使用者指南

AWS Control Tower

AWS Control Tower: 使用者指南

Table of Contents

什麼是 AWS Control Tower？

AWS Control Tower 提供簡單的方法，可按照規範的最佳實務來設定和管理 AWS 多帳戶環境。AWS Control Tower 可協調其他多項AWS 服務的功能 AWS Organizations，包括和 AWS Service Catalog AWS IAM Identity Center，在不到一小時的時間內建立 landing zone。資源是代表您設置和管理的。

AWS Control Tower 協調流程可擴展的 AWS Organizations功能。為了協助您的組織和帳戶免於偏離最佳實務，AWS Control Tower 會套用控制項 (有時稱為護欄)。例如，您可以使用控制項來協助確保已建立安全性記錄檔和必要的跨帳戶存取權限，而且不會變更。

如果您託管的帳戶數量不止一些，那麼擁有可促進帳戶部署和帳戶管理的協調流程層是有益的。您可以採用 AWS Control Tower 作為佈建帳戶和基礎設施的主要方式。使用 AWS Control Tower，您可以更輕鬆地遵守企業標準、符合法規要求，並遵循最佳實務。

AWS Control Tower 可讓分散式團隊中的最終使用者透過 Account Factory 中的可設定帳戶範本，快速佈建新 AWS 帳戶。同時，您的中央雲端管理員可以監控所有帳戶是否符合公司範圍內既定的合規性原則。

簡而言之，AWS Control Tower 根據與數千家企業合作所建立的最佳實務，提供最簡單的方式來設定和管理安全、合規的多帳戶 AWS 環境。如需使用 AWS Control Tower 的詳細資訊，以及 AWS 多帳戶策略中概述的最佳實務，請參閱AWS 多帳戶策略：最佳做法指南。

功能

AWS Control Tower 具有以下功能：

- landing zone：登陸區是一個架構良好的多帳戶環境，以安全性和合規性最佳做法為基礎。它是整個企業的容器，可容納您希望遵守法規遵循的所有組織單位 (OU)、帳戶、使用者和其他資源。登陸區域可以擴展至符合任何大小企業的需求。
- 控制項 — 控制項 (有時稱為護欄) 是一種高階規則，可為您的整體 AWS 環境提供持續的治理。其表示的方式是普通語言。存在三種控制：預防性，偵探和主動。三種類別的指引適用於控制：強制性、強烈建議或選修科目。如需控制項的詳細資訊，請參閱控制項如何運作。
- Account Factory — Account Factory 是可設定的帳戶範本，可協助使用預先核准的帳戶設定來標準化新帳戶的佈建。AWS Control Tower 提供內建的 Account Factory，可協助自動化組織中的帳戶佈建工作流程。如需詳細資訊，請參閱 使用 Account Factory 佈建和管理帳戶。
- 儀表板 — 儀表板可為您的中央雲端管理員團隊提供持續監督您的 landing zone。使用儀表板可查看整個企業中佈建的帳戶、針對原則強制執行啟用的控制項、為持續偵測原則不符合而啟用的控制項，以及依帳戶和 OU 組織的不符合標準資源。

AWS Control Tower 如何與其他服務互 AWS 動

AWS Control Tower 建立在受信任且可靠的 AWS 服務之上 AWS Service Catalog，包括 AWS IAM Identity Center、和 AWS Organizations。如需詳細資訊，請參閱 整合服務。

您可以將 AWS Control Tower 與其他 AWS 服務合併到可協助您將現有工作負載遷移到的解決方案中 AWS。如需詳細資訊，請參閱如何利用 AWS Control Tower 和將工作負載遷移 CloudEndure 到 AWS.

組態、控管與擴充性

- 自動化帳戶組態：AWS Control Tower 透過 Account Factory (或稱「自動售貨機」) 自動化帳戶部署和註冊，該工廠是以抽象方式建置在中已佈建產品之上。 AWS Service CatalogAccount Factory 可以建立和註冊 AWS 帳戶，並將控制項和政策套用至這些帳戶的程序自動化。
- 集中式控管：AWS Control Tower 透過運用的功能 AWS Organizations，建立一個框架，以確保在您的多帳戶環境中保持一致的合規性和管控。該 AWS Organizations 服務提供了管理多帳戶環境的基本功能，包括集中管理和管理帳戶，從 AWS Organizations API 創建帳戶以及服務控制策略（SCP）。

- 擴充性：您可以直接在 AWS Control Town 主控台和 AWS Control Town 主控台中工作 AWS Organizations，建立或擴充自己的 AWS Control 塔環境。註冊現有組織並將現有帳戶註冊到 AWS Control Tower 後，您可以在 AWS Control Tower 中看到您的變更。您可以更新 AWS Control Tower landing zone 以反映您的變更。如果您的工作負載需要進一步的進階功能，您可以利用其他 AWS 合作夥伴解決方案和 AWS Control Tower。

您是 AWS Control Tower 的首次使用者嗎？

若您是第一次使用此服務，我們建議您閱讀以下內容：

1. 如果您需要有關如何規劃和組織 landing zone 的詳細資訊，請參閱規劃您的 AWS Control Tower landing zone和AWS 適用於 AWS Control Tower landing zone 的多帳戶策略。
2. 若您已準備好建立第一個登陸區，請參閱開始使用 AWS Control Tower。
3. 如需漂移偵測和預防的資訊，請參閱偵測並解決 AWS Control Tower 中的漂移。
4. 如需安全詳細資訊，請參閱AWS Control Tower 中的安全性。
5. 如需更新 landing zone 和會員帳戶的資訊，請參閱AWS Control Tower 中的組態更新管理。

AWS Control Tower 的運作方式

本節將詳細介紹 AWS Control Tower 的運作方式。您的 landing zone 是一個架構良好的多帳戶環境，可存放所有資源。 AWS 您可以使用此環境對所有 AWS 帳戶強制執行法規遵循法規。

AWS Control Tower 登陸區的結構

AWS Control Tower 中的 landing zone 結構如下：

- 根 — 包含 landing zone 域中所有其他 OU 的父系。
- 安全性 OU — 此 OU 包含記錄封存和稽核帳戶。這些帳戶通常稱為共用帳戶。啟動 landing zone 時，您可以為這些共用帳戶選擇自訂名稱，並且可以選擇將現有 AWS 帳戶帶入 AWS Control Tower 以進行安全和記錄。不過，這些帳戶無法在稍後重新命名，並且在初始啟動之後，無法新增現有帳戶以確保安全性和記錄。
- 沙箱 OU — 沙箱 OU 會在您啟動 landing zone 時建立 (如果您啟用此功能)。這個和其他已註冊的 OU 包含您的使用者用來執行其 AWS 工作負載的已註冊帳戶。
- IAM 身分中心目錄 — 此目錄存放您的 IAM 身分中心使用者。它定義了每個 IAM 身分中心使用者的許可範圍。
- IAM 身分中心使用者 — 這些是您的使用者在 landing zone 執行 AWS 工作負載時可假設的身分識別。

設定 landing zone 時會發生什麼情況

當您設定 landing zone 域時，AWS Control Tower 會代表您在管理帳戶中執行下列動作：

- 建立兩個 AWS Organizations 組織單位 (OU)：安全性和沙箱 (選用)，包含在組織根結構中。
- 在安全性 OU 中建立或新增兩個共用帳戶：記錄封存帳戶和稽核帳戶。
- 如果您選擇預設的 AWS Control Tower 組態，或允許您自行管理身分供應商，請在 IAM 身分中心建立具有預先設定群組和單一登入存取權的雲端原生目錄。
- 套用所有強制性、預防性控制以強制執行原則。
- 套用所有必要的偵測控制項，以偵測組態違規。
- 預防性控制不會套用至管理帳戶。
- 除了管理帳戶外，控制項會套用至整個組織。

在 AWS Control Tower 登陸區域和帳戶內安全管理資源

- 當您建立 landing zone 域時，會建立許多 AWS 資源。若要使用 AWS Control Teck，您不得修改或刪除本指南所述支援的方法以外的這些 AWS Control Tower 受管資源。刪除或修改這些資源將導致您的 landing zone 進入未知狀態。如需詳細資訊，請參閱建立和修改 AWS Control Tower 資源的指導
- 當您啟用選用的控制項 (具有強烈建議或選擇性指導的控制項) 時，AWS Control Tower 會建立在您帳戶中管理的 AWS 資源。請勿修改或刪除 AWS Control Tower 建立的資源。這樣做可能會導致控制項進入未知的狀態。

什麼是共享帳戶？

在 AWS Control Tower 中，系統會在設定期間佈建 landing zone 域中的共用帳戶：管理帳戶、日誌存檔帳戶和稽核帳戶。

什麼是管理帳戶？

這是您專門為 landing zone 建立的帳戶。此帳戶用於為您的 landing zone 中的所有內容計費。它也可用於 Account Factory 佈建帳戶，以及管理 OU 和控制項。

> **Note**
>
> 不建議從 AWS Control Tower 管理帳戶執行任何類型的生產工作負載。建立個別的 AWS Control Tower 帳戶來執行工作負載。

如需詳細資訊，請參閱 管理帳戶。

什麼是日誌存檔帳戶？

此帳戶可做為 landing zone 中所有帳號之 API 活動記錄和資源設定的儲存庫。

如需詳細資訊，請參閱 日誌存檔帳戶。

什麼是審計帳戶？

稽核帳戶是受限制的帳戶，旨在讓安全性和法規遵循團隊讀取和寫入您 landing zone 中所有帳戶的權限。您可以從稽核帳戶透過僅授與 Lambda 函數的角色，以程式設計方式存取審核帳戶。稽核帳戶不

允許您手動登入其他帳戶。如需 Lambda 函數和角色的詳細資訊，請參閱設定 Lambda 函數以擔任另一個函數的角色 AWS 帳戶。

如需詳細資訊，請參閱 稽核帳戶。

控制項如何運作

控制項是一項高階規則，可為您的整體 AWS 環境提供持續的治理。每個控制項都會強制執行單一規則，並以簡單的語言表示。您可以隨時從 AWS Control Tower 主控台或 AWS Control Tower API 變更生效的選擇性或強烈建議的控制。一律套用強制控制項，而且無法變更。

預防性控制可防止動作發生。例如，名為「不允許變更 Amazon S3 儲存貯體政策」的選擇性控制項 (先前稱為「不允許變更日誌存檔政策」) 可防止日誌存檔共用帳戶中的任何 IAM 政策變更。任何嘗試執行已阻止的動作都會遭到拒絕並登入 CloudTrail。資源也會登入 AWS Config。

Detective 測控制項會偵測特定事件發生時，並將動作記錄在中CloudTrail。例如，強烈建議使用名為「偵測是否為連接到 Amazon Amazon EC2 執行個體的 Amazon EBS 磁碟區啟用加密」控制項，可偵測未加密的 Amazon EBS 磁碟區是否已連接到 landing zone 中的 EC2 執行個體。

在您的帳戶中佈建資源之前，主動控制會先檢查資源是否符合貴公司的政策和目標。如果資源不符合性，則不會佈建它們。主動式控制會透過 AWS CloudFormation 範本監控將部署在您帳戶中的資源。

對於熟悉的人 AWS：在 AWS Control Tower 中，預防控制是透過服務控制政策 (SCP) 來實作。Detective 控制項是透過 AWS Config 規則來實作。主動控制是通過 AWS CloudFormation 鉤子實現的。

相關主題

- 偵測並解決 AWS Control Tower 中的漂移

AWS Control Tower 如何搭配使用 StackSets

AWS Control Tower 用 AWS CloudFormation StackSets 於在您的帳戶中設定資源。每個堆棧集都具 StackInstances 有對應於帳戶和 AWS 區域 每個帳戶。AWS Control Tower 會為每個帳戶和區域部署一個堆疊集執行個體。

AWS Control Tower 將更新套用至特定帳戶，並根據 AWS CloudFormation 參數 AWS 區域 選擇性地套用更新。當更新套用至某些堆疊執行個體時，其他堆疊執行個體可能會留在 Outdated (過期) 狀態。這種行為是預期之中，且是正常的。

當堆疊執行個體進入 Outdated (過期) 狀態時，這通常表示對應於該堆疊執行個體的堆疊與堆疊集中的最新範本不符。堆疊會保留在較舊的範本中，因此可能不會包含最新的資源或參數。堆疊仍然完全可用。

以下是根據更新期間指定的 AWS CloudFormation 參數，快速摘要說明預期的行為：

如果堆疊集更新包含對範本的變更 (亦即，如果指定了或屬性)，`TemplateBody`或者如果已指定`TemplateURL`屬性，則會在更新指定帳戶中的堆疊執行個體和之前，將狀態為「過期」的所有堆疊執行個體 AWS CloudFormation 標記為「過期」的堆疊執行個體 AWS 區域。`Parameters`如果堆疊集更新不包含範本或參數的變更，請 AWS CloudFormation 更新指定帳戶和區域中的堆疊執行個體，同時保留所有其他堆疊執行個體的現有堆疊執行個體狀態。若要更新與堆疊集相關聯的所有堆疊執行個體，請勿指定 `Accounts` 或 `Regions` 屬性。

如需詳細資訊，請參閱《使用指南》中的 AWS CloudFormation 〈更新堆疊集〉。

術語

以下是您在 AWS Control Tower 文件中看到的一些術語的快速回顧。

首先，很高興知道 AWS Control Tower 與 AWS Organizations 服務分享了許多術語，包括本文件中出現的組織和組織單位 (OU) 術語。

- 如需有關組織和 OU 的詳細資訊，請參閱AWS Organizations 術語和概念。如果您是 AWS Control Tower 的新手，那麼該術語就是開始的好地方。
- AWS Organizations是一項 AWS 服務，可協助您集中控管環境，隨著您的工作負載擴充和擴展 AWS。AWS Control Tower 仰賴 AWS Organizations 建立帳戶、在 OU 層級強制執行預防控制，以及提供集中式帳單。
- AWS Account Factory 帳戶是使用 AWS Control Tower 中的 Account Factory 佈建的帳戶。 AWS 有時，Account Factory 被非正式地稱為帳戶的「自動售貨機」。
- 您的 AWS Control Tower 本地 AWS 區域是部署 AWS Control Tower landing zone 域的區域。您可以在 landing zone 設定中檢視您的居住區域。
- AWS Service Catalog可讓您集中管理常用部署的 IT 服務。在本文件的內容中，Account Factory 會使 AWS Service Catalog 用佈建新 AWS 帳戶，包括自訂藍圖中的帳戶。
- AWS CloudFormation StackSets是一種可擴充堆疊功能的資源，讓您可以透過單一作業和單一 CloudFormation範本，跨多個帳號和區域建立、更新或刪除堆疊。
- 堆棧實例是對區域內目標帳戶中堆棧的引用。
- 堆疊是您可以作為單一單元來管理的 AWS 資源集合。
- 彙總器是一種 AWS Config 資源類型，可從組織內的多個帳戶和區域收集組 AWS Config 態和符合性資料，可讓您在單一帳戶內檢視和查詢此符合性資料。
- 符合性套件是 AWS Config 規則和修正動作的集合，可部署為帳戶和區域中的單一實體，或在中的組織中部署。 AWS Organizations您可以使用一致性套件協助自訂 AWS Control Tower 環境。如需提供更多詳細資訊的技術部落格，請參閱相關資訊。
- AWS Control Tower 中的基準是一組可套用至目標的資源和特定組態。最常見的基準目標可能是組織單位 (OU)。例如，呼叫`AWSControlTowerBaseline`的基準可協助您向 AWS Control Tower 註冊 OU。在 landing zone 設定和更新期間，基準目標可能是共用帳戶，也可以是整個 landing zone 域的特定設定。
- 藍圖：藍圖是封裝某些中繼資料的成品，用於描述帳戶中部署的基礎結構元件。例如， AWS CloudFormation 範本可以做為 AWS Control Tower 帳戶的藍圖。

- 漂移：由 AWS Control Tower 安裝和設定的資源變更。沒有漂移的資源可讓 AWS Control Tower 正常運作。
- 不相容的資源：違反定義特定偵測控制 AWS Config 項之規則的資源。
- 共用帳戶：AWS Control Tower 在您設定 landing zone 時自動建立的三個帳戶之一：管理帳戶、記錄存檔帳戶和稽核帳戶。您可以在安裝期間為記錄封存帳戶和稽核帳戶選擇自訂名稱。
- 成員帳戶：成員帳戶屬於 AWS Control Tower 組織。成員帳戶可以在 AWS Control Tower 註冊或取消註冊。當註冊的 OU 包含已註冊和未註冊帳戶的混合時：
  - 在 OU 上啟用的預防性控制適用於其中的所有帳戶，包括未註冊的帳戶。這是因為預防性控制是在 OU 層級 (而不是帳戶層級) 使用 SCP 強制執行的。如需詳細資訊，請參閱 AWS Organizations 文件中的服務控制原則的繼承。
  - 在 OU 上啟用的 Detective 控制項不會套用至未註冊的帳戶。

  一個帳戶一次只能是一個組織的成員，其費用會計入該組織的管理帳戶中。成員帳戶可以移至組織的根容器。
- AWS account： AWS 帳號充當資源容器和資源隔離邊界。 AWS 帳戶可以與帳單和付款相關聯。AWS 帳戶與 AWS Control Tower 中的使用者帳戶 (有時稱為 IAM 使用者帳戶) 不同。透過 Account Factory 佈建程序建立的帳戶是 AWS 帳戶。 AWS 您也可以透過帳戶註冊或 OU 註冊程序，將帳戶新增至 AWS Control Tower。
- 控制：控制項 (也稱為護欄) 是一項高階規則，可為您的整體 AWS Control Tower 環境提供持續的管控。每個控制項都會強制執行單一規則。使用 SCP 來實作預防性控制。Detective 控制項是透過 AWS Config 規則來實作。主動控制是通過 AWS CloudFormation 鉤子實現的。如需詳細資訊，請參閱 控制項如何運作。
- landing zone 域：著陸區域是一種雲端環境，提供建議的起點，包括預設帳戶、帳戶結構、網路和安全性配置等。從 landing zone，您可以部署利用您的解決方案和應用程式的工作負載。
- 巢狀 OU：AWS Control Tower 中的巢狀 OU 是另一個 OU 中包含的 OU。巢狀 OU 只能有一個父 OU，而且每個帳戶只能是一個 OU 的成員。巢狀 OU 會建立階層。當您將原則附加至階層中的其中一個 OU 時，它會向下流動並影響其下的所有 OU 和帳戶。AWS Control Tower 中的巢狀 OU 階層最多可以有五個層級的深度。
- 父 OU：階層中目前 OU 正上方的 OU。每個 OU 只能有一個父 OU。
- 子系 OU：階層中目前 OU 之下的任何 OU。一個 OU 可以有許多子 OU。
- OU 階層：在 AWS Control Tower 中，巢狀 OU 的階層最多可有五個層級。巢狀的順序稱為「層級」。階層的頂端會指定為「層級 1」。
- 頂層 OU：頂層 OU 是直接位於根目錄下的任何 OU，而不是根本身。根目錄不被視為 OU。

定價

使用 AWS Control Tower 不會產生額外費用。您只需支付 AWS Control Tower 啟用的 AWS 服務，以及您在 landing zone 使用的服務付費。例如，您需要為使用 Account Factory 佈建帳戶以及在 landing zone 域中追蹤 AWS CloudTrail 的事件支付 Service Catalog 的費用。如需 AWS Control Tower 相關定價和費用的詳細資訊，請參閱 AWS Control Tower 定價。

如果您從 AWS Control Tower 中的帳戶執行臨時工作負載，您可能會看到與之相關的成本增加。 AWS Config如需詳細資訊，請參閱 AWS Config 定價。如需管理這些成本的詳細資訊，請連絡您的 AWS 客戶代表。要進一步了解如何使 AWS Config 用 AWS Control Tower，請參閱監視資源變更 AWS Config。

如果您在 AWS Control Tower 外部實作 AWS CloudTrail 追蹤，可以將它們與 AWS Control Tower 搭配使用。不過，如果您也選擇加入由 AWS Control Tower 管理的追蹤，則可能會產生重複費用。除非您有特定要求，否則我們不建議您設定外部軌跡。如果您選擇在 landing zone 設定或更新期間選擇加入，AWS Control Tower 會在管理帳戶中為您設定並啟用組織層級的 CloudTrail 追蹤。如需管理 CloudTrail 成本的相關資訊，請參閱管理 CloudTrail 成本。

設定

第一次使 AWS Control Tower 用前，請按照本節中的步驟建立 AWS 帳戶並保護您的 AWS Control Tower 管理帳戶。如需特別針對其他設定工作的資訊 AWS Control Tower，請參閱開始使用 AWS Control Tower。

註冊成為 AWS

當您註冊 Amazon Web Services (AWS) 時，您的 AWS 帳戶將自動註冊為中的所有服務 AWS，包括 AWS Control Tower. 如果您已經有 AWS 帳號，請跳至下一個工作。如果您沒有 AWS 帳戶，請使用下列步驟建立帳戶。

請記下您的 AWS 帳號，因為您需要它來執行其他任務。

註冊一個 AWS 帳戶

如果您沒有 AWS 帳戶，請完成以下步驟來建立一個。

若要註冊成為 AWS 帳戶

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

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

   當您註冊時 AWS 帳戶，會建立AWS 帳戶根使用者一個。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。安全性最佳做法是將管理存取權指派給使用者，並僅使用 root 使用者來執行需要 root 使用者存取權的工作。

AWS 註冊過程完成後，會向您發送確認電子郵件。您可以隨時登錄 https://aws.amazon.com/ 並選擇我的帳戶，以檢視您目前的帳戶活動並管理帳戶。

建立具有管理權限的使用者

註冊後，請保護 AWS 帳戶 AWS 帳戶根使用者、啟用和建立系統管理使用者 AWS IAM Identity Center，這樣您就不會將 root 使用者用於日常工作。

保護您的 AWS 帳戶根使用者

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

   如需使用根使用者登入的說明，請參閱 AWS 登入 使用者指南中的以根使用者身分登入。

2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

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

建立具有管理權限的使用者

1. 啟用 IAM Identity Center。

   如需指示，請參閱 AWS IAM Identity Center 使用者指南中的啟用 AWS IAM Identity Center。

2. 在 IAM 身分中心中，將管理存取權授予使用者。

   若要取得有關使用 IAM Identity Center 目錄 做為身分識別來源的自學課程，請參閱《使用指南》IAM Identity Center 目錄中的「以預設值設定使用AWS IAM Identity Center 者存取」。

以具有管理權限的使用者身分登入

- 若要使用您的 IAM Identity Center 使用者簽署，請使用建立 IAM Identity Center 使用者時傳送至您電子郵件地址的簽署 URL。

  如需使用 IAM 身分中心使用者登入的說明，請參閱使用AWS 登入 者指南中的登入 AWS 存取入口網站。

指派存取權給其他使用者

1. 在 IAM 身分中心中，建立遵循套用最低權限許可的最佳做法的權限集。

   如需指示，請參閱《AWS IAM Identity Center 使用指南》中的「建立權限集」。

2. 將使用者指派給群組，然後將單一登入存取權指派給群組。

   如需指示，請參閱《AWS IAM Identity Center 使用指南》中的「新增群組」。

帳戶的安全性

您可以在 AWS Organizations 文件中找到有關如何設定保護 AWS Control Tower 帳戶安全性的最佳做法的其他指引。

- 管理帳戶的最佳做法
- 會員帳戶的最佳做法

下一步驟

開始使用 AWS Control Tower

開始使用 AWS Control Tower

此入門程序適用於 AWS Control Tower 管理員。當您準備好使用 AWS Control 塔主控台或 API 設定 landing zone 時，請遵循此程序。

如果您目前是 AWS Control Tower 的新 AWS 客戶，您可能希望在繼續之前先檢閱名為規劃您的 AWS Control Tower landing zone的章節。

主題

AWS Control Tower 快速入門指南

如果您不是新手 AWS，可以按照本節中的步驟快速開始使用 AWS Control Tower。如果您想要立即自訂 AWS Control Tower 環境，請參閱 步驟 2. 設定並啟動您的 landing zone 。

> **Note**
>
> AWS Control Tower 設置了付費服務 AWS CloudTrail AWS Config，例如 CloudWatch，Amazon，Amazon S3 和 Amazon VPC。使用這些服務時，可能會產生費用，如定價頁面所示。 AWS 管理主控台會顯示任何付費服務的使用情況，以及產生的成本。AWS Control Tower 本身不會產生額外費用。

開始之前

在開始設定程序之前，最重要的決定是選擇您的居住地區。您的主地區 AWS 域是您執行大部分工作負載或儲存大部分資料的區域。在您設定 AWS Control Tower landing zone 之後，就無法變更它。如需如何選擇居住地區的詳細資訊，請參閱 landing zone 域設置的管理秘訣 。

> **Note**
>
> 根據預設，AWS Control Tower 會選擇帳戶目前所在的區域作為您的本地區域。您可以在 AWS 管理主控台畫面的右上角看到您目前的區域。

快速啟動程序假設您將接受 AWS Control Tower 環境中資源的預設值。這些選項中有許多可以稍後變更。名為的部分中列出了一些一次性的選擇 對 landing zone 配置的期望 。

如果您已建立新 AWS 帳戶，帳戶會自動符合設定 AWS Control Tower Tall 的必要條件。您可以繼續執行以下步驟。

快速啟動步驟

1. 使用您的系統 AWS 管理員使用者認證登入管理主控台。
2. 瀏覽至 AWS Control Tower 主控台主控台，網址為 https://console.aws.amazon.com/controltower。
3. 確認您是在您想要的居住地區工作。
4. 選擇 [設定 landing zone 域]。
5. 按照控制台中的說明進行操作，接受所有默認值。您需要輸入帳戶的電子郵件地址、記錄封存帳戶和稽核帳戶。
6. 確認您的選擇，然後選擇 [設定 landing zone]。
7. AWS Control Tower 大約需要 30 分鐘的時間來設定 landing zone 域中的所有資源。

如需如何設定 AWS Control Tower 的更詳細版本，包括自訂環境的方法，請閱讀並遵循接下來幾個主題中的程序。

> **Note**
>
> 如果您是初次使用的客戶，且遇到設定問題，請聯絡 Sup AWS port 部門以取得診斷協助。

先決條件：為您的管理帳戶自動化啟動前檢查

AWS Control Tower 設定 landing zone 之前，它會自動在您的帳戶中執行一系列啟動前檢查。對於這些檢查，您不需要採取任何動作，因此可確保您的管理帳戶已準備好應付建立 landing zone 域的變更。以下是 AWS Control Tower 在設定 landing zone 之前執行的檢查：

- 現有的服務限制 AWS 帳戶 必須足以啟動 AWS Control Tower。如需詳細資訊，請參閱 AWS Control Tower 的限制和配額。
- 必 AWS 帳戶 須訂閱以下 AWS 服務：
  - Amazon Simple Storage Service (Amazon S3)
  - Amazon Elastic Compute Cloud (Amazon EC2)
  - Amazon SNS
  - Amazon Virtual Private Cloud (Amazon VPC)
  - AWS CloudFormation
  - AWS CloudTrail
  - Amazon CloudWatch
  - AWS Config
  - AWS Identity and Access Management (IAM)
  - AWS Lambda

> **Note**
>
> 根據預設，所有帳戶都會訂閱這些服務。

AWS IAM Identity Center (IAM 身分中心) 客戶的注意事項

- 如果已設定 AWS IAM Identity Center (IAM 身分中心)，則 AWS Control Tower 的本地區域必須與 IAM 身分中心區域相同。
- IAM 身分中心只能安裝在組織的管理帳戶中。
- 根據您選擇的身分識別來源，將三個選項套用至 IAM 身分中心目錄：
  - IAM 身分中心使用者存放區：如果使用 IAM 身分中心設定 AWS Control Tower，則 AWS Control Tower 會在 IAM 身分中心目錄中建立群組，並為您選取的使用者為成員帳戶佈建這些群組的存取權限。
  - 作用中目錄：如果 AWS Control Tower 的 IAM 身分中心是透過使用中目錄設定的，則 AWS Control Tower 不會管理 IAM 身分中心目錄。它不會將使用者或群組指派給新 AWS 帳戶。
  - 外部身分供應商：如果 AWS Control 塔的 IAM 身分中心是透過外部身分供應商 (IdP) 設定的，則 AWS Control Tower 會在 IAM 身分中心目錄中建立群組，並為您為成員帳戶選取的使用者佈建這些群組的存取權限。您可以在帳戶建立期間從 Account Factory 的外部 IdP 指定現有使用者，而當該使用者在 IAM 身分中心和外部 IdP 之間同步處理相同名稱的使用者時，AWS Control Tower 可

讓此使用者存取新付款帳戶。您也可以在外部 IdP 中建立群組，以符合 AWS Control Tower 中預設群組的名稱。當您將使用者指派給這些群組時，這些使用者將擁有您註冊帳戶的存取權。

如需使用 IAM 身分中心和 AWS Control Tower 的詳細資訊，請參閱 IAM 身分中心帳戶和 AWS Control Tower 的注意事項

AWS Config 與 AWS CloudTrail 客戶的注意事項

- AWS 帳戶 無法在或的組織管理帳戶中啟用受信任的存 AWS Config 取 CloudTrail。如需如何停用受信任存取權的相關資訊，請參閱有關如何啟用或停用受信任存取的 AWS Organizations 文件。
- 如果您計劃在 AWS Control Tower 中註冊的任何現有帳戶中有現有的 AWS Config 記錄器、交付通道或彙總設定，則在設定 landing zone 之後，您必須在開始註冊帳戶之前修改或移除這些組態。此預先檢查不適用於 landing zone 啟動期間的 AWS Control Tower 管理帳戶。如需詳細資訊，請參閱註冊具有現有 AWS Config 資源的帳號。
- 如果您從 AWS Control Tower 的帳戶執行臨時工作負載，您可能會看到與 Config 相關的成本增加。AWS 如需管理這些成本的詳細資訊，請連絡您的 AWS 客戶代表。
- 當您在 AWS Control Tower 註冊帳戶時，您的帳戶受 AWS Control Tower 組織的 AWS CloudTrail 追蹤管理。如果帳戶中現有的 CloudTrail 追蹤部署，您可能會看到重複的費用，除非您在 AWS Control Tower 註冊帳戶之前刪除該帳戶的現有追蹤。如需組織層級追蹤和 AWS Control Tower 的相關資訊，請參閱。定價

> **Note**
>
> 啟動時，必須針對受 AWS Control Tower 管理的所有區域，在管理帳戶中啟用 AWS 安全性權杖服務 (STS) 端點。否則，啟動可能會在組態過程中途發生失敗。

從主控台開始使用 AWS Control Tower

此入門程序適用於 AWS Control Tower 管理員。當您準備好使用 AWS Control 塔主控台設定 landing zone 時，請遵循此程序。從開始到結束，大約需要半個小時。此程序需要一些先決條件和三個主要步驟。

如果您目前是 AWS Control Tower 的新 AWS 客戶，您可能希望在繼續之前先檢閱名為規劃您的 AWS Control Tower landing zone的章節。

主題

步驟 1：建立您的共用帳戶電子郵件地址

如果您要在新的 landing zone 中設定 AWS 帳戶，請參閱設定。

- 若要使用新的共用帳戶設定 landing zone，AWS Control Tower 需要兩個尚未與 AWS 帳戶. 這些電子郵件地址中的每一個都將作為共用電子郵件帳戶 (共用電子郵件帳戶) 提供給企業中將執行與 AWS Control Tower 相關的特定工作的各種使用者使用。
- 如果您是第一次設定 AWS Control Tower，而且要將現有的安全和日誌存檔帳戶導入 AWS Control Tower，則可以輸入現有 AWS 帳戶目前的電子郵件地址。

電子郵件地址是必需的：

- 稽核帳戶 — 此帳戶適用於需要存取 AWS Control Tower 提供之稽核資訊的使用者團隊。您也可以使用此帳戶做為第三方工具的存取點，執行環境的程式設計稽核，協助您針對合規稽核。
- 日誌封存帳戶 — 此帳戶適用於您的使用者團隊，他們需要存取 landing zone 中已註冊 OU 內所有註冊帳戶的所有記錄資訊。

當您建立 landing zone 時，這些帳戶會在安全性 OU 中設定。最佳做法是，建議您在這些帳戶中執行動作時，應使用具有適當範圍權限的 IAM Identity Center 使用者。

> **Note**
>
> 如果將現有 AWS 帳戶指定為稽核和日誌存檔帳戶，則現有帳戶必須通過一些啟動前檢查，以確保沒有資源與 AWS Control Tower 要求衝突。如果這些檢查不成功，您的 landing zone 設定可能無法成功。特別是，這些帳號不得有現有的 AWS Config 資源。如需詳細資訊，請參閱使用現有安全性或記錄帳戶的考量。

為了清楚起見，本用戶指南始終以其默認名稱提及共享帳戶：日誌存檔和審計。閱讀本文件時，如果您選擇自訂這些帳戶，請記得取代您最初提供給這些帳戶的自訂名稱。您可以在「帳戶詳細資訊」頁面上以其自訂名稱檢視您的帳戶。

> **Note**
>
> 我們正在變更有關某些 AWS Control Tower 組織單位 (OU) 的預設名稱的術語，以符合 AWS 多帳戶策略。當我們進行轉換以提高這些名稱的清晰度時，您可能會注意到一些不一致之處。安全性 OU 先前稱為核心 OU。沙箱 OU 先前稱為自訂 OU。

對 landing zone 配置的期望

設定 AWS Control Tower landing zone 的程序有多個步驟。AWS Control Tower landing zone 的某些方面是可設定的。其他選擇在設定後無法變更。

設定期間要設定的重要項目

- 您可以在設定期間選取頂層 OU 名稱，也可以在設定 landing zone 域後變更 OU 名稱。根據預設，最上層 OU 會命名為「安全性」和「沙箱」。如需詳細資訊，請參閱 建立架構良好環境的指引。
- 在設定期間，您可以為 AWS Control Tower 建立的共用帳戶選取自訂名稱，依預設稱為日誌存檔和稽核，但在設定之後無法變更這些名稱。（這是一次性的選擇。）
- 在設定期間，您可以選擇性地指定 AWS Control Tower 的現有 AWS 帳戶，以用作稽核和記錄存檔帳戶。如果您計劃指定現有 AWS 帳戶，而且這些帳戶有現有 AWS Config 資源，則必須先刪除現有 AWS Config 資源，然後才能將帳戶註冊到 AWS Control Tower。（這是一次性的選擇。）
- 如果您是第一次設定，或是要升級到 landing zone 3.0 版，您可以選擇是否允許 AWS Control Tower 為您的組織設定組織層級的 AWS CloudTrail 追蹤，或者您可以選擇退出由 AWS Control Tower 管理的追蹤並管理自己 CloudTrail 的軌跡。您可以在更新 landing zone 時選擇加入或退出由 AWS Control Tower 管理的組織層級追蹤。
- 您可以在設定或更新 landing zone 時，選擇性地為 Amazon S3 日誌儲存貯體和日誌存取儲存貯體設定自訂保留政策。
- 您可以選擇性地指定先前定義的藍圖，以便從 AWS Control Tower 主控台佈建自訂成員帳戶。如果您沒有可用的藍圖，您可以稍後自訂帳戶。請參閱使用 Account Factory 定制（AFC）自定義帳戶。

無法復原的組態選擇

- 設定 landing zone 後，就無法變更您的主地區域。
- 如果您使用 VPC 佈建帳 Account Factory 帳戶，則建立 VPC CIDR 後無法變更。

步驟 2. 設定並啟動您的 landing zone

在啟動 AWS Control Tower landing zone 域之前，請先確定最合適的本地區域。如需詳細資訊，請參閱 landing zone 域設置的管理秘訣 。

> **Important**
>
> 在部署 AWS Control Tower 登陸區域之後變更您的居住區域，需要停用以及 Sup AWS port 服務的協助。不建議使用這種做法。

瞭解如何使用 AWS CLI 中的設定和啟動 landing zone 使用 API 開始使用 AWS Control Tower。

若要在主機中設定並啟動您的 landing zone，請執行以下一系列步驟。

準備：導覽至 AWS Control Tower 主控台

1. 開啟網頁瀏覽器，然後瀏覽至 AWS Control Tower 主控台，網址為 https://console.aws.amazon.com/controltower。
2. 在主控台中，確認您是在想要的 AWS Control Tower Teck 主要區域工作。然後選擇「設定您的 landing zone」。

步驟二十一 查看並選擇您的 AWS 地區

請確定您已正確指定為您的居住 AWS 地區選取的地區。部署 AWS Control Tower 之後，就無法變更主區域。

在設定程序的這個區段中，您可以新增任何您需要的其他 AWS 區域。如有需要，您可以稍後新增更多區域，也可以從治理中移除區域。

若要選取要管理的其他 AWS 區域

1. 面板會顯示目前的「區域」選項。開啟下拉式功能表，查看可用於治理的其他區域清單。
2. 勾選每個區域旁邊的方塊，以透過 AWS Control Tower 進行管理。無法編輯您的居住地區選項。

拒絕存取特定區域

若要拒絕存取特定區 AWS 域中的 AWS 資源和工作負載，請在區域拒絕控制區段中選取已啟用。依預設，此控制項的設定為 [未啟用]。

步驟 2. 設定您的組織單位 (OU)

如果您接受這些 OU 的預設名稱，就不需要採取任何動作才能繼續安裝。若要變更 OU 的名稱，請直接在表單欄位中輸入新名稱。

- 基礎 OU — AWS Control Tower 仰賴最初命名為安全 OU 的基礎 OU。您可以在初始設定期間以及之後從 OU 詳細資料頁面變更此 OU 的名稱。此安全性 OU 包含您的兩個共用帳戶，依預設稱為記錄封存帳戶和稽核帳戶。
- 其他 OU — AWS Control Tower 可以為您設定一或多個其他 O U。除了安全性 OU 之外，我們建議您至少在 landing zone 域佈建一個其他 OU。如果此額外 OU 用於開發專案，建議您將其命名為沙箱 OU，如建立架構良好環境的指引. 如果 AWS Organizations 中已有現有的 OU，您可能會看到略過在 AWS Control Tower 中設定其他 OU 的選項。

步驟 2. 設定您的共用帳戶、記錄和加密

在設定程序的這個區段中，面板會顯示共用 AWS Control Tower 帳戶名稱的預設選項。這些帳戶是您 landing zone 的重要組成部分。請勿移動或刪除這些共用帳戶。您可以在設定期間為稽核和記錄封存帳戶選擇自訂名稱。或者，您可以單次選擇將現有 AWS 帳戶指定為共享帳戶。

您必須為記錄封存和稽核帳戶提供唯一的電子郵件地址，並且可以驗證先前為管理帳戶提供的電子郵件地址。選擇「編輯」按鈕以變更可編輯的預設值。

關於共享帳戶

- 管理帳戶 — AWS Control Tower 管理帳戶屬於根層級的一部分。管理帳戶允許 AWS Control Tower 計費。該帳戶也具有 landing zone 的管理員權限。您無法在 AWS Control Tower 中為帳單和管理員許可建立單獨的帳戶。

  在此設定階段期間，無法編輯管理帳戶顯示的電子郵件地址。它會顯示為確認訊息，因此您可以檢查您編輯的管理帳戶是否正確，以防您有多個帳戶。
- 兩個共享帳戶 — 您可以為這兩個帳戶選擇自定義名稱，也可以自帶帳戶，並且您必須為每個帳戶提供一個唯一的電子郵件地址，無論是新帳戶還是現有帳戶。如果您選擇讓 AWS Control Tower 為您建立新的共用帳戶，電子郵件地址必須尚未有關聯的 AWS 帳戶。

若要設定共用帳戶，請填寫要求的資訊。

1. 在主控台中，輸入最初稱為記錄封存帳戶的帳戶名稱。許多客戶決定保留此帳戶的預設名稱。
2. 為此帳戶提供唯一的電子郵件地址。

3. 輸入最初稱為稽核帳戶的帳戶名稱。許多客戶選擇將其稱為安全性帳戶。
4. 為此帳戶提供唯一的電子郵件地址。

選擇性設定記錄保留

在此設定階段，您可以針對 Amazon S3 儲存貯體自訂日誌保留政策，這些政策將 AWS CloudTrail 日誌存放在 AWS Control Tower 中，以天或年為增量，最長可達 15 年。如果您選擇不自訂記錄保留，則預設設定為標準帳戶記錄一年，存取記錄的預設設定為 10 年。當您更新或重設 landing zone 時，也可以使用此功能。

可選擇自行管理 AWS 帳戶 存取

您可以選擇 AWS Control Tower 是使用 AWS Identity and Access Management (IAM) 設定 AWS 帳戶存取權，還是要自行管理 AWS 帳戶 存取，可以透過 AWS IAM 身分中心使用者、角色和許可自行設定和自訂，或使用其他方法 (例如外部 IdP)，用於直接聯合帳戶或透過 IAM Identity Center 聯合到多個帳戶。您可以稍後變更此選項。

根據預設，AWS Control Tower 會為您的 landing zone 設定 AWS IAM 身分中心，並符合使用多個帳戶組織 AWS 環境中定義的最佳實務指導。大多數客戶會選擇預設值。為了符合特定產業或國家或地區的法規遵循，或在無法使用 AWS IAM Identity Center 的情 AWS 區域 況下，有時需要使用其他存取方法。

不支援在帳戶層級選取身分識別提供者。此選項僅適用於整個 landing zone 域。

如需詳細資訊，請參閱 IAM 身分識別中心指引。

選擇性設定 AWS CloudTrail 追蹤

最佳作法是建議您設定記錄。如果您希望允許 AWS Control Tower 設定組織層級的 CloudTrail 追蹤並為您管理，請選擇選擇加入。如果您想要使用自己的 CloudTrail 追蹤或第三方記錄工具來管理記錄，請選擇退出。請在主控台中確認您的選擇。當您更新 landing zone 域時，您可以變更您的選取項目，以及選擇加入或選擇退出組織層級的追蹤。

您可以隨時設置和管理自己的 CloudTrail 跟踪，包括組織級和帳戶級跟踪。如果您設定重複的 CloudTrail追蹤，可能會在記錄 CloudTrail 事件時產生重複的費用。

選擇性設定 AWS KMS keys

如果您想要使用加密金鑰 AWS KMS 加密和解密資源，請選取核取方塊。如果您有現有的金鑰，您可以從下拉式功能表中顯示的識別碼中選取它們。您可以選擇建立金鑰來產生新的金鑰。您可以隨時在更新 landing zone 域時新增或變更 KMS 金鑰。

選取 [設定 landing zone] 時，AWS Control Tower 會執行預先檢查以驗證您的 KMS 金鑰。金鑰必須符合下列要求：

- 已啟用
- 對稱
- 不是多區域金鑰
- 已將正確的權限新增至策略
- 關鍵在於管理賬戶

如果金鑰不符合這些需求，您可能會看到錯誤橫幅。在這種情況下，請選擇另一個金鑰或產生金鑰。請務必編輯金鑰的權限原則，如下一節所述。

更新 KMS 金鑰原則

您必須先建立 KMS 金鑰，才能更新 KMS 金鑰原則。如需詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的建立金鑰政策。

若要將 KMS 金鑰與 AWS Control Tower 搭配使用，您必須新增 AWS Config 和的最低必要許可，以更新預設 KMS 金鑰政策 AWS CloudTrail。最佳作法是建議您在任何原則中加入所需的最低權限。更新 KMS 金鑰原則時，您可以將權限新增為單一 JSON 陳述式中的群組，或逐行新增權限。

此程序說明如何透過新增允許 AWS Config 和用 AWS KMS 於加密的原則陳述式 CloudTrail 來更新 AWS KMS 主控台中的預設 KMS 金鑰原則。政策聲明要求您包括以下信息：

- **YOUR-MANAGEMENT-ACCOUNT-ID**— 將在其中設定 AWS Control Tower 的管理帳戶 ID。
- **YOUR-HOME-REGION**— 您在設定 AWS Control Tower 時選取的主區域。
- **YOUR-KMS-KEY-ID**— 將與原則搭配使用的 KMS 金鑰識別碼。

若要更新 KMS 金鑰原則

1. 開啟 AWS KMS 主控台的位置：https://console.aws.amazon.com/kms
2. 在瀏覽窗格中，選擇 [客戶管理的金鑰]。
3. 在表格中，選取您要編輯的機碼。
4. 在 [金鑰原則] 索引標籤中，確定您可以檢視金鑰原則。如果您無法檢視金鑰原則，請選擇 [切換到原則檢視]。
5. 選擇編輯，然後新增和的下列原則陳述式，以更新預設 KMS 金鑰原則 CloudTrail。 AWS Config

AWS Config 政策聲明

```
{
    "Sid": "Allow Config to use KMS for encryption",
    "Effect": "Allow",
    "Principal": {
        "Service": "config.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
    ],
    "Resource": "arn:aws:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-ID:key/YOUR-KMS-KEY-ID"
}
```

CloudTrail 政策聲明

```
{
    "Sid": "Allow CloudTrail to use KMS for encryption",
    "Effect": "Allow",
    "Principal": {
        "Service": "cloudtrail.amazonaws.com"
    },
    "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
    ],
    "Resource": "arn:aws:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-ID:key/YOUR-KMS-KEY-ID",
    "Condition": {
        "StringEquals": {
            "aws:SourceArn": "arn:aws:cloudtrail:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-ID:trail/aws-controltower-BaselineCloudTrail"
        },
        "StringLike": {
            "kms:EncryptionContext:aws:cloudtrail:arn": "arn:aws:cloudtrail:*:YOUR-MANAGEMENT-ACCOUNT-ID:trail/*"
        }
    }
}
```

6. 選擇儲存變更。

KMS 金鑰政策範例

下列範例原則顯示您新增授 AWS Config 與的原則陳述式以及最低必要權限後，KMS 金鑰原則 CloudTrail 的外觀。範例原則不包含您的預設 KMS 金鑰原則。

```
{
    "Version": "2012-10-17",
    "Id": "CustomKMSPolicy",
    "Statement": [
        {
        ... YOUR-EXISTING-POLICIES ...
        },
        {
            "Sid": "Allow Config to use KMS for encryption",
            "Effect": "Allow",
            "Principal": {
                "Service": "config.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-
ID:key/YOUR-KMS-KEY-ID"
        },
        {
            "Sid": "Allow CloudTrail to use KMS for encryption",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey*",
                "kms:Decrypt"
              ],
            "Resource": "arn:aws:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-
ID:key/YOUR-KMS-KEY-ID",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn": "arn:aws:cloudtrail:YOUR-HOME-REGION:YOUR-
MANAGEMENT-ACCOUNT-ID:trail/aws-controltower-BaselineCloudTrail"
```

```
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:aws:cloudtrail:*:YOUR-MANAGEMENT-ACCOUNT-ID:trail/*"
                }
            }
        }
    ]
}
```

若要檢視其他範例原則，請參閱下列頁面：

- 在AWS CloudTrail 使用者指南中授予加密權限。
- 開發人員指南中使用服務連結 RoleS3 儲存貯體傳遞時，KMS 金鑰的必要權限。AWS Config

> **防止攻擊者**
>
> 透過將某些條件新增至您的原則，您可以協助防止特定類型的攻擊 (稱為混淆的副攻擊)，如果實體強制授權較多的實體執行動作 (例如跨服務模擬)，就會發生這種攻擊。如需有關策略條件的一般資訊，另請參閱在政策中指定條件。

AWS Key Management Service (AWS KMS) 可讓您建立多區域 KMS 金鑰和非對稱金鑰；不過，AWS Control Tower 不支援多區域金鑰或非對稱金鑰。AWS Control Tower 會預先檢查您現有的金鑰。如果您選取多區域金鑰或非對稱金鑰，您可能會看到錯誤訊息。在這種情況下，請產生另一個金鑰以搭配 AWS Control Tower 資源使用。

如需詳細資訊 AWS KMS，請參閱AWS KMS 開發人員指南。

請注意，AWS Control Tower 中的客戶資料預設會使用 SSE-S3 加密。

選擇性地設定和建立自訂成員帳戶

當您按照建立帳戶工作流程新增成員帳戶時，可以選擇性地指定先前定義的藍圖，以便從 AWS Control Tower 主控台佈建自訂成員帳戶。如果您沒有可用的藍圖，您可以稍後自訂帳戶。請參閱使用 Account Factory 定制（AFC）自定義帳戶。

步驟 3。檢視和設定 landing zone

設定的下一節會顯示 AWS Control Tower 對您的 landing zone 域所需的許可。選擇核取方塊以展開每個主題。系統會要求您同意這些權限，這些權限可能會影響多個帳戶，並同意整體服務條款。

最終確定

1. 在主控台上，檢閱服務許可，當您準備就緒時，選擇 [我瞭解 AWS Control Tower 將用來代表我管理 AWS 資源和強制執行規則的許可]。
2. 若要完成選取並初始化啟動，請選擇「設定 landing zone 域」。

這一系列步驟會開始設定 landing zone 的程序，大約需要三十分鐘才能完成。在安裝期間，AWS Control Tower 會建立您的根層級、安全 OU 和共用帳戶。會建立、修改或刪除其他 AWS 資源。

> **確認 SNS 訂閱**
>
> 您為稽核帳戶提供的電子郵件地址將收到 AWS Control Tower 支援的每個 AWS 區域的AWS 通知 — 訂閱確認電子郵件。若要在稽核帳戶中接收合規電子郵件，您必須從 AWS Control Tower 支援的每個 AWS 區域中選擇每封電子郵件中的確認訂閱連結。

使用 API 開始使用 AWS Control Tower

此入門程序適用於 AWS Control Tower 管理員。此程序需要一些先決條件，並包括兩個主要步驟。

在此程序中，您將使用 AWS Control Tower 和其他 AWS 服務的 API 來設定和啟動 landing zone 域。這些 API 可讓您以程式設計方式建立 AWS Control 塔環境，透過 AWS CloudFormation 主控台或透過 AWS CLI.

