使用者指南

AWS Organizations

AWS Organizations: 使用者指南

Table of Contents

什麼是 AWS Organizations？

AWS Organizations 是一種帳戶管理服務，可讓您將多個 AWS 帳戶 合併成一個組織，讓您可以建立和集中管理。AWS Organizations 包括帳戶管理和合併帳單功能，可讓您更符合您商業的預算、安全及合規需求。身為組織的管理員，您可以在您的組織中建立帳戶，並邀請現有的帳戶加入組織。

此使用者指南會定義AWS Organizations 的主要概念，提供 教學課程，並解釋如何建立和管理組織。

主題

AWS Organizations 功能

AWS Organizations 提供下列功能：

集中管理所有 AWS 帳戶

您可以將現有帳戶合併到可讓您集中管理帳戶的組織。您可以建立會自動成為組織一部分的帳戶，也可以邀請其他帳戶來加入您的組織。您也可以連接會影響您的部分或所有帳戶的政策。

所有成員帳戶合併的帳單

合併帳單為 AWS Organizations 的功能。您可以使用組織的管理帳戶來合併並為所有成員帳戶支付費用。在合併帳單中，管理帳戶也可以存取其組織中成員帳戶的帳單資訊、帳戶資訊和帳戶活動。此資訊可用於 Cost Explorer 之類的服務，這可協助管理帳戶改善組織的成本績效。

將帳戶階層分組，以滿足您的預算、安全或合規需求

您可以將帳戶分組為組織單位 (OU)，並將不同的存取政策連接到每個 OU。例如，如果您的帳戶必須只能存取符合特定法規要求的 AWS 服務，您可以將這些帳戶放到一個 OU。然後，您可以將政策連接到該 OU，該政策會封鎖對不符合這些法規要求服務的存取。您可以在其他 OU 內形成巢狀 OU，成為五層的深度，對您建構帳戶群組的方式提供彈性。

集中控制每個帳戶能存取的 AWS 服務及 API 動作的政策

身為組織管理帳戶的管理員，您可以使用服務控制政策 (SCP) 來指定組織中成員帳戶的許可數量上限。在 SCP 中，您可以限制每個成員帳戶中使用者和角色所能存取的 AWS 服務、資源及個別 API

動作。您也可以定義條件，決定何時要限制 AWS 服務、資源及 API 動作的存取。這些限制甚至會覆寫組織中成員帳戶的管理員。當 AWS Organizations 禁止成員帳戶存取服務、資源或 API 動作時，該帳戶中的使用者或角色就無法存取這些項目。即使成員帳戶的管理員在 IAM 政策中明確授與這類許可，此封鎖仍然有效。

如需詳細資訊，請參閱 服務控制政策 (SCP)。

標準化組織帳戶中各資源標籤的政策

您可以使用標籤政策來維護標籤的一致性，包括標籤索引鍵和標籤值的慣用大小寫處理。

如需詳細資訊，請參閱標籤政策

控制 AWS 人工智慧 (AI) 和機器學習服務如何收集和存放資料的政策。

您可以使用 AI 服務選擇退出政策，為您不想使用的任何 AWS AI 服務選擇退出資料收集和儲存。

如需詳細資訊，請參閱AI 服務選擇退出政策

為組織帳戶中資源設定自動備份的政策

您可以使用備份政策來設定並將 AWS Backup 計劃自動套用至您組織所有帳戶的資源。

如需詳細資訊，請參閱備份政策

AWS Identity and Access Management (IAM) 的整合與支援

IAM 可提供個別帳戶中使用者及角色的細微控制。AWS Organizations 則會將該控制擴展至帳戶層級，讓您控制帳戶或帳戶群組中的使用者和角色能執行的作業。產生的許可為 AWS Organizations 在帳戶層級允許之許可與 IAM 在該帳戶內的使用者或角色層級所明確授予之許可的邏輯交集。換句話說，使用者只能存取 AWS Organizations 政策和 IAM 政策均允許的內容。若任一項政策封鎖了操作，使用者即無法存取該操作。

與其他 AWS 服務整合

您可以利用 AWS Organizations 中提供的多帳戶管理服務，搭配選取的 AWS 服務，在您所有的組織成員帳戶上執行任務。如需服務清單及了解在全組織層級上使用每個服務的優點，請參閱AWS 您可以搭配使用的服務 AWS Organizations。

在組織的成員帳戶中啟用 AWS 服務以代表您執行任務時，AWS Organizations 會在每個成員帳戶中建立 IAM 服務連結角色。此服務連結角色具有預先定義的 IAM 許可，允許另一項 AWS 服務在組織和其帳戶中執行特定任務。為此，組織中的所有帳戶都自動具有服務連結角色。此角色允許 AWS Organizations 服務，針對您啟用信任存取的 AWS 服務，建立所需的服務連結角色。這些額外的服務連結角色連接至 IAM 許可政策，可讓指定的服務僅執行組態選項所需的任務。如需詳細資訊，請參閱 搭配使用 AWS Organizations 與其他 AWS 服務。

全域存取

AWS Organizations 是一項全域服務，具有適用於任何和所有 AWS 區域 的單一端點。您不需要明確選取要在其中運作的區域。

最終一致的資料複寫

與許多其他 AWS 服務一樣，AWS Organizations 最終一致。AWS Organizations 在其區域內的 AWS 資料中心，跨多部伺服器複寫資料，以達到高可用性。如果變更一些資料的請求成功完成，則該變更經認可並安全儲存。不過，變更必須在多個伺服器間進行複製。如需詳細資訊，請參閱 我所做的變更不一定都會立即顯示。

免費使用

AWS Organizations 是 AWS 帳戶 可享的一項功能，無須額外付費。只有在您從組織中的帳戶訪問其他 AWS 服務時才需要付費。如需有關其他 AWS 產品的定價資訊，請參閱 Amazon Web Services 定價頁面。

AWS Organizations 定價

AWS Organizations 免費提供。您只需為您的成員帳戶中的使用者和角色使用的 AWS 資源付費。例如，您需針對您的成員帳戶中的使用者或角色使用的 Amazon EC2 執行個體支付標準費用。如需其他 AWS 服務定價的相關資訊，請參閱 AWS 定價。

存取 AWS Organizations

您可以透過以下任何方式來使用 AWS Organizations：

AWS Management Console

AWS Organizations 主控台是一種以瀏覽器為基礎的界面，可供您用來管理您的組織和 AWS 資源。您可以使用主控台在您的組織中執行任何任務。

AWS 命令列工具

您可以使用 AWS 命令列工具，在系統的命令列發出命令，以執行 AWS Organizations 和 AWS 任務。使用命令列比使用主控台更快、更方便。若您想要建構執行 AWS 任務的指令碼，命令列工具也非常實用。

AWS 提供兩組命令列工具：

- AWS Command Line Interface (AWS CLI). 如需安裝與使用 AWS CLI 的相關資訊，請參閱 AWS Command Line Interface 使用者指南。
- AWS Tools for Windows PowerShell. 如需安裝和使用 Tools for Windows PowerShell 的詳細資訊，請參閱 AWS Tools for Windows PowerShell 使用者指南。

AWS SDK

AWS SDK 以程式庫以及適用於多種程式設計語言及平台 (Java、Python、Ruby、.NET、iOS、Android 等) 的範本程式碼所組成。SDK 會負責的工作諸如以密碼演算法簽署請求、管理錯誤以及自動重試請求。如需 AWS SDK 的其他資訊 (包括如何下載並安裝開發套件)，請參閱 Amazon Web Services 工具。

AWS Organizations HTTPS 查詢 API

AWS Organizations HTTPS 查詢 API 可讓您以程式設計方式存取 AWS Organizations 和 AWS。HTTPS 查詢 API 可讓您直接向該服務發出 HTTPS 請求。當您使用 HTTPS API 時，必須包含使用您的憑證來數位簽署請求的程式碼。如需詳細資訊，請參閱執行 HTTP 查詢請求來呼叫 API 和 AWS Organizations API 參考。

AWS Organizations 的支援和意見回饋

我們誠摯歡迎您提供意見回饋。您可將意見傳送至 feedback-awsorganizations@amazon.com。您也可以將意見回饋和問題發佈到 AWS Organizations 支援論壇。如需 AWS 支援論壇的詳細資訊，請參閱「論壇說明」。

其他 AWS 資源

- AWS 培訓與課程 – 連結至以角色為基礎的專門課程與自主進度實驗室，以協助加強您的 AWS 技能，並取得實際體驗。
- AWS 開發人員工具 – 連結至開發人員工具與資源，其提供文件、程式碼範例、版本備註與其他資訊，以協助您使用 AWS 來建置創新的應用程式。
- AWS Support 中心 – 建立並管理您的 AWS 支援案例的中樞。同時包含與其他實用資源的連結，例如論壇、常見技術問答集、服務運作狀態，以及 AWS Trusted Advisor。
- AWS Support – AWS Support 相關資訊的主要網頁，為一對一的快速回應支援頻道，可協助您在雲端中建置並執行應用程式。
- 聯絡我們 – 查詢有關 AWS 帳單、帳戶、事件、濫用與其他問題的聯絡中心。
- AWS 網站條款 – 我們的著作權與商標；您的帳戶、授權與網站存取；以及其他主題的詳細資訊。

AWS Organizations 入門

下列主題提供的資訊可協助您開始學習和使用 AWS Organizations。

了解...

AWS Organizations 術語與概念

學習了解 AWS Organizations 所需的術語和核心概念。本節描述組織的每個元件，以及如何搭配使用這些元件來對這些帳戶中的使用者可以執行的操作提供新層級控制的基本知識。

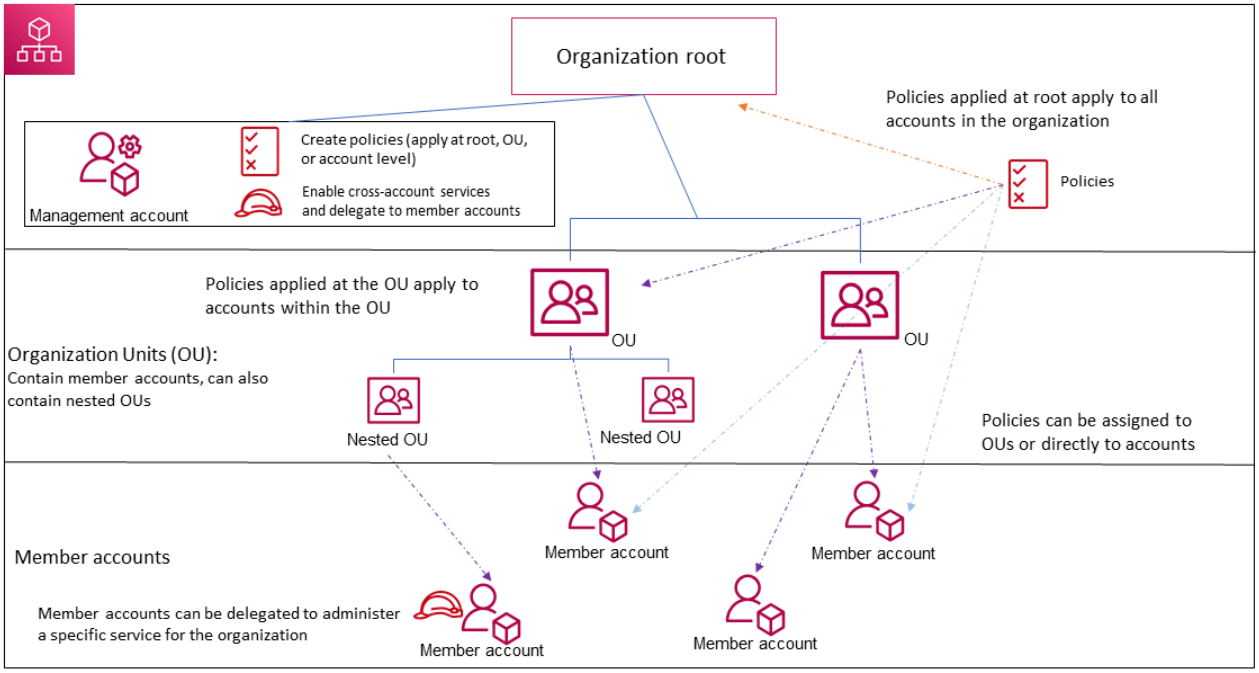
組織的合併帳單

AWS Organizations 的其中一個主要功能是合併組織中所有帳戶的帳單。進一步了解組織中帳單的處理方式，以及跨多個帳戶共用時各種折扣時的運作方式。該內容請參閱AWS Billing使用者指南。

AWS Organizations 術語與概念

為了協助您開始使用 AWS Organizations，本主題解釋一些重要概念。

下圖顯示的基本組織包含五個帳戶，這五個帳戶在根下組織成四個組織單位 (OU)。組織也有數個政策連接到其中的部分 OU 或直接連接至帳戶。對於每個項目的描述，請參閱本主題中的定義。



組織

您為了合併 AWS 帳戶所建立的實體，以便當做一個單位管理。您可以使用 AWS Organizations 主控台來集中檢視和管理您組織內的所有帳戶。組織具有一個管理帳戶，以及零個或多個成員帳戶。您可以將帳戶組織為階層式、類似樹狀目錄的結構，其中的根帳戶位於上方，而組織單位在根帳戶下形成巢狀。每個帳戶都可以直接放在根帳戶中，或放在階層中的其中一個 OU 中。組織具有的功能取決於您啟用的功能集。

根帳戶

組織中所有帳戶的父系容器。如果您將政策套用至根帳戶，該政策會套用至組織中的所有組織單位 (OU) 和帳戶。

> **Note**
>
> 目前，您只能有一個根帳戶。AWS Organizations 會在建立組織時為您自動建立該帳戶。

組織單位 (OU)

根內帳戶的容器。OU 也可以包含其他 OU，讓您能夠建立類似上下相反的樹狀目錄階層，其中的頂端有根帳戶，往下是 OU 分支，最終的帳戶是樹的葉子。將政策連接到階層的其中一個節點時，會往下流動並影響底下的所有分支 (OU) 和葉子 (帳戶)。OU 可以確切有一個父系，而目前的每個帳戶可以確切是一個 OU 的成員。

帳戶

Organizations 中的帳戶是標準 AWS 帳戶，其中包含您的 AWS 資源，以及可存取這些資源的身分。

> **Tip**
>
> AWS 帳戶與使用者帳戶不同。AWS 使用者是您使用 AWS Identity and Access Management (IAM) 建立的身分，並採用具有長期憑證的 IAM 使用者，或具有短期憑證的 IAM 角色的形式。單一 AWS 帳戶可以且通常包含許多使用者和角色。

組織中有兩種類型帳戶：指定為管理帳戶的單一帳戶，以及一個或多個成員帳戶。

- 管理帳戶是您用於建立組織的帳戶。您可以從組織的管理帳戶執行下列操作：
  - 建立組織中的帳戶
  - 邀請其他現有的帳戶加入組織
  - 從組織移除帳戶
  - 指定委派管理員帳戶
  - 管理邀請
  - 將政策套用至組織內的實體 (根帳戶、OU 或帳戶)
  - 啟用與支援的 AWS 服務的整合，在組織中跨所有帳戶提供服務功能。

  管理帳戶擁有付款人帳戶的責任，並要負責支付成員帳戶累積的所有費用。您無法變更組織的管理帳戶。
- 成員帳戶構成了組織中的所有其餘賬戶。一個帳戶一次只能是一個組織的成員。您可以將政策連接至帳戶，以僅對該單一帳戶套用控制。

> **Note**
>
> 您可以將某些成員帳戶指定為委派管理員帳戶。請參閱下面的委派管理員。

委派的管理員

我們建議您僅將 Organizations 管理帳戶及其使用者和角色用於僅由該帳戶執行的任務。我們建議您將 AWS 資源存放在組織內其他成員帳戶中，且將其保存在管理帳戶之外。這是因為安全性功能 (例如 Organizations 服務控制政策 (SCP)) 不會限制管理帳戶中任何使用者或角色。將資源與管理帳戶分開，也可協助您瞭解發票上的費用。從組織的管理帳戶中，您可以將一或多個成員帳戶指定為委派管理員帳戶以協助您實作此建議。委派管理員有兩種類型：

- Organizations 的委派管理員：您可以從這些帳戶管理組織政策，並將政策附加至組織內的實體 (根、OU 或帳戶)。管理帳戶可以在細微層級控制委派權限。如需詳細資訊，請參閱 AWS Organizations 的委派管理員。
- AWS 服務的委派管理員：您可以從這些帳戶管理與 Organizations 整合的 AWS 服務。管理帳戶可以根據需要將不同的會員帳戶註冊為委派管理員。這些帳戶具有特定服務的管理權限，以及 Organizations 唯讀動作的權限。如需詳細資訊，請參閱 與 Organizations 合作之 AWS 服務的委派管理員。

邀請

要求另一個帳戶加入組織的程序。只能由組織的管理帳戶發出邀請。邀請會延伸到與受邀帳戶相關聯的帳戶 ID 或電子郵件地址。獲邀請的帳戶接受邀請之後，就會變成組織中的成員帳戶。當組織需要所有成員核准從僅支援合併帳單功能變更為支援組織中所有功能的變更時，您也可以將邀請傳送到所有目前的成員帳戶。透過帳戶交換交握，邀請便可運作。您在 AWS Organizations 主控台可能看不到交握。但是，如果您使用 AWS CLI 或 AWS Organizations API，則必須直接使用交握。

交握

兩方之間交換資訊的多步驟程序。在 AWS Organizations 中的其中一個主要用途是做為邀請的基礎實作。交握發起方和接收發之間會傳遞和回應交握訊息。訊息的傳遞方式有助於確保雙方知道目前狀態。將組織從僅支援合併計費功能變更為支援提供的所有功能時，AWS Organizations也會使用交握。通常只有在您使用 AWS Organizations API 或命令列工具 (例如 AWS CLI) 時，才會需要直接與交握互動。

可用的功能集

- 所有功能 – 可供 AWS Organizations 使用的預設功能集。其中包含合併帳單的所有功能，還有可讓您進一步控制組織中帳戶的進階功能。例如，啟用所有功能時，組織的管理帳戶對於成員帳戶可以執行的操作具有完全控制。管理帳戶可以套用 SCP，以限制帳戶中的使用者 (包括超級使用者) 和角色可存取的服務和動作。管理帳戶也可以防止成員帳戶離開組織。您還可以啟用與支援的 AWS 服務的整合，在組織的所有帳戶中提供這些服務功能。

您可以建立已啟用所有功能的組織，或者您可以啟用最初只支援合併帳單功能之組織中的所有功能。若要啟用所有功能，所有獲邀請的成員帳戶必須透過接受在管理帳戶啟動程序時傳送的邀請來核准變更。

- 合併帳單 – 此功能集提供共用帳單功能，但不包含 AWS Organizations 的更進階功能。例如，您無法啟用其他 AWS 服務來與您的組織整合，以便在其所有帳戶中工作；或使用政策來限制不同帳戶中的使用者和角色可執行什麼動作。若要使用進階 AWS Organizations 功能，您必須在組織中啟用所有功能。

服務控制政策 (SCP)

指定在 SCP 影響的帳戶中，使用者和角色可使用服務和動作的政策。SCP 與 IAM 許可政策相似，差別在於不授予任何許可。SCP 會改為指定組織、組織單位 (OU) 或帳戶的許可數上限。當您將 SCP 連接到您的組織根帳戶或 OU 時，SCP 會限制成員帳戶中實體的許可。

允許清單與拒絕清單

當您套用 SCP 來篩選帳戶可用的許可時，可使用允許清單和拒絕清單做為補充策略。

- 允許清單策略 – 您明確指定允許的存取。所有其他存取權均已隱含封鎖。依預設，AWS Organizations 會將名為 `FullAWSAccess` 的 AWS 受管政策連接至所有根帳戶、OU 和帳戶。這有助於確保在您建立組織時，除非您希望進行封鎖，否則不會封鎖任何項目。換句話說，在預設情況下，所有許可均獲授與。在您準備好限制許可時，可以取代 `FullAWSAccess` 政策，其中一個只允許更有限、所需的許可集合。在受影響帳戶中的使用者和角色就可以僅執行該層級的存取，即使他們的 IAM 政策僅允許所有動作亦然。如果您取代根帳戶上的預設政策，組織中的所有帳戶都會受限制影響。您無法在階層中較低的層級上重新新增這些許可，因為 SCP 永遠無法授與許可，它只能篩選許可。
- 拒絕清單策略 – 您明確指定不允許的存取。所有其他存取權均獲授與。在此情況下，除非明確封鎖許可，否則會允許所有許可。這是 AWS Organizations 的預設行為。依預設，AWS Organizations 會將名為 `FullAWSAccess` 的 AWS 受管政策連接至所有根帳戶、OU 和帳戶。這樣一來，任何帳戶均可存取任何服務或操作，而不受限於AWS Organizations實施的限制。與上述允許清單技術不同，當使用拒絕清單時，您通常會保留預設的 `FullAWSAccess` 政策 (「全部」允許)。但接著您會連接其他政策，以明確拒絕存取不需要的服務和動作。如同 IAM 許可政策所載，明確拒絕的服務動作會覆寫任何對該動作的允許。

人工智慧 (AI) 服務選擇退出政策

一種政策類型，可協助您標準化組織中所有帳戶的 AWS AI 服務。某些 AWS AI 服務可存放和使用這些服務處理的客戶內容，以開發和持續改進 Amazon AI 服務和技術。作為 AWS 客戶，您可以使用 AI 服務選擇退出政策，來選擇退出存放或用於改進服務的內容。

備份政策

一種政策類型，可協助您將組織中所有帳戶的資源標準化及實作備份政策。在備份政策中，您可以為您的資源設定和部署備份計劃。

標籤政策

一種政策類型，可協助您標準化組織帳戶中所有帳戶各資源的標籤。在標籤政策中，您可以為特定資源指定標記規則。

AWS Organizations 教學課程

透過本節中的教學課程，您可以了解如何運用 AWS Organizations 來執行任務。

教學：建立和設定組織

依據逐步說明立即開始建立您的組織、邀請第一位成員帳戶加入、建立包含您的帳戶的 OU 階層，並且套用部分服務控制政策 (SCP)。

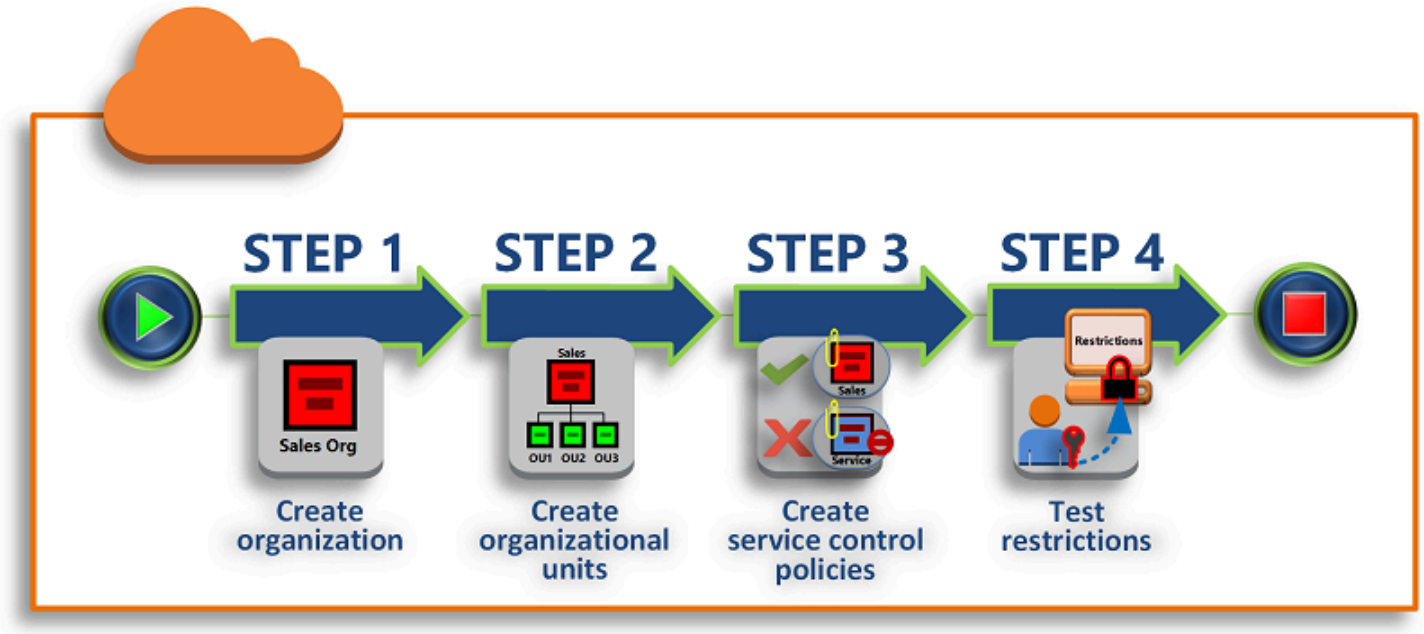
教學課程：使用 Amazon EventBridge 監控您組織的重要變更

當您指定的動作在組織內發生時，設定 Amazon EventBridge 來觸發以電子郵件形式、SMS 文字訊息或日誌項目顯示的警示電子郵件，以監控組織內的金鑰變更。例如，許多組織希望在建立新帳戶時、或是當帳戶嘗試離開組織時收到通知。

教學：建立和設定組織

在此教學中，您會建立您的組織，並為它設定兩個 AWS 成員帳戶。您會在您的組織中建立其中一個成員帳戶，及邀請其他帳戶加入您的組織。接著，您會使用允許清單技術，以指定帳戶管理員僅可以委派明確列出的服務和動作。透過這個方式，在允許公司中其他任何人使用 AWS 推出的任何新服務之前，管理員可先驗證這些服務。透過這種方式，若 AWS 引入新的服務，它仍會保持在受禁止的狀態，直到管理員運用適當政策將服務新增到允許清單為止。教學也會示範如何使用拒絕清單，確保成員帳戶中沒有使用者能夠變更 AWS CloudTrail 建立的稽核日誌組態。

下圖顯示教學的主要步驟。



[步驟 1：建立您的組織]

在此步驟中，您會建立一個組織，使用您目前的 AWS 帳戶 作為管理帳戶。您也可以邀請一個 AWS 帳戶 加入您的組織，並且將第二個帳戶建立為成員帳戶。

[步驟 2：建立組織單位]

接著，您可以在新組織中建立兩個組織單位 (OU)，並將這些成員帳戶放入 OU 中。

[步驟 3：建立服務控制政策]

您可以使用[服務控制政策 (SCP)]，將限制套用到可委派給成員帳戶中使用者及角色的動作。在此步驟中，您會建立兩個 SCP 並將他們連接到組織中的 OU。

[步驟 4：測試您組織的政策]

您可以以使用者身分從各測試帳戶登入，查看 SCP 對帳戶產生的影響。

此教學中的任何步驟都不會在 AWS 帳單中產生費用。AWS Organizations 為免費的服務。

先決條件

此教學假設您有權存取這兩個現有的 AWS 帳戶 (您會在此教學中建立第三個)，並且您可以以管理員的身分登入每個帳戶。

此教學會提到如下的帳戶：

- 111111111111 – 您用來建立組織的帳戶。此帳戶會成為管理帳戶。此帳戶擁有者的電子郵件地址為 OrgAccount111@example.com。
- 222222222222 – 您邀請加入組織作為成員帳戶的帳戶。此帳戶擁有者的電子郵件地址為 member222@example.com。
- 333333333333 – 您建立為組織成員的帳戶。此帳戶擁有者的電子郵件地址為 member333@example.com。

將上面的值替換成與您測試帳戶關聯的值。我們建議您不要在本教學中使用生產帳戶。

步驟 1：建立您的組織

在此步驟中，您會以管理員身分登入帳戶 111111111111、以管理帳戶身分使用該帳戶來建立組織，然後邀請現有帳戶 222222222222 加入為成員帳戶。

AWS Management Console

1. 以帳戶 111111111111 的管理員身分登入 AWS，並開啟 AWS Organizations主控台。
2. 在簡介頁面上，選擇 Create organization (建立組織)。
3. 在確認對話方塊中，選擇 Create an organization (建立組織)。

   > **Note**
   >
   > 在預設情況下，您建立的組織會啟用所有功能。您也可以建立組織，但選擇僅啟用合併帳單功能。

   AWS 會建立組織並顯示 AWS 帳戶 頁面。如果您在不同的頁面上，則選擇左側導覽窗格中的 AWS 帳戶。

   如果您使用的帳戶從未經由 AWS 驗證其電子郵件，則會自動傳送一封驗證電子郵件到與您的管理帳戶關聯的地址。在您收到驗證電子郵件之前，可能會有一些延遲的時間。
4. 請在 24 小時內驗證您的電子郵件地址。如需更多詳細資訊，請參閱 電子郵件地址驗證。

您的組織現已建立，其唯一成員即為您個人的帳戶。此為組織的管理帳戶。

邀請現有的帳戶加入您的組織

現在您已有了組織，就可以開始填入帳戶。在本節中的步驟，您會邀請現有帳戶加入為您組織的成員。

AWS Management Console

邀請現有的帳戶加入

1. 導覽至 AWS 帳戶 頁面，然後選擇 Add AWS 帳戶 (新增 AWS 帳戶 帳戶)。
2. 在新增 AWS 帳戶頁面中，選擇邀請現有的 AWS 帳戶。
3. 在 Email address or account ID of an AWS 帳戶 to invite (待邀請的 AWS 帳戶 帳戶的電子郵件地址或帳戶 ID) 方塊中，輸入您要邀請的帳戶擁有者電子郵件地址，如下所示：**member222@example.com**。或者，如果您知道 AWS 帳戶 ID 編號，則可改為輸入。
4. 在 Message to include in the invitation email message (要包含在邀請電子郵件訊息中的訊息) 方塊中，輸入您所需的任何文字。此文字包含在傳送到帳戶擁有者的電子郵件中。
5. 選擇 Send invitation (傳送邀請)。AWS Organizations 會傳送邀請給帳戶擁有者。

> **Important**
>
> 如果收到指示，請展開錯誤訊息。如果錯誤指出您已超出組織的帳戶限制，或是組織仍在初始化，因此無法新增帳戶，請在建立組織後等待一小時，然後再試一次。如果錯誤仍然存在，請聯絡 AWS Support。

6. 針對此教學的目的，您現在需要接受自己的邀請。執行以下其中一項，以進入主控台中的 Invitations (邀請) 頁面：
   - 開啟 AWS 從管理帳戶傳送的電子郵件，並選擇接受邀請的連結。提示您登入時，請以獲邀請成員帳戶中的管理員身分執行。
   - 開啟 AWS Organizations 主控台，導覽至 Invitations (邀請) 頁面。
7. 在 AWS 帳戶 頁面上，選擇 Accept (接受)，然後選擇 Confirm (確認)。

> **Tip**
>
> 邀請可能會延遲接收，您可能需要等待一段時間才能接受邀請。

8. 從您的帳戶成員登出，並再次在您的管理帳戶中以管理員身分登入。

建立成員帳戶

在本節中的步驟中，您會建立將自動成為組織的成員的 AWS 帳戶。我們在本教學中提到的帳戶為 333333333333。

AWS Management Console

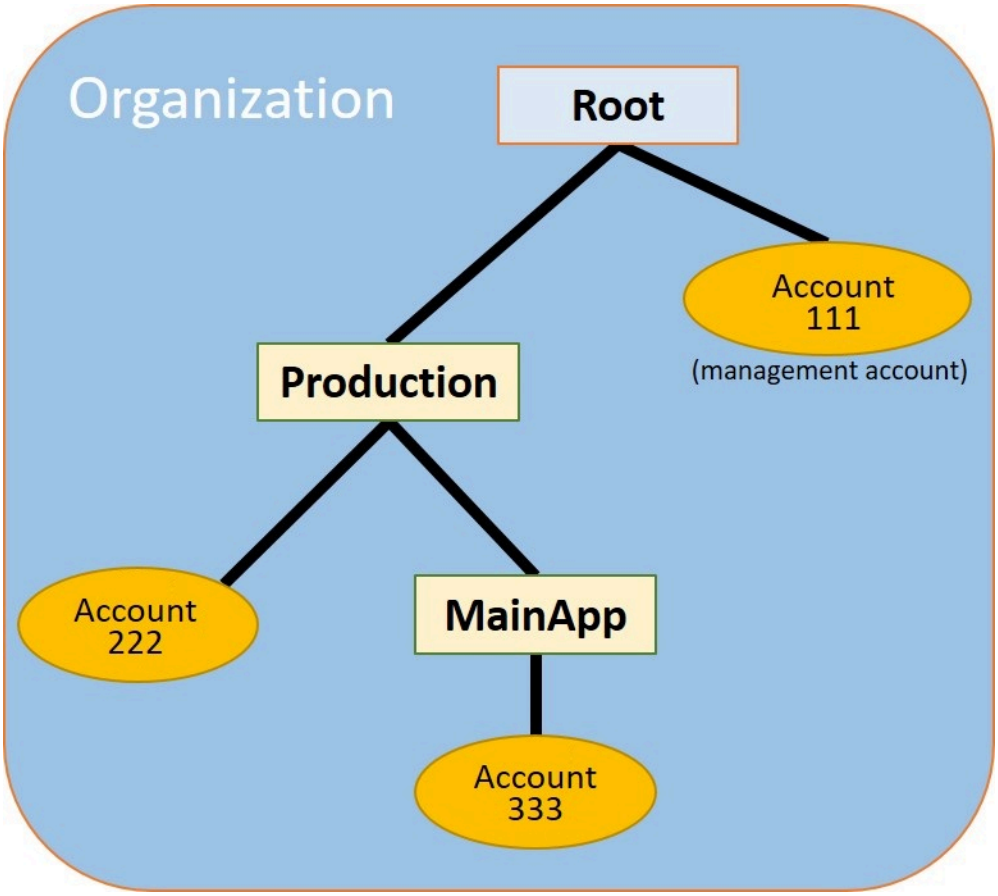
建立成員帳戶

1. 在 AWS Organizations 主控台上的 AWS 帳戶 頁面中，選擇 Add AWS 帳戶 (新增 AWS 帳戶帳戶)。
2. 在 Add an AWS 帳戶 (新增 AWS 帳戶 帳戶) 頁面上，選擇 Create an AWS 帳戶 (建立 AWS 帳戶 帳戶)。
3. 針對 AWS 帳戶 name (AWS 帳戶 帳戶名稱)，輸入帳戶的名稱，例如 **`MainApp Account`**。
4. 針對 Email address of the account's root user (帳戶根使用者的電子郵件地址)，輸入要為帳戶接收通訊的個人電子郵件地址。此值必須在全域必須是唯一的。沒有任兩個帳戶可以有相同的電子郵件地址。例如，您可以使用類似 **`mainapp@example.com`** 的內容。
5. 針對 IAM role name (IAM 角色名稱)，您可以將它保留空白，以自動使用 `OrganizationAccountAccessRole` 的預設角色名稱，或者您可以提供自己的名稱。此角色可讓您在以管理帳戶中 IAM 使用者的身分登入時存取新成員帳戶。在本教學中，請將它保留空白，以指示 AWS Organizations 使用預設名稱建立角色。
6. 選擇 Create AWS 帳戶 (建立 AWS 帳戶 帳戶)。您可能需要稍待片刻並重新整理頁面，才會看見新帳戶顯示在 AWS 帳戶 頁面。

> **Important**
>
> 如果您收到錯誤，指出您已超出組織的帳戶限制，或是因為您的組織仍在初始化，所以無法新增帳戶，請在建立組織後等待 1 小時，然後再試一次。如果錯誤仍然存在，請聯絡 AWS Support。

步驟 2：建立組織單位

在本節的步驟中，您會建立組織單位 (OU)，並將您的成員帳戶置放在其中。當您完成時，您的階層看起來會與下圖相似。管理帳戶會留在根中。一個成員帳戶已移至生產 OU，而另一個成員帳戶已移到生產的子系 MainApp OU 中。



AWS Management Console

若要建立並填入 OU

> **Note**
>
> 在接下來的步驟中，您可以與物件互動，您可以選擇物件本身的名稱或物件旁的選項按鈕。
>
> - 如果您選擇物件的名稱，則會開啟顯示物件詳細資訊的新頁面。
> - 如果您選擇物件旁邊的選項按鈕，則會識別要由其他動作執行的物件，例如選擇選單選項。
>
> 接下來的步驟會讓您選擇選項按鈕，以便您可以隨後透過選擇選單選項來處理關聯的物件。

1. 在 AWS Organizations 主控台上，導覽至 AWS 帳戶 頁面。

2. 選擇 Root (根) 容器旁邊的核取方塊

。
3. 在 Children (子項) 索引標籤上，選擇 Actions (動作)，然後在 Organizational unit (組織單位) 中，選擇 Create new (建立新的)。
4. 在 Create organizational unit in Root (在根中建立組織單位) 頁面，針對 Organizational unit name (組織單位名稱)，輸入 **`Production`**，然後選擇 Create organizational unit (建立組織單位)。
5. 選擇您的新 Production (生產) OU 旁邊的核取方塊

。
6. 選擇 Actions (動作)，然後在 Organizational unit (組織單位) 下，選擇 Create new (建立新的)。
7. 在 Create organizational unit in Production (在生產中建立組織單位) 頁面，針對第二個 OU 的名稱，輸入 **`MainApp`**，然後選擇 Create organizational unit (建立組織單位)。

   現在您可以將您的成員帳戶移到這些 OU。
8. 返回 AWS 帳戶 頁面，然後選擇 Production (生產) OU 旁邊的三角形

，以展開其下的樹狀目錄。這會顯示 MainApp OU 作為生產的子項。
9. 在 333333333333 旁邊，選擇核取方塊

(而不是其名稱)，選擇 Actions (動作)，然後在 AWS 帳戶 下，選擇 Move (移動)。
10. 在移動 AWS 帳戶 '333333333333' 頁面上，選擇生產環境旁邊的三角形以將其展開。在 MainApp (主應用程式) 旁邊，選擇單選按鈕

(而不是其名稱)，然後選擇 Move AWS 帳戶 (移動)。
11. 在 222222222222 旁邊，選擇核取方塊

(而不是其名稱)，選擇 Actions (動作)，然後在 AWS 帳戶 下，選擇 Move (移動)。
12. 在 Move AWS 帳戶 '222222222222' 頁面上，選擇 Production (生產) 旁邊的單選按鈕 (而非其名稱)，然後選擇 Move AWS 帳戶 (移動)。

步驟 3：建立服務控制政策

在本節的步驟中，您會建立三個服務控制政策 (SCP)，並將他們連接到根和 OU，以限制組織帳戶中的使用者可以執行的作業。第一個 SCP 會防止成員帳戶中的任何人建立或修改您設定的任何 AWS CloudTrail 日誌。管理帳戶不受任何 SCP 影響，因此在您套用 CloudTrail SCP 之後，您必須從管理帳戶建立任何日誌。

啟用組織的服務控制政策類型

在可以將任何類型的政策連接到根或根內的任何 OU 之前，您必須先啟用該組織的政策類型。預設不會啟用政策類型。本節中的步驟會說明如何為組織啟用服務控制政策 (SCP) 類型。

AWS Management Console

為組織啟用 SCP。

1. 導覽至 Policies (政策) 頁面，然後選擇 Service control policies (服務控制政策)。
2. 在 Service control policies (服務控制政策) 頁面中，選擇 Enable service control policies (啟用服務控制政策)。

   綠色橫幅即會出現，通知您現在可以在組織中建立 SCP。

建立 SCP

現在，組織中已啟用服務控制政策，您可以建立本教學課程所需的三項政策。

AWS Management Console

建立封鎖 CloudTrail 設定動作的第一個 SCP

1. 導覽至 Policies (政策) 頁面，然後選擇 Service control policies (服務控制政策)。
2. 在 Service control policies (服務控制政策) 頁面上，選擇 Create policy (建立政策)。
3. 針對 Policy name (政策名稱)，輸入 **`Block CloudTrail Configuration Actions`**。
4. 在 Policy (政策) 區段的右側服務清單中，針對服務選取 CloudTrail。然後選擇下列動作：AddTags、CreateTrail、DeleteTrail、RemoveTags、StartLogging、StopLogging 和 UpdateTrail。
5. 在右側窗格中選擇 Add resource (新增資源)，並指定 CloudTrail 和 All Resources (所有資源)。然後選擇 Add resource (新增資源)。

左側的政策陳述式看起來與以下內容相似。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1234567890123",
            "Effect": "Deny",
            "Action": [
                "cloudtrail:AddTags",
                "cloudtrail:CreateTrail",
                "cloudtrail:DeleteTrail",
                "cloudtrail:RemoveTags",
                "cloudtrail:StartLogging",
                "cloudtrail:StopLogging",
                "cloudtrail:UpdateTrail"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

6. 選擇建立政策。

第二個政策會定義您要為生產 OU 中使用者和角色啟用的所有服務及動作允許清單。完成之後，生產 OU 中的使用者便只會存取列出的服務和動作。

AWS Management Console

建立會為生產 OU 將核准的服務列入允許清單的第二個政策

1. 在 Service control policies (服務控制政策) 頁面中，選擇 Create policy (建立政策)。
2. 針對 Policy name (政策名稱)，輸入 **`Allow List for All Approved Services`**。
3. 將您的游標置放在 Policy (政策) 區段的右側窗格中，然後貼上政策，如下所示。

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

```
            "Sid": "Stmt1111111111111",
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "elasticloadbalancing:*",
                "codecommit:*",
                "cloudtrail:*",
                "codedeploy:*"
              ],
            "Resource": [ "*" ]
        }
    ]
}
```

4. 選擇建立政策。

最終政策會提供服務的拒絕清單，這些服務會遭到封鎖而無法在 MainApp OU 中使用。在本教學中，您會封鎖 MainApp OU 中的任何帳戶對 Amazon DynamoDB 的存取。

AWS Management Console

建立第三個政策來拒絕無法在 MainApp OU 中使用之服務的存取權

1. 在 Service control policies (服務控制政策) 頁面中，選擇 Create policy (建立政策)。
2. 針對 Policy name (政策名稱)，輸入 **`Deny List for MainApp Prohibited Services`**。
3. 在左側的 Policy (政策) 區段中，選取 Amazon DynamoDB 作為服務。針對動作，選擇 All actions (所有動作)。
4. 在左側窗格中選擇 Add resource (新增資源)，並指定 DynamoDB 和 All Resources (所有資源)。然後選擇 Add resource (新增資源)。

   右側的政策陳述式會進行更新，看起來與以下內容相似。

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

```
  ]
}
```

5. 選擇 Create policy (建立政策) 來儲存 SCP。

將 SCP 連接到您的 OU

現在 SCP 已存在，並且已為您的根帳戶啟用，您可以將它們連接到根帳戶和 OU。

AWS Management Console

將政策連接到根和 OU

1. 導覽至 AWS 帳戶 頁面。
2. 在 AWS 帳戶 頁面中，選擇 Root (根) (其名稱，而非單選按鈕)，以導覽至其詳細資訊頁面。
3. 在 Root (根) 詳細資訊頁面中，選擇 Policies (政策) 索引標籤，然後在 Service Control Policies (服務控制政策) 中，選擇 Attach (連接)。
4. 在 Attach a service control policy (連接服務控制政策) 頁面上，選擇名稱為 `Block CloudTrail Configuration Actions` 的 SCP 旁邊的選項按鈕，然後選擇 Attach (連接)。在此教學中，您會將其連接至根，從而會影響所有成員帳戶，以防止任何人改變您設定 CloudTrail 的方式。

   在 Root (根) 詳細資訊頁面，Policies (政策) 索引標籤現在會顯示連接至根的兩個 SCP：您剛剛連接的 SCP 和預設的 `FullAWSAccess` SCP。
5. 導覽回 AWS 帳戶 頁面，然後選擇 Production (生產) OU (其名稱，而非單選按鈕)，以導覽至其詳細資訊頁面。
6. 在 Production (生產) OU 的詳細資訊頁面中，選擇 Policies (政策) 索引標籤。
7. 在 Service Control Policies (服務控制政策) 中，選擇 Attach (連接)。
8. 在 Attach a service control policy (連接服務控制政策) 頁面上，選擇名 `Allow List for All Approved Services` 旁邊的選項按鈕，然後選擇 Attach (連接)。這可讓使用者或 Production (生產) OU 中成員帳戶的使用者或角色來存取核准的服務。
9. 選擇 Policies (政策) 索引標籤，查看連接至 OU 的那兩個 SCP：您剛剛連接的 SCP 和預設的 `FullAWSAccess` SCP。不過，因為 `FullAWSAccess` SCP 也在允許所有服務和動作的允許清單中，所以您現在必須分離此 SCP，以確保僅允許您所核准的服務。
10. 若要從 Production (生產) OU 移除預設政策，選擇 FullAWSAccess 選項按鈕，選擇 Detach (分離)，然後在確認對話方塊中，選擇 Detach policy (分離政策)。

移除此預設政策後，您在前面步驟中所連接允許清單 SCP 中的所有動作和服務，將立即無法提供 Production (生產) OU 下所有成員帳戶存取。任何對於使用不在 Allow List for All Approved Services (所有核准服務的允許清單) SCP 中之動作的請求都會遭到拒絕。即使帳戶中的管理員將 IAM 許可政策連接到其中一個成員帳戶的使用者，也是如此。

11. 現在您可以連接名為 `Deny List for MainApp Prohibited services` 的 SCP，防止 MainApp OU 中帳戶內的任何人使用任何受限制的服務。

    若要執行此動作，導覽至 AWS 帳戶 頁面，選擇三角形圖示以展開 Production (生產) OU 的分支，然後選擇 MainApp OU (其名稱，而非單選按鈕)，以導覽至其內容。

12. 在 MainApp 詳細資訊頁面，選擇 Policies (政策) 索引標籤。
13. 在 Service Control Policies (服務控制政策)，選擇 Attach (連接)，然後在可用政策的清單中，選擇 Deny List for MainApp Prohibited Services (拒絕 MainApp 禁止服務清單)，然後選擇 Attach policy (連接政策)。

步驟 4：測試您組織的政策

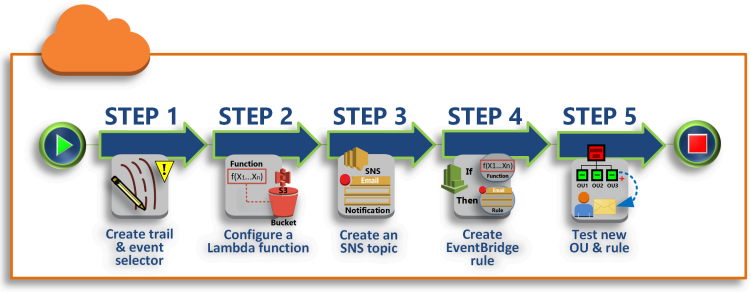
您現在可以以任何成員帳戶中的使用者身分登入，並嘗試執行各種 AWS 動作：

- 若您以管理帳戶中的使用者身分登入，您可以執行您 IAM 許可政策允許的任何操作。SCP 不會影響管理帳戶中的任何使用者或角色，無論帳戶位在哪一個根或 OU。
- 如果您以帳戶 222222222222 中的使用者身分登入，則可以執行允許清單所允許的任何動作。AWS Organizations 會拒絕執行不在允許清單之任何服務中動作的任何嘗試。同時，AWS Organizations 會拒絕嘗試執行其中一個 CloudTrail 組態動作。
- 如果您以帳戶 333333333333 中的使用者身分登入，您可以執行允許清單所允許，且未被拒絕清單所封鎖的任何動作。AWS Organizations 會拒絕所有嘗試執行不在允許清單的任何動作、以及在拒絕清單政策任何動作。同時，AWS Organizations 會拒絕嘗試執行其中一個 CloudTrail 組態動作。

教學課程：使用 Amazon EventBridge 監控您組織的重要變更

本教學課程說明如何設定 Amazon EventBridge、先前的 Amazon CloudWatch Events 來監控您組織的變更。首先設定規則，此規則會在使用者叫用特定 AWS Organizations 操作時觸發。接著，設定 Amazon EventBridge 在規則觸發時執行 AWS Lambda 函數，並設定 Amazon SNS 傳送電子郵件，內含關於此事件的詳細資訊。

下圖顯示教學的主要步驟。



步驟 1：設定追蹤記錄與事件選擇器

在 中建立稱為追蹤記錄AWS CloudTrail的日誌。您可以設定日誌來擷取所有 API 呼叫。

步驟 2：設定 Lambda 函數

建立 AWS Lambda 功能，此功能會將事件的相關詳細資訊記錄到 S3 儲存貯體。

步驟 3：建立傳送電子郵件給訂閱者的 Amazon SNS 主題

建立 Amazon SNS 主題，此主題會發送電子郵件給其訂閱者，然後讓訂閱者自行訂閱該主題。

步驟 4：建立 Amazon EventBridge 規則

建立規則，此規則會讓 Amazon EventBridge 將特定 API 呼叫的詳細資訊，傳給 Lambda 函數和 SNS 主題的訂閱者。

步驟 5：測試 Amazon EventBridge 規則

藉由執行其中一項受監控的操作，來測試您的新規則。在本教學課程中，受監控的操作會建立組織單位 (OU)。您可檢視 Lambda 函數所建立的日誌記錄，和檢視 Amazon SNS 傳送給訂閱者的電子郵件。

> **秘訣**
>
> 您也可以使用此教學作為設定類似操作 (例如在帳戶建立完成時傳送電子郵件通知) 的指南。由於帳戶建立是非同步的操作，當它完成時，您預設不會收到通知。如需有關搭配 AWS Organizations 使用 AWS CloudTrail 和 Amazon EventBridge 的詳細資訊，請參閱 AWS Organizations 中的記錄和監控。

先決條件

本教學課程的假設如下：

- 您可以從組織中的管理帳戶，以 IAM 使用者的身分登入 AWS Management Console。IAM 使用者必須擁有許可，以在 CloudTrail 中建立日誌、在 Lambda 中建立函數、在 Amazon SNS 中建立主題，以及在 Amazon EventBridge 中建立規則，並進行設定。如需關於授與許可的詳細資訊，請參閱 IAM 使用者指南中的存取管理，或針對您想要設定其存取的服務，參閱該服務的指南。
- 您可以存取現有的 Amazon Simple Storage Service (Amazon S3) 儲存貯體 (或者您擁有建立儲存貯體的許可)，來接收您在步驟 1 中所設定的 CloudTrail 日誌。

> **Important**
>
> 目前，AWS Organizations 只在美國東部 (維吉尼亞北部) 區域中託管 (雖然全球皆可使用)。若要執行此教學課程中的步驟，您必須設定 AWS Management Console 使用該區域。

步驟 1：設定追蹤記錄與事件選擇器

在此步驟中，您會登入管理帳戶，並且在 中設定日誌 (稱為追蹤記錄AWS CloudTrail)。您也會設定針對追蹤的事件選擇器，以擷取所有讀取/寫入 API 呼叫，以便 Amazon EventBridge 具有要觸發的呼叫。

若要建立追蹤記錄

1. 以組織管理帳戶管理員的身分登入 AWS，然後開啟位於 https://console.aws.amazon.com/cloudtrail/ 的 CloudTrail 主控台。
2. 在主控台右上角的導覽列中，選擇美國東部 (維吉尼亞北部) 區域。如果您選擇不同的區域，則在 Amazon EventBridge 的組態設定選項中不會出現 AWS Organizations，CloudTrail 也不會擷取關於 AWS Organizations 的資訊。
3. 在導覽窗格中，選擇 Trails (追蹤記錄)。
4. 選擇 Create trail (建立追蹤)。
5. 針對 Trail name (追蹤名稱)，輸入 **`My-Test-Trail`**。
6. 執行以下其中一個選項，指定 CloudTrail 交付其日誌的位置：
   - 如果您需要建立儲存貯體，請選擇 Create new S3 bucket (建立新的 S3 儲存貯體)，然後針對 Trail log bucket and folder (追蹤日誌儲存貯體和資料夾)，輸入新儲存貯體的名稱。

> **Note**
>
> S3 儲存貯體名稱必須在「全域」必須是唯一的。

- 如果您已經擁有儲存貯體，請選擇 Use existing S3 bucket (使用現有的 S3 儲存貯體)，然後從 S3 bucket (S3 儲存貯體) 清單中選擇儲存貯體的名稱。

7. 選擇 Next (下一步)。
8. 在 Choose log events (選擇日誌事件) 頁面的 Management events (管理事件) 區段中，選擇 Read (讀取) 和 Write (寫入)。
9. 選擇 Next (下一步)。
10. 檢閱選項，然後選擇 Create trail (建立追蹤)。

Amazon EventBridge 可讓您從幾種不同的方法中選擇其一，用來在警示規則符合傳入的 API 呼叫時傳送提醒。本教學示範兩種方法：叫用可以記錄 API 呼叫的 Lambda 函數，以及傳送資訊至 Amazon SNS 主題，而此主題會發送電子郵件或文字訊息給該主題的訂閱者。在接下來的兩個步驟中，會建立所需的元件：Lambda 函數和 Amazon SNS 主題。

步驟 2：設定 Lambda 函數

在此步驟中會建立 Lambda 函數，其中記錄根據 Amazon EventBridge 規則 (您稍後會進行設定) 傳送給該函數的 API 活動。

建立記錄 Amazon EventBridge 事件的 Lambda 函數

1. 開啟位於 AWS Lambda 的 https://console.aws.amazon.com/lambda/ 主控台。
2. 如果您是初次使用 Lambda，請選擇歡迎頁面上的 Get Started Now (立即開始使用)；否則請選擇 Create function (建立函數)。
3. 在 Create function (建立函數) 頁面上，選擇 Use a blueprint (使用藍圖)。
4. 從 Blueprints (藍圖) 搜尋方塊中，針對篩選條件輸入 **`hello`**，並選擇 hello-world 藍圖。
5. 選擇設定。
6. 在 Basic information (基本資訊) 頁面上，執行以下作業：

   a. 對於 Lambda 函數名稱，在 Name (名稱) 文字方塊中輸入 **`LogOrganizationEvents`**。

b. 針對 Role (角色)，選擇 Create a new role with basic Lambda permissions (建立具備基本 Lambda 許可的新角色)。此角色會授予許可給您的 Lambda 函數，讓函數存取所需的資訊和寫入其輸出日誌。

7. 如下列範例所示，編輯 Lambda 函數程式碼。

```
console.log('Loading function');

exports.handler = async (event, context) => {
    console.log('LogOrganizationsEvents');
    console.log('Received event:', JSON.stringify(event, null, 2));
    return event.key1;  // Echo back the first key value
    // throw new Error('Something went wrong');
};
```

此範本程式碼會記錄具有 **`LogOrganizationEvents`** 標記字串的事件，後面接續構成事件的 JSON 字串。

8. 選擇 建立函數。

步驟 3：建立傳送電子郵件給訂閱者的 Amazon SNS 主題

在此步驟中，您會建立一個 Amazon SNS 主題，此主題會透過電子郵件來傳送資訊給其訂閱者。這會讓此主題成為之後所建立 Amazon EventBridge 規則的目標。

若要建立 Amazon SNS 主題來傳送電子郵件給訂閱者

1. 在 https://console.aws.amazon.com/sns/v3/ 開啟 Amazon SNS 主控台。
2. 在導覽窗格中，選擇 Topics (主題)。
3. 請選擇 Create new topic (建立新主題)。

   a. 針對 Topic name (主題名稱)，輸入 **`OrganizationsCloudWatchTopic`**。

   b. 針對 Display name (顯示名稱)，輸入 **`OrgsCWEvnt`**。

   c. 請選擇 建立主題 。

4. 現在您可以建立該主題的訂閱。針對剛才所建立的主題，來選擇 ARN。
5. 選擇建立訂閱。

   a. 在 Create subscription (建立訂閱) 頁面上，針對 Protocol (通訊協定) 選擇 Email (電子郵件)。

   b. 針對 Endpoint (端點)，輸入電子郵件地址。

c. 選擇 Create subscription (建立訂閱)。AWS 會傳送一封電子郵件到您在先前步驟中指定的電子郵件地址。請等待該電子郵件送達，然後選取電子郵件中的 Confirm subscription (確認訂閱) 連結，來確認您已成功收到電子郵件。

d. 返回主控台並重新整理頁面。Pending confirmation (待確認) 訊息會關閉，改而顯示目前有效的訂閱 ID。

步驟 4：建立 Amazon EventBridge 規則

現在您帳戶中已經存在所需的 Lambda 函數，您可以建立 Amazon EventBridge 規則，以在規則中的條件滿足時叫用該函數。

若要建立 EventBridge 規則

1. 在 https://console.aws.amazon.com/events/ 開啟 Amazon EventBridge 主控台。
2. 將主控台設定為 US East (N. Virginia) (美國東部 (維吉尼亞北部)) 區域，否則組織的相關資訊將不可用。在主控台右上角的導覽列中，選擇美國東部 (維吉尼亞北部) 區域。
3. 如需有關建立規則的指示，請參閱 Amazon EventBridge user guide (《Amazon EventBridge 使用者指南》) 中的 Getting started with Amazon EventBridge (Amazon EventBridge 入門)。

步驟 5：測試 Amazon EventBridge 規則

在此步驟中，您會建立組織單位 (OU)、觀察 Amazon EventBridge 規則、產生日誌項目，並將電子郵件傳送給您自己，其中包含該事件的相關詳細資訊。

AWS Management Console

建立組織單位 (OU)

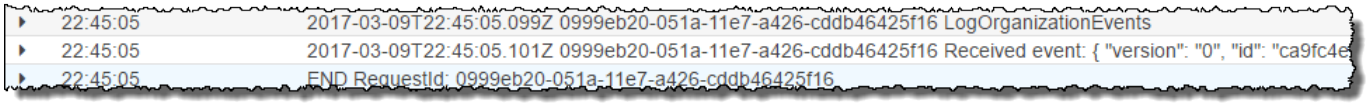
1. 在 AWS Organizations 主控台中開啟 AWS 帳戶 頁面。
2. 選擇核取方塊

   ☑

   Root (根) OU，選擇 Actions (動作)，然後在 Organizational unit (組織單位) 下，選擇 Create new (建立新的)。
3. 針對 OU 的名稱，輸入 **`TestCWEOU`**，然後選擇 Create organizational unit (建立組織單位)。

查看 EventBridge 日誌項目

1. 在 https://console.aws.amazon.com/cloudwatch/ 開啟 CloudWatch 主控台。
2. 在導覽頁面中，選擇 Logs (日誌)。
3. 在 Log Groups (日誌群組) 下方，選擇與您的 Lambda 函數：/aws/lambda/LogOrganizationEvents 關聯的群組。
4. 每個群組包含一或多個串流，而今天應該會有一個群組。請選擇此群組。
5. 檢視日誌。您應該會看到與以下內容相似的資料列。



6. 選取項目的中間資料列，檢視所接收事件的完整 JSON 文字。在輸出的 `requestParameters` 和 `responseElements` 片段中，可以看到 API 請求的所有詳細資訊。

```
2017-03-09T22:45:05.101Z 0999eb20-051a-11e7-a426-cddb46425f16 Received event:
{
    "version": "0",
    "id": "123456-EXAMPLE-GUID-123456",
    "detail-type": "AWS API Call via CloudTrail",
    "source": "aws.organizations",
    "account": "123456789012",
    "time": "2017-03-09T22:44:26Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "eventVersion": "1.04",
        "userIdentity": {
            ...
        },
        "eventTime": "2017-03-09T22:44:26Z",
        "eventSource": "organizations.amazonaws.com",
        "eventName": "CreateOrganizationalUnit",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "192.168.0.1",
        "userAgent": "AWS Organizations Console, aws-internal/3",
        "requestParameters": {
            "parentId": "r-exampleRootId",
            "name": "TestCWEOU"
        },
        "responseElements": {
```

```
            "organizationalUnit": {
                "name": "TestCWEOU",
                "id": "ou-exampleRootId-exampleOUId",
                "arn": "arn:aws:organizations::1234567789012:ou/o-exampleOrgId/ou-
exampleRootId-exampeOUId"
            }
        },
        "requestID": "123456-EXAMPLE-GUID-123456",
        "eventID": "123456-EXAMPLE-GUID-123456",
        "eventType": "AwsApiCall"
    }
}
```

7. 檢查您的電子郵件帳戶，看看是否有來自 OrgsCWEvnt (您 Amazon SNS 主題的顯示名稱) 的訊息。電子郵件的內文中，包含了與先前步驟所示日誌記錄相同的 JSON 文字輸出。

清除：移除不再需要的資源

為了避免產生費用，您應該刪除在此教學中建立但不想保留的所有 AWS 資源。

清除您的 AWS 環境

1. 使用 CloudTrail 主控台，來刪除您在步驟 1 中所建立的名稱為 **My-Test-Trail** 的追蹤。
2. 如果您在步驟 1 中建立了 Amazon S3 儲存貯體，則使用 Amazon S3 主控台來刪除該儲存貯體。
3. 使用 Lambda 主控台，來刪除您在步驟 2 中所建立名稱為 **LogOrganizationEvents** 的函數。
4. 使用Amazon SNS 主控台，來刪除您在步驟 3 中所建立的名稱為 **OrganizationsCloudWatchTopic** 的 Amazon SNS 主題。
5. 使用 CloudWatch 主控台，刪除您在步驟 4 中建立的名為 **OrgsMonitorRule** 的 EventBridge 規則。
6. 最後，使用 Organizations 主控台，來刪除您在步驟 5 中所建立名稱為 **TestCWEOU** 的 OU。

到此為止。在本教學課程中，您設定了 EventBridge 來監控組織的變更。您設定了規則，此規則會在使用者叫用特定 AWS Organizations 操作時觸發。此規則會執行記錄事件的 Lambda 函數，並傳送電子郵件，其中包含關於事件的詳細資訊。

多帳戶管理的最佳實務

請遵循下列建議，協助您逐步設定和管理 AWS Organizations 中的多帳戶環境。

主題

在單一組織內管理您的帳戶

我們建議您建立單一組織，並管理您在此組織內的所有帳戶。組織是一種安全性界限，可讓您在環境中維持各個帳戶之間的一致性。您可以跨組織內的帳戶集中套用政策或服務層級組態。如果您想要在多帳戶環境中啟用一致的政策、集中式可見性和程式設計控制，最好在單一組織中達成此目標。

為根使用者使用高強度密碼

我們建議您使用高強度且唯一的密碼。眾多密碼管理員和高強度密碼產生演算法和工具可協助您實現這些目標。如需詳細資訊，請參閱變更 AWS 帳戶根使用者 的密碼。使用您企業的資訊安全政策來管理長期儲存空間及根使用者密碼的存取。我們建議您將密碼儲存在符合組織安全性要求的密碼管理員系統或同等系統中。為了避免建立循環相依性，請勿使用依賴於 AWS 服務的工具來存放根使用者密碼，您會使用受保護帳戶登入該服務。無論您選擇哪種方法，我們都建議您優先考慮彈性，並可能考慮要求多

個參與者來授權存取此文件庫以獲得增強的保護。應記錄並監控任何對密碼的存取或其儲存位置。如需更多根使用者密碼建議，請參閱適用於 AWS 帳戶 的根使用者最佳實務。

記錄使用根使用者憑證的程序

記錄重要程序在執行時的效能，以確保您有每個步驟所涉及個人的記錄。若要管理密碼，我們建議使用安全的加密密碼管理器。提供有關可能發生的任何例外狀況和無法預見事件的文件也很重要。如需詳細資訊，請參閱 AWS 登入使用者指南中的疑難排解 AWS Management Console 登入問題和 IAM 使用者指南中的需要根使用者憑證的任務。

至少每個季度測試並驗證您是否繼續擁有根使用者的存取權，以及聯絡電話號碼。如此有助於向企業確認該程序正常運作，且您仍擁有根使用者的存取權。這也表示負責根存取權的人員瞭解為了讓程序成功而必須執行的步驟。若要增加回應時間和成功率，請務必確保所有參與程序的人員均確實瞭解在需要存取時必須執行的動作。

為您的根使用者啟用 MFA

我們建議您為 AWS 帳戶 中的 AWS 帳戶 根使用者和 IAM 使用者啟用多部多重要素驗證 (MFA) 裝置。這可讓您提高 AWS 帳戶 中的安全標準，並對高度權限使用者 (例如 AWS 帳戶 根使用者) 的存取權管理進行簡化。為了滿足不同的客戶需求，AWS 支援 IAM 三種類型的 MFA 裝置，包含 FIDO 安全金鑰、虛擬驗證器應用程式和以時間為基礎的一次性密碼 (TOTP) 硬體 Token。

每種驗證器類型的實體和安全屬性皆略有不同，最適合不同的使用案例。FIDO2 安全密鑰提供最高級別的安心保證，並且可防止網路釣魚陷阱。與僅使用密碼的驗證相比，任何形式的 MFA 均提供了更強大的安全狀態，我們強烈建議您將某種形式的 MFA 加入您的帳戶。選取最符合您安全性和營運需求的裝置類型。

如果您為主要驗證器選擇電池供電裝置 (例如 TOTP 硬體 Token)，請考慮同時註冊不依賴電池的驗證器作為備用機制。定期檢查裝置的功能並在到期日之前予以更換，這項作法對於保持不受中斷的存取極為重要。無論您選擇哪種類型的裝置，我們都建議至少註冊兩部裝置 (IAM 支援每位使用者最多八部 MFA 裝置)，藉此提高彈性以防止裝置遺失或故障。

請遵循組織針對儲存 MFA 裝置的資訊安全政策。建議您將 MFA 裝置與關聯的密碼分開存放。這可確保存取密碼和 MFA 裝置需要不同的資源 (人員、資料和工具)。這種隔離方式增加了一層額外的保護，防止未經授權的存取。我們也建議您記錄並監控對 MFA 裝置或其存放位置的任何存取。這有助於偵測並回應任何未經授權的存取。

如需詳細資訊，請參閱《IAM 使用者指南》中的使用多重要素驗證 (MFA) 保護您的根使用者登入。如需有關啟用 MFA 的指示，請參閱「在 AWS 中使用多重要素驗證 (MFA)」和「在 AWS 中為使用者啟用 MFA 裝置」。

套用控制以監控根使用者憑證的存取權

存取根使用者憑證應是罕見的事件。使用 Amazon EventBridge 之類的工具建立提醒，以宣告管理帳戶根使用者憑證的登入和使用。此警示應包含但不得限於根使用者本身所使用的電子郵件地址。此警示應該會很重要且很難會錯過。有關範例，請參閱監控和通知AWS 帳戶根使用者活動。請確認收到此類警示的人員瞭解如何驗證預期的根使用者存取權，以及如果他們認為安全事件正在進行中，該如何升級。如需詳細資訊，請參閱「回報可疑電子郵件」或「漏洞報告」。或者，您可以聯絡 AWS 以取得協助和其他指導。

讓聯絡電話號碼維持在最新狀態

若要恢復對您 AWS 帳戶 的存取權，請務必提供有效且目前正在使用的聯絡電話號碼，讓您可以接收簡訊或來電。我們建議您使用專用的電話號碼，確保 AWS 可以聯繫您以供帳戶支援和復原目的之用。您可以透過 AWS Management Console 或帳戶管理 API 輕鬆檢視並管理您帳戶的電話號碼。

有多種方法可以取得專用的電話號碼，確保 AWS 可以聯絡您。我們強烈建議您購買專用的 SIM 卡和實體電話。長期安全地存放手機和 SIM 卡，確保電話號碼仍可用於帳戶復原。還要確保負責行動帳單的團隊瞭解此號碼的重要性，即使號碼長時間不使用。您必須在組織內將此電話號碼保密以獲得額外的保護。

在「AWS 連絡人資訊」主控台頁面中記錄電話號碼，並與組織中必須瞭解此事項的特定團隊共用其詳細資訊。此方法有助於將電話號碼轉移到其他 SIM 卡的相關風險降至最低。根據您現有的資訊安全政策存放手機。不過，請勿將手機存放在與其他相關憑證資訊相同的位置。應記錄並監控任何對手機的存取或其儲存位置。如果與帳戶關聯的電話號碼有所更動，請實作程序以更新現有文件中的電話號碼。

使用適用於所有根帳戶的群組電子郵件地址

使用由您的企業管理的電子郵件地址。使用電子郵件地址，直接將收到的訊息轉寄給使用者群組。如果 AWS 必須聯絡帳戶的擁有者，例如，為了確認存取權，電子郵件訊息會分發給多個通話方。這種方法有助於減少回應延遲的風險，即使個人在度假、請病假或離開公司。

根據業務目的而非報告結構來群組工作負載

我們建議您將生產工作負載環境和資料隔離在頂層工作負載導向 OU 下。您的 OU 應以一組通用的控制項為基礎，而非仿照公司的報告結構。除了生產 OU 之外，我們建議您定義一或多個非生產 OU，其中包含用於開發和測試工作負載的帳戶和工作負載環境。如需其他指引，請參閱「組織以工作負載為導向的 OU」。

使用多個帳戶來組織您的工作負載

AWS 帳戶 可為您的 AWS 資源提供原生的安全性、存取權和帳單界限。使用多個帳戶有好處，因為它可以讓您分配帳戶級別配額和 API 請求率限制，並且享有此處列出的其他好處。我們建議您使用一些全組織的基本帳戶，例如安全性、記錄和基礎架構的帳戶。對於工作負載帳戶，您應該在不同帳戶中將生產工作負載與測試/開發工作負載分開。

使用服務主控台或 API/CLI 作業在組織層級啟用 AWS 服務

作為最佳實務，我們建議您啟用或停用任何您想要與使用該服務主控台的跨 AWS Organizations 整合的服務，或任何您想要與 API 作業/CLI 命令等效項目整合的服務。使用此方法，AWS 服務可以為您的組織執行所有必要的初始化步驟，例如在停用服務時建立任何必要的資源和清理資源。AWS Account Management 是唯一需要使用 AWS Organizations 主控台或 API 才能啟用的服務。若要檢閱與 AWS Organizations 整合的服務清單，請參閱 AWS 您可以搭配使用的服務 AWS Organizations。

使用帳單工具追蹤成本並最佳化資源用量

管理組織時，您會收到一份合併帳單，其中涵蓋了組織中帳戶的所有費用。對於需要存取成本可見度的企業使用者，您可以在管理帳戶中提供具有受限唯讀權限的角色來檢閱帳單和成本工具。例如，您可以建立可存取帳單報告的權限集，或使用 AWS Cost Explorer Service (檢視一段時間內成本趨勢的工具) 和成本效益服務 (例如 Amazon S3 Storage Lens 和 AWS Compute Optimizer)。

在組織資源中規劃標記策略並強制執行標籤

隨著帳戶和工作負載的擴展，標籤對於成本追蹤、存取控制和資源管理來說是一項實用的功能。對於標記命名策略，請遵循「標記您的 AWS 資源」中的指導。除了資源之外，您還可以在組織根目錄、帳戶、OU 和政策上建立標籤。請參閱「擬定您的標記策略」以取得其他資訊。

管理帳戶的最佳實務

請遵循這些推薦，協助保護 AWS Organizations 中管理帳戶的安全。這些推薦假設，您同時遵守僅將根使用者用於那些真正需要它的任務的最佳實務。

主題

限制有權存取管理帳戶的使用者

管理帳戶是所有上述管理任務的關鍵，例如帳戶管理、政策、與其他 AWS 服務的整合、合併計費等等。因此，您應該限制管理帳戶的存取權，並將此存取權侷限在需要權限來對組織進行變更的管理員使用者。

審查並追蹤誰擁有存取權

為確保您仍擁有管理帳戶的存取權，請定期檢閱您企業內有權存取與其關聯之電子郵件地址、密碼、MFA 和電話號碼的人員。將您的審查與現有的商業程序保持一致。為了確保只有正確的使用者才能存取，請新增此資訊的每月或每季審查。請確定，復原或重設根使用者憑證存取權的程序不依賴於任何特定個人來完成。所有程序都應解決人們無法使用的預期。

管理帳戶僅用於需要管理帳戶的任務

我們建議您僅將該管理帳戶及其使用者和角色用於必須僅由該帳戶執行的任務。將您的所有 AWS 資源存放在組織中的其他 AWS 帳戶 位置，並將其保存在管理帳戶之外。將資源保存在其他帳戶的一個重要原因是，因為 Organizations 服務控制政策 (SCP) 無法限制管理帳戶中的任何使用者或角色。將資源與管理帳戶分開，也會協助您瞭解發票上的費用。

避免將工作負載部署到組織的管理帳戶

獲得授權的作業可以在組織的管理帳戶內執行，SCP 不適用於管理帳戶。這就是為什麼您應該將管理帳戶中包含的雲端資源和資料限制為只能在管理帳戶中管理的資源和資料。

委派管理帳戶以外的職責來進行去集中化

如果可能的話，我們建議在管理帳戶之外委派職責和服務。為您的團隊提供自己帳戶中的權限，以便管理組織的需求，而無需存取管理帳戶。此外，您可以為支援此功能的服務 (例如可在整個組織中共用軟體的 AWS Service Catalog) 註冊多個委派管理員，或是用於編寫和部署堆疊的 AWS CloudFormation StackSets。

如需詳細資訊，請參閱安全性參考架構、使用多個帳戶組織您的 AWS 環境以及 AWS 您可以搭配使用的服務 AWS Organizations，以瞭解將成員帳戶註冊為各種 AWS 服務之委派管理員的建議。如需設定委派管理員的詳細資訊，請參閱為 AWS Account Management 啟用委派的管理員帳戶和 AWS Organizations 的委派管理員。

成員帳戶最佳實務

請遵循這些推薦，協助保護組織中成員帳戶的安全。這些推薦假設，您同時遵守僅將根使用者用於那些真正需要它的任務的最佳實務。

主題

- 定義帳戶名稱和屬性
- 有效率地擴展您的環境和帳戶使用情況
- 使用 SCP 來限制成員帳戶中根使用者可執行的動作

定義帳戶名稱和屬性

對於您的會員帳戶，請使用反映帳戶使用情況的命名結構和電子郵件地址。例如，`Workloads+fooA+dev@domain.com` 用於 `WorkloadsFooADev`，`Workloads+fooB+dev@domain.com` 用於 `WorkloadsFooBDev`。如果您已為組織定義了自訂標籤，建議您在反映帳戶使用情況、成本中心、環境和專案的帳戶上指派這些標籤。如此可讓您更容易識別、組織和搜尋帳戶。

有效率地擴展您的環境和帳戶使用情況

擴展規模時，在建立新帳戶之前，請確保不存在類似需求的帳戶，避免不必要的重複。AWS 帳戶 應根據常見的存取要求而定。如果您打算重複使用這些帳戶 (例如沙盒帳戶或同等帳戶)，建議您清除帳戶中不需要的資源或工作負載，但儲存帳戶以供日後使用。

關閉帳戶之前，請注意，這些帳戶必須遵守關閉帳戶配額限制。如需更多詳細資訊，請參閱 的配額 AWS Organizations。考慮實作清理過程以重複使用帳戶，而不是關閉帳戶，並在可能的情況下建立新帳戶。如此一來，您就可以避免因執行資源而產生成本，並達到 CloseAccount API 限制。

使用 SCP 來限制成員帳戶中根使用者可執行的動作

建議您在組織中建立服務控制政策 (SCP)，並將其附加至組織的根，以便套用至所有成員帳戶。如需詳細資訊，請參閱保護您的 Organizations 帳戶的根使用者登入資料。

您可以拒絕所有根動作，唯必須在成員帳戶中執行的特定僅限根動作除外。例如，下列 SCP 可防止任何成員帳戶中的根使用者進行任何 AWS 服務 API 呼叫，唯「更新設定錯誤且拒絕存取所有主體的 S3 儲存貯體政策」(這是其中一種需要根登入資料的動作) 除外。如需詳細資訊，請參閱 IAM 使用者指南中的需要根使用者憑證的任務。

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

    "Statement": [

        {

            "Effect": "Deny",

            "NotAction":[

            "s3:GetBucketPolicy",

            "s3:PutBucketPolicy",

            "s3:DeleteBucketPolicy"

                 ],

            "Resource": "*",

            "Condition": {
 "StringLike": { "aws:PrincipalArn": "arn:aws:iam::*:root" }

            }

        }

    ]
 }
```

在大多數情況下，任何管理任務都可由成員帳戶中具有相關管理員許可的 AWS Identity and Access Management (IAM) 角色執行。任何此類角色均應將套用適當的控制，以限制、記錄和監控活動。

建立和管理組織

您可以使用 AWS Organizations 主控台，或者執行 AWS Command Line Interface(AWS CLI) 命令或等效 AWS SDK API 操作來執行以下任務：

- 建立組織 建立您的組織，並使用您目前帳戶作為其管理帳戶。在您的組織內建立成員，並邀請其他帳戶加入您的組織。
- 啟用您組織的所有功能。啟用所有功能是使用 AWS Organizations 的慣用方式。當您建立組織時，您可以選擇啟用所有功能，或是僅啟用合併帳單的部分功能。預設會啟用所有功能，並且包含了合併帳單功能。

  啟用所有功能時，您可以使用 AWS Organizations 中提供的進階帳戶管理功能，像是服務控制政策 (SCP)。SCP 可讓您集中管理組織中所有帳戶可用的許可數上限，協助您確保帳戶符合您組織的存取控制準則。
- 檢視關於您組織的詳細資訊。檢視您的組織和其根帳戶、組織單位 (OU) 和帳戶的詳細資訊。
- 刪除組織。當您不再需要組織時，可刪除組織。

> **Note**
>
> 本節中的程序指定執行任務所需的最低許可。這些通常會套用到 API 或對命令列工具的存取。在主控台中執行任務可能需要額外的許可。例如，您可以對組織中的所有使用者授予唯讀許可，然後授予允許使用者執行特定任務的其他許可。

建立組織

您可以建立一個組織，從使用您的 AWS 帳戶 作為管理帳戶開始。建立組織時，您可以選擇組織是否支援所有功能 (建議) 或只支援合併帳單功能。

建立組織之後，您可以從管理帳戶透過以下方式將帳戶新增至您的組織：

- 建立會自動新增至組織作為成員帳戶的其他 AWS 帳戶 帳戶
- 驗證您的電子郵件地址後，邀請現有的 AWS 帳戶 加入您的組織作為成員帳戶

建立組織

您可以使用 AWS Management Console，或使用來自 AWS CLI 或其中一個 SDK API 的命令來建立組織。

最低許可

若要使用您目前的 AWS 帳戶 建立組織，您必須擁有以下許可：

- `organizations:CreateOrganization`
- `iam:CreateServiceLinkedRole`

  您可以將此許可限制為僅限服務委託人 `organizations.amazonaws.com`。

AWS Management Console

建立組織

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在預設情況下，您建立的組織會啟用所有功能。但是，您可以選擇下列其中一個步驟：

   - 若要建立已啟用所有功能的組織，在簡介頁面上，選擇 Create an organization (建立組織)。
   - 若要建立僅具有合併帳單功能的組織，請在「簡介」頁面和 Create an organization (建立組織) 下，選擇 consolidated billing features (合併帳單功能)，然後在 Confirmation (確認) 對話方塊中，選擇 Create an organization (建立組織)。

   如果您不小心選擇了錯誤的選項，您可以立即前往 Settings (設定) 頁面，然後選擇 Delete organization (刪除組織)，並重新開始
3. 組織會隨即建立，且 AWS 帳戶 頁面會隨即出現。唯一存在的帳戶是您的管理帳戶，並且其目前存放在根組織單位 (OU)。

   如有必要，Organizations 會自動傳送驗證電子郵件至與您管理帳戶關聯的地址。在您收到驗證電子郵件之前，可能會有一些延遲的時間。請在 24 小時內驗證您的電子郵件地址。如需詳細資訊，請參閱 電子郵件地址驗證。您可以建立帳戶以發展您的組織，而不驗證您的管理帳戶的電子郵件地址。不過，若要邀請現有的帳戶，您必須先完成電子郵件驗證。

> **Note**
>
> 如果此帳戶之前已驗證其電子郵件地址，則在您使用該帳戶建立組織時，就不會再發生這種情況。

AWS CLI & AWS SDKs

建立組織

您可以使用下列其中一項命令來建立組織：

- AWS CLI: create-organization

  下列範例會建立一個組織，並使目前登入的 AWS 帳戶 作為組織的管理帳戶。

```
$ aws organizations create-organization
{
    "Organization": {
        "Id": "o-aa111bb222",
        "Arn": "arn:aws:organizations::123456789012:organization/o-aa111bb222",
        "FeatureSet": "ALL",
        "MasterAccountArn": "arn:aws:organizations::123456789012:account/o-
aa111bb222/123456789012",
        "MasterAccountId": "123456789012",
        "MasterAccountEmail": "admin@example.com",
        "AvailablePolicyTypes": [  ...DEPRECATED - DO NOT USE ... ]
    }
}
```

  > **Important**
  >
  > 該 `AvailablePolicyTypes` 欄位已棄用，並且不包含有關在您的組織中啟用政策的準確資訊。若要查看實際針對組織啟用的準確且完整的政策類型清單，請使用 `ListRoots` 命令，如以下章節 AWS CLI 部分中所述。

- AWS SDKs: CreateOrganization

現在，您可以透過以下方式將其他帳戶新增至您的組織：

- 若要建立自動成為您的 AWS 組織一部分的 AWS 帳戶，請參閱在您的組織中建立成員帳戶。
- 若要邀請現有的帳戶加入您的組織，請參閱邀請加 AWS 帳戶 入您的組織。

電子郵件地址驗證

在您建立組織之後，以及在您可以邀請帳戶加入之前，必須驗證您擁有組織中為管理帳戶提供的電子郵件地址。

當您建立組織時，如果之前尚未驗證管理帳戶，AWS 會自動傳送驗證電子郵件到指定的電子郵件地址。在您收到驗證電子郵件之前，可能會有一些延遲的時間。

請在 24 小時內，遵循電子郵件中的指示來驗證您的電子郵件地址。

如果您未在 24 小時內驗證您的電子郵件地址，您可以重新發送請求，使得您可以邀請其他 AWS 帳戶加入您的組織。如果您未收到驗證電子郵件，請檢查您的電子郵件地址是否正確，並在必要時修改。

- 若要進一步了解與您的管理帳戶關聯的電子郵件地址，請參閱從管理帳戶檢視組織的詳細資訊。
- 若要變更與您的管理帳戶關聯的電子郵件地址，請參閱AWS Billing使用者指南中的管理 AWS 帳戶。

AWS Management Console

重新傳送驗證請求

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 導覽至 Settings (設定) 頁面，然後選擇 Send verification request (傳送驗證請求)。只有在未驗證管理帳戶時，才會出現此選項。
3. 請在 24 小時內驗證您的電子郵件地址。

   驗證您的電子郵件地址後，您將可邀請其他 AWS 帳戶 加入您的組織。如需詳細資訊，請參閱邀請加 AWS 帳戶 入您的組織。

若您變更管理帳戶的電子郵件地址，帳戶的狀態會回復到「電子郵件未驗證」，而您必須完成新電子郵件地址的驗證程序。

> **Note**
>
> 如果您在變更管理帳戶的電子郵件地址之前邀請帳戶加入組織，且這些邀請尚未被接受，則必須先驗證管理帳戶的新電子郵件地址，才能接受這些邀請。請使用上述程序重新傳送驗證請求。透過回覆電子郵件完成程序之後，您的受邀帳戶就可以接受邀請。

啟用組織中的所有功能

AWS Organizations 有兩個可用的功能集：

- 所有功能 – 此功能集是使用 AWS Organizations 的慣用方式，並包含了合併帳單功能。當您建立組織時，根據預設會啟用所有功能。啟用所有功能後，您就可以使用 AWS Organizations 中提供的進階帳戶管理功能，例如與支援的 AWS 服務整合和組織管理政策。
- 合併帳單功能 – 所有組織皆支援這項功能子集，提供基本的管理工具，可讓您用來集中管理組織中的帳戶。

若您建立僅具備合併帳單功能的組織，您可以在稍後啟用所有功能。本頁面描述啟用所有功能的程序。

啟用所有功能前

在從僅支援合併帳單功能的組織變更為支援所有功能的組織前，請注意下列事項：

- 當您啟用所有功能的程序時，AWS Organizations 會傳送請求到所有「受邀」加入您組織的成員帳戶。每個獲邀請的帳戶必須透過接受請求來核准啟用所有功能。只有這樣，您才能完成啟用組織中的所有功能的程序。如果帳戶拒絕請求，您必須從組織移除帳戶或重新傳送請求。您必須先接受請求，才能完成啟用所有功能的程序。您使用 AWS Organizations 建立的帳戶不會收到請求，因為他們不需要核准額外的控制。
- 您可以在啟用所有功能的同時，繼續邀請帳戶加入您的組織。受邀帳戶的擁有者會收到邀請通知，無論他們是加入僅合併帳單的組織，還是啟用了所有功能。
  - 如果您在啟用所有功能的程序期間邀請帳戶，邀請會指出他們所加入的組織已啟用所有功能。如果您在帳戶接受邀請之前取消啟用所有功能的程序，則該邀請會被取消。您必須再次邀請帳戶成為僅具備合併帳單功能之組織成員。
  - 如果您邀請帳戶但尚未接受邀請之前，您就會開始啟用所有功能的程序，該邀請會被取消，因為邀請指出該組織只有合併帳單功能。您必須再次邀請帳戶成為已啟用所有功能之組織的成員。
- 您也可以繼續在組織中建立帳戶。該程序不會受到此變更的影響。

- AWS Organizations 會驗證每個成員帳戶都具有名稱為 AWSServiceRoleForOrganizations 的服務連結角色。所有帳戶中均必須有此角色，才能啟用所有功能。如果您刪除獲邀請帳戶中的該角色，接受邀請會啟用重新建立角色的所有功能。如果您刪除使用 AWS Organizations 建立的帳戶中的角色，該帳戶會收到專門為了重新建立該角色的邀請。所有的邀請都必須獲得接受，組織才能完成啟用所有功能的程序。
- 由於啟用所有功能可讓您使用 SCP，請確認您的帳戶管理員了解將 SCP 連接到組織、組織單位或帳戶的效果。SCP 可限制受影響帳戶中使用者，甚至管理員可執行的作業。例如，管理帳戶可套用 SCP，防止成員帳戶離開組織。
- 管理帳戶不受任何 SCP 影響。您無法透過套用 SCP 來限制管理帳戶中使用者和角色可以執行的動作。SCP 只會影響成員帳戶。
- 從合併帳單功能到所有功能的移轉是單向的。啟用組織的所有功能之後，您就無法切換回僅具備合併帳單功能。
- (不推薦) 若您的組織只啟用了合併帳單功能，成員帳戶管理員可以選擇刪除名為 AWSServiceRoleForOrganizations 的服務連結角色。如果您稍後選擇啟用組織中的所有功能，這個角色便會是必要角色，並且做為接受啟用所有功能邀請的一部分，會在所有帳戶中重新建立。如需 AWS Organizations 如何使用此角色的詳細資訊，請參閱AWS Organizations 和服務連結角色。

開始啟用所有功能的程序

當您使用組織管理帳戶登入時，您可以開始啟用所有功能的程序。若要執行此動作，請執行下列步驟。

> **最低許可**
>
> 若要啟用組織中的所有功能，您必須擁有下列許可：
>
> - `organizations:EnableAllFeatures`
> - `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要

AWS Management Console

要求獲邀請的成員帳戶接受啟用組織中的所有功能

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。

2. 在 Settings (設定) 頁面中，選擇 Begin process to enable all features (開始啟用所有功能的程序)。
3. 在 Enable all features (啟用所有功能) 頁面上，確認您了解在切換後透過選擇 Begin process to enable all featers (開始程序以啟用所有功能)，無法傳回僅合併帳單功能。

   AWS Organizations 會傳送請求至組織中的每個受邀 (而非建立) 帳戶，要求進行核准以啟用組織中的所有功能。如果您有使用 AWS Organizations 建立的任何帳戶，並且成員帳戶管理員刪除了名為 `AWSServiceRoleForOrganizations` 的服務連結角色，AWS Organizations 會傳送請求給該帳戶，以重新建立角色。

   主控台會隨即顯示受邀帳戶的請求核准狀態清單。

   > **Tip**
   >
   > 若要稍後返回此頁面，請開啟 Settings (設定) 頁面，並在 Request sent date (已傳送請求日期) 區段中，選擇 View status (檢視狀態)。

4. Enable all features (啟用所有功能) 頁面會顯示組織中每個帳戶目前的請求狀態。已接受請求的帳戶會顯示 ACCEPTED (已接受) 狀態。尚未同意的帳戶會顯示 OPEN (未決) 狀態。

AWS CLI & AWS SDKs

要求獲邀請的成員帳戶接受啟用組織中的所有功能

您可以使用下列其中一項命令來啟用組織中的所有功能：

- AWS CLI: enable-all-features

  下列命令會開始在組織中啟用所有功能的程序。

```
$ aws organizations enable-all-features
{
    "Handshake": {
        "Id": "h-79d8f6f114ee4304a5e55397eEXAMPLE",
        "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
enable_all_features/h-79d8f6f114ee4304a5e55397eEXAMPLE",
        "Parties": [
            {
                "Id": "a1b2c3d4e5",
                "Type": "ORGANIZATION"
```

```
            }
        ],
        "State": "REQUESTED",
        "RequestedTimestamp": "2020-11-19T16:21:46.995000-08:00",
        "ExpirationTimestamp": "2021-02-17T16:21:46.995000-08:00",
        "Action": "ENABLE_ALL_FEATURES",
        "Resources": [
            {
                "Value": "o-a1b2c3d4e5",
                "Type": "ORGANIZATION"
            }
        ]
    }
}
```

輸出會顯示受邀成員帳戶必須同意的交握詳細資訊。

- AWS SDKs: EnableAllFeatures

> **備註**
>
> - 當請求傳送到成員帳戶時，即開始 90 天的倒數計時。所有帳戶必須在該時間內核准請求，否則請求會過期。如果請求過期，與此嘗試相關的所有請求都會取消，而且您必須從步驟 2 重新開始。
> - 一旦您要求啟用所有功能，現有未接受的帳戶邀請將全部遭到取消。
> - 在所有功能遷移過程中，您仍然可以啟動新帳戶邀請和建立新帳戶。

在組織中的所有受邀帳戶核准其請求之後，您就可以完成程序並啟用所有功能。如果您的組織沒有任何受邀成員帳戶，您也可以立即完成程序。若要完成此程序，請繼續完成啟用所有功能的程序。

核准啟用所有功能的請求或重新建立服務連結角色

以其中一個組織的受邀成員帳戶登入時，您可以從管理帳戶核准請求。如果您的帳戶原先獲邀請加入組織，該邀請是要啟用所有功能並隱含包含核准重新建立 AWSServiceRoleForOrganizations 角色 (必要時)。如果您的帳戶反而是使用 AWS Organizations 建立，而您刪除了 AWSServiceRoleForOrganizations 服務連結角色，您收到的邀請只會要重新建立角色。若要執行此動作，請執行下列步驟。

Important

如果您啟用所有功能，則組織中的管理帳戶可以對您的成員帳戶套用以政策為基礎的控制。對於使用者，甚至身為管理員的您，這些控制可以限制在您的帳戶中能夠執行什麼動作。這類限制可能會使您的帳戶無法離開組織。

最低許可

若要核准為您的成員帳戶啟用所有功能的請求，您必須擁有以下許可：

- `organizations:AcceptHandshake`
- `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要
- `organizations:ListHandshakesForAccount` – 僅在使用 Organizations 主控台時才需要
- `iam:CreateServiceLinkedRole` – 只有在必須在成員帳戶中重新建立 `AWSServiceRoleForOrganizations` 角色時才為必要

AWS Management Console

接受在組織中啟用所有功能的請求

1. 在 AWS Organizations 主控台，登入 AWS Organizations 主控台。您必須以 IAM 使用者的身分登入，擔任 IAM 角色，或以成員帳戶中的根使用者身分登入 (不建議)。
2. 了解接受組織中所有功能對您的帳戶所代表的意義，然後選擇 Accept (接受)。此頁面會繼續將程序顯示為未完成，直到組織中的所有帳戶接受請求，並且管理帳戶的管理員完成程序為止。

AWS CLI & AWS SDKs

接受在組織中啟用所有功能的請求

若要接受請求，您必須接受與 `"Action": "APPROVE_ALL_FEATURES"` 的交握。

- AWS CLI:
  - accept-handshake
  - list-handshakes-for-account

下列範例顯示如何列出帳戶可用的交握。輸出的第四行中 "Id" 的值是下一個命令所需的值。

```
$ aws organizations list-handshakes-for-account
{
    "Handshakes": [
        {
            "Id": "h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
            "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
approve_all_features/h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
            "Parties": [
                {
                    "Id": "a1b2c3d4e5",
                    "Type": "ORGANIZATION"
                },
                {
                    "Id": "111122223333",
                    "Type": "ACCOUNT"
                }
            ],
            "State": "OPEN",
            "RequestedTimestamp": "2020-11-19T16:35:24.824000-08:00",
            "ExpirationTimestamp": "2021-02-17T16:35:24.035000-08:00",
            "Action": "APPROVE_ALL_FEATURES",
            "Resources": [
                {
                    "Value": "c440da758cab44068cdafc812EXAMPLE",
                    "Type": "PARENT_HANDSHAKE"
                },
                {
                    "Value": "o-aa111bb222",
                    "Type": "ORGANIZATION"
                },
                {
                    "Value": "111122223333",
                    "Type": "ACCOUNT"
                }
            ]
        }
    ]
}
```

下列範例會使用上一個命令的交握 ID 來接受交握。

```
$ aws organizations accept-handshake --handshake-id h-
a2d6ecb7dbdc4540bc788200aEXAMPLE
{
    "Handshake": {
        "Id": "h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
        "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
approve_all_features/h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
        "Parties": [
            {
                "Id": "a1b2c3d4e5",
                "Type": "ORGANIZATION"
            },
            {
                "Id": "111122223333",
                "Type": "ACCOUNT"
            }
        ],
        "State": "ACCEPTED",
        "RequestedTimestamp": "2020-11-19T16:35:24.824000-08:00",
        "ExpirationTimestamp": "2021-02-17T16:35:24.035000-08:00",
        "Action": "APPROVE_ALL_FEATURES",
        "Resources": [
            {
                "Value": "c440da758cab44068cdafc812EXAMPLE",
                "Type": "PARENT_HANDSHAKE"
            },
            {
                "Value": "o-aa111bb222",
                "Type": "ORGANIZATION"
            },
            {
                "Value": "111122223333",
                "Type": "ACCOUNT"
            }
        ]
    }
}
```

- AWS SDKs:
  - list-handshakes-for-account
  - AcceptHandshake

完成啟用所有功能的程序

所有獲邀的成員帳戶都需核准請求，才能啟用所有功能。如果組織中沒有任何獲邀請的成員帳戶，Enable all features progress (啟用組織中的所有功能進度) 頁面會以綠色橫幅表示您可以完成程序。

最低許可

若要完成啟用組織中的所有功能的程序，您必須擁有下列許可：

- `organizations:AcceptHandshake`
- `organizations:ListHandshakesForOrganization`
- `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要

AWS Management Console

完成啟用所有功能的程序

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Settings (設定) 頁面上，如果所有受邀帳戶接受啟用所有功能的請求，頁面上方會出現綠色方塊，以便通知您。在綠色方塊中，選擇 Go to finalize (前往完成)。
3. 在 Enable all features (啟用所有功能) 頁面中，選擇 Finalize (完成)，然後在確認對話方塊中，選擇 Finalize (完成)。
4. 組織現在已啟用所有功能。

AWS CLI & AWS SDKs

完成啟用所有功能的程序

若要完成該程序，您必須接受與 `"Action": "ENABLE_ALL_FEATURES"` 的交握。

- AWS CLI:
  - list-handshakes-for-organization
  - accept-handshake

