估報告。
> 這些變更不會套用至您在變更加密設定之前，已建立的現有評估。出了現有的評估報告之外，這還包括了您根據現有評估建立的新評估報告。現有的評估及其所有評估報告都將繼續使用舊有的 KMS 金鑰。如果產生評估報告的 IAM 身分沒有使用舊有 KMS 金鑰的權限，您可以在金鑰政策層級授予權限。

如果我取消成員帳戶與組織的連結，Audit Manager 會發生什麼情況？

當您取消組織成員帳戶的連結時，Audit Manager 會收到有關此事件的通知。然後，Audit Manager 會自動從現有評估範圍中的帳戶清單中移除此 AWS 帳戶。當您指定新評估的範圍後，取消連結的帳戶將不會再出現在符合資格的 AWS 帳戶 清單中。

當 Audit Manager 從評估範圍中的帳戶中移除取消連結的成員帳戶時，系統不會通知您這項變更。此外，取消連結的成員帳戶也不會收到通知，得知帳戶已不再啟用 Audit Manager。

如果我將成員帳戶重新連結至組織，會發生什麼情況？

當您將成員帳戶重新連結至組織時，該帳戶不會自動新增至您現有 Audit Manager 評估的範圍。不過，當您指定評估中範圍中的帳戶後，重新連結的成員就會顯示為符合資格 AWS 帳戶。

- 對於現有評估，您可以手動編輯評估範圍，以新增重新連結的成員帳戶。如需指示，請參閱編輯在範圍內的 AWS 帳戶。
- 對於新的評估，您可以在評估設定期間新增重新連結的帳戶。如需指示，請參閱指定在範圍內的 AWS 帳戶。

如果我將成員帳戶從一個組織移到另一個組織，會發生什麼情況？

如果成員帳戶已在組織 1 中啟用 Audit Manager 然後移轉至組織 2，不會因此啟用組織 2 的 Audit Manager。

證據搜尋工具問題疑難排解

請參考此頁面提供的資訊，解決 Audit Manager 中常見的證據搜尋工具問題。

一般證據搜尋工具問題

- 我無法啟用證據搜尋工具
- 我已啟用證據搜尋工具，但在搜尋結果中看不到過去的證據
- 我無法停用證據搜尋工具
- 我的搜尋查詢失敗

證據搜尋工具評估報告問題

- 我無法從搜尋結果中產生多個評估報告
- 我無法在搜尋結果中加入特定證據
- 在評估報告中，並未包含所有來自證據搜尋工具的查找結果
- 我想從搜尋結果中產生評估報告，但我的查詢陳述式執行失敗
- 其他資源

證據搜尋工具 CSV 匯出問題

- 我的 CSV 匯出失敗
- 我無法從搜尋結果中匯出特定證據
- 我無法一次匯出多個 CSV 檔案

我無法啟用證據搜尋工具

無法啟用證據搜尋工具的常見原因如下：

您缺少權限

如果您是第一次嘗試啟用證據搜尋工具，請確定您有所需許可。這些許可允許您在 CloudTrail Lake 中建立和管理事件資料存放區，這對於支援證據搜尋工具搜尋查詢是必要的。許可還允許您在證據搜尋工具中執行搜尋查詢。

如需權限方面的協助，請聯絡您的 AWS 管理員。如果您是 AWS 系統管理員，則可以複製所需的權限聲明，並將其附加到 IAM 政策。

您正在使用組織管理帳戶

請記住，您無法使用管理帳戶來啟用證據搜尋工具。以委派系統管理員帳戶身分登入，然後重試。

您之前已停用證據搜尋工具

目前不支援重新啟用證據搜尋工具。如果您之前已停用證據搜尋工具，則無法再次啟用它。

我已啟用證據搜尋工具，但在搜尋結果中看不到過去的證據

當您啟用證據搜尋工具時，您過去的所有證據資料，最多需要 7 天才能存取使用。

在這 7 天期間，事件資料存放區會回填您過去兩年的證據資料。這意味著，如果您在啟用證據搜尋工具後立即使用操作，則在完成回填之前，無法獲取完整的搜尋結果。

關於如何檢查資料回填狀態的指示，請參閱確認證據搜尋工具的狀態。

我無法停用證據搜尋工具

這可能由以下其中一個原因造成。

您缺少權限

如果您要嘗試停用證據搜尋工具，請確定您有所需許可。這些許可允許您更新和刪除在 CloudTrail Lake 中的事件資料存放區，這對於停用證據搜尋工具是必要的。

如需權限方面的協助，請聯絡您的 AWS 管理員。如果您是 AWS 系統管理員，則可以複製所需的權限聲明，並將其附加到 IAM 政策。

啟用證據搜尋工具的要求仍在進行中

當您要求啟用證據搜尋工具時，我們會建立一個事件資料存放區，以支援證據搜尋工具查詢。建立事件資料存放區時，您無法停用證據搜尋工具。

若要繼續，請等到事件資料存放區建立完成，然後再試一次。如需更多資訊，請參閱確認證據搜尋工具的狀態。

您已要求停用證據搜尋工具

當您要求停用證據搜尋工具時，我們會刪除用於證據搜尋工具查詢的事件資料存放區。如果您在刪除事件資料存放區時再次嘗試停用證據搜尋工具，您會收到錯誤訊息。

在這種情況下，不需要採取任何動作。等待事件資料存放區刪除。一旦完成，證據搜尋工具將被禁用。如需更多資訊，請參閱確認證據搜尋工具的狀態。

我的搜尋查詢失敗

失敗的搜尋查詢可能由以下其中一項原因造成。

您缺少權限

驗證使用者是否具備執行搜尋查詢和存取搜尋結果的所需權限。具體而言，您需要以下 CloudTrail 操作權限：

- StartQuery
- DescribeQuery
- CancelQuery
- GetQueryResults

如需權限方面的協助，請聯絡您的 AWS 管理員。如果您是 AWS 系統管理員，則可以複製所需的權限聲明，並將其附加到 IAM 政策。

您的查詢數目已達上限

您一次最多可以執行 5 個查詢。如果您同時執行的查詢數目已達上限，則會導致 `MaxConcurrentQueriesException` 錯誤。如果您收到這個錯誤訊息，請稍候一分鐘讓部分查詢完成，然後再次執行查詢。

您的查詢陳述式有驗證錯誤

如果您使用 API 或 CLI 來執行 CloudTrail Lake StartQuery 作業，請確定您的 `queryStatement` 是有效的。如果查詢陳述式有驗證錯誤、語法不正確或不支援的關鍵字，這會導致 `InvalidQueryStatementException`。

如需有關撰寫查詢的詳細資訊，請參閱 AWS CloudTrail 使用指南中的建立或編輯查詢。

如需有效語法的範例，請檢閱下列可用來查詢 Audit Manager 事件資料存放區的查詢陳述式範例。

範例 1：調查證據及其合規狀態

此範例會在指定日期範圍內，尋找帳戶中所有評估中具有任何合規狀態的證據。

```
SELECT eventData.evidenceId, eventData.resourceArn,
 eventData.resourceComplianceCheck FROM $EDS_ID WHERE eventTime > '2022-11-02
 00:00:00.000' AND eventTime < '2022-11-03 00:00:00.000'
```

範例 2：判斷控制項的不合規證據

此範例會尋找特定評估和控制項在指定日期範圍內的所有不合規證據。

```
SELECT * FROM $EDS_ID WHERE eventData.assessmentId = '11aa33bb-55cc-77dd-99ee-
ff22gg44hh66' AND eventTime > '2022-10-27 22:05:00.000' AND eventTime
 < '2022-11-03 22:05:00.000' AND eventData.resourceComplianceCheck IN
 ('NON_COMPLIANT','FAILED','WARNING') AND eventData.controlId IN ('aa11bb22-cc33-
dd44-ee55-ff66gg77hh88')
```

範例 3：按名稱計算證據

此範例會列出指定日期範圍內評估的總證據，並依名稱分組，並依證據計數排序。

```
SELECT eventData.eventName as eventName, COUNT(*) as totalEvidence FROM  $EDS_ID
 WHERE eventData.assessmentId = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' AND eventTime
```

```
 > '2022-10-27 22:05:00.000' AND eventTime < '2022-11-03 22:05:00.000' GROUP BY
 eventData.eventName ORDER BY totalEvidence DESC
```

範例 4：依資料來源和服務探索證據

此範例會尋找特定資料來源和服務在指定日期範圍內的所有證據。

```
SELECT * FROM $EDS_ID WHERE eventTime > '2022-10-27 22:05:00.000' AND eventTime
 < '2022-11-03 22:05:00.000' AND eventData.service IN ('dynamodb') AND
 eventData.dataSource IN ('AWS API calls')
```

範例 5：依資料來源和控制項域探索合規證據

此範例尋找特定控制項域的合規證據，其中證據來自非 AWS Config 的資料來源。

```
 SELECT * FROM $EDS_ID WHERE eventData.resourceComplianceCheck IN
 ('PASSED','COMPLIANT') AND eventData.controlDomainName IN ('Logging and
 monitoring','Data security and privacy') AND eventData.dataSource NOT IN ('AWS
 Config')
```

其他 API 異常狀況

StartQuery API 可能會因為其他幾個原因而失敗。如需可能的錯誤和說明的完整清單，請參閱 AWS CloudTrail API 參考中的 StartQuery 錯誤。

我無法從搜尋結果中產生多個評估報告

此錯誤是由於同時執行太多 CloudTrail Lake 查詢所致。

如果您將搜尋結果分組，並嘗試針對群組結果中的每個明細項目立即產生評估報告，就會發生此錯誤。當您取得搜尋結果並產生評估報告時，每個動作都會觸發一次查詢。您一次最多可以執行 5 個查詢。如果您同時執行的查詢數目已達上限，則會返回 `MaxConcurrentQueriesException` 錯誤。

若要避免發生此錯誤，請確保您沒有一次產生過多的評估報告。如果您同時執行的查詢數目已達上限，則會返回 `MaxConcurrentQueriesException` 錯誤。如果您收到此錯誤訊息，請等待幾分鐘，讓進行中的評估報告完成。

您可以從 Audit Manager 主控台的下載中心頁面，檢查評估報告的狀態。報告完成後，在證據搜尋工具中返回您的分組結果。然後，您可以繼續取得結果，並為每個明細項目產生評估報告。

我無法在搜尋結果中加入特定證據

您的所有搜尋結果都包含在評估報告中。您無法從搜尋結果集中選擇性地新增個別列。

如果您只想在評估報告中包含特定的搜尋結果，建議您編輯目前的搜尋篩選器。如此一來，您就可以縮小結果範圍，僅鎖定您要包含在報告中的證據。

在評估報告中，並未包含所有來自證據搜尋工具的查找結果

當您產生評估報告時，您可以新增的證據數量有限。此限制取決於您評估的 AWS 區域、用作評估報告目的地的 S3 儲存貯體區域，以及您的評估是否使用了客戶受管的 AWS KMS key。

1. 相同區域報告的上限為 22,000 (S3 儲存貯體和評估都在同一個 AWS 區域 的情況下)
2. 跨區域報告的上限為 3,500 (S3 儲存貯體和評估在不同 AWS 區域 的情況下)
3. 如果評估使用客戶管理的 KMS 金鑰，則上限為 3,500

如果您超過此限制，報告仍會建立。不過，Audit Manager 只會將前 3,500 或 22,000 個證據項目新增至報告。

若要避免發生此問題，建議您編輯目前的搜尋篩選器。如此一來，您就可以針對較少量的證據來減少搜尋結果。如果需要，您可以重複此方法並產生多個評估報告，而不是一個較大的報告。

我想從搜尋結果中產生評估報告，但我的查詢陳述式執行失敗

如果您在使用 CreateExcomentrePort API 時，您查詢陳述式傳回驗證異常，請參閱下表以取得修正該異常的指南。

> **Note**
>
> 即使查詢陳述式在 CloudTrail 中可以運作，相同的查詢對於在 Audit Manager 中產生評估報告可能無效。這是因為兩個服務之間的查詢驗證有些差異。

子句	問題	解決方案	備註
SELECT	SELECT 子句包含一個列名	移除 SELECT 子句並替換為 SELECT eventJson 。	僅支援 SELECT eventJson 。

子句	問題	解決方案	備註
			此驗證由 Audit Manager 處理。
FROM	FROM 子句包含無效的事件資料存放區 ID 或 提供的事件資料存放區 ID 與 Audit Manager 設定中的事件資料存放區 ID 不符	移除子句 FROM 並替換為FROM *edsID*，其中的值 edsID 與 Audit Manager 設定中指定的事件資料存放區 ID 相符。 您可以從 Audit Manager 設定中擷取事件資料存放區的 ARN。如需詳細資訊，請參閱 AWS Audit Manager API 參考中的 GetSettings。	此驗證由 Audit Manager 處理。
GROUP BY	查詢中存在一個 GROUP BY 子句	移除 GROUP BY 子句。	此驗證由 Audit Manager 處理。
HAVING	查詢中存在一個 HAVING 子句	移除 HAVING 子句。	此驗證由 Audit Manager 處理。
LIMIT	LIMIT 子句包含的值超過允許的最大限制	如果 LIMIT 子句存在，請確保其值等於或小於支援的最大限制： • 對於同區域報表，上限為 22,000 • 對於跨區域報表，上限為 3,500 • 對於相關評估使用客戶管理的 AWS KMS key 之報告，上限為 3,500	在主控台中，可傳回的證據結果數量沒有限制。不過，產生評估報告時，您可以包含的證據數量會有限制。 如果您的查詢陳述式中未提供任何 LIMIT 值，則會套用預設的最大限制。 此驗證由 Audit Manager 處理。
ORDER BY	ORDER BY 子句包含 SELECT 子句中不存在的彙總函數或別名	請確保 ORDER BY 子句不包含任何使用彙總函數或別名的條件。	此驗證由 CloudTrail StartQuery API 處理。

子句	問題	解決方案	備註
WHERE	WHERE 子句包含多個 assessmentId 或 WHERE 子句包含一個 assessmentId ，其與您的 createAssessmentReport 要求的 assessmentId 不相符。 或 WHERE 子句包含一個不支援的列名	請確定您只指定一個 assessmentID，而且它符合您在 createAssessmentReport API 要求中指定的assessmentID參數。 移除任何不支援的欄位名稱。	此驗證由 CloudTrail StartQuery API 處理。

範例

下列範例示範如何在呼叫CreateAssessmentReport作業時使用 queryStatement 參數。使用這些查詢之前，請先用您自己的 edsId 和 assessmentId 值取代 ######。

範例 1：建立報表（適用相同區域限制）

此範例會建立一個報告，其中包含在 2022 年 1 月 22 日至 23 日之間建立之 S3 儲存貯體的結果。

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId
 = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' AND eventTime > '2022-01-22 00:00:00.000' AND
 eventTime < '2022-01-23 00:00:00.000' AND eventName='CreateBucket' LIMIT 22000
```

範例 1：建立報表（適用跨區域限制）

此範例會建立一個報告，其中包含指定事件資料存放區和評估的所有結果，但未指定日期範圍。

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId
 = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' LIMIT 7000
```