啟動 AWS Control Tower landing zone 之前，請先執行下列先決條件任務：

- 確定最合適的家庭區域。如需詳細資訊，請參閱 landing zone 域設置的管理秘訣 。
- 檢閱 先決條件：為您的管理帳戶自動化啟動前檢查 以了解自動啟動前檢查，以確保您的管理帳戶已準備好進行建立您的 landing zone 的變更。

主題

- 使用 API 進行 landing zone 配置的期望

- 步驟 1：設定您的 landing zone
- 步驟 2：啟動您的 landing zone
- 識別您的 landing zone
- 更新您的 landing zone
- 重置 landing zone 以解決漂移
- 解除使用您的 landing zone
- 範例：僅使用 API 設定 AWS Control Tower landing zone
- 使用啟動 landing zone AWS CloudFormation

使用 API 進行 landing zone 配置的期望

設定 AWS Control Tower landing zone 的程序有多個步驟。AWS Control Tower landing zone 的某些方面是可設定的。其他選擇在設定後無法變更。

設定期間要設定的重要項目

- 您可以在設定期間選取基礎 OU 名稱，也可以在設定 landing zone 域後變更 OU 名稱。根據預設，基礎 OU 會命名為「安全性」和「沙箱」。如需詳細資訊，請參閱 建立架構良好環境的指引。
- 在設定期間，您可以為 AWS Control Tower 建立的共用帳戶選取自訂名稱，依預設稱為日誌存檔和稽核，但在設定之後無法變更這些名稱。（這是一次性的選擇。）
- 在使用 API 進行設定期間，您必須指定 AWS Control Tower 的現有 AWS 帳戶，以用作稽核和記錄存檔帳戶。若要指定現有 AWS 帳戶，如果這些帳戶具有現有 AWS Config 資源，您必須先刪除或修改現有 AWS Config 資源，然後才能將帳戶註冊到 AWS Control Tower。（這是一次性的選擇。）
- 如果您是第一次設定，或是要升級到 landing zone 3.0 版，您可以選擇是否允許 AWS Control Tower 為您的組織設定組織層級的 AWS CloudTrail 追蹤，或者您可以選擇退出由 AWS Control Tower 管理的追蹤並管理自己 CloudTrail 的軌跡。您可以在更新 landing zone 時選擇加入或退出由 AWS Control Tower 管理的組織層級追蹤。
- 您可以在設定或更新 landing zone 時，選擇性地為 Amazon S3 日誌儲存貯體和日誌存取儲存貯體設定自訂保留政策。

無法復原的組態選擇

- 設定 landing zone 後，就無法變更您的主地區域。
- 如果您使用 VPC 佈建帳戶，則建立 VPC CIDR 後無法變更它們。

接下來的章節將詳細說明設定先決條件和步驟，並提供說明和注意事項。如需其他程式碼範例，請參閱範例：僅使用 API 設定 AWS Control Tower landing zone。

步驟 1：設定您的 landing zone

設定 AWS Control Tower landing zone 的程序有多個步驟。AWS Control Tower landing zone 的某些方面是可設定的，但設定後無法變更其他選項。若要在啟動 landing zone 之前深入瞭解這些重要考量事項，請檢閱 對 landing zone 配置的期望 。

在使用 AWS Control Tower landing zone API 之前，您必須先從其他 AWS 服務呼叫 API 來設定 landing zone，然後再啟動。該過程包括三個主要步驟：

- 建立新 AWS Organizations 組織
- 設定您的共用帳戶電子郵件地址、
- 並建立具有呼叫 landing zone API 所需許可的 IAM 角色或 IAM 身分中心使用者。

步驟 1. 建立將包含您 landing zone 的組織：

1. 呼叫 AWS Organizations `CreateOrganization` API 並啟用所有功能以建立基礎 OU。AWS Control Tower 最初將此命名為安全 OU。此安全性 OU 包含您的兩個共用帳戶，依預設稱為記錄封存帳戶和稽核帳戶。

   ```
   aws organizations create-organization --feature-set ALL
   ```

   AWS Control Tower 可以設定一或多個其他 OU。除了安全性 OU 之外，我們建議您至少在 landing zone 域佈建一個其他 OU。如果此額外 OU 用於開發專案，我們建議您將其命名為沙箱 OU，如AWS 適用於 AWS Control Tower landing zone 的多帳戶策略.

步驟 2. 視需要佈建共用帳戶：

若要設定您的 landing zone，AWS Control Tower 需要兩個電子郵件地址。如果您是第一次使用 landing zone 域 API 設定 AWS Control Tower，則必須使用現有的安全性和日誌存檔 AWS 帳戶。您可以使用現有的當前電子郵件地址 AWS 帳戶。這些電子郵件地址中的每一個都將作為共用電子郵件帳戶 (共用電子郵件帳戶) 提供給企業中將執行與 AWS Control Tower 相關的特定工作的各種使用者使用。

若要開始設定新的 landing zone，如果您沒有現有 AWS 帳戶，您可以使用 AWS Organizations API 佈建安全性和記錄封存 AWS 帳戶。

1. 呼叫 AWS Organizations `CreateAccount` API，在安全性 OU 中建立記錄封存帳戶和稽核帳戶。

```
aws organizations create-account --email mylog@example.com --account-name "Logging
 Account"
```

```
aws organizations create-account --email mysecurity@example.com --account-name
 "Security Account"
```

2. (選擇性) 使用 AWS Organizations `DescribeAccount` API 檢查`CreateAccount`作業狀態。

步驟 3. 建立必要的服務角色

建立下列 IAM 服務角色，讓 AWS Control Tower 執行設定 landing zone 所需的 API 呼叫：

- AWSControlTowerAdmin
- AWSControlTowerCloudTrailRole
- AWSControlTowerStackSetRole
- AWSControlTowerConfigAggregatorRoleForOrganizations

如需這些角色及其原則的詳細資訊，請參閱針對 AWS Control Tower 使用身分型政策 (IAM 政策)。

若要建立 IAM 角色：

1. 建立具有必要權限的 IAM 角色，以呼叫所有 landing zone API。或者，您可以建立 IAM 身分中心使用者並指派必要的許可。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "controltower:CreateLandingZone",
                "controltower:UpdateLandingZone",
                "controltower:ResetLandingZone",
                "controltower:DeleteLandingZone",
                "controltower:GetLandingZoneOperation",
                "controltower:GetLandingZone",
                "controltower:ListLandingZones",
```

```
                "controltower:ListTagsForResource",
                "controltower:TagResource",
                "controltower:UntagResource",
                "servicecatalog:*",
                "organizations:*",
                "sso:*",
                "sso-directory:*",
                "logs:*",
                "cloudformation:*",
                "kms:*",
                "iam:GetRole",
                "iam:CreateRole",
                "iam:GetSAMLProvider",
                "iam:CreateSAMLProvider",
                "iam:CreateServiceLinkedRole",
                "iam:ListRolePolicies",
                "iam:PutRolePolicy",
                "iam:ListAttachedRolePolicies",
                "iam:AttachRolePolicy",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:DetachRolePolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

步驟 2：啟動您的 landing zone

AWS Control Tower `CreateLandingZone` API 需要 landing zone 版本和資訊清單檔案作為輸入參數。您可以使用資訊清單檔案來設定下列功能：

- 選擇性設定記錄保留
- 可選擇自行管理 AWS 帳戶 存取
- 選擇性設定 AWS CloudTrail 追蹤
- 選擇性設定 AWS KMS keys

編譯清單文件後，您就可以創建一個新的 landing zone。

> **Note**
>
> 使用 API 設定和啟動登陸區域時，AWS Control Tower 不支援區域拒絕控制。使用 API 成功啟動 landing zone 域後，您可以使用 AWS Control Tower 主控台設定區域拒絕控制。

1. 呼叫 AWS Control Tower `CreateLandingZone` API。此 API 需要 landing zone 版本和資訊清單檔案作為輸入。

```
aws controltower create-landing-zone --landing-zone-version 3.3 --manifest "file://
LandingZoneManifest.json"
```

示例 LandingZoneManifest.json 清單：

```
{
   "governedRegions": ["us-west-2","us-west-1"],
   "organizationStructure": {
       "security": {
           "name": "CORE"
       },
       "sandbox": {
           "name": "Sandbox"
       }
   },
   "centralizedLogging": {
        "accountId": "222222222222",
        "configurations": {
            "loggingBucket": {
                "retentionDays": 60
            },
            "accessLoggingBucket": {
                "retentionDays": 60
            },
            "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/
e84XXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXX"
        },
        "enabled": true
   },
   "securityRoles": {
        "accountId": "333333333333"
   },
```

```
   "accessManagement": {
        "enabled": true
   }
}
```

> **Note**
>
> 如範例所示 AccountId， CentralizedLogging 和 SecurityRoles 帳戶必須不同。

輸出：

```
{
   "arn": "arn:aws:controltower:us-west-2:123456789012:landingzone/1A2B3C4D5E6F7G8H",
   "operationIdentifier": "55XXXXXX-e2XX-41XX-a7XX-446XXXXXXXXX"
}
```

2. 呼叫 GetLandingZoneOperation API 以檢查CreateLandingZone作業狀態。GetLandingZoneOperationAPI 會傳回SUCCEEDED、FAILED或的狀態IN_PROGRESS。

```
aws controltower get-landing-zone-operation --operation-identifier "55XXXXXX-
eXXX-4XXX-aXXX-44XXXXXXXXXX"
```

輸出：

```
{
    "operationDetails": {
        "operationType": "CREATE",
        "startTime": "Thu Nov 09 20:39:19 UTC 2023",
        "endTime": "Thu Nov 09 21:02:01 UTC 2023",
        "status": "SUCCEEDED"
    }
}
```

3. 當狀態返回為時SUCCEEDED，您可以呼叫 GetLandingZone API 來檢閱 landing zone 設定。

```
aws controltower get-landing-zone --landing-zone-identifier "arn:aws:controltower:us-
west-2:123456789123:landingzone/1A2B3C4D5E6F7G8H"
```

輸出：

```
{
    "landingZone": {
        "arn": "arn:aws:controltower:us-
west-2:123456789012:landingzone/1A2B3C4D5E6F7G8H",
        "driftStatus": {
            "status": "IN_SYNC"
        },
        "latestAvailableVersion": "3.3",
        "manifest": {
            "accessManagement": {
                "enabled": true
            },
            "securityRoles": {
                "accountId": "333333333333"
            },
            "governedRegions": [
                "us-west-1",
                "eu-west-3",
                "us-west-2"
            ],
            "organizationStructure": {
                "sandbox": {
                    "name": "Sandbox"
                },
                "security": {
                    "name": "CORE"
                }
            },
            "centralizedLogging": {
                "accountId": "222222222222",
                "configurations": {
                    "loggingBucket": {
                        "retentionDays": 60
                    },
                    "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/
e84XXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXX",
                    "accessLoggingBucket": {
                        "retentionDays": 60
                    }
                },
                "enabled": true
            }
        },
```

```
        "status": "PROCESSING",
        "version": "3.3"
    }
}
```

識別您的 landing zone

通話ListLandingZones可協助您判斷帳戶是否已透過 AWS Control Tower 設定。此 API 會傳回跨任何商業區域的一個 landing zone 識別碼 (ARN)，不論著陸區域的本地區域為何。著陸區 ARN 在區域上是獨一無二的。

```
aws controltower list-landing-zones --region us-east-1
```

對於選擇加入區域，只有當您在與 *ListLandingZones* API 本地區域相同的區域中呼叫 API 時，API 才會傳回登陸區域識別碼。例如，如果您的 landing zone 設定在 af-south-1，而您在 af-south-1 ListLandingZones 中呼叫，則 API 會傳回 landing zone 域識別碼。如果您的 landing zone 設定在 af-south-1，而您呼叫 ListLandingZones ap-east-1，則 API 不會傳回 landing zone 域識別碼。

輸出：

```
{
   "landingZones" [
        "arn": "arn:aws:controltower:us-
west-2:123456789123:landingzone/1A2B3C4D5E6F7G8H"
   ]
}
```

更新您的 landing zone

當有新的登陸區域版本可用時，或要對 landing zone 設定進行其他更新時，您可以呼叫 UpdateLandingZone API 並參考更新的資訊清單檔案。此 API 會傳回0perationIdentifier，接著您可以在呼叫 GetLandingZone0peration API 以檢查更新作業的狀態時使用此 API。

更新 landing zone 域

1. 呼叫 AWS Control Tower UpdateLandingZone API，並參閱更新的 landing zone 域版本或更新的資訊清單。

```
aws controltower update-landing-zone --landing-zone-version 3.3 --landing-zone-
identifier "arn:aws:controltower:us-west-2:123456789123:landingzone/1A2B3C4D5E6F7G8H"
 --manifest file://LandingZoneManifest.json
```

LandingZoneManifest.json：

```
{
   "governedRegions": ["us-west-2","us-west-1"],
   "organizationStructure": {
       "security": {
           "name": "CORE"
       },
       "sandbox": {
           "name": "Sandbox"
       }
   },
   "centralizedLogging": {
        "accountId": "222222222222",
        "configurations": {
            "loggingBucket": {
                "retentionDays":2555
            },
            "accessLoggingBucket": {
                "retentionDays": 2555
            },
            "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/
e84XXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXX"
        },
        "enabled": true
   },
   "securityRoles": {
        "accountId": "333333333333"
   },
   "accessManagement": {
        "enabled": true
   }
}
```

輸出：

```
{
```

```
    "operationIdentifier": "55XXXXXX-e2XX-41XX-a7XX-446XXXXXXXXX"
}
```

> **選擇性地重新註冊 OU 以更新帳號**
>
> 對於帳戶少於 300 個帳戶的已註冊 AWS Control Tower OU，您可以使用 AWS Control Tower 主控台存取儀表板中的 OU 頁面，然後選取重新註冊 OU 以更新該 OU 中的帳戶。

重置 landing zone 以解決漂移

當您建立 landing zone 域時，landing zone 域及所有組織單位 (OU)、帳戶和資源都符合您選擇的控制項強制執行的治理規則。當您和您的組織成員使用 landing zone 時，此規範狀態可能會發生變更。這些變化稱為漂移。

若要識別您的 landing zone 域是否處於漂移狀態，您可以呼叫 `GetLandingZone` API。此 API 會傳回或的著陸區域漂移**`DRIFTED`**狀態`IN_SYNC`。

若要解決 landing zone 內的漂移問題，您可以使用 `ResetLandingZone` API 將 landing zone 重設回原始設定。例如，AWS Control Tower 預設情況下會啟用 IAM 身分中心來協助您管理 AWS 帳戶-，但是如果您在停用 IAM 身分中心的情況下設定原始 landing zone 參數，則呼叫會`ResetLandingZone`維護已停用的 IAM 身分中心組態。

如果您使用的是最新的 landing zone 版本，則只能使用 `ResetLandingZone` API。您可以呼叫 `GetLandingZone` API，並將您的 landing zone 版本與最新可用版本進行比較。如有必要，您可以 更新您的 landing zone 讓您的 landing zone 使用最新的可用版本。在這些示例中，我們使用 3.3 版作為最新版本。

1. 呼叫 `GetLandingZone` API。如果 API 傳回的漂移狀態`DRIFTED`，表示您的 landing zone 域處於漂移狀態。
2. 呼叫 `ResetLandingZone` API，將您的 landing zone 重設為原始設定。

```
aws controltower reset-landing-zone --landing-zone-identifier
 "arn:aws:controltower:us-west-2:123456789123:landingzone/1A2B3C4D5E6F7G8H"
```

輸出：

```
{
```

```
   "operationIdentifier": "55XXXXXX-e2XX-41XX-a7XX-446XXXXXXXXX"
}
```

> **Note**
>
> 重設 landing zone 域不會更新 landing zone 版本。檢閱有 更新您的 landing zone 關更新 landing zone 版本的詳細資訊。

解除使用您的 landing zone

清理所有 landing zone 資源的程序稱為解除使用著陸區。

> **Important**
>
> 強烈建議您只有在想要停止使用登陸區域時，才執行此解除委任程序。解除委任後，將無法重新建立現有的登陸區域。

如需停用 landing zone 的詳細資訊，包括 AWS Control Tower 如何處理您的資料和現有資料的重要資訊 AWS Organizations，請參閱逐步解說：解除委任 AWS Control Tower 登陸區。

若要解除使用 landing zone，請呼叫 `DeleteLandingZone` API。此 API 會傳回`OperationIdentifier`，接著您可以在呼叫 `GetLandingZoneOperation` API 以檢查刪除作業的狀態時使用該 API。

```
aws controltower delete-landing-zone --landing-zone-identifier
"arn:aws:controltower:us-west-2:123456789012:landingzone/1A2B3C4D5E6F7G8H"
```

輸出：

```
{
   "operationIdentifier": "55XXXXXX-e2XX-41XX-a7XX-446XXXXXXXXX"
}
```

範例：僅使用 API 設定 AWS Control Tower landing zone

此範例逐步解說是隨附文件。如需說明、注意事項和詳細資訊，請參閱使用 API 開始使用 AWS Control Tower。

先決條件

在建立 AWS Control Tower landing zone 之前，您必須建立一個組織、兩個共用帳戶和一些 IAM 角色。本逐步解說教學課程包含這些步驟，以及 CLI 指令和輸出範例。

步驟 1. 建立組織和兩個必要帳戶。

```
aws organizations create-organization --feature-set ALL
aws organizations create-account --email example+log@example.com --account-name "Log
 archive account"
aws organizations create-account --email example+aud@example.com --account-name "Audit
 account"
```

步驟 2. 建立必要的 IAM 角色。

AWSControlTowerAdmin

```
cat <<EOF >controltower_trust.json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "controltower.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
EOF
aws iam create-role --role-name AWSControlTowerAdmin --path /service-role/ --assume-
role-policy-document file://controltower_trust.json
cat <<EOF >ct_admin_role_policy.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeAvailabilityZones",
            "Resource": "*"
```

```
        }
    ]
}
EOF
aws iam put-role-policy --role-name AWSControlTowerAdmin --policy-name
 AWSControlTowerAdminPolicy --policy-document file://ct_admin_role_policy.json
aws iam attach-role-policy --role-name AWSControlTowerAdmin --policy-arn
 arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy
```

AWSControlTowerCloudTrailRole

```
cat <<EOF >controltower_trust.json
        {
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
EOF
aws iam create-role --role-name AWSControlTowerCloudTrailRole --path /service-role/ --
assume-role-policy-document file://cloudtrail_trust.json
cat <<EOF >cloudtrail_role_policy.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "logs:CreateLogStream",
            "Resource": "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
            "Effect": "Allow"
        },
        {
            "Action": "logs:PutLogEvents",
            "Resource": "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
            "Effect": "Allow"
        }
    ]
}
```

```
EOF
aws iam put-role-policy --role-name AWSControlTowerCloudTrailRole --
policy-name AWSControlTowerCloudTrailRolePolicy --policy-document file://
cloudtrail_role_policy.json
```

AWSControlTowerStackSetRole

```
cat <<EOF >cloudformation_trust.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudformation.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
EOF
aws iam create-role --role-name AWSControlTowerStackSetRole --path /service-role/ --
assume-role-policy-document file://cloudformation_trust.json
cat <<EOF >stackset_role_policy.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/AWSControlTowerExecution"
            ],
            "Effect": "Allow"
        }
    ]
}
EOF
aws iam put-role-policy --role-name AWSControlTowerStackSetRole --policy-name
 AWSControlTowerStackSetRolePolicy --policy-document file://stackset_role_policy.json
```

AWSControlTowerConfigAggregatorRoleForOrganizations

```
cat <<EOF >config_trust.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "config.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
EOF
aws iam create-role --role-name AWSControlTowerConfigAggregatorRoleForOrganizations --
path /service-role/ --assume-role-policy-document file://config_trust.json
aws iam attach-role-policy --role-name
 AWSControlTowerConfigAggregatorRoleForOrganizations --policy-arn
 arn:aws:iam::aws:policy/service-role/AWSConfigRoleForOrganizations
```

步驟 3. 取得帳號 ID 並產生 landing zone 清單檔案。

下列範例中的前兩個指令會將您在步驟 1 中建立之帳戶的帳戶 ID 儲存到變數中。然後，這些變數有助於產生 landing zone 域資訊清單檔案。

```
sec_account_id=$(aws organizations list-accounts | jq -r '.Accounts[] | select(.Name ==
 "Audit account") | .Id')
log_account_id=$(aws organizations list-accounts | jq -r '.Accounts[] | select(.Name ==
 "Log archive account") | .Id')

cat <<EOF >landing_zone_manifest.json
{
   "governedRegions": ["us-west-1", "us-west-2"],
   "organizationStructure": {
       "security": {
           "name": "Security"
       },
       "sandbox": {
           "name": "Sandbox"
       }
   },
   "centralizedLogging": {
        "accountId": "$log_account_id",
```

```
        "configurations": {
            "loggingBucket": {
                "retentionDays": 60
            },
            "accessLoggingBucket": {
                "retentionDays": 60
            }
        },
        "enabled": true
    },
    "securityRoles": {
         "accountId": "$sec_account_id"
    },
    "accessManagement": {
         "enabled": true
    }
}
EOF
```

步驟 4. 使用最新版本建立 landing zone 域。

您必須使用資訊清單檔案和最新版本來設定 landing zone。此範例顯示 3.3 版本。

```
aws --region us-west-1 controltower create-landing-zone --manifest file://
landing_zone_manifest.json --landing-zone-version 3.3
```

輸出將包含 arn 和作業識別碼，如下列範例所示。

```
{
    "arn": "arn:aws:controltower:us-west-1:0123456789012:landingzone/4B3H0ULNUOL2AXXX",
    "operationIdentifier": "16bb47f7-b7a2-4d90-bc71-7df4ca1201xx"
}
```

步驟 5. (可選) 追蹤 landing zone 建立作業的狀態。

要跟踪狀態，請使用上一個`create-landing-zone`命令輸出中的操作標識符。

```
aws --region us-west-1 controltower get-landing-zone-operation --operation-identifier
 16bb47f7-b7a2-4d90-bc71-7df4ca1201xx
```

樣本狀態輸出：

```
{
    "operationDetails": {
        "operationType": "CREATE",
        "startTime": "2024-02-28T21:49:31Z",
        "status": "IN_PROGRESS"
    }
}
```

您可以使用下列範例指令碼來協助您設定迴圈，該迴圈會一遍又一遍地回報作業的狀態，就像記錄檔一樣。然後，您無需繼續輸入命令。

```
while true; do echo "$(date) $(aws --region us-west-1 controltower get-landing-
zone-operation --operation-identifier 16bb47f7-b7a2-4d90-bc71-7df4ca1201xx | jq -
r .operationDetails.status)"; sleep 15; done
```

顯示有關 landing zone 域的詳細資訊

步驟 1. 找到 landing zone 域的 ARN

```
aws --region us-west-1 controltower list-landing-zones
```

輸出將包括 landing zone 域的標識符，如下面的輸出示例所示。

```
{
    "landingZones": [
        {
            "arn": "arn:aws:controltower:us-
west-1:123456789012:landingzone/4B3H0ULNUOL2AXXX"
        }
    ]
}
```

步驟 2. 獲取信息

```
aws --region us-west-1 controltower get-landing-zone --landing-zone-identifier
 arn:aws:controltower:us-west-1:123456789012:landingzone/4B3H0ULNUOL2AXXX
```

以下是您可能會看到的輸出類型的示例：

```
{
    "landingZone": {
```

```
        "arn": "arn:aws:controltower:us-
west-1:123456789012:landingzone/4B3H0ULNUOL2AXXX",
        "driftStatus": {
            "status": "IN_SYNC"
        },
        "latestAvailableVersion": "3.3",
        "manifest": {
            "accessManagement": {
                "enabled": true
            },
            "securityRoles": {
                "accountId": "9750XXXX4444"
            },
            "governedRegions": [
                "us-west-1",
                "us-west-2"
            ],
            "organizationStructure": {
                "sandbox": {
                    "name": "Sandbox"
                },
                "security": {
                    "name": "Security"
                }
            },
            "centralizedLogging": {
                "accountId": "012345678901",
                "configurations": {
                    "loggingBucket": {
                        "retentionDays": 60
                    },
                    "accessLoggingBucket": {
                        "retentionDays": 60
                    }
                },
                "enabled": true
            }
        },
        "status": "ACTIVE",
        "version": "3.3"
    }
}
```

使用啟動 landing zone AWS CloudFormation

您可以透過主控台 AWS CloudFormation 或透過 AWS CloudFormation 主控台來設定和啟動 landing zone 域 AWS CLI。本節提供透過使用 API 啟動 landing zone 的指示和範例 AWS CloudFormation。

主題

使用啟動 landing zone 的先決條件 AWS CloudFormation

1. 從中 AWS CLI，使用 AWS Organizations `CreateOrganization` API 建立組織並啟用所有功能。

   如需更詳細的指示，請檢閱 步驟 1：設定您的 landing zone 。
2. 從主 AWS CloudFormation 控台或使用部署 AWS CloudFormation 範本 AWS CLI，以在管理帳戶中建立下列資源：
   - 日誌存檔帳戶（有時稱為「日誌記錄」帳戶）
   - 審計帳戶（有時稱為「安全性」帳戶）
   - AWSControlTowerAdmin、AWSControlTowerCloudTrailRoleAWSControlTowerConfigAggregatorRoleF和AWSControlTowerStackSetRole服務角色。

     如需 AWS Control Tower 如何使用這些角色執行 landing zone API 呼叫的相關資訊，請參閱步驟 1：設定您的 landing zone。

```
Parameters:
  LoggingAccountEmail:
    Type: String
    Description: The email Id for centralized logging account
  LoggingAccountName:
    Type: String
    Description: Name for centralized logging account
  SecurityAccountEmail:
    Type: String
    Description: The email Id for security roles account
  SecurityAccountName:
    Type: String
    Description: Name for security roles account
```

```
Resources:
  MyOrganization:
    Type: 'AWS::Organizations::Organization'
    Properties:
      FeatureSet: ALL
  LoggingAccount:
    Type: 'AWS::Organizations::Account'
    Properties:
      AccountName: !Ref LoggingAccountName
      Email: !Ref LoggingAccountEmail
  SecurityAccount:
    Type: 'AWS::Organizations::Account'
    Properties:
      AccountName: !Ref SecurityAccountName
      Email: !Ref SecurityAccountEmail
  AWSControlTowerAdmin:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSControlTowerAdmin
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: controltower.amazonaws.com
            Action: 'sts:AssumeRole'
      Path: '/service-role/'
      ManagedPolicyArns:
        - !Sub >-
          arn:${AWS::Partition}:iam::aws:policy/service-role/
AWSControlTowerServiceRolePolicy
  AWSControlTowerAdminPolicy:
    Type: 'AWS::IAM::Policy'
    Properties:
      PolicyName: AWSControlTowerAdminPolicy
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Action: 'ec2:DescribeAvailabilityZones'
            Resource: '*'
      Roles:
        - !Ref AWSControlTowerAdmin
  AWSControlTowerCloudTrailRole:
```

```
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSControlTowerCloudTrailRole
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: cloudtrail.amazonaws.com
            Action: 'sts:AssumeRole'
      Path: '/service-role/'
  AWSControlTowerCloudTrailRolePolicy:
    Type: 'AWS::IAM::Policy'
    Properties:
      PolicyName: AWSControlTowerCloudTrailRolePolicy
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Action:
              - 'logs:CreateLogStream'
              - 'logs:PutLogEvents'
            Resource: !Sub >-
              arn:${AWS::Partition}:logs:*:*:log-group:aws-controltower/
CloudTrailLogs:*
            Effect: Allow
      Roles:
        - !Ref AWSControlTowerCloudTrailRole
  AWSControlTowerConfigAggregatorRoleForOrganizations:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSControlTowerConfigAggregatorRoleForOrganizations
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: config.amazonaws.com
            Action: 'sts:AssumeRole'
      Path: '/service-role/'
      ManagedPolicyArns:
        - !Sub arn:${AWS::Partition}:iam::aws:policy/service-role/
AWSConfigRoleForOrganizations
  AWSControlTowerStackSetRole:
    Type: 'AWS::IAM::Role'
```

```
    Properties:
      RoleName: AWSControlTowerStackSetRole
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: cloudformation.amazonaws.com
            Action: 'sts:AssumeRole'
      Path: '/service-role/'
  AWSControlTowerStackSetRolePolicy:
    Type: 'AWS::IAM::Policy'
    Properties:
      PolicyName: AWSControlTowerStackSetRolePolicy
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Action: 'sts:AssumeRole'
            Resource: !Sub 'arn:${AWS::Partition}:iam::*:role/
AWSControlTowerExecution'
            Effect: Allow
      Roles:
        - !Ref AWSControlTowerStackSetRole

Outputs:
  LogAccountId:
    Value:
      Fn::GetAtt: LoggingAccount.AccountId
    Export:
      Name: LogAccountId
  SecurityAccountId:
    Value:
      Fn::GetAtt: SecurityAccount.AccountId
    Export:
      Name: SecurityAccountId
```

使用以下方式建立新 landing zone AWS CloudFormation

從主 AWS CloudFormation 控台或使用 AWS CLI部署下列 AWS CloudFormation 範本以建立 landing zone 域。

```
Parameters:
```

```
  Version:
    Type: String
    Description: The version number of Landing Zone
  GovernedRegions:
    Type: List
    Description: List of governed regions
  SecurityOuName:
    Type: String
    Description: The security Organizational Unit name
  SandboxOuName:
    Type: String
    Description: The sandbox Organizational Unit name
  CentralizedLoggingAccountId:
    Type: String
    Description: The AWS account ID for centralized logging
  SecurityAccountId:
    Type: String
    Description: The AWS account ID for security roles
  LoggingBucketRetentionPeriod:
    Type: Number
    Description: Retention period for centralized logging bucket
  AccessLoggingBucketRetentionPeriod:
    Type: Number
    Description: Retention period for access logging bucket
  KMSKey:
    Type: String
    Description: KMS key ARN used by CloudTrail and Config service to encrypt data in
 logging bucket
Resources:
  MyLandingZone:
    Type: 'AWS::ControlTower::LandingZone'
    Properties:
      Version:
        Ref: Version
      Tags:
        - Key: "keyname1"
          Value: "value1"
        - Key: "keyname2"
          Value: "value2"
      Manifest:
        governedRegions:
          Ref: GovernedRegions
        organizationStructure:
          security:
```

```
        name:
          Ref: SecurityOuName
      sandbox:
        name:
          Ref: SandboxOuName
    centralizedLogging:
      accountId:
        Ref: CentralizedLoggingAccountId
      configurations:
        loggingBucket:
          retentionDays:
            Ref: LoggingBucketRetentionPeriod
        accessLoggingBucket:
          retentionDays:
            Ref: AccessLoggingBucketRetentionPeriod
        kmsKeyArn:
          Ref: KMSKey
      enabled: true
    securityRoles:
      accountId:
        Ref: SecurityAccountId
    accessManagement:
      enabled: true
```

使用管理現有的 landing zone 域 AWS CloudFormation

您可 AWS CloudFormation 以在新的或現有的 AWS CloudFormation 堆疊中匯入 landing zone 域，來管理已啟動的 landing zone 域。檢閱將現有資源引入 CloudFormation 管理層，以取得詳細資訊和指示

若要偵測並解決 landing zone 內的漂移問題，您可以使用 AWS Control Tower 主控台 AWS CLI、或 ResetLandingZoneAPI。

後續步驟

現在您的 landing zone 已經設定完畢，就可以使用了。

若要進一步了解如何使用 AWS Control Tower，請參閱下列主題：

- 如需建議的管理實務，請參閱最佳實務。
- 您可以設定具有特定角色和許可的 IAM 身分中心使用者和群組。如需建議，請參閱 設定群組、角色和原則的建議 。

- 若要開始從您的 AWS Organizations 部署註冊組織和帳戶，請參閱管理現有組織和帳戶。
- 您的使用者可以使用 Account Factory 在您的 landing zone 佈建自己 AWS 的帳戶。如需詳細資訊，請參閱 設定和佈建帳戶的權限。
- 為了確保AWS Control Tower 的合規驗證您的中央雲端系統管理員可以檢閱記錄封存帳戶中的記錄封存，而指定的協力廠商稽核人員可以檢閱稽核 (共用) 帳戶 (屬於安全性 OU 成員) 中的稽核資訊。
- 若要進一步了解 AWS Control Tower 的功能，請參閱相關資訊。
- 嘗試瀏覽精選 YouTube 影片清單，其中詳細說明如何使用 AWS Control Tower 功能。
- 您可能需要不時更新您的 landing zone 域，以取得最新的後端更新、最新的控制項，以及保留您的 landing zone 域 up-to-date。如需詳細資訊，請參閱 AWS Control Tower 中的組態更新管理。
- 如果您在使用 AWS Control Tower 時遇到問題，請參閱故障診斷。

> **Important**
>
> 如果您尚未為帳戶的 root 使用者啟用 MFA，請立即執行。如需 root 使用者最佳做法的詳細資訊，請參閱保護帳戶 root 使用者的最佳做法。

AWS Control Tower 的限制和配額

本章介紹使用 AWS Control Tower 時應記住的 AWS 服務限制和配額。如果因為服務配額問題而無法設定 landing zone，請聯絡AWS Support。

如需控制項特定限制的詳細資訊，請參閱控制限制。

> **新的控制項參考指南**
>
> AWS Control Tower 控制的相關資訊已移至 AWS Control Tower 控制參考指南。

AWS Control Tower 的限制

本節說明 AWS Control Tower 中的已知限制和不支援的使用案例。

- AWS Control Tower 有整體並行限制。一般而言，允許一次執行一項作業。允許使用此限制的兩個例外情況：
  - 可透過非同步程序同時啟動和停用選用控制項。無論是從控制台還是從 API 調用，一次最多可以進行一百（100）個與控制項相關的操作。在這 100 項作業中，一次最多 20 個可以是主動式控制作業。
  - 您可以透過非同步程序在 Account Factory 中同時佈建、更新和註冊帳戶，最多可同時進行五 (5) 個帳戶相關作業。取消管理帳戶必須一次執行一個帳戶。
- 您可以變更安全 OU 中共用帳戶的電子郵件地址，但您必須更新 landing zone，才能在 AWS Control Tower 主控台中查看這些變更。
- 每個 OU 只能有五 (5) 個 SCP 適用於 AWS Control Tower landing zone 中的 OU。
- AWS Control Tower 在您的登陸區域組織中最多支援 10,000 個帳戶，分為所有 OU。
- 擁有超過 300 個直接巢狀帳戶的現有 OU 無法在 AWS Control Tower 註冊或重新註冊。如需註冊 OU 之限制的詳細資訊，請參閱區域和堆疊集限制。
- AWS Control Tower (CFCT) 的自訂無法在下列項目中使用 AWS 區域，因為某些相依性無法使用：
  - 亞太區域 (雅加達和大阪)
  - 以色列 (特拉維夫)
  - 中東 (阿拉伯聯合大公國)
  - 歐洲 (西班牙)

  - 亞太區域 (海德拉巴)
  - 歐洲 (蘇黎世)
  - 加拿大西部 (卡加利)

  如果您將 CFCT 部署到 AWS Control Tower 本地區域，但無法在這些區域中建立 CFCT，則可以使用 CFCT 在這些區域部署和管理資源。
- 下列項目無法使用適用於 Terraform 的 AWS Control Tower Account Factory (AFT) AWS 區域，因為某些相依性無法使用：
  - 以色列 (特拉維夫)
  - 中東 (阿拉伯聯合大公國)
  - 歐洲 (西班牙)
  - 亞太區域 (海德拉巴)
  - 歐洲 (蘇黎世)
  - 加拿大西部 (卡加利)
- 下列區域不支援 IAM 身分中心。
  - 中東（阿拉伯聯合酋長國）區域，me-central-1
  - 亞太區域 (海德拉巴) 區域，ap-south-2
  - 加拿大西部 (卡加利), ca-west-1

  如需 IAM 身分中心 AWS 區域 和支援的詳細資訊，請參閱 Identity and Access Management 使用者指南中的區域和端點。AWS
- 下列區域不支援 AWS Service Catalog。
  - 加拿大西部 (卡加利), ca-west-1

  如需不支援的區域中 AWS Control Tower 功能的詳細資訊 AWS Service Catalog，請參閱AWS Control Tower 於 AWS 加拿大西部 (卡加立) 提供。
- 呼叫控制 API 以啟用或停用控制項時，AWS Control Tower 中的`EnableControl`和`DisableControl`更新限制為一百 (100) 個並行操作。可以同時進行十個作業 (10)，剩餘的作業會排入佇列。您可能需要調整代碼以等待完成。
- 在 100 個控制作業的整體限制內，一次最多 20 個作業可以是主動式控制作業。
- 當您透過 Account Factory 自訂 (AFC) 佈建帳戶時，使用以 Terraform 為基礎的藍圖，您只能將這些藍圖部署到一個藍圖。 AWS 區域根據預設，AWS Control Tower 會部署到主區域。

請求提高配額

Service Quotas 主控台提供有關 AWS Control Tower 配額的資訊。您可以使用「Service Quotas」主控台來檢視預設服務配額，或要求增加可調配額的配額。

您可以透過「Service Quotas」主控台檢視下列配額

- 並行科目作業配額：可同時執行的並行科目作業數目上限。預設值：5，最大值：10，可調
- 單一 OU 中的帳戶數目：一個 OU 中可存在的 AWS Control Tower 受管帳戶數目上限。如果您新增帳戶超出此限制，則無法在 AWS Control Tower 中執行 OU 註冊程序。若要進一步了解每個 OU 的帳戶數量，請參閱 區域和堆疊集限制 AWS Control Tower 文件。預設值：300，不可調整。
- 組織單位 (OU) 的並行作業：可同時執行的並行 OU 相關作業數目上限。預設值：1，不可調整。

例如，您可以要求將配額提高至十個並行帳戶相關作業中的五項。部分 AWS Control Tower 效能特性可能會在配額增加後變更。例如，當 OU 中有更多帳戶時，更新 OU 可能需要較長的時間。或者，在具有五個 SCP 的 OU 上完成動作可能需要比使用三個 SCP 更長的時間。

> **Note**
>
> 增加服務配額的要求最多可能需要兩天才能生效。請務必從 AWS Control Tower 的本地區域申請增加配額。

或者，您也可以聯絡 Sup AWS port，要求增加 AWS Control Tower 中某些資源的配額。或者，您可以觀看接下來的視頻，並了解如何自動增加某些服務配額。

影片：在與 AWS Control Tower 相關的服務中自動增加服務配額的請求

此影片 (7:24) 說明如何根據 AWS Control Tower 中的部署，自動增加相關整合 AWS 服務的服務配額。它也會顯示如何自動將新帳戶註冊到組織的 AWS 企業支援中。若要獲得更佳的觀賞效果，請選取影片右下角的圖示，將影片放大至全螢幕。並提供字幕。

AWS Control Tower 配額增加的影片逐步解說。

在此環境中佈建新帳戶時，您可以使用生命週期事件觸發指定中增加服務配額的自動要求 AWS 區域。

有關 AWS 配額的更多資訊，請參閱一AWS 般參考資料。

控制限制

> **新的控制項參考指南**
>
> AWS Control Tower 控制的相關資訊已移至 AWS Control Tower 控制參考指南。

如果您修改 AWS Control Tower 資源 (例如 SCP)，或移除任何 AWS Config 資源 (例如 Config 記錄器或彙總器)，AWS Control Tower 將無法再保證控制按設計運作。因此，您的多帳戶環境的安全性可能會受到影響。安全性的 AWS 共同責任模式適用於您可能進行的任何此類更改。

> **Note**
>
> AWS Control Tower 可在您更新 landing zone 時，將控制的 SCP 重設為其標準組態，以協助維護環境的完整性。根據設計，您可能對 SCP 所做的變更會被控制項的標準版本取代。

AWS Control Tall 中的某些控制不會 AWS 區域 在 AWS Control Tower 提供的某些地方運作，因為這些區域不支援所需的基礎功能。此限制會影響 Security Hub 服務管理標準：AWS Control Twer 中的特定偵探控制、特定主動控制以及特定控制。如需區域可用性的詳細資訊，請參閱區域服務清單文件和 Security Hub 控制項參考文件。

在混合治理的情況下，控制行為也會受到限制。如需詳細資訊，請參閱 設定區域時避免混合控管。

如需 AWS Control Tower 如何管理區域和控制限制的詳細資訊，請參閱啟用 AWS 選擇加入區域的注意事項。

您可以在 AWS Control 塔主控台中檢視每個控制項的區域。

下列 AWS 區域不支援屬於 Security Hub 服務管理標準的控制：AWS Control Tower。

- 亞太區域 (香港) 地區，ap-east-1
- 亞太 (雅加達) 地區，ap-southeast-3
- 亞太區域 (大阪) 地區 (ap-northeast-3
- 歐洲 (米蘭) 地區，eu-south-1
- 非洲（開普敦）地區，af-south-1
- 中東（巴林）區域，me-south-1

- 以色列（特拉維夫），il-central-1
- 中東（阿拉伯聯合酋長國）區域，me-central-1
- 歐洲 (西班牙) 地區，eu-south-2
- 亞太區域 (海德拉巴) 區域，ap-south-2
- 歐洲（蘇黎世）區域，eu-central-2
- 亞太區域 (墨爾本) 地區，ap-southeast-4
- 加拿大西部 (卡加利), ca-west-1

下列項目 AWS 區域 不支援主動式控制。

- 加拿大西部 (卡加利)

下表顯示某些不支援的主動式控制項 AWS 區域。

控制標識符	不支援地區
CT.REDSHIFT.PR.5	ap-southeast-4，方向 ap-south-2，ap-southeast-3，eu-central-2，eu-south-2，il-central-1，me-central-1
CT.DAX.PR.2	us-west-1
CT.GLUE.PR.2	不支援

下表顯示某些不支援的 AWS Control Tower 偵測控制 AWS 區域。

控制標識符	不支援地區
AWS-GR_AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED	ap-northeast-3, ap-southeast-3, il-central-1, ap-southeast-4, ca-west-1
AWS-GR_LAMBDA_FUNCTION_PUBLIC_ACCESS_PROHIBITED	eu-south-2
AWS-GR_EMR_MASTER_NO_PUBLIC_IP	ap-northeast-3，ap-southeast-3，遠南 -1，歐盟-南 -1，中央 -1，me-central-1 il-central-1，

