AMS 加速概念和程序

AMS Accelerate 使用者指南

版本 October 3, 2025

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AMS Accelerate 使用者指南: AMS 加速概念和程序

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商標或商業外觀不得用於 Amazon 產品或服務之外的任何產品或服務，不得以可能在客戶中造成混淆的任何方式使用，不得以可能貶低或損毀 Amazon 名譽的任何方式使用。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能隸屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

Table of Contents

什麼是 AMS Accelerate？

歡迎使用 AMS Accelerate for Amazon Web Services (AWS)。AMS Accelerate 提供各種營運服務，協助您實現卓越營運 AWS。無論您是剛開始使用雲端、想要擴增目前的團隊，還是需要長期的營運解決方案， Accelerate 都可以協助您達成雲端的營運目標。利用自動化、組態和 Runbook 的 AWS 服務 程式庫，我們為新的和現有的 AWS 環境提供end-to-end操作解決方案。

Accelerate 服務利用一組原生 AWS 服務 和 功能，提供一組完整的基礎設施管理功能。其中 AWS 服務， Accelerate 會建立和維護一組精選的監控控制、偵測防護機制、自動化和 Runbook，以合規且安全的方式操作基礎設施。

主題

AMS 操作計劃

AWS Managed Services (AMS) 提供兩種操作計劃：AMS Accelerate 和 AMS Advanced。營運計劃提供一組特定的功能，並具有不同的服務水準、技術功能、需求、價格和限制。我們的營運計畫可讓您靈活地為每個 AWS 工作負載選擇適當大小的操作功能。本節概述功能和差異，以及與每個計劃相關的責任、功能和好處，以便您可以了解哪些操作計劃最適合您的帳戶。

如需兩個操作計劃的詳細功能比較，請參閱 AWS Managed Services 功能。

AMS Accelerate 操作計劃

AMS Accelerate 是 AMS 操作計劃，可協助您操作新環境或現有 AWS 環境的day-to-day基礎設施管理。AMS Accelerate 提供營運服務，例如監控、事件管理和安全性。AMS Accelerate 也為需要定期修補的 Amazon EC2 型工作負載提供選用的修補程式附加元件。

使用 AMS Accelerate，您可以決定 AWS 帳戶 要 AMS Accelerate 操作的 AWS 區域、您希望 AMS Accelerate 操作的 AWS 區域、您需要的附加元件，以及您需要的服務層級協議 (SLAs)。如需詳細資訊，請參閱使用 AMS Accelerate 操作計劃和服務描述。

AMS 進階操作計劃

AMS Advanced 提供完整生命週期服務來佈建、執行和支援您的基礎設施。除了 AMS Accelerate 提供的操作服務之外，AMS Advanced 還包含其他服務，例如登陸區域管理、基礎設施變更和佈建、存取管理和端點安全。

AMS Advanced 會部署登陸區域，讓您遷移 AWS 工作負載並接收 AMS 操作服務。我們的受管多帳戶登陸區域已預先設定 基礎設施，以促進身分驗證、安全性、聯網和記錄。

AMS Advanced 也包含變更和存取管理系統，可透過防止未經授權的存取或對 AWS 基礎設施實作風險變更來保護工作負載。客戶需要使用我們的變更管理系統來建立變更請求 (RFC)，以在 AMS Advanced 帳戶中實作大多數變更。您可以從由我們的安全與營運團隊預先審核的自動化變更程式庫中建立 RFCs，或在 AMS Advanced 認為安全且支援時，請求由營運團隊審查和實作的手動變更。

使用 AMS Accelerate 操作計劃

AMS Accelerate 是 AMS 操作計劃，可操作支援工作負載的 AWS 基礎設施。無論您的工作負載是否已在 AWS 帳戶中，或者您打算遷移新的工作負載，您都可以受益於 AMS Accelerate 操作服務，例如監控和提醒、事件管理、安全管理和備份管理，而無需進行新的遷移、遇到停機時間，或變更您使用 AWS 的方式。AMS Accelerate 也為需要定期修補的 EC2 型工作負載提供選用的修補程式附加元件。

使用 AMS Accelerate，您可以自由地原生使用、設定和部署所有 AWS 服務，或使用您偏好的工具。您可以繼續使用現有的存取和變更機制，同時 AMS 會一致地套用經過驗證的實務，以協助擴展您的團隊、最佳化成本、提高安全性和效率，以及改善彈性。

雖然 AMS Accelerate 可以簡化您的操作，但您仍需負責應用程式開發、部署、測試和調校和管理。AMS Accelerate 只會因為事件、警示、修復和某些服務請求，在您的帳戶中進行變更。AMS Accelerate 不會代表您在帳戶中佈建資源。AMS Accelerate 為會影響應用程式的基礎設施問題提供故障診斷協助，但 AMS Accelerate 不會在沒有您了解和核准的情況下存取或驗證您的應用程式組態。AMS Accelerate 服務和變更會直接在 AWS 主控台和 APIs中提供，因此您可以繼續使用現有的 帳戶搭配 AWS 和可用的 AWS 市集解決方案。AMS Accelerate 不會修改infrastructure-as-code，但可以引導您的團隊進行變更，以遵循最佳營運和安全實務。 AWS CloudFormation

AMS 金鑰術語

- AMS 進階：AMS 進階文件的「服務描述」一節中所述的服務。請參閱服務描述。
- AMS 進階帳戶：始終符合 AMS 進階加入要求中所有需求的 AWS 帳戶。如需 AMS Advanced 優點、案例研究以及聯絡銷售人員的資訊，請參閱 AWS Managed Services。
- AMS Accelerate Accounts： AWS 一直符合 AMS Accelerate Onboarding Requirements 中所有需求的帳戶。請參閱 AMS Accelerate 入門。
- AWS Managed Services：AMS 和 或 AMS Accelerate。
- AWS Managed Services 帳戶：AMS 帳戶和 或 AMS Accelerate 帳戶。
- 關鍵建議： AWS 透過服務請求發出的建議，通知您需要採取動作，以防止 資源或 的潛在風險或中斷 AWS 服務。如果您決定在指定日期之前不遵循關鍵建議，則需自行負責您的決定所造成的任何傷害。
- 客戶請求的組態：任何軟體、服務或其他未識別的組態：
  - 加速：支援的組態或 AMS 加速；服務描述。
  - AMS 進階：支援的組態或 AMS 進階；服務描述。
- 事件通訊：AMS 會與您通訊事件，或者您透過在 AMS Accelerate 支援中心和 AMS 主控台中建立的事件向 AMS 請求事件。AMS 加速主控台提供儀表板上的事件和服務請求摘要，以及支援中心的連結以取得詳細資訊。
- 受管環境：AMS 進階帳戶和 或由 AMS 操作的 AMS Accelerate 帳戶。

  對於 AMS Advanced，這些包括多帳戶登陸區域 (MALZ) 和單一帳戶登陸區域 (SALZ) 帳戶。
- 帳單開始日期： 的下一個工作日 AWS 會收到您在 AWS Managed Services 加入電子郵件中請求的資訊。AWS Managed Services 加入電子郵件是指 傳送給 AWS 您的電子郵件，以收集在帳戶中啟用 AWS Managed Services 所需的資訊。

  對於您後續註冊的帳戶，帳單開始日期是 AWS Managed Services 為註冊帳戶傳送 AWS Managed Services 啟用通知後的第二天。AWS Managed Services 啟用通知會在下列情況發生：

  1. 您授予相容 AWS 帳戶的存取權，並將其交給 AWS Managed Services。
  2. AWS Managed Services 設計並建置 AWS Managed Services 帳戶。
- 服務終止：您可以透過服務請求 AWS 提供至少 AWS Managed Services 30 天的通知，以終止所有 AWS Managed Services 帳戶的 AWS Managed Services 或指定 AWS Managed Services 帳戶的 AWS Managed Services。在服務終止日期，：

  1. AWS 視適用情況，將所有 AWS Managed Services 帳戶或指定 AWS Managed Services 帳戶的控制項交給您，或

2. 適用時，各方會移除授予所有 AWS Managed Services 帳戶或指定 AWS Managed Services 帳戶 AWS 存取權 AWS Identity and Access Management 的角色。

- 服務終止日期：服務終止日期是 30 天必要終止通知期間結束後日曆月的最後一天。如果必要的終止通知期間結束在日曆月的第 20 天之後，則服務終止日期是下一個日曆月的最後一天。以下是終止日期的範例案例。
  - 如果終止通知是在 4 月 12 日提供，則 30 天的通知會在 5 月 12 日結束。服務終止日期為 5 月 31 日。
  - 如果在 4 月 29 日提供終止通知，則 30 天的通知將於 5 月 29 日結束。服務終止日期為 6 月 30 日。
- 您可用 AWS Managed Services：makes 的佈建，您可以從服務開始日期開始，存取和使用每個 AWS Managed Services 帳戶的 AWS Managed Services。 AWS
- 指定 AWS Managed Services 帳戶的終止：您可以透過服務請求 (「AWS Managed Services 帳戶終止請求」) 提供 AWS 通知，以基於任何原因終止指定 AWS Managed Services 帳戶的 AWS Managed Services。

事件管理術語：

- 事件：您的 AMS 環境中的變更。
- 警示：每當支援的 事件 AWS 服務 超過閾值並觸發警示時，就會建立警示並傳送通知到您的聯絡人清單。此外，事件會在您的事件清單中建立。
- 事件：您的 AMS 環境或 AWS Managed Services意外中斷或效能降低，導致 AWS Managed Services或您回報的影響。
- 問題：一或多個事件的共用基礎根本原因。
- 事件解決或事件解決：
  - AMS 已將與該事件相關的所有無法使用 AMS 服務或資源還原為可用狀態，或
  - AMS 已判斷無法使用的堆疊或資源無法還原至可用狀態，或
  - AMS 已啟動您授權的基礎設施還原。
- 事件回應時間：建立事件以及 AMS 透過主控台、電子郵件、服務中心或電話提供初始回應之間的時間差異。
- 事件解決時間：AMS 或您建立事件與事件解決之間的時間差異。
- 事件優先順序：AMS 或您如何將事件的優先順序設定為低、中或高。
  - 低：AMS 服務的非關鍵問題。
  - 中：您受管環境中的 AWS 服務可用，但未如預期般執行 （根據適用的服務描述）。

  - 高：(1) AMS 主控台或受管環境中的一或多個 AMS APIs 無法使用；或 (2) 受管環境中的一或多個 AMS 堆疊或資源無法使用，且無法使用可防止應用程式執行其功能。

  AMS 可能會根據上述準則重新分類事件。
- 基礎設施還原：根據受影響的堆疊範本重新部署現有堆疊，並根據最後一個已知還原點啟動資料還原，除非您另有指定，否則無法解決事件。

基礎設施術語：

- 受管生產環境：客戶生產應用程式所在的客戶帳戶。
- 受管非生產環境：僅包含非生產應用程式的客戶帳戶，例如用於開發和測試的應用程式。
- AMS 堆疊：由 AMS 以單一單位管理的一或多個 AWS 資源群組。
- 不可變基礎設施：Amazon EC2 Auto Scaling 群組 (ASGs) 典型的基礎設施維護模型，其中針對每個部署替換了更新的基礎設施元件（在 AMI AWS中），而不是就地更新。不可變基礎設施的優點是所有元件都會保持同步狀態，因為它們一律從相同的基礎產生。抗擾性與建置 AMI 的任何工具或工作流程無關。
- 互斥基礎設施：典型的基礎設施維護模型，適用於非 Amazon EC2 Auto Scaling 群組且包含單一執行個體或僅包含少數執行個體的堆疊。此模型最緊密地代表傳統的硬體型系統部署，其中系統會在生命週期開始時部署，然後隨著時間的推移，更新會分層到該系統上。系統的任何更新都會個別套用到執行個體，並可能因應用程式或系統重新啟動而導致系統停機（取決於堆疊組態）。
- 安全群組：執行個體的虛擬防火牆，用於控制傳入和傳出流量。安全群組會在執行個體層級執行，而非子網路層級。因此，VPC 中子網路中的每個執行個體可以指派不同的安全群組集。
- 服務水準協議 (SLAs)：與您簽訂 AMS 合約的一部分，定義預期的服務水準。
- SLA 無法使用和無法使用：
  - 您提交的 API 請求會導致錯誤。
  - 您提交的主控台請求導致 5xx HTTP 回應（伺服器無法執行請求）。
  - 在 AMS 受管基礎設施中構成堆疊或資源的任何 AWS 服務 方案都處於「服務中斷」狀態，如服務運作狀態儀表板所示。
  - 在判斷服務點數的資格時，不會考慮直接或間接由 AMS 排除造成的無法使用。除非符合無法使用的條件，否則服務會被視為可用。
- 服務水準目標 (SLOs)：與您簽訂的一部分 AMS 合約，可定義 AMS 服務的特定服務目標。

修補詞彙：

- 強制性修補程式：重大安全性更新，以解決可能危及環境或帳戶安全狀態的問題。「重大安全性更新」是 AMS 支援之作業系統廠商評定為「重大」的安全性更新。
- 發佈的修補程式與發佈的修補程式：修補程式通常按排程發佈和發佈。緊急修補程式會在發現需要修補程式時宣佈，通常在修補程式發佈後不久宣佈。
- 修補程式附加元件：針對利用 AWS Systems Manager (SSM) 功能的 AMS 執行個體進行標籤型修補，讓您可以標記執行個體，並使用您設定的基準和視窗修補這些執行個體。
- 修補程式方法：
  - 就地修補：透過變更現有執行個體來完成的修補。
  - AMI 取代修補：透過變更現有 EC2 Auto Scaling 群組啟動組態的 AMI 參考參數來完成的修補。
- 修補程式提供者 (OS 廠商、第三方 ）：修補程式是由廠商或應用程式管理內文提供。
- 修補程式類型：
  - Critical Security Update (CSU)：受支援作業系統廠商評定為「Critical」的安全性更新。
  - 重要更新 (IU)：由受支援作業系統的廠商評定為「重要」或非安全性更新評定為「關鍵」的安全性更新。
  - 其他更新 (OU)：廠商對非 CSU 或 IU 之受支援作業系統的更新。
- 支援的修補程式：AMS 支援作業系統層級修補程式。廠商會釋出升級，以修正安全漏洞或其他錯誤，或改善效能。如需目前支援的OSs清單，請參閱支援組態。

安全術語：

- Detective Controls：由 AMS 建立或啟用的監控程式庫，可針對不符合安全、操作或客戶控制的組態持續監督客戶受管環境和工作負載，並透過通知擁有者、主動修改或終止資源來採取行動。

服務請求條款：

- 服務請求：您希望 AMS 代表您採取之動作的請求。
- 提醒通知：觸發 AMS 提醒時，AMS 發佈到您的服務請求清單頁面的通知。為您的帳戶設定的聯絡人也會透過設定的 方法 （ 例如電子郵件 ） 收到通知。如果您的執行個體/資源上有聯絡人標籤，並且已同意雲端服務交付管理員 (CSDM) 以標籤為基礎的通知，則標籤中的聯絡資訊 （ 金鑰值 ） 也會收到自動 AMS 提醒的通知。
- 服務通知：AMS 發佈到服務請求清單頁面的通知。

其他詞彙：

- AWS Managed Services介面：適用於 AMS：AWS Managed Services進階主控台、AMS CM API 和 支援 API。對於 AMS Accelerate： 支援 主控台和 支援 API。
- 客戶滿意度 (CSAT)：AMS CSAT 會收到深入分析的通知，包括提供每個案例或通訊的案例通訊評分、每季調查等。
- DevOps：DevOps 是一種開發方法，在所有步驟中都強烈倡導自動化和監控。DevOps 的目標在於縮短開發週期、提高部署頻率，以及更可靠的版本，透過自動化的基礎，結合傳統上分開的開發和操作功能。當開發人員可以管理 操作，並且 操作通知開發時，問題和問題會更快地被發現和解決，而業務目標也更容易實現。
- ITIL：Information Technology Infrastructure Library （稱為 ITIL) 是一種 ITSM 架構，旨在標準化 IT 服務的生命週期。ITIL 分為五個階段，涵蓋 IT 服務生命週期：服務策略、服務設計、服務轉換、服務操作和服務改進。
- IT 服務管理 (ITSM)：一組符合 IT 服務需求的實務。
- 受管監控服務 (MMS)：AMS 會操作自己的監控系統 Managed Monitoring Service (MMS)，其會取用 AWS 運作狀態事件，並彙總 Amazon CloudWatch 資料和其他資料 AWS 服務，通知 AMS 運算子（線上全年無休） 透過 Amazon Simple Notification Service (Amazon SNS) 主題建立的任何警示。
- 命名空間：當您建立 IAM 政策或使用 Amazon Resource Name (ARNs) 時，您可以使用命名空間 AWS 服務 來識別 。您會在識別動作和資源時使用命名空間。

服務描述

AMS Accelerate 是 AWS Managed Services 服務的操作計劃，用於管理 AWS 基礎設施的操作。

AWS Managed Services (AMS) AMS Accelerate 操作計劃功能

AMS Accelerate 提供下列功能：

- 事件管理：

  事件管理是 AMS 服務用來回應您回報事件的程序。

  AMS Accelerate 會主動偵測和回應事件，並協助您的團隊解決問題。您可以使用 AWS Support Center 全年無休地聯絡 AMS Accelerate 營運工程師，並根據您為帳戶選取的回應層級，提供回應時間 SLAs。
- 監控：

  監控是 AMS 服務用來追蹤 資源的程序。

在 AMS Accelerate 中註冊的帳戶設定了 Amazon CloudWatch 事件和警示的基準部署，這些事件和警示已經過最佳化，以減少雜訊並識別可能即將發生的事件。收到提醒後，AMS 團隊會使用自動化修復、人員和程序，將資源恢復到良好狀態，並在適當時與您的團隊互動，以提供有關行為和如何防止該行為的深入見解。如果修復失敗，AMS 會啟動事件管理程序。您可以更新預設組態檔案來變更基準。

- 安全性：

  安全管理是 AMS 服務用來保護 資源的程序。AWS Managed Services 會使用多個控制項來保護您的資訊資產，並協助確保 AWS 基礎設施的安全，包括 AWS Config 規則和 Amazon GuardDuty。

  AMS Accelerate 會維護 AWS Config 規則 和 修復動作的程式庫，以確保您的所有帳戶都符合業界的安全性和操作完整性標準。 AWS Config 規則 會持續追蹤所記錄資源之間的組態變更。如果變更違反任何規則條件，AMS 會報告其調查結果，並允許您根據違規的嚴重性自動或請求修復違規。 AWS Config 規則 協助符合以下標準：網際網路安全中心 (CIS)、國家標準與技術研究所 (NIST) 雲端安全架構 (CSF)、健康保險流通與責任法案 (HIPAA) 和支付卡產業 (PCI) 資料安全標準 (DSS)。

  此外，AMS Accelerate 利用 Amazon GuardDuty 來識別 AWS 環境中可能未經授權或惡意的活動。GuardDuty 調查結果由 AMS 全年無休監控。AMS 會與您合作，根據最佳實務建議了解調查結果和補救措施的影響。AMS 也支援 Amazon Macie 保護您的敏感資料，例如個人健康資訊 (PHI)、個人身分識別資訊 (PII) 和財務資料。最後，AMS 會監控並分類受管帳戶中產生的所有 Amazon Route 53 Resolver ALERT 和 BLOCK 事件，以進一步檢查網路流量並增強其偵測功能。

- 修補程式管理：

  修補程式管理是 AMS 服務用來更新 資源的程序。

  對於具有修補程式附加元件的 AWS 帳戶，AWS Managed Services 會在您選擇的維護時段期間，為支援的作業系統套用並安裝廠商更新至 Amazon EC2 執行個體。AMS 會在修補之前建立執行個體的快照、監控修補程式安裝，並通知您結果。如果修補程式失敗，則 AMS 會調查失敗，並建議您採取動作來修復問題。或者，如果請求，AMS 會將執行個體還原。AMS 提供修補程式合規涵蓋範圍的報告，並建議您為企業建議採取的動作。

- 備份管理：

  AMS 使用備份管理來擷取 資源的快照。

  AWS Managed Services 會為 支援 AWS 的服務建立、監控和存放快照 AWS Backup。您可以在加入帳戶和應用程式時建立 AWS Backup 計劃，藉此定義備份排程、頻率和保留期間。您可以將計劃與 資源建立關聯。AMS 會追蹤所有備份任務，並在備份任務失敗時提醒團隊執行修復。如有需

要，AMS 會利用您的快照在事件期間執行還原動作。AMS 為您提供備份涵蓋範圍報告和備份狀態報告。

- 問題管理：

  AMS 執行趨勢分析以識別和調查問題，並識別根本原因。問題可透過解決方法或永久解決方案來修復，以防止未來再次發生類似的服務影響。解決後，可能會針對任何「高」事件請求事件後報告 (PIR)。PIR 會擷取根本原因和採取的預防性動作，包括實作預防性措施。

- 指定的專家：

  AMS Accelerate 也會指定 Cloud Service Delivery Manager (CSDM) 和 Cloud Architect (CA) 與您的組織合作，並推動卓越營運和安全性。您的 CSDM 和 CA 會在設定和加入 AMS Accelerate 期間和之後為您提供指引，提供營運指標的每月報告，並與您合作，使用 AWS Cost Explorer、成本和用量報告和 等工具來識別潛在的成本節省 Trusted Advisor。

- 操作工具：

  AMS Accelerate 可以在 AWS 中提供工作負載基礎設施的持續操作。我們的修補程式、備份、監控和事件管理服務依賴於使用 IAM 執行個體描述檔在 Amazon EC2 執行個體上安裝和設定 資源標記，以及 AWS Systems Manager (SSM) 和 CloudWatch 代理程式，以授權他們與 SSM 和 Amazon CloudWatch 服務互動。AMS Accelerate 提供 Resource Tagger 等工具，協助您根據規則標記資源，以及自動執行個體組態，以便在 Amazon EC2 執行個體中安裝所需的代理程式。如果您遵循不可變的基礎設施實務，您可以直接在主控台或infrastructure-as-code範本中完成先決條件。

- 成本最佳化：

  AMS Resource Scheduler 會自動啟動和停止 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體、Amazon Relational Database Service (Amazon RDS) 執行個體和 Amazon EC2 Auto Scaling 群組。AMS Resource Scheduler 會停止未使用的資源，並在需要其容量時重新啟動這些資源，以協助您降低營運成本。

- 記錄和報告：

  AWS Managed Services 會彙總和儲存因 CloudWatch、CloudTrail 和 Amazon VPC 流程日誌中的操作所產生的日誌。從 AMS 記錄有助於更快速的事件解決和系統稽核。AMS Accelerate 還提供每月服務報告，摘要 AMS 的關鍵效能指標，包括執行摘要和洞察、營運指標、受管資源、AMS 服務水準協議 (SLA) 合規性，以及有關支出、節省和成本最佳化的財務指標。報告是由指派給您的 AMS 雲端服務交付管理員 (CSDM) 交付。

- 服務請求管理：

若要請求受管環境、AMS AWS 或服務產品的相關資訊，請使用 AMS Accelerate 主控台提交服務請求。您可以提交「如何」服務與功能相關問題 AWS 的服務請求，或請求其他 AMS 服務。

所有 AMS Accelerate 客戶都從事件管理、監控、安全監控、日誌記錄、必要工具、備份管理和報告功能開始。您可以以額外的價格新增 AMS 修補程式管理附加元件。

> **Note**
>
> 如需 中不支援的功能清單 AWS GovCloud (US)，請參閱 的 AMS Accelerate 差異 AWS GovCloud (US)

支援的組態

AMS Accelerate 支援下列組態：

- 語言：英文。
- 區域：請參閱 AWS Regional Services 網頁中 AWS Managed Services 支援的 AWS 區域。

> **Note**
>
> 2019 年 3 月 20 日之前推出的 AWS 區域會被視為「原始」區域，並預設為啟用。在此日期之後引入的區域為「選擇加入」區域，預設為停用。如果您的帳戶使用多個區域，而且您加入 AMS Accelerate 到已啟用「選擇加入」區域的帳戶做為預設區域，則 AMS 報告功能只能在該區域中使用。如果您未設定預設區域，則您造訪的最後一個區域是您的預設區域。
> 若要啟用區域，請參閱啟用區域。若要設定預設區域，請參閱選擇區域。如需每個區域的選擇加入狀態清單，請參閱《Amazon Elastic Compute Cloud 使用者指南》中的可用區域。

- 作業系統架構 (x86-64 或 ARM64)：Systems Manager 和 CloudWatch 支援的任何 。
- 支援的作業系統：
  - AlmaLinux 8.3-8.9、9.x (AlmaLinux 僅支援 x86 架構)
  - Amazon Linux 2023
  - Amazon Linux 2 (預期的 AMS 支援結束日期為 2026 年 6 月 30 日)
  - Oracle Linux 9.x、8.x
  - Red Hat Enterprise Linux (RHEL) 9.x、8.x

- SUSE Linux Enterprise Server 15 SP6
- SUSE Linux Enterprise Server for SAP 15 SP3 及更新版本
- Microsoft Windows Server 2022、2019、2016
- Ubuntu 20.04、22.04、24.04

- 支援的終止支援 (EOS) 作業系統：

> **Note**
>
> 終止支援 (EOS) 作業系統在作業系統製造商的一般支援期間之外，且具有更高的安全風險。只有當 AMS 所需的代理程式支援作業系統和...時，EOS 作業系統才會被視為支援的組態。
>
> 1. 您對作業系統廠商有延伸的支援，可讓您接收更新，或
> 2. 使用 EOS 作業系統的任何執行個體都遵循加速使用者指南中 AMS 指定的安全控制，或
> 3. 您遵守 AMS 要求的任何其他補償性安全控制。
>
> 如果 AMS 不再支援 EOS 作業系統，AMS 會發出關鍵建議來升級作業系統。
> AMS 所需的代理程式可能包括但不限於：Amazon CloudWatch AWS Systems Manager、端點安全 (EPS) 代理程式和 Active Directory (AD) Bridge （僅限 Linux)。

  - Ubuntu Linux 18.04
  - SUSE Linux Enterprise Server 15 SP3, SP4 和 SP5
  - SUSE Linux Enterprise Server for SAP 15 SP2
  - SUSE Linux Enterprise Server 12 SP5
  - SUSE Linux Enterprise Service for SAP 12 SP5
  - Microsoft Windows Server 2012/2012 R2
  - Red Hat Enterprise Linux (RHEL)：7.x
  - Oracle Linux 7.5-7.9
- 如果您使用 AWS Control Tower 管理您的多帳戶環境，請確定您正在執行最新版本的 AWS Control Tower ，以與 Accelerate 相容。不支援使用 2.7 以前 AWS Control Tower 版本 (2021 年 4 月發行）的環境。如需如何更新的資訊 AWS Control Tower，請參閱更新您的登陸區域。

支援的服務

AWS Managed Services 為下列服務提供操作管理支援服務 AWS 。每個 AWS 服務都是不同的，因此，AMS 的操作管理支援層級會根據基礎 AWS 服務的性質和特性而有所不同。如果您請求 AWS Managed Services 為下列清單中未明確識別為支援的任何軟體或服務提供服務，則根據服務條款，為此類客戶請求組態提供的任何 AWS Managed Services 都將被視為「Beta Service」。

- 事件：所有 AWS 服務
- 服務請求：所有 AWS 服務
- 修補：Amazon EC2
- 備份和還原： AWS 服務 支援的所有項目 AWS Backup。如需 支援的服務清單 AWS Backup，請參閱AWS Backup 支援的資源。
- 資源排程器：Amazon Elastic Compute Cloud (Amazon EC2) 執行個體、Amazon Relational Database Service (Amazon RDS) 和 Amazon EC2 Auto Scaling 群組
- 監控操作事件的服務：支援的檢查和 Trusted Advisor、Application Load Balancer、Aurora、Amazon EC2、Elastic Load Balancing、Amazon FSx for NetApp ONTAP、Amazon FSx for Windows File Server、NAT 閘道 （網路位址轉譯 (NAT) 服務）、OpenSearch AWS Health Dashboard、Amazon Redshift、Amazon Relational Database Service (Amazon RDS)、Site-to-Site VPN。若要進一步了解 AMS Accelerate 在服務中監控哪些項目，請參閱 AMS 中基準監控的提醒。
- 由安全 Config Rules： AWS Account 監控的服務 GuardDuty、 Macie、 Amazon API Gateway AWS Certificate Manager AWS Config、、 CloudTrail、 CloudWatch AWS CodeBuild、 AWS Database Migration Service、 Amazon DynamoDB、 Amazon EC2、 Amazon ElastiCache、 Amazon Elastic Block Store (Amazon EBS)、 Amazon Elastic File System (Amazon EFS)、 Amazon Elastic Kubernetes Service (Amazon EKS)， Elastic Load Balancing、 Amazon OpenSearch Service、 Amazon EMR， AWS Identity and Access Management (IAM) AWS Key Management Service AWS Lambda、、 Amazon Redshift、 Amazon Relational Database Service、 Amazon S3、 Amazon SageMaker AI AWS Secrets Manager 、 Amazon Simple Notification Service AWS Systems Manager、 Amazon VPC （安全群組、 磁碟區、 彈性 IP 地址、 VPN 連線、 網際網路閘道）、 Amazon VPC 流程日誌。如需詳細資訊，請參閱Accelerate 中的組態合規和Accelerate 中的資料保護。您可以在我們的私有安全性指南中找到其他 AMS 安全資訊 AWS Artifact，這些資訊可透過 AWS Managed Services 的報告索引標籤存取。

> **Note**
>
> AMS Accelerate for the Middle East (UAE) 區域支援一組範圍內功能，如下表所述。存取此區域中的 AMS 帳戶主控台和執行個體完全由傳入服務請求觸發程序驅動。如需中東（阿拉伯聯合大公國）區域中 Accelerate 可用性的詳細資訊，請洽詢您的客戶經理或 AWS Cloud Service Delivery Manager (CSDM)。

AMS 加速中東（阿拉伯聯合大公國）區域的範圍內功能	功能描述
事件管理	AMS 提供事件回應和協助，以協助您的團隊解決問題。若要讓 AMS 協助您管理事件，您需要提交服務請求。AMS 不會主動偵測或回應此區域中的事件。
監控	收到您的服務請求後，AMS 可以協助資源修復。AMS 使用自動化修復、人員和程序，讓您的資源恢復正常狀態。AMS 不會在此區域中設定基準 CloudWatch 事件和警示。如果您有現有的監控工具，則可以根據雲端架構師 (CA) 和 CSDM 評估主動追蹤您的資源。
安全性	收到來自您的服務請求後，AMS 可以協助修復安全問題。AMS 不會部署安全控制，例如 AWS Config 規則 和 GuardDuty，或監控此區域中的安全調查結果。如果您有現有的安全工具，可根據 CA 和 CSDM 評估提供主動安全監控。
修補管理	AMS 可以在選擇的維護時段將廠商更新套用至支援作業系統的 Amazon EC2 執行個體，並建立預先修補快照。若要讓 AMS 協助您管理修補程式，您需要提交服務請求。AMS 修補程式通知和報告不適用於此區域。
備份管理	AMS 可以為 AWS 服務 支援的 建立和存放快照 AWS Backup，並協助備份修復。若要讓

AMS 加速中東 （阿拉伯聯合大公國） 區域的範圍內功能	功能描述
	AMS 協助您進行備份管理，您需要提交服務請求。AMS 不會追蹤此區域中的備份任務。
指定的專家	AMS 指定 Cloud Architect (CA) 和 Cloud Service Delivery Manager (CSDM) 與客戶組織合作，並推動卓越營運和安全性。
服務請求管理	若要請求受管環境、AMS 或 AWS 服務 產品的相關資訊，請透過 AMS Accelerate 主控台提交服務請求。您可以提交有關 AWS 服務 和 功能問題的「如何」服務請求，或請求此區域中可用的 AMS 服務，如此表格所述。

角色和責任

AMS Accelerate 負責、負責、諮詢和告知 或 RACI，矩陣會將主要責任指派給客戶或 AMS 以進行各種活動。此表格說明您的 (「客戶」) 責任與我們的 (「AMS Accelerate」) 責任。

AMS Accelerate 執行的變更範圍 本節列出 AMS 獲授權對您的帳戶進行變更的特定情況；以及 AMS 從未進行的一些變更類型。

AMS Accelerate RACI 矩陣

AMS Accelerate 會管理您的 AWS 基礎設施。下表提供在受管環境中執行的應用程式生命週期中，您和 AMS Accelerate 的角色和責任的概觀。

- R 代表負責方，負責執行工作以達成任務。
- C 代表 Consulted；尋求意見的一方，通常是主題專家；以及與之進行雙邊溝通的一方。
- 我代表知情；收到進度通知的一方，通常是在任務完成時。

> **Note**
>
> 有些區段同時包含 AMS 和客戶的 'R'。這是因為在 AWS 共同責任模型中，AMS 和客戶都擁有共同所有權來回應基礎設施和應用程式問題。

活動	客戶	AWS Managed Services (AMS)
AMS 模式		
建立新的模式	I	R
部署和自訂模式	R	C、I
測試和移除模式	R	I
應用程式生命週期		
應用程式開發	R	I
應用程式基礎設施需求、分析和設計	R	I
應用程式部署	R	I
AWS 資源部署	R	I
應用程式監控	R	I
應用程式測試/最佳化	R	I
疑難排解和解決應用程式問題	R	I
故障診斷和解決問題	R	I
AWS 基礎設施支援的監控	C	R
AWS 網路問題的事件回應	C	R
AWS 資源問題的事件回應	C	R
受管帳戶加入		
授予 AMS 團隊和工具對 AWS 受管帳戶的存取權	R	C

活動	客戶	AWS Managed Services (AMS)
在帳戶或環境中實作變更，以允許在帳戶中部署工具。例如，服務控制政策 (SCPs的變更	R	C
在 EC2 執行個體中安裝 SSM 代理程式	R	C
安裝和設定提供 AMS 服務所需的工具。例如，CloudWatch 代理程式、修補指令碼、警示、日誌等	I	R
管理 AMS 工程師的存取和身分生命週期	I	R
收集所有必要的輸入以設定 AMS 服務。例如，修補維護時段持續時間、排程和目標	R	I
請求 AMS 服務的組態，並提供所有必要的輸入	R	I
依客戶要求設定 AMS 服務。例如，修補程式維護時段、資源標記程式和警示管理員	C	R
管理用於存取 AWS 帳戶和執行個體的本機目錄服務的使用者生命週期及其許可	R	I
建議預留執行個體最佳化	I	R
將帳戶加入（信任的修復程式）	C、I	R
修補程式管理		
收集所有必要的輸入，以設定修補程式維護時段、修補程式基準和目標	R	I
請求修補程式維護時段和基準的組態，並提供所有必要的輸入	R	I
依客戶要求設定修補程式維護時段、修補程式基準和目標	C	R
監控 EC2 執行個體的支援作業系統和預先安裝之支援作業系統的適用更新	I	R

活動	客戶	AWS Managed Services (AMS)
報告支援的作業系統和維護時段涵蓋範圍遺失更新	I	R
在套用更新之前擷取執行個體的快照	I	R
將更新套用至每個客戶組態的 EC2 執行個體	I	R
調查 EC2 執行個體的失敗更新	C	R
更新自動擴展群組 (ASGs) 的 AMIs 和堆疊	R	C
修補 Windows 作業系統，以及安裝在受 Windows Update 管理之作業系統上的 Microsoft 套件	I	R
修補程式安裝的應用程式、軟體或應用程式相依性不受 Windows Update 管理	R	I
修補 Linux 作業系統和作業系統原生套件管理員啟用管理的任何套件 （例如 Yum、Apt、Zypper)	I	R
修補程式安裝的應用程式、軟體或應用程式相依性，並非由 Linux 作業系統的原生套件管理員管理	R	I
備份		
收集所有必要的輸入，以設定備份計畫和目標資源	R	I
請求 Backup 計劃的組態，並提供所有必要的輸入	R	I
依客戶要求設定備份計劃和目標	C	R
指定備份排程和目標資源	R	I
執行每個計劃的備份	I	R
調查失敗的備份任務	I	R

活動	客戶	AWS Managed Services (AMS)
備份任務狀態和備份涵蓋範圍的報告	I	R
驗證備份	R	I
請求備份還原支援 AWS 服務資源的資源，做為事件管理的一部分	R	I
為支援的 AWS 服務的資源執行備份還原活動	I	R
還原受影響的自訂或第三方應用程式	R	I
聯網		
受管帳戶 VPCs、IGWs、直接連線和其他 AWS 網路服務的佈建和組態	R	I
在受管帳戶中設定和操作 AWS Security Groups/NAT/NACL	R	I
客戶網路內的網路組態和實作 （例如 DirectConnect)	R	I
AWS 網路內的網路組態和實作	R	I
AMS 為網路安全定義的監控，包括安全群組	I	R
網路層級記錄組態和管理 (VPC 流程日誌和其他）	I	R
日誌		
記錄所有應用程式變更日誌	R	I
記錄 AWS 基礎設施變更日誌	I	R
啟用和彙總 AWS 稽核線索	I	R
從 AWS 資源彙總日誌	I	R
監控和修復		
收集所有必要的輸入，以設定警示管理員、資源標記器和警示閾值	R	I

活動	客戶	AWS Managed Services (AMS)
請求警示管理員的組態，並提供所有必要的輸入	R	I
依客戶要求設定警示管理員、資源標記器和警示閾值。	C	R
依客戶組態部署 AMS CloudWatch 基準指標和警示	I	R
使用基準 CloudWatch 指標和警示監控支援的 AWS 資源	I	R
調查來自 AWS 資源的提醒	C	R
根據定義的組態修正提醒，或建立事件	I	R
定義、監控和調查客戶特定的監視器	R	I
從應用程式監控調查提醒	R	C
設定修復 Trusted Advisor 檢查	R	C
自動修復支援的 Trusted Advisor 檢查	I	R
手動修復支援的 Trusted Advisor 檢查	R	C
報告修復狀態	I	R
修復失敗的故障診斷	R	C
安全架構		
檢閱 AMS 資源和程式碼是否有安全問題和潛在威脅	I	R
在 AMS 資源和程式碼中實作安全控制，以降低安全風險	I	R
為帳戶及其 AWS 資源的安全管理啟用支援的 AWS 服務	I	R
管理 AMS 工程師的帳戶和作業系統存取的特權憑證	I	R
安全風險管理		

活動	客戶	AWS Managed Services (AMS)
監控支援的安全管理 AWS 服務，例如 GuardDuty 和 Macie	I	R
定義並建立 AMS 定義的 Config 規則，以偵測 AWS 資源是否符合網際網路安全中心 (CIS) 和 NIST 安全最佳實務。	I	R
監控 AMS 定義的 Config 規則	I	R
報告 Config 規則的一致性狀態	I	R
定義必要的 Config 規則清單並進行修復	I	R
評估修復 AMS 定義組態規則的影響	R	I
請求修復 AWS 帳戶中 AMS 定義的 Config 規則	R	I
追蹤從 AMS 定義的 Config 規則中排除的資源	R	I
修復 AWS 帳戶中支援的 AMS 定義 Config 規則	C	R
修復 AWS 帳戶中不支援的 AMS 定義組態規則	R	I
定義、監控和調查客戶特定的 Config 規則	R	I
事件管理		
通知 AMS 在 AWS 資源中偵測到的事件	I	R
通知 AWS 資源中的事件	R	I
根據監控通知 AWS 資源的事件	I	R
處理應用程式效能問題和中斷	R	I
分類事件優先順序	I	R
提供事件回應	I	R

活動	客戶	AWS Managed Services (AMS)
為具有可用備份的資源提供事件解決方案或基礎設施還原	C	R
安全事件回應 – 準備		
通訊		
提供並更新 AMS 在安全事件通知和安全呈報期間使用的客戶安全聯絡人詳細資訊	R	I
存放和管理提供的客戶安全聯絡人詳細資訊，以便在安全事件和安全呈報期間使用	C	R
訓練		
在事件回應程序期間為客戶提供支援 AMS 的文件	I	R
透過安全遊戲日在事件回應程序期間練習共同的責任	R	R
資源管理		
設定支援的 AWS 服務 警示、警示關聯性、降噪和其他規則的安全管理	I	R
維護 AWS 資源 (Amazon EC2、Amazon S3 等） 的全面清查，包括每個資產對業務的價值和重要性的詳細資訊。此資訊有助於判斷有效的遏制策略	R	C
使用 AWS 標籤來識別資源和工作負載	R	C
定義和設定日誌保留和封存	I	R
透過定義和強制執行組織 AWS 帳戶、服務和存取管理的安全政策和組態，建立安全的基準	R	I
安全事件回應 - Detect		
記錄、指標和監控		

活動	客戶	AWS Managed Services (AMS)
設定記錄和監控，以啟用執行個體和帳戶的事件管理	I	R
監控 AWS 服務 支援的安全提醒	I	R
部署和管理端點安全工具	R	I
使用端點安全性監控執行個體上的惡意軟體	R	I
透過傳出訊息通知客戶偵測到的事件	I	R
協調內部利益相關者通訊和領導更新，以改善回應時間	R	I
定義、部署和維護 AMS 標準偵測服務（例如 Amazon GuardDuty 和 AWS Config)	C	R
記錄 AWS 基礎設施變更日誌	R	I
啟用和設定記錄、監控以啟用應用程式的事件管理	R	C
在支援 AWS 的安全服務（例如 Amazon GuardDuty上實作和維護允許清單、拒絕清單和自訂偵測	R	R
安全事件報告		
通知 AMS 可疑活動或作用中的安全調查	R	I
將偵測到的安全事件和事件通知客戶	I	R
通知可能觸發安全事件回應程序的計劃事件	R	I
安全事件回應 - 分析		
調查和分析		
對受支援偵測來源產生的受支援安全提醒執行初始回應	I	R

活動	客戶	AWS Managed Services (AMS)
使用可用資料評估 false/true 陽性	R	R
視需要產生要與客戶共用之受影響執行個體的快照	I	R
執行鑑識任務，例如監管鏈、檔案系統分析、記憶體鑑識和二進位分析	R	C
收集應用程式日誌以協助調查	R	I
收集資料和日誌，以協助調查安全提醒	R	R
讓 中的SMEs AWS 服務 參與安全調查	C	R
在調查期間，將受支援的調查日誌分享 AWS 服務 給客戶	I	R
通訊		
從受管資源的 AMS 偵測來源傳送提醒和通知	I	R
管理應用程式安全事件的提醒和通知	R	I
在安全事件調查期間與客戶安全聯絡人互動	R	I
安全事件回應 - 包含		
遏制策略和執行		
評估風險並決定遏制策略，認可潛在的服務影響	R	C
備份受影響的系統以進行進一步分析	I	R
包含應用程式和工作負載（透過應用程式特定的組態或回應活動）	R	C
根據安全事件和受影響的資源定義遏制策略	I	R
啟用受影響系統時間點備份的加密和安全儲存	C	R
執行支援 AWS 的資源遏制動作，包括 EC2 執行個體、網路和 IAM	I	R

活動	客戶	AWS Managed Services (AMS)
安全事件回應 - 根除		
根除策略和執行		
根據安全事件和客戶應用程式工作負載上受影響的資源來定義根除選項	C	R
決定同意的根除策略、根除執行時間和後果	R	I
根據 AMS 受管工作負載上的安全事件和受影響的資源定義根除步驟	C	R
消除威脅並強化 AWS 資源，包括 EC2 執行個體、網路和 IAM 根除	R	C
消除威脅並強化應用程式和工作負載（透過應用程式特定的組態或回應活動）	R	I
安全事件回應 - 復原		
復原準備和執行		
依客戶要求設定備份計劃和目標	I	R
檢閱備份計劃以還原 AMS 受管工作負載	R	I
為支援的資源執行備份還原活動 AWS 服務	I	R
備份客戶應用程式、應用程式組態和部署設定，並檢閱備份計畫，以在事件發生後還原客戶應用程式和工作負載	R	I
還原應用程式和客戶工作負載（透過應用程式特定的還原步驟）	R	I
安全事件回應 – 事件後報告		
事件後報告		
視需要與客戶事後事件分享適當的經驗教訓和行動項目	I	R

活動	客戶	AWS Managed Services (AMS)
問題管理		
關聯事件以識別問題	I	R
針對問題執行根本原因分析 (RCA)	I	R
修復問題	I	R
識別和修復應用程式問題	R	I
服務管理		
使用服務請求請求資訊	R	I
回覆服務請求	I	R
提供成本最佳化建議	I	R
準備和交付每月服務報告	I	R
變更管理		
在受管環境中佈建和更新資源的變更管理程序和工具	R	I
應用程式變更行事曆的維護	R	I
即將到來的維護時段通知	R	I
記錄 AMS Operations 所做的變更	I	R
成本最佳化		
收集所有必要的輸入以設定 Resource Scheduler	R	I
請求資源排程器的加入、組態，並提供所有必要的輸入	R	I
依客戶組態部署資源排程器	C、I	R

活動	客戶	AWS Managed Services (AMS)
在客戶帳戶上停用和啟用資源排程器	R	C
建立、刪除、描述和更新排程	C	R
建立、刪除、描述和更新期間	C	R
使用 Resource Scheduler 調查問題並進行疑難排解	I	R
請求將資源排程器移出	R	I
從 帳戶移出資源排程器	C、I	R

AMS Accelerate 執行的變更範圍

AMS Accelerate 只會針對接下來所述的特定目的和情況進行變更。AMS 只會使用主控台或 APIs 在基礎設施層級進行變更。AMS 絕不會變更您的應用程式、控制項或網域層。您可以使用一組預先建置的查詢來查看 AMS （或其他使用者） 所做的任何變更；若要執行此操作，請參閱 追蹤 AMS Accelerate 帳戶中的變更。

AWS resources

AMS Accelerate 僅在下列情況中部署或更新 AWS 資源：

- 部署和更新 AMS 所需的工具和資源。
- 作為 AMS 監控的一部分，以回應事件和警示。
- 作為 的一部分來修復安全問題 在 Accelerate 中回應違規（使不合規的資源符合安全最佳實務）。
- 在修補和還原期間，做為事件回應的一部分。
- 回應客戶請求以設定 AMS 功能時，如下所示：
  - 警示管理員
  - 資源標記程式
  - 修補程式基準和維護時段
  - 資源排程器

- 備份計劃

AMS Accelerate 不會在這些情況下部署或更新資源。如果您需要 AMS 的協助，在其他情況下進行變更，請考慮使用隨需操作。

作業系統軟體

AMS Accelerate 可以透過服務水準協議中定義的事件解決，在無法使用的情況下變更您的作業系統軟體。AMS 也可以變更您的作業系統，做為 的一部分AMS Accelerate 中的自動化執行個體組態。

應用程式程式碼和組態

AMS Accelerate 絕不會修改您的程式碼（例如 AWS CloudFormation 範本、其他infrastructure-as-code範本或 Lambda 函數），但可以引導您的團隊進行需要變更才能遵循最佳操作和安全實務。AMS Accelerate 為會影響應用程式的基礎設施問題提供疑難排解協助，但 AMS Accelerate 無法存取或驗證您的應用程式組態。

Accelerate 中不支援的作業系統功能

不支援的作業系統是 中未列出的任何作業系統支援的組態。AMS 會將具有不支援作業系統的執行個體視為「客戶請求組態」，其受到 AWS Beta 版和預覽版服務條款的約束。

下列有限的 AMS 功能集可供具有不支援作業系統的執行個體使用：

功能	備註
事件管理	AMS 提供事件回應。
服務請求管理	AMS 會回應服務請求。
監控	AMS 會監控和回應 Amazon EC2 系統狀態檢查和執行個體狀態檢查。系統狀態檢查包括：網路連線中斷、系統電源中斷、實體主機上的軟體問題，以及實體主機上會影響網路連線能力的硬體問題。 執行個體狀態檢查包括：網路或啟動組態不正確、記憶體耗盡、檔案系統損毀，以及核心不相容。

功能	備註
安全管理	AMS 會監控和回應 Amazon EC2 GuardDuty 調查結果和AWS Config 規則。
備份管理	AMS 使用 AMS 自訂的 AWS Backup 計劃和保存庫，在 Accelerate for EC2 中提供持續性管理。

聯絡和呈報

您有指定的雲端服務交付經理 (CSDM)，可提供跨 AMS Accelerate 的諮詢協助，並對受管環境的使用案例和技術架構有詳細的了解。CSDMs會視情況與帳戶管理員、技術帳戶管理員、AWS Managed Services 雲端架構師 (CAs) 和 AWS 解決方案架構師 (SAs) 合作，協助啟動新專案，並在整個軟體開發和操作程序中提供最佳實務建議。CSDM 是 AMS 的主要聯絡人。CSDM 的主要責任為：

- 與客戶組織和主持每月服務審查會議。
- 提供有關安全性、環境軟體更新和最佳化機會的詳細資訊。
- 擁護您的需求，包括 AMS Accelerate 的功能請求。
- 回應並解決帳單和服務報告請求。
- 提供財務和容量最佳化建議的洞見。

聯絡時間

您可以因不同原因在不同時間聯絡 AMS Accelerate。

功能	AMS Accelerate
	高級方案
服務請求	全年無休
事件管理 (P2-P3)	全年無休
備份與復原	全年無休
修補管理	全年無休

功能	AMS Accelerate
	高級方案
監控和提醒	全年無休
雲端服務交付管理員 (CSDM)	週一至週五：08：00–17：00，當地上班時間

營業時間

功能	AMS Accelerate
	高級方案
服務請求	全年無休
事件管理 (P1)	全年無休
事件管理 (P2-P3)	全年無休
備份與復原	全年無休
修補管理	全年無休
監控和提醒	全年無休
雲端服務交付管理員 (CSDM)	週一至週五：09：00–17：00，當地上班時間

呈報路徑

根據套用至帳戶的 AMS 服務水準協議，AMS 全年無休支援客戶使用 Incident Management and Service Request Management。

若要報告影響受管環境的 AWS 或 AMS 服務效能問題，請使用 AMS 主控台並提交事件案例。如需詳細資訊，請參閱提交事件以加速。如需 AMS 事件管理的一般資訊，請參閱 AMS Accelerate 中的事件管理。

若要要求資訊或建議，或從 AMS 請求其他服務，請使用 AMS 主控台並提交服務請求。如需詳細資訊，請參閱在 Accelerate 中建立服務請求。如需 AMS 服務請求的一般資訊，請參閱 Accelerate 中的服務請求管理。

Accelerate 的資源庫存

AMS Accelerate 部署到您 AWS 帳戶 或 帳戶的所有資源都列在resource_inventory.zip檔案 resource_inventory.xlsx 試算表中 （壓縮）。

> **Note**
>
> 在資源名稱欄中，字首 CFN： 表示 CloudFormation 邏輯 ID，而不是資源名稱。這些會顯示於未命名的資源，例如 S3 儲存貯體政策。

AMS 會部署一組服務，如中所述服務描述。當部署到空帳戶時，部署它們的成本很低，但成本會隨著使用率的增加而增加。例如，會建立日誌，並在資源變更時叫用組態規則。

對組態規則進行多次變更時，可能會觸發多個組態合規調用，進而產生更高的成本。同樣的可能性適用於用於監控執行個體的 Amazon CloudWatch — 您的監控越精細，服務的成本就越高。 AWS Backup 是另一個範例。如果您儲存了多個備份，或者如果您的保留期較高，則會使用更多儲存空間且成本較高。

這些數字很難預測。在與雲端服務交付經理 (CSDM) 進行每月業務審查期間，請追蹤變更並努力找出降低成本的機會領域。

AMS Accelerate 入門

如果您還沒有 AWS Managed Services (AMS) 操作帳戶，請先使用我們的 AWS Managed Services - 聯絡銷售頁面聯絡 Amazon Web Services (AWS) 銷售代表。

在您註冊 AMS 之後，AMS Accelerate 團隊會引導您完成每個 的下列加入程序 AWS 帳戶。

檢閱此處的功能集：AWS Managed Services 功能

> **Note**
>
> AMS Accelerate 支援 GovCloud 區域。如果您的服務將位於 中 AWS GovCloud (US) Region，另請參閱 入門 AWS GovCloud (US)。

Accelerate 的帳戶加入程序

將帳戶加入 AMS Accelerate 有四個階段。

1. 步驟 1. Accelerate 中的帳戶探索 會評估您帳戶的目前狀態，並識別加入您帳戶的技術封鎖程式。
2. 步驟 2. 在 Accelerate 中加入管理資源 會要求您接受條款與條件；並為 AMS Accelerate 雲端架構師 (CAs) 建立加入角色，他們將協助您設定安全基準，並視需要解決問題。
3. 步驟 3。使用預設政策加入 AMS 功能 適用於 Accelerate 功能，例如監控、修補和備份。
4. 步驟 4. 在 Accelerate 中自訂功能 可確保已為您的應用程式正確設定資源，包括 EC2 執行個體。

加速入門先決條件

在您開始加入程序之前，請務必了解 Accelerate 元件所依賴的技術相依性。

> **Note**
>
> 若要使用 AMS Accelerate，您必須參與兩個支援的 支援 計畫之一：Enterprise On-Ramp 或 Enterprise。開發人員和商業計劃不符合 AMS Accelerate 的資格。若要進一步了解不同的計劃，請參閱比較 支援 計劃。

AMS Accelerate VPC 端點

VPC 端點可讓您的 VPC 與支援的 AWS 服務，以及採用 技術的 VPC 端點服務之間的私有連線 AWS。如果您需要篩選傳出網際網路連線，請設定下列 VPC 服務端點，以確保 AMS Accelerate 具有與其服務相依性的連線。

> **Note**
>
> 在下列清單中，*##*代表 AWS 區域的識別符，例如`us-east-2`美國東部（俄亥俄）區域。

```
com.amazonaws.region.logs
com.amazonaws.region.monitoring
com.amazonaws.region.ec2
com.amazonaws.region.ec2messages
com.amazonaws.region.ssm
com.amazonaws.region.ssmmessages
com.amazonaws.region.s3
com.amazonaws.region.events
```

如需如何設定 AWS VPC 端點的資訊，請參閱 VPC 端點。

> **Note**
>
> 如果您要為上述所有服務在帳戶中建立 VPC 端點，請參閱此範例 AWS CloudFormation 範本。您可以更新此範本，並根據您的使用案例移除或新增 VPC 端點定義。

Accelerate 中的傳出網際網路連線

1. 下載 `egressMgmt.zip`。
2. 開啟 **`ams-egress.json`** 檔案。
3. 尋找 JSON 屬性下的 URLs：
   - `WindowsPatching`
   - `RedHatPatching`
   - `AmazonLinuxPatching`
   - `EPELRepository`
4. 允許存取這些 URLs。

在 Accelerate 中測試傳出連線

使用下列其中一種方法測試傳出連線。

> **Note**
>
> 在執行指令碼/命令之前，請將紅色##取代為您的區域識別符，例如 us-east-1。

Windows PowerShell 指令碼

```
$region = 'region'
@('logs','monitoring','ec2','ec2messages','ssm','ssmmessages','s3','events') | `
ForEach-Object { `
Test-NetConnection ("$_" + '.' + "$region" + '.amazonaws.com') -Port 443 } | `
Format-Table ComputerName,RemotePort,RemoteAddress,PingSucceeded,TcpTestSucceeded -
AutoSize
```

Linux 命令

```
for endpoint in logs monitoring ec2 ec2messages ssm ssmmessages s3 events; do nc -zv
 $endpoint.region.amazonaws.com 443; done
```

Accelerate 中的 Amazon EC2 Systems Manager

您必須在您希望 AMS 管理的所有 EC2 執行個體上安裝 AWS Systems Manager 代理程式 (SSM 代理程式）。您也需要新增 SSM Agent 所需的儲存貯體許可。如需包含 Amazon EC2 的概觀，請參閱 步驟 3。使用預設政策加入 AMS 功能。

Accelerate 中的 IAM

若要允許使用者讀取和設定 AMS Accelerate 功能，例如存取 AMS 主控台或設定備份，您必須在 AWS Identity and Access Management (IAM) 中授予明確許可來執行這些動作。如需 IAM 政策範例，請參閱使用 AMS 功能的許可。

步驟 1. Accelerate 中的帳戶探索

AMS 會在帳戶探索期間與您合作，以評估您帳戶的目前狀態，並識別加入您帳戶的技術封鎖程式。AMS 不會在帳戶探索階段提供操作服務。AMS 使用AWSServiceRoleForSupport服務連結角色來識別技術封鎖程式，然後與您一起修復它們，然後再進入帳戶層級加入階段。

Accelerate 中的帳戶探索程序

為了協助您分析和探索您的帳戶，AMS 會執行操作檢查，透過唯讀 API 呼叫來識別技術封鎖程式。您的帳戶加入 AMS 後，這些檢查會隨需執行，以維護帳戶狀態。AMS 會在需要時與您合作，修復與這些檢查相關聯的任何問題清單。AMS 使用下列操作檢查和唯讀 API 動作做為帳戶探索的一部分：

操作檢查	用途	AWS 使用的 API 呼叫
AWS Control Tower 版本評估	識別 AWS Control Tower 版本，以確保它是加入 的最低支援版本 AWS 帳戶。	• ControlTower:GetLandingZone • ControlTower:ListEnabledControls • ControlTower:ListLandingZones
AWS CloudTrail 評估	識別要加入 的 AWS CloudTrail 線索及其組態 AWS 帳戶 ，以將 CloudTrail 線索成本降至最低。	• CloudTrail:GetTrail • CloudTrail:ListTrails • S3:GetBucketOwnershipControls • S3:GetBucketPolicy • KMS:GetKeyPolicy • CloudTrail:GetEventSelectors • S3:GetBucketLogging • S3: GetBucketLifecycleConfiguration • S3: GetBucketEncryption
AWS CloudFormation 勾點評估	識別加入中封鎖 AMS 服務部署 AWS 帳戶 的 CloudFormation 勾點 AWS 帳戶。	• CloudFormation:ListTypes

操作檢查	用途	AWS 使用的 API 呼叫
Amazon EC2 執行個體評估	識別 中未執行 AWS Systems Manager Agent AWS 帳戶 (SSM Agent) 且 AMS 不支援的 EC2 執行個體。	• `EC2:DescribeInstances` • `EC2:DescribeImages` • `SSM:DescribeInstanceInformation`

AMS Accelerate 遵循業界最佳實務，以符合和維護合規資格。您帳戶的 AMS Accelerate Discovery AWS CloudTrail 存取權會透過 AWSServiceRoleForSupport 服務連結角色記錄在 中。這有助於監控和稽核需求。如需 的詳細資訊 AWS CloudTrail，請參閱AWS CloudTrail 《 使用者指南》。

步驟 2. 在 Accelerate 中加入管理資源

這是入門管理資源程序的概觀。

您接受條款

您的雲端服務交付管理員 (CSDM) 會引導您完成接受程序。您需要接受條款與條件、選取、 AWS 區域附加元件和服務水準協議 (SLA)。

您授予許可給 AMS 角色

您需要授予對 AMS 程序和雲端架構師的存取權。您可以透過為每個角色建立 AWS CloudFormation 堆疊來執行此操作。請參閱 建立 AMS 角色的範本 ，然後參閱 aws_managedservices_onboarding_role 使用 建立 AWS CloudFormation for Accelerate。如需詳細資訊，請參閱AMS Accelerate 中的存取管理。

AMS 會檢閱您的組態

您的雲端架構師 (CA) 也會在帳戶中尋找可能的組態問題，例如服務控制政策 (SCPs)，以及可能阻止 AMS 部署 AMS 所需工具和資源的安全性調查結果。您的 CA 會與您合作，協助您修復問題清單，並移除 AMS 工具和資源部署的任何封鎖程式。

AMS 會檢閱您的 AWS CloudTrail 線索組態

您的 Cloud Architect (CA) 將檢閱 CloudTrail 追蹤組態，並確認您是否希望 AMS 部署全域 CloudTrail 追蹤，或將 Accelerate 與您的 CloudTrail 帳戶或 Organization 追蹤資源整合。如果您選擇讓

Accelerate 與您的 CloudTrail 追蹤整合，您的 CA 會引導您完成 CloudTrail 追蹤資源組態的必要更新。

AMS 部署管理資源

AMS 團隊會部署工具 AWS 和資源，以提供 AMS Accelerate 的不同服務。完成後，AMS 已建立 AWS Managed Services 帳戶，AMS 會通知您您的帳戶處於作用中狀態。

加入管理資源階段到此結束。您可以直接前往加入程序的下一個步驟：步驟 3。使用預設政策加入 AMS 功能。

> **Note**
>
> 現在您的帳戶處於作用中狀態，您可以選擇執行下列任何任務：
>
> - 使用支援中心主控台建立 AWS 基礎設施的事件和服務請求。請參閱 AMS Accelerate 中的事件報告、服務請求和帳單問題。
> - 查看 AMS 部署 AWS Config 規則帳戶中的一致性狀態Accelerate 中的組態合規。
> - 找出和分析 GuardDuty 和 Macie （選用） 調查結果。請參閱 使用 GuardDuty 監控。
> - 存取和稽核 CloudTrail 日誌
> - 追蹤 AMS Accelerate 帳戶中的變更。請參閱 追蹤 AMS Accelerate 帳戶中的變更。
> - 使用 Resource Tagger 建立標籤。請參閱 加速資源交錯。
> - 請求修補程式、備份和 AWS Config 報告。請參閱報告和選項。

檢閱並更新您的組態，讓 AMS Accelerate 使用您的 CloudTrail 追蹤

AMS Accelerate 倚賴 AWS CloudTrail 記錄來管理您帳戶中所有資源的稽核和合規。在加入期間，您可以選擇 Accelerate 在主要 AWS 區域中部署 CloudTrail 追蹤，還是使用現有 CloudTrail 帳戶或 Organization 追蹤所產生的事件。如果您的帳戶未設定線索，則 Accelerate 將在加入期間部署受管 CloudTrail 線索。

> **Important**
>
> 只有在您選擇將 AMS Accelerate 與您的 CloudTrail 帳戶或 Organization 追蹤整合時，才需要 CloudTrail 日誌管理組態。

使用 Cloud Architect (CA) 檢閱 CloudTrail 追蹤組態、Amazon S3 儲存貯體政策和 CloudTrail 事件交付目的地的 AWS KMS 金鑰政策

在 Accelerate 可以使用您的 CloudTrail 追蹤之前，您必須與 Cloud Architect (CA) 合作來檢閱和更新組態，以符合 Accelerate 要求。如果您選擇將 Accelerate 與您的 CloudTrail Organization 追蹤整合，則您的 CA 會與您一起更新 CloudTrail 事件交付目的地 Amazon S3 儲存貯體和 AWS KMS 金鑰政策，以從您的 Accelerate 帳戶啟用跨帳戶查詢。您的 Amazon S3 儲存貯體可以位於由 Accelerate 管理的帳戶或您管理的帳戶。在加入期間，加速會驗證是否可以對您的 CloudTrail Organization 追蹤事件交付目的地進行查詢，並在查詢失敗時暫停加入。您可以使用 CA 來更正這些組態，以便繼續加入。

檢閱和更新您的 CloudTrail 帳戶或組織追蹤組態

需要下列組態才能整合 Accelerate CloudTrail 日誌管理 CloudTrail 帳戶或組織追蹤資源：

- 您的 CloudTrail 追蹤已設定為記錄所有 的事件 AWS 區域。
- 您的 CloudTrail 追蹤已啟用全域服務事件。
- 您的 CloudTrail 帳戶或組織追蹤會記錄所有管理事件，包括讀取和寫入事件，並啟用 AWS KMS 和 Amazon RDS Data API 事件記錄。
- 您的 CloudTrail 追蹤已啟用日誌檔案完整性驗證。
- CloudTrail 追蹤的 Amazon S3 儲存貯體會提供事件，以使用 SSE-S3 或 SSE-KMS 加密來加密事件。
- CloudTrail 線索交付事件至 的 Amazon S3 儲存貯體已啟用伺服器存取記錄。
- CloudTrail 線索交付事件至 的 Amazon S3 儲存貯體具有生命週期組態，可保留您的 CloudTrail 線索資料至少 18 個月。
- CloudTrail 追蹤交付事件的 Amazon S3 儲存貯體已強制執行物件擁有權設定為儲存貯體擁有者。
- 您的 CloudTrail 線索交付事件的 Amazon S3 儲存貯體可透過 Accelerate 存取。

檢閱和更新 CloudTrail 事件交付目的地的 Amazon S3 儲存貯體政策

在加入期間，您會與 Cloud Architect (CA) 合作，將 Amazon S3 儲存貯體政策陳述式新增至 CloudTrail 事件交付目的地。若要讓使用者從 Accelerate 帳戶查詢 CloudTrail 事件交付目的地 Amazon S3 儲存貯體中的變更，您可以在 Accelerate 管理的組織的每個帳戶中部署統一命名的 IAM 角色，並將其新增至所有 Amazon S3 儲存貯體政策陳述式中的`aws:PrincipalArn`清單。透過此組態，您的使用者可以在 Accelerate using Athena 中查詢和分析帳戶的 CloudTrail Organization 追蹤事件。如需如何更新 Amazon S3 儲存貯體政策的詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的使用 Amazon S3 主控台新增儲存貯體政策。

Important

只有在 Accelerate 與將事件交付至集中式 Amazon S3儲存貯體的 CloudTrail 追蹤整合時，才需要更新您的 Amazon S3 儲存貯體政策。Accelerate 不支援與交付至集中式儲存貯體的 CloudTrail 追蹤整合，但組織下沒有帳戶 AWS 。

Note

更新 Amazon S3 儲存貯體政策之前，請以適用的值取代*##*欄位：

- *amzn-s3-demo-bucket*，其中包含來自您帳戶的追蹤事件的 Amazon S3 儲存貯體名稱。
- *your-organization-id*，其中包含您帳戶所屬 AWS 組織 ID。
- *your-optional-s3-log-delievery-prefix* 搭配 CloudTrail 追蹤的 Amazon S3 儲存貯體交付字首。例如，my-bucket-prefix您在建立 CloudTrail 追蹤時可能已設定的 。

  如果您尚未為線索設定 Amazon S3 儲存貯體交付字首，請從下列 Amazon S3 儲存貯體政策陳述式中移除「*your-Optional-s3-log-delievery-prefix*」和繼續斜線 (/)。

以下三個 Amazon S3 儲存貯體政策陳述式授予 Accelerate 存取權，以擷取 的組態並執行 AWS Athena 查詢，以從您的 Accelerate 帳戶分析事件交付目的地 Amazon S3 儲存貯體中的 CloudTrail 事件。 Amazon S3

```
{
    "Sid": "DONOTDELETE-AMS-ALLOWBUCKETCONFIGAUDIT",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": [
        "s3:GetBucketLogging",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetEncryptionConfiguration"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
    "Condition": {
        "StringEquals": {
            "aws:PrincipalOrgID": "your-organization-id"
```

```
        },
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/ams-access-*"
            ]
        }
    }
},
{
    "Sid": "DONOTDELETE-AMS-ALLOWLISTBUCKET",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": "s3:ListBucket",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": "athena.amazonaws.com"
        },
        "StringLike": {
            "s3:prefix": "your-optional-s3-log-delievery-prefix/AWSLogs/*"
        },
        "StringEquals": {
            "aws:PrincipalOrgID": "your-organization-id"
        },
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/ams-access-*"
            ]
        }
    }
},
{
    "Sid": "DONOTDELETE-AMS-ALLOWGETOBJECT",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/your-optional-s3-log-delievery-
prefix/AWSLogs/*",
    "Condition": {
        "ForAnyValue:StringEquals": {
```

```
            "aws:CalledVia": "athena.amazonaws.com"
        },
        "StringEquals": {
            "aws:PrincipalOrgID": "your-organization-id"
        },
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/ams-access-*"
            ]
        }
    }
}
```

檢閱和更新 CloudTrail 事件交付目的地的 AWS KMS 金鑰政策

在加入期間，您會與 Cloud Architect (CA) 合作，更新用於加密交付至 Amazon S3 儲存貯體之 CloudTrail 追蹤事件的 AWS KMS 金鑰政策。請務必將參考 AWS KMS 金鑰政策陳述式附加到現有的 AWS KMS 金鑰。這會將 Accelerate 設定為與您現有的 CloudTrail 追蹤事件交付目的地 Amazon S3 儲存貯體整合，並解密事件。若要讓使用者從 Accelerate 帳戶查詢 CloudTrail 事件交付目的地 Amazon S3 儲存貯體中的變更，您可以在 Accelerate 管理的每個組織中部署統一命名的 IAM 角色，並將其新增至「aws：PrincipalArn」清單。透過此組態，您的使用者可以查詢事件。

有不同的 AWS KMS 金鑰政策更新案例需要考慮。您可能只會將 AWS KMS 金鑰設定為 CloudTrail 追蹤以加密所有事件，而且沒有 AWS KMS 金鑰可加密 Amazon S3 儲存貯體中的物件。或者，您可能有一個 AWS KMS 金鑰會加密 CloudTrail 交付的事件，另一個 AWS KMS 金鑰則會加密存放在 Amazon S3 儲存貯體中的所有物件。當您有兩個 AWS KMS 金鑰時，請更新每個金鑰的 AWS KMS 金鑰政策，以授予加速存取您的 CloudTrail 事件。更新政策之前，請務必將參考 AWS KMS 金鑰政策陳述式修改為現有的 AWS KMS 金鑰政策。如需如何更新 AWS KMS 金鑰政策的詳細資訊，請參閱AWS Key Management Service 《 使用者指南》中的變更金鑰政策。

Important

只有在 Accelerate 與啟用日誌檔案 SSE-KMS 加密的 CloudTrail 追蹤整合時，才需要更新 AWS KMS 金鑰政策。

Note

將此 AWS KMS 金鑰政策陳述式套用至用來加密交付至 Amazon S3 儲存貯體 AWS CloudTrail 之事件的 AWS KMS 金鑰之前，請將下列##欄位取代為適用的值：

- *YOUR-ORGANIZATION-ID* 包含您帳戶所屬 AWS 組織 ID。

此 AWS KMS 金鑰政策陳述式授予 Accelerate 存取權，以解密和查詢從組織中每個帳戶交付至 Amazon S3 儲存貯體的線索事件，並僅限 Athena 存取，供 Accelerate 用於查詢和分析 CloudTrail 事件。

```
{
    "Sid": "DONOTDELETE-AMS-ALLOWTRAILOBJECTDECRYPTION",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": [
        "kms:Decrypt",
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": "athena.amazonaws.com"
        },
        "StringEquals": {
            "aws:PrincipalOrgID": "YOUR-ORGANIZATION-ID"
        },
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/ams-access-*"
            ]
        }
    }
}
```

建立 AMS 角色的範本

下列 AMS 角色會將許可授予您的 AMS 雲端架構師 (CA)。下列 zip 檔案包含 Terraform 程式碼和 AWS CloudFormation 範本，可簡化建立 IAM 角色、許可政策和信任政策的程序。如需詳細資訊，請洽詢您的 CA。

角色名稱	必要者	範例範本
`aws_managedservices_onboarding_role`	AMS personnel during onboarding only	onboarding_role_minimal.zip

> **Note**
>
> 在您選取並下載範例範本（每個角色一個）之後，您將在 中將這些範本上傳為 AWS CloudFormation 堆疊的定義`aws_managedservices_onboarding_role` 使用 建立 AWS CloudFormation for Accelerate。

`aws_managedservices_onboarding_role` 使用 建立 AWS CloudFormation for Accelerate

您可以從 使用 建立 AWS Identity and Access Management 角色 `aws_managedservices_onboarding_role` AWS CloudFormation AWS Management Console。或者，您可以使用來自 的命令 AWS CloudShell 來部署角色。

使用 AWS Management Console

> **Note**
>
> 開始之前，請準備好每個角色的 JSON 或 YAML 檔案以上傳。如需詳細資訊，請參閱建立 AMS 角色的範本。

若要從 建立角色 AWS Management Console，請完成下列步驟：

1. 登入 AWS Management Console ，並在 https：//https://console.aws.amazon.com/cloudformation 開啟 AWS CloudFormation 主控台。

2. 選擇使用新資源建立堆疊 >（標準）。您會看到以下頁面。

3. 選擇上傳範本檔案，上傳 IAM 角色的 JSON 或 YAML 檔案，然後選擇下一步。您會看到以下頁面。

4. 在堆疊名稱欄位中輸入堆疊名稱 "**ams-onboarding-role**"。使用格式 "YYYY-MM-DDT00：00：00Z" 輸入 DateOfExpiry（建議使用目前日期的 30 天）。繼續向下捲動並選擇下一步，直到您到達此頁面：

5. 確定已選取核取方塊，然後選取建立堆疊。
6. 確定堆疊已成功建立。

使用來自 的命令 AWS CloudShell

若要部署 aws_managedservices_onboarding_role IAM 角色，請在 中執行下列命令AWS CloudShell：

AWS CLI

```
curl -s "https://docs.aws.amazon.com/en_us/managedservices/latest/accelerate-guide/
samples/onboarding_role_minimal.zip" -o "onboarding_role_minimal.zip"
unzip -q -o onboarding_role_minimal.zip
aws cloudformation create-stack \
    --stack-name "aws-managedservices-onboarding-role" \
    --capabilities CAPABILITY_NAMED_IAM \
    --template-body file://onboarding_role_minimal.json \
    --parameters ParameterKey=DateOfExpiry,ParameterValue="`date -d '+30 days' -u '+
%Y-%m-%dT%H:%M:%SZ'`"
```

AWS Tools for PowerShell

```
Invoke-WebRequest -Uri 'https://docs.aws.amazon.com/en_us/managedservices/
latest/accelerate-guide/samples/onboarding_role_minimal.zip' -OutFile
 'onboarding_role_minimal.zip'
Expand-Archive -Path 'onboarding_role_minimal.zip' -DestinationPath . -Force
New-CFNStack `
    -StackName 'aws-managedservices-onboarding-role' `
    -Capability CAPABILITY_NAMED_IAM `
    -TemplateBody (Get-Content 'onboarding_role_minimal.json' -Raw) `
```

```
    -Parameter @{ParameterKey = "DateOfExpiry"; ParameterValue = (Get-
Date).AddDays(30).ToString('yyyy-MM-ddTHH:mm:ssZ')}
```

建立角色之後，請與您的 Cloud Architect (CA) 合作以完成步驟 2. 在 Accelerate 中加入管理資源程序。AMS 通知您帳戶處於作用中狀態後，您就可以加入執行個體。

步驟 3。使用預設政策加入 AMS 功能

在此階段中，您使用預設政策加入 AMS 功能。這些包括新增 Amazon EC2 執行個體，以及根據您的偏好設定設定監控、備份、修補和修補程式 AWS Config（如果適用，AMS Patch Orchestrator 是您必須特別請求的附加元件）。您可以自行執行此操作，或請求 AMS 根據您的輸入加入功能。若要向 AMS 請求協助，請建立服務請求並提供所有必要的輸入以完成任務。請記住，服務請求不會立即解決。

> **Note**
>
> 雖然帳戶可能會使用預設政策進行備份、修補或監控，但需要標記資源，讓適當的政策生效。

主題

- （選用）加速中的 Quick Start 範本
- 加入 加速監控
- 加入 EC2 執行個體以加速
- 在 Accelerate AWS Backup 中加入
- 在 Accelerate 中加入修補
- 在 Accelerate 中檢閱不合規報告

（選用）加速中的 Quick Start 範本

Quick Start 範本會在已啟用 Accelerate AWS 的帳戶中自動化 AMS Resource Tagger 的部署和組態。相較於手動設定，此範本可節省時間和精力。依原狀使用此範本來定義一個帳戶中的監控、修補和備份基本概念。或者，將其用作 StackSet，以在 Organizations Units 之間套用設定，以標準化多個帳戶的設定。

您也可以使用它做為起點來建置自己的自訂 AMS Resource Tagger 描述檔，並使用文件中的程式碼片段來建立更複雜的標籤定義。

Quick Start 範本功能

Quick Start 範本會完成下列任務：

- 建立和部署 AMS Resource Tagger 的組態版本。
- 將標籤套用至啟用 AMS 管理和建立監控資源的 Amazon EC2 執行個體。
- （選用）將標籤套用至受管 EC2 執行個體，使其能夠按照所需的排程進行修補，並建立修補維護時段以利修補。

> **Warning**
>
> 根據預設，執行個體會重新啟動，並自動啟動停止的執行個體以進行修補程式安裝。

- （選用）將標籤套用至受管 EC2 執行個體，使其可依預設 AMS Backup Plan 中所定義進行備份。
- （選用）將標籤套用至受管 Amazon Relational Database Service (Amazon RDS) 資源，這些資源可根據增強型備份計畫進行備份。備份計畫也會啟用 Amazon RDS 的時間點復原 (PITR)。如果未啟用 Amazon RDS 自動備份，則資料庫會在接近下一個備份時段的時間重新啟動。

Quick Start 範本覆寫和排除

使用此範本建立 Quick Start 堆疊後，請使用下列步驟從管理/監控、修補或備份中排除特定執行個體：

- 管理和監控：若要排除由 AMS 管理和監控的 EC2 執行個體，請將此標籤新增至執行個體：`ExcludeFromAMSQuickStartMonitoring=true`。
- 修補：屬於 Auto Scaling 群組、Amazon Elastic Container Service 或 Amazon Elastic Kubernetes Service 叢集成員的 EC2 執行個體，會由此 Quick Start 範本排除在修補之外。

  若要停用建立修補視窗和 EC2 執行個體的修補相關標記，請將 CloudFormation 堆疊參數設定為 `EnablePatching=false`。

  若要在 時將 EC2 執行個體排除為 Quick Start 修補視窗的目標`EnablePatching=true`，請將此標籤新增至執行個體：`ExcludeFromAMSQuickStartPatching=true`。
- 備份：屬於 Auto Scaling 群組、ECS 或 EKS 叢集成員的 EC2 執行個體會由此 Quick Start 範本從 Backup 中排除。

  若要排除 EC2 執行個體成為預設 AMS Backup Plan 的目標，當 時`EnableBackup=true`，請將此標籤新增至該執行個體：`ExcludeFromAMSQuickStartBackup=true`。

> **Tip**
>
> 您可以大量標記 EC2 執行個體。使用標籤編輯器，在 中的一個步驟中大量選取和標記資源 AWS Management Console。

Quick Start 範本參數

此 Quick Start 範本會設定 Resource Tagger 將標籤新增至帳戶`ams:rt:ams-managed=true`中的所有 EC2 執行個體，但您新增`ExcludeFromAMSQuickStartMonitoring=true`標籤的執行個體除外。使用下列參數，根據您的需求控制此堆疊的選用部分：

CFN 參數	Value	Effect
EnableBackup	'true'（預設）	根據預設 AMS Backup Plan，所有 AMS 受管 EC2 執行個體 (`ams:rt:ams-managed=true`) 都會在每日4AM 點 UTC 加上標籤`ams:rt:backup-orchestrator=true` 以供備份。 https://docs.aws.amazon.com/managedservices/latest/accelerate-guide/acc-backup-select-plan.html#acc-backup-plan-default 對於所有 RDS 執行個體和叢集，範本會根據增強型備份計劃，套用具有最長保留期 (31 天） 的`ams:rt:backup-orchestrator-enhanced=true` 「連續備份」。 https://docs.aws.amazon.com/aws-backup/latest/devguide/point-in-time-recovery.html#point-in-time-recovery-rds https://docs.aws.amazon.com/managedservices/latest/accelerate-guide/acc-backup-select-plan.html#acc-backup-plan-enhanced

CFN 參數	Value	Effect
		如果這變更了 PITR 保留期間，在某些情況下可能會重新啟動資料庫，例如，如果有其他待定的組態更新。
	'false'	此快速啟動範本不會以任何執行個體為目標進行備份。
EnablePatching	'false'（預設）	此 Quick Start 範本不會針對任何執行個體進行修補。
	'true'	所有 AMS 受管執行個體 (`ams:rt:ams-managed=true`) 都會標記 ，`ams:rt:Patch Group=AMSQuickStartPatchWindow` 並建立基本 SSM 維護時段資源，以便根據 中定義的排程進行修補`CronExpression` 。 若要將`ams:rt:Patch Group` 標籤套用至 EC2 執行個體，您必須關閉該執行個體執行個體中繼資料中標籤的存取權。
CronExpression	-	的預設值會根據 `Timezone` 參數，將每月第 2 個星期六`cron(0 30 19 ? * SAT#2 *)`設為下午 7：30。使用 cron 語法。
時區	-	根據 修補目標執行個體`CronExpression` 。使用 IANA 格式。

下載 Quick Start 範本

下載 AMSQuickStart.zip 檔案。

或者，在 中執行下列命令AWS CloudShell來部署 `AMSQuickStart.yaml`：

AWS Command Line Interface

```
curl -s "https://docs.aws.amazon.com/en_us/managedservices/latest/accelerate-guide/
samples/AMSQuickStart.zip" -o "AMSQuickStart.zip"
unzip -q -o AMSQuickStart.zip
for region in region1 region2 ;
do
aws cloudformation create-stack \
    --region $region \
    --stack-name "AMSQuickStart" \
    --template-body file://AMSQuickStart.yaml \
    --parameters \
        ParameterKey=EnableBackup,ParameterValue="true" \
        ParameterKey=EnablePatching,ParameterValue="false" \
        ParameterKey=Timezone,ParameterValue="US/Eastern" \
        ParameterKey=CronExpression,ParameterValue="cron(0 30 19 ? * SAT#2 *)" \
;
done
```

AWS Tools for PowerShell

```
Invoke-WebRequest -Uri 'https://docs.aws.amazon.com/en_us/managedservices/latest/
accelerate-guide/samples/AMSQuickStart.zip' -OutFile 'AMSQuickStart.zip'
Expand-Archive -Path 'AMSQuickStart.zip' -DestinationPath . -Force
@('region1', 'region2') | `
ForEach-Object { `
New-CFNStack `
    -Region $_ `
    -StackName 'AMSQuickStart' `
    -TemplateBody (Get-Content 'AMSQuickStart.yaml' -Raw) `
    -Parameter @(
        @{ParameterKey = "EnableBackup"; ParameterValue = "true"},
        @{ParameterKey = "EnablePatching"; ParameterValue = "false"},
        @{ParameterKey = "Timezone"; ParameterValue = "US/Eastern"},
        @{ParameterKey = "CronExpression"; ParameterValue = "cron(0 30 19 ? * SAT#2
 *)"}
    )
}
```

如需每個參數的說明，請參閱上一節：Quick Start 範本參數。

加入 加速監控

Amazon EC2 執行個體以外的所有新資源預設都會啟用監控。您可以標記執行個體，開始監控 Amazon EC2 執行個體。

若要加入監控，請先確定您的組態會監控您希望 AMS 監控的資源，並忽略您希望它忽略的資源。

您可以使用下列 CloudWatch 儀表板來探索 AMS 監控和標記鎖定多少資源，以及有多少資源未鎖定。在帳戶中，導覽至 CloudWatch 儀表板主控台，然後選取下列其中一項：

- AMS-Alarm-Manager-Reporting-Dashboard
- AMS-Resource-Tagger-Reporting-Dashboard

如需儀表板指標的完整說明，請參閱：

- 檢視 Alarm Manager for Accelerate 監控的資源數量
- 檢視 Resource Tagger 管理的資源數量

在 Accelerate 中監控的加入資源

若要覆寫預設行為，例如，若要停用non-EC2 資源的預設監控，您需要使用自訂組態設定檔取消標記這些資源。如需有關標記以進行監控的詳細資訊，請參閱 在 Accelerate 中監控。

在您加入執行個體之前，會停用 EC2 執行個體的監控，其中包括使用自訂組態設定檔標記執行個體。下一節說明 EC2 執行個體加入。

在 Accelerate 中建立監控組態描述檔

- 如需使用預設組態的詳細資訊，請參閱 加速警示管理員。
- 如需使用自訂組態的詳細資訊，請參閱 修改加速警示預設組態。

加入 EC2 執行個體以加速

EC2 執行個體會透過稱為自動化執行個體組態的程序加入 AMS Accelerate，以確保每個執行個體撰寫正確的日誌並發出正確的 AMS 指標，以正確管理執行個體。除非您特別希望 AMS 忽略部分，否則您應該加入所有 EC2 執行個體。自動化執行個體組態需要符合讓 AMS 設定執行個體的特定條件 （ 如需詳細資訊，請參閱 Accelerate 中自動化執行個體組態的先決條件)。最重要的條件是，您需要在您希望 AMS 為您管理的每個 Amazon EC2 執行個體上安裝 AWS Systems Manager 代理程式 (SSM 代理程式）。如需 SSM 代理程式的詳細資訊，請參閱使用 SSM 代理程式。

SSM 預先安裝在適用於 Accelerate 的標準 AMIs中

下列作業系統的 SSM 代理程式已安裝在 AWS提供的 AMIs 上。

- Amazon Linux 和 Amazon Linux 2
- SUSE Linux Enterprise Server (SLES) 12 和 15
- Microsoft Windows Server 2019、2016、2012 R2、2012
- Ubuntu Linux 18.04 和 20.04

如果您使用的是其中一個 AWS提供的 AMIs，請參閱 在 Accelerate 中標記執行個體。

在 Accelerate 中手動安裝 SSM

對於下列作業系統，或使用自訂 AMI 時，您可以手動安裝 SSM 代理程式。或者，您可以使用 AMS SSM Agent 自動安裝功能。若要進一步了解 SSM 自動安裝，請參閱 SSM Agent 自動安裝。如需手動安裝的指示，請選取您作業系統的連結：

- CentOS SSM 安裝
- Oracle SSM 安裝
- Red Hat SSM 安裝
- SUSE Linux Enterprise Server SSM 安裝
- Windows SSM 安裝

在 Accelerate 中標記執行個體

安裝 SSM 代理程式之後，您必須標記執行個體。請參閱 AMS Accelerate 中的標記。

Accelerate 中的自動化執行個體組態

標記執行個體後，AMS 會執行自動化執行個體組態，其中包括：

- 記錄作業系統日誌和指標
- 啟用 AMS 工程師的遠端存取
- 在執行個體上執行遠端命令

這些任務對於 AMS 監控、修補和日誌服務以及 AMS 回應事件至關重要。如需設定自動執行個體組態的詳細資訊，請參閱 AMS Accelerate 中的自動化執行個體組態。

自動化執行個體組態完成後，您就可以：

- 使用支援中心主控台建立 Amazon EC2 執行個體和作業系統的事件和服務請求。如需詳細資訊，請參閱AMS Accelerate 中的事件報告、服務請求和帳單問題。
- 存取和稽核 Amazon EC2 日誌
- 取得修補程式報告

在 Accelerate AWS Backup 中加入

若要設定備份，您需要建立稱為備份計劃的備份政策。備份計畫會指定要備份 AWS 的資源、需要備份的頻率，以及備份保留期間。我們建議您評估組織的持續性、安全性和合規要求，以判斷您需要的備份計劃。

選擇加入

- 請依照下列步驟，確保 AWS Backup 已針對每個帳戶、區域和資源類型啟用 ：

  入門 1：服務選擇加入。

  或者，入門 2：建立隨需備份。

選擇備份計畫

- 若要選擇備份計劃，請參閱 選取 AMS 備份計畫。

新增資源

根據預設，資源不會與備份計劃相關聯。它們需要新增至備份計劃。

- 若要將資源新增至備份計劃，請參閱 標記您的 資源以套用 AMS 備份計劃。
- 若要使用標籤在所有資源上啟用備份，請參閱 在 Accelerate 中管理備份的標籤。

在 Accelerate 中加入修補

您需要設定修補，以確保您的軟體是up-to-date，並符合您的合規政策。

AWS Backup 先決條件：若要允許在修補維護時段期間建立根磁碟區快照，請遵循以下步驟，確保 AWS Backup 針對 Amazon EBS 資源類型的每個帳戶和區域啟用 ：入門 1：服務選擇加入。（您不需要繼續進行入門 2：建立隨需備份。）

修補時機：修補會在維護時段期間發生。您可以排程維護時段，以便僅在預設時間套用修補程式。

要修補的內容：您必須將要修補的 Amazon EC2 執行個體與維護時段建立關聯。若要將執行個體與維護時段建立關聯，Amazon EC2 執行個體必須加上標籤，且維護時段應以這些標籤做為目標。

要安裝的修補程式：使用修補程式基準，您可以設定規則來自動核准特定類型的修補程式，例如作業系統或高嚴重性修補程式。您也可以指定規則的例外狀況，例如一律已核准或拒絕的修補程式清單。

如需 Amazon EC2 修補程式政策的指引，修補建議請參閱 。

- 若要開始設定修補程式管理，請參閱 了解 AMS Accelerate 中的修補程式管理
- 若要建立自訂修補程式組態，請參閱 使用 AMS Accelerate 自訂修補程式基準。

在 Accelerate 中檢閱不合規報告

AMS 部署的 AWS Config 規則可協助您根據美國國家標準與技術研究所 (NIST) 雲端安全架構 (CSF) 網際網路安全中心 (CIS) 設定的標準識別違規。我們建議您與交付團隊一起檢閱不合規報告，以排定修補動作的優先順序，讓您的帳戶以合規狀態為基準。

步驟 4. 在 Accelerate 中自訂功能

在此階段，您已使用預設政策加入監控、修補和備份。現在，您有機會自訂符合您需求的政策。

您可以選擇使用預設政策進行修補、備份或監控，或根據您的需求選擇自訂政策。AMS 使用標籤將資源與操作政策建立關聯。AMS 提供 Resource Tagger，可讓您根據應用程式分組或其他分組邏輯，指定如何將標籤套用至 AWS 資源的規則。如需詳細資訊，請參閱 加速資源交錯。

客戶提供的標籤功能可讓您新增和刪除 AMS 資源的自訂標籤。如需詳細資訊，請參閱Accelerate 中客戶提供的標籤。

主題

- 在 Accelerate 中自訂監控
- 在 Accelerate 中自訂備份
- 在 Accelerate 中自訂修補

在 Accelerate 中自訂監控

若要根據您的應用程式需求自訂雲端資源的監控：

1. 建立自訂監控政策。請參閱 修改加速警示預設組態。
2. 使用標籤將自訂政策套用至資源。請參閱在 Accelerate 中監控
3. 將提醒路由至資源擁有者。請參閱 標籤型提醒通知。

您可以使用下列 CloudWatch 儀表板來探索 AMS 監控和標記鎖定多少資源，以及有多少資源未鎖定。在您的帳戶中，導覽至 CloudWatch 儀表板主控台，然後選取下列其中一項：

- AMS-Alarm-Manager-Reporting-Dashboard
- AMS-Resource-Tagger-Reporting-Dashboard

如需儀表板指標的完整說明，請參閱：

- 檢視 Alarm Manager for Accelerate 監控的資源數量
- 檢視 Resource Tagger 管理的資源數量

在 Accelerate 中自訂備份

您無法自訂 AMS 預設備份計劃。相反地，根據您的應用程式需求建立新的備份計劃，然後使用標籤將資源連接到您的自訂計劃。您可以選擇 AMS 應備份的資源、頻率和保留期。我們建議您評估組織的持續性、安全性和合規要求，以判斷您需要的備份計劃。

- 若要建立備份計劃，請參閱建立備份計劃。
- 若要將資源指派給備份計畫，請參閱將資源指派給備份計畫。

在 Accelerate 中自訂修補

修補可確保您的軟體是up-to-date，並符合您的合規政策。

修補時機：修補會在維護時段期間發生。您可以排程維護時段，以便僅在預設時間套用修補程式。

要修補的內容：您必須將要修補的 Amazon EC2 執行個體與維護時段建立關聯。若要將執行個體與維護時段建立關聯，Amazon EC2 執行個體必須加上標籤，且維護時段應以這些標籤做為目標。

要安裝的修補程式：使用修補程式基準，您可以設定規則來自動核准特定類型的修補程式，例如作業系統或高嚴重性修補程式。您也可以指定規則的例外狀況，例如一律已核准或拒絕的修補程式清單。

- 如需一般修補建議，請參閱 修補建議。

- 若要建立自訂維護時段，請參閱 在 AMS 中建立修補程式維護時段。
- 若要建立自訂修補程式基準，請參閱 使用 AMS Accelerate 自訂修補程式基準。
- 若要將修補程式提醒路由到資源擁有者，請參閱 了解 AMS Accelerate 中的修補程式通知和修補程式失敗。

使用 AMS 主控台

AWS 管理主控台中的 AMS 主控台可讓您與 AMS 互動，並操作您的 AMS 進階受管和 AMS Accelerate 資源。AMS 主控台的行為通常類似於任何 AWS 主控台；不過，由於 AMS 是私有組織，因此只有為 AMS 啟用的帳戶才能存取主控台。在您的帳戶中啟用 AMS 後，您可以在統一搜尋列中搜尋「受管服務」來存取主控台。

> **Note**
>
> 視您的帳戶角色而定，您可以存取 AMS Advanced 主控台或 AMS Accelerate 主控台。

使用 AMS 主控台時，請注意下列注意事項：

- AMS 主控台是帳戶特定的。因此，如果您在組織的「測試」帳戶中，您將無法查看該組織的「產品」帳戶中的資源。同樣地，您必須擁有 AMS Advanced 角色才能存取 AMS Advanced 主控台。
- AMS 主控台會在您驗證時套用 IAM 政策，以決定您可以存取的主控台，以及您可以在其中執行的動作。您的管理員可能會將其他政策套用至預設 AMS 政策，以限制您可以在 主控台中看到和執行的操作。

AMS Accelerate 主控台具有下列功能：

- 開啟頁面：開啟頁面包含資訊方塊和連結，可協助您存取事件、服務請求和報告。
- 左側導覽窗格中的功能頁面、連結：
  - 儀表板：提供 帳戶目前狀態的概觀，包括：
    - 資源上的事件：在 AWS Support Center 中開啟事件案例的按鈕，以及有多少事件案例正在等待核准並需要您注意，以及有多少事件案例正在開啟
    - 合規狀態：連結至不合規或合規的規則和資源
    - 服務請求：在 AWS Support Center 中開啟服務請求案例的按鈕，以及有多少正在等待核准並需要您注意的按鈕，以及有多少是 Open

    - 帳戶層級安全性：連結至即時威脅偵測 GuardDuty 調查結果和資料安全和隱私權 Macie 調查結果的詳細資訊
    - 快速動作：開啟備份保存庫或修補程式執行個體組態頁面
  - 報告：開啟報告頁面和預設報告、每日備份和每日修補程式，以及每月計費
  - 組態：確保您的資源已成功根據您的規格進行管理。
    - 安裝 SSM 代理程式：需要 SSM 代理程式
    - 設定標記規則：開啟 AMS Resource Tagger
    - 設定警示：開啟 AMS CloudWatch 警示組態
    - 設定修補程式排程：開啟 AWS Systems Manager 主控台
    - 設定修補程式基準：開啟 AWS Patch Manager 主控台
    - 設定備份計劃：開啟 AWS Backup 主控台
- 功能焦點：主控台最新更新的相關資訊
- 文件：AWS Managed Services 文件登陸頁面

AMS 模式

AWS Managed Services (AMS) 模式是一種一般解決方案，可解決 AMS 受管環境中一系列的使用案例。

當您在 AMS 平台上操作時，AMS 雲端架構師 (CAs) 會與您合作，以符合您的業務和營運需求。雖然 AMS 客戶以獨特的方式運作，但我們注意到客戶有類似的使用案例。在這種情況下，CAs會建立一般解決方案範本或「模式」，用於多個客戶環境，且組態和部署工作最少。

AMS 模式的建置旨在協助將功能交付給 AMS 客戶，通常是由請求它的客戶帳戶 CA 所建置。

AMS 模式的運作方式

若要請求每個模式的更多詳細資訊，包括所需的雲端格式範本，以便您可以部署模式，請使用主旨「請求模式####」的其他詳細資訊 （替代您想要的模式） 提交 AMS 服務請求，並將您的 AMS 雲端架構師 (CA) 新增至其他聯絡人選項。

AMS 模式分為兩 (2) 個類別：

- 一般用途：由於多個 AMS 客戶已部署和使用模式，因此模式被視為穩定
- 預覽模式：AMS 建議您在非生產環境中部署預覽模式模式模式以進行驗證，並與您的 Cloud Architect 在部署之前討論使用案例。

> **Important**
>
> AMS 模式不遵守您的預設 AMS 服務水準協議服務水準協議 (SLAs) 和服務水準目標 (SLOs)。模式的支援和更新會盡最大努力完成。
> 此 AWS 內容是根據AWS 客戶協議的條款或客戶與 Amazon Web Services， Inc. 或 Amazon Web Services EMEA SARL (「AWS 歐洲」) 或兩者之間的其他書面協議所提供。
> 本軟體中包含的材料是以「原樣」方式提供給您，不提供任何類型的明示、暗示或其他保證，包括但不限於適用於特定用途的任何保證。

AMS 模式

AMS 模式。

AMS 模式

名稱	概觀	優勢	類別
自訂 CloudWatch 警示通知	自訂 CloudWatch 警示通知，以包含來自執行個體標籤的資訊，例如執行個體名稱、應用程式 ID 等。	將內容資訊新增至警示通知將使它們更有意義，並提供可行的資訊。	監控
磁碟用量報告	磁碟用量報告模式會收集多個應用程式帳戶的磁碟區使用空間，並在具有 Athena 資料表查詢功能的 Amazon S3 中呈現結果做為集中式報告。	提供帳戶磁碟區實際用量的洞見，以判斷節省成本的機會。	成本最佳化
Prowler 堆疊	使用 Amazon EC2 對無法使用 CloudShell 的帳戶執行 Prowler 檢查。	在因許可或逾時問題而無法使用 CloudShell 的情況下，協助解除封鎖 Accelerate 加入 (Prowler)，而不會	安全性

名稱	概觀	優勢	類別
		影響其目前的安全狀態。	
使用自訂物件金鑰的 AMS Amazon S3 複寫	複製 Amazon S3 物件，並保留所有中繼資料和物件金鑰（資料夾）。 分割部分來源物件金鑰，或在複寫期間建立自訂目的地物件金鑰。	在 Amazon S3 複寫期間自訂物件金鑰（資料夾），而不需要額外的指令碼，即可將物件移至所需的資料夾。	可靠性
Amazon EBS 快照刪除	以 Lambda 和 CloudWatch Events 為基礎的自動化 AWS Backup，可根據保留率自動刪除在 外部拍攝的 Amazon EBS 快照。	協助清除 AWS Backup 在協調器外拍攝的個別快照，隨著時間節省額外的成本。	成本最佳化
AMS Amazon RDS 秘密輪換	使用 CloudFormation 範本，自動部署輪換支援 Amazon RDS 資料庫、Redshift 和 DocumentDB 秘密所需的所有必要資源 (Lambda 函數、安全群組、彈性網路介面或 ENIs)。	自動化資料庫秘密輪換，並在輪換失敗時提供通知機制。	安全性
自動化金鑰輪換	根據 CloudWatch Events 和 Lambda，自動輪換 IAM 使用者的存取和私密金鑰。	更輕鬆地輪換 IAM 使用者的存取和私密金鑰。	安全性

名稱	概觀	優勢	類別
Amazon EBS 磁碟區快照交錯器	使用 Amazon EC2 執行個體中的標籤來標記所有 Amazon EBS 磁碟區和快照。	使用有意義的相關商業資訊協助分類和追蹤成本，讓您更輕鬆地驗證支出的位置，並啟用標記磁碟區和快照的自動化。 AWS 成本最佳化支柱強烈建議的最佳實務。	標記（成本最佳化、安全性、事件管理和自動化）

AMS Accelerate 中的自動化執行個體組態

AMS Accelerate 提供自動化執行個體組態服務。此服務可確保執行個體為 AMS 發出正確的日誌和指標，以正確管理執行個體。自動化執行個體組態有自己的入門先決條件和步驟，如本節稍後所述。

主題

加速中的自動化執行個體組態運作方式

自動化執行個體組態可讓 AMS Accelerate 根據您透過新增特定代理程式和標籤所指示的執行個體，每天執行特定組態。

Accelerate 中自動化執行個體組態的先決條件

必須滿足這些條件，才能讓 AMS Accelerate 在受管執行個體上執行先前描述的自動化動作。

SSM 代理程式已安裝

AMS Accelerate 自動化執行個體組態需要安裝 AWS Systems Manager SSM Agent。

如需使用 AMS SSM Agent 自動安裝功能的詳細資訊，請參閱 SSM Agent 自動安裝。

如需手動安裝 SSM Agent 的資訊，請參閱下列內容：

- Linux：在適用於 Linux 的 Amazon EC2 執行個體上手動安裝 SSM 代理程式 - AWS Systems Manager
- Windows：在適用於 Windows Server 的 Amazon EC2 執行個體上手動安裝 SSM 代理程式 - AWS Systems Manager

SSM 代理程式處於受管狀態

AMS Accelerate 自動化執行個體組態需要操作 SSM 代理程式。必須安裝 SSM Agent，Amazon EC2 執行個體必須處於受管狀態。如需詳細資訊，請參閱 AWS 文件：使用 SSM Agent。

自動化執行個體組態設定

假設符合先決條件，新增特定的 Amazon EC2 執行個體標籤會自動啟動 AMS Accelerate 自動化執行個體組態。使用下列其中一種方法來新增此標籤：

1. （強烈建議）使用 AMS Accelerate Resource Tagger

   若要設定帳戶的標記邏輯，請參閱 標記的運作方式。標記完成後，會自動處理標籤和自動執行個體組態。

2. 手動新增標籤

   手動將下列標籤新增至 Amazon EC2 執行個體：

   Key：ams：rt：ams-managed、Value：true。

> **Note**
>
> 一旦 ams：rt：ams 受管標籤套用至執行個體，執行個體組態服務會嘗試套用所需的 AMS 組態。每當執行個體啟動，以及 AMS 每日組態檢查發生時，服務都會宣告 AMS 所需的組態。