範例 3：建立報告（在預設限制下）

此範例會建立一個報告，其中包含指定事件資料存放區和評估的所有結果，其上限低於預設最大值。

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId
 = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' LIMIT 2000
```

其他資源

下列頁面提供關於評估報告的一般疑難問題排解指南：

- 評估報告問題疑難排解

我的 CSV 匯出失敗

您的 CSV 匯出失敗原因有很多種可能性。您可以透過檢查常見原因來對此問題進行故障排除。

首先，請確認您符合使用 CSV 匯出功能的必要條件：

您已成功啟用證據搜尋工具

如果您尚未啟用證據搜尋工具，則無法執行搜尋查詢並匯出搜尋結果。

事件資料存放區的回填已完成

如果您在啟用證據搜尋工具後立即使用證據搜尋工具，並且證據回填仍在進行中，則可能會有一些結果無法使用。如需檢查資料回填狀態，請參閱確認證據搜尋工具的狀態。

您的搜尋查詢成功

Audit Manager 無法匯出失敗查詢的結果。若要疑難排解失敗的查詢，請參閱 我的搜尋查詢失敗。

確認符合先決條件後，請使用下列檢查清單來檢查潛在問題：

1. 檢查您搜尋查詢的狀態：
   a. 查詢是否已取消？ 證據搜尋工具會顯示在取消查詢之前處理的部分結果。不過，Audit Manager 不會將部分結果匯出到 S3 儲存貯體或下載中心。
   b. 查詢是否已執行超過一個小時？ 執行時間超過一小時的查詢可能會逾時。證據搜尋工具會顯示在查詢逾時之前處理的部分結果。但是，Audit Manager 不會匯出部分結果。若要避免逾時，您可以透過編輯查詢指定較短的時間範圍，以減少掃描的證據量。
2. 檢查匯出目的地的 S3 儲存貯體名稱和 URI：

a. 指定的儲存貯體是否存在？ 如果您手動輸入儲存貯體 URI，請確保沒有錯誤輸入任何內容。當 Audit Manager 嘗試將 CSV 檔案匯出到 Amazon S3 時，錯字或不正確的 URI 可能會導致 `RESOURCE_NOT_FOUND` 錯誤。

3. 檢查匯出目的地的 S3 儲存貯體權限：

a. 您有 S3 儲存貯體的寫入權限嗎？ 您必須擁有用作匯出目的地的 S3 儲存貯體寫入權限。更具體地說，IAM 權限策略必須包含 `s3:PutObject` 動作和儲存貯體 ARN，並將 CloudTrail 列為服務主體。我們提供您可以使用的範例政策。關於如何使用不同 S3 儲存貯體的指南，請參閱匯出目的地設定。

4. 檢查您的任何 AWS 區域 資訊是否不相符：

a. 您客戶的管理金鑰的 AWS 區域 是否與您評估的 AWS 區域 相符？ 如果您為資料加密提供了客戶管理金鑰，則該金鑰必須與您的評估 AWS 區域 相同。關於如何變更 KMS 金鑰的指南，請參閱資料加密設定。

5. 檢查委派管理員的帳戶權限：

a. Audit Manager 設定中的客戶管理金鑰，是否會將權限授與委派系統管理員？ 如果您使用委派系統管理員帳戶，並指定了用於資料加密的客戶管理金鑰，請確定委派系統管理員擁有該 KMS 金鑰的存取權。如需指示，請參閱 AWS Key Management Service 開發人員指南中的允許其他帳戶中的使用者使用 KMS 金鑰。關於如何在 Audit Manager 中檢視和變更加密設定的指示，請參閱資料加密設定。

> **Note**
>
> 如果您變更 Audit Manager 資料加密設定，這些變更會套用至您未來建立的新評估。這包括從新的評估匯出的任何 CSV 檔案。
> 這些變更不會套用至您在變更加密設定之前，已建立的現有評估。除了現有的 CSV 匯出之外，這還包括基於現有評估匯出的新 CSV。現有的評估及其所有 CSV 報告都將繼續使用舊有的 KMS 金鑰。如果匯出 CSV 檔案的 IAM 身分沒有使用舊有 KMS 金鑰的權限，您可以在金鑰政策層級授予權限。

我無法從搜尋結果中匯出特定證據

您的所有搜尋結果都包含在結果中。

如果您只想在 CSV 檔案中包含特定的搜尋結果，建議您編輯目前的搜尋篩選器。如此一來，您就可以縮小結果範圍，僅鎖定您要匯出的證據。

我無法一次匯出多個 CSV 檔案

此錯誤是由於同時執行太多 CloudTrail Lake 查詢所致。

如果您將搜尋結果分組，並嘗試針對群組結果中的每個行項目立即匯出 CSV 檔案，就會發生此錯誤。當您在取得搜尋結果時同步匯出 CSV 檔案，這些動作都會引發一次查詢。您一次最多可以執行 5 個查詢。如果您同時執行的查詢數目已達上限，則會返回 `MaxConcurrentQueriesException` 錯誤。

若要避免發生此錯誤，請確保您沒有一次匯出太多 CSV 檔案。

若要解決此錯誤，請等待進行中的 CSV 匯出完成。大多數匯出動作需要幾分鐘的時間。不過，如果您要匯出非常大量的資料，則可能需要長達一個小時才能完成匯出作業。在匯出過程中，您可以隨時離開證據搜尋工具。

您可以從 Audit Manager 主控台的下載中心檢查匯出狀態。匯出的檔案準備就緒後，返回證據搜尋工具中的分組結果。然後，您可以繼續取得結果，並匯出每個明細項目的 CSV 檔案。

架構共享問題疑難排解

請參考此頁面提供的資訊來解決 Audit Manager 中常見的架構共享問題。

主題

我傳送的共享要求狀態顯示為失敗

如果您嘗試共享自訂架構，但作業失敗，建議您檢查下列項目：

1. 請確保已在收件者 AWS 帳戶 和指定區域中啟用 Audit Manager。如需支援 AWS Audit Manager 區域的清單，請參閱 Amazon Web Services 一般參考中的 AWS Audit Manager 端點和配額
2. 請確保您在指定收件人帳戶時輸入了正確的 AWS 帳戶 ID。
3. 請確保您未將 AWS Organizations 管理帳戶指定為收件者。您可以與委派系統管理員共享自訂架構，但是如果您嘗試與管理帳戶共享自訂架構，則作業會失敗。

4. 如果您使用客戶管理金鑰來加密 Audit Manager 資料，請確保您的 KMS 金鑰已啟用。如果您的 KMS 金鑰已停用，而您嘗試共享自訂架構，則作業會失敗。關於如何啟用已停用 KMS 金鑰的指南，請參閱 AWS Key Management Service 開發人員指南中的啟用和停用金鑰。

我的共享要求旁邊有一個藍點。這代表什麼意思？

藍點通知表示有共享要求需要您過目。

寄件者藍點通知

已傳送的共享要求旁會出現藍色通知圓點，且狀態為即將到期。Audit Manager 會顯示藍點通知，以便提醒收件者在共享要求到期之前對其採取行動。

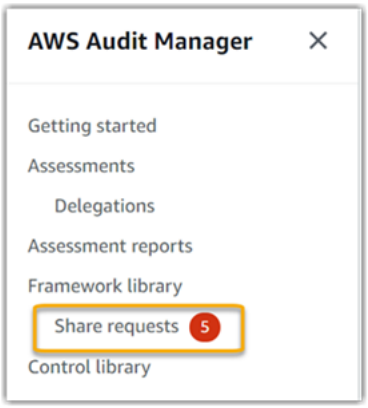
若要讓藍點通知消失，收件者必須接受或拒絕要求。如果您撤銷共享要求，藍點也會消失。

您可以使用下列程序來檢查，是否有任何即將到期的共享要求，並傳送選擇性提醒給收件者採取行動。

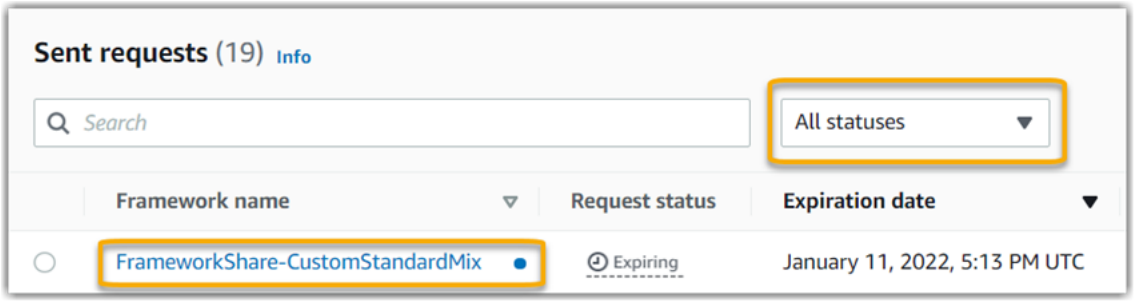
若要檢視已傳送要求的通知

1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 如果您有共享要求通知，Audit Manager 會在導覽功能表圖示旁邊顯示一個紅點。

3. 展開瀏覽窗格，然後查看共享要求的旁邊。通知圖示會指出需要處理的共享要求數目。



4. 選擇共享要求，然後選擇傳送要求索引標籤。
5. 尋找藍點，找出未來 30 天內到期的共享要求。或者，您也可以從所有狀態 篩選器下拉式清單中選取即將到期，檢視即將到期的共享要求。



6. （選擇性）提醒收件者，他們需要在共享要求到期前對其採取行動。此步驟為選擇性步驟，因為 Audit Manager 會在主控台中傳送通知，以便在共享要求處於作用中或即將到期時通知收件者。但是，您也可以使用偏好的通訊管道向收件人發送自己的提醒。

收件者藍點通知

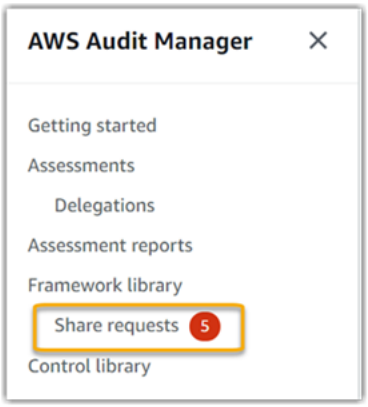
已傳送的共享要求旁會出現藍色通知圓點，且狀態為作用中或即將到期。Audit Manager 會顯示藍點通知，以便提醒收件者在共享請求到期之前對其採取行動。若要讓藍點通知消失，收件者必須接受或拒絕要求。如果傳送者撤銷共享要求，藍點也會消失。

您可以使用下列程序檢查作用中和即將到期的共享要求。

若要檢視已接收請求的通知

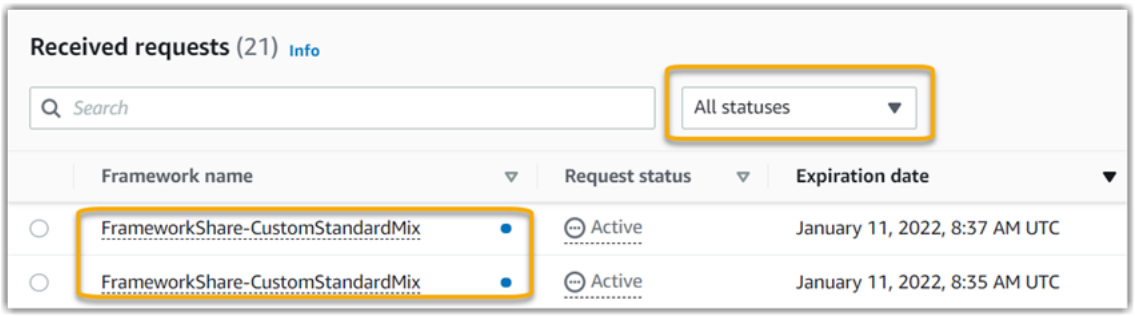
1. 開啟 AWS Audit Manager 主控台，網址為 https://console.aws.amazon.com/auditmanager/home。
2. 如果您有共享要求通知，Audit Manager 會在導覽功能表圖示旁邊顯示一個紅點。

3. 展開瀏覽窗格，然後查看共享要求的旁邊。通知圖示會指出需要您處理的共享要求數目。



4. 選擇共享要求。依預設，此頁面會在已接收的要求索引標籤上開啟。

5. 尋找帶有藍點的項目，以找出需要執行動作的共享要求。



6. （選擇性）若只要檢視未來 30 天內到期的要求，請尋找所有狀態下拉式清單，然後選取即將到期。

我的共享架構有使用自訂 AWS Config 規則作為資料來源的控制項。收件人可以收集這些控制項的證據嗎？

是的，收件人可以收集這些控制的證據，但需要幾個步驟來實現這一目標。

若要讓 Audit Manager 使用 AWS Config 規則作為資料來源映射項目來收集證據，必須符合下列條件。這些條件同時適用於受管規則和自訂規則。

- 規則必須存在於收件者的 AWS 環境中
- 必須在收件者的 AWS 環境中啟用規則

請記住，您帳戶中的 AWS Config 規則可能不存在於收件人的 AWS 環境中。此外，當收件者接受共享要求時，Audit Manager 不會在其帳戶中重新建立您的任何自訂規則。若要讓收件者使用您的自訂規則作為資料來源映射項目來收集證據，他們必須在 AWS Config 執行個體中建立相同的自訂規則。收件者在 AWS Config 中建立並啟用規則後，Audit Manager 可以從該資料來源收集證據。

我們建議您與收件者通訊，讓他們知道是否需要在其 AWS Config 執行個體中建立任何自訂 AWS Config 規則。

我更新了共享架構中使用的自訂規則。我需要採取任何動作嗎？

針對 AWS 環境中的規則更新

當您更新 AWS 環境中的自訂規則時，無需在 Audit Manager 中執行任何動作。Audit Manager 會依照下表所述的方式偵測和處理規則更新。偵測到規則更新時，Audit Manager 不會另行通知。

案例	Audit Manager 會做什麼	您需要執行的事項
自訂規則會在您的 AWS Config 執行個體中更新。	Audit Manager 會繼續使用更新的規則定義報告該規則的調查結果。	不需採取任何動作。
自訂規則會在您的 AWS Config 執行個體中刪除。	Audit Manager 會停止報告已刪除規則的調查結果。	不需採取任何動作。 如果需要，您可以編輯自訂控制項，使用已刪除規則作為資料來源映射項目。然後，您可以移除已刪除的規則，以清除控制項的資料來源設定。否則，刪除的規則名稱會保留為未使用的資料來源映射項目。

適用於 AWS 環境外部的規則更新

在收件者的 AWS 環境中，Audit Manager 不會偵測到規則更新。這是因為，寄件者和收件者各自在不同的 AWS 環境中工作。下表提供適用於此方案的建議作法。

您的角色	案例	建議的動作
Sender	• 您共享使用自訂規則作爲資料來源映射項目的架構。 • 在您共享架構之後，您就更新或刪除了 AWS Config 中的其中一個規則。	請連絡收件者，通知他們相關更新。如此一來，他們就可以套用相同的更新，並與最新的規則定義保持同步。
Recipie	• 您接受使用自訂規則做為資料來源映射項目的共享架構。 • 在 AWS Config 執行個體中重新建立自訂規則之後，寄件者就會更新或刪除其中一個規則。	在您自己的 AWS Config 執行個體中進行對應的規則更新。

通知問題疑難排解

請參考此頁面提供的資訊來解決 Audit Manager 中常見的通知問題。

主題

我在 Audit Manager 中指定了 Amazon SNS 主題，但沒有收到任何通知

如果您的 Amazon SNS 主題使用 AWS KMS 進行伺服器端加密 (SSE)，您可能會遺失 AWS KMS 金鑰政策的所需權限。如果您沒有將一個端點訂閱至主題中，也可能無法收到通知。

如果您沒有收到通知，請確認執行下列作業：

- 您已將所需的許可政策附加至 KMS 金鑰。範例政策可在本指南的通知頁面上找到。
- 您訂閱了發送通知的主題的端點。當您訂閱電子郵件端點至主題時，您會收到一封電子郵件，要求您確認訂閱。您必須確認訂閱，才能開始接收電郵通知。如需詳細資訊，請參閱 Amazon SNS 開發人員指南中的入門。

我指定了 FIFO 主題，但沒有依預期順序收到通知

Audit Manager 支援將通知傳送至 FIFO SNS 主題。但是，其無法保證 Audit Manager 會將通知依序傳送至您的 FIFO 主題。

權限和存取問題疑難排解

請參考此頁面提供的資訊來解決 Audit Manager 中常見的權限問題。

主題

我按照 Audit Manager 設定程序進行操作，但我沒有足夠的 IAM 權限

您用於存取 Audit Manage 的使用者、角色或群組必須具有所需的權限。除此之外，您的身份驗證政策不應設定的太嚴格。否則，主控台將無法如預期般運作。本指南中的設定程序提供的策略會授予設定 Audit Manager 所需的最低權限。根據您的使用案例，您可能需要更廣泛、更少限制的權限。舉例來說，我們建議稽核擁有者具備系統管理員存取權。這樣他們就可以修改 Audit Manager 設定並管理資源，例如評估、架構、控制項和評估報告。其他使用者（例如委派人員）可能只需要管理存取權或唯讀存取權。

請務必為您的使用者、角色或群組添加適當的權限。對於稽核擁有者，建議使用的政策為 AWSAuditManagerAdministratorAccess。對於委派人員，您可以使用IAM 政策範例頁面上提供的此範例。您可以使用這些範例政策作為起點，並根據您的需求進行必要的變更。

我們建議您花些時間自訂權限，以滿足您的特定需求。如果您需要 IAM 權限相關協助，請聯絡您的管理員或 AWS 支援人員。

我指定某人為稽核擁有者，但他們仍然無法完整存取評估。為什麼？

僅將某人指定為稽核擁有者，並不會提供評估的完整存取權限。稽核擁有者還必須擁有必要的 IAM 權限才能存取和管理 Audit Manager 資源。換句話說，除了將使用者指定為稽核擁有者之外，您還必須將必要的 IAM 政策附加到該使用者上。換句話說，只要同時具備兩者，Audit Manager 確保您可以完全控制每個評估的所有細節。

> **Note**
>
> 對於稽核擁有者，建議使用 AWSAuditManagerAdministratorAccess 政策。如需詳細資訊，請參閱 Audit Manager 中使用者角色的建議策略。

我無法在 Audit Manager 中執行動作

如果您沒有使用 AWS Audit Manager 主控台或 Audit Manager API 作業的必要權限，您可能會遇到 `AccessDeniedException` 錯誤訊息。

若要解決此問題，請聯絡管理員以取得協助。您的管理員是為您提供登入憑證的人員。

我想要允許我的 AWS 帳戶 以外的人員存取我的 Audit Manager 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對象取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您資源的許可。

若要進一步了解，請參閱以下內容：

- 如需了解 Audit Manager 是否支援這些功能，請參閱 如何與 IAM AWS Audit Manager 搭配使用。
- 若要了解如何存取您擁有的所有 AWS 帳戶 所提供的資源，請參閱《IAM 使用者指南》中的將存取權提供給您所擁有的另一個 AWS 帳戶 中的 IAM 使用者。
- 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擁有的 AWS 帳戶。
- 若要了解如何透過聯合身分提供存取權，請參閱《IAM 使用者指南》中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。
- 若要了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 角色與資源型政策的差異。

另請參閱

下列頁面提供因缺少權限而可能導致的其他問題的疑難排解指南：

- 我在評估中看不到任何控制項或控制集
- 當我設定控制項資料來源時，無法使用自訂規則選項
- 當我嘗試生成評估報告時，出現存取被拒絕的錯誤
- 當我嘗試使用委派系統管理員帳戶產生評估報告時，出現存取遭拒的錯誤
- 我無法啟用證據搜尋工具
- 我無法停用證據搜尋工具
- 我的搜尋查詢在證據搜尋工具中出現失敗結果
- 我在 Audit Manager 中指定了 Amazon SNS 主題，但沒有收到任何通知

AWS Audit Manager 的配額和限制

對於每項 AWS 服務，您的 AWS 帳戶 有預設配額，先前稱為限額。除非另有說明，否則每個配額都是區域特定規定。您可以要求提高某些配額，而其他配額無法提高。

大多數 Audit Manager 配額（但不是全部）都列在 Service Quotas 控制台的 AWS Audit Manager 命名空間下。如需要求增加配額，請參閱 管理您的 Audit Manager 配額。

預設 Audit Manager 配額

以下為每個區域之每個 AWS 帳戶 的 AWS Audit Manager 配額。

評估

- 每個帳戶的使用中評估數量：100

評估報告

- 您可以新增至評估報告的證據項目數量：
  - 相同區域報告 (評估和評估報告目的地 S3 儲存貯體位於相同AWS 區域)：22,000
  - 跨區域報告 (評估和評估報告目的地 S3 儲存貯體位於不同AWS 區域)：3,500
  - 客戶受管的AWS KMS key相關評估使用報告：3,500

控制

- 每個帳戶的自訂控制項數量：500

證據

- 單個手動證據檔案的大小上限：100 MB
- 每個控制項的每日手動證據上傳數量：100

> **Tip**
>
> 如果您需要將大量手動證據上傳至單一控制項，建議您在數天內分批上傳證據。

架構

- 每個帳戶的自訂架構數量：100

> **Note**
>
> 不論架構是誰建立的，架構配額會套用至架構程式庫中所有共享的自訂架構。

共享自訂架構收件人

- 使用中的收件人帳戶數量：100

API 存取

- 所有 API 的每秒交易次數 (TPS)：20 TPS

管理您的 Audit Manager 配額

AWS Audit Manager 與 Service Quotas 整合，這是可讓您集中檢視和管理配額的 AWS 服務。如需詳細資訊，請參閱Service Quotas 使用者指南中的什麼是 Service Quotas？。Service Quotas 可讓您輕鬆查詢 Amazon Manager 配額的值。

使用主控台來檢視 Audit Manager Service Quotas

1. 開啟 Service Quotas 主控台，網址為 https://console.aws.amazon.com/servicequotas/。
2. 在導覽窗格中，選擇 AWS 服務。
3. 從 AWS 服務 清單中，搜尋並選取 AWS Audit Manager。
4. 在 Service Quotas 清單中，您可以看到服務配額名稱、套用的配額值（如果有的話）、AWS 預設配額值，以及配額是否可調整。
5. 若要檢視服務配額的其他資訊 (例如說明)，請選擇配額名稱。
6. (選用) 若要請求增加配額，請選取您要增加的配額、選取 Request quota increase (請求增加配額)、輸入或選取必要資訊，然後選取 Request (請求)。

如需詳細資訊，請參閱《Service Quotas 使用者指南》中的請求提高配額。

中的安全性 AWS Audit Manager

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，這些架構是為了滿足對安全性最敏感的組織的需求而建置的。

安全是 AWS 與您之間共同承擔的責任。共同責任模型將其描述為雲端的安全性和雲端中的安全性：

- 雲端的安全性 — AWS 負責保護在 AWS 雲端中執行 AWS 服務的基礎架構。 AWS 還為您提供可以安全使用的服務。若要深入瞭解適用於的規範遵循計劃 AWS Audit Manager，請參閱合規計劃的 AWS 服務範圍範圍)。
- 雲端安全性 — 您的責任取決於您使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您公司的請求和適用法律和法規。

本文件可協助您瞭解如何在使用時套用共同責任模型 AWS Audit Manager。下列主題說明如何將 Audit Manager 設定為達到您的安全及合規目標。您也會學到如何使用其他 AWS 服務來協助您監控和保護 Audit Manager 資源。

主題

- 資料保護 AWS Audit Manager
- 的身分識別與存取管理 AWS Audit Manager
- 符合性驗證 AWS Audit Manager
- 韌性 AWS Audit Manager
- 基礎結構安全 AWS Audit Manager
- AWS Audit Manager 和介面 VPC 端端點 ()AWS PrivateLink
- 登錄和監控 AWS Audit Manager
- 中的配置和漏洞分析 AWS Audit Manager

資料保護 AWS Audit Manager

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

基於資料保護目的，我們建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 登入資料並設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源進行通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用設定 API 和使用者活動記錄 AWS CloudTrail。
- 使用 AWS 加密解決方案以及其中的所有默認安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在透過命令列介面或 API 存取時需要經 AWS 過 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需 FIPS 和 FIPS 端點的相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-2 概觀。

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

除此之外，我們特別建議 Audit Manager 客戶在建立評估、自訂控制項、自訂架構和委派評論時，不要在自由格式欄位中包含敏感識別資訊。

刪除 Audit Manager 資料

有幾種方法可以刪除 Audit Manager 資料。

停用 Audit Manager 時的資料刪除

停用 Audit Manager 時，您可以決定是否要刪除所有 Audit Manager 資料。如果您選擇刪除資料，資料會在停用 Audit Manager 後的 7 天內刪除。刪除資料後，您就無法復原。

自動刪除資料

某些 Audit Manager 資料會在特定時間後自動刪除。Audit Manager 會保留以下客戶資料。

資料類型	資料保留期間	備註
證據	資料會自建立之日起保留兩年。	包括自動化證據和手動證據

資料類型	資料保留期間	備註
客戶建立的資源	資料會無限期保留	包括評估、評估報告、自訂控制項和自訂架構

手動刪除資料

您可以隨時刪除單項 Audit Manager 資源。如需詳細說明，請參閱下列主題：

- 刪除評估
  - 另請參閱：DeleteAssessment在 AWS Audit Manager API 參考
- 刪除自訂架構
  - 另請參閱：DeleteAssessmentFramework在 AWS Audit Manager API 參考
- 刪除共享要求
  - 另請參閱：DeleteAssessmentFrameworkShare在 AWS Audit Manager API 參考
- 刪除評估報告
  - 另請參閱：DeleteAssessmentReport在 AWS Audit Manager API 參考
- 刪除自訂控制項
  - 另請參閱：DeleteControl在 AWS Audit Manager API 參考

如需刪除您在使用 Audit Manager 時可能已建立的其他資源資料，請參閱下列內容：

- AWS CloudTrail 使用者指南中，刪除事件資料存放區
- Amazon Simple Storage Service (Amazon S3) 使用者指南中的刪除儲存貯體

靜態加密

AWS 受管金鑰 為了加密靜態資料，Audit Manager 會針對其所有資料存放區和記錄使用伺服器端加密。

您的資料會以客戶管理的金鑰加密 AWS 擁有的金鑰，或根據您選取的設定而定。如果您未提供客戶管理的金鑰，Audit Manager 會使用 AWS 擁有的金鑰 來加密您的內容。Audit Manager 中的所有 DynamoDB 和 Amazon S3 服務中繼資料透過 AWS 擁有的金鑰加密。

Audit Manager 會依下列方式加密資料：

- 存放在 Amazon S3 中的服務中繼資料會 AWS 擁有的金鑰 使用 SSE-KMS 加密。
- 儲存在 DynamoDB 中的服務中繼資料使用 KMS 和 AWS 擁有的金鑰進行伺服器端加密。
- 您儲存在 DynamoDB 中的內容使用客戶管理金鑰或 AWS 擁有的金鑰進行用戶端加密。KMS 金鑰根據您選擇的設定而定。
- 您存放在 Audit Manager Amazon S3 中的內容使用 SSE-KMS 加密。KMS 金鑰根據您的選擇而定，可以是客戶管理金鑰或 AWS 擁有的金鑰。
- 發佈到 S3 儲存貯體的評估報告會進行以下加密：
  - 如果您提供客戶管理金鑰，您的資料會使用 SSE-KMS 加密。
  - 如果您使用 AWS 擁有的金鑰，則您的資料會使用 SSE-S3 加密。

傳輸中加密

Audit Manager 會提供安全且私有的端點，以供您加密傳輸中的資料。安全和私有端點允許 AWS 保護對 Audit Manager 的 API 請求的完整性。

跨服務傳輸

根據預設，所有服務間通訊皆受到 Transport Layer Security (TLS) 加密的保護。

金鑰管理

Audit Manager 支援 AWS 擁有的金鑰 和客戶受管金鑰，以加密所有 Audit Manager 資源 (儲存到帳戶中 S3 儲存貯體的評估、控制項、架構、證據和評估報告)。

建議您使用客戶管理金鑰。如此一來，您就可以檢視和管理用來保護資料的加密金鑰，包括在 AWS CloudTrail中檢視其使用日誌。選擇客戶管理金鑰時，Audit Manager 會針對 KMS 金鑰建立一個授權，以便可以用於加密您的內容。

> **Warning**
>
> 刪除或禁用用於加密 Audit Manager 資源的 KMS 金鑰之後，您就再也無法解密以該 KMS 金鑰加密的資源，這表示該資料已無法復原。
> 在 AWS Key Management Service (AWS KMS) 中刪除 KMS 金鑰具有破壞性且具有潛在危險性。如需有關刪除 KMS 金鑰的詳細資訊，請參閱AWS Key Management Service 使用者手冊 AWS KMS keys中的刪除。

當您使用稽核管理員 API 或 AWS Command Line Interface (AWS CLI) 啟用 Audit Manager Audit Manager 時，您可以指定加密設定。 AWS Management Console如需說明，請參閱啟用 AWS Audit Manager。

您可以隨時檢閱和變更您的加密設定。如需說明，請參閱資料加密。

如需如何設定客戶管理金鑰的詳細資訊，請參閱AWS Key Management Service 使用者指南中的建立金鑰。

的身分識別與存取管理 AWS Audit Manager

AWS Identity and Access Management (IAM) 可協助管理員安全地控制 AWS 資源存取權。 AWS 服務 IAM 管理員可以控制誰能完成身分驗證 (登入) 和獲得授權 (取得許可)，而得以使用 Audit Manager 資源。IAM 是您可以使用的 AWS 服務 ，無需額外付費。

主題

- 物件
- 使用身分驗證
- 使用政策管理存取權
- 如何與 IAM AWS Audit Manager 搭配使用
- 以身分識別為基礎的原則範例 AWS Audit Manager
- 預防跨服務混淆代理人
- AWS 受管理的政策 AWS Audit Manager
- 疑難排解 AWS Audit Manager 身分和存取
- 使用服務連結角色 AWS Audit Manager

物件

根據您在 Audit Manager 中執行的工作，使用方式 AWS Identity and Access Management (IAM) 會有所不同。

服務使用者 — 如果您使用 Audit Manager 服務執行工作，管理員會為您提供所需的憑證和許可。隨著您為了執行作業而使用的 Audit Manager 功能數量變多，您可能會需要額外的許可。瞭解存取許可的

管理方式可協助您向管理員請求正確的許可。若您無法存取 Audit Manager 中的某項功能，請參閱 疑難排解 AWS Audit Manager 身分和存取。

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

IAM 管理員：如果您是 IAM 管理員，建議您掌握如何撰寫政策以管理 Audit Manager 存取權的詳細資訊。如需檢視您可以在 IAM 中使用的 Audit Manager 身分型政策範例，請參閱 以身分識別為基礎的原則範例 AWS Audit Manager。

使用身分驗證

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

您可以使用透過 AWS 身分識別來源提供的認證，以聯合身分識別身分登入。 AWS IAM Identity Center (IAM 身分中心) 使用者、貴公司的單一登入身分驗證，以及您的 Google 或 Facebook 登入資料都是聯合身分識別的範例。您以聯合身分登入時，您的管理員先前已設定使用 IAM 角色的聯合身分。當您使 AWS 用同盟存取時，您會間接擔任角色。

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

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

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

AWS 帳戶 根使用者

當您建立時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取該帳戶中的所有資源 AWS 服務和資源。此身分稱為 AWS 帳戶 root 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常作業。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需這些任務的完整清單，了解需以根使用者登入的任務，請參閱《IAM 使用者指南》中的需要根使用者憑證的任務。

聯合身分

最佳作法是要求人類使用者 (包括需要系統管理員存取權的使用者) 使用與身分識別提供者的同盟，才能使用臨時登入資料進行存取 AWS 服務 。

聯合身分識別是來自企業使用者目錄的使用者、Web 身分識別提供者、Identi ty Center 目錄，或使用透過身分識別來源提供的認證進行存取 AWS 服務 的任何使用者。 AWS Directory Service同盟身分存取時 AWS 帳戶，他們會假設角色，而角色則提供臨時認證。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，也可以連線並同步到自己身分識別來源中的一組使用者和群組，以便在所有應用程式 AWS 帳戶 和應用程式中使用。如需 IAM Identity Center 的相關資訊，請參閱《AWS IAM Identity Center 使用者指南》中的什麼是 IAM Identity Center？。

IAM 使用者和群組

IAM 使用者是您內部的身分，具 AWS 帳戶 有單一人員或應用程式的特定許可。建議您盡可能依賴暫時憑證，而不是擁有建立長期憑證 (例如密碼和存取金鑰)的 IAM 使用者。但是如果特定使用案例需要擁有長期憑證的 IAM 使用者，建議您輪換存取金鑰。如需詳細資訊，請參閱 IAM 使用者指南中的為需要長期憑證的使用案例定期輪換存取金鑰。

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

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

IAM 角色

IAM 角色是您 AWS 帳戶 內部具有特定許可的身分。它類似 IAM 使用者，但不與特定的人員相關聯。您可以切換角色，在中暫時擔任 IAM 角色。 AWS Management Console 您可以透過呼叫 AWS CLI 或 AWS API 作業或使用自訂 URL 來擔任角色。如需使用角色方法的相關資訊，請參閱《IAM 使用者指南》中的使用 IAM 角色。

使用暫時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並取得由角色定義的許可。如需有關聯合角色

的詳細資訊，請參閱《IAM 使用者指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-idp.html中的為第三方身分供應商建立角色。如果您使用 IAM Identity Center，則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 中的角色相關聯。如需有關許可集的資訊，請參閱《AWS IAM Identity Center 使用者指南》中的許可集。

- 暫時 IAM 使用者許可 – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 跨帳户存取權 – 您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的委託人)存取您帳戶中的資源。角色是授予跨帳戶存取權的主要方式。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資源（而不是使用角色作為代理）。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 角色與資源類型政策的差異。
- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (Amazon S3) 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉寄存取工作階段 (FAS) — 當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。當您使用某些服務時，您可能會執行一個動作，而該動作之後會在不同的服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。
  - 服務角色：服務角色是服務擔任的 IAM 角色，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以委派許可給 AWS 服務服務。
  - 服務連結角色 — 服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。
- 在 Amazon EC2 上執行的應用程式 — 您可以使用 IAM 角色來管理在 EC2 執行個體上執行的應用程式以及發出 AWS CLI 或 AWS API 請求的臨時登入資料。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體並提供給其所有應用程式，請建立連接至執行個體的執行個體設定檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得暫時憑證。如需詳細資訊，請參閱《IAM 使用者指南》中的利用 IAM 角色來授予許可給 Amazon EC2 執行個體上執行的應用程式。

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

使用政策管理存取權

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

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

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

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

身分型政策

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

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

資源型政策

資源型政策是連接到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

資源型政策是位於該服務中的內嵌政策。您無法在以資源為基礎的政策中使用 IAM 的 AWS 受管政策。

存取控制清單 (ACL)

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

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

其他政策類型

AWS 支援其他較不常見的原則類型。這些政策類型可設定較常見政策類型授與您的最大許可。

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

如何與 IAM AWS Audit Manager 搭配使用

在您使用 IAM 管理 Audit Manager 的存取權之前，請了解搭配 Audit Manager 使用的 IAM 功能有哪些。

您可以搭配使用的 IAM 功能 AWS Audit Manager

IAM 功能	Audit Manager 報告
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	部分
ACL	否
ABAC (政策中的標籤)	是
臨時憑證	是
轉送存取工作階段 (FAS)	是
服務角色	否
服務連結角色	是

若要深入瞭解如何以 AWS Audit Manager 及其他 AWS 服務如何使用大多數 IAM 功能，請參閱 IAM 使用者指南中的搭配 IAM 使用的AWS 服務。

以身分識別為基礎的原則 AWS Audit Manager

支援身分型政策	是

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

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。若要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素參考。

AWS Audit Manager 會建立為稽核管理員管理員命名AWSAuditManagerAdministratorAccess的受管理策略。此政策會授予稽核管理員中的完整管理存取權。管理員可以將此政策附加至任何現有的角色或使用者，或使用此政策建立新角色。

中使用者角色的建議政策 AWS Audit Manager

AWS Audit Manager 可讓您使用不同的 IAM 政策，維護不同使用者之間的職責隔離，以及針對不同稽核。Audit Manager 中的兩個角色及其建議政策的定義如下。

角色	描述和建議政策
稽核擁有者	• 此角色必須具有管理中 AWS Audit Manager評量的必要權限。 • 建議用於此角色的受管理策略是名AWSAuditManagerAdministratorAccess為的受管理策略。您可以使用此政策作為起點，根據需要縮小這些許可的範圍。
委派代表	• 此角色可存取評估中委派的控制集。可以更新控制項狀態、添加評論、提交控制集以供審核，以及將證據添加至評估報告。 • 建議用於此角色的政策為下列範例政策：授予使用者 AWS Audit Manager的完整管理員存取權。您可以使用此政策作為起點，根據您的需求進行必要的變更。

以身分識別為基礎的原則範例 AWS Audit Manager

如需檢視 Audit Manager 身分型政策範例，請參閱 以身分識別為基礎的原則範例 AWS Audit Manager。

以資源為基礎的政策 AWS Audit Manager

支援以資源基礎的政策	否

資源型政策是附加到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源

的存取權。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。AWS 服務

若要啟用跨帳戶存取權，您可以指定在其他帳戶內的所有帳戶或 IAM 實體，作為資源型政策的主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主體和資源位於不同時 AWS 帳戶，受信任帳戶中的 IAM 管理員也必須授與主體實體 (使用者或角色) 權限，才能存取資源。其透過將身分型政策附加到實體來授予許可。不過，如果資源型政策會為相同帳戶中的主體授予存取，這時就不需要額外的身分型政策。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 角色與資源型政策有何差異。

的政策動作 AWS Audit Manager

支援政策動作	是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON 政策的 `Action` 元素描述您可以用來允許或拒絕政策中存取的動作。原則動作通常與關聯的 AWS API 作業具有相同的名稱。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。也有一些操作需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授與執行相關聯操作的許可。

若要查看 AWS Audit Manager 動作清單，請參閱服務授權參考中的 AWS Audit Manager 定義的動作。

中的策略動作在動作之前 AWS Audit Manager 使用下列前置詞。