```
$ aws organizations list-handshakes-for-organization
```

```
{
    "Handshakes": [
        {
            "Id": "h-43a871103e4c4ee399868fbf2EXAMPLE",
            "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
enable_all_features/h-43a871103e4c4ee399868fbf2EXAMPLE",
            "Parties": [
                {
                    "Id": "a1b2c3d4e5",
                    "Type": "ORGANIZATION"
                }
            ],
            "State": "OPEN",
            "RequestedTimestamp": "2020-11-20T08:41:48.047000-08:00",
            "ExpirationTimestamp": "2021-02-18T08:41:48.047000-08:00",
            "Action": "ENABLE_ALL_FEATURES",
            "Resources": [
                {
                    "Value": "o-aa111bb222",
                    "Type": "ORGANIZATION"
                }
            ]
        }
    ]
}
```

下列範例示範如何列出組織可用的交握。輸出的第四行中 "Id" 的值是下一個命令所需的值。

```
$ aws organizations accept-handshake \
    --handshake-id h-43a871103e4c4ee399868fbf2EXAMPLE
{
    "Handshake": {
        "Id": "h-43a871103e4c4ee399868fbf2EXAMPLE",
        "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
enable_all_features/h-43a871103e4c4ee399868fbf2EXAMPLE",
        "Parties": [
            {
                "Id": "a1b2c3d4e5",
                "Type": "ORGANIZATION"
            }
        ],
        "State": "ACCEPTED",
        "RequestedTimestamp": "2020-11-20T08:41:48.047000-08:00",
```

```
        "ExpirationTimestamp": "2021-02-18T08:41:48.047000-08:00",
        "Action": "ENABLE_ALL_FEATURES",
        "Resources": [
            {
                "Value": "o-aa111bb222",
                "Type": "ORGANIZATION"
            }
        ]
    }
}
```

- AWS SDKs:
  - AcceptHandshake
  - AcceptHandshake

後續步驟：

- 啟用您要使用的政策類型。之後，您可以將政策連接，以管理組織中的帳戶。如需更多詳細資訊，請參閱 管理 AWS Organizations 中的政策。
- 啟用與支援服務的整合。如需更多詳細資訊，請參閱 搭配使用 AWS Organizations 與其他 AWS 服務。

檢視關於您的組織的詳細資訊

您可以執行下列任務來檢視有關組織元素的詳細資訊。

主題

- 從管理帳戶檢視組織的詳細資訊
- 檢視根容器的詳細資訊
- 檢視 OU 的詳細資訊
- 檢視帳戶的詳細資訊
- 檢視政策的詳細資訊

從管理帳戶檢視組織的詳細資訊

在 AWS Organizations 主控台登入組織的管理帳戶時，您可以檢視組織的詳細資訊。

最低許可

若要檢視組織的詳細資訊，您必須擁有以下許可：

- `organizations:DescribeOrganization`

AWS Management Console

檢視您的組織的詳細資訊

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 瀏覽至 Settings (設定) 頁面。此頁面會顯示有關組織的詳細資訊，包括組織 ID、帳戶名稱和指派給組織管理帳戶的電子郵件地址。

AWS CLI & AWS SDKs

檢視您的組織的詳細資訊

您可以使用下列其中一項命令來檢視組織的詳細資訊：

- AWS CLI: describe-organization

以下範例顯示此命令輸出中包含的資訊。

```
$ aws organizations describe-organization
{
    "Organization": {
        "Id": "o-aa111bb222",
        "Arn": "arn:aws:organizations::123456789012:organization/o-aa111bb222",
        "FeatureSet": "ALL",
        "MasterAccountArn": "arn:aws:organizations::128716708097:account/o-
aa111bb222/123456789012",
        "MasterAccountId": "123456789012",
        "MasterAccountEmail": "admin@example.com",
        "AvailablePolicyTypes": [ ...DEPRECATED - DO NOT USE... ]
    }
}
```

> **Important**
>
> 該 `AvailablePolicyTypes` 欄位已棄用，並且不包含有關在您的組織中啟用政策的準確資訊。若要查看實際針對組織啟用的準確且完整的政策類型清單，請使用 `ListRoots` 命令，如以下章節 AWS CLI 部分中所述。

- AWS SDKs: DescribeOrganization

檢視根容器的詳細資訊

在 AWS Organizations 主控台登入組織的管理帳戶時，您可以檢視根容器的詳細資訊。

> **最低許可**
>
> 若要檢視根的詳細資訊，您必須擁有以下許可：
>
> - `organizations:DescribeOrganization` (僅限主控台)
> - `organizations:ListRoots`

根是組織單位 (OU) 階層中最上層的容器，而且通常會像 OU 一樣運作。不過，由於階層最頂端的容器，對根的變更會影響組織中其他所有 OU 和每個 AWS 帳戶。

AWS Management Console

檢視根的詳細資訊

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 導覽至 AWS 帳戶 頁面，然後選擇 Root (根) OU (其名稱，而非選項按鈕)。
3. Root (根) 詳細資訊會隨即出現，並顯示根的詳細資訊。

AWS CLI & AWS SDKs

檢視根的詳細資訊

您可以使用下列其中一項命令來檢視根帳戶的詳細資訊：

- AWS CLI: list-roots

  以下範例顯示如何擷取根的詳細資訊，包括目前在組織中啟用的政策類型：

```
$ aws organizations list-roots
{
    "Roots": [
        {
            "Id": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "PolicyTypes": [
                {
                    "Type": "BACKUP_POLICY",
                    "Status": "ENABLED"
                }
            ]
        }
    ]
}
```

- AWS SDKs: ListRoots

檢視 OU 的詳細資訊

在 AWS Organizations 主控台登入組織的管理帳戶時，您可以檢視組織中 OU 的詳細資訊。

最低許可

若要檢視組織單位 (OU) 的詳細資訊，您必須擁有以下許可：

- `organizations:DescribeOrganizationalUnit`
- `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要
- `organizations:ListOrganizationsUnitsForParent` – 僅在使用 Organizations 主控台時才需要
- `organizations:ListRoots` – 僅在使用 Organizations 主控台時才需要

AWS Management Console

檢視 OU 的詳細資訊

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 AWS 帳戶 頁面上，選擇您要檢查的 OU (而非選項按鈕) 名稱。如果您所需的 OU 是另一個 OU 的子項，選擇其父項 OU 旁邊的三角形圖示以將其展開，並查看階層下一級中的那些項目。重複此操作，直至您找到所需的 OU。

   Organizational unit details (組織單位詳細資訊) 方塊會顯示 OU 的相關資訊。

AWS CLI & AWS SDKs

檢視 OU 的詳細資訊

您可以使用下列命令來檢視 OU 的詳細資訊：

- AWS CLI, AWS SDKs:
  - list-roots
  - list-children
  - describe-organizational-unit

以下範例顯示如何使用 AWS CLI 來尋找 OU 的 ID。您可以透過從 `list-roots` 命令開始周遊階層，然後在根上執行 `list-children` 並對其每個子項反覆執行，來尋找 OU ID，直至找到您所需的一個。

```
$ aws organizations list-roots
{
    "Roots": [
        {
            "Id": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "PolicyTypes": []
        }
    ]
}
$ aws organizations list-children --parent-id r-a1b2 --child-type
 ORGANIZATIONAL_UNIT
```

```
{
    "Children": [
        {
            "Id": "ou-a1b2-f6g7h111",
            "Type": "ORGANIZATIONAL_UNIT"
        }
    ]
}
```

取得 OU ID 之後，下列範例顯示如何擷取 OU 的詳細資訊。

```
$ aws organizations describe-organizational-unit --organizational-unit-id ou-a1b2-
f6g7h111
{
    "OrganizationalUnit": {
        "Id": "ou-a1b2-f6g7h111",
        "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h111",
        "Name": "Production-Apps"
    }
}
```

- AWS SDKs:
  - ListRoots
  - ListChildren
  - DescribeOrganizationalUnit

檢視帳戶的詳細資訊

在 AWS Organizations 主控台登入組織的主帳戶時，您可以檢視帳戶的詳細資訊。

最低許可

若要檢視 AWS 帳戶 的詳細資訊，您必須擁有以下許可：

- `organizations:DescribeAccount`
- `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要
- `organizations:ListAccounts` – 僅在使用 Organizations 主控台時才需要

AWS Management Console

檢視 AWS 帳戶 的詳細資訊

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 導覽至 AWS 帳戶 頁面，然後選擇您要檢查的帳戶名稱 (而非選項按鈕)。如果您所需的帳戶是 OU 的子項，您可能需要選擇三角形圖示 ▶ ，以將其展開並查看其子項。重複此步驟，直到找到帳戶為止。

   Account details (帳戶詳細資訊) 方塊會顯示帳戶的相關資訊。

AWS CLI & AWS SDKs

檢視 AWS 帳戶 的詳細資訊

您可以使用下列命令來檢視帳戶的詳細資訊：

- AWS CLI:
  - list-accounts – 列出組織中所有帳戶的詳細資訊
  - describe-account – 僅列出指定帳戶的詳細資訊

  這兩個命令會針對回應中包含的每個帳戶傳回相同的詳細資訊。

  以下範例顯示如何擷取指定帳戶的詳細資訊。

```
$ aws organizations describe-account --account-id 123456789012

{
    "Account": {
        "Id": "123456789012",
        "Arn": "arn:aws:organizations::123456789012:account/o-
aa111bb222/123456789012",
        "Email": "admin@example.com",
        "Name": "Example.com Organization's Management Account",
        "Status": "ACTIVE",
        "JoinedMethod": "INVITED",
        "JoinedTimestamp": "2020-11-20T09:04:20.346000-08:00"
    }
```

```
}
```

- AWS SDKs:
  - ListAccounts
  - DescribeAccount

檢視政策的詳細資訊

在 AWS Organizations 主控台登入組織的主帳戶時，您可以檢視政策的詳細資訊。

> **最低許可**
>
> 若要檢視政策的詳細資訊，您必須擁有下列許可：
>
> - `organizations:DescribePolicy`
> - `organizations:ListPolicies`

AWS Management Console

檢視政策詳細資訊

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 執行下列其中一項：
   - 導覽至 Policies (政策) 頁面上，然後選擇您要檢查的政策的政策類型。
   - 導覽至 AWS 帳戶 頁面上，然後導覽至政策所連接的 OU 或帳戶。最後，請選擇 Policies (政策) 索引標籤,以查看連接政策的清單。
3. 選擇政策的名稱 (而非選項按鈕)。

   在政策 Details (詳細資訊) 頁面上，您可以檢視政策的所有相關資訊，包括 JSON 政策文字，以及政策所連接的 OU 和帳戶清單。

AWS CLI & AWS SDKs

檢視政策詳細資訊

您可以使用以下其中一個命令來檢視政策的詳細資訊：

- AWS CLI:
  - : list-policies
  - describe-policy – 僅列出指定政策的詳細資訊

  以下範例顯示如何尋找您要檢閱的政策的政策 ID。您必須指定政策類型，且命令只會傳回該類型的所有政策。

```
$ aws organizations list-policies --filter BACKUP_POLICY
{
    "Policies": [
        {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "test-backup-policy",
            "Description": "test-policy-description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        }
    ]
}
```

  回應包含除 JSON 政策文件之外的所有詳細資訊。

  下列範例顯示如何擷取僅指定政策的詳細資訊，包括 JSON 政策文件。

```
$ aws organizations describe-policy --policy-id p-i9j8k7l6m5
{
    "Policies": [
        {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "test-backup-policy",
            "Description": "test-policy-description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"plans\":{\"My-Backup-Plan\":{\"regions\":{\"@@assign\":
[\"us-west-2\"]},\"rules\":{\"My-Backup-Rule\"
```

```
                    :{\"target_backup_vault_name\":{\"@@assign\":\"My-Primary-
Backup-Vault\"}}},\"selections\":{\"tags\":{
                    \"My-Backup-Plan-Resource-Assignment\":{\"iam_role_arn\":
{\"@@assign\":\"arn:aws:iam::$account:role/
                    My-Backup-Role\"},\"tag_key\":{\"@@assign\":\"Stage\"},
\"tag_value\":{\"@@assign\":[\"Production\"]}}}}}}}"
    ]
}
```

- AWS SDKs:
  - ListPolicies
  - DescribePolicy

刪除組織

當您不再需要您的組織時，可以將它刪除。刪除組織並不會關閉管理帳戶，而是會從組織移除管理帳戶並刪除組織本身。先前的管理帳戶會變成不再由 AWS Organizations 管理的獨立 AWS 帳戶。然後，您有三個選項：您可以繼續使用它作為獨立帳戶、您可以用它來建立不同的組織，或者您可以接受來自其他組織的邀請，將帳戶新增至該組織作為成員帳戶。

Important

- 如果您刪除某個組織，則無法復原該組織。如果您已在組織內建立任何政策，則也會將它們刪除且無法對其復原。
- 只有在從組織移除所有成員帳戶之後，您才能夠刪除該組織。如果是使用 AWS Organizations 建立了您的一些成員帳戶，您可能會無法移除這些帳戶。只有在成員帳戶具有以獨立 AWS 帳戶 形式運作所需的所有資訊時，您才可以移除該成員帳戶。如需有關如何提供該資訊和移除帳戶的詳細資訊，請參閱從成員帳戶離開組織。
- 如果您在將成員帳戶從組織中移除之前，已關閉成員帳戶，它會進入「暫停」狀態一段時間，而且在最終關閉之前，您無法從組織中移除該帳戶。這最多可能需要 90 天的時間，而且可能會讓您在此之前無法刪除組織，直至所有成員帳戶都完全關閉。

透過刪除組織來從組織中移除管理帳戶時，可能會以下列方式來影響帳戶：

- 該帳戶只負責支付自己的費用，並且不再負責其他任何帳戶衍生的費用。

- 與其他服務的整合可能會停用。例如，AWS IAM Identity Center 需要組織來操作，因此，如果您從支援 IAM Identity Center 的組織移除某個帳戶，在該帳戶中的使用者將不再可使用該服務。

組織的管理帳戶絕不會受到服務控制政策 (SCP) 的影響，因此在 SCP 不再可用之後，許可中沒有變更。

主題

刪除組織

請使用下列程序來刪除組織，該組織會將先前的管理帳戶還原為不再由 AWS Organizations 管理的獨立帳戶 AWS 帳戶。

> **最低許可**
>
> 若要刪除組織，您必須以管理帳戶中的使用者或角色的身分登入，且您必須擁有以下許可：
>
> - `organizations:DeleteOrganization`
> - `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要

AWS Management Console

若要刪除組織

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在您能夠刪除組織之前，您必須先從組織移除所有帳戶。如需更多詳細資訊，請參閱 從組織移除成員帳戶。
3. 導覽至 Settings (設定) 頁面，然後選擇 Delete organization (刪除組織)。
4. 在 Delete organization (刪除組織) 確認對話方塊中，輸入顯示在文字方塊上方行中的組織 ID。然後，選擇 Delete organization (刪除組織)。

> **Important**
>
> 此作業不會關閉管理帳戶，但會將其退回至獨立帳戶 AWS 帳戶。若要關閉帳戶，請遵循 關閉組織中的成員帳戶 中的步驟。

AWS CLI & AWS SDKs

若要刪除組織

使用下列其中一項命令來刪除組織：

- AWS CLI: delete-organization

  以下範例會刪除使用其憑證的 AWS 帳戶 為管理帳戶的組織。

  ```
  $ aws organizations delete-organization
  ```

  此命令成功後就不會產生輸出。
- AWS SDKs: DeleteOrganization

管理您的組織中的 AWS 帳戶

組織是指您集中管理的 AWS 帳戶 集合。您可以執行以下任務來管理屬於您的組織一部分的帳戶：

- 檢視組織中帳戶的詳細資訊。您可以檢視帳戶的唯一 ID 號碼、其 Amazon Resource Name (ARN) 和其連接的政策。
- 匯出組織中所有 AWS 帳戶 的清單。您可以下載 .csv 檔案，其中包含組織內每個帳戶的帳戶詳細資訊。
- 邀請現有的 AWS 帳戶 加入您的組織。建立邀請、管理您建立的邀請，以及接受或拒絕邀請。
- 隨著您的組織建立 AWS 帳戶。自動建立和存取自動成為組織的一部分的 AWS 帳戶。
- 更新組織中的替代聯絡人。更新組織中的 AWS 帳戶 替代聯絡人。
- 從您的組織移除 AWS 帳戶。以管理帳戶的管理員身分，移除您不再要從組織管理的成員帳戶。以成員帳戶的管理員身分，從其組織移除您的帳戶。如果管理帳戶有與您的成員帳戶連接的政策，可能會封鎖您使您無法移除帳戶。
- 刪除 (或關閉) AWS 帳戶。當您不再需要 AWS 帳戶，您可以關閉帳戶以防止任何使用費或費用累積。

在一個組織中的影響

- 對加入組織的 AWS 帳戶 有什麼影響？
- 對在組織中建立的 AWS 帳戶 有什麼影響？

對加入組織的 AWS 帳戶 有什麼影響？

邀請 AWS 帳戶 加入組織，而該帳戶的擁有者接受邀請時，AWS Organizations 會自動對新成員帳戶進行下列變更：

- AWS Organizations 建立稱為 `AWSServiceRoleForOrganizations` 的服務連結角色。如果您的組織支援所有功能，則帳戶必須擁有此角色。只有在組織僅支援合併帳單功能集時，您才可以刪除角色。如果您刪除角色並稍後啟用組織中的所有功能，則 AWS Organizations 會為帳戶重新建立角色。
- 您可能有各種政策連接至組織根或包含該帳戶的 OU。如果是這樣，那些政策會立即套用至受邀帳戶中的所有使用者和角色。

- 您可以在組織中針對其他 AWS 服務啟用服務信任。當您這麼做時，該受信任的服務就可以在組織中的任何成員帳戶 (包括受邀的帳戶) 中，建立服務連結角色或執行動作。

> **Note**
>
> 對於受邀的成員帳戶，AWS Organizations不會自動建立 IAM 角色OrganizationAccountAccessRole。該角色會授予管理帳戶中的使用者存取成員帳戶的管理權限。如果想要啟用對邀請帳戶的該層級管理控制，可以手動新增該角色。如需詳細資訊，請參閱 在受邀 OrganizationAccountAccessRole 的成員帳戶中建立。

您可以邀請帳戶加入只啟用合併帳單功能的組織。如果您稍後想要為組織啟用所有功能，受邀帳戶必須核准變更。

對您在組織中建立的 AWS 帳戶 有哪些影響？

在您的組織中建立 AWS 帳戶 時，AWS Organizations 會自動對新的成員帳戶進行下列變更：

- AWS Organizations 建立稱為 `AWSServiceRoleForOrganizations` 的服務連結角色。如果您的組織支援所有功能，則帳戶必須擁有此角色。只有在組織僅支援合併帳單功能集時，您才可以刪除角色。如果您刪除角色並稍後啟用組織中的所有功能，則 AWS Organizations 會為帳戶重新建立角色。
- AWS Organizations建立 IAM 角色OrganizationAccountAccessRole。此角色會對新成員帳戶授予管理帳戶存取權。雖然可刪除該角色，建議您不要將其刪除，以便作為復原選項使用。
- 如果您有任何 政策連接到 OU 樹狀目錄的根，這些政策會立即套用到所建立帳戶中的所有使用者和角色。預設情況下，新帳戶會新增到根帳戶 OU。
- 如果您已為組織的另一個 AWS 服務啟用服務信任，該信任服務可以在組織的任何成員帳戶中 (包括您建立的帳戶) 建立服務連結角色或執行動作。

邀請加 AWS 帳戶 入您的組織

建立組織並確認您擁有與管理帳戶相關聯的電子郵件地址之後，您就可以邀請現有的組織 AWS 帳戶加入您的組織。

當您邀請帳戶時， AWS Organizations 會傳送邀請給帳戶擁有者，帳戶擁有者決定要接受還是拒絕邀請。您可以使用主 AWS Organizations 控台來啟動和管理傳送給其他帳戶的邀請。您只能從組織的管理帳戶傳送邀請給另一個帳戶。

> **Note**
>
> 所有帳戶的帳單歷史記錄和報告會保留在 Organization 中的付款人帳戶內。在您將帳戶移至新的 Organization 之前，請先下載任何您想要保留的成員帳戶的帳單和報告記錄。這可能包括成本和用量報告、詳細帳單報告或 Cost Explorer 服務產生的報告。

如果您是的管理員 AWS 帳戶，您也可以接受或拒絕來自組織的邀請。如果您接受，您的帳戶會變成該組織的成員。您的帳戶只可以加入一個組織，因此，如果您收到多個加入的邀請，您只能接受一個。

在帳戶接受邀請加入組織時，組織的管理帳戶將負責新成員帳戶累積的所有費用。不再使用連接至成員帳戶的付款方式。而是連接至組織管理帳戶的付款方式來支付成員帳戶產生的所有費用。

當受邀帳戶加入您的組織，且您的組織處於 [所有功能] 模式時，管理帳戶具有受邀成員帳戶的完整管理存取權和控制權。不過，與建立的帳戶不同，`OrganizationAccountAccessRole`IAM 角色不會在具有管理帳戶許可的成員帳戶中自動建立。若要在受邀的帳戶成為成員之後建立並設定此項目，請依照下列步驟執行在受邀 OrganizationAccountAccessRole 的成員帳戶中建立。

> **Note**
>
> 當您在組織中建立帳戶而非邀請現有帳戶加入時， AWS Organizations 會自動建立 IAM 角色 (`OrganizationAccountAccessRole`依預設命名)，您可以使用該角色授與管理帳戶管理員中的使用者存取已建立帳戶的權限。

AWS Organizations 會在受邀的成員帳戶中自動建立服務連結角色，以支援 AWS Organizations 與其他 AWS 服務之間的整合。如需詳細資訊，請參閱 AWS Organizations 和服務連結角色。

如需每天可傳送的邀請數目，請參閱最大值和最小值。已接受的邀請不會計入此限制之內。一旦有邀請被接受，當天即可以傳送另一個邀請。必須在 15 天內回應每個邀請，否則邀請會過期。

傳送到帳戶的邀請會計入組織中的帳戶配額。若受邀帳戶拒絕、管理帳戶取消邀請或邀請到期，便會還原計數。

若要建立會自動成為組織一部分的帳戶，請參閱在您的組織中建立成員帳戶。

> **Important**
>
> 由於法律和帳單限制，您 AWS 帳戶 只能從與管理帳戶相同的 AWS 賣家和 AWS 分區進行邀請。例如，在 AWS EMEA 組織中，您只能邀請來自 AWS EMEA SARL 記錄賣方的帳戶。

- 如果您組織的管理帳戶是由 Amazon Internet Services Pvt. Ltd (AISPL) 建立，則組織中的所有帳戶都必須來自與管理帳戶相同的名義賣家。例如，身為印度的 AWS 賣家，您只能邀請其他 AISPL 帳戶加入您的組織。您無法合併 AISPL 和/ AWS 或任何其他 AWS 賣家的帳戶。
- 組織中的所有帳戶必須來自與管理帳戶相同的 AWS 磁碟分割。商業 AWS 區域 分割區中的帳戶不能位於擁有來自中國區域磁碟分割區之帳戶的組織中，或是區 AWS GovCloud (US) 域磁碟分割中的帳戶。

傳送邀請給 AWS 帳戶

若要邀請帳戶加入您的組織，您必須先驗證您擁有與管理帳戶關聯的電子郵件地址。如需詳細資訊，請參閱 電子郵件地址驗證。在您驗證電子郵件地址之後，請完成下列步驟來邀請帳戶加入您的組織。

最低許可

若要邀請 AWS 帳戶 加入您的組織，您必須具備下列權限：

- `organizations:DescribeOrganization` (僅限主控台)
- `organizations:InviteAccountToOrganization`

AWS Management Console

邀請另一個帳戶加入組織

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 如果您已使用驗證電子郵件地址 AWS，請略過此步驟。

   如果您尚未驗證您的電子郵件地址，請在建立組織後 24 小時內遵循驗證電子郵件中的指示。在您收到驗證電子郵件訊息之前，可能會有一些延遲的時間。驗證您的電子郵件地址之前，您不可邀請帳戶加入您的組織。
3. 導覽至 AWS 帳戶 頁面，然後選擇 Add an AWS account (新增 AWS 帳戶)。
4. 在 Add an AWS 帳戶 (新增) 頁面中，選擇 Invite an existing AWS account (邀請現有的 AWS 帳戶)。

5. 在邀請現有 AWS頁面上，對於 AWS 帳戶 要邀請的電子郵件地址或帳戶 ID，請輸入與受邀帳戶相關聯的電子郵件地址或其帳戶 ID 號碼。
6. (選用) 對於要包含在邀請電子郵件訊息中的訊息，輸入您要包含在傳送給受邀帳戶擁有者電子郵件邀請中的任何文字。
7. (選用) 在 Add tags (新增標籤) 區段中，指定一個或多個在帳戶管理員接受邀請後自動套用至帳戶的標記。若要執行此操作，請選擇 Add tag (新增標籤)，然後輸入一個鍵和一個選用值。將值留空會將其設定為空白字串；而不是 null。您可以在 AWS 帳戶中連接最多 50 個標籤。
8. 選擇傳送邀請。

   > **Important**
   >
   > 如果您收到訊息，說明您已超出組織的帳戶配額，或因為您的組織仍在初始化而無法新增帳戶，請聯絡 AWS Support。

9. 主控台會將您重新導向至邀請頁面，您可以在此處檢視所有開啟和已接受的邀請。您剛建立的邀請會出現在清單上方，並且其狀態設定為 OPEN (開啟中)。

   AWS Organizations 傳送邀請至您邀請加入組織之帳戶擁有者的電子郵件地址。此電子郵件訊息包含 AWS Organizations 主控台的連結，帳戶擁有者可以在其中檢視詳細資料，並選擇接受或拒絕邀請。或者，受邀帳戶的擁有者也可以略過電子郵件訊息、直接前往 AWS Organizations 主控台、檢視邀請，以及接受或拒絕邀請。

   對此帳戶的邀請會立即計入您在組織中可以具有的帳戶數量上限。 AWS Organizations 不會等候直到帳戶接受邀請。如果獲邀請的帳戶拒絕，則管理帳戶會取消邀請。如果獲邀請的帳戶未在指定的時間期間內回應，則邀請會過期。在這兩種情況下，邀請不會計入您的配額。

AWS CLI & AWS SDKs

邀請另一個帳戶加入組織

您可以使用以下其中一個命令來邀請另一個帳戶加入您的組織：

- AWS CLI: invite-account-to-organization

```
$ aws organizations invite-account-to-organization \
    --target '{"Type": "EMAIL", "Id": "juan@example.com"}' \
    --notes "This is a request for Juan's account to join Bill's organization."
{
    "Handshake": {
```

```
        "Action": "INVITE",
        "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
        "ExpirationTimestamp": 1482952459.257,
        "Id": "h-examplehandshakeid111",
        "Parties": [
            {
                "Id": "o-exampleorgid",
                 "Type": "ORGANIZATION"
            },
            {
                 "Id": "juan@example.com",
                 "Type": "EMAIL"
            }
        ],
        "RequestedTimestamp": 1481656459.257,
        "Resources": [
            {
                "Resources": [
                    {
                        "Type": "MASTER_EMAIL",
                        "Value": "bill@amazon.com"
                    },
                    {
                         "Type": "MASTER_NAME",
                         "Value": "Management Account"
                    },
                    {
                         "Type": "ORGANIZATION_FEATURE_SET",
                         "Value": "FULL"
                    }
                ],
                "Type": "ORGANIZATION",
                "Value": "o-exampleorgid"
            },
            {
                "Type": "EMAIL",
                "Value": "juan@example.com"
            }
        ],
        "State": "OPEN"
    }
}
```

- AWS 軟體開發套件：InviteAccountToOrganization

管理組織等待中的邀請

登入到您的管理帳戶時，您可以檢視組織中的所有連結的 AWS 帳戶 ，以及取消任何等待中 (開啟) 的邀請。若要執行此動作，請執行下列步驟。

> **最低許可**
>
> 若要管理組織的等待中邀請，您必須擁有以下許可：
>
> - `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要
> - `organizations:ListHandshakesForOrganization`
> - `organizations:CancelHandshake`

AWS Management Console

檢視或取消從您的組織傳送到其他帳戶的邀請

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 導覽至邀請頁面。

   此頁面顯示從您的組織傳送的所有邀請及其目前狀態。

   > **Note**
   >
   > 已接受、已取消和已拒絕的邀請會繼續在清單中顯示 30 天。之後便會刪除它們，不再顯示在清單中。

3. 選擇您希望取消邀請旁邊的選項按鈕

   然後選擇 Cancel invitation (取消邀請)。如果選項按鈕呈現灰色，則無法取消該邀請。

   邀請的狀態會從 Open (開啟) 變更為 Canceled (已取消)。

   AWS 傳送電子郵件訊息給帳戶擁有者，說明您已取消邀請。除非您傳送新的邀請，否則該帳戶不再可以加入組織。

AWS CLI & AWS SDKs

檢視或取消從您的組織傳送到其他帳戶的邀請

您可以使用以下命令來檢視或取消邀請：

- AWS CLI：list-handshakes-for-organization，取消握手
- 下列範例顯示此組織傳送給其他帳戶的邀請。

```
$ aws organizations list-handshakes-for-organization
{
    "Handshakes": [
        {
            "Action": "INVITE",
            "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
            "ExpirationTimestamp": 1482952459.257,
            "Id": "h-examplehandshakeid111",
            "Parties": [
                {
                    "Id": "o-exampleorgid",
                    "Type": "ORGANIZATION"
                },
                {
                    "Id": "juan@example.com",
                    "Type": "EMAIL"
                }
            ],
            "RequestedTimestamp": 1481656459.257,
            "Resources": [
                {
                    "Resources": [
                        {
                            "Type": "MASTER_EMAIL",
                            "Value": "bill@amazon.com"
                        },
                        {
                            "Type": "MASTER_NAME",
                            "Value": "Management Account"
                        },
                        {
                            "Type": "ORGANIZATION_FEATURE_SET",
                            "Value": "FULL"
```

```
                        }
                    ],
                    "Type": "ORGANIZATION",
                    "Value": "o-exampleorgid"
                },
                {
                    "Type": "EMAIL",
                    "Value": "juan@example.com"
                },
                {
                    "Type":"NOTES",
                    "Value":"This is an invitation to Juan's account to join
 Bill's organization."
                }
            ],
            "State": "OPEN"
        },
        {
            "Action": "INVITE",
            "State":"ACCEPTED",
            "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
            "ExpirationTimestamp": 1.471797437427E9,
            "Id": "h-examplehandshakeid222",
            "Parties": [
                {
                    "Id": "o-exampleorgid",
                    "Type": "ORGANIZATION"
                },
                {
                    "Id": "anika@example.com",
                    "Type": "EMAIL"
                }
            ],
            "RequestedTimestamp": 1.469205437427E9,
            "Resources": [
                {
                    "Resources": [
                        {
                            "Type":"MASTER_EMAIL",
                             "Value":"bill@example.com"
                        },
                        {
                            "Type":"MASTER_NAME",
```

```
                            "Value":"Management Account"
                        }
                    ],
                    "Type":"ORGANIZATION",
                    "Value":"o-exampleorgid"
                },
                {
                    "Type":"EMAIL",
                    "Value":"anika@example.com"
                },
                {
                    "Type":"NOTES",
                    "Value":"This is an invitation to Anika's account to join
 Bill's organization."
                }
            ]
        }
    ]
}
```

下列範例顯示如何取消對帳戶的邀請。

```
$ aws organizations cancel-handshake --handshake-id h-examplehandshakeid111
{
    "Handshake": {
        "Id": "h-examplehandshakeid111",
        "State":"CANCELED",
        "Action": "INVITE",
        "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
        "Parties": [
            {
                "Id": "o-exampleorgid",
                "Type": "ORGANIZATION"
            },
            {
                "Id": "susan@example.com",
                "Type": "EMAIL"
            }
        ],
        "Resources": [
            {
                "Type": "ORGANIZATION",
```

```
                "Value": "o-exampleorgid",
                "Resources": [
                    {
                        "Type": "MASTER_EMAIL",
                        "Value": "bill@example.com"
                    },
                    {
                        "Type": "MASTER_NAME",
                        "Value": "Management Account"
                    },
                    {
                        "Type": "ORGANIZATION_FEATURE_SET",
                        "Value": "CONSOLIDATED_BILLING"
                    }
                ]
            },
            {
                "Type": "EMAIL",
                "Value": "anika@example.com"
            },
            {
                "Type": "NOTES",
                "Value": "This is a request for Susan's account to join Bob's
 organization."
            }
        ],
        "RequestedTimestamp": 1.47008383521E9,
        "ExpirationTimestamp": 1.47137983521E9
    }
}
```

- AWS 軟體開發套件：ListHandshakesForOrganization、CancelHandshake

接受或拒絕來自組織的邀請

您 AWS 帳戶 可能會收到加入組織的邀請。您可以接受或拒絕邀請。若要執行此動作，請執行下列步驟。

> **Note**
>
> 帳戶與組織的狀態，會影響顯示的成本和用量資料：

- 如果成員帳戶離開組織而成為獨立帳戶，則帳戶一旦是組織之成員就無法再存取時間範圍內的成本和用量資料。帳戶只能存取做為獨立帳戶時所產生的資料。
- 如果成員帳戶離開組織 A 而加入組織 B，則此帳戶就無法再存取其做為組織 A 成員之時間範圍內來自組織 A 的成本和用量資料。帳戶只能存取做為組織 B 成員時所產生的資料。
- 如果帳戶重新加入先前所屬的組織，此帳戶會重新獲得對其過去成本與使用狀況資料的存取權。

Note

只有成員帳戶和獨立帳戶可接受或拒絕加入組織的邀請。如果向成員帳戶傳送邀請，該帳戶應先離開目前組織，才能接受邀請。如果邀請傳送至已屬於 AWS Organization 的管理帳戶，則該帳戶將無法接受邀請，除非他們從其組織移除所有成員帳戶並刪除組織。

最低許可

若要接受或拒絕加入 AWS 組織的邀請，您必須具備下列權限：

- `organizations:ListHandshakesForAccount`— 需要在 AWS Organizations 控制台中查看邀請列表。
- `organizations:AcceptHandshake`.
- `organizations:DeclineHandshake`.
- `iam:CreateServiceLinkedRole`— 只有在接受邀請時，才需要在成員帳戶中建立服務連結角色以支援與其他 AWS 服務的整合時才需要。如需詳細資訊，請參閱 AWS Organizations 和服務連結角色。

AWS Management Console

接受或拒絕邀請

1. 加入組織的邀請會傳送到帳戶擁有者的電子郵件地址。如果您是帳戶擁有者，而且您收到邀請電子郵件訊息，請依照電子郵件邀請中的指示，或前往您的瀏覽器中的 AWS Organizations 主控台，然後選擇 Invitations (邀請)，或直接前往成員帳戶的邀請頁面。

2. 如果提示，請以擔任 IAM 角色的 IAM 使用者身分登入或以帳戶的根使用者身分登入 (不建議) 獲邀請的帳戶。
3. 會員帳戶的邀請頁面顯示您的帳戶加入組織的未結邀請。

   選擇 Accept invitation (接受邀請) 或 Decline invitation (拒絕邀請)。

   - 如果您在之前的步驟中選擇 Accept invitation (接受邀請)，主控台會將您重新導向至 Organization 概觀頁面，其中含有您的帳戶現在為其成員的組織的詳細資訊。您可以檢視組織的 ID 和擁有者的電子郵件地址。

     > **Note**
     >
     > 已接受的邀請會繼續在清單中顯示 30 天。之後便會刪除它們，不再顯示在清單中。

     AWS Organizations 自動在新成員帳戶中建立服務連結角色，以支援 AWS Organizations 與其他 AWS 服務之間的整合。如需詳細資訊，請參閱 AWS Organizations 和服務連結角色。

     AWS 傳送電子郵件訊息給組織管理帳戶的擁有者，說明您已接受邀請。它還會傳送一封電子郵件訊息給帳戶擁有者，說明帳戶現在為組織的成員。
   - 如果您在前面的步驟中選擇 Decline (拒絕)，則您的帳戶會維持在列出任何其他等待中邀請的成員帳戶邀請頁面上。

     AWS 傳送電子郵件訊息給組織的管理帳戶擁有者，說明您已拒絕邀請。

     > **Note**
     >
     > 已拒絕的邀請會繼續在清單中顯示 30 天。之後便會刪除它們，不再顯示在清單中。

AWS CLI & AWS SDKs

接受或拒絕邀請

您可以使用以下命令來接受或拒絕邀請：

- AWS CLI: accept-handshake, decline-handshake

下列範例顯示如何接受對加入組織的邀請。

```
$ aws organizations accept-handshake --handshake-id h-examplehandshakeid111
{
    "Handshake": {
        "Action": "INVITE",
        "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
        "RequestedTimestamp": 1481656459.257,
        "ExpirationTimestamp": 1482952459.257,
        "Id": "h-examplehandshakeid111",
        "Parties": [
            {
                "Id": "o-exampleorgid",
                "Type": "ORGANIZATION"
            },
            {
                "Id": "juan@example.com",
                "Type": "EMAIL"
            }
        ],
        "Resources": [
            {
                "Resources": [
                    {
                        "Type": "MASTER_EMAIL",
                        "Value": "bill@amazon.com"
                    },
                    {
                        "Type": "MASTER_NAME",
                        "Value": "Management Account"
                    },
                    {
                        "Type": "ORGANIZATION_FEATURE_SET",
                         "Value": "ALL"
                    }
                ],
                "Type": "ORGANIZATION",
                "Value": "o-exampleorgid"
            },
            {
                "Type": "EMAIL",
                "Value": "juan@example.com"
            }
        ],
```

```
        "State": "ACCEPTED"
    }
}
```

下列範例顯示如何拒絕對加入組織的邀請。

- AWS 軟體開發套件：AcceptHandshake、DeclineHandshake

在您的組織中建立成員帳戶

這個頁面會說明如何使用 AWS Organizations 在組織內建立 AWS 帳戶。若要了解 AWS 入門和建立單一 AWS 帳戶，請參閱資源中心入門。

組織是指您集中管理的 AWS 帳戶 集合。您可以執行以下程序來管理屬於您的組織一部分的帳戶：

- 建立屬於您的組織的 AWS 帳戶
- 存取擁有管理帳戶存取角色的成員帳戶

Important

- 在您的組織中建立成員帳戶時，AWS Organizations 會自動在成員帳戶中建立一個 AWS Identity and Access Management (IAM) 角色 `OrganizationAccountAccessRole`，讓管理帳戶中的使用者和角色能對成員帳戶執行完整的管理控制。這個角色會受限於套用至成員帳戶的任何服務控制政策 (SCP)。

  AWS Organizations 還會自動將受管政策以及 `OrganizationAccountAccessRole` 角色新增到成員帳戶中。此允許集中控制，以便在政策更新時，自動更新連接至相同受管政策的任何其他帳戶。過去，在組織內建立的新帳戶會得到一個僅適用於該單一帳戶的內嵌政策。如需內嵌和受管政策的詳細資訊，請參閱《IAM 使用者指南》中的受管政策和內嵌政策。

  AWS Organizations 也會自動建立名為 `AWSServiceRoleForOrganizations` 的服務連結角色，啟用與選取 AWS 服務的整合。您必須設定其他服務以允許整合。如需更多詳細資訊，請參閱 AWS Organizations 和服務連結角色。
- 如果該組織使用 AWS Control Tower 進行管理，則使用 AWS Control Tower 主控台或 API 中的 AWS Control Tower Account Factory 來建立帳戶。如果您在 Organizations 中建立帳戶，則該帳戶未在 AWS Control Tower 註冊。如需詳細資訊，請參閱AWS Control Tower使用者指南中的參照 AWS Control Tower 外部資源。

> **Note**
>
> 作為組織一部分而建立的 AWS 帳戶 不會自動訂閱 AWS 行銷電子郵件。若要選擇加入您的帳戶以接收行銷電子郵件，請參閱https://pages.awscloud.com/communication-preferences。

建立屬於您的組織的 AWS 帳戶

在登入組織的管理帳戶之後，您可以建立會自動成為組織一部分的成員帳戶。使用以下程序建立帳戶時，AWS Organizations 會自動將管理帳戶中的下列主要聯絡資訊複製到新的成員帳戶中：

- 電話號碼
- 公司名稱
- 網站 URL
- Address

它也會從管理帳戶複製通訊語言和 Marketplace 資訊 (部分 AWS 區域 帳戶供應商)。

> **Note**
>
> AWS 不會自動收集帳戶作為獨立帳戶運作所需的所有資訊。如果您曾從組織移除成員帳戶，並且讓它成為獨立帳戶，您必須為帳戶提供該資訊，之後才可以移除它。如需更多詳細資訊，請參閱 從成員帳戶離開組織。

> **最低許可**
>
> 若要在您的組織中建立成員帳戶，您必須擁有以下許可：
>
> - `organizations:CreateAccount`
> - `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要
> - `iam:CreateServiceLinkedRole` (授予委託人 `organizations.amazonaws.com` ，讓其可在成員帳戶中建立必要的服務連結角色)。

AWS Management Console

若要建立自動成為組織一部分的 AWS 帳戶

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 AWS 帳戶 頁面上，選擇新增 AWS 帳戶。
3. 在新增 AWS 帳戶 頁面上，選擇建立 AWS 帳戶(預設會選擇該項)。
4. 在建立 AWS 帳戶 頁面，針對AWS 帳戶名稱，輸入您要指派給帳戶的名稱。此名稱可協助您區分該帳戶與組織中的所有其他帳戶，並且與 IAM 別名或擁有者的電子郵件名稱不同。
5. 針對帳戶擁有者的電子郵件地址，輸入帳戶擁有者的電子郵件地址。此電子郵件地址不能與其他 AWS 帳戶 關聯，因為它會成為帳戶根使用者的使用者名稱憑證。
6. (選用) 指定要在新帳戶中自動建立、要指派給 IAM 角色的名稱。此角色會授予組織的管理帳戶許可，以存取新建立的成員帳戶。如果您不指定名稱，AWS Organizations 會提供該角色預設的名稱 `OrganizationAccountAccessRole`。建議您在所有帳戶中使用預設名稱以確保一致性。

   > **Important**
   >
   > 請記住此角色名稱。稍後您會需要它，以便為管理帳戶中的使用者和角色授予新帳戶的存取權。

7. (選用) 在 Tags (標籤) 區段中，透過選擇 Add tag (新增標籤)，然後輸入一個鍵和一個選用值，來將一個或多個標籤新增至新帳戶。將值留空會將其設定為空白字串；而不是 `null`。您可以在帳戶中連接最多 50 個標籤。
8. 選擇 Create (建立)AWS 帳戶。

   - 如果您收到錯誤，指出您已超出組織的帳戶配額，請參閱當我試著新增帳戶到我的組織時，出現「超過配額」訊息。
   - 如果您收到錯誤，指出因為您的組織仍在初始化，您無法新增帳戶，請等候一小時然後重試。
   - 您也可以查看 AWS CloudTrail 日誌來取得有關帳戶建立是否成功的資訊。如需更多詳細資訊，請參閱 AWS Organizations 中的記錄和監控。
   - 如果錯誤仍存在，請聯絡 AWS Support。

出現 AWS 帳戶 頁面時，將您的新帳戶新增至清單。

9. 現在帳戶已存在，並且具有的 IAM 角色可授予管理員存取給管理帳戶中的使用者，您可以遵循存取和組織的成員帳戶 中的步驟來存取帳戶。

> **Note**
>
> 建立帳戶時，AWS Organizations 最初會將長 (64 個字元)、複雜且隨機產生的密碼指派給根使用者。您無法擷取此初始密碼。若要第一次以根帳戶使用者的身分存取帳戶，您必須進行密碼復原程序。如需更多詳細資訊，請參閱 以根帳戶使用者身分存取成員帳戶。

AWS CLI & AWS SDKs

建立會自動成為組織一部分的 AWS 帳戶

您可以使用下列其中一項命令來建立帳戶：

- AWS CLI: create-account

```
$ aws organizations create-account \
    --email susan@example.com \
    --account-name "Production Account"
{
        "CreateAccountStatus": {
                "State": "IN_PROGRESS",
                "Id": "car-examplecreateaccountrequestid111"
        }
}
```

然後，可以使用以下命令檢查帳戶建立的狀態。

```
$ aws organizations describe-create-account-status \
    --create-account-request-id car-examplecreateaccountrequestid111
{
  "CreateAccountStatus": {
    "State": "SUCCEEDED",
    "AccountId": "555555555555",
    "AccountName": "Production account",
    "RequestedTimestamp": 1470684478.687,
    "CompletedTimestamp": 1470684532.472,
    "Id": "car-examplecreateaccountrequestid111"
  }
```

```
}
```

- AWS SDKs: CreateAccount

存取和組織的成員帳戶

當您在組織中建立帳戶時，除了根使用者之外，AWS Organizations 還會自動建立名為 `OrganizationAccountAccessRole` 的 IAM 角色。您可以在建立時指定不同的名稱，但建議您在所有帳戶中一致命名。我們會以預設名稱參考本指南中的角色。AWS Organizations 不會建立任何其他使用者或角色。若要存取組織中的帳戶，您必須使用以下其中一個方法：

- 如果是建立 AWS 帳戶，您會先有一個登入身分，可以完整存取帳戶中所有 AWS 服務 與資源。此身分稱為 AWS 帳戶 根使用者，使用建立帳戶時所使用的電子郵件地址和密碼即可登入並存取。強烈建議您不要以根使用者處理日常作業。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需這些任務的完整清單，了解需以根使用者登入的任務，請參閱《IAM 使用者指南》中的需要根使用者憑證的任務。如需更多根使用者安全建議，請參閱適用於 AWS 帳戶 的根使用者最佳實務。
- 如果您使用 AWS Organizations 隨附的工具建立帳戶，則可以使用預先設定的角色 `OrganizationAccountAccessRole` 來存取帳戶，以此方式建立的所有新帳戶中都有該角色。如需詳細資訊，請參閱 存取擁有管理帳戶存取角色的成員帳戶。
- 若是邀請現有帳戶加入組織，而該帳戶也接受邀請，您可以選擇建立 IAM 角色，以允許管理帳戶存取受邀的成員帳戶。此角色與 AWS Organizations 建立的帳戶中自動新增的角色完全相同。若要建立角色，請參閱在受邀 OrganizationAccountAccessRole 的成員帳戶中建立。在您建立角色後，您便可以使用存取擁有管理帳戶存取角色的成員帳戶中的步驟來存取它。
- 使用 AWS IAM Identity Center 並啟用具有 AWS Organizations 的 IAM Identity Center 受信任存取。這可讓使用者利用其企業憑證來登入 AWS 存取入口網站，並在其獲指派的管理帳戶或成員帳戶中存取資源。

  如需詳細資訊，請參閱 AWS IAM Identity Center 使用者指南中的多帳戶許可。如需設定 IAM Identity Center 的受信任存取的詳細資訊，請參閱 AWS IAM Identity Center 與 AWS Organizations。

> **最低許可**
>
> 若要從組織的任何其他帳戶存取 AWS 帳戶，您必須擁有以下許可：

- `sts:AssumeRole` – `Resource` 元素必須設為星號 (*) 或需要存取新成員帳戶之使用者帳戶的帳戶 ID

以根帳戶使用者身分存取成員帳戶

建立新帳戶時，AWS Organizations 最初會指派密碼給根帳戶使用者，長度至少為 64 個字元。所有字元會隨機產生，不保證外觀會出現特定的字元集。您無法擷取此初始密碼。若要第一次以根帳戶使用者的身分存取帳戶，您必須進行密碼復原程序。如需詳細資訊，請參閱AWS登入使用指南AWS 帳戶中的我忘記了我的 root 使用者密碼。

備註

- 做為最佳實務，我們建議您不要使用根使用者來存取帳戶，要建立具有更受限許可的其他使用者和角色除外。然後，以這些使用者或角色身分登入。
- 我們還建議您在根使用者上啟用多重要素驗證 (MFA)。重設密碼，並將 MFA 裝置指派給根使用者。
- 如果您在組織中使用錯誤的電子郵件地址建立成員帳戶，即無法以根帳戶使用者的身分登入帳戶。請聯絡 AWS 帳單和支援以取得協助。

在受邀 OrganizationAccountAccessRole 的成員帳戶中建立

依預設，如果您隨著組織建立成員帳戶，AWS 會自動在帳戶中建立一個角色，為管理帳戶中可以擔任該角色的 IAM 使用者授予管理員許可。在預設情況下，該角色名為 `OrganizationAccountAccessRole`。如需詳細資訊，請參閱 存取擁有管理帳戶存取角色的成員帳戶。

不過，您邀請加入組織的成員帳戶，不會自動建立管理員角色。您可以手動執行此動作，如以下程序所示。這基本上會複製自動為已建立帳戶設定的角色。我們建議您為手動建立的角色使用相同的名稱 `OrganizationAccountAccessRole`，以保有一致性並方便記住。

AWS Management Console

在成員帳戶中建立 AWS Organizations 管理員角色

1. 登入 IAM 主控台，網址為 https://console.aws.amazon.com/iam/。您必須以 IAM 使用者的身分登入，擔任 IAM 角色，或以成員帳戶中的根使用者身分登入 (不建議)。使用者或角色必須具有建立 IAM 角色和政策的許可。
2. 在 IAM 主控台中，導覽至 [角色]，然後選擇 [建立角色]。
3. 選擇 AWS 帳戶，然後選取 [其他] AWS 帳戶。
4. 輸入您要授與管理員存取權的管理帳戶的 12 位數帳號 ID 號碼。在選項下，請注意以下事項：
   - 針對此角色，因為帳戶是公司內部帳戶，您不應該選擇 Require external ID (需要外部 ID)。如需有關外部 ID 選項的詳細資訊，請參閱何時應該使用外部 ID？ 在 IAM 使用者指南中。
   - 如果您已啟用和設定 MFA 身分驗證，您可以選擇性地要求使用 MFA 裝置進行身分驗證。如需 MFA 的詳細資訊，請參閱 IAM 使用者指南中AWS的使用多重要素驗證 (MFA)。
5. 選擇下一步。
6. 在 [新增權限] 頁面上，選擇名為的AWS受管理策略，`AdministratorAccess`然後選擇 [下一步]。
7. 在 [名稱、檢閱和建立] 頁面上，指定角色名稱和選擇性描述。為求與新帳戶中指派給角色的預設名稱一致，建議您使用 `OrganizationAccountAccessRole`。若要遞交您的變更，請選擇 Create role (建立角色)。
8. 您的新角色會顯示在可用的角色清單中。選擇新角色的名稱來檢視其詳細資訊，特別注意提供的連結 URL。將此 URL 提供給成員帳戶中，需要存取角色的使用者。此外，請記下 Role ARN (角色 ARN)，因為您在步驟 15 中將需要它。
9. 登入 IAM 主控台，網址為 https://console.aws.amazon.com/iam/。這時，以管理帳戶中擁有許可能建立政策和將政策指派給使用者或群組的使用者身分登入。
10. 瀏覽至 [原則]，然後選擇 [建立原則]。
11. 針對 Service (服務)，選擇 STS。
12. 針對動作，首先在篩選條件方塊中輸入 **`AssumeRole`**，然後在出現時選中旁邊的核取方塊。
13. 在 [資源] 下，確定已選取 [特定]，然後選擇 [新增 ARN]。
14. 輸入 AWS 成員帳戶 ID 號碼，然後輸入您在之前的步驟 1–8 中建立的角色名稱。選擇新增 ARN。
15. 如果您要授予許可以擔任多個成員帳戶中的角色，請對每個帳戶重複步驟 14 和 15。
16. 選擇下一步。

17. 在 [檢閱並建立] 頁面上，輸入新原則的名稱，然後選擇 [建立原則] 以儲存變更。
18. 在功能窗格中選擇 [使用者群組]，然後選擇要用來委派成員帳戶管理的群組名稱 (而非核取方塊)。
19. 選擇許可索引標籤標籤。
20. 選擇 [新增權限]，選擇 [附加原則]，然後選取您在步驟 11—18 中建立的原則。

所選取群組成員的使用者現在可以使用您在步驟 9 中擷取的 URL 來存取每個成員帳戶的角色。他們可以透過您在組織中所建立帳戶的相同方式存取這些成員帳戶。如需使用角色來管理成員帳戶詳細資訊，請參閱存取擁有管理帳戶存取角色的成員帳戶。

存取擁有管理帳戶存取角色的成員帳戶

當您使用 AWS Organizations 主控台建立成員帳戶時，AWS Organizations 會自動在帳戶中建立名為 `OrganizationAccountAccessRole` 的 IAM 角色。此角色擁有成員帳戶內的完整管理許可。此角色的存取範圍包括管理帳戶中的所有主體，因此該角色設定為授予對該組織管理帳戶的存取權。您可以遵循 在受邀 OrganizationAccountAccessRole 的成員帳戶中建立中的步驟，為獲邀請成員帳戶建立完全相同的角色。若要使用此角色來存取成員帳戶，您必須以管理帳戶帳戶中擁有擔任此角色許可的使用者身分登入。若要設定這些許可，請執行下列程序。我們建議您將許可授予群組，而不是使用者，以方便維護。

AWS Management Console

授予管理帳戶中 IAM 群組成員的許可以存取角色

1. 登入 IAM 主控台 (https://console.aws.amazon.com/iam/)，以管理帳戶中擁有管理員許可的使用者身分。需要此項，才能將許可委派給其使用者將存取成員帳戶中角色的 IAM 群組。
2. 透過建立您稍後在??? 中需要的受管理政策來開始。

   在導覽窗格中，選擇 Policies (政策)，然後選擇 Create policy (建立政策)。
3. 在視覺化編輯器索引標籤上，選擇 Choose a service (選擇服務)，在搜尋方塊中輸入 **STS** 以篩選清單，然後選擇 STS 選項。
4. 在 [動作] 區段**assume**中，輸入搜尋方塊以篩選清單，然後選擇選AssumeRole項。
5. 在 [資源] 區段中，選擇 [特定]，選擇 [新增 ARN]，然後輸入成員帳號和您在上一節建立的角色名稱 (我們建議您命名它`OrganizationAccountAccessRole`)。
6. 當對話方塊顯示正確的 ARN 時，請選擇「新增 ARN」。

7. (選擇性) 如果您想要要求多重因素認證 (Multi-Factor Authentication，MFA)，或限制來自指定 IP 地址範圍的角色存取，請展開「請求條件」區段，然後選取您要強制執行的選項。
8. 選擇下一步。
9. 在 [檢閱並建立] 頁面上，輸入新原則的名稱。例如：**`GrantAccessToOrganizationAccountAccessRole`**。您也可以加入選用說明。
10. 選擇 Create policy (建立政策) 以儲存您的新受管政策。
11. 現在有了可用的政策，您就可以將其連接到群組。

    在功能窗格中，選擇 [使用者群組]，然後選擇您希望其成員能夠在成員帳戶中擔任角色的群組名稱 (而非核取方塊)。如果需要，您可以建立新群組。
12. 選擇 許可 標籤、選擇 新增許可，然後選擇 連接政策。
13. (選擇性) 在 Search (搜尋) 方塊中，您可以開始輸入政策名稱以篩選清單，直到您可以看到剛剛在Step 2 到Step 10 建立的政策名稱為止。您也可以選擇 [所有類型]，然後選擇 [客戶AWS 管理]，篩選掉所有受管理的政策。
14. 核取原則旁邊的方塊，然後選擇 [附加原則]。

作為群組成員的 IAM 使用者現在擁有許可，能夠遵循下列程序，在 AWS Organizations 主控台中切換到新角色。

AWS Management Console

切換到成員帳戶的角色

使用角色時，使用者擁有新成員帳戶中的管理員許可。指示身為群組成員的 IAM 使用者，執行下列動作切換到新的角色。

1. 從 AWS Organizations 主控台的右上角處，選取包含目前登入名稱的連結，然後選擇 Switch role (切換角色)。
2. 輸入管理員提供的帳戶 ID 號碼和角色名稱。
3. 對於 Display Name (顯示名稱)，輸入您要在右上角導覽列中顯示的文字，以在您使用該角色時取代您的使用者名稱。您可以選擇性地選擇顏色。
4. 選擇 Switch Role (切換角色)。現在您執行的所有動作，都是使用授予您切換目標角色的許可所完成。在您切換回去之前，您將不再擁有與原始 IAM 使用者建立關聯的許可。
5. 在您完成需要角色許可的執行動作後，您便可以切換回您的一般 IAM 使用者。選擇右上角的角色名稱 (無論您指定為 [顯示名稱])，然後選擇 [返回至] *`UserName`*。

其他資源

- 如需有關授予切換角色權限的詳細資訊，請參閱《IAM 使用者指南》中的授予使用者切換角色的權限。
- 如需有關使用已獲授與您承擔的角色的詳細資訊，請參閱《IAM 使用者指南》中的「切換到角色 (主控台)」。
- 如需使用角色進行跨帳戶存取的教學課程，請參閱 IAM AWS 帳戶 使用者指南中的教學課程：跨 IAM 角色委派存取權。
- 如需關閉 AWS 帳戶 的相關資訊，請參閱關閉組織中的成員帳戶。

匯出組織的 AWS 帳戶詳細資訊

使用 AWS Organizations，組織的管理帳戶使用者和委派管理員可以匯出含有組織內所有帳戶詳細資訊的 .csv 檔案。因此，組織管理員可以輕鬆檢視帳戶並依狀態進行篩選：ACTIVE、SUSPENDED 或 PENDING。如果您的組織有許多帳戶，.csv 檔案下載選項提供一種在試算表中輕鬆檢視及排序帳戶詳細資訊的方法。

以前，檢視帳戶的唯一方法是查看AWS Organizations 主控台中的帳戶階層或清單顯示。

> **Note**
>
> 只有管理帳戶中的主體可以下載帳戶清單。

匯出組織中所有 AWS 帳戶 的清單。

登入組織的管理帳戶時，您可以取得屬於組織一部分的所有帳戶的清單,格式為會 .csv 檔案。清單包含個別帳戶詳細資訊；但其未指出帳戶所屬的組織單位 (OU)。

.csv 檔案內含每個帳戶的以下資訊：

- Account ID (帳戶 ID) – 帳戶識別碼。例如：123456789012
- ARN – 帳戶的 Amazon 資源名稱。例如：arn:aws:organizations::123456789012account/o-o1gb0d1234/123456789012
- Email – 與帳戶相關聯的電子郵件地址。例如：marymajor@example.com
- Name (名稱) – 帳戶建立者提供的帳戶名稱。例如：階段測試帳戶
- Status (狀態) – 組織內的帳戶狀態。此值可以是 PENDING、ACTIVE 或 SUSPENDED。

- Joined method (加入的方法) – 指定帳戶的建立方式。此值可以是 `INVITED` 或 `CREATED`。
- Joined timestamp (加入時的時間戳記) – 帳戶加入組織的日期和時間。

> **最低許可**
>
> 若要匯出您組織中所有成員帳戶的 .csv 檔案，您必須擁有以下許可：
>
> - `organizations:DescribeOrganization`
> - `organizations:ListAccounts`

AWS Management Console

若要匯出您組織中所有 AWS 帳戶 的 .csv 檔案

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 選擇Actions (動作)，然後針對 AWS 帳戶 選擇 Export account list (匯出帳戶清單)。頁面頂端的藍色橫幅指示 "Export is in progress!" (「匯出進行中！」)
3. 當檔案準備就緒時，橫幅會變成綠色，並指示："Download is ready!" (「下載已準備就緒！」) 選擇 Download CSV (下載 CSV)。檔案 `Organization_accounts_information.csv` 下載到您的裝置。

AWS CLI & AWS SDKs

匯出含有帳戶詳細資訊的 .csv 檔案的唯一方法是使用 AWS Management Console。您無法使用 AWS CLI 匯出帳戶清單 .csv 檔案。

從組織移除成員帳戶

組織中的部分管理帳戶會將您不再需要的成員帳戶移除。移除成員帳戶並不會關閉帳戶，而是會從組織移除成員帳戶。先前的成員帳戶會變成不再由 AWS Organizations 管理的獨立 AWS 帳戶。之後，該帳戶不再受任何政策的約束，並負責自己的帳單支付。從組織移除帳戶後，該組織的管理帳戶不會再針對該帳戶所累積的任何費用收費。

如需移除管理帳戶的資訊，請參閱刪除組織。

主題

從組織移除帳戶前的考慮事項

在您移除帳戶前，必須先考慮以下項目：

- 只有在帳戶具有讓它以獨立帳戶形式運作所需的資訊時，您才能從組織移除帳戶。當您使用 AWS Organizations 主控台、API 或 AWS CLI 命令在組織建立帳戶時，不會自動收集獨立帳戶所需的所有資訊。對於您想要讓它獨立的每個帳戶，您必須接受選擇支援計劃，提供並驗證所需的聯絡資訊，然後提供目前的付款方法。AWS 會使用該付款方法來收取當帳戶未連接到組織時所發生的任何可計費 (非 AWS 免費方案) AWS 活動的費用。若要移除尚未取得此資訊的帳戶，請依照 從成員帳戶離開組織 中的步驟執行。
- 若要移除您在組織中建立的帳戶，您必須等到帳戶建立後至少七天。受邀的帳戶不受此等待期限的限制。
- 目前該帳戶成功離開組織，AWS 帳戶 擁有者負責累積的所有全新 AWS 成本，並使用帳戶的付款方式。組織的管理帳戶不再負責。
- 您想要移除的帳戶不得是為您組織啟用的任何 AWS 服務的委派管理員帳戶。如果帳戶是委派的系統管理員，您必須先將委派的管理員帳戶變更為組織中剩餘的另一個帳戶。如需有關如何停用或變更 AWS 服務的委派管理員帳戶的詳細資訊，請參閱該服務的文件。
- 即使在從組織內移除建立的帳戶 (使用 AWS Organizations 主控台或 `CreateAccount` API 建立的帳戶) 之後，(i) 建立的帳戶受到建立管理帳戶與我們簽訂的協議條款控管，以及 (ii) 建立的管理帳戶仍然聯合且個別負責其建立的帳戶所採取的任何動作。客戶與我們簽訂的協議，以及依據這些協議的權利和義務，在未經我們的同意的情況下，不能將其指派或轉讓。若要取得我們的同意，請聯絡 AWS。
- 當成員帳戶離開組織時，該帳戶就不再能夠帳戶存取作為組織成員期間的成本和使用狀況資料。不過，組織的管理帳戶仍然可以存取資料。如果帳戶重新加入組織，帳戶便能再次存取資料。
- 當成員帳戶離開組織時，會刪除連接至該帳戶的所有標籤。
- 當您從組織中移除成員帳戶時，不會自動刪除為啟用組織管理帳戶存取權而建立的任何 IAM 角色。如果您想要終止之前的組織管理帳戶的這種存取權，就必須手動刪除 IAM 角色。如需關於如何刪除角色的詳細資訊，請參閱 IAM 使用者指南中的刪除角色或執行個體設定檔。

從組織移除帳戶的影響

從組織移除帳戶時，不會對帳戶進行直接變更。不過，會發生以下間接影響：

- 帳戶現在要自行負責支付其費用，並且該帳戶必須連接有效的付款方法。
- 帳戶中的委託人不再受組織中套用的任何政策的影響。這表示 SCP 實施的限制將不再有效，而帳戶中的使用者和角色可能會較以前具有更多的許可。其他組織政策類型無法再強制執行或處理。
- 如果您使用任何政策中的 `aws:PrincipalOrgID` 條件鍵，以限制僅從組織中的 AWS 帳戶 存取使用者和角色，那麼您應檢閱並盡可能更新這些政策，再移除成員帳戶。如果您不更新政策，則帳戶離開組織時，帳戶中的使用者和角色可能會失去對資源的存取權。
- 與其他服務的整合可能會停用。如果您從已整合啟用的 AWS 服務的組織中移除帳戶，則該帳戶的使用者將無法再使用該服務。

從組織移除成員帳戶

登入組織的管理帳戶時，您可以從組織移除您不再需要的成員帳戶。若要這麼做，請執行下列作業：此程序僅適用於成員帳戶。若要移除管理帳戶，您必須刪除組織。

> **Note**
>
> 如果成員帳戶被從組織中移除，該成員帳戶即不再涵蓋於組織協議中。管理帳戶管理員應在從組織移除成員帳戶之前，與成員帳戶溝通此事，以便在必要時成員帳戶可以簽訂新的協議。您可以在AWS Artifact組織協議頁面的 AWS Artifact 主控台中，檢視作用中組織協議的清單。

> **最低許可**
>
> 若要從組織中移除一個或多個成員帳戶，您必須以管理帳戶中具有以下許可的使用者或角色身分登入：
>
> - `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要
> - `organizations:RemoveAccountFromOrganization`
>
> 如果您在步驟 5 中選擇以成員帳戶中的使用者或角色的身分登入，則該使用者或角色必須擁有以下許可：
>
> - `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要

- `organizations:LeaveOrganization` – 請注意，組織管理員可以套用會移除此許可的政策到您的帳戶，以防止您從您的組織移除帳戶。
- 如果您以 IAM 使用者的身分登入，而且帳戶缺少付款資訊，則使用者必須擁有 `aws-portal:ModifyBilling` 和 `aws-portal:ModifyPaymentMethods` 許可 (若該帳戶尚未遷移至精細許可) 或 `payments:CreatePaymentInstrument` 和 `payments:UpdatePaymentPreferences` 許可 (若該帳戶已遷移至精細許可)。此外，成員帳戶必須已啟用 IAM 使用者對帳單的存取權。如果尚未啟用，請參閱AWS Billing使用者指南中的啟用帳單和成本管理主控台的存取權。

AWS Management Console

從組織移除成員帳戶

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 AWS 帳戶 頁面上，尋找並選擇您要從您的組織移除的每個成員帳戶旁白的核取方塊 。

   您可以導覽 OU 階層，或啟用僅檢視 AWS 帳戶，以查看沒有 OU 結構的帳戶平面清單。如果您有許多帳戶，您可能需要在清單底部選擇載入更多採用 'ou-name' 的帳戶，以尋找您想要移動的所有內容。

   在 AWS 帳戶 頁面上，尋找並選擇您要從您的組織移除的成員帳戶的名稱。您可能需要展開 OU (選擇)，以尋找您想要的帳戶。
3. 選擇 Actions (動作)，然後在 AWS 帳戶 下，選擇 Remove from organization (從組織中移除)。
4. 在 Remove account 'account-name' (#account-id-num) from organization? (從組織中移除帳戶 'account-name' (#account-id-num)) 對話方塊中，選擇 Remove account (移除帳戶)。
5. 如果 AWS Organizations 無法移除一或多個帳戶，通常是因為您未提供帳戶以獨立帳戶形式運作所需的所有資訊。執行以下步驟：

   a. 登入失敗的帳戶。我們建議您透過選擇 Copy link (複製連結)，然後將連結貼到新無痕瀏覽器視窗的網址列來登入成員帳戶。如果您不使用無痕視窗，系統會將您從管理帳戶登出，並且將無法瀏覽回此對話方塊。

b. 您的瀏覽器會帶領您直接前往註冊程序，以完成此帳戶遺漏的任何步驟。完成提示的所有步驟。它們可能包含下列項目：

- 提供聯絡資訊
- 提供有效的付款方法
- 驗證電話號碼
- 選取支援計劃選項

c. 完成註冊最後一個步驟後，AWS 會自動將您的瀏覽器重新導向至該成員帳戶的 AWS Organizations 主控台。選擇 Leave organization (離開組織)，然後在確認對話方塊中確認您的選擇。系統會將您重新導向至 AWS Organizations 主控台的入門頁面，您可以在其中檢視任何擱置邀請，以便帳戶加入其他組織的。

d. 從組織移除授予帳戶存取權的 IAM 角色。

> **Important**
>
> 如果您的帳戶是在組織中建立的，則 Organizations 會自動在帳戶中建立 IAM 角色，使組織的管理帳戶具有存取權。如果帳戶是受邀加入，則 Organizations 不會自動建立此類角色，但是您或其他管理員可能已建立此類角色以獲得相同的利益。無論是哪一種情況，當您從組織移除帳戶時，任何此類角色都不會自動刪除。如果您想要終止之前的組織管理帳戶的這種存取權，就必須手動刪除此 IAM 角色。如需關於如何刪除角色的詳細資訊，請參閱 IAM 使用者指南中的刪除角色或執行個體設定檔。

AWS CLI & AWS SDKs

從組織移除成員帳戶

您可以使用下列其中一項命令來移除成員帳戶：

- AWS CLI: remove-account-from-organization

```
$ aws organizations remove-account-from-organization \
    --account-id 123456789012
```

此命令成功後就不會產生輸出。

- AWS SDKs: RemoveAccountFromOrganization

從組織移除帳戶之後，請確保從組織移除授予此帳戶存取權的 IAM 角色。

> **Important**
>
> 如果您的帳戶是在組織中建立的，則 Organizations 會自動在帳戶中建立 IAM 角色，使組織的管理帳戶具有存取權。如果帳戶是受邀加入，則 Organizations 不會自動建立此類角色，但是您或其他管理員可能已建立此類角色以獲得相同的利益。無論是哪一種情況，當您從組織移除帳戶時，任何此類角色都不會自動刪除。如果您想要終止之前的組織管理帳戶的這種存取權，就必須手動刪除此 IAM 角色。如需關於如何刪除角色的詳細資訊，請參閱 IAM 使用者指南中的刪除角色或執行個體設定檔。

會員帳戶可以使用 leave-organization 來移除自己。如需更多詳細資訊，請參閱 從成員帳戶離開組織。

從成員帳戶離開組織

登入某個成員帳戶時，您可以從其組織移除該帳戶。若要這麼做，請執行下列作業：此程序僅適用於成員帳戶。管理帳戶無法使用此技術來離開組織。若要移除管理帳戶，您必須刪除組織。

> **Note**
>
> 帳戶與組織的狀態，會影響顯示的成本和用量資料：
>
> - 如果成員帳戶離開組織而成為獨立帳戶，則帳戶一旦是組織之成員就無法再存取時間範圍內的成本和用量資料。帳戶只能存取做為獨立帳戶時所產生的資料。
> - 如果成員帳戶離開組織 A 而加入組織 B，則此帳戶就無法再存取其做為組織 A 成員之時間範圍內來自組織 A 的成本和用量資料。帳戶只能存取做為組織 B 成員時所產生的資料。
> - 如果帳戶重新加入先前所屬的組織，此帳戶會重新獲得對其過去成本與使用狀況資料的存取權。

> **Important**
>
> 如果您離開某個組織，您將不再受到組織的管理帳戶代表您接受的組織協議的涵蓋。您可以在 AWS Artifact Organization 協議頁面的 AWS Artifact 主控台中，檢視這些組織協議的清單。離

開組織之前，您應該判斷 (適當時，在您的法律、隱私權或合規團隊的協助下) 是否有必要設立新的協議。

最低許可

若要離開 AWS 組織，您必須擁有以下許可：

- `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要
- `organizations:LeaveOrganization` – 請注意，組織管理員可以套用會移除此許可的政策到您的帳戶，以防止您從您的組織移除帳戶。
- 如果您以 IAM 使用者的身分登入，而且帳戶缺少付款資訊，則使用者必須擁有 `aws-portal:ModifyBilling` 和 `aws-portal:ModifyPaymentMethods` 許可 (若該帳戶尚未遷移至精細許可) 或 `payments:CreatePaymentInstrument` 和 `payments:UpdatePaymentPreferences` 許可 (若該帳戶已遷移至精細許可)。此外，成員帳戶必須已啟用 IAM 使用者對帳單的存取權。如果尚未啟用，請參閱AWS Billing使用者指南中的啟用帳單和成本管理主控台的存取權。

AWS Management Console

若要從成員帳戶離開組織

1. 在 AWS Organizations 主控台，登入 AWS Organizations 主控台。您必須以 IAM 使用者的身分登入，擔任 IAM 角色，或以成員帳戶中的根使用者身分登入 (不建議)。

   依預設，在使用 AWS Organizations 建立的成員帳戶中，您沒有根使用者密碼的存取。如果必要，請遵循以根帳戶使用者身分存取成員帳戶的步驟來復原根使用者密碼。
2. 在組織儀表板頁面上，選擇離開此組織。
3. 在確認離開組織？對話方塊中，選擇離開組織。收到提示時，確認選擇移除帳戶。確認後，系統會將您重新導向至 AWS Organizations 主控台的入門頁面，您可以在其中檢視任何擱置邀請，以便帳戶加入其他組織的。

   如果顯示您目前無法離開組織訊息，表示您的帳戶沒有以獨立帳戶運作所需的完整資訊。如果是這種情況，請繼續下一個步驟。
4. 如果確認離開組織？對話方塊顯示您目前無法離開組織訊息，請選擇完成帳戶註冊步驟連結。
5. 在註冊 AWS 頁面上，輸入成為獨立帳戶所需的所有必要資訊。可能包括以下資訊類型：

- 聯絡人姓名及地址
- 有效的付款方式
- 電話號碼驗證
- 支援計劃選項

6. 看到說明註冊程序完成的對話方塊時，請選擇 Leave organization (離開組織)。

   出現確認對話方塊。確認選擇移除帳戶。系統會將您重新導向至 AWS Organizations 主控台的入門頁面，您可以在其中檢視任何擱置邀請，以便帳戶加入其他組織的。

7. 從組織移除授予帳戶存取權的 IAM 角色。

   > **Important**
   >
   > 如果您的帳戶是在組織中建立的，則 Organizations 會自動在帳戶中建立 IAM 角色，使組織的管理帳戶具有存取權。如果帳戶是受邀加入，則 Organizations 不會自動建立此類角色，但是您或其他管理員可能已建立此類角色以獲得相同的利益。無論是哪一種情況，當您從組織移除帳戶時，任何此類角色都不會自動刪除。如果您想要終止之前的組織管理帳戶的這種存取權，就必須手動刪除此 IAM 角色。如需關於如何刪除角色的詳細資訊，請參閱 IAM 使用者指南中的刪除角色或執行個體設定檔。

AWS CLI & AWS SDKs

以成員帳戶的身分離開組織

您可以使用下列其中一項命令來離開組織：

- AWS CLI: leave-organization

  下列範例會造成使用其憑證執行命令的帳戶離開組織。

  ```
  $ aws organizations leave-organization
  ```

  此命令成功後就不會產生輸出。

- AWS SDKs: LeaveOrganization

成員帳戶離開組織後，請確保從組織移除授予此帳戶存取權的 IAM 角色。

> **Important**
>
> 如果您的帳戶是在組織中建立的，則 Organizations 會自動在帳戶中建立 IAM 角色，使組織的管理帳戶具有存取權。如果帳戶是受邀加入，則 Organizations 不會自動建立此類角色，但是您或其他管理員可能已建立此類角色以獲得相同的利益。無論是哪一種情況，當您從組織移除帳戶時，任何此類角色都不會自動刪除。如果您想要終止之前的組織管理帳戶的這種存取權，就必須手動刪除此 IAM 角色。如需關於如何刪除角色的詳細資訊，請參閱 IAM 使用者指南中的刪除角色或執行個體設定檔。

管理帳戶中的使用者也可以改用 remove-account-from-organization 來移除成員帳戶。如需更多詳細資訊，請參閱 從組織移除成員帳戶。

關閉組織中的成員帳戶

如果您不再需要組織中的成員帳戶，可以按照本節中的說明從AWS Organizations 主控台關閉該帳戶。您只能在組織處於 [所有功能] 模式時，使用 AWS Organizations 主控台關閉成員帳戶。

您也可以在以 root 使用者身分登入 AWS Management Console 後， AWS 帳戶 直接從 [帳戶] 頁面關閉。如需相關 step-by-step 指示，請參閱《AWS 帳戶管理指南》 AWS 帳戶中的「關閉」。

若要關閉管理帳戶，請參閱關閉組織中的管理帳戶。

如何關閉成員帳戶

登入組織的管理帳戶時，您可以關閉屬於組織一部分的成員帳戶。若要執行此動作，請執行下列步驟。

> **Important**
>
> 在您關閉會員帳戶之前，我們強烈建議您檢閱考量事項並瞭解關閉帳戶的影響。如需詳細資訊，請參閱關閉帳戶前需要知道的事項和帳戶管理指南中關閉AWS 帳戶後的期望。

AWS Management Console

從 AWS Organizations 主控台關閉成員帳戶

1. 登入 AWS Organizations 主控台。

2. 在 AWS 帳戶 頁面上，尋找並選擇您要關閉的成員帳戶名稱。您可以導覽 OU 階層，或查看沒有 OU 結構的帳戶平面清單。
3. 選擇頁面頂端帳戶名稱旁的 Close (關閉)。處於合併帳單模式的 Organizations 無法在主控台中看到 [關閉] 按鈕。要以合併帳單模式關閉帳戶，請按照帳戶管理指南中如何關閉帳戶的獨立帳戶標籤中的AWS 步驟進行操作。
4. 選取每個核取方塊以確認所有必要的關閉帳戶敘述。
5. 輸入會員帳號 ID，然後選擇 [關閉帳戶]。

> **Note**
>
> 您關閉的任何成員帳戶都會在 AWS Organizations 主控台的帳戶名稱旁邊顯示一個SUSPENDED標籤。

從「帳戶」頁面關閉成員帳戶

或者，您可以直接從中的 [帳戶] 頁面關閉 AWS 成員帳戶 AWS Management Console。如需 step-by-step指引，請依照《AWS 帳戶管理指南》 AWS 帳戶中的關閉 a 中的指示進行。

AWS CLI & AWS SDKs

若要關閉 AWS 帳戶

您可以使用下列其中一項命令來關閉 AWS 帳戶：

- AWS CLI：close-account。

```
$ aws organizations close-account \
    --account-id 123456789012
```

此命令成功後就不會產生輸出。

- AWS 軟體開發套件：CloseAccount

保護成員帳戶以免遭關閉

如果您想保護成員以免遭意外關閉，您可以建立 IAM 政策，指定哪些帳戶免遭關閉。無法關閉受這些政策保護的任何成員帳戶。無法使用 SCP 達到這一點，因為不會影響管理帳戶中的主體。

您可以使用下列兩種方式，建立拒絕關閉帳戶的 IAM 政策：

- 在 Resource 元素中加入 arn，明確列出您要在政策中保護的每個帳戶。若要查看範例，請參閱 防止此政策中列出的成員帳戶遭關閉。
- 為個別帳戶加上標籤，以防遭關閉。在政策中使用 aws:ResourceTag 標籤全域條件金鑰，以防任何有該標籤的帳戶遭關閉。若要了解如何為帳戶加上標籤，請參閱為 Organizations 資源加上標籤。若要查看範例，請參閱 防止有標籤的成員帳戶遭關閉 。

防止關閉成員帳戶的範例 IAM 政策

下列程式碼範例顯示兩種不同的方法，可用來限制成員帳戶關閉其帳戶。

防止有標籤的成員帳戶遭關閉

您可以將以下政策連接至管理帳戶中的身分。此政策可防止管理帳戶中的主體關閉任何加上 aws:ResourceTag 標籤全域條件金鑰、AccountType 索引鍵和 Critical 標籤值的成員帳戶。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PreventCloseAccountForTaggedAccts",
            "Effect": "Deny",
            "Action": "organizations:CloseAccount",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/AccountType": "Critical"}
            }
        }
    ]
}
```

防止此政策中列出的成員帳戶遭關閉

您可以將以下政策連接至管理帳戶中的身分。此政策可防止管理帳戶中的主體關閉 Resource 元素中明確指定的成員帳戶。

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

```
        {
            "Sid": "PreventCloseAccount",
            "Effect": "Deny",
            "Action": "organizations:CloseAccount",
            "Resource": [
                "arn:aws:organizations::555555555555:account/
o-12345abcdef/123456789012",
                "arn:aws:organizations::555555555555:account/
o-12345abcdef/123456789014"
            ]
        }
    ]
}
```

關閉組織中的管理帳戶

若要關閉組織中的管理帳戶，您必須先關閉或移除組織中的所有成員帳戶。關閉管理帳戶的動作也會刪除的執行個體，以AWS Organizations及您在該組織內部建立的任何原則，在關閉後期間到期後。

如何關閉管理帳戶

請使用下列程序來關閉管理帳戶。

> **Important**
>
> 在您關閉管理帳戶之前，我們強烈建議您檢閱考量事項並瞭解關閉帳戶的影響。如需詳細資訊，請參閱關閉帳戶前需要知道的事項和帳戶管理指南中關閉帳戶後的AWS預期事項。

AWS Management Console

若要從 [帳戶] 頁面關閉管理帳戶

> **Note**
>
> 您無法直接從AWS Organizations主控台關閉管理帳戶。

1. 以您要關閉之AWS Management Console管理帳戶的根使用者身分登入。以 IAM 使用者或角色登入時，您無法關閉帳戶。

2. 確認您的組織中沒有任何作用中的成員帳戶。為此，請轉到AWS Organizations控制台，並確保所有成員帳戶都顯示在其帳戶名稱Suspended旁邊。如果您的會員帳戶仍處於活動狀態，則需要遵循中提供的指引，然關閉組織中的成員帳戶後才能進行下一個步驟。
3. 在右上角的導覽列上，選擇您的帳戶名稱或號碼，然後選擇 [帳戶]。
4. 在 [帳戶] 頁面上，捲動至頁面底部的 [關閉帳戶] 區段。閱讀並確保您了解帳戶關閉過程。
5. 選擇「關閉帳戶」按鈕以啟動科目關閉處理。
6. 在幾分鐘之內，您應該會收到一封電子郵件，確認您的帳戶已被關閉。

AWS CLI & AWS SDKs

AWS CLI 不支援此任務，其中一個 AWS SDK 中的 API 操作也不支援。您只能透過使用 AWS Management Console 執行此任務。

更新組織中的替代聯絡人

您可以使用 AWS Organizations 主控台，或以程式設計方式使用 AWS CLI 或 AWS SDK 來更新組織內帳戶的替代聯繫人。若要了解如何更新替代聯絡人，請參閱《AWS 帳戶管理參考》中的存取或更新替代聯絡人。

更新組織中的主要聯絡人資訊

您可以使用 AWS Organizations 主控台，或以程式設計的方式使用 AWS CLI 或 AWS SDK 來更新組織內帳戶的主要聯絡人。若要了解如何更新主要聯絡人資訊，請參閱《AWS 帳戶管理參考》中的存取或更新主要聯絡人。

更新組織中已啟用的 AWS 區域

您可使用 AWS Organizations 主控台，針對組織中的帳戶更新已啟用的 AWS 區域。若要了解如何更新已啟用的 AWS 區域，請參閱 AWS Account Management Reference (《AWS 帳戶管理參考》) 中的 Specifying which AWS 區域 your account can use (指定您的帳戶可以使用的 AWS 區域)。

管理 AWS Organizations 中的政策

AWS Organizations 中的政策可讓您對組織中的 AWS 帳戶 套用額外的管理類型。只有在您啟用組織中的所有功能時，才可以使用這些政策。

AWS Organizations 主控台會顯示每種政策類型的啟用或停用狀態。在 Organize accounts (組織帳戶) 索引標籤中，選擇左側導覽窗格中的 Root。畫面右側的詳細資訊窗格顯示所有可用的政策類型。此清單指出組織根中已啟用和已停用哪些政策類型。如果顯示 Enable (啟用) 類型的選項，則該類型目前已停用。如果顯示 Disable (停用) 類型的選項，則該類型目前已啟用。

政策類型

Organizations 提供下列兩大類別的政策類型：

授權政策

授權政策協助您集中管理組織中 AWS 帳戶 的安全。

- 服務控制政策 (SCP) 集中控制組織中所有帳戶可用的許可上限。

管理政策

管理政策可讓您集中設定和管理 AWS 服務及其功能。

- 人工智慧 (AI) 服務選擇退出政策可讓您控制組織所有帳戶的 AWS AI 服務的資料收集。
- 備份政策協助您集中管理備份計劃，並將備份計劃套用至組織各帳戶的 AWS 資源。
- 標籤政策協助您將標籤標準化，而這些標籤連接至組織帳戶中的 AWS 資源。

下表總結了每個政策類型的某些特性。如需這些政策類型的其他特性，請參閱 的配額 AWS Organizations。

Policy type (政策類型)	影響管理帳戶	可以連接至根、OU 或帳戶的數目上限	大小上限	支援檢視 OU 或帳戶的有效政策
SCP	 否	5	5120 個字元	 否
AI 服務選擇退出政策	 是	5	2500 個字元	 是
備份政策	 是	10	10,000 個字元	 是
標籤政策	 是	10	10,000 個字元	 是

在您的組織中使用政策

- 啟用和停用政策類型
- 取得組織政策的相關資訊
- AWS Organizations 的委派管理員
- 管理政策
- 服務控制政策 (SCP)

啟用和停用政策類型

啟用政策類型

建立政策並將其連接至組織之前，必須先啟用該政策類型以供使用。啟用政策類型是在組織根執行的一次性任務。您只能從組織的管理帳戶啟用政策類型。

最低許可

若要啟用政策類型，您必須有執行下列動作的許可：

- `organizations:EnablePolicyType`
- `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要
- `organizations:ListRoots` – 僅在使用 Organizations 主控台時才需要

AWS Management Console

啟用政策類型

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Policies (政策) 頁面上，選擇您要啟用的政策類型的名稱。
3. 在 Policy type (政策類型) 頁面上，選擇啟用 ***Policy type*** (政策類型)。

   此頁面會由指定類型的可用政策清單所取代。

AWS CLI & AWS SDKs

啟用政策類型

您可以使用下列其中一項命令來啟用政策類型：

- AWS CLI: enable-policy-type

  下列範例顯示如何啟用組織的備份政策。請注意，您必須指定組織根的 ID。

```
$ aws organizations enable-policy-type \
    --root-id r-a1b2 \
```

```
    --policy-type BACKUP_POLICY
{
    "Root": {
        "Id": "r-a1b2",
        "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
        "Name": "Root",
        "PolicyTypes": [
            {
                "Type": "BACKUP_POLICY",
                "Status": "ENABLED"
            }
        ]
    }
}
```

輸出中 `PolicyTypes` 的清單現在包含指定的政策類型且具有`ENABLED`Status。

- AWS SDKs: EnablePolicyType

停用政策類型

如果不想再在組織中使用特定政策類型，可以停用該類型以防止意外使用。您只能從組織的管理帳戶停用政策類型。

Important

- 當您停用政策類型時，所指定類型的所有政策都會自動與組織根的所有實體分離。這些政策不會被刪除。
- (僅限服務控制政策類型) 如果您稍後重新啟用 SCP 政策類型，組織根中的所有實體一開始只會連接至預設 `FullAWSAccess` SCP。在組織中停用 SCP 時，SCP 到實體的連接會中斷。如果您稍後想要重新啟用 SCP，必須視需要將其重新連接至組織的根、OU 和帳戶。

最低許可

若要停用 SCP，您需要具有執行下列動作的許可：

- `organizations:DisablePolicyType`
- `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要

- `organizations:ListRoots` – 僅在使用 Organizations 主控台時才需要

AWS Management Console

停用政策類型

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Policies (政策) 頁面上，選擇您要停用的政策類型的名稱。
3. 在 Policy type (政策類型) 頁面上，選擇停用 ***Policy type*** (政策類型)。
4. 在確認對話方塊上，輸入字詞 **disable**，然後選擇 Disable (停用)。

   指定類型的可用政策清單會消失。

AWS CLI & AWS SDKs

停用政策類型

您可以使用下列其中一項命令來停用政策類型：

- AWS CLI: disable-policy-type

  下列範例顯示如何停用組織的備份政策。請注意，您必須指定組織根的 ID。

```
$ aws organizations disable-policy-type \
    --root-id r-a1b2 \
    --policy-type BACKUP_POLICY
{
    "Root": {
        "Id": "r-a1b2",
        "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
        "Name": "Root",
        "PolicyTypes": []
    }
}
```

  輸出中 `PolicyTypes` 的清單不再包含指定的政策類型。

- AWS SDKs: DisablePolicyType

取得組織政策的相關資訊

本節描述取得組織中政策詳細資訊的各種方式。這些程序適用於所有政策類型。您必須在組織根上啟用政策類型，才能將該類型的政策連接至該組織根中的任何實體。

列出所有政策

最低許可

若要列出您的組織內的政策，您必須擁有以下許可：

- `organizations:ListPolicies`

您可以在 AWS Management Console 或使用 AWS Command Line Interface(AWS CLI) 命令或 AWS SDK 操作，來檢視組織中的政策。

AWS Management Console

列出組織中的所有政策

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Policies (政策) 頁面上，選擇您要列出的政策類型。

   如果已啟用指定的政策類型，主控台會顯示組織中目前可用的所有該類型政策的清單。
3. 返回 Policies (政策) 頁面，然後針對每個政策類型重複執行此操作。

AWS CLI & AWS SDKs

列出組織中的所有政策

您可以使用以下其中一項命令來列出組織中的政策：

- AWS CLI: list-policies

  下列範例顯示如何取得組織中所有服務控制政策的清單。您必須指定想要查看的政策類型。為每個您要包含在其中的政策類型重複該命令。

```
$ aws organizations list-policies \
```

```
    --filter SERVICE_CONTROL_POLICY
{
    "Policies": [
        {
            "Id": "p-FullAWSAccess",
            "Arn": "arn:aws:organizations::aws:policy/service_control_policy/p-
FullAWSAccess",
            "Name": "FullAWSAccess",
            "Description": "Allows access to every operation",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": true
        }
    ]
}
```

- AWS SDKs: ListPolicies

列出連接到根、OU 或帳戶的政策

最低許可

若要列出連接到您組織內的根、組織單位 (OU) 或帳戶的政策，您必須擁有以下許可：

- `organizations:ListPoliciesForTarget`，並在包含指定目標 (或 "*") 的 Amazon 資源名稱 (ARN) 的相同政策陳述式中具有 `Resource` 元素

AWS Management Console

列出直接連接到指定的根、OU 或帳戶的所有政策

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 AWS 帳戶 頁面上，選擇您要檢視其政策的根、OU 或帳戶的名稱。您可能需要展開 OU (選擇 ▶)，以尋找您想要的 OU。
3. 在根、OU 或帳戶頁面上，選擇 Policies (政策) 索引標籤。

   Policies (政策) 索引標籤會顯示連接至該根、OU 或帳戶的所有政策，並依政策類型分組。

AWS CLI & AWS SDKs

列出直接連接到指定的根、OU 或帳戶的所有政策

您可以使用下列其中一項命令來列出連接到實體的政策：

- AWS CLI: list-policies-for-target

  下列範例會列出連接至指定 OU 的所有服務控制政策。您必須同時指定根、OU 或帳戶的 ID，以及您想要列出的政策類型。

```
$ aws organizations list-policies-for-target \
    --target-id ou-a1b2-f6g7h222 \
    --filter SERVICE_CONTROL_POLICY
{
    "Policies": [
        {
            "Id": "p-FullAWSAccess",
            "Arn": "arn:aws:organizations::aws:policy/service_control_policy/p-
FullAWSAccess",
            "Name": "FullAWSAccess",
            "Description": "Allows access to every operation",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": true
        }
    ]
}
```

- AWS SDKs: ListPoliciesForTarget

列出政策連接的所有根帳戶、OU 和帳戶

最低許可

若要列出政策連接的實體，您必須擁有以下許可：

- `organizations:ListTargetsForPolicy`，並在包含指定政策 (或 "*") 的 ARN 的相同政策陳述式中具有 `Resource` 元素

AWS Management Console

列出已連接指定政策的所有根、OU 和帳戶

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在政策頁面上，選擇政策類型，然後選擇您要檢查其附件的政策名稱。
3. 選擇 Targets (目標)索引標籤，以顯示所選政策連接的每個根、OU 和帳戶的資料表。

AWS CLI & AWS SDKs

列出已連接指定政策的所有根、OU 和帳戶

您可以使用下列其中一項命令來列出擁有政策的實體：

- AWS CLI: list-targets-for-policy

  下列範例顯示指定政策的根、OU 和帳戶的所有連接。

```
$ aws organizations list-targets-for-policy \
    --policy-id p-FullAWSAccess
{
    "Targets": [
        {
            "TargetId": "ou-a1b2-f6g7h111",
            "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h111",
            "Name": "testou2",
            "Type": "ORGANIZATIONAL_UNIT"
        },
        {
            "TargetId": "ou-a1b2-f6g7h222",
            "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h222",
            "Name": "testou1",
            "Type": "ORGANIZATIONAL_UNIT"
        },
        {
            "TargetId": "123456789012",
            "Arn": "arn:aws:organizations::123456789012:account/o-
aa111bb222/123456789012",
            "Name": "My Management Account (bisdavid)",
```

```
            "Type": "ACCOUNT"
        },
        {
            "TargetId": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "Type": "ROOT"
        }
    ]
}
```

- AWS SDKs: ListTargetsForPolicy

取得關於政策的詳細資訊

最低許可

若要顯示政策的詳細資訊，您必須擁有以下許可：

- `organizations:DescribePolicy`，並在包含指定政策 (或 "*") 的 ARN 的相同政策陳述式中具有 `Resource` 元素

AWS Management Console

取得關於政策的詳細資訊

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Policies (政策) 頁面上，選擇您要檢查的政策類型，然後選擇政策名稱。

   政策頁面顯示關於政策的可用資訊，包括其 ARN、描述和連接的目標。

   - Content (內容) 索引標籤會以 JSON 格式顯示政策的目前內容。
   - Targets (目標) 索引標籤會顯示政策連接的根、OU 和帳戶的清單。
   - Tags (標籤) 索引標籤會顯示附加至政策的標籤。注意：Tags (標籤) 索引標籤不適用於 AWS 受管政策。

