AMS 進階帳戶加入資訊

AMS 進階入門指南

版本 September 25, 2025

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AMS 進階入門指南: AMS 進階帳戶加入資訊

Copyright © 2026 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，或由 Amazon 贊助。

Table of Contents

AWS Managed Services 加入簡介

歡迎使用 AWS Managed Services (AMS)。AMS 是一種企業服務，可提供 AWS 基礎設施的持續管理。本指南旨在協助您開始使用 AMS，包括如何為 AMS 設定新帳戶、設定聯網和存取 AMS，以及驗證您的加入設定。

它適用於負責準備和執行將 AMS 服務加入新 AWS 帳戶所需任務的 IT 管理員。加入 AMS 服務需要特殊權限，才能設定 Active Directory 信任並完成其他聯網層級任務。若要取得決定使用多帳戶登陸區域帳戶或單一帳戶登陸區域帳戶的協助，請造訪選擇單一 MALZ 或多個 MALZs。

> **Important**
>
> 本指南在簡介後分為兩個部分：一個用於多帳戶登陸區域帳戶，另一個用於單一帳戶登陸區域帳戶。兩者的加入截然不同，請前往適用於您情況的指南章節。

主題

了解 AMS

若要進一步了解 AMS，請參閱這些 AMS 使用者指南章節：

- 什麼是 AWS Managed Services 推出 AMS 服務，並說明主要功能、操作和介面，以及典型的 AMS 受管網路架構。本章也提供存取管理的相關資訊，包括如何存取 AMS 受管資源和使用堡壘。
- 關鍵術語提供 AMS 術語的定義和說明。
- 了解 AMS 預設值提供 AMS 使用的預設值，包括基本環境元件、IAM 和 EC2、代理、監控指標、記錄、端點安全 (EPS)、備份和修補的預設值。

- 變更管理提供變更請求 (RFCs) 和變更類型 (CTs運作方式的詳細資訊，並包含使用 AMS RFCs的範例。
- 幾個額外的章節涵蓋使用 AMS 變更管理系統、AMS SKMS、安全性、服務請求、事件、監控、日誌、EPS、備份和修補程式管理來存取 AMS 主控台、AMS CLI。

若要進一步了解 AMS 多帳戶登陸區域架構，請參閱多帳戶登陸區域網路架構

若要進一步了解 AMS 單一帳戶登陸區域架構，請參閱單一帳戶登陸區域網路架構

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。發生下列情況時，會發生 AWS Managed Services 啟用通知：

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 視需要將所有 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。
- 提供 AWS Managed Services： AWS makes 供您使用，而且您可以從服務開始日期開始，針對每個 AWS Managed Services 帳戶存取和使用 AWS Managed Services。
- 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為可用狀態，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 或您如何排定事件的優先順序，可以是低、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。此模型最密切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發佈，通常在修補程式發佈後不久發佈。
- 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）：修補程式由廠商或管理應用程式的內文提供。
- 修補程式類型：
  - Critical Security Update (CSU)：由受支援作業系統的廠商評定為「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)：由受支援作業系統的廠商更新，該作業系統不是 CSU 或 IU。
- 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，並已同意您的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。

AMS 模式

使用此選項可協助您根據所需的彈性和規範控管組合，選擇適當的 AWS Managed Services (AMS) 模式來託管您的應用程式，以實現您的業務成果。

此資訊的目標對象為：

- 客戶團隊負責其登陸區域的策略和管理。此資訊將協助團隊規劃 AMS 受管登陸區域的基礎，以及他們想要提供給其內部和外部客戶的 AMS 模式。
- 負責將應用程式遷移至 AMS 的業務和應用程式擁有者。此資訊將有助於規劃應用程式遷移，並使用適當的 AMS 模式來遷移/託管其應用程式。請注意，相同的應用程式可以在其軟體開發生命週期 (SDLC) 生命週期的不同階段，以多個 AMS 模式託管。
- AMS 合作夥伴的任務是引導客戶使用不同的選項來建置和遷移至 AMS。

此資訊假設您已決定利用 AMS 來加速雲端之旅。在雲端遷移旅程的兩個時間點參考此白皮書：首先，在設定 AMS 受管平台的基礎階段。其次，當您從基礎轉換到雲端採用之旅的遷移階段時，就在加入 AMS 完成之後，您專注於應用程式控管和操作。

AMS 模式和應用程式或工作負載

選擇正確的模式時，請考慮應用程式的營運和管理需求，方法是請求新的應用程式帳戶或在現有的應用程式帳戶中託管應用程式。為每個應用程式或工作負載選擇適當的 AMS 模式取決於下列因素：

- 環境將提供的 SDLC 生命週期函數類型（例如，具有未修改變更的沙盒、具有一些頻繁變更的 UAT、具有最少變更且受到高度管制的生產）
- 所需的控管政策（透過 OU 層級SCPs 強制執行）
- 操作模型（如果您想要承擔操作責任，或想要將其委外至 AMS)
- 所需的業務成果，例如在雲端中操作的時間，以及操作成本。

> **Note**
>
> 如需每個 AMS 服務的模式類型說明，請參閱 AMS 中的模式和帳戶的類型。
> 如需不同模式的實際使用案例，請參閱 AMS 模式的實際使用案例

下表概述應用程式擁有者的關鍵考量事項，以協助決定最適合的 AMS 模式。應用程式擁有者應在應用程式遷移之前包含評估階段，以完全了解適用於其特定應用程式的模式。範例：對於以雲端原生服務或無伺服器架構為基礎的應用程式，最佳選項可能是開始在開發人員模式下建置和反覆運算，並使用 AMS Managed – SSP 模式將最終基礎設施部署為程式碼。在這種情況下，可能需要進行光線重構，以確保為自動化部署建立的任何 CloudFormation 範本都符合 AMS 制定的擷取準則。此外，任何 IAM 許可都需要 AMS Security 核准，以確保它們遵循最低權限模型。

選取來託管應用程式的 AMS 模式，可協助您建置所需的雲端操作模型。

> **Note**
>
> 根據為託管應用程式選取的不同 AMS 模式，單一 AMS 受管登陸區域中可以存在多個雲端操作模型。

決策問題	標準 CM 模式/OOD*	AWS Service Catalog	直接變更模式	自助式佈建	開發人員模式	客戶受管
操作準備						
記錄、監控和事件管理	負責所有受管基礎設施的 AMS			負責自助服務佈建服務 (SSP) 的客戶	客戶負責在 AMS CM 系統外使用開發人員 IAM 角色佈建的資源	客戶負責
持續性管理	AMS 負責執行客戶選取的備份計劃			負責自助服務佈建服務 (SSP) 的客戶	客戶負責在 AMS CM 系統外使用開發人員 IAM 角色佈建的資源	
執行個體層級存取管理	使用內部部署網域透過單向 AD 信任管理的 AMS。需要受管基礎設施才能加入 AMS 網域			不適用	客戶負責在 AMS CM 系統外使用開發人員 IAM 角色佈建的資源	
安全管理和帳戶層級存取管理	所有受管帳戶的 AMS 責任			負責所有受管帳戶的 AMS	客戶負責在 AMS CM 系統外使用開發人員 IAM	

決策問題	標準 CM 模式/OOD*	AWS Service Catalog	直接變更模式	自助式佈建	開發人員模式	客戶受管
					角色佈建的資源	
修補管理	所有受管帳戶的 AMS 責任			負責自助服務佈建服務 (SSP) 的客戶	客戶負責在 AMS CM 系統外使用開發人員 IAM 角色佈建的資源	
變更管理	所有受管帳戶的 AMS 責任			負責自助服務佈建服務 (SSP) 的客戶	客戶負責在 AMS CM 系統外使用開發人員 IAM 角色佈建的資源	
佈建管理	AMS 中提供的佈建選項的規範和標準化	依照 AMS 規範標準直接使用 AWS Service Catalog 的 AWS 服務 API 的彈性	依照 AMS 規範標準直接使用 AWS 服務 API 的彈性	為 SSP 服務直接使用 AWS 服務 APIs彈性	直接使用 AWS 服務 API 進行佈建的彈性	
事件管理和稽核	所有受管帳戶的 AMS 回應				客戶負責在 AMS 變更管理系統外使用開發人員 IAM 角色佈建的資源	

決策問題	標準 CM 模式/OOD*	AWS Service Catalog	直接變更模式	自助式佈建	開發人員模式	客戶受管
GuardRails 和共用基礎設施（網路）和安全架構	使用 AMS 核心帳戶的規範和標準化					彈性和自訂運用 AMS 核心帳戶
應用程式整備						
應用程式重構	需要光線重構				需要光線重構（如果使用 AMS 標準 CM 佈建）	不需要重構
支援 AWS 服務	僅限於 AMS 支援的內容					不受限制
業務考量事項						
操作就緒時間	三到六個月			6 個月以上取決於客戶應用程式操作能力		6-18 個月取決於客戶基礎設施和應用程式操作能力
成本	$$$$			$$$	$$	$

決策問題	標準 CM 模式/OOD*	AWS Service Catalog	直接變更模式	自助式佈建	開發人員模式	客戶受管
應用程式範例	具有 3 層堆疊的 Web 伺服器，具有合規和法規要求的應用程式			使用 API Gateway 的 Web 伺服器，利用 ECS/EKS 的容器化應用程式	在使用 Lambda、Glue、Athena 等的 Data Lake 應用程式上反覆/最佳化	分散式帳戶/應用程式，例如沙盒、第三方受管應用程式

*隨需操作 (OOD) 提供客戶使用標準 CM 模式，透過專用資源管理其變更。如需詳細資訊，請參閱 方案的隨需操作目錄，並與您的雲端服務交付管理員 (CSDM) 交談。

> **Note**
>
> SSP 模式和開發人員模式之間的價格比較假設已佈建相同的 AWS 服務。

比較 AMS 模式與業務和 IT 目標

如所示，如果您要為應用程式尋找高度受控和標準化的控管模型，則 AMS 受管的標準變更、AWS Service Catalog 或直接變更模式是最適合的。如果您需要專注於應用程式創新的自訂控管模型，而不需要操作準備，請選取客戶受管模式。使用客戶受管模式，當您負責建立人員、程序和工具以支援操作功能時，可能需要更長的時間來操作應用程式，例如事件管理、組態管理、佈建管理、安全管理、修補程式管理等。

AMS 帳戶後方案指引

隨著組織採用分散式操作和 DevOps 實務，在部署工作負載之前，應該將一組核心操作功能套用至每個帳戶，以滿足 Well Architected 的支柱。

此連結會下載包含 Word 文件的 ZIP 檔案，以及包含指令碼和範例的 ZIP 檔案。自動化帳戶設定是一組指令碼，用於自動化或引導新應用程式帳戶的設定。

一旦新帳戶結束，並在部署任何工作負載之前，為了從營運、安全和管理的角度準備好帳戶，您可以設定預設備份計劃、修補程式時段和加密（等等）。為了協助改善應用程式帳戶設定的敏捷性、一致性和回應能力，以下範例提供「如何」供您參考。

自動化帳戶設定。

我們做什麼、我們不做什麼

AMS 為您提供了部署 AWS 基礎設施的標準化方法，並提供必要的持續營運管理。如需角色、責任和支援服務的完整描述，請參閱服務描述。

> **Note**
>
> 若要請求 AMS 提供額外的 AWS 服務，請提交服務請求。如需詳細資訊，請參閱提出服務請求。

- 我們做什麼：

  完成加入後，AMS 環境即可接收變更 (RFCs)、事件和服務請求。您與 AMS 服務的互動圍繞應用程式堆疊的生命週期進行。新堆疊是從預先設定的範本清單排序，啟動到特定的虛擬私有雲端 (VPC) 子網路，在操作生命週期內透過請求變更 (RFCs) 進行修改，並全年無休監控事件和事件。

  AMS 會監控和維護作用中的應用程式堆疊，包括修補，除非需要變更或停用堆疊，否則堆疊在堆疊生命週期內不需要進一步的動作。AMS 偵測到會影響堆疊運作狀態和功能的事件會產生通知，且可能需要或不需要您的動作來解決或驗證。方法問題和其他查詢可以透過提交服務請求提出。

  此外，AMS 可讓您啟用非由 AMS 管理的相容 AWS 服務。如需 AWS-AMS 相容服務的資訊，請參閱自助式佈建模式。

- 我們不執行的動作：

  雖然 AMS 透過提供許多手動和自動化選項來簡化應用程式部署，但您必須負責應用程式的開發、測試、更新和管理。AMS 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 無法存取或驗證您的應用程式組態。

AMS 輸出流量管理

根據預設，AMS 私有和客戶應用程式子網路目的地 CIDR 為 0.0.0.0/0 的路由具有網路位址轉譯 (NAT) 閘道做為目標。AMS 服務、TrendMicro 和修補是必須具有網際網路輸出存取權的元件，以便 AMS 能夠提供其服務，而 TrendMicro 和作業系統可以取得更新。

AMS 支援透過客戶管理的輸出裝置將輸出流量轉移到網際網路，只要：

- 它充當隱含（例如透明）代理。

  以及

- 它允許 AMS HTTP 和 HTTPS 相依性（列於本節），以允許 AMS 受管基礎設施的持續修補和維護。

部分範例如下：

- 傳輸閘道 (TGW) 具有預設路由，指向多帳戶登陸區域網路帳戶中透過 AWS Direct Connect 連線的客戶受管內部部署防火牆。
- TGW 有一個預設路由，指向多帳戶登陸區域輸出 VPC 中的 AWS 端點，利用 AWS PrivateLink，指向另一個 AWS 帳戶中的客戶受管代理。
- TGW 預設路由指向另一個 AWS 帳戶中的客戶受管防火牆，並以site-to-site連接做為多帳戶登陸區域 TGW 的連接。

AMS 已識別對應的 AMS HTTP 和 HTTPS 相依性，並持續開發和精簡這些相依性。請參閱 egressMgmt.zip。除了 JSON 檔案之外，ZIP 還包含 README。

> **Note**
>
> - 此資訊並不全面 - 此處未列出某些必要的外部網站。
> - 請勿在拒絕清單或封鎖策略下使用此清單。
> - 此清單旨在做為輸出篩選規則集的起點，預期報告工具將用於精確判斷實際流量與清單的差異。

若要詢問有關篩選輸出流量的資訊，請傳送電子郵件給您的 CSDM：ams-csdm@amazon.com。

AMS 中的 IAM 使用者角色

IAM 角色類似於 IAM 使用者，因為它是具有許可政策的 AWS 身分，可決定身分可以和不可以執行的操作 AWS。但是，角色的目的是讓需要它的任何人可代入，而不是單獨地與某個人員關聯。

對於標準 AMS 帳戶，目前有一個 AMS 預設使用者角色 `Customer_ReadOnly_Role`，對於具有 Managed Active Directory `customer_managed_ad_user_role`的 AMS 帳戶，則有一個額外的角色。

角色政策會設定 CloudWatch 和 Amazon S3 日誌動作、AMS 主控台存取、大多數的唯讀限制 AWS 服務、帳戶 S3 主控台的限制存取，以及 AMS 變更類型存取的許可。

此外，`Customer_ReadOnly_Role`具有變動的 reserved-instances 許可，可讓您保留執行個體。它有一些節省成本的值，因此，如果您知道需要長時間特定數量的 Amazon EC2 執行個體，您可以呼叫這些 APIs。若要進一步了解，請參閱 Amazon EC2 預留執行個體。

> **Note**
>
> 為 IAM 使用者建立自訂 IAM 政策的 AMS 服務層級目標 (SLO) 為四個工作天，除非將重複使用現有政策。如果您想要修改現有的 IAM 使用者角色，或新增新的角色，請分別提交 IAM：更新實體或 IAM：建立實體 RFC。

如果您不熟悉 Amazon IAM 角色，請參閱 IAM 角色以取得重要資訊。

多帳戶登陸區域 (MALZ)：若要查看 AMS 多帳戶登陸區域預設、非自訂的使用者角色政策，請參閱 MALZ：預設 IAM 使用者角色，下一步。

MALZ：預設 IAM 使用者角色

預設多帳戶 AMS 多帳戶登陸區域使用者角色的 JSON 政策陳述式。

> **Note**
>
> 使用者角色是可自訂的，而且可能因帳戶而異。提供尋找角色的說明。

這些是預設 MALZ 使用者角色的範例。為了確保您已設定所需的政策，請執行 AWS 命令`get-role`或登入 AWS Management -> IAM 主控台，然後在導覽窗格中選擇角色。

核心 OU 帳戶角色

核心帳戶是 MALZ 管理的基礎設施帳戶。AMS 多帳戶登陸區域 核心帳戶包括管理帳戶和聯網帳戶。

核心 OU 帳戶：常用角色和政策

角色	政策或政策
AWSManagedServicesReadOnlyRole	ReadOnlyAccess （公有 AWS 受管政策）。
AWSManagedServicesCaseRole	ReadOnlyAccess
	AWSSupportAccess （公有 AWS 受管政策）。
AWSManagedServicesChangeManagementRole （核心帳戶版本）	ReadOnlyAccess
	AWSSupportAccess
	AMSChangeManagementReadOnlyPolicy
	AMSChangeManagementInfrastructurePolicy

核心 OU 帳戶：管理帳戶角色和政策

角色	政策或政策
AWSManagedServicesBillingRole	AMSBillingPolicy (AMSBillingPolicy)。
AWSManagedServicesReadOnlyRole	ReadOnlyAccess （公有 AWS 受管政策）。
AWSManagedServicesCaseRole	ReadOnlyAccess
	AWSSupportAccess （公有 AWS 受管政策）。
AWSManagedServicesChangeManagementRole （管理帳戶版本）	ReadOnlyAccess
	AWSSupportAccess
	AMSChangeManagementReadOnlyPolicy
	AMSChangeManagementInfrastructurePolicy

角色	政策或政策
	AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

核心 OU 帳戶：聯網帳戶角色和政策

角色	政策或政策
AWSManagedServicesReadOnlyRole	ReadOnlyAccess （公有 AWS 受管政策）。
AWSManagedServicesCaseRole	ReadOnlyAccess
	AWSSupportAccess （公有 AWS 受管政策）。
AWSManagedServicesChangeManagementRole （網路帳戶版本）	ReadOnlyAccess
	AWSSupportAccess
	AMSChangeManagementReadOnlyPolicy
	AMSChangeManagementInfrastructurePolicy
	AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

應用程式帳戶角色

應用程式帳戶角色會套用至您的應用程式特定帳戶。

應用程式帳戶：角色和政策

角色	政策或政策
AWSManagedServicesReadOnlyRole	ReadOnlyAccess （公有 AWS 受管政策）。
AWSManagedServicesCaseRole	ReadOnlyAccess
	AWSSupportAccess （公有 AWS 受管政策）。

角色	政策或政策
AWSManagedServicesSecurityOpsRole	此政策提供所有支援操作和資源的存取權。如需詳細資訊，請參閱 AWS Support 入門。
	ReadOnlyAccess
	AWSSupportAccess 範例 此政策提供所有支援操作和資源的存取權。
	AWSCertificateManagerFullAccess 資訊，（公有 AWS 受管政策）
	AWSWAFFullAccess 資訊，（公有 AWS 受管政策）。此政策授予 AWS WAF 資源的完整存取權。
	AMSSecretsManagerSharedPolicy
AWSManagedServicesChangeManagementRole（應用程式帳戶版本）	ReadOnlyAccess
	AWSSupportAccess （公有 AWS 受管政策）。 此政策提供所有支援操作和資源的存取權。如需詳細資訊，請參閱 AWS Support 入門。
	AMSSecretsManagerSharedPolicy
	AMSChangeManagementPolicy
	AMSReservedInstancesPolicy
	AMSS3Policy
AWSManagedServicesAdminRole	ReadOnlyAccess
	AWSSupportAccess
	AMSChangeManagementInfrastructurePolicy
	AWSMarketplaceManageSubscriptions

角色	政策或政策
	AMSSecretsManagerSharedPolicy
	AMSChangeManagementPolicy
	AWSCertificateManagerFullAccess
	AWSWAFFullAccess
	AMSS3Policy
	AMSReservedInstancesPolicy

政策範例

範例適用於大多數使用的政策。若要檢視 ReadOnlyAccess 政策 （只要提供所有 AWS 服務的唯讀存取權），如果您有作用中的 AWS 帳戶：ReadOnlyAccess，您可以使用此連結。此外，此處也包含精簡版本。

AMSBillingPolicy

AMSBillingPolicy

您的會計部門可以使用新的帳單角色來檢視和變更 管理帳戶中的帳單資訊或帳戶設定。若要存取替代聯絡人、檢視帳戶資源用量，或保留帳單標籤，或甚至修改您的付款方式等資訊，您可以使用此角色。這個新角色包含 AWS Billing IAM 動作網頁中列出的所有許可。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "aws-portal:ViewBilling",
                "aws-portal:ModifyBilling"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToBilling"
```

```
        },
        {
            "Action": [
                "aws-portal:ViewAccount",
                "aws-portal:ModifyAccount"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToAccountSettings"
        },
        {
            "Action": [
                "budgets:ViewBudget",
                "budgets:ModifyBudget"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToAccountBudget"
        },
        {
            "Action": [
                "aws-portal:ViewPaymentMethods",
                "aws-portal:ModifyPaymentMethods"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToPaymentMethods"
        },
        {
            "Action": [
                "aws-portal:ViewUsage"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToUsage"
        },
        {
            "Action": [
                "cur:DescribeReportDefinitions",
                "cur:PutReportDefinition",
                "cur:DeleteReportDefinition",
                "cur:ModifyReportDefinition"
            ],
            "Resource": "*",
```

```
            "Effect": "Allow",
            "Sid": "AllowAccessToCostAndUsageReport"
        },
        {
            "Action": [
                "pricing:DescribeServices",
                "pricing:GetAttributeValues",
                "pricing:GetProducts"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToPricing"
        },
        {
            "Action": [
                "ce:*",
                "compute-optimizer:*"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToCostExplorerComputeOptimizer"
        },
        {
            "Action": [
                "purchase-orders:ViewPurchaseOrders",
                "purchase-orders:ModifyPurchaseOrders"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToPurchaseOrders"
        },
        {
            "Action": [
                "redshift:AcceptReservedNodeExchange",
                "redshift:PurchaseReservedNodeOffering"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToRedshiftAction"
        },
        {
            "Action": "savingsplans:*",
            "Resource": "*",
            "Effect": "Allow",
```

```
            "Sid": "AWSSavingsPlansFullAccess"
        }
    ]
}
```

AMSChangeManagementReadOnlyPolicy

AMSChangeManagementReadOnlyPolicy

檢視所有 AMS 變更類型的許可，以及所請求變更類型的歷史記錄。

AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

請求部署 | 受管登陸區域 | 管理帳戶 | 建立應用程式帳戶 （使用 VPC) 變更類型的許可。

AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

請求部署 | 受管登陸區域 | 網路帳戶 | 建立應用程式路由表變更類型的許可。

AMSChangeManagementInfrastructurePolicy

AMSChangeManagementInfrastructurePolicy （適用於管理 | 其他 | CTs)

請求管理 | 其他 | 其他 | 建立和管理 | 其他 | 更新變更類型的許可。

AMSSecretsManagerSharedPolicy

AMSSecretsManagerSharedPolicy

檢視 AMS 透過 共用之秘密密碼/雜湊的許可 AWS Secrets Manager （例如，稽核基礎設施的密碼）。

建立秘密密碼/雜湊以與 AMS 共用的許可 （例如，需要部署之產品的授權金鑰）。

JSON

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

```
    "Sid": "AllowAccessToSharedNameSpaces",
    "Effect": "Allow",
    "Action": "secretsmanager:*",
    "Resource": [
     "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
     "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
    ]
   },
   {
    "Sid": "DenyGetSecretOnCustomerNamespace",
    "Effect": "Deny",
    "Action": "secretsmanager:GetSecretValue",
    "Resource": "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
   },
   {
    "Sid": "AllowReadAccessToAMSNameSpace",
    "Effect": "Deny",
    "NotAction": [
     "secretsmanager:Describe*",
     "secretsmanager:Get*",
     "secretsmanager:List*"
    ],
    "Resource": "arn:aws:secretsmanager:*:*:secret:ams-shared/*"
   }
  ]
}
```

AMSChangeManagementPolicy

AMSChangeManagementPolicy

請求和檢視所有 AMS 變更類型的許可，以及請求變更類型的歷史記錄。

AMSReservedInstancesPolicy

AMSReservedInstancesPolicy

管理 Amazon EC2 預留執行個體的許可；如需定價資訊，請參閱 Amazon EC2 預留執行個體。

JSON

```
{
```

```
 "Version":"2012-10-17",
 "Statement": [{
  "Sid": "AllowReservedInstancesManagement",
  "Effect": "Allow",
  "Action": [
   "ec2:ModifyReservedInstances",
   "ec2:PurchaseReservedInstancesOffering"
  ],
  "Resource": [
   "*"
  ]
 }]
}
```

AMSS3Policy

AMSS3Policy

從現有 Amazon S3 儲存貯體建立和刪除檔案的許可。

> **Note**
>
> 這些許可不會授予建立 S3 儲存貯體的能力；這些儲存貯體必須使用部署 | 進階堆疊元件 | S3 儲存 | 建立變更類型來完成。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:PutObject"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

AWSSupportAccess

AWSSupportAccess

完整存取 支援。如需詳細資訊，請參閱 入門 支援。如需 Premium Support 資訊，請參閱 支援。

JSON

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

AWSMarketplaceManageSubscriptions

AWSMarketplaceManageSubscriptions（公有 AWS受管政策）

訂閱、取消訂閱和檢視 AWS Marketplace 訂閱的許可。

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
  "Action": [
   "aws-marketplace:ViewSubscriptions",
   "aws-marketplace:Subscribe",
   "aws-marketplace:Unsubscribe"
  ],
  "Effect": "Allow",
  "Resource": "*"
 }]
```

```
}
```

AWSCertificateManagerFullAccess

AWSCertificateManagerFullAccess

完整存取 AWS Certificate Manager。如需詳細資訊，請參閱AWS Certificate Manager。

AWSCertificateManagerFullAccess 資訊，（公有 AWS 受管政策）。

JSON

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

AWSWAFFullAccess

AWSWAFFullAccess

完整存取 AWS WAF。如需詳細資訊，請參閱 AWS WAF - Web Application Firewall。

AWSWAFFullAccess 資訊（公有 AWS 受管政策）。此政策授予 AWS WAF 資源的完整存取權。

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
  "Action": [
   "waf:*",
   "waf-regional:*",
   "elasticloadbalancing:SetWebACL"
```

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

ReadOnlyAccess

`ReadOnlyAccess`

AWS 主控台上所有 AWS 服務和資源的唯讀存取權。 AWS 啟動新服務時，AMS 會更新 ReadOnlyAccess 政策，為新服務新增唯讀許可。更新的許可會套用於政策連接到的所有主體實體。

這不會授予登入 EC2 主機或資料庫主機的能力。

如果您有作用中的 AWS 帳戶，則可以使用此連結 ReadOnlyAccess 來檢視整個 ReadOnlyAccess 政策。整個 ReadOnlyAccess 政策只要提供所有 的唯讀存取權即可 AWS 服務。以下是 ReadOnlyAccess 政策的部分摘錄。

單一帳戶登陸區域 (SALZ)：若要查看 AMS 單一帳戶登陸區域預設、非自訂的使用者角色政策，請參閱 SALZ：預設 IAM 使用者角色，下一步。

SALZ：預設 IAM 使用者角色

預設 AMS 單一帳戶登陸區域使用者角色的 JSON 政策陳述式。

> **Note**
>
> SALZ 預設使用者角色可自訂，且可能因帳戶而異。提供尋找角色的說明。

以下是預設 SALZ 使用者角色的範例。若要確保您已為您設定政策，請執行 `get-role`命令。或者，前往 https：//https://console.aws.amazon.com/iam/ 登入 AWS Identity and Access Management 主控台，然後選擇角色。

客戶唯讀角色是多個政策的組合。角色 (JSON) 的明細如下。

Managed Services 稽核政策：

Managed Services IAM ReadOnly 政策

Managed Services 使用者政策

```
{
 "Version": "2012-10-17",
 "Statement": [
   {
     "Sid": "AllowCustomerToListTheLogBucketLogs",
     "Effect": "Allow",
     "Action": [
       "s3:ListBucket"
     ],
     "Resource": [
       "arn:aws:s3:::mc-a*-logs-*"
     ],
     "Condition": {
       "StringLike": {
         "s3:prefix": [
           "aws/*",
           "app/*",
           "encrypted",
           "encrypted/",
           "encrypted/app/*"
         ]
       }
     }
   },
   {
     "Sid": "BasicAccessRequiredByS3Console",
     "Effect": "Allow",
     "Action": [
       "s3:ListAllMyBuckets",
       "s3:GetBucketLocation"
     ],
     "Resource": [
       "arn:aws:s3:::*"
     ]
   },
   {
     "Sid": "AllowCustomerToGetLogs",
     "Effect": "Allow",
     "Action": [
       "s3:GetObject*"
     ],
```

```
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*/aws/*",
        "arn:aws:s3:::mc-a*-logs-*/encrypted/app/*"
      ]
    },
    {
      "Sid": "AllowAccessToOtherObjects",
      "Effect": "Allow",
      "Action": [
        "s3:DeleteObject*",
        "s3:Get*",
        "s3:List*",
        "s3:PutObject*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AllowCustomerToListTheLogBucketRoot",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*"
      ],
      "Condition": {
        "StringEquals": {
          "s3:prefix": [
            "",
            "/"
          ]
        }
      }
    },
    {
      "Sid": "AllowCustomerCWLConsole",
      "Effect": "Allow",
      "Action": [
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups"
      ],
      "Resource": [
```

```
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Sid": "AllowCustomerCWLAccessLogs",
      "Effect": "Allow",
      "Action": [
        "logs:FilterLogEvents",
        "logs:GetLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:/aws/*",
        "arn:aws:logs:*:*:log-group:/infra/*",
        "arn:aws:logs:*:*:log-group:/app/*",
        "arn:aws:logs:*:*:log-group:RDSOSMetrics:*:*"
      ]
    },
    {
      "Sid": "AWSManagedServicesFullAccess",
      "Effect": "Allow",
      "Action": [
        "amscm:*",
        "amsskms:*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "ModifyAWSBillingPortal",
      "Effect": "Allow",
      "Action": [
        "aws-portal:Modify*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "DenyDeleteCWL",
      "Effect": "Deny",
      "Action": [
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream"
```

```
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Sid": "DenyMCCWL",
      "Effect": "Deny",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:PutLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:/mc/*"
      ]
    },
    {
      "Sid": "DenyS3MCNamespace",
      "Effect": "Deny",
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*/encrypted/mc/*",
        "arn:aws:s3:::mc-a*-logs-*/mc/*",
        "arn:aws:s3:::mc-a*-logs-*-audit/*",
        "arn:aws:s3:::mc-a*-internal-*/*",
        "arn:aws:s3:::mc-a*-internal-*"
      ]
    },
    {
      "Sid": "ExplicitDenyS3CfnBucket",
      "Effect": "Deny",
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::cf-templates-*"
      ]
    },
```

```
    {
      "Sid": "DenyListBucketS3LogsMC",
      "Action": [
        "s3:ListBucket"
      ],
      "Effect": "Deny",
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*"
      ],
      "Condition": {
        "StringLike": {
          "s3:prefix": [
            "auditlog/*",
            "encrypted/mc/*",
            "mc/*"
          ]
        }
      }
    },
    {
      "Sid": "DenyS3LogsDelete",
      "Effect": "Deny",
      "Action": [
        "s3:Delete*",
        "s3:Put*"
      ],
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*/*"
      ]
    },
    {
      "Sid": "DenyAccessToKmsKeysStartingWithMC",
      "Effect": "Deny",
      "Action": [
        "kms:*"
      ],
      "Resource": [
        "arn:aws:kms::*:key/mc-*",
        "arn:aws:kms::*:alias/mc-*"
      ]
    },
    {
      "Sid": "DenyListingOfStacksStartingWithMC",
      "Effect": "Deny",
```

```
      "Action": [
        "cloudformation:*"
      ],
      "Resource": [
        "arn:aws:cloudformation:*:*:stack/mc-*"
      ]
    },
    {
      "Sid": "AllowCreateCWMetricsAndManageDashboards",
      "Effect": "Allow",
      "Action": [
        "cloudwatch:PutMetricData"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AllowCreateandDeleteCWDashboards",
      "Effect": "Allow",
      "Action": [
        "cloudwatch:DeleteDashboards",
        "cloudwatch:PutDashboard"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Customer Secrets Manager 共用政策

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSecretsManagerListSecrets",
      "Effect": "Allow",
      "Action": "secretsmanager:listSecrets",
      "Resource": "*"
```

```
    },
    {
      "Sid": "AllowCustomerAdminAccessToSharedNameSpaces",
      "Effect": "Allow",
      "Action": "secretsmanager:*",
      "Resource": [
        "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
        "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
      ]
    },
   {
      "Sid": "DenyCustomerGetSecretCustomerNamespace",
      "Effect": "Deny",
      "Action": "secretsmanager:GetSecretValue",
      "Resource": "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
    },
    {
      "Sid": "AllowCustomerReadOnlyAccessToAMSNameSpace",
      "Effect": "Deny",
      "NotAction": [
        "secretsmanager:Describe*",
        "secretsmanager:Get*",
        "secretsmanager:List*"
      ],
      "Resource": "arn:aws:secretsmanager:*:*:secret:ams-shared/*"
    }
  ]
}
```

Customer Marketplace 訂閱政策

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowMarketPlaceSubscriptions",
      "Effect": "Allow",
      "Action": [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Subscribe"
```

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

預設存取防火牆規則

這些是存取執行個體所需的預設防火牆規則。

> **Note**
>
> 如需有關建立 AD 單向信任所需的防火牆規則和連接埠的資訊，請參閱 AMS 安全指南，方法是前往 AWS Artifact 主控台 -> 報告索引標籤並搜尋 AWS Managed Services。

Linux 堆疊執行個體連接埠

在 AMS Linux 堆疊中進行身分驗證時，需要這些規則。

Linux 執行個體連接埠規則 FROM：Linux Stack Instance TO： CORP Domain Controller

連接埠	通訊協定	服務	Direction
389	TCP	LDAP	Ingress
389	UDP	LDAP	Ingress
88	TCP	Kerberos	Ingress
88	UDP	Kerberos	Ingress

Windows Stack 執行個體連接埠

在 AMS Windows 堆疊中進行身分驗證時，需要這些規則。

FROM：Windows Stack Instance TO： CORP Domain Controller

連接埠	通訊協定	服務	Direction
88	TCP | UDP	Kerberos	輸入和輸出
135	TCP | UDP	DCE/RPC Locator 服務	輸入和輸出
389	TCP | UDP	LDAP	輸入和輸出
3268	TCP | UDP	msft-gc、Microsoft Global Catalog (LDAP 服務，其中包含來自 Active Directory 樹系的資料）	輸入和輸出
445	TCP	Microsoft-DS Active Directory 、Windows 共用	輸入和輸出
49152 - 65535	TCP	無法向 IANA 註冊的動態或私有連接埠。此範圍用於私有或自訂服務或暫時用途，以及用於暫時性連接埠的自動配置。	輸入和輸出

AWS Managed Services 中的服務管理

主題

AMS 服務的運作方式。

AWS Managed Services 中的帳戶控管

本節涵蓋 AMS 帳戶控管。

您被指派為雲端服務交付經理 (CSDM)，該經理提供跨 AMS 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 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。

AWS Managed Services 中的服務開始

服務起始：AWS Managed Services 帳戶的服務起始日期是第一個日曆月的第一天，之後 AWS 會通知您該 AWS Managed Services 帳戶加入要求中列出的活動已完成；前提是如果 AWS 在某個日曆月的 20 天後發出此類通知，則服務起始日期是該通知日期之後第二個日曆月的第一天。

服務起始

- R 代表負責方執行工作以達成任務。
- 我代表知情；在進度上收到通知的一方，通常只在完成任務或可交付項目時。

服務開始

步驟 #	步驟標題	描述	客戶	AMS
1.	客戶 AWS 帳戶移交	客戶建立新的 AWS 帳戶，並將其移交給 AWS Managed Services	R	I
2.	AWS Managed Services 帳戶 - 設計	完成 AWS Managed Services 帳戶的設計	I	R
3.	AWS Managed Services 帳戶 - 組建	AWS Managed Services 帳戶是根據步驟 2 中的設計建置	I	R

客戶關係管理 (CRM)

AWS Managed Services (AMS) 提供客戶關係管理 (CRM) 程序，以確保與您建立和維護明確定義的關係。此關係的基礎是根據 AMS 對您業務需求的洞察。CRM 程序有助於準確且全面地了解：

- 您的業務需求以及如何滿足這些需求
- 您的功能和限制條件
- AMS 和您的不同責任與義務

CRM 程序允許 AMS 使用一致的方法來為您提供服務，並對您與 AMS 的關係提供控管。CRM 程序包括：

- 識別您的關鍵利益相關者
- 建立控管團隊
- 與您舉行並記錄服務審查會議
- 使用呈報程序提供正式的服務投訴程序

- 實作和監控您的滿意度和意見回饋程序
- 管理您的合約

CRM 程序

CRM 程序包含下列活動：

- 識別和了解您的業務流程和需求。您與 AMS 的協議可識別您的利益相關者。
- 定義要提供的服務，以符合您的需求和要求。
- 在服務審查會議中與您開會，討論 AMS 服務範圍、SLA、合約和您的業務需求的任何變更。可能會與您舉行臨時會議，以討論績效、成就、問題和行動計劃。
- 使用客戶滿意度調查和會議上提供的意見回饋來監控您的滿意度。
- 報告每月內部測量效能報告的效能。
- 與您一起檢閱服務，以判斷改善的機會。這包括經常與您就所提供 AMS 服務的水準和品質進行通訊。

CRM 會議

AMS 雲端服務交付管理員 (CSDMs) 會定期與您進行會議，以討論服務追蹤（操作、安全性和產品創新）和執行追蹤 (SLA 報告、滿意度措施和業務需求的變更）。

會議	用途	Mode	參與者
每週狀態檢閱（選用）	未解決的問題或事件、修補、安全事件、問題記錄 12 週營運趨勢 (+/- 6) 應用程式運算子問題 週末排程	現場客戶location/Telecom/Chime	AMS：CSDM 和雲端架構師 (CA) 客戶指派的團隊成員（例如：雲端/基礎設施、應用程式支援、架構團隊等）
每月業務審查	檢閱服務水準效能（報告、分析和趨勢） 財務分析	現場客戶location/Telecom/Chime	AMS：CSDM、雲端架構師 (CA)、AMS 客戶團隊、AMS 技術

會議	用途	Mode	參與者
	產品藍圖 CSAT		產品經理 (TPM)（選用）、AMS OPS 經理（選用） 您：Application Operator 代表
每季業務審查	記分卡和服務水準協議 (SLA) 效能和趨勢 (6 個月） 即將到來的 3/6/9/12 個月計劃/遷移 風險與風險緩解措施 關鍵改進計劃 產品藍圖項目 符合未來方向的機會 財務 節省成本計畫 業務最佳化	現場客戶位置	AMS：CSDM、雲端架構師、AMS 客戶團隊、AMS 服務主管、AMS 操作管理員 您：Application Operator 代表、Service 代表、Service Director

CRM 會議安排

AMS CSDM 負責記錄會議，包括：

- 建立議程，包括動作項目、問題和出席者清單。
- 建立每次會議審查的動作項目清單，以確保項目按排程完成和解決。
- 在會議後的一個工作天內，透過電子郵件將會議記錄和動作項目清單分發給會議出席者。
- 將會議記錄存放在適當的文件儲存庫中。

如果沒有 CSDM，領導會議的 AMS 代表會建立和分發會議記錄。

> **Note**
>
> 您的 CSDM 會與您一起建立您的帳戶控管。

CRM 每月報告

您的 AMS CSDM 會準備並傳送每月服務效能簡報。簡報包含下列資訊：

- 報告日期
- 摘要和洞見：
  - 關鍵標註：總和作用中堆疊計數、堆疊修補狀態、帳戶加入狀態（僅限加入期間）、客戶特定問題摘要
  - 效能：事件解決、警示、修補、變更請求 (RFCs)、服務請求，以及主控台和 API 可用性的統計資料
  - 問題、挑戰、疑慮和風險：客戶特定問題狀態
  - 近期項目：客戶特定的加入或事件解決計劃
- 受管資源：堆疊的圖形和圓餅圖
- AMS 指標：監控和事件指標、事件指標、AMS SLA 遵循指標、服務請求指標、變更管理指標、儲存指標、持續性指標、Trusted Advisor 指標和成本摘要（以多種方式呈現）。功能請求。聯絡資訊。

> **Note**
>
> 除了所描述的資訊之外，您的 CSDM 也會通知您範圍或條款的任何重大變更，包括由 AMS 使用承包商進行營運活動。
>
> AMS 會產生有關 CSDM 包含在每月報告中的修補和備份的報告。在報告產生系統中，AMS 會將一些您無法存取的基礎設施新增至您的帳戶：
>
> - 報告原始資料的 S3 儲存貯體
> - Athena 執行個體，具有查詢定義來查詢資料
> - 從 S3 儲存貯體讀取原始資料的 Glue 爬蟲程式

AWS Managed Services 中的成本最佳化

AWS Managed Services 會在每月業務審查 (MBRs) 期間，每月為您提供詳細的成本使用率和節省報告。

AMS 遵循一組標準程序和機制，以識別受管帳戶中的成本節省管道，並協助您規劃和推展變更，以最佳化您的 AWS 支出。

> **Note**
>
> AMS 正在開發影片，以協助成本最佳化。第一步是為您提供 PDF 和 Excel 試算表，其中包含成本最佳化最佳實務。若要存取這些資源，請開啟成本最佳化 ZIP 檔案的快速指南。

成本最佳化架構

AMS 會遵循三個階段的方法，以最佳化您的 AWS 成本：

1. 識別受管環境中的成本最佳化管道
2. 向您介紹成本最佳化計劃
3. 協助以可衡量的方式實現成本最佳化

識別受管環境中的成本最佳化管道

AMS AWS 利用成本總管和 Trusted Advisor 等原生工具，同時利用架構最佳化、EC2 執行個體和以 AWS 帳戶為中心的最佳化等超過 20 種節省成本模式，為您建立量身打造的成本節省建議。

部分最佳化建議包括下列項目。

架構最佳化建議：

- 最佳 S3 儲存類別使用：Amazon S3 提供各種儲存類別，以根據資料存取、彈性和成本滿足各種工作負載需求。根據工作負載需求的 S3 Intelligent-Tiering 和 S3 儲存類別分析可讓您有效率地管理 S3 成本。
- 使用快取架構：在適用的情況下，利用快取執行個體可協助您取代某些資料庫執行個體，同時滿足您的 IOPS 需求。
- EBS 升級節省：將您的 EBS 磁碟區從 gp2 遷移至 gp3 可節省高達 20% 的成本，無論磁碟區大小為何，您都可以利用可預測的 3，000 IOPS 基準效能和 125 MiB/s。

- 使用彈性： AWS 提供的自動擴展功能允許有效的資源使用率和成本最佳化途徑。根據需求定期檢閱和更新執行個體擴展政策，進一步節省成本。

EC2 以執行個體為中心的建議

- 執行個體權利調整：專注於根據用量調整執行個體大小和最佳組態的建議。建議也包括使用 Amazon EC2 Auto Scaling 功能，並在適用於 Amazon S3 上的 AWS Lambda 或靜態 Web 內容時取代 EC2 執行個體。
- 執行個體排程：使用 AMS Resource Scheduler 根據時間排程自動啟動和停止執行個體有助於控制成本，尤其是在非營業時間內未使用的非生產執行個體。
- 訂閱 Savings Plans：Savings plan 是節省 AWS 用量最簡單的方式。相較於 Amazon ECEC2 Instance Savings Plans 最多可節省 72%。 Amazon EC2 Amazon SageMaker AI Savings Plans 為您的 Amazon SageMaker AI 服務用量提供高達 64% 的折扣。AMS 會根據您的 AWS 資源使用量，提供有關 Savings 計劃的適當建議。
- 預留執行個體 (RI) 用量和耗用量指引：Amazon EC2 預留執行個體 (RI) 提供相較於隨需定價的大幅折扣 （ 高達 75%)，並在用於特定可用區域時提供容量保留。
- Spot 執行個體用量：容錯工作負載可以使用 Spot 執行個體，並將價格降低至 90%。
- 閒置執行個體終止：識別和報告閒置或可終止的低使用率執行個體。

以帳戶為中心的建議

- 帳戶清除：在帳戶層級，AMS 也會識別未使用的 EBS 磁碟區、重複的 CloudTrail 追蹤、具有未使用資源的空帳戶等，並提供清除建議。
- SLA 建議：此外，AMS 會定期檢閱您的 Plus 和 Premium 帳戶，並建議為帳戶選擇正確的 SLA 層級。
- AMS 自動化最佳化：AMS 會持續最佳化用於提供 AMS 服務的 AMS 自動化和基礎設施。

向客戶展示並協助規劃

AMS 會與主要客戶利益相關者進行每月業務審查 (MBRs)，並呈現可節省成本的管道、機制和建議，以及潛在的節省成本。我們進一步與您合作，規劃所需的變更。

協助建議實作並衡量成本影響

AMS 可協助實現和衡量成本影響和最佳化變更。

您可以評估建議變更的應用程式影響、風險和成功條件，並透過 AMS 主控台提出適當的變更請求 (RFCs)。AMS 會與您合作，並在受管帳戶中實作與成本最佳化相關的變更。AMS 會測量成本影響，並在每月業務審查 (MBRs) 中包含實現的節省。

成本最佳化責任矩陣

AMS 成本最佳化中的責任。

成本最佳化 RACI

活動	客戶	AMS
編譯節省成本的建議並準備報告	I	R
呈現節省成本報告	C	R
規劃與節省成本相關的變更	R	C
評估變更的影響和風險	R	C
提高RFCs以實作變更	R	C
檢閱RFCs並實作變更	C	R
測試應用程式並驗證變更實作	R	C

活動	客戶	AMS
測量變更後的成本影響並向客戶展示	I	R

AWS Managed Services 中的服務時數

功能	AMS 進階
	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
監控和提醒	全年無休
自動化變更請求 (RFC)	全年無休
非自動化的變更請求 (RFC)	全年無休
雲端服務交付管理員 (CSDM)	週一至週五：當地上班時間 08：00–17：00

在 AWS Managed Services 中取得說明

AMS 一年 365 天、每週 7 天、每天 24 小時為您提供事件管理、服務請求管理和變更管理的支援（根據套用至帳戶的 AMS 服務水準協議）。

若要報告影響受管環境的 AWS 或 AMS 服務效能問題，請使用 AMS 主控台並提交事件報告。如需詳細資訊，請參閱報告事件。如需 AMS 事件管理的一般資訊，請參閱事件回應。

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，請建立服務請求。如需 AMS 服務請求的一般資訊，請參閱服務請求管理。

變更管理模式

AWS Managed Services (AMS) 使用變更管理模式來保護 AMS Advanced 中的變更。變更管理模式可協助您維持環境的高操作標準，並控制風險並防止負面影響。AMS Advanced 有不同的模式，可提供不同層級的控制和風險。除了客戶受管模式之外，所有模式都由 AMS 管理。以下是可用的變更管理模式：

- RFC 模式 （ 先前為標準 CM 模式 ）：提供「變更請求」(RFC) 系統和 AMS 自訂變更類型 (CTs)
- 直接變更模式：與 RFC 模式相同，加上使用 AWS APIs 和主控台來建立 AMS 受管資源
- AMS 上的 AWS Service Catalog：類似於直接變更模式，但不是使用 AMS 變更管理系統 (RFCs)，而是使用 AWS Service Catalog 來建立 AMS 接著管理的資源。
- 開發人員模式：與直接變更模式相同，只有您使用 AWS APIs 和主控台建立的資源不受 AMS 管理 - 您要負責其管理
- 自助服務佈建 (SSP) 模式：與開發人員模式相同，但無法存取 AMS 變更管理系統 （ 無 RFCs)
- 客戶受管模式：AMS 為您提供多帳戶登陸區域登陸區域，但所有資源管理都是您的責任

AWS Managed Services (AMS) 變更管理系統使用變更管理 (CM) API，為多帳戶登陸區域 (MALZ) 和單一帳戶登陸區域 (SALZ) 帳戶提供建立和管理變更請求 (RFCs) 的操作。

變更請求 (RFC) 是您或 AMS 透過 AMS 界面建立的請求，用於對受管環境進行變更，並包含特定操作的變更類型 (CT) ID。

AMS 變更管理 (CM) API 提供建立和管理變更請求 (RFCs的操作。您可以建立、更新、提交、核准、拒絕和取消 RFCs。AMS 運算子可以建立、更新、提交、核准、拒絕、取消並將 RFCs標記為關閉。

如需不在標籤或其他名稱中使用的 AMS 預留字首清單，請參閱預留字首。

如需每個變更類型的資訊，包括結構描述和範例，請參閱 AMS 變更類型參考。

> **Note**
>
> 所有變更管理 API 呼叫都會記錄在 AWS CloudTrail 中。如需詳細資訊，請參閱存取您的日誌。

模式概觀

使用此資訊來協助您選擇適當的 AWS Managed Services (AMS) 模式來託管您的應用程式，這取決於您實現業務成果所需的彈性和規範控管組合。

此資訊的目標對象為：

- 客戶團隊負責其登陸區域的策略和管理。此資訊將協助團隊規劃 AMS 受管登陸區域的基礎，以及他們想要提供給其內部和外部客戶的 AMS 模式。
- 負責將應用程式遷移至 AMS 的業務和應用程式擁有者。此資訊將有助於規劃應用程式遷移，並使用適當的 AMS 模式來遷移/託管其應用程式。請注意，相同的應用程式可以在其軟體開發生命週期 (SDLC) 生命週期的不同階段，以多個 AMS 模式託管。
- AMS 合作夥伴的任務是引導客戶了解建置和遷移至 AMS 的不同選項。

在設定 AMS 受管平台的基礎階段，以及當您從基礎轉換到雲端採用之旅的遷移階段時，這些資訊最有用，就在加入 AMS 完成後，而且您專注於應用程式控管和操作。

AMS 中的模式和帳戶類型

AWS Managed Services (AMS) 模式可以定義為在每種模式的特定控管架構下與 AMS 服務互動的方式。會記下登陸區域差異、多帳戶登陸區域或 MALZ 和單一帳戶登陸區域或 SALZ。

> **Note**
>
> 如需應用程式部署和選擇正確 AMS 模式的詳細資訊，請參閱 AMS 模式和應用程式或工作負載。
> 如需不同模式的實際使用案例，請參閱 AMS 模式的實際使用案例

下表提供每個 AMS 服務模式的說明。

AMS 功能	RFC 模式（先前為標準 CM 模式）/OOD*	直接變更模式	AWS Service Catalog	自助式佈建/開發人員模式	客戶受管
登陸區域組態	MALZ 和 SALZ	MALZ 和 SALZ		MALZ 和 SALZ	

AMS 功能	RFC 模式（先前為標準 CM 模式）/OOD*	直接變更模式	AWS Service Catalog	自助式佈建/開發人員模式	客戶受管
變更管理	變更排程、檢閱手動變更和變更記錄	與 RFC 模式相同，適用於高風險變更，例如 IAM 或安全群組	無		
記錄、監控、護欄和事件管理	是（支援的資源）			否	
持續性管理	是（支援的資源）			不適用/否	否
安全管理	執行個體層級安全控制和帳戶層級控制			帳戶層級控制項	AWS Org 層級控制
修補管理	是			不適用/否	否
事件和問題管理	AMS 支援資源的回應和解析 SLA			所產生資源的回應 SLA	否
報告	是			否	
服務請求管理	是			僅支援請求	否

*隨需操作 (OOD) 提供客戶使用 RFC 模式透過專用資源管理變更的服務。如需詳細資訊，請參閱 方案的隨需操作目錄，並與您的雲端服務交付管理員 (CSDM) 交談。

> **Note**
>
> AMS 中的自助式佈建模式 和 AMS 進階開發人員模式可能都適合根植於原生 AWS Services 的複雜架構的應用程式。架構工作負載時，您可以根據您的業務環境，在卓越營運和敏捷性之間

做出取捨。這是考慮為您的應用程式選取 SSP 模式或開發人員模式的好方法。選項也可能根據應用程式的 SDLC 階段而變更。例如：當應用程式為生產就緒時，SSP 模式可能會因為在此模式下的 AMS 護欄更嚴格，而成為更適當的選項。護欄是以預防性控制的形式強制執行，例如應用程式 OU 層級的 IAM 更新和 SCPs RFC 型變更控制。這些業務決策可以讓您了解工程設計的優先順序。您可以最佳化 ，以增加應用程式擁有者在「生產前」階段的彈性，而犧牲控管和營運支援。

MALZ 架構和相關聯的 AMS 模式

AMS 多帳戶登陸區域 (MALZ) 可讓您選擇自動佈建預設組織單位 (OU) 下的應用程式帳戶 （或資源帳戶）：客戶受管 OU、受管 OU 或開發 OU。在每個 OUs 下建立的應用程式帳戶中佈建的基礎設施，受限於這些基礎 OUs 提供的特定 AMS 模式。在同一個應用程式帳戶中尋找兩種或多種模式的混合是很常見的。例如：RFC 模式和 SSP 模式可以共存於託管由 API Gateway 和 Lambda 組成之管道架構的 AMS 受管帳戶中，用於觸發函數，以及用於擷取和協同運作的 EC2, S3 和 SQS。在此情況下，SSP 模式會套用至 Lambda 和 API Gateway。

圖 1 顯示如何在 AMS 中透過基礎 OUs 提供不同的模式。在 AMS 中請求新的應用程式帳戶時，您必須選取帳戶的 OU。

MALZ 架構和相關聯的 AMS 模式

AMS 利用以 AWS 最佳實務為基礎的基礎 OUs，做為使用服務控制政策 (SCPs) 邏輯管理帳戶的方法。這可做為對每個 AMS 模式強制執行控管架構的方法。套用至基礎 OUs 的任何控管和安全護欄（以 SCPs 的形式） 也會自動套用至自訂/子 OUs。您可以為子 OUs 請求其他 SCPs。請務必了解應用程式帳戶與 模式不同。模式會套用至帳戶內佈建的基礎設施，並定義 AMS 與客戶之間的操作責任。

圖 1：MALZ 架構和相關聯的 AMS 模式

> **Note**
>
> 「限制性」表示您可以為這些 OUs 請求自訂政策，這些政策由 AMS case-by-case核准，以確保它們不會干擾 AMS 提供卓越營運的能力。如需 AMS 護欄的詳細清單，請參閱《 使用者指南》中的 AMS 護欄。

AMS 模式和應用程式或工作負載

選擇正確的模式時，請考慮應用程式的營運和管理需求，方法是請求新的應用程式帳戶或在現有的應用程式帳戶中託管應用程式。為每個應用程式或工作負載選擇適當的 AMS 模式取決於下列因素：

- 環境將提供的 SDLC 生命週期函數類型（例如，具有未修改變更的沙盒、具有一些頻繁變更的 UAT、具有最少變更且受到高度管制的生產）
- 所需的控管政策（在 OU 層級透過 SCPs 強制執行）
- 操作模型（如果您想要承擔操作責任，或想要將其委外至 AMS)
- 所需的業務成果，例如在雲端中操作的時間，以及操作成本。

> **Note**
>
> 如需每個 AMS 服務的模式類型說明，請參閱 AMS 中的模式和帳戶的類型。
> 如需不同模式的實際使用案例，請參閱 AMS 模式的實際使用案例

下表概述應用程式擁有者的關鍵考量事項，以協助決定最適合的 AMS 模式。應用程式擁有者應在應用程式遷移之前包含評估階段，以完全了解適用於其特定應用程式的模式。範例：對於以雲端原生服務或無伺服器架構為基礎的應用程式，最佳選項可能是開始在開發人員模式下建置和反覆運算，並使用 AMS Managed – SSP 模式將最終基礎設施部署為程式碼。在這種情況下，可能需要進行光線重構，以確保為自動部署建立的任何 CloudFormation 範本都符合 AMS 制定的擷取準則。此外，任何 IAM 許可都需要 AMS Security 核准，以確保它們遵循最低權限模型。

選取來託管應用程式的 AMS 模式，可協助您建置所需的雲端操作模型。

> **Note**
>
> 根據為託管應用程式選取的不同 AMS 模式，單一 AMS 受管登陸區域中可以存在多個雲端操作模型。

決策問題	標準 CM 模式/OOD*	AWS Service Catalog	直接變更模式	自助式佈建	開發人員模式	客戶受管
操作準備						

決策問題	標準 CM 模式/OOD*	AWS Service Catalog	直接變更模式	自助式佈建	開發人員模式	客戶受管
記錄、監控和事件管理	負責所有受管基礎設施的 AMS			負責自助服務佈建服務 (SSP) 的客戶	客戶負責在 AMS CM 系統外使用開發人員 IAM 角色佈建的資源	客戶負責
持續性管理	AMS 負責執行客戶選取的備份計劃			負責自助服務佈建服務 (SSP) 的客戶	客戶負責在 AMS CM 系統外使用開發人員 IAM 角色佈建的資源	
執行個體層級存取管理	使用內部部署網域透過單向 AD 信任管理的 AMS。需要受管基礎設施才能加入 AMS 網域			不適用	客戶負責在 AMS CM 系統外使用開發人員 IAM 角色佈建的資源	
安全管理和帳戶層級存取管理	所有受管帳戶的 AMS 責任			負責所有受管帳戶的 AMS	客戶負責在 AMS CM 系統外使用開發人員 IAM 角色佈建的資源	

決策問題	標準 CM 模式/OOD*	AWS Service Catalog	直接變更模式	自助式佈建	開發人員模式	客戶受管
修補管理	所有受管帳戶的 AMS 責任			負責自助服務佈建服務 (SSP) 的客戶	客戶負責在 AMS CM 系統外使用開發人員 IAM 角色佈建的資源	
變更管理	所有受管帳戶的 AMS 責任			負責自助服務佈建服務 (SSP) 的客戶	客戶負責在 AMS CM 系統外使用開發人員 IAM 角色佈建的資源	
佈建管理	AMS 中提供的佈建選項的規範和標準化	依照 AMS 規範標準直接使用 AWS Service Catalog 的 AWS 服務 API 的彈性	依照 AMS 規範標準直接使用 AWS 服務 API 的彈性	為 SSP 服務直接使用 AWS 服務 APIs彈性	直接使用 AWS 服務 API 進行佈建的彈性	
事件管理和稽核	所有受管帳戶的 AMS 回應				客戶負責在 AMS 變更管理系統外使用開發人員 IAM 角色佈建的資源	

決策問題	標準 CM 模式/OOD*	AWS Service Catalog	直接變更模式	自助式佈建	開發人員模式	客戶受管
GuardRails 和共用基礎設施（網路）和安全架構	使用 AMS 核心帳戶的規範和標準化					彈性和自訂運用 AMS 核心帳戶
應用程式整備						
應用程式重構	需要光線重構				需要光線重構（如果使用 AMS 標準 CM 佈建）	不需要重構
支援 AWS 服務	僅限於 AMS 支援的內容					不受限制
業務考量事項						
操作就緒時間	三到六個月			6 個月以上取決於客戶應用程式操作能力		6-18 個月取決於客戶基礎設施和應用程式操作能力
成本	$$$$			$$$	$$	$

決策問題	標準 CM 模式/OOD*	AWS Service Catalog	直接變更模式	自助式佈建	開發人員模式	客戶受管
應用程式範例	具有 3 層堆疊的 Web 伺服器，具有合規和法規要求的應用程式			使用 API Gateway 的 Web 伺服器，利用 ECS/EKS 的容器化應用程式	在使用 Lambda、Glue、Athena 等的 Data Lake 應用程式上反覆/最佳化	分散式帳戶/應用程式，例如沙盒、第三方受管應用程式

*隨需操作 (OOD) 提供客戶使用標準 CM 模式，透過專用資源管理其變更。如需詳細資訊，請參閱 隨需操作方案目錄，並與您的雲端服務交付管理員 (CSDM) 交談。

> **Note**
>
> SSP 模式和開發人員模式之間的價格比較假設已佈建相同的 AWS 服務。

比較 AMS 模式與業務和 IT 目標

如所示，如果您要為應用程式尋找高度受控和標準化的控管模型，則 AMS 受管的標準變更、AWS Service Catalog 或直接變更模式是最適合的。如果您需要專注於應用程式創新的自訂控管模型，而不需要操作準備，請選取客戶受管模式。使用客戶受管模式，當您負責建立人員、程序和工具以支援操作功能時，可能需要更長的時間來操作應用程式，例如事件管理、組態管理、佈建管理、安全管理、修補程式管理等。

AMS 模式的真實使用案例

檢查這些項目，以協助判斷如何使用 AMS 模式。

- 使用案例 1，透過時間敏感的資料中心退出來降低成本的必要業務：具有吸引人業務事件的企業，例如資料中心退出，有興趣在雲端上重新託管其內部部署應用程式。大多數現場部署庫存都由 Windows 和 Linux 伺服器組成，並混合作業系統版本。如此一來，客戶也想要利用遷移到雲端提供的成本節省，並改善其應用程式的技術和安全狀態。客戶想要快速移動，但尚未建置內部雲端操作專業知識。客戶必須找到重構的平衡，太多重構可能會對緊迫的時間軸造成風險。不過，透過一些重

構，例如更新作業系統版本和最佳化資料庫，應用程式可以實現更高水準的效能。在此範例中，客戶可以選擇 AMS 受管 RFC 模式來重新託管大部分的應用程式。AMS 提供基礎設施操作，同時引導客戶操作團隊在雲端中安全操作的最佳實務。

AMS 受管 AWS Service Catalog 和 AMS 受管直接變更模式可為客戶提供額外的靈活性，同時實現相同的業務成果和目標。此外，客戶可以使用 AMS Operations On Demand (OOD) 產品，讓專用 AMS 操作工程師優先執行變更請求 (RFCs)。

將未差異化的基礎設施操作任務（修補、備份、帳戶管理等）卸載至 AMS 時，客戶可以繼續專注於最佳化其應用程式，並在雲端操作上提升其內部團隊。AMS 會每月向客戶提供節省成本的報告，並針對資源最佳化提出建議。在此使用案例中，如果在 Windows 2003 和 2008 等舊版作業系統上託管end-of-life應用程式，而客戶決定不重構，則這些應用程式也可以遷移到 AMS 並託管在利用客戶受管模式的帳戶。

- 使用案例 2，在安全的 AMS 界限內使用 Lambda、Glue、Athena 建置資料湖：企業希望設定 Data Lake，以滿足 AMS 中多個應用程式的報告需求。客戶想要使用 S3 儲存貯體來儲存資料集，而 AWS Athena 會針對每個報告的資料集進行查詢。S3 和 AWS Athena 將部署在不同的 AMS 受管帳戶中。使用 S3 的帳戶也有其他服務，例如 Glue、Lambda 和 Step Functions，以建置資料擷取管道。在這種情況下，Glue、Lambda、Athena 和 Step Functions 被視為自助式佈建 (SSP) 服務。客戶也在帳戶中部署 EC2 執行個體，做為臨機操作工具/指令碼伺服器。客戶從請求 AMS 在其 AMS 受管帳戶中啟用 SSP 服務開始。AMS 會為客戶可擔任的每個服務佈建 IAM 角色，一旦該角色加入到客戶的聯合解決方案。為了方便管理，客戶也可以將個別 IAM 角色的政策合併為一個自訂角色，減輕在 AWS 服務之間工作時切換角色的需求。在帳戶中啟用角色後，客戶就可以根據其需求設定服務。不過，客戶必須使用 AMS 變更管理系統來請求其他許可，視其使用案例而定。

  例如，若要存取 Glue 爬蟲程式，Glue 需要額外的許可。還需要其他許可才能建立 Lambda 的事件來源。客戶將使用 AMS 更新 IAM 角色，以允許 Athena 跨帳戶存取查詢 S3 儲存貯體。還需要透過 Lambda 的 AMS 變更管理更新服務角色或服務連結角色，以呼叫 Step Functions 服務，以及透過 Glue 讀取和寫入所有 S3 儲存貯體。AMS 與客戶合作，確保遵循最低權限的存取模型，並且請求的 IAM 變更不會過度寬鬆，並使環境面臨不必要的風險。客戶的資料湖團隊會花費時間規劃客戶架構特定服務所需的所有 IAM 許可，並請求 AMS 啟用這些許可。這是因為所有 IAM 變更都會手動處理，並經過 AMS 安全團隊的審核。應用程式部署排程中應考量處理這些請求的時間。

  由於 SSP 服務在帳戶中運作，客戶可以透過 AMS 事件管理和服務請求請求支援和報告問題。不過，AMS 不會主動監控 Lambda 的效能和並行指標，或 Glue 的工作指標。客戶有責任確保為 SSP 服務啟用適當的記錄和監控。帳戶中的 EC2 執行個體和 S3 儲存貯體完全由 AMS 管理。
- 使用案例 3，在 AMS 中快速且靈活地設定 CICD 部署管道：客戶希望設定以 Jenkins 為基礎的 CICD 管道，將程式碼管道部署到 AMS 中的所有應用程式帳戶。客戶可能會發現它最適合在 AMS

受管直接變更模式 (DCM) 或 AMS 受管開發人員模式下託管此 CICD 管道，因為它可靈活地在 EC2 上設定具有所需自訂組態的 Jenkins 伺服器，並具有所需的 IAM 許可來存取 CloudFormation 和託管成品儲存庫的 S3 儲存貯體。雖然這也可以在 AMS 受管 RFC 模式中完成，但客戶團隊需要為 IAM 角色建立多個手動 RFCs，以針對 AMS 手動檢閱的最低許可集進行反覆運算。DCM 可讓客戶在 AWS 上實現其營運目標，同時避免在使用 AMS 受管 RFCs 模式時為 IAM 角色建立多個手動 RFC 的需求，以針對 AMS 手動檢閱的最低寬鬆許可集進行反覆運算。這需要時間和客戶方面的教育，才能提升 AMS 程序和工具。使用開發人員模式，客戶可以從「開發人員角色」開始，使用原生 AWS APIs 佈建基礎設施。設定此管道最快速且最靈活的方法是使用 AMS Managed-Developer 模式。開發人員模式提供最快速且最簡單的方式，同時犧牲操作整合，而 DCM 的靈活性較低，但確實提供與 RFC 模式相同的操作支援層級。

- 使用案例 4，AMS 基礎中的自訂操作模型：客戶正在查看截止日期驅動的資料中心退出，且其其中一個企業應用程式完全由第三方 MSP 管理，包括應用程式操作和基礎設施操作。假設客戶沒有時間重新考慮此應用程式，因此可以由 AMS 操作，則客戶受管模式是適合的選項。客戶可以利用 AMS 受管登陸區域的自動化和快速設定。他們可以利用集中式帳戶管理，透過集中式聯網帳戶控制帳戶販賣和連線。它還透過 AMS Payer 帳戶合併所有客戶受管帳戶的費用，以簡化其帳單。客戶可以靈活地設定其自訂存取管理模型，其 MSP 與用於 AMS 受管帳戶的標準存取管理不同。如此一來，使用客戶受管模式，他們可以設定 AMS 受管環境，同時滿足清空內部部署環境的業務需求。在此情況下，如果客戶也有要遷移至雲端的 Windows 應用程式，並選擇將他們移至客戶受管帳戶，則客戶必須負責建立雲端操作模型。視客戶轉換傳統 IT 程序及訓練人員的能力而定，這可能會複雜、昂貴且耗時。客戶可以透過將此類工作負載「抬高和轉移」到 AMS 受管帳戶，並將基礎設施操作卸載到 AMS 來節省時間和成本。

  > **Note**
  >
  > 客戶有時可能會覺得需要在 RFC 或 SSP 模式的控管架構與開發人員模式之間移動應用程式帳戶。例如，客戶可以在 AMS 受管模式下託管應用程式，做為初始提升和轉移遷移的一部分，但加班想要重新寫入應用程式，以針對雲端原生 AWS 服務將其最佳化。他們可以將生產前帳戶的模式從 AMS 受管 RFC 變更為 AMS 受管開發人員模式，為他們提供佈建基礎設施的靈活性和敏捷性。不過，一旦使用「開發人員角色」進行基礎設施佈建變更，相同的基礎設施就無法移回 AMS 受管 RFC 模式。這是因為 AMS 無法保證在 AMS 變更管理系統之外佈建的基礎設施操作。客戶可能需要建立新的應用程式帳戶，以提供 AMS 受管 RFC 模式，然後透過 CloudFormation 範本或擷取至 AMS 受管帳戶的自訂 AMIs 重新部署「最佳化」基礎設施組態。這是部署生產就緒組態的乾淨方法。部署後，應用程式將受到規範的 AMS 控管和操作。這同樣適用於客戶受管模式和 AMS 受管模式之間的切換模式。

RFC 模式

RFC 模式是 AMS Advanced 操作計劃客戶的預設模式。其中包括變更管理系統，其中包含變更或 RFCs的請求，以及變更類型的目錄，可用來請求對帳戶新增或變更所需的變更。此變更管理系統提供安全層級，以限制誰可以變更您的帳戶。

如需 AMS 進階變更類型的詳細資訊，請參閱什麼是 AMS 變更類型？。

如需加入 AMS Advanced 的詳細資訊，請參閱 AWS Managed Services 加入簡介。

如需變更類型範例演練，請參閱 AMS 進階變更類型參考依分類變更類型一節中相關變更類型的「其他資訊」一節。

> **Note**
>
> RFC 模式先前稱為「變更管理模式」或「標準 CM 模式」。

主題

- 了解 RFCs
- 什麼是變更類型？
- 針對 AMS 中的 RFC 錯誤進行故障診斷

了解 RFCs

變更請求或 RFCs 會以兩倍的方式運作。首先，RFC 本身需要參數。這些是 `CreateRfc` API 中的選項。其次，RFC 的動作需要參數（執行參數）。若要了解`CreateRfc`選項，請參閱 AMS API 參考的 CreateRfc 一節。這些選項通常會出現在建立 RFC 頁面的其他組態區域中。

您可以使用 `CreateRfc` API、CLI 或使用 AMS `aws amscm create-rfc` 主控台建立 RFC 頁面來建立和提交 RFC。如需建立 RFC 的教學課程，請參閱 建立 RFC。

主題

- 什麼是 RFCs？
- 使用 AMS API/CLI 進行身分驗證
- 了解 RFC 安全性審查
- 了解 RFC 變更類型分類

- 了解 RFC 動作和活動狀態
- 了解 RFC 狀態碼
- 了解 RFC 更新 CTs和 CloudFormation 範本偏離偵測
- 排程 RFCs
- 核准或拒絕 RFCs
- 請求 RFC 限制執行期間
- 建立、複製、更新、尋找和取消 RFCs
- 搭配 RFCs 使用 AMS 主控台
- 了解常見的 RFC 參數
- 註冊 RFC 每日電子郵件

什麼是 RFCs？

變更請求或 RFC 是您在 AMS 受管環境中進行變更的方式，或要求 AMS 代表您進行變更的方式。若要建立 RFC，您可以選擇 AMS 變更類型、選擇 RFC 參數（例如排程），然後使用 AMS 主控台或 API 命令 CreateRfc 和 SubmitRfc 提交請求。

RFC 包含兩個規格，一個用於 RFC 本身，另一個用於變更類型 (CT) 參數。在命令列，您可以使用內嵌 RFC 命令或 JSON 格式的標準 CreateRfc 範本，該範本是您填寫並提交的，以及您建立的 CT JSON 結構描述檔案（根據 CT 參數）。CT 名稱是 CT 的非正式描述。CSIO（類別、子類別、項目、操作）是 CT 的更正式描述。建立 RFC 時，只能指定 CT ID。

當變更成功完成（成功）或失敗（失敗）時，AMS 會通知您。

> **Note**
>
> 如需 RFC 失敗疑難排解的資訊，請參閱 針對 AMS 中的 RFC 錯誤進行故障診斷。

下圖說明您提交的 RFC 工作流程。

使用 AMS API/CLI 進行身分驗證

使用 AMS API/CLI 時，您必須使用臨時憑證進行身分驗證。若要請求聯合身分使用者的臨時安全登入資料，請 cal GetFederationToken、AssumeRole、AssumeRoleWithSAML 或 AssumeRoleWithWebIdentity AWS 安全字符服務 (STS) APIs。

常見的選擇是 SAML。設定之後，您會將 引數新增至您呼叫的每個操作。例如：`aws --profile saml amscm list-change-type-categories`。

SAML 2.0 設定檔的捷徑是在每個 API/CLI 開始時使用 設定設定檔變數 `set AWS_DEFAULT_PROFILE=saml`（對於 Windows；對於 Linux，則為 `export AWS_DEFAULT_PROFILE=saml`）。如需設定 CLI 環境變數的詳細資訊，請參閱設定 AWS 命令列界面、環境變數。

了解 RFC 安全性審查

AWS Managed Services (AMS) 變更管理核准程序可確保我們對您帳戶中所做的變更執行安全審查。

AMS 會根據 AMS 技術標準評估所有變更請求 (RFCs)。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。在安全性審查期間，AMS 會強調相關風險，並且在高或極高安全性風險的情況下，您的授權安全人員會接受或拒絕 RFC。也會評估所有變更，以評估對 AMS 操作能力的負面影響。如果發現潛在的負面影響，則需要在 AMS 內進行額外的審核和核准。

AMS 技術標準

AMS 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。AMS 和您都必須遵循這些標準。

任何可能因為偏離技術標準而降低您帳戶安全狀態的變更，都會經過風險接受程序，其中 AMS 會反白顯示相關風險，並由授權安全人員從您端接受或拒絕。也會評估所有此類變更，以評估是否對 AMS 操作帳戶的能力有任何負面影響，如果是，則需要在 AMS 內進行額外的審核和核准。

RFC 客戶安全風險管理 (CSRM) 程序

當您的組織某人請求變更您的受管環境時，AMS 會檢閱變更，以判斷請求是否會因超出技術標準而使帳戶的安全狀態惡化。如果請求確實降低了帳戶的安全狀態，AMS 會向您的安全團隊聯絡人通知相關風險，並執行變更；或者，如果變更在環境中帶來高或非常高的安全風險，則 AMS 會以風險接受的形式向您的安全團隊聯絡人尋求明確核准（接下來說明）。AMS 客戶風險接受程序旨在：

- 確保明確識別風險並傳達給正確的擁有者
- 將已識別的環境風險降至最低
- 從了解組織風險設定檔的指定安全聯絡人取得並記錄核准
- 降低已識別風險的持續營運開銷

如何存取技術標準和高風險或極高風險

我們已提供 AMS 技術標準文件供您在 https://console.aws.amazon.com/artifact/ 中做為報告參考。使用 AMS 技術標準文件，了解在提交變更請求 (RFC) 之前，變更是否需要您的授權安全聯絡人接受風險。

使用預設 AWS Managed Services (AMS) 技術標準」，以尋找技術標準報告。 AWS Artifact AWSManagedServicesChangeManagementRole

> **Note**
>
> 單一帳戶登陸區域中的 Customer_ReadOnly_Role 可存取 AMS 技術標準文件。在多帳戶登陸區域中，安全管理員使用的 AWSManagedServicesAdminRole 和應用程式團隊使用的 AWSManagedServicesChangeManagementRole 可用來存取文件。如果您的團隊使用自訂角色，請建立其他 | 其他 RFC 來請求存取權，我們將更新指定的自訂角色。

了解 RFC 變更類型分類

您在提交 RFC 時使用的變更類型分為兩個廣泛的類別：

- 部署：此分類用於建立 資源。
- 管理：此分類用於更新或刪除資源。Management 類別也包含存取執行個體、加密或共用 AMIs，以及啟動、停止、重新啟動或刪除堆疊的變更類型。

了解 RFC 動作和活動狀態

`RfcActionState` (API) / 活動狀態 （ 主控台 ） 可協助您了解在 RFC 上人工介入或動作的狀態。主要用於手動 RFCs，`RfcActionState`可協助您了解 或 AMS 操作何時需要採取動作，並協助您了解 AMS 操作何時正在積極處理 RFC。這可提高 RFC 在其生命週期內所採取動作的透明度。

`RfcActionState` (API)/活動狀態 （ 主控台 ） 定義：

- AwsOperatorAssigned：AWS 運算子正在積極處理您的 RFC。
- AwsActionPending：預期來自 AWS 的回應或動作。
- CustomerActionPending：預期來自客戶的回應或動作。
- NoActionPending：AWS 或客戶不需要採取任何動作。
- NotApplicable：AWS 運算子或客戶無法設定此狀態，且僅用於在釋出此功能之前建立RFCs。

RFC 動作狀態會根據提交的變更類型是否需要手動檢閱，以及排程是否設定為 ASAP 而有所不同。

- RFC ActionState 在檢閱、核准和啟動具有延遲排程的手動變更類型期間變更：
  - 在您提交手動、排程的 RFC 之後，ActionState 會自動變更為 AwsActionPending，以指出操作員需要檢閱和核准 RFC。
  - 當運算子開始主動檢閱 RFC 時，ActionState 會變更為 AwsOperatorAssigned。
  - 當運算子核准您的 RFC 時，RFC 狀態會變更為已排程，而 ActionState 會自動變更為 NoActionPending。
  - 達到 RFC 的排程開始時間時，RFC 狀態會變更為 InProgress，而 ActionState 會自動變更為 AwsActionPending，表示需要指派運算子來檢閱 RFC。
  - 當運算子開始主動執行 RFC 時，他們會將 ActionState 變更為 AwsOperatorAssigned。
  - 完成後，運算子會關閉 RFC。這會自動將 ActionState 變更為 NoActionPending。

> **Important**
>
> - 您無法設定動作狀態。它們會根據 RFC 中的變更自動設定，或由 AMS 運算子手動設定。
> - 如果您將通訊新增至 RFC，ActionState 會自動設定為 AwsActionPending。
> - 建立 RFC 時，ActionState 會自動設定為 NoActionPending。
> - 提交 RFC 時，ActionState 會自動設定為 AwsActionPending。
> - 當 RFC 遭到拒絕、取消或完成且狀態為成功或失敗時，ActionState 會自動重設為 NoActionPending。
> - 動作狀態會同時針對自動和手動 RFCs 啟用，但對於手動 RFCs 來說主要很重要，因為這類 RFCs通常需要通訊。

檢閱 RFC 動作狀態使用案例範例

使用案例：手動 RFC 程序的可見性

- 提交手動 RFC 後，RFC 動作狀態會自動變更為 `AwsActionPending` ，表示操作員需要檢閱和核准 RFC。當運算子開始主動檢閱 RFC 時，RFC 動作狀態會變更為 `AwsOperatorAssigned`。
- 請考慮已獲核准並排定且已準備好開始執行的手動 RFC。一旦 RFC 狀態變更為 `InProgress`，RFC 動作狀態會自動變更為 `AwsActionPending`。當運算子開始主動執行 RFC `AwsOperatorAssigned` 時，它會再次變更為 。

- 手動 RFC 完成時（關閉為「成功」或「失敗」），RFC 動作狀態會變更為 NoActionPending，表示客戶或運算子不需要進一步的動作。

使用案例：RFC 通訊

- 當手動 RFC 為 時Pending Approval，AMS Operator 可能需要您提供進一步的資訊。運算子會將通訊發佈至 RFC，並將 RFC 動作狀態變更為 CustomerActionPending。當您透過新增 RFC 通訊來回應時，RFC 動作狀態會自動變更為 AwsActionPending。
- 當自動或手動 RFC 失敗時，您可以將通訊新增至 RFC 詳細資訊，向 AMS Operator 詢問 RFC 失敗的原因。新增通訊時，RFC 動作狀態會自動設定為 AwsActionPending。當 AMS 運算子挑選 RFC 以檢視您的通訊時，RFC 動作狀態會變更為 AwsOperatorAssigned。當運算子透過新增 RFC 通訊來回應時，RFC 動作狀態可能會設定為 CustomerActionPending，表示客戶預期有另一個回應，或 NoActionPending，表示不需要或預期客戶的任何回應。

了解 RFC 狀態碼

RFC 狀態碼可協助您追蹤請求。您可以在 CLI 輸出中的 RFC 執行期間觀察這些狀態碼，或在主控台中重新整理 RFC 清單頁面。

您也可以在該 RFC 的詳細資訊頁面上看到 RFC 的代碼，其可能如下所示：

您可能會在清單中看到您未提交的 RFC。當 AMS 運算子使用僅限內部的 CT 時，他們會在 RFC 中提交它，並顯示在 RFC 清單中。如需詳細資訊，請參閱僅限內部的變更類型。

> **Important**
>
> 您可以請求 RFC 狀態變更的通知。如需詳細資訊，請參閱 RFC 狀態變更通知。

RFC 狀態碼

成功	失敗
編輯：RFC 已建立但未提交 PendingApproval / Submitted：已提交 RFC，系統正在判斷是否需要核准，並視需要取得該核准	拒絕：RFCs通常會因為驗證失敗而遭到拒絕；例如，指定了無法使用的資源，即子網路 已取消：RFCs通常會因為在設定的開始時間之前未通過驗證而取消

成功	失敗
AWS 核准/客戶核准：RFC 已核准。自動化 RFCs 由 AWS 核准，手動 RFCs 由 Operators 核准，有時由客戶核准 已排程：RFC 已通過語法和需求檢查，並排定執行 InProgress：RFC 正在執行中，請注意，佈建多個資源或具有長時間執行 UserData RFCs 需要更長的時間才能執行 已執行：已執行 RFC 成功/成功：RFC 已成功完成	失敗：RFC 失敗；如需失敗原因，請參閱輸出中的 StatusReason，AMS 操作會自動建立故障票證並視需要與您通訊

> **Note**
>
> 已取消或拒絕RFCs 可以使用 UpdateRfc 重新提交；另請參閱 更新 RFCs。

如果 RFC 通過所有必要條件（例如，指定所有必要參數），狀態會變更為 `PendingApproval`（即使自動化 CTs 也需要核准，如果語法和參數檢查通過，也會自動發生）。如果未通過，狀態會變更為 `Rejected`。`StatusReason` 提供有關拒絕的資訊； `ExecutionOutput` 欄位提供有關核准和完成的資訊。錯誤代碼包括：

- InvalidRfcStateException：RFC 處於不允許呼叫操作的狀態。例如，如果 RFC 已移至提交狀態，則無法再修改。
- InvalidRfcScheduleException：已違反 StartTime、EndTime 或 TimeoutInMinutes 參數。
- InternalServerError：系統發生問題。
- InvalidArgumentException：未正確指定參數；例如，使用無法接受的值。
- ResourceNotFoundException：找不到堆疊 ID 等值。

如果排定的請求開始和結束時間（也稱為變更執行時段）在核准變更之前發生，RFC 狀態會變更為 `Canceled`。如果變更獲得核准，RFC 狀態會變更為 `Scheduled`。ASAP RFCs 的變更執行時段是提交的時間加上 CT `ExpectedExecutionDuration`的值。

在變更執行時段到達之前的任何時間，都可以修改或取消排定的變更 （ 在 CLI RequestedStartTime中使用 提交 ）。如果已修改排程變更，則必須重新提交。

當變更開始時間到達 （ 排程或 ASAP) 且核准完成後，狀態會變更為 InProgress且無法進行任何修改。如果在指定的變更執行時段內完成變更，狀態會變更為 Success。如果變更的任何部分失敗，或在變更執行時段結束時變更仍在進行中，狀態會變更為 Failure。

> **Note**
>
> 在 InProgress、 Success或 Failure變更狀態期間，無法修改或取消 RFC。

下圖說明從 CreateRFC 呼叫到解析的 RFC 狀態。

了解 RFC 更新 CTs和 CloudFormation 範本偏離偵測

在 AMS 中佈建的資源使用修改過的 CloudFormation 範本。如果資源直接透過服務的 AWS 管理主控台變更參數，則該資源的 CloudFormation 建立記錄會變得不同步。如果發生這種情況，且您嘗試使用 AMS 更新變更類型來更新 AMS 中的資源，則 AMS 會參考原始資源組態，並可能重設變更的參數。此重設可能會損壞，因此如果偵測到任何額外的 AMS 組態變更，AMS 會不允許具有更新變更類型的 RFCs。

如需更新變更類型的清單，請使用 主控台篩選條件。

漂移修復FAQs

AMS 漂移修復的問題和答案。您可以使用兩種變更類型來啟動偏離修復，一種是執行模式=手動或「需要檢閱」，另一種是執行模式=自動。

漂移修復支援的資源 (ct-3kinq0u4l33zf)

這些是漂移修復變更類型 (ct-3kinq0u4l33zf) 支援的資源。 若要修復任何資源，請改用「需要檢閱」(ct-34sxfo53yuzah) 變更類型。

```
AWS::EC2::Instance
AWS::EC2::SecurityGroup
AWS::EC2::VPC
AWS::EC2::Subnet
AWS::EC2::NetworkInterface
```

```
AWS::EC2::EIP
AWS::EC2::InternetGateway
AWS::EC2::NatGateway
AWS::EC2::NetworkAcl
AWS::EC2::RouteTable
AWS::EC2::Volume
AWS::AutoScaling::AutoScalingGroup
AWS::AutoScaling::LaunchConfiguration
AWS::AutoScaling::LifecycleHook
AWS::AutoScaling::ScalingPolicy
AWS::AutoScaling::ScheduledAction
AWS::ElasticLoadBalancing::LoadBalancer
AWS::ElasticLoadBalancingV2::Listener
AWS::ElasticLoadBalancingV2::ListenerRule
AWS::ElasticLoadBalancingV2::LoadBalancer
AWS::CloudWatch::Alarm
```

偏離修復變更類型

有關使用 AMS 偏離修復變更類型的問答。

如需偏離修補功能的支援資源清單，請參閱 漂移修復支援的資源 (ct-3kinq0u4l33zf)。

> **Important**
>
> 漂移修復會修改堆疊範本和/或參數，而且必須更新本機範本儲存庫或更新這些堆疊的任何自動化，才能使用最新的堆疊範本和參數。使用舊範本和/或參數而不同步可能會導致基礎資源的變更受損。
> 不需要的檢閱、自動化、CT (ct-3kinq0u4l33zf) 支援每個 RFC 僅修復 10 個資源。若要以 10 個批次修復剩餘的資源，請建立新的 RFCs，直到所有資源都修復為止。

我應該使用哪種偏離修復變更類型？

我們建議您在下列情況下使用不需要檢閱的自動化 CT (ct-3kinq0u4l33zf)：

- 您嘗試使用自動化 CT 執行現有堆疊資源的更新，而 RFC 會被拒絕，因為堆疊是 DRIFTED。
- 您過去曾使用更新 CT，但因為堆疊已 DRIFTED 而失敗。您不需要再次嘗試更新，可以改用檢閱所需的手動 CT。

我們建議僅在漂移修復不支援漂移資源類型時，才使用所需的檢閱手動 CT (ct-34sxfo53yuzah)，無需檢閱、自動化、CT (ct-3kinq0u4l33zf)，或漂移修復不需要檢閱、自動化、CT 失敗。

修補期間對堆疊執行哪些變更？

修復需要更新堆疊範本和/或參數，具體取決於漂移的屬性。修補也會在修補期間更新堆疊的堆疊政策，並在修補完成後將堆疊政策還原至先前的值。

如何查看對堆疊範本和/或參數執行的變更？

在 RFC 的回應中，會提供變更摘要，其中包含下列資訊：

- `ChangeSummaryJson`：包含堆疊範本和/或參數的變更摘要，做為偏離修復的一部分。修補會以多個階段執行。此變更摘要包含個別階段的變更。如果修復成功，請檢查最後一個階段的變更。如需依順序執行的階段，請參閱 JSON 中的 ExecutionPlan。例如，存在時的 RestoreReferences 區段一律在結尾執行，並包含修正後變更的 JSON。如果修復是在 DryRun 模式下執行，則這些變更都不會套用至堆疊。
- `PreRemediationStackTemplateAndConfigurationJson`：在堆疊上觸發修復之前，包含 CloudFormation Stack 的組態快照，包括範本、參數、輸出、StackPolicyBody。

執行修復之後，我需要做什麼？

> **Important**
>
> 您需要使用 RFC 摘要中提供的最新範本和參數，更新本機範本儲存庫或任何會更新修復堆疊的自動化。請務必這麼做，因為使用舊範本和/或參數可能會對堆疊資源造成進一步的破壞性變更。

在此修復期間，我的應用程式是否會生效？

修復是一種離線程序，僅在 CloudFormation 堆疊組態上執行。不會對基礎資源執行更新。

在修復之後，我可以繼續使用管理 | 其他 | 其他 RFCs 對資源執行更新嗎？

我們建議您一律使用可用的自動更新 CTs執行堆疊資源的更新。當可用的更新 CTs不支援您的使用案例時，請使用管理 | 其他 | 其他請求。

修補是否在堆疊中建立新的資源？

修復不會在堆疊中建立新的資源。不過，修補會建立新的輸出並更新堆疊範本中繼資料區段，以存放修補摘要供您參考。

修復是否一律成功？

修復需要仔細分析和驗證範本組態，以判斷是否可以執行。在這些驗證失敗的情況下，修復程序會停止，且堆疊範本或參數不會進行任何變更。此外，只能對支援的資源類型執行修復。

如果修復不成功，如何執行堆疊資源的更新？

您可以使用 管理 | 其他 | 其他 | 更新 CT (ct-0xdawir96cy7k) 來請求變更。AMS 會監控這類案例，並致力於改善修補解決方案。

我可以修復同時具有支援和不支援資源類型的堆疊嗎？

是。不過，只有在堆疊中找到支援的資源類型 DRIFTED 時，才會執行修復。如果任何不支援的資源類型為 DRIFTED，則不會繼續修復。

對於透過非 CFN 擷取 CTs 建立的堆疊，我可以請求修復嗎？

是。無論用於建立堆疊的變更類型為何，都可以在堆疊上執行修補。

我是否可以知道在修復之前將對堆疊執行的變更？

是。這兩種變更類型都提供 DryRun 選項，您可以用來請求在堆疊修復時執行的變更。不過，最終修復變更可能會因修復時堆疊上存在的偏離而有所不同。

排程 RFCs

排程功能可讓您選擇 RFCs的開始時間。下列選項可在 排程功能中使用：

- 盡快執行此變更：一旦核准，AMS 就會執行 RFC。大多數 CTs都會自動核准。如果不希望 RFC 在特定時間啟動，請使用此選項。
- 排程此變更：設定要執行 RFC 的日期、時間和時區。對於自動變更類型，最佳實務是在您計劃提交 RFC 至少 10 分鐘後請求開始時間。若要檢閱必要的變更類型，您必須在計劃提交 RFC 至少 24 小時後請求開始時間。如果設定的開始時間未核准 RFC，則會拒絕 RFC。

設定 RFC 排程

若要排程 RFC，請使用下列其中一種方法：

盡快執行此變更：

- 主控台：不執行任何動作。這會使用預設 RFC 排程。
- API 或 CLI：移除建立 RFC 操作中的 `RequestedStartTime`和 `RequestedEndTime`選項。

如果 RFCs提交後的三十天內未獲得核准，即會自動拒絕。

排程此變更：

- 主控台：選取排程此變更選項按鈕。開始時間區域隨即開啟。手動輸入一天，或使用行事曆小工具來挑選一天。以 UTC 輸入以 ISO 8601 格式表示的時間，並使用下拉式清單來挑選位置。根據預設，AMS 使用 ISO 8601 格式 YYYYMMDDThhmmssZ 或 YYYY-MM-DDThh：mm：ssZ，接受任一格式。

  > **Note**
  >
  > 預設結束時間是從您輸入的開始時間起算 4 小時。若要將排程變更的結束時間設定為超過 4 小時，請使用 API 或 CLI 來執行變更。

- API 或 CLI：在建立 RFC 操作中提交 `RequestedStartTime`和 `RequestedEndTime` 參數的值。傳遞已設定的 `RequestedEndTime` 不會停止已啟動的自動變更類型的執行。對於「需要檢閱」變更類型，如果`RequestedEndTime`在 AMS Operations 研究仍在進行中時達到 ，而且您正在與 AMS 通訊，則可以請求 延伸，或者您可能需要重新提交 RFC。

  > **Tip**
  >
  > 如需 UTC 時間讀取的範例，請參閱 Time-is 網站上的 UTC。日期/時間值為 2016-12-05 的 ISO 8601 格式範例，時間為下午 2：20：2016-12-05T14：20：00Z 或 20161205T142000Z。

如果您提供...