```
auditmanager
```

如需在單一陳述式中指定多個動作，請用逗號分隔。

```
"Action": [
      "auditmanager:GetEvidenceDetails",
      "auditmanager:GetEvidenceEventDetails"
         ]
```

您也可以使用萬用字元 (*) 來指定多個動作。例如，如需指定開頭是 Get 文字的所有動作，請包含以下動作：

```
"Action": "auditmanager:Get*"
```

如需檢視 Audit Manager 身分型政策範例，請參閱 以身分識別為基礎的原則範例 AWS Audit Manager。

的政策資源 AWS Audit Manager

支援政策資源	是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Resource JSON 政策元素可指定要套用動作的物件。陳述式必須包含 Resource 或 NotResource 元素。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出作業)，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 AWS Audit Manager 資源類型及其 ARN 的清單，請參閱服務授權參考中的 AWS Audit Manager 定義的資源。如需了解您可以使用哪些動作指定每個資源的 ARN，請參閱 AWS Audit Manager 定義的動作。

Audit Manager 的評估具有以下 Amazon Resource Name (ARN) 格式：

```
arn:${Partition}:auditmanager:${Region}:${Account}:assessment/${assessmentId}
```

Audit Manager 控制集具有以下 ARN 格式：

```
arn:${Partition}:auditmanager:${Region}:${Account}:assessment/
${assessmentId}controlSet/${controlSetId}
```

Audit Manager 控制項具有以下 ARN 格式：

```
arn:${Partition}:auditmanager:${Region}:${Account}:control/${controlId}
```

如需 ARN 格式的詳細資訊，請參閱 Amazon Resource Name (ARN)。

例如，如需在陳述式中指定 i-1234567890abcdef0 評估，請使用下列 ARN。

```
"Resource": "arn:aws:auditmanager:us-east-1:123456789012:assessment/
i-1234567890abcdef0"
```

如需指定屬於特定帳戶的所有執行個體，請使用萬用字元 (*)。

```
"Resource": "arn:aws:auditmanager:us-east-1:123456789012:assessment/*"
```

有些 Audit Manager 動作 (例如用來建立資源的動作) 無法在特定資源上執行。在這些情況下，您必須使用萬用字元 (*)。

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

許多 Audit Manager API 動作都涉及多個資源。例如，ListAssessments傳回目前登入者可存取的評估中繼資料清單 AWS 帳戶。因此，使用者必須具有檢視評估的許可。若要在單一陳述式中指定多項資源，請使用逗號分隔 ARN。

```
"Resource": [
      "resource1",
      "resource2"
```

如需查看 Audit Manager 資源類型及其 ARN 的清單，請參閱 IAM 使用者指南中的 AWS Audit Manager定義的資源。如需了解您可以使用哪些動作指定每個資源的 ARN，請參閱 AWS Audit Manager定義的動作。

部分 Audit Manager API 動作支援多個資源。例如，GetChangeLogs 存取 assessmentID、和 controlID 和 controlSetId，因此主體必須具有存取這些資源的許可。若要在單一陳述式中指定多項資源，請使用逗號分隔 ARN。