若要編輯政策，請選擇 Edit policy (編輯政策)。由於每個政策類型都有不同的編輯需求，因此，請參閱建立和更新指定政策類型之政策的指示。

AWS CLI & AWS SDKs

取得關於政策的詳細資訊

您可以使用下列其中一項命令來取得關於政策的詳細資訊：

- AWS CLI: describe-policy

  下列範例顯示指定政策的詳細資訊。

```
$ aws organizations describe-policy \
    --policy-id p-FullAWSAccess
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-FullAWSAccess",
            "Arn": "arn:aws:organizations::aws:policy/service_control_policy/p-
FullAWSAccess",
            "Name": "FullAWSAccess",
            "Description": "Allows access to every operation",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": true
        },
        "Content": "{\n  \"Version\": \"2012-10-17\",\n  \"Statement\": [\n    {\n
      \"Effect\": \"Allow\",\n      \"Action\": \"*\",\n      \"Resource\": \"*
\"\n    }\n  ]\n}"
    }
}
```

- AWS SDKs: DescribePolicy

AWS Organizations 的委派管理員

我們建議您僅將 AWS Organizations 管理帳戶及其使用者和角色用於必須由該帳戶執行的任務。我們也建議您將 AWS 資源存放在組織內其他成員帳戶中，且將其保存在管理帳戶之外。這是因為安全性功能 (例如 Organizations 服務控制政策 (SCP)) 不會限制管理帳戶中的使用者或角色。

從組織的管理帳戶，您可以將 Organizations 的政策管理委派給指定的成員帳戶，以執行預設僅適用於管理帳戶的政策動作。

建立或更新以資源為基礎的委派政策

從管理帳戶中，為組織建立或更新以資源為基礎的委派政策，並新增可指定哪些成員帳戶可對政策執行動作的陳述式。您可以在政策中新增多個陳述式，以表示成員帳戶的不同許可集。

最低許可

若要建立或更新以資源為基礎的委派政策，您需要具有下列動作的執行許可：

- `organizations:PutResourcePolicy`
- `organizations:DescribeResourcePolicy`

此外，您必須授與委派管理員帳戶中的角色和使用者對應的 IAM 許可，以執行必要動作。如果沒有 IAM 許可，則假設呼叫主體沒有必要許可，無法管理 AWS Organizations 政策。

AWS Management Console

使用以下其中一個方法，在 AWS Management Console 中將陳述式新增至以資源為基礎的委派政策：

- JSON 政策 – 貼上並自訂要在帳戶中使用的以資源為基礎的委派政策範例，或在 JSON 編輯器中輸入您自己的 JSON 政策文件。
- 視覺化編輯器 – 在視覺化編輯器中建構新的委派政策，此政策會引導您建立委派政策，而不需要撰寫 JSON 語法。

使用 JSON 政策編輯器來建立或更新委派政策

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 選擇 Settings (設定)。
3. 在 AWS Organizations 的委派管理員區段中，選擇委派以建立 Organizations 委派政策。若要更新現有的委派政策，請選擇 Edit (編輯)。

4. 輸入或貼上 JSON 政策文件。如需有關 IAM 政策語言的詳細資訊，請參閱 IAM JSON 政策參考。
5. 解決政策驗證期間產生的任何安全性警告、錯誤或一般性警告，然後選擇 Create policy (建立政策) 以儲存工作。

使用視覺化編輯器來建立或更新委派政策

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 選擇 Settings (設定)。
3. 在 AWS Organizations 的委派管理員區段中，選擇委派以建立 Organizations 委派政策。若要更新現有的委派政策，請選擇 Edit (編輯)。
4. 在 Create Delegation policy (建立委派政策) 頁面上，選擇 Add new statement (新增陳述式)。
5. 將 Effect (效果) 設定為 `Allow`。
6. 新增 `Principal` 以定義您要委派的成員帳戶。如需有關語法的詳細資訊，請參閱 以資源為基礎的委派政策範例。
7. 從 Actions (動作) 清單中，選擇您要委派的動作。您可使用 Filter actions (篩選動作)，以縮減選項。
8. 若要指定委派的成員帳戶是否可將政策連接至組織根目錄或組織單位 (OU)，請設定 `Resources`。您也必須選取 `policy` 作為資源類型。如需其他詳細資訊，請參閱 以資源為基礎的委派政策範例。您可採用以下方式來指定資源：
   - 選擇 Add a resource (新增資源)，並按照對話方塊中的提示建構 Amazon Resource Name (ARN)。
   - 在編輯器中手動列出資源 ARN。如需有關 ARN 語法的詳細資訊，請參閱《AWS 一般參考指南》中的 Amazon Resource Name (ARN)。如需有關在政策資源元素中使用 ARN 的詳細資訊，請參閱 IAM JSON 政策元素：Resource。
9. 選擇 Add a condition (新增條件) 以指定其他條件，包括您要委派的政策類型。選擇條件的 Condition key (條件索引鍵)、Tag key (標籤索引鍵)、Qualifier (修飾詞) 以及 Operator (運算子)，然後輸入 **`Value`**。如需其他詳細資訊，請參閱 以資源為基礎的委派政策範例。完成時，請選擇 Add condition (新增條件)。如需有關 Condition (條件) 元素的詳細資訊，請參閱 IAM JSON 政策參考中的 IAM JSON 政策元素：Condition。
10. 若要新增更多許可區塊，請選擇 Add new statement (新增陳述式)。針對每個區塊皆重複步驟 5 到 9。

11. 解決政策驗證期間產生的任何安全性警告、錯誤或一般性警告，然後選擇 Create policy (建立政策) 以儲存工作。

AWS CLI & AWS SDKs

建立或更新委派政策

您可以使用下列命令來建立或更新委派政策：

- AWS CLI：put-resource-policy

  以下範例會建立或更新委派政策。

```
$ aws organizations put-resource-policy --content
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Fully_manage_backup_policies",
            "Effect": "Allow",
            "Principal": {
                "AWS": "135791357913"
            }
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:CreatePolicy",
                "organizations:DescribePolicy",
                "organizations:UpdatePolicy",
                "organizations:DeletePolicy",
                "organizations:AttachPolicy",
                "organizations:DetachPolicy"
            ],
            "Resource": [
                "arn:aws:organizations::246802468024:root/o-abcdef/r-pqrstu",
                "arn:aws:organizations::246802468024:ou/o-abcdef/*",
                "arn:aws:organizations::246802468024:account/o-abcdef/*",
                "arn:aws:organizations::246802468024:organization/policy/
backup_policy/*",
            ],
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:PolicyType": [
```

```
                        "BACKUP_POLICY"
                    ]
                }
            }
        }
    ]
}
```

- AWS SDK：PutResourcePolicy

支援的委派政策動作

委派政策支援下列動作：

- AttachPolicy
- CreatePolicy
- DeletePolicy
- DescribeAccount
- DescribeCreateAccountStatus
- DescribeEffectivePolicy
- DescribeHandshake
- DescribeOrganization
- DescribeOrganizationalUnit
- DescribePolicy
- DescribeResourcePolicy
- DetachPolicy
- DisablePolicyType
- EnablePolicyType
- ListAccounts
- ListAccountsForParent
- ListAWSServiceAccessForOrganization
- ListChildren
- ListCreateAccountStatus

- ListDelegatedAdministrators
- ListDelegatedServicesForAccount
- ListHandshakesForAccount
- ListHandshakesForOrganization
- ListOrganizationalUnitsForParent
- ListParents
- ListPolicies
- ListPoliciesForTarget
- ListRoots
- ListTagsForResource
- ListTargetsForPolicy
- TagResource
- UntagResource
- UpdatePolicy

檢視以資源為基礎的委派政策

在管理帳戶中，檢視組織的以資源為基礎的委派政策，以了解哪些委派管理員有存取權，可管理哪些政策類型。

> **最低許可**
>
> 若要檢視以資源為基礎的委派政策，您需要具有下列動作的執行許可：organizations:DescribeResourcePolicy。

AWS Management Console

檢視委派政策

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 選擇 Settings (設定)。

3. 在 AWS Organizations 的委派管理員區段中，捲動以檢視完整的委派政策。

AWS CLI & AWS SDKs

檢視委派政策

您可以使用下列命令來檢視委派政策：

- AWS CLI：describe-resource-policy

  以下範例會擷取政策。

  ```
  $ aws organizations describe-resource-policy
  ```

- AWS SDK：DescribeResourcePolicy

刪除以資源為基礎的委派政策

當您不再需要委派組織中的政策管理時，可以從組織的管理帳戶中刪除以資源為基礎的委派政策。

> **Important**
>
> 如果刪除以資源為基礎的委派政策，則無法將其復原。

> **最低許可**
>
> 若要刪除以資源為基礎的委派政策，您需要具有下列動作的執行許可：`organizations:DeleteResourcePolicy`。

AWS Management Console

刪除委派政策

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 選擇 Settings (設定)。

3. 在 AWS Organizations 的委派管理員區段，選擇刪除。
4. 在 Delete policy (刪除政策) 確認對話方塊中，輸入 **delete**。然後，選擇 Delete policy (刪除政策)。

AWS CLI & AWS SDKs

刪除委派政策

您可以使用下列項命令來刪除委派政策：

- AWS CLI：delete-resource-policy

  以下範例會刪除政策。

  ```
  $ aws organizations delete-resource-policy
  ```

- AWS SDK：DeleteResourcePolicy

以資源為基礎的委派政策範例

下列程式碼範例示範如何使用以資源為基礎的委派政策。

範例

- 範例：檢視組織、OU、帳戶和政策
- 範例：用於管理組織備份政策的合併許可

範例：檢視組織、OU、帳戶和政策

在委派政策管理之前，您必須委派導覽組織結構的許可，並查看組織單位 (OU)、帳戶及其附加的政策。

此範例顯示如何將這些許可納入成員帳戶 *AccountId* 的以資源為基礎的委派政策中。

> **Important**
>
> 儘管您可以使用此政策委派任何 Organizations 唯讀動作，但建議您只包含範例中所示的最低必要動作的許可。

此委派政策範例僅會授予從 AWS API 或 AWS CLI 以程式設計方式完成動作的必要許可。若要使用此委派政策，請以您自己的資訊取代 *AccountId* 的 AWS 預留位置文字。然後，依照 AWS Organizations 的委派管理員中的指示操作。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegatingNecessaryDescribeListActions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::AccountId:root"
      },
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:ListTagsForResource"
      ],
      "Resource": "*"
    }
  ]
}
```

範例：用於管理組織備份政策的合併許可

此範例顯示如何建立以資源為基礎的委派政策，以允許管理帳戶委派在組織內管理備份政策所需的完整許可，包括 create、read、update 和 delete 動作，以及 attach 和 detach 政策動作。若要了解每個動作、資源和條件的重要性，請參閱以資源為基礎的委派政策範例。

> **Important**
>
> 此政策可讓委派管理員對組織中任何帳戶 (包括管理帳戶) 建立的政策執行指定的動作。

此委派政策範例僅會授予從 AWS API 或 AWS CLI 以程式設計方式完成動作的必要許可。若要使用此委派政策，請以您自己的資訊取代 *MemberAccountId*、*ManagementAccountId*、*OrganizationId* 和 *RootId* 的 AWS 預留位置文字。然後，依照 AWS Organizations 的委派管理員中的指示操作。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegatingNecessaryDescribeListActions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:ListTagsForResource"
      ],
      "Resource": "*",
      "Condition": {
        "StringLikeIfExists": {
          "organizations:PolicyType": "BACKUP_POLICY"
        }
      }
```

```
    },
    {
      "Sid": "DelegatingAllActionsForBackupPolicies",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
        "organizations:CreatePolicy",
        "organizations:UpdatePolicy",
        "organizations:DeletePolicy",
        "organizations:AttachPolicy",
        "organizations:DetachPolicy",
        "organizations:EnablePolicyType",
        "organizations:DisablePolicyType"
      ],
      "Resource": [
        "arn:aws:organizations::ManagementAccountId:root/o-OrganizationId/r-RootId",
        "arn:aws:organizations::ManagementAccountId:ou/o-OrganizationId/*",
        "arn:aws:organizations::ManagementAccountId:account/o-OrganizationId/*",
        "arn:aws:organizations::ManagementAccountId:policy/o-OrganizationId/
backup_policy/*"
      ]
    }
  ]
}
```

管理政策

管理政策可讓您集中設定和管理 AWS 服務及其功能。政策究竟如何影響繼承它們的 OU 和帳戶，取決於在 AWS Organizations 中套用的管理政策類型。檢閱本區段中的主題，以理解有關管理政策的相關術語和概念。

主題

- 理解管理政策繼承
- AI 服務選擇退出政策
- 備份政策
- 標籤政策

理解管理政策繼承

> **Note**
>
> 本區段中的資訊不適用於 SCP，因為 SCP 同時管理允許和拒絕 IAM 動作。雖然 SCP 會連接至根、OU 和帳戶，但允許執行動作需要每個層級的 SCP 中明確的 `allow` 陳述式，範圍從根目錄到帳戶直接路徑中的每個 OU (包括目標帳戶本身) 。如需 SCP 在 AWS Organizations 階層中的運作方式的詳細資訊，請參閱 SCP 評估。

您可以在組織中將這些管理政策連接至組織實體 (組織根、組織單位 (OU) 或帳戶) :

- 當您將管理政策連接至組織根時，組織中的所有 OU 和帳戶都會繼承該政策。
- 當您將管理政策連接至特定 OU 時，直屬於該 OU 或任何子 OU 的帳戶會繼承此政策。
- 當您將管理政策連接至特定帳戶時，它只會影響該帳戶。

因為您可以將管理政策連接至組織中的多個層級，所以帳戶可以繼承多個政策。

本節說明如何將父政策和子政策處理成帳戶的有效策略。

主題

繼承術語

本主題在討論管理政策繼承時會使用下列術語。

政策繼承

組織不同層級的政策互動，從組織的頂層根下移至組織單位 (OU) 階層，再到個別帳戶。

您可以將政策連接至組織根、OU、個別帳戶，以及這些組織實體的任何組合。政策繼承是指連接至組織根或 OU 的管理政策。在連接管理政策的組織根目錄或 OU 中，所有成員帳戶都繼承該政策。

例如，當管理政策連接至組織根時，組織中的所有帳戶都會繼承該政策。這是因為組織中的所有帳戶永遠都在組織根下。當您將標籤政策連接至特定 OU 時，直屬於該 OU 或任何子 OU 的帳戶會繼承該政策。因為您可以將政策連接至組織中的多個層級，所以帳戶可能會繼承單一政策類型的多個政策文件。

父政策

在組織樹狀結構中較上方連接的政策，高於樹狀結構中連接至較低實體的政策。

例如，如果您將管理政策 A 連接至組織根，就只是政策而已。如果您也將政策 B 連接至該根下的 OU，而政策 A 是政策 B 的父政策。政策 B 是政策 A 的子政策。政策 A 和政策 B 合併，為 OU 中的帳戶建立有效的標籤政策。

子政策

在組織樹狀結構中比父政策更低的層級上連接的政策。

有效政策

指定規則以套用至帳戶的最終單一政策文件。帳戶繼承的任何政策，加上直接連接至帳戶的任何政策，聚集而成有效政策。例如，標籤策略可讓您檢視適用於任何帳戶的有效標籤政策。如需更多詳細資訊，請參閱 檢視有效的標籤政策。

繼承運算子

控制繼承的政策如何合併成為單一有效政策的運算子。這些運算子視為進階功能。經驗豐富的政策作者可以使用這些運算子，限制子政策可以進行哪些變更和政策中的設定如何合併。如需更多詳細資訊，請參閱 繼承運算子。

政策語法與管理政策類型的繼承

政策究竟如何影響繼承它們的 OU 和帳戶，取決於所選管理政策的類型。管理政策類型包括：

- 人工智慧 (AI) 服務選擇退出政策
- 備份政策
- 標籤政策

管理政策類型的語法包含繼承運算子，可讓您精細地指定要套用父政策中的哪些元素，以及哪些元素在被子 OU 和帳戶繼承時可以被覆寫或修改。

有效政策是從組織根和 OU 繼承的一組規則，以及直接連接到帳戶的規則。有效政策會指定套用至帳戶的最終規則集。您可以檢視帳戶的有效政策，其中包含所套用政策中所有繼承運算子的效果。如需更多詳細資訊，請參閱 檢視有效的標籤政策。

繼承運算子

繼承運算子可控制繼承的政策和帳戶政策如何合併成為帳戶的有效政策。這些運算子包括值-設定運算子和子控制運算子。

當您在 AWS Organizations 主控台使用視覺化編輯器時，只能使用 @@assign 運算子。其他運算子視為進階功能。若要使用其他運算子，您必須手動撰寫 JSON 政策。經驗豐富的政策作者可以使用繼承運算子，控制哪些值套用至有效的政策，並限制子政策可以進行哪些變更。

值-設定運算子

您可以使用下列值-設定運算子來控制政策與其父政策的互動方式。

- `@@assign` – 使用指定的設定覆寫任何繼承的政策設定。如果未繼承指定的設定，此運算子會將其新增至有效政策。此運算子可套用至任何類型的任何政策設定。
  - 對於單值設定，此運算子會以指定的值取代繼承的值。
  - 對於多值設定 (JSON 陣列)，此運算子會移除任何繼承的值，並取代為此政策指定的值。
- `@@append` – 將指定的設定 (不刪除任何項目) 新增至繼承的設定。如果未繼承指定的設定，此運算子會將其新增至有效政策。此運算子只能與多值設定一起使用。
  - 此運算子會將指定的值新增至繼承陣列中的任何值。
- `@@remove` – 從有效政策中移除指定的繼承設定 (如果存在)。此運算子只能與多值設定一起使用。
  - 此運算子會從繼承自父政策的值陣列中，只移除指定的值。其他值可以繼續存在於陣列中，而且可以由子政策繼承。

子控制運算子

可自行決定是否使用子控制運算子。您可以使用 `@@operators_allowed_for_child_policies` 運算子來控制子政策可以使用哪些值-設定運算子。您可以允許所有運算子、某些特定運算子或不允許運算子。根據預設，允許所有運算子 (`@@all`)。

- `"@@operators_allowed_for_child_policies":["@@all"]` – 子 OU 和帳戶可以在政策中使用任何運算子。根據預設，子政策中允許所有運算子。

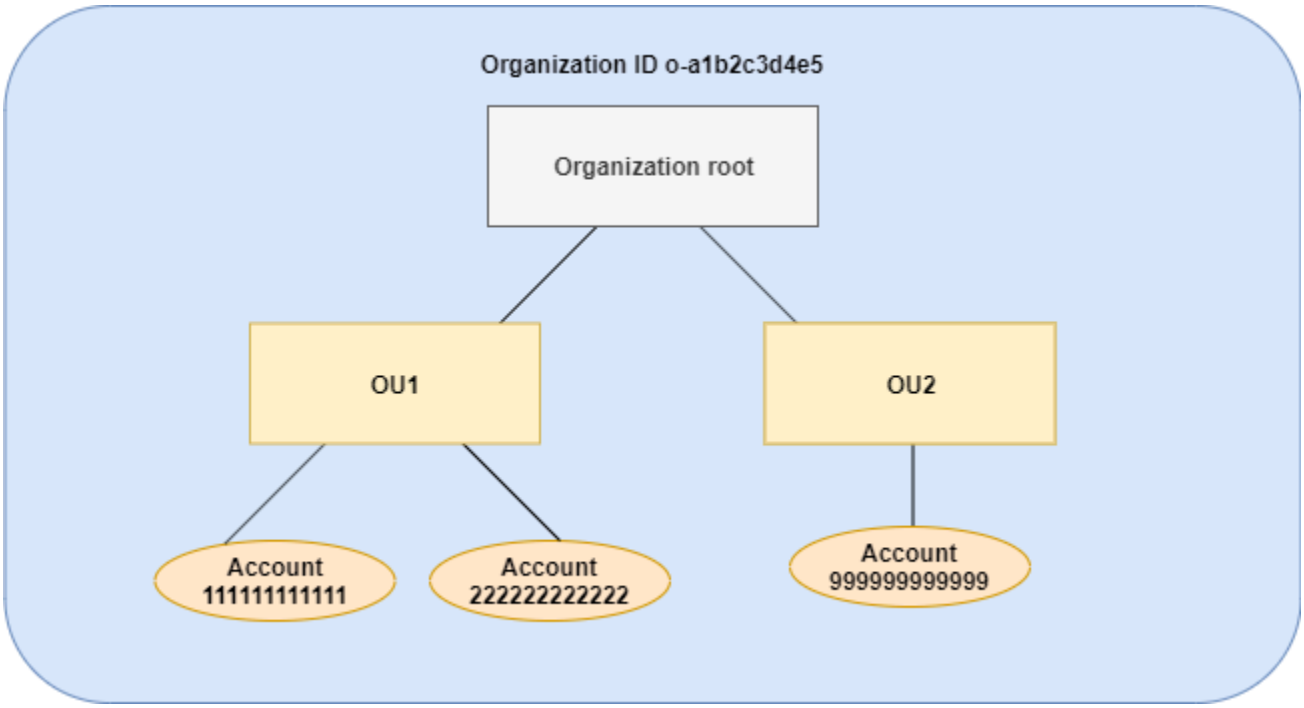
- `"@@operators_allowed_for_child_policies":["@@assign", "@@append", "@@remove"]` – 子 OU 和帳戶在子政策中只能使用指定的運算子。您可以在此子控制運算子中指定一或多個值-設定運算子。
- `"@@operators_allowed_for_child_policies":["@@none"]` – 子 OU 和帳戶在政策中無法使用運算子。您可以使用此運算子，有效封鎖父政策中定義的值，讓子政策無法新增、附加或移除這些值。

> **Note**
>
> 如果繼承的子控制運算子禁止使用某個運算子，則您無法在子政策中反轉該規則。如果您將子控制運算子包含在父政策中，則會限制所有子政策中的值-設定運算子。

繼承範例

這些範例顯示父標籤和子標籤政策如何合併成為帳戶的有效標籤政策，以示範政策繼承的運作方式。

這些範例假設您有如下圖所示的組織結構。



範例

- 範例 1：允許子政策只覆寫標籤值
- 範例 2：將新值附加到繼承的標籤

- 範例 3：從繼承的標籤中移除值
- 範例 4：限制對子政策的變更
- 範例 5：與子控制運算子衝突
- 範例 6：與相同階層層級上附加的值衝突

範例 1：允許子政策只覆寫標籤值

下列標籤政策定義 CostCenter 標籤鍵和兩個可接受的值 (Development 和 Support)。如果您將此政策連接至組織根，則會對組織中的所有帳戶產生效果。

政策 A – 組織根標籤政策

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "Development",
                    "Support"
                ]
            }
        }
    }
}
```

假設您希望 OU1 中的使用者對某個索引鍵使用不同的標籤值，而且想要針對特定的資源類型強制執行標籤政策。因為政策 A 未指定允許哪些子控制運算子，所以允許所有運算子。您可以使用 @@assign 運算子，並建立如下的標籤政策以連接至 OU1。

政策 B – OU1 標籤政策

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
```

```
                "@@assign": [
                    "Sandbox"
                ]
            },
            "enforced_for": {
                "@@assign": [
                    "redshift:*",
                    "dynamodb:table"
                ]
            }
        }
    }
}
```

當政策 A 和政策 B 合併以形成帳戶的有效標籤政策時，為標籤指定 @@assign 運算子會執行以下操作：

- 政策 B 覆寫父政策 (政策 A) 中指定的兩個標籤值。結果是 Sandbox 是 CostCenter 標籤鍵的唯一合規值。
- 新增的 enforced_for 指定在所有 Amazon Redshift 資源和 Amazon DynamoDB 資料表上，CostCenter 標籤必須使用指定的標籤值。

如圖所示，OU1 包含兩個帳戶：111111111111 和 222222222222。

帳戶 111111111111 和 222222222222 所產生的有效標籤政策

> **Note**
>
> 您無法直接使用顯示的有效政策的內容作為新政策的內容。語法不包括控制與其他子政策和父政策合併所需的運算子。顯示有效政策僅用於了解合併的結果。

```
{
    "tags": {
        "costcenter": {
            "tag_key": "CostCenter",
            "tag_value": [
                "Sandbox"
            ],
            "enforced_for": [
```

```
                "redshift:*",
                "dynamodb:table"
            ]
        }
    }
}
```

範例 2：將新值附加到繼承的標籤

在某些情況下，您希望組織中的所有帳戶以簡短的可接受值清單來指定標籤鍵。對於一個 OU 中的帳戶，在建立資源時，您可能想要允許只有這些帳戶才可以指定的額外值。此範例指出如何利用 @@append 運算子來這樣做。@@append 運算子是進階功能。

與範例 1 一樣，此範例一開始也以政策 A 當作組織根標籤政策。

政策 A – 組織根標籤政策

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "Development",
                    "Support"
                ]
            }
        }
    }
}
```

在此範例中，將政策 C 連接至 OU2。此範例的差異在於，在政策 C 中使用 @@append 運算子會新增至 (而非覆寫) 可接受的值清單和 enforced_for 規則。

政策 C – OU2 標籤政策，用於附加值

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
```

```
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@append": [
                    "Marketing"
                ]
            },
            "enforced_for": {
                "@@append": [
                    "redshift:*",
                    "dynamodb:table"
                ]
            }
        }
    }
}
```

當政策 A 和政策 C 合併形成帳戶的有效標籤政策時，將政策 C 連接至 OU2 會產生下列效果：

- 因為政策 C 包含 @@append 運算子，所以允許新增至 (而非覆寫) 政策 A 中指定的可接受標籤值清單。
- 與政策 B 一樣，新增的 enforced_for 指定在所有 Amazon Redshift 資源和 Amazon DynamoDB 資料表上，CostCenter 標籤必須做為指定的標籤值。如果父政策不含子控制運算子來限制子政策可指定的內容，則覆寫 (@@assign) 和新增 (@@append) 有相同的效果。

如圖所示，OU2 包含一個帳戶：999999999999。政策 A 和政策 C 合併，為帳戶 999999999999 建立有效的標籤政策。

帳戶 999999999999 的有效標籤政策

> **Note**
>
> 您無法直接使用顯示的有效政策的內容作為新政策的內容。語法不包括控制與其他子政策和父政策合併所需的運算子。顯示有效政策僅用於了解合併的結果。

```
{
    "tags": {
        "costcenter": {
            "tag_key": "CostCenter",
```

```
            "tag_value": [
                "Development",
                "Support",
                "Marketing"
            ],
            "enforced_for": [
                "redshift:*",
                "dynamodb:table"
            ]
        }
    }
}
```

範例 3：從繼承的標籤中移除值

在某些情況下，連接至組織的標籤政策所定義的標籤值，可能超過您希望帳戶使用的數量。此範例說明如何使用 @@remove 運算子修訂標籤政策。@@remove 是進階功能。

與其他範例一樣，此範例一開始也以政策 A 當作組織根標籤政策。

政策 A – 組織根標籤政策

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "Development",
                    "Support"
                ]
            }
        }
    }
}
```

在此範例中，將政策 C 連接至帳戶 999999999999。

政策 D – 帳戶 999999999999 標籤政策，用於移除值

```
{
```

```
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@remove": [
                    "Development",
                    "Marketing"
                ],
                "enforced_for": {
                    "@@remove": [
                        "redshift:*",
                        "dynamodb:table"
                    ]
                }
            }
        }
    }
}
```

當政策 A、政策 C 和政策 D 合併形成有效的標籤政策時，將政策 D 連接至帳戶 999999999999 會產生下列效果：

- 假設您已執行所有先前的範例，則政策 B、C 和 C 是 A 的子政策。政策 B 只連接至 OU1，因此不影響帳戶 9999999999999。
- 對於帳戶 9999999999999，`CostCenter` 標籤鍵唯一可接受的值是 `Support`。
- 不強制 `CostCenter` 標籤鍵合規。

帳戶 999999999999 新的有效標籤政策

> **Note**
>
> 您無法直接使用顯示的有效政策的內容作為新政策的內容。語法不包括控制與其他子政策和父政策合併所需的運算子。顯示有效政策僅用於了解合併的結果。

```
{
    "tags": {
        "costcenter": {
```

```
            "tag_key": "CostCenter",
            "tag_value": [
                "Support"
            ]
        }
    }
}
```

如果您稍後將更多帳戶新增至 OU2，其有效的標籤政策將與帳戶 999999999999 有所不同。這是因為更嚴格的政策 D 只在帳戶層級連接，而不是連接至 OU。

範例 4：限制對子政策的變更

在某些情況下，您可能想要限制子政策中的變更。此範例說明如何利用子控制運算子來這樣做。

此範例從新的組織根標籤政策開始，並假設標籤政策尚未連接至組織實體。

政策 E – 組織根標籤政策，用於限制子政策中的變更

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "Project"
            },
            "tag_value": {
                "@@operators_allowed_for_child_policies": ["@@append"],
                "@@assign": [
                    "Maintenance",
                    "Escalations"
                ]
            }
        }
    }
}
```

當您將政策 E 連接至組織根時，政策即可防止子政策變更 `Project` 標籤鍵。不過，子政策可以覆寫或附加標籤值。

假設您接著將下列政策 F 連接至 OU。

政策 F – OU 標記政策

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@assign": "PROJECT"
            },
            "tag_value": {
                "@@append": [
                    "Escalations - research"
                ]
            }
        }
    }
}
```

合併政策 E 和政策 F 會對 OU 的帳戶產生下列效果：

- 政策 F 是政策 E 的子政策。
- 政策 F 試圖變更大小寫處理，但無法這樣做。這是因為政策 E 在標籤鍵中包含 `"@@operators_allowed_for_child_policies": ["@@none"]` 運算子。
- 不過，政策 F 可以為索引鍵附加標籤值。這是因為政策 E 在標籤值中包含 `"@@operators_allowed_for_child_policies": ["@@append"]`。

OU 中帳戶的有效政策

> **Note**
>
> 您無法直接使用顯示的有效政策的內容作為新政策的內容。語法不包括控制與其他子政策和父政策合併所需的運算子。顯示有效政策僅用於了解合併的結果。

```
{
    "tags": {
        "project": {
            "tag_key": "Project",
            "tag_value": [
                "Maintenance",
                "Escalations",
                "Escalations - research"
```

```
            ]
        }
    }
}
```

範例 5：與子控制運算子衝突

子控制運算子可以存在於組織階層中相同層級上連接的標籤政策中。在此情況下，政策合併形成帳戶的有效政策時會使用允許運算子的交集。

假設政策 G 和政策 H 連接至組織根。

政策 G – 組織根標籤政策 1

```
{
    "tags": {
        "project": {
            "tag_value": {
                "@@operators_allowed_for_child_policies": ["@@append"],
                "@@assign": [
                    "Maintenance"
                ]
            }
        }
    }
}
```

政策 H – 組織根標籤政策 2

```
{
    "tags": {
        "project": {
            "tag_value": {
                "@@operators_allowed_for_child_policies": ["@@append", "@@remove"]
            }
        }
    }
}
```

在此範例中，組織根上的一個政策定義只能附加標籤鍵的值。連接至組織根的其他政策允許子政策附加和移除值。這兩個許可的交集用於子政策。結果是子政策可以附加值，但不能移除值。因此，子政策可以將值附加至標籤值清單，但無法移除 `Maintenance` 值。

範例 6：與相同階層層級上附加的值衝突

您可以將多個標籤政策連接至每個組織實體。當您這麼做時，連接至相同組織實體的標籤政策可能包含衝突的資訊。這些政策是根據連接至組織實體時的順序來評估。若要變更先評估哪個政策，您可以分離政策，再重新連接。

假設政策 J 最先連接至組織根，然後政策 K 才連接至組織根。

政策 J – 連接至組織根的第一個標籤政策

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@assign": "PROJECT"
            },
            "tag_value": {
                "@@append": ["Maintenance"]
            }
        }
    }
}
```

政策 K – 連接至組織根的第二個標籤政策

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@assign": "project"
            }
        }
    }
}
```

在此範例中，有效的標籤政策中會使用標籤鍵 PROJECT，因為定義此標籤鍵的政策最先連接至組織根。

政策 JK – 帳戶的有效標籤政策

帳戶的有效政策如下。

> **Note**
>
> 您無法直接使用顯示的有效政策的內容作為新政策的內容。語法不包括控制與其他子政策和父政策合併所需的運算子。顯示有效政策僅用於了解合併的結果。

```
{
    "tags": {
        "project": {
            "tag_key": "PROJECT",
            "tag_value": [
                "Maintenance"
            ]
        }
    }
}
```

AI 服務選擇退出政策

AWS 人工智慧 (AI) 服務，例如 Amazon Rekognition、Amazon CodeWhisperer、Amazon Transcribe 和 Contact Lens for Amazon Connect，可以存放和使用這些服務處理的客戶內容，以開發和持續改進其他 AWS 服務。作為 AWS 客戶，您可以選擇退出存放或用於改進服務的內容。

> **Note**
>
> AWS 人工智慧 (AI) 服務需要存放您的內容來提供服務，即使您選擇退出 AWS 使用您的資料進行服務改進。如需詳細資訊，請參閱您所使用 AI 服務的說明文件。

您可以設定一個組織政策，在屬於組織成員的所有帳戶上強制執行您的設定選項，而不是為您的組織使用的每個 AWS 帳戶 單獨進行此設定。您可以選擇退出內容儲存，並用於個別 AI 服務，或同時用於所有涵蓋的服務。您可以查詢適用於每個帳戶的有效政策，以查看設定選項的成效。

> **Important**
>
> - 當您指定服務的選擇加入或選擇退出偏好設定時，該設定為全域設定，並套用至所有 AWS 區域。將一個 AWS 區域 複寫中的值設定為所有其他區域。

- 當您選擇退出 AWS AI 服務使用的內容時，該服務會刪除在您設定該選項之前與 AWS 共享的所有關聯歷史內容。此刪除應僅限於提供服務功能不需要的存放資料。

開始使用 AI 服務選擇退出政策

請依照下列步驟開始使用人工智慧 (AI) 服務選擇退出政策。

1. 為您的組織啟用 AI 服務選擇退出政策。
2. 建立 AI 服務選擇退出政策。
3. 將 AI 服務選擇退出政策連接至組織的根、OU 或帳戶。
4. 檢視套用至帳戶的合併有效 AI 服務選擇退出政策。

對於所有這些步驟，請以 AWS Identity and Access Management (IAM) 使用者身分登入、擔任 IAM 角色，或以組織管理帳戶中的根使用者身分登入 (不建議)。

其他資訊

- 了解 AI 服務選擇退出政策的政策語法，並查看政策範例

建立、更新和刪除 AI 服務選擇退出政策

在本主題中：

- 對組織啟用 AI 服務選擇退出政策後，您就可以建立政策。
- 當選擇退出需求變更時，您可以更新現有的政策。
- 如果您不再需要某項政策，則將該政策從所有 OU 和帳戶中分離後，即可刪除政策。

建立 AI 服務選擇退出政策

最低許可

若要建立 AI 服務選擇退出政策，您需要具有執行下列動作的許可：

- `organizations:CreatePolicy`

AWS Management Console

建立 AI 服務選擇退出政策

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 AI services opt-out policies (AI 服務選擇退出政策) 頁面上，選擇 Create policy (建立政策)。
3. 在 Create new AI services opt-out policy (建立新的 AI 服務選擇退出政策) 頁面上，輸入 Policy name (政策名稱) 與選用的 Policy description (政策描述)。
4. (選用) 您可以透過選擇 Add tag (新增標籤)，然後輸入一個鍵和一個選用值，來將一個或多個標籤新增至政策。將值留空會將其設定為空白字串；而不是 null。您可以在政策中連接最多 50 個標籤。如需詳細資訊，請參閱 標記 AWS Organizations 資源。
5. 在 JSON 索引標籤中輸入或貼上政策文字。如需 AI 服務選擇退出政策語法的相關資訊，請參閱AI 服務選擇退出政策語法和範例。例如，您可以用作起點的政策，請參閱AI 服務選擇退出政策範例。
6. 當政策編輯完成時，請在頁面的右下角選擇 Create policy (建立政策)。

AWS CLI & AWS SDKs

建立 AI 服務選擇退出政策

您可以使用下列其中一項來建立標籤政策：

- AWS CLI: create-policy

1. 建立如下所示的 AI 服務選擇退出政策，並將其存放在文字檔案中。請注意，"optOut" 和 "optIn" 區分大小寫。

```
{
    "services": {
        "default": {
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optIn"
```

```
            }
        }
    }
}
```

此 AI 服務選擇退出政策規定，除了 Amazon Rekognition 以外，受政策影響的所有帳戶都選擇退出所有 AI 服務。

2. 匯入 JSON 政策檔案，以在組織中建立新的政策。在此範例中，之前的 JSON 檔案名稱為 `policy.json`。

```
$ aws organizations create-policy \
    --type AISERVICES_OPT_OUT_POLICY \
    --name "MyTestPolicy" \
    --description "My test policy" \
    --content file://policy.json
{
    "Policy": {
        "Content": "{\"services\":{\"default\":{\"opt_out_policy\":{\"@@assign
\":\"optOut\"}},\"rekognition\":{\"opt_out_policy\":{\"@@assign\":\"optIn
\"}}}}",
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5"
            "Arn": "arn:aws:organizations::o-aa111bb222:policy/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Description": "My test policy",
            "Name": "MyTestPolicy",
            "Type": "AISERVICES_OPT_OUT_POLICY"
        }
    }
}
```

- AWS SDKs: CreatePolicy

後續作業

建立 AI 服務選擇退出政策之後，您可以使選擇退出選項生效。若要執行該操作，您可以連接政策至組織根、組織單位 (OU)、組織內的 AWS 帳戶，或這三者全部的組合。

更新 AI 服務選擇退出政策

最低許可

若要更新 AI 服務選擇退出政策，您必須具有執行下列動作的許可：

- `organizations:UpdatePolicy`，並在包含指定政策 (或 "*") 的 ARN 的相同政策陳述式中具有 `Resource` 元素
- `organizations:DescribePolicy`，並在包含指定政策 (或 "*") 的 Amazon 資源名稱 (ARN) 的相同政策陳述式中具有 `Resource` 元素

AWS Management Console

更新 AI 服務選擇退出政策

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 AI services opt-out policies (AI 服務選擇退出政策) 頁面上，選擇您要更新的政策名稱。
3. 在政策的詳細資訊頁面上，選擇 Edit policy (編輯政策)。
4. 您可以輸入新的政策名稱、策略說明，或編輯 JSON 政策文字。如需 AI 服務選擇退出政策語法的相關資訊，請參閱AI 服務選擇退出政策語法和範例。例如，您可以用作起點的政策，請參閱AI 服務選擇退出政策範例。
5. 政策更新完成時，請選擇 Save changes (儲存變更)。

AWS CLI & AWS SDKs

更新政策

您可以使用下列其中一項來更新政策：

- AWS CLI: update-policy

  下列範例會重新命名 AI 服務選擇退出政策。

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed policy"
{
```

```
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Type": "AISERVICES_OPT_OUT_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"services\":{\"default\":{\"opt_out_policy\":
  ....TRUNCATED FOR BREVITY...   :{\"@@assign\":\"optIn\"}}}}"
    }
}
```

下列範例會新增或變更 AI 服務選擇退出政策的描述。

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "AISERVICES_OPT_OUT_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"services\":{\"default\":{\"opt_out_policy\":
  ....TRUNCATED FOR BREVITY...   :{\"@@assign\":\"optIn\"}}}}"
    }
}
```

下列範例會變更連接至 AI 服務選擇退出政策的 JSON 政策文件。在此範例中，內容擷取自名稱為 `policy.json` 的檔案，其中包含以下文字：

```
{
    "services": {
        "default": {
            "opt_out_policy": {
```

```
                "@@assign": "optOut"
            }
        },
        "comprehend": {
            "opt_out_policy": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "optOut"
            }
        },
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --content file://policy.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "AISERVICES_OPT_OUT_POLICY",
            "AwsManaged": false
        },
         "Content": "{\n\"services\": {\n\"default\": {\n\"   ....TRUNCATED FOR
 BREVITY....    ": \"optIn\"\n}\n}\n}\n}\n"}
}
```

- AWS SDKs: UpdatePolicy

編輯連接至 AI 服務選擇退出政策的標籤

登入您的組織的管理帳戶時，您可以新增或移除連接至 AI 服務選擇退出政策的標籤。如需標記的詳細資訊，請參閱標記 AWS Organizations 資源。

最低許可

若要編輯連接至您 AWS 組織的 AI 服務選擇退出政策標籤，您必須擁有以下許可：

- `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要
- `organizations:DescribePolicy` – 僅在使用 Organizations 主控台時才需要
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

編輯連接至 AI 服務選擇退出政策的標籤

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 AI services opt-out policies (AI 服務選擇退出政策) 頁面上，選擇您要編輯的附有標籤的政策名稱。
3. 在所選政策的詳細資訊頁面上，選擇 Tags (標籤) 索引標籤，然後選擇 Manage tags (管理標籤)。
4. 您可以在此頁面上執行任一動作：
   - 透過在舊值上輸入新值來編輯任何標籤的值。您無法修改標籤鍵。若要變更標籤鍵，您必須刪除含有舊標籤鍵的標籤，並新增含有新標籤鍵的標籤。
   - 選擇 Remove (移除) 以移除現有的標籤。
   - 新增標籤鍵值組。選擇 Add tag (新增標籤)，然後在提供的方塊中輸入新的標籤鍵名稱和選用值。如果您將 Value (值) 方塊保留空白，則值為空白字串；而不是 `null`。
5. 在您完成所有要進行的新增、移除和編輯之後，選擇 Save changes (儲存變更)。

AWS CLI & AWS SDKs

編輯連接至 AI 服務選擇退出政策的標籤

您可以使用下列其中一項命令來編輯連接至 AI 服務選擇退出政策的標籤：

- AWS CLI: tag-resource and untag-resource
- AWS SDKs: TagResource and UntagResource

刪除 AI 服務選擇退出政策

登入到您的組織的管理帳戶時，您可以刪除在您的組織中不再需要的政策。

您必須先將政策從所有連接的實體分離，才能刪除政策。

最低許可

若要刪除政策，您必須具有執行下列動作的許可：

- `organizations:DescribePolicy` (僅限主控台 – 導覽至政策)
- `organizations:DeletePolicy`

AWS Management Console

刪除 AI 服務選擇退出政策

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在AI 服務選擇退出政策頁面上，選擇您要刪除的政策名稱。
3. 您必須先將您要刪除的政策從所有根、OU 和帳戶分離。選擇 Targets (目標) 索引標籤，再選擇每個根、OU 或顯示於 Targets (目標) 清單中帳戶旁邊的選項按鈕，然後選擇 Detach (分離)。在確認對話方塊中，選擇 Detach (分離)。重複操作，直至移除所有目標。
4. 在頁面頂端，選擇 Delete (刪除)。
5. 在確認對話方塊中，輸入政策的名稱，然後選擇 Delete (刪除)。

AWS CLI & AWS SDKs

刪除 AI 服務選擇退出政策

您可以使用下列其中一項來刪除政策：

- AWS CLI: delete-policy

  以下範例會刪除指定的政策。只有在政策未連接至任何根、OU 或帳戶時才有效。

```
$ aws organizations delete-policy \
```

```
    --policy-id p-i9j8k7l6m5
```

此命令成功後就不會產生輸出。

- AWS SDKs: DeletePolicy

連接和分離 AI 服務選擇退出政策

您可以在整個組織及組織單位 (OU) 和個別帳戶上使用人工智慧 (AI) 服務選擇退出政策。AI 服務選擇退出政策適用的內容取決於您將其連接至哪個組織元素：

- 將 AI 服務選擇退出政策連接至組織根時，此政策會套用至該根的所有成員 OU 和帳戶。
- 將 AI 服務選擇退出政策連接至 OU 時，該政策會套用至屬於 OU 或其任何子 OU 的帳戶。這些帳戶也受制於連接至組織根的任何政策。
- 將 AI 服務選擇退出政策連接至帳戶 時，該政策只會套用至該帳戶。帳戶也受制於連接至組織根的任何政策及帳戶所屬的任何 OU。

帳戶從根和父 OU 繼承的任何 AI 服務選擇退出政策彙總，以及直接連接至帳戶的任何政策，即為有效政策。如需有關如何將政策合併為有效政策的資訊，請參閱理解管理政策繼承。

> **最低許可**
>
> 若要連接 AI 服務選擇退出政策，您必須具有執行下列動作的許可：
>
> - `organizations:AttachPolicy`

AWS Management Console

您可以導覽至政策或連接政策的根、OU 或帳戶，以連接 AI 服務選擇退出政策。

導覽至根、OU 或帳戶以連接 AI 服務選擇退出政策

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 AWS 帳戶 頁面上，導覽至您要連接政策的根、OU 或帳戶的名稱並選擇。您可能需要展開 OU (選擇 ▶)，以尋找您所需的 OU 和帳戶。

3. 在 Policies (政策) 索引標籤的 AI service opt-out policies (AI 服務選擇退出政策) 項目中，選擇 Attach (連接)。
4. 尋找您所需的政策，然後選擇 Attach policy (連接政策)。

   Policies (政策) 索引標籤上的連接的 AI 服務選擇退出政策清單會更新，以包含新的新增項目。政策變更會立即生效。

導覽至政策以連接 AI 服務選擇退出政策

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 AI services opt-out policies (AI 服務選擇退出政策) 頁面上，選擇您要連接的政策名稱。
3. 在 Targets (目標) 索引標籤上，選擇 Attach (連接)。
4. 選擇您要連接政策的根、OU 或帳戶旁的選項按鈕。您可能需要展開 OU (選擇 ▶)，以尋找您所需的 OU 和帳戶。
5. 選擇 Attach policy (連接政策)。

   Targets (目標) 索引標籤上的連接的 AI 服務選擇退出政策清單會更新，以包含新的新增項目。政策變更會立即生效。

AWS CLI & AWS SDKs

將 AI 服務選擇退出政策連接至組織的根、OU 或帳戶。

您可以使用下列其中一項來連接 AI 服務選擇退出政策：

- AWS CLI: attach-policy

  下列範例會將政策連接至 OU。

  ```
  $ aws organizations attach-policy \
      --target-id ou-a1b2-f6g7h222 \
      --policy-id p-i9j8k7l6m5
  ```

  此命令成功後就不會產生輸出。

- AWS SDKs: AttachPolicy

政策變更會立即生效。

分離 AI 服務選擇退出政策

登入組織的管理帳戶後，您可以將 AI 服務選擇退出政策從原本連接的組織根、OU 或帳戶中分離。從實體分離 AI 服務選擇退出政策後，該政策即不再套用至現在已分離的實體先前所影響的任何帳戶。若要分離政策，請完成下列步驟。

最低許可

若要從組織根、OU 或帳戶中分離 AI 服務選擇退出政策，您必須具有執行下列動作的許可：

- `organizations:DetachPolicy`

AWS Management Console

您可以導覽至政策或分離接政策的根、OU 或帳戶，以分離 AI 服務選擇退出政策。

導覽至連接的根、OU 或帳戶以分離 AI 服務選擇退出政策

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 AWS 帳戶 頁面導覽至您要從中分離政策的根、OU 或帳戶。您可能需要展開 OU (選擇 ▶)，以尋找您所需的 OU 和帳戶。選擇根、OU 或帳戶的名稱。
3. 在 Policies (政策) 索引標籤上，選擇您要分離的 AI 服務選擇退出政策旁邊的選項按鈕，然後選擇 Detach (分離)。
4. 在確認對話方塊中，選擇 Detach policy (分離政策)。

   已更新連接 AI 服務選擇退出政策的清單。政策變更會立即生效。

導覽至政策以分離 AI 服務選擇退出政策

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 AI services opt-out policies (AI 服務選擇退出政策) 頁面上，選擇您要從根、OU 或帳戶分離的政策名稱。

3. 在 Targets (目標) 索引標籤上，選擇您要分離政策的根、OU 或帳戶旁的選項按鈕。您可能需要展開 OU (選擇 )，以尋找您所需的 OU 和帳戶。
4. 請選擇 Detach (分離)。
5. 在確認對話方塊中，選擇 Detach (分離)。

   已更新連接 AI 服務選擇退出政策的清單。政策變更會立即生效。

AWS CLI & AWS SDKs

將 AI 服務選擇退出政策與組織的根、OU 或帳戶分離。

您可以使用下列其中一項來分離 AI 服務選擇退出政策：

- AWS CLI: detach-policy

  下列範例會將政策與 OU 分離。

  ```
  $ aws organizations detach-policy \
      --target-id ou-a1b2-f6g7h222 \
      --policy-id p-i9j8k7l6m5
  ```

  此命令成功後就不會產生輸出。
- AWS SDKs: DetachPolicy

政策變更會立即生效。

檢視有效的 AI 服務選擇退出政策

確定組織中帳戶的有效人工智慧 (AI) 服務選擇退出政策。

什麼是有效的 AI 服務選擇退出政策？

有效的 AI 服務選擇退出政策會指定適用於 AWS 帳戶 的最終規則。除了帳戶繼承的任何 AI 服務選擇退出政策的彙總，還有直接連接至帳戶的任何 AI 服務選擇退出政策。將 AI 服務選擇退出政策連接至組織根時，該政策會套用至組織中的所有帳戶。將 AI 服務選擇退出政策連接至 OU 時，該政策會套用至屬於此 OU 的所有帳戶和 OU。將政策直接連接至帳戶時，該政策只會套用至一個 AWS 帳戶。

例如，連接至組織根的 AI 服務選擇退出政策，可能會指定組織中的所有帳戶都選擇退出所有 AWS 機器學習服務使用的內容。直接連接至一個成員帳戶的單獨 AI 服務選擇退出政策，會指定其選擇加入僅針對 Amazon Rekognition 使用的內容。這些 AI 服務選擇退出政策的組合包括有效的 AI 服務選擇退出政策。因此，組織中的所有帳戶已選擇退出所有 AWS 服務，但選擇加入 Amazon Rekognition 的一個帳戶除外。

如需有關如何將 AI 服務選擇退出政策合併成最終有效政策的資訊，請參閱理解管理政策繼承。

如何檢視有效 AI 服務選擇退出政策。

您可以從 AWS Management Console、AWS API 或 AWS Command Line Interface 檢視帳戶的有效 AI 服務選擇退出政策。

> **最低許可**
>
> 若要檢視帳戶的有效 AI 服務選擇退出政策，您必須具有執行下列動作的許可：
>
> - `organizations:DescribeEffectivePolicy`
> - `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要

AWS Management Console

檢視帳戶的有效 AI 服務選擇退出政策

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 AWS 帳戶 頁面上，選擇您要檢視其有效 AI 服務選擇退出政策的帳戶名稱。您可能需要展開 OU (選擇 ▶)，以尋找您想要的帳戶。
3. 在 Policies (政策) 索引標籤的 AI services opt-out policies (AI 服務選擇退出政策) 區段中，選擇 View the effective AI policy for this AWS 帳戶 (檢視此 AWS 帳戶 帳戶的有效 AI 政策)。

   主控台會顯示套用至指定帳戶的有效政策。

> **Note**
>
> 在沒有重大變更的情況下，您無法複製並貼上有效政策作為另一個 AI 服務選擇退出政策的 JSON。AI 服務選擇退出政策文件必須包含繼承運算子，以指定如何將每一項設定合併成最終有效政策。

AWS CLI & AWS SDKs

檢視帳戶的有效 AI 服務選擇退出政策

您可以使用下列其中一項來檢視有效的 AI 服務選擇退出政策：

- AWS CLI: describe-effective-policy

  下列範例顯示帳戶的有效 AI 服務選擇退出政策。

```
$ aws organizations describe-effective-policy \
    --policy-type AISERVICES_OPT_OUT_POLICY \
    --target-id 123456789012
{
    "EffectivePolicy": {
        "PolicyContent": "{\"services\":{\"comprehend\":{\"opt_out_policy\":
\"optOut\"},   ....TRUNCATED FOR BREVITY....   "opt_out_policy\":\"optIn\"}}}",
        "LastUpdatedTimestamp": "2020-12-09T12:58:53.548000-08:00",
        "TargetId": "123456789012",
        "PolicyType": "AISERVICES_OPT_OUT_POLICY"
    }
}
```

- AWS SDKs: DescribeEffectivePolicy

AI 服務選擇退出政策語法和範例

本主題說明人工智慧 (AI) 服務選擇退出政策語法，並提供了範例。

AI 服務選擇退出政策的語法

AI 服務選擇退出政策是根據 JSON 規則建構的純文字檔。AI 服務選擇退出政策的語法遵循管理政策類型的語法。如需該語法的完整討論，請參閱理解管理政策繼承。本主題著重於以該一般語法滿足 AI 服務選擇退出政策類型的特定需求。

> **Important**
>
> 本節中討論的值的大小寫很重要。輸入具有大小寫字母的值，如本主題所示。如果您使用未預期的大小寫，政策將無法運作。

下列政策顯示基本的 AI 服務選擇退出政策語法。如果此範例直接連接至帳戶，則該帳戶會明確選擇退出某項服務，並選擇加入至另一項服務。從較高層級 (OU 或根政策) 繼承的政策可以選擇加入或選擇退出其他服務。

```
{
    "services": {
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "lex": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

想像下列連接至組織根的範例政策。它會設定組織選擇退出所有 AI 服務的預設值。這會自動包含任何未明確豁免的 AI 服務，包括 AWS 未來可能會部署的任何 AI 服務。您可以將子政策連接至 OU 或直接連接至帳戶，以覆寫除 Amazon Comprehend 之外的任何 AI 服務的此設定。下列範例中的第二個項目使用 `@@operators_allowed_for_child_policies` 來設定 `none` 以防止被覆寫。範例中的第三個項目會針對 Amazon Rekognition 進行整個組織的豁免。它在整個組織中選擇使用該服務，但正確確實允許子政策在適用時覆寫。

```
{
    "services": {
        "default": {
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "comprehend": {
            "opt_out_policy": {
```

```
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "optOut"
            }
        },
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

AI 服務選擇退出政策語法包含下列元素：

- services 元素。透過此固定名稱，AI 服務選擇退出政策將識別為包含元素的最外層 JSON。

  AI 服務選擇退出政策可在 services 元素下具有一個或多個陳述式。每個陳述式均包含下列要素：

  - 服務名稱鍵，以識別 AWS AI 服務。以下鍵名稱是該欄位的有效值：
    - **default** – 代表所有目前可用的 AI 服務，並隱含且自動包含未來可能新增的任何 AI 服務。
    - awssupplychain
    - chimesdkvoiceanalytics
    - cloudwatch
    - codeguruprofiler
    - codewhisperer
    - comprehend
    - connectamd
    - connectoptimization
    - contactlens
    - datazone
    - frauddetector
    - guardduty
    - lex
    - polly
    - q
    - quicksightq

- rekognition
- securitylake
- textract
- transcribe
- translate

透過服務名稱鍵識別的每個政策陳述式都可以包含下列元素：

- opt_out_policy 索引鍵。此鍵必須存在。這是您可以放置在服務名稱鍵下的唯一鍵。

  opt_out_policy 鍵可以僅包含 @@assign 運算子 (具有下列其中一個值)：

  - optOut – 您選擇退出指定 AI 服務使用的內容。
  - optIn – 您選擇加入指定 AI 服務使用的內容。

  > **備註**
  >
  > - 您無法使用 @@append 和 @@remove AI 服務選擇退出政策中的繼承運算子。
  > - 您無法使用 AI 服務選擇退出政策中的 @@enforced_for 運算子。

- 在任何層級，您都可以指定 @@operators_allowed_for_child_policies 運算子，來控制子政策可以執行哪些動作來覆寫父政策強加的設定。您可以指定下列其中一個值：

  - @@assign – 此政策的子政策可以使用 @@assign 運算子，以不同的值覆蓋繼承的值。
  - @@none – 此政策的子政策無法變更值。

  @@operators_allowed_for_child_policies 的行為取決於您放置它的位置。您可以在下列位置使用：

  - 在 services 鍵下方 – 控制子政策是否可以在有效政策中新增或變更服務清單。
  - 在特定 AI 服務的鍵下，或 default 鍵 - 控制子政策是否可以新增或變更此特定項目下的鍵清單。
  - 在特定服務的 opt_out_policies 鍵下 – 控制子政策是否只能變更此特定服務的設定。

AI 服務選擇退出政策範例

接下來的政策範例僅供參考。

範例 1：選擇退出組織中所有帳戶的所有 AI 服務

下列範例顯示您可以連接至組織根的政策，以選擇退出組織中帳戶的 AI 服務。

> **Tip**
>
> 如果您使用範例右上角的「複製」按鈕來複製下列範例，則複本不會包含行號。已經準備貼上。

```
    | {
    |     "services": {
[1] |         "@@operators_allowed_for_child_policies": ["@@none"],
    |         "default": {
[2] |             "@@operators_allowed_for_child_policies": ["@@none"],
    |             "opt_out_policy": {
[3] |                 "@@operators_allowed_for_child_policies": ["@@none"],
    |                 "@@assign": "optOut"
    |             }
    |         }
    |     }
    | }
```

- [1] – `"@@operators_allowed_for_child_policies": ["@@none"]` 在 `services` 下，可防止任何子政策針對個別服務新增已經存在的 `default` 區段之外的任何新區段。`Default` 代表「所有 AI 服務」的預留位置。
- [2] – `"@@operators_allowed_for_child_policies": ["@@none"]` 在 `default` 下，可防止任何子政策新增已經存在的 `opt_out_policy` 區段之外的任何新區段。
- [3] – `"@@operators_allowed_for_child_policies": ["@@none"]` 在 `opt_out_policy` 下，可防止子政策變更 `optOut` 設定的值或新增任何其他設定。

範例 2：為所有服務設定組織預設設定，但允許子政策覆寫個別服務的設定

下列範例政策會為所有 AI 服務設定整個組織的預設值。`default` 的值，可防止子政策變更服務 `default` 的 `optOut` 值，這是所有 AI 服務的預留位置。如果將此政策連接至根或 OU，以將其套用為父政策，則子政策仍然可以變更個別服務的選擇退出設定，如第二項政策所示。

- 因為沒有 `"@@operators_allowed_for_child_policies": ["@@none"]` 在 `services` 鍵下，子政策可以為個別服務新增區段。

- `"@@operators_allowed_for_child_policies": ["@@none"]` 在 `default` 下，可防止任何子政策新增已經存在的 `opt_out_policy` 區段之外的任何新區段。
- `"@@operators_allowed_for_child_policies": ["@@none"]` 在 `opt_out_policy` 下，可防止子政策變更 `optOut` 設定的值或新增任何其他設定。

組織根使用者 AI 服務選擇退出父政策

```
{
    "services": {
        "default": {
            "@@operators_allowed_for_child_policies": ["@@none"],
            "opt_out_policy": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "optOut"
            }
        }
    }
}
```

下列範例政策假設之前的範例政策已連接至組織根或父 OU，並且您將此範例連接至受父政策影響的帳戶。它會覆寫預設的選擇退出設定，並明確選擇僅使用 Amazon Lex 服務。

AI 服務選擇退出子政策

```
{
    "services": {
        "lex": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

由此產生的 AWS 帳戶 有效政策，即該帳戶僅選擇加入 Amazon Lex，並且選擇退出所有其他 AWS AI 服務，因為從父政策繼承 `default` 選擇退出設定。

範例 3：針對單一服務定義整個組織的 AI 服務選擇退出政策

下列範例顯示 AI 服務選擇退出政策，定義單一 AI 服務的 `optOut` 設定。如果此政策連接至組織的根，它會防止任何子政策覆寫這一項服務的 `optOut` 設定。其他服務並未透過此政策解決，但可能會受其他 OU 或帳戶中的子政策的影響。

```
{
    "services": {
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optOut",
                "@@operators_allowed_for_child_policies": ["@@none"]
            }
        }
    }
}
```

備份政策

AWS Backup 可讓您建立備份計劃，在計劃中定義如何備份 AWS 資源。計劃中的規則包括各種設定，例如備份頻率、備份時段、要備份的資源所在的 AWS 區域，以及儲存備份的保存庫。然後，您可以將備份計劃套用至標籤所識別的 AWS 資源群組。您也必須識別 AWS Identity and Access Management (IAM) 角色，該角色授權 AWS Backup 代表您執行備份操作。

AWS Organizations 中的備份政策將所有這些部分結合成 JSON 文字文件。您可以將備份政策連接至組織結構中的任何元素，例如根、組織單位 (OU) 和個別帳戶。Organizations 會套用繼承規則，以合併組織根、任何父 OU 或連接至帳戶的政策。這樣會為每個帳戶產生有效備份政策。此有效政策指示 AWS Backup 如何自動備份 AWS 資源。

備份政策可讓您精細控制在組織所需的任何層級上備份資源。例如，您可以在連接至組織根的政策中指定必須備份所有 Amazon DynamoDB 資料表。該政策可以包含預設備份頻率。然後，您可以將備份政策連接至 OU，以根據每個 OU 的需求來覆寫備份頻率。例如，`Developers` OU 可能指定備份頻率為每週一次，而 `Production` OU 指定每天一次。

您可以建立部分備份政策，僅個別包含成功備份資源所需的部分資訊。您可以將這些政策連接至組織樹狀結構的不同部分，例如根或父 OU，讓較低層級的 OU 和帳戶繼承這些部分政策。當 Organizations 使用繼承規則合併帳戶的所有政策時，產生的有效政策必須具有所有必要的元素。否則，AWS Backup 會將政策視為無效，且不會備份受影響的資源。

> **Important**
>
> 在完成具有所有必要元素的有效政策而對其叫用時，AWS Backup 只能執行成功的備份。雖然前述的部分政策策略沒問題，但如果帳戶的有效政策並不完整，則會導致錯誤或無法成功備份資源。另一種策略是考慮要求所有備份政策本身必須完整且有效。使用階層中較高層級連接的政策所提供的「預設」值，然後視需要在子政策中包含繼承子控制運算子，以覆寫這些預設值。

組織中每個 AWS 帳戶 的有效備份計劃，在 AWS Backup 主控台會顯示成該帳戶不可變的計劃。可檢視但不能變更。

當 AWS Backup 根據政策建立的備份計劃來開始備份時，您可以在 AWS Backup 主控台看到備份任務的狀態。成員帳戶中的使用者可以看到該成員帳戶中各備份任務的狀態和任何錯誤。如果您也啟用 AWS Backup 受信任的服務存取，則組織管理帳戶中的使用者可以看到組織中所有備份任務的狀態和錯誤。如需詳細資訊，請參閱AWS Backup開發人員指南中的啟用跨帳戶管理。

備份政策入門

請依照下列步驟開始使用備份政策。

1. 了解執行備份政策任務所需的許可
2. 了解使用備份政策時建議的一些最佳實務。
3. 為組織啟用備份政策。
4. 建立備份政策。
5. 將備份政策連接至組織的根、OU 或帳戶。
6. 檢視套用至帳戶的合併有效備份政策。

對於所有這些步驟，請以 IAM 使用者身分登入、擔任 IAM 角色，或以組織管理帳戶中的根使用者身分登入 (不建議)。

其他資訊

- 了解備份政策語法和查看政策範例

管理備份政策的先決條件和許可

此頁面介紹在 AWS Organizations 中管理備份政策的先決條件和必要許可。

主題

管理備份政策的先決條件

管理組織中的備份政策需要下列各項：

- 您的組織必須啟用所有功能。
- 您必須登入組織的管理帳戶。
- AWS Identity and Access Management (IAM) 使用者或角色必須具有下一節所列的許可。

管理備份政策的許可

下列 IAM 政策範例提供許可來管理組織中的所有備份政策層面。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageBackupPolicies",
            "Effect": "Allow",
            "Action": [
                "organizations:AttachPolicy",
                "organizations:CreatePolicy",
                "organizations:DeletePolicy",
                "organizations:DescribeAccount",
                "organizations:DescribeCreateAccountStatus",
                "organizations:DescribeEffectivePolicy",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribePolicy",
                "organizations:DetachPolicy",
                "organizations:DisableAWSServiceAccess",
                "organizations:DisablePolicyType",
                "organizations:EnableAWSServiceAccess",
                "organizations:EnablePolicyType",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
```

```
                "organizations:ListCreateAccountStatus",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListPolicies",
                "organizations:ListPoliciesForTarget",
                "organizations:ListRoots",
                "organizations:ListTargetsForPolicy",
                "organizations:UpdatePolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

如需有關 IAM 政策和許可的詳細資訊，請參閱 IAM 使用者指南。

使用備份政策的最佳實務

AWS 建議採取下列最佳實務來使用備份政策。

決定備份政策策略

您建立的備份政策可以是不完整的片段，經過繼承和合併後，形成每個成員帳戶的完整政策。如果這樣做，假設您在某個層級變更，但未仔細考量低於該層級的所有帳戶所受的影響，最後可能產生不完整的有效政策。為了避免這種情況，建議您確保在所有層級實作的備份政策本身是完整的。將父政策視為預設政策，可由子政策中指定的設定來覆寫。如此一來，即使子政策不存在，繼承的政策仍然完整並使用預設值。您可以使用子控制繼承運算子，以控制子政策可新增、變更或移除哪些設定。

使用 **GetEffectivePolicy** 驗證備份政策的變更

變更備份政策後，在低於您進行變更的層級之下，請檢查代表性帳戶的有效政策。您可以使用 AWS Management Console 來檢視有效政策，或使用 GetEffectivePolicy API 操作或其中一個 AWS CLI 或 AWS SDK 變體來檢視有效政策。請確定您所做的變更對有效政策產生預期的影響。

簡單開始，小小改變

若要簡化偵錯，請從簡單的政策開始，然後一次變更一項。每次變更後，請先驗證變更的行為和影響，再繼續變更。在發生錯誤或意外的結果時，此方法可減少您必須考慮的變數。

將備份的複本存放在其他 AWS 區域 和您組織中的帳戶中

若要改善災難復原位置，您可以存放備份的複本。

- 不同的區域 – 如果您將備份的複本存放在其他 AWS 區域，可協助保護備份，避免原始區域中意外損毀或刪除。使用政策的 copy_actions 區段，以在執行備份計劃相同帳戶的一個或多個區域中指定保存庫。若要執行此操作，當您指定用於存放備份複本的備份保存庫 ARN 時，請使用 $account 變數來識別帳戶。$account 變數會在執行時間自動取代為執行備份政策的帳戶 ID。
- 不同的帳戶 – 如果您將備份的複本存放在其他 AWS 帳戶，可新增安全屏障，以防範惡意行為侵害您其中一個帳戶的行為。使用政策的 copy_actions 區段，以在組織中的一個或多個帳戶中指定保存庫，與執行的備份計劃帳戶分開。若要執行此操作，當您指定用於存放備份複本的備份保存庫 ARN 時，請使用其實際帳戶 ID 來識別帳戶。

限制每個政策的計劃數目

包含多個計劃的政策在疑難排解時較複雜，因為有大量的輸出必須全部驗證。應該讓每個政策只包含一個備份計劃，以簡化偵錯和疑難排解。然後，您可以新增更多政策來包含其他計劃，以符合其他需求。此方法有助於將計劃的任何問題隔離在一個政策中，在對其他政策及其計劃的問題在疑難排解時，才不會因為這些問題而變得更複雜。

使用堆疊集建立必要的備份保存庫和 IAM 角色

使用 AWS CloudFormation StackSets 與 Organizations 的整合，在組織的每個成員帳戶中自動建立必要的備份保存庫和 AWS Identity and Access Management (IAM) 角色。您可以建立堆疊集，其中包含您希望在組織的每個 AWS 帳戶 中自動可用的資源。此方法可讓您執行備份計劃時確保已符合相依性。如需詳細資訊，請參閱AWS CloudFormation使用者指南中的建立具有自我管理許可的堆疊集。

檢閱每個帳戶中建立的第一個備份來檢查結果

當您變更政策時，請檢查該變更之後建立的下一個備份，以確保變更產生預期的影響。此步驟不僅要查看有效政策，還要確保 AWS Backup 按照您要的方式來解讀政策和實作備份計劃。

建立、更新和刪除備份政策

在本主題中：

- 對組織啟用備份政策後，您就可以建立政策。
- 當備份需求變更時，您可以更新現有的政策。
- 如果您不再需要某項政策，則將該政策從所有 OU 和帳戶中分離後，即可刪除政策。

建立備份政策

最低許可

若要建立備份政策，您需要具有執行下列動作的許可：

- `organizations:CreatePolicy`

AWS Management Console

在 AWS Management Console中有兩種方式建立備份政策：

- 視覺化編輯器，可讓您選擇選項，然後為您產生 JSON 政策文字。
- 文字編輯器，可讓您直接建立 JSON 政策文字。

視覺化編輯器讓程序變簡單，但彈性受限。若要建立第一個政策並熟悉使用政策，這是好方法。在了解政策的運作方式，並開始覺得受限於視覺化編輯器後，您可以自行編輯 JSON 政策文字，將進階功能新增至政策。視覺化編輯器只使用 @@assign 值設定運算子，完全不支援存取子控制運算子。只有在手動編輯 JSON 政策文字時，才能新增子控制運算子。

建立備份政策

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Backup policies (備份政策) 頁面上，選擇 Create policy (建立政策)。
3. 在 Create policy (建立政策) 頁面上，輸入政策的 Policy name (政策名稱) 與選用的 Policy description (政策描述)。
4. (選用) 您可以透過選擇 Add tag (新增標籤)，然後輸入一個鍵和一個選用值，來將一個或多個標籤新增至政策。將值留空會將其設定為空白字串；而不是 null。您可以在政策中連接最多 50 個標籤。如需標記的詳細資訊，請參閱標記 AWS Organizations 資源。
5. 您可以使用 Visual editor (視覺化編輯器) 建置政策，如本程序所述。您也可以在 JSON 索引標籤中輸入或貼上政策文字。如需備份政策語法的相關資訊，請參閱備份政策語法和範例。

   如果您選擇使用 Visual editor (視覺化編輯器)，請選取適合您情境的備份選項。備份計劃由三個部分組成。如需這些備份計劃元素的詳細資訊，請參閱AWS Backup開發人員指南中的建立備份計劃和指派資源。

a. 備份計劃一般詳細資訊

- Backup plan name (備份計劃名稱)只能由英數字元、連字號和底線字元組成。
- 您必須從清單中至少選取一個 Backup plan region (備份計劃區域)。計劃只能備份選取的 AWS 區域。

b. 一或多個備份規則，指定 AWS Backup 的運作方式和時機。每個備份規則定義下列項目：

- 包含備份頻率以及進行備份的時段的排程。
- 要使用的備份保存庫名稱。Backup vault name (備份保存庫名稱)只能由英數字元、連字號和底線字元組成。備份保存庫必須先存在，計劃才能順利執行。使用 AWS Backup 主控台或 AWS CLI 命令建立保存庫。
- (選用) 一或多個 Copy to region (複製到區域)規則，也將備份複製到其他 AWS 區域 中的保存庫。
- 一或多個標籤鍵和值配對，連接至每次執行此備份計劃時建立的備份復原點。
- 生命週期選項，指定備份何時轉移至不常用的儲存體及備份何時到期。

選擇 Add rule (新增規則)，將您需要的每個規則新增至計劃。

如需關於備份規則的詳細資訊，請參閱 AWS Backup 開發人員指南中的備份規則。

c. 資源指派，指定 AWS Backup 應該按照此計劃而備份的資源。透過指定 AWS Backup 用於尋找和比對資源的標籤對來進行該指派

- Resource assignment name (資源指派名稱)只能由英數字元、連字號和底線字元組成。
- 指定 IAM 角色，以便 AWS Backup 用於依名稱執行備份。

  在主控台，您不需要指定整個 Amazon 資源名稱 (ARN)。角色名稱及其前綴 (指定角色類型) 都必須包括在內。前綴通常是 `role` 或 `service-role`，並以正斜線 ('/') 與角色名稱分隔。例如，您可以輸入 `role/MyRoleName` 或 `service-role/MyManagedRoleName`。存放在基礎 JSON 中可轉換為完整 ARN。

  > **Important**
  >
  > 指定的 IAM 角色必須已存在於套用政策的帳戶中。否則，雖然備份計劃可能成功啟動備份任務，但這些備份任務會失敗。

- 指定一個或多個資源標籤標籤鍵和標籤值組，以識別您想要備份的資源。如果有多個標籤值，請以逗號分隔值。

選擇 Add assignment (新增指派)，將每個設定的資源指派新增至備份計劃。

如需詳細資訊，請參閱AWS Backup開發人員指南中的將資源指派至備份計劃。

6. 政策建立完成時，請選擇 Create policy (建立政策)。政策會出現在可用的備份政策清單中。

AWS CLI & AWS SDKs

建立備份政策

您可以使用下列其中一項來建立備份政策：

- AWS CLI: create-policy

  將備份計劃建立為類似以下內容的 JSON 文字，並將其存放在文字檔案中。如需語法的完整規則，請參閱備份政策語法和範例。

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": { "@@assign": [ "ap-northeast-2", "us-east-1", "eu-
north-1" ] },
            "rules": {
                "Hourly": {
                    "schedule_expression": { "@@assign": "cron(0 5/1 ? * * *)" },
                    "start_backup_window_minutes": { "@@assign": "480" },
                    "complete_backup_window_minutes": { "@@assign": "10080" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "180" },
                        "delete_after_days": { "@@assign": "270" }
                    },
                    "target_backup_vault_name": { "@@assign": "FortKnox" },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:secondary-
vault": {
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "10" },
                                "delete_after_days": { "@@assign": "100" }
                            }
                        }
                    }
                }
```

```
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyIamRole" },
                        "tag_key": { "@@assign": "dataType" },
                        "tag_value": { "@@assign": [ "PII" ] }
                    }
                }
            }
        }
    }
}
```

此備份計劃指定 AWS Backup 應備份受影響的 AWS 帳戶 中的所有資源，其位於指定的 AWS 區域 且具有值為 PII 的標籤 dataType。

然後，匯入 JSON 政策檔案備份計劃，以在組織中建立新的政策備份計劃。請注意輸出中的政策 ARN 結尾的政策 ID。

```
$ aws organizations create-policy \
    --name "MyBackupPolicy" \
    --type BACKUP_POLICY \
    --description "My backup policy" \
    --content file://policy.json{
    "Policy": {
        "PolicySummary": {
            "Arn": "arn:aws:organizations::o-aa111bb222:policy/backup_policy/p-
i9j8k7l6m5",
            "Description": "My backup policy",
            "Name": "MyBackupPolicy",
            "Type": "BACKUP_POLICY"
        }
        "Content": "...a condensed version of the JSON policy document you
 provided in the file...",
    }
}
```

- AWS SDKs: CreatePolicy

後續作業

建立備份政策之後，您可以使政策生效。若要執行該操作，您可以連接政策至組織根、組織單位 (OU)、組織內的 AWS 帳戶，或這三者全部的組合。

更新備份政策

登入組織的管理帳戶後，您可以在組織中編輯需要變更的政策。

> **最低許可**
>
> 若要更新備份政策，您必須具有執行下列動作的許可：
>
> - `organizations:UpdatePolicy`，並在同一政策陳述式中指定 `Resource` 元素，其中包含要更新的政策 ARN (或「*」)
> - `organizations:DescribePolicy`，並在同一政策陳述式中指定 `Resource` 元素，其中包含要更新的政策 ARN (或「*」)

AWS Management Console

更新備份政策

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Backup policies (備份政策) 頁面上，選擇您要更新的政策名稱。
3. 選擇 Edit Policy (編輯政策)。
4. 您可以輸入新的政策名稱、政策描述。您可以使用視覺化編輯器，或直接編輯 JSON，來變更政策內容。
5. 政策更新完成時，請選擇 Save changes (儲存變更)。

AWS CLI & AWS SDKs

建立備份政策

您可以使用下列其中一項來備份政策：

- AWS CLI: update-policy

  下列範例會重新命名備份政策。

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"plans\":{\"TestBackupPlan\":{\"regions\":{\"@@assign\":
  ....TRUNCATED FOR BREVITY....   "@@assign\":[\"Yes\"]}}}}}}"
    }
}
```

下列範例會新增或變更備份政策的描述。

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
       "Content": "{\"plans\":{\"TestBackupPlan\":{\"regions\":{\"@@assign\":
  ....TRUNCATED FOR BREVITY....   "@@assign\":[\"Yes\"]}}}}}}"
    }
}
```

下列範例會變更連接至備份政策的 JSON 政策文件。在此範例中，內容擷取自名稱為 policy.json 的檔案，其中包含以下文字：

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": { "@@assign": [ "ap-northeast-2", "us-east-1", "eu-
north-1" ] },
            "rules": {
                "Hourly": {
                    "schedule_expression": { "@@assign": "cron(0 5/1 ? * * *)" },
                    "start_backup_window_minutes": { "@@assign": "480" },
                    "complete_backup_window_minutes": { "@@assign": "10080" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "180" },
                        "delete_after_days": { "@@assign": "270" }
                    },
                    "target_backup_vault_name": { "@@assign": "FortKnox" },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:secondary-
vault": {
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "10" },
                                "delete_after_days": { "@@assign": "100" }
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyIamRole" },
                        "tag_key": { "@@assign": "dataType" },
                        "tag_value": { "@@assign": [ "PII" ] }
                    }
                }
            }
        }
    }
}
```

```
$ aws organizations update-policy \
```

```
    --policy-id p-i9j8k7l6m5 \
    --content file://policy.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"plans\":{\"TestBackupPlan\":{\"regions\":{\"@@assign\":
  ....TRUNCATED FOR BREVITY....   "@@assign\":[\"Yes\"]}}}}}}"
}
```

- AWS SDKs: UpdatePolicy

編輯附加至備份政策的標籤

登入您的組織的管理帳戶時，您可以新增或移除連接至備份政策的標籤。如需標記的詳細資訊，請參閱標記 AWS Organizations 資源。

> **最低許可**
>
> 若要編輯連接至您 AWS 組織的備份政策標籤，您必須擁有以下許可：
>
> - `organizations:DescribeOrganization` (僅限主控台 – 導覽至政策)
> - `organizations:DescribePolicy` (僅限主控台 – 導覽至政策)
> - `organizations:TagResource`
> - `organizations:UntagResource`

AWS Management Console

編輯連接至備份政策的標記

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。

2. 備份政策頁面
3. 選擇您要編輯其標籤的政策名稱。

   政策詳細資訊頁面會隨即出現。
4. 在 Tags (標籤) 索引標籤上，選擇 Manage tags (管理標籤)。
5. 您可以在此頁面上執行任一動作：

   - 透過在舊值上輸入新值來編輯任何標籤的值。您無法修改標籤鍵。若要變更標籤鍵，您必須刪除含有舊標籤鍵的標籤，並新增含有新標籤鍵的標籤。
   - 選擇 Remove (移除) 以移除現有的標籤。
   - 新增標籤鍵值組。選擇 Add tag (新增標籤)，然後在提供的方塊中輸入新的標籤鍵名稱和選用值。如果您將 Value (值) 方塊保留空白，則值為空白字串；而不是 `null`。
6. 在您完成所有要進行的新增、移除和編輯之後，選擇 Save changes (儲存變更)。

AWS CLI & AWS SDKs

編輯連接至備份政策的標記

您可以使用下列其中一項命令來編輯連接至備份政策的標籤：

- AWS CLI: tag-resource and untag-resource
- AWS SDKs: TagResource and UntagResource

刪除備份政策

登入到您的組織的管理帳戶時，您可以刪除在您的組織中不再需要的政策。

您必須先將政策從所有連接的實體分離，才能刪除政策。

> **最低許可**
>
> 若要刪除政策，您必須具有執行下列動作的許可：
>
> - `organizations:DeletePolicy`，並在同一政策陳述式中指定 `Resource` 元素，其中包含要刪除的政策 ARN (或「*」)

AWS Management Console

刪除備份政策

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 從 Backup policies (備份政策) 頁面中，選擇您要刪除的備份政策名稱。
3. 您必須先將您要刪除的備份政策從所有根、OU 和帳戶分離。選擇 Targets (目標) 索引標籤，再選擇每個根、OU 或顯示於 Targets (目標) 清單中帳戶旁邊的選項按鈕，然後選擇 Detach (分離)。在確認對話方塊中，選擇 Detach (分離)。重複操作，直至移除所有目標。
4. 在頁面頂端，選擇 Delete (刪除)。
5. 在確認對話方塊中，輸入政策的名稱，然後選擇 Delete (刪除)。

AWS CLI & AWS SDKs

刪除備份政策

您可以使用下列其中一項來刪除政策：

- AWS CLI: delete-policy

  以下範例會刪除指定的政策。只有在政策未連接至任何根、OU 或帳戶時才有效。

  ```
  $ aws organizations delete-policy \
      --policy-id p-i9j8k7l6m5
  ```

  此命令成功後就不會產生輸出。

- AWS SDKs: DeletePolicy

連接和卸離備份政策

您可以在整個組織及組織單位 (OU) 和個別帳戶上使用備份政策。請謹記以下幾點：

- 將備份政策連接至組織根時，此政策會套用至該根的所有成員 OU 和帳戶。
- 將備份政策連接至 OU 時，該政策會套用至屬於 OU 或其任何子 OU 的帳戶。這些帳戶也受制於連接至組織根的任何政策。

- 將備份政策連接至帳戶時，該政策只會套用至該帳戶。帳戶也受制於連接至組織根的任何政策及帳戶所屬的任何 OU。

帳戶從根和父 OU 繼承的任何備份政策集合，以及直接連接至帳戶的任何政策，即為有效政策。如需有關如何將政策合併為有效政策的資訊，請參閱理解管理政策繼承。

連接備份政策

登入組織的管理帳戶時，您可以將備份政策連接至組織的根、OU 或直接連接至帳戶。

最低許可

若要連接備份政策，您必須具有執行下列動作的許可：

- `organizations:AttachPolicy`

AWS Management Console

您可以導覽至政策或連接政策的根、OU 或帳戶，以連接備份政策。

導覽至根、OU 或帳戶以連接備份政策

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 AWS 帳戶 頁面上，導覽至您要連接政策的根、OU 或帳戶的名稱並選擇。您可能需要展開 OU (選擇 ▶)，以尋找您所需的 OU 和帳戶。
3. 在 Policies (政策) 索引標籤的 Backup policies (備份政策) 項目中，選擇 Attach (連接)。
4. 尋找您所需的政策，然後選擇 Attach policy (連接政策)。

   Policies (政策) 索引標籤上的連接的備份政策清單會更新，以包含新的新增項目。政策變更會立即生效。

導覽至政策以連接備份政策

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。

2. 在 Backup policies (備份政策) 頁面上，選擇您要連接的政策名稱。
3. 在 Targets (目標) 索引標籤上，選擇 Attach (連接)。
4. 選擇您要連接政策的根、OU 或帳戶旁的選項按鈕。您可能需要展開 OU (選擇)，以尋找您所需的 OU 和帳戶。
5. 選擇 Attach policy (連接政策)。

   Targets (目標) 索引標籤上的連接的備份政策清單會更新，以包含新的新增項目。政策變更會立即生效。

AWS CLI & AWS SDKs

將備份政策連接至組織根、OU 或帳戶

您可以使用下列其中一項命令來連接備份政策：

- AWS CLI: attach-policy

```
$ aws organizations attach-policy \
    --target-id 123456789012 \
    --policy-id p-i9j8k7l6m5
```

- AWS SDKs: AttachPolicy

政策變更會立即生效。

卸離備份政策

登入組織的管理帳戶後，您可以將備份政策從原本連接的組織根、OU 或帳戶分離。從實體分離備份政策後，該政策即不再套用至現在已分離的實體先前所影響的任何帳戶。若要分離政策，請完成下列步驟。

最低許可

若要從組織根、OU 或帳戶分離備份政策，您必須具有執行下列動作的許可：

- `organizations:DetachPolicy`

AWS Management Console

您可以導覽至政策或分離接政策的根、OU 或帳戶，以分離備份政策。

導覽至連接的根、OU 或帳戶以分離備份政策

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 AWS 帳戶 頁面導覽至您要從中分離政策的根、OU 或帳戶。您可能需要展開 OU (選擇 ▶)，以尋找您所需的 OU 和帳戶。選擇根、OU 或帳戶的名稱。
3. 在 Policies (政策) 索引標籤上，選擇您要分離的備份政策旁邊的選項按鈕，然後選擇 Detach (分離)。
4. 在確認對話方塊中，選擇 Detach policy (分離政策)。

   連接的備份政策清單會隨即更新。政策變更會立即生效。

導覽至政策以分離備份政策

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Backup policies (備份政策) 頁面上，選擇您要從根、OU 或帳戶分離的政策名稱。
3. 在 Targets (目標) 索引標籤上，選擇您要分離政策的根、OU 或帳戶旁的選項按鈕。您可能需要展開 OU (選擇 ▶)，以尋找您所需的 OU 和帳戶。
4. 請選擇 Detach (分離)。
5. 在確認對話方塊中，選擇 Detach (分離)。

   連接的備份政策清單會隨即更新。政策變更會立即生效。

AWS CLI & AWS SDKs

從組織根、OU 或帳戶分離備份政策

您可以使用下列其中一項命令來分離備份政策：

- AWS CLI: detach-policy

下列範例會將政策與 OU 分離。

```
$ aws organizations detach-policy \
    --target-id ou-a1b2-f6g7h222 \
    --policy-id p-i9j8k7l6m5
```

此命令成功後就不會產生輸出。

- AWS SDKs: DetachPolicy

政策變更會立即生效。

檢視有效的備份政策

您可以從 AWS 管理主控台，AWS API，或 AWS 命令列界面檢視帳戶的有效備份政策。以下章節提供有效備份政策的簡短概觀，包括範例。

什麼是有效的備份政策？

有效的備份政策指定套用至 AWS 帳戶 的最終備份計劃設定。除了帳戶繼承的任何備份政策的集合，還有直接連接至帳戶的任何備份政策。將備份政策連接至組織根時，該政策會套用至組織中的所有帳戶。將備份政策連接至組織單位 (OU) 時，該政策會套用至屬於此 OU 的所有帳戶和 OU。將政策直接連接至帳戶時，該政策只會套用至一個 AWS 帳戶。

例如，連接至組織根的備份政策，可能指定組織中的所有帳戶以每週一次的預設備份頻率，備份所有 Amazon DynamoDB 資料表。如果個別備份政策直接連接至一個成員帳戶，且在資料表中有重要資訊，則可以覆寫為每天一次的頻率值。這些備份政策的組合包含有效的備份政策。此有效備份政策針對組織中的每個帳戶而個別決定。在此範例中，結果是組織中的所有帳戶每週備份一次 DynamoDB 資料表，例外的是有一個帳戶每天都備份資料表。

如需有關如何將備份政策合併成最終有效備份政策的資訊，請參閱理解管理政策繼承。

檢視有效的備份政策

您可以使用 AWS Management Console、AWS API 或 AWS Command Line Interface 來檢視帳戶的有效備份政策。

> **最低許可**
>
> 若要檢視帳戶的有效備份政策，您必須具有執行下列動作的許可：

- `organizations:DescribeEffectivePolicy`
- `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要

AWS Management Console

檢視帳戶的有效備份政策

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 AWS 帳戶 頁面上，選擇您要檢視其有效備份政策的帳戶名稱。您可能需要展開 OU (選擇)，以尋找您想要的帳戶。
3. 在 Policies (政策) 索引標籤的 Backup policies (備份政策) 區段中，選擇 View the effective backup policy for this AWS 帳戶 (檢視此 AWS 帳戶 帳戶的有效備份政策)。

   主控台會顯示套用至指定帳戶的有效政策。

   > **Note**
   >
   > 在沒有重大變更的情況下，您無法複製並貼上有效政策，以及將其用作另一個備份政策的 JSON。備份政策文件必須包含繼承運算子，指定如何將每一項設定合併至最終有效政策。

AWS CLI & AWS SDKs

檢視帳戶的有效備份政策

您可以使用下列其中一項命令來檢視有效的備份政策：

- AWS CLI: describe-effective-policy

  以下範例顯示備份政策的詳細資訊。

```
$ aws organizations describe-effective-policy \
--policy-type BACKUP_POLICY \
--target-id 123456789012{
    "EffectivePolicy": {
```

```
        "LastUpdatedTimestamp": "2020-06-22T14:31:50.748000-07:00",
        "TargetId": "123456789012",
        "PolicyType": "BACKUP_POLICY",
        "PolicyContent": "{\"plans\":{\"pii_backup_plan\":{\"regions\":[\"ap-
northeast-2\",\"us-east-1\",\"eu-north-1\"],\
"selections\":{\"tags\":{\"datatype\":{\"iam_role_arn\":\"arn:aws:iam::
$account:role/MyIamRole\",\"tag_value\":[\"PII\"],\
"tag_key\":\"dataType\"}}},\"rules\":{\"hourly\":{\"complete_backup_window_minutes
\":\"10080\",\"target_backup_vault_name\
":\"FortKnox\",\"start_backup_window_minutes\":\"480\",\"schedule_expression\":
\"cron(0 5/1 ? * * *)\",\"lifecycle\":{\"mo
ve_to_cold_storage_after_days\":\"180\",\"delete_after_days\":\"270\"},
\"copy_actions\":{\"arn:aws:backup:us-east-1:$accou
nt:backup-vault:secondary-vault\":{\"lifecycle\":
{\"move_to_cold_storage_after_days\":\"10\",\"delete_after_days\":\"100\"
}}}}}}}"
    }
}
```

- AWS SDKs: DescribeEffectivePolicy

使用 AWS CloudTrail 事件監控組織中的備份政策

您可以使用 AWS CloudTrail 事件監控從 AWS 組織中的任何帳戶建立、更新或刪除備份政策的時間，或是組織備份計劃無效的時間。如需詳細資訊，請參閱 AWS Backup 開發人員指南中的記錄跨帳戶管理事件。

備份政策語法和範例

此頁面說明備份政策語法並提供範例。

備份政策的語法

備份政策是根據 JSON 規則建構的純文字檔。備份政策的語法遵循所有管理政策類型的語法。如需該語法的完整討論，請參閱管理政策類型的政策語法和繼承。本主題著重於以該一般語法滿足備份政策類型的特定需求。

備份政策的主體是備份計劃及其規則。備份原則中備份計畫的 AWS Organizations 語法在結構上與所使用的語法完全相同 AWS Backup，但金鑰名稱不同。在以下原則金鑰名稱的說明中，每個都包含對等的 AWS Backup 計劃金鑰名稱。如需有關 AWS Backup 方案的詳細資訊，請參閱CreateBackupPlan開AWS Backup 發人員指南中的。

> **Note**
>
> 使用 JSON 時，重複的密鑰名稱將被拒絕。如果您要在單一原則中包含多個方案、規則或選項，請確定每個金鑰的名稱都是唯一的。

有效的備份政策不僅必須包含備份計畫，還要有排程和規則，才算完整而能發揮作用。此政策還必須識別要備份的資源 AWS 區域 和資源，以及 AWS Backup 可用於執行備份的 AWS Identity and Access Management (IAM) 角色。

以下功能完整的政策顯示基本的備份政策語法。如果此範例直接附加至帳號，則 AWS Backup 會備份標籤值為PII或us-east-1之eu-north-1區域中該帳戶dataType的所有資源RED。每天上午 5:00 會將這些資源備份至 My_Backup_Vault，還會將複本儲存在 My_Secondary_Vault 中。這兩個存放庫都與資源位在相同的帳戶中。它也會將備份複本存放在不同且明確指定帳戶的 My_Tertiary_Vault 中。儲存庫必須已存在於每個針對接收有效策略 AWS 區域 的每個 AWS 帳戶 指定的儲存庫中。如果有任何備份資源是 EC2 執行個體，則會針對這些執行個體上的備份，啟用 Microsoft 磁碟區陰影複製服務 (VSS) 的支援。備份會將 Owner:Backup 標籤套用至每個復原點。

```
{
    "plans": {
        "PII_Backup_Plan": {
            "rules": {
                "My_Hourly_Rule": {
                    "schedule_expression": {"@@assign": "cron(0 5 ? * * *)"},
                    "start_backup_window_minutes": {"@@assign": "60"},
                    "complete_backup_window_minutes": {"@@assign": "604800"},
                    "enable_continuous_backup": {"@@assign": false},
                    "target_backup_vault_name": {"@@assign": "My_Backup_Vault"},
                    "recovery_point_tags": {
                        "Owner": {
                            "tag_key": {"@@assign": "Owner"},
                            "tag_value": {"@@assign": "Backup"}
                        }
                    },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": {"@@assign": "180"},
                        "delete_after_days": {"@@assign": "270"}
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-west-2:$account:backup-
vault:My_Secondary_Vault": {
```

```
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-west-2:$account:backup-
vault:My_Secondary_Vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {"@@assign": "180"},
                                "delete_after_days": {"@@assign": "270"}
                            }
                        },
                        "arn:aws:backup:us-east-1:$account:backup-
vault:My_Tertiary_Vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-
east-1:111111111111:backup-vault:My_Tertiary_Vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {"@@assign": "180"},
                                "delete_after_days": {"@@assign": "270"}
                            }
                        }
                    }
                }
            },
            "regions": {
                "@@append": [
                    "us-east-1",
                    "eu-north-1"
                ]
            },
            "selections": {
                "tags": {
                    "My_Backup_Assignment": {
                        "iam_role_arn": {"@@assign": "arn:aws:iam::$account:role/
MyIamRole"},
                        "tag_key": {"@@assign": "dataType"},
                        "tag_value": {
                            "@@assign": [
                                "PII",
                                "RED"
                            ]
                        }
                    }
                }
            },
```

```
            "advanced_backup_settings": {
                "ec2": {
                    "windows_vss": {"@@assign": "enabled"}
                }
            },
            "backup_plan_tags": {
                "stage": {
                    "tag_key": {"@@assign": "Stage"},
                    "tag_value": {"@@assign": "Beta"}
                }
            }
        }
    }
}
```

備份政策語法包含下列元素：

- $account 變數 – 在政策中的某些文字字串中，您可以使用 $account 變數來代表目前的 AWS 帳戶帳戶。在有效原則中 AWS Backup 執行計劃時，會自動以執行有效原則及其計劃 AWS 帳戶 的目前變數來取代此變數。

  > **Important**
  >
  > 只有在可包含 Amazon Resource Name (ARN) 的政策元素中，才能使用 $account 變數，例如指定備份保存庫以儲存備份的元素，或有權執行備份的 IAM 角色。

  例如，以下要求套用策略的每個儲My_Vault存庫中都 AWS 帳戶 存在名為的儲存庫。

  ```
  arn:aws:backup:us-west-2:$account:vault:My_Vault"
  ```

  建議您使用 AWS CloudFormation 堆疊集及其與組織整合，為組織中的每個成員帳戶自動建立和設定備份保存庫和 IAM 角色。如需詳細資訊，請參閱AWS CloudFormation 使用者指南中的建立具有自我管理許可的堆疊集。