- 只有 `RequestedStartTime`，RFC 會被視為已排程，並使用 `RequestedEndTime` `ExecutionDurationInMinutes`值填入 。
- 只有 `RequestedEndTime`，我們擲回 InvalidArgumentException。
- `RequestedStartTime` 和 ，`RequestedEndTime`我們`RequestedEndTime`都會以指定的開始時間加上 `ExecutionDurationInMinutes`值來覆寫 。
- 無論是 `RequestedStartTime`還是 `RequestedEndTime`，我們都會將這些值保留為 null，並將 RFC 視為 ASAP RFC。

> **Note**
>
> 對於所有排程RFCs，未指定的結束時間會寫入為指定的時間`RequestedStartTime`加上所提交變更類型的`ExpectedExecutionDurationInMinutes`屬性。例如，如果 `ExpectedExecutionDurationInMinutes`是 "60"（分鐘），且指定

的 RequestedStartTime是 2016-12-05T14:20:00Z(2016 年 12 月 5 日上午 4：20)，則實際結束時間將設定為 2016 年 12 月 5 日上午 5：20。若要尋找ExpectedExecutionDurationInMinutes特定變更類型的 ，請執行此命令：

```
aws amscm --profile saml get-change-type-version --
change-type-id CHANGE_TYPE_ID --query "ChangeTypeVersion.
{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

使用 RFC Priority 選項

在execution mode = manual變更類型中使用 Priority 選項，提醒 AMS Operations 請求的緊急程度。

中的優先順序選項execution mode = manual：

將手動 RFC 的優先順序指定為高、中或低。分類為高RFCs 會在分類為中RFCs 之前經過審核和核准，但需受 RFC 服務水準目標 SLOs) 及其提交時間的約束。具有低優先順序或未指定優先順序RFCs 會依提交順序進行處理。

核准或拒絕 RFCs

使用核准必要 （ 手動 ） CTs RFCs 必須經過您或 AMS 的核准。會自動處理預先核准的 CTs。如需詳細資訊，請參閱CT 核准要求。

> **Note**
>
> 使用「需要檢閱」CTs時，AMS 建議您使用 ASAP 排程選項 （ 在主控台中選擇 ASAP，在 API/CLI 中保留開始和結束時間空白 ），因為這些 CTs 需要 AMS 運算子來檢查 RFC，並在核准和執行之前與您通訊。如果您排程這些 RFCs，請務必至少允許 24 小時。如果未在排定的開始時間之前進行核准，則會自動拒絕 RFC。

如果 AMS 成功提交核准所需的 RFC，則必須獲得您的明確核准。或者，如果您提交核准所需的 RFC，則必須由 AMS 核准。如果您需要核准 AMS 提交的 RFC，則會傳送電子郵件或其他預先決定的通訊給您請求核准。通訊包含 RFC ID。傳送通訊後，請執行下列其中一項操作：

- 主控台核准或拒絕：使用相關 RFC 的 RFC 詳細資訊頁面：

- API/CLI 核准：ApproveRfc 會將變更標記為已核准。如果需要兩者，擁有者和運算子都必須採取 動作。以下是 CLI 核准命令的範例。在下列範例中，將 RFC_ID 取代為適當的 RFC ID。

```
aws amscm approve-rfc --rfc-id RFC_ID
```

- API/CLI 拒絕：RejectRfc 會將變更標記為已拒絕。以下是 CLI 拒絕命令的範例。在下列範例中，將 RFC_ID 取代為適當的 RFC ID。

```
aws amscm reject-rfc --rfc-id RFC_ID --reason "no longer relevant"
```

請求 RFC 限制執行期間

先前稱為中斷日，您可以請求限制特定時段。在此期間無法執行任何變更。

若要設定限制的執行期間，請使用 UpdateRestrictedExecutionTimes API 操作，並以 UTC 設定特定期間。您指定的期間會覆寫先前指定的任何期間。如果您在指定的限制執行時間提交 RFC，提交會失敗，並顯示無效的 RFC 排程錯誤。您最多可以指定 200 個限制時段。根據預設，不會設定限制期間。以下是範例 請求命令 （ 已設定 SAML 身分驗證 ）：

```
aws amscm  --profile saml update-restricted-execution-times --restricted-execution-
times="[{\"TimeRange\":{\"StartTime\":\"2018-01-01T12:00:00Z\",\"EndTime\":
\"2018-01-01T12:00:01Z\"}}]"
```

您也可以執行 RestrictedExecutionTimes API 操作來檢視目前的 RestrictedExecutionTimes 設定。ListRestrictedExecutionTimes 範例：

```
aws amscm  --profile saml list-restricted-execution-times
```

如果您想要在指定的限制執行時間提交 RFC，請使用 OverrideRestrictedTimeRanges 值新增 RestrictedExecutionTimesOverrideId，然後像平常一樣提交 RFC。最佳實務是僅將此方法用於關鍵或緊急 RFC。如需詳細資訊，請參閱 SubmitRfc 的 API 參考。

建立、複製、更新、尋找和取消 RFCs

下列範例會逐步解說各種 RFC 操作。

主題

- 建立 RFC

- 使用 AMS 主控台複製 RFCs（重新建立）
- 更新 RFCs
- 尋找 RFCs
- 取消 RFCs

建立 RFC

使用主控台建立 RFC

以下是 AMS 主控台中 RFC 建立程序的第一頁，其中開啟快速卡並啟用瀏覽變更類型：

以下是 AMS 主控台中 RFC 建立程序的第一頁，並啟用依類別選取：

運作方式：

1. 導覽至建立 RFC 頁面：在 AMS 主控台的左側導覽窗格中，按一下 RFCs以開啟 RFCs清單頁面，然後按一下建立 RFC。
2. 在預設瀏覽變更類型檢視中選擇熱門的變更類型 (CT)，或在依類別選擇檢視中選擇 CT。
   - 依變更類型瀏覽：您可以在快速建立區域中按一下熱門的 CT，以立即開啟執行 RFC 頁面。請注意，您無法透過快速建立選擇較舊的 CT 版本。

     若要排序 CTs，請使用卡片或資料表檢視中的所有變更類型區域。在任一檢視中，選取 CT，然後按一下建立 RFC 以開啟執行 RFC 頁面。如果適用，建立較舊版本選項會顯示在建立 RFC 按鈕旁。
   - 依類別選擇：選取類別、子類別、項目和操作，如果適用，CT 詳細資訊方塊會開啟，其中包含使用較舊版本建立的選項。按一下建立 RFC 以開啟執行 RFC 頁面。
3. 在執行 RFC 頁面上，開啟 CT 名稱區域以查看 CT 詳細資訊方塊。需要主旨（如果您在瀏覽變更類型檢視中選擇 CT，則會為您填入）。開啟其他組態區域以新增 RFC 的相關資訊。

   在執行組態區域中，使用可用的下拉式清單或輸入必要參數的值。若要設定選用的執行參數，請開啟其他組態區域。
4. 完成後，請按一下執行。如果沒有錯誤，RFC 成功建立的頁面會顯示已提交的 RFC 詳細資訊，以及初始的執行輸出。
5. 開啟執行參數區域以查看您提交的組態。重新整理頁面以更新 RFC 執行狀態。或者，取消 RFC 或使用頁面頂端的選項建立 RFC 的副本。

使用 CLI 建立 RFC

運作方式：

1. 使用內嵌建立（您發出包含所有 RFC 和執行參數的`create-rfc`命令）或範本建立（您建立兩個 JSON 檔案，一個用於 RFC 參數，另一個用於執行參數），並使用兩個檔案作為輸入發出`create-rfc`命令。此處說明這兩種方法。
2. 使用傳回的 RFC ID 提交 RFC： `aws amscm submit-rfc --rfc-id` *ID*命令。

   監控 RFC： `aws amscm get-rfc --rfc-id` *ID*命令。

若要檢查變更類型版本，請使用下列命令：

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> 您可以將任何`CreateRfc`參數與任何 RFC 搭配使用，無論它們是否為變更類型結構描述的一部分。例如，若要在 RFC 狀態變更時取得通知，請將此行新增至請求的 `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` RFC 參數部分（而非執行參數）。如需所有 CreateRfc 參數的清單，請參閱 AMS 變更管理 API 參考。

內嵌建立：

使用內嵌提供的執行參數發出建立 RFC 命令（在內嵌提供執行參數時逸出引號），然後提交傳回的 RFC ID。例如，您可以將內容取代為如下內容：

```
aws amscm create-rfc --change-type-id "CT_ID" --change-type-version "VERSION" --title
 "TITLE" --execution-parameters "{\"Description\": \"example\"}"
```

範本建立：

> **Note**
>
> 此建立 RFC 的範例使用Load Balancer (ELB) 堆疊變更類型。

1. 尋找相關的 CT。下列命令會搜尋項目名稱中包含 "ELB" 的 CT 分類摘要，並以資料表形式建立類別、項目、操作和 ChangeTypeID 的輸出（兩者的子類別都是 Advanced stack components)。

```
aws amscm list-change-type-classification-summaries --query
 "ChangeTypeClassificationSummaries[?contains(Item,'ELB')].
[Category,Item,Operation,ChangeTypeId]" --output table
```

```
-------------------------------------------------------------------
|                            CtSummaries                          |
+-----------+---------------------------+--------------------------+
| Deployment| Load balancer (ELB) stack | Create | ct-123h45t6uz7jl |
| Management| Load balancer (ELB) stack | Update | ct-0ltm873rsebx9 |
+-----------+---------------------------+--------------------------+
```

2. 尋找最新版本的 CT：

   ChangeTypeId 和 ChangeTypeVersion：此演練的變更類型 ID 為 ct-123h45t6uz7jl（建立 ELB)，若要了解最新版本，請執行此命令：

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=ct-123h45t6uz7jl
```

3. 了解選項和需求。下列命令會將結構描述輸出至名為 CreateElbParams.json.

```
aws amscm get-change-type-version --change-type-id "ct-123h45t6uz7jl" --query
 "ChangeTypeVersion.ExecutionInputSchema" --output text > CreateElbParams.json
```

4. 修改並儲存執行參數 JSON 檔案。此範例會命名檔案 CreateElbParams.json.

   對於佈建 CT，StackTemplateId 包含在結構描述中，且必須在執行參數中提交。

   對於 TimeoutInMinutes，允許在 RFC 失敗之前建立堆疊的分鐘數，此設定不會延遲 RFC 執行，但您必須提供足夠的時間（例如，不要指定 "5")。對於具有長時間執行 UserData CTs：建立 EC2 和建立 ASG，有效值為「60」至「360」。對於所有其他佈建 CTs，我們建議使用允許的上限 "60"。

   提供您要建立堆疊的 VPC ID；您可以使用 CLI 命令 取得 VPC IDaws amsskms list-vpc-summaries。

```
{
```

```
"Description":      "ELB-Create-RFC",
"VpcId":            "VPC_ID",
"StackTemplateId":  "stm-sdhopv00000000000",
"Name":             "MyElbInstance",
"TimeoutInMinutes": 60,
"Parameters":   {
    "ELBSubnetIds":                     ["SUBNET_ID"],
    "ELBHealthCheckHealthyThreshold":   4,
    "ELBHealthCheckInterval":           5,
    "ELBHealthCheckTarget":             "HTTP:80/",
    "ELBHealthCheckTimeout":            60,
    "ELBHealthCheckUnhealthyThreshold": 5,
    "ELBScheme":                        false
    }
}
```

5. 將 RFC JSON 範本輸出到目前資料夾中名為 CreateElbRfc.json:

```
aws amscm create-rfc --generate-cli-skeleton > CreateElbRfc.json
```

6. 修改並儲存 CreateElbRfc.json 檔案。由於您在不同的檔案中建立執行參數，請移除該`ExecutionParameters`行。例如，您可以將內容取代為類似以下內容：

```
{
"ChangeTypeVersion":    "2.0",
"ChangeTypeId":         "ct-123h45t6uz7jl",
"Title":                "Create ELB"
}
```

7. 建立 RFC。下列命令會指定執行參數檔案和 RFC 範本檔案：

```
aws amscm create-rfc --cli-input-json file://CreateElbRfc.json --execution-
parameters file://CreateElbParams.json
```

您會在回應中收到新 RFC 的 ID，並且可以使用它來提交和監控 RFC。在您提交之前，RFC 會保持在編輯狀態，不會啟動。

提示

> **Note**
>
> 您可以使用 AMS API/CLI 來建立 RFC，而無需建立 RFC JSON 檔案或 CT 執行參數 JSON 檔案。若要這樣做，您可以使用 `create-rfc`命令並將所需的 RFC 和執行參數新增至命令，這稱為「內嵌建立」。請注意，所有佈建 CTs都包含在`execution-parameters`具有資源參數的`Parameters`陣列區塊中。參數必須有引號以反斜線 (\) 逸出。
> 另一個建立 RFC 的記錄方法稱為「範本建立」。您可以在此處為 RFC 參數建立 JSON 檔案，並為執行參數建立另一個 JSON 檔案，並使用 `create-rfc`命令提交這兩個檔案。這些檔案可以做為範本，並再次用於未來的 RFCs。
> 使用 範本建立 RFCs 時，您可以使用 命令，透過發出命令來建立具有所需內容的 JSON 檔案，如下所示。這些命令會使用顯示的內容建立名為 "parameters.json" 的檔案；您也可以使用這些命令來建立 RFC JSON 檔案。

使用 AMS 主控台複製 RFCs （重新建立）

您可以使用 AMS 主控台來複製現有的 RFC。

若要使用 AMS 主控台複製或重新建立 RFC，請遵循下列步驟：

1. 尋找相關的 RFC。在左側導覽中，按一下 RFCs。

   RFCs儀表板隨即開啟。
2. 捲動頁面，直到您找到要複製的 RFC。使用篩選條件選項縮小清單範圍。選擇您要複製的 RFC。

   RFC 詳細資訊頁面隨即開啟。
3. 按一下建立複本。

   建立變更請求頁面隨即開啟，並將所有選項設定為原始 RFC 中的 。
4. 進行您想要的變更。若要設定其他選項，請將基本選項變更為進階。設定所有選項之後，請選擇提交。

   作用中 RFC 詳細資訊頁面會開啟，其中包含複製 RFC 的新 RFC ID，而複製的 RFC 會出現在 RFC 儀表板中。

更新 RFCs

您可以更新 RFC 然後提交或重新提交，以重新提交已被拒絕或尚未提交的 RFC。請注意，大多數 RFCs會遭到拒絕，因為在提交之前RequestedStartTime已通過指定的 ，或指定的 TimeoutInMinutes 不足以執行 RFC （ 由於 TimeoutInMinutes 不會延長成功的 RFC，我們建議針對 Amazon EC2 或具有長時間執行 UserData 的 Amazon EC2 Auto Scaling 群組，一律將此設定為至少 "60" 且最多 "360")。本節說明如何使用 UpdateRfc命令的 CLI 版本，使用新的 RFC 參數更新 RFC，或使用字串化 JSON 或更新的參數檔案更新新參數。

此範例說明使用 AMS UpdateRfc API 的 CLI 版本 （ 請參閱更新 RFC)。雖然更新某些資源 (DNS 私有和公有、負載平衡器堆疊和堆疊修補組態） 有變更類型，但沒有 CT 可更新 RFC。

我們建議您一次提交一個 UpdateRfc 操作。如果您提交多個更新，例如在 DNS 堆疊上，更新可能無法同時嘗試更新 DNS。

必要資料：RfcId：您正在更新的 RFC。

選擇性資料：ExecutionParameters：除非您更新非必要欄位，例如 Description，否則您可以提交修改後的執行參數，以解決導致 RFC 被拒絕或取消的問題。所有提交的非空值都會覆寫原始 RFC 中的這些值。

1. 尋找相關的已拒絕或取消 RFC，您可以使用此命令 （ 您可以使用 取代值Canceled)：

```
aws amscm list-rfc-summaries --filter Attribute=RfcStatusId,Value=Rejected
```

2. 您可以修改下列任何 RFC 參數：

```
{
    "Description": "string",
    "ExecutionParameters": "string",
    "ExpectedOutcome": "string",
    "ImplementationPlan": "string",
    "RequestedEndTime": "string",
    "RequestedStartTime": "string",
    "RfcId": "string",
    "RollbackPlan": "string",
    "Title": "string",
    "WorstCaseScenario": "string"}
```

更新描述欄位的範例命令：

```
aws amscm update-rfc --description "AMSTestNoOpsActionRequired" --rfc-id "RFC_ID"
 --region us-east-1
```

更新 ExecutionParameters VpcId 欄位的範例命令：

```
aws amscm update-rfc  --execution-parameters "{\"VpcId\":\"VPC_ID\"}" --rfc-id
 "RFC_ID" --region us-east-1
```

使用包含更新的執行參數檔案更新 RFC 的範例命令；請參閱 EC2 堆疊 | 建立之步驟 2 中的範例執行參數檔案：

```
aws amscm update-rfc --execution-parameters file://CreateEc2ParamsUpdate.json --
rfc-id "RFC_ID" --region us-east-1
```

3. 使用 `submit-rfc`和您在第一次建立 RFC 時擁有的相同 RFC ID 重新提交 RFC：

```
aws amscm submit-rfc --rfc-id RFC_ID
```

如果 RFC 成功，您在命令列不會收到確認或錯誤訊息。

4. 若要監控請求的狀態和檢視執行輸出，請執行下列命令。

```
aws amscm get-rfc --rfc-id RFC_ID
```

尋找 RFCs

使用主控台尋找變更請求 (RFC)

若要使用 AMS 主控台尋找 RFC，請遵循下列步驟。

> **Note**
>
> 此程序僅適用於排程RFCs，也就是未使用 ASAP 選項的 RFCs。

1. 在左側導覽中，按一下 RFCs。

   RFCs儀表板隨即開啟。

2. 捲動清單或使用篩選選項來精簡清單。

   RFC 清單會依篩選條件而變更。

3. 選擇您想要之 RFC 的主旨連結。

   RFC 詳細資訊頁面會開啟該 RFC，其中包含 RFC ID 等資訊。

4. 如果儀表板中有許多 RFCs，您可以使用篩選條件選項依 RFC 搜尋：

   - 主旨：建立 RFC 時提供給 RFC 的主旨行或標題 （在 API/CLI 中）。
   - RFC ID：RFC 的識別符。
   - 活動狀態：如果您知道 RFC 狀態，您可以在 AwsOperatorAssigned 之間進行選擇，表示運算子目前正在查看 RFC，AwsActionPending 表示 AMS 運算子必須執行某些動作，然後 RFC 執行才能繼續，或者 CustomerActionPending 表示您需要採取一些動作，才能繼續執行 RFC。
   - 狀態：如果您知道 RFC 狀態，您可以選擇：
     - 已排程：已排程RFCs。
     - 已取消：已取消RFCs。
     - 進行中：RFCs進行中。
     - 成功：成功執行RFCs。
     - 已拒絕：已拒絕RFCs。
     - 編輯：正在編輯RFCs。
     - 失敗：失敗RFCs。
     - 待核准：在 AMS 或您核准之前無法繼續進行RFCs。一般而言，這表示您需要核准 RFC。您會在服務請求清單中收到此服務通知。
   - 變更類型：挑選類別、子類別、項目和操作，然後為您擷取變更類型 ID。
   - 請求的開始時間或請求的結束時間：此篩選條件選項可讓您選擇之前或之後，然後輸入日期和選擇性的時間 (hh：mm 和時區）。此篩選條件只會在排程 RFCs （非 ASAP RFCs上成功運作。
   - 狀態：已排程、已取消、進行中、成功、已拒絕、編輯或失敗。
   - 主旨：您使用給定 RFC 的 API/CLI 建立 RFC 的主旨 （或標題）。
   - 變更類型 ID：使用與 RFC 一起提交的變更類型識別符。

   搜尋可讓您新增篩選條件，如下列螢幕擷取畫面所示。

5. 按一下您想要之 RFC 的主旨連結。

RFC 詳細資訊頁面會開啟該 RFC，其中包含 RFC ID 等資訊。

使用 CLI 尋找變更請求 (RFC)

您可以使用多個篩選條件來尋找 RFC。

若要檢查變更類型版本，請使用下列命令：

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> 您可以將任何CreateRfc參數與任何 RFC 搭配使用，無論它們是否為變更類型結構描述的一部分。例如，若要在 RFC 狀態變更時取得通知，請將此行新增至請求的 --notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}" RFC 參數部分（而非執行參數）。如需所有 CreateRfc 參數的清單，請參閱 AMS 變更管理 API 參考。

如果您不記下 RFC ID，且稍後需要找到它，您可以使用 AMS 變更管理 (CM) 系統來搜尋它，並使用篩選條件或查詢縮小結果範圍。

1. CM API ListRfcSummaries 操作具有篩選條件。您可以根據邏輯 AND 操作中的 Attribute和 Value組合，或根據 Attribute、 Condition和 來篩選結果Values。

   RFC 篩選

屬性	有效值	有效條件	預設條件	備註
ActualEndTime	任何代表 ISO8601 日期時間的字串（例如，「2017 0101T000000Z」）	之前、之後、之間	無	Before 或 After 條件只接受值欄位中的一個值。介於條件在值欄位中必須剛好有兩個值，其中第一個值應代表在第二個值之前發生的日期

屬性	有效值	有效條件	預設條件	備註
ActualStartTime	任何代表 ISO8601 日期時間的字串（例如，「2017 0101T000000Z」）	之前、之後、之間	無	Before 或 After 條件只接受值欄位中的一個值。介於條件在值欄位中必須剛好有兩個值，其中第一個值應代表在第二個值之前發生的日期
AutomationStatusId	手動、自動化	等於	等於	只有兩個自動化狀態
ChangeTypeId	任何有效的變更類型 ID；例如 ct-123h45 t6uz7jl	等於	等於	尋找變更類型或 CSIO
ChangeTypeVersion	任何有效的變更類型 ID；例如 1.0	等於	等於	尋找變更類型或 CSIO
CreatedBy	任何字串（長度上限為 2048 個字元）	包含	包含	RFC 的 CreatedBy 欄位包含建立它的使用者的 ARN
CreatedTime	任何代表 ISO8601 日期時間的字串（例如，「2017 0101T000000Z」）	之前、之後、之間	無	Before 或 After 條件只接受值欄位中的一個值。介於條件在值欄位中必須剛好有兩個值，其中第一個值應代表在第二個值之前發生的日期
LastModifiedTime	任何代表 ISO8601 日期時間的字串（例如，「2017 0101T000000Z」）	之前、之後、之間	無	Before 或 After 條件只接受值欄位中的一個值。介於條件在值欄位中必須剛好有兩個值，其中第一個值應代表在第二個值之前發生的日期

屬性	有效值	有效條件	預設條件	備註
LastSubmittedTime	任何代表 ISO8601 日期時間的字串（例如，「2017 0101T000000Z」）	之前、之後、之間	無	Before 或 After 條件只接受值欄位中的一個值。介於條件在值欄位中必須剛好有兩個值，其中第一個值應代表在第二個值之前發生的日期
RequestedEndTime	任何代表 ISO8601 日期時間的字串（例如，「2017 0101T000000Z」）	之前、之後、之間	無	Before 或 After 條件只接受值欄位中的一個值。介於條件在值欄位中必須剛好有兩個值，其中第一個值應代表在第二個值之前發生的日期
RequestedStartTime	任何代表 ISO8601 日期時間的字串（例如，「2017 0101T000000Z」）	之前、之後、之間	無	Before 或 After 條件只接受值欄位中的一個值。介於條件在值欄位中必須剛好有兩個值，其中第一個值應代表在第二個值之前發生的日期
RfcStatusId	已取消、編輯、失敗、InProgress、PendingApproval、已拒絕、已排程、成功	等於	等於	在 AMS 主控台重新整理 RFC 清單或執行 GetRfc
標題	任何有效的 RFC 標題	包含	包含	不支援每個個別欄位中的規則表達式。不區分大小寫的搜尋

範例：

若要尋找與 SQS 相關的所有 RFCs IDs（其中 SQS 包含在 CT 的項目部分），您可以使用此命令：

```
list-rfc-summaries --query 'RfcSummaries[?contains(Item.Name,`SQS`)].
[Category.Id,Subcategory.Id,Type.Id,Item.Id,RfcId]' --output table
```

這會傳回如下內容：

```
-------------------------------------------------------------------------------
|                          ListRfcSummaries                                   |
+----------+---------------------------------+-------+-------+---------------+
|Deployment| Advanced Stack Components       |SQS    |Create |ct-123h45t6uz7jl|
|Management| Monitoring & Notification  |SQS    |Update |ct-123h45t6uz7jl|
+----------+---------------------------------+-------+-------+---------------+
```

另一個適用於 的篩選條件`list-rfc-summaries`是 `AutomationStatusId`，用於尋找自動化或手動RFCs：

```
aws amscm list-rfc-summaries --filter Attribute=AutomationStatusId,Value=Automated
```

另一個適用於 的篩選條件`list-rfc-summaries`是 `Title`（主控台中的主旨）：

```
 Attribute=Title,Value=RFC-TITLE
```

JSON 中傳回 RFCs的新請求結構範例，其中：

- （標題包含「Windows 2012」或「Amazon Linux」）和
- (RfcStatusId EQUALS "Success" 或 "InProgress") 和
- (20170101T000000Z <= RequestedStartTime <= 20170103T000000Z) AND (ActualEndTime <= 20170103T000000Z)

```
{
  "Filters": [
    {
      "Attribute": "Title",
      "Values": ["Windows 2012", "Amazon Linux"],
      "Condition": "Contains"
```

```
    },
    {
      "Attribute": "RfcStatusId",
      "Values": ["Success", "InProgress"],
      "Condition": "Equals"
    },
    {
      "Attribute": "RequestedStartTime",
      "Values": ["20170101T000000Z", "20170103T000000Z"],
      "Condition": "Between"
    },
    {
      "Attribute": "ActualEndTime",
      "Values": ["20170103T000000Z"],
      "Condition": "Before"
    }
  ]
}
```

> **Note**
>
> 使用更進階的 `Filters`，AMS 打算在即將發行的版本中棄用下列欄位：
>
> - 值：值欄位是篩選條件欄位的一部分。使用支援更進階功能的值欄位。
> - RequestedEndTimeRange：在支援更進階功能的篩選條件欄位中使用 RequestedEndTime
> - RequestedStartTimeRange：在支援更進階功能的篩選條件欄位中使用 RequestedStartTime。

如需使用 CLI 查詢的相關資訊，請參閱如何使用 --query Option 篩選輸出，以及查詢語言參考 JMESPath Specification。

2. 如果您使用的是 AMS 主控台：

   前往 RFCs清單頁面。如有需要，您可以篩選 RFC 主體，這是您在建立 RFC `Title`時輸入的內容。

提示

> **Note**
>
> 此程序僅適用於排定的 RFCs，也就是未使用 ASAP 選項的 RFCs。

取消 RFCs

您可以使用 主控台或 AMS API/CLI 來取消 RFC。

若要使用主控台取消 RFC，請在 RFC 清單中尋找 RFC，開啟它，然後按一下取消。

必要資料：

- `Reason`：取消 RFC 的原因。
- `RfcId`：您要取消的 RFC。

1. 一般而言，您會在提交 RFC 後立即取消 RFC （因此 RFC ID 應該很方便）；否則，除非您已排定，且早於指定的開始時間，否則您將無法取消 RFC。如果您需要尋找 RFC ID，您可以使用此命令 （您可以將 `Value` 取代`PendingApproval`為手動核准的 RFC)：

   ```
   aws amscm list-rfc-summaries --filter Attribute=RfcStatusId,Value=Scheduled
   ```

2. 取消 RFC 的範例命令：

   ```
   aws amscm cancel-rfc --reason "Bad Stack ID" --rfc-id "RFC_ID" --profile saml --
   region us-east-1
   ```

搭配 RFCs 使用 AMS 主控台

AMS 主控台提供的功能可協助您成功建立和提交 RFCs。

使用 RFC 清單頁面 （主控台）

AMS 主控台 RFCs清單頁面為您提供下列選項：

- 透過篩選條件進行進階 RFC 搜尋。如需相關資訊，請參閱尋找 RFCs。
- 尋找上次修改 RFC 的時間。此值代表上次變更 RFC 狀態的時間。

- 使用 RFC 主體檢視 RFC 詳細資訊。選擇此連結會開啟該 RFC 的詳細資訊頁面。
- 檢視 RFC 狀態。如需相關資訊，請參閱了解 RFC 狀態碼。

使用 RFC 快速建立 （主控台）

使用 RFC 快速建立卡或清單資料表，或依分類選擇 RFCs的變更類型。

如需詳細資訊，請參閱 建立 RFC。

新增 RFC 通訊和附件 （主控台）

您可以在 RFC 提交之後並在核准之前新增通訊；例如，當 RFC 處於「PendingApproval」狀態時。核准 RFC 之後 （處於「排程」或「InProgress」的狀態），便無法新增通訊，因為它可以解釋為請求的變更。RFC 完成後 （狀態為「已取消」、「已拒絕」、「成功」或「失敗」），雖然 RFC 關閉超過 30 天後，會再次啟用通訊。

> **Note**
>
> 每個通訊限制為 5，000 個字元。

附件的限制：

- 每個通訊僅三個附件。
- 每個 RFC 限制 50 個附件。
- 每個附件的大小必須小於 5 MB。
- 只接受文字檔案，例如純文字 (`.txt`)、逗號分隔值 (`.csv`)、JSON (`.json`) 或 YAML (`.yaml`。如果是 YAML 格式，則必須使用副檔名 連接檔案`.yaml`。

  > **Note**
  >
  > 禁止包含 XML 內容的文字檔案。如果您有要與 AMS 共用的 XML 內容，請使用服務請求。

- 檔案名稱限制為 255 個字元，只有數字、字母、空格、破折號 (-)、底線 (_) 和點 (.)。
- 目前不支援更新和刪除 RFC 上的附件。

若要將通訊和附件新增至 RFC，請遵循下列步驟：

1. 在 AMS 主控台的 RFC 詳細資訊頁面上，找到頁面底部的對應區段。

   在任何通訊之前：

   在一些通訊之後：

2. 若要新增通訊，請在回覆文字方塊中輸入訊息。若要連接與通訊相關的檔案，請選擇新增附件，然後選擇您想要的檔案。

3. 完成後，請選擇提交。

   新的通訊以及附加檔案的連結會出現在 RFC 詳細資訊頁面上的通訊清單中。

設定 RFC 電子郵件通知（主控台）

AMS 主控台變更請求建立頁面可讓您選擇新增電子郵件地址，以接收 RFC 狀態變更的通知：

此外，您可以將通知的電子郵件地址新增至任何變更類型，例如：

```
aws amscm create-rfc --change-type-id <Change type ID>
                     --change-type-version 1.0 --title "TITLE"
                     --notification "{\"Email\": {\"EmailRecipients\" :
 [\"email@example.com\"]}}"
```

在請求的 RFC 參數部分中，將類似的行 (`--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"`) 新增至任何變更類型內嵌或範本請求，而非參數部分。

了解常見的 RFC 參數

以下是您必須提交的 RFC 參數，以及 RFCs 中常用的參數：

- 變更類型資訊：ChangeTypeId 和 ChangeTypeVersion。Ror 變更類型 IDs和版本編號的清單，請參閱變更類型參考。

使用 query引數在 CLI list-change-type-classification-summaries中執行 ，以縮小結果範圍。例如，縮小結果以變更Item名稱中包含「存取」的類型。

```
aws amscm list-change-type-classification-summaries --query
 "ChangeTypeClassificationSummaries [?contains (Item, 'access')].
[Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
```

執行 get-change-type-version 並指定變更類型 ID。下列命令會取得 ct-2tylseo8rxfsc 的 CT 版本。

```
aws amscm get-change-type-version --change-type-id ct-2tylseo8rxfsc
```

- 標題：RFC 的名稱；這會成為 AMS 主控台 RFC 清單中 RFC 的主體，您可以使用 GetRfc命令和上的篩選條件進行搜尋 Title
- 排程：如果您想要排程 RFC，則必須包含 RequestedStartTime和 RequestedEndTime 參數，或使用排程此變更主控台選項。對於 ASAP RFC （在核准後立即執行），在使用 CLI 時，請保留 RequestedStartTime和 RequestedEndTime null。使用主控台時，請接受 ASAP 選項。

  如果遺漏 RequestedStartTime ，RFC 會遭到拒絕。
- 佈建 CTs：執行參數或 Parameters是佈建資源所需的特定設定。它們因 CT 而異。
- 非佈建 CTs：未佈建資源的 CTs，例如存取 CTs 或其他 | 其他，或刪除堆疊，具有最少的執行參數且沒有Parameters區塊。
- 有些 RFCs還需要您指定 TimeoutInMinutes，或在 RFC 失敗之前，允許多少分鐘建立堆疊。對於長時間執行的 UserData，有效值為 60 （分鐘） 到 360。如果無法在超過 TimeoutInMinutes 之前完成執行，RFC 會失敗。不過，此設定不會延遲 RFC 的執行。
- 建立執行個體的 RFCs，例如 S3 儲存貯體或 ELB，通常提供結構描述，可讓您新增最多七個標籤（索引鍵/值對）。您可以使用部署 | 進階堆疊元件 | 標籤 | 建立變更類型 (ct-3cx7we852p3af) 提交 RFC，將更多標籤新增至 S3 儲存貯體。EC2、EFS、RDS 和多層 (HA 雙層和 HA 單層） 結構描述最多允許 50 個標籤。標籤是在結構描述ExecutionParameters的一部分中指定。提供標籤可能很有價值。如需詳細資訊，請參閱標記您的 Amazon EC2 資源。

  使用 AMS 主控台時，您必須開啟其他組態區域，才能新增標籤。

  > **Tip**
  >
  > 許多 CT 結構描述都有靠近結構描述頂端的 Description和 Name 欄位。這些欄位用於命名堆疊或堆疊元件，而不會命名您正在建立的資源。有些結構描述提供參數來命名您正在建

立的資源，有些則不會。例如，建立 EC2 堆疊的 CT 結構描述不提供參數來命名 EC2 執行個體。若要這樣做，您必須建立索引鍵為 "Name" 的標籤，以及您想要名稱的值。如果您未建立此類標籤，EC2 執行個體會顯示在 EC2 主控台中，但沒有名稱屬性。

使用 RFC AWS 區域選項

AMS API 和 CLI (amscm 和 amsskms) 端點位於 中us-east-1。如果您與安全性聲明標記語言 (SAML) 聯合，則在加入時會為您提供指令碼，將您的 AWS 區域設定為 us-east-1。如果您使用 SAML，則不需要在發出命令時指定 --region選項。如果您的 SAML 設定為使用 us-east-1，但您的帳戶不在該 AWS 區域中，則您必須在發出其他 AWS 命令時指定帳戶加入區域 （ 例如 aws s3)。

> **Note**
>
> 本指南中提供的大多數命令範例不包含 --region選項。

註冊 RFC 每日電子郵件

您可以使用 RFC 摘要功能，註冊每日電子郵件，總結您帳戶在過去 24 小時內的 RFC 活動。RFC 摘要功能是一個簡化的程序，可減少您收到有關帳戶 RFCs 的電子郵件通知數量。RFC 摘要可能會降低您錯過待回應動作的可能性。

若要開啟 RFC 摘要功能，請聯絡您的 AMS Cloud Service Delivery Manager (CSDM)。CSDM 會訂閱您。您最多可以請求將 20 個電子郵件地址 （ 或別名 ） 包含在 RFC 摘要電子郵件清單中。目前的電子郵件排程固定為 09：00 UTC-8。

若要關閉 RFC 摘要功能，請聯絡您的 CSDM 並提出您的請求。

如果您未設定 RFC 摘要並希望收到有關 RFCs通知，或者如果您想要 RFCs 比 RFC 摘要提供更詳細的資訊，請使用變更管理系統來設定 CloudWatch Events 通知，或針對您想要取得資訊的每個個別 RFC 傳送電子郵件通知。如需設定 RFC 通知的資訊，請參閱 RFC 狀態變更通知。

RFC 摘要中包含的主題包括下列項目：

- 待客戶核准：列出處於PendingApproval狀態的 RFCs，等待您的核准
- 待客戶回覆：列出正在等待 RFCs 通訊回覆的 RFC
- 待 AWS 核准或回覆：列出正在等待 AMS 回覆或核准的 RFCs
- 已完成：列出成功、失敗、已取消和已拒絕狀態RFCs

以下是 RFC 摘要範例：

什麼是變更類型？

變更類型是指 AWS Managed Services (AMS) 變更請求 (RFC) 執行並包含變更動作本身的動作，以及變更類型 – 手動與自動。AMS 有大量變更類型，其他 Amazon Web 服務不會使用。您可以在提交變更請求 (RFC) 以部署、管理或存取 資源時使用這些變更類型。

主題

自動化和手動 CTs

變更類型的限制條件是它們是自動還是手動，這是變更類型`AutomationStatusId`屬性，在 AMS 主控台中稱為執行模式。

自動化變更類型具有預期的結果和執行時間，並且通常在一小時內透過 AMS 自動化系統執行 （這主要取決於 CT 正在佈建的資源）。手動變更類型並不常見，但會受到不同的處理，因為它們需要 AMS 運算子先對 RFC 採取行動，才能執行。有時這表示與 RFC 提交者通訊，因此，手動變更類型需要不同的時間長度才能完成。

對於所有排程RFCs，未指定的結束時間會寫入為指定的時間`RequestedStartTime`加上所提交變更類型的`ExpectedExecutionDurationInMinutes`屬性。例如，如果`ExpectedExecutionDurationInMinutes`是 "60"（分鐘），且指定的 `RequestedStartTime`是`2016-12-05T14:20:00Z`(2016 年 12 月 5 日上午 4：20)，則實際結束時間將設定為 2016 年 12 月

5 日上午 5：20。若要尋找ExpectedExecutionDurationInMinutes特定變更類型的 ，請執行此命令：

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --
query "ChangeTypeVersion.{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

> **Note**
>
> 執行模式 = 手動RFCs 必須在主控台中設定為在未來至少 24 小時執行。此警告不適用於 AMS API/CLI，但請務必提前至少 8 小時排程手動 RFCs。

> **Note**
>
> 使用「需要檢閱」CTs時，AMS 建議您使用 ASAP 排程選項（在主控台中選擇 ASAP，在 API/CLI 中保留開始和結束時間空白），因為這些 CTs 需要 AMS 運算子來檢查 RFC，並在核准和執行之前與您通訊。如果您排程這些 RFCs，請務必允許至少 24 小時。如果未在排定的開始時間之前進行核准，RFC 會自動遭到拒絕。

AMS 旨在四小時內回應手動 CT，並會盡快對應，但實際執行 RFC 可能需要更長的時間。

如需手動且需要 AMS 檢閱CTs 清單，請參閱 主控台開發人員資源頁面上的變更類型 CSV 檔案。

YouTube 影片：如何尋找 AMS RFCs的自動變更類型？

若要在 AMS 主控台中尋找 CT 的執行模式，您必須使用瀏覽變更類型搜尋選項。結果會顯示相符變更類型或變更類型的執行模式。

若要使用 AMS CLI 尋找AutomationStatus特定變更類型的 ，請執行此命令：

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --
query "ChangeTypeVersion.{AutomationStatus:AutomationStatus.Name}"
```

您也可以在 AMS 變更類型參考中查詢變更類型，該參考提供有關所有 AMS 變更類型的資訊。

> **Note**
>
> AMS API/CLI 目前不是 AWS API/CLI 的一部分。若要存取 AMS API/CLI，您可以透過 AMS 主控台下載 AMS 開發套件。

CT 核准要求

AMS CTs一律有兩個核准條件：AwsApprovalId 和 CustomerApprovalId，指出 RFC 是否需要 AMS 或您或任何人核准執行。

核准條件與執行模式有些相關；如需詳細資訊，請參閱 自動化和手動 CTs。

若要了解 CT 的核准條件，您可以查看 AMS 變更類型參考，或執行 GetChangeTypeVersion。兩者也會為您提供 CT `AutomationStatusId`或執行模式。

您可以使用 AMS 主控台或下列命令來核准 RFCs：

```
aws amscm approve-rfc --rfc-id RFC_ID
```

CT 核准條件

如果 CT 核准條件為	它需要來自 的核准	及
`AwsApprovalId: Required`	AMS 變更類型系統、	無需採取任何動作。此條件是自動化 CTs 的典型條件。
`AwsApprovalId: NotRequiredIfSubmitter`	如果提交的 RFC 是針對其所提交的帳戶，則 AMS 變更類型系統不會有其他人，	無需採取任何動作。此條件適用於手動 CTs因為 AMS 運算子一律會檢閱它們。
`CustomerApprovalId: NotRequired`	AMS 變更類型系統、	如果 RFC 通過語法和參數檢查，則會自動核准。

如果 CT 核准條件為	它需要來自 的核准	及
`CustomerApprovalId: Required`	AMS 變更類型系統與您，	系統會傳送通知給您，您必須透過回應通知或執行 ApproveRfc 操作來明確核准 RFC。
`CustomerApprovalId: NotRequiredIfSubmitter`	如果您提交 RFC，則 AMS 變更類型系統不會有其他人。	如果 RFC 通過語法和參數檢查，則會自動核准。
緊急安全事件或修補程式	AMS	已自動核准並實作。

變更類型版本

變更類型會進行版本控制，並在對變更類型進行主要更新時變更版本。

使用 AMS 主控台選取變更類型之後，您可以選擇開啟其他組態區域並選取變更類型版本。您也可以在 API/CLI 命令列指定變更類型版本。您可能會因為各種原因而想要這樣做，包括：

- 您知道您想要的更新變更類型版本必須符合您用來建立現在要更新之資源的建立變更類型版本。例如，您可能有一個使用 ELB 建立變更類型版本 1 建立的 Elastic Load Balancer (ELB) 執行個體。若要更新它，請選擇 ELB 更新第 1 版。
- 您想要使用的變更類型版本，其中包含與最新變更類型不同的選項。我們不建議這麼做，因為 AMS 更新變更類型主要基於安全考量，建議您一律選擇最新版本。

建立變更類型

建立變更類型會比對version-to-version與更新變更類型。也就是說，您用來佈建資源的變更類型版本必須符合稍後用來修改該資源的更新變更類型版本。例如，如果您使用建立 S3 儲存貯體變更類型 2.0 版建立 S3 儲存貯體，且稍後想要提交 RFC 來修改該 S3 儲存貯體，則您也必須使用更新 S3 儲存貯體變更類型 2.0 版，即使更新 S3 儲存貯體變更類型具有 3.0 版。

我們建議您保留在佈建具有建立變更類型的資源時所使用的變更類型 ID 和版本記錄，以防您稍後想要使用更新變更類型進行修改。

更新變更類型

AMS 提供更新變更類型，以更新使用建立變更類型建立的資源。更新變更類型必須與最初用於佈建資源version-to-version的建立變更類型相符。

建議您保留您在佈建資源時所使用的變更類型 ID 和版本記錄，以便輕鬆更新。

YouTube 影片：如何使用更新 CTs來變更 AWS Managed Services (AMS) 帳戶中的資源？

僅限內部的變更類型

您可以查看僅供內部使用的變更類型。這是為了讓您知道 AMS 可以或會採取哪些動作。如果您想要有僅供內部使用的變更類型，請提交服務請求。

例如，有一個管理 | 監控和通知 | CloudWatch 警示抑制 | 更新僅限內部的 CT。AMS 會使用它來部署基礎設施更新（例如修補），以關閉更新可能錯誤觸發的警示通知。提交此 CT 時，您會在 RFC 清單中注意到 CT 的 RFC。在 RFC 中部署的任何僅限內部 CT 都會顯示在 RFC 清單中。

變更類型結構描述

所有變更類型都會為資源的建立、修改或存取中的輸入提供 JSON 結構描述。結構描述提供參數及其描述，供您建立變更請求 (RFC)。

成功執行 RFC 會產生執行輸出。對於佈建 RFCs，執行輸出包含代表 CloudFormation 中堆疊的 "stack_id"，並且可以在 CloudFormation 主控台中搜尋。執行輸出有時包含所建立執行個體 ID 的輸出，該 ID 可用於在對應的 AWS 主控台中搜尋執行個體。例如，建立 ELB CT 執行輸出包含可在 CloudFormation 中搜尋的 "stack_id"，並輸出可在 Elastic Load Balancing 的 Amazon EC2 主控台中搜尋的 key=ELB value=<stack-xxxx>。

讓我們檢查 CT 結構描述。這是 CodeDeploy Application Create 的結構描述，這是一個相當小的結構描述。有些結構描述的區域非常大`Parameter`。

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "name": "Create CodeDeploy application",
  "description": "Use to create an AWS CodeDeploy applicati
on
  resource with the specified name.",
  "type": "object",
  "properties": {
    "Description": {
```

結構描述的第一部分提供 AMS 所請求變更類型的相關資訊。

```
      "description": "The reason for the request.",
      "type": "string",
      "minLength": 1,
      "maxLength": 500
    },
    "VpcId": {
      "description": "ID of the vpc to use, in the form
 vpc-0123abcd or vpc-01234567890abcdef.",
      "type": "string",
      "pattern": "^vpc-[a-z0-9]{8}$"
    },
    "StackTemplateId": {
      "description": "Must be stm-sft6rv00000000000",
      "type": "string",
      "enum": ["stm-sft6rv00000000000"]
    },
    "Name":{
      "description": "A name for the stack or stack component
;
      this becomes the Stack Name.",
      "type": "string",
      "minLength": 1,
      "maxLength": 255
    },
    "Tags": {
      "description": "Up to seven tags (key/value pairs) to
      categorize the resource.",
      "type": "array",
      "items": {
        "type": "object",
        "properties": {
          "Key": {
            "type": "string",
            "minLength": 1,
            "maxLength": 127
          },
          "Value": {
            "type": "string",
            "minLength": 1,
            "maxLength": 255
          }
        },
        "additionalProperties": false,
        "required": [
```

TimeoutInMinutes 參數可讓您指出執行變更類型的界限時間。對於長時間執行的 UserData，有效值為 60 到 360。

```
          "Key",
          "Value"
        ]
      },
      "minItems": 1,
      "maxItems": 7
    },
    "TimeoutInMinutes": {
      "description": "The maximum amount of time, in minutes,
to
      allow for execution of the change. This will not prolong
execution,
      but the RFC fails if the change is not completed in the
specified time.
      Valid values are 60 up to 360, for long-running
UserData.",
      "type": "number",
      "minimum": 0,
      "maximum": 60
    },
    "Parameters": {
      "description": "Specifications for the stack.",
      "type": "object",
      "properties": {
        "CodeDeployApplicationName": {
          "description": "The name of an AWS CodeDeploy
application.",
          "type": "string",
          "minLength": 1,
          "maxLength": 100,
          "pattern": "^[a-zA-Z0-9._+=,@-]{1,100}$"
        }
      },
      "additionalProperties": false,
      "required": [
        "CodeDeployApplicationName"
      ]
    }
  },
  "additionalProperties": false,
```

參數區段可讓您為要建立的資源或您要請求的動作指定設定。

「其他屬性」區段可讓您知道需要哪些參數，以及哪些參數是選用的。

```
  "required": [
    "Description",
    "VpcId",
    "StackTemplateId",
    "Name",
    "TimeoutInMinutes",
    "Parameters"
  ]
}
```

> **Note**
>
> 此結構描述最多允許七個標籤；不過，EC2、EFS、RDS 和多層建立結構描述最多允許 50 個標籤。

管理變更類型的許可

您可以使用自訂政策來限制哪些變更類型 CTs) 可供不同的群組或使用者使用。

若要進一步了解如何執行此作業，請參閱 AMS 使用者指南一節設定許可。

從變更類型編輯敏感資訊

AMS 變更類型結構描述提供參數屬性，`"metadata":"ams:sensitive":"true"`用於包含敏感資訊的參數，例如密碼。設定此屬性時，提供的輸入會隱藏。請注意，您無法設定此參數屬性；不過，如果您使用 AMS 來建立變更類型，並具有您想要在輸入時隱藏的參數，您可以請求此參數。

使用查詢選項尋找變更類型

此範例示範如何使用 AMS 主控台來尋找您要提交之 RFC 的適當變更類型。

您可以使用 主控台或 API/CLI 來尋找變更類型 ID (CT) 或版本。有兩種方法：搜尋或選擇分類。對於這兩種選擇類型，您可以選擇最常使用、最近使用或按字母順序排序搜尋。

YouTube 影片：如何使用 AWS Managed Services CLI 建立 RFC，以及在哪裡可以找到 CT 結構描述？

在 AMS 主控台的 RFCs -> 建立 RFC 頁面上：

- 選取依變更類型瀏覽（預設）時：
  - 使用快速建立區域從 AMS 最熱門CTs 中選取。按一下標籤，隨即開啟執行 RFC 頁面，並自動為您填入主旨選項。視需要完成其餘選項，然後按一下執行以提交 RFC。
  - 或者，向下捲動至所有變更類型區域，並開始在選項方塊中輸入 CT 名稱，您不需要具有確切或完整的變更類型名稱。您也可以輸入相關字詞，依變更類型 ID、分類或執行模式（自動或手動）搜尋 CT。

    選取預設卡檢視後，相符的 CT 卡會在您輸入時顯示，選取卡片並按一下建立 RFC。選取資料表檢視後，選擇相關的 CT，然後按一下建立 RFC。這兩種方法都會開啟執行 RFC 頁面。
- 或者，若要探索變更類型選擇，請按一下頁面頂端的依類別選擇，以開啟一系列的下拉式清單選項方塊。
- 選擇類別、子類別、項目和操作。該變更類型的資訊方塊會顯示頁面底部的面板。
- 當您準備好時，請按 Enter，並顯示相符的變更類型清單。
- 從清單中選擇變更類型。該變更類型的資訊方塊會出現在頁面底部。
- 在您擁有正確的變更類型之後，請選擇建立 RFC。

> **Note**
>
> 必須安裝 AMS CLI，這些命令才能運作。若要安裝 AMS API 或 CLI，請前往 AMS 主控台開發人員資源頁面。如需 AMS CM API 或 AMS SKMS API 的參考資料，請參閱《使用者指南》中的 AMS 資訊資源一節。您可能需要新增身分驗證`--profile`選項，例如 `aws amsskms` *`ams-cli-command`* `--profile SAML`。您可能還需要新增 `--region`選項，因為所有 AMS 命令都用盡 us-east-1；例如 `aws amscm` *`ams-cli-command`* `--region=us-east-1`。

> **Note**
>
> AMS API/CLI (amscm 和 amsskms) 端點位於 AWS N. Virginia 區域 `us-east-1`。根據身分驗證的設定方式，以及您的帳戶和資源所在的 AWS 區域，您可能需要在發出命令`--region us-east-1`時新增 。如果這是您的身分驗證方法`--profile saml`，您可能還需要新增 。

若要使用 AMS CM API（請參閱 ListChangeTypeClassificationSummaries) 或 CLI 搜尋變更類型：

您可以使用篩選條件或查詢來搜尋。ListChangeTypeClassificationSummaries 操作具有 `Category`、`Item`、 `Subcategory`和 的篩選條件選項`Operation`，但值必須完全符合現有的值。若要在使用 CLI 時獲得更靈活的結果，您可以使用 `--query`選項。

使用 AMS CM API/CLI 變更類型篩選

屬性	有效值	有效/預設條件	備註
ChangeTypeId	代表 ChangeTypeId 的任何字串 （ 例如：ct-abc123xyz7890)	等於	如需變更類型 IDs，請參閱變更類型參考。 如需變更類型 IDs，請參閱尋找變更類型或 CSIO。
類別	任何自由格式文字	包含	不支援每個個別欄位中的規則表達式。不區分大小寫的搜尋
Subcategory			
項目			
作業			

1. 以下是列出變更類型分類的一些範例：

   下列命令會列出所有變更類型類別。

   ```
   aws amscm list-change-type-categories
   ```

   下列命令會列出屬於指定類別的子類別。

   ```
   aws amscm list-change-type-subcategories --category CATEGORY
   ```

   下列命令會列出屬於指定類別和子類別的項目。

   ```
   aws amscm list-change-type-items --category CATEGORY --subcategory SUBCATEGORY
   ```

2. 以下是使用 CLI 查詢搜尋變更類型的一些範例：

下列命令會搜尋項目名稱中包含 "S3" 的 CT 分類摘要，並以資料表形式建立類別、子類別、項目、操作和變更類型 ID 的輸出。

```
aws amscm list-change-type-classification-summaries --query
 "ChangeTypeClassificationSummaries [?contains(Item, 'S3')].
[Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
```

```
+-------------------------------------------------------------+
|               ListChangeTypeClassificationSummaries         |
+----------+-------------------------+--+------+--------------+
|Deployment|Advanced Stack Components|S3|Create|ct-1a68ck03fn98r|
+----------+-------------------------+--+------+--------------+
```

3. 然後，您可以使用變更類型 ID 來取得 CT 結構描述並檢查參數。下列命令會將結構描述輸出至名為 CreateS3Params.schema.json.

```
aws amscm get-change-type-version --change-type-id "ct-1a68ck03fn98r"
 --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
 CreateS3Params.schema.json
```

如需有關使用 CLI 查詢的資訊，請參閱如何使用 --query Option 篩選輸出和查詢語言參考 JMESPath Specification。

4. 在您擁有變更類型 ID 之後，建議您驗證變更類型的版本，以確保它是最新版本。使用此命令來尋找指定變更類型的版本：

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CHANGE_TYPE_ID
```

若要尋找AutomationStatus特定變更類型的 ，請執行此命令：

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --
query "ChangeTypeVersion.{AutomationStatus:AutomationStatus.Name}"
```

若要尋找ExpectedExecutionDurationInMinutes特定變更類型的 ，請執行此命令：

```
aws amscm --profile saml get-change-type-version --change-type-id ct-14027q0sjyt1h
 --query "ChangeTypeVersion.{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

針對 AMS 中的 RFC 錯誤進行故障診斷

許多 AMS 佈建 RFC 失敗可以透過 CloudFormation 文件進行調查。請參閱對 AWS CloudFormation 進行故障診斷：對錯誤進行故障診斷

以下各節提供其他疑難排解建議。

AMS 中的「管理」RFC 錯誤

AMS「管理」類別變更類型 CTs) 可讓您請求存取資源，以及管理現有的資源。本節說明一些常見問題。

RFC 存取錯誤

- 請確定您在 RFC 中指定的使用者名稱和 FQDN 正確且存在於網域中。如需尋找 FQDN 的說明，請參閱尋找 FQDN。
- 請確定您為存取指定的堆疊 ID 是 EC2-related堆疊。ELB 和 Amazon Simple Storage Service (S3) 等堆疊不是存取 RFCs的候選項目，而是使用您的唯讀存取角色來存取這些堆疊資源。如需尋找堆疊 ID 的說明，請參閱尋找堆疊 IDs
- 請確定您提供的堆疊 ID 正確且屬於相關帳戶。

如需其他存取 RFC 失敗的說明，請參閱存取管理。

YouTube 影片：如何正確提出變更請求 (RFC)，以避免拒絕和失敗？

RFC （手動） CT 排程錯誤

大多數變更類型是 ExecutionMode=Automated，但有些是 ExecutionMode=Manual，這會影響您應該如何排程它們以避免 RFC 失敗。

如果您使用 AMS 主控台建立 RFCs則使用 ExecutionMode=Manual 的排程 RFC 必須設定為未來至少 24 小時執行。此警告不適用於 AMS API/CLI，但請務必提前至少 8 小時排程手動 RFCs。

AMS 旨在四小時內回應手動 CT，並會盡快對應，但實際執行 RFC 可能需要更長的時間。

搭配手動更新 CTs使用 RFCs

當您要更新的堆疊類型有更新變更類型時，AMS Operations 會拒絕管理 | 其他 | 其他 RFCs 更新堆疊。

RFC 刪除堆疊錯誤

RFC 刪除堆疊失敗：如果您使用管理 | 標準堆疊 | 堆疊 | 刪除 CT，您會在 CloudFormation 主控台中看到具有 AMS 堆疊名稱之堆疊的詳細事件。您可以對照 AMS 主控台中的堆疊名稱來檢查堆疊。CloudFormation 主控台提供有關失敗原因的更多詳細資訊。

在刪除堆疊之前，您應該考慮堆疊的建立方式。如果您使用 AMS CT 建立堆疊，但未新增或編輯堆疊資源，則可以預期刪除堆疊，而不會發生問題。不過，建議您先從堆疊移除任何手動新增的資源，再提交刪除堆疊 RFC。例如，如果您使用完整堆疊 CT (HA Two Tier) 建立堆疊，它會包含安全群組 - SG1。如果您接著使用 AMS 建立另一個安全群組 - SG2SG2，並在建立為完整堆疊一部分的 SG1 中參考新的 SG2，然後使用刪除堆疊 CT 刪除堆疊，則 SG1 不會刪除，因為它由 SG2 參考。

> **Important**
>
> 刪除堆疊可能會產生不想要和非預期的後果。基於此原因，AMS 偏好 *not* 代表客戶刪除堆疊或堆疊資源。請注意，AMS 只會代表您刪除無法使用適當的自動變更類型刪除的資源（透過提交的管理 | 其他 | 其他 | 更新變更類型）。其他考量
>
> - 如果資源已啟用「刪除保護」，則如果您提交管理 | 其他 | 其他 | 更新變更類型，且刪除保護移除後，您可以使用自動 CT 來刪除該資源，則 AMS 可協助解除封鎖。
> - 如果堆疊中有多個資源，而且您只想要刪除一部分的堆疊資源，請使用 CloudFormation 更新變更類型（請參閱 CloudFormation 擷取堆疊：更新)。您也可以提交管理 | 其他 | 其他 | 更新變更類型，如有需要，AMS 工程師可協助您製作變更集。
> - 如果您提交管理 | 其他 | 其他 | 更新以解決偏離（在 AWS CloudFormation CloudFormation Service 支援的範圍內），並提供 ChangeSet，然後您可以使用自動化 CT、管理/自訂堆疊/堆疊從 CloudFormation 範本/核准變更集和更新來驗證和執行，則 AMS 可以提供協助。
>
> AMS 會維護上述限制，以協助確保沒有非預期或非預期的資源刪除。

如需詳細資訊，請參閱對 AWS CloudFormation 進行故障診斷：刪除堆疊失敗。

RFC 更新 DNS 錯誤

更新 DNS 託管區域的多個 RFCs 可能會失敗，有些可能沒有原因。同時建立多個 RFCs以更新 DNS 託管區域（私有或公有）可能會導致某些 RFCs因為它們同時嘗試更新相同的堆疊。AMS 變更管理會拒絕或失敗無法更新堆疊的 RFCs，因為堆疊已由另一個 RFC 更新。AMS 建議您一次建立一個 RFC，並等待 RFC 成功，然後再為相同的堆疊提出新的 RFC。

RFC IAM 實體錯誤

AMS 會將多個預設 IAM 角色和設定檔佈建至專為滿足您的需求而設計的 AMS 帳戶。不過，您可能需要偶爾請求額外的 IAM 資源。

提交請求自訂 IAM 資源RFCs 程序遵循手動 RFCs的標準工作流程，但核准程序也包含安全審查，以確保採取適當的安全控制。因此，程序通常需要比其他手動 RFCs更長的時間。若要縮短這些 RFCs的週期時間，請遵循下列準則。

如需 IAM 審核的意義及其如何映射至技術標準和風險接受程序的資訊，請參閱 了解 RFC 安全性審查。

常見的 IAM 資源請求：

- 如果您要求與主要雲端相容應用程式相關的政策，例如 CloudEndure，請參閱 AMS 預先核准的 IAM CloudEndure 政策：解壓縮 WIGs 雲端持久性登陸區域範例檔案並開啟 `customer_cloud_endure_policy.json`

  > **Note**
  >
  > 如果您想要更寬鬆的政策，請與您的 CloudArchitect/CSDM 討論您的需求，並視需要在提交實作政策的 RFC 之前取得 AMS 安全審查和簽署。

- 如果您想要修改 AMS 預設在帳戶中部署的資源，建議您要求修改後的資源複本，而不是變更現有的資源複本。
- 如果您要請求人類使用者的許可（而不是將許可連接到使用者），請將許可連接到角色，然後授予使用者擔任該角色的許可。如需執行此操作的詳細資訊，請參閱暫時 AMS Advanced 主控台存取。
- 如果您需要臨時遷移或工作流程的特殊許可，請在請求中提供這些許可的結束日期。
- 如果您已與安全團隊討論請求的主旨，請盡可能向 CSDM 提供其核准的證據，並提供詳細資訊。

如果 AMS 拒絕 IAM RFC，我們會提供拒絕的明確原因。例如，我們可能會拒絕 IAM 政策建立請求，並解釋政策的不適當之處。在這種情況下，您可以進行已識別的變更並重新提交請求。如果需要進一步釐清請求的狀態，請提交服務請求，或聯絡您的 CSDM。

下列清單說明 AMS 檢閱 IAM RFCs 時嘗試緩解的典型風險。如果您的 IAM RFC 有任何這些風險，可能會導致 RFC 遭到拒絕。如果您需要例外狀況，AMS 會向您的安全團隊請求核准。若要尋求此類例外狀況，請與 CSDM 協調。

> **Note**
>
> AMS 可能會基於任何原因拒絕對帳戶內部 IAM 資源的任何變更。如需有關 RFC 拒絕的疑慮，請透過服務請求聯絡 AMS Operations，或聯絡您的 CSDM。

- 權限提升，例如允許您修改自己的許可，或修改帳戶中其他資源許可的許可。範例：
  - 使用 `iam:PassRole`搭配另一個更特殊權限的角色。
  - 從角色或使用者連接/提取 IAM 政策的許可。
  - 帳戶中 IAM 政策的修改。
  - 在管理基礎設施環境中進行 API 呼叫的能力。
- 修改為您提供 AMS 服務所需的資源或應用程式的許可。範例：
  - 修改 AMS 基礎設施，例如堡壘、管理主機或 EPS 基礎設施。
  - 刪除日誌管理 AWS Lambda 函數或日誌串流。
  - 預設 CloudTrail 監控應用程式的刪除或修改。
  - Directory Services Active Directory (AD) 的修改。
  - 停用 CloudWatch (CW) 警示。
  - 修改 帳戶中部署做為登陸區域一部分的主體、政策和命名空間。
- 在最佳實務之外部署基礎設施，例如允許在危及資訊安全的狀態下建立基礎設施的許可。範例：
  - 建立公有或未加密的 S3 儲存貯體或公開共用 EBS 磁碟區。
  - 公有 IP 地址的佈建。
  - 修改安全群組以允許廣泛存取。
- 過於廣泛的許可，可能造成應用程式影響，例如可能導致基礎設施和帳戶中應用程式的資料遺失、完整性遺失、不當組態或服務中斷的許可。範例：
  - 透過 `ModifyNetworkInterfaceAttribute`或 等 APIs 停用或重新導向網路流量`UpdateRouteTable`。
  - 透過從受管主機分離磁碟區來停用受管基礎設施。
- 不屬於 AMS 服務描述且 AMS 不支援的服務許可。

  AMS 服務描述中未列出的服務無法在 AMS 帳戶中使用。若要請求支援某項功能或服務，請聯絡您的 CSDM。

- 不符合您所述目標的許可，因為這些許可太慷慨或過於保守，或是套用至錯誤的資源。範例

- 請求對具有強制 KMS 加密的 S3 儲存貯體`s3:PutObject`的許可，而沒有相關金鑰的`KMS:Encrypt`許可。
- 與帳戶中不存在的資源相關的許可。
- IAM RFCs，其中 RFC 的描述似乎不符合請求。

「部署」RFC 錯誤

AMS「部署」類別變更類型 CTs) 可讓您請求將各種 AMS 支援的資源新增至您的帳戶。

大多數建立資源的 AMS CTs 都是以 CloudFormation 範本為基礎。身為客戶，您可以唯讀存取所有 AWS 服務 CloudFormation，包括，您可以使用 CloudFormation 主控台，根據堆疊描述快速識別 CloudFormation 代表您堆疊的堆疊。失敗的堆疊可能處於 DELETE_COMPLETE 狀態。識別 CloudFormation 堆疊後，事件會顯示無法建立的特定資源，以及原因。

使用 CloudFormation 文件進行疑難排解

大多數 AMS 佈建 RFCs使用 CloudFormation 範本，該文件有助於進行故障診斷。請參閱該 CloudFormation 範本的文件：

- 建立應用程式負載平衡器失敗：AWS::ElasticLoadBalancingV2::LoadBalancer (Application Load Balancer)
- 建立 Auto Scaling 群組：AWS::AutoScaling::AutoScalingGroup (Auto Scaling 群組）
- 建立 memcached 快取：AWS::ElastiCache::CacheCluster （快取叢集）
- 建立 Redis 快取：AWS::ElastiCache::CacheCluster （快取叢集）
- 建立 DNS 託管區域 （與建立 DNS 私有/公有搭配使用）：AWS::Route53::HostedZone (R53 託管區域）
- 建立 DNS 紀錄集 （與建立 DNS 私有/公有搭配使用）：AWS::Route53::RecordSet （資源紀錄集）
- 建立 EC2 堆疊：AWS::EC2::Instance （彈性運算雲端）
- 建立彈性檔案系統 (EFS)：AWS::EFS::FileSystem （彈性檔案系統）
- Create Load Balancer：AWS::ElasticLoadBalancing::LoadBalancer (Elastic Load Balancer)
- 建立 RDS 資料庫：AWS::RDS::DBInstance （關聯式資料庫）
- 建立 Amazon S3：AWS::S3::Bucket （簡易儲存服務）
- 建立佇列：AWS::SQS::Queue （簡易佇列服務）

RFC 建立 AMIs錯誤

Amazon Machine Image (AMI) 是一種範本，其中包含軟體組態 (例如作業系統、應用程式伺服器和應用程式)。您可從 AMI 啟動執行個體，執行個體是 AMI 的複本，在雲端中以虛擬伺服器的形式執行。AMIs 非常有用，而且需要建立 EC2 執行個體或 Auto Scaling 群組；不過，您必須遵守一些需求：

- 您為 指定的執行個體`Ec2InstanceId`必須處於停止狀態，RFC 才能成功。請勿將 Auto Scaling 群組 (ASG) 執行個體用於此參數，因為 ASG 會終止已停止的執行個體。
- 若要建立 AMS Amazon Machine Image (AMI)，您必須從 AMS 執行個體開始。在您可以使用執行個體來建立 AMI 之前，您必須先確保其已停止並從其網域中退出，以做好準備。如需詳細資訊，請參閱使用 Sysprep 建立標準 Amazon Machine Image
- 您為新 AMI 指定的名稱在帳戶中必須是唯一的，否則 RFC 失敗。如何執行此作業，請參閱 AMI | Create，如需詳細資訊，請參閱 和 AWS AMI Design。

> **Note**
>
> 如需準備建立 AMI 的詳細資訊，請參閱 AMI | Create。

建立 EC2s或 ASGs錯誤的 RFCs

對於具有逾時的 EC2 或 ASG 失敗，AMS 建議您確認使用的 AMI 是否已自訂。如果是，請參閱本指南中包含的 AMI 建立步驟 （ 請參閱 AMI | Create)，以確保正確建立 AMI。建立自訂 AMI 時的常見錯誤未遵循指南中的步驟來重新命名或叫用 Sysprep。

建立 RDS RFCs

Amazon Relational Database Service (RDS) 失敗可能有許多不同的原因，因為您可以在建立 RDS 時使用許多不同的引擎，而且每個引擎都有自己的需求和限制。嘗試建立 AMS RDS 堆疊之前，請仔細檢閱 AWS RDS 參數值，請參閱 CreateDBInstance。

若要進一步了解 Amazon RDS，包括大小建議，請參閱 Amazon Relational Database Service 文件。

建立 Amazon S3s 錯誤的 RFCs

建立 S3 儲存貯體時，一個常見的錯誤不是使用儲存貯體的唯一名稱。如果您提交的名稱與先前提交的名稱相同的 S3 儲存貯體建立 CT，將會失敗，因為 S3 儲存貯體已存在於該 BucketName。這將在 CloudFormation 主控台中詳細說明，您將在其中看到堆疊事件顯示儲存貯體名稱已在使用中。

RFC 驗證與執行錯誤

RFC 失敗和相關訊息在所選 RFC 的 AMS 主控台 RFC 詳細資訊頁面上的輸出訊息中不同：

- 驗證失敗原因僅適用於狀態欄位
- 執行失敗原因可在執行輸出和狀態欄位中取得。

RFC 錯誤訊息

當您遇到下列所列變更類型 (CTs的錯誤時，您可以使用這些解決方案來協助您尋找問題來源並加以修正。

```
{"errorMessage":"An error has occurred during RFC execution. We are
investigating the issue.","errorType":"InternalError"}
```

如果您在參考下列疑難排解選項後需要進一步協助，請透過 RFC 通訊聯絡 AMS 或建立服務請求。如需詳細資訊，請參閱 RFC 通訊和連接（主控台）和在 AMS 中建立服務請求。

工作負載擷取 (WIGS) 錯誤

> **Note**
>
> 您可以下載適用於 Windows 和 Linux 的驗證工具，並直接在內部部署伺服器以及 AWS 中的 EC2 執行個體上執行。這些可透過 AMS 進階應用程式開發人員指南的遷移工作負載：Linux 擷取前驗證和遷移工作負載：Windows 擷取前驗證找到。

- 確定 EC2 執行個體存在於目標 AMS 帳戶中。例如，如果您已將 AMI 從非 AMS 帳戶共用到 AMS 帳戶，您必須先使用共用 AMI 在 AMS 帳戶中建立 EC2 執行個體，才能提交工作負載擷取 RFC。
- 檢查連接至執行個體的安全群組是否允許輸出流量。SSM 代理程式需要能夠連線到其公有端點。
- 檢查執行個體是否具有與 SSM 代理程式連線的正確許可。這些許可隨附於 `customer-mc-ec2-instance-profile`，您可以在 EC2 主控台中檢查此項目：

EC2 執行個體堆疊停止錯誤

- 檢查執行個體是否已處於已停止或終止狀態。

- 如果 EC2 執行個體在線上且您看到`InternalError`錯誤，請提交服務請求讓 AMS 進行調查。
- 請注意，您無法使用變更類型管理 | 進階堆疊元件 | EC2 執行個體堆疊 | 停止 ct-3mvvt2zkyveqj 來停止 Auto Scaling 群組 (ASG) 執行個體。如果您需要停止 ASG 執行個體，請提交服務請求。

EC2 執行個體堆疊建立錯誤

`InternalError` 訊息來自 CloudFormation；CREATION_FAILED 狀態原因。您可以依照下列步驟，在 CloudWatch 堆疊事件中找到堆疊失敗的詳細資訊：

- 在 AWS 管理主控台中，您可以在建立、更新或刪除堆疊時檢視堆疊事件的清單。從這個清單中找到故障的事件，然後檢視該事件的狀態原因。

  狀態原因可能包含來自 AWS CloudFormation 或特定服務的錯誤訊息，可協助您了解問題。
- 如需檢視堆疊事件的詳細資訊，請參閱 AWS 管理主控台上的檢視 AWS CloudFormation 堆疊資料和資源。

EC2 執行個體磁碟區還原錯誤

當 EC2 執行個體磁碟區還原失敗時，AMS 會建立內部故障診斷 RFC。這是因為 EC2 執行個體磁碟區還原是災難復原 (DR) 的重要部分，而 AMS 會自動為您建立此內部故障診斷 RFC。

建立內部故障診斷 RFC 時，會顯示橫幅，為您提供 RFC 的連結。此內部故障診斷 RFC 可讓您更清楚了解 RFC 失敗，而不是提交導致相同錯誤的重試 RFCs，或讓您針對此失敗手動聯絡 AMS，您可以追蹤變更並知道 AMS 正在處理失敗。這也減少了其變更time-to-recovery (TTR) 指標，因為 AMS Operators 會主動處理 RFC 失敗，而不是等待您的請求。

如何取得 RFC 的協助

您可以聯絡 AMS 來識別失敗的根本原因。AMS 營業時間為 24 小時，全年無休。

AMS 提供多種管道，供您尋求協助或提出服務請求。

- 若要要求資訊或建議，或存取 AMS 受管 IT 服務，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，請參閱建立服務請求。如需 AMS 服務請求的一般資訊，請參閱服務請求管理。
- 若要報告影響受管環境的 AWS 或 AMS 服務效能問題，請使用 AMS 主控台並提交事件報告。如需詳細資訊，請參閱報告事件。如需 AMS 事件管理的一般資訊，請參閱事件回應。
- 有關您或您的資源或應用程式如何使用 AMS 的特定問題，或要呈報事件，請傳送電子郵件至下列一或多個：

1. 首先，如果您不滿意服務請求或事件報告回應，請傳送電子郵件給 CSDM：ams-csdm@amazon.com
2. 接下來，如果需要呈報，您可以傳送電子郵件給 AMS Operations Manager（但您的 CSDM 可能會這樣做）：ams-opsmanager@amazon.com
3. 進一步呈報將向 AMS Director 呈報：ams-director@amazon.com
4. 最後，您可以隨時聯絡 AMS VP：ams-vp@amazon.com

AMS 中的直接變更模式

主題

AWS Managed Services (AMS) 直接變更模式 (DCM) 透過提供 AMS Advanced Plus 和 Premium 帳戶的原生 AWS 存取權來佈建和更新 AWS 資源，以擴展 AMS 進階變更管理。使用 DCM 時，您可以選擇使用原生 AWS API（主控台或 CLI/SDK) 或 AMS 進階變更管理變更請求 (RFCs)，而且在任何一種情況下，AMS 都完全支援資源和變更，包括監控、修補程式、備份、事件回應管理。透過 DCM 佈建的資源會在 AMS 服務知識管理系統 (SKMS) 中註冊、加入 AMS 受管 Active Directory 網域（如適用），並執行 AMS 管理代理程式。使用現有的工具（例如 CloudFormation、 AWS SDK 和 CDK) 來開發和部署 AMS 受管 CloudFormation 堆疊。

> **Note**
>
> 直接變更模式不會移除 AMS 變更管理 RFCs。您可以使用 DCM 完整存取 AMS RFCs。

觀看 Akash 的影片以進一步了解 (6：30)

直接變更模式入門

首先檢查先決條件，然後在符合資格的 AMS Advanced 帳戶中提交變更請求 (RFC)。

1. 確認您想要與 DCM 搭配使用的帳戶符合要求：

   - 帳戶是 AMS Advanced Plus 或 Premium。
   - 帳戶未啟用 Service Catalog。我們目前不支援同時將帳戶加入 DCM 和服務目錄。如果您已加入 Service Catalog，但對 DCM 感興趣，請與您的雲端服務交付管理員 (CSDM) 討論您的需求。如果您決定從 Service Catalog 切換到 DCM、離機 Service Catalog，若要這樣做，請在下面的變更請求中加入 ask。如需 AMS 中 Service Catalog 的詳細資訊，請參閱 AMS 和服務目錄。

2. 使用 管理 | 受管帳戶 | 直接變更模式 | 啟用變更類型 (ct-3rd4781c2nnhp) 提交變更請求 (RFC)。如需逐步解說範例，請參閱直接變更模式 | 啟用。

   處理 CT 之後，預先定義的 IAM 角色`AWSManagedServicesCloudFormationAdminRole`和 `AWSManagedServicesUpdateRole` 會在指定的帳戶中佈建。

3. 使用內部聯合程序，將適當的角色指派給需要 DCM 存取的使用者。

> **Note**
>
> 您可以指定任意數量的 SAMLIdentityProviders、 AWS Services 和 IAM 實體 （ 角色、使用者等） 來擔任角色。您必須提供至少一個：`SAMLIdentityProviderARNs`、`IAMEntityARNs`或 `AWSServicePrincipals`。如需詳細資訊，請洽詢您公司的 IAM 部門或 AMS 雲端架構師 (CA)。

直接變更模式 IAM 角色和政策

在 帳戶中啟用直接變更模式時，會部署這些新的 IAM 實體：

`AWSManagedServicesCloudFormationAdminRole`：此角色會授予 CloudFormation 主控台的存取權、建立和更新 CloudFormation 堆疊、檢視偏離報告，以及建立和執行 CloudFormation ChangeSets。此角色的存取權是透過 SAML 供應商管理。

部署並連接到角色`AWSManagedServicesCloudFormationAdminRole`的受管政策如下：

- AMS 進階多帳戶登陸區域 (MALZ) 應用程式帳戶
  - AWSManagedServices_CloudFormationAdminPolicy1
  - AWSManagedServices_CloudFormationAdminPolicy2

    - 此政策代表授予 的許可AWSManagedServicesCloudFormationAdminRole。您和合作夥伴使用此政策來授予帳戶中現有角色的存取權，並允許該角色啟動和更新帳戶中的 CloudFormation 堆疊。這可能需要額外的 AMS 服務控制政策 (SCP) 更新，以允許其他 IAM 實體啟動 CloudFormation 堆疊。
- AMS 進階單一帳戶登陸區域 (SALZ) 帳戶
    - AWSManagedServices_CloudFormationAdminPolicy1
    - AWSManagedServices_CloudFormationAdminPolicy2
    - cdk-legacy-mode-s3-access 【內嵌政策】
    - AWS ReadOnlyAccess 政策

AWSManagedServicesUpdateRole：此角色會授予下游 AWS 服務 APIs的限制存取權。該角色部署的受管政策提供變動和非變動 API 操作，但一般限制變動操作 （ 例如Create/Delete/PUT)，針對某些服務，例如 IAM、KMS、GuardDuty、VPC、AMS 基礎設施資源和組態等。此角色的存取是透過 SAML 供應商管理。

部署並連接到角色AWSManagedServicesUpdateRole的受管政策如下：

- AMS 進階多帳戶登陸區域 應用程式帳戶
    - AWSManagedServicesUpdateBasePolicy
    - AWSManagedServicesUpdateDenyPolicy
    - AWSManagedServicesUpdateDenyProvisioningPolicy
    - AWSManagedServicesUpdateEC2AndRDSPolicy
    - AWSManagedServicesUpdateDenyActionsOnAMSInfraPolicy
- AMS 進階單一帳戶登陸區域帳戶
    - AWSManagedServicesUpdateBasePolicy
    - AWSManagedServicesUpdateDenyProvisioningPolicy
    - AWSManagedServicesUpdateEC2AndRDSPolicy
    - AWSManagedServicesUpdateDenyActionsOnAMSInfraPolicy1
    - AWSManagedServicesUpdateDenyActionsOnAMSInfraPolicy2

除此之外，受管政策AWSManagedServicesUpdateRole角色還ViewOnlyAccess連接了 AWS 受管政策。

安全與合規

安全與合規是 AMS Advanced 與身為客戶的您共同的責任。AMS Advanced Direct Change 模式不會變更此共同責任。

直接變更模式中的安全性

AMS Advanced 提供具有規範登陸區域、變更管理系統和存取管理的額外值。使用直接變更模式時，此責任模型不會變更。不過，您應該知道其他風險。

直接變更模式「更新」角色（請參閱直接變更模式 IAM 角色和政策) 提供提升的許可，允許可存取該角色的實體變更您帳戶中 AMS 支援服務的基礎設施資源。隨著許可提高，根據資源、服務和動作，存在各種風險，尤其是在由於監督、錯誤或沒有遵守內部程序和控制架構而導致不正確的變更的情況下。

根據 AMS 技術標準，已識別下列風險並提出建議，如下所示。有關 AMS 技術標準的詳細資訊可透過 取得 AWS Artifact。若要存取 AWS Artifact，請聯絡您的 CSDM 以取得指示，或前往 入門 AWS Artifact。

AMS-STD-001：標記

標準	是否會中斷	風險	建議
所有 AMS 擁有的資源都必須具有下列鍵值對 除了上述標籤之外，所有 AMS 擁有的標籤都必須具有字首，例如 AMS*或MC*upper/lower/mix大小寫。	是。CloudFormation、CloudTrail、EFS、OpenSearch、CloudWatch Logs、SQS、SSM、標記 api 的中斷 - 因為這些服務不支援限制 AMS 命名空間標記aws:TagsKey 的條件。 下表 AMS-STD-003 中提供的標準說明您可以變更 AppId、Environment 和 AppName，但不能變更 AMS 擁有的資	AMS 資源的不正確標記可能會對 AMS 端的資源的報告、提醒和修補操作產生不利影響。	必須重新分配存取權，才能對 AMS 團隊以外的任何人對 AMS 預設標記要求進行任何變更。

標準	是否會中斷	風險	建議
	源。無法透過 IAM 許可達成。		
不得根據您的變更請求刪除 AMS 擁有的堆疊上的任何標籤。	是。CloudFormation 不支援限制 AMS 命名空間標籤`aws:TagsKey` 的條件。		
不允許您在基礎設施中使用 AMS 標籤命名慣例，如下表 AMS-STD-002 所述。	是。中斷 CloudFormation、CloudTrail、Amazon Elastic File System (EFS)、OpenSearch、CloudWatch Logs、Amazon Simple Queue Service (SQS)、Amazon EC2 Systems Manager (SSM)、標記 API；這些服務不支援限制 AMS 命名空間標記`aws:TagsKey` 的條件。		

AMS-STD-002：身分與存取管理 (IAM)

標準	是否會中斷	風險	建議
4.7 不允許繞過變更管理程序 (RFC) 的動作，例如啟動或停止執行個體、建立 S3 儲存貯體或 RDS 執行個體等。只要在指派角色的邊界內執行動	是。自助服務動作的目的可讓您執行繞過 AMS RFC 系統的動作。	安全存取模型是 AMS 的核心技術面向，而主控台或程式設計存取的 IAM 使用者會規避此存取控制。AMS 變更管理不會監控 IAM 使用者存	IAM 使用者應該有時間限制，並根據最低權限和need-to-know授予許可。

標準	是否會中斷	風險	建議
作，開發人員模式帳戶和自助式佈建模式服務 (SSPS) 就會豁免。		取。存取只會記錄在 CloudTrail 中。	

AMS-STD-003：網路安全

標準	是否會中斷	風險	建議
S2. EC2 執行個體上的彈性 IP 只能與正式的風險接受協議或內部團隊的有效使用案例搭配使用。	是。自助服務動作可讓您關聯和取消關聯彈性 IP 地址 (EIP)。	將彈性 IP 新增至執行個體會公開至網際網路。這會增加資訊公開和未經授權的活動的風險。	透過安全群組封鎖對該執行個體的任何不必要的流量，並確認您的安全群組已與執行個體連接，以確保只允許基於業務原因而需要的流量。
S14. 您可以允許屬於相同客戶的帳戶之間的 VPC 對等互連和端點連線。	是。無法透過 IAM 政策進行。	離開帳戶界限後，不會監控離開您 AMS 帳戶的流量。	我們建議僅與您擁有的 AMS 帳戶進行對等互連。如果您的使用案例需要，請使用安全群組和路由表來限制哪些流量範圍、資源和類型可以透過相關連線輸出。
AMS 基礎 AMIs 可以在 AMS 受管和未受管帳戶之間共用，只要我們可以驗證它們是否屬於同一個 AWS 組織即可。		AMIs可能包含敏感資料，而且可能會公開給非預期的帳戶。	僅與組織擁有的帳戶共用 AMIs，或在組織外部共用之前驗證使用案例和帳戶資訊。

AMS-STD-007：記錄

標準	是否會中斷	風險	建議
19. 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。			
20. 只有在非 AMS 帳戶由相同 AMS 客戶擁有（透過確認他們位於相同 AWS Organizations 帳戶，或將電子郵件網域與客戶的公司名稱和 PAYER 連結帳戶相符）時，才能使用內部工具，從 AMS 轉送任何日誌到非 AMS 帳戶。	是。無法透過 IAM 政策實現客戶日誌的潛在不安全，因為無法驗證同一組織中的客戶帳戶。	日誌可能包含敏感資料，而且可能會公開給非預期的帳戶。	僅與 AWS 組織管理的帳戶共用日誌，或在組織外部共用之前驗證使用案例和帳戶資訊。我們可以透過多種方式進行驗證，請洽詢您的雲端服務交付管理員 (CSDM)。

與您的內部授權和身分驗證團隊合作，相應地控制直接變更模式角色的許可。

直接變更模式中的合規

直接變更模式與生產和非生產工作負載相容。您有責任確保遵守任何合規標準（例如 PHI、HIPAA、PCI），並確保使用直接變更模式符合您的內部控制架構和標準。

直接變更模式中的變更管理

變更管理是 AMS Advanced 用來實作變更請求的程序。變更請求 (RFC) 是您或 AMS Advanced 透過 AMS Advanced 界面建立的請求，用於變更受管環境，並包含特定操作的 AMS Advanced 變更類型 (CT) ID。如需詳細資訊，請參閱變更管理。

> **Note**
>
> 直接變更模式不會移除 AMS 變更管理 RFCs，您仍然可以使用 DCM 完整存取 AMS RFCs。

AMS 直接變更模式 (DCM) 透過提供 AMS Advanced Plus 和 Premium 帳戶的原生 AWS 存取權來佈建和更新 AWS 資源，以擴展 AMS 進階變更管理。已透過 IAM 角色授予直接變更模式許可的使用者，可以使用原生 AWS API 存取來佈建和變更其 AMS Advanced 帳戶中的資源。使用者仍然可以使用相同的 IAM 角色來使用 AMS 進階變更管理 RFCs。在這兩種情況下，AMS 都完全支援資源和變更，包括監控、修補、備份、事件回應管理。在這些帳戶中沒有適當角色的使用者，必須使用 AMS 進階變更管理 RFC 程序進行變更。

變更管理使用案例

基於安全考量，AMS Advanced 中的某些變更只能透過變更管理請求 (RFC) 程序來完成。`AWSManagedServicesCloudFormationAdminRole` 僅限於透過 CloudFormation (CFN) 採取的動作。如需如何透過 DCM 建立堆疊的詳細資訊，請參閱使用直接變更模式建立堆疊。`AWSManagedServicesUpdateRole` 受限於下列動作。

如需每個變更類型的範例逐步解說，包括管理 | 受管帳戶 | 直接變更模式 | 啟用 (ct-3rd4781c2nnhp) 變更類型，請參閱 AMS 進階變更類型參考依分類變更類型一節中的相關變更類型的「其他資訊」一節。

服務	動作
AWS Key Management Service (AWS KMS)	更新
AWS Certificate Manager	建立
AWS Identity and Access Management (IAM)	任何
Site-to-Site VPN	任何
AMS 資源排程器	
AWS Backup	建立備份計畫
AMS 工作負載擷取 (WIGs)	任何
AMS 輸出篩選 （ 受管 Palo Alto)	
AMS Advanced MALZ 帳戶變更	
Amazon GuardDuty	
AMS 進階堆疊存取	任何

服務	動作
Amazon Elastic Block Store (EBS) 磁碟區	刪除
Amazon Elastic Block Store (EBS) 預設加密	啟用預設加密
Amazon Elastic Compute Cloud (Amazon EC2)	變更主機名稱
Amazon Machine Image (AMI)	刪除、共用
Amazon EC2 安全群組	任何
AMS 進階 SSPS	
AWS Managed Microsoft AD	
AMS Advanced 開發人員模式	
Amazon Simple Storage Service (Amazon S3)	建立 S3 儲存貯體政策
AWS Systems Manager	建立

使用直接變更模式建立堆疊

使用 在 CloudFormation 中啟動堆疊時，有兩個要求`AWSManagedServicesCloudFormationAdminRole`，以便 AMS 管理堆疊：

- 範本必須包含 `AmsStackTransform`。
- 堆疊名稱必須以字首開頭，`stack-`後面接著 17 個字元的英數字串。

> **Note**
>
> 若要成功使用 `AmsStackTransform`，您必須確認堆疊範本包含`CAPABILITY_AUTO_EXPAND`功能，以便 CloudFormation (CFN) 建立或更新堆疊。您可以在 create-stack 請求中傳遞 `CAPABILITY_AUTO_EXPAND`來執行此操作。如果在範本中`AmsStackTransform`包含 時未確認此功能，CFN 會拒絕請求。如果您的範本中有轉換，CFN 主控台會確保您傳遞此功能，但當您透過其 APIs 與 CFN 互動時，可能會遺漏此功能。

每當您使用下列 CFN API 呼叫時，都必須傳遞此功能：

- CreateChangeSet
- CreateStack
- UpdateStack

使用 DCM 建立或更新堆疊時，會在堆疊上執行 CFN 擷取和堆疊更新 CTs 的相同驗證和增強，如需詳細資訊CloudFormation ，請參閱擷取指導方針、最佳實務和限制。例外情況是，AMS 預設安全群組 (SGs) 不會連接到 Auto Scaling 群組 (ASGs) 中的任何獨立 EC2 執行個體或 EC2 執行個體。當您使用獨立 EC2 執行個體或 ASGs 建立 CloudFormation 範本時，您可以連接預設 SGs。

> **Note**
>
> IAM 角色現在可以使用 建立和管理AWSManagedServicesCloudFormationAdminRole。

AMS 預設 SGs 具有輸入和輸出規則，允許執行個體成功啟動，並在稍後透過 AMS 操作與您透過 SSH 或 RDP 存取。如果您發現 AMS 預設安全群組過於寬鬆，您可以使用更嚴格的規則建立自己的 SGs，並將其連接到執行個體，只要它仍然允許您和 AMS 操作在事件期間存取執行個體。

AMS 預設安全群組如下：

- SentinelDefaultSecurityGroupPrivateOnly：可透過此 SSM 參數在 CFN 範本中存取 `/ams/${VpcId}/SentinelDefaultSecurityGroupPrivateOnly`
- SentinelDefaultSecurityGroupPrivateOnlyEgressAll：可透過此 SSM 參數在 CFN 範本中存取 `/ams/${VpcId}/SentinelDefaultSecurityGroupPrivateOnlyEgressAll`

AMS 轉換

將`Transform`陳述式新增至 CloudFormation 範本。這會新增 CloudFormation 巨集，以在啟動時向 AMS 驗證和註冊堆疊。

JSON 範例

```
"Transform": {
    "Name": "AmsStackTransform",
    "Parameters": {
      "StackId": {"Ref" : "AWS::StackId"}
```

```
    }
  }
```

YAML 範例

```
Transform:
  Name: AmsStackTransform
  Parameters:
    StackId: !Ref 'AWS::StackId'
```

更新現有堆疊的範本時，也請新增 Transform陳述式。

JSON 範例

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description" : "Create an SNS Topic",
    "Transform": {
      "Name": "AmsStackTransform",
      "Parameters": {
        "StackId": {"Ref" : "AWS::StackId"}
     }
  },
  "Parameters": {
    "TopicName": {
      "Type": "String",
      "Default": "HelloWorldTopic"
    }
  },
  "Resources": {
    "SnsTopic": {
      "Type": "AWS::SNS::Topic",
      "Properties": {
        "TopicName": {"Ref": "TopicName"}
      }
    }
  }
}
```

YAML 範例

```
AWSTemplateFormatVersion: '2010-09-09'
```

```
Description: Create an SNS Topic
Transform:
  Name: AmsStackTransform
  Parameters:
    StackId: !Ref 'AWS::StackId'
Parameters:
  TopicName:
    Type: String
    Default: HelloWorldTopic
Resources:
  SnsTopic:
    Type: AWS::SNS::Topic
    Properties:
      TopicName: !Ref TopicName
```

堆疊名稱

堆疊名稱必須以字首開頭，stack-後面接著 17 個字元的英數字串。這是為了維持與在 AMS 堆疊 IDs 上操作之其他 AMS 系統的相容性。

以下是產生相容堆疊 IDs的方法範例：

Bash：

```
echo "stack-$(env LC_CTYPE=C tr -dc 'a-z0-9' < /dev/urandom | head -c 17)"
```

Python：

```
import string
import random

'stack-' + ''.join(random.choices(string.ascii_lowercase + string.digits, k=17))
```

Powershell：

```
"stack-" + ( -join ((0x30..0x39) + ( 0x61..0x7A) | Get-Random -Count 17  | %
 {[char]$_}) )
```

直接變更模式使用案例

以下是直接變更模式的使用案例：

透過 進行資源佈建和管理 CloudFormation

- 整合現有的 CloudFormation 型工具和程序。

持續的資源管理和更新

- 低風險的小型原子變化。
- 否則會透過手動或自動 RFC 執行的變更。
- 需要原生 AWS API 存取的工具。
- 如果您處於遷移階段，則可以使用 DCM 角色。遷移團隊會利用 DCM 上的許可來建立或修改堆疊。
- DCM 角色可用於 CI/CD 管道，以建立新的 AMIs、建立 Amazon ECS 任務等。

AMS 進階開發人員模式

主題

AWS Managed Services (AMS) 開發人員模式使用 AMS Advanced Plus 和 Premium 帳戶中的更高許可，在 AMS Advanced 變更管理程序之外佈建和更新 AWS 資源。AMS Advanced Developer 模式透過在 AMS Advanced Virtual Private Cloud (VPC) 中利用原生 AWS API 呼叫來執行此操作，讓您能夠在受管環境中設計和實作基礎設施和應用程式。

使用已啟用開發人員模式的帳戶時，系統會為透過 AMS 進階變更管理程序或使用 AMS Amazon Machine Image (AMI) 佈建的資源提供持續性管理、修補程式管理和變更管理。不過，這些 AMS 管理功能不適用於透過 AWS APIs 佈建的資源。

您有責任監控在 AMS 進階變更管理程序之外佈建的基礎設施資源。開發人員模式與生產和非生產工作負載相容。透過提高的許可，您更有責任確保遵守內部控制。

> **Important**
>
> 您使用開發人員模式建立的資源只有在使用 AMS 進階變更管理程序建立時，才能由 AMS Advanced 管理。

開發人員模式是您可以採用的 AMS 進階模式之一。如需詳細資訊，請參閱模式概觀。

AMS 進階開發人員模式入門

了解具有 AMS 進階開發人員模式的各種 AMS 進階帳戶，以及如何成功實作開發人員模式。

主題

開始使用 AMS 開發人員模式之前

在實作開發人員模式之前，您應該知道幾件事。

AMS Advanced 無法管理 DevMode 帳戶中透過變更請求 (RFCs) 在 AMS Advanced 變更管理程序之外建立的現有堆疊或資源。不過，當帳戶位於 DevMode 時，AMS Advanced 會繼續使用 RFCs 管理透過 AMS Advanced 變更管理程序佈建的資源。

您無法從 DevMode 帳戶開始，之後再將其隱藏到 AMS 進階受管應用程式帳戶。

AMS 開發人員模式的先決條件

以下是實作開發人員模式的先決條件：

- 您必須是至少擁有一個已加入 AMS Advanced Plus 或 Premium 帳戶的 AMS Advanced 客戶。
- 您使用的任何帳戶都必須是 AMS Advanced Plus 或 Premium 帳戶。

- 多帳戶登陸區域 (MALZ)：您必須使用AWSManagedServicesDevelopmentRole預先定義的 AWS Identity and Access Management (IAM) 角色。您請求此角色。下一節說明如何取得開發人員模式許可。
- 單一帳戶登陸區域 (SALZ)：您必須使用customer_developer_role預先定義的 AWS Identity and Access Management (IAM) 角色。您請求此角色。下一節說明如何取得開發人員模式許可。

如何實作 AMS 進階開發人員模式

您可以請求使用預先定義的 IAM 角色佈建符合資格的 AMS Advanced 帳戶，以實作開發人員模式：

- MALZ： AWSManagedServicesDevelopmentRole
- SALZ： customer_developer_role

然後，您將角色指派給聯合網路中的相關使用者。

AMS Advanced 建議您確保使用開發人員模式符合您的內部控制架構和標準，因為開發人員模式會建立兩種變更向量：適用於 AMS 進階受管資源的 AMS 進階變更管理，以及適用於您身為客戶管理之資源的客戶受管角色聯合。雖然 AMS Advanced 程序仍符合我們的宣告，但客戶程序和控制架構可能需要更新。

在 AMS Advanced 帳戶中實作開發人員模式

1. 確認您想要與開發人員模式搭配使用的帳戶符合 中列出的要求AMS 開發人員模式的先決條件。
2. 使用變更類型 (CT) 管理 | 受管帳戶 | 開發人員模式 | 啟用 （需要檢閱） 提交變更請求 (RFC)。如需如何使用此 CT 的範例，請參閱開發人員模式 | 啟用 （需要檢閱）。

   處理 CT 之後，預先定義的 IAM 角色 (AWSManagedServicesDevelopmentRoleMALZ 為 ，SALZ customer_developer_role為) 會在請求的帳戶中佈建。
3. 使用內部聯合程序，將適當的角色指派給需要開發人員模式存取的使用者。

   AMS Advanced 建議您限制存取，以防止不需要或未核准的資源佈建或變更。

AMS 進階開發人員模式許可

預先定義的角色 (AWSManagedServicesDevelopmentRole適用於 MALZ、customer_developer_role適用於 SALZ) 會授予許可，以在 AMS Advanced VPC 內建立應用程式基礎設施資源，包括 IAM 角色，同時限制存取由 AMS Advanced 操作的共用服務元件 （例

如，管理主機、網域控制站、Trend Micro EPS、堡壘和不支援的 AWS 服務）。此角色也會限制對下列項目的存取 AWS 服務：Amazon GuardDuty AWS Organizations、 AWS Directory Service APIs 和 AMS Advanced 日誌。

雖然角色可讓您建立其他 IAM 角色，但開發人員模式存取中包含的相同許可界限會在 建立的任何 IAM 角色上強制執行`AWSManagedServicesDevelopmentRole`。

開發人員模式中的安全性和合規性

安全與合規是 AMS Advanced 與身為客戶的您共同的責任。AMS Advanced Developer 模式會將變更管理程序外佈建或透過變更管理佈建，但使用開發人員模式許可更新之資源的共同責任轉移給您。如需共同責任的詳細資訊，請參閱 AWS Managed Services。

注意：

- DevMode 可讓您和您的授權團隊略過 AMS 安全性核心的deny-by-default原則。優點、自助服務、較少等待 AMS 的時間必須權衡缺點，任何人都可以在不了解其安全團隊的情況下執行非預期且破壞性的動作。用於啟用開發模式和直接變更模式的自動變更類型會公開，且組織中任何獲授權的人員都可以執行這些 CTs 並啟用這些模式。
- 您負責從使用者基礎管理 CT 執行的許可。
- AMS 不會管理 CT 執行許可

建議：

- 保護
  - 客戶可以透過許可防止存取此 CT，請參閱使用 IAM 角色政策陳述式限制許可
  - 透過實作 ITSM 系統等代理來防止存取此 CT
  - 使用可視需要防止政策和行為的服務控制政策 (SCPs)，請參閱 AMS Preventative and Detective Controls Library
- 偵測
  - 監控 RFC 的這些 CTs （啟用開發人員模式 ct-1opjmhuddw194 和直接變更模式、啟用 ct-3rd4781c2nnhp) 是否正在執行並相應地回應
  - 檢閱和/或稽核您的帳戶是否存在 IAM 資源，以識別已部署開發人員模式或直接變更模式的帳戶
- 回應
  - 視需要在開發人員模式中移除帳戶

開發人員模式中的安全性

AMS Advanced 提供具有規範登陸區域、變更管理系統和存取管理的額外值。使用開發人員模式時，會使用建立基準 AMS Advanced 安全性強化網路的標準 AMS Advanced 帳戶之相同帳戶組態，來保留 AMS Advanced 的安全值。網路受到角色中強制執行的許可界限 (`AWSManagedServicesDevelopmentRole`適用於 MALZ，`customer_developer_role`適用於 SALZ) 的保護，這會限制使用者分解帳戶設定時建立的參數保護。

例如，具有 角色的使用者可以存取 Amazon Route 53，但 AMS Advanced 內部託管區域受到限制。相同的許可界限會在 建立的 IAM 角色上強制執行`AWSManagedServicesDevelopmentRole`，在上強制執行許可界限`AWSManagedServicesDevelopmentRole`，以限制使用者細分帳戶加入 AMS Advanced 時建立的參數保護。