```
"Resource": [
      "assessmentId",
      "controlId",
```

```
        "controlSetId"
```

的政策條件索引鍵 AWS Audit Manager

支援服務特定政策條件金鑰	部分

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素 (或 Condition 區塊)可讓您指定使陳述式生效的條件。Condition 元素是選用項目。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

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

當政策陳述式中的主體是 AWS 服務主體時，強烈建議您使用政策中的 aws:SourceArn 或 aws:SourceAccount 全域條件索引鍵。您可以使用這些全域條件內容索引鍵來協助防止混淆代理人案例。下列記錄的政策示範如何使用 Audit Manager 中的 aws:SourceArn 和 aws:SourceAccount 全域條件內容索引鍵，來預防混淆代理人問題。

- 用於 Audit Manager 通知的 SNS 主題範例政策
- 與 SNS 主題搭配使用的 KMS 金鑰範例政策

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使用者名稱標記時，將存取資源的許可授予該使用者。如需詳細資訊，請參閱 IAM 使用者指南中的 IAM 政策元素：變數和標籤。

Audit Manager 不提供任何服務專用條件索引鍵，但它支援一些全域條件索引鍵的使用。若要查看所有 AWS 全域條件金鑰，請參閱《IAM 使用者指南》中的AWS 全域條件內容金鑰。

AWS Audit Manager中的存取控制清單 (ACL)

支援 ACL	否

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

以屬性為基礎的存取控制 (ABAC) 搭配 AWS Audit Manager

支援 ABAC (政策中的標籤)	是

屬性型存取控制 (ABAC) 是一種授權策略，可根據屬性來定義許可。在中 AWS，這些屬性稱為標籤。您可以將標籤附加到 IAM 實體 (使用者或角色) 和許多 AWS 資源。為實體和資源加上標籤是 ABAC 的第一步。您接著要設計 ABAC 政策，允許在主體的標籤與其嘗試存取的資源標籤相符時操作。

ABAC 在成長快速的環境中相當有幫助，並能在政策管理變得繁瑣時提供協助。

若要根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件金鑰，在政策的條件元素中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需 ABAC 的詳細資訊，請參閱《IAM 使用者指南》中的「什麼是 ABAC?」。如要查看含有設定 ABAC 步驟的教學課程，請參閱《IAM 使用者指南》中的使用屬性型存取控制 (ABAC)。

如需標記 AWS Audit Manager 資源的更多資訊，請參閱標記 AWS Audit Manager 資源。

使用臨時登入資料 AWS Audit Manager

支援臨時憑證	是

當您使用臨時憑據登錄時，某些 AWS 服務 不起作用。如需其他資訊，包括哪些 AWS 服務 與臨時登入資料搭配AWS 服務 使用，請參閱 IAM 使用者指南中的 IAM。

如果您使用除了使用者名稱和密碼以外的任何方法登入，則您正在 AWS Management Console 使用臨時認證。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取時，該程序會自動建立暫時認證。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需切換角色的相關資訊，請參閱《IAM 使用者指南》中的切換至角色 (主控台)。

您可以使用 AWS CLI 或 AWS API 手動建立臨時登入資料。然後，您可以使用這些臨時登入資料來存取 AWS。 AWS 建議您動態產生臨時登入資料，而非使用長期存取金鑰。如需詳細資訊，請參閱 IAM 中的暫時性安全憑證。

轉寄存取工作階段 AWS Audit Manager

支援轉寄存取工作階段 (FAS)	是

當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。當您使用某些服務時，您可能會執行一個動作，而該動作之後會在不同的服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。

AWS Audit Manager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給 AWS 服務服務。

> **Warning**
>
> 變更服務角色的許可有可能會讓 AWS Audit Manager 功能出現故障。只有 Audit Manager 提供指引時，才能編輯服務角色。

服務連結角色 AWS Audit Manager

支援服務連結角色	是

服務連結角色是一種連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需有關的服務連結角色的詳細資訊 AWS Audit Manager，請參閱使用服務連結角色 AWS Audit Manager。

以身分識別為基礎的原則範例 AWS Audit Manager

根據預設，使用者和角色不具備建立或修改 Audit Manager 資源的權限。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 來執行工作。若要授與使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

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。

如需 AWS Audit Manager 所定義之動作和資源類型的詳細資訊，包括每種資源類型的 ARN 格式，請參閱服務授權參考中的適用 AWS Audit Manager 的動作、資源和條件索引鍵。

主題

政策最佳實務

身分型政策會判斷您帳戶中的某個人員是否可以建立、存取或刪除 Audit Manager 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，請遵循下列指導方針及建議事項：

- 開始使用 AWS 受管原則並邁向最低權限權限 — 若要開始授與使用者和工作負載的權限，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們可用在您的 AWS 帳戶. 建議您透過定義特定於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。如需詳細資訊，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之許可。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權。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。您也可以使用條件來授與對服務動作的存取權 (如透過特定) 使用這些動作 AWS 服務，例如 AWS CloudFormation。如需詳細資訊，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，可協助您編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 IAM Access Analyzer 政策驗證。
- 需要多因素身份驗證 (MFA) — 如果您的案例需要 IAM 使用者或根使用者 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。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 使用者指南中的設定 MFA 保護的 API 存取。

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

允許啟用 Audit Manager 所需的最低許可

此範例會示範如何允許不具有管理員角色的帳戶啟用 AWS Audit Manager。

> **Note**
>
> 我們在此提供的是基本政策，可授予啟用 Audit Manager 所需的最低许可。以下政策中的所有许可均属必要许可。您不得省略此政策的任何部分，否則，您將無法啟用 Audit Manager。我們建議您花時間自訂權限，以滿足您的特定需求。如需任何協助，請聯絡您的管理員或 Amazon Web Services Support。

如需授予啟用 Audit Manager 所需的最低存取權，請使用下列許可。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "auditmanager:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
```

```
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        },
        {
            "Sid": "CreateEventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutRule"
            ],
            "Resource": "*",
            "Condition": {
                "ForAllValues:StringEquals": {
                    "events:source": [
                        "aws.securityhub"
                    ]
                }
            }
        },
        {
            "Sid": "EventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/
AuditManagerSecurityHubFindingsReceiver"
        },
        {
            "Effect": "Allow",
            "Action": "kms:ListAliases",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        }
    ]
}
```

您不需要為僅對 AWS CLI 或 AWS API 進行呼叫的使用者允許最低主控台權限。反之，只需允許存取符合您嘗試執行之 API 操作的動作就可以了。

授予使用者 AWS Audit Manager的完整管理員存取權

下列範例原則會授與對的完整管理員存取權 AWS Audit Manager。

- 範例 1 (受管政策，AWSAuditManagerAdministratorAccess)
- 範例 2 (評估報表目的地許可)
- 範例 3 (匯出目的地許可)
- 範例 4 (啟用證據搜尋工具的許可)
- 範例 5 (停用證據搜尋工具的許可)

範例 1 (受管政策，**AWSAuditManagerAdministratorAccess**)

本範例中此政策屬於受管政策 AWSAuditManagerAdministratorAccess。此政策包括啟用和停用 Audit Manager、變更 Audit Manager 設定以及管理所有 Audit Manager 資源 (例如評估、架構、控制項和評估報告) 的能力。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "OrganizationsAccess",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren"
```

```
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowOnlyAuditManagerIntegration",
            "Effect": "Allow",
            "Action": [
                "organizations:RegisterDelegatedAdministrator",
                "organizations:DeregisterDelegatedAdministrator",
                "organizations:EnableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:ServicePrincipal": [
                        "auditmanager.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "IAMAccess",
            "Effect": "Allow",
            "Action": [
                "iam:GetUser",
                "iam:ListUsers",
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMAccessCreateSLR",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        },
        {
            "Sid": "IAMAccessManageSLR",
```

```
            "Effect": "Allow",
            "Action": [
                "iam:DeleteServiceLinkedRole",
                "iam:UpdateRoleDescription",
                "iam:GetServiceLinkedRoleDeletionStatus"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*"
        },
        {
            "Sid": "S3Access",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsAccess",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListKeys",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsCreateGrantAccess",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                },
                "StringLike": {
                    "kms:ViaService": "auditmanager.*.amazonaws.com"
                }
            }
        },
        {
```

```
            "Sid": "SNSAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateEventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutRule"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "events:detail-type": "Security Hub Findings - Imported"
                },
                "ForAllValues:StringEquals": {
                    "events:source": [
                        "aws.securityhub"
                    ]
                }
            }
        },
        {
            "Sid": "EventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:DeleteRule",
                "events:DescribeRule",
                "events:EnableRule",
                "events:DisableRule",
                "events:ListTargetsByRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/
AuditManagerSecurityHubFindingsReceiver"
        },
        {
            "Sid": "TagAccess",
            "Effect": "Allow",
            "Action": [
```

```
                "tag:GetResources"
            ],
            "Resource": "*"
        }
    ]
}
```

範例 2 (評估報表目的地許可)

此政策授予您存取特定 S3 儲存貯體，以及在其中添加檔案和刪除檔案的許可。因此，您可使用指定的儲存貯體作為 Audit Manager 中的評估報告目的地。

以您自己的資訊取代*######*。包括用作評估報告目的地的 S3 儲存貯體，以及用於加密評估報告的 KMS 金鑰。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
               "s3:PutObject",
               "s3:GetObject",
               "s3:ListBucket",
               "s3:DeleteObject",
               "s3:GetBucketLocation",
               "s3:PutObjectAcl"
            ],
            "Resource": "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET/*"
        }
    ]
},
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:Encrypt",
                "kms:GenerateDataKey"
            ],
```

```
            "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ]
}
```

範例 3 (匯出目的地許可)

下列政策允許 CloudTrail 將證據尋找器查詢結果傳遞至指定的 S3 儲存貯體。作為安全性最佳實務，IAM 全域條件金鑰aws:SourceArn有助於確保僅針對事件資料存放區 CloudTrail 寫入 S3 儲存貯體。

以您自己的資訊取代######，如下所示：

- 將 *DOC-EXAMPLE-DESTINATION-BUCKET* 取代為您用作匯出目的地的 S3 儲存貯體。
- 將 [*myQueryRunning##*] 取代 AWS 區域 為適合您組態的 [區域]。
- 將我的*## AWS ## ID* 取代為使用的識別碼。 CloudTrail此 ID 可能不同於 S3 儲存貯體的 AWS 帳戶 ID。如果這是組織事件資料存放區，您必須使 AWS 帳戶 用管理帳戶。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
                "s3:PutObject*",
                "s3:Abort*"
            ],
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET",
                "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET/*"
            ],
            "Condition": {
                "StringEquals": {
                    "AWS:SourceArn":
 "arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
                }
            }
```

```
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET",
            "Condition": {
                "StringEquals": {
                    "AWS:SourceArn":
 "arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt*",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt*",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        }
    ]
}
```

範例 4 (啟用證據搜尋工具的許可)

如需啟用和使用證據搜尋工具功能，則需要以下許可政策。此原則陳述式可讓 Audit Manager 建立 CloudTrail Lake 事件資料存放區並執行搜尋查詢。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
           "Sid": "ManageCloudTrailLakeQueryAccess",
           "Effect": "Allow",
           "Action": [
               "cloudtrail:StartQuery",
               "cloudtrail:DescribeQuery",
               "cloudtrail:GetQueryResults",
               "cloudtrail:CancelQuery"
           ],
           "Resource": "arn:aws:cloudtrail:*:*:eventdatastore/*"
        },
        {
           "Sid": "ManageCloudTrailLakeAccess",
           "Effect": "Allow",
           "Action": [
                "cloudtrail:CreateEventDataStore"
           ],
           "Resource": "arn:aws:cloudtrail:*:*:eventdatastore/*"
         }
    ]
}
```

範例 5 (停用證據搜尋工具的許可)

此範例政策授予在 Audit Manager 中停用證據搜尋工具功能的許可。這涉及刪除您第一次啟用該功能時建立的事件資料存放區。

使用此政策前，請將######取代為您的資訊。您應該指定啟用證據搜尋工具時建立的事件資料存放區的 UUID。您可以從 Audit Manager 設定中擷取事件資料存放區的 ARN。如需詳細資訊，請參閱 AWS Audit Manager API 參考中的 GetSettings。

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

```
            "Effect": "Allow",
            "Action": [
               "cloudtrail:DeleteEventDataStore",
               "cloudtrail:UpdateEventDataStore"
            ],
            "Resource": "arn:aws:cloudtrail:::event-data-store-UUID"
        }
    ]
}
```

授予使用者 AWS Audit Manager管理存取權

此範例會示範如何授予非管理員 AWS Audit Manager管理存取權。

此策略授予管理所有 Audit Manager 資源 (評估、架構和控制項) 的能力，但不授予啟用或停用 Audit Manager 或修改 Audit Manager 設定的能力。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:GetAccountStatus",
                "auditmanager:ListAssessmentFrameworks",
                "auditmanager:CreateAssessmentFramework",
                "auditmanager:GetAssessmentFramework",
                "auditmanager:UpdateAssessmentFramework",
                "auditmanager:DeleteAssessmentFramework",
                "auditmanager:ListAssessmentReports",
                "auditmanager:ListAssessments",
                "auditmanager:CreateAssessment",
                "auditmanager:ListControls",
                "auditmanager:CreateControl",
                "auditmanager:GetControl",
                "auditmanager:UpdateControl",
                "auditmanager:DeleteControl",
                "auditmanager:ListKeywordsForDataSource",
                "auditmanager:GetDelegations",
                "auditmanager:ValidateAssessmentReportIntegrity",
                "auditmanager:ListNotifications",
                "auditmanager:GetServicesInScope",
```

```
                "auditmanager:GetSettings",
                "auditmanager:ListTagsForResource",
                "auditmanager:TagResource",
                "auditmanager:UntagResource"
            ],
            "Resource": "*"
        },
        {
            "Sid": "OrganizationsAccess",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMAccess",
            "Effect": "Allow",
            "Action": [
                "iam:GetUser",
                "iam:ListUsers",
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "S3Access",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsAccess",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
```

```
                "kms:ListKeys",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SNSAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Sid": "TagAccess",
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*"
        }
    ]
}
```

允許使用者唯讀存取 AWS Audit Manager

此原則授予評估、架構和控制等 AWS Audit Manager 資源的唯讀存取權。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:Get*",
                "auditmanager:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

允許使用者檢視他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視附加到他們使用者身分的內嵌及受管政策。此原則包含在主控台上或以程式設計方式使用 AWS CLI 或 AWS API 完成此動作的權限。

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

允許 AWS Audit Manager 傳送通知給 Amazon SNS 主題

此範例中的政策授予 Audit Manager 傳送通知到現有 Amazon SNS 主題的許可。

- 範例 1 — 如果您想要接收來自 Audit Manager 的通知，請使用此範例將許可添加至您的 SNS 主題存取政策。
- 範例 2 — 如果您的 SNS 主題使用 AWS Key Management Service (AWS KMS) 進行伺服器端加密 (SSE)，請使用此範例將權限新增至 KMS 金鑰存取原則。

在下列政策中，取得許可的主體是 Audit Manager 服務主體，即 auditmanager.amazonaws.com。當政策陳述式中的主體是 AWS 服務主體時，強烈建議您使用政策中的 aws:SourceArn 或 aws:SourceAccount 全域條件索引鍵。您可以使用這些全域條件內容索引鍵來協助防止混淆代理人案例。

範例 1 (SNS 主題的許可)

此政策陳述式允許 Audit Manager 將事件發佈至特定 SNS 主題。任何發佈至指定 SNS 主題的要求都必須符合政策條件。

使用此政策前，請將######取代為您的資訊。謹記下列事項：

- 如果您在此政策中使用 aws:SourceArn 條件索引鍵，則該值必須是通知來源之 Audit Manager 資源的 ARN。在以下範例中，aws:SourceArn 使用萬用字元 (*) 作為資源 ID。這允許對所有 Audit Manager 資源進行來自 Audit Manager 的所有請求。透過 aws:SourceArn 全域條件索引鍵，您可以使用 StringLike 或 ArnLike 條件運算子。最佳實務建議您使用 ArnLike。
- 透過 aws:SourceAccount 條件索引鍵，您可以使用 StringEquals 或 StringLike 條件運算子。最佳作法是，建議您使用 StringEquals 來實作最低權限。
- 如果您同時使用 aws:SourceAccount 和 aws:SourceArn，帳戶值必須顯示相同的帳戶 ID。

```
{
  "Version": "2012-10-17",
  "Statement": {
      "Sid": "AllowAuditManagerToUseSNSTopic",
      "Effect": "Allow",
      "Principal": {
        "Service": "auditmanager.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:accountID:topicName",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "accountID"
```

```
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:auditmanager:region:accountID:*"
        }
      }
    }
}
```

透過 StringLike 條件運算子，下列替代範例僅使用 aws:SourceArn 條件索引鍵：

```
    "Condition": {
      "StringLike": {
        "aws:SourceArn": "arn:aws:auditmanager:region:accountID:*"
      }
    }
```

透過 StringLike 條件運算子，下列替代範例僅使用 aws:SourceAccount 條件索引鍵：

```
  "Condition": {
    "StringLike": {
      "aws:SourceAccount": "accountID"
    }
  }
```

範例 2 (添加至 SNS 主題之 KMS 金鑰的許可)

政策陳述式允許 Audit Manager 使用 KMS 金鑰產生資料金鑰，它可用來加密 SNS 主題。針對指定操作使用 KMS 金鑰的任何請求都必須滿足政策條件。

使用此政策前，請將######取代為您的資訊。謹記下列事項：

- 如果您在此政策中使用 aws:SourceArn 條件索引鍵，則值必須是正在加密之資源的 ARN。例如，在這種情況下，它是您帳戶中的 SNS 主題。將值設定為 ARN 或具有萬用字元 (*) 的 ARN 模式。透過 aws:SourceArn 條件索引鍵，您可以使用 StringLike 或 ArnLike 條件運算子。最佳實務建議您使用 ArnLike。
- 透過 aws:SourceAccount 條件索引鍵，您可以使用 StringEquals 或 StringLike 條件運算子。最佳作法是，建議您使用 StringEquals 來實作最低權限。如果您不知道 SNS 主題的 ARN，可以使用 aws:SourceAccount。
- 如果您同時使用 aws:SourceAccount 和 aws:SourceArn，帳戶值必須顯示相同的帳戶 ID。

```
{
     "Version": "2012-10-17",
     "Statement": {
       "Sid": "AllowAuditManagerToUseKMSKey",
       "Effect": "Allow",
       "Principal": {
           "Service": "auditmanager.amazonaws.com"
       },
       "Action": [
           "kms:Decrypt",
           "kms:GenerateDataKey"
       ],
       "Resource": "arn:aws:kms:region:accountID:key/*",
       "Condition": {
           "StringEquals": {
                "aws:SourceAccount": "accountID"
            }
            "ArnLike": {
                 "aws:SourceArn": "arn:aws:sns:region:accountID:topicName"
            }
      }
    }
  ]
}
```

透過 StringLike 條件運算子，下列替代範例僅使用 aws:SourceArn 條件索引鍵：

```
      "Condition": {
        "StringLike": {
          "aws:SourceArn": "arn:aws:sns:region:accountID:topicName"
        }
      }
```

透過 StringLike 條件運算子，下列替代範例僅使用 aws:SourceAccount 條件索引鍵：