- 繼承運算子 – 備份政策可以使用繼承值設定運算子和子控制運算子。
- plans

  政策的最上層索引鍵是 plans 索引鍵。備份政策在政策檔案的頂端，一定要以這個固定索引鍵名稱開頭。您在此索引鍵下可以有一或多個備份計劃。

- plans 最上層索引鍵之下的每個計劃都有索引鍵名稱，由使用者指派的備份計劃名稱組成。在上述範例中，備份計劃名稱為 PII_Backup_Plan。您可以在一個政策中有多個計劃，每個計劃各有自己的 rules、regions、selections 和 tags。

  備份原則中的這個備份計劃索引鍵名稱會對應至 AWS Backup 計劃中BackupPlanName金鑰的值。

  每個計劃都可以包含下列元素：

  - rules – 此索引鍵包含規則的集合。每個規則會轉譯為排程任務，其中含有開始時間和時段，以備份有效備份政策中的 selections 和 regions 元素所識別的資源。
  - regions— 此索引鍵包含可由此原則備份 AWS 區域 其資源的陣列清單。
  - selections – 此索引鍵包含由指定的 rules 所備份的一或多個資源集合 (在指定的 regions 內)。
  - advanced_backup_settings – 此索引鍵包含在特定資源上執行之備份的特定設定。
  - backup_plan_tags – 這指定標籤以連接至備份計劃本身。
- rules

  rules 政策索引鍵對應至 AWS Backup 計劃中的 Rules 索引鍵。rules 索引鍵之下可以有一或多個規則。每個規則會變成排程任務，以備份所選的資源。

  每個規則都包含索引鍵，而其名稱即規則的名稱。在上一個範例中，規則名稱為「My_Hourly_Rule」。規則索引鍵的值是下列規則元素的集合：

  - schedule_expression— 此原則金鑰對應至 AWS Backup 計劃中的ScheduleExpression金鑰。

    指定備份的開始時間。此索引鍵包含@@assign繼承值運算子和含有 CRON 運算式的字串值，該表示式可指定何時 AWS Backup 起始備份工作。CRON 字串的一般格式為："cron( )"。每個都是數字或萬用字元。例如，cron(0 5 ? * 1,3,5 *) 在每個星期一、星期三和星期五上午 5 點開始備份。cron(0 0/1 ? * * *) 在一週中每一天每小時整點開始備份。
  - target_backup_vault_name— 此原則金鑰對應至 AWS Backup 計劃中的TargetBackupVaultName金鑰。

    指定用來儲存備份的備份保存庫名稱。您可以使用來建立值 AWS Backup。此索引鍵包含 @@assign 繼承值運算子和具有保存庫名稱的字串值。

> **Important**
>
> 第一次啟動備份計劃時，保存庫必須已存在。建議您使用 AWS CloudFormation 堆疊集及其與組織整合，為組織中的每個成員帳戶自動建立和設定備份保存庫和 IAM 角色。如需詳細資訊，請參閱AWS CloudFormation 使用者指南中的建立具有自我管理許可的堆疊集。

- `start_backup_window_minutes`— 此原則金鑰對應至 AWS Backup 計劃中的`StartWindowMinutes`金鑰。

  (選用) 指定在取消未成功啟動的任務之前等待的分鐘數。此索引鍵包含 @@assign 繼承值運算子和整數分鐘數的值。

- `complete_backup_window_minutes` – 此政策索引鍵對應至 AWS Backup 計劃中的 `CompletionWindowMinutes` 索引鍵。

  (選用) 指定備份任務成功啟動之後到必須完成之前的分鐘數，否則會被 AWS Backup取消。此索引鍵包含 @@assign 繼承值運算子和整數分鐘數的值。

- `enable_continuous_backup`— 此原則金鑰對應至 AWS Backup 計劃中的`EnableContinuousBackup`金鑰。

  (選擇性) 指定是否 AWS Backup 建立連續備份。 `True`會導 AWS Backup 致建立能夠 point-in-time 還原 (PITR) 的連續備份。 `False`(或未指定) 會建 AWS Backup 立快照備份。

  > **Note**
  >
  > 由於啟用 PITR 的備份最多可保留 35 天，因此如果您可以設定下列任一選項，您必須選擇 `False` 或不指定值：
  >
  > - 將 `delete_after_days` 設為大於 35。
  > - 將 `move_to_cold_storage_after_days` 設定為任何值。

  如需有關連續備份的詳細資訊，請參閱AWS Backup 開發人員指南中的 P oint-in-time 復原。

- `lifecycle`— 此原則金鑰對應至 AWS Backup 計劃中的`Lifecycle`金鑰。

  (選擇性) 指定何時將此備份 AWS Backup 轉換至冷儲存區，以及何時到期。

  - `move_to_cold_storage_after_days` — 此原則金鑰對應至 AWS Backup 計劃中的`MoveToColdStorageAfterDays`金鑰。

指定備份開始之後到 AWS Backup 將復原點移至不常用儲存體之前的天數。此索引鍵包含 @@assign 繼承值運算子和整數天數的值。

- delete_after_days— 此原則金鑰對應至 AWS Backup 計劃中的DeleteAfterDays金鑰。

  指定備份開始之後到 AWS Backup 刪除復原點之前的天數。此索引鍵包含 @@assign 繼承值運算子和整數天數的值。如果將備份轉移至不常用的儲存體，則備份必須保留至少 90 天，所以，此值必須比 move_to_cold_storage_after_days 值至少再多 90 天。

- copy_actions— 此原則金鑰對應至 AWS Backup 計劃中的CopyActions金鑰。

  (選擇性) 指定 AWS Backup 應將備份複製到一或多個其他位置。每個備份複本位置的說明如下：

  - 名稱唯一識別此複製動作的索引鍵。此時，索引鍵名稱必須是備份保存庫的 Amazon Resource Name (ARN)。此索引鍵包含兩個項目。

    - target_backup_vault_arn – 此政策索引鍵對應至 AWS Backup 計劃中的 DestinationBackupVaultArn 索引鍵。

      (選擇性) 指定 AWS Backup 儲存其他備份複本的資料保險箱。此索引鍵的值包含 @@assign 繼承值運算子和保存庫的 ARN。

      - 若要參考執行備份策略所在的儲存庫，請使用 ARN 中的$account變數來取代帳號 ID 號碼。 AWS 帳戶 AWS Backup 執行備份計畫時，它會自動以執行策略所 AWS 帳戶 在的帳戶 ID 號碼取代變數。如此可在備份政策套用至組織中的多個帳戶時，正確執行備份。
      - 若要同一組織中不同 AWS 帳戶 的保管庫，請使用 ARN 中的實際帳戶 ID 編號。

      > **Important**
      >
      > - 如果缺少此索引鍵，則使用父索引鍵名稱中 ARN 的全小寫版本。由於 ARN 區分大小寫，此字串可能與錯誤的實際 ARN 不相符，且計劃會失敗。因此，我們建議您始終提供此索引鍵和值。
      > - 首次啟動備份計劃時，要將複製備份的目標備份保存庫必須已經存在。建議您使用 AWS CloudFormation StackSets 及其與 Organizations 的整合，自動為組織中的每個成員帳戶，建立並設定備份保存庫和 IAM 角色。如需詳細資訊，請參閱AWS CloudFormation 使用者指南中的建立具有自我管理許可的堆疊集。

    - lifecycle— 此原則金鑰對應至 AWS Backup 計劃中CopyAction金Lifecycle鑰下的金鑰。

      (選擇性) 指定何時將此備份複本 AWS Backup 轉換至冷存放區，以及何時到期。

- move_to_cold_storage_after_days – 此政策索引鍵對應至 AWS Backup 計劃中的 MoveToColdStorageAfterDays 索引鍵。

  指定備份在將復原點 AWS Backup 移至冷存放區之前的天數。此索引鍵包含 @@assign 繼承值運算子和整數天數的值。

- delete_after_days – 此政策索引鍵對應至 AWS Backup 計劃中的 DeleteAfterDays 索引鍵。

  指定備份在 AWS Backup 刪除復原點之前的天數。此索引鍵包含 @@assign 繼承值運算子和整數天數的值。如果將備份轉移至不常用的儲存體，則備份必須保留至少 90 天，所以，此值必須比 move_to_cold_storage_after_days 值至少再多 90 天。

- recovery_point_tags— 此原則金鑰對應至 AWS Backup 計劃中的RecoveryPointTags金鑰。

  (選擇性) 指定 AWS Backup 貼附至其從此計劃建立之每個備份的標籤。此索引鍵的值包含下列一或多個元素：

  - 此索引鍵名稱和值配對的識別符。即使 recovery_point_tags 有不同的大小寫處理方式，對於 tag_key 之下每個元素，此名稱是全部小寫的標籤鍵名稱。此識別符「不」區分大小寫。在上一個範例中，此索引鍵配對由名稱 Owner 所識別。每個索引鍵配對都包含下列元素：

    - tag_key – 指定標籤鍵名稱以連接至備份計劃。此索引鍵包含 @@assign 繼承值運算子和字串值。 值會區分大小寫。

    - tag_value – 指定值以連接至備份計劃並與 tag_key 相關聯。此索引鍵包含任何繼承值運算子，以及要在有效政策中取代、附加或移除的一或多個值。這些值區分大小寫。

- regions

  regions原則索引鍵會指 AWS 區域 定 AWS Backup 尋找符合金selections鑰中條件的資源的內容。此索引鍵包含任何繼承值運算子以及 AWS 區域 代碼的一或多個字串值，例如：["us-east-1", "eu-north-1"]。

- selections

  selections 政策索引鍵指定此政策中的計劃規則所備份的資源。此鍵大致對應於中的BackupSelection物件 AWS Backup。由查詢比對標籤鍵名稱和值來指定資源。selections 索引鍵之下包含一個索引鍵 – tags。

  - tags – 指定用於識別資源的標籤，以及有權查詢和備份資源的 IAM 角色。此索引鍵的值包含下列一或多個元素：

- 此標籤元素的識別符。即使要查詢的標籤有不同的大小寫處理方式，在 tags 之下，此識別符是全部小寫的標籤鍵名稱。此識別符「不」區分大小寫。在上一個範例中，有一個元素由名稱 My_Backup_Assignment 所識別。tags 之下的每個識別符都包含下列元素：
  - iam_role_arn – 指定 IAM 角色，該角色有權在 regions 索引鍵所指定的 AWS 區域 中，存取由標籤查詢所識別的資源。這個值包含@@assign繼承值運算子和包含角色 ARN 的字串值。 AWS Backup 使用此角色來查詢和探索資源，以及執行備份。

    您可以在 ARN 中使用 $account 變數來代替帳戶 ID 號碼。當備份計劃由執行時 AWS Backup，它會自動以執行原則的實際帳戶 ID 號碼來取代變數。 AWS 帳戶

    > **Important**
    >
    > 第一次啟動備份計劃時，此角色必須已存在。建議您使用 AWS CloudFormation 堆疊集及其與組織整合，為組織中的每個成員帳戶自動建立和設定備份保存庫和 IAM 角色。如需詳細資訊，請參閱AWS CloudFormation 使用者指南中的建立具有自我管理許可的堆疊集。

  - tag_key – 指定要搜尋的標籤鍵名稱。此索引鍵包含 @@assign 繼承值運算子和字串值。 值會區分大小寫。
  - tag_value— 指定必須與符合的金鑰名稱相關聯的值tag_key。 AWS Backup 只有在tag_key和tag_value相符時才會在備份中包含資源。此索引鍵包含任何繼承值運算子，以及要在有效政策中取代、附加或移除的一或多個值。這些值區分大小寫。
- advanced_backup_settings – 指定特定備份案例的設定。此索引鍵包含一個或多個設定。每個設定都是包含下列元素的 JSON 物件字串：
  - 物件索引鍵名稱 – 字串，指定要套用下列進階設定的資源類型。
  - 物件值 – JSON 物件字串，其中包含特定於相關資源類型的一個或多個備份設定。

  目前，唯一支援的進階備份設定可為在 Amazon EC2 執行個體上執行的 Windows 或 SQL 伺服器，啟用 Microsoft 磁碟區陰影複製服務 (VSS) 備份。索引鍵名稱必須是 "ec2" 資源類型，且值會指定 "windows_vss" 支援是 enabled 或 disabled，以在這些 Amazon EC2 執行個體上執行備份。如需此功能的詳細資訊，請參閱AWS Backup 開發人員指南中的建立支援 VSS 的 Windows Backup。

```
"advanced_backup_settings": {
    "ec2": {
        "windows_vss": {
            "@@assign": "enabled"
```

```
        }
    }
}
```

- backup_plan_tags – 指定標籤以連接至備份計劃本身。這不會影響任何規則或選項中指定的標籤。

  (選擇性) 您可以將標籤連接至備份計劃。此索引鍵的值是元素的集合。

  即使要查詢的標籤有不同的大小寫處理方式，對於 backup_plan_tags 之下每個元素，索引鍵名稱是全部小寫的標籤鍵名稱。此識別符「不」區分大小寫。其中每個項目的值都包含下列索引鍵：

  - tag_key – 指定標籤鍵名稱以連接至備份計劃。此索引鍵包含 @@assign 繼承值運算子和字串值。此值區分大小寫。
  - tag_value – 指定值以連接至備份計劃並與 tag_key 相關聯。此索引鍵包含 @@assign 繼承值運算子和字串值。此值區分大小寫。

備份政策範例

接下來的備份政策範例僅供參考。在下列某些範例中，可能會壓縮 JSON 空白格式以節省空間。

範例 1：指派給父節點的政策

下列範例顯示備份政策指派給帳戶的其中一個父節點。

父政策 – 此政策可以連接至組織的根，或任何 OU (所有預定帳戶的父系)。

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": {
                "@@assign": [
                    "ap-northeast-2",
                    "us-east-1",
                    "eu-north-1"
                ]
            },
            "rules": {
                "Hourly": {
                    "schedule_expression": {
                        "@@assign": "cron(0 5/1 ? * * *)"
                    },
                    "start_backup_window_minutes": {
```

```
                        "@@assign": "480"
                    },
                    "complete_backup_window_minutes": {
                        "@@assign": "10080"
                    },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": {
                            "@@assign": "180"
                        },
                        "delete_after_days": {
                            "@@assign": "270"
                        }
                    },
                    "target_backup_vault_name": {
                        "@@assign": "FortKnox"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {
                                    "@@assign": "30"
                                },
                                "delete_after_days": {
                                    "@@assign": "120"
                                }
                            }
                        },
                        "arn:aws:backup:us-west-1:111111111111:backup-
vault:tertiary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-
west-1:111111111111:backup-vault:tertiary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {
                                    "@@assign": "30"
                                },
                                "delete_after_days": {
                                    "@@assign": "120"
```

```
                                }
                            }
                        }                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": {
                            "@@assign": "arn:aws:iam::$account:role/MyIamRole"
                        },
                        "tag_key": {
                            "@@assign": "dataType"
                        },
                        "tag_value": {
                            "@@assign": [
                                "PII",
                                "RED"
                            ]
                        }
                    }
                }
            },
            "advanced_backup_settings": {
                "ec2": {
                    "windows_vss": {
                        "@@assign": "enabled"
                    }
                }
            }
        }
    }
}
```

如果沒有其他政策繼承或附加至帳戶，則每個適用的有效策略 AWS 帳戶 如下列範例所示。CRON 運算式導致每小時整點執行一次備份。帳戶 ID 123456789012 將是每個帳戶的實際帳戶 ID。

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": [
                "us-east-1",
                "ap-northeast-3",
```

```
                "eu-north-1"
            ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/1 ? * * *)",
                    "start_backup_window_minutes": "60",
                    "target_backup_vault_name": "FortKnox",
                    "lifecycle": {
                        "to_delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:
$account:vault:secondary_vault"
                            },
                            "lifecycle": {
                                "to_delete_after_days": "28",
                                "move_to_cold_storage_after_days": "180"
                            }
                        },
                        "arn:aws:backup:us-west-1:111111111111:vault:tertiary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-
west-1:111111111111:vault:tertiary_vault"
                            },
                            "lifecycle": {
                                "to_delete_after_days": "28",
                                "move_to_cold_storage_after_days": "180"
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::123456789012:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [
                            "PII",
                            "RED"
                        ]
```

```
                    }
                }
            },
            "advanced_backup_settings": {
                "ec2": {
                    "windows_vss": "enabled"
                }
            }
        }
    }
}
```

範例 2：父政策與子政策合併

在下列範例中，繼承的父策略和子策略會繼承或直接附加至 AWS 帳戶 合併以形成有效策略。

父政策 – 此政策可以連接至組織的根或任何父 OU。

```
{
    "plans": {
       "PII_Backup_Plan": {
            "regions": { "@@append":[ "us-east-1", "ap-northeast-3", "eu-north-1" ] },
            "rules": {
                "Hourly": {
                    "schedule_expression": { "@@assign": "cron(0 0/1 ? * * *)" },
                    "start_backup_window_minutes": { "@@assign": "60" },
                    "target_backup_vault_name": { "@@assign": "FortKnox" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "28" },
                        "to_delete_after_days": { "@@assign": "180" }
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault" : {
                            "target_backup_vault_arn" : {
                                "@@assign" : "arn:aws:backup:us-east-1:
$account:vault:secondary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "28" },
                                "to_delete_after_days": { "@@assign": "180" }
                            }
                        }
                    }
```

```
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyIamRole" },
                        "tag_key": { "@@assign": "dataType" },
                        "tag_value": { "@@assign": [ "PII", "RED" ] }
                    }
                }
            }
        }
    }
}
```

子政策 – 此政策可以直接連接至帳戶，或父政策所連接 OU 之下任何層級的 OU。

```
{
    "plans": {
       "Monthly_Backup_Plan": {
            "regions": {
                "@@append":[ "us-east-1", "eu-central-1" ] },
            "rules": {
                "Monthly": {
                    "schedule_expression": { "@@assign": "cron(0 5 1 * ? *)" },
                    "start_backup_window_minutes": { "@@assign": "480" },
                    "target_backup_vault_name": { "@@assign": "Default" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "30" },
                        "to_delete_after_days": { "@@assign": "365" }
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:Default" : {
                            "target_backup_vault_arn" : {
                                "@@assign" : "arn:aws:backup:us-east-1:
$account:vault:Default"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "30" },
                                "to_delete_after_days": { "@@assign": "365" }
                            }
```

```
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "MonthlyDatatype": {
                        "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyMonthlyBackupIamRole" },
                        "tag_key": { "@@assign": "BackupType" },
                        "tag_value": { "@@assign": [ "MONTHLY", "RED" ] }
                    }
                }
            }
        }
    }
}
```

產生的有效政策 – 套用至帳戶的有效政策包含兩個計劃，每個計劃各自有一組規則和一組要套用規則的資源。

```
{
    "plans": {
       "PII_Backup_Plan": {
            "regions": [ "us-east-1", "ap-northeast-3", "eu-north-1" ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/1 ? * * *)",
                    "start_backup_window_minutes": "60",
                    "target_backup_vault_name": "FortKnox",
                    "lifecycle": {
                        "to_delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault" : {
                            "target_backup_vault_arn" : {
                                "@@assign" : "arn:aws:backup:us-east-1:
$account:vault:secondary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": "28",
                                "to_delete_after_days": "180"
```

```
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::$account:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [ "PII", "RED" ]
                    }
                }
            }
        },
        "Monthly_Backup_Plan": {
            "regions": [ "us-east-1", "eu-central-1" ],
            "rules": {
                "monthly": {
                    "schedule_expression": "cron(0 5 1 * ? *)",
                    "start_backup_window_minutes": "480",
                    "target_backup_vault_name": "Default",
                    "lifecycle": {
                        "to_delete_after_days": "365",
                        "move_to_cold_storage_after_days": "30"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:Default" : {
                            "target_backup_vault_arn": {
                                "@@assign" : "arn:aws:backup:us-east-1:
$account:vault:Default"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": "30",
                                "to_delete_after_days": "365"
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "monthlydatatype": {
```

```
                        "iam_role_arn": "arn:aws:iam::&ExampleAWSAccountNo3;:role/
MyMonthlyBackupIamRole",
                        "tag_key": "BackupType",
                        "tag_value": [ "MONTHLY", "RED" ]
                    }
                }
            }
        }
    }
}
```

範例 3：父政策防止子政策做出任何變更

在下列範例中，繼承的父政策使用子控制運算子來強制執行所有設定，並防止子政策變更或覆寫這些設定。

父政策 – 此政策可以連接至組織的根或任何父 OU。政策的每個節點上都出現 "@@operators_allowed_for_child_policies": ["@@none"]，表示子政策完全無法變更計劃。子政策也無法將其他計劃新增至有效政策。此政策成為所連接的 OU 之下每個 OU 和帳戶的有效政策。

```
{
    "plans": {
        "@@operators_allowed_for_child_policies": ["@@none"],
        "PII_Backup_Plan": {
            "@@operators_allowed_for_child_policies": ["@@none"],
            "regions": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@append": [
                    "us-east-1",
                    "ap-northeast-3",
                    "eu-north-1"
                ]
            },
            "rules": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "Hourly": {
                    "@@operators_allowed_for_child_policies": ["@@none"],
                    "schedule_expression": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "@@assign": "cron(0 0/1 ? * * *)"
                    },
                    "start_backup_window_minutes": {
```

```
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "@@assign": "60"
                    },
                    "target_backup_vault_name": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "@@assign": "FortKnox"
                    },
                    "lifecycle": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "move_to_cold_storage_after_days": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "28"
                        },
                        "to_delete_after_days": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "180"
                        }
                    },
                    "copy_actions": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:
$account:vault:secondary_vault",
                                "@@operators_allowed_for_child_policies": ["@@none"]
                            },
                            "lifecycle": {
                                "@@operators_allowed_for_child_policies": ["@@none"],
                                "to_delete_after_days": {
                                    "@@operators_allowed_for_child_policies":
 ["@@none"],
                                    "@@assign": "28"
                                },
                                "move_to_cold_storage_after_days": {
                                    "@@operators_allowed_for_child_policies":
 ["@@none"],
                                    "@@assign": "180"
                                }
                            }
                        }
                    }
                },
```

```
            "selections": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "tags": {
                    "@@operators_allowed_for_child_policies": ["@@none"],
                    "datatype": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "iam_role_arn": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "arn:aws:iam::$account:role/MyIamRole"
                        },
                        "tag_key": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "dataType"
                        },
                        "tag_value": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": [
                                "PII",
                                "RED"
                            ]
                        }
                    }
                },
                "advanced_backup_settings": {
                    "@@operators_allowed_for_child_policies": ["@@none"],
                    "ec2": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "windows_vss": {
                            "@@assign": "enabled",
                            "@@operators_allowed_for_child_policies": ["@@none"]
                        }
                    }
                }
            }
        }
}
```

產生的有效政策 – 忽略任何存在的子備份政策，父政策會成為有效政策。

```
{
    "plans": {
        "PII_Backup_Plan": {
```

```
            "regions": [
                "us-east-1",
                "ap-northeast-3",
                "eu-north-1"
            ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/1 ? * * *)",
                    "start_backup_window_minutes": "60",
                    "target_backup_vault_name": "FortKnox",
                    "lifecycle": {
                        "to_delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180"
                    },
                    "copy_actions": {
                        "target_backup_vault_arn": "arn:aws:backup:us-
east-1:123456789012:vault:secondary_vault",
                        "lifecycle": {
                            "move_to_cold_storage_after_days": "28",
                            "to_delete_after_days": "180"
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::123456789012:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [
                            "PII",
                            "RED"
                        ]
                    }
                }
            },
            "advanced_backup_settings": {
                "ec2": {"windows_vss": "enabled"}
            }
        }
    }
}
```

範例 4：父政策防止子政策變更備份計劃

在下列範例中，繼承的父政策使用子控制運算子來強制執行單一計劃的設定，並防止子政策變更或覆寫這些設定。子政策仍然可以新增其他計劃。

父政策 – 此政策可以連接至組織的根或任何父 OU。此範例與上一個範例類似，一樣都封鎖所有子繼承運算子，但 plans 最上層除外。該層級的 @@append 設定可讓子政策將其他計劃新增至有效政策中的集合。仍然完全禁止變更繼承的計劃。

為了清楚起見，已截斷計劃中的區段。

```
{
    "plans": {
        "@@operators_allowed_for_child_policies": ["@@append"],
        "PII_Backup_Plan": {
            "@@operators_allowed_for_child_policies": ["@@none"],
            "regions": { ... },
            "rules": { ... },
            "selections": { ... }
        }
    }
}
```

子政策 – 此政策可以直接連接至帳戶，或父政策所連接 OU 之下任何層級的 OU。這個子政策定義新的計劃。

為了清楚起見，已截斷計劃中的區段。

```
{
    "plans": {
        "MonthlyBackupPlan": {
            "regions": { ... },
            "rules": { ... },
            "selections": { … }
        }
    }
}
```

產生的有效政策 – 有效政策包含這兩個計劃。

```
{
```

```
    "plans": {
        "PII_Backup_Plan": {
            "regions": { ... },
            "rules": { ... },
            "selections": { ... }
        },
        "MonthlyBackupPlan": {
            "regions": { ... },
            "rules": { ... },
            "selections": { … }
        }
    }
}
```

範例 5：子政策覆寫父政策中的設定

在下列範例中，子政策使用值設定運算子來覆寫從父政策繼承的某些設定。

父政策 – 此政策可以連接至組織的根或任何父 OU。子政策可以覆寫任何設定，因為沒有子控制運算子出面禁止，所以預設行為允許子政策 @@assign、@@append 或 @@remove。父政策包含有效備份計劃的所有必要元素，因此，只要原封不動繼承，就會成功備份資源。

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": {
                "@@append": [
                    "us-east-1",
                    "ap-northeast-3",
                    "eu-north-1"
                ]
            },
            "rules": {
                "Hourly": {
                    "schedule_expression": {"@@assign": "cron(0 0/1 ? * * *)"},
                    "start_backup_window_minutes": {"@@assign": "60"},
                    "target_backup_vault_name": {"@@assign": "FortKnox"},
                    "lifecycle": {
                        "to_delete_after_days": {"@@assign": "2"},
                        "move_to_cold_storage_after_days": {"@@assign": "180"}
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:t2": {
```

```
                            "target_backup_vault_arn": {"@@assign": "arn:aws:backup:us-
east-1:$account:vault:t2"},
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {"@@assign": "28"},
                                "to_delete_after_days": {"@@assign": "180"}
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": {"@@assign": "arn:aws:iam::$account:role/
MyIamRole"},
                        "tag_key": {"@@assign": "dataType"},
                        "tag_value": {
                            "@@assign": [
                                "PII",
                                "RED"
                            ]
                        }
                    }
                }
            }
        }
    }
}
```

子政策 – 子政策只能包含的設定必須不同於繼承的父政策。合併到有效政策時，必須有繼承的父政策提供其他必要的設定。否則，有效的備份政策會包含無效的備份計劃，而無法如預期般備份資源。

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": {
                "@@assign": [
                    "us-west-2",
                    "eu-central-1"
                ]
            },
            "rules": {
                "Hourly": {
```

```
                    "schedule_expression": {"@@assign": "cron(0 0/2 ? * * *)"},
                    "start_backup_window_minutes": {"@@assign": "80"},
                    "target_backup_vault_name": {"@@assign": "Default"},
                    "lifecycle": {
                        "move_to_cold_storage_after_days": {"@@assign": "30"},
                        "to_delete_after_days": {"@@assign": "365"}
                    }
                }
            }
        }
    }
}
```

產生的有效政策 – 有效政策包含兩個政策的設定，而子政策所提供的設定會覆寫從父政策繼承的設定。此範例中有下列變更：

- 區域清單換成完全不同的清單。如果您要將區域新增至繼承的清單，請在子政策中使用 `@@append`，而不是 `@@assign`。
- AWS Backup 每隔一小時執行一次，而不是每小時。
- AWS Backup 允許 80 分鐘開始備份，而不是 60 分鐘。
- AWS Backup 使用資`Default`料保險箱而不是`FortKnox`。
- 生命週期延長，而得以轉移至不常用的儲存體及最終刪除備份。

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": [
                "us-west-2",
                "eu-central-1"
            ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/2 ? * * *)",
                    "start_backup_window_minutes": "80",
                    "target_backup_vault_name": "Default",
                    "lifecycle": {
                        "to_delete_after_days": "365",
                        "move_to_cold_storage_after_days": "30"
                    },
                    "copy_actions": {
```

```
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault": {
                            "target_backup_vault_arn": {"@@assign": "arn:aws:backup:us-
east-1:$account:vault:secondary_vault"},
                            "lifecycle": {
                                "move_to_cold_storage_after_days": "28",
                                "to_delete_after_days": "180"
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::$account:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [
                            "PII",
                            "RED"
                        ]
                    }
                }
            }
        }
    }
}
```

標籤政策

您可以使用標籤政策來維護標籤的一致性，包括標籤索引鍵和標籤值的慣用大小寫處理。

什麼是標籤？

標籤是您所指派或 AWS 指派給 AWS 資源的自訂屬性標籤。每個標籤有兩個部分：

- 標籤鍵 (例如，CostCenter、Environment 或 Project)。標籤鍵會區分大小寫。
- 選用欄位，稱為標籤值 (例如 111122223333 或 Production)。忽略標籤值基本上等同於使用空字串。與標籤鍵相同，標籤值會區分大小寫。

此頁面的其餘部分說明標籤政策。如需標籤的詳細資訊，請參閱下列來源：

- 有關標籤的一般資訊，包括命名和使用慣例，請參閱《標記AWS資源使用指南》。

- 關於支援標記的服務清單，請參閱Resource Groups 標記 API 參考。
- 如需使用標籤分類資源的相關資訊，請參閱標記資AWS源的最佳做法白皮書。
- 如需有關標記 Organizations 資源的資訊，請參閱標記 AWS Organizations 資源。
- 如需標記其他AWS服務中資源的相關資訊，請參閱該服務的說明文件。

什麼是標籤政策？

標籤政策是協助您將組織帳戶中各資源的標籤標準化的一種政策。在標籤政策中，您指定在標記資源時適用的標記規則。

例如，標籤政策可以指定當 `CostCenter` 標籤連接至資源時，必須使用標籤政策所定義的大小寫處理和標籤值。標籤政策也可以指定在指定的資源類型上，強制執行不合規的標記操作。換句話說，防止完成指定的資源類型上不合規的標記請求。對於未標記的資源或標籤政策中未定義的標籤，不會評估是否符合標籤政策。

使用標籤政策涉及使用多個 AWS 服務：

- 使用 AWS Organizations 管理標籤政策。登入組織的管理帳戶時，您可以使用 Organizations 來啟用標籤政策功能。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。然後，您就可以建立標籤政策並連接至組織實體，使這些標記規則生效。
- 使用 AWS Resource Groups 管理是否符合標籤政策。登入組織中的帳戶時，您可以使用 Resource Groups 在帳戶中的資源上尋找不合規標籤。您可以在建立資源的 AWS 服務中更正不合規標籤。

  如果您登入組織中的管理帳戶，您可以檢視組織所有帳戶的合規資訊。

只有在已啟用所有功能的組織中，才能使用標籤政策。如需使用標籤政策所需條件的詳細資訊，請參閱管理標籤政策的先決條件和許可。

> **Important**
>
> 若要開始使用標籤政策，AWS 強烈建議您先遵循開始使用標籤政策中所述的範例工作流程，之後才繼續使用更進階的標籤政策。將標籤政策擴及整個 OU 或組織之前，最好先了解將簡單標籤政策連接至單一帳戶的效果。在您強制符合任何標籤政策之前，尤其要了解標籤政策的效果。開始使用標籤政策 頁面上的表格也提供連結來說明更進階政策的相關任務。

管理標籤政策的先決條件和許可

此頁面說明在 AWS Organizations 中管理標籤政策的先決條件和必要許可。

主題

管理標籤政策的先決條件

需要符合下列條件才能使用標籤政策：

- 您的組織必須啟用所有功能。
- 您必須登入組織的管理帳戶。
- 您需要有管理標籤政策的許可中列出的許可。

若要評估是否符合標籤政策，請使用 AWS Resource Groups。如需評估合規性需求的相關資訊，請參閱 AWS Resource Groups 使用者指南中的先決條件和許可。

管理標籤政策的許可

下列範例 IAM 政策提供管理標籤政策的許可。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageTagPolicies",
            "Effect": "Allow",
            "Action": [
                "organizations:ListPoliciesForTarget",
                "organizations:ListTargetsForPolicy",
                "organizations:DescribeEffectivePolicy",
                "organizations:DescribePolicy",
                "organizations:ListRoots",
                "organizations:DisableAWSServiceAccess",
                "organizations:DetachPolicy",
                "organizations:DeletePolicy",
                "organizations:DescribeAccount",
                "organizations:DisablePolicyType",
```

```
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListPolicies",
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:EnableAWSServiceAccess",
                "organizations:ListCreateAccountStatus",
                "organizations:DescribeOrganization",
                "organizations:UpdatePolicy",
                "organizations:EnablePolicyType",
                "organizations:DescribeOrganizationalUnit",
                "organizations:AttachPolicy",
                "organizations:ListParents",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:CreatePolicy",
                "organizations:DescribeCreateAccountStatus"
            ],
            "Resource": "*"
        }
    ]
}
```

如需有關 IAM 政策和許可的詳細資訊，請參閱 IAM 使用者指南。

使用標籤政策的最佳實務

AWS 建議採取下列最佳實務來使用標籤政策。

決定標籤大寫策略

決定標籤如何使用大寫，並對所有資源類型一致地實作該策略。例如，決定要使用 `Costcenter`、`costcenter` 還是 `CostCenter`，並針對所有標籤使用相同的慣例。為了讓合規報告產生一致的結果，請避免使用大小寫處理不一致的相似標籤。此策略可協助您定義組織的標籤政策。

使用建議的工作流程

從小的開始，建立簡單的標籤政策。然後連接至可用於測試的成員帳戶。使用開始使用標籤政策中所述的工作流程。

決定標籤規則

這將取決於您組織的需求。例如，建議您指定當 `CostCenter` 標籤連接至 AWS Secrets Manager 秘密時，必須使用指定的大小寫處理。建立標籤政策來定義合規標籤，並將標籤政策連接至您希望這些標記規則生效的組織實體。

教導帳戶管理員

當您準備擴大使用標籤政策時，請教導帳戶管理員，如下所示：

- 傳達您的標記策略。
- 強調指出管理員需要在特定資源類型上使用標籤。

  這很重要，因為未標記的資源在合規結果中不會顯示為不合規。
- 提供指引來檢查是否符合標籤政策。指示管理員尋找並更正其帳戶中資源的不相容標籤，使用 AWS Resource Groups 使用者指南中的評估帳戶的合規性。讓他們知道您希望他們多久檢查一次合規性。

強制合規性時請小心。

強制合規性可能會使組織帳戶中的使用者無法標記他們所需的資源。檢閱了解強制中的資訊。另請參閱開始使用標籤政策中所述的工作流程。

考慮建立 SCP 以防護資源建立請求

從未貼上標籤的資源在報告中不會顯示為不合規。帳戶管理員仍然可以建立未標記的資源。在某些情況下，您可以使用服務控制政策 (SCP) 來為資源建立請求設定防護。如需 SCP 範例，請參閱 需要在建立的指定資源上使用標籤。若要了解 AWS 服務是否支援使用標籤控制存取，請參閱《IAM 使用者指南》中的與 IAM 搭配使用的 AWS 服務。尋找依據標籤授權欄中為是的服務。選擇服務的名稱，以檢視該服務的授權和存取控制文件。

開始使用標籤政策

使用標籤政策涉及使用多個 AWS 服務。若要開始使用，請檢閱下列頁面。然後遵循此頁面上的工作流程，熟悉標籤政策及其效果。

- 管理標籤政策的先決條件和許可
- 使用標籤政策的最佳實務

第一次使用標籤政策

請依照下列步驟，開始首次使用標籤政策。

任務	要登入的帳戶	要使用的 AWS 服務主控台
步驟 1：為您的組織啟用標籤政策。	組織的管理帳戶。[1]	AWS Organizations
步驟 2：建立標籤政策。 讓第一個標籤政策保持簡單。以您要使用的大小寫處理輸入一個標籤鍵，所有其他選項都保留預設值。	組織的管理帳戶。[1]	AWS Organizations
步驟 3：將標籤政策連接至可用於測試的單一成員帳戶。 您在下一個步驟必須登入此帳戶。	組織的管理帳戶。[1]	AWS Organizations
步驟 4：建立一些含有合規標籤的資源，也建立一些含有不合規標籤的資源。	您用於測試的成員帳戶。	您習慣使用的任何 AWS 服務。例如，您可以使用 AWS Secrets Manager 並遵循建立基本秘密中的程序，建立含有合規和不合規秘密的秘密。
步驟 5：檢視有效的標籤政策並評估帳戶的合規狀態。	您用於測試的成員帳戶。	用來建立資源的 Resource Groups 和 AWS 服務。 如果您建立的資源含有合規和不合規標籤，您在結果中應該會看到不合規標籤。
步驟 6：重複過程來尋找並更正合規問題，直到測試帳戶中的資源符合標籤政策為止。	您用於測試的成員帳戶。	用來建立資源的 Resource Groups 和 AWS 服務。
您可以隨時評估組織整體合規性。	組織的管理帳戶。[1]	資源群組

[1] 您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。

擴大使用標籤政策

您可以依任何順序執行下列任務，以擴大使用標籤政策。

進階任務	要登入的帳戶	要使用的 AWS 服務主控台
建立更進階的標籤政策。 請遵循與新手使用者相同的程序，但嘗試其他任務。例如，定義其他鍵或值，或為標籤鍵指定不同的大小寫處理方式。 您可以使用 理解管理政策繼承 和 標籤政策語法 中的資訊，建立更詳細的標籤政策。	組織的管理帳戶。[1]	AWS Organizations
將標籤政策連接至其他帳戶或 OU。 將更多政策連接至帳戶，或帳戶隸屬的任何 OU 之後，請檢查帳戶的有效標籤政策。	組織的管理帳戶。[1]	AWS Organizations
建立 SCP 以在任何人建立新資源時要求標籤。如需範例，請參閱 需要在建立的指定資源上使用標籤。	組織的管理帳戶。[1]	AWS Organizations
當帳戶的合規狀態改變時，根據有效的標籤政策，持續評估帳戶的合規狀態。更正不合規標籤。	含有效標籤政策的成員帳戶。	用來建立資源的 Resource Groups 和 AWS 服務。
評估組織整體合規性。	組織的管理帳戶。[1]	資源群組

[1] 您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。

第一次強制執行標籤政策

若要第一次強制執行標籤政策，請遵循類似於第一次使用標籤政策的工作流程，並使用測試帳戶。

> **Warning**
>
> 強制合規性時請小心。請確定您了解使用標籤政策的效果，並遵循建議的工作流程。在擴大強制更多帳戶之前，請先在測試帳戶上測試強制的效果。否則，可能會使組織帳戶中的使用者無法標記他們所需的資源。如需更多詳細資訊，請參閱 了解強制。

強制任務	要登入的帳戶	要使用的 AWS 服務主控台
步驟 1：建立標籤政策。 讓第一個強制的標籤政策保持簡單。以您要使用的大小寫處理輸入一個標籤鍵，然後選擇 Prevent noncompliant operations for this tag (防止對此標籤執行不合規操作) 選項。然後指定一個要強制執行標籤政策的資源類型。延續先前的範例，您可以選擇對 Secrets Manager 秘密強制執行標籤政策。	組織的管理帳戶。[1]	AWS Organizations
步驟 2：將標籤政策連接至單一測試帳戶。	組織的管理帳戶。[1]	AWS Organizations
步驟 3：嘗試建立一些含有合規標籤的資源，也建立一些含有不合規標籤的資源。如果資源是含不合規標籤的標籤政策中所指定的類型，應該就不允許您在此資源上建立標籤。	您用於測試的成員帳戶。	您習慣使用的任何 AWS 服務。例如，您可以使用 AWS Secrets Manager 並遵循建立基本秘密中的程序，建立含有合規和不合規秘密的秘密。

強制任務	要登入的帳戶	要使用的 AWS 服務主控台
步驟 4：根據有效的標籤政策，評估帳戶的合規狀態，並更正不合規標籤。	您用於測試的成員帳戶。	用來建立資源的 Resource Groups 和 AWS 服務。
步驟 5：重複過程來尋找並更正合規問題，直到測試帳戶中的資源符合標籤政策為止。	您用於測試的成員帳戶。	用來建立資源的 Resource Groups 和 AWS 服務。
您可以隨時評估組織整體合規性。	組織的管理帳戶。[1]	資源群組

[1] 您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。

建立、更新和刪除標籤政策

在本主題中：

- 對組織啟用標籤政策後，您就可以建立政策。
- 當標記需求變更時，您可以更新現有的政策。
- 如果您不再需要某項政策，則將該政策從所有 OU 和帳戶中分離後，即可刪除政策。

> **Important**
>
> 未標記的資源由於不合規而無法出現在結果中。

建立標籤政策

> **最低許可**
>
> 若要建立標籤政策，您需要具有執行下列動作的許可：
>
> - `organizations:CreatePolicy`

在 AWS Management Console 中有兩種方式建立標記政策：

- 視覺化編輯器，可讓您選擇選項，然後為您產生 JSON 政策文字。
- 文字編輯器，可讓您直接建立 JSON 政策文字。

視覺化編輯器讓程序變簡單，但彈性受限。若要建立第一個政策並熟悉使用政策，這是好方法。在了解政策的運作方式，並開始覺得受限於視覺化編輯器後，您可以自行編輯 JSON 政策文字，將進階功能新增至政策。視覺化編輯器只使用 @@assign 值設定運算子，完全不支援存取子控制運算子。只有在手動編輯 JSON 政策文字時，才能新增子控制運算子。

AWS Management Console

建立標籤政策

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Tag policies (標籤政策) 頁面上，選擇 Create policy (建立政策)。
3. 在 Create policy (建立政策) 頁面上，輸入政策的 Policy name (政策名稱) 與選用的 Policy description (政策描述)。
4. (選用) 您可以將一個或多個標籤新增至政策物件本身。這些標籤不是政策的一部分。若要執行此操作，請選擇 Add tag (新增標籤)，然後輸入一個鍵和一個選用值。將值留空會將其設定為空白字串；而不是 null。您可以在政策中連接最多 50 個標籤。如需更多詳細資訊，請參閱標記 AWS Organizations 資源。
5. 您可以使用 Visual editor (視覺化編輯器) 建立標籤政策，如本程序所述。您也可以在 JSON 索引標籤中輸入或貼上標籤政策。如需標籤政策語法的相關資訊，請參閱標籤政策語法。

   針對 New Tag Key 1(新標籤鍵 1)，指定要新增的標籤鍵名稱。
6. 對於 Tag key capitalization compliance (標籤鍵大寫合規)，維持不選取此選項 (預設)，以指定父標籤政策應該定義標籤鍵的大小寫處理。

   如果您要使用此政策來強制標籤鍵的特定大寫，請啟用此選項。如果您選取此選項，您為 Tag Key (標籤鍵) 指定的大寫，將覆寫父政策中指定的大小寫處理。

   如果父政策不存在且您未選取此選項，則只有完全小寫字元的標籤鍵才視為合規。如需父政策中有關繼承的詳細資訊，請參閱理解管理政策繼承。

> **Tip**
>
> 在建立標籤政策來定義標籤鍵及其大小寫處理時，請考慮使用範例 1：定義整個組織的標籤鍵大小寫中顯示的範例標籤政策作為指南。將此標籤政策連接至組織根目錄。稍後，您可以建立額外的標籤政策，並連接至 OU 或帳戶，以建立其他標記規則。

7. 適用於標籤值合規，如果您要將此標籤鍵的允許值新增到從父政策繼承的任何值，請啟用此選項。

   依預設會清除此選項，這表示只有從父政策定義和繼承的那些值才視為合規。如果父政策不存在或未指定標籤值，則任何值 (包括完全沒有值) 都視為合規。

   若要更新可接受的標籤值清單，請選取 Specify allowed values for this tag key (指定此標籤鍵的允許值)，然後選取 Specify values (指定值)。出現提示時，輸入新的值 (每個方塊一個值)，然後選擇 Save changes (儲存變更)。

8. 對於 Prevent noncompliant operations for this tag (防止對此標籤執行不合規操作)，建議除非您使用標籤政策很有經驗，否則請維持不選取此選項 (預設)。請確定您已檢閱了解強制中的建議，並全面測試。否則，可能會使組織帳戶中的使用者無法標記他們所需的資源。

   如果您確實想要強制此標籤鍵合規，請選取此核取方塊，然後選取 Specify resource types (指定資源類型)。提示後，請選取要包含在政策中的資源類型。接著選擇 Save changes (儲存變更)。

> **Important**
>
> 選取此選項後，任何操縱指定類型資源標籤的操作，僅在操作使標籤符合政策時才會成功。

9. (選用) 若要將另一個標籤鍵新增至此標籤政策，請選擇 Add tag key (新增標籤鍵)。然後執行步驟 6–9 來定義標籤鍵。
10. 標籤政策建置完成時，請選擇 Save Changes (儲存變更)。

AWS CLI & AWS SDKs

建立標籤政策

您可以使用下列其中一項來建立標籤政策：

- AWS CLI: create-policy

  您可以使用任何文字編輯器來建立標籤政策。使用 JSON 語法，並在您選擇的位置中，以任何名稱和副檔名將標籤政策儲存為檔案。標籤政策最多可包含 2,500 個字元，包括空格。如需標籤政策語法的相關資訊，請參閱標籤政策語法。

  建立標籤政策

  1. 文字檔案中建立看起來類似下列內容的標籤政策：

     testpolicy.json 的內容：

     ```
     {
         "tags": {
             "CostCenter": {
                 "tag_key": {
                     "@@assign": "CostCenter"
                 }
             }
         }
     }
     ```

     此標籤政策定義 CostCenter 標籤鍵。標籤可以接受或不接受任何值。這樣的政策表示，帶有CostCenter 標籤的資源 (無論是否連接任何值) 都符合規定。

  2. 建立包含檔案中政策內容的政策。為了便於閱讀，輸出中的額外空白字元已被截斷。

     ```
     $ aws organizations create-policy \
         --name "MyTestTagPolicy" \
         --description "My Test policy" \
         --content file://testpolicy.json \
         --type TAG_POLICY
     {
         "Policy": {
             "PolicySummary": {
                 "Id": "p-a1b2c3d4e5",
                 "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
     tag_policy/p-a1b2c3d4e5",
                 "Name": "MyTestTagPolicy",
                 "Description": "My Test policy",
                 "Type": "TAG_POLICY",
                 "AwsManaged": false
             },
     ```

```
        "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign
\":\"CostCenter\"\n}\n}\n}\n}\n\n"
    }
}
```

- AWS SDKs: CreatePolicy

後續作業

建立標籤政策後，您可以使標記規則生效。若要這樣做，請連接政策至組織根、組織單位 (OU)、組織內的 AWS 帳戶，或組織實體的組合。

更新標籤策略

> **最低許可**
>
> 若要更新標籤政策，您必須具有執行下列動作的許可：
>
> - `organizations:UpdatePolicy`，並在包含指定政策 (或 "*") 的 ARN 的相同政策陳述式中具有 `Resource` 元素
> - `organizations:DescribePolicy`，並在包含指定政策 (或 "*") 的 ARN 的相同政策陳述式中具有 `Resource` 元素

AWS Management Console

更新標籤政策

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Tag policies (標籤政策) 頁面上，選擇您要更新的標籤政策。
3. 選擇 Edit Policy (編輯政策)。
4. 您可以輸入新的政策名稱、政策描述。可以使用視覺化編輯器或直接編輯 JSON，來變更政策內容。
5. 標籤政策更新完成時，請選擇 Save Changes (儲存變更)。

AWS CLI & AWS SDKs

更新政策

您可以使用下列其中一項來更新政策：

- AWS CLI: update-policy

  下列範例會重新命名標籤政策。

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed tag policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-i9j8k7l6m5",
            "Name": "Renamed tag policy",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
        "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign\":
\"CostCenter\"\n}\n}\n}\n}\n\n"
    }
}
```

  下列範例會新增或變更標籤政策的描述。

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new tag policy description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-i9j8k7l6m5",
            "Name": "Renamed tag policy",
            "Description": "My new tag policy description",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
       "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign\":
\"CostCenter\"\n}\n}\n}\n}\n\n"
    }
```

```
}
```

下列範例會變更連接至 AI 服務選擇退出政策的 JSON 政策文件。在此範例中，內容擷取自名稱為 policy.json 的檔案，其中包含以下文字：

```
{
  "tags": {
    "Stage": {
      "tag_key": {
        "@@assign": "Stage"
      },
      "tag_value": {
        "@@assign": [
          "Production",
          "Test"
        ]
      }
    }
  }
}
```

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --content file://policy.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-i9j8k7l6m5",
            "Name": "Renamed tag policy",
            "Description": "My new tag policy description",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"tags\":{\"Stage\":{\"tag_key\":{\"@@assign\":\"Stage
\"},\"tag_value\":{\"@@assign\":[\"Production\",\"Test\"]},\"enforced_for\":
{\"@@assign\":[\"ec2:instance\"]}}}}"
}
```

- AWS SDKs: UpdatePolicy

編輯連接至標籤政策的標籤

登入您的組織的管理帳戶時，您可以新增或移除連接至標籤政策的標籤。若要執行此動作，請執行下列步驟。

最低許可

若要編輯連接至您 AWS 組織的標籤政策標籤，您必須擁有以下許可：

- `organizations:DescribeOrganization` (僅限主控台 – 導覽至政策)
- `organizations:DescribePolicy` (僅限主控台 – 導覽至政策)
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

編輯連接至 AI 服務選擇退出政策的標籤

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Tag policies (標籤政策) 頁面上，選擇您要編輯的附有標籤的政策名稱。
3. 在所選政策的詳細資訊頁面上，選擇 Tags (標籤) 索引標籤，然後選擇 Manage tags (管理標籤)。
4. 您可以在此頁面上執行任一動作：
   - 透過在舊值上輸入新值來編輯任何標籤的值。您無法修改標籤鍵。若要變更標籤鍵，您必須刪除含有舊標籤鍵的標籤，並新增含有新標籤鍵的標籤。
   - 選擇 Remove (移除) 以移除現有的標籤。
   - 新增標籤鍵值組。選擇 Add tag (新增標籤)，然後在提供的方塊中輸入新的標籤鍵名稱和選用值。如果您將 Value (值) 方塊保留空白，則值為空白字串；而不是 `null`。
5. 在您完成所有要進行的新增、移除和編輯之後，選擇 Save changes (儲存變更)。

AWS CLI & AWS SDKs

編輯連接至標籤政策的標記

您可以使用下列其中一項命令來編輯連接至標籤政策的標籤：

- AWS CLI: tag-resource and untag-resource
- AWS SDKs: TagResource and UntagResource

刪除標籤政策

登入到您的組織的管理帳戶時，您可以刪除在您的組織中不再需要的政策。

您必須先將政策從所有連接的實體分離，才能刪除政策。

> **最低許可**
>
> 若要刪除標籤政策，您必須具有執行下列動作的許可：
>
> - `organizations:DeletePolicy`

AWS Management Console

刪除標籤政策

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2.
3. 在 Tag policies (標籤政策) 頁面上，選擇您要刪除的政策。
4. 您必須先將您要刪除的政策從所有根、OU 和帳戶分離。選擇 Targets (目標) 索引標籤，再選擇每個根、OU 或顯示於 Targets (目標) 清單中帳戶旁邊的選項按鈕，然後選擇 Detach (分離)。在確認對話方塊中，選擇 Detach (分離)。
5. 在頁面頂端，選擇 Delete (刪除)。
6. 在確認對話方塊中，輸入政策的名稱，然後選擇 Delete (刪除)。

AWS CLI & AWS SDKs

刪除標籤政策

您可以使用下列其中一項來刪除政策：

- AWS CLI: delete-policy

以下範例會刪除指定的政策。只有在政策未連接至任何根、OU 或帳戶時才有效。

```
$ aws organizations delete-policy \
    --policy-id p-i9j8k7l6m5
```

此命令成功後就不會產生輸出。

- AWS SDKs: DeletePolicy

連接和分離標籤政策

您可以在整個組織及組織單位 (OU) 和個別帳戶上使用標籤政策。

- 當您將標籤政策連接至組織根時，此標籤政策會套用至該根的所有成員 OU 和帳戶。
- 當您將標籤政策連接至 OU 時，該標籤政策會套用至屬於此 OU 的帳戶。這些帳戶也遵從連接至組織根的任何標籤政策。
- 當您將標籤政策連接至帳戶時，該標籤政策會套用至此帳戶。此外，該帳戶受制於連接至組織根的任何標籤政策，還有連接至該帳戶所屬 OU 的任何標籤政策。

帳戶繼承的任何標籤政策，加上直接連接至帳戶的任何標籤政策，聚集而成有效的標籤政策。如需更多詳細資訊，請參閱 理解管理政策繼承。

Important

未標記的資源由於不合規而無法出現在結果中。

最低許可

若要連接標籤政策，您必須具有執行下列動作的許可：

- `organizations:AttachPolicy`

AWS Management Console

您可以導覽至政策或連接政策的根、OU 或帳戶，以連接標籤政策。

導覽至根、OU 或帳戶以連接標籤政策

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 AWS 帳戶 頁面上，導覽至您要連接政策的根、OU 或帳戶的名稱並選擇。您可能需要展開 OU (選擇 ▶)，以尋找您所需的 OU 和帳戶。
3. 在 Policies (政策) 索引標籤的 Tag policies (標籤政策) 項目中，選擇 Attach (連接)。
4. 尋找您所需的政策，然後選擇 Attach policy (連接政策)。

   Policies (政策) 索引標籤上的連接的標籤政策清單會更新，以包含新的新增項目。政策變更會立即生效。

導覽至政策以連接標籤政策

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Tag policies (標籤政策) 頁面上，選擇您要連接的政策名稱。
3. 在 Targets (目標) 索引標籤上，選擇 Attach (連接)。
4. 選擇您要連接政策的根、OU 或帳戶旁的選項按鈕。您可能需要展開 OU (選擇 ▶)，以尋找您所需的 OU 和帳戶。
5. 選擇 Attach policy (連接政策)。

   Targets (目標) 索引標籤上的連接的標籤政策清單會更新，以包含新的新增項目。政策變更會立即生效。

AWS CLI & AWS SDKs

將標籤政策連接至組織根、OU 或帳戶

您可以使用下列其中一項來連接標籤政策：

- AWS CLI: attach-policy

  下列程序顯示如何將剛建立的標籤政策連接至單一測試帳戶。

- 執行下列命令，將標籤政策連接至測試帳戶：

```
$ aws organizations attach-policy \
    --target-id <account-id> \
    --policy-id p-a1b2c3d4e5
```

此命令如果成功就不會有輸出。

- AWS SDKs: AttachPolicy

政策變更會立即生效。

後續作業

連接標籤政策之後，您可以了解您的資源遵從該標籤政策的情形。若要執行此操作，請使用 Resource Groups 主控台。如需相關資訊，請參閱AWS Resource Groups使用者指南中的評估帳戶的合規性。

分離標籤政策

登入組織的管理帳戶後，您可以將標籤政策從原本連接的組織根、OU 或帳戶中分離。從實體分離標籤政策後，該政策即不再套用至現在已分離的實體所影響的任何帳戶。若要分離政策，請完成下列步驟。

最低許可

若要從組織根、OU 或帳戶中分離標籤政策，您必須具有執行下列動作的許可：

- `organizations:DetachPolicy`

AWS Management Console

您可以導覽至政策或分離接政策的根、OU 或帳戶，以分離標籤政策。

導覽至連接的根、OU 或帳戶以分離標籤政策

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 AWS 帳戶 頁面導覽至您要從中分離政策的根、OU 或帳戶。您可能需要展開 OU (選擇) ，以尋找您所需的 OU 和帳戶。選擇根、OU 或帳戶的名稱。

3. 在 Policies (政策) 索引標籤上，選擇您要分離的標籤政策旁邊的選項按鈕，然後選擇 Detach (分離)。
4. 在確認對話方塊中，選擇 Detach policy (分離政策)。

   連接的標籤政策清單會隨即更新。政策變更會立即生效。

導覽至標籤政策以分離備份政策

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Tag policies (標籤政策) 頁面上，選擇您要從根、OU 或帳戶分離的政策名稱。
3. 在 Targets (目標) 索引標籤上，選擇您要分離政策的根、OU 或帳戶旁的選項按鈕。您可能需要展開 OU (選擇 ▶)，以尋找您所需的 OU 和帳戶。
4. 請選擇 Detach (分離)。
5. 在確認對話方塊中，選擇 Detach (分離)。

   連接的標籤政策清單會隨即更新。政策變更會立即生效。

AWS CLI & AWS SDKs

從組織根、OU 或帳戶中分離標籤政策

您可以使用下列其中一項來分離標籤政策：

- AWS CLI: detach-policy
- AWS SDKs: DetachPolicy

政策變更會立即生效。

檢視有效的標籤政策

在您開始檢查帳戶中已標記資源的合規狀態之前，最好先決定帳戶的有效標籤政策。

什麼是有效的標籤政策？

有效的標籤政策指定套用至帳戶的標記規則。帳戶繼承的任何標籤政策，加上直接連接至帳戶的任何標籤政策，聚集而成有效的標籤政策。當您將標籤政策連接至組織根時，該標籤政策會套用至組織中的所有帳戶。當您將標籤政策連接至 OU 時，該標籤政策會套用至屬於此 OU 的所有帳戶和 OU。

例如，連接至組織根的標籤政策，可能定義具有四個合規值的 `CostCenter` 標籤。連接至帳戶的另一個標籤政策，可能限制 `CostCenter` 索引鍵只能有四個合規值之中的兩個。這些標籤政策的組合構成有效的標籤政策。結果是組織根標籤政策中定義的四個合規標籤值之中，只有兩個是帳戶的合規值。

如需有關如何產生有效標籤政策的詳細資訊，以及其他進階範例，請參閱理解管理政策繼承。

如何檢視有效的標籤政策

您可以從 AWS Management Console、AWS API 或 AWS Command Line Interface 檢視帳戶的有效標籤政策。

最低許可

若要檢視帳戶的有效標籤政策，您必須具有執行下列動作的許可：

- `organizations:DescribeEffectivePolicy`
- `organizations:DescribeOrganization`

AWS Management Console

檢視帳戶的有效標籤政策

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 AWS 帳戶 頁面上，選擇您要檢視其有效標籤政策的帳戶名稱。您可能需要展開 OU (選擇) ，以尋找您想要的帳戶。
3. 在 Policies (政策) 索引標籤的 Tag policies (標籤政策) 區段中，選擇 View the effective tag policy for this AWS 帳戶 (檢視此 AWS 帳戶 帳戶的有效標籤政策)。

   主控台會顯示套用至指定帳戶的有效政策。

> **Note**
>
> 在沒有重大變更的情況下，您無法複製並貼上有效政策作為另一個標籤政策的 JSON。標籤政策文件必須包含繼承運算子，以指定如何將每一項設定合併成最終有效政策。

AWS CLI & AWS SDKs

檢視帳戶的有效標籤政策

您可以使用下列其中一項來檢視有效的標籤政策：

- AWS CLI: describe-effective-policy

  若要找出哪些標記規則繼承自或連接至帳戶，請從帳戶執行下列命令，並將結果儲存為檔案：

```
$ aws organizations describe-effective-policy \
    --policy-type TAG_POLICY
{
    "EffectivePolicy": {
        "PolicyContent": "{\"tags\":{\"costcenter\":{\"tag_value\":[\"*\"],
\"tag_key\":\"CostCenter\"}}}",
        "LastUpdatedTimestamp": "2020-06-09T08:34:25.103000-07:00",
        "TargetId": "123456789012",
        "PolicyType": "TAG_POLICY"
    }
}
```

  如果標籤政策連接至該帳戶及根或任何 OU，則這所有繼承的政策共同定義該帳戶的有效標籤政策。在這些情況下，從該帳戶執行 `describe-effective-policy` 會傳回該帳戶階層中所有標籤政策的合併內容。

- AWS SDKs: DescribeEffectivePolicy

使用 Amazon EventBridge 監控不合規標籤

您可以使用 Amazon EventBridge、先前的 Amazon CloudWatch Events 監控何時引入不合規標籤。在下列範例事件中，`tag-policy-compliant` 的 `"false"` 值表示新標籤不符合有效的標籤政策。

```
{
```

```
  "detail-type": "Tag Change on Resource",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa"
  ],
  "detail": {
    "changed-tag-keys": [
      "a-new-key"
    ],
    "service": "ec2",
    "resource-type": "instance",
    "version": 3,
    "tag-policy-compliant": "false",
    "tags": {
      "a-new-key": "tag-value-on-new-key-just-added"
    }
  }
}
```

您可以訂閱事件，並指定要監控的字串或模式。如需詳細資訊，請參閱《Amazon EventBridge 使用者指南》。

了解強制

標籤政策可以指定在指定的資源類型上，強制執行不合規的標記操作。換句話說，防止完成指定的資源類型上不合規的標記請求。

> **Important**
>
> 強制對於未使用標籤來建立的資源沒有影響。

若要強制要求符合標籤政策，請在建立標籤政策時執行下列其中一項動作：

- 從 Visual editor (視覺化編輯器) 索引標籤中，選取 Prevent noncompliant operations for this tag (防止對此標籤執行不合規操作)。
- 從 JSON 索引標籤中，使用 `enforced_for` 欄位。如需標籤政策語法的相關資訊，請參閱標籤政策語法和範例。

遵循以下最佳實務來強制符合標籤政策：

- 強制合規性時請小心 – 確定您了解使用標籤政策的效果，並遵循 開始使用標籤政策 中所述的建議工作流程。在擴大強制更多帳戶之前，請先在測試帳戶上測試強制的效果。否則，可能會使組織帳戶中的使用者無法標記他們所需的資源。
- 注意您可以強制的資源類型 – 您只能在支援的資源類型上強制符合標籤政策。當您使用視覺化編輯器建置標籤政策時，將會列出支援強制合規的資源類型。
- 了解與某些服務的互動 – 某些 AWS 服務具有類似容器的資源群組，可自動為您建立資源，而標籤可以從一個服務中的資源傳播到另一個服務。例如，Amazon EC2 Auto Scaling 群組和 Amazon EMR 叢集上的標籤可自動傳播至包含的 Amazon EC2 執行個體。相較於 Auto Scaling 群組或 EMR 叢集，您對於 Amazon EC2 的標籤政策可能更嚴格。如果您啟用強制，標籤政策會防止標記資源，還可能禁止動態擴展和佈建。

下列各節說明如何尋找不符合規資源，並將其修正為合規。

搜尋帳戶的不合規資源

針對每個帳戶，您可以取得不合規資源的相關資訊。您應該從帳戶資源所在的每個區域執行此命令。

若要針對使用標籤政策的帳戶尋找不合規資源，您可以在登入帳戶時執行下列命令，並將結果儲存為檔案：

```
$ aws resourcegroupstaggingapi get-resources  --region us-east-1 \
    --include-compliance-details \
    --exclude-compliant-resources > outputfile.txt
```

更正資源中的不合規標籤

找到不合規標籤後，請使用下列任何方法來更正。您登入的帳戶中，資源必須有不合規標籤：

- 對建立不合規資源的 AWS 服務，使用該服務的主控台或標記 API 操作。
- 使用 AWS Resource Groups TagResources 和 UntagResources 操作，以新增符合有效政策的標籤，或移除不合規標籤。

搜尋並更正其他不合規問題

尋找和更正合規問題是反覆的程序。重複上述兩節中的步驟，直至您關注的資源符合標籤政策。

產生組織整體合規報告

您隨時可以產生報告，以列出整個組織的 AWS 帳戶 中所有已標記的資源。此報告顯示每個資源是否符合有效標籤政策。請注意，您對標籤政策或資源所做的變更，可能需要經過長達 48 小時，才會反映在組織整體合規報告中。例如，假設您有一個標籤政策為某個資源類型定義新的標準化標籤。如果該類型的資源沒有此標籤，則在報告中會顯示為合規，時間長達 48 小時。

只要組織的管理帳戶具有 Amazon S3 儲存貯體的存取權，您可以在 us-east-1 區域中從該帳戶產生報告。儲存貯體必須具有連接的儲存貯體政策，如用於存放報告的 Amazon S3 儲存貯體政策中所示。若要產生報告，請執行下列命令：

```
$ aws resourcegroupstaggingapi get-compliance-summary --region us-east-1
{
    "SummaryList": [
        {
            "LastUpdated": "2020-06-09T18:40:46Z",
            "NonCompliantResources": 0
        }
    ]
}
```

您每次可以產生一個報告。

此報告可能需要一些時間才能完成。您可以執行下列命令來檢查狀態：

```
$ aws resourcegroupstaggingapi describe-report-creation --region us-east-1
{
    "Status": "SUCCEEDED"
}
```

當上述命令傳回 SUCCEEDED 時，您可以從 Amazon S3 儲存貯體開啟報告。

支援強制執行的服務和資源類型

下列服務和資源類型支援強制符合標籤政策功能：

服務名稱	資源類型	JSON 語法
Amazon API Gateway	• API 金鑰 • 網域名稱	• "apigateway:apikeys" • "apigateway:domainnames"

服務名稱	資源類型	JSON 語法
	• REST API 操作 • 階段	• "apigateway:restapis" • "apigateway:restapis/stages"
AWS Amplify	• 元件 • 主題	• "amplifyuibuilder:app/environment/components" • "amplifyuibuilder:app/environment/themes"
AWS AppConfig	• 應用程式 • 組態設定檔 • 部署 • 部署策略 • 環境	• "appconfig:application" • "appconfig:application/configurationprofile" • "appconfig:application/environment/deployment" • "appconfig:deploymentstrategy" • "appconfig:application/environment"
AWS App Mesh	• 全部 • 閘道路由 • 網格 • 路由 • 虛擬閘道 • 虛擬節點 • 虛擬路由器 • 虛擬服務	• "appmesh:*" • "appmesh:mesh/virtualGateway/gatewayRoute" • "appmesh:mesh" • "appmesh:mesh/virtualRouter/route" • "appmesh:mesh/virtualGateway" • "appmesh:mesh/virtualNode" • "appmesh:mesh/virtualRouter" • "appmesh:mesh/virtualService"
Amazon Athena	• 全部 • 工作群組	• "athena:*" • "athena:workgroup"

服務名稱	資源類型	JSON 語法
AWS Audit Manager	• 評估 • 評定架構 • 控制項	• "auditmanager:assessment " • "auditmanager:assessmentFramework " • "auditmanager:control "
AWS Backup	• 備份計劃 • 保存庫 • 閘道 • Hypervisor • VM	• "backup:backup-plan" • "backup:backup-vault" • "backup-gateway:gateway" • "backup-gateway:hypervisor" • "backup-gateway:vm"
AWS Batch	• 任務 • 任務定義 • 任務佇列	• "batch:job" • "batch:job-definition" • "batch:job-queue"
AWS BugBust	• 事件	• "bugbust:event"
AWS Certificate Manager	• 全部 • 憑證 • Private certificate authority	• "acm:*" • "acm:certificate" • "acm-pca:certificate-authority"
Amazon Chime	• 應用程式執行個體 • 頻道 • 媒體管道 • 會議 • SIP 媒體應用程式 • 使用者應用程式執行個體 • 語音連接器	• "chime:app-instance" • "chime:app-instance/channel" • "chime:media-pipeline" • "chime:meeting" • "chime:sma" • "chime:app-instance/user" • "chime:vc"

服務名稱	資源類型	JSON 語法
AWS Clean Rooms	• 協作 • 設定的資料表 • 成員資格 • 設定的資料表關聯	• "cleanrooms:collaboration" • "cleanrooms:configuredtable" • "cleanrooms:membership" • "cleanrooms:membership/configuredtableassociation"
AWS Cloud9	• 環境	• "cloud9:environment"
Amazon CloudFront	• 全部 • 發佈 • 串流分發	• "cloudfront:*" • "cloudfront:distribution" • "cloudfront:streaming-distribution"
AWS CloudTrail	• 全部 • 追蹤	• "cloudtrail:*" • "cloudtrail:trail"
Amazon CloudWatch	• 全部 • 警示 • Contributor Insights 規則 • 指標串流	• "cloudwatch:*" • "cloudwatch:alarm" • "cloudwatch:insight-rule" • "cloudwatch:metric-stream"
Amazon CloudWatch 網絡監控	• 監控	• "internetmonitor:monitor"
Amazon CloudWatch 日誌	• 日誌群組	• "logs:log-group"
Amazon CloudWatch 觀測訪問管理器	• 連結 • 接收	• "oam:link" • "oam:sink"
AWS CodeBuild	• 全部 • 專案	• "codebuild:*" • "codebuild:project"

服務名稱	資源類型	JSON 語法
Amazon CodeCatalyst	• 連線	• "codecatalyst:connections"
AWS CodeCommit	• 全部 • 儲存庫	• "codecommit:*" • "codecommit:repository"
AWS CodePipeline	• 全部 • 動作類型 • 管道 • Webhook	• "codepipeline:*" • "codepipeline:actiontype" • "codepipeline:pipeline" • "codepipeline:webhook"
Amazon Cognito 身分	• 全部 • 身分集區	• "cognito-identity:*" • "cognito-identity:identitypool"
Amazon Cognito 使用者集區	• 全部 • 使用者集區	• "cognito-idp:*" • "cognito-idp:userpool"
Amazon Comprehend	• 全部 • 文件分類器 • 實體辨識器	• "comprehend:*" • "comprehend:document-classifier" • "comprehend:entity-recognizer"
AWS Config	• 全部 • 彙整授權 • Config 彙整工具 • Config 規則	• "config:*" • "config:aggregation-authorization" • "config:config-aggregator" • "config:config-rule"
Amazon 評論 CodeGuru 家	• 關聯	• "codeguru-reviewer:association"
Amazon CodeGuru 安全	• Scan	• "codeguru-security:scans"

服務名稱	資源類型	JSON 語法
CodeConnections	• 連線 • 主機	• "codestar-connections:connection" • "codestar-connections:host"
Amazon Connect	• 聯絡流程 • 整合關聯 • 佇列 • Quick Connect • 轉接設定檔 • 使用者	• "connect:instance/contact-flow" • "connect:instance/integration-association" • "connect:instance/queue" • "connect:instance/transfer-destination" • "connect:instance/routing-profile" • "connect:instance/agent"
Amazon Connect Wisdom	• 助理 • 關聯 • 內容 • 知識庫 • Session (工作階段)	• "wisdom:assistant" • "wisdom:association" • "wisdom:content" • "wisdom:knowledge-base" • "wisdom:session"
AWS Database Migration Service	• 全部 • 端點 • ES • Rep • Subgrp • 任務	• "dms:*" • "dms:endpoint" • "dms:es" • "dms:rep" • "dms:subgrp" • "dms:task"
Amazon Data Lifecycle Manager	• 政策	• "dlm:policy"

服務名稱	資源類型	JSON 語法
AWS Direct Connect	• 全部 • Dxcon • Dxlag • Dxvif	• `"directconnect:*"` • `"directconnect:dxcon"` • `"directconnect:dxlag"` • `"directconnect:dxvif"`
Amazon DynamoDB	• 全部 • 資料表	• `"dynamodb:*"` • `"dynamodb:table"`

服務名稱	資源類型	JSON 語法
Amazon EC2	• 容量保留 • 用戶端 VPN 端點 • 客戶閘道 • DHCP 選項 • 彈性 IP • 機群 • FPGA Image • 主機保留 • 映像 • 執行個體 • 網際網路閘道 • 啟動範本 • NAT 閘道 • 網路 ACL • 網路介面 • 預留執行個體 • 路由表 • 安全群組 • 快照 • Spot 執行個體請求 • 子網路 • 流量鏡像篩選條件 • 流量鏡像工作階段 • 流量鏡像目標 • 資料量 • VPC • VPC 端點 • VPC 端點服務 • VPC 對等連線	• `"ec2:capacity-reservation"` • `"ec2:client-vpn-endpoint"` • `"ec2:customer-gateway"` • `"ec2:dhcp-options"` • `"ec2:elastic-ip"` • `"ec2:fleet"` • `"ec2:fpga-image"` • `"ec2:host-reservation"` • `"ec2:image"` • `"ec2:instance"` • `"ec2:internet-gateway"` • `"ec2:launch-template"` • `"ec2:natgateway"` • `"ec2:network-acl"` • `"ec2:network-interface"` • `"ec2:reserved-instances"` • `"ec2:route-table"` • `"ec2:security-group"` • `"ec2:snapshot"` • `"ec2:spot-instances-request"` • `"ec2:subnet"` • `"ec2:traffic-mirror-filter"` • `"ec2:traffic-mirror-session"` • `"ec2:traffic-mirror-target"` • `"ec2:volume"` • `"ec2:vpc"` • `"ec2:vpc-endpoint"` • `"ec2:vpc-endpoint-service"` • `"ec2:vpc-peering-connection"`

服務名稱	資源類型	JSON 語法
	• VPN 連接 • VPN 閘道	• "ec2:vpn-connection" • "ec2:vpn-gateway"
Amazon EC2 資源回收筒	• 規則	• "rbin:rule"
Amazon Elastic Container Registry	• 儲存庫	• "ecr:repository"
AWS Elastic Beanstalk	• 應用程式 • 應用程式版本 • 組態範本 • 平台	• "elasticbeanstalk:application" • "elasticbeanstalk:applicationversion" • "elasticbeanstalk:configurationtemplate" • "elasticbeanstalk:platform"
Amazon Elastic Container Service	• 叢集 • 服務 • 任務集	• "ecs:cluster" • "ecs:service" • "ecs:task-set"
Amazon Elastic File System	• 全部 • 檔案系統	• "elasticfilesystem:*" • "elasticfilesystem:file-system"
Amazon Elastic Inference	• 加速器	• "elastic-inference:elastic-inference-accelerator"
Amazon Elastic Kubernetes Service	• 叢集	• "eks:cluster"
Amazon Elastic 搜尋	• 網域	• "es:domain"
Amazon EMR	• 叢集 • 編輯器	• "elasticmapreduce:cluster" • "elasticmapreduce:editor"

服務名稱	資源類型	JSON 語法
Amazon EMR Serverless	• 應用程式	• "emr-serverless:applications"
AWS 實體解析度	• 匹配流程 • 結構描述映射	• "entityresolution:matchingworkflow" • "entityresolution:schemamapping"
Amazon ElastiCache	• 叢集	• "elasticache:cluster"
Amazon EventBridge	• 全部 • 事件匯流排 • 規則	• "events:*" • "events:event-bus" • "events:rule"
Amazon EventBridge 管道	• 管道	• "pipes:pipe"
Amazon EventBridge 排程	• 排程群組	• "scheduler:schedule-group"
Amazon Fraud Detector	• 偵測器 • 偵測器版本 • 模型 • 規則 • 變數	• "frauddetector:detector" • "frauddetector:detector-version" • "frauddetector:model" • "frauddetector:rule" • "frauddetector:variable"
Amazon Global Accelerator	• 加速器	• "globalaccelerator:accelerator"
Elastic Load Balancing	• 全部 • 負載平衡器 • 目標群組	• "elasticloadbalancing:*" • "elasticloadbalancing:loadbalancer" • "elasticloadbalancing:targetgroup"

服務名稱	資源類型	JSON 語法
Amazon FSx	• 全部 • 備份 • 檔案系統	• "fsx:*" • "fsx:backup" • "fsx:file-system"
Amazon GuardDuty	• 偵測器 • 篩選條件 • IP 集合 • 威脅情資集合	• "guardduty:detector" • "guardduty:detector/filter" • "guardduty:detector/ipset" • "guardduty:detector/threatintelset"
AWS HealthLake	• 資料儲存	• "healthlake:datastore "
AWS HealthOmics	• 註解存放區 • 註解存放區版本 • 參考存放區 • 參考資料 • 執行 • 執行群組 • 序列存放區 • 讀取集合 • 變量存放區 • 工作流程	• "omics:annotationStore" • "omics:annotationStore/version" • "omics:referenceStore" • "omics:referenceStore/reference" • "omics:run" • "omics:runGroup" • "omics:sequenceStore" • "omics:sequenceStore/readSet" • "omics:variantStore" • "omics:workflow"
Amazon Inspector	• 篩選條件	• "inspector2:filter "

服務名稱	資源類型	JSON 語法
AWS Identity and Access Management	• 執行個體描述檔 • MFA • OIDC 供應商 • 政策 • SAML 供應商 • 伺服器憑證	• "iam:instance-profile" • "iam:mfa" • "iam:oidc-provider" • "iam:policy" • "iam:saml-provider" • "iam:server-certificate"
AWS IoT Analytics	• 全部 • 頻道 • 資料集 • 資料儲存 • 管道	• "iotanalytics:*" • "iotanalytics:channel" • "iotanalytics:dataset" • "iotanalytics:datastore" • "iotanalytics:pipeline"
AWS IoT Events	• 全部 • 偵測器模型 • 輸入	• "iotevents:*" • "iotevents:detectorModel" • "iotevents:input"
AWS IoT Fleet Hub	• 應用程式	• "iotfleethub:application"
AWS IoT SiteWise	• 資產 • 資產模型	• "iotsitewise:asset" • "iotsitewise:asset-model "

服務名稱	資源類型	JSON 語法
AWS IoT Greengrass	• 大量部署 • 連接器定義 • 核心定義 • 裝置定義 • 函數定義 • 記錄器定義 • 資源定義 • 訂閱定義	• "greengrass:bulk" • "greengrass:connectorsDefinition" • "greengrass:coresDefinition" • "greengrass:devicesDefinition" • "greengrass:functionsDefinition" • "greengrass:loggersDefinition" • "greengrass:resourcesDefinition" • "greengrass:subscriptionsDefinition"
AWS Key Management Service	• 全部 • 金鑰	• "kms:*" • "kms:key"
Amazon Kinesis	• 全部 • 應用程式	• "kinesisanalytics:*" • "kinesisanalytics:application"
Amazon 數據 Firehose	• 全部 • 交付串流	• "firehose:*" • "firehose:deliverystream"
AWS Lambda	• 全部 • 函式	• "lambda:*" • "lambda:function"
Amazon Macie	• 自訂資料識別碼	• "macie2:custom-data-identifier"
Amazon MediaStore	• 容器	• "mediastore:container"
Amazon MQ	• 代理程式 • 組態	• "mq:broker" • "mq:configuration"

服務名稱	資源類型	JSON 語法
Amazon Network Firewall	• 防火牆 • 防火牆政策 • 狀態規則群組 • 無狀態規則群組	• "network-firewall:firewall" • "network-firewall:firewall-policy" • "network-firewall:stateful-rulegroup" • "network-firewall:stateless-rulegroup"
Amazon OpenSearch 無服務器	• 收集	• "aoss:collection"
AWS Organizations	• 帳戶 • Organizational Unit (組織單位) • 政策 • 根帳戶	• "organizations:account" • "organizations:ou" • "organizations:policy" • "organizations:root"
Amazon Pinpoint SMS Voice V2	• 組態集合 • 選擇退出清單 • 電話號碼 • 集區 • 寄件者 Id	• "sms-voice:configuration-set" • "sms-voice:opt-out-list" • "sms-voice:phone-number" • "sms-voice:pool" • "sms-voice:sender-id"

服務名稱	資源類型	JSON 語法
Amazon RDS	• 叢集參數群組 • 叢集端點 • 事件訂閱 • 資料庫選項群組 • DB parameter group (資料庫參數群組) • 資料庫代理 • 資料庫代理端點 • 預留資料庫執行個體 • 資料庫安全群組 • DB subnet group (資料庫子網路群組) • 目標群組	• `"rds:cluster-pg"` • `"rds:cluster-endpoint"` • `"rds:es"` • `"rds:og"` • `"rds:pg"` • `"rds:db-proxy"` • `"rds:db-proxy-endpoint"` • `"rds:ri"` • `"rds:secgrp"` • `"rds:subgrp"` • `"rds:target-group"`
Amazon Redshift	• 全部 • 叢集 • 資料庫群組 • 資料庫名稱 • 資料庫使用者 • 事件訂閱 • HSM 用戶端憑證 • HSM 組態 • 參數群組 • 快照 • 快照複製授予 • 快照排程 • 子網路群組	• `"redshift:*"` • `"redshift:cluster"` • `"redshift:dbgroup"` • `"redshift:dbname"` • `"redshift:dbuser"` • `"redshift:eventsubscription"` • `"redshift:hsmclientcertificate"` • `"redshift:hsmconfiguration"` • `"redshift:parametergroup"` • `"redshift:snapshot"` • `"redshift:snapshotcopygrant"` • `"redshift:snapshotschedule"` • `"redshift:subnetgroup"`

服務名稱	資源類型	JSON 語法
Amazon Redshift Serverless	• 命名空間 • 工作群組	• "redshift-serverless:namespace" • "redshift-serverless:workgroup"
AWS Resource Access Manager	• 全部 • 資源共享	• "ram:*" • "ram:resource-share"
AWS Resource Groups	• 全部 • 群組	• "resource-groups:*" • "resource-groups:group"
Amazon Route 53	• 託管區域	• "route53:hostedzone"
Amazon Route 53 Resolver	• 全部 • 解析程式端點 • 解析程式規則	• "route53resolver:*" • "route53resolver:resolver-endpoint" • "route53resolver:resolver-rule"
Amazon S3	• 儲存貯體 • Storage Lens	• "s3:bucket" • "s3:storage-lens"

服務名稱	資源類型	JSON 語法
Amazon SageMaker	• App Image Config • Artifact • Context • 訓練工作 • 正在處理任務 • 模型套件群組 • 人力任務 UI • 模型套件 • 動作 • 管道 • 實驗 • 流程定義 • 專案	• "sagemaker:app-image-config" • "sagemaker:artifact" • "sagemaker:context" • "sagemaker:training-job" • "sagemaker:processing-job " • "sagemaker:model-package-group" • "sagemaker:human-task-ui" • "sagemaker:model-package" • "sagemaker:action" • "sagemaker:pipeline" • "sagemaker:experiment" • "sagemaker:flow-definition" • "sagemaker:project"
AWS Secrets Manager	• 全部 • 秘密	• "secretsmanager:*" • "secretsmanager:secret"
AWS 安全湖	• 資料湖 • Subscriber	• "securitylake:data-lake" • "securitylake:subscriber"
AWS Service Catalog	• 應用程式 • 屬性群組 • 產品組合 • 產品	• "servicecatalog:applications" • "servicecatalog:attribute-groups " • "catalog:portfolio " • "catalog:product "
Amazon Simple Notification Service (SNS)	• 主題	• "sns:topic"

服務名稱	資源類型	JSON 語法
Amazon Simple Queue Service (SQS)	• 佇列	• `"sqs:queue"`
Amazon States Language	• 全部 • 活動 • State Machine (狀態機器)	• `"states:*"` • `"states:activity "` • `"states:stateMachine  "`
AWS Step Functions	• 活動	• `"states:activity"`
AWS Storage Gateway	• 全部 • 閘道 • Share (分享) • 磁帶 • 資料量	• `"storagegateway:*"` • `"storagegateway:gateway"` • `"storagegateway:share"` • `"storagegateway:tape"` • `"storagegateway:gateway/volume"`
AWS Systems Manager	• 關聯 • 自動化執行 • 文件 • 維護時段 • 受管的執行個體 • Ops 項目 • 修補基準 • Session (工作階段) • 聯絡人	• `"ssm:association"` • `"ssm:automation-execution"` • `"ssm:document"` • `"ssm:maintenancewindow"` • `"ssm:managed-instance"` • `"ssm:opsitem"` • `"ssm:patchbaseline"` • `"ssm:session"` • `"ssm-contacts:contact"`
AWS Transfer Family	• Server • 使用者 • 工作流程	• `"transfer:server"` • `"transfer:user"` • `"transfer:workflow"`
Amazon Well-Architected	• 工作負載	• `"wellarchitected:workload"`

服務名稱	資源類型	JSON 語法
AWS Wickr	• 網路	• "wickr:network"
Amazon WorkSpaces	• 全部 • 目錄 • WorkSpace • WorkSpaces 捆綁 • WorkSpaces 形象 • WorkSpaces IP 群組	• "workspaces:*" • "workspaces:directory" • "workspaces:workspace" • "workspaces:workspacebundle" • "workspaces:workspaceimage" • "workspaces:workspaceipgroup"
Amazon WorkLink	• 機群	• "worklink:fleet"

標籤政策語法和範例

此頁面說明標籤政策語法並提供範例。

標籤政策語法

標籤政策是根據 JSON 規則建構的純文字檔。標籤政策的語法遵循管理政策類型的語法。如需該語法的完整討論，請參閱理解管理政策繼承。本主題著重於以該一般語法滿足標籤政策類型的特定需求。

下列標籤政策顯示基本的標籤政策語法：

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "100",
                    "200"
                ]
            },
            "enforced_for": {
                "@@assign": [
                    "secretsmanager:*"
```

```
                ]
            }
        }
    }
}
```

標籤政策語法包括下列元件：

- tags 欄索引鍵名稱。標籤政策一律以此固定索引鍵名稱開頭。這是上面範例政策的第一行。
- 唯一識別政策陳述式的政策索引鍵。必須符合「標籤鍵」的值 (大小寫處理除外)。與標籤鍵 (於下方說明) 不同，政策值不區分大小寫。

  在此範例中，costcenter 是政策索引鍵。
- 至少有一個標籤鍵，指定允許的標籤鍵含有您希望資源符合的大寫。如果沒有定義大小寫處理，則小寫為標籤鍵的預設大小寫處理。標籤鍵的值必須符合政策鍵的值。但由於政策索引鍵值不區分大小寫，大寫可能有所不同。

  在此範例中，CostCenter 是標籤鍵。這是符合標籤政策規範的大小寫處理。此標籤鍵具有替代大小寫處理的資源，不符合標籤政策規範。

  您可以在標籤政策中定義多個標籤鍵。
- (選用) 標籤鍵可接受的一或多個標籤值的清單。如果標籤政策未指定標籤鍵的標籤值，則任何值 (包括完全沒有值) 都視為合規。

  在此範例中，CostCenter 標籤鍵的可接受值為 100 和 200。
- (選用) enforced_for 選項，指出是否防止對指定的服務和資源執行任何不合規的標記操作。在主控台，這是視覺化編輯器中用於建立標籤政策的 Prevent noncompliant operations for this tag (防止對此標籤執行不合規操作) 選項。此選項的預設設定為 null。

  範例標籤政策指定所有 AWS Secrets Manager 資源都必須具有此標籤。

  > **Warning**
  >
  > 只有在您使用標籤政策很有經驗時，才應該變更此選項的預設值。否則，可能會使組織帳戶中的使用者無法建立他們所需的資源。

- 運算子，指定標籤政策如何與組織樹狀結構中的其他標籤政策合併，以建立帳戶的有效的標籤政策。此範例中使用 @@assign，將字串指定給 tag_key、tag_value 和 enforced_for。如需運算子的詳細資訊，請參閱繼承運算子。

- – 您可以在標籤值和 enforced_for 欄位中使用 * 萬用字元：
  - 每個標籤值中只能使用一個萬用字元。例如，允許 *@example.com，但不允許 *@*.com。
  - 對於 enforced_for，您可以對某些服務搭配使用 <service>:*，以對該服務的所有資源啟用強制執行。如需支援 enforced_for 的服務和資源類型清單，請參閱支援強制執行的服務和資源類型。

    萬用字元無法用來指定所有服務，也無法用來指定所有服務的某些資源。

標籤政策範例

接下來的範例標籤政策僅供參考。

> **Note**
>
> 在您嘗試在組織中使用這些範例標籤政策之前，請注意下列事項：
>
> - 請確定您已按照建議的工作流程開始使用標籤政策。
> - 您應該仔細檢閱和自訂這些標籤政策，以滿足您的獨特需求。
> - 標籤政策中的所有字元都受制於大小上限。本指南中的範例添加額外空格來顯示標籤政策，以改善可讀性。不過，如果政策大小接近大小上限，為了節省空間，您可以刪除任何空格。空白字元的例子包括引號外面的空格字元和換行符號。
> - 未標記的資源由於不合規而無法出現在結果中。

範例 1：定義整個組織的標籤鍵大小寫

下列範例顯示的標籤政策只定義兩個標籤鍵，以及您希望組織中的帳戶標準化所依據的大小寫。

政策 A – 組織根標籤政策

```
{
    "tags": {
        "CostCenter": {
            "tag_key": {
                "@@assign": "CostCenter",
                "@@operators_allowed_for_child_policies": ["@@none"]
            }
        },
        "Project": {
```

```
            "tag_key": {
                "@@assign": "Project",
                "@@operators_allowed_for_child_policies": ["@@none"]
            }
        }
    }
}
```

此標籤政策定義兩個標籤鍵：CostCenter 和 Project。將此標籤政策連接至組織根，會產生下列影響：

- 組織中的所有帳戶都會繼承此標籤政策。
- 組織中所有帳戶都必須使用已定義的大小寫處理以符合規範。具有 CostCenter 和 Project 標籤的資源符合規範。標籤鍵具有替代大小寫處理的資源 (例如 costcenter、Costcenter 或 COSTCENTER) 不符合規範。
- @@operators_allowed_for_child_policies": ["@@none"] 行會封鎖標籤鍵。在組織樹狀結構中較下方連接的標籤政策 (子政策)，不能使用值-設定運算子來變更標籤鍵 (包括其大小寫處理)。
- 與所有標籤政策一樣，對於未標記的資源或標籤政策中未定義的標籤，不會評估是否符合標籤政策規範。

在針對您要使用的標籤鍵建立類似的標籤政策時，AWS 建議使用此範例當作指南。將此標籤政策連接至組織根目錄。然後，建立類似於下一個範例的標籤政策，只為已定義的標籤鍵定義可接受的值。

下一步：定義值

假設您已將先前的標籤政策連接至組織根。接下來，您可以建立如下所示的標籤政策，並連接至帳戶。此政策定義 CostCenter 和 Project 標籤鍵可接受的值。

政策 B – 帳戶標籤政策

```
{
    "tags": {
        "CostCenter": {
            "tag_value": {
                "@@assign": [
                    "Production",
                    "Test"
                ]
```

```
            }
        },
        "Project": {
            "tag_value": {
                "@@assign": [
                    "A",
                    "B"
                ]
            }
        }
    }
}
```

如果您將政策 A 連接至組織根，將政策 B 連接至帳戶，則這些政策合併起來，為帳戶建立下列有效的標籤政策：

政策 A + 政策 B = 帳戶的有效標籤政策

```
{
    "tags": {
        "Project": {
            "tag_value": [
                "A",
                "B"
            ],
            "tag_key": "Project"
        },
        "CostCenter": {
            "tag_value": [
                "Production",
                "Test"
            ],
            "tag_key": "CostCenter"
        }
    }
}
```

如需政策繼承的詳細資訊，包括繼承運算子如何運作的範例，以及有效標籤政策的範例，請參閱理解管理政策繼承。

範例 2：禁止使用標籤鍵

若要禁止使用標籤鍵，您可以將如下所示的標籤政策連接至組織實體。

此範例政策指定 Color 標籤鍵不接受任何值。也會指定在子標籤政策中不允許運算子。因此，在受影響帳號中，資源上的任何 Color 標籤都會被系統視為不相容。然而，enforced_for 選項實際上會阻止受影響帳戶僅標記使用 Color 標籤的 Amazon DynamoDB 資料表。

```
{
    "tags": {
        "Color": {
            "tag_key": {
                "@@operators_allowed_for_child_policies": [
                    "@@none"
                ],
                "@@assign": "Color"
            },
            "tag_value": {
                "@@operators_allowed_for_child_policies": [
                    "@@none"
                ],
                "@@assign": []
            },
            "enforced_for": {
                "@@assign": [
                    "dynamodb:table"
                ]
            }
        }
    }
}
```

支援地區

下列區域可使用標籤政策功能：

區域名稱	區域參數
美國東部 (維吉尼亞北部) 區域[1]	**us-east-1**
美國東部 (俄亥俄) 區域	us-east-2
美國西部 (加利佛尼亞北部) 區域	us-west-1
美國西部 (奧勒岡) 區域	us-west-2

區域名稱	區域參數
非洲 (開普敦) 區域[2]	af-south-1
亞太區域 (香港) 區域[2]	ap-east-1
亞太 (孟買) 區域	ap-south-1
亞太區域 (海德拉巴) [2]	ap-south-2
亞太區域 (東京) 區域	ap-northeast-1
亞太區域 (首爾) 區域	ap-northeast-2
亞太 (大阪) 區域	ap-northeast-3
亞太區域 (新加坡) 區域	ap-southeast-1
亞太區域 (雪梨) 區域	ap-southeast-2
亞太 (雅加達) 區域 [2]	ap-southeast-3
亞太區域 (墨爾本) [2]	ap-southeast-4
加拿大西部 (卡加利) [2]	ca-west-1
加拿大 (中部) 區域	ca-central-1
歐洲 (法蘭克福) 區域	eu-central-1
歐洲 (蘇黎世) 地區 [2]	eu-central-2
歐洲 (米蘭) 區域[2]	eu-south-1
歐洲 (西班牙) [2]	eu-south-2
歐洲 (愛爾蘭) 區域	eu-west-1
歐洲 (倫敦) 區域	eu-west-2
歐洲 (巴黎) 區域	eu-west-3

區域名稱	區域參數
歐洲 (斯德哥爾摩) 區域	eu-north-1
中東 (阿拉伯聯合大公國) [2]	me-central-1
中東 (巴林) 區域[2]	me-south-1
南美洲 (聖保羅) 區域	sa-east-1
以色列 (特拉維夫) [2]	il-central-1

[1]呼叫下列 Organizations 操作時，您必須指定 **us-east-1** 區域：

- DeletePolicy
- DisablePolicyType
- EnablePolicyType
- 組織根目錄上的任何其他作業，例如 ListRoots.