開發人員模式中的合規

開發人員模式與生產和非生產工作負載相容。您有責任確保遵守任何合規標準 （ 例如 PHI、HIPAA、PCI)，並確保使用開發人員模式符合您的內部控制架構和標準。

在開發人員模式下變更管理

變更管理是 AMS Advanced 服務用來實作變更請求的程序。變更請求 (RFC) 是由您或 AMS Advanced 透過 AMS Advanced 界面建立的請求，用於對受管環境進行變更，並包含特定操作的變更類型 (CT) ID。如需詳細資訊，請參閱變更管理模式。

在授予開發人員模式許可的 AMS Advanced 帳戶中，不會強制執行變更管理。已使用 IAM 角色 (`AWSManagedServicesDevelopmentRole`適用於 MALZ、`customer_developer_role`適用於 SALZ) 授予開發人員模式許可的使用者，可以使用原生 AWS API 存取來佈建和變更其 AMS Advanced 帳戶中的資源。在這些帳戶中沒有適當角色的使用者，必須使用 AMS 進階變更管理程序進行變更。

> **Important**
>
> 您使用開發人員模式建立的資源，只有在使用 AMS 進階變更管理程序建立時，才能由 AMS Advanced 管理。AMS Advanced 會拒絕針對在 AMS Advanced 變更管理程序之外建立的資源提交至 AMS Advanced 的變更請求，因為這些變更必須由您處理。

自助式佈建服務 API 限制

開發人員模式支援所有 AMS Advanced 自行佈建服務。對自行佈建服務的存取受個別使用者指南章節中概述的限制約束。如果您的開發人員模式角色無法使用自助佈建服務，您可以透過開發人員模式變更類型請求更新的角色。

下列服務不提供服務 APIs的完整存取權：

開發人員模式中限制的自助佈建服務

服務	備註
Amazon API Gateway	允許所有閘道 APIs呼叫，但 除外`SetWebACL`。
Application Auto Scaling	只能註冊或取消註冊可擴展的目標，並放置或刪除擴展政策。
AWS CloudFormation	無法存取或修改名稱字首為 的 CloudFormation 堆疊`mc-`。
AWS CloudTrail	無法存取或修改名稱字首為 `ams-`和/或 的 CloudTrail 資源`mc-`。
Amazon Cognito （使用者集區）	無法關聯軟體字符。 無法建立使用者集區、使用者匯入任務、資源伺服器或身分提供者。
AWS Directory Service	`Connect` 和 `WorkSpaces` 服務只需要下列 Directory Service 動作。開發人員模式許可界限政策會拒絕所有其他 Directory Service 動作： • `ds:AuthorizeApplication` • `ds:CreateAlias` • `ds:CreateIdentityPoolDirectory` • `ds:DeleteDirectory` • `ds:DescribeDirectories`

服務	備註
	• ds:GetAuthorizedApplication Details • ds:ListAuthorizedApplications • ds:UnauthorizeApplication 在單一帳戶登陸區域帳戶中，邊界政策明確拒絕存取 AMS Advanced 使用的 AMS Advanced 受管目錄，以維護對已啟用開發模式之帳戶的存取。
Amazon Elastic Compute Cloud	無法存取包含字串的 Amazon EC2 APIs：DhcpOptions 、Gateway、Subnet、VPC和 VPN。 無法存取或修改標籤字首為 AMS、ManagementHostASG 、 mc和/或 的 Amazon EC2 資源sentinel。
Amazon EC2 （報告）	僅授予檢視存取權 （無法修改）。注意：Amazon EC2 報告正在移動。報告選單項目將從 Amazon EC2 主控台導覽選單中移除。若要在移除之後檢視 Amazon EC2 用量報告，請使用 AWS Billing 和 Cost Management 主控台。

服務	備註
AWS Identity and Access Management (IAM)	無法刪除現有的許可界限，或修改 IAM 使用者密碼政策。 除非您使用正確的 IAM 角色 (AWSManagedServicesDevelopmentRole 適用於 MALZ、customer_developer_role 適用於 SALZ))，否則無法建立或修改 IAM 資源。 無法修改字首為：ams、customer_deny_policy 、 mc和/或 的 IAM 資源sentinel。 建立新的 IAM 資源 （角色、使用者或群組） 時，必須連接許可界限 (MALZ：AWSManagedServicesDevelopmentRolePermissionsBoundary 、SALZ：ams-app-infra-permissions-boundary)。
AWS Key Management Service (AWS KMS)	無法存取或修改 AMS 進階受管 KMS 金鑰。
AWS Lambda	無法存取或修改字首為 的 AWS Lambda 函數AMS。
CloudWatch Logs	無法存取名稱字首為 mc、、 awslambda和/或 的 CloudWatch 日誌串流AMS。
Amazon Relational Database Service (Amazon RDS)	無法存取或修改名稱字首為 的 Amazon Relational Database Service (Amazon RDS) 資料庫 (DBs)：mc-。
AWS Resource Groups	只能存取 Get、 List和 Search 資源群組 API 動作。
Amazon Route 53	無法存取或修改 Route53 AMS 進階維護的資源。

服務	備註
Amazon S3	無法存取名稱字首為：ams-*、ms-a、 ams或的 Amazon S3 儲存貯體mc-a。
AWS Security Token Service	唯一允許的安全性字符服務 API 是 DecodeAuthorizationMessage 。
Amazon SNS	無法存取名稱字首為：AMS-、 Energon-Topic 或 的 SNS 主題MMS-Topic 。
AWS Systems Manager 管理員 (SSM)	無法修改字首為 ams、 mc或 的 SSM 參數svc。 無法SendCommand 針對標籤字首為 ams或 的 Amazon EC2 執行個體使用 SSM APImc。
AWS 標記	您只能存取字首為 的 AWS 標記 API 動作Get。
AWS Lake Formation	下列 AWS Lake Formation API 動作遭拒： • lakeformation:DescribeResource • lakeformation:GetDataLakeSettings • lakeformation:DeregisterResource • lakeformation:RegisterResource • lakeformation:UpdateResource • lakeformation:PutDataLakeSettings
Amazon Elastic Inference	您只能呼叫 Elastic Inference API 動作 elastic-inference:Connect 。此許可包含在連接到 customer_sagemaker_admin_policy 的 中customer_sagemaker_admin_role 。此動作可讓您存取 Elastic Inference 加速器。

服務	備註
AWS Shield	無法存取任何此服務 APIs或主控台。
Amazon Simple Workflow Service	無法存取任何此服務 APIs或主控台。

在 AMS 開發人員模式下佈建基礎設施

沒有開發人員模式 IAM 角色的使用者`AWSManagedServicesDevelopmentRole`，在已啟用開發人員模式的帳戶中，必須遵循利用 AMS 進階 AMIs 的 AMS 進階變更管理程序。具有正確角色 (MALZ：`AWSManagedServicesDevelopmentRole`、SALZ：`customer_developer_role`) 的使用者可以使用 AMS 進階變更管理系統和 AMS 進階 AMIs但不需要。

> **Note**
>
> 尚未透過 AMS 進階工作負載擷取處理，或在 AWS AMS 進階帳戶中建立的 AMI，將不會包含 AMS 進階所需組態。

AMS 開發人員模式下的偵測控制

本節已修訂，因為它包含敏感的 AMS 安全相關資訊。此資訊可透過 AMS 主控台文件取得。若要存取 AWS Artifact，您可以聯絡 CSDM 以取得指示，或前往 AWS Artifact 入門。

在 AMS 開發人員模式下記錄、監控和事件管理

記錄、監控和事件管理不適用於在 AMS 進階變更管理程序之外佈建的資源，也不適用於透過變更管理佈建，然後使用開發人員模式許可由帳戶修改的資源。

AMS 開發人員模式下的事件管理

事件回應時間沒有變更。對於在變更管理程序之外佈建的資源，或是透過變更管理佈建，然後使用開發人員模式許可由帳戶修改的資源，事件解決是最大的努力。

> **Note**
>
> AMS 服務水準協議 (SLA) 不適用於在 AMS 變更管理系統 （變更請求或 RFCs) 之外建立或更新的資源，包含開發人員模式；因此，在開發人員模式中更新或建立的資源會自動降級為 P3，AMS 支援會盡最大努力。

AMS 開發人員模式下的修補程式管理

修補程式管理不適用於在 AMS 進階變更管理程序之外佈建的資源，或透過變更管理佈建的資源，然後使用開發人員模式許可由帳戶修改。修補時間：

- 對於重大安全性更新：在廠商發佈後 10 個工作天內，透過變更管理佈建的資源，然後由使用開發人員模式許可的帳戶進行變更。
- 重要更新：在廠商發佈後 2 個月內，透過變更管理佈建的資源，然後由使用開發人員模式許可的帳戶更改。

AMS 開發人員模式下的持續性管理

持續性管理不適用於在 AMS 進階變更管理程序之外佈建的資源，或透過變更管理佈建，然後使用開發人員模式許可由 帳戶修改的資源。

對於在 AMS 進階變更管理程序之外佈建的資源，或透過變更管理佈建，然後使用開發人員模式許可由帳戶修改的資源，環境復原啟動時間最多可能需要 12 小時。

AMS 開發人員模式下的安全性和存取管理

對於在 AMS 進階變更管理程序之外佈建的資源，或是透過變更管理佈建，然後使用開發人員模式許可由帳戶修改的資源，反惡意軟體保護是您的責任。未透過 AMS Advanced 變更管理佈建的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的存取權可能由金鑰對控制，而不是提供聯合存取。

AMS 中的自助式佈建模式

AWS Managed Services (AMS) 自助式佈建 (SSP) 模式可讓您完整存取 AMS 受管帳戶中的原生 AWS 服務和 API 功能。您可以透過標準化、縮小範圍、 AWS Identity and Access Management 角色來存取 服務。AMS 提供服務請求和事件管理。警示、監控、記錄、修補、備份和變更管理是您的責任。在許多情況下，自助式佈建服務 (SSPS) 是自我管理或無伺服器，不需要管理特定操作任務，例如修補。

您可以在 AMS 防護機制定義的環境界限內使用這些服務，而任何 IAM 變更（包括服務連結角色、服務角色、跨帳戶角色或政策更新）都需要經過 AMS Operations 核准，才能維護平台的基準安全性。您可以利用 CloudFormation 範本來自動化這些服務的部署，但並非所有 SSP 服務都支援此功能。

> **Important**
>
> 在 AWS Managed Services (AMS) 帳戶中使用 SSP 模式來存取和使用 AWS 服務，但有上述限制。

您可以在沒有 AMS 管理的情況下，在您的 AMS 帳戶中 AWS 服務 使用一些 。「自助式佈建模式」服務，或簡稱為「SSPS」，說明如何將它們新增至您的 AMS 帳戶和每個帳戶的FAQs」，如 一節所述。

自助式佈建服務會照原樣提供，而且您需負責管理這些服務。AMS 不會對與這些服務相關聯的資源提供提醒、監控、記錄或修補。AMS 提供 IAM 角色，可讓您安全地在 AMS 帳戶中使用服務。AMS SLAs 不適用。

對於您透過自助服務佈建的資源，AMS 提供事件管理、偵測控制和防護機制、報告、指定資源 (Cloud Service Delivery Manager 和 Cloud Architect)、安全性和存取，以及透過服務請求提供的技術支援。此外，在適用的情況下，您需為在 AMS 變更管理系統之外佈建或設定的資源承擔持續性管理、修補程式管理、基礎設施監控和變更管理的責任。

AMS 中的 SSP 模式入門

自助式佈建是您可以用於多帳戶登陸區域 (MALZ) 的 AMS 模式之一。如需詳細資訊，請參閱模式概觀。

為了提供自助式佈建功能，AMS 已建立具有許可界限的提升 IAM 角色，以限制直接 AWS 服務 存取的意外變更。這些角色不會阻止所有變更，而且您必須遵守內部控制和合規政策，並驗證所有 AWS 服務正在使用的 都符合必要的認證。這是自助式佈建模式。如需 AWS 合規要求的詳細資訊，請參閱AWS 合規。

若要將自助式佈建服務新增至多帳戶登陸區域應用程式帳戶，請依照服務的指示，使用 管理 | AWS 服務 | 自助佈建服務 | 新增變更類型 (CT)，包括檢閱所需的 CT 或自動 CT。

> **Note**
>
> 若要請求 AMS 提供額外的自助式佈建服務，請提交服務請求。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon API Gateway

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon API Gateway 功能。Amazon API Gateway 是一項全受管服務，可讓開發人員輕鬆建立、發佈、維護、監控和保護任何規模APIs。您可以使用 AWS 管理主控台 建立 REST 和 WebSocket APIs，做為應用程式從後端服務存取資料、商業邏輯或功能的大門，例如在 Amazon Elastic Compute Cloud (Amazon EC2) 上執行的工作負載、在 上執行的程式碼AWS Lambda、任何 Web 應用程式或即時通訊應用程式。

API Gateway 會處理所有涉及接受和處理多達數十萬個並行 API 呼叫的任務，包括流量管理、授權和存取控制、監控和 API 版本管理。API Gateway 沒有最低費用或啟動成本。您只需為收到的 API 呼叫和傳出的資料量付費，並且使用 API Gateway 分層定價模型，您可以隨著 API 用量的擴展而降低成本。若要進一步了解，請參閱 Amazon API Gateway。

常見問答集：AMS 中的 API Gateway

問：如何請求存取 AMS 帳戶中的 Amazon API Gateway？

透過使用 管理 | AWS 服務 | 自助佈建服務 | 新增 (ct-1w8z66n899dct) 變更類型提交 RFC，請求存取 API Gateway。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_apigateway_author_role`和 `customer_apigateway_cloudwatch_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon API Gateway 有哪些限制？

- API Gateway 組態僅限於沒有 `AMS-`或 字`MC-`首的資源，以防止對 AMS 基礎設施進行任何修改。
- `CREATE` VPCLink 的 權限已停用，以防止 Elastic Load Balancer 不受管制的建立。如果需要 VPCLinks，請參閱 Application Load Balancer | Create。

問：在我的 AMS 帳戶中使用 Amazon API Gateway 的先決條件或相依性是什麼？

這取決於您要部署的 API Gateway 類型。它可以是獨立服務，但也可以請求存取現有的服務 （ 例如網路負載平衡器 ）。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Alexa for Business

使用 AMS 自助式佈建 (SSP) 模式直接在您的 AMS 受管帳戶中存取 Alexa for Business 功能。Alexa for Business 是一項服務，可讓您的組織和員工使用 Alexa 來完成更多工作。透過 Alexa for Business，您可以使用 Alexa 作為智慧助理，在會議室、桌上，甚至在家裡或外出時使用的 Alexa 裝

置中提高生產力。IT 和設施管理員可以使用 Alexa for Business 來衡量和提高其工作場所中現有會議室的使用率。

若要進一步了解，請參閱 Alexa for Business。

AWS Managed Services 中的 Alexa for Business 常見問答集

問：如何在我的 AMS 帳戶中請求存取 Alexa for Business？

透過提交管理 | AWS 服務 | 自助佈建服務 | 新增 （需要檢閱）(ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_alexa_console_role`。`customer_alexa_device_setup_user` 也會為 Alexa for Business 提供的裝置設定工具建立 ；然後，可以使用此裝置設定工具來設定您的裝置。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

Alexa for Business 閘道可讓您將 Alexa for Business 連接至 Cisco Webex 和 Poly Group 系列端點，以使用語音控制會議。閘道軟體會在您的現場部署硬體上執行，並安全地將 Alexa for Business 的會議指令代理到 Cisco 端點。閘道需要兩對 AWS 登入資料才能與 Alexa for Business 通訊。我們提供兩個有限存取的 IAM 使用者： `customer_alexa_gateway_execution_user` `customer_alexa_gateway_installer_user`和您的 Alexa for Business 閘道，一個用於安裝閘道，另一個用於操作閘道；您可以透過使用 部署 | 進階堆疊元件 | Identity and Access Management (IAM) | 建立實體或政策 （需要檢閱） 變更類型 (ct-3dpd8mdd9jn1r) 提交 RFC 來請求這些使用者。

> **Note**
>
> 若要產生用量報告並將其傳送至 Amazon S3，請在自行佈建的服務 RFC 中指定 Amazon S3 儲存貯體名稱。

問：在我的 AMS 帳戶中使用 Alexa for Business 有哪些限制？

沒有限制。Alexa for Business 的完整功能可供 Alexa for Business 自助佈建服務角色使用。

問：在我的 AMS 帳戶中使用 Alexa for Business 的先決條件或相依性是什麼？

- 如果您想要使用 WPA2 Enterprise Wi-Fi 來設定共用裝置，請在裝置設定工具中指定此網路安全類型，其中 AWS 私有憑證授權單位 需要 。
- AMS 只會建立以命名空間 "A4B" 開頭的私密金鑰。這僅限於此命名空間。

問：什麼 Alexa for Business 功能需要單獨的 RFCs？

若要向 Alexa for Business 註冊 Alexa Voice Service (AVS) 裝置，請提供 Alexa 內建裝置製造商的存取權。若要這樣做，需要在 Alexa for Business 主控台中建立 IAM 角色，該角色可以使用 管理 | 其他 | 其他變更類型進行部署。這可讓 AVS 裝置製造商代表您向 Alexa for Business 註冊和管理裝置。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon AppStream 2.0

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon AppStream 2.0 (AppStream 2.0) 功能。AppStream 2.0 可讓您將桌面應用程式移至 AWS，而無需重寫。您可以在 AppStream 2.0 上安裝應用程式、設定啟動組態，並將應用程式提供給使用者。AppStream 2.0 提供多種虛擬機器選項，讓您可以選取最符合您應用程式需求的執行個體類型，並設定自動調整規模參數，以便輕鬆滿足最終使用者的需求。AppStream 2.0 可讓您在自己的網路中啟動應用程式，這表示您的應用程式可以與您現有的 AWS 資源互動。

Amazon AppStream 2.0 可讓您使用映像建置器快速輕鬆地安裝、測試和更新應用程式。支援在 Microsoft Windows Server 2012 R2、Windows Server 2016 或 Windows Server 2019 上執行的任何應用程式，而且您不需要進行任何修改。測試完成後，您可以設定應用程式啟動組態、預設使用者設定，並發佈映像以供使用者存取。

若要進一步了解，請參閱 AppStream 2.0。

AWS Managed Services 常見問答集中的 AppStream 2.0

問：如何請求存取 AMS 帳戶中的 AppStream 2.0？

透過使用 Management | AWS service | Self-visioned Service | Add (ct-3qe6io8t6jtny) 變更類型提交 RFC，請求存取 AppStream 2.0。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_appstream_console_role`。

`customer_appstream_stream_role` 也會部署 ，以串流要求使用者使用其 Active Directory 登入憑證進行身分驗證的應用程式。

在帳戶中佈建後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 AppStream 2.0 有哪些限制？

- 下列功能必須由 AMS 支援團隊設定，且需要特定的 RFCs。有關請求其他功能的說明，請參閱第 4 節。
  - 從介面 VPC 端點建立和串流。
  - 支援 Amazon S3 端點的主資料夾和私有網路上的應用程式設定持續性。
  - 建立並選擇可在所有機群串流執行個體上使用的 IAM 角色。

- 加入 AppStream 2.0 機群和映像建置器 Microsoft Active Directory 網域。
- 建立 AppStream 2.0 自訂用量報告。
- 目前不支援自訂品牌。

問：在我的 AMS 帳戶中使用 AppStream 2.0 有哪些先決條件或相依性？

提交 RFC 以加入 AppStream 2.0 時，請包含要用於 AppStream 2.0 用量報告的 Amazon S3 儲存貯體名稱。儲存貯體名稱會新增至 AppStream 2.0 加入時`customer-appstream-usagereports-policy`建立的 。

問：哪些 AppStream 2.0 功能需要單獨的 RFCs？

- 若要選擇 AppStream 2.0 的介面 VPC 端點，請提交管理 | 其他 | 其他 | 更新變更類型 RFC，以在您的帳戶中建立 VPC 端點。如需為 AppStream 2.0 建立自訂端點的步驟，請參閱 AppStream 2.0 使用者指南中的從介面 VPC 端點建立和串流。
- 透過使用管理 | 其他 | 其他 | 建立變更類型 RFC 請求 Amazon S3 VPC 端點，即可設定對私有網路上主資料夾和應用程式設定持續性的 Amazon S3 端點支援。RFC 必須分別包含託管主資料夾內容的目標 Amazon S3 儲存貯體，或 Amazon S3 儲存貯體的應用程式設定。此 RFC 將為 AppStream 2.0 提供存取 Amazon S3 VPC 端點所需的許可。如需為串流建立自訂端點的步驟，請參閱 AppStream 2.0 使用者指南中的將 Amazon S3 VPC 端點用於主資料夾和應用程式設定持續性。
- 若要建立和選擇可在所有機群串流執行個體上使用的 IAM 角色，請提交部署 | 進階堆疊元件 | 身分與存取管理 (IAM) | 建立實體或政策 （需要檢閱） 變更類型 (ct-3dpd8mdd9jn1r) RFC，以使用所需的政策請求 IAM 角色。IAM 角色名稱應一律以字首 ："customer_appstream" 開頭。
- Amazon AppStream 2.0 機群和映像建置器可以加入 Microsoft Active Directory 中的網域，方法是提交管理 | 其他 | 其他 | 更新 Active Directory (AD) 中服務帳戶建立的變更類型 RFC。在授予建立和管理 Active Directory 電腦物件的許可的 AppStream 2.0 文件中，定義了加入 Microsoft Active Directory 所需的最低許可。 https://docs.aws.amazon.com/appstream2/latest/developerguide/active-directory-admin.html#active-directory-permissions
- 若要建立自訂 AppStream 2.0 用量報告，請提交管理 | 其他 | 其他 | 建立變更類型 RFC 請求如下：
  - 建立「AppStreamUsageReports」CFN 堆疊
  - 帳戶中佈建「customer_appstream_usagereports_role」
  - 此外，請提供下列詳細資訊：
    - 提供 CRON 表達式來排程爬蟲程式執行。根據預設，每天為 23：00 UTC。
    - 用於 Athena 查詢結果的 Amazon S3 儲存貯體 ARN。此儲存貯體應有字首： `aws-athena-query-results`

- AppStream 2.0 用量報告日誌的 Amazon S3 儲存貯體 ARN。

佈建角色後，將角色加入您的聯合解決方案並登入，然後存取 AWS GlueAWS Glue 和 Athena 以使用用量報告角色產生自訂報告。如需使用 AppStream 2.0 用量報告的詳細資訊，請參閱 AppStream 2.0 文件中的建立自訂報告和分析 AppStream 2.0 用量資料。 AppStream

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Athena

使用 AMS 自助式佈建 (SSP) 模式，直接在您的 AMS 受管帳戶中存取 Amazon Athena (Athena) 功能。Athena 是一種互動式查詢服務，可協助您使用標準 SQL 分析 Amazon S3 中的資料。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。您可以指向 Amazon S3 中的資料、定義結構描述，並使用標準 SQL 開始查詢。大多數結果會在幾秒鐘內交付。使用 Athena，您不需要複雜的 extract-transform-load (ETL) 任務來準備資料以供分析。這可讓具備 SQL 技能的任何人直接分析大規模資料集。若要進一步了解，請參閱 Amazon Athena。

常見問答集：AMS 中的 Athena

問：如何請求存取 AMS 帳戶中的 Amazon Athena？

透過使用 Management | AWS service | Self-visioned Service | Add (ct-1w8z66n899dct) 變更類型提交 RFC 來請求存取 Athena。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_athena_console_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon Athena 有哪些限制？

沒有限制。Amazon Athena 的完整功能可在您的 AMS 帳戶中使用。

問：在我的 AMS 帳戶中使用 Amazon Athena 的先決條件或相依性是什麼？

Athena 使用以 建立的資料目錄/中繼存放區，因此對 AWS Glue 服務具有主要相依性 AWS Glue。因此， AWS Glue 許可會包含在成功的 Athena RFC 中。

角色`customer_athena_console_role`具有 Amazon S3 儲存貯體的先決條件。若要建立新的儲存貯體，請使用自動化 CT `ct-1a68ck03fn98r`（部署 | 進階堆疊元件 | S3 儲存 | 建立）。當您使用此自動化 CT 為 Athena 建立 S3 儲存貯體時，儲存貯體名稱必須以字首 開頭`athena-query-results-*`。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Bedrock

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon Bedrock 功能。Amazon Bedrock 是一項全受管服務，可讓領先業界的 AI 新創公司提供高效能的基礎模型 (FMs)，並透過統一

的 API AWS 供您使用。您可以從各種基礎模型中做選擇，找出最適合您使用案例的模型。Amazon Bedrock 還提供了一系列廣泛的功能，以建置具有安全性、隱私性和負責任之 AI 的生成式 AI 應用程式。使用 Amazon Bedrock 時，您可以輕鬆地為您的使用案例進行試驗，並評估最佳基礎模型，利用微調和檢索增強生成 (RAG) 等技術私下自訂資料，以及建置使用企業系統和資料來源執行任務的代理程式。

藉助 Amazon Bedrock 的無伺服器體驗，您可以快速入門，使用您自己的資料私下自訂基礎模型，並使用 AWS 工具輕鬆安全地整合和部署到您的應用程式中，而無需管理任何基礎設施。如需詳細資訊，請參閱 Amazon Bedrock。

常見問答集：AMS 中的 Amazon Bedrock

問：如何請求存取 AMS 帳戶中的 Amazon Bedrock？

若要請求存取 Amazon Bedrock，請使用 Management | AWS service | Self-visioned service | Add（需要檢閱）(ct-3qe6io8t6jtny) 變更類型提交 RFC。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_bedrock_console_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon Bedrock 有哪些限制？

- 預設不支援 Amazon Bedrock 知識庫做為 SSPS 角色的一部分，因為其相依於 AMS 上目前不支援的 Amazon OpenSearch Service Serverless。
- 由於 Bedrock Studio 依賴於 Amazon DataZone 等不支援的服務，因此不支援 Bedrock Studio。

問：在我的 AMS 帳戶中使用 Amazon Bedrock 的先決條件或相依性是什麼？

- 需要 AWS Marketplace 許可的第三方模型訂閱必須由預設角色完成 (`AWSManagedServicesAdminRole`在 MALZ 上和在 SALZ `Customer_ReadOnly_Role`上）。這是因為預設角色包含 AWS Marketplace 許可。
- 如果使用資料加密，則您必須在請求建立主控台角色時提供 AWS KMS 金鑰 ARN。此外，使用中的 Amazon S3 儲存貯體名稱中必須有「bedrock」。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon CloudSearch

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon CloudSearch 功能。Amazon CloudSearch 是 AWS 雲端中的受管服務，可讓您以經濟實惠的方式設定、管理和擴展網站或應用程式

的搜尋解決方案。Amazon CloudSearch 支援 34 種語言和熱門搜尋功能，例如反白、自動完成和地理空間搜尋。若要進一步了解，請參閱 Amazon CloudSearch。

> **Note**
>
> AWS 自 2024 年 7 月 25 日起， 已關閉新客戶對 Amazon CloudSearch 的存取權。Amazon CloudSearch 現有客戶可以繼續正常使用服務。 AWS 會繼續投資 Amazon CloudSearch 的安全性、可用性和效能改善，但我們不打算推出新功能。
> 若要了解 Amazon CloudSearch 和 Amazon OpenSearch Service 之間的差異，以及轉換至 OpenSearch Service 的方式，請聯絡您的雲端架構師 (CA) 以取得指引。如需轉換至 OpenSearch Service 的詳細資訊，請參閱從 Amazon CloudSearch 轉換至 Amazon OpenSearch Service 服務。

AWS Managed Services 常見問答集中的 Amazon CloudSearch

問：如何請求存取 AMS 帳戶中的 Amazon CloudSearch？

透過使用 Management | AWS service | Self-visioned Service | Add (ct-1w8z66n899dct) 變更類型提交 RFC，請求存取 Amazon CloudSearch。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_csearch_admin_role`和 `customer_csearch_dev_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon CloudSearch 有哪些限制？

Amazon CloudSearch 的完整功能可在您的 AMS 帳戶中使用。Amazon CloudSearch 目前支援所有 AMS 支援的資料庫解決方案。請注意，DynamoDB 目前是唯一無法編製索引的受管 AWS 資料庫解決方案。

問：在我的 AMS 帳戶中使用 Amazon CloudSearch 的先決條件或相依性是什麼？

Amazon CloudSearch 依賴 Amazon S3 與身分提供者合作，以自動分析輸入資料並判斷資料表欄位。此 RFC 不提供對 Amazon S3 的存取，且必須在服務請求中另外請求。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon CloudWatch Synthetics

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon CloudWatch Synthetics 功能。您可以使用 Amazon CloudWatch Synthetics 建立 'canary' 來監控您的端點和 APIs。

Canary 是可設定的指令碼，以 Node.js 或 Python 撰寫，按排程執行。Canary 會使用 Node.js 或 Python 作為架構，在您的帳戶中建立 Lambda 函數。Canary 透過 HTTP 和 HTTPS 通訊協定運

作。Canary 會檢查端點的可用性和延遲，並可儲存載入時間資料和 UI 螢幕擷取畫面。它們會監控您的 REST API、URL 和網站內容，並且可以檢查來自網路釣魚、程式碼插入和跨網站指令碼的未經授權變更。

Canary 遵循與客戶相同的路由並執行相同的動作，讓您可以持續驗證客戶體驗，即使您的應用程式上沒有任何客戶流量。透過使用 Canary，您可以在客戶之前發現問題。若要進一步了解，請參閱 Amazon CloudWatch：使用合成監控。

AWS Managed Services 中的 Amazon CloudWatch Synthetics 常見問答集

問：如何請求存取 AMS 帳戶中的 Amazon CloudWatch Synthetics？

透過使用 Management | AWS service | Self-visioned Service | Add (ct-1w8z66n899dct) 變更類型提交 RFC，請求存取 Amazon CloudWatch Synthetics。此 RFC 會將下列 IAM 角色佈建至您的帳戶：'customer_cw_synthetics_console_role' 和 'customer_cw_synthetics_canary_lambda_role'。在帳戶中佈建後，您必須在聯合解決方案中加入 'customer_cw_synthetics_console_role' 角色。

問：在我的 AMS 帳戶中使用 Amazon CloudWatch Synthetics 有哪些限制？

在您的 AMS 帳戶中使用 Amazon CloudWatch Synthetics 沒有限制。禁止為 AMS 提供服務角色 'customer_cw_synthetics_canary_lambda_role' 以外的 Canary 建立角色。

問：在我的 AMS 帳戶中使用 Amazon CloudWatch Synthetics 有哪些先決條件或相依性？

Canary 建立並使用預設的 Amazon CloudWatch Synthetics S3 儲存貯體："cw-syn-results-*${accountnumber}*-*${default-region}*"

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Cognito 使用者集區

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon Cognito 使用者集區功能。Amazon Cognito 使用者集區提供安全的使用者目錄，可擴展到數億使用者。Amazon Cognito 使用者集區是全受管服務，無需擔心伺服器基礎設施。此服務可讓您管理最終使用者的集區，可用來與內部應用程式整合。此服務為您提供自訂資料庫或 Web 或行動應用程式最終使用者目錄的替代方案。同時，Amazon Cognito 使用者集區提供目錄服務的完整功能，例如密碼政策、多重要素驗證、密碼復原和自我註冊服務。它還允許應用程式聯合其他熱門公有服務的存取，例如 OpenID、Facebook、Amazon 或 Google。

Amazon Cognito 分為兩個主要產品。Amazon Cognito 使用者集區和 Amazon Cognito 身分提供者。本節著重於 Amazon Cognito 使用者集區，提供 Amazon S3 或 DynamoDB 等 AWS 其他服務的存取權。此服務可讓您使用 Amazon Cognito 使用者集區或第三方身分提供者來提供 AWS 服務的存取權。它也提供使用匿名訪客存取 AWS 的服務存取權。由於 Amazon Cognito 使用者集區的強大性質，它將

以操作手動服務的形式case-by-case手動管理，以避免潛在的安全中斷到帳戶中。若要進一步了解，請參閱 Amazon Cognito 使用者集區。

AWS Managed Services 常見問答集中的 Amazon Cognito 使用者集區

常見問題和解答：

問：如何請求存取 AMS 帳戶中的 Amazon Cognito 使用者集區？

在 AMS 中實作 Amazon Cognito 使用者集區是 2 個步驟：

1. 提交管理 | 其他 | 其他 | 建立 (ct-1e1xtak34nx76) 變更類型，並請求在您的 AMS 帳戶中建立 Amazon Cognito 使用者集區。加入下列資訊：
   - AWS 區域。
   - Cognito 使用者集區的名稱。
   - 如果您想要使用 Amazon Simple Email Service (Amazon SES) 來傳送訊息和通知，而不是預設的內部 Cognito 郵件服務，則客戶應在帳戶中為 Amazon SES Service 提供已驗證的電子郵件地址。此地址將用於訊息的「寄件人」和「REPLY-TO」欄位。他們還必須指出啟用 Amazon SES 的區域 (us-east-1、eu-west-1 或 us-west-2)。
   - 如果您想要使用簡訊進行一次性密碼和驗證，則客戶應該指出這一點。
2. 透過提交管理 | AWS 服務 | 自助佈建服務 | 新增變更類型 (ct-1w8z66n899dct) 來請求使用者存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶： `customer_cognito_admin_role`和 `customer_cognito_importjob_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。這些角色可讓您管理 Amazon Cognito 使用者集區、管理集區中的使用者和群組、為使用者建立 importjobs、修改通知和訂閱訊息、將應用程式與使用者集區建立關聯、將聯合服務自我管理新增至集區，以及刪除已建立的集區。

問：在我的 AMS 帳戶中使用 Amazon Cognito 使用者集區有哪些限制？

您將無法建立 Amazon Cognito 使用者集區。該動作需要建立 IAM 角色，才能利用 Amazon Cognito 使用的服務，例如 Amazon SES 和 Amazon Simple Notification Service (Amazon SNS)。

問：在我的 AMS 帳戶中使用 Amazon Cognito 使用者集區的先決條件或相依性是什麼？

如果您想要使用 Amazon SES 透過電子郵件將訊息和通知傳送到使用者集區，他們應該已在帳戶中啟用 Amazon SES 服務，並已驗證應該在已傳送電子郵件的「FROM」和「REPLY-TO」欄位中使用的電子郵件地址。如需使用 Amazon SES 驗證電子郵件地址的詳細資訊，請參閱在 Amazon SES 中驗證電子郵件地址。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Comprehend

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon Comprehend 功能。Amazon Comprehend 是一種自然語言處理 (NLP) 服務，使用機器學習在文字中尋找洞見和關係，不需要機器學習體驗。Amazon Comprehend 使用機器學習來協助您探索非結構化資料中的洞見和關係。服務可識別文字的語言；擷取關鍵片語、位置、人物、品牌或事件；了解文字的正面或負面程度；使用字符化和部分語音分析文字；並自動依主題組織文字檔案的集合。您也可以在 Amazon Comprehend 中使用 AutoML 功能來建置一組自訂的實體或文字分類模型，這些模型專為您的組織需求量身打造。若要進一步了解，請參閱 Amazon Comprehend。

AWS Managed Services 常見問答集中的 Amazon Comprehend

問：如何請求存取 AMS 帳戶中的 Amazon Comprehend？

您可以透過提交兩個 AMS Service RFCs 來請求 Amazon Comprehend 主控台和資料存取角色：

透過提交管理 | AWS 服務 | 自助佈建服務 | 新增 （需要檢閱） (ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_comprehend_console_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon Comprehend 有哪些限制？

透過 Amazon Comprehend 主控台建立新的 IAM 角色功能受到限制。否則，Amazon Comprehend 的完整功能可在您的 AMS 帳戶中使用。

問：在我的 AMS 帳戶中使用 Amazon Comprehend 的先決條件或相依性是什麼？

如果 Amazon S3 儲存貯體使用 AWS KMS 金鑰加密，則需要 Amazon S3 和 AWS Key Management Service (AWS KMS) 才能使用 Amazon Comprehend。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Connect

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

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon Connect 功能。Amazon Connect 是全通道雲端聯絡中心，可協助公司以較低的成本提供卓越的客戶服務。Amazon Connect 可為客戶和客服人員提供順暢的語音和聊天體驗。這包括一組用於技能型路由的工具、功能強大的即時和歷史分析，以及easy-to-use管理工具 – 全部都具有pay-as-you-go定價。

您可以在 AMS 多帳戶登陸區域或單一帳戶登陸區域帳戶中建立一或多個虛擬聯絡中心執行個體。您可以使用現有的 SAML 2.0 身分提供者進行代理程式存取，或使用 Amazon Connect 原生支援進行使用者生命週期管理。

此外，您可以從 Amazon Connect 主控台為每個 Amazon Connect 執行個體申請免付費電話/直撥電話號碼。您可以使用easy-to-use圖形使用者介面建立豐富的聯絡流程，以實現所需的客戶體驗和轉接。聯絡流程可以利用 AWS Lambda 函數與內部部署資料存放區和 API 整合。您也可以使用 Kinesis Streams 和 Firehose 啟用資料串流。

通話錄音、聊天文字記錄和報告存放在使用 AWS KMS 金鑰加密的 Amazon S3 儲存貯體中。聯絡流程日誌可以儲存到 CloudWatch 日誌群組。

若要進一步了解，請參閱 Amazon Connect。

AWS Managed Services 常見問答集中的 Amazon Connect

問：如何請求存取 AMS 帳戶中的 Amazon Connect？

透過提交管理 | AWS 服務 | 自行佈建服務 | 新增 （需要檢閱） (ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶： `customer_connect_console_role`和 `customer_connect_user_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon Connect 有哪些限制？

沒有限制。Amazon Connect 的完整功能可在您的 AMS 帳戶中使用。

問：在我的 AMS 帳戶中使用 Amazon Connect 有哪些先決條件或相依性？

- 您必須使用標準 AMS RFCs 建立 AWS KMS 金鑰和 Amazon S3 儲存貯體；儲存通話錄音和聊天文字記錄時需要 Amazon S3 儲存貯體。
- 如果您想要與 Active Directory (AD) 整合，則需要 AD Connector 才能整合 AMS 託管的 Amazon Connect 執行個體和您的內部部署目錄服務。AD Connector 可以在您的帳戶中設定，方法是請求 'Management | Other | Other' RFC。
- 您可以根據您的聯絡流程需求，啟用下列選用的自行佈建服務。
  - AWS Lambda：您可以使用 Lambda 函數來擴展聯絡流程，以利用現有的內部部署資料存放區或 APIs。您可以使用 Lambda 自行佈建服務來建立 Lambda 函數。

- Amazon Kinesis Data Streams：您可以建立資料串流，以啟用資料串流至外部應用程式。您可以串流聯絡追蹤記錄或客服人員事件。
- Amazon Kinesis Data Firehose：您可以建立 Data Firehose，將大量聯絡追蹤記錄串流至外部應用程式。
- Amazon Lex：您可以利用 Amazon Lex Chatbots，利用 Amazon Alexa 服務建立智慧聯絡流程，以獲得豐富的客戶體驗和自動化。

- 問：如何請求新增撥出或撥入通話的國家/地區清單？

  若要新增撥出或撥入通話的國家/地區清單，請向 AMS 提交服務請求。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Data Firehose

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon Data Firehose 功能。Firehose 是可靠地將串流資料載入資料湖、資料存放區和分析工具的最簡單方法。它可以擷取、轉換串流資料，並將資料載入 Amazon S3、Amazon Redshift、Amazon OpenSearch Service 和 Splunk，以便使用您目前已使用的現有商業智慧工具和儀表板進行近乎即時的分析。這是一種全受管服務，可自動擴展以符合資料的輸送量，而且不需要持續管理。它也可以在載入資料之前批次處理、壓縮、轉換和加密資料，將目的地使用的儲存量降至最低，並提高安全性。若要進一步了解，請參閱什麼是 Amazon Data Firehose？

AWS Managed Services 常見問答集中的 Firehose

常見問題和解答：

問：如何請求存取 AMS 帳戶中的 Amazon Data Firehose？

透過提交管理 | AWS 服務 | 自助佈建服務 | 新增 （需要檢閱） (ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_kinesis_firehose_user_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Firehose 有哪些限制？

沒有限制。Amazon Data Firehose 的完整功能可在您的 AMS 帳戶中使用。

問：在我的 AMS 帳戶中使用 Firehose 的先決條件或相依性是什麼？

必須為每個交付串流請求新的服務連結 IAM 角色。您也可以使用所需的資源許可 （包括 S3 儲存貯體/KMS 金鑰/Lambda 函數/Kinesis 串流） 更新角色政策，為所有串流重複使用單一服務連結角色。

在您提交 RFC 以新增 Firehose 之後，AMS Operations 工程師將透過您想要與 Data Firehose 連線之資源 ARNs 的服務請求 （ 例如 AWS KMS S3、Lambda 和 Kinesis Streams) 與您聯絡。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon DevOpsGuru

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon DevOpsGuru 功能。Amazon DevOpsGuru 是一項全受管操作服務，可讓開發人員和操作員輕鬆改善其應用程式的效能和可用性。DevOpsGuru 可讓您卸載與識別操作問題相關的管理任務，以便快速實作建議以改善應用程式。DevOpsGuru 會建立反應式洞見，您現在可以用來改善您的應用程式。它也會建立主動洞見，協助您避免未來可能會影響應用程式的操作問題。DevOpsGuru 會套用機器學習來分析您的操作資料和應用程式指標和事件，以識別偏離正常操作模式的行為。當 DevOpsGuru 偵測到操作問題或風險時，您會收到通知。對於每個問題，DevOps 都會提供智慧型建議，以解決目前和預測的未來營運問題。

若要進一步了解，請參閱什麼是 Amazon DevOpsGuru。

AWS Managed Services 常見問答集中的 Amazon DevOpsGuru

問：如何在我的 AMS 帳戶中請求存取 Amazon DevOpsGuru？

若要請求存取，請提交管理 | AWS 服務 | 自助佈建服務 | 新增 （ 需要檢閱 ） (ct-3qe6io8t6jtny) 變更類型。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_devopsguru_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon DevOpsGuru 有哪些限制？

沒有限制。Amazon DevOpsGuru 的完整功能可在您的 AMS 帳戶中使用。

問：在我的 AMS 帳戶中使用 Amazon DevOpsGuru 的先決條件或相依性是什麼？

沒有先決條件。DevOpsGuru 會利用下列 AWS 服務：Amazon CloudWatch Logs、RDS Insights AWS X-Ray AWS Lambda和 AWS CloudTrail。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon DocumentDB （ 與 MongoDB 相容 ）

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon DocumentDB （ 具有 MongoDB 相容性 ） 功能。Amazon DocumentDB （ 與 MongoDB 相容 ） 是一種快速、可擴展、高可用性且全受管的文件資料庫服務，可支援 MongoDB 工作負載。Amazon DocumentDB 為您提供大規模操作關鍵任務 MongoDB 工作負載時所需的效能、可擴展性和可用性。Amazon DocumentDB 會透過模擬 MongoDB 用戶端從 MongoDB 伺服器預期的回應來實作 Apache 2.0 開放原始碼 MongoDB 3.6 API，讓您將現有的 MongoDB 驅動程式和工具與 Amazon DocumentDB 搭配使用。在 Amazon

DocumentDB 中，儲存和運算會分離，允許每個 獨立擴展，而且無論您的資料大小為何，您都可以新增最多 15 個低延遲僅供讀取複本，將讀取容量增加到每秒數百萬個請求。Amazon DocumentDB 旨在提供 99.99% 的可用性，並跨三個 AWS 可用區域 (AZs) 複寫資料的六個副本。您可以使用 AWS Database Migration Service (DMS) 免費 （六個月） 將內部部署或 Amazon Elastic Compute Cloud (Amazon EC2) MongoDB 資料庫遷移至 Amazon DocumentDB，幾乎沒有停機時間。若要進一步了解，請參閱 Amazon DocumentDB （與 MongoDB 相容）。

AWS Managed Services 常見問答集中的 Amazon DocumentDB

問：如何請求存取 AMS 帳戶中的 Amazon DocumentDB？

您可以透過提交兩個 AMS RFCs 來請求 Amazon DocumentDB 主控台和資料存取角色：主控台存取和資料存取：

透過使用 Management | AWS 服務 | 自助佈建服務 | 新增 (ct-1w8z66n899dct) 變更類型提交 RFC，請求存取 Amazon DocumentDB。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_documentdb_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon DocumentDB 有哪些限制？

Amazon DocumentDB 需要 Amazon RDS 特定的許可。由於 AMS 完全管理 Amazon RDS，Amazon DocumentDB 的 IAM 角色包含對 Amazon RDS 上動作的一些限制。將適用以下限制：

- 對 `DeleteDBInstance`和 `DeleteDBCluster` APIs存取已受到限制。若要使用這些刪除 APIs，請提交 RFC 與 管理 | 進階堆疊元件 | Identity and Access Management (IAM) | 更新實體或政策 （需要檢閱） 變更類型 (ct-27tuth19k52b4)。
- 您無法從 Amazon RDS 執行個體新增或移除標籤。
- 您無法將 Amazon DocumentDB 執行個體設為公有。

問：在我的 AMS 帳戶中使用 Amazon DocumentDB 的先決條件或相依性是什麼？

如果 Amazon S3 儲存貯體使用 AWS KMS 金鑰加密， AWS KMS 則需要 Amazon S3 和 才能使用 Amazon DocumentDB。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon DynamoDB

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon DynamoDB (DynamoDB) 功能。Amazon DynamoDB 是金鑰值和文件資料庫，可在任何規模提供單一位數毫秒的效能。它是一個全受管、多區域、多活動資料庫，具有內建安全性、備份和還原，以及適用於網際網路擴展應用程式的記憶體內快取。如需詳細資訊，請參閱 Amazon DynamoDB。

Amazon DynamoDB Accelerator (DAX) 是全部寫入快取服務，設計目的是要簡化將快取新增至 DynamoDB 資料表的程序。DAX 適用於需要高效能讀取的應用程式。

AWS Managed Services 常見問答集中的 DynamoDB

問：如何在我的 AMS 帳戶中請求存取 DynamoDB 和 DAX？

透過使用 Management | AWS 服務 | 自助佈建服務 | 新增 (ct-1w8z66n899dct) 變更類型提交 RFC，請求存取 DynamoDB 和 DAX。此 RFC 會將下列 IAM 角色和政策佈建至您的帳戶：

- DynamoDB 角色名稱： `customer_dynamodb_role`

  DAX 服務角色名稱： `customer_dax_service_role`
- DynamoDB 政策名稱： `customer_dynamodb_policy`

  DAX 服務政策： `customer_dax_service_policy`

在帳戶中佈建後，您必須在聯合解決方案`customer_dynamodb_role`中加入 。

問：在我的 AMS 帳戶中使用 DynamoDB 有哪些限制？

支援所有 DynamoDB 功能，包括 DynamoDB Accelerator (DAX)。

為任何指定資料表建立警示時，警示名稱必須以「客戶*」字首；例如 `customer-employee-table-high-put-latency`。

為 DynamoDB 建立 Amazon SNS 主題時，必須命名為：dynamodb。

若要刪除 DynamoDB 建立的 Amazon SNS 主題，請提交管理 | 其他 | 其他 | 更新變更類型 RFC。

問：在我的 AMS 帳戶中使用 DynamoDB 的先決條件或相依性是什麼？

在您的 AMS 帳戶中使用 DynamoDB 沒有先決條件或相依性。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Elastic Container Registry

使用 AMS 自助式佈建 (SSP) 模式，直接在您的 AMS 受管帳戶中存取 Amazon Elastic Container Registry (Amazon ECR) 功能。Amazon Elastic Container Registry 是全受管的 Docker 容器登錄檔，可讓開發人員輕鬆儲存、管理和部署 Docker 容器映像。Amazon ECR 與 Amazon Elastic Container Service (Amazon ECS) 整合，可簡化生產工作流程的開發。Amazon ECR 無需操作您自己的容器儲存庫，也無需擔心擴展基礎基礎設施。Amazon ECS 會將您的映像託管在高可用性和可擴展的架構中，

讓您可以可靠地部署應用程式的容器。與 AWS Identity and Access Management (IAM) 整合可提供每個儲存庫的資源層級控制。使用 Amazon ECR，無需預付費用或承諾。您只需為存放在儲存庫中的資料量和傳輸至網際網路的資料付費。

若要進一步了解，請參閱 Amazon Elastic Container Registry。

AWS Managed Services 常見問答集中的 Amazon Elastic Container Registry

問：如何請求存取 AMS 帳戶中的 Amazon ECR？

透過使用 管理 | AWS 服務 | 自助佈建服務 | 新增 (ct-1w8z66n899dct) 變更類型提交 RFC，請求存取 Amazon ECR。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_ecr_console_role`和 `customer_ecr_poweruser_instance_profile_policy`分別`customer_ecr_poweruser_instance_profile`搭配相關聯的 IAM 政策`customer_ecr_console_policy`和 。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon ECR 有哪些限制？

AMS 命名空間有在您的 AMS 帳戶中使用 Amazon ECR 的限制。容器映像的字首不得為 "AMS-" 或 "Sentinel-"。

問：在我的 AMS 帳戶中使用 Amazon ECR 的先決條件或相依性是什麼？

在您的 AMS 帳戶中使用 Amazon ECR 沒有先決條件或相依性。

使用 AMS SSP 在您的 AMS 帳戶中佈建 EC2 Image Builder

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 EC2 Image Builder 功能。EC2 Image Builder 是一項全受管 AWS 服務，可讓您更輕鬆地自動化自訂、安全且up-to-date「黃金」伺服器映像的建立、管理和部署，這些映像已預先安裝並預先設定軟體和設定，以符合特定 IT 標準。

您可以使用 AWS 管理主控台、 AWS CLI 或 APIs 在 AWS 帳戶中建立自訂映像。當您使用 時 AWS 管理主控台，Amazon EC2 Image Builder 精靈會引導您完成以下步驟：

- 提供起始成品
- 新增和移除軟體
- 自訂設定和指令碼
- 執行選取的測試
- 將映像分佈至 AWS 區域

您建置的映像會在您的帳戶中建立，並且可以持續針對作業系統修補程式進行設定。若要進一步了解，請參閱 EC2 Image Builder。

AWS Managed Services 常見問答集中的 EC2 Image Builder

常見問題和解答：

問：如何請求存取 AMS 帳戶中的 EC2 Image Builder？

透過提交管理 | AWS 服務 | 自助佈建服務 | 新增 （需要檢閱） (ct-3qe6io8t6jtny) 變更類型來請求存取權。透過此 RFC，會在您的帳戶中佈建下列 IAM 角色： `customer_ec2_imagebuilder_role`。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

問：EC2 Image Builder 有哪些限制？

AMS 不支援使用基礎設施組態的服務預設值。您可以建立新的基礎設施組態或使用現有的基礎設施組態。

AMS 目前不支援建立容器配方。

問：啟用 EC2 Image Builder 的先決條件或相依性有哪些？

- EC2 Image Builder 服務連結角色：您不需要手動建立服務連結角色。當您在 AWS 管理主控台、CLI 或 AWS API AWS 中建立第一個 Image Builder 資源時，Image Builder 會為您建立服務連結角色。
- 用於使用 Image Builder 建置映像和執行測試的執行個體必須能夠存取 Systems Manager 服務。如果來源映像尚未存在，則 SSM 代理程式會安裝在來源映像上，並在建立映像之前將其移除。
- AWS IAM：與執行個體描述檔建立關聯的 IAM 角色必須具有許可，才能執行映像中包含的建置和測試元件。下列 IAM 角色政策必須連接到與執行個體描述檔相關聯的 IAM 角色：`EC2InstanceProfileForImageBuilder`和 `AmazonSSMManagedInstanceCore`。IAM 角色名稱應該包含 `*imagebuilder*`關鍵字。
- 如果您設定記錄，基礎設施組態中指定的執行個體描述檔必須具有目標儲存貯體 () 的`s3:PutObject`許可`arn:aws:s3:::{bucket-name}/*`。例如：

  JSON

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

```
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::{bucket-name}/*"
        }
    ]
}
```

- 建立名為 'imagebuilder' 的 SNS 主題，以接收來自 EC2 Image Builder 的任何提醒和通知。

使用 AMS SSP 在 AMS 帳戶中的 AWS Fargate 上佈建 Amazon ECS

使用 AMS 自助式佈建 (SSP) 模式直接在 AMS 受管帳戶中存取 Amazon ECS on AWS Fargate 功能。AWS Fargate 是一項技術，您可以與 Amazon ECS 搭配使用來執行容器（請參閱 上的容器 AWS），而無需管理 Amazon EC2 執行個體的伺服器或叢集。使用 AWS Fargate，您不再需要佈建、設定或擴展虛擬機器叢集來執行容器。這樣一來即無須選擇伺服器類型、決定何時擴展叢集，或最佳化叢集壓縮。

若要進一步了解，請參閱 上的 Amazon ECS AWS Fargate。

AWS Managed Services 常見問答集中的 Fargate 上的 Amazon ECS

問：如何在 AMS 帳戶中請求存取 Fargate 上的 Amazon ECS？

透過使用 管理 | AWS 服務 | 自助佈建服務 | 新增 (ct-1w8z66n899dct) 變更類型提交 RFC，請求存取 Fargate 上的 Amazon ECS。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_ecs_fargate_console_role`（如果沒有提供現有 IAM 角色將 ECS 政策與 建立關聯）`customer_ecs_fargate_events_service_role`、、`customer_ecs_task_execution_servic` `customer_ecs_codedeploy_service_role`和 `AWSServiceRoleForApplicationAutoScaling_ECSService`。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中在 Fargate 上使用 Amazon ECS 有哪些限制？

- Amazon ECS 任務監控和記錄會被視為您的責任，因為容器層級活動發生在 Hypervisor 上方，而記錄功能受到 Fargate 上的 Amazon ECS 限制。身為 Fargate 上的 Amazon ECS 使用者，我們建議您採取必要步驟來啟用 Amazon ECS 任務的記錄。如需詳細資訊，請參閱為您的容器啟用 awslogs 日誌驅動程式。

- 容器層級的安全和惡意軟體保護也被視為您的責任。Fargate 上的 Amazon ECS 不包含 Trend Micro 或預先設定的網路安全元件。
- 此服務適用於多帳戶登陸區域和單一帳戶登陸區域 AMS 帳戶。
- 根據預設，自我佈建角色中的 Amazon ECS Service Discovery 會受到限制，因為建立 Route 53 私有託管區域需要更高的許可。若要在服務上啟用服務探索，請提交管理 | 其他 | 其他 | 更新變更類型。若要提供為 Amazon ECS Service 啟用 Service Discovery 所需的資訊，請參閱 Service Discovery 手冊。
- AMS 目前不會管理或限制用於在 Amazon ECS Fargate 上部署至容器的映像。您將能夠從 Amazon ECR、Docker Hub 或任何其他私有映像儲存庫部署映像。因此，我們建議不要部署公有或任何不安全的影像，因為它們可能會導致帳戶中的惡意活動。

問：在我的 AMS 帳戶中在 Fargate 上使用 Amazon ECS 的先決條件或相依性是什麼？

- 以下是 Fargate 上 Amazon ECS 的相依性；不過，使用自行佈建角色啟用這些服務不需要其他動作：
  - CloudWatch Logs
  - CloudWatch 活動
  - CloudWatch 警示
  - CodeDeploy
  - App Mesh
  - 雲端地圖
  - Route 53
- 根據您的使用案例，以下是 Amazon ECS 所依賴的資源，在帳戶中使用 Fargate 上的 Amazon ECS 之前可能需要的資源：
  - 要與 Amazon ECS 服務搭配使用的安全群組。您可以使用部署 | 進階堆疊元件 | 安全群組 | 建立（自動）(ct-3pc215bnwb6p7)，或者，如果您的安全群組需要特殊規則，請使用部署 | 進階堆疊元件 | 安全群組 | 建立（需要檢閱）(ct-1oxx2g2d7hc90)。注意：您使用 Amazon ECS 選取的安全群組必須專門為 Amazon ECS 服務或叢集所在的 Amazon ECS 建立。您可以在 Amazon Elastic Container Service 中的設定 Amazon ECS 和安全性一節中進一步了解。
  - 應用程式負載平衡器 (ALB)、網路負載平衡器 (NLB)、用於任務之間負載平衡的傳統負載平衡器 (ELB)。
  - ALBs 的目標群組。

- 要與您的 Amazon ECS 叢集整合的應用程式網格資源 （例如 Virtual Router、Virtual Services、Virtual Nodes)。
- 目前，當在標準 AMS 變更類型之外建立時，AMS 無法自動降低與支援安全群組許可相關的風險。我們建議您請求特定安全群組以搭配 Fargate 叢集使用，以限制使用未指定用於 Amazon ECS 的安全群組的可能性。

使用 AMS SSP AWS Fargate 在 AMS 帳戶中佈建 Amazon EKS

使用 AMS 自助式佈建 (SSP) 模式直接在您的 AMS 受管帳戶中存取 Amazon EKS on AWS Fargate 功能。 AWS Fargate 是一種技術，可為容器提供隨需、大小正確的運算容量 （若要了解容器，請參閱什麼是容器？)。使用 AWS Fargate，您不再需要佈建、設定或擴展虛擬機器群組來執行容器。這樣一來即無須選擇伺服器類型、決定何時擴展節點群組，或最佳化叢集壓縮。

Amazon Elastic Kubernetes Service (Amazon EKS) 透過 AWS Fargate 使用 Kubernetes 提供的 AWS 上游可擴展模型建置的控制器，將 Kubernetes 與 整合。這些控制器作為 Amazon EKS 受管 Kubernetes 控制平面的一部分執行，並負責將原生 Kubernetes Pod 排程到 Fargate。Fargate 控制器包括新的排程器，除了數個變換與驗證許可控制器之外，也會隨著預設 Kubernetes 排程器執行。當您啟動符合在 Fargate 上執行之條件的 Pod 時，在叢集中執行的 Fargate 控制器便會辨識、更新及將 Pod 排程至 Fargate。

若要進一步了解，請參閱 Amazon EKS on AWS Fargate Now Generally Available 和 Amazon EKS 安全最佳實務指南 （包括「建議」，例如「檢閱和撤銷不必要的匿名存取」等）。

> **Tip**
>
> AMS 具有變更類型：部署 | 進階堆疊元件 | 身分與存取管理 (IAM) | 建立 OpenID Connect 提供者 (ct-30ecvfi3tq4k3)，可與 Amazon EKS 搭配使用。如需範例，請參閱 Identity and Access Management (IAM) | Create OpenID Connect Provider。

AWS Managed Services 常見問答集 AWS Fargate 中的 Amazon EKS on

問：如何在我的 AMS 帳戶中請求存取 Fargate 上的 Amazon EKS？

透過提交管理 | AWS 服務 | 自行佈建服務 | 新增 （需要檢閱） (ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶。

- `customer_eks_fargate_console_role`.

在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

- 這些服務角色授予 Amazon EKS on Fargate 代表您呼叫其他 AWS 服務的許可：
  - `customer_eks_pod_execution_role`
  - `customer_eks_cluster_service_role`

問：在我的 AMS 帳戶中在 Fargate 上使用 Amazon EKS 有哪些限制？

- AMS 不支援建立受管或自我管理的 EC2 節點群組。如果您需要使用 EC2 工作者節點，請聯絡您的 AMS Cloud Service Delivery Manager (CSDM) 或 Cloud Architect (CA)。
- AMS 不包含 Trend Micro 或預先設定的容器映像網路安全元件。您需要管理自己的映像掃描服務，以在部署之前偵測惡意容器映像。
- 由於 CloudFormation 相互依存性，不支援 EKSCTL。
- 在叢集建立期間，您有停用叢集控制平面記錄的許可。如需詳細資訊，請參閱 Amazon EKS 控制平面記錄。我們建議您在建立叢集時啟用所有重要的 API、身分驗證和稽核記錄。
- 在叢集建立期間，Amazon EKS 叢集的叢集端點存取預設為公有；如需詳細資訊，請參閱 Amazon EKS 叢集端點存取控制。建議您將 Amazon EKS 端點設定為私有。如果公有存取需要端點，則最佳實務是僅針對特定 CIDR 範圍將其設定為公有。
- AMS 沒有強制和限制用於部署到 Amazon EKS Fargate 容器之映像的方法。您可以從 Amazon ECR、Docker Hub 或任何其他私有映像儲存庫部署映像。因此，部署可能在該帳戶上執行惡意活動的公有映像會有風險。
- AMS 不支援透過雲端開發套件 (CDK) 或 CloudFormation Ingest 部署 EKS 叢集。
- 您必須使用 ct-3pc215bnwb6p7 部署 | 進階堆疊元件 | 安全群組 | 在資訊清單檔案中建立和參考，以建立輸入。這是因為角色`customer-eks-alb-ingress-controller-role`未獲授權建立安全群組。

問：在我的 AMS 帳戶中在 Fargate 上使用 Amazon EKS 的先決條件或相依性是什麼？

若要使用 服務，必須設定下列相依性：

- 如需驗證服務，必須安裝 KUBECTL 和 aws-iam-authenticator；如需詳細資訊，請參閱管理叢集身分驗證。
- Kubernetes 倚賴稱為「服務帳戶」的概念。為了在 EKS 上利用 kubernetes 叢集內的服務帳戶功能，必須使用下列輸入進行管理 | 其他 | 更新 RFC：
  - 【必要】 Amazon EKS 叢集名稱

- 【必要】 將部署服務帳戶 (SA) 的 Amazon EKS 叢集命名空間。
- 【必要】 Amazon EKS 叢集 SA 名稱。
- 【必要】 要關聯的 IAM 政策名稱和許可/文件。
- 【必要】 正在請求的 IAM 角色名稱。
- 【選用】 OpenID Connect 提供者 URL。如需詳細資訊，請參閱
  - 在叢集上啟用服務帳戶的 IAM 角色
  - 為服務帳戶介紹精細的 IAM 角色
- 建議您設定和監控 Config 規則
  - 公有叢集端點
  - 停用 API 記錄

  您有責任監控和修復這些 Config 規則。

如果您想要部署 ALB 傳入控制器，請提交管理 | 其他 | 其他更新 RFC，以佈建要與 ALB 傳入控制器 Pod 搭配使用的必要 IAM 角色。建立要與 ALB 傳入控制器建立關聯的 IAM 資源 （ 請在 RFC 中包含這些資源 ） 需要下列輸入：

- 【必要】 Amazon EKS 叢集名稱
- 【選用】 OpenID Connect 提供者 URL
- 【選用】 Amazon EKS 叢集命名空間，其中將部署應用程式負載平衡器 (ALB) 輸入控制器服務。【預設：kube-system】
- 【選用】 Amazon EKS 叢集服務帳戶 (SA) 名稱。【預設：aws-load-balancer-controller】

如果您想要在叢集中啟用信封秘密加密 （ 我們建議 ），請在 RFC 的描述欄位中提供您要使用的 KMS 金鑰 IDs，以新增服務 (Management | AWS service | Self-visioned service | Add (ct-1w8z66n899dct)。若要進一步了解信封加密，請參閱 Amazon EKS 使用 AWS KMS 新增秘密的信封加密。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon EMR

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon EMR 功能。Amazon EMR 是領先業界的雲端大數據平台，可使用 Apache Spark、Apache Hive、Apache HBase、Apache Flink、Apache Hudi 和 Presto 等開放原始碼工具來處理大量資料。使用 Amazon EMR，您可以執行 PB 級分析，成本不到傳統內部部署解決方案的一半，比標準 Apache Spark 快 3 倍以上。對於短期執

行的任務，您可以向上和向下旋轉叢集，並為使用的執行個體每秒付費。對於長時間執行的工作負載，您可以建立高度可用的叢集，以自動擴展以滿足需求。

您可以在 AMS 多帳戶登陸區域或單一帳戶登陸區域帳戶中建立一或多個 Amazon EMR 叢集執行個體，以支援暫時性和持久性 Amazon EMR 叢集。您也可以啟用 Kerberos 身分驗證，以啟用來自內部部署 Active Directory 網域的身分驗證使用者。

您可以使用 Amazon EMR 叢集利用多個資料存放區，以支援使用案例特定的 Hadoop 工具和程式庫。您可以使用 OnDemand 或 Spot 執行個體建立 Amazon EMR 叢集，並設定自動擴展以管理容量並降低成本。

叢集日誌檔案可以封存到 Amazon S3 儲存貯體以進行記錄和偵錯。您也可以存取 Amazon EMR 叢集中託管的 Web 介面，以支援雜湊管理要求或為客戶記錄書籍體驗。

若要進一步了解，請參閱 Amazon EMR。

AWS Managed Services 常見問答集中的 Amazon EMR

問：如何請求存取 AMS 帳戶中的 Amazon EMR？

透過提交管理 | AWS 服務 | 自助佈建服務 | 新增 （需要檢閱） (ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：

- `customer_emr_cluster_instance_profile`
- `customer_emr_cluster_autoscaling_role`
- `customer_emr_console_role`
- `customer_emr_cluster_service_role`

在帳戶中佈建後，您必須在聯合解決方案中加入 customer_emr_console_role。

問：在我的 AMS 帳戶中使用 Amazon EMR 有哪些限制？

從 AWS 主控台在 EC2 叢集上建立 Amazon EMR 時，我們建議您使用建立叢集 – 進階選項。Amazon EMR 叢集必須透過新增索引鍵為「for-use-with-amazon-emr-managed-policies」且值為「true」的標籤來建立。在安全選項中選取下列組態：

- 選取叢集的自訂角色：
  - EMR 角色：Customer_emr_cluster_service_role

  - EC2 執行個體設定檔：Customer_emr_cluster_instance_profile
  - Auto Scaling 角色：Customer_emr_cluster_autoscaling_role
- EC2 安全群組：
  - 主要 ：ams-emr-master-security-group
  - 核心與任務：ams-emr-worker-security-group
  - 服務存取：ams-emr-serviceaccess-security-group

問：在我的 AMS 帳戶中使用 Amazon EMR 的先決條件或相依性是什麼？

AMS 會為 Amazon EMR 主節點、工作者節點和服務節點建立預設安全群組。

要與 Amazon EMR 叢集搭配使用的啟動範本和安全群組必須具有值為 "true" 的標籤索引鍵 "for-use-with-amazon-emr-managed-policies"。

預設 Amazon EMR 叢集執行個體描述檔可讓您存取 資源，例如 s3 儲存貯體和 dynamodb 資料表，其名稱包含 "emr"。您可以請求其他 IAM 政策，以使用與 Amazon EMR 搭配使用的任何其他資源。下列資源 ARN 可與使用 customer_emr_cluster_instance_profile 的 Amazon EMR 任務搭配使用：

- arn：aws：dynamodb：*：*：table/*emr*
- arn：aws：kinesis：*：*：stream/*emr*
- arn：aws：sns：*：*：*emr*arn：aws：sqs：*：*：*emr*
- arn：aws：sqs：*：*：*emr*
- arn：aws：sqs：*：*：AWS-ElasticMapReduce-*
- arn：aws：sdb：*：*：domain：*emr*
- arn：aws：s3：：*emr*

如果 Amazon EMR 叢集需要 kerberos 身分驗證：

- 提供要用於每個角化 Amazon EMR 叢集的領域名稱和內部部署 Active Directory IP 地址。
- 基礎設施需求：

  多帳戶登陸區域 (MALZ)：提交 RFC 以在現有應用程式帳戶中建立新的受管應用程式帳戶或新的 VPC。

  單一帳戶登陸區域 (SALZ)：提交 RFC 以在 VPC 中建立新的子網路。

- 在內部部署 Active Directory 上設定叢集領域傳入的信任。
- 在 Managed AD 中提交 RFC 來設定領域 DNS 區域。
- 領域組態：

  MALZ：提交管理 | 其他 | 其他 | 更新 (ct-0xdawir96cy7k) RFC 以更新 VPC DHCP 選項集，以使用網域名稱尾碼的領域名稱。

  SALZ：提交管理 | 其他 | 其他 | 更新 (ct-0xdawir96cy7k) RFC，以產生新的 Amazon EMR AMI，以使用網域名稱尾碼的特定領域。

若要部署 Amazon EMR Studio，角色`customer_emr_cluster_service_role`具有 Amazon Simple Storage Service 儲存貯體的先決條件。若要建立儲存貯體，請使用自動化 CT `ct-1a68ck03fn98r`（部署 | 進階堆疊元件 | S3 儲存 | 建立）。當您使用此自動化 CT 為 Amazon EMR 建立 Amazon S3 儲存貯體時，儲存貯體名稱必須以字首 開頭`customer-emr-*`。此外，您必須在與 Amazon EMR 叢集相同的 AWS 區域中建立儲存貯體。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon EventBridge

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon EventBridge 功能。Amazon EventBridge 為無伺服器事件匯流排服務，可讓您輕鬆將應用程式與來自各種來源的資料互相連線。EventBridge 可從您自己的應用程式、Software-as-a-Service(SaaS) 應用程式 AWS 和服務提供即時資料串流，並將該資料路由至 等目標 AWS Lambda。您可設定路由規則來決定要將資料送往何處，以便建立即時對您所有資料來源做出反應的應用程式架構。EventBridge 可讓您建置鬆耦合和分散式的事件驅動架構。

若要進一步了解，請參閱 Amazon EventBridge。

AWS Managed Services 常見問答集中的 EventBridge

問：如何請求存取 AMS 帳戶中的 EventBridge？

透過使用 Management | AWS 服務 | 自助佈建服務 | 新增 (ct-1w8z66n899dct) 變更類型提交 RFC，請求存取 EventBridge。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_eventbridge_role`和 `customer_eventbridge_scheduler_execution_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

執行角色 `customer_eventbridge_scheduler_execution_role` 是 EventBridge 排程器擔任的 IAM 角色， AWS 服務 可代表您與其他 互動。連接到此角色的許可政策會授予 EventBridge 排程器調用目標的存取權。

> **Note**
>
> 根據預設，EventBridge 排程器會使用 EventBridge 的 AWS 擁有金鑰來加密資料。若要使用 EventBridge 的客戶受管金鑰來加密資料，請使用 Management | AWS 服務 | 自助佈建服務 | 新增 （需要檢閱） 變更類型 (ct-3qe6io8t6jtny) 提交 RFC 以進行服務佈建。

問：在我的 AMS 帳戶中使用 EventBridge 有哪些限制？

您必須提交 AMS RFCs 並建立下列資源：觸發批次任務的服務角色、SQS 佇列、CodeBuild、CodePipeline 和 SSM 命令。

問：在我的 AMS 帳戶中使用 EventBridge 的先決條件或相依性是什麼？

您必須使用 部署 | EventBridge 進階堆疊元件 | Identity and Access Management (IAM) | 建立實體或政策 （需要檢閱） 變更類型 (ct-3dpd8mdd9jn1r) 請求具有 RFC 的 EventBridge 服務角色，才能使用 EventBridge 觸發其他 AWS 資源 AWS Batch，例如 Lambda、Amazon SNS、Amazon SQS 或 Amazon CloudWatch Logs 資源。指定請求您的服務角色時要叫用的服務。若要了解叫用目標所需的許可，請參閱使用 EventBridge 的資源型政策。

EventBridge 已與 整合 AWS CloudTrail，此服務提供由使用者、角色或 EventBridge AWS 服務 中 所採取動作的記錄。必須啟用並允許 CloudTrail 將日誌檔案存放到 S3 儲存貯體。注意：所有 AMS 帳戶都已啟用 CloudTrail，因此不需要採取任何動作。

問：角色 customer_eventbridge_scheduler_execution_role 具有 AWS Key Management Service 金鑰的先決條件 （選用，如果用於加密）。如何在靜態/傳輸資料加密中採用 AWS KMS CMKs？

根據預設，EventBridge 排程器會加密儲存在 AWS 擁有金鑰 （靜態加密） 下的事件中繼資料和訊息資料。EventBridge 排程器也會使用 Transport Layer Security (TLS) （傳輸中加密） 加密 EventBridge 排程器與其他 服務之間傳遞的資料。

如果您的特定使用案例要求您控制和稽核可在 EventBridge 排程器上保護資料的加密金鑰，您可以使用客戶受管金鑰。

在使用 Amazon EventBridge 加入 AWS KMS 許可之前，您必須使用 管理 | AWS 服務 | 自助佈建服務 | 新增 （需要檢閱） 變更類型來請求 RFC。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Forecast

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon Forecast （預測） 功能。Amazon Forecast 是一種全受管服務，使用機器學習來提供高度準確的預測。

> **Note**
>
> AWS 自 2024 年 7 月 29 日起， 已關閉新客戶對 Amazon Forecast 的存取權。Amazon Forecast 現有客戶可以繼續照常使用服務。 AWS 會繼續投資 Amazon Forecast 的安全性、可用性和效能改善，但不 AWS 打算推出新功能。
> 如果您想要使用 Amazon Forecast，請聯絡您的 CSDM，以便他們可以進一步引導您如何將 Amazon Forecast 用量轉移至 Amazon SageMaker Canvas。

根據 Amazon.com 使用的相同技術，Forecast 使用機器學習來結合時間序列資料和其他變數來建置預測。預測不需要機器學習經驗即可開始。您只需要提供歷史資料，以及您認為可能會影響預測的任何其他資料。例如，對襯衫特定顏色的需求可能會隨季節和存放位置而改變。這種複雜的關係很難自行判斷，但機器學習非常適合識別它。提供資料後，Forecast 會自動檢查資料、識別有意義的內容，並產生預測模型，能夠進行比僅查看時間序列資料高出 50% 的預測。

若要進一步了解，請參閱 Amazon Forecast。

AWS Managed Services 常見問答集中的 Amazon Forecast

問：如何請求存取 AMS 帳戶中的預測？

透過使用 管理 | AWS 服務 | 自助佈建服務 | 新增 (ct-1w8z66n899dct) 變更類型提交 RFC AWS Firewall Manager 來請求存取 。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_forecast_admin_role`。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用預測有哪些限制？

預設 S3 儲存貯體存取僅允許您存取命名模式為 'customer-forecast-*' 的儲存貯體。如果您有自己的資料儲存貯體命名慣例，請與您的 Cloud Architect (CA) 討論儲存貯體命名和相關存取設定。例如：

- 您可以使用 'AmazonForecast-ExecutionRole-*' 等命名和相關聯的適當 S3 儲存貯體存取來定義特定 AmazonForecast 服務角色。請參閱 IAM 主控台中的服務角色 - AmazonForecast-ExecutionRole-Admin 和 IAM 政策 - customer_forecast_default_s3_access_policy。
- 您可能需要將相關的 S3 儲存貯體存取與 IAM 聯合角色建立關聯。請參閱 IAM 主控台中的 IAM 政策 - customer_forecast_default_s3_access_policy。

問：在我的 AMS 帳戶中使用 Forecast 有哪些先決條件或相依性？

- 使用 Forecast 之前，必須先建立適當的 Amazon S3 儲存貯體 (Amazon S3)。特別是，預設 S3 儲存貯體存取是使用命名模式「customer-forecast-*」
- 如果您想要在 'customer-forecast-*' 以外的 S3 儲存貯體上使用命名模式，則必須在儲存貯體上建立具有 S3 存取許可的新服務角色：
  1. 要使用命名 'AmazonForecast-ExecutionRole-{suffix}' 建立新的服務角色。
  2. 要建立的新 IAM 政策類似於 customer_forecast_default_s3_access_policy，並與新服務角色和相關聯合管理角色相關聯 （例如 'customer_forecast_admin_role')

問：如何使用 Amazon Forecast 增強資料安全性？

- 對於靜態資料加密，您可以使用 AWS KMS 來佈建客戶管理的 CMK，以保護 Amazon S3 服務上的資料儲存：
  - 使用佈建金鑰在儲存貯體上啟用預設加密，並設定儲存貯體政策以接受 AWS KMS 資料加密，同時放置資料。
  - 以 AWS KMS 金鑰使用者身分啟用 Amazon Forecast 服務角色 'AmazonForecast-ExecutionRole-*' 和聯合管理角色 （例如 'customer_forecast_admin_role')。
- 對於傳輸中的資料加密，您可以設定 HTTPS 通訊協定，這是在 Amazon S3 儲存貯體政策上傳輸物件時的必要通訊協定。
- 存取控制的進一步限制，為 Amazon Forecast 服務角色 'AmazonForecast-ExecutionRole-*' 和管理員角色 （例如 'customer_forecast_admin_role') 的已核准存取權啟用儲存貯體政策。

問：使用 Amazon Forecast 時的最佳實務為何？

- 您應該充分了解資料分類實務，並在搭配 Amazon Forecast 使用 S3 儲存貯體時，找出相關的資料安全需求。
- 對於 Amazon S3 儲存貯體組態，強烈建議您在 S3 儲存貯體政策中啟用 HTTPS 強制執行。
- 您必須知道 Amazon S3 儲存貯體上的管理員角色 'customer_forecast_admin_role' 支援許可存取 (Get/Delete/Put S3 物件），其命名為 'customer-forecast-*'。 Amazon S3 注意：如果您需要多個團隊的精細存取控制，請遵循下列實務：
  - 定義以團隊為基礎的存取 IAM 身分 （角色/使用者），具有對相關 Amazon S3 儲存貯體的最低權限存取權。
  - 建立以團隊/專案為基礎的 AWS KMS CMKs會授予對對應 IAM 身分的適當存取權。（使用者存取權和 'AmazonForecast-ExecutionRole-{team/project}'。

- 使用已建立 AWS KMS CMKs 設定 S3 儲存貯體預設加密。
- 在 S3 儲存貯體政策上使用 HTTPS 通訊協定強制執行 S3 API 流量。
- 強制執行 S3 儲存貯體組態，以針對相關 IAM 身分 （ 使用者存取和儲存貯體的 'AmazonForecast-ExecutionRole-{team/project}'。
- 如果您想要將 'customer_forecast_admin_role' 用於一般用途，請考慮先前列出的點以保護 S3 儲存貯體。

問：Amazon Forecast 的合規資訊在哪裡？

請參閱 AWS 服務合規計劃。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon FSx

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon FSx 功能。Amazon FSx 提供全受管第三方檔案系統。Amazon FSx 為您提供第三方檔案系統的原生相容性，其功能集適用於 Windows 型儲存、高效能運算 (HPC)、機器學習和電子設計自動化 (EDA) 等工作負載。Amazon FSx 會自動執行耗時的管理任務，例如硬體佈建、軟體組態、修補和備份。Amazon FSx 將檔案系統與雲端原生 AWS 服務整合，因此對更廣泛的工作負載更加有用。

Amazon FSx 為您提供兩種檔案系統供您選擇：適用於 Windows 應用程式的 Amazon FSx for Windows File Server 和適用於運算密集型工作負載的 Amazon FSx for Lustre。若要進一步了解，請參閱 Amazon FSx。

AWS Managed Services 常見問答集中的 Amazon FSx

問：如何請求存取 AMS 帳戶中的 Amazon FSx？

透過使用 管理 | AWS 服務 | 自助佈建服務 | 新增 (ct-1w8z66n899dct) 變更類型提交 RFC，請求存取 Amazon FSx。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_fsx_admin_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon FSx 有哪些限制？

沒有限制。服務的完整功能可供使用。

問：在我的 AMS 帳戶中使用 Amazon FSx 的先決條件或相依性是什麼？

沒有先決條件。不過，對於多可用區等進階組態，您必須安裝和管理 DFS 複寫和 DFS 命名空間服務。如需詳細資訊，請參閱部署多可用區域檔案系統。

問：如何將 Amazon FSx 檔案系統與多帳戶登陸區域 Managed AD 整合？

建立 Amazon FSx 檔案系統時，您可以將 MALZ Managed AD 指定為 'AWS Managed Microsoft Active Directory' for Windows Authentication。如需詳細資訊，請參閱搭配 AWS Directory Service for Microsoft Active Directory 使用 Amazon FSx

您也必須先將 Managed AD 分享給應用程式帳戶。透過使用 Management | Directory Service | Directory | Share Directory 變更類型 (ct-369odosk0pd9w) 提交 RFC 來執行此操作。

問：哪些使用者屬於 AWS 委派 FSx 管理員群組？

只有 IT 檔案伺服器管理員。此群組具有所有檔案共享的完整存取權限。

問：我應該使用佈建 FSx 系統時建立的預設檔案共享、共享嗎？

否，我們不建議使用佈建的預設檔案共享、共享。它將完整存取權授予每個人，這違反最低權限原則。反之，請建立符合您業務需求的較小自訂檔案共享。

問：如何為業務中的特定組織建立自訂檔案共享？

如需建立自訂檔案共享的說明，請參閱檔案共享。使用最低權限原則限制每個檔案共享的存取。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon FSx for OpenZFS

使用 AMS 自助式佈建 (SSP) 模式，直接在您的 AMS 受管帳戶中存取 Amazon FSx for OpenZFS 功能。FSx for OpenZFS 是一種全受管檔案儲存服務，可讓您輕鬆地將內部部署 ZFS 或其他 Linux 型檔案伺服器中的資料移至 AWS，而無需變更應用程式程式碼或管理資料的方式。它提供以開放原始碼 OpenZFS 檔案系統建置的高度可靠、可擴展性、高效能和功能豐富的檔案儲存，提供 OpenZFS 檔案系統的熟悉功能和功能，以及全受管 AWS 服務的敏捷性、可擴展性和簡易性。對於建置雲端原生應用程式的開發人員，它提供簡單、高效能的儲存體，具有豐富的資料使用功能。

FSx for OpenZFS 檔案系統可使用業界標準的 NFS 通訊協定 (v3、v4.0、v4.1、v4.2)，從 Linux、Windows 和 macOS 運算執行個體和容器廣泛存取。FSx for OpenZFS 採用 AWS Graviton 處理器和最新的 AWS 磁碟和聯網技術 （ 包括 AWS 可擴展可靠資料包聯網和 AWS Nitro 系統 ），可提供高達 100 萬個 IOPS，延遲數百微秒。透過對即時point-in-time快照和資料複製等 OpenZFS 功能的完整支援，FSx for OpenZFS 可讓您輕鬆地將現場部署檔案伺服器取代為提供熟悉檔案系統功能的 AWS 儲存體，並消除執行冗長資格和變更或重新建構現有應用程式或工具的需求。此外，FSx for OpenZFS 結合了 OpenZFS 資料管理功能的強大功能與最新 AWS 技術的高效能和成本效益，可讓您建置和執行高效能的資料密集型應用程式。

做為全受管服務，FSx for OpenZFS 可讓您在 上輕鬆啟動、執行和擴展全受管檔案系統 AWS ，以取代您在內部部署中執行的檔案伺服器，同時協助提供更好的敏捷性和降低成本。使用 FSx for OpenZFS，您不再需要擔心設定和佈建檔案伺服器和儲存磁碟區、複寫資料、安裝和修補檔案伺服器軟體、偵測和解決硬體故障，以及手動執行備份。它還提供與其他 AWS 服務的豐富整合，例如 AWS Identity and Access Management (IAM)、 AWS Key Management Service (AWS KMS)、Amazon CloudWatch 和 AWS CloudTrail。

Amazon FSx 為您提供兩種檔案系統供您選擇：適用於 Windows 應用程式的 Amazon FSx for Windows File Server 和適用於運算密集型工作負載的 Amazon FSx for Lustre。若要進一步了解，請參閱 Amazon FSx。

AWS Managed Services 常見問答集中的 Amazon FSx for OpenZFS

問：如何請求在我的 AMS 帳戶中使用 FSx for OpenZFS 的存取權？

透過使用 Management | AWS service | Self-visioned Service | Add (ct-1w8z66n899dct) 變更類型提交 RFC，請求存取 Amazon FSx OpenZFS。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_fsx_ontap_admin_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 FSx for OpenZFS 有哪些限制？

取代 Amazon FSx 彈性網路介面 (ENIs) 上的安全群組需要您提交管理 | 其他 | 其他 | 更新 RFCs因為安全群組是 AMS 環境的關鍵周邊。這是唯一的限制。

問：在我的 AMS 帳戶中使用 FSx for OpenZFS 的先決條件或相依性是什麼？

沒有先決條件。不過，您必須使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon FSx已安裝 。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon FSx for NetApp ONTAP

使用 AMS 自助式佈建 (SSP) 模式，直接在您的 AMS 受管帳戶中存取 Amazon FSx for NetApp ONTAP 功能。Amazon FSx for NetApp ONTAP 是一項全受管服務，可在 NetApp 的熱門 ONTAP 檔案系統上提供高度可靠、可擴展、高效能且功能豐富的檔案儲存。它提供 NetApp 檔案系統的熟悉功能、效能、功能和 APIs，具有全受管系統的靈活性、可擴展性和簡易性 AWS 服務。

Amazon FSx for NetApp ONTAP 提供功能豐富、快速且靈活的共用檔案儲存，可從 Linux、Windows 和在內部部署中執行 AWS 的 macOS 運算執行個體廣泛存取。FSx for ONTAP 提供低於毫秒延遲的高效能 SSD 儲存體，讓您只要按一下按鈕，即可快速且輕鬆地管理您的資料。它也會自動將資料分層為成本較低的彈性儲存，無需佈建或管理容量，並可讓您為工作負載達到 SSD 效能層級，同時只需為一

小部分的資料支付 SSD 儲存費用。它提供高可用性和耐用的儲存，具有全受管備份和支援跨區域災難復原，並支援熱門的資料安全和防毒應用程式，讓您更輕鬆地保護和保護您的資料。對於使用 NetApp ONTAP 內部部署的客戶，FSx for ONTAP 是將檔案型應用程式從內部部署遷移、備份或爆量到 的理想解決方案， AWS 而無需變更應用程式程式碼或管理資料的方式。

Amazon FSx for NetApp ONTAP 是全受管服務，可讓您在雲端輕鬆啟動和擴展可靠、高效能且安全的共用檔案儲存。使用 Amazon FSx for NetApp ONTAP，您不再需要擔心設定和佈建檔案伺服器和儲存磁碟區、複寫資料、安裝和修補檔案伺服器軟體、偵測和解決硬體故障、管理容錯移轉和容錯回復，以及手動執行備份。它也提供與其他 的豐富整合 AWS 服務，例如 AWS Identity and Access Management Amazon WorkSpaces AWS Key Management Service和 AWS CloudTrail。

Amazon FSx 為您提供兩種檔案系統供您選擇：適用於 Windows 應用程式的 Amazon FSx for Windows File Server 和適用於運算密集型工作負載的 Amazon FSx for Lustre。若要進一步了解，請參閱 Amazon FSx。

AWS Managed Services 常見問答集中的 Amazon FSx for NetApp ONTAP

問：如何在我的 AMS 帳戶中請求存取 Amazon FSx for NetApp ONTAP？

透過使用 Management | AWS service | Self-visioned Service | Add (ct-1w8z66n899dct) 變更類型提交 RFC，請求存取 Amazon FSx for NetApp ONTAP。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_fsx_ontap_admin_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon FSx for NetApp ONTAP 有哪些限制？

取代 Amazon FSx for NetApp ONTAP 彈性網路介面 (ENIs) 上的安全群組需要您提交管理 | 其他 | 其他 | 更新 RFCs因為安全群組是 AMS 環境的關鍵周邊。這是唯一的限制。

問：在我的 AMS 帳戶中使用 Amazon FSx for NetApp ONTAP 的先決條件或相依性是什麼？

沒有先決條件。不過，您必須使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon FSx已安裝 。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Inspector Classic

> **Note**
>
> 支援結束通知：2026 年 5 月 20 日， AWS 將結束對 Amazon Inspector Classic 的支援。2026 年 5 月 20 日之後，您將無法再存取 Amazon Inspector Classic 主控台或 Amazon Inspector Classic 資源。Amazon Inspector Classic 將不再提供給新帳戶，以及過去六個月內尚未完成評估的帳戶。對於所有其他帳戶，存取將持續有效至 2026 年 5 月 20 日，之後您將無法再存取

Amazon Inspector Classic 主控台或 Amazon Inspector Classic 資源。如需詳細資訊，請參閱 Amazon Inspector Classic 終止支援。

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon Inspector Classic 功能。Amazon Inspector Classic 是一種自動化安全評估服務，可協助改善部署在 上的應用程式的安全性和合規性 AWS。Amazon Inspector Classic 會自動評估應用程式是否有暴露、漏洞和與最佳實務的偏差。執行評估後，Amazon Inspector Classic 會產生依嚴重性層級排定優先順序的安全調查結果詳細清單。這些調查結果可以直接檢閱，也可以作為詳細評估報告的一部分，這些報告可透過 Amazon Inspector Classic 主控台或 API 取得。若要進一步了解，請參閱 Amazon Inspector Classic。

AWS Managed Services 常見問答集中的 Amazon Inspector

問：如何在我的 AMS 帳戶中請求存取 Amazon Inspector Classic？

透過使用 管理 | AWS 服務 | 自助佈建服務 | 新增 (ct-1w8z66n899dct) 變更類型提交 RFC，請求存取 Amazon Inspector Classic。此 RFC 會將 `customer_inspector_admin_role` IAM 角色佈建至您的帳戶。此角色包含受 AWS管 AmazonInspectorFullAccess 政策。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon Inspector Classic 有哪些限制？

沒有限制。Amazon Inspector Classic 的完整功能可在您的 AMS 帳戶中使用。

問：在我的 AMS 帳戶中使用 Amazon Inspector Classic 的先決條件或相依性是什麼？

在您的 AMS 帳戶中使用 Amazon Inspector Classic 沒有先決條件或相依性。

在 AMS 中使用新的 Amazon Inspector

您現在可以在 AMS 帳戶中使用新的 Amazon Inspector。

對於 Amazon Inspector Classic，`AmazonInspectorFullAccess`需要 `customer-inspector-admin-role-ssm-inspector-agent-policy`和 。不過，SSPS 角色 已更新`customer-inspector-admin-role`，現在包含額外的 `policyAmazonInspector2FullAccess`。此新政策允許新版本 Amazon Inspector 的 API 許可。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Kendra

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon Kendra 功能。Amazon Kendra 是一種智慧型搜尋服務，使用自然語言處理和進階機器學習演算法傳回從資料搜尋問題的

特定答案。與傳統的關鍵字式搜尋不同，Amazon Kendra 會使用其語意和內容理解功能來判斷文件是否與搜尋查詢相關。Amazon Kendra 會傳回問題的特定答案，因此您的體驗即將與人類專家互動。Amazon Kendra 具有高度可擴展性，能夠滿足效能需求，與 Amazon S3 和 Amazon Lex 等 AWS 其他服務緊密整合，並提供企業級安全性。若要進一步了解，請參閱 Amazon Kendra ; 。

AWS Managed Services 常見問答集中的 Amazon Kendra

問：如何請求存取 AMS 帳戶中的 Amazon Kendra？

若要請求存取 Amazon Inspector Classic，請使用 Management | AWS service | Self-visioned Service | Add (ct-3qe6io8t6jtny) 變更類型提交 RFC。此 RFC 會將 `customer_kendra_console_role` IAM 角色佈建至您的帳戶。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon Kendra 有哪些限制？

沒有限制。Amazon Kendra 的完整功能可在您的 AMS 帳戶中使用。

問：在我的 AMS 帳戶中使用 Amazon Kendra 的先決條件或相依性是什麼？

Amazon Kendra 入門沒有先決條件或相依性。不過，根據您的特定使用案例，您可能需要存取其他 AWS 服務。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Kinesis Data Streams

使用 AMS 自助式佈建 (SSP) 模式，直接在您的 AMS 受管帳戶中存取 Amazon Kinesis Data Streams (KDS) 功能。Amazon Kinesis Data Streams 是一種高度可擴展且耐用的即時資料串流服務。KDS 可以持續從數十萬個來源擷取每秒 GB 的資料，例如網站點擊串流、資料庫事件串流、金融交易、社交媒體摘要、IT 日誌和位置追蹤事件。收集的資料以毫秒為單位提供，以啟用即時分析使用案例，例如即時儀表板、即時異常偵測、動態定價等。若要進一步了解，請參閱 Amazon Kinesis Data Streams。

AWS Managed Services 中的 Kinesis Data Streams 常見問答集

常見問題和解答：

問：如何請求存取 AMS 帳戶中的 Amazon Kinesis Data Streams？

透過使用 Management | AWS 服務 | 自助佈建服務 | 新增變更類型 (ct-1w8z66n899dct) 提交 RFC，請求存取 Amazon Kinesis Data Streams。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_kinesis_data_streaming_user_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon Kinesis Data Streams 有哪些限制？

沒有限制。Amazon Kinesis Data Streams 的完整功能可在您的 AMS 帳戶中使用。

問：在我的 AMS 帳戶中使用 Amazon Kinesis Data Streams 的先決條件或相依性是什麼？

在您的 AMS 帳戶中使用 Amazon Kinesis Data Streams 沒有先決條件或相依性。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Kinesis Video Streams

使用 AMS 自助式佈建 (SSP) 模式，直接在您的 AMS 受管帳戶中存取 Amazon Kinesis Video Streams (KVS) 功能。Amazon Kinesis Video Streams 可協助您安全地將視訊從連線裝置串流到 ， AWS 以進行分析、機器學習 (ML)、播放和其他處理。Kinesis Video Streams 會自動佈建並彈性擴展從數百萬個裝置擷取串流影片資料所需的所有基礎設施。它也會長期儲存、加密和索引串流中的影片資料，並可讓您透過easy-to-use存取資料。 APIs Kinesis Video Streams 可讓您播放影片以進行即時和隨需檢視，並透過與 Amazon Rekognition Video 整合，以及適用於 Apache MxNet、TensorFlow 和 OpenCV 等 ML 架構的程式庫，快速建置利用電腦視覺和影片分析的應用程式。若要進一步了解，請參閱 Amazon Kinesis Video Streams。

AWS Managed Services 中的 Amazon Kinesis Video Streams 常見問答集

常見問題和解答：

問：如何請求存取 AMS 帳戶中的 Amazon Kinesis Video Streams？

透過使用 Management | AWS 服務 | 自助佈建服務 | 新增變更類型 (ct-1w8z66n899dct) 提交 RFC，請求存取 Amazon Kinesis Video Streams。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_kinesis_video_streaming_user_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon Kinesis Video Streams 有哪些限制？

沒有限制。Amazon Kinesis Video Streams 的完整功能可在您的 AMS 帳戶中使用。

問：在我的 AMS 帳戶中使用 Amazon Kinesis Video Streams 的先決條件或相依性是什麼？

在您的 AMS 帳戶中使用 Amazon Kinesis Video Streams 沒有先決條件或相依性。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Lex

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon Lex 功能。Amazon Lex 是一種使用語音和文字在任何應用程式中建置對話界面的服務。Amazon Lex 提供自動語音辨識 (ASR) 的

進階深度學習功能，可將語音轉換為文字，以及自然語言理解 (NLU) 來辨識文字的意圖，讓您能夠建置具有高度吸引力使用者體驗和逼真的對話互動的應用程式。透過 Amazon Lex，任何開發人員現在可以使用支援 Amazon Alexa 的相同深度學習技術，讓您快速輕鬆地建置複雜的自然語言、對話式機器人或聊天機器人。若要進一步了解，請參閱 Amazon Lex。

AWS Managed Services 中的 Amazon Lex 常見問答集

常見問題和解答：

問：如何請求存取 AMS 帳戶中的 Amazon Lex？

透過提交管理 | AWS 服務 | 自行佈建服務 | 新增變更類型 (ct-1w8z66n899dct) 來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_lex_author_role`。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon Lex 有哪些限制？

Amazon Lex 與 Lambda 的整合僅限於沒有「AMS-」字首的 Lambda 函數，以防止對 AMS 基礎設施進行任何修改。

問：在我的 AMS 帳戶中使用 Amazon Lex 的先決條件或相依性是什麼？

在您的 AMS 帳戶中使用 Amazon Lex 沒有先決條件或相依性。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon MQ

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon MQ 功能。Amazon MQ 是 Apache ActiveMQ 的受管訊息代理程式服務，可協助您在雲端中設定和操作訊息代理程式。訊息代理程式允許不同的軟體系統，通常使用不同的程式設計語言，並在不同的平台上進行通訊和交換資訊。Amazon MQ 透過管理熱門開放原始碼訊息代理程式 ActiveMQ 的佈建、設定和維護來降低您的操作負載。將您目前的應用程式連線至 Amazon MQ 會使用業界標準 APIs和通訊協定進行傳訊，包括 JMS、NMS、AMQP、STOMP、MQTT 和 WebSocket。使用標準表示在大多數情況下，遷移到 時不需要重寫任何訊息程式碼 AWS。若要進一步了解，請參閱什麼是 Amazon MQ？