SSM Agent 自動安裝

若要讓 AMS 管理您的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，您必須在每個執行個體上安裝 AWS Systems Manager SSM Agent。如果您的執行個體未安裝 SSM Agent，您可以使用 AMS SSM Agent 自動安裝功能。

> **Note**
>
> - 如果您的帳戶在 6/03/2024 之後加入 AMS Accelerate，則預設會啟用此功能。若要關閉此功能，請聯絡您的 CA 或 CSDM。
> - 若要在 6/03/2024 之前加入的帳戶中開啟此功能，請聯絡您的 CA 或 CSDM。
> - 此功能僅適用於不在 Auto Scaling 群組中且執行 AMS 支援的 Linux 作業系統的 EC2 執行個體。

SSM Agent 使用的先決條件

- 確定與目標執行個體相關聯的執行個體描述檔具有下列其中一個政策（或與其允許清單相同的許可）：
  - AmazonSSMManagedEC2InstanceDefaultPolicy
  - AmazonSSMManagedInstanceCore
- 請確定 AWS Organizations 層級沒有明確拒絕前述政策中所列許可的服務控制政策。

  如需詳細資訊，請參閱設定 Systems Manager 所需的執行個體許可。
- 若要封鎖傳出流量，請確定已在目標執行個體所在的 VPC 上啟用下列界面端點（適當地取代 URL 中的「區域」）：
  - ssm.<region>.amazonaws.com
  - ssmmessages.<region>.amazonaws.com
  - ec2messages.<region>.amazonaws.com

  如需詳細資訊，請參閱使用適用於 Systems Manager 的 VPC 端點來改善 EC2 執行個體的安全性。

如需啟用或停用受管節點可用性疑難排解的一般秘訣，請參閱解決方案 2：確認已為執行個體指定 IAM 執行個體描述檔（僅限 EC2 執行個體）。

> **Note**
>
> AMS 會在自動安裝程序中停止和啟動每個執行個體。當執行個體停止時，存放在執行個體儲存體磁碟區中的資料和存放在 RAM 上的資料都會遺失。如需詳細資訊，請參閱停止執行個體時會發生的情況。

請求在您的執行個體上自動安裝 SSM Agent

如果您的帳戶已加入 AMS Accelerate Patch Add-On，請為執行個體設定修補程式維護時段 (MW)。需要有效的 SSM 代理程式才能完成修補程序。如果執行個體上缺少 SSM 代理程式，則 AMS 會嘗試在修補程式維護時段期間自動安裝它。

> **Note**
>
> AMS 會在自動安裝程序中停止和啟動每個執行個體。當執行個體停止時，存放在執行個體儲存體磁碟區中的資料和存放在 RAM 上的資料都會遺失。如需詳細資訊，請參閱停止執行個體時會發生的情況。

SSM Agent 自動安裝的運作方式

AMS 使用 EC2 使用者資料在您的執行個體上執行安裝指令碼。若要新增使用者資料指令碼並在執行個體上執行，AMS 必須停止並啟動每個執行個體。

如果您的執行個體已有現有的使用者資料指令碼，則 AMS 會在自動安裝程序期間完成下列步驟：

1. 建立現有使用者資料指令碼的備份。
2. 以 SSM Agent 安裝指令碼取代現有的使用者資料指令碼。
3. 重新啟動執行個體以安裝 SSM Agent。
4. 停止執行個體並還原原始指令碼。
5. 使用原始指令碼重新啟動執行個體。

自動化執行個體組態變更

AMS Accelerate 執行個體組態自動化會在您的帳戶中進行下列變更：

1. IAM 許可

   新增必要的 IAM 受管政策，以授予執行個體使用 AMS Accelerate 安裝代理程式的許可。

2. 代理

   a. Amazon CloudWatch Agent 負責發出作業系統日誌和指標。執行個體組態自動化可確保 CloudWatch 代理程式已安裝並執行 AMS Accelerate 最低版本。

b. AWS Systems Manager SSM Agent 負責在執行個體上執行遠端命令。執行個體組態自動化可確保 SSM Agent 正在執行 AMS Accelerate 最低版本。

3. CloudWatch 組態

a. 為了確保發出所需的指標和日誌，AMS Accelerate 會自訂 CloudWatch 組態。如需詳細資訊，請參閱下一節：CloudWatch 組態變更詳細資訊。

自動化執行個體組態會對 IAM 執行個體設定檔和 CloudWatch 組態進行變更或新增。

IAM 許可變更詳細資訊

每個受管執行個體都必須具有 AWS Identity and Access Management 角色，其中包含下列受管政策：

- arn：aws：iam：：aws：policy/AmazonSSMManagedInstanceCore
- arn：aws：iam：：aws：policy/CloudWatchAgentServerPolicy
- arn：aws：iam：：aws：policy/AMSInstanceProfileBasePolicy

前兩個是 AWS受管政策。AMS 受管政策為：

AMSInstanceProfileBasePolicy

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "secretsmanager:CreateSecret",
                "secretsmanager:UpdateSecret"
            ],
            "Resource": [
                "arn:aws:secretsmanager:*:*:secret:/ams/byoa/*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "kms:Encrypt"
            ],
```

```
            "Resource": [
                "*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

如果您的執行個體已連接 IAM 角色，但缺少任何這些政策，則 AMS 會將缺少的政策新增至您的 IAM 角色。如果您的執行個體沒有 IAM 角色，則 AMS 會連接 AMSOSConfigurationCustomerInstanceProfile IAM 角色。AMSOSConfigurationCustomerInstanceProfile IAM 角色具有 AMS Accelerate 所需的所有政策。

> **Note**
>
> 如果達到預設執行個體描述檔限制 10，則 AMS 會將限制增加到 20，以便連接所需的執行個體描述檔。

CloudWatch 組態變更詳細資訊

CloudWatch 組態的其他詳細資訊。

- 執行個體上的 CloudWatch 組態檔案位置：
  - Windows：%ProgramData%\Amazon\AmazonCloudWatchAgent\amazon-cloudwatch-agent.json
  - Linux：/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/ams-accelerate-config.json
- Amazon S3 中的 CloudWatch 組態檔案位置：
  - Windows：https：//ams-configuration-artifacts-*REGION_NAME*.s3.*REGION_NAME*.amazonaws.com/configurations/cloudwatch/latest/windows-cloudwatch-config.json
  - Linux：https：//ams-configuration-artifacts-*REGION_NAME*.s3.*REGION_NAME*.amazonaws.com/configurations/cloudwatch/latest/linux-cloudwatch-config.json
- 收集的指標：
  - Windows：
    - AWS Systems Manager SSM 代理程式 (CPU_Usage)

    - CloudWatch 代理程式 (CPU_Usage)
    - 所有磁碟的磁碟空間使用率 (% 可用空間)
    - 記憶體 (% 使用中的遞交位元組)
  - Linux：
    - AWS Systems Manager SSM 代理程式 (CPU_Usage)
    - CloudWatch 代理程式 (CPU_Usage)
    - CPU (cpu_usage_idle、cpu_usage_iowait、cpu_usage_user、cpu_usage_system)
    - Disk (used_percent、inodes_used、inodes_total)
    - Diskio (io_time、 write_bytes、 read_bytes、 writes、 reads)
    - Mem (mem_used_percent)
    - 交換 (swap_used_percent)
- 收集的日誌：
  - Windows：
    - AmazonSSMAgentLog
    - AmazonCloudWatchAgentLog
    - AmazonSSMErrorLog
    - AmazonCloudFormationLog
    - ApplicationEventLog
    - EC2ConfigServiceEventLog
    - MicrosoftWindowsAppLockerEXEAndDLLEventLog
    - MicrosoftWindowsAppLockerMSIAndScriptEventLog
    - MicrosoftWindowsGroupPolicyOperationalEventLog
    - SecurityEventLog
    - SystemEventLog
  - Linux：
    - /var/log/amazon/ssm/amazon-ssm-agent.log
    - /var/log/amazon/ssm/errors.log
    - /var/log/audit/audit.log
    - /var/log/cloud-init-output.log

    - /var/log/cloud-init.log

- /var/log/cron
- /var/log/dpkg.log
- /var/log/maillog
- /var/log/messages
- /var/log/secure
- /var/log/spooler
- /var/log/syslog
- /var/log/yum.log
- /var/log/zypper.log

從 AMS Accelerate 離線

AMS Accelerate 提供操作企業級操作環境的簡單方法。此外，AMS Accelerate 為 AWS 遷移和用量提供了支援的基礎設施操作模型。不過，使用 AMS Accelerate 之後，您可以決定在來源內或將 AWS 基礎設施操作責任重新指派給其他團隊。若要這樣做，您必須將帳戶從 AMS 服務中移出。

當您從 AMS Accelerate 離職帳戶時，AMS 會將服務描述中定義的所有責任轉返給您。例如，您將無法切斷對 AMS 的事件或服務請求。同樣地，我們的營運工程師和自動化將無法再存取您的 Accelerate 帳戶，導致我們無法修復運作狀態、可用性，以及安全與合規問題清單。您的 AWS 工作負載可以繼續在 AMS 操作的相同帳戶中執行。

未來將執行基礎設施操作服務的團隊必須包含在內，以定義您在加速離職後將使用的人員、工具和程序。AMS 會保留一些 AMS 工具，例如護欄和日誌，以允許開發「成為」操作環境和模型。請仔細檢閱下列文件，以了解您可以繼續使用的工具，以及如何請求退出帳戶。

AMS 加速離職效果

準備從 Accelerate 離職時，請記住下列考量事項。

- 存取：不會刪除定義`ams-access-management` AWS Identity and Access Management 角色的`ams-access-management` AWS CloudFormation 堆疊。離職後，這些資源仍會保留，但會由剩餘的其他元件使用。您可以方便地刪除堆疊和角色。
- AMS 資源保留：離職後，某些 AMS 資源會保留在您的 帳戶中。若要查看保留哪些資源以及您可以使用哪些資源，請參閱resource_inventory.zip試算表 （壓縮）。
- 自動化：在離職後，不再提供 AMS 策劃的 AWS SSM 自動化 Runbook 和 AWS Lambda 函數。

- 備份管理：AMS 使用備份管理來擷取 資源的快照。離職後，您可以繼續使用 上定義的備份排程、頻率和保留期，但 AMS 備份計畫 AWS Backup 除外；請參閱 選取 AMS 備份計畫。AMS Backup Orchestrator 建立 AWS Identity and Access Management 的資源會移除，但不會移除 AMS 撰寫的備份保存庫和對應的 AWS KMS 金鑰。加速不再監控備份任務或在事件期間執行還原動作。
- 成本最佳化：離職後，會刪除 AMS Resource Scheduler。AMS Resource Scheduler 會停止未使用的資源，並在需要其容量時重新啟動這些資源，以協助您降低營運成本。AMS 不會繼續提供成本最佳化建議。如需資源排程器的詳細資訊，請參閱使用 AMS 資源排程器進行成本最佳化。
- 指定專家：離職後，您指定的 Cloud Service Delivery Manager (CSDM) 和 Cloud Architect (CA) 不再為您的離職 Accelerate 帳戶提供指導、報告或推動卓越營運和安全性。
- 事件管理：事件管理是 AMS 服務用來回應您回報事件的程序。離職後，加速不再偵測和回應事件，或協助您的團隊解決問題。您將無法與 Accelerate 和 Accelerate 主控台交換事件和服務請求通訊，並停用 Accelerate 帳戶的存取。
- 記錄和報告：離職後，您會保留因 CloudWatch、CloudTrail 和 VPC 流程日誌而儲存的日誌。您可以依原狀保留這些服務的組態，以繼續產生日誌；不過，AMS 不會再監控這類組態。Accelerate 不再提供摘要 AMS 關鍵效能指標的每月服務報告。您可以保留從自助服務報告 (SSR) 產生的資料（請參閱 自助式報告），但 Accelerate 不會產生新的資料。
- 監控：監控是 AMS 服務用來追蹤 資源的程序。在離職期間，AMS 會移除 AMS 特定的工具，例如 Alarm Manager 和 Resource Tagger，以及 AMS 部署做為 AMS 監控基準一部分的任何 EventBridge 事件規則和 CloudWatch 警示。在離職後，加速將不再回應警示或設定新的警示。如需警示管理員和資源交錯的詳細資訊，請參閱標籤型警示管理員和資源交錯。
- 操作工具：AMS Accelerate 可以在 AWS 中提供工作負載基礎設施的持續操作。退出 Accelerate 帳戶後，您便無法再存取 Resource Tagger 等工具，以協助您根據規則標記資源，或自動執行個體組態在 EC2 執行個體中安裝所需的代理程式。執行個體上的 CloudWatch 和 SSM 代理程式會保留在現有的組態中。IAM `AMSOSConfigurationCustomerInstanceRole` 設定檔和 `AMSInstanceProfileBasePolicy`會與您的執行個體分離，並從您的 Accelerate 帳戶移除。
- 修補程式管理：修補程式管理是 AMS 服務用來更新 EC2 執行個體的程序。離職後，AMS 不會再在修補之前建立執行個體的快照、不再安裝和監控修補安裝，也不會再通知您結果。您可以保留過去建立的修補程式基準和快照。此外，修補程式維護時段的組態仍會保留，但 Accelerate 不會再安裝修補程式。
- 問題管理：離職後，加速不再執行分析以識別和調查問題，並識別根本原因。
- 安全性：安全管理是 AMS 服務用來保護 資源的程序。離職後，您可以保留 Amazon GuardDuty 偵測器和調查結果，以及您建立的任何 AWS Config 規則。由 Accelerate 部署的 AWS Config 規則都會移除。加速不再監控、修復或報告這些工具的問題清單。

- 服務終止日期：服務終止日期是 30 天必要終止通知期間結束後日曆月的最後一天。如果必要的終止通知期間結束在日曆月的第 20 天之後，則服務終止日期是下一個日曆月的最後一天。以下是終止日期的範例案例。
  - 如果終止通知是在 4 月 12 日提供，則 30 天的通知會在 5 月 12 日結束。服務終止日期為 5 月 31 日。
  - 如果在 4 月 29 日提供終止通知，則 30 天的通知將於 5 月 29 日結束。服務終止日期為 6 月 30 日。

從 AMS 離職 使用 Alarm Manager 和 Resource Tagger 的相依性加速

當您從 AWS Managed Services 離職時，部署與 Alarm Manager 或 Resource Tagger 相關組態的自訂 AWS CloudFormation 堆疊，以及 AMS 提供的 Alarm Manager 和 Resource Tagger 組態堆疊，會保留在您的帳戶中。

若要在卸任程序期間刪除 AMS 組態堆疊，您必須在啟動卸任程序之前，從自訂 CloudFormation 範本中移除 Alarm Manager 或 Resource Tagger 的任何相依性和參考。當您從 AMS 離職時，移除參考有助於確保堆疊已從您的帳戶正確移除。

> **Important**
>
> 在開始離職程序之前，請仔細檢閱您的 CloudFormation 範本，並移除任何 Alarm Manager 和 Resource Tagger 的參考。否則可能會導致您的帳戶保留這些堆疊，即使您從 AMS 離職也一樣。請注意，雖然這些堆疊包含 Alarm Manager 和 Resource Tagger 特有的組態資訊，但其存在不會產生持續的費用或費用。

取得 Accelerate 帳戶的離職協助

在透過 AMS 帳戶服務終止請求收到至少 30 天的通知後，AMS 會終止您的帳戶。服務終止日期是 30 天必要終止通知期間結束後當月的最後一天；前提是，如果必要終止通知期間結束日落在當月的第 20 天之後，服務終止日期將是下一個日曆月的最後一天。

若要請求讓帳戶離職，您必須：

1. 提交正式請求，以使用服務請求讓帳戶離職。一個服務請求 (SR)，記錄您想要離職的所有帳戶，或每個帳戶一個 SR。

   在請求中，提供要離職的帳戶 IDs 清單、離職原因，以及任何其他考量事項。

2. 通知 CSDM 您想要離職的帳戶，並請求他們協助執行離職程序。

Accelerate 中的通知設定

您與 AMS 之間的通訊有許多原因：

- 透過監控提醒建立的事件
- 如果您已選擇加入修補程式附加元件，則修補服務通知
- 服務請求和事件報告
- 偶爾重要 AWS 公告 （ 如果需要您採取任何動作，您的 CSDM 會與您聯絡 ）

所有通知都會使用您在加入時為修補程式通知提供的電子郵件傳送。否則，通知會傳送至您在加入時提供給 AMS 的預設電子郵件。由於難以保持個別電子郵件的更新，我們建議您使用可在結束時更新的群組電子郵件。AMS 操作也會收到傳送給您的所有通知，並在做出回應之前進行分析。

您可以使用以非資源為基礎的通知的聯絡人具名清單，例如以 GuardDuty 或 AWS Config 為基礎的提醒。例如，您可能有一個名為 的清單`SecurityContacts`和另一個名為 的清單`OperationsContacts`。AMS 會將警示和通知傳送至這些清單。

如需詳細資訊，請參閱AWS Config 控制合規報告。

AMS Accelerate 中的標記

大多數 Accelerate 功能（修補、備份、監控）使用標籤和組態描述檔來決定要管理哪些資源、要套用的動作，以及何時套用它們。標籤是您套用至資源的標籤。組態設定檔包含以這些標籤為基礎的規則。

每個加速功能都有自己的標記需求。有些功能要求您使用特定標籤，有些則允許您使用任何自己的標籤。

如需必要標籤的資訊，請參閱 Accelerate 中的客戶受管標籤。

如需可定義客戶之標籤的相關資訊，請參閱 Accelerate 中客戶提供的標籤

內容

AMS Accelerate 中的標籤

內容

什麼是標籤？

標籤是您指派給 AWS 資源的標籤。每個標籤皆包含由您定義的一個索引鍵與一個選用值。

您可以使用標籤以不同的方式分類 AWS 資源，例如，依用途、擁有者或環境。例如，您可以為帳戶的 Amazon EC2 執行個體定義一組標籤，協助您追蹤每個執行個體的擁有者和堆疊層級。

標籤對 Amazon EC2 來說不具有任何語意意義，並會嚴格解譯為字元字串。

若要進一步了解，請參閱標記 AWS 資源。

標記的運作方式

有多種方式可將標籤套用至您的 資源。您可以在建立資源時，直接在每個 AWS 服務的主控台中標記資源；使用 AWS 標籤編輯器來新增、移除或編輯多個資源的標籤；或使用佈建工具， AWS CloudFormation 例如資源標籤。AMS Accelerate 也提供 AMS Accelerate Resource Tagger，您可用來定義自動標籤生命週期管理器的規則。如需在 AMS Accelerate 中使用 Resource Tagger 的詳細資訊，請參閱 加速資源交錯。AMS Accelerate 也提供客戶提供的標籤，以新增和移除 AMS 資源的自訂標籤。如需客戶提供標籤的詳細資訊，請參閱 Accelerate 中客戶提供的標籤。

Accelerate 中的客戶受管標籤

需要特定標籤才能觸發各種 AMS Accelerate 動作。

內容

- 在 Accelerate 中監控
- 在 Accelerate 中設定 EC2 執行個體的標籤
- 在 Accelerate 中管理備份的標籤

在 Accelerate 中監控

AMS Accelerate 會監控支援的資源的運作狀態、可用性和可靠性。如需此服務產品的詳細資訊，請參閱 AMS Accelerate 中的監控和事件管理。

AMS Accelerate 會定期加入 AWS 服務 基準監控的其他 。如果您使用 Resource Tagger 預設組態，這些更新會自動部署到您的帳戶，而變更會反映到支援的資源。

若要選擇讓 AMS Accelerate 管理您的 Amazon EC2 執行個體，您必須透過 AppConfig 中的自訂設定檔套用下列標籤；如需詳細資訊，請參閱步驟 3：建立組態和組態設定檔。

將下列標籤套用至您的 資源：

金鑰	值
ams:rt:ams-managed	true

例如，您可以像這樣建立自訂組態文件，將標籤套用至所有 AMS 支援的 EC2 資源：

```
{
    "AWS::EC2::Instance": {
        "AllEC2": {
            "Enabled": true,
            "Filter": {
                "Platform": "*"
            },
            "Tags": [
                {
                    "Key": "ams:rt:ams-managed",
                    "Value": "true"
                }
            ]
        }
    }
}
```

> **Important**
>
> 請記得在進行組態變更之後部署組態變更。在 SSM AppConfig 中，您必須在建立組態後部署新版本。

Amazon EC2 以外的服務將具有預設基準監控。若要選擇不讓 AMS Accelerate 監控您的資源，您可以使用自訂組態描述檔來排除特定資源或 AWS 服務。這可讓您控制哪些資源應具有監控標籤，以部署基準警示定義。請參閱 AMS Accelerate 中的資源交錯使用案例。

使用資源交錯器

如果您套用此標籤 (ams：rt：ams-managed)，帳戶中的 AMS Accelerate Resource Tagger 組態有助於確保自動部署下列標籤。

您會看到下列標籤套用到支援的 資源以進行基準監控。

金鑰	值	規則
ams:rt:ams-monitoring-policy	ams-monitored	適用於 AMS 支援的所有 EC2 資源

金鑰	值	規則
ams：rt：ams-monitoring-policy-platform	ams-monitored-linux	適用於所有執行 Linux 作業系統的 Amazon EC2 執行個體
ams：rt：ams-monitoring-policy-platform	ams-monitored-windows	適用於所有執行 Windows OS 的 Amazon EC2 執行個體

對於其他支援的 服務

根據指定的規則，將下列標籤套用至您的 資源：

金鑰	值	規則
ams:rt:ams-monitoring-policy	ams-monitored	適用於 AMS Accelerate 監控支援的所有資源。
ams：rt：ams-monitoring-with-kms	ams-monitored-with-kms	使用 KMS 的 OpenSearch 網域
ams：rt：ams-monitoring-with-master	ams-monitored-with-master	具有專用主節點的 OpenSearch 網域

如果您不是使用 Resource Tagger

無需 Resource Tagger 即可加速標籤 如需使用 AMS Resource Tagger 以外的方法套用正確監控標籤的說明，請參閱 。

在 Accelerate 中設定 EC2 執行個體的標籤

AMS Accelerate 會管理 Amazon EC2 執行個體上的代理程式，例如 SSM 代理程式和 CloudWatch 代理程式。如需此服務產品的詳細資訊，請參閱 AMS Accelerate 中的自動化執行個體組態

若要選擇讓 AMS Accelerate 管理 Amazon EC2 執行個體，您必須將下列標籤套用至 Amazon EC2 執行個體：

金鑰	值
ams:rt:ams-managed	true

在 Accelerate 中管理備份的標籤

AMS Accelerate 會管理支援資源的備份。如需此服務產品的詳細資訊，請參閱 AMS Accelerate 中的持續性管理。

AMS Accelerate 備份管理使用標籤來識別應該自動備份哪些資源 （並提供手動備份功能）。您可以使用任何標籤索引鍵：值組合，將資源與備份計劃建立關聯。若要使用 ams-default-backup-plan AWS Backup 計劃選擇加入自動備份，您必須將下列標籤套用至支援的資源：

金鑰	值
ams:rt:backup-orchestrator	true

> **Note**
>
> 在加入期間，AMS Accelerate 會使用 ams：rt：backup-orchestrator-onboarding 標記所有資源，並在短間隔、短保留快照中值為 true。這是由 ams-onboarding-backup-plan 備份計劃管理。如需 AMS Accelerate 受管 AWS Backup 計劃的詳細資訊，請參閱 選取 AMS 備份計畫。

加速受管標籤

在加入 AMS Accelerate 期間，您的帳戶會部署數個 AWS 資源。因此，您可以識別這些資源，這些資源會加上下列標籤：

金鑰	值
ams：resourceOwner	AMS
ams：resourceOwnerService	描述哪些 AMS Accelerate 服務提供此資源，例如 AMS 部署、備份、控制、監控、修補程式等。

金鑰	值
AppId	AMSInfrastructure
AppName	
環境	

> **Note**
>
> 這些標籤使用 AWS CloudFormation 堆疊層級標籤套用，並依賴將標籤 AWS CloudFormation 傳播到建立的資源。如需詳細資訊，請參閱資源標籤。

Accelerate 中客戶提供的標籤

什麼是客戶提供的標籤？

客戶提供的標籤是 AMS Accelerate 服務功能，用於指定管理帳戶中如何標記 AMS 資源的規則。使用客戶提供的標籤，您可以將使用者定義的自訂標籤新增至部署到帳戶的 AMS 資源。當您使用自動化服務請求 Cloud Service Delivery Manager (CSDM) 時，客戶提供的標籤功能會自動新增至請求的帳戶。請注意，您無法覆寫 AMS 標籤。AMS 標籤開頭為 'ams：'。

您可以定義自己的標籤（標籤），並為所有 AMS Accelerate 資源指定這些標籤的功能。您可以在加入 AMS 之前提供這些標籤，以便在啟動程序期間套用 AMS 標籤和自訂標籤。或者，您可以在加入後提供標籤。

如何新增客戶提供的標籤？

若要請求將這些標籤新增至您的 資源，請聯絡您的 CSDM。這些標籤會套用至您帳戶中的 AMS 資源。

標籤的範圍為何？

此功能目前僅適用於 Accelerate 客戶和 AWS 商業區域。您可以將標籤新增至您擁有的所有帳戶或特定帳戶清單。

> **Note**
>
> 這些標籤僅適用於 AMS 資源，不會影響您自己的資源。

適用於 Accelerate 的標籤管理工具

內容

加速資源交錯

使用 Resource Tagger，您可以指定規則來管理資源在帳戶中的 AWS 標記方式。加入帳戶時，AMS Accelerate 會部署您的標記政策，以確保受管帳戶中的資源已加上標記。

內容

- 設定 Terraform 以忽略 Resource Tagger 標籤
- 檢視 Resource Tagger 管理的資源數量

什麼是 Resource Tagger？

Resource Tagger 是一項 AMS Accelerate 服務，可讓您指定規則來管理帳戶中 AWS 資源的標記方式。它旨在為您提供標籤如何 AWS 套用至資源的完整可見性。

Resource Tagger 會根據您在組態設定檔中指定的標記規則，自動在支援 AWS 的資源上建立、更新和刪除標籤。例如，您可以指定將標籤套用至 Amazon EC2 執行個體集合的規則，指出它們應該由 AMS Accelerate 管理，這會導致執行個體受到監控或備份。您可以使用像這樣的標籤，根據 AWS AppConfig 組態設定檔中定義的政策來識別資源的 AWS 合規狀態。如需詳細資訊，請參閱AWS AppConfig。

AMS Accelerate 提供預設的受管標記組態，讓您可以讓 AMS Accelerate 監控資源。您可以定義哪些資源應該由 AMS Accelerate 管理，而受管標記規則可確保具有適當標籤的資源受到 AMS Accelerate 的監控。

使用 Resource Tagger，如果您選擇覆寫或停用預設 AMS Accelerate 受管標籤，提供您自己的標記規則以符合您的政策，並使用其他機制，例如 Terraform，以避免偏離。您可以根據您的操作定義要擴展的例外狀況。例如，您可以定義政策，為具有支援平台 （ 例如 Windows 和 Linux) 的所有 Amazon EC2 執行個體套用標籤，並排除標記特定執行個體 IDs。

> **Important**
>
> Resource Tagger 會控制您帳戶中具有 ams：rt： 字首的所有標籤。任何以此字首開頭的標籤都會刪除，除非它們出現在 Resource Tagger 的組態規則中。總而言之，以 ams：rt： 開頭的支援資源上的任何標籤都視為由 Resource Tagger 擁有。如果您手動標記某些項目，例如 ams：rt： ，如果該標籤未在其中一個 Resource Tagger 組態設定檔中指定，則會自動移除該標籤。

Resource Tagger 的運作方式

當您的帳戶加入 AMS Accelerate 時，系統會將兩份 JSON 組態文件部署至您的帳戶 AWS AppConfig。兩個稱為組態設定檔的文件稱為 AMSManagedTags，稱為預設組態設定檔，而 CustomerManagedTags 稱為自訂組態設定檔。您可以使用自訂組態描述檔為您的帳戶定義自己的政策和規則，而 AMS Accelerate 不會覆寫這些政策和規則。

這兩個設定檔都位於 AMSResourceTagger 應用程式和 AMSInfrastructure 環境中。資源標記程式套用的所有標籤都有金鑰字首 ams：rt：。

自訂組態設定檔：

在帳戶加入時，自訂組態描述檔一開始是空的；不過，除了預設組態描述檔中的規則之外，還會強制執行設定檔文件中放置的任何規則。自訂組態設定檔中的任何組態都完全由您管理，AMS Accelerate 不會覆寫，除非您的請求。

您可以在支援的 AWS 資源的自訂組態設定檔中指定您想要的任何自訂標記規則，也可以在此處指定對 AMS Accelerate 受管預設組態的修改，請參閱 AMS Accelerate 中的資源交錯使用案例。

> **Important**
>
> 如果您更新此設定檔，Resource Tagger 會自動強制執行您 中所有相關資源的變更 AWS 帳戶。變更會自動制定，但最多可能需要 60 分鐘才會生效。

您可以使用 AWS Management Console或透過 CLI/SDK AWS 工具更新此設定檔。如需有關更新自訂組態設定檔的資訊，請參閱 AWS AppConfig 使用者指南：什麼是 AWS AppConfig？

預設組態設定檔：

預設組態設定檔文件位於 AMS Accelerate 內部，其中包含您無法永久修改或刪除的 AMS Accelerate 提供的預設規則。AMS Accelerate 可以隨時更新此設定檔，並供您檢閱；您對它所做的任何變更都會自動刪除。如果您想要修改或停用使用自訂組態設定檔的任何預設組態規則，請參閱 AMS Accelerate 中的資源交錯使用案例。

AMS Accelerate 中的資源交錯器組態設定檔

組態描述檔有助於確保在整個資源生命週期內將標籤統一套用至資源。

語法和結構

組態設定檔是具有下列結構的 JSON 物件：

```
{
   "Options": {
      "ReadOnly": false
   },
```

```
   "ResourceType": {
      "ConfigurationID": {
      "Enabled": true,
      "Filter": { ... },
      "Tags": [  ...  ]
      },
      "ConfigurationID": {
      ...
      }
   },
   "ResourceType": {
     ...
   }
}
```

選項：（選用）指定您希望 ResourceTagger 的行為方式的選項。省略 區塊等同於將所有選項設定為其預設值。如需可用的選項設定，請參閱以下內容：

- ReadOnly：（選用，預設為 false)：指定 Resource Tagger 的 ReadOnly 模式。將 ReadOnly 設為 true，以停用 Resource Tagger 在 AWS 資源上建立或移除標籤。如需詳細資訊，請參閱防止 Resource Tagger 修改資源。

ResourceType：此金鑰必須是下列支援的字串之一，並代表與指出的資源類型相關的所有組態：

- AWS::AutoScaling::AutoScalingGroup
- AWS::DynamoDB::Table
- AWS::EC2::Instance
- AWS::EC2::NatGateway
- AWS::EC2::VPNConnection
- AWS::EFS::FileSystem
- AWS::EKS::Cluster
- AWS::ElasticLoadBalancing::LoadBalancer
- AWS::ElasticLoadBalancingV2::LoadBalancer
- AWS::Elasticsearch::Domain
- AWS::FSx::FileSystem
- AWS::OpenSearch::Domain

- AWS::RDS::DBCluster
- AWS::RDS::DBInstance
- AWS::Redshift::Cluster
- AWS::S3::Bucket
- AWS::Synthetics::Canary

ConfigurationID：此金鑰在設定檔文件中必須是唯一的，並唯一命名下列組態區塊。如果相同 ResourceType 區塊中的兩個組態區塊具有相同的 ConfigurationID，則設定檔中最後出現的組態區塊會生效。如果您在自訂描述檔中指定的 ConfigurationID 與預設文件中指定的 ConfigurationID 相同，則自訂描述檔中定義的組態區塊會生效。

> **Important**
>
> ConfigurationID **##**與 AMS Accelerate 設定檔重疊；例如，它不應是 AMSMonitoringLinux 或 AMSMonitoringWindows，否則會停用 AMSManagedTags 組態設定檔的個別組態。

已啟用 （選用，預設為 true)：指定組態區塊是否生效。將此設定為 false 以停用組態區塊。停用的組態區塊沒有效果。

篩選條件：指定組態套用的資源。每個篩選條件物件可以有下列任一 （但只能有一個） 欄位：

- AWS::AutoScaling::AutoScalingGroup：
  - AutoScalingGroupName：Autoscaling 群組名稱。此欄位支援萬用字元比對。
- AWS::DynamoDB::Table：
  - TableName：DynamoDB 資料表的名稱。此欄位支援萬用字元比對。
- AWS::EC2::Instance：
  - AvailabilityZone：篩選條件符合指定可用區域中的 EC2 執行個體。此欄位支援萬用字元比對，因此 *a 符合 us-east-1a、ap-northeast-1a 等。
  - InstanceId：篩選條件會比對具有指定執行個體 ID 的 EC2 執行個體。此欄位支援萬用字元比對，因此 i-00000* 會比對執行個體 ID 開頭為 i-00000 的任何執行個體。
  - 平台：篩選條件會比對具有指定平台的 EC2 執行個體。有效值為 windows、linux 或萬用字元 * （以比對任何平台）。
- AWS::EC2::NatGateway：
  - NatGatewayId：NAT 閘道的 ID。此欄位支援萬用字元比對。

  - 狀態：NAT 閘道的狀態（待定 | 失敗 | 可用 | 刪除 | 已刪除或萬用字元 "*")
  - VpcId：NAT Gateway 所在的 VPC ID。此欄位支援萬用字元比對。
  - SubnetId：NAT Gateway 所在的子網路 ID。此欄位支援萬用字元比對
- AWS::EC2::VPNConnection：
  - VpnConnectionId：連線的 ID。此欄位支援萬用字元比對。
- AWS::EFS::FileSystem：
  - FileSystemId：EFS 檔案系統的 ID。此欄位支援萬用字元比對。
- AWS::EKS::Cluster：
  - ClusterName：叢集的名稱。此欄位支援萬用字元比對。
- AWS::ElasticLoadBalancing::LoadBalancer (Classic Load Balancer)：
  - LoadBalancerName：LoadBalancer 名稱。此欄位支援萬用字元比對。
  - 結構描述：可以是「面向網際網路」、「內部」或萬用字元「*」。
  - VPCId：部署負載平衡器的 VPCId 可以是萬用字元 "*"。
- AWS::ElasticLoadBalancingV2::LoadBalancer (Application Load Balancer(ALB))：
  - LoadBalancerArn：LoadBalancer Amazon Resource Name (ARN)。
  - DNSName：LoadBalancer 的 DNSName。此欄位支援萬用字元比對。
  - LoadBalancerName：LoadBalancer 名稱。此欄位支援萬用字元比對。
- AWS::Elasticsearch::Domain：
  - DomainId：ElasticSearch 資源的 DomainId。此欄位支援萬用字元比對。
  - DomainName：ElasticSearch 資源的 DomainName。此欄位支援萬用字元比對。
  - HasMasterNode：布林值為 true 或 false。如果網域具有專用主節點，則相符。
  - HasKmsKey 布林值為 true 或 false。如果網域具有用於靜態加密的 KMS 金鑰，則相符。
- AWS::FSx::FileSystem：
  - FileSystemId：FSx 檔案系統的 ID。此欄位支援萬用字元比對。
- AWS::OpenSearch::Domain：
  - DomainId：OpenSearch 資源的 DomainId。此欄位支援萬用字元比對。
  - DomainName：OpenSearch 資源的 DomainName。此欄位支援萬用字元比對。
  - HasMasterNode：布林值；如果網域具有專用主節點，這可以設定為 true。
  - HasKmsKey：如果網域具有用於靜態加密的 KMS 金鑰，則可以將此設定為 true。
- AWS::RDS::DBCluster：

  - DBClusterIdentifier：篩選條件會比對 RDS 叢集識別符與指定的識別符。此欄位不支援萬用字元比對，因此必須指定叢集識別符。
  - 引擎：RDS 執行個體使用的引擎。此欄位支援萬用字元比對。
  - EngineVersion：引擎版本。此欄位支援萬用字元比對。
- AWS::RDS::DBInstance：
  - DBInstanceIdentifier：篩選條件會比對具有指定執行個體 ID 的 RDS 執行個體。此欄位不支援萬用字元比對，因此必須指定執行個體識別符。
  - 引擎：RDS 執行個體使用的引擎。此欄位支援萬用字元比對。
  - EngineVersion：引擎版本。此欄位支援萬用字元比對。
- AWS::Redshift::Cluster：
  - ClusterIdentifier：叢集識別符。此欄位支援萬用字元比對。
- AWS::S3::Bucket：
  - BucketName：S3 儲存貯體的名稱。此欄位支援萬用字元比對。
- AWS::Synthetics::Canary：
  - CanaryName：Synthetics Canary 的名稱。

其他篩選條件屬性：

- 標籤：篩選條件會套用至已套用指定標籤的任何資源。此屬性的值必須是具有下列欄位的 JSON 物件：
  - 金鑰：必須是確切的字串，並指定資源必須具有具有該確切金鑰的標籤。
  - 值：指定標籤的相符值。支援萬用字元，因此 Sample 的值符合以 Sample 字串結尾的任何值。
- Fn：：AND：JSON 物件的 JSON 陣列。每個物件都遵循與篩選條件組態區塊相同的規則。這會指定篩選條件符合所有子篩選條件的任何資源。
- Fn：：OR：JSON 物件的 JSON 陣列。每個物件都遵循與篩選條件組態區塊相同的規則。這會指定篩選條件符合任何符合任何子篩選條件的資源。
- Fn：：NOT：遵循與篩選條件組態區塊相同規則的 JSON 物件。這會指定篩選條件明確不符合任何符合子篩選條件的資源。使用此選項來指定標記規則的排除。

標籤：要套用至相符資源的標籤。（請參閱標籤命名和使用慣例。）此欄位是鍵/值對的陣列：

- 金鑰：要套用之標籤的金鑰。
- 值：要套用的標籤值。

> **Note**
>
> Resource Tagger 套用的標籤一律具有開頭為 ams：rt： 的金鑰。如果您未在設定檔中指定此字首，Resource Tagger 會為您插入。這是 Resource Tagger 將其擁有和管理的標籤與其他工具用於其他用途的標籤區分開來的方式。

AMS Accelerate 中的資源交錯使用案例

本節列出具有 Resource Tagger 的常用動作。

檢視由 Resource Tagger 套用的標籤

Resource Tagger 套用的所有標籤都有金鑰字首 ams：rt：。例如，下列標籤定義會產生具有金鑰 ams：rt：sampleKey 和值 sampleValue 的標籤。具有此字首的所有標籤都會視為 Resource Tagger 的一部分。

```
{
 "Key": "sampleKey",
 "Value": "sampleValue"
}
```

> **Important**
>
> 如果您使用 ams：rt： 字首手動建立自己的標籤，則視為由 Resource Tagger 管理。這表示如果資源是由 Resource Tagger 管理，但組態描述檔未指出應套用標籤，則 Resource Tagger 會移除手動新增的標籤。如果您手動標記由 Resource Tagger 管理的資源，請勿使用 ams：rt： 字首做為標籤索引鍵。

使用 Resource Tagger 建立標籤

AMS Accelerate Resource Tagger 是在 AMS Accelerate 加入期間部署在您的帳戶中的元件。Resource Tagger 具有一組可設定的規則，可定義資源的標記方式，然後強制執行這些規則，自動新增和移除資源上的標籤，以確保它們符合您的規則。

如果您想要使用 Resource Tagger 來標記資源，請參閱 加速資源交錯。

以下是 Resource Tagger 組態程式碼片段範例，會將值為 true 的標籤 ams：rt：ams-managed 新增至所有 Amazon EC2 執行個體。ams：rt：ams 受管標籤會選擇讓 AMS Accelerate 監控您的資源。

```
{
    "AWS::EC2::Instance": {
        "SampleConfigurationBlock": {
            "Enabled": true,
            "Filter": {
                "Platform": "*"
            },
            "Tags": [
                {
                    "Key": "ams:rt:ams-managed",
                    "Value": "true"
                }
            ]
        }
    }
}
```

Warning

指定新組態的名稱時請小心 (SampleConfigurationBlock在提供的範例中），因為您可能會不小心以相同的名稱覆寫 AMS 受管組態。

防止 Resource Tagger 修改資源

Resource Tagger 可以設定為唯讀模式，以防止其新增或移除資源上的任何標籤。如果您想要提供自己的標記機制，這會很有用。

在唯讀模式中，Resource Tagger 仍會檢查受管和客戶組態設定檔中指定的標記規則，並掃描不符合這些標記規則的資源。任何不合規的資源都會以 呈現 AWS Config。您可以尋找 AWS Config 規則 的 具有 AMSResourceTagger-字首。例如，AMSResourceTagger-EC2Instance AWS Config 規則會根據組態描述檔，評估是否為AWS::EC2::Instance資源建立適當的標籤。

Resource Tagger 此時會停止，不會對您的資源進行任何變更 （不會新增或移除標籤）。

您可以修改客戶組態設定檔以在選項區塊中包含 ReadOnly 金鑰，以啟用唯讀模式。例如，下列組態設定檔程式碼片段會顯示這可能看起來如何：

```
{
    "Options": {
        "ReadOnly": true
```

```
    },
    "AWS::EC2::Instance": {
        [... the rest of your configuration ...]
    }
}
```

一旦完成部署，Resource Tagger 就會對此新組態做出反應，並停止新增和移除資源上的標籤。

> **Note**
>
> 若要重新啟用標籤修改，請將 ReadOnly 值變更為 false，或完全移除金鑰，因為預設值為 false。

如需選項設定的詳細資訊，請參閱語法和結構下一步。

範例組態描述檔

下列範例設定檔文件指定 AMS Accelerate 管理屬於堆疊* CloudFormation 堆疊的所有 Windows EC2 執行個體；不過， 會明確排除 ID 為 i-00000000000000001 的特定 EC2 執行個體。

```
{
    "AWS::EC2::Instance": {
        "AMSMonitoringWindows": {
            "Enabled": true,
            "Filter": {
                "Fn::AND": [
                    {
                        "Platform": "Windows"
                    },
                    {
                        "Tag": {
                            "Key": "aws:cloudformation:stack-name",
                            "Value": "stack-*"
                        }
                    },
                    {
                        "Fn::NOT": {
                            "InstanceId": "i-00000000000000001"
                        }
                    }
                ]
```

```
            },
            "Tags": [
                {
                    "Key": "ams:rt:ams-managed",
                    "Value": "true"
                }
            ]
        }
    }
}
```

> **Warning**
>
> 指定新組態的名稱時請小心 (SampleConfigurationBlock在提供的範例中），因為您可能會不小心以相同的名稱覆寫 AMS 受管組態。

合併預設組態

預設組態設定檔會在帳戶加入時由 AMS Accelerate 提供。此設定檔提供部署在帳戶中的預設規則。

雖然您無法修改預設組態設定檔，但您可以在自訂組態設定檔中使用與預設組態區塊相同的 ConfigurationID 來指定組態區塊，以提供預設值的覆寫。如果您這樣做，您的組態區塊會覆寫預設組態區塊。

例如，請考慮下列預設組態文件：

```
{
 "AWS::EC2::Instance": {
  "AMSManagedBlock1": {
   "Enabled": true,
   "Filter": {
    "Platform": "Windows"
   },
   "Tags": [{
    "Key": "my-tag",
    "Value": "SampleValueA"
   }]
  }
 }
}
```

若要將此處套用的標籤值從 變更為 SampleValueA SampleValueB，並將標籤套用至所有執行個體，而不只是 Windows 執行個體，您會提供下列自訂組態設定檔：

```
{
 "AWS::EC2::Instance": {
  "AMSManagedBlock1": {
   "Enabled": true,
   "Filter": {
    "Platform": "*"
   },
   "Tags": [{
    "Key": "my-tag",
    "Value": "SampleValueB"
   }]
  }
 }
}
```

> **Important**
>
> 請記得在進行組態變更之後部署組態變更。如需詳細資訊，請參閱部署組態變更。在 SSM AppConfig 中，您必須在建立組態後部署新版本。

停用預設組態

您可以將具有相同 ConfigurationID 的組態區塊新增至自訂組態描述檔，並為啟用欄位提供 false 值，以停用預設組態規則。

例如，如果預設組態設定檔中存在下列組態：

```
{
 "AWS::EC2::Instance": {
  "AMSManagedBlock1": {
   "Enabled": true,
   "Filter": {
    "Platform": "Windows"
   },
   "Tags": [{
    "Key": "my-tag",
    "Value": "SampleValueA"
   }]
```

```
  }
 }
}
```

您可以在自訂組態設定檔中包含下列項目，以停用此標記規則：

```
{
 "AWS::EC2::Instance": {
  "AMSManagedBlock1": {
   "Enabled": false
  }
 }
}
```

> **Important**
>
> 請記得在進行組態變更後部署組態變更；如需相關資訊，請參閱 部署組態變更。在 SSM AppConfig 中，您必須在建立組態後部署新版本。

移除 Resource Tagger 套用的標籤

如果標籤不存在於組態設定檔中，或者存在篩選條件不相符，則 Resource Tagger 會移除任何字首為 ams：rt 的標籤。這表示您可以執行下列其中一項動作來移除 Resource Tagger 套用的標籤：

- 修改定義標籤的自訂組態區段。
- 新增特定資源的例外狀況，使其不再符合篩選條件。

例如：如果 Linux 執行個體具有下列標籤：

```
"Tags": [{
    "Key": "ams:rt:MyOwnTag",
    "Value": true
},{
    "Key": "myTag",
    "Value": true
}]
```

您也可以部署下列 Resource Tagger 組態設定檔：

```
{
    "AWS::EC2::Instance": {
        "AMSMonitoringWindows": {
            "Enabled": true,
            "Filter": {
                "Platform": "Windows"
            },
            "Tags": [{
                "Key": "ams:rt:ams-managed",
                "Value": "true"
            }]
        }
    }
}
```

Resource Tagger 會回應新的組態變更，而執行個體上唯一的標籤會變成：

```
"Tags": [{
    "Key": "myTag",
    "Value": true
}]
```

> **Warning**
>
> 指定新組態的名稱時請小心 (SampleConfigurationBlock在提供的範例中），因為您可能會不小心以相同的名稱覆寫 AMS 受管組態。

> **Important**
>
> 請記得在進行組態變更後部署組態變更；如需相關資訊，請參閱 部署組態變更。在 SSM AppConfig 中，您必須在建立組態後部署新版本。

檢視或變更 Resource Tagger 組態

在加入和駐留在 AMSResourceTagger 應用程式和 AMSInfrastructure 環境中的 AWS AppConfig 中，部署到您帳戶的兩個 JSON 組態設定檔 AMSManagedTags 和 CustomerManagedTags，可透過 AppConfig 的 GetConfiguration API 進行檢閱。 AppConfig AMSResourceTagger AMSInfrastructure

以下是此 GetConfiguration 呼叫的範例：

```
aws appconfig get-configuration
 --application AMSResourceTagger
 --environment AMSInfrastructure
 --configuration AMSManagedTags
 --client-id ANY_STRING
 outfile.json
```

應用程式：AppConfig 邏輯單位可提供 資源交錯器的功能，這是 AMSResourceTagger。

- 環境：AMSInfrastructure。
- 組態：若要檢視 AMS Accelerate 預設標籤定義，值為 AMSManagedTags，而若要檢視客戶標籤定義，值為 CustomerManagedTags。
- 用戶端 ID：唯一的應用程式執行個體識別符，可以是任何字串。
- 然後，您可以在指定的輸出檔案中檢視標籤定義，在此案例中為 outfile.json。

然後，您可以在指定的輸出檔案中檢視警示定義，在此情況下為 outfile.json。

您可以在 AMSInfrastructure 環境中檢視過去的部署，以查看部署至您帳戶的組態版本。

若要覆寫標籤規則：

透過 AWS CloudFormation 使用 AWS CloudFormation for Accelerate 部署組態設定檔或 更新自訂描述檔，或直接使用 AppConfig 的 CreateHostedConfigurationVersion API 來覆寫任何現有的標籤規則。使用相同的 ConfigurationID 做為預設組態標籤規則會覆寫預設規則，並套用自訂規則。

若要部署對 CustomerManagedTags 文件所做的變更：

對自訂組態描述檔進行變更後，您必須為其部署變更。若要部署新的變更，必須使用 AWS AppConfig 主控台或 CLI 執行 AppConfig 的 StartDeployment API。

部署組態變更

自訂完成後，必須透過 StartDeployment API 部署 AWS AppConfig 這些變更。下列指示說明如何使用部署 AWS CLI。此外，您可以使用 AWS Management Console 進行這些變更。如需詳細資訊，請參閱步驟 5：部署組態。

```
aws appconfig start-deployment
--application-id <application_id>
--environment-id <environment_id>
```

```
--deployment-strategy-id <deployment_strategy_id>
--configuration-profile-id <configuration_profile_id>
--configuration-version 1
```

- 應用程式 ID：應用程式 AMSResourceTagger 的應用程式 ID。透過 ListApplications API 呼叫取得此項目。
- 環境 ID：環境 ID；透過 ListEnvironments API 呼叫取得此 ID。
- 部署策略 ID：部署策略 ID；透過 ListDeploymentStrategies API 呼叫取得此 ID。
- 組態設定檔 ID：CustomerManagedTags 的組態設定檔 ID；透過 ListConfigurationProfiles API 呼叫取得此 ID。
- 組態版本：您要部署的組態設定檔版本。

> **Important**
>
> Resource Tagger 會套用組態設定檔中指定的標籤。您對資源標籤所做的任何手動修改（使用 AWS Management Console或 CloudWatch CLI/SDK) 都會自動還原，因此請確定您的變更是透過 Resource Tagger 定義。若要了解 Resource Tagger 建立哪些標籤，請尋找字首為 的標籤索引鍵`ams:rt:`。

使用 StartDeployment 和 StopDeployment API 動作限制對部署的存取，以便信任的使用者了解將新組態部署到目標的責任和後果。

若要進一步了解如何使用 AWS AppConfig 功能來建立和部署組態，請參閱使用 AWS AppConfig 中的文件。

設定 Terraform 以忽略 Resource Tagger 標籤

如果您使用 Terraform 佈建資源，而且想要使用 Resource Tagger 來標記資源，Terraform 可能會將 Resource Tagger 標籤識別為偏離。

您可以使用生命週期組態區塊或 ignore_tags 全域組態區塊，將 Terraform 設定為忽略所有 Resource Tagger 標籤。如需詳細資訊，請參閱資源標記中資源標記的 Terraform 文件。

下列範例示範如何建立全域組態，以忽略以 Resource Tagger 標籤字首 開頭的所有標籤`ams:rt:`：

```
provider "aws" {
  # ... potentially other configuration ...
```

```
  ignore_tags {
    key_prefixes = ["ams:rt:"]
  }
}
```

檢視 Resource Tagger 管理的資源數量

Resource Tagger 每小時將指標傳送至 AMS/ResourceTagger 命名空間中的 Amazon CloudWatch。只會針對 Resource Tagger 支援的資源類型發出指標。

指標名稱	維度	描述
ResourceCount	元件、ResourceType	在此區域中部署的資源數量（指定資源類型的）。 單位：計數
ResourcesMissingManagedTags	元件、ResourceType	根據組態描述檔，需要受管標籤但尚未由 Resource Tagger 標記的資源（指定資源類型的）數量。 單位：計數
UnmanagedResources	元件、ResourceType	Resource Tagger 未套用受管標籤的資源數量（指定資源類型的）。一般而言，這些資源不符合任何 Resource Tagger 組態區塊，或明確地從組態區塊中排除。 單位：計數
MatchingResourceCount	元件、ResourceType、ConfigClauseName	符合 Resource Tagger 組態區塊的資源數量（指定資源類型的）。若要讓資源符合組態區塊，必須啟用區塊，且資源必須符合區塊的篩選條件。 單位：計數

這些指標也可以在 AMS-Resource-Tagger-Reporting-Dashboard 中以圖形形式檢視。若要查看儀表板，請從 Amazon CloudWatch 管理主控台選取 AMS-Resource-Tagger-Reporting-Dashboard。根據預設，此儀表板中的圖形會顯示過去 12 小時期間的資料。

AMS Accelerate 會將 CloudWatch 警示部署到您的帳戶，以偵測未受管資源數量的顯著增加，例如 AMS Resource Tagger 從管理中排除的資源。AMS Operations 將調查超過以下三個未受管資源的增加：相同類型的三個資源，或相同類型的所有資源增加 50%。如果變更似乎不是刻意的，AMS Operations 可能會與您聯絡以檢閱變更。

使用 CloudFormation 為 AMS Accelerate 建立標籤

您可以使用 在堆疊層級（請參閱 AWS CloudFormation 文件、資源標籤) 或個別資源層級（例如，請參閱標記 Amazon EC2 資源） AWS CloudFormation 套用標籤。

> **Important**
>
> 有些 AMS Accelerate 服務元件需要具有 ams：rt： 字首的標籤。Resource Tagger 認為其擁有這些標籤，如果資源 Tagger 組態規則不允許，則會將其刪除。即使您使用的是 AWS CloudFormation 或 Terraform，您一律需要為這些標籤部署 Resource Tagger 組態描述檔。

AWS CloudFormation AMS Accelerate 的使用案例

本節列出常用執行的動作 AWS CloudFormation。

主題

- 使用 AWS CloudFormation for Accelerate 標記 EC2 執行個體
- 使用 標記 AutoScaling 群組 (ASG) AWS CloudFormation 以加速
- 使用 AWS CloudFormation for Accelerate 部署組態設定檔

使用 AWS CloudFormation for Accelerate 標記 EC2 執行個體

以下是如何將值為 true 的 ams：rt：ams-managed 標籤套用至由 管理的 Amazon EC2 執行個體的範例 AWS CloudFormation。ams：rt：ams 受管標籤會選擇讓 AMS Accelerate 監控您的資源。

```
 Type: AWS::EC2::Instance

Properties:
  InstanceType: "t3.micro"

  # ...other properties...
```

```
  Tags:
    - Key: "ams:rt:ams-managed"
      Value: "true"
```

使用 標記 AutoScaling 群組 (ASG) AWS CloudFormation 以加速

以下是如何將值為 true 的 ams：rt：ams-managed 標籤套用至受管 Auto Scaling 群組的範例 AWS CloudFormation。請注意，Auto Scaling 群組會將標籤傳播到由其建立的 Amazon EC2 執行個體。ams：rt：ams 受管標籤會選擇讓 AMS Accelerate 監控您的資源。

```
  Type: AWS::AutoScaling::AutoScalingGroup
Properties:
  AutoScalingGroupName: "SampleASG"

  # ...other properties...

  Tags:
    - Key: "ams:rt:ams-managed"
      Value: "true"
```

使用 AWS CloudFormation for Accelerate 部署組態設定檔

如果您想要使用 部署`CustomerManagedTags`組態設定檔 AWS CloudFormation，您可以使用下列 CloudFormation 範本。在 `AMSResourceTaggerConfigurationVersion.Content` 欄位中放入您想要的 JSON 組態。

當您在 CloudFormation Stack 或 Stack Set 中部署範本時，如果您未遵循組態所需的 JSON 格式，`AMSResourceTaggerDeployment` 資源的部署將會失敗。語法和結構 如需預期格式的詳細資訊，請參閱 。

如需將這些範本部署為 CloudFormation 堆疊或堆疊集的說明，請參閱下列 AWS CloudFormation 相關文件：

- 在 AWS CloudFormation 主控台上建立堆疊
- 使用 建立堆疊 AWS CLI
- 建立堆疊集

> **Note**
>
> 如果您使用其中一個範本部署組態版本，然後刪除 CloudFormation 堆疊/堆疊集，則範本組態版本會保留為目前部署的版本，而且不會進行任何額外的部署。如果您想要還原為預設組態，則需要手動部署空白組態（也就是只有 {}），或將堆疊更新為空白組態，而不是刪除堆疊。

JSON

```
{
  "Description": "Custom configuration for the AMS Resource Tagger.",
  "Resources": {
    "AMSResourceTaggerConfigurationVersion": {
      "Type": "AWS::AppConfig::HostedConfigurationVersion",
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-ApplicationId"
        },
        "ConfigurationProfileId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-CustomerManagedTags-
ProfileID"
        },
        "Content": "{\"Options\": {\"ReadOnly\": false}}",
        "ContentType": "application/json"
      }
    },
    "AMSResourceTaggerDeployment": {
      "Type": "AWS::AppConfig::Deployment",
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-ApplicationId"
        },
        "ConfigurationProfileId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-CustomerManagedTags-
ProfileID"
        },
        "ConfigurationVersion": {
          "Ref": "AMSResourceTaggerConfigurationVersion"
        },
        "DeploymentStrategyId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-Deployment-StrategyID"
        },
```

```
        "EnvironmentId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-EnvironmentId"
        }
      }
    }
  }
}
```

YAML

```
Description: Custom configuration for the AMS Resource Tagger.
Resources:
  AMSResourceTaggerConfigurationVersion:
    Type: AWS::AppConfig::HostedConfigurationVersion
    Properties:
      ApplicationId:
        !ImportValue AMS-ResourceTagger-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-ResourceTagger-Configuration-CustomerManagedTags-ProfileID
      Content: |
        {
          "Options": {
            "ReadOnly": false
          }
        }
      ContentType: application/json
  AMSResourceTaggerDeployment:
    Type: AWS::AppConfig::Deployment
    Properties:
      ApplicationId:
        !ImportValue AMS-ResourceTagger-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-ResourceTagger-Configuration-CustomerManagedTags-ProfileID
      ConfigurationVersion:
        !Ref AMSResourceTaggerConfigurationVersion
      DeploymentStrategyId:
        !ImportValue AMS-ResourceTagger-Configuration-Deployment-StrategyID
      EnvironmentId:
        !ImportValue AMS-ResourceTagger-Configuration-EnvironmentId
```

使用 Terraform 為 AMS Accelerate 建立標籤

如果您不想使用 AMS Accelerate Resource Tagger，您可以使用 Terraform 套用自己的標籤。不過，如果您因為 Resource Tagger 從 Terraform 定義漂移而不想使用 Resource Tagger，有一種方法可讓您使用 Resource Tagger 並忽略它造成的漂移；請參閱 設定 Terraform 以忽略 Resource Tagger 標籤。

> **Important**
>
> 有些 AMS Accelerate 服務元件需要具有 ams：rt： 字首的標籤。Resource Tagger 認為它擁有這些標籤，如果資源 Tagger 組態規則不允許，則會刪除它們。您必須為這些標籤部署 Resource Tagger 組態描述檔，即使您使用的是 AWS CloudFormation 或 Terraform。

以下是如何將值為 true 的 ams：rt：ams 受管標籤套用至 Terraform 管理的 Amazon EC2 執行個體的範例。ams：rt：ams 受管標籤會選擇讓 AMS Accelerate 監控您的資源。

```
  resource "aws_instance" "sample_linux_instance" {
    # ...ami and other properties...

    instance_type = "t3.micro"

    tags = {
        "ams:rt:ams-managed" = "true"
    }
}
```

以下是如何將值為 true 的 ams：rt：ams 受管標籤套用至 Terraform 管理的 Auto Scaling 群組的範例。請注意，Auto Scaling 群組會將標籤傳播至由其建立的 Amazon EC2 執行個體。ams：rt：ams 受管標籤會選擇讓 AMS Accelerate 監控您的資源。

```
  resource "aws_autoscaling_group" "sample_asg" {
    # ...other properties...

    name = "terraform-sample"

    tags = {
        "ams:rt:ams-managed" = "true"
```

```
    }
}
```

如需如何管理 Terraform 建立的資源標籤的說明，請參閱 設定 Terraform 以忽略 Resource Tagger 標籤。

AMS Accelerate 中的事件報告、服務請求和帳單問題

使用 AMS Accelerate，您可以隨時透過 中的 AWS 支援中心請求有關操作問題和請求的協助 AWS Management Console。AMS Accelerate 操作工程師可以round-the-clock回應您的事件和服務請求，以及服務的回應時間服務水準協議 (SLAs)。AMS Accelerate 營運工程師會使用相同的機制，主動通知您重要的提醒和問題。

AMS Accelerate 提供各種營運服務，協助您實現卓越營運 AWS。若要快速了解 AMS 如何 AWS 雲端透過我們的一些關鍵營運功能，包括round-the-clock服務台、主動監控、安全性、修補、記錄和備份，協助您的團隊在 中實現整體卓越營運，請參閱 AMS 參考架構圖表。

主題

AMS Accelerate 中的事件管理

在 AMS Accelerate 中，您可以使用 AWS Support Center Console來提交事件報告。事件是影響受管環境 AWS 服務 的效能問題，由 AMS Accelerate 或您決定。AMS Accelerate 團隊識別的事件會先收到事件 （監控擷取的系統狀態變更）。如果超過設定的閾值，事件會觸發警示，也稱為警示。AMS Accelerate 操作團隊會判斷事件是不會影響事件，還是事件 （服務中斷或降級），還是問題 （一或多個事件的潛在根本原因）。

> **Note**
>
> AMS Accelerate 團隊也會透過程式設計方式，使用服務代碼為 的 AWS Support API 來接收您建立的事件`service-ams-operations-report-incident`。

如需使用 的詳細資訊 支援，請參閱 入門 支援。

什麼是事件管理？

事件管理是 AMS 用來記錄、處理、傳達作用中事件進度並提供通知的程序。

事件管理程序的目標是確保盡快還原受管服務的正常操作、將業務影響降至最低，並隨時通知所有相關各方。

事件的範例包括（但不限於）網路連線遺失或降級、無回應的程序或 API，或未執行的排程任務（例如備份失敗）。

下圖說明您向 AMS 報告之事件的工作流程。

此圖描述 AMS 向您報告之事件的工作流程。

事件優先順序

在 AWS Support 中心、主控台或 Support API (SAPI) 中建立的事件，其分類與在 AMS 主控台中建立的事件不同。

- 低：與 AWS 或 AMS 資源相關的業務服務或應用程式的非關鍵函數會受到影響。
- 中：與 AWS 和/或 AMS 資源相關的商業服務或應用程式受到中度影響，且運作狀態降低。
- 高：您的業務會受到重大影響。與 AWS 和/或 AMS 資源相關的應用程式重要功能無法使用。預留給影響生產系統的最重要中斷。

> **Note**
>
> AWS Support Console 提供五個層級的事件優先順序，我們可將其轉換為三個 AMS 層級。

事件回應和解決方案的運作方式

AMS Accelerate 使用 IT 服務管理 (ITSM) 事件管理最佳實務，在需要時盡快還原服務。

我們透過全球各地的營運中心，提供全年無休follow-the-sun支援，讓專屬的操作員主動監看監控儀表板和事件佇列。

我們的營運工程師使用內部事件追蹤工具來識別、記錄、分類、排定優先順序、診斷、解決和關閉事件；我們透過 AWS 支援中心和 AWS 支援 API 為您提供所有這些活動的更新。我們的運算子利用各種內部 AWS 支援工具，協助處理所有這些活動。這些運算子非常熟悉 AMS Accelerate 支援的基礎設施，並具備專家層級的技術技能來解決已識別的支援問題。如果我們的營運商需要協助，Premium Support AWS 和服務團隊會提供服務。

在 AMS Accelerate 操作團隊收到您的事件之後，我們會驗證優先順序和分類，如果需要任何釐清，我們會與您合作。例如，如果事件報告更好的分類為服務請求，則會重新分類，AMS Accelerate 服務請求團隊會接管並通知您。如果事件可由接收運算子解決，則會採取步驟來快速解決事件。AMS Accelerate 運算子會參考內部文件以取得解決方案，並視需要將事件呈報給其他支援資源，直到事件解決為止。解決後，AMS Accelerate 操作團隊會記錄事件和解決方案以供日後使用。

如果關鍵嚴重性事件影響您的關鍵工作負載，AMS Accelerate 可能會建議基礎設施還原。故障診斷問題和僅從已知的功能備份還原之間，通常存在權衡，而您的風險和服務停機時間的影響是決定因素。如果您有時間對問題進行故障診斷，AMS Accelerate 會協助您，您的雲端服務交付管理員 (CSDM) 可能會參與其中，但如果還原的急迫性很高，AMS Accelerate 可以立即啟動還原。

在 AMS Accelerate 中使用事件

從 AWS 支援中心，您可以執行下列任務：

- 報告和更新事件。若要報告 AMS Accelerate 事件，請從服務功能表中選擇 AMS Operations -- Report Incident。
- 取得所有已提交事件的清單和詳細資訊。
- 依狀態和其他篩選條件縮小搜尋事件的範圍。
- 將通訊和檔案附件新增至您的事件，並新增電子郵件收件人以進行案例通訊。
- 啟動即時聊天或請求回撥您的事件。

> **Note**
>
> 即時聊天功能不適用於安全事件；對於安全問題，請建立高優先順序 (P1 或 P2) 支援案例。

- 解決事件。
- 為事件通訊評分。

下列範例說明使用 支援中心來提交事件。提交後，AMS Accelerate 團隊會與您合作，根據標準 AMS Accelerate SLA 解決事件。

提交事件以加速

若要使用支援中心報告事件，請參閱支援文件：建立支援案例

若要使用 支援 中心報告事件：

1. 按一下建立案例。建立事件案例頁面隨即開啟。

2. 開啟技術支援問題類型選單，然後選擇 AMS Operations -- Report Incident。提供事件的相關資訊，然後選擇建立。
3. 若要在事件解決程序的每個步驟透過電子郵件收到通知，請務必填寫 CC 電子郵件選項；如果您透過聯合連線，請先登入，再遵循 AMS Accelerate 傳送給您的事件相關電子郵件中的連結。

> **Note**
>
> 就您的描述盡可能提供詳細資訊。請附上相關資源以及其他有助於我們了解您問題的任何資訊。例如，若要解決效能問題，描述時應包括時間戳記和日誌。如果是功能請求或一般指導問題，描述中應包含您的環境和用途。在所有情況下，都請您遵循案例提交表單上顯示的 Description Guidance (描述指導方針)。
> 當您提供的資訊愈詳細，將可提高您的案例快速解決的機會。

您也可以使用 AWS Support API 搭配服務代碼`service-ams-operations-report-incident`來報告事件。

監控和更新 Accelerate 事件

您可以使用支援中心，或以程式設計方式使用 支援 API `DescribeCases`操作，來更新、監控和檢閱事件報告和服務請求，這兩者稱為 案例。

若要使用 支援 Center 監控案例、事件或服務請求，請遵循下列步驟。

1. 在 AWS 管理主控台中，瀏覽至支援。
2. 從左側導覽中，選取您的支援案例，瀏覽至案例，然後選擇主旨連結以開啟包含目前狀態和通訊的詳細資訊頁面。

   如果您想要此時使用電話或聊天，請按一下支援中心的開啟案例，在 支援 中心開啟案例建立頁面，自動填入 AMS 服務類型。

   當 Accelerate 操作團隊更新報告的事件或服務請求案例時，您會收到一封電子郵件，以及支援中心中事件的連結，以便您可以回應。

   > **Note**
   >
   > 您無法透過回覆電子郵件來回應案例通訊。

如果儀表板中有許多案例，您可以使用 Filteroption：

- 主旨：使用此篩選條件搜尋案例主旨中的關鍵字。
- 嚴重性：使用此項目可依嚴重性篩選案例，方法是從清單中選取嚴重性。
- 案例類型：使用此項目可查看特定案例類型的所有案例。加速事件和服務請求，連同任何服務特定案例都會出現在技術支援案例類型下。
- 狀態：使用此項目可透過從清單中選擇特定狀態，依狀態篩選案例。

3. 若要檢查最新狀態，請重新整理頁面。
4. 如果有許多通訊並未全部顯示在頁面上，請選擇載入更多。
5. 若要提供案例狀態的更新，請選擇回覆、輸入新的通訊，然後選擇提交。
6. 若要在案例解決到滿意程度後關閉案例，請選擇關閉案例。

請務必透過 1-5 星評分來評定服務，讓 AMS 知道我們的表現。

使用 支援 API 管理 Accelerate 事件

您可以使用 支援 API 來建立事件，並在調查您的問題時新增與 支援 員工之間的通訊。 支援 API 建立AWS 支援中心的大部分行為模型。

如需有關您可以使用此 AWS 支援服務的資訊，請參閱程式設計 AWS 支援案例的生命週期。

> **Note**
>
> AMS Accelerate 團隊會以程式設計方式使用具有服務代碼 的 來接收您建立的事件`service-ams-operations-report-incident`。

回應 AMS Accelerate 產生的事件

AMS Accelerate 會主動監控您的資源。如需詳細資訊，請參閱 AMS Accelerate 中的監控和事件管理。有時 AMS Accelerate 會識別並建立事件，最常通知您事件。如果需要您採取動作來解決事件，AMS Accelerate 團隊會將通知傳送至您為帳戶提供的聯絡資訊。您以與任何其他事件相同的方式回應此通知，通常是透過支援中心，但在某些情況下需要透過電子郵件或電話聯絡。

> **Important**
>
> 若要接收事件案例或服務請求的狀態變更通知，請在地址欄位中輸入電子郵件地址。

觀看 Akshay 的影片以進一步了解 (4：15)

Accelerate 中的服務請求管理

主題

AMS Accelerate 使用服務請求管理來記錄、處理、傳達進度，並提供作用中服務請求的通知。

服務請求管理程序的目標是確保您的受管服務提供您需要的服務。

對於帳單相關查詢，請建立服務請求。

> **Note**
>
> AMS Accelerate 團隊會以程式設計方式使用服務代碼為 的 AWS Support API 來接收您建立的服務請求`service-ams-operations-service-request`。

使用 AWS Support Center，您可以執行下列任務：

- 報告和更新服務請求。在 AMS Accelerate 服務請求中，從服務功能表中選擇 AMS 操作 -- 服務請求。
- 取得所有已提交服務請求的清單和詳細資訊。
- 依狀態和其他篩選條件縮小搜尋服務請求的範圍。
- 將通訊和檔案附件新增至您的請求，並新增電子郵件收件人以進行案例通訊。

- 解決服務請求。
- 評價服務請求通訊。

何時使用 Accelerate 的服務請求

下列範例說明服務請求。在您提交服務請求後，AMS Accelerate 團隊會與您合作，根據您的 AMS SLA 解決請求。

- AMS 或 AWS 一般指引
- 修補程式 MW 相關問題
- 備份排程相關問題
- 有關 AWS 服務功能的問題

以下是不應在服務請求中提出的範例：

- 存取問題
- 修補程式失敗
- 備份失敗

服務請求管理如何在 Accelerate 中運作

服務請求由待命 AMS Accelerate 操作團隊處理。

AMS Accelerate 操作團隊收到您的服務請求後，會檢閱該請求，以確保其正確分類為服務請求或事件。如果將其重新分類為事件，則 AMS Accelerate 事件管理程序會開始，並會傳送通知給您。

如果 AMS Accelerate Operator 可以解決服務請求，則會立即採取步驟。例如，如果服務請求是針對架構建議或其他資訊，則運算子會將您參考適當的資源或直接回答問題。

如果您的服務請求分析發現錯誤或功能請求，則 AMS 會透過服務請求傳送通知給您。由於功能請求或錯誤修正沒有 ETA，因此原始服務請求會關閉。如需與原始服務請求相關的後續問題，請聯絡您的 CSDM。

如果服務請求超出 AMS Accelerate 操作的範圍，運算子會傳送請求給您的雲端服務交付管理員，讓他們可以與您或適當的 AWS 支援團隊通訊，並傳送電子郵件給您，告知您正在採取哪些步驟。

在您表示您對結果感到滿意之前，服務請求不會解決。

> **Note**
>
> 在所有情況下，我們建議您提供聯絡人電子郵件、名稱和電話號碼，以利通訊。

在 Accelerate 中建立服務請求

若要建立服務請求，請遵循下列步驟：

1. 從 AMS Accelerate 主控台，瀏覽至儀表板。
2. 選擇開啟服務請求，會預先選取 AMS – 服務請求。
3. 選擇 aCategory。
4. ChooseSeverity （僅限 Plus 或 Premium 方案）。
5. 輸入以下資訊：
   - 主旨：服務請求的描述性標題。
   - 描述：服務請求的完整描述、受影響的系統，以及解決的預期結果。
6. 若要新增附件，請選擇附件檔案，瀏覽至您想要的附件，然後選擇開啟。若要刪除附件，請選擇刪除圖示
7. 聯絡我們：透過 Web 預設聯絡 AMS。若要選取其他選項：
   - 偏好的聯絡語言：英文是 AMS Accelerate 服務請求支援的語言。
   - Web：您的服務請求是透過 Web 提交，並由 AMS 操作團隊處理。
   - 聊天：與 AMS Accelerate 操作代表線上聊天。此選項會將您新增至聊天佇列。
   - 電話：AMS 操作代表會回撥給您。如果適用，請輸入您的 AWS 區域、電話號碼和延伸項目。
   - 其他聯絡人：輸入您想要在服務請求上複製的任何其他電子郵件地址。
8. 選擇提交。

   案例詳細資訊頁面隨即開啟，其中包含服務請求的相關資訊，例如 Type、Subject、Created、ID 和Status。此外，包含您建立之請求描述的 aCorrespondencearea。

   若要開啟通訊區域並提供其他詳細資訊或狀態更新，請選擇回覆。

   解決服務請求後，選擇解決案例。

   如果有許多通訊並未全部顯示在頁面上，請選擇載入更多。

請務必透過 1-5 星評分來評定服務，讓 AMS 知道我們的表現。

> **Note**
>
> 如果您要測試服務請求功能，建議您將無動作旗標新增至服務請求的主體，例如 `AMSTestNoOpsActionRequired`。然後，您可以在不啟動服務請求解決程序的情況下進行測試。
> AMS Accelerate 團隊會以程式設計方式，使用服務代碼為 的 AWS Support API 來接收您建立的服務請求`service-ams-operations-service-request`。

監控和更新 Accelerate 的服務請求

若要使用 支援 Center 監控案例、事件或服務請求，請遵循下列步驟。

1. 在 AWS 管理主控台中，瀏覽至支援。
2. 從左側導覽中，選取您的支援案例，瀏覽至案例，然後選擇主旨連結以開啟包含目前狀態和通訊的詳細資訊頁面。

   如果您想要此時使用電話或聊天，請按一下支援中心的開啟案例，在 支援 中心開啟案例建立頁面，自動填入 AMS 服務類型。

   當 Accelerate 操作團隊更新報告的事件或服務請求案例時，您會收到一封電子郵件，以及支援中心中事件的連結，以便您可以回應。

   > **Note**
   >
   > 您無法透過回覆電子郵件來回應案例通訊。

   如果儀表板中有許多案例，您可以使用 Filteroption：

   - 主旨：使用此篩選條件搜尋案例主旨中的關鍵字。
   - 嚴重性：使用此項目可依嚴重性篩選案例，方法是從清單中選取嚴重性。
   - 案例類型：使用此項目可查看特定案例類型的所有案例。加速事件和服務請求，連同任何服務特定案例都會出現在技術支援案例類型下。

- 狀態：使用此項目可透過從清單中選擇特定狀態，依狀態篩選案例。

3. 若要檢查最新狀態，請重新整理頁面。
4. 如果有許多通訊並未全部顯示在頁面上，請選擇載入更多。
5. 若要提供案例狀態的更新，請選擇回覆、輸入新的通訊，然後選擇提交。
6. 若要在案例解決到滿意程度後關閉案例，請選擇關閉案例。

   請務必透過 1-5 星評分來評定服務，讓 AMS 知道我們的表現。

使用 Accelerate 的支援 API 管理服務請求

您可以使用AWS Support API 來建立服務請求，並在問題調查以及與 AWS 支援人員的互動期間新增通訊。 AWS 支援 API 模型大部分的AWS 支援中心行為。

AMS 團隊也會透過使用 AWS Support API 搭配服務碼 service-ams-operations-service-request，以程式設計方式接收您建立的服務請求。

如需如何使用此 AWS 支援服務的詳細資訊，請參閱程式設計 AWS 支援案例的生命週期。

回應 AMS Accelerate 產生的服務請求

AMS Accelerate 會主動監控您的資源；如需詳細資訊，請參閱 AMS Accelerate 中的監控和事件管理。有時 AMS Accelerate 會為您建立服務請求或服務通知，通常是在需要您採取動作來解決服務請求時。在這種情況下，AMS Accelerate 團隊會傳送通知給您為帳戶提供的聯絡人。您以與任何其他案例相同的方式回應此服務請求，通常是透過支援中心，但在某些情況下，需要電子郵件或電話通訊。

> **Important**
>
> 若要接收服務請求或事件案例的狀態變更通知，您必須在地址欄位中輸入電子郵件地址。通知只會傳送至建立案例時新增至案例的電子郵件地址。

只有在 AMS Accelerate 聯合網路上使用電子郵件伺服器時，通知電子郵件中的連結才能運作。否則，您可以前往 AMS Accelerate 主控台並使用案例詳細資訊頁面來回應通訊。

> **Note**
>
> AMS Accelerate 會將通訊傳送到您 AWS 帳戶的主要電子郵件地址；我們建議您新增替代操作聯絡人電子郵件別名，以促進服務請求/通知管理程序。這在 AMS Accelerate 加入程序和相關的加入文件中涵蓋。

Accelerate 中的事件報告和服務請求測試

測試事件報告或服務請求時，我們會要求您在主旨文字中包含 AMSTestNoOpsActionRequired。這可讓 AMS 知道事件或請求僅用於測試。當 AMS 操作工程師看到它時，他們不會以任何方式回應。

AMS Accelerate 的帳單問題

若要提交帳單相關問題，請完成下列步驟：

1. 在 https：//https://console.aws.amazon.com/support/home#/ 開啟 AWS 支援 中心。
2. 選擇帳戶和帳單。
3. 選擇建立案例。
4. 選擇帳戶和帳單，然後依照提示提交您的案例。

AWS Managed Services 中的計劃事件管理

AWS Managed Services (AMS) 計劃事件管理 (PEM) 是一種 AMS 服務產品。PEM 使用 AMS 服務在客戶事件和專案期間進行互動、協調和協助。PEM 可協助協調一組符合 PEM 事件或專案商定範圍和時間表的相關活動。

AMS PEM 條件

規劃的事件是範圍限制和時間限制的專案。AMS 會使用您提供的詳細資訊（包括計劃和範圍、預期成果，以及預期 AMS 操作會執行的變更），以便在 PEM 活動期間有效支援您。然後，您的雲端架構師 (CAs) 會檢閱和評估 PEM 活動的完整性、技術實作和 AMS 操作參與。在 CA 審查之後，AMS 操作會審查計劃，並與您的雲端服務交付經理 (CSDM) 協調營運團隊參與度。

PEM 的類型

以下是可用的 PEM 類型：

- 遊戲日
  - 操作遊戲日：一種以案例為基礎的操作回應遊戲方法，旨在驗證程序、人員和系統的整合。
  - 安全遊戲日：安全事件回應策略，採用以案例為基礎的遊戲方法來評估系統、程序和人員的整合。
- 客戶安全事件：規劃的安全事件。例如，滲透測試。
- 遷移支援：支援計劃的加入和遷移活動。

此工作流程有助於與 AMS 協作，以協調與 AMS 支援相關的計劃事件和遷移活動。如需特定需求的協助，請聯絡您的 CSDM。

AMS PEM 程序

PEM 程序包含下列階段：

- PEM 啟動：您可以使用 CSDM 來定義規劃事件的目標，並判斷 AMS 操作所需的內容。AMS CAs會檢閱 PEM 計劃的技術層面。CAs 在合規、執行最佳化和自動化方面與 AMS Security and Operations 合作，並定義 PEM 前執行任務和交付項目。然後，您的 CSDM 會建立 PEM 票證，並向 AMS 提供專案資訊和技術詳細資訊。AMS 需要 14 個日曆天的前置時間，才能讓 AMS 營運團隊有時間規劃、提供技術審查，以及指派資源。

- PEM 檢閱：AMS 操作團隊會檢閱 PEM 請求，並與 CSDM 合作，確認 PEM 計畫中的資訊正確且完整。
- PEM 接受：AMS 會檢閱提供的資訊，並與 CSDM 溝通 PEM 活動期間的支援層級。如果 PEM 包含完整資訊，且您的 CSDM 同意工作範圍，則 PEM 會獲得核准。
- 準備和執行：AMS 可確保 PEM 開始之前所需的任務已完成，並促進內部和客戶通訊。AMS 可確保 PEM 計劃正確執行，並提供狀態和進度報告。

PEM FAQs

如何在 PEM 事件期間透過 Cases：Service Request SRs)/Incident 與 AMS 互動？

- 使用 CSDM 在 RFC/SR 主旨行中以 格式共用的 PEM ID*PEM-ID*。

  如適用，您可以使用即時聯絡選項。
- 您也可以建立服務請求 (SR) 來討論您的使用案例，或詢問有關計劃事件的問題。如果您使用 SR，則 PEM 不必有效。

提交 PEM 相關案例時，會執行哪些驗證？

- 驗證帳戶 ID 已列在 PEM 上。
- 驗證提供的開始和結束日期之間的 PEM 狀態是否已核准且處於作用中狀態。
- PEM 詳細資訊的連結會在內部提供給 AMS 工程師。

PEM 請求是否有 SLAs 或 SLOs？

- PEMs不會與 SLAs 或 SLOs建立關聯。
- PEM 相關工作項目 SLOs （服務請求、事件） 的 SLAs 和 SLO 由 AMS SLOs 定義。

  如需詳細資訊，請參閱 AMS Accelerate 中的事件報告、服務請求和帳單問題。

我們是否可以透過服務請求 (SR) 建立 PEM？

- 否，PEM 建立必須由 Cloud Service Delivery Manager (CSDM) 管理。

隨需操作

隨需操作 (OOD) 是一種 AWS Managed Services (AMS) 功能，可透過提供 AMS 操作計劃或 目前未原生提供的操作服務，來擴展 AMS 操作計劃的標準範圍 AWS。 選取後，目錄產品會透過自動化和高技能 AMS 資源的組合提供。沒有長期承諾或其他合約，可讓您視需要擴展現有的 AMS 和 AWS 操作和功能。您同意每月購買每個區塊 20 小時的時數區塊 (OOD 區塊）。

您可以從標準化方案目錄中選取 ，並透過服務請求啟動新的 OOD 參與。OOD 產品的範例包括協助維護 Amazon EKS、操作 AWS Control Tower和管理 SAP 叢集。根據需求和我們最常看到的操作使用案例，定期新增新的目錄產品。

OOD 同時適用於 AMS Advanced 和 AMS Accelerate 操作計劃，並可在 AMS 提供的所有 AWS 區域中使用。

AMS 會在實作您請求的變更時，執行客戶安全風險管理 (CSRM)。若要進一步了解 CSRM 程序，請參閱變更請求安全性審查。

隨需操作方案目錄

隨需操作 (OOD) 為您提供下表所述的服務。

> **Note**
>
> 如需關鍵術語的定義，請參閱 AWS Managed Services 文件關鍵術語。

營運計畫	標題	描述	預期結果
AMS Accelerate	Amazon EKS 叢集維護	AMS 透過處理 Amazon Elastic Kubernetes Service (Amazon EKS) 部署的持續維護，釋放您的容器開發人員。AMS 會執行更新叢集所需的end-to-end程序，以解決控制平面、附加元件和節點的元件。AMS 會執行受管節點類型的更新，以及一組精選的 Amazon EKS 和 Kubernetes 附加元件。	客戶團隊協助進行更新 Amazon EKS 叢集的基礎操作工作。

AMS Accelerate	AMI 建置和販賣	AMS 持續為客戶提供 AMI 建置和販賣的管理。 我們的工程師會執行每月發行的訂閱 AMIs、發行緊急修補活動的隨需 AMIs、使用 Runbook 管理變更，以及使用 CloudWatch Monitoring 監控 AMI 組建。我們也為指定帳戶中使用的所有 AMIs 提供故障診斷協助和詳細報告。此服務需要透過 EC2 Image Builder 部署 AMI build Pipelines。AMS 不支援與 EC2 Image Builder 互動的任何其他自動化或服務。	客戶安全狀態改善，客戶花費在建置和販賣 AMIs上的時間減少。
AMS Accelerate	統籌變更執行	與我們的熟練營運工程師合作，將您的業務需求轉換為可在 AWS 環境中安全執行的已驗證變更請求。利用我們自動化的獨特方法和操作最佳實務的知識（例如，影響評估、轉返、兩人規則），無論是大規模的簡單變更，還是具有下游影響的複雜動作。	客戶協助定義、建立和執行自訂變更請求。變更可以是手動或自動化 (CloudFormation、SSM)。必要時，包括諮詢 支援以取得組態指引。不適用於變更應用程式程式碼、應用程式安裝/部署、資料遷移或作業系統組態變更。

AMS Accelerate	AWS Network Firewall 操作	AMS 會與您合作加入防火牆，並實作和管理持續防火牆操作的政策和規則。我們的工程師會利用我們的營運最佳實務和自動化來設定標準化政策和規則，並啟用監控來偵測自動化程序外所做的變更，藉此達成此目的。AMS 會快速通知您不需要的變更，並在要求時提供包含這些變更的選項，或將帳戶還原至先前的組態，以確保您系統的整體穩定性。	客戶團隊透過快速偵測意外的網路防火牆變更，協助降低管理開銷，進而改善事件解決並縮短預期和非預期問題的根本原因分析時間。
AMS Accelerate	AWS Control Tower 操作	持續操作和管理 AWS Control Tower 登陸區域，包括 AWS Transit Gateway 和 AWS Organizations - 提供全面的登陸區域解決方案。我們透過自訂控制和護欄程式庫來處理帳戶販賣、SCP 和 OU 管理、偏離修復、SSO 使用者管理和 AWS Control Tower 升級。	客戶團隊協助一些管理 AWS Control Tower、 AWS Transit Gateway 和 的基礎操作工作 AWS Organizations。
AMS Accelerate	AWS 登陸區域加速操作	AMS 提供透過 AWS 登陸區域加速器 (LZA) 部署之 AWS 登陸區域的持續操作。 我們的工程師會處理組態檔案變更、 AWS Control Tower (CT) 環境管理 （帳戶販賣、OU 建立、CT 護欄）、服務內容政策 (SCP) 管理、CT 偏離偵測和修復、網路組態管理，以及 CT 和 LZA 架構的更新。 AWS LZA 提供一種方法來使用操作最佳實務和服務來設定和管理安全、多帳戶 AWS 環境，例如 AWS Control Tower。	客戶團隊協助持續操作和管理 AWS 登陸區域加速器解決方案。

AMS Accelerate	SAP 叢集協助	SAP 叢集的專用警示、監控、叢集修補、備份和事件修復。此目錄項目可讓您從 SAP 操作團隊卸載一些正在進行的操作工作，以便他們可以專注於容量管理和效能調校。	客戶或合作夥伴 SAP 團隊協助一些基礎操作工作。仍然需要客戶提供其他 SAP 功能，例如容量管理、效能調校、DBA 和 SAP 基礎管理。
AMS Accelerate	EC2 操作上的 SQL Server	AMS 會與您合作，以加入、實作和管理部署在 EC2 執行個體上 SQL Server 資料庫的持續操作。 我們的工程師利用我們的操作最佳實務和自動化，透過執行備份和修補等任務、將 AMS 操作支援延伸至 SQL Server 修補，以包含叢集感知的滾動更新、符合我們勒索軟體防禦策略的備份和還原服務，以及監控對客戶提供的備份和修補控制的遵守情況，來釋放資料庫團隊。	除了將自己的授權 (BYOL) 帶入 EC2 之外，SQL Server 客戶還協助卸載修補和備份資料庫操作，以提高工作負載的彈性和安全狀態。
AMS 進階	Amazon EKS 叢集維護	AMS 透過處理 Amazon Elastic Kubernetes Service (Amazon EKS) 部署的持續維護和運作狀態，釋放您的容器開發人員。AMS 會執行更新叢集所需的end-to-end程序，以解決控制平面、附加元件和節點的元件。AMS 會執行受管節點類型的更新，以及一組精選的 Amazon EKS 和 Kubernetes 附加元件。	客戶團隊協助進行更新 Amazon EKS 叢集的基礎操作工作。
AMS 進階	優先順序 RFC 執行	指定 AMS 操作工程師容量，以優先執行您的變更請求 (RFC)。透過 Amazon Chime 會議室直接與工程師互動，可以調整所有提交的回應層級和優先順序。	客戶會收到 RFCs 的 8 小時回應 SLO。

AMS 進階和 AMS 加速	舊版作業系統升級	將執行個體升級至支援的作業系統版本，以避免執行個體遷移。我們可以利用自動化和軟體廠商的升級功能（例如，Microsoft Windows 2008 R2 到 Microsoft Windows 2012 R2），在您選取的執行個體上執行就地升級。此方法非常適合無法輕鬆在新執行個體上重新安裝的舊版應用程式，並針對舊版作業系統上的已知和未緩解安全威脅提供額外的保護。 就地升級支援下列作業系統： • Microsoft Windows 2012 R2 到 Microsoft Windows 2016 及更高版本 • Microsoft Windows 2016 到 Microsoft Windows 2022 及更高版本 • Red Hat Enterprise Linux 7 到 Red Hat Enterprise Linux 8 • Red Hat Enterprise Linux 8 到 Red Hat Enterprise Linux 9 • Oracle Linux 7 到 Oracle Linux 8	此解決方案適用於無法再重新安裝在新執行個體上的應用程式（例如，遺失原始碼、ISV 停止營業等）。您可以將失敗的升級轉返至其原始狀態。從操作角度來看，回復是偏好的，因為它會使用最新的安全修補程式，將執行個體置於更可支援的狀態。

主題

隨需請求 AMS 操作

AWS Managed Services (AMS) Operations on Demand (OOD) 適用於所有已加入 AMS AWS 帳戶的 。若要利用隨需操作，請向雲端服務交付管理員 (CSDM)、解決方案架構師 (SA)、帳戶管理員或雲

端架構師 (CA) 請求其他資訊。可用的 OOD 方案會列在上述 方案的隨需操作目錄中。業務開發範圍完成後，向 AMS Operations 提交服務請求，以啟動 OOD 業務開發。

每個 OOD 服務請求必須包含與參與相關的下列詳細資訊：

- 請求的特定 OOD 方案，以及每個特定 OOD 方案：
  - 要配置給特定 OOD 方案的區塊數量（一個區塊等於指定日曆月的 20 小時操作資源時間，以適用隨需操作方案 AWS的當時標準費率收費）。
  - 請求特定 OOD 方案的每個 AWS Managed Services 帳戶的帳戶 ID。

您必須透過下列任一方式提交 OOD 服務請求：

- 接收適用隨需操作方案的 AWS Managed Services 帳戶，或
- 一種 AWS Managed Services 帳戶，在所有功能模式下為 AWS Organizations 管理帳戶，代表其屬於 AWS Managed Services 帳戶的任何成員帳戶。

收到 OOD 服務請求後，AMS Operations 會使用帳戶核准、部分核准或拒絕來檢閱和更新帳戶。

一旦 OOD 方案服務請求獲得核准，AMS 和您就會協調以開始參與。在服務請求獲得核准且約定參與開始日期之前，不會啟動 OOD 方案。

AMS 會使用 OOD 區塊的每月訂閱分配。我們會從參與開始日期開始，每月分配已核准的區塊數量，直到您透過新的服務請求請求退出為止。OOD 區塊在日曆月內有效。未使用的區塊或區塊部分不會轉換或轉送至未來幾個月。

無論實際使用多少小時，您每個月至少需要支付一個 OOD 區塊的費用。不使用任何額外、已配置的 OOD 區塊，則不會計費。

變更隨需操作方案

若要請求變更隨選操作 (OOD) 方案的持續參與，請提交包含以下資訊的服務請求：

- 正在請求的修改（和）
- 修改生效的請求日期。

收到 OOD 服務請求後，AMS Operations 會檢閱請求，並使用其核准進行更新，或請求指派的 CSDM 與您合作，以判斷修改的範圍和影響。如果判斷修改需要 CSDM 的範圍工作，您必須在範圍練習完成後提交第二個 OOD 服務請求，以啟動修改後的參與。

核准後，最新修改的區塊配置會變成並持續保持作用中狀態，取代任何先前的區塊配置，除非 AWS 和您另有同意。

報告和選項

AWS Managed Services (AMS) 會整理各種原生 AWS 服務的資料，以提供主要 AMS 產品的加值報告。

AMS 提供兩種類型的詳細報告：

- 請求報告：您可以透過 Cloud Service Delivery Manager (CSDM) 臨時請求特定報告。這些報告沒有限制，因為您可能需要在加入或關鍵事件期間多次請求這些報告。不過，請注意，這些報告並非設計為按照每週報告等排程提供。若要進一步了解您的需求或使用自助式報告的詳細資訊，請聯絡您的 CSDM。
- 自助式報告：AMS 自助式報告可讓您視需要隨時直接查詢和分析資料。使用自助式報告從 AMS 主控台存取報告，並透過 S3 儲存貯體 （每個帳戶一個儲存貯體） 報告資料集。這可讓您將資料整合到您偏好的商業智慧 (BI) 工具，以便根據您的需求自訂報告。

主題

隨需報告

主題

AMS 會整理來自各種原生 AWS 服務的資料，以提供主要 AMS 產品的附加價值報告。如需這些報告的副本，請向 Cloud Service Delivery Manager (CSDM) 提出請求。

AMS 主機管理報告

可用的報告

- SSM 代理程式涵蓋範圍報告

SSM 代理程式涵蓋範圍報告

AMS SSM 代理程式涵蓋範圍報告會通知您帳戶中的 EC2 執行個體是否已安裝 SSM 代理程式。

欄位名稱	定義
客戶名稱	有多個子客戶之情況的客戶名稱
資源區域	AWS 資源所在的區域
帳戶名稱	帳戶的名稱
AWS 帳戶 ID	AWS 帳戶的 ID
資源 ID	EC2 執行個體的 ID
資源名稱	EC2 執行個體的名稱
合規旗標	指出資源是否已安裝 SSM Agent (「合規」) (「NON_COMPLIANT」)

AMS 備份報告

可用的報告

- 備份任務成功/失敗報告
- 備份摘要報告
- 備份摘要/涵蓋報告

備份任務成功/失敗報告

備份任務成功/失敗報告提供有關過去幾週內執行的備份的資訊。若要自訂報告，請指定您要擷取資料的週數。預設週數為 12。下表列出報告中包含的資料：

欄位名稱	定義
AWS 帳戶 ID	資源所屬的 AWS 帳戶 ID
帳戶名稱	AWS 帳戶名稱
備份任務 ID	Backup 任務的 ID
資源 ID	備份資源的 ID
資源類型	正在備份的資源類型
資源區域	備份資源 AWS 的區域
備份狀態	備份的狀態。如需詳細資訊，請參閱備份任務狀態
復原點 ID	復原點的唯一識別符
狀態訊息	描述備份任務期間發生的錯誤或警告
備份大小	備份的大小，以 GB 為單位
復原點 ARN	已建立備份的 ARN
復原點存留期，以天為單位	自建立復原點以來經過的天數
少於 30 天	少於 30 天的備份指標

備份摘要報告

欄位名稱	定義
客戶名稱	多個子客戶的情況的客戶名稱
備份月份	備份的月份
備份年份	備份年份
資源類型	正在備份的資源類型

欄位名稱	定義
資源數量	已備份的資源數量
復原點的數量	不同快照的數量
少於 30 天的備份	少於 30 天的備份計數
最大復原點存留期	以天為單位的最舊復原點存留期
最小復原點存留期	最近的復原點存留期，以天為單位

備份摘要/涵蓋報告

備份摘要/涵蓋報告列出有多少資源目前不受任何 AWS Backup 計劃保護。與您的 CDSM 討論適當的計畫，以盡可能提高涵蓋範圍，並降低資料遺失的風險。

欄位名稱	定義
客戶名稱	多個子客戶的情況的客戶名稱
Region	AWS 資源所在的區域
帳戶名稱	帳戶的名稱
AWS 帳戶 ID	AWS 帳戶的 ID
資源類型	資源的類型。資源受 AWS Backup (Aurora、DocumentDB、DynamoDB、EBS、EC2、EFS、FSx、RDS 和 S3) 支援
資源 ARN	資源的 ARN
資源 ID	資源的 ID
涵蓋範圍	指出資源是否涵蓋 (「COVERED」或「NOT_COVERED」)
資源數量	帳戶中支援的資源數量

欄位名稱	定義
perc_coverage	過去 30 天內執行備份的支援資源百分比。

AWS Config 控制合規報告

Control AWS Config Compliance 報告可讓您深入了解 AMS 帳戶的資源和 AWS Config 規則合規性。您可以依 Config Rule Severity 篩選報告，以排定最關鍵的問題清單的優先順序。下表列出此報告提供的資料：

欄位	描述
日期	報告日期
客戶名稱	客戶名稱
AWS 帳戶 ID	客戶的關聯 AWS 帳戶 ID
來源識別符	AWS Config 規則唯一來源識別符
規則描述	AWS Config 規則描述
規則類型	AWS Config 規則類型
合規旗標	AWS Config 規則合規狀態
資源類型	AWS 資源類型
資源名稱	AWS 資源名稱
嚴重性	AMS 為 AWS Config 規則定義的預設建議嚴重性
修復類別	AWS Config 規則的相關修補回應類別
修復描述	解釋的修補動作可讓 AWS Config 規則合規
客戶動作	使 AWS Config 規則合規所需的客戶動作
Delta 指標報告	指定 2 個日期之間規則合規的變更

AMS Config 規則回應組態報告

AMS Config 規則回應組態報告可讓您深入了解目前如何將 Accelerate 設定為回應不合規的 AMS 組態規則。如需如何變更 AMS 組態規則回應的詳細資訊，請參閱 AMS Accelerate Customized 調查結果回應。

此報告只會顯示您已變更的組態，並排除 AMS Config 規則程式庫中列出的 AMS 預設組態。報告提供 AMS 帳戶的資源和 AMS 組態規則回應組態資料，包括下列項目：

- 您變更 AMS 組態規則預設回應 AWS 的帳戶清單。
- 您已關聯 AMS 組態規則回應的標籤清單。
- 每個規則、帳戶和標籤的回應組態清單。
- 您已變更 AMS 組態規則預設回應的資源清單。

最新回應組態報告

欄位	描述
日期	產生報告的日期
客戶名稱	客戶名稱
AWS 帳戶 ID	與組態相關聯的 AWS 帳戶 ID
帳戶名稱	AWS 帳戶層級資源群組的帳戶名稱
問題清單類型	已識別的問題清單類型。在這種情況下， AWS Config
來源識別符	AWS Config 規則唯一來源識別符
資源群組 ID	與回應組態相關聯的資源群組 ID
已設定的回應動作	AMS 觸發的動作類型
關聯的 SSM Runbook	將執行的修復 Runbook，如果有的話
資源群組類型	這可以是帳戶或標籤

具有 Config 規則自訂預設回應的資源

欄位名稱	定義
客戶名稱	客戶名稱
日期	產生報告的日期
AWS 帳戶名稱	AWS 帳戶名稱
帳戶 ID	關聯 AWS 帳戶 ID
AMS Config 規則	針對資源並套用組態的 AMS 組態規則
資源 ID	AMS 組態規則目標客戶帳戶中的資源 ID
資源區域	套用組態 AWS 的區域
資源類型	AWS 資源類型
資源群組 ID	與回應組態相關聯的資源群組 ID
資源 AMS 旗標	如果 AWS 資源是由 AMS 部署，則此欄位會設定為 `True`
觸發類型	為資源設定的回應類型
合規旗標	AMS 組態規則合規狀態

防止和監控熱門發言者報告的事件

可用的報告

- 已防止的事件報告
- 監控熱門發言者報告

已防止的事件報告

Incidents Prevented 報告會列出自動修復的 Amazon CloudWatch 警示，以防止可能發生的事件。若要進一步了解，請參閱自動修復。下表列出此報告中包含的資訊：

欄位名稱	定義
execution_start_time_utc	執行自動化的日期
customer_name	帳戶客戶名稱
account_name	帳戶的名稱
AwsAccountId	AWS 帳戶的 ID
document_name	執行的 SSM 文件或自動化名稱
duration_in_minutes	自動化的長度，以分鐘為單位
Region	AWS 資源所在的區域
automation_execution_id	執行的 ID
automation_execution_status	執行的狀態

監控熱門發言者報告

監控熱門發言者報告會顯示在特定期間內產生的 Amazon CloudWatch 警示數量，並提供產生最多警示的資源視覺化效果。此報告可協助您識別產生最高數量提醒的資源。這些資源可能是執行根本原因分析以修復問題或修改警示閾值的候選者，以防止沒有實際問題時不必要的觸發。下表列出此報告中包含的資訊：

欄位名稱	定義
客戶名稱	客戶名稱
AccountId	AWS 帳戶的 ID
警示類別	觸發的提醒類型
描述	提醒的描述
資源 ID	觸發提醒的資源 ID
資源名稱	觸發提醒的資源名稱

欄位名稱	定義
Region	AWS資源所在的區域
事件狀態	警示產生之事件的最新狀態
第一次出現	第一次觸發提醒
最近出現	觸發提醒的最近時間
提醒計數	在第一次和最近出現之間產生的提醒數量

帳單費用詳細資訊報告

AWS Managed Services (AMS) 帳單費用詳細資訊報告提供連結帳戶和個別 AWS 服務的 AMS 帳單費用詳細資訊，包括：

- AMS 服務層級費用、提升百分比、帳戶層級 AMS 服務方案和 AMS 費用。
- 連結帳戶和 AWS 使用費

欄位名稱	定義
帳單月份	計費服務的月份和年份
付款人帳戶 ID	識別將負責支付 AMS 費用之帳戶的 12 位數 ID
連結的帳戶 ID	識別使用產生費用之服務的 AMS 帳戶的 12 位數 ID
AWS 服務名稱	使用 AWS 的服務
AWS 費用	AWS 服務名稱中列出的 AWS 服務名稱 AWS 費用
定價計劃	與連結帳戶相關聯的定價計劃名稱
提升比例	根據 pricing_plan、SLA 和 AWS 服務的提升百分比（以小數 V.WXYZ 表示）