呼叫下列 Resource Groups 標記 API 操作時 (標籤政策功能的一部分)，您也必須指定 **us-east-1** 區域：

- DescribeReportCreation
- GetComplianceSummary
- GetResources
- StartReportCreation

> **Note**
>
> 若要評估整個組織是否符合標籤政策，您還必須具有美國東部 (維吉尼亞北部) 區域中 Amazon S3 儲存貯體的存取權以便儲存報告。如需詳細資訊，請參閱標記 AWS 資源使用者指南中的報告儲存的 Amazon S3 儲存貯體政策。

[2]必須手動啟用這些區域。若要深入瞭解如何啟用和停用 AWS 區域，請參閱《帳戶管理參考指南》中的「指定 AWS 區域 您的AWS 帳戶可以使用的項目」。在這些區域中無法使用 Resource Groups 主控台。

服務控制政策 (SCP)

服務控制政策 (SCP) 是一種組織政策類型，可用來管理您的組織中的許可。SCP 可集中控制組織中 IAM 使用者和 IAM 角色的最大可用許可。SCP 可協助您確保您的帳戶符合組織的存取控制指導方針。SCP 只有在啟用所有功能的組織中才能使用。若您的組織只啟用了合併帳單功能，便無法使用 SCP。如需啟用 SCP 的說明，請參閱 啟用和停用政策類型。

SCP 不會將許可授予組織中的 IAM 使用者和 IAM 角色。SCP 沒有授予與任何許可。SCP 會針對您組織中的 IAM 使用者和 IAM 角色可執行的動作，定義權限保護或設定限制。若要授予許可，管理員必須附加政策以控制存取權限，例如附加到 IAM 使用者和 IAM 角色的身分型政策，以及附加至帳戶中資源的資源型政策。有效權限是 SCP 允許的項目與身分識別和以資源為基礎的原則所允許的項目之間的邏輯交集。

> **Important**
>
> SCP 不會影響管理帳戶中的使用者或角色。它們只會影響組織中的成員帳戶。

本頁主題

測試 SCP 的效果

AWS 強烈建議您不要在未徹底測試政策對帳戶的影響之前，將 SCP 附加到組織的根目錄。而是建立一個 OU，讓您一次將一個帳戶 (或至少為少量帳戶) 移至其中，確保您不會不慎將使用者鎖在重要服務之外。判斷服務是否正由帳戶使用的其中一種方法是檢查 IAM 中上次存取資料的服務。另一種方法是使 AWS CloudTrail 用在 API 級別記錄服務使用情況。

> **Note**
>
> 您不應移除「完整」AWSAccess 策略，除非您使用允許的動作將其修改或取代為單獨的策略，否則來自成員帳號的所有 AWS 動作都將失敗。

SCP 的大小上限

您 SCP 中所有的字元都會計入其大小上限。本指南中範例顯示的 SCP 格式具有額外的空格，以改善其可讀性。不過，若您的政策大小接近大小上限，為了節省空間，您可以刪除引號外部的任何空格，例如空格字元和換行字元。

> **Tip**
>
> 使用視覺化編輯器建置您的 SCP。它會自動移除額外空格。

將 SCP 連接至組織中的不同層級

如需 SCP 運作方式的詳細說明，請參閱 SCP 評估。

SCP 對許可的影響

SCP 與 AWS Identity and Access Management (IAM) 權限政策類似，且使用幾乎相同的語法。但是，SCP 永遠不會授予許可。SCP 是 JSON 政策，可為組織中的 IAM 使用者和 IAM 角色指定最大許可。如需詳細資訊，請參閱 IAM 使用者指南中的政策評估邏輯。

- SCP 只會影響由屬於組織一部分的帳戶管理的 IAM 使用者和角色。SCP 不會直接影響資源型政策。也不會影響來自組織外部帳戶的使用者或角色。例如，假設組織中的帳戶 A 擁有一個 Amazon S3 儲存貯體。儲存貯體政策 (資源型政策) 會授予來自組織外部帳戶 B 的使用者存取。帳戶 A 有連接一個 SCP。SCP 不會套用至帳戶 B 中的外部使用者。SCP 僅會套用至組織中帳戶 A 管理的使用者。

- SCP 會限制 IAM 使用者和成員帳戶中 IAM 使用者和角色的許可，包括成員帳戶的根使用者。任何帳戶只會擁有其上「每個」父系允許的許可。如果帳戶上方的任何層級封鎖了許可，無論是隱含 (不包含在 `Allow` 政策陳述式中) 或是明確 (包含在 `Deny` 政策陳述式中)，受影響的帳戶中的使用者或角色都將無法使用該許可，即使帳戶管理員將具備 */* 許可的 `AdministratorAccess` IAM 政策連接到使用者也一樣。
- SCP 僅影響組織中的成員帳戶。它們對管理帳戶中的使用者或角色沒有影響。
- 使用者和角色仍必須使用適當的 IAM 許可政策授予許可。沒有任何 IAM 許可政策的使用者將不具備存取權，即使適用的 SCP 允許所有服務和動作。
- 如果使用者或角色擁有的 IAM 許可政策，會授予存取適用 SCP 也允許的動作，使用者或角色即可執行該動作。
- 如果使用者或角色擁有的 IAM 許可政策，會授予存取權給適用的 SCP 不允許或明確拒絕的動作，使用者或角色即無法執行該動作。
- SCP 會影響連接的帳戶中的所有使用者和角色，包括根帳戶使用者。唯一的例外狀況，詳述於 任務和實體不受 SCP 的限制。
- SCP 不會影響任何服務連結角色。服務連結角色可讓其他 AWS 服務與 SCP 整合， AWS Organizations 且不受 SCP 限制。
- 當您停用根目錄中的 SCP 原則類型時，所有 SCP 都會自動從該根目錄中的所有 AWS Organizations 實體中斷連結。 AWS Organizations 實體包括組織單位、組織和帳戶。如果您在根帳戶重新啟用 SCP，該根帳戶只會還原為根帳戶中自動連接到所有實體的預設 `FullAWSAccess` 政策。停用 SCP 之前對 AWS Organizations 實體的任何 SCP 連接都會遺失，並且無法自動復原，雖然您可以手動重新連接他們。
- 若許可邊界 (進階 IAM 功能) 和 SCP 同時存在，則邊界、SCP 和身分類型政策必須全部允許動作。

使用存取資料來改進 SCP

使用管理帳戶登入資料登入後，您可以在 IAM 主控台的AWS Organizations區段中檢視 AWS Organizations 實體或政策上次存取的服務資料。您也可以在 IAM 中使用 AWS Command Line Interface (AWS CLI) 或 AWS API 擷取上次存取的服務資料。此資料包括有關 AWS Organizations 帳戶中 IAM 使用者和角色最後嘗試存取哪些服務以及何時允許存取的服務的資訊。您可以使用此資訊來找出未使用的許可，以便微調您的 SCP，使其更完善地遵循最低權限的原則。

例如，您可能有一個禁止存取三個 AWS 服務的拒絕清單 SCP。未列在 SCP `Deny` 陳述式中的所有服務都可獲允。IAM 中最後存取的服務資料會告訴您 SCP 允許哪些 AWS 服務，但從未使用過。有了該資訊，您可以更新 SCP 以拒絕存取您不需要的服務。

如需詳細資訊，請參閱《IAM 使用者指南》中的以下主題：

- 檢視 Organizations 的 Organizations 服務上次存取資料
- 使用資料來調整組織單位的許可

任務和實體不受 SCP 的限制

您無法使用 SCP 限制下列任務：

- 管理帳戶執行的任何動作
- 任何使用連接到服務連結角色之許可所執行的動作
- 以根帳戶使用者身分註冊企業支援計劃
- 以 root 使用者身分變更 AWS 支援層級
- 為 CloudFront 私人內容提供受信任的簽署者功能
- 以根使用者身分為 Amazon Lightsail 電子郵件伺服器和 Amazon EC2 執行個體設定反向 DNS
- 部分 AWS相關服務的工作：
  - Alexa Top Sites
  - Alexa Web Information Service
  - Amazon Mechanical Turk
  - Amazon 產品行銷 API

建立、更新和刪除服務控制政策

登入您組織的管理帳戶時，您可以建立及更新服務控制政策 (SCP)。您可以透過建置陳述式，拒絕或允許存取您指定的服務和動作，來建立 SCP。

適用於 SCP 的預設組態使用「封鎖清單」策略，其中隱含允許所有動作，但要透過建立拒絕存取的陳述式來封鎖的那些動作除外。使用拒絕陳述式，您可以為陳述式指定資源和條件，並使用 NotAction 元素。用於允許陳述式時，您只能指定服務和動作。如需拒絕存取權及允許存取權的陳述式詳細資訊，請參閱 SCP 評估。

> **Tip**
>
> 您可以使用IAM中服務上次存取的資料作為更新 SCP 的資料點，以限制僅存取您所需的 AWS 服務。如需詳細資訊，請參閱 IAM 使用者指南中的檢視 Organizations 的 Organizations 服務上次存取資料。

在本主題中：

- 對組織啟用服務控制政策後，您就可以建立政策。
- 當 SCP 需求變更時，您可以更新現有的政策。
- 如果您不再需要某項政策，則將該政策從所有 OU 和帳戶中分離後，即可刪除政策。

建立 SCP

> **最低許可**
>
> 若要建立 SCP，您需要具有執行下列動作的許可：
>
> - `organizations:CreatePolicy`

AWS Management Console

建立服務控制政策

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Service control policies (服務控制政策) 頁面上，選擇 Create policy (建立政策)。
3. 在 Create policy (建立政策) 頁面上，輸入政策的 Policy name (政策名稱) 與選用的 Policy description (政策描述)。
4. (選用) 選擇 Add tag (新增標籤)，然後輸入一個鍵和一個選用值，來新增一個或多個標籤。將值留空會將其設定為空白字串；而不是 null。您可以在政策中連接最多 50 個標籤。如需更多詳細資訊，請參閱 標記 AWS Organizations 資源。

   > **Note**
   >
   > 在接下來的大部分步驟中，我們會討論使用 JSON 編輯器右側的控制項，逐元素建構政策。或者，您可以隨時在視窗左側的 JSON 編輯器中輸入文字。您可以直接輸入，或者可以使用複製和貼上。

5. 若要建置政策，您的下一個步驟會因您是否希望新增陳述式，拒絕或允許存取而有所不同。如需更多詳細資訊，請參閱 SCP 評估。您可以使用 Deny 陳述式，您可以擁有額外的控制，因

為您可以限制存取特定資源、定義 SCP 生效的條件，以及使用 NotAction 元素。如需語法的詳細資訊，請參閱SCP 語法。

新增「拒絕」存取的陳述式：

a. 在編輯器右側的 Edit statement (編輯陳述式) 窗格的 Add actions (新增動作) 下，選擇 AWS 服務。

   在您選擇右側的選項時，JSON 編輯器會隨即更新，在左側顯示相應的 JSON 政策。

b. 選取服務之後，包含該服務可用動作的清單即會開啟。您可以選擇 All actions (所有動作)，或選擇您要拒絕的一個或多個個別動作。

   左側的 JSON 會隨即更新，以包含您選取的動作。

   > **Note**
   >
   > 如果您選取個別動作，然後返回上一步並選取 All actions (所有動作)，*servicename*/* 的預期項目會新增至 JSON，但您之前選取的個別動作會留在 JSON 中，而不會移除。

c. 如果您想要從其他服務新增動作，可以選擇 Statement (陳述式) 方塊頂部的 All Services (所有服務)，然後視需要重複之前的兩個步驟。

d. 指定要包含在陳述式中的資源。

   - 在 Add a resource (新增資源) 旁邊，選擇 Add (新增)。
   - 在 Add resource (新增資源) 對話方塊，從清單中選擇您要控制其資源的服務。您只能從在上一步選擇的服務中進行選擇。
   - 在 Resource Type (資源類型)下，選擇您要控制的資源類型。
   - 最後，完成 Resource ARN (資源 ARN) 中的 Amazon 資源名稱 (ARN)，以識別您要控制存取的特定資源。您必須取代由大括號 {} 包圍的所有預留位置。您可以指定資源類型的 ARN 語法允許的萬用字元 (*) 。如需有關可以在何處使用萬用字元的資訊，請參閱文件以取得特定資源類型。
   - 選擇 Add resource (新增資源)，以儲存您對政策的新增。JSON 中的 `Resource` 元素會反映您的新增或變更。資源元素為必要項目。

> **Tip**
>
> 如果您想要為所選取的服務指定所有資源，請選擇 All resources (所有資源) 選項，或 JSON 中直接編輯 `Resource` 語句來讀取 `"Resource":"*"`。

e. (選用) 若要指定在政策陳述式生效時限制的條件，請在 Add a resource (新增資源) 旁邊，選擇 Add (新增)。

- 條件索引鍵 – 從清單中，您可以選擇任何適用於所有 AWS 服務 (例如，`aws:SourceIp`) 的任何條件索引鍵，或僅用於您為此陳述式選取的其中一項服務的服務特定索引鍵。
- 限定詞 – (選用) 若您為條件提供多個值 (取決於指定的條件索引鍵)，可以指定一個限定詞，針對值來測試請求。
  - 預設值 – 針對政策中的條件索引鍵值，測試請求中的單一值。如果請求中的值符合政策中的值，則條件會傳回 true。如果政策指定多個值，則會將其視為「或」測試，如果請求值符合任何政策值，則條件會傳回 true。
  - 對於請求中的任意值 – 當請求可以有多個值時，此選項會測試是否至少一個請求值符合政策中至少其中一個條件索引鍵值。如果請求中任一鍵值符合政策中的任一條件值，則條件會傳回 true。如果沒有相符金鑰或為 null 資料集，則條件會傳回 false。
  - 對於請求中的所有值 – 當請求可以有多個值時，此選項會測試是否每一個請求值均符合政策中的條件索引鍵值。如果請求中每個索引鍵值至少符合政策中的一個值，則條件會傳回 true。如果請求中沒有索引鍵，或索引鍵值解析為 null 資料集 (例如空白字串)，則也會傳回 true。
- 運算子 – 運算子指定要進行的比較類型。顯示的選項取決於條件索引鍵的資料類型。例如，`aws:CurrentTime` 全域條件索引鍵可讓您從任何日期比較運算子中選擇，或 `Null`，您可以用於測試該值是否存在於請求中。

  針對除 `Null` 測試之外的任何條件運算子，您可以選擇 IfExists 選項。
- 數值 – (選用) 指定您要測試請求的一個或多個值。

選擇新增條件。

如需有關條件索引鍵的詳細資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：條件。

f. (選用) 若要使用 NotAction 元素拒絕存取除指定動作之外的所有動作，請在左側窗格中，將 "Effect": "Deny", 元素之後的 Action 替換為 NotAction。如需詳細資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：NotAction。

6. 新增「允許」存取的陳述式：

a. 在左側的 JSON 編輯器中，將行 "Effect": "Deny" 變更為 "Effect": "Allow"。

在您選擇右側的選項時，JSON 編輯器會隨即更新，在左側顯示相應的 JSON 政策。

b. 選取服務之後，包含該服務可用動作的清單即會開啟。您可以選擇 All actions (所有動作)，或選擇您要允許的一個或多個個別動作。

左側的 JSON 會隨即更新，以包含您選取的動作。

> **Note**
>
> 如果您選取個別動作，然後返回上一步並選取 All actions (所有動作)，*servicename*/* 的預期項目會新增至 JSON，但您之前選取的個別動作會留在 JSON 中，而不會移除。

c. 如果您想要從其他服務新增動作，可以選擇 Statement (陳述式) 方塊頂部的 All Services (所有服務)，然後視需要重複之前的兩個步驟。

7. (選用) 若要將另一個陳述式新增到政策，請選擇 Add statement (新增陳述式) 並使用視覺編輯器來建置下一個陳述式。

8. 當您完成新增陳述式後，請選擇 Create policy (建立政策) 來儲存完成的 SCP。

您的新 SCP 會出現在組織的政策清單中。您現在可以將 SCP 連接至根、OU 或帳戶。

AWS CLI & AWS SDKs

建立服務控制政策

您可以使用下列其中一項命令來建立 SCP：

- AWS CLI: create-policy

以下範例假設您已有名稱為 Deny-IAM.json 的檔案，且包含 JSON 政策文字。它會使用該檔案來建立新的服務控制政策。

```
$ aws organizations create-policy \
```

```
    --content file://Deny-IAM.json \
    --description "Deny all IAM actions" \
    --name DenyIAMSCP \
    --type SERVICE_CONTROL_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "DenyIAMSCP",
            "Description": "Deny all IAM actions",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

- AWS SDKs: CreatePolicy

> **Note**
>
> 遇到管理帳戶與少數其他幾種情況時，SCP 沒有任何作用。如需更多詳細資訊，請參閱 任務和實體不受 SCP 的限制。

更新 SCP

登入到您組織的管理帳戶時，您可以重新命名或變更政策的內容。變更 SCP 的內容會立即影響所有連接帳戶中的任何使用者、群組和角色。

> **最低許可**
>
> 若要更新 SCP，您需要具有執行下列動作的許可：
>
> - `organizations:UpdatePolicy`，並在包含指定政策 (或 "*") 的 ARN 的相同政策陳述式中具有 `Resource` 元素

- `organizations:DescribePolicy`，並在包含指定政策 (或 "*") 的 ARN 的相同政策陳述式中具有 `Resource` 元素

AWS Management Console

更新政策

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Service control policies (服務控制政策) 頁面上，選擇您要更新的政策名稱。
3. 在政策的詳細資訊頁面上，選擇 Edit policy (編輯政策)。
4. 進行下列任一或所有變更：
   - 您可以在 Policy name (政策名稱) 中輸入新名稱，來重新命名政策。
   - 您可以在 Policy description (政策描述) 輸入新文字，來變更描述。
   - 您可以在左側窗格中以 JSON 格式編輯政策，來編輯政策文字。或者，您可以在右側的編輯器中選擇陳述式，同時使用控制項來變更其元素。如需每個控制項的詳細資訊，請參閱本主題稍早介紹的建立 SCP 程序。
5. 完成時，請選擇 Save changes (儲存變更)。

AWS CLI & AWS SDKs

更新政策

您可以使用下列其中一項命令來更新政策：

- AWS CLI: update-policy

  下列範例會重新命名政策。

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "MyRenamedPolicy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
```

```
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "Blocks all IAM actions",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

下列範例會新增或變更服務控制政策的描述。

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new policy description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "My new policy description",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

下列範例會指定包含新 JSON 政策文字的檔案，以變更 SCP 的政策文件。

```
$ aws organizations update-policy \
    --policy-id p-zlfw1r64
    --content file://MyNewPolicyText.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
```

```
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "My new policy description",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"AModifiedPolicy\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*
\"]}]}"
    }
}
```

- AWS SDKs: UpdatePolicy

如需詳細資訊

如需有關建立 SCP 的詳細資訊，請參閱下列主題：

- 服務控制政策範例
- SCP 語法

編輯連接至 SCP 的標籤

登入您的組織的管理帳戶時，您可以新增或移除連接至 SCP 的標籤。如需標記的詳細資訊，請參閱標記 AWS Organizations 資源。

> **最低許可**
>
> 若要編輯連接至您 AWS 組織的 SCP 的標籤，您必須擁有以下許可：
>
> - `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要
> - `organizations:DescribePolicy` – 僅在使用 Organizations 主控台時才需要
> - `organizations:TagResource`
> - `organizations:UntagResource`

AWS Management Console

編輯連接至 SCP 的標籤

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Service control policies (服務控制政策) 頁面上，選擇您要編輯的附有標籤的政策名稱。
3. 在政策詳細資訊頁面上，選擇 Tags (標籤) 索引標籤，然後選擇 Manage tags (管理標籤)。
4. 進行下列任一或所有變更：
   - 透過在舊值上輸入新值來變更標籤的值。您無法直接修改標籤鍵。若要變更標籤鍵，您必須刪除含有舊標籤鍵的標籤，然後新增含有新標籤鍵的標籤。
   - 選擇 Remove (移除) 以移除現有的標籤。
   - 新增標籤鍵值組。選擇 Add tag (新增標籤)，然後在提供的方塊中輸入新的標籤鍵名稱和選用值。如果您將 Value (值) 方塊保留空白，則值為空白字串；而不是 `null`。
5. 完成時，請選擇 Save changes (儲存變更)。

AWS CLI & AWS SDKs

編輯連接至 SCP 的標籤

您可以使用下列其中一項命令來編輯連接至 SCP 的標籤：

- AWS CLI: tag-resource and untag-resource
- AWS SDKs: TagResource and UntagResource

刪除 SCP

登入到您的組織的管理帳戶時，您可以刪除在您的組織中不再需要的政策。

> **備註**
>
> - 您必須先將政策從所有連接的實體分離，才能刪除政策。
> - 您無法刪除任何 AWS 受管 SCP，例如名稱為 `FullAWSAccess` 的 SCP。

最低許可

若要刪除 SCP，您需要具有執行下列動作的許可：

- `organizations:DeletePolicy`

AWS Management Console

刪除 SCP

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Service control policies (服務控制政策) 頁面上，選擇您要刪除的 SCP 名稱。
3. 您必須先將您要刪除的政策從所有根、OU 和帳戶分離。選擇 Targets (目標) 索引標籤，再選擇每個根、OU 或顯示於 Targets (目標) 清單中帳戶旁邊的選項按鈕，然後選擇 Detach (分離)。在確認對話方塊中，選擇 Detach (分離)。重複操作，直至移除所有目標。
4. 在頁面頂端，選擇 Delete (刪除)。
5. 在確認對話方塊中，輸入政策的名稱，然後選擇 Delete (刪除)。

AWS CLI & AWS SDKs

刪除 SCP

您可以使用下列其中一項命令來刪除政策：

- AWS CLI: delete-policy

  以下範例會刪除指定的 SCP。

  ```
  $ aws organizations delete-policy \
      --policy-id p-i9j8k7l6m5
  ```

  此命令成功後就不會產生輸出。

- AWS SDKs: DeletePolicy

連接和分離服務控制政策

登入組織的管理帳戶時，您可以連接先前建立的服務控制政策 (SCP)。您可以將 SCP 連接至組織根、組織單位 (OU)，或直接連接至帳戶。若要建立 SCP，請完成下列步驟。

最低許可

若要將 SCP 連接至根、OU 或帳戶，您需要具有執行下列動作的許可：

- `organizations:AttachPolicy`，並在包含 "*" 或指定政策的 Amazon Resource Name（ARN）和您要連接政策的根、OU 或帳戶的 ARN 的相同政策陳述式中具有 `Resource` 元素

AWS Management Console

您可以導覽至政策或連接政策的根、OU 或帳戶，以連接 SCP 政策。

導覽至根、OU 或帳戶以連接 SCP 政策

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 AWS 帳戶 頁面上，導覽至您要連接 SCP 的根、OU 或帳戶旁邊的核取方塊，然後選擇。您可能需要展開 OU (選擇)，以尋找您所需的 OU 和帳戶。
3. 在 Policies (政策) 索引標籤的 Service control policies (服務控制政策) 項目中，選擇 Attach (連接)。
4. 尋找您所需的政策，然後選擇 Attach policy (連接政策)。

   Policies (政策) 索引標籤上的連接的 SCP 清單會更新，以包含新的新增項目。政策變更會立即影響連接的帳戶中 IAM 使用者和角色或連接的根或 OU 下所有帳戶的許可。

導覽至政策以連接 SCP

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Service control policies (服務控制政策) 頁面上，選擇您要連接的政策名稱。

3. 在 Targets (目標) 索引標籤上，選擇 Attach (連接)。
4. 選擇您要連接政策的根、OU 或帳戶旁的選項按鈕。您可能需要展開 OU (選擇 ▶)，以尋找您所需的 OU 和帳戶。
5. 選擇連接政策。

   Targets (目標) 索引標籤上的連接的 SCP 清單會更新，以包含新的新增項目。政策變更會立即影響連接的帳戶中 IAM 使用者和角色或連接的根或 OU 下所有帳戶的許可。

AWS CLI & AWS SDKs

導覽至根、OU 或帳戶以連接 SCP 政策

您可以使用下列其中一項命令來連接 SCP：

- AWS CLI: attach-policy

  下列範例會將 SCP 連接至 OU。

```
$ aws organizations attach-policy \
    --policy-id p-i9j8k7l6m5 \
    --target-id ou-a1b2-f6g7h222
```

  此命令成功後就不會產生輸出。

- AWS 軟體開發套件：AttachPolicy

政策變更會立即影響連接的帳戶中 IAM 使用者和角色或連接的根或 OU 下所有帳戶的許可。

從組織根、OU 或帳戶中分離 SCP

登入組織的管理帳戶後，您可以將 SCP 從原本連接的組織根、OU 或帳戶中分離。從實體中離開 SCP 後，該 SCP 不再適用於受現在已分離實體影響的任何 IAM 使用者和 IAM 角色。若要分離 SCP，請完成下列步驟。

> **Note**
>
> 您無法從根、OU 或帳戶分離最後一個 SCP。必須始終有至少一個 SCP 連接至每一個根、OU 和帳戶。

> **最低許可**
>
> 若要從根、OU 或帳戶中分離 SCP，您需要具有執行下列動作的許可：
>
> - `organizations:DetachPolicy`

AWS Management Console

您可以導覽至政策或您要分離政策的根、OU 或帳戶，以分離 SCP 政策。

導覽至連接的目標根、OU 或帳戶以分離 SCP

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 AWS 帳戶 頁面導覽至您要從中分離政策的根、OU 或帳戶。您可能需要展開 OU (選擇)，以尋找您所需的 OU 和帳戶。選擇根、OU 或帳戶的名稱。
3. 在 Policies (政策) 索引標籤上，選擇您要分離的 SCP 旁邊的選項按鈕，然後選擇 Detach (分離)。
4. 在確認對話方塊中，選擇 Detach policy (分離政策)。

   連接的 SCP 清單隨即更新。分離 SCP 導致的 SCP 變更會立即生效。例如，對於先前連接的帳戶，或先前連接的根或 OU 下的帳戶，分離 SCP 會立即影響其中 IAM 使用者和角色的許可。

導覽至政策以分離 SCP

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Service control policies (服務控制政策) 頁面上，選擇您要從根、OU 或帳戶分離的政策名稱。

3. 在 Targets (目標) 索引標籤上，選擇您要分離政策的根、OU 或帳戶旁的選項按鈕。您可能需要展開 OU (選擇 ▶)，以尋找您所需的 OU 和帳戶。
4. 請選擇分離。
5. 在確認對話方塊中，選擇 Detach (分離)。

   連接的 SCP 清單隨即更新。分離 SCP 導致的 SCP 變更會立即生效。例如，對於先前連接的帳戶，或先前連接的根或 OU 下的帳戶，分離 SCP 會立即影響其中 IAM 使用者和角色的許可。

AWS CLI & AWS SDKs

將 SCP 從根、OU 或帳戶分離

您可以使用下列其中一項命令來分離 SCP：

- AWS CLI: detach-policy

  下列範例會將指定的 SCP 與指定的 OU 分離。

```
$ aws organizations detach-policy \
    --policy-id p-i9j8k7l6m5 \
    --target-id ou-a1b2-f6g7h222
```

- AWS 軟體開發套件：DetachPolicy

政策變更會立即影響連接的帳戶中 IAM 使用者和角色或連接的根或 OU 下所有帳戶的許可

SCP 評估

> **Note**
>
> 本節中的資訊不適用於管理政策類型，包括 AI 服務選擇退出政策、備份政策或標記政策。如需更多詳細資訊，請參閱 理解管理政策繼承。

由於可以在 AWS Organizations 中連接不同層級的多個服務控制政策 (SCP)，因此理解 SCP 的評估方式可協助您撰寫產生正確結果的 SCP。

主題

- SCP 如何使用允許陳述式
- SCP 如何使用拒絕陳述式
- 使用 SCP 的策略

SCP 如何使用允許陳述式

對於為特定帳戶允許的許可，每個層級都必須有明確的 **`Allow`** 陳述式，範圍從根目錄到帳戶直接路徑中的每個 OU (包括目標帳戶本身)。這就是為什麼當您啟用 SCP 時，AWS Organizations 會連接名為 FullAWSAccess 的 AWS 受管 SCP 政策，該政策允許所有服務和動作。如果移除此政策且未在組織的任何層級取代，則該層級下的所有 OU 和帳戶都會遭到封鎖，無法執行任何動作。

例如，讓我們逐步瀏覽圖 1 和圖 2 中顯示的場景。對於在帳戶 B 中允許的許可或服務，應將允許此許可或服務的 SCP 連接至根、生產 OU 和帳戶 B 本身。

SCP 評估遵循預設拒絕模型，這意味著 SCP 中未明確允許的任何許可都將被拒絕。如果在 SCP 中的任何層級 (例如根目錄、生產 OU 或帳戶 B) 均沒有允許陳述式，則會拒絕存取。

> **備註**
>
> - SCP 中的 `Allow` 陳述式允許 `Resource` 元素只有一個 `"*"` 項目。
> - SCP 中的 `Allow` 陳述式完全不能有 `Condition` 元素。

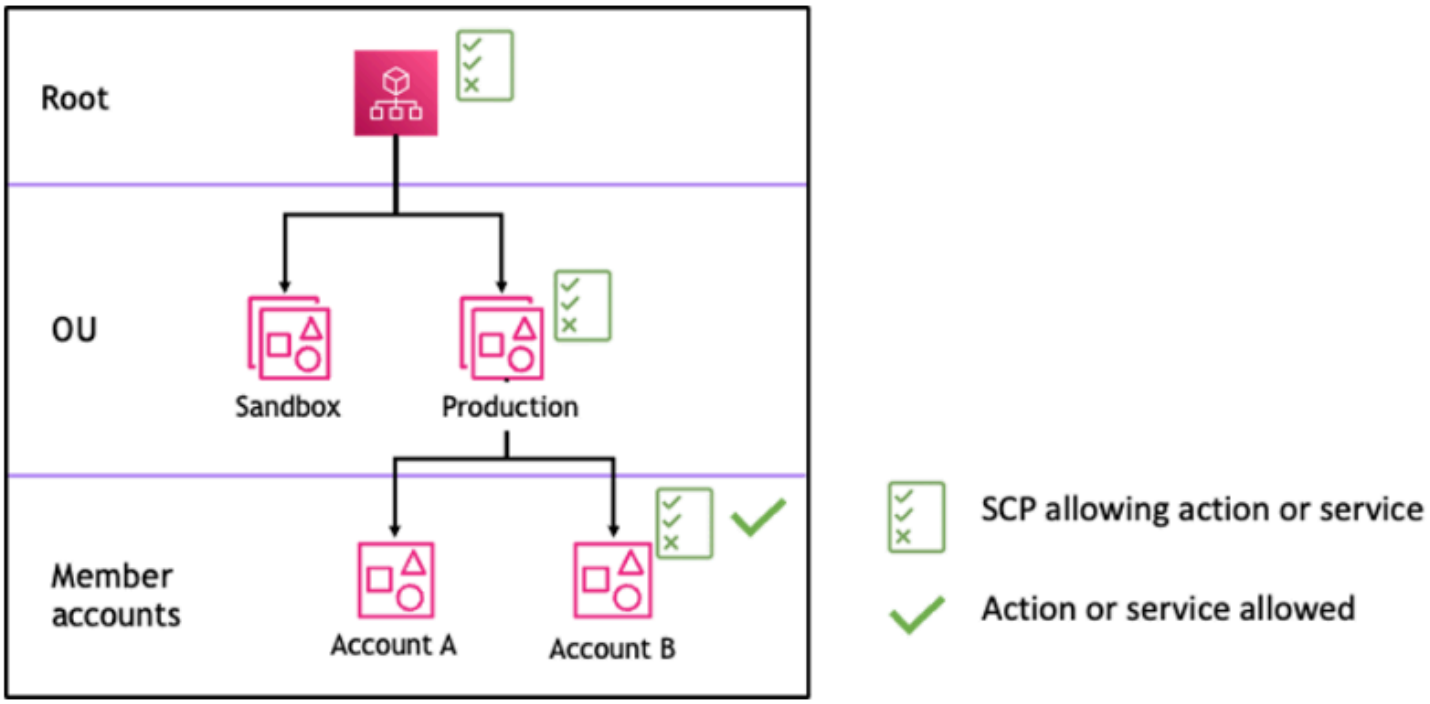


圖 1：在根、生產 OU 和帳戶 B 中連接 *Allow* 陳述式的範例組織結構

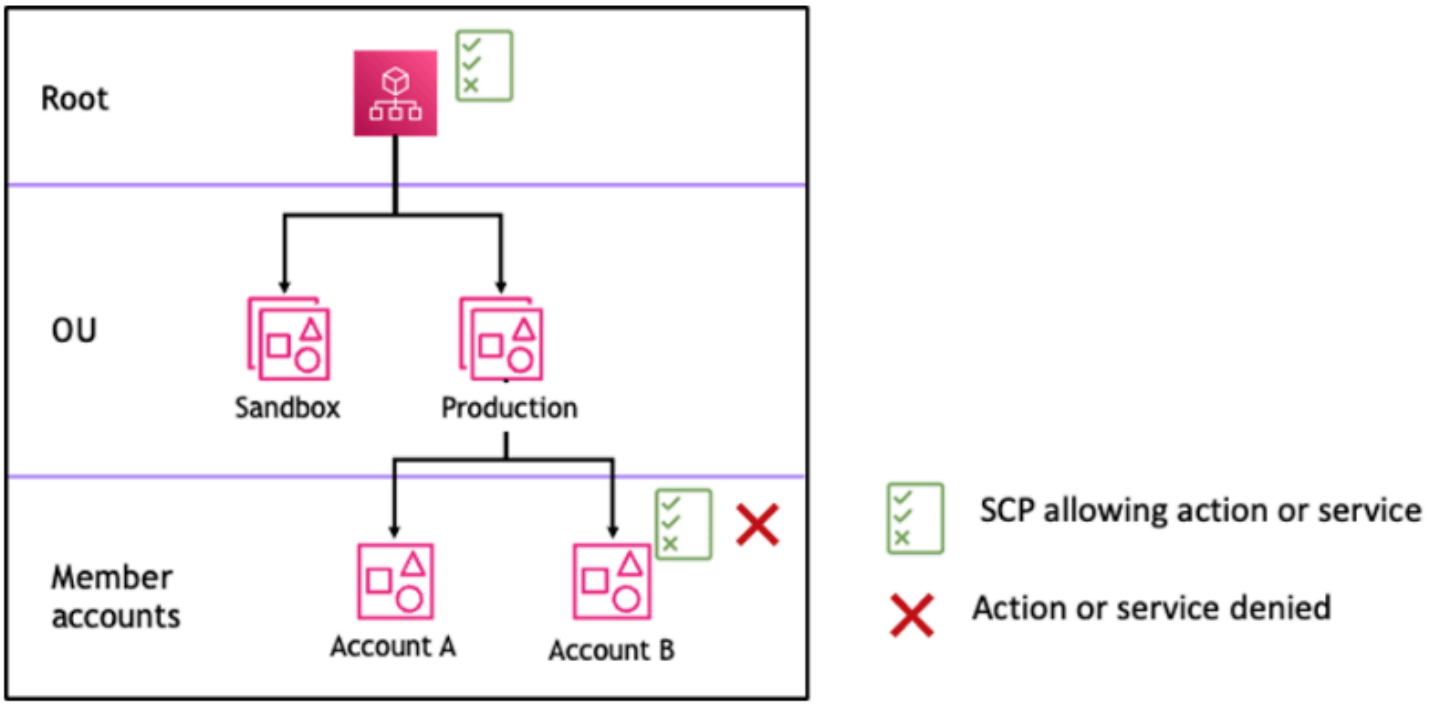


圖 2：生產 OU 中缺少 *Allow* 陳述式的範例組織結構及其對帳戶 B 的影響

SCP 如何使用拒絕陳述式

對於為特定帳戶拒絕的許可，從根目錄到帳戶直接路徑中的每個 OU (包括目標帳戶本身) 的任何 SCP 都可以拒絕該許可。

例如，假設有一個 SCP 連接至生產 OU，該 SCP 具有針對特定服務指定的明確 Deny 陳述式。剛好有另一個 SCP 連接至根和帳戶 B，其明確允許存取該相同的服務，如圖 3 所示。因此，帳戶 A 和帳戶 B 都會遭到拒絕存取該服務，因為系統會針對所有 OU 和成員帳戶評估連接至組織中任何層級的拒絕政策。

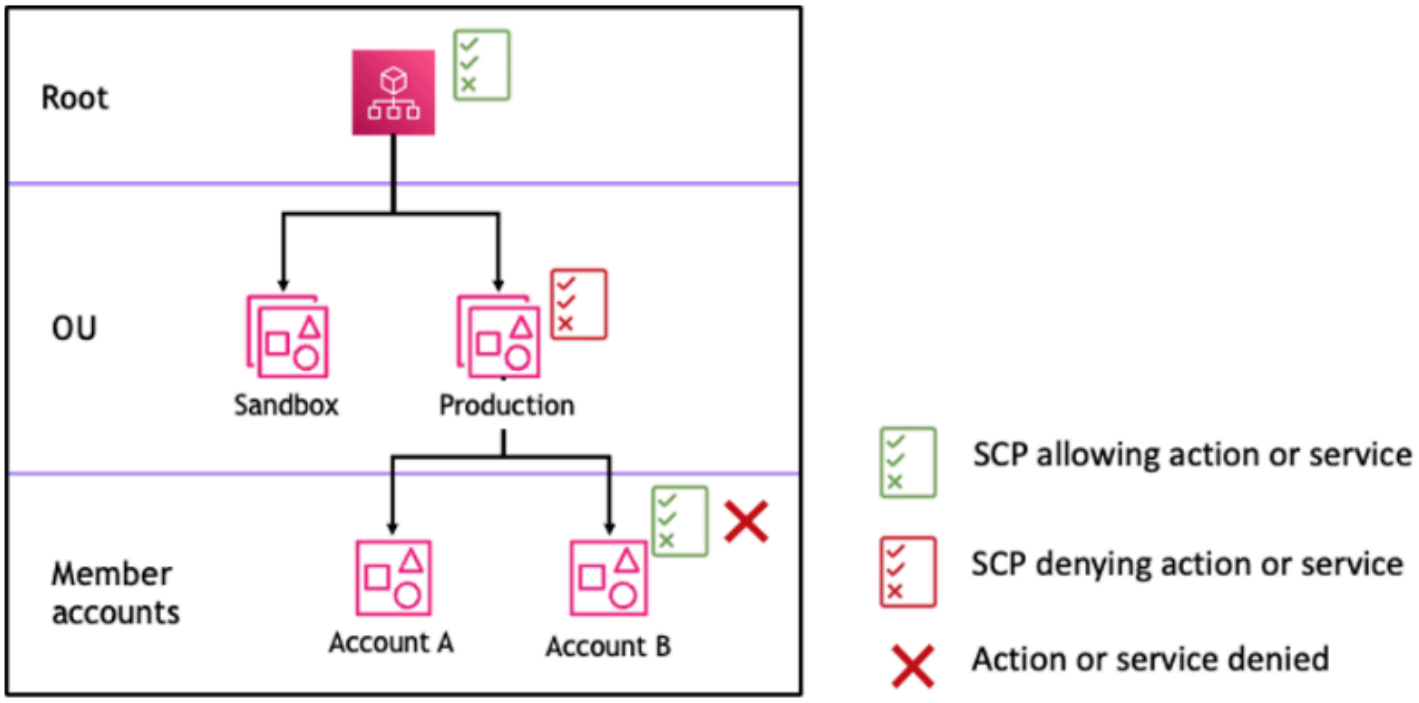


圖 3：在生產 OU 中連接 *Deny* 陳述式的範例組織結構及其對帳戶 B 的影響

使用 SCP 的策略

撰寫 SCP 時，您可以使用 Allow 和 Deny 陳述式的組合，以允許組織中預期的動作和服務。 Deny 陳述式是實作限制的強大方法，這些限制對於組織或 OU 的較廣泛部分來說應該有效，因為在根層級或 OU 層級套用時，它們會影響其下的所有帳戶。

例如，您可以在根層級使用 防止成員帳戶離開組織。 實作政策，該政策對組織中的所有帳戶都有效。拒絕陳述式也支援可協助建立例外狀況的條件元素。

> **Tip**
>
> 您可以使用IAM中服務上次存取的資料更新 SCP，以限制僅存取您所需的 AWS 服務。如需詳細資訊，請參閱 IAM 使用者指南中的檢視 Organizations 的 Organizations 服務上次存取資料。

AWS Organizations 會在建立時將名為 FullAWSAccess 的 AWS 受管 SCP 連接至每個根、OU 和帳戶。此政策會允許所有服務和動作。您可以使用僅允許一組服務的政策取代 FullAWSAccess，從而除非透過更新 SCP 明確允許新的 AWS 服務，否則不允許這些服務。例如，如果您的組織只想要允許在環境中使用服務子集，可以使用 `Allow` 陳述式來僅允許特定的服務。

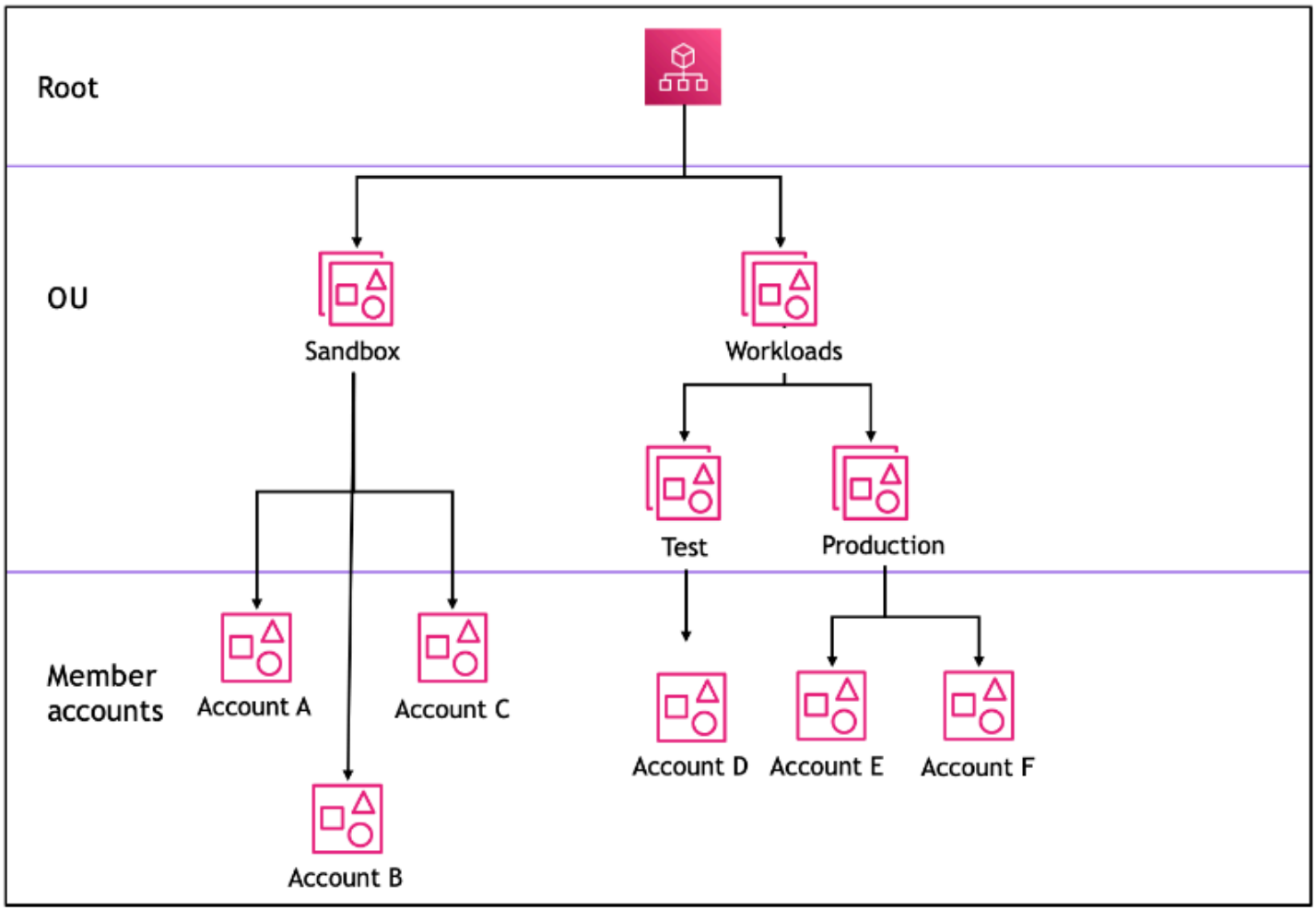
```
{
"Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "cloudwatch:*",
                "organizations:*"
            ],
            "Resource": "*"
        }
    ]
}
```

結合這兩種陳述式的政策可能如以下範例所示，其中會阻止成員帳戶離開組織並允許使用所需的 AWS 服務。組織管理員可以分離 FullAWSAccess 政策，並改為連接此政策。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "cloudwatch:*",
                "organizations:*"
            ],
            "Resource": "*"
```

```
        },
        {
            "Effect": "Deny",
            "Action":"organizations:LeaveOrganization",
            "Resource": "*"
        }
    ]
}
```

現在，請考慮下列範例組織結構，以理解如何在組織中的不同層級套用多個 SCP。



如下資料表顯示沙盒 OU 中的有效政策。

案例	根中的 SCP	沙盒 OU 中的 SCP	帳戶 A 中的 SCP	帳戶 A 中的產生政策	帳戶 B 和帳戶 C 中的產生政策
1	完整 AWS 存取	完整 AWS 存取 + 拒絕 S3 存取	完整 AWS 存取 + 拒絕 EC2 存取	無 S3 存取，無 EC2 存取	無 S3 存取
2	完整 AWS 存取	允許 Amazon Elastic Compute Cloud (Amazon EC2) 存取	允許 EC2 存取	僅允許 EC2 存取	僅允許 EC2 存取
3	拒絕 S3 存取	允許 S3 存取	完整 AWS 存取	無服務存取	無服務存取

如下資料表顯示工作負載 OU 中的有效政策。

案例	根中的 SCP	工作負載 OU 中的 SCP	測試 OU 中的 SCP	帳戶 D 中的產生政策	生產 OU、帳戶 E 和帳戶 F 中的產生政策
1	完整 AWS 存取	完整 AWS 存取	完整 AWS 存取 + 拒絕 EC2 存取	無 EC2 存取	完整 AWS 存取
2	完整 AWS 存取	完整 AWS 存取	允許 EC2 存取	允許 EC2 存取	完整 AWS 存取
3	拒絕 S3 存取	完整 AWS 存取	允許 S3 存取	無服務存取	無服務存取

SCP 語法

服務控制政策 (SCP) 使用的語法與 (IAM) 許可政策和以資源為基礎的政策 AWS Identity and Access Management (例如 Amazon S3 儲存貯體政策) 所使用的語法類似。如需 IAM 政策及其語法的詳細資訊，請參閱 IAM 使用者指南中的 https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html指南中的 IAM 政策概觀。

SCP 是根據 JSON 規則進行結構化的純文字檔。本主題描述它使用的元素。

> **Note**
>
> 您 SCP 中所有的字元都會計入其大小上限。本指南中範例顯示的 SCP 格式具有額外的空格，以改善其可讀性。不過，若您的政策大小接近大小上限，為了節省空間，您可以刪除引號外部的任何空格，例如空格字元和換行字元。

如需 SCP 的一般資訊，請參閱服務控制政策 (SCP)。

元素摘要

下表摘要說明您可以在 SCP 中使用的政策元素。有些政策元素僅能在拒絕動作的 SCP 中使用。Supported effects (支援效果) 欄會列出您在 SCP 中可搭配每個政策元素使用的效果類型。

Element	用途	支援效果
版本	指定用於處理政策的語言語法規則。	`Allow, Deny`
Statement	做為政策元素的容器。SCP 中可包含多個陳述式。	`Allow, Deny`
Statement ID (Sid)	(選用) 提供陳述式	`Allow, Deny`

Element	用途	支援效果
	的易記名稱。	
效果	定義 SCP 陳述式是要允許還是拒絕存取帳戶中的 IAM 使用者和角色。	`Allow`, `Deny`
Action	指定 SCP 允許或拒絕的 AWS 服務和動作。	`Allow`, `Deny`
NotAction	指定從 SCP 排除的 AWS 服務和動作。使用此項目以取代 `Action` 元素。	`Deny`
Resource	指定 SCP 套用至的 AWS 資源。	`Deny`

Element	用途	支援效果
Condition	指定決定陳述式生效時機的條件。	Deny

下列各節提供如何在 SCP 中使用政策元素的更多資訊及範例。

`Version` 元素

每個 SCP 必須包含具有值 "2012-10-17" 的 Version 元素。這是與 IAM 許可政策的最新版本相同的版本值。

```
    "Version": "2012-10-17",
```

如需詳細資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：版本。

`Statement` 元素

SCP 包含一或多個 Statement 元素。您在政策中只能有一個 Statement 關鍵字，但其值可以是 JSON 陣列的陳述式 (加上 [ ] 字元)。

以下範例顯示單一陳述式，其中包含單一 Effect、Action 和 Resource 元素。

```
    "Statement": {
        "Effect": "Allow",
        "Action": "*",
        "Resource": "*"
    }
```

以下範例包含兩個陳述式，在一個 Statement 元素內有陣列清單。第一個陳述式會允許所有動作，第二個則會拒絕任何 EC2 動作。其結果是帳戶中的管理員可委派除了 Amazon Elastic Compute Cloud (Amazon EC2) 之外的任何許可。

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
```

```
        },
        {
            "Effect": "Deny",
            "Action": "ec2:*",
            "Resource": "*"
        }
    ]
```

如需詳細資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：陳述式。

Statement ID (**Sid**) 元素

Sid 是一種您可以為政策陳述式提供的選用識別符。您可以將 Sid 值指派給陳述式陣列中的每個陳述式。以下範例 SCP 會顯示範例 Sid 陳述式。

```
{
    "Statement": {
        "Sid": "AllowsAllActions",
        "Effect": "Allow",
        "Action": "*",
        "Resource": "*"
    }
}
```

如需詳細資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：ID。

Effect 元素

每個陳述式必須包含一個 Effect 元素。此值可以是 Allow 或 Deny。它會影響任何相同陳述式中列出的動作。

如需詳細資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：效果。

"Effect": "Allow"

以下範例會顯示一個具備陳述式的 SCP，該陳述式中包含了值為 Allow 的 Effect 元素，允許帳戶使用者執行 Amazon S3 服務的動作。此範例在使用允許清單策略的組織中很有用 (默認 FullAWSAccess 政策全部分離，因為這樣就能讓許可按預設隱含獲得拒絕)。結果是，陳述式允許任何連接帳戶的 Amazon S3 許可：

```
{
    "Statement": {
```

```
        "Effect": "Allow",
        "Action": "s3:*",
        "Resource": "*"
    }
}
```

即使此陳述式使用與 IAM 許可政策相同的 `Allow` 值關鍵字，在 SCP 中，它仍不會實際授予使用者執行任何動作的許可。而是，SCP 會充當篩選器，為組織中的 IAM 使用者和 IAM 角色指定最大許可。在上述範例中，即使帳戶中的使用者已有連接的 `AdministratorAccess` 受管政策，此 SCP 仍會將受影響帳戶中的所有使用者限制為僅能存取 Amazon S3 動作。

"Effect": "Deny"

在 `Effect` 元素的值為 `Deny` 的陳述式中，您也可以將存取限制在特定資源，或是定義決定 SCP 何時生效的條件。

以下顯示範例，示範如何在拒絕陳述式中使用條件金鑰。

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": "ec2:RunInstances",
        "Resource": "arn:aws:ec2:*:*:instance/*",
        "Condition": {
            "StringNotEquals": {
                "ec2:InstanceType": "t2.micro"
            }
        }
    }
}
```

此 SCP 中的陳述式會設定一個防撞欄，防止受影響的帳戶 (其中 SCP 已連接到帳戶本身，或是連接到包含帳戶的組織根或 OU) 在 Amazon EC2 執行個體的類型並未設為 `t2.micro` 時啟動 Amazon EC2 執行個體。即使允許此動作的 IAM 政策已連接到帳戶，SCP 建立的防撞欄也會防止該操作。

Action 和 NotAction 元素

每個陳述式都必須包含以下其中一個項目：

- 在允許和拒絕陳述式中，必須包含一個 `Action` 元素。
- 針對拒絕陳述式 (`Effect` 元素的值為 `Deny`)，必須包含一個 `Action`「或」`NotAction` 元素。

Actionor NotAction 元素的值是字串清單 (JSON 陣列)，可識別陳述式允許或拒絕的 AWS 服務和動作。

每個字串都包含服務的縮寫 (例如 "s3"、"ec2"、"iam" 或 "organizations")，採用全部小寫，後面接著冒號，然後是來自該服務的動作。動作和非動作 (notaction) 區分大小寫，因此必須如每個服務文件中所示的方式輸入。一般而言，輸入時每個字會以首字大寫字母開始，然後其餘為小寫。例如："s3:ListAllMyBuckets"。

您也可以在 SCP 中使用萬用字元，例如星號 (*) 或問號 (?)：

- 使用星號 (*) 作為萬用字元，以比對部分名稱相同的多個動作。值 "s3:*" 表示 Amazon S3 服務中的所有動作。值 "ec2:Describe*" 只會符合開頭為 "Describe" 的 EC2 動作。
- 使用問號 (?) 萬用字元來比對單一字元。

> **Note**
>
> 在 SCP 中，Action 或 NotAction 元素中的萬用字元 (*) 和 (?) 只能單獨使用或用在字串結尾。它不能出現在字串開頭或中間。因此，在 SCP 中，"servicename:action*" 有效，但 "servicename:*action" 和 "servicename:some*action" 都無效。

如需 S AWS Organizations CP 和 IAM 權限政策中所支援的所有服務及其支援動作的清單，請參閱 IAM 使用者指南中的AWS 服務適用的動作、資源和條件金鑰。

如需詳細資訊，請參閱 IAM JSON 政策元素：動作和 IAM JSON 政策元素： NotAction在 IAM 使用者指南中。

Action 元素的範例

以下範例顯示的 SCP 包含一個陳述式，允許帳戶管理員委派帳戶中 EC2 執行個體的描述、啟動、停止和終止許可。這是允許名單的範例，當預設的 Allow * 政策未連接時非常有用，使得依預設會隱含拒絕許可。若預設的 Allow * 政策仍然連接到以下政策所連接的根、OU 或帳戶，則該政策不會有任何作用。

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
          "ec2:DescribeInstances", "ec2:DescribeImages", "ec2:DescribeKeyPairs",
```

```
          "ec2:DescribeSecurityGroups", "ec2:DescribeAvailabilityZones",
 "ec2:RunInstances",
          "ec2:TerminateInstances", "ec2:StopInstances", "ec2:StartInstances"
        ],
        "Resource": "*"
    }
}
```

以下範例示範如何將您不要在連接帳戶中使用的服務加入拒絕清單。它會假設預設的 "Allow *" SCP 仍連接到所有 OU 和根帳戶。此範例政策可防止連接的帳戶中的帳戶管理員針對 IAM、Amazon EC2 和 Amazon RDS 服務委派任何許可。可以委派來自其他服務的任何動作，只要沒有連接的另一個附加政策拒絕他們。

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": [ "iam:*", "ec2:*", "rds:*" ],
        "Resource": "*"
    }
}
```

NotAction 元素的範例

下列範例顯示如何使用NotAction元素將 AWS 服務排除在策略的影響之外。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LimitActionsInRegion",
      "Effect": "Deny",
      "NotAction": "iam:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": "us-west-1"
         }
       }
     }
   ]
}
```

使用此聲明，受影響的帳戶僅限於在指定的中執行操作 AWS 區域，但使用 IAM 操作除外。

`Resource` 元素

在 `Effect` 元素的值為 `Allow` 的陳述式中，您只能在 SCP 的 `Resource` 元素內指定 "*"。您無法指定個別資源的 Amazon 資源名稱 (ARN)。

您也可以在資源元素中使用萬用字元，例如星號 (*) 或問號 (?)：

- 使用星號 (*) 作為萬用字元，以比對部分名稱相同的多個動作。
- 使用問號 (?) 萬用字元來比對單一字元。

在 `Effect` 元素的值為 `Deny` 的陳述式中，您「可以」指定個別 ARN，如以下範例所示。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessToAdminRole",
      "Effect": "Deny",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
      ],
      "Resource": [
        "arn:aws:iam::*:role/role-to-deny"
      ]
    }
  ]
}
```

此 SCP 會限制受影響帳戶中的 IAM 使用者和角色，對您組織中所有帳戶內建立的常見管理 IAM 角色進行變更。

如需詳細資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：資源。

`Condition` 元素

您可以在 SCP 中的拒絕陳述式內指定 `Condition` 元素。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAllOutsideEU",
            "Effect": "Deny",
            "NotAction": [
                "cloudfront:*",
                "iam:*",
                "route53:*",
                "support:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-central-1",
                        "eu-west-1"
                    ]
                }
            }
        }
    ]
}
```

除了所列出服務中的動作外，此 SCP 會拒絕存取任何位於 `eu-central-1` 和 `eu-west-1` 區域外的操作。

如需詳細資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：條件

不支援的元素

SCP 不支援以下元素：

- `Principal`
- `NotPrincipal`

- NotResource

服務控制政策範例

本主題中顯示的範例服務控制政策 (SCP) 僅供參考。

> **使用這些範例之前**
>
> 您在組織中使用這些範例 SCP 前，請執行下列操作：
>
> - 詳閱及自訂 SCP，使其符合您的獨特需求。
> - 徹底測試您環境中的 SCP 與您使用的 AWS 服務。
>
> 本節中的範例政策示範 SCP 的實作與使用。他們並非闡述為完全如圖所示實作的官方 AWS 建議或最佳實務。您有責任仔細測試任何拒絕型政策是否適合解決您環境的商業需求。拒絕型服務控制政策可能會意外限制或封鎖您使用 AWS 服務，除非您將必要的例外狀況新增至政策。如需此類例外狀況的範例，請參閱第一個範例，其從封鎖存取不需要的 AWS 區域 的規則中豁免全域服務。
> - 請記住，SCP 會影響其連接到每個帳戶中的每個使用者、角色，包括根使用者。

> **Tip**
>
> 您可以使用IAM中服務上次存取的資料更新 SCP，以限制僅存取您所需的 AWS 服務。如需詳細資訊，請參閱 IAM 使用者指南中的檢視 Organizations 的 Organizations 服務上次存取資料。

以下每一個政策都是拒絕清單政策策略的範例。拒絕清單政策必須隨著在受影響帳戶中允許已核准動作的其他政策連接。例如，預設的 FullAWSAccess 政策會允許使用帳戶中的所有服務。此政策預設連接到根帳戶、所有組織單位 (OU) 和所有帳戶。它不會實際授予許可；沒有任何 SCP 會這麼做。相反地，此政策可讓該帳戶中的管理員，將標準 AWS Identity and Access Management (IAM) 許可政策連接至帳戶中的使用者、角色或群組，以委派對這些動作的存取。然後，這些拒絕清單政策會個別藉由封鎖對指定的服務或動作的存取，來覆寫任何政策。

範例

- 一般範例

    - 根據請求的 AWS 區域 拒絕存取 AWS
    - 防止 IAM 使用者和角色進行某些變更
    - 防止 IAM 使用者和角色進行指定變更，且指定的管理員角色除外
    - 要求 MFA 執行 API 動作
    - 封鎖根使用者的服務存取
    - 防止成員帳戶離開組織。
- Amazon CloudWatch 範例 SCP
    - 防止使用者停用 CloudWatch 或更改其組態
- AWS Config 的範例 SCP
    - 防止使用者停用 AWS Config 或變更其規則
- Amazon Elastic Compute Cloud (Amazon EC2) 的範例 SCP
    - 要求 Amazon EC2 執行個體使用特定類型
    - 防止在沒有 IMDSv2 的情況下啟動 EC2 執行個體
    - 防止停用預設的 Amazon EBS 加密
- Amazon GuardDuty 的範例 SCP
    - 防止使用者停用 GuardDuty 或修更其組態
- AWS Resource Access Manager 的範例 SCP
    - 防止外部共享
    - 允許特定帳戶僅共享指定的資源類型
    - 防止與組織或組織單位 (OU) 共享
    - 僅允許與指定的 IAM 使用者和角色共享
- Amazon Route 53 Application Recovery Controller 的 SCP 範例
    - 防止使用者更新 Route 53 ARC 路由控制狀態
- 適用於 Amazon S3 的 SCP 範例
    - 防止 Amazon S3 未加密物件上傳
- 標記資源的 SCP 範例
    - 需要在建立的指定資源上使用標籤
    - 防止標籤被授權委託人以外的人員修改
- Amazon Virtual Private Cloud (Amazon VPC) 的範例 SCP
    - 防止使用者刪除 Amazon VPC 流程日誌

- 防止尚沒有網際網路存取的任何 VPC 取得存取

一般範例

根據請求的 AWS 區域 拒絕存取 AWS

此 SCP 拒絕存取任何位於指定區域外的操作。以您希望使用的 AWS 區域 取代 `eu-central-1` 和 `eu-west-1`。它為核准之全域服務中的操作提供豁免。此範例也顯示了如何豁免由兩個指定的管理員角色之一所提出的請求。

> **Note**
>
> 若要將區域拒絕 SCP 與 AWS Control Tower 搭配使用，請參閱 根據請求的 AWS 區域 拒絕存取 AWS。

此政策會使用此 `Deny` 效果，來拒絕存取不以兩個核准區域 (`eu-central-1` 和 `eu-west-1`) 之一為目標之操作的所有請求。NotAction 元素可讓您列出服務，這些服務的操作 (或個別操作) 都免受此限制的約束。由於全域服務具有由 `us-east-1` 區域實體託管的端點，因此必須以這種方式豁免這些端點。透過以這種方式結構化的 SCP，如果要求的服務包含在 `NotAction` 元素中，則允許對 `us-east-1` 區域內全域服務提出的請求。此範例政策會拒絕任何其他對 `us-east-1` 區域內服務的請求。

> **Note**
>
> 此範例可能不包含所有最新的全域 AWS 服務或操作。請將服務和營運項目清單替換成您組織中帳戶所使用的全球服務。
>
> > **秘訣**
> >
> > 您可以在 IAM 主控台中檢視服務上次存取的資料，以判斷您的組織使用的全域服務。IAM 使用者、群組或角色詳細資訊頁面上的 Access Advisor 索引標籤會顯示該實體已使用的 AWS 服務，按最近存取排序。

考量事項

- AWS KMS 和 AWS Certificate Manager 支援區域端點。然而，如果您想要將其與全域服務 (例如 Amazon CloudFront) 搭配使用，則必須將其包含在下列範例 SCP 的全域服務排除清單中。Amazon CloudFront 之類的全域服務通常需要存取相同區域的 AWS KMS 和 ACM，而全域服務則為美國東部 (維吉尼亞北部) 區域 (us-east-1)。
- 依據預設，AWS STS 為全域服務，且必須包含在全域服務排除清單中。不過，您可以啟用 AWS STS 以使用區域端點，而不是單一全域端點。如果您執行此操作，可從下列範例 SCP 的全域服務豁免清單中移除 STS。如需詳細資訊，請參閱在 AWS 區域 中管理 AWS STS。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAllOutsideEU",
            "Effect": "Deny",
            "NotAction": [
                "a4b:*",
                "acm:*",
                "aws-marketplace-management:*",
                "aws-marketplace:*",
                "aws-portal:*",
                "budgets:*",
                "ce:*",
                "chime:*",
                "cloudfront:*",
                "config:*",
                "cur:*",
                "directconnect:*",
                "ec2:DescribeRegions",
                "ec2:DescribeTransitGateways",
                "ec2:DescribeVpnGateways",
                "fms:*",
                "globalaccelerator:*",
                "health:*",
                "iam:*",
                "importexport:*",
                "kms:*",
                "mobileanalytics:*",
```

```
                "networkmanager:*",
                "organizations:*",
                "pricing:*",
                "route53:*",
                "route53domains:*",
                "route53-recovery-cluster:*",
                "route53-recovery-control-config:*",
                "route53-recovery-readiness:*",
                "s3:GetAccountPublic*",
                "s3:ListAllMyBuckets",
                "s3:ListMultiRegionAccessPoints",
                "s3:PutAccountPublic*",
                "shield:*",
                "sts:*",
                "support:*",
                "trustedadvisor:*",
                "waf-regional:*",
                "waf:*",
                "wafv2:*",
                "wellarchitected:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-central-1",
                        "eu-west-1"
                    ]
                },
                "ArnNotLike": {
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
        }
    ]
}
```

防止 IAM 使用者和角色進行某些變更

此 SCP 會限制 IAM 使用者和角色，對您組織中所有帳戶內建立的指定 IAM 角色進行變更。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessToASpecificRole",
      "Effect": "Deny",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
      ],
      "Resource": [
        "arn:aws:iam::*:role/name-of-role-to-deny"
      ]
    }
  ]
}
```

防止 IAM 使用者和角色進行指定變更，且指定的管理員角色除外

此 SCP 是以前一個範例為基礎，為管理員設置了例外狀況。它會防止受影響帳戶中 IAM 使用者和角色，對您組織中所有帳戶內建立的常見管理 IAM 角色進行變更，但使用指定角色的管理員則除外。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessWithException",
      "Effect": "Deny",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
```

```
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
      ],
      "Resource": [
        "arn:aws:iam::*:role/name-of-role-to-deny"
      ],
      "Condition": {
        "StringNotLike": {
          "aws:PrincipalARN":"arn:aws:iam::*:role/name-of-admin-role-to-allow"
        }
      }
    }
  ]
}
```

要求 MFA 執行 API 動作

使用如下的 SCP，來要求先啟用多重要素驗證 (MFA)，IAM 使用者和角色才能停止執行動作。在此範例中，動作是停止 Amazon EC2 執行個體。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyStopAndTerminateWhenMFAIsNotPresent",
      "Effect": "Deny",
      "Action": [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource": "*",
      "Condition": {"BoolIfExists": {"aws:MultiFactorAuthPresent": false}}
    }
  ]
}
```

封鎖根使用者的服務存取

下列政策會限制對成員帳戶中根使用者的所有存取。若您希望防止您的帳戶以特定方式使用根憑證，請將您自己的動作新增到此政策。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RestrictEC2ForRoot",
      "Effect": "Deny",
      "Action": [
        "ec2:*"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::*:root"
          ]
        }
      }
    }
  ]
}
```

防止成員帳戶離開組織。

下列政策會封鎖使用 LeaveOrganization API 操作，讓成員帳戶的管理員無法從組織中移除其帳戶。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "organizations:LeaveOrganization"
            ],
            "Resource": "*"
        }
    ]
}
```

Amazon CloudWatch 範例 SCP

此類別中的範例

- 防止使用者停用 CloudWatch 或更改其組態

防止使用者停用 CloudWatch 或更改其組態

較低級別的 CloudWatch 操作人員需要監控儀表板和警報。然而，操作人員必須無法刪除或變更資深人員可能會設置的任何儀表板或警示。此 SCP 可防止任何受影響帳戶中的使用者或角色執行可能刪除或變更儀表板或警示的任何 CloudWatch 命令。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DeleteDashboards",
        "cloudwatch:DisableAlarmActions",
        "cloudwatch:PutDashboard",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:SetAlarmState"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS Config 的範例 SCP

此類別中的範例

- 防止使用者停用 AWS Config 或變更其規則

防止使用者停用 AWS Config 或變更其規則

此 SCP 可防止任何受影響帳戶中的使用者或角色執行可能停用 AWS Config 或更改其規則或觸發的 AWS Config 操作。

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "config:DeleteConfigRule",
        "config:DeleteConfigurationRecorder",
        "config:DeleteDeliveryChannel",
        "config:StopConfigurationRecorder"
      ],
      "Resource": "*"
    }
  ]
}
```

Amazon Elastic Compute Cloud (Amazon EC2) 的範例 SCP

此類別中的範例

- 要求 Amazon EC2 執行個體使用特定類型
- 防止在沒有 IMDSv2 的情況下啟動 EC2 執行個體
- 防止停用預設的 Amazon EBS 加密

要求 Amazon EC2 執行個體使用特定類型

使用這項 SCP，任何未使用 `t2.micro` 執行個體類型啟動的執行個體都會遭到拒絕。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RequireMicroInstanceType",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ec2:InstanceType": "t2.micro"
        }
      }
```

```
    }
  ]
}
```

防止在沒有 IMDSv2 的情況下啟動 EC2 執行個體

以下政策限制所有使用者在沒有 IMDSv2 的情況下啟動 EC2 執行個體。

```
[
   {
      "Effect":"Deny",
      "Action":"ec2:RunInstances",
      "Resource":"arn:aws:ec2:*:*:instance/*",
      "Condition":{
         "StringNotEquals":{
            "ec2:MetadataHttpTokens":"required"
         }
      }
   },
   {
      "Effect":"Deny",
      "Action":"ec2:RunInstances",
      "Resource":"arn:aws:ec2:*:*:instance/*",
      "Condition":{
         "NumericGreaterThan":{
            "ec2:MetadataHttpPutResponseHopLimit":"3"
         }
      }
   },
   {
      "Effect":"Deny",
      "Action":"*",
      "Resource":"*",
      "Condition":{
         "NumericLessThan":{
            "ec2:RoleDelivery":"2.0"
         }
      }
   },
   {
      "Effect":"Deny",
      "Action":"ec2:ModifyInstanceMetadataOptions",
      "Resource":"*"
   }
```

```
]
```

以下政策限制所有使用者在沒有 IMDSv2 的情況下啟動 EC2 執行個體，但允許特定 IAM 身分修改執行個體中繼資料選項。

```
[
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "StringNotEquals": {
        "ec2:MetadataHttpTokens": "required"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "NumericGreaterThan": {
        "ec2:MetadataHttpPutResponseHopLimit": "3"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "*",
    "Resource": "*",
    "Condition": {
      "NumericLessThan": {
        "ec2:RoleDelivery": "2.0"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:ModifyInstanceMetadataOptions",
    "Resource": "*",
    "Condition": {
      "StringNotLike": {
        "aws:PrincipalARN": [
```

```
          "arn:aws:iam::{ACCOUNT_ID}:{RESOURCE_TYPE}/{RESOURCE_NAME}"
        ]
      }
    }
  }
]
```

防止停用預設的 Amazon EBS 加密

以下政策限制所有使用者停用預設的 Amazon EBS 加密。

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:DisableEbsEncryptionByDefault"
  ],
  "Resource": "*"
}
```

Amazon GuardDuty 的範例 SCP

此類別中的範例

- 防止使用者停用 GuardDuty 或修更其組態

防止使用者停用 GuardDuty 或修更其組態

此 SCP 可防止任何受影響帳戶中的使用者或角色停用 GuardDuty，或更改其組態，無論直接以命令形式或透過主控台。它有效地啟用對 GuardDuty 資訊和資源的唯讀存取。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "guardduty:AcceptInvitation",
                "guardduty:ArchiveFindings",
                "guardduty:CreateDetector",
                "guardduty:CreateFilter",
                "guardduty:CreateIPSet",
                "guardduty:CreateMembers",
                "guardduty:CreatePublishingDestination",
```

```
                "guardduty:CreateSampleFindings",
                "guardduty:CreateThreatIntelSet",
                "guardduty:DeclineInvitations",
                "guardduty:DeleteDetector",
                "guardduty:DeleteFilter",
                "guardduty:DeleteInvitations",
                "guardduty:DeleteIPSet",
                "guardduty:DeleteMembers",
                "guardduty:DeletePublishingDestination",
                "guardduty:DeleteThreatIntelSet",
                "guardduty:DisassociateFromMasterAccount",
                "guardduty:DisassociateMembers",
                "guardduty:InviteMembers",
                "guardduty:StartMonitoringMembers",
                "guardduty:StopMonitoringMembers",
                "guardduty:TagResource",
                "guardduty:UnarchiveFindings",
                "guardduty:UntagResource",
                "guardduty:UpdateDetector",
                "guardduty:UpdateFilter",
                "guardduty:UpdateFindingsFeedback",
                "guardduty:UpdateIPSet",
                "guardduty:UpdatePublishingDestination",
                "guardduty:UpdateThreatIntelSet"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS Resource Access Manager 的範例 SCP

此類別中的範例

- 防止外部共享
- 允許特定帳戶僅共享指定的資源類型
- 防止與組織或組織單位 (OU) 共享
- 僅允許與指定的 IAM 使用者和角色共享

防止外部共享

下列範例 SCP 可防止使用者建立資源共享，以允許與不屬於組織的 IAM 使用者和角色共享。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:CreateResourceShare",
                "ram:UpdateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "ram:RequestedAllowsExternalPrincipals": "true"
                }
            }
        }
    ]
}
```

允許特定帳戶僅共享指定的資源類型

下列 SCP 允許帳戶 111111111111 和 222222222222 以建立共享字首清單的資源共享，並將字首清單與現有的資源共享關聯。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "OnlyNamedAccountsCanSharePrefixLists",
            "Effect": "Deny",
            "Action": [
                "ram:AssociateResourceShare",
                "ram:CreateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalAccount": [
                        "111111111111",
                        "222222222222"
                    ]
                },
                "StringEquals": {
```

```
                    "ram:RequestedResourceType": "ec2:PrefixList"
                }
            }
        }
    ]
}
```

防止與組織或組織單位 (OU) 共享

下列 SCP 可防止使用者建立與 AWS 組織或 OU 共享資源的資源共享。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:CreateResourceShare",
                "ram:AssociateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringLike": {
                    "ram:Principal": [
                        "arn:aws:organizations::*:organization/*",
                        "arn:aws:organizations::*:ou/*"
                    ]
                }
            }
        }
    ]
}
```

僅允許與指定的 IAM 使用者和角色共享

下列範例 SCP 允許使用者僅與組織 o-12345abcdef、組織單位 ou-98765fedcba，以及帳戶 111111111111 共享資源。

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

```
            "Action": [
                "ram:AssociateResourceShare",
                "ram:CreateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringNotEquals": {
                    "ram:Principal": [
                        "arn:aws:organizations::123456789012:organization/
o-12345abcdef",
                        "arn:aws:organizations::123456789012:ou/o-12345abcdef/
ou-98765fedcba",
                        "111111111111"
                    ]
                }
            }
        }
    ]
}
```

Amazon Route 53 Application Recovery Controller 的 SCP 範例

此類別中的範例

- 防止使用者更新 Route 53 ARC 路由控制狀態

防止使用者更新 Route 53 ARC 路由控制狀態

較低級別的 Route 53 ARC 操作員需要監控儀表板並檢視 Route 53 ARC 資訊。不過，操作員不得更新路由控制，以便將應用程式從一個 AWS 區域 容錯移轉至另一個區域，因為資深操作員才可這麼做。此 SCP 可防止任何受影響帳戶中的使用者或角色執行可能更新 Route 53 ARC 路由控制的 Route 53 ARC 操作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAll",
            "Effect": "Deny",
            "Action": [
                "route53-recovery-cluster:UpdateRoutingControlState",
                "route53-recovery-cluster:UpdateRoutingControlStates"
            ],
```

```
            "Resource": "*",
            "Condition": {
                "ArnNotLike": {
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
        }
    ]
}
```

適用於 Amazon S3 的 SCP 範例

此類別中的範例

- 防止 Amazon S3 未加密物件上傳

防止 Amazon S3 未加密物件上傳

以下政策限制所有使用者將未加密的物件上傳至 S3 儲存貯體。

```
{
  "Effect": "Deny",
  "Action": "s3:PutObject",
  "Resource": "*",
  "Condition": {
    "Null": {
      "s3:x-amz-server-side-encryption": "true"
    }
  }
}
```

以下政策限制所有使用者將未加密的物件上傳至 S3 儲存貯體，並強制執行指定的加密類型 (AES256 或 aws:kms)，以便在其儲存貯體中進行物件上傳。

```
[
  {
    "Effect": "Deny",
    "Action": "s3:PutObject",
    "Resource": "*",
```

```
    "Condition": {
      "Null": {
        "s3:x-amz-server-side-encryption": "true"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "s3:PutObject",
    "Resource": "*",
    "Condition": {
      "StringNotEquals": {
        "s3:x-amz-server-side-encryption": "AES256"
      }
    }
  }
]
```

標記資源的 SCP 範例

此類別中的範例

- 需要在建立的指定資源上使用標籤
- 防止標籤被授權委託人以外的人員修改

需要在建立的指定資源上使用標籤

如果請求未包含指定的標籤，下列 SCP 可防止受影響帳戶中的 IAM 使用者和角色建立某些資源類型。

> **Important**
>
> 請記得透過您在環境中使用的服務來測試拒絕型政策。下列範例是建立未標記機密或執行未標記 Amazon EC2 執行個體的簡單區塊，且不包含任何例外狀況。
> 以下範例政策與 AWS CloudFormation 不相容，因為該服務會建立一個機密，然後將其標記為兩個單獨的步驟。此範例政策會有效阻止 AWS CloudFormation 建立機密作為堆疊的一部分，因為這樣的動作會導致未根據需要標記的機密。

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

```
    {
      "Sid": "DenyCreateSecretWithNoProjectTag",
      "Effect": "Deny",
      "Action": "secretsmanager:CreateSecret",
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:RequestTag/Project": "true"
        }
      }
    },
    {
      "Sid": "DenyRunInstanceWithNoProjectTag",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition": {
        "Null": {
          "aws:RequestTag/Project": "true"
        }
      }
    },
    {
      "Sid": "DenyCreateSecretWithNoCostCenterTag",
      "Effect": "Deny",
      "Action": "secretsmanager:CreateSecret",
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:RequestTag/CostCenter": "true"
        }
      }
    },
    {
      "Sid": "DenyRunInstanceWithNoCostCenterTag",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
```

```
      "Condition": {
        "Null": {
          "aws:RequestTag/CostCenter": "true"
        }
      }
    }
  ]
}
```

如需所有服務的清單，及其在 AWS Organizations SCP 和 IAM 許可政策中支援的動作，請參閱 IAM 使用者指南中的AWS 服務的動作、資源和條件索引鍵。

防止標籤被授權委託人以外的人員修改

下列 SCP 顯示政策如何僅允許授權委託人修改連接至您資源的標籤。這是使用以屬性為基礎的存取控制 (ABAC) 作為 AWS 雲端安全策略的重要部分。該政策允許呼叫者僅修改以下資源上的標籤：其授權標籤 (在本例中為 `access-project`) 與連接至發出請求的使用者或角色的相同授權標籤完全相符。該政策也會防止授權使用者變更用於授權的標籤值。呼叫委託人必須具有授權標籤，才能完全進行任何變更。

該政策只會阻止未經授權的使用者變更標記。未被此政策封鎖的授權使用者仍必須具有單獨的 IAM 政策，明確授予相關標記 API 上的 `Allow` 許可。舉例來說，如果您的使用者具有`Allow */*`的管理員政策 (允許所有服務和所有操作)，則組合會導致允許管理員使用者僅變更以下標籤：具有與連接至使用者委託人的授權標籤值相符的授權標籤值。這是因為該政策中的明確`Deny`會覆寫管理員政策中的明確`Allow`。

> **Important**
>
> 這並非完整的政策解決方案，不得如下所示使用。此範例僅用於說明 ABAC 策略的一部分，且需要針對生產環境進行自訂與測試。
> 如需完整的政策及其運作方式的詳細分析，請參閱AWS Organizations中的使用服務控制政策來保護用於授權的資源標籤
> 請記得透過您在環境中使用的服務來測試拒絕型政策。

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

```
            "Effect": "Deny",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ec2:ResourceTag/access-project": "${aws:PrincipalTag/access-
project}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
                },
                "Null": {
                    "ec2:ResourceTag/access-project": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/access-project": "${aws:PrincipalTag/access-
project}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "access-project"
                    ]
                }
            }
        },
```

```
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
                },
                "Null": {
                    "aws:PrincipalTag/access-project": true
                }
            }
        }
    ]
}
```

Amazon Virtual Private Cloud (Amazon VPC) 的範例 SCP

此類別中的範例

- 防止使用者刪除 Amazon VPC 流程日誌
- 防止尚沒有網際網路存取的任何 VPC 取得存取

防止使用者刪除 Amazon VPC 流程日誌

此 SCP 可防止任何受影響帳戶中的使用者或角色刪除 Amazon Elastic Compute Cloud (Amazon EC2) 流程日誌或 CloudWatch 日誌群組或日誌串流。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ec2:DeleteFlowLogs",
```

```
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream"
      ],
      "Resource": "*"
    }
  ]
 }
```

防止尚沒有網際網路存取的任何 VPC 取得存取

此 SCP 可防止任何受影響帳戶中的使用者或角色變更您的 Amazon EC2 Virtual Private Cloud (VPC) 的組態，以授予它們網際網路的直接存取。它不會封鎖現有的直接存取，或透過您的現場部署網路環境路由的任何存取。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ec2:AttachInternetGateway",
        "ec2:CreateInternetGateway",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateVpcPeeringConnection",
        "ec2:AcceptVpcPeeringConnection",
        "globalaccelerator:Create*",
        "globalaccelerator:Update*"
      ],
      "Resource": "*"
    }
  ]
}
```

管理組織單位

您可以使用組織單位 (OU) 將帳戶群組在一起，以單一單位的形式進行管理。這可大幅簡化帳戶的管理。例如，您可以將以政策為基礎的控制連接到 OU，而 OU 內的所有帳戶會自動繼承政策。您可以在單一組織內建立多個 OU，您也可以在其他 OU 內建立 OU。每個 OU 可以包含多個帳戶，而且您可以在 OU 之間移動帳戶。但是，OU 的名稱在父系 OU 或根中必須是唯一的。

> **Note**
>
> 組織中有一個根，它 AWS Organizations 會在您第一次設定組織時為您建立。

主題

您也可以檢閱組織中的所有 OU。如需詳細資訊，請參閱檢視 OU 的詳細資訊。

導覽根帳戶和 OU 階層

在移動帳戶或連接政策時，若要導覽至不同的 OU 或導覽至根，您可以使用預設「樹狀目錄」檢視。

AWS Management Console

將組織作為「樹狀目錄」導覽

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 AWS 帳戶 頁面 Organization (組織) 區段的頂部，選取Hierarchy (階層) 切換 (而不是List (清單))。

3. 樹狀目錄一開始會顯示根，僅顯示子 OU 和帳戶的第一層。若要展開樹狀目錄以顯示更深的層級，請選擇任何父實體旁的展開圖示 ()。若要降低雜亂和收合樹狀目錄的分支，請選擇已展開的父實體旁的折疊圖示 ()。
4. 選擇 OU 或根的名稱，以檢視其詳細資訊並執行特定操作。或者，您可以選擇名稱旁的選項按鈕，並在 Actions (動作) 選單中執行對該實體的特定操作。

您還可以僅以表格形式檢視組織中帳戶的清單，而不必先導覽至 OU 來尋找它們。在此檢視中，您無法看到任何 OU，或操控連接到它們的政策。

AWS Management Console

以沒有階層的平面帳戶清單來檢視組織

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在AWS 帳戶頁面的 [組織] 區段頂端，選擇 [AWS 帳戶 僅檢視] 切換開關圖示將其開啟。  。
3. 不含任何階層的帳戶清單會隨即顯示。

建立 OU

登入您的組織的管理帳戶時，您可以在組織的根建立一個 OU。OU 可以建立最多達五層的巢狀。若要建立您的第一個 OU，請完成以下步驟。

> **Important**
>
> 如果使用管理此組織 AWS Control Tower，請使用 AWS Control Tower 主控台或 API 建立 OU。如果您在 Organizations 中建立 OU，則該 OU 不會在中註冊 AWS Control Tower。如需詳細資訊，請參閱AWS Control Tower 使用者指南中的參照 AWS Control Tower外部資源。

> **最低許可**
>
> 若要在您的組織的根帳戶內建立 OU，您必須擁有以下許可：

- `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要
- `organizations:CreateOrganizationalUnit`

AWS Management Console

建立組織單位 (OU)

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 導覽至 AWS 帳戶 頁面。

   主控台會顯示根及其內容。第一次瀏覽根時，主控台會在該最上層檢視中顯示所有的 AWS 帳戶 。如果您之前建立了 OU，並將帳戶移至其中，主控台只會顯示最上層 OU 以及尚未移至 OU 的任何帳戶。
3. (選用) 如果您想要在現有 OU 內建立 OU，請透過選擇子 OU 的名稱 (而不是核取方塊)，或在樹狀檢視中選擇 OU 旁白的

   直至看到您所需的 OU，然後選擇其名稱，來導覽至子 OU。
4. 當您在階層中選取正確的父 OU 時，請在 Actions (動作) 選單的 Organizational Unit (組織單位) 下方，選擇 Create new (建立新的)
5. 在 Create organizational unit (建立組織單位) 對話方塊中，輸入您要建立的 OU 名稱。
6. (選用) 選擇 Add tag (新增標籤)，然後輸入一個鍵和一個選用值，來新增一個或多個標籤。將值留空會將其設定為空白字串；而不是 `null`。您可以在 OU 中連接最多 50 個標籤。
7. 最後，選擇 Create organizational unit (建立組織單位)。

您的新 OU 會顯示在父系內。您現在可以將帳戶移至此 OU，或將政策連接至此 OU。

AWS CLI & AWS SDKs

建立組織單位 (OU)

您可以使用下列其中一項命令來建立 OU：

- AWS CLI: create-organizational-unit

  若要建立 OU，您必須先尋找要作為新 OU 父項的根或 OU 的 ID。

若要尋找根的 ID，使用 list-roots 命令。若要尋找 OU 的 ID，使用 list-children 導覽至您所需的 OU。

下列範例顯示如何尋找根的 ID，然後在根下尋找 OU 的 ID。最後一個命令顯示如何在找到的 OU 中建立新的 OU。

```
$ aws organizations list-roots
{
    "Roots": [
        {
            "Id": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "PolicyTypes": []
        }
    ]
}
$ aws organizations list-children \
    --parent-id r-a1b2 \
    --child-type ORGANIZATIONAL_UNIT
{
    "Children": [
        {
            "Id": "ou-a1b2-f6g7h111",
            "Type": "ORGANIZATIONAL_UNIT"
        }
    ]
}
$ aws organizations create-organizational-unit \
    --parent-id ou-a1b2-f6g7h111 \
    --name New-Child-OU
{
    "OrganizationalUnit": {
        "Id": "ou-a1b2-f6g7h222",
        "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h222",
        "Name": "New-Child-OU"
    }
}
```

- AWS 軟體開發套件：CreateOrganizationalUnit

重新命名 OU

登入您的組織的管理帳戶時，您可以重新命名 OU。若要執行此動作，請執行下列步驟。

最低許可

若要重新命名組 AWS 織中根目錄內的 OU，您必須具備下列權限：

- `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要
- `organizations:UpdateOrganizationalUnit`

AWS Management Console

重新命名 OU

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 AWS 帳戶 頁面上，導覽至您要重新命名的 OU，然後執行以下其中一個步驟：
   - 選擇想要重新命名的 OU 旁邊的選項按鈕
     然後，在 Actions (動作) 選單的 Organizational unit (組織單位) 中，選擇 Rename (重新命名)。
   - 選擇 OU 的名稱，以存取 OU 的詳細資訊頁面。然後，在頁面頂端選擇 Rename (重新命名)。
3. 在 Rename organizational unit (重新命名組織單位) 對話方塊中，輸入新名稱，然後選擇 Save changes (儲存變更)。

AWS CLI & AWS SDKs

重新命名 OU

您可以使用下列其中一項命令來重新命名 OU：

- AWS CLI: update-organizational-unit

  下列範例顯示如何將 OU 重新命名。

```
$ aws organizations update-organizational-unit \
    --organizational-unit-id ou-a1b2-f6g7h222 \
    --name "Renamed-OU"
{
    "OrganizationalUnit": {
        "Id": "ou-a1b2-f6g7h222",
        "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h222",
        "Name": "Renamed-OU"
    }
}
```

- AWS 軟體開發套件：UpdateOrganizationalUnit

編輯連接至 OU 的標籤

登入您的組織的管理帳戶時，您可以新增或移除連接至 OU 的標籤。若要執行此動作，請執行下列步驟。

最低許可

若要編輯附加至組 AWS 織根目錄內 OU 的標籤，您必須具備下列權限：

- `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要
- `organizations:DescribeOrganizationalUnit` – 僅在使用 Organizations 主控台時才需要
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

編輯連接至 OU 的標籤

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 AWS 帳戶 頁面上，導覽至您要編輯其標籤的 OU 並選擇其名稱。
3. 在 OU 的詳細資訊頁面上，選擇 Tags (標籤) 索引標籤，然後選擇 Manage tags (管理標籤)。

4. 您可以在此索引標籤上執行以下任一動作：

   - 透過在舊值上輸入新值來編輯任何標籤的值。您無法修改標籤鍵。若要變更標籤鍵，您必須刪除含有舊標籤鍵的標籤，並新增含有新標籤鍵的標籤。
   - 透過選擇您要移除的標籤旁邊的 Remove (移除)，移除現有的標籤。
   - 新增標籤鍵值組。選擇 Add tag (新增標籤)，然後在提供的方塊中輸入新的標籤鍵名稱和選用值。如果您將 Value (值) 方塊保留空白，則值為空白字串；而不是 `null`。

5. 在您完成所有要進行的新增、移除和編輯之後，選擇 Save changes (儲存變更)。

AWS CLI & AWS SDKs

編輯連接至 OU 的標籤

您可以使用下列其中一項命令來變更連接至 OU 的標籤：

- AWS CLI: tag-resource and untag-resource

  下列範例會將標籤 `"Department"="12345"` 連接至 OU。請注意，`Key` 和 `Value` 區分大小寫。

  ```
  $ aws organizations tag-resource \
      --resource-id ou-a1b2-f6g7h222 \
      --tags Key=Department,Value=12345
  ```

  此命令成功後就不會產生輸出。

  下列範例會從 OU 中移除 `Department` 標記。

  ```
  $ aws organizations untag-resource \
      --resource-id ou-a1b2-f6g7h222 \
      --tag-keys Department
  ```

  此命令成功後就不會產生輸出。

- AWS 軟體開發套件：TagResource和 UntagResource

將帳戶移動到 OU 或在根與 OU 之間移動

登入到您的組織的管理帳戶時，您可以將您的組織中的帳戶從根移至 OU，在 OU 間移動，或從 OU 回到根。將帳戶放置在 OU 內，可讓它受限於連接至父 OU 和父系鏈結中任何 OU 的任何政策。如果帳戶不在 OU 中，則僅受限於直接連接至根政策，以及直接連接帳戶的任何政策。若要移動帳戶，請完成以下步驟。

最低許可

若要將帳戶移至 OU 階層中的新位置，您必須擁有以下許可：

- `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要
- `organizations:MoveAccount`

AWS Management Console

將帳戶移至 OU

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 AWS 帳戶 頁面上，尋找您要移動的一個或多個帳戶。您可以導覽 OU 階層，或啟用僅檢視 AWS 帳戶 ，以查看沒有 OU 結構的帳戶平面清單。如果您有許多帳戶，您可能需要在清單底部選擇載入更多採用 'ou-name' 的帳戶，以尋找您想要移動的所有內容。
3. 選擇您要移動的每個帳戶名稱旁邊的核取方塊
   ☑ 。
4. 在 Actions (動作) 選單的 AWS 帳戶 下，選擇 Move (移動)。
5. 在 Move AWS 帳戶 (啟動 AWS 帳戶帳戶)對話方塊中，導覽至至您要移動帳戶的目標 OU 或根並選擇，然後選擇 Move AWS 帳戶(移動 AWS 帳戶帳戶)。

AWS CLI & AWS SDKs

將帳戶移至 OU

您可以使用下列其中一項命令來移動帳戶：

- AWS CLI: move-account

下列範例會將 AWS 帳戶 從根目錄移至 OU。請注意，您必須指定來源和目的地容器的 ID。

```
$ aws organizations move-account \
    --account-id 111122223333 \
    --source-parent-id r-a1b2 \
    --destination-parent-id ou-a1b2-f6g7h111
```

此命令成功後就不會產生輸出。

- AWS 軟體開發套件：MoveAccount

刪除 OU

登入到您的組織的管理帳戶時，您可以刪除不再需要的任何 OU。

您必須先將所有帳戶從 OU 和任何子 OU 移出，然後才能刪除子 OU。

最低許可

若要刪除 OU，您必須擁有以下許可：

- `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要
- `organizations:DeleteOrganizationalUnit`

AWS Management Console

刪除 OU

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 AWS 帳戶 頁面上，尋找您要刪除的 OU，然後選擇每個 OU 名稱旁邊的核取方塊  。
3. 選擇 Actions (動作)，然後在 Organizational unit (組織單位) 下，選擇 Delete (刪除)。
4. 若要確認您要刪除 OU，請輸入 OU 的名稱 (如果您選擇僅刪除一個 OU) 或 'delete' 一詞 (如果您選擇多個 OU)，然後選擇 Delete (刪除)。

   AWS Organizations 刪除 OU 並將其從清單中移除。

AWS CLI & AWS SDKs

刪除 OU

您可以使用下列其中一項命令來刪除 OU：

- AWS CLI: delete-organizational-unit

  下列範例顯示如何刪除 OU。

  ```
  $ aws organizations delete-organizational-unit \
      --organizational-unit-id ou-a1b2-f6g7h222
  ```

  此命令成功後就不會產生輸出。
- AWS 軟體開發套件：DeleteOrganizationalUnit

標記 AWS Organizations 資源

標籤是一個自訂屬性標籤，您可將其新增到 AWS 資源以便輕鬆地識別、組織和搜尋資源。每個標籤有兩個部分：

- 標籤鍵 (例如，`CostCenter`、`Environment` 或 `Project`)。標籤鍵最大長度為 128 個字元且區分大小寫。
- 標籤值 (例如 `111122223333` 或 `Production`)。標籤值最大長度為 256 個字元，且與標籤鍵一樣需要區分大小寫。您可以將標籤的值設為空白字串，但您無法將標籤的值設為 Null。忽略標籤值基本上等同於使用空字串。

如需標籤鍵或值中允許哪些字元的詳細資訊，請參閱 Resource Groups 標記 API 參考中的標籤 API 的標籤參數。

您可使用標籤來依照用途、擁有者、環境或其他條件分類資源。如需詳細資訊，請參閱標記AWS資源的最佳做法。

> **Tip**
>
> 使用標籤政策，協助將組織帳戶中各資源的標籤實作標準化。

當您登入管理帳戶，AWS Organizations 目前支援以下標籤操作：

- 您可以將標籤新增至以下組織資源：
  - AWS 帳戶
  - 組織單位
  - 組織的根
  - 政策

您可以在下列時間新增標籤：

- 建立資源時 – 在 Organizations 主控台中指定標籤，或使用 `Tags` 參數與其中一個 `Create` API 操作來指定標籤。這不適用於組織的根。
- 建立資源之後 – 使用 Organizations 主控台，或呼叫 `TagResource` 操作。

您可以使用主控台或呼叫 `ListTagsForResource` 操作，來檢視任何可標記 AWS Organizations 資源上的標籤。

您可以使用主控台或呼叫 `UntagResource` 操作指定要移除的鍵，來從資源中移除標籤。

使用標籤

標籤可讓您按對您有用的任何類別分組資源，從而協助您整理組織中的資源。例如，您可以指派追蹤擁有部門的「部門」標記。您可以指派「環境」標籤，來追蹤指定的資源是否屬於 alpha、beta、gamma 或生產環境的一部分。

您也可以使用標籤執行以下動作：

- 在您的資源上強制執行標記標準。
- 控制誰可以存取您的資源。

新增、更新和移除標籤

登入您的組織的管理帳戶時，您可以為組織中的資源新增標籤。

建立資源時新增標籤

> **最低許可**
>
> 若要在建立資源時將標籤新增至資源，您需要具有以下許可：
>
> - 建立指定類型之資源的許可
> - `organizations:TagResource`
> - `organizations:ListTagsForResource` – 僅在使用 Organizations 主控台時才需要