AWS Managed Services 常見問答集中的 Amazon MQ

常見問題和解答：

問：如何請求存取 AMS 帳戶中的 Amazon MQ？

在您的 AMS 帳戶中使用 Amazon MQ 是一個兩步驟的程序：

1. 佈建 Amazon MQ 中介裝置。若要這樣做，請透過 RFC 提交包含 Amazon MQ 代理程式的 CFN 範本，並使用 部署 | 擷取 | 從 CloudFormation 範本堆疊 | 建立變更類型 (ct-36cn2avfrrj9v)，或使用 管理 | 其他 | 其他 | 建立變更類型 (ct-1e1xtak34nx76) 變更類型，請求在您的帳戶中佈建 Amazon MQ 代理程式。
2. 存取 Amazon MQ 主控台。佈建 Amazon MQ 中介裝置之後，透過使用 Management | AWS service | Self-visioned service | Add change type (ct-1w8z66n899dct) 提交 RFC 來取得 Amazon MQ 主控台的存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_mq_console_role`。

在帳戶中佈建角色之後，您必須在聯合解決方案中加入該角色。

問：在我的 AMS 帳戶中使用 Amazon MQ 有哪些限制？

Amazon MQ 的完整功能可在您的 AMS 帳戶中使用；不過，由於所需的許可提高，因此無法透過政策佈建 Amazon MQ 代理程式。如需如何在帳戶中佈建 Amazon MQ 代理程式的詳細資訊，請參閱上述內容。

問：在我的 AMS 帳戶中使用 Amazon MQ 的先決條件或相依性是什麼？

在您的 AMS 帳戶中使用 Amazon MQ 沒有先決條件或相依性。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Managed Service for Apache Flink

使用 AMS 自助式服務佈建 (SSP) 模式，直接在您的 AMS 受管帳戶中存取 Amazon Managed Service for Apache Flink 功能。Managed Service for Apache Flink 是分析串流資料、取得可行洞見以及即時回應業務和客戶需求的最簡單方法。Amazon Managed Service for Apache Flink 可降低建置、管理和整合串流應用程式與其他 AWS 服務的複雜性。SQL 使用者可以輕鬆查詢串流資料，或使用 範本和互動式 SQL 編輯器建置整個串流應用程式。Java 開發人員可以使用開放原始碼 Java 程式庫和 AWS 整合快速建置複雜的串流應用程式，以即時轉換和分析資料。Amazon Managed Service for Apache Flink 會處理持續執行即時應用程式所需的一切，並自動擴展以符合傳入資料的磁碟區和輸送量。使用 Amazon Managed Service for Apache Flink，您只需為串流應用程式使用的資源付費。沒有最低費用或設定成本。若要進一步了解，請參閱 Amazon Managed Service for Apache Flink。

AWS Managed Services 常見問答集中的 Managed Service for Apache Flink

常見問題和解答：

問：如何請求存取 AMS 帳戶中的 Amazon Managed Service for Apache Flink？

透過提交管理 | AWS 服務 | 自助佈建服務 | 新增 （需要檢閱）(ct-3qe6io8t6jtny)
變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳
戶：`customer_kinesis_analytics_application_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon Managed Service for Apache Flink 有哪些限制？

- 組態僅限於沒有「AMS-」或「MC-」字首的資源，以防止對 AMS 基礎設施進行任何修改。
- 刪除或建立新的 Kinesis Data Streams 或 Firehose 的許可已從政策中移除。我們有另一個允許此動作的政策。

問：在我的 AMS 帳戶中使用 Amazon Kinesis Data Streams 的先決條件或相依性是什麼？

有幾個相依性：

- Amazon Managed Service for Apache Flink 要求在使用 Managed Service for Apache Flink 設定應用程式之前，必須先建立 Kinesis Data Streams 或 Firehose。
- 資源型政策許可應指出特定的輸入資料來源。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Managed Streaming for Apache Kafka

使用 AMS 自助式佈建 (SSP) 模式直接在您的 AMS 受管帳戶中存取 Amazon Managed Streaming for Apache Kafka (Amazon MSK) 功能。Amazon Managed Streaming for Apache Kafka 是一種全受管 AWS 串流資料服務，可讓您輕鬆地建置和執行使用 Apache Kafka 處理串流資料的應用程式，而無需成為操作 Apache Kafka 叢集的專家。Amazon MSK 會為您管理 Apache Kafka 叢集和 Apache ZooKeeper 節點的佈建、組態和維護。Amazon MSK 也會在 AWS 主控台中顯示關鍵 Apache Kafka 效能指標。

Amazon MSK 為您的 Apache Kafka 叢集提供多層安全性，包括 VPC 網路隔離、控制平面 API 授權的 AWS IAM、靜態加密、傳輸中的 TLS 加密、TLS 型憑證身分驗證、安全 SASL/SCRAM 身分驗證 AWS Secrets Manager。若要進一步了解，請參閱 Amazon MSK。

AWS Managed Services 常見問答集中的 Amazon MSK

常見問題和解答：

問：如何請求存取 AMS 帳戶中的 Amazon MSK？

透過提交管理 | AWS 服務 | 自行佈建服務 | 新增 （需要檢閱） (ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 政策和角色佈建至您的帳戶：

- `customer-msk-admin-policy.json`
- `AmazonMSKFullAccess`
- `customer-msk-admin-role.json`

在帳戶中佈建後，您必須在聯合解決方案中加入角色。

問：使用 Amazon MSK 有哪些限制？

若要讓 Amazon MSK 將代理程式日誌交付至您設定的目的地，請確定`AmazonMSKFullAccess`政策已連接至您的 IAM 角色。因此，完整存取許可已就緒。

問：使用 Amazon MSK 有哪些先決條件或相依性？

在建立 MSK 叢集之前，您必須在該 VPC 內擁有 VPC 和子網路。根據預設，AMS 在預設建立 AMS VPC 時會涵蓋此項目。

若要了解 Amazon MSK 的限制，請參閱 Amazon MSK 限制。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Managed Service for Prometheus

使用 AMS 自助式服務佈建 (SSP) 模式，直接在您的 AMS 受管帳戶中存取 Amazon Managed Service for Prometheus (AMP) 功能。Amazon Managed Service for Prometheus 是無伺服器、且與 Prometheus 相容的監控服務，適用於容器指標，可讓您更輕鬆地大規模監控容器環境。透過 Amazon Managed Service for Prometheus，您可以使用目前用來監控容器化工作負載效能的相同開放原始碼 Prometheus 資料模型和查詢語言，並享有改良的可擴展性、可用性和安全性，而無需管理基礎設施。

隨著工作負載的擴展和縮減，Amazon Managed Service for Prometheus 會自動擴展操作指標的擷取、儲存和查詢。它與 AWS 安全服務整合，以快速且安全地存取資料。如需詳細資訊，請參閱什麼是 Amazon Managed Service for Prometheus？

AWS Managed Services 常見問答集中的 Amazon Managed Service for Prometheus

常見問題和解答：

問：如何請求存取 AMS 帳戶中的 Amazon Managed Service for Prometheus？

透過提交管理 | AWS 服務 | 自行佈建服務 | 新增 （需要檢閱） (ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer-prometheus-console-role`。在帳戶中佈建之後，您必須在聯合解決方案中加入`customer-prometheus-console-role`角色。

問：在我的 AMS 帳戶中使用 Amazon Managed Service for Prometheus 有哪些限制？

支援所有功能。

問：在我的 AMS 帳戶中使用 Amazon Managed Service for Prometheus 的先決條件或相依性是什麼？

Amazon Managed Service for Prometheus 沒有先決條件或相依性。不過，根據您的特定使用案例，您可能需要存取其他 AWS 服務。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Personalize

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon Personalize 功能。Amazon Personalize 是一種機器學習服務，可讓開發人員輕鬆地使用其應用程式為客戶建立個人化建議。

機器學習越來越常用於透過提供個人化產品和內容建議、量身訂做的搜尋結果和有針對性的行銷活動來提高客戶參與度。不過，由於複雜性，開發產生這些複雜建議系統所需的機器學習功能，現在已超過大多數組織觸手可及的範圍。Amazon Personalize 可讓沒有先前機器學習經驗的開發人員輕鬆在其應用程式中建置複雜的個人化功能，使用從 Amazon.com 上多年使用的機器學習技術。

使用 Amazon Personalize，您可以從應用程式提供活動串流 – 按一下、頁面檢視、註冊、購買等 – 以及您想要建議的項目清單，例如文章、產品、影片或音樂。您也可以選擇向 Amazon Personalize 提供來自使用者的其他人口統計資訊，例如年齡或地理位置。Amazon Personalize 將處理和檢查資料、識別有意義的內容、選取正確的演算法，以及訓練和最佳化針對您的資料自訂的個人化模型。Amazon Personalize 分析的所有資料都會保持私有和安全，僅用於您的自訂建議。您可以透過簡單的 API 呼叫開始提供個人化的建議。您只需支付使用量的費用，而且沒有最低費用，也沒有預付承諾。

若要進一步了解，請參閱 Amazon Personalize。

AWS Managed Services 中的 Amazon Personalize 常見問答集

問：如何請求存取 AMS 帳戶中的 Amazon Personalize？

透過提交管理 | AWS 服務 | 自行佈建服務 | 新增 （需要檢閱） (ct-3qe6io8t6jtny) 變更類型來請求存取權，而且您需要指定要由 AWS 個人化用來產生建議的資料的 S3 儲存貯體。此

RFC 會將下列 IAM 角色佈建至您的帳戶： customer_personalize_console_role和 customer_personalize_service_role。

- 在帳戶中佈建 customer_personalize_console_role 後，您必須在聯合解決方案中加入角色。您也可以將 連接到 以外的customer_personalize_console_policy其他現有角色Customer_ReadOnly_Role。
- 將 customer_personalize_service_role 提供給您的帳戶後，您可以在建立新的資料集群組時參考其 ARN。

目前，AMS Operations 也會在您的帳戶中部署此服務角色：aws_code_pipeline_service_role_policy。

問：在我的 AMS 帳戶中使用 Amazon Personalize 有哪些限制？

Amazon Personalize 組態僅限於沒有 'ams-' 或 'mc-' 字首的資源，以防止對 AMS 基礎設施進行任何修改。

問：在我的 AMS 帳戶中使用 Amazon Personalize 有哪些先決條件或相依性？

- 如果存放資料的 S3 儲存貯體已加密，則必須提供 KMS 金鑰 ID，以便我們允許 Amazon Personalize 使用的角色解密儲存貯體。

  Amazon Personalize 不支援預設 KMS S3 金鑰。如果需要使用 KMS，請建立自訂金鑰，並透過開啟變更類型 KMS 金鑰 | Create （需要檢閱） 的 RFC 來新增下列政策：

  JSON

```
{
    "Version":"2012-10-17",
    "Id": "key-consolepolicy-3",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
                "Service": "personalize.amazonaws.com"
            },
            "Action": "kms:*",
            "Resource": "*"
        }
    ]
```

```
}
```

- 必須使用下列儲存貯體政策建立 S3 儲存貯體。透過提交變更類型為 S3 儲存 | 建立政策的 RFC 來執行此操作。此政策允許 Amazon Personalize 存取資料；該儲存貯體將包含 Amazon Personalize 要使用的資料。

  JSON

```
{
"Version":"2012-10-17",
"Id": "PersonalizeS3BucketAccessPolicy",
"Statement": [
{
"Sid": "PersonalizeS3BucketAccessPolicy",
"Effect": "Allow",
"Principal": {
"Service": "personalize.amazonaws.com"
},
"Action": [
"s3:GetObject",
"s3:ListBucket"
],
"Resource": [
"arn:aws:s3:::bucket-name",
"arn:aws:s3:::bucket-name/*"
]
}
]
}
```

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon QuickSight

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 QuickSight 功能。QuickSight 是一種快速、雲端驅動的商業智慧服務，可為您組織中的每個人提供洞見。作為全受管服務，QuickSight 可讓您輕鬆建立和發佈互動式儀表板，其中包含機器學習 (ML) 洞見。若要進一步了解，請參閱 Amazon QuickSight。

AWS Managed Services 中的 QuickSight 常見問答集

常見問題和解答：

問：如何請求存取 AMS 帳戶中的 QuickSight？

透過提交管理 | AWS 服務 | 自行佈建服務 | 新增變更類型 (ct-1w8z66n899dct) 來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_quicksight_console_admin_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 QuickSight 有哪些限制？

- AWS 由於 IAM 政策相依性，您將無法存取 QuickSight 上的資源設定。不過，AMS 團隊會為您啟用每個資源，以回應啟用服務的請求。
- 此模型不支援個別使用者和群組的資源存取，因為此功能可讓使用者修改可能影響 AMS 基礎設施的 IAM 許可。
- 由於變更 IAM 物件涉及風險，因此不支援從 QuickSight 中邀請 IAM 身分的功能。
- QuickSight 服務提供兩種版本：Enterprise 和 Standard。兩者都提供 AMS 上支援的單一登入 (SSO) 選項。不過，Enterprise Edition 可以選擇將 QuickSight 與 Active Directory (AD) 整合。AMS 上的 QuickSight 不支援與 AD 整合，因為 AMS 帳戶結構與 QuickSight 信任要求之間不相容。

問：在我的 AMS 帳戶中使用 QuickSight 的先決條件或相依性是什麼？

- 當 AMS 收到此 RFC 以新增 QuickSight 時，系統會傳送服務請求給您以取得其他資訊；請提供下列項目：
  - QuickSight 帳戶名稱（例如，*CustomerName*-quicksight
  - QuickSight 版本 (Standard 與 Enterprise)
  - 要啟用 QuickSight 服務 AWS 的區域（預設為您的 AMS AWS 區域）。
  - QuickSight 帳戶的通知電子郵件地址。
  - （選用）要分析的資料檔案所在的 S3 儲存貯體。
  - 連線至 QuickSight 的 VPC 和子網路 IDs 支援新增 VPC 連線的功能，可啟用 QuickSight 與帳戶內部資源之間的私有連線。

AMS 運算子會代表您執行註冊程序，並設定兩個 QuickSight 功能：

- 自動探索資料來源。
- VPC 連線。

> **Note**
>
> 這些動作必須由 AMS 運算子執行，因為在登入過程中需要更高的 IAM 和 VPC 許可。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Rekognition

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon Rekognition 功能。Amazon Rekognition 可讓您使用經過驗證、可擴展性高的深度學習技術，輕鬆地將映像和影片分析新增至應用程式，無需機器學習專業知識。使用 Amazon Rekognition，您可以識別影像和影片中的物件、人物、文字、場景和活動，以及偵測任何不適當的內容。Amazon Rekognition 還提供高度準確的臉部分析和臉部搜尋功能，可用於偵測、分析和比較各種使用者驗證、人員計數和公共安全使用案例的臉部。

透過 Amazon Rekognition 自訂標籤，您可以在影像中識別特定於您業務需求的物件和場景。例如，您可以建置模型來分類組裝線上的特定機器組件，或偵測運作狀態不佳的植物。Amazon Rekognition 自訂標籤會為您處理模型開發繁重的工作，因此不需要機器學習體驗。您只需要提供您要識別的物件或場景的影像，而服務會處理其餘項目。

若要進一步了解，請參閱 Amazon Rekognition。

AWS Managed Services 常見問答集中的 Amazon Rekognition

常見問題和解答：

問：如何請求存取 AMS 帳戶中的 Amazon Rekognition？

透過提交管理 | AWS 服務 | 自助佈建服務 | 新增 （需要檢閱） (ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_rekognition_console_role` & `customer_rekognition_service_role`。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon Rekognition 有哪些限制？

Amazon Rekognition 的完整功能可供 Amazon Rekognition 自行佈建服務角色使用。

問：在我的 AMS 帳戶中使用 Amazon Rekognition 有哪些先決條件或相依性？

如果您使用 Kinesis Video Streams 為 Amazon Rekognition Video 串流處理器或資料串流提供來源串流影片，做為將資料寫入 Kinesis Data Streams 的目的地，請在建立 RFC `kinesisStreamName`時為 AMS 提供 。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon SageMaker AI

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon SageMaker AI 功能。SageMaker AI 可讓每位開發人員和資料科學家快速建置、訓練和部署機器學習模型。Amazon SageMaker AI 是一項全受管服務，涵蓋整個機器學習工作流程，以標記和準備您的資料、選擇演算法、訓練模型、調校和最佳化部署、進行預測，以及採取動作。您的模型可以更快地進入生產環境，同時更少的精力和更低的成本。若要進一步了解，請參閱 Amazon SageMaker AI。

AWS Managed Services 常見問答集中的 SageMaker AI

常見問題和解答：

問：如何請求存取 AMS 帳戶中的 SageMaker AI？

透過提交管理 | AWS 服務 | 自行佈建服務 | 新增 (ct-1w8z66n899dct) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶： `customer_sagemaker_admin_role` 和服務角色 `AmazonSageMaker-ExecutionRole-Admin`。在您的帳戶中佈建 SageMaker AI 之後，您必須在聯合解決方案中加入`customer_sagemaker_admin_role`角色。您無法直接存取服務角色；SageMaker AI 服務會在執行各種動作時使用它，如下所述：傳遞角色。

問：在我的 AMS 帳戶中使用 SageMaker AI 有哪些限制？

- AMS Amazon SageMaker AI IAM 角色不支援下列使用案例：
  - 目前不支援 SageMaker AI Studio。
  - 不支援 SageMaker AI Ground Truth 來管理私有人力資源，因為此功能需要對 Amazon Cognito 資源的過度允許存取。如果需要管理私有人力資源，您可以請求具有合併 SageMaker AI 和 Amazon Cognito 許可的自訂 IAM 角色。否則，我們建議您使用公有人力資源 （ 由 Amazon Mechanical Turk 提供支援 ） 或 AWS Marketplace 服務供應商進行資料標記。
- 建立 VPC 端點以支援對 SageMaker AI 服務的 API 呼叫 (aws.sagemaker.{region}.notebook、com.amazonaws.{region}.sagemaker.api 和 com.amazonaws.{region}.sagemaker.runtime)，因為許可範圍不能僅限於 SageMaker AI 相關服務。若要支援此使用案例，請提交管理 | 其他 | 其他 RFC 以建立相關的 VPC 端點。
- 不支援 SageMaker AI 端點自動擴展，因為 SageMaker AI 需要任何 ("*") 資源的`DeleteAlarm`許可。若要支援端點自動擴展，請提交管理 | 其他 | 其他 RFC 來設定 SageMaker AI 端點的自動擴展。

問：在我的 AMS 帳戶中使用 SageMaker AI 的先決條件或相依性是什麼？

- 下列使用案例在使用前需要特殊組態：
  - 如果 S3 儲存貯體將用於存放模型成品和資料，則您必須使用部署 | 進階堆疊元件 | S3 儲存 | 建立 RFC，請求名為 且具有必要關鍵字 ("SageMaker"、"Sagemaker"、"sagemaker" 或 "aws-glue") 的 S3 儲存貯體。
  - 如果將使用彈性檔案存放區 (EFS)，則必須在相同的子網路中設定 EFS 儲存，並由安全群組允許。
  - 如果其他資源需要直接存取 SageMaker AI 服務 （筆記本、API、執行時間等），則必須由下列人員請求組態：
    - 提交 RFC 以建立端點的安全群組 （部署 | 進階堆疊元件 | 安全群組 | 建立 （自動））。
    - 提交管理 | 其他 | 其他 | 建立 RFC 以設定相關的 VPC 端點。

問： **customer_sagemaker_admin_role**可以直接存取的資源支援哪些命名慣例？ （以下用於更新和刪除許可；如果您需要其他支援的 資源命名慣例，請聯絡 AMS Cloud Architect 進行諮詢。）

- 資源：傳遞`AmazonSageMaker-ExecutionRole-*`角色
  - 許可：SageMaker AI 自我佈建服務角色支援搭配 AWS Glue AWS RoboMaker和 使用 SageMaker AI 服務角色 (`AmazonSageMaker-ExecutionRole-*`) AWS Step Functions。
- 資源：Secrets Manager 上的 AWS 秘密
  - 許可：使用`AmazonSageMaker-*`字首描述、建立、取得、更新秘密。
  - 許可：描述，當`SageMaker`資源標籤設定為 時取得秘密`true`。
- 資源： 上的儲存庫 AWS CodeCommit
  - 許可：建立/刪除字`AmazonSageMaker-*`首為 的儲存庫。
  - 許可：在具有下列字首 、 `*sagemaker**SageMaker*`和 的儲存庫上提取/推送 Git`*Sagemaker*`。
- 資源：Amazon ECR (Amazon Elastic Container Registry) 儲存庫
  - 許可：許可：使用下列資源命名慣例 時，設定、刪除儲存庫政策並上傳容器映像`*sagemaker*`。
- 資源：Amazon S3 儲存貯體
  - 許可：當資源具有下列字首時，取得、放置`*Sagemaker*`、刪除物件、中止分段上傳 S3 物件：`*SageMaker*`、 `*sagemaker*`和 `aws-glue`。
  - 許可：當`SageMaker`標籤設定為 時取得 S3 物件`true`。
- 資源：Amazon CloudWatch Log Group
  - 許可：建立日誌群組或串流、放置日誌事件、列出、更新、建立、刪除具有下列字首的日誌交付：`/aws/sagemaker/*`。

- 資源：Amazon CloudWatch 指標
  - 許可：使用下列字首時放置指標資料：AWS/SageMaker、AWS/SageMaker/、aws/SageMaker、aws/SageMaker/、aws/sagemaker、 aws/sagemaker/和 /aws/sagemaker/.。
- 資源：Amazon CloudWatch Dashboard
  - 許可：使用下列字首時建立/刪除儀表板：customer_*。
- 資源：Amazon SNS （簡易通知服務） 主題
  - 許可：使用下列字首時訂閱/建立主題：*SageMaker*、 *sagemaker*和 *Sagemaker*。

問： **AmazonSageMakerFullAccess**和 之間的差異是什麼**customer_sagemaker_admin_role**？

customer_sagemaker_admin_role 搭配 的 customer_sagemaker_admin_policy提供幾乎與 AmazonSageMakerFullAccess 相同的許可，除了：

- 與 AWS RoboMaker、Amazon Cognito 和資源連線的許可 AWS Glue 。
- SageMaker AI 端點自動擴展。您必須提交 RFC 與管理 | 進階堆疊元件 | Identity and Access Management (IAM) | 更新實體或政策 （需要檢閱） 變更類型 (ct-27tuth19k52b4)，以暫時或永久提升自動擴展許可，因為自動擴展需要在 CloudWatch 服務上進行寬鬆存取。

問：如何在靜態資料加密中採用 AWS KMS 客戶受管金鑰？

您必須確保金鑰政策已在客戶受管金鑰上正確設定，以便相關的 IAM 使用者或角色可以使用金鑰。如需詳細資訊，請參閱AWS KMS 金鑰政策文件。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Simple Email Service

使用 AMS 自助式佈建 (SSP) 模式，直接在您的 AMS 受管帳戶中存取 Amazon Simple Email Service (Amazon SES) 功能。Amazon Simple Email Service 是一種雲端電子郵件傳送服務，旨在協助數位行銷人員和應用程式開發人員、傳送行銷、通知和交易電子郵件。

您可以使用 SMTP 界面或其中一個 AWS SDKs，將 Amazon SES 直接整合到現有的應用程式。您也可以將 Amazon SES 的電子郵件傳送功能整合至您已使用的軟體，例如票證系統和電子郵件用戶端。

若要進一步了解，請參閱 Amazon Simple Email Service。

AWS Managed Services 常見問答集中的 Amazon SES

問：如何請求存取 AMS 帳戶中的 Amazon SES？

透過使用 Management | AWS 服務 | 自助佈建服務 | 新增 (ct-1w8z66n899dct) 變更類型提交 RFC，請求存取 Amazon SES。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_ses_admin_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon SES 的先決條件或相依性是什麼？

- 您必須設定 S3 儲存貯體政策，以允許 Amazon SES 將事件發佈至儲存貯體。
- 您必須使用預設 (AWS SES) 或設定 CMK 金鑰，以允許 Amazon SES 加密電子郵件，並將事件推送至屬於帳戶的其他服務資源，例如 Amazon S3、Amazon SNS、Lambda 和 Firehose。

問：在我的 AMS 帳戶中使用 Amazon SES 有哪些限制？

您必須提出 RFCs才能建立下列資源：

- 具有 PutEvents 許可的 SMTP 使用者和 IAM 服務角色，傳送至 Kinesis Firehose 串流。
- 您必須使用 AMS 變更類型建立新的 AWS 資源，例如 S3 儲存貯體、Firehose 串流、SNS 主題，Amazon SES 規則和組態集的目的地才能使用這些資源。
- SMTP 登入資料。若要請求新的 SMTP 登入資料，請使用變更類型 （ 管理 | 其他 | 其他 | 建立 ）。AMS 會建立登入資料，並將其新增至 Secrets Manager。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Simple Workflow Service

使用 AMS 自助式佈建 (SSP) 模式，直接在您的 AMS 受管帳戶中存取 Amazon Simple Workflow Service (Amazon SWF) 功能。Amazon Simple Workflow Service 可協助開發人員建置、執行和擴展具有平行或循序步驟的背景任務。您可以在 雲端中將 Amazon SWF 視為全受管狀態追蹤器和任務協調器。如果您應用程式的步驟需要超過 500 毫秒才能完成，您需要追蹤處理狀態，或者如果任務失敗，則需要復原或重試，Amazon SWF 可以為您提供協助。若要進一步了解，請參閱 Amazon Simple Workflow Service。

AWS Managed Services 常見問答集中的 Amazon SWF

常見問題和解答：

問：如何請求存取 AMS 帳戶中的 Amazon SWF？

透過提交管理 | AWS 服務 | 自行佈建服務 | 新增變更類型 (ct-1w8z66n899dct) 來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_swf_role`。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon SWF 有哪些限制？

Lambda `InvokeFunction`許可已包含在此服務中，但新增至所有 AMS 客戶角色`customer_deny_policy`的 AMS 明確拒絕存取 AMS Lambda 函數和 AMS 擁有的資源。若要標記或取消標記 Amazon SWF 中的資源，請提交管理 | 其他 | 其他變更類型。

問：在我的 AMS 帳戶中使用 Amazon SWF 的先決條件或相依性是什麼？

Amazon SWF 取決於 AWS Lambda 服務，因此，已提供叫用 Lambda 的許可做為此角色的一部分，而且從 Amazon SWF 叫用 Lambda 不需要額外的許可。否則，使用 Amazon SWF 沒有先決條件。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Textract

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon Textract 功能。Amazon Textract 是一項全受管的機器學習服務，可自動從掃描文件中擷取列印的文字、手寫和其他資料，這些文件超出簡易光學字元辨識 (OCR)，以識別、了解並從表單和資料表擷取資料。若要進一步了解，請參閱 Amazon Textract。

AWS Managed Services 常見問答集中的 Amazon Textract

常見問題和解答：

問：如何請求在我的 AMS 帳戶中設定 Amazon Textract？

透過提交管理 | AWS 服務 | 自助佈建服務 | 新增 （需要檢閱） (ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_textract_human_review_execution_role`、`customer_textract_console_role`和 `customer_ec2_textract_instance_profile`。在帳戶中佈建後，您必須在聯合解決方案`customer_textract_console_role`中加入角色。

問：在我的 AMS 帳戶中使用 Amazon Textract 有哪些限制？

在您的 AMS 帳戶中使用 Amazon Textract 沒有限制。

問：在我的 AMS 帳戶中使用 Amazon Textract 有哪些先決條件或相依性？

您必須提交 RFC 部署 | 進階堆疊元件 |S3 儲存 | 建立 (ct-1a68ck03fn98r) 來請求建立 S3 儲存貯體。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Transcribe

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon Transcribe 功能。Amazon Transcribe 是一種全受管且持續訓練的自動語音辨識服務，可從音訊檔案自動產生時間戳記的文字文字

記錄。Amazon Transcribe 可讓開發人員輕鬆地將speech-to-text功能新增至其應用程式。音訊資料幾乎無法讓電腦搜尋和分析。因此，錄製的語音需要轉換為文字，才能用於應用程式。從歷史上來看，客戶必須與轉錄供應商合作，這些供應商需要他們簽署昂貴的合約，並且很難整合到他們的技術堆疊中來完成此任務。其中許多供應商使用過時的技術無法很好地適應不同的案例，例如聯絡中心中常見的低保真電話音訊，這會導致準確性不佳。

Amazon Transcribe 使用稱為自動語音辨識 (ASR) 的深度學習程序，快速且準確地將語音轉換為文字。Amazon Transcribe 可用來轉錄客戶服務呼叫、自動化隱藏式字幕和字幕，以及產生媒體資產的中繼資料，以建立可完全搜尋的封存。您可以使用 Amazon Transcribe Medical 將醫療speech-to-text功能新增至臨床文件應用程式。若要進一步了解，請參閱 Amazon Transcribe。

AWS Managed Services 常見問答集中的 Amazon Transcribe

常見問題和解答：

問：如何請求在我的 AMS 帳戶中設定 Amazon Transcribe？

透過提交管理 | AWS 服務 | 自助佈建服務 | 新增 （需要檢閱） (ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_transcribe_role`。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon Transcribe 有哪些限制？

除非 RA 和 另有指定，否則在使用轉錄時，您必須使用 'customer-transcribe*' 做為儲存貯體的字首。

您無法在 Amazon 轉錄中建立 IAM 角色。

您無法針對預設 SSPS 中的輸出資料使用服務受管 S3 儲存貯體 （如有需要，請聯絡您的 帳戶 CA)。

如果您想要使用不屬於 AMS 命名空間的客戶受管 KMS 金鑰，則必須提交風險接受。

問：在我的 AMS 帳戶中使用 Amazon Transcribe 有哪些先決條件或相依性？

S3 必須能夠存取名稱為 'customer-transcribe*' 的儲存貯體。如果您的 S3 儲存貯體使用 KMS 金鑰加密，則需要 KMS 才能使用 Amazon Transcribe。如果儲存貯體不需要加密，則可以移除「KMStranscribeAllow」。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon WorkSpaces

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 WorkSpaces 功能。WorkSpaces 可讓您為使用者佈建以雲端為基礎的虛擬 Microsoft Windows 或 Amazon Linux 桌面，稱為

WorkSpaces。WorkSpaces 無需採購和部署硬體或安裝複雜軟體。您可以在需求變更時快速新增或移除使用者。使用者從支援的裝置使用用戶端應用程式，或針對 Windows WorkSpaces 使用 Web 瀏覽器來存取其 WorkSpaces，並使用其現有的內部部署 Active Directory (AD) 登入資料來登入。WorkSpaces

若要進一步了解，請參閱 Amazon WorkSpaces。

AWS Managed Services 常見問答集中的 WorkSpaces

常見問題和解答：

問：如何請求存取 AMS 帳戶中的 WorkSpaces？

透過提交管理 | AWS 服務 | 自助佈建服務 | 新增 （需要檢閱） (ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_workspaces_console_role`。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 WorkSpaces 有哪些限制？

Amazon WorkSpaces 自我佈建服務角色提供工作區的完整功能。

問：在我的 AMS 帳戶中使用 WorkSpaces 的先決條件或相依性是什麼？

- WorkSpaces 受限於 AWS 區域；因此，AD Connector 必須在託管 WorkSpaces 執行個體 AWS 的相同區域中設定。

  客戶可以使用下列兩種方法之一，將 WorkSpaces 連線至客戶 AD：

  1. 使用 AD 連接器將身分驗證代理到內部部署 Active Directory 服務 （偏好）：

     在整合 WorkSpaces 執行個體與內部部署目錄服務之前，在您的 AMS 帳戶中設定 Active Directory (AD) Connector。AD Connector 可做為現有 AD 使用者 （來自您的網域） 的代理，以使用現有的內部部署 AD 登入資料連線至 WorkSpaces。這是偏好的做法，因為 WorkSpaces 會直接加入客戶的內部部署網域，同時充當資源和使用者樹系，進而在客戶端獲得更多控制。

     如需詳細資訊，請參閱部署 Amazon WorkSpaces 的最佳實務 （案例 1)。
  2. 搭配使用 AD Connector 與 AWS Microsoft AD、共用服務 VPC，以及對內部部署的單向信任：

     您也可以先建立從 AMS 受管 AD 到內部部署 AD 的單向傳出信任，以使用內部部署目錄驗證使用者。WorkSpaces 將使用 AD Connector 加入 AMS 受管 AD。然後，WorkSpaces 存取許可將透過 AMS 受管 AD 委派給 WorkSpaces 執行個體，而無需與您的內部部署環境建立雙向信任。在此案例中，使用者樹系將位於客戶 AD 中，而資源樹系將位於 AMS 受管 AD 中 （可透過 RFC 請

求對 AMS 受管 AD 的變更）。請注意，WorkSpaces VPC 與執行 AMS 受管 AD 的 MALZ 共用服務 VPC 之間的連線是透過 Transit Gateway 建立。

如需詳細資訊，請參閱部署 Amazon WorkSpaces 的最佳實務（案例 6)。

> **Note**
>
> AD Connector 可以透過提交具有必要 AD 組態詳細資訊的管理 | 其他 | 其他 | 建立變更類型 RFC 來進行設定；如需詳細資訊，請參閱建立 AD Connector。如果方法 2 用於在 AMS 受管 AD 中建立資源樹系，請執行 AMS 受管 AD，在 AMS 共用服務帳戶中提交另一個管理 | 其他 | 建立變更類型 RFC。

使用 AMS SSP 在您的 AMS 帳戶中佈建 AMS Code 服務

使用 AMS 自助式服務佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 AMS Code 服務功能。AMS Code 服務是 AWS 程式碼管理服務的專屬綁定，如下所示。您可以選擇使用 AMS Code 服務在 AMS 中部署所有服務，也可以在 AMS 中個別部署。

AMS Code 服務包含下列服務：

- AWS CodeCommit：全受管來源控制服務，可託管安全的 Git 型儲存庫。它讓團隊可以在安全且高度可擴展的生態系統中協作程式碼。CodeCommit 無需操作您自己的來源控制系統或擔心擴展其基礎設施。您可以使用 CodeCommit 安全地存放從原始程式碼到二進位檔的任何內容，並與您現有的 Git 工具無縫搭配使用。如需進一步了解，請參閱 AWS CodeCommit

  若要在獨立於 AMS Code 服務的 AMS 帳戶中部署此項目，請參閱 使用 AMS SSP AWS CodeCommit 在您的 AMS 帳戶中佈建。
- AWS CodeBuild：全受管持續整合服務，可編譯原始程式碼、執行測試，並產生準備好部署的軟體套件。使用 CodeBuild，您便不必佈建、管理、擴展自己的組建伺服器。CodeBuild 會持續擴展並同時處理多個組建，所以您的組建不必排入佇列中等候。您可以利用預先封裝好的組建環境立即開始使用，或是建立自訂的組建環境來使用您自己的組建工具。使用 CodeBuild 時，將依據您使用運算資源的分鐘數計費。如需進一步了解，請參閱 AWS CodeBuild

  若要在獨立於 AMS Code 服務的 AMS 帳戶中部署此項目，請參閱 使用 AMS SSP AWS CodeBuild 在您的 AMS 帳戶中佈建。
- AWS CodeDeploy：全受管部署服務，可將軟體部署自動化至各種運算服務，例如 Amazon EC2 和您的內部部署伺服器。 AWS CodeDeploy 可協助您快速發行新功能，協助您避免在應用程式部署期

間停機，並處理更新應用程式的複雜性。您可以使用 AWS CodeDeploy 來自動化軟體部署，無需容易出錯的手動操作。服務會擴展以符合您的部署需求。如需進一步了解，請參閱 AWS CodeDeploy

若要在獨立於 AMS Code 服務的 AMS 帳戶中部署此項目，請參閱 使用 AMS SSP AWS CodeDeploy 在您的 AMS 帳戶中佈建。

- AWS CodePipeline：全受管持續交付服務，可協助您自動化發行管道，以實現快速可靠的應用程式和基礎設施更新。根據您定義的發行模型，CodePipeline 可以自動在每次程式碼變更時建置、測試和部署程式碼。這可讓您快速且可靠地交付功能和更新。您可以輕鬆地 AWS CodePipeline 與第三方服務整合，例如 GitHub 或您自己的自訂外掛程式。使用 時 AWS CodePipeline，您只需支付使用量的費用。沒有預付費用，也無需長期承諾。如需進一步了解，請參閱 AWS CodePipeline

  若要在獨立於 AMS Code 服務的 AMS 帳戶中部署此項目，請參閱 使用 AMS SSP AWS CodePipeline 在您的 AMS 帳戶中佈建。

AWS Managed Services 常見問答集中的 AMS 程式碼服務

問：如何請求存取 AMS 帳戶中的 AMS Code 服務？

透過提交管理 | AWS 服務 | 自助佈建服務 | 新增 （需要檢閱） (ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_code_suite_console_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。此時，AMS Operations 也會在您的帳戶中部署 CodeBuild`customer_codebuild_service_role`、CodeDeploy 和 CodePipeline `customer_codedeploy_service_role`、`aws_code_pipeline_service_role`服務的 、 服務角色。如果需要 的其他 IAM 許可`customer_codebuild_service_role`，請提交 AMS 服務請求。

> **Note**
>
> 您也可以個別新增這些服務；如需相關資訊使用 AMS SSP AWS CodePipeline 在您的 AMS 帳戶中佈建，請分別參閱 使用 AMS SSP AWS CodeBuild 在您的 AMS 帳戶中佈建使用 AMS SSP AWS CodeDeploy 在您的 AMS 帳戶中佈建、 和 。

問：在我的 AMS 帳戶中使用 AMS Code 服務有哪些限制？

- AWS CodeCommit：CodeCommit 上的觸發功能會因為建立 SNS 主題的相關權限而停用。針對 CodeCommit 的直接驗證受到限制；使用者應該使用登入資料協助程式進行驗證。有些 KMS 命令也會受到限制： kms:Encrypt、 kms:Decrypt、 kms:ReEncrypt、 kms:GenereteDataKey、 kms:GenerateDataKeyWithoutPlaintext 和 kms:DescribeKey。

- CodeBuild：對於 AWS CodeBuild 主控台管理員存取，許可在資源層級受到限制；例如，CloudWatch 動作在特定資源上受到限制，且`iam:PassRole`許可受到控制。
- CodeDeploy：目前 CodeDeploy 僅支援在 Amazon EC2/內部部署部署。不支援透過 CodeDeploy 在 ECS 和 Lambda 上部署。
- CodePipeline：CodePipeline 功能、階段和提供者僅限於下列項目：
  - 部署階段：Amazon S3 和 AWS CodeDeploy
  - 來源階段：Amazon S3 AWS CodeCommit、Bit 儲存貯體和 GitHub
  - 組建階段： AWS CodeBuild 和 Jenkins
  - 核准階段：Amazon SNS
  - 測試階段： AWS CodeBuild、Jenkins、BlazeMeter、Ghost Inspector UI 測試、Micro Focus StormRunner Load、Runscope API 監控
  - 調用階段：Step Functions 和 Lambda

> **Note**
>
> AMS Operations 會在您的帳戶`customer_code_pipeline_lambda_policy`中部署 ；它必須與 Lambda 叫用階段的 Lambda 執行角色連接。提供您要新增此政策的 Lambda 服務/執行角色名稱。如果沒有自訂 Lambda 服務/執行角色，則 AMS 會建立名為 的新角色`customer_code_pipeline_lambda_execution_role`，這是 `customer_lambda_basic_execution_role`與 的複本`customer_code_pipeline_lambda_policy`。

問：在我的 AMS 帳戶中使用 AMS Code 服務的先決條件或相依性是什麼？

- CodeCommit：如果 S3 儲存貯體使用 AWS KMS 金鑰加密， AWS KMS 則需要 S3 和 才能使用 AWS CodeCommit。
- CodeBuild：如果定義的 AWS CodeBuild 服務角色需要額外的 IAM 許可，請透過 AMS 服務請求請求它們。
- CodeDeploy：無。
- CodePipeline：None. AWS supported 服務—AWS CodeCommit、 AWS CodeBuild、 AWS CodeDeploy—必須在啟動 CodePipeline 之前啟動，或與 CodePipeline 一起啟動。不過，這由 AMS 工程師完成。

使用 AMS SSP AWS Amplify 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Amplify 的功能。 AWS Amplify 是完整的解決方案，可讓前端 Web 和行動開發人員輕鬆建置、連線和託管完整堆疊應用程式。Amplify 提供彈性，可隨著使用案例的演進而利用 AWS 服務的廣度。Amplify 提供建置完整堆疊 iOS、Android、Flutter、Web 和 React Native 應用程式的產品。如需詳細資訊，請參閱 AWS Amplify。

AWS Amplify 在 AWS Managed Services 常見問答集中

常見問題和解答：

問：如何 AWS Amplify 請求在我的 AMS 帳戶中設定 ？

透過提交管理 | AWS 服務 | 自助佈建服務 | 新增 （需要檢閱） (ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_amplify_console_role`。佈建至您的帳戶後，您必須在聯合解決方案中加入該角色。

此外，您必須提供風險接受，因為 AWS Amplify 具有基礎設施變更許可。若要這樣做，請使用您的 Cloud Service Delivery Manager (CSDM)。

問： AWS Amplify 在我的 AMS 帳戶中使用 有哪些限制？

除非 RA 和 另有指定，否則在使用 Amplify 時，您必須使用 `'amplify*'`做為儲存貯體的字首。

問： AWS Amplify 在我的 AMS 帳戶中使用 的先決條件或相依性是什麼？

AWS Amplify 在您的 AMS 帳戶中使用 沒有先決條件。

僅限 Malz 環境：Amplify 的預設加入角色為「customer_amplify_console_role」。若要使用自訂角色，請先部署 IAM 實體。然後，建立額外的 RFC，將您的自訂角色新增至應用程式帳戶允許清單的服務控制政策。

使用 AMS SSP 佈建 AWS AppSync

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS AppSync 的功能。 可讓您建立彈性 API 來安全地存取、操作和合併來自一或多個資料來源的資料，以 AWS AppSync 簡化應用程式開發。 AWS AppSync 是一種受管服務，可使用 GraphQL 讓應用程式輕鬆取得他們所需的資料。

透過 AWS AppSync，您可以在 NoSQL 資料存放區、關聯式資料庫、HTTP APIs 和自訂資料來源等各種資料來源上建置可擴展的應用程式，包括需要即時更新的應用程式 AWS Lambda。對於行動和 Web

應用程式， AWS AppSync 還會在裝置離線時提供本機資料存取，並在恢復上線時提供與可自訂衝突解決方案的資料同步。如需詳細資訊，請參閱 AWS AppSync。

AWS AppSync 在 AWS Managed Services 常見問答集中

常見問題和解答：

問：如何在我的 AMS AWS AppSync 帳戶中請求存取權？

透過提交管理 | AWS 服務 | 自行佈建服務 | 新增變更類型 (ct-1w8z66n899dct) 來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶： `customer_appsync_service_role`和 `customer_appsync_author_role`。在帳戶中佈建後，您必須在聯合解決方案`customer_appsync_author_role`中加入 。

問：使用 有哪些限制 AWS AppSync？

- 在 AppSync 上建立資料來源時，客戶需要指定先前建立的服務角色，不允許建立新角色，因此將傳回拒絕存取
- AppSync 角色設定為將許可限制為包含「AMS-」或「MC-」字首的資源，以防止對 AMS 基礎設施進行任何修改。

問：要使用哪些先決條件或相依性 AWS AppSync？

此服務允許將多個其他 服務用作資料來源，使用它們的基本許可包含在服務角色 (`customer_appsync_service_role`) 中，但您必須在使用服務時手動選取服務角色。

使用 AMS SSP AWS App Mesh 在您的 AMS 帳戶中佈建

使用 AMS 自助式服務佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS App Mesh 的功能。 AWS App Mesh 提供應用程式層級聯網，讓您的服務可以輕鬆地跨多種類型的運算基礎設施彼此通訊。App Mesh 會標準化您的服務通訊方式，為您提供end-to-end可見性，並確保應用程式的高可用性。

AWS App Mesh 透過為跨多種運算基礎設施建置的服務提供一致的可見性和網路流量控制，讓您輕鬆執行服務。App Mesh 不需要更新應用程式程式碼，即可變更監控資料的收集方式或在服務之間路由流量的方式。App Mesh 會設定每個服務以匯出監控資料，並跨應用程式實作一致的通訊控制邏輯。這可讓您輕鬆地快速找出錯誤的確切位置，並在發生故障或需要部署程式碼變更時自動重新路由網路流量。如需詳細資訊，請參閱 AWS App Mesh。

AWS App Mesh AWS Managed Services 常見問答集中的

常見問題和解答：

問：如何在我的 AMS AWS App Mesh 帳戶中請求存取權？

透過提交管理 | AWS 服務 | 自行佈建服務 | 新增變更類型 (ct-1w8z66n899dct) 來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_app_mesh_console_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：使用 有哪些限制 AWS App Mesh？

完整功能 AWS App Mesh 可在您的 AMS 帳戶中使用。

問：要使用哪些先決條件或相依性 AWS App Mesh？

AWS App Mesh 您的 AMS 帳戶中沒有要使用的先決條件或相依性。

使用 AMS SSP AWS Audit Manager 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Audit Manager 功能。Audit Manager 可協助您持續稽核 AWS 用量，以簡化您評估風險的方式，以及是否符合法規和業界標準。Audit Manager 會自動化證據收集，讓您更容易評定您的政策、程序和活動是否有效運作。進行稽核時，Audit Manager 可協助您管理控制項的利益相關者審查，並協助您以大幅減少手動作業的方式建立稽核就緒的報告。若要進一步了解，請參閱 Audit Manager。

AWS Audit Manager 在 AWS Managed Services 常見問答集中

常見問題和解答：

問：如何請求存取 AMS 帳戶中 AWS Audit Manager 的 ？

您可以透過提交 AWS 服務 RFC 管理 | AWS 服務 | 自助佈建服務 | 新增 （需要檢閱） (ct-3qe6io8t6jtny) 來請求存取權。此 RFC 會在您的帳戶中佈建下列 IAM 角色：`customer-audit-manager-admin-Role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：使用 有哪些限制 AWS Audit Manager？

AWS Audit Manager 在您的 AMS 帳戶中使用 沒有限制。 AWS Audit Manager 提供 的完整功能。

問：要使用哪些先決條件或相依性 AWS Audit Manager？

1. 您需要將您希望報告/評估所在的 s3 儲存貯體提供給 AMS。
2. 如果您想要使用 服務進行加密，您需要向 AMS 提供要使用的 KMS CMK ARN。

3. 如果您想要將 SNS 通知傳送至主題，您必須提供主題的名稱或 arn。
4. （選用）如果您想要在 Audit Manager 中啟用 Organizations 做為多帳戶登陸區域的一部分，並且想要委派管理員帳戶，則需要額外的先決條件：在 RFC （管理 | AWS 服務 | 相容服務 | 新增）的描述欄位中，提及您想要在 Audit Manager 設定中使用委派管理員帳戶，並提供下列詳細資訊：
   - KMS CMK ARN （最初用於設定 Audit Manager)
   - 做為此多帳戶登陸區域一部分的 Audit Manager 委派管理員帳戶 ID （可以是 MALZ 應用程式帳戶）

使用 AMS SSP AWS Batch 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Batch 的功能。 AWS Batch 可讓開發人員、科學家和工程師輕鬆有效地執行數十萬個批次運算任務 AWS。 會根據所提交批次任務的磁碟區和特定資源需求， AWS Batch 動態佈建最佳數量和類型的運算資源 （例如 CPU 或記憶體最佳化執行個體）。使用 AWS Batch，您不需要安裝和管理用於執行任務的批次運算軟體或伺服器叢集，讓您專注於分析結果和解決問題。如需詳細資訊，請參閱 AWS Batch。

AWS Batch 在 AWS Managed Services 常見問答集中

常見問題和解答：

問：如何請求存取 AMS 帳戶中 AWS Batch 的 ？

1. 若要請求存取 AWS Batch，請提交 RFC 管理 | AWS 服務 | 自助佈建服務 | 新增 (ct-1w8z66n899dct)。此 RFC 會在您的帳戶中佈建下列 IAM 角色和政策：

IAM 角色：

- `customer_batch_console_role`
- `customer_batch_ecs_instance_role`
- `customer_batch_events_service_role`
- `customer_batch_service_role`
- `customer_batch_ecs_task_role`

政策：

- `customer_batch_console_role_policy`
- `customer_batch_service_role_policy`

- customer_batch_events_service_role_policy

2. 在帳戶中佈建之後，您必須在聯合解決方案customer_batch_console_role中加入角色。

問：使用 有哪些限制 AWS Batch？

建立運算環境時，應將 EC2 執行個體標記為「customer_batch」或「customer-batch」。如果執行個體未加上標籤，則當任務完成時，執行個體將不會以批次方式終止。

問：要使用哪些先決條件或相依性 AWS Batch？

AWS Batch 您的 AMS 帳戶中沒有要使用的先決條件或相依性。

使用 AMS SSP 在您的 AMS AWS Certificate Manager 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 AWS Certificate Manager (ACM) 功能。 AWS Certificate Manager 是一種服務，可讓您佈建、管理和部署公有和私有 Secure Sockets Layer/Transport Layer Security (SSL/TLS) 憑證，以搭配 AWS 服務和您的內部連線資源使用。SSL/TLS 憑證用於保護網路通訊，並透過網際網路以及私有網路上的資源建立網站身分。 AWS Certificate Manager 移除了購買、上傳和續約 SSL/TLS 憑證的耗時手動程序。

透過 AWS Certificate Manager，您可以請求憑證，將其部署在 ACM 整合 AWS 的資源上，例如 Elastic Load Balancer、Amazon CloudFront 分佈和 APIs上的 API，並讓 AWS Certificate Manager 處理憑證續約。它還可讓您為內部資源建立私有憑證，並集中管理憑證生命週期。透過 佈建 AWS Certificate Manager 以與 ACM 整合服務搭配使用的公有和私有憑證是免費的。您只需為執行應用程式所建立 AWS 的資源付費。使用 AWS 私有憑證授權單位，您每月為 的操作和您發行的 AWS 私有 CA 私有憑證付費。若要進一步了解，請參閱 AWS Certificate Manager - AWS Documentation。

AWS Managed Services 常見問答集中的 ACM

常見問題和解答：

問：如何請求存取 AMS 帳戶中 AWS Certificate Manager 的 ？

透過提交管理 | AWS 服務 | 自行佈建服務 | 新增變更類型 (ct-1w8z66n899dct) 來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_acm_create_role。您可以使用此角色來建立和管理 ACM 憑證。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

即使您尚未新增 IAM 角色，也可以使用下列變更類型建立 ACM customer_acm_create_role 憑證：

- ACM | 建立公有憑證
- ACM | 建立私有憑證
- 具有其他 SANs ACM 憑證 | 建立

問：使用 有哪些限制 AWS Certificate Manager？

您必須向 AMS 提交變更請求 (RFC) 來刪除或修改現有的憑證，因為這些動作需要完整的管理員存取權 （ 使用管理 | 其他 | 更新變更類型 (ct-0xdawir96cy7k)。 請注意，IAM 政策無法根據標籤名稱 (mc*、ams* 等） 排除權限。憑證不會產生成本，因此刪除未使用的憑證不限時。

問：使用 Certificate Manager 有哪些先決條件或相依性？

現有的公有 DNS 名稱，以及建立 DNS CNAME 記錄的存取權，但這些記錄不需要託管在受管帳戶中。

使用 AMS SSP AWS 私有憑證授權單位 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS 私有憑證授權單位 的功能。私有憑證用於識別和保護私有網路上連線資源之間的通訊， 例如伺服器、 行動、 和 IoT 裝置和應用程式。AWS 私有 CA 是一項受管私有 CA 服務，可協助您輕鬆安全地管理私有憑證的生命週期。 AWS 私有 CA 為您提供高可用性的私有 CA 服務，無需預付投資和持續的維護成本來操作您自己的私有 CA。 將 ACM 的憑證管理功能 AWS 私有 CA 延伸至私有憑證。 可讓您集中建立和管理公有和私有憑證。您可以使用 AWS 管理主控台或 ACM API，輕鬆建立和部署 AWS 資源的私有憑證。對於 EC2 執行個體、容器、IoT 裝置和內部部署資源，您可以輕鬆建立和追蹤私有憑證，並使用您自己的用戶端自動化程式碼進行部署。您也可以靈活地建立私有憑證，並針對需要自訂憑證生命週期、金鑰演算法或資源名稱的應用程式自行管理它們。如需進一步了解，請參閱 AWS 私有 CA。

AWS 私有 CA AWS Managed Services 常見問答集中的

常見問題和解答：

問：如何在我的 AMS AWS 私有 CA 帳戶中請求存取權？

透過提交 AWS 服務 RFC 請求存取權 （ 管理 | AWS 服務 | 相容服務 ）。透過此 RFC，將在您的帳戶中佈建下列 IAM 角色：`customer_acm_pca_role`。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

問：使用 有哪些限制 AWS 私有 CA？

目前， AWS Resource Access Manager (AWS RAM) 無法用來共用您的 AWS 私有 CA 跨帳戶。

問：要使用哪些先決條件或相依性 AWS 私有 CA？

1. 如果您打算建立 CRL，則需要 S3 儲存貯體來存放。 AWS 私有 CA 會自動將 CRL 存放在您指定的 Amazon S3 儲存貯體中，並定期更新。設定 CRL 之前，S3 儲存貯體必須具有下列儲存貯體政策。為了繼續此請求，請使用 ct-0fpjlxa808sh2（管理 | 進階堆疊元件 | S3 儲存 | 更新政策） 建立 RFC，如下所示：

- 提供 S3 儲存貯體名稱或 ARN。
- 將下列政策複製到 RFC，並以您想要`bucket-name`的 S3 儲存貯體名稱取代 。

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"acm-pca.amazonaws.com"
         },
         "Action":[
            "s3:PutObject",
            "s3:PutObjectAcl",
            "s3:GetBucketAcl",
            "s3:GetBucketLocation"
         ],
         "Resource":[
            "arn:aws:s3:::bucket-name/*",
            "arn:aws:s3:::bucket-name"
         ]
      }
   ]
}
```

2. 如果上述 S3 儲存貯體已加密，則 Service Principal acm-pca.amazonaws.com 需要解密許可。為了繼續此請求，請使用 ct-3ovo7px2vsa6n（管理 | 進階堆疊元件 | KMS 金鑰 | 更新） 建立 RFC，如下所示：

- 提供必須更新政策的 KMS 金鑰 ARN。
- 將下列政策複製到 RFC，並以您想要bucket-name的 S3 儲存貯體名稱取代 。

```
{
   "Sid":"Allow ACM-PCA use of the key",
   "Effect":"Allow",
   "Principal":{
      "Service":"acm-pca.amazonaws.com"
   },
   "Action":[
      "kms:GenerateDataKey",
      "kms:Decrypt"
   ],
   "Resource":"*",
   "Condition":{
      "StringLike":{
         "kms:EncryptionContext:aws:s3:arn":[
            "arn:aws:s3:::bucket_name/acm-pca-permission-test-key",
            "arn:aws:s3:::bucket_name/acm-pca-permission-test-key-private",
            "arn:aws:s3:::bucket_name/audit-report/*",
            "arn:aws:s3:::bucket_name/crl/*"
         ]
      }
   }
}
```

3. AWS 私有 CA CRLs不支援 S3 設定「封鎖透過新存取控制清單 (ACLs公開存取」。您必須使用 S3 帳戶和儲存貯體停用此設定，以允許 AWS 私有 CA 寫入 CRLs，如如何安全地建立和存放 ACM Private CA 的 CRL。如果您想要停用，請使用 ct-0xdawir96cy7k 建立新的 RFC （管理 | 其他 | 其他 | 更新） 並連接風險接受。如果您對風險接受有任何疑問，請聯絡您的 Cloud Architect。

使用 AMS SSP 在您的 AMS 帳戶中 provision AWS CloudEndure

> **Note**
>
> 成功啟動 後 AWS Application Migration Service，CloudEndure Migration 服務會在所有 AWS 區域中終止生命週期。我們建議客戶使用 AWS Application Migration Service 來提升和轉移遷移至 GovCloud 區域和商業區域。如需詳細資訊，請參閱什麼是 AWS Application Migration Service？。

如果您想要使用 AWS Application Migration Service，請聯絡您的 CA，讓他們可以引導您。

使用 AMS 自助式佈建 (SSP) 模式直接在您的 AMS 受管帳戶中存取 AWS CloudEndure 功能。AWS CloudEndure 遷移可簡化、加速和自動化從實體、虛擬和雲端基礎設施到 的大規模遷移 AWS。CloudEndure 災難復原 (DR) 可防止停機時間和資料因任何威脅而遺失，包括勒索軟體和伺服器損毀。

AWS Managed Services 常見問答集中的AWS CloudEndure

問：如何請求存取 AMS 帳戶中的 CloudEndure？

透過提交管理 | AWS 服務 | 自行佈建服務 | 新增 （需要檢閱） (ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 使用者佈建至您的帳戶：`customer_cloud_endure_user`。在帳戶中佈建後，使用者存取金鑰和私密金鑰會在 AWS Secrets Manager 中共用。

這些政策也會佈建至 帳戶： `customer_cloud_endure_policy`和 `customer_cloud_endure_deny_policy`。

此外，您必須提供風險接受，因為用於應用程式整合的 CloudEndure DR 解決方案具有基礎設施變更許可。若要這樣做，請與您的雲端服務交付管理員 (CSDM) 合作。

問：在我的 AMS 帳戶中使用 CloudEndure 有哪些限制？

雲端持久性複寫和轉換執行個體只能在您指定的子網路中啟動。

問：在我的 AMS 帳戶中使用 CloudEndure 的先決條件或相依性是什麼？ 透過 RFC 雙向通訊共用下列項目：

- 要啟動的複寫和轉換執行個體的 VPC 子網路詳細資訊。
- 如果 EBS 磁碟區已加密，則為 KMS Key Amazon Resource Name (ARN)。

使用 AMS SSP AWS CloudHSM 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS CloudHSM 的功能。 AWS CloudHSM 可協助您符合公司、 合約、 在 AWS 雲端中使用專用硬體安全模組 (HSM) 執行個體，確保資料安全的 和 法規合規要求。 AWS和 AWS Marketplace 合作夥伴 提供各種解決方案來保護 AWS 平台內的敏感資料， 但對於某些受合約或法規要求管理密碼編譯金鑰的應用程式和資料， 可能需要額

外的保護。 AWS CloudHSM 會補足現有的資料保護解決方案，並允許您保護 HSMs 內的加密金鑰，這些加密金鑰是根據政府標準設計和驗證的安全金鑰管理。 AWS CloudHSM 可讓您安全地產生 。存放區、 和管理用於資料加密的密碼編譯金鑰，只有您才能存取金鑰。如需詳細資訊，請參閱 AWS CloudHSM。

AWS CloudHSM 在 AWS Managed Services 常見問答集中

常見問題和解答：

問：如何請求存取 AMS 帳戶中 AWS CloudHSM 的 ？

在您的 AMS 帳戶中使用 是兩個步驟：

1. 請求 AWS CloudHSM 叢集。透過使用 管理 | 其他 | 其他 | 建立 (ct-1e1xtak34nx76) 變更類型提交 RFC 來執行此操作。包含下列詳細資訊：
   - AWS 區域。
   - VPC ID/ARN。提供與您提交的 RFC 位於相同帳戶中的 VPC ID/VPC ARN。
   - 為叢集指定至少兩個可用區域。
   - 將連線至 HSM 叢集的 Amazon EC2 執行個體 ID。
2. 存取 AWS CloudHSM 主控台。透過使用 管理 | AWS 服務 | 自助佈建服務 | 新增 (ct-1w8z66n899dct) 變更類型提交 RFC 來執行此操作。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_cloudhsm_console_role`。

在帳戶中佈建角色之後，您必須在聯合解決方案中加入該角色。

問： AWS CloudHSM 在我的 AMS 帳戶中使用 有哪些限制？

存取 AWS CloudHSM 主控台無法讓您建立、終止或還原叢集。若要執行這些動作，請提交管理 | 其他 | 其他 | 建立變更類型 (ct-1e1xtak34nx76) 變更類型。

問： AWS CloudHSM 在我的 AMS 帳戶中使用 的先決條件或相依性是什麼？

您必須允許透過 VPC 中的用戶端 Amazon EC2 執行個體使用連接埠 2225 的 TCP 流量，或針對想要存取 HSM 叢集的內部部署伺服器使用 Direct Connect VPN。 AWS CloudHSM 安全群組和網路介面依賴 Amazon EC2。對於日誌監控或稽核，HSM 依賴 CloudTrail (AWS API 操作 ） 和 CloudWatch Logs 進行所有本機 HSM 裝置活動。

問：誰會將更新套用至 AWS CloudHSM 用戶端和相關軟體程式庫？

您負責套用程式庫和用戶端更新。您會想要監控 CloudHSM 版本歷史記錄頁面的版本，然後使用 CloudHSM 用戶端升級套用更新。

> **Note**
>
> 服務一律會自動套用 HSM AWS CloudHSM 設備的軟體修補程式。

使用 AMS SSP AWS CodeBuild 在您的 AMS 帳戶中佈建

使用 AMS 自助式服務佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS CodeBuild 的功能。 AWS CodeBuild 是一種全受管持續整合服務，可編譯原始程式碼、執行測試，並產生準備好部署的軟體套件。使用 CodeBuild，您便不必佈建、管理、擴展自己的組建伺服器。CodeBuild 會持續擴展並同時處理多個組建，所以您的組建不必排入佇列中等候。您可以利用預先封裝好的組建環境立即開始使用，或是建立自訂的組建環境來使用您自己的組建工具。使用 CodeBuild 時，將依據您使用運算資源的分鐘數計費。如需詳細資訊，請參閱 AWS CodeBuild。

> **Note**
>
> 若要使用單一 RFC 加入 CodeCommit、CodeBuild、CodeDeploy 和 CodePipeline，請提交管理 | AWS 服務 | 自助佈建服務 | 新增 （ 需要檢閱 ） (ct-3qe6io8t6jtny) 變更類型，並請求三種服務：CodeBuild、CodeDeploy 和 CodePipeline。然後，在您的帳戶中`aws_code_pipeline_service_role`佈建所有三個角色 `customer_codebuild_service_role`、`customer_codedeploy_service_role` 和 。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

AWS Managed Services 常見問答集中的 CodeBuild

常見問題和解答：

問：如何請求存取 AMS 帳戶中 AWS CodeBuild 的 ？

AWS CodeBuild 在您的 AMS 帳戶中使用 是兩個步驟：

1. 佈建`CodeBuild Service Role`用於建置程序的 ，以與 AWS S3 儲存貯體、Amazon CloudWatch 和日誌群組協調
2. 請求存取 CodeBuild 主控台

您可以向 Management | AWS service | Self-visioned service | Add change type (ct-1w8z66n899dct) 提交 RFC，請求在您的 AMS 帳戶中設定兩者。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問： AWS CodeBuild 在我的 AMS 帳戶中使用 有哪些限制？

對於 AWS CodeBuild 主控台管理員存取，許可在資源層級受到限制；例如，CloudWatch 動作在特定資源上受到限制，且`iam:PassRole`許可受到控制。

問：在我的 AMS 帳戶中使用 CodeBuild 的先決條件或相依性是什麼？

如果定義的 AWS CodeBuild 服務角色需要額外的 IAM 許可，請透過 AMS 服務請求請求它們。

使用 AMS SSP AWS CodeCommit 在您的 AMS 帳戶中佈建

> **Note**
>
> AWS 自 2024 年 7 月 25 日起 AWS CodeCommit， 已關閉新客戶對 的存取權。 AWS CodeCommit 現有客戶可以繼續如常使用服務。 AWS 會繼續投資 的安全性、可用性和效能改善 AWS CodeCommit，但我們不打算推出新功能。
> 若要將 AWS CodeCommit Git 儲存庫遷移至其他 Git 供應商，請聯絡您的雲端架構師 (CA) 以取得指引。如需遷移 Git 儲存庫的詳細資訊，請參閱如何將 AWS CodeCommit 儲存庫遷移至另一個 Git 供應商。

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS CodeCommit 的功能。 AWS CodeCommit 是一種全受管來源控制服務，可託管安全的 Git 型儲存庫。它可協助團隊在安全且可擴展的生態系統中協作程式碼。CodeCommit 無需操作您自己的來源控制系統或擔心擴展其基礎設施。您可以使用 CodeCommit 安全地存放從原始程式碼到二進位檔的任何內容，並與您現有的 Git 工具無縫搭配使用。如需詳細資訊，請參閱 AWS CodeCommit。

> **Note**
>
> 若要使用單一 RFC 加入 CodeCommit、CodeBuild、CodeDeploy 和 CodePipeline，請提交管理 | AWS 服務 | 自助佈建服務 | 新增 （ 需要檢閱 ） (ct-3qe6io8t6jtny) 變更類型，並請求三種服務：CodeBuild、CodeDeploy 和 CodePipeline。然後，在您的帳戶中`aws_code_pipeline_service_role`佈建所有三個角色 `customer_codebuild_service_role`、`customer_codedeploy_service_role` 和 。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

AWS Managed Services 常見問答集中的 CodeCommit

問：如何請求存取 AMS 帳戶中的 CodeCommit？

AWS CodeCommit 主控台和資料存取角色可以透過提交兩個 AWS 服務 RFCs、主控台存取和資料存取來請求：

- 透過使用 管理 | AWS 服務 | 自助佈建服務 | 新增 (ct-1w8z66n899dct) 變更類型提交 RFC AWS CodeCommit 來請求存取 。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_codecommit_console_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

  資料存取 （例如訓練和實體清單） 需要每個指定 S3 資料來源 （必要）、輸出儲存貯體 （必要） 和 KMS （選用） 之資料來源的個別 CTs。只要所有資料來源都已授予存取角色， AWS CodeCommit 工作建立就沒有限制。若要請求資料存取，請使用 管理 | 其他 | 其他 | 建立 (ct-1e1xtak34nx76) 提交 RFC。

問： AWS CodeCommit 在我的 AMS 帳戶中使用 有哪些限制？

CodeCommit 上的觸發功能會因為建立 SNS 主題的相關權限而停用。針對 CodeCommit 的直接驗證受到限制，使用者應該使用登入資料協助程式進行驗證。有些 KMS 命令也會受到限制：`kms:Encrypt`、`kms:Decrypt`、`kms:ReEncrypt`、`kms:GenerateDataKeyWithoutPlaintext`、`kms:GenereteDataKey`和 `kms:DescribeKey`。

問： AWS CodeCommit 在我的 AMS 帳戶中使用 的先決條件或相依性是什麼？

如果 S3 儲存貯體使用 KMS 金鑰加密，則需要 S3 和 KMS 才能使用 AWS CodeCommit。

使用 AMS SSP AWS CodeDeploy 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS CodeDeploy 的功能。 AWS CodeDeploy 是一項全受管部署服務，可將軟體部署自動化至各種運算服務，例如 Amazon EC2 AWS Fargate AWS Lambda和您的內部部署伺服器。 AWS CodeDeploy 可協助您快速發行新功能，協助您避免在應用程式部署期間停機，並處理更新應用程式的複雜性。您可以使用 AWS CodeDeploy 來自動化軟體部署，無需進行容易出錯的手動操作。服務會擴展以符合您的部署需求。如需詳細資訊，請參閱 AWS CodeDeploy。

> **Note**
>
> 若要使用單一 RFC 加入 CodeCommit、CodeBuild、CodeDeploy 和 CodePipeline，請提交管理 | AWS 服務 | 自助佈建服務 | 新增（需要檢閱）(ct-3qe6io8t6jtny) 變更類型，並請求三種服務：CodeBuild、CodeDeploy 和 CodePipeline。然後，在您的帳戶中`aws_code_pipeline_service_role`佈建所有三個角色`customer_codebuild_service_role`、`customer_codedeploy_service_role` 和 。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

AWS Managed Services 常見問答集中的 CodeDeploy

問：如何請求存取 AMS 帳戶中的 CodeDeploy？

透過使用 管理 | AWS 服務 | 自助佈建服務 | 新增 (ct-1w8z66n899dct) 變更類型提交 RFC，請求存取 CodeDeploy。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_codedeploy_console_role`和 `customer_codedeploy_service_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入`customer_codedeploy_console_role`角色。

問：在我的 AMS 帳戶中使用 CodeDeploy 有哪些限制？

目前我們僅支援運算平台做為 — Amazon EC2/內部部署。不支援藍/綠部署。

問：在我的 AMS 帳戶中使用 CodeDeploy 的先決條件或相依性是什麼？

在您的 AMS 帳戶中使用 CodeDeploy 沒有先決條件或相依性。

使用 AMS SSP AWS CodePipeline 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS CodePipeline 的功能。 AWS CodePipeline 是一種全受管持續交付服務，可協助您自動化發行管道，以快速且可靠的應用程式和基礎設施更新。根據您定義的發行模型，CodePipeline 可以自動在每次程式碼變更時建置、測試和部署程式碼。這可讓您快速且可靠地交付功能和更新。您可以輕鬆地 AWS CodePipeline 與第三方服務整合，例如 GitHub 或您自己的自訂外掛程式。使用 時 AWS CodePipeline，您只需支付使用量的費用。沒有預付費用，也無需長期承諾。如需詳細資訊，請參閱 AWS CodePipeline。

> **Note**
>
> 若要使用單一 RFC 加入 CodeCommit、CodeBuild、CodeDeploy 和 CodePipeline，請提交管理 | AWS 服務 | 自助佈建服務 | 新增（需要檢閱）(ct-3qe6io8t6jtny)

變更類型，並請求三種服務：CodeBuild、CodeDeploy 和 CodePipeline。然後，在您的帳戶中`aws_code_pipeline_service_role`佈建所有三個角色`customer_codebuild_service_role`、`customer_codedeploy_service_role` 和 。在帳戶中佈建後，您必須在聯合解決方案中加入角色。
AMS 中的 CodePipeline 不支援來源階段的「Amazon CloudWatch Events」，因為它需要更高的許可才能建立服務角色和政策，這會略過最低權限模型和 AMS 變更管理程序。

AWS Managed Services 常見問答集中的 CodePipeline

問：如何請求存取 AMS 帳戶中的 CodePipeline？

為相關帳戶中的 提交服務請求，以請求 CodePipeline `customer_code_pipeline_console_role` 的存取權。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

目前，AMS Operations 也會在您的帳戶中部署此服務角色：`aws_code_pipeline_service_role_policy`。

問：在我的 AMS 帳戶中使用 CodePipeline 有哪些限制？

是。CodePipeline 功能、階段和提供者僅限於下列項目：

1. 部署階段：僅限 Amazon S3，以及 AWS CodeDeploy
2. 來源階段：僅限 Amazon S3 AWS CodeCommit、BitBucket 和 GitHub
3. 建置階段：僅限 AWS CodeBuild和 Jenkins
4. 核准階段：僅限 Amazon SNS
5. 測試階段：僅限 Jenkins AWS CodeBuild、BlazeMeter、Ghost Inspector UI 測試、Micro Focus StormRunner Load 和 Runscope API 監控
6. 調用階段：僅限 Step Functions 和 Lambda

> **Note**
>
> AMS Operations 將在您的帳戶`customer_code_pipeline_lambda_policy`中部署；它必須與 Lambda 執行角色連接，以用於 Lambda 調用階段。請提供您要新增此政策的 Lambda 服務/執行角色名稱。如果沒有自訂 Lambda 服務/執行角色，AMS 將建立新的角色，名為 `customer_code_pipeline_lambda_execution_role`，這會是 `customer_lambda_basic_execution_role`與 的複本`customer_code_pipeline_lambda_policy`。

問：在我的 AMS 帳戶中使用 CodePipeline 有哪些先決條件或相依性？

AWS 支援的 服務， AWS CodeCommit AWS CodeBuild AWS CodeDeploy 必須在啟動 CodePipeline 之前或同時啟動。

使用 AMS SSP AWS Compute Optimizer 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Compute Optimizer 的功能。 AWS Compute Optimizer 建議工作負載的最佳 AWS 運算資源，以使用機器學習分析歷史使用率指標來降低成本並改善效能。過度佈建運算 (Amazon EC2 和 ASGs) 可能會導致不必要的基礎設施成本，而佈建不足的運算可能會導致應用程式效能不佳。Compute Optimizer 可協助您根據您的使用率資料，選擇最佳的 Amazon EC2 執行個體類型，包括屬於 Amazon EC2 Auto Scaling 群組的執行個體類型。如需詳細資訊，請參閱 AWS Compute Optimizer。

AWS Managed Services 常見問答集中的 Compute Optimizer

問：如何請求存取 AMS 帳戶中的 Compute Optimizer？

透過提交管理 | AWS 服務 | 自助佈建服務 | 新增 （需要檢閱）(ct-3qe6io8t6jtny)
變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳
戶：`customer_compute_optimizer_readonly_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Compute Optimizer 有哪些限制？

沒有限制。完整功能 AWS Compute Optimizer 可在您的 AMS 帳戶中使用。

問：在我的 AMS 帳戶中使用 Compute Optimizer 的先決條件或相依性是什麼？

- 您必須提交 RFC （管理 | 其他 | 其他 | 更新），授權 AMS Ops 在帳戶中啟用服務。
  在部署期間，會建立服務連結角色 (SLR)，以允許收集指標和產生報告。SLR 標記為「AWSServiceRoleForComputeOptimizer」。如需詳細資訊，請參閱使用 的服務連結角色 AWS Compute Optimizer
- 必須為下列指標啟用 CloudWatch 指標：
  - CPU 使用率：執行個體上使用的已配置 Amazon EC2 運算單位百分比。此指標可識別在所選執行個體上執行應用程式所需的處理能力。
  - 記憶體使用率：在取樣期間以某種方式使用的記憶體量。此指標識別在所選執行個體上執行應用程式所需的記憶體。記憶體使用率只會針對已安裝統一 CloudWatch 代理程式的資源進行分析。如需詳細資訊，請參閱使用 CloudWatch Agent 啟用記憶體使用率 （第 10 頁）。

- 網路傳入：執行個體在所有網路界面上接收的位元組數。此指標可識別傳入至單一執行個體的網路流量。
- 網路輸出：執行個體在所有網路界面上傳送的位元組數。此指標可識別來自單一執行個體的傳出網路流量。
- 本機磁碟輸入/輸出 (I/O)：本機磁碟的輸入/輸出操作數目。此指標可識別執行個體根磁碟區的效能

使用 AMS SSP AWS DataSync 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS DataSync 的功能。 會在內部部署儲存體與 Amazon S3、Amazon Elastic File System (Amazon Elastic File System) 或 Amazon FSx 之間線上 AWS DataSync 移動大量資料。與資料傳輸相關的手動任務可能會降低遷移速度和 IT 操作的負擔。DataSync 消除或自動處理許多這些任務，包括編寫複製任務指令碼、排程和監控傳輸、驗證資料，以及最佳化網路使用率。DataSync 軟體代理程式會連線至您的網路檔案系統 (NFS) 和伺服器訊息區塊 (SMB) 儲存體，因此您不需要修改應用程式。DataSync 可以透過網際網路或 AWS Direct Connect 連結，以高達開放原始碼工具 10 倍的速度傳輸數百 TB 和數百萬個檔案。您可以使用 DataSync 將作用中資料集或封存遷移至 AWS、將資料傳輸至雲端以進行及時分析和處理，或將資料複寫至 AWS 以進行業務連續性。

如需詳細資訊，請參閱 AWS DataSync。

AWS Managed Services 常見問答集中的 DataSync

問：如何請求存取 AMS 帳戶中的 DataSync？

透過提交管理 | AWS 服務 | 自助佈建服務 | 新增 （需要檢閱） (ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_datasync_console_role`。

在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

要用來串流任務日誌的 CloudWatch 日誌群組是 "/aws/datasync"。

問：在我的 AMS 帳戶中使用 DataSync 有哪些限制？

完整功能 AWS DataSync 可在您的 AMS 帳戶中使用。

問：在我的 AMS 帳戶中使用 DataSync 的先決條件或相依性是什麼？

- 與將使用 DataSync 服務角色 執行的 DataSync 任務相關聯的所有 S3 儲存貯體都需要 Amazon S3 ARNs (Amazon Resource Name)`customer_datasync_service_role`。 DataSync

- DataSync 代理程式的 VPC 端點和安全群組必須在使用 VPC 端點之前，使用 RFC 搭配 管理 | 其他 | 其他 | 建立 (ct-1e1xtak34nx76) 變更類型來請求。
- AWS DataSync 代理程式會以設備身分在 AMS 中執行。 AWS DataSync 代理程式由 服務修補和更新；如需詳細資訊，請參閱AWS DataSync 常見問答集。
- 若要啟動 AWS DataSync 代理程式，請使用 Management | Other | Other | Create (ct-1e1xtak34nx76) 變更類型提交 RFC，請求部署代理程式。提供 AWS DataSync Amazon EC2 AMI ID、執行個體類型、子網路、安全群組；並參考現有的 Amazon EC2 金鑰對或請求建立新的金鑰對。

> **Note**
>
> AMS 代表客戶手動佈建 AWS DataSync 代理程式，不需要在 AWS DataSync Amazon EC2 AMI 上進行 WIGS 擷取程序。

使用 AMS SSP AWS Device Farm 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Device Farm 的功能。 AWS Device Farm 是一種應用程式測試服務，可讓您透過廣泛的桌面瀏覽器和真實行動裝置測試 Web 和行動應用程式，藉此改善其品質；無需佈建和管理任何測試基礎設施。此服務可讓您在多個桌面瀏覽器或真實裝置上同時執行測試，以加速測試套件的執行，並產生影片和日誌，協助您快速識別應用程式的問題。

如需詳細資訊，請參閱 AWS Device Farm。

AWS Device Farm 在 AWS Managed Services 常見問答集中

問：如何請求存取 AMS 帳戶中 AWS Device Farm 的 ？

透過提交管理 | AWS 服務 | 自助佈建服務 | 新增 （需要檢閱） (ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_devicefarm_role`。

在帳戶中佈建後，您必須在聯合解決方案中加入角色。

問： AWS Device Farm 在我的 AMS 帳戶中使用 有哪些限制？

除了在 'Name' 標籤中使用 AMS 命名空間之外，還提供 AWS Device Farm 服務的完整存取權。

問： AWS Device Farm 在我的 AMS 帳戶中使用 的先決條件或相依性是什麼？

無。

使用 AMS SSP AWS Elastic Disaster Recovery 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Elastic Disaster Recovery 的功能。 使用經濟實惠的儲存、最少的運算和point-in-time復原，透過快速、可靠的內部部署和雲端應用程式復原，將停機時間和資料遺失 AWS Elastic Disaster Recovery 降至最低。當您使用 AWS Elastic Disaster Recovery 複寫在支援的作業系統上執行的內部部署或雲端型應用程式時，可以提高 IT 彈性。使用 AWS 管理主控台 來設定複寫和啟動設定、監控資料複寫，以及啟動執行個體以進行演練或復原。

如需詳細資訊，請參閱 AWS Elastic Disaster Recovery。

AWS Elastic Disaster Recovery AWS Managed Services 常見問答集中的

問：如何請求存取 AMS 帳戶中 AWS Elastic Disaster Recovery 的 ？

透過提交管理 | AWS 服務 | 自行佈建服務 | 新增 （需要檢閱） (ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_drs_console_role`。

在您的帳戶中佈建之後，您必須在聯合解決方案中加入該角色。

問： AWS Elastic Disaster Recovery 在我的 AMS 帳戶中使用 有哪些限制？

AWS Elastic Disaster Recovery 在您的 AMS 帳戶中沒有使用 的限制。

問： AWS Elastic Disaster Recovery 在我的 AMS 帳戶中使用 的先決條件或相依性是什麼？

- 存取主控台角色之後，您必須初始化 Elastic Disaster Recovery 服務，以在帳戶中建立所需的 IAM 角色。
  - 您必須提交變更類型 管理 | 應用程式 | IAM 執行個體描述檔 | 建立 （需要檢閱） 變更類型 ct-0ixp4ch2tiu04 RFC，以建立`customer-mc-ec2-instance-profile`執行個體描述檔的複製並連接`AWSElasticDisasterRecoveryEc2InstancePolicy`政策。您必須指定要連接新政策的機器。
  - 如果執行個體未使用預設執行個體描述檔，則 AMS 可以透過自動化`AWSElasticDisasterRecoveryEc2InstancePolicy`連接。
- 您必須使用客戶擁有的 KMS 金鑰進行跨帳戶復原。來源帳戶的 KMS 金鑰必須遵循政策更新，以允許目標帳戶存取。如需詳細資訊，請參閱與目標帳戶共用 EBS 加密金鑰。
- 必須更新 KMS 金鑰政策，以便在您不想切換角色以檢視時允許 `customer_drs_console_role` 檢視政策。

- 對於跨帳戶、跨區域災難復原，AMS 必須將來源和目標帳戶設定為信任帳戶，並透過此帳戶部署容錯回復和AWS 適當大小的角色 CloudFormation。

使用 AMS SSP AWS Elemental MediaConvert 在您的 AMS 帳戶中佈建

使用 AMS 自助式服務佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Elemental MediaConvert 的功能。 AWS Elemental MediaConvert 是一種具有廣播級功能的檔案型視訊轉碼服務。它可讓您建立 video-on-demand(VOD) 內容，以進行大規模廣播和多螢幕交付。此服務結合了進階視訊和音訊功能，以及簡單的 Web 服務界面和pay-as-you-go定價。透過 AWS Elemental MediaConvert，您可以專注於提供令人信服的媒體體驗，而不必擔心建置和操作您自己的影片處理基礎設施的複雜性。

如需詳細資訊，請參閱 AWS Elemental MediaConvert。

AWS Managed Services 常見問答集中的 MediaConvert

問：如何請求存取 AMS 帳戶中的 MediaConvert？

透過提交管理 | AWS 服務 | 自助佈建服務 | 新增 （需要檢閱） (ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_mediaconvert_author_role`。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

`customer_MediaConvert_Default_Role`MediaConvert 將使用第二個角色 來讀取來源 S3 儲存貯體並將輸出寫入目的地 S3 儲存貯體，並在您需要數位版權管理 (DRM) 時叫用 API 閘道。

問：在我的 AMS 帳戶中使用 MediaConvert 有哪些限制？

在 AMS 中使用 MediaConvert 沒有限制。

問：在我的 AMS 帳戶中使用 MediaConvert 有哪些先決條件或相依性？

在您的 AMS 帳戶中使用 MediaConvert 沒有先決條件或相依性。

使用 AMS SSP AWS Elemental MediaLive 在您的 AMS 帳戶中佈建

使用 AMS 自助式服務佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Elemental MediaLive 的功能。 AWS Elemental MediaLive 是一種廣播級即時視訊處理服務。它可讓您建立高品質的影片串流，以交付至廣播電視和網際網路連線的多螢幕裝置，例如連接的TVs、平板電腦、智慧型手機和機上盒。此服務的運作方式是即時編碼您的即時視訊串流、取得較大的即時視訊來源，並將其壓縮為較小的版本，以分發給您的檢視器。使用 AWS Elemental MediaLive，您可以輕鬆地為即時事件和全年無休頻

道設定串流，具有進階廣播功能、高可用性和pay-as-you-go定價。 AWS Elemental MediaLive 可讓您專注於為觀眾建立令人信服的即時視訊體驗，而不需要建置和操作廣播級視訊處理基礎設施的複雜性。

如需詳細資訊，請參閱 AWS Elemental MediaLive。

AWS Managed Services 常見問答集中的 MediaLive

問：如何請求存取 AMS 帳戶中的 MediaLive？

透過提交管理 | AWS 服務 | 自助佈建服務 | 新增 （需要檢閱） (ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_medialive_author_role`。

作為此 RFC 的一部分，第二個角色會部署到您的帳戶；`customer_medialive_service_role`此角色可指派給您的 Media Live 頻道和輸入，以與其他 服務互動，例如 Amazon S3、MediaStore 和 CloudWatch Logs。

在帳戶中佈建角色之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 MediaLive 有哪些限制？

在 AMS 中使用 MediaLive 沒有限制。

問：在我的 AMS 帳戶中使用 MediaLive 的先決條件或相依性是什麼？

在您的 AMS 帳戶中使用 MediaLive 沒有先決條件或相依性。

使用 AMS SSP AWS Elemental MediaPackage 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Elemental MediaPackage 的功能。 AWS Elemental MediaPackage 可靠地準備和保護您的視訊，以便透過網際網路交付。從單一視訊輸入， AWS Elemental MediaPackage 會建立格式化的視訊串流，以便在連接的TVs、行動電話、電腦、平板電腦和遊戲主控台上播放。它可以輕鬆為瀏覽者實作熱門的影片功能 （開始、暫停、倒轉等），就像 DVRs上常見的功能一樣。 AWS Elemental MediaPackage 也可以使用數位版權管理 (DRM) 自動保護您的內容。 會自動 AWS Elemental MediaPackage 擴展以回應載入，因此您的瀏覽者將永遠獲得絕佳的體驗，而無需事先準確預測您需要的容量。

如需詳細資訊，請參閱 AWS Elemental MediaPackage。

AWS Managed Services 常見問答集中的 MediaPackage

問：如何請求存取 AMS 帳戶中 AWS Elemental MediaPackage 的 ？

透過提交管理 | AWS 服務 | 自助佈建服務 | 新增 （需要檢閱） (ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_mediapackage_author_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

系統會提供第二個角色 `customer_mediapackage_service_role`，該角色可指派給您的 Media Live 頻道和輸入，以便與其他 服務互動，例如 S3 和 Secrets Manager。

問：在我的 AMS 帳戶中使用 MediaPackage 有哪些限制？

在 AMS 中使用 MediaPackage 沒有限制。

問：在我的 AMS 帳戶中使用 MediaPackage 的先決條件或相依性是什麼？

在您的 AMS 帳戶中使用 MediaPackage 沒有先決條件或相依性。

使用 AMS SSP AWS Elemental MediaStore 在您的 AMS 帳戶中佈建

> **Note**
>
> 在仔細考慮之後， AWS 決定停止 MediaStore，自 2025 年 11 月 13 日起生效。如果您是 MediaStore 的作用中客戶，您可以正常使用 MediaStore，直到 2025 年 11 月 13 日服務支援結束為止。在此日期之後，您將無法再使用 MediaStore 或此服務提供的任何功能。

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Elemental MediaStore 的功能。AWS Elemental MediaStore 是一種針對媒體最佳化的 AWS 儲存服務。它為您提供提供即時串流影片內容所需的效能、一致性和低延遲。 AWS Elemental MediaStore 會做為影片工作流程中的原始儲存體。其高效能功能可滿足最嚴苛媒體交付工作負載的需求，並結合長期、經濟實惠的儲存體。如需詳細資訊，請參閱 AWS Elemental MediaStore。

AWS Managed Services 中的 MediaStore 常見問答集

問：如何請求存取 AMS 帳戶中的 MediaStore？

透過使用 Management | AWS 服務 | 自助佈建服務 | 新增 (ct-1w8z66n899dct) 變更類型提交 RFC，請求存取 MediaStore。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_mediastore_author_role`。作為此 RFC 的一部分，第二個角色會部署到您的帳戶；如果您選擇啟用該功能，則 MediaStore 服務會使用該`MediaStoreAccessLogs`角色來記錄 CloudWatch 中的活動。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

目前，AMS Operations 也會在您的帳戶中部署此服務角色：`aws_code_pipeline_service_role_policy`。

問：在我的 AMS 帳戶中使用 MediaStore 有哪些限制？

在 AMS 中使用 MediaStore 沒有限制。

問：在我的 AMS 帳戶中使用 MediaStore 有哪些先決條件或相依性？

在您的 AMS 帳戶中使用 MediaStore 沒有先決條件或相依性。

使用 AMS SSP AWS Elemental MediaTailor 在您的 AMS 帳戶中佈建

使用 AMS 自助式服務佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Elemental MediaTailor 的功能。 AWS Elemental MediaTailor lets 影片提供者會將個別目標式廣告插入其影片串流，而不會犧牲廣播層級quality-of-service。使用 AWS Elemental MediaTailor時，即時或隨需影片的瀏覽者都會收到串流，將您的內容與個人化的廣告結合在一起。但與其他個人化廣告解決方案不同， AWS Elemental MediaTailor 您的整個串流 - 影片和廣告 - 都會提供廣播級影片品質，以改善觀眾的體驗。會根據用戶端和伺服器端廣告交付指標 AWS Elemental MediaTailor 提供自動化報告，以準確測量廣告曝光和觀眾行為。您可以使用 輕鬆獲利非預期的高需求檢視事件，無需預付成本 AWS Elemental MediaTailor。它還可以提高廣告交付率，協助您從每個影片中獲利更多，並適用於更廣泛的內容交付網路、廣告決策伺服器和用戶端裝置。

如需詳細資訊，請參閱 AWS Elemental MediaTailor。

AWS Managed Services 常見問答集中的 MediaTailor

問：如何請求存取 AMS 帳戶中的 MediaTailor？

透過使用 Management | AWS 服務 | 自助佈建服務 | 新增 (ct-1w8z66n899dct) 變更類型提交 RFC，請求存取 MediaTailor。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer-mediatailor-role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 MediaTailor 有哪些限制？

在 AMS 中使用 MediaTailor 沒有限制。

問：在我的 AMS 帳戶中使用 MediaTailor 的先決條件或相依性是什麼？

在您的 AMS 帳戶中使用 MediaTailor 沒有先決條件或相依性。

使用 AMS SSP AWS Global Accelerator 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Global Accelerator 功能。Global Accelerator 是一種網路層服務，您可以在其中建立加速器，以改善全球受眾使用的網際網路應用程式的可用性和效能。若要進一步了解，請參閱 Global Accelerator。

AWS Managed Services 中的 Global Accelerator 常見問答集

常見問題和解答：

問：如何請求在我的 AMS 帳戶中設定 Global Accelerator？

透過提交 AWS 服務 RFC 請求存取權（管理 | AWS 服務 | 自助佈建服務）。透過此 RFC，會在您的帳戶中佈建下列 IAM 角色：`customer_global_accelerator_console_role`。在帳戶中佈建後，您必須在聯合解決方案中加入主控台角色。

問：在我的 AMS 帳戶中使用 Global Accelerator 有哪些限制？

Global Accelerator 是一種全域服務，支援多個 AWS 區域中的端點，列於AWS 區域資料表中。

問：在我的 AMS 帳戶中使用 Global Accelerator 有哪些先決條件或相依性？

當您設定加速器與 Global Accelerator 時，您可以將靜態 IP 地址與一或多個 AWS 區域中的區域端點建立關聯。對於標準加速器，端點為 Network Load Balancer、Application Load Balancer、Amazon EC2 執行個體或彈性 IP 地址。對於自訂路由加速器，端點是具有一或多個 EC2 執行個體的虛擬私有雲端 (VPC) 子網路。

使用 AMS SSP AWS Glue 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Glue 的功能。 AWS Glue 是一種全受管擷取、轉換和載入 (ETL) 服務，可協助您準備和載入資料以供分析。您可以在 中按幾下滑鼠來建立和執行 ETL 任務 AWS 管理主控台。您可以指向存放在 上的 AWS Glue 資料 AWS，並 AWS Glue 探索您的資料，並將相關聯的中繼資料（例如資料表定義和結構描述）存放在 中 AWS Glue Data Catalog。編製目錄後，您的資料即可立即搜尋、查詢，並可用於 ETL 動作。如需詳細資訊，請參閱 AWS Glue。

AWS Glue 在 AWS Managed Services 常見問答集中

常見問題和解答：

問：如何 AWS Glue 請求在我的 AMS 帳戶中設定 ？

透過使用 管理 | AWS 服務 | 自助佈建服務 | 新增變更類型 (ct-1w8z66n899dct) 提交 RFC AWS Glue 來請求存取 。此 RFC 會將下列 IAM 角色佈建至您的帳戶：

- `customer_glue_console_role`
- `customer_glue_service_role`

上述角色包括下列連接的政策：

- `customer_glue_secrets_manager_policy`
- `customer_glue_deny_policy`

在帳戶中佈建角色之後，您必須在聯合解決方案中加入這些角色。

若要存取爬蟲程式、任務和開發端點（特定使用案例所需的角色），請使用 部署 | 進階堆疊元件 | Identity and Access Management (IAM) | 建立實體或政策 (ct-3dpd8mdd9jn1r) 提交 RFC。

問： AWS Glue 在我的 AMS 帳戶中使用 有哪些限制？

沒有限制。完整功能 AWS Glue 可在您的 AMS 帳戶中使用。對於您可以在其中撰寫和測試 ETL 指令碼的互動式環境，請在 AWS Glue Studio 上使用筆記本。 AWS Glue 互動式工作階段和任務筆記本是的無伺服器功能 AWS Glue ，您可以在 中使用 AWS Glue 並使用 AWS Glue 服務角色。

AWS Glue 2.0 之前： AWS Glue 筆記本是非受管資源，可在 帳戶中啟動 Amazon EC2 執行個體。最佳實務是啟動您自己的 Amazon EC2 執行個體，並安裝支援筆記本環境和開發所需的軟體。如需詳細資訊，請參閱教學課程：設定本機 Apache Zeppelin 筆記本來測試和偵錯 ETL 指令碼，以及使用開發端點來開發指令碼。

問： AWS Glue 在我的 AMS 帳戶中使用 的先決條件或相依性是什麼？

AWS Glue 具有 Amazon S3、CloudWatch 和 CloudWatch Logs 的相依性。暫時性相依性會根據資料來源而有所不同，而其他服務 AWS Glue 功能可能會與之互動（例如：Amazon Redshift、Amazon RDS、Athena)。

使用 AMS SSP AWS Lake Formation 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Lake Formation 的功能。 AWS Lake Formation 是一種可在幾天內輕鬆設定安全資料湖的服務。資料湖是一個集中式、經策管且安全

的儲存庫，可用原始格式存放您的所有資料並準備進行分析。資料湖可讓您細分資料孤島，再結合不同類型的分析來取得洞察並指導得出更佳的商業決策。

使用 Lake Formation 建立資料湖，就跟定義資料來源、您想要套用哪些資料存取和安全政策一樣簡單。Lake Formation 之後有助於您從資料庫和物件儲存中收集和編製資料目錄、將資料移至新的 Amazon S3 資料湖、使用機器學習演算法清理和分類資料，以及安全存取敏感資料。您的使用者可以存取集中式資料目錄（如需詳細資訊，請參閱AWS Glue 常見問答集)，說明可用的資料集及其適當的使用方式。然後，您的使用者會利用這些資料集搭配他們選擇的分析和機器學習服務，例如 Amazon Redshift、Amazon Athena 和（測試版） Amazon EMR for Apache Spark。Lake Formation 以 中可用的功能為基礎AWS Glue。

如需詳細資訊，請參閱 AWS Lake Formation。

AWS Managed Services 中的 Lake Formation 常見問答集

問：如何請求存取 AMS 帳戶中 AWS Lake Formation 的 ？

透過提交管理 | AWS 服務 | 自助佈建服務 | 新增（需要檢閱）(ct-3qe6io8t6jtny)
變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_lakeformation_data_analyst_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

此外，以下兩個角色是選用的：

- `customer_lakeformation_admin_role`
- `customer_lakeformation_workflow_role`

對於管理員許可，您可以選擇將角色加入`customer_lakeformation_admin_role`為相同 SSPS 變更類型 (ct-3qe6io8t6jtny) 的一部分。

如果您想要在 AWS Lake Formation 主控台中建立藍圖，您需要提交管理 | 其他 | 其他 RFC (ct-1e1xtak34nx76) 以部署 `customer_lakeformation_workflow_role`。在 RFC 中，如果建立藍圖時儲存貯體是來源，您必須提供 S3 儲存貯體名稱。如果藍圖類型為 Classic Load Balancer Logs 或 Application Load Balancer Logs AWS CloudTrail，則 S3 儲存貯體適用。

問： AWS Lake Formation 在我的 AMS 帳戶中使用 有哪些限制？

Lake Formation 的完整功能可在 AMS 中使用。

問： AWS Lake Formation 在我的 AMS 帳戶中使用 的先決條件或相依性是什麼？

Lake Formation 與 AWS Glue 服務整合，因此 AWS Glue 使用者只能存取具有 Lake Formation 許可的資料庫和資料表。此外， AWS Athena 和 Amazon Redshift 使用者只能查詢具有 Lake Formation 許可的 AWS Glue 資料庫和資料表。

使用 AMS SSP AWS Lambda 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Lambda 的功能。 AWS Lambda 無需佈建或管理伺服器即可執行程式碼。您只需為使用的運算時間付費，程式碼未執行時無需付費。使用 Lambda，您可以為幾乎任何類型的應用程式或後端服務執行程式碼，完全無需管理。 上傳您的程式碼，Lambda 會處理執行和擴展程式碼所需的一切，並提供高可用性。您可以將程式碼設定為自動從其他 AWS 服務觸發，或直接從任何 Web 或行動應用程式呼叫它。如需詳細資訊，請參閱 AWS Lambda。

AWS Managed Services 常見問答集中的 Lambda

問：如何請求存取 AMS 帳戶中 AWS Lambda 的 ？

透過提交管理 | AWS 服務 | 自助佈建服務 | 新增 （需要檢閱） (ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶： `customer_lambda_admin_role`和 `customer_lambda_basic_execution_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問： AWS Lambda 在我的 AMS 帳戶中使用 有哪些限制？

- Lambda 函數旨在由事件來源調用。如需可做為 Lambda 事件來源的服務清單，請參閱搭配使用 AWS Lambda 與其他 服務。目前並非所有這些服務都可在 AMS 帳戶中使用。如果您需要無法使用的服務，請使用您的 AMS CSDM 來提交例外狀況。
- 根據預設，AMS 為您提供基本的 Lambda 啟動角色，其中包含 `AWSLambdaBasicExecutionRole`和 `AWSXrayWriteOnlyAccess`許可；如需詳細資訊，請參閱AWS Lambda 啟動角色。如果您需要其他許可，例如能夠在 AMS VPC 中佈建 Lambda 函數，請使用 Management | AWS 服務 | 自助佈建服務 | 新增 （需要檢閱） (ct-3qe6io8t6jtny) 變更類型提交 RFC。

問： AWS Lambda 在我的 AMS 帳戶中使用 的先決條件或相依性是什麼？

沒有先決條件或相依性可開始使用 AWS Lambda；不過，根據您的特定使用案例，您可能需要存取其他 AWS 服務來建立事件來源，或您的函數執行各種動作的額外許可。如果需要其他許可，請使用 管理 | AWS 服務 | 自助佈建服務 | 新增 （需要檢閱） 變更類型 (ct-3qe6io8t6jtny) 提交 RFC。

問：我需要做什麼才能在任何帳戶中執行 Lambda 函數？

若要在核心帳戶中部署 Lambda 函數，請使用下列準則：

- 確定 的 SSPS AWS Lambda 已加入。
- 只要 AMS 資源受到保護且合規，就沒有特定限制禁止在 AMS 責任下進行此部署。
- 如果您希望 AMS 建立 Lambda 函數，則必須先使用 提供的 SSPS 角色 AWS Lambda。然後，如果您仍希望 AMS 協助部署或支援 函數，請聯絡您的 CA 並開始超出範圍 (OOS) 程序。

使用 AMS SSP AWS License Manager 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS License Manager 的功能。 與 AWS 服務 AWS License Manager 整合，透過單一 AWS 帳戶簡化跨多個 AWS 帳戶、IT 目錄和內部部署的授權管理。 AWS License Manager 可讓管理員建立模擬其授權協議條款的自訂授權規則，然後在 Amazon EC2 執行個體啟動時強制執行這些規則。中的規則 AWS License Manager 可讓您透過實際停止執行個體啟動或通知管理員有關違規的情況來限制授權違規。如需詳細資訊，請參閱 AWS License Manager。

AWS Managed Services 常見問答集中的 License Manager

常見問題和解答：

問：如何 AWS License Manager 請求在我的 AMS 帳戶中設定 ？

透過使用 管理 | AWS 服務 | 自助佈建服務 | 新增 (ct-1w8z66n899dct) 變更類型提交 RFC AWS License Manager 來請求存取 。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_license_manager_role`。在您的帳戶中佈建 License Manager IAM 角色後，您必須在聯合解決方案中加入該角色。

問： AWS License Manager 在我的 AMS 帳戶中使用 有哪些限制？

您可以將 AWS License Manager 規則與您擁有AMIs 建立關聯（依「由我擁有」進行篩選）。如果您選擇強制執行與 AMI 的限制關聯（例如： 只能支援此 AMI 的 100 個 vCPU) 並耗盡限制，則未來使用該 AMI 啟動會遭到封鎖，並傳回錯誤，指出「沒有可用的授權」。這是此服務的預期行為（不允許授權耗盡）。如果您用盡限制，但需要再次啟動 AMI，則必須修改在 中設定的規則 AWS License Manager。

問： AWS License Manager 在我的 AMS 帳戶中使用 的先決條件或相依性是什麼？

AWS License Manager 您的 AMS 帳戶中沒有要使用的先決條件或相依性。

使用 AMS SSP AWS Migration Hub 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Migration Hub 的功能。 AWS Migration Hub 提供單一位置，可讓您追蹤跨多個 AWS 和 合作夥伴解決方案的應用程式遷移進度。使用 Migration Hub 可讓您選擇最符合您需求的 AWS 和 合作夥伴遷移工具，同時提供跨應用程式產品組合遷移狀態的可見性。Migration Hub 也為個別應用程式提供關鍵指標和進度，無論使用哪些工具來進行遷移。這可讓您快速取得所有遷移的進度更新、輕鬆識別和疑難排解任何問題，並減少遷移專案所花費的整體時間和精力。如需詳細資訊，請參閱 AWS Migration Hub。

AWS Managed Services 常見問答集中的遷移中樞

常見問題和解答：

問：如何請求存取 AMS 帳戶中的 Migration Hub？

透過使用 Management | AWS service | Self-visioned service | Add (ct-1w8z66n899dct) 變更類型提交 RFC，請求存取 Migration Hub。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_migrationhub_author_role`。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

問：Migration Hub 有哪些限制？

無。

問：啟用 Migration Hub 的先決條件有哪些？

在您的 AMS 帳戶中開始使用 Migration Hub 沒有先決條件。不過，在管理服務期間，可能需要 Migration Hub 以外的許可，例如將許可寫入 Amazon S3 以上傳伺服器資訊。

使用 AMS SSP AWS Outposts 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Outposts 的功能。 AWS Outposts 是一項全受管服務，可將 AWS 基礎設施、 AWS 服務、APIs 和工具延伸至幾乎所有資料中心、主機代管空間或內部部署設施，以獲得一致的混合體驗。 AWS Outposts 非常適合需要低延遲存取內部部署系統、本機資料處理或本機資料儲存的工作負載。如需詳細資訊，請參閱 AWS Outposts。

AWS Outposts 在 AWS Managed Services 常見問答集中

常見問題和解答：

問：如何 AWS Outposts 請求在我的 AMS 帳戶中設定 ？

透過使用 管理 | AWS 服務 | 自助佈建服務 | 新增 (ct-1w8z66n899dct) 變更類型提交 RFC AWS Outposts 來請求存取 。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_outposts_role`。在帳戶中佈建角色後，您必須在聯合解決方案中加入該角色。

問： AWS Outposts 在我的 AMS 帳戶中使用 有哪些限制？

AWS Outposts 在您的 AMS 帳戶中使用 沒有限制。

問： AWS Outposts 在我的 AMS 帳戶中使用 的先決條件或相依性是什麼？

AWS Outposts 您的 AMS 帳戶中沒有要使用的先決條件或相依性。

使用 AMS SSP AWS Resilience Hub 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Resilience Hub 的功能。 AWS Resilience Hub 可協助您主動準備和保護您的 AWS 應用程式免受中斷。Resilience Hub 提供彈性評估和驗證，整合到您的軟體開發生命週期中，以發現彈性弱點。Resilience Hub 可協助您預估應用程式是否可以符合復原時間目標 (RTO) 和復原點目標 (RPO) 目標，並協助在問題發佈到生產環境之前解決問題。在生產環境中部署 AWS 應用程式之後，您可以使用 Resilience Hub 繼續追蹤應用程式的彈性狀態。如果發生中斷，Resilience Hub 會傳送通知給操作員，以啟動相關聯的復原程序。

AWS Resilience Hub 在 AWS Managed Services 常見問答集中

常見問題和解答：

問：如何請求存取 AMS 帳戶中 AWS Resilience Hub 的 ？

透過使用 Management | AWS service | Self-visioned Service | Add (ct-1w8z66n899dct) 變更類型提交 RFC，請求存取 Resilience Hub。此 RFC 會將下列 IAM 角色和政策佈建至您的帳戶：

IAM 角色

- `customer_resiliencehub_console_role`
- `customer_resiliencehub_service_role`

Policies

- `customer_resiliencehub_console_policy`

- customer_resiliencehub_service_policy

在帳戶中佈建角色之後，您必須在聯合解決方案customer_resiliencehub_console_role中加入角色。

問： AWS Resilience Hub 在我的 AMS 帳戶中使用 有哪些限制？

沒有限制。您的 AMS 帳戶中提供 Resilience Hub 的完整功能。

問： AWS Resilience Hub 在我的 AMS 帳戶中使用 的先決條件或相依性是什麼？

在您的 AMS 帳戶中使用 Resilience Hub 沒有先決條件或相依性。

使用 AMS SSP AWS Secrets Manager 在您的 AMS 帳戶中佈建

使用 AMS 自助式服務佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Secrets Manager 的功能。AWS Secrets Manager 可協助您保護存取應用程式、服務和 IT 資源所需的秘密。此服務可讓您在整個生命週期中輕鬆輪換、管理和擷取資料庫登入資料、API 金鑰和其他秘密。使用者和應用程式透過呼叫 Secrets Manager APIs 來擷取秘密，無需以純文字硬式編碼敏感資訊。Secrets Manager 提供秘密輪換與 Amazon RDS、Amazon Redshift 和 Amazon DocumentDB 的內建整合。此外，此服務可延伸至其他類型的秘密，包括 API 金鑰和 OAuth 權杖。如需詳細資訊，請參閱 AWS Secrets Manager。

> **Note**
>
> 根據預設，AMS 運算子可以在 中存取使用帳戶預設 AWS KMS 金鑰 AWS Secrets Manager (CMK) 加密的秘密。如果您希望 AMS Operations 無法存取您的秘密，請使用自訂 CMK，並搭配 AWS Key Management Service (AWS KMS) 金鑰政策來定義適用於存放在秘密中資料的許可。

AWS Managed Services 常見問答集中的 Secrets Manager

問：如何請求存取 AMS 帳戶中 AWS Secrets Manager 的 ？

透過使用 Management | AWS 服務 | 自助佈建服務 | 新增 (ct-3qe6io8t6jtny) 變更類型提交 RFC 來請求 Secrets Manager 的存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_secrets_manager_console_role和 customer-rotate-secrets-lambda-role。customer_secrets_manager_console_role 用作佈建和管理

秘密的管理員角色，並customer-rotate-secrets-lambda-role用作輪換秘密的 Lambda 函數的 Lambda 執行角色。在帳戶中佈建之後，您必須在聯合解決方案中加入customer_secrets_manager_console_role角色。

問： AWS Secrets Manager 在我的 AMS 帳戶中使用 有哪些限制？

完整功能 AWS Secrets Manager 可在您的 AMS 帳戶中使用，以及秘密的自動輪換功能。不過，請注意，不支援使用「建立新的 Lambda 函數以執行輪換」來設定輪換，因為它需要更高的許可才能建立 CloudFormation 堆疊 (IAM 角色和 Lambda 函數建立），這會略過變更管理程序。AMS Advanced 僅支援「使用現有的 Lambda 函數來執行輪換」，您可以在其中管理 Lambda 函數，以使用 AWS Lambda SSPS Admin 角色輪換秘密。AMS Advanced 不會建立或管理 Lambda 來輪換秘密。

問： AWS Secrets Manager 在我的 AMS 帳戶中使用 的先決條件或相依性是什麼？

下列命名空間保留供 AMS 使用，無法做為直接存取的一部分使用 AWS Secrets Manager：

- arn：aws：secretsmanager：*：*：secret：ams-shared/*
- arn：aws：secretsmanager：*：*：secret：customer-shared/*
- arn：aws：secretsmanager：*：*：secret：ams/*

使用 Secrets Manager (AMS SSPS) 共用金鑰

在 RFC、服務請求或事件報告的純文字中與 AMS 共用秘密會導致資訊公開事件，而 AMS 會修訂您重新產生金鑰的案例和請求中的資訊。

您可以在此命名空間 下使用 AWS Secrets Manager(Secrets Manager)customer-shared。

使用 Secrets Manager 共用金鑰常見問答集

問：必須使用 Secrets Manager 共用哪種類型的秘密？

幾個範例是用於建立 VPN 的預先共用金鑰、身分驗證金鑰 (IAM、SSH)、授權金鑰和密碼等機密金鑰。

問：如何使用 Secrets Manager 與 AMS 共用金鑰？

1. 使用您的聯合存取和適當的角色登入 AWS 管理主控台：

   對於 SALZ， Customer_ReadOnly_Role

對於 MALZ，AWSManagedServicesChangeManagementRole。

2. 導覽至 AWS Secrets Manager 主控台，然後按一下存放新的秘密。
3. 選取 Other type of secrets (其他機密類型)。
4. 以純文字形式輸入秘密值，並使用預設 KMS 加密。按一下 Next (下一步)。
5. 輸入秘密名稱和描述，名稱一律以客戶共用/ 開頭。例如，Customer-shared/mykey2022。按一下 Next (下一步)。
6. 保持停用自動輪換，按一下下一步。
7. 檢閱並按一下儲存以儲存秘密。
8. 透過服務請求、RFC 或事件報告以秘密名稱回覆我們，以便我們識別和擷取秘密。

問：使用 Secrets Manager 共用金鑰需要哪些許可？

SALZ：尋找customer_secrets_manager_shared_policy受管 IAM 政策，並確認政策文件與以下建立步驟中附加的政策文件相同。確認政策已連接至下列 IAM 角色：Customer_ReadOnly_Role。

MALZ：驗證 AMSSecretsManagerSharedPolicy已連接至角色，該AWSManagedServicesChangeManagementRole角色可讓您在ams-shared命名空間中執行GetSecretValue動作。

範例：