控制標識符	不支援地區
	歐盟-南部 -2，歐盟-中央 -2，歐盟-東南 -2，ap-southeast-4，ca-west-1
AWS-GR_EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK	eu-south-2
AWS-GR_NO_UNRESTRICTED_ROUTE_TO_IGW	ap-northeast-3, ap-southeast-3, ap-south-2, eu-south-2, ca-west-1
AWS-GR_SAGEMAKER_NOTEBOOK_NO_DIRECT_INTERNET_ACCESS	ap-northeast-3，ap-southeast-3，遠南 -1，歐盟-南 -1，中央 -1，me-central-1 il-central-1，歐盟-南部 -2，歐盟-中央 -2，歐盟-東南 -2，ap-southeast-4，ca-west-1
AWS-GR_EC2_INSTANCE_NO_PUBLIC_IP	ap-northeast-3
AWS-GR_EKS_ENDPOINT_NO_PUBLIC_ACCESS	AP-東北 -3，AP-東南 -3，南方 -1，歐盟-南 -1，us-west-1，中央 -1，我中 me-central-1，歐盟南部 -2，歐盟 ap-south-2，eu-central-2，阿里-東南 -4，ca-west-1
AWS-GR_ELASTICSEARCH_IN_VPC_ONLY	ap-southeast-3，中央 -1，eu-south-2，公里 ap-south-2，eu-central-2，ap-southeast-4，ca-west-1
AWS-GR_RESTRICTED_SSH	自動對 af-south-1，ap-northeast-3，公里 ap-south-2，ap-southeast-3，ap-southeast-4，eu-central-2，歐盟-南 -1，eu-south-2，中央 -1，中央 -1，me-central-1
AWS-GR_DMS_REPLICATION_NOT_PUBLIC	自動對焦-南 -1，AP-南 -2，AP-東南-3，ap-southeast-4，eu-central-2，eu-south-1，eu-south-2，il-central-1，me-central-1，ca-west-1
AWS-GR_RDS_SNAPSHOTS_PUBLIC_PROHIBITED	自動對 af-south-1, ap-southeast-4, eu-central-2, 歐洲-南 -1, 歐南 -2, il-central-1

控制標識符	不支援地區
AWS-GR_SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED	ap-northeast-3
AWS-GR_ENCRYPTED_VOLUMES	自動對 af-south-1, 東北 -3, eu-south-1, il-central-1
AWS-GR_RESTRICTED_COMMON_PORTS	自動對 af-south-1，ap-northeast-3，eu-central-2，歐盟-南 -1，歐南 -2，il-central-1，me-central-1
AWS-GR_IAM_USER_MFA_ENABLED	中央 -1，me-central-1，eu-south-2，公里 ap-south-2，eu-central-2，ap-southeast-4，ca-west-1
AWS-GR_MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS	中央 -1，me-central-1，eu-south-2，公里 ap-south-2，eu-central-2，ap-southeast-4，ca-west-1
AWS-GR_SSM_DOCUMENT_NOT_PUBLIC	il-central-1，ca-west-1
AWS-GR_ROOT_ACCOUNT_MFA_ENABLED	il-central-1，me-central-1，ca-west-1
AWS-GR_S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS_PERIODIC	il-central-1，eu-south-2，eu-central-2
AWS-GR_RDS_STORAGE_ENCRYPTED	eu-central-2, eu-south-2
AWS-GR_RDS_INSTANCE_PUBLIC_ACCESS_CHECK	ap-south-2, eu-south-2
AWS-GR_REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK	ap-south-2, ap-southeast-3, eu-south-2, ca-west-1
AWS-GR_EC2_VOLUME_INUSE_CHECK	ca-west-1
AWS-GR_EBS_OPTIMIZED_INSTANCE	ca-west-1

區域和堆疊集限制

如果您打算將控管擴展到擁有大量帳戶的 OU AWS 區域，則可能會遇到 AWS CloudFormation 堆疊集對組織整體規模所建立的限制。您可以使用以下公式估計限制：

組織中受管理的帳號數目 x 受管理的區域數目 <= 150,000

一般而言，我們預期擴充控管至 OU 時，支援的帳戶數目會隨著管理的區域數目而減少。

如果您在將管理擴展到 OU 時啟動了超過 15 個可用 AWS Control Tower 的區域，則此限制就很明顯。減少每個組織單位 (OU) 的帳號數目上限。

例如，如果啟動了 22 個區域，則限制為每個 OU 220 個帳戶，而不是 300 個。如果您需要將控管擴展到擁有 220 個帳戶以上的 OU，則必須減少啟動區域的數量。這種減少是由於堆棧集限制。

指引：

- 擁有 15 個已啟動的區域，最多可支援 300 個帳戶的作業單位
- 擁有 22 個已啟用的區域，最多可支援 220 個帳戶的作業單位
- 啟用 16 至 21 個區域後，支援的 OU 大小上限在 220-300 個帳戶範圍內
- 在超過 23 個啟用區域的情況下，支援的 OU 大小上限少於 220 個帳戶

AWS Control Tower 功能的區域差異

AWS Control Tower 各地的行為存在某些差異 AWS 區域，因為 AWS Control Tower 協調了其他 AWS 服務的行為。例如：

- AWS Service Catalog 並非所有提供 AWS Control Tall 的 AWS 區域 地方均可使用，這會改變 Account Factory 在這些區域的行為。
- 在某些區域中，Account Factory 自訂 (AFC) 無法使用，因為 Service Catalog 無法支援藍圖的基礎功能。
- AWS 區域 由於缺乏基礎功能，某些控制項並不完全可用。
- AWS 區域 由於缺乏基礎功能，AFT 和 CFCT 並不完全可用。

為了確定 AWS Control Tower 環境的最佳行為，請確定您的居住區域。然後，評估下列項目。如需詳細資訊，請參閱 AWS Control Tower 中的限制和配額。

- 是否 AWS Service Catalog 適用於您想要的地區？

- 您需要的控制項是否可用？ 請參閱控制限制。
- IAM 身分中心是否可在您想要的本地區域使用？

新增：AWS Control Tower 控制參考指南

AWS Control Tower 中的控制相關資訊已移至新指南，即 AWS Control Tower 控制參考指南。

AWS Control Tower 管理員的最佳實務

本主題主要針對管理帳戶管理員。

管理帳戶管理員負責說明 AWS Control Tower 控制項阻止其成員帳戶管理員執行的一些任務。本主題說明傳輸這些知識的一些最佳實務和程序，並提供其他有效設定和維護 AWS Control Tower 環境的秘訣。

說明對使用者的存取

AWS Control 塔主控台僅適用於具有管理帳戶管理員許可的使用者。只有這些使用者可以在您的 landing zone 域內執行管理工作。根據最佳實務，這表示大多數使用者和成員帳戶管理員永遠不會看到 AWS Control Tower 主控台。身為管理帳戶管理員群組的成員，您有責任視情況向成員帳戶的使用者和管理員說明下列資訊。

- 說明使用者和系統管理員在 landing zone 域內可存取的 AWS 資源。
- 列出適用於每個組織單位 (OU) 的預防性控制項，以便其他管理員可以相應地規劃和執行其 AWS 工作負載。

說明資源存取

某些系統管理員和其他使用者可能需要解釋他們在您的 landing zone 域內可存取的 AWS 資源。此存取可以包括程式設計存取和以主控台為基礎的存取。一般來說，允許對 AWS 資源的讀取訪問和寫入訪問。若要在其中執行工作 AWS，您的使用者需要某種層級的存取權，才能存取他們執行工作所需的特定服務。

某些使用者 (例如您的 AWS 開發人員) 可能需要瞭解他們可存取的資源，以便建立工程解決方案。其他使用者 (例如在 AWS 服務上執行的應用程式的一般使用者) 不需要瞭解 landing zone 內的 AWS 資源。

AWS 提供識別使用者 AWS 資源存取範圍的工具。識別使用者存取的範圍之後，您可以根據組織的資訊管理政策，與使用者分享該資訊。如需這些工具的詳細資訊，請參閱下列連結。

- AWS 存取顧問 — AWS Identity and Access Management (IAM) 存取顧問工具可讓您透過分析 IAM 實體 (例如使用者、角色或群組) 呼叫 AWS 服務時的最後時間戳記，來判斷開發人員擁有的許可。您可以稽核服務存取和移除不必要的權限，而且可以視需要自動化程序。如需詳細資訊，請參閱我們的 AWS 安全部落格文章。

- IAM 政策模擬器 — 使用 IAM 政策模擬器，您可以測試和疑難排解基於 IAM 的政策和以資源為基礎的政策。如需詳細資訊，請參閱使用 IAM 政策模擬器測試 IAM 政策。
- AWS CloudTrail log — 您可以檢閱 AWS CloudTrail 防護記錄，以查看使用者、角色或所採取的動作 AWS 服務。若要取得有關的更多資訊 CloudTrail，請參閱AWS CloudTrail 使用者指南。

  AWS Control Tower landing zone 管理員所採取的動作可在 landing zone 管理帳戶中檢視。成員帳戶管理員和使用者所採取的動作可在共用記錄封存帳戶中檢視。

  您可以在活動頁面中檢視 AWS Control Tower 事件的摘要表。

解釋預防控制

預防性控制可確保您組織的帳戶符合您公司政策的規定。預防性控制的狀態可能是強制執行或未啟用。預防性控制可使用服務控制策略 (SCP) 來防止策略違規。相較之下，偵探控制項會透過定義的 AWS Config 規則，通知您各種事件或狀態存在。

您的某些使用者 (例如 AWS 開發人員) 可能需要瞭解適用於他們使用之任何帳戶和 OU 的預防性控制，以便他們能夠建立工程解決方案。以下程序根據貴組織的資訊管理政策，針對如何為適當的使用者提供此資訊，提供一些指導方針。

> **Note**
>
> 此程序假設您已在 landing zone 域內建立至少一個子 OU，以及至少一個 AWS IAM Identity Center 使用者。

為有需要了解的使用者顯示預防性控制

1. 登入 AWS Control Tower 主控台主控台，網址為 https://console.aws.amazon.com/controltower/。
2. 從左側導覽中選擇 [組織]。
3. 從表格中，選擇其中一個 OU 的名稱，您的使用者需要有關適用控制項的資訊。
4. 請記下 OU 的名稱，以及套用至此 OU 的控制項。
5. 對於使用者所需資訊的每個 OU 重複前兩個步驟。

如需控制及其功能的詳細資訊，請參閱關於 AWS Control Tower 中的控制。

規劃您的 AWS Control Tower landing zone

當您完成設定程序時，AWS Control Tower 會啟動與您帳戶相關聯的關鍵資源 (稱為 landing zone)，作為組織及其帳戶的住所。

> **Note**
>
> 每個組織可以有一個登陸區域。

如需有關規劃和設定 landing zone 域時應遵循的一些最佳作法的資訊，請參閱AWS 適用於 AWS Control Tower landing zone 的多帳戶策略。

設定 AWS Control Tower 的方法

您可以在現有組織中設定 AWS Control Tower landing zone，也可以先建立包含 AWS Control Tower landing zone 的新組織。

- 在現有組織中啟動 AWS Control Tower：本節適用於已 AWS Organizations 準備好透過 AWS Control Tower 進行管理的客戶。
- 在新組織中啟動 AWS Control Tower：此區段適用於沒有現有 AWS Organizations、OU 和帳戶的客戶。

> **Note**
>
> 如果您已經有 AWS Organizations landing zone 域，則可以將 AWS Control Tower 管理從現有的 landing zone 擴展到部分或全部現有 OU 和組織內的帳戶。請參閱管理現有組織和帳戶。

功能比較

以下是將 AWS Control Tower 新增至現有組織或將 AWS Control Tower 管理延伸至 OU 和帳戶之間的差異的簡短比較。此外，如果您要從 AWS 著陸區解決方案移至 AWS Control Tower，則需要一些特殊考量。

關於新增至現有組織：在現有組織中新增 AWS Control Tower 是您可以在主控 AWS 台中完成的工作。在這種情況下，您已經有一個在 AWS Organizations 服務中建立的組織，該組織目前尚未向 AWS Control Tower 註冊，而您之後想要新增 landing zone。

將 landing zone 新增至現有組織時，AWS Control Tower 會在 AWS Organizations 層級設定 parallel 結構。它不會變更現有組織內的 OU 和帳戶。

關於擴展管理：擴展管理適用於已向 AWS Control Tower 註冊的單一組織內的特定 OU 和帳戶，這表示該組織已經存在 landing zone 域。擴展管理意味著 AWS Control Tower 控制已擴展，以便其限制適用於該註冊組織內的特定 OU 和帳戶。在這種情況下，您不會啟動新的 landing zone，而只是擴充組織目前的 landing zone 域。

> **Important**
>
> 特別注意事項：如果您目前正在使用AWS 著陸區解決方案 (ALZ) AWS Organizations，請在嘗試在組織中啟用 AWS Control Tower 之前，先諮詢您的解 AWS 決方案架構師。AWS Control Tower 無法執行預先檢查，判斷 AWS Control Tower 是否會干擾您目前的 landing zone 部署。如需詳細資訊，請參閱 逐步解說：從 ALZ 移至 AWS Control Tower。此外，如需將帳戶從一個登陸區域移至另一個登陸區域的資訊，請參閱 如果帳戶不符合先決條件怎麼辦？

在現有組織中啟動 AWS Control Tower

透過在現有組織中設定 AWS Control Tower landing zone，您可以立即開始與現有 AWS Organizations 環境 parallel 工作。您在其中 AWS Organizations 建立的其他 OU 不會變更，因為它們並未在 AWS Control Tower 註冊。您可以繼續依現狀使用該些 OU 和帳戶。

AWS Control Tower 使用現有組織的管理帳戶作為其管理帳戶進行整合。不需要新的管理帳戶。您可以從現有的管理帳戶啟動 AWS Control Tower landing zone。

> **Note**
>
> 若要在現有組織上設定 AWS Control Tower，您的服務限制必須允許建立至少兩個額外帳戶。

將 AWS Control Tower 新增至現有組織的影響

AWS Control Tower 會在您的組織中建立兩個帳戶：稽核帳戶和記錄帳戶。這些帳戶會在您的團隊個別使用者帳戶中記錄您的團隊所採取的動作。稽核和日誌存檔帳戶會顯示在 AWS Control Tower landing zone 內的安全 OU 中。

當您設定 landing zone 域時，AWS Control Tower 新增的帳戶會成為現有帳戶的一部分 AWS Organizations，因此它們會成為現有組織帳單的一部分。

功能摘要

在現有 AWS Organizations 組織上啟用 AWS Control Tower 可為組織提供數個主要增強功能。

- 由於 AWS Control Tower 新增的帳戶將成為您現有組織的一部分，因此允許整個組織的整個帳戶進行統一計費。
- 它可讓您從 OU 中的一個管理帳戶管理所有帳戶。
- 它簡化了您對現有和新帳戶的應用和強制執行涵蓋安全性和合規性的控制方式。

> **Important**
>
> 在現有 AWS Organizations 組織中啟動 AWS Control Tower landing zone 無法讓您將 AWS Control Tower 管理從該組織延伸到其他 OU 或未在 AWS Control Tower 註冊的帳戶。

若要在現有組織中啟動 AWS Control Tower，請遵循中所述的程序開始使用 AWS Control Tower。

如需 AWS Control Tower 如何與現有 AWS Organizations 組織互動的詳細資訊，請參閱使用 AWS Control Tower 管理組織和帳戶。

在新組織中啟動 AWS Control Tower

如果您是 AWS Control Tower 的新手，但尚未使用 AWS Organizations，最好的開始就是閱讀我們的設定文件。

當您沒有設定組織時，AWS Control Tower 會自動為您設定組織。

AWS 適用於 AWS Control Tower landing zone 的多帳戶策略

AWS Control Tower 客戶經常會尋求有關如何設定 AWS 環境和帳戶的指導，以獲得最佳結果。AWS 建立了一組統一的建議 (稱為多帳戶策略)，以協助您充分利用 AWS 資源，包括 AWS Control Tower landing zone。

基本上，AWS Control Tower 可作為與其他 AWS 服務搭配使用的協調流程層，協助您實作 AWS 帳戶和. AWS AWS Organizations設定 landing zone 後，AWS Control Tower 會繼續協助您跨多個帳戶和工作負載維護公司政策和安全實務。

大多數著陸區隨著時間的推移發展 隨著 AWS Control Tower landing zone 中的組織單位 (OU) 和帳戶數量增加，您可以使用有效地組織工作負載的方式擴展 AWS Control Tower Town 部署。本章提供規

範指導，說明如何規劃和設定 AWS Control Tower landing zone，以配合 AWS 多帳戶策略，並隨著時間的推移進行擴充。

如需有關組織單位最佳作法的一般討論，請參閱使用的組織單位最佳做法 AWS Organizations。

AWS 多帳戶策略：最佳做法指南

AWS 架構良好的環境的最佳實務建議您將資源和工作負載分成多個 AWS 帳戶。您可以將 AWS 帳戶視為隔離的資源容器：它們提供工作負載分類，以及在出錯時減少爆炸半徑。

AWS 帳戶的定義

AWS 帳號充當資源容器和資源隔離邊界。

> **Note**
>
> AWS 帳戶與透過聯合或 AWS Identity and Access Management (IAM) 設定的使用者帳戶不同。

更多關於 AWS 帳戶

AWS 帳戶提供隔離資源並遏止 AWS 工作負載安全威脅的功能。帳戶還提供了一種計費機制，以及用於工作負載環境的控管。

AWS 帳戶是為工作負載提供資源容器的主要實作機制。如果您的環境架構良好，則可以有效管理多個 AWS 帳戶，因此可以管理多個工作負載和環境。

AWS Control Tower 設定了架構良好的環境。它依賴 AWS 帳戶以及可協助管理可跨多個帳戶延伸的環境變更。 AWS Organizations

一個結構良好的環境的定義

AWS 將架構良好的環境定義為以 landing zone 開始的環境。

AWS Control Tower 提供自動設定的 landing zone。它會強制執行控制，以確保您環境中的多個帳戶符合企業準則。

landing zone 的定義

landing zone 域是一種雲端環境，提供建議的起點，包括預設帳戶、帳戶結構、網路和安全性配置等。從 landing zone，您可以部署利用您的解決方案和應用程式的工作負載。

建立架構良好環境的指引

結構良好的環境的三個關鍵元件，在以下各節中說明：

- 多個 AWS 帳戶
- 多個組織單位 (OU)
- 精心規劃的結構

使用多個 AWS 帳戶

一個帳戶不足以設置一個架構良好的環境。通過使用多個帳戶，您可以最好地支持您的安全目標和業務流程。以下是使用多帳戶方法的一些好處：

- 安全性控制 — 應用程式具有不同的安全性設定檔，因此需要不同的控制原則和機制。例如，與稽核員交談並指向託管支付卡產業 (PCI) 工作負載的單一帳戶要容易得多。
- 隔離 — 帳戶是安全保護的一個單位。帳戶中可能包含潛在風險和安全威脅，而不會影響其他人。因此，安全性需求可能會要求您將帳戶彼此隔離。例如，您的團隊可能具有不同的安全性設定檔。
- 許多團隊 — 團隊有不同的職責和資源需求。通過設置多個帳戶，團隊不能互相干擾，因為他們可能在使用同一帳戶時。
- 資料隔離 — 將資料存放區隔離至帳戶，有助於限制可存取資料並可以管理資料存放區的人數。這種隔離有助於防止未經授權暴露高度私密的數據。例如，資料隔離有助於支援符合一般資料保護規範 (GDPR) 的規定。
- 業務流程 — 業務單位或產品通常具有完全不同的目的和流程。可以建立個人帳戶以滿足特定業務需求。
- 帳單 — 帳戶是在帳單層級分隔項目的唯一方法，包括轉移費用等項目。多帳戶策略有助於跨業務單位、功能團隊或個別使用者建立個別的可計費項目。
- AWS 配額分配 — 以每個帳戶為基礎設定配額。將工作負載分隔到不同的帳戶中，可為每個帳戶 (例如專案) 提供明確定義的個別配額。

使用多個組織單位

AWS Control Tower 和其他帳戶協調架構可以跨帳戶界限進行變更。因此，最 AWS 佳做法可解決跨帳戶的變更，這可能會破壞環境或破壞其安全性。在某些情況下，變更可能會影響整體環境，而不是政策。因此，我們建議您至少設定兩個強制性帳戶，即生產和預備帳戶。

此外，出於治理和控制目的， AWS 帳戶通常被分為組織單位（OU）。OU 是專為處理跨多個帳戶執行原則而設計的。

我們的建議是，您至少要使用不同的控制項和原則，建立與生產環境不同的生產前 (或預備) 環境。您可以將生產環境和預備環境建立為個別的 OU，並以個別帳戶計費。此外，您可能會想要設定用於程式碼測試的沙箱 OU。

在您的 landing zone 使用規劃良好的 OU 結構

AWS Control Tower 會自動為您設定部分 OU。隨著您的工作負載和需求隨著時間的推移而擴展，您可以擴展原始的 landing zone 配置以滿足您的需求。

> **Note**
>
> 範例中提供的名稱遵循建議的 AWS 命名慣例來設定多帳戶 AWS 環境。您可以在設定 landing zone 域後重新命名 OU，方法是選取 OU 詳細資料頁面上的 [編輯]。

建議

AWS Control Tower 為您設定第一個必要的 OU (安全 OU) 之後，我們建議您在 landing zone 建立一些額外的 OU。

建議您允許 AWS Control Tower 至少建立一個額外的 OU，稱為沙箱 OU。此 OU 適用於您的軟體開發環境。如果您選取了登陸區域，AWS Control Tower 可以在建立 landing zone 期間為您設定沙箱 OU。

您可以自行設定兩個建議的其他 OU：包含共用服務和網路帳戶的基礎結構 OU，以及用來包含生產工作負載的 OU (稱為工作負載 OU)。您可以透過組織單位頁面上的 AWS Control 塔主控台，在您的 landing zone 域新增其他 OU。

除了自動設定的 OU 之外，還建議使用

- 基礎結構 OU — 包含您的共用服務和網路帳戶。

> **Note**
>
> AWS Control Tower 不會為您設定基礎設施 OU。

- 沙箱 OU — 軟體開發 OU。例如，它可能有固定的支出限制，或者可能沒有連接到生產網絡。

> **Note**
>
> AWS Control Tower 建議您設定沙箱 OU，但這是選擇性的。它可以在配置 landing zone 域時自動進行設置。

- 工作負載 OU — 包含執行工作負載的帳戶。

> **Note**
>
> AWS Control Tower 不會為您設定工作負載 OU。

如需詳細資訊，請參閱使用 AWS Control Tower 的生產入門組織。

具有完整多帳戶 OU 結構的 AWS Control Tower 範例

AWS Control Tower 支援巢狀 OU 階層，這表示您可以建立符合組織需求的階層式 OU 結構。您可以建立 AWS Control Tower 環境，以符合 AWS 多帳戶策略指導。

您也可以建置一個更簡單、平整的 OU 結構，該結構的效能良好，並符合 AWS 多帳戶指引。僅僅因為您可以建置階層式 OU 結構，並不代表您必須這麼做。

- 若要檢視在具有 AWS 多帳戶指導的擴充扁平 AWS Control Tower 境中顯示 OU 範例集的圖表，請參閱範例：扁平 OU 結構中的工作負載。
- 如需 AWS Control Tower 如何與巢狀 OU 結構搭配使用的詳細資訊，請參閱AWS Control Tower 中的巢狀 OU。
- 如需 AWS Control Tower 如何與 AWS 指導一致的詳細資訊，請參閱使用多個帳戶組織 AWS 環境的 AWS 白 paper。

連結頁面上的圖表顯示已建立更多基礎 OU 和更多其他 OU。這些 OU 可滿足較大部署的額外需求。

在「基礎 OU」欄中，已將兩個 OU 新增至基本結構：

- Security_Prod OU — 提供安全性原則的唯讀區域，以及中斷安全性稽核區域。
- 基礎結構 OU — 您可能希望將先前建議的基礎結構 OU 分為兩個 OU：基礎結構 _Test (適用於生產前基礎結構) 和基礎結構 _Prod (適用於生產基礎結構)。

在「其他 OU」區域中，基本結構已新增多個 OU。以下是隨著環境成長而建立的下一個建議 OU：

- 工作負載 OU — 先前建議但選用的工作負載 OU 已分為兩個 OU：Workloads_Test (適用於生產前工作負載) 和 Workloads_Prod (適用於生產工作負載)。
- PolicyStaging OU — 可讓系統管理員先測試他們對控制項和原則的變更，然後再完全套用它們。
- 已暫停的 OU — 為可能已暫時停用的帳戶提供位置。

關於根

根目錄不是 OU。它是管理帳戶以及組織中所有 OU 和帳戶的容器。從概念上講，根包含所有 OU。無法將其刪除。您無法在 AWS Control Tower 內的根層級管理註冊帳戶。而是管理 OU 中的已註冊帳戶。如需有用的圖表，請參閱 AWS Organizations 文件。

landing zone 域設置的管理秘訣

- 您從事最多工作的 AWS 地區應該是您的家區域。
- 設定您的 landing zone 域，並從您的所在地區部署您的 Account Factory 帳戶。
- 如果您要在多個區 AWS 域進行投資，請確保您的雲端資源位於您將執行大部分雲端管理工作並執行工作負載的區域。
- 將工作負載和記錄保留在同一個 AWS 區域，可以降低跨區域移動和擷取記錄資訊所產生的相關成本。
- 稽核和其他 Amazon S3 儲存貯體是在您啟動 AWS Control Tower 的相同 AWS 區域中建立的。建議不要移動這些儲存貯體。
- 您可以在日誌存檔帳戶中創建自己的日誌存儲桶，但不建議這樣做。請務必保留 AWS Control Tower 建立的儲存貯體。
- 您的 Amazon S3 存取日誌必須與來源儲存貯體位於相同的 AWS 區域。
- 啟動時，必須針對 AWS Control Tower 支援的所有區域，在管理帳戶中啟用 AWS 安全性權杖服務 (STS) 端點。否則，啟動可能會在組態過程中途發生失敗。
- AWS Control Tower 僅支援已啟用控制的標記。如需詳細資訊，請參閱 AWS Control Tower 支援已啟用控制的標記。

- 我們建議您為 AWS Control Tower 管理的每個帳戶啟用多因素身份驗證 (MFA)。

關於 VPC 的注意事項

- AWS Control Tower 建立的 VPC 僅限 AWS 區域 於可使用 AWS Control Tower 的 VPC。在不支援的區域中執行工作負載的某些客戶可能想要停用使用您的 Account Factory 帳戶建立的 VPC。他們可能偏好使用 Service Catalog 產品組合建立新的 VPC，或建立僅在所需區域執行的自訂 VPC。
- AWS Control Tower 建立的 VPC 與為所有人建立的預設 VPC 不同。 AWS 帳戶在支援 AWS Control Tower 的區域中，AWS Control Tower 會在建立 AWS Control Tower VPC 時刪除預設 VPC。
- 如果您刪除本地 AWS 區中的預設 VPC，最好在所有其他區 AWS 域中將其刪除。

設定群組、角色和原則的建議

設定登陸區域時，建議您先決定好哪些使用者需要存取特定帳戶以及原因。例如，安全性帳戶應該只能由安全團隊存取，管理帳戶應該只能由雲端系統管理員的團隊存取，依此類推。

如需有關此主題的更多資訊，請參閱AWS Control Tower 中的身分和存取管理。

建議限制

您可以透過設定 IAM 角色或政策來限制組織的管理存取權限範圍，以僅允許管理員管理 AWS Control Tower 動作。建議的方法是使用 IAM 政策`arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy`。啟用`AWSControlTowerServiceRolePolicy`角色後，管理員只能管理 AWS Control Tower。請務必在每個帳戶中包含適當的存取權，以便 AWS Organizations 管理您的預防性控制項 AWS Config、SCP 以及管理偵探控制項的存取權。

當您在登錄區域中設定共用稽核帳戶時，建議您將 `AWSSecurityAuditors` 群組指派至帳戶的任何第三方稽核員。此群組會提供其成員唯讀權限。帳戶不得在正在稽核的環境中擁有寫入權限，因為這可能違反稽核員的責任分離規定。

您可以在角色信任政策中施加條件，以限制與 AWS Control Tower 中特定角色互動的帳戶和資源。強烈建議您限制`AWSControlTowerAdmin`角色的存取權，因為它允許廣泛的存取權限。如需詳細資訊，請參閱角色信任關係的選用條件。

建立和修改 AWS Control Tower 資源的指導

我們建議您在 AWS Control Tower 中建立和修改資源時採用下列最佳實務。這個指導可能會隨服務更新而變更。請記住，共同的責任模型適用於您的 AWS Control Tower 環境。

一般指導

- 請勿修改或刪除 AWS Control Tower 建立的任何資源，包括管理帳戶、共用帳戶和成員帳戶中的資源。如果您修改這些資源，您可能需要更新 landing zone 域或重新註冊 OU，而修改可能會導致不正確的合規性報告。

  尤其是：

  - 保持活動的 AWS Config 記錄器。如果您刪除 Config 記錄器，偵探控制項將無法偵測並報告漂移。由於資訊不足，可能會將不相容的資源報告為「符合標準」。
  - 請勿修改或刪除安全性組織單位 AWS Identity and Access Management (OU) 中共用帳戶中建立的 (IAM) 角色。修改這些角色可能需要更新您的登陸區域。
  - 請勿從您的成員帳戶中刪除`AWSControlTowerExecution`角色，即使是在未註冊的帳戶中也是如此。如果這樣做，您將無法在 AWS Control Tower 註冊這些帳戶，或註冊其直屬父 OU。
- 不要禁止 AWS 區域 通過 SCP 或 AWS Security Token Service （ ）使用任何內容。AWS STS這樣做會導致 AWS Control Tower 進入未定義的狀態。如果您不允許使用 [區域] AWS STS，您在這些區域中的功能將會失敗，因為在這些區域中無法使用驗證。相反地，請依靠 AWS Control Tower 區域拒絕功能 (如控制項所示)「AWS 根據要求 AWS 區域拒絕存取」(在 landing zone 層級運作)，或者控制區域拒絕控制套用至 OU (在 OU 層級運作以限制區域的存取)。
- 必須套用 AWS Organizations `FullAWSAccess` SCP，且不應與其他 SCP 合併。此 SCP 的變更不會報告為漂移；不過，如果拒絕存取某些資源，某些變更可能會以無法預測的方式影響 AWS Control Tower 功能。例如，如果 SCP 已分離或修改，則帳戶可能會失去對 CloudTrail 記錄器的存取權，或在記 AWS Config 錄時產生間隙。
- 請勿使用 AWS Organizations `DisableAWSServiceAccess` API 來關閉已設定 landing zone 之組織的 AWS Control Tower 服務存取權。如果您這樣做，某些 AWS Control Tower 漂移偵測功能可能無法正常運作，而且沒有來自的簡訊支援 AWS Organizations。這些漂移偵測功能有助於保證 AWS Control Tower 可以準確地報告組織單位、帳戶和控制項的合規狀態。如需詳細資訊，請參閱 AWS Organizations API 參考API_DisableAWSServiceAccess中的。
- 一般而言，AWS Control Tower 一次執行單一動作，必須先完成此動作，才能開始另一個動作。例如，如果您嘗試在啟用控制項的程序已經在作業中佈建帳戶，則帳號佈建將會失敗。

  例外狀況：

- AWS Control Tower 允許同時執行動作部署選用的控制項。如需詳細資訊，請參閱選用控制項的並行部署。
- AWS Control Tower 允許在 Account Factory 中同時建立、更新或註冊帳戶動作，最多可同時建立、更新或註冊動作。

> **Note**
>
> 如需 AWS Control Tower 建立之資源的詳細資訊，請參閱什麼是共享帳戶？。

有關帳戶和 OU 的提示

- 我們建議您將每個已註冊的 OU 保留為最多 300 個帳戶，以便在需要帳戶更新時 (例如當您設定新的區域進行管理時)，使用重新註冊 OU 功能更新這些帳戶。
- 為了減少註冊 OU 時所需的時間，我們建議您將每個 OU 的帳戶數目保持在 150 左右，即使每個 OU 的帳戶限制為 300 個。一般而言，註冊 OU 所需的時間會根據 OU 作業的區域數目而增加，乘以 OU 中的帳戶數目。
- 根據估計，擁有 150 個帳戶的 OU 需要大約 2 小時才能註冊和啟用控制項，而重新註冊則需要大約 1 小時。此外，具有許多控制項的 OU 註冊所花費的時間比具有少數控制項的 OU 更長的時間。
- 允許更長的時間範圍註冊 OU 的一個問題是，這個程序會封鎖其他動作。有些客戶願意允許更長的時間註冊或重新註冊 OU，因為他們希望在每個 OU 中允許更多帳戶。

何時以 root 使用者身分登入

特定管理工作需要您以根使用者的身分登入。您可以以 root 使用者身分登入 AWS Control Tower 中由帳戶工廠建立的帳戶工廠。 AWS 帳戶

您必須以根使用者的身分登入，才能執行下列動作：

- 變更特定帳戶設定，包括帳戶名稱、根使用者密碼或電子郵件地址。如需詳細資訊，請參閱 使用 AWS Control Tower 或使用更新和移動帳戶工廠帳戶 AWS Service Catalog。
- 若要關閉 AWS 帳戶.
- 如需需要 root 使用者登入認證之動作的詳細資訊，請參閱《AWS Account Management 參考指南》中的需要 root 使用者認證的工作。

> **Note**
>
> 若要變更或啟用 Sup AWS port 方案，您必須以 root 使用者身分登入，或是具有適當 IAM 許可的使用者。 。

以根使用者身分登入

1. 開啟AWS 登入頁面。

   如果您沒有需要存取的 AWS 帳戶 電子郵件地址，可以從 AWS Control Tower 取得該地址。開啟管理帳戶的主控台，選擇 [帳戶]，然後尋找電子郵件地址。
2. 輸入您需要存取的 AWS 帳戶 電子郵件地址，然後選擇 [下一步]。
3. 選擇 Forgot password? (忘記密碼？)，將密碼重設說明寄送至根使用者電子郵件地址。
4. 開啟來自根使用者信箱的密碼重設電子郵件訊息，然後依照說明重設您的密碼。
5. 開啟AWS 登入頁面，然後使用重設密碼登入。

AWS Organizations 指導

- 您可以在 AWS Organizations 文件中找到有關保護 AWS Control Tower 管理帳戶和成員帳戶安全性的最佳實務指導。
  - 管理帳戶的最佳做法
  - 會員帳戶的最佳做法
- 請勿用於更新連接 AWS Organizations 至 AWS Control Tower 註冊之 OU 的服務控制政策 (SCP)。這樣做可能會導致控制項進入未知的狀態，因此您必須重設 landing zone 或在 AWS Control Tower 中重新註冊 OU。相反地，您可以建立新的 SCP 並將這些 SCP 附加到 OU，而不必編輯 AWS Control Tower 建立的 SCP。
- 將已註冊的個人帳戶從已註冊的 OU 之外移至 AWS Control Tower，會導致必須解決的漂移問題。請參閱管控偏離的類型。
- 如果您使 AWS Organizations 用在 AWS Control Tower 註冊的組織內建立、邀請或移動帳戶，AWS Control Tower 不會註冊這些帳戶，而且不會記錄這些變更。如果您需要透過 SSO 存取這些帳戶，請參閱成員帳戶存取。
- 如果您使用將 OU 移 AWS Organizations 到 AWS Control Tower 建立的組織中，則外部 OU 不會由 AWS Control Tower 註冊。

- AWS Control Tower 處理權限篩選的方式與處理方式不 AWS Organizations 同。如果您的帳戶是透過 AWS Control Tower 帳戶工廠佈建的，最終使用者可以在 AWS Control Twer 主控台中看到所有 OU 的名稱和父母，即使他們沒有 AWS Organizations 直接擷取這些姓名和父母的權限。
- AWS Control Tower 不支援組織的混合許可，例如檢視 OU 父項的權限，但不支援檢視 OU 名稱的權限。基於這個原因，AWS Control Tower 管理員應具有完整許可。
- 必須套用 AWS Organizations `FullAWSAccess` SCP，且不應與其他 SCP 合併。此 SCP 的變更不會報告為漂移；不過，如果拒絕存取某些資源，某些變更可能會以無法預測的方式影響 AWS Control Tower 功能。例如，如果 SCP 已分離或修改，則帳戶可能會失去對 CloudTrail 記錄器的存取權，或在記 AWS Config 錄時產生間隙。
- 請勿使用 AWS Organizations `DisableAWSServiceAccess` API 來關閉已設定 landing zone 之組織的 AWS Control Tower 服務存取權。如果您這樣做，某些 AWS Control Tower 漂移偵測功能可能無法正常運作，而且沒有來自的簡訊支援 AWS Organizations。這些漂移偵測功能有助於保證 AWS Control Tower 可以準確地報告組織單位、帳戶和控制項的合規狀態。如需詳細資訊，請參閱 AWS Organizations API 參考API_DisableAWSServiceAccess中的。

IAM 身分識別中心指引

> **Note**
>
> SSO 是技術產業中用來表示單一登入的縮寫。一般而言，SSO 是工作階段和使用者驗證服務。它允許某人使用一組登錄憑據來訪問許多應用程序。提及中的單一登入功能時 AWS，我們指的是稱AWS Identity and Access Management為「IAM」或「IAM 身分中心」的 AWS 服務。

AWS Control Tower 建議您使用 AWS Identity and Access Management (IAM) 來規範對 AWS 帳戶. 不過，您可以選擇 AWS Control Tower 是否為您設定 IAM 身分中心、是否為自己設定 IAM 身分中心、以最有效的方式滿足您的業務需求，或是否選取其他帳戶存取方式。

根據預設，AWS Control Tower 會為您的 landing zone 設定 AWS IAM 身分中心，並符合使用多個帳戶組織 AWS 環境中定義的最佳實務指導。大多數客戶會選擇預設值。為了符合特定產業或國家或地區的法規遵循，或在無法使用 AWS IAM Identity Center 的情 AWS 區域 況下，有時需要使用其他存取方法。

選擇一個選項

在主控台中，您可以選擇在 landing zone 設定過程中自行管理 IAM 身分中心，而不是讓 AWS Control Tower 為您設定。稍後，您可以隨時選擇變更此選項，方法是修改 landing zone 域設定，並在 landing zone 設定頁面上更新您的 landing zone 域。

停止 AWS Control Tower 中的 AWS IAM 身分中心，或開始使用 AWS IAM 身分中心

1. 導覽至 landing zone 設定頁面
2. 選擇模型組態標籤
3. 然後選擇適當的選項按鈕，以變更 AWS IAM 身分中心的選擇。

選擇自行管理 AWS IAM 身分中心做為 IdP 後，AWS Control Tower 只會建立管理 AWS Control Tower 所需的角色和政策，例如`AWSControlTowerAdmin`和。`AWSControlTowerAdminPolicy`對於自我管理的登陸區域，AWS Control Tower 不再為客戶特定用途建立 IAM 角色和分組，而不是在 landing zone 域設定過程期間，也不會在帳戶 Account Factory 佈建帳戶期間建立 IAM 角色和分組。

> **Note**
>
> 如果您從 AWS Control 塔 landing zone 移除 AWS IAM 身分中心，則不會移除 AWS Control Tower 建立的使用者、群組和許可集。我們建議您移除這些資源。

擁有替代身分識別提供者 (IdPs) (例如 Azure AD、Ping 或 Okta) 的 Account Factory 客戶可依照 AWS IAM 身分中心程序連線至外部身分識別提供者並將其 IdP 上線。您可以隨時修改 landing zone 設定，讓 AWS Control Tower 產生您的分組和角色。

- 有關 AWS Control Tower 如何根據您的身分來源與 IAM 身分中心搭配使用的特定資訊，請參閱本使用者指南的入門頁面「啟動前檢查」一節中的 AWS IAM Identity Center 客戶考量。
- 如需 AWS Control Tower 行為如何與 IAM 身分中心和不同身分來源互動的詳細資訊，請參閱 IAM 身分中心使用者指南中的變更身分來源的注意事項。
- 使用 AWS IAM 身分中心和 AWS Control Tower如需使用 AWS Control Tower 和 IAM 身分中心的詳細資訊，請參閱。

Account Factory 指南

使用 Account Factory 在 AWS Control Tower 佈建新帳戶時可能會遇到問題。如需有關如何疑難排解這些問題的詳細資訊，請參閱 AWS Control Tower 使用者指南疑難排解一節新帳戶佈建失敗。

建議您建立聯合身分使用者或 IAM 角色，而不要建立 IAM 使用者。聯合身分使用者和 IAM 角色為您提供臨時登入資料。IAM 使用者擁有難以管理的長期登入資料。如需詳細資訊，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)。

在 Account Factory 佈建新帳戶或使用註冊帳戶功能 AWS Control Tower 時，如果您以 IAM 使用者或 IAM 身分中心使用者身分驗證，請確認您的使用者是否可存取您的 AWS Service Catalog 產品組合。否則，您可能會從 Service Catalog 收到錯誤訊息。如需詳細資訊，請參閱 找不到啟動路徑錯誤 AWS Control Tower 使用者指南的疑難排解一節。

> **Note**
>
> 一次最多可以佈建五個帳戶。

訂閱 SNS 主題的指引

- `aws-controltower-AllConfigNotifications`SNS 主題會接收由發佈的所有事件 AWS Config，包括合規通知和 Amazon CloudWatch 事件通知。例如，本主題會通知您是否發生了控制違規。它還提供了有關其他類型的事件的信息。從AWS Config設定此主題時發佈的內容，進一步了解這些內容。)
- `aws-controltower-BaselineCloudTrail`追蹤中的資料事件也設定為發佈至 `aws-controltower-AllConfigNotifications` SNS 主題。
- 若要接收詳細的合規性通知，建議您訂閱 `aws-controltower-AllConfigNotifications` SNS 主題。本主題彙總來自所有子帳戶的合規性通知。
- 若要接收漂移通知和其他通知以及合規性通知，但整體通知較少，我們建議您訂閱 `aws-controltower-AggregateSecurityNotifications` SNS 主題。
- 若要接收有關 AWS Control Tower Account Factory 的 Terraform (AFT) 錯誤通知，您可以訂閱名為的 SNS 主題 aft_failure_notifications，顯示在 AFT 儲存庫中。例如：

```
resource "aws_sns_topic" "aft_failure_notifications" {
    name = "aft-failure-notifications"
    kms_master_key_id = "alias/aws/sns"
}
```

- 所有 SNS 主題都會使用磁碟加密進行靜態加密。如需詳細資訊，請參閱資料加密。

如需 SNS 主題與符合性的詳細資訊，請參閱預防和通知。

KMS 金鑰的指引

AWS Control Tower 與 AWS Key Management Service (AWS KMS) 搭配使用。或者，如果您想要使用您管理的加密金鑰來加密和解密 AWS Control Tower 資源，您可以產生和設定 AWS KMS keys。您可以隨時在更新 landing zone 域時新增或變更 KMS 金鑰。最佳做法是，我們建議您使用自己的 KMS 金鑰，並不時變更它們。

AWS KMS 可讓您建立多區域 KMS 金鑰和非對稱金鑰。不過，AWS Control Tower 不支援多區域金鑰或非對稱金鑰。AWS Control Tower 會對您現有的金鑰執行預先檢查。如果您選取多區域金鑰或非對稱金鑰，您可能會看到錯誤訊息。在這種情況下，請產生另一個金鑰以搭配 AWS Control Tower 資源使用。

對於操作 AWS CloudHSM 叢集的客戶：建立與 CloudHSM 叢集關聯的自訂金鑰存放區。然後，您可以建立 KMS 金鑰，該金鑰位於您建立的 CloudHSM 自訂金鑰存放區中。您可以將此 KMS 金鑰新增至 AWS Control Tower。

您必須對 KMS 金鑰的許可政策進行特定更新，才能使其與 AWS Control Tower 搭配使用。如需詳細資訊，請參閱名為的章節更新 KMS 金鑰原則。

以 AI 為基礎的服務和 AWS Control Tower

您可以建立服務控制政策 (SCP)，讓您選擇不要將資料儲存在基於 AI 的服務上。 AWS這些 SCP 政策規定，以人工智慧為基礎的服務 (例如 Amazon Rekognition 或 Amazon CodeWhisperer) 無法存放和使用您的資料來改善其他人工智慧型服務。 AWS

這些 AI 退出 SCP 原則可套用至整個組織、OU 或特定帳戶。這些政策是全域生效的。您可以在 AWS Organizations 文件中的 AI 服務退出政策中找到有關這些政策的詳細資訊。

如需使用 AI 的 AWS 服務清單以及原則範例，請參閱使用AWS Organizations 者指南中的 AI 服務退出政策語法和範例。

AWS Control Tower 中的組態更新管理

您的中央雲端管理員團隊成員有責任保持 landing zone 域的最新狀態。更新您的 landing zone 可確保 AWS Control Tower 已修補和更新。此外，為了保護您的 landing zone 免受潛在的合規性問題影響，中央雲端管理員團隊的成員應該在偵測到並回報漂移問題後立即解決問題。

> **Note**
>
> AWS Control 塔主控台會指出您的 landing zone 域何時需要更新。如果您沒有看到更新選項，表示您的 landing zone 域已是最新狀態。

下表包含 AWS Control Tower landing zone 更新版本清單，以及每個版本說明的連結。

版本	版本日期	描述
3.3	12-12-2023	著陸區 3.3 版
3.2	6-09-2023	著陸區 3.2 版
3.1	2-09-2023	著陸區 3.1 版
3.0	7-26-2022	著陸區 3.0 版
2.9	4-22-2022	著陸區 2.9 版
2.8	2-10-2022	著陸區 2.8 版
2.7	4-8-2021	著陸區 2.7 版
2.6	12-29-2020	著陸區 2.6 版
2.5	11-18-2020	著陸區 2.5 版
2.4	無	無
2.3	3-5-2020	著陸區 2.3 版
2.2	11-13-19	登陸區 2.2 版

版本	版本日期	描述
2.1	6-24-19	登陸區 2.1 版

每次更新 landing zone 域時，您都有機會修改 landing zone 設定。

更新的好處

- 您可以變更您管理的區域
- 您可以變更記錄保留原則
- 您可以新增或移除區域拒絕控制
- 您可以套用 AWS KMS 加密金鑰
- 您可以啟用或停用組織層級追蹤 CloudTrail 。
- 您可以解決 landing zone 漂移

當您更新 landing zone 域時，您會自動收到 AWS Control Tower 的最新功能。在「landing zone 設定」頁面上檢視您目前的登陸區版本。

如果更新失敗，AWS Control Tower 不會復原為先前的 landing zone 版本。您可能會發現您的 landing zone 處於不確定狀態。如果是這樣，請聯繫 AWS 支持。如需疑難排解更新失敗的詳細資訊，請參閱無法更新著陸區。

當您更新 landing zone 域時，您有機會清除未使用的 AWS 身分識別中心 (之前稱為 AWS SSO) 對應。如需詳細資訊，請參閱欄位備註：在 AWS Control Tower 升級期間自動清除未使用的 IAM 身分中心對應。

> **更新和重設的先決條件 — 關閉請求者付費**
>
> 更新或重設 landing zone 之前，請確定日誌存檔帳戶的 Amazon S3 記錄儲存貯體未啟用請求者付費功能。您必須先關閉該功能，然後才能開始更新或重設程序。當 AWS Control Tower 設定您的記錄儲存貯體時，此功能不會啟用。因此，只有已經確實啟用要求者付費功能的客戶才能將其關閉。如需詳細資訊，請參閱 Amazon S3 儲存貯體政策 CloudTrail和使用請求者付費儲存貯體。

關於更新

需要更新才能糾正治理偏移，或移至新版本的 AWS Control Tower。若要執行 AWS Control Tower 的完整更新，您必須先更新 landing zone，然後個別更新註冊的帳戶。您可能需要在不同的時間執行三種類型的更新。

- 登陸區域更新：大多數情況下，這種類型的更新是在「landing zone 域設定」 頁面上選擇「更新」來執行。您可能需要執行 landing zone 域更新以解決特定類型的漂移問題，並且可以在必要時選擇「重設」。
- 一或多個個別帳戶的更新：如果相關資訊發生變更，或者發生某些類型的偏離，您必須更新帳戶。如果帳戶需要更新，帳戶的狀態會在 [帳戶] 頁面上顯示 [可用的更新]。

  若要更新單一帳戶，請切換作業選項至帳戶詳細資訊頁面，然後選取更新帳戶。您也可以透過手動程序、選擇重新註冊 OU 或使用自動指令碼方法來更新帳戶，如本頁稍後的章節所述。
- 完整更新：完整更新包括更新登陸區域，後續更新您註冊的 OU 中的所有註冊帳戶。新版 AWS Control Tower (例如 2.9、3.0 等) 需要完整更新。

> **Note**
>
> 完成 landing zone 域更新後，您無法復原更新或降級至舊版本。

更新您的登陸區域

更新 AWS Control Tower landing zone 最簡單的方法是透過登陸區域設定頁面，您可以在 AWS Control Tower 儀表板的左側導覽中選擇登陸區域設定來存取。

landing zone 設定頁面會顯示目前的登陸區域版本，並列出任何可用的更新版本。如果您需要更新版本，可以選擇 Update (更新) 按鈕。

> **Note**
>
> 或者，您可以手動更新登陸區域。無論是使用 Update (更新) 按鈕或手動處理，更新大約需要相同的時間。若只要手動更新登陸區域，請參閱以下步驟 1 和步驟 2。

手動更新

下列程序會引導您手動完成 AWS Control Tower 完整更新的步驟。若要更新個人帳戶，請參閱更新主控台中的帳戶。

若要手動更新您的 landing zone，每個 OU 使用任意數量的帳戶

1. 開啟網頁瀏覽器，然後瀏覽至 AWS Control Tower 主控台，網址為 https://console.aws.amazon.com/controltower/home/update。
2. 在精靈中檢閱資訊，然後選擇 Update (更新)。這會更新 landing zone 域的後端以及您的共享帳戶。此過程可能需要半小時以上的時間。
3. 更新您的成員帳戶 (包含超過 300 個帳戶的 OU 必須遵循此程序)。
4. 在左側導覽窗格中，選擇 [組織]。
5. 要更新每個帳戶，請按照中給出的步驟進行操作更新主控台中的帳戶。

> **選擇性地重新註冊 OU 以更新帳號**
>
> 對於擁有少於 300 個帳戶的已註冊 AWS Control Tower OU，您可以前往儀表板中的 OU 頁面，然後選取重新註冊 OU 以更新該 OU 中的帳戶。

通過重置和重新註冊解決漂移

當您和您的組織成員使用 landing zone 時，通常會發生漂移。

AWS Control Tower 中的漂移偵測是自動的。SCP 的自動掃描可協助您識別需要變更的資源，或必須進行設定更新才能解決偏移問題。

若要修復大多數類型的漂移，請在「著陸區設定」頁面上選擇「重設」。此外，您可以選擇重新註冊 OU 來解決某些類型的漂移問題。有關漂移類型以及如何解決它們的更多信息，請參閱管控偏離的類型和偵測並解決 AWS Control Tower 中的漂移。

角色漂移的一個特殊情況發生漂移分辨率。如果無法使用必要角色，主控台會顯示警告頁面以及如何還原角色的一些指示。在角色漂移解決之前，您的 landing zone 將無法使用。此漂移重置與完全 landing zone 域重置不同。如需詳細資訊，請參閱名為的章節中的不要刪除必要角色要立即解決的漂移類型。

⚠ 當您採取行動解決 landing zone 版本上的漂移問題時，有兩種行為可能。

- 如果您使用的是最新的登陸區域版本，當您選擇「重設」然後選擇「確認」時，漂移的 landing zone 域資源會重設為儲存的 AWS Control Tower 組態。landing zone 版本保持不變。
- 如果您不是使用最新版本，則必須選擇「更新」。landing zone 已升級至最新的 landing zone 版本。漂移已作為此過程的一部分解決。

使用自動化佈建和更新帳戶

您可以使用多種方法在 AWS Control Tower 中佈建或更新個別帳戶：

- 您可以使用適用於地形 (AFT) 的 AWS Control Tower Account Factory 佈建和自訂帳戶。如需詳細資訊，請參閱 適用於地形的 AWS Control Tower Account Factory (AFT) 概觀。
- 您可以使用 AWS Control Tower (CFCT) 的自訂更新帳戶。如需詳細資訊，請參閱 AWS Control Tower (CFCT) 的自訂項目概觀 。
- 指令碼自動化：如果您偏好使用 API 方法，可以使用 Service Catalog 的 API 架構 AWS CLI 來更新帳戶，並在批次程序中更新帳戶。您可以為每個帳戶呼叫 Service Catalog 的 `UpdateProvisionedProduct`API。您可以使用此 API，編寫指令碼來逐一更新帳戶。有關此方法的更多資訊，在新增區域進行治理時，請參閱部落格文章：在新 AWS 區域啟用護欄。

  您一次最多可以更新五 (5) 個帳戶。您必須等待至少一個帳戶更新成功，才能開始下一個帳戶更新。因此，如果您有很多帳戶，這個程序可能需要很長的時間，但並不複雜。如需有關此方法的詳細資訊，請參閱逐步解說：依 Service Catalog API 在 AWS Control Tower 中自動佈建帳戶。

ⓘ 影片演練

專影片演練為使用指令碼自動化帳戶佈建而設計，但這些步驟也適用於帳戶更新。使用 `UpdateProvisionedProduct` API 而不是 `ProvisionProduct` API。

指令碼自動化的進一步步驟是檢查 AWS Control Tower `UpdateLandingZone` 生命週期事件的成功狀態。使用它作為觸發器來開始更新個別帳戶，如影片中所述。生命週期事件標誌著一系列活動的完成，因此此事件的發生意味著 landing zone 域更新已完成。登陸區域更新必須先完成，才能開始更新帳戶。如需使用生命週期事件的詳細資訊，請參閱生命週期事件。

另請參閱：

- 使用 AWS CloudShell 來使用 AWS Control Tower.
- AWS Control Tower 中的自動化任務 .