欄位名稱	定義
調整後 AWS 的費用	AWS 針對 AMS 調整的用量
提高的 AWS 費用	AMS； adjusted_aws_charges * uplift_percent 要收取的 AWS 費用百分比
執行個體 EC2 RDS 支出	EC2 和 RDS 執行個體上的支出
AMS 費用	產品的總 AMS 費用；uplifted_aws_charges + instance_ec2_rds_spend + uplifted_ris + uplifted_sp
按比例分配的最低費用	我們為了符合合約下限而收取的金額
最低費用	AMS 最低費用 （ 如適用 ）
連結的帳戶總 AMS 費用	linked_account 的所有費用總和
付款人帳戶 AMS 費用總計	付款人帳戶的所有費用總和

信任的修復程式報告

可用的報告

- 信任的修復程式修復摘要報告
- 信任的修復程式組態摘要報告
- Trusted Advisor 檢查摘要報告

信任的修復程式修復摘要報告

信任的修復程式修復狀態報告提供先前修復週期中發生的修復的相關資訊。預設週數為 1。若要自訂報告，請根據您的修復排程指定週數。

欄位名稱	定義
日期	收集資料的日期。

欄位名稱	定義
帳戶 ID	資源所屬 AWS 的帳戶 ID
帳戶名稱	AWS 帳戶名稱
檢查類別	AWS Trusted Advisor 檢查類別
檢查名稱	修復的 Trusted Advisor 檢查名稱
檢查 ID	修復檢查的 ID Trusted Advisor
執行模式	針對特定 Trusted Advisor 檢查設定的執行模式
OpsItem ID	Trusted Advisor 為修復而建立的 OpsItem ID
OpsItem 狀態	報告 Trusted Advisor 時由 建立的 OpsItem 狀態
資源 ID	為修復而建立之資源的 ARN

信任的修復程式組態摘要報告

Trusted Remediator Configuration Summary 報告提供每個 Trusted Advisor 檢查目前 Trusted Remediator Remediation 組態的相關資訊。

欄位名稱	定義
日期	收集資料的日期。
帳戶 ID	套用組態 AWS 的帳戶 ID
帳戶名稱	AWS 帳戶名稱
檢查類別	AWS Trusted Advisor 檢查類別
檢查名稱	套用組態的修復 Trusted Advisor 檢查名稱
檢查 ID	套用組態的修復 Trusted Advisor 檢查 ID
執行模式	針對特定 Trusted Advisor 檢查設定的執行模式

欄位名稱	定義
覆寫至自動化	如果已設定標籤模式，將執行模式覆寫為自動化
覆寫為手動	如果已設定標籤模式，將執行模式覆寫為手動

Trusted Advisor 檢查摘要報告

Trusted Advisor 檢查摘要報告提供目前 Trusted Advisor 檢查的相關資訊。此報告會在每週修補排程之後收集資料。預設週數為 1。若要自訂報告，請根據您的修復週期指定週數。

欄位名稱	定義
日期	收集資料的日期。
帳戶 ID	套用組態 AWS 的帳戶 ID
客戶名稱	AWS 帳戶名稱
檢查類別	AWS Trusted Advisor 檢查類別
檢查名稱	套用組態的修復 Trusted Advisor 檢查名稱
檢查 ID	套用組態的修復 Trusted Advisor 檢查 ID
狀態	檢查的提醒狀態。可能的狀態為正常（綠色）、警告（黃色）、錯誤（紅色）或無法使用
資源已標記	由 Trusted Advisor 檢查標記（列出） AWS 的資源數量。
忽略的資源	由於 Trusted Advisor 您將其標示為隱藏而忽略 AWS 的資源數量。
處於嚴重狀態的資源	處於嚴重狀態的資源數量
處於警告狀態的資源	處於警告狀態的資源數量

自助式報告

AWS Managed Services (AMS) 自助式報告 (SSR) 是一項功能，可從各種原生 AWS 服務收集資料，並提供主要 AMS 產品報告存取權。SSR 提供可用來支援操作、組態管理、資產管理、安全管理和合規的資訊。

使用 SSR 從 AMS 主控台存取報告，並透過 Amazon S3 儲存貯體 （每個帳戶一個儲存貯體） 報告資料集。您可以將資料插入您最愛的商業智慧 (BI) 工具，以根據您的獨特需求自訂報告。AMS 會在您的主要 AWS 區域中建立此 S3 儲存貯體 (S3 儲存貯體名稱： (ams-reporting-data-a<Account_ID>)，並從 us-east-1 區域中託管的 AMS 控制平面共用資料。

若要允許使用者在 AMS 主控台中檢視 AMS Accelerate 報告，您必須在 AWS Identity and Access Management (IAM) 中授予明確許可來執行這些動作。如需 IAM 政策範例，請參閱使用 AMS 功能的許可。

> **Important**
>
> 搭配 使用自訂金鑰 AWS Glue
> 若要使用客戶受管 KMS 金鑰加密 AWS Glue 中繼資料，您必須執行下列額外步驟，以允許 AMS 從帳戶彙總資料：
>
> 1. 在 https：//https://console.aws.amazon.com/kms 開啟 AWS Key Management Service 主控台，然後選擇客戶受管金鑰。
> 2. 選取您計劃用來加密 AWS Glue 中繼資料的金鑰 ID。
> 3. 選擇別名索引標籤，然後選擇建立別名。
> 4. 在文字方塊中，輸入 AmsReportingFlywheelCustomKey，然後選擇建立別名。

主題

- 資料保留政策
- 從 SSR 離職

內部 API 操作

如果您監控 API 操作，您可能會看到對下列僅限內部操作的呼叫：

- `GetDashboardUrl`
- `ListReportsV2`

內部 API 操作：GetDashboardUrl

當 AMS 主控台調用時，此操作會出現在系統日誌中。它沒有其他使用案例。它不適用於您的直接使用。

傳回對應報告的內嵌儀表板 URL。此操作接受 `dashboardName`傳回的 `ListReports`。

請求語法

```
HTTP/1.1 200
Content-type: application/json
{
    "dashboardName": "string"
}
```

請求元素

`dashboardName`：請求 URL 的 QuickSight 儀表板名稱。儀表板名稱會在 ListReportsV2 中傳回。

類型：字串

回應語法

```
HTTP/1.1 200
Content-type: application/json
{
  "url": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。服務會傳回下列 JSON 格式的資料。

`url`：傳回所請求 的 QuickSight URL`dashboardName`。

類型：字串

錯誤

如需所有動作常見錯誤的相關資訊，請參閱常見錯誤。

`BadRequestException`:

提交的請求無效。例如，如果輸入不完整或不正確。如需詳細資訊，請參閱隨附的錯誤訊息。

HTTP 狀態碼：400

`NotFoundException`:

找不到請求的資源。請確定請求 URI 正確。

HTTP 狀態碼：404

`TooManyRequestsException`:

請求已達到其限流限制。在指定的時段後重試。

HTTP 狀態碼：429

`UnauthorizedException`:

請求遭拒，因為發起人沒有足夠的許可。

HTTP 狀態碼：401

內部 API 操作：ListReportsV2

當 AMS 主控台調用時，此 API 會出現在系統日誌中。它沒有其他使用案例。它不適用於您的直接使用。

傳回指定帳戶可用的操作報告清單。

請求語法

請求沒有請求內文。

回應語法

```
HTTP/1.1 200
Content-type: application/json
{
  "reportsList": [
    {
        "dashboard": "string",
        "lastUpdatedTime": "string",
    }
  ],
  "reportsType": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。服務會傳回下列 JSON 格式的資料。

reportsList：可用操作報告的清單。

類型：儀表板物件陣列

reportsType：指出是否跨多個帳戶彙總報告。

類型：字串

錯誤

如需所有動作常見錯誤的相關資訊，請參閱常見錯誤。

BadRequestException:

提交的請求無效。例如，輸入不完整或不正確。如需詳細資訊，請參閱隨附的錯誤訊息。

HTTP 狀態碼：400

NotFoundException:

找不到請求的資源。請確定請求 URI 正確。

HTTP 狀態碼：404

TooManyRequestsException:

請求已達到其限流限制。在指定的時段後重試。

HTTP 狀態碼：429

`UnauthorizedException`:

請求遭拒，因為發起人沒有足夠的許可。

HTTP 狀態碼：401

修補程式報告 （每日）

可用的報告

- AMS 修補的執行個體詳細資訊摘要
- 修補程式詳細資訊
- 遺漏修補程式的執行個體

AMS 修補的執行個體詳細資訊摘要

這是資訊報告，可協助識別加入 AMS 修補的所有執行個體、帳戶狀態、執行個體詳細資訊、維護時段涵蓋範圍、維護時段執行時間、堆疊詳細資訊和平台類型。

此資料集提供：

- 帳戶的生產和非生產執行個體上的資料。生產和非生產階段衍生自帳戶名稱，而非執行個體標籤。
- 依平台類型分佈執行個體的資料。當 AWS Systems Manager (SSM) 無法取得平台資訊時，就會發生「不適用」平台類型。
- 執行個體狀態分佈的資料、執行、停止或終止的執行個體數量。

主控台欄位名稱	資料集欄位名稱	定義
存取限制	access_restrictions	限制存取的區域
帳戶 ID	aws_account_id	AWS 執行個體 ID 所屬的帳戶 ID
管理員帳戶 ID	aws_admin_account_id	由您啟用的信任 AWS Organizations 帳戶。
帳戶名稱	account_name	AWS 帳戶名稱
帳戶狀態	account_status	AMS 帳戶狀態

主控台欄位名稱	資料集欄位名稱	定義
	account_sla	AMS 帳戶服務承諾
帳戶類型	malz_role	MALZ 角色
Auto Scaling 群組名稱	instance_asg_name	包含執行個體的 Auto Scaling 群組 (ASG) 名稱
執行個體 ID	instance_id	EC2 執行個體的 ID
執行個體名稱	instance_name	EC2 執行個體的名稱
執行個體修補程式群組	instance_patch_group	用來將執行個體分組並套用相同維護時段的修補程式群組名稱
執行個體修補程式群組類型	instance_patch_group_type	修補程式群組類型
執行個體平台類型	instance_platform_type	作業系統 (OS) 類型
執行個體平台名稱	instance_platform_name	作業系統 (OS) 名稱
執行個體狀態	instance_state	EC2 執行個體生命週期內的狀態
執行個體標籤	ec2_tags	與 Amazon EC2 執行個體 ID 相關聯的標籤
登陸區域	malz_flag	MALZ 相關帳戶的旗標
維護時段涵蓋範圍	mw_covered_flag	如果執行個體至少有一個已啟用且具有未來執行日期的維護時段，則視為已涵蓋，否則未涵蓋
維護時段執行日期時間	earliest_window_execution_time	下次預期執行維護時段時

主控台欄位名稱	資料集欄位名稱	定義
維護時段執行日期時間	earliest_window_execution_time	下次預期執行維護時段時
生產帳戶	prod_account	AMS prod、非prod 帳戶的識別符，取決於帳戶名稱是否包含值 'PROD'、'NONPROD'。
報告日期時間	dataset_datetime	產生報告的日期和時間。
堆疊名稱	instance_stack_name	包含執行個體的堆疊名稱
堆疊類型	instance_stack_type	AMS 堆疊（客戶帳戶中的 AMS 基礎設施）或客戶堆疊（支援客戶應用程式的 AMS 受管基礎設施）

修補程式詳細資訊

此報告提供各種執行個體的修補程式詳細資訊和維護時段涵蓋範圍。

此報告提供：

- 修補程式群組及其類型上的資料。
- 維護時段、持續時間、截止日期、維護時段執行的未來日期（排程）和在每個時段中受影響的執行個體上的資料。
- 帳戶下所有作業系統的資料，以及安裝作業系統的執行個體數量。

欄位名稱	資料集欄位名稱	定義
報告日期時間	dataset_datetime	產生報告的日期和時間。
帳戶 ID	aws_account_id	AWS 執行個體 ID 所屬的帳戶 ID
帳戶名稱	account_name	AWS 帳戶名稱

欄位名稱	資料集欄位名稱	定義
帳戶狀態	account_status	AMS 帳戶狀態
合規 - 關鍵	compliance_critical	嚴重性為「關鍵」的合規修補程式計數
合規 - 高	compliance_high	嚴重性為「高」的合規修補程式計數
合規 - 中	compliant_medium	嚴重性為 "medium" 的合規修補程式計數
合規 - 低	compliance_low	嚴重性為「低」的合規修補程式計數
合規 - 資訊性	compliant_informational	具有「資訊」嚴重性的合規修補程式計數
合規 - 未指定	compliant_unspecified	嚴重性為「未指定」的合規修補程式計數
合規 - 總計	compliant_total	合規修補程式計數 （ 所有嚴重性 ）
執行個體 ID	instance_id	EC2 執行個體的 ID
執行個體名稱	instance_name	EC2 執行個體的名稱
	account_sla	AMS 帳戶服務方案
執行個體平台類型	instance_platform_type	作業系統 (OS) 類型
執行個體平台名稱	instance_platform_name	作業系統 (OS) 名稱

欄位名稱	資料集欄位名稱	定義
執行個體修補程式群組類型	instance_patch_group_type	DEFAULT：具有預設維護時段的預設修補程式群組，由執行個體上的 AMSDefaultPatchGroup：True 標籤決定 CUSTOMER：客戶建立的修補程式群組 NOT_ASSIGNED：未指派修補程式群組
執行個體修補程式群組	instance_patch_group	用來將執行個體分組並套用相同維護時段的修補程式群組名稱
執行個體狀態	instance_state	EC2 執行個體生命週期內的狀態
執行個體標籤	ec2_tags	與 Amazon EC2 執行個體 ID 相關聯的標籤
上次執行維護時段	last_execution_window	執行維護時段的最新時間
維護時段 ID	window_id	維護時段 ID
維護時段狀態	window_state	維護時段狀態
維護時段類型	window_type	維護時段類型
維護時段下次執行日期時間	window_next execution_time	下次預期執行維護時段時
維護時段持續時間（小時）	window_duration	維護時段的持續時間，以小時為單位

欄位名稱	資料集欄位名稱	定義
維護時段涵蓋範圍	mw_covered_flag	如果執行個體至少有一個已啟用且具有未來執行日期的維護時段，則視為已涵蓋，否則未涵蓋
不合規 - 關鍵	noncompliant_critical	嚴重性為「關鍵」的不合規修補程式計數
不合規 - 高	noncompliant_high	嚴重性為「高」的不合規修補程式計數
不合規 - 中	noncompliant_medium	嚴重性為 "medium" 的不合規修補程式計數
不合規 - 低	noncompliant_low	嚴重性為「低」的不合規修補程式計數
不合規 - 資訊性	不合規 _資訊	具有「資訊」嚴重性的不合規修補程式計數
不合規 - 未指定	不合規 _未指定	嚴重性為「未指定」的不合規修補程式計數
不合規 - 總計	noncompliant_total	不合規修補程式的計數（所有嚴重性）
修補程式基準 ID	patch_baseline_id	目前連接至執行個體的修補程式基準
修補程式狀態	patch_status	整體修補程式合規狀態。如果至少有一個缺少的修補程式，則執行個體會被視為不合規，否則為合規。

欄位名稱	資料集欄位名稱	定義
生產帳戶	prod_account	AMS prod、非prod 帳戶的識別符，取決於帳戶名稱是否包含值 'PROD'、'NONPROD'。
堆疊類型	instance_stack_type	AMS 堆疊（客戶帳戶中的 AMS 基礎設施）或客戶堆疊（支援客戶應用程式的 AMS 受管基礎設施）
	window_next_exec_yyyy	window_next_execution_time 的年份部分
	window_next_exec_mm	window_next_execution_time 的月份部分
	window_next_exec_D	window_next_execution_time 的天數部分
	window_next _exec_HHMI	window_next_execution_time 的小時：分鐘部分

遺漏修補程式的執行個體

此報告提供上次維護時段執行期間遺漏修補程式之執行個體的詳細資訊。

此報告提供：

- 修補程式 ID 層級缺少修補程式的資料。
- 至少有一個遺失修補程式和屬性的所有執行個體上的資料，例如修補程式嚴重性、未修補的天數、範圍和修補程式的發行日期。

欄位名稱	資料集欄位名稱	定義
報告日期時間	dataset_datetime	產生報告的日期和時間

欄位名稱	資料集欄位名稱	定義
帳戶 ID	aws_account_id	AWS 執行個體 ID 所屬的帳戶 ID
帳戶名稱	account_name	AWS 帳戶名稱
客戶名稱父系	customer_name_parent	
客戶名稱	customer_name	
生產帳戶	prod_account	AMS prod 或非 prod 帳戶的識別符，取決於帳戶名稱是否包含值 'PROD' 或 'NONPROD'。
帳戶狀態	account_status	AMS 帳戶狀態
帳戶類型	account_type	
	account_sla	AMS 帳戶服務方案
執行個體 ID	instance_id	EC2 執行個體的 ID
執行個體名稱	instance_name	EC2 執行個體的名稱
執行個體平台類型	instance_platform_type	作業系統 (OS) 類型
執行個體狀態	instance_state	EC2 執行個體生命週期內的狀態
執行個體標籤	ec2_tags	與 Amazon EC2 執行個體 ID 相關聯的標籤
修補程式 ID	patch_id	已發行修補程式的 ID
修補程式嚴重性	patch_sev	每個發佈者的修補程式嚴重性
修補程式分類	patch_class	每個修補程式發佈者的修補程式分類

欄位名稱	資料集欄位名稱	定義
修補程式發行日期時間 (UTC)	release_dt_utc	每個發佈者的修補程式發行日期
修補程式安裝狀態	install_state	每個 SSM 在執行個體上安裝修補程式的狀態
未修補的天數	days_unpatched	自上次 SSM 掃描以來執行個體未修補的天數
未修補範圍的天數	days_unpatched_bucket	未修補天數的儲存貯體

備份報告（每日）

備份報告涵蓋主要和次要（如適用）區域。它涵蓋備份（成功/失敗）的狀態，以及所拍攝快照上的資料。

此報告提供：

- 備份狀態
- 拍攝的快照數量
- 復原點
- 備份計畫和保存庫資訊

欄位名稱	資料集欄位名稱	定義
報告日期時間	dataset_datetime	產生報告的日期和時間。
帳戶 ID	aws_account_id	執行個體 ID 所屬的 AWS 帳戶 ID
管理員帳戶 ID	aws_admin_account_id	由您啟用的信任 AWS Organizations 帳戶。
帳戶名稱	account_name	AWS 帳戶名稱

欄位名稱	資料集欄位名稱	定義
帳戶 SLA	account_sla	AMS 帳戶服務承諾
	malz_flag	MALZ 相關帳戶的旗標
	malz_role	MALZ 角色
	access_restrictions	限制存取的區域
備份快照排程的開始日期時間	start_by_dt_utc	快照排程開始的時間戳記
備份快照實際開始日期時間	create_dt_utc	快照實際開始時的時間戳記
備份快照完成日期時間	completion_dt_utc	快照完成時的時間戳記
備份快照過期日期時間	expiration_dt_utc	快照過期時的時間戳記
備份任務狀態	backup_job_status	快照的狀態
備份類型	backup_type	備份類型
備份任務 ID	backup_job_id	備份任務的唯一識別符
位元組中的備份大小	backup_size_in_bytes	以位元組為單位的備份大小
備份計畫 ARN	backup_plan_arn	備份計畫 ARN
備份計畫 ID	backup_plan_id	備份計畫唯一識別符
備份計劃名稱	backup_plan_name	備份計畫名稱
備份計畫版本	backup_plan_version	備份計畫版本
備份規則 ID	backup_rule_id	備份規則 ID
備份保存庫 ARN	backup_vault_arn	備份保存庫 ARN
備份文件庫名稱	backup_vault_name	備份保存庫名稱
IAM 角色 ARN	iam_role_arn	IAM 角色 ARN

欄位名稱	資料集欄位名稱	定義
執行個體 ID	instance_id	唯一執行個體 ID
執行個體狀態	instance_state	執行個體狀態
執行個體標籤	ec2_tags	與 EC2 執行個體 ID 相關聯的標籤
資源 ARN	resource_arn	Amazon 資源名稱
資源 ID	resource_id	唯一資源識別符
資源區域	resource_region	資源的主要（和次要，如適用）區域。
資源類型	resource_type	資源的類型
復原點 ARN	recovery_point_arn	復原點的 ARN
復原點 ID	recovery_point_id	復原點的唯一識別符
復原點狀態	recovery_point_status	復原點狀態
在 天後刪除復原點	recovery_point_delete_after_days	天之後的復原點刪除
復原點會在 天後移至冷儲存	recovery_point_move_to_cold_storage_after_days	將備份快照移至冷儲存的完成日期後天數
復原點加密狀態	recovery_point_is_encrypted	復原點加密狀態
復原點加密金鑰 ARN	recovery_point_encryption_key_arn	復原點加密金鑰 ARN
堆疊 ID	stack_id	Cloudformation 堆疊唯一識別符
堆疊名稱	stack_name	堆疊名稱

欄位名稱	資料集欄位名稱	定義
標籤：AMS 預設修補程式群組	tag_ams_default_patch_group	標籤值：AMS 預設修補程式群組
標籤：應用程式 ID	tag_app_id	標籤值：應用程式 ID
標籤：應用程式名稱	tag_app_name	標籤值：應用程式名稱
標籤：備份	tag_backup	標籤值：備份
標籤：合規架構	tag_compliance_framework	標籤值：合規架構
標籤：成本中心	tag_cost_center	標籤值：成本中心
標籤：客戶	tag_customer	標籤值：客戶
標籤：資料分類	tag_data_classification	標籤值：資料分類
標籤：環境類型	tag_environment_type	標籤值：環境類型
標籤：營運時數	tag_hours_of_operation	標籤值：操作時數
標籤：擁有者團隊	tag_owner_team	標籤值：擁有者團隊
標籤：擁有者團隊電子郵件	tag_owner_team_email	標籤值：擁有者團隊電子郵件
標籤：修補程式群組	tag_patch_group	標籤值：修補程式群組
標籤：支援優先順序	tag_support_priority	標籤值：支援優先順序
磁碟區狀態	volume_state	磁碟區狀態

事件報告（每週）

此報告提供事件的彙總清單及其優先順序、嚴重性和最新狀態，包括：

- 分類為受管帳戶事件的支援案例資料
- 視覺化受管帳戶的事件指標所需的事件資訊
- 每個事件的事件類別和修復狀態資料

視覺化和資料都可以用於每週事件報告。

- 您可以透過 帳戶中的 AMS 主控台，透過報告頁面存取視覺化。
- 具有下列結構描述的資料集，可透過 受管帳戶中的 S3 儲存貯體存取。
- 使用提供的日期欄位，根據事件建立或解決的月、季、週和/或日來篩選事件。

欄位名稱	資料集欄位名稱	定義
報告日期時間	dataset_datetime	產生報告的日期和時間。
帳戶 ID	aws_account_id	AWS 事件所屬的帳戶 ID。
管理員帳戶 ID	aws_admin_account_id	由您啟用的信任 AWS Organizations 帳戶。
帳戶名稱	account_name	AWS 帳戶名稱。
案例 ID	case_id	事件的 ID。
建立月份	created_month	事件建立的月份。
優先順序	priority	事件的優先順序。
嚴重性	severity	事件的嚴重性。
狀態	status	事件的狀態。
類別	yuma_category	事件的類別。
建立日期	create_day	事件以 YYYY-MM-DD 格式建立的日期。
建立的週	created_wk	事件以 YYYY-WW 格式建立的一週。週日至週六視為一週的開始和結束。週是從 01 到 52。第 01 週一律是包含一年第一天的一週。例如，2023-12-31 和 2024-01-01 位於 2024 年 1 週。

欄位名稱	資料集欄位名稱	定義
建立的季度	created_qtr	事件以 YYYY-Q 格式建立的季度。01/01 至 03/31 定義為 Q1，以此類推。
已解決日期	resolved_day	事件以 YYYY-MM-DD 格式解決的日期。
已解決的週	resolved_wk	事件以 YYYY-WW 格式解決的一週。週日至週六視為一週的開始和結束。週是從 01 到 52。第 01 週一律是包含一年第一天的一週。對於 exmaple，2023-12-31 和 2024-01-01 位於 2024 年 1 週。
解析月份	resolved_month	事件以 YYYY-MM 格式解決的月份。
已解決的季度	resolved_qtr	事件以 YYYY-Q 格式解決的季度。01/01 至 03/31 定義為 Q1，以此類推。
建立的分組規則	grouping_rule	套用至事件的分組規則。"no_grouping" 或 "instance_grouping"。
執行個體 IDs	instance_ids	與事件相關聯的執行個體。
提醒數量	number_of_alerts	與該事件相關聯的提醒數量。如果您已啟用分組，則此數字可以大於 1。如果您沒有啟用分組，則一律為 1。
建立時間	created_at	建立事件時的時間戳記。

欄位名稱	資料集欄位名稱	定義
警示 ARNs	alarm_arns	與您的事件相關聯之警示的 Amazon Resource Name ("arn")。
相關警示	related_alarms	與事件關聯之所有警示的人類可讀取名稱。

帳單報告（每月）

帳單費用詳細資訊

此報告提供連結帳戶和個別 AWS 服務之 AMS 帳單費用的詳細資訊。

此報告提供：

- AMS 服務層級費用、提升百分比、帳戶層級 AMS 服務方案和 AMS 費用的資料。
- 連結帳戶和 AWS 使用費的資料。

> **Important**
>
> 每月帳單報告僅適用於您的管理付款人帳戶 (MPA) 或您定義的費用帳戶。這些是傳送 AMS 每月帳單的帳戶。如果您找不到這些帳戶，請聯絡您的 Cloud Service Delivery Manager (CSDM) 尋求協助。

欄位名稱	資料集欄位名稱	定義
帳單日期	date	計費服務的月份和年份
付款人帳戶 ID	payer_account_id	識別負責支付 AMS 費用之帳戶的 12 位數 ID
連結的帳戶 ID	linked_account_id	識別使用產生擴展之服務的 AMS 帳戶的 12 位數 ID

欄位名稱	資料集欄位名稱	定義
AWS 服務名稱	product_name	使用 AWS 的服務
AWS 費用	aws_charges	AWS 服務名稱中 AWS 服務名稱 AWS 的費用
定價計劃	pricing_plan	與連結帳戶相關聯的定價計劃
AMS 服務群組	tier_uplifting_groups	決定提升百分比的 AMS 服務群組程式碼
提升比例	uplift_percent	以 pricing_plan、SLA AWS 和服務為基礎的提升百分比（以小數 V.WXYZ 表示）
調整後 AWS 的費用	adjusted_aws_usage	AWS 針對 AMS 調整的用量
調高 AWS 費用	uplifted_aws_charges	AMS； adjusted_aws_charges * uplift_percent AWS 要支付的費用百分比
執行個體 EC2 RDS 支出	instance_ec2_rds_spend	EC2 和 RDS 執行個體上的支出
預留執行個體費用	ris_charges	預留執行個體費用
提高預留執行個體費用	uplifted_ris	AMS；ris_charges * uplift_percent 要收取的預留執行個體費用百分比
Savings Plan 費用	sp_charges	SavingsPlan 使用費
提高的 Savings Plan 費用	uplifted_sp	需支付 AMS； sp_charges * uplift_percent 的節省計劃費用百分比

欄位名稱	資料集欄位名稱	定義
AMS 費用	ams_charges	產品的總 ams 費用；uplifted_aws_charges + instance_ec2_rds_spend + uplifted_ris + uplifted_sp
按比例分配的最低費用	prorated_minimum	我們為了符合合約下限而收取的金額
連結的帳戶總 AMS 費用	linked_account_total ams_charges	linked_account 的所有費用總和
付款人帳戶 AMS 費用總計	payer_account_total ams_charges	付款人帳戶的所有費用總和
最低費用	minimum_fees	AMS 最低費用 （如適用）
預留執行個體和 Savings Plan 折扣	adj_ri_sp_charges	要套用至 RI/SP 費用的 RI/SP 折扣 （適用於特定情況）

彙總報告

彙總自助式報告 (SSR) 可讓您檢視組織層級、跨帳戶彙總的現有自助式報告。這可讓您查看 AMS 管理下的所有帳戶的關鍵操作指標，例如修補程式合規、備份涵蓋範圍和事件 AWS Organizations。

彙總 SSR 可在 AWS Managed Services 提供的所有商業 AWS 區域 環境中使用。如需可用區域的完整清單，請參閱區域資料表。

啟用彙總報告

您必須從 AWS Organizations 管理帳戶管理彙總的 SSR。管理帳戶是您用來建立組織的 AWS 帳戶。

若要為已加入 AMS 的 AWS Organizations 管理帳戶啟用彙總 SSR，請存取您的 AMS 主控台並導覽至報告。選取top-right-hand的組織存取，開啟 AWS Managed Services主控台：組織檢視窗格。在此窗格中，您可以管理彙總的 SSR 功能。

AWS Organizations 未加入 AMS 的管理帳戶無法存取 AMS 主控台。若要為未加入 AMS 的 AWS Organizations 管理帳戶啟用彙總 SSR，請先向您的 進行身分驗證 AWS 帳戶，然後導覽至AWS 主控台並搜尋 Managed Services。這會開啟 AMS 行銷頁面。在此頁面上，選取導覽列中的組織存取連結以開啟 AWS Managed Services 主控台：Organization View，您可以在其中管理彙總 SSR 功能。

第一次存取 AWS Managed Services主控台：Organization View 時，請完成下列步驟：

1. 如果您尚未設定 AWS Organizations，請從主控台選擇啟用 AWS Organizations。如需設定的其他資訊 AWS Organizations，請參閱AWS Organizations 《 使用者指南》。如果您已使用 ，可以略過此步驟 AWS Organizations。
2. 若要啟用彙總自助式報告服務，請選取在主控台上啟用受信任存取。
3. （選用）註冊委派管理員，以擁有組織檢視的讀取存取權。

以委派管理員身分檢視彙總報告

委派管理員是您選擇擁有彙總報告讀取存取權的帳戶。委派管理員必須是加入 AMS 的帳戶，並且是唯一具有彙總報告讀取存取權的帳戶。

若要選擇委派管理員，請在 AWS Managed Services主控台：組織檢視的步驟 3 中輸入帳戶 ID。您一次只能註冊一個委派管理員帳戶。請注意，委派管理員帳戶必須是 AMS 受管帳戶。

若要更新委派管理員帳戶，請導覽至 AWS Managed Services主控台：組織檢視，然後選取移除委派管理員。主控台會提示您插入新的帳戶 ID，以註冊為委派管理員。

讀取彙總報告

如果您未註冊委派管理員，且您的 AWS Organizations 管理帳戶已加入 AMS，則 AWS Organizations 管理帳戶預設會取得彙總報告的讀取存取權。如果 AWS Organizations 管理帳戶不是由 AMS 管理，則您必須選擇委派管理員帳戶，才能讀取彙總報告。

在任何時候，只有加入 AMS 的單一帳戶才能讀取彙總報告，無論是 AWS Organizations 管理帳戶或註冊的委派管理員。組織內的所有其他成員帳戶 （並加入 AMS) 仍然只能存取每個個別帳戶的單一帳戶報告。

啟用彙總 SSR 後，導覽至您的報告。所有現有的自助式報告都會列在本節中，藍色標籤表示它們已彙總。請注意，您必須從您選擇的帳戶存取 AMS 主控台，才能讀取彙總報告。這是 AWS Organizations 管理帳戶或委派管理員帳戶。

啟用彙總 SSR 之後，即可從下一個報告週期開始取得彙總報告。

停用彙總報告

若要停用彙總 SSR，請開啟 AWS Managed Services主控台：組織檢視。選取停用受信任存取。停用彙總 SSR 的受信任存取後，您的 AMS 自助式服務報告會在組織層級跨帳戶彙總。另請注意，停用會從下一個報告週期開始生效。

停用彙總 SSR 之後，在 AMS 主控台中的報告顯示為單一帳戶報告之前會有等待。發生此延遲是因為功能停用會從下一個報告週期開始生效。

AMS 自助式報告儀表板

AMS 自助式報告提供兩個儀表板： Resource Tagger 儀表板和 安全組態規則儀表板。

Resource Tagger 儀表板

AMS Resource Tagger Dashboard 提供 Resource Tagger 支援之資源的詳細資訊，以及 Resource Tagger 設定為套用至這些資源之標籤的目前狀態。

依資源類型劃分的資源交錯範圍

此資料集包含資源清單，其中包含由 Resource Tagger 管理的標籤。

依資源類型的資源涵蓋範圍視覺化為四個折線圖，描述下列指標：

- 資源計數：依資源類型區分，區域中的資源總數。
- 資源遺失受管標籤： 區域中需要受管標籤但未由 Resource Tagger 標記的 資源總數，依資源類型排序。
- 未受管資源： 區域中資源的總數，依資源類型，這些資源類型未由 Resource Tagger 套用受管標籤。這通常表示這些資源不符合任何 Resource Tagger 組態，或明確地從組態中排除。
- 受管資源：與未受管資源指標 (資源計數 - 未受管資源） 相反。

下表列出此報告所提供的資料。

欄位名稱	資料集欄位名稱	定義
報告日期時間	dataset_datetime	產生報告的日期和時間 (UTC 時間）
AWS 帳戶 ID	aws_account_id	AWS 帳戶 ID

欄位名稱	資料集欄位名稱	定義
管理員帳戶 ID	aws_admin_account_id	由您啟用的信任 AWS Organizations 帳戶。
Region	region	AWS 區域
資源類型	resource_type	此欄位可識別資源的類型。僅包含 Resource Tagger 支援的資源類型。
資源計數	resource_count	在此區域中部署的資源數量（指定資源類型的）。
ResourcesMissingManagedTags	resource_missing_managed_tags_count	根據組態描述檔，需要受管標籤但尚未由 Resource Tagger 標記的資源（指定資源類型的）數量。
UnmanagedResources	unmanaged_resource_count	資源數量（指定資源類型的），沒有由 Resource Tagger 套用的受管標籤。一般而言，這些資源不符合任何 Resource Tagger 組態區塊，或明確地從組態區塊中排除。

資源 Tagger 組態規則合規

此資料集包含 中 AWS 區域依資源類型列出的資源清單，這些資源已套用特定組態描述檔。它被視覺化為折線圖。

下表列出此報告所提供的資料。

欄位名稱	資料集欄位名稱	定義
報告日期時間	dataset_datetime	產生報告的日期和時間 (UTC 時間)

欄位名稱	資料集欄位名稱	定義
AWS 帳戶 ID	aws_account_id	AWS 帳戶 ID
管理員帳戶 ID	aws_admin_account_id	由您啟用的信任 AWS Organizations 帳戶。
Region	region	AWS 區域
資源類型	resource_type	此欄位可識別資源的類型。僅包含 Resource Tagger 支援的資源類型。
組態設定檔 ID	configuration_profile_id	Resource Tagger 組態設定檔的 ID。組態設定檔用於定義用來標記資源的政策和規則。
MatchingResourceCount	resource_count	符合 Resource Tagger 組態設定檔 ID 的資源數量（指定資源類型的）。若要讓資源符合組態描述檔，必須啟用描述檔，且資源必須符合描述檔的規則。

Resource Tagger 不合規資源

此資料集包含單一 Resource Tagger 組態不合規的資源清單。此資料是資源合規的每日快照，顯示這些報告交付到客戶帳戶時客戶資源的狀態（沒有歷史檢視）。它被視覺化為樞紐分析表，由特定組態不合規的資源組成。

下表列出此報告所提供的資料。

欄位名稱	資料集欄位名稱	定義
報告日期時間	dataset_datetime	產生報告的日期和時間 (UTC 時間)
AWS 帳戶 ID	aws_account_id	AWS 帳戶 ID

欄位名稱	資料集欄位名稱	定義
管理員帳戶 ID	aws_admin_account_id	由您啟用的信任 AWS Organizations 帳戶。
Region	region	AWS 區域
資源類型	resource_type	此欄位可識別資源的類型。僅包含 Resource Tagger 支援的資源類型。
資源 ID	resource_id	Resource Tagger 支援之資源的唯一識別符。
涵蓋狀態	coverage_state	此欄位指出資源是否依 Resource Tagger 組態 ID 所設定進行標記。
組態設定檔 ID	configuration_profile_id	Resource Tagger 組態設定檔的 ID。組態設定檔用於定義用來標記資源的政策和規則。

安全組態規則儀表板

安全設定規則儀表板提供 AMS 帳戶資源和 AWS Config 規則合規性的深入檢視。您可以依規則嚴重性篩選報告，以排定最關鍵的問題清單的優先順序。下表列出此報告所提供的資料。

欄位名稱	資料集欄位名稱	定義
AWS 帳戶 ID	AWS 帳戶 ID	與相關資源繫結的帳戶 ID。
管理員帳戶 ID	aws_admin_account_id	由您啟用的信任 AWS Organizations 帳戶。
報告日期時間	報告日期	產生報告的日期和時間。
customer_name	客戶名稱	客戶名稱。
account_name	帳戶名稱	與帳戶 ID 相關聯的名稱

欄位名稱	資料集欄位名稱	定義
resource_id	資源 ID	資源的識別符。
resource_region	資源區域	AWS 區域 資源所在的 。
resource_type	資源類型	AWS 服務 或 資源類型。
resource_name	資源名稱	資源的名稱。
resource_ams_flag	資源 AMS 旗標	如果資源為 AMS 擁有，則此旗標設定為 TRUE。如果資源是客戶擁有，則此旗標設定為 FALSE。如果所有權不明，則此旗標會設為 UNKNOWN。
config_rule	Config 規則	組態規則不可自訂的名稱。
config_rule_description	組態規則描述	組態規則的描述。
source_identifier	來源識別符	受管組態規則的唯一識別符，而自訂組態規則沒有識別符。
compliance_flag	合規旗標	顯示資源是否符合組態規則。
rule_type	規則類型	指出規則是預先定義還是自訂建置。
exception_flag	例外狀況旗標	資源例外狀況旗標顯示對不合規資源接受的風險。如果資源的資源例外狀況旗標為 TRUE，則會豁免資源。如果例外狀況旗標為 NULL，則不會排除資源。
cal_dt	日期	規則的評估日期。
remediation_description	修復描述	如何修復規則合規的描述。

欄位名稱	資料集欄位名稱	定義
severity	嚴重性	組態規則嚴重性表示不合規的影響。
customer_action	客戶動作	修正 規則所需的動作。
建議	建議	組態規則檢查內容的描述。
remediation_category	修復類別	AMS 在此規則變得不合規時所採取的預設動作。

資料保留政策

在報告的期間之後，AMS SSR 具有每個報告的資料保留政策，資料會清除且不再可用。

報告名稱	資料保留 SSR 主控台	資料保留 SSR S3 儲存貯體
AMS 修補的執行個體詳細資訊摘要	2 個月	2 年
修補程式詳細資訊	2 個月	2 年
在維護時段執行期間遺漏修補程式的執行個體	2 個月	2 年
AMS 帳單費用詳細資訊	2 年	2 年
每日備份報告	1 個月	2 年
每週事件報告	2 個月	2 年
安全組態規則儀表板	3 個月	2 年
Resource Tagger 儀表板	1 年	2 年

從 SSR 離職

若要從 SSR 服務離職，請透過 AMS 主控台建立服務請求 (SR)。提交 SR 之後，AMS 操作工程師會協助您從 SSR 中離職。在 SR 中，提供您要離職的原因。

若要退出帳戶並執行資源清除，請透過 AMS 主控台建立 SR。提交 SR 之後，AMS 操作工程師會協助您刪除 SSR Amazon S3 儲存貯體。

如果您從 AMS 離職，您會自動從 AMS SSR 主控台離職。AMS 會自動停止傳送資料至您的帳戶。AMS 會在離職程序中刪除您的 SSR S3 儲存貯體。

AMS Accelerate 中的存取管理

存取管理是透過僅允許授權和驗證的存取來保護資源的方式。透過 AMS Accelerate，您需負責管理對 AWS 帳戶 及其基礎資源的存取，例如存取管理解決方案、存取政策和相關程序。為了協助您管理存取解決方案，AMS Accelerate 部署偵測常見 IAM 錯誤組態的 AWS Config 規則，然後傳遞修補通知。常見的 IAM 設定錯誤是根使用者具有存取金鑰。`iam-root-access-key-check` 組態規則會檢查根使用者存取金鑰是否可用且合規，或存取金鑰是否不存在。如需 AMS 部署的組態規則清單，請參閱 AMS AWS Config 規則程式庫。

主題

存取 Accelerate 主控台

當您使用 Accelerate 加入時，您會自動存取 Accelerate 主控台。您可以在 AWS 管理主控台中搜尋 Managed Services 來存取 主控台。Accelerate 主控台可讓您使用 Accelerate 對功能進行摘要檢視。此檢視包含顯示在儀表板和組態頁面上的個別元件。

使用 AMS 功能的許可

若要允許使用者讀取和設定 AMS Accelerate 功能，例如存取 AMS 主控台或設定備份，您必須授予其 IAM 角色執行這些動作的明確許可。下列 AWS CloudFormation 範本包含讀取和設定與 AMS 相關聯的服務所需的政策，讓您可以將它們指派給 IAM 角色。它們旨在與 IT 產業中需要管理員或唯讀許可的常見任務責任密切一致；不過，如果您需要將不同的許可授予使用者，您可以編輯政策以包含或排除特定許可。您也可以建立自己的自訂政策。

範本提供兩個政策。此`AMSAccelerateAdminAccess`政策旨在用於設定和操作 AMS Accelerate 元件。此政策通常由 IT 管理員擔任，並授予許可來設定 AMS 功能，例如修補和備份。`AMSAccelerateReadOnly` 授予檢視 AMS Accelerate 相關資源所需的最低許可。

```
AWSTemplateFormatVersion: 2010-09-09
Description: AMSAccelerateCustomerAccessPolicies
```

```
Resources:
  AMSAccelerateAdminAccess:
    Type: 'AWS::IAM::ManagedPolicy'
    Properties:
      ManagedPolicyName: AMSAccelerateAdminAccess
      Path: /
      PolicyDocument:
        Fn::Sub:
        - |
          {
            "Version": "2012-10-17",
            "Statement": [
              {
                 "Sid": "AmsSelfServiceReport",
                 "Effect": "Allow",
                 "Action": "amsssrv:*",
                 "Resource": "*"
              },
              {
                "Sid": "AmsBackupPolicy",
                "Effect": "Allow",
                "Action": "iam:PassRole",
                "Resource": "arn:aws:iam::${AWS::AccountId}:role/ams-backup-iam-role"
              },
              {
                "Sid": "AmsChangeRecordKMSPolicy",
                "Effect": "Allow",
                "Action": [
                  "kms:Encrypt",
                  "kms:Decrypt",
                  "kms:GenerateDataKey"
                ],
                "Resource": [
                  "arn:aws:kms:${AWS::Region}:${AWS::AccountId}:key/*"
                ],
                "Condition": {
                  "ForAnyValue:StringLike": {
                    "kms:ResourceAliases": "alias/AMSCloudTrailLogManagement"
                  }
                }
              },
              {
                "Sid": "AmsChangeRecordAthenaReadPolicy",
```

```
                "Effect": "Allow",
                "Action": [
                  "athena:BatchGetNamedQuery",
                  "athena:Get*",
                  "athena:List*",
                  "athena:StartQueryExecution",
                  "athena:UpdateWorkGroup",
                  "glue:GetDatabase*",
                  "glue:GetTable*",
                  "s3:GetAccountPublicAccessBlock",
                  "s3:ListAccessPoints",
                  "s3:ListAllMyBuckets"
                ],
                "Resource": "*"
              },
              {
                "Sid": "AmsChangeRecordS3ReadPolicy",
                "Effect": "Allow",
                "Action": [
                  "s3:Get*",
                  "s3:List*"
                ],
                "Resource": [
                  "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}",
                  "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}/
*",
                  "arn:aws:s3:::ams-a${AWS::AccountId}-cloudtrail-${AWS::Region}",
                  "arn:aws:s3:::ams-a${AWS::AccountId}-cloudtrail-${AWS::Region}/*"
                ]
              },
              {
                "Sid": "AmsChangeRecordS3WritePolicy",
                "Effect": "Allow",
                "Action": [
                  "s3:PutObject",
                  "s3:PutObjectLegalHold",
                  "s3:PutObjectRetention"

                ],
                "Resource": [
                  "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}/*"
                ]
              },
              {
```

```
      "Sid": "MaciePolicy",
      "Effect": "Allow",
      "Action": [
        "macie2:GetFindingStatistics"
      ],
      "Resource": "*"
    },
    {
      "Sid": "GuardDutyPolicy",
      "Effect": "Allow",
      "Action": [
        "guardduty:GetFindingsStatistics",
        "guardduty:ListDetectors"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SupportPolicy",
      "Effect": "Allow",
      "Action": "support:*",
      "Resource": "*"
    },
    {
      "Sid": "ConfigPolicy",
      "Effect": "Allow",
      "Action": [
        "config:Get*",
        "config:Describe*",
        "config:Deliver*",
        "config:List*",
        "config:StartConfigRulesEvaluation"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AppConfigReadPolicy",
      "Effect": "Allow",
      "Action": [
        "appconfig:List*",
        "appconfig:Get*"
      ],
      "Resource": "*"
    },
    {
```

```
                "Sid": "AppConfigPolicy",
                "Effect": "Allow",
                "Action": [
                  "appconfig:StartDeployment",
                  "appconfig:StopDeployment",
                  "appconfig:CreateHostedConfigurationVersion",
                  "appconfig:ValidateConfiguration"
                ],
                "Resource": [
                  "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSAlarmManagerConfigurationApplicationId}",
                  "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSAlarmManagerConfigurationApplicationId}/configurationprofile/
${AMSAlarmManagerConfigurationCustomerManagedAlarmsProfileID}",
                  "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSAlarmManagerConfigurationApplicationId}/environment/*",
                  "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSResourceTaggerConfigurationApplicationId}",
                  "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSResourceTaggerConfigurationApplicationId}/configurationprofile/
${AMSResourceTaggerConfigurationCustomerManagedTagsProfileID}",
                  "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSResourceTaggerConfigurationApplicationId}/environment/*",
                  "arn:aws:appconfig:*:${AWS::AccountId}:deploymentstrategy/*"
                ]
              },
              {
                "Sid": "CloudFormationStacksPolicy",
                "Effect": "Allow",
                "Action": [
                  "cloudformation:DescribeStacks"
                ],
                "Resource": "*"
              },
              {
                "Sid": "EC2Policy",
                "Action": [
                  "ec2:DescribeInstances"
                ],
                "Effect": "Allow",
                "Resource": "*"
              },
              {
                "Sid": "SSMPolicy",
```

```
                "Effect": "Allow",
                "Action": [
                  "ssm:AddTagsToResource",
                  "ssm:CancelCommand",
                  "ssm:CancelMaintenanceWindowExecution",
                  "ssm:CreateAssociation",
                  "ssm:CreateAssociationBatch",
                  "ssm:CreateMaintenanceWindow",
                  "ssm:CreateOpsItem",
                  "ssm:CreatePatchBaseline",
                  "ssm:DeleteAssociation",
                  "ssm:DeleteMaintenanceWindow",
                  "ssm:DeletePatchBaseline",
                  "ssm:DeregisterPatchBaselineForPatchGroup",
                  "ssm:DeregisterTargetFromMaintenanceWindow",
                  "ssm:DeregisterTaskFromMaintenanceWindow",
                  "ssm:Describe*",
                  "ssm:Get*",
                  "ssm:List*",
                  "ssm:PutConfigurePackageResult",
                  "ssm:RegisterDefaultPatchBaseline",
                  "ssm:RegisterPatchBaselineForPatchGroup",
                  "ssm:RegisterTargetWithMaintenanceWindow",
                  "ssm:RegisterTaskWithMaintenanceWindow",
                  "ssm:RemoveTagsFromResource",
                  "ssm:SendCommand",
                  "ssm:StartAssociationsOnce",
                  "ssm:StartAutomationExecution",
                  "ssm:StartSession",
                  "ssm:StopAutomationExecution",
                  "ssm:TerminateSession",
                  "ssm:UpdateAssociation",
                  "ssm:UpdateAssociationStatus",
                  "ssm:UpdateMaintenanceWindow",
                  "ssm:UpdateMaintenanceWindowTarget",
                  "ssm:UpdateMaintenanceWindowTask",
                  "ssm:UpdateOpsItem",
                  "ssm:UpdatePatchBaseline"
                ],
                "Resource": "*"
              },
              {
                "Sid": "AmsPatchRestrictAMSResources",
                "Effect": "Deny",
```

```
      "Action": [
        "ssm:DeletePatchBaseline",
        "ssm:UpdatePatchBaseline"
      ],
      "Resource": [
        "arn:aws:ssm:${AWS::Region}:${AWS::AccountId}:patchbaseline/*"
      ],
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/ams:resourceOwner": "*"
        }
      }
    },
    {
      "Sid": "AmsPatchRestrictAmsTags",
      "Effect": "Deny",
      "Action": [
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringLike": {
          "aws:TagKeys": [
            "AMS*",
            "Ams*",
            "ams*"
          ]
        }
      }
    },
    {
      "Sid": "TagReadPolicy",
      "Effect": "Allow",
      "Action": [
        "tag:GetResources",
        "tag:GetTagKeys"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CloudtrailReadPolicy",
      "Effect": "Allow",
      "Action": [
```

```
                  "cloudtrail:DescribeTrails",
                  "cloudtrail:GetTrailStatus",
                  "cloudtrail:LookupEvents"
                ],
                "Resource": "*"
              },
              {
                "Sid": "EventBridgePolicy",
                "Effect": "Allow",
                "Action": [
                  "events:Describe*",
                  "events:List*",
                  "events:TestEventPattern"
                ],
                "Resource": "*"
              },
              {
                "Sid": "IAMReadOnlyPolicy",
                "Action": [
                    "iam:ListRoles",
                    "iam:GetRole"
                ],
                "Effect": "Allow",
                "Resource": "*"
              },
              {
                "Sid": "AmsResourceSchedulerPassRolePolicy",
                "Effect": "Allow",
                "Action": "iam:PassRole",
                "Resource": "arn:aws:iam::${AWS::AccountId}:role/
ams_resource_scheduler_ssm_automation_role",
                "Condition": {
                    "StringEquals": {
                        "iam:PassedToService": "ssm.amazonaws.com"
                    }
                }
              }
            ]
          }
        - AMSAlarmManagerConfigurationApplicationId: !ImportValue "AMS-Alarm-Manager-
Configuration-ApplicationId"
          AMSAlarmManagerConfigurationCustomerManagedAlarmsProfileID: !ImportValue
 "AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-ProfileID"
```

```
          AMSResourceTaggerConfigurationApplicationId: !ImportValue "AMS-
ResourceTagger-Configuration-ApplicationId"
          AMSResourceTaggerConfigurationCustomerManagedTagsProfileID: !ImportValue
 "AMS-ResourceTagger-Configuration-CustomerManagedTags-ProfileID"

  AMSAccelerateReadOnly:
    Type: 'AWS::IAM::ManagedPolicy'
    Properties:
      ManagedPolicyName: AMSAccelerateReadOnly
      Path: /
      PolicyDocument: !Sub |
        {
          "Version": "2012-10-17",
          "Statement": [
          {
                "Sid": "AmsSelfServiceReport",
                "Effect": "Allow",
                "Action": "amsssrv:*",
                "Resource": "*"
             },
           {
              "Sid": "AmsBackupPolicy",
              "Effect": "Allow",
              "Action": [
                "backup:Describe*",
                "backup:Get*",
                "backup:List*"
              ],
              "Resource": "*"
           },
           {
               "Action": [
                   "rds:DescribeDBSnapshots",
                   "rds:ListTagsForResource",
                   "rds:DescribeDBInstances",
                   "rds:describeDBSnapshots",
                   "rds:describeDBEngineVersions",
                   "rds:describeOptionGroups",
                   "rds:describeOrderableDBInstanceOptions",
                   "rds:describeDBSubnetGroups",
                   "rds:DescribeDBClusterSnapshots",
                   "rds:DescribeDBClusters",
                   "rds:DescribeDBParameterGroups",
                   "rds:DescribeDBClusterParameterGroups",
```

```
                "rds:DescribeDBInstanceAutomatedBackups"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "dynamodb:ListBackups",
                "dynamodb:ListTables"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "elasticfilesystem:DescribeFilesystems"
            ],
            "Resource": "arn:aws:elasticfilesystem:*:*:file-system/*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "ec2:DescribeSnapshots",
                "ec2:DescribeVolumes",
                "ec2:describeAvailabilityZones",
                "ec2:DescribeVpcs",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeImages",
                "ec2:DescribeSubnets",
                "ec2:DescribePlacementGroups",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "tag:GetTagKeys",
                "tag:GetTagValues",
                "tag:GetResources"
            ],
            "Effect": "Allow",
```

```
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:DescribeCachediSCSIVolumes",
                "storagegateway:DescribeStorediSCSIVolumes"
            ],
            "Resource": "arn:aws:storagegateway:*:*:gateway/*/volume/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:ListGateways"
            ],
            "Resource": "arn:aws:storagegateway:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:DescribeGatewayInformation",
                "storagegateway:ListVolumes",
                "storagegateway:ListLocalDisks"
            ],
            "Resource": "arn:aws:storagegateway:*:*:gateway/*"
        },
        {
            "Action": [
                "iam:ListRoles",
                "iam:GetRole"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "organizations:DescribeOrganization",
            "Resource": "*"
        },
        {
            "Action": "fsx:DescribeBackups",
            "Effect": "Allow",
            "Resource": "arn:aws:fsx:*:*:backup/*"
        },
```

```
            {
                "Action": "fsx:DescribeFileSystems",
                "Effect": "Allow",
                "Resource": "arn:aws:fsx:*:*:file-system/*"
            },
            {
                "Action": "ds:DescribeDirectories",
                "Effect": "Allow",
                "Resource": "*"
            },
            {
              "Sid": "AmsChangeRecordKMSPolicy",
              "Effect": "Allow",
              "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:GenerateDataKey"
              ],
              "Resource": [
                "arn:aws:kms:${AWS::Region}:${AWS::AccountId}:key/*"
              ],
              "Condition": {
                "ForAnyValue:StringLike": {
                  "kms:ResourceAliases": "alias/AMSCloudTrailLogManagement"
                }
              }
            },
            {
              "Sid": "AmsChangeRecordAthenaReadPolicy",
              "Effect": "Allow",
              "Action": [
                "athena:BatchGetNamedQuery",
                "athena:Get*",
                "athena:List*",
                "athena:StartQueryExecution",
                "athena:UpdateWorkGroup",
                "glue:GetDatabase*",
                "glue:GetTable*",
                "s3:GetAccountPublicAccessBlock",
                "s3:ListAccessPoints",
                "s3:ListAllMyBuckets"
              ],
              "Resource": "*"
            },
```

```
            {
              "Sid": "AmsChangeRecordS3ReadPolicy",
              "Effect": "Allow",
              "Action": [
                "s3:Get*",
                "s3:List*"
              ],
              "Resource": [
                "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}",
                "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}/*",
                "arn:aws:s3:::ams-a${AWS::AccountId}-cloudtrail-${AWS::Region}",
                "arn:aws:s3:::ams-a${AWS::AccountId}-cloudtrail-${AWS::Region}/*"
              ]
            },
            {
              "Sid": "AmsChangeRecordS3WritePolicy",
              "Effect": "Allow",
              "Action": [
                "s3:PutObject",
                "s3:PutObjectLegalHold",
                "s3:PutObjectRetention"
              ],
              "Resource": [
                "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}/*"
              ]
            },
            {
              "Sid": "MaciePolicy",
              "Effect": "Allow",
              "Action": [
                "macie2:GetFindingStatistics"
              ],
              "Resource": "*"
            },
            {
              "Sid": "GuardDutyReadPolicy",
              "Effect": "Allow",
              "Action": [
                "guardduty:GetFindingsStatistics",
                "guardduty:ListDetectors"
              ],
              "Resource": "*"
            },
            {
```

```
            "Sid": "SupportReadPolicy",
            "Effect": "Allow",
            "Action": "support:Describe*",
            "Resource": "*"
          },
          {
            "Sid": "ConfigReadPolicy",
            "Effect": "Allow",
            "Action": [
              "config:Get*",
              "config:Describe*",
              "config:List*"
            ],
            "Resource": "*"
          },
          {
            "Sid": "AppConfigReadPolicy",
            "Effect": "Allow",
            "Action": [
              "appconfig:List*",
              "appconfig:Get*"
            ],
            "Resource": "*"
          },
          {
            "Sid": "CloudFormationReadPolicy",
            "Effect": "Allow",
            "Action": [
              "cloudformation:DescribeStacks"
            ],
            "Resource": "*"
          },
          {
            "Sid": "EC2ReadPolicy",
            "Effect": "Allow",
            "Action": [
              "ec2:DescribeInstances"
            ],
            "Resource": "*"
          },
          {
            "Sid": "SSMReadPolicy",
            "Effect": "Allow",
            "Action": [
```

```
                "ssm:Describe*",
                "ssm:Get*",
                "ssm:List*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "TagReadPolicy",
            "Effect": "Allow",
            "Action": [
                "tag:GetResources",
                "tag:GetTagKeys"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudtrailReadPolicy",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:LookupEvents"
            ],
            "Resource": "*"
        },
        {
            "Sid": "EventBridgePolicy",
            "Effect": "Allow",
            "Action": [
                "events:Describe*",
                "events:List*",
                "events:TestEventPattern"
            ],
            "Resource": "*"
        }
    ]
}
```

AMS 存取您帳戶的原因和時間

AMS Accelerate (Accelerate) 運算子在某些情況下可以存取您的帳戶主控台和執行個體，以管理您的資源。這些存取事件會記錄在 AWS CloudTrail (CloudTrail) 日誌中。如需如何檢閱 AMS Accelerate

Operations 團隊和 AMS Accelerate 自動化帳戶中活動的詳細資訊，請參閱 追蹤 AMS Accelerate 帳戶中的變更。

下列主題說明 AMS 為何、何時以及如何存取您的帳戶。

AMS 客戶帳戶存取觸發條件

AMS 客戶帳戶存取活動是由觸發條件驅動。今天的觸發條件是在問題管理系統中建立的 AWS 票證，以回應 Amazon CloudWatch (CloudWatch) 警示和事件，以及您提交的事件報告或服務請求。每個存取可能會執行多個服務呼叫和主機層級活動。

下表列出存取理由、觸發條件和觸發條件的啟動者。

存取觸發條件

存取	啟動者	觸發條件
修補	AMS	修補程式問題
內部問題調查	AMS	問題（已識別為系統性的問題）
警示調查和修復	AMS	AWS Systems Manager 操作工作項目 (SSM OpsItems)
事件調查和修復	您	傳入支援案例（您提交的事件或服務請求）
傳入服務請求履行	您	

AMS 客戶帳戶存取 IAM 角色

AMS 運算子需要下列角色來服務您的帳戶。

> **Note**
>
> AMS 存取角色可讓 AMS 運算子存取您的 資源，以提供 AMS 功能（請參閱 服務描述）。變更這些角色可能會抑制我們提供這些功能的能力。如果您需要變更 AMS 存取角色，請洽詢您的雲端架構師。

AMS 存取客戶帳戶的 IAM 角色

角色名稱	描述
ams-access-admin	此角色對您的帳戶具有完整的管理存取權，不受限制。AMS 服務使用此角色搭配限制性工作階段政策，以限制部署 AMS 基礎設施和操作帳戶的存取權。
ams-access-admin-operations	此角色會授予 AMS 運算子管理許可來操作您的帳戶。此角色不會授予 Amazon Simple Storage Service、Amazon Relational Database Service、Amazon DynamoDB、Amazon Redshift 和 Amazon ElastiCache 等常見資料存放區 AWS 服務中客戶內容的讀取、寫入或刪除許可。只有對存取管理有深入理解和背景的合格 AMS 操作員才能擔任此角色。這些運算子可做為存取管理問題的升級點，並存取您的帳戶來疑難排解 AMS 運算子存取問題。
ams-access-management	在加入期間手動部署。AMS Access 系統需要此角色來管理和`ams-access-roles ams-access-managed-policies` 堆疊。
ams-access-operations	此角色具有在您的帳戶中執行管理任務的許可。此角色對經常用作資料存放區的 AWS 服務中的客戶內容沒有讀取、寫入或刪除許可，例如 Amazon Simple Storage Service、Amazon Relational Database Service、Amazon DynamoDB、Amazon Redshift 和 Amazon ElastiCache。此角色也會排除執行 AWS Identity and Access Management 寫入操作的許可。AMS Accelerate 操作人員和雲端架構師 (CAs) 可以擔任此角色。
ams-access-read-only	此角色具有您帳戶的唯讀存取權。AMS Accelerate 操作人員和雲端架構師 (CAs) 可以擔任此角色。不會授予 Amazon S3、Amazon RDS、DynamoDB、Amazon Redshift 和 ElastiCache 等常見資料存放區 AWS 服務中客戶內容的讀取許可。

角色名稱	描述
ams-access-security-analyst	此 AMS 安全角色在您的 AMS 帳戶中具有執行專用安全提醒監控和安全事件處理的許可。只有極少數特定 AMS 安全人員可以擔任此角色。
ams-access-security-analyst-read-only	此 AMS 安全角色僅限於您 AMS 帳戶中的唯讀許可，以執行專用安全提醒監控和安全事件處理。

> **Note**
>
> 這是 ams-access-management 角色的範本。這是雲端架構師 (CAs) 在加入時在您的帳戶中手動部署的堆疊： management-role.yaml。
> 這是不同存取層級之不同存取角色的範本：ams-access-read-only、ams-access-operations、ams-access-admin-operations、ams-access-admin：accelerated-roles.yaml。

AMS 如何存取您的帳戶

在某些情況下，AMS Accelerate 運算子可以存取您的帳戶主控台和執行個體。

AMS 運算子使用內部 AMS Accelerate 存取服務，以安全且稽核的方式存取您的帳戶。若要存取您的執行個體，AMS 運算子會使用與代理程式相同的內部 AMS 存取服務，並在授予存取權後，AMS Accelerate 運算子會使用 SSM 工作階段管理員，使用工作階段憑證來取得存取權。Windows 執行個體的 RDP 存取是透過建立連接埠轉送至執行個體，並使用 SSM 建立本機使用者來提供。本機使用者登入資料會用於 RDP 存取，並在工作階段結束時移除。

在 AMS 中使用根使用者帳戶的方式和時間

根使用者是您帳戶中的超級使用者 AWS 。AMS 會監控根用量。我們建議您只將根用於需要它的一些任務，例如：變更您的帳戶設定、啟用 AWS Identity and Access Management (IAM) 對帳單和成本管理的存取、變更根密碼，以及啟用多重驗證 (MFA)。請參閱AWS Identity and Access Management《 使用者指南》中的需要根使用者憑證的任務。

AMS Accelerate 的根目錄：

AMS 不會禁止您使用根使用者帳戶。不過，AMS Operations and Security 確實將其用量視為調查的問題，我們會在每次使用時聯絡您的安全團隊。

我們建議您提前 24 小時聯絡 CSDM 和 CA，告知他們您要執行的根存取工作。

根用量的 AMS 操作和安全性回應：

使用根使用者帳戶時，AMS 會收到警示。如果根登入資料用量未排定，他們會聯絡 AMS 安全團隊和您的客戶團隊，以確認這是否為預期的活動。如果不是預期的活動，AMS 會與您的安全團隊合作調查問題。

AMS Accelerate 中的安全管理

AWS Managed Services 使用多個控制項來保護您的資訊資產，並協助您保護 AWS 基礎設施的安全。AMS Accelerate 會維護 AWS Config 規則 和 修復動作的程式庫，以確保您的所有帳戶都符合業界的安全性和操作完整性標準。 AWS Config 規則 會持續追蹤所記錄資源之間的組態變更。如果變更違反任何規則條件，AMS 會報告其調查結果，並允許您根據違規的嚴重性自動或請求修復違規。 AWS Config 規則 協助符合以下標準：網際網路安全中心 (CIS)、國家標準與技術研究所 (NIST) 雲端安全架構 (CSF)、健康保險流通與責任法案 (HIPAA) 和支付卡產業 (PCI) 資料安全標準 (DSS)。

此外，AMS 利用 Amazon GuardDuty 來識別 AWS 環境中可能未經授權或惡意的活動。AMS 全年無休監控 GuardDuty 調查結果。AMS 會與您合作，以了解調查結果的影響，並根據最佳實務建議識別修復。AMS 也會使用 Amazon Macie 來保護您的敏感資料，例如個人健康資訊 (PHI)、個人身分識別資訊 (PII) 和財務資料。

> **Note**
>
> Amazon Macie 是選用服務，預設不會啟用。

AMS Accelerate 提供各種營運服務，協助您實現卓越營運 AWS。若要進一步了解 AMS 如何 AWS 雲端 透過 AMS 金鑰操作功能，包括全年無休的服務台、主動監控、安全性、修補、記錄和備份，協助您的團隊在 中實現整體卓越營運，請參閱 AMS 參考架構圖表。

主題

- 變更請求安全性審查
- 安全性常見問答集

使用 Log4j SSM 文件來探索 Accelerate 中的事件

Log4j AWS Systems Manager 文件 (SSM 文件） 可協助您在擷取的工作負載中搜尋 Apache Log4j2 程式庫。自動化文件提供 Log4j2 程式庫作用中之 Java 應用程式 (Java) 的程序 ID 報告。

此報告包含 Java Archives (JAR 檔案） 的相關資訊，可在包含 JndiLookup 類別的指定環境中找到。最佳實務是將探索到的程式庫升級至最新的可用版本。此升級可減少透過 CVE-2021-44228 識別的遠端程式碼執行 (RCE)。從 Apache 下載最新版的 Log4j 程式庫。如需詳細資訊，請參閱下載 Apache Log4j 2。

文件會與加入 Accelerate 的所有區域共用。若要存取文件，請完成下列步驟：

1. 在 https：//https://console.aws.amazon.com/systems-manager/ 開啟 AWS Systems Manager 主控台。
2. 在導覽窗格中，選擇 Documents (文件)。
3. 選擇與我共用。
4. 在搜尋方塊中，輸入 AWSManagedServices-GatherLog4jInformation。
5. 使用速率控制大規模執行文件。

AWSManagedServices-GatherLog4jInformation 文件會收集下列參數：

- InstanceId：（必要） EC2 執行個體的 ID。
- S3Bucket體：（選用） 上傳結果的 S3 預先簽章 URL 或 S3 URI (s3：//BUCKET_NAME)。
- AutomationAssumeRole：（必要） 允許自動轉換代表您執行動作之角色的 ARN。

最佳實務是使用速率控制執行本文件。您可以將速率控制參數設定為 InstanceId，並為其指派執行個體清單，或套用標籤索引鍵組合以鎖定具有特定標籤的所有 EC2 執行個體。AWS Managed Services 也建議您提供 Amazon Simple Storage Service (Amazon S3) 儲存貯體來上傳結果，以便從存放在 S3 中的資料建置報告。如需如何在 S3 中彙總結果的範例，請參閱 EC2 執行個體堆疊 | 收集 Log4j 資訊。

如果您無法升級套件，請遵循使用 AWS 安全服務保護、偵測和回應 Log4j 漏洞中 AWS 安全性概述的指導方針。若要透過移除 JndiLookup 類別功能來緩解漏洞，請使用 Java 應用程式（內嵌） 執行 Log4j 熱修補程式。如需熱修補程式的詳細資訊，請參閱 Apache Log4j 的熱修補程式。

有關自動化輸出或如何繼續其他緩解措施的問題，請提交服務請求。

AMS 中的基礎設施安全監控

當您加入 AMS Accelerate 時， AWS 部署下列 AWS Config 基準基礎設施和一組規則，AMS Accelerate 會使用這些規則來監控您的帳戶。

- AWS Config 服務連結角色：AMS Accelerate 部署名為 AWSServiceRoleForConfig 的服務連結角色， AWS Config 供 用來查詢其他服務的狀態 AWS 。AWSServiceRoleForConfig 服務連結角色信任 AWS Config 服務擔任該角色。AWSServiceRoleForConfig 角色的許可政策包含 AWS Config 資源的唯讀和唯讀許可，以及 AWS Config 支援之其他服務中資源的唯讀許可。如果您已使用 AWS Config Recorder 設定角色，AMS Accelerate 會驗證現有角色是否已連接 AWS Config 受管政策。如果沒有，AMS Accelerate 會將角色取代為服務連結角色 AWSServiceRoleForConfig。
- AWS Config 記錄器和交付通道： AWS Config 使用組態記錄器偵測資源組態中的變更，並將這些變更擷取為組態項目。AMS Accelerate 在所有服務中部署組態記錄器 AWS 區域，並持續記錄所有資源。AMS Accelerate 也會建立組態交付管道，即 Amazon S3 儲存貯體，用於記錄 AWS 資源中發生的變更。組態記錄器會透過交付管道更新組態狀態。需要組態記錄器和交付管道 AWS Config 才能運作。AMS Accelerate 會在所有 中建立記錄器 AWS 區域，並在單一 中建立交付管道 AWS 區域。如果您已在 中擁有記錄器和交付管道 AWS 區域，則 AMS Accelerate 不會刪除現有 AWS Config 資源，而是在驗證其已正確設定之後，AMS Accelerate 會使用您現有的記錄器和交付管道。如需如何降低成本的詳細資訊 AWS Config ，請參閱降低 Accelerate 中的 AWS Config 成本。
- AWS Config 規則：AMS Accelerate 會維護 AWS Config 規則 和 修補動作的程式庫，以協助您符合業界的安全性和操作完整性標準。 AWS Config 規則 會持續追蹤所記錄資源之間的組態變更。如果變更違反任何規則條件，AMS 會報告其調查結果，並允許您根據違規的嚴重性自動或透過請求修復違規。 可 AWS Config 規則 促進符合以下標準：網際網路安全中心 (CIS)、國家標準與技術研究所 (NIST) 雲端安全架構 (CSF)、健康保險流通與責任法案 (HIPAA) 和支付卡產業 (PCI) 資料安全標準 (DSS)。
- AWS Config 彙總工具授權：彙總工具是一種 AWS Config 資源類型，可從多個帳戶和多個區域收集 AWS Config 組態和合規資料。AMS Accelerate 會將您的帳戶加入組態彙總器，AMS Accelerate 會從中彙總您帳戶的資源組態資訊和組態合規資料，並產生合規報告。如果在 AMS 擁有的帳戶中設定了現有的彙總工具，則 AMS Accelerate 會部署額外的彙總工具，而且不會修改現有的彙總工具。

> **Note**
>
> 您的帳戶中未設定 Config 彙總工具；而是在 AMS 擁有的帳戶中設定 （並且您的帳戶已加入）。

若要進一步了解 AWS Config，請參閱：

- AWS Config：什麼是 Config？
- AWS Config 規則：使用 規則評估資源
- AWS Config 規則：動態合規檢查： AWS Config 規則 – 雲端資源的動態合規檢查
- AWS Config 彙總工具：多帳戶多區域資料彙總

如需報告的資訊，請參閱 AWS Config 控制合規報告。

使用 AMS Accelerate 的服務連結角色

AMS Accelerate 使用 AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色 (SLR) 是直接連結至 AMS Accelerate 的唯一 IAM 角色類型。服務連結角色由 AMS Accelerate 預先定義，並包含該服務代表您呼叫其他 AWS 服務所需的所有許可。

服務連結角色可讓您更輕鬆地設定 AMS Accelerate，因為您不必手動新增必要的許可。AMS Accelerate 定義其服務連結角色的許可，除非另有定義，否則只有 AMS Accelerate 可以擔任其角色。定義的許可包括信任政策和許可政策，且該許可政策無法附加至其他 IAM 實體。

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

AMS Accelerate 的部署工具組服務連結角色

AMS Accelerate 使用名為 AWSServiceRoleForAWSManagedServicesDeploymentToolkit 的服務連結角色 (SLR) – 此角色會將 AMS Accelerate 基礎設施部署到客戶帳戶。

> **Note**
>
> 此政策最近已更新；如需詳細資訊，請參閱 加速服務連結角色的更新。

AMS Accelerate 部署工具組 SLR

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

- `deploymenttoolkit.managedservices.amazonaws.com`

名為 AWSManagedServicesDeploymentToolkitPolicy 的政策允許 AMS Accelerate 對下列資源執行動作：

- `arn:aws*:s3:::ams-cdktoolkit*`
- `arn:aws*:cloudformation:*:*:stack/ams-cdk-toolkit*`
- `arn:aws:ecr:*:*:repository/ams-cdktoolkit*`

此 SLR 授予 Amazon S3 許可，以建立和管理 AMS 使用的部署儲存貯體，將 CloudFormation 範本或 Lambda 資產套件等資源上傳至元件部署的帳戶中。此 SLR 授予 CloudFormation 許可，以部署定義部署儲存貯體的 CloudFormation 堆疊。如需詳細資訊或下載政策，請參閱 AWSManagedServices_DeploymentToolkitPolicy。

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。

建立適用於 AMS Accelerate 的部署工具組 SLR

您不需要手動建立一個服務連結角色。當您在 AWS Management Console AWS CLI、 或 AWS API 中加入 AMS 時，AMS Accelerate 會為您建立服務連結角色。

> **Important**
>
> 如果您在 2022 年 6 月 9 日之前使用 AMS Accelerate 服務，而該服務連結角色開始支援服務連結角色，則 AMS Accelerate 會在您的帳戶中建立 AWSServiceRoleForAWSManagedServicesDeploymentToolkit 角色。若要進一步了解，請參閱我的 IAM 帳戶中出現的新角色。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您加入 AMS 時，AMS Accelerate 會再次為您建立服務連結角色。

編輯 AMS Accelerate 的部署工具組 SLR

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

刪除 AMS Accelerate 的部署工具組 SLR

您不需要手動刪除 AWSServiceRoleForAWSManagedServicesDeploymentToolkit 角色。當您從 AWS Management Console AWS CLI、 或 AWS API 的 AMS 離職時，AMS Accelerate 會為您清除資源並刪除服務連結角色。

您也可以使用 IAM 主控台、 AWS CLI 或 AWS API 手動刪除服務連結角色。若要執行此操作，您必須先手動清除服務連結角色的資源，然後才能手動刪除它。

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

刪除 AWSServiceRoleForAWSManagedServicesDeploymentToolkit 服務連結角色所使用的 AMS Accelerate 資源

在 AMS 中刪除您帳戶加入的所有區域中的`ams-cdk-toolkit`堆疊 （您可能需要先手動清空 S3 儲存貯體）。

使用 IAM 手動刪除服務連結角色

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

AMS Accelerate 的 Detective 控制服務連結角色

AMS Accelerate 使用名為 AWSServiceRoleForManagedServices_DetectiveControlsConfig 的服務連結角色 (SLR) – AWS Managed Services 使用此服務連結角色來部署 config-recorder、config 規則和 S3 儲存貯體偵測控制項。

連接至 AWSServiceRoleForManagedServices_DetectiveControlsConfig 服務連結角色的受管政策如下：AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy。如需更新此政策，請參閱「加速 AWS 受管政策的更新」。

AMS Accelerate 的偵測控制 SLR 許可

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

- detectivecontrols.managedservices.amazonaws.com

連接到此角色是 AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy AWS 受管政策 AWS 受管政策：AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy（請參閱 服務使用 角色在您的帳戶中建立設定 AMS Detective 控制項，這需要部署 資源，例如 s3 儲存貯體、組態規則和 彙總工具。 您必須設定許可，以允許 IAM 實體（例如使用者、群組或角色）建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱《 AWS Identity and Access Management 使用者指南》中的服務連結角色許可。

建立 AMS Accelerate 的偵測控制 SLR

您不需要手動建立一個服務連結角色。當您在 AWS Management Console AWS CLI、 或 AWS API 中加入 AMS 時，AMS Accelerate 會為您建立服務連結角色。

> **Important**
>
> 如果您在 2022 年 6 月 9 日之前使用 AMS Accelerate 服務，則此服務連結角色會出現在您的帳戶中，當它開始支援服務連結角色時，AMS Accelerate 會在您的帳戶中建立 AWSServiceRoleForManagedServices_DetectiveControlsConfig 角色。若要進一步了解，請參閱我的 IAM 帳戶中出現的新角色。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您加入 AMS 時，AMS Accelerate 會再次為您建立服務連結角色。

編輯 AMS Accelerate 的偵測控制項 SLR

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

刪除 AMS Accelerate 的偵測性控制項 SLR

您不需要手動刪除 AWSServiceRoleForManagedServices_DetectiveControlsConfig 角色。當您從 AWS Management Console AWS CLI、 或 AWS API 的 AMS 離職時，AMS Accelerate 會為您清除資源並刪除服務連結角色。

您也可以使用 IAM 主控台、 AWS CLI 或 AWS API 手動刪除服務連結角色。若要執行此操作，您必須先手動清除服務連結角色的資源，然後才能手動刪除它。

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

刪除 AWSServiceRoleForManagedServices_DetectiveControlsConfig 服務連結角色所使用的 AMS Accelerate 資源

在 AMS 中刪除您帳戶加入的所有區域中的 `ams-detective-controls-config-recorderams-detective-controls-config-rules-cdk`和 `ams-detective-controls-infrastructure-cdk`堆疊 （您可能必須先手動清空 S3 儲存貯體）。

使用 IAM 手動刪除服務連結角色

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

AMS Accelerate 的 Amazon EventBridge 規則服務連結角色

AMS Accelerate 使用名為 AWSServiceRoleForManagedServices_Events 的服務連結角色 (SLR)。此角色信任其中一個 AWS Managed Services 服務主體 (events.managedservices.amazonaws.com：//) 為您擔任該角色。服務會使用 角色來建立 Amazon EventBridge 受管規則。此規則是您 AWS 帳戶中將警示狀態變更資訊從您的帳戶交付至 AWS Managed Services 所需的基礎設施。

適用於 AMS Accelerate 的 EventBridge SLR 許可

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

- `events.managedservices.amazonaws.com`

連接到此角色是 `AWSManagedServices_EventsServiceRolePolicy` AWS 受管政策 （請參閱 AWS 受管政策：AWSManagedServices_EventsServiceRolePolicy)。服務會使用 角色，將警示狀態變更資訊從您的帳戶傳遞至 AMS。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AWS Identity and Access Management 《 使用者指南》中的服務連結角色許可。

您可以在此 ZIP： EventsServiceRolePolicy.zip 中下載 JSON AWSManagedServices_EventsServiceRolePolicy。 EventsServiceRolePolicy.zip

為 AMS Accelerate 建立 EventBridge SLR

您不需要手動建立一個服務連結角色。當您在 AWS Management Console AWS CLI、 或 AWS API 中加入 AMS 時，AMS Accelerate 會為您建立服務連結角色。

> **Important**
>
> 如果您在 2023 年 2 月 7 日之前使用 AMS Accelerate 服務，則此服務連結角色會出現在您的帳戶中，當它開始支援服務連結角色時，AMS Accelerate 會在您的帳戶中建立 AWSServiceRoleForManagedServices_Events 角色。若要進一步了解，請參閱我的 IAM 帳戶中出現的新角色。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您加入 AMS 時，AMS Accelerate 會再次為您建立服務連結角色。

編輯 AMS Accelerate 的 EventBridge SLR

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

刪除 AMS Accelerate 的 EventBridge SLR

您不需要手動刪除 AWSServiceRoleForManagedServices_Events 角色。當您從 AWS Management Console AWS CLI、 或 AWS API 的 AMS 離職時，AMS Accelerate 會為您清除資源並刪除服務連結角色。

您也可以使用 IAM 主控台、 AWS CLI 或 AWS API 手動刪除服務連結角色。若要執行此操作，您必須先手動清除服務連結角色的資源，然後才能手動刪除它。

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

刪除 AWSServiceRoleForManagedServices_Events 服務連結角色所使用的 AMS Accelerate 資源

使用 IAM 手動刪除服務連結角色

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

聯絡 AMS Accelerate 的服務連結角色

AMS Accelerate 使用名為 AWSServiceRoleForManagedServices_Contacts 的服務連結角色 (SLR) – 此角色可讓服務讀取受影響資源的現有標籤，並擷取適當聯絡人的設定電子郵件，以便在事件發生時加速自動通知。

這是唯一使用此服務連結角色的服務。

連接至 AWSServiceRoleForManagedServices_Contacts 服務連結角色的受管政策如下：AWSManagedServices_ContactsServiceRolePolicy。如需更新此政策，請參閱「加速 AWS 受管政策的更新」。

AMS Accelerate 的聯絡 SLR 許可

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

- `contacts-service.managedservices.amazonaws.com`

連接到此角色是 `AWSManagedServices_ContactsServiceRolePolicy` AWS 受管政策 （ 請參閱 AWS 受管政策：AWSManagedServices_ContactsServiceRolePolicy)。服務使用 角色讀取任何 AWS 資源上的標籤，並尋找標籤中包含的電子郵件，適用於事件發生時的適當聯絡點。此角色可讓 AMS 在受影響的資源上讀取該標籤並擷取電子郵件，以便在事件發生時促進自動通知。如需詳細資訊，請參閱《 AWS Identity and Access Management 使用者指南》中的服務連結角色許可。

> **Important**
>
> 請勿將個人識別資訊 (PII) 或其他機密或敏感資訊儲存在標籤中。AMS 使用標籤來為您提供管理服務。標籤不適用於私人或敏感資料。

名為 AWSManagedServices_ContactsServiceRolePolicy 的角色許可政策可讓 AMS Accelerate 對指定的資源完成下列動作：

- 動作：允許 Contacts Service 讀取專門設定的標籤，以包含 AMS 在任何 AWS 資源上傳送事件通知的電子郵件。

您可以在此 ZIP：ContactsServicePolicy.zip 中下載 JSON AWSManagedServices_ContactsServiceRolePolicy。 ContactsServicePolicy.zip

為 AMS Accelerate 建立聯絡人 SLR

您不需要手動建立一個服務連結角色。當您在 AWS Management Console、 AWS CLI或 AWS API 中加入 AMS 時，AMS Accelerate 會為您建立服務連結角色。

> **Important**
>
> 如果您在 2023 年 2 月 16 日之前使用 AMS Accelerate 服務，此服務連結角色會出現在您的帳戶中，當它開始支援服務連結角色時，AMS Accelerate 會在您的帳戶中建立 AWSServiceRoleForManagedServices_Contacts 角色。若要進一步了解，請參閱我的 IAM 帳戶中出現的新角色。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您加入 AMS 時，AMS Accelerate 會再次為您建立服務連結角色。

編輯 AMS Accelerate 的聯絡人 SLR

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

刪除 AMS Accelerate 的聯絡人 SLR

您不需要手動刪除 AWSServiceRoleForManagedServices_Contacts 角色。當您從 AWS Management Console AWS CLI、 或 AWS API 的 AMS 離職時，AMS Accelerate 會為您清除資源並刪除服務連結角色。

您也可以使用 IAM 主控台、 AWS CLI 或 AWS API 手動刪除服務連結角色。若要執行此操作，您必須先手動清除服務連結角色的資源，然後才能手動刪除它。

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

刪除 AWSServiceRoleForManagedServices_Contacts 服務連結角色所使用的 AMS Accelerate 資源

使用 IAM 手動刪除服務連結角色

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

AMS Accelerate 服務連結角色支援的區域

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

加速服務連結角色的更新

檢視自此服務開始追蹤這些變更以來，加速服務連結角色更新的詳細資訊。如需此頁面變更的自動提醒，請訂閱加速頁面上的 RSS 摘要AMS Accelerate 使用者指南的文件歷史記錄。

變更	描述	日期

更新的政策 – 部署工具組	• 已為資源 新增這些新許可arn:aws:ecr:*:*:repository/ams-cdktoolkit* ：
	`ecr:BatchGetRepositoryScanningConfiguration`
	`ecr:PutImageScanningConfiguration`
		2024 年 4 月 4 日

更新的政策 – 部署工具組	• 已為資源 新增這些新許可arn:aws:cloudformation:*:*:stack/ams-cdk-toolkit* ：
	`cloudformation:DeleteChangeSet`
	`cloudformation:DescribeStackEvents`
	`cloudformation:GetTemplate`
	`cloudformation:TagResource`
	`cloudformation:UntagResource`
	• 已為資源 新增這些新許可arn:aws:ecr:*:*:repository/ams-cdktoolkit* ：
	`ecr:CreateRepository`
	`ecr:DeleteLifecyclePolicy`
	`ecr:DeleteRepository`
	`ecr:DeleteRepositoryPolicy`
	`ecr:DescribeRepositories`
		2023 年 5 月 9 日

變更	描述	日期
	ecr:GetLifecyclePolicy ecr:ListTagsForResource ecr:PutImageTagMutability ecr:PutLifecyclePolicy ecr:SetRepositoryPolicy ecr:TagResource ecr:UntagResource • 此外，一些使用萬用字元的現有動作範圍縮小為個別動作： - s3:DeleteObject* + s3:DeleteObject + s3:DeleteObjectTagging + s3:DeleteObjectVersion + s3:DeleteObjectVersionTagging - s3:GetObject* + s3:GetObject + s3:GetObjectAcl + s3:GetObjectAttributes + s3:GetObjectLegalHold + s3:GetObjectRetention + s3:GetObjectTagging + s3:GetObjectVersion + s3:GetObjectVersionAcl + s3:GetObjectVersionAttributes + s3:GetObjectVersionForReplication + s3:GetObjectVersionTagging + s3:GetObjectVersionTorrent - cloudformation:UpdateTermination* + cloudformation:UpdateTerminationProtection	
更新的政策 – Detective 控制項	• 與安全與存取團隊確認後CloudFormation 動作已進一步縮小範圍 • Lambda 動作已從政策中移除，因為不會影響加入/離開加入	2023 年 4 月 10 日

變更	描述	日期
更新的政策 – Detective 控制項	已更新政策並新增許可界限政策。	2023 年 3 月 21 日
新的服務連結角色 – 聯絡 SLR	加速新增 Contacts 服務的新服務連結角色。 此角色可讓服務讀取受影響資源的現有標籤，並擷取適當聯絡人的已設定電子郵件，以便在事件發生時促進自動通知。	2023 年 2 月 16 日
新的服務連結角色 – EventBridge	加速為 Amazon EventBridge 規則新增了新的服務連結角色。 此角色信任其中一個 AWS Managed Services 服務主體 (events.managedservices.amazonaws.com：//) 為您擔任該角色。服務會使用 角色來建立 Amazon EventBridge 受管規則。此規則是您 AWS 帳戶中將警示狀態變更資訊從您的帳戶交付至 AWS Managed Services 所需的基礎設施。	2023 年 2 月 7 日

更新服務連結角色 – 部署工具組	使用新的 S3 許可加速更新的 AWSServiceRoleForAWSManagedServicesDeploymentToolkit。
	
	已新增這些新許可：
	
	`"s3:GetLifecycleConfiguration",`
	`"s3:GetBucketLogging",`
	`"s3:ListBucket",`
	`"s3:GetBucketVersioning",`
	`"s3:PutLifecycleConfiguration",`
	`"s3:GetBucketLocation",`
	`"s3:GetObject*"`
		2023 年 1 月 30 日

加速開始追蹤變更	加速開始追蹤其服務連結角色的變更。	2022 年 11 月 30 日

變更	描述	日期
新的服務連結角色 – Detective 控制項	Accelerate 新增了新的服務連結角色來部署 Accelerate 偵測控制項。 AWS Managed Services 使用此服務連結角色來部署組態記錄器、組態規則和 S3 儲存貯體偵測控制項。	2022 年 10 月 13 日
新的服務連結角色 – 部署工具組	Accelerate 新增了部署 Accelerate 基礎設施的新服務連結角色。 此角色會將 AMS Accelerate 基礎設施部署到客戶帳戶。	2022 年 6 月 9 日

AWS AMS Accelerate 的 受管政策

AWS 受管政策是由 AWS AWS 受管政策建立和管理的獨立政策旨在為許多常用案例提供許可，以便您可以開始將許可指派給使用者、群組和角色。

請記住， AWS 受管政策可能不會授予特定使用案例的最低權限許可，因為這些許可可供所有 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 AWS 受管政策中定義的許可。如果 AWS 更新受 AWS 管政策中定義的許可，則更新會影響政策連接的所有委託人身分（使用者、群組和角色）。當新的 AWS 服務 啟動或新的 API 操作可供現有服務使用時， AWS 最有可能更新 AWS 受管政策。

如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

如需變更資料表，請參閱 加速 AWS 受管政策的更新。

AWS 受管政策：AWSManagedServices_AlarmManagerPermissionsBoundary

AWS Managed Services (AMS) 使用 `AWSManagedServices_AlarmManagerPermissionsBoundary` AWS 受管政策。此 AWS受管政策用於 AWSManagedServices_AlarmManager_ServiceRolePolicy，以限制由 AWSServiceRoleForManagedServices_AlarmManager 建立之 IAM 角色的許可。

此政策會授予建立為 一部分的 IAM 角色警示管理員的運作方式、執行 Config AWS 評估、擷取 Alarm Manager 組態的 AWS Config 讀取，以及建立必要 Amazon CloudWatch 警示等操作的許可。

AWSManagedServices_AlarmManagerPermissionsBoundary 政策會連接到AWSServiceRoleForManagedServices_DetectiveControlsConfig服務連結角色。如需此角色的更新，請參閱 加速服務連結角色的更新。

您可以將此政策連接至 IAM 身分。

許可詳細資訊

此政策包含以下許可。

- AWS Config – 允許評估組態規則和選取資源組態的許可。
- AWS AppConfig – 允許擷取 AlarmManager 組態的許可。
- Amazon S3 – 允許操作 AlarmManager 儲存貯體和物件的許可。
- Amazon CloudWatch – 允許讀取和放置 AlarmManager 受管警示和指標的許可。
- AWS Resource Groups and Tags – 允許讀取資源標籤的許可。
- Amazon EC2 – 允許讀取 Amazon EC2 資源的許可。
- Amazon Redshift – 允許讀取 Redshift 執行個體和叢集的許可。
- Amazon FSx – 允許描述檔案系統、磁碟區和資源標籤的許可。
- Amazon CloudWatch Synthetics – 允許讀取 Synthetics 資源的許可。
- Amazon Elastic Kubernetes Service – 允許描述 Amazon EKS 叢集的許可。
- Amazon ElastiCache – 允許描述 資源的許可。

您可以在此 ZIP：RecommendedPermissionBoundary.zip 中下載政策檔案。

AWS 受管政策：AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy

AWS Managed Services (AMS) 使用 AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy AWS 受管政策。此AWS受管政策會連接至AWSServiceRoleForManagedServices_DetectiveControlsConfig服務連結角色 （請參閱 AMS Accelerate 的 Detective 控制服務連結角色)。如需AWSServiceRoleForManagedServices_DetectiveControlsConfig服務連結角色的更新，請參閱 加速服務連結角色的更新。

此政策允許服務連結角色為您完成動作。

您可以將 AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy 政策連接至您的 IAM 實體。

如需詳細資訊，請參閱使用 AMS Accelerate 的服務連結角色。

許可詳細資訊

此政策具有下列許可，允許 AWS Managed Services Detective Controls 部署和設定所有必要的資源。

- `CloudFormation` – 允許 AMS Detective Controls 部署具有 s3 儲存貯體、組態規則和組態記錄器等資源的 CloudFormation 堆疊。
- `AWS Config` – 允許 AMS Detective 控制項建立 AMS 組態規則、設定彙總器和標籤資源。
- `Amazon S3` – 允許 AMS Detective Controls 管理其 s3 儲存貯體。

您可以在此 ZIP 中下載 JSON 政策檔案：DetectiveControlsConfig_ServiceRolePolicy.zip。

AWS 受管政策：AWSManagedServicesDeploymentToolkitPolicy

AWS Managed Services (AMS) 使用 `AWSManagedServicesDeploymentToolkitPolicy` AWS 受管政策。此 AWS受管政策會連接至`AWSServiceRoleForAWSManagedServicesDeploymentToolkit`服務連結角色 （請參閱 AMS Accelerate 的部署工具組服務連結角色)。此政策允許服務連結角色為您完成動作。您無法將此政策連接至 IAM 實體。如需詳細資訊，請參閱使用 AMS Accelerate 的服務連結角色。

如需`AWSServiceRoleForManagedServicesDeploymentToolkitPolicy`服務連結角色的更新，請參閱 加速服務連結角色的更新。

許可詳細資訊

此政策具有下列許可，允許 AWS Managed Services Detective Controls 部署和設定所有必要的資源。

- `CloudFormation` – 允許 AMS Deployment Toolkit 使用 CDK 所需的 S3 資源部署 CFN 堆疊。
- `Amazon S3` – 允許 AMS Deployment Toolkit 管理其 S3 儲存貯體。
- `Elastic Container Registry` – 允許 AMS Deployment Toolkit 管理其 ECR 儲存庫，用於部署 AMS CDK 應用程式所需的資產。

您可以在此 ZIP 中下載 JSON 政策檔案：AWSManagedServicesDeploymentToolkitPolicy.zip。

AWS 受管政策：AWSManagedServices_EventsServiceRolePolicy

AWS Managed Services (AMS) 使用 `AWSManagedServices_EventsServiceRolePolicy` AWS 受管政策。此 AWS受管政策會連接至`AWSServiceRoleForManagedServices_Events`服務連結角

色。此政策允許服務連結角色為您完成動作。您無法將此政策連接至 IAM 實體。如需詳細資訊，請參閱使用 AMS Accelerate 的服務連結角色。

如需AWSServiceRoleForManagedServices_Events服務連結角色的更新，請參閱 加速服務連結角色的更新。

許可詳細資訊

此政策具有下列許可，允許 Amazon EventBridge 將警示狀態變更資訊從您的帳戶傳遞至 AWS Managed Services。

- events – 允許 Accelerate 建立 Amazon EventBridge 受管規則。此規則是 中從您的帳戶 AWS 帳戶交付警示狀態變更資訊所需的基礎設施 AWS Managed Services。

您可以在此 ZIP： EventsServiceRolePolicy.zip 中下載 JSON 政策檔案。

AWS 受管政策：AWSManagedServices_ContactsServiceRolePolicy

AWS Managed Services (AMS) 使用 AWSManagedServices_ContactsServiceRolePolicy AWS 受管政策。此 AWS受管政策會連接至AWSServiceRoleForManagedServices_Contacts服務連結角色 （ 請參閱 為 AMS Accelerate 建立聯絡人 SLR)。此政策允許 AMS Contacts SLR 在 AWS 資源上查看您的資源標籤及其值。您無法將此政策連接至 IAM 實體。如需詳細資訊，請參閱使用 AMS Accelerate 的服務連結角色。

> **Important**
>
> 請勿將個人識別資訊 (PII) 或其他機密或敏感資訊儲存在標籤中。AMS 使用標籤來為您提供管理服務。標籤不適用於私人或敏感資料。

如需AWSServiceRoleForManagedServices_Contacts服務連結角色的更新，請參閱 加速服務連結角色的更新。

許可詳細資訊

此政策具有下列許可，允許 Contacts SLR 讀取您的資源標籤，以擷取您事先設定的資源聯絡資訊。

- IAM – 允許 Contacts 服務查看 IAM 角色和 IAM 使用者的標籤。
- Amazon EC2 – 允許 Contacts 服務查看 Amazon EC2 資源上的標籤。

- Amazon S3 – 允許 Contacts Service 查看 Amazon S3 儲存貯體上的標籤。此動作使用 條件，以確保 AMS 使用 HTTP 授權標頭、使用 SigV4 簽章通訊協定，以及搭配 TLS 1.2 或更新版本使用 HTTPS 來存取您的儲存貯體標籤。如需詳細資訊，請參閱身分驗證方法和 Amazon S3 Signature 第 4 版身分驗證特定政策金鑰。
- Tag – 允許 Contacts 服務查看其他 AWS 資源上的標籤。

- "iam：ListRoleTags"、"iam：ListUserTags"、"tag：GetResources"、"tag：GetTagKeys"、"tag：GetTagValues"、"ec2：DescribeTags"、"s3：GetBucketTagging"

您可以在此 ZIP：ContactsServicePolicy.zip 中下載 JSON 政策檔案。

加速 AWS 受管政策的更新

檢視自此服務開始追蹤這些變更以來的 Accelerate AWS 受管政策更新詳細資訊。

變更	描述	日期

更新的政策 – 部署工具組	• 已為資源 新增這些新許可arn:aws:ecr:*:*:repository/ams-cdktoolkit* ：
	`ecr:BatchGetRepositoryScanningConfiguration`
	`ecr:PutImageScanningConfiguration`
		2024 年 4 月 4 日

更新的政策 – 部署工具組	• 已為資源 新增這些新許可arn:aws:cloudformation:*:*:stack/ams-cdk-toolkit* ：
	`cloudformation:DeleteChangeSet`
	`cloudformation:DescribeStackEvents`
	`cloudformation:GetTemplate`
	`cloudformation:TagResource`
	`cloudformation:UntagResource`
	• 已為資源 新增這些新許可arn:aws:ecr:*:*:repository/ams-cdktoolkit* ：
	`ecr:CreateRepository`
		2023 年 5 月 9 日

變更	描述	日期
	ecr:DeleteLifecyclePolicy ecr:DeleteRepository ecr:DeleteRepositoryPolicy ecr:DescribeRepositories ecr:GetLifecyclePolicy ecr:ListTagsForResource ecr:PutImageTagMutability ecr:PutLifecyclePolicy ecr:SetRepositoryPolicy ecr:TagResource ecr:UntagResource • 此外，一些使用萬用字元的現有動作範圍縮小為個別動作： - s3:DeleteObject* + s3:DeleteObject + s3:DeleteObjectTagging + s3:DeleteObjectVersion + s3:DeleteObjectVersionTagging - s3:GetObject* + s3:GetObject + s3:GetObjectAcl + s3:GetObjectAttributes + s3:GetObjectLegalHold + s3:GetObjectRetention + s3:GetObjectTagging + s3:GetObjectVersion + s3:GetObjectVersionAcl + s3:GetObjectVersionAttributes + s3:GetObjectVersionForReplication + s3:GetObjectVersionTagging + s3:GetObjectVersionTorrent - cloudformation:UpdateTermination* + cloudformation:UpdateTerminationProtection	

變更	描述	日期
更新的政策 – Detective 控制項	• 與安全與存取團隊確認後CloudFormation 動作已進一步縮小範圍 • Lambda 動作已從政策中移除，因為不會影響加入/離開加入	2023 年 4 月 10 日
更新的政策 – Detective 控制項	`ListAttachedRolePolicies` 動作會從政策中移除。動作具有資源做為萬用字元 (*)。由於「清單」是非變動動作，因此可以存取所有資源，而且不允許萬用字元。	2023 年 3 月 28 日
更新的政策 – Detective 控制項	已更新政策並新增許可界限政策。	2023 年 3 月 21 日
新政策 – Contacts Service	加速新增政策，以查看來自資源標籤的帳戶聯絡資訊。 加速新增政策以讀取您的資源標籤，讓它可以擷取您事先設定的資源聯絡資訊。	2023 年 2 月 16 日
新政策 – Events Service	加速新增政策，將警示狀態變更資訊從您的帳戶傳遞至 AWS Managed Services。 授予在警示管理員的運作方式許可中建立的 IAM 角色，以建立必要的 Amazon EventBridge 受管規則。	2023 年 2 月 7 日
更新的政策 – 部署工具組	新增 S3 許可，以支援客戶從 Accelerate 離職。	2023 年 1 月 30 日
新政策 – Detective 控制項	允許服務連結角色 AMS Accelerate 的 Detective 控制服務連結角色為您完成部署加速偵測控制項的動作。	2022 年 12 月 19 日
新政策 – Alarm Manager	加速新增政策，以允許執行警示管理員任務的許可。 授予在警示管理員的運作方式許可中建立的 IAM 角色，以執行 Config AWS 評估、 AWS Config 讀取以擷取警示管理員組態、建立必要的 Amazon CloudWatch 警示等操作。	2022 年 11 月 30 日

變更	描述	日期
加速開始追蹤變更	加速開始追蹤其 AWS 受管政策的變更。	2022 年 11 月 30 日
新政策 – 部署工具組	加速為部署任務新增此政策。 授予服務連結角色 AWSServiceRoleForAWSManagedServicesDeploymentToolkit 存取和更新部署相關 Amazon S3 儲存貯體和 AWS CloudFormation 堆疊的許可。	2022 年 6 月 9 日

Accelerate 中的資料保護

AMS Accelerate 利用原生 AWS 服務 Amazon GuardDuty、Amazon Macie （選用） 和其他內部專屬工具和程序，持續監控您的受管帳戶。警示觸發後，AMS Accelerate 會承擔初始分類和警示回應的責任。AMS 回應程序是以 NIST 標準為基礎。AMS Accelerate 會使用安全事件回應模擬定期測試回應程序，讓您的工作流程與現有的客戶安全回應計劃保持一致。

當 AMS Accelerate 偵測到 或您的安全政策違規 AWS 或即將發生的違規威脅時，Accelerate 會收集資訊，包括受影響的資源和任何組態相關變更。AMS Accelerate 每週 365 天、每天 24 小時提供follow-the-sun支援，並搭配專門的運算子，主動審查和調查所有受管帳戶的監控儀表板、事件佇列和服務請求。Accelerate 會與內部安全專家調查調查結果，以分析活動，並透過您帳戶中列出的安全呈報聯絡人通知您。