```
{
 "Action": "secretsmanager:*",
 "Resource": [
 "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
 "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
 ],
 "Effect": "Allow",
 "Sid": "AllowAccessToSharedNameSpaces"
 }
```

> **Note**
>
> 當您新增 AWS Secrets Manager 做為自助式佈建服務時，會授予必要的許可。

使用 AMS SSP AWS Security Hub CSPM 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Security Hub CSPM 的功能。AWS Security Hub CSPM 為您提供安全狀態的全方位檢視， AWS 以及安全產業標準和最佳實務的合規性。Security Hub 會集中並優先處理來自 AWS 帳戶、服務和支援的第三方合作夥伴的安全和合規調查結果，以協助您分析安全趨勢並識別最高優先順序的安全問題。如需詳細資訊，請參閱 AWS Security Hub CSPM。

AWS Managed Services 常見問答集中的 Security Hub

問：如何請求存取 AMS 帳戶中 AWS Security Hub CSPM 的 ？

透過使用 管理 | AWS 服務 | 自助佈建服務 | 新增 (ct-1w8z66n899dct) 變更類型提交 RFC 來請求存取 Security Hub。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_securityhub_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Security Hub 有哪些限制？

封存功能已被記錄為潛在的安全和操作風險，並已被限制為自我佈建服務安全角色的一部分。

問： AWS Security Hub CSPM 在我的 AMS 帳戶中使用 的先決條件或相依性是什麼？

AWS Security Hub CSPM 您的 AMS 帳戶中沒有要使用的先決條件或相依性。

使用 AMS SSP AWS Service Catalog AppRegistry 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 AppRegistry 功能。AppRegistry 可從中央位置啟用應用程式搜尋、報告和管理動作。建置器很少在單一 AWS 帳戶中建立應用程式。它們通常會依生命週期階段區隔應用程式資源，例如開發、測試和生產。AppRegistry 可讓您將 AWS 定義帳戶中的所有資源集合分組和檢視。

使用 AppRegistry，您可以存放 AWS 應用程式、與應用程式相關聯的資源集合，以及應用程式屬性群組。若要進一步了解，請參閱什麼是 AppRegistry。

常見問答集：在 AMS AWS Service Catalog AppRegistry 中

問：如何請求存取 AMS 帳戶中 AWS Service Catalog AppRegistry 的 ？

透過使用 管理 | AWS 服務 | 自助佈建服務 | 新增 （ 需要檢閱 ） (ct-3qe6io8t6jtny) 變更類型提交 RFC，請求存取 AppRegistry。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer-appregistry-console-role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問： AWS Service Catalog AppRegistry 在我的 AMS 帳戶中使用 有哪些限制？

除了在 'Name'標籤中使用 AMS 命名空間之外，還提供 AppRegistry 服務的完整存取權。

問： AWS Service Catalog AppRegistry 在我的 AMS 帳戶中使用 的先決條件或相依性是什麼？

在您的 AMS 帳戶中使用 AppRegistry 沒有先決條件或相依性。

使用 AMS SSP AWS Shield Advanced 在您的 AMS 帳戶中佈建

使用 AMS 自助式服務佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Shield Advanced 的功能。AWS Shield Advanced 是一種受管分散式拒絕服務 (DDoS) 保護服務，可保護在 上執行的應用程式 AWS。Shield Advanced 提供全年無休的偵測和自動內嵌緩解措施，可將應用程式停機時間和延遲降至最低，因此不需要讓 AWS Support 參與，即可受益於 DDoS 保護。有兩種方案 AWS Shield ：標準和進階；AMS 提供 Shield Advanced。若要進一步了解，請參閱 Shield Advanced。

所有 AWS 客戶都能從自動保護中受益 AWS Shield Standard，無需額外付費。 可 AWS Shield Standard 防禦以您的網站或應用程式為目標的最常見、經常發生的網路和傳輸層 DDoS 攻擊。當您 AWS Shield Standard 搭配 Amazon CloudFront 和 Amazon Route 53 使用 時，您可以獲得針對所有已知基礎設施 （ 第 3 層和第 4 層 ） 攻擊的全方位可用性保護。

如需針對在 Amazon Elastic Compute Cloud (Amazon EC2)、Elastic Load Balancing (ELB) AWS Global Accelerator、Amazon CloudFront 和 Amazon Route 53 資源上執行的應用程式進行攻擊的更高層級保護，您可以訂閱 AWS Shield Advanced。

除了 隨附的網路和傳輸層保護之外 AWS Shield Standard， AWS Shield Advanced 還提供額外偵測和防禦，以防範大型和複雜的 DDoS 攻擊、近乎即時的攻擊可見性，以及與 AWS WAF Web 應用程式防火牆整合。 AWS Shield Advanced 也可讓您全年無休地存取 AWS Shield 回應團隊 (SRT)，並保護 Amazon Elastic Compute Cloud (Amazon EC2)、Elastic Load Balancing (Elastic Load Balancing) AWS Global Accelerator、Amazon CloudFront 和 Amazon Route 53 費用中的 DDoS 相關峰值。

AWS Managed Services 常見問答集中的 Shield Advanced

問：如何請求存取 AMS 帳戶中的 Shield Advanced？

透過使用 管理 | AWS 服務 | 自行佈建服務 | 新增 (ct-1w8z66n899dct) 變更類型提交 RFC 來請求存取 Shield Advanced。此 RFC 會將下列 IAM 角色佈建至您的帳戶： `customer_shield_role`和 `aws_drt_shield_role`。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

在角色部署到您的帳戶後，您可以使用 `customer_shield_role` 來確認 AWS Shield Advanced 帳戶中的 訂閱。

> **Note**
>
> 請注意，使用 會產生月費和一年的承諾 AWS Shield Advanced。此外，在 AMS AWS Shield Advanced 中使用 可授權 AMS 升級至 AWS Shield (SRT)，其可能會在升級分散式拒絕服務 (DDoS AWS WAF) 事件期間變更您的 Web 應用程式防火牆 () 規則。這些變更將與 AMS 協調進行。

問：在我的 AMS 帳戶中使用 Shield Advanced 有哪些限制？

雖然不是限制，但您應該了解使用 Shield Advanced 部署 `aws_drt_shield_role`，這可讓 AWS Shield 團隊 (SRT) 在升級的 DDoS 事件期間對 AMS 帳戶內的 AWS WAF 規則進行緊急變更。AMS 建議這樣做，以最快的速度修復 DDoS 攻擊，並在 AMS 升級至 SRT 之後發生。

問：在我的 AMS 帳戶中使用 Shield Advanced 的先決條件或相依性是什麼？

在您的 AMS 帳戶中使用 Shield Advanced 沒有先決條件或相依性。

使用 AMS SSP AWS Snowball Edge 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Snowball Edge 功能。Snowball Edge 是一種 PB 級資料傳輸解決方案，使用專為安全而設計的裝置，將大量資料傳入和傳出 AWS 雲端。Snowball Edge 透過大規模資料傳輸解決常見的挑戰，包括高網路成本、長傳輸時間和安全問題。您可以使用 Snowball Edge 遷移分析資料、基因體資料、影片庫、映像儲存庫、備份，以及封存部分資料中心關機、磁帶取代或應用程式遷移專案。使用 Snowball Edge 傳輸資料簡單、快速、更安全，而且使用高速網際網路傳輸資料的成本可能低至五分之一。

使用 Snowball Edge，您不需要撰寫任何程式碼或購買任何硬體來傳輸資料。從使用 AWS 管理主控台為 Snowball 建立匯入任務開始，Snowball 裝置會自動運送給您。一旦裝置送達，請將裝置連接到您的本機網路，下載並執行 Snowball 用戶端 (「用戶端」) 以建立連線，然後使用用戶端選取您要傳輸至裝置的檔案目錄。然後，用戶端會高速加密檔案並將其傳輸至裝置。傳輸完成且裝置準備好要送回後，E Ink 運送標籤會自動更新，而且您可以使用 Amazon Simple Notification Service (Amazon SNS)、文字訊息或直接在主控台中追蹤任務狀態。如需詳細資訊，請參閱 AWS Snowball Edge。

AWS Managed Services 常見問答集中的 Snowball Edge

常見問題和解答：

問：如何請求存取 AMS 帳戶中 AWS Snowball Edge 的 ？

在 AMS 中實作 Snowball Edge 是一個兩步驟的程序：

1. 提交管理 | 其他 | 其他 | 建立 (ct-1e1xtak34nx76) 變更類型，並為您的 AMS 帳戶請求 Snowball Edge 的服務角色。
2. 透過提交管理 | AWS 服務 | 自助佈建服務 | 新增變更類型 (ct-1w8z66n899dct) 來請求使用者存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_snowball_console_role`、`customer_snowball_export_role`和 `customer_snowball_import_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問： AWS Snowball Edge 在我的 AMS 帳戶中使用 有哪些限制？

完整功能 AWS Snowball Edge 可在您的 AMS 帳戶中使用。

問： AWS Snowball Edge 在我的 AMS 帳戶中使用 的先決條件或相依性是什麼？

您必須擁有上述的服務角色帳戶。

使用 AMS SSP AWS Step Functions 在您的 AMS 帳戶中佈建

使用 AMS 自助式服務佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Step Functions 的功能。 AWS Step Functions 是一種 Web 服務，可讓您使用視覺化工作流程來協調分散式應用程式和微服務元件。您可以從個別元件建立應用程式，這些元件會各自執行不同的功能或任務，讓您快速擴展及變更應用程式。Step Functions 提供可靠的方法來協調元件，並逐步完成應用程式的函數。Step Functions 提供圖形主控台，將應用程式的元件視覺化為一系列步驟。它會自動觸發和追蹤每個步驟，並在發生錯誤時重試，因此您的應用程式每次都會按照預期順序執行。Step Functions 會記錄每個步驟的狀態，因此當發生問題時，您可以快速診斷和偵錯問題。如需詳細資訊，請參閱 AWS Step Functions。

AWS Managed Services 常見問答集中的步驟函數

常見問題和解答：

問：如何請求存取 AMS 帳戶中 AWS Step Functions 的 ？

透過使用 管理 | AWS 服務 | 自助佈建服務 | 新增變更類型 (ct-1w8z66n899dct) 提交 RFC AWS Step Functions 來請求存取 。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_step_functions_role`。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

問： AWS Step Functions 在我的 AMS 帳戶中使用 有哪些限制？

完整功能 AWS Step Functions 可在您的 AMS 帳戶中使用。

問： AWS Step Functions 在我的 AMS 帳戶中使用 的先決條件或相依性是什麼？

在執行時間，Step Functions 使用的角色必須能夠存取 Step Functions 使用的服務。例如，步驟函數可以依賴 Lambda 函數。撰寫步驟函數的人可能同時建立 Lambda 函數，也需要請求存取該服務。

使用 AMS SSP 在您的 AMS 帳戶中佈建 AWS Systems Manager 參數存放區

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 AWS Systems Manager 參數存放區功能。 AWS Systems Manager 參數存放區為組態資料管理和秘密管理提供安全的階層式儲存。您可以存放密碼、資料庫字串和授權碼之類的資料做為參數值。您存放的值可以是純文字或加密資料。然後您可以使用建立參數時指定的唯一名稱來參考它的值。參數存放區具有高度可擴展性、可用性和耐用性，由 AWS 雲端提供支援。若要進一步了解，請參閱AWS Systems Manager 參數存放區。

> **Note**
>
> 如果您想要具有生命週期管理的專用秘密存放區，請使用 使用 AMS SSP AWS Secrets Manager 在您的 AMS 帳戶中佈建而非 參數存放區。Secrets Manager 可讓您自動輪換秘密，協助您滿足安全和合規要求。Secrets Manager 為 Amazon RDS 上的 MySQL、PostgreSQL 和 Amazon Aurora 提供內建整合，可透過自訂 Lambda 函數擴充到其他類型的秘密。

AWS Systems Manager AWS Managed Services 常見問答集中的參數存放區

常見問題和解答：

問：如何請求存取 AMS 帳戶中的 Systems Manager 參數存放區？

透過使用 管理 | AWS 服務 | 自助佈建服務 | 新增變更類型 (ct-1w8z66n899dct) 提交 RFC 來請求存取 AWS Systems Manager 參數存放區。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_systemsmanager_parameterstore_console_role`。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 AWS Systems Manager 參數存放區有哪些限制？

您必須使用 AWS 受管金鑰；存取會受到限制，無法建立自訂 KMS 金鑰。不過，如果需要自訂金鑰，請提交 RFC 以使用此 IAM 角色建立客戶受管金鑰 (CMK) | 進階堆疊元件 | KMS 金鑰 | 建立變更類型 (ct-1d84keiri1jhg)，`customer_systemsmanager_parameterstore_console_role`做為

IAMPrincipalsRequiringDecryptPermissions和 IAMPrincipalsRequiringEncryptPermissionsPrincipal 參數的值。建立 KMS 金鑰之後，您可以使用它建立安全字串。

問：在我的 AMS 帳戶中使用 AWS Systems Manager 參數存放區的先決條件或相依性為何？

沒有先決條件；不過，SSM 參數存放區依賴 KMS 來建立安全字串，因此您可以加密和解密儲存在參數存放區中的值。

使用 AMS SSP 在您的 AMS 帳戶中佈建 AWS Systems Manager 自動化

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 AWS Systems Manager 自動化功能。 AWS Systems Manager 自動化使用 Runbook、動作和服務配額，簡化 Amazon Elastic Compute Cloud 執行個體和其他 AWS 資源的常見維護和部署任務。它可讓您大規模建置、執行和監控自動化。Systems Manager Automation 是一種 Systems Manager 文件，可定義 Systems Manager 在受管執行個體上執行的動作。您用來執行常見維護和部署任務的 Runbook，例如在受管執行個體中執行命令或自動化指令碼。Systems Manager 包含可協助您使用 Amazon Elastic Compute Cloud 標籤以大型執行個體群組為目標的功能，以及協助您根據定義限制推展變更的速度控制。Runbook 是使用 JavaScript 物件標記法 (JSON) 或 YAML 撰寫。使用 Systems Manager Automation 主控台中的 Document Builder (文件建置器)，不過，您可以建立 Runbook，而無需以原生 JSON 或 YAML 撰寫。或者，您可以使用 Systems Manager 提供的 Runbook 搭配符合您需求的預先定義步驟。若要進一步了解，請參閱 AWS Systems Manager 文件中的使用 Runbook。

> **Note**
>
> 雖然 Systems Manager Automation 支援 20 種可在 Runbook 中使用的動作類型，但是在編寫要在 AMS Advanced 帳戶中使用的 Runbook 時，您可以使用有限數量的動作。同樣地，Systems Manager 提供的 Runbook 數量有限，可以直接使用，也可以從您自己的 Runbook 中使用。如需詳細資訊，請參閱下列常見問答集中的限制。

AWS Systems Manager AWS Managed Services 中的自動化常見問答集

常見問題和解答：

問：如何請求存取 AMS 帳戶中的 Systems Manager Automation？

透過使用 管理 | AWS 服務 | 自助佈建服務 | 新增變更類型 (ct-1w8z66n899dct) 提交 RFC 來請求存取 AWS Systems Manager 自動化。此 RFC 會將下列 IAM 角色佈建至您的帳

戶：customer_systemsmanager_automation_console_role。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 AWS Systems Manager 自動化有哪些限制？

您必須使用有限的一組 Systems Manager 支援動作來撰寫 Runbook，才能在受管執行個體內執行命令和/或指令碼。您可以搭配任何限制使用的動作概述如下。

AWS Systems Manager 自動化限制

動作	描述	限制
aws：assertAwsResou rceProperty –	宣告 AWS 資源狀態或事件狀態	僅限 EC2 執行個體
aws：aws：branch –	執行條件式自動化步驟	無限制
aws：createTags –	建立 AWS 資源的標籤	僅適用於您撰寫的 SSM 自動化 Runbook
aws：executeAutomation –	執行另一個自動化	只有您撰寫的自動化 Runbook
aws：executeScript –	執行指令碼	僅限不對任何 服務進行任何 API 呼叫的指令碼
aws：暫停 –	暫停自動化	無限制
aws：runCommand –	在受管執行個體上執行命令	僅使用 System Manager 提供的文件 - AWS-RunShellScript 和 AWS-RunPowerShellScript
aws：sleep –	延遲自動化	無限制
aws：waitForAwsReso urceProperty –	等待 AWS 資源屬性	僅限 EC2 執行個體

您也可以選擇使用 Systems Manager 提供的 Runbook AWS-RunShellScript 和 AWS-RunPowerShellScript，從 Systems Manager 主控台使用「執行命令」功能直接執行命令或指令碼。您也可以將這些 Runbook 巢狀化為 Runbook，以因應額外的驗證前和/或驗證後或任何複雜的自動化邏輯。

該角色遵循最低權限原則，並且只提供在受管執行個體中撰寫、執行和擷取 Runbook 執行命令和/或指令碼所需的許可。它不會為 AWS Systems Manager 服務提供的任何其他功能提供許可。雖然此功能可讓您撰寫自動化 Runbook，但執行 Runbook 無法以 AMS 擁有的資源為目標。

問：在我的 AMS 帳戶中使用 AWS Systems Manager 自動化的先決條件或相依性是什麼？

沒有先決條件；不過，您必須確保在撰寫 Runbook 時遵循內部程序和/或合規控制。我們也建議在針對生產資源執行 Runbook 之前，先徹底測試 Runbook。

問：Systems Manager 政策是否可以**`customer_systemsmanager_automation_policy`**連接到其他 IAM 角色？

否，與其他已啟用自行佈建的服務不同，此政策只能指派給佈建的預設角色 `customer_systemsmanager_automation_console_role`。

與其他 SSPS 角色的政策不同，此 SSM SSPS 政策無法與其他自訂 IAM 角色共用，因為此 AMS 服務僅適用於在受管執行個體內執行命令或自動化指令碼。如果這些許可被允許連接到其他自訂 IAM 角色，可能具有其他服務的許可，則允許的動作範圍可以擴展到受管服務，並可能降低您帳戶的安全狀態。

若要根據我們的 AMS 技術標準評估任何變更請求 (RFCs)，請使用各自的 Cloud Architect 或服務交付管理員，請參閱 RFC 安全性審查。

> **Note**
>
> AWS Systems Manager 可讓您使用與 帳戶共用的 Runbook。我們建議您在使用共用 Runbook 時小心謹慎，並執行盡職調查檢查，並確保在執行 Runbook 之前檢閱內容以了解其執行的命令/指令碼。如需詳細資訊，請參閱共用 SSM 文件的最佳實務。

使用 AMS SSP AWS Transfer Family 在您的 AMS 帳戶中佈建

使用 AMS 自助式服務佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 AWS Transfer Family (Transfer 系列） 功能。 AWS Transfer Family 是一種全受管 AWS 服務，可讓您透過安全檔案傳輸通訊協定 (SFTP) 傳輸檔案，進出 Amazon Simple Storage Service (Amazon S3) 儲存體。SFTP 也稱為 Secure Shell (SSH) 檔案傳輸通訊協定。SFTP 已應用在不同業界間的資料交換工作流程，例如金融服務、健保、廣告、零售等。

透過 AWS SFTP，您可以在 中存取 SFTP 伺服器， AWS 而不需要執行任何伺服器基礎設施。您可以使用此服務將以 SFTP 為基礎的工作流程遷移至 ， AWS 同時維持最終使用者的用戶端和組態。您

必須先將主機名稱與 SFTP 伺服器端點建立關聯，然後新增您的使用者，並以適當的存取層級佈建他們。完成後，使用者的傳輸請求會直接從 AWS SFTP 伺服器端點服務。若要進一步了解，請參閱AWS Transfer for SFTP，也請參閱建立啟用 SFTP 的伺服器。

AWS Transfer for SFTP 在 AWS Managed Services 常見問答集中

常見問題和解答：

問：如何請求存取 AMS 帳戶中 AWS Transfer for SFTP 的 ？

透過使用 管理 | AWS 服務 | 自助佈建服務 | 新增變更類型 (ct-1w8z66n899dct) 提交 RFC AWS Transfer for SFTP 來請求存取 。透過此 RFC，會在您的帳戶中佈建下列 IAM 角色和政策：

- `customer_transfer_author_role`。 此角色旨在讓您透過主控台管理 SFTP 服務。
- `customer_transfer_sftp_server_logging_role`。 此角色旨在連接到 SFTP 伺服器。它允許 SFTP 伺服器將日誌提取到 CloudWatch。
- `customer_transfer_sftp_user_role`。 此角色旨在連接到 SFTP 使用者。它允許 SFTP 使用者與 S3 儲存貯體互動。
- `policy customer_transfer_scope_down_policy`。 此政策是縮小範圍的政策，可套用至 SFTP 使用者，以將 S3 儲存貯體的存取權限制在其主資料夾。
- `customer_transfer_sftp_efs_user_role`。 此角色旨在連接到 SFTP 使用者。它允許 SFTP 使用者與 EFS 檔案系統互動。

在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問： AWS Transfer for SFTP 在我的 AMS 帳戶中使用 有哪些限制？

AWS SFTP 組態的傳輸僅限於沒有「AMS-」或「MC-」字首的資源，以防止對 AMS 基礎設施進行任何修改。

問： AWS Transfer for SFTP 在我的 AMS 帳戶中使用 的先決條件或相依性是什麼？

- 在建立 AWS Transfer for SFTP 伺服器和使用者之前，您必須擁有名稱包含關鍵字「傳輸」的 Amazon S3 儲存貯體。
- 若要使用「客戶識別提供者」，您必須部署 API Gateway、Lambda 函數和使用者儲存庫 (AD、Secrets Manager 等）。如需詳細資訊，請參閱啟用 AWS Transfer for SFTP 使用 和使用身分提供者的密碼身分驗證 AWS Secrets Manager。 https://docs.aws.amazon.com/transfer/latest/userguide/authenticating-users.html

使用 AMS SSP AWS Transit Gateway 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Transit Gateway 的功能。 AWS Transit Gateway 是一種服務，可讓您將 Amazon Virtual Private Cloud (VPCs) 和內部部署網路連線至單一閘道。隨著執行中的工作負載數量增加 AWS，您需要能夠跨多個帳戶和 Amazon VPCs 擴展網路，以跟上成長速度。今天，您可以使用對等互連來連接對 Amazon VPCs。不過，在不能夠集中管理連線政策的情況下，管理多個 Amazon VPCspoint-to-point連線，可能成本高昂且繁瑣。對於內部部署連線，您需要將 AWS VPN 連接到每個個別的 Amazon VPC。此解決方案在 VPCs 數量增加到數百個時，建置和難以管理可能會很耗時。如需詳細資訊，請參閱 AWS Transit Gateway。

AWS Transit Gateway 在 AWS Managed Services 常見問答集中

常見問題和解答：

問：如何請求存取 AMS 帳戶中 AWS Transit Gateway 的 ？

透過使用 管理 | AWS 服務 | 自助佈建服務 | 新增變更類型 (ct-1w8z66n899dct) 提交 RFC AWS Transit Gateway 來請求存取 。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_tgw_console_role`。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

問： AWS Transit Gateway 在我的 AMS 帳戶中使用 有哪些限制？

完整功能 AWS Transit Gateway 可在您的 AMS 單一帳戶登陸區域帳戶中使用，但 Transit Gateway 路由的路由表修改除外。透過提交管理 | 其他 | 其他 | 建立變更類型 (ct-1e1xtak34nx76) 來請求路由表變更。

> **Note**
>
> 此服務僅支援單一帳戶登陸區域 (SALZ)，不支援多帳戶登陸區域 (MALZ)。

問： AWS Transit Gateway 在我的 AMS 帳戶中使用 的先決條件或相依性是什麼？

AWS Transit Gateway 您的 AMS 帳戶中沒有要使用的先決條件或相依性。

使用 AMS SSP 在您的 AMS 帳戶中佈建 AWS WAF Web 應用程式防火牆

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS WAF 的功能。 AWS WAF 是一種 Web 應用程式防火牆 (AWS WAF)，可協助保護您的 Web 應用程式免受可能影響應用程式可用性、危及安全性或耗用過多資源的常見 Web 入侵。透過定義可自訂的 Web 安全規則， AWS WAF 您可以控

制 Web 應用程式要允許或封鎖哪些流量。您可以使用 AWS WAF 建立自訂規則來封鎖常見的攻擊模式，例如 SQL Injection 或跨網站指令碼；以及專為您的特定應用程式設計的規則。

若要進一步了解，請參閱 AWS WAF - Web Application Firewall。

AMS 不支援監控 (CloudWatch 警示/事件/MS 警示） AWS WAF。由於 的性質 AWS WAF，您必須為您的應用程式建立自訂規則；AMS 無法在沒有應用程式內容的情況下為您量化和建立警示。若要進一步了解，請參閱 AWS WAF - Web Application Firewall。

AWS WAF 在 AWS Managed Services 常見問答集中

常見問題和解答：

問：如何 AWS WAF 請求在我的 AMS 帳戶中設定 ？

透過 管理 | AWS 服務 | 自助佈建服務 | 新增變更類型 (ct-1w8z66n899dct) 提交 RFC AWS WAF 來請求存取 。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_waf_role`。在您的帳戶中佈建 AWS WAF IAM 角色之後，您必須在聯合解決方案中加入該角色。

問：使用 有哪些限制 AWS WAF？

佈建許可後，您即擁有 的完整功能 AWS WAF。

問：要使用哪些先決條件或相依性 AWS WAF？

AWS WAF 您的 AMS 帳戶中沒有要使用的先決條件或相依性。

使用 AMS SSP AWS Well-Architected Tool 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Well-Architected Tool 的功能。AWS Well-Architected Tool 可協助您檢閱工作負載的狀態，並將其與最新的 AWS 架構最佳實務進行比較。此工具以 AWS Well-Architected Framework 為基礎，旨在協助雲端架構師建置安全、高效能、彈性且高效率的應用程式基礎設施。此架構為您提供評估架構的一致方法，已在解決方案架構團隊執行 AWS 的數萬個工作負載檢閱中使用，並提供指引，以協助實作可隨時間擴展應用程式需求的設計。如需詳細資訊，請參閱 AWS Well-Architected Tool。

AWS WA Tool 在 AWS Managed Services 常見問答集中

常見問題和解答：

問：如何請求存取 AMS 帳戶中 AWS Well-Architected Tool 的 ？

透過使用 管理 | AWS 服務 | 自行佈建服務 | 新增變更類型 (ct-1w8z66n899dct) 提交 RFC AWS Well-Architected Tool 來請求存取 。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_well_architected_tool_console_admin_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問： AWS Well-Architected Tool 在我的 AMS 帳戶中使用 有哪些限制？

完整功能 AWS Well-Architected Tool 可在您的 AMS 帳戶中使用。

問： AWS Well-Architected Tool 在我的 AMS 帳戶中使用 的先決條件或相依性是什麼？

AWS Well-Architected Tool 您的 AMS 帳戶中沒有要使用的先決條件或相依性。

使用 AMS SSP AWS X-Ray 在您的 AMS 帳戶中佈建

使用 AMS 自助式服務佈建 (SSP) 模式直接在您的 AMS 受管帳戶中存取 AWS X-Ray (X-Ray) 功能。AWS X-Ray 可協助開發人員分析和偵錯生產、分散式應用程式，例如使用微服務架構建置的應用程式。透過 X-Ray，您可以了解應用程式及其基礎服務的效能，以識別效能問題和錯誤的根本原因並進行故障診斷。X-Ray 會在請求通過您的應用程式時，提供請求的end-to-end檢視，並顯示應用程式基礎元件的映射。您可以使用 X-Ray 來分析開發中和生產中的應用程式，從簡單的三層應用程式到由數千種服務組成的複雜微服務應用程式。如需詳細資訊，請參閱 AWS X-Ray。

AWS Managed Services 常見問答集中的 X-Ray

常見問題和解答：

問：如何請求存取 AMS 帳戶中 AWS X-Ray 的 ？

透過提交管理 | AWS 服務 | 自助佈建服務 | 新增 (ct-1w8z66n899dct) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_xray_console_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。此外，您必須擁有 `customer_xray_daemon_write_instance_profile`，才能將資料從 Amazon EC2 執行個體推送至 X-Ray。當您收到 時，就會建立此執行個體描述檔`customer_xray_console_role`。

您可以向 AMS Operations 提交服務請求，將 `customer_xray_daemon_write_policy` 指派給現有的執行個體描述檔，也可以使用 AMS Operations 為您啟用 X-Ray 時建立的執行個體描述檔。

問： AWS X-Ray 在我的 AMS 帳戶中使用 有哪些限制？

除了使用 AWS KMS 金鑰 (KMS 金鑰) 加密之外，您的 AMS 帳戶中 AWS X-Ray 提供 的完整功能。預設會 AWS X-Ray 加密所有追蹤資料。根據預設，X-Ray 會加密追蹤和靜態相關資料。如果您需要使

用金鑰加密靜態資料，您可以選擇受管 KMS 金鑰 AWS(aws/xray) 或 KMS 客戶受管金鑰。對於適用於 X-Ray 加密的 KMS 客戶受管金鑰，請提交管理 | 其他 | 其他 | 建立變更類型 (ct-1e1xtak34nx76)。

問： AWS X-Ray 在我的 AMS 帳戶中使用 的先決條件或相依性是什麼？

AWS X-Ray 具有對 Amazon S3、CloudWatch 和 CloudWatch Logs 的相依性，這些日誌已在 AMS 帳戶中實作。暫時性相依性會根據資料來源和功能可能互動 AWS AWS X-Ray 的其他服務 （ 例如 Amazon Redshift、Amazon RDS、Athena) 而有所不同。

使用 AMS SSP 在您的 AMS 帳戶中佈建 VM Import/Export

使用 AMS 自助式佈建 (SSP) 模式，直接在您的 AMS 受管帳戶中存取 VM Import/ Exportcapabilities。VM Import/Export 可讓您輕鬆地將虛擬機器映像從現有環境匯入 Amazon EC2 執行個體，並將其匯出回內部部署環境。此方案可讓您利用在虛擬機器中現有的投資，透過將這些虛擬機器作為ready-to-use型執行個體帶入 Amazon EC2 來滿足您的 IT 安全性、組態管理和合規要求。您也可以將匯入的執行個體匯出回內部部署虛擬化基礎設施，讓您跨 IT 基礎設施部署工作負載。若要進一步了解，請參閱 VM Import/Export。

AWS Managed Services 常見問答集中的 VM Import/Export

常見問題和解答：

問：如何請求存取 AMS 帳戶中的 VM Import/Export？

透過使用 Management | AWS service | Self-visioned service | Add change type (ct-1w8z66n899dct) 提交 RFC，請求存取 VM Import/Export。此 RFC 會將下列 IAM 政策佈建至您的帳戶：`customer_vmimport_policy`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

需要額外的角色，即 VM Import/Export Service 角色，服務才能在您的帳戶中執行動作。

問：在我的 AMS 帳戶中使用 VM Import/Export 有哪些限制？

- AMS VM Import/Export 提供匯入自訂機器映像和資料磁碟區的功能。不過，已縮小 S3 的許可範圍，將動作限制為符合名稱的儲存貯體，`customer-vmimport-*`以限制對帳戶內資訊的存取。
- AMS VM Import/Export 支援映像和快照匯入。不過，由於安全措施，執行個體匯入和執行個體匯出功能無法使用。
- 此外，匯出功能已停用，以降低匯出受限和敏感資料的風險。

問：在我的 AMS 帳戶中使用 VM Import/Export 的先決條件或相依性是什麼？

- 您必須提供支援的磁碟映像，才能匯入 AWS 環境。如需詳細資訊，請參閱 VM Import/Export Requirements。
- VM Import/Export 無法透過 AWS 主控台存取。您必須透過 AWS CLI AWS Tools for PowerShell或 AWS SDKs 存取此服務。或者，您可以透過提交變更類型 ct-117rmp64d5mvb 來請求執行個體描述檔：部署 | 進階堆疊元件 | Identity and Access Management (IAM) | 建立 EC2 執行個體描述檔。此執行個體描述檔可讓工具從執行個體執行命令。

客戶受管模式

AWS Managed Services (AMS) 客戶受管模式提供靈活且可根據您的需求進行調整的控管模型。對於 AMS 無法為您操作的服務和應用程式，這可以被視為備用選項。AMS 不會操作在此模式下建立之帳戶中託管的基礎設施。不過，您可以在此模式中利用集中式多帳戶管理。在此模式下，可以使用下列多帳戶登陸區域功能：

- 自動化帳戶部署
- 網路帳戶中透過 Transit Gateway 的連線
- AMS Config 規則程式庫
- 將日誌副本儲存在日誌帳戶中
- 將客戶受管 Guard Duty 警示彙總至安全帳戶
- Consolidated Billing (合併帳單)
- 啟用自訂服務控制政策。

例如：如果您想要在 Ubuntu Pro 上執行工作負載，而 Ubuntu Pro 不是由 AMS 管理的作業系統，您可以使用客戶受管帳戶來託管它。您也可以透過客戶受管帳戶合併工作負載，以利用透過跨 AWS 組織共用提供的預留執行個體/共享計劃的大量折扣。

Customer Managed 模式入門

AMS 客戶受管模式可透過特殊的多帳戶登陸區域應用程式帳戶使用。

如需詳細資訊，包括如何建立客戶受管應用程式帳戶，請參閱客戶受管應用程式帳戶。

AMS 和 AWS Service Catalog

AWS Managed Services (AMS) 中的 Service Catalog 可讓組織建立和管理 AWS 資訊技術 (IT) 服務的目錄，並讓 IT 管理員建立、管理和分發已核准產品的目錄給帳戶中的最終使用者，然後他們可以在個

人化的服務入口網站中存取他們所需的產品。管理員可以控制哪些使用者可以存取每個產品，以強制遵守組織業務政策。管理員也可以設定角色，讓最終使用者只需要 IAM 存取 Service Catalog，即可部署核准的資源。Service Catalog 可讓您的組織受益於提高靈活性和降低成本，因為最終使用者可以從您控制的目錄中找到並啟動他們所需的產品。

Service Catalog 為您提供 AMS 變更請求 (RFC) 程序的替代方案，用於佈建和更新 AMS 受管帳戶中的資源。AMS 會針對透過 Service Catalog 佈建的所有基礎設施資源，管理大規模執行 AWS 所需的所有基礎設施操作任務，包括安全性、合規性、佈建、可用性、修補程式、監控、提醒、報告、事件回應和成本最佳化。在您的 AMS 受管帳戶中使用 Service Catalog 可為您提供一種機制，以集中管理經常部署的 IT 服務，並協助您實現一致的控管，同時允許使用者僅將他們所需的已核准 IT 服務快速部署到其受管環境中。

Service Catalog 入門

若要開始使用 AMS 中的 Service Catalog，請透過 AMS 主控台提交服務請求，以請求存取 Service Catalog。提交請求時，三個 IAM 角色將部署到您的 帳戶 （以及包含叫用 AMS `Transform`的 CloudFormation 巨集） 的 AMS 受管堆疊中，以便我們可以在系統中註冊產品，並對透過 Service Catalog 佈建的基礎設施執行操作。部署的三個 IAM 角色包括 IT 管理員以 Service Catalog 管理員身分管理產品的角色；應用程式擁有者和最終使用者設定、啟動和管理產品的角色；以及將用作啟動限制的角色，定義 Service Catalog 在啟動或更新產品時將使用的許可。

開始之前，AMS 中的 Service Catalog

Service Catalog 是否會取代現有的 AMS 變更請求 (RFC) 程序？

在啟用 Service Catalog 的帳戶中，它將充當變更管理系統，您可以在其中透過預先定義的產品目錄在 AMS 帳戶中佈建和更新 IT 服務；AMS 將提供預設產品組合/產品目錄，而且您的 IT 管理員可以建立和設定您自己的 。Service Catalog 只會認可透過 Service Catalog 佈建的堆疊。同樣地，透過 Service Catalog 佈建的服務將無法透過 AMS RFC 程序進行修改，因為在 Service Catalog 之外進行修改會將堆疊偏離核准的產品組態。

我可以在 AMS 主控台中查看透過服務目錄佈建的堆疊嗎？

是。您可以在 AMS 主控台中檢視透過服務目錄佈建的所有堆疊。透過服務目錄佈建的堆疊可透過「SC-」的堆疊 ID 輕鬆識別。雖然堆疊可在 AMS 主控台中檢視，但您將無法透過 AMS RFC 程序進行更新。AMS 變更管理系統 (RFCs的存取權僅限於存取請求、修補程式協同運作和備份 RFCs。

如果我透過 Service Catalog 佈建和/或更新堆疊，AMS 主控台中是否會有對應的 RFC？

AMS 主控台中顯示的唯一 RFC 是在最初佈建堆疊時向 AMS 註冊堆疊的 RFC。透過 Service Catalog 啟動堆疊時觸發的 AMS 驗證程序會自動提交此 RFC。所有其他佈建和變更都會直接在

Service Catalog 中追蹤，並且可以在 Service Catalog 主控台中檢視。此外，您可以使用 Service Catalog 中的佈建產品計畫功能，檢視在佈建或更新產品之前將對資源進行的變更清單。

我是否必須執行在 AMS 受管帳戶中佈建產品的特定動作？

是。在 AMS 帳戶中佈建的所有 Service Catalog 產品都必須在定義該產品的 CFN 範本中包含此行 JSON：

```
"Transform":{"Name":"AmsStackTransform","Parameters":{"StackId":
{"Ref":"AWS::StackId"}}}
```

此 CloudFormation 程式碼片段會觸發在 AMS 受管帳戶中佈建資源之前所需的 AMS 驗證。您有責任將此程式碼行包含在產品定義中。如果未包含，佈建將會失敗，並顯示下列錯誤訊息：「無法建立產品。此帳戶由 AMS 管理。AMS 帳戶中的所有產品都必須在範本中具有 AMS `Transform`程式碼。」

AMS 客戶在啟動時是否有任何 Service Catalog 功能無法使用和/或受限？

是，下列 SC 功能在初始啟動時不適用於 AMS 客戶：

- 透過 Service Catalog 建立帳戶
- 能夠在 AMS 受管帳戶中透過 Service Catalog 啟動所有 AWS 服務。AWS 服務可用性僅限於 AMS 支援的服務（受管和自行佈建）。如需 AMS 支援服務的詳細資訊，請參閱 AMS 服務描述。
- Service Catalog IT Service Manager (ITSM) 連接器不會與 AMS 事件報告和服務請求通訊。
- 能夠利用 Service Catalog 快速啟動和參考架構，無需修改。請記住，適用於 AMS 帳戶的 Service Catalog 產品必須包含此行 JSON 程式碼：

  ```
  "Transform":{"Name":"AmsStackTransform","Parameters":{"StackId":
  {"Ref":"AWS::StackId"}}}
  ```

  CNF 範本中的 。請注意，此行不是典型 AWS CloudFormation 範本的一部分，必須明確新增。
- AMS 目前不支援佈建 Service Catalog 產品的 Terraform。
- AMS 不支援 AWS CFN 堆疊集。
- 您無法建立自訂 IAM 角色。
- 服務動作僅限於：
  - AWS-RebootRdsInstance
  - AWS-RestartEC2Instance

- AWS-StartEC2Instance
- AWS-StartRdsInstance
- AWS-StopEC2Instance
- AWS-StopRdsInstance
- AWS-CreateImage
- AWS-CreateRdsSnapshot
- AWS-CreateSnapshot

> **Note**
>
> 建立服務動作時，您可以將執行角色設定為最終使用者的許可、啟動角色或您選擇的自訂 IAM 角色。選取的執行角色必須具有足夠的許可才能執行服務動作，並具有 TrustPolicy，允許 Service Catalog 擔任該角色，否則該服務動作會在執行時失敗。我們建議使用 AWSManagedServicesServiceCatalogLaunchRole，它具有正確的許可和信任政策，可用作服務動作。

使用 AMS RFC 系統所需的用途為何？

在一般可用性 (GA) 時，您仍然需要使用 RFCS 來執行下列動作：

- 設定修補程式協調器
- 設定備份政策
- 請求執行個體存取
- 建立和指派 AMS 準則以外的安全群組。
- 執行工作負載擷取 (WIGS)
- 建立 IAM 角色

我可以使用 Service Catalog CLI 來存取 AMS 受管帳戶中的 Service Catalog 嗎？

是，可透過 CLI 使用並啟用 Service Catalog APIs。可透過佈建和終止這些成品來管理 Service Catalog 成品的動作可供使用。如需詳細資訊，請參閱 AWS Service Catalog 資源，或下載最新的 AWS 開發套件或 CLI。

誰會建立、管理和分發客戶的核准產品目錄？

客戶的目錄管理員和/或 IT 管理員或指派的資源負責管理您的 Service Catalog 目錄和核准的產品。

我可以使用 AMS AMIs嗎？

2020 年 3 月之後提供的 AMS AMIs 可透過 AWS Service Catalog 部署。

如何使用 Service Catalog 遷移至 AMS？

若要使用 Service Catalog 將工作負載遷移至 AMS，請先依照工作負載擷取 (WIGs) 程序在 AMS 中建立 AMI。您可以使用 WIGS 產生的 AMI 在 Service Catalog 中建立產品。如何執行此操作，請參閱 AWS Service Catalog - 入門。

AMS 多帳戶登陸區域 (MALZ) 加入

MALZ 網路架構

關於多帳戶登陸區域網路架構

在您開始 AWS Managed Services (AMS) 多帳戶登陸區域 (MALZ) 的加入程序之前，請務必了解 AMS 代表您建立的基準架構或登陸區域、其元件和函數。

AMS 多帳戶登陸區域是一種多帳戶架構，已預先設定基礎設施，以促進身分驗證、安全性、聯網和記錄。

> **Note**
>
> 如需成本的預估，請參閱 AMS 多帳戶登陸區域環境基本元件。

主題

- 服務區域
- 組織單位
- 服務控制政策和 AWS Organization

下圖以高層級概述帳戶結構，以及如何將基礎設施隔離到每個帳戶：

服務區域

由於 Active Directory 和 Transit Gateway 目前的跨區域限制，AMS 多帳戶登陸區域內的所有資源都會部署在您選擇的單一 AWS 區域內。

組織單位

典型的 AMS 多帳戶登陸區域由四個最上層組織單位 (OUs) 組成：

- 核心組織單位 (OU)（用來將帳戶分組，以單一單位形式管理）
- 應用程式 OU

- 客戶管理的 OU
- 加速 OU

AMS 受管多帳戶登陸區域也可讓您建立自訂 OUs以分組和組織 AWS 帳戶，並將自訂 SCPs 與其建立關聯；如需執行此操作的範例，請參閱管理帳戶 | 建立自訂 OUs和管理帳戶 | 分別建立自訂 SCP （需要檢閱）。AMS 提供四個可請求新 OUs 和帳戶的現有 OUs：加速、應用程式 > 受管、應用程式 > 開發和客戶受管。

- 加速 OU：

  這是 AMS 多帳戶登陸區域 (MALZ) 中最上層的 OU。此 OU 下的帳戶是由具有 RFC 的 AMS 佈建（部署 | 受管登陸區域 | 管理帳戶 | 建立加速帳戶，變更類型 ID：ct-2p93tyd5angmi)。在這些加速應用程式帳戶中，您可以受益於加速營運服務，例如監控和提醒、事件管理、安全管理和備份管理。如需詳細資訊，請參閱 AMS Accelerate 帳戶。

- 應用程式 > 受管 OU：

  在 Application OU 的這個子組織單位中，帳戶完全由 AMS 管理，包括所有操作任務。操作任務包括服務請求管理、事件管理、安全管理、持續性管理、修補程式管理、成本最佳化、監控和事件管理。這些任務會針對您基礎設施的管理執行。您可以視需要建立多個子 OUs，直到達到 AWS 組織的巢狀 OUs 上限為止。如需詳細資訊，請參閱 AWS Organizations 的配額。

- 應用程式 > 開發 OU：

  在 AMS 受管登陸區域中應用程式 OU 的這個子 OU 下，帳戶是開發人員模式帳戶，可提供您在 AMS 變更管理程序之外佈建和更新 AWS 資源的更高許可。此 OU 也支援視需要建立新的子系 OU。

- 客戶受管 OU：

  這是 AMS 多帳戶登陸區域中最上層的 OU。此 OU 下的帳戶是由 AMS 使用 RFC 佈建。在這些帳戶中，工作負載和 AWS 資源的操作是您的責任。此 OU 也支援視需要建立新的子系 OU。

根據最佳實務，我們建議這些 OUs 和自訂請求的子 OUs 下的帳戶根據其功能和政策進行分組。

服務控制政策和 AWS Organization

AWS 為 AWS Organization 中的許可管理提供服務控制政策 (SCPs)。SCPs用於為使用者可以在哪些 OUs 中執行的動作定義額外的護欄。根據預設，AMS 提供一組部署在管理帳戶中SCPs，可在不同的預設 OU 層級提供保護。如需 SCP 限制，請聯絡您的 CSDM。

您也可以建立自訂 SCPs並將其連接至特定 OUs。您可以使用變更類型 ct-33ste5yc7hprs 從您的 管理帳戶請求它們。AMS 接著會檢閱請求SCPs，再將其套用至目標 OUs。如需範例，請參閱管理帳戶 | 建立自訂 OUs和管理帳戶 | 建立自訂 SCP （需要檢閱）。

選擇單一 MALZ 或多個 MALZs

下表提供在單一多帳戶登陸區域 (MALZ) 與多個多帳戶登陸區域 （例如兩個多帳戶登陸區域 - Prod 和非 Prod) 之間決定的一些高層級考量。一般而言，選擇取決於個別需求、法律要求和操作實務。

單一多帳戶登陸區域與多個多帳戶登陸區域

實體	單一 AMS 登陸區域	多個 （兩個或更多） 登陸區域
基本成本	較低，最佳化程度約為每月 3，000 美元。	較高，每個環境的額外費用約為 3，000 美元。
計費	單一帳單，因為單一帳單/管理帳戶。	每個多帳戶登陸區域的單獨帳單。目前，AWS Org 不支援單一帳單的多管理帳戶。
現有預留執行個體 (RIs可攜性	低。AWS RIs目前無法跨多個帳單帳戶轉換。您會將現有的 RIs 重新用於多帳戶登陸區域。	更低。您會在所有多帳戶登陸區域重新利用和分配 RIs。
產品分層折扣	高。請參閱磁碟區折扣。	低。請參閱磁碟區折扣。
初始設定額外負荷 （在專案/遷移時間表上）	低。Active Directory、聯網和單一登入 (SSO) 整合僅限一次。	高。您將為每個登陸區域執行 Active Directory、網路整合和 SSO 整合。這可能會導致任何遷移專案的潛在延遲。
常見服務可設定性	工作量低。您可以設定常見/共用的服務，例如 DNS、備份、監控、記錄等。	大量努力。需要額外的規劃，以解決常見的基礎設施或服務將位於何處。通過每個登陸區域中多個傳輸閘道 (TGWs) 的流量周遊可能會導致額外費用。
可擴展性	中。AMS 目前的實際限制為每個多帳戶登陸區域 150 個帳戶。在同一帳戶中執行應用程式的多個團隊或供應商可以存取不同團隊擁有的堆疊。透過	高。能夠利用多個多帳戶登陸區域來分配帳戶，同時實現帳戶或應用程式層級的隔離。管理大量帳戶可能會導致營運或成本開銷。

實體	單一 AMS 登陸區域	多個（兩個或更多）登陸區域
	控制 ServiceNow 層的應用程式特定堆疊存取權（整合 AMS ServiceNow Connector 應用程式和使用標籤），可以減輕此限制。詢問 AMS 技術交付管理員 (TDMs) 或雲端架構師 (CAs) 如何實作。	
營運風險	（相依）低。只有一次操作整合和整備。降低程序偏離的機率。	（相依）低。多個整合和操作活動。在此期間多個登陸區域中的偏離可能會導致操作風險。
多 AWS 區域	單一 AWS 區域。AMS 多帳戶登陸區域僅限於單一 AWS 區域。若要跨越多個 AWS 區域，請使用多個多帳戶登陸區域。	多 AWS 區域。使用多個多帳戶登陸區域，您可以將每個 MALZ 部署在一個區域中，並使用傳輸閘道 (TGW) 對等互連。
帳戶遷移或可攜性	是。可以在同一個 AWS Organization 中將帳戶從一個 OU 移至另一個 OU。	否。AMS 不支援跨登陸區域遷移帳戶，也就是跨 AWS Organizations。工作負載可以使用傳輸閘道 (TGW) 或 VPC 對等互連跨登陸區域進行連接。
變更管理	中。對 TGW、Active Directory (AD) 或傳出（輸出）等常見元件進行破壞性變更可能會影響多帳戶登陸區域中的所有工作負載。不過，對 AMS 受管元件的變更會在內部測試，並在滾動更新中推送。	低。對 TGW、AD 或傳出（輸出）等常見元件進行破壞性變更只會影響該特定多帳戶登陸區域中的工作負載。
資料和存取控制	（相依）如果您想要連線至適用於 Prod 和非 Prod 工作負載的不同內部部署 ADs 和網路，請使用低控制。SAML 聯合、TGW 網域和安全群組 (SGs) 也有助於實作必要的控制項。	（相依）如果您想要連線至適用於 Prod 和非 Prod 工作負載的不同內部部署 ADs 和網路，請進行高度控制。針對嚴格的合規要求，使用個別的登陸區域。

實體	單一 AMS 登陸區域	多個（兩個或更多）登陸區域
合規與安全	（相依）如果有嚴格的合規需求，需要完全隔離材料與非材料工作負載，則為低。AMS 標準預防性和偵測性控制已就緒。	（相依）由於多個多帳戶登陸區域可以透過完全隔離材料與非材料工作負載，協助達成嚴格的合規要求。AMS 標準預防性和偵測性控制已就緒。

建議：如果沒有嚴格的合規或多區域需求，從單一 AMS 多帳戶登陸區域開始，將在成本、安全性、卓越營運和遷移複雜性之間取得良好的平衡。如果遇到任何帳戶或業務限制，您可以隨時設定其他登陸區域。

單一多帳戶登陸區域與多個多帳戶登陸區域FAQs

選擇設定單一多帳戶登陸區域或多個多帳戶登陸區域時的一些常見問題：

Q1：如果遇到任何帳戶限制或業務限制，是否可以從單一多帳戶登陸區域開始，並移至多個多帳戶登陸區域？

答：是。您可以選擇在任何指定時間設定另一個多帳戶登陸區域：

- 必須設定新的帳單付款人帳戶（目前 AWS 不支援單一 AWS 組織中的多付款人帳戶）。
- 一旦填寫多帳戶登陸區域問卷，多帳戶登陸區域基礎建置最多需要 2 週的前置時間。
- 每個多帳戶登陸區域代表增加 ~3K USD/每月執行成本。
- 需要 N/W、AD、DNS 和 SSO 整合才能建立新的 MALZ。
- 任何預留執行個體 (RIs)、成本節省計劃將需要為新的多帳戶登陸區域設定 (RIs不可轉移）。
- AMS 多帳戶登陸區域不支援跨多帳戶登陸區域帳戶遷移帳戶，例如跨 AWS Orgs。不過，若要將應用程式從一個帳戶移至另一個帳戶，可以使用標準遷移方法。

Q2：什麼是對基礎/共用基礎設施進行 MALZ 更新/變更，並量化客戶風險的 AMS 方法？ 提供有關在程序中包裝哪些保證的詳細資訊。客戶如何放心 MALZ 更新/變更不會影響客戶？ 客戶是否需要採取任何措施來防止中斷？

答：AMS 使用內部工具遵循嚴格的變更方法，讓我們能夠定義、檢閱、排程和執行客戶環境的變更。

發佈更新的程序會強制執行程式碼檢閱、整合測試、在 Gamma 和 Beta 環境中部署，以及在 Beta 和 Gamma 環境中額外的製作時間和測試，然後再發佈給客戶環境。所有版本都包含轉返程序，並由版本

團隊和建立和請求變更的團隊密切監控。版本範圍僅限於 AMS 擁有和佈建的堆疊。平均而言，我們每週至少執行一個版本。

除此之外：

- AMS SLA 適用。根據 AMS 服務描述，任何事件引發的共用內部維護活動都會遵循具備解決權的 SLA 或點數。
- 客戶不需要採取特殊的預防措施，以防止對常見基礎設施造成中斷。客戶在 AWS Org 或 Core OU 帳戶中具有唯讀許可，因此客戶無法對 MALZ 核心環境進行任何破壞性變更。所有客戶對 核心基礎設施的請求都需要 AMS 審核和核准。
- 在 App OU 層級傳播變更之前，客戶可以在個別非產品帳戶層級測試特定組織層級變更，例如 SCPs/角色。它正在 AMS 藍圖上，以允許多個 APP OUs (2020 年第 2 季），這可進一步減輕進行某些 ORG 層級變更的風險。MALZ 團隊已針對「建置模式」帳戶發行個別的 OU，以確保客戶所有權和個別控制項的明確區隔。
- 其中大多數都是允許 AMS 以有效和有效率的方式操作工作負載的變更，不一定會影響客戶的工作負載。當 AMS 認為共用的基礎設施變更可能會影響客戶的工作負載，然後與客戶的變更時段保持一致。

高階建議，從多個多帳戶登陸區域開始，如果：

- 如果它可協助您達成任何特定的合規。
- 如果您需要使用多區域。
- 如果您有不同的現場部署 ADs和網路，用於生產/材料和非生產/非材料工作負載，請明確隔離 b/w 工作負載。

多帳戶登陸區域帳戶

主題

- 管理帳戶
- 網路帳戶
- 共用服務帳戶
- Log Archive 帳戶
- 安全帳戶
- 應用程式帳戶類型

- AMS 工具帳戶（遷移工作負載）

管理帳戶

當您開始使用 AMS 時，管理帳戶是您初始的 AWS 帳戶。它利用 AWS Organizations 做為管理帳戶（也稱為支付所有成員帳戶費用的付款人帳戶），讓帳戶能夠建立和財務管理成員帳戶。它包含 AWS 登陸區域 (ALZ) 架構、帳戶組態堆疊集、AWS Organization 服務控制政策 (SCPs等。

如需使用管理帳戶的詳細資訊，請參閱管理帳戶的最佳實務。

下圖提供管理帳戶中所含資源的高階概觀。

管理帳戶中的資源

除了上述標準服務之外，在加入期間，管理帳戶中不會建立其他 AWS 資源。加入 AMS 期間需要以下輸入：

- 管理帳戶 ID：您最初建立的 AWS 帳戶 ID。
- 核心帳戶電子郵件：提供與每個核心帳戶相關聯的電子郵件：聯網、共享服務、記錄和安全帳戶。
- 服務區域：提供將部署您 AMS 登陸區域所有資源的 AWS 區域。

網路帳戶

網路帳戶是 AMS 多帳戶登陸區域帳戶、內部部署網路和輸出流量之間網路路由的中樞。此外，此帳戶包含公有 DMZ 堡壘，是 AMS 工程師存取 AMS 環境中主機的進入點。如需詳細資訊，請參閱下列網路帳戶的高階圖表。

網路帳戶架構

下圖說明 AMS 多帳戶登陸區域環境，顯示跨帳戶的網路流量，並且是高可用性設定的範例。

AMS 會根據我們的標準範本和您在加入期間提供的所選選項，為您設定聯網的所有層面。標準 AWS 網路設計會套用至您的 AWS 帳戶，並為您建立 VPC，並透過 VPN 或 Direct Connect 連線至 AMS。

如需 Direct Connect 的詳細資訊，請參閱 AWS Direct Connect。標準 VPCs包括 DMZ、共用服務和應用程式子網路。在加入過程中，可能會請求和建立額外的 VPCs，以符合您的需求（例如，客戶部門、合作夥伴）。加入後，您會收到網路圖表：說明網路設定方式的環境文件。

> **Note**
>
> 如需所有作用中服務的預設服務限制和限制的相關資訊，請參閱 AWS 服務限制文件。

我們的網路設計是以 Amazon「最低權限原則」為基礎建置。為了達成此目的，我們透過 DMZ 路由所有流量、輸入和輸出，但來自信任網路的流量除外。唯一信任的網路是透過使用 VPN 和/或 AWS Direct Connect (DX) 在內部部署環境和 VPC 之間設定的網路。透過使用堡壘執行個體授予存取權，從而防止直接存取任何生產資源。您的所有應用程式和資源都位於可透過公有負載平衡器連線的私有子網路內。公有輸出流量會透過輸出 VPC 中的 NAT 閘道（在網路帳戶中）流向網際網路閘道，然後流向網際網路。或者，流量可以透過 VPN 或 Direct Connect 流向內部部署環境。

私有網路連線至 AMS 多帳戶登陸區域環境

AWS 透過虛擬私有網路 (VPN) 連線或專用線路與 AWS Direct Connect 提供私有連線。多帳戶環境中的私有連線，是使用下列其中一種方法設定：

- 使用 Transit Gateway 的集中式 Edge 連線
- 將 Direct Connect (DX) 和/或 VPN 連線至帳戶虛擬私有雲端 (VPCs)

使用傳輸閘道的集中式邊緣連線

AWS Transit Gateway 是一項服務，可讓您將 VPCs 和內部部署網路連線至單一閘道。傳輸閘道 (TGW) 可用來合併現有的邊緣連線，並透過單一輸入/輸出點路由。傳輸閘道會在您 AMS 多帳戶環境的網路帳戶中建立。如需傳輸閘道的詳細資訊，請參閱 AWS Transit Gateway。

AWS Direct Connect (DX) 閘道用於透過傳輸虛擬介面將 DX 連接連接到傳輸閘道VPCs VPNs。您將 Direct Connect 閘道與傳輸閘道建立關聯。然後，為您的 AWS Direct Connect 連線至 Direct Connect 閘道建立傳輸虛擬介面。如需 DX 虛擬介面的資訊，請參閱 AWS Direct Connect 虛擬介面。

此組態具有以下好處。您可以：

- 管理相同 AWS 區域中多個 VPCs 或 VPNs單一連線。
- 將字首從內部部署公告至 AWS，以及從 AWS 公告至內部部署。

> **Note**
>
> 如需搭配 AWS 服務使用 DX 的詳細資訊，請參閱彈性工具組一節 Classic。如需詳細資訊，請參閱傳輸閘道關聯。

若要提高連線能力，建議您從不同 AWS Direct Connect 位置將至少兩個傳輸虛擬介面連接至 Direct Connect 閘道。如需詳細資訊，請參閱 AWS Direct Connect 彈性建議。

將 DX 或 VPN 連線至帳戶 VPCs

使用此選項時，您 AMS 多帳戶登陸區域中VPCs 會直接連線至 Direct Connect 或 VPN。流量會直接從 VPCs 流向 Direct Connect 或 VPN，而不會周遊傳輸閘道。

網路帳戶中的資源

如聯網帳戶圖表所示，下列元件會在帳戶中建立，並需要您的輸入。

網路帳戶包含兩個 VPCs：輸出 VPC 和 DMZ VPC，也稱為周邊 VPC。

AWS Network Manager

AWS Network Manager 是一項服務，可讓您將傳輸閘道 (TGW) 網路視覺化，而無須支付 AMS 額外費用。它提供 AWS 資源和內部部署網路的集中式網路監控、拓撲圖和地理地圖中私有網路的單一全域檢視，以及使用率指標，例如位元組輸入/輸出、封包輸入/輸出、捨棄的封包，以及拓撲、路由和上/下連線狀態的變更提醒。如需相關資訊，請參閱AWS Network Manager。

使用下列其中一個角色來存取此資源：

- AWSManagedServicesCaseRole
- AWSManagedServicesReadOnlyRole
- AWSManagedServicesChangeManagementRole

輸出 VPC

輸出 VPC 主要用於輸出流量到網際網路，由最多三個可用區域 (AZs) 中的公有/私有子網路組成。網路位址轉譯 (NAT) 閘道佈建在公有子網路中，傳輸閘道 (TGW) VPC 連接則建立在私有子網路中。來自所有網路的輸出或傳出網際網路流量會透過 TGW 透過私有子網路進入，然後透過 VPC 路由表路由至 NAT。

對於在公有子網路中包含公開應用程式的 VPCs，來自網際網路的流量會包含在該 VPC 中。傳回流量不會路由至 TGW 或輸出 VPC，而是透過 VPC 中的網際網路閘道 (IGW) 傳回。

> **Note**
>
> 網路 VPC CIDR 範圍：建立 VPC 時，您必須以無類別網域間路由 (CIDR) 區塊的形式指定 VPC 的 IPv4 地址範圍；例如 10.0.16.0/24。這是您 VPC 的主要 CIDR 區塊。
> AMS 多帳戶登陸區域團隊建議 24 的範圍（具有更多 IP 地址），以便在未來部署其他資源/設備時提供一些緩衝。

Managed Palo Alto 輸出防火牆

AMS 提供受管 Palo Alto 輸出防火牆解決方案，可為多帳戶登陸區域環境（不包括公有服務）中的所有網路啟用網際網路繫結傳出流量篩選。此解決方案結合了領先業界的防火牆技術 (Palo Alto VM-300) 與 AMS 的基礎設施管理功能，可在合規的操作環境中部署、監控、管理、擴展和還原基礎設施。包括 Palo Alto Networks 在內的第三方無法存取防火牆；它們僅由 AMS 工程師管理。

流量控制

受管傳出防火牆解決方案會管理網域允許清單，其中包含備份和修補程式等服務所需的 AMS 網域，以及您定義的網域。當傳出網際網路流量路由到防火牆時，會開啟工作階段、評估流量，如果符合允許的網域，流量會轉送到目的地。

架構

受管輸出防火牆解決方案遵循高可用性模型，其中會根據可用區域 (AZs) 的數量部署兩到三個防火牆。解決方案利用來自預設輸出 VPC 的部分 IP 空間，但也為管理防火牆所需的其他資源佈建 VPC 延伸 (/24)。

網路流程

在高階，公有輸出流量路由保持不變，但流量從輸出 VPC 路由到網際網路的方式除外：

1. 目的地為網際網路的輸出流量會透過 VPC 路由表傳送至傳輸閘道 (TGW)
2. TGW 會透過 TGW 路由表將流量路由至輸出 VPC

3. VPC 透過私有子網路路由表將流量路由至網際網路
   a. 在預設的多帳戶登陸區域環境中，網際網路流量會直接傳送到網路位址轉譯 (NAT) 閘道。受管防火牆解決方案會重新設定私有子網路路由表，將預設路由 (0.0.0.0/0) 指向防火牆介面。

防火牆本身包含三個界面：

1. 信任的界面：用於接收要處理的流量的私有界面。
2. 不受信任的界面：將流量傳送至網際網路的公有界面。由於防火牆執行 NAT，外部伺服器接受來自這些公有 IP 地址的請求。
3. 管理界面：防火牆 API、更新、主控台等的私有界面。

在所有路由中，流量都會維持在相同的可用區域 (AZ) 內，以減少跨可用區域流量。流量只會在容錯移轉發生時跨越 AZs。

允許清單修改

加入後，`ams-allowlist`會建立名為 的預設允許清單，其中包含 AMS 所需的公有端點，以及用於修補 Windows 和 Linux 主機的公有端點。操作完成後，您可以在管理 | 受管防火牆 | 傳出 (Palo Alto) 類別下的 AMS 主控台中建立 RFC 的 ，以建立或刪除允許清單，或修改網域。請注意， `ams-allowlist`無法修改。RFC 的 是以完全自動化處理 （並非手動）。

自訂安全政策

安全政策會根據流量屬性來決定是否封鎖或允許工作階段，例如來源和目的地安全區域、來源和目的地 IP 地址，以及 服務。全自動化 RFCs支援自訂安全政策。您可以在 Management | Managed Firewall | Outbound (Palo Alto) 類別中找到建立或刪除安全政策CTs，也可以在 Deployment | Managed Firewall | Outbound (Palo Alto) 類別中找到編輯現有安全政策的 CT。您將能夠建立新的安全政策、修改安全政策或刪除安全政策。

> **Note**
>
> `ams-allowlist` 無法修改預設安全政策

CloudWatch PA 輸出儀表板

您可以在 CloudWatch 中找到兩個儀表板，以提供 Palo Alto (PA) 的彙總檢視。AMS-MF-PA-Egress-Config-Dashboard 提供 PA 組態概觀、允許清單的連結，以及包含其屬性的所有安全政策清單。AMS-

MF-PA-Egress-Dashboard 可以自訂來篩選流量日誌。例如，若要建立安全政策的儀表板，您可以使用下列篩選條件建立 RFC：