您可以在建立以下資源時包含連接至該資源的標籤鍵和值。

- AWS 帳戶
  - 建立的帳戶
  - 受邀帳戶
- 組織單位 (OU)

- 政策
  - AI 服務選擇退出政策
  - 備份政策
  - 服務控制政策
  - 標籤政策

組織根會在您初始建立組織時建立，因此，您只能將標籤作為現有資源新增至組織。

新增或更新現有資源的標籤

您還可以新增標籤或更新連接至現有資源的標籤值。

> **最低許可**
>
> 若要將標籤新增或更新至組織中的資源，您需要具有以下許可：
>
> - `organizations:TagResource`
> - `organizations:ListTagsForResource` – 僅在使用 Organizations 主控台時才需要
>
> 若要從組織的資源中移除標籤，您需要具有以下許可：
>
> - `organizations:UntagResource`

AWS Management Console

新增、更新或移除現有資源的標籤

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 導覽並選擇帳戶、根、OU 或政策，然後按一下其名稱以開啟其詳細資訊頁面。
3. 在 Tags (標籤) 索引標籤上，選擇 Manage tags (管理標籤)。
4. 您可以新增標籤、修改現有標籤的值或移除標籤。

   若要新增標籤，請選擇 Add tag (新增標籤)，然後輸入標籤的 Key (鍵) 和選用的 Value (值)。

   若要移除標籤，請選擇 Remove (移除)。

標籤鍵與值皆區分大小寫。使用您要標準化的大小寫。您還必須遵守任何適用標籤政策的要求。

5. 視需要重複上一個步驟。
6. 選擇儲存變更。

AWS CLI & AWS SDKs

將標籤新增或更新至現有資源

您可以使用下列其中一個命令，將標籤新增至組織中的可標記資源：

- AWS CLI：tag-resource
- AWS軟體開發套件：TagResource

從組織的資源中刪除標籤

您可以使用下列其中一項命令來刪除標籤：

- AWS CLI：untag-resource
- AWS軟體開發套件：UntagResource

搭配使用 AWS Organizations 與其他 AWS 服務

您可以使用受信任的存取來啟用您指定的支援的 AWS 服務，稱為信任的服務，以代表您在您的組織及其帳戶中執行任務。這包括授予許可給信任的服務，但不會影響使用者或角色的許可。啟用存取權後，受信任的服務可在需要該角色時，在您組織的每個帳戶中建立一個稱為服務連結角色的 IAM 角色。該角色擁有的許可政策，會允許信任的服務執行該服務文件中所述的任務。這可讓您指定您想要信任的服務代表您在組織的帳戶中維護的設定和組態詳細資訊。受信任的服務只有在需要於帳戶上執行管理動作時，才會建立服務連結角色，而且不一定會在組織的所有帳戶中執行。

Important

我們強烈建議，當該選項可用時，您僅使用受信任服務的主控台，或其 AWS CLI 或 API 操作等效項，來啟用和停用受信任存取。這可讓受信任的服務在啟用受信任的存取時執行任何必要的初始化，例如在停用受信任的存取時，建立任何必要的資源和任何必要的資源清除。
如需如何使用受信任的服務來啟用或停用組織的受信任服務存取的相關資訊，請參閱 AWS 您可以搭配使用的服務 AWS Organizations 的支援受信任的存取欄下方的進一步了解連結。
如果您使用 Organizations 主控台、CLI 命令或 API 操作來停用存取權，則會導致發生下列動作：

- 服務無法再在您組織的帳戶中建立服務連結角色。這意味著服務無法代表您在組織的任何新帳戶上執行操作。服務仍然可以在較舊的帳戶中執行操作，直至服務完成從 AWS Organizations 中清除。
- 除非附加至您角色的 IAM 政策明確允許這些操作，否則服務無法再在組織的成員帳戶中執行任務。這包括從成員帳戶到管理帳戶，或委派管理員帳戶 (如相關) 的任何資料彙總。
- 某些服務會偵測到這一點，並清除與整合相關的任何剩餘的資料或資源，而其他服務會停止存取組織，但會保留任何歷史資料和組態，以針對可能的重新啟用整合提供支援。

而使用其他服務的主控台或命令來停用整合，可確保其他服務可以清除僅用於整合所需的任何資源。服務如何清除組織帳戶中的資源取決於該服務。如需詳細資訊，請參閱其他 AWS 服務的安全文件。

啟用信任的存取所需的許可

信任的存取需要兩個服務的許可：AWS Organizations 和信任的服務。若要啟用信任的存取，請選擇以下其中一個案例：

- 如果您在 AWS Organizations 和信任的服務中擁有許可的憑證，請使用信任的服務中提供的工具 (主控台或 AWS CLI) 來啟用存取。這可讓的服務代表您在 AWS Organizations 中啟用受信任的存取，並建立讓服務在您的組織中運作所需的任何資源。

  這些登入資料的最低許可如下：

  - `organizations:EnableAWSServiceAccess`.您也可以使用 `organizations:ServicePrincipal` 條件金鑰搭配此操作，來限制這些操作對核准的服務委託人名稱清單所做的請求。如需更多詳細資訊，請參閱 條件索引鍵。
  - `organizations:ListAWSServiceAccessForOrganization` – 如果您使用 AWS Organizations 主控台則為必要。
  - 信任的服務所需的最低許可取決於服務。如需詳細資訊，請參閱信任的服務的文件。
- 如果某個人員擁有 AWS Organizations 中許可的憑證，但其他人擁有信任的服務中許可的憑證，請以下列順序執行這些步驟：

  1. 擁有 AWS Organizations 中許可憑證的人員應該使用 AWS Organizations 主控台、AWS CLI 或 AWS SDK 來為信任的服務啟用信任的存取。在執行以下步驟 (步驟 2) 時，這會授予其他服務的許可，以在組織中執行所需的組態。

     最低的 AWS Organizations 許可如下：

     - `organizations:EnableAWSServiceAccess`
     - `organizations:ListAWSServiceAccessForOrganization` – 只有在使用 AWS Organizations 主控台時為必要

     如需在 AWS Organizations 中啟用信任的存取的詳細資訊，請參閱如何啟用或停用信任的存取。
  2. 擁有信任的服務中許可的憑證的人員，可讓該服務與 AWS Organizations 搭配使用。這會指示服務執行任何必要的初始化，例如建立讓信任的服務在組織中操作所需的任何資源。如需詳細資訊，請參閱服務特定指示，位於AWS 您可以搭配使用的服務 AWS Organizations。

停用信任的存取所需的許可

當您不想允許信任的服務在您的組織上或其帳戶上運作，請選擇以下其中一個案例。

> **Important**
>
> 停用信任的服務存取不會 防止具有適當的許可的使用者和角色使用該服務。若要完全封鎖使用者和角色存取 AWS 服務，您可以移除授予該存取權的 IAM 許可，或者您可以使用 AWS Organizations 中的服務控制政策 (SCP)。

您只能將 SCP 套用至成員帳戶。SCP 不會套用至管理帳戶。建議您不要在管理帳戶中執行服務。而是在成員帳戶中執行，您可以在此使用 SCP 控制安全性。

- 如果您在 AWS Organizations 和信任的服務中擁有許可的憑證，請使用信任的服務中可用的工具 (主控台或 AWS CLI) 來停用存取。此服務會藉由移除不再需要的資源，以及代表您停用 AWS Organizations 中服務的信任的存取來進行清理。

  這些登入資料的最低許可如下：

  - `organizations:DisableAWSServiceAccess`.您也可以使用 `organizations:ServicePrincipal` 條件金鑰搭配此操作，來限制這些操作對核准的服務委託人名稱清單所做的請求。如需更多詳細資訊，請參閱 條件索引鍵。
  - `organizations:ListAWSServiceAccessForOrganization` – 如果您使用 AWS Organizations 主控台則為必要。
  - 信任的服務所需的最低許可取決於服務。如需詳細資訊，請參閱信任的服務的文件。
- 如果具有 AWS Organizations 中許可的憑證，不是信任的服務中許可的憑證，請以下列順序執行這些步驟：

  1. 擁有信任的服務中許可的人員會先使用該服務停用存取。這會指示信任的服務透過移除信任的存取所需的資源來進行清理。如需詳細資訊，請參閱服務特定指示，位於AWS 您可以搭配使用的服務 AWS Organizations。
  2. 然後擁有 AWS Organizations 中許可的人員便可以使用 AWS Organizations 主控台、AWS CLI 或 AWS SDK 來停用信任的服務的存取。這會從組織及其帳戶移除信任的服務的許可。

     最低的 AWS Organizations 許可如下：

     - `organizations:DisableAWSServiceAccess`
     - `organizations:ListAWSServiceAccessForOrganization` – 只有在使用 AWS Organizations 主控台時為必要

     如需在 AWS Organizations 中停用信任的存取的詳細資訊，請參閱如何啟用或停用信任的存取。

如何啟用或停用信任的存取

如果您僅有 AWS Organizations 的許可，而您想要代表其他 AWS 服務的管理員啟用或停用對您的組織的信任的存取，請使用下列程序。

Important

我們強烈建議，當該選項可用時，您僅使用受信任服務的主控台，或其 AWS CLI 或 API 操作等效項，來啟用和停用受信任存取。這可讓受信任的服務在啟用受信任的存取時執行任何必要的初始化，例如在停用受信任的存取時，建立任何必要的資源和任何必要的資源清除。
如需如何使用受信任的服務來啟用或停用組織的受信任服務存取的相關資訊，請參閱 AWS 您可以搭配使用的服務 AWS Organizations 的支援受信任的存取欄下方的進一步了解連結。
如果您使用 Organizations 主控台、CLI 命令或 API 操作來停用存取權，則會導致發生下列動作：

- 服務無法再在您組織的帳戶中建立服務連結角色。這意味著服務無法代表您在組織的任何新帳戶上執行操作。服務仍然可以在較舊的帳戶中執行操作，直至服務完成從 AWS Organizations 中清除。
- 除非附加至您角色的 IAM 政策明確允許這些操作，否則服務無法再在組織的成員帳戶中執行任務。這包括從成員帳戶到管理帳戶，或委派管理員帳戶 (如相關) 的任何資料彙總。
- 某些服務會偵測到這一點，並清除與整合相關的任何剩餘的資料或資源，而其他服務會停止存取組織，但會保留任何歷史資料和組態，以針對可能的重新啟用整合提供支援。

而使用其他服務的主控台或命令來停用整合，可確保其他服務可以清除僅用於整合所需的任何資源。服務如何清除組織帳戶中的資源取決於該服務。如需詳細資訊，請參閱其他 AWS 服務的安全文件。

AWS Management Console

啟用受信任的服務存取

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在服務頁面，尋找您要啟用的服務的資料列，然後選擇其名稱。
3. 選擇 Enable trusted access (啟用信任存取)。
4. 在確認對話方塊中，勾選顯示啟用受信任的存取選項，在方塊中輸入 **`enable`**，然後選擇啟用受信任存取。
5. 如果您要啟用存取，請告知其他 AWS 服務的管理員，他們現在可以啟用其他服務以與 AWS Organizations 搭配運作。

若要停用受信任的服務存取

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在服務頁面，尋找您要停用的服務的資料列，然後選擇其名稱。
3. 請等候直到其他服務的管理員告知您已停用服務並且已清除資源為止。
4. 在確認對話方塊中，輸入 **disable**，然後選擇停用受信任的存取。

AWS CLI, AWS API

啟用或停用受信任的服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以啟用或停用信任的服務存取：

- AWS CLI: AWS organizations enable-aws-service-access
- AWS CLI: AWS organizations disable-aws-service-access
- AWS API: EnableAWSServiceAccess
- AWS API：DisableAWSServiceAccess

AWS Organizations 和服務連結角色

AWS Organizations 使用 IAM 服務連結角色來啟用信任的服務，以代表您在組織的成員帳戶中執行任務。設定信任的服務並授權它來與您的組織整合時，該服務可以請求 AWS Organizations 在其成員帳戶中建立服務連結角色。信任的服務會視需要以非同步方式執行此動作，但不一定會同時在組織的所有帳戶中建立。服務連結角色具有預先定義的 IAM 許可，允許受信任的服務僅在該帳戶內執行特定任務。一般而言，AWS 會管理所有服務連結角色，這表示您通常無法更改角色或連接的政策。

為了讓它可行，當您在組織中建立帳戶或接受將您的現有帳戶加入組織的邀請時，AWS Organizations 會為該成員帳戶佈建名為 `AWSServiceRoleForOrganizations` 的服務連結角色。只有 AWS Organizations 服務本身可擔任此角色。角色擁有的許可允許 AWS Organizations 為其他 AWS 服務建立服務連結角色。此服務連結角色會出現在所有組織中。

雖然我們不建議這麼做，如果您的組織只啟用了合併帳單功能，則絕不會使用名為 `AWSServiceRoleForOrganizations` 的服務連結角色，您可以將其刪除。如果您稍後想要在組織中啟用所有功能，則需要該角色，您必須將它還原。當您開始啟用所有功能的程序時，會發生下列檢查：

- 對於獲邀加入組織的每個成員帳戶 – 帳戶管理員會收到請求，請求接受啟用所有功能。若要成功同意請求，管理員必須同時擁有 `organizations:AcceptHandshake` 和 `iam:CreateServiceLinkedRole` 許可，如果服務連結角色 (`AWSServiceRoleForOrganizations`) 尚不存在。如果 `AWSServiceRoleForOrganizations` 角色已存在，管理員只需要 `organizations:AcceptHandshake` 許可即可接受請求。當管理員接受請求，AWS Organizations 會建立服務連結角色 (如果尚不存在)。
- 對於在組織中建立的每個成員帳戶 – 帳戶管理員會收到請求，請求重新建立服務連結角色。(成員帳戶的管理員不會收到啟用所有功能的請求，因為管理帳戶 (之前稱為「主帳戶」) 的管理員會被視為建立成員帳戶的擁有者。) 當成員帳戶管理員接受請求時，AWS Organizations 會建立服務連結角色。管理員必須同時擁有 `organizations:AcceptHandshake` 和 `iam:CreateServiceLinkedRole` 許可，才能成功接受交握。

在組織中啟用所有功能之後，您不再可以從任何帳戶刪除 `AWSServiceRoleForOrganizations` 服務連結角色。

> **Important**
>
> AWS Organizations SCP 永遠不會影響服務連結角色。這些角色不受任何 SCP 的限制。

AWS 您可以搭配使用的服務 AWS Organizations

AWS Organizations 您可以透過 AWS 帳戶 將多個帳戶整合到單一組織中，大規模執行帳戶管理活動。整合帳戶可簡化您使用其他 AWS 服務的方式。您可以利用特定服務中 AWS Organizations 提供的多帳戶管理 AWS 服務，對屬於組織成員的所有帳戶執行任務。

下表列出可搭配使用的 AWS 服務 AWS Organizations，以及在整個組織層級上使用每項服務的好處。

受信任的存取 — 您可以啟用相容的 AWS 服務，以便在組織 AWS 帳戶 中的所有部門執行作業。如需詳細資訊，請參閱 搭配使用 AWS Organizations 與其他 AWS 服務。

委派的 AWS 服務管理員 — 相容的 AWS 服務可以將組織中的 AWS 成員帳戶註冊為該服務中組織帳戶的管理員。如需詳細資訊，請參閱 與 Organizations 合作之 AWS 服務的委派管理員。

AWS 服務	搭配使用的好處 AWS Organizations	支援受信任存取	支援委派的管理員	
AWS Account Management 管理所有組織的詳細資料和中繼資料。AWS 帳戶	您可以建立、更新和刪除組織中所有帳戶的替代聯絡人資訊。	 是 進一步了解	 進一步了解	是
AWS 應用程式移轉服務 (MGN) AWS 應用程式遷移服務可讓企業連接 lift-and-shift 到 AWS 大量的實體、虛擬或雲端伺服器，而不會出現相容性問題、效能中斷或長時間切換時間。	您可以管理跨多個帳戶的大規模遷移。	 是 進一步了解	 進一步了解	是
AWS Artifact 下載 AWS 安全性符合性報告，例如 ISO 和 PCI 報告。	可以代表組織中的所有成員帳戶接受協議。	 是 進一步了解	 請參閱AWS Artifact。	是

AWS 服務	搭配使用的好處 AWS Organizations	支援受信任存取	支援委派的管理員	
AWS Audit Manager 自動化持續收集證據，協助您稽核雲端服務的使用情況。	持續稽核組織中多個帳戶的 AWS 使用情況，以簡化評估風險與合規性的方式。	 是 進一步了解	 是 進一步了解	
AWS Backup 管理及監視組織中所有帳戶的備份。	您可以為整個組織或組織單位 (OU) 中的帳戶群組設定及管理備份計劃。您可以集中監視所有帳戶的備份。	 是 進一步了解	 是 進一步了解	

AWS 服務	搭配使用的好處 AWS Organizations	支援受信任存取	支援委派的管理員	
AWS CloudFormation Stacksets 以單一操作建立、更新或刪除跨多個帳戶與區域的堆疊。	管理帳戶或委派管理員帳戶中的使用者可以建立具有服務受管許可的堆疊集，將堆疊執行個體部署至組織中的帳戶。	 是 進一步了解	 是 進一步了解	
AWS CloudTrail 針對帳戶啟用監管、合規、操作和風險稽核。	管理帳戶或委派管理員帳戶中的使用者可以建立組織追蹤或事件資料存放區，其中會記錄組織中所有成員帳戶的所有事件。	 是 進一步了解	 是 進一步了解	

AWS 服務	搭配使用的好處 AWS Organizations	支援受信任存取	支援委派的管理員	
AWS Compute Optimizer 取得 AWS 運算最佳化建議。	您可以分析您組織帳戶中的所有資源以獲得最佳化建議。 如需詳細資訊，請參閱AWS Compute Optimizer使用者指南中的Compute Optimizer支援的帳戶。	 是 進一步了解	 是 進一步了解	

AWS 服務	搭配使用的好處 AWS Organizations	支援受信任存取	支援委派的管理員	
AWS Config 評定、稽核和評估 AWS 資源的組態。	您可以取得整個組織的合規狀態檢視。您還可以使用 AWS Config API 操作來管理組織 AWS 帳戶 中所有內容的 AWS Config 規則和一致性套件。 您可以使用委派的管理員帳戶，從 AWS Organizations中組織的所有成員帳戶彙總資源組態與合規資料。如需詳細	 是 進一步了解	 是 進一步了解： Config 規則 一致性套件 多帳戶多區域資料彙整	

AWS 服務	搭配使用的好處 AWS Organizations	支援受信任存取	支援委派的管理員	
	資訊，請參閱 AWS Config《開發人員指南》中的註冊委派管理員。			

AWS 服務	搭配使用的好處 AWS Organizations	支援受信任存取	支援委派的管理員	
AWS Control Tower 設定和管控安全、合規的多帳戶 AWS 環境。	您可以為所有 AWS 資源設置一個 landing zone，這是一個多帳戶環境。此環境包含組織和組織實體。您可以使用此環境對所有 AWS 帳戶. 如需詳細資訊，請參閱 AWS Control Tower 使用者指南中的 如何 AWS Control Tower 以及透過 AWS Organizat	 是 進一步了解	 否	

AWS 服務	搭配使用的好處 AWS Organizations	支援受信任存取	支援委派的管理員	
	ions管理帳戶。			
AWS 成本最佳化中心 收集跨 AWS 最佳化產品的成本建議。	您可以輕鬆識別、篩選和彙總跨 AWS Organizations 會員帳戶和 AWS 區域的 AWS 成本最佳化建議。 如需詳細資訊，請參閱成本最佳化中樞使用者指南中的成本最佳化中樞。	 是 進一步了解		否

AWS 服務	搭配使用的好處 AWS Organizations	支援受信任存取	支援委派的管理員	
Amazon Detective 從日誌資料產生視覺化效果，以便分析、調查並快速識別安全問題清單或可疑活動的根本原因。	您可以將 Amazon Detecess 與整合，AWS Organizations 以確保您的 Detective 行為圖表可讓您查看所有組織帳戶的活動。	 是 進一步了解	 是 進一步了解	

AWS 服務	搭配使用的好處 AWS Organizations	支援受信任存取	支援委派的管理員	
Amazon DevOps 大師 分析營運資料和應用程式指標與事件，以識別與正常操作模式不同的行為。當 DevOps Guru 偵測到操作問題或風險時，使用者會收到通知。	您可以與整合 AWS Organizations 以管理整個組織中所有客戶的見解。您可以委派管理員檢視、排序和篩選來自所有帳戶的洞察，以取得所有受監控應用程式的組織範圍運作狀態。	 是 進一步了解	 是 進一步了解	

AWS 服務	搭配使用的好處 AWS Organizations	支援受信任存取	支援委派的管理員	
AWS Directory Service 在 AWS 雲端中設定和執行目錄，或將您的 AWS 資源與現有的內部部署 Microsoft Active Directory 連線。	您可以 AWS Directory Service 與整合，以 AWS Organizations 便跨多個帳戶和區域中的任何 VPC 進行無縫目錄共用。	 是 進一步了解	 否	

AWS 服務	搭配使用的好處 AWS Organizations	支援受信任存取	支援委派的管理員	
Amazon EventBridge 即時監控您的 AWS 資源和執行 AWS 的應用程式。	您可以在組織中的所有帳戶中啟用共享所有 Amazon CloudWatch 事件，以前是 Amazon 活動。EventBridge 如需詳細資訊，請參閱 Amazon EventBridge 使用者指南 AWS 帳戶中的傳送和接收 Amazon EventBridge 事件。	 否	 否	

AWS 服務	搭配使用的好處 AWS Organizations	支援受信任存取	支援委派的管理員	
AWS Firewall Manager 跨帳戶和應用程式，集中設定和管理 web 應用程式的防火牆規則。	您可以集中配置和管理組織中各帳戶的 AWS WAF 規則。	 是 進一步了解	 是 進一步了解	

AWS 服務	搭配使用的好處 AWS Organizations	支援受信任存取	支援委派的管理員	
Amazon GuardDuty GuardDuty 是一種持續的安全監控服務，用於分析和處理來自各種數據源的信息。它使用威脅智慧饋送和機器學習) 以在您的 AWS 環境中識別意外和可能未經授權且惡意的活動。	您可以指定一個成員帳戶來檢視和管 GuardDuty 理組織中所有帳戶的帳戶。新增成員帳戶會自動啟 GuardDuty 用所選帳戶中的那些帳戶 AWS 區域。您也可以針對新增至組織的新帳戶自動 GuardDuty 啟用。 如需詳細資訊，請參閱 Amazon GuardDuty 使用者指南中	 是 進一步了解	 是 進一步了解	

AWS 服務	搭配使用的好處 AWS Organizations	支援受信任存取	支援委派的管理員	
	的GuardDut和Organizations。			
AWS Health 瞭解可能會影響您的資源效能或 AWS 服務可用性問題的事件。	您可以彙總組織中各帳戶的 AWS Health 事件。	 是 進一步了解	 是 進一步了解	

AWS 服務	搭配使用的好處 AWS Organizations	支援受信任存取	支援委派的管理員	
AWS Identity and Access Management 安全地控制對 AWS 資源的存取。	您可以在 IAM 中使用上次存取的服務資料，以協助您更好地了解整個組織的 AWS 活動。您可以使用此資料來建立和更新服務控制政策 (SCP)，將存取限制在僅限您組織帳戶所用的 AWS 服務。 如需範例，請參閱 IAM 使用者指南中的使用資料來精簡組織	 否	 否	

AWS 服務	搭配使用的好處 AWS Organizations	支援受信任存取	支援委派的管理員	
	單位的許可中的			
IAM Access Analyzer 分析 AWS 環境中以資源為基礎的政策，以識別任何將存取權授與信任區域以外的主體存取權的原則。	您可以將成員帳戶指定為 IAM Access Analyzer 的管理員。 如需詳細資訊，請參閱 IAM 使用者指南中的啟用 Access Analyzer。	 是 進一步了解	 是 進一步了解	

AWS 服務	搭配使用的好處 AWS Organizations	支援受信任存取	支援委派的管理員	
Amazon Inspector 自動掃描 AWS 工作負載中的漏洞，以探索 Amazon ECR 中的 Amazon EC2 執行個體和容器映像，以找出軟體漏洞和意外的網路暴露。	委派管理員啟用或停用成員帳戶掃描、檢視整個組織的彙總問題清單資料、建立和管理隱藏規則。 如需詳細資訊，請參閱《Amazon Inspector 使用者指南》中的使用 AWS Organizations管理多個帳戶。	 是 進一步了解	 是 進一步了解	

AWS 服務	搭配使用的好處 AWS Organizations	支援受信任存取	支援委派的管理員	
AWS License Manager 簡化將軟體授權轉送到雲端的程序。	您可啟用跨帳戶探索組織中的運算資源。	 是 進一步了解	 進一步了解	是

AWS 服務	搭配使用的好處 AWS Organizations	支援受信任存取	支援委派的管理員	
Amazon Macie 使用機器學習探索並分類您的關鍵商業內容，以協助您符合資料安全性和隱私權需求。它會持續評估您儲存在 Amazon S3 中的內容並通知您潛在的問題。	您可以為組織中的所有帳戶設定 Amazon Macie，以便從指定的 Macie 管理員帳戶中，在所有帳戶中的 Amazon S3，取得所有資料的合併檢視。您可以將 Macie 設定為在組織成長時自動保護新帳戶中的資源。系統會警示您修復整個組織中 S3 儲存貯體的	 是 進一步了解	 是 進一步了解	

AWS 服務	搭配使用的好處 AWS Organizations	支援受信任存取	支援委派的管理員	
	政策配置不當。			
AWS Marketplace 經策管數位目錄，您可以用於尋找、購買、部署和管理第三方軟體、資料和服務，而您需要這些軟體、資料和服務，來建置解決方案並執行您的業務。	您可以跨組織中的帳戶共用 AWS Marketplace 訂閱和購買項目的授權。	 是 進一步了解	 否	

AWS 服務	搭配使用的好處 AWS Organizations	支援受信任存取	支援委派的管理員	
AWS Marketplace 私人 Marketplace 為您提供廣泛的產品目錄 AWS Marketplace，以及對這些產品的細粒度控制。	可讓您建立與整個組織、一或多個 OU 或組織中的一或多個帳戶相關聯的多個私人市集體驗，每個帳戶都有自己的核准產品集。您的 AWS 管理員也可以使用公司或團隊的標誌、訊息和色彩配置，將公司品牌套用至每個私人市集體驗。	 是 進一步了解	 是 進一步了解	

AWS 服務	搭配使用的好處 AWS Organizations	支援受信任存取	支援委派的管理員	
AWS Network Manager 可讓您跨 AWS 帳戶、區域和內部部署位置，集中管理 AWS Cloud WAN 核心網路和 AWS Transit Gateway 網路。	您可以在組織內的多個 AWS 帳戶中，利用運輸閘道及其附加資源，集中管理和監控您的全球網路。	 是 進一步了解	 是 進一步了解	

AWS 服務	搭配使用的好處 AWS Organizations	支援受信任存取	支援委派的管理員	
AWS Resource Access Manager 與其他帳號共用您擁有的指定 AWS 資源。	您可以在組織內共用資源，完全無需交換額外的邀請。您可以共享的資源包括 Route 53 解析程式規則、隨需容量保留等。 如需共享容量保留的資訊，請參閱 Amazon EC2 Linux 執行個體使用者指南或 Amazon EC2 Windows 執行個體使用者指南。	 是 進一步了解	 否	

AWS 服務	搭配使用的好處 AWS Organizations	支援受信任存取	支援委派的管理員	
	如需可共享資源的清單，請參閱AWS RAM 使用者指南中的可共享資源。			
AWS 資源總管 在類似網際網路搜尋引擎的體驗中探索您的資源	啟用多帳戶搜尋。	 是 進一步了解	 是 進一步了解	

AWS 服務	搭配使用的好處 AWS Organizations	支援受信任存取	支援委派的管理員	
AWS Security Hub 在中檢視您的安全狀態，AWS 並根據安全性產業標準和最佳實務來檢查您的環境。	您可以為組織的所有帳戶自動啟用 Security Hub，包括新增的新帳戶。這會增加 Security Hub 檢查和問題清單的涵蓋範圍，從而提供更準確的整體安全狀態。	 是 進一步了解	 是 進一步了解	

AWS 服務	搭配使用的好處 AWS Organizations	支援受信任存取	支援委派的管理員	
Amazon S3 Storage Lens 透過可執行的建議來最佳化儲存，取得 Amazon S3 儲存用量和活動指標的可見性。	設定 Amazon S3 Storage Lens 以了解 Amazon S3 儲存用量和活動趨勢，以及針對您組織中所有成員帳戶的建議。	 是 進一步了解	 進一步了解	是
Amazon Security Lake Amazon Security Lake 將來自雲端、內部部署和自訂來源的安全資料，集中到存放在您的帳戶的資料湖中。	建立可跨帳戶收集日誌和事件的資料湖。	 是 進一步了解	 進一步了解	是

AWS 服務	搭配使用的好處 AWS Organizations	支援受信任存取	支援委派的管理員	
AWS Service Catalog 建立和管理已核准在 AWS上使用的 IT 服務型錄。	您可以更輕鬆地跨帳戶複製共用產品組合和複製產品，無需共用產品組合 ID。	 是 進一步了解	 進一步了解	是
Service Quotas 集中檢視和管理您的服務配額 (也稱為限制)。	您可以建立配額請求範本，以便於組織中建立帳戶時自動請求提高配額。	 是 進一步了解		否
AWS IAM Identity Center 為所有帳戶和雲端應用程式提供單一登入存取。	使用者可以使用其公司認證登入 AWS 存取入口網站，並在其指派的管理帳戶或成員帳戶中存取資源。	 是 進一步了解	 進一步了解	是

AWS 服務	搭配使用的好處 AWS Organizations	支援受信任存取	支援委派的管理員	
AWS Systems Manager 啟用 AWS 資源的可見性和控制權。	您可以使用「系統管理員總管」同步處理組織 AWS 帳戶 中所有的作業資料。 您可以使用 Systems Manager 變更管理員，從委派的系統管理員帳戶來管理組織中所有成員帳戶的變更範本、核准和報告。	 是 進一步了解	 是 進一步了解	

AWS 服務	搭配使用的好處 AWS Organizations	支援受信任存取	支援委派的管理員
標籤政策 使用組織帳戶中各資源的標準化標籤。	您可以建立標籤政策來定義特定資源和資源類型的標記規則，並將這些政策連接至組織單位和帳戶，以強制執行這些規則。	 是 進一步了解	 否
AWS Trusted Advisor Trusted Advisor 檢查您的 AWS 環境並在存在機會時提出建議，以節省資金、改善系統可用性和效能，或協助縮小安全性漏洞。	Trusted Advisor 針對組織 AWS 帳戶中的所有項目執行檢查。	 是 進一步了解	 是 進一步了解

AWS 服務	搭配使用的好處 AWS Organizations	支援受信任存取	支援委派的管理員	
AWS Well-Architected Tool 可 AWS Well-Architected Tool 協助您記錄工作負載的狀態，並將它們與最新的 AWS 架構最佳做法進行比較。	可讓 AWS WA Tool 與「組 Organizations」客戶簡化與其組織中其他成員共用 AWS WA Tool 資源的程序。	 是 進一步了解	 否	
Amazon VPC IP 地址管理員 (IPAM) IPAM 是 VPC 功能，可讓您更輕鬆地為工作負載規劃、追蹤和監控 IP 位址。 AWS	監控整個組織的 IP 地址使用情況，並在成員帳戶之間共用 IP 地址集區。	 是 進一步了解	 是 進一步了解	

AWS 服務	搭配使用的好處 AWS Organizations	支援受信任存取	支援委派的管理員	
Amazon VPC Reachability Analyzer Reachability Analyzer 是一種組態分析工具，可讓您在虛擬私有雲端 (VPC) 中的來源資源和目的地資源之間執行連線測試。	追蹤組織中跨帳戶的路徑。	 是 進一步了解	 是 進一步了解	

AWS Account Management 與 AWS Organizations

AWS Account Management 可協助您管理組織內所有 AWS 帳戶 的帳戶資訊和中繼資料。您可以設定、修改或刪除組織每個成員帳戶的替代聯絡人資訊。如需詳細資訊，請參閱 AWS Account Management 使用者指南中的在組織中使用 AWS Account Management。

使用以下資訊可協助整合 AWS Account Management 與 AWS Organizations。

使用 Account Management 啟用受信任存取

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

Account Management 需要對 AWS Organizations 的受信任存取，才能為組織指定成員帳戶作為此服務的委派管理員。

您只能使用 Organizations 工具來啟用受信任存取。

您可以使用 AWS Organizations 主控台，執行 AWS CLI 命令，或呼叫其中一個 AWS 開發套件中的 API 操作，來啟用受信任的存取

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Services (服務) 頁面上，尋找 AWS Account Management 列，選擇服務的名稱，然後選擇 Enable trusted access (啟用受信任存取)。
3. 在確認對話方塊中，啟用顯示啟用受信任存取選項，在方塊中輸入 **enable**，然後選擇啟用受信任的存取。
4. 如果您只是 AWS Organizations 的系統管理員，請告訴 AWS Account Management 的管理員，他們現在可使用其主控台啟用該服務，以便與 AWS Organizations 搭配使用。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以啟用受信任的服務存取：

- AWS CLI: enable-aws-service-access

  您可以執行下列命令來啟用 AWS Account Management 作為 Organizations 受信任的服務。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal account.amazonaws.com
  ```

  此命令成功後就不會產生輸出。
- AWS API: EnableAWSServiceAccess

使用 Account Management 停用受信任存取

如需啟用受信任的存取所需許可的資訊，請參閱停用信任的存取所需的許可。

只有 AWS Organizations 管理帳戶中的管理員才能使用 AWS Account Management 停用受信任的存取。

您只能使用 Organizations 工具來停用受信任的存取。

您可以使用 AWS Organizations 主控台，執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS 開發套件中的 Organizations API 操作，來停用受信任的存取

AWS Management Console

使用 Organizations 主控台來受信停用任的服務存取

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Services (服務) 頁面上，尋找 AWS Account Management 列，然後選擇服務的名稱。
3. 選擇停用受信任的存取。
4. 在確認對話方塊中，輸入 **disable**，然後選擇停用受信任的存取。
5. 如果您只是 AWS Organizations 的系統管理員，請告訴 AWS Account Management 的管理員，他們現在可使用其主控台或工具停用該服務，以便與 AWS Organizations 搭配使用。

AWS CLI, AWS API

使用 Organizations CLI/開發套件來受信停用任的服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以停用信任的服務存取：

- AWS CLI: disable-aws-service-access

  您可以執行下列命令來停用 AWS Account Management 作為 Organizations 受信任的服務。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal account.amazonaws.com
  ```

  此命令成功後就不會產生輸出。
- AWS API：DisableAWSServiceAccess

啟用 Account Management 的委派管理員帳戶

當您將成員帳戶指定為組織的委派管理員時，來自指定帳戶的使用者和角色可以為組織中的其他成員帳戶管理 AWS 帳戶 中繼資料。如果您未啟用委派系統管理員帳戶，則只有組織的管理帳戶才能執行這任務。這可協助您將組織的管理與帳戶詳細資訊的管理分開。

最低許可

只有 Organizations 管理帳戶中的使用者或角色，才能將成員帳戶設定為組織中進行 Account Management 的委派管理員。

如需關於如何設定委派政策的一般指示，請參閱 建立或更新以資源為基礎的委派政策。

AWS CLI, AWS API

如果您想要使用 AWS CLI 或其中一個 AWS SDK，可以使用下列命令：

- AWS CLI:

```
$  aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal account.amazonaws.com
```

- AWS SDK：呼叫 Organizations `RegisterDelegatedAdministrator` 操作和成員帳戶的 ID 號碼，並識別帳戶服務主體 `account.amazonaws.com` 作為參數。

AWS Application Migration Service (MGN) 和 AWS Organizations

AWS Application Migration Service 可簡化、加速並降低將應用程式遷移至 AWS 的成本。透過與 Organizations 整合，您可以使用全域檢視功能來管理跨多個帳戶的大規模遷移。如需詳細資訊，請參閱《MGN 使用者指南》中的「設定您的 AWS Organizations」。

使用以下資訊可協助您整合 AWS Application Migration Service 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下服務連結角色。該角色允許 MGN 在您組織的組織帳戶中執行支援的操作。

只有在您停用 MGN 和 Organizations 之間的受信任存取，或者從組織中刪除成員帳戶時，才能移除或修改此角色。

- `AWSServiceRoleForApplicationMigrationService`

MGN 使用的服務主體

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。MGN 使用的服務連結角色會將存取權授予下列服務委託人：

- mgn.amazonaws.com

使用 MGN 啟用受信任的存取

當您使用 MGN 啟用受信任存取時，您可以使用全域檢視功能，讓您管理跨多個帳戶的大規模遷移。全域檢視提供可見度，並能夠在不同 AWS 帳戶中的來源伺服器、應用程式和波紋上執行特定動作。如需詳細資訊，請參閱《AWS Application Migration Service 使用者指南》中的「設定您的 AWS Organizations」。

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

您可以使用 AWS Application Migration Service 主控台或 AWS Organizations 主控台來啟用受信任存取。

> **Important**
>
> 強烈建議您盡可能使用 AWS Application Migration Service 主控台或工具來啟用與 Organizations 整合。這可讓 AWS Application Migration Service 執行其需要的任何組態，例如建立服務所需的資源。只有在您無法使用 AWS Application Migration Service 提供的工具啟用整合時，才能繼續執行這些步驟。如需詳細資訊，請參閱本說明。
> 如果您使用 AWS Application Migration Service 主控台或工具啟用受信任存取，則不需要完成這些步驟。

您可以使用 AWS Organizations 主控台，執行 AWS CLI 命令，或呼叫其中一個 AWS SDK 中的 API 操作，來啟用受信任存取。

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。

2. 在 服務 頁面上，尋找 AWS Application Migration Service 的橫列，選擇服務的名稱，然後選擇啟用受信任存取。
3. 在確認對話方塊中，啟用顯示啟用受信任存取選項，在方塊中輸入 **enable**，然後選擇啟用受信任的存取。
4. 如果您只是 AWS Organizations 的系統管理員，請告訴 AWS Application Migration Service 的管理員，他們現在可使用其主控台啟用該服務，以便與 AWS Organizations 搭配使用。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以啟用受信任的服務存取：

- AWS CLI: enable-aws-service-access

  您可以執行下列命令來啟用 AWS Application Migration Service 作為 Organizations 受信任服務。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal mgn.amazonaws.com
  ```

  此命令成功後就不會產生輸出。
- AWS API: EnableAWSServiceAccess

使用 MGN 停用受信任存取

只有 Organizations 管理帳戶中的管理員才能使用 MGN 停用受信任的存取。

您可以使用 AWS Application Migration Service 或 AWS Organizations 工具停用受信任存取。

> **Important**
>
> 強烈建議您盡可能使用 AWS Application Migration Service 主控台或工具來停用與 Organizations 整合。這可讓 AWS Application Migration Service 執行其所需的任何清除，例如刪除服務不再需要的資源或存取角色。只有在您無法使用 AWS Application Migration Service 提供的工具停用整合時，才能繼續執行這些步驟。
> 如果您使用 AWS Application Migration Service 主控台或工具停用受信任存取，則不需要完成這些步驟。

您可以使用 AWS Organizations 主控台，執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDK 中的 Organizations API 操作，來停用受信任存取。

AWS Management Console

使用 Organizations 主控台來受信停用任的服務存取

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在服務頁面上，尋找 AWS Application Migration Service，然後選擇服務的名稱。
3. 選擇停用受信任的存取。
4. 在確認對話方塊中，輸入 **disable**，然後選擇停用受信任的存取。
5. 如果您只是 AWS Organizations 的系統管理員，請告訴 AWS Application Migration Service 的管理員，他們現在可使用其主控台或工具停用該服務，以便與 AWS Organizations 搭配使用。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以停用信任的服務存取：

- AWS CLI: disable-aws-service-access

  您可以執行下列命令來停用 AWS Application Migration Service 作為 Organizations 受信任服務。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal mgn.amazonaws.com
  ```

  此命令成功後就不會產生輸出。

- AWS API：DisableAWSServiceAccess

啟用 MGN 的委派管理員帳戶

當您將成員帳戶指定為組織的委派管理員時，該帳戶的使用者和角色可以對 MGN 執行管理動作，否則只能由組織管理帳戶中的使用者或角色執行。這可協助您將組織的管理與 MGN 的管理分開。如需詳細資訊，請參閱《MGN 使用者指南》中的「設定您的 AWS Organizations」。

最低許可

只有 Organizations 管理帳戶中的使用者或角色，才能將成員帳戶設定為組織中 MGN 的委派管理員

AWS CLI, AWS API

如果您想要使用 AWS CLI 或其中一個 AWS SDK，可以使用下列命令：

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal mgn.amazonaws.com
```

- AWS SDK：呼叫 Organizations `RegisterDelegatedAdministrator` 操作和成員帳戶的 ID 號碼，並識別帳戶服務 `mgn.amazonaws.com` 作為參數。

停用 MGN 的委派管理員

只有組織管理帳戶中的管理員可以移除 MGN 的委派管理員。您可以使用 Organizations `DeregisterDelegatedAdministrator` CLI 或 SDK 操作來移除委派管理員。

AWS Artifact 與 AWS Organizations

AWS Artifact 是一項服務，可讓您下載 AWS 安全合規報告，例如 ISO 和 PCI 報告。使用 AWS Artifact，組織管理帳戶中的使用者可以代表組織中的所有成員帳戶自動接受協議，甚至是在新增了新報告和帳戶時。成員帳戶使用者可以檢視和下載協議。如需詳細資訊，請參閱AWS Artifact使用者指南中的管理 AWS Artifact 中多個帳戶的合約。

使用以下資訊可協助整合 AWS Artifact 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下服務連結角色。該角色允許 AWS Artifact 在您組織的組織帳戶中執行支援的操作。

只有在您停用 AWS Artifact 和 Organizations 之間的受信任存取，或者從組織中刪除成員帳戶時，才能移除或修改此角色。

雖然如果您從組織中移除成員帳戶就能刪除或修改此角色，但我們不建議這樣做。

不建議修改角色，因為其可能會導致安全問題，如跨服務混淆代理人。如需進一步了解如何預防混淆代理人，請參閱《AWS Artifact 使用者指南》中的預防跨服務代理人。

- `AWSServiceRoleForArtifact`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。AWS Artifact 使用的服務連結角色會將存取權授予下列服務委託人：

- `artifact.amazonaws.com`

使用 AWS Artifact 啟用受信任的存取

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

您只能使用 Organizations 工具來啟用受信任存取。

您可以使用 AWS Organizations 主控台，執行 AWS CLI 命令，或呼叫其中一個 AWS 開發套件中的 API 操作，來啟用受信任的存取

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Services (服務) 頁面上，尋找 AWS Artifact 列，選擇服務的名稱，然後選擇 Enable trusted access (啟用受信任存取)。
3. 在確認對話方塊中，啟用顯示啟用受信任存取選項，在方塊中輸入 **`enable`**，然後選擇啟用受信任的存取。
4. 如果您只是 AWS Organizations 的系統管理員，請告訴 AWS Artifact 的管理員，他們現在可使用其主控台啟用該服務，以便與 AWS Organizations 搭配使用。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以啟用受信任的服務存取：

- AWS CLI: enable-aws-service-access

  您可以執行下列命令來啟用 AWS Artifact 作為 Organizations 受信任的服務。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal artifact.amazonaws.com
  ```

  此命令成功後就不會產生輸出。
- AWS API: EnableAWSServiceAccess

使用 AWS Artifact 停用受信任的存取

如需啟用受信任的存取所需許可的資訊，請參閱停用信任的存取所需的許可。

只有 AWS Organizations 管理帳戶中的管理員才能使用 AWS Artifact 停用受信任的存取。

您只能使用 Organizations 工具來停用受信任的存取。

AWS Artifact 需要 AWS Organizations 的受信任的存取才能處理組織協議。如果您在使用 AWS Artifact 進行組織協議時使用 AWS Organizations 停用信任的存取，它會停止運作，因為它無法存取組織。您在 AWS Artifact 中接受的任何組織協議會保留，但無法供 AWS Artifact 存取。AWS Artifact 建立的 AWS Artifact 角色仍然存在。如果您之後重新啟用信任的存取，AWS Artifact 會繼續如之前般運作，而不需重新設定服務。

從組織移除的獨立帳戶不再可存取任何組織協議。

您可以使用 AWS Organizations 主控台，執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS 開發套件中的 Organizations API 操作，來停用受信任的存取

AWS Management Console

使用 Organizations 主控台來受信停用任的服務存取

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Services (服務) 頁面上，尋找 AWS Artifact 列，然後選擇服務的名稱。
3. 選擇停用受信任的存取。

4. 在確認對話方塊中，輸入 **disable**，然後選擇停用受信任的存取。
5. 如果您只是 AWS Organizations 的系統管理員，請告訴 AWS Artifact 的管理員，他們現在可使用其主控台或工具停用該服務，以便與 AWS Organizations 搭配使用。

AWS CLI, AWS API

使用 Organizations CLI/開發套件來受信停用任的服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以停用信任的服務存取：

- AWS CLI: disable-aws-service-access

  您可以執行下列命令來停用 AWS Artifact 作為 Organizations 受信任的服務。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal artifact.amazonaws.com
  ```

  此命令成功後就不會產生輸出。
- AWS API：DisableAWSServiceAccess

啟用 AWS Artifact 的委派管理員帳戶

若要瞭解如何為 AWS Artifact 啟用委派管理員，請參閱AWS Artifact。

AWS Audit Manager 與 AWS Organizations

AWS Audit Manager 可協助您持續稽核 AWS 使用情況，以簡化評定風險與法規與業界標準的法規遵循方式。Audit Manager 會自動化證據收集，讓您更容易評定您的政策、程序和活動是否有效運作。需要稽核時，Audit Manager 可協助您管理對控制的利害關係人審查，並協助您以較少的手動工作來建立稽核就緒報表。

當您將 Audit Manager 與 AWS Organizations 整合時，可以透過在您的評定範圍內包含您組織的多個 AWS 帳戶，從更廣泛的來源收集證據。

如需詳細資訊，請參閱 Audit Manager 使用者指南中的啟用 AWS Organizations。

使用以下資訊可協助整合 AWS Audit Manager 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下服務連結角色。該角色允許 Audit Manager 在您組織的組織帳戶中執行支援的操作。

只有在您停用 Audit Manager 和 Organizations 之間的受信任存取，或者從組織中刪除成員帳戶時，才能移除或修改此角色。

如需 Audit Manager 如何使用此角色的詳細資訊，請參閱AWS Audit Manager使用者指南中的使用服務連結角色。

- `AWSServiceRoleForAuditManager`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。Audit Manager 使用的服務連結角色會將存取權授予下列服務委託人：

- `auditmanager.amazonaws.com`

使用 Audit Manager 來啟用受信任的存取

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

Audit Manager 需要對 AWS Organizations 的受信任存取，才能將成員帳戶指定為組織的委派管理員。

您可以使用 AWS Audit Manager 主控台或 AWS Organizations 主控台來啟用信任存取。

> **Important**
>
> 強烈建議您盡可能使用 AWS Audit Manager 主控台或工具來啟用與 Organizations 整合。這可讓 AWS Audit Manager 執行其需要的任何組態，例如建立服務所需的資源。只有在您無法使用 AWS Audit Manager 提供的工具啟用整合時，才能繼續執行這些步驟。如需詳細資訊，請參閱本說明。
>
> 如果您使用 AWS Audit Manager 主控台或工具啟用受信任存取，則不需要完成這些步驟。

使用 Audit Manager 主控台來啟用受信任的存取

如需啟用受信任存取的相關指示，請參閱AWS Audit Manager使用者指南中的設定。

> **Note**
>
> 如果您使用 AWS Audit Manager 主控台設定委派管理員，則 AWS Audit Manager 會自動為您啟用受信任的存取。

您可以執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS 開發套件中的 Organizations API 操作，來啟用受信任的存取

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以啟用受信任的服務存取：

- AWS CLI: enable-aws-service-access

  您可以執行下列命令來啟用 AWS Audit Manager 作為 Organizations 受信任的服務。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal auditmanager.amazonaws.com
  ```

  此命令成功後就不會產生輸出。
- AWS API: EnableAWSServiceAccess

使用 Audit Manager 來停用受信任的存取

如需啟用受信任的存取所需許可的資訊，請參閱停用信任的存取所需的許可。

只有 AWS Organizations 管理帳戶中的管理員才能使用 AWS Audit Manager 停用受信任的存取。

您只能使用 Organizations 工具來停用受信任的存取。

您可以執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDK 中的 Organizations API 操作，來停用受信任存取。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以停用信任的服務存取：

- AWS CLI: disable-aws-service-access

  您可以執行下列命令來停用 AWS Audit Manager 作為 Organizations 受信任的服務。

```
$ aws organizations disable-aws-service-access \
    --service-principal auditmanager.amazonaws.com
```

  此命令成功後就不會產生輸出。

- AWS API：DisableAWSServiceAccess

為 Audit Manager 啟用委派的管理員帳戶

當您將成員帳戶指定為組織的委派管理員時，該帳戶的使用者和角色可以對 Audit Manager 執行管理動作，否則只能由組織管理帳戶中的使用者或角色執行。這可協助您將組織的管理與 Audit Manager 的管理分開。

> **最低許可**
>
> 只有具有下列許可之 Organizations 管理帳戶中的使用者或角色，才能將成員帳戶設定為組織中 Audit Manager 的委託管理員：
> `audit-manager:RegisterAccount`

如需啟用 Audit Manager 委派管理員帳戶的指示，請參閱AWS Audit Manager使用者指南中的設定。

如果您使用 AWS Audit Manager 主控台設定委派管理員，則 Audit Manager 會自動為您啟用受信任的存取。

AWS CLI, AWS API

如果您想要使用 AWS CLI 或其中一個 AWS SDK，可以使用下列命令：

- AWS CLI:

```
$  aws audit-manager register-account \
    --delegated-admin-account 123456789012
```

- AWS SDK：呼叫 `RegisterAccount` 操作並提供 `delegatedAdminAccount` 作為參數，以委派系統管理員帳戶。

AWS Backup 與 AWS Organizations

AWS Backup 這項服務可讓您管理和監視組織中的 AWS Backup 任務。如果您以組織管理帳戶的使用者身分登入，則可以使用 AWS Backup 來啟用整個組織的備份保護和監控。此服務可協助您使用備份政策，將 AWS Backup 計劃集中套用至組織中所有帳戶的資源，以達成合規性。AWS Backup 和 AWS Organizations 一起使用時有下列好處：

保護

您可以在組織中啟用備份政策類型，然後建立備份政策以連接至組織的根、OU 或帳戶。備份政策會將 AWS Backup 計劃與自動將計劃套用至帳戶所需的其他詳細資訊結合起來。直接連接至帳戶的政策會與繼承自組織根和任何父 OU 的政策合併，以建立套用至帳戶的有效政策。政策包含 IAM 角色的 ID，該角色具有對帳戶中的資源執行 AWS Backup 的許可。AWS Backup 使用 IAM 角色，依有效政策中的備份計劃所規定，代表您執行備份。

監控

當您在組織中啟用 AWS Backup 受信任的存取時，您可以使用 AWS Backup 主控台，檢視組織中任何帳戶中的備份、還原和複製任務的詳細資訊。如需詳細資訊，請參閱AWS Backup開發人員指南中的監控您的備份任務。

如需 AWS Backup 的詳細資訊，請參閱《AWS Backup 開發人員指南》。

使用以下資訊可協助整合 AWS Backup 與 AWS Organizations。

使用 AWS Backup 啟用受信任的存取

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

您可以使用 AWS Backup 主控台或 AWS Organizations 主控台來啟用信任存取。

> **Important**
>
> 強烈建議您盡可能使用 AWS Backup 主控台或工具來啟用與 Organizations 整合。這可讓 AWS Backup 執行其需要的任何組態，例如建立服務所需的資源。只有在您無法使用 AWS Backup 提供的工具啟用整合時，才能繼續執行這些步驟。如需詳細資訊，請參閱本說明。

如果您使用 AWS Backup 主控台或工具啟用受信任存取，則不需要完成這些步驟。

若要使用 AWS Backup啟用受信任存取，請參閱AWS Backup開發人員指南中的在多個 AWS 帳戶 中啟用備份。

使用 AWS Backup 停用受信任的存取

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

AWS Backup 需要有 AWS Organizations 受信任的存取，才能監控組織帳戶的備份、還原和複製任務。如果您停用 AWS Backup 受信任的存取，則無法檢視目前帳戶外面的任務。AWS Backup 建立的 AWS Backup 角色仍然存在。如果您後來重新啟用信任的存取，AWS Backup 會像以前一樣繼續運作，您不需重新設定服務。

您只能使用 Organizations 工具來停用受信任的存取。

您可以執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDK 中的 Organizations API 操作，來停用受信任存取。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以停用信任的服務存取：

- AWS CLI: disable-aws-service-access

  您可以執行下列命令來停用 AWS Backup 作為 Organizations 受信任的服務。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal backup.amazonaws.com
  ```

  此命令成功後就不會產生輸出。
- AWS API：DisableAWSServiceAccess

啟用 AWS Backup 的委派管理員帳戶

請參閱《AWS Backup 開發人員指南》中的委派管理員。

AWS CloudFormation StackSet 和 AWS Organizations

AWS CloudFormation StackSet 可讓您以單一操作來建立、更新或刪除跨多個 AWS 帳戶 和 AWS 區域 的堆疊。StackSets 與 AWS Organizations 整合，可讓您使用每個成員帳戶中具有相關許可的服務連結角色，建立具有服務管理許可的堆疊集。這可讓您將堆疊執行個體部署至組織中的成員帳戶。您不必建立必要的 AWS Identity and Access Management 角色；StackSets 會代表您在每個成員帳戶中建立 IAM 角色。

您可以選擇自動部署到未來新增至組織的帳戶。啟用自動部署後，關聯堆疊集執行個體的角色和部署會自動新增至未來在該 OU 中新增的所有帳戶。

啟用 StackSets 和 Organizations 之間的受信任存取後，管理帳戶會擁有為您的組織建立和管理堆疊集的許可。管理帳戶最多可將五個成員帳戶註冊為委派管理員。啟用受信任存取之後，委派管理員也會擁有為您的組織建立和管理堆疊集的許可。具有服務管理許可的堆疊集是在管理帳戶中建立的，包括由委派管理員建立的堆疊集。

> **Important**
>
> 委派管理員具有部署至組織中帳戶的完整許可。管理帳戶無法限制部署至特定 OU 或執行特定堆疊集操作的委派管理員許可。

如需整合 StackSets 與 Organizations 的詳細資訊，請參閱AWS CloudFormation使用者指南中的使用 AWS CloudFormation StackSets。

使用以下資訊可協助整合 AWS CloudFormation StackSets 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下服務連結角色。該角色允許 AWS CloudFormation Stacksets 在您組織的組織帳戶中執行支援的操作。

只有在您停用 AWS CloudFormation Stacksets 和 Organizations 之間的受信任存取，或者從組織中刪除成員帳戶時，才能移除或修改此角色。

- 管理帳戶：`AWSServiceRoleForCloudFormationStackSetsOrgAdmin`

若要為您組織中的成員帳戶建立服務連結角色 `AWSServiceRoleForCloudFormationStackSetsOrgMember`，您需要先在管理帳戶中建立堆疊集。此將建立一個堆疊集執行個體，然後在成員帳戶中建立角色。

- 成員帳戶：`AWSServiceRoleForCloudFormationStackSetsOrgMember`

如需建立堆疊集的詳細資訊，請參閱《AWS CloudFormation 使用者指南》中的使用 AWS CloudFormation StackSets。

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。AWS CloudFormation Stacksets 使用的服務連結角色會將存取權授予下列服務委託人：

- 管理帳戶：`stacksets.cloudformation.amazonaws.com`

  只有在您停用 StackSets 和 Organizations 之間的受信任存取時，才能修改或刪除此角色。
- 成員帳戶：`member.org.stacksets.cloudformation.amazonaws.com`

  只有在您首先停用 StackSets 和 Organizations 之間的受信任存取，或者首先從目標組織或組織單位 (OU) 中移除帳戶時，才能從帳戶中修改或刪除此角色。

使用 AWS CloudFormation Stacksets 啟用受信任的存取

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

只有組織管理帳戶中的管理員，才具有使用其他 AWS 服務啟用受信任存取的許可。您可以使用 AWS CloudFormation 主控台或 Organizations 主控台來啟用信任存取。

您可以僅使用 AWS CloudFormation StackSets 啟用受信任存取。

若要使用 AWS CloudFormation Stacksets 主控台啟用受信任存取，請參閱 AWS CloudFormation 使用者指南中的使用 AWS Organizations 啟用受信任存取。

使用 AWS CloudFormation Stacksets 停用受信任的存取

如需啟用受信任的存取所需許可的資訊，請參閱停用信任的存取所需的許可。

只有 Organizations 管理帳戶中的管理員，才具有使用其他 AWS 服務停用受信任存取的許可。您只能使用 Organizations 主控台來停用受信任的存取。如果您在使用 StackSets 時停用 Organizations 的受

信任存取，則會保留所有先前建立的堆疊執行個體。不過，使用服務連結角色許可部署的堆疊集，無法再對 Organizations 管理的帳戶執行部署。

您可以使用 AWS CloudFormation 主控台或 Organizations 主控台來停用受信任存取。

> **Important**
>
> 如果您以程式設計的方式停用受信任存取 (例如使用 AWS CLI 或 API)，請注意到這將會移除許可。最好使用 AWS CloudFormation 主控台停用受信任存取。

您可以使用 AWS Organizations 主控台，執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS 開發套件中的 Organizations API 操作，來停用受信任的存取

AWS Management Console

使用 Organizations 主控台來受信停用任的服務存取

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Services (服務) 頁面上，尋找 AWS CloudFormation StackSets 列，然後選擇服務的名稱。
3. 選擇停用受信任的存取。
4. 在確認對話方塊中，輸入 **`disable`**，然後選擇停用受信任的存取。
5. 如果您只是 AWS Organizations 的管理員，請告訴 AWS CloudFormation StackSets 的管理員，他們現在可使用其主控台或工具停止該服務與 AWS Organizations 搭配使用。

AWS CLI, AWS API

使用 Organizations CLI/開發套件來受信停用任的服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以停用信任的服務存取：

- AWS CLI: disable-aws-service-access

  您可以執行下列命令來停用 AWS CloudFormation StackSets，作為 Organizations 受信任的服務。

```
$ aws organizations disable-aws-service-access \
    --service-principal stacksets.cloudformation.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API：DisableAWSServiceAccess

啟用 AWS CloudFormationStackset 的委派管理員帳戶

當您將成員帳戶指定為組織的委派管理員時，該帳戶的使用者和角色可以對 AWS CloudFormation Stacksets 執行管理動作，否則只能由組織管理帳戶中的使用者或角色執行。這可協助您將組織的管理與 AWS CloudFormation Stacksets 的管理分開。

如需如何將成員帳戶指定為組織中 AWS CloudFormation Stacksets 的堆疊集，請參閱AWS CloudFormation使用者指南中的註冊委派管理員。

AWS CloudTrail 和 AWS Organizations

AWS CloudTrail 是一項 AWS 服務，可協助您啟用 AWS 帳戶. 使用管理帳戶中的使用者可以建立組織追蹤 AWS CloudTrail，以記錄該組織 AWS 帳戶 中所有人的所有事件。組織線索會自動套用到組織中的所有成員帳戶。成員帳戶可以查看組織線索，但無法進行修改或刪除。依預設，成員帳戶無法存取在 Amazon S3 儲存貯體中組織追蹤的日誌檔案。這個做法可協助您統一套用並強制執行組織中帳戶的事件日誌策略。

如需詳細資訊，請參閱AWS CloudTrail 使用者指南中的建立組織追蹤。

請使用下列資訊來協助您 AWS CloudTrail 與整合 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下服務連結角色。此角色可 CloudTrail 讓您在組織中的組織帳戶內執行支援的作業。

只有在您停用 CloudTrail 和 Organizations 之間的受信任存取，或者從組織中刪除成員帳戶時，才能移除或修改此角色。

- `AWSServiceRoleForCloudTrail`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。將存取 CloudTrail 權授與下列服務主體所使用的服務連結角色：

- `cloudtrail.amazonaws.com`

使用 CloudTrail 啟用受信任的存取

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

如果您透過從 AWS CloudTrail 主控台建立追蹤來啟用受信任的存取，則會自動為您設定受信任的存取 (建議使用)。您也可以使用 AWS Organizations 控制台啟用受信任的存取。您必須使用 AWS Organizations 管理帳戶登入才能建立組織追蹤。

如果您選擇使用 AWS CLI 或 AWS API 建立組織追蹤，則必須手動設定受信任的存取。 CloudTrail 如需詳細資訊，請參閱《AWS CloudTrail 使用指南》 AWS Organizations中的「啟用為信任的服務」。

> **Important**
>
> 我們強烈建議您盡可能使用 AWS CloudTrail 主控台或工具來啟用與 Organizations 的整合。

您可以執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDK 中的 Organizations API 作業，以啟用受信任的存取。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

您可以使用下列 AWS CLI 命令或 API 作業來啟用受信任的服務存取：

- AWS CLI: enable-aws-service-access

  您可以執行下列命令， AWS CloudTrail 以啟用 Organizations 的信任服務。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal cloudtrail.amazonaws.com
  ```

  此命令成功後就不會產生輸出。
- AWS API：啟用 AWSServiceAccess

使用 CloudTrail 停用受信任的存取

如需啟用受信任的存取所需許可的資訊，請參閱停用信任的存取所需的許可。

AWS CloudTrail 需要受信任的存取權，才 AWS Organizations 能使用組織追蹤和組織事件資料存放區。如果您在使用 AWS Organizations 時停用受信任的存取權 AWS CloudTrail，則會刪除成員帳戶的所有組織軌跡，因為 CloudTrail 無法存取組織。所有管理帳戶組織追蹤和組織事件資料存放區都會轉換為帳戶層級追蹤和事件資料存放區。為在帳戶之間進行整合而建立的`AWSServiceRoleForCloudTrail`角色， CloudTrail 並 AWS Organizations 保留在帳戶中。如果您重新啟用受信任的存取， CloudTrail 將不會對現有追蹤和事件資料存放區採取動作。管理帳戶必須更新任何帳戶層級追蹤和事件資料存放區，才能將其套用至組織。

若要將帳戶層級追蹤或事件資料倉庫轉換為組織追蹤或組織事件資料倉庫，請執行下列操作：

- 從 CloudTrail 主控台更新追蹤或事件資料存放區，然後選擇 [為組織中的所有帳戶啟用] 選項。
- 從中 AWS CLI，執行下列操作：
  - 若要更新系統線，請執行update-trail指令並包含`--is-organization-trail`參數。
  - 若要更新事件資料倉庫，請執行update-event-data-store指令並包含`--organization-enabled`參數。

只有 AWS Organizations 管理帳戶中的系統管理員可以使用停用受信任的存取 AWS CloudTrail。您只能使用 Organizations 工具停用受信任的存取，使用 AWS Organizations 主控台、執行 Organizations AWS CLI 命令，或在其中一個 AWS SDK 中呼叫 Organizations API 作業。

您可以使用 AWS Organizations 主控台、執行 Organizations AWS CLI 命令或呼叫其中一個 AWS SDK 中的 Organizations API 作業來停用受信任的存取。

AWS Management Console

使用 Organizations 主控台來受信停用任的服務存取

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Services (服務) 頁面上，尋找 AWS CloudTrail 列，然後選擇服務的名稱。
3. 選擇停用受信任的存取。
4. 在確認對話方塊中，輸入 **`disable`**，然後選擇停用受信任的存取。
5. 如果您只是管理員，請告訴管理員 AWS Organizations，他們現在可以使用其主控台或工具停用該服務，無法使用該服務 AWS Organizations。 AWS CloudTrail

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

您可以使用下列 AWS CLI 命令或 API 作業來停用受信任的服務存取：

- AWS CLI: disable-aws-service-access

  您可以執行下列命令，將 AWS CloudTrail 其停用為「Organizations」的信任服務。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal cloudtrail.amazonaws.com
  ```

  此命令成功後就不會產生輸出。

- AWS API：停用 AWSServiceAccess

啟用委派管理員帳戶 CloudTrail

當您與 Organization CloudTrail 搭配使用時，您可以註冊組織內的任何帳戶，以擔任 CloudTrail 委派管理員，以代表組織管理組織的追蹤和事件資料存放區。委派的系統管理員是組織中的成員帳戶，可以執行與管理帳戶相同的管理工 CloudTrail 作。

> **最低許可**
>
> 只有「Organizations」管理帳戶中的管理員可以為其註冊委派的管理員 CloudTrail。

您可以使用 CloudTrail 主控台或使用 Organizations `RegisterDelegatedAdministrator` CLI 或 SDK 作業來註冊委派的系統管理員帳戶。若要使用 CloudTrail 主控台註冊委派的管理員，請參閱新增 CloudTrail 委派的管理員。

停用的委派管理員 CloudTrail

只有「Organizations」管理帳戶中的管理員可以移除的委派管理員 CloudTrail。您可以使用 CloudTrail 主控台或使用 Organizations `DeregisterDelegatedAdministrator` CLI 或 SDK 作業來移除委派的系統管理員。如需如何使用 CloudTrail 主控台移除委派系統管理員的相關資訊，請參閱移除 CloudTrail 委派的系統管理員。

AWS Compute Optimizer 與 AWS Organizations

AWS Compute Optimizer 是一項可分析 AWS 資源組態和使用率指標的服務。資源範例包括 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體和 Auto Scaling 群組。Compute Optimizer 會報告您的資源是否最佳化並產生最佳化推薦，以降低成本並改善工作負載的效能。如需有關 Compute Optimizer 的詳細資訊，請參閱AWS Compute Optimizer使用者指南。

使用以下資訊可協助整合 AWS Compute Optimizer 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下服務連結角色。該角色允許 Compute Optimizer 在您組織的組織帳戶中執行支援的操作。

只有在您停用 Compute Optimizer 和 Organizations 之間的信任存取，或從組織中移除成員帳戶時，才能移除或修改此角色。

- `AWSServiceRoleForComputeOptimizer`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。Compute Optimizer 使用的服務連結角色會將存取權授予下列服務委託人：

- `compute-optimizer.amazonaws.com`

使用 Compute Optimizer 來啟用受信任存取

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

您可以使用 AWS Compute Optimizer 主控台或 AWS Organizations 主控台來啟用信任存取。

> **Important**
>
> 強烈建議您盡可能使用 AWS Compute Optimizer 主控台或工具來啟用與 Organizations 整合。這可讓 AWS Compute Optimizer 執行其需要的任何組態，例如建立服務所需的資源。只有在您無法使用 AWS Compute Optimizer 提供的工具啟用整合時，才能繼續執行這些步驟。如需詳細資訊，請參閱本說明。

如果您使用 AWS Compute Optimizer 主控台或工具啟用受信任存取，則不需要完成這些步驟。

使用 Compute Optimizer 主控台來啟用受信任存取

您必須使用組織的管理帳戶登入 Compute Optimizer 主控台。請遵循AWS Compute Optimizer使用者指南中的選擇加入您的帳戶，代表您的組織選擇加入。

您可以使用 AWS Organizations 主控台，執行 AWS CLI 命令，或呼叫其中一個 AWS 開發套件中的 API 操作，來啟用受信任的存取

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Services (服務) 頁面上，尋找 AWS Compute Optimizer 列，選擇服務的名稱，然後選擇 Enable trusted access (啟用受信任存取)。
3. 在確認對話方塊中，啟用顯示啟用受信任存取選項，在方塊中輸入 **enable**，然後選擇啟用受信任的存取。
4. 如果您只是 AWS Organizations 的系統管理員，請告訴 AWS Compute Optimizer 的管理員，他們現在可使用其主控台啟用該服務，以便與 AWS Organizations 搭配使用。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以啟用受信任的服務存取：

- AWS CLI: enable-aws-service-access

  您可以執行下列命令來啟用 AWS Compute Optimizer 作為 Organizations 受信任的服務。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal compute-optimizer.amazonaws.com
  ```

  此命令成功後就不會產生輸出。

- AWS API: EnableAWSServiceAccess

使用 Compute Optimizer 來停用受信任存取

如需啟用受信任的存取所需許可的資訊，請參閱停用信任的存取所需的許可。

只有 AWS Organizations 管理帳戶中的管理員才能使用 AWS Compute Optimizer 停用受信任的存取。

您可以執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS 開發套件中的 Organizations API 操作，來停用受信任的存取

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以停用信任的服務存取：

- AWS CLI: disable-aws-service-access

  您可以執行下列命令來停用 AWS Compute Optimizer 作為 Organizations 受信任的服務。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal compute-optimizer.amazonaws.com
  ```

  此命令成功後就不會產生輸出。
- AWS API：DisableAWSServiceAccess

啟用 Compute Optimizer 的委派管理員帳戶

當您將成員帳戶指定為組織的委派管理員時，來自指定帳戶的使用者和角色可以為組織中的其他成員帳戶管理 AWS 帳戶 中繼資料。如果您未啟用委派系統管理員帳戶，則只有組織的管理帳戶才能執行這任務。這可協助您將組織的管理與帳戶詳細資訊的管理分開。

> **最低許可**
>
> 只有 Organizations 管理帳戶中的使用者或角色，才能將成員帳戶設定為組織中 Compute Optimizer 的委派管理員

如需啟用 Compute Optimizer 委派管理員帳戶的說明，請參閱《AWS Compute Optimizer 使用者指南》中的 https://docs.aws.amazon.com/compute-optimizer/latest/ug/delegate-administrator-account.html。

AWS CLI, AWS API

如果您想要使用 AWS CLI 或其中一個 AWS SDK，可以使用下列命令：

- AWS CLI:

```
$  aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal compute-optimizer.amazonaws.com
```

- AWS SDK：呼叫 Organizations `RegisterDelegatedAdministrator` 操作和成員帳戶的 ID 號碼，並識別帳戶服務主體 `account.amazonaws.com` 作為參數。

停用 Compute Optimizer 的委派管理員帳戶

只有組織管理帳戶中的管理員可以設定 Compute Optimizer 的委派管理員。

若要使用 Compute Optimizer 主控台停用委派管理員 Compute Optimizer 帳戶，請參閱《AWS Compute Optimizer 使用者指南》中的 https://docs.aws.amazon.com/compute-optimizer/latest/ug/delegate-administrator-account.html。

若要使用 AWS AWS CLI 移除委派管理員，請參閱 AWS AWS CLI 命令參考中的 deregister-delegated-administrator。

AWS Config 與 AWS Organizations

AWS Config 中的多帳戶多區域資料彙總可讓您將多個帳戶和 AWS 區域 的 AWS Config 資料彙總至單一帳戶。多帳戶多區域資料彙總對中央 IT 管理員監控企業中多個 AWS 帳戶 的合規性非常有用。彙整工具是 AWS Config 中的資源類型，可收集多個來源帳戶和區域的 AWS Config 資料。在您要查看彙整 AWS Config 資料的區域中建立彙整工具。建立彙總工具時，您可以選擇新增個別帳戶 ID 或您的組織。如需 AWS Config 的詳細資訊，請參閱《AWS Config 開發人員指南》。

您也可以使用 AWS Config API 來管理組織內所有 AWS 帳戶 的 AWS Config 規則：如需詳細資訊，請參閱AWS Config開發人員指南中的啟用組織中所有帳戶的 AWS Config 規則。

使用以下資訊可協助整合 AWS Config 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的帳戶中建立以下服務連結角色。該角色允許 AWS Config 在您組織的帳戶中執行支援的操作。

- `AWSServiceRoleForConfig`

您透過建立多帳戶彙總工具在組織中啟用 AWS Config 時，會創建該角色。AWS Config 會要求您選擇或建立一個角色，並讓您提供名稱。沒有自動產生的名稱。

只有在您停用 AWS Config 和 Organizations 之間的受信任存取，或者從組織中刪除成員帳戶時，才能移除或修改此角色。

使用 AWS Config 啟用受信任的存取

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

您可以使用 AWS Config 主控台或 AWS Organizations 主控台來啟用信任存取。

> **Important**
>
> 強烈建議您盡可能使用 AWS Config 主控台或工具來啟用與 Organizations 整合。這可讓 AWS Config 執行其需要的任何組態，例如建立服務所需的資源。只有在您無法使用 AWS Config 提供的工具啟用整合時，才能繼續執行這些步驟。如需詳細資訊，請參閱本說明。
> 如果您使用 AWS Config 主控台或工具啟用受信任存取，則不需要完成這些步驟。

使用 AWS Config 主控台來啟用受信任的存取權

若要使用 AWS Config 來啟用 對 AWS Organizations 的受信任存取，建立多帳戶彙總工具，並新增組織。如需如何設定多帳戶彙總的資訊，請參閱AWS Config開發人員指南中的使用主控台設定彙總工具。

您可以使用 AWS Organizations 主控台，執行 AWS CLI 命令，或呼叫其中一個 AWS 開發套件中的 API 操作，來啟用受信任的存取

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Services (服務) 頁面上，尋找 AWS Config 列，選擇服務的名稱，然後選擇 Enable trusted access (啟用受信任存取)。
3. 在確認對話方塊中，啟用顯示啟用受信任存取選項，在方塊中輸入 **enable**，然後選擇啟用受信任的存取。
4. 如果您只是 AWS Organizations 的系統管理員，請告訴 AWS Config 的管理員，他們現在可使用其主控台啟用該服務，以便與 AWS Organizations 搭配使用。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以啟用受信任的服務存取：

- AWS CLI: enable-aws-service-access

  您可以執行下列命令來啟用 AWS Config 作為 Organizations 受信任的服務。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal config.amazonaws.com
  ```

  此命令成功後就不會產生輸出。
- AWS API: EnableAWSServiceAccess

使用 AWS Config 停用受信任的存取

如需啟用受信任的存取所需許可的資訊，請參閱停用信任的存取所需的許可。

您只能使用 Organizations 工具來停用受信任的存取。

您可以執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDK 中的 Organizations API 操作，來停用受信任存取。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以停用信任的服務存取：

- AWS CLI: disable-aws-service-access

  您可以執行下列命令來停用 AWS Config 作為 Organizations 受信任的服務。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal config.amazonaws.com
  ```

  此命令成功後就不會產生輸出。

- AWS API：DisableAWSServiceAccess

AWS 成本最佳化中心 和 AWS Organizations

AWS 成本最佳化中心 是一項「B AWS illing and Cost Management」功能，可協助您整合 AWS 帳戶和 AWS 區域的成本最佳化建議並排定優先順序，以便充分利用您的 AWS 支出。搭配使用成本最佳化中樞時， AWS Organizations 您可以輕鬆識別、篩選和彙總跨 Organizations AWS 成員帳戶和 AWS 區域的成本最佳化建議。

如需詳細資訊，請參閱AWS Cost Management 使用者指南中的成本最佳化中樞。

請使用下列資訊來協助您整 AWS 成本最佳化中心 合 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下服務連結角色。此角色可讓成本最佳化中樞在組織的帳戶內執行支援的作業。

只有在停用「成本最佳化中樞」與「組織」之間的信任存取，或從組織中移除成員帳戶時，才能刪除或修改此角色。

如需詳細資訊，請參閱AWS Cost Management 使用者指南中的成本最佳化中樞的服務連結角色權限。

- `AWSServiceRoleForCostOptimizationHub`

成本最佳化中樞使用的服務主體

成本最佳化中樞使用`cost-optimization-hub.bcm.amazonaws.com`服務主體。

使用成本最佳化中樞啟用受信任的

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

當您使用組織的管理帳戶選擇加入並包含組織內的所有成員帳戶時，您的組織帳戶中會自動啟用 Cost Optimization Hub 的受信任存取權。

您可以使用 AWS Organizations 主控台、執行 AWS CLI 命令或呼叫其中一個 AWS SDK 中的 API 作業來啟用受信任存取。

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Services (服務) 頁面上，尋找 AWS 成本最佳化中心 列，選擇服務的名稱，然後選擇 Enable trusted access (啟用受信任存取)。
3. 在確認對話方塊中，啟用顯示啟用受信任存取選項，在方塊中輸入 **`enable`**，然後選擇啟用受信任的存取。
4. 如果您只是管理員 AWS Organizations，請告訴管理員 AWS 成本最佳化中心 ，他們現在可以使用其控制台啟用該服務 AWS Organizations。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

您可以使用下列 AWS CLI 命令或 API 作業來啟用受信任的服務存取：

- AWS CLI: enable-aws-service-access

  您可以執行下列命令， AWS 成本最佳化中心 以啟用 Organizations 的信任服務。

```
$ aws organizations enable-aws-service-access \
    --service-principal cost-optimization-hub.bcm.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API：啟用 AWSServiceAccess

停用受信任存取權

如需啟用受信任的存取所需許可的資訊，請參閱停用信任的存取所需的許可。

您只能使用 Organizations 工具來停用受信任的存取。

> **Important**
>
> 如果您在選擇加入後停用成本最佳化中樞信任存取，則成本最佳化中樞會拒絕存取組織成員帳戶的建議。此外，組織內的成員帳戶不會選擇加入成本最佳化中心。請參閱AWS Cost Management 使用者指南中的成本最佳化中樞和 Organizations 信任存取權，深入了解。

您可以執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDK 中的 Organizations API 作業來停用受信任的存取。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

您可以使用下列 AWS CLI 命令或 API 作業來停用受信任的服務存取：

- AWS CLI: disable-aws-service-access

  您可以執行下列命令，將 AWS 成本最佳化中心 其停用為 Organizations 的信任服務。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal cost-optimization-hub.bcm.amazonaws.com
  ```

  此命令成功後就不會產生輸出。

- AWS API：停用 AWSServiceAccess

AWS Control Tower 與 AWS Organizations

AWS Control Tower 提供了一種簡單的方法來設置和管理 AWS 多帳戶環境，遵循指示的最佳實務。AWS Control Tower 協同運作擴大了 AWS Organizations 的功能。AWS Control Tower 應用預防性和偵測性控制 (防護機制)，協助您的組織和帳戶不會背離最佳實務 (偏離)。

AWS Control Tower 協同運作擴大了 AWS Organizations 的功能。

如需詳細資訊，請參閱 《AWS Control Tower 使用者指南》。

使用以下資訊可協助整合 AWS Control Tower 與 AWS Organizations。

進行整合時所需要的角色

所有已註冊的帳戶中都必須存在有 `AWSControlTowerExecution` 角色。其可讓 AWS Control Tower 管理您的個別帳戶，並向稽核和日誌歸檔帳戶報告與個別帳戶有關的資訊。

若要進一步了解 AWS Control Tower 使用的角色，請參閱《AWS Control Tower 如何與角色搭配來建立和管理帳戶》和《使用適合 AWS Control Tower 的身分型政策 (IAM 政策)》。

AWS Control Tower 使用的服務主體

AWS Control Tower 使用 `controltower.amazonaws.com` 服務主體。

使用 AWS Control Tower 啟用受信任的存取

AWS Control Tower 使用受信任的存取來偵測偏離以進行預防性控制，並追蹤可能導致偏離的帳戶和 OU 變更。

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

您只能使用 Organizations 工具來啟用受信任存取。

若要從 Organizations 主控台啟用受信任存取，請選擇 AWS Control Tower 旁的 **`Enable access`**。

您可以執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDK 中的 Organizations API 操作，來啟用受信任存取。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以啟用受信任的服務存取：

- AWS CLI: enable-aws-service-access

  您可以執行下列命令來啟用 AWS Control Tower 作為 Organizations 受信任的服務。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal controltower.amazonaws.com
  ```

  此命令成功後就不會產生輸出。

- AWS API: EnableAWSServiceAccess

使用 AWS Control Tower 停用受信任的存取

如需啟用受信任的存取所需許可的資訊，請參閱停用信任的存取所需的許可。

您只能使用 Organizations 工具來停用受信任的存取。

> **Important**
>
> 停用 AWS Control Tower 的受信任存取權會導致您的 AWS Control Tower 登陸區域漂移。修正此漂移問題的唯一方法是使用 AWS Control Tower 的登陸區域修復。在 Organizations 中重新啟用受信任的存取權並不能修正此漂移。在 AWS Control Tower 用戶指南中進一步了解漂移。

您可以執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDK 中的 Organizations API 操作，來停用受信任存取。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以停用信任的服務存取：

- AWS CLI: disable-aws-service-access

  您可以執行下列命令來停用 AWS Control Tower 作為 Organizations 受信任的服務。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal controltower.amazonaws.com
  ```

此命令成功後就不會產生輸出。

- AWS API：DisableAWSServiceAccess

Amazon Detective 和 AWS Organizations

Amazon Detective 會使用您的日誌資料產生視覺化效果，以便您分析、調查並識別安全問題清單或可疑活動的根本原因。

使用 AWS Organizations 允許您確保 Detective 行為圖提供對所有組織帳戶活動的可見性。

當您向 Detective 授予受信任存取權時，Detective 服務可以自動對組織成員身分的變更做出反應。委派管理員可以在行為圖中將任何組織帳戶作為成員帳戶啟用。Detective 還可以自動將新組織帳戶作為成員帳戶啟用。組織帳戶無法將自己與行為圖解除關聯。

如需詳細資訊，請參閱《Amazon Detective 管理指南》中的在組織中使用 Amazon Detective。

使用以下資訊可協助您整合 Amazon Detective 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下服務連結角色。此角色允許 Detective 在您組織的組織帳戶中執行支援的操作。

只有在您停用 Detective 和 Organizations 之間的受信任存取，或者從組織中移除成員帳戶時，才能刪除或修改此角色。

- `AWSServiceRoleForDetective`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。Detective 使用的服務連結角色會將存取權授予下列服務委託人：

- `detective.amazonaws.com`

使用 Detective 啟用受信任存取

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

> **Note**
>
> 當您指定 Amazon Detective 的委派管理員時，Detective 會自動啟用組織中 Detective 的受信任存取。
> Detective 需要對 AWS Organizations 的受信任存取，才能為組織指定成員帳戶作為此服務的委派管理員。

您只能使用 Organizations 工具來啟用受信任存取。

使用 AWS Organizations 主控台來啟用受信任存取。

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Services (服務) 頁面上，尋找 Amazon Detective 列，選擇服務的名稱，然後選擇 Enable trusted access (啟用受信任存取)。
3. 在確認對話方塊中，啟用顯示啟用受信任存取選項，在方塊中輸入 **`enable`**，然後選擇啟用受信任的存取。
4. 如果您只是 AWS Organizations 的系統管理員，請告訴 Amazon Detective 的管理員，他們現在可使用其主控台啟用該服務，以便與 AWS Organizations 搭配使用。

使用 Detective 停用受信任存取

如需啟用受信任的存取所需許可的資訊，請參閱停用信任的存取所需的許可。

只有 AWS Organizations 管理帳戶中的管理員才能使用 Amazon Detective 停用受信任存取。

您只能使用 Organizations 工具來停用受信任的存取。

您可以使用 AWS Organizations 主控台來停用受信任存取。

AWS Management Console

使用 Organizations 主控台來受信停用任的服務存取

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Services (服務) 頁面上，尋找 Amazon Detective 列，然後選擇服務的名稱。
3. 選擇停用受信任的存取。
4. 在確認對話方塊中，輸入 **disable**，然後選擇停用受信任的存取。
5. 如果您只是 AWS Organizations 的系統管理員，請告訴 Amazon Detective 的管理員，他們現在可使用其主控台或工具停止該服務與 AWS Organizations 搭配使用。

啟用 Detective 的委派管理員帳戶

Detective 的委派管理員帳戶是 Detective 行為圖的管理員帳戶。委派管理員會判斷要在該行為圖中啟用和停用哪些作為成員帳戶的組織帳戶。委派管理員可以設定 Detective，使其在將新的組織帳戶新增到組織時自動將其作為成員帳戶啟用。如需委派管理員如何管理組織帳戶的資訊，請參閱《Amazon Detective 管理指南》中的將組織帳戶作為成員帳戶管理。

只有組織管理帳戶中的管理員可以設定 Detective 的委派管理員。

您可以從 Detective 主控台或 API，或使用 Organizations CLI 或 SDK 操作，指定委派的管理員帳戶。

> 最低許可
>
> 只有 Organizations 管理帳戶中的使用者或角色，才能將成員帳戶設定為組織中 Detective 的委派管理員

若要使用 Detective 主控台或 API 設定委派管理員，請參閱《Amazon Detective 管理指南》中的為組織指定 Detective 管理員帳戶。

AWS CLI, AWS API

如果您想要使用 AWS CLI 或其中一個 AWS SDK，可以使用下列命令：

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
```

```
    --account-id 123456789012 \
    --service-principal detective.amazonaws.com
```

- AWS SDK：呼叫 Organizations `RegisterDelegatedAdministrator` 操作和成員帳戶的 ID 號碼，並識別帳戶服務主體 `account.amazonaws.com` 作為參數。

停用 Detective 的委派管理員

您可以使用 Detective 主控台或 API，或透過使用 Organizations `DeregisterDelegatedAdministrator` CLI 或 SDK 操作，移除委派管理員。關於如何使用 Detective 主控台或 API 或 Organizations API 移除委派管理員的資訊，請參閱《Amazon Detective 管理指南》中的為組織指定 Detective 管理員帳戶。

Amazon DevOps Guru 和 AWS Organizations

Amazon DevOps Guru 分析營運資料和應用程式指標與事件，以識別與正常操作模式不同的行為。當 DevOps Guru 檢測到操作問題或風險時，會通知使用者。

使用 DevOps Guru 可以使用 AWS Organizations 實現多帳戶支援，如此您就可以指定成員帳戶來管理整個組織的洞察。然後，此委派管理員可以檢視、排序和篩選組織內所有帳戶的洞察，以便從整體上了解組織內所有受監控應用程式的運作狀態，而無需進行任何其他自訂。

如需詳細資訊，請參閱《Amazon DevOps Guru 使用者指南》中的監控組織中的帳戶。

使用以下資訊可協助您整合 Amazon DevOps Guru 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下服務連結角色。此角色允許 DevOps Guru 在您組織的組織帳戶中執行支援的操作。

只有在您停用 DevOps Guru 和 Organizations 之間的受信任存取，或者從組織中移除成員帳戶時，才能刪除或修改此角色。

- `AWSServiceRoleForDevOpsGuru`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。DevOps Guru 使用的服務連結角色會將存取權授予下列服務委託人：

- devops-guru.amazonaws.com

如需詳細資訊，請參閱《Amazon DevOps Guru 使用者指南》中的將服務連結角色用於 DevOps Guru。

使用 DevOps Guru 啟用受信任存取

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

> **Note**
>
> 當您指定 Amazon DevOps Guru 的委派管理員時，DevOps Guru 會自動啟用組織中 DevOps Guru 的受信任存取。
> DevOps Guru 需要對 AWS Organizations 的受信任存取，才能為組織指定成員帳戶作為此服務的委派管理員。

> **Important**
>
> 強烈建議您盡可能使用 Amazon DevOps Guru 主控台或工具來啟用與 Organizations 的整合。這可讓 Amazon DevOps Guru 執行其需要的任何組態，例如建立服務所需的資源。只有在您無法使用 Amazon DevOps Guru 提供的工具啟用整合時，才能繼續執行這些步驟。如需詳細資訊，請參閱本說明。

您可以使用 AWS Organizations 主控台或 DevOps Guru 主控台來啟用受信任存取。

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Services (服務) 頁面上，尋找 Amazon DevOps Guru 列，選擇服務的名稱，然後選擇 Enable trusted access (啟用受信任存取)。
3. 在確認對話方塊中，啟用顯示啟用受信任存取選項，在方塊中輸入 **enable**，然後選擇啟用受信任的存取。

4. 如果您只是 AWS Organizations 的管理員，請告訴 Amazon DevOps Guru 的管理員，他們現在可使用其主控台啟用該服務，以便與 AWS Organizations 搭配使用。

DevOps Guru console

使用 DevOps Guru 主控台來啟用受信任服務存取

1. 在管理帳戶中以管理員身分登入並開啟 DevOps Guru 主控台：Amazon DevOps Guru 主控台
2. 選擇 Enable trusted access (啟用信任存取)。

使用 DevOps Guru 停用受信任存取

如需啟用受信任的存取所需許可的資訊，請參閱停用信任的存取所需的許可。

只有 AWS Organizations 管理帳戶中的管理員才能使用 Amazon DevOps Guru 停用受信任存取。

您只能使用 Organizations 工具來停用受信任的存取。

您可以使用 AWS Organizations 主控台來停用受信任存取。

AWS Management Console

使用 Organizations 主控台來受信停用任的服務存取

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Services (服務) 頁面上，尋找 Amazon DevOps Guru 列，然後選擇服務的名稱。
3. 選擇停用受信任的存取。
4. 在確認對話方塊中，輸入 **`disable`**，然後選擇停用受信任的存取。
5. 如果您只是 AWS Organizations 的管理員，請告訴 Amazon DevOps Guru 的管理員，他們現在可使用其主控台或工具停止該服務與 AWS Organizations 搭配使用。

啟用 DevOps Guru 的委派管理員帳戶

DevOps Guru 的委派管理員帳戶可以查看所有成員帳戶中的洞察資料，這些帳戶是從組織加入 DevOps Guru。如需委派管理員如何管理組織帳戶的資訊，請參閱《Amazon DevOps Guru 使用者指南》中的監控組織中的帳戶。

只有組織管理帳戶中的管理員可以設定 DevOps Guru 的委派管理員。

您可以從 DevOps Guru 主控台，或使用 Organizations `RegisterDelegatedAdministrator`CLI 或 SDK 操作，指定委派管理員帳戶。

> **最低許可**
>
> 只有 Organizations 管理帳戶中的使用者或角色，才能將成員帳戶設定為組織中 DevOps Guru 的委派管理員

DevOps Guru console

在 DevOps Guru 主控台中設定委派管理員

1. 在管理帳戶中以管理員身分登入並開啟 DevOps Guru 主控台：Amazon DevOps Guru 主控台
2. 選擇 Register delegated administrator (註冊委派管理員)。您可以選擇管理帳戶或任何成員帳戶作為委派管理員。

AWS CLI, AWS API

如果您想要使用 AWS CLI 或其中一個 AWS SDK，可以使用下列命令：

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal devops-guru.amazonaws.com
```

- AWS SDK：呼叫 Organizations `RegisterDelegatedAdministrator` 操作和成員帳戶的 ID 號碼，並識別帳戶服務主體 `account.amazonaws.com` 作為參數。

停用 DevOps Guru 的委派管理員

您可以使用 DevOps Guru 主控台或使用 Organizations `DeregisterDelegatedAdministrator` CLI 或 SDK 操作，移除委派管理員。如需有關如何使用 DevOps Guru 主控台移除委派管理員的資訊，請參閱《Amazon DevOps Guru 使用者指南》中的監控組織中的帳戶。

AWS Directory Service 與 AWS Organizations

適用於 Microsoft Active Directory 的 AWS Directory Service，或 AWS Managed Microsoft AD 可讓您以受管服務的形式執行 Microsoft Active Directory (AD)。AWS Directory Service 可讓您輕鬆地在 AWS Cloud 中設定和執行目錄，或將您的 AWS 資源與現有的現場部署 Microsoft Active Directory 連接。AWS Managed Microsoft AD 還能與 AWS Organizations 緊密整合，以跨多個 AWS 帳戶 和區域中的任何 VPC 進行無縫的目錄共享。如需詳細資訊，請參閱 AWS Directory Service管理員指南。

使用以下資訊可協助整合 AWS Directory Service 與 AWS Organizations。

使用 AWS Directory Service 啟用受信任的存取

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

您可以使用 AWS Directory Service 主控台或 AWS Organizations 主控台來啟用信任存取。

> **Important**
>
> 強烈建議您盡可能使用 AWS Directory Service 主控台或工具來啟用與 Organizations 整合。這可讓 AWS Directory Service 執行其需要的任何組態，例如建立服務所需的資源。只有在您無法使用 AWS Directory Service 提供的工具啟用整合時，才能繼續執行這些步驟。如需詳細資訊，請參閱本說明。
> 如果您使用 AWS Directory Service 主控台或工具啟用受信任存取，則不需要完成這些步驟。

使用 AWS Directory Service 主控台來啟用受信任的存取權

若要共享自動啟用受信任存取的目錄，請參閱AWS Directory Service管理指南中的共享您的目錄。如需逐步說明，請參閱教學課程：共享您的 AWS 受管 Microsoft AD 目錄。

使用 AWS Organizations 主控台來啟用受信任存取。

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Services (服務) 頁面上，尋找 AWS Directory Service 列，選擇服務的名稱，然後選擇 Enable trusted access (啟用受信任存取)。

3. 在確認對話方塊中，啟用顯示啟用受信任存取選項，在方塊中輸入 **enable**，然後選擇啟用受信任的存取。
4. 如果您只是 AWS Organizations 的系統管理員，請告訴 AWS Directory Service 的管理員，他們現在可使用其主控台啟用該服務，以便與 AWS Organizations 搭配使用。

使用 AWS Directory Service 停用受信任的存取

如需啟用受信任的存取所需許可的資訊，請參閱停用信任的存取所需的許可。

如果您在使用 AWS Directory Service 時使用 AWS Organizations 來停用受信任存取，所有之前共享的目錄會繼續正常運作。不過，您不再能夠以在組織內共享新目錄，直到您重新啟用信任的存取為止。

您只能使用 Organizations 工具來停用受信任的存取。

您可以使用 AWS Organizations 主控台來停用受信任存取。

AWS Management Console

使用 Organizations 主控台來受信停用任的服務存取

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Services (服務) 頁面上，尋找 AWS Directory Service 列，然後選擇服務的名稱。
3. 選擇停用受信任的存取。
4. 在確認對話方塊中，輸入 **disable**，然後選擇停用受信任的存取。
5. 如果您只是 AWS Organizations 的系統管理員，請告訴 AWS Directory Service 的管理員，他們現在可使用其主控台或工具停用該服務，以便與 AWS Organizations 搭配使用。

AWS Firewall Manager 與 AWS Organizations

AWS Firewall Manager 是一種安全管理服務，您可以用於集中設定和管理防火牆規則，以及組織中 AWS 帳戶 和應用程式的其他防護。使用 Firewall Manager，您可以啟用 AWS WAF 規則，建立 AWS Shield Advanced 防護、設定和稽核 Amazon Virtual Private Cloud (Amazon VPC) 安全群組，以及部署 AWS Network Firewall。只需使用 Firewall Manager 設定一次防護，並將它們在您的組織內的所有帳戶和資源間自動套用，甚至是新增了新資源和帳戶亦然。如需 AWS Firewall Manager 的詳細資訊，請參閱《AWS Firewall Manager 開發人員指南》。