```
   "Condition": {
     "StringLike": {
       "aws:SourceAccount": "accountID"
     }
    }
```

允許使用者在證據搜尋工具中執行搜索查詢

下列原則授與對 CloudTrail Lake 事件資料存放區執行查詢的權限。如需使用證據搜尋工具功能，則需要此許可政策。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageCloudTrailLakeQueryAccess",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:StartQuery",
                "cloudtrail:DescribeQuery",
                "cloudtrail:GetQueryResults",
                "cloudtrail:CancelQuery"
            ],
            "Resource": "*"
        }
    ]
}
```

預防跨服務混淆代理人

混淆代理人問題屬於安全性問題，其中沒有執行動作許可的實體可以強制具有更多許可的實體執行該動作。在中 AWS，跨服務模擬可能會導致混淆的副問題。在某個服務 (呼叫服務)呼叫另一個服務 (被呼叫服務)時，可能會發生跨服務模擬。可以操縱呼叫服務來使用其許可，以在未經許可的情況下對其他客戶的資源採取動作。為了預防這種情況，Amazon Web Services 提供的工具可協助您保護所有服務的資料，而這些服務主體已獲得您帳戶中資源的存取權。

我們建議在資源策略中使用`aws:SourceArn`和`aws:SourceAccount`全域條件前後關聯鍵字，以限制授 AWS Audit Manager 予其他服務以存取您資源的權限。

- 如果您想要僅允許一個資源與跨服務存取權相關聯，則請使用 `aws:SourceArn`。如需指定多個資源，您也可以使用萬用字元 (*) `aws:SourceArn`。

  例如，您可以使用 Amazon SNS 主題接收來自 Audit Manager 的活動通知。在此情況下，在您的 SNS 主題存取政策中，`aws:SourceArn` 的 ARN 值是作為通知來源的 Audit Manager 資源。因為

您可能有多個 Audit Manager 資源，因此建議您使用萬用字元 aws:SourceArn。因此，您可在 SNS 主題存取政策中指定所有 Audit Manager 資源。

- 如果您想要允許該帳戶中的任何資源與跨服務使用相關聯，請使用 aws:SourceAccount。
- 如果 aws:SourceArn 值不包含帳戶 ID (例如 Amazon Simple Storage Service (Amazon S3) 儲存貯體 ARN)，則必須使用這兩個全域條件內容索引鍵來限制許可。
- 如果使用兩項條件，且如果 aws:SourceArn 值包含帳戶 ID，則在相同政策陳述式中使用 aws:SourceAccount 值和 aws:SourceArn 值中的帳戶時，必須顯示相同的帳戶 ID。
- 防範混淆代理人問題的最有效方法是使用 aws:SourceArn 全域條件內容索引鍵，以及資源的完整 ARN。如果不知道資源的完整 Amazon Resource Name (ARN)，或者如果您指定了多個資源，請使用 aws:SourceArn 全域內容條件索引鍵搭配萬用字元 (*) 來表示 ARN 的未知部分。例如 arn:aws:*servicename*:*:*123456789012*:*。

Audit Manager 混淆代理人支援

Audit Manager 在下列情況下會提供混淆代理人支援。下列政策範例示範如何使用 aws:SourceArn 和 aws:SourceAccount 條件索引鍵來預防混淆代理人問題。

- 範例政策：您用來接收 Audit Manager 通知的 SNS 主題
- 範例政策：您用來加密 SNS 主題的 KMS 金鑰

Audit Manager 不會為您在 Audit Manager 資料加密 設定中提供的客戶管理金鑰提供混淆代理人支援。如果您提供了自己的客戶管理金鑰，則無法在該 KMS 金鑰政策中使用 aws:SourceAccount 或 aws:SourceArn 條件。

AWS 受管理的政策 AWS Audit Manager

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

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

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

如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

主題

AWS 受管理的策略： AWSAuditManagerAdministratorAccess

您可將 `AWSAuditManagerAdministratorAccess` 政策連接到 IAM 身分。

此原則會授與允許完整管理存取權的管理權限 AWS Audit Manager。此存取權包括啟用和停用 AWS Audit Manager、變更中 AWS Audit Manager的設定以及管理所有 Audit Manager 資源 (例如評估、架構、控制項和評估報告) 的功能。

AWS Audit Manager 需要跨多個 AWS 服務的廣泛權限。這是因為與多項 AWS 服務 AWS Audit Manager 整合，可自動從評估範圍內的 AWS 帳戶 和服務收集證據。

許可詳細資訊

此政策包含以下許可：

- `Audit Manager` — 授予主體 AWS Audit Manager 資源的完整許可。
- `Organizations` — 授予主體列出帳號和組織單位，以及註冊或取消註冊委派管理員。這是必要的，以便您可以啟用多帳戶支援，並允許 AWS Audit Manager 對多個帳戶執行評估，並將證據合併到委派的管理員帳戶中。
- `iam` — 允許主體取得和列出 IAM 中使用者，以及建立服務連結角色。這是必要的，以便您可以指定評估的稽核擁有者和代理人。此政策也允許主體刪除服務連結角色，並擷取刪除狀態。這是必要的， AWS Audit Manager 以便在您選擇停用中的服務時清除資源並刪除服務連結角色。 AWS Management Console
- `s3` — 允許主體列出可用 Amazon Simple Storage Service (Amazon S3) 儲存貯體。這是必要的，以便您可以指定您要在其中存放證據報告或上傳手動證據的 S3 儲存貯體。
- `kms` — 允許主體列出和描述金鑰、列出別名以及建立授權。這是必要的，以便您可以選擇客戶管理金鑰進行資料加密。
- `sns` — 允許主體列出 Amazon SNS 中的訂閱主題。這是必要的，以便您可以指定您希望作為 AWS Audit Manager 傳送通知目的地的 SNS 主題。
- `events`-允許主參與者從 AWS Security Hub中列出及管理檢查。這是必要的， AWS Audit Manager 以便能夠自動收集受監視之 AWS 服務的 AWS Security Hub 發現項目 AWS Security Hub。然後，它可以將此資料轉換為證據，以包含在您的 AWS Audit Manager 評估中。

- tag — 允許主體擷取已標籤化的資源。這是必要的，以便您可以在 AWS Audit Manager中瀏覽架構、控制項和評估時使用標籤作為搜尋篩選條件。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "OrganizationsAccess",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowOnlyAuditManagerIntegration",
            "Effect": "Allow",
            "Action": [
                "organizations:RegisterDelegatedAdministrator",
                "organizations:DeregisterDelegatedAdministrator",
                "organizations:EnableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:ServicePrincipal": [
                        "auditmanager.amazonaws.com"
                    ]
```

```
                }
            }
        },
        {
            "Sid": "IAMAccess",
            "Effect": "Allow",
            "Action": [
                "iam:GetUser",
                "iam:ListUsers",
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMAccessCreateSLR",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        },
        {
            "Sid": "IAMAccessManageSLR",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteServiceLinkedRole",
                "iam:UpdateRoleDescription",
                "iam:GetServiceLinkedRoleDeletionStatus"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*"
        },
        {
            "Sid": "S3Access",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
```

```
        {
            "Sid": "KmsAccess",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListKeys",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsCreateGrantAccess",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                },
                "StringLike": {
                    "kms:ViaService": "auditmanager.*.amazonaws.com"
                }
            }
        },
        {
            "Sid": "SNSAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateEventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutRule"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "events:detail-type": "Security Hub Findings - Imported"
```

```
                },
                "ForAllValues:StringEquals": {
                    "events:source": [
                        "aws.securityhub"
                    ]
                }
            }
        },
        {
            "Sid": "EventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:DeleteRule",
                "events:DescribeRule",
                "events:EnableRule",
                "events:DisableRule",
                "events:ListTargetsByRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/
AuditManagerSecurityHubFindingsReceiver"
        },
        {
            "Sid": "TagAccess",
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 受管理的策略： AWSAuditManagerServiceRolePolicy

您不得將 AWSAuditManagerServiceRolePolicy 連接到 IAM 實體。此原則附加至服務連結角色AWSServiceRoleForAuditManager，可 AWS Audit Manager 讓您代表執行動作。如需詳細資訊，請參閱使用 AWS Audit Manager的服務連結角色。

角色許可政策，AWSAuditManagerServiceRolePolicy，允許 AWS Audit Manager 代表您執行下列動作來收集自動化證據：

- 從下列資料來源收集資料：
  - 管理事件 AWS CloudTrail
  - 符合性檢查來源 AWS Config 規則
  - 符合性檢查來源 AWS Security Hub
- 使用 API 呼叫描述下列 AWS 服務的資源組態。

> **Tip**
>
> 如需 Audit Manager 用來從這些服務收集證據之 API 呼叫的詳細資訊，請參閱本指南中的 自訂控制項資料來源支援的 API 呼叫。

  - AWS Certificate Manager
  - AWS Backup
  - Amazon Bedrock
  - AWS CloudTrail
  - Amazon CloudWatch
  - Amazon CloudWatch 日誌
  - Amazon Cognito 使用者集區
  - AWS Config
  - AWS Direct Connect
  - Amazon DynamoDB
  - Amazon EC2
  - Amazon Elastic Container Service
  - Amazon Elastic File System
  - Amazon Elastic Kubernetes Service
  - Amazon ElastiCache
  - Elastic Load Balancing
  - Amazon EMR
  - Amazon EventBridge
  - Amazon 數據 Firehose
  - Amazon FSx

- Amazon GuardDuty
- AWS Identity and Access Management (IAM)
- Amazon Kinesis
- AWS KMS
- AWS Lambda
- AWS License Manager
- Amazon Managed Streaming for Apache Kafka
- AWS Organizations
- Amazon Relational Database Service
- Amazon Redshift
- Amazon Route 53
- Amazon S3
- AWS Security Hub
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- AWS WAF

許可詳細資訊

`AWSAuditManagerServiceRolePolicy`允許 AWS Audit Manager 對指定的資源完成以下操作：

- `acm:GetAccountConfiguration`
- `acm:ListCertificates`
- `backup:ListRecoveryPointsByResource`
- `bedrock:GetCustomModel`
- `bedrock:GetFoundationModel`
- `bedrock:GetModelCustomizationJob`
- `bedrock:GetModelInvocationLoggingConfiguration`
- `bedrock:ListCustomModels`
- `bedrock:ListFoundationModels`
- `bedrock:ListModelCustomizationJobs`
- `cloudtrail:DescribeTrails`

- cloudtrail:LookupEvents
- cloudwatch:DescribeAlarms
- cloudwatch:DescribeAlarmsForMetric
- cloudwatch:GetMetricStatistics
- cloudwatch:ListMetrics
- cognito-idp:DescribeUserPool
- config:DescribeConfigRules
- config:DescribeDeliveryChannels
- config:ListDiscoveredResources
- directconnect:DescribeDirectConnectGateways
- directconnect:DescribeVirtualGateways
- dynamodb:DescribeTable
- dynamodb:ListBackups
- dynamodb:ListGlobalTables
- dynamodb:ListTables
- ec2:DescribeAddresses
- ec2:DescribeCustomerGateways
- ec2:DescribeEgressOnlyInternetGateways
- ec2:DescribeFlowLogs
- ec2:DescribeInstances
- ec2:DescribeInternetGateways
- ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations
- ec2:DescribeLocalGateways
- ec2:DescribeLocalGatewayVirtualInterfaces
- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSnapshots
- ec2:DescribeTransitGateways

- ec2:DescribeVolumes
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs
- ec2:DescribeVpnConnections
- ec2:DescribeVpnGateways
- ec2:GetEbsDefaultKmsKeyId
- ec2:GetEbsEncryptionByDefault
- ecs:DescribeClusters
- eks:DescribeAddonVersions
- elasticache:DescribeCacheClusters
- elasticache:DescribeServiceUpdates
- elasticfilesystem:DescribeAccessPoints
- elasticfilesystem:DescribeFileSystems
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeSslPolicies
- elasticloadbalancing:DescribeTargetGroups
- elasticmapreduce:ListClusters
- elasticmapreduce:ListSecurityConfigurations
- events:DeleteRule
- events:DescribeRule
- events:DisableRule
- events:EnableRule
- events:ListConnections
- events:ListEventBuses
- events:ListEventSources
- events:ListRules
- events:ListTargetsByRule
- events:PutRule
- events:PutTargets

- events:RemoveTargets
- firehose:ListDeliveryStreams
- fsx:DescribeFileSystems
- guardduty:ListDetectors
- iam:GenerateCredentialReport
- iam:GetAccountAuthorizationDetails
- iam:GetAccountPasswordPolicy
- iam:GetAccountSummary
- iam:GetCredentialReport
- iam:ListEntitiesForPolicy
- iam:ListGroupPolicies
- iam:ListGroups
- iam:ListOpenIdConnectProviders
- iam:ListPolicies
- iam:ListRolePolicies
- iam:ListRoles
- iam:ListSamlProviders
- iam:ListUserPolicies
- iam:ListUsers
- iam:ListVirtualMFADevices
- kafka:ListClusters
- kafka:ListKafkaVersions
- kinesis:ListStreams
- kms:DescribeKey
- kms:GetKeyPolicy
- kms:GetKeyRotationStatus
- kms:ListGrants
- kms:ListKeyPolicies
- kms:ListKeys
- lambda:ListFunctions

- license-manager:ListAssociationsForLicenseConfiguration
- license-manager:ListLicenseConfigurations
- license-manager:ListUsageForLicenseConfiguration
- logs:DescribeDestinations
- logs:DescribeExportTasks
- logs:DescribeLogGroups
- logs:DescribeMetricFilters
- logs:DescribeResourcePolicies
- logs:FilterLogEvents
- organizations:DescribeOrganization
- organizations:DescribePolicy
- rds:DescribeCertificates
- rds:DescribeDbClusterEndpoints
- rds:DescribeDbClusterParameterGroups
- rds:DescribeDbClusters
- rds:DescribeDBInstances
- rds:DescribeDbSecurityGroups
- redshift:DescribeClusters
- route53:GetQueryLoggingConfig
- s3:GetBucketPolicy
  - 此 API 動作會在可用位 AWS 帳戶 置的範圍內 service-linked-role 運作。它無法存取跨帳戶儲存貯體政策。
- s3:GetBucketPublicAccessBlock
- s3:GetBucketVersioning
- s3:GetEncryptionConfiguration
- s3:GetLifecycleConfiguration
- s3:ListAllMyBuckets
- securityhub:DescribeStandards
- sns:ListTopics
- sqs:ListQueues

- waf-regional:GetLoggingConfiguration
- waf-regional:ListRuleGroups
- waf-regional:ListSubscribedRuleGroups
- waf-regional:ListWebACLs
- waf:ListActivatedRulesInRuleGroup

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "acm:GetAccountConfiguration",
    "acm:ListCertificates",
    "backup:ListRecoveryPointsByResource",
    "bedrock:GetCustomModel",
    "bedrock:GetFoundationModel",
    "bedrock:GetModelCustomizationJob",
    "bedrock:GetModelInvocationLoggingConfiguration",
    "bedrock:ListCustomModels",
    "bedrock:ListFoundationModels",
    "bedrock:ListModelCustomizationJobs",
    "cloudtrail:DescribeTrails",
    "cloudtrail:LookupEvents",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:DescribeAlarmsForMetric",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics",
    "cognito-idp:DescribeUserPool",
    "config:DescribeConfigRules",
    "config:DescribeDeliveryChannels",
    "config:ListDiscoveredResources",
    "directconnect:DescribeDirectConnectGateways",
    "directconnect:DescribeVirtualGateways",
    "dynamodb:DescribeTable",
    "dynamodb:ListBackups",
    "dynamodb:ListGlobalTables",
    "dynamodb:ListTables",
    "ec2:DescribeAddresses",
    "ec2:DescribeCustomerGateways",
    "ec2:DescribeEgressOnlyInternetGateways",
```

```
    "ec2:DescribeFlowLogs",
    "ec2:DescribeInstances",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
    "ec2:DescribeLocalGateways",
    "ec2:DescribeLocalGatewayVirtualInterfaces",
    "ec2:DescribeNatGateways",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSnapshots",
    "ec2:DescribeTransitGateways",
    "ec2:DescribeVolumes",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcPeeringConnections",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpnConnections",
    "ec2:DescribeVpnGateways",
    "ec2:GetEbsDefaultKmsKeyId",
    "ec2:GetEbsEncryptionByDefault",
    "ecs:DescribeClusters",
    "eks:DescribeAddonVersions",
    "elasticache:DescribeCacheClusters",
    "elasticache:DescribeServiceUpdates",
    "elasticfilesystem:DescribeAccessPoints",
    "elasticfilesystem:DescribeFileSystems",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeSslPolicies",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticmapreduce:ListClusters",
    "elasticmapreduce:ListSecurityConfigurations",
    "events:DescribeRule",
    "events:ListConnections",
    "events:ListEventBuses",
    "events:ListEventSources",
    "events:ListRules",
    "firehose:ListDeliveryStreams",
    "fsx:DescribeFileSystems",
    "guardduty:ListDetectors",
    "iam:GenerateCredentialReport",
    "iam:GetAccountAuthorizationDetails",
    "iam:GetAccountPasswordPolicy",
    "iam:GetAccountSummary",
    "iam:GetCredentialReport",
```

```
    "iam:ListEntitiesForPolicy",
    "iam:ListGroupPolicies",
    "iam:ListGroups",
    "iam:ListOpenIdConnectProviders",
    "iam:ListPolicies",
    "iam:ListRolePolicies",
    "iam:ListRoles",
    "iam:ListSamlProviders",
    "iam:ListUserPolicies",
    "iam:ListUsers",
    "iam:ListVirtualMFADevices",
    "kafka:ListClusters",
    "kafka:ListKafkaVersions",
    "kinesis:ListStreams",
    "kms:DescribeKey",
    "kms:GetKeyPolicy",
    "kms:GetKeyRotationStatus",
    "kms:ListGrants",
    "kms:ListKeyPolicies",
    "kms:ListKeys",
    "lambda:ListFunctions",
    "license-manager:ListAssociationsForLicenseConfiguration",
    "license-manager:ListLicenseConfigurations",
    "license-manager:ListUsageForLicenseConfiguration",
    "logs:DescribeDestinations",
    "logs:DescribeExportTasks",
    "logs:DescribeLogGroups",
    "logs:DescribeMetricFilters",
    "logs:DescribeResourcePolicies",
    "logs:FilterLogEvents",
    "organizations:DescribeOrganization",
    "organizations:DescribePolicy",
    "rds:DescribeCertificates",
    "rds:DescribeDbClusterEndpoints",
    "rds:DescribeDbClusterParameterGroups",
    "rds:DescribeDbClusters",
    "rds:DescribeDBInstances",
    "rds:DescribeDbSecurityGroups",
    "redshift:DescribeClusters",
    "route53:GetQueryLoggingConfig",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetBucketVersioning",
    "s3:GetEncryptionConfiguration",
    "s3:GetLifecycleConfiguration",
```