```
fields @timestamp, @message
| filter @logStream like /pa-traffic-logs/
| filter @message like /<Security Policy Name>/
| parse @message
 "*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*
 as x1, @x2, @x3, @x4, @type, @x6, @x7, @source_ip, @destination_ip, @source_nat_ip,
 @dest_nat_ip, @rule, @x13, @x14, @application, @x16, @from_zone, @to_zone,
 @x19, @x20, @x21, @x22, @session_id, @x24, @source_port, @destination_port,
 @source_nat_port, @destination_nat_port, @x29, @protocol, @action, @bytes,
 @bytes_sent, @bytes_recieved, @packets, @x36, @x37, @category, @x39, @x40, @x41,
 @source_country, @destination_country, @x44, @packets_sent, @packets_recieved,
 @session_end_reason, @x48, @x49, @x50
| display @timestamp, @rule, @action, @session_end_reason, @protocol, @source_ip,
 @destination_ip, @source_port, @destination_port, @session_id, @from_zone,
 @to_zone, @category, @bytes_sent, @bytes_recieved, @packets_sent, @packets_recieved,
 @source_country, @destination_country
```

容錯移轉模型

防火牆解決方案包含兩到三個 Palo Alto (PA) 主機 （每個可用區域一個）。運作狀態檢查 Canary 會以固定排程執行，以評估主機的運作狀態。如果主機識別為運作狀態不良，AMS 會收到通知，並透過路由表變更，自動將該 AZ 的流量轉移到不同 AZ 中運作狀態良好的主機。由於運作狀態檢查工作流程持續執行，如果主機因為暫時性問題或手動修復而再次運作狀態良好，則流量會使用運作狀態良好的主機切換回正確的可用區域。

擴展

AMS 會監控防火牆的輸送量和擴展限制。當輸送量限制超過較低的浮水印閾值 (CPU/網路） 時，AMS 會收到提醒。低浮水印閾值表示資源接近飽和，到達 AMS 將評估一段時間內指標的時間點，並尋求擴展解決方案的建議。

備份與恢復

備份會在初始啟動期間、任何組態變更後，以及定期間隔建立。初始啟動備份是以每個主機為基礎建立，但組態變更和定期間隔備份會在叫用備份工作流程時跨所有防火牆主機執行。AMS 工程師可以在這些時段之外建立其他備份，或應要求提供備份詳細資訊。

如有需要，AMS 工程師可以執行組態備份的還原。如果需要還原，則會在所有主機之間進行，以保持主機之間的組態同步。

當主機需要完整回收執行個體時，也會發生還原。佈建新的 EC2 執行個體時，會自動還原最新的備份。一般而言，主機不會定期回收，並且會保留給嚴重故障或必要的 AMI 交換。主機資源回收會手動啟動，並在資源回收發生之前通知您。

除了防火牆組態備份之外，您的特定允許清單規則會分別備份。修改您定義的允許清單規則時，會自動建立備份。如有必要，AMS 工程師可以執行允許清單備份的還原。

更新

AMS Managed Firewall Solution 需要一段時間的各種更新，才能對系統、其他功能或防火牆作業系統 (OS) 或軟體進行更新。

大多數變更不會影響執行環境，例如更新自動化基礎設施，但防火牆執行個體輪換或作業系統更新等其他變更可能會導致中斷。評估因更新造成的潛在服務中斷時，AMS 會與您協調以適應維護時段。

運算子存取

AMS 運算子會使用其 ActiveDirectory 登入資料登入 Palo Alto 裝置來執行操作（例如修補、回應事件等）。解決方案會保留標準 AMS Operator 身分驗證和組態變更日誌，以追蹤在 Palo Alto 主機上執行的動作。

預設日誌

根據預設，防火牆產生的日誌位於每個防火牆的本機儲存體中。加班，本機日誌將根據儲存使用率刪除。AMS 解決方案可將日誌從機器即時傳送至 CloudWatch 日誌；如需詳細資訊，請參閱 CloudWatch Logs 整合。

AMS 工程師仍然能夠在需要時直接從機器查詢和匯出日誌。此外，日誌可以運送到客戶擁有的 Panorama；如需詳細資訊，請參閱 全景整合。

解決方案收集的日誌如下：

RFC 狀態碼

日誌類型	描述
流量	顯示每個工作階段開始和結束的項目。每個項目都包含日期和時間、來源和目的地區域、地址和連接埠、應用程式名稱、套用至流程的安全規則名稱、規則動作（允許、拒絕或捨棄）、輸入和輸出界面、位元組數，以及工作階段結束原因。

日誌類型	描述
	類型欄指出項目是用於工作階段的開始或結束，還是工作階段遭到拒絕或捨棄。"drop" 表示封鎖指定 "any" 應用程式之流量的安全規則，而 "deny" 表示規則已識別特定應用程式。 如果在識別應用程式之前捨棄流量，例如當規則捨棄特定服務的所有流量時，應用程式會顯示為「不適用」。
威脅	顯示防火牆產生之每個安全警示的項目。每個項目都包含日期和時間、威脅名稱或 URL、來源和目的地區域、地址和連接埠、應用程式名稱，以及警示動作（允許或封鎖）和嚴重性。 類型欄指出威脅類型，例如「病毒」或「間諜軟體」；名稱欄是威脅描述或 URL；類別欄是威脅類別（例如「鍵盤記錄器」）或 URL 類別。
URL 篩選	顯示 URL 篩選條件的日誌，可控制對網站的存取，以及使用者是否可以將登入資料提交至網站。
組態	顯示每個組態變更的項目。每個項目都包含日期和時間、管理員使用者名稱、進行變更的 IP 地址、用戶端類型 (Web 介面或 CLI)、命令執行類型、命令是否成功或失敗、組態路徑，以及變更前後的值。
系統	顯示每個系統事件的項目。每個項目都包含日期和時間、事件嚴重性和事件描述。
警報	警示日誌會記錄系統所產生警示的詳細資訊。此日誌中的資訊也會在警示中報告。請參閱「定義警示設定」。
身分驗證	顯示當最終使用者嘗試存取由身分驗證政策規則控制存取的網路資源時，所發生身分驗證事件的相關資訊。使用者可以使用此資訊來協助疑難排解存取問題，並視需要調整使用者身分驗證政策。結合相互關聯物件，使用者也可以使用身分驗證日誌來識別使用者網路上的可疑活動，例如暴力破解攻擊。 或者，使用者可以設定身分驗證規則來記錄身分驗證逾時。這些逾時與使用者只需要對資源進行身分驗證一次，但可以重複存取的時間有關。查看逾時的相關資訊，有助於使用者決定是否及如何調整逾時。

日誌類型	描述
統一	在單一檢視中顯示最新的流量、威脅、URL 篩選、WildFire 提交和資料篩選日誌項目。集體日誌檢視可讓使用者一起調查和篩選這些不同類型的日誌（而不是分別搜尋每個日誌集）。或者，使用者可以選擇要顯示的日誌類型：按一下篩選欄位左側的箭頭，然後選取流量、威脅、url、資料和/或森林大火，以僅顯示選取的日誌類型。

事件管理

AMS 會持續監控防火牆的容量、運作狀態和可用性。從防火牆產生的指標，以及 AWS/AMS 產生的指標，會用來建立 AMS 操作工程師收到的警示，他們將調查並解決問題。目前的警示涵蓋下列案例：

事件警示：

- 防火牆資料平面 CPU 使用率
  - CPU 使用率 - 資料平面 CPU（處理流量）
- 防火牆資料平面封包使用率高於 80%
  - 封包使用率 - 資料平面（處理流量）
- 防火牆資料平面工作階段使用率
- 防火牆資料平面工作階段作用中
- 防火牆 CPU 使用率彙總
  - 所有 CPU CPUs 使用率
- 依可用區域進行容錯移轉
  - 在 AZ 中發生容錯移轉時的警示
- 運作狀態不佳的 Syslog 主機
  - Syslog 主機運作狀態檢查失敗

管理警示：

- 運作狀態檢查監控失敗警示
  - 當運作狀態檢查工作流程意外失敗時
  - 這是針對工作流程本身，而不是防火牆運作狀態檢查失敗時
- 密碼輪換失敗警示

- 當密碼輪換失敗時
- API/Service 使用者密碼每 90 天輪換一次

指標

所有指標都會擷取並儲存在網路帳戶中的 CloudWatch 中。您可以透過取得網路帳戶的主控台存取權，以及導覽至 CloudWatch 主控台來檢視這些屬性。您可以在指標索引標籤下檢視個別指標，也可以透過導覽至儀表板索引標籤，然後選取 AMS-MF-PA-Egress-Dashboard 來檢視特定指標和彙總指標的單一窗格儀表板檢視。

自訂指標：

- 運作狀態檢查
  - 命名空間：AMS/MF/PA/輸出
    - PARouteTableConnectionsByAZ
    - PAUnhealthyByInstance
    - PAUnhealthyAggregatedByAZ
    - PAHealthCheckLockState
- 防火牆產生
  - 命名空間：AMS/MF/PA/Egress/<instance-id>
    - DataPlaneCPUUtilizationPct
    - DataPlanePacketBuffferUtilization
    - panGPGatewayUtilizationPct
    - panSessionActive
    - panSessionUtilization

CloudWatch Logs 整合

CloudWatch Logs 整合會將日誌從防火牆轉送到 CloudWatch Logs，以降低由於本機儲存使用率而遺失日誌的風險。當防火牆產生日誌時，日誌會即時填入，並且可以透過主控台或 API 隨需檢視。

可以使用 CloudWatch Insights 建置複雜的查詢以進行日誌分析或匯出至 CSV。此外，自訂 AMS Managed Firewall CloudWatch 儀表板也會顯示特定流量日誌查詢的快速檢視，以及一段時間內流量和政策命中次數的圖形視覺化。使用 CloudWatch 日誌也可以原生整合其他 AWS 服務，例如 AWS Kinesis。

> **Note**
>
> PA 日誌無法直接轉送至現有的內部部署或第三方 Syslog 收集器。AMS Managed Firewall 解決方案可將 PA 機器的日誌即時運送到 AWS CloudWatch Logs。您可以使用 CloudWatch Logs Insight 功能來執行臨機操作查詢。此外，日誌可以運送到 Palo Alto 的 Panorama 管理解決方案。CloudWatch 日誌也可以使用 CloudWatch Subscription Filters 轉送到其他目的地。在下一節中進一步了解 Panorama。若要進一步了解 Splunk，請參閱與 Splunk 整合。

全景整合

AMS 受管防火牆可以選擇性地與您現有的 Panorama 整合。這可讓您從 Panorama 檢視防火牆組態，或從防火牆將日誌轉送至 Panorama。與 AMS Managed Firewall 的 Panorama 整合是唯讀的，不允許從 Panorama 對防火牆進行組態變更。Panorama 由您完全管理和設定，AMS 僅負責設定防火牆以與其通訊。

授權

AMS Managed Firewall 的價格取決於使用的授權類型、每小時或自備授權 (BYOL)，以及設備執行的執行個體大小。您必須透過 AWS Marketplace 訂購您偏好的執行個體大小和 Palo Alto 防火牆授權。

- Marketplace 授權：從 MALZ 中的網路帳戶接受 VM 系列新一代防火牆套件 1 的條款與條件。
- BYOL 授權：從 MALZ 的網路帳戶接受 VM 系列新一代防火牆 (BYOL) 的條款與條件，並共用購買授權給 AMS 後取得的「BYOL 驗證程式碼」。

限制

目前，AMS 支援 VM-300 系列或 VM-500 系列防火牆。您可以在此處找到組態：AWS EC2 執行個體上的 VM 系列模型、

> **Note**
>
> AMS 解決方案會在主動-主動模式下執行，因為其 AZ 中的每個 PA 執行個體都會處理其受尊重 AZ 的輸出流量。因此，使用兩個 AZs，每個 PA 執行個體處理高達 5 Gbps 的輸出流量，並有效地在兩個 AZs 中提供整體 10 Gbps 輸送量。對於每個 AZ 中的所有限制也是如此。如果 AMS 運作狀態檢查失敗，我們會將流量從具有錯誤 PA 的 AZ 轉移到另一個 AZ，並且在執行個體替換期間，容量會減少到剩餘的 AZs限制。

AMS 目前不支援 AWS Marketplace 上可用的其他 Palo Alto 套件；例如，您無法要求「VM 系列新一代防火牆套件 2」。請注意，使用 Palo Alto 的 AMS 受管防火牆解決方案目前僅提供輸出流量篩選產品，因此使用進階 VM 系列套件不會提供任何額外的功能或優點。

加入要求

- 您必須檢閱並接受 AWS Marketplace 中來自 Palo Alto 的 VM 系列新一代防火牆的條款與條件。
- 您必須根據預期的工作負載，確認要使用的執行個體大小。
- 您必須提供不會與多帳戶登陸區域環境或內部部署中的網路衝突的 /24 CIDR 區塊。它必須與輸出 VPC 的類別相同 （解決方案為輸出 VPC 佈建 /24 VPC 延伸）。

定價

AMS Managed Firewall 基礎基礎設施成本分為三個主要驅動程式：託管 Palo Alto 防火牆的 EC2 執行個體、軟體授權 Palo Alto VM 系列授權，以及 CloudWatch Integrations。

下列定價是以 VM-300 系列防火牆為基礎。

- EC2 執行個體：Palo Alto 防火牆會以 2-3 個 EC2 執行個體的高可用性模型執行，其中執行個體是以預期的工作負載為基礎。執行個體的成本取決於 AZs 的區域和數量
  - 例如 us-east-1、m5.xlarge、3AZs
    - $0.192 * 24 * 30 * 3 = $414.72
  - https://aws.amazon.com/ec2/pricing/on-demand/
- Palo Alto 授權：Palo Alto VM-300 新一代防火牆的軟體授權成本取決於 AZ 數量和執行個體類型。
  - 例如 us-east-1、m5.xlarge、3AZs
    - $0.87 * 24 * 30 * 3 = $1879.20
    - https://aws.amazon.com/marketplace/pp/B083M7JPKB?ref_=srh_res_product_title#pdp-pricing
- CloudWatch Logs 整合：CloudWatch Logs 整合使用 SysLog 伺服器 (EC2 - t3.medium)、NLB 和 CloudWatch Logs。伺服器的成本是根據 AZs 的區域和數量而定，而 NLB/CloudWatch 日誌的成本會根據流量使用率而有所不同。
  - 例如 us-east-1、t3.medium、3AZ
    - $0.0416 * 24 * 30 * 3 = $89.86
  - https://aws.amazon.com/ec2/pricing/on-demand/
  - https://aws.amazon.com/cloudwatch/pricing/

周邊 (DMZ) VPC

周邊或 DMZ、VPC 包含 AMS Operations 工程師存取 AMS 網路所需的資源。它包含跨 2-3 個AZs公有子網路，並在 Auto Scaling 群組 (ASG) 中包含 SSH Bastions 主機，供 AMS Operations 工程師登入或通道。連接至 DMZ 堡壘的安全群組包含來自 Amazon Corp Networks 的連接埠 22 傳入規則。

DMZ VPC CIDR 範圍：建立 VPC 時，您必須以無類別網域間路由 (CIDR) 區塊的形式指定 VPC 的 IPv4 地址範圍；例如 10.0.16.0/24。這是您 VPC 的主要 CIDR 區塊。

> **Note**
>
> AMS 團隊建議 24 的範圍（具有更多 IP 地址），以便在將來部署防火牆等其他資源時提供一些緩衝。

AWS Transit Gateway

AWS Transit Gateway (TGW) 是一項服務，可讓您將 Amazon Virtual Private Clouds (VPCs) 和內部部署網路連線至單一閘道。傳輸閘道是處理 AMS 帳戶網路與外部網路之間路由的網路骨幹。如需傳輸閘道的相關資訊，請參閱 AWS Transit Gateway。

提供下列輸入來建立此資源：

- 傳輸閘道 ASN 編號*：為您的傳輸閘道提供私有自治系統編號 (ASN)。此為邊界閘道協定 (BGP) 工作階段的 AWS 端 ASN。16 位元的 ASN 範圍應介於 64512 到 65534。

共用服務帳戶

共用服務帳戶可做為大多數 AMS 資料平面服務的中樞。帳戶包含存取管理 (AD)、端點安全管理 (Trend Micro) 所需的基礎設施和資源，並包含客戶堡壘 (SSH/RDP)。 共享服務帳戶中包含的資源的高階概觀如下圖所示。

共用服務 VPC 由三個可用區域 (AZs) 中的 AD 子網路、EPS 子網路和客戶堡壘子網路組成。共享服務 VPC 中建立的資源列於下方，需要您的輸入。

- 共用服務 VPC CIDR 範圍：建立 VPC 時，您必須以無類別網域間路由 (CIDR) 區塊的形式指定 VPC 的 IPv4 地址範圍；例如 10.0.1.0/24。這是您 VPC 的主要 CIDR 區塊。

> **Note**
>
> AMS 團隊建議 /23 的範圍。

- Active Directory 詳細資訊：Microsoft Active Directory (AD) 用於所有 AMS 多帳戶登陸區域帳戶的使用者/資源管理、身分驗證/授權和 DNS。AMS AD 也會設定對 Active Directory 的單向信任，以進行信任型身分驗證。建立 AD 需要下列輸入：
  - 網域完整網域名稱 (FQDN)：AWS Managed Microsoft AD 目錄的完整網域名稱。網域不應是您網路中現有網域的現有網域或子網域。
  - 網域 NetBIOS 名稱：如果您未指定 NetBIOS 名稱，AMS 會將名稱預設為目錄 DNS 的第一部分。例如，DNS corp.example.com 目錄的 corp。

- Trend Micro – 端點保護安全 (EPS)：Trend Micro 端點保護 (EPS) 是 AMS 中用於作業系統安全的主要元件。系統包含 Deep Security Manager (DSM)、EC2 執行個體、轉送 EC2 執行個體，以及存在於所有資料平面和客戶 EC2 執行個體中的代理程式。

  您必須在`EPSMarketplaceSubscriptionRole`共用服務帳戶中擔任 ，並訂閱 Trend Micro Deep Security (BYOL) AMI 或 Trend Micro Deep Security (Marketplace)。

  建立 EPS 需要下列預設輸入 （ 如果您想要從預設值變更 ）：
  - 轉送執行個體類型：預設值 - m5.large
  - DSM 執行個體類型：預設值 - m5.xlarge
  - 資料庫執行個體大小：預設值 - 200 GB
  - RDS 執行個體類型：預設值 - db.m5.large

- 客戶堡壘：共用服務帳戶中會提供 SSH 或 RDP 堡壘 （ 或兩者 ），供您存取 AMS 環境中的其他主機。若要以使用者身分存取 AMS 網路 (SSH/RDP)，您必須使用「客戶」堡壘做為進入點。網路路徑源自內部部署網路，經過 DX/VPN 到傳輸閘道 (TGW)，然後路由到共用服務 VPC。一旦您能夠存取堡壘，就可以跳到 AMS 環境中的其他主機，前提是已授予存取請求。
  - SSH 堡壘需要下列輸入。
    - SSH 堡壘所需執行個體容量：預設值 - 2。
    - SSH 堡壘上限執行個體：預設值 - 4。
    - SSH 堡壘最小執行個體：預設值 -2。
    - SSH 堡壘執行個體類型：預設值 - m5.large （ 可以變更為節省成本，例如 t3.medium)。

    - SSH 堡壘傳入 CIDRs：您網路中的使用者存取 SSH 堡壘的 IP 地址範圍。
- Windows RDP 堡壘需要下列輸入。
    - RDP 堡壘執行個體類型：預設值 - t3.medium。
    - RDP 堡壘所需最短工作階段：預設值 - 2。
    - RDP 工作階段上限：預設值 -10。
    - RDP 堡壘組態類型：您可以選擇下列其中一個組態
        - SecureStandard = 使用者會收到一個堡壘，只有一個使用者可以連接到堡壘。
        - SecureHA = 使用者在兩個不同的可用區域中接收兩個堡壘以連接到 ，只有一個使用者可以連接到堡壘。
        - SharedStandard = 使用者會收到一個要連線的堡壘，兩個使用者可以一次連線到相同的堡壘。
        - SharedHA = 使用者可以在兩個不同的可用區域中接收兩個堡壘以連接到 ，而兩個使用者可以一次連接到相同的堡壘。
    - 客戶 RDP 傳入 CIDRs：IP 地址範圍，您網路中的使用者將從其中存取 RDP 堡壘。

共用服務的更新：多帳戶登陸區域

AMS 會每月將資料平面版本套用至受管帳戶，恕不另行通知。

AMS 使用核心 OU 來提供共用服務，例如存取、聯網、EPS、日誌儲存、多帳戶登陸區域中的提醒彙總。AMS 負責解決這些共用服務的漏洞、修補和部署。AMS 會定期更新用於提供這些共用服務的資源，讓使用者可存取最新功能和安全性更新。更新通常每月進行。屬於這些更新一部分的資源包括：

- 屬於核心 OU 的帳戶。

  管理帳戶、共享服務帳戶、網路帳戶、安全帳戶和日誌封存帳戶具有 RDP 和 SSH 堡壘、代理、管理主機和端點安全 (EPS) 的資源，通常每月更新。AMS 使用不可變的 EC2 部署做為共用服務基礎設施的一部分。
- 整合最新更新的新 AMS AMIs。

> **Note**
>
> AMS 運算子會在執行資料平面變更時利用內部警示抑制變更類型 (CT)，且該 CT 的 RFC 會出現在您的 RFC 清單中。這是因為在部署資料平面版本時，各種基礎設施可能會關閉、重新啟

動、離線，或者可能會有 CPU 峰值或其他觸發警示的部署效果，這些警示在資料平面部署期間是不必要的。部署完成後，所有基礎設施都會驗證為正確執行，且警示會重新啟用。

Log Archive 帳戶

Log Archive 帳戶做為在 AMS 多帳戶登陸區域環境中封存日誌的中心中樞。帳戶中有一個 S3 儲存貯體，其中包含來自每個 AMS 多帳戶登陸區域環境帳戶的 AWS CloudTrail 和 AWS Config 日誌檔案副本。您可以使用此帳戶搭配 AWS Firehose 或 Splunk 等集中式記錄解決方案。此帳戶的 AMS 存取僅限於少數使用者；僅限稽核人員和安全團隊進行與帳戶活動相關的合規和鑑識調查。

安全帳戶

安全帳戶是用於存放安全相關操作的中樞，也是將通知和提醒漏接至 AMS 控制平面服務的要點。此外，安全帳戶會存放 Amazon Guard Duty 管理帳戶和 AWS Config 彙總工具。

應用程式帳戶類型

應用程式帳戶是您用來託管工作負載的 AMS 受管登陸區域架構中的 AWS 帳戶。AMS 提供三種類型的應用程式帳戶：

- AMS 受管應用程式帳戶
- AMS Accelerate 帳戶
- 客戶受管應用程式帳戶

根據應用程式帳戶類型，應用程式帳戶會在 AWS Organizations 中的不同 OUs 中分組：

- 根 OU：
  1. 應用程式 OU
     - 受管 OU：AMS 受管帳戶
     - 開發 OU：啟用開發人員模式的 AMS 受管帳戶
  2. 加速 OU：AMS 加速應用程式帳戶
  3. 客戶受管 OU：客戶受管應用程式帳戶

應用程式帳戶是透過從 管理帳戶提交的 RFC 佈建：

- 使用 VPC ct-1zdasmc2ewzrs 建立應用程式帳戶
- 建立加速帳戶 ct-2p93tyd5angmi
- 建立客戶受管應用程式帳戶 ct-3pwbixz27n3tn

AMS 受管應用程式帳戶

AMS 完全管理的應用程式帳戶稱為 AMS 受管應用程式帳戶，其中部分或所有操作任務，例如服務請求管理、事件管理、安全管理、持續性管理（備份）、修補程式管理、成本最佳化，或基礎設施的監控和事件管理，皆由 AMS 執行。

AMS 執行的任務數量取決於您選擇的變更管理模式。AMS 受管帳戶支援不同的變更管理模式：

- RFC 模式
- AMS 中的直接變更模式
- AMS 和 AWS Service Catalog
- AMS 進階開發人員模式
- AMS 中的自助式佈建模式

如需變更管理和不同模式的詳細資訊，請參閱 變更管理模式。

有些 AWS 服務可在 AMS 受管帳戶中使用，無需 AMS 管理。這些 AWS 服務的清單以及如何將其新增至您的 AMS 帳戶，如自助式佈建一節所述。

AMS Accelerate 帳戶

AMS Accelerate 是 AMS 操作計劃，可操作支援工作負載的 AWS 基礎設施。您可以受益於 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。您將使用您偏好的存取和變更機制，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。

> **Note**
>
> AMS Advanced 中的 AMS Accelerate 帳戶沒有 AMS 變更管理 (RFCs) 或 AMS Advanced 主控台。相反地，它們具有 AMS Accelerate 主控台和功能。

加速帳戶只能從您的 AMS 多帳戶登陸區域管理帳戶佈建。Accelerate 提供不同的操作功能。如需進一步了解，請參閱加速服務描述。

- 您將繼續享受多帳戶登陸區域 (MALZ) 核心帳戶的一些功能，例如集中式記錄、單一帳單、安全帳戶和 SCPs中的組態彙總器。
- AMS Accelerate 不提供某些 AMS Advanced 服務，例如 EPS、存取管理、變更管理和佈建。我們建議您遵循後續步驟來存取和設定傳輸閘道 (TGW)。

如需 Accelerate 的詳細資訊，請參閱什麼是 Accelerate。

建立您的 Accelerate 帳戶

若要建立 Accelerate 帳戶，請依照此處概述的步驟建立 Accelerate 帳戶。

存取您的 Accelerate 帳戶

在多帳戶登陸區域 (MALZ) 帳戶中佈建 Accelerate 帳戶後，具有管理存取許可 的角色`AccelerateDefaultAdminRole`會位於帳戶中供您擔任。

若要存取新的 Accelerate 帳戶：

1. 使用 `CustomerDefaultAssumeRole`角色登入管理帳戶的 IAM 主控台。
2. 在 IAM 主控台的導覽列上，選擇您的使用者名稱。
3. 選擇 Switch Role (切換角色)。如果這是第一次選擇此選項，則頁面會顯示更多資訊。讀取後，選擇 Switch Role (切換角色)。如果清除瀏覽器 cookie，則此頁面可以再次顯示
4. 在切換角色頁面上，輸入加速帳戶 ID 和要擔任的角色名稱：`AccelerateDefaultAdminRole`。

現在您已擁有存取權，您可以建立新的 IAM 角色，以繼續存取您的環境。如果您想要為 Accelerate 帳戶利用 SAML 聯合，請參閱啟用 SAML 2.0 聯合身分使用者以存取 AWS 管理主控台。

將您的 Accelerate 帳戶與 Transit Gateway 連線

AMS 不會管理 Accelerate 帳戶的網路設定。您可以選擇使用 AWS APIs 管理自己的網路 （請參閱網路解決方案)，或使用 AMS MALZ 中部署的現有 Transit Gateway (TGW) 連線至 AMS 管理的 MALZ 網路。

> **Note**
>
> 如果 Accelerate 帳戶位於相同的 AWS 區域，您只能將 VPC 連接到 TGW。如需詳細資訊，請參閱傳輸閘道。

若要將 Accelerate 帳戶新增至 Transit Gateway，請使用 部署 | 受管登陸區域 | 網路帳戶 | 新增靜態路由 (ct-3r2ckznmt0a59) 變更類型來請求新路由，請包含此資訊：

- Blackhole：True 表示路由的目標無法使用。當傳輸閘道要捨棄靜態路由的流量時，請執行此操作。將流量路由到指定 TGW 連接 ID 的 False。預設值為 false。
- DestinationCidrBlock：用於目的地比對的 IPV4 CIDR 範圍。路由決策是根據最明確的匹配。範例：10.0.2.0/24。
- TransitGatewayAttachmentId：做為路由表目標的 TGW 附件 ID。如果 Blackhole 為 false，則需要此參數，否則將此參數保留空白。範例：tgw-attach-04eb40d1e14ec7272。
- TransitGatewayRouteTableId：TGW 路由表的 ID。範例：tgw-rtb-06ddc751c0c0c881c。

在 TGW 路由表中建立路由以連線至此 VPC：

1. 根據預設，此 VPC 將無法與 MALZ 網路中的任何其他 VPCs通訊。
2. 與您的解決方案架構師一起決定您希望此加速 VPCs 與哪些 VPC 通訊。
3. 提交部署 | 受管登陸區域 | 網路帳戶 | 新增靜態路由 (ct-3r2ckznmt0a59) 變更類型，包括此資訊：
   - Blackhole：True 表示路由的目標無法使用。當傳輸閘道要捨棄靜態路由的流量時，請執行此操作。將流量路由到指定 TGW 連接 ID 的 False。預設值為 false。
   - DestinationCidrBlock：用於目的地比對的 IPV4 CIDR 範圍。路由決策是根據最明確的匹配。範例：10.0.2.0/24。
   - TransitGatewayAttachmentId：做為路由表目標的 TGW 附件 ID。如果 Blackhole 為 false，則需要此參數，否則將此參數保留空白。範例：tgw-attach-04eb40d1e14ec7272。
   - TransitGatewayRouteTableId：TGW 路由表的 ID。範例：tgw-rtb-06ddc751c0c0c881c。

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 ）：

1. 在您的多帳戶登陸區域聯網帳戶中，開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Transit Gateways (傳輸閘道)。記錄您看到的傳輸閘道的 TGW ID。
3. 在您的 Accelerate 帳戶中，開啟 Amazon VPC 主控台。

4. 在導覽窗格中，選擇傳輸閘道附件 > 建立傳輸閘道附件。做出這些選擇：
   - 針對傳輸閘道 ID，選擇您在步驟 2 中記錄的傳輸閘道 ID。
   - 在 Attachment type (連接類型)中，選擇 VPC。
   - 在 VPC Attachment (VPC 連接) 中，您可選擇輸入 Attachment name tag (連接名稱標籤) 的名稱。
   - 選擇是否啟用 DNS support (DNS 支援) 和 IPv6 Support (IPv6 支援)。
   - 對於 VPC ID，請選擇要連接至傳輸閘道的 VPC。此 VPC 必須至少有一個子網路與之建立關聯。
   - 在子網路 ID 中，為每個可用區域選取傳輸閘道用來路由流量的一個子網路。您必須選擇至少一個子網路。一個可用區域只能選取一個子網路。
5. 選擇 Create attachment (建立連接)。記錄新建立的 TGW 附件 ID。

將 TGW 連接與路由表建立關聯：

1. 決定要與 VPC 建立關聯的 TGW 路由表。建議您使用部署 | 受管登陸區域 | 網路帳戶 | 建立傳輸閘道路由表 (ct-3dscwaeyi6cup) 變更類型，為加速帳戶 VPCs 建立新的應用程式路由表。
2. 在網路帳戶上提交管理 | 受管登陸區域 | 網路帳戶 | 關聯 TGW 連接 (ct-3nmhh0qr338q6) RFC，將 VPC 或 TGW 連接與您選取的路由表建立關聯。

在 TGW 路由表中建立路由以連線至此 VPC：

1. 根據預設，此 VPC 將無法與多帳戶登陸區域網路中的任何其他 VPCs 通訊。
2. 與您的解決方案架構師一起決定您希望此加速帳戶 VPCs 與哪些 VPC 通訊。
3. 提交部署 | 受管登陸區域 | 網路帳戶 | 針對網路帳戶新增靜態路由 (ct-3r2ckznmt0a59) RFC，以建立您需要的 TGW 路由。

將 VPC Route 資料表設定為指向 AMS 多帳戶登陸區域傳輸閘道：

1. 與您的解決方案架構師一起決定您要將哪些流量傳送至 AMS 多帳戶登陸區域傳輸閘道。
2. 提交部署 | 受管登陸區域 | 網路帳戶 | 針對網路帳戶新增靜態路由 (ct-3r2ckznmt0a59) RFC，以建立您需要的 TGW 路由。

客戶受管應用程式帳戶

您可以建立 AMS 未以標準方式管理的帳戶。這些帳戶稱為客戶受管帳戶，可讓您完全控制在帳戶中自行操作基礎設施，同時享受由 AMS 管理的集中式架構的優點。

客戶受管帳戶無法存取 AMS 主控台或我們提供的任何服務（修補程式、備份等）。

客戶受管帳戶只能從您的 AMS 多帳戶登陸區域管理帳戶佈建。

不同的 AMS 模式以不同的方式使用應用程式帳戶；若要進一步了解模式，請參閱 AWS Managed Services 模式。

若要建立您的客戶受管應用程式帳戶，請參閱管理帳戶 | 建立客戶受管應用程式帳戶。

若要刪除客戶受管應用程式帳戶，請使用管理帳戶 | 離線應用程式帳戶。(確認離職 CT 不適用於客戶受管應用程式帳戶。)

存取您的客戶受管帳戶

在多帳戶登陸區域中佈建客戶受管帳戶 (CMA) 之後，管理員角色 (MALZ) `CustomerDefaultAdminRole`會位於帳戶中，供您透過 SAML 聯合身分擔任以設定帳戶。

若要存取 CMA：

1. 使用 CustomerDefaultAssumeRole 角色登入管理帳戶的 IAM 主控台。
2. 在 IAM 主控台的導覽列上，選擇您的使用者名稱。
3. 選擇 Switch Role (切換角色)。如果這是第一次選擇此選項，則頁面會顯示更多資訊。讀取後，選擇 Switch Role (切換角色)。如果清除瀏覽器 cookie，則此頁面可以再次顯示
4. 在切換角色頁面上，輸入客戶受管帳戶 ID 和要擔任的角色名稱：CustomerDefaultAdminRole。

現在您已擁有存取權，您可以建立新的 IAM 角色，以繼續存取您的環境。如果您想要為 CMA 帳戶利用 SAML 聯合，請參閱啟用 SAML 2.0 聯合身分使用者以存取 AWS 管理主控台。

將您的 CMA 與 Transit Gateway 連線

AMS 不會管理客戶受管帳戶 (CMAs) 的網路設定。您可以選擇使用 AWS APIs 管理自己的網路（請參閱網路解決方案)，或使用 AMS MALZ 中部署的現有 Transit Gateway (TGW) 連線至 AMS 管理的多帳戶登陸區域網路。

> **Note**
>
> 如果 CMA 位於相同的 AWS 區域，您只能將 VPC 連接到 TGW。如需詳細資訊，請參閱傳輸閘道。

若要將 CMA 新增至 Transit Gateway，請使用網路帳戶請求新路由 | 新增靜態路由 (ct-3r2ckznmt0a59) 變更類型，並包含此資訊：

- Blackhole：True 表示路由的目標無法使用。當傳輸閘道要捨棄靜態路由的流量時，請執行此操作。將流量路由到指定 TGW 連接 ID 的 False。預設值為 false。
- DestinationCidrBlock：用於目的地比對的 IPV4 CIDR 範圍。路由決策是根據最明確的匹配。範例：`10.0.2.0/24`。
- TransitGatewayAttachmentId：做為路由表目標的 TGW 附件 ID。如果 Blackhole 為 false，則需要此參數，否則將此參數保留空白。範例：`tgw-attach-04eb40d1e14ec7272`。
- TransitGatewayRouteTableId：TGW 路由表的 ID。範例：`tgw-rtb-06ddc751c0c0c881c`。

將新的客戶受管 VPC 連線至 AMS 多帳戶登陸區域網路（建立 TGW VPC 連接）：

1. 在您的多帳戶登陸區域聯網帳戶中，開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇傳輸閘道。記錄您看到的傳輸閘道的 TGW ID。
3. 在您的客戶受管帳戶中，開啟 Amazon VPC 主控台。
4. 在導覽窗格中，選擇傳輸閘道附件 > 建立傳輸閘道附件。做出這些選擇：
    a. 針對傳輸閘道 ID，選擇您在步驟 2 中記錄的傳輸閘道 ID。
    b. 在 Attachment type (連接類型)中，選擇 VPC。
    c. 在 VPC Attachment (VPC 連接) 中，您可選擇輸入 Attachment name tag (連接名稱標籤) 的名稱。
    d. 選擇是否啟用 DNS support (DNS 支援) 和 IPv6 Support (IPv6 支援)。
    e. 對於 VPC ID，請選擇要連接至傳輸閘道的 VPC。此 VPC 必須至少有一個子網路與之建立關聯。
    f. 在子網路 ID 中，為每個可用區域選取傳輸閘道用來路由流量的一個子網路。您必須選擇至少一個子網路。一個可用區域只能選取一個子網路。
5. 選擇 Create attachment (建立連接)。記錄新建立的 TGW 附件 ID。

將 TGW 連接與路由表建立關聯：

決定要與 VPC 建立關聯的 TGW 路由表。我們建議您提交部署 | 受管登陸區域 | 網路帳戶 | 建立傳輸閘道路由表 (ct-3dscwaeyi6cup) RFC，為客戶受管 VPCs 建立新的應用程式路由表。若要將 VPC 或 TGW 連接與您選取的路由表建立關聯，請在網路帳戶上提交部署 | 受管登陸區域 | 網路帳戶 | 關聯 TGW 連接 (ct-3nmhh0qr338q6) RFC。

在 TGW 路由表中建立路由以連線至此 VPC：

1. 根據預設，此 VPC 將無法與多帳戶登陸區域中的任何其他 VPCs 通訊。
2. 與您的解決方案架構師一起決定您希望此客戶受管 VPCs 與哪些 VPC 通訊。提交部署 | 受管登陸區域 | 網路帳戶 | 針對網路帳戶新增靜態路由 (ct-3r2ckznmt0a59) RFC，以建立您需要的 TGW 路由。

> **Note**
>
> 此 CT (ct-3r2ckznmt0a59) 不允許將靜態路由新增至核心路由表 EgressRouteDomain；如果您的 CMA 需要允許輸出流量，請使用 ct-0xdawir96cy7k 提交管理 | 其他 | 其他 (MOO) RFC。

將 VPC Route 資料表設定為指向 AMS 多帳戶登陸區域傳輸閘道：

與您的解決方案架構師一起決定您要將哪些流量傳送至 AMS 多帳戶登陸區域傳輸閘道。更新您的 VPC 路由表，將流量傳送至先前建立的 TGW 連接

取得客戶受管帳戶的操作說明

AMS 可以透過將帳戶加入 AMS Accelerate，協助您操作您在客戶受管帳戶中部署的工作負載。透過 AMS Accelerate，您可以受益於營運服務，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使用方式 AWS。AMS Accelerate 也為需要定期修補的 EC2-based工作負載提供選用的修補程式附加元件。透過 AMS Accelerate，您可以繼續使用、設定和部署所有原生 AWS 服務，或使用您偏好的工具；就像使用 AMS Advanced Customer Managed 帳戶一樣。您會使用偏好的存取和變更機制，同時 AMS 會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。如需進一步了解，請參閱加速服務描述。

若要將客戶受管帳戶加入 Accelerate，請聯絡您的 CSDM，並遵循 AMS Accelerate 入門中的步驟。

> **Note**
>
> AMS Advanced 中的 AMS Accelerate 帳戶沒有 AMS 變更管理 （變更請求或 RFCs) 或 AMS Advanced 主控台。相反地，它們具有 AMS Accelerate 主控台和功能。

AMS 工具帳戶 （遷移工作負載）

您的多帳戶登陸區域工具帳戶 （使用 VPC) 有助於加速遷移工作、提高安全位置、降低成本和複雜性，以及標準化您的使用模式。

工具帳戶提供下列項目：

- 明確定義的界限，可讓您在生產工作負載之外存取系統整合商的複寫執行個體。
- 可讓您建立隔離的培養室，在將工作負載放入具有其他工作負載的 帳戶之前，檢查工作負載是否有惡意軟體或未知的網路路由。
- 作為定義的帳戶設定，它可以更快地加入和設定遷移工作負載。
- 隔離的網路路由可保護來自內部部署 -> CloudEndure -> 工具帳戶 -> AMS 擷取映像的流量。擷取映像後，您可以透過 AMS 管理 | 進階堆疊元件 | AMI | 共用 (ct-1eiczxw8ihc18) RFC 將映像分享至目的地帳戶。

高階架構圖：

使用部署 | 受管登陸區域 | 管理帳戶 | 建立工具帳戶 （使用 VPC) 變更類型 (ct-2j7q1hgf26x5c)，快速部署工具帳戶，並在多帳戶登陸區域環境中執行個體化工作負載擷取程序。請參閱管理帳戶、工具帳戶：建立 （使用 VPC)。

> **Note**
>
> 我們建議您有兩個可用區域 AZs)，因為這是遷移中樞。
> 根據預設，AMS 會在每個帳戶中建立下列兩個安全群組 SGs)。確認這兩個 SGs存在。如果它們不存在，請向 AMS 團隊開啟新的服務請求，以請求它們。
>
> - SentinelDefaultSecurityGroupPrivateOnlyEgressAll
> - InitialGarden-SentinelDefaultSecurityGroupPrivateOnly

確保 CloudEndure 複寫執行個體是在有路由傳回內部部署的私有子網路中建立。您可以確認私有子網路的路由表具有傳回 TGW 的預設路由。不過，執行 CloudEndure 機器切換應該進入「隔離」私有子網路，其中沒有傳回內部部署的路由，僅允許網際網路傳出流量。請務必確保隔離子網路中發生切換，以避免內部部署資源的潛在問題。

事前準備：

1. Plus 或 Premium 支援層級。
2. 部署 AMIs 之 KMS 金鑰的應用程式帳戶 IDs。
3. 工具帳戶，如先前所述建立。

AWS 應用程式遷移服務 (AWS MGN)

AWS Application Migration Service (AWS MGN) 可以透過工具帳戶佈建期間自動建立的 `AWSManagedServicesMigrationRole` IAM 角色，在您的 MALZ Tools 帳戶中使用。您可以使用 AWS MGN 遷移在支援的 Windows 和 Linux 作業系統版本上執行的應用程式和資料庫。

如需 AWS 區域 支援up-to-date，請參閱AWS 區域服務清單。

如果 AWS MGN AWS 區域 目前不支援您的偏好，或 AWS MGN 目前不支援應用程式執行所在的作業系統，請考慮改為在工具帳戶中使用 CloudEndure 遷移。

請求 AWS MGN 初始化

AWS MGN 必須在第一次使用前由 AMS 初始化。若要為新的工具帳戶請求此項目，請從工具帳戶提交管理 | 其他 | 其他 RFC，其中包含下列詳細資訊：

```
RFC Subject=Please initialize AWS MGN in this account
RFC Comment=Please click 'Get started' on the MGN welcome page here:

    https://console.aws.amazon.com/mgn/home?region=MALZ_PRIMARY_REGION#/welcome using
 all default values
    to 'Create template' and complete the initialization process.
```

一旦 AMS 成功完成 RFC 並初始化工具帳戶中的 AWS MGN，您可以使用 `AWSManagedServicesMigrationRole` 來編輯預設範本以符合您的需求。

啟用對新 AMS 工具帳戶的存取

工具帳戶建立後，AMS 會為您提供帳戶 ID。您的下一個步驟是設定新帳戶的存取權。請遵循下列步驟。

1. 將適當的 Active Directory 群組更新為適當的帳戶 IDs。

   新 AMS 建立的帳戶會佈建 ReadOnly 角色政策，以及允許使用者提交 RFCs的角色。

   工具帳戶也有額外的 IAM 角色和可用的使用者：

   - IAM 角色： `AWSManagedServicesMigrationRole`
   - IAM 使用者： `customer_cloud_endure_user`
2. 請求政策和角色，以允許服務整合團隊成員設定下一個層級的工具。

   導覽至 AMS 主控台並存檔下列 RFCs：

   a. 建立 KMS 金鑰。使用建立 KMS 金鑰 （ 自動 ） 或建立 KMS 金鑰 （ 需要檢閱 ）。

      當您使用 KMS 加密擷取的資源時，使用與其餘多帳戶登陸區域應用程式帳戶共用的單一 KMS 金鑰，可為可在目的地帳戶中解密的擷取影像提供安全性。

   b. 共用 KMS 金鑰。

      使用 管理 | 進階堆疊元件 | KMS 金鑰 | 共用 （ 需要檢閱 ） 變更類型 (ct-05yb337abq3x5)，請求將新的 KMS 金鑰分享給將存放擷取 AMIs 的應用程式帳戶。

最終帳戶設定的範例圖形：

範例 AMS 預先核准的 IAM CloudEndure 政策

若要查看 AMS 預先核准的 IAM CloudEndure 政策：解壓縮 WIGS 雲端持久性登陸區域範例檔案，然後開啟 `customer_cloud_endure_policy.json`。

測試 AMS Tools 帳戶連線和end-to-end設定

1. 從設定 CloudEndure 開始，並在將複寫至 AMS 的伺服器上安裝 CloudEndure 代理程式。
2. 在 CloudEndure 中建立專案。
3. 透過 Secrets Manager，輸入執行先決條件時共用的 AWS 登入資料。
4. 在複寫設定中：

a. 針對選擇要套用至複寫伺服器的安全群組選項，選取兩個 AMS "Sentinel" 安全群組 （僅限私有和 EgressAll)。

b. 定義機器的切換選項 （執行個體）。如需詳細資訊，請參閱步驟 5。剪下

c. 子網路：私有子網路。

5. 安全群組：

a. 選取兩個 AMS "Sentinel" 安全群組 （僅限私有和 EgressAll)。

b. 切換執行個體必須與 AMS 受管 Active Directory (MAD) 和 AWS 公有端點通訊：

i. 彈性 IP：無

ii. 公有 IP：否

iii. IAM 角色：Customer-mc-ec2-instance-profile

c. 根據您的內部標記慣例設定標籤。

6. 在機器上安裝 CloudEndure 代理程式，並在 EC2 主控台中尋找要在 AMS 帳戶中出現的複寫執行個體。

AMS 擷取程序：

AMS Tools 帳戶衛生

在帳戶中完成共用 AMI 且不再需要複寫的執行個體之後，您會想要清除 ：

- 執行個體後 WIGs擷取：
  - 切換執行個體：在工作完成後，至少透過 AWS 主控台停止或終止此執行個體
  - 擷取前 AMI 備份：擷取執行個體並終止現場部署執行個體後移除
  - AMS 擷取的執行個體：共用 AMI 後關閉堆疊或終止
  - AMS 擷取AMIs：與目的地帳戶共用完成後刪除
- 遷移清除結束：記錄透過開發人員模式部署的資源，以確保定期進行清除，例如：
  - 安全群組
  - 透過 Cloud-formation 建立的資源
  - 網路 ACK
  - 子網路
  - VPC
  - 路由表

- 角色
- 使用者和帳戶

大規模遷移 - 遷移工廠

請參閱 AWS CloudEndure 遷移工廠解決方案簡介。

MALZ：核心帳戶加入

加入 AWS 多帳戶登陸區域核心帳戶時，您需要完成的關鍵任務如下：

主題

- 在 AMS 中建立 AWS 多帳戶登陸區域核心帳戶
- 為 AMS 建立 IAM 角色以存取您的帳戶
- 使用 AMS 中根使用者的多重要素驗證 (MFA) 保護新帳戶
- 訂閱適用於 Trend Micro Endpoint Protection (EPS) AWS Marketplace 的
- 設定聯網
- 設定存取管理

如有加入問題，請聯絡您的 Cloud Architect。

在 AMS 中建立 AWS 多帳戶登陸區域核心帳戶

AMS 多帳戶登陸區域需要佈建新的 Amazon Web Services (AWS) 帳戶，才能做為 AMS 多帳戶登陸區域中的管理帳戶。若要建立 AWS 帳戶，請遵循這些step-by-step指示：如何建立和啟用新的 Amazon Web Services 帳戶？

簡單步驟為：前往建立帳戶，然後按一下立即註冊，然後在開啟的頁面上，按一下建立新 AWS 帳戶帳戶。遵循畫面上的指示，包括接聽電話並使用電話鍵盤輸入 PIN 碼。您也需要輸入信用卡。AMS 使用此帳戶做為新多帳戶登陸區域的管理帳戶或付款人帳戶。

> **Note**
>
> 加入後，請與您的雲端服務交付經理 (CSDM) 討論如何將帳單從信用卡移出並移至發票系統。將需要以下資訊：
>
> - 帳單公司名稱

- 帳單聯絡人名稱
- 帳單聯絡人電話號碼
- 帳單聯絡人電子郵件
- 帳單地址

您的 CSDM 將協助您進行此更新。完成後，若要變更付款方式，請參閱管理您的 AWS 付款方式。

Note

請勿將您的新帳戶連結至現有的管理帳戶或付款人帳戶。
確保您的帳戶不是現有 的一部分 AWS Organizations；如需資訊，請參閱什麼是 AWS Organizations？

Important

請務必確保電子郵件地址（分發清單，而不是個人的電子郵件地址）和電話號碼與帳戶相關聯，以便收到對潛在安全事件的回應。在未重設帳戶密碼的情況下，無法變更帳戶的電話號碼和電子郵件地址，這是 AMS 根帳戶的重要任務。為了確保這些值穩定，請務必選取與個人無關的聯絡資訊，這可能會變更。選擇可以指向群組的電子郵件別名。在選取電話號碼時，請遵循相同的實務：選擇可以指向群組的號碼，或指向公司擁有的號碼，而非個人。

如需要求您將核心帳戶加入 AMS 多帳戶登陸區域之問題的詳細資訊，請參閱 附錄：多帳戶登陸區域 (MALZ) 加入考量清單。

為 AMS 建立 IAM 角色以存取您的帳戶

現在您已成功建立新的 AWS 帳戶，程序的下一個步驟是允許 AMS 存取新帳戶，以建立和設定您的 AMS 環境，以及持續的變更和佈建請求要履行。如需詳細資訊，請參閱使用 IAM 角色跨 AWS 帳戶委派存取權。

AWS Identity and Access Management (IAM) 是一種 Web 服務，可協助您安全地控制使用者對 AWS 資源的存取。您可以使用 IAM 來控制誰可以使用您的 AWS 資源（身分驗證），以及他們可以使用哪些資源，以及其使用方式（授權）。

啟用 AWS 主控台的 IAM 存取

1. 使用您的根帳戶登入資料（您用來建立 的電子郵件和密碼 AWS 帳戶) 登入 AWS Management 主控台。請勿使用其他 IAM 登入資料登入。隨即開啟 AWS Management 主控台首頁。
2. 在頂端導覽列中，開啟您帳戶名稱的下拉式選單，然後選擇帳戶。帳單首頁隨即開啟。
3. 向下捲動至 IAM 使用者和角色存取帳單資訊，然後選擇編輯。啟用 IAM 存取區域隨即開啟。
4. 選取核取方塊，然後選擇更新。您現在可以使用 IAM 政策來控制使用者可以存取的頁面。

建立 AMS 要使用的 IAM 角色

1. 取得 JSON 或 YAML 檔案，定義 AMS 用來建立基礎設施的 IAM 角色。任何一個：
   - 您的 AMS 雲端架構師 (CA) 為您提供 JSON 或 YAML 檔案。
   - 您可以下載 onboarding_iam_roles.zip，然後選擇下列其中一項：
     - onboarding_role_admin.json（較短，授予完整的管理員存取權）
     - onboarding_role_minimal.json（較長，授予最低權限)
2. 登入 AWS 管理主控台 並在 https：//https://console.aws.amazon.com/cloudformation 開啟 CloudFormation 主控台。
3. 選擇 Create Stack (建立堆疊)。您會看到以下頁面。
4. 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。
5. 在堆疊名稱區段**ams-onboarding-role**中輸入 ，並繼續向下捲動並選取下一步，直到您到達此頁面為止。
6. 確定已選取核取方塊，然後選取建立堆疊。
7. 確定堆疊已成功建立。

使用 AMS 中根使用者的多重要素驗證 (MFA) 保護新帳戶

本節已修訂，因為它包含敏感的 AMS 安全相關資訊。此資訊可透過 AMS 主控台文件取得。若要存取 AWS Artifact，您可以聯絡 CSDM 以取得指示，或前往 AWS Artifact 入門。

訂閱適用於 Trend Micro Endpoint Protection (EPS) AWS Marketplace 的

Trend Micro Endpoint Protection (EPS) 是 AMS 中維護作業系統安全的主要元件。若要在 AMS 登陸區域建立開始後設定 EPS，您需要登入共用服務核心帳戶並訂閱 Trend Micro Deep Security AMI AWS Marketplace。您的 CSDM 或 CA 會建議您。

1. 使用您在 加入問卷中指定的角色或使用者登入 AWS 主控台 `CustomerEPSSubscriptionIAMRoleOrUser`
2. 導覽至切換角色畫面。

   - 帳戶：由 AMS 提供
   - 角色：`EPSMarketplaceSubscriptionRole`
   - 顯示名稱：EPS 訂閱工作階段

   若要在 中訂閱 Trend Micro Deep Security AWS Marketplace，請在主控台中切換角色之後遵循下列步驟：

   1. 導覽至 AWS Marketplace。
   2. 在尋找符合您需求 AWS Marketplace 的產品下，選取下列選項：
      a. 供應商：Trend Micro
      b. 定價計劃：如果您有授權或依主機計費，請自帶授權
      c. 交付方法：Amazon Machine Image
   3. 按一下右側面板中的繼續訂閱。
   4. 檢閱條款與條件，然後按一下右上角的接受條款。
   5. 登出帳戶，並與您的 Cloud Architect 確認程序已完成。

此時，AMS 會將基礎設施部署到您的 AMS 環境，且一旦您連接網路並設定您的存取，環境即可供您使用。

設定聯網

AMS 環境中的網路主要在網路核心帳戶中處理。

設定 AWS Managed Services (AMS) 的聯網需要完成幾個程序：

- 為您的 AMS 環境配置 IP 空間
- 建立私有網路連線至 AWS
- 設定防火牆以允許 AMS 操作

為您的 AMS 環境配置 IP 空間

您應該已經與 Cloud Architect 合作，為您的 AMS 環境定義 IP 空間，同時填寫入門問卷。

在 AMS AWS 中建立私有網路連線至

AWS 透過 AWS Direct Connect 使用 VPN 連線和專用線路提供私有連線。可透過兩種方式設定私有連線：

- 使用 Transit Gateway 的集中式 Edge 連線
- 將 Direct Connect 和/或 VPN 連線至帳戶 VPCs

使用 Transit Gateway 的集中式邊緣連線

AWS Transit Gateway 是一項服務，可讓您將 Amazon Virtual Private Clouds (VPCs) 和內部部署網路連線至單一閘道。Transit Gateway 可用來合併現有的邊緣連線，並透過單一輸入/輸出點進行路由。如需詳細資訊，請參閱 AWS Transit Gateway。

將 Direct Connect 連線至 Transit Gateway

您可以使用現有的 Direct Connect 連線，或在現有帳戶中建立新的 Direct Connect 連線 AWS 。Direct Connect 連線應為以 1 Gbps 或更高速度執行的專用或託管連線。

> **Note**
>
> 如需搭配 AWS 服務使用 Direct Connect 的詳細資訊，請參閱 AWS Direct Connect 位置入門。

若要使用現有的 Direct Connect 專用連線，連線上建立的傳輸虛擬介面不得超過 3 個。這是因為 Direct Connect 專用連線每個連線有 4 個傳輸虛擬介面的限制。

如需 Direct Connect 限制的詳細資訊，請參閱 AWS Direct Connect 限制。

在 Direct Connect 連線可用之後，會發生下列情況：

1. AMS 會在聯網帳戶中建立 Direct Connect Gateway。您必須為 Direct Connect Gateway 提供自治系統編號 (ASN) 號碼，以及必須從 Direct Connect Gateway 公告的字首。此 ASN 用作 Amazon ASN。
2. 您可以建立新的 Transit VIF，並將虛擬介面擁有者設定為聯網帳戶。
3. AMS 登入聯網帳戶並接受連線提案。
4. AMS 會將傳輸閘道與 Direct Connect 閘道建立關聯。
5. AMS 會將附件與內部部署 Transit Gateway 路由表建立關聯。

> **Note**
>
> 為 Direct Connect 閘道和 Transit Gateway 提供的 ASN 必須不同。

為了提高連線能力，最佳實務是將至少 2 個傳輸虛擬介面從不同的 AWS Direct Connect 位置連接到 Direct Connect 閘道。如需詳細資訊，請參閱Direct Connect 彈性建議。

將 VPN 連線至 Transit Gateway

欲將 VPN 連線附加至您的傳輸閘道，您必須指定客戶閘道。如需客戶閘道需求的詳細資訊，請參閱《Amazon VPC 網路管理員指南》中的客戶閘道需求。

您需要提供 BGP ASN 號碼、靜態公有 IP 地址和路由選項 （靜態或動態）。提供這些詳細資訊後，AMS 會建立 VPN 連接，並將連接與內部部署 Transit Gateway 路由表建立關聯。

如需傳輸閘道附件的詳細資訊，請參閱傳輸閘道 VPN 附件。

將 Direct Connect 和/或 VPN 連線至帳戶 VPCs

您也可以直接將 VPCs連線至 Direct Connect 或 VPN。流量會直接從 VPCs 流向 Direct Connect 或 VPN，而不會周遊傳輸閘道。

> **Note**
>
> 共用服務 VPC 和應用程式帳戶 VPCs 必須連線至 Direct Connect 或 VPN 連線，才能建立私有連線。

Direct Connect 在 AMS 中設定

設定 Direct Connect 以在 AMS 受管 VPC 和內部網路之間進行通訊。

> **Note**
>
> 如需搭配 AWS 服務使用 Direct Connect 的詳細資訊，請參閱 Direct Connect 位置入門。

若要設定 Direct Connect 連線，請完成下列步驟：

1. 註冊 Amazon Web Services (AWS)
2. 提交 Direct Connect 連線請求。
3. 完成 Cross Connect。
4. （選用）使用 設定備援連線 Direct Connect。
5. 由 AMS 執行：建立虛擬界面。
6. 由 AMS 執行：下載路由器組態。
7. 驗證您的虛擬界面。

VPN 設定

AMS 設定 VPN 以在您的 AMS 受管 VPC 與內部網路之間通訊時遵循的基本步驟。

> **Note**
>
> 若要全面了解將 VPN 與 AWS 服務搭配使用，請參閱什麼是 AWS Site-to-Site VPN 和您的客戶閘道（您的 VPN 設備）。

我們遵循 AWS VPN 使用者指南入門和測試Site-to-Site連接章節來完成以下步驟：

1. 在您的 AWS VPC 中，建立客戶閘道。

2. 在您的 AWS VPC 中，建立虛擬私有閘道。
3. 在您的 AWS VPC 中，在您的路由表中啟用路由傳播。
4. 在您的 AWS VPC 中，更新您的安全群組以啟用傳入 SSH、RDP 和 ICMP 存取。
5. 在您的內部網路中，建立 VPN 連線並設定客戶閘道。
6. 測試 VPC 與內部網路之間的 VPN 連線。

設定存取管理

使用由 AWS Managed Services (AMS) 管理的網路表示授予 AMS 管理雲端基礎設施的存取權。您需要設定在私有網路和 AMS 之間安全連線的方法。這從一些決策開始：

- AMS API/CLI 和主控台存取：您會想要安裝 AMS CLI（本文件提供說明）。您可以使用 AMS 變更管理 API 向 AMS 和 AMS SKMS API 提出變更請求，以了解您的 AMS 受管資源。使用 Active Directory Federation Services (AD FS)，您可以存取 AMS 主控台。
- 使用者存取：必須在 AMS 端的 AD（透過 Directory Services) 與您用來管理使用者的目錄之間建立連線。
- 執行個體存取：透過單向信任組態完成執行個體層級存取。Directory Services 信任 CORP AD 中的登入資料，允許 AMS 端內的堆疊允許使用 CORP 登入資料進行登入。

> **Note**
>
> AMS 設定信任的 Active Directory (AD) 必須是擁有您授權之使用者帳戶的目錄，才能存取您的 AWS 資源。

建立 Active Directory 信任

若要設定信任，AMS 需要網域控制站本機政策 -> 安全選項 -> 網路存取：可匿名存取的具名管道，請列出 Netlogon 和 lsarpc 管道。這些管道預設會列出，但有時會因安全性考量而移除。建立信任之後，即可再次從清單中移除信任。

設定條件式轉寄站

1. 在 AD DNS Manager -> 建立新的條件式轉寄站中，在 DNS 網域下：使用提供給您的網域名稱 AMS；例如，https：//A523434123.amazonaws.com（將此變更為加入問卷中選取的網域名稱。
2. 在主伺服器的 IP 地址下：新增 AMS 提供的 IP 地址。驗證這兩個地址，確認沒有連線問題。

3. 選取將此條件式轉送器儲存在 Active Directory 中，並如下複寫：此網域中的所有 DNS 伺服器，然後按確定。

設定 AD 信任

遵循此 Microsoft AD 文章使用本節所述的設定和選項，為信任的一側建立單向、傳入、樹系信任。

1. 開啟開始 -> 管理工具 -> Active Directory 網域和信任對話方塊。在您要建立信任之網域的網域節點上按一下滑鼠右鍵，然後按一下屬性 -> 信任 -> 新信任以開啟新信任精靈。輸入 AMS 針對信任名稱提供給您的網域名稱，然後按下一步。
2. 在信任類型下，選取適當的信任層級 （ 例如樹系信任 ）。PressNext。
3. 在信任方向下，選取單向：傳入。按下 Next (下一步)。
4. 在信任面下，僅選取此網域。按下 Next (下一步)。
5. 在信任密碼下，輸入您選擇的密碼。按下 Next (下一步)。
6. 對於信任選擇已完成和信任建立完成，只需按下一步。
7. 在確認傳入信任下，選取否，不要確認傳入信任。按下 Next (下一步)。
8. 在完成新的信任精靈下，選取完成，然後確定關閉。
9. 提供信任密碼 （ 基於安全理由，請透過 CSDM 的電話號碼聯絡我們 ）。AMS 將完成信任組態。

Active Directory 網站和服務

若要降低登入延遲，請將 VPC CIDR 範圍新增至您的 Active Directory 網站和服務 (Start -> 管理工具 -> Active Directory 網站和服務)。將 VPC CIDR 範圍新增至 Active Directory 網站，其中包含最接近 AWS 的網域控制站。

將 AMS 專用網站的 AD 網站名稱提供給 CSDM。AMS 將重新命名 AD AMS 端的預設網站，以符合提供的名稱。

Active Directory 名稱尾碼路由

建立單向樹系信任之後，請完成下列步驟以驗證尾碼路由：

1. 在開始 > 所有程式 > 管理工具下，按一下 Active Directory 網域和信任。

   Active Directory 網域和信任主控台隨即開啟。
2. 在公司網域上按一下滑鼠右鍵，然後按一下屬性

   該網域的屬性對話方塊隨即開啟。

3. 按一下信任索引標籤。

   信任頁面隨即開啟。

4. 按一下 Amazon 網域名稱，然後按一下屬性。

   Amazon 網域信任的屬性頁面隨即開啟。

5. 按一下名稱尾碼路由，然後按一下重新整理。

   請確定沒有衝突，以確保服務委託人名稱 (SPNs) 可以透過信任解析。

將 Active Directory 與 AMS IAM 角色聯合

將您的目錄與 AMS IAM 角色聯合的目的是讓企業使用者使用其企業憑證與 AWS 主控台和 AWS APIs 互動，因此 AMS 主控台和 APIs。

聯合程序範例

此範例使用 Active Directory Federation Services (AD FS)；不過，支援 AWS IAM Federation 的任何技術都受到支援。如需 AWS 支援的 IAM 聯合的詳細資訊，請參閱 IAM 合作夥伴和身分提供者和聯合。您的 CSDM 將協助您完成此程序，這涉及與 AD 團隊和 AMS 的共同工作。

如需整合 SAML for API 存取的詳細資訊，請參閱此 AWS 部落格：如何使用 SAML 2.0 和 AD FS 實作聯合 API 和 CLI 存取。

如需安裝 AMS CLI 和 SAML 的範例，請參閱附錄：AD FS 宣告規則和 SAML 設定。

設定 AMS 主控台的聯合 (MALZ)

下表中詳述的 IAM 角色和 SAML 身分提供者（受信任實體）已佈建為 AMS 基礎設施的一部分。這些角色可讓您稽核和檢視 AMS 核心帳戶。

角色	權限
AWSManagedServicesReadOnlyRole	可讓您檢視核心帳戶中的 AMS 基礎設施。
AWSManagedServicesCaseRole	可讓您檢視新應用程式帳戶中的資源，並提交 AMS 事件和服務請求。
AWSManagedServicesChangeManagementRole	可讓您檢視核心帳戶中的 AMS 基礎設施、提交 AWS Support 票證，以及請求一些 RFCs。

如需不同帳戶下可用角色的完整清單，請參閱 AMS 中的 IAM 使用者角色。

驗證主控台存取

使用 ADFS 設定好並具有要用於身分驗證的 AMS URL 後，請依照下列步驟進行。

使用 Active Directory 聯合服務 (ADFS) 組態，您可以遵循下列步驟：

1. 開啟瀏覽器視窗，並前往為您的帳戶提供給您的登入頁面。您帳戶的 ADFS IdpInitiatedSignOn 頁面隨即開啟。
2. 選取登入下列其中一個網站旁的選項按鈕。登入網站挑選清單會變成作用中。
3. 選擇 signin.aws.amazon.com 網站，然後按一下登入。用於輸入登入資料的選項會開啟。
4. 輸入您的 CORP 登入資料，然後按一下登入。隨即 AWS 管理主控台 開啟。
5. 將 AMS 主控台 URL 貼到位置列，然後按 Enter 鍵。AMS 主控台隨即開啟。

驗證 API 存取

AMS 使用 AWS API，搭配一些您可以在 AMS API 參考中閱讀的 AMS 特定操作。

AWS 提供數個 SDK，您可以在 Tools for Amazon Web Services 中存取這些SDKs。如果您不想使用 SDK，您可以直接進行 API 呼叫。如需身分驗證的資訊，請參閱簽署 AWS API 請求。如果您不是使用 SDK，或直接提出 HTTP API 請求，則可以使用適用於變更管理 (CM) 和 SKMS 的 AMS CLIs。

安裝 AMS CLIs

AWS CLI 是使用 AMS CLIs（變更管理和 SKMS) 的先決條件。

1. 若要安裝 AWS CLI，請參閱安裝 AWS 命令列界面，並遵循適當的指示。請注意，在該頁面底部有使用不同安裝程式、Linux、MS Windows、macOS、虛擬環境、 Bundled Installer (Linux、macOS 或 Unix) 的說明。
2. 安裝之後，請執行 aws 協助來驗證安裝。
3. 安裝 AWS CLI 後，若要安裝或升級 AMS CLI，請下載 AMS 可分發 zip 檔案並解壓縮。您可以透過 AMS 主控台左側導覽中的文件連結存取 AMS CLI 可分發項目，或要求雲端服務交付管理員 (CSDM) 傳送 zip 檔案給您。
4. 根據您的作業系統開啟 Managed Cloud Distributables -> CLI -> Windows 或 Managed Cloud Distributables -> CLI -> Linux / MacOS 目錄，以及：
5. 對於 Windows，請執行適當的安裝程式（此方法僅適用於 Windows 32 或 64 位元系統）：

- 32 位元：ManagedCloudAPI_x86.msi
- 64 位元：ManagedCloudAPI_x64.msi

6. 對於 Mac/Linux，執行此命令來執行名為：MC_CLI.sh 的檔案：sh MC_CLI.sh。請注意，amscm 和 amsskms 目錄及其內容必須與 MC_CLI.sh 檔案位於相同的目錄中。
7. 如果您的公司登入資料是透過與 AWS (AMS 預設組態） 聯合使用，您必須安裝登入資料管理工具，以存取您的聯合服務。例如，您可以使用此 AWS 安全部落格 如何使用 SAML 2.0 和 AD FS 實作聯合 API 和 CLI 存取，以協助設定您的憑證管理工具。
8. 安裝之後，請執行 `aws amscm help`和 `aws amsskms help` 以查看命令和選項。

MALZ：應用程式帳戶加入

您必須先使用核心帳戶設定多帳戶 AWS Managed Services (AMS) 環境，才能請求新的應用程式帳戶。以下是您在設定環境之後需要採取的步驟。

主題

如有加入問題，請聯絡您的雲端服務交付經理 (CSDM)。另請參閱應用程式帳戶：AMS 受管、開發模式、客戶受管。如需模式的一般資訊，請參閱 AMS 模式AWS Managed Services 中的服務管理。

如需應用程式帳戶不同模式的資訊，請參閱應用程式帳戶：AMS 受管、開發模式、客戶受管。如需模式的一般資訊，請參閱 AMS 模式。

請求新的應用程式帳戶

您必須先使用核心帳戶設定多帳戶 AWS Managed Services (AMS) 環境，才能請求新的應用程式帳戶。如需使用核心帳戶設定多帳戶環境的資訊，請參閱 MALZ：核心帳戶加入。

您可以為應用程式帳戶中的初始 VPC 選擇下列其中一個 Amazon VPC 類型：

- 私有：此 VPC 未連接網際網路閘道。這適用於不需要存取網際網路或從網際網路存取的私有應用程式。

- 公有：此 VPC 已連接網際網路閘道，並具有公有和私有子網路。這適用於需要存取網際網路或從網際網路存取的公有應用程式。

您可以提交部署 | 受管登陸區域 | 管理帳戶 | 建立應用程式帳戶 （ 使用 VPC) (ct-1zdasmc2ewzrs) RFC，並在 RFC 中提供下列值，以請求新的應用程式帳戶：

- 帳戶名稱：帳戶的自訂名稱。請注意，帳戶名稱的長度上限為 50 個字元。
- 帳戶電子郵件：帳戶的分發清單電子郵件。此電子郵件 ID 用於建立 AWS 帳戶。
- 支援層級：AWS Support 層級、Premium 或 Plus。
- VPC 名稱：VPC 的名稱。
- 可用區域 (AZs) 數量：2 或 3。
- VPC CIDR：VPC 的 CIDR 區塊。
- 路由類型：可以是 `routable`或 `isolated`。 `Routable`表示與 Transit Gateway (TGW) 應用程式路由表相關聯的應用程式 VPCs 可以連接到此 VPC。 `Isolated`表示與 TGW 應用程式路由表相關聯的應用程式 VPCs 無法連接到此 VPC。預設值為 `routable`。
- Transit Gateway 應用程式路由表：應用程式帳戶 VPC 必須與之建立關聯的 Transit Gateway 路由表。如果未提供任何值，`defaultAppRouteDomain`則會使用預設值，這表示此帳戶將能夠與相同路由表下的所有其他帳戶通訊。
- AZ 1 中公有子網路的 PublicSubnetAZ<1-3>CIDRCIDR：可用區域 1 中公有子網路的 CIDR。
- AZ 1 中公有子網路的 PrivateSubnet<1-10>AZ*<I-3>*CIDRCIDR：可用區域 1 中公有子網路的 CIDR。

此時，AMS 會使用指定的 VPC 組態，將新的應用程式帳戶部署到您的 AMS 管理帳戶。

設定 Active Directory 以聯合存取 AMS IAM 角色

將您的目錄與 AMS IAM 角色聯合，讓公司使用者能夠使用其公司登入資料與 AWS 主控台和 AWS APIs，以及 AMS 主控台和 AMS APIs 互動。

聯合程序範例

此範例使用 Active Directory Federation Services (ADFS)。不過，支援 AWS IAM Federation 的任何技術都受到支援。如需 AWS 支援的 IAM 聯合的詳細資訊，請參閱 IAM 合作夥伴和身分提供者和聯合。您的 CSDM 將協助您完成此程序，這涉及與 AD 團隊和 AMS 的共同工作。

如需整合 SAML for API 存取的詳細資訊，請參閱此 AWS 部落格：如何使用 SAML 2.0 和 AD FS 實作聯合 API 和 CLI 存取。

如需安裝 AMS CLI 和 SAML 的範例，請參閱《AMS 使用者指南》中的附錄：AD FS 宣告規則和 SAML 設定。

設定 AMS 主控台的聯合

下表中詳述的 IAM 角色和 SAML 身分提供者（受信任實體）會在您的新應用程式帳戶中佈建。這些角色可讓您存取新的應用程式帳戶和檔案 RFCs、寫入 S3 儲存貯體，以及執行其他動作。

Role	權限
AWSManagedServicesReadOnlyRole	可讓您檢視新應用程式帳戶中的資源。
AWSManagedServicesCaseRole	可讓您檢視新應用程式帳戶中的資源，並提交 AWS Support 票證。
AWSManagedServicesChangeManagementRole	可讓您檢視應用程式帳戶中的 AMS 基礎設施、檔案 RFCs、檔案 AWS Support 票證、寫入 S3 儲存貯體、管理 Secrets Manager 秘密，以及管理預留 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體。
AWSManagedServicesSecurityOpsRole	可讓您檢視應用程式帳戶中的 AMS 基礎設施、管理 Secrets Manager 秘密、管理 Web Application Firewall 規則、管理憑證和檔案 AWS Support 票證。
AWSManagedServicesAdminRole	可讓您檢視應用程式帳戶中的 AMS 基礎設施、管理 Marketplace 訂閱、管理 Secrets Manager 秘密、管理 Web Application Firewall 規則、管理憑證、建立 RFCs、管理預留 Amazon EC2 執行個體、寫入 S3 儲存貯體、檔案 AWS Support 票證，以及管理 AWS Artifacts 協議。

將聯合請求提交至 AMS

如果這是您的第一個帳戶，請使用您的 CSDM 和/或 Cloud Architect(s)，為您的身分提供者提供中繼資料 XML 檔案。

如果您要加入其他帳戶或身分提供者，並有權存取管理帳戶或所需的應用程式帳戶，請遵循下列步驟。

1. 從 AMS 主控台建立服務請求。

> **Note**
>
> - 如果為應用程式帳戶建立身分提供者，請從應用程式帳戶本身或管理帳戶提交此請求。
> - 如果為 AMS 核心帳戶建立身分提供者，請從管理帳戶提交此請求。
> - 如果為管理帳戶建立身分提供者，請從管理帳戶提交此請求，或聯絡您的 CSDM 尋求協助。

在服務請求中，提供新增身分提供者所需的詳細資訊：

- 將建立新身分提供者的帳戶的 AccountId。
- 所需的身分提供者名稱，若未提供，預設值將為 customer-saml；通常，這必須符合聯合提供者中設定的設定。
- 對於現有帳戶，包括是否應將新的身分提供者傳播至所有現有的主控台角色，或提供應信任新身分提供者的角色清單。
- 將從您的聯合代理程式匯出的中繼資料 XML 檔案做為檔案附件連接到服務請求。

2. 從您建立服務請求的相同帳戶中，使用 CT-ID ct-1e1xtak34nx76（管理 | 其他 | 其他 | 建立）建立新的 RFC，並包含下列資訊。

- 標題：「帳戶 <AccountId> 的內建 SAML IDP <Name>」。
- 要建立身分提供者之帳戶的 AccountId。
- 身分提供者名稱。
- 對於現有帳戶：身分提供者是否應傳播至所有現有的主控台角色，或應信任新身分提供者的角色清單。
- 在步驟 1 中建立的服務請求的案例 ID，其中連接中繼資料 XML 檔案。

驗證主控台存取

使用 AD FS 設定並具有用於身分驗證的 AMS URL 之後，您可以執行下列程序。

使用 Active Directory 聯合服務 (AD FS) 組態，您可以遵循下列步驟：

1. 開啟瀏覽器視窗，並前往為您的帳戶提供給您的登入頁面。您帳戶的 AD FS IdpInitiatedSignOn 頁面隨即開啟。
2. 選取登入下列其中一個網站旁的選項按鈕。登入網站清單會變成作用中。
3. 選擇 signin.aws.amazon.com 網站，然後選擇登入。用於輸入登入資料的選項會開啟。
4. 輸入您的 CORP 登入資料，然後選擇登入。AWS 管理主控台隨即開啟。
5. 將 AMS 主控台 URL 貼到位置列，然後按 Enter 鍵。AMS 主控台隨即開啟。

驗證 API 存取

AMS 使用 AWS API，搭配一些您可以在 AMS API 參考中閱讀的 AMS 特定操作。

AWS 提供數個 SDK，您可以在 Tools for Amazon Web Services 中存取這些SDKs。如果您不想使用 SDK，您可以直接進行 API 呼叫。如需身分驗證的資訊，請參閱簽署 AWS API 請求。如果您不是使用 SDK，或直接提出 HTTP API 請求，則可以使用適用於變更管理 (CM) 和 SKMS 的 AMS CLIs。

使用新的應用程式帳戶設定聯網

設定應用程式帳戶的聯網包括設定防火牆規則，以及可能設定其他 Transit Gateway (TGW) 路由表。

設定防火牆

若要使用 AMS 環境中部署的應用程式，您必須建立一些防火牆規則。您不需要這些規則來存取執行個體，就可以跳過堡壘到執行個體。

應用程式存取的防火牆規則

您必須為透過防火牆的流量開啟下列連接埠：

- 從內部部署網路到輸入和輸出方向的新應用程式 VPC CIDRs。
- 從新應用程式 VPC CIDRs 到內部部署網路的輸入和輸出方向 （如果您的雲端應用程式需要連線到內部部署應用程式）。

連接埠	通訊協定	服務	往返	往返
80	TCP	HTTP Web 存取	在內部部署網路上	AMS 應用程式 VPC
443	TCP	HTTPS Web 存取	在內部部署網路上	AMS 應用程式 VPC

設定其他傳輸閘道應用程式路由表

AWS Managed Services (AMS) 網路具有彈性，並支援各種聯網使用案例。

- 相同帳戶中應用程式 VPCs之間的通訊。
- 不同帳戶中應用程式 VPCs之間的通訊。
- 隔離不同帳戶中的應用程式 VPCs。
- 相同帳戶中應用程式 VPCs之間的隔離。

如果您對於聯網有唯一/特殊的需求，請聯絡您的 AMS Cloud Architect，他們會制定 AMS 網路架構符合您需求的計劃。

根據應用程式帳戶 VPCs 所採取的聯網決策，您可以透過提交部署 | 受管登陸區域 | 網路帳戶 | 建立傳輸閘道路由表 (ct-3dscwaeyi6cup) RFC 來建立多個 Transit Gateway (TGW) 應用程式路由表。

變更類型需要您指定 `TransitGatewayRouteTableName`(TGW 路由表的有意義的名稱) `TransitGatewayId`、 和 `TGWRouteTableType`。

> **Note**
>
> 如果為 TGWRouteTableType 選取 createCustomRouteDomain，則建立的路由表為空白。您必須使用部署 | 受管登陸區域 | 網路帳戶 | 新增靜態路由 (ct-3r2ckznmt0a59) 變更類型來提交 RFC。

在應用程式帳戶中設定其他 VPCs

您可以提交部署 | 受管登陸區域 | 應用程式帳戶 | 建立 VPC (ct-1j3503fres5a5) RFC 來請求額外的應用程式帳戶 VPC。

這的運作方式與為新應用程式帳戶設定 VPC 的方式相同。如需詳細資訊，請參閱請求新的應用程式帳戶。

附錄：多帳戶登陸區域 (MALZ) 加入考量清單

在規劃 AMS 多帳戶登陸區域部署時，您需要考慮幾個關鍵考量事項。您的選擇將提供 AMS 所需的資訊，以判斷您需要的基礎設施元件。您的雲端架構師 (CA) 將為您提供問卷，協助您完成這項工作。

主題

> **Note**
>
> 如需執行個體類型的詳細資訊，請參閱 Amazon EC2 執行個體類型。
> 如需資料庫執行個體類型的詳細資訊，請參閱 Amazon RDS 執行個體類型。
> 如果您需要直接連線，請參閱 AMS 單一帳戶登陸區域加入指南，以建立 Direct Connect 連線。

您會收到 Cloud Service Delivery Manager (CSDM) 的入門問卷，其中包含有關帳戶所需組態設定的問題。使用 CSDM 完成問卷，然後再繼續。

AMS 多帳戶登陸區域帳戶組態

- 新帳戶 ID

  您為 AMS 多帳戶登陸區域建立的 AWS 帳戶 ID。不應成為 AWS 組織的一部分。
- 服務區域

  要部署 AMS 多帳戶登陸區域環境的主要區域。

- 用於通知的核心帳戶電子郵件。（這些應該都位於相同的網域中）。為每個 提供電子郵件地址：
  - 共用服務帳戶
  - 網路帳戶
  - 記錄帳戶
  - 安全帳戶
- 您的服務類型，Premium 或 Plus

  這會決定解決您環境中問題的服務層級協議 (SLAs)

AMS 多帳戶登陸區域監控提醒

AMS 可讓您直接收到特定監控提醒的提醒（而不是收到 AMS 服務通知）。若要註冊，請確定您的 Cloud Architect (CA) 或 Cloud Service Delivery Manager (CSDM) 收到此資訊：

直接提醒電子郵件：這些是您希望 AMS 傳送特定資源型提醒的電子郵件地址。如需哪些提醒會直接傳送到電子郵件的詳細資訊，請參閱《AMS 進階使用者指南》中的 AMS 中基準監控的提醒。 如需 AMS 監控的詳細資訊，請參閱《AMS 單一帳戶登陸區域使用者指南》中的監控管理。

網路組態

- 傳輸閘道 ASN 號碼

  這是邊界閘道協定 (BGP) 工作階段 AWS 端的自治系統編號 (ASN)，必須是唯一的，且不能與 Direct Connect 或 VPN 相同的系統編號。 16 位元 ASNs 的範圍為 64512 到 65534（含）。
- 您的 AMS 多帳戶登陸區域基礎設施 VPC CIDR 範圍。

  這些 CIDR 範圍不能與您的內部部署網路重疊

  您可以包含 /22 CIDR 範圍，或個別提供每個 VPC CIDR。請注意，只允許這些 CIDR 範圍：
  - 10.0.0.0 – 10.255.255.255 (10/8 字首)
  - 172.16.0.0 – 172.31.255.255 (172.16/12 字首)
  - 192.168.0.0 – 192.168.255.255 (192.168/16 字首)

  請注意，可能無法使用 IP 範圍 198.18.0.0/15（由 AWS Directory Service 保留）。
  - 核心基礎設施 VPC CIDR 範圍（建議 /22 範圍）
  - 網路 VPC CIDR 範圍（建議 /24 範圍）

- 共享服務 VPC CIDR 範圍 （ 建議 /23 範圍 ）
- DMZ VPC CIDR 範圍 （ 建議 /25 範圍 ）

- VPN ECMP （ 啟用或停用 ）

  若您要在 VPN 連線中取得等價多路徑 (ECMP) 路由支援，請在 VPN ECMP support (VPN ECMP 支援) 中選擇 enable (啟用)。若連接公告相同 CIDR，則流量就是在其之間平均分佈。

網路存取控制清單 (NACL)

網路存取控制清單 (NACL) 是 VPC 的選用安全層，可做為防火牆來控制傳入和傳出一或多個子網路的流量。您可以使用與您的安全群組相似的規則來設定網路 ACL，以為您的 VPC 新增額外的安全 layer。如需安全群組和網路 ACLs 之間差異的詳細資訊，請參閱安全群組和網路 ACLs的比較。

不過，在 AMS 多帳戶登陸區域中，為了讓 AMS 有效管理和監控基礎設施，NACLs 的使用僅限於下列範圍：

- 多帳戶登陸區域核心帳戶不支援 NACLs：管理、聯網、共享服務、記錄和安全性。
- 多帳戶登陸區域應用程式帳戶支援 NACLs，只要它們只用作「拒絕」清單即可。此外，他們必須設定「允許全部」以確保 AMS 監控和管理操作。

在大規模的多帳戶環境中，您也可以利用集中式輸出防火牆等功能來控制 AMS 多帳戶登陸區域中的傳出流量和/或 AWS Transit Gateway 路由表，以隔離 VPCs之間的網路流量。

Active Directory 組態

AMS 受管 Active Directory 的網域 FQDN

Trend Micro Endpoint Protection (EPS)

- EC2 執行個體和 Auto Scaling 群組的執行個體大小

  Trend Micro Endpoint Protection (EPS) 是 AMS 中維護作業系統安全的主要元件。系統包含 Deep Security Manager (DSM) EC2 執行個體、轉送 EC2 執行個體，以及存在於所有 AMS 資料平面和 EC2 執行個體中的代理程式。

  - 轉送執行個體類型 (AMS 支援的最小值為 m5.large)
  - 資料庫執行個體大小 （ 建議 200 GB)
  - RDS 執行個體類型 （ 僅允許 db.m5.large 或 db.m5.xlarge)

- DSM 授權類型 (Marketplace 或 BYOL)

  如果您已經有授權，請選擇 BYOL （使用您自己的授權）。AMS 會與您聯絡，以取得授權的必要資訊。

- AWS Trend Micro Deep Security 訂閱的 IAM 使用者或角色 Amazon 資源名稱 (ARN) （角色 ARN：arn：aws：iam：：*ACCOUNT_ID*：role/*ROLE_NAME*)

  提供 IAM 角色、ARN 或 IAM 使用者 ARN，這些 ARN 來自 AWS 帳戶 您具有存取權的現有 之一。AMS 會建立 IAM 角色；在您的 AMS 多帳戶登陸區域共用服務帳戶中，並新增在共用服務中信任 IAM 角色時提供的角色或使用者，讓您可以擔任該角色以訂閱 Trend Micro Deep Security AWS Marketplace。

存取：堡壘、SSH 和 RDP

- SSH 堡壘設定

  AMS 會在您的共用服務帳戶中提供 SSH 堡壘，以存取 AMS 環境中的主機。若要以 SSH 使用者身分存取 AMS 網路，您必須使用 SSH 堡壘做為進入點。網路路徑源自現場部署網路，經過 DX/VPN 到傳輸閘道 (TGW)，然後路由到共用服務 VPC。一旦能夠存取堡壘，您就可以跳到 AMS 環境中的其他主機，前提是已授予適當的存取請求。

  - 所需的執行個體計數 （建議 2 個）
  - 執行個體上限 （建議使用 4 個）
  - 最小執行個體 （建議 2 個）
  - 執行個體類型 （建議使用 m5.large)
  - 輸入 CIDRs：IP 地址範圍，網路中的使用者將從中存取 SSH 堡壘 (ip 範圍 1、ip 範圍 2、ip 範圍 3、... 等）

- RDP 堡壘設定

  AMS 可選擇在您的共用服務帳戶中提供 RDP 堡壘，以存取 AMS 環境中的主機。若要以 RDP 使用者身分存取 AMS 網路，您必須使用 RDP 堡壘做為進入點。網路路徑源自現場部署網路，經過 DX/VPN 到 TGW，然後路由到共用服務 VPC。一旦能夠存取堡壘，您就可以跳到 AMS 環境中的其他主機，前提是已授予適當的存取請求。

  - 執行個體類型 （建議使用 t3.medium)
  - 所需的最小工作階段 （建議 2 個）
  - 所需的工作階段上限 （建議 10 個）

- RDP 堡壘組態類型、共用標準或共用 HA （預設為共用標準）

  SecureStandard = 使用者會收到一個堡壘，只有一個使用者可以連接到堡壘。

  SecureHA = 使用者在兩個不同的可用區域中接收兩個堡壘以連接到 ，只有一個使用者可以連接到堡壘。

  SharedStandard = 使用者會收到一個要連線的堡壘，兩個使用者可以一次連線到相同的堡壘。

  SharedHA = 使用者可以在兩個不同的可用區域中接收兩個堡壘以連接到 ，而兩個使用者可以一次連接到相同的堡壘。

聯合

身分提供者 (IDP) 名稱

預設為 `customer-saml`

AMS 單一帳戶登陸區域 (SALZ) 加入

AMS SALZ 加入程序

若要加入 AMS 單一帳戶登陸區域 (SALZ) 帳戶，您需要採取下列步驟：

1. 建立新的 AWS 帳戶，AMS 會將其設定為託管防火牆的網路帳戶。如果您有新帳戶，請在 AWS 組織內建立新的帳戶。AMS 將遵循建立一般 AMS 帳戶的程序，因此必須收集所有必要的資訊（例如 CIDR、EPS 授權和使用者）。注意：/24 的 CIDR 配置良好。
2. 指定是否要從輸出流量帳戶移除網際網路閘道 (IGWs)。
3. 判斷您核准的網域。AMS 可透過維護核准的網域清單來啟用目的地篩選；清單稍後可以修改。
4. 根據預期的輸送量，確認您想要使用的執行個體大小。根據預設，執行個體是在 m4.xlarge 執行個體中建立，其中我們發現防火牆輸送量為 350Mbps。AMS 可以將大小增加到 c4.8xLarge 執行個體，預期輸送量為 1.25 Gbps。
5. 設定 AMS 和私有網路之間的聯網。這包含多個任務：
    a. 配置 IP 空間
    b. 建立私有網路連線至 AWS
    c. 設定您的防火牆
    d. 設定存取管理
    e. 排程備份
6. 提供 AMS 對已建立帳戶的存取權。
7. 驗證 AMS 服務是否正常運作。

AMS 將能夠在初始請求日期的 2 週 (10 個工作日） 內執行您帳戶的帳戶建置 （加入）。您可以使用 AMS 計劃事件管理 (PEM) 來執行任何後續活動。

> **Note**
>
> - 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)
- 歐洲西部 （ 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)

新區域會經常新增。如需最新清單，請參閱 AWS 區域和可用區域。

SALZ 網路架構

下圖說明 AWS Managed Services (AMS) 單一帳戶登陸區域 (SALZ) VPC 網路配置，是高可用性設定的範例。

AMS 會根據我們的標準範本和您在加入期間提供的所選選項，為您設定聯網的所有層面。標準 AWS 網路設計會套用至您的 AWS 帳戶，並為您建立虛擬私有雲端 (VPC)，並透過 VPN 或 Direct Connect 連線至 AMS。進一步了解 AWS Direct Connect 的 Direct Connect。標準 VPCs包括 DMZ、共用服務和應用程式子網路。在加入過程中，可能會請求並建立其他 VPCs 以符合您的需求 （ 例如，客戶部門、合作夥伴 ）。加入後，您會收到網路圖表。 環境文件，說明您的網路設定方式。

> **Note**
>
> 若要了解所有作用中服務的預設服務限制和限制，請參閱 AWS 服務限制文件。

我們的網路設計是以 Amazon「最低權限原則」為基礎建置。為了達成此目的，我們透過閘道路由所有傳入和傳出流量，但來自信任網路的流量除外。唯一信任的網路是透過使用 VPN 和/或 AWS Direct

Connect (DX) 在內部部署環境和 VPC 之間設定的網路。透過使用堡壘執行個體授予存取權，從而防止直接存取任何生產資源。您的所有應用程式和資源都位於可透過公有負載平衡器連線的私有子網路內。公有輸出流量會透過我們的轉送代理流向網際網路閘道，然後流向網際網路。或者，流量可以透過 VPN 或 Direct Connect 流向內部部署環境。

AMS 單一帳戶登陸區域共用服務

共用服務子網路包含 AMS Directory Services、自動化佈建和常見任務的 Management Host、防毒 (TrendMicro) 管理伺服器，以及內部堡壘主機：

- AMS Directory Services = AD 網域控制站

  在 AMS 帳戶中建立 Active Directory、建立 AMS 網域、在啟動時將受管堆疊加入網域。
- 管理主機 = AMS 管理主機 （ 自動佈建和常見任務 ）

  做為要修改的 API 端點 Directory Service，並與 Directory Service 網域控制站互動。
- 安全服務：防毒 (TrendMicro) 管理伺服器 = EPS DSM + EPS 轉送

  利用 Trend Micro++ Deep Security 軟體 (DSM)，在用戶端伺服器模型中運作，並具有後端資料庫，包括 Deep Security 管理員、代理程式和轉送。
- 內部堡壘主機 = 客戶堡壘

  特殊用途伺服器，設計為網際網路的主要存取點，並做為其他 Amazon EC2 執行個體的代理。

SALZ：為 AMS 建立新 AWS 帳戶

為 AWS Managed Services (AMS) 建立新 AWS 帳戶的五個步驟如下：

1. 建立 AWS 帳戶
2. 設定合併帳單 - 將新帳戶連結至付款人帳戶
3. 設定您的 AWS 帳戶 以進行 AMS 存取
4. 使用 AMS 中根使用者的多重要素驗證 (MFA) 保護新帳戶
5. 訂閱 AWS Marketplace for EPS

如果您有任何問題，請聯絡您的客戶服務交付經理 (CSDM)。

建立 AWS 帳戶

AMS 計劃需要佈建新的 Amazon Web Services (AWS) 帳戶。以下影片提供逐步說明：如何建立和啟用新的 Amazon Web Services 帳戶？ 簡單步驟包括：

註冊 AWS 帳戶

如果您沒有 AWS 帳戶，請完成下列步驟來建立一個。

註冊 AWS 帳戶

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

   部分註冊程序需接收來電或簡訊，並在電話鍵盤輸入驗證碼。

   當您註冊 時 AWS 帳戶，AWS 帳戶根使用者會建立 。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。作為安全最佳實務，請將管理存取權指派給使用者，並且僅使用根使用者來執行需要根使用者存取權的任務。

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

建立具有管理存取權的使用者

註冊 後 AWS 帳戶，請保護 AWS 帳戶根使用者、啟用 AWS IAM Identity Center和建立管理使用者，以免將根使用者用於日常任務。

保護您的 AWS 帳戶根使用者

1. 選擇根使用者並輸入 AWS 帳戶 您的電子郵件地址，以帳戶擁有者AWS 管理主控台身分登入 。在下一頁中，輸入您的密碼。

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

   如需說明，請參閱《IAM 使用者指南》中的為您的 AWS 帳戶 根使用者 （ 主控台 ） 啟用虛擬 MFA 裝置。

建立具有管理存取權的使用者

1. 啟用 IAM Identity Center。

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的啟用 AWS IAM Identity Center。

2. 在 IAM Identity Center 中，將管理存取權授予使用者。

   如需使用 IAM Identity Center 目錄 做為身分來源的教學課程，請參閱AWS IAM Identity Center 《 使用者指南》中的使用預設值設定使用者存取 IAM Identity Center 目錄。

以具有管理存取權的使用者身分登入

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

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

指派存取權給其他使用者

1. 在 IAM Identity Center 中，建立一個許可集來遵循套用最低權限的最佳實務。

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的建立許可集。

2. 將使用者指派至群組，然後對該群組指派單一登入存取權。

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的新增群組。

> **Note**
>
> 如果您已有 帳戶，您可以前往AWS 定價頁面，然後按一下建立免費帳戶。請務必至少註冊 EC2 服務。註冊一項服務可讓您存取 中的所有服務 AWS。您只需支付實際使用服務的費用。如果您計劃將新帳戶連結至付款人帳戶以進行合併帳單，則不需要在出現提示時輸入付款方式資訊。相反地，當您到達畫面輸入信用卡資訊時，只需瀏覽即可。您需要與付款人帳戶相關聯的電子郵件地址，才能傳送合併帳單/連結帳戶請求，請參閱下一節。

> **Important**
>
> 請務必確保電子郵件地址和電話號碼與帳戶相關聯，以便收到潛在安全事件的回應。在未重設帳戶密碼的情況下，無法變更帳戶的電話號碼和電子郵件地址，這是 AMS 根帳戶的重要任務。為了確保這些值穩定，請務必選取與個人無關的聯絡資訊，這可能會變更。選擇可以指向群組的電子郵件別名。在選取電話號碼時，請遵循相同的最佳實務：選擇可以指向群組的號碼，或指向公司擁有的號碼，而不是個人。

設定合併帳單 - 將新帳戶連結至付款人帳戶

如果您想要將新的 AMS 受管 AWS 帳戶 帳單轉換為現有 AWS Organizations 管理帳戶的付款，則需要設定合併帳單並連結帳戶。如需執行此作業的詳細資訊，請參閱

- 和多帳戶帳單策略的合併 AWS Organizations帳單。 AWS
- 邀請 AWS 帳戶 加入您的組織

> **Note**
>
> 您可以在執行帳戶移交給 AMS 之前執行這些步驟。交接之後，即可透過變更管理程序完成加入組織的步驟 （ 如前所述 ）。如果您需要協助，請洽詢您的雲端服務交付管理員 (CSDM) 或雲端架構師 (CA)。

如需管理合併帳單的一般帳單資訊，請參閱什麼是 AWS 帳單。如需帳戶如何一起運作的 AWS Organizations 一般資訊，請參閱什麼是 AWS Organizations 。如需 AWS Organizations 管理帳戶的規範指引，請參閱管理帳戶、受信任存取和委派管理員

設定您的 AWS 帳戶 以進行 AMS 存取

完成上述步驟後，您已成功保護新的 AWS 帳戶 和確保相關的成本，並適當地計費。程序的最後一步是允許 AMS 存取新帳戶以進行初始堆疊組態，以及持續的變更和佈建請求。如需詳細資訊，請參閱使用 IAM 角色跨 AWS 帳戶委派存取權。本節說明基本步驟。

啟用 AWS 對網站的存取

若要授予 IAM 使用者存取您帳戶的帳單資訊和工具的權限，您必須啟用 功能。

請遵循下列步驟：

1. AWS 管理主控台 使用您的根帳戶登入資料 （您用來建立 的電子郵件和密碼 AWS 帳戶) 登入 。請勿使用您的 IAM 使用者登入資料進行登入。

   AWS 管理主控台 首頁隨即開啟。
2. 在頂端導覽列中，開啟您帳戶名稱的下拉式選單，然後選擇我的帳戶。

   帳單首頁隨即開啟。
3. 向下捲動至 IAM 使用者存取帳單資訊區域，然後按一下右側的編輯。除非您##################。

   啟用 IAM 存取區域隨即開啟。
4. 選取核取方塊，然後按一下更新。

   您現在可以使用 IAM 政策來控制使用者可以存取的頁面。

如需 中此程序的詳細資訊 AWS，請參閱管理存取許可的概觀。

建立可存取 AWS 網站的 IAM 角色

AWS Identity and Access Management (IAM) 是一種 Web 服務，可協助您安全地控制使用者對 AWS 資源的存取。您可以使用 IAM 來控制誰可以使用您的 AWS 資源 （身分驗證），以及他們可以使用哪些資源，以及其使用方式 （授權）。

1. 前往 IAM 管理主控台，按一下左側導覽窗格中的角色。

   角色管理頁面隨即開啟，其中包含 IAM 角色、建立角色選項和現有角色清單的相關資訊。

2. 按一下建立角色。

   建立角色 選取受信任實體的類型頁面隨即開啟。按一下其他 AWS 帳戶，設定區域隨即開啟如下。

   輸入 AMS 提供給您的 AMS 信任帳戶 ID。保留取消選取需要外部 ID 和需要 MFA 選項。

3. 按一下 Next: Permissions (下一步：許可)。

   建立角色連接許可政策頁面隨即開啟，其中包含建立新政策、
   重新整理頁面和搜尋現有政策的選項。提供現有政策的清單。

4. 選取 AdministratorAccess 政策，然後按一下下一步：檢閱。

   建立角色檢閱頁面隨即開啟。

5. 將新角色命名為 aws_managedservices_onboarding_role，並輸入角色描述的「AMS 加入角色」。檢閱新角色的設定，如果滿意，請按一下建立角色。

   角色管理頁面隨即開啟，並列出您的新角色。

訂閱 AWS Marketplace for EPS

AMS 端點安全 (EPS) 的最新變更需要您透過 訂閱 TrendMicro Deep Security， AWS Marketplace 並接受軟體條款。

TrendMicro 提供兩種授權模式：每個受保護執行個體小時和自帶授權 (BYOL)。

- BYOL：
  1. 您可以使用自己透過外部管道購買的授權。
  2. 您必須將所有授權金鑰提供給 AMS，才能建置 EPS 基礎設施。您可以提供授權所有模組的啟用碼，或授權特定組模組的個別啟用碼。AMS 只會建立與您提供的啟用碼對應的授權檔案。由於授權啟用會在上線期間發生，因此在 AMS 首席工程師和 CSDM 存在的情況下，您可以共用該資訊。
  3. 此外，您必須訂閱 BYOL TrendMicro Market Place AMI 訂閱。請參閱 Trend Micro Deep Security (BYOL)。
- 每個受保護執行個體小時數：
  1. 在此訂閱中，您不需要擁有任何先前取得的 Trend 授權。
  2. 不過，您必須訂閱 Marketplace 訂閱。
  3. 此模型不需要與 AMS 共用授權金鑰，因為會自動計量趨勢用量，包括軟體授權 + EC2 基礎設施用量。請參閱 Trend Micro Deep Security。

若要訂閱 Trend Micro，請依照下列步驟進行：

1. 登入您的 AWS 帳戶。
2. 導覽至 Trend Micro Deep Security (BYOL 或每個受保護執行個體小時） 產品頁面。

3. 按一下右側面板中的繼續訂閱。
4. 按一下右上角的接受條款。

在 Trend Micro Deep Security 中啟用 IDS 和 IPS

您可以請求 AMS 為您的帳戶啟用 Trend Micro 入侵偵測系統 (IDS) 和入侵保護系統 (IPS)，非預設功能。

若要這樣做，請提交更新請求（管理 | 其他 | 其他 | 更新），並包含接收 IDS 和 IPS 通知的電子郵件地址清單。這些地址會新增至您帳戶中的 SNS 主題，AMS 會為您建立該主題。

> **Note**
>
> AMS 無法新增任何可能干擾我們提供其他 AMS 服務能力的 Trend Micro 服務。

後續步驟：使用 AMS 中根使用者的多重要素驗證 (MFA) 保護新帳戶

訂閱 AWS Marketplace 適用於 CentOS 7.6 的

AMS 現在提供 CentOS 7 (x86_64) - 搭配由 Centos.org 販售的更新 HVM，做為 AMS AMI。若要使用此 AMI，您必須選擇加入 免費 Cent 作業系統授權，並接受所有 AMS 帳戶的授權。

若要訂閱，請前往 AWS Marketplace並遵循選擇加入的指示。

使用此產品不會產生軟體費用，但您仍需支付其他 AWS 費用，包括 EC2 用量。如果這是「自帶授權」產品，您必須擁有有效的軟體授權才能使用它。

您可以在 CentOS 7 (x86_64) - 透過更新 HVM 檢閱此軟體的資訊。

使用 AMS 中根使用者的多重要素驗證 (MFA) 保護新帳戶

本節已修訂，因為它包含敏感的 AMS 安全相關資訊。此資訊可透過 AMS 主控台文件取得。若要存取 AWS Artifact，您可以聯絡 CSDM 以取得指示，或前往 AWS Artifact 入門。

SALZ：設定聯網

設定 AWS Managed Services (AMS) 的聯網需要完成幾個程序：

1. 為您的 AMS 環境配置 IP 空間
2. 建立私有網路連線至 AWS
3. 設定防火牆以允許 AMS 操作

為您的 AMS 環境配置 IP 空間

AMS 的設計和測試使用 /16 CIDR 區塊做為建議的網路配置。連接至 AMS 的受信任網路必須使用與指派給 AMS 的 CIDR 區塊不重疊的 CIDR 區塊。設定虛擬私有雲端 (VPC) 和子網路需要這些地址。如需 AWS VPCs 的詳細資訊，請參閱 Amazon VPC 限制和 Amazon VPC FAQs。

雖然 /16 CIDR 區塊看起來像是許多 IP 地址，但一旦建立 VPC，就無法展開。因此，此配置可確保您的 AMS 受管 VPC 可在相當長的時間內運作。在 CIDR 區塊中，您必須為至少兩個私有子網路和兩個公有子網路配置 IP 地址範圍。

AWS 接受透過原生 AWS 虛擬私有網路 (VPN) 功能連線至 AMS 環境。在您這方面，您可以透過 AWS Direct Connect (DX)、硬體 VPN 或軟體 VPN 來達成。在 AMS 方面，我們使用 VPCs的虛擬閘道功能。

基本環境元件

使用者Network-to-Amazon VPC 連線選項	
硬體 VPN	建立從遠端網路上的網路設備到連接到 VPC 的 AMS 受管網路設備的硬體 VPN 連線。
AWS Direct Connect (DX)	利用 AWS Direct Connect，建立從遠端網路到 Amazon VPC 的私有、邏輯（或加密，如果與 VPN 搭配使用）連線。
軟體 VPN	建立從遠端網路設備到在 Amazon VPC 內執行之使用者受管軟體 VPN 設備的 VPN 連線。

> **Note**
>
> AMS 建議備援私有 VPN 到 DX 連線。您的客戶服務交付經理 (CSDM) 將在您的帳戶加入時協助設定此項目。

建立私有網路連線至 AWS

將 AMS 新增至您的公司 Active Directory 以建立連線。您可能想要透過私有網路連線執行管理動作或使用者存取。AWS 透過 提供 VPN 連線和專用線路 Direct Connect。下列步驟說明如何使用 AMS 來建立 （或兩者） 連線方式。

VPN 設定

本節說明設定 VPN 在 AMS 受管 VPC 與內部網路之間通訊的基本步驟。

> **Note**
>
> 若要全面了解將 VPN 與 AWS 服務搭配使用，請參閱什麼是 AWS Site-to-Site VPN 以及所有關於客戶閘道 （您的 VPN 設備）。

遵循 AWS VPN 使用者指南入門和測試Site-to-Site連接章節來完成以下步驟。

- 步驟 1：在您的 AWS VPC 中建立客戶閘道
- 步驟 2：在您的 AWS VPC 中，建立虛擬私有閘道
- 步驟 3：在您的 AWS VPC 中，在您的路由表中啟用路由傳播
- 步驟 4：在您的 AWS VPC 中，更新您的安全群組以啟用傳入 SSH、RDP 和 ICMP 存取
- 步驟 5：在您的內部網路中，建立 VPN 連線並設定客戶閘道
- 步驟 6：測試 VPC 與內部網路之間的 VPN 連線

Direct Connect 設定

本節說明設定 a Direct Connect (DX) 在 AMS 受管 VPC 與內部網路之間通訊的基本步驟。

> **Note**
>
> 如需搭配 AWS 服務使用 DX 的詳細資訊，請參閱 Direct Connect 位置入門。

若要設定 DX 連線，您需要完成下列步驟：

1. 註冊 Amazon Web Services
2. 提交 AWS Direct Connect 連線請求

3. 完成 Cross Connect
4. （選用）使用 AWS Direct Connect 設定備援連線
5. 由 AMS 執行：建立虛擬介面
6. 由 AMS 執行：下載路由器組態
7. 驗證您的虛擬界面

設定您的防火牆

本節已修訂，因為它包含敏感的 AMS 安全相關資訊。此資訊可透過 AMS 主控台文件取得。若要存取 AWS Artifact，您可以聯絡 CSDM 以取得指示，或前往 AWS Artifact 入門。

應用程式遷移/加入期間的 AMS 堡壘選項

為了在遷移工作期間為您提供最佳體驗，以下是 AMS 目前可以利用的潛在選項：

- 選項 1：僅針對遷移工作繞過堡壘（出於安全目的，您必須為此登出，作為臨時措施）。

  注意：稽核功能仍然存在，以確保 AMS 能夠查看每個請求。
- 選項 2：使用所選工具的 SSH 通道；例如 PuTTy，如圖所示。

  描述的環境元件必須已就緒，才能使用此選項。

  AMS 會提供其他備註和指示。

使用 PuTTy 的 SSH 通道步驟：

在 PuTTY 中，您會使用堡壘主機的公有 IP 建立 SSH 工作階段，在 AUTH 區段中提供 PEM 金鑰，然後建立通道。通道的來源連接埠應該是未使用的本機連接埠（例如 5000)，而 IP 是附加 RDP 連接埠的目的地主機（您嘗試到達的 Windows 方塊）的 IP (3389)。請務必儲存您的組態，因為您不想在每次登入方塊時都這麼做。連線至堡壘主機，然後登入。然後，啟動 localhost：5000（或您選擇的任何連接埠）的 RDP 工作階段。

1. 設定堡壘主機的主機名稱或公有 IP

2. 在 SSH ->Auth 中，以 .ppk 格式設定私有金鑰檔案

3. 在 SSH ->Tunnels 中，新增新的轉送連接埠。來源連接埠應該是任意未使用的連接埠，而目的地應該是堡壘主機後方目的地伺服器的 IP，並附加 RDP 連接埠。

4. 透過 PuTTY 連線到堡壘主機並登入。

5. 啟動至 localhost：5000 的 RDP 工作階段，以到達目的地伺服器。

SALZ：設定存取管理

使用由 AWS Managed Services (AMS) 管理的網路表示授予 AMS 管理雲端基礎設施的存取權。您需要設定在私有網路和 AMS 之間安全連線的方法。這從有關您要提供的存取類型的一些決策開始：

- 對於 AMS API/CLI 和主控台存取：您會想要安裝 AMS CLI (本文件提供說明）。您可以使用 AMS 變更管理 API 向 AMS 和 AMS SKMS API 提出變更請求，以了解您的 AMS 受管資源。使用 Active Directory Federation Services (AD FS)，您可以存取 AMS 主控台。

  > **Note**
  >
  > 如果您要設定自己的 ITSM，則需要將 AWS Support API (SAPI) 用於服務請求和事件報告。SAPI 記錄在AWS 支援 API 參考中。

- 對於使用者存取：無論您使用 Windows Active Directory (AD) 或 Linux/LDAP 解決方案管理使用者，都必須在 AMS 端的 AD （透過 Directory Services) 和您的目錄之間建立連線。
- 執行個體存取：透過單向樹系信任組態完成執行個體層級存取。Directory Services 信任其 CORP AD 中的登入資料，允許 AMS 端內的堆疊允許使用 CORP 登入資料進行登入。

  請注意，AMS 設定信任的 Active Directory (AD) 必須是擁有您授權存取 AWS 資源之使用者帳戶的目錄。

> **Important**
>
> 若要設定樹系信任，AMS 需要網域控制站本機政策 -> 安全選項 -> 網路存取：可匿名存取的具名管道，請列出 Netlogon 和 lsarpc 管道。這些管道預設會列出，但有時會因安全性考量而移除。建立信任之後，即可再次從清單中移除信任。

建立 Active Directory (AD) 信任

開始為 AWS Managed Services (AMS) 帳戶建立 Active Directory (AD) 信任之前，請確定已開啟適當的防火牆連接埠。

來自 AMS 受管 Active Directory 和您公司目錄服務的信任可讓您使用公司受管憑證來存取 AMS 受管執行個體，以執行開發、測試或管理功能。

建立信任連線是兩部分練習：

首先，設定條件式轉送、DNS 組態，讓 DNS 查詢知道要前往哪個 DNS 伺服器。

其次，設定信任、Active Directory (AD) 建構，以允許某個網域中的使用者存取，以使用另一個網域中的資源。

設定條件式轉送器

遵循此 Microsoft AD 文章為網域名稱指派條件式轉寄站，並使用下列設定和選項：

1. 在 AD DNS Manager -> 建立新的條件式轉寄站中，DNS 網域下：使用提供給您的網域名稱 AMS，例如 *A523434123.amazonaws.com*。
2. 在主伺服器的 IP 地址下：新增 AMS 提供的 IP 地址。驗證這兩個地址，確認沒有連線問題。
3. 選取將此條件式轉送器儲存在 Active Directory 中，並如下複寫：此網域中的所有 DNS 伺服器，然後按確定。

設定信任

若要設定 AWS Managed Services (AMS) 帳戶的信任，請遵循此 MicroSoft AD 文章使用本節所述的設定和選項，為信任的一側建立單向、傳入、樹系信任。

1. 開啟開始 -> 管理工具 -> Active Directory 網域和信任對話方塊。在您要建立信任之網域的網域節點上按一下滑鼠右鍵，然後按一下屬性 -> 信任 -> 新信任以開啟新信任精靈。輸入 AMS 針對信任名稱提供給您的網域名稱，然後按下一步。
2. 在信任類型下，選取樹系信任。按下 Next (下一步)。
3. 在信任方向下，選取單向：傳入。按下 Next (下一步)。
4. 在信任方下，僅選取此網域。按下 Next (下一步)。
5. 在信任密碼下，輸入您選擇的密碼。按下 Next (下一步)。

6. 對於信任選擇已完成和信任建立完成，只需按下一步。
7. 在確認傳入信任下，選取否，不要確認傳入信任。按下 Next (下一步)。
8. 在完成新的信任精靈下，選取完成，然後確定關閉。
9. 提供信任密碼（基於安全理由，請透過 CSDM 的電話號碼聯絡我們）。AMS 將完成信任組態。

Active Directory 網站和服務

若要降低登入延遲，請將 VPC CIDR 範圍新增至您的 Active Directory 網站和服務 (Start -> 管理工具 -> Active Directory 網站和服務)。將 VPC CIDR 範圍新增至 Active Directory 網站，其中包含最接近 AWS 的網域控制站。

Active Directory 名稱尾碼路由

建立單向樹系信任之後，請完成其他步驟。

1. 在開始 > 所有程式 > 管理工具下，按一下 Active Directory 網域和信任。

   Active Directory 網域和信任主控台隨即開啟。
2. 在公司網域上按一下滑鼠右鍵，然後按一下屬性

   該網域的屬性對話方塊隨即開啟。
3. 按一下信任索引標籤。

   信任頁面隨即開啟。
4. 按一下 Amazon 網域名稱，然後按一下屬性。

   Amazon 網域信任的屬性頁面隨即開啟。
5. 按一下名稱尾碼路由，然後按一下重新整理。

   這些步驟可確保服務委託人名稱 (SPNs) 可透過信任解析。

故障診斷

如果您遇到問題，可以嘗試一些方法：

- AMS 受管 Active Directory 傳出安全群組需要允許透過 CIDR 區塊（例如 10.27.0.0/16) 連線到您的網域控制器。

- 在 AWS 主控台中追蹤從網域控制站到網域控制站的路由，一路檢查所有安全群組。
- 如果允許網際網路控制訊息通訊協定 (ICMP)，請確定您可以 ping AMS 受管 Active Directory 網域控制器。
- 請確定您的網域控制站可以與 AWS Directory Services 通訊。
- 確定條件式轉送器解析並經過驗證。
- 如果您在新信任精靈中沒有看到樹系信任，則您的條件式轉送器可能無法正常運作：
  - 使用 nslookup 測試解析度
  - 嘗試重新啟動網域控制器

AMS 受管 Active Directory

AMS 現在提供稱為 Managed Active Directory （又稱為 Managed AD) 的新服務，可讓 AMS 處理 Active Directory (AD) 基礎設施操作，同時讓您控制 Active Directory 管理。

Managed AD 的 AMS 支援類似於 Amazon Relational Database Service (Amazon RDS) 的 AMS 支援。在這兩種情況下， AWS （包括 AMS) 都支援建立和管理執行服務的基礎設施，同時執行存取控制和所有管理功能。此模型具有下列優點：

- 限制安全風險： AWS 且 AMS 不需要網域的管理權限。
- 直接整合：您可以使用目前的授權模型並與 AD 整合，而不需要與 AMS 連接。

備註：

- AMS 和您都無法存取 Managed AD 網域控制站，因此網域控制站上無法安裝任何軟體。這很重要，因為不允許在網域控制站上安裝軟體的第三方解決方案。

  存取的運作方式如下：
  - AWS Directory Service 團隊：可存取網域控制站。
  - AMS：可存取 Directory Service APIs以在網域上執行特定動作。這些動作包括拍攝 AD 快照、變更 AD 結構描述和其他動作。
  - 您：可存取網域 (AD) 以建立使用者、群組等。
- 我們建議您在遷移公司 AD 之前先在 Managed AD 上執行概念驗證，因為並非所有來自傳統 AD 環境的功能都可在 Managed AD 環境中使用。
- AMS 不會管理 AD 管理或提供有關 AD 管理的指導。例如，AMS 不會提供有關組織單位結構、群組政策結構、AD 使用者命名慣例等的指導。

它的運作方式如下：

1. 除了您的 AMS 帳戶之外，AMS 還會 AWS 帳戶 為您加入新的 ，並透過 AWS Directory Service 佈建 Active Directory (AD) 環境 （ 另請參閱什麼是 AWS Directory Service？)。

   以下是系統整合商需要從您收集的資訊，以便 AMS 加入 Managed AD：

   - 帳戶資訊
     - 為 AMS 受管 AD： AWS 帳戶 number AWS 帳戶 建立之 的帳戶 ID
     - 要加入 Managed AD 的區域： AWS 區域
   - 受管 Active Directory 資訊：
     - Microsoft AD Edition：Standard/Enterprise。AWS Microsoft AD (Standard Edition) 包含 1 GB 的目錄物件儲存。此容量最多可支援 5，000 個使用者或 30，000 個目錄物件，包括使用者、群組和電腦。AWS Microsoft AD (Enterprise Edition) 包含 17 GB 的目錄物件儲存體，最多可支援 100，000 個使用者或 500，000 個物件。

       如需詳細資訊，請參閱 AWS Directory Service FAQs。
     - 網域 FQDN：AMS Managed AD 網域的 FQDN。
     - 網域 NetBIOS 名稱：AMS Managed AD 網域的 NetBIOS 名稱。
     - 您想要 Managed AD 整合的 AMS 標準帳戶帳號 (AMS 會設定從 AMS 標準帳戶的 AD 到 Managed AD 的單向信任)
     - 是否需要修改 Active Directory 結構描述，如果需要，要修改什麼？
     - 根據預設，會佈建兩個網域控制站。您需要更多嗎？ 如果是這樣，您需要多少？原因是什麼？
   - 受管 Active Directory 資訊的聯網：
     - 網域控制站的 Managed AD VPC CIDR (Managed AD 網域控制站私有子網路範圍內的 CIDR)：
       - 網域控制站的子網路 CIDR 1：【您的 CIDR 需要屬於 AMS Managed AD VPC CIDR】
       - 網域控制站的子網路 CIDR 2：【您的 CIDR 需要屬於 AMS Managed AD VPC CIDR】

       例如：

       - Managed AD VPC CIDR：192.168.0.0/16
       - 網域控制器的 CIDR 1：192.168.1.0/24
       - 網域控制器的 CIDR 2：192.168.2.0/24

       為了避免 IP 地址衝突，請確定您指定的 Managed AD VPC CIDR 不會與您公司網路中使用的任何其他私有子網路 CIDR 衝突。

- VPN 技術 （選用）：【Direct Connect/Direct Connect 和 VPN】
  - 閘道的 BGP 自治系統編號 (ASN)：【客戶提供的 ASN】
  - 閘道外部界面的網際網路可路由 IP 地址，地址必須為靜態：【客戶提供的 IP 地址】
  - 您的 VPN 連接是否需要靜態路由：【是/否】

2. AMS 為您提供 AD 環境的管理員帳戶密碼，並要求您重設密碼，以便 AMS 工程師無法再存取您的 AD 環境。
3. 若要重設管理員帳戶密碼，請使用 Active Directory 使用者和電腦 (ADUC) 連線至您的 Active Directory 環境。ADUC 和其他遠端伺服器管理工具 (RSAT) 應該安裝在您在非 AMS 基礎設施上佈建的管理主機上並執行。Microsoft 有保護此類管理主機的最佳實務。如需詳細資訊，請參閱實作安全管理主機。您可以使用這些管理主機來管理 Active Directory 環境。
4. 在日常操作中，AMS 最多會管理物件的 AWS 帳戶 AWS Directory Service 端；例如，VPC 組態、AD 備份、AD 信任建立和刪除等。您可以使用並管理您的 AD 環境；例如，使用者建立、群組建立、群組政策建立等。

如需最新的 RACI 資料表，請參閱《請參閱服務描述》中的「角色與責任」一節。

將 Active Directory 與 AMS AWS Identity and Access Management 角色聯合

將目錄與 AMS IAM 角色聯合的目的是讓企業使用者使用其企業登入資料與 AWS 管理主控台 和 AWS APIs，進而與 AMS 主控台和 APIs互動。

聯合程序範例

此範例使用 Active Directory Federation Services (AD FS)；不過，支援 AWS Identity and Access Management 聯合的任何技術都受到支援。如需 AWS 支援的 IAM 聯合的詳細資訊，請參閱 IAM 合作夥伴和身分提供者和聯合。您的 CSDM 將協助您完成此程序，這涉及與 AD 團隊和 AMS 的共同工作。

如需整合 SAML for API 存取的詳細資訊，請參閱此 AWS 部落格：如何使用 SAML 2.0 和 AD FS 實作聯合 API 和 CLI 存取。

> **Note**
>
> 如需安裝 AMS CLI 和 SAML 的範例，請參閱 附錄：ActiveDirectory 聯合服務 (ADFS) 宣告規則和 SAML 設定。

設定 AMS 主控台的聯合 (SALZ)

下表中詳述的 IAM 角色和 SAML 身分提供者（受信任實體）已佈建為帳戶加入的一部分。這些角色可讓您提交和監控 RFCs、服務請求和事件報告，以及取得 VPCs和堆疊的相關資訊。

角色	身分提供者	權限
Customer_ReadOnly_Role	SAML	對於標準 AMS 帳戶。可讓您提交 RFCs 以變更 AMS 受管基礎設施，以及建立服務請求和事件。
customer_managed_ad_user_role	SAML	對於 AMS Managed Active Directory 帳戶。可讓您登入 AMS 主控台以建立服務請求和事件（無 RFCs)。

如需不同帳戶下可用角色的完整清單，請參閱 AMS 中的 IAM 使用者角色。

加入團隊的成員將中繼資料檔案從您的聯合解決方案上傳至預先設定的身分提供者。當您想要在 Shibboleth 或 Active Directory Federation Services 等 SAML 相容 IdP（身分提供者）之間建立信任時，您可以使用 SAML 身分提供者，以便組織中的使用者可以存取 AWS 資源。IAM 中的 SAML 身分提供者在具有上述角色的 IAM 信任政策中用作主體。

雖然其他聯合解決方案為 AWS 提供整合指示，但 AMS 有單獨的指示。使用下列部落格文章，使用 Windows Active Directory、AD FS 和 SAML 2.0 啟用 AWS 聯合，以及以下提供的修訂，可讓您的公司使用者從單一瀏覽器存取多個 AWS 帳戶。

根據部落格文章建立依賴方信任之後，請以下列方式設定宣告規則：

- NameId：遵循部落格文章。
- RoleSessionName：使用下列值：
  - 宣告規則名稱：RoleSessionName
  - 屬性存放區：Active Directory

  - LDAP 屬性：SAM-Account-Name
  - 傳出宣告類型：https：//https://aws.amazon.com/SAML/Attributes/RoleSessionName
- 取得 AD 群組：遵循部落格文章。
- 角色宣告：遵循部落格文章，但對於自訂規則，請使用以下內容：