根據調查結果，加速主動與您互動。如果您發現活動未經授權或可疑，AMS 會與您一起調查並修復或包含問題。GuardDuty 會產生某些問題清單類型，需要您在 Accelerate 採取任何動作之前確認影響。例如，GuardDuty 調查結果類型 UnauthorizedAccess：IAMUser/ConsoleLogin 表示您的其中一個使用者已從異常位置登入；AMS 會通知您，並要求您檢閱調查結果以確認此行為是否合法。

使用 Amazon Macie 監控

AMS Accelerate 支援，而且最佳實務是使用 Amazon Macie 來偵測大量且完整的敏感資料清單，例如個人健康資訊 (PHI)、個人身分識別資訊 (PII) 和財務資料。

您可以設定 Macie 在任何 Amazon S3 儲存貯體上定期執行。這會自動評估儲存貯體中隨時間變化的新物件或修改過的物件。產生安全性問題清單時，AMS 會通知您，並視需要與您合作修復問題清單。

如需詳細資訊，請參閱分析 Amazon Macie 調查結果。

使用 GuardDuty 監控

GuardDuty 是一種持續的安全監控服務，使用威脅情報摘要，例如惡意 IP 地址和網域的清單，以及機器學習，以識別您 AWS 環境中非預期和可能未經授權的惡意活動。這可能包括權限提升、使用公開的登入資料，或與惡意 IP 地址或網域的通訊等問題。GuardDuty 會監控 AWS 帳戶 存取行為是否有入侵跡象，例如未經授權的基礎設施部署、部署在 中的執行個體、您從未使用的 AWS 區域。GuardDuty 也會偵測不尋常的 API 呼叫，例如變更密碼政策以降低密碼強度。如需詳細資訊，請參閱 GuardDuty 使用者指南。

若要檢視和分析 GuardDuty 調查結果，請完成下列步驟：

1. 前往 https://console.aws.amazon.com/guardduty/ 開啟 GuardDuty 主控台。
2. 選擇問題清單，然後選擇特定問題清單以檢視詳細資訊。每個調查結果的詳細資訊會根據調查結果類型、涉及的資源和活動的性質而有所不同。

如需可用調查結果欄位的詳細資訊，請參閱 GuardDuty 調查結果詳細資訊。

使用 GuardDuty 禁止規則來篩選問題清單

禁止規則是一組條件，其中包含與值配對的篩選條件屬性。您可以使用隱藏規則來篩選您不打算採取行動的低價值問題清單，例如誤報問題清單或已知活動。篩選問題清單有助於更輕鬆地識別可能對您的環境影響最大的安全威脅。

若要篩選問題清單，隱藏規則會自動封存符合您指定條件的新問題清單。封存的問題清單不會傳送至 AWS Security Hub、Amazon S3 或 CloudTrail Events。因此，如果您透過 Security Hub 或第三方 SIEM 警示和票證應用程式取用 GuardDuty 調查結果，抑制篩選條件可減少不可行的資料。

AMS 具有一組已定義的條件來識別受管帳戶的禁止規則。當受管帳戶符合此條件時，AMS 會套用篩選條件並建立服務請求 (SR)，其中會詳細說明部署的禁止篩選條件。

您可以透過 SR 與 AMS 通訊，以修改或還原抑制篩選條件。

檢視封存的問題清單

GuardDuty 會持續產生調查結果，即使這些調查結果符合您的禁止規則。隱藏的問題清單會標示為已封存。GuardDuty 會將封存的問題清單存放 90 天。您可以在 GuardDuty 主控台中檢視這 90 天的已封存問題清單，方法是從問題清單表格中選取已封存。或者，使用 ListFindings API 搭配 findingCriteria of service.archived 等於 true，透過 GuardDuty API 檢視封存的問題清單。

禁止規則的常見使用案例

下列調查結果類型具有套用抑制規則的常見使用案例。

- Recon：EC2/Portscan：使用授權漏洞掃描器時，使用抑制規則自動封存問題清單。
- UnauthorizedAccess：EC2/SSHBruteForce：當問題清單以堡壘執行個體為目標時，請使用抑制規則自動封存問題清單。
- Recon：EC2/PortProbeUnprotectedPort：當問題清單鎖定在刻意公開的執行個體時，請使用隱藏規則自動封存問題清單。

使用 Amazon Route 53 Resolver DNS 防火牆進行監控

Amazon Route 53 Resolver 會以遞迴方式回應來自公開記錄、Amazon VPC 特定 DNS 名稱和 Amazon Route 53 私有託管區域的 AWS 資源的 DNS 查詢，且預設可在所有 VPCs 中使用。使用 Route 53 Resolver DNS 防火牆，您可以篩選和調節 Virtual Private Cloud (VPC) 的傳出 DNS 流量。為此，您可以在 DNS 防火牆規則群組中建立可重複使用的篩選規則集合、將規則群組與 VPC 產生關聯，然後監控 DNS 防火牆日誌和指標中的活動。根據活動，您可以相應地調整 DNS 防火牆的行為。如需詳細資訊，請參閱使用 DNS 防火牆篩選傳出 DNS 流量。

若要檢視和管理 Route 53 Resolver DNS 防火牆組態，請使用下列程序：

1. 登入 AWS Management Console ，並在 https://console.aws.amazon.com/vpc/：// 開啟 Amazon VPC 主控台。
2. 在 DNS 防火牆下，選擇規則群組。
3. 檢閱、編輯或刪除現有的組態，或建立新的規則群組。如需詳細資訊，請參閱 Route 53 Resolver DNS Firewall 的運作方式。

Amazon Route 53 Resolver DNS 防火牆監控和安全性

Amazon Route 53 DNS Firewall 使用規則關聯、規則動作和規則評估優先順序的概念。網域清單是一組可重複使用的網域規格，可在規則群組的 DNS Firewall 規則中使用。當您將規則群組與 VPC 建立關聯時，DNS 防火牆會比較您的 DNS 查詢與規則中使用的網域清單。如果 DNS 防火牆找到相符項目，則會根據相符規則的動作來處理 DNS 查詢。如需規則群組和規則的詳細資訊，請參閱 DNS 防火牆規則群組和規則。

網域清單可分為兩個主要類別：

- 受管網域清單，可為您 AWS 建立和維護。

- 您自己的網域清單，由您建立和維護。

規則群組會根據其關聯優先順序索引進行評估。

根據預設，AMS 會部署基準組態，其中包含下列規則和規則群組：

- 一個名為 的規則群組`DefaultSecurityMonitoringRule`。規則群組具有最高關聯優先順序，可在建立時針對每個啟用的每個現有 VPC 使用 AWS 區域。
- 在規則群組中使用`AWSManagedDomainsAggregateThreatList`受管網域清單搭配動作 ALERT，名為 且優先順序`DefaultSecurityMonitoringRule`為 1 的`DefaultSecurityMonitoringRule`規則。

如果您有現有的組態，則會以低於現有組態的優先順序部署基準組態。您現有的組態是預設值。如果您現有的組態不提供如何處理查詢解析的較高優先順序指示，則可以使用 AMS 基準組態做為全部截獲。若要變更或移除基準組態，請執行下列其中一項操作：

- 請聯絡您的 Cloud Service Delivery Manager (CSDM) 或 Cloud Architect (CA)。
- 建立服務請求。

AMS Accelerate 中的資料加密

AMS Accelerate 使用數個 AWS 服務 進行資料加密。

Amazon Simple Storage Service 提供多種物件加密選項，可保護傳輸中和靜態的資料。伺服器端加密會先加密您的物件，再將該物件儲存至其資料中心內的磁碟，接著在下載物件時予以解密。只要您驗證要求並具備存取許可，存取加密物件或未加密物件的方式並無不同。如需詳細資訊，請參閱 Amazon S3 中的資料保護。

AWS Identity and Access Management 在 AMS Accelerate 中

AWS Identity and Access Management 是一種 Web 服務，可協助您安全地控制對 AWS 資源的存取。您可以使用 IAM 來控制 (已登入) 的身分驗證和授權使用資源的 (許可)。在 AMS Accelerate 加入期間，您有責任在每個受管帳戶中建立跨帳戶 IAM 管理員角色。

在 AMS Accelerate 中，您負責管理對 AWS 帳戶 及其基礎資源的存取，例如存取管理解決方案、存取政策和相關程序。這表示您管理使用者生命週期、目錄服務和聯合身分驗證系統中的許可，以存取

AWS 主控台或 AWS APIs。為了協助您管理存取解決方案，AMS Accelerate 部署偵測常見 IAM 錯誤組態的 AWS Config 規則，並提供修補通知。如需詳細資訊，請參閱 AWS Config 受管服務。

在 AMS Accelerate 中使用身分進行驗證

AMS 使用 IAM 角色，這是一種 IAM 身分。IAM 角色類似於使用者，因為它是具有許可政策的身分，可決定身分可以和不可以執行的操作 AWS。不過，角色沒有與其相關聯的登入資料，而不是與一個人唯一關聯，而是由任何需要它的人擔任。IAM 使用者可擔任一個角色，為了特定任務來臨時採用不同許可。

存取角色由內部群組成員資格控制，由 Operations Management 管理並定期審查。AMS 使用以下 IAM 角色。

> **Note**
>
> AMS 存取角色可讓 AMS 運算子存取您的 資源，以提供 AMS 功能 （ 請參閱 服務描述)。變更這些角色可能會抑制我們提供這些功能的能力。如果您需要變更 AMS 存取角色，請洽詢您的雲端架構師。

Role name (角色名稱)	描述
由 （ 實體 ） 使用：僅限 AMS Access Service	
ams-access-management	您在加入期間手動部署。僅由 AMS 存取擔任，以部署或更新存取角色。為存取角色的任何未來更新加入後， 會保留在您的帳戶中。
由 （ 實體 ） 使用：AMS 操作	
ams-access-admin-operations	此角色具有在帳戶中操作的管理許可，但沒有許可讀取、寫入或刪除常用於資料存放區的 AWS 服務中的客戶內容，例如 Amazon Simple Storage Service、Amazon Relational Database Service、Amazon DynamoDB、Amazon Redshift 和 Amazon ElastiCache。只有極少數特定 AMS 個人可以擔任此角色。

Role name (角色名稱)	描述
ams-access-operations	此 AMS 操作角色具有在您的帳戶中執行管理任務的許可。此角色對經常用作資料存放區的 AWS 服務中的客戶內容沒有讀取、寫入或刪除許可，例如 Amazon Simple Storage Service、Amazon Relational Database Service、Amazon DynamoDB、Amazon Redshift 和 Amazon ElastiCache。此角色也會排除執行 AWS Identity and Access Management 寫入操作的許可。
ams-access-read-only	此 AMS 唯讀角色僅限於 AMS 帳戶中的唯讀許可。此角色不會授予通常用作資料存放區 AWS 之服務中客戶內容的讀取許可，例如 Amazon S3、Amazon RDS、DynamoDB、Amazon Redshift 和 ElastiCache。
供（實體）使用：AMS 操作和 AMS 服務	
ams_ssm_automation_role	由 擔任 AWS Systems Manager ，以在您的帳戶中執行 SSM Automation 文件。
ams_ssm_automation_role	
由（實體）使用：AMS 安全	
ams-access-security-analyst	此 AMS 安全角色在您的 AMS 帳戶中具有執行專用安全提醒監控和安全事件處理的許可。只有極少數特定 AMS 安全人員可以擔任此角色。此角色不會授予通常用作資料存放區 AWS 之服務中客戶內容的讀取許可，例如 Amazon S3；、Amazon RDS；、Amazon DynamoDB、Amazon Redshift 和 ElastiCache。

Role name (角色名稱)	描述
ams-access-security-analyst-read-only	此 AMS 安全角色僅限於您 AMS 帳戶中的唯讀許可，以執行專用安全提醒監控和安全事件處理。此角色不會授予通常用作資料存放區 AWS 之服務中客戶內容的讀取許可，例如 Amazon S3；、Amazon RDS；、Amazon DynamoDB、Amazon Redshift 和 ElastiCache。
由 （實體） 使用：AWS Services	
ams-access-admin	此 AMS 管理員角色具有在 帳戶中操作的完整許可，不受限制。只有 AMS 內部服務 （具有縮小範圍的工作階段政策） 可以擔任管理員角色。
ams-opscenter-eventbridge-role	由 Amazon EventBridge 擔任，將 create AWS Systems Manager OpsItems 作為 AMS 特定 AWS Config 規則 修補工作流程的一部分。
AMSOSConfigurationCustomerInstanceRole	當 AMS OS-Configuration 服務發現缺少必要的 IAM 政策時，此 IAM 角色會套用至您的 Amazon EC2 執行個體。它可讓您的 Amazon EC2 執行個體與 AWS Systems Manager Amazon CloudWatch 和 Amazon EventBridge 服務互動。它還連接了 AMS 自訂受管政策，以啟用對 Windows 執行個體的 RDP 存取。
mc-patch-glue-service-role	由 AWS Glue ETL 工作流程擔任，以執行資料轉換，並為 AMS 修補程式報告產生器做好準備。
由 （實體） 使用：AMS 服務	
ams-alarm-manager-AWSManagedServices AlarmManagerDe-<8 位數雜湊 >	由 AMS 帳戶中的 AMS 警示管理員基礎設施擔任，以執行 AWS Config 規則 新 AWS AppConfig 部署的評估。

Role name (角色名稱)	描述
ams-alarm-manager-AWSManagedServices AlarmManagerRe-<8 位數雜湊 >	由 AMS 帳戶中的 AMS 警示管理員修復基礎設施擔任，以允許建立或刪除警示以進行修復。
ams-alarm-manager-AWSManagedServices AlarmManagerSS-<8 位數雜湊 >	由 擔任 AWS Systems Manager ，以在 AMS 帳戶中叫用 AMS 警示管理員修復服務。
ams-alarm-manager-AWSManagedServices AlarmManagerTr-<8 位數雜湊 >	由 AWS 帳戶中的 AMS 警示管理員基礎設施擔任，以執行定期 AMS AWS Config 規則 評估。
ams-alarm-manager-AWSManagedServices AlarmManagerVa-<8 位數雜湊 >	由 AMS 帳戶中的 AMS 警示管理員基礎設施擔任，以確保 AWS 帳戶中存在必要的警示。
ams-backup-iam-role	此角色用於 AWS Backup 在您的 帳戶中執行。
ams-monitoring-AWSManagedServicesLog GroupLimitLamb-<8 位數雜湊 >	由 AMS 帳戶中的 AMS 記錄和監控基礎設施擔任，以評估 Amazon CloudWatch Logs 群組限制，並與服務配額進行比較。
ams-monitoring-AWSManagedServicesRDS MonitoringRDSE-<8 位數雜湊 >	由 AMS 帳戶中的 AMS 記錄和監控基礎設施擔任，將 Amazon RDS 事件轉送至 Amazon CloudWatch Events。
ams-monitoring-AWSManagedServicesRed shiftMonitorin-<8 位數雜湊 >	由 AMS 帳戶中的 AMS 記錄和監控基礎設施擔任，將 Amazon Redshift 事件 (CreateCluster 和 DeleteCuster) 轉送至 Amazon CloudWatch Events。
ams-monitoring-infrastruc-AWSManaged ServicesMonito-<8 位數雜湊 >	由 AMS 帳戶中的 AMS 記錄和監控基礎設施擔任，以將訊息發佈至 Amazon Simple Notification Service，以驗證帳戶是否報告所有必要資料。
ams-opscenter-role	由您 AMS 帳戶中的 AMS Notification Management system 擔任，以管理與您帳戶中提醒相關的 AWS Systems Manager OpsItems。

Role name (角色名稱)	描述
ams-opsitem-autoexecution-role	由 AMS Notification Management system 擔任，使用 SSM 文件處理自動修復，以監控與帳戶中資源相關的提醒。
ams-patch-infrastructure-amspatchconfigruleroleC1-<8 位數雜湊 >	由 擔任 AWS Config ，以評估 AMS 修補程式資源並偵測其 AWS CloudFormation 堆疊中的偏離。
ams-patch-infrastructure-amspatchcwruleopsitemams-<8 位數雜湊 >	由 Amazon EventBridge 擔任以 create AWS Systems Manager OpsItems 修補失敗。
ams-patch-infrastructure-amspatchservicebusamspat-<8 位數雜湊 >	由 Amazon EventBridge 擔任，以將事件傳送至 AWS Systems Manager 維護 Windows 狀態變更通知的 AMS 修補程式協調器事件匯流排。
ams-patch-reporting-infra-amspatchreportingconfigr-<8 位數雜湊 >	由 擔任 AWS Config ，以評估 AMS 修補程式報告資源並偵測其 AWS CloudFormation 堆疊中的偏離。
ams-resource-tagger-AWSManagedServicesResourceTagg-<8 位數雜湊 >	由 AMS 帳戶中的 AMS Resource Tagger 基礎設施擔任，以在新 AWS AppConfig 部署時執行 AWS Config 規則 評估。
ams-resource-tagger-AWSManagedServicesResourceTagg-<8 位數雜湊 >	由 AMS 帳戶中的 AMS Resource Tagger 基礎設施擔任，以驗證受管資源是否存在所需的 AWS 標籤。
ams-resource-tagger-AWSManagedServicesResourceTagg-<8 位數雜湊 >	由 擔任 AWS Systems Manager ，以在 AMS 帳戶中調用 AMS Resource Tagger 修復工作流程。
ams-resource-tagger-AWSManagedServicesResourceTagg-<8 位數雜湊 >	由 AMS 帳戶中的 AMS Resource Tagger 修復基礎設施擔任，以建立或刪除受管資源的 AWS 標籤。

Role name (角色名稱)	描述
ams-resource-tagger-AWSManagedServicesResourceTagg-<8 位數雜湊 >	由您 AWS 帳戶中的 AMS Resource Tagger 基礎設施擔任，以執行定期 AMS Config 規則評估。
ams_os_configuration_event_rule_role-<AWS 區域 >	由 Amazon EventBridge 擔任，將事件從您的帳戶轉送至正確區域中的 AMS OS-Configuration 服務 EventBus。
mc-patch-reporting-service	由 AMS 修補程式資料彙總器和報告產生器所擔任。

> **Note**
>
> 這是 ams-access-management 角色的範本。這是雲端架構師 (CAs) 在加入時在您的帳戶中手動部署的堆疊： management-role.yaml。
> 這是不同存取角色和存取層級的範本：ams-access-read-only、ams-access-operations、ams-access-admin-operations、ams-access-admin：accelerated-roles.yaml。

若要進一步了解 AWS Cloud Development Kit (AWS CDK) (AWS CDK) 識別符，包括雜湊，請參閱 UniqueIDs

AMS Accelerate 功能服務會擔任帳戶程式設計存取的 ams-access-admin 角色，但工作階段政策會針對個別功能服務縮小範圍（例如修補程式、備份、監控等）。

AMS Accelerate 遵循業界最佳實務，以符合和維護合規資格。AMS Accelerate 存取您的帳戶會記錄在 CloudTrail 中，也可透過變更追蹤供您檢閱。如需有關可用來取得此資訊之查詢的資訊，請參閱 追蹤 AMS Accelerate 帳戶中的變更。

使用政策管理存取權

各種 AMS Accelerate 支援團隊，例如 Operations Engineers、Cloud Architects 和 Cloud Service Delivery Manager (CSDMs)，有時需要存取您的帳戶，才能回應服務請求和事件。其存取權由內部 AMS 存取服務管理，該服務會強制執行控制，例如業務理由、服務請求、操作項目和支援案例。預設存取為唯讀，所有存取都會受到追蹤和記錄；另請參閱 追蹤 AMS Accelerate 帳戶中的變更。

驗證 IAM 資源

AMS Accelerate 存取系統會定期擔任您帳戶中的角色（至少每 24 小時一次），並驗證我們所有的 IAM 資源是否如預期。

為了保護您的帳戶，AMS Accelerate 有一個「canary」，可監控和警示 IAM 角色的存在和狀態，以及上述的附加政策。Canary 會定期擔任 ams-access-read-only 角色，並對您的帳戶啟動 CloudFormation 和 IAM API 呼叫。Canary 會評估 AMS Accelerate 存取角色的狀態，以確保這些角色一律未修改且up-to-date狀態。此活動會在帳戶中建立 CloudTrail 日誌。

Canary 的 AWS Security Token Service (AWS STS) 工作階段名稱為 AMS-Access-Roles-Auditor-{uuid4()}，如 CloudTrail 所示，並發生下列 API 呼叫：

- Cloud Formation API 呼叫： `describe_stacks()`
- IAM API 呼叫：
  - `get_role()`
  - `list_attached_role_policies()`
  - `list_role_policies()`
  - `get_policy()`
  - `get_policy_version()`
  - `get_role_policy()`

AMS 中的安全事件回應

安全是 AWS Managed Services (AMS) 的首要任務。AMS 會在您的帳戶中部署資源和控制項來管理這些資源和控制項。 AWS 具有共同的責任模型： AWS 管理雲端的安全性，而您需負責雲端的安全性。AMS 會使用安全控制和主動監控安全問題，來保護您的資料和資產，並協助確保 AWS 基礎設施的安全。這些功能可協助您為在 AWS 雲端中執行的應用程式建立安全基準。AMS 透過安全事件回應與您合作來評估效果，然後根據最佳實務建議執行遏制和修復。

發生與基準的偏差時，例如組態錯誤或外部因素變更，您需要回應和調查。若要成功執行此作業，您需要了解 AMS 環境中安全事件回應的基本概念。您還必須了解在發生安全問題之前準備、教育和培訓雲端團隊的需求。請務必了解您可以使用的控制項和功能、為使用者帳戶入侵或濫用特權帳戶等常見安全問題準備回應計劃，以及識別使用自動化來改善回應速度和一致性的修補方法。此外，您需要了解您的合規和法規要求，因為它們與建置安全事件回應計劃相關，以滿足這些要求。

安全事件回應可能很複雜，但透過實作反覆方法，您可以簡化程序，並允許事件回應團隊透過提供早期和持續的偵測和回應來保持資產利益相關者的滿意度。在本指南中，我們為您提供 AMS 用於事件回應的方法、AMS 責任矩陣 (RACI)、如何為安全事件做好準備、如何在安全事件期間與 AMS 互動，以及 AMS 使用的一些事件回應執行手冊。

AMS 安全事件回應的運作方式

AWS Managed Services 符合 NIST 800-61 電腦安全事件處理指南的安全事件回應。透過符合此產業標準，我們提供一致的安全事件管理方法，並遵循最佳實務來保護和回應雲端中的安全事件。

事件回應生命週期

當偵測識別並產生安全提醒，或您請求安全協助時，AWS Managed Services Operations 團隊會確保及時調查、執行自動化以執行資料收集、分類和分析、通知您分析、執行調查和任何遏制活動，然後發佈事件分析。

在事件回應期間執行的資料收集、分類、分析和遏制活動會根據正在調查的安全事件類型而有所不同。特定案例的安全事件回應工作流程範例位於本文件結尾。

在事件期間，AMS 會動態判斷正確的動作過程，這可能會導致適當時重新排序或繞過記錄的步驟，以確保產生正確的結果。

準備

隨著威脅態勢的演進，AMS 持續擴展偵測和回應功能。新增偵測時，AMS 會將來自這些新偵測的提醒納入偵測和回應平台。AMS 安全回應者經過訓練，可調查並在整個安全事件回應生命週期中與您合作。

由於這種合作夥伴關係，您的安全和應用程式團隊必須準備好與 AMS 互動，在這些事件發生時處理安全事件。本文件說明安全事件期間預期會發生的情況，並協助您準備在安全事件發生時快速回應。

本文件使用事件的 NIST 800-61 定義作為系統或網路中任何可觀察到的事件，並將事件作為違反或即將發生的違反政策、可接受的使用政策或標準安全實務威脅。

準備作業核對清單

與您的 AMS 雲端解決方案交付管理員 (CSDM) 和 AMS 雲端架構師 (CA) 一起完成下列檢查清單：

- 了解哪些 帳戶中正在執行哪些工作負載。

- 了解哪些內部團隊負責各種工作負載，並在工作負載中適當標記這些工作負載。
- 為在安全事件調查期間可能需要的其他團隊和遏制決策保留內部聯絡詳細資訊。
- 確認安全聯絡人是最新的，並新增至所有受管 AWS 帳戶。聯絡人是以每個帳戶為基礎進行管理。
- 了解如何向 AMS 引發安全事件，並熟悉嚴重性和預期的回應時間。
- 確保收到安全通知時，它們會路由到適當的人員和系統，例如分頁器或您的安全操作中心。
- 了解您可以使用哪些日誌來源、這些來源儲存在您的帳戶中，以及誰可以存取它們。
- 了解如何在調查期間使用 CloudWatch Insights 查詢日誌。
- 了解資源 (EC2、IAM、S3 和 son on) 可用的遏制選項，以及遏制時工作負載可用性的後果。

偵測

在管理 AWS 您的帳戶期間，AMS 會使用從偵測來源和控制項收集的資料來監控使用者行為、帳戶活動和潛在安全事件的異常，包括但不限於 Amazon CloudWatch、Amazon GuardDuty、VPC Flow Logs、Amazon Macie AWS Config 和 Amazon 內部威脅情報摘要。

AMS 同時使用原生 AWS 服務和其他偵測技術來回應由下列人員建立的安全事件：

- 組態一致性調查結果類型
- GuardDuty 調查結果類型
- Macie 調查結果類型
- Amazon Route 53 Resolver DNS 防火牆事件
- AMS 安全事件 （雲端監看警示）

隨著服務、產品和威脅生態系統的演進，會新增其他問題清單。

向 AMS 報告安全事件

透過 AMS 支援入口網站或 支援 中心引發事件，以通知 AMS 安全事件或請求調查。

分析

識別並報告安全事件後，下一個步驟是分析報告的事件是誤報還是實際事件。AMS 使用自動化和手動調查技術來處理安全事件。分析包括調查來自不同偵測來源的日誌，例如網路流量日誌、主機日誌、CloudTrail 事件、 AWS 服務日誌等。分析也會尋找透過相互關聯顯示異常行為的模式。

需要您的合作夥伴關係，才能了解帳戶環境的特定內容，並確定帳戶和工作負載的正常情況。這有助於 AMS 更快地識別異常並加速事件回應。

處理來自 AMS 有關安全事件的通訊

AMS 透過事件票證與您的安全聯絡人互動，在調查期間通知您。您的 AMS 雲端服務交付管理員 (CSDM) 和 AMS 雲端架構師 (CA) 是主動安全調查期間任何通訊的聯絡窗口。

通訊包括產生安全提醒時的自動通知、事件分析後的通訊、建立呼叫橋接和持續交付成品，例如日誌檔案、受感染資源的快照，以及在安全事件期間取得調查結果。

AMS 安全性提醒通知中包含的標準欄位如下所列。這些欄位為您提供資訊，讓您可以將事件路由到組織內的適當團隊以進行修復。

- 問題清單類型
- 問題清單識別符 （相關）
- 問題清單嚴重性
- 問題清單描述
- 調查結果建立的日期和時間
- AWS 帳戶 ID
- 區域 （在相關區域）
- AWS 資源 (IAM user/role/policy、EC2, S3、EKS)

根據調查結果類型提供其他欄位，例如 EKS 調查結果，包括 Pod、容器和叢集詳細資訊。

包含

AMS 的遏制方法是與您建立合作夥伴關係。您了解您的業務以及因網路隔離、IAM 使用者或角色取消佈建、執行個體重新建置等遏制活動而可能發生的工作負載影響。

抑制的重要部分是決策。例如，關閉系統、隔離資源與網路，或關閉存取或結束工作階段。如果有預先決定的策略和程序來包含事件，這些決策會更容易做出。AMS 提供遏制策略，然後在您考慮實作遏制動作所涉及的風險之後，實作解決方案。

根據分析中的資源，有不同的遏制選項。AMS 預期在事件調查期間會同時部署多種類型的遏制。其中一些範例包括：

- 套用保護規則來封鎖未經授權的流量（安全群組、NACL、WAF 規則、SCP 規則、拒絕清單、將簽章動作設定為隔離或封鎖）
- 資源隔離
- 網路隔離
- 停用 IAM 使用者、角色和政策
- 修改/減少 IAM 使用者、角色權限
- 終止/暫停/刪除運算資源
- 限制來自受影響資源的公開存取
- 輪換存取金鑰、API 金鑰和密碼
- 刷新已公開的登入資料和敏感資訊

AMS 鼓勵您考慮在其風險偏好範圍內的每個主要事件類型的遏制策略類型，並清楚記錄有助於在事件發生時做出決策的條件。決定適當策略的條件包括：

- 資源可能受損
- 保留證據
- 服務無法使用（例如，網路連線、提供給外部各方的服務）
- 實作策略所需的時間和資源
- 策略的有效性（例如，部分遏制、完全遏制）
- 解決方案的持久性（例如，單向門與雙向門決策）
- 解決方案的持續時間（例如，四小時內要移除的緊急解決方法、兩週內要移除的暫時解決方法、永久解決方案）。
- 套用您可以開啟的安全控制，以降低風險，並留出時間來定義和實作更有效的遏制。

遏制的速度至關重要，AMS 建議分階段方法，透過制定短期和長期方法的策略來實現高效和有效的遏制。

使用本指南來考慮根據資源類型涉及不同技術的遏制策略。

- 遏制策略
  - AMS 是否可以識別安全事件的範圍？
    - 如果是，請識別所有資源（使用者、系統、資源）。
    - 如果否，請平行調查並對已識別的資源執行下一個步驟。

- 資源可以隔離嗎？
  - 如果是，請繼續隔離受影響的資源。
  - 如果否，則與系統擁有者和管理員合作，以決定包含問題所需的進一步動作。
- 是否將所有受影響的資源與未受影響的資源隔離？
  - 如果是，請繼續下一個步驟。
  - 如果否，則繼續隔離受影響的資源，直到完成短期遏制，以防止事件進一步升級。
- 系統備份
  - 是否為進一步分析而建立受影響系統的備份副本？
  - 鑑識複本是否加密並存放在安全的位置？
    - 如果是，請繼續下一個步驟。
    - 如果否，請加密鑑識影像，然後將它們存放在安全的位置，以防止意外使用、損壞和竄改。

根除

包含事件之後，可能需要消除威脅來源，才能保護系統，然後再繼續進行下一個復原階段。根除步驟可能包括刪除惡意軟體和移除遭到入侵的使用者帳戶，以及識別和緩解所有遭到利用的漏洞。在根除期間，請務必識別環境中所有受影響的帳戶、資源和執行個體，以便進行修復。

最佳實務是以分階段方法完成根除和復原，以排定修復步驟的優先順序。對於大規模事件，復原可能需要幾個月的時間。早期階段的用意必須是透過相對快速（數天到數週）的高價值變更來提高整體安全性，以防止未來發生事件。後期階段必須專注於長期變更（例如，基礎設施變更）和持續工作，以盡可能確保企業的安全。

對於某些事件，不需要根除或在復原期間執行。

考慮下列各項：

- 系統是否可以重新製作映像，然後使用修補程式或其他對策進行強化，以防止或降低攻擊風險？
- 是否移除攻擊者留下的所有惡意軟體和其他成品，並強化受影響的系統以抵禦進一步的攻擊？

復原

AMS 會與您合作，將系統還原至正常操作、確認系統正常運作，以及（如適用）修復漏洞以防止類似事件。

考慮下列各項：

- 受影響的系統是否已修補和強化（針對最近的攻擊和可能的未來攻擊）？
- 何時可以將受影響的系統還原到生產環境？
- 您將使用哪些工具來測試、監控和驗證您還原至生產環境的系統是否不容易受到初始攻擊技術的影響？

事件後報告

在事件發生後，AMS 會針對所有安全事件執行調查審查程序。此外，AMS 會啟動錯誤校正 (COE) 程序，以解決系統造成的安全事件，或可合理改善的程序遺漏。AMS 會與您合作，持續改善安全調查體驗。COE 程序可協助 AMS 識別影響客戶事件的促成因素，並將這些原因連接到下一個動作項目，以防止類似事件重複發生，或協助減輕影響的持續時間或層級。

安全性事件的調查審查程序會處理下列項目，以識別改進的機會：

- 從事件開始到事件探索、初始影響評估，以及事件處理程序的每個階段（例如，遏制、復原）經過了多少時間？
- 事件回應團隊需要多長時間才能回應事件的初始報告？
- 執行初始影響分析需要多長時間？
- 這可以預防嗎？如何預防？ 是否有可以防止這種情況的工具或程序？
- 我們可以更快地及如何偵測到此問題嗎？
- 什麼可以讓調查更快進行？
- 是否遵循記錄的事件回應程序？ 它們是否足夠？
- 與其他利益相關者的資訊共用是否及時完成 如何改進？
- 與其他團隊 (AWS 安全、客戶團隊、 AWS 開發團隊和客戶安全團隊）的協作是否有效？ 如果沒有，可以改善哪些項目？
- 缺少哪些可能有幫助的準備步驟、呈報矩陣、RACI、共同責任模型等？ 是否需要更新任何 Runbook？
- 初始影響評估和最終影響評估之間的差異是什麼？ 我們可以如何改善事件回應中稍早評估的準確性？
- 所學課程的動作項目有哪些？

AMS 中的安全事件回應 Runbook

本節包含兩個 Runbook：

- 對根使用者活動的回應
- 對惡意軟體事件的回應

對根使用者活動的回應

根使用者是您 AWS 帳戶中的超級使用者。請注意，AMS 會監控根用量。最佳實務是僅針對需要根使用者的少數任務使用根使用者，例如變更您的帳戶設定、啟用 AWS Identity and Access Management (IAM) 存取帳單和成本管理、變更根密碼，以及開啟多重要素驗證 (MFA)。如需詳細資訊，請參閱需要根使用者憑證的任務。

如需如何通知 AMS 計劃根用量的詳細資訊，請參閱何時以及如何在 AMS 中使用根帳戶。

偵測到根使用者活動時，嘗試登入失敗，這可能表示成功登入後帳戶中發生暴力攻擊或活動，會產生事件，並將事件傳送至您定義的安全聯絡人。

AWS Managed Services Operations 會調查意外的根使用者活動、執行資料收集、分類和分析，以及依照您的方向執行遏制活動，然後執行事件後分析。

如果您有 AMS Advanced 操作模型，您會收到來自 AMS CSDM 和 AMS Ops 工程師的額外通訊，確認意外的根使用者活動，因為 AMS 有責任保護根使用者憑證。AMS 會調查根使用者活動，直到您確認路徑向前為止。

準備

向 AMS 告知任何計劃使用的根使用者，方法是使用計劃事件的資料和時間提交 AMS 服務請求，以防止不必要的事件回應活動。

定期使用 AMS 執行 GameDays，以驗證 AMS 的客戶事件回應程序、人員和系統是最新的，並與負責的人員建立肌肉記憶體，以實現更快的事件回應。

階段 A：偵測

AMS 透過偵測來源監控帳戶中的根活動，包括 GuardDuty 和 AMS 監控。

如果您有 AMS Accelerate，操作模型會回應請求調查非預期根使用者活動的事件。發生這種情況時，AMS Operations 會啟動遭入侵的帳戶 Runbook。

如果您有 AMS Advanced，操作模型會回應事件，或通知 CSDM 任何計劃的根使用者活動，以終止作用中的帳戶入侵調查。

階段 B：分析

AMS 會在判斷活動未獲授權時，對根使用者事件進行徹底調查。使用自動化和 AMS 安全回應團隊，會針對根使用者的異常和非預期行為來分析日誌和事件。日誌會提供給您，以協助判斷活動是否未知、是否為授權的根使用者事件，或是否需要進一步調查。

調查期間為支援內部檢查而提供的資訊範例包括：

- 帳戶資訊：根帳戶用於哪個帳戶？
- 根使用者的電子郵件地址：每個根使用者都與您組織的電子郵件地址相關聯
- 身分驗證詳細資訊：根使用者從何處和何時存取您的環境？
- 活動記錄：使用者以根登入時做了什麼？ 這些記錄的格式為 CloudWatch 事件。了解如何閱讀這些日誌有助於調查。

最佳實務是，您已準備好接收分析資訊，並規劃如何聯絡組織內帳戶的授權聯絡人。由於根使用者不會命名為個人，因此判斷誰可以存取組織中用於帳戶的根電子郵件地址，有助於快速在內部路由問題。

階段 C：包含和消除

AMS 與您的安全團隊合作，在您授權的客戶安全聯絡人指示下執行遏制。遏制選項包括：

- 輪換適當的登入資料和金鑰。
- 終止對帳戶和資源的作用中工作階段。
- 消除已建立的資源。

在遏制活動期間，AMS 與您的安全團隊緊密合作，以確保工作負載的任何中斷都最小化，並且根登入資料得到適當的保護。

遏制計畫完成後，您可以視需要與 AMS Operations 團隊合作執行任何復原動作。

事件後報告

AMS 會視需要啟動調查審查程序，以識別學到的任何教訓。在完成 COE 的過程中，AMS 會將任何相關調查結果傳達給受影響的客戶，以協助他們改善事件回應程序。

AMS 會記錄調查的所有最終詳細資訊、收集適當的指標，然後將事件報告給需要資訊的任何 AMS 內部團隊，包括您指派的 CSDM 和 CA。

對惡意軟體事件的回應

Amazon EC2 執行個體用於託管各種工作負載，包括第三方軟體和由組織內應用程式團隊部署的自訂開發軟體。AMS 提供並鼓勵您在 AMS 持續修補和維護的映像上部署工作負載。

在執行個體操作期間，AMS 會透過各種安全偵測控制來監控行為或活動的異常，包括 Amazon GuardDuty、Network Traffic 和 Amazon internal Threat Intelligence 饋送。

AMS 也會監控 GuardDuty 惡意軟體調查結果。如果啟用，這些都可以在 AMS Advanced 和 AMS Accelerate 上使用。如需詳細資訊，請參閱 Amazon GuardDuty 中的惡意軟體防護。

> **Note**
>
> 如果您選擇使用自有 EPS，則事件回應的程序會與此頁面上概述的程序不同。如需詳細資訊，請參閱參考的文件。

偵測到惡意軟體時，會建立事件並通知您該事件。此通知後面接著發生的任何修復活動。AMS Operations 會調查、執行資料收集、分類和分析，然後依照您的指示執行遏制活動，接著執行事件後分析。

階段 A：偵測

AMS 會使用 GuardDuty 監控執行個體上的事件。AMS 會決定適當的擴充和分類活動，以協助您根據調查結果或提醒類型做出遏制或風險接受決策。

資料收集是根據調查結果類型執行。資料收集涉及查詢受影響帳戶內部和外部的多個資料來源，以建立觀察到的活動或關注組態的影像。

AMS 會執行調查結果與任何受影響帳戶或 AMS 威脅情報平台之任何其他警示和警示或遙測的相互關聯。

階段 B：分析

收集資料後，會對其進行分析，以識別任何活動或關注指標。在調查的這個階段，AMS 會與您合作，整合執行個體和工作負載的商業和網域知識，以協助了解預期內容和異常情況。

調查期間為支援內部檢查而提供的資訊範例包括：

- 帳戶資訊：在哪個帳戶上觀察到惡意軟體活動？
- 執行個體詳細資訊：哪些（些）執行個體與惡意軟體事件有關？
- 事件時間戳記：警示何時觸發？

- 工作負載資訊：執行個體上執行什麼項目？
- 惡意軟體詳細資訊，如果相關：惡意軟體系列和有關惡意軟體的開放原始碼資訊。
- 使用者或角色詳細資訊：哪些使用者或角色受到活動的影響和參與活動？
- 活動記錄：執行個體上會記錄哪些活動？ 這些是 CloudWatch 事件的形式，以及來自執行個體的系統事件。了解如何讀取這些日誌將協助您進行調查
- 網路活動：哪些端點正在連接到執行個體、執行個體正在連接到什麼，以及流量分析是什麼？

最佳實務是準備接收調查資訊，並規劃如何聯絡組織內帳戶、執行個體和工作負載的適當聯絡窗口。了解您的網路拓撲和預期的連線有助於加速影響分析。了解環境中規劃的滲透測試，以及應用程式擁有者執行的最新部署，也可以加速調查。

如果您確定活動已規劃並授權，則會更新事件並結束調查。如果已確認入侵，您和 AMS 會決定適當的遏制計畫。

Phace C：包含和消除

AMS 會與您合作，根據收集的資料和已知資訊來判斷適當的遏制活動。遏制選項包括但不限於：

- 透過快照保留資料
- 修改網路規則以限制傳入或傳出執行個體的流量
- 修改 SCP、IAM 使用者和角色政策以限制存取
- 終止、暫停或關閉執行個體
- 終止任何持久性連線
- 輪換適當的登入資料/金鑰

如果您選擇對執行個體執行根除活動，則 AMS 會支援您達成此目標。選項包括但不限於：

- 移除任何不需要的軟體
- 從乾淨的完全修補映像重建執行個體，並重新部署應用程式和組態
- 從先前的備份還原執行個體
- 將應用程式和服務部署到您帳戶中可能適合託管工作負載的另一個執行個體。

在還原服務之前，請務必判斷惡意軟體在執行個體上交付和執行的方式，以確保套用任何其他控制，以防止執行個體上的惡意軟體再次發生。AMS 會視需要為您的鑑識合作夥伴或團隊提供額外的洞見或資訊，以支援鑑識。

此時，您會使用 AMS Operations 進行復原活動。AMS 與您緊密合作，將對工作負載的干擾降至最低，並保護執行個體。

事件後報告

AMS 會視需要啟動調查審查程序，以識別學到的經驗教訓。在完成 COE 的過程中，AMS 會與您溝通相關調查結果，以協助您改善事件回應程序。

AMS 會記錄調查的最終詳細資訊、收集適當的指標，並向需要資訊的 AMS 內部團隊報告事件，包括您指派的 CSDM 和 CA。

Accelerate 中的安全事件記錄和監控

在 AMS Accelerate 中註冊的帳戶設定了 CloudWatch Events 和警示的基準部署，這些警示已經過最佳化，可降低雜訊並識別真實事件的跡象。AMS Accelerate 也採用 GuardDuty 進行帳戶監控。如需詳細資訊，請參閱使用 GuardDuty 監控。

Accelerate 中的組態合規

AMS Accelerate 可協助您將資源設定為高標準的安全性和操作完整性，並符合下列業界標準：

- 網際網路安全中心 (CIS)
- 國家標準技術研究所 (NIST) 雲端安全架構 (CSF)
- 美國健康保險流通與責任法案 (HIPAA)
- 支付卡產業 (PCI) 資料安全標準 (DSS)

我們透過將整個合規 AWS Config 規則集部署到您的帳戶來執行此操作，請參閱 AMS Config 規則程式庫。 AWS Config 規則代表資源所需的組態，並根據 AWS 資源設定的組態變更進行評估。任何組態變更都會觸發大量規則來測試合規性。例如，假設您建立 Amazon S3 儲存貯體，並將其設定為可公開讀取，而違反 NIST 標準。ams-nist-cis-s3-bucket-public-read-prohibited 規則會偵測違規情況，並在組態報告中標記 S3 儲存貯體不合規。由於此規則屬於 Auto Incident 修復類別，因此會立即建立 Incident Report，提醒您此問題。其他更嚴重的規則違規可能會導致 AMS 自動修復問題。請參閱 在 Accelerate 中回應違規。

> **Important**
>
> 如果您希望我們執行更多操作，例如，如果您希望 AMS 為您修復違規，無論其修復類別為何，請提交服務請求，要求 AMS 為您修復不合規的資源。在服務請求中，包含註解，例如

「作為 AMS 組態規則修復的一部分，請修復非投訴資源 *RESOURCE_ARNS_OR_IDs*、在帳戶中設定規則 *CONFIG_RULE_NAME*」，並新增必要的輸入以修復違規。
如果您希望我們做較少的事，例如，如果您不希望我們對需要設計公開存取的特定 S3 儲存貯體採取動作，您可以建立例外狀況，請參閱 在 Accelerate 中建立規則例外狀況。

AMS Config 規則程式庫

加速部署 AMS 組態規則的程式庫，以保護您的帳戶。這些組態規則以 開頭ams-。您可以從 AWS Config 主控台、 AWS CLI 或 AWS Config API 檢視帳戶中的規則及其合規狀態。如需使用 的一般資訊 AWS Config，請參閱 ViewingConfiguration 合規。

> **Note**
>
> 對於選擇加入 AWS 區域和 Gov 雲端區域，由於區域限制，我們只會部署一部分的組態規則。檢查 AMS Accelerate 組態規則表中與識別符相關聯的連結，以檢查區域中的規則可用性。
> 您無法移除任何已部署的 AMS Config 規則。

規則表

下載為 ams_config_rules.zip。

AMS 組態規則

規則名稱	服務	觸發條件	動作	架構
ams-nist-cis-guardduty-enabled-centralized	GuardDuty	定期	修復	CIS：CIS.13，CIS.14；NIST-CSF：PR.DS-1；HIPAA：164.312(a)(2)(iv)、164.312(e)(2)(ii)；PCI：2.2，3.4，8.2.1；
ams-nist-cis-vpc-flow-logs-enabled	VPC	定期	修復	CIS：CIS.6；NIST-CSF：DE.AE-1，DE.AE-3，PR.DS-5，PR.PT-1；HIPAA：164.308(a)(3)(ii)(A)，164.31

規則名稱	服務	觸發條件	動作	架構
				2(b)；PCI：2.2，10.1、10.3.2、10.3.3、10.3.4、10.3.5、、10.3.6；
ams-eks-secrets-encrypted	EKS	定期	事件	CIS：NA； NIST-CSF：NA； HIPAA： NA； PCI： NA；
ams-eks-endpoint-no-public-access	EKS	定期	事件	CIS：NA； NIST-CSF：NA； HIPAA： NA； PCI： NA；
ams-nist-cis-vpc-default-security-group-closed	VPC	組態變更	事件	CIS：CIS.11、CIS.12、CIS.9；NIST-CSF：DE.AE-1、PR.AC-3、PR.AC-5、PR.PT-4；HIPAA：164.312(e)(1)；PCI：1.2、1.3、2.1、2.2、1.2.1、1.3.1、1.3.2、2.2；
ams-nist-cis-iam-password-policy	IAM	定期	事件	CIS：NA；NIST-CSF：PR.AC-1，PR.AC-4；HIPAA：164.308(a)(3)(i)，164.308(a)(3)(ii)(A)，164.308(a)(3)(ii)(B)，164.308(a)(4)(ii)(i)，164.308(a)(4)(ii)(B)，164.308(a)(4)(ii)(C)，164.312(a)(1)；PCI：7.1.2，7.1.3，7.2.1)；

規則名稱	服務	觸發條件	動作	架構
ams-nist-cis-iam-root-access-key-check	IAM	定期	事件	CIS：CIS.16，CIS.4；NIST-CSF：PR.AC-1，PR.AC-4，PR.PT-3；HIPAA：164.308(a)(3)(i)，164.308(a)(3)(ii)(A)，164.308(a)(3)(ii)(B)，164.308(a)(4)(ii)(A)，164.308(a)(4)(ii)(B)，164.308(a)(4)(ii)(C)，164.312(a)；PCI：2.2，7.1.2，7.1.3，7.1.2；
ams-nist-cis-iam-user-mfa-enabled	IAM	定期	事件	CIS：CIS.16；NIST-CSF：PR.AC-1，PR.AC-4；HIPAA：164.308(a)(3)(i)，164.308(a)(3)(ii)(A)，164.308(a)(3)(ii)(B)，164.308(a)(4)(i)，164.308(a)(4)(ii)(B)，164.308(a)(4)(ii)(C)，164.312(a)(1)；PCI：2.2，7.1.2，7.1.3，7.2.2；
ams-nist-cis-restricted-ssh	安全群組	組態變更	事件	CIS：CIS.16；NIST-CSF：PR.AC-1，PR.AC-4；HIPAA：164.308(a)(3)(i)，164.308(a)(4)(ii)(A)，164.308(a)(4)(ii)(B)，164.308(a)(4)(ii)(C)，164.312(a)(1)；PCI：2.2，7.2.1，8.1.4；

規則名稱	服務	觸發條件	動作	架構
ams-nist-cis-restricted-common-ports	安全群組	組態變更	事件	CIS：CIS.11，CIS.12，CIS.9；NIST-CSF： DE.AE-1，PR.AC-3，PR.AC-5，PR.PT-4；HIPAA： 164.308(a)(3)(i)，164.308(a)(3)(ii)(B)，164.308(a)(4)(i)，164.308(a)(4)(ii)(A)，164.308(a)(4)(ii)(C)，164.312(a)(1)，164.312(e)(1)；PCI：1.2，1.3，2.2.2
ams-nist-cis-s3-account-level-public-access-blocks	S3	組態變更	事件	CIS：CIS.9，CIS.12，CIS.14；NIST-CSF：PR.AC-3，PR.AC-4，PR.AC-5，PR.DS-5，PR.PT-3，PR.PT-4；HIPAA：164.308(a)(3)(i)，164.308(a)(4)(ii)(A)，164.308(a)(4)(ii)(C)，164.312(a)(1)，164.312(e)(1)；PCI：1.2，1.2.1，1.3，1.3.1，1.3.2，1.3.4，1.3.6，2.2；

規則名稱	服務	觸發條件	動作	架構
ams-nist-cis-s3-bucket-public-read-prohibited	S3	組態變更	事件	CIS：CIS.12，CIS.14，CIS.9；NIST-CSF：PR.AC-3，PR.AC-4，PR.AC-5，PR.DS-5，PR.PT-3，PR.PT-4；HIPAA：164.308(a)(3)(i)，164.308(a)(4)(ii)(A)，164.308(a)(4)(ii)(C)，164.312(a)(1)，164.312(e)(1)；PCI：1.2，1.3，2.2，1.2.1，1.3.1，1.3.2，1.3.4，1.3.6，2.2；
ams-nist-cis-s3-bucket-public-write-prohibited	S3	組態變更	事件	CIS：CIS.12，CIS.14，CIS.9；NIST-CSF：PR.AC-3，PR.AC-4，PR.AC-5，PR.DS-5，PR.PT-3，PR.PT-4；HIPAA：164.308(a)(3)(i)，164.308(a)(4)(ii)(A)，164.308(a)(4)(ii)(C)，164.312(a)(1)，164.312(e)(1)；PCI：1.2，1.3，2.2，1.2.1，1.3.1，1.3.2，1.3.4，1.3.6，2.2；
ams-nist-cis-s3-bucket-server-side-encryption-enabled	S3	組態變更	事件	CIS：CIS.13，CIS.14；NIST-CSF：PR.DS-1；HIPAA：164.312(a)(2)(iv)、164.312(c)(2)、164.312(e)(2)(ii)；PCI：2.2，3.4，10.5，8.2.1；

規則名稱	服務	觸發條件	動作	架構
ams-nist-cis-securityhub-enabled	安全中樞	定期	事件	CIS：CIS.3、CIS.4、CIS.6、CIS.12、CIS.16、CIS.19；NIST-CSF：PR.DS-5，PR.PT-1；HIPAA：164.312(b)；PCI：NA；
ams-nist-cis-ec2-instance-managed-by-systems-manager	EC2	組態變更	報告	CIS：CIS.2，CIS.5；NIST-CSF：ID.AM-2，PR.IP-1；HIPAA：164.308(a)(5)(ii)(B)；PCI：2.4；
ams-nist-cis-cloudtrail-enabled	CloudTrail	定期	報告	CIS：CIS.16，CIS.6；NIST-CSF：DE.AE-1，DE.AE-3，PR.DS-5，PR.MA-2，PR.PT-1；HIPAA：164.308(a)(3)(ii)(A)，164.308(a)(5)(ii)(C)，164.312(b)；PCI：10.1、10.2.1、10.2.2、10.2.310.2.4、10.2.5、、10.2.610.2.7、10.3.1、10.3.2、、10.3.3、、10.3.4、10.3.510.3.6；
ams-nist-cis-access-keys-rotated	IAM	定期	報告	CIS：CIS.16；NIST-CSF：PR.AC-1；HIPAA：164.308(a)(4)(ii)(B)；PCI：2.2；

規則名稱	服務	觸發條件	動作	架構
ams-nist-cis-acm-certificate-expiration-check	Certificate Manager	組態變更	報告	CIS：CIS.13，CIS.14；NIST-CSF：PR.AC-5，PR.PT-4；HEAA：NA；PCI：4.1；
ams-nist-cis-alb-http-to-https-redirection-check	ALB	定期	報告	CIS：CIS.13，CIS.14；NIST-CSF：PR.DS-2；HIPAA：164.312(a)(2)(iv)、164.312(e)(1)、164.312(e)(2)(i)、164.312(e)(2)(ii)；PCI：2.3，4.1，8.2.1；
ams-nist-cis-api-gw-cache-enabled-and-encrypted	API Gateway	組態變更	報告	CIS：CIS.13、CIS.14；NIST-CSF：PR.DS-1；HIPAA：164.312(a)(2)(iv)、164.312(e)(2)(ii)；PCI：3.4；
ams-nist-cis-api-gw-execution-logging-enabled	API Gateway	組態變更	報告	CIS：CIS.6；NIST-CSF：DE.AE-1，DE.AE-3，PR.PT-1；HIPAA：164.312(b)；PCI：10.1，10.3.1，10.3.2，10.3.310.3.4，10.3.5，10.3.6，，，10.5.4；
ams-nist-autoscaling-group-elb-healthcheck-required	ELB	組態變更	報告	CIS：NA；NIST-CSF：PR.PT-1，PR.PT-5；HIPAA：164.312(b)；PCI：2.2；

規則名稱	服務	觸發條件	動作	架構
ams-nist-cis-cloud-trail-encryption-enabled	CloudTrail	定期	報告	CIS：CIS.13，CIS.14；NIST-CSF：PR.DS-1；HIPAA：164.312(a)(2)(iv)、164.312(e)(2)(ii)；PCI：2.2，3.4，10.5；
ams-nist-cis-cloud-trail-log-file-validation-enabled	CloudTrail	定期	報告	CIS：CIS.6；NIST-CSF：PR.DS-6；HIPAA：164.312(c)(1)、164.312(c)(2)；PCI：2.2，10.5，11.5，10.5.2，10.5.5；
ams-nist-cis-cloudtrail-s3-dataevents-enabled	CloudTrail	定期	報告	CIS：CIS.6；NIST-CSF：DE.AE-1，DE.AE-3，PR.DS-5，PR.PT-1；HIPAA：164.308(a)(3)(ii)(A)，164.312(b)；PCI：2.2，10.1、10.2.1、10.2.2、10.2.3、10.2.5、10.3.110.3.2、10.3.3、10.3.4、10.3.5、、10.3.6；
ams-nist-cis-cloudwatch-alarm-action-check	CloudWatch	組態變更	報告	CIS：CIS.13、CIS.14；NIST-CSF：NA；HIPAA：164.312(a)(2)(iv)、164.312(e)(2)(ii)；PCI：3.4；
ams-nist-cis-cloudwatch-log-group-encrypted	CloudWatch	定期	報告	CIS：CIS.13、CIS.14；NIST-CSF：NA；HIPAA：164.312(a)(2)(iv)、164.312(e)(2)(ii)；PCI：3.4；

規則名稱	服務	觸發條件	動作	架構
ams-nist-cis-codebuild-project-envvar-awscred-check	CodeBuild	組態變更	報告	CIS：CIS.18；NIST-CSF：PR.DS-5；HIPAA：164.308(a)(3)(i)、164.308(a)(4)(ii)(A)、164.308(a)(4)(ii)(C)、164.312(a)(1)；PCI：8.2.1；
ams-nist-cis-codebuild-project-source-repo-url-check	CodeBuild	組態變更	報告	CIS：CIS.18；NIST-CSF：PR.DS-5；HIPAA：164.308(a)(3)(i)、164.308(a)(4)(ii)(A)、164.308(a)(4)(ii)(C)、164.312(a)(1)；PCI：8.2.1；
ams-nist-cis-db-instance-backup-enabled	RDS	組態變更	報告	CIS：CIS.10；NIST-CSF：ID.BE-5，PR.DS-4，PR.IP-4，PR.PT-5，RC.RP-1；HIPAA：164.308(a)(7)(i)、164.308(a)(7)(ii)(A)、164.308(a)(7)(ii)(B)；PCI：NA；

規則名稱	服務	觸發條件	動作	架構
ams-nist-cis-dms-replication-not-public	DMS	定期	報告	CIS：CIS.12，CIS.14，CIS.9；NIST-CSF：PR.AC-3，PR.AC-4，PR.AC-5，PR.DS-5，PR.PT-3，PR.PT-4；HIPAA：164.308(a)(3)(i)，164.308(a)(4)(ii)(A)，164.308(a)(4)(ii)(C)，164.312(a)(1)，164.312(e)(1)；PCI：1.2，1.3，1.2.1，1.3.1，1.3.2，1.3.4，1.3.6，2.2；
ams-nist-dynamodb-autoscaling-enabled	DynamoDB	定期	報告	CIS：NA；NIST-CSF：ID.BE-5，PR.DS-4，PR.PT-5，RC.RP-1；HIPAA：164.308(a)(7)(i)，164.308(a)(7)(ii)(C)；PCI：NA；
ams-nist-cis-dynamodb-pitr-enabled	DynamoDB	定期	報告	CIS：CIS.10；NIST-CSF：ID.BE-5，PR.DS-4，PR.IP-4，PR.PT-5，RC.RP-1；HIPAA：164.308(a)(7)(i)、164.308(a)(7)(ii)(A)、164.308(a)(7)(ii)(B)；PCI：NA；
ams-nist-dynamodb-throughput-limit-check	DynamoDB	定期	報告	CIS：NA；NIST-CSF：NA；HIPAA：164.312(b)；PCI：NA；

規則名稱	服務	觸發條件	動作	架構
ams-nist-ebs-optimized-instance	EBS	組態變更	報告	CIS：NA；NIST-CSF：NA；HIPAA：164.308(a)(7)(i)；PCI：NA；
ams-nist-cis-ebs-snapshot-public-restorable-check	EBS	定期	報告	CIS：CIS.12，CIS.14，CIS.9；NIST-CSF：PR.AC-3，PR.AC-4，PR.AC-5，PR.DS-5，PR.PT-3，PR.PT-4；HIPAA：164.308(a)(3)(i)，164.308(a)(4)(ii)(A)，164.308(a)(4)(ii)(C)，164.312(a)(1)，164.312(e)(1)；PCI：1.2，1.3，1.2.1，1.3.1，1.3.2，1.3.4，1.3.6，2.2；
ams-nist-ec2-instance-detailed-monitoring-enabled	EC2	組態變更	報告	CIS：NA；NIST-CSF：DE.AE-1，PR.PT-1；HIPAA：164.312(b)；PCI：NA；

規則名稱	服務	觸發條件	動作	架構
ams-nist-cis-ec2-instance-no-public-ip	EC2	組態變更	報告	CIS：CIS.12，CIS.14，CIS.9；NIST-CSF：PR.AC-3，PR.AC-4，PR.AC-5，PR.PT-3，PR.PT-4；HIPAA：164.308(a)(3)(i)，164.308(a)(4)(ii)(A)，164.308(a)(4)(ii)(C)，164.312(a)(1)，164.312(e)；PCI：1.2，1.3，1.2.1，1.3.1，1.3.2，1.3.4，1.3.6，2.2；
ams-nist-cis-ec2-managedinstance-association-compliance-status-check	EC2	組態變更	報告	CIS：CIS.12，CIS.9；NIST-CSF：PR.AC-3，PR.AC-4，PR.AC-5，PR.PT-3，PR.PT-4；HIPAA：164.308(a)(3)(i)，164.308(a)(4)(ii)(A)，164.308(a)(4)(ii)(C)，164.312(e)(1)；PCI：1.2，1.3，1.2.1，1.3.1，1.3.3.2，1.3.4，1.3.6，2.2；
ams-nist-cis-ec2-managedinstance-patch-compliance-status-check	EC2	組態變更	報告	CIS：CIS.2，CIS.5；NIST-CSF：ID.AM-2，PR.IP-1；HIPAA：164.308(a)(5)(ii)(B)；PCI：6.2；

規則名稱	服務	觸發條件	動作	架構
ams-nist-cis-ec2-stopped-instance	EC2	定期	報告	CIS：CIS.2；NIST-CSF：ID.AM-2，PR.IP-1；HEAA：NA；PCI：NA；
ams-nist-cis-ec2-volume-inuse-check	EC2	組態變更	報告	順式：CIS.2；NIST-CSF：PR.IP-1；HEAA：NA；PCI：NA；
ams-nist-cis-efs-encrypted-check	EFS	定期	報告	CIS：CIS.13，CIS.14；NIST-CSF：PR.DS-1；HIPAA：164.312(a)(2)(iv)、164.312(e)(2)(ii)；PCI：3.4，8.2.1；
ams-nist-cis-eip-attached	EC2	組態變更	報告	CIS：CIS.13，CIS.14；NIST-CSF：PR.DS-1；HIPAA：164.312(a)(2)(iv)、164.312(e)(2)(ii)；PCI：3.4，8.2.1；
ams-nist-cis-elasticache-redis-cluster-automatic-backup-check	ElastiCache	定期	報告	CIS：CIS.10；NIST-CSF：ID.BE-5，PR.DS-4，PR.IP-4，PR.PT-5，RC.RP-1；HIPAA：164.308(a)(7)(i)、164.308(a)(7)(ii)(A)、164.308(a)(7)(ii)(B)；PCI：NA；
ams-nist-cis-opensearch-encrypted-at-rest	OpenSearch	定期	報告	CIS：CIS.14，CIS.13；NIST-CSF：PR.DS-1；HIPAA：164.312(a)(2)(iv)、164.312(e)(2)(ii)；PCI：3.4，8.2.1；

規則名稱	服務	觸發條件	動作	架構
ams-nist-cis-opensearch-in-vpc-only	OpenSearch	定期	報告	CIS：CIS.13，CIS.14；NIST-CSF：PR.DS-1；HIPAA：164.312(a)(2)(iv)、164.312(e)(2)(ii)；PCI：3.4，8.2.1；
ams-nist-cis-elb-acm-certificate-required	Certificate Manager	組態變更	報告	CIS：CIS.12，CIS.9；NIST-CSF：PR.AC-3，PR.AC-4，PR.AC-5，PR.DS-5，PR.PT-3，PR.PT-4；HIPAA：164.308(a)(3)(i)，164.308(a)(4)(ii)(A)，164.308(a)(4)(ii)(C)，164.312(a)(1)，164.312(e)(1)；PCI：1.2，1.3，1.2.1，1.3.1，1.3.2，1.3.3.4，1.3.6，2.2；
ams-nist-elb-deletion-protection-enabled	ELB	組態變更	報告	CIS：CIS.13，CIS.14；NIST-CSF：PR.DS-2；HIPAA：164.312(a)(2)(iv)、164.312(e)(1)、164.312(e)(2)(i)、164.312(e)(2)(ii)；PCI：4.1，8.2.1；
ams-nist-cis-elb-logging-enabled	ELB	組態變更	報告	CIS：CIS.6；NIST-CSF：DE.AE-1，DE.AE-3，PR.PT-1；HIPAA：164.312(b)；PCI：10.1，10.3.1，10.3.2，10.3.310.3.4，10.3.5，10.3.6，，10.5.4；

規則名稱	服務	觸發條件	動作	架構
ams-nist-cis-emr-kerberos-enabled	EMR	定期	報告	CIS：CIS.6；NIST-CSF：DE.AE-1，DE.AE-3，PR.PT-1；HIPAA：164.312(b)；PCI：10.1，10.3.1，10.3.2，10.3.310.3.4，10.3.5，10.3.6，，10.5.4；
ams-nist-cis-emr-master-no-public-ip	EMR	定期	報告	CIS：CIS.14，CIS.16；NIST-CSF：PR.AC-1，PR.AC-4，PR.AC-6；HIPAA：164.308(a)(3)(i)，164.308(a)(3)(ii)(A)，164.308(a)(3)(ii)(B)，164.308(a)(4)(i)，164.308(a)(4)(ii)(B)，164.308(a)(4)(ii)(c)(C)，164.312(a)；PCI：7.2.1；
ams-nist-cis-encrypted-volumes	EBS	組態變更	報告	CIS：CIS.12，CIS.9；NIST-CSF：PR.AC-3，PR.AC-4，PR.AC-5，PR.PT-3，PR.PT-4；HIPAA：164.308(a)(3)(i)，164.308(a)(4)(ii)(A)，164.308(a)(4)(ii)(C)，164.312(e)(1)；PCI：1.2，1.3，1.2.1，1.3.1，1.3.3.2，1.3.4，1.3.6，2.2；

規則名稱	服務	觸發條件	動作	架構
ams-nist-cis-guardduty-non-archived-findings	GuardDuty	定期	報告	CIS：CIS.12，CIS.13，CIS.16，CIS.19，CIS.3，CIS.4，CIS.6，CIS.8；NIST-CSF：DE.AE-2，DE.AE-3，DE.CM-4，DE.DP-5，ID.RA-1，ID.RA-3，PR.DS-5，PR.PT-1；HIPAA：164.308(a)(5)(ii)(C)，164.308(a)(6)(ii)，164.312(b)；PCI：6.1，11.4，5.1.2；
ams-nist-iam-group-has-users-check	IAM	組態變更	報告	CIS：NA；NIST-CSF：PR.AC-4，PR.AC-1；HIPAA：164.308(a)(3)(i)，164.308(a)(3)(ii)(A)，164.308(a)(3)(ii)(B)，164.308(a)(4)(ii)(i)，164.308(a)(4)(ii)(B)，164.308(a)(4)(ii)(C)，164.312(a)(1)；PCI：7.1.2，7.1.3，7.2.1)；
ams-nist-cis-iam-policy-no-statements-with-admin-access	IAM	組態變更	報告	CIS：CIS.16；NIST-CSF：PR.AC-6，PR.AC-7；HIPAA：164.308(a)(4)(ii)(B)，164.308(a)(5)(ii)(D)，164.312(d)；PCI：8.2.3，8.2.4，8.2.5；

規則名稱	服務	觸發條件	動作	架構
ams-nist-cis-iam-user-group-membership-check	IAM	組態變更	報告	CIS：CIS.16，CIS.4；NIST-CSF：PR.AC-1，PR.AC-4，PR.PT-3；HIPAA：164.308(a)(3)(i)，164.308(a)(4)(ii)(A)，164.308(a)(4)(ii)(B)，164.308(a)(4)(ii)(C)，164.312(a)(1)，164.312(a)(2)(i)；PCI：2.2，7.1.2，7.2.1，8.1；
ams-nist-cis-iam-user-no-policies-check	IAM	組態變更	報告	CIS：CIS.16；NIST-CSF：PR.AC-1，PR.AC-7；HIPAA：164.308(a)(4)(ii)(B)，164.312(d)；PCI：8.3；
ams-nist-cis-iam-user-unused-credentials-check	IAM	定期	報告	CIS：CIS.16；NIST-CSF：PR.AC-1，PR.AC-4，PR.PT-3；HIPAA：164.308(a)(3)(i)，164.308(a)(3)(ii)(A)，164.308(a)(3)(ii)(B)，164.308(a)(4)(i)，164.308(a)(4)(ii)(B)，164.308(a)(4)(ii)(C)，164.312(a)；PCI：2.2，7.1.2，7.13，7.2.2；

規則名稱	服務	觸發條件	動作	架構
ams-nist-cis-ec2-instances-in-vpc	EC2	組態變更	報告	CIS：CIS.11，CIS.12，CIS.9；NIST-CSF： DE.AE-1，PR.AC-3，PR.AC-5，PR.PT-4；HIPAA： 164.308(a)(3)(i)，164.308(a)(3)(ii)(B)，164.308(a)(4)(i)，164.308(a)(4)(ii)(A)，164.308(a)(4)(ii)(C)，164.312(a)(1)，164.312(e)(1)；PCI：1.2，1.3，2.2.2
ams-nist-cis-internet-gateway-authorized-vpc-only	網際網路閘道	定期	報告	CIS：CIS.9，CIS.12；NIST-CSF：NA；HEAA：NA；PCI：NA；
ams-nist-cis-kms-cmk-not-scheduled-for-deletion	KMS	定期	報告	CIS：CIS.13，CIS.14；NIST-CSF：PR.DS-1；HEAA：NA；PCI：3.5，
ams-nist-lambda-concurrency-check	Lambda	組態變更	報告	CIS：NA；NIST-CSF：NA；HIPAA：164.312(b)；PCI：NA；
ams-nist-lambda-dlq-check	Lambda	組態變更	報告	CIS：NA；NIST-CSF：NA；HIPAA：164.312(b)；PCI：NA；

規則名稱	服務	觸發條件	動作	架構
ams-nist-cis-lambda-function-public-access-prohibited	Lambda	組態變更	報告	CIS：CIS.12，CIS.9；NIST-CSF：PR.AC-3，PR.AC-4，PR.ACPR.DS-5，PR.PT-3，PR.PT-4；HIPAA：164.308(a)(3)(i)，164.308(a)(4)(ii)(A)，164.308(a)(4)(ii)(C)，164.312(a)(1)，164.312(e)(1)；PCI：1.2，1.3，1.2.1，1.3.1，1.3.2.4，2.2；
ams-nist-cis-lambda-inside-vpc	Lambda	組態變更	報告	CIS：CIS.12，CIS.9；NIST-CSF：PR.AC-3，PR.AC-4，PR.AC-5，PR.PT-3，PR.PT-4；HIPAA：164.308(a)(3)(i)，164.308(a)(4)(ii)(A)，164.308(a)(4)(ii)(C)，164.312(a)(1)，164.312(e)(1)；PCI：1.2，1.3，1.2.1，1.3.1，1.3.3.2，1.3.4，2.2；
ams-nist-cis-mfa-enabled-for-iam-console-access	IAM	定期	報告	CIS：CIS.16；NIST-CSF：PR.AC-7；HIPAA：164.312(d)；PCI：2.2，8.3；

規則名稱	服務	觸發條件	動作	架構
ams-nist-cis-multi-region-cloudtrail-enabled	CloudTrail	定期	報告	CIS：CIS.6；NIST-CSF：DE.AE-1，DE.AE-3，PR.DS-5，PR.MA-2，PR.PT-1；HIPAA：164.308(a)(3)(ii)(A)，164.312(b)；PCI：2.2，10.1，10.2.1、10.2.2、10.2.3、10.2.4、10.2.510.2.6、10.2.7、、10.3.1、10.3.2、10.3.3、10.3.4、10.3.510.3.6；
ams-nist-rds-enhanced-monitoring-enabled	RDS	組態變更	報告	CIS：NA；NIST-CSF：PR.PT-1；HIPAA：164.312(b)；PCI：NA；
ams-nist-cis-rds-instance-public-access-check	RDS	組態變更	報告	CIS：CIS.12，CIS.14，CIS.9；NIST-CSF：PR.AC-3，PR.AC-4，PR.AC-5，PR.DS-5，PR.PT-3，PR.PT-4；HIPAA：164.308(a)(3)(i)，164.308(a)(4)(ii)(A)，164.308(a)(4)(ii)(C)，164.312(a)(1)，164.312(e)(1)；PCI：1.2，1.3，1.2.1，1.3.1，1.3.2，1.3.4，1.3.6，2.2；

規則名稱	服務	觸發條件	動作	架構
ams-nist-rds-multi-az-support	RDS	組態變更	報告	CIS：NA；NIST-CSF：ID.BE-5，PR.DS-4，PR.PT-5，RC.RP-1；HIPAA：164.308(a)(7)(i)，164.308(a)(7)(ii)(C)；PCI：NA；
ams-nist-cis-rds-snapshots-public-prohibited	RDS	組態變更	報告	CIS：CIS.12，CIS.14，CIS.9；NIST-CSF：PR.AC-3，PR.AC-4，PR.AC-5，PR.DS-5，PR.PT-3，PR.PT-4；HIPAA：164.308(a)(3)(i)，164.308(a)(4)(ii)(A)，164.308(a)(4)(ii)(C)，164.312(a)(1)，164.312(e)(1)；PCI：1.2，1.3，1.2.1，1.3.1，1.3.2，1.3.4，1.3.6，2.2；
ams-nist-cis-rds-storage-encrypted	RDS	組態變更	報告	CIS：CIS.13、CIS.5、CIS.6；NIST-CSF：DE.AE-1、DE.AE-3、PR.DS-1、PR.PT-1；HIPAA：164.312(a)(2)(iv)、164.312(b)、164.312(e)(2)(ii)；PCI：3.4，10.1、10.2.1、10.2.310.2.2、、10.2.4、10.2.5、10.3.1、10.3.2、10.3.3、10.3.4、、10.3.5、、10.3.6、8.2.1；

規則名稱	服務	觸發條件	動作	架構
ams-nist-cis-redshift-cluster-configuration-check	RedShift	組態變更	報告	CIS：CIS.6，CIS.13，CIS.5；NIST-CSF：DE.AE-1，DE.AE-3，PR.DS-1，PR.PT-1；HIPAA：164.312(a)(2)(iv)，164.312(b)，164.312(e)(2)(ii)；PCI：3.4，8.2.1，10.1，10.2.1、10.2.2、10.2.3、10.2.4、10.2.5、、10.3.1、10.3.3、10.3.2、10.3.410.3.5、10.3.6；
ams-nist-cis-redshift-cluster-public-access-check	RedShift	組態變更	報告	CIS：CIS.12，CIS.14，CIS.9；NIST-CSF：PR.AC-3，PR.AC-4，PR.AC-5，PR.DS-5，PR.PT-3，PR.PT-4；HIPAA：164.308(a)(3)(i)，164.308(a)(4)(ii)(A)，164.308(a)(4)(ii)(C)，164.312(a)(1)，164.312(e)(1)；PCI：1.2，1.3，1.2.1，1.3.1，1.3.2，1.3.4，1.3.6，2.2；
ams-nist-cis-redshift-require-tls-ssl	RedShift	定期	報告	CIS：CIS.13，CIS.14；NIST-CSF：PR.DS-2；HIPAA：164.312(a)(2)(iv)、164.312(e)(1)、164.312(e)(2)(i)、164.312(e)(2)(ii)；PCI：2.3，4.1；

規則名稱	服務	觸發條件	動作	架構
ams-nist-cis-root-account-hardware-mfa-enabled	IAM	定期	報告	CIS：CIS.16，CIS.4；NIST-CSF：PR.AC-7；HIPAA：164.312(d)；PCI：2.2，8.3；
ams-nist-cis-root-account-mfa-enabled	IAM	定期	報告	CIS：CIS.16，CIS.4；NIST-CSF：PR.AC-7；HIPAA：164.312(d)；PCI：2.2，8.3；
ams-nist-cis-s3-bucket-default-lock-enabled	S3	組態變更	報告	CIS：CIS.14，CIS.13；NIST-CSF：ID.BE-5，PR.PT-5，RC.RP-1；HEAA：NA；PCI：NA；
ams-nist-cis-s3-bucket-logging-enabled	S3	組態變更	報告	CIS：CIS.6；NIST-CSF：DE.AE-1，DE.AE-3，PR.DS-5，PR.PT-1；HIPAA：164.308(a)(3)(ii)(A)，164.312(b)；PCI：2.2，10.1、10.2.1、10.2.2、10.2.3、10.2.4、10.2.5、10.2.7、10.3.110.3.2、10.3.3、10.3.4、、10.3.5、10.3.6；
ams-nist-cis-s3-bucket-replication-enabled	S3	組態變更	報告	CIS：CIS.10；NIST-CSF：ID.BE-5，PR.DS-4，PR.IP-4，PR.PT-5，RC.RP-1；HIPAA：164.308(a)(7)(i)、164.308(a)(7)(ii)(A)、164.308(a)(7)(ii)(B)；PCI：2.2，10.5.3；

規則名稱	服務	觸發條件	動作	架構
ams-nist-cis-s3-bucket-ssl-requests-only	S3	組態變更	報告	CIS：CIS.13，CIS.14；NIST-CSF：PR.DS-2；HIPAA：164.312(a)(2)(iv)、164.312(c)(2)、164.312(e)(1)、164.312(e)(2)(i)、164.312(e)(2)(ii)；PCI：2.2，4.1，8.2.1；
ams-nist-cis-s3-bucket-versioning-enabled	S3	定期	報告	CIS：CIS.10；NIST-CSF：ID.BE-5，PR.DS-4，PR.DS-6，PR.IP-4，PR.PT-5，RC.RP-1；HIPAA：164.308(a)(7)(i)，164.308(a)(7)(ii)(A)，164.308(a)(7)(ii)(B)，164.312(c)(1)，164.312(c)(2)；PCI：10.5.3；
ams-nist-cis-sagemaker-endpoint-configuration-kms-key-configured	SageMaker	定期	報告	CIS：CIS.13，CIS.14；NIST-CSF：PR.DS-1；HIPAA：164.312(a)(2)(iv)、164.312(e)(2)(ii)；PCI：3.4，8.2.1；
ams-nist-cis-sagemaker-notebook-instance-kms-key-configured	SageMaker	定期	報告	CIS：CIS.13，CIS.14；NIST-CSF：PR.DS-1；HIPAA：164.312(a)(2)(iv)、164.312(e)(2)(ii)；PCI：3.4，8.2.1；

規則名稱	服務	觸發條件	動作	架構
ams-nist-cis-sagemaker-notebook-no-direct-internet-access	SageMaker	定期	報告	CIS：CIS.12，CIS.9；NIST-CSF：PR.AC-3，PR.AC-4，PR.ACPR.DS-5，PR.PT-3，PR.PT-4；HIPAA：164.308(a)(3)(i)，164.308(a)(4)(ii)(A)，164.308(a)(4)(ii)(C)，164.312(a)(1)，164.312(e)(1)；PCI：1.2，1.3，1.2.1，1.3.1，1.3.1，1.3.2，1.3.4，1.3.6，2.2；
ams-nist-cis-secretsmanager-rotation-enabled-check	Secrets Manager	組態變更	報告	CIS：CIS.16；NIST-CSF：PR.AC-1；HIPAA：164.308(a)(4)(ii)(B)；PCI：NA；
ams-nist-cis-secretsmanager-scheduled-rotation-success-check	Secrets Manager	組態變更	報告	CIS：CIS.16；NIST-CSF：PR.AC-1；HIPAA：164.308(a)(4)(ii)(B)；PCI：NA；
ams-nist-cis-sns-encrypted-kms	SNS	組態變更	報告	CIS：CIS.13、CIS.14；NIST-CSF：PR.DS-1；HIPAA：164.312(a)(2)(iv)、164.312(e)(2)(ii)；PCI：8.2.1；

規則名稱	服務	觸發條件	動作	架構
ams-nist-cis-vpc-sg-open-only-to-authorized-ports	VPC	組態變更	報告	CIS：CIS.11、CIS.12、CIS.9；NIST-CSF：DE.AE-1、PR.AC-3、PR.AC-5、PR.PT-4；HIPAA：164.312(e)(1)；PCI：1.2、1.3、1.2.1、1.3.1、1.3.2、2.2.2；
ams-nist-vpc-vpn-2-tunnels-up	VPC	組態變更	報告	CIS：NA；NIST-CSF：ID.BE-5，PR.DS-4，PR.PT-5，RC.RP-1；HIPAA：164.308(a)(7)(i)；PCI：NA；
ams-cis-ec2-ebs-encryption-by-default	EC2	定期	報告	CIS：CIS.13，CIS.14；NIST-CSF：PR.DS-1；HIPAA：164.312(a)(2)(iv)、164.312(e)(2)(ii)；PCI：2.2，3.4，8.2.1；
ams-cis-rds-snapshot-encrypted	RDS	組態變更	報告	CIS：CIS.13，CIS.14；NIST-CSF：PR.DS-1；HIPAA：164.312(a)(2)(iv)、164.312(e)(2)(ii)；PCI：3.4，8.2.1；
ams-cis-redshift-cluster-maintenance settings-check	RedShift	組態變更	報告	CIS：CIS.5；NIST-CSF：PR.DS-4，PR.IP-1，PR.IP-4；HIPAA：164.308(a)(5)(ii)(A)，164.308(a)(7)(ii)(A)；PCI：6.2；

在 Accelerate 中回應違規

所有組態規則違規都會出現在您的組態報告中。這是通用回應。根據規則的修復類別（嚴重性），AMS 可能會採取其他動作，摘要如下表所示。如需如何為特定規則自訂動作程式碼的詳細資訊，請參閱 自訂問題清單回應。

修復動作

動作代碼	AMS 動作
Report	1. 新增至 Config 報告
Incident	1. 新增至 Config 報告 2. Accelerate 中的自動事件報告
Remediate	1. 新增至 Config 報告 2. Accelerate 中的自動事件報告 3. Accelerate 中的自動修復

請求其他說明

> **Note**
>
> AMS 可以為您修復任何違規，無論其修復類別為何。若要請求協助，請提交服務請求，並指出您希望 AMS 使用「作為 AMS 設定規則修復的一部分」等評論來修復哪些資源，請修復非投訴資源 *RESOURCE_ARNS_OR_IDs* 資源 ARNs/IDs>，在帳戶中設定規則 *CONFIG_RULE_NAME*，並新增必要的輸入來修復違規。

AMS Accelerate 具有 AWS Systems Manager 自動化文件和 Runbook 的程式庫，可協助修復不合規的資源。

新增至 Config 報告

AMS 會產生 Config 報告，追蹤您帳戶中所有規則和資源的合規狀態。您可以從 CSDM 請求報告。您也可以從 AWS Config 主控台、 AWS CLI 或 AWS Config API 檢閱合規狀態。您的 Config 報告包括：

- 在您的環境中發現潛在威脅和設定錯誤的首要不合規資源

- 一段時間內資源和組態規則的合規
- 設定規則描述、規則嚴重性，以及修正不合規資源的建議修補步驟

當任何資源進入不合規狀態時，資源狀態（和規則狀態）會在您的 Config 報告中變成不合規。如果規則屬於 Config Report Only 修復類別，根據預設，AMS 不會採取進一步動作。您可以隨時建立服務請求，向 AMS 請求其他協助或修復。

如需詳細資訊，請參閱AWS 組態報告。

Accelerate 中的自動事件報告

對於中度嚴重的規則違規，AMS 會自動建立事件報告，通知您資源已進入不合規狀態，並詢問您要執行的動作。在回應事件時，您有下列選項：

- 請求 AMS 修復事件中列出的不合規資源。然後，我們會嘗試修復不合規的資源，並在解決基礎事件後通知您。
- 您可以在 主控台或透過自動化部署系統（例如 CI/CD 管道範本更新）手動解決不合規項目；然後，您可以解決事件。不合規資源會根據規則的排程重新評估，如果資源評估為不合規，則會建立新的事件報告。
- 您可以選擇不解析不合規資源，只解析事件。如果您稍後更新資源的組態， AWS Config 會觸發重新評估，並再次提醒您評估該資源的不合規情況。

Accelerate 中的自動修復

最關鍵的規則屬於 Auto Remediate 類別。不遵守這些規則可能會嚴重影響帳戶的安全性和可用性。當資源違反下列其中一個規則時：

1. AMS 會自動透過事件報告通知您。
2. AMS 使用我們的自動化 SSM 文件開始自動化修復。
3. AMS 會在自動修復成功或失敗時更新事件報告。
4. 如果自動修復失敗，AMS 工程師會調查問題。

在 Accelerate 中建立規則例外狀況

AWS Config 規則 資源例外狀況功能可讓您針對特定規則禁止報告特定、不合規的資源。

> **Note**
>
> 豁免的資源仍會在您的 Config Service AWS 主控台中顯示為不合規。豁免的資源會在 Config 報告 (resource_exception：True) 中出現特殊旗標。產生報告時，您的 CSDMs 可以根據該資料欄篩選掉這些資源。

如果您有已知不合規的資源，您可以在其組態報告中消除特定組態規則的特定資源。若要執行此作業：

提交服務請求以針對您的帳戶加速，其中包含要從報告中排除的組態規則和資源清單。您必須提供明確的業務理由（例如，不需要報告未備份 *resource_name_1* 和 *resource_name_2*，因為我們不希望備份它們）。如需提交 Accelerate 服務請求的說明，請參閱 在 Accelerate 中建立服務請求。

將下列輸入（針對每個資源新增包含所有必要欄位的個別區塊，如下所示）貼到請求中，然後提交：

```
[
    {
        "resource_name": "resource_name_1",
        "config_rule_name": "config_rule_name_1",
        "business_justification": "REASON_TO_EXEMPT_RESOURCE",
        "resource_type": "resource_type"
    },
    {
        "resource_name": "resource_name_2",
        "config_rule_name": "config_rule_name_2",
        "business_justification": "REASON_TO_EXEMPT_RESOURCE",
        "resource_type": "resource_type"
    }
]
```

降低 Accelerate 中的 AWS Config 成本

您可以使用 選項定期記錄`AWS::EC2::Instance`資源類型，以減少 AWS Config 成本。定期記錄會每 24 小時擷取一次資源的最新組態變更，減少交付的變更數量。啟用時， AWS Config 只會在 24 小時期間結束時記錄資源的最新組態。這可讓您根據特定營運規劃、合規和稽核使用案例量身打造組態資料，而不需要持續監控。只有在您有依賴暫時性架構的應用程式時，才建議進行此變更，這表示您持續擴展或縮減執行個體的數量。

若要選擇加入`AWS::EC2::Instance`資源類型的定期記錄，請聯絡您的 AMS 交付團隊。

自訂問題清單回應

您可以選擇您希望 AMS Accelerate 如何回應某些問題清單（不合規的 Config 規則）。您可以設定 AMS 來回應問題清單，方法是修復問題清單、請求您的核准進行修復，或在下一次的每月商業審查 (MBR) 中向您報告。您可以變更 AMS Accelerate Config 規則的預設回應。若要查看規則，請前往組態合規 > 規則表，或將規則表下載為 ZIP 檔案 ams_config_rules.zip。

變更預設回應可讓您修復更多問題清單，以協助您提高帳戶的安全性和合規狀態。當您修復更多問題清單時，需要等待手動檢閱和核准的案例較少。廣泛的 AMS 修復 Runbook 程式庫會持續修正不合規的資源，而且只會在需要時與您聯絡。

自訂回應只會與新資源或具有新事件的現有資源搭配使用。例如，在變更後變成不合規的資源。這是因為較舊的資源在修復之前往往需要更深入的檢查，並且更容易在建立或變更資源修復時強制執行資源修復。若要隨時請求修復任何資源的問題清單，請提交服務請求。

請求變更預設回應

雲端架構師 (CAs) 會在加入期間與您合作，以收集您的偏好設定。CAs 接著會在內部 AMS 系統上設定初始組態。加入後，建立服務請求以請求更新組態。您可以視需要請求任意次數的組態更新。請注意，操作只會更新建立服務請求之帳戶的組態。如果您需要同時更新多個帳戶，請聯絡您的 Cloud Architect。您的 CA 會要求您使用偏好設定來剪下服務請求，以供稽核之用。

變更問題清單和帳戶的預設回應

您一律需要每個帳戶和調查結果的回應偏好設定。AMS 提供預設回應（請參閱組態合規），因此此組態是選用的。您可以將每個問題清單的預設回應變更為下列選項：

- 修復：AMS 手動或自動修復問題清單。AMS 會檢閱修復，並讓您知道是否失敗。
- 請求核准：AMS 會建立傳出案例，以通知您調查結果。當您想要在核准或排除問題清單之前檢閱問題清單時，請使用此選項。AMS 接著會執行您偏好的動作。
- 無動作（僅限報告）：AMS 不採取任何動作來修復或呈報問題清單。問題清單可能仍然會出現在主控台上，以及在 MBRs期間呈現的報告。

> **Note**
>
> 您無法變更 AMS 必須修復的規則組態。例如，啟用 Amazon GuardDuty 和 VPC 流程日誌。

依資源變更預設回應

您可以使用標籤進一步設定對特定資源的回應。您可以使用預先存在的標籤，或使用 Resource Tagger 標記資源。如需詳細資訊，請參閱 加速資源交錯)。具有標籤的資源組態優先於問題清單的預設動作。當資源具有多個具有不同關聯組態的標籤時，AMS 無法執行自訂修復。反之，AMS 會傳送傳出服務請求給您，通知您此情況。例如，對於 s3-bucket-server-side-encryption-enabled 調查結果，您可以：

- 使用標籤鍵值對 "Regulated： True" 將回應變更為 'remediate' unencrypted S3 儲存貯體
- 當未加密的 S3 儲存貯體具有 "Regulated： False" 標籤時，將回應變更為「no action」，以及
- 將未加密 S3 儲存貯體的預設回應變更為「請求核准」。這適用於所有沒有「管制：True」或「管制：False」標籤的 S3 儲存貯體

您也可以新增執行自訂問題清單回應所需的輸入。例如，對於需要加密金鑰的修復，您可以將金鑰 IDs 提供給 AMS。您可以變更修復 Runbook 的輸入參數，但 AMS 不支援與自訂 Runbook 整合。如需 Config 報告中 AMS 修復 Runbook 的說明，請參閱 AWS Config 控制合規報告。

Accelerate 中的事件回應

收到提醒時，AMS 團隊會使用自動化和手動修補，將資源恢復為正常運作狀態。如果修復失敗，AMS 會啟動事件管理程序，以與您的團隊協作。您可以透過更新組態檔案中的預設組態來變更基準。

AMS Accelerate 中的事件回應和加入

在加入期間，AMS Accelerate 會隱藏現有不合規資源的自動事件建立；反之，您的 Cloud Service Deliver Manager (CSDM) 會提供一份報告，其中包含所有不合規規則和資源供您檢閱。在您識別您希望 AMS 修復的規則之後，請在 支援 中心主控台中建立服務請求，指出這些規則和資源。下列服務請求範本是客戶向 AMS 請求以手動修復不合規資源的範例。如果 AMS 有其他問題，我們會在服務請求中與您合作，以收集所需的資訊。

```
Hello,
Please remediate the following resources for the Config Rule "ENCRYPTED_VOLUMES".
Resource List:
    "Vol-12345678"
    "Vol-87654312"
Thank you
```

加入程序完成後，AMS Accelerate 會自動為標示為自動事件之規則的每個不合規資源建立事件。

Accelerate 中的彈性

AWS 全球基礎設施是以 AWS 區域 和 可用區域為基礎建置。 AWS 區域 提供多個實體隔離和隔離的可用區域，這些區域與低延遲、高輸送量和高度備援的聯網連接。透過可用區域，您可以設計和操作在區域之間自動容錯移轉的應用程式和資料庫，而不會中斷。相較於傳統的單一或多個資料中心基礎設施，可用區域具有更高的可用性、容錯能力和可擴展性。

如需 AWS 區域 和可用區域的詳細資訊，請參閱 AWS 全球基礎設施。

如需 AMS Accelerate 持續性管理的資訊，請參閱 AMS Accelerate 中的持續性管理。

end-of-support作業系統的安全控制

在作業系統製造商「end-of-support」或 EOS 一般支援期間之外且未收到安全更新的作業系統，會有更高的安全風險。

AWS 提供一些 服務，以協助處理end-of-support作業系統。如需 Windows end-of-support的相關資訊，請參閱 Windows Server End-of-Support遷移計劃。

> **Note**
>
> 如需本主題的其他資訊，請參閱 AWS Artifact 報告。如需詳細資訊，請參閱在 AWS Artifact 中下載報告。若要存取 AWS Artifact，您可以聯絡 CSDM 以取得指示，或前往 AWS Artifact 入門。此資訊不包含在本使用者指南中，因為它包含敏感的安全內容。

Accelerate 中的安全最佳實務

AMS Accelerate 使用一致性套件，提供一般用途的合規架構，可讓您使用受管或自訂 AWS Config 規則 和 AWS Config 修補動作來建立安全、營運或成本最佳化控管檢查。如需如何最佳設定這些一致性套件的資訊，請參閱 NIST CSF AWS Config的操作最佳實務和 CIS 前 20 名的操作最佳實務。 https://docs.aws.amazon.com/config/latest/developerguide/operational-best-practices-for-nist-csf.html

變更請求安全性審查

AWS Managed Services 變更請求審核程序可確保 AMS 在代表您在帳戶中實作請求的變更時，對請求的變更執行安全審核。

AMS Accelerate 技術標準 定義最低安全標準、組態和程序，以建立帳戶的基準安全性。當 AMS 實作請求的變更時，我們會遵循這些標準。

AMS 會根據 AMS 技術標準評估所有變更請求。任何可能因為偏離技術標準而降低您帳戶安全性狀態的變更都會經過安全性審查程序。在此過程中，AMS 會反白顯示相關風險，並由您授權的風險核准者審查和核准，以平衡安全和業務需求。

客戶安全風險管理程序

AMS Accelerate Customer Security Risk Management (CSRM) 程序有助於清楚地識別風險，並向正確的擁有者傳達風險。此程序可將您環境中的安全風險降至最低，並減少已識別風險的持續營運開銷。

根據預設，當組織的人員請求 AMS 對您的受管環境實作變更時，AMS 會檢閱變更，以判斷請求是否超出技術標準，這可能會改變您帳戶的安全狀態。如果安全風險很高或非常高，則您的授權安全人員會接受或拒絕變更審查。也會評估請求的變更，是否對 AMS 操作帳戶的能力造成負面影響。如果審查發現可能的負面影響，則需要在 AMS 內進行額外的審查和核准。

對於高風險或極高風險，您可以在 CSRM 程序中選擇退出核准型工作流程。若要將特定帳戶的 CSRM 選項從標準 CSRM 變更為僅限通知，請與您的 Cloud Service Delivery Manager 合作，建立一次性風險接受。如果您選擇繼續僅通知選項，則無論風險類別為何，AMS 都會實作請求的變更。此外，AMS 會向您的授權風險核准者傳送風險通知，而不是在變更實作之前尋求核准。如需 AMS CSRM 程序、如何在加入新的 AMS 帳戶時變更預設 CSRM 選項，或如何更新現有帳戶的詳細資訊，請洽詢您的 Cloud Architects 或 Cloud Service Delivery Manager。

> **Note**
>
> AMS 強烈建議您在所有帳戶中使用標準 CSRM 的預設選項。

AMS Accelerate 技術標準

以下是加速技術標準類別：

ID	類別
AMS-STD-X002	AWS Identity and Access Management
AMS-STD-X003	網路安全
AMS-STD-X004	滲透測試

ID	類別
AMS-STD-X005	Amazon GuardDuty
AMS-STD-X007	日誌

AMS Accelerate 中的標準控制項

以下是 AMS 中的標準控制項：

AMS-STD-X002 - AWS Identity and Access Management (IAM)

ID	技術標準
1.0	逾時持續時間
1.1	聯合身分使用者預設逾時工作階段為一小時，最多可增加四個小時。
1.2	Microsoft Windows Server 的 RDP 工作階段逾時設定為 15 分鐘，可根據使用案例進行擴展。
2.0	AWS 根帳戶用量
2.1	如果根帳戶因任何原因使用，Amazon GuardDuty 必須設定為產生相關調查結果。
2.2	不得建立根帳戶的存取金鑰。
3.0	使用者建立和修改
3.1	可以建立具有程式設計存取和唯讀許可的 IAM 使用者/角色，而不需要任何時間限制政策。不過，不允許許可讀取帳戶中所有 Amazon Simple Storage Service 儲存貯體中的物件（例如 S3：GetObject)。
3.1.1	用於主控台存取和具有唯讀許可的 IAM 人類使用者可以使用時間限制政策（最多 180 天）建

ID	技術標準
	立，而removal/renewal/extension時間限制政策將導致風險通知。不過，不允許讀取帳戶中所有 S3 儲存貯體中物件 （ 例如 S3：GetObject) 的許可。 S3
3.2	在沒有接受風險的情況下，不得在客戶帳戶中建立具有任何基礎設施變更許可 （ 寫入和許可管理 ） 的主控台和程式設計存取的 IAM 使用者和角色。S3 物件層級寫入許可存在例外狀況，只要特定儲存貯體位於非 AMS 相關標籤的範圍和標記操作中，這些許可就可以接受風險。
3.3	在 Microsoft Windows Server 上，僅必須建立 Microsoft 群組受管服務帳戶 (gMSA)。
4.0	政策、動作和 APIs
4.4	政策不得以等同於「效果」：「允許」搭配「動作」：「*」而非「資源」：「*」的陳述式提供管理員存取權，而不接受風險。
4.6	客戶 IAM 政策中不得針對 AMS 基礎設施金鑰對 KMS 金鑰政策進行 API 呼叫。
4.8	不允許對 Amazon Route 53 中的 AMS 基礎設施 DNS 記錄進行變更的動作。
4.9	具有遵循到期程序後建立主控台存取權的 IAM 人類使用者，除了信任政策、擔任角色和時間有限的政策之外，不得直接連接任何政策。
4.10	您可以在相同帳戶中建立具有特定秘密或命名空間讀取存取權 AWS Secrets Manager 的 Amazon EC2 執行個體設定檔。

ID	技術標準
4.12	IAM 政策不得包含任何動作，其中包括在任何 AMS Amazon CloudWatch 日誌群組上允許 log：DeleteLogGroup 和 logs：DeleteLogStream 的動作。
4.13	不允許建立多區域金鑰的許可。
4.14	透過使用服務特定 S3 條件金鑰 s3：ResourceAccount 指定帳戶號碼，即可限制對客戶帳戶存取儲存貯體，藉此提供尚未在客戶帳戶中建立的 S3 儲存貯體 ARN 存取權。
4.15.1	您可以檢視、建立、列出和刪除對 S3 儲存鏡頭自訂儀表板的存取權。
4.16	可以將 SQL Workbench 相關的完整許可授予角色/使用者，以便在 Amazon Redshift 資料庫上運作。
4.17	可將任何 AWS CloudShell 許可授予客戶角色，做為 CLI 的替代方案。
4.18	AWS 服務為信任委託人的 IAM 角色也需要符合 IAM 技術標準。
4.19	服務連結角色 (SLRs) 不受 AMS IAM 技術標準的約束，因為它們是由 IAM 服務團隊建置和維護。
4.20	IAM 政策不應允許讀取帳戶中所有 S3 儲存貯體中的物件 （ 例如 S3：GetObject)。 S3
4.21	資源類型「savingsplan」的所有 IAM 許可都可以授予客戶。

ID	技術標準
4.22	AMS 工程師不得在 Amazon S3、Amazon Relational Database Service、Amazon DynamoDB 等任何資料儲存服務中，或在作業系統檔案系統中手動複製或移動客戶資料（檔案、S3 物件、資料庫等）。 Amazon S3
6.0	跨帳戶政策
6.1	您可以根據客戶記錄設定屬於相同客戶的 AMS 帳戶之間的 IAM 角色信任政策。
6.2	只有在非 AMS 帳戶由相同 AMS 客戶擁有時（透過確認其位於相同 AWS Organizations 帳戶下，或將電子郵件網域與客戶的公司名稱相符），才能設定 AMS 和非 AMS 帳戶之間的 IAM 角色信任政策。
6.3	未經風險接受，不得設定 AMS 帳戶與第三方帳戶之間的 IAM 角色信任政策。
6.4	您可以設定跨帳戶政策，在相同客戶的 AMS 帳戶之間存取任何客戶管理的 CMKs。
6.5	您可以設定跨帳戶政策，以透過 AMS 帳戶存取非 AMS 帳戶中的任何 KMS 金鑰。
6.6	在未接受風險的情況下，不允許跨帳戶政策存取第三方帳戶在 AMS 帳戶中的任何 KMS 金鑰。
6.6.1	只有在非 AMS 帳戶由相同 AMS 客戶擁有時，才能設定跨帳戶政策以存取 AMS 帳戶內的任何 KMS 金鑰。
6.7	您可以設定跨帳戶政策，在相同客戶的 AMS 帳戶之間存取可存放資料的任何 S3 儲存貯體資料或資源（例如 Amazon RDS、Amazon DynamoDB 或 Amazon Redshift)。

ID	技術標準
6.8	可從具有唯讀存取權的 AMS 帳戶存取任何 S3 儲存貯體資料或資源的跨帳戶政策，其中的資料可存放在非 AMS 帳戶中（例如 Amazon RDS、Amazon DynamoDB 或 Amazon Redshift)。
6.9	存取任何 S3 儲存貯體資料或資源的跨帳戶政策（例如 Amazon RDS、Amazon DynamoDB 或 Amazon Redshift)，其具有從 AMS 到非 AMS 帳戶（或非 AMS 到 AMS 帳戶）的寫入許可，只有在非 AMS 帳戶為相同 AMS 客戶所擁有（透過確認其位於相同 AWS Organizations 帳戶或將電子郵件網域與客戶的公司名稱相符）時，才必須設定。
6.10	跨帳戶政策，可從具有唯讀存取權的 AMS 帳戶存取任何 S3 儲存貯體資料或可存放資料的資源（例如 Amazon RDS、Amazon DynamoDB 或 Amazon Redshift)。
6.11	從具有寫入存取權的 AMS 帳戶存取任何 S3 儲存貯體資料或資源（例如 Amazon RDS、Amazon DynamoDB 或 Amazon Redshift) 的跨帳戶政策不得設定。
6.12	在未接受風險的情況下，不得設定來自第三方帳戶的跨帳戶政策來存取可存放資料的 AMS 客戶 S3 儲存貯體或資源 (asAmazon RDS、Amazon DynamoDB 或 Amazon Redshift)。
7.0	User Groups (使用者群組)
7.1	允許具有唯讀和非變動許可的 IAM 群組。
8.0	以資源為基礎的政策

ID	技術標準
8.4	AMS 基礎設施資源應透過附加以資源為基礎的政策，不受未經授權的身分管理。
8.2	除非客戶明確指定不同的政策，否則應使用最低權限的資源型政策來設定客戶資源。