AWS Control Tower 中的自動化任務

許多客戶偏好在 AWS Control Tower 中自動執行任務，例如帳戶佈建、控制指派和稽核。您可以通過呼叫以下方式設置這些自動操作：

- AWS Service Catalog API
- AWS Organizations API
- AWS Control Tower API
- 中央 AWS 指 CLI

此相關資訊頁面包含許多優秀技術部落格文章的連結，這些文章可協助您在 AWS Control Tower 中自動執行任務。以下各節提供此 AWS Control Tower 使用者指南中各區域的連結，可協助您自動執行任務。

自動化控制工作

您可以透過 AWS Control Tower API 自動執行與套用和移除控制相關的任務 (也稱為護欄)。如需詳細資訊，請參閱 AWS Control Tower API 參考。

有關如何使用 AWS Control Tower API 執行控制操作的詳細資訊，請參閱 AWS Control To wer 發布 API，以及針對組織單位預先定義的控制項的部落格文章。

自動化 landing zone 工作

AWS Control Tower landing zone API 可協助您自動化與 landing zone 相關的特定任務。如需詳細資訊，請參閱 AWS Control Tower API 參考。

自動化 OU 註冊

AWS Control Tower 基準 API 可協助您自動化特定任務，例如註冊 OU。如需詳細資訊，請參閱 AWS Control Tower API 參考。

自動關閉帳戶

您可以使用 AWS Organizations API 自動關閉 AWS Control Tower 成員帳戶。如需詳細資訊，請參閱透過以下方式關閉 AWS Control Tower 成員帳戶 AWS Organizations。

自動化帳戶佈建和更新

AWS Control Tower Account Factory 自訂 (AFC) 可協助您從 AWS Control Tower 主控台建立帳戶，並使用我們稱為藍圖的自訂 AWS CloudFormation 範本。此程序是自動化的，因為您可以在設定單一藍圖之後重複建立新帳戶並更新帳戶，而無需維護管道。

適用於 Terraform (AFT) 的 AWS Control Tower Account Factory 遵循 GitOps 模型，自動化 AWS Control Tower 中的帳戶佈建和帳戶更新程序。如需詳細資訊，請參閱 使用 AWS Control Tower Account Factory 為地形 (AFT) 佈建帳戶 。

AWS Control Tower (CFCT) 的自訂可協助您自訂 AWS Control Tower landing zone，並與 AWS 最佳實務保持一致。自訂是透過 AWS CloudFormation 範本和服務控制原則 (SCP) 來實作。如需詳細資訊，請參閱 AWS Control Tower (CFCT) 的自訂項目概觀 。

如需有關自動化帳戶佈建的詳細資訊和影片，請參閱逐步解說：AWS Control Tower 中的自動化帳戶佈建和使用 IAM 角色自動佈建。

另請參閱透過指令碼更新帳戶。

帳戶的程序化審計

如需有關以程式設計方式稽核帳戶的詳細資訊，請參閱 AWS Control Tower 稽核帳戶的程式設計角色和信任關係。

自動化其他工作

如需如何使用自動請求方法增加特定 AWS Control Tower 服務配額的相關資訊，請觀看此影片：自動增加服務限制。

如需涵蓋自動化與整合使用案例的技術部落格，請參閱自動化與整合。

有兩個開放原始碼範例可協 GitHub 助您處理與安全性相關的特定自動化工作。

- 名為 aws-control-tower-org-setup-sample 的範例顯示如何自動將稽核帳戶設定為安全性相關服務的委派系統管理員。
- 名為 aws-control-tower-account-setup-using-step-functions 示範如何在佈建和設定新帳戶時，使用 Step Functions 自動執行安全性最佳作法。此範例包括將主參與者新增至組織共用的產品組合，以及將整個 AWS Service Catalog 組織的 AWS IAM 身分中心群組自動關聯至新帳戶。同時也說明如何刪除每個區域中的預設 VPC。

AWS 安全參考架構包含自動化與 AWS Control Tower 相關任務的程式碼範例。如需詳細資訊，請參閱AWS 規定指引頁面和相關的 GitHub 存放庫。

如需將 AWS Control Tower 搭配 AWS CloudShell使用有助於在 AWS CLI 中工作的 AWS 服務的詳細資訊，請參閱AWS CloudShell 和 AWS CLI。

由於 AWS Control Tower 是的協調流程層 AWS Organizations，因此許多其他 AWS 服務都可以透過 API 和 AWS CLI 取得。如需詳細資訊，請參閱相關 AWS 服務。

使用 AWS CloudShell 來使用 AWS Control Tower

AWS CloudShell 是一項有助於在 AWS CLI 中工作的 AWS 服務-它是一種基於瀏覽器的預先驗證 shell，您可以直接從. AWS Management Console無需下載或安裝命令列工具。您可以從偏好的 AWS Control Tower 殼層 (Bash PowerShell 或 Z 殼層) 執行其他 AWS 服務的 AWS CLI 命令。

當您AWS CloudShell 從啟動時 AWS Management Console，您用來登入主控台的 AWS 認證可在新的 shell 工作階段中使用。當您與 AWS Control Tower 其他 AWS 服務互動時，您可以略過輸入設定認證，而您將使用預先安裝在 shell 運算環境中的 AWS CLI 版本 2。您已預先驗證。 AWS CloudShell

取得的 IAM 許可 AWS CloudShell

AWS Identity and Access Management 提供存取管理資源，讓管理員可以將權限授與 IAM 使用者和 IAM 身分中心使用者以供存取 AWS CloudShell。

系統管理員授與使用者存取權的最快方法是透過 AWS 受管理的原則。AWS 受管政策是由 AWS建立並管理的獨立政策。的下列 AWS 受管政策 CloudShell 可附加至 IAM 身分：

- `AWSCloudShellFullAccess`：授予使用權限 AWS CloudShell 以完全訪問所有功能。

如果您想要限制 IAM 使用者或 IAM Identity Center 使用者可以執行的動作範圍 AWS CloudShell，您可以建立使用`AWSCloudShellFullAccess`受管政策做為範本的自訂政策。如需有關限制中使用者可使用的動作的詳細資訊 CloudShell，請參閱《使用AWS CloudShell 者指南》中的「使用 IAM 政策管理 AWS CloudShell 存取和使用」。

> **Note**
>
> 您的 IAM 身分還需要授予撥打電話權限的政策 AWS Control Tower。如需詳細資訊，請參閱使用 AWS Control Tower 主控台所需的權限。

與 AWS Control Tower 使用互動 AWS CloudShell

AWS CloudShell 從啟動之後 AWS Management Console，您可以立即 AWS Control Tower 從指令行介面開始與互動。 AWS CLI 指令以中的標準方式運作 CloudShell。

> **Note**
>
> AWS CLI 在中使用時 AWS CloudShell，您無需下載或安裝任何其他資源。您已經在命令介面中進行驗證，因此在撥打電話之前不需要設定認證。

啟動 AWS CloudShell

- 從中 AWS Management Console，您可以選擇 CloudShell 導覽列上的下列可用選項來啟動：
  - 選擇圖 CloudShell 示。
  - 開始在搜索框中輸入「cloudshell」，然後選擇該 CloudShell選項。

  現在您已經開始 CloudShell，您可以輸入任何您需要使用的 AWS CLI 命令 AWS Control Tower。例如，您可以檢查您的 AWS Config 狀態。

用 AWS CloudShell 來協助設定 AWS Control Tower

執行這些程序之前，除非另有說明，否則您必須登入登陸區域中的主區域，而且您必須以 IAM Identity Center 使用者或 IAM 使用者身分登入，並且具有您 landing zone 域之管理帳戶的管理許可。 AWS Management Console

1. 在開始設定 AWS Control Tower landing zone 域之前，您可 AWS CloudShell 以在中使用 AWS Config CLI 命令來判斷組態記錄器和傳送通道的狀態的方法。

   檢查您的 AWS Config 狀態

   檢視命令：

   - `aws configservice describe-delivery-channels`
   - `aws configservice describe-delivery-channel-status`
   - `aws configservice describe-configuration-recorders`
   - `The normal response is something like "name": "default"`

2. 如果您在設定 AWS Control Tower landing zone 域之前需要刪除現有的 AWS Config 記錄器或傳送頻道，您可以輸入以下指令：

   管理您預先存 AWS Config 在的資源

   刪除命令：

   - `aws configservice stop-configuration-recorder --configuration-recorder-name NAME-FROM-DESCRIBE-OUTPUT`
   - `aws configservice delete-delivery-channel --delivery-channel-name NAME-FROM-DESCRIBE-OUTPUT`
   - `aws configservice delete-configuration-recorder --configuration-recorder-name NAME-FROM-DESCRIBE-OUTPUT`

   > **Important**
   >
   > 請勿刪除 AWS Config 的 AWS Control Tower 資源。遺失這些資源可能會導致 AWS Control Tower 進入不一致的狀態。

   如需詳細資訊，請參閱 AWS Config 文件

   - 管理組態記錄器 (AWS CLI)
   - 管理交付通路

3. 此範例顯示您輸入來啟用或停用受信任存取權的 AWS CLI 命令 AWS Organizations。 AWS CloudShell 因為 AWS Control Tower 您不需要啟用或禁用受信任的訪問 AWS Organizations，這只是一個例子。不過，如果您要在 AWS Control Tower中自動化或自訂動作，則可能需要啟用或停用其他 AWS 服務的受信任存取權。

   啟用或停用信任的服務存取

   - `aws organizations enable-aws-service-access`
   - `aws organizations disable-aws-service-access`

使用創建一個 Amazon S3 存儲桶 AWS CloudShell

在下列範例中，您可 AWS CloudShell 以使用建立 Amazon S3 儲存貯體，然後使用該PutObject方法將程式碼檔案新增為該儲存貯體中的物件。

1. 若要在指定的「區域」中建立值 AWS 區，請在指令列中輸入下列指 CloudShell 令：

```
aws s3api create-bucket --bucket insert-unique-bucket-name-here --region us-east-1
```

如果呼叫成功，命令列會顯示類似下列輸出的服務回應：

```
{
    "Location": "/insert-unique-bucket-name-here"
}
```

> **Note**
>
> 如果您不遵守命名值區的規則 (例如，僅使用小寫字母)，則會顯示下列錯誤：呼叫 CreateBucket 作業時發生錯誤 (InvalidBucketName)：指定的值區無效。

2. 要上傳文件並將其作為對象添加到剛創建的存儲桶中，請調用以下PutObject方法：

```
aws s3api put-object --bucket insert-unique-bucket-name-here --key add_prog --body
 add_prog.py
```

如果物件成功上傳到 Amazon S3 儲存貯體，命令列會顯示來自服務的回應，類似下列輸出：

```
{
           "ETag": "\"ab123c1:w:wad4a567d8bfd9a1234ebeea56\""}
```

ETag是已儲存物件的雜湊值。它可以用來檢查上傳到 Amazon S3 的物件的完整性。

建立 AWS Control Tower 資源 AWS CloudFormation

AWS Control Tower 與整合的服務可協助您建立資源模型並設定資 AWS 源 AWS CloudFormation，以減少建立和管理資源和基礎架構的時間。您可以建立描述您想要的所有 AWS 資源 (例如AWS::ControlTower::EnabledControl用於控制項) 的範本。 AWS CloudFormation 為您佈建和配置這些資源。

使用時 AWS CloudFormation，您可以重複使用範本，以一致且重複地設定 AWS Control Tower 資源。描述您的資源一次，然後在多個區域中一遍又一遍地佈建相同 AWS 帳戶 的資源。

AWS Control Tower 和 AWS CloudFormation 範本

若要佈建和設定 AWS Control Tower 與相關服務的資源，您必須瞭解AWS CloudFormation 範本。範本是以 JSON 或 YAML 格式化的文本檔案。這些範本說明您要在 AWS CloudFormation 堆疊中佈建的資源。如果您不熟悉 JSON 或 YAML，可以使用 AWS CloudFormation 設計師來協助您開始 AWS CloudFormation 使用範本。如需更多詳細資訊，請參閱 AWS CloudFormation 使用者指南 中的 什麼是 AWS CloudFormation 設計器？。

AWS Control Tower 支援在中建立 `AWS::ControlTower::EnabledControl` (控制資源)、`AWS::ControlTower::LandingZone` (著陸區域) 和 `AWS::ControlTower::EnabledBaseline` (基準線) AWS CloudFormation。如需詳細資訊，包括這些資源類型的 JSON 和 YAML 範本範例，請參閱AWS CloudFormation 使用者指南AWS Control Tower中的。

> **Note**
>
> 中的限制`EnableControl`與`DisableControl`更新 AWS Control Tower 為 100 個並行作業，其中最多 20 項與「主動式控制」相關的作業。

若要檢視 CLI 和主控台的一些 AWS Control Tower 範例，請參閱使用啟用控制項 AWS CloudFormation。

進一步了解 AWS CloudFormation

若要進一步了解 AWS CloudFormation，請參閱下列資源：

- AWS CloudFormation
- AWS CloudFormation 使用者指南
- AWS CloudFormation API 參考
- AWS CloudFormation 指令行介面使用者指南

自訂您的 AWS Control Tower landing zone

AWS Control Tower landing zone 域的某些方面可在主控台中進行設定，例如選擇區域和選用控制項。其他變更可能會在主控台外部進行，並具有自動化功能。

例如，您可以使用 AWS Control Tower 的自訂功能建立更廣泛的 landing zone 自訂功能，這是一種可與 AWS CloudFormation 範本搭配使用的 GitOps風格自訂架構和 AWS Control Tower 生命週期事件。

從 AWS Control Tower 主控台進行自訂

若要對您的 landing zone 進行這些自訂，請按照 AWS Control 塔主控台提供的步驟進行。

在設定期間選取自訂名稱

- 您可以在安裝期間選取頂層 OU 名稱。您可以隨時使用 AWS Organizations 主控台重新命名 OU，但是在中變更 OU 可 AWS Organizations 能會導致修復偏移。
- 您可以選取共用稽核和記錄封存帳戶的名稱，但在設定之後就無法變更名稱。（這是一次性的選擇。）

> **秘訣**
>
> 請記住，在中重新命名 OU AWS Organizations 並不會更新 Account Factory 中對應的佈建產品。若要自動更新佈建的產品 (並避免漂移)，您必須透過 AWS Control Tower Teck 執行 OU 操作，包括建立、刪除或重新註冊 OU。

選擇 AWS 地區

- 您可以選取要管理的特定區 AWS 域，以自訂您的登陸區域。按照 AWS Control Tower 主控台中的步驟操作。
- 您可以在更新 landing zone AWS 域時，選取和取消選取要控管的區域。
- 您可以將 [區域拒絕] 控制項設定為 [已啟用] 或 [未啟用]，並控制使用者對未受管理區 AWS 域中大部分 AWS 服務的存取。

如需 CcCT 具有部署限制之 AWS 區域 位置的相關資訊，請參閱控制限制。

透過新增選用控制項自訂

- 強烈建議您選擇性的控制功能是可選的，這表示您可以透過選擇啟用哪些控制來自訂 landing zone 的執法等級。依預設，不會啟用選擇性控制項。
- 選用的資料駐留控制項可讓您自訂儲存的區域，並允許存取資料。
- 整合式 Security Hub 標準的選用控制項可讓您掃描 AWS Control Tower 環境以檢查安全風險。
- 選用的主動式控制可讓您在佈建 AWS CloudFormation 資源之前檢查資源，以確保新資源符合您環境的控制目標。

自訂您的 AWS CloudTrail 路線

- 將 landing zone 域更新為 3.0 版或更新版本時，您可以選擇加入或選擇退出由 AWS Control Tower 管理的組織層級 CloudTrail 追蹤。您可以隨時更新 landing zone 域時變更此選項。AWS Control Tower 會在您的管理帳戶中建立組織層級的追蹤，該追蹤會根據您的選擇進入作用中或非作用中狀態。著陸區 3.0 不支援帳戶層級 CloudTrail 追蹤；不過，如果您需要這些追蹤，您可以設定和管理自己的追蹤。重複的軌跡可能會產生額外費用。

在控制台中創建自定義會員帳戶

- 您可以建立自訂的 AWS Control Tower 成員帳戶，也可以從 AWS Control Tower 台更新現有成員帳戶以新增自訂項目。如需詳細資訊，請參閱 使用 Account Factory 定制（AFC）自定義帳戶。

在 AWS Control Tower 主控台外部自動化自訂

某些自訂無法透過 AWS Control Tower 主控台使用，但可以透過其他方式實作。例如：

- 您可以使用 Terraform 的 Account Factory (AFT)，在佈建期間以 GitOps樣式工作流程自訂帳戶。

  AFT 與地形模塊一起部署，該模塊可在 AFT 存儲庫中使用。
- 您可以使用 AWS Control Tower (CFCT) 的自訂功能套件來自訂 AWS Control Tower landing zone，這是以 AWS CloudFormation 範本和服務控制政策 (SCP) 為基礎建置的功能套件。您可以將自訂範本和原則部署到組織內的個別帳戶和組織單位 (OU)。

  CcCT 的源代碼可在GitHub 存儲庫中找到。

AWS Control Tower (CFCT) 的自訂優勢

我們稱為 AWS Control Tower (CFCT) 的自訂功能套件可協助您為 landing zone 域建立比在 AWS Control Twer 主控台建立更廣泛的自訂項目。它提供了一種 GitOps風格的自動化過程。您可以重新塑造您的 landing zone 域，以滿足您的業務需求。

此infrastructure-as-code自訂程序將 AWS CloudFormation 範本與 AWS 服務控制政策 (SCP) 和 AWS Control Tower 生命週期事件整合在一起，讓您的資源部署與您的 landing zone 保持同步。例如，當您使用 Account Factory 建立新帳戶時，可以自動部署附加至該帳戶和 OU 的資源。

> **Note**
>
> 與 Account Factory 和 AFT 不同，CFCT 並非專門用於建立新帳戶，而是透過部署您指定的資源，在 landing zone 域中自訂帳戶和 OU。

優勢

- 擴展自訂且安全的 AWS 環境 — 您可以更快速地擴展多帳戶 AWS Control Tower 環境，並將 AWS 最佳實務納入可重複的自訂工作流程中。
- 實例化您的需求 — 您可以使用表達政策意圖的 AWS CloudFormation 範本和服務控制政策，根據您的業務需求自訂 AWS Control Tower landing zone。
- 使用 AWS Control Tower 生命週期事件進一步自動化 — 生命週期事件可讓您根據先前一系列事件的完成情況部署資源。您可以仰賴生命週期事件來協助您將資源自動部署到帳戶和 OU。
- 擴充您的網路架構 — 您可以部署自訂的網路架構，以改善和保護您的連線能力，例如傳輸閘道。

其他 CFCT 例子

- AWS 架構部落格文章：使用 Service Catalog 和 AWS Control Tower 自訂部署一致的 DNS，提供 AWS Control Tower (CFCT) 自訂項目的範例聯網使用案例。
- aws-samples儲存庫 GitHub 中提供了與 CFCT 和 Amazon GuardDuty 相關的特定範例。
- 有關 CFCT 的其他代碼示例可作為 AWS 安全參考架構的一部分，在aws-samples存儲庫中使用。這些範例中有許多在名為的目錄中包含範例`manifest.yaml`檔案`customizations_for_aws_control_tower`。

如需有關 AWS 安全性參考架構的詳細資訊，請參閱AWS 規定指引頁面。

AWS Control Tower (CFCT) 的自訂項目概觀

AWS Control Tower (CFCT) 的自訂可協助您自訂 AWS Control Tower landing zone，並與 AWS 最佳實務保持一致。自訂是透過 AWS CloudFormation 範本和服務控制原則 (SCP) 來實作。

此 CFCT 功能已與 AWS Control Tower 生命週期事件整合，因此您的資源部署與您的 landing zone 保持同步。例如，當透過帳號工廠建立新帳號時，會自動部署所有附加至該帳號的資源。您可以將自訂範本和原則部署到組織內的個別帳戶和組織單位 (OU)。

下列影片說明部署可擴充的 CcCT 管線和常見的 CcCT 自訂項目的最佳實務。

以下部分提供部署 AWS Control Tower (CFCT) 自訂的架構考量和組態步驟。它包含AWS CloudFormation範本的連結，可啟動、設定和執行必要的 AWS 服務，以符合安全性和可用性的 AWS 最佳作法。

本主題適用於具備 AWS 雲端架構實務經驗的 IT 基礎架構設計師和開發人員。

如需 AWS Control Tower (CFCT) 的最新更新和自訂變更的相關資訊，請參閱儲存庫中的變更日誌 .md 檔案。 GitHub

架構概觀

部署 CFCT 在 AWS 雲中構建以下環境。

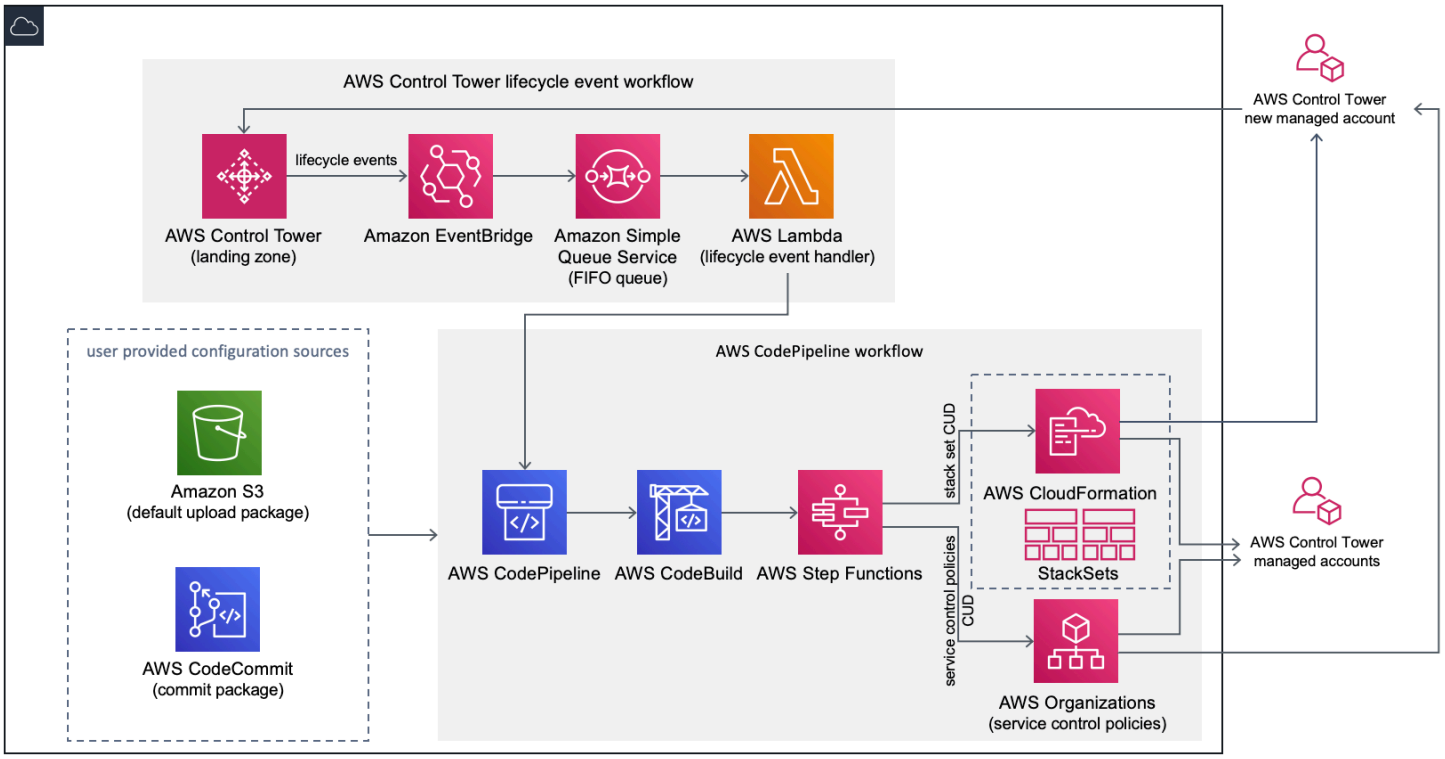


圖 1：AWS Control Tower 架構的自訂

CcCT 包含您在 AWS Control Tower 管理帳戶中部署的 AWS CloudFormation 範本。範本會啟動建立工作流程所需的所有元件，因此您可以自訂 AWS Control Tower landing zone。

> **注意**
>
> CFCT 必須部署在 AWS Control Tower 主區域和 AWS Control Tower 管理帳戶中，因為這是 AWS Control Tower landing zone 域的部署位置。如需設定 AWS Control Tower landing zone 的相關資訊，請參閱開始使用。

當您部署 CFCT 時，它會透過 Amazon 簡單儲存服務 (Amazon S3) 將自訂資源封裝並上傳到程式碼管道來源。上傳程序會自動叫用服務控制原則 (SCP) 狀態機器和狀AWS CloudFormation StackSets態機器，以在 OU 層級部署 SCP，或在 OU 或帳戶層級部署堆疊執行個體。

> **注意**
>
> 根據預設，CFCT 會建立 Amazon S3 儲存貯體來存放管道來源，但您可以將位置變更為AWS CodeCommit存放庫。如需詳細資訊，請參閱將 Amazon S3 設定為組態來源。

CcCT 部署了兩個工作流程：

- 一個AWS CodePipeline工作流
- 以及 AWS Control Tower 生命週期事件工作流程。

AWS CodePipeline 工作流程

AWS CodePipeline 工作流程可設定 AWS CodePipeline、AWS CodeBuild專案，並AWS Step Functions協調組織中 SCP AWS CloudFormation StackSets 和 SCP 的管理。

當您上傳組態套件時，CFCT 會叫用程式碼管線來執行三個階段。

- 建置階段 — 使用 AWS CodeBuild 驗證組態套件的內容。
- SCP 階段 — 叫用服務控制原則狀態機器，此機器會呼叫 AWS Organizations API 以建立 SCP。
- AWS St CloudFormation age — 叫用堆疊集狀態機器，以部署您在資訊清單檔案中提供的帳戶或 OU 清單中指定的資源。

在每個階段，程式碼管線都會叫用堆疊集和 SCP 步驟函式，這些函式會將自訂堆疊集和 SCP 部署到目標個別帳戶或整個組織單位。

> **注意**
>
> 如需有關自訂組態套件的詳細資訊，請參閱CFCT 定制指南。

AWS Control Tower 生命週期事件工作流程

在 AWS Control Tower 中建立新帳戶時，生命週期事件可以叫用 AWS CodePipeline 工作流程。您可以透過此工作流程自訂組態套件，該工作流程包含 Amazon EventBridge 事件規則、Amazon 簡單佇列服務 (Amazon SQS) 先進先出 (FIFO) 佇列和函數。AWS Lambda

當 Amazon EventBridge 事件規則偵測到相符的生命週期事件時，會將事件傳遞至 Amazon SQS FIFO 佇列、叫用 AWS Lambda 函數，然後叫用程式碼管道以執行堆疊集和 SCP 的下游部署。

費用

執行 CFCT 的成本取決於執行次數、 AWS CodePipeline 執行持續時間、 AWS Lambda 函數的數量和持續時間，以及發佈的 Amazon EventBridge 事件數量。 AWS CodeBuild 例如，如果您使用 build.general1.small 在一個月內執行 100 個組建，且每個組建執行 5 分鐘，則執行 CFCT 的大約費用為每月 3.00 美元。如需完整詳細資訊，您可以檢閱所執行之每項 AWS 服務的定價網頁。

刪除範本後，會保留 Amazon 簡易儲存服務 (Amazon S3) 儲存貯體和 AWS Git CodeCommit 型儲存庫資源，以保護您的組態資訊。根據您選取的選項，系統會根據 Amazon S3 儲存貯體中存放的資料量和 Git 請求數量 (不適用於 Amazon S3 資源) 向您收費。如需詳細資訊，請參閱 Amazon S3 和 AWS CodeCommit 定價。

組件服務

下列 AWS 服務是 AWS Control Tower (CFCT) 的自訂元件。

AWS CodeCommit

根據您對 AWS CloudFormation 範本的輸入，CFCT 可以使用 Amazon 簡單儲存服務一節中所述的相同範例組態來建立儲存AWS CodeCommit庫。

若要將 CFCT AWS CodeCommit 儲存庫複製到您的本機電腦，您必須建立可暫時存取儲存庫的認證，如《AWS CodeCommit 使用者指南》中所述。如需有關版本相容性的資訊，請參閱設定 AWS CodeCommit。

AWS CodePipeline

AWS CodePipeline 根據您將在預設 Amazon S3 儲存貯體或 AWS CodeCommit 儲存庫中進行的組態套件更新來驗證、測試和實作變更。如需將組態原始檔控制變更為的詳細資訊 AWS CodeCommit，請參閱使用 Amazon S3 做為組態來源。管道包括驗證和管理組態檔案和範本、核心帳戶、 AWS Organizations 服務控制政策和的階段 AWS CloudFormation StackSets。如需管線階段的詳細資訊，請參閱 CFCT 定制指南

AWS Key Management Service

CcCT 會建立 AWS Key Management Service(AWS KMS) `CustomControlTowerKMSKey` 加密金鑰。此金鑰可用來加密 Amazon S3 組態儲存貯體、Amazon SQS 佇列中的物件，以及 AWS Systems Manager 參數存放區中的敏感參數。根據預設，只有 CFCT 佈建的角色才有權使用此金鑰執行加密或解密作業。若要存取組態檔、FIFO 佇列或參數存放區`SecureString`值，必須將管理員新增至`CustomControlTowerKMSKey`原則。自動按鍵旋轉預設為啟用狀態。

AWS Lambda

在 AWS Control Tower 生命週期事件期間 AWS CloudFormation StackSets 或 AWS Organizations SCP 的初始安裝和部署期間，CFCT 會使用 AWS Lambda 函數來叫用安裝元件。

Amazon Simple Notification Service

CcCT 可能會在工作流程期間發佈通知，例如亞馬遜簡單通知服務 (Amazon SNS) 主題的管道核准。只有在您選擇接收管道核准通知時，才會啟動 Amazon SNS。

Amazon Simple Storage Service

當您部署 CFCT 時，CFCT 會建立具有唯一名稱的亞馬遜簡單儲存服務 (Amazon S3) 儲存貯體：

範例：Amazon S3 儲存貯體名稱

`custom-control-tower-configuration-`*`accountID`*`-`*`region`*

存儲桶包含一個名為的示例配置文件 `_custom-control-tower-configuration.zip`

請注意檔案名稱中的前導底線。

此 zip 檔案提供範例資訊清單，以及描述必要資料夾結構的相關範例範本。這些範例可協助您開發組態套件以自訂 AWS Control Tower landing zone。範例資訊清單會識別您實作自訂時所需的堆疊集和服務控制原則 (SCP) 的必要組態。

您可以使用此範例組態套件做為模型，來開發和上傳自訂套件，這會自動觸發 CFCT 組態管線。

若要取得有關自訂規劃檔的資訊，請參閱CFCT 定制指南。

Amazon Simple Queue Service

CFCT 使用 Amazon Simple Queue Service (Amazon SQS) FIFO 佇列從 Amazon 擷取生命週期事件。 EventBridge它觸發一個 AWS Lambda 函數，該函數調 AWS CodePipeline 用部署 AWS CloudFormation StackSets 或 SCP。如需 SCP 的詳細資訊，請參閱AWS Organizations。

AWS Step Functions

CcCT 會建立 Step Functions 來協調自訂部署。這些 Step Functions 式會翻譯組態檔案，以便視需要跨環境部署自訂。

AWS Systems Manager 參數儲存

AWS Systems Manager Parameter Store 會存放 CFCT 組態參數。這些參數可讓您整合相關的組態範本。例如，您可以設定每個帳戶將 AWS CloudTrail 資料記錄到集中式 Amazon S3 儲存貯體。此外，Systems Manager 員參數存放區提供了一個集中的位置，管理員可以在其中檢視 CFCT 輸入和參數。

部署考量

請務必在部署 AWS Control Tower landing zone 區域的相同帳戶和區域中啟動 AWS Control Tower (CFCT) 的自訂項目；也就是說，您必須將其部署到 AWS Control Tower 本地區域的 AWS Control Tower 管理帳戶中。依預設，CFCT 會透過在該帳戶和區域中設定組態管線來建立和執行 landing zone 規劃套件。

準備部署

當您準備 AWS CloudFormation 範本以進行初始部署時，您可以選擇一些選項。您可以選擇組態來源，也可以允許手動核准管線部署。接下來兩節將詳細說明這些選項。

選擇您的組態來源

依預設，範本會建立 Amazon Simple Storage Service (Amazon S3) 儲存貯體，將範例組態套件存放為名為的`.zip`檔案`_custom-control-tower-configuration.zip`。Amazon S3 儲存貯體受版本控制，您可以視需要更新組態套件。如需更新組態套件的詳細資訊，請參閱使用 Amazon S3 做為組態來源。

> **注意**
>
> 範例組態套件檔案名稱以底線 (_) 開頭，因此 AWS CodePipeline 不會自動啟動。完成自訂規劃套件後，請務必上傳`custom-control-tower-configuration.zip`不帶底線 (_) 的，以便在中開始部署 AWS CodePipeline。

您可以選取 AWS CloudFormation 參數中的`AWS CodeCommit`選項，將組態套件的儲存位置從 S3 儲存貯體變更為 AWS CodeCommit Git 儲存庫。此選項可讓您輕鬆管理版本控制。

> **注意**
>
> 當您使用預設 S3 儲存貯體時，請確定組態套件是以`.zip`檔案形式提供。當您使用 AWS CodeCommit 儲存庫時，請確定組態套件已放置在儲存庫中，而不壓縮檔案。如需在中建立和儲存組態套件的詳細資訊 AWS CodeCommit，請參閱CFCT 定制指南。

您可以使用範例組態套件來建立您自己的自訂組態來源。當您準備好部署自訂組態時，請手動將組態套件上傳到 Amazon S3 儲存貯體或 AWS CodeCommit 儲存庫。當您上載組態檔案時，管線會自動開始。

> **注意**
>
> 當您使 AWS CodeCommit 用儲存組態套件時，不需要壓縮套件。如需有關在中建立和儲存組態套件的詳細資訊 AWS CodeCommit，請參閱CFCT 定制指南。

選擇您的管道組態核准參數

AWS CloudFormation 範本提供手動核准組態變更部署的選項。依預設，不會啟用手動核准。如需詳細資訊，請參閱步驟 1。啟動堆棧。

啟用手動核准後，組態管道會驗證對 AWS Control Tower 檔案資訊清單和範本所做的自訂，然後暫停程序，直到獲得手動核准為止。核准後，部署會視需要繼續執行剩餘的管道階段，以實作 AWS Control Tower (CFCT) 功能的自訂。

您可以使用手動核准參數拒絕第一次嘗試在管道中執行，以防止 AWS Control Tower 組態的自訂執行。此參數也可讓您手動驗證 AWS Control Tower 組態變更的自訂項目，作為實施前的最終控制。

更新 AWS Control Tower 的自訂

如果您之前已部署 CFCT，則必須更新 AWS CloudFormation 堆疊以取得最新版本的 CFCT 架構。如需詳細資訊，請參閱更新堆疊。

模板和源代碼

啟動 AWS CloudFormation 範本後，AWS Control Tower (CFCT) 的自訂項目會部署在您的管理帳戶中。您可以從中下載範本， GitHub 然後從中啟動範本AWS CloudFormation。

customizations-for-aws-control塔. 範本會部署下列項目：

- 一個 AWS CodeBuild 項目
- 一個 AWS CodePipeline 項目
- Amazon EventBridge 規則
- AWS Lambda 函數
- Amazon 簡單隊列服務隊列
- 具有範例組態套件的 Amazon 簡易儲存服務儲存貯體
- AWS Step Functions

> **Note**
>
> 您可以根據自己的特定需求自定義模板。

源代碼儲存庫

您可以訪問我們的GitHub 存儲庫以下載 CFCT 的模板和腳本，並與其他人共享您的 landing zone 自定義。

自動化部署

啟動自動化部署之前，請檢閱考量事項。按照本節中的 step-by-step 說明設定解決方案，並將其部署到您的 AWS Control Tower 管理帳戶。

部署時間：約 15 分鐘

必要條件

CcCT 必須部署在您的 AWS Control Tower 管理帳戶和 AWS Control Tower 本地區域中。如果您沒有設置平 landing zone，請參閱開始使用。

部署步驟

部署 CFCT 的程序包括兩個主要步驟。如需詳細說明，請點選各項步驟連結。

步驟 1. 啟動 堆疊

- 將 AWS CloudFormation 範本啟動至您的管理帳戶。
- 檢閱範本參數，並視需要進行調整。

步驟 2. 建立自訂套件

- 建立自訂組態套件。

> **Important**
>
> 要下載正確的 AWS CloudFormation 模板並啟動 CFCT，請點擊本節中給出的 GitHub 鏈接。請勿追蹤任何先前指定之 S3 儲存貯體的舊連結。

步驟 1. 啟動 堆疊

本節中的 AWS CloudFormation 範本會在您的帳戶中部署 AWS Control Tower (CFCT) 的自訂項目。

> **注意**
>
> 您需要負責運行 CFCT 時使用的 AWS 服務的費用。如需詳細資訊，請參閱費用。

1. 若要啟動 AWS Control Tower 的自訂，請從中下載範本， GitHub然後從中啟動範本AWS CloudFormation。
2. 依預設，範本會在美國東部 (維吉尼亞北部) 區域啟動。若要在不同的 AWS 區域中啟動 CFCT，請使用主控台導覽列中的「地區」選取器。

> **Note**
>
> CcCT 必須在您部署 AWS Control Tower 登陸區域的相同區域和帳戶中啟動，也就是您的本地區域。

3. 在 [建立堆疊] 頁面上，確認 [URL] 文字方塊中顯示正確的範本 URL，然後選擇 [下一步]。
4. 在 [指定堆疊詳細資料] 頁面上，為 CFCT 堆疊指派名稱。
5. 在「參數」(Parameters) 下，檢閱下列參數，並視需要在樣板中修改它們。

配管組態		
參數	預設	描述
管道審批階段	No	選擇是否要將管線組態從預設的自動核准階段變更為手動核准階段。如需詳細資訊，請參閱 the section called “CFCT 定制指南”。
管道核准電子郵件地	<Optional Input>	核准通知的電子郵件地址。若要使用此參數，您必須將「管線核准階段」參數設定為Yes。
AWS CodePipeline 來源	Amazon S3	AWS 的來源，可協 CodePipeline 助您選取儲存和設定 CFCT 自訂的位置。

AWS CodeCommit 安裝程式		
參數	**預設**	**描述**
現有的 CodeCommit儲存庫？	No	選擇是否使用現有的 CodeCommit Git 儲存庫。如果您選擇Yes，則必須將「CodePipeline 來源」參數設定為AWS CodeCommit 。
CodeCommit 儲存庫名稱	custom-control-tower-configuration	Git 儲存庫名稱。若要使用此參數，您必須將 AWS 來CodePipeline源參數設定為AWS CodeCommit 。此名稱用於建立新的 Git 儲存庫，且必須是唯一的。如果您提供現有 Git 存儲庫的名稱，則必須設置現有 CodeCommit 存儲庫？ 參數為「是」，然後輸入該存放庫的確切名稱。
CodeCommit 分行名稱	main	儲存自訂套件的 Git 分支。Git 存儲庫可以有許多分支。這是指定給 Git 儲存庫中分支的預設名稱。若要使用此參數，您必須將 S CodePipeline ource 參數設定為AWS CodeCommit 。
AWS CloudFormation StackSets 組態設定		
參數	**預設**	**描述**
區域並行類型	PARALLEL	在區域中選取部署 StackSets 作業的並行類型。此設定適用於建立、更新和刪除工作流程。其他允許的值為SEQUENTIAL 。

AWS CloudFormation StackSets 組態設定		
參數	預設	描述
最大並行百分比	100	執行此操作時，一次可用的帳戶百分比上限。允許的最大值為 100。如需詳細資訊，請參閱堆疊集合作業選項。
失敗允差百分比	10	在 AWS CloudFormation 停止在該區域的操作之前，此堆疊操作可能會失敗的每個區域的帳戶百分比。允許的最小值為 0，允許的最大值為 100。如需詳細資訊，請參閱堆疊集合作業選項。