```
c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-([^d]{12})-"]
 => issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value =
 RegExReplace(c.Value, "AWS-([^d]{12})-",
 "arn:aws:iam::$1:saml-provider/customer-readonly-saml,arn:aws:iam::$1:role/"));
```

使用 AD FS 時，您必須以下表所示的格式為每個角色建立 Active Directory 安全群組 (customer_managed_ad_user_role 僅適用於 AMS Managed AD 帳戶）：

群組	角色
AWS-【AccountNo】-Customer_ReadOnly_Role	Customer_ReadOnly_Role
AWS-【AccountNo】-customer_managed_ad_user_role	customer_managed_ad_user_role

如需詳細資訊，請參閱設定身分驗證回應的 SAML 聲明。

> **Tip**
>
> 若要協助疑難排解，請下載瀏覽器的 SAML 追蹤器外掛程式。

將聯合請求提交至 AMS

如果這是您的第一個帳戶，請使用您的 CSDM 和/或 Cloud Architect(s)，為您的身分提供者提供中繼資料 XML 檔案。

如果您要加入其他帳戶或身分提供者，並有權存取管理帳戶或所需的應用程式帳戶，請遵循下列步驟。

1. 從 AMS 主控台建立服務請求，提供新增身分提供者所需的詳細資訊：
   - 將建立新身分提供者的帳戶的 AccountId。

- 所需的身分提供者名稱，若未提供，預設值將為 customer-saml；通常，這必須符合聯合提供者中設定的設定。
- 對於現有帳戶，包括是否應將新的身分提供者傳播至所有現有的主控台角色，或提供應信任新身分提供者的角色清單。
- 將從您的聯合代理程式匯出的中繼資料 XML 檔案做為檔案附件連接到服務請求。

2. 從您建立服務請求的相同帳戶中，使用 CT-ID ct-1e1xtak34nx76（管理 | 其他 | 其他 | 建立）建立新的 RFC，並包含下列資訊。

   - 標題：「帳戶 <AccountId> 的內建 SAML IDP <Name>」。
   - 要建立身分提供者之帳戶的 AccountId。
   - 身分提供者名稱。
   - 對於現有帳戶：身分提供者是否應傳播至所有現有的主控台角色，或應信任新身分提供者的角色清單。
   - 在步驟 1 中建立的服務請求的案例 ID，其中連接中繼資料 XML 檔案。

驗證主控台存取

使用 ADFS 設定好並具有要用於身分驗證的 AMS URL 後，請依照下列步驟進行。

使用 Active Directory 聯合服務 (ADFS) 組態，您可以遵循下列步驟：

1. 開啟瀏覽器視窗，並前往為您的帳戶提供給您的登入頁面。您帳戶的 ADFS IdpInitiatedSignOn 頁面隨即開啟。
2. 選取登入下列其中一個網站旁的選項按鈕。登入網站挑選清單會變成作用中。
3. 選擇 signin.aws.amazon.com 網站，然後按一下登入。用於輸入登入資料的選項會開啟。
4. 輸入您的 CORP 登入資料，然後按一下登入。隨即 AWS 管理主控台 開啟。
5. 將 AMS 主控台 URL 貼到位置列，然後按 Enter 鍵。AMS 主控台隨即開啟。

驗證 API 存取

AMS 使用 AWS API，搭配一些您可以在 AMS API 參考中閱讀的 AMS 特定操作。

AWS 提供數個 SDK，您可以在 Tools for Amazon Web Services 中存取這些SDKs。如果您不想使用 SDK，您可以直接進行 API 呼叫。如需身分驗證的資訊，請參閱簽署 AWS API 請求。如果您不是使用 SDK，或直接提出 HTTP API 請求，則可以使用適用於變更管理 (CM) 和 SKMS 的 AMS CLIs。

安裝 AMS CLIs

如需安裝 AWS Managed Services (AMS) CLI 以搭配 SAML 使用的範例，請參閱 附錄：ActiveDirectory 聯合服務 (ADFS) 宣告規則和 SAML 設定。

如果您需要暫時存取，若要取得和安裝 AWS Managed Services (AMS) SDKs，請參閱暫時 AMS 主控台存取。

> **Note**
>
> 您必須擁有此程序的管理員登入資料。

AWS CLI 是使用 AWS Managed Services (AMS) CLIs（變更管理和 SKMS) 的先決條件。

1. 若要安裝 AWS CLI，請參閱安裝 AWS 命令列界面，並遵循適當的指示。請注意，在該頁面底部有使用不同安裝程式、Linux、MS Windows、macOS、虛擬環境、 Bundled Installer (Linux、macOS 或 Unix) 的說明。

   安裝之後，請執行 `aws help`來驗證安裝。
2. 安裝 AWS CLI 後，若要安裝或升級 AMS CLI，請下載 AMS AMS CLI 或 AMS SDK 可分發 zip 檔案並解壓縮。您可以透過 AMS 主控台左側導覽中的開發人員資源連結來存取 AMS CLI 可分發項目。
3. README 檔案提供任何安裝的指示。

   開啟：

   - CLI zip：僅提供 AMS CLI。
   - SDK zip：提供所有 AMS APIs和 AMS CLI。

   對於 Windows，請執行適當的安裝程式（僅限 32 或 64 位元系統）：

   - 32 位元：ManagedCloudAPI_x86.msi
   - 64 位元：ManagedCloudAPI_x64.msi

   對於 Mac/Linux，執行此命令以執行名為 AWSManagedServices_InstallCLI.sh 的檔案：`sh AWSManagedServices_InstallCLI.sh`。請注意，amscm 和 amsskms 目錄及其內容必須與 AWSManagedServices_InstallCLI.sh 檔案位於相同的目錄中。

4. 如果您的公司登入資料是透過 AWS (AMS 預設組態） 聯合使用，您必須安裝登入資料管理工具，以存取您的聯合服務。例如，您可以使用此 AWS 安全部落格 如何使用 SAML 2.0 和 AD FS 實作聯合 API 和 CLI 存取，以協助設定您的憑證管理工具。
5. 安裝之後，請執行 `aws amscm help`和 `aws amsskms help` 以查看命令和選項。

> **Note**
>
> 必須安裝 AMS CLI，這些命令才能運作。若要安裝 AMS API 或 CLI，請前往 AMS 主控台開發人員資源頁面。如需 AMS CM API 或 AMS SKMS API 的參考資料，請參閱《 使用者指南》中的 AMS 資訊資源一節。您可能需要新增身分驗證`--profile`選項，例如 `aws amsskms ams-cli-command --profile SAML`。您可能還需要新增 `--region`選項，因為所有 AMS 命令都用盡 us-east-1；例如 `aws amscm ams-cli-command --region=us-east-1`。

在 VPC 層級排程 AMS 備份

在已配置目標執行個體的 VPC 中，AWS Managed Services (AMS) 備份排程會在帳戶加入期間建立，並在 VPC 建立結構描述中使用預設標籤。備份系統會根據該 VPC 標籤排程快照的執行。您可以透過建立服務請求來修改排程。如需詳細資訊，請參閱 VPC 標籤和預設值。

如需備份預設值，請參閱了解 AMS 預設值

SALZ：預設設定

您的 AWS Managed Services (AMS) 網路是以標準化方式設定，且大部分服務都有預設值。

本節說明 AMS 用於安全性、存取、監控、記錄、持續性和修補、管理的預設設定。

如需基礎設施成本的範例，請參閱基本元件。

防火牆規則提供於 設定您的防火牆

端點安全 (EPS)

您在 AMS Advanced 環境中佈建的資源會自動包含端點安全 (EPS) 監控用戶端的安裝。此程序可確保 24 小時全年無休監控和支援 AMS 進階受管資源。此外，AMS Advanced 會監控所有代理程式活動，並在偵測到任何安全事件時建立事件。

> **Note**
>
> 安全事件會視為事件處理；如需詳細資訊，請參閱事件回應。

端點安全提供反惡意軟體保護，特別是支援下列動作：

- EC2 執行個體向 EPS 註冊
- EC2 執行個體從 EPS 取消註冊
- EC2 執行個體即時反惡意軟體保護
- EPS 代理程式起始的心跳
- EPS 還原隔離的檔案
- EPS 事件通知
- EPS 報告

AMS Advanced 使用 Trend Micro 進行端點安全 (EPS)。這些是預設的 EPS 設定。若要進一步了解 Trend Micro，請參閱 Trend Micro Deep Security Help Center；請注意，非 Amazon 連結可能會變更，恕不另行通知。

AMS 進階多帳戶登陸區域 (MALZ) 預設設定如下列各節所述；對於非預設 AMS 多帳戶登陸區域 EPS 設定，請參閱 AMS 進階多帳戶登陸區域 EPS 非預設設定。

> **Note**
>
> 您可以自備 EPS，請參閱 AMS 自備 EPS。

一般 EPS 設定

端點安全一般網路設定。

EPS 預設值

設定	預設
防火牆連接埠 （執行個體的安全群組）	EPS Deep Security Manager 代理程式 (DSMs) 必須針對 Agent/Relay to Manager 通訊開啟連接埠 4120，以及針對 Manager Console 開啟連

設定	預設
	接埠 4119。EPS 轉送必須開啟連接埠 4122，管理員/客服人員才能轉送通訊。客戶執行個體傳入通訊不應開啟任何特定連接埠，因為客服人員會啟動所有請求。
通訊方向	代理程式/應用程式啟動
活動訊號間隔	十分鐘
警示之前的遺失活動訊號數目	Two
伺服器時間之間允許的偏離上限（差異）	無限制
為非作用中（已註冊但未上線）虛擬機器引發離線錯誤	否
預設政策	基本政策（接下來說明）
啟用具有相同主機名稱的多部電腦	允許
已提出待定更新的提醒	七天後
更新排程	AMS 以 Trend Micro Deep Security Manager (DSM) / Deep Security Agent (DSA) 軟體更新的每月發行週期為目標。不過，AMS 不會維護更新用的 SLA。AMS 開發人員團隊會在部署期間在整個機群中執行更新。 DSA/DSA 更新會記錄在 Trend Micro DSM 系統事件中，AMS 預設會在本機保留 13 週。如需廠商文件，請參閱 Trend Micro Deep Security Help Center 中的系統事件。日誌也會匯出至 Amazon CloudWatch 中的日誌群組 /aws/ams/eps/var/log/DSM.log。
更新來源	Trend Micro Update Server (https://ipv6-iaus.trendmicro.com/iau_server.dll/：//)

設定	預設
事件或日誌資料刪除	事件和日誌會在七天後從 DSM 資料庫刪除。
保留代理程式軟體版本	最多五個
保留最新的規則更新	最多十個
日誌儲存	根據預設，日誌檔案會安全地存放在 Amazon S3 中，但您也可以將其封存至 Amazon Glacier，以協助滿足稽核和合規要求。

基本政策

端點安全基礎政策預設設定。

EPS 基本政策

設定	預設
已啟用的模組	反惡意軟體
已停用的模組	Web 評價
	防火牆
	入侵保護
	完整性監控
	日誌檢查
	應用程式控制

反惡意軟體

端點安全反惡意軟體設定。

EPS 反惡意軟體預設值

設定	預設	備註
即時掃描	掃描所有項目 每天/全天 (24 小時)	隔離所有可疑病毒。啟用 IntelliTrap 和間諜軟體/灰色軟體保護。 間諜軟體和灰色軟體會觸發反惡意軟體，並導致項目隔離。
手動掃描	掃描所有項目	必須請求，然後遵循預設的即時掃描組態。
排程掃描	掃描所有項目	為每月最後一個星期日上午 6 點進行設定。
智慧保護	已停用	N/A
隔離的檔案	Trend Micro Deep Security Manager (DSM)	大約保留 1GB 的磁碟進行隔離。
掃描限制	Trend Micro DSM	掃描所有大小的檔案。
允許的間諜軟體或灰色軟體	無	N/A
本機事件通知	是	N/A

安全群組

在 AWS VPCs 中，AWS 安全群組充當虛擬防火牆，控制一或多個堆疊 （執行個體或一組執行個體） 的流量。啟動堆疊時，它會與一或多個安全群組相關聯，以決定允許哪些流量到達該群組：

- 對於公有子網路中的堆疊，預設安全群組接受來自所有位置（網際網路）的 HTTP (80) 和 HTTPS (443) 流量。堆疊也接受來自您公司網路和 AWS 堡壘的內部 SSH 和 RDP 流量。然後，這些堆疊可以透過任何連接埠輸出到網際網路。它們也可以輸出到您的私有子網路和公有子網路中的其他堆疊。
- 私有子網路中的堆疊可以輸出到私有子網路中的任何其他堆疊，而堆疊中的執行個體可以完全透過任何通訊協定互相通訊。

> **Important**
>
> 私有子網路上堆疊的預設安全群組允許私有子網路中的所有堆疊與該私有子網路中的其他堆疊通訊。如果您想要限制私有子網路中堆疊之間的通訊，您必須建立新的安全群組來描述限制。例如，如果您想要限制與資料庫伺服器的通訊，以便該私有子網路中的堆疊只能透過特定連接埠從特定應用程式伺服器通訊，請請求特殊安全群組。本節將說明如何執行此操作。

預設安全群組

MALZ

下表說明堆疊的預設傳入安全群組 (SG) 設定。SG 名為 "SentinelDefaultSecurityGroupPrivateOnly-vpc-ID"，其中 *ID* 是 AMS 多帳戶登陸區域帳戶中的 VPC ID。允許所有流量透過此安全群組傳出至 "mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnly"（允許堆疊子網路中的所有本機流量）。

第二個安全群組 "SentinelDefaultSecurityGroupPrivateOnly" 允許所有流量傳出至 0.0.0.0/0。

> **Tip**
>
> 如果您要為 AMS 變更類型選擇安全群組，例如 EC2 建立或 OpenSearch 建立網域，您可以使用此處所述的其中一個預設安全群組，或您建立的安全群組。您可以在 AWS EC2 主控台或 VPC 主控台中找到每個 VPC 的安全群組清單。

還有其他預設安全群組用於內部 AMS 用途。

AMS 預設安全群組（傳入流量）

類型	通訊協定	連接埠範圍	來源
所有流量	全部	全部	SentinelDefaultSecurityGroupPrivateOnly（限制相同安全群組成員的傳出流量）
所有流量	全部	全部	SentinelDefaultSecurityGroupPrivateOnlyEgressAll（不限制傳出流量）
HTTP、HS、SSH、	TCP	80 / 443（來源 0.0.0.0/0） 允許從堡壘存取 SSH 和 RDP	SentinelDefaultSecurityGroupPublic（不限制傳出流量）
MALZ 堡壘：			
SSH	TCP	22	SharedServices VPC CIDR 和 DMZ VPC CIDR，以及客戶提供的內部部署 CIDRs
SSH	TCP	22	
RDP	TCP	3389	
RDP	TCP	3389	
SALZ 堡壘：			
SSH	TCP	22	mc-initial-garden-LinuxBastionSG
SSH	TCP	22	mc-initial-garden-LinuxBastionDMZSG
RDP	TCP	3389	mc-initial-garden-WindowsBastionSG
RDP	TCP	3389	mc-initial-garden-WindowsBastionDMZSG

SALZ

下表說明堆疊的預設傳入安全群組 (SG) 設定。SG 名為 "mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnly-*ID*"，其中 *ID* 是唯一的識別符。允許所有流量透過此安

全群組傳出至 "mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnly"（允許堆疊子網路中的所有本機流量）。

第二個安全群組 "mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnlyEgressAll-ID" 允許所有流量傳出至 0.0.0.0/0。

> **Tip**
>
> 如果您要為 AMS 變更類型選擇安全群組，例如 EC2 建立或 OpenSearch 建立網域，您可以使用此處所述的其中一個預設安全群組，或您建立的安全群組。您可以在 AWS EC2 主控台或 VPC 主控台中找到每個 VPC 的安全群組清單。

還有其他預設安全群組用於內部 AMS 用途。

AMS 預設安全群組（傳入流量）

類型	通訊協定	連接埠範圍	來源
所有流量	全部	全部	SentinelDefaultSecurityGroupPrivateOnly（限制相同安全群組成員的傳出流量）
所有流量	全部	全部	SentinelDefaultSecurityGroupPrivateOnlyEgressAll（不限制傳出流量）
HTTP、HS、SSH、	TCP	80 / 443（來源 0.0.0.0/0) 允許從堡壘存取 SSH 和 RDP	SentinelDefaultSecurityGroupPublic（不限制傳出流量）
MALZ 堡壘：			
SSH	TCP	22	SharedServices VPC CIDR 和 DMZ VPC CIDR，以及客戶提供的內部部署 CIDRs
SSH	TCP	22	
RDP	TCP	3389	
RDP	TCP	3389	

類型	通訊協定	連接埠範圍	來源
SALZ 堡壘：			
SSH	TCP	22	mc-initial-garden-LinuxBastionSG
SSH	TCP	22	mc-initial-garden-LinuxBastionDMZSG
RDP	TCP	3389	mc-initial-garden-WindowsBastionSG
RDP	TCP	3389	mc-initial-garden-WindowsBastionDMZSG

建立、變更或刪除安全群組

您可以請求自訂安全群組。如果預設安全群組不符合應用程式或組織的需求，您可以修改或建立新的安全群組。這類請求會被視為需要核准，並由 AMS 操作團隊審核。

若要在堆疊和 VPCs 外部建立安全群組，請使用`Deployment | Advanced stack components | Security group | Create (review required)`變更類型 (ct-1oxx2g2d7hc90) 提交 RFC。

針對 Active Directory (AD) 安全群組修改，請使用下列變更類型：

- 若要新增使用者：使用管理 | Directory Service | 使用者和群組 | 新增使用者至群組 【ct-24pi85mjtza8k】 提交 RFC
- 若要移除使用者：使用 Management | Directory Service | User and group | Remove user from group 【ct-2019s9y3nfml4】 提交 RFC

> **Note**
>
> 使用「需要檢閱」CTs時，AMS 建議您使用 ASAP 排程選項（在主控台中選擇 ASAP，在 API/CLI 中保留開始和結束時間空白），因為這些 CTs 需要 AMS 運算子來檢查 RFC，並在核准和執行之前與您通訊。如果您排程這些 RFCs，請務必至少允許 24 小時。如果未在排定的開始時間之前進行核准，則會自動拒絕 RFC。

尋找安全群組

若要尋找連接到堆疊或執行個體的安全群組，請使用 EC2 主控台。找到堆疊或執行個體後，您可以看到連接到該堆疊或執行個體的所有安全群組。

如需在命令列尋找安全群組並篩選輸出的方法，請參閱 describe-security-groups。

EC2 IAM 執行個體描述檔

執行個體描述檔是適用於 IAM 角色的容器，可讓您在執行個體啟動時將角色資訊傳遞至 EC2 執行個體。

MALZ

有兩個 AMS 預設執行個體描述檔 `customer-mc-ec2-instance-profile`和 `customer-mc-ec2-instance-profile-s3`。這些執行個體描述檔提供下表所述的許可。

政策描述

設定檔	Policies
`customer-mc-ec2-instance-profile`	`AmazonSSMManagedInstanceCore` ：允許 Ec2 執行個體使用 SSM 代理程式。
	`AMSInstanceProfileLoggingPolicy` ：允許 Ec2 執行個體將日誌推送至 S3 和 CloudWatch。
	`AMSInstanceProfileManagementPolicy` ：允許 Ec2 執行個體執行開機動作，例如加入 Active Directory。
	`AMSInstanceProfileMonitoringPolicy` ：允許 Ec2 執行個體向 AMS 監控服務報告問題清單。
	`AMSInstanceProfilePatchPolicy` ：允許 Ec2 執行個體接收修補程式。
`customer-mc-ec2-instance-profile-s3`	`AMSInstanceProfileBYOEPSPolicy` ：允許 Ec2 執行個體使用 AMS 帶來您自己的 EPS。
	`AMSInstanceProfileLoggingPolicy` ：允許 Ec2 執行個體將日誌推送至 S3 和 CloudWatch。

設定檔	Policies
	AMSInstanceProfileManagementPolicy ：允許 Ec2 執行個體執行開機動作，例如加入 Active Directory。
	AMSInstanceProfileMonitoringPolicy ：允許 Ec2 執行個體向 AMS 監控服務報告問題清單。
	AMSInstanceProfilePatchPolicy ：允許 Ec2 執行個體接收修補程式。
	AMSInstanceProfileS3WritePolicy ：允許 Ec2 執行個體讀取/寫入客戶 S3 儲存貯體。

SALZ

有一個 AMS 預設執行個體描述檔 customer-mc-ec2-instance-profile，授予 IAM 執行個體政策 的許可customer_ec2_instance_profile_policy。此執行個體描述檔提供下表所述的許可。設定檔會將許可授予執行個體上執行的應用程式，而非登入執行個體的使用者。

政策通常包含多個陳述式，其中每個陳述式會將許可授予一組不同的資源，或在特定條件下授予許可。

CW = CloudWatch。ARN = Amazon Resource Name。* = 萬用字元 （任何）。

EC2 預設 IAM 執行個體描述檔許可

CW = CloudWatch。ARN = Amazon Resource Name。* = 萬用字元 （任何）。			
政策聲明	Effect	動作	描述和資源 (ARN)
Amazon Elastic Compute Cloud (Amazon EC2)			
EC2 訊息動作	允許	AcknowledgeMessage、 DeleteMessage、 FailMessage、 GetEndpoint、	允許帳戶中的 EC2 Systems Manager 訊息動作。

CW = CloudWatch。ARN = Amazon Resource Name。* = 萬用字元（任何）。			
政策聲明	Effect	動作	描述和資源 (ARN)
		GetMessages、 SendReply	
Ec2 描述	允許	*（全部）	允許主控台顯示您帳戶中 EC2 的組態詳細資訊。
Iam 取得角色 ID	允許	GetRole	允許 EC2 從 `aws:iam::*:role/customer-*` 和 取得您的 IAM ID`aws:iam::*:role/customer_*` 。
上傳日誌事件的執行個體	允許	建立日誌群組	允許在以下位置建立日誌：`aws:logs:*:*:log-group:i-*`
		建立日誌串流	允許將日誌串流至： `aws:logs:*:*:log-group:i-*`
MMS 的 CW	允許	DescribeAlarms、 PutMetricAlarm、 PutMetricData	允許 CloudWatch 擷取您帳戶中的警示。 允許 CW 建立或更新警示，並將其與指定的指標建立關聯。 允許 CW 將指標資料點發佈至您的帳戶。
Ec2 標籤	允許	CreateTags、 DescribeTags、	允許在您帳戶中的指定執行個體上新增、覆寫和描述標籤。
明確拒絕 CW 日誌	拒絕	DescribeLogStreams、 FilterLogEvents、 GetLogEvents	不允許列出、篩選或取得日誌串流： `aws:logs:*:*:log-group:/mc/*`

CW = CloudWatch。ARN = Amazon Resource Name。* = 萬用字元（任何）。			
政策聲明	Effect	動作	描述和資源 (ARN)
Amazon EC2 Simple Systems Manager (SSM)			
SSM 動作	允許	DescribeAssociation、 GetDocument、 ListAssociations、 UpdateAssociationStatus、 UpdateInstanceInformation	允許帳戶中的各種 SSM 函數。
S3 中的 SSM 存取	允許	GetObject、 PutObject、 AbortMultipartUpload、 ListMultipartUploadPorts、 ListBucketMultipartUploads	允許 EC2 上的 SSM 在 中取得和更新物件，並中止分段物件上傳，以及列出 中可用於分段上傳的連接埠和儲存貯體`aws:s3:::mc-*-internal-*/aws/ssm*` 。
Amazon EC2 Simple Storage Service (S3)			
在 S3 中取得物件	允許	取得 清單	允許 EC2 應用程式擷取和列出您帳戶中 S3 儲存貯體中的物件。
客戶加密日誌 S3 存取	允許	PutObject	允許 EC2 應用程式更新 中的物件 `aws:s3:::mc-*-logs-*/encrypted/app/*`

CW = CloudWatch。ARN = Amazon Resource Name。* = 萬用字元（任何）。

政策聲明	Effect	動作	描述和資源 (ARN)
修補程式資料放置物件 S3	允許	PutObject	允許 EC2 應用程式將修補資料上傳至 S3 儲存貯體 `aws:s3:::awsms-a*-patch-data-*`
將自有日誌上傳至 S3	允許	PutObject	允許 EC2 應用程式將自訂日誌上傳至： `aws:s3:::mc-a*-logs-*/aws/instances/*/${aws:userid}/*`
明確拒絕 MC 命名空間 S3 日誌	拒絕	GetObject* Put*	不允許 EC2 應用程式從下列位置取得或放置任何物件： `aws:s3:::mc-*-logs-*/encrypted/mc*` ， `aws:s3:::mc-*-logs-*/mc/*`， `aws:s3:::mc-a*-logs-*-audit/*`
明確拒絕 S3 刪除	拒絕	*（全部）	不允許 EC2 應用程式對下列物件採取任何動作： `aws:s3:::mc-a*-logs-*/*` ， `aws:s3:::mc-a*-internal-*/*` ，
明確拒絕 S3 CFN 儲存貯體	拒絕	刪除*	不允許 EC2 應用程式從下列位置刪除任何物件： `aws:s3:::cf-templates-*`

CW = CloudWatch。ARN = Amazon Resource Name。* = 萬用字元（任何）。			
政策聲明	Effect	動作	描述和資源 (ARN)
明確拒絕清單儲存貯體 S3	拒絕	ListBucket	不允許您從下列位置列出任何加密、稽核日誌或預留 (mc) 物件：`aws:s3:::mc-*-logs-*`
AWS Secrets Manager 在 Amazon EC2 中			
Trend Cloud One 秘密存取	允許	GetSecretValue	允許 Amazon EC2 存取 Trend Cloud One 遷移的秘密： `aws:secretsmanager:*:*:secret:/ams/eps/cloud-one-agent-tenant-id*` ， `arn:aws:secretsmanager:*:*:secret:/ams/eps/cloud-one-agent-activation-token*` ， `aws:secretsmanager:*:*:secret:/ams/eps/cloud-one-agent-tenant-id*` ， `aws:secretsmanager:*:*:secret:/ams/eps/cloud-one-agent-tenant-guid*`
AWS Key Management Service 在 Amazon EC2 中			

CW = CloudWatch。ARN = Amazon Resource Name。* = 萬用字元 （任何）。			
政策聲明	Effect	動作	描述和資源 (ARN)
Trend Cloud One 解密金鑰	允許	解密	允許 Amazon EC2 以別名名稱 / ams/eps/cloudone-migration 解密 AWS KMS 金鑰 `arn:aws:kms:*:*:alias/ams/eps/cloudone-migration`

如果您不熟悉 Amazon IAM 政策，請參閱 IAM 政策概觀以取得重要資訊。

> **Note**
>
> 政策通常包含多個陳述式，其中每個陳述式會將許可授予一組不同的資源，或在特定條件下授予許可。

監控指標預設值

下表顯示監控的項目和預設提醒閾值。您可以使用變更管理變更請求 (RFC) 來變更預設值。

> **Note**
>
> CloudWatch 已於 2016 年 11 月 1 日啟動指標的延長保留。如需詳細資訊，請參閱 CloudWatch 限制。

基準監控的提醒

服務	安全提醒	警示名稱和觸發條件	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，這些提醒可以直接傳送到您的電子郵件 （如果您已選擇加入 Direct-Customer-Alerts SNS 主題）。			

服務	安全提醒	警示名稱和觸發條件	備註
Application Load Balancer (ALB) 執行個體	否	RejectedConnectionCount 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，CloudWatch 會發出警示。
Application Load Balancer (ALB) 目標	否	TargetConnectionErrorCount 總和 > 0，持續 1 分鐘，連續 5 次。	如果負載平衡器與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 – Windows	否	SecureChannelFailure 過去 15 個資料點中的 10 個 > 0.0。	Windows 執行個體上的 CloudWatch 警示會在安全頻道連線失敗時發出警示。
Aurora 執行個體	否	CPUUtilization > 85% 持續 5 分鐘，連續 2 次。	CloudWatch 警示。
AWS Backup	是	DeleteRecoveryPoint 非預期的 IAM 角色主體或 IAM 使用者主體已刪除 AWS Backup 復原點。	CloudWatch 事件。刪除備份復原點時發出。
AWS Outposts	是	AMSOutpostsInstanceFamilyCapacityAvailability InstanceFamilyCapacityAvailability = 80%，持續 5 分鐘，連續 12 次。	資源之執行個體系列容量可用性的 CloudWatch AWS Outposts 警示。

服務	安全提醒	警示名稱和觸發條件	備註
EC2 執行個體 - OSs	否	AMSOutpostsInstanceTypeCapacityAvailability TypeCapacityAvailability = 80%，持續 5 分鐘，連續 12 次。	資源之執行個體類型容量可用性的 CloudWatch AWS Outposts 警示。
		AMSOutpostsConnectedStatusConnectedStatus < 1 表示 5 分鐘，連續 1 次。	AWS Outposts 服務連結連線上的 CloudWatch 警示，少於 1 個會受損。
		AMSOutpostsCapacityExceptionCapacityExceptions 0 表示 5 分鐘，連續 1 次。	執行個體啟動 AWS Outposts 資源的容量不足錯誤上的 CloudWatch 警示 .
		CPUUtilization* >= 95%，持續 5 分鐘，連續 6 次。	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。
		StatusCheckFailed > 0 持續 5 分鐘，連續 3 次。	CloudWatch 警示。
		根磁碟區用量 >= 95%，持續 5 分鐘，連續 6 次。	

服務	安全提醒	警示名稱和觸發條件	備註
		非根磁碟區用量 > 85% 持續 5 分鐘，連續 2 次。 預設停用；如需其他資訊，請參閱 https://docs.aws.amazon.com/managedservices/latest/ctref/management-monitoring-cloudwatch-enable-non-root-volumes-monitoring.html#management-monitoring-cloudwatch-enable-non-root-volumes-monitoring-info。	
		記憶體可用* MemoryFree < 5%，持續 5 分鐘，連續 6 次。	
	是	EPS 惡意軟體 執行個體上發現惡意軟體。	CloudWatch 事件。
Amazon EC2 執行個體 - Linux	否	根磁碟區 Inode 用量 平均 >= 95%，持續 5 分鐘，連續 6 次。	CloudWatch 警示。僅適用於 Linux 執行個體。
		免費交換* 記憶體交換 < 5% 持續 5 分鐘，連續 6 次。	
ElastiCache 叢集	否	CurrConnections = 65000	此警示會通知 AMS ElastiCache 主機的最大連線限制。 CloudWatch 警示。如果您想要更新此閾值，請聯絡 AMS 支援。

服務	安全提醒	警示名稱和觸發條件	備註
ElastiCache 節點	否	CPUUtilization 平均 > 15 分鐘的預先定義值，連續 2 次。	CloudWatch 警示。預設為 90。如果是 Redis，請根據執行個體類型使用下列其中一個值： • cache.t1.micro：90% • cache.m1.small：90% • cache.m1.medium：90% • cache.m1.large：45% • cache.m1.xlarge：22.5% • cache.m2.xlarge：45% • cache.m2.4xlarge：11.25% • cache.c1.xlarge：11.25% • cache.t2.micro：90% • cache.t2.small：90% • cache.t2.medium：45% • cache.m3.medium：90% • cache.m3.large：45% • cache.m3.xlarge：22.5% • cache.m3.2xlarge：11.25% • cache.r3.large：45% • cache.r3.xlarge：22.5% • cache.r3.2xlarge：11.25% • cache.r3.4xlarge：5.625% • cache.r3.8xlarge：2.8125%
ElastiCache 節點 - memcached	否	SwapUsage 最大 > 50，000，000 位元組，持續 5 分鐘，連續 5 次。	CloudWatch 警示。僅適用於 memcached。

服務	安全提醒	警示名稱和觸發條件	備註
OpenSearch 叢集	否	ClusterStatus.red 最大值為 >= 1，持續 1 分鐘，連續 1 次。 當觸發此提醒時，AMS 會採取主動動作來降低操作影響。	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 Red Cluster 狀態。
OpenSearch 網域	否	KMSKeyError >= 1 表示 1 分鐘，連續 1 次。	CloudWatch 警示。用於在您的網域中加密靜態資料的 KMS 加密金鑰停用。重新啟用它來恢復正常操作。若要進一步了解，請參閱 OpenSearch Service Service 的靜態資料加密。
		ClusterStatus.yellow 最大值為 >= 1 持續 1 分鐘，連續 1 次 當觸發此提醒時，AMS 會採取主動動作來降低操作影響。	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。
		FreeStorageSpace 最小值為 <= 20480，持續 1 分鐘，連續 1 次 當觸發此提醒時，AMS 會採取主動動作來降低操作影響。	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。
		ClusterIndexWritesBlocked >= 1 持續 5 分鐘，連續 1 次 當觸發此提醒時，AMS 會採取主動動作來降低操作影響。	叢集正在封鎖寫入請求。若要進一步了解，請參閱 ClusterBlockException。

服務	安全提醒	警示名稱和觸發條件	備註
		節點 最小值為 < x，持續 1 天，連續 1 次 當觸發此提醒時，AMS 會採取主動動作來降低操作影響。	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。
		CPUUtilization 平均 >= 80%，持續 15 分鐘，連續 3 次 當觸發此提醒時，AMS 會採取主動動作來降低操作影響。	100% 的 CPU 使用率很常見，但持續高平均值卻有問題。可考慮使用較大的執行個體類型或新增執行個體。
		JVMMemoryPressure 最大值 >= 80%，持續 5 分鐘，連續 3 次 當觸發此提醒時，AMS 會採取主動動作來降低操作影響。	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。Amazon ES 會將執行個體 RAM 的一半用於 Java 堆積，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。
		MasterCPUUtilization 平均 >= 50%，持續 15 分鐘，連續 3 次 當觸發此提醒時，AMS 會採取主動動作來降低操作影響。	請考慮為您的專用主節點使用較大的執行個體類型。由於其在叢集穩定性和藍/綠部署中扮演的角色，專用主節點的平均 CPU 用量應該低於資料節點。

服務	安全提醒	警示名稱和觸發條件	備註
		MasterJVMMemoryPressure 最大值 >= 80%，持續 15 分鐘，連續 1 次 當觸發此提醒時，AMS 會採取主動動作來降低操作影響。	請考慮為您的專用主節點使用較大的執行個體類型。由於其在叢集穩定性和藍/綠部署中扮演的角色，專用主節點的平均 CPU 用量應該低於資料節點。
OpenSearch 執行個體	否	AutomatedSnapshotFailure 最大值為 >= 1，持續 1 分鐘，連續 1 次。	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。請參閱紅色叢集狀態。
Elastic Load Balancing 執行個體	否	SurgeQueueLength > 100 持續 1 分鐘，連續 15 次。	如果待定路由的請求數量過多，CloudWatch 會發出警示。
		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。
		SpilloverCount > 1 持續 1 分鐘，連續 15 次。	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。
GuardDuty 服務	是	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。	支援的 GuardDuty 調查結果類型清單位於 GuardDuty 作用中調查結果類型上。

服務	安全提醒	警示名稱和觸發條件	備註
醫療保健	各有不同	AWS Health 儀板表	與 AMS 支援的基準服務相關的 AWS Health 儀板表 (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。
AWS Managed Microsoft AD	否	Active Directory 狀態 AWS Managed Microsoft AD 執行個體會傳送作用中狀態事件。	服務事件。當目錄在事件後正常運作時發出。
		目錄狀態受損 AWS Managed Microsoft AD 執行個體會傳送受損的目錄狀態事件。	服務事件。當目錄以降級狀態執行時發出。已偵測到一個或多個問題，且並非所有目錄操作都能以完整的操作容量運作；
		無法運作的目錄狀態 AWS Managed Microsoft AD 執行個體會傳送無法操作的狀態事件。	服務事件。當目錄無法運作時發出。所有目錄端點均已回報問題。
		刪除目錄狀態 AWS Managed Microsoft AD 執行個體會傳送刪除目錄狀態事件。	服務事件。當目錄目前正在刪除時發出。
		失敗的目錄狀態 AWS Managed Microsoft AD 執行個體會傳送失敗狀態事件。	服務事件。當無法建立目錄時發出。
		RestoreFailed Directory 狀態 AWS Managed Microsoft AD 執行個體會傳送還原失敗的目錄狀態事件。	服務事件。從快照還原目錄時發出失敗。

服務	安全提醒	警示名稱和觸發條件	備註
Amazon RDS 執行個體	否	低儲存提醒會在資料庫執行個體的配置儲存用盡時觸發。	RDS-EVENT-0007，請參閱使用 Amazon RDS 事件通知的詳細資訊。
		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。	服務事件。RDS-EVENT-0031、Amazon RDS 事件類別和事件訊息。
		未嘗試容錯移轉 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。	服務事件。RDS-EVENT-0034、Amazon RDS 事件類別和事件訊息。
		資料庫執行個體的參數無效 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，因此客戶動作會是修改記憶體參數並重新啟動資料庫執行個體。	服務事件。RDS-EVENT-0035、Amazon RDS 事件類別和事件訊息。
		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、Amazon RDS 事件類別和事件訊息。
		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。	服務事件。RDS-EVENT-0045、Amazon RDS 事件類別和事件訊息。

服務	安全提醒	警示名稱和觸發條件	備註
		資料庫執行個體讀取複寫已結束 僅供讀取複本上的複寫已結束。	服務事件。RDS-EVENT-0057、Amazon RDS 事件類別和事件訊息。
		建立 statspack 使用者帳戶時發生錯誤 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、Amazon RDS 事件類別和事件訊息。
		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、Amazon RDS 事件類別和事件訊息。
		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。
		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、Amazon RDS 事件類別和事件訊息。
		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	安全提醒	警示名稱和觸發條件	備註
		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	RDS-EVENT-0089，請參閱 Amazon RDS 事件類別和事件訊息的詳細資訊。
		Aurora Serverless 資料庫叢集擴展失敗時的通知服務。	RDS-EVENT-0143，請參閱 Amazon RDS 事件類別和事件訊息的詳細資訊。
		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。
		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。
		此事件表示 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。
		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。
		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。
		RDS 無法佈建代理的容量，因為子網路中沒有足夠的可用 IP 地址。	RDS-EVENT-0243，請參閱 Amazon RDS 事件類別和事件訊息的詳細資訊。
		您 AWS 帳戶的儲存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	安全提醒	警示名稱和觸發條件	備註
		CPUUtilization 平均 CPU 使用率 > 90%，持續 15 分鐘，連續 2 次。	CloudWatch 警示。
		DiskQueueDepth 總和 > 75 持續 1 分鐘，連續 15 次。	
		FreeStorageSpace 平均 < 1，073，741，824 個位元組，持續 5 分鐘，連續 2 次。	
		SwapUsage 平均 >= 104，857，600 個位元組，持續 5 分鐘，連續 2 次。	
Amazon Redshift 叢集	否	RedshiftClusterStatus 叢集在 5 分鐘內未處於維護模式 < 1 時的運作狀態。	1 代表運作狀態良好的叢集。
Amazon Macie	是	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 Macie 提醒類型清單，請參閱分析 Amazon Macie 調查結果。請注意，並非所有帳戶都啟用 Macie。

日誌保留和輪換預設值

本節說明 AMS 日誌管理預設值；如需詳細資訊，請參閱日誌管理。

- 輪換 = 執行個體內的日誌周轉

- 保留 = 我們在 Amazon CloudWatch Logs 和 Amazon Simple Storage Service (S3) 中保留日誌的期間

日誌會視需要保留在 CloudWatch Logs 中（您可以設定此項目）和 S3 中。它們不會過期或遭到刪除，且會受限於服務耐久性。如需詳細的 S3 耐久性資訊，請參閱 Amazon S3 中的資料保護。

您可以請求變更所有日誌的日誌保留，但 AWS CloudTrail 日誌為稽核和安全性原因無限期保留。

日誌輪換是在執行個體內設定。根據預設，作業系統和安全性日誌會在達到超過 100MB 時每小時輪換，這樣做是為了確保您不會在執行個體中的磁碟上執行短時間。

執行個體內的日誌代理程式會將日誌線上上傳至 CloudWatch Logs，再從該處將日誌封存至 S3。

日誌會以產生的原始格式存放在 CloudWatch Logs 和 S3 中，不會進行預先處理。

持續性管理預設值

本節說明 AMS 持續性管理預設值；如需 AMS 備份的詳細資訊，請參閱 AMS 使用者指南持續性管理章節。

備份組態會在加入時完成。這些是預設（建議）備份設定。

VPC 標籤和預設值

如需 AMS 備份的最新資訊，請參閱持續性管理。

> **Important**
>
> 預設會停用 EC2 堆疊備份 (Backup = False)。您可以在建立時透過 RFC (CT ct-140EC27q0sjyt1h) 請求 EC2 堆疊`Key: Backup, Value: True`時新增標籤，以啟用 EC2 執行個體備份。 EC2 如果您想要在建立執行個體之後新增標籤，請提交 RFC 與 管理 | 進階堆疊元件 | EC2 執行個體堆疊 | 更新 CT (ct-38s4s4tm4ic4u)。

EC2 執行個體標籤和預設值

EC2 堆疊備份標籤指定堆疊是否需要連接的 EBS 磁碟區的快照。

`標籤 Key: Backup`

`標籤 Value: True, False`

根據預設， 值為False備份標籤不存在，且堆疊沒有排程備份。

將 標籤變更為 Key: Backup Value: True 以啟用備份，然後按照具有 VPC 備份標籤的排程集完成備份。

> **Note**
>
> 標籤值 （僅限值） 的大小寫不敏感，因此 True/true 或 False/false 都是可接受的。

RDS 執行個體備份和預設值

Amazon Relational Database Service (RDS) 預設值會在堆疊範本中定義：

```
Backup: Yes

Backup Window: 22:00-23:00 (RDS local time zone)

Retention Period: 7 (7 snapshots stored)
```

修補預設值

本節說明 AMS 修補預設值；如需 AMS 修補的詳細資訊，請參閱 AMS 使用者指南修補程式管理章節。

AMS 每月發行修補AMIs；所有新的堆疊請求都應設定最新的 AMS AMI。

> **Important**
>
> AMS Patch Orchestrator，標籤型修補，使用 AWS Systems Manager (SSM) 功能來允許您標記執行個體，或為您標記 AMS 標籤，並使用您設定的基準和視窗來修補這些執行個體。若要進一步了解，請參閱 Patch Orchestrator：以標籤為基礎的修補模型。

AMS-standard、以帳戶為基礎、修補：對於每個具有堆疊且接收到就地修補的帳戶，將在「修補星期二」之後不久傳送即將推出適用修補程式的通知。通知包含所有堆疊和適用修補程式的清單，以及建議的修補程式視窗。對於關鍵修補程式，視窗設定為不超過 10 天前，對於標準修補則為不超過 14 天前。如果您未回覆通知，則不會進行修補。如果您想要排除特定修補程式、回覆通知或提交服務請求。如果您回覆時同意修補，但未特別要求不同的排程，則會套用修補程式，如您收到的通知中所述。

> **Note**
>
> 修補程式服務通知是傳送給帳戶聯絡人的電子郵件，其中包含 AWS Support 主控台的連結。您可以透過 AWS Support 主控台或透過 AMS 服務請求頁面回覆，其中通知會顯示為服務通知。

在 AMS 標準修補程序時，AMS 會執行下列動作：

1. 您會在建議的修補時段前十四天收到修補服務通知。修補服務通知會透過電子郵件傳送至您帳戶中存檔的聯絡電子郵件地址。
2. 根據修補通知中提供的堆疊清單，識別堆疊中所有可連線的 EC2 執行個體。在此情況下，"Reachable" 表示處於 "Running" EC2 狀態的執行個體，並讓 EC2 Run Command 代理程式完全運作。
3. AMS 執行修補的方式可確保有足夠數量的 EC2 執行個體同時執行（透過 `healthy-host-threshold` 設定設定），讓堆疊保持正常運作。
4. 所有 EC2 執行個體的修補操作完成後，AMS 會以修補狀態更新 RFC：成功、部分成功或失敗。如果是成功以外的任何狀態，則會建立票證，讓操作員追蹤修補結果並採取任何修正動作。

驗證 AMS 服務 (SALZ)

為了驗證 AWS Managed Services (AMS) 服務是否如預期般運作，本章會說明您可以執行的一些練習。

尋找 AMS 帳戶設定

帳戶設定，用於建立 AMS RFCs、設定排程，以及判斷誰會收到通知。

某些設定會在加入期間建立，並要求變更服務請求。您應該記下這些帳戶的詳細資訊，因為您將在與 AMS 通訊時使用它們：

- 登入資料：如果您需要擷取 AMS 使用者名稱或密碼，請聯絡本機 IT 管理員--AMS 使用您的公司 Active Directory。
- Cloud Service Delivery Manager (CSDM)：此人員是您與 AMS 的聯絡人，可用於回答服務問題。您在加入時會收到此人員的聯絡資訊，而且應該讓組織中與 AMS 互動的所有人員都能使用。您可以預期從此人員收到有關 AMS 服務的每月報告。

- 主控台存取：您可以在專門為您的帳戶設定的 URL 中存取 AMS 主控台。您可以從 CSDM 取得 URL。
- AMS CLI：您可以透過 AMS 主控台開發人員的資源頁面或您從 CSDM 取得的可分發套件來取得 AMS CLI。在您擁有可分發套件之後，請遵循安裝或升級 AMS CLI 中概述的步驟。
- 維護時段：維護時段會決定 EC2 執行個體何時進行修補。AWS Managed Services 維護時段（或維護時段）會執行 AWS Managed Services (AMS) 的維護活動，並在每個月的第二個星期四太平洋時間下午 3 點至下午 4 點重複執行。AMS 可能會變更維護時段，但需提前 48 小時通知。您可能已在加入時選擇不同的時段 -- 保留所選維護時段的記錄。
- 監控：AMS 預設提供一組 CloudWatch 指標，但您也可以請求其他指標。如果您這樣做，請保留這些記錄。
- 日誌：根據預設，您的日誌會存放在 ams-a-*ACCOUNT_ID*-log-management-*REGION*，其中 *REGION* 是產生日誌的區域。
- 緩解：加入時，AMS 會記錄您選擇的緩解動作，以防發現對資源的惡意軟體攻擊。例如，聯絡特定人員。將此資訊提供給組織中與 AMS 互動的所有人員。
- 區域：您可以在 AMS 主控台中查看 VPC 詳細資訊頁面。您也可以在安裝 AMS SKMS CLI 之後執行此命令（此命令使用 SAML 設定檔，如果您的身分驗證方法不同，請移除）：

```
aws --profile saml amsskms get-vpc --vpc-id VPC_ID
```

Important

Note

AMS API/CLI (amscm 和 amsskms) 端點位於 AWS N. Virginia 區域 `us-east-1`。根據身分驗證的設定方式，以及您的帳戶和資源所在的 AWS 區域，您可能需要在發出命令`--region us-east-1`時新增 。如果這是您的身分驗證方法`--profile saml`，您可能還需要新增 。

在 AMS 中尋找 FQDNs

AWS Managed Services (AMS) 存取變更類型 (CTs) 需要 AMS 信任網域的完整網域名稱或 FQDN，格式為 `C844273800838.amazonaws.com`。若要探索您的 AWS FQDN，請執行下列其中一項操作：

- AWS 主控台：查看目錄名稱欄中的 AWS Directory Service 主控台。
- CLI：登入您的網域時，請使用下列命令：

  Windows（傳回使用者和 FQDN)：

```
whoami /upn
```

  或 (DC+DC+DC=FQDN)

```
whoami /fqdn
```

  Linux：

```
hostname --fqdn
```

> **Note**
>
> AMS API/CLI (amscm 和 amsskms) 端點位於 AWS N. Virginia 區域 `us-east-1`。根據身分驗證的設定方式，以及您的帳戶和資源所在的 AWS 區域，您可能需要在發出命令`--region us-east-1`時新增 。如果這是您的身分驗證方法`--profile saml`，您可能還需要新增 。

在 AMS 中尋找可用區域 AZs)

可用區域：所有帳戶至少有兩個可用區域。若要準確尋找您的可用區域名稱，您必須先知道相關聯的子網路 ID。

- AMS 主控台：在導覽窗格中按一下 VPCs，然後視需要按一下相關的 VPC。在 VPCs詳細資訊頁面上，選取子網路資料表中的相關子網路，以使用相關聯的可用區域名稱開啟子網路詳細資訊頁面。
- AMS SKMS API/CLI：

```
aws amsskms list-subnet-summaries --output table
```

```
aws amsskms get-subnet --subnet-id SUBNET_ID
```

> **Note**
>
> AMS API/CLI (amscm 和 amsskms) 端點位於 AWS N. Virginia 區域 `us-east-1`。根據身分驗證的設定方式，以及您的帳戶和資源所在的 AWS 區域，您可能需要在發出命令`--region us-east-1`時新增 。如果這是您的身分驗證方法`--profile saml`，您可能還需要新增 。

在 AMS 中尋找 SNS 主題

您的 SNS 主題會決定在各種情況下收到通知的人員。AMS 提供 AMI 通知的 SNS 主題 （ 請參閱使用 SNS 的 AMS AMI 通知)、CloudWatch 警示和 EC2 資源 （ 請參閱接收 AMS 產生的提醒) 等。若要探索現有的 SNS 主題：

- AWS 主控台：使用 SNS 主控台檢視所有主題、應用程式和訂閱，以及訊息圖表。同時建立、刪除、訂閱和發佈至主題。
- API/CLI （ 登入您的 AMS 帳戶時， 需要 AWS CLI)：

  列出您的 SNS 主題：

  ```
  aws sns list-topics
  ```

  列出您的 SNS 訂閱：

  ```
  aws sns list-subscriptions
  ```

> **Note**
>
> AMS API/CLI (amscm 和 amsskms) 端點位於 AWS N. Virginia 區域 `us-east-1`。根據身分驗證的設定方式，以及您的帳戶和資源所在的 AWS 區域，您可能需要在發出命令`--region us-east-1`時新增 。如果這是您的身分驗證方法`--profile saml`，您可能還需要新增 。

在 AMS 中尋找備份設定

備份和快照是由 AMS 透過原生AWS Backup服務管理。

組態是透過 AWS Backup 計劃管理。您可以有多個 AWS Backup 計劃，將標記的資源與備份排程和保留政策建立關聯。若要尋找您的 AMS 帳戶 AWS Backup 設定，請使用 https://console.aws.amazon.com/backup 主控台或備份命令的 AWS CLI 命令參考。

如需 AMS 和 的詳細資訊 AWS Backup，請參閱持續性管理。

尋找執行個體 ID 或 IP 地址

您需要執行個體 IP 地址才能登入執行個體。

- 若要請求存取執行個體、登入執行個體或建立 AMI，您必須擁有執行個體 ID。對於 EC2 執行個體（獨立執行個體或堆疊的一部分）或資料庫執行個體，您可以透過幾種不同的方式找到 ID：
  - ASG 堆疊中執行個體的 AMS 主控台：查看建立堆疊之 RFC 的 RFC 詳細資訊頁面。在執行輸出區段中，您會找到 ASG 堆疊的堆疊 ID，然後您可以前往 EC2 Console Auto Scaling Groups 頁面，搜尋該堆疊 ID 並尋找其執行個體。當您找到執行個體時，請選取它，並在頁面底部開啟包含詳細資訊的區域，包括 IP 地址。
  - 獨立 EC2 或資料庫（資料庫）執行個體的 AMS 主控台：查看建立 EC2 堆疊或資料庫執行個體之 RFC 的 RFC 詳細資訊頁面。在執行輸出區段中，您會找到執行個體 ID 和 IP 地址。
  - AWS EC2 主控台：
    1. 在導覽窗格中，選取 Instances (執行個體)。執行個體頁面隨即開啟。
    2. 按一下您想要 ID 的執行個體。執行個體詳細資訊頁面隨即開啟，並顯示 ID 和 IP 地址。
  - AWS 資料庫主控台：
    1. 在 首頁上，選取資料庫執行個體。執行個體頁面隨即開啟。
    2. 篩選您要為其 ID 的資料庫執行個體。執行個體詳細資訊頁面隨即開啟，並顯示 ID。
  - AMS CLI/API。

> **Note**
>
> 必須安裝 AMS CLI，這些命令才能運作。若要安裝 AMS API 或 CLI，請前往 AMS 主控台開發人員資源頁面。如需 AMS CM API 或 AMS SKMS API 的參考資料，請參閱《使用者指南》中的 AMS 資訊資源一節。您可能需要新增身分驗證`--profile`選項，例如 `aws amsskms ams-cli-command --profile SAML`。您可能還需要新增 `--region`選項，因為所有 AMS 命令都用盡 us-east-1；例如 `aws amscm ams-cli-command --region=us-east-1`。

> **Note**
>
> AMS API/CLI (amscm 和 amsskms) 端點位於 AWS N. Virginia 區域 `us-east-1`。根據身分驗證的設定方式，以及您的帳戶和資源所在的 AWS 區域，您可能需要在發出命令`--region us-east-1`時新增 。如果這是您的身分驗證方法`--profile saml`，您可能還需要新增 。

執行下列命令以取得堆疊執行輸出詳細資訊：

```
aws amsskms get-stack --stack-id STACK_ID
```

輸出看起來像這樣，InstanceId 出現在底部下方 `Outputs`（顯示的值為範例）：

```
{
    "Stack": {
        "StackId": "stack-7fa52bd5eb8240123",
        "Status": {
            "Id": "CreateCompleted",
            "Name": "CreateCompleted"
        },
        "VpcId": "vpc-01234567890abcdef",
        "Description": "Amazon",
        "Parameters": [
            {
                "Value": "sg-01234567890abcdef,sg-01234567890abcdef",
                "Key": "SecurityGroups"
            },
            {
                "Value": "subnet-01234567890abcdef",
                "Key": "InstanceSubnetId"
            },
            {
                "Value": "t2.large",
                "Key": "InstanceType"
            },
            {
                "Value": "ami-01234567890abcdef",
                "Key": "InstanceAmiId"
```

```
            }
        ],
        "Tags": [],
        "Outputs": [
            {
                "Value": "i-0b22a22eec53b9321",
                "Key": "InstanceId"
            },
            {
                "Value": "10.0.5.000",
                "Key": "InstancePrivateIP"
            }
        ],
        "StackTemplateId": "stm-s6xvs000000000000",
        "CreatedTime": "1486584508416",
        "Name": "Amazon"
    }
}
```

DNS 易記堡壘名稱

MALZ

對於多帳戶登陸區域 (MALZ)，系統會為 AMS 受管 Active Directory 的 FQDN 中的堡壘建立 DNS 記錄。AMS 會視需要取代 Linux 和 Windows 堡壘。例如，如果有新的堡壘 AMI 必須部署，堡壘 DNS 記錄會動態更新，以指向新的有效堡壘。

1. 若要存取 SSH (Linux) 堡壘，請使用如下所示的 DNS 記錄：
   `sshbastion(1-4).Your_Domain.com`

   例如，其中網域為 `Your_Domain`：

   - `sshbastion1.Your_Domain.com`
   - `sshbastion2.Your_Domain.com`
   - `sshbastion3.Your_Domain.com`
   - `sshbastion4.Your_Domain.com`
2. 若要存取 RDP (Windows) 堡壘，請使用如下所示的 DNS 記錄：`rdp-Username.Your_Domain.com`。

例如，其中使用者名稱為 alex、demo、 test或 bob，網域為 *Your_Domain*.com：

- rdp-alex.*Your_Domain*.com
- rdp-test.*Your_Domain*.com
- rdp-demo.*Your_Domain*.com
- rdp-bob.*Your_Domain*.com

SALZ

單一帳戶登陸區域 (SALZ) 會視需要取代 Linux 和 Windows 堡壘。例如，如果有新的堡壘 AMI 必須部署，堡壘 DNS 記錄會動態更新，以指向新的有效堡壘。

1. 若要存取 SSH (Linux) 堡壘，請使用如下所示的 DNS 記錄：sshbastion*(1-4)*.A*AccountNumber*.amazonaws.com.

   例如，其中 123456789012是帳戶號碼：

   - sshbastion1.A123456789012.amazonaws.com
   - sshbastion2.A123456789012.amazonaws.com
   - sshbastion3.A123456789012.amazonaws.com
   - sshbastion4.A123456789012.amazonaws.com

2. 若要存取 RDP (Windows) 堡壘，請使用如下所示的 DNS 記錄：rdpbastion*(1-4)*.A*ACCOUNT_NUMBER*.amazonaws.com。

   例如，其中 123456789012是帳戶號碼：

   - rdpbastion1.A123456789012.amazonaws.com
   - rdpbastion2.A123456789012.amazonaws.com
   - rdpbastion3.A123456789012.amazonaws.com
   - rdpbastion4.A123456789012.amazonaws.com

尋找堡壘 IP 地址

AMS 客戶可以使用先前DNS 易記堡壘名稱所述的 SSH 和 RDP 堡壘，或堡壘 IP 地址。

若要尋找您帳戶的堡壘 IP 地址、SSH 和 RDP：

1. 僅適用於多帳戶登陸區域：登入共用服務帳戶。
2. 開啟 EC2 主控台，然後選擇執行中的執行個體。

   執行個體頁面隨即開啟。
3. 在頂端的篩選方塊中，輸入 ssh-bastion 或 rdp-bastion。

   在頂端的篩選方塊中，輸入 customer-ssh 或 customer-rdp。

   顯示您帳戶的 SSH 和/或 RDP 堡壘。

   請注意，除了 SSH 堡壘之外，您可能會在清單中看到無法使用的 AMS 周邊網路堡壘。
4. 選取 SSH 或 RDP 堡壘。如果您使用 Windows 電腦並想要登入 Linux 執行個體，請使用 SSH 堡壘。如果您想要登入 Windows 執行個體，請使用 RDP 堡壘。如果您使用 Linux 作業系統並想要登入 Windows 執行個體，您可以透過 RDP 通道使用 SSH 堡壘（這樣您就可以存取 Windows 桌面）。若要從 Linux 作業系統存取 Linux 執行個體，請使用 SSH 堡壘。

EC2 執行個體：建立

您可以使用 AMS 主控台或 API/CLI 來建立具有額外磁碟區的 Amazon EC2 和 Amazon EC2。

建立堆疊

使用主控台建立 EC2 執行個體

以下顯示 AMS 主控台中的此變更類型。

運作方式：

1. 導覽至建立 RFC 頁面：在 AMS 主控台的左側導覽窗格中，按一下 RFCs以開啟 RFCs清單頁面，然後按一下建立 RFC。
2. 在預設瀏覽變更類型檢視中選擇熱門的變更類型 (CT)，或在依類別選擇檢視中選擇 CT。
   - 依變更類型瀏覽：您可以在快速建立區域中按一下熱門的 CT，以立即開啟執行 RFC 頁面。請注意，您無法透過快速建立選擇較舊的 CT 版本。

     若要排序 CTs，請使用卡片或資料表檢視中的所有變更類型區域。在任一檢視中，選取 CT，然後按一下建立 RFC 以開啟執行 RFC 頁面。如果適用，建立較舊版本選項會顯示在建立 RFC 按鈕旁。

- 依類別選擇：選取類別、子類別、項目和操作，如果適用，CT 詳細資訊方塊會開啟，其中包含使用較舊版本建立的選項。按一下建立 RFC 以開啟執行 RFC 頁面。

3. 在執行 RFC 頁面上，開啟 CT 名稱區域以查看 CT 詳細資訊方塊。需要主旨（如果您在瀏覽變更類型檢視中選擇 CT，則會為您填寫）。開啟其他組態區域以新增 RFC 的相關資訊。

   在執行組態區域中，使用可用的下拉式清單或輸入必要參數的值。若要設定選用的執行參數，請開啟其他組態區域。

4. 完成後，請按一下執行。如果沒有錯誤，RFC 成功建立的頁面會顯示已提交的 RFC 詳細資訊，以及初始的執行輸出。

5. 開啟執行參數區域以查看您提交的組態。重新整理頁面以更新 RFC 執行狀態。或者，取消 RFC 或使用頁面頂端的選項建立 RFC 的副本。

使用 CLI 建立 EC2 執行個體

運作方式：

1. 使用內嵌建立（您發出包含所有 RFC 和執行參數的`create-rfc`命令）或範本建立（您建立兩個 JSON 檔案，一個用於 RFC 參數，另一個用於執行參數），並使用兩個檔案作為輸入發出`create-rfc`命令。此處說明這兩種方法。
2. 使用傳回的 RFC ID 提交 RFC： `aws amscm submit-rfc --rfc-id` *`ID`*命令。

   監控 RFC： `aws amscm get-rfc --rfc-id` *`ID`*命令。

若要檢查變更類型版本，請使用下列命令：

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> 您可以將任何`CreateRfc`參數與任何 RFC 搭配使用，無論它們是否為變更類型結構描述的一部分。例如，若要在 RFC 狀態變更時取得通知，請將此行新增至請求的 `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` RFC 參數部分（而非執行參數）。如需所有 CreateRfc 參數的清單，請參閱 AMS 變更管理 API 參考。

內嵌建立：

使用內嵌提供的執行參數發出建立 RFC 命令（在內嵌提供執行參數時逸出引號），然後提交傳回的 RFC ID。例如，您可以將內容取代為如下內容：

```
aws amscm create-rfc --change-type-id "ct-14027q0sjyt1h" --change-type-version "4.0"
 --title "EC2-Create-RFC" --execution-parameters "{\"Description\": \"Create a new
 EC2 Instance stack\",\"VpcId\": \"vpc-0a60eb65b4EXAMPLE\",\"Name\": \"My-EC2\",
\"TimeoutInMinutes\": 60,\"Parameters\": {\"InstanceAmiId\": \"ami-1234567890EXAMPLE\",
\"InstanceDetailedMonitoring\": false,\"InstanceEBSOptimized\": false,\"InstanceProfile
\": \"customer-mc-ec2-instance-profile\",\"InstanceRootVolumeIops\": 3000,
\"InstanceRootVolumeType\": \"gp3\",\"InstanceType\": \"t2.large\",\"InstanceUserData
\": \"\",\"InstanceSubnetId\": \"subnet-0bb1c79de3EXAMPLE\",\"EnforceIMDSV2\":
 \"false\"}}"
```

範本建立：

1. 將此變更類型的執行參數輸出至 JSON 檔案；此範例會將其命名為 CreateEC2Params.json:

   ```
   aws amscm get-change-type-version --change-type-id "ct-14027q0sjyt1h" --query
    "ChangeTypeVersion.ExecutionInputSchema" --output text > CreateEC2Params.json
   ```

2. 修改並儲存 CreateEC2Params 檔案。例如，您可以將內容取代為如下內容：

   ```
   {
     "Description": "Create a new EC2 Instance stack",
     "VpcId": "vpc-0a60eb65b4EXAMPLE",
     "Name": "My-EC2",
     "TimeoutInMinutes": 60,
     "Parameters": {
       "InstanceAmiId": "ami-1234567890EXAMPLE",
       "InstanceDetailedMonitoring": false,
       "InstanceEBSOptimized": false,
       "InstanceProfile": "customer-mc-ec2-instance-profile",
       "InstanceRootVolumeIops": 3000,
       "InstanceRootVolumeType": "gp3",
       "InstanceType": "t2.large",
       "InstanceUserData": "",
       "InstanceSubnetId": "subnet-0bb1c79de3EXAMPLE",
       "EnforceIMDSV2": "false"
     }
   }
   ```

3. 將 RFC 範本輸出至目前資料夾中的檔案；此範例會將其命名為 CreateEC2Rfc.json:

```
aws amscm create-rfc --generate-cli-skeleton > CreateEC2Rfc.json
```

4. 修改並儲存 CreateEC2Rfc.json 檔案。例如，您可以將內容取代為類似以下內容：

```
{
"ChangeTypeVersion":    "4.0",
"ChangeTypeId":         "ct-14027q0sjyt1h",
"Title":                "EC2-Create-RFC"
}
```

5. 建立 RFC，指定 CreateEC2Rfc 檔案和 CreateEC2Params 檔案：

```
aws amscm create-rfc --cli-input-json file://CreateEC2Rfc.json  --execution-
parameters file://CreateEC2Params.json
```

   您會在回應中收到新 RFC 的 ID，並且可以使用它來提交和監控 RFC。在您提交之前，RFC 會保持在編輯狀態，不會啟動。

提示

安全群組

從此變更類型的 3.0 版開始，如果您指定自己的安全群組，AMS 不會連接預設 AMS 安全群組。如果您未在請求中指定自己的安全群組，AMS 會連接 AMS 預設安全群組。在舊版中，無論您是否提供自己的安全群組，AMS 都會連接預設安全群組。
目前，如果您指定自訂安全群組，您還必須為您的帳戶指定預設 AMS 安全群組IDs，`mc-initial-garden-SG-name`以及 `mc-initial-garden-SG-name`。

執行個體類型

AMS 不建議使用 t2.micro/t3.micro 和 t2.nano/t3.nano 類型。這些是較小的執行個體類型，可能會降低應用程式和 AMS 工具的效能。除了應用程式工作負載之外，EC2 執行個體還需要足夠的容量來支援 EPS、SSM 和 Cloudwatch 等 AMS 工具。如需詳細資訊，請參閱為您的應用程式選擇正確的 EC2 執行個體類型。

若要使用其他磁碟區建立 EC2 堆疊，請參閱 EC2 堆疊 | 建立（使用其他磁碟區）。

您最多可以新增 50 個標籤，但若要這樣做，您必須啟用其他組態檢視。

如有需要，請參閱 EC2 執行個體堆疊建立失敗。

建立堆疊（使用其他磁碟區）

使用主控台建立 EC2 執行個體和其他磁碟區

以下顯示 AMS 主控台中的此變更類型。

運作方式：

1. 導覽至建立 RFC 頁面：在 AMS 主控台的左側導覽窗格中，按一下 RFCs以開啟 RFCs清單頁面，然後按一下建立 RFC。
2. 在預設瀏覽變更類型檢視中選擇熱門的變更類型 (CT)，或在依類別選擇檢視中選擇 CT。
   - 依變更類型瀏覽：您可以在快速建立區域中按一下熱門的 CT，以立即開啟執行 RFC 頁面。請注意，您無法透過快速建立選擇較舊的 CT 版本。

     若要排序 CTs，請使用卡片或資料表檢視中的所有變更類型區域。在任一檢視中，選取 CT，然後按一下建立 RFC 以開啟執行 RFC 頁面。如果適用，建立較舊版本選項會顯示在建立 RFC 按鈕旁。
   - 依類別選擇：選取類別、子類別、項目和操作，如果適用，CT 詳細資訊方塊會開啟，其中包含使用較舊版本建立的選項。按一下建立 RFC 以開啟執行 RFC 頁面。
3. 在執行 RFC 頁面上，開啟 CT 名稱區域以查看 CT 詳細資訊方塊。需要主旨（如果您在瀏覽變更類型檢視中選擇 CT，則會為您填入）。開啟其他組態區域以新增 RFC 的相關資訊。

   在執行組態區域中，使用可用的下拉式清單或輸入必要參數的值。若要設定選用的執行參數，請開啟其他組態區域。
4. 完成後，請按一下執行。如果沒有錯誤，RFC 成功建立的頁面會顯示已提交的 RFC 詳細資訊，以及初始的執行輸出。
5. 開啟執行參數區域以查看您提交的組態。重新整理頁面以更新 RFC 執行狀態。或者，取消 RFC 或使用頁面頂端的選項建立 RFC 的副本。

使用 CLI 建立 EC2 執行個體和其他磁碟區

運作方式：

1. 使用內嵌建立（您發出包含所有 RFC 和執行參數的create-rfc命令）或範本建立（您建立兩個 JSON 檔案，一個用於 RFC 參數，另一個用於執行參數），並使用兩個檔案作為輸入發出create-rfc命令。此處說明這兩種方法。
2. 使用傳回的 RFC ID 提交 RFC： `aws amscm submit-rfc --rfc-id ID`命令。

   監控 RFC： `aws amscm get-rfc --rfc-id ID`命令。

若要檢查變更類型版本，請使用下列命令：

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> 您可以將任何CreateRfc參數與任何 RFC 搭配使用，無論它們是否為變更類型結構描述的一部分。例如，若要在 RFC 狀態變更時取得通知，請將此行新增至請求的 `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` RFC 參數部分（而非執行參數）。如需所有 CreateRfc 參數的清單，請參閱 AMS 變更管理 API 參考。

內嵌建立：

使用內嵌提供的執行參數發出建立 RFC 命令（在內嵌提供執行參數時逸出引號），然後提交傳回的 RFC ID（範例僅顯示必要參數）。例如，您可以將內容取代為如下內容：

```
aws amscm create-rfc --change-type-id "ct-1aqsjf86w6vxg" --change-type-version "4.0"
 --title "EC2-Create-A-V-QC" --execution-parameters "{\"Description\":\"My EC2 stack
 with addl vol\",\"VpcId\":\"VPC_ID\",\"Name\":\"My Stack\",\"StackTemplateId\":
\"stm-nn8v8ffhcal611bmo\",\"TimeoutInMinutes\":60,\"Parameters\":{\"InstanceAmiId\":
\"AMI_ID\",\"InstanceSubnetId\":\"SUBNET_ID\"}}
```

範本建立：

1. 將此變更類型的執行參數輸出至名為 CreateEC2AVParams.json.

   ```
   aws amscm get-change-type-version --change-type-id "ct-1aqsjf86w6vxg" --query
    "ChangeTypeVersion.ExecutionInputSchema" --output text > CreateEC2AVParams.json
   ```

2. 修改並儲存 CreateEC2AVParams 檔案（範例顯示大多數參數）。例如，您可以將內容取代為如下內容：

```
{
"Description":      "EC2-Create-1-Addl-Volumes",
"VpcId":            "VPC_ID",
"StackTemplateId":  "stm-nn8v8ffhcal611bmo",
"Name":             "My-EC2-1-Addl-Volume",
"TimeoutInMinutes": 60,
"Parameters":   {
    "InstanceAmiId":    "AMI_ID",
    "InstanceSecurityGroupIds": "SECURITY_GROUP_ID",
    "InstanceCoreCount": 1,
    "InstanceThreadsPerCore": 2,
    "InstanceDetailedMonitoring": "true",
    "InstanceEBSOptimized": "false",
    "InstanceProfile": "customer-mc-ec2-instance-profile",
    "InstanceRootVolumeIops": 100,
    "InstanceRootVolumeName": "/dev/xvda",
    "InstanceRootVolumeSize": 50,
    "InstanceRootVolumeType": "io1",
    "RootVolumeKmsKeyId": "default",
    "InstancePrivateStaticIp": "10.27.0.100",
    "InstanceSecondaryPrivateIpAddressCount": 0,
    "InstanceTerminationProtection": "false",
    "InstanceType": "t3.large",
    "CreditSpecification": "unlimited",
    "InstanceUserData": "echo $",
    "Volume1Encrypted": "true",
    "Volume1Iops":      "IOPS"
    "Volume1KmsKeyId":  "KMS_MASTER_KEY_ID",
    "Volume1Name":      "xvdh"
    "Volume1Size":      "2 GiB",
    "Volume1Snapshot":  "SNAPSHOT_ID",
    "Volume1Type":      "iol",
    "InstanceSubnetId": "SUBNET_ID"
    }
}
```

3. 將 RFC 範本輸出至目前資料夾中的檔案；此範例會將其命名為 CreateEC2AVRfc.json:

```
aws amscm create-rfc --generate-cli-skeleton > CreateEC2AVRfc.json
```

4. 修改並儲存 CreateEC2AVRfc.json 檔案。例如，您可以將內容取代為如下內容：

```
{
"ChangeTypeVersion":    "4.0",
"ChangeTypeId":         "ct-1aqsjf86w6vxg",
"Title":                "EC2-Create-1-Addl-Volume-RFC"
}
```

5. 建立 RFC，指定 CreateEC2AVRfc 檔案和 CreateEC2AVParams 檔案：

```
aws amscm create-rfc --cli-input-json file://CreateEC2AVRfc.json  --execution-
parameters file://CreateEC2AVParams.json
```

您會在回應中收到新 RFC 的 ID，並且可以使用它來提交和監控 RFC。在您提交之前，RFC 會保持在編輯狀態，不會啟動。

提示

Important

此變更類型有新版本 v 4.0，使用不同的 StackTemplateId (stm-nn8v8ffhcal611bmo)。
如果您在命令列使用此變更類型提交 RFC，這很重要。新版本引進兩個新參數 (RootVolumeKmsKeyId 和 CreditSpecification)，並變更一個現有參數 (InstanceType) 的預設值。

執行個體類型

- 如果您選擇指定核心或執行緒的數量，則必須指定兩者的值。使用參數 `InstanceCoreCount`和 `InstanceThreadsPerCore`。若要尋找核心/執行緒的有效組合，請參閱每個執行個體類型每個 CPU 核心的 CPU 核心和執行緒。
- AMS 不建議使用 t2.micro/t3.micro 或 t2.nano/t3.nano 執行個體類型。除了您的業務工作負載之外，這些太小而無法支援 EPS、SSM 和 Cloudwatch 等 AMS 工具。如需詳細資訊，請參閱為您的應用程式選擇正確的 EC2 執行個體類型。
- 在 4.0 版中，預設類型已從 t2.large 提升為 t3.large。根據預設，T3 執行個體會使用「無限制額度」啟動。即使執行個體使用所有 CPU 點數，您也不會體驗 CPU 限流。您可以改為選擇 T2 執行個體，並使用 CreditSpecification 無限制選項。

- 如需 Amazon EC2 的詳細資訊，包括大小建議，請參閱 Amazon Elastic Compute Cloud 文件。

若要在建立 EC2 堆疊之後以其他磁碟區更新，請參閱 EC2 執行個體堆疊：更新（使用其他磁碟區）

存取、請求

請求管理存取權

使用主控台請求管理員存取權

以下顯示 AMS 主控台中的此變更類型。

運作方式：

1. 導覽至建立 RFC 頁面：在 AMS 主控台的左側導覽窗格中，按一下 RFCs以開啟 RFCs清單頁面，然後按一下建立 RFC。
2. 在預設瀏覽變更類型檢視中選擇熱門的變更類型 (CT)，或在依類別選擇檢視中選擇 CT。
   - 依變更類型瀏覽：您可以在快速建立區域中按一下熱門的 CT，以立即開啟執行 RFC 頁面。請注意，您無法透過快速建立選擇較舊的 CT 版本。

     若要排序 CTs，請使用卡片或資料表檢視中的所有變更類型區域。在任一檢視中，選取 CT，然後按一下建立 RFC 以開啟執行 RFC 頁面。如果適用，建立舊版選項會顯示在建立 RFC 按鈕旁。
   - 依類別選擇：選取類別、子類別、項目和操作，如果適用，CT 詳細資訊方塊會開啟，其中包含使用較舊版本建立的選項。按一下建立 RFC 以開啟執行 RFC 頁面。
3. 在執行 RFC 頁面上，開啟 CT 名稱區域以查看 CT 詳細資訊方塊。需要主旨（如果您在瀏覽變更類型檢視中選擇 CT，則會為您填寫）。開啟其他組態區域以新增 RFC 的相關資訊。

   在執行組態區域中，使用可用的下拉式清單或輸入必要參數的值。若要設定選用的執行參數，請開啟其他組態區域。
4. 完成後，請按一下執行。如果沒有錯誤，RFC 成功建立的頁面會顯示已提交的 RFC 詳細資訊，以及初始的執行輸出。
5. 開啟執行參數區域以查看您提交的組態。重新整理頁面以更新 RFC 執行狀態。或者，取消 RFC 或使用頁面頂端的選項建立 RFC 的副本。

使用 CLI 請求管理員存取權

運作方式：

1. 使用內嵌建立（您發出包含所有 RFC 和執行參數的`create-rfc`命令）或範本建立（您建立兩個 JSON 檔案，一個用於 RFC 參數，另一個用於執行參數），並使用兩個檔案作為輸入發出`create-rfc`命令。此處說明這兩種方法。
2. 使用傳回的 RFC ID 提交 RFC： `aws amscm submit-rfc --rfc-id` *ID*命令。

   監控 RFC： `aws amscm get-rfc --rfc-id` *ID*命令。

若要檢查變更類型版本，請使用下列命令：

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> 您可以將任何`CreateRfc`參數與任何 RFC 搭配使用，無論它們是否為變更類型結構描述的一部分。例如，若要在 RFC 狀態變更時取得通知，請將此行新增至請求的 `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` RFC 參數部分（而非執行參數）。如需所有 CreateRfc 參數的清單，請參閱 AMS 變更管理 API 參考。

內嵌建立：

使用內嵌提供的執行參數發出建立 RFC 命令（在內嵌提供執行參數時逸出引號），然後提交傳回的 RFC ID。例如，您可以將內容取代為如下內容：

```
aws --profile saml amscm create-rfc --change-type-id "ct-1dmlg9g1l91h6" --change-type-
version "3.0" --title "Stack-Admin-Access-QC" --execution-parameters "{\"DomainFQDN
\":\"TEST.com\",\"StackIds\":[\"stack-01234567890abcdef\"],\"TimeRequestedInHours\":1,
\"Usernames\":[\"TEST\"],\"VpcId\":\"VPC_ID\"}"
```

範本建立：

1. 將此變更類型的執行參數 JSON 結構描述輸出至檔案；此範例會將其命名為 GrantAdminAccessParams.json:

```
aws amscm get-change-type-version --change-type-id "ct-1dmlg9g1l91h6"
 --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
 GrantAdminAccessParams.json
```

修改並儲存 GrantAdminAccessParams 檔案。例如，您可以將內容取代為如下內容：

```
{
"DomainFQDN":           "mycorpdomain.acme.com",
"StackIds":             [STACK_ID, STACK_ID],
"TimeRequestedInHours": 12,
"Username":             ["USERNAME", "USERNAME"],
"VpcId":                "VPC_ID"
}
```

請注意， TimeRequestedInHours選項預設為一小時。您最多可以請求 12 小時。

2. 將 RFC 範本輸出至目前資料夾中的檔案；此範例會將其命名為 GrantAdminAccessRfc.json:

```
aws amscm create-rfc --generate-cli-skeleton > GrantAdminAccessRfc.json
```

3. 修改並儲存 GrantAdminAccessRfc.json 檔案。例如，您可以將內容取代為如下內容：

```
{
"ChangeTypeId":         "ct-1dmlg9g1l91h6",
"ChangeTypeVersion":    "3.0",
"Title":                "Request-Admin-Access-to-EC2-RFC"
}
```

4. 建立 RFC，指定 GrantAdminAccessRfc 檔案和 GrantAdminAcessParams 檔案：

```
aws amscm create-rfc --cli-input-json file://GrantAdminAccessRfc.json --execution-
parameters file://GrantAdminAccessParams.json
```

您會在回應中收到新 RFC 的 ID，並使用它來提交和監控 RFC。在您提交之前，RFC 會保持在編輯狀態，不會啟動。

若要透過堡壘登入執行個體，請遵循下一個程序：執行個體存取範例。

提示

> **Note**
>
> 您可以在存取請求過期之前提交更新。如需詳細資訊，請參閱堆疊管理員存取 | 更新。
> 若要登入屬於 ASG 的執行個體，您可以請求存取 ASG 堆疊，這可讓您存取所有相關聯的執行個體。

如需請求 ReadOnly 存取的範例，請參閱 ReadOnly 存取： 請求。

請求 ReadOnly 存取

使用主控台請求 ReadOnly 存取

以下顯示 AMS 主控台中的此變更類型。

運作方式：

1. 導覽至建立 RFC 頁面：在 AMS 主控台的左側導覽窗格中，按一下 RFCs以開啟 RFCs清單頁面，然後按一下建立 RFC。
2. 在預設瀏覽變更類型檢視中選擇熱門的變更類型 (CT)，或在依類別選擇檢視中選擇 CT。
   - 依變更類型瀏覽：您可以在快速建立區域中按一下熱門的 CT，以立即開啟執行 RFC 頁面。請注意，您無法透過快速建立選擇較舊的 CT 版本。

     若要排序 CTs，請使用卡片或資料表檢視中的所有變更類型區域。在任一檢視中，選取 CT，然後按一下建立 RFC 以開啟執行 RFC 頁面。如果適用，建立較舊版本選項會顯示在建立 RFC 按鈕旁。
   - 依類別選擇：選取類別、子類別、項目和操作，如果適用，CT 詳細資訊方塊會開啟，其中包含使用較舊版本建立的選項。按一下建立 RFC 以開啟執行 RFC 頁面。
3. 在執行 RFC 頁面上，開啟 CT 名稱區域以查看 CT 詳細資訊方塊。需要主旨 （如果您在瀏覽變更類型檢視中選擇 CT，則會為您填入）。開啟其他組態區域以新增 RFC 的相關資訊。

   在執行組態區域中，使用可用的下拉式清單或輸入必要參數的值。若要設定選用的執行參數，請開啟其他組態區域。
4. 完成後，請按一下執行。如果沒有錯誤，RFC 成功建立的頁面會顯示已提交的 RFC 詳細資訊，以及初始的執行輸出。

5. 開啟執行參數區域以查看您提交的組態。重新整理頁面以更新 RFC 執行狀態。或者，取消 RFC 或使用頁面頂端的選項建立 RFC 的副本。

使用 CLI 請求 ReadOnly 存取

運作方式：

1. 使用內嵌建立（您發出包含所有 RFC 和執行參數的`create-rfc`命令）或範本建立（您建立兩個 JSON 檔案，一個用於 RFC 參數，另一個用於執行參數），並使用兩個檔案作為輸入發出`create-rfc`命令。此處說明這兩種方法。
2. 使用傳回的 RFC ID 提交 RFC： `aws amscm submit-rfc --rfc-id` *`ID`*命令。

   監控 RFC： `aws amscm get-rfc --rfc-id` *`ID`*命令。

若要檢查變更類型版本，請使用下列命令：

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> 您可以將任何`CreateRfc`參數與任何 RFC 搭配使用，無論它們是否為變更類型結構描述的一部分。例如，若要在 RFC 狀態變更時取得通知，請將此行新增至請求的 `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` RFC 參數部分（而非執行參數）。如需所有 CreateRfc 參數的清單，請參閱 AMS 變更管理 API 參考。

內嵌建立：

使用內嵌提供的執行參數發出建立 RFC 命令（在內嵌提供執行參數時逸出引號），然後提交傳回的 RFC ID。例如，您可以將內容取代為如下內容：

```
aws --profile saml amscm create-rfc --change-type-id "ct-199h35t7uz6jl" --change-type-
version "3.0" --title "Stack-RO-Access-QC" --execution-parameters "{\"DomainFQDN\":
\"TEST.com\",\"StackIds\":[\"stack-01234567890abcdef\"],\"TimeRequestedInHours\":1,
\"Usernames\":[\"TEST\"],\"VpcId\":\"VPC_ID\"}"
```

範本建立：

1. 將此變更類型的執行參數 JSON 結構描述輸出至檔案；此範例會將其命名為 GrantReadOnlyAccessParams.json:

```
aws amscm get-change-type-version --change-type-id "ct-199h35t7uz6jl"
 --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
 GrantReadOnlyAccessParams.json
```

修改並儲存 GrantReadOnlyAccessParams 檔案。例如，您可以將內容取代為如下內容：

```
{
"DomainFQDN":           "mycorpdomain.acme.com",
"StackIds":             [STACK_ID, STACK_ID],
"TimeRequestedInHours": 12,
"Usernames":             ["USERNAME", "USERNAME"],
"VpcId":                "VPC_ID"
}
```

請注意， TimeRequestedInHours選項預設為一小時。您最多可以請求 12 小時。

2. 將 RFC 範本輸出至目前資料夾中的檔案；此範例會將其命名為 GrantReadOnlyAccessRfc.json:

```
aws amscm create-rfc --generate-cli-skeleton > GrantReadOnlyAccessRfc.json
```

3. 修改並儲存 GrantReadOnlyAccessRfc.json 檔案。例如，您可以將內容取代為如下內容：

```
{
"ChangeTypeId":         "ct-199h35t7uz6jl",
"ChangeTypeVersion":    "3.0",
"Title":                "Request-ReadOnly-Access-to-EC2-RFC"
}
```

4. 建立 RFC，指定 GrantReadOnlyAccessRfc 檔案和 GrantReadOnlyAcessParams 檔案：

```
aws amscm create-rfc --cli-input-json file://GrantReadOnlyAccessRfc.json --
execution-parameters file://GrantReadOnlyAccessParams.json
```

您會在回應中收到新 RFC 的 ID，並且可以使用它來提交和監控 RFC。在您提交之前，RFC 會保持在編輯狀態，不會啟動。

若要透過堡壘登入執行個體，請遵循下一個程序：執行個體存取範例。

提示

> **Note**
>
> 您可以在存取請求過期之前提交更新。如需詳細資訊，請參閱堆疊唯讀存取 | 更新。
> 若要登入屬於 EC2 Auto Scaling 群組 (ASG) 的執行個體，您可以請求存取 ASG 堆疊，這可讓您存取所有相關聯的執行個體。

如需請求管理員存取權的逐步解說，請參閱管理員存取權：請求。

其他 | 其他 RFC，建立 (CLI)

此範例說明如何使用管理 | 其他 | 其他 | 建立 CTs (ct-1e1xtak34nx76)，請求變更任何可用的 CT 地址。

當您找不到所需的變更類型時，請使用此 CT；不過，如果您不確定在現有 CT 中指定參數，最好提交服務請求以尋求協助。如需提交服務請求的資訊，請參閱服務請求範例。

這種類型的 RFC 是核准的必要項目，這表示它需要 AMS 核准才能實作。提交 RFC 之後，AMS 運算子會與您聯絡，以討論您要部署的堆疊。

> **Note**
>
> 使用「需要檢閱」CTs時，AMS 建議您使用 ASAP 排程選項（在主控台中選擇 ASAP，在 API/CLI 中保留開始和結束時間空白），因為這些 CTs 需要 AMS 運算子來檢查 RFC，並在核准和執行之前與您通訊。如果您排程這些 RFCs，請務必至少允許 24 小時。如果未在排定的開始時間之前進行核准，則會自動拒絕 RFC。

必要資料：

- `Comment`：RFC 的用途。
- `ChangeTypeId` 和 `ChangeTypeVersion`：使用其他 | 建立 (`ct-1e1xtak34nx76`) 來請求新資源，使用其他 | 更新 (`ct-0xdawir96cy7k`) 來變更現有資源；兩者皆為 `v1`。

選擇性資料：Priority：可接受的值為 High、 Medium或 Low。

內嵌建立：

- 使用內嵌提供的執行參數發出建立 RFC 命令 （ 在內嵌提供執行參數時逸出引號 ）。範例使用其他 | 建立。

```
aws amscm create-rfc --change-type-id "ct-1e1xtak34nx76" --change-type-version "1.0"
 --title "TITLE" --execution-parameters "{\"Comment\": \"What you want created\"}"
```

- 使用建立 RFC 操作中傳回的 RFC ID 提交 RFC。在提交之前，RFC 會保持 Editing 狀態，且不會採取任何動作。

```
aws amscm submit-rfc --rfc-id RFC_ID
```

- 監控 RFC 狀態並檢視執行輸出：

```
aws amscm get-rfc --rfc-id RFC_ID
```

範本建立：

1. 建立並儲存執行參數的 JSON 檔案；範例會將其命名為 OtherParams.json，並包含選用Priority參數：

```
{
"Comment":          "What you want created",
"Priority":         "Medium"
}
```

2. 建立並儲存 RFC 參數的 JSON 檔案；範例會將其命名為 OtherRfc.json.