AMS-STD-X003 - 網路安全

以下是 X003 - 網路安全的標準控制項：

ID	技術標準
	聯網
1.0	預留供未來控制
2.0	允許 EC2 執行個體上的彈性 IP
3.0	必須使用 AMS 控制平面和資料平面 TLS 1.2+ 中的延伸。
5.0	如果根據 9.0 未連接到負載平衡器，則安全群組在傳入規則中不得具有 0.0.0.0/0 的來源
6.0	未經風險接受，不得公開 S3 儲存貯體或物件。
7.0	連接埠 SSH/22 或 SSH/2222 （非 SFTP/2222)、TELNET/23、RDP/3389、WinRM/ 5985-5986、VNC/ 5900-5901 TS/CITRIX/1494 或 1604、LDAP/389 或 636 和 RPC/135、N ETBIOS/137-139 上的伺服器管理存取權不得透過安全群組從 VPC 外部進行。
8.0	連接埠 (MySQL/3306、PostgreSQL/5432 、Oracle/1521、MSSQL/1433) 或自訂連接埠上的資料庫管理存取權，不得允許來自未透過

ID	技術標準
	DX、VPC 對等或 VPN 透過安全群組路由至 VPC 的公IPs。
8.1	任何可存放客戶資料的資源都不應直接公開至公有網際網路。
9.0	透過連接埠 HTTP/80、HTTPS/8443 和 HTTPS/443 從網際網路存取的直接應用程式僅允許載入平衡器，但不允許直接存取任何運算資源，例如 EC2 執行個體、ECS/EKS/Fargate 容器等。
10.0	允許從客戶私有 IP 範圍透過連接埠 HTTP/80 和 HTTPS/443 存取應用程式。
11.0	未經風險接受，不得允許對控制 AMS 基礎設施存取的安全群組進行任何變更。
12.0	每次請求將安全群組連接到執行個體時，AMS Security 都會參考標準。
14.0	只有在相同 AMS 客戶擁有非 AMS 帳戶時（透過確認它們位於相同的 AWS Organization 帳戶下，或將電子郵件網域與客戶的公司名稱相符），才能使用內部工具，設定私有託管區域與 VPCs 從 AMS 到非 AMS 帳戶（或非 AMS 到 AMS 帳戶）的跨帳戶關聯。
15.0	您可以允許屬於相同客戶之帳戶之間的 VPC 對等互連。
16.0	AMS 基礎 AMIs 可以使用內部工具與非 AMS 帳戶共用，只要這兩個帳戶都由相同客戶擁有（透過確認他們位於相同 AWS Organizations 帳戶下，或將電子郵件網域與客戶的公司名稱相符）。

ID	技術標準
17.0	未經風險接受，不得在任何安全群組中設定 FTP 連接埠 21。
18.0	只要客戶擁有所有帳戶，就可以透過傳輸閘道進行跨帳戶網路連線。
19.0	不允許將私有子網路設為公有
20.0	不允許與第三方帳戶（非客戶擁有）建立 VPC 互連連線。
21.0	不允許透過第三方帳戶（非客戶擁有）連接 Transit Gateway。
22.0	AMS 為客戶提供服務所需的任何網路流量，不得在客戶網路輸出點遭到封鎖。
23.0	從客戶基礎設施向 Amazon EC2 發出的傳入 ICMP 請求將需要風險通知。
24.0	允許透過 DX、VPC 對等或 VPN 透過安全群組路由至 Amazon VPC 的公IPs 傳入請求。
25.0	未透過 DX、VPC 對等或 VPN 透過安全群組路由至 Amazon VPC 的公IPs 傳入請求需要接受風險。
26.0	允許從 Amazon EC2 到任何目的地的傳出 ICMP 請求。
27.0	安全群組共用
27.1	如果安全群組符合此安全標準，則可以在相同帳戶中VPCs 和相同組織中的 帳戶之間共用。

ID	技術標準
27.2	如果安全群組不符合此標準，且此安全群組先前需要接受風險，則不允許在相同帳戶中的 VPCs 之間或相同組織中的 帳戶之間使用安全群組共用功能，而不接受該 VPC 或帳戶的新帳戶的風險。

AMS-STD-X004 - 滲透測試

以下是 X004 - 滲透測試的標準控制項

1. AMS 不支援 pentest 基礎設施。這是客戶的責任。例如，Kali 不是 Linux 的 AMS 支援發行版本。
2. 客戶需要遵守滲透測試。
3. 如果客戶想要在帳戶中執行基礎設施滲透測試，AMS 會提前 24 小時預先通知。
4. AMS 會根據客戶在變更請求或服務請求中明確陳述的客戶需求，佈建客戶滲透基礎設施。
5. 客戶滲透基礎設施的身分管理是客戶的責任。

AMS-STD-X005 - GuardDuty

以下是 X005 - GuardDuty 的標準控制項

1. GuardDuty 必須隨時在所有客戶帳戶中啟用。
2. GuardDuty 提醒必須存放在相同帳戶或相同組織下的任何其他受管帳戶中。
3. 不得使用 GuardDuty 的信任 IP 清單功能。反之，自動封存可以用作替代方案，這適用於稽核目的。

AMS-STD-X007 - 記錄

以下是 X007 - 記錄的標準控制項

ID	技術標準
1.0	日誌類型

ID	技術標準
1.1	作業系統日誌：所有主機必須至少記錄主機身分驗證事件、所有使用提升權限的存取事件，以及所有存取和權限組態變更的存取事件，包括成功和失敗。
1.2	AWS CloudTrail：必須啟用並設定 CloudTrail 管理事件記錄，才能將日誌交付至 S3 儲存貯體。
1.3	VPC 流程日誌：所有網路流量日誌都必須透過 VPC 流程日誌記錄。
1.4	Amazon S3 伺服器存取記錄：存放日誌的 AMS 強制 S3 儲存貯體必須啟用伺服器存取記錄。
1.5	AWS Config 快照： AWS Config 必須記錄所有區域中所有支援資源的組態變更，並每天至少將組態快照檔案交付至 S3 儲存貯體一次。
1.7	應用程式日誌：客戶有權在其應用程式中啟用記錄，並存放在 CloudWatch Logs 日誌群組或 S3 儲存貯體中。
1.8	S3 物件層級記錄：客戶有權在其 S3 儲存貯體中啟用物件層級記錄。
1.9	服務記錄：客戶有權啟用和轉送 SSPS 服務的日誌，例如任何核心服務。
1.10	Elastic Load Balancing(Classic/Application Load Balancer/Network Load Balancer) 日誌：存取和錯誤日誌項目必須存放在 AMS 2.0 受管 S3 儲存貯體中。
2.0	存取控制

ID	技術標準
2.3	存放日誌的 AMS 授權 S3 儲存貯體不得允許第三方將使用者視為儲存貯體政策中的原則。
2.4	未經客戶授權的安全聯絡人明確核准，不得刪除來自 CloudWatch Logs 日誌群組的日誌。
3.0	日誌保留
3.1	AMS 指定的 CloudWatch Logs 日誌群組在日誌上必須至少保留 90 天。
3.2	存放日誌的 AMS 授權 S3 儲存貯體在日誌上必須至少保留 18 個月。
3.3	AWS Backup 快照應可在支援的 資源上至少保留 31 天。
4.0	加密
4.1	必須在存放日誌的 AMS 團隊所需的所有 S3 儲存貯體中啟用加密。
4.2	任何從客戶帳戶轉送到任何其他帳戶的日誌都必須加密。
5.0	完整性
5.1	必須啟用日誌檔案完整性機制。這表示在 AMS 團隊所需的 AWS CloudTrail 線索中設定「記錄檔案驗證」。
6.0	日誌轉送
6.1	任何日誌都可以從一個 AMS 帳戶轉送到相同客戶的另一個 AMS 帳戶。

ID	技術標準
6.2	只有在相同 AMS 客戶擁有非 AMS 帳戶時（透過確認他們位於相同 AWS Organizations 帳戶下，或將電子郵件網域與客戶的公司名稱和 PAYER 連結帳戶相符），才能使用內部工具，從 AMS 轉送任何日誌到非 AMS 帳戶。

在您的環境中帶來高或極高安全風險的變更

下列變更會在您的環境中帶來高或非常高的安全風險：

AWS Identity and Access Management

- High_Risk-IAM-001：建立根帳戶的存取金鑰
- High_Risk-IAM-002：修改 SCP 政策以允許其他存取
- High_Risk-IAM-003：修改 SCP 政策可能會破壞 AMS 基礎設施
- High_Risk-IAM-004：在客戶帳戶中建立具有基礎設施變動許可（寫入、許可管理或標記）的角色/使用者
- High_Risk-IAM-005：IAM 角色信任 AMS 帳戶與第三方帳戶之間的政策（非客戶所擁有）
- High_Risk-IAM-006：跨帳戶政策，透過第三方帳戶從 AMS 帳戶存取任何 KMS 金鑰）
- High_Risk-IAM-007：來自第三方帳戶的跨帳戶政策，用於存取可存放資料的 AMS 客戶 S3 儲存貯體或資源（例如 Amazon RDS、Amazon DynamoDB 或 Amazon Redshift)
- High_Risk-IAM-008：指派具有客戶帳戶中任何基礎設施變動許可的 IAM 許可
- High_Risk-IAM-009：允許列出和讀取帳戶中的所有 S3 儲存貯體

網路安全

- High_Risk-NET-001：從網際網路開啟作業系統管理連接埠 SSH/22 或 SSH/2222（非 SFTP/2222)、TELNET/23、RDP/3389、WinRM/5985-5986、VNC/5900-5901 TS/CITRIX/1494 或 1604、LDAP/389 或 636 和 NETBIOS/137-139
- High_Risk-NET-002：從網際網路開啟資料庫管理連接埠 MySQL/3306、PostgreSQL/5432、Oracle/1521、MSSQL/1433 或任何管理客戶連接埠
- High_Risk-NET-003：直接在任何運算資源上開啟應用程式連接埠 HTTP/80、HTTPS/8443 和 HTTPS/443。例如，EC2 執行個體、ECS/EKS/Fargate 容器等來自網際網路

- High_Risk-NET-004：安全群組的任何變更，可控制對 AMS 基礎設施的存取
- High_Risk-NET-006：VPC 與第三方帳戶互連 （非客戶擁有）
- High_Risk-NET-007：新增客戶防火牆作為所有 AMS 流量的輸出點
- High_Risk-NET-008：不允許與第三方帳戶連接 Transit Gateway
- High_Risk-S3-001：在 S3 儲存貯體中佈建或啟用公開存取

日誌

- High_Risk-LOG-001：停用 CloudTrail。
- High_Risk-LOG-002：停用 VPC 流程日誌。
- High_Risk-LOG-003：透過任何方法 (S3 事件通知、SIEM 代理程式提取、SIEM 代理程式推送等）將日誌從 AMS 受管帳戶轉送至第三方帳戶 （非客戶擁有）
- High_Risk-LOG-004：針對 CloudTrail 使用非 AMS 追蹤

Miscellaneous (其他)

- High_Risk-ENC-001：啟用任何資源時停用加密

安全性常見問答集

AMS 透過全球營運中心提供全年無休follow-the-sun支援。專用 AMS 操作工程師會主動監控儀表板和事件佇列。AMS 通常會透過自動化管理您的帳戶。在極少數需要特定故障診斷或部署專業知識的情況下，AMS 操作工程師可能會存取 AWS 您的帳戶。

以下是有關 AMS Accelerate 在 AMS 操作工程師或自動化存取您的帳戶時所使用的安全最佳實務、控制項、存取模型和稽核機制的常見問題。

AMS 操作工程師何時存取我的環境？

AMS 操作工程師無法持續存取您的帳戶或執行個體。只有在合理的商業使用案例中，例如提醒、事件、變更請求等，才能授予 AMS 營運商存取客戶帳戶的權限。存取會記錄在 AWS CloudTrail 日誌中。

如需存取理由、觸發和觸發啟動器的詳細資訊，請參閱 AMS 客戶帳戶存取觸發條件。

AMS 操作工程師在存取我的帳戶時擔任哪些角色？

在極少數情況下 (~5%)，在您的環境中需要人工介入的情況下，AMS 操作工程師會使用預設的唯讀存取角色登入您的帳戶。預設角色無法存取任何常存放在資料存放區的內容，例如 Amazon Simple Storage Service、Amazon Relational Database Service、Amazon DynamoDB、Amazon Redshift 和 Amazon ElastiCache。

如需 AMS 操作工程師和系統在帳戶中提供服務所需的角色清單，請參閱 AMS 客戶帳戶存取 IAM 角色。

AMS 操作工程師如何存取我的帳戶？

若要存取客戶帳戶，AMS 操作工程師會使用 AWS 內部 AMS 存取服務。此內部服務只能透過安全的私有管道提供，以便安全地存取您的帳戶並進行稽核。

1. AMS 操作工程師使用內部 AMS 存取服務身分驗證以及雙重驗證。此外，營運工程師必須提供業務理由 （事件票證或服務請求 ID)，概述存取 AWS 您的帳戶的需求。
2. 根據操作工程師的授權，AMS 存取服務為工程師提供適當的角色 (only/Operator/Admin) 和 AWS 主控台的登入 URL。存取您的帳戶是短期且有時間限制的。
3. 若要存取 Amazon EC2 執行個體，AMS 操作工程師會使用與代理程式相同的內部 AMS 存取服務。授予存取權後，AMS 操作工程師會使用 AWS Systems Manager Session Manager 來存取具有短期工作階段登入資料的執行個體。

   為了提供 Windows 執行個體的 RDP 存取權，操作工程師會使用 Amazon EC2 Systems Manager 在執行個體上建立本機使用者，並建立連接埠轉送至執行個體。操作工程師會使用本機使用者登入資料來存取執行個體。本機使用者登入資料會在工作階段結束時移除。

下圖概述 AMS 操作工程師用來存取您 帳戶的程序：

如何追蹤 AMS 在我的 AMS 受管 AWS 帳戶中所做的變更？

帳戶存取

為了協助您追蹤自動化或 AMS Accelerate 操作團隊所做的變更，AMS 會在 Amazon Athena 主控台和 AMS Accelerate 日誌中提供變更記錄 SQL 界面。這些資源提供下列資訊：

- 存取您帳戶的對象。

- 存取帳戶的時間。
- 使用哪些權限來存取您的帳戶。
- AMS Accelerate 在您帳戶中所做的變更。
- 為什麼在您的 帳戶中進行了變更。

資源組態

檢視 CloudTrail 日誌以追蹤過去 90 天內 AWS 資源中的組態。如果您的組態超過 90 天，請存取 Amazon S3 中的日誌。

執行個體日誌

Amazon CloudWatch Agent 會收集作業系統日誌。檢視 CloudWatch 日誌，以查看作業系統支援的登入和其他動作日誌。

如需詳細資訊，請參閱追蹤 AMS Accelerate 帳戶中的變更。

AMS 操作工程師存取我帳戶的程序控制是什麼？

在加入 AMS 之前，營運工程師會進行刑事背景檢查。由於 AMS 工程師管理客戶基礎設施，因此他們還必須進行年度背景檢查。如果工程師未通過背景檢查，則會撤銷存取權。

所有 AMS 操作工程師都必須完成必要的安全訓練，例如基礎設施安全性、資料安全性和事件回應，才能獲得資源的存取權。

如何管理特殊權限存取？

一部分使用者必須完成額外的訓練，並維護特殊存取權限，以提高存取權。會檢查和稽核存取和用量。AMS 限制特殊情況或最低權限存取無法滿足您的請求時的特權存取。特殊權限存取也會有時間限制。

AMS 操作工程師是否使用 MFA？

是。所有使用者都必須使用 MFA 和存在證明來為您提供服務。

當 AMS 員工離開組織或變更任務角色時，他們的存取權會發生什麼情況？

透過內部群組成員資格佈建對客戶帳戶和資源的存取權。成員資格是以嚴格的條件為基礎，包括 AMS 中的特定任務角色、報告管理員和僱用狀態。如果操作工程師的工作系列變更或其使用者 ID 已停用，則會撤銷存取權。

哪些存取控制會管理 AMS 操作工程師對我帳戶的存取？

有多層技術控制可強制執行「需要知道」和「最低權限」原則來存取您的環境。以下是存取控制的清單：

- 所有操作工程師都必須是特定內部 AWS 群組的一部分，才能存取客戶帳戶和資源。群組成員資格嚴格基於需要知道的基礎，並使用預先定義的條件自動化。
- AMS 會實務「非持久性」存取您的環境。這表示透過 AMS 操作存取 AWS 您的帳戶是「just-in-time」，具有短期憑證。只有在提交並檢閱內部業務案例理由（服務請求、事件、變更管理請求等）之後，才會提供帳戶的存取權。
- AMS 遵循最低權限原則。因此，授權操作工程師預設會擔任唯讀存取。只有在因事件或變更請求而需要變更環境時，工程師才會使用寫入存取權。
- AMS 使用易於識別的標準角色，這些 AWS Identity and Access Management 角色使用「ams」字首來監控和管理您的帳戶。所有存取都會登入 AWS CloudTrail 供您稽核。
- AMS 使用自動化後端工具，在變更執行的客戶資訊驗證階段偵測您帳戶的未經授權變更。

AMS 如何監控根使用者存取？

根存取一律會觸發事件回應程序。AMS 使用 Amazon GuardDuty 偵測來監控根使用者活動。如果 GuardDuty 產生警示，則 AMS 會建立事件以進行進一步調查。如果偵測到非預期的根帳戶活動，AMS 會通知您，且 AMS 安全團隊會啟動調查。

AMS 如何回應安全事件？

AMS 會調查從 Amazon GuardDuty、Amazon Macie 等偵測服務以及客戶回報的安全問題所產生的安全事件。AMS 與您的安全回應團隊合作，以執行安全事件回應 (SIR) 程序。AMS SIR 程序以 NIST SP 800-61 修訂版 2 電腦安全事件處理指南架構為基礎，並提供全年無休follow-the-sun回應。AMS 會與您一起快速分析和控制安全事件。

AMS 遵循哪些產業標準認證和架構？

如同其他服務 AWS ，AWS Managed Services 已通過
OSPAR、HIPAA、HITRUST、GDPR、SOC*、ISO*、FedRAMP（中/高）、IRP 和 PCI 認證。如需 AWS 符合的客戶合規認證、法規和架構的詳細資訊，請參閱 AWS 合規。

安全護欄

AWS Managed Services 使用多個控制項來保護您的資訊資產，並協助您確保 AWS 基礎設施的安全。AMS Accelerate 會維護 AWS Config 規則和修補動作的程式庫，協助您確保帳戶符合安全與操作完整性的產業標準。 AWS Config 規則會持續追蹤所記錄資源的組態變更。如果變更違反規則的條件，則 AMS 會向您報告其調查結果。您可以根據違規的嚴重性，自動或根據請求修復違規。

AMS 使用 AWS Config 規則來協助滿足下列標準的要求：

- 網際網路安全中心 (CIS)
- 國家標準技術研究所 (NIST) 雲端安全架構 (CSF)
- 美國健康保險流通與責任法案 (HIPAA)
- 支付卡產業 (PCI) 資料安全標準 (DSS)

如需詳細資訊，請參閱AMS Accelerate 中的安全管理

如何存取有關安全認證、架構和合規的最新報告 AWS？

您可以使用下列方法找到 AWS 服務的目前安全與合規報告：

- 您可以使用 AWS Artifact 下載 AWS 服務安全性、可用性和機密性的最新報告。
- 如需符合全球合規架構的大多數 AWS 服務清單，包括 AWS Managed Services，請參閱 https://aws.amazon.com/compliance/services-in-scope/。例如，選取 PCI 並搜尋 AWS Managed Services。

  您可以搜尋「AMS」，從 AMS 受管 AWS 帳戶尋找 AMS 特定的安全成品。AWS Managed Services 在 SOC 3 的範圍內。
- AWS SOC 2 （系統和組織控制） 報告會發佈至 AWS Artifact 儲存庫。此報告會在美國註冊公眾會計協會 (AICPA) TSP 第 100 節信任服務標準中，評估符合安全性、可用性和機密性標準的 AWS 控制項。

AMS 是否會共用 AMS 功能不同層面的參考架構圖表？

若要檢視 AMS 參考架構，請下載 AWS Managed Services for Proactive Monitoring PDF。

AMS 如何追蹤誰存取我的帳戶，以及存取所需的業務需求？

為了支援服務持續性和帳戶的安全性，AMS 只會為了回應主動運作狀態或維護、運作狀態或安全事件、計劃活動或客戶請求而存取您的帳戶或執行個體。如 AMS Accelerate 的存取模型所述，透過

AMS 程序授權存取您的帳戶。這些授權流程包含防護機制，以防止意外或不適當的存取。作為存取流程的一部分，AMS 為授權系統提供業務需求。此業務需求可能是與您的帳戶相關聯的工作項目，例如您使用 AMS 開啟的案例。或者，業務需求可能是授權的工作流程，例如修補解決方案。所有存取都需要由內部 AMS 系統根據業務規則即時驗證、驗證和授權的正當性，才能使存取請求符合業務需求。

如果沒有有效的業務需求，AMS 操作工程師就無法存取您的帳戶。所有帳戶存取和相關聯的業務需求都會傳送到您 AWS 帳戶內的 AWS CloudTrail 項目。這可提供完整的透明度，並讓您有機會執行自己的稽核和檢查。除了您的檢查之外，AMS 還具有自動檢查，並視需要執行存取請求的手動檢查，並對工具和人工存取執行稽核，以檢閱異常存取。

AMS 工程師是否可以存取存放在資料儲存服務中的 AWS 資料，例如 Amazon S3、Amazon RDS、DynamoDB 和 Amazon Redshift？

AMS 工程師無法存取存放在常用於資料儲存 AWS 的服務中的客戶內容。用於讀取、寫入、修改或刪除這些服務中資料的 AWS APIs 存取，受限於與用於 AMS 工程師存取的 IAM 角色相關聯的明確 IAM 拒絕政策。此外，內部 AMS 護欄和自動化可防止 AMS 操作工程師移除或修改拒絕條件。

AMS 工程師是否可以存取存放在 Amazon EBS、Amazon EFS 和 Amazon FSx 中的客戶資料？

AMS 工程師可以管理員身分登入 Amazon EC2 執行個體。在某些情況下需要管理員存取權才能修復，包括但不限於作業系統 (OS) 問題和修補程式失敗。AMS 工程師通常會存取系統磁碟區來修復偵測到的問題。不過，AMS 工程師的存取不會限制或受限於系統磁碟區。

如何限制或控制對我的環境具有高權限的自動化角色的存取？

此`ams-access-admin`角色僅供 AMS 自動化使用。這些自動化會部署、管理和維護 AMS 用來部署到您的環境的必要資源，以用於遙測、運作狀態和安全資料收集，以執行操作功能。AMS 工程師無法擔任自動化角色，且受到內部系統中角色映射的限制。在執行時間，AMS 會動態將範圍縮小的最低權限工作階段政策套用至每個自動化。此工作階段政策會限制自動化的功能和許可。

AMS 如何實作 AWS Well-Architected Framework for Automation Role 中倡議的最低權限原則？

在執行時間，AMS 會將範圍縮小的最低權限工作階段政策套用至每個自動化。此縮小範圍的工作階段政策會限制自動化的功能和許可。具有建立 IAM 資源許可的工作階段政策也需要連接許可界限。此許可界限可降低權限提升風險。每個團隊都會加入僅供該團隊使用的工作階段政策。

哪些記錄和監控系統用於偵測未經授權的存取嘗試或涉及自動化角色的可疑活動？

AWS 會維護集中式儲存庫，提供核心日誌封存功能供 AWS 服務團隊內部使用。這些日誌存放在 Amazon S3 中，以實現高可擴展性、耐用性和可用性。 AWS 服務團隊接著可以在中央日誌服務中收集、封存和檢視服務日誌。

的生產主機 AWS 是使用主基準映像進行部署。基準映像配備一組標準組態和函數，包括基於安全目的的記錄和監控。 AWS 安全團隊會存放和存取這些日誌，以便在發生可疑的安全事件時進行根本原因分析。

指定主機的日誌可供擁有該主機的團隊使用。團隊可以搜尋其日誌以進行操作和安全性分析。

如何處理與自動化基礎設施相關的安全事件或違規，以及哪些通訊協定有助於快速回應和緩解？

AWS 應變計畫和事件回應程序手冊已定義並測試工具和程序，以偵測、緩解、調查和評估安全事件。這些計劃和手冊包含根據合約和法規要求回應潛在資料外洩的指導方針。

是否定期在自動化基礎設施上執行安全評估、漏洞掃描和滲透測試？

AWS 安全性會使用各種工具，在 AWS 環境中主機作業系統、Web 應用程式和資料庫上執行定期漏洞掃描。 AWS 安全團隊也會訂閱適用廠商瑕疵的新聞摘要，並主動監控廠商的網站和其他相關管道，以取得新修補程式。

如何限制只有授權人員才能存取自動化基礎設施？

AWS 系統存取權是根據最低權限配置，並由獲授權的個人核准。職責和責任領域 （例如，存取請求和核准、變更管理請求和核准、變更開發、測試和部署等） 會隔離到不同的個人，以減少未經授權或無意修改或濫用 AWS 系統。系統界限內不允許群組或共用帳戶。

實作哪些措施來維護安全標準，並防止自動化管道中未經授權的存取或資料外洩？

資源的存取，包括服務、主機、網路裝置，以及 Windows 和 UNIX 群組，已由適當的擁有者或管理員在 AWS 專屬許可管理系統中核准。許可管理工具日誌會擷取存取變更的請求。任務函數變更會自動撤銷員工對 資源的存取權。必須請求並核准該員工的持續存取權。

AWS 需要透過核准的密碼編譯管道進行雙重驗證，才能從遠端位置對內部 AWS 網路進行身分驗證。防火牆裝置會限制對運算環境的存取、強制執行運算叢集的界限，以及限制對生產網路的存取。

實作程序是為了保護稽核資訊和稽核工具免於未經授權的存取、修改和刪除。稽核記錄包含一組資料元素，以支援必要的分析需求。此外，稽核記錄可供授權使用者隨需檢查或分析，並回應安全相關或影響業務的事件。

AWS 系統（例如網路、應用程式、工具等）的使用者存取權會在終止或停用後 24 小時內撤銷。停用和/或移除非作用中使用者帳戶至少每 90 天一次。

是否針對存取或稽核記錄開啟異常偵測或監控，以偵測權限提升或存取濫用，以主動提醒 AMS 團隊？

的生產主機 AWS 具有記錄功能，以維護安全。此服務會在主機上記錄人類動作，包括登入、失敗的登入嘗試和登出。 AWS 安全團隊會存放和存取這些日誌，以便在發生可疑的安全事件時進行根本原因分析。擁有該主機的團隊也可以使用指定主機的日誌。前端日誌分析工具可供服務團隊搜尋其日誌以進行操作和安全性分析。實作程序有助於保護日誌和稽核工具免於未經授權的存取、修改和刪除。 AWS 安全團隊會執行日誌分析，根據定義的風險管理參數來識別事件。

從 AMS 受管帳戶擷取哪些類型的客戶資料，以及如何使用和儲存這些資料？

AMS 不會出於任何目的存取或使用您的內容。AMS 將客戶內容定義為軟體（包括機器映像）、資料、文字、音訊、視訊或影像，客戶或任何最終使用者透過使用 而從上述衍生的任何運算結果，透過 AWS 服務 傳輸到 AWS 來處理、儲存或託管 AWS 服務。

AMS Accelerate 中的監控和事件管理

AMS Accelerate 監控系統可監控您的 AWS 資源是否有故障、效能降低和安全問題。

作為受管帳戶，AMS Accelerate 會設定和部署適用 AWS 資源的警示、監控這些資源，並視需要執行修復。

AMS Accelerate 監控系統依賴內部工具，例如 Resource Tagger 和 Alarm Manager，並利用 AWS AppConfig、Amazon CloudWatch (CloudWatch) AWS 服務、Amazon EventBridge （先前稱為 CloudWatch)、Amazon GuardDuty、Amazon Macie 和 AWS Health。

AMS Accelerate 提供各種營運服務，協助您實現卓越營運 AWS。若要快速了解 AMS 如何 AWS 雲端透過我們的一些關鍵營運功能，包括全年無休服務台、主動監控、安全性、修補、記錄和備份，協助您的團隊在 中實現整體卓越營運，請參閱 AMS 參考架構圖表。

主題

如需監控 Amazon EKS 的資訊，請參閱 AMS Accelerate 中 Amazon EKS 的監控和事件管理

什麼是監控？

AMS Accelerate 監控提供下列優點：

- 一種預設組態，可針對您選取的所有或支援 AWS 的資源，在您的受管帳戶中建立、管理和部署政策。
- 監控基準，可讓您擁有預設層級的保護，即使您未為受管帳戶設定任何其他監控。如需詳細資訊，請參閱AMS 中基準監控的提醒。

- 自訂基準資源警示以符合您的需求的能力。
- AMS Operations 會盡可能自動修復提醒，以防止或降低對應用程式的影響。例如，如果您使用獨立的 Amazon EC2 執行個體，但系統運作狀態檢查失敗，則 AMS 會停止並重新啟動執行個體，以嘗試復原執行個體。如需詳細資訊，請參閱 AMS 自動修復提醒。
- 使用 OpsCenter 顯示作用中和先前已解決的提醒。例如，如果您在 Amazon EC2 執行個體上有非預期的高 CPU 使用率，您可以請求存取 AWS Systems Manager 主控台（包括存取 OpsCenter 主控台），並直接在 OpsCenter 主控台中檢視 OpsItem。 OpsCenter
- 調查警示以判斷適當的動作。如需詳細資訊，請參閱AMS Accelerate 中的事件管理。
- 根據您帳戶中的組態和支援的 AWS 服務產生的提醒。帳戶的監控組態是指帳戶中建立提醒的所有資源參數。帳戶的監控組態包括 CloudWatch 警示定義，以及產生警示的 EventBridge（先前稱為 CloudWatch Events)（警示或事件）。如需資源參數的詳細資訊，請參閱 AMS 中基準監控的提醒。
- 通知即將發生、持續發生、下降或潛在的故障；效能降低；或帳戶中設定的基準監控所產生的安全問題（稱為警示）。警示的範例包括 CloudWatch 警示、事件或來自 AWS 服務的調查結果，例如 GuardDuty 或 AWS Health。

監控的運作方式

請參閱下列 AWS Managed Services (AMS) 中監控架構的圖形。

下圖說明 AMS Accelerate 監控架構。

根據使用資源標記器定義的政策標記資源，並部署警示定義後，以下清單會說明 AMS 監控程序。

- 產生：在帳戶加入時，AMS 會為您在受管帳戶中建立的所有資源設定基準監控 (CloudWatch (CW) 警示和 CW 事件規則的組合）。基準監控組態會在觸發 CW 警示或產生 CW 事件時產生警示。
- 彙總：您的資源所產生的所有提醒都會透過導向至帳戶中的 SNS 主題，傳送至 AMS 監控系統。您也可以設定 AMS 如何將 Amazon EC2 警示分組在一起。AMS 會將與相同 EC2 執行個體相關的所有警示分組為單一事件，或根據您的偏好設定，為每個警示建立一個事件。您可以隨時使用 Cloud Service Delivery Manager 或 Cloud Architect 來變更此組態。
- 處理：AMS 會分析警示，並根據它們的潛在影響進行處理。警示的處理方式如下。
  - 具有已知客戶影響的提醒：這些提醒會導致建立新的事件報告，而 AMS 會遵循事件管理程序。

    警示範例：Amazon EC2 執行個體未通過系統運作狀態檢查，AMS 會停止並重新啟動執行個體以嘗試復原執行個體。

- 具有不確定客戶影響的提醒：對於這些類型的提醒，AMS 會傳送事件報告，在許多情況下會要求您在 AMS 採取動作之前驗證影響。不過，如果基礎設施相關檢查通過，則 AMS 不會將事件報告傳送給您。

  例如：Amazon EC2 執行個體上 >85% CPU 使用率超過 10 分鐘的提醒無法立即分類為事件，因為根據使用量，可能預期會發生此行為。在此範例中，AMS Automation 會對資源執行基礎設施相關檢查。如果這些檢查通過，即使 CPU 用量超過 99%，AMS 也不會傳送提醒通知。如果自動化偵測到資源上的基礎設施相關檢查失敗，則 AMS 會傳送提醒通知，並檢查是否需要緩解。本節會詳細討論提醒通知。AMS 會在通知中提供緩解選項。當您回覆確認警示是事件 AMS 的通知時，會建立新的事件報告，並開始 AMS 事件管理程序。收到「無客戶影響」或三天內完全沒有回應的服務通知會標記為已解析，而對應的提醒會標記為已解析。
- 沒有客戶影響的提醒：如果在評估之後，AMS 判斷提醒沒有客戶影響，則提醒會關閉。

  例如， AWS Health 通知需要替換的 EC2 執行個體，但該執行個體已終止。

EC2 執行個體分組通知

您可以設定 AMS 監控，將來自相同 EC2 執行個體的警示分組為單一事件。您的 Cloud Service Delivery Manager 或 Cloud Architect 可以為您設定。您可以為每個 AMS 受管帳戶設定四個參數。

1. 範圍：選擇全帳戶或以標籤為基礎的。
   - 若要指定適用於該帳戶中每個 EC2 執行個體的組態，請選擇範圍 = 整個帳戶。
   - 若要指定僅適用於該帳戶中具有特定標籤之 EC2 執行個體的組態，請選擇範圍 = 標籤型。
2. 分組規則：選擇傳統或執行個體。
   - 若要設定您帳戶中每個資源的執行個體層級分組，請選擇範圍 = 全帳戶和分組規則 = 執行個體。
   - 若要將帳戶中的特定資源設定為使用執行個體層級分組，請標記這些執行個體，然後選擇範圍 = 標籤型和分組規則 = 執行個體層級。
   - 若要不對帳戶中的提醒使用執行個體分組，請選擇分組規則 = 傳統。
3. 參與選項：選擇無、僅報告或預設。
   - 若要讓 AMS 在組態作用中時不為這些資源的警示建立事件或執行自動化，請選擇無。
   - 若要讓 AMS 在組態作用中時不為這些資源的警示建立事件或執行自動化，也不要執行自動修復 Systems Manager 文件，但要在報告中包含這些事件的記錄，請僅選擇報告。如果您想要減少與之互動的事件支援案例數量，以及某些資源的某些事件不需要立即關注，例如非生產帳戶中的事件，這可能會很有用。
   - 若要讓 AMS 處理您的提醒、執行自動化，並在需要時建立事件案例，請選擇預設值。

4. 解決時間：選擇 24 小時、48 小時或 72 小時。最後，設定事件案例自動關閉的時間。如果上次案例對應的時間在值後達到設定的解析，則事件會關閉。

提醒通知

在警示處理過程中，AWS Managed Services (AMS) 會根據影響分析建立事件，並在可以判斷影響時啟動事件管理程序以進行修復。如果無法判斷影響，則 AMS 會透過服務通知，將提醒通知傳送至與您帳戶相關聯的電子郵件地址。在某些情況下，不會傳送此提醒通知。例如，如果基礎設施相關的檢查傳遞高 CPU 使用率警示，則不會傳送提醒通知給您。如需詳細資訊，請參閱 中警示處理程序的 AMS 監控架構圖表監控的運作方式。

標籤型提醒通知

使用標籤將資源的提醒通知傳送到不同的電子郵件地址。最佳實務是使用標籤型提醒通知，因為當多個開發人員團隊使用相同的帳戶時，傳送至單一電子郵件地址的通知可能會導致混淆。標籤型提醒通知不受您選擇的EC2 執行個體分組通知設定影響。

透過標籤型提醒通知，您可以：

- 將提醒傳送至特定電子郵件地址：使用 `key = OwnerTeamEmail`標記具有提醒的資源，這些提醒必須傳送至特定電子郵件地址`value = EMAIL_ADDRESS`。
- 傳送提醒到多個電子郵件地址：若要使用多個電子郵件地址，請指定以逗號分隔的值清單。例如 `key = OwnerTeamEmail` 和 `value = EMAIL_ADDRESS_1, EMAIL_ADDRESS_2, EMAIL_ADDRESS_3, ...`。值欄位的字元總數不能超過 260。
- 使用自訂標籤金鑰：若要使用自訂標籤金鑰，請在明確同意啟用標籤型通訊自動通知的電子郵件中提供自訂標籤金鑰名稱給 CSDM。最佳實務是針對所有執行個體和資源的聯絡標籤使用相同的標記策略。

> **Note**
>
> `OwnerTeamEmail` 的鍵值不必在駝色案例中。不過，標籤區分大小寫，最佳實務是使用建議的格式。
> 電子郵件地址必須完整指定，並以「簽署時」(@) 分隔本機部分與網域。無效的電子郵件地址範例：`Team.AppATabc.xyz` 或 `john.doe`。如需標記策略的一般指引，請參閱標記 AWS 資源。請勿在標籤中新增個人身分識別資訊 (PII)。盡可能使用分發清單或別名。
> 來自下列 Amazon Services 的資源支援標籤型提醒通知：EC2、Elastic Block Store (EBS)、Elastic Load Balancing (ELB)、Application Load Balancer (ALB)、Network

Load Balancer、Relational Database Service (RDS)、OpenSearch、Elastic File System (EFS)、FSx 和 Site-to-Site VPN。

AMS 中基準監控的提醒

了解 AMS Accelerate 監控預設值。如需詳細資訊，請參閱AMS Accelerate 中的監控和事件管理。

下表顯示監控的項目和預設提醒閾值。您可以使用自訂組態文件變更提醒閾值，或提交服務請求。如需變更自訂警示組態的指示，請參閱 變更加速警示組態。若要在警示超過閾值時接收通知，除了 AMS 的標準警示程序之外，您還可以覆寫警示組態。如需說明，請參閱加速警示管理員。

Amazon CloudWatch 提供指標的延長保留。如需詳細資訊，請參閱 CloudWatch 限制。

> **Note**
>
> AMS Accelerate 會定期校正其基準監控。新帳戶一律使用最新的基準監控加入，而表格說明新加入帳戶的基準監控。AMS Accelerate 會定期更新現有帳戶中的基準監控，而且在進行更新之前，您可能會遇到延遲。

基準監控的提醒

服務/資源類型	警示來源和觸發條件	提醒名稱和備註
對於星號 (*) 警示，AMS 會盡可能主動評估影響並修復；如果無法修復，AMS 會建立事件。當自動化無法修正問題時，AMS 會通知您事件案例，並聘請 AMS 工程師。此外，如果您選擇加入 Direct-Customer-Alerts SNS 主題，則這些提醒會直接傳送到您的電子郵件。		
Application Load Balancer 執行個體	ApplicationLoadBalancerErrorCount (HTTPCode_ELB_5XX_Count/RequestCount)*100 總和 > 15%，持續 1 分鐘，連續 5 次。	Application LoadBalancer HTTP 5XX 錯誤計數 Loadbalancer 產生的過多 HTTP 5XX 回應代碼的 CloudWatch 警示。
Application Load Balancer 執行個體	RejectedConnectionCount	Application LoadBalancer 拒絕的連線計數

服務/資源類型	警示來源和觸發條件	提醒名稱和備註
	總和 > 0%，持續 1 分鐘，連續 5 次。	如果因負載平衡器達到其上限而遭到拒絕的連線數目，則 CloudWatch 警示
Application Load Balancer 目標	TargetConnectionErrorCount (HTTPCode_Target_5 XX_Count/RequestCount)*100 總和 > 15%，持續 1 分鐘，連續 5 次。	${ElasticLoadBalancingV2：：TargetGroup：：FullName} - Application LoadBalancer 目標連線錯誤計數 - ${ElasticLoadBalancingV2：：TargetGroup：：UUID} 目標產生的過多 HTTP 5XX 回應碼的 CloudWatch 警示。
Application Load Balancer 目標	ApplicationLoadBalancerTargetGroupErrorCount 總和 > 0%，持續 1 分鐘，連續 5 次。	${ElasticLoadBalancingV2：：TargetGroup：：FullName} - Application LoadBalancer Target HTTP 5XX 錯誤計數 - ${ElasticLoadBalancingV2：：TargetGroup：：UUID} 如果負載平衡器和已註冊執行個體之間的連線數目未成功建立，則 CloudWatch 會發出警示。
Amazon EC2 執行個體 - 所有 OSs	CPUUtilization* > 95% 持續 5 分鐘，連續 6 次。	${EC2：：InstanceId}：CPU 太高 CloudWatch 警示。高 CPU 使用率是應用程式狀態變更的指標，例如死鎖、無限迴圈、惡意攻擊和其他異常。 這些是 Direct-Customer-Alerts 警示。

服務/資源類型	警示來源和觸發條件	提醒名稱和備註
Amazon EC2 執行個體 - 所有 OSs	StatusCheckFailed > 0% 持續 5 分鐘，連續 3 次。	${EC2：：InstanceId}：狀態檢查失敗 CloudWatch 警示。狀態檢查失敗表示具有指定 ID 的 Amazon EC2 執行個體已失敗其一或多個自動狀態檢查。這表示執行個體發生問題，導致無法正常運作或無法連線。
Amazon EC2 執行個體 - Linux	最小 mem_used_percent >= 95%，持續 5 分鐘，連續 6 次。	${EC2：：InstanceId}：記憶體可用 CloudWatch 警示。Memory Free 表示指定 Amazon EC2 執行個體上的可用記憶體 (RAM) 已低於定義的閾值。這可能會導致記憶體問題、系統當機，並指出執行個體可能需要更多 RAM。 這些是 Direct-Customer-Alerts 警示。

服務/資源類型	警示來源和觸發條件	提醒名稱和備註
Amazon EC2 執行個體 - Linux	平均 swap_used_percent **>=** 95%，持續 5 分鐘，連續 6 次。	${EC2：：InstanceId}：交換免費 CloudWatch 警示。Amazon EC2 執行個體的平均 swap_used_percent 表示目前使用中配置的交換空間的平均百分比已超過預先定義的閾值。這可能會導致效能降低、瓶頸和記憶體問題。 這些是 Direct-Customer-Alerts 警示。
Amazon EC2 執行個體 - Linux	disk_used_percent 上限 **>=** 95%，持續 5 分鐘，連續 6 次。	${EC2：：InstanceId}：磁碟用量太高 - ${EC2：：Disk：：UUID} CloudWatch 警示。磁碟用量太高表示特定 Amazon EC2 或已識別磁碟上的磁碟使用率接近其容量。這可能會導致效能降低、應用程式錯誤和系統不穩定。 這些是 Direct-Customer-Alerts 警示。

服務/資源類型	警示來源和觸發條件	提醒名稱和備註
Amazon EC2 執行個體 - Windows	使用中已遞交位元組的記憶體百分比下限 **>=** 95%，持續 5 分鐘，連續 6 次。	${EC2：：InstanceId}：記憶體可用 CloudWatch 警示。Memory Free 表示指定 Amazon EC2 執行個體上的可用記憶體 (RAM) 已低於定義的閾值。這可能會導致記憶體問題、系統當機，並指出執行個體可能需要更多 RAM。 這些是 Direct-Customer-Alerts 警示。
Amazon EC2 執行個體 - Windows	LogicalDisk % 可用空間上限 **<=** 5%，持續 5 分鐘，連續 6 次。	${EC2：：InstanceId}：磁碟用量太高 - ${EC2：：Disk：：UUID} CloudWatch 警示。指出 Amazon EC2 Windows 執行個體內邏輯磁碟（檔案系統分割區）的可用空間百分比已超過預先定義的閾值。磁碟空間不足可能會導致磁碟空間不足 這些是 Direct-Customer-Alerts 警示。
Amazon EFS	AMSEFSBurstCreditBalanceExhausted。 BurstCreditBalance 少於 1000，持續 15 分鐘。	${EFS：：FileSystemId}：EFS：爆量額度餘額 Amazon EFS 檔案系統 BurstCreditBalance 上的 CloudWatch 警示。

服務/資源類型	警示來源和觸發條件	提醒名稱和備註
Amazon EFS	AMSEFSClientConnectionsLimit。 ClientConnections > 24，000 15 分鐘。	${EFS：：FileSystemId}：EFS：用戶端連線限制 Amazon EFS 檔案系統 ClientConnections 上的 CloudWatch 警示。
Amazon EFS	AMSEFSThroughputUtilizationLimit。 EFS 一小時輸送量使用率 > 80%。	${EFS：：FileSystemId}：EFS：輸送量使用率限制 Amazon EFS 檔案系統輸送量使用率的 CloudWatch 警示。
Amazon EFS	AMSEFSPercentIOLimit。 PercentIOLimit > 95 持續七十五分鐘。	${EFS：：FileSystemId}：EFS： PercentIOLimit Amazon EFS 檔案系統之 PercentIOLimit 上的 CloudWatch 警示。
Amazon EKS	請參閱 Amazon EKS AMS Accelerate 中 Amazon EKS 監控和事件管理的基準警示。	
Elastic Load Balancing 執行個體	SpilloverCountBackendConnectionErrors > 1 表示 1 分鐘，連續 15 次。	Classic LoadBalancer 溢出計數警示 如果因為突增佇列已滿而遭到拒絕的請求數量過多，CloudWatch 會發出警示。
Elastic Load Balancing 執行個體	HTTPCode_ELB_5XX_Count 總和 > 0，持續 5 分鐘，連續 3 次。	來自負載平衡器之過多 HTTP 5XX 回應碼的 CloudWatch 警示。

服務/資源類型	警示來源和觸發條件	提醒名稱和備註
Elastic Load Balancing 執行個體	SurgeQueueLength > 100 持續 1 分鐘，連續 15 次。	Classic LoadBalancer 突增佇列長度警示。 如果待定路由的請求數量過多，CloudWatch 會發出警示。
FSx for OnTAP	AMSFSXONTAPIOPSUtilization。 FSX：ONTAP IOPS 使用率 > 80%，持續兩小時。	${FSx：：FileSystemId}：FSX：ONTAP IOPS 使用率 FSx for ONTAP 執行個體 IOPS 使用率限制上的 CloudWatch 警示。
FSx for OnTAP	AMSFSXONTAPThroughputUtilization。 FSX：ONTAP 輸送量使用率 > 80%，持續兩小時。	${FSx：：FileSystemId}：FSX：ONTAP 輸送量使用率 FSx for ONTAP 磁碟區的輸送量限制上的 CloudWatch 警示。
FSx for OnTAP	AMSFSXONTAPVolumeInodeUtilization。 FSX：ONTAP Inode 使用率 > 80%，持續兩小時。	${FSx：：FileSystemId}：${FSx：：ONTAP：：VolumeId} FSX：ONTAP Inode 使用率 FSx for ONTAP 磁碟區的檔案容量使用率限制上的 CloudWatch 警示。
FSx for OnTAP	AMSFSXONTAPVolumeCapacityUtilization。 FSX：ONTAP 磁碟區容量使用率 > 80%，持續兩小時。	${FSx：：FileSystemId}：${FSx：：ONTAP：：VolumeId} FSx for ONTAP 磁碟區的磁碟區容量使用率限制上的 CloudWatch 警示。

服務/資源類型	警示來源和觸發條件	提醒名稱和備註
FSx for Windows File Server	AMSFSXWindowsThroughputUtilization。 FSX：Windows 兩小時輸送量使用率 > 80%。	${FSx：：FileSystemId}：FSX：Windows 輸送量使用率 FSx for Windows File Server 執行個體輸送量限制上的 CloudWatch 警示。
FSx for Windows File Server	AMSFSXWindowsIOPSUtilization。 FSX：Windows IOPS 使用率 > 80%，持續兩小時。	${FSx：：FileSystemId}：FSX：Windows IOPS 使用率 FSx for Windows File Server 執行個體 IOPS 使用率限制上的 CloudWatch 警示。
GuardDuty 服務	不適用；所有調查結果（威脅目的）都會受到監控。每個問題清單對應至 提醒。 GuardDuty 調查結果的變更。這些變更包括新產生的問題清單或後續出現的現有問題清單。	如需支援的 GuardDuty 調查結果類型清單，請參閱 GuardDuty 作用中調查結果類型。
醫療保健	AWS Health Dashboard	與 AMS 監控的服務相關的 AWS Health Dashboard (AWS Health) 事件狀態變更時，會傳送通知。如需詳細資訊，請參閱支援的 服務。
IAM	Amazon EC2 IAM 執行個體設定檔不存在。 IAM 執行個體描述檔遺失。	如需取代 Amazon EC2 IAM 執行個體描述檔的說明，請參閱取代 IAM 角色中的 IAM 文件。

服務/資源類型	警示來源和觸發條件	提醒名稱和備註
IAM	Amazon EC2 IAM 執行個體描述檔的政策過多。 IAM 執行個體描述檔有 10 個政策，無法新增其他政策。	• 修改 IAM 的服務 AWS 配額，將每個角色的受管政策數目增加到 20。如需服務配額的相關資訊，請參閱檢視服務配額。 • 透過移除與這些執行個體相關聯之 IAM 角色的不必要受管政策，將受管政策計數降至低於目前的 IAM 配額。請務必保留 AMS 所需的政策。 • 透過合併與這些執行個體相關聯之 IAM 角色的政策，將受管政策計數降至低於目前的 IAM 配額。請務必保留 AMS 所需的政策。 如需 AMS 必要政策，請參閱 AMS Accelerate 使用者指南：IAM 許可變更詳細資訊。
Macie	新產生的提醒和現有提醒的更新。 Macie 會在問題清單中找到任何變更。這些變更包括新產生的問題清單或後續出現的現有問題清單。	Amazon Macie 提醒。如需支援的 Amazon Macie 警示類型清單，請參閱分析 Amazon Macie 調查結果。請注意，並非所有帳戶都啟用 Macie。
NATGateways	PacketsDropCount ：如果 packetsdropcount 在 15 分鐘內 > 0 時發出警示	NatGateway PacketsDr opCount 大於 0 的值可能表示，目前 NAT 閘道發生暫時性的問題。

服務/資源類型	警示來源和觸發條件	提醒名稱和備註
NATGateways	ErrorPortAllocation：如果 NAT Gateways 無法配置連接埠超過 15 分鐘的評估期間，則發出警示	NatGateway ErrorPortAllocation NAT 閘道無法配置來源連接埠的次數。大於零的值表示開啟太多並行衝突。
OpenSearch 叢集	叢集狀態 紅色最大值為 >= 1 持續 1 分鐘，連續 1 次。	ClusterStatus 紅色 CloudWatch 警示。用於加密網域中靜態資料的 AWS KMS 加密金鑰已停用。重新啟用它來恢復正常操作。若要進一步了解，請參閱 Red Cluster 狀態。
OpenSearch 網域	KMSKeyError >= 1 表示 1 分鐘，連續 1 次。	KMS 金鑰錯誤 CloudWatch 警示。至少一個主要碎片及其複本不會分配到節點。若要進一步了解，請參閱 Amazon OpenSearch Service 的靜態資料加密。
OpenSearch 網域	KMSKeyInaccessible >= 1 表示 1 分鐘，連續 1 次。	KMS 金鑰無法存取錯誤 CloudWatch 警示。至少一個主要碎片及其複本不會分配到節點。若要進一步了解，請參閱 Amazon OpenSearch Service 的靜態資料加密。
OpenSearch 網域	叢集狀態 黃色最大值為 >= 1 持續 1 分鐘，連續 1 次。	ClusterStatus 黃色 至少一個複本碎片不會分配到節點。若要進一步了解，請參閱黃色叢集狀態。

服務/資源類型	警示來源和觸發條件	提醒名稱和備註
OpenSearch 網域	FreeStorageSpace 最小值為 <= 20480，持續 1 分鐘，連續 1 次。	可用儲存空間不足 您叢集內的節點縮減至 20 GiB 的可用儲存空間。若要進一步了解，請參閱缺少可用的儲存空間。
OpenSearch 網域	ClusterIndexWritesBlocked >= 1 持續 5 分鐘，連續 1 次。	叢集索引寫入已封鎖 叢集正在封鎖寫入請求。若要進一步了解，請參閱 ClusterBlockException。
OpenSearch 網域	節點 最短 < x 持續 1 天，連續 1 次。	節點關閉 x 是您叢集中的節點數。此警示表示您叢集中至少有一個節點已無法連線達 1 天時間。若要進一步了解，請參閱失敗的叢集節點。
OpenSearch 網域	CPUUtilization 平均 >= 80%，持續 15 分鐘，連續 3 次。	資料節點中的高 CPU 用量 100% CPU 使用率不稀有，但持續高平均值會有問題。請考慮調整現有執行個體類型的大小，或新增執行個體。

服務/資源類型	警示來源和觸發條件	提醒名稱和備註
OpenSearch 網域	JVMMemoryPressure 最大值 >= 80%，持續 5 分鐘，連續 3 次。	資料節點中的高記憶體用量 如果使用量增加，叢集可能遇到記憶體不足錯誤。可考慮垂直擴展。OpenSearch 針對 Java 堆積使用執行個體 RAM 的一半，堆積大小上限為 32 GiB。您可以垂直擴展執行個體高達 64 GiB 的 RAM，屆時便能透過新增執行個體進行水平擴展。
OpenSearch 網域	MasterCPUUtilization 平均 >= 50%，持續 15 分鐘，連續 3 次。	主節點 CPU 使用率高 請考慮為您的專用主節點使用較大的執行個體類型。因為其在叢集穩定性中的角色和藍/綠部署，專用主節點應該具有比資料節點較低的平均 CPU 使用量。
OpenSearch 網域	MasterJVMMemoryPressure 最大值 >= 80%，持續 15 分鐘，連續 1 次。	主節點 JVM 記憶體壓力過高 請考慮為您的專用主節點使用較大的執行個體類型。因為其在叢集穩定性中的角色和藍/綠部署，專用主節點應該具有比資料節點較低的平均 CPU 使用量。

服務/資源類型	警示來源和觸發條件	提醒名稱和備註
OpenSearch 執行個體	AutomatedSnapshotFailure 最大值為 >= 1，持續 1 分鐘，連續 1 次。	自動化快照失敗 CloudWatch 警示。自動快照失敗。此故障通常是紅色叢集運作狀態的結果。若要進一步了解，請參閱 Red Cluster 狀態。
Amazon RDS	平均 CPU 使用率 > 90%，持續 15 分鐘，連續 2 次。	${RDS：：DBInstanceIdentifier}：CPUUtilization CloudWatch 警示。
Amazon RDS	DiskQueueDepth 的總和 > 75%，持續 1 分鐘，連續 15 次。	${RDS：：DBInstanceIdentifier}：DiskQueue CloudWatch 警示。
Amazon RDS	平均 FreeStorageSpace < 1，073，741，824 位元組，持續 5 分鐘，連續 2 次。	${RDS：：DBInstanceIdentifier}：FreeStorageSpace CloudWatch 警示。
Amazon RDS	低儲存提醒 當資料庫執行個體的配置儲存體用盡時觸發。	RDS-EVENT-0007，請參閱使用 Amazon RDS 事件通知的詳細資訊。
Amazon RDS	資料庫執行個體失敗 因為不相容的組態或基礎儲存問題，資料庫執行個體已失敗。開始資料庫執行個體的時間點還原。	RDS-EVENT-0031，請參閱 Amazon RDS 事件類別和事件訊息的詳細資訊。

服務/資源類型	警示來源和觸發條件	提醒名稱和備註
Amazon RDS	未嘗試 RDS -0034 容錯移轉。 Amazon RDS 不會因為資料庫執行個體最近發生的容錯移轉，而嘗試請求的容錯移轉。	RDS-EVENT-0034，請參閱 Amazon RDS 事件類別和事件訊息的詳細資訊。
Amazon RDS	RDS - 0035 資料庫執行個體無效的參數 例如，MySQL 無法啟動，因為此執行個體類別的記憶體相關參數設定過高，因此您的動作會是修改記憶體參數並重新啟動資料庫執行個體。	RDS-EVENT-0035，請參閱 Amazon RDS 事件類別和事件訊息的詳細資訊。
Amazon RDS	無效的子網路 IDs 資料庫執行個體 資料庫執行個體位於不相容的網路中。部分指定的子網路 ID 無效或不存在。	服務事件。RDS-EVENT-0036，請參閱 Amazon RDS 事件類別和事件訊息的詳細資訊。
Amazon RDS	RDS-0045 資料庫執行個體僅供讀取複本錯誤 僅供讀取複寫程序發生錯誤。如需更多詳細資訊，請參閱事件訊息。如需有關對僅供讀取複本錯誤進行故障診斷的資訊，請參閱對 MySQL 僅供讀取複本問題進行故障診斷。	RDS-EVENT-0045，請參閱 Amazon RDS 事件類別和事件訊息的詳細資訊。
Amazon RDS	RDS-0057 建立 statspack 使用者帳戶時發生錯誤 僅供讀取複本上的複寫已結束。	服務事件。RDS-EVENT-0057，請參閱 Amazon RDS 事件類別和事件訊息的詳細資訊。

服務/資源類型	警示來源和觸發條件	提醒名稱和備註
Amazon RDS	RDS-0058 資料庫執行個體讀取複寫已結束 建立 Statspack 使用者帳戶 PERFSTAT 時發生錯誤。在新增 Statspack 選項之前捨棄帳戶。	服務事件。RDS-EVENT-0058，請參閱 Amazon RDS 事件類別和事件訊息的詳細資訊。
Amazon RDS	資料庫執行個體復原開始 SQL Server 資料庫執行個體正在重新建立其鏡像。將會降低效能，直到鏡像重新建立完成。找到含有非 FULL 還原模型的資料庫。復原模型已變更回 FULL 並開始鏡像復原。(<dbname>：<recovery model found>【，...】)	服務事件。RDS-EVENT-0066 請參閱 Amazon RDS 事件類別和事件訊息的詳細資訊。
Amazon RDS	資料庫叢集的容錯移轉已失敗。	RDS-EVENT-0069，請參閱 Amazon RDS 事件類別和事件訊息的詳細資訊。
Amazon RDS	無效的許可復原 S3 儲存貯體 您用來為 SQL Server 原生備份與還原存取 Amazon S3 儲存貯體的 IAM 角色設定不正確。如需詳細資訊，請參閱設定原生備份和還原。	服務事件。RDS-EVENT-0081 在 Amazon RDS 事件類別和事件訊息中查看詳細資訊。
Amazon RDS	Aurora 無法從 Amazon S3 儲存貯體複製備份資料。	RDS-EVENT-0082，請參閱 Amazon RDS 事件類別和事件訊息的詳細資訊。

服務/資源類型	警示來源和觸發條件	提醒名稱和備註
Amazon RDS	資料庫執行個體耗用其配置儲存體的 90% 以上時，會發出低儲存提醒。	服務事件。RDS-EVENT-0089 在 Amazon RDS 事件類別和事件訊息中查看詳細資訊。
Amazon RDS	Aurora Serverless 資料庫叢集擴展失敗時的通知服務。	服務事件。RDS-EVENT-0143 在 Amazon RDS 事件類別和事件訊息中查看詳細資訊。
Amazon RDS	資料庫執行個體處於無效狀態。無需採取任何動作。稍後將重試自動擴展。	RDS-EVENT-0219，請參閱 Amazon RDS 事件類別和事件訊息的詳細資訊。
Amazon RDS	資料庫執行個體已達到儲存已滿閾值，且資料庫已關閉。	RDS-EVENT-0221，請參閱 Amazon RDS 事件類別和事件訊息的詳細資訊。
Amazon RDS	此事件表示 Amazon RDS 執行個體儲存體自動擴展無法擴展，可能有多個原因導致自動擴展失敗。	RDS-EVENT-0223，請參閱 Amazon RDS 事件類別和事件訊息的詳細資訊。
Amazon RDS	儲存自動擴展已觸發將達到最大儲存閾值的擱置擴展儲存任務。	RDS-EVENT-0224，請參閱 Amazon RDS 事件類別和事件訊息的詳細資訊。
Amazon RDS	資料庫執行個體具有目前在可用區域中無法使用的儲存類型。稍後將重試自動擴展。	RDS-EVENT-0237，請參閱 Amazon RDS 事件類別和事件訊息的詳細資訊。
Amazon RDS	Amazon RDS 無法佈建代理的容量，因為子網路中沒有足夠的 IP 地址可用。	RDS-EVENT-0243，請參閱 Amazon RDS 事件類別和事件訊息的詳細資訊。
Amazon RDS	的儲存 AWS 帳戶 體已超過允許的儲存體配額。	RDS-EVENT-0254，請參閱 Amazon RDS 事件類別和事件訊息的詳細資訊。

服務/資源類型	警示來源和觸發條件	提醒名稱和備註
Amazon Redshift 叢集	未處於維護模式時的叢集運作狀態 < 1 持續 5 分鐘	RedshiftClusterHealthStatus 如需詳細資訊，請參閱使用 CloudWatch 指標監控 Amazon Redshift。
站台對站台 VPN	VPNTunnelDown TunnelState <= 0，持續 1 分鐘，連續 20 次。	${AWS::EC2::VpnConnectionId} - VPNTunnelDown 兩個通道都關閉時 TunnelState 為 0，一個通道啟動時為 .5，兩個通道都啟動時為 1.0。
Systems Manager 代理程式	非由 Systems Manager 管理的 EC2 執行個體 未安裝 SSM 代理程式。SSM 代理程式已安裝在執行個體上，但代理程式服務未執行。SSM 代理程式沒有 AWS Systems Manager 服務的網路路由。	還有其他條件會導致 Systems Manager Agent 中斷；如需詳細資訊，請參閱對受管節點可用性進行故障診斷。

如需修補工作的資訊，請參閱 AMS 自動修復提醒。

觀看 Andrew 的影片以進一步了解 (7：03)

AMS 中的應用程式感知事件通知

使用應用程式感知自動事件通知來自訂您的通訊體驗，以取得 AMS 代表您建立的支援案例。當您使用此功能時，AMS 會從 AWS Service Catalog AppRegistry 擷取自訂工作負載偏好設定，以充實 AMS 事件與應用程式中繼資料的通訊，並自訂 AMS 代表您建立的支援案例嚴重性。若要使用此功能，您必須先加入 to AWS Service Catalog AppRegistry。

若要進一步了解 AMS Accelerate 監控預設值，請參閱 AMS Accelerate 中的監控和事件管理。

加入 AppRegistry 並建立應用程式

若要加入 AppRegistry，請參閱 AppRegistry 管理員指南中的 AppRegistry 入門。 AWS Service Catalog AppRegistry 加入後，請使用下列其中一種方法來建立應用程式：

1. AWS 主控台：若要進一步了解如何透過 AWS 主控台在 AppRegistry 中建立應用程式，請參閱AWS Service Catalog AppRegistry 管理員指南》中的建立應用程式。
2. CloudFormation：您可以定義 AppRegistry 應用程式，就像定義任何其他資源一樣。如需詳細資訊，請參閱AWS CloudFormation 《 使用者指南》中的 AWS Service Catalog AppRegistry 資源類型參考。
3. AMS 自動化：為了簡化應用程式註冊程序，AMS 為您提供 SSM 自動化文件 `AWSManagedServices-CreateAppRegistryApplication`。若要使用此方法，請從 AWS Systems Manager 主控台叫用 文件，網址為 https：//https://console.aws.amazon.com/systems-manager/ AWS CLI 。

```
# The following registers a new application with customized severity
aws ssm start-automation-execution \
  --document-name "AWSManagedServices-CreateAppRegistryApplication" \
  --parameters '{"ResourceAssociationType":["TAGS"],"AppTagValue":
["MyApp"],"CFNStackNames":[],"ApplicationName":
["BananaStand"],"ApplicationDescription":["This is my banana stand
 application"],"AppCriticality":["normal"],"AutomationAssumeRole":
["arn:aws:iam::123456789012:role/SSMAdminRole"]}' \
  --region us-east-1
# The following registers a new application with no customizations
aws ssm start-automation-execution \
  --document-name "AWSManagedServices-CreateAppRegistryApplication" \
  --parameters '{"ResourceAssociationType":["TAGS"],"AppTagValue":
["MyApp"],"CFNStackNames":[],"ApplicationName":
["BananaStand"],"ApplicationDescription":["This is my banana stand
 application"],"AppCriticality":["unset"],"AutomationAssumeRole":
["arn:aws:iam::123456789012:role/SSMAdminRole"]}' \
  --region us-east-1
# You can also register applications using CloudFormation stacks
aws ssm start-automation-execution \
  --document-name "AWSManagedServices-CreateAppRegistryApplication" \
  --parameters '{"ResourceAssociationType":["STACKS"],"AppTagValue":
[""],"CFNStackNames":["arn:aws:cloudformation:us-east-1:123456789012:stack/
stack-2343eddq/1a2b3c4d-5e6f-7g8h-9i0j-1k2l3m4n5o6p"],"ApplicationName":
["BananaStand"],"ApplicationDescription":["This is my banana stand
```

```
 application"],"AppCriticality":["unset"],"AutomationAssumeRole":
["arn:aws:iam::123456789012:role/SSMAdminRole"]}' \
  --region us-east-1
```

建立標籤以啟用案例擴充

您必須先標記應用程式，AMS 才能存取應用程式中繼資料。下表列出所需的標籤。

字首為 的標籤`ams:rt:`會透過 Resource Tagger 套用。

標籤鍵	標籤值
ams 受管	true
ams:rt:ams-managed	true

為您的應用程式自訂 AMS 支援案例嚴重性

您可以指定應用程式對組織的重要性，以自訂 AMS 建立支援案例的嚴重性。此設定是由 AppRegistry 中與您應用程式相關聯的屬性群組所控制。屬性群組名稱的名稱必須符合下列模式：

```
AMS.<ApplicationName>.CommunicationOptions
```

在上述模式中，當您建立應用程式時， `ApplicationName` 必須符合 AppRegistry 中使用的名稱。

範例內容：

```
{
"SchemaVersion": "1.0",
"Criticality": "low"
}
```

SchemaVersion

這會決定您正在使用的結構描述版本，以及可用的功能子集。

結構描述版本	功能
1.0	根據 Criticality 值自訂支援案例嚴重性

重要性

此應用程式的重要性決定了 AMS 自動化系統所建立支援案例的嚴重性。

有效值：

```
low|normal|high|urgent|critical
```

如需嚴重性等級的詳細資訊，請參閱 AWS 支援 API 參考中的SeverityLevel。

必要：是

檢閱必要的許可

若要使用此功能，AMS 需要存取下列 AWS Identity and Access Management 許可：

- iam：ListRoleTags
- iam：ListUserTags
- resourcegroupstaggingapi：GetResources
- servicecatalog-appregistry：GetApplication
- servicecatalog-appregistry：ListAssociatedAttributeGroups
- servicecatalog-appregistry：GetAttributeGroup

> **Important**
> 請確定沒有拒絕上述動作的 IAM 政策或服務控制政策 (SCP)。

API 呼叫是由 `ams-access-admin`角色進行。以下是您可能會看到的範例：

```
arn:aws:sts::111122223333:assumed-role/ams-access-admin/AMS-AMSAppMetadataLookup-*
```

加速警示管理員

AMS Accelerate 使用標籤型警示管理員將警示套用至您的 AWS 資源，以實作基準監控策略，並確保您的所有 AWS 資源都受到監控和保護。透過與標籤型警示管理員整合，您可以根據資源的 AWS 類型、平台和其他標籤自訂資源組態，以確保資源受到監控。警示管理員會在加入期間部署到您的 Accelerate 帳戶。

警示管理員的運作方式

當您的帳戶加入 AMS Accelerate 時，兩個稱為組態設定檔的 JSON 文件會在 AWS AppConfig 中部署在您的帳戶中。這兩個設定檔文件都位於 Alarm Manager 應用程式和 AMS Accelerate 基礎設施環境中。

這兩個組態設定檔命名為 AMSManagedAlarms （ 預設組態設定檔 ） 和CustomerManagedAlarms （ 自訂組態設定檔 ）。

- 預設組態設定檔：
  - 此設定檔中找到的組態包含 AMS Accelerate 在所有客戶帳戶中部署的預設組態。此組態包含預設 AMS Accelerate 監控政策，您不應修改此政策，因為 AMS Accelerate 可以隨時更新此設定檔，清除您所做的任何變更。
  - 如果您想要修改或停用任何這些定義，請參閱 修改加速警示預設組態和 停用預設加速警示組態。
- 自訂組態設定檔：
  - 此設定檔中的任何組態完全由您管理；除非您明確請求，否則 AMS Accelerate 不會覆寫此設定檔。
  - 您可以在此設定檔中指定您想要的任何自訂警示定義，也可以指定對 AMS Accelerate 受管預設組態的修改。如需詳細資訊，請參閱修改加速警示預設組態及停用預設加速警示組態。
  - 如果您更新此設定檔，Alarm Manager 會自動強制執行您 AWS 帳戶中所有相關資源的變更。請注意，雖然您的變更會自動生效，但最多可能需要 60 分鐘才能生效。
  - 您可以使用 AWS Management Console 或 AWS CLI/SDK 工具來更新此設定檔。如需更新組態的指示，請參閱 AWS AppConfig 使用者指南。
  - 自訂設定檔一開始是空的；不過，除了預設組態之外，還會強制執行設定檔文件中放置的任何警示定義。

警示管理員建立的所有 CloudWatch 警示都包含標籤金鑰 ams：alarm-manager：managed 和標籤值 true。這是為了確保警示管理員僅管理其建立的警示，而不會干擾您自己的任何警示。您可以使用 Amazon CloudWatch ListTagsForResource API 來查看這些標籤。

> **Important**
>
> 如果使用相同的 ConfigurationID 指定自訂警示定義和預設警示定義 （ 請參閱 加速組態設定檔：監控)，則自訂定義會優先於預設規則。

Accelerate Alarm Manager 入門

根據預設，當您使用 AMS Accelerate 加入時，您的組態會部署到 AWS AppConfig，為您的 資源定義警示基準。警示定義只會套用至具有 ams：rt：* 標籤的資源。我們建議您使用 套用這些標籤加速資源交錯：您可以設定基本的 Resource Tagger 組態，讓 AMS Accelerate 知道您想要管理哪些資源。

使用 Resource Tagger 將標籤索引鍵 ams：rt：ams-managed with tag value true 套用至您希望 AMS Accelerate 監控的任何資源。

以下是 Resource Tagger 自訂設定檔範例，您可以用來選擇加入以監控所有 Amazon EC2 執行個體。如需一般資訊，請參閱 加速資源交錯。

```
{
    "AWS::EC2::Instance": {
        "AMSManageAllEC2Instances": {
            "Enabled": true,
            "Filter": {
                "InstanceId": "*"
            },
            "Tags": [
                {
                    "Key": "ams:rt:ams-managed",
                    "Value": "true"
                }
            ]
        }
    }
}
```

如需如何套用此 Resource Tagger 組態的資訊，請參閱 檢視或變更 Resource Tagger 組態。

加速警示管理員標籤

根據預設，當您使用 AMS Accelerate 加入時，您的組態會部署到 AWS AppConfig，為您的 資源定義警示基準。警示定義只會套用至具有 ams：rt：* 標籤的資源。我們建議您使用 套用這些標籤加速資源交錯：您可以設定基本的 Resource Tagger 組態，讓 AMS Accelerate 知道您想要管理哪些資源。

使用 Resource Tagger 將標籤索引鍵 ams：rt：ams-managed with tag value true 套用至您希望 AMS Accelerate 監控的任何資源。

主題

使用 Resource Tagger 加速標籤

標籤型警示管理員會管理每個資源 CloudWatch 警示的生命週期；不過，它需要受管資源具有 AMS Accelerate 定義的特定標籤。若要使用 Resource Tagger 將預設的 AMS 受管警示集套用至 Linux 和 Windows 型執行個體，請遵循下列步驟。

1. 瀏覽至您帳戶中的 AppConfig 主控台。
2. 選取 ResourceTagger 應用程式。
3. 選取組態設定檔索引標籤，然後選取 CustomerManagedTags。
4. 按一下建立以建立新的設定檔。
5. 選取 JSON 並定義您的組態。如需篩選條件和平台定義的更多範例，請參閱 加速資源交錯。

```
{
"AWS::EC2::Instance": {
   "MonitorAllInstances": {
       "Enabled": true,
       "Filter": {
           "Platform": "*"
       },
       "Tags": [
           {
               "Key": "ams:rt:ams-managed",
               "Value": "true"
```

```
            }
        ]
    }
}
}
```

6. 按一下建立託管組態版本。
7. 按一下開始部署。
8. 定義下列部署詳細資訊：

```
Environment: AMSInfrastructure Hosted configuration version: <Select the version
 that you have just created>
               Deployment Strategy: AMSNoBakeDeployment
```

9. 按一下開始部署。

您的執行個體會加上 標記"ams:rt:ams-managed": "true"，以確保將額外的 "ams:rt:ams-monitoring-policy": "ams-monitored"和 "ams:rt:ams-monitoring-policy-platform": "ams-monitored-linux" 套用至執行個體。然後，這些標籤會導致為執行個體建立適當的警示。如需此程序的詳細資訊，請參閱在 Accelerate 中監控。

觀看 Himanshu 的影片以進一步了解 (11：04)

無需 Resource Tagger 即可加速標籤

標籤型警示管理員會管理每個資源 CloudWatch 警示的生命週期；不過，它需要受管資源具有 AMS Accelerate 定義的特定標籤。AMS Accelerate 提供預設組態設定檔，假設您的標籤已由 Resource Tagger 套用。

如果您想要使用替代方法來將標籤套用至資源，例如 AWS CloudFormation 或 Terraform，而不是 Resource Tagger，則需要停用 Resource Tagger，使其不會將標籤套用至您的資源，並與您選擇的標記方法競爭。如需變更自訂 Resource Tagger 組態設定檔以啟用唯讀模式的說明，請參閱 防止 Resource Tagger 修改資源。

在將 Resource Tagger 設定為唯讀模式並部署組態設定檔之後，請根據下列準則，使用您選擇的標記方法將標籤套用至您的資源：

資源類型	標籤鍵	標籤值
所有支援的資源 （此表格中所述）	ams:rt:ams-monitoring-policy	ams-monitored
EC2 執行個體 (Linux)	ams：rt：ams-monitoring-policy-platform	ams-monitored-linux
EC2 執行個體 (Windows)	ams：rt：ams-monitoring-policy-platform	ams-monitored-windows
使用 KMS 的 OpenSearch 網域	ams：rt：ams-monitoring-with-kms	ams-monitored-with-kms
具有專用主節點的 OpenSearch 網域	ams：rt：ams-monitoring-with-master	ams-monitored-with-master

具有這些標籤索引鍵和值的資源由 AMS Accelerate Alarm Manager 管理。

使用 加速標籤 AWS CloudFormation

> **Note**
>
> 在使用 套用標籤之前，請確定您已將 Resource Tagger 設定為唯讀模式 AWS CloudFormation，否則 Resource Tagger 可能會根據組態描述檔修改標籤。如需將 Resource Tagger 設定為唯讀模式的資訊，以及提供您自己的標籤的指導方針，請參閱 無需 Resource Tagger 即可加速標籤。

若要使用 套用標籤 AWS CloudFormation，您可以在堆疊層級套用標籤 （請參閱 CloudFormation 資源標籤），或在個別資源層級套用標籤 （例如，請參閱建立 EC2 執行個體標籤）。

以下是如何將 AMS Accelerate 警示管理標籤套用至由 管理的 Amazon EC2 執行個體的範例 AWS CloudFormation：

```
Type: AWS::EC2::Instance
Properties:
 InstanceType: "t3.micro"
```

```
 # ...other properties...

 Tags:
   - Key: "aws:rt:ams-monitoring-policy"
     Value: "ams-monitored"
   - Key: "aws:rt:ams-monitoring-policy-platform"
     Value: "ams-monitored-linux"
```

以下是如何將 AMS Accelerate 警示管理標籤套用至由 管理的 Auto Scaling 群組的範例 AWS CloudFormation。請注意，Auto Scaling 群組會將標籤傳播到由其建立的 Amazon EC2 執行個體：

```
Type: AWS::AutoScaling::AutoScalingGroup
Properties:
 AutoScalingGroupName: "TestASG"

 # ...other properties...

 Tags:
   - Key: "aws:rt:ams-monitoring-policy"
     Value: "ams-monitored"
   - Key: "aws:rt:ams-monitoring-policy-platform"
     Value: "ams-monitored-linux"
```

使用 Terraform 加速標籤

> **Note**
>
> 在使用 套用標籤之前，請確定您已將 Resource Tagger 設定為唯讀模式 AWS CloudFormation，否則 Resource Tagger 可能會根據組態描述檔修改標籤。如需將 Resource Tagger 設定為唯讀模式的資訊，以及提供您自己的標籤的指導方針，請參閱 無需 Resource Tagger 即可加速標籤。

如需如何使用 Terraform 管理資源標籤的說明，請參閱 Terraform 文件資源標記。

以下是如何將 AMS Accelerate 警示管理標籤套用至 Terraform 管理的 Amazon EC2 執行個體的範例。

```
resource "aws_instance" "test_linux_instance" {
     # ...ami and other properties...
```

```
    instance_type = "t3.micro"

    tags = {
      "aws:rt:ams-monitoring-policy" = "ams-monitored"
      "aws:rt:ams-monitoring-policy-platform" = "ams-monitored-linux"
    }
  }
```

以下是如何將 AMS 警示管理標籤套用至 Terraform 管理的 Auto Scaling 群組的範例。請注意，Auto Scaling 群組會將標籤傳播至由其建立的 EC2 執行個體：

```
resource "aws_autoscaling_group" "test_asg" {
name = "terraform-test"
# ...other properties...

tags = {
  "aws:rt:ams-monitoring-policy" = "ams-monitored"
  "aws:rt:ams-monitoring-policy-platform" = "ams-monitored-linux"
}
}
```

加速警示管理員組態設定檔

當您的帳戶加入 AMS Accelerate 時，兩個稱為組態設定檔的 JSON 文件會透過 AWS AppConfig 部署在您的帳戶中（請參閱什麼是 AWS AppConfig)。這兩個設定檔文件都位於 Alarm Manager 應用程式和 AMS Accelerate 基礎設施環境中。

主題

- 停用預設加速警示組態

加速組態設定檔：監控

預設組態設定檔文件和自訂組態設定檔文件都遵循相同的結構 ：

```
  {
    "<ResourceType>": {
        "<ConfigurationID>": {
            "Enabled": true,

            "Tag": {
                "Key": "...",
                "Value": "..."
            },
            "AlarmDefinition": {
                ...
            }
        },
        "<ConfigurationID>": {
            ...
        }
    },
    "<ResourceType>": {
        ...
    }
}
```

- ResourceType：此金鑰必須是下列其中一個支援的字串。此 JSON 物件中的組態只會與指定的 AWS 資源類型相關聯。支援的資源類型：

```
AWS::EC2::Instance
AWS::EC2::Instance::Disk
AWS::RDS::DBInstance
AWS::RDS::DBCluster
AWS::Elasticsearch::Domain
AWS::OpenSearch::Domain
AWS::Redshift::Cluster
AWS::ElasticLoadBalancingV2::LoadBalancer
AWS::ElasticLoadBalancingV2::LoadBalancer::TargetGroup
AWS::ElasticLoadBalancing::LoadBalancer
AWS::FSx::FileSystem::ONTAP
```

```
AWS::FSx::FileSystem::ONTAP::Volume
AWS::FSx::FileSystem::Windows
AWS::EFS::FileSystem
AWS::EC2::NatGateway
AWS::EC2::VPNConnection
```

- ConfigurationID：此金鑰在設定檔中必須是唯一的，並唯一命名下列組態區塊。如果相同 ResourceType 區塊中的兩個組態區塊具有相同的 ConfigurationID，則設定檔中顯示的最新組態區塊會生效。如果您在自訂設定檔中指定與預設設定檔中指定的ConfigurationID，則自訂設定檔中定義的組態區塊會生效。
  - 已啟用：（選用， default=true) 指定組態區塊是否生效。將此設定為 false 以停用組態區塊。停用的組態區塊的行為就好像在設定檔中不存在一樣。
  - 標籤：指定此警示定義套用的標籤。具有此標籤索引鍵和值的任何資源（適當資源類型）都會使用指定的定義建立 CloudWatch 警示。此欄位是具有下列欄位的 JSON 物件：
    - 金鑰：要比對之標籤的金鑰。請注意，如果您使用 Resource Tagger 將標籤套用至資源，則標籤的金鑰一律會以ams：rt： 開頭。
    - 值：要比對的標籤值。
  - AlarmDefinition：定義要建立的警示。這是 JSON 物件，其欄位會依原狀傳遞至 CloudWatch `PutMetricAlarm` API 呼叫（虛擬參數除外；如需詳細資訊，請參閱 加速組態設定檔：虛擬參數替換)。如需哪些欄位是必要欄位的詳細資訊，請參閱 PutMetricAlarm 文件。

    或

    CompositeAlarmDefinition：定義要建立的複合警示。當您建立複合警示時，您可以指定警示的規則表達式，該規則表達式會將您建立的其他警示的警示狀態納入考量。這是 JSON 物件，其欄位會依原狀傳遞至 `CloudWatchPutCompositeAlarm`。僅在符合規則的所有條件時，複合警示才會進入 ALARM 狀態。複合警示規則表達式中指定的警示可以包括指標警示和其他複合警示。如需有關需要哪些欄位的資訊，請參閱 PutCompositeAlarm 文件。

    這兩個選項都提供下列欄位：

    - AlarmName：指定您要為資源建立的警示名稱。此欄位具有與 PutMetricAlarm 文件指定的所有相同規則；不過，由於警示名稱在區域中必須是唯一的，因此警示管理員有一項額外要求：您必須在警示名稱中指定唯一識別符虛擬參數（否則，警示管理員會將資源的唯一識別符附加到警示名稱的前面）。例如，對於 AWS::EC2::Instance 資源類型，您必須在警示名稱`${EC2::InstanceId}`中指定 ，或在警示名稱的開頭隱含新增它。如需識別符清單，請參閱 加速組態設定檔：虛擬參數替換。

      所有其他欄位如 PutMetricAlarm 或 PutCompositeAlarm 文件中所指定。

- AlarmRule：指定要評估哪些其他警示來判斷此複合警示的狀態。對於您參考的每個警示，它們必須存在於 CloudWatch 中，或在帳戶中的警示管理員組態設定檔中指定。

> **Important**
>
> 您可以在 Alarm Manager 組態文件中指定 AlarmDefinition 或 CompositeAlarmDefinition，但兩者無法同時使用。

在下列範例中，系統會在兩個指定的指標警示超過閾值時建立警示：

```
{
  "AWS::EC2::Instance": {
    "LinuxResourceAlarm": {
      "Enabled": true,
      "Tag": {
        "Key": "ams:rt:mylinuxinstance",
        "Value": "true"
      },
      "CompositeAlarmDefinition": {
        "AlarmName": "${EC2::InstanceId} Resource Usage High",
        "AlarmDescription": "Alarm when a linux EC2 instance is using too much CPU and
 too much Disk",
        "AlarmRule": "ALARM(\"${EC2::InstanceId}: Disk Usage Too High -
 ${EC2::Disk::UUID}\") AND ALARM(\"${EC2::InstanceId}: CPU Too High\")"
      }
    }
  }
}
```

> **Important**
>
> 當警示管理員因為組態中斷而無法建立或刪除警示時，它會將通知傳送至 Direct-Customer-Alerts SNS 主題。此警示稱為 AlarmDependencyError。
> 強烈建議您已確認訂閱此 SNS 主題。若要接收發佈至主題的訊息，您必須訂閱 主題的端點。
> 如需詳細資訊，請參閱步驟 1：建立主題。

> **Note**
>
> 建立異常偵測警示時，警示管理員會自動為指定的指標建立所需的異常偵測模型。刪除異常偵測警示時，警示管理員不會刪除相關聯的異常偵測模型。
> Amazon CloudWatch 會限制您在指定區域中可以擁有的異常偵測模型數量 AWS 。如果您超過模型配額，警示管理員不會建立新的異常偵測警示。您必須刪除未使用的模型，或與您的 AMS 合作夥伴合作以請求提高限制。
> 許多 AMS Accelerate 提供的基準警示定義會將 SNS 主題 MMS-Topic 列為目標。這是用於 AMS Accelerate 監控服務，也是您的警示通知到達 AMS Accelerate 的傳輸機制。請勿將 MMS-Topic 指定為基準中所提供之警示（以及相同警示的覆寫）以外的任何警示的目標，因為服務會忽略未知的警示。這不會導致 AMS Accelerate 對您的自訂警示採取行動。

加速組態設定檔：虛擬參數替換

在任一組態設定檔中，您可以指定替代的虛擬參數，如下所示：

- 全域 - 設定檔中的任何位置：
  - ${AWS：：AccountId}：以 AWS 您的帳戶 ID 取代
  - ${AWS：：Partition}：以資源所在的分割區取代 AWS 區域（對於大多數區域為「aws」）；如需詳細資訊，請參閱 ARN 參考中的分割區項目。
  - ${AWS：：Region}： 取代為資源部署所在區域的區域名稱（例如 us-east-1)
- 在 AWS::EC2::Instance 資源類型區塊中：
  - ${EC2：：InstanceId}： (識別符) 已由 Amazon EC2 執行個體的執行個體 ID 取代。
  - ${EC2：：InstanceName}： 已由 Amazon EC2 執行個體的名稱取代。
- 在 AWS::EC2::Instance：：Disk 資源類型區塊中：
  - ${EC2：：InstanceId}： (識別符) 以 Amazon EC2 執行個體的執行個體 ID 取代。
  - ${EC2：：InstanceName}：以 Amazon EC2 執行個體的名稱取代。
  - ${EC2：：Disk：：Device}： (識別符) 以磁碟的名稱取代。（僅限 Linux，適用於 CloudWatch Agent 管理的執行個體）。
  - ${EC2：：Disk：：FSType}： (識別符) 以磁碟的檔案系統類型取代。（僅限 Linux，適用於 CloudWatchAgent 管理的執行個體）。
  - ${EC2：：Disk：：Path}： (識別符) 由磁碟路徑取代。在 Linux 上，這是磁碟的掛載點（例如 /)，而在 Windows 中，這是磁碟機標籤（例如 c：/）（僅適用於由 CloudWatch Agent 管理的執行個體）。

  - ${EC2：：Disk：：UUID}：(識別符) 由唯一識別磁碟的產生 UUID 取代，這必須在警示名稱中指定為 AWS::EC2::Instance：：Disk 資源類型下的警示，每個磁碟區都會建立一個警示。指定 ${EC2：：Disk：：UUID} 將維持警示名稱的唯一性。
- 在 AWS::EKS::Cluster 資源類型區塊中：
  - ${EKS：：ClusterName}：(識別符) 已由 EKS 叢集的名稱取代。
- 在 AWS::OpenSearch::Domain 資源類型區塊中：
  - ${OpenSearch：：DomainName}：(識別符) 被您的 EKS 網域名稱取代。
- 在 AWS::ElasticLoadBalancing::LoadBalancer 資源類型區塊中：
  - ${ElasticLoadBalancing：：LoadBalancer：：Name}：(識別符) 已由 V1 Load Balancer 的名稱取代。
- 在 AWS::ElasticLoadBalancingV2::LoadBalancer 資源類型區塊中：
  - ${ElasticLoadBalancingV2：：LoadBalancer：：Arn}：(識別符) 已由 V2 Load Balancer 的 ARN 取代。
  - ${ElasticLoadBalancingV2：：LoadBalancer：：Name}：(識別符) 已由 V2 Load Balancer 的名稱取代。
  - ${ElasticLoadBalancingV2：：LoadBalancer：：FullName}：(識別符) 已由 V2 Load Balancer 的完整名稱取代。
- 在 AWS::ElasticLoadBalancingV2::LoadBalancer：：TargetGroup 資源類型區塊中：
  - ${ElasticLoadBalancingV2：：TargetGroup：FullName}：(識別符) 已由 V2 Load Balancer 的目標群組名稱取代。
  - ${ElasticLoadBalancingV2：：TargetGroup：：UUID}：(識別符)，由 V2 Load Balancer 產生的 UUID 取代。
- 在 AWS::EC2::NatGateway 資源類型區塊中：
  - ${NatGateway：：NatGatewayId}：(識別符) 已由 NAT Gateway ID 取代。
- 在 AWS::RDS::DBInstance 資源類型區塊中：
  - ${RDS：：DBInstanceIdentifier}：(識別符) 已由 RDS 資料庫執行個體識別符取代。
- 在 AWS::RDS::DBCluster 資源類型區塊中：
  - ${RDS：：DBClusterIdentifier}：(識別符) 已由 RDS 資料庫叢集識別符取代。
- 在 AWS::Redshift::Cluster 資源類型區塊中：
  - ${Redshift：：ClusterIdentifier}：(Identifier) 已由 Redshift 叢集識別符取代。
- 在 AWS::Synthetics::Canary 資源類型區塊中：
  - ${Synthetics：：CanaryName}：(識別符) 已由 CloudWatch Synthetics Canary 的名稱取代。

- 在 AWS::EC2::VPNConnection 資源類型區塊中：
  - ${AWS::EC2::VpnConnectionId}：(識別符) 已由您的 VPN ID 取代。
- 在 AWS::EFS::FileSystem 資源類型區塊中：
  - ${EFS：：FileSystemId}：(識別符) 以 EFS 檔案系統的檔案系統 ID 取代。
- 在 AWS::FSx::FileSystem：：ONTAP 資源類型區塊中：
  - ${FSx：：FileSystemId}：(識別符) 以 FSX 檔案系統的檔案系統 ID 取代。
  - ${FSx：：FileSystem：：Throughput}：以 FSX 檔案系統的輸送量取代。
  - ${FSx：：FileSystem：：Iops}：取代為 FSX 檔案系統的 IOPS。
- 在 AWS::FSx::FileSystem：：ONTAP：：Volume 資源類型區塊中：
  - ${FSx：：FileSystemId}：(識別符) 以 FSX 檔案系統的檔案系統 ID 取代。
  - ${FSx：：ONTAP：：VolumeId}：(識別符) 以磁碟區 ID 取代。
- 在 AWS::FSx::FileSystem：：Windows 資源類型區塊中：
  - ${FSx：：FileSystemId}：(識別符) 以 FSX 檔案系統的檔案系統 ID 取代。
  - ${FSx：：FileSystem：：Throughput}：以 FSX 檔案系統的輸送量取代。

> **Note**
>
> 除非您在警示名稱中指定該識別符，否則所有標記有識別符的參數都會做為已建立警示名稱的字首。

加速警示組態範例

在下列範例中，系統會為每個連接至相符 Linux 執行個體的磁碟建立警示。

```
{
    "AWS::EC2::Instance::Disk": {
        "LinuxDiskAlarm": {
            "Tag": {
                "Key": "ams:rt:mylinuxinstance",
                "Value": "true"
            },
            "AlarmDefinition": {
                "MetricName": "disk_used_percent",
                "Namespace": "CWAgent",
                "Dimensions": [
```

```
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
                    },
                    {
                        "Name": "device",
                        "Value": "${EC2::Disk::Device}"
                    },
                    {
                        "Name": "fstype",
                        "Value": "${EC2::Disk::FSType}"
                    },
                    {
                        "Name": "path",
                        "Value": "${EC2::Disk::Path}"
                    }
                ],
                "AlarmName": "${EC2::InstanceId}: Disk Usage Too High -
 ${EC2::Disk::UUID}"
                ...
            }
        }
    }
}
```

在下列範例中，系統會為每個連接至相符 Windows 執行個體的磁碟建立警示。

```
{
     "AWS::EC2::Instance::Disk": {
        "WindowsDiskAlarm": {
            "Tag": {
                "Key": "ams:rt:mywindowsinstance",
                "Value": "true"
            },
            "AlarmDefinition": {
                "MetricName": "LogicalDisk % Free Space",
                "Namespace": "CWAgent",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
                    },
                    {
```

```
                        "Name": "objectname",
                        "Value": "LogicalDisk"
                    },
                    {
                        "Name": "instance",
                        "Value": "${EC2::Disk::Path}"
                    }
                ],
                "AlarmName": "${EC2::InstanceId}: Disk Usage Too High -
 ${EC2::Disk::UUID}"
                ...
            }
        }
    }
}
```

檢視您的 Accelerate Alarm Manager 組態

AMSManagedAlarms 和 CustomerManagedAlarms 都可以在 AppConfig with GetConfiguration 中檢閱。

以下是 GetConfiguration呼叫的範例：

```
aws appconfig get-configuration --application AMSAlarmManager --environment
 AMSInfrastructure --configuration AMSManagedAlarms --client-id
      any-string outfile.json
```

- 應用程式：這是 AppConfig 提供功能的邏輯單位；對於警示管理員，這是 AMSAlarmManager
- 環境：這是 AMSInfrastructure 環境
- 組態：若要檢視 AMS Accelerate 基準警示，值為 AMSManagedAlarms；若要檢視客戶警示定義，組態為 CustomerManagedAlarms
- 用戶端 ID：這是唯一的應用程式執行個體識別符，可以是任何字串
- 您可以在指定的輸出檔案中檢視警示定義，在此案例中為 outfile.json

您可以在 AMSInfrastructureenvironment 中檢視過去的部署，以查看部署至您帳戶的組態版本。

變更加速警示組態

若要新增或更新新的警示定義，您可以部署組態文件 使用 AWS CloudFormation 來部署加速組態變更，或叫用 CreateHostedConfigurationVersion API。

這是 Linux 命令列命令，可在 base64 中產生參數值，這是 AppConfig CLI 命令預期的值。如需詳細資訊，請參閱 AWS CLI 文件 Binary/Blob （二進位大型物件）。

舉例來說：

```
aws appconfig create-hosted-configuration-version --application-id application-id --
configuration-profile-id configuration-profile-id --content base64-string
      --content-type application/json
```

- 應用程式 ID：應用程式 AMS AlarmManager 的 ID；您可以透過 ListApplications API 呼叫找到此資訊。
- 組態設定檔 ID：CustomerManagedAlarms 組態的 ID；您可以透過 ListConfigurationProfiles API 呼叫找到此資訊。
- 內容：要建立內容的 Base64 字串，方法是在 base64 中建立文件並對其進行編碼：cat alarm-v2.json | base64 （請參閱 Binary/Blob （二進位大型物件））。

  內容類型：MIME 類型，`application/json`因為警示定義是以 JSON 撰寫。

> **Important**
>
> 將對 StartDeployment 和 StopDeployment API 動作的存取限制在瞭解將新組態部署至目標的責任和後果的受信任使用者。

若要進一步了解如何使用 AWS AppConfig 功能來建立和部署組態，請參閱使用 AWS AppConfig。

修改加速警示預設組態

雖然您無法修改預設組態設定檔，但您可以在自訂設定檔中使用與預設組態區塊相同的 ConfigurationID 來指定組態區塊，以提供預設值的覆寫。如果您這樣做，整個組態區塊會覆寫要套用標記組態的預設組態區塊。

例如，請考慮下列預設組態設定檔：

```
{
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": true,
            "Tag": {
```

```
                "Key": "ams:rt:ams-monitoring-policy",
                "Value": "ams-monitored"
            },
            "AlarmDefinition": {
                "AlarmName": "${EC2::InstanceId}: AMS Default Alarm",
                "Namespace": "AWS/EC2",
                "MetricName": "CPUUtilization",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
                    }
                ],
                "Threshold": 5,
                ...
            }
        }
    }
}
```

若要將此警示的閾值變更為 10，您必須提供整個警示定義，而不只是要變更的部分。例如，您可以提供下列自訂設定檔：

```
{
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": true,
            "Tag": {
                "Key": "ams:rt:ams-monitoring-policy",
                "Value": "ams-monitored"
            },
            "AlarmDefinition": {
                "AlarmName": "${EC2::InstanceId}: AMS Default Alarm",
                "Namespace": "AWS/EC2",
                "MetricName": "CPUUtilization",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
                    }
                ],
                "Threshold": 10,
                ...
```

```
            }
        }
    }
}
```

> **Important**
>
> 請記得在進行組態變更之後部署組態變更。在 SSM AppConfig 中，您必須在建立組態後部署新版本。

部署加速警示組態變更

完成自訂後，您需要使用 AppConfig 或 部署它 AWS CloudFormation。

主題

- 使用 AppConfig 部署加速警示組態變更
- 使用 AWS CloudFormation 來部署加速組態變更

使用 AppConfig 部署加速警示組態變更

自訂完成後，請使用 AppConfig 透過 StartDeployment 部署您的變更。

```
  aws appconfig start-deployment --application-id application_id
   --environment-id environment_id Vdeployment-strategy-id
   deployment_strategy_id --configuration-profile-id configuration_profile_id --
configuration-version 1
```

- 應用程式 ID：應用程式 的 IDAMSAlarmManager，您可以使用 ListApplications API 呼叫找到它。
- 環境 ID：您可以使用 ListEnvironments API 呼叫找到此 ID。
- 部署策略 ID：您可以使用 ListDeploymentStrategies API 呼叫找到此選項。
- 組態設定檔 ID： 的 IDCustomerManagedAlarms；您可以使用 ListConfigurationProfiles API 呼叫找到此 ID。
- 組態版本：要部署的組態設定檔版本。

> **Important**
>
> 警示管理員會套用組態設定檔中指定的警示定義。使用 AWS Management Console 或 CloudWatch CLI/SDK 對 CloudWatch 警示所做的任何手動修改都會自動還原，因此請確定您的變更是透過 Alarm Manager 定義。若要了解警示管理員建立哪些警示，您可以尋找值為的`ams:alarm-manager:managed`標籤`true`。
> 將 StartDeployment 和 StopDeployment API 動作的存取權限制為信任的使用者，這些使用者了解將新組態部署到目標的責任和後果。

若要進一步了解如何使用 AWS AppConfig 功能來建立和部署組態，請參閱 AWS AppConfig 文件。

使用 AWS CloudFormation 來部署加速組態變更

如果您想要使用 部署`CustomerManagedAlarms`組態設定檔 AWS CloudFormation，您可以使用下列 AWS CloudFormation 範本。將您想要的 JSON 組態放在 `AMSAlarmManagerConfigurationVersion.Content` 欄位中。

當您在 AWS CloudFormation 堆疊或堆疊集中部署範本時，如果您未遵循組態所需的 JSON 格式，`AMSResourceTaggerDeployment`資源的部署將會失敗。加速組態設定檔：監控 如需預期格式的詳細資訊，請參閱 。

如需將這些範本部署為 CloudFormation 堆疊或堆疊集的說明，請參閱下列相關的 AWS CloudFormation 文件：

- 在 AWS CloudFormation 主控台上建立堆疊
- 使用 AWS CLI 建立堆疊
- 建立堆疊集

> **Note**
>
> 如果您使用其中一個範本部署組態版本，然後刪除 CloudFormation 堆疊/堆疊集，則範本組態版本會保留為目前部署的版本，而且不會進行任何額外的部署。如果您想要還原為預設組態，您將需要手動部署空白組態 （ 即僅 {}），或將堆疊更新為空白組態，而不是刪除堆疊。

JSON

```
{
  "Description": "Custom configuration for the AMS Alarm Manager.",
  "Resources": {
    "AMSAlarmManagerConfigurationVersion": {
      "Type": "AWS::AppConfig::HostedConfigurationVersion",
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-ApplicationId"
        },
        "ConfigurationProfileId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-
ProfileID"
        },
        "Content": "{}",
        "ContentType": "application/json"
      }
    },
    "AMSAlarmManagerDeployment": {
      "Type": "AWS::AppConfig::Deployment",
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-ApplicationId"
        },
        "ConfigurationProfileId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-
ProfileID"
        },
        "ConfigurationVersion": {
          "Ref": "AMSAlarmManagerConfigurationVersion"
        },
        "DeploymentStrategyId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-Deployment-StrategyID"
        },
        "EnvironmentId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-EnvironmentId"
        }
      }
    }
  }
}
```

YAML

```
Description: Custom configuration for the AMS Alarm Manager.
Resources:
  AMSAlarmManagerConfigurationVersion:
    Type: AWS::AppConfig::HostedConfigurationVersion
    Properties:
      ApplicationId:
        !ImportValue AMS-Alarm-Manager-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-ProfileID
      Content: |
        {

        }
      ContentType: application/json
  AMSAlarmManagerDeployment:
    Type: AWS::AppConfig::Deployment
    Properties:
      ApplicationId:
        !ImportValue AMS-Alarm-Manager-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-ProfileID
      ConfigurationVersion:
        !Ref AMSAlarmManagerConfigurationVersion
      DeploymentStrategyId:
        !ImportValue AMS-Alarm-Manager-Configuration-Deployment-StrategyID
      EnvironmentId:
        !ImportValue AMS-Alarm-Manager-Configuration-EnvironmentId
```

轉返 加速警示變更

您可以指定先前的組態設定檔版本並執行 StartDeployment，透過相同的部署機制轉返警示定義。

保留加速警示

刪除 AMS 監控的資源時，警示管理員為這些資源建立的任何警示都會由警示管理員自動刪除。如果您需要保留特定警示以進行稽核、合規或歷史用途，請使用警示管理員保留標記功能。

若要即使在刪除警示受監控的資源之後仍保留警示，請將 "ams:alarm-manager:retain" 標籤新增至警示的自訂組態，如下列範例所示。

```
{
  "AWS::EC2::Instance": {
```

```
    "AMSCpuAlarm": {
      "Enabled": true,
      "Tag": {
        "Key": "ams:rt:ams-monitoring-policy",
        "Value": "ams-monitored"
      },
      "AlarmDefinition": {
        "AlarmName": "${EC2::InstanceId}: CPU Too High",
        "AlarmDescription": "AMS Baseline Alarm for EC2 CPUUtilization",
        [...]
        "Tags": [
          {
            "Key": "ams:alarm-manager:retain",
            "Value": "true"
          }
        ]
      }
    }
  }
}
```

使用 "ams:alarm-manager:retain"標籤設定的警示，在受監控的資源終止時，警示管理員不會自動刪除。保留的警示會無限期保留在 CloudWatch 中，直到您使用 CloudWatch 手動將其移除為止。

停用預設加速警示組態

AMS Accelerate 會根據基準警示，在您的帳戶中提供預設組態設定檔。不過，您可以透過覆寫任何警示定義來停用此預設組態。您可以透過覆寫自訂組態設定檔中規則的 ConfigurationID，並使用 false 值指定啟用的欄位，來停用預設組態規則。

例如，如果預設組態設定檔中存在下列組態：

```
{
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": true,
            "Tag": {
                "Key": "ams:rt:ams-monitoring-policy",
                "Value": "ams-monitored"
            },
            "AlarmDefinition": {
                ...
            }
```

```
        }
    }
```

您可以在自訂組態設定檔中包含下列項目，以停用此標記規則：

```
{
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": false
        }
    }
}
```

若要進行這些變更，必須使用 JSON 設定檔文件呼叫 CreateHostedConfigurationVersion API（請參閱 變更加速警示組態)，隨後必須部署（請參閱 部署加速警示組態變更)。請注意，當您建立新的組態版本時，您還必須在 JSON 設定檔文件中包含任何先前建立的自訂警示。

> **Important**
>
> 當 AMS Accelerate 更新預設組態設定檔時，不會針對您設定的自訂警示進行校正，因此當您在自訂組態設定檔中覆寫預設警示時，請檢閱預設警示的變更。

為 Accelerate 建立其他 CloudWatch 警示

您可以使用 Amazon EC2 執行個體的自訂 CloudWatch 指標和警示，為 AMS Accelerate 建立額外的 CloudWatch 警示。

產生您的應用程式監控指令碼和自訂指標。如需範例指令碼的詳細資訊和存取權，請參閱監控 Amazon EC2 Linux 執行個體的記憶體和磁碟指標。

Linux Amazon EC2 執行個體的 CloudWatch 監控指令碼示範如何產生和使用自訂 CloudWatch 指標。這些範例 Perl 指令碼包含功能完整的範例，可報告 Linux 執行個體的記憶體、交換和磁碟空間使用率指標。

> **Important**
>
> AMS Accelerate 不會監控您建立的 CloudWatch 警示。

檢視 Alarm Manager for Accelerate 監控的資源數量

警示管理員每小時將指標傳送至 AMS/AlarmManager 命名空間中的 Amazon CloudWatch。只會針對 Alarm Manager 支援的資源類型發出指標。

指標名稱	維度	描述
ResourceCount	元件、ResourceType	在此區域中部署的資源數量（指定資源類型的）。 單位：計數
ResourcesMissingManagedAlarms	元件、ResourceType	需要受管警示但 Alarm Manager 尚未套用警示的資源數量（指定資源類型的）。 單位：計數
UnmanagedResources	元件、ResourceType	未由 Alarm Manager 套用任何受管警示的資源（指定資源類型的）數量。一般而言，這些資源不符合任何 Alarm Manager 組態區塊，或明確地從組態區塊中排除。 單位：計數
MatchingResourceCount	元件、ResourceType、ConfigClauseName	（指定資源類型的）符合 Alarm Manager 組態區塊的資源數量。若要讓資源符合組態區塊，必須啟用該區塊，且資源必須在組態區塊中指定相同的標籤。 單位：計數

這些指標也可以在 AMS-Alarm-Manager-Reporting-Dashboard 中以圖形形式檢視。若要查看儀表板，請從 AWS CloudWatch 管理主控台選取 AMS-Alarm-Manager-Reporting-Dashboard。根據預設，此儀表板中的圖形會顯示過去 12 小時期間的資料。

AMS Accelerate 會將 CloudWatch 警示部署到您的 帳戶，以偵測未受管資源數量的顯著增加，例如 AMS Alarm Manager 從管理中排除的資源。AMS Operations 將調查超過以下三個未受管資源的增加：相同類型的三個資源，或相同類型的所有資源增加 50%。如果變更似乎不是刻意的，AMS Operations 可能會與您聯絡以檢閱變更。

AMS 自動修復提醒

驗證後，AWS Managed Services (AMS) 會根據本節所述的特定條件和程序，自動修復特定提醒。

提醒名稱	描述	閾值	動作
狀態檢查失敗	可能的硬體故障或執行個體的故障狀態。	系統在過去 15 分鐘內至少偵測到一次失敗狀態。	AMS 自動修復會先驗證執行個體是否可存取。如果無法存取執行個體，則會停止並重新啟動執行個體。停止和啟動可讓執行個體遷移至新的基礎硬體。如需詳細資訊，請參閱下列「EC2 狀態檢查失敗修復自動化」一節。
AMSLinuxDiskUsage	當 EC2 執行個體上 1 個掛載點（磁碟區上的指定空間）的磁碟用量填滿時觸發。	閾值在過去 30 分鐘超過定義的值 6 次。	AMS 自動修復會先刪除暫存檔案。如果這無法釋放足夠的磁碟空間，它會擴展磁碟區，以防止在磁碟區已滿時停機。
AMSWindowsDiskUsage	當 EC2 執行個體上 1 個掛載點（磁碟區上的指定空間）的磁碟用量填滿時。	閾值在過去 30 分鐘內超過定義的值 6 次。	AMS 自動修復會先刪除暫存檔案。如果這無法釋放足夠的磁碟空間，它會擴展磁碟區，以防止在磁碟區已滿時停機。
RDS-EVENT-0089	資料庫執行個體已消耗超過其分配儲存容量的 90%。	儲存空間配置超過 90%。	AMS 自動修復會先驗證資料庫是否處於可修改且可用或完整儲存狀態。然後，它會嘗試透過 CloudFormation 變更集增加配置的儲存、IOPS 和儲存輸送量。如果偵測到堆疊偏離，則會回到 RDS API 以防止停機時間。

提醒名稱	描述	閾值	動作
			將下列標籤新增至 RDS 資料庫執行個體，即可選擇退出此功能： "Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".
RDS-EVENT-0007	資料庫執行個體的配置儲存體已用盡。若要解決此問題，請配置額外的儲存空間。	儲存空間是 100% 配置。	AMS 自動修復會先驗證資料庫是否處於可修改且可用或完整儲存狀態。然後，它會嘗試透過 CloudFormation 變更集增加配置的儲存、IOPS 和儲存輸送量。如果偵測到堆疊偏離，則會回到 RDS API 以防止停機時間。 將下列標籤新增至 RDS 資料庫執行個體，即可選擇退出此功能： "Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".