6. 選擇下一步。
7. 在 Configure stack options (設定堆疊選項) 頁面，選擇 Next (下一步)。
8. 在 Review (檢視) 頁面上，檢視和確認的設定。請確保确认模板範本将创建 AWS Identity and Access Management (IAM)資源的核取方塊。
9. 選擇 Create stack (建立堆疊) 以部署堆疊。

   您可以在 AWS CloudFormation 主控台的 [狀態] 欄中檢視堆疊的狀態。您應該會在大約 15 分鐘內看到「建立 _ 完成」狀態。

步驟 2. 建立自訂套件

透過啟動的堆疊，您可以透過自訂隨附的組態套件，將自訂項目新增到 AWS Control Tower landing zone 和服務控制政策 (SCP)。如需建立自訂套件的詳細指示，請參閱CFCT 定制指南。

> **注意**
>
> 如果沒有上傳自訂組態套件，則管線不會執行。

更新堆疊

如果您之前已部署 AWS Control Tower (CFCT) 的自訂，請按照程序更新最新版本 CFCT 架構的 AWS CloudFormation 堆疊。

> **Important**
>
> 您必須先將最新範本從 Amazon 簡單儲存服務 (Amazon S3) 儲存貯體上傳 GitHub至 Amazon S3 儲存貯體，才能完成下列程序。如需有關如何開始使用 Amazon S3 的指示，請參閱 Amazon 簡單儲存服務使用者指南中的開始使用 Amazon S3。

1. 登入 AWS CloudFormation 主控台。
2. 選取 AWS Control Tower (CFCT) CloudFormation 堆疊的現有自訂，然後選取 [更新]。
3. 在必要條件-準備範本下，選取取代目前範本。
4. 在「指定樣板」下，執行下列操作：
   a. 選取「取代目前範本」做為「範本來源」。
   b. 對於 Amazon S3 URL，請輸入您先前從 GitGub Amazon S3 上傳的範本的範本 URL，然後選擇 [下一步]。
   c. 確認範本 URL 是否正確。然後再次選擇下一步和下一步。
5. 在「參數」下，檢閱範本的參數，並視需要修改它們。請參閱步驟 1。啟動堆棧以獲取有關參數的詳細信息。
6. 選擇下一步。
7. 在 Configure stack options (設定堆疊選項) 頁面，選擇 Next (下一步)。
8. 在 Review (檢視) 頁面上，檢視和確認的設定。請務必核取方塊，確認範本可能會建立 AWS Identity and Access Management (IAM) 資源。
9. 選擇 [檢視變更集] 並確認變更。
10. 選擇 [更新堆疊] 以部署堆疊。

    您可以在 AWS CloudFormation 主控台的 [狀態] 欄中檢視堆疊的狀態。您應該會在大約 15 分鐘內看到「更新 _ 完成」的狀態。

刪除堆疊集

如果您已在資訊清單檔案中啟用堆疊集刪除功能，則可以刪除堆疊集。依預設，enable_stack_set_deletion 參數設為 false。在此配置中，從 CFCT 資訊清單檔案中移除資源時，不會採取任何動作來刪除相關聯的堆疊集合。

如果您enable_stack_set_deletion將資訊清單檔案true中的值變更為，當您從資訊清單檔案中移除關聯的資源時，CFCT 會刪除堆疊集及其所有資源。

資訊清單檔案 v2 支援此功能。

> **Important**
>
> 當您初始enable_stack_set_deletion將的值設定為時true，下次呼叫 CFCT 時，會暫存以前置詞開頭的所有資源CustomControlTower-，這些資源具有相關聯的索引鍵標記Key:AWS_Solutions, Value: CustomControlTowerStackSet，且未在資訊清單檔案中宣告，以供刪除。

以下是如何在manifest.yaml檔案中設定此參數的範例：

```
version: 2021-03-15
region: us-east-1
enable_stack_set_deletion: true   #New opt-in functionality


resources:
  - name: demo_resource_1
    resource_file: s3://demo_bucket/resource.template
    deployment_targets:
      accounts:
        - 012345678912
    deploy_method: stack_set
    ...
    regions:
    - us-east-1
    - us-west-2

  - name: demo_resource_2
    resource_file: s3://demo_bucket/resource.template
    deployment_targets:
      accounts:
```

```
    - 012345678912
deploy_method: stack_set
...
regions:
- us-east-1
- eu-north-1
```

將 Amazon S3 設置為組態來源

當您為 AWS Control Tower 設定自訂時，它會在 Amazon Simple Storage Service (Amazon S3) 儲存貯體中存放一個名為_custom-control-tower-configuration.zip檔案的初始組態檔案custom-control-tower-configuration-*account-ID*-*region*。

> **注意**
>
> 如果您選擇下載並修改此檔案，請記得壓縮變更、儲存為名為的新檔案custom-control-tower-configuration.zip，然後將其上傳回相同的 Amazon S3 儲存貯體。Amazon S3 儲存貯體是管道的預設來源。設定預設設定後，將檔案名稱中不含底線前置詞的組態 zip 檔案上傳至 S3 儲存貯體，將會自動啟動管道。

zip 檔案受到伺服器端加密 (SSE) 與 AWS Key Management Service (AWS KMS) 保護，並拒絕使用 KMS 金鑰。若要存取 zip 檔案，您必須更新 KMS 金鑰原則，以指定應授與存取權的角色。角色可以是系統管理員角色、使用者或兩者。請遵循以下程序：

1. 導覽至 AWS Key Management Service 主控台。
2. 在客戶管理的金鑰中，選取 CustomControlTowerKMSKey。
3. 選取金鑰原則索引標籤。然後，選取「編輯」。
4. 在 [編輯金鑰原則] 頁面中，找到程式碼中的 [允許使用金鑰] 區段，然後新增下列其中一個權限：
   - 若要新增管理角色：

     ```
     arn:aws:iam::<account-ID>:role/<administrator-role>
     ```
   - 若要新增使用者：

     ```
     arn:aws:iam::<account-ID>:user/<username>
     ```
5. 選取 Save Changes (儲存變更)。

6. 導覽至 Amazon S3 主控台，尋找包含組態壓縮檔案的 S3 儲存貯體，然後選取下載。
7. 對資訊清單檔案和範本檔案進行必要的組態變更。如需有關自訂資訊清單和範本檔案的資訊，請參閱the section called “CFCT 定制指南”。
8. 上傳您的變更：
   a. 壓縮修改後的組態檔案，並將檔案命名為：`custom-control-tower-configuration.zip`。
   b. 使用具有 AWS KMS 主金鑰的 SSE 將檔案上傳到 Amazon S3：。`CustomControlTowerKMSKey`

運營指標的集合

AWS Control Tower (CFCT) 的自訂項目包含將匿名操作指標傳送至 AWS的選項。 AWS 使用這些數據來了解客戶如何使用 CcCT，以及其他相關服務和產品。啟用資料收集時，會將下列資訊傳送至 AWS：

- 解決方案 ID： AWS 解決方案識別碼
- 唯一識別碼 (UUID)：為每個部署隨機產生的唯一識別碼
- 時間戳記：資料收集時間戳記
- 狀態機器執行計數：逐步計算此狀態機運行的次數
- 清單版本：配置中使用的清單版本

> **Note**
>
> AWS 擁有它收集的數據。數據收集受AWS 隱私政策的約束。

若要選擇退出傳送匿名作業指標 AWS，請完成下列其中一項工作：

- 更新 AWS CloudFormation 範本對應區段，如下所示：

  從

```
AnonymousData:
     SendAnonymousData:
        Data: Yes
```

設定為

```
AnonymousData:
     SendAnonymousData:
        Data: No
```

- 部署 CFCT 之後，在參數存放區主控台中尋找 **/org/primary/metrics_flag** SSM 參數金鑰，並將值更新為。**No**

CFCT 定制指南

AWS Control Tower (CFCT) 的自訂指南適用於想要為公司和客戶自訂和擴充 AWS Control Tower 環境的管理員、 DevOps 專業人員、獨立軟體廠商、IT 基礎設施架構師和系統整合商。它提供有關使用 CFCT 自訂套件自訂和擴充 AWS Control Tower 環境的資訊。

> **Note**
>
> 若要部署和設定 (CFCT)，您必須透過 AWS CodePipeline部署和處理組態套件。以下各節將詳細描述該過程。

程式碼管線概觀

該配置包需要 Amazon Simple Storage Service (Amazon S3) 和 AWS CodePipeline. 組態套件包含下列項目：

- 清單文件
- 隨附的一組範本
- 用於描述和實作 AWS Control Tower 環境自訂的其他 JSON 檔案

依預設，`_custom-control-tower-configuration.zip`組態套件會以下列命名慣例載入 Amazon S3 儲存貯體中：

`custom-control-tower-configuration-`*`accountID`*`-`*`region`*.

> **Note**
>
> 根據預設，CFCT 會建立 Amazon S3 儲存貯體來存放管道來源，但您可以將來源位置變更為 AWS CodeCommit 儲存庫。如需詳細資訊，請參閱《AWS CodePipeline 使用指南》CodePipeline中的〈編輯管線〉。

資訊清單檔案是一個文字檔案，描述您可以部署以自訂 landing zone 的 AWS 資源。 CodePipeline 執行以下任務：

- 擷取資訊清單檔案、隨附的範本集和其他 JSON 檔案
- 執行清單和模板驗證
- 調用清單文件中的部分以運行特定的管道階段。

當您透過自訂資訊清單檔案並從組態封裝檔案名稱中移除底線 (_) 來更新組態封裝時，它會自動啟動 AWS CodePipeline。

> **Note**
>
> 範例組態套件檔案名稱以底線 (_) 開頭，因此 AWS CodePipeline 不會自動觸發。完成組態套件的自訂後，請上傳`custom-control-tower-configuration.zip`不帶底線 (_) 的檔案，以便在中觸發部署 AWS CodePipeline。

AWS CodePipeline 階段

CFCT 管道需要數個 AWS CodePipeline 階段來實作和更新您的 AWS Control Tower 環境。

1. 來源階段

   來源階段是初始階段。您的自訂組態套件會啟動此管線階段。的來源 AWS CodePipeline 可以是 Amazon S3 儲存貯體或 AWS CodeCommit 儲存庫，可以在其中託管組態套件。

2. 構建階段

   構建階段需 AWS CodeBuild 要驗證配置包的內容。這些檢查包括測試`manifest.yaml`檔案語法和結構描述，以及包含在套件中或遠端託管的所有 AWS CloudFormation 範本，使用 AWS CloudFormation `validate-template`和`cfn_nag`。如果資訊清單檔案和 AWS CloudFormation

範本通過測試，管線會繼續進入下一個階段。如果測試失敗，您可以檢閱 CodeBuild 記錄檔以識別問題，並視需要編輯組態來源檔案。

3. 手動核准階段 (選擇性)

   手動核准階段是選擇性的。如果啟用此階段，它會提供對組態管線的額外控制。它會在部署期間暫停管線，直到獲得核准為止。您可以在啟動堆疊時，將「管線核准階段」參數編輯為 「是」，以選擇手動核准。

4. 服務控制政策階段

   服務控制原則階段會呼叫服務控制原則狀態機器，以呼叫建立服務控制原則 (SCP) 的 AWS Organizations API。

5. AWS CloudFormation 資源階段

   資 AWS CloudFormation 源階段會呼叫堆疊集狀態機器，以部署您在資訊清單檔案中提供的帳號或組織單位 (OU) 清單中指定的資源。除非指定了 AWS CloudFormation 資源相依性，否則狀態機會按照資訊清單檔案中指定的順序建立資源。

定義自訂組態

您將使用資訊清單檔案、隨附的範本集和其他 JSON 檔案來定義自訂 AWS Control Tower 組態。您將這些檔案封裝到資料夾結構中，並將它們作為`.zip`檔案放置在 Amazon S3 儲存貯體中，如下列程式碼範例所示。

自訂組態資料夾結構

```
- manifest.yaml
- policies/                                                [optional]
   - service control policies files (*.json)
- templates/                                               [optional]
   - template files for AWS CloudFormation Resources (*.template)
```

上一個範例說明自訂組態資料夾的結構。無論您選擇 Amazon S3 還是儲存 AWS CodeCommit 庫做為來源儲存位置，資料夾結構都會保持不變。如果您選擇 Amazon S3 做為來源儲存，請將所有資料夾和檔案壓縮到`custom-control-tower-configuration.zip`檔案中，然後僅將`.zip`檔案上傳到指定的 Amazon S3 儲存貯體。

> **Note**
>
> 如果您正在使用 AWS CodeCommit，請將檔案放置在存放庫中，而不壓縮檔案。

清單文件

該文`manifest.yaml`件是描述您的 AWS 資源的文本文件。下列範例顯示資訊清單檔案的結構。

```
---
region: String
version: 2021-03-15

resources:
  #set of CloudFormation resources or SCP policies
...
```

如前面的程式碼範例所示，資訊清單檔案的前兩行會指定區域和 version 關鍵字的值。以下是這些關鍵字的定義。

區域 — AWS Control Tower 預設區域的文字字串。此值必須是有效的 AWS 區域名稱 (例如`us-east-1`、`eu-west-1`或`ap-southeast-1`)。除非指定更多資源特定區域，否則建立自訂 AWS Control Tower 資源 (例如 AWS CloudFormation StackSets) 時，AWS Control Tower 主區域為預設區域。

```
region:your-home-region
```

版本 — 資訊清單結構描述版本號碼。支援的最新版本為

```
version: 2021-03-15
```

> **Note**
>
> 我們強烈建議您使用最新版本。若要更新最新版本的資訊清單屬性，請參閱清單版本升級。

上一個範例中顯示的下一個關鍵字是 resources 關鍵字。清單文件的資源部分具有高度結構化。它包含 AWS 資源，這將由 CFCT 管道自動部署的詳細列表。下一節會提供這些資源及其可用參數的說明。

清單文件的資源部分

本主題說明資訊清單檔案的資源區段，您將在其中定義自訂所需的資源。清單文件的這一部分從關鍵字資源開始，並繼續到文件的末尾。

資訊清單檔案的資源區段會指定 CcCT 透過程式碼管線自動部署的 AWS CloudFormation StackSets 或 AWS Organizations SCP。您可以列出要部署堆疊執行個體的 OU、帳戶和區域。

堆疊執行個體部署在帳戶層級而非 OU 層級。SCP 會在 OU 層級部署。如需詳細資訊，請參閱建立您自己的自訂。

下列範例範本說明資訊清單檔案的資源區段可用的可能項目。

```
resources: # List of resources
  - name: [String]
    resource_file: [String] [Local File Path, S3 URI, S3 URL]
    deployment_targets: # account and/or organizational unit names
      accounts: # array of strings, [0-9]{12}
        - 012345678912
        - AccountName1
      organizational_units: #array of strings
        - OuName1
        - OuName2
    deploy_method: scp | stack_set
    parameters: # List of parameters [SSM, Alfred, Values]
      - parameter_key: [String]
        parameter_value: [String]
    export_outputs: # list of ssm parameters to store output values
      - name: /org/member/test-ssm/app-id
        value: $[output_ApplicationId]
    regions: #list of strings
    - [String]
```

本主題的其餘部分會針對上一個程式碼範例中顯示的關鍵字提供詳細定義。

名稱 — 與相關聯的名稱 AWS CloudFormation StackSets。 您提供的字串會為堆疊集指派更容易使用的名稱。

- 類型：字串
- 必要：是
- 有效值：a-z、A-Z、0-9 和底線 (_)。任何其他字元都會自動以底線 (_) 取代。

描述 — 資源的描述。

- 類型：字串
- 必要：否

resource_file — 此檔案可指定為資訊清單檔案的相對位置，也就是指向 JSON 中用於建立 AWS CloudFormation 資源或 SCP 的 AWS CloudFormation 範本或 AWS Organizations 服務控制政策的 Amazon S3 URI 或 URL。

- 類型：字串
- 必要：是

1. 下列範例顯示`resource_file`，指定為組態套件內資源檔案的相對位置。

```
resources:
  - name: SecurityRoles
    resource_file: templates/custom-security.template
```

2. 下面的示例顯示了作為一個 Amazon S3 URI 給出的資源文件

```
resources:
  - name: SecurityRoles
    resource_file: s3://bucket-name/[key-name]
```

3. 下列範例顯示以 Amazon S3 HTTPS 網址形式提供的資源檔案

```
resources:
  - name: SecurityRoles
    resource_file: https://bucket-name.s3.Region.amazonaws.com/key-name
```

> **Note**
>
> 如果您提供 Amazon S3 URL，請確認儲存貯體政策是否允許您從中部署 CFCT 的 AWS Control Tower 管理帳戶讀取存取。如果您提供 Amazon S3 HTTPS 網址，請確認路徑使用點標記法。例如 `S3.us-west-1`。CFCT 不支援在 S3 和區域之間包含破折號的端點，例如`S3-us-west-2`.

4. 下列範例顯示 Amazon S3 儲存貯體政策和存放資源的 ARN。

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
        "Effect": "Allow",
        "Principal": {"AWS": "arn:aws:iam::AccountId:root"},
        "Action": "s3:GetObject",
        "Resource": "arn:aws:s3:::my-bucket/*”
       }
   ]
}
```

您將以部署 CFCT 之管理 AWS 帳戶的帳戶 ID 取代範例中顯示的*AccountId*變數。如需更多範例，請參閱 Amazon 簡易儲存服務使用者指南中的儲存貯體政策範例。

參數 — 指定參 AWS CloudFormation 數的名稱和值。

- 類型: MapList
- 必要：否

參數部分包含對鍵/值參數。下列虛擬範本概述了參數區段。

```
parameters:
  - parameter_key: [String]
    parameter_value: [String]
```

- 參數鍵 — 與參數相關聯的關鍵字。
  - 類型：字串
  - 必要：是 (在參數屬性下)
  - 有效值：a-z、A-Z 和 0-9
- 參數值 — 與參數相關聯的輸入值。
  - 類型：字串
  - 必要：是 (在參數屬性下)

deploy_method — 將資源部署到帳戶的部署方法。目前，deploy_method 支援使用透過資源部署`stack_set`選項來部署資源 AWS CloudFormation StackSets，或使用選`scp`項 (如果您正在部署 SCP) 來部署資源。

- 類型：字串
- 有效值：`stack_set` | `scp`
- 必要：是

部署目標 — 帳戶或組織單位 (OU) 清單，CFCT 將部署 AWS CloudFormation 資源 (指定為帳戶或組織單位)。

> **Note**
>
> 如果您想要部署 SCP，目標必須是 OU，而不是帳戶。

- 類型：字串清單`account name`或`account number`表示此資源將部署到指定的帳號清單中，或`OU names`指示此資源將部署到指定的 OU 清單中。
- 必要：至少一個科目或組織單位
  - 帳戶：

    類型：字串清單`account name`或`account number`表示此資源將部署到指定的帳號清單中。
  - 組織單位 (_S)：

    類型：字串清單`OU names`，表示此資源將部署到指定的 OU 清單中。如果您提供的 OU 不包含帳戶，且未新增帳戶屬性，CFCT 只會建立堆疊集。

    > **Note**
    >
    > 組織的管理帳戶 ID 不是允許的值。CFCT 不支援將堆疊執行個體部署到組織的管理帳戶中。

匯出 — 代表 SSM 參數金鑰的名稱/值配對清單。這些 SSM 參數金鑰可讓您將範本輸出儲存至 SSM 參數存放區。輸出旨在供其他資源參考，該資源先前在清單文件中定義。

```
export_outputs: # List of SSM parameters
```

```
  - name: [String]
    value: [String]
```

- 類型：名稱和值鍵配對的清單。名稱包含 SSM 參數存放區金鑰的`name`字串，而值則包含參數的`value`字串。
- 有效值：任何字串或其中 *`CfnOutput-Logical-ID`* 對應於範本輸出`$[output_`*`CfnOutput-Logical-ID`*`]`變數的變數。如需有關 AWS CloudFormation 範本中「輸出」區段的詳細資訊，請參閱AWS CloudFormation 使用者指南中的「輸出」。
- 必要：否

例如，下列程式碼片段會將範本`VPCID`輸出變數儲存到名`/org/member/audit/vpc_id`為的 SSM 參數金鑰中。

```
export_outputs: # List of SSM parameters
  - name: /org/member/audit/VPC-ID
    value: $[output_VPCID]
```

> **Note**
>
> 輸出密鑰名稱可以包含以外的值。`output`例如，如果名稱是`/org/environment-name`，則值可能是`production`。

區域 — CcCT 將在其中部署 AWS CloudFormation 堆疊執行個體的區域清單。

- 類型：任何 AWS 商業區域名稱清單，以表示此資源將部署到指定的區域清單中。如果資訊清單檔案中不存在此關鍵字，則資源只會部署在主區域中。
- 必要：否

根 OU

CFCT 支援根作為資訊清單 V2 版本 (2021-03-15) 下**`organizational_units`**的組織單位 (OU) 的值。

- 如果您選擇的部署方法`scp`，則在下方新增根時`organizational_units`，AWS Control Tower 會將政策套用至根目錄下的所有 OU。如果您選擇的部署方法`stack_set`，當您在下面新增 Root

時organizational_units，CFCT 會在 AWS Control Tower 註冊的所有根帳戶中部署堆疊集，但管理帳戶除外。

- 根據 AWS Control Tower 最佳實務，管理帳戶僅用於管理成員帳戶和計費目的。請勿在 AWS Control Tower 管理帳戶中執行生產工作負載。

  根據最佳實務指導，AWS Control Tower 部署會將管理帳戶置於根 OU 之下，以便擁有完整存取權，而且不會執行其他資源。因此，AWSControlTowerExecution角色不會部署至管理帳戶。

- 我們建議您遵循管理帳戶的下列最佳做法。如果您的特定使用案例需要在管理帳戶中部署堆疊集，請將帳戶納入為部署目標並指定管理帳戶。否則，請勿將帳戶納入為部署目標。您必須在管理帳戶中建立遺失的資源，包括必要的 IAM 角色。

若要在管理帳戶中部署堆疊集，請包含accounts做為部署目標並指定管理帳戶。否則，請勿將帳戶納入為部署目標。

```
---
region: your-home-region
version: 2021-03-15

resources:

  …truncated…

    deployment_targets:
      organizational_units:
        - Root
```

> **Note**
>
> 根 OU 功能僅在 V2 版的資訊清單檔案 (2021-03-15) 中受支援。如果您在下面新增根作為 OUorganizational_units，請勿新增任何其他 OU。

巢狀 OU

CcCT 支援在資訊清單 V2 版本 (2021-03-15) 的organizational_units關鍵字下列出一或多個巢狀 OU。

巢狀 OU 需要完整路徑 (不包括根目錄)，並使用冒號做為 OU 之間的分隔符號。針對部署方法`scp`，AWS Control Tower 會將 SCP 部署到巢狀 OU 路徑中的最後一個 OU。針對部署方法`stack_set`，AWS Control Tower 會將堆疊集部署到巢狀 OU 路徑中最後一個 OU 下的所有帳戶。

例如，考慮路徑`OUName1:OUName2:OUName3`。路徑中的最後一個 OU 是`OUName3`。CFCT 將 SCP 部署到`OUName3`並將其堆疊到直接下`OUName3`的所有帳戶，只。

```
---
region: your-home-region
version: 2021-03-15

resources:

  …truncated…

    deployment_targets:
      organizational_units:
        - OuName1:OUName2:OUName3
```

> **Note**
>
> 巢狀 OU 功能僅在 V2 版的資訊清單檔案 (2021-03-15) 中受支援。

建立您自己的自訂

若要建立您自己的自訂，您可以透過新增或更新服務控制原則 (SCP) 和 AWS CloudFormation 資源來修改`manifest.yaml`檔案。對於必須部署的資源，您可以新增或移除帳戶和 OU。您可以在封裝資料夾中新增或修改範本、建立自己的資料夾，以及參考`manifest.yaml`檔案中的範本或資料夾。

本節說明建立自訂的兩個主要部分：

- 如何為服務控制策略設置自己的配置包
- 如何為 AWS CloudFormation 堆棧集設置自己的配置包

設定服務控制政策的組態套件

本節說明如何建立服務控制原則 (SCP) 的組態套件。這個過程的兩個主要部分是（1）準備清單文件，和（2）準備你的文件夾結構。

步驟 1：編輯清單 .yaml 文件

使用範例manifest.yaml檔案做為起點。輸入所有必要的組態。新增resource_file和deployment_targets詳細資訊。

下面的代碼片段顯示了默認的清單文件。

```
---
region: us-east-1
version: 2021-03-15

resources: []
```

的值會在部署期間自動加入。region它必須與您部署 CFCT 的區域相符。此區域必須與 AWS Control Tower 區域相同。

若要在 Amazon S3 儲存貯體中儲存的 zip 套件中的example-configuration資料夾中新增自訂 SCP，請開啟example-manifest.yaml檔案並開始編輯。

```
---
region: your-home-region
version: 2021-03-15

resources:
  - name: test-preventive-controls
    description: To prevent from deleting or disabling resources in member accounts
    resource_file: policies/preventive-controls.json
    deploy_method: scp
    #Apply to the following OU(s)
    deployment_targets:
      organizational_units: #array of strings
        - OUName1
        - OUName2

…truncated…
```

下列程式碼片段顯示自訂資訊清單檔案的範例。您可以在一次變更中新增多個策略。

```
---
region: us-east-1
version: 2021-03-15
```

```
resources:
  - name: block-s3-public-access
    description: To S3 buckets to have public access
    resource_file: policies/block-s3-public.json
    deploy_method: scp
    #Apply to the following OU(s)
    deployment_targets:
      organizational_units: #array of strings
        - OUName1
        - OUName2
```

步驟 2：建立資料夾結構

如果您對資源檔使用 Amazon S3 URL，並將參數與鍵/值配對搭配使用，則可以略過此步驟。

您必須包含 JSON 格式的 SCP 原則才能支援資訊清單，因為資訊清單檔案會參考 JSON 檔案。請確定檔案路徑與資訊清單檔案中提供的路徑資訊相符。

- 原則 JSON 檔案包含要部署至作業單位的 SCP。

下列程式碼片段顯示範例資訊清單檔案的資料夾結構。

```
- manifest.yaml
- policies/
   - block-s3-public.json
```

下列程式碼片段是block-s3-public.json原則檔的範例。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"GuardPutAccountPublicAccessBlock",
         "Effect":"Deny",
         "Action":"s3:PutAccountPublicAccessBlock",
         "Resource":"arn:aws:s3:::*"
      }
   ]
}
```

設定下列項目的組態套件 AWS CloudFormation StackSets

本節說明如何設定的組態套件 AWS CloudFormation StackSets。這個過程的兩個主要部分是：（1）準備清單文件，和（2）更新文件夾結構。

步驟 1：編輯現有的清單文件

將新 AWS CloudFormation StackSets 資訊新增至您先前編輯過的資訊清單檔案。

僅供檢閱，下列程式碼片段包含先前用來設定 SCP 組態套件時所顯示的相同自訂資訊清單檔案。現在，您可以進一步編輯此文件，以包含有關資源的詳細信息。

```
---
region: us-east-1
version: 2021-03-15

resources:

  - name: block-s3-public-access
    description: To S3 buckets to have public access
    resource_file: policies/block-s3-public.json
    deploy_method: scp
    #Apply to the following OU(s)
    deployment_targets:
    organizational_units: #array of strings
    - OUName1
    - OUName2
```

下列程式碼片段顯示包含詳細資訊的已編輯範例`resources`資訊清單檔案。的順序`resources`會決定建立`resources`相依性的執行順序。您可以根據業務需求編輯下列範例資訊清單檔案。

```
---
region: your-home-region
version: 2021-03-15

…truncated…

resources:
  - name: stackset-1
    resource_file: templates/create-ssm-parameter-keys-1.template
    parameters:
      - parameter_key: parameter-1
```

```
        parameter_value: value-1
    deploy_method: stack_set
    deployment_targets:
      accounts: # array of strings, [0-9]{12}
        - account number or account name
        - 123456789123
      organizational_units: #array of strings, ou ids, ou-xxxx
        - OuName1
        - OUName2
    export_outputs:
      - name: /org/member/test-ssm/app-id
        value: $[output_ApplicationId]
    regions:
      - region-name

  - name: stackset-2
    resource_file: s3://bucket-name/key-name
    parameters:
      - parameter_key: parameter-1
        parameter_value: value-1
    deploy_method: stack_set
    deployment_targets:
      accounts: # array of strings, [0-9]{12}
        - account number or account name
        - 123456789123
      organizational_units: #array of strings
        - OuName1
        - OUName2
regions:
  - region-name
```

下列範例顯示您可以在資訊清單檔案中新增多個 AWS CloudFormation 資源。

```
---
region: us-east-1
version: 2021-03-15

resources:
  - name: block-s3-public-access
    description: To S3 buckets to have public access
    resource_file: policies/block-s3-public.json
    deploy_method: scp
    #Apply to the following OU(s)
```

```
    deployment_targets:
      organizational_units: #array of strings
        - Custom
        - Sandbox

  - name: transit-network
    resource_file: templates/transit-gateway.template
    parameter_file: parameters/transit-gateway.json
    deploy_method: stack_set
    deployment_targets:
      accounts: # array of strings, [0-9]{12}
        - Prod
        - 123456789123 #Network
      organizational_units: #array of strings
        - Custom
    export_outputs:
      - name: /org/network/transit-gateway-id
        value: $[output_TransitGatewayID]
    regions:
      - us-east-1
```

步驟 2：更新文件夾結構

當您更新資料夾結構時，您可以包含資訊清單檔案中的所有支援 AWS CloudFormation 範本檔案和 SCP 原則檔案。驗證檔案路徑是否符合資訊清單檔案中提供的路徑。

- 範本檔案包含要部署在 OU 和帳戶中的 AWS 資源。
- 原則檔案包含範本檔案中使用的輸入參數。

下列範例顯示在步驟 1 中建立的範例資訊清單檔案的資料夾結構。

```
- manifest.yaml
- policies/
   - block-s3-public.json
- templates/
   - transit-gateway.template
```

'阿爾弗雷德' 助手和 AWS CloudFormation 參數文件

CFCT 為您提供稱為 fred Helper 的機制，以取得範本中定義的 SSM 參數存放區金鑰的值。AWS CloudFormation 使用 fred 輔助程式，您可以使用儲存在 SSM 參數存放區中且不更新 AWS

CloudFormation 範本的值。如需詳細資訊，請參閱什麼是 AWS CloudFormation 範本？ 在《AWS CloudFormation 使用者指南》中。

> **Important**
>
> 阿爾弗雷德幫手有兩個限制。參數僅適用於 AWS Control Tower 管理帳戶的本地區域。最佳做法是考慮使用不會從堆疊執行個體變更為堆疊執行個體的值。當 'fred' 幫助器檢索參數時，它會從導出變量的堆棧集中選擇一個隨機堆棧實例。

範例

假設你有兩個 AWS CloudFormation 堆棧集。堆疊集 1 有一個堆疊執行個體，並部署到一個區域中的一個帳戶。它會在可用區域中建立 Amazon VPC 和子網路，並且subnet ID必須將VPC ID和作為參數值傳入堆疊集 2。在VPC ID和subnet ID可以傳遞到堆棧集 2 之前，VPC ID和subnet ID必須使用存儲在堆棧集 1 中AWS:::SSM::Parameter。如需詳細資訊，請參閱《AWS CloudFormation 使用者指南》中的 AWS:::SSM::Parameter。

AWS CloudFormation 堆棧集 1：

在下面的代碼片段中，fred helper 可以subnet ID從參數存儲中獲取VPC ID和的值，並將它們作為輸入傳遞給 StackSet 狀態機。

```
VpcIdParameter:
    Type: AWS::SSM::Parameter
    Properties:
      Name: '/stack_1/vpc/id'
      Description: Contains the VPC id
      Type: String
      Value: !Ref MyVpc

SubnetIdParameter:
    Type: AWS::SSM::Parameter
    Properties:
      Name: '/stack_1/subnet/id'
      Description: Contains the subnet id
      Type: String
      Value: !Ref MySubnet
```

AWS CloudFormation 堆棧集 2：

程式碼片段會顯示 AWS CloudFormation 堆疊 2 `manifest.yaml` 檔案中指定的參數。

```
parameters:
      - parameter_key: VpcId
        parameter_value: $[alfred_ssm_/stack_1/vpc/id]
      - parameter_key: SubnetId
        parameter_value: $[alfred_ssm_/stack_1/subnet/id]
```

AWS CloudFormation 堆棧集合 2.1：

程式碼片段顯示您可以列出要支援類型參數的`alfred_ssm`性質CommaDelimitedList。如需詳細資訊，請參閱《AWS CloudFormation 使用者指南》中的 `Parameters`。

```
parameters:
      - parameter_key: VpcId # Type: String
        parameter_value: $[alfred_ssm_/stack_1/vpc/id']
      - parameter_key: SubnetId # Type: String
        parameter_value: $[ alfred_ssm_/stack_1/subnet/id']
      - parameter_key: AvailablityZones # Type: CommaDelimitedList
        parameter_value:
  - "$[alfred_ssm_/availability_zone_1]"
 - "$[alfred_ssm_/availability_zone_2]"
```

自訂套件的 JSON 結構定義

CFCT 自訂套件的 JSON 結構描述位於的原始程式碼儲存庫中。 GitHub您可以將結構描述與許多您最愛的開發工具搭配使用，而且在建置自己的`manifest.yaml`檔案時可能有助於減少錯誤。

清單版本升級

如需 AWS Control Tower (CFCT) 最新版自訂的相關資訊，請參閱儲存庫中的變更日誌 .md 檔案。GitHub

Warning

AWS Control Tower (CFCT) 2.2.0 版的自訂功能引入了資訊清單結構描述 (版本 2021-03-15)，以便與相關服務 API 保持一致。 AWS 資訊清單結構描述允許單一資訊清

單 .yaml 檔案透過解耦工作流程來管理支援的資源 (AWS CloudFormation 範本和 SCP)。DevOps

我們強烈建議您將資訊清單結構描述從 2020-01-01 版更新為版本 2021- 03-15 或更新版本。中心繼續支持該文件的版本 2021-03-15 和 2020- 01-01 版本。`manifest.yaml`不需要變更現有的組態。但是，版本 2020-01-01 已停止 Support。我們不再提供 2020-01-01 版本的更新或增強功能。2020-01-01 版本不支援根 OU 和巢狀 OU 功能。

清單版本 2021- 03-15 中已過時的屬性：

```
organization_policies
policy_file
apply_to_accounts_in_ou

cloudformation_resources
template_file
deploy_to_account
deploy_to_ou
ssm_parameters
```

強制升級步驟

當您升級到資訊清單結構描述版本 2021-03-15 版本時，您必須進行以下變更才能更新檔案。接下來幾節概述了轉換的強制性和建議變更。

Organizations 政策

1. 在新屬性資源下的組織政策下移動 SCP。
2. 將策略文件屬性更改為新屬性資源文件。
3. 將套用至帳戶內容變更為新的內容部署目標。OU 清單應在子屬性組織單位下定義。組織策略不支援帳號子屬性。
4. 添加具有 scp 值的新屬性部署方法。

AWS CloudFormation 資源

1. 在新的屬性 CloudFormation 資源下移動資源雲形式資源下的資源。
2. 將模板文件屬性更改為新屬性資源文件。
3. 將部署變更為新的內容部署目標。OU 清單應在子屬性組織單位下定義。

4. 將部署至帳戶變更為新屬性部署目標。帳戶列表應在子屬性帳戶下定義。
5. 將 ssm_ 參數屬性更改為新屬性導出輸出。

強烈建議的升級步驟

AWS CloudFormation 參數

1. 將參數檔案性質變更為新性質參數。
2. 移除參數檔案屬性值中的檔案路徑。
3. 將參數金鑰和參數值從現有參數 JSON 檔案複製到參數屬性的新格式。這將幫助您在清單文件中管理它們。

> **Note**
>
> 資訊清單版本 2021-03-15 中支援參數檔案屬性。

AWS Control Tower 中的聯網

AWS Control Tower 提供透過 VPC 聯網的基本支援。

如果 AWS Control Tower VPC 的預設組態或功能不符合您的需求，您可以使用其他 AWS 服務來設定 VPC。如需如何使用 VPC 和 AWS Control Tower 的詳細資訊，請參閱建立可擴展且安全的多虛擬私人雲端 AWS網路基礎設施。

相關主題

- 如需註冊具有現有 VPC 的帳戶時，AWS Control Tower 如何運作的相關資訊，請參閱使用 VPC 註冊現有帳戶。
- 使用 Account Factory，您可以佈建包含 AWS Control 塔 VPC 的帳戶，也可以在沒有 VPC 的情況下佈建帳戶。如需如何在沒有 VPC 的情況下刪除 AWS Control Tower VPC 或設定 AWS Control Tower 帳戶的相關資訊，請參閱。逐步解說：在沒有 VPC 的情況下設定 AWS Control Tower
- 如需如何變更 VPC 帳戶設定的相關資訊，請參閱更新帳戶的 Account Factory 文件。
- 如需有關在 AWS Control Tower 中使用聯網和 VPC 的詳細資訊，請參閱本使用者指南的相關資訊頁面中有關聯網的章節。

AWS Control Tower 中的 VPC 和 AWS 區域

作為帳戶建立的標準部分， AWS 會在每個區域建立一個 AWS預設的 VPC，即使您不是使用 AWS Control Tower 管理的區域也是如此。此預設 VPC 與 AWS Control Tower 為佈建帳戶建立的 VPC 不同，但 IAM 使用者可以存取非受管區域中的 AWS 預設 VPC。

管理員可以啟用區域拒絕控制，如此一來，您的最終使用者就沒有權限連線到 AWS Control Tower 支援但管轄區域之外的區域中的 VPC。若要設定「區域」拒絕控制，請前往「著陸區設定」頁面，然後選取「修改設定」。

區域拒絕控制會封鎖對非受管理 AWS 區域中大部分服務的 API 呼叫。如需詳細資訊，請參閱AWS 根據要求拒絕存取 AWS 區域。 。

> **Note**
>
> 區域拒絕控制可能無法阻止 IAM 使用者連線到不支援 AWS Control Tower 的區域中的 AWS 預設 VPC。

或者，您可以移除非受控管區域中的 AWS 預設 VPC。若要列出區域中的預設 VPC，您可以使用類似下列範例的 CLI 命令：

```
aws ec2 --region us-west-1 describe-vpcs --filter Name=isDefault,Values=true
```

AWS Control Tower 和虛擬私人雲端概觀

以下是有關 AWS Control Tower VPC 的一些重要事實：

- AWS Control Tower 在 Account Factory 佈建帳戶時建立的 VPC 與 AWS 預設 VPC 不同。
- 當 AWS Control Tower 在支援的 AWS 區域中設定新帳戶時，AWS Control Tower 會自動刪除預設 AWS VPC，並設定 AWS Control Tower 設定的新 VPC。
- 每個 AWS Control Tower 帳戶允許一個由 AWS Control Tower 建立的 VPC。帳戶可以在帳戶限制內擁有額外的 AWS VPC。
- 每個 AWS Control Tower VPC 在美國西部 (加利佛尼亞北部) 區域以外的所有區域都有三個可用區域`us-west-1`，以及中`us-west-1`的兩個可用區域。根據預設，各可用區域會指派一個公有子網路和兩個私有子網路。因此，在美國西部 (加利佛尼亞北部) 以外的區域中，每個 AWS Control Tower VPC 預設都包含九個子網路，分成三個可用區域。在美國西部 (加利佛尼亞北部)，六個子網路分為兩個可用區域。
- AWS Control Tower VPC 中的每個子網路都會指派一個大小相同的唯一範圍。
- VPC 中的子網路數量可以設定。如需如何變更 VPC 子網路組態的詳細資訊，請參閱 Account Factory 主題。
- 由於 IP 地址不重疊，因此 AWS Control Tower VPC 中的六個或九個子網路可以不受限制地互相通訊。

使用 VPC 時，AWS Control Tower 在區域層級沒有區別。每個子網路都是從您指定的確切 CIDR 範圍配置。VPC 子網路可以存在於任何區域。

備註

> **管理 VPC 成本**
>
> 如果您設定 Account Factory VPC 組態，以便在佈建新帳戶時啟用公用子網路，Account Factory 會設定 VPC 以建立 NAT 閘道。Amazon VPC 將向您收取您的使用費用。

⚠ VPC 和控制設定

如果在啟用 VPC 網際網路存取設定的情況下佈建 Account Factory 帳戶，則該 Account Factory 設定會覆寫客戶管理之 Amazon VPC 執行個體的「禁止網際網路存取」控制項。若要避免為新佈建的帳戶啟用網際網路存取，您必須變更 Account Factory 中的設定。如需詳細資訊，請參閱逐步解說：在沒有 VPC 的情況下設定 AWS Control Tower。

適用於 VPC 和 AWS Control Tower 的 CIDR 和對等互連

本節主要供網路管理員使用。您公司的網路管理員通常是為 AWS Control Tower 組織選擇整體 CIDR 範圍的人員。網路管理員之後會因特定目的，從該範圍內配置子網路。

當您為 VPC 選擇 CIDR 範圍時，AWS Control Tower 會根據 RFC 1918 規格驗證 IP 地址範圍。Account Factory 允許 CIDR 區塊達到/16以下範圍：

- `10.0.0.0/8`
- `172.16.0.0/12`
- `192.168.0.0/16`
- `100.64.0.0/10`（僅當您的互聯網提供商允許使用此範圍時）

/16 分隔符號允許多達 65,536 個不同的 IP 位址。

您可以從下列範圍指派任何有效的 IP 位址：

- `10.0.x.x to 10.255.x.x`
- `172.16.x.x - 172.31.x.x`
- `192.168.0.0 - 192.168.255.255`（沒有超出 192.168 範圍的 IP）

如果您指定的範圍超出這些範圍，AWS Control Tower 會提供錯誤訊息。

預設 CIDR 範圍為 `172.31.0.0/16`。

當 AWS Control Tower 使用您選取的 CIDR 範圍建立 VPC 時，會為您在組織單位 (OU) 內建立的每個帳戶指派相同的 CIDR 範圍給每個 VPC。由於 IP 地址的預設重疊，此實作一開始不允許在 OU 中的任何 AWS Control Tower VPC 之間進行對等互連。

子網

在每個 VPC 中，AWS Control Tower 會將您指定的 CIDR 範圍平均劃分為九個子網路 (美國西部 (加利佛尼亞北部) 除外，其中有六個子網路)。VPC 內沒有任何子網路重疊。因此，它們都可以在 VPC 內相互通信。

總而言之，根據預設，VPC 內的子網路通訊不受限制。必要時，控制 VPC 子網路之間通訊的最佳實務，就是使用定義允許之流量的規則設定存取控制清單。使用安全群組來控制特定執行個體之間的流量。如需在 AWS Control Tower 中設定安全群組和防火牆的詳細資訊，請參閱逐步解說：使用 AWS Firewall Manager 員在 AWS Control Tower 中設定安全群組。

對等互連

AWS Control Tower 不會限制 VPC 到 VPC 的對等互連，以便在多個 VPC 之間進行通訊。不過，依預設，所有 AWS Control Tower VPC 都具有相同的預設 CIDR 範圍。若要支援對等互連，您可以在 Account Factory 的設定中修改 CIDR 範圍，讓 IP 位址不會重疊。

如果您在 Account Factory 的設定中變更 CIDR 範圍，AWS Control Tower Town 隨後建立的所有新帳戶 (使用 Account Factory) 都會指派新的 CIDR 範圍。舊帳戶不會更新。例如，您可以建立一個帳戶，然後變更 CIDR 範圍並建立新的帳戶，並互連配置給這兩個帳戶的 VPC。由於其 IP 地址範圍並不相同，因此可以互連。

必要的角色和許可

AWS Control Tower 使用 IAM 角色來協助管理資源的存取。

如需有關角色的一般資訊，請參閱使用者群組、角色和權限集。

關於許可

- 如需 AWS Control Tower 中 IAM 群組及其許可的相關資訊，請參閱 AWS Control Tower 的 IAM 身分中心群組。
- 如需佈建帳戶所需權限的相關資訊，請參閱帳戶所需的權限。
- 有關 AWS Control Tower 所需的主控台許可的詳細資訊，請參閱使用 AWS Control 塔主控台所需的許可。

關於角色

- 有關如何建立角色的資訊 (包括專為程式設計存取設計的許可)，請參閱建立角色和指派許可，以及 AWS Control Tower 稽核帳戶的程式化角色和信任關係。
- 有關 AWS Control Tower 用於管理帳戶的其他角色的資訊，請參閱 AWS Control Tower 使用身分型政策 (IAM 政策) 和 AWS Control Tower 的受管政策。
- 如需 AWS Control Tower 和 AWS Config 角色的相關資訊，請參閱 AWS Control Tower ConfigRecorderRole。
- 如需 AWS Control Tower 用來彙總帳戶資訊之角色的相關 AWS Config 資訊，請參閱 AWS Control Tower 如何彙總非受管 OU 和帳戶中的 AWS Config 規則。
- 如需如何在指派角色和權限時保護資源的詳細資訊，請參閱角色信任關係的選擇性條件、選擇性地設定 AWS KMS 金鑰和防止跨服務模擬。
- 有關使用 IAM 角色在 AWS Control Tower 中自動化帳戶佈建的特定資訊，請參閱使用 IAM 角色自動化帳戶佈建。
- 若要檢視保護 AWS Config SNS 主題的原則，請參閱 AWS Config SNS 主題政策。

AWS Control Tower 如何與角色搭配建立和管理帳戶

一般而言，角色是中身分識別與存取管理 (IAM) 的一部分 AWS。有關 IAM 和角色的一般資訊 AWS，請參閱 IAM 使用者指南中的AWS IAM 角色主題。

角色和帳戶建立

AWS Control Tower 透過呼叫的 `CreateAccount` API 來建立客戶的帳戶 AWS Organizations。 AWS Organizations 建立此帳戶時，會在該帳戶內建立角色，AWS Control Tower 會透過將參數傳入 API 來命名該角色。角色的名稱是 `AWSControlTowerExecution`。

AWS Control Tower 接管 Account Factory 建立的所有帳戶的`AWSControlTowerExecution`角色。AWS Control Tower 使用此角色時，會對帳戶進行基準化，並套用強制性 (以及任何其他已啟用) 控制，進而建立其他角色。這些角色依次被其他服務使用，例如 AWS Config。