使用以下資訊可協助整合 AWS Firewall Manager 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下服務連結角色。該角色允許 Firewall Manager 在您組織的組織帳戶中執行支援的操作。

只有在您停用 Firewall Manager 和 Organizations 之間的受信任存取，或從組織中移除成員帳戶時，才能移除或修改此角色。

- `AWSServiceRoleForFMS`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。Firewall Manager 使用的服務連結角色會將存取權授予下列服務委託人：

- `fms.amazonaws.com`

使用 Firewall Manager 啟用受信任存取

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

您可以使用 AWS Firewall Manager 主控台或 AWS Organizations 主控台來啟用信任存取。

> **Important**
>
> 強烈建議您盡可能使用 AWS Firewall Manager 主控台或工具來啟用與 Organizations 整合。這可讓 AWS Firewall Manager 執行其需要的任何組態，例如建立服務所需的資源。只有在您無法使用 AWS Firewall Manager 提供的工具啟用整合時，才能繼續執行這些步驟。如需詳細資訊，請參閱本說明。
>
> 如果您使用 AWS Firewall Manager 主控台或工具啟用受信任存取，則不需要完成這些步驟。

您必須使用您的 AWS Organizations 管理帳戶登入，並將組織內的帳戶設定為 AWS Firewall Manager 管理員帳戶。如需詳細資訊，請參閱AWS Firewall Manager開發人員指南中的設定 AWS Firewall Manager 管理員帳戶。

您可以使用 AWS Organizations 主控台，執行 AWS CLI 命令，或呼叫其中一個 AWS 開發套件中的 API 操作，來啟用受信任的存取

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Services (服務) 頁面上，尋找 AWS Firewall Manager 列，選擇服務的名稱，然後選擇 Enable trusted access (啟用受信任存取)。
3. 在確認對話方塊中，啟用顯示啟用受信任存取選項，在方塊中輸入 **enable**，然後選擇啟用受信任的存取。
4. 如果您只是 AWS Organizations 的系統管理員，請告訴 AWS Firewall Manager 的管理員，他們現在可使用其主控台啟用該服務，以便與 AWS Organizations 搭配使用。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以啟用受信任的服務存取：

- AWS CLI: enable-aws-service-access

  您可以執行下列命令來啟用 AWS Firewall Manager 作為 Organizations 受信任的服務。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal fms.amazonaws.com
  ```

  此命令成功後就不會產生輸出。
- AWS API: EnableAWSServiceAccess

使用 Firewall Manager 停用受信任存取

如需啟用受信任的存取所需許可的資訊，請參閱停用信任的存取所需的許可。

您可以使用 AWS Firewall Manager 或 AWS Organizations 工具停用受信任存取。

> **Important**
>
> 強烈建議您盡可能使用 AWS Firewall Manager 主控台或工具來停用與 Organizations 整合。這可讓 AWS Firewall Manager 執行其所需的任何清除，例如刪除服務不再需要的資源或存取角

色。只有在您無法使用 AWS Firewall Manager 提供的工具停用整合成時，才能繼續執行這些步驟。
如果您使用 AWS Firewall Manager 主控台或工具停用受信任的存取，則不需要完成這些步驟。

使用 Firewall Manager 主控台來停用受信任的存取

遵循AWS Firewall Manager開發人員指南中的指定不同的帳戶作為 AWS Firewall Manager 管理員帳戶，您可以變更或撤銷 AWS Firewall Manager 管理員帳戶。

如果撤銷管理員帳戶，必須登入 AWS Organizations 管理帳戶，並設定 AWS Firewall Manager 的新管理員帳戶。

您可以使用 AWS Organizations 主控台，執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDK 中的 Organizations API 操作，來停用受信任存取。

AWS Management Console

使用 Organizations 主控台來受信停用任的服務存取

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Services (服務) 頁面上，尋找 AWS Firewall Manager 列，然後選擇服務的名稱。
3. 選擇停用受信任的存取。
4. 在確認對話方塊中，輸入 **disable**，然後選擇停用受信任的存取。
5. 如果您只是 AWS Organizations 的系統管理員，請告訴 AWS Firewall Manager 的管理員，他們現在可使用其主控台或工具停用該服務，以便與 AWS Organizations 搭配使用。

AWS CLI, AWS API

使用 Organizations CLI/開發套件來受信停用任的服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以停用信任的服務存取：

- AWS CLI: disable-aws-service-access

  您可以執行下列命令來停用 AWS Firewall Manager 作為 Organizations 受信任的服務。

```
$ aws organizations disable-aws-service-access \
```

```
    --service-principal fms.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API：DisableAWSServiceAccess

啟用 Firewall Manager 的委派管理員帳戶

當您將成員帳戶指定為組織的委派管理員時，該帳戶的使用者和角色可以對 Firewall Manager 執行管理動作，否則只能由組織管理帳戶中的使用者或角色執行。這可協助您將組織的管理與 Firewall Manager 的管理分開。

> **最低許可**
>
> 只有 Organizations 管理帳戶中的使用者或角色，才能將成員帳戶設定為組織中 Firewall Manager 的委託管理員。

如需如何將成員帳戶指定為組織 Firewall Manager 管理員的指示，請參閱AWS Firewall Manager開發人員指南中的設定 AWS Firewall Manager 管理員帳戶。

Amazon GuardDuty 和 AWS Organizations

Amazon GuardDuty 是持續性安全監控服務，可分析和處理各種資料來源，並使用威脅智慧饋送和機器學習技術來識別您的AWS 環境中的非預期和可能未經授權的惡意活動。這可能包括權限升級、使用暴露的憑證、與惡意 IP 地址、URL 或網域的通訊，或者 Amazon Elastic Compute Cloud 執行個體和容器工作負載中出現惡意軟體等問題。

您可以透過 Organizations 管理組織中所有帳戶的 GuardDuty，來協助簡化 GuardDuty 的管理。

如需詳細資訊，請參閱 Amazon GuardDuty 使用者指南中的使用 AWS Organizations 管理 GuardDuty 帳戶

使用以下資訊可協助整合 Amazon GuardDuty 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下服務連結角色。這些角色允許 GuardDuty 在您組織的組織帳戶中執行支援的操作。只有在您停用 GuardDuty 與 Organizations 之間的受信任存取，或從組織中移除成員帳戶時，才能刪除此角色。

- 會在已將 GuardDuty 與 Organizations 整合的帳戶中自動建立 `AWSServiceRoleForAmazonGuardDuty` 服務連結角色。如需詳細資訊，請參閱 Amazon GuardDuty 使用者指南中的使用 Organizations 管理 GuardDuty 帳戶
- 會在已啟用 GuardDuty 惡意軟體防護的帳戶中自動建立 `AmazonGuardDutyMalwareProtectionServiceRolePolicy` 服務連結角色。如需詳細資訊，請參閱 Amazon GuardDuty 使用者指南中的用於 GuardDuty 惡意軟體防護的服務連結角色許可

服務連結角色所使用的服務委託人

- `guardduty.amazonaws.com`，由 `AWSServiceRoleForAmazonGuardDuty` 服務連結角色使用。
- `malware-protection.guardduty.amazonaws.com`，由 `AmazonGuardDutyMalwareProtectionServiceRolePolicy` 服務連結角色使用。

使用 GuardDuty 來啟用受信任存取

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

您只能使用 Amazon GuardDuty 來啟用受信任存取。

Amazon GuardDuty 需要對 AWS Organizations 的受信任存取，才能將成員帳戶指定為組織的 GuardDuty 管理員。如果您使用 GuardDuty 主控台設定委派管理員，則 GuardDuty 會自動為您啟用受信任的存取。

不過，如果您想要使用 AWS CLI 或其中一個 AWS SDK 來設定委派的管理員帳戶，則必須明確地呼叫 EnableAWSServiceAccess 操作，並提供服務委託人作為參數。然後，可以呼叫 EnableOrganizationAdminAccount，來委派 GuardDuty 管理員帳戶。

使用 GuardDuty 來停用受信任存取

如需啟用受信任的存取所需許可的資訊，請參閱停用信任的存取所需的許可。

您只能使用 Organizations 工具來停用受信任的存取。

您可以執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDK 中的 Organizations API 操作，來停用受信任存取。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以停用信任的服務存取：

- AWS CLI: disable-aws-service-access

  您可以執行下列命令來停用 Amazon GuardDuty 作為 Organizations 受信任的服務。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal guardduty.amazonaws.com
  ```

  此命令成功後就不會產生輸出。
- AWS API：DisableAWSServiceAccess

啟用 GuardDuty 的委派管理員帳戶

當您將成員帳戶指定為組織的委派管理員時，該帳戶的使用者和角色可以對 GuardDuty 執行管理動作，否則只能由組織管理帳戶中的使用者或角色執行。這可協助您將組織的管理與 GuardDuty 的管理分開。

> **最低許可**
>
> 如需將成員帳戶指定為委派管理員所需許可的相關資訊，請參閱Amazon GuardDuty 使用者指南中的指定委派管理員所需的許可

將成員帳戶指定為 GuardDuty 的委派管理員

請參閱指定委派的管理員並新增成員帳戶 (主控台)和指定委派的管理員並新增成員帳戶 (API)

AWS Health 與 AWS Organizations

AWS Health 可提供對資源效能，以及 AWS 服務和帳戶可用性的持續洞察。當您的 AWS 資源和服務受到問題影響，或將會受到即將發生變化的影響時，AWS Health 會傳遞事件。啟用組織檢視之後，組織管理帳戶中的使用者可以彙總 AWS Health 跨組織中所有帳戶的事件。組織檢視僅顯示啟用該功能後傳遞的 AWS Health 事件，並將其保留 90 天。

您可以使用 AWS Health主控台、AWS Command Line Interface(AWS CLI) 或 AWS HealthAPI 啟用組織檢視。

如需詳細資訊，請參閱AWS Health使用者指南中的彙總 AWS Health 事件。

使用以下資訊可協助整合 AWS Health 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下服務連結角色。該角色允許 AWS Health 在您組織的組織帳戶中執行支援的操作。

只有在您停用 AWS Health 和 Organizations 之間的受信任存取，或者從組織中刪除成員帳戶時，才能移除或修改此角色。

- `AWSServiceRoleForHealth_Organizations`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。AWS Health 使用的服務連結角色會將存取權授予下列服務委託人：

- `health.amazonaws.com`

使用 AWS Health 啟用受信任的存取

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

當您啟用 AWS Health 的組織檢視功能時，也會自動為您啟用受信任存取。

您可以使用 AWS Health 主控台或 AWS Organizations 主控台來啟用信任存取。

> **Important**
>
> 強烈建議您盡可能使用 AWS Health 主控台或工具來啟用與 Organizations 整合。這可讓 AWS Health 執行其需要的任何組態，例如建立服務所需的資源。只有在您無法使用 AWS Health 提供的工具啟用整合時，才能繼續執行這些步驟。如需詳細資訊，請參閱本說明。
> 如果您使用 AWS Health 主控台或工具啟用受信任存取，則不需要完成這些步驟。

使用 AWS Health 主控台來啟用受信任的存取權

您可以使用 AWS Health 和下列其中一個選項來啟用受信任存取：

- 使用 AWS Health 主控台。如需詳細資訊，請參閱AWS Health使用者指南中的組織檢視 (主控台)。
- 使用 AWS CLI。如需詳細資訊，請參閱AWS Health使用者指南中的組織檢視 (CLI)。
- 呼叫 EnableHealthServiceAccessForOrganization API 操作。

您可以執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS 開發套件中的 Organizations API 操作，來啟用受信任的存取

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以啟用受信任的服務存取：

- AWS CLI: enable-aws-service-access

  您可以執行下列命令來啟用 AWS Health 作為 Organizations 受信任的服務。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal health.amazonaws.com
  ```

  此命令成功後就不會產生輸出。
- AWS API: EnableAWSServiceAccess

使用 AWS Health 停用受信任的存取

如需啟用受信任的存取所需許可的資訊，請參閱停用信任的存取所需的許可。

停用組織檢視功能之後，AWS Health 會停止彙總組織中所有其他帳戶的事件。這也會為您自動停用受信任存取。

您可以使用 AWS Health 或 AWS Organizations 工具停用受信任存取。

> **Important**
>
> 強烈建議您盡可能使用 AWS Health 主控台或工具來停用與 Organizations 整合。這可讓 AWS Health 執行其所需的任何清除，例如刪除服務不再需要的資源或存取角色。只有在您無法使用 AWS Health 提供的工具停用整合成時，才能繼續執行這些步驟。
> 如果您使用 AWS Health 主控台或工具停用受信任的存取，則不需要完成這些步驟。

使用 AWS Health 主控台來停用受信任存取

您可以使用以下其中一個選項來停用受信任存取：

- 使用 AWS Health 主控台。如需詳細資訊，請參閱AWS Health使用者指南中的停用組織檢視 (主控台)。
- 使用 AWS CLI。如需詳細資訊，請參閱AWS Health使用者指南中的停用組織檢視 (CLI)。
- 呼叫 DisableHealthServiceAccessForOrganization API 操作。

您可以執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS 開發套件中的 Organizations API 操作，來停用受信任的存取

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以停用信任的服務存取：

- AWS CLI: disable-aws-service-access

  您可以執行下列命令來停用 AWS Health 作為 Organizations 受信任的服務。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal health.amazonaws.com
  ```

  此命令成功後就不會產生輸出。
- AWS API：DisableAWSServiceAccess

啟用 AWS Health 的委派管理員帳戶

當您將成員帳戶指定為組織的委派管理員時，該帳戶的使用者和角色可以對 AWS Health 執行管理動作，否則只能由組織管理帳戶中的使用者或角色執行。這可協助您將組織的管理與 AWS Health 的管理分開。

將成員帳戶指定為 AWS Health 的委派管理員

參見註冊委派管理員以進行組織檢視

移除 AWS Health 的委派管理員

參見移除組織檢視中的委派管理員

Amazon Inspector 與 AWS Organizations

Amazon Inspector 是一項自動化漏洞管理服務，可持續掃描 Amazon EC2 和容器工作負載，以尋找軟體漏洞和意外的網路暴露。

使用 Amazon Inspector，您只需為 Amazon Inspector 委派管理員帳戶，即可管理透過 AWS Organizations 關聯的多個帳戶。委派管理員管理組織的 Amazon Inspector，並被授予代表組織執行任務所需的特殊許可，例如：

- 啟用或停用成員帳戶掃描
- 檢視整個組織的彙總問題清單資料
- 建立和管理隱藏規則

如需詳細資訊，請參閱《Amazon Inspector 使用者指南》中的使用 AWS Organizations 管理多個帳戶。

使用以下資訊可協助您整合 Amazon Inspector 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下服務連結角色。此角色允許 Amazon Inspector 在您組織的組織帳戶中執行支援的操作。

只有在您停用 Amazon Inspector 和 Organizations 之間的受信任存取，或者從組織中移除成員帳戶時，才能刪除或修改此角色。

- `AWSServiceRoleForAmazonInspector2`

如需詳細資訊，請參閱《Amazon Inspector 使用者指南》中的將服務連結角色用於 Amazon Inspector。

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。Amazon Inspector 使用的服務連結角色會將存取權授予下列服務委託人：

- `inspector2.amazonaws.com`

使用 Amazon Inspector 啟用受信任存取

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

Amazon Inspector 需要對 AWS Organizations 的受信任存取，才能為組織指定成員帳戶作為此服務的委派管理員。

當您指定 Amazon Inspector 的委派管理員時，Amazon Inspector 會自動啟用組織中 Amazon Inspector 的受信任存取。

不過，如果您想要使用 AWS CLI 或其中一個 AWS SDK 來設定委派管理員帳戶，則必須明確地呼叫 `EnableAWSServiceAccess` 操作，並提供服務委託人作為參數。然後，您可以呼叫 `EnableDelegatedAdminAccount` 以委派 Inspector 管理員帳戶。

您可以執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDK 中的 Organizations API 操作，來啟用受信任存取。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以啟用受信任的服務存取：

- AWS CLI: enable-aws-service-access

  您可以執行下列命令來啟用 Amazon Inspector 作為 Organizations 受信任的服務。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal inspector2.amazonaws.com
  ```

  此命令成功後就不會產生輸出。

- AWS API: EnableAWSServiceAccess

> **Note**
>
> 如果您使用 `EnableAWSServiceAccess` API，您還需要呼叫 `EnableDelegatedAdminAccount` 以委派 Inspector 管理員帳戶。

使用 Amazon Inspector 來停用受信任存取

如需啟用受信任的存取所需許可的資訊，請參閱停用信任的存取所需的許可。

只有 AWS Organizations 管理帳戶中的管理員才能使用 Amazon Inspector 停用受信任存取。

您只能使用 Organizations 工具來停用受信任的存取。

您可以執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDK 中的 Organizations API 操作，來停用受信任存取。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以停用信任的服務存取：

- AWS CLI: disable-aws-service-access

  您可以執行下列命令來停用 Amazon Inspector 作為 Organizations 受信任的服務。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal inspector2.amazonaws.com
  ```

  此命令成功後就不會產生輸出。
- AWS API：DisableAWSServiceAccess

啟用 Amazon Inspector 的委派管理員帳戶

透過 Amazon Inspector，您可以使用 AWS Organizations 服務搭配委派管理員來管理組織中的多個帳戶。

此 AWS Organizations 管理帳戶將組織內的帳戶指定為 Amazon Inspector 的委派管理員帳戶。委派管理員管理組織的 Amazon Inspector，並被授予代表組織執行任務所需的特殊許可，例如：啟用或停用成員帳戶掃描、檢視整個組織的彙總問題清單資料，以及建立和管理隱藏規則

如需有關委派管理員如何管理組織帳戶的資訊，請參閱《Amazon Inspector 使用者指南》中的了解管理員和成員帳戶之間的關係。

只有組織管理帳戶中的管理員可以設定 Amazon Inspector 的委派管理員。

您可以從 Amazon Inspector 主控台或 API，或使用 Organizations CLI 或 SDK 操作，指定委派管理員帳戶。

> **最低許可**
>
> 只有 Organizations 管理帳戶中的使用者或角色，才能將成員帳戶設定為組織中 Amazon Inspector 的委派管理員

若要使用 Amazon Inspector 主控台設定委派管理員，請參閱《Amazon Inspector 使用者指南》中的步驟 1：啟用 Amazon Inspector - 多帳戶環境。

> **Note**
>
> 您必須在您使用 Amazon Inspector 的每個區域中呼叫 `inspector2:enableDelegatedAdminAccount`。

AWS CLI, AWS API

如果您想要使用 AWS CLI 或其中一個 AWS SDK，可以使用下列命令：

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal inspector2.amazonaws.com
```

- AWS SDK：呼叫 Organizations `RegisterDelegatedAdministrator` 操作和成員帳戶的 ID 號碼，並識別帳戶服務主體 `account.amazonaws.com` 作為參數。

停用 Amazon Inspector 的委派管理員

只有 AWS Organizations 管理帳戶中的管理員可以移除組織中的委派管理員帳戶。

您可以使用 Amazon Inspector 主控台或 API，或使用 Organizations `DeregisterDelegatedAdministrator` CLI 或 SDK 操作，移除委派管理員。若要使用 Amazon Inspector 主控台移除委派管理員，請參閱《Amazon Inspector 使用者指南》中的移除委派管理員。

AWS License Manager 與 AWS Organizations

AWS License Manager 能夠簡化將軟體廠商授權遷往雲端的程序。在 AWS 上建置雲端基礎設施時，可使用自有授權 (BYOL) 來節省成本。即重新規劃現有的授權庫存，以利搭配雲端資源使用。有了規則為基礎的授權消費限制，管理員即可針對現有雲端部署設定嚴格或寬鬆的限制，藉此預防不合規伺服器使用情形發生。

如需有關 License Manager 的詳細資訊，請參閱 License Manager 使用者指南。

透過將 License Manager 與 AWS Organizations 進行連結，您可以：

- 在組織中實現運算資源的跨帳戶探索。
- 檢視和管理您擁有的並在 AWS 上執行的商業 Linux 訂閱。如需詳細資訊，請參閱 AWS License Manager 中的 Linux 訂閱。

使用以下資訊可協助整合 AWS License Manager 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下服務連結角色。這些角色允許 License Manager 在您組織的組織帳戶中執行支援的操作。

只有在您停用 License Manager 和 Organizations 之間的受信任存取，或從組織中移除成員帳戶時，才能移除或修改角色。

- `AWSLicenseManagerMasterAccountRole`
- `AWSLicenseManagerMemberAccountRole`
- `AWSServiceRoleForAWSLicenseManagerRole`
- `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService`

如需詳細資訊，請參閱 License Manager – 管理帳戶角色、License Manager – 成員帳戶角色和 License Manager – Linux 訂閱角色。

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。License Manager 使用的服務連結角色會將存取權授予下列服務委託人：

- `license-manager.amazonaws.com`
- `license-manager.member-account.amazonaws.com`
- `license-manager-linux-subscriptions.amazonaws.com`

使用 License Manager 來啟用受信任存取

您可以僅使用 AWS License Manager 來啟用受信任存取。

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

使用 License Manager 來啟用受信任存取

您必須使用 AWS Organizations 管理帳戶登入 License Manager 主控台，並將其與您的 License Manager 帳戶建立關聯。如需詳細資訊，請參閱 AWS License Manager 中的設定。

使用 License Manager 來停用受信任存取

如需啟用受信任的存取所需許可的資訊，請參閱停用信任的存取所需的許可。

您只能使用 Organizations 工具來停用受信任的存取。

您可以執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDK 中的 Organizations API 操作，來停用受信任存取。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以停用信任的服務存取：

- AWS CLI: disable-aws-service-access

  您可以執行下列命令來停用 AWS License Manager 作為 Organizations 受信任的服務。

```
$ aws organizations disable-aws-service-access \
    --service-principal license-manager.amazonaws.com
```

  此命令成功後就不會產生輸出。

  若要停用 Linux 訂閱的受信任存取，請使用：

```
$  aws organizations disable-aws-service-access \
```

```
    --service-principal license-manager-linux-subscriptions.amazonaws.com
```

- AWS API：DisableAWSServiceAccess

啟用 License Manager 的委派管理員帳戶

當您將成員帳戶指定為組織的委派管理員時，該帳戶的使用者和角色可以對 License Manager 執行管理動作，否則只能由組織管理帳戶中的使用者或角色執行。這可協助您將組織的管理與 License Manager 的管理分開。

若要將成員帳戶委派為 License Manager 的管理員，請遵循License Manager 使用者指南中的註冊委派管理員。

Amazon Macie 和 AWS Organizations

Amazon Macie 是一種全受管資料安全和資料隱私權服務，該服務使用機器學習和模式比對來探索、監控和協助您保護 Amazon Simple Storage Service (Amazon S3) 中的敏感資料。Macie 會自動探索敏感資料，例如個人身分識別資訊 (PII) 和智慧財產權，讓您更清楚了解組織在 Amazon S3 中存放在的資料。

如需詳細資訊，請參閱Amazon Macie 使用者指南中的使用 AWS Organizations 管理 Amazon Macie 帳戶。

使用以下資訊可協助您整合 Amazon Macie 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會自動為您組織的委派 Macie 管理員帳戶建立以下服務連結角色。該角色允許 Macie 為您組織的帳戶執行支援的操作。

只有在您停用 Macie 和 Organizations 之間的受信任存取，或從組織中移除成員帳戶時，才能刪除此角色。

- `AWSServiceRoleRorAmazonMacie`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。Macie 使用的服務連結角色會將存取權授予下列服務委託人：

- `macie.amazonaws.com`

使用 Macie 來啟用受信任存取

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

您可以使用 Amazon Macie 主控台或 AWS Organizations 主控台來啟用受信任存取。

> **Important**
>
> 強烈建議您盡可能使用 Amazon Macie 主控台或工具來啟用與 Organizations 整合。這可讓 Amazon Macie 執行其需要的任何組態，例如建立服務所需的資源。只有在您無法使用 Amazon Macie 提供的工具啟用整合時，才能繼續執行這些步驟。如需詳細資訊，請參閱本說明。
>
> 如果您使用 Amazon Macie 主控台或工具啟用受信任的存取，則不需要完成這些步驟。

使用 Amazon Macie 主控台來啟用受信任存取

Amazon Macie 需要對 AWS Organizations 的受信任存取，才能將成員帳戶指定為組織的 Macie 管理員。如果您使用 Macie 管理主控台設定委派管理員，則 Macie 會自動為您啟用受信任的存取。

如需詳細資訊，請參閱 Amazon Macie 使用者指南中的在 Amazon Macie 中整合和設定組織。

您可以執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDK 中的 Organizations API 操作，來啟用受信任存取。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以啟用受信任的服務存取：

- AWS CLI: enable-aws-service-access

  您可以執行下列命令來啟用 Amazon Macie 作為 Organizations 受信任的服務。

```
$ aws organizations enable-aws-service-access \
    --service-principal macie.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API: EnableAWSServiceAccess

啟用 Macie 的委派管理員帳戶

當您將成員帳戶指定為組織的委派管理員時，該帳戶的使用者和角色可以對 Macie 執行管理動作，否則只能由組織管理帳戶中的使用者或角色執行。這可協助您將組織的管理與 Macie 的管理分開。

> **最低許可**
>
> 只有具有下列許可之 Organizations 管理帳戶中的使用者或角色，才能將成員帳戶設定為組織中 Macie 的委託管理員：
>
> - `organizations:EnableAWSServiceAccess`
> - `macie:EnableOrganizationAdminAccount`

將成員帳戶指定為 Macie 的委派管理員

Amazon Macie 需要對 AWS Organizations 的受信任存取，才能將成員帳戶指定為組織的 Macie 管理員。如果您使用 Macie 管理主控台設定委派管理員，則 Macie 會自動為您啟用受信任的存取。

如需詳細資訊，請參閱 https://docs.aws.amazon.com/macie/latest/user/macie-organizations.html#register-delegated-admin

AWS Marketplace 與 AWS Organizations

AWS Marketplace 經策管數位目錄，您可以用於尋找、購買、部署和管理第三方軟體、資料和服務，而您需要這些軟體、資料和服務，來建置解決方案並執行您的業務。

AWS Marketplace 使用 AWS License Manager 為您在 AWS Marketplace 中的購買項目建立和管理授權。當您與組織中的其他帳戶共享您的授權 (授予存取權) 時，AWS Marketplace 會為這些帳戶建立和管理新的授權。

如需詳細資訊，請參閱 AWS Marketplace 買家指南中的 AWS Marketplace 的服務連結角色。

使用以下資訊可協助整合 AWS Marketplace 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下服務連結角色。該角色允許 AWS Marketplace 在您組織的組織帳戶中執行支援的操作。

只有在您停用 AWS Marketplace 和 Organizations 之間的受信任存取，或者從組織中刪除成員帳戶時，才能移除或修改此角色。

- `AWSServiceRoleForMarketplaceLicenseManagement`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。AWS Marketplace 使用的服務連結角色會將存取權授予下列服務委託人：

- `license-management.marketplace.amazonaws.com`

使用 AWS Marketplace 啟用受信任的存取

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

您可以使用 AWS Marketplace 主控台或 AWS Organizations 主控台來啟用信任存取。

> **Important**
>
> 強烈建議您盡可能使用 AWS Marketplace 主控台或工具來啟用與 Organizations 整合。這可讓 AWS Marketplace 執行其需要的任何組態，例如建立服務所需的資源。只有在您無法使用 AWS Marketplace 提供的工具啟用整合時，才能繼續執行這些步驟。如需詳細資訊，請參閱本說明。
>
> 如果您使用 AWS Marketplace 主控台或工具啟用受信任存取，則不需要完成這些步驟。

使用 AWS Marketplace 主控台來啟用受信任的存取權

請參閱 AWS Marketplace Buyer Guide (《AWS Marketplace 買家指南》) 中的 Creating a service-linked role for AWS Marketplace (建立 AWS Marketplace 的服務連結角色)。

您可以使用 AWS Organizations 主控台，執行 AWS CLI 命令，或呼叫其中一個 AWS 開發套件中的 API 操作，來啟用受信任的存取

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Services (服務) 頁面上，尋找 AWS Marketplace 列，選擇服務的名稱，然後選擇 Enable trusted access (啟用受信任存取)。
3. 在確認對話方塊中，啟用顯示啟用受信任存取選項，在方塊中輸入 **enable**，然後選擇啟用受信任的存取。
4. 如果您只是 AWS Organizations 的系統管理員，請告訴 AWS Marketplace 的管理員，他們現在可使用其主控台啟用該服務，以便與 AWS Organizations 搭配使用。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以啟用受信任的服務存取：

- AWS CLI: enable-aws-service-access

  您可以執行下列命令來啟用 AWS Marketplace 作為 Organizations 受信任的服務。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal license-management.marketplace.amazonaws.com
  ```

  此命令成功後就不會產生輸出。

- AWS API: EnableAWSServiceAccess

使用 AWS Marketplace 停用受信任的存取

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

您只能使用 Organizations 工具來啟用受信任的存取。

您可以執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS 開發套件中的 Organizations API 操作，來停用受信任的存取

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以停用信任的服務存取：

- AWS CLI: disable-aws-service-access

  您可以執行下列命令來停用 AWS Marketplace 作為 Organizations 受信任的服務。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal license-management.marketplace.amazonaws.com
  ```

  此命令成功後就不會產生輸出。
- AWS API：DisableAWSServiceAccess

AWS Marketplace 私人 Marketplace 和 AWS Organizations

AWS Marketplace 是精心策劃的數位目錄，您可以使用它來尋找、購買、部署和管理建置解決方案和經營業務所需的第三方軟體、資料和服務。私人市場為您提供廣泛的產品目錄 AWS Marketplace，以及對這些產品的細粒度控制。

AWS Marketplace 私人 Marketplace 可讓您建立與整個組織、一或多個 OU 或組織中的一或多個帳戶相關聯的多個私人市集體驗，每個帳戶都有自己的核准產品集。您的 AWS 管理員也可以使用公司或團隊的標誌、訊息和色彩配置，將公司品牌套用至每個私人市集體驗。

如需詳細資訊，請參閱AWS Marketplace 購買指南中 AWS Marketplace的使用角色設定私人 Marketplace。

使用下列資訊來協助您將 AWS Marketplace 私人 Marketplace 與之整合 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您使用 AWS Marketplace Private Marketplace 主控台啟用受信任的存取時，系統會在組織的管理帳戶中自動建立下列服務連結角色。此角色可讓私人 Marketplace 在您組織的帳戶內執行支援的作業。只有在您停用私人 Marketplace 與組織之間的信任存取，並取消組織中所有 AWS Marketplace 私人市集體驗的關聯性時，您才可以刪除或修改此角色。

如果您直接從 Organizations 主控台、CLI 或 SDK 啟用受信任存取，則不會自動建立服務連結角色。

- `AWSServiceRoleForPrivateMarketplaceAdmin`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。私人 Marketplace 所使用的服務連結角色會授與下列服務主體的存取權：

- `private-marketplace.marketplace.amazonaws.com`

透過私人 Marketplace 啟用受信任存取

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

您可以使用 AWS Marketplace 私人 Marketplace 主控台或主控台啟用受信任的 AWS Organizations 存取。

> **Important**
>
> 我們強烈建議您盡可能使用 AWS Marketplace 私人 Marketplace 主控台或工具來啟用與 Organizations 的整合。這可讓 AWS Marketplace 私人 Marketplace 執行所需的任何設定，例如建立服務所需的資源。只有在您無法使用 AWS Marketplace 私人 Marketplace 提供的工具啟用整合時，才能繼續執行這些步驟。如需詳細資訊，請參閱本說明。
> 如果您使用 AWS Marketplace 私人 Marketplace 主控台或工具啟用受信任存取，則不需要完成這些步驟。

使用私人 Marketplace 主控台啟用受信任的存取

請參閱AWS Marketplace 購買指南中的「開始使用私人 Marketplace」。

您可以使用 AWS Organizations 主控台、執行 AWS CLI 命令或呼叫其中一個 AWS SDK 中的 API 作業來啟用受信任存取。

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。

2. 在 [服務] 頁面上，尋找 [AWS Marketplace 私人 Marketplace] 的資料列，選擇服務的名稱，然後選擇 [啟用信任的存取]。
3. 在確認對話方塊中，啟用顯示啟用受信任存取選項，在方塊中輸入 **enable**，然後選擇啟用受信任的存取。
4. 如果您只是的管理員 AWS Organizations，請告訴 AWS Marketplace 私人 Marketplace 的管理員，他們現在可以使用其控制台啟用該服務 AWS Organizations。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

您可以使用下列 AWS CLI 命令或 API 作業來啟用受信任的服務存取：

- AWS CLI: enable-aws-service-access

  您可以執行下列命令，將 AWS Marketplace 私人 Marketplace 啟用為 Organizations 的信任服務。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal private-marketplace.marketplace.amazonaws.com
  ```

  此命令成功後就不會產生輸出。
- AWS API：啟用 AWSServiceAccess

透過私人 Marketplace 停用受信任存取

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

您只能使用 Organizations 工具來停用受信任的存取。

您可以執行「Organizations」 AWS CLI 命令，或呼叫其中一個 AWS SDK 中的 Organizations API 作業來停用受信任的存取。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

您可以使用下列 AWS CLI 命令或 API 作業來停用受信任的服務存取：

- AWS CLI: disable-aws-service-access

您可以執行下列命令，將 AWS Marketplace 私人 Marketplace 停用為 Organizations 的信任服務。

```
$ aws organizations disable-aws-service-access \
    --service-principal private-marketplace.marketplace.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API：停用 AWSServiceAccess

啟用私人 Marketplace 的委派管理員帳戶

管理帳戶管理員可以將 Private Marketplace 管理權限委派給指定的成員帳戶 (稱為委派管理員)。若要將帳戶註冊為私人市集的委派管理員，管理帳戶管理員必須確保已啟用受信任存取和服務連結角色，選擇 [註冊新的系統管理員]，提供 12 位數的 AWS 帳號，然後選擇 [提交]。

管理帳戶和委派的管理員帳戶可以執行 Private Marketplace 管理工作，例如建立體驗、更新品牌設定、關聯或取消關聯對象、新增或移除產品，以及核准或拒絕待決請求。

若要使用私人 Marketplace 主控台設定委派的管理員，請參閱AWS Marketplace 購買指南中的建立和管理私人市集。

您也可以使用 Organizations `RegisterDelegatedAdministrator` API 來設定委派的管理員。若要取得更多資訊，請參閱 RegisterDelegatedAdministratorOrgan izations 指令參考中的〈〉。

停用私人 Marketplace 的委派管理員

只有組織管理帳戶中的系統管理員可以為私人 Marketplace 設定委派的管理員。

您可以使用私人 Marketplace 主控台或 API，或使用 Organizations `DeregisterDelegatedAdministrator` CLI 或 SDK 作業來移除委派的管理員。

若要使用私人 Marketplace 主控台停用委派的管理員私人 Marketplace 帳戶，請參閱AWS Marketplace 購買者指南中的建立和管理私人市集

AWS Network Manager 和 AWS Organizations

Network Manager 可讓您跨 AWS 帳戶、區域和內部部署位置，集中管理您的 AWS Cloud WAN 核心網路和您的 AWS Transit Gateway 網路。透過多帳戶支援，您可以為您的任一 AWS 帳戶建立單一全域網路，並使用 Network Manager 主控台將多個帳戶中的傳輸閘道註冊至全域網路。

啟用 Network Manager 和 Organizations 之間受信任的存取權後，已註冊的委派管理員和管理帳戶可以利用成員帳戶中部署的服務連結角色來描述連接至全域網路的資源。在 Network Manager 主控台中，註冊的委派管理員和管理帳戶可以承擔在成員帳戶中部署的自訂 IAM 角色：`CloudWatch-CrossAccountSharingRole` 用於多帳戶監控和事件，以及 `IAMRoleForAWSNetworkManagerCrossAccountResourceAccess` 用於主控台交換機角色存取權限，以查看和管理多帳戶資源。

> **Important**
>
> - 我們強烈建議使用 Network Manager 主控台來管理多帳戶設定 (啟用/停用受信任的存取權，以及註冊/取消註冊委派管理員)。若從主控台管理這些設定，即會自動將所有必需的服務連結角色和自訂 IAM 角色部署和管理至多帳戶存取所需的成員帳戶。
> - 當您在 Network Manager 主控台中啟用 Network Manager 的受信任存取時，主控台也會啟用 AWS CloudFormation StackSets 服務。Network Manager 使用 StackSets 部署多帳戶管理所需的自訂 IAM 角色。

如需有關將 Network Manager 與組織整合的詳細資訊，請參閱 Amazon VPC 使用者指南中的使用 AWS Organizations 管理多個 Network Manager 中的帳戶。

使用以下資訊可協助整合 AWS Network Manager 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在列出的組織帳戶中自動建立以下服務連結角色。這些角色允許 Network Manager 在您組織的帳戶中執行支援的操作。如果停用受信任的存取，Network Manager 將不會從組織中的帳戶刪除這些角色。您可以使用 IAM 主控台手動將其刪除。

管理帳戶

- `AWSServiceRoleForNetworkManager`
- `AWSServiceRoleForCloudFormationStackSetsOrgAdmin`
- `AWSServiceRoleForCloudWatchCrossAccount`

成員帳戶

- `AWSServiceRoleForNetworkManager`

- AWSServiceRoleForCloudFormationStackSetsOrgMember

當您將成員帳戶註冊為委派管理員時，將在委派管理員帳戶中自動建立以下附加角色：

- AWSServiceRoleForCloudWatchCrossAccount

服務連結角色所使用的服務委託人

服務連結角色只能由依據角色定義的信任關係所授權的服務主體來假設。

- 對於 AWSServiceRoleForNetworkManager service-linked 角色，networkmanager.amazonaws.com 是唯一具有存取權限的服務主體。
- 對於 AWSServiceRoleForCloudFormationStackSetsOrgMember 服務連結角色，member.org.stacksets.cloudformation.amazonaws.com 是唯一具有存取權限的服務主體。
- 對於 AWSServiceRoleForCloudFormationStackSetsOrgAdmin 服務連結角色，stacksets.cloudformation.amazonaws.com 是唯一具有存取權限的服務主體。
- 對於 AWSServiceRoleForCloudWatchCrossAccount 服務連結角色，cloudwatch-crossaccount.amazonaws.com 是唯一具有存取權限的服務主體。

刪除這些角色將影響 Network Manager 的多帳戶功能。

使用 Network Manager 啟用受信任存取

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

只有組織管理帳戶中的管理員，才具有使用其他 AWS 服務啟用受信任存取的許可。請務必使用 Network Manager 主控台來啟用受信任的存取，以避免權限問題。如需詳細資訊，請參閱 Amazon VPC 使用者指南中的使用 AWS Organizations 管理多個 Network Manager 中的帳戶。

使用 Network Manager 來停用受信任存取

如需啟用受信任的存取所需許可的資訊，請參閱停用信任的存取所需的許可。

只有 Organizations 管理帳戶中的管理員，才具有使用其他 AWS 服務停用受信任存取的許可。

> **Important**
>
> 我們強烈建議您使用 Network Manager 主控台來停用受信任的存取。如果您以任何其他方式停用受信任的存取權限 (例如使用 AWS CLI、使用 API 或使用 AWS CloudFormation 主控台)，則已部署 AWS CloudFormation StackSets 和自訂 IAM 角色可能無法正確清理。若要停用受信任的服務存取，請登入 Network Manager 主控台。

為 Network Manager 啟用委派的管理員帳戶

當您將成員帳戶指定為組織的委派管理員時，該帳戶的使用者和角色可以對 Network Manager 執行管理動作，否則只能由組織管理帳戶中的使用者或角色執行。這可協助您將組織的管理與 Network Manager 的管理分開。

如需如何將成員帳戶指定為組織中 Network Manager 的委派管理員，請參閱 Amazon VPC 使用者指南中的註冊委派管理員。

AWS Resource Access Manager 與 AWS Organizations

AWS Resource Access Manager (AWS RAM) 可讓您與其他 AWS 帳戶 共享您所擁有的特定 AWS 資源。這是一個集中化的服務，可為在多個帳戶間共用多種 AWS 資源提供一致的體驗。

如需有關 AWS RAM 的詳細資訊，請參閱《AWS RAM 使用者指南》。

使用以下資訊可協助整合 AWS Resource Access Manager 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下服務連結角色。該角色允許 AWS RAM 在您組織的組織帳戶中執行支援的操作。

只有在您停用 AWS RAM 和 Organizations 之間的受信任存取，或者從組織中刪除成員帳戶時，才能移除或修改此角色。

- `AWSServiceRoleForResourceAccessManager`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。AWS RAM 使用的服務連結角色會將存取權授予下列服務委託人：

- `ram.amazonaws.com`

使用 AWS RAM 啟用受信任的存取

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

您可以使用 AWS Resource Access Manager 主控台或 AWS Organizations 主控台來啟用信任存取。

> **Important**
>
> 強烈建議您盡可能使用 AWS Resource Access Manager 主控台或工具來啟用與 Organizations 整合。這可讓 AWS Resource Access Manager 執行其需要的任何組態，例如建立服務所需的資源。只有在您無法使用 AWS Resource Access Manager 提供的工具啟用整合時，才能繼續執行這些步驟。如需詳細資訊，請參閱本說明。
> 如果您使用 AWS Resource Access Manager 主控台或工具啟用受信任存取，則不需要完成這些步驟。

使用 AWS RAM 主控台或 CLI 來啟用受信任存取

請參閱AWS RAM使用者指南中的啟用與 AWS Organizations 共享。

您可以使用 AWS Organizations 主控台，執行 AWS CLI 命令，或呼叫其中一個 AWS 開發套件中的 API 操作，來啟用受信任的存取

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Services (服務) 頁面上，尋找 AWS Resource Access Manager 列，選擇服務的名稱，然後選擇 Enable trusted access (啟用受信任存取)。
3. 在確認對話方塊中，啟用顯示啟用受信任存取選項，在方塊中輸入 **`enable`**，然後選擇啟用受信任的存取。
4. 如果您只是 AWS Organizations 的系統管理員，請告訴 AWS Resource Access Manager 的管理員，他們現在可使用其主控台啟用該服務，以便與 AWS Organizations 搭配使用。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以啟用受信任的服務存取：

- AWS CLI: enable-aws-service-access

  您可以執行下列命令來啟用 AWS Resource Access Manager 作為 Organizations 受信任的服務。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal ram.amazonaws.com
  ```

  此命令成功後就不會產生輸出。

- AWS API: EnableAWSServiceAccess

使用 AWS RAM 停用受信任的存取

如需啟用受信任的存取所需許可的資訊，請參閱停用信任的存取所需的許可。

您可以使用 AWS Resource Access Manager 或 AWS Organizations 工具停用受信任存取。

> **Important**
>
> 強烈建議您盡可能使用 AWS Resource Access Manager 主控台或工具來停用與 Organizations 整合。這可讓 AWS Resource Access Manager 執行其所需的任何清除，例如刪除服務不再需要的資源或存取角色。只有在您無法使用 AWS Resource Access Manager 提供的工具停用整合成時，才能繼續執行這些步驟。
> 如果您使用 AWS Resource Access Manager 主控台或工具停用受信任的存取，則不需要完成這些步驟。

使用 AWS Resource Access Manager 主控台或 CLI 來停用受信任存取

請參閱AWS RAM使用者指南中的啟用與 AWS Organizations 共享。

您可以使用 AWS Organizations 主控台，執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS 開發套件中的 Organizations API 操作，來停用受信任的存取

AWS Management Console

使用 Organizations 主控台來受信停用任的服務存取

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Services (服務) 頁面上，尋找 AWS Resource Access Manager 列，然後選擇服務的名稱。
3. 選擇停用受信任的存取。
4. 在確認對話方塊中，輸入 **disable**，然後選擇停用受信任的存取。
5. 如果您只是 AWS Organizations 的系統管理員，請告訴 AWS Resource Access Manager 的管理員，他們現在可使用其主控台或工具停用該服務，以便與 AWS Organizations 搭配使用。

AWS CLI, AWS API

使用 Organizations CLI/開發套件來受信停用任的服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以停用信任的服務存取：

- AWS CLI: disable-aws-service-access

  您可以執行下列命令來停用 AWS Resource Access Manager 作為 Organizations 受信任的服務。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal ram.amazonaws.com
  ```

  此命令成功後就不會產生輸出。
- AWS API：DisableAWSServiceAccess

AWS 資源總管 與 AWS Organizations

AWS 資源總管 是一項資訊搜尋和探索服務。憑藉 Resource Explorer，您可以在類似網際網路搜尋引擎的體驗中探索您的資源，例如 Amazon Elastic Compute Cloud 執行個體、Amazon Kinesis Data Streams 或 Amazon DynamoDB 資料表。您可以使用名稱、標籤和 ID 等資源中繼資料來搜尋資源。Resource Explorer 在帳戶的 AWS 區域之間運作，可簡化您的跨區域工作負載。

當您將 Resource Explorer 與 AWS Organizations 整合時，可以透過在您的評定範圍內包含您組織的多個 AWS 帳戶，從更廣泛的來源收集證據。

使用以下資訊可協助整合 AWS 資源總管 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下服務連結角色。該角色允許 Resource Explorer 在您組織的組織帳戶中執行支援的操作。

只有在您停用 Resource Explorer 和 Organizations 之間的受信任存取，或者從組織中刪除成員帳戶時，才能移除或修改此角色。

如需有關 Resource Explorer 如何使用此角色的詳細資訊，請參閱《AWS 資源總管 使用者指南》中的使用服務連結角色。

- `AWSServiceRoleForResourceExplorer`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。Resource Explorer 使用的服務連結角色會將存取權授予下列服務主體：

- `resource-explorer-2.amazonaws.com`

若要啟用 AWS 資源總管 的受信任存取

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

Resource Explorer 需要對 AWS Organizations 的受信任存取，才能將成員帳戶指定為組織的委派管理員。

您可以使用 Resource Explorer 主控台或 Organizations 主控台來啟用受信任存取。我們強烈建議您盡可能使用 Resource Explorer 主控台或工具來啟用與 Organizations 整合。這可讓 AWS 資源總管 執行其需要的任何組態，例如建立服務所需的資源。

若要使用 Resource Explorer 主控台來啟用受信任存取

如需有關啟用受信任存取的說明，請參閱《AWS 資源總管 使用者指南》中的使用 Resource Explorer 的先決條件。

> **Note**
>
> 如果您使用 AWS 資源總管 主控台設定委派管理員，則 AWS 資源總管 會自動為您啟用受信任的存取。

您可以執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS 開發套件中的 Organizations API 操作，來啟用受信任的存取

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以啟用受信任的服務存取：

- AWS CLI: enable-aws-service-access

  您可以執行下列命令來啟用 AWS 資源總管 作為 Organizations 受信任的服務。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal resource-explorer-2.amazonaws.com
  ```

  此命令成功後就不會產生輸出。
- AWS API: EnableAWSServiceAccess

若要停用 Resource Explorer 的受信任存取

如需啟用受信任的存取所需許可的資訊，請參閱停用信任的存取所需的許可。

只有 AWS Organizations 管理帳戶中的管理員才能使用 AWS 資源總管 停用受信任的存取。

您可以使用 AWS 資源總管 或 AWS Organizations 工具停用受信任存取。

> **Important**
>
> 強烈建議您盡可能使用 AWS 資源總管 主控台或工具來停用與 Organizations 整合。這可讓 AWS 資源總管 執行其所需的任何清除，例如刪除服務不再需要的資源或存取角色。只有在您無法使用 AWS 資源總管 提供的工具停用整合成時，才能繼續執行這些步驟。
> 如果您使用 AWS 資源總管 主控台或工具停用受信任的存取，則不需要完成這些步驟。

您可以執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDK 中的 Organizations API 操作，來停用受信任存取。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以停用信任的服務存取：

- AWS CLI: disable-aws-service-access

  您可以執行下列命令來停用 AWS 資源總管 作為 Organizations 受信任的服務。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal resource-explorer-2.amazonaws.com
  ```

  此命令成功後就不會產生輸出。

- AWS API：DisableAWSServiceAccess

啟用 Resource Explorer 的委派管理員帳戶

使用您的委派管理員帳戶建立多帳戶資源檢視畫面，然後將範圍調整為組織單位或您的整個組織。您可以建立資源共用，透過 AWS Resource Access Manager 與您組織中的任何帳戶共用多帳戶檢視畫面。

> **最低許可**
>
> 只有具有下列許可之 Organizations 管理帳戶中的使用者或角色，才能將成員帳戶設定為組織中 Resource Explorer 的委派管理員：
> `resource-explorer:RegisterAccount`

如需有關啟用 Resource Explorer 委派管理員帳戶的說明，請參閱《AWS 資源總管 使用者指南》中的設定。

如果您使用 AWS 資源總管 主控台設定委派管理員，則 Resource Explorer 會自動為您啟用受信任的存取。

AWS CLI, AWS API

如果您想要使用 AWS CLI 或其中一個 AWS SDK，可以使用下列命令：

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal resource-explorer-2.amazonaws.com
```

- AWS SDK：呼叫 Organizations `RegisterDelegatedAdministrator` 操作和成員帳戶的 ID 號碼，並識別帳戶服務 `resource-explorer-2.amazonaws.com` 作為參數。

停用 Resource Explorer 的委派管理員

只有 Organizations 管理帳戶或 Resource Explorer 委派管理員帳戶中的管理員可以移除 Resource Explorer 的委派管理員。您可以使用 Organizations `DeregisterDelegatedAdministrator` CLI 或 SDK 操作停用受信任存取。

AWS Security Hub 和 AWS Organizations

AWS Security Hub 提供您中安全性狀態的全面檢視， AWS 並協助您根據安全性產業標準和最佳實務來檢查環境。

Security Hub 會從您的各個服務 AWS 帳戶、您使用的 AWS 服務以及支援的協力廠商合作夥伴產品收集安全性資料。它可協助您分析安全趨勢，並識別最高優先級的安全問題。

當您同時使用 Security Hub 和 AWS Organizations 同時使用時，您可以自動為所有帳戶啟用 Security Hub，包括新增帳戶時的新帳戶。這會增加 Security Hub 檢查和問題清單的涵蓋範圍，從而提供更全面和準確的整體安全狀態。

如需有關 Security Hub 的詳細資訊，請參閱 AWS Security Hub 使用者指南。

請使用下列資訊來協助您 AWS Security Hub 與整合 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下服務連結角色。該角色允許 Security Hub 在您組織的組織帳戶中執行支援的操作。

只有在您停用 Security Hub 和 Organizations 之間的受信任存取，或從組織中移除成員帳戶時，才能移除或修改此角色。

- `AWSServiceRoleForSecurityHub`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。Security Hub 使用的服務連結角色會將存取權授予下列服務委託人：

- `securityhub.amazonaws.com`

使用 Security Hub 來啟用受信任存取

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

當您指定 Security Hub 的委派管理員時，Security Hub 會自動啟用組織中 Security Hub 的受信任存取。

啟用 Security Hub 的委派管理員帳戶

當您將成員帳戶指定為組織的委派管理員時，該帳戶的使用者和角色可以對 Security Hub 執行管理動作，否則只能由組織管理帳戶中的使用者或角色執行。這可協助您將組織的管理與 Security Hub 的管理分開。

如需相關資訊，請參閱AWS Security Hub 使用者指南中的指定 Security Hub 管理員帳戶。

將成員帳戶指定為 Security Hub 的委派管理員

1. 使用 Organizations 管理帳戶登入。
2. 執行下列其中一項：
   - 如果您的管理帳戶未啟用 Security Hub，則在 Security Hub 主控台上選擇 Go to Security Hub (移至 Security Hub)。
   - 如果您的管理帳戶確實已啟用 Security Hub，請在 Security Hub 主控台的 [一般] 下選擇 [設定]。
3. 在 Delegated Administrator (委派的管理員) 下，輸入帳戶 ID。

Amazon S3 Storage Lens 與 AWS Organizations

透過授予 Amazon S3 Storage Lens 對您組織的受信任存取，您可以允許其收集和彙總您組織中所有 AWS 帳戶 的指標。S3 Storage Lens 會透過存取屬於您組織的帳戶清單，收集並分析所有這些帳戶的儲存體、用量和活動指標來執行此操作。

如需詳細資訊，請參閱 《Amazon S3 torage Lens 使用者指南》中的使用 Amazon S3 Storage Lens 的服務連結角色。

使用以下資訊可協助您整合 Amazon S3 Storage Lens 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取，且 Storage Lens 組態已套用至您的組織時，會自動在您組織的委派管理員帳戶建立以下服務連結角色。該角色允許 Amazon S3 Storage Lens 在您組織的組織帳戶中執行支援的操作。

只有在您停用 Amazon S3 Storage Lens 和 Organizations 之間的受信任存取，或從組織中移除該成員帳戶時，才能移除或修改此角色。

- `AWSServiceRoleForS3StorageLens`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。Amazon S3 Storage Lens 使用的服務連結角色會將存取權授予下列服務委託人：

- `storage-lens.s3.amazonaws.com`

啟用 Amazon S3 Storage Lens 的受信任存取

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

您可以使用 Amazon S3 Storage Lens 主控台或 AWS Organizations 主控台來啟用受信任存取。

> **Important**
>
> 強烈建議您盡可能使用 Amazon S3 Storage Lens 主控台或工具來啟用與 Organizations 整合。這可讓 Amazon S3 Storage Lens 執行其需要的任何組態，例如建立服務所需的資源。只

有在您無法使用 Amazon S3 Storage Lens 提供的工具啟用整合時，才能繼續執行這些步驟。如需詳細資訊，請參閱本說明。
如果您使用 Amazon S3 Storage Lens 主控台或工具啟用受信任的存取，則不需要完成這些步驟。

使用 Amazon S3 主控台來啟用受信任存取

請參閱 Amazon Simple Storage Service 使用者指南中的如何啟用受信任存取。

您可以使用 AWS Organizations 主控台，執行 AWS CLI 命令，或呼叫其中一個 AWS SDK 中的 API 操作，來啟用受信任存取。

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在服務頁面上，尋找 Amazon S3 Storage Lens 列，選擇服務的名稱，然後選擇啟用受信任存取。
3. 在確認對話方塊中，啟用顯示啟用受信任存取選項，在方塊中輸入 **enable**，然後選擇啟用受信任的存取。
4. 如果您只是 AWS Organizations 的系統管理員，請告訴 Amazon S3 Storage Lens 的管理員，他們現在可使用其主控台啟用該服務，以便與 AWS Organizations 搭配使用。

AWS CLI, AWS API

使用 Organizations CLI/開發套件來啟用受信任的服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以啟用受信任的服務存取：

- AWS CLI: enable-aws-service-access

  您可以執行下列命令來啟用 Amazon S3 Storage Lens 作為 Organizations 受信任的服務。

```
$ aws organizations enable-aws-service-access \
    --service-principal storage-lens.s3.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API: EnableAWSServiceAccess

停用 Amazon S3 Storage Lens 的受信任存取

如需啟用受信任的存取所需許可的資訊，請參閱停用信任的存取所需的許可。

您只能使用 Amazon S3 Storage Lens 工具來停用受信任存取。

您可以使用 Amazon S3 主控台、AWS CLI 或任何 AWS 開發套件來停用受信任存取。

使用 Amazon S3 主控台來停用受信任存取

請參閱 Amazon Simple Storage Service 使用者指南中的如何停用受信任存取。

啟用 Amazon S3 Storage Lens 的委派管理員帳戶

當您將成員帳戶指定為組織的委派管理員時，該帳戶的使用者和角色可以對 Amazon S3 Storage Lens 執行管理動作，否則只能由組織管理帳戶中的使用者或角色執行。這可協助您將組織的管理與 Amazon S3 Storage Lens 的管理分開。

> **最低許可**
>
> 只有具有下列許可的 Organizations 管理帳戶中的使用者或角色，才能將成員帳戶設定為組織中 Amazon S3 Storage Lens 的委託管理員：
> `organizations:RegisterDelegatedAdministrator`
> `organizations:DeregisterDelegatedAdministrator`

Amazon S3 Storage Lens 最多可支援您組織中的 5 個委派管理員帳戶。

將成員帳戶指定為 Amazon S3 Storage Lens 的委派管理員

您可以使用 Amazon S3 主控台、AWS CLI 或任何 AWS 開發套件來註冊委派管理員。若要使用 Amazon S3 主控台將成員帳戶註冊為組織的委派管理員帳戶，請參閱 Amazon Simple Storage Service 使用者指南中的如何註冊委派管理員。

取消註冊 Amazon S3 Storage Lens 的委派管理員。

您可以使用 Amazon S3 主控台、AWS CLI 或任何 AWS 開發套件來取消註冊委派管理員。若要使用 Amazon S3 主控台註銷委派管理員，請參閱 Amazon Simple Storage Service 使用者指南中的如何註銷委派管理員。

Amazon Security Lake 和 AWS Organizations

Amazon Security Lake 將來自雲端、內部部署和自訂來源的安全資料，集中到存放在您的帳戶的資料湖中。透過與 Organizations 整合，您可以建立資料湖來收集跨帳戶的日誌和事件。如需詳細資訊，請參閱 Amazon Security Lake 使用者指南中的 使用 AWS Organizations 管理多個帳戶。

使用下列資訊可協助您將 Amazon 安全湖與 AWS Organizations.

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下服務連結角色。此角色可讓 Amazon Security Lake 在組織帳戶內執行受支援的操作。

只有在停用 Amazon Security Lake 和組織之間的受信任存取，或從組織中移除成員帳戶時，才可以刪除或修改此角色。

- `AWSServiceRoleForSecurityLake`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。Amazon 安全湖使用的服務連結角色可授與下列服務主體的存取權：

- `securitylake.amazonaws.com`

透過 Amazon 安全湖啟用受信任存取

當您使用 Security Lake 啟用受信任存取時，Security Lake 可以自動對組織成員資格的變更做出回應。委派的系統管理員可以啟用任何組織帳戶中支援服務的 AWS 記錄收集功能。如需詳細資訊，請參閱 Amazon Security Lake 使用者指南中的 Amazon Security Lake 的服務連結角色。

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

您只能使用 Organizations 工具來啟用受信任存取。

您可以使用 AWS Organizations 主控台、執行 AWS CLI 命令或呼叫其中一個 AWS SDK 中的 API 作業來啟用受信任的存取。

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在服務頁面上，尋找 Amazon Security Lake 列，選擇服務的名稱，然後選擇啟用受信任存取。
3. 在確認對話方塊中，啟用顯示啟用受信任存取選項，在方塊中輸入 **enable**，然後選擇啟用受信任的存取。
4. 如果您只是管理員 AWS Organizations，請告訴 Amazon Security Lake 的管理員，他們現在可以使用其主控台啟用該服務 AWS Organizations。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

您可以使用下列 AWS CLI 命令或 API 作業來啟用受信任的服務存取：

- AWS CLI: enable-aws-service-access

  您可以執行下列命令來啟用 Amazon Security Lake 作為 Organizations 受信任的服務。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal securitylake.amazonaws.com
  ```

  此命令成功後就不會產生輸出。
- AWS API：啟用 AWSServiceAccess

使用 Amazon 安全湖停用受信任存取

只有 Organizations 管理帳戶中的管理員可以使用 Amazon 安全湖停用受信任的存取。

您只能使用 Organizations 工具來停用受信任的存取。

您可以使用 AWS Organizations 主控台、執行 Organizations AWS CLI 命令或呼叫其中一個 AWS SDK 中的 Organizations API 作業來停用受信任的存取。

AWS Management Console

使用 Organizations 主控台來受信停用任的服務存取

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在服務頁面上，尋找 Amazon Security Lake 列，然後選擇服務的名稱。
3. 選擇停用受信任的存取。
4. 在確認對話方塊中，輸入 **disable**，然後選擇停用受信任的存取。
5. 如果您是唯一的管理員 AWS Organizations，請告訴 Amazon Security Lake 的管理員，他們現在可以使用其主控台或工具停用該服務，無法使用該服務 AWS Organizations。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

您可以使用下列 AWS CLI 命令或 API 作業來停用受信任的服務存取：

- AWS CLI: disable-aws-service-access

  您可以執行下列命令來停用 Amazon Security Lake 作為 Organizations 受信任的服務。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal securitylake.amazonaws.com
  ```

  此命令成功後就不會產生輸出。
- AWS API：停用 AWSServiceAccess

啟用 Amazon 安全湖的委派管理員帳戶

Amazon 安全湖委派管理員會將組織中的其他帳戶新增為成員帳戶。委派的管理員可以啟用 Amazon 安全湖，並為成員帳戶設定 Amazon 安全湖設定。委派的管理員可以在啟用 Amazon Security Lake 的所有 AWS 區域中，跨組織收集日誌 (無論您目前使用的是哪個區域端點)。

您還可以設定委派管理員在組織中自動將新帳戶新增為成員。Amazon 安全湖委派管理員可以存取關聯成員帳戶中的日誌和事件。因此，您可以設定 Amazon 安全湖來收集關聯成員帳戶擁有的資料。您還可以授權訂閱用戶取用關聯成員帳戶擁有的資料。

如需詳細資訊，請參閱 Amazon Security Lake 使用者指南中的 使用 AWS Organizations 管理多個帳戶。

> **最低許可**
>
> 只有組 Organizations 管理帳戶中的管理員可以將成員帳戶設定為組織中 Amazon Security Lake 的委派管理員

您可以使用 Amazon 安全湖控制台、Amazon 安全湖 `CreateDatalakeDelegatedAdmin` API 動作或 `create-datalake-delegated-admin` CLI 命令來指定委派的管理員帳戶。或者，您可以使用 Organizations `RegisterDelegatedAdministrator` CLI 或 SDK 操作。如需針對 Amazon Security Lake 啟用委派管理員帳戶的相關指示，請參閱 Amazon Security Lake 使用者指南中的指定委派的安全湖管理員和新增成員帳戶。

AWS CLI, AWS API

如果您想要使用 AWS CLI 或其中一個 AWS SDK 來設定委派的系統管理員帳戶，可以使用下列命令：

- AWS CLI:

```
$  aws organizations register-delegated-administrator \
    --account-id 123456789012 \ --service-principal securitylake.amazonaws.com
```

- AWS SDK：呼叫「Organizations」`RegisterDelegatedAdministrator` 作業和成員帳戶的 ID 號碼，並將帳戶服務主體識別`account.amazonaws.com`為參數。

停用 Amazon 安全湖的委派管理員

只有組 Organizations 管理帳戶或 Amazon Security Lake 委派管理員帳戶中的管理員可以從組織中移除委派的管理員帳戶。

您可以使用 Amazon 安全湖 `DeleteDatalakeDelegatedAdmin` API 動作、`delete-datalake-delegated-admin` CLI 命令或使用 Organizations `DeregisterDelegatedAdministrator` CLI

或 SDK 作業來移除委派的管理員帳戶。若要使用 Amazon 安全湖移除委派的管理員，請參閱 Amazon 安全湖使用者指南中的移除 Amazon 安全湖委派管理員。

AWS Service Catalog 與 AWS Organizations

Service Catalog 可讓您建立和管理已核准在 AWS 上使用的 IT 服務目錄。

Service Catalog 與 AWS Organizations 整合可簡化組織中產品組合的共用及產品的複製。Service Catalog 管理員可以在共用產品組合時參照 AWS Organizations 中的現有組織，而且可以與組織樹狀結構中的任何可信組織單位 (OU) 共用產品組合。這會消除共用產品組合 ID 的需求，且接收帳戶可在匯入產品組合時手動參考產品組合 ID。透過此機制共用的產品組合會列在 Service Catalog 中管理員之 Imported Portfolio (匯入產品組合) 檢視的共用帳戶中。

如需有關 Service Catalog 的詳細資訊，請參閱《Service Catalog 管理員指南》。

使用以下資訊可協助整合 AWS Service Catalog 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

AWS Service Catalog 不會建立任何服務連結的角色，作為啟用受信任存取的一部分。

用於授予許可的服務委託人

若要啟用受信任存取，必須指定下列服務委託人：

- `servicecatalog.amazonaws.com`

使用 Service Catalog 啟用可信存取

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

您可以使用 AWS Service Catalog 主控台或 AWS Organizations 主控台來啟用信任存取。

> **Important**
>
> 強烈建議您盡可能使用 AWS Service Catalog 主控台或工具來啟用與 Organizations 整合。這可讓 AWS Service Catalog 執行其需要的任何組態，例如建立服務所需的資源。只有在您無法使用 AWS Service Catalog 提供的工具啟用整合時，才能繼續執行這些步驟。如需詳細資訊，請參閱本說明。

如果您使用 AWS Service Catalog 主控台或工具啟用受信任存取，則不需要完成這些步驟。

使用 Service Catalog CLI 或 AWS SDK 來啟用可信存取

呼叫以下其中一個命令或一項操作：

- AWS CLI: aws servicecatalog enable-aws-organizations-access
- AWS SDKs: AWSServiceCatalog::EnableAWSOrganizationsAccess

您可以使用 AWS Organizations 主控台，執行 AWS CLI 命令，或呼叫其中一個 AWS SDK 中的 API 操作，來啟用受信任存取。

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Services (服務) 頁面上，尋找 AWS Service Catalog 列，選擇服務的名稱，然後選擇 Enable trusted access (啟用受信任存取)。
3. 在確認對話方塊中，啟用顯示啟用受信任存取選項，在方塊中輸入 **enable**，然後選擇啟用受信任的存取。
4. 如果您只是 AWS Organizations 的系統管理員，請告訴 AWS Service Catalog 的管理員，他們現在可使用其主控台啟用該服務，以便與 AWS Organizations 搭配使用。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以啟用受信任的服務存取：

- AWS CLI: enable-aws-service-access

  您可以執行下列命令來啟用 AWS Service Catalog 作為 Organizations 受信任的服務。

```
$ aws organizations enable-aws-service-access \
    --service-principal servicecatalog.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API: EnableAWSServiceAccess

使用 Service Catalog 停用可信存取

如需啟用受信任的存取所需許可的資訊，請參閱停用信任的存取所需的許可。

如果您要在使用 Service Catalog 時透過 AWS Organizations 來停用可信存取，則將不會刪除目前的共用，但您也無法經由組織建立新的共用。如果呼叫此動作導致目前共享變更，將不會在您的組織結構中同步。

您可以使用 AWS Service Catalog 或 AWS Organizations 工具停用受信任存取。

> **Important**
>
> 強烈建議您盡可能使用 AWS Service Catalog 主控台或工具來停用與 Organizations 整合。這可讓 AWS Service Catalog 執行其所需的任何清除，例如刪除服務不再需要的資源或存取角色。只有在您無法使用 AWS Service Catalog 提供的工具停用整合成時，才能繼續執行這些步驟。
>
> 如果您使用 AWS Service Catalog 主控台或工具停用受信任的存取，則不需要完成這些步驟。

使用 Service Catalog CLI 或 AWS SDK 來停用可信存取

呼叫以下其中一個命令或一項操作：

- AWS CLI: aws servicecatalog disable-aws-organizations-access
- AWS SDKs: DisableAWSOrganizationsAccess

您可以使用 AWS Organizations 主控台，執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS 開發套件中的 Organizations API 操作，來停用受信任的存取

AWS Management Console

使用 Organizations 主控台來受信停用任的服務存取

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。

2. 在 Services (服務) 頁面上，尋找 AWS Service Catalog 列，然後選擇服務的名稱。
3. 選擇停用受信任的存取。
4. 在確認對話方塊中，輸入 **disable**，然後選擇停用受信任的存取。
5. 如果您只是 AWS Organizations 的系統管理員，請告訴 AWS Service Catalog 的管理員，他們現在可使用其主控台或工具停用該服務，以便與 AWS Organizations 搭配使用。

AWS CLI, AWS API

使用 Organizations CLI/開發套件來受信停用任的服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以停用信任的服務存取：

- AWS CLI: disable-aws-service-access

  您可以執行下列命令來停用 AWS Service Catalog 作為 Organizations 受信任的服務。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal servicecatalog.amazonaws.com
  ```

  此命令成功後就不會產生輸出。
- AWS API：DisableAWSServiceAccess

Service Quotas 與 AWS Organizations

Service Quotas 是一種 AWS 服務，可供您集中查看和管理您的配額。「配額」也稱為限制，即您的 AWS 帳戶 中的資源、動作與項目的最大值。

Service Quotas 與 AWS Organizations 如果已有關聯，您便可以建立配額請求範本，以供帳戶建立時自動請求提高配額。

如需 Service Quotas 的詳細資訊，請參閱 Service Quotas 使用者指南。

使用以下資訊可協助整合 Service Quotas 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下服務連結角色。該角色允許 Service Quotas 在您組織的組織帳戶中執行支援的操作。

只有在您停用 Service Quotas 和 Organizations 之間的受信任存取，或從組織中移除成員帳戶時，才能移除或修改此角色。

- `AWSServiceRoleForServiceQuotas`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。Service Quotas 使用的服務連結角色會將存取權授予下列服務委託人：

- `servicequotas.amazonaws.com`

啟用受信任存取與其他 Service Quotas 服務

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

您可以僅使用 Service Quotas 來啟用受信任存取。

您可以使用 Service Quotas 主控台、AWS CLI 或 SDK 來啟用受信任存取：

- 使用 Service Quotas 主控台來啟用受信任存取。

  登入您的 AWS Organizations 管理帳戶，接著在 Service Quotas 主控台上設定範本。如需詳細資訊，請參閱 Service Quotas 使用者指南中的使用 Service Quota 範本。
- 使用 Service Quotas AWS CLI 或開發套件來啟用受信任存取。

  呼叫以下命令或操作：

  - AWS CLI: aws service-quotas associate-service-quota-template
  - AWS SDKs: AssociateServiceQuotaTemplate

AWS IAM Identity Center 與 AWS Organizations

AWS IAM Identity Center 為所有 AWS 帳戶 和雲端應用程式提供單一登入存取。它會透過 AWS Directory Service 與 Microsoft Active Directory 連接，允許該目錄中的使用者使用他們現有的 Active Directory 使用者名稱和密碼，來登入個人化的 AWS 存取入口網站。從 AWS 存取入口網站，使用者可存取他們具有許可的所有 AWS 帳戶 和雲端應用程式。

如需 IAM Identity Center 的詳細資訊，請參閱 《AWS IAM Identity Center 使用者指南》。

使用以下資訊可協助整合 AWS IAM Identity Center 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下服務連結角色。此角色允許 IAM Identity Center 在您組織的組織帳戶中執行支援的操作。

只有在您停用 IAM Identity Center 與 Organizations 之間的受信任存取，或者從組織中移除成員帳戶時，才能刪除或修改此角色。

- `AWSServiceRoleForSSO`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。IAM Identity Center 使用的服務連結角色會將存取權授予下列服務主體：

- `sso.amazonaws.com`

使用 IAM Identity Center 來啟用受信任存取

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

您可以使用 AWS IAM Identity Center 主控台或 AWS Organizations 主控台來啟用信任存取。

> **Important**
>
> 強烈建議您盡可能使用 AWS IAM Identity Center 主控台或工具來啟用與 Organizations 整合。這可讓 AWS IAM Identity Center 執行其需要的任何組態，例如建立服務所需的資源。只有在您無法使用 AWS IAM Identity Center 提供的工具啟用整合時，才能繼續執行這些步驟。如需詳細資訊，請參閱本說明。
>
> 如果您使用 AWS IAM Identity Center 主控台或工具啟用受信任存取，則不需要完成這些步驟。

IAM Identity Center 需要受信任存取和 AWS Organizations 才能運作。當您設定 IAM Identity Center 時會啟用受信任的存取。如需詳細資訊，請參閱AWS IAM Identity Center使用者指南中的入門 – 步驟 1：啟用AWS IAM Identity Center。

您可以使用 AWS Organizations 主控台，執行 AWS CLI 命令，或呼叫其中一個 AWS 開發套件中的 API 操作，來啟用受信任的存取

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Services (服務) 頁面上，尋找 AWS IAM Identity Center 列，選擇服務的名稱，然後選擇 Enable trusted access (啟用受信任存取)。
3. 在確認對話方塊中，啟用顯示啟用受信任存取選項，在方塊中輸入 **enable**，然後選擇啟用受信任的存取。
4. 如果您只是 AWS Organizations 的系統管理員，請告訴 AWS IAM Identity Center 的管理員，他們現在可使用其主控台啟用該服務，以便與 AWS Organizations 搭配使用。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以啟用受信任的服務存取：

- AWS CLI: enable-aws-service-access

  您可以執行下列命令來啟用 AWS IAM Identity Center 作為 Organizations 受信任的服務。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal sso.amazonaws.com
  ```

  此命令成功後就不會產生輸出。
- AWS API: EnableAWSServiceAccess

使用 IAM Identity Center 來停用受信任存取

如需啟用受信任的存取所需許可的資訊，請參閱停用信任的存取所需的許可。

IAM Identity Center 需要受信任存取和 AWS Organizations 才能操作。如果您在使用 IAM Identity Center 時，使用 AWS Organizations 停用受信任存取，則會因為無法存取組織而停止運作。使用

者無法使用 IAM Identity Center 來存取帳戶。會保留 IAM Identity Center 建立的任何角色，但 IAM Identity Center 服務無法加以存取。會保留 IAM Identity Center 服務連結角色。如果您重新啟用受信任存取，IAM Identity Center 會繼續如之前般運作，而不需重新設定服務。

如果從您的組織移除帳戶，IAM Identity Center 自動會清理任何中繼資料和資源，例如其服務連結角色。從組織移除的獨立帳戶，不再能與 IAM Identity Center 搭配使用。

您只能使用 Organizations 工具來停用受信任的存取。

您可以使用 AWS Organizations 主控台，執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS 開發套件中的 Organizations API 操作，來停用受信任的存取

AWS Management Console

使用 Organizations 主控台來受信停用任的服務存取

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Services (服務) 頁面上，尋找 AWS IAM Identity Center 列，然後選擇服務的名稱。
3. 選擇停用受信任的存取。
4. 在確認對話方塊中，輸入 **disable**，然後選擇停用受信任的存取。
5. 如果您只是 AWS Organizations 的系統管理員，請告訴 AWS IAM Identity Center 的管理員，他們現在可使用其主控台或工具停用該服務，以便與 AWS Organizations 搭配使用。

AWS CLI, AWS API

使用 Organizations CLI/開發套件來受信停用任的服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以停用信任的服務存取：

- AWS CLI: disable-aws-service-access

  您可以執行下列命令來停用 AWS IAM Identity Center 作為 Organizations 受信任的服務。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal sso.amazonaws.com
  ```

  此命令成功後就不會產生輸出。
- AWS API：DisableAWSServiceAccess

啟用 IAM Identity Center 的委派管理員帳戶

當您將成員帳戶指定為組織的委派管理員時，該帳戶的使用者和角色可以對 IAM Identity Center 執行管理動作，否則只能由組織管理帳戶中的使用者或角色執行。這可協助您將組織的管理與 IAM Identity Center 的管理分開。

> **最低許可**
>
> 只有 Organizations 管理帳戶中的使用者或角色，才能將成員帳戶設定為組織中 IAM Identity Center 的委派管理員。

如需有關如何為 IAM Identity Center 啟用委派管理員帳戶的說明，請參閱 AWS IAM Identity Center 使用者指南中的委派的管理員。

AWS Systems Manager 與 AWS Organizations

AWS Systems Manager 是一組可呈現和控制 AWS 資源的功能。在您組織的所有 AWS 帳戶 中，以下 Systems Manager 功能皆可與 Organizations 搭配使用：

- Systems Manager Explorer 是一項可自訂操作儀表板，用於報告 AWS 資源的相關資訊。您可以使用 Organizations 和 Systems Manager Explorer，同步組織中所有 AWS 帳戶 的操作資料。如需詳細資訊，請參閱AWS Systems Manager使用者指南中的 Systems Manager Explorer。
- Systems Manager Change Manager 是一個企業變更管理架構，用於請求、核准、實作和報告應用程式組態和基礎結構的操作變更。如需詳細資訊，請參閱AWS Systems Manager使用者指南中的 AWS Systems ManagerChange Manager。
- Systems Manager OpsCenter 提供一個集中的位置，操作工程師和 IT 專業人員可在此檢視、調查和解決與 AWS 資源相關的操作工作項目 (OpsItems)。當您將 OpsCenter 與 Organizations 搭配使用時，其支援在單一工作階段期間從管理帳戶 (Organizations 管理帳戶或 Systems Manager 委派的管理員帳戶) 與另一個帳戶使用 OpsItems。設定完成後，使用者可以執行以下類型的動作：
  - 在另一個帳戶中建立、檢視和更新 OpsItems。
  - 檢視另一個帳戶中 OpsItems 指定之 AWS 資源的詳細資訊。
  - 啟動 Systems Manager 自動化執行腳本，以修補另一個帳戶中 AWS 資源的問題。

  如需詳細資訊，請參閱《AWS Systems Manager 使用者指南》中的AWS Systems Manager OpsCenter。

使用以下資訊可協助整合 AWS Systems Manager 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下服務連結角色。該角色允許 Systems Manager 在您組織的組織帳戶中執行支援的操作。

只有在您停用 Systems Manager 和 Organizations 之間的受信任存取，或是從組織中移除成員帳戶時，才能移除或修改此角色。

- `AWSServiceRoleForAmazonSSM_AccountDiscovery`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。Systems Manager 使用的服務連結角色會將存取權授予下列服務委託人：

- `ssm.amazonaws.com`

使用 Systems Manager 來啟用受信任存取

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

您只能使用 Organizations 工具來啟用受信任存取。

您可以使用 AWS Organizations 主控台，執行 AWS CLI 命令，或呼叫其中一個 AWS 開發套件中的 API 操作，來啟用受信任的存取

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Services (服務) 頁面上，尋找 AWS Systems Manager 列，選擇服務的名稱，然後選擇 Enable trusted access (啟用受信任存取)。
3. 在確認對話方塊中，啟用顯示啟用受信任存取選項，在方塊中輸入 **`enable`**，然後選擇啟用受信任的存取。

4. 如果您只是 AWS Organizations 的系統管理員，請告訴 AWS Systems Manager 的管理員，他們現在可使用其主控台啟用該服務，以便與 AWS Organizations 搭配使用。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以啟用受信任的服務存取：

- AWS CLI: enable-aws-service-access

  您可以執行下列命令來啟用 AWS Systems Manager 作為 Organizations 受信任的服務。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal ssm.amazonaws.com
  ```

  此命令成功後就不會產生輸出。
- AWS API: EnableAWSServiceAccess

使用 Systems Manager 來停用受信任存取

如需啟用受信任的存取所需許可的資訊，請參閱停用信任的存取所需的許可。

Systems Manager 需要 AWS Organizations 的受信任存取，才能同步您組織中 AWS 帳戶 的操作資料。如果您停用信任存取，則 Systems Manager 無法同步操作資料，還會報告錯誤。

您只能使用 Organizations 工具來停用受信任的存取。

您可以使用 AWS Organizations 主控台，執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS 開發套件中的 Organizations API 操作，來停用受信任的存取

AWS Management Console

使用 Organizations 主控台來受信停用任的服務存取

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Services (服務) 頁面上，尋找 AWS Systems Manager 列，然後選擇服務的名稱。
3. 選擇停用受信任的存取。

4. 在確認對話方塊中，輸入 **disable**，然後選擇停用受信任的存取。
5. 如果您只是 AWS Organizations 的系統管理員，請告訴 AWS Systems Manager 的管理員，他們現在可使用其主控台或工具停用該服務，以便與 AWS Organizations 搭配使用。

AWS CLI, AWS API

使用 Organizations CLI/開發套件來受信停用任的服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以停用信任的服務存取：

- AWS CLI: disable-aws-service-access

  您可以執行下列命令來停用 AWS Systems Manager 作為 Organizations 受信任的服務。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal ssm.amazonaws.com
  ```

  此命令成功後就不會產生輸出。
- AWS API：DisableAWSServiceAccess

啟用 Systems Manager 的委派管理員帳戶

當您將成員帳戶指定為組織的委派管理員時，該帳戶的使用者和角色可以對 Systems Manager 執行管理動作，否則只能由組織管理帳戶中的使用者或角色執行。這可協助您將組織的管理與 Systems Manager 的管理分開。

如果您在整個組織中使用 Change Manager，則會使用委派管理員帳戶。這是已指定為 Change Manager 中用於管理變更範本、變更請求、變更 Runbook 和核准工作流程的 AWS 帳戶。委派的帳戶會管理整個組織的變更活動。當您設定組織以配合 Change Manager 使用時，可以指定哪些帳號擔任此角色。它不必是組織的管理帳戶。如果您僅以單一帳戶使用 Change Manager，則不需要委派管理員帳戶。

若要將成員帳戶指定為委派管理員，請查看《AWS Systems Manager 使用者指南》中的以下主題：

- 關於 Explorer 和 OpsCenter，請參閱《設定委派管理員》。
- 關於 Systems Manager Change Manager，請參閱設定 Change Manager 的組織和委派帳戶。

標籤政策和 AWS Organizations

標籤政策是 AWS Organizations 中的一種政策，可協助您標準化組織帳戶中各資源的標籤。如需標籤政策的詳細資訊，請參閱標籤政策。

使用以下資訊可協助整合標籤整合與 AWS Organizations。

服務連結角色所使用的服務委託人

Organizations 使用下列服務委託人與連接至您資源的標籤互動。

- `tagpolicies.tag.amazonaws.com`

啟用標籤政策的受信任存取

您可以透過啟用組織中的標籤政策，或使用 AWS Organizations 主控台來啟用受信任存取。

> **Important**
>
> 強烈建議您透過啟用標記政策來啟用受信任存取。這可讓 Organizations 執行必要的設定任務。

您可以在 AWS Organizations 主控台中啟用標籤政策類型，來啟用標籤政策的受信任存取。如需詳細資訊，請參閱 啟用政策類型。

您可以使用 AWS Organizations 主控台，執行 AWS CLI 命令，或呼叫其中一個 AWS 開發套件中的 API 操作，來啟用受信任的存取

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在服務頁面上，尋找標籤政策列，選擇服務的名稱，然後選擇啟用受信任存取。
3. 在確認對話方塊中，啟用顯示啟用受信任存取選項，在方塊中輸入 **`enable`**，然後選擇啟用受信任的存取。

4. 如果您只是 AWS Organizations 的系統管理員，請告訴標籤政策的管理員，他們現在可使用其主控台啟用該服務，以便與 AWS Organizations 搭配使用。

AWS CLI, AWS API

使用 Organizations CLI/開發套件來啟用受信任的服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以啟用受信任的服務存取：

- AWS CLI: enable-aws-service-access

  您可以執行下列命令來啟用標籤政策作為 Organizations 受信任的服務。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal tagpolicies.tag.amazonaws.com
  ```

  此命令成功後就不會產生輸出。
- AWS API: EnableAWSServiceAccess

使用標籤政策來停用受信任存取

您可以在 AWS Organizations 主控台中停用標籤政策類型，來停用標籤政策的受信任存取。如需詳細資訊，請參閱 停用政策類型。

AWS Trusted Advisor 與 AWS Organizations

AWS Trusted Advisor 可檢查您的 AWS 環境，並在有可能節省成本、提升系統可用性與效能或填補安全漏洞時向您提出建議。與 Organizations 整合後，您可以接收組織中所有帳戶的 Trusted Advisor 檢查結果，以及下載報告，以檢視檢查和任何受影響資源的報告。

如需詳細資訊，請參閱AWS Support使用者指南中的 AWS Trusted Advisor 的 組織檢視。

使用以下資訊可協助整合 AWS Trusted Advisor 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下服務連結角色。該角色允許 Trusted Advisor 在您組織的組織帳戶中執行支援的操作。

只有在您停用 Trusted Advisor 和 Organizations 之間的受信任存取，或者從組織中刪除成員帳戶時，才能移除或修改此角色。

- `AWSServiceRoleForTrustedAdvisorReporting`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。Trusted Advisor 使用的服務連結角色會將存取權授予下列服務委託人：

- `reporting.trustedadvisor.amazonaws.com`

使用 Trusted Advisor 啟用受信任的存取

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

您可以僅使用 AWS Trusted Advisor 來啟用受信任存取。

使用 Trusted Advisor 主控台來啟用受信任的存取權

請參閱AWS Support使用者指南中的啟用組織檢視。

使用 Trusted Advisor 停用受信任的存取

如需啟用受信任的存取所需許可的資訊，請參閱停用信任的存取所需的許可。

停用此功能之後，Trusted Advisor 會停止記錄組織中所有其他帳戶的檢查資訊。您無法檢視或下載現有的報告或建立新的報告。

您可以使用 AWS Trusted Advisor 或 AWS Organizations 工具停用受信任存取。

> **Important**
>
> 強烈建議您盡可能使用 AWS Trusted Advisor 主控台或工具來停用與 Organizations 整合。這可讓 AWS Trusted Advisor 執行其所需的任何清除，例如刪除服務不再需要的資源或存取角色。只有在您無法使用 AWS Trusted Advisor 提供的工具停用整合成時，才能繼續執行這些步驟。
>
> 如果您使用 AWS Trusted Advisor 主控台或工具停用受信任的存取，則不需要完成這些步驟。

使用 Trusted Advisor 主控台來停用受信任存取

請參閱AWS Support使用者指南中的停用組織檢視。

您可以執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS 開發套件中的 Organizations API 操作，來停用受信任的存取

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以停用信任的服務存取：

- AWS CLI: disable-aws-service-access

  您可以執行下列命令來停用 AWS Trusted Advisor 作為 Organizations 受信任的服務。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal reporting.trustedadvisor.amazonaws.com
  ```

  此命令成功後就不會產生輸出。
- AWS API：DisableAWSServiceAccess

啟用 Trusted Advisor 的委派管理員帳戶

當您將成員帳戶指定為組織的委派管理員時，來自指定帳戶的使用者和角色可以為組織中的其他成員帳戶管理 AWS 帳戶 中繼資料。如果您未啟用委派系統管理員帳戶，則只有組織的管理帳戶才能執行這任務。這可協助您將組織的管理與帳戶詳細資訊的管理分開。

> **最低許可**
>
> 只有 Organizations 管理帳戶中的使用者或角色，才能將成員帳戶設定為組織中 Trusted Advisor 的委派管理員

如需有關如何啟用 Trusted Advisor 委派管理員帳戶的說明，請參閱《AWS Support 使用者指南》中的註冊委派管理員。

AWS CLI, AWS API

如果您想要使用 AWS CLI 或其中一個 AWS SDK，可以使用下列命令：

- AWS CLI:

```
$  aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal reporting.trustedadvisor.amazonaws.com
```

- AWS SDK：呼叫 Organizations `RegisterDelegatedAdministrator` 操作和成員帳戶的 ID 號碼，並識別帳戶服務主體 `account.amazonaws.com` 作為參數。

停用 Trusted Advisor 的委派管理員

您可以使用 Trusted Advisor 主控台或使用 Organizations `DeregisterDelegatedAdministrator` CLI 或 SDK 操作，移除委派管理員。如需如何使用 Trusted Advisor 主控台停用委派管理員 Trusted Advisor 帳戶的資訊，請參閱《AWS Support 使用者指南》中的取消註冊委派管理員。

AWS Well-Architected Tool 與 AWS Organizations

AWS Well-Architected Tool 可協助您記錄工作負載的狀態，並將其與最新的 AWS 架構最佳實務做比較。

使用 AWS Well-Architected Tool 搭配 Organizations 讓 AWS Well-Architected Tool 和 Organizations 客戶都能簡化與其組織的其他成員共用 AWS Well-Architected Tool 資源的流程。

如需詳細資訊，請參閱《AWS Well-Architected Tool 使用者指南》中的共用 AWS Well-Architected Tool 資源。

使用以下資訊可協助整合 AWS Well-Architected Tool 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下服務連結角色。該角色允許 AWS WA Tool 在您組織的組織帳戶中執行支援的操作。

只有在您停用 AWS WA Tool 和 Organizations 之間的受信任存取，或者從組織中刪除成員帳戶時，才能移除或修改此角色。

- `AWSServiceRoleForWellArchitected`

服務角色政策為 `AWSWellArchitectedOrganizationsServiceRolePolicy`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。AWS WA Tool 使用的服務連結角色會將存取權授予下列服務委託人：

- `wellarchitected.amazonaws.com`

使用 AWS WA Tool 啟用受信任的存取

允許更新 AWS WA Tool 以反映組織中的階層變更。

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

您可以使用 AWS Well-Architected Tool 主控台或 AWS Organizations 主控台來啟用信任存取。

> **Important**
>
> 強烈建議您盡可能使用 AWS Well-Architected Tool 主控台或工具來啟用與 Organizations 整合。這可讓 AWS Well-Architected Tool 執行其需要的任何組態，例如建立服務所需的資源。只有在您無法使用 AWS Well-Architected Tool 提供的工具啟用整合時，才能繼續執行這些步驟。如需詳細資訊，請參閱本說明。
>
> 如果您使用 AWS Well-Architected Tool 主控台或工具啟用受信任存取，則不需要完成這些步驟。

使用 AWS WA Tool 主控台來啟用受信任的存取權

請參閱《AWS Well-Architected Tool 使用者指南》中的共用 AWS Well-Architected Tool 資源。

您可以使用 AWS Organizations 主控台，執行 AWS CLI 命令，或呼叫其中一個 AWS SDK 中的 API 操作，來啟用受信任存取。

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在 Services (服務) 頁面上，尋找 AWS Well-Architected Tool 列，選擇服務的名稱，然後選擇 Enable trusted access (啟用受信任存取)。

3. 在確認對話方塊中，啟用顯示啟用受信任存取選項，在方塊中輸入 **enable**，然後選擇啟用受信任的存取。
4. 如果您只是 AWS Organizations 的系統管理員，請告訴 AWS Well-Architected Tool 的管理員，他們現在可使用其主控台啟用該服務，以便與 AWS Organizations 搭配使用。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以啟用受信任的服務存取：

- AWS CLI: enable-aws-service-access

  您可以執行下列命令來啟用 AWS Well-Architected Tool 作為 Organizations 受信任的服務。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal wellarchitected.amazonaws.com
  ```

  此命令成功後就不會產生輸出。
- AWS API: EnableAWSServiceAccess

使用 AWS WA Tool 停用受信任的存取

如需啟用受信任的存取所需許可的資訊，請參閱停用信任的存取所需的許可。

您可以使用 AWS Well-Architected Tool 或 AWS Organizations 工具停用受信任存取。

> **Important**
>
> 強烈建議您盡可能使用 AWS Well-Architected Tool 主控台或工具來停用與 Organizations 整合。這可讓 AWS Well-Architected Tool 執行其所需的任何清除，例如刪除服務不再需要的資源或存取角色。只有在您無法使用 AWS Well-Architected Tool 提供的工具停用整合成時，才能繼續執行這些步驟。
> 如果您使用 AWS Well-Architected Tool 主控台或工具停用受信任的存取，則不需要完成這些步驟。

使用 AWS WA Tool 主控台來停用受信任存取

請參閱《AWS Well-Architected Tool 使用者指南》中的共用 AWS Well-Architected Tool 資源。

您可以執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDK 中的 Organizations API 操作，來停用受信任存取。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以停用信任的服務存取：

- AWS CLI: disable-aws-service-access

  您可以執行下列命令來停用 AWS Well-Architected Tool 作為 Organizations 受信任的服務。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal wellarchitected.amazonaws.com
  ```

  此命令成功後就不會產生輸出。
- AWS API：DisableAWSServiceAccess

Amazon VPC IP 地址管理員 (IPAM) 和 AWS Organizations

Amazon VPC IP 地址管理員 (IPAM) 是一項 VPC 功能，可讓您更輕鬆地規劃、追蹤和監控您 AWS 工作負載的 IP 地址。

使用 AWS Organizations 讓您能監控整個組織的 IP 地址使用情況，並在成員帳戶之間共用 IP 地址集區。

如需詳細資訊，請參閱 Amazon VPC IPAM 使用者指南中的整合 IPAM 與 AWS Organizations。

使用以下資訊可協助您整合 Amazon VPC IP 地址管理員 (IPAM) 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

使用 IPAM 主控台或使用 IPAM 的 `EnableIpamOrganizationAdminAccount` API 將 IPAM 與 AWS Organizations 整合時，會在組織的管理帳戶和每個成員帳戶中自動建立下列服務連結角色。

- `AWSServiceRoleForIPAM`

如需詳細資訊，請參閱 Amazon VPC 使用者指南中的IPAM 的服務連結角色。

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。IPAM 使用的服務連結角色會授予存取權給下列服務委託人：

- `ipam.amazonaws.com`

使用 IPAM 啟用受信任存取

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

> **Note**
>
> 當您指定 IPAM 的委派管理員時，其會自動啟用組織中 IPAM 的受信任存取。
> IPAM 需要對 AWS Organizations 的受信任存取，才能為組織指定成員帳戶作為此服務的委派管理員。

您只能使用 Amazon VPC IP 地址管理員 (IPAM) 工具啟用受信任存取。

如果您使用 IPAM 主控台或使用 IPAM `EnableIpamOrganizationAdminAccount` API 將 IPAM 與 AWS Organizations 整合時，會自動將受信任存取授予 IPAM。授予受信任存取會在管理帳戶中和組織內所有成員帳戶中建立服務連結角色 `AWSServiceRoleForIPAM`。IPAM 使用服務連結角色來監控與組織中 EC2 聯網資源相關聯的 CIDR，並將與 IPAM 相關的指標存放在 Amazon CloudWatch 中。如需詳細資訊，請參閱 Amazon VPC IPAM 使用者指南中的IPAM 的服務連結角色。

如需啟用受信任存取的相關說明，請參閱 Amazon VPC IPAM 使用者指南中的整合 IPAM 與 AWS Organizations。

> **Note**
>
> 您無法利用 AWS Organizations 主控台或使用 `EnableAWSServiceAccess` API，透過 IPAM 啟用受信任存取。

使用 IPAM 停用受信任存取

如需啟用受信任的存取所需許可的資訊，請參閱停用信任的存取所需的許可。

只有在 AWS Organizations 管理帳戶中的管理員才能利用 AWS Organizations `disable-aws-service-access` API，使用 IPAM 停用受信任存取。

如需停用 IPAM 帳戶許可和刪除服務連結角色的詳細資訊，請參閱 Amazon VPC 使用者指南中的IPAM 的服務連結角色。

您可以執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDK 中的 Organizations API 操作，來停用受信任存取。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以停用信任的服務存取：

- AWS CLI: disable-aws-service-access

  您可以執行下列命令來停用 Amazon VPC IP 地址管理員 (IPAM) 作為 Organizations 的受信任服務。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal ipam.amazonaws.com
  ```