```
    "s3:ListAllMyBuckets",
    "securityhub:DescribeStandards",
    "sns:ListTopics",
    "sqs:ListQueues",
    "waf-regional:GetLoggingConfiguration",
    "waf-regional:ListRuleGroups",
    "waf-regional:ListSubscribedRuleGroups",
    "waf-regional:ListWebACLs",
    "waf:ListActivatedRulesInRuleGroup"
   ],
   "Resource": "*",
   "Sid": "AuditManagerAPICallAccess"
  },
  {
   "Sid": "AuditManagerS3GetBucketPolicyAccess",
   "Effect": "Allow",
   "Action": [
    "s3:GetBucketPolicy"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": [
      "${aws:PrincipalAccount}"
     ]
    }
   }
  },
  {
   "Sid": "CreateEventsAccess",
   "Effect": "Allow",
   "Action": [
    "events:PutRule"
   ],
   "Resource": "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver",
   "Condition": {
    "StringEquals": {
     "events:detail-type": "Security Hub Findings - Imported"
    },
    "Null": {
     "events:source": "false"
    },
    "ForAllValues:StringEquals": {
     "events:source": [
```

```
      "aws.securityhub"
     ]
    }
   }
  },
  {
   "Sid": "EventsAccess",
   "Effect": "Allow",
   "Action": [
    "events:DeleteRule",
    "events:DescribeRule",
    "events:EnableRule",
    "events:DisableRule",
    "events:ListTargetsByRule",
    "events:PutTargets",
    "events:RemoveTargets"
   ],
   "Resource": "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
  }
 ]
}
```

AWS Audit ManagerAWS 受管理策略的更新

檢視 AWS Audit Manager 自此服務開始追蹤這些變更以來的 AWS 受管理策略更新詳細資料。如需有關此頁面變更的自動警示，請訂閱「 AWS Audit Manager 文件歷史記錄」頁面上的 RSS 摘要。

變更	描述	日期
AWSAuditManagerServiceRolePolicy – 更新現有政策	服務連結角色現在允 AWS Audit Manager 許執行動`s3:GetBucketPolicy` 作。 需要此 API 動作才能支援 AWS 生成式 AI 最佳實務架構 v1。它可讓 Audit Manager 收集有關您生成式 AI 模型資料訓練資料集之政策限制的自動化證據。 動`GetBucketPolicy` 作會在可用位 AWS 帳戶 置的範圍內 service-linked-role 運作。它無法存取跨帳戶儲存貯體政策。	12/06/2023

變更	描述	日期
AWSAuditManagerServiceRolePolicy – 更新現有政策	我們已將下列權限新增至AWSAuditManagerServiceRolePolicy 。AWS Audit Manager 現在可以執行下列動作來收集您的 AWS 帳戶. • acm:GetAccountConfiguration • acm:ListCertificates • backup:ListRecoveryPointsByResource • bedrock:GetCustomModel • bedrock:GetFoundationModel • bedrock:GetModelCustomizationJob • bedrock:GetModelInvocationLoggingConfiguration • bedrock:ListCustomModels • bedrock:ListFoundationModels • bedrock:ListModelCustomizationJobs • cloudtrail:LookupEvents • cloudwatch:DescribeAlarmsForMetric • cloudwatch:GetMetricStatistics • cloudwatch:ListMetrics • directconnect:DescribeDirectConnectGateways • directconnect:DescribeVirtualGateways • dynamodb:ListBackups • dynamodb:ListGlobalTables • ec2:DescribeAddresses	11/06/2023

變更	描述	日期
	• ec2:DescribeCustomerGateways • ec2:DescribeEgressOnlyInternetGateways • ec2:DescribeInternetGateways • ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations • ec2:DescribeLocalGateways • ec2:DescribeLocalGatewayVirtualInterfaces • ec2:DescribeNatGateways • ec2:DescribeTransitGateways • ec2:DescribeVpcPeeringConnections • ec2:DescribeVpnConnections • ec2:DescribeVpnGateways • ec2:GetEbsDefaultKmsKeyId • ec2:GetEbsEncryptionByDefault • ecs:DescribeClusters • eks:DescribeAddonVersions • elasticache:DescribeCacheClusters • elasticache:DescribeServiceUpdates • elasticfilesystem:DescribeAccessPoints • elasticloadbalancing:DescribeLoadBalancers • elasticloadbalancing:DescribeSslPolicies	

變更	描述	日期
	• elasticloadbalancing:DescribeTargetGroups • elasticmapreduce:ListClusters • elasticmapreduce:ListSecurityConfigurations • events:ListConnections • events:ListEventBuses • events:ListEventSources • events:ListRules • firehose:ListDeliveryStreams • fsx:DescribeFileSystems • iam:GetAccountPasswordPolicy • iam:GetCredentialReport • iam:ListOpenIdConnectProviders • iam:ListSamlProviders • iam:ListVirtualMFADevices • kafka:ListClusters • kafka:ListKafkaVersions • kinesis:ListStreams • lambda:ListFunctions • logs:DescribeDestinations • logs:DescribeExportTasks • logs:DescribeLogGroups • logs:DescribeMetricFilters • logs:DescribeResourcePolicies • logs:FilterLogEvents • rds:DescribeCertificates • rds:DescribeDbClusterEndpoints	

變更	描述	日期
	• rds:DescribeDbClusterParameterGroups • rds:DescribeDbClusters • rds:DescribeDbSecurityGroups • redshift:DescribeClusters • s3:GetBucketPublicAccessBlock • s3:GetBucketVersioning • sns:ListTopics • sqs:ListQueues • waf-regional:GetLoggingConfiguration • waf-regional:ListRuleGroups • waf-regional:ListSubscribedRuleGroups • waf-regional:ListWebACLs	
AWSAuditManagerServiceRolePolicy – 更新現有政策	我們將以下許可新增到 AWSAuditManagerServiceRolePolicy： • dynamodb:DescribeTable • dynamodb:ListTables • ec2:DescribeVolumes • kms:GetKeyPolicy • kms:GetKeyRotationStatus • kms:ListKeyPolicies • rds:DescribeDBInstances • redshift:DescribeClusters • s3:GetEncryptionConfiguration • s3:ListAllMyBuckets	2022 年 7 月 7 日

變更	描述	日期
AWSAuditManagerServiceRolePolicy – 更新現有政策	服務連結角色現在允 AWS Audit Manager 許執行動`organizations:DescribeOrganization` 作。 我們還將 `CreateEventsAccess` 資源範圍從萬用字元 (*) 縮小到特定類型的資源 (`arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver`)。 最後，我們為 `Null` 條件索引鍵添加 `events:source` 條件運算子，以確認來源值存在且其值不為 null。	2022 年 5 月 20 日
AWSAuditManagerAdministratorAccess – 更新現有政策	我們已更新的金鑰條件政策，`events:source` 以反映這是多值金鑰。	04/29/2022
AWSAuditManagerServiceRolePolicy – 更新現有政策	我們已更新的金鑰條件政策，`events:source` 以反映這是多值金鑰。	03/16/2022
AWS Audit Manager 開始追蹤變更	AWS Audit Manager 開始追蹤其 AWS 受管理策略的變更。	2021 年 6 月 5 日

疑難排解 AWS Audit Manager 身分和存取

請使用以下資訊來協助您診斷和修正使用 Audit Manager 和 IAM 時發生的常見問題。

主題

- 我沒有執行操作的授權 AWS Audit Manager
- 我沒有授權執行 iam：PassRole
- 我想允許我以外的人訪 AWS 帳戶 問我的 AWS Audit Manager 資源

我沒有執行操作的授權 AWS Audit Manager

`AccessDeniedException`當使用者沒有使用權限 AWS Audit Manager 或 Audit Manager API 作業時，會出現錯誤。

在此情況下，管理員必須將政策更新為允許您存取。

我沒有授權執行 iam：PassRole

如果錯誤訊息告知您未獲得授權，無法執行 `iam:PassRole` 動作，您的政策就必須更新，允許您將角色傳遞給 Audit Manager。

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

當名為 `marymajor` 的 IAM 使用者嘗試使用主控台在 Audit Manager 中執行動作時，發生下列範例錯誤。但是，該動作要求服務具備服務角色授與的許可。Mary 沒有將角色傳遞至該服務的許可。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在這種情況下，Mary 的政策必須更新，允許她執行 `iam:PassRole` 動作。

如果您需要協助，請聯絡您的 AWS 系統管理員。您的管理員提供您的登入憑證。

我想允許我以外的人訪 AWS 帳戶 問我的 AWS Audit Manager 資源

您可以建立一個角色，讓其他帳戶中的使用者或您的組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。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：

- 如需了解 Audit Manager 是否支援這些功能，請參閱 如何與 IAM AWS Audit Manager 搭配使用。
- 若要了解如何提供對您所擁有資源 AWS 帳戶 的存取權，請參閱 IAM 使用者指南中您擁有的另一 AWS 帳戶 個 IAM 使用者提供存取權限。
- 若要了解如何將資源存取權提供給第三方 AWS 帳戶，請參閱 IAM 使用者指南中的提供第三方 AWS 帳戶 擁有的存取權。
- 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 角色與資源型政策的差異。

使用服務連結角色 AWS Audit Manager

AWS Audit Manager 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 Audit Manager 的特殊 IAM 角色類型。服務連結角色由 Audit Manager 預先定義，並包含服務代表您呼叫其他服 AWS 務所需的所有權限。

服務連結角色可讓您 AWS Audit Manager 更輕鬆地設定，因為您不必手動新增必要的權限。Audit Manager 定義其服務連結角色的許可，除非另有定義，否則僅有 Audit Manager 可以擔任其角色。定義的許可包括信任政策和許可政策，並且該許可政策不能連接到任何其他 IAM 實體。

如需關於支援服務連結角色的其他服務資訊，請參閱可搭配 IAM 運作的AWS 服務，並尋找在服務連結角色欄中顯示為是的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

服務連結角色權限 AWS Audit Manager

Audit Manager 使用名為的服務連結角色**`AWSServiceRoleForAuditManager`**，可存取使用或管理的 AWS 服務和資源。 AWS Audit Manager

`AWSServiceRoleForAuditManager` 服務連結角色信任 `auditmanager.amazonaws.com` 服務來擔任該角色。

角色權限原則可讓 Audit Manager 收集有關您 AWS 使用情況的自動證據。`AWSAuditManagerServiceRolePolicy`具體而言，它可以代表您執行以下動作。

- Audit Manager 可用 AWS Security Hub 來收集合規性檢查證據。在此情況下，Audit Manager 會使用下列權限直接從中報告安全性檢查結果 AWS Security Hub。然後，將結果附加到您的相關評估控制項中作為證據。
  - `securityhub:DescribeStandards`

> **Note**
>
> 如需有關 Audit Manager 可描述的特定 Security Hub 控制項的詳細資訊，請參閱 AWS Audit Manager支援的AWS Security Hub 控制項。

- Audit Manager 可用 AWS Config 來收集合規性檢查證據。在這種情況下，Audit Manager 會使用下列權限直接從 AWS Config中報告 AWS Config 規則評估的結果。然後，將結果附加到您的相關評估控制項中作為證據。
  - `config:DescribeConfigRules`
  - `config:DescribeDeliveryChannels`
  - `config:ListDiscoveredResources`

  > **Note**
  >
  > 如需有關 Audit Manager 可描述哪些特定 AWS Config 規則的詳細資訊，請參閱受支援的 AWS Config 規則 AWS Audit Manager。

- Audit Manager 可用 AWS CloudTrail 來收集使用者活動證據。在此情況下，Audit Manager 會使用下列權限從 CloudTrail 記錄擷取使用者活動。然後，將活動附加到您的相關評估控制項中作為證據。
  - `cloudtrail:DescribeTrails`
  - `cloudtrail:LookupEvents`

  > **Note**
  >
  > 如需有關 Audit Manager 可描述哪些特定 CloudTrail 事件的詳細資訊，請參閱受支援的AWS CloudTrail 事件名稱 AWS Audit Manager。

- Audit Manager 可以使用 AWS API 呼叫來收集資源組態證據。在此情況下，Audit Manager 會使用下列許可來呼叫描述下列 AWS 服務之資源組態的唯讀 API。然後，將 API 回應附加到您的相關評估控制項中作為證據。
  - `acm:GetAccountConfiguration`
  - `acm:ListCertificates`
  - `backup:ListRecoveryPointsByResource`
  - `bedrock:GetCustomModel`
  - `bedrock:GetFoundationModel`
  - `bedrock:GetModelCustomizationJob`
  - `bedrock:GetModelInvocationLoggingConfiguration`
  - `bedrock:ListCustomModels`

- bedrock:ListFoundationModels
- bedrock:ListModelCustomizationJobs
- cloudwatch:DescribeAlarms
- cloudwatch:DescribeAlarmsForMetric
- cloudwatch:GetMetricStatistics
- cloudwatch:ListMetrics
- cognito-idp:DescribeUserPool
- directconnect:DescribeDirectConnectGateways
- directconnect:DescribeVirtualGateways
- dynamodb:DescribeTable
- dynamodb:ListBackups
- dynamodb:ListGlobalTables
- dynamodb:ListTables
- ec2:DescribeAddresses
- ec2:DescribeCustomerGateways
- ec2:DescribeEgressOnlyInternetGateways
- ec2:DescribeFlowLogs
- ec2:DescribeInstances
- ec2:DescribeInternetGateways
- ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations
- ec2:DescribeLocalGateways
- ec2:DescribeLocalGatewayVirtualInterfaces
- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSnapshots
- ec2:DescribeTransitGateways
- ec2:DescribeVolumes
- ec2:DescribeVpcEndpoints

- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs
- ec2:DescribeVpnConnections
- ec2:DescribeVpnGateways
- ec2:GetEbsDefaultKmsKeyId
- ec2:GetEbsEncryptionByDefault
- ecs:DescribeClusters
- eks:DescribeAddonVersions
- elasticache:DescribeCacheClusters
- elasticache:DescribeServiceUpdates
- elasticfilesystem:DescribeAccessPoints
- elasticfilesystem:DescribeFileSystems
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeSslPolicies
- elasticloadbalancing:DescribeTargetGroups
- elasticmapreduce:ListClusters
- elasticmapreduce:ListSecurityConfigurations
- events:DeleteRule
- events:DescribeRule
- events:DisableRule
- events:EnableRule
- events:ListConnections
- events:ListEventBuses
- events:ListEventSources
- events:ListRules
- events:ListTargetsByRule
- events:PutRule
- events:PutTargets
- events:RemoveTargets
- firehose:ListDeliveryStreams

- fsx:DescribeFileSystems
- guardduty:ListDetectors
- iam:GenerateCredentialReport
- iam:GetAccountAuthorizationDetails
- iam:GetAccountPasswordPolicy
- iam:GetAccountSummary
- iam:GetCredentialReport
- iam:ListEntitiesForPolicy
- iam:ListGroupPolicies
- iam:ListGroups
- iam:ListOpenIdConnectProviders
- iam:ListPolicies
- iam:ListRolePolicies
- iam:ListRoles
- iam:ListSamlProviders
- iam:ListUserPolicies
- iam:ListUsers
- iam:ListVirtualMFADevices
- kafka:ListClusters
- kafka:ListKafkaVersions
- kinesis:ListStreams
- kms:DescribeKey
- kms:GetKeyPolicy
- kms:GetKeyRotationStatus
- kms:ListGrants
- kms:ListKeyPolicies
- kms:ListKeys
- lambda:ListFunctions
- license-manager:ListAssociationsForLicenseConfiguration
- license-manager:ListLicenseConfigurations

- license-manager:ListUsageForLicenseConfiguration
- logs:DescribeDestinations
- logs:DescribeExportTasks
- logs:DescribeLogGroups
- logs:DescribeMetricFilters
- logs:DescribeResourcePolicies
- logs:FilterLogEvents
- organizations:DescribeOrganization
- organizations:DescribePolicy
- rds:DescribeCertificates
- rds:DescribeDbClusterEndpoints
- rds:DescribeDbClusterParameterGroups
- rds:DescribeDbClusters
- rds:DescribeDBInstances
- rds:DescribeDbSecurityGroups
- redshift:DescribeClusters
- route53:GetQueryLoggingConfig
- s3:GetBucketPolicy
  - 此 API 動作會在可用位 AWS 帳戶 置的範圍內 service-linked-role 運作。它無法存取跨帳戶儲存貯體政策。
- s3:GetBucketPublicAccessBlock
- s3:GetBucketVersioning
- s3:GetEncryptionConfiguration
- s3:GetLifecycleConfiguration
- s3:ListAllMyBuckets
- sns:ListTopics
- sqs:ListQueues
- waf-regional:GetLoggingConfiguration
- waf-regional:ListRuleGroups

- waf-regional:ListSubscribedRuleGroups

- `waf-regional:ListWebACLs`
- `waf:ListActivatedRulesInRuleGroup`

> **Note**
>
> 如需有關 Audit Manager 可以描述的特定 API 呼叫的詳細資訊，請參閱 自訂控制項資料來源支援的 API 呼叫。

若要檢視服務連結角色的完整權限詳細資料`AWSServiceRoleForAuditManager`，請參閱AWS 受管理策略參考指南AWSAuditManagerServiceRolePolicy中的。

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的服務連結角色許可。

建立 AWS Audit Manager 服務連結角色

您不需要手動建立一個服務連結角色。當您啟用時 AWS Audit Manager，服務會自動為您建立服務連結角色。您可以從的上架頁面或透過 API 或 AWS CLI啟用 Audit Manager。 AWS Management Console如需詳細資訊，請參閱本使用者指南中的 啟用 AWS Audit Manager。

若您刪除此服務連結角色然後需要再次建立，便可在帳戶中使用相同程序重新建立角色。

編輯 AWS Audit Manager 服務連結角色

AWS Audit Manager 不允許您編輯`AWSServiceRoleForAuditManager`服務連結角色。因為可能有各種實體會參考服務連結角色，所以您無法在建立角色之後變更其名稱。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱 IAM 使用者指南中的編輯服務連結角色。

如需允許 IAM 實體編輯 **`AWSServiceRoleForAuditManager`** 服務連結角色的描述

將下列陳述式新增至 IAM 實體編輯服務連結角色描述所需的許可政策：

```
{
    "Effect": "Allow",
    "Action": [
        "iam:UpdateRoleDescription"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/
AWSServiceRoleForAuditManager*",
```