> **Note**
>
> 基準帳戶是設定其資源，其中包括 Account Factory 範本 (有時稱為藍圖) 和控制項。基準處理程序也會在帳戶上設定集中式記錄和安全性稽核角色，做為部署範本的一部分。AWS Control Tower 基準包含在您套用至每個註冊帳戶的角色中。

如需帳號和資源的詳細資訊，請參閱關 AWS 帳戶 於 AWS Control Tower。

AWSControlTowerExecution 角色，解釋

所有已註冊的帳戶中都必須存在有 `AWSControlTowerExecution` 角色。它可讓 AWS Control Tower 管理您的個別帳戶，並將其相關資訊報告給稽核和日誌存檔帳戶。

您可以透過數種方式將`AWSControlTowerExecution`角色新增至帳戶，如下所示：

- 對於安全 OU 中的帳戶 (有時稱為核心帳戶)，AWS Control Tower 會在初始 AWS Control Tower 設定時建立角色。
- 對於透過 AWS Control 塔主控台建立的 Account Factory 帳戶，AWS Control Tower 會在帳戶建立時建立此角色。
- 對於單一帳戶註冊，我們要求客戶手動建立角色，然後在 AWS Control Tower 註冊帳戶。
- 將管理擴展到 OU 時，AWS Control Tower 會使用 StackSet-AWSControlTowerExecutionRole 在該 OU 中的所有帳戶中建立角色。

`AWSControlTowerExecution`角色的目的：

- `AWSControlTowerExecution`可讓您使用指令碼和 Lambda 函數自動建立和註冊帳戶。

- AWSControlTowerExecution 可協助您設定組織的日誌記錄，以便將每個帳戶的所有日誌傳送至日誌帳戶。
- AWSControlTowerExecution可讓您在 AWS Control Tower 中註冊個別帳戶。首先，您必須將AWSControlTowerExecution角色新增至該帳戶。如需如何新增角色的步驟，請參閱手動將所需的 IAM 角色新增至現有角色 AWS 帳戶 並註冊。

此AWSControlTowerExecution角色如何與 OU 搭配運作：

該AWSControlTowerExecution角色可確保您選取的 AWS Control Tower 控制項會自動套用到組織中的每個個別帳戶、每個 OU，以及您在 AWS Control Tower 中建立的每個新帳戶。因此：

- 您可以根據 AWS Control Tower 控制所包含的稽核和記錄功能，更輕鬆地提供合規和安全報告。
- 您的安全及合規團隊可以確認所有要求都符合，而且沒有發生任何組織偏離。

如需有關漂移的詳細資訊，請參閱在 AWS Control Tower 中偵測和解決漂移。

總而言之，AWSControlTowerExecution 角色及其相關政策可讓您彈性地控制整個組織的安全與合規。因此，違反安全性或通訊協定的可能性較小。

角色信任關係的選擇性條件

您可以在角色信任政策中施加條件，以限制與 AWS Control Tower 中特定角色互動的帳戶和資源。強烈建議您限制AWSControlTowerAdmin角色的存取權，因為它允許廣泛的存取權限。

為協助防止攻擊者取得您資源的存取權，請手動編輯 AWS Control Tower 信任政策，在政策聲明中至少新增一個aws:SourceArn或aws:SourceAccount條件式。作為安全性最佳作法，我們強烈建議您新增aws:SourceArn條件，因為它比aws:SourceAccount限制對特定帳號和特定資源的存取更具體。

如果您不知道資源的完整 ARN，或者您要指定多個資源，則可以使用
帶有萬用字元 (*) 的aws:SourceArn條件來表示 ARN 的未知部分。例
如，arn:aws:controltower:*:123456789012:*如果您不希望指定「區域」，則可以使用。

下列範例示範如何將 aws:SourceArn IAM 條件與 IAM 角色信任政策搭配使用。
在AWSControlTowerAdmin角色的信任關係中新增條件，因為 AWS Control Tower 服務主體會與其互動。

如範例所示，來源 ARN 的格式如
下：arn:aws:controltower:*${HOME_REGION}*:*${CUSTOMER_AWSACCOUNT_id}*:*

替換字符串${HOME_REGION}並${CUSTOMER_AWSACCOUNT_id}使用您自己的主區域和呼叫帳戶的帳戶 ID。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "controltower.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:controltower:us-west-2:012345678901:*"
        }
      }
    }
  ]
}
```

在此範例中，指定為的來源 ARN arn:aws:controltower:us-west-2:012345678901:* 是唯一允許執行動作的 ARN。sts:AssumeRole換句話說，只有能夠在us-west-2區域中登入帳戶 ID 012345678901 的使用者才能執行需要此特定角色和信任關係的 AWS Control Tower 作 (指定為) controltower.amazonaws.com。

下一個範例顯示套用至角色信任原則的aws:SourceAccount和aws:SourceArn條件。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "controltower.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
```

```
        "StringEquals": {
          "aws:SourceAccount": "012345678901"
        },
        "StringLike": {
          "aws:SourceArn": "arn:aws:controltower:us-west-2:012345678901:*"
        }
      }
    }
  ]
}
```

此範例說明了aws:SourceArn條件陳述式，並附加了aws:SourceAccount條件陳述式。如需詳細資訊，請參閱 防止跨服務模擬。

如需 AWS Control Tower 中許可政策的一般資訊，請參閱管理資源存取。

建議：

建議您在 AWS Control Tower 建立的角色中新增條件，因為這些角色直接由其他 AWS 服務承擔。如需詳細資訊，請參閱本節先前所示的範例。AWSControlTowerAdmin對於 AWS Config 記錄器角色，我們建議新增aws:SourceArn條件，並將 Config 定記錄程式 ARN 指定為允許的來源 ARN。

對於 AWS Control Tower Audit 帳戶在所有受管帳戶中可承擔的角色AWSControlTowerExecution或其他程式設計角色，建議您將aws:PrincipalOrgID條件新增至這些角色的信任政策，以驗證存取資源的主體是否屬於正確 AWS 組織中的帳戶。請勿新增aws:SourceArn條件陳述式，因為它無法如預期般運作。

> **Note**
>
> 在漂移的情況下，可能會在特定情況下重設 AWS Control Tower 角色。如果您已自訂角色，建議您定期重新檢查角色。

AWS Control Tower 如何彙總非受管 OU 和帳戶中的 AWS Config 規則

AWS Control Tower 管理帳戶可建立組織層級彙總工具，協助偵測外部 AWS Config 規則，因此 AWS Control Tower 不需要取得未受管帳戶的存取權。AWS Control Tower 主控台會顯示指定帳戶的外部建立 AWS Config 規則數量。您可以在「帳戶詳細資料」頁面的「外部 Config 規則符合性」標籤中檢視這些外部規則的詳細資訊。

為了建立彙總工具，AWS Control Tower 會新增一個角色，其中包含描述組織並列出其下帳戶所需的許可。AWSControlTowerConfigAggregatorRoleForOrganizations角色需要AWSConfigRoleForOrganizations受管理的原則以及與的信任關係config.amazonaws.com。

以下是附加到該角色的 IAM 政策（JSON 成品）：

```
{
    "Version": "2012-10-17",
      "Statement": [
       {
        "Effect": "Allow",
        "Action": [
          "organizations:ListAccounts",
          "organizations:DescribeOrganization",
          "organizations:ListAWSServiceAccessForOrganization"
         ],
       "Resource": "*"
      }
    ]
  }
```

這是AWSControlTowerConfigAggregatorRoleForOrganizations信任關係：

```
{
    "Version": "2012-10-17",
      "Statement": [
      {
        "Effect": "Allow",
        "Principal": {
        "Service": "config.amazonaws.com"
        },
        "Action": "sts:AssumeRole"
      }
    ]
  }
}
```

若要在管理帳戶中部署此功能，受管理的策略會新增下列權限AWSControlTowerServiceRolePolicy，這些權限會在建立 AWS Config 彙總器時由AWSControlTowerAdmin角色使用：

```
{
  "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
          "config:PutConfigurationAggregator",
          "config:DeleteConfigurationAggregator",
          "iam:PassRole"
          ],
        "Resource": [
          "arn:aws:iam:::role/service-role/
AWSControlTowerConfigAggregatorRoleForOrganizations",
          "arn:aws:config:::config-aggregator/"
          ]
        },
      {
        "Effect": "Allow",
        "Action": "organizations:EnableAWSServiceAccess",
        "Resource": "*"
      }
    ]
}
```

已建立的新資源：AWSControlTowerConfigAggregatorRoleForOrganizations和 aws-controltower-ConfigAggregatorForOrganizations

準備就緒後，您可以個別註冊帳戶，或透過註冊 OU 將其註冊為群組。註冊帳戶後，如果您在中建立規則 AWS Config，AWS Control Tower 會偵測到新規則。彙總器會顯示外部規則的數量，並提供 AWS Config 主控台連結，您可以在其中檢視帳戶的每個外部規則的詳細資料。使用主控 AWS Config 台和 AWS Control Tower 主控台中的資訊，判斷是否已為該帳戶啟用適當的控制項。

AWS Control Tower 稽核帳戶的程式化角色和信任關係

您可以登入稽核帳戶，並擔任以程式設計方式檢閱其他帳戶的角色。稽核帳戶不允許您手動登入其他帳戶。

稽核帳戶只會授與 AWS Lambda 函數的某些角色，讓您以程式設計方式存取其他帳戶。為了安全起見，這些角色與其他角色具有信任關係，這意味著可以使用角色的條件是嚴格定義的。

AWS Control Tower 堆疊集StackSet-AWSControlTowerBP-BASELINE-ROLES會在稽核帳戶中建立下列僅限程式設計的跨帳戶角色：

- AWS-控制塔-AdministratorExecutionRole
- AWS-控制塔-AuditAdministratorRole
- AWS-控制塔-ReadOnlyExecutionRole
- AWS-控制塔-AuditReadOnlyRole

ReadOnlyExecutionRole:請注意，此角色可讓稽核帳戶讀取整個組織中 Amazon S3 儲存貯體中的物件 (與政策相反，該SecurityAudit政策僅允許中繼資料存取)。

AWS-控制塔-: AdministratorExecutionRole

- 具有管理員權限
- 無法從控制台假定
- 只能由稽核帳戶中的角色假設 — aws-controltower-AuditAdministratorRole

下列人工因素顯示的信任關係aws-controltower-AdministratorExecutionRole。預留位置編號012345678901將由您稽核帳戶的Audit_acct_ID編號取代。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/aws-controltower-AuditAdministratorRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

AWS-控制塔-: AuditAdministratorRole

- 只能由 AWS Lambda 服務假設
- 有權在名稱以字串日誌開頭的 Amazon S3 物件上執行讀取 (取得) 和寫入 (放入) 操作

附加政策：

1. AWSLambdaExecute— AWS 受管理策略

2. AssumeRole-aws-Control 塔 AuditAdministratorRole — 內嵌政策 — 由 AWS Control Tower 建立，工件如下。

```
{
  "Version": "2012-10-17",
  "Statement": [
 {
 "Action": [
   "sts:AssumeRole"
   ],
 "Resource": [
   "arn:aws:iam::*:role/aws-controltower-AdministratorExecutionRole"
   ],
 "Effect": "Allow"
 }
   ]
}
```

下列人工因素顯示的信任關係aws-controltower-AuditAdministratorRole：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

AWS-控制塔-: ReadOnlyExecutionRole

- 無法從控制台假定
- 只能由稽核帳戶中的另一個角色假設 — AuditReadOnlyRole

下列人工因素顯示的信任關係aws-controltower-ReadOnlyExecutionRole。預留位置編號012345678901將由您稽核帳戶的Audit_acct_ID編號取代。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/aws-controltower-AuditReadOnlyRole "
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

AWS-控制塔-: AuditReadOnlyRole

- 只能由 AWS Lambda 服務假設
- 有權在名稱以字串日誌開頭的 Amazon S3 物件上執行讀取 (取得) 和寫入 (放入) 操作

附加政策：

1. AWSLambdaExecute— AWS 受管理策略

2. AssumeRole-aws-Control 塔 AuditReadOnlyRole — 內嵌政策 — 由 AWS Control Tower 建立，工件如下。

```
{
  "Version": "2012-10-17",
  "Statement": [
 {
 "Action": [
  "sts:AssumeRole"
 ],
 "Resource": [
  "arn:aws:iam::*:role/aws-controltower-ReadOnlyExecutionRole"
 ],
 "Effect": "Allow"
   }
  ]
}
```

下列人工因素顯示的信任關係`aws-controltower-AuditAdministratorRole`：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

使用 IAM 角色自動帳戶佈建

若要以更自動化的方式設定 Account Factory 帳戶，您可以在 AWS Control Tower Tall 管理帳戶中建立 Lambda 函數，該帳戶擔任該成員帳戶中的AWSControlTowerExecution角色。然後，管理帳戶會使用角色在每個成員帳戶中執行所需的設定步驟。

如果您使用 Lambda 函數佈建帳戶，則執行此工作的身分識別除了還必須具有下列 IAM 許可政策AWSServiceCatalogEndUserFullAccess。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSControlTowerAccountFactoryAccess",
            "Effect": "Allow",
            "Action": [
                "sso:GetProfile",
                "sso:CreateProfile",
                "sso:UpdateProfile",
                "sso:AssociateProfile",
                "sso:CreateApplicationInstance",
                "sso:GetSSOStatus",
                "sso:GetTrust",
                "sso:CreateTrust",
                "sso:UpdateTrust",
                "sso:GetPeregrineStatus",
                "sso:GetApplicationInstance",
                "sso:ListDirectoryAssociations",
                "sso:ListPermissionSets",
```

```
                "sso:GetPermissionSet",
                "sso:ProvisionApplicationInstanceForAWSAccount",
                "sso:ProvisionApplicationProfileForAWSAccountInstance",
                "sso:ProvisionSAMLProvider",
                "sso:ListProfileAssociations",
                "sso-directory:ListMembersInGroup",
                "sso-directory:AddMemberToGroup",
                "sso-directory:SearchGroups",
                "sso-directory:SearchGroupsWithGroupName",
                "sso-directory:SearchUsers",
                "sso-directory:CreateUser",
                "sso-directory:DescribeGroups",
                "sso-directory:DescribeDirectory",
                "sso-directory:GetUserPoolInfo",
                "controltower:CreateManagedAccount",
                "controltower:DescribeManagedAccount",
                "controltower:DeregisterManagedAccount",
                "s3:GetObject",
                "organizations:describeOrganization",
                "sso:DescribeRegisteredRegions"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS Control Tower Account Factory 需要許sso:GetPeregrineStatus可sso:ProvisionApplicationProfileForAWSAccountInstance、和sso:ProvisionSAMLProvide才能與 AWS IAM 身分中心互動。sso:ProvisionApplicationInstanceForAWSAccount

AWS Control Tower 中的資源

- 如需 AWS Control Tower 中資源擁有權的一般資訊，請參閱管理 AWS Control Tower 資源存取許可的概觀。
- 如需 AWS Control Tower 在共用帳戶中建立的資源的相關資訊，請參閱關於共享帳戶。
- 如需 AWS Control Tower 在透過 Account Factory 佈建帳戶時所建立的資源的相關資訊，請參閱Account Factory 的資源考量。
- 若要檢視 AWS Control Tower 所定義之 AWS 資源類型的詳細資訊，以搭配 AWS Control Tower API 使用，請參閱使用AWS CloudFormation 者指南中的 AWS Control Tower 資源類型參考。

AWS 區域如何與 AWS Control Tower 搭配使用

目前，下列 AWS 區域支援 AWS Control Tower：

- 美國東部 (維吉尼亞北部)
- 美國東部 (俄亥俄)
- 美國西部 (奧勒岡)
- 加拿大 (中部)
- 亞太區域 (悉尼)
- 亞太區域 (新加坡)
- 歐洲 (法蘭克福)
- 歐洲 (愛爾蘭)
- 歐洲 (倫敦)
- 歐洲 (斯德哥爾摩)
- 亞太區域 (孟買)
- 亞太區域 (首爾)
- 亞太區域 (東京)
- Europe (Paris)
- 南美洲 (聖保羅)
- 美國西部 (加利佛尼亞北部)
- 亞太區域 (香港)
- 亞太區域 (雅加達)
- 亞太區域 (大阪)
- 歐洲 (米蘭)
- 非洲 (開普敦)
- Middle East (Bahrain)
- 以色列 (特拉維夫)
- 中東 (阿拉伯聯合大公國)
- 歐洲 (西班牙)
- 亞太區域 (海德拉巴)

- 歐洲 (蘇黎世)
- 亞太區域 (墨爾本)
- 加拿大西部 (卡加利)

關於您的家鄉地區

建立 landing zone 域時，用於存取 AWS 管理主控台的區域會成為 AWS Control Tower 的主 AWS 區域。在建立程序期間，會在主區域中佈建一些資源。其他資源 (例如 OU 和 AWS 帳戶) 是全域的。

選取主地區後，就無法變更它。

控制項和區域

目前，所有的預防性控制在全球範圍內 不過，Detective 和主動控制僅適用於支援 AWS Control Tower 的區域。如需在新區域中啟用 AWS Control 塔時控制項行為的詳細資訊，請參閱設定您的 AWS Control Tower 區域。

設定您的 AWS Control Tower 區域

本節說明將 AWS Control Tower 登陸區域擴展到新區 AWS 域，或從登陸區域組態中移除區域時，可預期的行為。一般而言，此動作是透過 AWS Control 塔主控台的更新功能執行。

> **Note**
>
> 建議您避免將 AWS Control Tower landing zone 擴展到不需要執行工作負載的區 AWS 域。選擇退出某個區域並不會阻止您在該區域部署資源，但這些資源仍不在 AWS Control Tower 管理範圍之外。

在設定新區域期間，AWS Control Tower 會更新 landing zone 域，這表示它會基準您的 landing zone 域 —

- 在所有新選取的區域中積極運作，以及
- 停止管理取消選定區域的資源。

由 AWS Control Tower 管理的組織單位 (OU) 中的個別帳戶不會作為此 landing zone 更新程序的一部分進行更新。因此，您必須重新註冊 OU 來更新您的帳戶。

設定 AWS Control Tower 區域時，請注意以下建議和限制：

- 選取您計劃在其中託管 AWS 資源或工作負載的區域。
- 選擇退出某個區域並不會阻止您在該區域部署資源，但這些資源仍不在 AWS Control Tower 管理範圍之外。

為新區域設定 landing zone 域時，AWS Control Tower 偵測控制會遵守下列規則：

- 已存在的項目保持不變。現有區域、現有 OU 中現有帳戶的偵測性和預防性護欄行為不會變更。
- 您無法將新的偵探控制套用至包含未更新帳戶的現有 OU。將 AWS Control Tower 登陸區域設定為新區域後 (透過更新您的 landing zone 域)，您必須先更新現有 OU 中的現有帳戶，才能在這些 OU 和帳戶上啟用新的偵探控制。
- 一旦您更新帳戶，您現有的偵測控制項就會在新設定的「區域」中開始運作。當您更新 AWS Control Tower landing zone 域以設定新區域，然後更新帳戶時，OU 上已啟用的偵探控制將開始在新設定的區域中使用該帳戶。

設定 AWS Control Tower 區域

1. 登入 AWS Control Tower 主控台，網址為：https://console.aws.amazon.com/controltower
2. 在左窗格導覽功能表中，選擇「著陸區域設定」。
3. 在「登陸區域設定」頁面的「詳細資料」區段中，選擇右上角的 「修改設定」按鈕。系統會將您導向至更新 landing zone 域工作流程，因為管理新的區域或從治理中移除區域，都需要您更新為最新的 landing zone 域版本。
4. 在 [其他 AWS 區域進行治理] 下方，搜尋您要管理 (或停止管理) 的區域。「狀態」(State) 欄會指出您目前管理的區域，以及哪些區域不管理。
5. 勾選要管理的其他每個區域的核取方塊。取消選取您要移除控管的每個區域的核取方塊。

> **Note**
>
> 如果您選擇不管理某個區域，您仍然可以在該區域部署資源，但這些資源將保留在 AWS Control Tower 管理之外。

6. 完成工作流程的其餘部分，然後選擇「更新 landing zone 域」。
7. 當 landing zone 域設定完成時，請重新註冊 OU 以更新新區域中的帳戶。如需詳細資訊，請參閱何時更新 AWS Control Tower OU 和帳戶。

在設定新區域之後，另一種佈建或更新個別帳戶的方法是使用 Service Catalog 的 API 架構，並在批次程序中更新帳戶。 AWS CLI如需詳細資訊，請參閱 使用自動化佈建和更新帳戶。

設定區域時避免混合控管

將 AWS Control Tower 管理擴展到新的管理之後，以及從區域移除 AWS Control Tower 管理後 AWS 區域，請務必更新 OU 中的所有帳戶。

如果管理 OU 的控制項與管理 OU 中每個帳戶的控制項不完全相符，則可能會發生混合治理是不希望的情況。如果 AWS Control Tower 將管理擴展到新的管理或移除管理之後，帳戶未更新 AWS 區域，則會在 OU 中發生混合控管。

在此情況下，OU 中的某些帳戶可能會在不同的區域中套用不同的控制項，與 OU 中的其他帳戶相比，或與著陸區域的整體控管狀態相比。

在具有混合治理的 OU 中，如果您佈建新帳戶，則該新帳戶會收到與登陸區域相同 (已更新) 的區域和 OU 控管狀態。不過，尚未更新的現有帳號不會收到更新的區域控管狀態。

一般而言，混合管理可能會在 AWS Control Tower 主控台中建立矛盾或不正確的狀態指標。例如，在混合治理期間，對於尚未更新的帳戶，在已註冊 OU 中，選擇加入區域會顯示為「未受控管」狀態。

> **Note**
>
> AWS Control Tower 不允許在混合管理狀態期間啟用控制。

混合治理期間的控制項行為

- 在混合控管期間，AWS Control Tower 無法在 OU 已顯示為受控管的區域中一致地部署以 AWS Config 規則 (亦即偵探控制) 為基礎的控制，因為 OU 中的某些帳戶尚未更新。您可能會收到`FAILED_TO_ENABLE`錯誤訊息。
- 在混合治理期間，如果您將登陸區域的治理延伸至選擇加入區域，而 OU 中的任何帳戶尚未更新，則 OU 上的 `EnableControl` API 作業會因偵探和主動控制而失敗。您會收到`FAILED_TO_ENABLE`錯誤訊息，因為 OU 中未更新的成員帳戶尚未選擇加入這些區域。
- 在混合控管期間，屬於安全中心服務管理標準的一部分的控制：AWS Control Tower 無法在登陸區域組態與未更新帳戶不相符的區域準確報告合規。
- 混合治理不會變更以 SCP 為基礎的控制項 (預防性控制) 的行為，這些控制項會統一套用至每個受控區域中 OU 中的每個帳戶。

> **Note**
>
> 混合治理與漂移不同，並且不報告為漂移。

若要修復混合治理

- 在主控台的 [Organ izations] 頁面上，針對 OU 中顯示 [可用更新] 狀態的每個帳戶選擇 [更新帳戶]。
- 在 [Organ izations] 頁面上選擇 [重新註冊 OU]，該頁面會針對擁有少於 300 個帳戶的 OU 自動更新 OU 中的所有帳戶。

啟用 AWS 選擇加入區域的注意事項

雖然大部分 AWS 區域 區域預設為使用中狀態 AWS 帳戶，但只有當您手動選取某些區域時，才會啟用。本文件將這些區域稱為選擇加入區域。相比之下，默認情況下處於活動狀態的區域，一旦您 AWS 帳戶 創建，就被稱為商業區域，或者簡稱為「區域」。

選擇加入一詞具有歷史基礎。在 2019 年 3 月 20 日之後 AWS 區域 推出的任何內容都被視為選擇加入區域。選擇加入區域比商業區域具有更高的安全要求，因為透過在選擇加入區域中有效的帳戶共用 IAM 資料。透過 IAM 服務管理的所有資料都被視為身分識別資料，包括使用者、群組、角色、政策、身分識別提供者、其關聯資料 (例如 X.509 簽署憑證或內容特定登入資料)，以及其他帳戶層級設定，例如密碼政策和帳戶別名。

您可以在設定 landing zone 域時自動啟用選擇加入的區域，方法是選取這些區域。您的 landing zone 域會在所有選取的區域中啟用。

如果您選擇選擇加入區域作為 AWS Control Tower 本地區域，請先按照登入 AWS 管理主控台時啟用區域中的步驟啟用該區域。若要從選擇加入的區域使用您自己現有的記錄封存和稽核帳戶，請先手動啟用該區域。

AWS 選擇加入的區域包括可使用 AWS Control Tower 的數個區域：

- 亞太區域 (香港) 地區，ap-east-1
- 亞太 (雅加達) 地區，ap-southeast-3
- 歐洲 (米蘭) 地區，eu-south-1
- 非洲（開普敦）地區，af-south-1
- 中東（巴林）區域，me-south-1
- 以色列（特拉維夫），il-central-1

- 中東（阿拉伯聯合酋長國）區域，me-central-1
- 歐洲 (西班牙) 地區，eu-south-2
- 亞太區域 (海德拉巴)，ap-south-2
- 歐洲（蘇黎世）區域，eu-central-2
- 亞太區域 (墨爾本) 地區，ap-southeast-4
- 加拿大西部 (卡加利) 地區，ca-west-1

AWS Control Tower 的某些控制項在選擇加入區域中的運作方式與商業區域的運作方式不同。如需詳細資訊，請參閱 控制限制。當您將工作負載部署到選擇加入區域時，請記住以下幾點考量事項。

> **管理或激活？**
>
> 請記住，管理區域是您可以從 AWS Control Tower 主控台選取的動作，以便在該區域套用控制項。啟用或停用選擇加入「區域」是您可以在 AWS 主控台中選擇的另一個動作，它會向您的帳戶開啟「區域」，以便您可以在區域中部署資源和工作負載。

行為考量事項

- 如果您選擇管理選擇加入區域，我們建議您不要停用 (選擇退出) 任何受控管的選擇加入區域，因為這可能會導致工作負載失敗。AWS Control Tower 不允許在 AWS Control Twer 主控台內停用受管轄區域，但請確保您不會停用 AWS Control Tall 以外的來源 (例如 AWS 帳單主 AWS Control Tower 或 AWS 開發套件) 的受管轄區域。
- 當 AWS Control Tower 將管理擴展到選擇加入的區域時，它會在所有成員帳戶中啟用 (選擇加入) 該區域。當您從管理中移除區域時，AWS Control Tower 不會停用 (選擇退出) 成員帳戶中的區域。
- 在區域取消選擇期間，如果從 AWS Control Tower 外部的來源 (例如帳 AWS 單主控台或開發套件) 的帳戶手動停用該區域，則 AWS Control Tower 會略過從選擇加入區域移除該區域的資源。 AWS 我們建議您從已停用的區域移除資源，否則可能會收到這些資源的非預期帳單費用。
- 如果您的 landing zone 域停用，AWS Control Tower 會清除所有受管轄區域的資源，包括選擇加入的區域。不過，AWS Control Tower 不會停用選擇加入區域。解除委任後，您可以停用選擇加入的區域作為其他步驟。
- 如果您的主地區域是選擇加入的區域，而且您打算將現有帳戶註冊為記錄封存和稽核帳戶，則必須手動啟用選擇加入的區域，然後才能將其選取為登陸區域的主地區域。請參閱啟用區域。
- 如果 AWS Control Tower 設定為選擇加入區域作為您的主區域，而且如果您從任何其他區域的主控 AWS 台造訪 AWS Control Tower 服務，則主控台不會自動將您重新導向至主區域。

- 基礎 API 具有容量限制，這可能會將延遲時間從幾分鐘增加到數小時，具體取決於區域數量，帳戶和服務負載。最佳做法是，只選擇加入您要執行工作負載的位 AWS 區域 置，並一次選擇加入一個區域。

治理和控制的重要限制

- 如果您目前已啟用選擇加入區域不支援的 AWS Control Tower Control Tall 控制，則在該區域支援該控制之前，您將無法將 AWS Control Tall 管理擴展到該選擇加入區域。如需更多資訊，請參閱控制限制。
- 如果您將 AWS Control Tower 管理延伸到不支援特定控制項的選擇加入區域，則在您使用 AWS Control Tower 管理的所有區域都支援該控制項之前，您將無法在任何區域啟用該控制項。如需詳細資訊，請參閱 控制限制
- 如果 AWS Control Tower 提供的所有 22 個商業區域均已啟用 (包括選擇加入區域)，則在將管理擴展到 OU 時，每個組織單位 (OU) 的帳戶數量上限將會降低。限制是 220 個，而不是 300 個帳戶。這種減少是由於 StackSet限制。如果您需要將控管擴展到擁有 220 個帳戶以上的 OU，請減少啟動區域的數量。

設定區域拒絕控制

AWS Control Tower 提供兩種區域拒絕控制。啟用時GRREGIONDENY，一個控制項會套用至整個 landing zone。另一個控制項 (啟動時) 可套用至您指定的特定 OU。CTMULTISERVICEPV1如需詳細資訊，請參閱拒絕 AWS 根據要求的存取權限 AWS 區域和套用至 OU 的區域拒絕控制。

區域拒絕控制GRREGIONDENY是唯一的，因為它會套用至整體的 landing zone 域，而不是任何特定的 OU。若要設定區域拒絕控制，請前往「著陸區設定」頁面，然後選取「修改設定」。

- 您可以稍後變更此設定。
- 啟用時，此控制項會套用至所有已註冊的 OU。
- 無法針對個別 OU 設定此控制項。

> **Note**
>
> 啟用「區域」拒絕控制之前，請確定這些區域中沒有現有的資源，因為套用控制項之後，您將無法存取資源。啟用控制項後，您將無法在拒絕的區域中部署資源。

區域拒絕控制會根據您的 AWS Control Tower 區域組態禁止存取 AWS 服務。它會拒絕存取狀態為「未受管理」的 AWS 區域。區域拒絕控制也會拒絕存取無法使用 AWS Control Tower 的區域。您無法拒絕存取您的家居區域。某些全球 AWS 服務 (例如 IAM 和 AWS Organizations) 免於區域拒絕控制。若要深入瞭解，請參閱AWS 根據要求拒絕存取 AWS 區域。

當您啟用控制項時，它會套用至階層中所有已註冊的最上層 OU，而且它會由鏈結中較低的 OU 繼承。移除控制時，所有已註冊 OU 上的控制項都會移除，AWS Control Tower 中的所有非受管理區域都會維持「不受控管」狀態，而且您可以在 AWS Control Tower 可用性以外的區域部署資源。

- 完整控制名稱： AWS 根據要求的 AWS 區域拒絕存取
- 護欄說明：禁止訪問指定區域以外的全球和區域服務中的非上市業務。
- 這是具有預防性指導的選修控制。

若要檢視區域拒絕控制 SCP 的範本，請參閱AWS 根據 AWS Control Tower 控制參考 AWS 區域中的要求拒絕存取。AWS Control Tower SCP 類似於 SCP AWS Organizations，但不完全相同。

您可以在 [區域服務] 頁面上判斷區域服務端點。

歐盟層級區域拒絕控制的考量

歐盟層級區域拒絕控制的主要考量，是決定如果兩者都啟動，它將如何與 landing zone 域拒絕控制互動。如需詳細資訊，請參閱套用至 OU 的區域拒絕控制。

在 AWS Control Tower 中佈建和管理帳戶

本章包含在 AWS Control Tower landing zone 中佈建和管理成員帳戶的概觀和程序。

其中也包含將現有 AWS 帳戶註冊到 AWS Control Tower 的概觀和程序。

如需 AWS Control Tower 中帳戶的詳細資訊，請參閱關 AWS 帳戶 於 AWS Control Tower。如需將多個帳戶註冊到 AWS Control Tower 的相關資訊，請參閱。向 AWS Control Tower 註冊現有的組織單位

> **Note**
>
> 您最多可同時執行五 (5) 項與帳戶相關的作業，包括佈建、更新和註冊。

佈建方法

AWS Control Tower 提供多種建立和更新成員帳戶的方法。有些方法主要是基於控制台的，有些方法主要是自動化的。

概觀

建立成員帳戶的標準方式是透過 Account Factory，這是 Service Catalog 一部分的主控台型產品。如果您的 landing zone 非處於漂移狀態，您可以使用 Create 帳戶做為從主控台新增帳戶的方法，也可以使用註冊帳戶將現有 AWS 帳戶註冊到 AWS Control Tower。

透過 Account Factory，您可以依賴 AWS Control Tower 預設設定來佈建基本帳戶。您也可以佈建符合特殊使用案例需求的自訂帳戶。

Account Factory 自訂 (AFC) 是從 AWS Control Tower 主控台佈建自訂帳戶的一種方式，可自動化帳戶的自訂和部署。它允許在一些單次設置步驟後基於控制台的自動佈建，從而無需編寫腳本或設置管道。如需詳細資訊，請參閱 使用 Account Factory 定制（AFC）自定義帳戶。

基於控制台的方法：

- 透過屬於基本或自訂帳戶之一部分的 AWS Service Catalog Account Factory 主控台。檢閱使用 Account Factory 佈建和管理帳戶詳細資訊和指示。
- 如果您的 landing zone 域不處於漂移狀態，請透過 AWS Control Tower 內的註冊帳戶功能。請參閱註冊現有帳戶。

- 在 AWS Control Tower 主控台中，您可以使用 Account Factory 同時建立、更新或註冊最多五個帳戶。

自動化方法：

- Lambda 程式碼：從您的 AWS Control Tower 登陸區域的管理帳戶，使用 Lambda 程式碼和適當的 IAM 角色。請參閱使用 IAM 角色自動化帳戶佈建。
- Terraform：來自適用於 Terraform 的 AWS Control Tower Account Factory (AFT)，該工廠依賴 Account Factory 和 GitOps 模型來自動化帳戶佈建和更新。請參閱 使用 AWS Control Tower Account Factory 為地形 (AFT) 佈建帳戶 。
- AWS Control Tower 主控台中的 Account Factory 自訂：完成設定步驟後，future 佈建自訂帳戶不需要額外的組態或管道維護。帳戶是透過稱為藍圖的 AWS Service Catalog 產品佈建。藍圖可以使用 AWS CloudFormation 範本或地形範本。

> **Note**
>
> AWS CloudFormation 藍圖可以將資源部署到多個區域。地形藍圖只能將資源部署到單一區域。默認情況下，這是主地區域。

AWS Control Tower 建立帳戶時會發生什麼情況

在 AWS Control Tower 中建立新帳戶，然後透過 AWS Control Tower AWS Organizations、和之間的互動佈建 AWS Service Catalog。如需 AWS 帳戶 使用 AWS Control 塔主控台註冊現有的步驟，請參閱註冊現有帳戶。

帳戶創建的幕後花絮

1. 例如，您可以從 AWS Control Tower Account Factory 頁面或直接從主控 AWS Service Catalog 台或呼叫 Service Catalog `ProvisionProduct` API 啟動請求。
2. AWS Service Catalog 呼叫 AWS Control Tower。
3. AWS Control Tower 會啟動工作流程，第一步會呼叫 AWS Organizations `CreateAccount` API。
4. AWS Organizations 建立帳戶後，AWS Control Tower 會套用藍圖和控制來完成佈建程序。
5. Service Catalog 會繼續輪詢 AWS Control Tower，以檢查佈建程序是否完成。
6. AWS Control Tower 中的工作流程完成後，Service Catalog 會完成帳戶的狀態，並通知您 (請求者) 結果。

帳戶所需的權限

每個章節分別討論每種佈建和更新帳戶方法所需的權限。透過適當的使用者群組權限，佈建程式可以為其組織中的任何帳戶指定標準化基準和網路組態。

> **Note**
>
> 佈建帳戶時，帳戶請求者一律必須具有`CreateAccount`和`DescribeCreateAccountStatus`權限。此權限集是管理員角色的一部分，當請求者擔任管理員角色時，會自動提供此權限集。如果您委派佈建帳戶的權限，您可能需要直接為帳戶要求者新增這些權限。

當您使用 Account Factory 從 AWS Control Tower 主控台建立帳戶時，您必須使用已啟用`AWSServiceCatalogEndUserFullAccess`政策的 IAM 使用者登入帳戶，以及使用 AWS Control Tower 主控台的許可，而且您無法以 root 使用者身分登入。

如需 AWS Control Tower 所需許可的一般資訊，請參閱針對 AWS Control Tower 使用身分型政策 (IAM 政策)。如需 AWS Control Tower 中角色和帳戶的相關資訊，請參閱角色和帳戶。

> **您帳戶的安全性**
>
> 您可以在 AWS Organizations 文件中找到有關保護 AWS Control Tower 管理帳戶和成員帳戶安全性的最佳實務指導。
>
> - 管理帳戶的最佳做法
> - 會員帳戶的最佳做法

關 AWS 帳戶 於 AWS Control Tower

A AWS 帳戶 是您所有擁有資源的容器。這些資源包括帳戶接受的 AWS Identity and Access Management (IAM) 身分識別，可決定誰有權存取該帳戶。IAM 身分可以包括使用者、群組、角色等。有關在 AWS Control Tower 中使用 IAM、使用者、角色和政策的詳細資訊，請參閱 AWS Control Tower 中的身分和存取管理。

資源和帳號建立時間

AWS Control Tower 建立或註冊帳戶時，會為該帳戶部署最低必要的資源組態，包括 Account Factory 範本形式的資源和您的 landing zone 中的其他資源。這些資源可能包括 IAM 角色、 AWS CloudTrail 追蹤、Service Catalog 佈建的產品，以及 IAM 身分中心使用者。AWS Control Tower 也會根據控制組態的要求，為新帳戶注定要成為成員帳戶的組織單位 (OU) 部署資源。

AWS Control Tower 代表您協調這些資源的部署。每個資源可能需要數分鐘才能完成部署，因此請在建立或註冊帳號之前考慮總時間。如需管理帳戶中資源的詳細資訊，請參閱建立和修改 AWS Control Tower 資源的指導。

使用現有安全性或記錄帳戶的考量

在接受 AWS 帳戶 作為安全或記錄帳戶之前，AWS Control 塔會檢查帳戶中是否有與 AWS Control Tower 要求衝突的資源。例如，您可能擁有與 AWS Control Tower 所需名稱相同的記錄值區。此外，AWS Control Tower 也會驗證帳戶是否可佈建資源；例如，確保 AWS Security Token Service (AWS STS) 已啟用、帳戶未暫停，以及 AWS Control Tower 有權在帳戶內佈建資源。

AWS Control Tower 不會移除您提供的記錄和安全帳戶中的任何現有資源。不過，如果您選擇啟用 AWS 區域 拒絕功能，區域拒絕控制會阻止存取拒絕區域中的資源。

檢視您的帳戶

「組織」頁面會列出組織中的所有 OU 和帳戶，無論 AWS Control Tower 中的 OU 或註冊狀態為何。如果每個帳戶都符合註冊的先決條件，您可以個別或按 OU 群組檢視和註冊 AWS Control Tower 的成員帳戶。

若要在 [組織] 頁面上檢視特定帳戶，您可以從右上角的下拉式功能表中選擇 [僅限帳戶]，然後從表格中選取您的帳戶名稱。或者，您可以從表格中選取父項 OU 的名稱，也可以在該 OU 的 [詳細資訊] 頁面上檢視該 OU 內所有帳戶的清單。

在 [組織] 頁面和 [帳戶詳細資料] 頁面上，您可以看到帳戶的 [狀態]，這是下列其中一項：

- 未註冊 — 帳戶是父 OU 的成員，但並非由 AWS Control Tower 完全管理。如果已註冊上階 OU，帳戶會受到針對其已註冊上階 OU 所設定的預防性控制所控制，但 OU 的偵探控制項不適用於此帳戶。如果父 OU 未註冊，則不會對此帳戶套用任何控制項。
- 註冊 — AWS Control Tower 將該帳戶納入管理中。我們正在使帳戶與父 OU 的控制組態對齊。每個帳號資源可能需要數分鐘的時間。
- 已註冊 — 帳戶受其上層 OU 所配置的控制項所控制。它由 AWS Control Tower 完全管理。
- 註冊失敗 — 帳戶無法註冊 AWS Control Tower。如需詳細資訊，請參閱 註冊失敗的常見原因。

- 可用的更新 — 帳戶有可用的更新。處於此狀態的帳戶仍為已註冊，但必須更新帳戶以反映最近對環境所做的變更。若要更新單一帳戶，請瀏覽至帳戶詳細資訊頁面，然後選取更新帳戶。

  如果您在單一 OU 下有多個具有此狀態的帳戶，您可以選擇重新註冊 OU 並同時更新這些帳戶。

在共享帳戶中創建的資源

本節顯示當您設定 landing zone 時，AWS Control Tower 在共用帳戶中建立的資源。

如需有關成員帳號資源的資訊，請參閱Account Factory 的資源考量。

管理帳號資源

當您設定 landing zone 域時，會在您的管理帳戶中建立下列 AWS 資源。

AWS 服務	資源類型	資源名稱
AWS Organizations	帳戶	audit log archive
AWS Organizations	OU	Security Sandbox
AWS Organizations	服務控制政策	aws-guardrails-*
AWS CloudFormation	堆疊	AWSControlTowerBP-BASELINE-CLOUDTRAIL-MASTER AWSControlTowerBP-BASELINE-CONFIG-MASTER（在 2.6 版及更高版本中）
AWS CloudFormation	StackSets	AWSControlTowerBP-BASELINE-CLOUDTRAIL（在 3.0 及更高版本中未部署）

AWS 服務	資源類型	資源名稱
		AWSControlTowerBP_BASELINE_SERVICE_LINKED_ROLE (Deployed in 3.2 and later)
		AWSControlTowerBP-BASELINE-CLOUDWATCH
		AWSControlTowerBP-BASELINE-CONFIG
		AWSControlTowerBP-BASELINE-ROLES
		AWSControlTowerBP-BASELINE-SERVICE-ROLES
		AWSControlTowerBP-SECURITY-TOPICS
		AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-READ-PROHIBITED
		AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED
		AWSControlTowerLoggingResources
		AWSControlTowerSecurityResources
		AWSControlTowerExecutionRole

AWS 服務	資源類型	資源名稱
AWS Service Catalog	產品	AWS Control Tower Account Factory
AWS Config	彙整工具	aws-controltower-ConfigAggregatorForOrganizations
AWS CloudTrail	追蹤	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch 日誌	aws-controltower/CloudTrailLogs
AWS Identity and Access Management	角色	AWSControlTowerAdmin AWSControlTowerStackSetRole AWSControlTowerCloudTrailRolePolicy
AWS Identity and Access Management	政策	AWSControlTowerServiceRolePolicy AWSControlTowerAdminPolicy AWSControlTowerCloudTrailRolePolicy AWSControlTowerStackSetRolePolicy

AWS 服務	資源類型	資源名稱
AWS IAM Identity Center	目錄群組	AWSAccountFactory AWSAuditAccountAdmins AWSControlTowerAdmins AWSLogArchiveAdmins AWSLogArchiveViewers AWSSecurityAuditors AWSSecurityAuditPowerUsers AWSServiceCatalogAdmins
AWS IAM Identity Center	許可集	AWSAdministratorAccess AWSPowerUserAccess AWSServiceCatalogAdminFullAccess AWSServiceCatalogEndUserAccess AWSReadOnlyAccess AWSOrganizationsFullAccess

> **Note**
>
> 不 AWS CloudFormation StackSet `BP_BASELINE_CLOUDTRAIL`會部署在 3.0 或更新版本的 landing zone 域中。不過，它會繼續存在於舊版的 landing zone 域中，直到您更新 landing zone 域為止。

記錄封存帳號資源

當您設定 landing zone 時，系統會在您的記錄封存帳戶中建立下列 AWS 資源。

AWS 服務	資源類型	資源名稱
AWS CloudFormation	堆疊	StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-READ-PROHIBITED- StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH- StackSet-AWSControlTowerBP-BASELINE-CONFIG- StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL- StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES- StackSet-AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLE-(In 3.2 and later) StackSet-AWSControlTowerBP-BASELINE-ROLES-

AWS 服務	資源類型	資源名稱
		StackSet-AWSControlTowerLoggingResources-
AWS Config	AWS Config 規則	AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_READ_PROHIBITED AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_WRITE_PROHIBIT
AWS CloudTrail	線索	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch 活動規則	aws-controltower-ConfigComplianceChangeEventRule
Amazon CloudWatch	CloudWatch 日誌	/aws/lambda/aws-controltower-NotificationForwarder
AWS Identity and Access Management	角色	aws-controltower-AdministratorExecutionRole aws-controltower-CloudWatchLogsRole aws-controltower-ConfigRecorderRole aws-controltower-ForwardSnsNotificationRole aws-controltower-ReadOnlyExecutionRole AWSControlTowerExecution

AWS 服務	資源類型	資源名稱
AWS Identity and Access Management	政策	AWSControlTowerServiceRolePolicy
Amazon Simple Notification Service	主題	aws-controltower-SecurityNotifications
AWS Lambda	應用程式	StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-*
AWS Lambda	函數	aws-controltower-NotificationForwarder
Amazon Simple Storage Service	儲存貯體	aws-controltower-logs-* aws-controltower-s3-access-logs-*

稽核帳號資源

當您設定 landing zone 域時，會在您的稽核帳戶中建立下列 AWS 資源。

AWS 服務	資源類型	資源名稱
AWS CloudFormation	堆疊	StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-READ-PROHIBITED- StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED-

AWS 服務	資源類型	資源名稱
		StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH- StackSet-AWSControlTowerBP-BASELINE-CONFIG- StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL- StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES- StackSet-AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLE-(In 3.2 and later) StackSet-AWSControlTowerBP-SECURITY-TOPICS- StackSet-AWSControlTowerBP-BASELINE-ROLES- StackSet-AWSControlTowerSecurityResources-*
AWS Config	彙整工具	aws-controltower-GuardrailsComplianceAggregator

AWS 服務	資源類型	資源名稱
AWS Config	AWS Config 規則	AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_READ_PROHIBITED AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_WRITE_PROHIBITED
AWS CloudTrail	追蹤	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch 活動規則	aws-controltower-ConfigComplianceChangeEventRule
Amazon CloudWatch	CloudWatch 日誌	/aws/lambda/aws-controltower-NotificationForwarder

AWS 服務	資源類型	資源名稱
AWS Identity and Access Management	角色	aws-controltower-AdministratorExecutionRole aws-controltower-CloudWatchLogsRole aws-controltower-ConfigRecorderRole aws-controltower-ForwardSnsNotificationRole aws-controltower-ReadOnlyExecutionRole aws-controltower-AuditAdministratorRole aws-controltower-AuditReadOnlyRole AWSControlTowerExecution
AWS Identity and Access Management	政策	AWSControlTowerServiceRolePolicy
Amazon Simple Notification Service	主題	aws-controltower-AggregateSecurityNotifications aws-controltower-AllConfigNotifications aws-controltower-SecurityNotifications
AWS Lambda	函數	aws-controltower-NotificationForwarder