提醒名稱	描述	閾值	動作
RDS-EVENT-0224	請求的配置儲存達到或超過設定的最大儲存閾值。	資料庫執行個體的最大儲存閾值已用盡，或大於或等於請求的已配置儲存。	AMS 自動修復會先驗證請求的 RDS 儲存量是否超過最大儲存閾值。如果確認，AMS 會嘗試使用 CloudFormation 變更集將最大儲存閾值提高 30%，如果資源未透過 CloudFormation 佈建，則請直接 RDS API。 將下列標籤新增至 RDS 資料庫執行個體，即可選擇退出此功能： `"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".`

提醒名稱	描述	閾值	動作
RDS-Storage-Capacity	少於 1GB 會保留在資料庫執行個體的配置儲存體中。	已配置 99% 的儲存空間。	AMS 自動修復會先驗證資料庫是否處於可修改且可用或完整儲存狀態。然後，它會嘗試透過 CloudFormation 變更集增加配置的儲存、IOPS 和儲存輸送量。如果偵測到堆疊偏離，則會回到 RDS API 以防止停機時間。 將下列標籤新增至 RDS 資料庫執行個體，即可選擇退出此功能： `"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".`

EC2 狀態檢查失敗：修復自動化備註

AMS 自動修復如何與 EC2 狀態檢查失敗問題搭配使用：

- 如果您的 Amazon EC2 執行個體無法連線，執行個體必須停止並再次啟動，才能遷移至新的硬體並復原。
- 如果問題的根目錄在作業系統中（缺少 fstab 中的裝置、核心損毀等），自動化將無法復原您的執行個體。
- 如果您的執行個體屬於 Auto Scaling 群組，自動化不會採取任何動作，AutoScalingGroup 擴展動作會取代執行個體。
- 如果您的執行個體已啟用 EC2 Auto Recovery，則修復不會採取動作。

EC2 磁碟區用量修復自動化

AWS Managed Services (AMS) 自動修復如何處理 EC2 磁碟區用量問題：

- 自動化會先驗證是否需要磁碟區擴展，以及是否可以執行。如果認為擴展是適當的，自動化可以增加磁碟區容量。此自動化程序會平衡成長需求與受控制的有限擴展。
- 在擴展磁碟區之前，自動化會在執行個體上執行清除任務 (Windows：磁碟清理程式、Linux：Logrotate + Simple Service Manager 代理程式日誌移除），以嘗試釋放空間。

> **Note**
>
> 清理任務不會在 EC2 "T" 系列執行個體上執行，因為它們依賴 CPU 點數來持續運作。

- 在 Linux 上，自動化僅支援擴展類型為 EXT2, EXT3, EXT4和 XFS 的檔案系統。
- 在 Windows 上，自動化僅支援新技術檔案系統 (NTFS) 和彈性檔案系統 (ReFS)。
- 自動化不會擴展屬於邏輯磁碟區管理員 (LVM) 或 RAID 陣列一部分的磁碟區。
- 自動化不會擴展執行個體存放區磁碟區。
- 如果受影響的磁碟區已大於 2 TiB，則自動化不會採取動作。
- 透過自動化的擴展限制為每週最多三次，系統生命週期內總計五次。
- 如果先前的擴展在過去六小時內發生，自動化不會擴展磁碟區。

當這些規則阻止自動化採取動作時，AMS 會透過傳出服務請求與您聯絡，以決定要採取的下一個動作。

Amazon RDS 低儲存體事件修復自動化

AWS Managed Services (AMS) 自動修復如何與 Amazon RDS 低儲存體事件問題搭配使用：

- 在嘗試擴展 Amazon RDS 執行個體儲存體之前，自動化會執行多項檢查，以確保 Amazon RDS 執行個體處於可修改且可用，或儲存已滿的狀態。
- 在偵測到 CloudFormation 堆疊偏離之處，修復會透過 Amazon RDS API 進行。
- 修復動作不會在下列情況下執行：
  - Amazon RDS 執行個體狀態不是「可用」或「完整儲存」。
  - Amazon RDS 執行個體儲存體目前無法修改（例如在過去六小時內修改儲存體時）。
  - Amazon RDS 執行個體已啟用自動擴展儲存。
  - Amazon RDS 執行個體不是 CloudFormation 堆疊中的資源。
- 修補限制為每六小時一次擴展，且在滾動十四天內不超過三次擴展。
- 當這些案例發生時，AMS 會透過傳出事件與您聯絡，以判斷下一個動作。

在 AMS 中使用 Amazon EventBridge 受管規則

AMS Accelerate 使用 Amazon EventBridge 受管規則。受管規則是直接連結至 AMS 的唯一規則類型。這些規則符合傳入的事件，並將其傳送至目標進行處理。受管規則由 AMS 預先定義，並包含服務管理客戶帳戶所需的事件模式，除非另有定義，否則只有擁有的服務才能利用這些受管規則。

AMS Accelerate 受管規則會連結到`events.managedservices.amazonaws.com`服務主體。這些受管規則是透過AWSServiceRoleForManagedServices_Events服務連結角色進行管理。若要刪除這些規則，客戶需要特別確認。如需詳細資訊，請參閱刪除 AMS 的受管規則。

如需規則的詳細資訊，請參閱《Amazon EventBridge 使用者指南》中的規則。

AMS 部署的 Amazon EventBridge 受管規則

Amazon EventBridge 受管規則

規則名稱	描述	定義

AmsAccessRolesRule	此規則會接聽特定 AMS Accelerate 角色和政策中的修改。	<pre>{
		"source": ["aws.iam"],
		"detail-type": ["AWS API Call via CloudTrail"],
		"detail": {
		"eventName": [
		"DeleteRole",
		"DeletePolicy",
		"CreatePolicyVersion",
		"AttachRolePolicy",
		"DetachRolePolicy"
		],
		"requestParameters": {
		"$or": [
		{
		"roleName": [
		"ams-access-admin",
		"ams-access-admin-operations",
		"ams-access-operations",
		"ams-access-read-only",
		"ams-access-security-analyst",
		"ams-access-security-analyst-
		read-only"
		]

規則名稱	描述	定義

```
            },
            {
                "policyArn": [
                    "arn:*:iam::*:policy/ams-ac
cess-allow-pass-role",
                    "arn:*:iam::*:policy/ams-ac
cess-deny-cloudshell-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-deny-operations-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-deny-update-iam-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-ssr-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-security-analyst-read-only-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-security-analyst-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-security-analyst-extended-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-admin-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-admin-operations-policy"
                ]
            },
          ]
        },
    },
}
```

規則名稱	描述	定義

AMSCoreRule	此規則會將 AWS Config 和 Amazon CloudWatch 事件轉送至 AMS Config 修復和 AMS 監控服務。AWS Config 事件會建立和 resolve AWS Systems Manager OpsItems。Amazon CloudWatch 事件會監控 CloudWatch 警示。	<pre>{
		    {
		        "source": ["aws.config", "aws.cloudwatch"],
		        "detail-type": ["Config Rules Compliance Change", "CloudWatch Alarm State Change"],
		    }
		}</pre>

建立 AMS 的受管規則

您不需要手動建立 Amazon EventBridge 受管規則。當您在 AWS 管理主控台 AWS CLI、 或 AWS API 中加入 AMS 時，AMS 會為您建立它們。

編輯 AMS 的受管規則

AMS 不允許您編輯受管規則。AMS 會預先定義每個受管規則的名稱和事件模式。

刪除 AMS 的受管規則

您不需要手動刪除 受管規則。當您從 AWS 管理主控台、 AWS CLI或 AWS API 的 AMS 離職時，AMS 會為您清除資源，並刪除 AMS 擁有的所有受管規則。

如果 AMS 在離職期間無法移除受管規則，您也可以使用 Amazon EventBridge 主控台、 AWS CLI 或 AWS API 手動刪除受管規則。若要這樣做，您必須先從 AMS 離職，並強制刪除受管規則。

AMS 中的信任修復程式

Trusted Remediator 是一種 AWS Managed Services 解決方案，可自動修復 AWS Trusted Advisor和 AWS Compute Optimizer建議。當 Trusted Advisor 和 Compute Optimizer 指出降低成本、改善系統可用性、最佳化效能或填補安全漏洞的機會時，信任的修復程式會建立建議 AWS 帳戶。透過 Trusted Remediator，您可以透過使用已建立最佳實務的安全標準化方式，處理這些安全性、效能、成本最佳化、容錯能力和服務限制建議。Trusted Remediator 可讓您設定修復解決方案，並依照您建立的排程自動執行，簡化修復程序。這種簡化方法可以一致、有效率地解決問題，無需手動介入。

信任的修復程式主要優點

以下是信任的修復程式的主要優點：

- 改善安全性、效能和成本最佳化：信任的補救措施可協助您增強帳戶的整體安全狀態、最佳化資源使用率，以及降低營運成本。
- 自助式設定和組態：您可以設定信任的修復程式，以符合您的需求和偏好設定。
- 自動化 Trusted Advisor 檢查和 AWS Compute Optimizer 建議修復：設定之後，信任的修復程式會自動執行所選檢查的修復動作。此自動化不需要手動介入。
- 最佳實務實作：修補動作是以已建立的最佳實務為基礎，因此問題會以標準化且有效的方式解決。
- 排程執行：您可以選擇與day-to-day操作工作流程一致的修復排程。

Trusted Remediator 可讓您主動解決 AWS 環境中已識別的問題，協助您遵守最佳實務，並維護安全、高效能且符合成本效益的雲端基礎設施。

可信任修復程式的運作方式

以下是信任修復程式工作流程的圖例：

Trusted Remediator 會評估 的 Trusted Advisor 和 Compute Optimizer 建議， AWS 帳戶 並在 OpsCenter 中建立 AWS Systems Manager OpsItems。 OpsItems OpsCenter 然後，您可以使用信任的修復程式自動化文件自動或手動修復 OpsItems。以下是每種修復類型的詳細資訊：

- 自動化修復：信任的修復程式會執行自動化文件並監控執行。自動化文件完成後，信任的修復程式會解析 Opsitem。
- 手動修復：信任的修復程式會建立 OpsItem 供您檢閱。檢閱後，您會啟動自動化文件。

修復日誌存放在 Amazon S3 儲存貯體中。您可以使用 S3 儲存貯體中的資料來建置自訂 QuickSight 儀表板以進行報告。AMS 也為信任的修復程式提供隨需報告。若要接收這些報告，請聯絡您的 CSDM。如需詳細資訊，請參閱信任的修復程式報告。

Trusted Remediator 的關鍵術語

以下是在 AMS 中使用受信任修復程式時，有助於了解的術語：

- AWS Trusted Advisor 和 AWS Compute Optimizer： AWS和 Trusted Advisor Compute Optimizer 提供的雲端最佳化服務會 AWS 檢查您的環境，並根據以下六個類別的最佳實務提供建議：
  - 成本最佳化
  - 效能
  - 安全性
  - 容錯能力
  - 卓越營運
  - 服務限制

  如需詳細資訊，請參閱AWS Trusted Advisor及AWS Compute Optimizer。
- 信任的修復程式：適用於Trusted Advisor檢查和AWS Compute Optimizer建議的 AMS 修復解決方案。Trusted Remediator 可協助您使用已知的最佳實務安全地修復 Trusted Advisor 檢查和 Compute Optimizer 建議，以改善安全性、效能並降低成本。可信任的修復程式易於設定。您設定一次，信任的修復程式會根據您偏好的排程 （每日或每週） 執行修復。
- AWS Systems Manager SSM 文件：JSON 或 YAML 檔案，定義對 AWS 資源 AWS Systems Manager 執行的動作。SSM 文件可做為宣告性規格，以自動化跨多個 AWS 資源和執行個體的操作任務。
- AWS Systems Manager OpsCenter OpsItem：一種雲端操作問題管理資源，可協助您追蹤和解決環境中 AWS 的操作問題。OpsItems 為跨 和資源的操作資料和問題提供集中式檢視 AWS 服務 和管理系統。每個 OpsItem 都代表一個操作問題，例如潛在的安全風險、效能問題或操作事件。
- 組態：組態是一組儲存在 中的屬性AWS AppConfig，即 的功能 AWS Systems Manager。中的信任修復程式應用程式 AWS AppConfig 有助於在帳戶層級設定修復。您可以使用 AWS AppConfig 主控台或 API 來編輯組態。
- 執行模式：執行模式是一種組態屬性，可決定如何針對每個 Trusted Advisor 檢查結果執行修復。支援四種執行模式：自動化、手動、條件式、非作用中。
- 資源覆寫：此功能使用資源標籤覆寫特定資源的組態。

- 修復項目日誌：信任的修復程式修復 S3 日誌儲存貯體中的日誌檔案。修復項目日誌會在修復 OpsItems 建立時建立。此日誌檔案包含手動執行修復 OpsItems 和自動執行修復 OpsItems。使用此日誌檔案來追蹤所有修復項目。
- 自動化修復執行日誌：信任的修復器修復 S3 日誌儲存貯體中的日誌檔案。自動執行 SSM 文件時，會建立自動修復執行日誌。此日誌包含自動執行修復 OpsItems 的 SSM 執行詳細資訊。使用此日誌檔案來追蹤自動化修復。

在 AMS 中開始使用信任的修復程式

可信任的修復程式可在 AMS 中使用，無需額外費用。Trusted Remediator 支援單一帳戶和多帳戶組態。

加入信任的修復程式

若要將您的 AMS 帳戶加入信任的修復程式，請傳送電子郵件給 Cloud Architects 或 Cloud Service Delivery Manager (CSDMs)。在電子郵件中，包含以下資訊：

- AWS 帳戶：12 位數的帳戶識別號碼。您想要加入信任的修復程式的所有帳戶必須屬於同一個 Accelerate 客戶。
  - 委派管理員帳戶：用於單一或多個帳戶的 Trusted Advisor 和 Compute Optimizer 檢查組態的帳戶。
  - 成員帳戶：這些是連結至委派管理員帳戶的帳戶。這些帳戶會從委派的管理員帳戶繼承組態。您可以有一個成員帳戶或多個成員帳戶。

  > **Note**
  >
  > 成員帳戶會從委派的管理員帳戶繼承組態。如果您需要特定帳戶的不同組態，請使用您偏好的組態加入多個委派管理員帳戶。在加入之前，請與您的 Cloud Architects 規劃帳戶結構和組態。

- AWS 區域： AWS 區域 資源所在的 。如需 的清單 AWS 區域，請參閱AWS 服務 依區域。
- 修補排程和時間：您偏好的修補排程 （每日或每週）。Trusted Remediator 會收集 Trusted Advisor 檢查並在排程時間啟動修復。例如，您可以設定每週週日凌晨 1：00 的修復排程，澳洲東部標準時間。
- 通知電子郵件：信任的修復程式會使用通知電子郵件，在有修復時每天通知您。通知電子郵件主旨是「可信修復摘要」，內容提供過去 24 小時內執行的可信任修復的資訊。

> **Note**
>
> 每次排定的修補後，請檢閱您的應用程式和資源。如需其他支援，請聯絡 AMS。

在您向 CA 或 CSDM 提交包含必要詳細資訊的加入請求之後，AMS 會將您的帳戶加入信任的修復程式。Trusted Remediator 使用 AWS AppConfig的功能 AWS Systems Manager來定義 Trusted Advisor 檢查的組態。這些組態是一組存放在其中的屬性 AWS AppConfig。為了防止您的 資源產生未經授權的費用，所有支援的 Trusted Advisor 檢查都會在帳戶加入信任的修復程式時設定為非作用中。加入後，您可以使用 AWS AppConfig 主控台或 API 來管理組態。這些組態可協助您自動修復特定 Trusted Advisor 檢查，或評估和手動修復剩餘的檢查。這些組態可高度自訂，可讓您為每個 Trusted Advisor 檢查套用組態。如需詳細資訊，請參閱在信任的修復程式中設定 Trusted Advisor 檢查修復。

選擇要修復的檢查和建議

根據預設，修復執行模式對於組態中的所有 Trusted Advisor 檢查和 Compute Optimizer 建議都是非作用中的。這可防止未經授權的修復並保護資源。AMS 提供精選的 SSM 自動化文件，用於 Trusted Advisor 檢查修復。

若要選取您想要使用信任的修復程式修復的檢查，請完成下列步驟：

1. 檢閱支援的 Trusted Advisor 和 Compute Optimizer 建議清單或相關聯的 SSM 自動化文件名稱，以決定您要使用信任的修復程式修復哪些檢查和建議。
2. 更新您的組態，以開啟所選 Trusted Advisor 檢查的修復。如需如何選取檢查的說明，請參閱 在信任的修復程式中設定 Trusted Advisor 檢查修復。

在信任的修復程式中追蹤您的修復

在您更新帳戶層級組態之後，信任的修復程式會為每個修復建立 OpsItems。Trusted Remediator 會執行 SSM 文件，以根據您的修復排程自動修復 OpsItems。如需如何從 Systems Manager OpsCenter 主控台檢視所有修復 OpsItems 的說明，請參閱 在信任的修復程式中追蹤修復。 OpsCenter

在信任的修復程式中執行手動修復

您可以手動修復 Trusted Advisor 檢查。當您啟動手動修復時，信任的修復程式會建立手動執行 OpsItem。您必須檢閱並啟動 SSM 自動化文件，才能修復 OpsItems。如需詳細資訊，請參閱在信任的修復程式中執行手動修復。

受信任修復程式支援的 Compute Optimizer 建議

下表列出支援的 Compute Optimizer 建議、SSM 自動化文件、預先設定的參數，以及自動化文件的預期結果。在啟用 SSM 自動化文件進行檢查修復之前，請檢閱預期成果，以協助您根據您的業務需求了解可能的風險。

對於您要啟用修復的支援檢查，請確定每個 Compute Optimizer 檢查的對應組態規則都存在。如需詳細資訊，請參閱選擇 AWS Compute Optimizer 接受 Trusted Advisor 檢查。

最佳化選項	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
精簡化		
Amazon EC2 執行個體建議	AWSManagedServices-TrustedRemediatorResizeInstanceByComputeOptimizerRecommendation 根據 Compute Optimizer 建議更新 Amazon EC2 執行個體類型。如果選項存在，則會選擇最佳選項，同時維護相同的平台參數（架構、Hypervisor、網路介面、虛擬化類型等）。	• MinimumDaysSinceLastChange：指定自上次執行個體類型變更以來最短天數的參數。預設值是 7 天。 無限制條件 • CreateAMIBeforeResize：若要在調整大小之前將執行個體 AMI 建立為備份，請將 設為 'True'。若要不建立備份，請將 設定為 'False'。預設為 'True'。 無限制條件
Amazon EBS 磁碟區建議	AWSManagedServices-ModifyEBSVolume Amazon EBS 磁碟區會根據 Compute Optimizer 建議進行修改。修改可能包括磁碟區類型、大小、IOPS、磁碟區產生 (gp2、gp3 等）。	• CreateSnapshot：若要在修改磁碟區之前建立快照，請將 設定為 'True'。若要不建立快照，請將 設定為 'False'。預設值為 'True'。 無限制條件 • VolumeType：所需的磁碟區類型。如果未指定類型，則會保留現有類型。 無限制條件 • VolumeSize：所需的磁碟區大小，以 GiB 為單位。目標磁碟區大小必

最佳化選項	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
		須大於或等於磁碟區的現有大小。如果未指定大小，則會保留現有的大小。 無限制條件 • Iops：每秒請求的 I/O 操作數 (IOPS)。此參數僅適用於 io1、io2 和 gp3 磁碟區。 無限制條件 • 輸送量：為磁碟區佈建的輸送量，上限為 1000 MiB/s。此參數僅適用於 gp3 磁碟區。 無限制條件 • RemediateStackDrift：若要啟動偏離修復，如果任何偏離是由磁碟區修改造成，請將 設為 'True'。若要不嘗試漂移修復，請將 設定為 'False'。預設為 'True'。 無限制條件
Lambda 函數建議	AWSManagedServices-TrustedRemediatorOptimizeLambdaMemory AWS Lambda 根據 Compute Optimizer 建議最佳化 函數記憶體。	RecommendedMemorySize ：如果與建議選項不同，則為自訂記憶體大小。 無限制條件
閒置資源		

最佳化選項	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
閒置 Amazon EBS 磁碟區	AWSManagedServices-DeleteUnusedEBSVolume 未連接的 Amazon EBS 磁碟區將被刪除。	• CreateSnapshot：若要在刪除磁碟區之前建立快照，請將 設定為 'True'。若要不建立快照，請將 設定為 'False'。預設值為 'True'。 無限制條件 • MinimumUnattachedDays：要刪除的 Amazon EBS 磁碟區未連接天數下限，最長可達 62 天。預設為 7。 無限制條件
閒置 Amazon EC2 執行個體	AWSManagedServices-StopEC2Instance 閒置的 Amazon EC2 執行個體將會停止。	ForceStopWithInstanceStore：若要使用執行個體存放區強制停止執行個體，請將 設為 'True'。若要不強制停止，請將 設定為 'False'。預設值 'False' 可防止執行個體停止。 無限制條件
閒置 Amazon RDS 執行個體	AWSManagedServices-StopIdleRDSInstance 停止閒置的 Amazon RDS 執行個體。支援的引擎包括：MariaDB、Microsoft SQL Server、MySQL、Oracle、PostgreSQL。本文件不適用於 Aurora MySQL 和 Aurora PostgreSQL。執行個體最多會停止 7 天，並自動重新啟動。	不允許預先設定的參數。 無限制條件

Trusted Advisor Trusted Remediator 支援的檢查

下表列出支援的 Trusted Advisor 檢查、SSM 自動化文件、預先設定的參數，以及自動化文件的預期結果。在啟用 SSM 自動化文件進行檢查修復之前，請檢閱預期成果，以協助您根據您的業務需求了解可能的風險。

請確定您要啟用修復之支援檢查的每個 Trusted Advisor 檢查都有對應的組態規則。如需詳細資訊，請參閱檢視支援的 AWS Trusted Advisor 檢查 AWS Config。如果檢查有對應的 AWS Security Hub 控制項，請確定 Security Hub 控制項已啟用。如需詳細資訊，請參閱在 Security Hub 中啟用控制項。如需管理預先設定參數的資訊，請參閱在信任的修復程式中設定 Trusted Advisor 檢查修復。

Trusted Advisor Trusted Remediator 支援的成本最佳化檢查

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Z4AUBRNSmz 無關聯彈性 IP 地址	AWSManagedServices-TrustedRemediatorReleaseElasticIP 釋出與任何資源無關的彈性 IP 地址。	不允許預先設定的參數。 無限制條件
c18d2gz150 - Amazon EC2 執行個體已停止	AWSManagedServices-TerminateEC2InstanceStoppedForPeriodOfTime - Amazon EC2 執行個體已停止幾天。	• CreateAMIBeforeTermination：若要在終止 Amazon EC2 執行個體之前建立執行個體 AMI 做為備份，請選擇 `true`。若要在終止之前不建立備份，請選擇 `false`。預設值為 `true`。 • AllowedDays：執行個體在終止前處於停止狀態的天數。預設值為 30。 無限制條件
c18d2gz128 未設定生命週期政策的 Amazon ECR 儲存庫	AWSManagedServices-TrustedRemediatorPutECRLifecyclePolicy 如果生命週期政策尚未存在，請為指定的儲存庫建立生命週期政策。	ImageAgeLimit：Amazon ECR 儲存庫中「任何」映像的最大存留期限制，以天 (1-365) 為單位。 無限制條件
DAvU99Dc4C 利用率過低的 Amazon EBS 磁碟區	AWSManagedServices-DeleteUnusedEBSVolume 如果過去 7 天內未連接磁碟區，則刪除未充分利用的 Amazon EBS 磁碟區。預設會建立 Amazon EBS 快照。	• CreateSnapshot：如果設定為 `true`，則自動化會在刪除之前建立 Amazon EBS 磁碟區的快照。預設設定為 `true`。有效值為 `true`和 `false`（區分大小寫）。

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
		• MinimumUnattachedDays：EBS 磁碟區的刪除未連接天數下限，最長可達 62 天。如果設定為 0，則 SSM 文件不會檢查未連接的期間，如果磁碟區目前未連接，則刪除磁碟區。預設值為 7。 無限制條件
hjLMh88uM8 閒置負載平衡器	AWSManagedServices-DeleteIdleClassicLoadBalancer 如果閒置的 Classic Load Balancer 未使用且未註冊任何執行個體，則會將其刪除。	IdleLoadBalancerDays：Classic Load Balancer 在考慮閒置之前有 0 個請求連線的天數。預設值為七天。 如果啟用自動執行，如果沒有作用中的後端執行個體，自動化會刪除閒置的 Classic Load Balancer。對於具有作用中後端執行個體但沒有運作狀態良好的後端執行個體的所有閒置 Classic Load Balancer，不會使用自動修復，並會建立用於手動修復 OpsItems。
Ti39halfu8 Amazon RDS 閒置資料庫執行個體	AWSManagedServices-StopIdleRDSInstance 過去七天處於閒置狀態的 Amazon RDS 資料庫執行個體會停止。	不允許預先設定的參數。 無限制條件
COr6dfpM05 AWS Lambda 記憶體大小過度佈建的函數	AWSManagedServices-ResizeLambdaMemory AWS Lambda 函數的記憶體大小會調整為 提供的建議記憶體大小 Trusted Advisor。	RecommendedMemorySize：Lambda 函數的建議記憶體配置。值範圍介於 128 到 10240 之間。 如果在自動化執行之前修改 Lambda 函數大小，則此自動化可能會以 建議的值覆寫設定 Trusted Advisor。

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Qch7DwouX1 Amazon EC2 執行個體低使用率	AWSManagedServices-StopEC2Instance（自動和手動執行模式的預設 SSM 文件）。 低使用率的 Amazon EC2 執行個體會停止。	ForceStopWithInstanceStore：設定為 `true` 以使用執行個體存放區強制停止執行個體。否則，請設定為 `false`。的預設值`false`可防止執行個體停止。有效值為 true 或 false（區分大小寫）。 無限制條件
Qch7DwouX1 Amazon EC2 執行個體低使用率	AWSManagedServices-ResizeInstanceByOneLevel Amazon EC2 執行個體的大小會由相同執行個體系列類型的一個執行個體類型縮減。執行個體會在調整大小操作期間停止和啟動，並在 SSM 文件執行完成後回到初始狀態。此自動化不支援調整 Auto Scaling 群組中的執行個體大小。	• MinimumDaysSinceLastChange：自上次執行個體類型變更以來的天數下限。如果在指定的時間內修改執行個體類型，則不會變更執行個體類型。使用 `0` 略過此驗證。預設值為 7。 • CreateAMIBeforeResize：若要在調整大小之前建立執行個體 AMI 做為備份，請選擇 `true`。若要不建立備份，請選擇 `false`。預設值為 `false`。有效值為 `true`和 `false`（區分大小寫）。 • ResizeIfStopped：若要繼續變更執行個體大小，即使執行個體處於停止狀態，請選擇 `true`。如果執行個體處於停止狀態，若要不自動調整其大小，請選擇 `false`。有效值為 `true`和 `false`（區分大小寫）。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Qch7DwouX1 Amazon EC2 執行個體低使用率	AWSManagedServices-TerminateInstance 如果不屬於 Auto Scaling 群組，且未啟用終止保護，則會終止低使用率的 Amazon EC2 執行個體。預設會建立 AMI。	CreateAMIBeforeTermination：將此選項設定為 `true`或 `false`，以在終止 EC2 執行個體之前建立執行個體 AMI 做為備份。預設值為 `true`。有效值為 `true`和 `false`（區分大小寫）。 無限制條件
G31sQ1E9U 利用率過低的 Amazon Redshift 叢集	AWSManagedServices-PauseRedshiftCluster Amazon Redshift 叢集已暫停。	不允許預先設定的參數。 無限制條件
c1cj39rr6v Amazon S3 不完整的分段上傳中止組態	AWSManagedServices-TrustedRemediatorEnableS3AbortIncompleteMultipartUpload Amazon S3 儲存貯體已設定生命週期規則，以中止在特定天後仍未完成的分段上傳。	DaysAfterInitiation：Amazon S3 停止未完成分段上傳的天數。預設值設定為 7 天。 無限制條件
c1z7kmr00n 執行個體的 Amazon EC2 成本最佳化建議	使用 Amazon EC2 執行個體建議和來自 的閒置 Amazon EC2 執行個體受信任修復程式支援的 Compute Optimizer 建議。	不允許預先設定的參數。 無限制條件
c1z7kmr02n 磁碟區的 Amazon EBS 成本最佳化建議	使用 Amazon EBS 磁碟區建議和來自的閒置 Amazon EBS 磁碟區受信任修復程式支援的 Compute Optimizer 建議。	不允許預先設定的參數。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
c1z7kmr03n 資料庫執行個體的 Amazon RDS 成本最佳化建議	從 使用閒置 Amazon RDS 執行個體受信任修復程式支援的 Compute Optimizer 建議。	不允許預先設定的參數。 無限制條件
c1z7kmr05n AWS Lambda 函數的成本最佳化建議	使用來自 的 Lambda 函數建議受信任修復程式支援的 Compute Optimizer 建議。	不允許預先設定的參數。 無限制條件

Trusted Advisor Trusted Remediator 支援的安全檢查

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
12Fnkpl8Y5 存取金鑰已暴露	AWSManagedServices-TrustedRemediatorDeactivateIAMAccessKey 公開的 IAM 存取金鑰已停用。	不允許預先設定的參數。 使用公開的 IAM 存取金鑰設定的應用程式無法驗證。
Hs4Ma3G127 - 應啟用 API Gateway REST 和 WebSocket API 執行記錄 對應的 AWS Security Hub 檢查：APIGateway.1	AWSManagedServices-TrustedRemediatorEnableAPIGateWayExecutionLogging 執行記錄會在 API 階段上啟用。	LogLevel：記錄層級以啟用執行記錄， ERROR - 僅針對錯誤啟用記錄。 INFO- 為所有事件啟用記錄。 您必須授予 API Gateway 許可，以讀取和寫入您帳戶的日誌至 CloudWatch，以啟用執行日誌，請參閱在 API Gateway 中設定 REST APIs 的 CloudWatch 日誌記錄以取得詳細資訊。
Hs4Ma3G129 - API Gateway REST API 階段	AWSManagedServices-EnableApiGateWayXRayTracing 在 API 階段上啟用 X-Ray 追蹤。	不允許預先設定的參數。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
應該已啟用 AWS X-Ray 追蹤 對應的 AWS Security Hub 檢查：APIGateway.3		
Hs4Ma3G202 - API Gateway REST API 快取資料應靜態加密 對應的 AWS Security Hub 檢查：APIGateway.5	AWSManagedServices-EnableAPIGatewayCacheEncryption 如果 API Gateway REST API 階段已啟用快取，請啟用 API Gateway REST API 快取資料的靜態加密。	不允許預先設定的參數。 無限制條件
Hs4Ma3G177 - 對應的 AWS Security Hub 檢查 - 與負載平衡器相關聯的自動擴展群組應使用負載平衡器運作狀態檢查 AutoScaling.1	AWSManagedServices-TrustedRemediatorEnableAutoScalingGroupELBHealthCheck Auto Scaling 群組已啟用 Elastic Load Balancing 運作狀態檢查。	HealthCheckGracePeriod：Auto Scaling 在檢查已開始服務的 Amazon Elastic Compute Cloud 執行個體的運作狀態之前等待的時間，以秒為單位。 如果連接到 Auto Elastic Load Balancing 群組的任何 Elastic Load Balancing 負載平衡器回報運作狀態不佳，開啟 Elastic Load Balancing 運作狀態檢查可能會導致取代執行中的執行個體。 Auto Scaling 如需詳細資訊，請參閱將 Elastic Load Balancing 負載平衡器連接至 Auto Scaling 群組

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G245 - AWS CloudFormation 堆疊應與 Amazon Simple Notification Service 整合 對應的 AWS Security Hub 檢查：CloudFormation.1	AWSManagedServices-EnableCFNStackNotification 將 CloudFormation 堆疊與 Amazon SNS 主題建立關聯以進行通知。	NotificationARNs：要與所選 CloudFormation 堆疊建立關聯的 Amazon SNS 主題 ARNs。 若要啟用自動修復，必須提供NotificationARNs 預先設定的參數。
Hs4Ma3G210 - CloudFront 分佈應該已啟用記錄 對應的 AWS Security Hub 檢查：CloudFront.2	AWSManagedServices-EnableCloudFrontDistributionLogging Amazon CloudFront 分佈已啟用記錄功能。	• BucketName：您要存放存取日誌的 Amazon S3 儲存貯體名稱。 • S3KeyPrefix：theAmazon CloudFront 分發日誌 S3 儲存貯體中位置的字首。 • IncludeCookies：指出是否要在存取日誌中包含 Cookie。 若要啟用自動修復，必須提供下列預先設定的參數： • BucketName • S3KeyPrefix • IncludeCookies 如需此修復限制，請參閱如何開啟 CloudFront 分佈的記錄功能？

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G109 - 應啟用 CloudTrail 日誌檔案驗證 對應的 AWS Security Hub 檢查：CloudTrail.4	AWSManagedServices-TrustedRemediatorEnableCloudTrailLogValidation 啟用 CloudTrail 追蹤日誌驗證。	不允許預先設定的參數。 無限制條件
Hs4Ma3G108 - CloudTrail 追蹤應與 Amazon CloudWatch Logs 整合 對應的 AWS Security Hub 檢查：CloudTrail.5	AWSManagedServices-IntegrateCloudTrailWithCloudWatch AWS CloudTrail 已與 CloudWatch Logs 整合。	• CloudWatchLogsLogGroupName：交付 CloudTrail 日誌的 CloudWatch Logs 日誌群組名稱。 CloudTrail 您必須使用帳戶中存在的日誌群組。 • CloudWatchLogsRoleName：CloudWatch Logs 端點的 IAM 角色名稱，以假設 寫入使用者的日誌群組。您必須使用帳戶中存在的角色。 若要啟用自動修復，必須提供下列預先設定的參數： • CloudWatchLogsLogGroupName • CloudWatchLogsRoleName
Hs4Ma3G217 - CodeBuild 專案環境應具有記錄 AWS 組態 對應的 AWS Security Hub 檢查：CodeBuild.4	AWSManagedServices-TrustedRemediatorEnableCodeBuildLoggingConfig 啟用 CodeBuild 專案的記錄。	不允許預先設定的參數。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G306 - Neptune 資料庫叢集應該啟用刪除保護 對應的 AWS Security Hub 檢查：DocumentDB.3	AWSManagedServices-TrustedRemediatorDisablePublicAccessOnDocumentDBSnapshot 從 Amazon DocumentDB 手動叢集快照移除公有存取權。	不允許預先設定的參數。 無限制條件
Hs4Ma3G308 - Amazon DocumentDB 叢集應該啟用刪除保護 對應的 AWS Security Hub 檢查：DocumentDB.5	AWSManagedServices-TrustedRemediatorEnableDocumentDBClusterDeletionProtection 啟用 Amazon DocumentDB 叢集的刪除保護。	不允許預先設定的參數。 無限制條件
Hs4Ma3G323 - DynamoDB 資料表應該啟用刪除保護 對應的 AWS Security Hub 檢查：DynamoDB.6	AWSManagedServices-TrustedRemediatorEnableDynamoDBTableDeletionProtection 啟用非 AMS DynamoDB 資料表的刪除保護。	不允許預先設定的參數。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
ePs02jT06w - Amazon EBS 公有快照	AWSManagedServices-TrustedRemediatorDisablePublicAccessOnEBSSnapshot Amazon EBS 快照的公開存取已停用。	不允許預先設定的參數。 無限制條件
Hs4Ma3G118 - VPC 預設安全群組不應允許傳入或傳出流量 對應的 AWS Security Hub 檢查：EC2.2	AWSManagedServices-TrustedRemediatorRemoveAllRulesFromDefaultSG 預設安全群組中的所有輸入和輸出規則都會移除。	不允許預先設定的參數。 無限制條件
Hs4Ma3G117 - 連接的 EBS 磁碟區應該靜態加密 對應的 AWS Security Hub 檢查：EC2.3	AWSManagedServices-EncryptInstanceVolume 執行個體上連接的 Amazon EBS 磁碟區已加密。	• KMSKeyId： AWS KMS key ID 或 ARN 來加密磁碟區。 • DeleteStaleNonEncryptedSnapshotBackups：決定是否應刪除舊未加密磁碟區的快照備份的旗標。 作為修復的一部分，執行個體會重新啟動，如果 `DeleteStaleNonEncryptedSnapshotBackups` 設定為 `false` ，則復原可以協助還原。
Hs4Ma3G120 - 在指定時段後應移除已停止的 EC2 執行個體 對應的 AWS Security Hub 檢查：EC2.4	AWSManagedServices-TerminateInstance（自動和手動執行模式的預設 SSM 文件） Amazon EC2 執行個體已停止 30 天。	CreateAMIBeforeTermination：。若要在終止 EC2 執行個體之前建立執行個體 AMI 做為備份，請選擇 `true`。若要在終止之前不建立備份，請選擇 `false`。預設值為 `true`。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G120 - 在指定時段後應移除已停止的 EC2 執行個體 對應的 AWS Security Hub 檢查：EC2.4	AWSManagedServices-TerminateEC2InstanceStoppedForPeriodOfTime - 在 Security Hub 中定義的天數內停止的 Amazon EC2 執行個體（預設值為 30) 會終止。	CreateAMIBeforeTermination：若要在終止 EC2 執行個體之前建立執行個體 AMI 做為備份，請選擇 `true`。若要在終止之前不建立備份，請選擇 `false`。預設值為 `true`。 無限制條件
Hs4Ma3G121 - 應啟用 EBS 預設加密 對應的 AWS Security Hub 檢查：EC2.7	AWSManagedServices-EncryptEBSByDefault Amazon EBS 加密預設為針對特定 啟用 AWS 區域	不允許預先設定的參數。 預設加密是區域特有設定。如果您為區域啟用此功能，則無法針對該區域中的個別磁碟區或快照停用此功能。
Hs4Ma3G124 - Amazon EC2 執行個體應使用執行個體中繼資料服務第 2 版 (IMDSv2) 對應的 AWS Security Hub 檢查：EC2.8	AWSManagedServices-TrustedRemediatorEnableEC2InstanceIMDSv2 Amazon EC2 執行個體使用執行個體中繼資料服務第 2 版 (IMDSv2)。	• IMDSv1MetricCheckPeriod：在 CloudWatch 中分析 IMDSv1 用量指標的天數 (`42-455`)。如果 Amazon EC2 執行個體是在指定的期間內建立，則分析會從執行個體的建立日期開始。 • HttpPutResponseHopLimit：執行個體中繼資料字符允許的網路跳轉數目上限。此值可在 1和 2 躍點之間設定。的跳轉限制會將字符存取 1限制為直接在執行個體上執行的程序，而 的跳轉限制則2允許從執行個體上執行的容器存取。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G207 - EC2 子網路不應自動指派公有 IP 地址 對應的 AWS Security Hub 檢查：EC2.15	AWSManagedServices-UpdateAutoAssignPublicIpv4Addresses VPC 子網路設定為不會自動指派公有 IP 地址。	不允許預先設定的參數。 無限制條件
Hs4Ma3G209 - 移除未使用的網路存取控制清單 對應的 AWS Security Hub 檢查：EC2.16	AWSManagedServices-DeleteUnusedNACL 刪除未使用的網路 ACL	不允許預先設定的參數。 無限制條件
Hs4Ma3G215 - 應移除未使用的 Amazon EC2 安全群組 對應的 AWS Security Hub 檢查：EC2.22	AWSManagedServices-DeleteSecurityGroups 刪除未使用的安全群組。	不允許預先設定的參數。 無限制條件
Hs4Ma3G247 - Amazon EC2 Transit Gateway 不應自動接受 VPC 連接請求 對應的 AWS Security Hub 檢查：EC2.23	AWSManagedServices-TrustedRemediatorDisableTGWAutoVPCAttach - 停用自動接受指定非 AMS Amazon EC2 Transit Gateway 的 VPC 連接請求。	不允許預先設定的參數。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G235 - ECR 私有儲存庫應設定標籤不可變性 對應的 AWS Security Hub 檢查：ECR.2	AWSManagedServices-TrustedRemediatorSetImageTagImmutability 將指定儲存庫的影像標籤可變性設定設定為 IMMUTABLE。	不允許預先設定的參數。 無限制條件
Hs4Ma3G216 - ECR 儲存庫應至少設定一個生命週期政策 對應的 AWS Security Hub 檢查：ECR.3	AWSManagedServices-PutECRRepositoryLifecyclePolicy ECR 儲存庫已設定生命週期政策。	LifecyclePolicyText：要套用至儲存庫的 JSON 儲存庫政策文字。 若要啟用自動修復，必須提供下列預先設定的參數： LifecyclePolicyText
Hs4Ma3G325 - EKS 叢集應該啟用稽核記錄 對應的 AWS Security Hub 檢查：EKS.8	AWSManagedServices-TrustedRemediatorEnableEKSAuditLog EKS 叢集已啟用稽核日誌。	不允許預先設定的參數。 無限制條件
Hs4Ma3G183 - 應用程式負載平衡器應設定為捨棄 HTTP 標頭 對應的 AWS Security Hub 檢查：ELB.4	AWSConfigRemediation-DropInvalidHeadersForALB Application Load Balancer 設定為無效的標頭欄位。	不允許預先設定的參數。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G184 - 應啟用 Application Load Balancer 和 Classic Load Balancer 記錄 對應的 AWS Security Hub 檢查：ELB.5	AWSManagedServices-EnableELBLogging（自動和手動執行模式的預設 SSM 文件） Application Load Balancer 和 Classic Load Balancer 記錄已啟用。	• BucketName：儲存貯體名稱（非 ARN)。請確定儲存貯體政策已正確設定以供記錄。 • S3KeyPrefix：Elastic Load Balancing 日誌的 Amazon S3 儲存貯體中位置的字首。 若要啟用自動修復，必須提供下列預先設定的參數： • BucketName • S3KeyPrefix Amazon S3 儲存貯體必須有儲存貯體政策，授予 Elastic Load Balancing 將存取日誌寫入儲存貯體的許可。

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G184 - 應啟用 Application Load Balancer 和 Classic Load Balancer 記錄 對應的 AWS Security Hub 檢查：ELB.5	AWSManagedServices-EnableELBLoggingV2 Application Load Balancer 和 Classic Load Balancer 記錄已啟用。	• TargetBucketTagKey：用於識別目標 Amazon S3 儲存貯體的標籤名稱（區分大小寫）。將此與 搭配使用TargetBucketTagValue ，以標記將做為存取記錄目的地儲存貯體的儲存貯體。 • TargetBucketTagValue：用於識別目標 Amazon S3 儲存貯體的標籤值（區分大小寫）。將此與 搭配使用TargetBucketTagKey ，以標記將做為存取記錄目的地儲存貯體的儲存貯體。 • S3BucketPrefix：Amazon S3 儲存貯體的字首（邏輯階層）。您指定的字首不得包含字串 AWSLogs。如需詳細資訊，請參閱使用字首組織物件。 若要啟用自動修復，必須提供下列預先設定的參數： • TargetBucketTagKey • TargetBucketTagValue • S3BucketPrefix Amazon S3 儲存貯體必須有儲存貯體政策，授予 Elastic Load Balancing 將存取日誌寫入儲存貯體的許可。

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G326 - 應啟用 Amazon EMR 封鎖公開存取設定 對應的 AWS Security Hub 檢查：EMR.2	AWSManagedServices-TrustedRemediatorEnableEMRBlockPublicAccess 帳戶已開啟 Amazon EMR 封鎖公開存取設定。	不允許預先設定的參數。 無限制條件
Hs4Ma3G135 - AWS KMS 金鑰不應意外刪除 對應的 AWS Security Hub 檢查：KMS.3	AWSManagedServices-CancelKeyDeletion AWS KMS 金鑰刪除已取消。	不允許預先設定的參數。 無限制條件
Hs4Ma3G299 - Amazon DocumentDB 手動叢集快照不應公開 對應的 AWS Security Hub 檢查：Neptune.4	AWSManagedServices-TrustedRemediatorEnableNeptuneDBClusterDeletionProtection 啟用 Amazon Neptune 叢集的刪除保護。	不允許預先設定的參數。 無限制條件
Hs4Ma3G319 - Network Firewall 防火牆應該啟用刪除保護 對應 AWS Security Hub 檢查：NetworkFirewall.9	AWSManagedServices-TrustedRemediatorEnableNetworkFirewallDeletionProtection - 啟用 AWS Network Firewall 的刪除保護。	不允許預先設定的參數。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G223 - OpenSearch 網域應該加密節點之間傳送的資料 對應的 AWS Security Hub 檢查：OpenSearch.3	AWSManagedServices-EnableOpenSearchNodeToNodeEncryption 網域已啟用節點對節點加密。	不允許預先設定的參數。 啟用node-to-node加密後，您無法停用設定。反之，請手動擷取加密網域的快照、建立另一個網域、遷移您的資料，然後刪除舊網域。
Hs4Ma3G222 - 應啟用記錄至 CloudWatch Logs 的 OpenSearch 網域錯誤 對應的 AWS Security Hub 檢查：Opensearch.4	AWSManagedServices-EnableOpenSearchLogging OpenSearch 網域已啟用錯誤記錄。	CloudWatchLogGroupArn：anAmazon CloudWatch Logs 日誌群組的 ARN。 若要啟用自動修復，必須提供下列預先設定的參數：CloudWatchLogGroupArn。 Amazon CloudWatch 資源政策必須設定 許可。如需詳細資訊，請參閱《Amazon OpenSearch Service 使用者指南》中的啟用稽核日誌
Hs4Ma3G221 - OpenSearch 網域應該啟用稽核記錄 對應的 AWS Security Hub 檢查：Opensearch.5	AWSManagedServices-EnableOpenSearchLogging OpenSearch 網域設定為啟用稽核記錄。	CloudWatchLogGroupArn：要發佈日誌的 CloudWatch Logs 群組 ARN。 若要啟用自動修復，必須提供下列預先設定的參數：CloudWatchLogGroupArn Amazon CloudWatch 資源政策必須設定 許可。如需詳細資訊，請參閱《Amazon OpenSearch Service 使用者指南》中的啟用稽核日誌

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G220 - 應使用 TLS 1.2 加密與 OpenSearch 網域的連線 對應的 AWS Security Hub 檢查：Opensearch.8	AWSManagedServices-EnableOpenSearchEndpointEncryptionTLS1.2 TLS 政策設定為 `Policy-Min-TLS-1-2-2019-07`，且僅允許透過 HTTPS (TLS) 的加密連線。	不允許預先設定的參數。 使用 TLS 1.2 需要連線至 OpenSearch 網域。加密傳輸中的資料可能會影響效能。使用此功能測試您的應用程式，以了解效能描述檔和 TLS 的影響。
Hs4Ma3G194 - Amazon RDS 快照應為私有 對應的 AWS Security Hub 檢查：RDS.1	AWSManagedServices-DisablePublicAccessOnRDSSnapshotV2 Amazon RDS 快照的公開存取已停用。	不允許預先設定的參數。 無限制條件
Hs4Ma3G192 - RDS 資料庫執行個體應禁止公開存取，如 PubliclyAccessible AWS 組態所決定 對應的 AWS Security Hub 檢查：RDS.2	AWSManagedServices-TrustedRemediatorDisablePublicAccessOnRDSInstance 在 RDS 資料庫執行個體上停用公有存取。	不允許預先設定的參數。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G189 - 針對 Amazon RDS 資料庫執行個體設定增強型監控 對應的 AWS Security Hub 檢查：RDS.6	AWSManagedServices-TrustedRemediatorEnableRDSEnhancedMonitoring 啟用 Amazon RDS 資料庫執行個體的增強型監控	• MonitoringInterval：針對資料庫執行個體收集增強型監控指標的點之間的間隔，以秒為單位。有效間隔為 0、1、5、10、15、30 和 60。若要停用收集增強型監控指標，請指定 0。 • MonitoringRoleName：允許 Amazon RDS 將增強型監控指標傳送至 Amazon CloudWatch Logs 的 IAM 角色名稱。如果未指定角色，則會`rds-monitoring-role` 使用或建立預設角色，如果該角色不存在。 如果在自動化執行之前啟用增強型監控，則此自動化可能會使用預先設定參數中設定的 MonitoringInterval 和 MonitoringRoleName 值來覆寫設定。
Hs4Ma3G190 - Amazon RDS 叢集應該啟用刪除保護 對應的 AWS Security Hub 檢查：RDS.7	AWSManagedServices-TrustedRemediatorEnableRDSDeletionProtection Amazon RDS 叢集已啟用刪除保護。	不允許預先設定的參數。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G198 - Amazon RDS 資料庫執行個體應啟用刪除保護 對應的 AWS Security Hub 檢查：RDS.8	AWSManagedServices-TrustedRemediatorEnableRDSDeletionProtection Amazon RDS 執行個體已啟用刪除保護。	不允許預先設定的參數。 無限制條件
Hs4Ma3G199 - RDS 資料庫執行個體應將日誌發佈至 CloudWatch Logs 對應的 AWS Security Hub 檢查：RDS.9	AWSManagedServices-TrustedRemediatorEnableRDSLogExports 已針對 RDS 資料庫執行個體或 RDS 資料庫叢集啟用 RDS 日誌匯出。	不允許預先設定的參數。 服務連結角色 AWSServiceRoleForRDS 為必要項目。
Hs4Ma3G160 - 應為 RDS 執行個體設定 IAM 身分驗證 對應的 AWS Security Hub 檢查：RDS.10	AWSManagedServices-UpdateRDSIAMDatabaseAuthentication AWS Identity and Access Management 已為 RDS 執行個體啟用身分驗證。	ApplyImmediately：指出是否盡快非同步套用此請求中的修改和任何待定修改，若要立即套用變更，請選擇 `true`。若要排程下一個維護時段的變更，請選擇 `false`。 無限制條件
Hs4Ma3G161 - 應為 RDS 叢集設定 IAM 身分驗證 對應的 AWS Security Hub 檢查：RDS.12	AWSManagedServices-UpdateRDSIAMDatabaseAuthentication RDS 叢集已啟用 IAM 身分驗證。	ApplyImmediately：指出此請求中的修改和任何待定修改是否以非同步方式盡快套用，若要立即套用變更，請選擇 `true`。若要排程下一個維護時段的變更，請選擇 `false`。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G162 - 應啟用 RDS 自動次要版本升級 對應的 AWS Security Hub 檢查：RDS.13	AWSManagedServices-UpdateRDSInstanceMinorVersionUpgrade Amazon RDS 的自動次要版本升級組態已啟用。	不允許預先設定的參數。 Amazon RDS 執行個體必須處於 `available` 狀態，才能進行此修復。
Hs4Ma3G163 - RDS 資料庫叢集應設定為將標籤複製到快照 對應的 AWS Security Hub 檢查：RDS.16	AWSManagedServices-UpdateRDSCopyTagsToSnapshots `CopyTagtosnapshot` Amazon RDS 叢集的設定已啟用。	不允許預先設定的參數。 Amazon RDS 執行個體必須處於可用狀態，才能進行此修復。
Hs4Ma3G164 - RDS 資料庫執行個體應設定為將標籤複製到快照 對應的 AWS Security Hub 檢查：RDS.17	AWSManagedServices-UpdateRDSCopyTagsToSnapshots `CopyTagsToSnapshot` Amazon RDS 的設定已啟用。	不允許預先設定的參數。 Amazon RDS 執行個體必須處於可用狀態，才能進行此修復。
rSs93HQwa1 Amazon RDS 公有快照	AWSManagedServices-DisablePublicAccessOnRDSSnapshotV2 Amazon RDS 快照的公開存取已停用。	不允許預先設定的參數。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G103 - Amazon Redshift 叢集應禁止公開存取 對應的 AWS Security Hub 檢查：Redshift.1	AWSManagedServices-DisablePublicAccessOnRedshiftCluster Amazon Redshift 叢集上的公開存取已停用。	不允許預先設定的參數。 停用公有存取會封鎖來自網際網路的所有用戶端。而且 Amazon Redshift 叢集處於修改狀態幾分鐘，而修復會停用叢集上的公有存取。
Hs4Ma3G106 - Amazon Redshift 叢集應該啟用稽核記錄 對應的 AWS Security Hub 檢查：Redshift.4	AWSManagedServices-TrustedRemediatorEnableRedshiftClusterAuditLogging 稽核記錄會在維護時段期間啟用到您的 Amazon Redshift 叢集。	不允許預先設定的參數。 若要啟用自動修復，必須提供下列預先設定的參數。 BucketName：儲存貯體必須位於相同的 中 AWS 區域。叢集必須具有讀取儲存貯體並放置物件許可。 如果在自動化執行之前啟用 Redshift 叢集記錄，則記錄設定可能會由此自動化覆寫，並在預先設定的參數中設定 `BucketName` 和 `S3KeyPrefix` 值。
Hs4Ma3G105 - Amazon Redshift 應已啟用自動升級至主要版本 對應的 AWS Security Hub 檢查：Redshift.6	AWSManagedServices-EnableRedshiftClusterVersionAutoUpgrade - 主要版本升級會在維護時段期間自動套用至叢集。Amazon Redshift 叢集不會立即停機，但如果升級到主要版本，您的 Amazon Redshift 叢集可能會在維護時段期間停機。	不允許預先設定的參數。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G104 - Amazon Redshift 叢集應使用增強型 VPC 路由 對應的 AWS Security Hub 檢查：Redshift.7	AWSManagedServices-TrustedRemediatorEnableRedshiftClusterEnhancedVPCRouting Amazon Redshift 叢集已啟用增強型 VPC 路由。	不允許預先設定的參數。 無限制條件
Hs4Ma3G173 - 應在儲存貯體層級啟用 S3 封鎖公開存取設定 對應的 AWS Security Hub 檢查：S3.8	AWSManagedServices-TrustedRemediatorBlockS3BucketPublicAccess 儲存貯體層級的公有存取區塊會套用至 Amazon S3 儲存貯體。	不允許預先設定的參數。 此修復可能會影響 S3 物件可用性。如需 Amazon S3 如何評估存取權的資訊，請參閱封鎖對 Amazon S3 儲存體的公開存取權。

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G230 - 應啟用 S3 儲存貯體伺服器存取記錄 對應的 AWS Security Hub 檢查：S3.9	AWSManagedServices-EnableBucketAccessLogging （自動和手動執行模式的預設 SSM 文件） Amazon S3 伺服器存取記錄已啟用。	• TargetBucket：儲存伺服器存取日誌的 S3 儲存貯體名稱。 • TargetObjectKeyFormat：日誌物件的 Amazon S3 金鑰格式（值區分大小寫）。若要針對日誌物件使用 S3 金鑰的簡單格式，請選擇 `SimplePrefix` 。若要將分割的 S3 金鑰用於日誌物件，並將 EventTime 用於分割的字首，請選擇 `PartitionedPrefixEventTime` 。若要將分割的 S3 金鑰用於日誌物件，並將 DeliveryTime 用於分割的字首，請選擇 `PartitionedPrefixDeliveryTime` 。有效值為 `SimplePrefix` 、`PartitionedPrefixEventTime` 和 `PartitionedPrefixDeliveryTime` 。 若要啟用自動修復，必須提供下列預先設定的參數：TargetBucket。 目的地儲存貯體必須與來源儲存貯體位於相同 AWS 帳戶 AWS 區域 且具有正確的日誌交付許可。如需詳細資訊，請參閱啟用 Amazon S3 伺服器存取記錄。

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G230 – 應啟用 S3 儲存貯體伺服器存取記錄 對應的 AWS Security Hub 檢查：S3.9	AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV2 - 已啟用 Amazon S3 儲存貯體記錄。	• TargetBucketTagKey：用於識別目標儲存貯體的標籤名稱（區分大小寫）。使用此 和 TargetBucketTagValue 來標記要用作存取記錄目的地儲存貯體的儲存貯體。 • TargetBucketTagValue：用於識別目標儲存貯體的標籤值（區分大小寫），請使用此值和 TargetBucketTagKey 來標記要用作存取記錄目的地儲存貯體的儲存貯體。 • TargetObjectKeyFormat：日誌物件的 Amazon S3 金鑰格式（值區分大小寫）：若要將 S3 金鑰的簡單格式用於日誌物件，請選擇 SimplePrefix。若要將分割 S3 金鑰用於日誌物件，並將 EventTime 用於分割字首，請選擇PartitionedPrefixEventTime 若要將分割 S3 金鑰用於日誌物件，並將 DeliveryTime 用於分割字首，請選擇 PartitionedPrefixDeliveryTime。預設值為 PartitionedPrefixEventTime。 若要啟用自動修復，必須提供下列參數：TargetBucketTagKey 和 TargetBucketTagValue。 目的地儲存貯體必須與來源儲存貯體位於相同 AWS 帳戶 AWS 區域 且具有正確的日誌交付許可。如需詳細資訊，請參閱啟用 Amazon S3 伺服器存取記錄。

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Pfx0RwqBli Amazon S3 儲存貯體許可	AWSManagedServices-TrustedRemediatorBlockS3BucketPublicAccess 封鎖公有存取權	不允許預先設定的參數。 此檢查包含多個提醒條件。此自動化可修復公有存取問題。不支援修復 Trusted Advisor 標記的其他組態問題。此修復支援修復 AWS 服務 已建立的 S3 儲存貯體 （ 例如 cf-templates-000000000000)。
Hs4Ma3G272 - 使用者不應擁有 SageMaker 筆記本執行個體的根存取權 對應的 AWS Security Hub 檢查：SageMaker.3	AWSManagedServices-TrustedRemediatorDisableSageMakerNotebookInstanceRootAccess SageMaker 筆記本執行個體已停用使用者的根存取權。	不允許預先設定的參數。 如果 SageMaker 筆記本執行個體處於 InService 狀態，則此修復會導致中斷。
Hs4Ma3G179 - SNS 主題應使用靜態加密 AWS KMS 對應的 AWS Security Hub 檢查：SNS.1	AWSManagedServices-EnableSNSEncryptionAtRest SNS 主題是以伺服器端加密設定。	KmsKeyId：Amazon SNS 的 AWS 受管客戶主金鑰 (CMK) 或用於伺服器端加密 (SSE) 的自訂 CMK ID。預設值設為 `alias/aws/sns` 。 如果使用自訂 AWS KMS 金鑰，則必須設定正確的許可。如需詳細資訊，請參閱啟用 Amazon SNS 主題的伺服器端加密 (SSE)

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G158 - SSM 文件不應公開 對應的 AWS Security Hub 檢查：SSM.4	AWSManagedServices-TrustedRemediatorDisableSSMDocPublicSharing - 停用 SSM 文件的公開共用。	不允許預先設定的參數。 無限制條件
Hs4Ma3G136 - Amazon SQS 佇列應靜態加密 對應的 AWS Security Hub 檢查：SQS.1	AWSManagedServices-EnableSQSEncryptionAtRest Amazon SQS 中的訊息會加密。	• SqsManagedSseEnabled：設定為 `true` 以使用 Amazon SQS 擁有的加密金鑰啟用伺服器端佇列加密，設定為 `false` 以使用 AWS KMS 金鑰啟用伺服器端佇列加密。 • KMSKeyId：Amazon SQS 的 AWS 受管客戶主金鑰 (CMK) 或自訂 CMK 的 ID 或別名，用於佇列的伺服器端加密。如果未提供，則會使用alias/aws/sqs。 • KmsDataKeyReusePeriodSeconds：Amazon SQS 可以在 AWS KMS 再次呼叫之前重複使用資料金鑰來加密或解密訊息的時間長度，以秒為單位。代表秒數的整數，介於 60 秒 (1 分鐘) 和 86,400 秒 (24 小時) 之間。如果 `SqsManagedSseEnabled` 設定為 `true`，則會忽略此設定。 對加密佇列的匿名 SendMessage 和 ReceiveMessage 請求會遭到拒絕。所有對啟用 SSE 之佇列的請求都必須使用 HTTPS 和簽章版本 4。

Trusted Advisor Trusted Remediator 支援的容錯能力檢查

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
c18d2gz138 Amazon DynamoDB 時間點復原	AWSManagedServices-TrustedRemediatorEnableDDBPITR 啟用 DynamoDB 資料表的point-in-time復原。	不允許預先設定的參數。 無限制條件
R365s2Qddf Amazon S3 Bucket Versioning	AWSManagedServices-TrustedRemediatorEnableBucketVersioning Amazon S3 儲存貯體版本控制已啟用。	不允許預先設定的參數。 此修復不支援修復 AWS 服務 已建立的 S3 儲存貯體 （例如 cf-templates-000000000000)。
BueAdJ7NrP Simple Storage Service (Amazon S3) 儲存貯體記錄	AWSManagedServices-EnableBucketAccessLogging Amazon S3 儲存貯體記錄已啟用。	• TargetBucket：儲存伺服器存取日誌的 S3 儲存貯體名稱。 • TargetObjectKeyFormat：日誌物件的 Amazon S3 金鑰格式，若要將 S3 金鑰的簡單格式用於日誌物件，請選擇 SimplePrefix 。若要將分割的 S3 金鑰用於日誌物件，並將 EventTime 用於分割的字首，請選擇 PartitionedPrefixEventTime 。若要將分割的 S3 金鑰用於日誌物件，並將 DeliveryTime 用於分割的字首，請選擇 PartitionedPrefixDeliveryTime 。預設值為 PartitionedPrefixEventTime 。有效值為 SimplePrefix 、PartitionedPrefixEventTime 和 PartitionedPrefixDeliveryTime （區分大小寫）。

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
		若要啟用自動修復，必須提供下列預先設定的參數： • TargetBucket 目的地儲存貯體必須與來源儲存貯體位於相同 AWS 帳戶 AWS 區域 且具有正確的日誌交付許可。如需詳細資訊，請參閱啟用 Amazon S3 伺服器存取記錄。
f2iK5R6Dep Amazon RDS Multi-AZ	AWSManagedServices-TrustedRemediatorEnableRDSMultiAZ 已啟用多可用區域部署。	不允許預先設定的參數。 在此變更期間，可能會發生效能降低。
H7IgTzjTYb Amazon EBS 快照	AWSManagedServices-TrustedRemediatorCreateEBSSnapshot Amazon EBSsnapshots 已建立。	不允許預先設定的參數。 無限制條件
opQPADkZvH RDS 備份	AWSManagedServices-EnableRDSBackupRetention 資料庫已啟用 Amazon RDS 備份保留。	• BackupRetentionPeriod：保留自動備份的天數 (1-35)。 • ApplyImmediately：指出是否盡快非同步套用 RDS 備份保留變更和任何待定修改。選擇立即`true`套用變更，或`false`為下一個維護時段排程變更。 如果 `ApplyImmediately` 參數設定為 `true`，則 db 上的待定變更會與 RDSBackup 保留設定一起套用。

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
c1qf5bt013 Amazon RDS 資料庫執行個體已關閉儲存體自動調整規模	AWSManagedServices-TrustedRemediatorEnableRDSInstanceStorageAutoScaling - 針對 Amazon RDS 資料庫執行個體啟用儲存體自動擴展。	• MaxAllocatedStorageIncreasePercentage：目前 Allocated Storage 的增加百分比，用於設定 MaxAllocatedStorage。預設值設為 26。 您必須將最大儲存閾值設定為比目前配置的儲存多至少 10%。最佳實務是將最大儲存閾值設定為至少多 26%。如需詳細資訊，請參閱使用 Amazon Relational Database Service 儲存體自動調整規模自動管理容量。 無限制條件
7qGXsKIUw Classic Load Balancer 連線耗盡	AWSManagedServices-TrustedRemediatorEnableCLBConnectionDraining Classic Load Balancer 已啟用連線耗盡。	ConnectionDrainingTimeout：取消註冊執行個體之前，保持現有連線開啟的最長時間，以秒為單位。預設值設為300秒。 無限制條件
c18d2gz106 AWS Backup 計劃中不包含 Amazon EBS	AWSManagedServices-TrustedRemediatorAddVolumeToBackupPlan Amazon EBS 包含在 AWS Backup 計劃中。	修復會使用下列標籤對來標記 Amazon EBS 磁碟區。標籤對必須符合 的標籤型資源選擇條件 AWS Backup。 • TagKey • TagValue 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
c18d2gz107 AWS Backup 計劃中不包含 Amazon DynamoDB 資料表	AWSManagedServices-TrustedRemediatorAddDynamoDBToBackupPlanAddDynamoDBToBackupPlan Amazon DynamoDB 資料表包含在 AWS Backup 計劃中。	修復會使用下列標籤對來標記 Amazon DynamoDB。標籤對必須符合 的標籤型資源選擇條件 AWS Backup。 • TagKey • TagValue 無限制條件
c18d2gz117 AWS Backup 計劃中不包含 Amazon EFS	AWSManagedServices-TrustedRemediatorAddEFSToBackupPlan Amazon EFS 包含在 AWS Backup 計劃中。	修復會使用下列標籤對來標記 Amazon EFS。標籤對必須符合 的標籤型資源選擇條件 AWS Backup。 • TagKey • TagValue 無限制條件
c18d2gz105 跨負載平衡的 Network Load Balancer	AWSManagedServices-TrustedRemediatorEnableNLBCrossZoneLoadBalancing Network Load Balancer 上已啟用跨區域負載平衡。	不允許預先設定的參數。 無限制條件
c1qf5bt026 Amazon RDS `synchronous_commit` 參數已關閉	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Amazon RDS 的 參數`synchronous_commit` 已開啟。	不允許預先設定的參數。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
c1qf5bt030 Amazon RDS `innodb_flush_log_at_trx_commit` 參數不是 1	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Amazon RDS 1 的 參數`innodb_flush_log_at_trx_commit` 設定為 。	不允許預先設定的參數。 無限制條件
c1qf5bt031 Amazon RDS `sync_binlog` 參數已關閉	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Amazon RDS 的 參數`sync_binlog` 已開啟。	不允許預先設定的參數。 無限制條件
c1qf5bt036 Amazon RDS `innodb_default_row_format` 參數設定不安全	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Amazon RDS `DYNAMIC` 的 參數`innodb_default_row_format` 設定為 。	不允許預先設定的參數。 無限制條件
c18d2gz144 未啟用 Amazon EC2 詳細監控	AWSManagedServices-TrustedRemediatorEnableEC2InstanceDetailedMonitoring Amazon EC2 已啟用詳細監控。	不允許預先設定的參數。 無限制條件

Trusted Advisor Trusted Remediator 支援的效能檢查

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
COr6dfpM06	AWSManagedServices-ResizeLambdaMemory	RecommendedMemorySize：Lambda 函數的建議記憶體配置。值範圍介於 128 和 10240 之間。

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
AWS Lambda 記憶體大小的佈建不足函數	Lambda 函數的記憶體大小會調整為 提供的建議記憶體大小 Trusted Advisor。	如果在自動化執行之前修改 Lambda 函數大小，則此自動化可能會以 建議的值覆寫設定 Trusted Advisor。
ZRxQlPsb6c Amazon EC2 執行個體高使用率	AWSManagedServices-ResizeInstanceByOneLevel Amazon EC2 執行個體的大小會由相同執行個體系列類型的一個執行個體類型調整。執行個體會在調整大小操作期間停止和啟動，並在執行完成後返回初始狀態。此自動化不支援調整 Auto Scaling 群組中的執行個體大小。	• MinimumDaysSinceLastChange：自上次執行個體類型變更以來的天數下限。如果在指定的時間內修改執行個體類型，則不會變更執行個體類型。使用 0 略過此驗證。預設值為 7。 • CreateAMIBeforeResize：若要在調整大小之前建立執行個體 AMI 做為備份，請選擇 true。若要不建立備份，請選擇 false。預設值為 false。有效值為 true和 false（區分大小寫）。 • ResizeIfStopped：若要繼續變更執行個體大小，即使執行個體處於停止狀態，請選擇 true。如果執行個體處於停止狀態，若要不自動調整其大小，請選擇 false。有效值為 true和 false（區分大小寫）。 無限制條件
c1qf5bt021 使用低於最佳值的 Amazon RDS innodb_change_buffering 參數	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Amazon RDS 的 innodb_change_buffering 參數值設定為 NONE。	不允許預先設定的參數。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
c1qf5bt025 Amazon RDS `autovacuum` 參數已關閉	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Amazon RDS 的 參數`autovacuum` 已開啟。	不允許預先設定的參數。 無限制條件
c1qf5bt028 Amazon RDS `enable_indexonlyscan` 參數已關閉	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Amazon RDS 的 參數`enable_indexonlyscan` 已開啟。	不允許預先設定的參數。 無限制條件
c1qf5bt029 Amazon RDS `enable_indexscan` 參數已關閉	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Amazon RDS 的 參數`enable_indexscan` 已開啟。	不允許預先設定的參數。 無限制條件
c1qf5bt032 Amazon RDS `innodb_stats_persistent` 參數已關閉	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Amazon RDS 的 參數`innodb_stats_persistent` 已開啟。	不允許預先設定的參數。 無限制條件
c1qf5bt037 Amazon RDS `general_logging` 參數已開啟	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Amazon RDS 的參數`general_logging` 已關閉。	不允許預先設定的參數。 無限制條件

Trusted Advisor Trusted Remediator 支援的 服務限制檢查

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
lN7RR0l7J9 EC2-VPC 彈性 IP 地址	AWSManagedServices-UpdateVpcElasticIPQuota 系統會請求 EC2-VPC 彈性 IP 地址的新限制。根據預設，限制會增加 3。	增量：增加目前配額的數字。預設值為 3。 如果此自動化在 Trusted Advisor 檢查更新為 OK 狀態之前執行多次，則可能會提高限制。
kM7QQ0l7J9 VPC 網際網路閘道	AWSManagedServices-IncreaseServiceQuota - 請求 VPC 網際網路閘道的新限制。根據預設，限制會增加 3。	增加：增加目前配額的數字。預設值為 3。 如果此自動化在 Trusted Advisor 檢查更新為 OK 狀態之前執行多次，則可能會提高限制。
jL7PP0l7J9 VPC	AWSManagedServices-IncreaseServiceQuota 已請求 VPC 的新限制。根據預設，限制會增加 3。	增加：增加目前配額的數字。預設值為 3。 如果此自動化在 Trusted Advisor 檢查更新為 OK 狀態之前執行多次，則可能會提高限制。
fW7HH0l7J9 Auto Scaling 群組	AWSManagedServices-IncreaseServiceQuota 已請求 Auto Scaling 群組的新限制。根據預設，限制會增加 3。	增加：增加目前配額的數字。預設值為 3。 如果此自動化在 Trusted Advisor 檢查更新為 OK 狀態之前執行多次，則可能會提高限制。
3Njm0DJQO9 RDS 選項群組	AWSManagedServices-IncreaseServiceQuota 已請求 Amazon RDS 選項群組的新限制。根據預設，限制會增加 3。	增加：增加目前配額的數字。預設值為 3。 如果此自動化在 Trusted Advisor 檢查更新為 OK 狀態之前執行多次，則可能會提高限制。

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
EM8b3yLRTr ELB Application Load Balancer	AWSManagedServices-IncreaseServiceQuota 會請求 ELB Application Load Balancer 的新限制。根據預設，限制會增加 3。	增加：增加目前配額的數字。預設值為 3。 如果此自動化在 Trusted Advisor 檢查更新為 OK 狀態之前執行多次，則可能會提高限制。
8wlqYSt25K ELB Network Load Balancer	AWSManagedServices-IncreaseServiceQuota 會請求 ELB Network Load Balancer 的新限制。根據預設，限制會增加 3。	增加：增加目前配額的數字。預設值為 3。 如果此自動化在 Trusted Advisor 檢查更新為 OK 狀態之前執行多次，則可能會提高限制。

Trusted Advisor Trusted Remediator 支援的卓越營運檢查

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
c18d2gz125 Amazon API Gateway 未記錄執行日誌	AWSManagedServices-TrustedRemediatorEnableAPIGateWayExecutionLogging 執行記錄會在 API 階段上啟用。	不允許預先設定的參數。 您必須授予 API Gateway 許可，以讀取和寫入您帳戶的日誌至 CloudWatch，以啟用執行日誌，請參閱在 API Gateway 中設定 REST APIs的 CloudWatch 日誌記錄以取得詳細資訊。
c18d2gz168 未針對負載平衡器啟用 Elastic Load Balancing 刪除保護	為 Elastic Load Balancer 開啟 AWSManagedServices-TrustedRemediatorEnableELBDeletionProtection - 刪除保護。	不允許預先設定的參數。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
c1qf5bt012 Amazon RDS Performance Insights 已關閉	AWSManagedServices-TrustedRemediatorEnableRDSPerformanceInsights Amazon RDS 的績效詳情已開啟。	• PerformanceInsightsRetentionPeriod：保留績效詳情資料的天數。有效值： 7或月 * 31，其中月是從 1-23 的月數。範例： 93 (3 個月 * 31)、 341(11 個月 * 31)、589(19 個月 * 31) 或 731。 • PerformanceInsightsKMSKeyId：Performance Insights 資料的加密 AWS KMS 金鑰 ID。如果您未指定 PerformanceInsightsKMSKeyId 的值，則 Amazon RDS 會使用預設 AWS KMS 金鑰。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
c1fd6b96l4 已啟用 Amazon S3 存取日誌	AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV2 Amazon S3 儲存貯體存取記錄已啟用。	• TargetBucketTagValue：用於識別目標儲存貯體的標籤值（區分大小寫），請使用此值和 TargetBucketTagKey 來標記要用作存取記錄目的地儲存貯體的儲存貯體。 • TargetObjectKeyFormat：日誌物件的 Amazon S3 金鑰格式（值區分大小寫）。若要針對日誌物件使用 S3 金鑰的簡單格式，請選擇 `SimplePrefix` 。若要將分割的 S3 金鑰用於日誌物件，並將 EventTime 用於分割的字首，請選擇 `PartitionedPrefixEventTime` 。若要將分割的 S3 金鑰用於日誌物件，並將 DeliveryTime 用於分割的字首，請選擇 `PartitionedPrefixDeliveryTime` 。有效值為 `SimplePrefix` 、`PartitionedPrefixEventTime` 和 `PartitionedPrefixDeliveryTime` 。 若要啟用自動修復，必須提供下列預先設定的參數：TargetBucketTagKey 和 TargetBucketTagValue。 目的地儲存貯體必須與來源儲存貯體位於相同 AWS 帳戶 AWS 區域 且具有正確的日誌交付許可。如需詳細資訊，請參閱啟用 Amazon S3 伺服器存取記錄。

在信任的修復程式中設定 Trusted Advisor 檢查修復

組態會存放在 中 AWS AppConfig ，做為信任的修復程式應用程式的一部分。每個 Trusted Advisor 檢查類別都有單獨的組態描述檔。如需 Trusted Advisor 類別的詳細資訊，請參閱檢視檢查類別。

您可以根據每個資源或每個 Trusted Advisor 檢查來設定修復。您可以使用資源標籤套用例外狀況。

> **Note**
>
> 問題 Trusted Advisor 清單的修復目前是使用 設定 AWS AppConfig，且此功能目前完全支援。AMS 預期這會在未來變更。最佳實務是避免建置相依的自動化 AWS AppConfig，因為此方法可能會有所變更。請注意，為了實現相容性，您可能需要更新或修改以目前 AWS AppConfig 實作為基礎的自動化。
> Compute Optimizer -> EC2 執行個體功能旗標具有額外的參數：
>
> - allow-upscale 允許升級佈建不足的非最佳化 EC2 執行個體。預設值為 "false"。
> - min-savings-opportunity-percentage 自動化修復的最低節省百分比機會。預設值為 10%

預設修復組態

個別 Trusted Advisor 檢查的組態會儲存為 AWS AppConfig 旗標。旗標名稱符合檢查名稱。每個檢查組態都包含下列屬性：

- execution-mode：決定信任的修復程式如何執行預設修復：
  - 自動化：信任的修復程式會自動修復資源，方法是建立 OpsItem、執行 SSM 文件，然後在成功執行後解決 OpsItem。
  - 手動：OpsItem 已建立，但 SSM 文件不會自動執行。您可以從 AWS Systems Manager OpsCenter 主控台中的 OpsItem 檢閱並手動執行 SSM 文件。
  - 條件式：修補預設為停用。您可以使用標籤為特定資源啟用此功能。如需詳細資訊，請參閱下列各節使用資源標籤自訂修復和 使用資源覆寫標籤自訂修復。
  - 非作用中：不會發生修復，也不會建立 OpsItem。您無法覆寫設定為非作用中之 Trusted Advisor 檢查的執行模式。
- pre configured-parameters：輸入自動化修復所需的 SSM 文件參數值，格式為 `Parameter=Value`，以逗號 (,) 分隔。Trusted Advisor Trusted Remediator 支援的檢查 如需每個檢查之相關聯 SSM 文件的支援預先設定參數，請參閱 。

- alternative-automation-document：此屬性有助於使用另一個支援的文件（如果適用於特定檢查）覆寫現有的自動化文件。根據預設，不會選取此屬性。

> **Note**
>
> `alternative-automation-document` 屬性不支援自訂自動化文件。您可以使用 中列出的現有支援信任的修復程式自動化文件Trusted Advisor Trusted Remediator 支援的檢查。例如，針對檢查 `Qch7DwouX1`，有三個相關聯的 SSM 文件：AWSManagedServices-StopEC2Instance、AWSManagedServices-ResizeInstanceByOneLevel 和 AWSManagedServices-TerminateInstance。的值`alternative-automation-document`可以是 AWSManagedServices-ResizeInstanceByOneLevel 或 AWSManagedServices-TerminateInstance (AWSManagedServices-StopEC2Instance 是要修復 的預設 SSM 文件`Qch7DwouX1`)。

每個屬性的值必須符合該屬性的限制。

> **Tip**
>
> 套用 Trusted Advisor 檢查的預設組態之前，最佳實務是考慮使用下列各節所述的資源標記和資源覆寫功能。預設組態會套用至帳戶內的所有資源，這在所有情況下可能並不理想。

以下是範例主控台螢幕擷取畫面，其中執行模式設定為手動，且屬性符合其限制條件。

使用資源標籤自訂修復

檢查組態中的automated-for-tagged-only屬性和manual-for-tagged-only屬性，可讓您針對如何修復個別檢查指定資源標籤。當您需要將一致的修補行為套用至共用相同標籤的資源群組時，最佳實務是使用此方法。以下是這些標籤的說明：

- automated-for-tagged-only：指定資源標籤（一或多個標籤對，以逗號分隔），讓檢查自動修復，無論預設執行模式為何。
- manual-for-tagged-only：為應手動執行的修復指定資源標籤（一或多個標籤對，逗號分隔），無論預設執行模式為何。

例如，如果您想要為所有非生產資源啟用自動修復，並強制執行生產資源的手動修復，您可以設定組態，如下所示：

```
"execution-mode": "Conditional",
"automated-for-tagged-only": "Environment=Non-Production",
"manual-for-tagged-only": "Environment=Production",
```

在您的 資源上設定上述組態後，請檢查修復行為，如下所示：

- 標記 'Environment=Non-Production' 的資源會自動修復。
- 標記為 'Environment=Production' 的資源需要手動介入才能修復。
- 沒有 'Environment' 標籤的資源遵循預設執行模式（在此情況下為 `Conditional`。 因此，不會對剩餘的資源採取任何動作）。

如需組態的其他支援，請聯絡您的 Cloud Architect。

使用資源覆寫標籤自訂修復

資源覆寫標籤可讓您自訂個別資源的修補行為，無論其標籤為何。透過將特定標籤新增至資源，您可以覆寫該資源的預設執行模式和 Trusted Advisor 檢查。資源覆寫標籤優先於預設組態和資源標記設定。因此，如果您使用資源覆寫標籤將資源的預設執行模式設定為自動、手動或條件式，則會覆寫預設執行模式和任何資源標記組態。

若要覆寫資源的執行模式，請完成下列步驟：

1. 識別您要覆寫修復組態的資源。
2. 決定您要覆寫之 Trusted Advisor 檢查的檢查 ID。您可以在 中找到受支援檢查IDsTrusted Advisor Trusted Remediator 支援的檢查。 Trusted Advisor
3. 使用下列索引鍵和值將標籤新增至資源：

   - 標籤索引鍵： `TR-`*`Trusted Advisor check ID`*`-Execution-Mode`（區分大小寫）

     在上述標籤索引鍵範例中，將 取代`Trusted Advisor check ID`為您要覆寫之 Trusted Advisor 檢查的唯一識別。
   - 標籤值：將下列其中一個值用於標籤值：
     - 自動化：信任的修復程式會自動修復此 Trusted Advisor 檢查的資源。
     - 手動：為資源建立 OpsItem，但不會自動執行修復。您可以從 OpsItem 手動檢閱和執行修復。

- 非作用中：不會為此資源和指定的 Trusted Advisor 檢查執行修復和 OpsItem 建立。

例如，若要使用 Trusted Advisor 檢查 ID 自動修復 Amazon EBS 磁碟區，請將DAvU99Dc4C標籤新增至 EBS 磁碟區。標籤索引鍵為 `TR-DAvU99Dc4C-Execution-Mode`，標籤值為 `Automated`。

以下是顯示標籤區段的 主控台範例：

執行模式決策工作流程

有多個層級可為您的資源和每個 Trusted Advisor 檢查設定執行模式。下圖顯示 Trusted Remediator 如何根據您的組態決定要使用的執行模式：

設定修復教學課程

下列教學課程提供在信任的修復程式中建立常見修復的範例

手動修復所有資源

此範例會設定 Trusted Advisor 檢查 ID DAvU99Dc4C （未充分利用的 Amazon EBS 磁碟區） 的所有 Amazon EBS 磁碟區的手動修復。

使用檢查 ID DAvU99Dc4C 設定 Amazon EBS 磁碟區的手動修復

1. 在 https：//https://console.aws.amazon.com/systems-manager/appconfig 開啟 AWS AppConfig 主控台。

   請確定您以委派管理員帳戶身分登入。
2. 從應用程式清單中選取信任的修復程式。
3. 選擇成本最佳化組態設定檔。
4. 選取未充分利用的 Amazon EBS 磁碟區旗標。
5. 對於執行模式，選取手動。
6. 請確定automated-for-tagged-only和manual-for-tagged-only屬性為空白。這些屬性用於覆寫具有相符標籤之資源的預設執行模式。

   以下是屬性區段的範例，其中空白值表示automated-for-tagged-only和manual-for-tagged-only，而手動表示執行模式：

7. 選擇儲存以更新值，然後選擇儲存新版本以套用變更。您必須選擇儲存新版本，信任的修復程式才能辨識變更。
8. 請確定您的 Amazon EBS 磁碟區沒有具有 金鑰的標籤`TR-DAvU99Dc4C-Execution-Mode`。此標籤金鑰會覆寫該 EBS 磁碟區的預設執行模式。

自動修復所有資源，但選取的資源除外

此範例會針對具有 Trusted Advisor 檢查 ID DAvU99Dc4C （未充分利用的 Amazon EBS 磁碟區） 的所有 Amazon EBS 磁碟區設定自動修復，但不會修復的指定磁碟區 （指定為非作用中) 除外。

使用檢查 ID DAvU99Dc4C 設定 Amazon EBS 磁碟區的自動修復，所選非作用中資源除外

1. 在 https：//https://console.aws.amazon.com/systems-manager/appconfig 開啟 AWS AppConfig 主控台。

   請確定您以委派管理員帳戶身分登入。
2. 從應用程式清單中選取信任的修復程式。
3. 選擇成本最佳化組態設定檔。
4. 選取未充分利用的 Amazon EBS 磁碟區旗標。
5. 針對執行模式，選取自動化。
6. 請確定automated-for-tagged-only和manual-for-tagged-only屬性為空白。這些屬性用於覆寫具有相符標籤之資源的預設執行模式。

   以下是屬性區段的範例，其中空白值表示automated-for-tagged-only和manual-for-tagged-only，而 自動化表示執行模式：

7. 選擇儲存以更新值，然後選擇儲存新版本以套用變更。您必須選擇儲存新版本，信任的修復程式才能辨識變更。

   此時，所有 Amazon EBS 磁碟區都會設定為自動修復。
8. 覆寫所選 Amazon EBS 磁碟區的自動修復：

   a. 前往 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。

   b. 選擇彈性區塊存放區、磁碟區。

   c. 選擇標籤。

d. 選擇管理標籤。

e. 新增下列標籤：

- 金鑰：TR-DAvU99Dc4C-Execution-Mode
- 值：非作用中

以下是標籤區段的範例，其中顯示金鑰和值欄位：

f. 針對您要從修復中排除的所有 Amazon EBS 磁碟區，重複步驟 2 到 5。

自動修復已標記的資源

此範例會針對具有 Trusted Advisor 檢查 ID DAvU99Dc4C （未充分利用的 Amazon EBS 磁碟區）`Stage=NonProd`標籤的所有 Amazon EBS 磁碟區設定自動修復。所有其他沒有此標籤的資源都無法修復。

使用檢查 ID DAvU99Dc4C 的標籤**`Stage=NonProd`**設定 Amazon EBS 磁碟區的自動修復

1. 在 https：//https://console.aws.amazon.com/systems-manager/appconfig 開啟 AWS AppConfig 主控台。

   請確定您以委派管理員帳戶身分登入。
2. 從應用程式清單中選取信任的修復程式。
3. 選擇成本最佳化組態設定檔。
4. 選取未充分利用的 Amazon EBS 磁碟區旗標。
5. 對於執行模式，選取條件式。
6. 將automated-for-tagged-only設為 `Stage=NonProd`。此屬性會覆寫具有相符標籤之資源`execution-mode`的預設值。確定manual-for-tagged-only屬性為空白。

   以下是屬性區段的範例，其中automated-for-tagged-only設定為 Stage=NonProd 且適用於執行模式的條件式：

7. 或者，將預先設定的參數設定為下列其中一項：

- `CreateSnapshot=false` 在刪除之前不建立 Amazon EBS 磁碟區的快照
- `MinimumUnattachedDays=10` 將 Amazon EBS 磁碟區的未連接天數下限設定為 10 天

- `CreateSnapshot=false`，`MinimumUnattachedDays=10`適用於上述兩者

8. 選擇儲存以更新值，然後選擇儲存新版本以套用變更。您必須選擇儲存新版本，信任的修復程式才能辨識變更。
9. 請確定您的 Amazon EBS 磁碟區沒有具有 金鑰的標籤`TR-DAvU99Dc4C-Execution-Mode`。此標籤金鑰會覆寫該 EBS 磁碟區的預設執行模式。

在信任的修復程式中使用修復

在信任的修復程式中追蹤修復

若要追蹤 OpsItems 修補，請完成下列步驟：

1. 在 https：//https://console.aws.amazon.com/systems-manager/ 開啟 AWS Systems Manager 主控台。
2. 選擇 Operations Management、OpsCenter。
3. （選用）依 Source=Trusted Remediator 篩選清單，以在清單中僅包含 Trusted Remediator OpsItems。

   以下是由 Source=Trusted Remediator 篩選的 OpsCenter 畫面範例：

> **Note**
>
> 除了從 OpsCenter 檢視 OpsItems 之外，您還可以在 AMS S3 儲存貯體中檢視修復日誌。OpsCenter 如需詳細資訊，請參閱信任的修復程式中的修復日誌。

在信任的修復程式中執行手動修復

Trusted Remediator 會為設定為手動修復的檢查建立 OpsItems。您必須檢閱這些檢查，並手動開始修復程序。

若要手動修復 OpsItem，請完成下列步驟：

1. 在 https：//https://console.aws.amazon.com/systems-manager/ 開啟 AWS Systems Manager 主控台。

2. 選擇 Operations Management、OpsCenter。
3. （選用）依 Source=Trusted Remediator 篩選清單，以在清單中僅包含 Trusted Remediator OpsItems。
4. 選擇您要檢閱的 OpsItem。
5. 檢閱 OpsItem 的操作資料。操作資料包含下列項目：

   - trustedAdvisorCheckCategory： Trusted Advisor 檢查 ID 的類別。例如，容錯能力
   - trustedAdvisorCheckId：唯一的 Trusted Advisor 檢查 ID。
   - trustedAdvisorCheckMetadata：資源中繼資料，包括資源 ID。
   - trustedAdvisorCheckName： Trusted Advisor 檢查的名稱。
   - trustedAdvisorCheckStatus：針對資源偵測到的 Trusted Advisor 檢查狀態。

6. 若要手動修復 OpsItem，請完成下列步驟：

   a. 從 Runbook 中，選擇其中一個相關聯的 Runbook (SSM 文件）。
   b. 選擇 Execute (執行)。
   c. 針對 AutomationAssumeRole ，選擇 `arn:aws:iam::AWS ## ID:role/ams_ssm_automation_role`。將 AWS 帳戶 ID 取代為修復執行所在的帳戶 ID。如需其他參數值，請參閱操作資料。

      若要手動修復資源，用於向 驗證 的角色或使用者 AWS 帳戶 必須具有 IAM 角色的`iam:PassRole`許可`ams-ssm-automation-role`。如需詳細資訊，請參閱授予使用者將角色傳遞至 的許可 AWS 服務，或聯絡您的 Cloud Architect。
   d. 選擇 Execute (執行)。
   e. 在最新狀態和結果欄中監控 SSM 文件執行的進度。
   f. 文件完成後，選擇設定狀態、已解析以手動解析 OpsItem。如果文件失敗，請檢閱詳細資訊並重新執行 SSMdocument。如需其他故障診斷支援，請建立服務請求。

   若要在沒有修復的情況下解析 OpsItem，請選取將狀態設定為已解決。
7. 針對所有剩餘的手動修復 OpsItems，重複步驟 3 和 4。

對信任的修復程式中的修復進行故障診斷

如需手動修復和修復失敗的協助，請聯絡 AMS。

若要檢視修復狀態和結果，請完成下列步驟：

1. 在 https：//https://console.aws.amazon.com/systems-manager/ 開啟 AWS Systems Manager 主控台。
2. 選擇 Operations Management、OpsCenter。
3. （選用）依 Source=Trusted Remediator 篩選清單，以在清單中僅包含 Trusted Remediator OpsItems。
4. 選擇您要檢閱的 OpsItem。
5. 在自動化執行區段中，檢閱文件名稱、狀態和結果。
6. 檢閱下列常見的自動化失敗。如果您的問題未列在此處，請聯絡您的 CSDM 尋求協助。

常見的修復錯誤

自動化執行中未列出任何執行

沒有與 OpsItem 相關聯的執行可能表示執行因為不正確的參數值而無法啟動。

疑難排解步驟

1. 在操作資料中，檢閱 `trustedAdvisorCheckAutoRemediation` 屬性值。
2. 驗證 DocumentName 和參數值是否正確。如需正確的值，在信任的修復程式中設定 Trusted Advisor 檢查修復請檢閱 以取得如何設定 SSM 參數的詳細資訊。若要檢閱支援的檢查參數，請參閱 Trusted Advisor Trusted Remediator 支援的檢查
3. 驗證 SSM 文件中的值是否符合允許的模式。若要檢視文件內容中的參數詳細資訊，請在 Runbooks 區段中選取文件名稱。
4. 在您檢閱和更正參數之後，請再次手動執行 SSM 文件。
5. 若要防止此錯誤再次發生，請確定您使用組態中的正確參數值來設定修復。如需詳細資訊，請參閱在信任的修復程式中設定 Trusted Advisor 檢查修復

自動化執行中失敗的執行

修復文件包含多個步驟，這些步驟與透過 APIs AWS 服務 執行各種動作互動。若要識別失敗的特定原因，請完成下列步驟：

疑難排解步驟

1. 若要檢視個別執行步驟，請選擇執行 ID、自動化執行區段中的連結。以下是 Systems Manager 主控台的範例，其中顯示所選自動化的執行步驟：

2. 選擇狀態為失敗的步驟。以下是錯誤訊息範例：

   - `NoSuchBucket - An error occurred (NoSuchBucket) when calling the GetPublicAccessBlock operation: The specified bucket does not exist`

     此錯誤表示在修復組態的預先設定參數中指定了不正確的儲存貯體名稱。

     若要解決此錯誤，請使用正確的儲存貯體名稱手動執行自動化。為避免此問題再次發生，請使用正確的儲存貯體名稱更新修復組態。

   - `DB instance my-db-instance-1 is not in available status for modification.`

     此錯誤表示自動化無法進行預期的變更，因為資料庫執行個體處於無效狀態。

     若要解決此錯誤，請手動執行自動化。

信任的修復程式中的修復日誌

Trusted Remediator 會以 JSON 格式建立日誌，並將其上傳至 Amazon Simple Storage Service。日誌檔案會上傳至 AMS 建立且名為 的 S3 儲存貯體`ams-trusted-remediator-{your-account-id}-logs`。AMS 會在委派管理員帳戶中建立 S3 儲存貯體。您可以將日誌檔案匯入 QuickSight，以產生自訂的修補報告。

如需詳細資訊，請參閱與 QuickSight 的信任修復程式整合。

修復項目日誌

建立修復 OpsItem `Remediation item log`時，信任的修復程式會建立 。此日誌包含手動修復 OpsItem 和自動修復 OpsItem。您可以使用 `Remediation item log`來追蹤所有修補的概觀。

Compute Optimizer 建議的修復項目日誌位置

`s3://ams-trusted-remediator-`*`delegated-administrator-account-id`*`-logs/compute_optimizer_remediation_items/`*`remediation creation time in yyyy-mm-dd format`*`/`*`10 digits epoch time or unix timestamp`*`-`*`Trusted Advisor check ID`*`-`*`Resource ID`*`.json`

Trusted Advisor 檢查的修復項目日誌位置

s3://ams-trusted-remediator-*delegated-administrator-account-id*-logs/remediation_items/*remediation creation time in yyyy-mm-dd format*/*10 digits epoch time or unix timestamp*-*Trusted Advisor check ID*- *Resource ID*.json

修復項目日誌範例檔案 URL

s3:///ams-trusted-remediator-*111122223333*-logs/remediation_items/*2023-02-06*/*1675660464-DAvU99Dc4C-vol-00bd8965660b4c16d.json*

Compute Optimizer Remediation 項目日誌格式

```
{
  "AccountID": "Account_ID",
  "ComputeOptimizerCheckID": "Compute Optimizer check ID",
  "ComputeOptimizerCheckName": "Compute Optimizer check name",
  "ResourceID": "Resource ID",
  "RemediationTime": Remediation creation time,
  "ExecutionMode": "Automated or Manual",
  "OpsItemID": "OpsItem ID"
}
```

Trusted Advisor 修復項目日誌格式

```
{
   "TrustedAdvisorCheckID": Trusted Advisor check ID,
   "TrustedAdvisorCheckName": Trusted Advisor check name,
   "TrustedAdvisorCheckResultTime": 10 digits epoch time or unix timestamp,
   "ResourceID": Resource ID,
   "RemediationTime": Remediation creation time,
   "ExecutionMode": Automated or Manual,
   "OpsItemID": OpsItem ID
}
```

Compute Optimizer Remediation 項目日誌格式範例內容

```
{
  "AccountID": "123456789012",
  "ComputeOptimizerCheckID": "compute-optimizer-ebs",
  "ComputeOptimizerCheckName": "EBS volumes",
  "ResourceID": "vol-1235589366f77aca7",
  "RemediationTime": 1755044783,
```

```
  "ExecutionMode": "Manual",
  "OpsItemID": "oi-b8888b38fe78"
}
```

Trusted Advisor 修復項目日誌格式範例內容

```
{
    "TrustedAdvisorCheckID": "DAvU99Dc4C",
    "TrustedAdvisorCheckName": "Underutilized Amazon EBS Volumes",
    "TrustedAdvisorCheckResultTime": 1675614749,
    "ResourceID": "vol-00bd8965660b4c16d",
    "RemediationTime": 1675660464,
    "OpsItemID": "oi-cca5df7af718"
}
```

自動化修復執行日誌、Compute Optimizer 和 Trusted Advisor

當自動化 SSM 文件執行完成Automated remediation execution log時，信任的修復程式會建立 。此日誌僅包含自動修復 OpsItem 的 SSM 執行詳細資訊。您可以使用此日誌檔案來追蹤自動化修復。