  此命令成功後就不會產生輸出。

- AWS API：DisableAWSServiceAccess

啟用 IPAM 的委派管理員帳戶

IPAM 的委派管理員帳戶負責建立 IPAM 和 IP 地址集區、管理和監控組織中 IP 地址的使用情況，並進行跨成員帳戶的 IP地位址集區共用。如需詳細資訊，請參閱 Amazon VPC IPAM 使用者指南中的整合 IPAM 與 AWS Organizations。

只有組織管理帳戶中的管理員可以設定 IPAM 的委派管理員。

您可以從 IPAM 主控台或使用 `enable-ipam-organization-admin-account` API 指定委派的管理員帳戶。如需詳細資訊，請參閱《AWS AWS CLI 命令參考》中的enable-ipam-organization-admin-account。

最低許可

只有 Organizations 管理帳戶中的使用者或角色，才能將成員帳戶設定為組織中 IPAM 的委託管理員。

若要使用 IPAM 主控台設定委派管理員，請參閱《Amazon VPC IPAM 使用者指南》中的整合 IPAM 與 AWS Organizations。

停用 IPAM 的委派管理員

只有組織管理帳戶中的管理員可以設定 IPAM 的委派管理員。

若要使用 AWS AWS CLI 移除委派管理員，請參閱《AWS AWS CLI 命令參考》中的disable-ipam-organization-admin-account。

若要使用 IPAM 主控台停用委派管理員 IPAM 帳戶，請參閱《Amazon VPC IPAM 使用者指南》中的整合 IPAM 與 AWS Organizations。

Amazon VPC Reachability Analyzer 和 AWS Organizations

Reachability Analyzer 是一種組態分析工具，可讓您在虛擬私有雲端 (VPC) 中的來源資源和目的地資源之間執行連線測試。

將 AWS Organizations 與 Reachability Analyzer 結合使用可讓您追蹤組織中跨帳戶的路徑。

如需詳細資訊，請參閱 Reachability Analyzer user guide (《Reachability Analyzer 使用者指南》) 中的 Cross-account analyses for Reachability Analyzer (Reachability Analyzer 的跨帳戶分析)。

使用以下資訊可協助整合 Reachability Analyzer 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下服務連結角色。該角色允許 Reachability Analyzer 在您組織的組織帳戶中執行支援的操作。

只有在您停用 Reachability Analyzer 和 Organizations 之間的受信任存取，或者從組織中移除成員帳戶時，才能刪除或修改此角色。

- `AWSServiceRoleForReachabilityAnalyzer`

如需詳細資訊，請參閱 Reachability Analyzer user guide (《Reachability Analyzer 使用者指南》) 中的 Cross-account analyses for Reachability Analyzer (Reachability Analyzer 的跨帳戶分析)。

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。Reachability Analyzer 使用的服務連結角色會將存取權授予下列服務主體：

- `reachabilityanalyzer.networkinsights.amazonaws.com`

啟用 Reachability Analyzer 的受信任存取

如需啟用受信任存取所需許可的資訊，請參閱啟用信任的存取所需的許可。

當您指定 Reachability Analyzer 的委派管理員時，會自動啟用組織中 Reachability Analyzer 的受信任存取。

Reachability Analyzer 需要對 AWS Organizations 的受信任存取，才能為組織指定成員帳戶作為此服務的委派管理員。

> **Important**
>
> - 您可以使用 Reachability Analyzer 主控台或 Organizations 主控台來啟用受信任存取。但是，我們強烈建議您使用 Reachability Analyzer 主控台或 `EnableMultiAccountAnalysisForAwsOrganization` API 來啟用與 Organizations 的整合。這可讓 Reachability Analyzer 執行其需要的任何組態，例如建立服務所需的資源。
> - 授予受信任存取會在管理帳戶中和組織內所有成員帳戶中建立服務連結角色 `AWSServiceRoleForReachabilityAnalyzer`。Reachability Analyzer 使用服務連結角色來允許管理，委派管理員則可以在組織中的任何資源之間執行連線分析。Reachability Analyzer 可拍攝組織中帳戶的網路元素快照，以回答連線查詢。
> - 如需詳細資訊，以及有關透過 Reachability Analyzer 啟用受信任存取的指示，請參閱 Reachability Analyzer user guide (《Reachability Analyzer 使用者指南》)中的 Cross-account analyses for Reachability Analyzer (Reachability Analyzer 的跨帳戶分析)。

您可以使用 AWS Organizations 主控台，執行 AWS CLI 命令，或呼叫其中一個 AWS SDK 中的 API 操作，來啟用受信任存取。

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在服務頁面上，尋找 VPC Reachability Analyzer 列，選擇服務的名稱，然後選擇啟用受信任存取。
3. 在確認對話方塊中，啟用顯示啟用受信任存取選項，在方塊中輸入 **enable**，然後選擇啟用受信任的存取。
4. 如果您只是 AWS Organizations 的管理員，請告訴 Reachability Analyzer 的管理員，他們現在可使用其主控台啟用該服務，以便搭配使用 AWS Organizations。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

您可以使用以下 AWS CLI 命令或 API 操作，以啟用受信任的服務存取：

- AWS CLI: enable-aws-service-access

  您可以執行下列命令來啟用 Reachability Analyzer，作為受信任服務搭配使用 Organizations。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal reachabilityanalyzer.networkinsights.amazonaws.com
  ```

  此命令成功後就不會產生輸出。

- AWS API: EnableAWSServiceAccess

停用 Reachability Analyzer 的受信任存取

如需啟用受信任的存取所需許可的資訊，請參閱停用信任的存取所需的許可。

您可以使用 Reachability Analyzer 主控台 (建議) 或 Organizations 主控台來停用受信任存取。若要使用 Reachability Analyzer 主控台停用受信任存取，請參閱 Reachability Analyzer user guide (《Reachability Analyzer 使用者指南》) 中的 Cross-account analyses for Reachability Analyzer (Reachability Analyzer 的跨帳戶分析)。

啟用 Reachability Analyzer 的委派管理員帳戶

委派管理員帳戶可以在組織中跨任何資源執行連線分析。如需詳細資訊，請參閱《Reachability Analyzer 使用者指南》中的整合 Reachability Analyzer 與 AWS Organizations。

只有組織管理帳戶中的管理員可以設定 Reachability Analyzer 的委派管理員。

您可以從 Reachability Analyzer 主控台或使用 `RegisterDelegatedAdministrator` API 指定委派管理員帳戶。如需詳細資訊，請參閱 Organizations Command Reference (Organizations 命令參考) 中的 RegisterDelegatedAdministrator。

> **最低許可**
>
> 只有 Organizations 管理帳戶中的使用者或角色，才能將成員帳戶設定為組織中 Reachability Analyze 的委派管理員

若要使用 Reachability Analyzer 主控台設定委派管理員，請參閱《Reachability Analyzer 使用者指南》中的整合 Reachability Analyzer 與 AWS Organizations。

停用 Reachability Analyzer 的委派管理員

只有組織管理帳戶中的管理員可以設定 Reachability Analyzer 的委派管理員。

您可以使用 Reachability Analyzer 主控台或 API，或透過使用 Organizations `DeregisterDelegatedAdministrator` CLI 或 SDK 操作，移除委派管理員。

若要使用 Reachability Analyzer 主控台停用委派的管理員 Reachability Analyzer 帳戶，請參閱 Reachability Analyzer user guide (《Reachability Analyzer 使用者指南》)中的 Cross-account analyses for Reachability Analyzer (Reachability Analyzer 的跨帳戶分析)。

與 Organizations 合作之 AWS 服務的委派管理員

我們建議您僅將 AWS Organizations 管理帳戶及其使用者和角色用於必須由該帳戶執行的任務。我們也建議您將 AWS 資源存放在組織內其他成員帳戶中，且將其保存在管理帳戶之外。這是因為安全性功能 (例如 Organizations 服務控制政策 (SCP)) 不會限制管理帳戶中的使用者或角色。將資源與管理帳戶分開，也可協助您瞭解發票上的費用。

許多與 Organizations 整合的 AWS 服務可讓您減少管理帳戶的用量。這些服務可讓您將一或多個成員帳戶註冊為管理員，以管理服務中使用的所有組織帳戶。這些帳戶稱為該特定服務的委派管理員。

透過將成員帳戶註冊為 AWS 服務的委派管理員，您可以讓該帳戶擁有該服務的某些管理權限，以及 Organizations 唯讀動作的權限。

在您將帳戶註冊為服務的委派管理員之前：

- 確認該服務支援委派管理員。請參閱 AWS 您可以搭配使用的服務 AWS Organizations 的表格，瞭解哪些服務支援委派管理員。
- 為該服務啟用受信任存取。

> **Note**
>
> 若要瞭解如何為委派管理員啟用服務，請參閱 AWS 您可以搭配使用的服務 AWS Organizations 中的表格，並在該服務的支援委派管理員直欄中，選取瞭解更多連結。

授與委派管理員帳戶的權限

每個服務特定的委派管理員帳戶都有該服務授與的權限。若要瞭解更多，請參閱 AWS 您可以搭配使用的服務 AWS Organizations 中的表格，並在該服務的支援委派管理員直欄中，選取瞭解更多連結。

委派管理員帳戶也具有下列唯讀權限：

- `DescribeAccount`
- `DescribeCreateAccountStatus`
- `DescribeEffectivePolicy`
- `DescribeHandshake`
- `DescribeOrganization`
- `DescribeOrganizationalUnit`
- `DescribePolicy`
- `DescribeResourcePolicy`
- `ListAccounts`
- `ListAccountsForParent`
- `ListAWSServiceAccessForOrganization`
- `ListChildren`
- `ListCreateAccountStatus`

- ListDelegatedAdministrators
- ListDelegatedServicesForAccount
- ListHandshakesForAccount
- ListHandshakesForOrganization
- ListOrganizationalUnitsForParent
- ListParents
- ListPolicies
- ListPoliciesForTarget
- ListRoots
- ListTagsForResource
- ListTargetsForPolicy

這些權限可讓您檢視 (但不能變更) 這些主控台項目：

- 組織結構、所有帳戶與 OU，以及組織政策
- 成員資格
- 所有帳戶和 OU。
- 組織政策

中的安全性 AWS Organizations

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，該架構專為滿足對安全性最敏感的組織的需求而打造。

安全是 AWS 與您之間共同承擔的責任。共同責任模型 將此描述為雲端的安全和雲端內的安全：

- 雲端的安全性 — AWS 負責保護在 AWS 雲端中執行 AWS 服務的基礎架構。 AWS 還為您提供可以安全使用的服務。在 AWS 合規計畫中，第三方稽核員會定期測試並驗證我們的安全功效。若要深入瞭解適用於的規範遵循計劃 AWS Organizations，請參閱合規方案的AWS 服務範圍。
- 雲端中的安全性 — 您的責任取決於您使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件有助於您了解如何在使用 Organizations 時套用共同責任模型。下列主題將示範如何設定 Organizations 以達到您的安全和合規目標。您也會學到如何使用其他可 AWS 協助您監控和保護 Organizations 資源的服務。

主題

- AWS PrivateLink 對於 AWS Organizations
- AWS Identity and Access Management 與 AWS Organizations
- AWS Organizations 中的記錄和監控
- AWS Organizations 的合規驗證
- 中的恢復能力AWS Organizations
- AWS Organizations 中的基礎設施安全

AWS PrivateLink 對於 AWS Organizations

使 AWS PrivateLink 用 of AWS Organizations，您可以從 Virtual Private Cloud (VPC)（VPC）中訪問 AWS Organizations 服務，而無需跨越公共互聯網。

Amazon VPC 可讓您在自訂虛擬網路中啟動 AWS 資源。您可利用 VPC 來控制您的網路設定，例如 IP 地址範圍、子網路、路由表和網路閘道。如需有關 Amazon VPC 的詳細資訊，請參閱《Amazon VPC 使用者指南》。

若要將 Amazon VPC 連線到 AWS Organizations，您必須先定義一個介面 VPC 人雲端端點 (介面端點)。介面端點由一個或多個彈性網路介面 (ENI) 來表示，這些是在 VPC 的子網路中指派的私有 IP 地址。從您的 VPC 到 AWS Organizations 透過介面端點的請求會保留在 Amazon 網路上。

有關界面端點的一般資訊，請參閱 Amazon VPC 使用者指南中的使用界面 VPC 端點存取 AWS 服務。

主題

- 的 AWS PrivateLink 限制和限制 AWS Organizations
- 建立一個 VPC 端點
- 為 AWS Organizations建立 VPC 端點政策

的 AWS PrivateLink 限制和限制 AWS Organizations

適用 AWS PrivateLink 於 AWS Organizations的 VPC 限制。如需詳細資訊，請參閱 Amazon VPC 使用者指南中的使用界面 VPC 端點存取 AWS 服務和AWS PrivateLink 配額。此外，適用下列限制：

- 僅在該us-east-1地區提供
- 不支援傳輸層安全性 (TLS) 1.1

建立一個 VPC 端點

您可以使用 Amazon VPC 主控台 AWS Command Line Interface (AWS CLI) 或在 VPC 中建立 AWS Organizations 端點。 AWS CloudFormation

如需使用 Amazon VPC 主控台建立和設定端點的相關資訊 AWS CLI，請參閱 Amazon VPC 使用者指南中的建立 VPC 端點。如需使用建立和設定端點的相關資訊 AWS CloudFormation，請參閱使用者指南中的 AWS:: EC2:: vpcendPoint 資源。AWS CloudFormation

建立 AWS Organizations 端點時，請使用下列項目做為服務名稱：

```
com.amazonaws.us-east-1.organizations
```

如果您在存取時需要經過 FIPS 140-2 驗證的加密模組 AWS，請使用下列 AWS Organizations FIPS 服務名稱：

```
com.amazonaws.us-east-1.organizations-fips
```

為 AWS Organizations建立 VPC 端點政策

您可以將端點策略附加到控制對 Organizations 的存取權的 VPC 端點。此政策會指定下列資訊：

- 可執行動作的主體。
- 可執行的動作。
- 可供執行動作的資源。

如需詳細資訊，請參閱 Amazon VPC 使用者指南中的使用端點政策控制對 VPC 端點的存取。

範例： AWS Organizations 動作的 VPC 端點政策

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "Organizations:DescribeAccount"
         ],
         "Resource":"*"
      }
   ]
}
```

AWS Identity and Access Management 與 AWS Organizations

存取 AWS Organizations 需要憑證。這些憑證必須有存取 AWS 資源的許可，例如 Amazon Simple Storage Service (Amazon S3) 儲存貯體、Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或 AWS Organizations 組織單位 (OU)。下列各節會提供如何使用 AWS Identity and Access Management (IAM) 的詳細資訊，以協助您安全存取組織，並控制可以管理這些組織的對象。

為了決定誰可管理您的組織的哪些部分，AWS Organizations 會使用與其他 AWS 服務相同的以 IAM 為基礎的模型。身為組織的管理帳戶中的管理員，您可以授予以 IAM 為基礎的許可，以透過將政策附加到管理帳戶中的使用者、群組和角色來執行 AWS Organizations 任務。這些政策會指定這些委託人可執行的動作。您可以將 IAM 許可政策附加到使用者為其成員的群組，或直接附加至使用者或角色。作為最佳實務，我們建議您將政策附加到群組，而非使用者。您也可以選擇將完整的管理員許可授予其他人。

對於 AWS Organizations 的大多數管理員操作，您需要將許可連接至管理帳戶中的使用者或群組。如果成員帳戶中的使用者需要為組織執行管理員操作，您需要將 AWS Organizations 許可授予管理帳戶中的 IAM 角色，並讓成員帳戶中的使用者擔任該角色。關於 IAM 許可政策的一般資訊，請參閱 IAM 使用者指南中的 IAM 政策概觀。

主題

身分驗證

您可以使用下列身分類型來存取 AWS：

- AWS 帳戶 根使用者 – 在註冊 AWS 時，您會提供與 AWS 帳戶 關聯的電子郵件地址和密碼。這些是您的根憑證，可完整存取您的所有 AWS 資源。

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

- IAM 使用者 – IAM 使用者是您 AWS 帳戶 中的一種身分，擁有特定的自訂許可 (例如，在 Amazon Elastic File System 中建立檔案系統的許可)。您可以使用 IAM 使用者名稱和密碼登入安全 AWS 網頁，例如，AWS Management Console、AWS 開發論壇或AWS支援中心。

  除了使用者名稱和密碼之外，您可以為每位使用者產生存取金鑰。以程式設計的方式存取 AWS 服務時，您可以使用這些金鑰，方法是透過幾個 SDK 中的其中一個或使用 AWS Command Line Interface (AWS CLI)。此軟體開發套件和 AWS CLI 工具使用存取金鑰，以加密方式簽署您的請求。如果您不使用 AWS 工具，便必須自行簽署請求。AWS Organizations 支援簽章版本 4，此通訊協定可用來驗證送入的 API 請求。如需驗證請求的詳細資訊，請參閱 IAM 使用者指南中的簽署 AWS API 請求。

- IAM 角色 – IAM 角色是您可以在帳戶中建立的另一種 IAM 身分，具有特定的許可。這類似 IAM 使用者，但未與特定的人員相關聯。IAM 角色允許您取得臨時存取金鑰，可存取 AWS 服務和資源。使用臨時憑證的 IAM 角色在下列情況中非常有用：
  - 聯合身分使用者存取 – 您可以使用 AWS Directory Service、您的企業使用者目錄或 web 身分提供者中預先存在的使用者身分，而不建立 IAM 使用者。這些稱為聯合身分使用者。透過身分提供者身分提供者來請求存取時，AWS 會指派角色給聯合身分使用者。如需聯合身分使用者的詳細資訊，請參閱 IAM 使用者指南中的聯合身分使用者和角色。
  - 跨帳戶存取 - 您可以使用帳戶中的 IAM 角色，來授與許可給另一個 AWS 帳戶 帳戶，以存取您帳戶的資源。如需範例，請參閱 IAM 使用者指南中的教學課程：AWS 帳戶使用 IAM 角色委派存取權。
  - AWS 服務存取 – 您可以使用帳戶中的 IAM 角色，授予 AWS 服務許可來存取您帳戶中的資源。例如，您可以建立角色，以允許 Amazon Redshift 代表您存取 Amazon S3 儲存貯體，然後將存放於該儲存貯體中的資料載入到 Amazon Redshift 叢集。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以委派許可給 AWS 服務。
  - Amazon EC2 上執行的應用程式 – 對於在 EC2 執行個體上執行且發出 AWS API 請求的應用程式，您可以使用 IAM 角色來管理臨時憑證，而不需將存取金鑰存放於執行個體中供這些應用程式使用。若要指派 AWS 角色給 EC2 執行個體，並提供給執行個體所有的應用程式使用，您可以建立連結到執行個體的執行個體描述檔。執行個體描述檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得臨時憑證。如需詳細資訊，請參閱IAM 使用者指南中的利用 IAM 角色來授予許可給 Amazon EC2 執行個體上執行的應用程式。

存取控制

您可以透過有效憑證來對請求進行身分驗證，但除非您擁有許可，否則您無法管理或存取 AWS Organizations 資源。例如，您必須擁有許可來建立 OU 或將服務控制政策 (SCP) 連接至帳戶。

以下章節說明如何管理 AWS Organizations 的許可。

- 管理您的 AWS 組織的存取許可
- 針對 AWS Organizations 使用以身分為基礎的政策 (IAM 政策)
- 包含標籤和 AWS Organizations 的以屬性為基礎的存取控制

管理您的 AWS 組織的存取許可

組織中的所有 AWS 資源，包括根、OU、帳戶和政策，是由 AWS 帳戶 管理，而建立或存取資源的許可，則是由許可政策所控管。如果是組織，其管理帳戶擁有所有資源。身為帳戶管理員，您可以透過連接許可政策到 IAM 身分 (使用者、群組和角色) 來控制對於 AWS 資源的存取。

> **Note**
>
> 帳戶管理員 (或管理員使用者) 是具有管理員許可的使用者。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 中的安全性最佳實務。

當您授予許可時，能夠決定取得許可的對象、這些對象取得的資源許可，以及可對上述資源進行的特定動作。

根據預設，IAM 使用者、群組和角色沒有許可。身為組織的管理帳戶中的管理員，您可以對管理帳戶中的其他 IAM 使用者或角色執行管理任務或委派管理員許可。若要委派許可，您必須將 IAM 許可政策附加到 IAM 使用者、群組或角色。根據預設，使用者不具任何許可；這種情況有時稱為隱含拒絕。政策會將隱含拒絕覆寫為明確允許，其指定使用者可以執行的動作，以及可以對其執行動作的資源。如果將許可授予角色，則組織中其他帳戶的使用者可以擔任該角色。

AWS Organizations 資源和操作

本節旨在討論將 AWS Organizations 概念對應至 IAM 同等概念的方式。

資源

在 AWS Organizations 中，您可以控制對下列資源的存取：

- 組成組織階層結構的根和 OU
- 屬於組織成員的帳戶
- 您連接到組織中實體的政策
- 您用來變更組織狀態的交握

這些資源中每一項都擁有一個相關聯的唯一 Amazon Resource Name (ARN)。您會在 IAM 許可政策的 `Resource` 元素中指定 ARN，藉此控制對資源的存取。如需中使用之資源之 ARN 格式的完整清單 AWS Organizations，請參閱服務授權參考AWS Organizations中所定義的資源類型。

操作

AWS 提供一組操作以搭配使用組織中的資源。它們可讓您執行建立、列出、修改、存取資源的內容、刪除資源等動作。大多數操作都在 IAM 政策的 Action 元素中參考，以控制能使用該操作的對象。如需可用AWS Organizations作 IAM 政策中許可的作業清單，請參閱服務授權參考中的 Organ AWS izations 定義的動作。

當您在單一許可政策 Statement 中結合 Resource 和 Action 時，您可以控制可使用該特定動作所在的資源。

條件索引鍵

AWS 提供可供您查詢的條件金鑰，以對特定動作提供更精確的控制。您可以在 IAM 政策的 Condition 元素中參考這些條件金鑰，以指定必須符合陳述式才能被視為相符的額外情況。

以下條件金鑰對於 AWS Organizations 特別有用：

- aws:PrincipalOrgID – 簡化在以資源為基礎的政策中指定 Principal 元素。此全球金鑰提供了列出組織中所有 AWS 帳戶 的所有帳戶 ID 的替代方法。您可以在 Condition 元素中指定組織 ID，而不是列出組織成員的所有帳戶。

  > **Note**
  >
  > 此全域條件也適用於組織的管理帳戶。

  如需詳細資訊，請參閱《IAM 使用者指南》中的PrincipalOrgIDAWS全域條件內容金鑰說明。
- aws:PrincipalOrgPaths – 使用此條件金鑰來比對特定組織根、OU 或其子系的成員。當提出請求的委託人 (根使用者、IAM 使用者或角色) 位於指定的組織路徑時，aws:PrincipalOrgPaths 條件金鑰會傳回 true。路徑是 AWS Organizations 實體結構的文字表示。如需有關路徑的詳細資訊，請參閱《IAM 使用者指南》中的了解AWS Organizations實體路徑。如需有關使用此條件金鑰的詳細資訊，請參閱 IAM 使用者指南PrincipalOrgPaths中的 aws:。

  例如，下列條件元素符合相同組織中兩個 OU 之中任一個的成員。

```
        "Condition": {
            "ForAnyValue:StringLike": {
                "aws:PrincipalOrgPaths": [
                    "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/",
                    "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-jkl0-awsddddd/"
```

```
                    ]
                }
            }
```

- `organizations:PolicyType` – 您可以使用此條件金鑰，將 Organizations 政策相關 API 操作限制為僅在指定類型的 Organizations 政策上運作。您可以將此條件金鑰套用至任何政策陳述式，其中包含與 Organizations 政策互動的動作。

  您可以搭配此條件金鑰使用下列值：

  - `AISERVICES_OPT_OUT_POLICY`
  - `BACKUP_POLICY`
  - `SERVICE_CONTROL_POLICY`
  - `TAG_POLICY`

  例如，下列範例政策允許使用者執行任何 Organizations 操作。不過，如果使用者執行一個採取政策引數的操作，則只有在指定的政策是標記政策時，才允許此操作。如果使用者指定任何其他類型的政策，則此操作會失敗。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "IfTaggingAPIThenAllowOnOnlyTaggingPolicies",
            "Effect": "Allow",
            "Action": "organizations:*",
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:PolicyType": [ "TAG_POLICY" ]
                }
            }
        }
    ]
}
```

- `organizations:ServicePrincipal`— 如果您使用 [啟用] 或 [停用] AWSServiceAccess 作業來啟用AWSServiceAccess或停用對其他AWS服務的受信任存取，則可作為條件使用。您可以使用 `organizations:ServicePrincipal` 來限制這些操作對核准的服務委託人名稱清單所做的請求。

例如，對 AWS Organizations 啟用和停用信任存取時，以下政策只允許使用者指定 AWS Firewall Manager。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowOnlyAWSFirewallIntegration",
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:ServicePrincipal": [ "fms.amazonaws.com" ]
                }
            }
        }
    ]
}
```

如需可在 IAM 政策中用作許可的所有 AWS Organizations —specific 條件金鑰清單，請參閱服務授權參考AWS Organizations中的條件金鑰。

了解資源所有權

AWS 帳戶 擁有在帳戶內所建立的資源，無論資源的建立者是誰。具體而言，資源擁有者就是對資源建立請求進行身分驗證的主體實體 (即根使用者、IAM 使用者或 IAM 角色) 的 AWS 帳戶。對於 AWS 組織，一律會是管理帳戶。您無法呼叫從成員帳戶建立或存取組織資源的大多數操作。下列範例說明其如何運作：

- 如果您使用管理帳戶的根憑證來建立 OU，則您的管理帳戶即為資源的擁有者。(在 AWS Organizations 中，資源為 OU。)
- 如果您在管理帳戶中建立 IAM 使用者，並將建立 OU 的許可授予該使用者，則該使用者可以建立 OU。不過，使用者所屬的管理帳戶會擁有資源。
- 如果您在管理帳戶中建立 IAM 角色，並將建立 OU 的許可授予該角色，則任何可擔任該角色的人都能建立 OU。角色所屬的管理帳戶 (非擔任使用者) 會擁有該 OU 資源。

管理資源存取

許可政策描述誰可以存取哪些資源。下一節說明可用來建立許可政策的選項。

> **Note**
>
> 本節著重討論如何在 AWS Organizations 的環境中使用 IAM，它不提供 IAM 服務的詳細資訊。如需完整的 IAM 文件，請參閱 IAM 使用者指南。如需 IAM 政策語法和說明的相關資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策參考資料。

附加至 IAM 身分的政策稱為以身分為基礎的政策 (IAM 政策)。連接至資源的政策稱為以資源為基礎的政策。AWS Organizations 僅支援以身分為基礎的政策 (IAM 政策)。

主題

- 身分型許可政策 (IAM 政策)
- 資源型政策

身分型許可政策 (IAM 政策)

您可以將策略連接至 IAM 身分，以允許這些身分對 AWS 資源執行操作。例如，您可以執行下列動作：

- 將許可政策連接至您帳戶中的使用者或群組 – 若要授予使用者建立 AWS Organizations 資源的許可，例如服務控制政策 (SCP) 或 OU ，您可以將許可政策連接至使用者或使用者所屬的群組。使用者或群組必須位在組織的管理帳戶中。
- 將許可政策連接至角色 (授予跨帳戶許可) – 您可以將以身分為基礎的許可政策連接至 IAM 角色，藉此對組織授予跨帳戶許可。例如，管理帳戶中的管理員可以建立角色，將跨帳戶許可授予成員帳戶中的使用者，如下所示：
  1. 管理帳戶管理員會建立 IAM 角色，並將會授予許可給組織資源的許可政策連接至該角色。
  2. 管理帳戶管理員將信任政策連接至角色，該角色會將成員帳戶 ID 識別為可以擔任角色的 `Principal`。
  3. 然後成員帳戶管理員可以委派許可給成員帳戶中的任何使用者，以擔任該角色。這樣做可讓成員帳戶中的使用者可以在管理帳戶和組織中建立或存取資源。如果您想要將許可授予 AWS 服務來擔任該角色，則信任政策的委託人也可以是 AWS 服務委託人。

  如需使用 IAM 來委派許可的詳細資訊，請參閱 IAM 使用者指南中的存取管理。

以下為允許使用者在您的組織中執行 CreateAccount 動作的範例政策。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"Stmt1OrgPermissions",
         "Effect":"Allow",
         "Action":[
            "organizations:CreateAccount"
         ],
         "Resource":"*"
      }
   ]
}
```

您也可在政策的 Resource 元素中提供部分 ARN，用於指示資源的類型。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"AllowCreatingAccountsOnResource",
         "Effect":"Allow",
         "Action":"organizations:CreateAccount",
         "Resource":"arn:aws:organizations::*:account/*"
      }
   ]
}
```

您也可以拒絕建立未將特定標籤納入正在建立的帳戶中的帳戶。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"DenyCreatingAccountsOnResourceBasedOnTag",
         "Effect":"Deny",
         "Action":"organizations:CreateAccount",
         "Resource":"*",
         "Condition":{
            "StringEquals":{
```

```
                "aws:ResourceTag/key":"value"
            }
         }
      }
   ]
}
```

如需有關使用者、群組、角色和許可的詳細資訊，請參閱 IAM 使用者指南中的 IAM 身分（使用者、使用者群組和角色）。

資源型政策

某些服務 (例如 Amazon S3) 支援以資源為基礎的許可政策。例如，您可以將政策連接到 Amazon S3 儲存貯體，以管理對該儲存貯體的存取許可。AWS Organizations 目前不支援以資源為基礎的政策。

指定政策元素：Actions、Conditions、Effects 和 Resources

對於每個 AWS Organizations 資源，服務會定義一組 API 操作或動作，可用來以某種方式與資源互動。為授予對這些操作的許可，AWS Organizations 定義了一組您可以在政策中指定的動作。例如，針對 OU 資源，AWS Organizations 會定義如下的動作：

- `AttachPolicy` 和 `DetachPolicy`
- `CreateOrganizationalUnit` 和 `DeleteOrganizationalUnit`
- `ListOrganizationalUnits` 和 `DescribeOrganizationalUnit`

在某些情況下，執行 API 操作可能需要多個動作的許可，並且可能需要多個資源的許可。

以下是您可以在 IAM 許可政策中使用的最基本元素：

- 動作 – 使用此關鍵字，可辨識要允許或拒絕的操作 (動作)。例如，`organizations:CreateAccount` 會根據指定的 `Effect`，進而允許或拒絕使用者執行 AWS Organizations `CreateAccount` 操作的許可。如需詳細資訊，請參閱 IAM JSON 政策元素：IAM 使用者指南中的動作。
- 資源 – 使用此關鍵字指定政策陳述式套用的資源的 ARN。如需詳細資訊，請參閱 IAM JSON 政策元素：IAM 使用者指南中的資源。
- 條件 – 使用此關鍵字，可指定必須達到才能套用政策陳述式的條件。`Condition` 通常會指定必須成立政策才會符合的額外情況。如需更多資訊，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素：條件。

- 效果 – 使用此關鍵字，可指定政策陳述式應允許或拒絕對資源執行動作。如果您未明確授予存取 (或允許) 資源，則隱含地拒絕存取。您也可以明確拒絕存取資源，您可能會這樣做，以確保使用者無法對特定資源執行特定動作，即使另有其他政策授予存取。如需詳細資訊，請參閱 IAM JSON 政策元素：IAM 使用者指南中的效果。
- 委託人 – 在以身分為基礎的政策 (IAM 政策) 中，政策附加到的使用者會自動且隱含成為委託人。對於以資源為基礎的政策，您可以指定想要收到許可的使用者、帳戶、服務或其他實體 (僅適用於以資源為基礎的政策)。AWS Organizations 目前僅支援以身分為基礎的政策，不支援以資源為基礎的政策。

若要進一步了解 IAM 政策語法和說明，請參閱 IAM 使用者指南中的 IAM JSON 政策參考資料。

針對 AWS Organizations 使用以身分為基礎的政策 (IAM 政策)

作為組織管理帳戶的管理員，您可以將許可政策連接至組織內的 AWS Identity and Access Management (IAM) 身分 (使用者、群組和角色) 來控制對 AWS 資源的存取。當您授予許可時，能夠決定取得許可的對象、這些對象取得許可的資源，以及可對上述資源進行的特定動作。如果將許可授予角色，組織中其他帳戶的使用者可以擔任該角色。

根據預設，使用者沒有任何類型的許可。所有許可皆需透過政策明確提供給使用者。如果沒有明確授予許可，則會隱含拒絕此許可。如果許可明確遭到拒絕，則該結果凌駕於任何其他允許存取的政策。換言之，使用者僅可擁有明確授予的許可，且這些許可不會被明確拒絕。

除了本主題中描述的基本技術之外，您還可以使用套用至組織資源的標籤來控制組織的存取：組織根、組織單位 (OU)、帳戶和政策。如需詳細資訊，請參閱 包含標籤和 AWS Organizations 的以屬性為基礎的存取控制。

提供完整管理員許可給使用者

您可以建立 IAM 政策，以授權完整 AWS Organizations 管理員許可給組織中 IAM 使用者。您可以在 IAM 主控台中使用 JSON 政策編輯器來執行此操作。

若要使用 JSON 政策編輯器來建立政策

1. 登入 AWS Management Console，並開啟位於 https://console.aws.amazon.com/iam/ 的 IAM 主控台。
2. 在左側的導覽窗格中，選擇 Policies (政策)。

   如果這是您第一次選擇 Policies (政策)，將會顯示 Welcome to Managed Policies (歡迎使用受管政策) 頁面。選擇 Get Started (開始使用)。

3. 在頁面頂端，選擇 Create policy (建立政策)。
4. 在政策編輯器中，選擇 JSON 選項。
5. 輸入下列 JSON 政策文件：

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

6. 選擇下一步。

> **Note**
>
> 您可以隨時切換視覺化與 JSON 編輯器選項。不過，如果您進行變更或在視覺化編輯器中選擇下一步，IAM 就可能會調整您的政策結構，以便針對視覺化編輯器進行最佳化。如需詳細資訊，請參閱 IAM 使用者指南中的調整政策結構。

7. 在檢視與建立頁面上，為您正在建立的政策輸入政策名稱與描述 (選用)。檢視此政策中定義的許可，來查看您的政策所授予的許可。
8. 選擇 Create policy (建立政策) 儲存您的新政策。

若要進一步了解如何建立 IAM 政策，請參閱 IAM 使用者指南中的建立 IAM 政策。

透過動作授予有限的存取

如果您想要授予有限的許可而非完整的許可，您可以建立一個政策，列出在 IAM 許可政策的 `Action` 元素中所允許的個別許可。如下列範例所示，您可以使用萬用字元 (*) 字元來授予 `Describe*` 和 `List*` 許可，也就是提供存取您的密碼的唯讀存取權：

> **Note**
>
> 在服務控制政策 (SCP)，`Action` 元素中的萬用字元 (*) 字元只能單獨使用或用在字串結尾。它不能出現在字串開頭或中間。因此，在 SCP 中，`"servicename:action*"` 有效，但 `"servicename:*action"` 和 `"servicename:some*action"` 都無效。

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

如需 IAM 政策中可指派的所有權限清單，請參閱服務授權參考中的 Organ AWS izations 定義的動作。

授予對特定資源的存取

除了限制存取特定動作，您可以限制對阻止中特定實體的存取。在之前章節範例中的 Resource 元素皆指定萬用字元 (「*」)，這表示「該動作可存取的任何資源」。反之，您可以以允許存取的特定實體之 Amazon Resource Name (ARN) 來取代「*」。

範例：授予單一 OU 的存取許可

下列政策的第一個陳述式允許 IAM 使用者對整個組織的讀取存取，但第二個陳述式允許執行 AWS Organizations 管理動作的使用者只能在單一指定的組織單位 (OU) 中。這不會延伸至任何子項 OU。未授予帳單存取。請注意，這不會授予您對 OU 中 AWS 帳戶 的管理存取。它只授予在指定 OU 內帳戶上執行 AWS Organizations 操作的許可：

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

```
      "Resource": "arn:aws:organizations::<masterAccountId>:ou/o-<organizationId>/ou-
<organizationalUnitId>"
    }
  ]
}
```

您可以從 AWS Organizations 主控台或呼叫 `List*` API，取得 OU 和組織的 ID。您將此政策套用至其中的使用者或群組可以執行任何動作 (`"organizations:*"`)，這直接包含在指定 OU 中的任何實體上。OU 依據 Amazon Resource Name (ARN) 識別。

如需有關各種資源之 ARN 的詳細資訊，請參閱服務授權參考AWS Organizations中所定義的資源類型。

授予對有限服務委託人啟用受信任存取的能力

您可以使用政策陳述式 `Condition` 元素，以進一步限制政策聲明符合的情況。

範例：授予對一個指定服務啟用受信任存取的許可

下列陳述式顯示了如何限制只能對您指定的那些服務啟用受信任存取的能力。如果使用者嘗試使用不同於 AWS IAM Identity Center 的服務委託人來呼叫 API，則此政策不相符且請求會遭拒絕：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "organizations:EnableAWSServiceAccess",
            "Resource": "*",
            "Condition": {
                "StringEquals" : {
                    "organizations:ServicePrincipal" : "sso.amazonaws.com"
                }
            }
        }
    ]
}
```

如需有關各種資源之 ARN 的詳細資訊，請參閱服務授權參考AWS Organizations中所定義的資源類型。

包含標籤和 AWS Organizations 的以屬性為基礎的存取控制

以屬性為基礎的存取控制可讓您使用管理員受管屬性，例如連接至 AWS 資源和 AWS 身分的標籤，來控制對這些資源的存取。例如，您可以指定當使用者和資源對特定標籤具有相同的值時，使用者可以存取資源。

AWS Organizations 可標記資源包括 AWS 帳戶、組織的根、組織單位 (OU)，或者政策。當您將標籤連接至 Organizations 資源時，您可以使用這些標籤來控制誰可以存取這些資源。作法如下：將 `Condition` 元素新增至您的 AWS Identity and Access Management (IAM) 許可政策陳述式，可在允許執行動作之前檢查某些標籤鍵和值是否存在。這可讓您建立 IAM 政策，以有效地說明「允許使用者僅管理那些以鍵 X 和值 Y 來標記的 OU」或「允許使用者僅管理那些使用與使用者連接的 Z 標籤鍵具有相同值的鍵 Z 來標記的 OU。」

您可以根據 IAM 政策中不同類型的標籤參考來進行 `Condition` 測試。

- 檢查連接至請求中指定資源的標籤
- 檢查連接至提出請求之 IAM 使用者或角色的標籤
- 檢查請求中包含作為參數的標籤

如需有關在政策中使用標籤進行存取控制的詳細資訊，請參閱使用資源標籤來控制對 IAM 使用者和角色的存取。如需 IAM 許可政策的完整語法，請參閱 IAM JSON 政策參考

檢查連接至請求中指定資源的標籤

當您使用 AWS Management Console、AWS Command Line Interface (AWS CLI)，或其中一個 AWS 開發套件提出請求時，您可以指定要使用該請求存取的資源。無論您是嘗試列出指定類型的可用資源、讀取資源，或者寫入、修改或更新資源，都必須指定要存取的資源作為請求中的參數。這類請求由您連接至使用者和角色的 IAM 許可政策控制。在這些政策中，您可以比較連接至請求資源的標籤，並根據這些標籤的鍵和值選擇允許或拒絕存取。

若要檢查連接至資源的標籤，您可以使用以下字串前面的標籤鍵名稱參考 `Condition` 元素中的標籤：`aws:ResourceTag/`

例如，下列範例政策允許使用者或角色執行任何 AWS Organizations 操作，除非該資源具有包含鍵 `department` 和值 `security` 的標籤。如果該鍵和值存在，則政策會明確拒絕 `UntagResource` 操作。

```
{
```

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

        },
        {
            "Effect" : "Deny",
            "Action" : "organizations:UntagResource",
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "aws:ResourceTag/department" : "security"
                }
            }
        }
    ]
}
```

如需如何使用此元素的詳細資訊，請參閱 IAM 使用者指南中的控制對資源的存取和 aws:ResourceTag。

檢查連接至提出請求之 IAM 使用者或角色的標籤

您可以根據連接至該人員 IAM 使用者或角色的標籤，控制提出請求的人員 (委託人) 可執行的操作。若要執行此操作，請使用 `aws:PrincipalTag/`*`key-name`* 條件索引鍵來指定哪些標籤和值必須連接至呼叫的使用者或角色。

以下範例顯示如何僅在以下情況下允許動作：指定的標籤 (`cost-center`) 在呼叫操作的委託人和操作正在存取的資源上均具有相同的值。在此範例中，呼叫使用者只有在使用與使用者相同的 `cost-center` 值標記執行個體時，才會開始和停止 Amazon EC2 執行個體。

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "ec2:startInstances",
            "ec2:stopInstances"
        ],
```

```
        "Resource": "*",
        "Condition": {"StringEquals":
            {"ec2:ResourceTag/cost-center": "${aws:PrincipalTag/cost-center}"}}
    }
}
```

如需如何使用此元素的詳細資訊，請參閱 IAM 使用者指南中的控制對 IAM 委託人的存取和 aws:PrincipalTag。

檢查請求中包含作為參數的標籤

若干操作可讓您指定標籤作為請求的一部分。例如，當您建立資源時，可以指定連接至新資源的標籤。您可以指定 Condition 元素，其使用 aws:TagKeys 以根據請求中是否包含特定標籤鍵或一組鍵，來允許或拒絕操作。此比較運算子不關心標籤包含的值。它只檢查具有指定鍵的標籤是否存在。

若要檢查標籤鍵或標籤鍵清單，請指定具有以下語法的 Condition 元素：

```
"aws:TagKeys": [ "tag-key-1", "tag-key-2", ... , "tag-key-n" ]
```

您可以使用 ForAllValues: 以比較運算子為開頭，確保請求中的所有鍵都必須符合政策中指定的其中一個鍵。例如，下列範例政策僅在全部三個指定標籤鍵均存在於請求中時，才會允許任何 Organizations 操作。

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "organizations:*",
        "Resource": "*",
        "Condition": {
            "ForAllValues:StringEquals": {
                "aws:TagKeys": [
                    "department",
                    "costcenter",
                    "manager"
                ]
            }
        }
    }
}
```

或者，您可以使用 ForAnyValue: 以比較運算子為開頭，確保請求中的至少其中一個鍵必須符合政策中指定的其中一個鍵。例如，下列政策僅在至少一個指定標籤鍵均存在於請求中時，才會允許任何 Organizations 操作。

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "organizations:*",
        "Resource": "*",
        "Condition": {
            "ForAnyValue:StringEquals": {
                "aws:TagKeys": [
                    "stage",
                    "region",
                    "domain"
                ]
            }
        }
    }
}
```

若干操作可讓您在請求中指定標籤。例如，當您建立資源時，可以指定連接至新資源的標籤。您可以將政策中的標籤鍵/值對與請求隨附的鍵/值對作比較。為此，透過在標籤鍵名稱前面加上以下字串來參考 Condition 元素中的標籤：aws:RequestTag/*key-name*，然後指定必須存在的標籤值。

例如，下列範例政策會拒絕使用者或角色建立 AWS 帳戶 的任何請求，其中請求要么缺少 costcenter 標籤，要麼為該標籤提供了 1、2 或 3 之外的值。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "organizations:CreateAccount",
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/costcenter": "true"
                }
            }
        },
```

```
        {
            "Effect": "Deny",
            "Action": "organizations:CreateAccount",
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringNotEquals": {
                    "aws:RequestTag/costcenter": [
                        "1",
                        "2",
                        "3"
                    ]
                }
            }
        }
    ]
}
```

如需如何使用這些元素的詳細資訊，請參閱 IAM 使用者指南中的 aws:TagKeys 和 aws:RequestTag。

AWS Organizations 中的記錄和監控

最佳實務是應該監控您的組織，以確保所做的變更都會記錄。這可協助您確保任何非預期的變更都可受到調查，且任何不需要的變更都可復原。AWS Organizations 目前支援兩個 AWS 服務，可讓您監控組織與其中發生的活動。

主題

- 使用 AWS CloudTrail 記錄 AWS Organizations API 呼叫
- Amazon EventBridge

使用 AWS CloudTrail 記錄 AWS Organizations API 呼叫

AWS Organizations 已與 AWS CloudTrail 整合，這項服務可提供由使用者、角色或 AWS Organizations 中的 AWS 服務所採取之動作的記錄。CloudTrail 將 AWS Organizations 的所有 API 呼叫擷取為事件，包括來自 AWS Organizations 主控台以及來自對 AWS Organizations API 發出的程式碼呼叫。若您建立追蹤，便可將 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 AWS Organizations 的事件。即使您未設定追蹤，仍可透過 CloudTrail 主控台中的 Event history (事件歷史記錄) 檢視最新事件。您可以利用 CloudTrail 收集的資訊來判斷向 AWS Organizations 發出的請求，以及發出請求的 IP 地址、人員、時間和其他詳細資訊。

若要進一步了解 CloudTrail，請參閱《AWS CloudTrail 使用者指南》。

> **Important**
>
> 您可以僅在美國東部 (維吉尼亞北部) 區域檢視 AWS Organizations 的所有 CloudTrail 資訊。如果您沒有在 CloudTrail 主控台看到您的 AWS Organizations 活動，請使用右上角的功能表將您的主控台設定為美國東部 (維吉尼亞北部)。如果您使用 AWS CLI 或開發套件工具查詢 CloudTrail，請將您的查詢導向美國東部 (維吉尼亞北部) 端點。

CloudTrail 中的 AWS Organizations 資訊

當您建立帳戶時，系統即會在 AWS 帳戶 中啟用 CloudTrail。當活動發生於 AWS Organizations 中時，系統便會將該活動記錄於 CloudTrail 事件，並將其他 AWS 服務事件記錄至 Event history (事件歷史) 中。您可以檢視、搜尋和下載 AWS 帳戶 的最新事件。如需詳細資訊，請參閱使用 CloudTrail 事件歷史記錄檢視事件。

如需您 AWS 帳戶 帳戶中正在進行事件的記錄 (包含 AWS Organizations 的事件)，請建立追蹤。追蹤可讓 CloudTrail 將日誌檔案交付至 Amazon S3 儲存貯體。當您的 AWS 帳戶 啟用 CloudTrail 記錄功能時，對 AWS Organizations 動作發出的 API 呼叫會在 CloudTrail 日誌檔案中追蹤，與其他 AWS 服務記錄編寫在一起。您可設定其他 AWS 服務，進一步分析和處理 CloudTrail 記錄中所收集的事件資料。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務和整合
- 設定 CloudTrail 的 Amazon SNS 通知

CloudTrail 會記錄所有 AWS Organizations 動作，列在 AWS Organizations API 參考中。例如，對 `CreateAccount` (包括 `CreateAccountResult` 事件)、`ListHandshakesForAccount`、`CreatePolicy` 及 `InviteAccountToOrganization` 的呼叫，都會在 CloudTrail 日誌檔案中產生項目。

每個日誌項目都會包含產生要求之人員的資訊。日誌記錄中的使用者身分資訊，可協助您判斷下列事項：

- 該請求是否使用根使用者或 IAM 使用者憑證提出
- 提出該請求時，是否使用了特定 IAM 角色或聯合身分使用者的暫時安全憑證
- 該請求是否由另一項 AWS 服務提出

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

了解 AWS Organizations 日誌檔案項目

追蹤是一種組態，可讓事件以日誌檔案的形式交付至您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一或多個日誌項目。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時間、請求參數等資訊。CloudTrail 日誌檔並非依公有 API 呼叫的堆疊追蹤排序，因此不會以任何特定順序出現。

範例日誌項目：CloseAccount

下列範例顯示在呼叫 API 並且關閉帳戶的工作流程在後台開始處理時，所產生範例 `CloseAccount` 呼叫的 CloudTrail 日誌項目。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE:my-admin-role",
        "arn": "arn:aws:sts::111122223333:assumed-role/my-admin-role/my-session-id",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDAMVNPBQA3EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/my-admin-role",
                "accountId": "111122223333",
                "userName": "my-session-id"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2022-03-18T18:17:06Z"
            }
        }
    },
    "eventTime": "2022-03-18T18:17:06Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "CloseAccount",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.168.0.1",
    "userAgent":  "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)...",
```

```
    "requestParameters": {
        "accountId": "555555555555"
    },
    "responseElements": null,
    "requestID": "e28932f8-d5da-4d7a-8238-ef74f3d5c09a",
    "eventID": "19fe4c10-f57e-4cb7-a2bc-6b5c30233592",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

下列範例顯示關閉帳戶的後台工作流程成功完成後，CloseAccountResult 呼叫的 CloudTrail 日誌項目。

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "organizations.amazonaws.com"
  },
  "eventTime": "2022-03-18T18:17:06Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CloseAccountResult",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "organizations.amazonaws.com",
  "userAgent": "organizations.amazonaws.com",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "closeAccountStatus": {
      "accountId": "555555555555",
      "state": "SUCCEEDED",
      "requestedTimestamp": "Mar 18, 2022 6:16:58 PM",
      "completedTimestamp": "Mar 18, 2022 6:16:58 PM"
```

```
    }
   },
   "eventCategory": "Management"
}
```

範例日誌項目：CreateAccount

下列範例顯示在呼叫 API 並且建立帳戶的工作流程在後台開始處理時，產生的範例 CreateAccount 呼叫的 CloudTrail 日誌項目。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE:my-admin-role",
        "arn": "arn:aws:sts::111122223333:assumed-role/my-admin-role/my-session-id",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDAMVNPBQA3EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/my-admin-role",
                "accountId": "111122223333",
                "userName": "my-session-id"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-09-16T21:16:45Z"
            }
        }
    },
    "eventTime": "2018-06-21T22:06:27Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "CreateAccount",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.168.0.1",
    "userAgent":  "Mozilla/5.0 (Windows NT 10.0; Win64; x64)...",
    "requestParameters": {
        "tags": [],
        "email": "****",
        "accountName": "****"
```

```
    },
    "responseElements": {
        "createAccountStatus": {
            "accountName": "****",
            "state": "IN_PROGRESS",
            "id": "car-examplecreateaccountrequestid111",
            "requestedTimestamp": "Sep 16, 2020 9:20:50 PM"
        }
    },
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```

下列範例顯示了建立帳戶的後台工作流程成功完成後，CreateAccount 呼叫的 CloudTrail 日誌項目。

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "..."
  },
  "eventTime": "2020-09-16T21:20:53Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CreateAccountResult",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "....",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "createAccountStatus": {
      "id": "car-examplecreateaccountrequestid111",
      "state": "SUCCEEDED",
      "accountName": "****",
      "accountId": "444455556666",
      "requestedTimestamp": "Sep 16, 2020 9:20:50 PM",
```

```
      "completedTimestamp": "Sep 16, 2020 9:20:53 PM"
    }
  }
}
```

下列範例顯示了建立帳戶的 CreateAccount 後台工作流程失敗後，產生的 CloudTrail 日誌項目。

```
  {
  "eventVersion": "1.06",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2018-06-21T22:06:27Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CreateAccountResult",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "createAccountStatus": {
      "id": "car-examplecreateaccountrequestid111",
      "state": "FAILED",
      "accountName": "****",
      "failureReason": "EMAIL_ALREADY_EXISTS",
      "requestedTimestamp": Jun 21, 2018 10:06:27 PM,
      "completedTimestamp": Jun 21, 2018 10:07:15 PM
    }
  }
}
```

範例日誌項目：CreateOrganizationalUnit

下列範例顯示了範例 CreateOrganizationalUnit 呼叫的 CloudTrail 日誌項目。

```
{
```

```
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111111111111:user/diego",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "diego"
    },
    "eventTime": "2017-01-18T21:40:11Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "CreateOrganizationalUnit",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
    "requestParameters": {
        "name": "OU-Developers-1",
        "parentId": "r-a1b2"
    },
    "responseElements": {
        "organizationalUnit": {
            "arn": "arn:aws:organizations::111111111111:ou/o-aa111bb222/ou-
examplerootid111-exampleouid111",
            "id": "ou-examplerootid111-exampleouid111",
            "name": "test-cloud-trail"
        }
    },
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```


範例日誌項目：InviteAccountToOrganization

下列範例顯示了範例 `InviteAccountToOrganization` 呼叫的 CloudTrail 日誌項目。


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111111111111:user/diego",
```

```
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "diego"
    },
    "eventTime": "2017-01-18T21:41:17Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "InviteAccountToOrganization",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
    "requestParameters": {
        "notes": "This is a request for Mary's account to join Diego's organization.",
        "target": {
            "type": "ACCOUNT",
            "id": "111111111111"
        }
    },
    "responseElements": {
        "handshake": {
            "requestedTimestamp": "Jan 18, 2017 9:41:16 PM",
            "state": "OPEN",
            "arn": "arn:aws:organizations::111111111111:handshake/o-aa111bb222/invite/
h-examplehandshakeid111",
            "id": "h-examplehandshakeid111",
            "parties": [
                {
                    "type": "ORGANIZATION",
                    "id": "o-aa111bb222"
                },
                {
                    "type": "ACCOUNT",
                    "id": "222222222222"
                }
            ],
            "action": "invite",
            "expirationTimestamp": "Feb 2, 2017 9:41:16 PM",
            "resources": [
                {
                    "resources": [
                        {
                            "type": "MASTER_EMAIL",
                            "value": "diego@example.com"
                        },
```

```
                        {
                            "type": "MASTER_NAME",
                            "value": "Management account for organization"
                        },
                        {
                            "type": "ORGANIZATION_FEATURE_SET",
                            "value": "ALL"
                        }
                    ],
                    "type": "ORGANIZATION",
                    "value": "o-aa111bb222"
                },
                {
                    "type": "ACCOUNT",
                    "value": "222222222222"
                },
                {
                    "type": "NOTES",
                    "value": "This is a request for Mary's account to join Diego's
 organization."
                }
            ]
        }
    },
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```

範例日誌項目：AttachPolicy

下列範例顯示了範例 `AttachPolicy` 呼叫的 CloudTrail 日誌項目。回應表示呼叫失敗，因為請求的政策類型未於嘗試連接請求的根帳戶中啟用。

```
{
    "eventVersion": "1.06",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111111111111:user/diego",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
```

```
        "userName": "diego"
    },
    "eventTime": "2017-01-18T21:42:44Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "AttachPolicy",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
    "errorCode": "PolicyTypeNotEnabledException",
    "errorMessage": "The given policy type ServiceControlPolicy is not enabled on the
 current view",
    "requestParameters": {
        "policyId": "p-examplepolicyid111",
        "targetId": "ou-examplerootid111-exampleouid111"
    },
    "responseElements": null,
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```

Amazon EventBridge

AWS Organizations 可以搭配 Amazon EventBridge、先前的 Amazon CloudWatch Events 使用，以在管理員指定的動作在組織內發生時引發事件。例如，由於這類動作的靈敏度，多數管理員會想要在每次有人在組織中建立新帳戶，或在成員帳戶的管理員嘗試離開組織時收到警告。您可以設定尋找這些動作的 EventBridge 規則，然後將產生的事件傳送到管理員定義的目標。目標可以是傳送電子郵件或文字訊息給其訂閱者的 Amazon SNS 主題。您也可以建立 AWS Lambda 函式，記錄動作的詳細資訊以供日後審閱。

如需示範如何啟用 EventBridge 來監控組織內關鍵活動的教學資訊，請參閱教學課程：使用 Amazon EventBridge 監控您組織的重要變更。

若要進一步了解 EventBridge (包括如何配置及啟用 CloudWatch Events)，請參閱 Amazon EventBridge 使用者指南。

AWS Organizations 的合規驗證

要瞭解 AWS 服務 是否在特定法規遵循方案範圍內，請參閱法規遵循方案範圍內的 AWS 服務，並選擇您感興趣的法規遵循方案。如需一般資訊，請參閱 AWS 法規遵循方案。

您可使用 AWS Artifact 下載第三方稽核報告。如需詳細資訊，請參閱 AWS Artifact 中的下載報告。

您使用 AWS 服務 時的法規遵循責任取決於資料的敏感度、您的公司的合規目標，以及適用的法律和法規。AWS 提供以下資源協助您處理法規遵循事宜：

- 安全與合規快速入門指南 – 這些部署指南討論在 AWS 上部署以安全及合規為重心的基準環境的架構考量和步驟。
- Amazon Web Services 的 HIPAA 安全與法規遵循架構：本白皮書說明公司可如何運用 AWS 來建立符合 HIPAA 規定的應用程式。

> **Note**
>
> 並非全部的 AWS 服務 都符合 HIPAA 資格。如需詳細資訊，請參閱 HIPAA 資格服務參照。

- AWS 法規遵循資源：這組手冊和指南可能適用於您的產業和位置。
- AWS 客戶合規指南：透過合規角度瞭解共同的責任模式。這份指南總結了多個架構 (包括美國國家標準技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO)) 中，保護 AWS 服務並符合安全控制指引的最佳實務。
- AWS Config 開發人員指南中的使用規則評估資源：AWS Config 服務可評估資源組態對於內部實務、業界準則和法規的合規狀態。
- AWS Security Hub – 此 AWS 服務 可供您全面檢視 AWS 中的安全狀態。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 Security Hub controls reference。
- AWS Audit Manager – 此 AWS 服務 可協助您持續稽核 AWS 使用情況，以簡化管理風險與法規與業界標準的法規遵循方式。

中的恢復能力AWS Organizations

AWS 全球基礎架構是以 AWS 區域 與可用區域為中心建置的。AWS 區域 提供多個分開且隔離的實際可用區域，並以具備低延遲、高輸送量和高度備援特性的聯網相互連結。透過可用區域，您所設計與操作的應用程式和資料庫，就能夠在可用區域之間自動容錯移轉，而不會發生中斷。可用區域的可用性、容錯能力和擴充能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域 與可用區域的詳細資訊，請參閱AWS全球基礎架構。

AWS Organizations 中的基礎設施安全

作為一種受管服務，AWS Organizations 受 AWS 全球網路安全保護。如需有關 AWS 安全服務以及 AWS 如何保護基礎設施的詳細資訊，請參閱 AWS 雲端安全。若要使用基礎設施安全性的最佳實務來設計您的 AWS 環境，請參閱安全性支柱 AWS 架構良好的框架中的基礎設施保護。

您可使用 AWS 發佈的 API 呼叫，透過網路存取 Organizations。用戶端必須支援下列項目：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 具備完美轉送私密 (PFS) 的密碼套件，例如 DHE (Ephemeral Diffie-Hellman) 或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。現代系統 (如 Java 7 和更新版本) 大多會支援這些模式。

此外，請求必須使用存取索引鍵 ID 和與 IAM 主體相關聯的私密存取索引鍵來簽署。或者，您可以使用 AWS Security Token Service (AWS STS) 來產生暫時安全憑證來簽署請求。

如果您在透過命令列介面或 API 存取 AWS 時，需要 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的詳細資訊，請參閱聯邦資訊處理標準 (FIPS) 140-2 概觀。

AWS Organizations 參考

在此節使用此主題，針對 AWS Organizations 的各種面向來尋找詳細的參考資訊。

主題

的配額 AWS Organizations

本節指出會影響 AWS Organizations的配額。

命名指導方針

以下是您在中建立名稱的準則 AWS Organizations，包括帳戶名稱、組織單位 (OU)、根目錄和策略：

- 名稱必須由 Unicode 字元組成
- 名稱的最大字串長度因物件而異。若要查看每個項目的實際限制，請參閱 AWS Organizations API 參考，並尋找建立物件的 API 操作。查看該操作 Name 參數的詳細資訊。例如：Account name (帳戶名稱) 或 OU name (OU 名稱)。

最大值和最小值

以下是中實體的預設最大值。 AWS Organizations

> **Note**
>
> 您可以使用 Service Quotas 主控台，請求增加某些值。
> Organizations 是實體託管在美國東部 (維吉尼亞北部) 區域 (us-east-1) 的全域服務。因此，在使用 Service Quotas 主控台、或 AWS SDK 時，您必須使用us-east-1來存取 AWS CLI Organizations 配額。

組織 AWS 帳戶 中的數目	10 – 組織中允許的預設帳戶上限。如果您需要更多，可以使用 Service Quotas 主控台請求增加。

	傳送給帳戶的邀請計入此配額。若受邀帳戶拒絕、管理帳戶取消邀請或邀請到期，便會退回計數。 新建立的帳戶和組織可能會具有低於預設 10 個帳戶的配額。
組織中根帳戶的數量	1
組織中 OU 的數量	1000
組織中每個類型的政策數目	每個政策類型 1,000 個
政策文件的大小上限	服務控制政策：5120 個字元 AI 服務選擇退出政策：2500 個字元 備份政策：10,000 個字元 標籤政策：10,000 個字元 附註：如果您使用儲存原則 AWS Management Console，JSON 元素之間和引號之外的額外空格 (例如空格和分行符號) 將會移除且不計算在內。如果您使用 SDK 作業或儲存原則 AWS CLI，則原則會完全依照您提供的方式儲存，且不會自動移除字元。
在根帳戶中形成巢狀的最大 OU 數量	在根帳戶下可以有 5 個層級的 OU。
您在 24 小時期間內可執行的邀請嘗試上限	您的組織允許的帳戶為 20 或數目上限，以較大者為準。已接受的邀請不會計入此限制之內。一旦有邀請被接受，當天即可以傳送另一個邀請。 如果組織中允許的帳戶數目上限少於 20，如果您嘗試邀請的帳戶超過組織所能包含的帳戶數目時，則會出現「超出帳戶限制」例外狀況。不過，您可以在一天內取消邀請並傳送新邀請，最多可嘗試 20 次。
您可以同時建立的成員帳戶數量	5 個 – 一旦一個完成，您便可以開始另一個，但一次只能有 5 個進行中。

您可以在 30 天內關閉的成員帳戶數量	組織中成員帳戶的 10%，最多 1000 個。 • 小於 100 個帳戶 – 您最多可以關閉 10 個成員帳戶 • 100-10,000 個帳戶 — 您最多可以關閉 10% 的會員帳戶 • 超過一萬個帳戶 — 您最多可以關閉 1000 個會員帳戶 例如，如果您擁有 10,500 個會員帳戶，則可以在 30 天內關閉多達 1000 個（而非 1050 個）帳戶。達到此配額後，您可以在 AWS Billing 主控台中關閉其他帳戶，或者等待配額重置。如需更多資訊，請參閱《帳戶管理指南》中關閉帳戶前需要知道的事項AWS 。
您可以同時關閉的成員帳戶數量	3 個，一次只能關閉三個帳戶。完成後，您便可關閉另一個帳戶。
您可以連接政策的目標實體數目	無限制
您可以連接至根、OU 或帳戶的標籤數目	50
以資源為基礎的委派政策大小上限	40,000 個字元

交握過期時間

以下是握手的超時時間。 AWS Organizations

邀請加入組織	15 天
請求啟用組織中的所有功能	90 天
刪除交握並且不再顯示在清單中	完成交握之後的 30 天

您可以連接實體的政策數量

下限和上限取決於政策類型和您要連接政策的目標實體。下表顯示每個政策類型，以及您可以連接每個類型的目標實體數量。

> **Note**
>
> 這些數目只適用於那些直接連接至 OU 或帳戶的政策。透過繼承影響 OU 或帳戶的政策並未根據這些限制計數。

Policy type (政策類型)	連接至實體的數目下限	連接至根的數目上限	每個 OU 的連接數目上限	每個帳戶的連接數目上限
服務控制政策	1 – 每個實體必須至少隨時連接一個 SCP。您無法從實體移除最後一個 SCP。	5	5	5
AI 服務選擇退出政策	0	5	5	5
備份政策	0	10	10	10
標籤政策	0	10	10	10

> **Note**
>
> 目前，在組織中只能有一個根帳戶。

節流限制

下表依管理類別列出 AWS Organizations API，並顯示帳戶與組織層級各自的節流率。

AWS Organizations API	每個帳戶限制（費率，爆發）	每個組織限制 (速率、爆發)
帳戶管理		
CloseAccount	.05	
CreateAccount, CreateGovCloudAccount	0.1, 3	
DescribeAccount	20, 30	24, 36
DescribeCreateAccountStatus	二	2, 3
LeaveOrganization	1, 1	
ListCreateAccountStatus	5、8	六、十
握手管理		
AcceptHandshake, DescribeHandshake	1, 1	
CancelHandshake	2, 3	
DeclineHandshake	1, 3	
InviteAccountToOrganization	3, 5	
ListHandshakesForAccount, ListHandshakesForOrganization	5、8	六、十
組織管理		
CreateOrganization, DeleteOrganization, EnableFullControl	1, 1	
CreateOrganizationalUnit, DescribeOrganization	1、2	

AWS Organizations API	每個帳戶限制（費率，爆發）	每個組織限制 (速率、爆發)
MoveAccount, UpdateOrganizationalUnit, DeleteOrganizationalUnit	2, 3	
DescribeOrganizationalUnit	二	2, 3
ListAccounts	八、十二	9, 15
ListChildren	六、十	七、十二
ListParents, ListAccountsForParent, ListOrganizationalUnitsForParent	5、8	六、十
ListRoots	1、2	1, 3
ListTagsForResource	10, 15	12, 18
RemoveAccountFromOrganization	二	
TagResource, UntagResource	四、六	
政策管理		
CreatePolicy, DeletePolicy, AttachPolicy, DetachPolicy	2, 3	
DescribePolicy	二	2, 3
DisablePolicyType, EnablePolicyType	1, 1	
ListPolicies, ListPoliciesForTarget, ListTargetsForPolicy	5、8	六、十
UpdatePolicy	2, 3	
服務管理		

AWS Organizations API	每個帳戶限制（費率，爆發）	每個組織限制 (速率、爆發)
啟用AWSServiceAccess、停用 AWSServiceAccess	1、2	
列表AWSServiceAccess ForOrganization， ListDeleg atedServicesForAccount	1, 3	1, 4
ListDelegatedAdministrators	5、8	六、十
RegisterDelegatedAdministra tor, DeregisterDelegate dAdministrator	1、2	

可搭配 AWS Organizations 使用的 AWS 受管政策

此小節將說明供您用於管理組織的 AWS 受管政策。您無法修改或刪除 AWS 受管政策，但可以根據需要，將這些政策與您組織中的實體連接或分離。

可搭配 AWS Identity and Access Management (IAM) 使用的 AWS Organizations 受管政策

IAM 受管政策由 AWS 提供並維護。受管政策提供一般任務的許可，您可透過將受管政策連接至適當的 IAM 使用者或角色物件來指派給使用者。您不必自己編寫政策，並且在 AWS 視需要更新政策以支援新服務時，您會自動且立即獲得更新的優勢。您可以在 IAM 主控台的 Policies (政策) 頁面中看到 AWS 受管政策清單。使用 Filter policies (篩選政策) 下拉式清單，以選取 AWS 受管。

您會使用下列受管政策，以將許可授予組織中的使用者和角色。

政策名稱	描述	ARN
AWSOrganizationsFullAccess	提供建立和完整管理組織所需的所有許可。本政策聲明的內容顯示在以下程式碼片段中： `{ "Version": "2012-10-17",`	ARN: AW: IAM:: AWS: 策略/AWSOrganizationsFullAccess

政策名稱	描述	ARN
	"Statement": [{ "Sid": "AWSOrganizationsFullAccess", "Effect": "Allow", "Action": "organizations:*", "Resource": "*" }, { "Sid": "AWSOrganizationsFullAccessAccount", "Effect": "Allow", "Action": ["account:PutAlternateContact", "account:DeleteAlternateContact", "account:GetAlternateContact", "account:GetContactInformation", "account:PutContactInformation", "account:ListRegions", "account:EnableRegion", "account:DisableRegion"], "Resource": "*" }, { "Sid": "AWSOrganizationsFullAccessCreateSLR", "Effect": "Allow", "Action": "iam:CreateServiceLinkedRole",	

政策名稱	描述	ARN
	"Resource": "*", "Condition": { "StringEq uals": { "iam:AWSS erviceName": "organiza tions.amazonaws.com" } } }] }	

政策名稱	描述	ARN
AWSOrganizationsReadOnlyAccess	提供組織相關資訊的唯讀存取權。它不允許使用者進行任何變更。本政策聲明的內容顯示在以下程式碼片段中： `{ "Version":"2012-10-17", "Statement":[{ "Sid": "AWSOrganizationsReadOnly", "Effect":"Allow", "Action":["organizations:Describe*", "organizations:List*"], "Resource": "*" }, { "Sid": "AWSOrganizationsReadOnlyAccount", "Effect":"Allow", "Action":["account:GetAlternateContact", "account:GetContactInformation", "account:ListRegions"], "Resource": "*" }] }`	ARN: AW: IAM:: AWS: 策略/AWSOrganizationsReadOnlyAccess

Organizations AWS 受管政策更新

下表提供自此服務開始追蹤這些變更時 AWS 受管政策更新詳細資訊。如需有關此頁面變更的自動提醒，請訂閱 AWS Organizations文件歷史記錄頁面上的 RSS 摘要。

變更	描述	日期
AWSOrganizationsFullAccess-已更新以包含描述政策聲明的Sid元素。	Organizations 為AWSOrganizationsFullAccess 受管理的策略新增Sid元素。	2024年2月6日
AWSOrganizationsReadOnlyAccess-已更新以包含描述政策聲明的Sid元素。	Organizations 為AWSOrganizationsReadOnlyAccess 受管理的策略新增Sid元素。	2024年2月6日
AWSOrganizationsFullAccess— 已更新，允許AWS 區域透過 Organizations 主控台啟用或停用所需的帳戶 API 權限。	Organizations 將 account:ListRegions 、account:EnableRegion 和 account:DisableRegion 動作新增至政策，以啟用寫入存取權，來啟用或停用帳戶的區域。	2022 年 12 月 22 日
AWSOrganizationsReadOnlyAccess— 已更新，允許AWS 區域透過 Organizations 主控台列出所需的帳號 API 權限。	Organizations 將 account:ListRegions 動作新增至政策，以啟用檢視帳戶區域的存取權。	2022 年 12 月 22 日
AWSOrganizationsFullAccess— 已更新，允許透過 Organizations 主控台新增或編輯帳戶聯絡人所需的帳戶 API 權限。	Organizations 將 account:GetContactInformation 和 account:PutContactInformation 動作新增至政策，以啟用修改帳戶聯絡人的寫入存取權。	2022 年 10 月 21 日
AWSOrganizationsReadOnlyAccess— 已更新，允許透過 Organizations 主控台檢視帳戶聯絡人所需的帳戶 API 權限。	Organizations 將 account:GetContactInformation 動作新增至政策，以啟用檢視帳戶聯絡人的存取權。	2022 年 10 月 21 日

變更	描述	日期
AWSOrganizationsFullAccess-已更新以允許建立組織。	Organizations 已新增 `CreateServiceLinkedRole` 許可至政策，以啟用建立建立組織所需的服務連結角色。許可限於建立角色，該角色只能透過 `organizations.amazonaws.com` 服務使用。	2022 年 8 月 24 日
AWSOrganizationsFullAccess— 已更新，允許透過 Organizations 主控台新增、編輯或刪除帳戶替代聯絡人所需的帳戶 API 權限。	Organizations 新增了 `account:GetAlternateContact` 、`account:DeleteAlternateContact` 、`account:PutAlternateContact` 動作至政策，以啟用寫入存取權限來修改帳戶的替代聯絡人。	2022 年 2 月 7 日
AWSOrganizationsReadOnlyAccess— 已更新，允許透過 Organizations 主控台檢視帳戶替代聯絡人所需的帳戶 API 權限。	Organizations 新增了 `account:GetAlternateContact` 動作至政策，以啟用存取權限來檢視帳戶的替代聯絡人。	2022 年 2 月 7 日

AWS Organizations 受管服務控制政策

服務控制政策 (SCP) 類似 IAM 許可政策，但屬於 AWS Organizations (而不是 IAM) 的功能。您可以使用 SCP 指定受影響實體的最大許可。您可以將 SCP 連接到根、組織單位 (OU)，或者您組織中的帳戶。您可以建立自己的政策，或者可以使用 IAM 定義的政策。您可以在 Organizations 主控台的 Policies (政策) 頁面上，查看組織中的政策清單。

> **Important**
>
> 每個根、OU 和帳戶必須隨時至少連接一個 SCP。

政策名稱	描述	ARN
完整 AWSAccess	為 AWS Organizations 管理帳戶提供對成員帳戶的存取。	ARN: AW: 組織:: AWS: 原則/服務控制原則 /P-完整 AWSAccess

故障診斷 AWS Organizations

如果您在使用 AWS Organizations 時遇到問題，即可參閱本節中的各個主題。

主題

疑難排解一般問題

使用此處的資訊，來協助您針對在使用 AWS Organizations 時可能遇到的拒絕存取或其他常見問題進行診斷和修正。

主題

當我對 AWS Organizations 提出請求時，出現「存取遭拒」的訊息

- 確定您擁有許可來叫用所請求的動作和資源。管理員必須將 IAM 政策連接到您的使用者、群組或角色，以授予許可。如果授予這些許可的政策內容中包含了任何條件，例如時刻或 IP 地址的限制，則當您傳送請求時，也必須滿足這些要求。關於檢視或修改使用者、群組或角色的政策方面的相關資訊，請參閱《IAM 使用者指南》中的政策的使用。
- 如果您是手動簽署 API 請求 (而未使用 AWS SDK)，請確認您已正確地簽署請求。

當我使用臨時安全憑證來發出請求時，出現「存取遭拒」訊息

- 確認您用來發出請求的 使用者或角色，擁有正確的許可。暫時安全登入資料的許可衍生自 使用者或角色，因此許可僅限於授予 使用者或角色的範圍。關於臨時安全憑證許可的決定方式，詳細資訊請參閱 IAM 使用者指南中的控管臨時安全憑證的許可。
- 確認您的請求正確簽署且請求的格式也正確。如需詳細資訊，請參閱已選開發套件的工具組文件，或參閱 IAM 使用者指南 中的使用臨時安全憑證來請求存取 AWS 資源。
- 確認您的臨時安全憑證並未過期。如需詳細資訊，請參閱 IAM 使用者指南中的請求臨時安全憑證。

嘗試以成員帳戶身分離開組織或以管理帳戶身分移除成員帳戶時遇到「存取遭拒」訊息

- 只有在您啟用 IAM 使用者存取成員帳戶中的帳單時，才可以移除成員帳戶。如需詳細資訊，請參閱AWS Billing使用者指南中的啟用帳單和成本管理主控台的存取權。
- 只有在帳戶具有讓它以獨立帳戶形式運作所需的資訊時，您才能從組織移除帳戶。當您使用 AWS Organizations 主控台、API 或 AWS CLI 命令在組織建立帳戶時，不會自動收集該資訊。對於您想要讓它獨立的帳戶，您必須接受 AWS 客戶協議，選擇支援計劃，提供並驗證所需的聯絡資訊，然後提供目前的付款方法。AWS 會使用該付款方法來收取當帳戶未連接到組織時所發生的任何可計費 (非 AWS 免費方案) AWS 活動的費用。如需更多詳細資訊，請參閱 從成員帳戶離開組織。

當我試著新增帳戶到我的組織時，出現「超過配額」訊息

組織中可以擁有的帳戶數量有上限。即使帳戶已刪除或關閉，仍會計入此配額。

加入的邀請會計入組織中的帳戶數量上限。若受邀帳戶拒絕、管理帳戶取消邀請或邀請到期，便會退回計數。

- 關閉或刪除 AWS 帳戶 之前，請從您的組織移除它，使它不會繼續計入您的配額中。
- 如需有關如何請求增加配額的資訊，請參閱最大值和最小值。

我在新增或移除帳戶時遇到「此操作需要一段等待時間」訊息

有些動作需要等待期間。例如，您無法立即移除新建立的帳戶。請在幾天後再嘗試該動作。如果您在新增和移除帳戶時遇到帳戶配額的問題，請參閱最大值和最小值了解如何請求增加配額的相關資訊。

嘗試新增帳戶到我的組織時遇到「組織仍在初始化」訊息

如果您遇到此錯誤，而且在您建立組織後已超過一小時，請聯絡 AWS Support。

當我嘗試邀請帳戶加入我的組織時，收到「邀請已停用」訊息。

當啟用您組織中的所有功能時，就會發生這種情況。此操作可能需要一些時間，並且需要所有成員帳戶有所回應。操作完成之前，您無法邀請新帳戶加入組織。

我所做的變更不一定都會立即顯示

為供全球各地資料中心的電腦存取服務，AWS Organizations 採用稱為最終一致性的分散式運算模式。您在 AWS Organizations 中所進行的任何變更，均需要一段時間才能出現在所有可能的端點中。由於在各伺服器、各複寫區域之間傳送資料需耗費一些時間，因此會導致延遲。AWS Organizations 還會使用快取功能來改善效能，但在某些情況下，這將增加所花費的時間。直到先前快取的資料逾時後，才能看到變更。

在設計您的全球應用程式時，請將這些可能的延遲納入考量，並確保即使在某地點所進行的變更不會立即顯示於其他位置時，這些應用程式也能如預期運作。

如需此模式如何影響其他 AWS 服務的詳細資訊，請參閱下列資源：

- Amazon Redshift 資料庫開發人員指南中的管理資料一致性
- Amazon Simple Storage Service 使用者指南中的 Amazon S3 資料一致性模式
- 大數據部落格中的在使用 Amazon S3 和適用於 ETL 工作流程的 Amazon Elastic MapReduce 時確保一致性AWS
- Amazon EC2 API 參考中的 EC2 最終一致性

故障排除 AWS Organizations 政策

使用此處的資訊來協助您診斷並修正在 AWS Organizations 政策找到的常見錯誤。

服務控制政策

AWS Organizations 中的服務控制政策 (SCP) 類似 IAM 政策，並共享共同的語法。此語法的開頭為 JavaScript 物件標記法 (JSON) 規則。JSON 描述物件，其具有的名稱和值組會構成物件。IAM 政策文法透過定義名稱和值具有的意義作為建置基礎，使得使用政策來授予許可的 AWS 服務可了解它。

AWS Organizations 使用 IAM 語法和文法的子集。如需詳細資訊，請參閱SCP 語法。

常見的政策錯誤

- 多個政策物件
- 多個陳述式元素
- 政策文件大小超過上限

多個政策物件

一個 SCP 必須僅包含一個 JSON 物件。可在兩旁放置 { } 括弧來表示物件。雖然您可以在外側括弧對中嵌入額外的 { } 括弧以在 JSON 物件中巢套其他物件，但是一個政策只能包含一個最外層的 { } 括弧對。以下範例不正確，因為它在最上層包含兩個物件 (以##標示)：

```
{
  "Version": "2012-10-17",
  "Statement":
  {
     "Effect":"Allow",
     "Action":"ec2:Describe*",
     "Resource":"*"
  }
}
{
  "Statement": {
     "Effect": "Deny",
     "Action": "s3:*",
     "Resource": "*"
  }
}
```

不過，您可以使用正確的政策語法來達成前述範例的意圖。可以將兩個資料塊合併到單個 Statement 元素中，而非包含兩個各自擁有 Statement 元素的完整政策物件。Statement 元素將兩個物件組成的陣列作為其值，如以下範例所示：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
```

```
      "Resource":" *"
    },
    {
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

此範例無法進一步的壓縮到具有一個元素的 Statement，因為這兩個元素有不同的效果。一般而言，只有在每個陳述式中的 Effect 和 Resource 元素完全相同時，您才可以結合陳述式。

多個陳述式元素

此錯誤可能會先以上一章節中錯誤的變異顯示。但是，它在語法上是不同類型的錯誤。在以下範例中，頂層只有一個政策物件，由單一 { } 括弧組表示。但是，該物件包含兩個 Statement 元素。

一個 SCP 只能包含一個 Statement 元素，名稱 (Statement) 在冒號左側，它的值在冒號右側。Statement 元素的值必須是物件，以 { } 括弧表示，其中包含一個 Effect 元素、一個 Action 元素和一個 Resource 元素。以下範例不正確，因為在政策物件中包含兩個 Statement 元素：

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "ec2:Describe*",
    "Resource": "*"
  },
  "Statement": {
    "Effect": "Deny",
    "Action": "s3:*",
    "Resource": "*"
  }
}
```

由於值物件可以是多個值物件的陣列，您可以將兩個 Statement 元素結合到具有物件陣列的一個元素來解決這個問題，如以下範例所示：

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

```
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource":"*"
    },
    {
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

Statement 元素的值是一種物件陣列。此範例中的陣列包含兩個物件，每個物件是 Statement 元素的正確值。陣列中的每個物件之間用逗號隔開。

政策文件大小超過上限

SCP 文件的大小上限是 5,120 個字元。此大小上限包括所有字元 (包含空格)。若要減少 SCP 的大小，您可以移除引號外部的所有空格字元 (例如空格和換行字元)。

提出 HTTP 查詢請求以呼叫 API

本節包含使用 AWS Organizations 的查詢 API 的一般資訊。如需 API 操作和錯誤的詳細資訊，請參閱 AWS Organizations API 參考。

> **Note**
>
> 除了直接呼叫 AWS Organizations 查詢 API，您可以使用其中一個 AWS 開發套件。AWS 開發套件以程式庫以及適用於多種程式設計語言及平台 (Java、Ruby、.NET、iOS、Android 等) 的範本程式碼所組成。軟體開發套件提供便捷方法來建立對 AWS Organizations 和 AWS 的程式化存取。例如，開發套件會負責的工作諸如以密碼演算法簽署請求、管理錯誤以及自動重試請求。如需 AWS 開發套件的其他資訊 (包括如何下載並安裝開發套件)，請參閱 Amazon Web Services 工具。

AWS Organizations 的查詢 API 可讓您呼叫服務動作。查詢 API 請求為 HTTPS 請求，其一定含有 `Action` 參數，以指示所要執行的動作。AWS Organizations 支援使用 GET 和 POST 請求於所有操作。也就是說，API 不會要求您在某些動作上使用 GET，在其他動作上使用 POST。不過，GET 請求受限於 URL 的限制大小。此限制取決於瀏覽器，但一般限制為 2048 個位元組。因此，對於需要較大流量的查詢 API 請求，必須使用 POST 請求。

回應為 XML 文件。如需回應的詳細資訊，請參閱 AWS Organizations API 參考中的個別動作頁面。

主題

- 端點
- 必要的 HTTPS
- 簽署 AWS Organizations API 請求

端點

AWS Organizations 有託管在美國東部 (維吉尼亞北部) 區域的單一全域 API 端點。

如需有關所有服務之AWS端點和區域的詳細資訊，請參閱 AWS 一般參考.

必要的 HTTPS

由於查詢 API 會傳回安全憑證等敏感資訊，必須使用 HTTPS 加密所有 API 請求。

簽署 AWS Organizations API 請求

請求必須使用存取金鑰 ID 和私密存取金鑰簽署。強烈建議您不要使用 AWS 帳戶根使用者 憑證來執行 AWS Organizations 的日常作業。您可以使用使用者或角色的憑證。

若要簽署 API 請求，您必須使用 AWS 簽章第 4 版。如需有關使用 Signature 第 4 版的資訊，請參閱《IAM 使用者指南》中的簽署 AWS API 請求。

AWS Organizations 不支援先前版本，例如簽章第 2 版。

如需詳細資訊，請參閱下列內容：

- AWS 安全憑證 – 提供關於可用來存取 AWS 之憑證類型的一般資訊。
- IAM 最佳實務 – 提供使用 IAM 服務來協助保護 AWS 資源 (包括 AWS Organizations 中的資源) 的建議。
- IAM 暫時性安全憑證 – 描述如何建立和使用暫時性安全憑證。

AWS Organizations 的文件歷程記錄

下表會說明 AWS Organizations 的主要文件更新。

- API 版本：2016-11-28

變更	描述	日期
更新的政策聲明	已將新Sid元素新增至受AWS Organizations管理的原則陳述式。	2024年2月6日
新增關閉管理帳戶主題	已新增考量事項和詳細步驟的連結，逐步瞭解如何關閉管理帳戶。	2024年2月1日
更新的最佳實務	在最佳實務區段新增資訊，以協助符合 IAM 最佳實務。	2023 年 6 月 12 日
更新了 AWSOrganizationsFullAccess 和 AWSOrganizationsReadOnlyAccess受管理的策略	已更新這兩個受管政策，以啟用對帳戶聯絡人的寫入或讀取存取權。	2022 年 10 月 21 日
更新了 AWSOrganizationsFullAccess 受管策略	受管政策已更新，允許透過新增必要的許可，來建立新組織所需的服務連結角色，從而建立組織。	2022 年 8 月 24 日
Organizations 從 AWS Organizations 主控台關閉帳戶功能	管理帳戶中的主體可從 AWS Organizations 主控台關閉成員帳戶，並使用 IAM 政策保護成員帳戶以免遭意外關閉。	2022 年 3 月 29 日
已更新使用 AWS Organizations 主控台更新替代聯絡人的通知	Organizations 現在提供使用 AWS Organizations 主控台更新組織內帳戶替代聯絡人的功	2022 年 2 月 8 日

	能。宣佈新功能，並指向帳戶管理參考，以獲得指示。	
Organizations 受管政策更新 - 更新至現有政策	更新 AWSOrganizationsFullAccess 和受 AWSOrganizationsReadOnlyAccess管政策，允許透過AWS Organizations主控台更新或檢視帳戶替代聯絡人所需的帳戶 API 權限。	2022 年 2 月 7 日
Organizations 與 Amazon DevOps 大師集成	您可以將 Amazon DevOps Guru 與整合，以全面監控所有組織帳戶的應用程式運作狀態，並取得深AWS Organizations入見解。	2022 年 1 月 3 日
Organizations 與 Amazon Detective 的整合	您可以將 Amazon Detective 與 AWS Organizations 整合，以確保 Detective 行為圖提供對所有組織帳戶活動的可見性。	2021 年 12 月 16 日
Organizations 與 AWS Config 整合，現在支援多帳戶多區域資料彙總。	您可以使用委派的管理員帳戶，從組織的所有成員帳戶彙總資源組態與合規資料。如需詳細資訊，請參閱AWS Config開發人員指南中的多帳戶多區域資料彙總。	2021 年 6 月 16 日
Organizations 與 AWS Firewall Manager 的整合現在包含對委派管理員的支援	您現在可以將組織中的成員帳戶指定為整個組織的 Firewall Manager StackSets 管理員。這樣可以更好地將許可與組織的管理帳戶分離。	2021 年 4 月 30 日
Organizations 備份政策現在支援持續備份	您可以使用 AWS Backup 持續備份功能與您組織的備份政策。	2021 年 3 月 10 日

Organizations 與 AWS CloudFormation StackSets 的整合現在包含對委派管理員的支援	您現在可以將組織中的成員帳戶指定為整個組織的AWS CloudFormation StackSets 管理員。這樣可以更好地將許可與組織的管理帳戶分離。	2021 年 2 月 18 日
啟用所有功能的同時繼續邀請帳戶	AWS 已更新程序以啟用組織中的所有功能。您現在可以繼續邀請新帳戶加入您的組織，同時等待現有帳戶回應其邀請。	2021 年 2 月 3 日
推出 2.0 版 AWS Organizations 主控台	AWS 推出了新版 AWS 主控台。所有文件已更新，以反映執行任務的新方式。	2021 年 1 月 21 日
Organizations 現在支援與 AWS Marketplace 整合	您現在可以啟用 AWS Marketplace，以在組織中跨所有帳戶更輕鬆地共享軟體授權。	2020 年 12 月 3 日
Organizations 現在支援與 Amazon S3 Lens 整合	Amazon S3 Lens 支援 Organizations 的受信任存取和委派管理員。如需詳細資訊，請參閱 Amazon Simple Storage Service 使用者指南中的 Amazon S3 Storage Lens。	2020 年 11 月 18 日
跨帳戶備份複本	當您使用備份政策來備份組織中的資源時，現在可以將備份的複本存放在組織的其他 AWS 帳戶 中。	2020 年 11 月 18 日
中國的 AWS 區域 現在支援 AWS Resource Access Manager 作為 Organizations 受信任服務	當您使用 Organizations 和中國的 AWS RAM 時，您現在可以使用 AWS RAM 功能，這項功能可與 Organizations 整合為受信任服務。	2020 年 11 月 18 日

Organizations 現在支援與 AWS Security Hub 整合	您可以跨組織中的所有帳戶啟用 Security Hub，並將組織的其中一個成員帳戶指定為 Security Hub 的委派系統管理員帳戶。	2020 年 11 月 12 日
已重新命名主要帳戶	AWS Organizations 已將「主要帳戶」的名稱變更為「管理帳戶」。這只是名稱變更，且功能沒有任何改變。	2020 年 10 月 20 日
新增最佳實務區段和主題	新增章節，以取得 AWS Organizations 的最佳實務。新章節包含討論管理帳戶和成員帳戶根使用者及密碼管理的最佳實務的主題。	2020 年 10 月 6 日
新增最佳實務區段和前兩頁	主體有一個新的章節，用於描述 AWS Organizations 的最佳實務。此更新包含組織管理帳戶的最佳實務主題，以及成員帳戶的最佳實務主題。	2020 年 10 月 2 日
Organizations 備份政策現在使用 VSS (磁碟區陰影複製服務)，支援 Windows EC2 執行個體上應用程式一致的備份	備份政策支援新的 `advanced_backup_settings` 區段。該新區段中的第一個項目是稱為 `WindowsVSS` 的 `ec2` 設定，您可以啟用或停用。如需詳細資訊，請參閱AWS Backup開發人員指南中的建立啟用 VSS 的 Windows Backup。	2020 年 9 月 24 日

Organizations 支持 tag-on-create 和基於標籤的訪問控制	您可以在建立 Organizations 資源時向其新增標籤。您可以使用標籤政策來標準化 Organizations 資源的標籤使用情況。您可以使用IAM 政策，來限制僅存取具有指定標籤鍵和值的資源。	2020 年 9 月 15 日
已新增 AWS Health 作為受信任服務	您可以彙總組織中跨帳戶的 AWS Health 事件。	2020 年 8 月 4 日
人工智慧 (AI) 服務選擇退出政策	您可以使用 AI 服務選擇退出政策來控制 AWS AI 服務是否會存放和使用由這些服務 (AI 內容) 處理的客戶內容，以便開發和持續改善 AWS 人工智慧服務與技術。	2020 年 7 月 8 日
已新增備份政策和與 AWS Backup 的整合	您可以使用備份政策，以建立和強制執行組織中所有帳戶的備份政策。	2020 年 6 月 24 日
支援 IAM Access Analyzer 的委派管理	您可將組織中 Access Analyzer 的管理存取權委派給指定的成員帳戶。	2020 年 3 月 30 日
與 AWS CloudFormation 整合 StackSets	您可以建立服務管理的堆疊集，將堆疊執行個體部署到由 AWS Organizations 管理的帳戶。	2020 年 2 月 11 日
與 Compute Optimizer 整合	Compute Optimizer 已作為一項服務新增，可與您組織中的帳戶搭配運作。	2020 年 2 月 4 日
標籤政策	您可以使用標籤政策，協助將組織帳戶中各資源的標籤標準化。	2019 年 11 月 26 日

與 Systems Manager 整合	您可以在 Systems Manager Explorer 中，同步組織中所有 AWS 帳戶 的操作資料。	2019 年 11 月 26 日
AWS：PrincipalOrgPaths	針對提出請求的 IAM 使用者、IAM 角色或 AWS 帳戶 根使用者，新的全域條件金鑰會檢查 AWS Organizations 路徑。	2019 年 11 月 20 日
與 AWS Config 規則整合	您可以使用 AWS Config API 操作來管理組織中所有 AWS 帳戶 的 AWS Config 規則。	2019 年 7 月 8 日
用於受信任存取的新服務	新增了 Service Quotas 做為服務，可以與組織中的帳戶搭配運作。	2019 年 6 月 24 日
與 AWS Control Tower 整合	新增了 AWS Control Tower 做為服務，可以與組織中的帳戶搭配運作。	2019 年 6 月 24 日
與 AWS Identity and Access Management 整合	針對您的組織實體 (組織根、OU 和帳戶)，IAM 會提供服務上次存取的資料。您可以使用此資料，將存取限制在僅限您需要的 AWS 服務。	2019 年 6 月 20 日
標記帳戶	您可以在您的組織中標記和取消標記帳戶，以及檢視組織中帳戶上的標籤。	2019 年 6 月 6 日
服務控制政策 (SCP) 中的資源、條件和 NotAction 元素	您現在可以在 SCP 中指定資源、條件及 NotAction 元素，拒絕您組織或組織單位 (OU) 中的跨帳戶存取。	2019 年 3 月 25 日

用於受信任存取的新服務	新增了 AWS License Manager 和 Service Catalog 服務，其可以與組織中的帳戶搭配運作。	2018 年 12 月 21 日
用於受信任存取的新服務	新增了 AWS CloudTrail 和 AWS RAM 做為服務，可以與組織中的帳戶搭配運作。	2018 年 12 月 4 日
用於受信任存取的新服務	新增了 AWS Directory Service 做為服務，可以與組織中的帳戶搭配運作。	2018 年 9 月 25 日
電子郵件地址驗證	您必須先驗證您擁有與管理帳戶關聯的電子郵件地址，之後才可以邀請現有的帳戶加入您的組織。	2018 年 9 月 20 日
CreateAccount 通知	`CreateAccount` 通知會發佈至管理帳戶的 CloudTrail 記錄檔。	2018 年 6 月 28 日
用於受信任存取的新服務	新增了 AWS Artifact 做為服務，可以與組織中的帳戶搭配運作。	2018 年 6 月 20 日
用於受信任存取的新服務	新增了 AWS Config 和 AWS Firewall Manager 做為服務，可以與組織中的帳戶搭配運作。	2018 年 4 月 18 日
受信任服務存取	您現在可以啟用或停用精選 AWS 服務的存取，以在您組織的帳戶中工作。IAM Identity Center 是一開始就支援的受信任服務。	2018 年 3 月 29 日

帳戶移除現在為自助服務	您現在可以移除從 AWS Organizations 內建立的帳戶，無需聯絡 AWS Support。	2017 年 12 月 19 日
已新增對新服務 AWS IAM Identity Center 的支援	AWS Organizations 現在支援與 AWS IAM Identity Center (IAM Identity Center) 整合。	2017 年 12 月 7 日
AWS 新增了對所有組織帳戶的服務連結角色	名為 `AWSServiceRoleForOrganizations` 的服務連結角色已新增至組織中的所有帳戶，以啟用 AWS Organizations 與其他 AWS 服務之間的整合。	2017 年 10 月 11 日
您現在可以移除已建立的帳戶	客戶現在可以透過 AWS Support 的協助，從組織中移除已建立的帳戶。	2017 年 6 月 15 日
服務啟動	隨著新服務的推出，提供 AWS Organizations 文件的初始版本。	2017 年 2 月 17 日

AWS 詞彙表

如需最新的 AWS 術語，請參閱《AWS 詞彙表 參考》中的 AWS 詞彙表。

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。