```
{
"ChangeTypeId":         "ct-1e1xtak34nx76",
"ChangeTypeVersion":    "1.0",
"Title":                "TITLE"
}
```

3. 建立 RFC，指定 OtherRfc 檔案和 OtherParams 檔案：

```
aws amscm create-rfc --cli-input-json file://OtherRfc.json  --execution-parameters
 file://OtherParams.json
```

您會在回應中收到新 RFC 的 RfcId。例如：

```
{
"RfcId": "RFC-ID"
}
```

4. 提交 RFC：

```
aws amscm submit-rfc --rfc-id RFC-ID
```

如果未回報錯誤，表示操作成功。

5. 若要監控請求的狀態和檢視執行輸出：

```
aws amscm get-rfc --rfc-id RFC-ID
```

任何堆疊：刪除、重新啟動、啟動、停止

您可以使用 AMS 主控台或 API/CLI 來刪除、重新啟動、啟動或停止 AMS 堆疊。

刪除堆疊

使用主控台刪除堆疊

AMS 主控台中此變更類型的螢幕擷取畫面：

運作方式：

1. 導覽至建立 RFC 頁面：在 AMS 主控台的左側導覽窗格中，按一下 RFCs以開啟 RFCs清單頁面，然後按一下建立 RFC。
2. 在預設瀏覽變更類型檢視中選擇熱門的變更類型 (CT)，或在依類別選擇檢視中選擇 CT。
   - 依變更類型瀏覽：您可以在快速建立區域中按一下熱門的 CT，以立即開啟執行 RFC 頁面。請注意，您無法透過快速建立選擇較舊的 CT 版本。

若要排序 CTs，請使用卡片或資料表檢視中的所有變更類型區域。在任一檢視中，選取 CT，然後按一下建立 RFC 以開啟執行 RFC 頁面。如果適用，建立較舊版本選項會顯示在建立 RFC 按鈕旁。

- 依類別選擇：選取類別、子類別、項目和操作，如果適用，CT 詳細資訊方塊會開啟，其中包含使用較舊版本建立的選項。按一下建立 RFC 以開啟執行 RFC 頁面。

3. 在執行 RFC 頁面上，開啟 CT 名稱區域以查看 CT 詳細資訊方塊。需要主旨（如果您在瀏覽變更類型檢視中選擇 CT，則會為您填寫）。開啟其他組態區域以新增 RFC 的相關資訊。

   在執行組態區域中，使用可用的下拉式清單或輸入必要參數的值。若要設定選用的執行參數，請開啟其他組態區域。

4. 完成後，請按一下執行。如果沒有錯誤，RFC 成功建立的頁面會顯示已提交的 RFC 詳細資訊，以及初始的執行輸出。
5. 開啟執行參數區域以查看您提交的組態。重新整理頁面以更新 RFC 執行狀態。或者，取消 RFC 或使用頁面頂端的選項建立 RFC 的副本。

使用 CLI 刪除堆疊

運作方式：

1. 使用內嵌建立（您發出包含所有 RFC 和執行參數的`create-rfc`命令）或範本建立（您建立兩個 JSON 檔案，一個用於 RFC 參數，另一個用於執行參數），並使用兩個檔案作為輸入發出`create-rfc`命令。此處說明這兩種方法。
2. 使用傳回的 RFC ID 提交 RFC： `aws amscm submit-rfc --rfc-id` *`ID`*命令。

   監控 RFC： `aws amscm get-rfc --rfc-id` *`ID`*命令。

若要檢查變更類型版本，請使用下列命令：

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> 您可以將任何`CreateRfc`參數與任何 RFC 搭配使用，無論它們是否為變更類型結構描述的一部分。例如，若要在 RFC 狀態變更時取得通知，請將此行新增至請求的 `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` RFC 參

數部分（而非執行參數）。如需所有 CreateRfc 參數的清單，請參閱 AMS 變更管理 API 參考。

內嵌建立：

使用內嵌提供的執行參數發出建立 RFC 命令（在內嵌提供執行參數時逸出引號），然後提交傳回的 RFC ID。例如，您可以將內容取代為如下內容：

```
aws amscm create-rfc --change-type-id "ct-0q0bic0ywqk6c" --change-type-version "1.0" --
title "Delete My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

範本建立：

1. 將 RFC 範本輸出至目前資料夾中的檔案；此範例會將其命名為 DeleteStackRfc.json:

   ```
   aws amscm create-rfc --generate-cli-skeleton > DeleteStackRfc.json
   ```

2. 修改並儲存 DeleteStackRfc.json 檔案。

   ExecutionParameters JSON 延伸中的內部引號必須以反斜線 (\) 逸出。沒有開始和結束時間的範例：

   ```
   {
   "ChangeTypeVersion":    "1.0",
   "ChangeTypeId":         "ct-0q0bic0ywqk6c",
   "Title":                "Delete-My-Stack-RFC"
   "ExecutionParameters":  "{
           \"StackId\":\"STACK_ID\"}"
   }
   ```

3. 建立 RFC：

   ```
   aws amscm create-rfc --cli-input-json file://DeleteStackRfc.json
   ```

   您會在回應中收到新 RFC 的 ID，並且可以使用它來提交和監控 RFC。在您提交之前，RFC 會保持在編輯狀態，不會啟動。

提示

> **Note**
>
> 如果刪除 S3 儲存貯體，必須先清空物件。

> **Important**
>
> 刪除堆疊可能會產生不想要和非預期的後果。如需重要注意事項，請參閱 RFC 故障診斷一節刪除堆疊RFCs。

重新啟動堆疊

使用主控台重新啟動堆疊

AMS 主控台中此變更類型的螢幕擷取畫面：

運作方式：

1. 導覽至建立 RFC 頁面：在 AMS 主控台的左側導覽窗格中，按一下 RFCs以開啟 RFCs清單頁面，然後按一下建立 RFC。
2. 在預設瀏覽變更類型檢視中選擇熱門的變更類型 (CT)，或在依類別選擇檢視中選擇 CT。
   - 依變更類型瀏覽：您可以在快速建立區域中按一下熱門的 CT，以立即開啟執行 RFC 頁面。請注意，您無法透過快速建立選擇較舊的 CT 版本。

     若要排序 CTs，請使用卡片或資料表檢視中的所有變更類型區域。在任一檢視中，選取 CT，然後按一下建立 RFC 以開啟執行 RFC 頁面。如果適用，建立較舊版本選項會顯示在建立 RFC 按鈕旁。
   - 依類別選擇：選取類別、子類別、項目和操作，如果適用，CT 詳細資訊方塊會開啟，其中包含使用較舊版本建立的選項。按一下建立 RFC 以開啟執行 RFC 頁面。
3. 在執行 RFC 頁面上，開啟 CT 名稱區域以查看 CT 詳細資訊方塊。需要主旨 （如果您在瀏覽變更類型檢視中選擇 CT，則會為您填入）。開啟其他組態區域以新增 RFC 的相關資訊。

   在執行組態區域中，使用可用的下拉式清單或輸入必要參數的值。若要設定選用的執行參數，請開啟其他組態區域。

4. 完成後，請按一下執行。如果沒有錯誤，RFC 成功建立的頁面會顯示已提交的 RFC 詳細資訊，以及初始的執行輸出。
5. 開啟執行參數區域以查看您提交的組態。重新整理頁面以更新 RFC 執行狀態。或者，取消 RFC 或使用頁面頂端的選項建立 RFC 的副本。

使用 CLI 重新啟動堆疊

運作方式：

1. 使用內嵌建立（您發出包含所有 RFC 和執行參數的`create-rfc`命令）或範本建立（您建立兩個 JSON 檔案，一個用於 RFC 參數，另一個用於執行參數），並使用兩個檔案作為輸入發出`create-rfc`命令。此處說明這兩種方法。
2. 使用傳回的 RFC ID 提交 RFC： `aws amscm submit-rfc --rfc-id` *`ID`*命令。

   監控 RFC： `aws amscm get-rfc --rfc-id` *`ID`*命令。

若要檢查變更類型版本，請使用下列命令：

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> 您可以將任何`CreateRfc`參數與任何 RFC 搭配使用，無論它們是否為變更類型結構描述的一部分。例如，若要在 RFC 狀態變更時取得通知，請將此行新增至請求的 `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` RFC 參數部分（而非執行參數）。如需所有 CreateRfc 參數的清單，請參閱 AMS 變更管理 API 參考。

內嵌建立：

使用內嵌提供的執行參數發出建立 RFC 命令（在內嵌提供執行參數時逸出引號），然後提交傳回的 RFC ID。例如，您可以將內容取代為如下內容：

```
aws amscm create-rfc --change-type-id "ct-02u0hoaa9grat" --change-type-version "1.0" --
title "Reboot My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

範本建立：

1. 將 RFC 範本輸出到目前資料夾中的檔案。此範例將其命名為 RebootStackRfc.json. 請注意，由於只有一個用於停止（重新啟動或啟動）執行個體的執行參數，因此執行參數可以位於結構描述 JSON 檔案本身，而且不需要建立單獨的執行參數 JSON 檔案。

```
aws amscm create-rfc --generate-cli-skeleton > StopInstanceRfc.json
```

2. 修改並儲存 RebootStackRfc.json 檔案。

   `ExecutionParameters` JSON 延伸中的內部引號必須以反斜線 (\) 逸出。範例：

```
{
"ChangeTypeId":          "ct-02u0hoaa9grat",
"Title":                 "Reboot-My-EC2-RFC",
"TimeoutInMinutes":      60,
"ExecutionParameters":   "{
        \"StackId\":\"STACK_ID\"
    }"
}
```

3. 建立 RFC：

```
aws amscm create-rfc --cli-input-json file://RebootStackRfc.json
```

   您會在回應中收到新 RFC 的 ID，並且可以使用它來提交和監控 RFC。在您提交之前，RFC 會保持在編輯狀態，不會啟動。

提示

如需有關 Application Load Balancer 的資訊，請參閱 Application Load Balancer。

啟動堆疊

使用主控台啟動堆疊

AMS 主控台中此變更類型的螢幕擷取畫面：

運作方式：

1. 導覽至建立 RFC 頁面：在 AMS 主控台的左側導覽窗格中，按一下 RFCs以開啟 RFCs清單頁面，然後按一下建立 RFC。
2. 在預設瀏覽變更類型檢視中選擇熱門的變更類型 (CT)，或在依類別選擇檢視中選擇 CT。
   - 依變更類型瀏覽：您可以在快速建立區域中按一下熱門的 CT，以立即開啟執行 RFC 頁面。請注意，您無法透過快速建立選擇較舊的 CT 版本。

     若要排序 CTs，請使用卡片或資料表檢視中的所有變更類型區域。在任一檢視中，選取 CT，然後按一下建立 RFC 以開啟執行 RFC 頁面。如果適用，建立較舊版本選項會顯示在建立 RFC 按鈕旁。
   - 依類別選擇：選取類別、子類別、項目和操作，如果適用，CT 詳細資訊方塊會開啟，其中包含使用較舊版本建立的選項。按一下建立 RFC 以開啟執行 RFC 頁面。
3. 在執行 RFC 頁面上，開啟 CT 名稱區域以查看 CT 詳細資訊方塊。需要主旨 （如果您在瀏覽變更類型檢視中選擇 CT，則會為您填入）。開啟其他組態區域以新增 RFC 的相關資訊。

   在執行組態區域中，使用可用的下拉式清單或輸入必要參數的值。若要設定選用的執行參數，請開啟其他組態區域。
4. 完成後，請按一下執行。如果沒有錯誤，RFC 成功建立的頁面會顯示已提交的 RFC 詳細資訊，以及初始的執行輸出。
5. 開啟執行參數區域以查看您提交的組態。重新整理頁面以更新 RFC 執行狀態。或者，取消 RFC 或使用頁面頂端的選項建立 RFC 的副本。

使用 CLI 啟動堆疊

運作方式：

1. 使用內嵌建立 （您發出包含所有 RFC 和執行參數的`create-rfc`命令） 或範本建立 （您建立兩個 JSON 檔案，一個用於 RFC 參數，另一個用於執行參數），並使用兩個檔案作為輸入發出`create-rfc`命令。此處說明這兩種方法。
2. 使用傳回的 RFC ID 提交 RFC： `aws amscm submit-rfc --rfc-id` *`ID`*命令。

   監控 RFC： `aws amscm get-rfc --rfc-id` *`ID`*命令。

若要檢查變更類型版本，請使用下列命令：

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> 您可以將任何CreateRfc參數與任何 RFC 搭配使用，無論它們是否為變更類型結構描述的一部分。例如，若要在 RFC 狀態變更時取得通知，請將此行新增至請求的 `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` RFC 參數部分（而非執行參數）。如需所有 CreateRfc 參數的清單，請參閱 AMS 變更管理 API 參考。

內嵌建立：

使用內嵌提供的執行參數發出建立 RFC 命令（在內嵌提供執行參數時逸出引號），然後提交傳回的 RFC ID。例如，您可以將內容取代為如下內容：

```
aws amscm create-rfc --change-type-id "ct-1h5xgl9cr4bzy" --change-type-version "1.0" --
title "Start My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

範本建立：

1. 將 RFC 範本輸出到目前資料夾中的檔案。此範例會將其命名為 StartInstanceRfc.json. 請注意，由於啟動堆疊只有一個執行參數，因此執行參數可以位於結構描述 JSON 檔案本身，而且不需要建立單獨的執行參數 JSON 檔案。

   ```
   aws amscm create-rfc --generate-cli-skeleton > StartStackRfc.json
   ```

2. 修改並儲存 StartStackRfc.json 檔案。例如，您可以將內容取代為如下內容：

   ```
   {
   "ChangeTypeId":         "ct-1h5xgl9cr4bzy",
   "Title":                "Start-My-EC2-RFC",
   "TimeoutInMinutes":     60,
   "ExecutionParameters":  "{
           \"StackId\":\"STACK_ID\"
       }"
   }
   ```

3. 建立 RFC：

   ```
   aws amscm create-rfc --cli-input-json file://StartStackRfc.json
   ```

您會在回應中收到新 RFC 的 ID，並且可以使用它來提交和監控 RFC。在您提交之前，RFC 會保持在編輯狀態，不會啟動。

提示

如需 Application Load Balancer 的詳細資訊，請參閱 Application Load Balancer。

停止堆疊

使用主控台停止堆疊

AMS 主控台中此變更類型的螢幕擷取畫面：

運作方式：

1. 導覽至建立 RFC 頁面：在 AMS 主控台的左側導覽窗格中，按一下 RFCs以開啟 RFCs清單頁面，然後按一下建立 RFC。
2. 在預設瀏覽變更類型檢視中選擇熱門的變更類型 (CT)，或在依類別選擇檢視中選擇 CT。
   - 依變更類型瀏覽：您可以在快速建立區域中按一下熱門的 CT，以立即開啟執行 RFC 頁面。請注意，您無法透過快速建立選擇較舊的 CT 版本。

     若要排序 CTs，請使用卡片或資料表檢視中的所有變更類型區域。在任一檢視中，選取 CT，然後按一下建立 RFC 以開啟執行 RFC 頁面。如果適用，建立較舊版本選項會顯示在建立 RFC 按鈕旁。
   - 依類別選擇：選取類別、子類別、項目和操作，如果適用，CT 詳細資訊方塊會開啟，其中包含使用較舊版本建立的選項。按一下建立 RFC 以開啟執行 RFC 頁面。
3. 在執行 RFC 頁面上，開啟 CT 名稱區域以查看 CT 詳細資訊方塊。需要主旨 （如果您在瀏覽變更類型檢視中選擇 CT，則會為您填入）。開啟其他組態區域以新增 RFC 的相關資訊。

   在執行組態區域中，使用可用的下拉式清單或輸入必要參數的值。若要設定選用的執行參數，請開啟其他組態區域。
4. 完成後，請按一下執行。如果沒有錯誤，RFC 成功建立的頁面會顯示已提交的 RFC 詳細資訊，以及初始的執行輸出。
5. 開啟執行參數區域以查看您提交的組態。重新整理頁面以更新 RFC 執行狀態。或者，取消 RFC 或使用頁面頂端的選項建立 RFC 的副本。

使用 CLI 停止堆疊

運作方式：

1. 使用內嵌建立（您發出包含所有 RFC 和執行參數的`create-rfc`命令）或範本建立（您建立兩個 JSON 檔案，一個用於 RFC 參數，另一個用於執行參數），並使用兩個檔案作為輸入發出`create-rfc`命令。此處說明這兩種方法。
2. 使用傳回的 RFC ID 提交 RFC： `aws amscm submit-rfc --rfc-id` *`ID`*命令。

   監控 RFC： `aws amscm get-rfc --rfc-id` *`ID`*命令。

若要檢查變更類型版本，請使用下列命令：

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> 您可以將任何`CreateRfc`參數與任何 RFC 搭配使用，無論它們是否為變更類型結構描述的一部分。例如，若要在 RFC 狀態變更時取得通知，請將此行新增至請求的 `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` RFC 參數部分（而非執行參數）。如需所有 CreateRfc 參數的清單，請參閱 AMS 變更管理 API 參考。

內嵌建立：

使用內嵌提供的執行參數發出建立 RFC 命令（在內嵌提供執行參數時逸出引號），然後提交傳回的 RFC ID。例如，您可以將內容取代為如下內容：

```
aws amscm create-rfc --change-type-id "ct-3dgbnh6gpst4d" --change-type-version "1.0" --
title "Stop My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

範本建立：

1. 將 RFC 範本輸出到目前資料夾中的檔案。此範例將其命名為 StopStackRfc.json. 請注意，由於只有一個用於停止（重新啟動或啟動）執行個體的執行參數，因此執行參數可以位於結構描述 JSON 檔案本身，而且不需要建立單獨的執行參數 JSON 檔案。

```
aws amscm create-rfc --generate-cli-skeleton > StopStackRfc.json
```

2. 修改並儲存 StopStackRfc.json 檔案。例如，您可以將內容取代為如下內容：

```
{
"ChangeTypeId":          "ct-3dgbnh6gpst4d",
"Title":                 "Stop-My-EC2-RFC",
"TimeoutInMinutes":      60,
"ExecutionParameters":   "{
        \"StackId\":\"STACK_ID\"
    }"
}
```

3. 建立 RFC：

```
aws amscm create-rfc --cli-input-json file://StopInstanceRfc.json
```

您會在回應中收到新 RFC 的 ID，並且可以使用它來提交和監控 RFC。在您提交之前，RFC 會保持在編輯狀態，不會啟動。

提示

停止的執行個體會保持停止狀態，除非您已使用 AMS Resource Scheduler 排程重新啟動。

如有需要，請參閱 EC2 執行個體堆疊停止失敗。

存取範例

這些範例示範如何在透過 RFC 授予存取權後，透過堡壘登入執行個體。如需取得授予存取權的詳細資訊，請參閱存取請求。

> **Note**
>
> 透過 Auto Scaling 群組建立的 EC2 執行個體將具有循環進出的 IP 地址，而且您必須使用 EC2 主控台來尋找該 IP 地址。

必要資料：

- 堡壘 DNS 易記名稱或 IP 地址：如 所述使用 DNS 易記名稱，DNS 易記堡壘名稱或如 所述尋找堡壘 IP 地址尋找堡壘 IP 地址。
- 使用者名稱 （ 例如 username@customerdomain.com) 和密碼：帳戶的登入資料。
- 堆疊 IP 地址：查看您要登入之堆疊的 AMS 主控台 Stacks 頁面，然後在帳戶的 EC2 主控台中篩選該堆疊 ID，以達成此目的。對於單一 EC2 執行個體，您也可以使用 AMS SKMS 命令 對於 AMS SKMS API 參考，請參閱 AWS Artifact 主控台中的報告索引標籤。 尋找堆疊 ID，然後對於 AMS SKMS API 參考，請參閱 AWS Artifact 主控台中的報告索引標籤。 尋找堆疊 IP 地址。

視需要存取堡壘 IP 地址 SSH 或 RDP，並使用下列其中一個程序登入。

Linux 電腦到 Linux 執行個體

使用 SSH 連接到 SSH 堡壘，然後連接到 Linux 執行個體。

MALZ

如需易記堡壘名稱的詳細資訊，請參閱 DNS 堡壘。

若要連線到 Linux 執行個體，您必須先連線到 SSH 堡壘。

1. 開啟 shell 視窗並輸入：

```
ssh Domain_FQDN\\Username@SSH_bastion_name
    or SSH_bastion_IP
```

如果您的 Domain_FQDN 是 "corp.domain.com"、您的帳號是 "123456789123"、您的 _Domain 是 "amazonaws.com"、您選擇堡壘 "4"，且您的使用者名稱是 "JoeSmith"，則看起來像這樣：

```
ssh corp.domain.com\\JoeSmith sshbastion4.A123456789123.amazonaws.com
```

2. 使用您的公司 Active Directory 登入資料登入。
3. 當出現 Bash 提示時，SSH 會傳入執行個體，然後輸入：

```
ssh Domain_FQDN\\Username@Instance_IP
```

或者，您可以使用登入旗標 (-l)：

```
ssh -l Domain_FQDN\\Username@Instance_IP
```

SALZ

如需易記堡壘名稱的詳細資訊，請參閱 DNS 堡壘。

若要連線到 Linux 執行個體，您必須先連線到 SSH 堡壘。

1. 開啟 shell 視窗並輸入：

```
ssh DOMAIN_FQDN\\USERNAME@SSH_BASTION_name
    or SSH_BASTION_IP
```

如果您的帳號是 123456789123，您可以選擇堡壘 4，而您的使用者名稱是 JoeSmith，這看起來像這樣：

```
ssh corp.domain.com\\JoeSmith sshbastion1.A123456789123.amazonaws.com
```

2. 使用您的公司 Active Directory 登入資料登入。
3. 當出現 Bash 提示時，SSH 會傳入執行個體，然後輸入：

```
ssh DOMAIN_FQDN\\USERNAME@INSTANCE_IP
```

或者，您可以使用登入旗標 (-l)：

```
ssh -l DOMAIN_FQDN\\USERNAME@INSTANCE_IP
```

Linux 電腦到 Windows 執行個體

使用 SSH 通道和 RDP 用戶端從 Linux 電腦連線至 Windows 執行個體。

MALZ

此程序需要適用於 Linux 的遠端桌面連線用戶端；此範例使用 Microsoft 遠端桌面 （連線至 Windows 遠端桌面服務的開放原始碼 UNIX 用戶端）。Rdesktop 是替代方案。

> **Note**
>
> 登入 Windows 執行個體的方式可能會根據使用的遠端桌面用戶端而變更。

首先建立 SSH 通道，然後登入。

如需易記堡壘名稱的詳細資訊，請參閱 DNS 易記堡壘名稱。

開始之前：

- 請求存取您要連線的執行個體；如需資訊，請參閱存取請求。
- 選擇要連線的易記 DNS SSH 堡壘名稱；例如：

```
sshbastion(1-4).Your_Domain
```

如果您的 Domain_FQDN 是 "corp.domain.com"、您的 AMS 受管 Your_Domain 是 "amazonaws.com"、您選擇堡壘 "4"，且您的使用者名稱是 "JoeSmith"，這看起來像這樣：

```
ssh corp.domain.com\\JoeSmith sshbastion4.amazonaws.com
```

- 尋找您要連線之執行個體的 IP 地址；如需資訊，請參閱尋找執行個體 ID 或 IP 地址。

1. 透過 SSH 通道從 Linux 桌面設定 RDP 到 Windows 執行個體。為了發出具有正確值的ssh命令，有幾種方式可以繼續：

   - 在 Linux shell 中，設定變數，然後輸入 SSH 連線命令：

   ```
   BASTION="sshbastion(1-4).Your_Domain""
   WINDOWS="Windows_Instance_Private_IP"
   AD="AD_Account_Number"
   USER="AD_Username"
   ssh -L 3389:$WINDOWS:3389 A$AD\\\\$USER@$BASTION
   ```

   範例，如果使用下列值：

   ```
   BASTION="sshbastion4.A123456789123.amazonaws.com"

   WINDOWS="172.16.3.254"
   ```

```
AD="ACORP_example"

USER="john.doe"
```

- 將變數值直接新增至ssh命令。

在任何一種情況下，這就是轉譯的請求（假設相同的變數值集）：

```
ssh -L 3389:172.16.3.254:3389 ACORP_example\\\\john.doe@myamsadomain.com
```

2. 任一種：開啟遠端桌面用戶端，輸入迴路地址和連接埠 127.0.0.1：3389，然後開啟連線。

   或者，從新的 Linux 桌面 Shell 登入 Windows 執行個體。如果您使用 RDesktop，命令如下所示：

   ```
   rdesktop 127.0.0.1:3389
   ```

   Windows 執行個體的遠端桌面視窗會顯示在您的 Linux 桌面上。

   > **Tip**
   >
   > 如果遠端桌面工作階段無法啟動，請確認步驟 1 中的連接埠 3389 允許從 SSH 堡壘連線至 Windows 執行個體 (private_ip_address_of_windows_instance正確取代）：
   >
   > ```
   > nc private_ip_address_of_windows_instance 3389 -v -z
   > ```
   >
   > 成功：
   >
   > ```
   > nc 172.16.0.83 3389 -v -z
   >        Connection to 172.16.0.83 3389 port [tcp/ms-wbt-server] succeeded
   >        netstat -anvp | grep 3389
   >        tcp    0     0 172.16.0.253:48079 172.16.3.254:3389 ESTABLISHED
   > ```

SALZ

單一帳戶登陸區域的此程序需要 Linux 的遠端桌面連線用戶端；範例使用 Microsoft 遠端桌面 （連線至 Windows 遠端桌面服務的開放原始碼 UNIX 用戶端）。Rdesktop 是替代方案。

> **Note**
>
> 登入 Windows 執行個體的方式可能會根據使用的遠端桌面用戶端而變更。

首先建立 SSH 通道，然後登入。

如需易記堡壘名稱的詳細資訊，請參閱 DNS 易記堡壘名稱。

開始之前：

- 請求存取您要連線的執行個體；如需資訊，請參閱存取請求。
- 選擇要連線的易記 DNS SSH 堡壘名稱；例如：

```
sshbastion(1-4).AAMSAccountNumber.amazonaws.com
```

如果您的帳號是 123456789123 且您選擇堡壘 4，這看起來像這樣：

```
sshbastion4.A123456789123.amazonaws.com
```

- 尋找您要連線之執行個體的 IP 地址；如需資訊，請參閱尋找執行個體 ID 或 IP 地址。

1. 透過 SSH 通道從 Linux 桌面設定 RDP 到 Windows 執行個體。為了發出具有正確值的ssh命令，有幾種方式可以繼續：

   - 在 Linux shell 中，設定變數，然後輸入 SSH 連線命令：

   ```
   BASTION="sshbastion(1-4).AAMSAccountNumber.amazonaws.com"
   WINDOWS="WINDOWS_INSTANCE_PRIVATE_IP"
   AD="AD_ACCOUNT_NUMBER"
   USER="AD_USERNAME"
   ssh -L 3389:$WINDOWS:3389 A$AD\\\\$USER@$BASTION
   ```

   範例，如果使用下列值：

```
BASTION="sshbastion4.A123456789123.amazonaws.com"

WINDOWS="172.16.3.254"

AD="ACORP_example"

USER="john.doe"
```

- 將變數值直接新增至ssh命令。

在任何一種情況下，這就是轉譯的請求（假設相同的變數值集）：

```
ssh -L 3389:172.16.3.254:3389 ACORP_example\\\
\john.doe@sshbastion4.A123456789123.amazonaws.com
```

2. 任一種：開啟遠端桌面用戶端，輸入迴路地址和連接埠 127.0.0.1：3389，然後開啟連線。

或者，從新的 Linux 桌面 Shell 登入 Windows 執行個體。如果您使用 RDesktop，命令如下所示：

```
rdesktop 127.0.0.1:3389
```

Windows 執行個體的遠端桌面視窗會顯示在您的 Linux 桌面上。

> **Tip**
>
> 如果遠端桌面工作階段無法啟動，請確認步驟 1 中的連接埠 3389 允許從 SSH 堡壘連線至 Windows 執行個體 (private_ip_address_of_windows_instance正確取代）：
>
> ```
> nc private_ip_address_of_windows_instance 3389 -v -z
> ```
>
> 成功：
>
> ```
> nc 172.16.0.83 3389 -v -z
>         Connection to 172.16.0.83 3389 port [tcp/ms-wbt-server] succeeded
>         netstat -anvp | grep 3389
>         tcp    0     0 172.16.0.253:48079 172.16.3.254:3389 ESTABLISHED
> ```

Windows 電腦到 Windows 執行個體

使用 Windows 遠端桌面連線用戶端從 Windows 電腦連線至 Windows 執行個體。

MALZ

如需易記堡壘名稱的詳細資訊，請參閱 DNS 易記堡壘名稱。

1. 開啟遠端桌面連線程式，這是標準的 Windows 程式，然後在主機名稱欄位中輸入 Windows 堡壘的易記 DNS 名稱。

2. 選擇連線。遠端桌面連線會嘗試與堡壘建立 RDP 連線。

   如果成功，會開啟登入資料對話方塊。若要取得存取權，請使用您的公司 Active Directory 登入資料，就像使用 Windows 執行個體一樣。

3. 在堡壘上開啟遠端桌面連線程式，然後輸入您要連線的 Windows 執行個體 IP 地址（例如 10.0.0.100)，然後選擇連線。連線至 Windows 執行個體之前，需要再次使用您的公司 Active Directory 登入資料。

SALZ

如需易記堡壘名稱的詳細資訊，請參閱 DNS 易記堡壘名稱。

1. 開啟遠端桌面連線程式，這是標準的 Windows 程式，並在主機名稱欄位中輸入 Windows 堡壘的易記 DNS 名稱；例如，如果您的帳戶號碼為 123456789123 且您選擇堡壘 4，`rdpbastion(1-4).AAMSAccountNumber.amazonaws.com`則 會像這樣`rdpbastion4.A123456789123.amazonaws.com`。

2. 選擇連線。遠端桌面連線會嘗試與堡壘建立 RDP 連線。

   如果成功，會開啟登入資料對話方塊。若要取得存取權，請使用您的公司 Active Directory 登入資料，就像使用 Windows 執行個體一樣。

3. 在堡壘上開啟遠端桌面連線程式，然後輸入您要連線的 Windows 執行個體 IP 地址（例如 10.0.0.100)，然後選擇連線。連線至 Windows 執行個體之前，需要再次使用您的公司 Active Directory 登入資料。

Windows 電腦到 Linux 執行個體

若要從 Windows 環境 RDP 到 SSH 堡壘，請遵循下列步驟。

MALZ

開始之前：

- 請求存取您要連線的執行個體；如需資訊，請參閱存取請求。
- 選擇要連線的易記 DNS SSH 堡壘名稱；例如：

```
sshbastion(1-4).YOUR_DOMAIN
```

如果 YOUR_DOMAIN 是 myamsaddomain.com：//" 且您選擇堡壘 4：

```
sshbastion4.myamsaddomain.com
```

- 尋找您要連線之執行個體的 IP 地址；如需資訊，請參閱尋找執行個體 ID 或 IP 地址。

若要從 Windows 機器連線至 Linux 執行個體，您必須先連線至 SSH 堡壘。

使用原生 Windows OpenSSH 用戶端，或在本機電腦上安裝 PuTTY。若要進一步了解 OpenSSH，請參閱 Windows 中的 OpenSSH。

1. 使用原生 Windows 或開啟 PuTTY，然後輸入 SSH 堡壘主機名稱或 SSH 堡壘的 IP 地址。例如，10.65.2.214 (22 是用於 SSH 的連接埠，預設為)。
2. OpenSSH 或 PuTTY 會嘗試 SSH 連線到堡壘，並開啟 shell 視窗。
3. 像使用 RDP 主機一樣使用您的公司 Active Directory 登入資料來取得存取權。
4. 當出現 Bash 提示時，SSH 會進入執行個體。輸入：

```
ssh DOMAIN_FQDN\USERNAME@INSTANCE_IP
```

SALZ

開始之前：

- 請求存取您要連線的執行個體；如需資訊，請參閱存取請求。
- 選擇要連線的易記 DNS SSH 堡壘名稱；例如：

```
sshbastion(1-4).AAMSAccountNumber.amazonaws.com
```

如果您的帳號是 123456789123，而且您選擇堡壘 4，這看起來像這樣：

```
sshbastion4.A123456789123.amazonaws.com
```

- 尋找您要連線之執行個體的 IP 地址；如需資訊，請參閱尋找執行個體 ID 或 IP 地址。

若要從 Windows 機器連線至 Linux 執行個體，您必須先連線至 SSH 堡壘。

使用原生 Windows OpenSSH 用戶端，或在本機電腦上安裝 PuTTY。若要進一步了解 OpenSSH，請參閱 Windows 中的 OpenSSH。

1. 使用原生 Windows 或開啟 PuTTY，然後輸入 SSH 堡壘主機名稱或 SSH 堡壘的 IP 地址。例如，10.65.2.214 (22 是用於 SSH 的連接埠，預設為)。
2. OpenSSH 或 PuTTY 會嘗試 SSH 連線到堡壘，並開啟 shell 視窗。
3. 像使用 RDP 主機一樣使用您的公司 Active Directory 登入資料來取得存取權。
4. 當出現 Bash 提示時，SSH 會進入執行個體。輸入：

```
ssh DOMAIN_FQDN\USERNAME@INSTANCE_IP
```

報告事件

使用 AMS 主控台報告事件。請務必為每個新問題建立新的事件。開啟與舊查詢相關的案例時，包含相關的案例編號會很有幫助，以便我們可以參考先前的通訊。

> **Note**
> 如果案例通訊偏離原始問題，AMS 運算子可能會要求您報告新的事件。

若要使用 AMS 主控台報告事件：

1. 從左側導覽中，選擇事件

事件清單隨即開啟：

如果您的事件清單是空的，清除篩選條件選項會將篩選條件重設為任何狀態。

如果您知道要使用電話或聊天，請按一下支援中心中的建立事件，以在支援中心主控台中開啟事件建立頁面，自動填入 AMS 服務類型。

> **Important**
>
> - 支援 系統會記錄使用 起始的通話，以改善回應。如果通話中斷，您必須透過支援中心案例回撥， AWS 沒有機制可以回撥給您。
> - 電話和聊天支援旨在協助處理支援案例、事件和服務請求，而不是 RFC 或安全問題。
> - 對於 RFC 問題，請使用相關 RFC 詳細資訊頁面上的通訊選項來聯絡 AMS 工程師。
> - 針對安全問題，請建立高優先順序 (P1 或 P2) 支援案例。即時聊天功能不適用於安全事件。

2. 如果您想要尋找現有的事件，請在下拉式清單中選取事件狀態篩選條件。

	• 所有尚未解決的事件。 • 尚未指派的新事件。 • 已指派的事件。 • 您重新開啟的事件。 • 指派的複雜事件。 • 在下一個步驟之前需要您的意見回饋的事件。 • 您最近提交資訊的事件。 • 已結束的事件。 • 帳戶中的所有事件。

3. 選擇建立。

建立事件頁面隨即開啟：

4. 選取優先順序：

   - 低：與 AWS/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/AMS 資源相關的商業服務或應用程式會受到中度影響，並在降級狀態下運作。
   - 高：您的業務會受到重大影響。與 AWS/AMS 資源相關的應用程式關鍵函數無法使用。預留給影響生產系統的最重要中斷。

5. 選取類別。

   > **Note**
   >
   > 如果您要測試事件功能，請將無動作旗標 (AMSTestNoOpsActionRequired) 新增至您的事件標題。

6. 輸入以下資訊：

   - 主旨：事件報告的描述性標題。
   - CC 電子郵件：您想要通知有關事件報告和解決方案的人員的電子郵件地址清單。
   - 詳細資訊：事件的完整描述、受影響的系統，以及解決方案的預期結果。回答預先設定的問題，或刪除它們並輸入任何相關資訊。

   若要新增附件，請選擇新增附件，瀏覽至您想要的附件，然後
   按一下開啟。若要刪除附件，請按一下刪除圖
   示：

   。

7. 選擇提交。

   系統會開啟詳細資訊頁面，其中包含事件的相關資訊，例如類型、主旨、已建立、ID 和狀態，以及包含您所建立請求描述的通訊區域。

   按一下回覆以開啟通訊區域，並提供其他詳細資訊或狀態更新。

   事件解決後，請按一下關閉案例。

   如果通訊數量超過一頁的數量，請按一下載入更多。

   請不要忘記為通訊評分！

您的事件會顯示在事件清單頁面上。

建立服務請求

若要使用 AWS Managed Services (AMS) 主控台建立服務請求：

1. 從左側導覽中，選擇服務請求。

   服務請求清單隨即開啟。

   如果您的服務請求清單是空的，清除篩選條件選項會將篩選條件重設為任何狀態。

   如果您知道要使用電話或聊天，請按一下支援中心中的建立服務請求，以在支援中心主控台中開啟服務請求建立頁面，自動填入 AMS 服務類型。

   > **Note**
   >
   > 系統會記錄使用 支援 中心起始的通話，以改善回應。如果通話中斷，您必須透過支援中心案例回撥， AWS 沒有機制可以回撥給您。

   > **Important**
   >
   > 電話和聊天支援旨在協助處理支援案例、事件和服務請求。對於 RFC 問題，請使用相關 RFC 詳細資訊頁面上的通訊選項來聯絡 AMS 工程師。

2. 如果您想要尋找現有的服務請求，請在下拉式清單中選取服務請求狀態篩選條件。

	• 所有尚未解決的服務請求。 • 尚未指派的新服務請求。 • 已指派的服務請求。 • 您已重新開啟的服務請求。 • 已指派、複雜的服務請求。

- 在下一個步驟之前需要您的意見回饋的服務請求。
- 您最近提交資訊的服務請求。
- 已結束的服務請求。
- 帳戶中的所有服務請求。

3. 選擇建立。

   建立服務請求頁面隨即開啟。

4. 選取類別。

   > **Note**
   >
   > 如果您要測試服務請求功能，請將無動作旗標 `AMSTestNoOpsActionRequired`. 新增至您的服務請求標題。

5. 輸入以下資訊：

   - 主旨：這會建立清單頁面上服務請求詳細資訊的連結。
   - CC 電子郵件：除了您的預設電子郵件聯絡人之外，這些電子郵件也會收到通訊。
   - 詳細資訊：在此盡可能多提供資訊。

   若要新增附件，請選擇新增附件，瀏覽至您想要的附件，然後
   按一下開啟。若要刪除附件，請按一下刪除圖
   示：

   。

6. 選擇提交。

   詳細資訊頁面隨即開啟，其中包含服務請求的相關資訊，例如類型、主旨、已建立、ID 和狀態，以及包含您建立之請求描述的通訊區域。

   此外，您的服務請求會顯示在服務請求清單頁面上。當您有提醒但尚未收到 AMS 的通知時，請使用此選項。

   按一下回覆以開啟通訊區域，並提供其他詳細資訊或狀態更新。

當服務請求已解決時，請按一下解決案例。

按一下載入更多以檢視不符合初始頁面的其他通訊。

請不要忘記為通訊評分！

對於帳單相關查詢，請使用 AMS 主控台中的其他類別；AMS CM API `ChangeTypeId` `ct-1e1xtak34nx76`中的 ，或 AWS Support API `IssueType=AMS`中的 。

加入後步驟

現在您已加入 AMS 帳戶，您需要閱讀更多 AMS 文件。請參閱這些文件：

- 接下來，使用 HA 兩層堆疊 CT 建立全功能 WordPress 堆疊的教學課程會提供完整的 AMS 體驗。
- AMS 使用者指南：AMS 使用者指南說明 AMS 功能、列出關鍵術語、操作、界面，並提供典型 AMS 受管基礎設施架構的概觀。此外，也會提供存取管理詳細資訊和 AMS 預設值。也提供如何使用 AMS 變更管理系統的詳細說明，並提供數個演練。也會說明其他管理概念。
- AMS API 參考：此 API 參考提供所有 API 呼叫的說明，包括請求、回應和範例。
- AMS 應用程式指南：AMS 應用程式指南說明在 AMS 中部署和維護應用程式的不同選項和方法。

教學課程

下列教學課程詳細說明使用 CLI 和主控台，使用高可用性 （進階） CT (ct-06mjngx5flwto) 建立雙層堆疊的步驟。提供部署 Linux Auto Scaling 群組 (ASG) 和部署 Windows ASG 的教學課程。

您可以在 AMS 變更類型參考中找到所有 CT 選項的描述，包括 ChangeTypeId。

CLI 教學課程：高可用性兩層堆疊 (Linux/RHEL)

本節說明如何使用 AMS CLI 將高可用性 (HA) 雙層堆疊部署至 AMS 環境。

> **Note**
>
> 此部署演練已在 AMZN Linux 和 RHEL 環境中進行測試。

任務和所需 RFCs的摘要：

1. 建立基礎設施 (HA 雙層堆疊）
2. 為 CodeDeploy 應用程式建立 S3 儲存貯體
3. 建立 WordPress 應用程式套件並將其上傳至 S3 儲存貯體
4. 使用 CodeDeploy 部署應用程式
5. 存取 WordPress 網站並登入以驗證部署

開始之前

部署 | 進階堆疊元件 | 高可用性 兩層堆疊進階 | 建立 CT 會建立 Auto Scaling 群組、負載平衡器、資料庫，以及 CodeDeploy 應用程式名稱和部署群組 （與您提供應用程式的名稱相同）。如需 CodeDeploy 的資訊，請參閱什麼是 CodeDeploy？

本演練使用包含 UserData 的高可用性兩層堆疊 （進階） RFC，並說明如何建立 CodeDeploy 可以部署的 WordPress 套件。

範例中`UserData`顯示的 透過查詢位於 https：//http://169.254.169.254/latest/meta-data/ 的 EC2 執行個體中繼資料服務，從執行中的執行個體中取得執行個體 ID、區域等執行個體中繼資料。使用者資料指令碼中的此行：`REGION=$(curl 169.254.169.254/latest/meta-data/placement/availability-zone/ | sed 's/[a-z]$//')`，會將中繼資料服務的可用區域名稱擷取到支援區域的 $REGION 變數，並使用它來完成下載 CodeDeploy 代理程式的 S3 儲存貯體 URL。169.254.169.254 IP 只能在 VPC 內路由 （所有 VPCs都可以查詢服務）。如需 服務的資訊，請參閱執行個體中繼資料和使用者資料。另請注意，輸入為 UserData 的指令碼會以「根」使用者身分執行，不需要使用「sudo」命令。

此演練會將下列參數保留為預設值 （顯示）：

- Auto Scaling 群組：`Cooldown=300, DesiredCapacity=2, EBSOptimized=false, HealthCheckGracePeriod=600, IAMInstanceProfile=customer-mc-ec2-instance-profile, InstanceDetailedMonitoring=true, InstanceRootVolumeIops=0, InstanceRootVolumeType=standard, InstanceType=m3.medium, MaxInstances=2, MinInstances=2, ScaleDownPolicyCooldown=300, ScaleDownPolicyEvaluationPeriods=4, ScaleDownPolicyPeriod=60, ScaleDownPolicyScalingAdjustment=-1, ScaleDownPolicyStatistic=Average, ScaleDownPolicyThreshold=35, ScaleMetricName=CPUUtilization, ScaleUpPolicyCooldown=60, ScaleUpPolicyEvaluationPeriods=2, ScaleUpPolicyPeriod=60, ScaleUpPolicyScalingAdjustment=2, ScaleUpPolicyStatistic=Average, ScaleUpPolicyThreshold=75`。

- Load Balancer：`HealthCheckInterval=30, HealthCheckTimeout=5`。
- 資料庫：`BackupRetentionPeriod=7, Backups=true, InstanceType=db.m3.medium, IOPS=0, MultiAZ=true, PreferredBackupWindow=22:00-23:00, PreferredMaintenanceWindow=wed:03:32-wed:04:02, StorageEncrypted=false, StorageEncryptionKey="", StorageType=gp2`。
- 應用程式：`DeploymentConfigName=CodeDeployDefault.OneAtATime`。
- S3 儲存貯體：`AccessControl=Private`。

其他設定：

`RequestedStartTime` `RequestedEndTime` 如果您想要排程 RFC：您可以使用 Time.is 來判斷正確的 UTC 時間。所提供的範例必須適當調整。如果已超過開始時間，RFC 將無法繼續。或者，您可以將這些值保留為關閉，以建立 ASAP RFC，在通過核准後立即執行。

> **Note**
>
> 您可以選擇以不同於所示的方式設定許多參數。範例中顯示的參數值已經過測試，但可能不適合您。

建立基礎設施

在開始之前收集下列資料，可讓部署更快進行。

必要資料 HA 堆疊：

- AutoScalingGroup：
  - `UserData`：此值在本教學課程中提供。它包含用於設定 CodeDeploy 資源並啟動 CodeDeploy 代理程式的命令。
  - `AMI-ID`：此值決定 Auto Scaling 群組 (ASG) 將啟動的 EC2 執行個體類型。請務必在您帳戶中選取以「customer-」開頭的 AMI，且為您想要的作業系統。使用 尋找 AMI IDs 如需 AMS SKMS API 參考，請參閱 AWS 成品主控台中的報告索引標籤。 操作 (CLI：list-amis) 或 AMS 主控台 VPCs VPCs 詳細資訊頁面。此逐步解說適用於設定為使用 Linux AMI 的 ASGs。
- 資料庫：
  - 這些參數 `DBEngine`、 和 `LicenseModel`應根據您的情況設定`EngineVersion`，但範例中顯示的值已經過測試。

  - 部署應用程式套件時，MasterUserPassword需要這些參數、MasterUsername、、RDSSubnetIds DBName和 。對於 RDSSubnetIds請使用兩個私有子網路。
- LoadBalancer：
  - 這些參數 DBEngine、 和 LicenseModel應根據您的情況設定EngineVersion，但範例中顯示的值已經過測試。
  - ELBSubnetIds：使用兩個公有子網路。
- 應用程式： ApplicationName值會設定 CodeDeploy 應用程式名稱和 CodeDeploy 部署群組名稱。您可以使用它來部署應用程式。它在帳戶中必須是唯一的。若要檢查您的帳戶是否有 CodeDeploy 名稱，請參閱 CodeDeploy 主控台。此範例使用「WordPress」，但如果您將使用該值，請確定該值尚未使用。

此程序使用高可用性雙層堆疊（進階） CT (ct-06mjngx5flwto) 和建立 S3 儲存 CT (ct-1a68ck03fn98r)。從您的已驗證帳戶中，遵循命令列的這些步驟。

1. 啟動基礎設施堆疊。

   a. 將 HA 兩層堆疊 CT 的執行參數 JSON 結構描述輸出到名為 CreateStackParams.json.

```
aws amscm get-change-type-version --change-type-id "ct-06mjngx5flwto"
 --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
 CreateStackParams.json
```

   b. 修改結構描述。視需要取代*##*。例如，針對 ASG 將建立的 EC2 執行個體，使用您想要的作業系統。將 記錄ApplicationName為稍後用來部署應用程式的方式。請注意，您最多可以新增 50 個標籤。

```
{
"Description":      "HA two tier stack for WordPress",
"Name":             "WordPressStack",
"TimeoutInMinutes":  360,
"Tags": [
        {
            "Key": "ApplicationName",
            "Value": "WordPress"
        }
    ],
"AutoScalingGroup": {
            "AmiId":    "AMI-ID",
            "UserData": "#!/bin/bash \n
```

```
            REGION=$(curl 169.254.169.254/latest/meta-data/placement/
availability-zone/ | sed 's/[a-z]$//') \n
            yum -y install ruby httpd \n
            chkconfig httpd on \n
            service httpd start \n
            touch /var/www/html/status \n
            cd /tmp \n
            curl -O https://aws-codedeploy-$REGION.s3.amazonaws.com/latest/
install \n
            chmod +x ./install \n
            ./install auto \n
            chkconfig codedeploy-agent on \n
            service codedeploy-agent start"
    },
    "LoadBalancer": {
        "Public":               true,
        "HealthCheckTarget":    "HTTP:80/status"
    },
    "Database":     {
        "DBEngine":             "MySQL",
        "DBName":               "wordpress",
        "EngineVersion":        "8.0.16 ",
        "LicenseModel":         "general-public-license",
        "MasterUsername":       "admin",
        "MasterUserPassword":   "p4ssw0rd"
    },
    "Application":  {
    "ApplicationName":  "WordPress"
        }
}
```

c. 將 CreateRfc JSON 範本輸出到目前資料夾中名為 CreateStackRfc.json:

```
aws amscm create-rfc --generate-cli-skeleton > CreateStackRfc.json
```

d. 如下所示修改並儲存 RFC 範本，您可以刪除和取代內容。請注意，RequestedStartTime和 現在RequestedEndTime是選用的；排除它們會建立 ASAP RFC，在核准後立即執行（通常會自動執行）。若要提交排定的 RFC，請新增這些值。

```
{
"ChangeTypeVersion":    "3.0",
"ChangeTypeId":         "ct-06mjngx5flwto",
"Title":                "HA-Stack-For-WP-RFC"
```

```
}
```

e. 建立 RFC，指定 CreateStackRfc.json 檔案和 CreateStackParams.json 執行參數檔案：

```
aws amscm create-rfc --cli-input-json file://CreateStackRfc.json --execution-
parameters file://CreateStackParams.json
```

您會在回應中收到 RFC ID。儲存後續步驟的 ID。

f. 提交 RFC：

```
aws amscm submit-rfc --rfc-id  RFC_ID
```

如果 RFC 成功，您不會收到任何輸出。

g. 若要檢查 RFC 狀態，請執行

```
aws amscm get-rfc --rfc-id RFC_ID
```

請記下 RFC ID。

2. 啟動 S3 儲存貯體

在開始之前收集下列資料，可讓部署更快進行。

必要資料 S3 儲存貯體：

- VPC-ID：此值會決定 S3 儲存貯體的位置。使用您先前使用的相同 VPC ID。
- BucketName：此值會設定 S3 儲存貯體名稱，您可以使用它來上傳應用程式套件。它在帳戶區域必須是唯一的，且不能包含大寫字母。將您的帳戶 ID 包含在 BucketName 中不是必要項目，但之後更容易識別儲存貯體。若要查看帳戶中存在哪些 S3 儲存貯體名稱，請前往您帳戶的 Amazon S3 主控台。

a. 將 S3 儲存體的 JSON 結構描述輸出至名為 CreateS3StoreParams.json.

```
aws amscm get-change-type-version --change-type-id "ct-1a68ck03fn98r"
 --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
 CreateS3StoreParams.json
```

b. 修改結構描述，如下所示，您可以刪除和取代內容。適當地取代 *VPC_ID*。範例中的值已經過測試，但可能不適合您。

> **Tip**
>
> 在整個 帳戶區域BucketName必須是唯一的，且不能包含大寫字母。將您的帳戶 ID 包含在 BucketName 中不是必要項目，但之後更容易識別儲存貯體。若要查看帳戶中存在哪些 S3 儲存貯體名稱，請前往您帳戶的 Amazon S3 主控台。

```
{
"Description":      "S3BucketForWordPressBundle",
"VpcId":            "VPC_ID",
"StackTemplateId":  "stm-s2b72beb000000000",
"Name":             "S3BucketForWP",
"TimeoutInMinutes":  60,
"Parameters":   {
    "AccessControl":    "Private",
    "BucketName":       "ACCOUNT_ID-BUCKET_NAME"
    }
}
```

c. 將 CreateRfc 的 JSON 範本輸出至目前資料夾中名為 CreateS3StoreRfc.json:

```
aws amscm create-rfc --generate-cli-skeleton > CreateS3StoreRfc.json
```

d. 修改並儲存 CreateS3StoreRfc.json 檔案，您可以刪除並取代內容。請注意，RequestedStartTime和 現在RequestedEndTime是選用的；排除它們會建立 ASAP RFC，在核准後立即執行 （通常會自動執行）。若要提交排定的 RFC，請新增這些值。

```
{
"ChangeTypeVersion":    "1.0",
"ChangeTypeId":         "ct-1a68ck03fn98r",
"Title":                "S3-Stack-For-WP-RFC"
}
```

e. 建立 RFC，指定 CreateS3StoreRfc.json 檔案和 CreateS3StoreParams.json 執行參數檔案：

```
aws amscm create-rfc --cli-input-json file://CreateS3StoreRfc.json  --
execution-parameters file://CreateS3StoreParams.json
```

您會在回應中收到新 RFC 的 RfcId。儲存後續步驟的 ID。

f. 提交 RFC：

```
aws amscm submit-rfc --rfc-id RFC_ID
```

如果 RFC 成功，您不會收到任何輸出。

g. 若要檢查 RFC 狀態，請執行

```
aws amscm get-rfc --rfc-id RFC_ID
```

建立、上傳和部署應用程式

首先，建立 WordPress 應用程式套件，然後使用 CodeDeploy CTs 來建立和部署應用程式。

1. 下載 WordPress、解壓縮檔案並建立 ./scripts 目錄。

   Linux 命令：

   ```
   wget https://github.com/WordPress/WordPress/archive/master.zip
   ```

   Windows：貼`https://github.com/WordPress/WordPress/archive/master.zip`入瀏覽器視窗並下載 zip 檔案。

   建立要在其中組合套件的暫時目錄。

   Linux：

   ```
   mkdir /tmp/WordPress
   ```

   Windows：建立「WordPress」目錄，稍後您將使用目錄路徑。

2. 將 WordPress 來源解壓縮至「WordPress」目錄，並建立 ./scripts 目錄。

   Linux：

   ```
   unzip master.zip -d /tmp/WordPress_Temp
   cp -paf /tmp/WordPress_Temp/WordPress-master/* /tmp/WordPress
   rm -rf /tmp/WordPress_Temp
   ```

```
rm -f master
cd /tmp/WordPress
mkdir scripts
```

Windows：前往您建立的「WordPress」目錄，並在該處建立「scripts」目錄。

如果您在 Windows 環境中，請務必將指令碼檔案的中斷類型設定為 Unix (LF)。在記事本 ++ 中，這是視窗右下角的選項。

3. 在 WordPress 目錄中建立 CodeDeploy apppec.yml 檔案（如果複製範例，請檢查縮排，每個空格都會計算）。重要：確保「來源」路徑正確，可將 WordPress 檔案（在本例中為 WordPress 目錄中）複製到預期的目的地 (/var/www/html/WordPress)。在此範例中，appapppec.yml 檔案位於具有 WordPress 檔案的 目錄中，因此只需要 "/"。此外，即使您為 Auto Scaling 群組使用 RHEL AMI，也請保持原狀。Apppec.yml 檔案範例：

```
version: 0.0
os: linux
files:
  - source: /
    destination: /var/www/html/WordPress
hooks:
  BeforeInstall:
    - location: scripts/install_dependencies.sh
      timeout: 300
      runas: root
  AfterInstall:
    - location: scripts/config_wordpress.sh
      timeout: 300
      runas: root
  ApplicationStart:
    - location: scripts/start_server.sh
      timeout: 300
      runas: root
  ApplicationStop:
    - location: scripts/stop_server.sh
      timeout: 300
      runas: root
```

4. 在 WordPress ./scripts 目錄中建立 bash 檔案指令碼。

首先，`config_wordpress.sh`使用下列內容建立（如果您願意，可以直接編輯 wp-config.php 檔案）。

> **Note**
>
> 將 *DBName* 取代為 HA 堆疊 RFC 中指定的值 （例如 wordpress)。
> 將 *DB_MasterUsername* 取代為 HA 堆疊 RFC 中指定的MasterUsername值 （例如 admin)。
> 將 *DB_MasterUserPassword* 取代為 HA 堆疊 RFC 中指定的MasterUserPassword值 （例如 p4ssw0rd)。
> 在 HA Stack RFC 的執行輸出中，將 *DB_ENDPOINT* 取代為端點 DNS 名稱 （例如 srt1cz23n45sfg.clgvd67uvydk.us-east-1.rds.amazonaws.com)。您可以使用 GetRfc 操作 (CLI：get-rfc --rfc-id RFC_ID) 或在先前提交的 HA Stack RFC 的 AMS 主控台 RFC 詳細資訊頁面中找到此項目。

```
#!/bin/bash
chmod -R 755 /var/www/html/WordPress
cp /var/www/html/WordPress/wp-config-sample.php /var/www/html/WordPress/wp-
config.php
cd /var/www/html/WordPress
sed -i "s/database_name_here/DBName/g" wp-config.php
sed -i "s/username_here/DB_MasterUsername/g" wp-config.php
sed -i "s/password_here/DB_MasterUserPassword/g" wp-config.php
sed -i "s/localhost/DB_ENDPOINT/g" wp-config.php
```

5. 在相同的目錄中install_dependencies.sh，使用下列內容建立 ：

```
#!/bin/bash
yum install -y php
yum install -y php-mysql
yum install -y mysql
service httpd restart
```

> **Note**
>
> HTTPS 會在啟動時安裝為使用者資料的一部分，以允許運作狀態檢查從頭開始。

6. 在相同的目錄中start_server.sh，使用下列內容建立 ：

   - 對於 Amazon Linux 執行個體，請使用：

```
#!/bin/bash
service httpd start
```

- 對於 RHEL 執行個體，請使用此（額外的命令是允許 SELINUX 接受 WordPress 的政策）：

```
#!/bin/bash
setsebool -P  httpd_can_network_connect_db 1
setsebool -P  httpd_can_network_connect 1
chcon -t httpd_sys_rw_content_t /var/www/html/WordPress/wp-content -R
restorecon -Rv /var/www/html
service httpd start
```

7. 在相同的目錄中stop_server.sh，使用下列內容建立 ：

```
#!/bin/bash
service httpd stop
```

8. 建立 zip 套件。

   Linux：

```
$ cd /tmp/WordPress
$ zip -r wordpress.zip .
```

   Windows：前往您的「WordPress」目錄，選取所有檔案並建立 zip 檔案，請務必將其命名為 wordpress.zip。

1. 將應用程式套件上傳至 S3 儲存貯體。

   套件必須就位，才能繼續部署堆疊。

   您會自動存取您建立的任何 S3 儲存貯體執行個體。您可以透過堡壘或透過 S3 主控台存取，並使用drag-and-drop或瀏覽上傳 WordPress 套件至 ，然後選取 zip 檔案。

   您也可以在 shell 視窗中使用下列命令；請確定您擁有 zip 檔案的正確路徑：

```
aws s3 cp wordpress.zip s3://BUCKET_NAME/
```

2. 部署 WordPress 應用程式套件。

在開始之前收集下列資料，可讓部署更快進行。

必要資料：

- VPC-ID：此值會決定 S3 儲存貯體的位置。使用您先前使用的相同 VPC ID。
- CodeDeployApplicationName 和 CodeDeployApplicationName：您在 HA 2-Tier堆疊 RFC 中使用的ApplicationName值會設定 CodeDeployApplicationName 和 CodeDeployDeploymentGroupName。此範例使用「WordPress」，但您可能已使用不同的值。
- S3Location：對於 S3Bucket，請使用您先前建立BucketName的 。S3BundleType 和 S3Key來自您放在 S3 存放區上的套件。

a. 輸出 CodeDeploy 應用程式的執行參數 JSON 結構描述，將 CT 部署到名為 DeployCDAppParams.json.

```
aws amscm get-change-type-version --change-type-id "ct-2edc3sd1sqmrb"
 --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
 DeployCDAppParams.json
```

b. 如下所示修改結構描述並將其儲存為 ，您可以刪除並取代內容。

```
{
"Description":                          "DeployWPCDApp",
"VpcId":                                "VPC_ID",
"Name":                                 "WordPressCDAppDeploy",
"TimeoutInMinutes":                     60,
"Parameters":   {
    "CodeDeployApplicationName":                "WordPress",
    "CodeDeployDeploymentGroupName":            "WordPress",
    "CodeDeployIgnoreApplicationStopFailures":   false,
    "CodeDeployRevision": {
      "RevisionType": "S3",
      "S3Location": {
        "S3Bucket":     "BUCKET_NAME",
        "S3BundleType": "zip",
        "S3Key":        "wordpress.zip" }
        }
    }
}
```

c. 將 CreateRfc 的 JSON 範本輸出至目前資料夾中名為 DeployCDAppRfc.json:

```
aws amscm create-rfc --generate-cli-skeleton > DeployCDAppRfc.json
```

d. 修改並儲存 DeployCDAppRfc.json 檔案，您可以刪除和取代內容。請注意，RequestedStartTime和 現在RequestedEndTime是選用的；排除它們會建立 ASAP RFC，在核准後立即執行 （通常會自動執行）。若要提交排定的 RFC，請新增這些值。

```
{
"ChangeTypeVersion":    "1.0",
"ChangeTypeId":         "ct-2edc3sd1sqmrb",
"Title":                "CD-Deploy-For-WP-RFC"
}
```

e. 建立 RFC，指定 DeployCDAppRfc 檔案和 DeployCDAppParams 執行參數檔案：

```
aws amscm create-rfc --cli-input-json file://DeployCDAppRfc.json  --execution-
parameters file://DeployCDAppParams.json
```

您會在回應中收到新 RFC 的 RfcId。儲存後續步驟的 ID。

f. 提交 RFC：

```
aws amscm submit-rfc --rfc-id RFC_ID
```

如果 RFC 成功，您不會收到任何輸出。

g. 若要檢查 RFC 狀態，請執行

```
aws amscm get-rfc --rfc-id RFC_ID
```

驗證應用程式部署

導覽至先前建立負載平衡器的端點 (ELB CName)，並使用 WordPress 部署的路徑：/WordPress。例如：

```
http://stack-ID-FOR-ELB.us-east-1.elb.amazonaws.com/WordPress
```

向下傾斜應用程式部署

完成教學課程後，您會想要拆解部署，才不會向您收取資源的費用。

以下是一般堆疊刪除操作。您會想要提交兩次，一次用於 HA 2-Tier堆疊，一次用於 S3 儲存貯體堆疊。作為最後的後續操作，請提交服務請求，以刪除 S3 儲存貯體的所有快照（包括服務請求中的 S3 儲存貯體堆疊 ID)。它們會在 10 天後自動刪除，但提早刪除會節省一些成本。

此逐步解說提供使用 AMS 主控台刪除 S3 堆疊的範例；此程序適用於使用 AMS 主控台刪除任何堆疊。

> **Note**
>
> 如果刪除 S3 儲存貯體，必須先清空物件。

必要資料：

- `StackId`：要使用的堆疊。您可以查看 AMS 主控台堆疊頁面，透過左側導覽中的連結取得。使用 AMS SKMS API/CLI，執行 AMS SKMS API 參考，請參閱 AWS Artifact Console. 操作中的報告索引標籤 (`list-stack-summaries` CLI 中的)。
- 此演練的變更類型 ID 為 `ct-0q0bic0ywqk6c`，版本為 "1.0"，若要了解最新版本，請執行此命令：

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=ct-0q0bic0ywqk6c
```

內嵌建立：

- 使用內嵌提供的執行參數發出建立 RFC 命令（在內嵌提供執行參數時逸出引號）。E

```
aws amscm create-rfc --change-type-id "ct-0q0bic0ywqk6c" --change-type-version "1.0"
 --title "Delete My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

- 使用建立 RFC 操作中傳回的 RFC ID 提交 RFC。在提交之前，RFC 會保持 `Editing` 狀態，且不會採取任何動作。

```
aws amscm submit-rfc --rfc-id RFC_ID
```

- 監控 RFC 狀態並檢視執行輸出：

```
aws amscm get-rfc --rfc-id RFC_ID
```

範本建立：

1. 將 RFC 範本輸出到目前資料夾中的檔案；範例將其命名為 DeleteStackRfc.json:

   ```
   aws amscm create-rfc --generate-cli-skeleton > DeleteStackRfc.json
   ```

2. 修改並儲存 DeleteStackRfc.json 檔案。由於刪除堆疊只有一個執行參數，因此執行參數可以位於 DeleteStackRfc.json 檔案本身（不需要使用執行參數建立單獨的 JSON 檔案）。

   ExecutionParameters JSON 延伸中的內部引號必須以反斜線 (\) 逸出。沒有開始和結束時間的範例：

   ```
   {
   "ChangeTypeVersion":    "1.0",
   "ChangeTypeId":         "ct-0q0bic0ywqk6c",
   "Title":                "Delete-My-Stack-RFC"
   "ExecutionParameters":  "{
           \"StackId\":\"STACK_ID\"}"
   }
   ```

3. 建立 RFC：

   ```
   aws amscm create-rfc --cli-input-json file://DeleteStackRfc.json
   ```

   您會在回應中收到新 RFC 的 RfcId。例如：

   ```
   {
   "RfcId": "daaa1867-ffc5-1473-192a-842f6b326102"
   }
   ```

   儲存後續步驟的 ID。

4. 提交 RFC：

   ```
   aws amscm submit-rfc --rfc-id RFC_ID
   ```

   如果 RFC 成功，您在命令列不會收到確認。

5. 若要監控請求的狀態和檢視執行輸出：

```
aws amscm get-rfc --rfc-id RFC_ID --query "Rfc.
{Status:Status.Name,Exec:ExecutionOutput}" --output table
```

主控台教學課程：高可用性兩層堆疊 (Linux/RHEL)

本節說明如何使用 AMS 主控台將高可用性 (HA) WordPress 網站部署至 AMS 環境。

> **Note**
>
> 此部署演練已在 AMZN Linux 和 RHEL 環境中進行測試。

任務和必要 RFCs的摘要：

1. 建立基礎設施 (HA 雙層堆疊)
2. 為 CodeDeploy 應用程式建立 S3 儲存貯體
3. 建立 WordPress 應用程式套件並將其上傳至 S3 儲存貯體
4. 使用 CodeDeploy 部署應用程式
5. 存取 WordPress 網站並登入以驗證部署
6. 向下拉動部署

您可以在 AMS 變更類型參考中找到所有 CT 選項的描述，包括 ChangeTypeId。

開始之前

部署 | 進階堆疊元件 | 高可用性兩層堆疊 | 建立 CT 會建立 Auto Scaling 群組、負載平衡器、資料庫，以及 CodeDeploy 應用程式名稱和部署群組 （具有您提供應用程式相同的名稱）。如需 CodeDeploy 的資訊，請參閱什麼是 CodeDeploy？

本演練使用高可用性兩層堆疊 RFC，其中包含`UserData`並同時說明如何建立 CodeDeploy 可以部署的 WordPress 套件。

範例中`UserData`顯示的 透過查詢位於 https：//http://169.254.169.254/latest/meta-data/ 的 EC2 執行個體中繼資料服務，從執行中的執行個體中取得執行個體 ID、區域等執行個體中繼資料。使用者資料指令碼中的此行：`REGION=$(curl 169.254.169.254/latest/meta-data/placement/availability-zone/ | sed 's/[a-z]$//')`，會將中繼資料服務的可用區域

名稱擷取到支援區域的 $REGION 變數，並使用它來完成下載 CodeDeploy 代理程式的 S3 儲存貯體 URL。169.254.169.254 IP 只能在 VPC 內路由（所有 VPCs都可以查詢服務）。如需 服務的資訊，請參閱執行個體中繼資料和使用者資料。另請注意，輸入為 UserData 的指令碼會以「根」使用者身分執行，不需要使用「sudo」命令。

此演練會將下列參數保留為預設值（顯示）：

- Auto Scaling 群組：`Cooldown=300, DesiredCapacity=2, EBSOptimized=false, HealthCheckGracePeriod=600, IAMInstanceProfile=customer-mc-ec2-instance-profile, InstanceDetailedMonitoring=true, InstanceRootVolumeIops=0, InstanceRootVolumeType=standard, InstanceType=m3.medium, MaxInstances=2, MinInstances=2, ScaleDownPolicyCooldown=300, ScaleDownPolicyEvaluationPeriods=4, ScaleDownPolicyPeriod=60, ScaleDownPolicyScalingAdjustment=-1, ScaleDownPolicyStatistic=Average, ScaleDownPolicyThreshold=35, ScaleMetricName=CPUUtilization, ScaleUpPolicyCooldown=60, ScaleUpPolicyEvaluationPeriods=2, ScaleUpPolicyPeriod=60, ScaleUpPolicyScalingAdjustment=2, ScaleUpPolicyStatistic=Average, ScaleUpPolicyThreshold=75`。
- Load Balancer：`HealthCheckInterval=30, HealthCheckTimeout=5`。
- 資料庫：`BackupRetentionPeriod=7, Backups=true, InstanceType=db.m3.medium, IOPS=0, MultiAZ=true, PreferredBackupWindow=22:00-23:00, PreferredMaintenanceWindow=wed:03:32-wed:04:02, StorageEncrypted=false, StorageEncryptionKey="", StorageType=gp2`。
- 應用程式：`DeploymentConfigName=CodeDeployDefault.OneAtATime`。

變數參數：

主控台提供開始時間的 ASAP 選項，此演練建議使用它。ASAP 會在通過核准後立即執行 RFC。

> **Note**
>
> 您可以選擇以不同於所示的方式設定許多參數。範例中顯示的參數值已經過測試，但可能不適合您。範例中只會顯示所需的值。應該變更###字型中的值，因為這些值專屬於您的帳戶。

建立基礎設施

此程序使用高可用性雙層堆疊 CT，後面接著建立 S3 儲存體 CT。

在開始之前收集下列資料，可讓部署更快進行。

必要資料 HA 堆疊：

- AutoScalingGroup：
  - UserData：此值在本教學課程中提供。它包含用於設定 CodeDeploy 資源並啟動 CodeDeploy 代理程式的命令。
  - AMI-ID：此值決定 Auto Scaling 群組 (ASG) 將啟動的 EC2 執行個體作業系統。在您的帳戶中選取以「customer-」開頭的 AMI，並且是您想要的作業系統。在 AMS 主控台 VPCs -> VPCs詳細資訊頁面中尋找 AMI IDs。此逐步解說適用於設定為使用 Amazon Linux 或 RHEL AMI 的 ASGs。
- 資料庫：
  - 這些參數 DBEngine、En EngineVersion 和 LicenseModel 應根據您的情況設定，但範例中顯示的值已經過測試。教學課程分別使用這些值：*MySQL*、*8.0.16*、*general-public-license*。
  - 部署應用程式套件時，需要這些參數、DBName、MasterUserPassword 和 MasterUsername。教學課程分別使用這些值：*wordpressDB*、*p4ssw0rd*、*admin*。請注意，DBName 只能包含英數字元。
  - 當您輸入 RDS 資料庫的 MasterUsername 時，它會以純文字顯示，因此請儘快登入資料庫，並變更密碼以確保您的安全。
  - 對於 RDSSubnetIds請使用兩個私有子網路。在每個項目之後按「Enter」一次輸入一個項目。使用 尋找子網路 IDs 如需 AMS SKMS API 參考，請參閱 AWS 成品主控台中的報告索引標籤。 操作 (CLI：list-subnet-summaries) 或 AMS 主控台 VPCs -> VPC 詳細資訊頁面。
- LoadBalancer：
  - 將此參數公有設為 true，因為教學課程使用公有 ELB 子網路。
  - ELBSubnetIds：使用兩個公有子網路。在每個項目之後按「Enter」一次輸入一個項目。使用 尋找子網路 IDs 如需 AMS SKMS API 參考，請參閱 AWS 成品主控台中的報告索引標籤。 操作 (CLI：list-subnet-summaries) 或 AMS 主控台 VPCs -> VPC 詳細資訊頁面。
- 應用程式：ApplicationName 值會設定 CodeDeploy 應用程式名稱和 CodeDeploy 部署群組名稱。您可以使用它來部署應用程式。它在帳戶中必須是唯一的。若要檢查您的帳戶是否有 CodeDeploy 名稱，請參閱 CodeDeploy 主控台。此範例使用 *WordPress*，但如果您將使用該值，請確定它尚未使用。

1. 啟動高可用性堆疊。

   a. 在建立 RFC 頁面上，從清單中選取類別部署、子類別標準堆疊、項目高可用性雙層堆疊和操作建立。

b. 重要：選擇進階並如所示設定值。

您只需輸入星號 (*) 選項的值，測試的值會顯示在範例中；您可以將不需要的空白選項保留空白。

c. 對於 RFC 描述區段：

```
Subject: WP-HA-2-Tier-RFC
```

d. 在資源資訊區段中，設定 AutoScalingGroup、資料庫、LoadBalancer、應用程式和標籤的參數。

此外，「AppName」標籤金鑰的目的是讓您輕鬆地在 EC2 主控台中搜尋 ASG 執行個體；您可以呼叫此標籤金鑰「Name」或任何其他您想要的金鑰名稱。請注意，您最多可以新增 50 個標籤。

```
UserData:
    #!/bin/bash
    REGION=$(curl 169.254.169.254/latest/meta-data/placement/availability-zone/
 | sed 's/[a-z]$//')
    yum -y install ruby httpd
    chkconfig httpd on
    service httpd start
    touch /var/www/html/status
    cd /tmp
    curl -O https://aws-codedeploy-$REGION.s3.amazonaws.com/latest/install
    chmod +x ./install
    ./install auto
    chkconfig codedeploy-agent on
    service codedeploy-agent start
AmiId:              AMI-ID
Description:        WP-HA-2-Tier-Stack

Database:
    LicenseModel:    general-public-license (USE RADIO BUTTON)
    EngineVersion:   8.0.16
    DBEngine:        MySQL
    RDSSubnetIds:    PRIVATE_AZ1 PRIVATE_AZ2 (ENTER ONE AT A TIME PRESSING
 "ENTER" AFTER EACH)
    MasterUserPassword:  p4ssw0rd
    MasterUsername:      admin
    DBName:              wordpressDB
```

```
LoadBalancer:
    Public:              true (USE RADIO BUTTON)
    ELBSubnetIds:        PUBLIC_AZ1 PUBLIC_AZ2

Application:
    ApplicationName:     WordPress

Tags:
    Name:                WP-Rhel-Stack
```

e. 完成後按一下提交。

2. 登入您建立的資料庫並變更密碼。
3. 啟動 S3 儲存貯體堆疊。

   在開始之前收集下列資料，可讓部署更快進行。

   必要資料 S3 儲存貯體：

   - VPC-ID：此值會決定 S3 儲存貯體的位置。使用 尋找 VPC IDs 如需 AMS SKMS API 參考，請參閱 AWS 成品主控台中的報告索引標籤。 操作 (CLI：list-vpc-summaries) 或 AMS 主控台 VPCs頁面中的報告索引標籤。
   - BucketName：此值會設定 S3 儲存貯體名稱，您可以使用它來上傳應用程式套件。它在帳戶區域必須是唯一的，且不能包含大寫字母。將您的帳戶 ID 包含在 BucketName 中不是必要項目，但之後更容易識別儲存貯體。若要查看帳戶中存在哪些 S3 儲存貯體名稱，請前往您帳戶的 Amazon S3 主控台。

   a. 在建立 RFC 頁面上，從 RFC CT 挑選清單選取類別部署、子類別進階堆疊元件、項目 S3 儲存和操作建立。

   b. 保留預設的基本選項，並如所示設定值。

```
Subject:             S3-Bucket-WP-HA-RFC
Description:         S3BucketForWordPressBundles
BucketName:          ACCOUNT_ID-BUCKET_NAME
AccessControl:       Private
VpcId:               VPC_ID
Name:                S3-Bucket-WP-HA-Stack
TimeoutInMinutes:    60
```

   c. 完成後按一下提交。使用此變更類型部署的儲存貯體允許完整讀取/寫入存取整個帳戶。

建立、上傳和部署應用程式

首先，建立 WordPress 應用程式套件，然後使用 CodeDeploy CTs 來建立和部署應用程式。

1. 下載 WordPress、擷取檔案並建立 ./scripts 目錄。

   Linux 命令：

   ```
   wget https://github.com/WordPress/WordPress/archive/master.zip
   ```

   Windows：貼`https://github.com/WordPress/WordPress/archive/master.zip`到瀏覽器視窗並下載 zip 檔案。

   建立要在其中組合套件的暫時目錄。

   Linux：

   ```
   mkdir /tmp/WordPress
   ```

   Windows：建立「WordPress」目錄，稍後您將使用目錄路徑。
2. 將 WordPress 來源解壓縮至「WordPress」目錄，並建立 ./scripts 目錄。

   Linux：

   ```
   unzip master.zip -d /tmp/WordPress_Temp
   cp -paf /tmp/WordPress_Temp/WordPress-master/* /tmp/WordPress
   rm -rf /tmp/WordPress_Temp
   rm -f master
   cd /tmp/WordPress
   mkdir scripts
   ```

   Windows：前往您建立的「WordPress」目錄，並在該處建立「scripts」目錄。

   如果您在 Windows 環境中，請務必將指令碼檔案的中斷類型設定為 Unix (LF)。在記事本 ++ 中，這是視窗右下角的選項。
3. 在 WordPress 目錄中建立 CodeDeploy appspec.yml 檔案（如果複製範例，請檢查縮排，每個空間計數）。重要：確保「來源」路徑正確，可將 WordPress 檔案（在本例中為 WordPress 目錄中）複製到預期的目的地 (/var/www/html/WordPress)。在此範例中，appapppec.yml 檔案位於

具有 WordPress 檔案的 目錄中，因此只需要 "/"。此外，即使您為 Auto Scaling 群組使用 RHEL AMI，也請保持原狀。Apppec.yml 檔案範例：

```
version: 0.0
os: linux
files:
  - source: /
    destination: /var/www/html/WordPress
hooks:
  BeforeInstall:
    - location: scripts/install_dependencies.sh
      timeout: 300
      runas: root
  AfterInstall:
    - location: scripts/config_wordpress.sh
      timeout: 300
      runas: root
  ApplicationStart:
    - location: scripts/start_server.sh
      timeout: 300
      runas: root
  ApplicationStop:
    - location: scripts/stop_server.sh
      timeout: 300
      runas: root
```

4. 在 WordPress ./scripts 目錄中建立 bash 檔案指令碼。

   首先，`config_wordpress.sh`使用下列內容建立（如果您願意，可以直接編輯 wp-config.php 檔案）。

   > **Note**
   >
   > 將 *DBName* 取代為 HA 堆疊 RFC 中指定的值（例如 `wordpress`)。
   > 將 *DB_MasterUsername* 取代為 HA 堆疊 RFC 中指定的`MasterUsername`值（例如 `admin`)。
   > 將 *DB_MasterUserPassword* 取代為 HA Stack RFC 中指定的`MasterUserPassword`值（例如 `p4ssw0rd`)。
   > 將 *DB_ENDPOINT* 取代為 HA Stack RFC 執行輸出中的端點 DNS 名稱（例如 `srt1cz23n45sfg.clgvd67uvydk.us-east-1.rds.amazonaws.com`)。您可以使用

GetRfc 操作 (CLI：get-rfc --rfc-id RFC_ID) 或在先前提交的 HA Stack RFC 的 AMS 主控台 RFC 詳細資訊頁面中找到此項目。

```
#!/bin/bash
chmod -R 755 /var/www/html/WordPress
cp /var/www/html/WordPress/wp-config-sample.php /var/www/html/WordPress/wp-
config.php
cd /var/www/html/WordPress
sed -i "s/database_name_here/DBName/g" wp-config.php
sed -i "s/username_here/DB_MasterUsername/g" wp-config.php
sed -i "s/password_here/DB_MasterUserPassword/g" wp-config.php
sed -i "s/localhost/DB_ENDPOINT/g" wp-config.php
```

5. 在相同的目錄中`install_dependencies.sh`，使用下列內容建立 ：

```
#!/bin/bash
yum install -y php
yum install -y php-mysql
yum install -y mysql
service httpd restart
```

> **Note**
>
> HTTPS 會在啟動時安裝為使用者資料的一部分，以允許運作狀態檢查從頭開始運作。

6. 在相同的目錄中`start_server.sh`，使用下列內容建立 ：

   - 對於 Amazon Linux 執行個體，請使用：

   ```
   #!/bin/bash
   service httpd start
   ```

   - 對於 RHEL 執行個體，請使用此 （額外的命令是允許 SELINUX 接受 WordPress 的政策）：

   ```
   #!/bin/bash
   setsebool -P  httpd_can_network_connect_db 1
   setsebool -P  httpd_can_network_connect 1
   chcon -t httpd_sys_rw_content_t /var/www/html/WordPress/wp-content -R
   restorecon -Rv /var/www/html
   ```

```
service httpd start
```

7. 在相同的目錄中stop_server.sh，使用下列內容建立 ：

```
#!/bin/bash
service httpd stop
```

8. 建立 zip 套件。

   Linux：

```
$ cd /tmp/WordPress
$ zip -r wordpress.zip .
```

   Windows：前往您的「WordPress」目錄，選取所有檔案並建立 zip 檔案，請務必將其命名為 wordpress.zip。

1. 將應用程式套件上傳至 S3 儲存貯體

   套件必須就位，才能繼續部署堆疊。

   您會自動存取您建立的任何 S3 儲存貯體執行個體。您可以透過堡壘 （ 請參閱存取執行個體) 或透過 S3 主控台存取，並使用drag-and-drop上傳 CodeDeploy 套件，或瀏覽並選取檔案。

   您也可以在 shell 視窗中使用以下命令；請確定您有 zip 檔案的正確路徑：

```
aws s3 cp wordpress/wordpress.zip s3://BUCKET_NAME/
```

2. 部署 WordPress CodeDeploy 應用程式套件

   所需的資料碼部署應用程式部署：

   - CodeDeployApplicationName：您提供 CodeDeploy 應用程式的名稱。
   - CodeDeployGroupName：由於 CodeDeploy 應用程式和群組都是從您在 HA 堆疊 RFC 中提供 CodeDeploy 應用程式的名稱建立的，因此這是與 CodeDeployApplicationName 相同的名稱。
   - S3Bucket體：您提供 S3 儲存貯體的名稱。
   - S3BundleType 和 S3Key：這些是您部署的 WordPress 應用程式套件的一部分。
   - VpcId：相關的 VPC。

a. 在建立 RFC 頁面上，從 RFC CT 挑選清單選取類別部署、子類別應用程式、項目 CodeDeploy 應用程式和操作部署。

b. 保留預設的基本選項，並如所示設定值。

> **Note**
>
> 參考先前建立的 CodeDeploy 應用程式、CodeDeploy 部署群組、S3 儲存貯體和套件。

```
Subject:                                    WP-CD-Deploy-RFC
Description:                                DeployWordPress
S3Bucket:                                   BUCKET_NAME
S3Key:                                      wordpress.zip
S3BundleType:                               zip
CodeDeployApplicationName:                  WordPress
CodeDeployDeploymentGroupName:              WordPress
CodeDeployIgnoreApplicationStopFailures:    false
RevisionType:                               S3



VpcId:                                      VPC_ID
Name:                                       WP-CD-Deploy-Op
TimeoutInMinutes:                           60
```

c. 完成後按一下提交。

驗證應用程式部署

導覽至先前建立負載平衡器的端點 (LoadBalancerCName)，並使用 WordPress 部署的路徑：/WordPress。例如：

```
http://stack-ID-FOR-ELB.us-east-1.elb.amazonaws.com/WordPress
```

您應該會看到如下的頁面：

向下拉動高可用性部署

若要縮減部署，您可以針對 HA 兩層堆疊和 S3 儲存貯體提交刪除堆疊 CT，並請求刪除 RDS 快照（這些快照會在十天後自動刪除，但在那裡需要支付少量費用）。收集 HA 堆疊IDs，然後遵循下列步驟。 S3 請參閱堆疊 | 刪除。

附錄：SALZ 入門問卷

主題

這是您在加入帳戶之前需要考慮的一些資訊。

部署摘要

部署的描述。例如：

- 此帳戶適用於Line-of-Business應用程式部署（而不是產品應用程式部署）。
- 部署涉及帳戶公有或 DMZ 子網路內的自動擴展 ARP（已驗證的反向代理）。
- Web 和應用程式伺服器將部署在帳戶的私有子網路中。
- RDS (Amazon Relational Database Service) 執行個體也會部署在帳戶的私有子網路內。
- 伺服器 (ARP、Web、應用程式、資料庫、負載平衡器等）會分成不同的安全群組。
- 帳戶需要跨可用區域 (AZs) 分散的 HA（高可用性）設計，即「異地同步備份」。

環境架構考量事項

在決定如何設定環境和架構時，請考慮下列條件。

- 您的虛擬資料中心是否會重新連線至您的公司網路？
  - 您是否有現有的 AWS DirectConnect 服務，還是需要新的 DirectConnect 服務？

  - 您有現有的 VPN 連線，還是需要新的 VPN 服務？
- 您可以配置的內部地址的可用 CIDR 區塊範圍是多少？（建議使用 /16，不得與公司網路範圍重疊）
- 您的虛擬資料中心是否需要網際網路存取？
- 您想要使用哪個區域（些區域）？（雪梨/N. 維吉尼亞/都柏林）
- 您需要共享服務子網路來託管連線至所有其他子網路的應用程式嗎？
- 您希望託管為個別子網路的組織部門有哪些。對於每個 ：
  - 您需要與其他子網路的哪些連線？
  - 子網路是否需要網際網路存取？
  - 該子網路是否有任何應用程式部署限制？
  - 該子網路是否有任何特定的網路需求？
- 您想要單獨的開發和/或測試環境嗎？（將包含重複的共用服務，以便隨時存取）
- 您的快照備份需求是什麼？
- 您有現有的維護程序或修補程式時段（您想要保留）嗎？
- 您的網域註冊要求是什麼？
- 您是否有任何單一登入要求？（例如 AD、LDAP)
- 您的整體預期作業系統和預期的容量需求為何？

單一帳戶登陸區域監控提醒

AMS 可讓您直接收到特定監控提醒的提醒（而不是收到 AMS 服務通知）。若要註冊，請確定您的 Cloud Architect (CA 或 Cloud Service Delivery Manager (CSDM) 收到此資訊：

直接提醒電子郵件：這些是您希望 AMS 傳送特定資源型提醒的電子郵件地址。如需哪些警示會直接傳送到電子郵件的詳細資訊，請參閱《AMS 單一帳戶登陸區域使用者指南》中的 AMS 中基準監控的警示。如需 AMS 監控的詳細資訊，請參閱《AMS 單一帳戶登陸區域使用者指南》中的監控管理。

維護時段

您會想要建立維護時段，以考慮不同的應用程式需求 AWS 區域、不同和不同的壓力期間。您的維護時段是 AMS 套用修補的時間。以下是一些準則：

- 若要限制對使用者的影響，請根據部署環境 AWS 區域 的 來規劃維護時段。
- 在正常營業時間之外以及生產伺服器上預期流量最少時，排定時段。
- 一般而言，基礎設施堆疊需要每月更新。

- 排程維護時段至少 300 分鐘。作業系統修補需要 60-90 分鐘，基礎設施堆疊修補需要 180-300 分鐘。

後續步驟

AMS 加入團隊將協助您在帳戶加入 AMS 的每個步驟。以下是加入要求：

- 佈建新的 AWS 帳戶 以用於 AMS，並提供 AWS 帳戶 ID。
- 註冊所需的支援層級。
- 建立跨帳戶 IAM 角色以授予 AMS 佈建帳戶存取權，並將角色名稱提供給 AMS。
- 將帳戶 753102745277 新增為受信任實體。

附錄：ActiveDirectory 聯合服務 (ADFS) 宣告規則和 SAML 設定

如需如何安裝和設定 AD FS step-by-step說明，請參閱使用 Windows Active Directory、ADFS 和 SAML 2.0 啟用與 AWS 的聯合。

ADFS 宣告規則組態

如果您已有 ADFS 實作，請設定以下內容：

- 依賴方信任
- 宣告規則

依賴方信任和宣告規則步驟是從使用 Windows Active Directory、AD FS 和 SAML 2.0 部落格啟用聯合到 AWS

- 宣告規則：
  - Nameid：每個部落格文章的組態
  - RoleSessionName：如下所示設定
    - 宣告規則名稱： **RoleSessionName**
    - 屬性存放區： **Active Directory**
    - LDAP 屬性： **SAM-Account-Name**
    - 傳出宣告類型： **https://aws.amazon.com/SAML/Attributes/RoleSessionName**
    - 取得 AD 群組：每個部落格文章的組態
    - 角色宣告：如下所示設定

```
c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-([^d]{12})-"]
```

```
=> issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value =
 RegExReplace(c.Value, "AWS-([^d]{12})-", "arn:aws:iam::$1:saml-provider/
customer-readonly-saml,arn:aws:iam::$1:role/"));
```

Web 主控台

您可以使用以下連結，將 *#ADFS-FQDN#* 取代為 ADFS 實作的 FQDN，來存取 AWS Web 主控台。

https：//*#ADFS-FQDN#*/adfs/ls/IdpInitiatedSignOn.aspx

您的 IT 部門可以透過群組政策，將上述連結部署至使用者人口。

使用 SAML 存取 API 和 CLI

如何使用 SAML 設定 API 和 CLI 存取。

python 套件來源於以下部落格文章：

- NTLM：如何使用 SAML 2.0 和 AD FS 實作聯合 API 和 CLI 存取
- 表單：如何使用 SAML 2.0 實作聯合 API/CLI 存取的一般解決方案
- PowerShell：如何使用 Windows PowerShell 設定對 AWS 的聯合 API 存取

指令碼組態

1. 使用記事本++，將預設區域變更為正確的區域
2. 使用記事本++，停用測試和開發環境的 SSL 驗證
3. 使用記事本++，設定 idpentryurl

```
https://[ADFS-FDQN]/adfs/ls/IdpInitiatedSignOn.aspx?
loginToRp=urn:amazon:webservices
```

Windows 組態

以下說明適用於 python 套件。產生的登入資料有效期為 1 小時。

1. 下載並安裝 python (2.7.11)
2. 下載並安裝 AWS CLI 工具
3. 安裝 AMS CLI：

    a. 下載雲端服務交付管理員 (CSDM) 提供的 AMS 可分發 zip 檔案並解壓縮。

    有數個目錄和檔案可供使用。

b. 根據您的作業系統開啟 Managed Cloud Distributables -> CLI -> Windows 或 Managed Cloud Distributables -> CLI -> Linux / MacOS 目錄，以及：

   對於 Windows，請執行適當的安裝程式（此方法僅適用於 Windows 32 或 64 位元系統）：

   - 32 位元：ManagedCloudAPI_x86.msi
   - 64 位元：ManagedCloudAPI_x64.msi

   對於 Mac/Linux，請執行名為 的檔案：MC_CLI.sh。您可以執行此命令來執行此操作：`sh MC_CLI.sh`。請注意，amscm 和 amsskms 目錄及其內容必須與 MC_CLI.sh 檔案位於相同的目錄中。

c. 如果您的公司登入資料是透過與 AWS (AMS 預設組態）聯合使用，您必須安裝登入資料管理工具，以存取您的聯合服務。例如，您可以使用此 AWS 安全部落格 如何使用 SAML 2.0 和 AD FS 實作聯合 API 和 CLI 存取，以協助設定憑證管理工具。

d. 安裝之後，請執行 `aws amscm help`和 `aws amsskms help` 以查看命令和選項。

4. 下載必要的 SAML 指令碼

   下載至 c：\aws\scripts

5. 下載 PIP

   下載至 c：\aws\downloads

6. 使用 PowerShell 安裝 PIP

   <pythondir>。\python.exe c：\aws\downloads\get-pip.py

7. 使用 PowerShell 安裝 boto 模組

   <pythondir\scripts>pip 安裝 boto

8. 使用 PowerShell 安裝請求模組

   <pythondir\scripts>pip 安裝請求

9. 使用 PowerShell 安裝請求安全模組

   <pythondir\scripts>pip 安裝請求【安全性】

10. 使用 PowerShell 安裝 beautifulsoup 模組

    <pythondir\scripts>pip 安裝 beautifulsoup4

11. 使用 PowerShell，在使用者設定檔中建立名為 .aws 的資料夾 (%userprofile%\.aws)

mkdir .aws

12. 使用 PowerShell，在 .aws 資料夾中建立登入資料檔案

    新項目登入資料 - 類型檔案 -force

    登入資料檔案不得有副檔名

    檔案名稱必須全部小寫，且具有名稱登入資料

13. 使用記事本開啟登入資料檔案並貼上下列資料，指定正確的區域

```
[default]
output = json
region = us-east-1
aws_access_key_id =
aws_secret_access_key =
```

14. 使用 PowerShell、SAML 指令碼和登入

    <pythondir>。\python.exe c：\aws\scripts\samlapi.py

    使用者名稱：【USERNAME】@upn

    選擇您要擔任的角色

Linux 組態

產生的登入資料有效期為 1 小時。

1. 使用 WinSCP 傳輸 SAML 指令碼
2. 使用 WinSCP 傳輸根 CA 憑證（忽略用於測試和開發）
3. 將 ROOT CA 新增至信任的根憑證（忽略用於測試和開發）

   $ openssl x509 -inform der -in 【certname】.cer -out certificate.pem（忽略用於測試和開發）

   將 certificate.pem 的內容新增至 /etc/ssl/certs/ca-bundle.crt 檔案結尾（忽略用於測試開發）
4. 在 home/ec2-user 5 中建立 .aws 資料夾

```
[default]
output = json
region = us-east-1
aws_access_key_id =
aws_secret_access_key =
```

5. 使用 WinSCP，將登入資料檔案傳輸至 .aws 資料夾
6. 安裝 boto 模組

   $ sudo pip 安裝 boto
7. 安裝請求模組

   $ sudo pip 安裝請求
8. 安裝 beautifulsoup 模組

   $ sudo pip 安裝 beautifulsoup4
9. 將指令碼複製到 home/ec2-user

   設定必要的許可

   執行指令碼：https：//samlapi.py

文件歷史記錄

下表說明自上次發行 AMS 以來文件的重要變更。

- API 版本：2019-05-21
- 文件最近更新時間：2025 年 9 月 23 日

變更	描述	日期
更新 AWS Managed Services 常見問答集章節中 SageMaker AI 中端點自動擴展的變更類型	使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon SageMaker AI。 使用管理提交 RFC | 進階堆疊元件 | Identity and Access Management (IAM) | 更新實體或政策（需要檢閱）變更類型 (ct-27tuth19k52b4)，以暫時或永久提升自動擴展許可，因為自動擴展需要在 CloudWatch 服務上進行許可存取。	2025 年 9 月 25 日
精確的變更類型參考	建立、變更或刪除安全群組。 若要新增使用者：使用 Management | Directory Service | 使用者和群組 | 新增使用者至群組 【ct-24pi85mjtza8k】 和移除使用者：使用 Management | Directory Service | 使用者和群組 提交 RFC | 從群組 【ct-2019s9y3nfml4】 移除使用者	2025 年 8 月 8 日
已移除 TOC 連結	TOC AWS 詞彙表連結已移除。	2025 年 8 月 8 日
新增了處方指引的連結	設定合併帳單 - 將新帳戶連結至付款人帳戶.	2025 年 5 月 8 日
更新啟用 IAM 存取的指示 AWS 管理主控台	說明啟用 IAM 存取的指示 AWS 管理主控台。	啟用 AWS 主控台的 IAM 存取

變更	描述	日期
更新 Direct Connect 專用連線上允許的傳輸虛擬介面數量	Direct Connect 專用連線現在限制每個連線 4 個傳輸虛擬介面	將 Direct Connect 連線至 Transit Gateway
改善措辭。	指定「僅用於「拒絕」清單」必須包含「允許全部」，以確保 AMS 監控和管理操作。	網路組態
有關使用 AMS CLI 的其他資訊。	「新增了注意，某些 CLI 命令可能需要 `--region`選項」	安裝 AMS CLIs
更新：一致性和可讀性的章節標題，將一些主題子區段移至更適當的區段	「變更管理模式」是「變更管理」的新標題	變更管理模式
已更新內容	先前稱為「變更管理模式」或「標準 CM 模式」的 AMS 模式現在稱為「RFC 模式」。模式區段已展開。	RFC 模式.
已更新內容	先前稱為「變更管理模式」或「標準 CM 模式」的 AMS 模式現在稱為「RFC 模式」。已縮短模式區段，並連結至新增模式的 AMS 進階使用者指南區段。	AMS 模式.
MALZ：更新網路架構圖	網路帳戶架構m	2022 年 6 月 16 日
已將主題清單移至開啟段落下方	AWS Managed Services 加入簡介	2022 年 6 月 16 日
已更新內容、包容性語言計畫	「管理帳戶」不是「主帳戶」。	AMS 中的 IAM 使用者角色、「政策範例」區段

變更	描述	日期
已更新內容、工具帳戶角色名稱	將角色名稱 CustomerMigrationAccessRole 更新為 AWSManagedServicesMigrationRole。	AWS 應用程式遷移服務 (AWS MGN)
SALZ：持續性管理預設值	已更新連結並從 移除過時的資訊 VPC 標籤和預設值	2022 年 2 月 28 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。