關於共享帳戶

三個特殊項 AWS 帳戶 目與 AWS Control Tower 相關聯：管理帳戶、稽核帳戶和記錄存檔帳戶。這些帳戶通常稱為共享帳戶，有時也稱為核心帳戶。

- 您可以在設定 landing zone 時為稽核和記錄封存帳戶選取自訂名稱。如需變更帳戶名稱的相關資訊，請參閱外部變更 AWS Control Tower 資源名稱。
- 您也可以在初始 landing zone 設定程序期間，將現有帳戶指定 AWS 帳戶 為 AWS Control Tower 安全或記錄帳戶。此選項無需 AWS Control Tower 建立新的共用帳戶。（這是一次性的選擇。）

如需共用帳戶及其相關資源的詳細資訊，請參閱在共享帳戶中創建的資源。

管理帳戶

這將 AWS 帳戶 啟動 AWS Control Tower。根據預設，此帳戶的根使用者以及此帳戶的 IAM 使用者或 IAM 管理員使用者可以完整存取您 landing zone 內的所有資源。

> **Note**
>
> 最佳做法是，建議您在 AWS Control Tower 主控台內執行管理功能時，以具有管理員權限的 IAM 身分中心使用者身分登入，而不是以此帳戶的根使用者或 IAM 管理員使用者身分登入。

如需管理帳戶中可用角色和資源的詳細資訊，請參閱在共享帳戶中創建的資源。

日誌存檔帳戶

記錄封存共用帳戶會在您建立 landing zone 時自動設定。

此帳戶包含一個中央 Amazon S3 儲存貯體，用於存放 landing zone 域中所有其他帳戶的所有其他帳戶的副本 AWS CloudTrail 和 AWS Config 日誌檔。最佳作法是，我們建議將記錄封存帳戶存取限制為負責合規性和調查的團隊，以及其相關安全性或稽核工具。此帳戶可用於自動化安全稽核，或託管自訂 AWS Config 規則(例如 Lambda 函數) 以執行修復動作。

> **Amazon S3 存儲桶政策**
>
> 對於 AWS Control Tower landing zone 3.3 版及更新版本，帳戶必須符合稽核儲存貯體的任何寫入許可的`aws:SourceOrgID`條件。這種情況可確保 CloudTrail 只能代表組織內的帳戶將日

誌寫入 S3 儲存貯體；它可防止組織外部的 CloudTrail 日誌寫入 AWS Control Tower S3 儲存貯體。如需詳細資訊，請參閱 AWS Control Tower landing zone 3.3 版。

如需記錄封存帳戶中可用角色和資源的詳細資訊，請參閱 記錄封存帳號資源

> **Note**
>
> 無法變更這些記錄檔。所有記錄都會儲存在與帳戶活動相關的稽核和合規性調查之用。

稽核帳戶

此共享帳戶會在您建立 landing zone 時自動設定。

稽核帳戶應該僅限於安全性和規範遵循團隊，其稽核人員 (唯讀) 和系統管理員 (完全存取) 跨帳戶角色可存取 landing zone 中所有帳戶。這些角色旨在供安全性和規範遵循團隊用於：

- 透過 AWS 機制執行稽核，例如託管自訂 AWS Config 規則 Lambda 函數。
- 執行自動化安全作業，例如補救動作。

稽核帳戶也會透過 Amazon Simple Notification Service (Amazon SNS) 服務接收通知。可以收到三種類別的通知：

- 所有組態事件 — 本主題彙總了 landing zone 中所有帳戶的所有 AWS Config 通知 CloudTrail 和通知。
- 彙總安全性通知 — 本主題彙總來自特定 CloudWatch 事件、 AWS Config 規則 規範遵循狀態變更事件和 GuardDuty 發現項目的所有安全性通知。
- 漂移通知 — 本主題彙總了您 landing zone 中所有帳戶、使用者、OU 和 SCP 中發現的所有漂移警告。如需漂移的詳細資訊，請參閱偵測並解決 AWS Control Tower 中的漂移。

在成員帳戶內觸發的稽核通知也可以傳送警示至本機 Amazon SNS 主題。此功能可讓帳戶管理員訂閱個別成員帳戶特定的稽核通知。因此，管理員可以解決影響個別帳戶的問題，同時仍將所有帳戶通知彙總到您的集中式稽核帳戶。如需詳細資訊，請參閱《Amazon Simple Notification Service 開發人員指南》。

如需稽核帳號中可用角色和資源的詳細資訊，請參閱稽核帳號資源。

如需程式化稽核的詳細資訊，請參閱 AWS Control Tower 稽核帳戶的程式化角色和信任關係。

> **Important**
>
> 您為稽核帳戶提供的電子郵件地址會收到 AWS Control Tower AWS 區域 支援的每封AWS 通知-訂閱確認電子郵件。若要在稽核帳戶中接收合規電子郵件，您必須從 AWS Control Tower AWS 區域 支援的每封電子郵件中選擇確認訂閱連結。

關於會員帳戶

成員帳戶是您的使用者透過其執行其 AWS 工作負載的帳戶。這些成員帳戶可以在 Account Factory 中建立、在 Service Catalog 主控台中具有管理員權限的 IAM Identity Center 使用者，或透過自動化方式建立。建立時，這些成員帳戶會存在於 AWS Control Teck 主控台中建立或向 AWS Control Tower 註冊的 OU 中。如需詳細資訊，請參閱下列相關主題：

- 使用 Account Factory 佈建和管理帳戶
- AWS Control Tower 中的自動化任務
- AWS 《AWS Organizations 使用者指南》中的 Organ@@ izations 術語和概念。

另請參閱 使用 AWS Control Tower Account Factory 為地形 (AFT) 佈建帳戶 。

> **帳戶和控制**
>
> 成員帳戶可以在 AWS Control Tower 註冊，也可以取消註冊。控制項會以不同方式套用至已註冊和未註冊的帳戶，而且控制項可能會套用至巢狀 OU 中的帳戶 (依據繼承

如需 AWS Control Tower 配置的成員帳戶資源的相關資訊，請參閱Account Factory 的資源考量。

註冊現有的 AWS 帳戶

您可以將 AWS Control Tower 管理擴展到個人， AWS 帳戶 當您將其註冊到已由 AWS Control Tower 管理的組織單位 (OU) 時即可使用。合格的帳戶存在於未註冊的 OU 中，與 AWS Control Tower OU 屬於相同 AWS Organizations 組織的一部分。

> **Note**
>
> 除非在初始 landing zone 設定期間，否則您無法將現有帳戶註冊為稽核或記錄封存帳戶。

首先設定受信任的存取

您必須先授予 AWS Control Tower 管理或管理帳戶的權限，才能 AWS 帳戶 將現有的 AWS Control Tower 註冊到 AWS 控制塔。具體來說，AWS Control Tower 需要許可，才能 AWS Organizations 在您之間 AWS CloudFormation 和代表您建立受信任的存取權限， AWS CloudFormation 以便自動將堆疊部署到所選組織中的帳戶。透過此受信任存取權，`AWSControlTowerExecution`角色會執行管理每個帳戶所需的活動。這就是為什麼您必須在註冊之前將此角色添加到每個帳戶中的原因。

啟用受信任存取時， AWS CloudFormation 可以透過單一作業跨多個帳戶建立、更新或刪除堆疊。AWS 區域 AWS Control Tower 仰賴此信任功能，因此在將現有帳戶移入註冊的組織單位之前，可將角色和許可套用至現有帳戶，進而使其受到管理。

若要進一步了解受信任存取權限 AWS CloudFormation StackSets，請參閱AWS CloudFormationStackSets和 AWS Organizations。

帳戶註冊期間會發生什麼

在註冊程序期間，AWS Control Tower 會執行下列動作：

- 確立帳戶的基準，其中包括部署這些堆疊集：
  - `AWSControlTowerBP-BASELINE-CLOUDTRAIL`
  - `AWSControlTowerBP-BASELINE-CLOUDWATCH`
  - `AWSControlTowerBP-BASELINE-CONFIG`
  - `AWSControlTowerBP-BASELINE-ROLES`
  - `AWSControlTowerBP-BASELINE-SERVICE-ROLES`
  - `AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLES`
  - `AWSControlTowerBP-VPC-ACCOUNT-FACTORY-V1`

  檢閱這些堆疊集的範本，並確定它們與您現有的政策沒有衝突是個不錯的主意。
- 透過 AWS IAM Identity Center 或識別帳戶 AWS Organizations。
- 將帳戶放入您指定的 OU 中。請務必套用目前 OU 中套用的所有 SCP，使您的安全狀態能夠保持一致。

- 透過套用至所選 OU 整體的 SCP，將強制控制套用至帳戶。
- 啟用 AWS Config 並設定它，以記錄帳號中的所有資源。
- 新增將 AWS Control Tower 偵探控制套用至帳戶的 AWS Config 規則。

> **帳戶和組織層 CloudTrail 級追蹤**
>
> OU 中的所有成員帳戶都受 OU 的 AWS CloudTrail 追蹤管理 (無論是否已註冊)：
>
> - 當您在 AWS Control Tower 註冊帳戶時，您的帳戶受到新組織的 AWS CloudTrail 追蹤管理。如果您現有的 CloudTrail 追蹤部署，您可能會看到重複的費用，除非您在 AWS Control Tower 註冊帳戶之前刪除該帳戶的現有追蹤。
> - 如果您將帳戶移到已註冊的 OU (例如透過主控 AWS Organizations 台)，並且未繼續將該帳戶註冊到 AWS Control Tower，您可能希望移除該帳戶剩餘的帳戶層級追蹤。如果您有 CloudTrail 追蹤的現有部署，則會產生重複 CloudTrail 費用。
>
> 如果您更新 landing zone 域並選擇退出組織層級的追蹤，或者您的 landing zone 域舊於 3.0 版，則組織層級的 CloudTrail追蹤不會套用至您的帳戶。

使用 VPC 註冊現有帳戶

當您在 Account Factory 佈建新帳戶時，與註冊現有帳戶相比，AWS Control Tower 處理 VPC 的方式不同。

- 當您建立新帳戶時，AWS Control Tower 會自動移除 AWS 預設 VPC，並為該帳戶建立新的 VPC。
- 當您註冊現有帳戶時，AWS Control Tower 不會為該帳戶建立新的 VPC。
- 註冊現有帳戶時，AWS Control Tower 不會移除與該帳戶相關聯的任何現有 VPC 或 AWS 預設 VPC。

> **Tip**
>
> 您可以透過設定 Account Factory 來變更新帳戶的預設行為，這樣它就不會在 AWS Control Tower 下為組織中的帳戶預設設定 VPC。如需詳細資訊，請參閱 在沒有 VPC 的 AWS Control Tower 中建立帳戶。

註冊的先決條件

註冊 AWS Control Tower AWS 帳戶 中的現有項目之前，必須具備以下先決條件：

1. 若要註冊現有角色 AWS 帳戶，該AWSControlTowerExecution角色必須出現在您註冊的帳戶中。您可以查看註冊帳戶以獲取詳細信息和說明。
2. 除了AWSControlTowerExecution角色之外， AWS 帳戶 您要註冊的現有項目還必須具有下列權限和信任關係。否則，註冊將會失敗。

   角色權限：AdministratorAccess(AWS 受管理策略)

   角色信任關係

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::Management Account ID:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

3. 我們建議該帳戶不應該有組 AWS Config 態記錄器或傳遞通道。您可以在註冊帳戶 AWS CLI 之前，透過中刪除或修改這些內容。否則，請檢閱具有現有 AWS Config 資源的註冊帳號，以取得如何修改現有資源的指示。
4. 您要註冊的帳戶必須與 AWS Control Tower 管理帳戶位於相同的 AWS Organizations 組織中。現有帳戶只能註冊到與 AWS Control Tower 管理帳戶相同的組織，也就是已在 AWS Control Tower 註冊的 OU 中。

若要查看註冊的其他先決條件，請參閱 AWS Control Tower 入門。

> **Note**
>
> 當您在 AWS Control Tower 註冊帳戶時，您的帳戶受 AWS Control Tower 組織的 AWS CloudTrail 追蹤管理。如果您現有的 CloudTrail追蹤部署，您可能會看到重複的費用，除非您在 AWS Control Tower 註冊帳戶之前刪除該帳戶的現有追蹤。

註冊現有帳戶

AWS Control 塔主控台提供註冊帳戶功能，用於註冊現有帳戶， AWS 帳戶 以便由 AWS Control Tower 管理。如需詳細資訊，請參閱註冊現有的 AWS 帳戶.

當您的 landing zone 未處於漂移狀態時，可以使用註冊帳戶功能。若要在主控台中檢視此功能：

- 導覽至 AWS Control Tower 中的組織頁面。
- 找到您要註冊的帳戶名稱。要找到它，請從右上角的下拉菜單中選擇「僅帳戶」，然後在篩選的表格中找到帳戶名稱。
- 請按照以下步驟註冊個人帳戶，如註冊帳戶的步驟本節所示。

> **Note**
>
> 當您註冊現有的電子郵件地址時 AWS 帳戶，請務必驗證現有的電子郵件地址。否則，可能會創建一個新帳戶。

某些錯誤可能需要您重新整理頁面，然後再試一次。如果登陸區域處於偏離狀態，您可能無法成功使用 Enroll account (註冊帳戶) 佈建。您需要透過 Account Factory 佈建新帳戶，直到您的 landing zone 漂移解決為止。

當您從 AWS Control Tower 主控台註冊帳戶時，必須使用已啟用`AWSServiceCatalogEndUserFullAccess`政策的使用者登入帳戶，以及使用 AWS Control Tower 主控台的管理員存取權限，而且您無法以 root 使用者身分登入。

您註冊的帳戶可以透過 AWS Service Catalog 和 AWS Control Tower 帳戶工廠進行更新，如同您會更新任何其他帳戶一樣。稱為使用 AWS Control Tower 或使用更新和移動帳戶工廠帳戶 AWS Service Catalog的小節會提供更新程序。

註冊帳戶的步驟

在您現有帳戶中設定AdministratorAccess權限 (政策) 之後，請依照下列步驟註冊帳戶：

在 AWS Control Tower 註冊個人帳戶

- 導覽至 AWS Control Tower 組織頁面。
- 在 [組織] 頁面上，符合註冊資格的帳戶可讓您從區段頂端的 [動作] 下拉式功能表中選取 [註冊]。當您在 [帳戶詳細資料] 頁面上檢視時，這些帳戶也會顯示 [註冊帳戶] 按鈕。
- 當您選擇 [註冊帳戶] 時，您會看到 [註冊帳戶] 頁面，系統會提示您將`AWSControlTowerExecution`角色新增至帳戶。如需某些指示，請參閱手動將所需的 IAM 角色新增至現有角色 AWS 帳戶 並註冊。
- 接下來，從下拉式清單中選取已註冊的 OU。如果帳戶已在已註冊的 OU 中，此清單會顯示 OU。
- 選擇 Enroll acount (註冊帳戶)。
- 您會看到強制回應提醒，以新增`AWSControlTowerExecution`角色並確認動作。
- 選擇「註冊」。
- AWS Control Tower 會開始註冊程序，然後您會返回帳戶詳細資訊頁面。

註冊失敗的常見原因

- 若要註冊現有帳戶，該`AWSControlTowerExecution`角色必須出現在您註冊的帳戶中。
- 您的 IAM 委託人可能缺乏佈建帳戶的必要許可。
- AWS Security Token Service (AWS STS) 已 AWS 帳戶 在您的家用區域或 AWS Control Tower 支援的任何區域停用。
- 您可能已登入需要新增至中的 Account Factory 投資組合的帳戶 AWS Service Catalog。您必須先新增帳戶，才能存取 Account Factory，以便在 AWS Control Tower 中建立或註冊帳戶。如果適當的使用者或角色未新增至 Account Factory 產品組合，您將在嘗試新增帳戶時收到錯誤訊息。如需如何授與 AWS Service Catalog 學檔存取權的指示，請參閱授與使用者存取權。
- 您可以 root 身分登入。
- 您嘗試註冊的帳戶可能具有剩餘的 AWS Config 設定。特別是，該帳戶可能具有配置記錄器或交付通道。您必須 AWS CLI 先透過刪除或修改這些內容，才能註冊帳戶。如需詳細資訊，請參閱 註冊具有現有 AWS Config 資源的帳號 及 與 AWS Control Tower 使用互動 AWS CloudShell。
- 如果帳戶屬於另一個擁有管理帳戶的 OU (包括另一個 AWS Control Tower OU)，您必須先終止其目前 OU 中的帳戶，才能加入另一個 OU。必須移除原始 OU 中的現有資源。否則，註冊將會失敗。

- 如果目的地 OU 的 SCP 不允許您建立該帳戶所需的所有資源，則帳戶佈建和註冊會失敗。例如，目的地 OU 中的 SCP 可能會在沒有特定標籤的情況下封鎖資源建立。在此情況下，帳戶佈建或註冊會失敗，因為 AWS Control Tower 不支援標記資源。如需協助，請聯絡您的客戶代表，或 AWS Support。

有關 AWS Control Tower 在建立新帳戶或註冊現有帳戶時如何與角色搭配使用的詳細資訊，請參閱角色和帳戶。

> **Tip**
>
> 如果您無法確認現有的 AWS 帳戶 符合註冊先決條件，您可以設定註冊 OU，並將帳戶註冊到該 OU。註冊成功後，您可以將帳戶移至所需的 OU。如果註冊碰巧失敗，則沒有其他帳戶或 OU 會受到失敗的影響。

如果您對現有帳戶及其組態與 AWS Control Tower 相容有疑問，可以遵循以下部分建議的最佳實務。

建議：您可以為帳戶註冊設定雙步驟方法

- 首先，使用一 AWS Config 致性套件評估您的帳戶可能受到某些 AWS Control Tower 控制項的影響。要確定註冊 AWS Control Tall 可能會對您的帳戶AWS Config 造成什麼影響，請參閱使用一致性套件擴展 AWS Control Tower 管理。
- 接下來，您可能希望註冊該帳戶。如果合規結果令人滿意，遷移路徑會更容易，因為您可以在預期的情況下註冊帳戶。
- 完成評估後，如果您決定設定 AWS Control Tower landing zone，可能需要移除為評估建立的 AWS Config 交付通道和組態記錄器。然後，您就可以成功設定 AWS Control Tower。

> **Note**
>
> 一致性套件也適用於帳戶位於 AWS Control Tower 所註冊的 OU 中，但工作負載在沒有 AWS Control Tower 支援的 AWS 區域中執行。您可以使用一致性套件來管理尚未部署 AWS Control Tall 之區域中存在的帳戶中的資源。

如果帳戶不符合先決條件怎麼辦？

請記住，符合 AWS Control Tower 管理資格註冊的帳戶必須屬於同一個整體組織，做為先決條件。若要滿足帳戶註冊的先決條件，您可以按照下列準備步驟將帳戶移至與 AWS Control Tower 相同的組織。

將帳戶帶入與 AWS Control Tower 相同組織的準備步驟

1. 從其現有組織中刪除帳戶。如果您使用此方法，您必須提供個別的付款方式。
2. 邀請帳戶加入 AWS Control Tower 組織。如需詳細資訊，請參閱AWS Organizations 使用者指南中的邀請 AWS 帳戶加入您的組織。
3. 接受邀請。該帳戶顯示在組織的根目錄中。此步驟會將帳戶移至與 AWS Control Tower 相同的組織。並建立 SCP 和合併帳單。

> **Tip**
>
> 您可以在帳戶退出舊組織之前傳送新組織的邀請。當帳戶正式退出其現有組織時，邀請將等待。

完成剩餘先決條件的步驟：

1. 建立必要的`AWSControlTowerExecution`角色。
2. 清除預設的 VPC。（此部分是可選的。 AWS Control Tower 不會變更您現有的預設 VPC。）
3. 透過或刪除或修改任何現有的 AWS Config 組態記錄程式 AWS CLI 或傳遞通道 AWS CloudShell。如需詳細資訊，請參閱 資源狀態的 AWS Config CLI 命令範例 和 註冊具有現有 AWS Config 資源的帳號

完成這些準備步驟後，您可以將該帳戶註冊到 AWS Control Tower。如需詳細資訊，請參閱 註冊帳戶的步驟。此步驟會將帳戶納入完整的 AWS Control Tower 管控。

取消佈建帳戶的選擇性步驟，以便註冊帳戶並保留其堆疊

1. 若要保留套用的 AWS CloudFormation 堆疊，請從堆疊組合中刪除堆疊實體，然後為實體選擇「保留堆疊」。
2. 在 Account Factory 中終止 AWS Service Catalog 帳戶佈建的產品。(此步驟只會從 AWS Control Tower 移除佈建的產品。 它不會刪除帳戶。)

3. 根據不屬於組織的任何帳戶的要求，設定具有必要帳單詳細資訊的帳戶。然後從組織中移除帳戶。您可以這麼做，因此帳戶不會計入配額中的總 AWS Organizations 額。)
4. 如果資源仍然存在，請清除帳號，然後按照中的帳號關閉步驟將其關閉取消管理帳戶。
5. 如果您有已定義控制項的已暫停 OU，您可以將帳戶移至該處，而不是執行步驟 1。

資源狀態的 AWS Config CLI 命令範例

以下是一些可用來判斷組態記錄程式和傳遞通道狀態的 AWS Config CLI 命令範例。

檢視命令：

- `aws configservice describe-delivery-channels`
- `aws configservice describe-delivery-channel-status`
- `aws configservice describe-configuration-recorders`

正常的反應是這樣的 `"name": "default"`

刪除命令：

- `aws configservice stop-configuration-recorder --configuration-recorder-name NAME-FROM-DESCRIBE-OUTPUT`
- `aws configservice delete-delivery-channel --delivery-channel-name NAME-FROM-DESCRIBE-OUTPUT`
- `aws configservice delete-configuration-recorder --configuration-recorder-name NAME-FROM-DESCRIBE-OUTPUT`

手動將所需的 IAM 角色新增至現有角色 AWS 帳戶 並註冊

如果您已經設定 AWS Control 塔 landing zone，則可以開始將組織的帳戶註冊到已向 AWS Control Tower 註冊的 OU。如果您尚未設定 landing zone，請按照入門步驟 2 中 AWS Control 塔使用者指南中所述的步驟進行操作。在 landing zone 準備就緒後，請完成以下步驟，以手動方式將現有帳戶納入 AWS Control Tower 的管理。

請務必檢閱本章註冊的先決條件前面提到的內容。

在 AWS Control Tower 註冊帳戶之前，您必須授予 AWS Control Tower 管理該帳戶的權限。若要這麼做，您將新增具有帳戶完整存取權限的角色，如下列步驟所示。必須針對您註冊的每個帳戶執行這些步驟。

對於每個帳戶：

步驟 1：以管理員存取權登入目前包含您要註冊之帳戶之組織的管理帳戶。

例如，如果您從中建立此帳戶， AWS Organizations 並使用跨帳戶 IAM 角色登入，則可以按照以下步驟操作：

1. 登入貴組織的管理帳戶。
2. 前往 AWS Organizations。
3. 在帳戶下，選取您要註冊的帳戶，並複製其帳戶 ID。
4. 打開頂部導航欄上的帳戶下拉菜單，然後選擇切換角色。
5. 在 [切換角色] 表單上，填寫下列欄位：
   - 在「帳戶」下，輸入您複製的帳戶 ID。
   - 在「角色」下，輸入允許跨帳戶存取此帳戶的 IAM 角色名稱。此角色的名稱是在建立帳號時定義的。如果您在建立帳號時未指定角色名稱，請輸入預設角色名稱`OrganizationAccountAccessRole`。
6. 選擇 Switch Role (切換角色)。
7. 現在，您應該以兒童帳戶的 AWS Management Console 身份登錄。
8. 完成後，請留在子女帳戶中繼續進行下一個程序。
9. 記下管理帳戶 ID，因為您需要在下一步中輸入它。

步驟 2：授與 AWS Control Tower 管理帳戶的權限。

1. 前往 IAM。
2. 前往「角色」。
3. 選擇建立角色。
4. 當系統詢問您是否要選取角色的服務時，請選擇 [自訂信任原則]。
5. 複製此處顯示的程式碼範例，並將其貼到「政策文件」中。將字串*`Management Account ID`*取代為管理帳戶的實際管理帳戶 ID。以下是要粘貼的策略：

```
{
```

```
  "Version":"2012-10-17",
  "Statement":[
     {
     "Effect":"Allow",
     "Principal":{
        "AWS": "arn:aws:iam::Management Account ID:root"
        },
        "Action": "sts:AssumeRole",
        "Condition": {}
     }
  ]
 }
```

6. 當系統要求您附加策略時，請選擇AdministratorAccess。
7. 選擇 Next: Add Tags (下一步：新增標籤)。
8. 您可能會看到標題為「新增標籤」的選用畫面。選擇「下一步:檢閱」，立即略過此畫面
9. 在「複查」畫面的「角色名稱」欄位中，輸入AWSControlTowerExecution。
10. 在 [說明] 方塊中輸入簡短說明，例如 [允許註冊的完整帳戶存取權]。
11. 選擇建立角色。

步驟 3：透過將帳戶移入已註冊的 OU 來註冊帳戶，並驗證註冊。

建立角色來設定必要的權限後，請依照下列步驟註冊帳戶並驗證註冊。

1. 以管理員身分再次登入，然後前往 AWS Control Tower。
2. 註冊帳戶。
   - 在 AWS Control Tower 的「組織」頁面中，選取您的帳戶，然後從右上角的「動作」下拉式功能表中選擇「註冊」。
   - 按照註冊帳戶的步驟頁面上顯示的步驟註冊個人帳戶。
3. 驗證註冊。
   - 在 AWS Control Tower 中，選擇左側導覽中的 [組織]。
   - 尋找您最近註冊的帳戶。其初始狀態將顯示註冊狀態。
   - 當狀態變更為 [已註冊] 時，移動成功。

若要繼續此程序，請登入組織中要註冊 AWS Control Tower 的每個帳戶。針對每個帳戶重複先決條件步驟和註冊步驟。

自動註冊 AWS Organizations 帳戶

您可以使用部落格文章中所述的註冊方法將現有 AWS 帳戶註冊到 AWS Control Tower，透過程式設計程序將 AWS Organizations 帳戶註冊到 AWS Control Tower。

下列 YAML 範本可協助您在帳戶中建立必要的角色，以便以程式設計方式註冊該角色。

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure the AWSControlTowerExecution role to enable use of your
  account as a target account in AWS CloudFormation StackSets.
Parameters:
  AdministratorAccountId:
    Type: String
    Description: AWS Account Id of the administrator account (the account in which
      StackSets will be created).
    MaxLength: 12
    MinLength: 12
Resources:
  ExecutionRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: AWSControlTowerExecution
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              AWS:
                - !Ref AdministratorAccountId
            Action:
              - sts:AssumeRole
      Path: /
      ManagedPolicyArns:
        - !Sub arn:${AWS::Partition}:iam::aws:policy/AdministratorAccess
```

註冊具有現有 AWS Config 資源的帳號

本主題提供如何註冊具有現有 AWS Config 資源之帳號的 step-by-step 方法。如需如何檢查現有資源的範例，請參閱資源狀態的 AWS Config CLI 命令範例。

> **Note**
>
> 如果您打算將現有 AWS 帳戶作為稽核和日誌存檔帳戶帶入 AWS Control Tower，而且這些帳戶具有現有 AWS Config 資源，則必須完全刪除現有 AWS Config 資源，然後才能將這些帳戶註冊到 AWS Control Tower 以達到此目的。對於不想成為稽核和記錄封存帳戶的帳戶，您可以修改現有的 Config 資源。

AWS Config 資源的例子

以下是您的帳戶可能已經擁有的一些 AWS Config 資源類型。您可能需要修改這些資源，才能將帳戶註冊到 AWS Control Tower。

- AWS Config 錄音機
- AWS Config 交付渠道
- AWS Config 聚合授權

前提

- 您已部署 AWS Control Tower landing zone
- 您的帳戶尚未向 AWS Control Tower 註冊。
- 您的帳戶至少有一個受管理帳戶管理的 AWS Control Tower 區域中有至少一個預先存在的 AWS Config 資源。
- 您的帳戶不是 AWS Control Tower 管理帳戶。
- 您的帳戶不處於治理偏移狀態。

如需說明使用現有 AWS Config 資源註冊帳戶的自動化方法的部落格，請參閱自動將具有現有 AWS Config 資源的帳戶註冊到 AWS Control Tower。如下所述，您可以為所有希望註冊的帳戶提交單一支援票證。步驟 1：提供票證聯絡客戶支援，將帳戶新增至 AWS Control Tower 允許清單

限制

- 只有使用 AWS Control Tower 工作流程來擴展管理，才能註冊帳戶。
- 如果資源已修改並在帳戶上建立漂移，AWS Control Tower 不會更新資源。
- AWS Config 不受 AWS Control Tower 管理的區域中的資源不會變更。

> **Note**
>
> 如果您嘗試註冊具有現有 Config 資源的帳戶，但未將帳戶新增至允許清單，則註冊將失敗。之後，如果您隨後嘗試將同一帳戶新增至允許清單，AWS Control Tower 將無法驗證該帳戶是否已正確佈建。您必須先從 AWS Control Tower 取消佈建帳戶，然後才能請求允許清單，然後註冊。如果您只將帳戶移至不同的 AWS Control Tower OU，則會導致管理偏移，這也會防止帳戶新增至允許清單。

這個過程有 5 個主要步驟。

1. 將帳戶新增至 AWS Control Tower 允許清單。
2. 在帳戶中建立新的 IAM 角色。
3. 修改預先存在的資 AWS Config 源。
4. 在不存在的 AWS 區域中建立 AWS Config 資源。
5. 在 AWS Control Tower 註冊帳戶。

在繼續之前，請考慮以下對此過程的期望。

- AWS Control Tower 不會在此帳戶中建立任何 AWS Config 資源。
- 註冊後，AWS Control Tower 控制會自動保護您建立的 AWS Config 資源，包括新的 IAM 角色。
- 如果在註冊後對 AWS Config 資源進行任何變更，則必須先更新這些資源以符合 AWS Control Tower 設定，然後才能重新註冊帳戶。

步驟 1：提供票證聯絡客戶支援，將帳戶新增至 AWS Control Tower 允許清單

在您的票證主題行中包含此短語：

將具有現有 AWS Config 資源的帳戶註冊到 AWS Control Tower

在您的機票正文中包含以下詳細信息：

- 管理帳號
- 具有現有 AWS Config 資源之成員帳號的帳號
- 針對 AWS Control Tower 設定選取的本地區域

> **Note**
>
> 將帳戶添加到允許列表所需的時間為 2 個工作日。

步驟 2：在成員帳戶中建立新的 IAM 角色

1. 開啟成員帳戶的 AWS CloudFormation 主控台。
2. 使用下列範本建立新堆疊

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure AWS Config

Resources:
  CustomerCreatedConfigRecorderRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: aws-controltower-ConfigRecorderRole-customer-created
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - config.amazonaws.com
            Action:
              - sts:AssumeRole
      Path: /
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/service-role/AWS_ConfigRole
        - arn:aws:iam::aws:policy/ReadOnlyAccess
```

3. 將堆疊名稱提供為「CustomerCreatedConfigRecorderRoleForControl塔」
4. 建立堆疊。

> **Note**
>
> 您建立的任何 SCP 都應排除`aws-controltower-ConfigRecorderRole*`角色。請勿修改限制 AWS Config 規則執行評估能力的權限。

請遵循這些準則，以便AccessDeniedException當您有阻止aws-controltower-ConfigRecorderRole*調用 Config 的 SCP 時，您不會收到。

步驟 3：識別具有預先存在資源的 AWS 區域

對於帳戶中的每個受控區域 (AWS Control Tower 管理)，識別並記下至少具有先前顯示的現有 AWS Config 資源範例類型之一的區域。

步驟 4：確定沒有任何 AWS Config 資源的 AWS 區域

對於帳戶中的每個受控區域 (AWS Control Tower 管理)，識別並記下沒有先前顯示的範例類型 AWS Config 資源的區域。

步驟 5：修改每個 AWS 區域中的現有資源

在此步驟中，需要下列有關 AWS Control Tower 設定的資訊。

- LOGGING_ACCOUNT-記錄帳戶 ID
- AUDIT_ACCOUNT-審計帳戶 ID
- IAM_ROLE_ARN-在步驟 1 中建立的身分與存取權管理角色 ARN
- ORGANIZATION_ID-管理帳戶的組織 ID
- MEMBER_ACCOUNT_NUMBER-正在修改的會員帳戶
- HOME_REGION-AWS Control Tower 設定的主區域。

按照第 5a 至 5c 節中的說明修改每個現有資源，如下所示。

步驟一個。 AWS Config 記錄器資源

每個 AWS 區域只能存在一個 AWS Config 記錄器。如果存在，請如圖所示修改設定。在您的居住地區域中將該物品GLOBAL_RESOURCE_RECORDING替換為 true。對於 AWS Config 記錄器存在的其他區域，請將該項目替換為 false。

- 產品名稱:不要改變
- RoleARN： IAM_ROLE_ARN
  - RecordingGroup:

- AllSupported: 真
- IncludeGlobalResourceTypes: GLOBAL_RESOURCE_RECORDING
- ResourceTypes: 空白

此修改可以通過 AWS CLI 使用以下命令進行。將字串取代為現RECORDER_NAME有的 AWS Config 記錄器名稱。

```
aws configservice put-configuration-recorder --configuration-recorder
  name=RECORDER_NAME,roleARN=arn:aws:iam::MEMBER_ACCOUNT_NUMBER:role/
aws-controltower-ConfigRecorderRole-customer-created --recording-group
 allSupported=true,includeGlobalResourceTypes=GLOBAL_RESOURCE_RECORDING --
region CURRENT_REGION
```

步驟五. 修改 AWS Config 交付管道資源

每個區域只能有一個 AWS Config 傳遞通道。如果存在另一個，請如圖所示修改設定。

- 產品名稱:不要改變
- ConfigSnapshotDeliveryProperties: TwentyFour _ 小時
- S3BucketName：來自 AWS Control Tower 記錄帳戶的記錄儲存貯體名稱

  `aws-controltower-logs-LOGGING_ACCOUNT-HOME_REGION`
- S3KeyPrefix：##識別碼 (_ID)
- SnsTopicARN：來自稽核帳戶的 SNS 主題 ARN，格式如下：

  `arn:aws:sns:CURRENT_REGION:AUDIT_ACCOUNT:aws-controltower-AllConfigNotifications`

此修改可以通過 AWS CLI 使用以下命令進行。將字串取代為現*DELIVERY_CHANNEL_NAME*有的 AWS Config 記錄器名稱。

```
aws configservice put-delivery-channel --delivery-channel
 name=DELIVERY_CHANNEL_NAME,s3BucketName=aws-controltower-
logs-LOGGING_ACCOUNT_ID-
```

```
HOME_REGION,s3KeyPrefix="ORGANIZATION_ID",configSnapshotDeliveryProperties={deliveryFrequency=T
controltower-AllConfigNotifications --region CURRENT_REGION
```

步驟 5c。修改 AWS Config 彙總授權資源

每個區域可以存在多個彙總授權。AWS Control Tower 需要彙總授權，將稽核帳戶指定為授權帳戶，並將 AWS Control Tower 的主區域作為授權區域。如果它不存在，請使用以下設置創建一個新的：

- AuthorizedAccountId：稽核帳戶識別碼
- AuthorizedAwsRegion：AWS Control Tower 設定的本地區域

您可以使用下列命令透過 AWS CLI 進行此修改：

```
aws configservice put-aggregation-authorization --authorized-account-
id AUDIT_ACCOUNT_ID --authorized-aws-region HOME_REGION --region
CURRENT_REGION
```

步驟 6：在 AWS Control Tower 管理的區域中建立不存在的資源

修改 AWS CloudFormation 範本，以便在您的主區域中，IncludeGlobalResourcesTypes參數具有值GLOBAL_RESOURCE_RECORDING，如下列範例所示。同時更新範本中的必要欄位，如本節所指定。

在您的居住地區域中將該物品GLOBAL_RESOURCE_RECORDING替換為 true。對於 AWS Config 記錄器存在的其他區域，請將該項目替換為 false。

1. 瀏覽至管理帳戶的 AWS CloudFormation 主控台。
2. StackSet 使用名稱建立新的CustomerCreatedConfigResourcesForControlTower。
3. 複製並更新下列範本：

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure AWS Config
Resources:
  CustomerCreatedConfigRecorder:
    Type: AWS::Config::ConfigurationRecorder
    Properties:
      Name: aws-controltower-BaselineConfigRecorder-customer-created
      RoleARN: !Sub arn:aws:iam::${AWS::AccountId}:role/aws-controltower-
ConfigRecorderRole-customer-created
```