Compute Optimizer 自動化修復日誌位置

s3://ams-trusted-remediator-*delegated-administrator-account-id*-logs//remediation_executions/*remediation creation time in yyyy-mm-dd format*/*10 digits epoch time or unix timestamp*-*Compute Optimizer recommendation ID*.json

Trusted Advisor 自動化修復日誌位置

s3://ams-trusted-remediator-*delegated-administrator-account-id*-logs//remediation_executions/*remediation creation time in yyyy-mm-dd format*/*10 digits epoch time or unix timestamp*-*Trusted Advisor check ID*-*Resource ID*.json

Compute Optimizer 自動化修復日誌位置範例

s3://ams-trusted-remediator-*111122223333*-logs/remediation_executions/2025-06-26/1750908858-123456789012-compute-optimizer-ec2-i-1235173471d2cd789.json

Trusted Advisor 自動化修復日誌位置範例

s3://ams-trusted-remediator-*111122223333*-logs/remediation_executions/2023-02-06/1675660573-DAvU99Dc4C-vol-00bd8965660b4c16d.json

自動化修復日誌格式範例內容

```
{
    "OpsItemID": "oi-767c77e05301",
    "SSMExecutionID": "93d091b2-778a-4cbc-b672-006954d76b86",
    "SSMExecutionStatus": "Success"}
```

成員帳戶日誌

當您的帳戶加入或退出Member accounts log時，信任的修復程式會建立 。您可以使用 Member accounts log 尋找每個成員帳戶的帳戶 ID AWS 區域、加入的 和執行時間。

成員帳戶日誌位置

s3://ams-trusted-remediator-*delegated-administrator-account-id*-logs/configuration_logs/member_accounts.json

成員帳戶日誌範例檔案 URL

s3://ams-trusted-remediator-*111122223333*-logs/configuration_logs/member_accounts.json

成員帳戶日誌格式

```
{
    "delegated_administrator_account_id": Delegated Administrator account id,
    "appconfig_configuration_region": Trusted Remediator AppConfig Region,
    "member_accounts": [
        {
            "account_id": Member account id
            "account_partition": Member account partition (for example, aws),
            "regions": [
                {
                    "execution_time": Remediation execution time in cron schedule
 expression,
                    "execution_timezone": Timezone for the remediation execution time,
                    "region_name": AWS ## name
                }
                ...
```

```
            ]
        }
        ...
    ],
    "updated_at": Log update time,
}
```

成員帳戶日誌格式範例內容

```
{
    "delegated_administrator_account_id": "111122223333",
    "appconfig_configuration_region": "ap-southeast-2",
    "member_accounts": [
        {
            "account_id": "222233334444",
            "account_partition": "aws",
            "regions": [
                {
                    "execution_time": "0 9 * * 6",
                    "execution_timezone": "Australia/Sydney",
                    "region_name": "ap-southeast-2"
                },
                {
                    "execution_time": "0 5 * * 7",
                    "execution_timezone": "UTC",
                    "region_name": "us-east-1"
                }
            ]
        },
        {
            "account_id": "333344445555",
            "account_partition": "aws",
            "regions": [
                {
                    "execution_time": "0 1 * * 5",
                    "execution_timezone": "Asia/Seoul",
                    "region_name": "ap-northeast-2"
                }
            ]
        }
    ],
    "updated_at": "1730869607"
}
```

與 QuickSight 的信任修復程式整合

您可以將存放在 Amazon S3 中的受信任修復程式日誌與 QuickSight 整合，以建置自訂修復報告。QuickSight 整合是選用的。此功能可讓您使用日誌來建置自訂報告儀表板。若要取得受信任修復程式的請求報告，請聯絡您的 CSDM。如需可用 Trusted Remediator 報告的詳細資訊，請參閱 信任的修復程式報告。

如需在 QuickSight 中視覺化資料的詳細資訊，請參閱在 QuickSight 中視覺化資料。

將資料集新增至 QuickSight for Remediation 項目日誌

若要將資料集新增至 QuickSight for the Remediation 項目日誌，請遵循下列步驟：

1. 登入 QuickSight 主控台。您可以在 QuickSight 支援的任何 中建立 AWS 區域 QuickSight 報告。不過，為了提升效能並降低成本，最佳實務是在信任的還原程式記錄儲存貯體所在的區域中建立報告。
2. 選擇資料集。
3. 選擇 S3。
4. 在新的 S3 資料來源中，輸入下列值：

   - 資料來源名稱： `trusted-remediator-`*`delegated_administrator_account_id`*`-`*`account_region`*`-remediation-items`。
   - 上傳資訊清單檔案：使用下列內容建立 JSON 檔案，並使用它。建立檔案時，請在 URIPrefixes 金鑰`logging_bucket_name`中取代 。

```
{
    "fileLocations": [
        {
            "URIPrefixes": [
                "s3://{logging_bucket_name}/remediation_items/"
            ]
        }
    ],
    "globalUploadSettings": {
        "format": "JSON",
        "delimiter": ",",
        "textqualifier": "'",
        "containsHeader": "true"
```

```
    }
}
```

- 選擇連線。
- 從完成資料集建立視窗中，選擇視覺化。
- QuickSight 會開啟新的分析工作表頁面。您現在可以使用修復項目日誌建立新的分析。

以下是範例分析：

將資料集新增至 QuickSight 以取得自動化修復執行日誌

1. 登入 QuickSight 主控台。您可以在 QuickSight 支援的任何 中建立 AWS 區域 QuickSight 報告。不過，為了提升效能並降低成本，最佳實務是在信任的還原程式記錄儲存貯體所在的區域中建立報告。
2. 選擇資料集。
3. 選擇 S3。
4. 在新的 S3 資料來源中，輸入下列值：

   - 資料來源名稱：`trusted-remediator-`*`delegated_administrator_account_id`*`-`*`account_region`*`-remediation-executions`。
   - 上傳資訊清單檔案：使用下列內容建立 JSON 檔案，然後使用此檔案。建立檔案時，請在 URIPrefixes 金鑰`logging_bucket_name`中取代 。

```
{
    "fileLocations": [
        {
            "URIPrefixes": [
                "s3://{logging_bucket_name}/remediation_executions/"
            ]
        }
    ],
    "globalUploadSettings": {
        "format": "JSON",
        "delimiter": ",",
        "textqualifier": "'",
        "containsHeader": "true"
    }
```

```
}
```

- 選擇連線。
- 從完成資料集建立視窗中，選擇視覺化。
- QuickSight 會開啟新的分析工作表頁面。您現在可以使用修復項目日誌建立新的分析。

以下是範例分析：

Trusted Remediator 中的最佳實務

以下是協助您使用受信任修復程式的最佳實務：

- 如果您不確定修復結果，請從手動執行模式開始。有時，從一開始針對修復套用自動執行可能會導致非預期的結果。
- 每週檢閱修復和 OpsItems，以取得信任的修復程式結果的洞見。
- 成員帳戶會從委派管理員帳戶繼承組態。因此，請務必以可協助您管理具有相同組態的多個帳戶的方式來建構帳戶。您可以使用標籤從預設組態中豁免資源。

信任的修復程式FAQs

以下是有關信任修復程式的常見問題：

什麼是信任的修復程式，它如何使我受益？

當 Compute Optimizer 識別出不合規 Trusted Advisor 或發出建議時，信任的補救措施會根據您指定的偏好設定回應，方法是套用補救措施、透過手動補救措施尋求核准，或在即將到來的每月商業審查 (MBR) 期間報告補救措施。修復會在您偏好的修復時間或排程進行。Trusted Remediator 可讓您自行執行 Trusted Advisor 檢查，並對檢查採取動作，並靈活地個別或大量設定和修復檢查。透過經過測試的修補文件程式庫，AMS 會持續套用安全檢查並遵循 AWS 最佳實務來提高您的帳戶。只有在組態中指定這麼做時，您才會收到通知。AMS 使用者可以選擇加入 Trusted Remediator，無需額外費用。

信任的修復程式與其他 有何關聯和搭配 AWS 服務？

您可以在現有的企業支援計劃中存取 Trusted Advisor 檢查和運算最佳化工具建議。Trusted Remediator 與 Trusted Advisor 和 Compute Optimizer 整合，以利用現有的 AMS 自動化功能。具體而言，AMS 使用 AWS Systems Manager 自動化文件 （執行手冊） 進行自動化修復。 AWS AppConfig

用於設定修復工作流程。您可以透過 Systems Manager OpsCenter 檢視所有目前和過去的修補。修復日誌存放在 Amazon S3 儲存貯體中。您可以使用日誌在 QuickSight 中匯入和建置自訂報告儀表板。

誰會設定修補？

您擁有帳戶中的組態。管理您的組態是您的責任。您可以聯絡 CA 或 CDSM 以協助管理您的組態。您也可以透過 服務請求來聯絡 AMS，以取得組態支援、手動修復和故障診斷修復失敗。

如何安裝 SSM 自動化文件？

SSM 自動化文件會自動與加入的 AMS 帳戶共用。

AMS 擁有的資源也會修復嗎？

AMS 擁有的資源不會由信任的修復程式標記。Trusted Remediator 僅專注於您的 資源。

AWS 區域 什麼是 中的可信任修復程式，以及誰可以使用它？

AMS Accelerate 客戶可以使用信任的補救程式。如需支援區域的最新清單，請參閱AWS 服務 依區域。

信任的修復程式會造成資源漂移嗎？

由於 SSM 自動化文件會透過 AWS API 直接更新資源，因此可能會發生資源偏離。您可以使用標籤來隔離透過現有 CI/CD 套件建立的資源。您可以設定信任的修復程式，忽略已標記的資源，同時仍然修復其他資源。

如何暫停或停止信任的修復程式？

您可以透過 AWS AppConfig 應用程式關閉信任的修復程式。若要暫停或停止信任的修復程式，請完成下列步驟：

1. 在 https：//https://console.aws.amazon.com/systems-manager/appconfig 開啟 AWS AppConfig 主控台。
2. 選取信任的修復程式。
3. 在組態設定檔上選擇設定。
4. 選取暫停信任的修復程式旗標。
5. 將 `suspended` 屬性的值設定為 `true`。

> **Note**
>
> 使用此程序時請小心，因為這會停止與委派管理員帳戶連結的所有帳戶的信任修復程式。

如何修復受信任修復程式不支援的檢查？

您可以繼續透過 Operations On Demand (OOD) 聯絡 AMS 以進行不支援的檢查。AMS 可協助您修復這些檢查。如需詳細資訊，請參閱隨需操作。

信任的修復程式與 AWS Config 修復有何不同？

AWS Config 修補是另一種解決方案，可協助您最佳化雲端資源並維持最佳實務的合規性。以下是兩個解決方案之間的一些操作差異：

- Trusted Remediator 使用 Trusted Advisor 和 Compute Optimizer 做為偵測機制。 AWS Config Remediation 使用 AWS Config 規則做為偵測機制。
- 對於信任的修復程式，修復會按照您預先定義的修復排程進行。在 中 AWS Config，修復會即時發生。
- 可信任修復程式中每個修復的參數可根據您的使用案例輕鬆自訂，而且可以透過在資源上新增標籤來自動化或手動進行修復。
- Trusted Remediator 提供報告功能。
- Trusted Remediator 會傳送電子郵件通知給您，其中包含修復清單和修復狀態。

有些 Trusted Advisor 檢查和 Compute Optimizer 建議可能有相同的規則 AWS Config。如果存在相符的 AWS Config 規則和 Trusted Advisor 檢查，最佳實務是僅啟用一個修復。如需每個 Trusted Advisor 檢查的 AWS Config 規則資訊，請參閱 Trusted Advisor Trusted Remediator 支援的檢查。

信任的修復程式會將哪些資源部署到您的帳戶？

Trusted Remediator 會在 Trusted Remediator 委派管理員帳戶中部署下列資源：

- 名為 的 Amazon S3 儲存貯體`ams-trusted-remediator-{your-account-id}-logs`。建立修復 OpsItem 時，信任的修復程式會以 `Remediation item log` JSON 格式建立 ，並將日誌檔案上傳至此儲存貯體。
- 保留支援 Trusted Advisor 檢查和 Compute Optimizer 建議的修復組態 AWS AppConfig 的應用程式。

Trusted Remediator 不會在 Trusted Remediator 成員帳戶中部署資源。

AMS Accelerate 中 Amazon EKS 的監控和事件管理

Amazon EKS 的監控和事件管理會監控您的 Amazon EKS 資源是否有故障、效能降低和安全問題。AMS Accelerate 會設定和部署 Amazon Managed Service for Prometheus 警示管理員規則、監控警示，然後在觸發這些警示時執行事件管理。Amazon EKS 的監控和事件管理依賴 AMS 警示管理員，並利用原生 AWS 服務，例如 Amazon Managed Service for Prometheus、Amazon Managed Grafana、Amazon GuardDuty、 AWS Lambda和 AWS Config。

> **Note**
>
> Amazon EKS 的監控和事件管理不支援 AWS GovCloud (US) Windows 節點或 Windows 容器。

什麼是 AMS Accelerate 中 Amazon EKS 的監控和事件管理？

Amazon EKS 的監控和事件管理提供下列項目：

- 一種預設組態，可針對您選取的 Amazon EKS 叢集，在您的受管帳戶中建立、管理和部署監視器和政策。
- 監控基準，可讓您的 Amazon EKS 工作負載具有更高的可用性，即使您未為 Amazon EKS 叢集設定任何其他監控。如需詳細資訊，請參閱AMS Accelerate 中 Amazon EKS 監控和事件管理的基準警示。
- 為您的 Amazon EKS 叢集設定的基準監控所產生的通知。這些通知稱為提醒。當有即將發生、持續發生、下降或潛在故障、效能降低或安全問題時，就會產生警示。提醒的範例包括 Prometheus 提醒、事件或來自 AWS 服務的問題清單，例如 Amazon GuardDuty。
- 警示調查，並指導您可以採取的適當修補動作。如需詳細資訊，請參閱 AMS Accelerate 中的事件報告和服務請求。
- 盡可能修復 AMS 操作的警示和事件並取得您的核准，以防止或減少對應用程式的影響。如需詳細資訊，請參閱 AMS Accelerate 中的事件報告和服務請求。
- 選用的預先定義 Amazon Managed Grafana 儀表板，可讓您查看資源使用率、效能、CoreDNS 的運作狀態、作用中提醒和先前已解決的提醒。如果您使用 AMS 提供的範本設定 Amazon Managed Grafana，則可以開啟 Amazon Managed Grafana 主控台來檢視 Amazon EKS 叢集的指標和提醒。

Amazon EKS 的監控和事件管理如何在 AMS Accelerate 中運作

產生：作為 EKS 加入監控和事件管理的一部分，AMS 會為您在受管帳戶中選取的 Amazon EKS 叢集設定基準監控。AMS 使用 Amazon Managed Service for Prometheus 警示管理員規則和 Amazon CloudWatch 事件規則的組合來設定基準監控。叢集中的 AMS 設定 Prometheus 伺服器會抓取您的 Prometheus 指標並將其遠端寫入相同區域中的 Amazon Managed Service for Prometheus 端點。觸發 Prometheus 警示管理員規則或產生 CloudWatch 事件時，基準監控組態會產生警示。

彙總：AMS 透過將資源導向 AMS 管理的 Amazon Simple Notification Service 主題，將資源產生的所有提醒傳送至 AMS 監控系統。

處理和影響分析：AMS 會分析警示，然後根據其影響的可能性進行處理。AMS 會將警示分類如下：

- 具有已知客戶影響的提醒：對於這些提醒，AMS 會使用事件管理程序建立新的事件報告。
- 具有不確定客戶影響的提醒：對於這些提醒，AMS 會傳送事件報告。在許多情況下，這些提醒會要求您驗證影響，AMS 才能採取行動。對於此類提醒，AMS 會傳送包含詳細資訊的提醒通知，並檢查提醒是否需要緩解動作。AMS 提供在通知中緩解動作的選項。如果您的回覆確認警示是事件，則 AMS 會觸發建立新事件報告，並啟動事件管理程序。收到「無客戶影響」或三天內完全沒有回應的任何服務通知都會標記為已解決。此外，對應的提醒會標示為已解析。
- 沒有客戶影響的提醒：如果在評估之後，AMS 判斷提醒沒有任何客戶影響，則提醒會關閉。

AMS 責任矩陣 (RACI)

AMS 負責、負責、諮詢和告知，或 RACI 矩陣會將主要責任指派給客戶或 AMS 以進行各種活動。下表概述了客戶和 AMS 在使用 Amazon EKS 監控和事件管理的應用程式中活動的責任。

- R 代表負責執行任務以達成任務的一方。
- 代表責任方。
- C 代表已諮詢的對象；尋求意見的對象，通常是主題專家；以及與之進行雙邊溝通的對象。
- 我代表知情；收到進度通知的一方，通常只在完成任務或可交付項目時。

活動	客戶	AMS
探索 AMS 需求	I	R

活動	客戶	AMS
啟用叢集存取的 AMS 許可 (RBAC)	R	C
如果工作者節點尚未存在，請在其上安裝 Amazon EC2 Systems Manager Agent	R	C
視需要在 AMS 命名空間中部署 AMS 叢集上元件，例如 Prometheus、Prometheus Node Exporter 和 kube-state-metrics。	C	R
在 AMS 控制平面中佈建 Amazon Managed Service for Prometheus	I	R
在 AMS 控制平面中設定 Prometheus 警示管理員	I	R
提供 Amazon Managed Grafana 範本並協助設定	C	R
啟用 GuardDuty EKS 稽核日誌監控	C	R
啟用 Amazon EKS 控制平面記錄	I	R
監控 Amazon EKS 控制平面的運作狀態和效能	I	R
監控 Amazon EKS 叢集（叢集、節點、工作負載、Pod、API Server 和 CoreDNS) 的運作狀態和效能	I	R

活動	客戶	AMS
分類警示並提供 Amazon EKS 的事件回應	I	R
在事件期間執行診斷命令	I	R
在事件期間分析日誌 （控制平面和 Pod 日誌）	I	R
AWS 網路問題的事件回應	I	R
回應 GuardDuty EKS 稽核日誌監控問題清單	I	R
針對盡可能修復事件的動作提供客戶指引	I	R

AMS Accelerate 中 Amazon EKS 監控和事件管理的基準警示

驗證警示後，AMS 會為 Amazon EKS 啟用下列警示，然後為您選取的 Amazon EKS 叢集進行監控和事件管理。服務水準協議 (SLAs) 和服務水準目標 (SLOs回應時間取決於您選擇的帳戶服務層 (Plus、Premium)。如需詳細資訊，請參閱 AMS Accelerate 中的事件報告和服務請求。

提醒和動作

下表列出 AMS 採取的 Amazon EKS 警示和個別動作：

警示	閾值	動作
容器 OOM 已終止	過去 10 分鐘內重新啟動的容器總數至少為 1，且 Pod 中的 Kubernetes 容器已在過去 10 分鐘內因「OOMKilled」而終止。	AMS 會調查 OOM 刪除是否因為達到容器限制或記憶體超額遞交而導致，然後建議您採取修正動作。

警示	閾值	動作
Pod 任務失敗	Kubernetes 任務無法完成。失敗是透過至少有一個失敗的任務狀態來表示。	AMS 會調查 Kubernetes 任務或對應 Cron 任務失敗的原因，然後為您提供修正動作的建議。
StatefulSet Down	準備好提供流量的複本數量，與每個 StatefulSet 的現有複本目前數量不符至少 1 分鐘。	AMS 透過檢閱 Pod 事件中的錯誤訊息和 Pod 日誌中的錯誤日誌程式碼片段，判斷 Pod 為何未就緒，然後建議您採取修正動作。
HPA 擴展功能	由於狀態條件「AbleToScale」至少 2 分鐘為 false，Horizontal Pod Autoscaler (HPA) 無法擴展。	AMS 會判斷哪些 Kubernetes Horizontal Pod Autoscaler (HPA) 無法為其後續工作負載資源擴展 Pod，例如部署或 StatefulSet。
HPA 指標可用性	由於狀態條件「ScalingActive」至少 2 分鐘為 false，Horizontal Pod Autoscaler (HPA) 無法收集指標。	AMS 會判斷 HPA 為何無法收集指標，例如與伺服器組態問題或 RBAC 授權問題相關的指標。
Pod 未就緒	Kubernetes Pod 會維持在非執行中狀態（例如待定、未知或失敗）超過 15 分鐘。	AMS 會調查受影響的 Pod (s) 以取得詳細資訊、檢閱 Pod 日誌是否有相關的錯誤和事件，然後為您提供修正動作的建議。
Pod 損毀迴圈	在 1 小時期間內，Pod 容器至少每 15 分鐘重新啟動一次。	AMS 會調查 Pod 未啟動的原因，例如資源不足、另一個容器鎖定的檔案、另一個容器鎖定的資料庫、服務相依性失敗、外部服務的 DNS 問題，以及設定錯誤。

警示	閾值	動作
Daemonset 排程錯誤	至少有一個 Kubernetes Daemonset Pod 在 10 分鐘內排程錯誤。	AMS 會判斷為什麼 Daemonset 排程在節點上，而節點不應該執行。當將錯誤的 Pod nodeSelector/taints/affinities 套用到 Daemonset Pod 或節點（節點集區）上色且未排定要移出的現有 Pod 時，可能會發生這種情況。
Kubernetes API 錯誤	Kubernetes API 伺服器錯誤率在 2 分鐘內超過 3%。	AMS 會分析控制平面日誌，以判斷造成此警示的錯誤數量和類型，並識別主節點或等自動擴展群組的任何資源爭用問題。如果 API 伺服器未復原，AMS 會與 Amazon EKS 服務團隊互動。
Kubernetes API 延遲	對 Kubernetes API 伺服器提出請求的第 99 個百分位數延遲在 2 分鐘內超過 1 秒。	AMS 會分析控制平面日誌，以判斷導致延遲的錯誤數量和類型，並識別主節點或等自動擴展群組的任何資源爭用問題。如果 API 伺服器未復原，AMS 會與 Amazon EKS 服務團隊互動。
Kubernetes 用戶端憑證即將到期	用於向 Kubernetes API 伺服器進行身分驗證的用戶端憑證將在 24 小時內過期。	AMS 會傳送此通知，通知您叢集憑證將在 24 小時內過期。
節點未就緒	節點「就緒」條件狀態至少為 false 10 分鐘。	AMS 會調查節點條件和事件，例如網路問題，以防止 kubelet 存取 API 伺服器。

警示	閾值	動作
節點高 CPU	CPU 負載在 5 分鐘內超過 80%。	AMS 會判斷一或多個 Pod 是否使用異常大量的 CPU。然後，AMS 會與您確認請求、限制和 Pod 活動是否如預期。
偵測到節點 OOM 刪除	在 4 分鐘的時段內，節點至少會報告一個主機 OOM 刪除。	AMS 會判斷 OOM 終止是否因為達到容器限制或節點過度遞交而導致。如果應用程式活動正常，AMS 會建議您提出超額承諾和修訂 Pod 限制的請求和限制。
節點連線限制	在 5 分鐘內，目前連線追蹤項目數量與上限的比率超過 80%。	AMS 建議您了解每個核心的建議連線值。Kubernetes 節點會設定與節點的總記憶體容量成比例的 conntrack 最大值。高負載應用程式，特別是在較小的節點上，可以輕鬆超過連接最大值，導致連線重設和逾時。
節點時鐘未同步	2 分鐘期間的最小同步狀態為 0，以秒為單位的最大錯誤為 16 或更高。	AMS 會判斷網路時間通訊協定 (NTP) 是否已安裝並正常運作。
Pod 高 CPU	容器的 CPU 用量在 3 分鐘的速率內超過 80%，持續至少 2 分鐘。	AMS 會調查 Pod 日誌，以判斷耗用大量 CPU 的 Pod 任務。
Pod 高記憶體	在 2 分鐘內，容器的記憶體用量超過其指定記憶體限制的 80%。	AMS 會調查 Pod 日誌，以判斷耗用大量記憶體的 Pod 任務。

警示	閾值	動作
CoreDNS 關閉	CoreDNS 已從 Prometheus 目標探索消失超過 15 分鐘。	這是一個重要提醒，指出內部或外部叢集服務的網域名稱解析已停止。AMS 會檢查 CoreDNS Pod 的狀態、驗證 CoreDNS 組態、驗證指向 CoreDNS Pod 的 DNS 端點、驗證 CoreDNS 限制，並在您的核准下啟用 CoreDNS 除錯記錄。
CoreDNS 錯誤	CoreDNS 會在 10 分鐘內傳回超過 3% DNS 請求的 SERVFAIL 錯誤。	此提醒可能表示應用程式發生問題或組態錯誤。AMS 會檢查 CoreDNS Pod 的狀態、驗證 CoreDNS 組態、驗證指向 CoreDNS Pod 的 DNS 端點、驗證 CoreDNS 限制，並在您的核准下啟用 CoreDNS 除錯記錄。
CoreDNS 延遲	DNS 請求持續時間的第 99 個百分位數超過 4 秒，持續 10 分鐘。	此提醒 表示 CoreDNS 可能超載。AMS 會檢查 CoreDNS Pod 的狀態、驗證 CoreDNS 組態、驗證指向 CoreDNS Pod 的 DNS 端點、驗證 CoreDNS 限制，並在您的核准下啟用 CoreDNS 除錯記錄。

警示	閾值	動作
CoreDNS 轉送延遲	CoreDNS 轉送請求至 kube-dns 的回應時間第 99 個百分位數，在 10 分鐘的期間內超過 4 秒。	當 CoreDNS 不是授權伺服器或沒有 Domanin 名稱的快取項目時，CoreDNS 會將 DNS 請求轉送到上游 DNS 伺服器。此提醒表示 CoreDNS 可能過載，或上游 DNS 伺服器可能有問題。AMS 會檢查 CoreDNS Pod 的狀態、驗證 CoreDNS 組態、驗證指向 CoreDNS Pod 的 DNS 端點、驗證 CoreDNS 限制，並在您的核准下啟用 CoreDNS 除錯記錄。
CoreDNS 轉送錯誤	超過 3% 的 DNS 查詢在 5 分鐘內失敗。	當 CoreDNS 不是授權伺服器或沒有 Domanin 名稱的快取項目時，CoreDNS 會將 DNS 請求轉送到上游 DNS 伺服器。此提醒會向上游 DNS 伺服器發出可能組態錯誤或問題訊號。AMS 會檢查 CoreDNS Pod 的狀態、驗證 CoreDNS 組態、驗證指向 CoreDNS Pod 的 DNS 端點、驗證 CoreDNS 限制，並在您的核准下啟用 CoreDNS 除錯記錄。

AMS Accelerate 中 Amazon EKS 監控和事件管理的需求

這些是 Amazon EKS for AMS Accelerate 監控和事件管理的支援和/或必要資源

- 支援的 Kubernetes 版本：請參閱《Amazon EKS 使用者指南》中的 Amazon EKS Kubernetes 版本。
- 節點類型：支援 Amazon EKS 受管節點。不支援 Windows 節點和容器。
- Kubernetes 叢集存取：AMS 需要 system：masters RBAC 叢集角色和叢集使用者。

- Amazon EC2 節點上的 SSM 代理程式： Bottle Rocket 和 Amazon EKS AMIs 都已預先安裝 SSM 代理程式。請確定您的自訂 AMIs 和 Amazon EC2 節點上安裝 SSM Agent。
- Service Quotas 如需詳細資訊，請參閱 Amazon Managed Service for Prometheus 和 Amazon Managed Grafana 的服務配額。
- 支援 AWS 的區域：

區域名稱	Region	指標儲存區域
美國東部 (俄亥俄)	us-east-2	us-east-2
美國東部 (維吉尼亞北部)	us-east-1	us-east-1
美國西部 (奧勒岡)	us-west-2	us-west-2
亞太區域 (東京)	ap-northeast-1	ap-northeast-1
亞太區域 (首爾)	ap-northeast-2	ap-northeast-2
亞太區域 (新加坡)	ap-southeast-1	ap-southeast-1
亞太區域 (雪梨)	ap-southeast-2	ap-southeast-2
歐洲 (法蘭克福)	eu-central-1	eu-central-1
歐洲 (愛爾蘭)	eu-west-1	eu-west-1
歐洲 (倫敦)	eu-west-2	eu-west-2
Africa (Cape Town)	af-south-1	eu-west-1 eu-west-2
亞太區域 (香港)	ap-east-1	ap-northeast-1 ap-northeast-2

> **Note**
>
> af-south-1、非洲（開普敦）和 ap-east-1、亞太區域（香港）中 Amazon EKS 叢集的指標 AWS 區域分別匯出至相同 中的 AMS 監控服務。然後，這些指標 AWS 區域 會在 AMS 監控服務中傳輸到處理和儲存它們的不同區域。如需 AMS 監控服務用來存放指標的區域，請參閱上表。

在 AMS Accelerate 中加入 Amazon EKS 的監控和事件管理

執行下列步驟以加入 Amazon EKS 的監控和事件管理。

1. 啟用 Amazon EKS 成本最佳化標籤：請參閱《Amazon EKS 使用者指南》中的標記您的資源以進行計費。
2. 開始加入 EKS 的監控和事件管理：請聯絡您的 Cloud Service Delivery Manager (CSDM)，其中包含要加入的帳戶 IDs和叢集名稱。
3. 驗證需求：您的雲端架構師 (CA) 會在加入開始之前驗證是否符合所有需求。
4. 更新 Kubernetes 角色型存取控制 (RBAC)：AMS 會共用`eksctl`命令以實作這些變更。您可以檢閱這些變更，然後部署。您必須部署 RBAC 更新，讓 AMS 具有代表您執行命令的許可。這些更新包括將 AMS IAM 角色映射至 Kubernetes 使用者、為 AMS 建立新的 Kubernetes 叢集角色，以及將 AMS Kubernetes 叢集角色繫結至使用者。
5. 部署叢集元件：AMS 會在叢集上的 AMS 受管命名空間中部署下列元件：
   - Prometheus 伺服器
   - Prometheus 節點匯出工具（不適用於 AWS Fargate)
   - kube-state-metrics
6. 執行 Prometheus 組態更新：AMS 設定 Prometheus 為指標啟用遠端寫入。
7. （選用）設定儀表板：您的 CA 可協助您在帳戶中設定 Amazon Managed Grafana 儀表板。

> **Note**
>
> 加入 Amazon EKS 叢集之後，AMS 會分析警示訊號並執行基準評估，以識別叢集中現有的問題。基準評估完成後，AMS 會透過 Trusted Advisor 分享問題清單和修復建議，以及可用來解決叢集問題的服務請求。從評估中，AMS 會調整我們的帳戶層級警示閾值，以建立 EKS 叢集

專屬的 Amazon EKS 監控基準。為了消除這些調查結果的重複 AMS 回應，我們調整監控以排除這些警示訊號。我們會重新調整監控，以在 CSDM 通知我們基礎問題已修復時包含訊號。

AMS Accelerate 中的 Amazon EKS 監控和事件管理離線

使用帳戶 IDs和叢集名稱通知雲端服務交付管理員 (CSDM)，以開始離職程序。在您離職後，系統會暫停警示處理、指標儲存和指標查詢，並根據預設的 Amazon Managed Service for Prometheus 資料保留政策刪除指標。

AMS 會執行下列離職步驟：

1. AMS 會停用傳送給您和 AMS Operations 的提醒。
2. AMS 會從 Amazon EKS 叢集中移除 Prometheus 執行個體。
3. AMS 會移除您帳戶中安裝的其他 AWS 資源，例如 IAM 角色和 AWS Config 規則。

完成這些步驟後，您必須完成下列離職步驟：

1. 使用 從 `eksctl`移除 Kubernetes RBAC `aws-auth` 許可`ConfigMap`。
2. 如果您先前已安裝，請移除您設定為連線至 AMS 的 Amazon Managed Grafana 執行個體。

AMS Accelerate 中的持續性管理

AMS 利用 AWS Backup 來集中和自動化跨 AWS 服務備份您的資料。AMS 備份計畫提供各種使用案例的最佳實務；不過，歡迎您繼續使用現有的備份計畫。加入 AMS 備份管理後，AMS 會提供備份報告，而 AMS 專家會持續監控您的備份任務，以確保您擁有可靠的備份解決方案。

若要進一步了解，請參閱 AWS Backup：運作方式和支援 AWS 的資源和第三方應用程式。

AMS Accelerate 提供各種營運服務，協助您實現卓越營運 AWS。若要快速了解 AMS 如何 AWS 雲端透過我們的一些關鍵營運功能，包括全年無休服務台、主動監控、安全性、修補、記錄和備份，協助您的團隊在 中實現整體卓越營運，請參閱 AMS 參考架構圖表。

觀看 Carl 的影片以進一步了解 (9：29)

主題

持續性管理如何在 AMS 中運作

AMS 備份計畫會定義資料備份的頻率，以及備份的保留政策。AMS 備份保存庫可整理您的備份資料。一旦資源與備份計劃相關聯，相容的資源就會遞增備份。第一個備份是完整副本，後續備份會擷取增量變更。根據選取的資源和 AMS 備份計畫，Point-in-time(PITR) 可讓您透過選取復原時間來倒轉資源。若要開始使用 AMS Backup Management，只需選取 AMS 備份計劃並標記您的 資源。

> **Note**
>
> 請依照此處的步驟：入門 1：服務選擇加入 AWS 區域，確保已為每個帳戶 AWS Backup 啟用和資源類型。
> 您不需要繼續入門 2：在隨需備份上建立。

的相關主題來自 AWS Backup

- 使用備份（建立、編輯、複製、還原、刪除）
- 建立隨需備份
- 跨 建立備份複本 AWS 區域
- AWS Backup 支援的服務
- Point-in-time還原
- AWS Backup 功能

選取 AMS 備份計畫

AMS 提供三種不同的備份計畫與第四個備份計畫，以盡可能降低加入期間的成本。若要為每個支援的資源選取 AMS 備份計劃，請使用計劃的關聯標籤來標記資源。當您加入 Accelerate 時，AMS 將與您合作，找出最符合您需求的備份計畫。

> **Important**
>
> 請勿編輯您的 AMS 預設備份計劃，因為變更可能會遺失。反之，請為您的自訂組態建立新的計劃。如需詳細資訊，請參閱建立備份計劃。

預設 AMS 備份計畫

AWS Backup 此備份計畫未啟用連續備份；如需詳細資訊，請參閱使用point-in-time。

TAG 金鑰： `ams:rt:backup-orchestrator`

TAG 值： `true`

預設 AMS 備份計畫	開始時間	Retention
hourly backup	N/A	N/A
daily backup	daily 4:00 UTC	7 days
weekly backup	Saturday, 2:00 UTC	4 weeks
monthly backup	1st of the month, 2:00 UTC	26 weeks

預設 AMS 備份計畫	開始時間	Retention
yearly backup	Jan 1st, 2:00 UTC	2 years

增強型備份計劃

AWS Backup 連續備份會在支援的資源上以最大保留期 (31 天） 啟用；如需詳細資訊，請參閱使用point-in-time還原 (PITR) 還原至指定時間，以及用於point-in-time(PITR) 的支援服務和應用程式。

TAG 金鑰： `ams:rt:backup-orchestrator-enhanced`

TAG 值： `true`

增強型備份計劃	開始時間	Retention
hourly backup	N/A	N/A
daily backup	daily 4:00 UTC	31 天
weekly backup	Saturday, 2:00 UTC	6 週
monthly backup	1st of the month, 2:00 UTC	26 weeks
yearly backup	Jan 1st, 2:00 UTC	2 years

資料敏感備份計畫

AWS Backup 連續備份會在支援的資源上啟用最大保留期 (31 天）；如需詳細資訊，請參閱使用point-in-time還原 (PITR) 還原至指定的時間，以及point-in-time還原 (PITR) 的支援服務和應用程式。

TAG 金鑰： `ams:rt:backup-orchestrator-data-sensitive`

TAG 值： `true`

資料敏感備份計畫	開始時間	Retention
hourly backup	every hour	7 天
daily backup	daily 4:00 UTC	31 天

資料敏感備份計畫	開始時間	Retention
weekly backup	Saturday, 2:00 UTC	6 週
monthly backup	1st of the month, 2:00 UTC	26 weeks
yearly backup	Jan 1st, 2:00 UTC	2 years

AMS Accelerate 入門備份計劃

AWS Backup 此備份計劃未啟用連續備份；如需詳細資訊，請參閱使用point-in-time。

TAG 金鑰： `ams:rt:backup-orchestrator-onboarding`

TAG 值： `true`

AMS Accelerate 入門備份計劃	開始時間	Retention
hourly backup	every hour	2 週
daily backup	N/A	N/A
weekly backup	N/A	N/A
monthly backup	N/A	N/A
yearly backup	N/A	N/A

相關 AWS Backup 主題

- 建立備份計劃
- Point-in-time(PITR) 可連續備份支援的資源，並可讓您選取復原的特定時間。如需支援的資源清單，請參閱依資源的功能可用性。

標記您的 資源以套用 AMS 備份計劃

若要將資源指派給 AMS 備份計劃，請使用計劃的標籤鍵/值對來標記資源。您可以使用 AMS Resource Tagger 將 AMS 備份計劃套用至您資源的子集或帳戶中所有支援的資源。如果您想要使用替代方法將

標籤套用至資源，例如 AWS CloudFormation 或 Terraform，請關閉 Resource Tagger，使其不會與您選擇的標記方法競爭。如需詳細資訊，請參閱防止 Resource Tagger 修改資源。

下列範例示範如何使用 Resource Tagger 在帳戶中的 Amazon Elastic Compute Cloud 執行個體上套用預設 AMS 備份計劃。對於此備份計畫，請套用標籤索引鍵 `ams:rt:backup-orchestrator` 和值 `true`。若要使用不同的備份計劃，請變更 金鑰以符合所需的備份計劃的標籤金鑰。若要了解 AMS Resource Tagger 並了解如何將下列參考的設定檔與 Accelerate 帳戶中的目前 （已設定） 設定檔整合，請參閱 加速資源交錯。

1. 在 https：//https://console.aws.amazon.com/systems-manager/appconfig 開啟 AWS AppConfig 主控台。
2. 選擇 ResourceTagger 應用程式。
3. 選擇組態設定檔索引標籤，然後選擇 CustomerManagedTags
4. 選擇建立以建立新的版本。
5. 選擇 JSON，然後複製並貼上下列 JSON 物件：

```
{
    "AWS::EC2::Instance": {
        "AccelerateBackupPlan": {
            "Enabled": true,
            "Filter": {
                "Fn::AND": [
                    {
                        "Platform": "*"
                    }
                ]
            },
            "Tags": [
                {
                    "Key": "ams:rt:backup-orchestrator",
                    "Value": "true"
                }
            ]
        }
    }
}
```

6. 選擇建立託管組態版本。
7. 選擇 Start deployment (啟動部署)。
8. 定義下列部署詳細資訊：

```
Environment: AMSInfrastructure
Hosted configuration version: Select the version that you have just created.
Deployment Strategy: AMSNoBakeDeployment
```

9. 選擇 Start deployment (啟動部署)。Resource Tagger 會標記您的執行個體 `ams:rt:backup-orchestrator: true`，確保您的執行個體根據預設 AMS 備份計畫進行備份。

檢視 AMS 保存庫中的備份

您可以使用標籤，在個別保存庫層級控制備份保存庫通知。您可以新增 標籤，`AMSNotificationOptOut`並將 值設定為特定保存庫`True`上的 ，以選擇不接收特定保存庫的通知。若要繼續從保存庫取得通知，請移除 標籤。

若要檢視 AMS 備份的清單，請開啟 AWS Backup 主控台。在導覽窗格中，選擇備份保存庫，然後從下表中選取其中一個 AMS 備份保存庫。在備份區段中，檢視備份文件庫中所有備份的清單。選取要編輯、刪除或還原的備份。

AMS 備份計劃的保存庫

AMS 保存庫名稱	AMS 備份計畫標籤金鑰
ams-automated-backups	ams:rt:backup-orchestrator
ams-automated-enhanced-backups	ams:rt:backup-orchestrator-enhanced
ams-automated-data-sensitive-backups	ams:rt:backup-orchestrator-data-sensitive
ams-onboarding-backups	ams:rt:backup-orchestrator-onboarding

其他 AMS 保存庫

AMS 保存庫名稱	描述
ams-manual-backups	This vault contains manually started backups created by the `AWSManagedServices-StartBackupJob` SSM Automation

AMS 保存庫名稱	描述
	document and pre-patch backups created by AMS patch automations before patching.
ams-custom-backups	This is the recommended vault for backups created outside of AMS backup plans.

相關 AWS Backup 主題

- 依資源檢視備份
- 使用備份

AMS 備份監控和報告

> **Important**
>
> AMS 備份監控和報告僅適用於 AMS 支援的 區域。這些是美國東部（維吉尼亞）、美國西部（加利佛尼亞北部）、美國西部（奧勒岡）、美國東部（俄亥俄）、加拿大（中部）、南美洲（聖保羅）、歐洲（愛爾蘭）、歐洲（法蘭克福）、歐洲（倫敦）、歐洲（巴黎）、亞太區域（孟買）、亞太區域（首爾）、亞太區域（新加坡）、亞太區域（雪梨）、亞太區域（東京）。

AMS 會產生每日自助式報告，以及資源涵蓋範圍和備份任務狀態的每月報告。每月報告會在每月商業審核 (MBRs) 中共用。若要進一步了解每日備份報告，請參閱每日備份報告

AMS 專家會監控您使用 設定的所有備份任務 AWS Backup。如果發生備份失敗，AMS 會調查失敗情況，並在可行時通知您根本原因和修復選項。為了避免警示雜訊，在導致帳戶中發生大量備份失敗的事件期間，AMS 會透過 CSDM 提出集體建議，而不是針對每個個別失敗通知您。

請注意，AMS 不會監控使用 AWS 服務的獨立備份功能設定的任何備份。

了解 AMS Accelerate 中的修補程式管理

Important

加速修補程式報告會定期部署以 AWS Glue 資源為基礎的政策。請注意，修補系統的 AMS 更新會覆寫現有的 AWS Glue 資源型政策。

Important

您可以為受管節點指定替代修補程式儲存庫。當 AMS 實作您請求的修補程式組態時，您需負責選取和驗證所選儲存庫的安全性。您也必須接受使用這些儲存庫的任何風險，例如供應鏈風險。

以下是修補程式管理程序安全的最佳實務：

- 僅使用受信任且經過驗證的儲存庫來源
- 盡可能預設為標準作業系統廠商儲存庫
- 定期稽核自訂儲存庫組態

您可以使用 AMS Accelerate 修補系統修補程式附加元件，透過安全相關和其他類型的更新來修補您的執行個體。Accelerate Patch Add-On 是一項功能，可為 AMS 執行個體提供標籤型修補。它利用 AWS Systems Manager (SSM) 功能，因此您可以標記執行個體，並使用您設定的基準和視窗修補這些執行個體。AMS Accelerate Patch 附加元件是一種加入選項，如果您在加入 Accelerate 帳戶期間未取得，請聯絡您的雲端服務交付經理 (CSDM) 以取得。

AMS Accelerate 修補程式管理使用 Systems Manager 修補程式基準功能來控制套用至執行個體的修補程式定義。修補程式基準包含預先核准的修補程式清單；例如，所有安全修補程式。根據與其相關聯的修補程式基準來衡量執行個體的合規性。AMS Accelerate 預設會安裝所有可用的修補程式，讓執行個體保持最新狀態。

Note

AMS Accelerate 僅適用於作業系統 (OS) 修補程式。例如，對於 Windows，只會套用 Windows 更新，而非 Microsoft 更新。

如需報告的資訊，請參閱 AMS 主機管理報告。

AMS Accelerate 提供各種營運服務，協助您實現卓越營運 AWS。若要快速了解 AMS 如何 AWS 雲端透過我們的一些關鍵營運功能，包括全年無休服務台、主動監控、安全性、修補、記錄和備份，協助您的團隊在 中實現整體卓越營運，請參閱 AMS 參考架構圖表。

主題

修補建議

如果您參與應用程式或基礎設施操作，您會了解作業系統 (OS) 修補解決方案的重要性，其彈性和可擴展性足以滿足您的應用程式團隊的各種需求。在典型組織中，某些應用程式團隊使用涉及不可變執行個體的架構，而其他則將其應用程式部署在可變執行個體上。

如需修補 AWS 規範指引的詳細資訊，請參閱使用 的混合雲端中可變執行個體的自動修補 AWS Systems Manager。

> **Note**
>
> Accelerate Patch Add-On 是一項功能，可為 AMS 執行個體提供標籤型修補。它利用 AWS Systems Manager (SSM) 功能，因此您可以標記執行個體，並使用您設定的基準和視窗修補這些執行個體。AMS Accelerate Patch 附加元件是一種加入選項，如果您在加入 Accelerate 帳戶期間未取得，請聯絡您的雲端服務交付經理 (CSDM) 以取得。

修補程式責任建議

持久性執行個體的修補程序應涉及下列團隊和動作：

- 應用程式 (DevOps) 團隊會根據應用程式環境、作業系統類型或其他條件，為其伺服器定義修補程式群組。它們也會定義每個修補程式群組特定的維護時段。此資訊應存放在連接到執行個體的標籤上。

建議的標籤名稱為「修補程式群組」和「維護時段」。在每個修補週期期間，應用程式團隊會準備修補、在修補後測試應用程式，以及在修補期間疑難排解其應用程式和作業系統的任何問題。

- 安全操作團隊會定義應用程式團隊使用的各種作業系統類型的修補程式基準，並透過 Systems Manager Patch Manager 提供修補程式。
- 自動化修補解決方案會定期執行，並根據使用者定義的修補程式群組和維護時段，部署修補程式基準中定義的修補程式。
- 控管和合規團隊會定義修補準則和例外狀況程序與機制。

如需詳細資訊，請參閱針對可變 EC2 執行個體的修補解決方案設計。

應用程式團隊的指引

- 檢閱並熟悉建立和管理維護時段；請參閱AWS Systems Manager 維護時段和建立 SSM 維護時段以進行修補以進一步了解。了解一般結構和維護時段的使用可協助您了解，如果您不是建立資訊的人員，應提供哪些資訊。
- 對於高可用性 (HA) 設定，計劃在每個可用區域和每個環境 (Dev/Test/Prod) 有一個維護時段。這可確保修補期間的持續可用性。
- 建議的維護時段持續時間為 4 小時，間隔 1 小時，加上每 50 個執行個體額外 1 小時
- 具有足夠時間的修補程式開發和測試版本，可讓您在生產修補之前識別任何潛在問題。
- 透過 SSM 自動化自動化常見的修補前和修補後任務，並將其做為維護時段任務執行。請注意，對於修補後任務，您必須確保配置足夠的時間，因為一旦達到截止值，任務就不會啟動。
- 熟悉修補程式基準及其功能 - 特別是修補程式嚴重性類型的自動核准延遲，這些嚴重性類型可用於確保只有在開發/測試中套用的修補程式才能在日後的生產中套用。如需詳細資訊，請參閱關於修補程式基準。

安全營運團隊的指引

- 檢閱並熟悉修補程式基準。修補程式核准會以自動化方式處理，並具有不同的規則選項。如需詳細資訊，請參閱關於修補程式基準。
- 與應用程式團隊討論修補 Dev/Test/Prod 的需求，並開發多個基準以滿足這些需求。

控管和合規團隊的指引

- 修補應該是「選擇退出」函數。預設維護時段和自動標記應該存在，以確保沒有未修補的內容。AMS Resource Tagger 可以提供這項協助；請與您的雲端架構師 (CA) 或雲端服務交付管理員 (CSDM) 討論此選項，以取得實作指引。
- 請求豁免修補應該需要文件證明豁免。資訊安全長 (CISO) 或其他核准主管應核准或拒絕請求。
- 修補合規應透過修補程式管理員主控台、Security Hub 或漏洞掃描器定期審查。

高可用性 Windows 應用程式的範例設計

概觀：

- 每個可用區域一個維護時段。
- 每個環境一組維護時段。
- 每個環境一個修補程式基準：
  - 開發：核准 0 天後的所有嚴重性和分類。
  - 測試：在 0 天後核准關鍵安全性更新修補程式，並在 7 天後核准所有其他嚴重性和分類。
  - 生產：在 0 天後核准關鍵安全性更新修補程式，並在 14 天後核准所有其他嚴重性和分類。

CloudFormation 指令碼：

這些指令碼的設定是使用上述基準核准設定，為兩個可用區域 Windows HA EC2 應用程式建置維護時段、基準和修補任務。

- Windows 開發 CFN 堆疊範例：HA-Patching-Dev-Stack.json
- Windows 測試 CFN 堆疊範例：HA-Patching-Test-Stack.json
- Windows 產品 CFN 堆疊範例：HA-Patching-Prod-Stack.json

修補程式建議FAQs

問：如何處理「0」日攻擊的未排程修補？

答：SSM 支援立即修補功能，該功能使用執行個體作業系統的目前預設基準。AMS 部署一組預設的修補程式基準，在 0 天後核准所有修補程式。不過，使用立即修補功能時，不會擷取預先修補快照，因為此命令會執行 AWS-RunPatchBaseline SSM 文件。我們建議您在修補之前手動備份。

問：AMS 是否支援自動擴展群組 (ASGs) 中執行個體的修補？

答：否。加速客戶目前不支援 ASG 修補。

問：維護 Windows 是否有任何需要記住的限制？

答：是，您應該注意一些限制。

- 每個帳戶的維護時段：50
- 每個維護時段的任務數：20
- 每個維護時段的並行自動化數目上限：20
- 並行維護時段數目上限：5

如需預設 SSM 限制的完整清單，請參閱AWS Systems Manager 端點和配額。

在 AMS 中建立修補程式維護時段

修補程式維護時段會根據目標 Amazon EC2 執行個體的設定排程執行 AMS 修補程式自動化。目標由一組執行個體的標籤或標籤定義。您可以根據修補程式星期二前後的日期和時間來設定排程，也可以使用 Cron 表達式定義排程。如需詳細資訊，請參閱AWS Systems Manager 《 使用者指南》中的參考：Systems Manager 的 Cron 和 Rate 表達式。在修補之前，AMS 會建立每個執行個體根磁碟區的快照。如果 AMS 偵測到修補會影響執行個體的運作狀態，或者如果您通知 AMS 修補的應用程式影響，則 AMS 會使用此快照將根磁碟區還原為預先修補狀態。

AMS Accelerate 修補程式維護時段限制

AMS 修補 use AWS Systems Manager (Systems Manager)。除了 Systems Manager 服務限制之外，AMS 修補在每個修補程式維護時段都有 300 個目標執行個體的限制。假設每個執行個體的一般修補程式完成時間為 30 分鐘，下表提供維護時段和持續時間數量的範例。

要修補的執行個體	維護時段持續時間 （小時）	需要並行維護時段
100	1	1

要修補的執行個體	維護時段持續時間（小時）	需要並行維護時段
200	1	1
300	2	1
600	3	2
800	4	3
1200	6	4
1500	8	5

> **Important**
>
> 這些範例假設沒有其他 Systems Manager 維護時段處於作用中狀態，也沒有其他自動化正在執行。

如需限制的詳細資訊，請參閱AWS Systems Manager 端點和配額。

主題

- 從 AMS 主控台建立週期性「修補程式」維護時段（建議）
- 使用 AWS CloudFormation for AMS Accelerate 建立修補程式維護時段
- 從適用於 AMS Accelerate 的 Systems Manager 主控台建立維護時段
- 使用適用於 AMS Accelerate 的 Systems Manager 命令列界面 (CLI) 建立維護時段

從 AMS 主控台建立週期性「修補程式」維護時段（建議）

Microsoft 會在每個月的第二個星期二為其作業系統發行修補程式，也稱為修補程式星期二。相對於修補程式星期二，排程 Windows 和 Linux 執行個體的修補很常見。若要排定修補程式週二後第一個或第二個週末的週期性修補程式維護時段，請造訪 AMS 主控台並遵循下列步驟：

1. 為您的修補程式維護時段提供名稱。
2. 【選用】 提供修補程式維護時段的描述。
3. 選取相對於修補程式星期二的日期。

4. 輸入修補程式維護時段以 hh：mm 開始的時間。例如，午夜是 00：00，11pm 是 23：00。然後選取時區。
5. 【選用】 變更持續時間以符合您的需求。AMS 建議最短持續時間為四小時。
6. 輸入目標的修補程式標籤索引鍵和值。如需詳細資訊，請參閱什麼是標籤？。
7. 【選用】 展開選用參數以調整並行、錯誤率和維護時段截止。

    1. 並行控制同時修補的目標執行個體數量。例如，10 個目標執行個體的 50% 並行不會一次修補超過 5 個執行個體，而 100% 並行會一次修補全部 10 個執行個體。
    2. 錯誤率可在修補暫停之前控制錯誤的容錯能力。例如，10 個目標執行個體的 100% 錯誤率會修補所有執行個體，無論失敗多少，而 50% 錯誤率會在 5 個執行個體無法修補時暫停修補。AMS 建議 100% 錯誤率。
    3. 修補程式維護時段截止點可在修補程式維護時段結束前的指定小時暫停開始新的修補活動，以防止違反修補程式維護時段。例如，截止 1 小時 （建議），會在修補程式維護時段結束前 1 小時停止新的修補程式活動。

> **Important**
>
> 驗證下一次執行時間。
> 請造訪 SSM 維護時段主控台 ，搜尋新建立的修補程式維護時段，並驗證下一次執行時間。如果您有任何問題或需要編輯修補程式維護時段，請建立服務請求以與 AMS 修補程式專家交談

若要使用 CloudFormation 排程 CRON 型修補程式維護時段，請參閱 使用 AWS CloudFormation for AMS Accelerate 建立修補程式維護時段。

使用 AWS CloudFormation for AMS Accelerate 建立修補程式維護時段

若要使用 建立 AMS Accelerate 修補程式維護時段 AWS CloudFormation，請先登入您的 Accelerate 帳戶，然後選取 AWS 區域 目標執行個體所在的 。然後遵循 https：//https://console.aws.amazon.com/cloudformation 上的下列步驟：

1. 選取兩個自訂加速修補 CloudFormation 範本的其中一個。

    - 修補程式星期二排程：Microsoft 會在每個月的第二個星期二發佈其作業系統的修補程式，也稱為修補程式星期二，以在修補程式星期二之後的第一個或第二個週末排程修補程式維護時段：登入加速主控台後，請使用此連結 PatchTuesdayScheduling CloudFormation 範本 。

- CRON 排程：若要使用 CRON 建立修補程式維護時段來定義開始日期，請使用此連結 CRONScheduling CloudFormation 範本。請記住，Systems Manager CRON 編號天數為 1-7 天（如需 Systems Manager CRON 的詳細資訊，請參閱 Systems Manager 的參考：Cron 和 Rate 運算式)。

選擇其中一個連結會導致範本自動載入 CloudFormation 主控台。然後按一下 Next (下一步)。

2. 在指定堆疊詳細資訊頁面上（建立堆疊頁面的步驟 2)，輸入堆疊名稱和範本參數（顯示的預設參數是 AMS 建議的預設值，為您的使用案例選取日期和時間）。完成後，請按一下下一步。
3. 設定堆疊選項（選用）。如需選項的資訊，請參閱設定 AWS CloudFormation 堆疊選項。完成後，請按一下下一步。
4. 檢閱堆疊值（選用）。如需檢閱堆疊詳細資訊以估算成本的資訊，請參閱檢閱堆疊和估算堆疊成本。準備就緒時，請按一下建立堆疊。

   堆疊最多可能需要一分鐘的時間才能建立。成功建立堆疊後，您的修補程式維護時段會在指定的時間執行。您可以透過建立和執行 CloudFormation 變更集（建議）（如需執行此操作的詳細資訊，請參閱使用變更集建立堆疊) 或更新 Systems Manager 維護時段主控台 () 上的修補程式維護時段，來變更修補程式維護時段https://console.aws.amazon.com/systems-manager/maintenance-windows。

觀看 Namrata 的影片以進一步了解 (5：41)

從適用於 AMS Accelerate 的 Systems Manager 主控台建立維護時段

若要從 Systems Manager 主控台建立 AMS Accelerate 維護時段，請遵循下列步驟：

1. 在變更管理區域的左側導覽列中，按一下維護時段，然後按一下畫面右上角的建立維護時段。填寫表單。如需任何選項的詳細資訊，請參閱建立維護時段（主控台）。完成後，請按一下建立維護時段。

   維護時段清單頁面隨即開啟。
2. 選取新建立的維護時段。

   維護時段詳細資訊頁面隨即開啟。
3. 前往目標索引標籤，然後選擇註冊目標。

   註冊目標頁面隨即開啟。

4. 新增您的加速目標。如需目標的資訊，請參閱將目標指派給維護時段（主控台）。完成後，請按一下註冊目標。記下您稍後需要的目標。

   維護時段詳細資訊頁面會在目標索引標籤上重新開啟，其中包含包含新目標的清單。

5. 在維護時段詳細資訊頁面的任務索引標籤上，選擇註冊任務，然後從下拉式清單中選擇註冊自動化任務。填寫表單。加速備註：

   - 提供有意義的任務名稱。例如：AcceleratePatch。
   - 在自動化文件區域中按一下搜尋方塊中，選擇擁有者，然後選擇共用文件。
   - 在搜尋方塊中按一下並選擇文件名稱字首 --> 等於，然後輸入：AWSManagedServices-PatchInstance，以選取自動化文件。然後選取其選項按鈕，以選取 AWSManagedServices-PatchInstance 文件。
   - 在文件版本下，選擇執行時間的預設版本。
   - 在目標區段中：
     - 將目標設定為：選取已註冊的目標群組。
     - 在目標清單中，選取您在目標索引標籤中註冊的目標。
   - 在輸入參數區段中，填寫表單。
     - InstanceId： {{*TARGET_ID*}}
     - StartInactiveInstances：在修補程式維護時段期間停止執行個體時`True`啟動執行個體。

     > **Note**
     >
     > InstanceId 參數值區分大小寫，且 StartInactiveInstances 參數值可以是 True 或 False。
     > 當標籤鎖定目標時，無法啟動已停止的執行個體。如需詳細資訊，請參閱無要執行的調用。

   - 在速率控制區段中，選擇百分比。AMS Accelerate 建議 100% 用於並行，100% 用於錯誤閾值，以嘗試同時修補所有執行個體，無論自動化錯誤為何。例如，如果您希望一次修補一半的目標，讓一半的目標執行個體保持在負載平衡執行後，請將並行設定為 50%。
   - 在 IAM 服務角色區段中，選擇使用自訂服務角色，然後選擇 ams_ssm_automation_role。

   按一下註冊自動化任務。

   修補維護時段已建立。在描述索引標籤下，您可以看到下一次執行時間。

使用適用於 AMS Accelerate 的 Systems Manager 命令列界面 (CLI) 建立維護時段

若要使用命令列界面建立 AMS Accelerate 維護時段：

1. 遵循 SSM 教學課程：建立和設定維護時段 (AWS CLI)。對於教學課程的每個步驟，以下是用於修補的範例 CLI 命令。

> **Note**
>
> 這些範例專屬於 Linux 或 macOS。命令也可以從中執行 AWS CloudShell ，其可能比`awscli`在本機電腦上設定更簡單。如需詳細資訊，請參閱使用 AWS CloudShell 。

   a. 在教學課程的步驟 1 中，若要建立維護時段：

```
aws ssm create-maintenance-window \
                --name Sample-Maintenance-Window \
                --schedule "cron(0 30 23 ? * TUE#2 *)" \
                --duration 4 \
                --cutoff 1 \
                --allow-unassociated-targets \
                --tags "Key=Environment,Value=Production"
```

   成功完成時，`window-id`會傳回 。

   b. 在教學課程的步驟 2 中，註冊目標節點：

```
aws ssm register-target-with-maintenance-window \
                --window-id "mw-xxxxxxxxx" \
                --resource-type "INSTANCE" \
                --target "Key=tag:Environment,Values=Prod"
```

   成功完成時，會傳回 `WindowTargetID`。

   c. 在教學課程的步驟 3 中，註冊任務：

```
aws ssm register-task-with-maintenance-window \
    --window-id "mw-xxxxxx" \
    --targets "Key=WindowTargetIds,Values=63d4f63c-xxxxxx-9b1d-xxxxxfff" \
    --task-arn "AWSManagedServices-PatchInstance" \
```

```
    --service-role-arn "arn:aws:iam::AWS-Account-ID:role/ams_ssm_automation_role"
 \
    --task-invocation-parameters "{\"Automation\":{\"DocumentVersion\":\"\$DEFAULT
\",\"Parameters\":{\"InstanceId\":[\"{{TARGET_ID}}\"],\"StartInactiveInstances\":
[\"True\"]}}}" \
    --max-concurrency 50 \
    --max-errors 50 \
    --name "AutomationExample" \
    --description "Sample Description" \
    --task-type=AUTOMATION
```

具有勾點的修補程式

您可以使用 AMS 修補程式掛鉤，將 AMS 修補設定為在修補前後執行作業系統 (OS) 層級命令。使用 AMS 修補程式掛鉤在修補之前執行 SSM 命令文件來停止服務，然後在修補之後啟動服務，或在修補之後執行命令來確認您的應用程式運作狀態良好。

若要使用 AMS 修補程式掛鉤，您需要執行下列動作：

1. 建立 SSM 命令文件以用作修補程式掛鉤。
2. 建立 AMS 修補程式維護時段，或使用現有的 AMS 修補程式維護時段。如需詳細資訊，請參閱 AMS 修補程式維護時段。
3. 設定 AMS 修補程式維護時段，以將 SSM 命令文件用於 AMS 修補程式掛鉤。

AMS 修補程式掛鉤 RACI

負責、負責、諮詢和告知 或 RACI，矩陣會將主要責任指派給客戶或 AMS 以進行各種活動。下表提供使用 AMS 修補程式勾點之應用程式中活動的客戶和 AMS 責任概觀。

- R 代表負責方執行工作以達成任務
- 代表責任方
- C 代表已諮詢的對象；尋求意見的對象，通常是主題專家；以及與之進行雙邊溝通的對象
- 我代表知情；收到進度通知的一方，通常只在完成任務或可交付項目時

活動	客戶	AMS
建立修補前/後 SSM 命令文件和文件內容	R	C
設定 AMS 修補的修補程式掛鉤參數	R	C
執行前/後修補程式 SSM 命令文件	I	R
分類和回應修補程式掛接失敗	I	R
通知客戶修補程式掛接失敗	I	R
如果客戶要求，則轉返至預先修補狀態	C	R

建立修補程式掛鉤的 SSM 文件

AMS 修補程式掛鉤會在修補期間使用 Amazon EC2 Systems Manager (SSM) 文件。建立 SSM 命令文件，或與發生修補的帳戶共用現有的 SSM 命令文件。如需 SSM 文件的資訊，包括限制，請參閱共用 SSM 文件。

若要建立 SSM 命令文件，請遵循下列步驟：

1. 建立文件類型 = "Command" 的 SSM 文件。
2. 在 內容 （ 內容 ） 區段中輸入您的命令。如需詳細資訊，請參閱建立 SSM 文件內容。

> **Note**
>
> AMS 修補程式掛鉤的 SSM 文件也可以使用 AWS CLI 或 建立 AWS CloudFormation。如果您需要為 AMS 修補程式掛鉤建立 SSM 文件的協助，請聯絡您的 Cloud Architect。

設定 AMS 修補程式維護時段，以使用您的 SSM 命令文件做為 AMS 修補程式掛鉤

AMS 修補程式維護時段是 Systems Manager 維護時段，可執行您設定的 AMS 修補程式自動化。

若要編輯 AMS 修補程式維護時段以使用修補程式掛鉤，請遵循下列步驟：

1. 在 https://console.aws.amazon.com/systems-manager/ 左側導覽窗格的變更管理工具下，選取維護時段。

   隨即開啟列出現有維護時段的頁面。
2. 選取以 mw- 開頭的視窗 ID。

   該維護時段的詳細資訊頁面隨即開啟。
3. 選取任務索引標籤和具有 AMS-PatchInstance 任務 ARN 的視窗任務 ID，然後按一下編輯。

4. 向下捲動至參數區段，並更新下列參數。

AMS 修補程式掛鉤參數：

- PrePatchHook：您要在修補之前執行的類型為 "Command" 的 SSM 文件名稱。如果您在修補之前未執行命令，請保留此空白或輸入「AWS-Noop」（區分大小寫）。
- PostPatchHook：您想要在修補後執行之類型為「命令」的 SSM 文件名稱。如果您在修補後未執行命令，請保留此空白或輸入「AWS-Noop」（區分大小寫）。
- ExecutePatchBasedOnPreHookStatus：根據 PrePatchHook 執行的成功或失敗執行修補，請選擇一項：
  - OnPreHookSuccess：只有在 PrePatchHook 成功時才執行 AMS 修補程式自動化。
  - 一律：在 PrePatchHook 成功且失敗時執行 AMS 修補程式自動化。
  - OnPreHookFailure - 僅在 PrePatchHook 失敗時執行 AMS 修補程式自動化。
  - 從不：請勿執行 AMS 修補程式自動化。這在測試 PrePatchHook 時可能很有用。
- ExecutePostHookBasedOnPatchStatus：根據 AMS 修補程式自動化的成功或失敗執行修補程式後勾點，請選擇一項：
  - OnPatchSuccess：只有在 AMS 修補程式自動化成功執行時，才能執行 PostPatchHook。
  - 一律：在 AMS 修補程式自動化成功且失敗時執行 PostPatchHook。

- OnPatchFailure - 僅在 AMS 修補程式自動化失敗時執行 PostPatchHook。

> **Note**
>
> 如果其中任何變數缺少文字方塊，請捲動至相同頁面上的自動化文件區段，然後選取不同的文件，然後重新選取原始文件，以修正此問題。這會重新整理輸入參數，讓您可以編輯它們。

AMS Accelerate 修補程式基準

修補程式基線會定義在您的執行個體上核准安裝的修補程式。您可以逐一指定核准或拒絕修補程式。您也可以建立自動核准規則，以指定應自動核准某些類型的更新 (例如，關鍵的更新)。拒絕清單會覆寫規則與核准清單。

預設修補程式基準

當您加入 AMS Accelerate 修補時，下列作業系統的預設修補基準會由 AMS Accelerate 預設修補基準覆寫。

- Windows
- Amazon Linux 1
- Amazon Linux 2
- CentOS
- 暫停
- Rhel
- Ubuntu

> **Important**
>
> 預設修補程式基準由 AMS 管理。請勿編輯預設修補程式基準，因為您的變更可能會遺失。反之，請建立自訂修補程式基準。請參閱使用 AMS Accelerate 自訂修補程式基準

> **Note**
>
> AMS Accelerate 修補程式基準定義為 product = *，表示所有修補程式都會套用至所有安全性和分類的執行個體。

使用 AMS Accelerate 自訂修補程式基準

若要搭配 AMS Accelerate 使用自訂修補程式基準，請先確定您有修補程式群組，然後建立自訂基準。

如需詳細資訊，請參閱下列資源：

- 使用修補程式群組
- 建立自訂修補基準 (Windows)
- 建立自訂修補基準 (Linux)
- 更新或刪除自訂修補基準 （ 主控台 ）

建立 IAM 角色以隨需修補 AMS Accelerate

在您的帳戶加入 AMS Accelerate 修補之後，AMS Accelerate 會部署受管政策 amspatchmanagedpolicy。此政策包含使用 AMS 自動化文件 進行隨需修補的必要許可`AWSManagedServices-PatchInstance`。若要使用此自動化文件，帳戶管理員會為使用者建立 IAM 角色。請遵循下列步驟：

使用 建立角色 AWS Management Console：

1. 登入 AWS Management Console 並開啟 IAM 主控台。
2. 在主控台的導覽窗格中，選擇角色，然後建立角色。
3. 選擇 Anotherrole AWS 帳戶 類型。
4. 對於帳戶 ID，輸入您要授予資源存取權 AWS 的帳戶 ID。

   指定帳戶的管理員可以授予許可給該帳戶中的任何 IAM 使用者來擔任此角色。若要這樣做，管理員會將政策連接至使用者或群組，以授予sts：AssumeRoleaction 的許可。該政策必須指定角色的 Amazon Resource Name (ARN) 做為資源。請注意以下內容：

   - 如果您要從您未控制的 帳戶將許可授予使用者，而使用者將以程式設計方式擔任此角色，則 chooseRequire external ID。外部 ID 可以是您和第三方帳戶管理員之間商定的任何文字或數字。

此選項會自動將條件新增至信任政策，讓使用者只有在請求包含 correctsts：ExternalID 時才能擔任角色。如需詳細資訊，請參閱如何將 AWS 資源的存取權授予第三方時使用外部 ID。

- 如果您想要將角色限制為使用多重要素驗證 (MFA) 登入的使用者，請選擇要求 MFA。這會新增條件到角色的信任政策，以檢查 MFA 登入。想要擔任該角色的使用者必須從設定的 MFA 裝置使用臨時的一次性密碼登入。沒有 MFA 身分驗證的使用者無法擔任該角色。如需 MFA 的詳細資訊，請參閱在 中使用多重要素驗證 (MFA) AWS。

5. 選擇下一步：許可。

   IAM 包含帳戶中的政策清單。在新增許可下，在篩選方塊中輸入 amspatchmanagedpolicy，然後選取此許可政策的核取方塊。按一下 Next (下一步)。

6. 在角色詳細資訊下，輸入角色名稱，例如 PatchRole，為角色新增描述 （建議），也新增標籤以協助您識別此角色。角色名稱不區分大小寫，但在 中必須是唯一的 AWS 帳戶。完成後，按一下建立角色。

> **Note**
>
> 角色名稱建立後就無法編輯。

了解 AMS Accelerate 中的修補程式通知和修補程式失敗

> **Important**
>
> 從 2025 年 2 月 1 日開始，AMS 客戶將不再收到其受管帳戶中空修補程式維護 Windows 的通知。

修補程式服務請求和電子郵件通知

AMS 會在下一個修補程式維護時段的四天前建立新的服務請求。例如，在名為 App1 PROD 的修補程式維護時段執行前四天，AMS 會為帳戶 【帳戶 ID】 的 App1 Prod 建立名為四月修補程式維護時段的服務請求。如果您需要調整排定的修補程式，請使用修補程式服務請求與 AMS 通訊，或略過即將發生的修補程式。建立服務請求時，系統會傳送一封電子郵件到您的修補程式通知地址，其中包含服務請求的連結。每次 AMS 更新服務請求時，您會收到額外的電子郵件。

> **Note**
>
> AMS 會建立新的服務請求，即使修補程式維護時段是在排程執行前四天內建立的。修補程式維護時段必須處於「啟用」狀態，才能接收服務請求通知。

修補開始前一小時，AMS 會透過修補服務請求通知您。修補完成後，AMS 會使用修補程式管理員主控台的連結來更新修補程式服務請求。使用連結檢視修補程式維護時段鎖定之執行個體的修補程式合規。

> **Note**
>
> 修補程式管理員主控台中的連結會顯示執行個體目前的合規。如果在 AMS 完成修補且您存取連結之間發行新的修補程式，修補程式管理員會將執行個體顯示為不合規。

透過 CloudWatch Events 的修補程式通知

AMS 在修補程序期間會傳送 CloudWatch Events 三次，包括下列項目：

- 修補程式維護時段執行前四天。
- 修補程式維護時段執行前一小時。
- 當修補程式維護時段完成時。

以下是修補程式維護時段預先通知事件結構描述：

```
{
    "version": "0",
    "id": "37004d81-458d-2cef-fe1c-8afa8af30406",
    "detail-type": "AMS Patch Window Execution State Change",
    "source": "aws.managedservices",
    "account": "145917996532",
    "time": "2021-05-20T02:00:00Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/mw-00000001235",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaab"
    ],
    "detail": {
        "State": "PREEMPTIVE",
```

```
        "StartTime": "2021-05-24T02:00:00.000000",
        "WindowArn": "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/
mw-00000001235",
        "Results": "[{\"instanceId\": \"i-0000000aaaaaaaaaa\"}, {\"instanceId\":
 \"i-0000000aaaaaaaaab\"}]"
    }
}
```

下表說明修補程式維護時段預先通知事件結構描述：

修補程式通知詳細資訊

屬性名稱	描述	範例值
State	修補維護時段的狀態	PREEMPTIVE - 排定的修補時段即將開始
狀態	修補維護時段的狀態	成功 - 所有執行個體都是修補且未失敗 失敗 – 至少有一個執行個體無法修補
StartTime	修補維護時段的開始時間，採用 ISO 格式	2021-02-03T22：14：05.814308
WindowArn	修補維護時段的唯一識別符	arn：aws：ssm：us-east-1： 123456789012：maintenancewindow/mw-00000001235
結果	修補程式視窗鎖定目標的執行個體清單	InstanceId – 目標執行個體的執行個體 ID

以下是修補程式維護時段結束事件結構描述：

```
{"version": "0",
    "id": "0f25add5-44a9-0702-d2bc-bd2102affefe",
    "detail-type": "AMS Patch Window Execution State Change",
    "source": "aws.managedservices",
    "account": "123456789012",
```

```
    "time": "2021-02-03T22:14:06Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/mw-00000001235",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaab"
    ],
    "detail": {"State": "[COMPLETED]",
        "Status": "SUCCESS",
        "StartTime": "2021-02-03T22:12:00.814308",
        "EndTime": "2021-02-03T22:14:05.814309",
        "WindowArn": "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/
mw-00000001235",
        "WindowExecutionId": "e32088eb-c05f-4c63-b766-6866e163c818",
        "Results": "[{\"instanceId\": \"i-0000000aaaaaaaaaa\", \"status\":
 \"Success\", \"missing_critical_patch_count\": 0, \"missing_total_patch_count
\": 0} }, {\"instanceId\": \"i-0000000aaaaaaaaab\", \"status\": Success},
 \"missing_critical_patch_count\": 0, \"missing_total_patch_count\": 0}]"
    }
}
```

下表說明修補程式維護時段結束事件結構描述：

修補程式視窗結束詳細資訊

屬性名稱	描述	範例值
State	修補維護時段的狀態	已完成 – 修補時段已完成
狀態	修補維護時段的狀態	成功 – 所有執行個體都是修補且未失敗 失敗 – 至少有一個執行個體無法修補
StartTime	修補維護時段的開始時間，採用 ISO 格式	2021-02-03T22：14：05.814308
EndTime	修補維護時段的結束時間，採用 ISO 格式	2021-02-03T23：14：05.814308
WindowArn	修補維護時段的唯一識別符。	arn：aws：ssm：us-east-1： 123456789012：

屬性名稱	描述	範例值
		maintenancewindow/mw-00000001235
WindowExecutionId	視窗執行 ID，可從 SSM 維護時段主控台查看	e32088eb-c05f-4c63-b766-6866e163c818
結果	修補程式視窗將鎖定目標的執行個體清單	InstanceId – 目標執行個體 ID 狀態 – 執行個體修補程式狀態 missing_critical_patch_count - 執行個體上遺失的關鍵修補程式計數 missing_total_patch_count - 執行個體上遺失的修補程式總數

您可以使用 CloudWatch Events 事件來觸發 CloudWatch 規則，以便在傳送修補維護時段預先通知時通知您。若要這樣做，請使用下列組態設定 CloudWatch 規則：

```
{
    "source": [
        "aws.managedservices"
    ],
    "detail-type": [
        "AMS Patch Window Execution State Change"
    ],
    "detail": {
        "State": ["PREEMPTIVE"]
    }
}
```

> **Note**
>
> 如果執行個體的作業系統不受支援，或在維護時段內停止，則不會建立修補程式失敗提醒。

AMS 中的修補程式失敗調查

AWS Managed Services (AMS) 會管理修補，並包含修補失敗修復。修補失敗時，AMS Operations 會收到提醒，並遵循 AWS 和 AMS 最佳實務來嘗試修復問題。

如果修補程式失敗，則 AMS 會在帳戶中建立具有下列標題的 SSM OpsItem：AWS Managed Services – 執行個體 <instance-id> 的修補程式執行個體失敗。

AMS 接著會調查 OpsItem。如果 AMS 可以在不介入的情況下修正故障，則 AMS 會解析 OpsItem。如果需要您的介入，則 AMS 會透過包含調查結果和建議修復步驟的服務請求通知您。如果您不採取行動來解決問題，則 AMS 會在下一個排定的修補程式維護時段嘗試修補執行個體。

> **Note**
>
> 修補程式失敗 OpsItems 不會針對具有不支援作業系統，或在修補程式維護時段處於已停止狀態的執行個體建立。

使用 AMS Resource Scheduler 進行成本最佳化

AWS 解決方案上的 AMS Resource Scheduler 透過停止未使用的資源，以及在需要容量時啟動資源，協助您降低 AWS 和 AMS 成本。例如，您可以在開發環境中使用 AWS 上的 AMS Resource Scheduler，在每天上班時間之外自動停止執行個體。如果您讓所有執行個體以完全使用率執行，此解決方案可以降低執行個體使用率，進而根據您設定的排程降低整體成本。

使用 AWS Managed Services (AMS) Resource Scheduler 來排程自動啟動和停止您帳戶中的 Auto Scaling 群組、Amazon EC2 執行個體和 Amazon RDS 執行個體。這有助於降低資源不應全年無休執行的基礎設施成本。解決方案建置在AWS 執行個體排程器之上，但包含 AMS 客戶需求的其他功能和自訂項目。自訂包含排程 Auto Scaling 群組的支援、Elastic Load Balancing 警示的 CloudWatch 警示抑制器、Amazon EC2 的多個 AWS Systems Manager 維護時段的支援、節省成本估算器，以及 AMS 的操作支援。

AMS Resource Scheduler 使用期間和排程。期間定義資源應執行的時間，例如開始時間、結束時間和當月天數。排程包含您定義的期間，以及其他組態：SSM 維護時段、時區、休眠等，並指定資源應何時執行。您可以使用 AMS 提供的 AWS Systems Manager 自動化 Runbook 來設定這些期間和排程。每個排程必須至少包含一個期間（定義執行個體應執行的時間）。排程可以包含多個期間。當排程中使用多個期間時，執行個體排程器會在至少一個期間規則為 true 時套用適當的啟動動作。如需排程和期間的詳細資訊，請參閱 AWS 執行個體排程器的解決方案元件。

AMS Resource Scheduler 使用 AWS 資源標籤將排程與一或多個資源建立關聯，以將其設為排程開始和停止動作的目標。您可以使用排程器中設定的標籤索引鍵（預設為 `Schedule`) 來標記資源，並以排程名稱做為值。您可以為排程器的成本估算器功能設定與 中的成本分配標籤相同的標籤索引鍵 AWS Cost Explorer ，以追蹤和報告成本節省。

AMS Resource Scheduler 是一種選擇加入功能，您可以為每個帳戶啟用此功能。

搭配 AMS Resource Scheduler 使用資源

Amazon EC2

- AMS Resource Scheduler 不會個別處理和略過屬於 Auto Scaling 群組的 Amazon EC2 執行個體，即使這些執行個體已加上標籤也一樣。
- 如果目標執行個體根磁碟區使用 AWS KMS 客戶主金鑰 (CMK) 加密，則需要將額外的`kms:CreateGrant`許可新增至您的 Resource Scheduler IAM 角色，排程器才能啟動此類執行個體。根據預設，此許可不會新增至角色，以改善安全性。如果您需要此許可，您可以透過更新

CloudFormation 堆疊 來新增許可`ams-resource-scheduler`，並將 CMK 清單做為 `UseCMK` 參數的值（使用 格式的一或多個 CMK 金鑰 ARNs，`arn:`*`partition`*`:kms:`*`region`*`:`*`account-id`*`:key/`*`key-id`*而非 KMS 別名）。

- 如果您的 Amazon EC2 執行個體設定了特定軟體或由 管理的廠商授權 AWS License Manager，Resource Scheduler 需要特定 AWS License Manager 授權的許可，才能啟動執行個體。您可以將 AWS License Manager 授權的 ARN 清單新增至 CloudFormation 堆疊 () EC2 執行個體參數的 License Manager 授權，以授予 Resource Scheduler 必要的許可`ams-resource-scheduler`。

Amazon EC2 Auto Scaling

- AMS Resource Scheduler 會啟動或停止 Auto Scaling 群組的自動擴展，而不是群組中的個別執行個體。也就是說，排程器會還原 Auto Scaling 群組的大小（開始）或將大小設定為 0（停止）。
- 使用指定的標籤標記 Auto Scaling 群組，而不是群組中的執行個體。
- 在停止期間，AMS Resource Scheduler 會存放 Auto Scaling 群組的最小、預期和最大容量值，並將最小和預期容量設定為 0。在啟動期間，排程器會還原停止期間的 Auto Scaling 群組大小。因此，Auto Scaling 群組執行個體必須使用適當的容量組態，以便執行個體的終止和重新啟動不會影響 Auto Scaling 群組中執行的任何應用程式。
- 如果在執行期間修改 Auto Scaling 群組（最小或最大容量），排程器會存放新的 Auto Scaling 群組大小，並在停止排程結束時還原群組時使用。

Amazon RDS

- 排程器可以在停止 RDS 執行個體之前擷取快照（不適用於 Aurora 資料庫叢集）。此功能預設為開啟，且建立 RDS 執行個體快照 AWS CloudFormation 範本參數設為 true。快照會保留到下次停止 Amazon RDS 執行個體並建立新的快照為止。
- 排程器可以啟動/停止屬於叢集或 Amazon RDS Aurora 資料庫或多可用區域 (Multi-AZ) 組態的 Amazon RDS 執行個體。不過，當排程器無法停止 Amazon RDS 執行個體時，請檢查 Amazon RDS 限制，尤其是多可用區域執行個體。
- 若要排程 Aurora 叢集啟動或停止，請使用排程 Aurora 叢集範本參數（預設為 true)。Aurora 叢集（而非叢集內的個別執行個體）必須使用初始組態期間定義的標籤索引鍵和排程名稱做為標籤值來標記，以排程該叢集。

> **Note**
>
> 資源排程器不會驗證資源是否已啟動或停止。它會為相關服務發出 API 呼叫並繼續。如果 API 呼叫失敗，它會記錄錯誤以進行調查。
> AMS Resource Scheduler 不支援 AWS Backup 視窗。如果您將 AWS Backup已啟用 RDS 執行個體與 Resource Scheduler 排程對應，備份必須位於排程的執行時段內，才能如預期運作。

加入 AMS 資源排程器

當您的帳戶加入 AMS Accelerate 操作計劃時，您的帳戶不會自動加入 AMS Resource Scheduler。不過，作為加入 AMS Accelerate 操作計劃帳戶的一部分，或之後隨時，您可以請求 Cloud Service Delivery Manager (CSDM) 將帳戶加入 AMS Resource Scheduler。一旦您的 CSDM 加入帳戶，包含具有預設組態之 AMS Resource Scheduler 資源的 CloudFormation 堆疊會自動佈建至您的帳戶。

在您的帳戶中佈建 AMS Resource Scheduler 之後，我們建議您檢閱預設組態，並視需要根據您的偏好設定自訂組態，例如標籤索引鍵、時區、排程服務等。如需建議自訂的詳細資訊，請參閱 自訂 AMS 資源排程器，下一步。

自訂 AMS 資源排程器

加入時，AMS Resource Scheduler 會部署為 CloudFormation 堆疊，其名稱為 `ams-resource-scheduler`，位於 AMS Accelerate 帳戶的主要 AWS 區域中。您可以透過 CloudFormation 堆疊參數和執行堆疊更新，根據您的偏好設定來設定 AMS Resource Scheduler 的屬性。如需更新 CloudFormation 堆疊的資訊，請參閱直接更新堆疊。

我們建議您自訂下列屬性，並將其餘屬性保留在預設狀態，以獲得最佳功能。

- 標籤名稱：Resource Scheduler 用來將執行個體排程與 資源建立關聯的標籤名稱。預設值為 `Schedule`。
- 要排程的 Service(s)：以逗號分隔的清單，列出 Resource Scheduler 可以管理的服務。預設值為 `ec2,rds,autoscaling`。有效值為 "ec2"、"rds" 和 "autoscaling"。
- 預設時區：指定資源排程器要使用的預設時區。預設值為 `UTC`。
- 加密 EBS 磁碟區的 CMK：以逗號分隔的 Amazon KMS 客戶受管金鑰 (CMK) ARNs 清單，可將許可授予資源排程器。

- EC2 執行個體的授權管理員授權：可以授予該資源排程器以逗號分隔的 AWS Licence Manager ARNs 清單許可。

> **Note**
>
> AMS 偶爾會發行功能和修正，讓 AMS Resource Scheduler 在您的帳戶中保持最新狀態。發生這種情況時，您透過堆疊參數對 AMS Resource Scheduler 堆疊進行的任何自訂都會保留。我們強烈建議不要直接對 AMS Resource Scheduler 的任何元件資源進行任何自訂。這樣做會影響 Resource Scheduler 功能和 AMS 保持最新狀態的能力。

使用 AMS 資源排程器

如何在 AMS Accelerate 帳戶中使用 AMS Resource Scheduler 期間。

使用下列一組 AWS Systems Manager 自動化 Runbook，在 AMS Resource Scheduler 中管理所需的排程和期間。

> **Note**
>
> 這些 SSM 自動化 Runbook 可在您帳戶的主要 AWS 區域中使用。

- `AWSManagedServices-AddOrUpdatePeriod`
- `AWSManagedServices-AddOrUpdateSchedule`
- `AWSManagedServices-DeleteScheduleOrPeriod`
- `AWSManagedServices-DescribeScheduleOrPeriods`
- `AWSManagedServices-EnableOrDisableAMSResourceScheduler`

此外，AMS 會佈建角色 `ams_resource_scheduler_ssm_automation_role`，此 AWS Identity and Access Management 角色 AWS Systems Manager 需要 和 ，才能使用 Runbook。IAM 角色的範圍縮小，具有授予執行手冊功能所需 SSM 許可的最低權限內嵌政策。

先決條件

在您開始使用 SSM 自動化 Runbook 和 AMS Resource Scheduler 之前，請執行下列步驟。

將下列政策連接至您要允許 使用自動化 Runbook 在 AMS Resource Scheduler 中管理排程和期間的適當 IAM 實體 （使用者、群組或角色）。如果您的 IAM 實體在帳戶中具有管理員或 PowerUser 許可，則不需要此政策。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowPassingResourceSchedulerRole",
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::111122223333:role/
ams_resource_scheduler_ssm_automation_role",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "ssm.amazonaws.com"
                }
            }
        },
        {
            "Sid": "ListAndDescribeAutomationExecutions",
            "Effect": "Allow",
            "Action": [
                "ssm:GetAutomationExecution",
                "ssm:DescribeAutomationStepExecutions"
            ],
            "Resource": "arn:aws:ssm:*:111122223333:automation-execution/*"
        },
        {
            "Sid": "ListAndDescribeResourceSchedulerSSMDocuments",
            "Effect": "Allow",
            "Action": [
                "ssm:ListDocumentVersions",
                "ssm:DescribeDocument",
                "ssm:ListDocumentMetadataHistory",
                "ssm:DescribeDocumentParameters",
                "ssm:GetDocument",
                "ssm:DescribeDocumentPermission"
            ],
            "Resource": [
```

```
                "arn:aws:ssm:*::document/AWSManagedServices-AddOrUpdatePeriod",
                "arn:aws:ssm:*::document/AWSManagedServices-AddOrUpdateSchedule",
                "arn:aws:ssm:*::document/AWSManagedServices-
DeleteScheduleOrPeriod",
                "arn:aws:ssm:*::document/AWSManagedServices-
DescribeScheduleOrPeriods",
                "arn:aws:ssm:*::document/AWSManagedServices-
EnableOrDisableAMSResourceScheduler"
            ]
        },
        {
            "Sid": "AllowExecutionOfResourceSchedulerSSMDocuments",
            "Effect": "Allow",
            "Action": [
                "ssm:StartAutomationExecution"
            ],
            "Resource": [
                "arn:aws:ssm:*::automation-definition/AWSManagedServices-
AddOrUpdatePeriod:*",
                "arn:aws:ssm:*::automation-definition/AWSManagedServices-
AddOrUpdateSchedule:*",
                "arn:aws:ssm:*::automation-definition/AWSManagedServices-
DeleteScheduleOrPeriod:*",
                "arn:aws:ssm:*::automation-definition/AWSManagedServices-
DescribeScheduleOrPeriods:*",
                "arn:aws:ssm:*::automation-definition/AWSManagedServices-
EnableOrDisableAMSResourceScheduler:*"
            ]
        },
        {
            "Sid": "AllowListingAllDocuments",
            "Effect": "Allow",
            "Action": "ssm:ListDocuments",
            "Resource": "*"
        },
        {
            "Sid": "AllowListingAllSSMExecutions",
            "Effect": "Allow",
            "Action": "ssm:DescribeAutomationExecutions",
            "Resource": "*"
        },
        {
            "Sid": "AllowListingIAMRolesForStartingExecutionViaConsole",
            "Effect": "Allow",
```

```
            "Action": "iam:ListRoles",
            "Resource": "*"
        }
    ]
}
```

您可以從 AWS Systems Manager 主控台或使用 CLI AWS 執行自動化。如果使用 AWS CLI，您可能需要安裝和設定它，或尚未安裝 PowerShell AWS 的工具。如需詳細資訊，請參閱安裝或升級 AWS 命令列工具。

觀看 Navish 的影片以進一步了解 (4：52)

在 AWS Managed Services Resource Scheduler 中使用期間和排程

您可以使用 AMS Resource Scheduler 在 AMS Accelerate 帳戶中新增、更新或刪除排程或期間。

在 AMS Resource Scheduler 中新增或更新期間

新增或更新 AMS 帳戶中的資源排程器期間。

您需要的資料：

- 動作：要執行的操作類型。如果您想要新增期間，請使用「新增」；如果您想要更新現有期間，請使用「更新」。
- 名稱：期間的名稱。如果您要新增期間，則必須指定唯一的值。
- AutomationAssumeRole：允許 Runbook 代表您新增或更新期間之 AWS Identity and Access Management (IAM) 角色的 ARN。將角色指定為 `ams_resource_scheduler_ssm_automation_role`。
- 描述（選用）：期間有意義的描述。
- BeginTime（選用）：您想要啟動資源的時間，以 HH：MM 格式顯示。
- EndTime（選用）：您想要停止資源的時間，以 HH：MM 格式顯示。
- 月（選用）：以逗號分隔的月清單或連字號分隔的月範圍，在此期間資源應執行。
- MonthDays（選用）：以逗號分隔的月份天數清單，或資源應執行的連字號天數範圍。
- WeekDays（選用）：以逗號分隔的一週內天數清單，或資源應執行的一週內天數範圍。

如何執行：

- 在 AWSManagedServices-AddOrUpdatePeriod 中檢視文件（您可能需要選擇加入的區域）。

在輸入參數區段中指定需求，然後選擇執行。操作完成後，請在輸出索引標籤中檢視結果。

- AWS CLI：

  執行下列命令來啟動自動化。將####取代為您自己的資訊。

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
AddOrUpdatePeriod" --document-version "\$DEFAULT"
     --parameters '{"Action":["add" or "update"], "Name":["NAME"],
    "Description":["DESCRIPTION"],"BeginTime":["TIME"], "EndTime":["TIME"],
    "Months":["MONTH"],"MonthDays":["DAY"], "WeekDays":["DAY"],
    "AutomationAssumeRole" : ["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"] }' --region ONBOARDED_REGION
```

範例：

下列範例示範如何使用 AWS Systems Manager 主控台新增期間。我們已命名 period-Name，並設定每月前 15 天從週一到週五上午 9AM-6PM。

1. 在 AWSManagedServices-AddOrUpdatePeriod 檢視 AWS Systems Manager 自動化文件 （您可能需要選擇加入的區域）。

2. 提供參數的值。

3. 按一下執行並等待自動化完成。

在 AMS Resource Scheduler 中新增或更新排程

在 AMS Accelerate 帳戶中新增或更新資源排程器排程。

您需要的資料：

- 動作：要執行的操作類型。如果您想要新增排程，請使用「新增」；如果您想要更新現有的排程，請使用「更新」。
- 名稱：排程的名稱。如果您要新增排程，則必須指定唯一的值。
- AutomationAssumeRole：允許 Runbook 代表您新增或更新排程的 AWS Identity and Access Management (IAM) 角色 ARN。指定角色 `ams_resource_scheduler_ssm_automation_role`。

- 描述（選用）：排程的有意義的描述。
- 排程（選用）：指定要與此排程搭配使用的逗號分隔期間清單。必須已建立每個期間。
- RetainRunning（選用）：指定「true」，以防止資源排程器在執行期間結束時停止執行中的資源，如果資源是在執行操作開始之前手動啟動。根據預設，資源排程器會停止資源。
- StopNewInstances（選用）：指定「false」，以防止資源排程器在執行期間之外執行時，第一次標記資源時停止資源。根據預設，資源排程器會停止資源。
- SSMMaintenanceWindow（選用）：指定要新增為排程執行期間之 AWS Systems Manager (SSM) 維護時段的逗號分隔清單。您還必須將 "UseMaintenanceWindow" 屬性指定為 "true"。
- TimeZone（選用）：指定您希望資源排程器使用的時區。根據預設，Resource Scheduler 會使用 UTC。
- UseMaintenanceWindow（選用）：如果您想要 Resource Scheduler 將 Amazon Relational Database Service (RDS) 維護時段視為 Amazon RDS 執行個體排程的執行期間，或將 AWS Systems Manager (SSM) 維護時段新增為 Amazon EC2 執行個體排程的執行期間，請指定「true」。
- UseMetrics（選用）：指定「true」以在排程層級啟用 CloudWatch 指標，並指定「false」停用 CloudWatch 指標。指定此屬性會覆寫堆疊層級設定的 CloudWatch 指標設定。

如何執行：

- 在 AWSManagedServices-AddOrUpdateSchedule 中檢視文件（您可能必須選擇加入的區域）。

  在輸入參數區段中指定需求，然後選擇執行。操作完成後，請在輸出索引標籤中檢視結果。

- AWS CLI：

  執行下列命令來啟動自動化。將####取代為您自己的資訊。

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
AddOrUpdateSchedule" --document-version "\$DEFAULT"
     --parameters '{"Action":["add" or "update"], "Name":["NAME"], "Description":
["DESCRIPTION"],
    "Hibernate":["true or false"],"Enforced":["true or false"],
    "OverrideStatus":["running or stopped"],"Periods":["PERIOD-A, PERIOD-B"],
    "RetainRunning":["true or false"],"StopNewInstances":["true or false"],
    "SSMMaintenanceWindow":["WINDOW-NAME"],"TimeZone":["TIMEZONE"],
    "UseMaintenanceWindow":["true or false"],"UseMetrics":["true or false"],
    "AutomationAssumeRole" : ["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"] }' --region ONBOARDED_REGION
```

範例：

下列範例顯示如何新增 AMS Resource Scheduler 的排程。在此範例中，您會使用 CustomPeriod 新增名為 CustomSchedule 的排程。 CustomPeriod

1. 在 AWSManagedServices-AddOrUpdateSchedule 中檢視 AWS Systems Manager 自動化文件（您可能需要選擇加入的區域）。

2. 提供參數的值。

3. 按一下執行並等待自動化完成。

在 AMS Resource Scheduler 中刪除期間或排程

若要刪除 AMS Accelerate 帳戶中的資源排程器期間或排程，您需要下列資料：

- ConfigurationType：您要刪除的組態類型。如果您想要刪除期間，請使用「期間」；如果您要刪除排程，請使用「排程」。
- 名稱：您要刪除的排程或期間的名稱。
- AutomationAssumeRole： AWS Identity and Access Management (IAM) 角色的 ARN，允許 Runbook 代表您刪除排程或期間。指定角色 `ams_resource_scheduler_ssm_automation_role`。

如何執行：

- 在 AWSManagedServices-DeleteScheduleOrPeriod 中檢視文件（您可能3必須選擇加入的區域）。

  在輸入參數區段中指定需求，然後選擇執行。操作完成後，請在輸出索引標籤中檢視結果。
- AWS CLI：

  執行下列命令來啟動自動化。將####取代為您自己的資訊。

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
DeleteScheduleOrPeriod" --document-version "\$DEFAULT"
--parameters '{"ConfigurationType":["period" or "schedule"],"Name":["NAME"],
    "AutomationAssumeRole":["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"]}' --region ONBOARDED_REGION
```

範例：

下列範例示範如何使用 AWS Systems Manager 主控台刪除期間。

1. 在 AWSManagedServices-DeleteScheduleOrPeriod 中檢視 AWS Systems Manager 自動化文件（您可能需要選擇加入的區域）。

2. 提供參數的值。

3. 按一下執行並等待自動化完成。

在 AMS Resource Scheduler 中描述期間或排程

若要在 AMS Accelerate 帳戶中描述（檢視詳細資訊）資源排程器期間或排程，您需要下列資料：

- ConfigurationType：您要描述的組態類型。如果您想要描述所有期間，請使用「期間」；如果您想要描述所有排程，請使用「排程」。
- AutomationAssumeRole： AWS Identity and Access Management (IAM) 角色的 ARN，允許 Runbook 代表您描述排程或期間。指定角色 `ams_resource_scheduler_ssm_automation_role`。

如何執行：

- 在 AWSManagedServices-DescribeScheduleOrPeriods 中檢視文件（您可能需要選擇加入的區域）：
  1. 在輸入參數區段中指定需求，然後選擇執行。
  2. 操作完成後，請在輸出索引標籤中檢視結果。
- AWS CLI：
  1. 執行下列命令來啟動自動化。將*####*取代為您自己的資訊。