```
    "Condition": {"StringLike": {"iam:AWSServiceName": "auditmanager.amazonaws.com"}}
}
```

刪除 AWS Audit Manager 服務連結角色

如果您不再需要使用 Audit Manager，我們建議您刪除 AWSServiceRoleForAuditManager 服務連結角色。這樣就不會有未積極監控或維護的未使用實體。然而，務必清除服務連結角色，之後才能將其刪除。

清除服務連結角色

您必須先確認 Audit Manager 服務連結角色沒有作用中的工作階段，並移除該角色使用的資源，之後才能使用 IAM 將其刪除。若要這麼做，請確定 Audit Manager 已全部 AWS 區域取消註冊。取消註冊後，Audit Manager 將不再使用服務連結角色。

如需有關如何取消註冊 Audit Manager 的說明，請參閱以下資源：

- 本指南中的 停用 AWS Audit Manager
- AWS Audit Manager API 參考中的 DeregisterAccount
- 撤銷註冊-帳戶的參考AWS CLI AWS Audit Manager

如需有關如何手動刪除 Audit Manager 資源的說明，請參閱本指南中的刪除 Audit Manager 資料。

刪除 服務連結角色

您可以使用 IAM 主控台、 AWS Command Line Interface (AWS CLI) 或 IAM API 來刪除服務連結角色。

IAM console

請依照下列步驟，在 IAM 主控台中刪除服務連結角色：

刪除服務連結角色 (主控台)

1. 登入 AWS Management Console 並開啟 IAM 主控台，網址為 https://console.aws.amazon.com/iam/。
2. 在 IAM 主控台的導覽窗格中，選擇 Roles (角色)。選擇 AWSServiceRoleForAuditManager 旁的核取方塊，而非名稱或列本身。
3. 在頁面頂端的角色動作下選擇刪除。

4. 在確認對話方塊中，檢閱上次存取資訊，以顯示每個所選擇角色上次存取 AWS 服務的時間。這可協助您確認角色目前是否作用中。如果您想要繼續進行，在文字輸入欄位中輸入 **AWSServiceRoleForAuditManager**，然後選擇刪除來提交服務連結角色以進行刪除。
5. 查看 IAM 主控台通知，監視服務連結角色刪除的進度。因為 IAM 服務連結角色刪除不同步，所以在您提交角色進行刪除之後，刪除任務可能會成功或失敗。如果任務成功，則會從清單中移除角色，而且成功訊息會出現在頁面頂端。

AWS CLI

您可以使用的 IAM 命令 AWS CLI 來刪除服務連結角色。

刪除服務連結角色 (AWS CLI)

1. 輸入以下命令來列出您帳戶中的角色：

```
aws iam get-role --role-name AWSServiceRoleForAuditManager
```

2. 因為無法刪除正在使用或具有相關聯資源的服務連結角色，所以您必須提交刪除要求。如果不符合這些條件，則可以拒絕該請求。您必須從回應中擷取 `deletion-task-id`，以檢查刪除任務的狀態。

   輸入下列命令，以提交服務連結角色刪除要求：

```
aws iam delete-service-linked-role --role-name AWSServiceRoleForAuditManager
```

3. 使用下列命令，以檢查刪除任務的狀態：

```
aws iam get-service-linked-role-deletion-status --deletion-task-id deletion-task-id
```

   刪除任務的狀態可以是 `NOT_STARTED`、`IN_PROGRESS`、`SUCCEEDED` 或 `FAILED`。如果刪除失敗，則呼叫會傳回失敗原因，以進行疑難排解。

IAM API

您可以使用 IAM API 刪除服務連結角色。

刪除服務連結角色 (API)

1. GetRole打電話列出您帳戶中的角色。在請求中，指定 AWSServiceRoleForAuditManager 為 RoleName。
2. 因為無法刪除正在使用或具有相關聯資源的服務連結角色，所以您必須提交刪除要求。如果不符合這些條件，則可以拒絕該請求。您必須從回應中擷取 DeletionTaskId，以檢查刪除任務的狀態。

   若要提交服務連結名單的刪除請求，請呼叫 DeleteServiceLinkedRole。在請求中，指定 AWSServiceRoleForAuditManager 為 RoleName。
3. 若要檢查刪除的狀態，請呼叫 GetServiceLinkedRoleDeletionStatus。在請求中，指定 DeletionTaskId。

   刪除任務的狀態可以是 NOT_STARTED、IN_PROGRESS、SUCCEEDED 或 FAILED。如果刪除失敗，則呼叫會傳回失敗原因，以進行疑難排解。

> **Tip**
>
> 如果 Audit Manager 服務正在使用該角色或具有相關聯的資源，則刪除失敗。只有在您仍在一或多個 AWS 區域中註冊 Audit Manager 時，才會發生這種情況。取消註冊後，Audit Manager 將不再使用服務連結角色。
> 若要解決刪除失敗的問題，請先確定您已在使用該服務的所有 AWS 區域 位置取消註冊 Audit Manager。然後，再次執行上一個程序中的步驟。

支援 AWS Audit Manager 服務連結角色的區域

AWS Audit Manager 支援在所有可用服務的 AWS 區域 地方使用服務連結角色。如需詳細資訊，請參閱 AWS 服務端點。

符合性驗證 AWS Audit Manager

若要瞭解 AWS 服務 是否屬於特定規範遵循方案的範圍內，請參閱AWS 服務 遵循規範計劃方案中的，並選擇您感興趣的合規方案。如需一般資訊，請參閱AWS 規範計劃AWS。

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

您在使用時的合規責任取決 AWS 服務 於資料的敏感性、公司的合規目標以及適用的法律和法規。AWS 提供下列資源以協助遵循法規：

- 安全性與合規性快速入門指南 — 這些部署指南討論架構考量，並提供部署以安全性和合規性 AWS 為重點的基準環境的步驟。
- 在 Amazon Web Services 上架構 HIPAA 安全性與合規性 — 本白皮書說明公司如何使用建立符合 HIPAA 資格的應 AWS 用程式。

> **Note**
>
> 並非所有人 AWS 服務 都符合 HIPAA 資格。如需詳細資訊，請參閱 HIPAA 資格服務參照。

- AWS 合規資源AWS — 此工作簿和指南集合可能適用於您的產業和所在地。
- AWS 客戶合規指南 — 透過合規的角度瞭解共同的責任模式。這份指南總結了在多個架構 (包括美國國家標準技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO)) 中，保 AWS 服務 護指引並對應至安全控制的最佳實務。
- 使用AWS Config 開發人員指南中的規則評估資源 — 此 AWS Config 服務會評估您的資源組態符合內部實務、產業準則和法規的程度。
- AWS Security Hub— 這 AWS 服務 提供了內部安全狀態的全面視圖 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 Security Hub controls reference。
- AWS Audit Manager— 這 AWS 服務 有助於您持續稽核您的 AWS 使用情況，以簡化您管理風險的方式，以及遵守法規和業界標準的方式。

韌性 AWS Audit Manager

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

透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和可擴展性能力，均較單一或多個資料中心的傳統基礎設施還高。

如需區域和可用區域的相關 AWS 資訊，請參閱AWS 全域基礎結構。

基礎結構安全 AWS Audit Manager

AWS 稽核管理員身為受管服務，受到 AWS 全球網路安全的保護。有關 AWS 安全服務以及如何 AWS 保護基礎結構的詳細資訊，請參閱AWS 雲端安全 若要使用基礎架構安全性的最佳做法來設計您的 AWS 環境，請參閱安全性支柱架構良 AWS 好的架構中的基礎結構保護。

您可以使用 AWS 已發佈的 API 呼叫透過網路存取 AWS Audit Manager。用戶端必須支援下列項目：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 具備完美轉送私密(PFS)的密碼套件，例如 DHE (Ephemeral Diffie-Hellman)或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，請求必須使用存取索引鍵 ID 和與 IAM 主體相關聯的私密存取金鑰來簽署。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。

您可以從任何網路位置呼叫這些 API 作業，但支 AWS Audit Manager 援以資源為基礎的存取原則，其中可能包含以來源 IP 位址為基礎的限制。您也可以使用 Audit Manager 政策來控制從特定 Amazon Virtual Private Cloud (Amazon VPC) 的端點或特定 VPC的存取。實際上，這會將對特定 Audit Manager 資源的網路存取從網路內的特定 VPC 隔離出來 AWS 。

AWS Audit Manager 和介面 VPC 端端點 ()AWS PrivateLink

您可以在 VPC 和 AWS Audit Manager 建立介面 VPC 端點之間建立私人連線。介面端點是由 AWS PrivateLink 提供技術支援，這項技術可讓您在沒有網際網路閘道、NAT 裝置、VPN 連接或 AWS Direct Connect 連線的情況下私密地存取 Audit Manager API。VPC 中的執行個體不需要公有 IP 地址，即能與 Audit Manager API 通訊。您的 VPC 和 AWS Audit Manager 不會離開 AWS 網路之間的流量。

每個介面端點都是由您子網路中的一或多個彈性網路介面表示。

如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的介面 VPC 端點 (AWS PrivateLink)。

AWS Audit Manager VPC 端點的考量

在為其設定介面 VPC 端點之前 AWS Audit Manager，請務必先查看 Amazon VPC 使用者指南中的界面端點屬性和限制。

AWS Audit Manager 支援從您的 VPC 呼叫其所有 API 動作。

為 AWS Audit Manager建立介面 VPC 端點

您可以使用 Amazon VPC 主控台或 AWS Command Line Interface ()AWS CLI建立 AWS Audit Manager 服務的 VPC 端點。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的建立介面端點。

建立 VPC 端點以 AWS Audit Manager 使用下列服務名稱：

- `com.amazonaws.region.auditmanager`

如果您為端點啟用私有 DNS，則可以 AWS Audit Manager 使用該區域的預設 DNS 名稱發出 API 要求，例如`auditmanager.us-east-1.amazonaws.com`。

如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的透過介面端點存取服務。

建立 VPC 端點原則 AWS Audit Manager

您可以將端點政策連接至控制 AWS Audit Manager存取權限的 VPC 端點。此政策會指定下列資訊：

- 可執行動作的主體。
- 可執行的動作。
- 可供執行動作的資源。

如需詳細資訊，請參閱 Amazon VPC 使用者指南中的使用 VPC 端點控制對服務的存取。

範例：用於動作的 VPC 端點原則 AWS Audit Manager

以下是的端點策略範例 AWS Audit Manager。附加至端點後，此政策會針對所有資源上的所有主體，授予列出的 Audit Manager 動作的存取權限。

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "auditmanager:GetAssessments",
            "auditmanager:GetServicesInScope",
            "auditmanager:ListNotifications"
         ],
         "Resource":"*"
```

```
        }
    ]
}
```

登錄和監控 AWS Audit Manager

監控是維持 Audit Manager 和其他 AWS 解決方案的可靠性、可用性和效能的重要組成部分。 AWS 提供下列監視工具來監視 Audit Manager、在發生錯誤時報告，並在適當時採取自動動作：

- AWS CloudTrail 擷取您 AWS 帳戶 發出或代表發出的 API 呼叫和相關事件，並傳送日誌檔案至您指定的 Amazon S3 儲存貯體。您可以找出哪些使用者和帳戶呼叫 AWS、發出呼叫的來源 IP 地址，以及呼叫的發生時間。如需詳細資訊，請參閱《AWS CloudTrail 使用者指南》https://docs.aws.amazon.com/awscloudtrail/latest/userguide/。
- Amazon EventBridge 是一種無伺服器事件匯流排服務，可讓您輕鬆地將應用程式與各種來源的資料連接起來。 EventBridge 從您自己的應用程式、S oftware-as-a 服務 (SaaS) 應用程式以及服務提供即時資料串流，並 AWS 將該資料路由到目標 (例如 Lambda)。這可讓您監控在服務中發生的事件，並建置事件導向的架構。如需詳細資訊，請參閱 Amazon EventBridge 使用者指南。

AWS Audit Manager 使用 Amazon 監控 EventBridge

Amazon 可 EventBridge 協助您自動化 AWS 服務 並自動回應系統事件，例如應用程式可用性問題或資源變更。

您可以使用 EventBridge規則來偵測 Audit Manager 事件並對其做出回應。根據您建立的規則，當事件符合您在規則中指定的值時， EventBridge 叫用一或多個目標動作。根據事件的類型，您可能會想要傳送通知、擷取事件資訊，採取修正動作、啟動事件，或採取其他動作。

例如，每當您的帳戶中發生下列 Audit Manager 事件時，您可以進行偵測：

- 稽核擁有者建立、更新或刪除評估
- 稽核擁有者委派控制集以供檢閱
- 委派人員完成其檢閱，並將已檢閱的控制集交回稽核擁有者
- 稽核擁有者更新評估控制項的狀態

可以自動觸發的動作如下：

- 使用 AWS Lambda 函數將通知傳遞給 Slack 通道。

- 將有關檢查的資料推送到 Amazon Kinesis Data Streams，以支援完整且即時的狀態監控。
- 向您的電子郵件傳送 Amazon Simple Notification Service (Amazon SNS)主題。
- 通過 Amazon CloudWatch 警報操作獲得通知。

> **Note**
>
> Audit Manager 持續傳遞事件。這表示 Audit Manager 至少會成功嘗試將事件傳遞至 EventBridge 少一次。如果事件因為 EventBridge 服務中斷而無法傳遞，則 Audit Manager 將於稍後重試最多 24 小時。

EventBridge Audit Manager 的範例格式

下列 JSON 程式碼顯示 Audit Manager 中評估建立事件的範例。如需有關此事件中任何欄位的資訊，請參閱事件結構參考。

```
{
    "version": "0",
    "id": "55c5a6f3-6183-3989-49ec-a3c998857644",
    "detail-type": "Assessment Created",
    "source": "aws.auditmanager",
    "account": "111122223333",
    "time": "2023-07-27T00:38:33Z",
    "region": "us-west-2",
    "resources":
        [
            "arn:aws:auditmanager:us-west-2:111122223333:assessment/a1b2c3d4-e5f6-g7h8-
i9j0-k1l2m3n4o5p6"
        ],
    "detail":
    {
        "eventID": "4e939b2f-9429-3141-beec-d640d83ef68e",
        "author": "arn:aws:sts::111122223333:assumed-role/roleName/role-session-name",
        "assessmentTenantId": "111122223333",
        "assessmentName": "myAssessment",
        "eventTime": 1690418289068,
        "eventName": "CREATE",
        "eventType": "ASSESSMENT",
        "assessmentID": "a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6"
    }
```

```
}
```

建立 EventBridge 規則的先決條件

建議您在為 Audit Manager 事件建立規則之前，執行以下操作：

- 熟悉中的事件、規則和目標。 EventBridge如需詳細資訊，請參閱什麼是 Amazon EventBridge？ 在 Amazon 用 EventBridge 戶指南。
- 建立要在事件規則中使用的目標。例如，您可建立 Amazon SNS 主題，以便每當完成控制集檢閱時，您都會收到文字訊息或電子郵件。如需詳細資訊，請參閱EventBridge 目標。

建立 Audit Manager 的 EventBridge 規則

請遵循下列步驟來建立在 Audit Manager 發出的事件上觸發的 EventBridge 規則。盡可能發出事件。

建立 Audit Manager EventBridge 規則的步驟

1. 在以下位置打開 Amazon EventBridge 控制台 https://console.aws.amazon.com/events/。
2. 在導覽窗格中，選擇 Rules(規則)。
3. 選擇 Create rule (建立規則)。
4. 在定義規則詳細資訊頁面中，輸入規則名稱和描述。
5. 請保留事件匯流排和規則類型的預設值，然後選擇 下一步。
6. 在 [建立事件模式] 頁面上，針對 [事件來源] 選擇AWS 事件或 EventBridge 合作夥伴事件。
7. 對於建立方法，選擇自訂模式 (JSON 編輯器)。
8. 在事件模式下，以 JSON 撰寫事件模式，並指定要用於比對的欄位。

   如需比對 Audit Manager 事件，您可以使用以下簡單模式：

   ```
   {
     "detail-type": ["Event"]
   }
   ```

   以下列其中一個支援的值取代##：

   a. 輸入 `Assessment Created` 以在建立評估時收到通知。
   b. 輸入 `Assessment Updated` 以在更新評估時收到通知。
   c. 輸入 `Assessment Deleted` 以在刪除評估時收到通知。

d. 輸入 `Assessment ControlSet Delegation Created` 以在委派控制集進行檢閱時收到通知。

e. 輸入 `Assessment ControlSet Reviewed` 以在檢閱評估控制集時收到通知。

f. 輸入 `Assessment Control Reviewed` 以在檢閱評估控制項時收到通知。

> **Tip**
>
> 根據需要將更多欄位添加到您的事件模式中。如需有關可用欄位的詳細資訊，請參閱 Amazon EventBridge 事件模式。

9. 選擇下一步。
10. 在選擇目標頁面上，選擇您為此規則建立的目標類型，然後設定該類型所需的任何其他選項。例如，如果您選擇 Amazon SNS，請確認您的 SNS 主題設定正確，以便透過電子郵件或簡訊通知您。

> **Tip**
>
> 顯示的欄位會因選擇的服務而異。如需有關可用目標的詳細資訊，請參閱 EventBridge 主控台中可用的目標。

11. 對於許多目標類型， EventBridge 需要將事件傳送至目標的權限。在這些情況下， EventBridge 可以建立執行規則所需的 IAM 角色。

    a. 如需自動建立 IAM 角色，請選擇 為此特定資源建立新角色。

    b. 如需使用您早前建立的 IAM 角色，請選擇 使用現有角色 。

12. (選用) 選擇新增其他目標，為此規則新增另一個目標。
13. 選擇 Next (下一步)。
14. (選用) 在 設定標籤頁面，新增任何標籤，然後選擇下一步。
15. 在檢閱並建立頁面上，檢閱您的規則設定，並確定其符合您的事件監控要求。
16. 選擇 Create rule (建立規則)。您的規則現在將監控 Audit Manager 事件，然後將這些事件傳送至您指定的目標。

使用記錄 AWS Audit Manager API 呼叫 CloudTrail

Audit Manager 與服務整合 CloudTrail，可提供使用者、角色或 Audit Manager AWS 服務 中所採取的動作記錄的服務。 CloudTrail 將 Audit Manager 的所有 API 呼叫擷取為事件。擷取的呼叫包括從 Audit Manager 主控台進行的呼叫，以及針對 Audit Manager API 操作的程式碼呼叫。

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

使用收集的資訊 CloudTrail，您可以判斷向 Audit Manager 提出的請求、提出請求的 IP 位址、提出請求的人員、提出請求的時間以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱使AWS CloudTrail 用者指南。

Audit Manager 資訊 CloudTrail

CloudTrail 在您創建帳戶 AWS 帳戶 時啟用。當活動在 Audit Manager 中發生時，該活動會與事件歷程記錄中的其他 CloudTrail AWS 服務 事件一起記錄在事件中。

您可以查看，搜索和下載最近的事件 AWS 帳戶。如需詳細資訊，請參閱使用 CloudTrail 事件歷程記錄檢視事件。

如需您的正在進行中的 AWS 帳戶事件記錄 (包括 Audit Manager 的事件)，請建立追蹤。追蹤可 CloudTrail 將日誌檔交付到 Amazon S3 儲存貯體。依預設，當您在主控台中建立追蹤時，該追蹤會套用至所有的 AWS 區域。追蹤記錄來自 AWS 分區中所有區域的事件，並將日誌檔傳送到您指定的 Amazon S3 儲存貯體。

此外，您可以設定其他， AWS 服務 以進一步分析 CloudTrail 記錄中收集的事件資料並採取行動。如需詳細資訊，請參閱下列內容：

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

所有 Audit Manager 動作都會記錄在 API 參考中， CloudTrail 並記錄在 AWS Audit Manager API 參考中。例如，呼叫`DeleteControl`和 `UpdateAssessmentTemplate` API 作業會在 CloudTrail 記錄檔中產生項目。`CreateCustomControl`