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
DescribeScheduleOrPeriods" --document-version "\$DEFAULT"
                --parameters '{"ConfigurationType":["period" or
 "schedule"],"AutomationAssumeRole":["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"]}'
                --region ONBOARDED_REGION
```

範例：

下列範例顯示如何使用 AWS Systems Manager 主控台描述期間。

1. 在 AWSManagedServices-DescribeScheduleOrPeriods 中檢視 AWS Systems Manager 自動化文件（您可能需要選擇加入的區域）。

2. 提供參數的值。

3. 按一下執行並等待自動化完成。

AMS Resource Scheduler 的標記資源

標記 AMS Resource Scheduler 的資源。

將排程和期間新增至 AMS 資源排程後，您需要使用資源排程器標籤名稱作為標籤索引鍵，或您的自訂標籤名稱，並將排程名稱作為標籤值。如需如何在 AMS Accelerate 帳戶中標記資源的詳細資訊，請參閱 AMS Accelerate 中的標記。

> **Note**
>
> 如果使用 Resource Tagger 來標記資源，則資源排程器的預設標籤金鑰必須自訂為具有字首 'ams:rt:'，因為資源標記器套用的所有標籤都有金鑰字首 'ams:rt:'。否則，資源排程器將不會管理以資源標記程式標記的資源。若要進一步了解如何自訂資源排程器的預設標籤金鑰，請參閱 自訂 AMS 資源排程器。

AMS 資源排程器中的成本估算器

為了追蹤成本節省，AMS Resource Scheduler 具有一個元件，可每小時計算排程器管理的 Amazon EC2 和 Amazon RDS 資源的預估成本節省。此節省成本資料接著會發佈為 CloudWatch 指標 (AMS/ResourceScheduler)，以協助您追蹤資料。成本節省估算器只會預估執行個體執行時數的節省。它不會考慮任何其他成本，例如與資源相關聯的資料傳輸成本。

成本節省估算器已透過 Resource Scheduler 啟用。它會每小時執行一次，並從中擷取成本和用量資料 AWS Cost Explorer。從該資料中，它會計算每個執行個體類型的每小時平均成本，然後在未排定的情況下執行整天的預估成本。節省成本是特定日期的預計成本與 Cost Explorer 實際報告成本之間的差異。

例如，如果執行個體 A 使用 Resource Scheduler 設定為從上午 9 點到下午 5 點執行，即指定日期的八個小時。Cost Explorer 會將成本報告為 $1，用量報告為 8。因此，每小時的平均成本為 0.125 美元。如果未使用 Resource Scheduler 排程執行個體，則執行個體會在當天執行 24 小時。在這種情況下，成本會是 24x0.125 = $3。資源排程器可協助您節省 2 美元的成本。

為了節省成本估算器僅從 Cost Explorer 擷取由 Resource Scheduler 管理的資源的成本和用量，Resource Scheduler 用於目標資源的標籤索引鍵需要啟用為帳單儀表板中的成本分配標籤。如果帳戶屬於組織，則需要在組織的管理帳戶中啟用標籤金鑰。如需執行此操作的詳細資訊，請參閱啟用使用者定義的成本分配標籤和使用者定義的成本分配標籤

在標籤金鑰啟用為成本分配標籤後，AWS 帳單會開始追蹤資源排程器所管理資源的成本和用量，並在該資料可用之後，成本節省估算器會開始計算成本節省，並在 CloudWatch 中的`AMS/ResourceScheduler`指標命名空間下發佈資料。

如果未啟用成本分配標籤，估算器就無法計算節省成本並發佈指標，即使已啟用也一樣。

> **Note**
>
> 成本節省估算器不接受折扣，例如預留執行個體、節省計劃等，並將其計算納入考量。估算器會從 Cost Explorer 取得使用成本，並計算資源每小時的平均成本。如需詳細資訊，請參閱了解您的 AWS 成本資料集：備忘單。

AMS 資源排程器中的警示抑制器

AMS Resource Scheduler 隨附 CloudWatch 警示抑制器，部署為名為 的個別 Lambda 函數`AMSAlarmSuppressor`，可抑制 Elastic Load Balancing、Application Load Balancer 或 Network Load Balancer 後方執行個體的警示。函數每 5 分鐘執行一次，擷取帳戶中存在的所有警示，並根據命名空間進行分組；例如，`AWS/ELB`、`AWS/ApplicationELB`、`AWS/NetworkELB`。對於每個警示群組，禁止程式會從警示維度找到負載平衡器名稱和/或目標群組 （適用於 ALB/NLB)，尋找向負載平衡器和/或目標群組註冊的執行個體，並檢查執行個體狀態，以探索執行個體是否由 AMS Resource Scheduler 排程。如果執行個體是由 Resource Scheduler 排程，而由 Resource Scheduler 停止，則抑制器會標記警示以停用它們。如果已註冊執行個體清單中至少有一個執行個體正在執行，抑制器會標記對應的警示，以啟用標示為啟用的警示，並停用標示為停用的警示。此項目的日誌會存放在`/aws/lambda/AMSAlarmSuppressor`日誌群組中。

AMS Accelerate 中的日誌管理

AMS Accelerate 會設定支援的 AWS 服務來收集日誌。AMS Accelerate 使用這些日誌，以確保您的帳戶內資源的合規性和稽核。

AMS Accelerate 提供各種營運服務，協助您在 AWS 上實現卓越營運。若要快速了解 AMS 如何透過我們的一些關鍵營運功能，包括全年無休服務台、主動監控、安全性、修補、記錄和備份，協助您的團隊在 AWS 雲端中實現整體卓越營運，請參閱 AMS 參考架構圖表。

主題

日誌管理 — AWS CloudTrail

AWS CloudTrail 是一項用於帳戶控管的服務：合規、營運稽核和風險稽核。使用 CloudTrail，您可以記錄、持續監控和保留 AWS 與基礎設施中動作相關的帳戶活動。

AMS Accelerate 需要 AWS CloudTrail 記錄才能管理您帳戶中所有資源的稽核和合規。加入時，您可以選擇下列其中一個選項：

- AMS 部署的線索：如果您選擇此選項，AMS 會在主要區域中建立、部署和管理 CloudTrail 多區域線索 AWS ，與您帳戶中的任何現有線索無關。
- 使用您自己的線索：如果您選擇提供自己的帳戶或組織 CloudTrail 線索，則必須與您的 Cloud Architect (CA) 合作，以確保它符合 Accelerate 所需的組態。如果您選擇此選項，但未提供自己的線索，則 Accelerate 會自動部署自己的 CloudTrail 線索，以維持持續的安全性和稽核涵蓋範圍。如果您稍後提供自己的線索，AMS 會移除其部署的線索，以避免備援和額外費用。此方法有助於在您的帳戶中維護單一作用中的 CloudTrail 追蹤，並避免重複的記錄成本。

> **Note**
>
> 如果您的帳戶有現有的 CloudTrail 追蹤，而且您在加入期間尚未特別設定或請求 AMS 受管追蹤，AMS Accelerate 會自動從您的帳戶中移除 AMS 部署的追蹤。這可防止重複記錄、最佳化資源用量，並節省額外的成本。

AMS Accelerate 會為 Accelerate 部署的 CloudTrail 追蹤建立 Amazon S3 儲存貯體，做為事件交付目的地並使用 AWS Key Management Service (AWS KMS) 加密。AMS Accelerate 運算子會存取您的追蹤事件，以進行調查和診斷。如果帳戶已啟用現有的 CloudTrail 追蹤，如果您選擇在加入期間讓 Accelerate 部署 Accelerate 受管追蹤，則此追蹤是額外的。

AMS Accelerate 部署 AWS Config 規則以確保您的 CloudTrail 帳戶追蹤，包括 Accelerate 部署的 CloudTrail 追蹤已正確設定和加密。如需詳細資訊，請參閱 AWS Config。這些是使用的規則，以說明這些規則 AWS 的文件連結呈現：

- multi-region-cloudtrail-enabled。檢查 AMS Accelerate CloudTrail 是否使用正確的組態正確設定。
- cloud-trail-encryption-enabled。檢查 AWS CloudTrail 已設定為搭配 AWS KMS 客戶主金鑰 (CMK) 加密使用伺服器端加密 (SSE)。
- cloud-trail-log-file-validation-enabled。啟用時， 會檢查 是否 AWS CloudTrail 使用日誌建立已簽署的摘要檔案。我們強烈建議您在所有線索上啟用檔案驗證。
- s3-bucket-default-lock-enabled。啟用時， 會檢查 Amazon S3 儲存貯體是否已啟用鎖定。
- 啟用 s3-bucket-logging-enabled。啟用時， 會檢查是否已為 Amazon S3 儲存貯體啟用記錄。

AMS Accelerate 使用 AWS KMS 來加密帳戶中 Accelerate 部署 CloudTrail 追蹤的記錄事件。此金鑰由帳戶管理員、AMS Accelerate 運算子和 CloudTrail 控制並可存取。如需 的詳細資訊 AWS KMS，請參閱 AWS Key Management Service 功能產品文件。

存取和稽核 CloudTrail 日誌

AMS Accelerate 部署的 CloudTrail 追蹤的 CloudTrail 日誌會存放在您帳戶中的 Amazon S3 儲存貯體中。 CloudTrail 存放在 Amazon S3 儲存貯體中的追蹤資料會使用佈建 CloudTrail 資源時建立的 AWS KMS 金鑰進行加密。

Amazon S3 儲存貯體利用 ams-***aaws ## id***-cloudtrail-***AWS ###***命名模式 （ 例如：ams-a123456789-cloudtrail-us-east-1a)，且所有事件都會以 AWS/CloudTrail 字首存放。系統會記錄主儲存貯體的所有存取權，並加密日誌物件並進行版本控制，以供稽核之用。

如需追蹤變更和查詢日誌的詳細資訊，請參閱 追蹤 AMS Accelerate 帳戶中的變更。

保護和保留 CloudTrail 日誌

AMS Accelerate 為 Accelerate 部署的 CloudTrail 追蹤啟用具有控管模式的 Amazon S3 物件鎖定，以確保使用者在沒有特殊許可的情況下，無法覆寫或刪除物件版本或更改其鎖定設定。如需詳細資訊，請參閱 Amazon S3 物件鎖定。

根據預設，此儲存貯體中的所有日誌都會無限期保留。如果您想要變更保留期間，您可以透過 AWS 支援 中心提交服務請求，以設定不同的保留政策。

存取 Amazon EC2 日誌

您可以使用 存取 Amazon EC2 執行個體日誌 AWS Management Console。執行個體 AWS 和服務產生的日誌可在 CloudWatch Logs 中使用，該日誌可在 AMS Accelerate 管理的每個帳戶中使用。如需有關存取日誌的資訊，請參閱 CloudWatch Logs 文件。

保留 Amazon EC2 日誌

根據預設，Amazon EC2 執行個體日誌會無限期保留。如果您想要變更保留期間，您可以透過 AWS 支援 中心提交服務請求，以設定不同的保留政策。

日誌管理 — Amazon EC2

AMS Accelerate 會在您已識別為 AMS Accelerate 受管的所有 Amazon EC2 執行個體上安裝 CloudWatch 代理程式。此代理程式會將系統層級日誌傳送至 Amazon CloudWatch Logs。如需詳細資訊，請參閱什麼是 Amazon CloudWatch Logs？

下列日誌檔案會傳送至 CloudWatch Logs，並傳送至與日誌同名的日誌群組。在每個日誌群組中，會為每個 Amazon EC2 執行個體建立日誌串流，根據 Amazon EC2 執行個體 ID 命名。

Linux

- /var/log/amazon/ssm/amazon-ssm-agent.log
- /var/log/amazon/ssm/errors.log
- /var/log/audit/audit.log
- /var/log/auth.log
- /var/log/cloud-init-output.log
- /var/log/cron
- /var/log/dnf.log
- /var/log/dpkg.log
- /var/log/maillog
- /var/log/messages
- /var/log/secure

- /var/log/spooler
- /var/log/syslog
- /var/log/yum.log
- /var/log/zypper.log

如需詳細資訊，請參閱手動建立或編輯 CloudWatch 代理程式組態檔案。

Windows

- AmazonSSMAgentLog
- AmazonCloudWatchAgentLog
- AmazonSSMErrorLog
- AmazonCloudFormationLog
- ApplicationEventLog
- EC2ConfigServiceEventLog
- MicrosoftWindowsAppLockerEXEAndDLLEventLog
- MicrosoftWindowsAppLockerMSIAndScriptEventLog
- MicrosoftWindowsGroupPolicyOperationalEventLog
- SecurityEventLog
- SystemEventLog

如需詳細資訊，請參閱 Quick Start：啟用執行 Windows Server 2016 的 Amazon EC2 執行個體，以使用 CloudWatch Logs 代理程式將日誌傳送至 CloudWatch Logs。

日誌管理 — Amazon VPC 流程日誌

VPC 流程日誌是一項功能，可擷取進出 VPC 中網路介面之 IP 流量的相關資訊。流程日誌資料可以發佈到 Amazon CloudWatch logs或 Amazon S3。流程日誌資料收集不會影響網路輸送量或延遲。您可以建立或刪除流程日誌，而不會影響網路效能。

流量日誌可協助您處理多項任務，例如：

- 診斷過於嚴格的安全群組規則
- 監控到達執行個體的流量

- 判斷網路介面往來流量的方向

您不需要為 Accelerate 帳戶中每個新建立的 VPC 啟用 VPC 流程日誌。AMS 會使用 ams-nist-cis-vpc-flow-logs-enabled Config 規則，自動偵測 VPC 是否有流程日誌。如果未啟用 VPC 流程日誌，AMS 將透過使用自訂欄位建立 VPC 流程日誌來自動修復它。擁有這些額外的欄位可讓 AMS 和客戶更妥善地監控 VPC 流量、了解網路相依性、疑難排解網路連線問題，以及識別網路威脅。

如需檢視和搜尋流程日誌的資訊，請參閱使用流程日誌。

追蹤 AMS Accelerate 帳戶中的變更

Important

自 2025 年 7 月 1 日起，變更記錄服務已棄用。
新帳戶無法加入變更記錄服務。
若要查詢 AMS Accelerate 帳戶中的 CloudTrail 資料，您可以使用這些服務：

- 在 中 AWS CloudTrail，選擇事件歷史記錄，並使用查詢屬性篩選事件。您可以使用時間範圍篩選條件，並選擇依`s3.amazon.aws.com`指定事件來源篩選事件歷史記錄，或選擇依使用者名稱篩選事件歷史記錄。如需詳細資訊，請參閱使用 CloudTrail 事件歷史記錄。
- 使用 AWS CloudTrail Lake 透過查詢收集資料。在 AWS CloudTrail 選擇 Lake 中，然後選擇查詢。您可以建立自己的查詢、使用查詢產生器，或使用範例查詢來收集事件型資料。例如，您可以詢問過去一週誰刪除了 Amazon EC2 執行個體。如需詳細資訊，請參閱從 AWS CloudTrail 來源建立資料湖和 CloudTrailLake 查詢。
- 在 中建立 Amazon Athena 資料表， AWS CloudTrail 並將儲存位置設定為與您的線索相關聯的 Amazon S3 儲存貯體。確認您的線索和 Amazon S3 儲存貯體的主區域相同。在 Amazon Athena 中，使用查詢編輯器執行 Accelerate 提供的預設查詢，以搭配 Athena 主控台使用。如需如何建立 Athena 資料表以查詢 CloudTrail 日誌的詳細資訊，請參閱查詢 AWS CloudTrail 日誌。

主題

AWS Managed Services 透過使用 Amazon Athena (Athena) 主控台和 AMS Accelerate 日誌管理提供可查詢的界面，協助您追蹤 AMS Accelerate Operations 團隊和 AMS Accelerate 自動化所做的變更。

Athena 是一種互動式查詢服務，您可以使用標準結構化查詢語言 (SQL) 來分析 Amazon S3 中的資料（請參閱 Amazon Athena 的 SQL 參考）。Athena 無伺服器，所以不需管理基礎設施，而且您只需支付所執行查詢的費用。AMS Accelerate 會透過 CloudTrail 日誌建立具有每日分割區的 Athena 資料表，並在主要 AWS 區域和 ams-change-record 工作群組中提供查詢。您可以選擇任何預設查詢，並視需要執行它們。若要進一步了解 Athena 工作群組，請參閱工作群組的運作方式。

> **Note**
>
> 只有 Accelerate 可以在 Accelerate 與您的 CloudTrail Organization trail 整合時，使用 Athena 查詢您 Accelerate 帳戶的 CloudTrail 事件，除非您的 Organization 管理員在加入期間部署了 IAM 角色以使用 Athena 查詢和分析您帳戶中的 CloudTrail 事件。

使用變更記錄，您可以輕鬆回答以下問題：

- 誰 (AMS Accelerate Systems 或 AMS Accelerate Operators) 已存取您的帳戶
- AMS Accelerate 在您帳戶中所做的變更
- AMS Accelerate 何時在您的帳戶中執行變更
- 在何處檢視您帳戶中所做的變更
- 為什麼 AMS Accelerate 需要在您的帳戶中進行變更
- 如何修改查詢，以取得所有非 AMS 變更問題的答案

檢視您的變更記錄

若要使用 Athena 查詢，請登入 AWS 管理主控台，然後導覽至主要 AWS 區域中的 Athena 主控台。

> **Note**
>
> 如果您在執行任何步驟時看到 Amazon Athena 入門頁面，請按一下入門。即使您的變更記錄基礎設施已就緒，這也可能會為您顯示。

1. 從 Athena 主控台的上方導覽面板中選擇工作群組。
2. 選擇 ams-change-record 工作群組，然後按一下切換工作群組。
3. 從資料庫組合方塊中選擇 ams-change-record-database。ams-change-record-database 包含 ams-change-record-table 資料表。
4. 從上方導覽面板中選擇已儲存的查詢。
5. 儲存的查詢視窗會顯示 AMS Accelerate 提供的查詢清單，您可以執行。從已儲存的查詢清單中選擇您要執行的查詢。例如，ams_session_accesses_v1 查詢。

   如需預設 AMS Accelerate 查詢的完整清單，請參閱 預設查詢。

6. 視需要調整查詢編輯器方塊中的日期時間篩選條件；預設情況下，查詢只會檢查從最後一天以來的變更。
7. 選擇 Run query (執行查詢)。

預設查詢

AMS Accelerate 提供數個您可以在 Athena 主控台中使用的預設查詢。預設查詢會列在下表中。

> **Note**
>
> - 所有查詢都接受日期範圍做為選用篩選條件；所有查詢預設會在過去 24 小時內執行。如需預期的輸入，請參閱下列小節：修改查詢中的日期時間篩選條件。
> - 您可以或需要變更的參數輸入會在查詢中顯示為具有角括號的 *<PARAMETER_NAME>*。將預留位置和角括號取代為您的參數值。
> - 所有篩選條件都是選用的。在查詢中，某些選用篩選條件會在行開頭以雙破折號 (--) 標註。所有查詢都會在沒有它們的情況下執行，並使用預設參數。如果您想要指定這些選用篩選條件的參數值，請移除行開頭的雙破折號 (--)，並視需要取代 參數。
> - 所有查詢都會在輸出`IAM SessionId`中傳回 `IAM PincipalId`和
> - 執行查詢的計算成本取決於為帳戶產生多少 CloudTrail 日誌。若要計算成本，請使用 AWS Athena 定價計算器。

標準查詢

目的/描述	輸入	Outputs
查詢名稱： `ams_access_session_query_v1`		
追蹤 AMS Accelerate 存取工作階段 提供特定 AMS Accelerate 存取工作階段的相關資訊。查詢接受 IAM Principal ID 做為選用篩選條件，並傳回事件時間、	（選用） `IAM PrincipalId` ：嘗試存取之資源的 IAM Principal 識別符。格式為 *`UNIQUE_ID ENTIFIER`* ：*`RESOURCE_NAME`* 。如需詳細資訊，請參閱唯一識別符。您	• EventTime：取得存取權的時間 • EventName：AWS 事件名稱 (AssumeRole) • EventRegion：取得請求的 AWS 區域 • EventId：CloudTrail 事件 ID

目的/描述	輸入	Outputs
存取帳戶的商業需求、請求者等。 您可以取消註解行，並在查詢編輯器中將預留位置 IAM *PrincipalId ##### ID###### IAM Principal* ID。 您也可以在查詢的 WHERE 子句中移除使用者代理程式篩選列，以列出非 AMS 存取工作階段。	可以在沒有此篩選條件的情況下執行查詢，以決定您要篩選的確切 IAM PrincipalId。	• BusinessNeed 類型：存取帳戶的商業原因類型。允許的值為：SupportCase、OpsItem、 Issue、 Text。 • BusinessNeed：企業需要存取帳戶。例如，支援案例 ID、Ops 項目 ID 等。 • 申請者：存取帳戶的運算子 ID，或存取帳戶的自動化系統。 • RequestAccessType：申請者類型 (System、OpsConsole、OpsAPI、Unset)
查詢名稱： ams_events_query_v1		
追蹤 AMS Accelerate 完成的所有變動動作 傳回使用該 AMS Accelerate 角色篩選條件對帳戶執行的所有寫入動作。 您也可以從查詢的 WHERE 子句中移除 useridentity.arn 篩選條件行，追蹤非 AMS 角色完成的變動動作。	(選用) 僅限日期時間範圍。請參閱 修改查詢中的日期時間篩選條件。	• AccountId：AWS 帳戶 ID • RoleArn：申請者的 RoleArn • EventTime：取得存取權的時間 • EventName：AWS 事件名稱 (AssumeRole) • EventRegion：取得請求的 AWS 區域 • EventId：CloudTrail 事件 ID • RequestParameters ：請求的參數 • ResponseElements：回應的回應元素。 • UserAgent：AWS CloudTrail 使用者代理程式
查詢名稱： ams_instance_access_sessions_query_v1		

目的/描述	輸入	Outputs
透過 AMS Accelerate 追蹤執行個體存取 傳回 AMS Accelerate 執行個體存取的清單；每個記錄都包含事件時間、事件區域、執行個體 ID、IAM Principal ID、IAM 工作階段 ID、SSM 工作階段 ID。您可以使用 IAM Principal ID，透過 `ams_access_sessions_query_v1` Athena 查詢取得存取執行個體之業務需求的更多詳細資訊。您可以使用 SSM 工作階段 ID 取得執行個體存取工作階段的詳細資訊，包括工作階段的開始和結束時間、日誌詳細資訊，以及使用執行個體 AWS 區域中的 AWS Session Manager 主控台。 使用者也可以透過移除查詢的 WHERE 子句中的 useridentity 篩選列來列出非 AMS 執行個體存取。	僅有 `datetime range`。請參閱 修改查詢中的日期時間篩選條件。	• InstanceId：執行個體 ID • SSMSession ID：SSM 工作階段 ID • RoleArn：申請者的 RoleArn • EventTime：取得存取權的時間 • EventName：AWS 事件名稱 (AssumeRole) • EventRegion：取得請求的 AWS 區域 • EventId：CloudTrail 事件 ID
查詢名稱：`ams_privilege_escalation_events_query_v1`		

目的/描述	輸入	Outputs
追蹤 AMS 和非 AMS 使用者的許可（呈報）事件 提供可直接或可能導致權限提升的事件清單。查詢接受 ActionedBy 作為選用篩選條件，並傳回 EventName、EventId、EventTime 等。也會傳回與事件相關聯的所有欄位。如果不適用於該事件，則欄位為空白。ActionedBy 篩選條件預設為停用；若要啟用，請從該行移除 "--"。 根據預設，ActionedBy 篩選條件已停用（它會顯示來自所有使用者的權限提升事件）。若要顯示特定使用者或角色的事件，請從 WHERE 子句中的使用者身分篩選列中移除雙破折號 (--)，並將預留位置 *ACTIONEDBY_PUT_USER_NAME_HERE* 取代為 IAM 使用者或角色名稱。您可以在沒有篩選條件的情況下執行查詢，以決定要篩選的確切使用者。	（選用）`ACTIONEDBY_PUT_USER_NAME`：actionedBy 使用者的使用者名稱。可以是 IAM 使用者或角色。例如，ams-access-admin。 （選用）`datetime range`。請參閱 修改查詢中的日期時間篩選條件。	• AccountId：帳戶 ID • ActionedBy：ActionedBy 使用者名稱 • EventTime：取得存取權的時間 • EventName：AWS 事件名稱 (AssumeRole)。 • EventRegion：取得請求的 AWS 區域 • EventId：CloudTrail 事件 ID
查詢名稱：`ams_resource_events_query_v1`		

目的/描述	輸入	Outputs
追蹤特定資源 AMS 或非 AMS 的寫入事件 提供在特定資源上完成的事件清單。查詢接受資源 ID 做為篩選條件的一部分（在查詢的 WHERE 子句中取代預留位置 *RESOURCE_INFO* ），並傳回對該資源執行的所有寫入動作。	（必要）RESOURCE_INFO ：資源識別符，可以是帳戶中任何 AWS 資源的 ID。請勿將此與資源 ARNs 混淆。例如，EC2 執行個體的執行個體 ID、DynamoDB 資料表的資料表名稱、CloudWatch Log 的 logGroupName 等。 （選用）datetime range。請參閱 修改查詢中的日期時間篩選條件。	• AccountId：帳戶 ID • ActionedBy：ActionedBy 使用者名稱 • EventTime：取得存取權的時間 • EventName：AWS 事件名稱 (AssumeRole)。 • EventRegion：取得請求的 AWS 區域 • EventId：CloudTrail 事件 ID
查詢名稱： ams_session_events_query_v1		
追蹤 AMS Accelerate 在特定工作階段期間執行的寫入動作 提供在特定工作階段上完成的事件清單。查詢接受 IAM Principal ID 做為篩選條件的一部分（在查詢的 WHERE 子句中取代預留位置 *PRINCIPAL_ID* ），並傳回對該資源執行的所有寫入動作。	（必要）PRINCIPAL_ID ：工作階段的主體 ID。格式為 *UNIQUE_ID ENTIFIER* ：*RESOURCE_NAME* 。如需詳細資訊，請參閱唯一識別符。您可以執行查詢 "ams_session_ids_by_requester_v1"，以取得申請者的 IAM 主體 IDs 清單。您也可以在沒有此篩選條件的情況下執行查詢，以決定要篩選的確切 IAM PrincipalId。 （選用）datetime range。請參閱 修改查詢中的日期時間篩選條件。	• AccountId：帳戶 ID • ActionedBy：ActionedBy 使用者名稱 • EventTime：取得存取權的時間 • EventName：AWS 事件名稱 (AssumeRole) • EventRegion：取得請求的 AWS 區域 • EventId：CloudTrail 事件 ID

目的/描述	輸入	Outputs
查詢名稱： ams_session_ids_by_requester_v1		
追蹤特定請求者的 IAM 主體/工作階段 IDs。 查詢接受「請求者」（在查詢的 WHERE 子句中取代預留位置###），並在指定的時間範圍內傳回該請求者的所有 IAM 主體 ID。	（必要） Requester ：存取帳戶的運算子 ID （例如：運算子的別名），或存取帳戶的自動化系統（例如：OsConfiguration、AlarmManager 等）。 （選用） datetime range。請參閱 修改查詢中的日期時間篩選條件。	• IAM PrincipalId - 工作階段的 IAM Principal ID。格式為 *UNIQUE_ID ENTIFIER* ：*RESOURCE_NAME* 。如需詳細資訊，請參閱唯一識別符。您可以在沒有此篩選條件的情況下執行查詢，以決定要篩選的確切 IAM PrincipalId。 • IAM SessionId - 存取工作階段的 IAM 工作階段 ID • EventTime：取得存取權的時間

修改查詢中的日期時間篩選條件

所有查詢都接受日期範圍做為選用篩選條件。根據預設，所有查詢都會在過去一天執行。

用於日期時間欄位的格式為 yyyy/MM/dd （例如：2021/01/01)。請記住，它只會存放日期，而不是整個時間戳記。對於整個時間戳記，請使用 欄位平衡時間，其會將時間戳記以 ISO 8601 格式 yyyy-MM-ddT HH：mm：ssZ （例如：2021-01-01T23：59：59Z) 存放。不過，由於資料表在日期時間欄位上進行分割，因此您需要同時將日期時間和事件時間篩選條件傳遞至查詢。請參閱以下範例。

> **Note**
>
> 若要查看修改範圍的所有已接受方法，請參閱目前用於日期和時間函數和運算子的 Athena 引擎版本的最新 Presto 函數文件，以查看修改範圍的所有已接受方法。

日期層級：過去 1 天或過去 24 小時 （預設） 範例：如果 CURRENT_DATE='2021/01/01'，篩選條件會從目前日期減去一天，並將其格式化為日期時間 > '2020/12/31'

```
datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
```

日期層級：過去 2 個月範例：

```
datetime > date_format(date_add('month', - 2, CURRENT_DATE), '%Y/%m/%d')
```

日期層級：介於 2 個日期之間範例：

```
datetime > '2021/01/01'
      AND
      datetime < '2021/01/10'
```

時間戳記層級：過去 12 小時範例：

掃描到過去 1 天的分割區資料，然後篩選過去 12 小時內的所有事件

```
datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND
      eventtime > date_format(date_add('hour', - 12, CURRENT_TIMESTAMP), '%Y-%m-%dT%H:
%i:%sZ')
```

時間戳記層級：介於 2 個時間戳記之間範例：

取得 2021 年 1 月 1 日中午 12：00 到 2021 年 1 月 10 日下午 3：00 之間的事件。

```
datetime > '2021/01/01' AND datetime < '2021/01/10'
      AND
      eventtime > '2021-01-01T12:00:00Z' AND eventtime < '2021-01-10T15:00:00Z'
```

預設查詢範例

ams_access_session_query_v1

```
Name: ams_access_session_query_v1

Description: >-
   The query provides more information on specific AMS access session.
   The query accepts IAM Principal Id as an optional filter and returns event time,
 business need for accessing the account, requester, ... etc.
   By default; the query filter last day events only, the user can change the datetime
 filter to search for more wide time range.
   By default; the IAM PrincipalId filter is disabled. To enable it, remove "-- " from
 that line.

AthenaQueryString: |-
```

```
  /*
    The query provides list of AMS access sessions during specific time range.
    The query accepts IAM Principal Id as an optional filter and returns event time,
business need for accessing the account, requester, ... etc.

    By default, the query filters the last day's events only; you can change the
"datetime" filter to search for a wider time range.

    By default; the IAM Principal ID filter is disabled (it shows access sessions for
all IAM principals).
    If you want to only show access sessions for a particular IAM principal ID, remove
the double-dash (--) from
    the "IAM Principal ID" filter line in the WHERE clause of the query, and replace
the placeholder "<IAM PrincipalId>" with the specific ID that you want.
    You can run the query without the filter to determine the exact IAM PrincipalId
you want to filter with.

    By default; the query only shows AMS access sessions. If you also want to show
non-AMS access sessions,
    remove the "useragent" filter in the WHERE clause of the query.

    For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
in your AMS Accelerate accounts -> Default Queries
  */

  SELECT
     json_extract_scalar(responseelements, '$.assumedRoleUser.assumedRoleId') AS "IAM
PrincipalId",
     json_extract_scalar(responseelements, '$.credentials.accessKeyId') AS "IAM
SessionId",
     eventtime AS "EventTime",
     eventname AS "EventName",
     awsregion AS "EventRegion",
     eventid AS "EventId",
     json_extract_scalar(requestparameters, '$.tags[0].value') AS "BusinessNeed",
     json_extract_scalar(requestparameters, '$.tags[1].value') AS "BusinessNeedType",
     json_extract_scalar(requestparameters, '$.tags[2].value') AS "Requester",
     json_extract_scalar(requestparameters, '$.tags[3].value') AS "AccessRequestType"
  FROM
      "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
  WHERE
     datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
     AND eventname = 'AssumeRole'
     AND useragent = 'access.managedservices.amazonaws.com'
```

```
      -- AND  json_extract_scalar(responseelements, '$.assumedRoleUser.assumedRoleId')
 = '<IAM PrincipalId>'
   ORDER BY eventtime

InsightsQueryString: |-
   # The query provides list of AMS access sessions during specific time range.
   # The query accepts IAM Principal Id as an optional filter and returns event time,
 business need for accessing the account, requester, ... etc.
   #
   # By default; the IAM Principal ID filter is disabled (it shows access sessions for
 all IAM principals).
   # If you want to only show access sessions for a particular IAM principal ID, remove
 the # (#) from
   # the "IAM Principal ID" filter of the query, and replace the placeholder "<IAM
 PrincipalId>" with the specific ID that you want.
   # You can run the query without the filter to determine the exact IAM PrincipalId
 you want to filter with.
   #
   # By default; the query only shows AMS access sessions. If you also want to show
 non-AMS access sessions,
   # remove the "useragent" filter from the query.
   #
   # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries

   filter eventName="AssumeRole" AND userAgent="access.managedservices.amazonaws.com"
   # | filter responseElements.assumedRoleUser.assumedRoleId= "<IAM PrincipalId>"
   | sort eventTime desc
   | fields
      responseElements.assumedRoleUser.assumedRoleId as IAMPrincipalId,
      responseElements.credentials.accessKeyId as IAMSessionId,
      eventTime as EventTime,
      eventName as EventName,
      awsRegion as EventRegion,
      eventID as EventId,
      requestParameters.tags.0.value as BusinessNeed,
      requestParameters.tags.1.value as BusinessNeedType,
      requestParameters.tags.2.value as Requester,
      requestParameters.tags.3.value as AccessRequestType
```

ams_events_query_v1

```
ams_events_query_v1.yaml
/*
  The query provides list of events to track write actions for all AMS changes.
  The query returns all write actions done on the account using that AMS role filter.

  By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

  You can also track mutating actions done by non-AMS roles by removing the
 "useridentity.arn" filter lines from the WHERE clause of the query.

  For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes in
 your AMS Accelerate accounts -> Default Queries
*/

SELECT
   useridentity.principalId AS "IAM PrincipalId",
   useridentity.accesskeyid AS "IAM SessionId",
   useridentity.accountid AS "AccountId",
   useridentity.arn AS "RoleArn",
   eventid AS "EventId",
   eventname AS "EventName",
   awsregion AS "EventRegion",
   eventsource AS "EventService",
   eventtime AS "EventTime",
   requestparameters As "RequestParameters",
   responseelements AS "ResponseElements",
   useragent AS "UserAgent"
FROM
   "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
WHERE
   readonly <> 'true'
   AND
   (
      LOWER(useridentity.arn) LIKE '%/ams%'
      OR LOWER(useridentity.arn) LIKE '%/customer_ssm_automation_role%'
   )
ORDER BY eventtime
```

ams_instance_access_sessions_query_v1

```
ams_instance_access_sessions_query_v1
/*
  The query provides list of AMS Instance accesses during specific time range.

  The query returns the list of AMS instance accesses; every record includes the event
 time, the event AWS Region, the instance ID, the IAM session ID, and the SSM session
 ID.
  You can use the IAM Principal ID to get more details on the business need for
 accessing the instance by using ams_access_session_query_v1 athena query.
  You can use the SSM session ID to get more details on the instance access session,
 including the start and end time of the session and log details, using the AWS Session
 Manager Console in the instance's AWS Region.

  You can also list non-AMS instance accesses by removing the "useridentity" filter
 line in the WHERE clause of the query.

  By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

  For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes in
 your AMS Accelerate accounts -> Default Queries
*/

SELECT
   useridentity.principalId AS "IAM PrincipalId",
   useridentity.accesskeyid AS "IAM SessionId",
   json_extract_scalar(requestparameters, '$.target') AS "InstanceId",
   json_extract_scalar(responseelements, '$.sessionId') AS "SSM SessionId",
   eventname AS "EventName",
   awsregion AS "EventRegion",
   eventid AS "EventId",
   eventsource AS "EventService",
   eventtime AS "EventTime"
FROM
   "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
WHERE
   useridentity.sessionContext.sessionIssuer.arn like '%/ams_%'
   AND eventname = 'StartSession'
ORDER BY eventtime
```

ams_privilege_escalation_events_query_v1

```
ams_privilege_escalation_events_query_v1.yaml
/*
  The query provides list of events that can directly or potentially lead to a
 privilege escalation.

  The query accepts ActionedBy as an optional filter and returns EventName, EventId,
 EventTime, ... etc.
  All fields associated with the event are also returned. Some fields are blank if not
 applicable for that event.
  You can use the IAM Session ID to get more details about events happened in that
 session by using ams_session_events_query_v1 query.

  By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

  By default, the ActionedBy filter is disabled (it shows privilege escalation events
 from all users).
  To show events for a particular user or role, remove the double-dash (--) from the
 useridentity filter line in the WHERE clause of the query
  and replace the placeholder "<ACTIONEDBY_PUT_USER_NAME_HERE>" with an IAM user or
 role name.
  You can run the query without the filter to determine the exact user you want to
 filter with.

  For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes in
 your AMS Accelerate accounts -> Default Queries
*/

SELECT
   useridentity.principalId AS "IAM PrincipalId",
   useridentity.accesskeyid AS "IAM SessionId",
   useridentity.accountid AS "AccountId",
   reverse(split_part(reverse(useridentity.arn), ':', 1)) AS "ActionedBy",
   eventname AS "EventName",
   awsregion AS "EventRegion",
   eventid AS "EventId",
   eventtime AS "EventTime",
   json_extract_scalar(requestparameters, '$.userName') AS "UserName",
   json_extract_scalar(requestparameters, '$.roleName') AS "RoleName",
   json_extract_scalar(requestparameters, '$.groupName') AS "GroupName",
   json_extract_scalar(requestparameters, '$.policyArn') AS "PolicyArn",
   json_extract_scalar(requestparameters, '$.policyName') AS "PolicyName",
```

```
   json_extract_scalar(requestparameters, '$.permissionsBoundary') AS
 "PermissionsBoundary",
   json_extract_scalar(requestparameters, '$.instanceProfileName') AS
 "InstanceProfileName",
   json_extract_scalar(requestparameters, '$.openIDConnectProviderArn') AS
 "OpenIDConnectProviderArn",
   json_extract_scalar(requestparameters, '$.serialNumber') AS "SerialNumber",
   json_extract_scalar(requestparameters, '$.serverCertificateName') AS
 "ServerCertificateName",
   json_extract_scalar(requestparameters, '$.accessKeyId') AS "AccessKeyId",
   json_extract_scalar(requestparameters, '$.certificateId') AS "CertificateId",
   json_extract_scalar(requestparameters, '$.newUserName') AS "NewUserName",
   json_extract_scalar(requestparameters, '$.newGroupName') AS "NewGroupName",
   json_extract_scalar(requestparameters, '$.newServerCertificateName') AS
 "NewServerCertificateName",
   json_extract_scalar(requestparameters, '$.name') AS "SAMLProviderName",
   json_extract_scalar(requestparameters, '$.sAMLProviderArn') AS "SAMLProviderArn",
   json_extract_scalar(requestparameters, '$.sSHPublicKeyId') AS "SSHPublicKeyId",
   json_extract_scalar(requestparameters, '$.virtualMFADeviceName') AS
 "VirtualMFADeviceName"
FROM
   "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
WHERE
   (
     -- More event names can be found at https://docs.aws.amazon.com/IAM/latest/
UserGuide/list_identityandaccessmanagement.html
     eventname LIKE 'Add%' OR
     eventname LIKE 'Attach%' OR
     eventname LIKE 'Delete%' AND eventname != 'DeleteAccountAlias' OR
     eventname LIKE 'Detach%' OR
     eventname LIKE 'Create%' AND eventname != 'CreateAccountAlias' OR
     eventname LIKE 'Put%' OR
     eventname LIKE 'Remove%' OR
     eventname LIKE 'Update%' OR
     eventname LIKE 'Upload%' OR
     eventname = 'DeactivateMFADevice' OR
     eventname = 'EnableMFADevice' OR
     eventname = 'ResetServiceSpecificCredential' OR
     eventname = 'SetDefaultPolicyVersion'
   )
   AND eventsource = 'iam.amazonaws.com'
ORDER BY eventtime
```

ams_resource_events_query_v1

```
Name: ams_resource_events_query_v1

Description: >-
   The query provides list of events done on specific resource.
   The query accepts resource id as part of the filters, and return all write actions
 done on that resource.
   By default; the query list the accesses for last day, the user can change the time
 range by changing the datetime filter.

AthenaQueryString: |-
   /*
     The query provides list of events done on specific resource.

     The query accepts the resource ID as part of the filters (replace the placeholder
 "<RESOURCE_INFO>" in the WHERE clause of the query),
     and returns all write actions done on that resource. The resource ID can be an ID
 for any AWS resource in the account.
     Example: An instance ID for an EC2 instance, table name for a DynamoDB table,
 logGroupName for a CloudWatch Log, etc.

     By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

     For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
   */

   SELECT
      useridentity.principalId AS "IAM PrincipalId",
      useridentity.accesskeyid AS "IAM SessionId",
      useridentity.accountid AS "AccountId",
      reverse(split_part(reverse(useridentity.arn), ':', 1)) AS "ActionedBy",
      eventname AS "EventName",
      awsregion AS "EventRegion",
      eventid AS "EventId",
      eventsource AS "EventService",
      eventtime AS "EventTime"
   FROM
       "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
   WHERE
      datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND readonly <> 'true'
```

```
      AND
      (
         requestparameters LIKE '%<RESOURCE_INFO>%'
         OR responseelements LIKE '%<RESOURCE_INFO>%'
      )
   ORDER BY eventtime

InsightsQueryString: |-
   # The query provides list of events done on specific resource.
   #
   # The query accepts the resource ID as part of the filters (replace the placeholder
 "<RESOURCE_INFO>" in the filter of the query),
   # and returns all write actions done on that resource. The resource ID can be an ID
 for any AWS resource in the account.
   # Example: An instance ID for an EC2 instance, table name for a DynamoDB table,
 logGroupName for a CloudWatch Log, etc.
   #
   # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries

   filter readOnly=0
   | parse @message '"requestParameters":{*}' as RequestParameters
   | parse @message '"responseElements":{*}' as ResponseElements
   # | filter RequestParameters like "RESOURCE_INFO" or ResponseElements like
 "<RESOURCE_INFO>"
   | fields
      userIdentity.principalId as IAMPrincipalId,
      userIdentity.accessKeyId as IAMSessionId,
      userIdentity.accountId as AccountId,
      userIdentity.arn as ActionedBy,
      eventName as EventName,
      awsRegion as EventRegion,
      eventID as EventId,
      eventSource as EventService,
      eventTime as EventTime
   | display IAMPrincipalId, IAMSessionId, AccountId, ActionedBy, EventName,
 EventRegion, EventId, EventService, EventTime
   | sort eventTime desc
```

ams_session_events_query_v1

```
Name: ams_session_events_query_v1
```

```
Description: >-
   The query provides list of events done on specific session.
   The query accepts IAM Principal Id as part of the filters, and return all write
 actions done on that resource.
   By default; the query list the accesses for last day, the user can change the time
 range by changing the datetime filter.

AthenaQueryString: |-
   /*
     The query provides a list of events executed on a specific session.

     The query accepts the IAM principal ID as part of the filters (replace the
 placeholder "<PRINCIPAL_ID>" in the WHERE clause of the query),
     and returns all write actions done on that resource.

     By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

     For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
   */

   SELECT
      useridentity.principalId AS "IAM PrincipalId",
      useridentity.accesskeyid AS "IAM SessionId",
      useridentity.accountid AS "AccountId",
      reverse(split_part(reverse(useridentity.arn), ':', 1)) AS "ActionedBy",
      eventname AS "EventName",
      awsregion AS "EventRegion",
      eventsource AS "EventService",
      eventtime AS "EventTime",
      requestparameters As "RequestParameters",
      responseelements AS "ResponseElements",
      useragent AS "UserAgent"
   FROM
       "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate   WHERE
      useridentity.principalid = '<PRINCIPAL_ID>'
      AND datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND readonly <> 'true'
   ORDER BY eventtime

InsightsQueryString: |-
   # The query provides a list of events executed on a specific session.
   #
```

```
  # The query accepts the IAM principal ID as part of the filters (replace the
placeholder "<PRINCIPAL_ID>" in the filter of the query),
  # and returns all write actions done on that resource.
  #
  # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
in your AMS Accelerate accounts -> Default Queries

  filter readOnly=0 AND userIdentity.principalId = "<IAM Principal>"
  | sort eventTime desc
  | fields
     userIdentity.accessKeyId as IAMSessionId,
     userIdentity.principalId as IAMPrincipalId,
     userIdentity.accountId as AccountId,
     userIdentity.arn as ActionedBy,
     eventName as EventName,
     awsRegion as EventRegion,
     eventSource as EventService,
     eventTime as EventTime,
     userAgent as UserAgent
  | parse @message '"requestParameters":{*}' as RequestParameters
  | parse @message '"responseElements":{*}' as ResponseElements
```

ams_session_ids_by_requester_v1

```
Name: ams_session_ids_by_requester_v1

Description: >-
   The query provides list of IAM Principal/Session Ids for specific requester.
   The query accepts requester and return all IAM Principal/Session Ids by that
 requester during specific time range.
   By default; the query list the accesses for last day, the user can change the time
 range by changing the datetime filter.

AthenaQueryString: |-
   /*
     The query provides list of IAM Principal IDs for a specific requester.

     The query accepts the requester (replace placeholder "<Requester>" in the WHERE
 clause of the query),
     and returns all IAM Principal IDs by that requester during a specific time range.

     By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.
```

```
    For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
   */

   SELECT
      json_extract_scalar(responseelements, '$.assumedRoleUser.assumedRoleId') AS "IAM
 PrincipalId",
      json_extract_scalar(responseelements, '$.credentials.accessKeyId') AS "IAM
 SessionIId",
      eventtime AS "EventTime"
   FROM
       "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
   WHERE
      datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND json_extract_scalar(requestparameters, '$.tags[2].value') = '<Requester>'
   ORDER BY eventtime

InsightsQueryString: |-
   # The query provides list of IAM Principal IDs for a specific requester.
   #
   # The query accepts the requester (replace placeholder "<Requester>" in the filter
 of the query),
   # and returns all IAM Principal IDs by that requester during a specific time range.
   #
   # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
   filter eventName="AssumeRole" AND requestParameters.tags.2.value="<Requester>"
   | sort eventTime desc
   | fields
      responseElements.assumedRoleUser.assumedRoleId as IAMPrincipalId,
      responseElements.credentials.accessKeyId as IAMSessionId,
      eventTime as EventTime
```

變更記錄許可

執行變更記錄查詢需要下列許可：

- Athena
  - athena:GetWorkGroup
  - athena:StartQueryExecution

  - athena:ListDataCatalogs
  - athena:GetQueryExecution
  - athena:GetQueryResults
  - athena:BatchGetNamedQuery
  - athena:ListWorkGroups
  - athena:UpdateWorkGroup
  - athena:GetNamedQuery
  - athena:ListQueryExecutions
  - athena:ListNamedQueries
- AWS KMS
  - kms:解密
  - AWS KMS 如果 Accelerate 使用 CloudTrail 追蹤事件 Amazon S3 儲存貯體資料存放區 （使用 SSE-KMS 加密），則為 AMSCloudTrailLogManagement 的金鑰 ID 或您的 AWS KMS 金鑰 ID。 CloudTrail Amazon S3 https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingKMSEncryption.html
- AWS Glue
  - glue：GetDatabase
  - glue：GetTables
  - glue：GetDatabases
  - glue：GetTable
- Amazon S3 讀取存取
  - Amazon S3 儲存貯體 CloudTrail 資料存放區：ams-a*AccountId*-cloudtrail-*primary region*，或您的 Amazon S3 儲存貯體名稱、CloudTrail 追蹤事件 Amazon S3 儲存貯體資料存放區。
- Amazon S3 寫入存取
  - Athena 事件查詢結果 Amazon S3 儲存貯體：ams-a*AccountId* athena-results-*primary region*

AWS Systems Manager 在 Accelerate 中

AWS Systems Manager 文件 (SSM 文件） 定義 Systems Manager 對 AWS 資源執行的動作。Systems Manager 包含十幾個預先設定的文件，您可以在執行時間指定參數。文件使用 JavaScript 物件標記法 (JSON) 或 YAML，其中包括您指定的步驟和參數。

AWS Managed Services (AMS) 是 SSM 文件的受信任發佈者。AMS 擁有的 SSM 文件只會與加入的 AMS 帳戶共用，一律以預留字首 (AWSManagedServices-*) 開頭，並在 Systems Manager 主控台中顯示，如 Amazon 所擁有。SSM 文件開發和發佈的 AMS 程序遵循 AWS 最佳實務，並在整個文件生命週期中需要多個對等審核。如需共用 SSM 文件的 AWS 最佳實務的詳細資訊，請參閱共用 SSM 文件的最佳實務。

可用的 AMS Accelerate SSM 文件

AMS Accelerate SSM 文件僅供 AMS Accelerate 客戶使用，用於自動化操作工作流程以操作您的帳戶。

若要從 查看可用的 AMS Accelerate SSM 文件 AWS Management Console：

1. 在AWS Systems Manager 主控台開啟 Systems Manager主控台。
2. 選擇與我共用。
3. 在搜尋列中，依文件名稱字首篩選，然後等於，並將值設定為 AWSManagedServices-。

   如需 AWS CLI 說明，請參閱使用共用的 SSM 文件。

AMS Accelerate SSM 文件版本

SSM 文件支援版本控制。AMS Accelerate SSM 文件無法從客戶的帳戶修改，也無法重新共用。它們由 AMS Accelerate 集中管理和維護，以便操作帳戶。

版本編號會隨著特定 AWS 區域中的每個文件更新而遞增。當新區域可用時，兩個區域中的相同文件內容可以有不同的版本編號；這是典型的，並不表示其行為會有所不同。如果您想要比較兩份 AMS Accelerate SSM 文件，建議您將其雜湊與 進行比較 AWS CLI：

```
aws ssm describe-document \
--name AWSManagedServices-DOCUMENTNAME \
```

```
    --output text --query "Document.Hash"
```

如果兩個 SSM 文件的雜湊相符，則它們是相同的。

Systems Manager 定價

AMS Accelerate SSM 文件存取沒有相關的成本。執行時間成本會根據 SSM 文件的類型、其步驟和執行時間持續時間而有所不同。如需詳細資訊，請參閱 AWS Systems Manager 定價。

AMS Accelerate 使用者指南的文件歷史記錄

下表說明 AMS Accelerate 使用者指南每個版本的重要變更。如需有關此文件更新的通知，您可以訂閱 RSS 訂閱源。

變更	描述	日期
已更新日誌管理 — AWS CloudTrail 區段	有關 AWS CloudTrail 記錄的新資訊和備註。	2025 年 9 月 25 日
新增 4 個受信任修復程式支援的新 Trusted Advisor 成本最佳化檢查	新增下列成本最佳化檢查： • c1z7kmr00n - 執行個體的 Amazon EC2 成本最佳化建議 • c1z7kmr02n - 磁碟區的 Amazon EBS 成本最佳化建議 • c1z7kmr03n - 資料庫執行個體的 Amazon RDS 成本最佳化建議 • c1z7kmr05n - 函數 AWS Lambda 的成本最佳化建議	2025 年 9 月 22 日
更新變更記錄服務的棄用備註	使用替代解決方案更新變更記錄服務的棄用備註。	2025 年 9 月 11 日
更新受信任修復程式支援 Trusted Advisor 的安全性檢查	更新檢查 Hs4Ma3G108 支援的預先設定參數和限制條件 - CloudTrail 追蹤應與 Amazon CloudWatch Logs 整合	2025 年 9 月 5 日
更新受信任修復程式支援 Trusted Advisor 的安全性檢查	已更新 Trusted Advisor 安全檢查以新增 Hs4Ma3G184 第 2 版 - 應啟用 Application Load Balancer 和 Classic Load Balancer 記錄	2025 年 9 月 5 日

更新受信任修復程式區段支援的卓越 Trusted Advisor 營運檢查	已更新 Trusted Remediator 支援的卓越 Trusted Advisor 營運檢查，以新增新的支援檢查 c1fd6b96l4 啟用的 Amazon S3 存取日誌。	2025 年 8 月 28 日
已更新信任的修復程式區段，以包含 Compute Optimizer 的新內容	已更新信任的修復程式區段，以包含支援 AWS Compute Optimizer 建議的新內容。	2025 年 8 月 18 日
TOC 詞彙表連結已移除	AWS 詞彙表。	2025 年 8 月 8 日
TOC 詞彙表連結已移除	AWS 詞彙表。	2025 年 8 月 8 日
修補程式每日報告中的新欄位	執行個體標籤：與 Amazon EC2 執行個體 ID 相關聯的標籤。	2025 年 8 月 8 日

新的信任修復程式檢查	Trusted Advisor Trusted Remediator Hs4Ma3G120–AWSManagedServices-TerminateEC2InstanceStoppedForPeriodOfTime、Hs4Ma3G230–AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV2 和 c18d2gz150–AWSManagedServices-TerminateEC2InstanceStoppedForPeriodOfTime 支援的成本最佳化Trusted Advisor 檢查。Hs4Ma3G120 AWSManagedServices-TerminateEC2InstanceStoppedForPeriodOfTime Hs4Ma3G230AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV2 AWSManagedServices-TerminateEC2InstanceStoppedForPeriodOfTime	2025 年 8 月 8 日
在點 3.2 中更新 IAM 標準	釐清語言並移除提及標記。	2025 年 7 月 25 日
已更新 Accelerate 中的資源交錯器組態設定檔	在 Accelerate 的 Resource Tagger 組態設定檔中新增了新的 AvailabilityZone 篩選條件。	2025 年 7 月 25 日
已更新 Accelerate 中的事件報告、服務請求和帳單問題。	使用服務 SLA 的連結取代對 Plus 和 Premium 服務方案的參考。	2025 年 7 月 25 日
已更新 Accelerate 中的事件管理。	已更新操作中心的相關資訊。	2025 年 7 月 25 日

使用正確的連結更新 AMS 模式頁面。	已修正 SLA 和 SLO 連結。	2025 年 7 月 25 日
更新提醒選擇退出選項	新增標籤可讓您選擇不接收額外的兩個提醒。	2025 年 7 月 25 日
備份的新功能	使用新標籤自訂備份文件庫上的通知。	2025 年 7 月 25 日
已更新 Accelerate 中支援組態的章節	更新 Accelerate 中支援的作業系統和支援的終止支援 (EOS) 作業系統的支援組態。	2025 年 6 月 26 日
已移除頁面 在 Accelerate 中管理修補程式管理的標籤	已移除頁面 在 Accelerate 中管理修補程式管理的標籤，因為此功能已棄用。	2025 年 6 月 19 日
替代修補程式儲存庫的修補程式管理重要安全備註。	在 AMS Accelerate 中使用替代修補程式儲存庫的重要安全注意事項和最佳實務。	2025 年 6 月 10 日
AMS Accelerate 變更記錄棄用。	AMS Accelerate Change Record 服務自 2025 年 7 月 1 日起已棄用。	2025 年 5 月 27 日
支援的作業系統更新。	AMS Accelerate 支援的作業系統已更新，有些已新增，有些已移除。	2025 年 5 月 22 日
中東（阿拉伯聯合大公國）區域支援服務的注意事項。	中東（阿拉伯聯合大公國）區域部分服務的有限支援。	2025 年 5 月 22 日
僅限內部 APIs。	某些 CloudWatch 日誌中出現的僅限APIs。	2025 年 5 月 22 日
新增遺失的日誌位置。	已新增一些缺少的 Windows 日誌位置。	2025 年 5 月 22 日

AMS Accelerate Trusted Remediator 更新。	如何使用新參數 `preconfigured-parameters` 來自訂信任的修復程式中的 Trusted Advisor 檢查。	2025 年 5 月 22 日
AMS Accelerate Trusted Remediator 常見問答集和更新。	支援的 Trusted Advisor 檢查、信任的修復程式常見問答集（新增「信任的修復程式部署到您的帳戶有哪些資源？」）等有幾項更新。另請參閱 Trusted Advisor Trusted Remediator 支援的檢查。	2025 年 5 月 8 日
AMS Accelerate Standard 安全控制更新。	新增「安全群組共用」控制項。	2025 年 5 月 8 日
加速監控提醒更新。	新增其他提醒，以及新增至備註欄的提醒名稱。	2025 年 4 月 28 日
加速資源庫存。	資源庫存試算表檔案（壓縮）已更新。	2025 年 4 月 24 日
加速日誌位置。	已新增其他日誌位置。	2025 年 4 月 24 日
加速安全事件回應的新角色和責任 (RACI)。	安全事件回應的 RACI。	2025 年 3 月 27 日
加速新的 Amazon RDS 自動修復提醒。	警示 ID：- 0224，當請求的已配置儲存達到或超過設定的最大儲存閾值時觸發。	2025 年 3 月 27 日
加速加入角色範本更新。	AMS Accelerate 加入角色範本已更新，以支援 AWS GovCloud 區域。	2025 年 3 月 25 日
加速新的自動修復 RDS 提醒。	已新增 RDS-EVENT-0224。	2025 年 3 月 17 日

加速新功能：事件通知。	您可以使用 AppRegistry 來建立應用程式，並自訂這些應用程式的事件通知。	2025 年 3 月 13 日
加速更新至 RDS 警示監控閾值。	RDS 平均 CPU 使用率警示閾值已從 75% 變更為 90%。	2025 年 2 月 20 日
加速警示資料表的 AMS 自動修復更新。	提醒修補資料表已擴展為新的內容。	2025 年 2 月 20 日
加速新功能：保留警示。	您可以設定警示管理員在 CloudWatch 中保留警示，而不是自動刪除。	2025 年 2 月 20 日
使用彙總報告檢視的新資料選項更新自助式報告	新增資料選項以包含新的欄位名稱：`Admin Account ID`、資料集欄位名稱：`aws_admin_account_id` 和定義：`Trusted AWS Organization account enabled by the customer`適用於下列自助式報告： • 修補程式報告（每日） • 備份報告（每日） • 事件報告（每週） • Resource Tagger 儀表板 • 安全組態規則儀表板	2025 年 1 月 28 日

新增受信任修復程式支援的其他 AWS Trusted Advisor 檢查	Trusted Remediator 現在支援下列 Trusted Advisor 檢查：
	• 成本最佳化
	  • c1cj39rr6v - Amazon S3 不完整的分段上傳中止組態
	• 安全性
	  • Hs4Ma3G199 - RDS 資料庫執行個體應將日誌發佈至 CloudWatch Logs
	  • Hs4Ma3G326 - 應啟用 Amazon EMR 封鎖公開存取設定
	  • Hs4Ma3G272 - 使用者不應具有 SageMaker AI 筆記本執行個體的根存取權
	  • Hs4Ma3G325 - EKS 叢集應該啟用稽核記錄
	  • HHs4Ma3G118 - VPC 預設安全群組不應允許傳入或傳出流量
	  • Hs4Ma3G127 - 應啟用 API Gateway REST 和 WebSocket API 執行記錄
	  • Hs4Ma3G124 - Amazon EC2 執行個體應使用執行個體中繼資料服務第 2 版 (IMDSv2)
	• 容錯能力
	  • c1qf5bt013 - Amazon RDS 資料庫執行個體已關閉儲存體自動擴展
		2025 年 1 月 28 日

- 7qGXsKIUw - Classic Load Balancer 連線耗盡
- c18d2gz106 - Amazon EBS 不包含在 AWS Backup 計劃中
- c18d2gz107 - Amazon DynamoDB 資料表不包含在 AWS Backup計劃中
- cc18d2gz117 - Amazon EFS 不包含在 AWS Backup計劃中
- c18d2gz105 - Network Load Balancer Cross Load Balancing
- c1qf5bt026 - Amazon RDS synchrono us_commit 參數已關閉
- c1qf5bt030 - Amazon RDS innodb_flush_log_a t_trx_commit 參數不是 1
- c1qf5bt031 - Amazon RDS sync_binlog 參數已關閉
- c1qf5bt036 - Amazon RDS innodb_default_row _format 參數設定不安全
- c18d2gz144 - Amazon EC2 詳細監控未啟用

- 操作效能
  - c18d2gz125 - Amazon API Gateway 未記錄執行日誌
  - c18d2gz168 - 負載平衡器未啟用 Elastic

	Load BalancingDeletion Protection • c1qf5bt012 - Amazon RDS 績效詳情已關閉 • 效能 • c1qf5bt021 - 使用低於最佳值的 Amazon RDS innodb_change_buffering 參數 • c1qf5bt025 - Amazon RDS 自動清空參數已關閉 • c1qf5bt028 - Amazon RDS enable_indexonlyscan 參數已關閉 • c1qf5bt029 - Amazon RDS enable_indexscan 參數已關閉 • c1qf5bt032 - 關閉 Amazon RDS innodb_stats_persistent 參數 • c1qf5bt037 - Amazon RDSgeneral_logging 參數已開啟	
已更新資源庫存試算表	已更新資源庫存試算表。	2025 年 1 月 23 日
新的 AMS 功能：彙總自助服務報告	彙總自助式報告 (SSR) 可讓您檢視組織層級跨帳戶彙總的現有自助式報告。	2025 年 1 月 21 日
新的加速修補功能：修補程式掛鉤	使用此功能設定「勾點」搭配 SSM Command 文件，以在修補之前或之後執行作業系統層級命令。	2025 年 1 月 16 日

更新至監控的運作方式區段	新增新功能的相關資訊，依資源或執行個體 ID 而非依事件設定提醒通知。	2025 年 1 月 8 日
EKS 監控和事件管理的加入章節更新	更新加入程序備註，以釐清警示訊號何時暫停和恢復。	2024 年 12 月 19 日
成員帳戶日誌已新增至信任的修復程式	您可以使用成員帳戶日誌來尋找每個成員帳戶的帳戶 ID AWS 區域、加入和執行時間。	2024 年 12 月 19 日
SSM Agent 使用的先決條件	封鎖傳出流量的內容會更新。	2024 年 12 月 4 日
亞太區域（香港）現在支援加速監控和事件管理 EKS AWS 區域	Accelerate Monitoring and Incident Management for EKS 現在支援亞太區域（香港）	2024 年 11 月 21 日
已更新隨需操作方案資料表	就地升級支援下列作業系統： • Microsoft Windows 2016 到 Microsoft Windows 2022 及更高版本	2024 年 11 月 11 日
非洲（開普敦）現在支援加速 EKS 的監控和事件管理 AWS 區域。	非洲（開普敦）現在由 Accelerate Monitoring and Incident Management for EKS 支援	2024 年 11 月 4 日

已更新隨需操作方案資料表	就地升級支援下列作業系統： • Microsoft Windows 2012 R2 到 Microsoft Windows 2016 及更高版本 • Red Hat Enterprise Linux 7 到 Red Hat Enterprise Linux 8 • Red Hat Enterprise Linux 8 到 Red Hat Enterprise Linux 9 • Oracle Linux 7 到 Oracle Linux 8	2024 年 11 月 1 日
更新的 Quick Start 範本	更新圖表、範本參數和 yaml 範本檔案。	2024 年 10 月 28 日

Trusted Advisor 檢查已新增至 AMS 中的信任修復程式	下列 Trusted Advisor 檢查現在可在信任的修復程式中使用： • Z4AUBRNSmz - 未關聯的彈性 IP 地址 • c18d2gz128 - 未設定生命週期政策的 Amazon ECR 儲存庫 • c18d2gz138 - DynamoDB Point-in-time復原 • Hs4Ma3G323 - DynamoDBtables 應該啟用刪除保護 • Hs4Ma3G247 - Amazon EC2 Transit Gateway 不應自動接受 VPC 連接請求 • Hs4Ma3G308 - Amazon DocumentDB 叢集應該啟用刪除保護 • Hs4Ma3G299 - Neptune 資料庫叢集應該啟用刪除保護 • Hs4Ma3G306 - Amazon DocumentDB 手動叢集快照不應公開 • Hs4Ma3G109 - 應啟用 CloudTrail 日誌檔案驗證 • Hs4Ma3G217 - CodeBuild 專案環境應具有記錄 AWS Configuration4 • Hs4Ma3G158 - SSM 文件不應公開 • Hs4Ma3G319 - Network Firewall 防火牆應該已啟用刪除保護	2024 年 10 月 25 日

已更新支援的組態	將支援的 Oracle Linux 作業系統更新為 9.0-9.3、8.0-8.9、7.5-7.9。	2024 年 10 月 24 日
從 AMS Accelerate 新增至 Offboard 的新區段	有關如何從 AMS Accelerate 將 Alarm Manager 和 Resource Tagger 相依性新增至 Offboard 的指示。	2024 年 10 月 24 日
Resource Tagger 儀表板現已可用。	Resource Tagger 儀表板現在可在自助式報告中使用。	2024 年 9 月 26 日
您現在可以在標籤型提醒中包含多個電子郵件地址。	標籤型提醒現在支援多個電子郵件地址。	2024 年 9 月 20 日
AMS Accelerate 限制現在包含在 AMS 修補程式管理中。	AMS Accelerate 限制包含在修補程式管理 - 建立修補程式維護時段中。	2024 年 8 月 30 日
AMS 加速帳戶探索更新	Amazon EC2 執行個體評估已新增帳戶探索中的新區段。	2024 年 8 月 29 日
AMS Accelerate 預設修補基準現已可用於 Ubuntu 作業系統。	AMS Accelerate 預設修補基準現已可用於 Ubuntu 作業系統。	2024 年 8 月 22 日
AMS 加速帳戶探索更新	操作檢查資料表中的 AWS CloudTrail 評估區段已新增四個新的 AWS API 呼叫。	2024 年 8 月 2 日
Trusted Remediator 現在支援額外的檢查	Trusted Remediator 現在支援安全檢查 Hs4Ma3G192 - RDS 資料庫執行個體應禁止公開存取。	2024 年 7 月 30 日
AMS 現在支援 Amazon Route 53 Resolver DNS 防火牆	AMS 現在支援 Amazon Route 53 Resolver DNS 防火牆	2024 年 7 月 30 日

AMS Accelerate onboarding_role_minimal.zip 現在包含 Terraform 程式碼	AMS Accelerate onboarding_role_minimal.zip 現在包含 Terraform 程式碼。	2024 年 7 月 30 日
安全設定規則儀表板	安全設定規則儀表板現在可在自助式報告中使用。	2024 年 7 月 24 日
AMS Accelerate 現在支援 Oracle Linux 8.9、RHEL 8.10 和 RHEL 9.4。	AMS Accelerate 現在支援 Oracle Linux 8.9、RHEL 8.10 和 RHEL 9.4。	2024 年 7 月 5 日
AMS Accelerate 帳戶探索程序已更新。	AWS 帳戶 加入 AMS Accelerate 時所使用的帳戶探索程序已更新。	2024 年 7 月 1 日
Trusted Remediator 現已推出。	Trusted Remediator 是自動化 AWS Trusted Advisor 檢查修復的 AWS Managed Services 解決方案，現已推出。	2024 年 6 月 24 日
安全事件回應中的 Amazon Route 53 Resolver DNS 防火牆事件。	AMS 現在會在安全事件回應中監控 Amazon Route 53 Resolver DNS 防火牆事件	2024 年 6 月 21 日
更新支援的作業系統	AMS Accelerate 現在支援 AlmaLinux 8.3-8.9、9.0-9.2 (AlmaLinux 僅支援 x86 架構)	2024 年 6 月 19 日
如果符合預設值，則自動執行個體描述檔限制現在會增加。	如果達到預設限制 10，AMS 現在會將預設執行個體設定檔限制增加到 20。	2024 年 6 月 18 日
AMS SSM Agent 自動安裝功能現在預設為啟用。	6/03/2024 之後加入的帳戶預設會啟用 AMS SSM Agent 自動安裝功能。	2024 年 6 月 7 日

安全常見問答集已新增至安全管理。	現已提供安全性常見問答集，涵蓋 AMS 操作工程師或自動化存取您的帳戶時所使用的安全性最佳實務、控制、存取模型和稽核機制的常見問題。	2024 年 6 月 3 日
Amazon EKS 的監控和事件管理現在支援其他 AWS 區域。	Amazon EKS 的監控和事件管理現在支援三個額外的 AWS 區域。	2024 年 5 月 23 日
服務請求修補程式通知現在會在修補程式維護時段之前傳送。	AMS Accelerate 修補會在修補程式維護時段的 4 天前建立新的服務請求。您可以使用服務請求來與 AMS 通訊，以調整修補程式或略過修補程式。	2024 年 5 月 3 日
警示閾值已新增至 AMS Accelerate EKS 監控基準警示資料表。	詳細的提醒閾值現在可在 Amazon EKS 監控的基準提醒表格中使用。	2024 年 5 月 3 日
已更新：警示管理員組態設定檔。	新增有關使用 Alarm Manager 建立異常偵測警示的備註。	2024 年 4 月 25 日
資源 Tagger 組態設定檔的新增項目。	DynamoDB 資料表和 Amazon S3 儲存貯體現在可在 Resource Tagger 中使用	2024 年 4 月 25 日
已新增計劃事件管理 (PEM) 資訊區段。	有關 PEM 服務產品的詳細資訊現在可在 AMS Accelerate 使用者指南中找到。	2024 年 4 月 25 日
AMS 支援 Red Hat Enterpise Linux (RHEL) 9.x。	AMS 支援 Red Hat Enterprise Linux (RHEL) 9.x。	2024 年 4 月 25 日
AMS Accelerate 支援報告所有 AWS 區域組態。	AMS Accelerate 支援所有 AWS 區域組態的 SSM 庫存報告。	2024 年 4 月 25 日

已更新： AWS 受管政策。	使用新的 ECR 許可更新 AWSManagedServices DeploymentToolkitPolicy。	2024 年 4 月 4 日
已更新：資源交錯器組態設定檔區段	已AWS::EFS::FileSystem 新增至 ResourceType 清單。	2024 年 3 月 21 日
已更新：加速區段中的事件報告和服務請求。	將主題標題變更為 Accelerate 中的事件報告、服務請求和帳單問題。已新增帳單問題一節。	2024 年 3 月 21 日
更新：服務請求管理的運作方式區段。	新增說明 AMS 如何處理包含功能請求或錯誤的 服務請求。	2024 年 3 月 21 日
已更新：使用 AWS CloudFormation 區段建立 aws_managedservices_onboarding_role 角色	新增從中建立角色的命令 AWS CloudShell。	2024 年 3 月 21 日
已更新：（選用）Quick Start 範本	新增從中下載範本的命令 AWS CloudShell。	2024 年 3 月 21 日
警示管理員組態設定檔可用的新資源類型。	將 Amazon FSx、Amazon EFS 和 Elasticsearch 的資源類型新增至警示管理員組態描述檔。	2024 年 3 月 21 日
可用於組態描述檔的其他虛擬參數替換。	新增了 Amazon EFS 和 Amazon FSx 虛擬參數替換。	2024 年 3 月 21 日
在服務描述主題中的功能中新增新章節。	新增了 AMS Accelerate 功能下的服務請求管理一節。	2024 年 3 月 21 日
新增到自助式報告每週事件報告的新資料欄	每週事件報告中已新增新資料欄，讓您可以根據事件建立或解決的季度、月、週或日來篩選事件。	2024 年 3 月 11 日

舊版更新

下表說明 2024 年 3 月之前 AMS Accelerate 指南文件的重要變更。

變更	描述	日期
AMS Accelerate CloudTrail 線索加入的改善	AMS Accelerate CloudTrail 線索加入的改善： • 在單一區塊中收集所有儲存貯體政策 • 移除政策陳述式中的第二個 AWS 組織 ID • 釐清客戶環境需求 如需詳細資訊，請參閱檢閱並更新您的組態，讓 AMS Accelerate 使用您的 CloudTrail 追蹤。	2024 年 2 月 23 日
已更新：帳戶加入程序。	重組帳戶加入程序區段，讓步驟更加清楚。也刪除了用於加入功能的選用 Quick Start 範本。 請參閱 （選用） 加速中的 Quick Start 範本。	2024 年 2 月 22 日
已更新：離職 AMS Accelerate。	更新 AMS 加速離職考量章節，指出離職程序不會刪除 `ams-access-management` CloudFormation 堆疊和 `ams-access-management` IAM 角色。 請參閱 AMS 加速離職效果。	2024 年 2 月 22 日
更新：Acceleration 中的組態合規。	在適用的情況下，將「事件報告」變更為「服務請求」，以避免混淆這些條款。 請參閱 Accelerate 中的組態合規。	2024 年 2 月 22 日
更新：Accelerion 中的帳戶探索。	在 Accelerate 中重組帳戶探索，以使用相關區段將先決條件分組得更好。 請參閱 步驟 1. Accelerate 中的帳戶探索。	2024 年 2 月 22 日

變更	描述	日期
重新命名：向 AMS 主機管理報告 AMS 修補程式。	已將 AMS 修補程式報告重新命名為 AMS 主機管理，並將報告、修補程式詳細資訊報告重新命名為 SSM 代理程式涵蓋範圍報告。 請參閱 AMS 主機管理報告。	2024 年 2 月 22 日
更新隨需目錄上的操作	更新了 產品目錄的隨需操作目錄，以移除 中對「運作狀態」的參考`Amazon EKS cluster maintenance` 。 請參閱 隨需請求 AMS 操作。	2024 年 2 月 22 日
更新的 AMS 事件路由器	已更新 AMS Event Router 區段`AMSCoreRule` 中的 。 請參閱 在 AMS 中使用 Amazon EventBridge 受管規則。	2024 年 2 月 22 日
已更新支援的作業系統。	更新支援的作業系統以包含 SUSE Linux Enterprise Server 15 SP5。 請參閱 支援的組態。	2024 年 2 月 22 日
更新 EC2 磁碟區用量修復自動化	以正確的容量擴展排程更新 EC2 磁碟區用量修訂自動化區段。 請參閱 EC2 磁碟區用量修復自動化。	2024 年 2 月 22 日
更新：檢閱並更新您的組態，讓 Accelerate 使用您的 CloudTrail 追蹤	更新 AMS Accelerate Organization CloudTrail S3 儲存貯體政策一節。請參閱檢閱並更新您的組態，讓 AMS Accelerate 使用您的 CloudTrail 追蹤	2024 年 2 月 15 日
新增了新功能：SSM Agent 自動安裝	新增 SSM Agent 自動安裝的新章節 請參閱 SSM Agent 自動安裝。	2024 年 1 月 26 日

變更	描述	日期
已更新：支援的組態	新增有關支援的 版本的資訊 AWS Control Tower 請參閱 支援的組態。	2024 年 1 月 26 日
更新：AMS 修補程式報告。	從 AMS 修補程式報告中移除三個區段： • 修補程式執行個體詳細資訊摘要報告 • 修補程式詳細資訊報告 • 遺漏修補程式報告的執行個體 請參閱 AMS 主機管理報告。	2023 年 12 月 22 日
已更新：加速入門先決條件。	更新了加入 AMS Accelerate 所需的支援計畫。 請參閱 加速入門先決條件。	2023 年 12 月 15 日
已更新：建立修補程式維護時段。	移除預設修補程式週期區段，因為此功能已棄用。 請參閱 在 AMS 中建立修補程式維護時段。	2023 年 12 月 13 日
已更新：加速中的通知設定。	釐清用於通知的電子郵件。 如需詳細資訊，請參閱Accelerate 中的通知設定。	2023 年 12 月 12 日
已更新： `AMSAccelerateCustomerAccessPolicies` 範本。	更新`AMSAccelerateCustomerAccessPolicies` 範本以更正語法錯誤。 如需詳細資訊，請參閱使用 AMS 功能的許可。	2023 年 12 月 12 日
新增：變更請求安全性審查	在安全管理下新增變更請求安全審查一節。 如需詳細資訊，請參閱變更請求安全性審查。	2023 年 12 月 11 日

變更	描述	日期
已更新：resource_inventory.xlsx	更新 resource_inventory.xlsx 以包含安全分析師角色。 如需詳細資訊，請參閱Accelerate 的資源庫存。	2023 年 11 月 17 日
已更新：ams-access-admin-operations 角色描述	已更新 ams-access-admin-operations 描述。 如需詳細資訊，請參閱 AMS 存取您帳戶的原因和時間 和 在 AMS Accelerate 中使用身分進行驗證。	2023 年 11 月 17 日
更新：AMS Accelerate 離職考量事項	更新安全性章節，說明離職後可從 Amazon GuardDuty 和 AWS Config 規則取得的內容。 如需詳細資訊，請參閱AMS 加速離職效果。	2023 年 11 月 17 日
新增：Amazon EKS 的監控和事件管理	Amazon EKS 的監控和事件管理會監控 Amazon EKS 資源是否有故障、效能降低和安全問題。 如需詳細資訊，請參閱AMS Accelerate 中 Amazon EKS 的監控和事件管理。	2023 年 11 月 14 日
已更新：標記	新增有關客戶提供的標記的資訊。 如需詳細資訊，請參閱Accelerate 中客戶提供的標籤。	2023 年 11 月 7 日
已更新：資源交錯器組態設定檔	新增 AWS::AutoScaling::AutoScalingGroup、AWS::EKS::Cluster、AWS::Elasticsearch::Domain 和 AWS::FSx::FileSystem 至篩選條件區段。 如需詳細資訊，請參閱AMS Accelerate 中的資源交錯器組態設定檔。	2023 年 10 月 27 日
已更新：服務描述	已將 Ubuntu 22.04 新增至支援的作業系統。請參閱服務描述	2023 年 9 月 29 日

變更	描述	日期
更新：AMS Accelerate Onboarding 先決條件	新增備註至 AMS Accelerate VPC 端點以包含 CloudFormation 範本。請參閱 加速入門先決條件。	2023 年 9 月 29 日
已更新： Detect	從 AMS Accelerate 安全回應中移除端點保護類型。請參閱 偵測。	2023 年 9 月 29 日
已更新：AMS 中基準監控的提醒	已 AWS Outposts 新增至基準監控警示資料表。請參閱 偵測 monitoring-default-metrics。	2023 年 9 月 29 日
已更新：使用 建立 aws_managedservices_onboarding_role 角色 AWS CloudFormation	已更新指定堆疊詳細資訊的螢幕擷取畫面。請參閱 aws_managedservices_onboarding_role 使用 建立 AWS CloudFormation for Accelerate。	2023 年 9 月 29 日
更新：AMS Accelerate 部署的 Amazon EventBridge 受管規則	新增 AMS Accelerate Amazon EventBridge 受管規則 AMSCoreRule。 更新 AMS Accelerate Amazon EventBridge Managed Rule AMSAccessRolesRule 以新增角色。 如需詳細資訊，請參閱AMS 部署的 Amazon EventBridge 受管規則 。	2023 年 9 月 19 日
已更新：警示管理員組態設定檔	新增 AWS Outposts 虛擬參數替換識別符。請參閱 AMS Accelerate 中的監控和事件管理。	2023 年 9 月 11 日
已更新：資源交錯器組態設定檔	新增 AWS Outposts 資源類型。請參閱 加速組態設定檔：虛擬參數替換。	2023 年 9 月 11 日
已更新：支援的 服務	已將 Amazon Elastic File System 新增至 CloudWatch 警示監控的服務區段。 如需詳細資訊，請參閱服務描述。	2023 年 9 月 6 日

變更	描述	日期
更新：修補程式監控和故障修復	已將下列注意事項新增至使用修補程式協調器章節： 「不為具有不支援作業系統的執行個體建立修補程式失敗提醒，或在維護時段期間停止的執行個體建立修補程式失敗提醒」 如需詳細資訊，請參閱了解 AMS Accelerate 中的修補程式管理。	2023 年 9 月 6 日
更新：釐清對惡意軟體事件 Runbook 的回應	釐清安全事件回應的惡意軟體事件 Runbook 回應。如需詳細資訊，請參閱AMS 中的安全事件回應 。	2023 年 9 月 6 日
已更新：將您的 Accelerate 帳戶與 Transit Gateway 連線	釐清將新的 Accelerate 帳戶 VPC 連線至 AMS 多帳戶登陸區域網路 （建立 TGW VPC 連接） 的步驟：如需詳細資訊，請參閱將您的 Accelerate 帳戶withTransit Gateway 連線。	2023 年 9 月 5 日
已更新：AMS 中基準監控的提醒	已移除兩個已棄用警示 AMSReadLatencyAlarm 和 AMSWriteLatencyAlarm 的參考。如需詳細資訊，請參閱AMS 中基準監控的提醒。	2023 年 9 月 5 日
新增：AMS 事件路由器	新增 AMS 事件路由器的文件 如需詳細資訊在 AMS 中使用 Amazon EventBridge 受管規則，請參閱 。	2023 年 9 月 5 日
已更新：Alarm Manager 虛擬參數的清單。	已更新 Alarm Manager 虛擬參數的清單。EC2 執行個體名稱參數已新增至 EC2 執行個體和 EC2 磁碟警示組態。如需詳細資訊，請參閱加速組態設定檔：虛擬參數替換。	2023 年 8 月 29 日
新增：AMS Access Offboarding	新增了離職 AMS Access 時的考量。請參閱 AMS 加速離職效果。	2023 年 8 月 24 日
新增：AMS 安全事件回應	新增使用 AMS 安全事件回應的文件。請參閱 AMS 中的安全事件回應 。	2023 年 8 月 18 日

變更	描述	日期
更新：AMS Accelerate 存取角色	更正角色名稱中的錯別字。請參閱 AWS Identity and Access Management 在 AMS Accelerate 中。	2023 年 8 月 10 日
已更新：政策陳述式	以萬用字元取代硬式編碼角色名稱。請參閱 檢閱並更新您的組態，讓 AMS Accelerate 使用您的 CloudTrail 追蹤。	2023 年 8 月 10 日
已更新：具有 EFS 警示的受監控服務清單。	使用 AMS 基準監控的新 EFS 警示更新監控服務的清單。已新增 4 個新的 EFS 警示類型。如需詳細資訊，請參閱AMS 中基準監控的提醒。	2023 年 8 月 3 日
更新：加速資源庫存資料表	已移除 ams-backup-config-rule-stack 和相關資源。請參閱 Accelerate 的資源庫存。	2023 年 7 月 18 日
更新：AMS Accelerate 存取角色	已移除角色 ams-backup-config-rule-st-amsBackupAlertConfigRule-<8 位數雜湊> 和 ams-backup-config-rule-st-amsBackupPlanConfigRuleH-<8 位數雜湊 > 。請參閱 AWS Identity and Access Management 在 AMS Accelerate 中。	2023 年 7 月 18 日
已更新：監控 RDS 警示的清單。	更新了 AMS 基準監控的 RDS 警示清單。新增了 9 種新的 RDS 警示類型，並移除了 3 種現有的 RDS 警示類型。如需詳細資訊，請參閱AMS 中基準監控的提醒。	2023 年 6 月 19 日
新增：AMS Accelerate 存取角色	新增 AMS Security 的新存取角色。	2023 年 6 月 16 日
新增：AMS Accelerate CloudTrail 日誌管理現在可以使用客戶 CloudTrail 追蹤。	更新了 CloudTrail 日誌管理的 Accelerate 支援選項，包括加速部署追蹤，或與客戶受管 CloudTrail 帳戶或 Organization 追蹤整合。如需詳細資訊，請參閱檢閱並更新您的組態，讓 AMS Accelerate 使用您的 CloudTrail 追蹤。	2023 年 6 月 9 日

變更	描述	日期
已更新：AMS Accelerate Config Rules Response Configuration Report。	已更新 Config Rules Response Configuration Report AWS 的隨需報告。請參閱加速對隨需報告的更新。請參閱 AMS Config 規則回應組態報告。	2023 年 5 月 26 日
已更新：服務帳單開始日期政策。	更新 中帳單開始日期的定義AMS 金鑰術語。	2023 年 5 月 15 日
已更新： AWS 受管政策。	使用新的 CFN 和 ECR 許可更新 AWSManagedServicesDeploymentToolkitPolicy，並使用萬用字元縮小現有動作的範圍。請參閱加速服務連結角色的更新。請參閱 加速服務連結角色的更新。	2023 年 5 月 9 日
已更新：存取角色政策連結。	存取角色現在可以直接從 Accelerate S3 儲存貯體位置下載。 請參閱 AMS 存取您帳戶的原因和時間 和 AWS Identity and Access Management 在 AMS Accelerate 中。	
已更新：每月帳單自助服務報告。	新增的備註：每月帳單報告僅適用於管理付款人帳戶 (AMS 進階多帳戶登陸區域），但適用於所有連結的 AMS Accelerate 受管帳戶。 請參閱 帳單報告 （每月）。	2023 年 4 月 13 日
已更新：警示清單。	已移除 CloudTrail 參考。 請參閱 AMS Accelerate 中的日誌管理。	2023 年 4 月 13 日
已更新：警示清單。	新增三個新的 SSM 代理程式警示。 請參閱 AMS 中基準監控的提醒。	2023 年 4 月 13 日

變更	描述	日期
更新：加速先決條件。	釐清 Accelerate 需要四個 AWS Support 計劃的其中之一，並排除開發人員計劃。 請參閱 加速入門先決條件。	2023 年 4 月 13 日
更新：加速服務連結角色政策。	Contacts Service 政策 zip 檔案已更新。 請參閱 AWS AMS Accelerate 的 受管政策。	2023 年 4 月 13 日
已更新：AMS Resource Scheduler。	不正確的角色名稱 AWSManagedServices-DescribeScheduleOrPeriod，已更正為 AWSManagedServices-DescribeScheduleOrPeriods。請參閱 使用 AMS Resource Scheduler 進行成本最佳化。	2023 年 4 月 13 日
已更新： AWS 受管政策。	自訂問題清單回應 更新了在單一或多個帳戶中更新自訂回應的指示。	2023 年 4 月 13 日
已更新：資源交錯	新增了有關「指定新組態的名稱（所提供範例中的 SampleConfigurationBlock) 的警告，因為您可能會不小心以相同名稱覆寫 AMS 受管組態」的警告。請參閱 AMS Accelerate 中的資源交錯使用案例。	2023 年 3 月 16 日
已更新：修補程式 RACI	RACI 的多次更新和澄清以進行修補。請參閱 服務描述。	2023 年 3 月 16 日
已更新：部署工具組 SLR JSON 中的動作	已更新政策和動作。請參閱：使用 AMS Accelerate 的服務連結角色。	2023 年 3 月 16 日
更新：自動修復	已移除對 EC2 磁碟區自動化的 LVM 支援。請參閱：AMS 自動修復提醒。	2023 年 3 月 16 日
更新：加速加入。	釐清角色的使用方式，特別是最小角色 建立 AMS 角色的範本。	2023 年 3 月 16 日

變更	描述	日期
已更新：自助式報告。	每日備份報告現在支援主要和次要區域。兩者都會在 的資源區域欄位中報告備份報告 （每日）。	2023 年 3 月 16 日
更新：修補指引	新增警告，不自訂由 AMS 管理的預設修補基準。請改為建立新的自訂修補基準。請參閱： 預設修補程式基準和 使用 AMS Accelerate 自訂修補程式基準。	2023 年 3 月 16 日
已更新服務終止政策。	更新 中服務終止和服務終止日期的定義AMS 金鑰術語。終止通知必須在上個月前一個月的第 20 天發出。	2023 年 3 月 16 日
已更新： AWS 受管政策。	釐清的政策名稱：聯絡 AMS Accelerate 的服務連結角色。	2023 年 2 月 16 日
New： AWS managed 政策。	新增政策：聯絡 AMS Accelerate 的服務連結角色。	2023 年 2 月 16 日
已更新：組態合規。	修正 中的拼寫錯誤單字：Accelerate 中的組態合規。	2023 年 2 月 16 日
新內容：不支援OSes	新增有關 AMS 為不支援的作業系統 (OSes) 提供哪些服務的資訊，請參閱 Accelerate 中不支援的作業系統功能。	2023 年 2 月 16 日
更新：建立修補程式時段	已新增使用 CloudShell 的連結至 使用適用於 AMS Accelerate 的 Systems Manager 命令列界面 (CLI) 建立維護時段。	2023 年 2 月 16 日
更新內容：加入管理資源	更新 中的壓縮 JSON 範本建立 AMS 角色的範本。	2023 年 2 月 16 日
新內容：組態合規	新增了新主題：自訂問題清單回應。	2023 年 2 月 16 日

變更	描述	日期
New： AWS managed 政策。	新增政策：AMS Accelerate 的 Amazon EventBridge 規則服務連結角色。	2023 年 2 月 7 日
已更新： AWS 受管政策。	`AWSManagedServicesDeploymentToolkitPolicy` 使用新的 S3 許可更新 。請參閱 加速服務連結角色的更新。	2023 年 1 月 30 日
新的選擇加入區域：CPT。	AMS Accelerate 現已在開普敦 (CPT) 選擇加入區域提供。若要選擇加入，請參閱管理 AWS 區域。	2023 年 1 月 12 日
已更新：服務描述。	已將 CloudWatch 警示監控的 FSx 服務新增至服務描述。	2023 年 1 月 12 日
已更新：監控預設指標。	已將 6 個 FSx 警示新增至 AMS 中基準監控的提醒。	2023 年 1 月 12 日
已更新：AMS 模式。	已將自訂 Cloudwatch 警示通知新增至 AMS 模式。	2023 年 1 月 12 日
已更新：加入管理資源。	更新 範本的資料表，在 `ams-onboarding-ssm-execution-role` 中新增 的資料列建立 AMS 角色的範本。	2023 年 1 月 12 日
已更新：組態合規。	在 上請求自訂修復（在重要方塊中）的其他詳細資訊Accelerate 中的組態合規。	2023 年 1 月 12 日
已更新：Service-linked-role許可。	已移除較舊或重複的許可。請參閱 使用 AMS Accelerate 的服務連結角色。	2022 年 12 月 15 日
更新：修補程式管理、維護時段。	為建立維護時段的主控台指示新增指引，步驟 5。請參閱 從適用於 AMS Accelerate 的 Systems Manager 主控台建立維護時段。	2022 年 12 月 15 日
新增：修補程式管理區段。	已新增修補程式星期二維護時段的區段。請參閱從 AMS 主控台建立週期性「修補程式」維護時段（建議）。	2022 年 12 月 15 日

變更	描述	日期
已更新：AMS Resource Scheduler。	已更新 AWS CloudFormation 堆疊名稱。請參閱 搭配 AMS Resource Scheduler 使用資源。	2022 年 12 月 15 日
已更新：標記您的 資源以進行備份。	新增使用 AMS Resource Tagger 的指引。請參閱 標記您的 資源以套用 AMS 備份計劃。	2022 年 12 月 15 日
已更新：選取備份計劃。	指出哪些計劃提供持續備份。請參閱 選取 AMS 備份計畫。	2022 年 12 月 15 日
已更新：AMS Resource Scheduler。	更新刪除期間或排程的 AWS CLI 範例。請參閱 在 AWS Managed Services Resource Scheduler 中使用期間和排程。	2022 年 12 月 15 日
已更新： AWS 受管政策。	新增 `AWSManagedServicesDeploymentToolkitPolicy` 。請參閱 AWS AMS Accelerate 的 受管政策。	2022 年 12 月 15 日
新增：新增章節，說明 AMS 新服務連結角色 AWSServiceRoleForManagedServices_DetectiveControlsConfig。	新增 GovCloud 區域和許可。請參閱 AMS Accelerate 的 Detective 控制服務連結角色。	2022 年 12 月 15 日
新增： AWS受管政策	新增章節，說明如何在服務連結角色政策 AWSManagedServices_AlarmManagerPermissionsBoundary 中使用 AWS受管政策 AWSManagedServices_AlarmManager_ServiceRolePolicy，以限制服務連結角色 AWSServiceRoleForManagedServices_AlarmManager 建立的 IAM 角色許可。請參閱 AWS AMS Accelerate 的 受管政策。	2022 年 12 月 15 日
已更新：隨需操作。	新增了方案：EC2 操作上的 SQL Server 和 AMI 建置和販賣。請參閱 隨需操作。	2022 年 11 月 10 日
更新：監控和事件管理。	更新服務通知和事件報告的說明。請參閱 監控的運作方式。	2022 年 11 月 10 日

變更	描述	日期
已更新：服務連結角色區域	新增 GovCloud 區域和許可。請參閱 使用 AMS Accelerate 的服務連結角色。	2022 年 11 月 10 日
新增：服務連結角色。	新增了 角色：AWSServiceRoleForAMSDetectiveControls 。 請參閱 AMS Accelerate 的 Detective 控制服務連結角色。	2022 年 11 月 10 日
已更新：存取管理。	以改善的指示更新子區段。請參閱 AMS Accelerate 中的存取管理。	2022 年 11 月 10 日
已更新：服務描述。	已更新 RACI 矩陣中的 AMS 模式。請參閱 服務描述。	2022 年 11 月 10 日
已更新：AMS 模式。	客戶負責模式部署。請參閱 AMS 模式。	2022 年 11 月 10 日
已更新：離職。	新增在離職期間，特定 Backup and Monitoring 資源會發生什麼情況的詳細資訊。請參閱 從 AMS Accelerate 離線。	2022 年 11 月 10 日
已更新：修補程式管理。	更新和縮短了有關 IAM 政策的指引。請參閱 建立 IAM 角色以隨需修補 AMS Accelerate。	2022 年 11 月 10 日
新功能：架構圖的連結。	已將 AMS 參考架構圖表的連結新增至各種主題。如需範例，請參閱 AMS Accelerate 中的監控和事件管理。	2022 年 11 月 10 日
新增：Operations on Demand 產品	新增「Landing Zone Accelerator Operations」。請參閱 隨需操作。	2022 年 10 月 13 日
更新：監控管理。提醒會產生事件報告，而不是服務請求	監控的運作方式.	2022 年 10 月 13 日

變更	描述	日期
新增：使用 Accelerate-custom CFN 範本建立修補程式維護時段	AWS CloudFormation 修補程式視窗組態範本。請參閱 在 AMS 中建立修補程式維護時段。	2022 年 9 月 15 日
已更新：離職	強調 Accelerate 中的備份計劃在離職後不再運作。請參閱 從 AMS Accelerate 離線。	2022 年 9 月 15 日
已更新：CloudWatch 組態變更詳細資訊	更正 Windows 和 Linux 範例中的錯誤。請參閱 CloudWatch 組態變更詳細資訊。	2022 年 9 月 15 日
更新：使用 AMS 資源排程器	新增有關成本分配標籤的指引。請參閱 AMS 資源排程器中的成本估算器。	2022 年 9 月 15 日
已更新：AMS Config 規則程式庫	已將兩個ams-eks-組態規則新增至規則表。請參閱 AMS Config 規則程式庫。	2022 年 9 月 15 日
更新：備份管理	從備份計畫標題和描述中移除誤導性標籤 PITR point-in-time-recovery)。請參閱 選取 AMS 備份計畫。	2022 年 9 月 15 日
更新：加速服務描述	已更新組態規則和 Canary 的說明。請參閱 服務描述。	2022 年 9 月 15 日
更新：服務描述、支援的組態	已移除 Windows 2008 R2 的end-of-service日期。Accelerate 不支援 Windows 2008。請參閱 支援的組態。	2022 年 8 月 11 日
更新：服務描述、角色和責任	已更新 RACI 資料表。從網路區段的最後一列移除 ELB 存取日誌。我們不會為 Accelerate 客戶啟用 ELB 存取日誌。請參閱 角色和責任。	2022 年 8 月 11 日
已更新：組態合規	更正規則表、架構欄中的錯別字。NIST-CSF 錯誤地列為 NIST-CIS。請參閱 Accelerate 中的組態合規。	2022 年 8 月 11 日
新增：加速離職	離職的考量事項和程序。請參閱離職 AMS Accelerate。	2022 年 8 月 11 日

變更	描述	日期
已更新：預先安裝 SSM 代理程式的作業系統清單	已將「Ubuntu Linux 18.04 和 20.04」新增至清單。請參閱 加入 EC2 執行個體以加速。	2022 年 8 月 11 日
新增：資源排程器	使用 AMS Resource Scheduler 僅視需要停止和啟動資源，以最佳化成本。請參閱 使用 AMS Resource Scheduler 進行成本最佳化。	2022 年 7 月 14 日
已更新：Resource Scheduler 的服務描述	已針對新的 Resource Scheduler 產品更新服務描述的數個區段。請參閱 服務描述。	2022 年 7 月 14 日
新增：AMS 模式	AMS 提供模式範本，這是一種一般解決方案，可解決 AMS 受管環境中一系列的使用案例。優惠的第一個模式：AMS 模式。	2022 年 7 月 14 日
新增：成本最佳化備註	新增說明成本如何隨著資源用量增加的備註。請參閱 Accelerate 的資源庫存。	2022 年 7 月 14 日
已更新：AMS Config 規則	重新組織 中的資料表AMS Config 規則程式庫。HTML 資料表的資料欄較少，可讓您輕鬆一目了然地閱讀。可下載的試算表具有額外的資料欄，以允許排序和篩選。	2022 年 7 月 14 日
更新：存取管理	更新 中的範例 CloudFormation 範本使用 AMS 功能的許可。`AMSAccelerateAdminAccess` 政策現在包含 `AmsResourceSchedulerPassRolePolicy` 和 `IAMReadOnlyPolicy` 政策。	2022 年 7 月 14 日
更新：自助式報告	新增使用 KMS 金鑰加密 AWS Glue 中繼資料的指示。請參閱在 上標記為重要 的方塊自助式報告。	2022 年 7 月 14 日
更新：AMS 基準監控	新增 DeleteRecoveryPoint 備份提醒。 AMS 中基準監控的提醒	2022 年 7 月 14 日
更新：支援的作業系統	新增 Amazon Linux 2 的終止支援日期。 服務描述	2022 年 7 月 14 日

變更	描述	日期
更新：AMS 報告	新增選擇加入區域的注意事項。 報告和選項	2022 年 7 月 14 日
資源排程器	新增了有關加入和使用 AMS Resource Scheduler 的資訊，透過排程資源停止和開始時間來協助成本最佳化。此外，更新了 Accelerate 服務描述，以包含對 Resource Scheduler 的提及。此外， 已將 Amazon Linux 2 支援的支援結束日期更新為 2024 年。請參閱 使用 AMS Resource Scheduler 進行成本最佳化 和 服務描述	2022 年 6 月 30 日
新警示	新增 AWS Backup 警示。 AMS 中基準監控的提醒	2022 年 6 月 21 日
新內容	新增服務連結角色內容。 使用 AMS Accelerate 的服務連結角色	2022 年 6 月 16 日
	AWS Network Firewall Operations 已新增至 方案的隨需操作 (OOD) 目錄。 隨需操作	2022 年 6 月 16 日
	新增問題管理功能描述。 服務描述	2022 年 6 月 16 日
	新增有關在特定選擇加入區域中不支援的一組組態規則的備註。 Accelerate 中的組態合規	2022 年 6 月 16 日
已更新內容	組態合規。"AMS Config Rule Library" -> "Table of rules"，已更新並僅移除至 ZIP。 Accelerate 中的組態合規	2022 年 6 月 16 日
	已移除呈報電子郵件。 呈報路徑	2022 年 6 月 16 日
	已將主題清單移至開啟段落下方。 什麼是 AMS Accelerate？	2022 年 6 月 16 日

變更	描述	日期
	已更新自動修復內容。 AMS 自動修復提醒	2022 年 6 月 16 日
更新內容：服務描述	已將 EKS 新增至 中由 AMS Config 規則監控的服務清單支援的服務。 更新 中 RACI 資料表的監控描述角色和責任。	2022 年 5 月 12 日
更新內容：組態合規	新增與 EKS 相關的組態規則。請參閱 Accelerate 中的組態合規。	2022 年 5 月 12 日
更新內容：入門、帳戶探索	在 中新增了較新版本的 AwsAccountDiscoveryCli 指令碼 （在帳戶探索變更日誌 zip 檔案中)步驟 1. Accelerate 中的帳戶探索。	2022 年 5 月 12 日
更新內容：監控、預設指標	更新 ALB 相關指標的觸發條件。請參閱 AMS 中基準監控的提醒。	2022 年 5 月 12 日
更新內容：修補加入	新增明確的修補先決條件：您需要選擇加入 EBS。請參閱 在 Accelerate 中加入修補。	2022 年 5 月 12 日
更新內容：加速資源庫存資料表	已變更 ams-detective-controls-config-rules-cdk 規則，新增 ams-detective-controls-recorder-cdk 和 ams-detective-controls-infrastructure-cdk 的規則。請參閱 Accelerate 的資源庫存。	2022 年 4 月 14 日
更新內容：組態合規	產業標準、組態規則和回應類型簡介。強調客戶不會選擇個別組態規則或回應。 Accelerate 中的組態合規	2022 年 4 月 14 日
更新內容：服務描述	已將現有的變更範圍區段移至角色和責任下。請參閱 角色和責任。	2022 年 4 月 14 日
更新內容：標記和監控	已`AWS::Synthetics:Canary` 新增至允許用於標記和監控的資源類型清單。請參閱 AMS Accelerate 中的資源交錯器組態設定檔 和 加速組態設定檔：虛擬參數替換。	2022 年 4 月 14 日

變更	描述	日期
更新內容：加速先決條件	已將 SSM 所需的儲存貯體許可新增至 Accelerate 中的 Amazon EC2 Systems Manager 。	2022 年 4 月 14 日
新內容：修補和監控	新增使用 Cloudformation 部署標記和監控組態的範例程式碼。請參閱 使用 AWS CloudFormation for Accelerate 部署組態設定檔 和 使用 AWS CloudFormation 來部署加速組態變更。	2022 年 3 月 10 日
更新內容：修補程式維護主控台	在 中重新排序步驟從適用於 AMS Accelerate 的 Systems Manager 主控台建立維護時段以符合主控台界面。	2022 年 3 月 10 日
更新內容：修補程式維護 CLI	更新 的 CLI 參數 （ 排程、持續時間和截止 ） 使用適用於 AMS Accelerate 的 Systems Manager 命令列界面 (CLI) 建立維護時段	2022 年 3 月 10 日
新內容：自動執行個體組態	已將 的定義`AMSInstanceProfile BasePolicy` 新增至 IAM 許可變更詳細資訊	2022 年 3 月 10 日
新內容：加入	已新增範例 Linux 命令至 Accelerate 中的傳出網際網路連線	2022 年 3 月 10 日
新內容：加入	已將最低權限選項新增至 建立 AMS 角色的範本。	2022 年 3 月 10 日
更新內容：加速呈報指示	新增指引、連結和電子郵件聯絡人至 呈報路徑	2022 年 3 月 10 日
更新內容：支援的組態	AMS 預計將於 2023 年 3 月 14 日結束對 RHEL 6 和 CentOs支援。請參閱支援的組態	2022 年 3 月 10 日
已更新內容：資源資料表	已將 AMS 存取 IAM 角色新增至Accelerate 的資源庫存資源資料表	2022 年 3 月 10 日
更新內容：加入和備份	新增選擇加入 AWS Backup 在 Accelerate AWS Backup 中加入和 的指示 AMS Accelerate 中的持續性管理	2022 年 3 月 10 日

變更	描述	日期
更新內容：Access Management	從加速指引 中移除進階特定指示在 AMS 中使用根使用者帳戶的方式和時間。	2022 年 3 月 10 日
更新內容：支援的組態	AMS 現在支援 Oracle Linux 8.3 和 Ubuntu 18.04 和 20.04。請參閱 支援的組態。	2022 年 2 月 28 日
更新內容：服務水準協議	已更新 中的可下載服務水準協議支援的服務。	2022 年 2 月 28 日
更新內容：Access Management	AMS 如何存取您的帳戶 更新為 AMS 操作員主控台角色的FAQs，以及不修改或刪除這些角色的警告。	2022 年 2 月 28 日
更新內容：Alarm Manager	已更新加速組態設定檔：監控。警示管理員不再受限於單一指標警示。	2022 年 2 月 28 日
更新內容：入門	已更新步驟 2. 在 Accelerate 中加入管理資源。已新增具有最低加入資源存取權的 IAM 角色。	2022 年 2 月 28 日
新內容：服務描述的變更範圍	新增章節，AMS Accelerate 執行的變更範圍強調 AMS Accelerate 未執行的界限和動作。	2022 年 2 月 10 日
更新內容：入門	新的加入程序從設定預設功能和組態開始，然後再自訂。子區段包含功能特定的目標和相關連結。請參閱 AMS Accelerate 入門。	2022 年 2 月 10 日
更新內容：AMS Backup Management。	縮短和重組AMS Accelerate 中的持續性管理章節，以提高可讀性。	2022 年 2 月 10 日
更新內容：標記	新增標記工具區段，以容納 CloudFormation 和其他工具的程式碼範例。請參閱 AMS Accelerate 中的標記。	2022 年 2 月 10 日
更新內容：基準監控	改善 RedShift 叢集警示的觸發條件，可減少維護期間的錯誤警示。請參閱 AMS 中基準監控的提醒。	2022 年 2 月 10 日

變更	描述	日期
更新內容：修補	更新範例 CLI 命令以註冊維護時段。請參閱 使用適用於 AMS Accelerate 的 Systems Manager 命令列界面 (CLI) 建立維護時段。	2022 年 2 月 10 日
已更新 content： AWS Config 規則庫存。	`ams-nist-cis-ec2-security-group-attached-to-eni` 從 Config Rules Inventory 資料表中移除已棄用 AWS 的設定規則。請參閱 規則表。	2022 年 1 月 27 日
新內容：建立修補程式維護時段。	已新增 SSM 教學課程的連結，以及從命令列建立修補程式維護時段的範例命令。請參閱 使用適用於 AMS Accelerate 的 Systems Manager 命令列界面 (CLI) 建立維護時段。	2022 年 1 月 27 日
新內容：Resource Tagger 可識別新的 Auto Scaling 群組 (ASG) 資源類型。	已將 Auto Scaling 群組新增至可使用 Resource Tagger 組態描述檔篩選的資源類型。請參閱 語法和結構。	2022 年 1 月 13 日
新內容：其他備份計畫和保存庫。	新增備份計畫和保存庫，以緩解高風險案例，包括勒索軟體攻擊。請參閱 檢視 AMS 保存庫中的備份 和 檢視 AMS 保存庫中的備份。	2022 年 1 月 13 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。