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

- 該請求是否使用根使用者憑證提出。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 該請求是否由另一項 AWS 服務服務提出。

如需詳細資訊，請參閱 CloudTrail 使用者身分元素。

了解 Audit Manager 日誌檔案項目

追蹤是一種組態，可讓事件以日誌檔的形式傳遞到您指定的 Amazon S3 儲存貯體。 CloudTrail 記錄檔包含一或多個記錄項目。事件代表來自任何來源的單一請求，包括有關請求的操作，動作的日期和時間，請求參數等信息。 CloudTrail 日誌文件不是公共 API 調用的有序堆棧跟踪，因此它們不會以任何特定順序顯示。

下列範例顯示示範`CreateAssessment`動作的 CloudTrail 記錄項目。

```
{
      eventVersion:"1.05",
      userIdentity:{
        type:"IAMUser",
        principalId:"principalId",
        arn:"arn:aws:iam::accountId:user/userName",
        accountId:"111122223333",
        accessKeyId:"accessKeyId",
        userName:"userName",
        sessionContext:{
          sessionIssuer:{
          },
          webIdFederationData:{
          },
          attributes:{
            mfaAuthenticated:"false",
            creationDate:"2020-11-19T07:32:06Z"
          }
        }
      },
      eventTime:"2020-11-19T07:32:36Z",
      eventSource:"auditmanager.amazonaws.com",
      eventName:"CreateAssessment",
      awsRegion:"us-west-2",
```

```
      sourceIPAddress:"sourceIPAddress",
      userAgent:"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
      requestParameters:{
        frameworkId:"frameworkId",
        assessmentReportsDestination:{
          destination:"***",
          destinationType:"S3"
        },
        clientToken:"***",
        scope:{
          awsServices:[
            {
              serviceName:"license-manager"
            }
          ],
          awsAccounts:"***"
        },
        roles:"***",
        name:"***",
        description:"***",
        tags:"***"
      },
      responseElements:{
        assessment:"***"
      },
      requestID:"0d950f8c-5211-40db-8c37-2ed38ffcc894",
      eventID:"a782029a-959e-4549-81df-9f6596775cb0",
      readOnly:false,
      eventType:"AwsApiCall",
      recipientAccountId:"recipientAccountId"
    }
```

中的配置和漏洞分析 AWS Audit Manager

配置和 IT 控制是與您（我們的客戶）AWS 之間的共同責任。如需詳細資訊，請參閱 AWS 共用的責任模型。

標記 AWS Audit Manager 資源

標籤是您或 AWS 指派給 AWS 資源的中繼資料標籤。每個標籤皆包含鍵與值。對於您指派的標籤，您可以定義鍵與值。例如，您可以將鍵定義為 `stage`，將資源的值定義為 `test`。

標籤可協助您執行以下操作：

- 輕鬆找到您的 Audit Manager 資源。瀏覽架構程式庫和控制項程式庫時，您可以將標籤用作搜尋條件。
- 將您的資源與合規類型建立關聯。您可以使用合規特定標籤來標記多個資源，以便將這些資源與特定架構建立關聯。
- 識別和組織您的 AWS 資源。許多 AWS 服務支援標記，因此您可以對來自不同服務的資源指派相同的標籤，指出資源是相關的。
- 追蹤您的 AWS 成本。您可以在 AWS Billing and Cost Management 儀表板上啟用這些標籤。AWS 會使用標籤分類您的成本，並交付每月成本配置報告給您。如需詳細資訊，請參閱 AWS Billing and Cost Management 使用者指南中的使用成本配置標籤。

以下部分提供有關 AWS Audit Manager 中標籤的詳細資訊。

Audit Manager 中支援的資源

下列 Audit Manager 資源支援標記：

- 評估
- 控制
- 架構

標籤限制

下列基本限制適用於 Audit Manager 資源上的標籤：

- 您可以指派給資源的標籤數量上限：50
- 索引鍵長度上限：128 個 Unicode 字元
- 數值長度上限：256 個 Unicode 字元
- 鍵與值的有效字元：a-z、A-Z、0-9、空格和下列字元：_ . : / = + - 及 @

- 鍵和值會區分大小寫
- 請不要使用 `aws:` 做為鍵的字首；它已保留供 AWS 使用

管理標籤

您可以在建立評估、架構或控制項時將標籤設定為屬性。您可以透過 Audit Manager 主控台、AWS Command Line Interface (AWS CLI) 和 Audit Manager API 新增、編輯及刪除標籤。如需詳細資訊，請參閱下列連結：

- 對於評估：
  - 建立評估 和 編輯評估 見本指南的評估區段
  - 標籤索引標籤 見本指南檢閱評估區段
  - CreateAssessment 和 UpdateAssessment 見 AWS Audit ManagerAPI 參考
  - TagResource 和 UntagResource 見 AWS Audit Manager API 參考
- 對於架構：
  - 建立自訂架構 和 編輯自訂架構 見本指南的架構程式庫區段
  - 標籤索引標籤 見本指南的檢閱架構詳細資訊區段
  - AWS Audit Manager API 參考中的 CreateAssessmentFramework 和 UpdateAssessmentFramework
  - TagResource 和 UntagResource 見 AWS Audit Manager API 參考
- 對於控制項：
  - 建立自訂控制項 和 編輯自訂控制項 見本指南的控制項程式庫區段
  - 標籤索引標籤 見本指南的檢閱控制項詳細資訊區段
  - CreateControl 和 UpdateControl 見 AWS Audit Manager API 參考
  - TagResource 和 UntagResource 見 AWS Audit Manager API 參考

透過 AWS CloudFormation 建立 AWS Audit Manager 資源

AWS Audit Manager 已與 AWS CloudFormation 整合，這項服務可協助您建立 AWS 資源的模型和設定，以減少建立和管理資源和基礎設施的時間。您可以建立一個範本，描述所有您想要的 AWS 資源 (例如評估)，AWS CloudFormation 就會為您佈建和設定那些資源。

當您使用 AWS CloudFormation 時，您可以重複使用您的範本，重複、一致的設定您的 Audit Manager 資源。只需描述一次您的資源，即可在多個 AWS 帳戶與區域內重複佈建相同資源。

Audit Manager 和 AWS CloudFormation 範本

如需佈建和設定 Audit Manager 與相關服務的資源，您必須了解 AWS CloudFormation 範本。範本是以 JSON 或 YAML 格式化的文本檔案。而您亦可以透過這些範本的說明，了解欲在 AWS CloudFormation 堆疊中佈建的資源。如果您不熟悉 JSON 或 YAML，您可以使用 AWS CloudFormation Designer 協助您開始使用 AWS CloudFormation 範本。如需詳細資訊，請參閱 AWS CloudFormation 使用者指南中的什麼是 AWS CloudFormation Designer？。

Audit Manager 支援在 AWS CloudFormation 中建立評估。如需更多詳細資訊 (包括評估的 JSON 和 YAML 範本範例)，請參閱 AWS CloudFormation 使用者指南中的 AWS Audit Manager 資源類型參考。

進一步了解 AWS CloudFormation

如需進一步了解 AWS CloudFormation，請參閱下列資源：

- AWS CloudFormation
- 《AWS CloudFormation 使用者指南》https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/Welcome.html
- AWS CloudFormation API 參考
- 《AWS CloudFormation 命令列介面使用者指南》https://docs.aws.amazon.com/cloudformation-cli/latest/userguide/what-is-cloudformation-cli.html

AWS Audit Manager 使用者指南的文件歷史記錄

下表說明 2020 年 12 月 8 日後各版 AWS Audit Manager 使用者指南的重要變更。

變更	描述	日期
支援的新架構：PCI DSS V4.0	新預先建置架構現已在中 AWS Audit Manager 提供。如需詳細資訊，請參閱 PCI DSS V4.0。	2023 年 12 月 19 日
支援其他 AWS API 呼叫	您現在可以將其他 AWS API 呼叫用作 Audit Manager 中自訂控制項的資料來源。如需詳細資訊，請參閱自訂控制項資料來源支援的 API 呼叫。	2023 年 12 月 7 日
已更新 AWS 受管政策	AWS Audit Manager 更新了 AWSAuditManagerServiceRolePolicy。如需詳細資訊，請參閱 AWS Audit Manager 的 AWS 受管政策。	2023 年 12 月 6 日
支援 AWS Security Hub 合併控制項調查結果	Audit Manager 現在支援 AWS Security Hub 中的合併控制項。如需詳細資訊，請參閱 AWS Audit Manager 支援的 AWS Security Hub 控制項。	2023 年 11 月 16 日
與 MetricStream 整合	您現在可以將 Audit Manager 的證據擷取到 MetricStream 中。如需詳細資訊，請參閱與第三方 GRC 產品的整合。	2023 年 11 月 14 日
新支援架構：AWS 生成式 AI 最佳實務	新預先建置架構現已在中 AWS Audit Manager 提供。如需詳	2023 年 11 月 8 日

	細資訊，請參閱AWS 生成式 AI 最佳實務架構 v1。	
已更新 AWS 受管政策	AWS Audit Manager 更新了 AWSAuditManagerServiceRolePolicy。如需詳細資訊，請參閱 AWS Audit Manager 的 AWS 受管政策。	2023 年 11 月 6 日
整合 Amazon EventBridge	您現在可以監視發生在 AWS Audit Manager 中的事件，並將這些事件用作事件驅動架構的一部分。如需詳細資訊，請參閱使用 Amazon EventBridge 監測 AWS Audit Manager。	2023 年 8 月 18 日
支援風險評估和新的手動證據選項	您現在可以使用自訂控制項建立流程來支援風險評估。現在，一個控制項可以代表一個風險評估問題，您可以透過上傳檔案或輸入文字作為手動證據來提供答案。如需詳細資訊，請參閱建立自訂控制項和新增手動證據。	2023 年 6 月 12 日
支援 CSV 匯出	您現在可以匯出 CSV 格式的證據搜尋工具的搜尋結果。如需詳細資訊，請參閱匯出搜尋結果。	2023 年 6 月 9 日
新支援架構：澳大利亞網路安全中心 (ACSC) 資訊安全手冊	新預先建置架構現已在中 AWS Audit Manager 提供。如需詳細資訊，請參閱澳大利亞網路安全中心 (ACSC) 資訊安全手冊。	2023 年 3 月 24 日

改善的評估報告	我們改善了 Audit Manager 評估報告的格式和內容。如需有關如何導覽及理解評估報告的詳細資訊，請參閱評估報告。	2023 年 3 月 23 日
支援分頁 API 呼叫	AWS Audit Manager 現在支援分頁 API 呼叫用作證據收集的資料來源。如需詳細資訊，請參閱分頁 API 呼叫。	2023 年 3 月 8 日
新支援架構：HIPAA 最終綜合安全規則 2013	新預先建置架構現已在中 AWS Audit Manager 提供。如需詳細資訊，請參閱HIPAA 最終綜合安全規則 2013。出於差異化目的，之前存在的 HIPAA 架構 (在架構程式庫中層稱為 HIPAA) 現在命名為 HIPAA 安全規則 2003。	2023 年 3 月 8 日
支援其他 AWS API 呼叫	您現在可以將其它 9 種 AWS API 呼叫用作 Audit Manager 中自訂控制項的資料來源。如需詳細資訊，請參閱自訂控制項資料來源支援的 API 呼叫。	2023 年 3 月 3 日
更新了指南以符合 IAM 最佳實務	更新了指南以符合 IAM 最佳實務。如需更多詳細資訊，請參閱 IAM 中的安全最佳實務。	2023 年 1 月 6 日
新資料保留設定	現在，您可以指定是否要在停用 Audit Manager 時刪除所有資料。如需詳細資訊，請參閱停用 AWS Audit Manager和刪除 Audit Manager 資料。	2023 年 1 月 6 日

支援證據搜尋工具	您現在可以使用證據搜尋工具對證據資料執行搜尋查詢。如需詳細資訊，請參閱證據搜尋工具疑難排解。	2022 年 11 月 18 日
新支援架構：澳大利亞網路安全中心 (ACSC) 基本八項策略	新預先建置架構現已在中 AWS Audit Manager 提供。如需詳細資訊，請參閱澳大利亞網路安全中心 (ACSC) 基本八項策略.	2022 年 8 月 24 日
已更新 AWS 受管政策	AWS Audit Manager 更新了 AWSAuditManagerServiceRolePolicy。如需詳細資訊，請參閱 AWS Audit Manager 的 AWS 受管政策。	2022 年 7 月 7 日
已更新 AWS 受管政策	AWS Audit Manager 更新了 AWSAuditManagerServiceRolePolicy。如需詳細資訊，請參閱 AWS Audit Manager 的 AWS 受管政策。	2022 年 5 月 20 日
新支援架構：加拿大網路安全中心中型雲端控制設定檔	新預先建置架構現已在中 AWS Audit Manager 提供。如需詳細資訊，請參閱加拿大網路安全中心中型雲端控制設定檔。	2022 年 5 月 6 日
已更新 AWS 受管政策	AWS Audit Manager 已更新 AWSAuditManagerAdministratorAccess 政策。如需詳細資訊，請參閱 AWS Audit Manager 的 AWS 受管政策。	2022 年 4 月 29 日

支援其他 AWS Config 管理規則	您現在可以將其它 91 項 AWS Config 管理規則用作 Audit Manager 中自訂控制項的資料來源。如需詳細資訊，請參閱透過 AWS Audit Manager 使用 AWS Config 受管規則。	2022 年 4 月 27 日
支援 AWS Config 自訂規則	您現在可以將 AWS Config 自訂規則用作 Audit Manager 中自訂控制項的資料來源。如需詳細資訊，請參閱AWS Audit Manager 使用 AWS Config 自訂規則。	2022 年 4 月 27 日
新支援架構：ISO/IEC 27001:2013 附件 A	新預先建置架構現已在中 AWS Audit Manager 提供。如需詳細資訊，請參閱 ISO/IEC 27001:2013 附件 A。	2022 年 4 月 7 日
已更新 AWS 受管政策	AWS Audit Manager 更新了 AWSAuditManagerServiceRolePolicy。如需詳細資訊，請參閱 AWS Audit Manager 的 AWS 受管政策。	2022 年 3 月 16 日

新支援架構：適用於 CIS Amazon Web Services Foundations Benchmark v1.4 的 CIS 基準	現在，AWS Audit Manager 中提供了兩個新預先建置架構：適用於 CIS Amazon Web Services Foundations Benchmark v1.4 的 CIS 基準，1 級和 適用於 CIS Amazon Web Services Foundations Benchmark v1.4 的 CIS 基準，1 級和 2 級。如需詳細資訊，請參閱 適用於 CIS AWS Audit Manager Foundations Benchmark v1.4.0 的 CIS 基準。	2022 年 3 月 2 日
新支援架構：CIS 控制措施 v8 IG1	新預先建置架構現已在中 AWS Audit Manager 提供。如需詳細資訊，請參閱CIS 控制項 v8 IG1。	2022 年 3 月 2 日
AWS Audit Manager 儀表板	您現在可以使用 Audit Manager 儀表板來監控您的作用中評估，並快速識別不合規的證據。如需詳細資訊，請參閱使用 Audit Manager 儀表板。	2021 年 11 月 18 日
自訂架構共用	您現在可以與其他 AWS 帳戶共用自訂 Audit Manager 架構，或將它們複製到您自己帳戶下的另一 AWS 區域。如需詳細資訊，請參閱共用自訂架構。	2021 年 10 月 22 日

AWS Audit Manager 控制項的新範例	您現在可以檢閱控制項範例，並了解 Audit Manager 如何協助確保您的 AWS 環境符合其需求。如需詳細資訊，請參閱 AWS Audit Manager 控制項範例。	2021 年 9 月 21 日
新支援架構：金融服務業現代化法 (GLBA)	新預先建置架構現已在中 AWS Audit Manager 提供。如需詳細資訊，請參閱金融服務業現代化法 (GLBA)。	2021 年 9 月 2 日
新增疑難排解章	添加了疑難排解章節。如需詳細資訊，請參閱 AWS Audit Manager 疑難排解。	2021 年 8 月 23 日
新增委派章節和教學課程	我們擴展了委派文件，編為新章節。如需詳細資訊，請參閱AWS Audit Manager 中委派。我們還添加了針對在 AWS Audit Manager 中首次檢閱控制項集的委派代表的新教學課程。如需詳細資訊，請參閱委派代表教學課程：檢閱控制集。	2021 年 6 月 25 日
新支援架構：NIST SP 800-171 Rev. 2	新預先建置架構現已在中 AWS Audit Manager 提供。如需詳細資訊，請參閱 NIST SP 800-171 Rev. 2。	2021 年 6 月 17 日
改善的評估報告	我們改善了 AWS Audit Manager 評估報告的格式和內容。有關如何導覽和理解新評估報告的詳細資訊，請參閱評估報告。	2021 年 6 月 8 日

新的 AWS 受管政策頁面	AWS Audit Manager 已開始追蹤其受管政策的變更。如需詳細資訊，請參閱 AWS Audit Manager 的 AWS 受管政策。	2021 年 5 月 6 日
新支援架構：NIST 網路安全架構 1.1 版	新預先建置架構現已在中 AWS Audit Manager 提供。如需詳細資訊，請參閱 NIST 網路安全架構 1.1 版。	2021 年 5 月 5 日
新支援架構：AWSWell-Architected	新預先建置架構現已在中 AWS Audit Manager 提供。如需詳細資訊，請參閱 AWS Well-Architected。	2021 年 5 月 5 日
新支援架構：AWS 基礎安全最佳實務	新預先建置架構現已在中 AWS Audit Manager 提供。如需詳細資訊，請參閱 AWS 基礎安全最佳實務。	2021 年 5 月 5 日
新支援架構：GxP 歐盟附件 11	新預先建置架構現已在中 AWS Audit Manager 提供。如需詳細資訊，請參閱 GxP 歐盟附件 11。	2021 年 4 月 28 日
新支援架構：NIST 800-53 (Rev. 5) 低-中-高	新預先建置架構現已在中 AWS Audit Manager 提供。如需詳細資訊，請參閱 NIST 800-53 (Rev. 5) 低-中-高。	2021 年 3 月 25 日

新支援架構：適用於 CIS AWS Audit Manager Foundations Benchmark v1.3 的 CIS 基準	現在，AWS Audit Manager 中提供了兩個新預先建置架構：適用於 CIS AWS Audit Manager Foundations Benchmark v1.3.0 的 CIS 基準，1 級和適用於 CIS AWS Audit Manager Foundations Benchmark v1.3.0 的 CIS 基準，1 級和 2 級。如需詳細資訊，請參閱適用於 CIS AWS Audit Manager Foundations Benchmark v1.3.0 的 CIS 基準。	2021 年 3 月 22 日
初始版本	AWS Audit Manager 使用者指南和 API 參考初始版本。	2020 年 12 月 8 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。

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。