```
      RecordingGroup:
        AllSupported: true
        IncludeGlobalResourceTypes: GLOBAL_RESOURCE_RECORDING
        ResourceTypes: []
  CustomerCreatedConfigDeliveryChannel:
    Type: AWS::Config::DeliveryChannel
    Properties:
      Name: aws-controltower-BaselineConfigDeliveryChannel-customer-created
      ConfigSnapshotDeliveryProperties:
        DeliveryFrequency: TwentyFour_Hours
      S3BucketName: aws-controltower-logs-LOGGING_ACCOUNT-HOME_REGION
      S3KeyPrefix: ORGANIZATION_ID
      SnsTopicARN: !Sub arn:aws:sns:${AWS::Region}:AUDIT_ACCOUNT:aws-controltower-
AllConfigNotifications
  CustomerCreatedAggregationAuthorization:
    Type: "AWS::Config::AggregationAuthorization"
    Properties:
      AuthorizedAccountId: AUDIT_ACCOUNT
      AuthorizedAwsRegion: HOME_REGION
```

使用必填欄位更新範本：

a. *# S3 BucketName ########## ID #####*

b. 在 S3 KeyPrefix 欄位中，取代*## ID*

c. *# SnsTopicARN ##########*

d. 在AuthorizedAccountId欄位中，取代*##*帳戶

e. 在該AuthorizedAwsRegion字段中，替換*##* _ 地區

4. 在 AWS CloudFormation 主控台上部署期間，請新增成員帳戶號碼。
5. 新增在步驟 4 中識別的 AWS 區域。
6. 部署堆疊集。

步驟 7：向 AWS Control Tower 註冊 OU

在 AWS Control Tower 儀表板中，註冊 OU。

> **Note**
>
> 註冊帳戶工作流程無法成功執行此工作。您必須選擇 [註冊 OU] 或 [重新註冊 OU]。

使用 Account Factory 佈建和管理帳戶

本章包含在 AWS Control Tower landing zone 透過 Account Factory 佈建新成員帳戶的概觀和程序。

設定和佈建帳戶的權限

AWS Control 塔 Account Factory 可讓雲端管理員和使用者在 AWS IAM Identity Center 您的 landing zone 佈建帳戶。根據預設，佈建帳戶的 IAM 身分中心使用者必須位於`AWSAccountFactory`群組或管理群組中。

> **Note**
>
> 使用管理帳戶時請小心謹慎，就像在整個組織中使用任何具有權限的帳戶一樣。

AWS Control Tower 管理帳戶與`AWSControlTowerExecution`角色具有信任關係，允許從管理帳戶設定帳戶，包括一些自動化帳戶設定。如需有關角色的`AWSControlTowerExecution`詳細資訊，請參閱角色和帳號。

> **Note**
>
> 若要 AWS 帳戶 將現有的 AWS Control Tower 註冊，該帳戶必須啟用`AWSControlTowerExecution`角色。如需如何註冊現有帳戶的詳細資訊，請參閱註冊現有的 AWS 帳戶。

如需許可的詳細資訊，請參閱「帳戶所需的權限」。

使用 AWS Service Catalog Account Factory 佈建帳戶

下列程序說明如何透過 IAM 身分中心以使用者身分建立和佈建帳戶 AWS Service Catalog。此程序也稱為進階帳戶佈建或手動帳號佈建。或者，您也可以透過 AWS CLI 或使用適用於 Terraform (AFT) 的 AWS Control Tower Account Factory 以程式設計方式佈建帳戶。如果您先前已設定自訂藍圖，則可以在主控台中佈建自訂帳戶。如需自訂的更多資訊，請參閱〈〉使用 Account Factory 定制（AFC）自定義帳戶。

以使用者身分在 Account Factory 中個別佈建帳戶

1. 從您的使用者入口網站 URL 登入。

2. 從您的應用程式中，選擇AWS 帳戶。
3. 從帳戶清單中，選擇管理帳戶的帳戶 ID。此 ID 也可能有標籤，例如 (管理)。
4. 從中AWSServiceCatalogEndUserAccess選擇 [管理主控台]。這會在此帳戶中 AWS Management Console 為此使用者開啟。
5. 確保您已選擇正確的佈 AWS 區域 建帳戶，這應該是您的 AWS Control Tower 區域。
6. 搜尋並選擇 Service Catalog 以開啟 Service Catalog 主控台。
7. 在導覽窗格中，選擇 [產品]。
8. 選取 AWS Control Tower Account Factory，然後選擇啟動產品按鈕。選擇後系統就會啟動精靈來佈建新的帳戶。
9. 填入資訊，並牢記下列各項：
   - SSO UserEmail 可以是新的電子郵件地址，也可以是與現有 IAM 身分中心使用者相關聯的電子郵件地址。無論選擇為何，這名使用者都會擁有您要佈建的帳戶管理存取權。
   - 必AccountEmail須是尚未關聯的電子郵件地址 AWS 帳戶。如果您在 SSO 中使用了新的電子郵件地址UserEmail，則可以在此處使用該電子郵件地址。
10. 請勿定義TagOptions或不啟用通知，否則可能無法佈建帳戶。完成後，請選擇 [啟動產品]。
11. 檢閱您的帳戶設定，然後選擇 Launch (啟動)。請勿建立資源計劃，否則將無法佈建帳號。
12. 正在佈建您的帳戶。這可能需要幾分鐘的時間。您可以重新整理頁面來更新顯示的狀態資訊。

> **Note**
>
> 一次最多可以佈建五個帳戶。

在 Account Factory 中管理帳戶的注意事項

您可以透過 Account Factory 更新、取消管理和關閉您建立和佈建的帳戶。您可以透過更新要重新用途之帳戶中的使用者參數來回收帳戶。您也可以變更帳戶的組織單位 (OU)。

> **Note**
>
> 更新與 Account Factory 出售的帳戶相關聯的佈建產品時，如果您為其指定新的使用者電子郵件地址 AWS IAM Identity Center，AWS Control Tower 會在 IAM 身分中心建立新使用者。先前創建的帳戶不會被刪除。如需從 IAM 身分中心移除先前的 IAM 身分中心使用者電子郵件地址的相關資訊，請參閱停用使用者。

使用 AWS Control Tower 或使用更新和移動帳戶工廠帳戶 AWS Service Catalog

更新註冊帳戶最簡單的方法是透過 AWS Control 塔主控台進行。個人帳戶更新對於解決漂移很有用，例如移動成員帳戶後。作為完整 landing zone 更新的一部分，也需要更新帳號。

如果您將帳戶從一個組織單位 (OU) 移到另一個組織單位 (OU)，請記住，新 OU 套用的控制項可能與先前 OU 中的控制項不同。請確定新 OU 中的控制項符合帳戶的原則需求。

控制在兩者之間移動帳號時的行為 OU

當您在 OU 之間移動帳戶時，目的地 OU 的控制項會套用至 帳戶。不過，從前一個 OU 套用至帳戶的控制項並不是 刪除。控制項的確切行為特定於 在先前 OU 和目的地 OU 上處於作用中的控制項。

- 針對使用 AWS Config 規則實作的控制項：先前 OU 的控制項 不會移除。必須手動移除這些控制項。
- 對於使用 SCP 實作的控制項：先前 OU 中的以 SCP 為基礎的控制項為 刪除。目的地 OU 的以 SCP 為基礎的控制項會在此帳戶上生效。
- 對於使用 AWS CloudFormation 鉤子實現的控件：此行為 取決於新 OU 中控制項的狀態。
  - 如果目標 OU 沒有作用中的掛接式控制項：舊 已移動帳戶的控制項會保持作用中狀態，除非您將其移除 手動。
  - 如果目的地 OU 具有作用中的掛接控制項：舊的控制項為 已移除，目的地 OU 中的控制項會套用至 帳戶。

更新主控台中的帳戶

在 AWS Control Tower 主控台中更新帳戶

1. 登入 AWS Control Tower 後，導覽至組織頁面。
2. 在 OU 和帳戶清單中，選取您要更新的帳戶名稱。可用於更新的帳號會顯示 [可用的更新] 狀態。
3. 接下來，您將看到所選帳戶的「帳戶詳細信息」頁面。
4. 選擇右上角的 [更新帳戶]。

更新佈建的產品

下列程序會引導您如何更新帳戶在 [Account Factory] 中更新您的帳戶，或將其移至新的 OU，方法是更新 Service Catalog 中帳戶的佈建產品。

透過 Service Catalog 更新帳戶 Account Factory 帳戶或變更其 OU

1. 登入 AWS 管理主控台，然後開啟 AWS Service Catalog 主控台，網址為 https://console.aws.amazon.com/servicecatalog/。

   > **Note**
   >
   > 您必須以具有權限的使用者身分登入，才能在 Service Catalog 中佈建新產品 (例如，IAM 身分中心使用者`AWSAccountFactory`或`AWSServiceCatalogAdmins`群組)。

2. 在瀏覽窗格中，選擇佈建，然後選擇已佈建的產品。
3. 對於列出的每個成員帳戶，執行下列步驟來更新所有成員帳戶：

   a. 選擇一個成員帳戶。系統會將您導向至該帳戶的佈建產品詳細資料頁面。

   b. 在佈建的產品詳細資訊頁面上，選擇事件索引標籤。

   c. 記下以下參數：

      - SSO UserEmail (可在佈建的產品詳細資料中找到)
      - AccountEmail(可在佈建產品詳細資料中找到)
      - SSO UserFirstName (適用於 IAM 身分識別中心)
      - SSU SerLastName (適用於 IAM 身分識別中心)
      - AccountName(適用於 IAM 身分識別中心)

   d. 從 Actions (動作)，選擇 Update (更新)。

   e. 選擇要更新產品之 Version (版本) 旁的按鈕，然後選擇 Next (下一步)。

   f. 提供前述的參數值。

      - 如果您想要保留現有的 OU ManagedOrganizationalUnit，請選擇帳戶所在的 OU。
      - 如果您要將帳戶遷移到新的 OU ManagedOrganizationalUnit，請選擇該帳戶的新 OU。

      中央雲端管理員可以在 AWS Control Tower 主控台的組織頁面上找到此資訊。

   g. 選擇下一步。

   h. 檢閱您的變更，然後選擇 Update (更新)。每個帳戶的這個過程都需要幾分鐘的時間。

更改註冊帳戶的電子郵件地址

若要在 AWS Control Tower 中變更已註冊成員帳戶的電子郵件地址，請遵循本節中的程序。

> **Note**
>
> 下列程序不允許您變更管理帳戶、記錄封存帳戶或稽核帳戶的電子郵件地址。如需詳細資訊，請參閱如何變更與我 AWS 帳戶相關聯的電子郵件地址？ 或聯絡 S AWS upport。

變更 AWS Control Tower 建立之帳戶的電子郵件地址

1. 復原帳號的根使用者密碼。您可以按照文章中的步驟操作如何恢復丟失或忘記的 AWS 密碼？
2. 使用 root 使用者密碼登入帳戶。
3. 如同其他電子郵件地址一樣變更電子郵件地址 AWS 帳戶，然後等待變更反映出來 AWS Organizations。電子郵件地址變更完成更新時，您可能會遇到延遲的情況。
4. 使用先前屬於帳戶的電子郵件地址更新 Service Catalog 中的佈建產品。更新已佈建產品的程序包括將新的電子郵件地址與已佈建產品相關聯。如此一來，電子郵件地址變更會在 AWS Control Tower 中生效。使用新的電子郵件地址更新後續佈建的產品。

若要變更您所建立之成員帳戶的密碼或電子郵件地址 AWS Organizations，請參閱《使用指南》中的「以 root 使用者身分存取成員帳戶」AWS Organizations 。

變更已註冊帳戶的名稱

請按照本節中的程序變更已註冊 AWS Control Tower 帳戶的名稱。

> **Note**
>
> 若要變更管理 AWS 員帳戶的名稱，您必須擁有管理員權限，並以該帳戶的 root 使用者身分登入。

變更 AWS Control Tower 建立的帳戶名稱

1. 復原帳號的根密碼。您可以按照本文中概述的步驟操作：如何恢復丟失或忘記的 AWS 密碼？
2. 使用 root 密碼登入帳戶。
3. 在 AWS Billing 主控台中，瀏覽至 [帳戶設定] 頁面。

4. 變更 [帳戶] 設定中的名稱，就像您變更其他任何其他名稱一樣 AWS 帳戶。
5. AWS Control Tower 會自動更新以反映名稱變更。此更新不會反映在中的佈建產品中 AWS Service Catalog。

使用 Amazon 虛擬私有雲設定來設定 Account Factory

Account Factory 可讓您為組織中的帳戶建立預先核准的基準和組態選項。您可以透過 AWS Service Catalog設定和佈建新的帳戶。

在 [Account Factory] 頁面上，您可以看到組織單位 (OU) 的清單及其允許清單狀態。根據預設，所有 OU 都在允許清單中，這表示帳戶可以在這些 OU 下佈建。您可以透過停用帳戶佈建的特定 OU AWS Service Catalog。

您可以檢視最終使用者佈建新帳戶時可用的 Amazon VPC 組態選項。

若要在 Account Factory 中設定 Amazon VPC 設定

1. 身為中央雲端管理員，使用管理帳戶中的管理員許可登入 AWS Control Tower 主控台。
2. 從儀表板的左側，選取「Account Factory」以導覽至「Account Factory」網路組態頁面。您可以在該處看到顯示的預設網路設定。若要編輯，請選取編輯並檢視 Account Factory 網路組態設定的可編輯版本。
3. 您可以視需要修改預設設定的每個欄位。選擇您要為最終使用者可能建立的所有新 Account Factory 帳戶建立的 VPC 組態選項，然後在欄位中輸入您的設定。

- 選擇停用或啟用以在 Amazon VPC 中建立公有子網路。根據預設，不允許可從網際網路存取的子網路。

> **Note**
>
> 如果您設定帳戶工廠 VPC 配置，以便在佈建新帳戶時啟用公用子網路，則帳戶工廠會設定 Amazon VPC 以建立 NAT 閘道。Amazon VPC 將向您收取您的使用費用。如需詳細資訊，請參閱VPC; 定價。

- 從清單中選擇 Amazon VPC 中私有子網路的最大數量。根據預設，選取 1。每個可用區域允許的私有子網路數目上限為 2 個。
- 輸入建立帳戶 VPC 的 IP 地址範圍。此值必須是無類別網域間路由 (CIDR) 區塊的格式 (例如，預設為 `172.31.0.0/16`)。此 CIDR 區塊為 Account Factory 為您的帳戶建立的 VPC 提供子網路 IP 位

址的整體範圍。在您的 VPC 中，子網路會從您指定的範圍自動指派，且大小相等。根據預設，VPC 中的子網路不會重疊。不過，在您所有已佈建帳戶的 VPC 中，子網路 IP 位址範圍可能會重疊。

- 選擇佈建帳戶時，建立 VPC 的一個區域或所有區域。預設為選取所有可用的區域。
- 從清單選擇可用區域數，以在每個 VPC 中設定子網路。預設及建議數字是三個。
- 選擇儲存。

您可以設定這些組態選項，以建立不包含 VPC 的新帳戶。請參閱演練。

取消管理帳戶

如果您在 Account Factory 建立帳戶或註冊帳戶 AWS 帳戶，但不想再由 landing zone 中的 AWS Control Tower 管理該帳戶，則可以從 AWS Control Tower 主控台取消管理該帳戶。

取消管理 AWS Control Tower 帳戶時，AWS Control Tower 佈建的所有資源都會移除，包括任何藍圖。該帳戶會從任何 AWS Control Tower OU 移出並移至根區域。該帳戶不再是已註冊 OU 的一部分，而且不再受 AWS Control Tower SCP 的約束。您可以透過以下方式關閉帳戶 AWS Organizations。

取消管理帳戶也可以由`AWSAccountFactory`群組中的 IAM 身分中心使用者在 Service Catalog 主控台中完成，方法是終止已佈建的產品。如需 IAM 身分中心使用者或群組的詳細資訊，請參閱管理使用者和透過存取 AWS IAM Identity Center。下列程序說明如何取消管理 Service Catalog 中的成員帳戶。

若要取消管理已註冊的帳戶

1. 在您的網頁瀏覽器中開啟 Service Catalog 主控台，位於https://console.aws.amazon.com/servicecatalog。
2. 在左側導覽窗格中，選擇已佈建的產品清單。
3. 從佈建帳戶清單中，選擇您希望 AWS Control Tower 不再管理的帳戶名稱。
4. 在 Provisioned product details (佈建的產品詳細資訊) 頁面上，從 Actions (動作) 選單選擇 Terminate (終止)。
5. 從出現的對話方塊選擇 Terminate (終止)。

> **Important**
>
> 終止字詞特定於 Service Catalog。當您終止 Service Catalog 帳戶 Factory 中的帳戶時，帳戶不會關閉。此動作會將帳戶從其 OU 和您的 landing zone 移除。

6. 帳戶未受管理時，其狀態會變更為「未註冊」。
7. 如果您不再需要該帳戶，請將其關閉。如需關閉 AWS 帳戶的詳細資訊，請參閱AWS Billing 使用者指南中的關閉帳戶

取消管理自訂帳戶時，AWS Control Tower 會移除藍圖已部署的資源，以及 AWS Control Tower 在帳戶中建立的任何其他資源。取消管理帳戶後，您可以透過 AWS Organizations以下方式關閉帳戶。

> **Note**
>
> 未受管理的帳戶不會關閉或刪除。帳戶未受管理時，您在帳戶 Factory 中建立帳戶時選取的 IAM 身分中心使用者仍具有該帳戶的管理存取權。如果您不希望此使用者具有管理存取權，則必須在 IAM 身分中心變更此設定，方法是更新 Account Factory 中的帳戶，並變更帳戶的 IAM 身分中心使用者電子郵件地址。如需詳細資訊，請參閱 使用 AWS Control Tower 或使用更新和移動帳戶工廠帳戶 AWS Service Catalog。

影片演練

這部影片 (3:25) 說明如何從 AWS Control Tower 移除帳戶、取得帳戶的 root 存取權，最後關閉. AWS 帳戶您也可以使用 AWS Organizations API 關閉帳戶。若要獲得更佳的觀賞效果，請選取影片右下角的圖示，將影片放大至全螢幕。並提供字幕。

在 AWS Control Tower 中關閉帳戶的影片逐步解說。

您可以在 AWS Control Tower 中檢 AWS YouTube 視說明常見任務的影片清單。

關閉在 Account Factory 中創建的帳戶

在「Account Factory」中創建的帳戶是 AWS 帳戶。如需關閉的詳細資訊 AWS 帳戶，請參閱《帳戶管理參考指南》中的關閉AWS帳戶。

> **Note**
>
> 關閉帳 AWS 帳戶 戶與從 AWS Control Tower 取消管理帳戶並不相同 — 這些是單獨的動作。您必須先取消管理帳戶，才能關閉帳戶。

透過以下方式關閉 AWS Control Tower 成員帳戶 AWS Organizations

您可以從組織的管理帳戶關閉 AWS Control Tower 成員帳戶，而無需透過 root 登入資料個別登入每個成員帳戶登入 AWS Organizations。但是，您無法以這種方式關閉管理帳戶。

當您調用 AWS Organizations CloseAccountAPI 或在 AWS Organizations 控制台中關閉帳戶時，成員帳戶 AWS 帳戶 將被隔離 90 天，就像任何一樣。該帳戶在 AWS Control Tower 和中顯示已暫停狀態 AWS Organizations。如果您在該 90 天內嘗試使用該帳戶，AWS Control Tower 會顯示錯誤訊息。

在 90 天到期之前，您可以恢復成員帳戶，就像使用任何帳戶一樣 AWS 帳戶。在 90 天之後，帳戶的記錄將被刪除。

我們建議您在關閉帳戶之前取消管理會員帳戶，做為最佳作法。如果您在未先取消管理的情況下關閉成員帳戶，AWS Control Tower 會將該帳戶的狀態顯示為「已暫停」，但也會顯示為「已註冊」。因此，如果您在 90 天期間嘗試重新註冊帳戶的 OU，AWS Control Tower 會產生錯誤訊息。暫停的帳戶基本上會在預先檢查失敗的情況下封鎖重新註冊動作。如果您從 OU 中移除帳戶，您可以重新註冊 OU，但可 AWS 能會產生關於該帳戶缺少付款方式的錯誤。若要解決此限制，請先建立另一個 OU，然後將帳戶移至該 OU，然後再嘗試重新註冊。我們建議將此 OU 命名為 [暫停的 OU]。

> **Note**
>
> 如果您沒有在關閉帳戶之前取消管理帳戶，則必須在 90 天完成 AWS Service Catalog 後刪除帳戶的佈建產品。

有關更多信息，請參 AWS Organizations 閱有關 CloseAccountAPI 的文檔。

Account Factory 的資源考量

使用帳戶 Factory 佈建帳戶時，會在帳戶中建立下列 AWS 資源。

AWS 服務	資源類型	資源名稱
AWS CloudFormation	堆疊	StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL-* StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-*

AWS 服務	資源類型	資源名稱
		StackSet-AWSControlTowerBP-BASELINE-CONFIG-* StackSet-AWSControlTowerBP-BASELINE-ROLES-* StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES-*
AWS CloudTrail	追蹤	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch 活動規則	aws-controltower-ConfigComplianceChangeEventRule
Amazon CloudWatch	CloudWatch 日誌	aws-controltower/CloudTrailLogs /aws/lambda/aws-controltower-NotificationForwarder

AWS 服務	資源類型	資源名稱
AWS Identity and Access Management	角色	aws-controltower-AdministratorExecutionRole aws-controltower-CloudWatchLogsRole aws-controltower-ConfigRecorderRole aws-controltower-ForwardSnsNotificationRole aws-controltower-ReadOnlyExecutionRole AWSControlTowerExecution
AWS Identity and Access Management	政策	AWSControlTowerServiceRolePolicy
Amazon Simple Notification Service	主題	aws-controltower-SecurityNotifications
AWS Lambda	應用程式	StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-*
AWS Lambda	函數	aws-controltower-NotificationForwarder

使用 Account Factory 定制（AFC）自定義帳戶

當您從 AWS Control Tower 主控台佈建資源 AWS 帳戶 時，AWS Control Tower 可讓您自訂新的和現有的資源。設定帳戶工廠自訂後，AWS Control Tower 會自動執行此程序以供 future 佈建使用，因此您不必維護任何管道。自訂帳戶可在佈建資源後立即使用。

您的自訂帳戶是在帳戶工廠、透過 AWS CloudFormation 範本或 Terraform 佈建。您將定義做為自訂帳戶藍圖的範本。您的藍圖描述佈建帳戶時所需的特定資源和組態。同時也提供由 AWS 合作夥伴建置和管理的預先定義藍圖。如需有關合作夥伴管理的藍圖的詳細資訊，請參閱AWS Service Catalog 入門程式庫。

> **Note**
>
> AWS Control Tower 包含主動控制，可監控 AWS Control Tower 中的 AWS CloudFormation 資源。或者，您可以在 landing zone 中啟用這些控制項。當您套用主動式控制時，它們會檢查以確保您將要部署到帳戶的資源符合組織的政策和程序。如需主動式控制的詳細資訊，請參閱主動式控制。

您的帳戶藍圖存儲在 AWS 帳戶，出於我們的目的，稱為 Hub 帳戶。藍圖會以 Service Catalog 產品的形式儲存。我們稱此產品為藍圖，以便與其他任何 Service Catalog 產品區分開來。若要深入瞭解如何建立 Service Catalog 產品，請參閱《AWS Service Catalog 管理員指南》中的〈建立產品〉。

將藍圖套用至現有帳戶

您也可以依照 AWS Control Tower 主控台中的更新帳戶步驟，將自訂藍圖套用至現有帳戶。如需詳細資訊，請參閱 更新主控台中的帳戶。

> **開始之前**
>
> 在 AWS Control 塔 Account Factory 開始建立自訂帳戶之前，您必須部署 AWS Control Tower landing zone 環境，而且您必須在 AWS Control Tower 註冊組織單位 (OU)，並在其中放置新建立的帳戶。

如需使用 AFC 的詳細資訊，請參閱使用 AWS Control Tower 中的 Account Factory 自訂自動化帳戶。

定制準備

- 您可以建立新帳戶做為 Hub 帳戶，也可以使用現有帳戶 AWS 帳戶。強烈建議您不要使用 AWS Control Tower 管理帳戶做為藍圖中樞帳戶。
- 如果您打算註冊 AWS Control Tower 並對其 AWS 帳戶 進行自訂，則必須先將`AWSControlTowerExecution`角色新增到這些帳戶，就像對註冊 AWS Control Tower 的任何其他帳戶一樣。

- 如果您計劃使用具有市場訂閱需求的合作夥伴藍圖，則必須先從 AWS Control Tower 管理帳戶設定這些藍圖，然後再將合作夥伴藍圖部署為帳戶工廠自訂藍圖。

主題

設定以進行自訂

接下來的章節提供了為自訂程序設定 Account Factory 的步驟。我們建議您先為 Hub 帳戶設定委派管理員，然後再開始執行這些步驟。

Summary

- 步驟 1. 建立必要的角色。建立 IAM 角色，授予 AWS Control Tower 存取 (Hub) 帳戶的權限，該帳戶存放 Service Catalog 產品 (也稱為藍圖)。
- 步驟 2. 建立 AWS Service Catalog 產品。建立基準自訂帳戶所 AWS Service Catalog 需的產品 (也稱為「藍圖產品」)。
- 步驟 3. 檢閱您的自訂藍圖。檢查您建立的 AWS Service Catalog 產品 (藍圖)。
- 步驟 4. 呼叫您的藍圖以建立自訂帳戶。在建立帳戶時，在 AWS Control Tower 主控台的 Account Factory 的適當欄位中輸入藍圖產品資訊和角色資訊。

步驟 1. 建立必要的角色

在開始自訂帳戶之前，您必須設定包含 AWS Control Tower 和您的中樞帳戶之間信任關係的角色。假設此角色時，此角色會授予 AWS Control Tower 管理中樞帳戶的存取權。角色必須命名AWSControlTowerBlueprintAccess。

AWS Control Tower 擔任此角色代表您建立 Portfolio 資源 AWS Service Catalog，然後將藍圖作為 Service Catalog 產品新增至此產品組合，然後在帳戶佈建期間與您的成員帳戶共用此產品組合和您的藍圖。

您將建立AWSControlTowerBlueprintAccess角色，如以下各節所述。

導覽至 IAM 主控台以設定所需角色。

在已註冊的 AWS Control Tower 帳戶中設定角色

1. 在 AWS Control Tower 管理帳戶中聯合或以主體身分登入。
2. 從管理帳戶中的聯合主體中，假設角色或將角色切換為您選擇作為藍圖中樞帳戶的已註冊 AWS Control Tower 帳戶中的角色。AWSControlTowerExecution
3. 從已註冊 AWS Control Tower 帳戶中的AWSControlTowerBlueprintAccess角色建立具有適當許可和信任關係的角色。AWSControlTowerExecution

Note

為了遵守 AWS 最佳做法指引，建立角色後立即登出AWSControlTowerExecution角色非常重要。AWSControlTowerBlueprintAccess
為防止資源發生意外變更，此AWSControlTowerExecution角色僅供 AWS Control Tower 使用。

如果您的藍圖中樞帳戶未在 AWS Control Tower 中註冊，則該AWSControlTowerExecution角色不會存在於帳戶中，而且在繼續設定角色之前不需要假設AWSControlTowerBlueprintAccess角色。

若要在取消註冊的成員帳戶中設定角色

1. 透過您偏好的方法，聯合或以您想要指定為 Hub 帳戶的帳戶中的主體身分登入。

2. 以帳戶中的主參與者身分登入時，請建立具有適當權限和信任關係的AWSControlTowerBlueprintAccess角色。

必須將AWSControlTowerBlueprintAccess角色設定為將信任授與兩個主體：

- 在 AWS Control Tower 管理帳戶中執行 AWS Control Tower 的主體 (使用者)。
- AWS Control Tower 管理帳戶AWSControlTowerAdmin中指名的角色。

以下是信任政策範例，類似於您角色需要包含的信任政策。此原則示範授與最低權限存取權的最佳作法。當您制定自己的政策時，請使*YourManagementAccountId*用 AWS Control Tower 管理帳戶的實際會員 ID 取代該術語，並以管理帳戶*YourControlTowerUserRole*的 IAM 角色識別碼取代該術語。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                "arn:aws:iam::YourManagementAccountId:role/service-role/
AWSControlTowerAdmin",
                "arn:aws:iam::YourManagementAccountId:role/YourControlTowerUserRole"
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

必要的權限原則

AWS Control Tower 要求AWSServiceCatalogAdminFullAccess必須將具名的受管政策附加到AWSControlTowerBlueprintAccess角色上。此政策提供許可，以 AWS Service Catalog 尋找何時允許 AWS Control Tower 管理您的產品組合和 AWS Service Catalog 產品資源。您可以在 IAM 主控台中建立角色時附加此政策。

可能需要其他權限

- 如果您將藍圖存放在 Amazon S3，AWS Control Tower 也需要該`AWSControlTowerBlueprintAccess`角色的`AmazonS3ReadOnlyAccess`許可政策。
- 如果您不使用預設管理政策，則 AWS Service Catalog Terraform 類型的產品會要求您在 AFC 自訂 IAM 政策中新增一些其他許可。除了建立您在地形範本中定義的資源所需的權限之外，還需要這些權限。

步驟 2. 建立產 AWS Service Catalog 品

若要建立 AWS Service Catalog 產品，請遵循《AWS Service Catalog 管理員指南》中〈建立產品〉中的步驟。建立產品時，您會將帳戶藍圖新增為範 AWS Service Catalog 本。

Important

由於 Terraform 授權 HashiCorp的更新，將對 T erraform 開放原始碼產品和佈建產品的支援 AWS Service Catalog 變更為新的產品類型 (稱為外部)。若要深入瞭解此變更如何影響 AFC，包括如何將現有帳戶藍圖更新為外部產品類型，請參閱轉換為外部產品類型。

建立藍圖的步驟摘要

- 建立或下載將成為您帳戶藍圖的 AWS CloudFormation 範本或地形 tar.gz 設定檔。本節稍後會提供一些範本範例。
- 登入您儲存 Account Factory 藍圖的 AWS 帳戶 位置 (有時稱為 Hub 帳戶)。
- 導覽至主 AWS Service Catalog 控台。選擇 [產品清單]，然後選擇 [上傳新產品]。
- 在產品詳細資料窗格中，輸入藍圖產品的詳細資料，例如名稱和描述。
- 選取「使用範本檔案」，然後選取「選擇檔案」。選取或貼上您已開發或下載以用作藍圖的範本或設定檔。
- 選擇主控台頁面底部的 [建立產品]。

您可以從 AWS Service Catalog 參考架構存儲庫下載 AWS CloudFormation 模板。該儲存庫中的一個範例有助於為您的資源設定備份計畫。

這是一個名為 B est Pets 的虛構公司的示例模板。它有助於建立到他們的寵物數據庫的連接。

```
Resources:
  ConnectionStringGeneratorLambdaRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - lambda.amazonaws.com
            Action:
              - "sts:AssumeRole"
  ConnectionStringGeneratorLambda:
    Type: AWS::Lambda::Function
    Properties:
      FunctionName: !Join ['-', ['ConnectionStringGenerator', !Select [4, !Split
 ['-', !Select [2, !Split ['/', !Ref AWS::StackId]]]]]]
      Description: Retrieves the connection string for this account to access the Pet
 Database
      Role: !GetAtt ConnectionStringGeneratorLambdaRole.Arn
      Runtime: nodejs16.x
      Handler: index.handler
      Timeout: 5
      Code:
        ZipFile: >
          const response = require("cfn-response");
          exports.handler = function (event, context) {
            const awsAccountId = context.invokedFunctionArn.split(":")[4]
            const connectionString= "fake connection string that's specific to account
 " + awsAccountId;
            const responseData = {
              Value: connectionString,
            }
            response.send(event, context, response.SUCCESS, responseData);
            return connectionString;
          };

  ConnectionString:
    Type: Custom::ConnectionStringGenerator
    Properties:
      ServiceToken: !GetAtt ConnectionStringGeneratorLambda.Arn
```

```
  PetDatabaseConnectionString:
    DependsOn: ConnectionString
    # For example purposes we're using SSM parameter store.
    # In your template, use secure alternatives to store
    # sensitive values such as connection strings.
    Type: AWS::SSM::Parameter
    Properties:
      Name: pet-database-connection-string
      Description: Connection information for the BestPets pet database
      Type: String
      Value: !GetAtt ConnectionString.Value
```

步驟 3。檢閱您的自訂藍圖

您可以在 AWS Service Catalog 主控台中檢視藍圖。如需詳細資訊，請參閱《Service Catalog 管理員指南》中的〈管理產品〉。

步驟 4. 呼叫您的藍圖以建立自訂帳戶

在 AWS Control Tower 主控台中按照建立帳戶工作流程進行操作時，您會看到一個選擇性部分，您可以在其中輸入要用於自訂帳戶之藍圖的相關資訊。

> **Note**
>
> 您必須先設定自訂中樞帳戶並新增至少一個藍圖 (Service Catalog 產品)，然後才能將該資訊輸入 AWS Control Tower 主控台並開始佈建自訂帳戶。

在 AWS Control Tower 主控台中建立或更新自訂帳戶。

1. 輸入包含藍圖之帳戶的帳戶 ID。
2. 從該帳戶中，選取現有的 Service Catalog 產品 (現有藍圖)。
3. 如果您有多個版本，請選取藍圖 (Service Catalog 產品) 的正確版本。
4. (選擇性) 您可以在程序中此時新增或變更藍圖佈建原則。藍圖佈建政策以 JSON 撰寫並連結至 IAM 角色，因此可佈建藍圖範本中指定的資源。AWS Control Tower 會在成員帳戶中建立此角色，讓 Service Catalog 可以使用 AWS CloudFormation 堆疊集部署資源。角色已命名 `AWSControlTower-BlueprintExecution-bp-xxxx`。依預設，此處會套用`AdministratorAccess`原則。
5. 根據此藍圖選擇您要在其中部署帳戶的 AWS 區域 或區域。

6. 如果藍圖包含參數，則可以在 AWS Control Tower 工作流程的其他欄位中輸入參數值。其他值可能包括： GitHub 存放庫名稱、分 GitHub 支、Amazon ECS 叢集名稱以及儲存庫擁有者的 GitHub 身分。
7. 如果您的 Hub 帳戶或藍圖尚未準備就緒，您可以在稍後按照帳戶更新程序自訂帳戶。

如需詳細資訊，請參閱從藍圖建立自訂帳戶。

從藍圖建立自訂帳戶

建立自訂藍圖之後，您可以開始在 AWS Control Tower 帳戶工廠中建立自訂帳戶。

建立新 AWS 帳戶時，請依照下列步驟部署自訂藍圖：

1. 前往中的 AWS Control Tower AWS Management Console。
2. 選擇帳戶工廠和創建帳戶。
3. 輸入帳戶詳細信息，例如帳戶名稱和電子郵件地址。
4. 使用電子郵件地址和使用者名稱設定 IAM 身分中心詳細資料
5. 選取要在其中新增帳戶的已註冊 OU。
6. 展開「帳戶工廠自訂」區段。
7. 輸入包含 Service Catalog 產品之藍圖中樞帳戶的帳戶識別碼，然後選擇驗證。如需藍圖中樞帳戶的相關資訊，請參閱使用 Account Factory 定制（AFC）自定義帳戶。
8. 從 Service Catalog 產品清單 (所有自訂和合作夥伴藍圖) 中選取包含所有藍圖的下拉式功能表。選擇要部署的藍圖和對應版本。
9. 如果您的藍圖包含參數，則會顯示這些欄位供您填入。預設值會預先填入。
10. 最後，選取您要部署藍圖的位置，無論是「主區域」或「所有受控管的區域」。全球資源 (例如 Route 53 或 IAM) 可能只需要部署到單一區域。區域資源 (例如 Amazon EC2 執行個體或 Amazon S3 儲存貯體) 可部署到所有受管轄的區域
11. 完成所有欄位後，選取 [建立帳戶]。

> **Note**
>
> 使用 Terraform 建立的藍圖只能部署到一個區域，而不能部署到多個區域。

您可以在 [組織] 頁面上檢視帳戶佈建的進度。帳戶佈建完成後，藍圖指定的資源已在其中部署。若要檢視帳戶和藍圖的詳細資料，請移至帳戶詳細資料頁面。

註冊和自訂帳戶

在 AWS Control Tower 主控台中註冊和自訂帳戶。

1. 導覽至 AWS Control 塔主控台，然後從左側導覽選取組織。
2. 您將看到可用帳戶的列表。識別您要使用自訂藍圖註冊的帳戶。該帳戶的 [狀態] 欄應反映帳戶處於 [未註冊] 狀態。
3. 選取帳號左側的選項按鈕，然後選擇畫面右上角的 [動作] 下拉式功能表。在這裡，您將選擇註冊選項。
4. 使用帳戶的 IAM 身分中心資訊完成存取設定部分。
5. 選擇您的帳戶將成為會員的註冊 OU。
6. 使用與建立帳戶程序的 7-12 相同的步驟完成「帳戶工廠自訂」區段。如需詳細資訊，請參閱使用佈建 Account Factory 帳戶 AWS Service Catalog。

您可以在「組織」頁面上查看帳戶進度的狀態。帳戶註冊完成後，藍圖指定的資源已在其中部署。

將藍圖新增到 AWS Control Tower 帳戶

若要將藍圖新增到現有的 AWS Control Tower 成員帳戶，請按照 AWS Control Tower 主控台中的更新帳戶工作流程進行操作，然後選擇要新增到帳戶的新藍圖。如需詳細資訊，請參閱使用 AWS Control Tower 或使用更新和移動 Account Factory 帳戶 AWS Service Catalog。

> **Note**
>
> 如果您將新藍圖新增至帳戶，則會覆寫現有藍圖。

> **Note**
>
> 每個 AWS Control Tower 帳戶可部署一個藍圖。

更新藍圖

下列程序說明如何更新自訂藍圖以及如何部署它們。

更新您的自訂藍圖

1. 使用新的組態更新 AWS CloudFormation 範本或地形 tar.gz 檔案 (藍圖)。
2. 將更新的藍圖儲存為中的新版本 AWS Service Catalog。

部署更新的藍圖

1. 導覽至 AWS Control Tower 主控台中的組織頁面。
2. 依藍圖名稱和版本篩選 [組織] 頁面。
3. 遵循更新帳戶程序，並在您的帳戶中部署最新的藍圖版本。

如果藍圖更新不成功

當佈建的產品處於AVAILABLE狀態時，AWS Control Tower 允許藍圖更新。如果您佈建的產品處於某個TAINTED狀態，則更新將會失敗。我們建議使用下列因應措施：

1. 在 AWS Service Catalog 主控台中，手動更新TAINTED已佈建的產品以將狀態變更為AVAILABLE。如需詳細資訊，請參閱更新佈建的產品。
2. 接著，依照 AWS Control Tower 的更新帳戶程序，修正藍圖部署錯誤。

我們建議您執行此手動步驟，因為：移除藍圖時，可能會導致成員帳戶中的資源遭到移除。移除資源可能會影響現有的工作負載。因此，我們建議使用此方法，而不是更新藍圖的替代方法，也就是移除和取代原始藍圖，尤其是在執行生產工作負載時。

從帳戶移除藍圖

若要從帳戶移除藍圖，請按照更新帳戶工作流程移除藍圖，並將該帳戶返回 AWS Control Tower 預設組態。

當您在主控台中輸入 Update 帳戶工作流程時，您會看到所有帳戶詳細資料都已填入，而且不會填入自訂詳細資料。如果將這些 AFC 詳細資料保留空白，AWS Control Tower 會從帳戶中移除藍圖。在動作開始之前，您會看到警告訊息。

> **Note**
>
> 只有在建立帳戶或更新帳戶程序期間選取藍圖時，AWS Control Tower 才會將藍圖新增至帳戶。

合作夥伴藍圖

AWS Control Tower Account Factory 自訂 (AFC) 可讓您存取由 AWS 合作夥伴建立和管理的預先定義自訂藍圖。這些合作夥伴藍圖可協助您針對特定使用案例自訂帳戶。每個合作夥伴的藍圖都可協助您建立自訂帳戶，這些帳戶已預先設定為與該特定合作夥伴提供的產品供應項目搭配使用。

若要檢視 AWS Control Tower 合作夥伴藍圖的完整清單，請導覽至主控台中的 Service Catalog 入門程式庫。搜尋來源類型 AWS Control Tower 藍圖。

Account Factory 自訂 (AFC) 的注意事項

- AFC 僅支援使用單一 AWS Service Catalog 藍圖產品進行自訂。
- AWS Service Catalog 藍圖產品必須在 Hub 帳戶中建立，並在與 AWS Control Tower 登陸區域主區域相同的區域中建立。
- `AWSControlTowerBlueprintAccess`IAM 角色必須使用適當的名稱、許可和信任政策建立。
- AWS Control Tower 支援兩種藍圖的部署選項：僅部署到本地區域，或部署到由 AWS Control Tower 管理的所有區域。無法選取區域。
- 當您更新成員帳戶中的藍圖時，無法變更藍圖中樞帳戶 ID 和 AWS Service Catalog 藍圖產品。
- AWS Control Tower 不支援在單一藍圖更新作業中移除現有藍圖和新增藍圖。您可以移除藍圖，然後在不同的作業中新增藍圖。
- AWS Control Tower 會根據您要建立或註冊自訂帳戶或非自訂帳戶而變更行為。如果您不是使用藍圖建立或註冊自訂帳戶，AWS Control Tower 會在 AWS Control Tower 管理帳戶中建立 Account Factory 佈建的產品 (透過 Service Catalog)。如果您在使用藍圖建立或註冊帳戶時指定自訂，AWS Control Tower 不會在 AWS Control Tower 管理帳戶中建立 Account Factory 佈建的產品。

如果發生藍圖錯誤

套用藍圖時發生錯誤

如果在將藍圖套用至帳戶 (新帳戶或您註冊 AWS Control Tower 的現有帳戶) 的過程中發生錯誤，復原程序也是相同的。該帳戶將存在，但不是自訂帳戶，也不會註冊到 AWS Control Tower。若要繼續，請按照以下步驟將帳戶註冊到 AWS Control Tower，並在註冊時新增藍圖。

建立**`AWSControlTowerBlueprintAccess`**角色時發生錯誤，以及因應措施

從 AWS Control Tower 帳戶建立AWSControlTowerBlueprintAccess角色時，您必須使用該AWSControlTowerExecution角色以主體身分登入。如果您以任何其他方式登入，則 SCP 會阻止該CreateRole作業，如下列成品所示：

```
{
            "Condition": {
                "ArnNotLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::*:role/AWSControlTowerExecution",
                        "arn:aws:iam::*:role/stacksets-exec-*"
                    ]
                }
            },
            "Action": [
                "iam:AttachRolePolicy",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:DeleteRolePermissionsBoundary",
                "iam:DeleteRolePolicy",
                "iam:DetachRolePolicy",
                "iam:PutRolePermissionsBoundary",
                "iam:PutRolePolicy",
                "iam:UpdateAssumeRolePolicy",
                "iam:UpdateRole",
                "iam:UpdateRoleDescription"
            ],
            "Resource": [
                "arn:aws:iam::*:role/aws-controltower-*",
                "arn:aws:iam::*:role/*AWSControlTower*",
                "arn:aws:iam::*:role/stacksets-exec-*"
            ],
            "Effect": "Deny",
            "Sid": "GRIAMROLEPOLICY"
        }
```

以下是可用的因應措施：

- (最建議使用) AWSControlTowerExecution 扮演角色並建立AWSControlTowerBlueprintAccess角色。如果您選擇此因應措施，請務必在之後立即登出AWSControlTowerExecution角色，以防止資源發生意外變更。
- 登入未註冊 AWS Control Tower 的帳戶，因此不受此 SCP 約束。

- 暫時編輯此 SCP 以允許此作業。
- (強烈不建議使用) 使用您的 AWS Control Tower 管理帳戶做為您的中樞帳戶，因此不受 SCP 的約束。

根據 AFC 藍圖自訂政策文件 CloudFormation

當您透過帳戶工廠啟用藍圖時，AWS Control Tower 會 AWS CloudFormation 指示代表您建 StackSet 立藍圖。 AWS CloudFormation 需要存取您的受管理帳戶，才能在中建立 AWS CloudFormation 堆疊 StackSet。雖然 AWS CloudFormation 已經透過`AWSControlTowerExecution`角色在受管理帳戶中擁有系統管理員權限，但無法保證此角色。 AWS CloudFormation

AWS Control Tower 會在成員帳戶中建立角色，做為啟用藍圖的一部分，該角色 AWS CloudFormation 可能會假設完成 StackSet 管理任務。透過帳戶工廠啟用自訂藍圖的最簡單方法是使用允許所有原則，因為這些原則與任何藍圖範本相容。

不過，最佳做法建議您必須限制目標帳戶 AWS CloudFormation 中的權限。您可以提供自訂政策，AWS Control Tower 將該政策套用至其建立 AWS CloudFormation 要使用的角色。例如，如果您的藍圖建立稱為某些重要的 SSM 參數，您可以提供下列原則：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCloudFormationActionsOnStacks",
            "Effect": "Allow",
            "Action": "cloudformation:*",
            "Resource": "arn:aws:cloudformation:*:*:stack/*"
        },
        {
            "Sid": "AllowSsmParameterActions",
            "Effect": "Allow",
            "Action": [
                "ssm:PutParameter",
                 "ssm:DeleteParameter",
                 "ssm:GetParameter",
                 "ssm:GetParameters"
            ],
            "Resource": "arn:*:ssm:*:*:parameter/something-important"
        }
    ]
```

```
}
```

所有 AFC 自訂原則都需要此`AllowCloudFormationActionsOnStacks`陳述式； AWS CloudFormation 使用此角色建立堆疊執行個體，因此需要對堆疊執行 AWS CloudFormation 動作的權限。此`AllowSsmParameterActions`區段專屬於要啟用的範本。

解決權限問題

當您啟用具有受限原則的藍圖時，您可能會發現沒有足夠的權限無法啟用藍圖。若要解決這些問題，請修訂您的政策文件，並更新成員帳戶的藍圖偏好設定，以使用更正後的原則。若要檢查原則是否足以啟用藍圖，請確定已授與 AWS CloudFormation 權限，並且您可以直接使用該角色建立堆疊。

建立以 Terraform 為基礎的 Service Catalog 產品所需的其他權限

當您使用 AFC 的 Terraform 設定檔建立 AWS Service Catalog 外部產品時，除了建立範本中定義的資源所 AWS Service Catalog 需的許可之外，還需要將某些許可新增至您的 AFC 自訂 IAM 政策。如果您選擇預設的完整管理員原則，則不需要新增這些額外權限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "resource-groups:CreateGroup",
                "resource-groups:ListGroupResources",
                "resource-groups:DeleteGroup",
                "resource-groups:Tag"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "tag:GetResources",
                "tag:GetTagKeys",
                "tag:GetTagValues",
                "tag:TagResources",
                "tag:UntagResources"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
```

```
        {
            "Action": "s3:GetObject",
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "s3:ExistingObjectTag/servicecatalog:provisioning": "true"
                }
            }
        }
    ]
}
```

如需有關在中使用外部產品類型建立 Terraform 產品的詳細資訊 AWS Service Catalog，請參閱《Service Catalog 管理員指南》中的步驟 5：建立啟動角色。

使用 AWS Control Tower Account Factory 為地形 (AFT) 佈建帳戶

適用於地形 (AFT) 的 AWS Control Tower Account Factory 採用一種 GitOps 模型，可在 AWS Control Tower 中自動化帳戶佈建和更新程序。

> **Note**
>
> AFT 不會影響 AWS Control Tower 的工作流程效能。如果您透過 AFT 或 Account Factory 佈建帳戶，則會發生相同的後端工作流程。

使用 AFT 時，您可以建立帳戶要求 Terraform 檔案，其中包含呼叫 AFT 工作流程的輸入。帳戶佈建和更新完成後，AFT 工作流程會繼續執行 AFT 帳戶佈建架構和帳戶自訂步驟。

必要條件

開始使用 AFT 之前，您必須建立下列項目：

- 完全部署的 AFT 環境。如需詳細資訊，請參閱地形 (AFT) 的 AWS Control Tower Account Factory 概觀和部署適用於地形的 AWS Control Tower Account Factory (AFT)
- 完全部署的 AFT 環境中的一或多個 AFT `git` 儲存庫。如需詳細資訊，請參閱 AFT 的部署後步驟。

> **Tip**
>
> 或者，您可以在aft-account-customizations存放庫中建立帳戶範本資料夾。

如需 AFT AWS 區域 在何處有部署限制的資訊，請參閱AWS Control Tower 的限制和配額和控制限制。

在 AFT 提供新帳戶

要使用 AFT 佈建新帳戶，請創建一個帳戶請求 Terraform 文件。此檔案包含aft-account-request儲存庫中參數的輸入。建立帳戶要求 Terraform 檔案後，請開始執行處理您的帳戶要求。`git push`此命令會叫用中的`ct-aft-account-request`作業 AWS CodePipeline，該作業會在帳戶佈建完成後於 AFT 管理帳戶中建立。如需詳細資訊，請參閱 AFT 帳戶佈建管線。

帳戶請求地形文件參數

您必須在帳戶要求 Terraform 檔案中包含下列參數。您可以在上檢視帳戶請求範例 Terraform 檔案。GitHub

- 的值在每個 AWS 帳戶 請求中`module name`必須是唯一的。
- 的值`module source`是 AFT 提供的帳戶要求 Terraform 模組的路徑。
- 的值會`control_tower_parameters`擷取建立 AWS Control Tower 帳戶所需的輸入。該值包括下列輸入欄位：
  - `AccountEmail`
  - `AccountName`
  - `ManagedOrganizationalUnit`
  - `SSOUserEmail`
  - `SSOUserFirstName`
  - `SSOUserLastName`

> **Note**
>
> 您提供的輸入`control_tower_parameters`在帳戶佈建期間無法變更。
> 在aft-account-request儲存庫`ManagedOrganizationalUnit`中指定的支援格式包括`OUName`和`OUName (OU-ID)`。

- account_tags會擷取使用者定義的索引鍵與值，這些索引鍵與值可 AWS 帳戶 根據商業準則 如需詳細資訊，請參閱《使用指南》中的AWS Organizations 〈標記 AWS Organizations 資源〉。
- 的值會change_management_parameters擷取其他資訊，例如建立帳戶請求的原因以及啟動帳戶請求的人員。該值包括下列輸入欄位：
  - change_reason
  - change_requested_by
- custom_fields在 /aft/帳戶請求/自訂欄位/ 下，擷取其他中繼資料，其中包含以 SSM 參數部署為 SSM 參數的金鑰和值。您可以在帳戶自訂期間參考此中繼資料，以部署適當的控制。例如，受法規遵循的帳戶可能會部署其他帳戶 AWS Config 規則。您收集的中繼資料custom_fields可以在帳戶佈建和更新期間叫用其他處理。如果從帳戶要求中移除自訂欄位，則會從付費帳戶的 SSM 參數存放區中移除自訂欄位。
- (選擇性) account_customizations_name 擷取aft-account-customizations存放庫中的帳戶範本資料夾。如需詳細資訊，請參閱帳戶自訂。

提交多個帳戶請求

AFT 一次處理一個帳戶請求，但您可以向 AFT 管道提交多個帳戶請求。當您向 AFT 管道提交多個帳戶請求時，AFT 會以先進先出的順序將帳戶請求排入佇列並處理。

> **Note**
>
> 您可以為每個要 AFT 佈建或串聯在單一帳戶請求 Terraform 檔案中的帳戶建立帳戶請求 Terraform 檔案。

更新現有帳戶

您可以編輯先前提交的帳戶請求並執行git push，以更新 AFT 佈建的帳戶。此命令會叫用帳戶佈建工作流程，並可處理帳戶更新要求。您可以在帳戶請求 Terraform 檔案中更新輸入 (屬於必要值的一部分)control_tower_parameters，以及其他參數。ManagedOrganizationalUnit如需詳細資訊，請參閱使用 AFT 佈建新帳戶。

> **Note**
>
> 您提供的輸入在帳戶佈建期間control_tower_parameters無法變更。

在aft-account-request儲存庫ManagedOrganizationalUnit中指定的支援格式包括OUName和OUName (OU-ID)。

更新未佈建 AFT 的帳戶

您可以在aft-account-request儲存庫中指定帳戶，更新在 AFT 以外建立的 AWS Control Tower 帳戶。

> **Note**
>
> 確保所有帳戶詳細資料均正確無誤，並與 AWS Control Tower 組織及個別 AWS Service Catalog 佈建的產品一致。

AWS 帳戶 使用 AFT 更新現有的先決條件

- 必 AWS 帳戶 須在 AWS Control Tower 註冊。
- AWS 帳戶 必須是 AWS Control Tower 組織的一員。

部署適用於地形 (AFT) 的 AWS Control Tower Account Factory

本節適用於希望在現有環境中設定 Terraform (AFT) Account Factory 的 AWS Control Tower 環境管理員。它說明如何使用新的專用 AFT 管理帳戶為 Terraform (AFT) 環境設定 Account Factory。

> **Note**
>
> 地形模塊部署 AFT。該模塊可在 AFT 存儲庫中使用 GitHub，整個 AFT 存儲庫被視為模塊。我們建議您參考的 AFT 模組， GitHub 而不是複製 AFT 儲存庫。通過這種方式，您可以控制和使用模塊的更新，因為它們是可用的。

如需有關適用於 Traform (AFT) 的 AWS Control Tower Account Factory 最新版本的詳細資訊，請參閱此儲存庫的版本檔案。 GitHub

部署先決條

在設定及啟動 AFT 環境之前，您必須具備下列條件：

- AWS Control Tower landing zone。如需詳細資訊，請參閱規劃 AWS Control Tower landing zone。
- AWS Control Tower 登陸區域的本地區域。如需詳細資訊，請參閱如何 AWS 區域 使用 AWS Control Tower。
- 地形版本和發行版本。如需詳細資訊，請參閱地形和 AF T 版本。
- 用於追蹤和管理程式碼和其他檔案變更的 VCS 提供者。依預設，AFT 會使用 AWS CodeCommit。如需詳細資訊，請參閱什麼是 AWS CodeCommit？ 在《AWS CodeCommit 使用者指南》中。如果您想選擇其他 VCS 提供程序，請參閱 AFT 中源代碼版本控制的替代方法。
- 一個運行時環境，您可以在其中運行安裝 AFT 的 Terraform 模塊。
- 尾部功能選項。如需詳細資訊，請參閱啟用功能選項。

設定和啟動適用於地形的 AWS Control Tower Account Factory

下列步驟假設您熟悉 Terraform 工作流程。您也可以參閱 AWS Workshop Studio 網站上的 AFT 實驗室簡介，進一步了解如何部署 AFT。

步驟 1：啟動 AWS Control Tower landing zone

完成 AWS Control Tower 入門中的步驟。您可以在這裡建立 AWS Control Tower 管理帳戶並設定 AWS Control Tower landing zone。

> **Note**
>
> 確保為具有AdministratorAccess登入資料的 AWS Control Tower 管理帳戶建立角色。如需詳細資訊，請參閱下列內容：
>
> - 使用者指南中的 IAM 身分 (使用者、使AWS Identity and Access Management 用者群組和角色)
> - AdministratorAccess在《AWS 受管理策略參考指南》中

步驟 2：為 AFT 建立新的組織單位 (建議使用)

建議您在 AWS 組織中建立個別的 OU。這是您部署 AFT 管理帳戶的地方。使用 AWS Control Tower 管理帳戶建立新的 OU。如需詳細資訊，請參閱建立新的 OU。

步驟 3：提供 AFT 管理帳戶

AFT 要求您佈建專用於 AFT 管理作業的 AWS 帳戶。與 AWS Control Tower landing zone 相關聯的 AWS Control Tower 管理帳戶會由 AFT 管理帳戶提供服務。如需詳細資訊，請參閱使用帳 AWS Service Catalog 戶 Factory 佈建帳戶。

> **Note**
>
> 如果您為 AFT 建立了個別的 OU，請務必在建立 AFT 管理帳戶時選取此 OU。

完全佈建 AFT 管理帳戶最多可能需要 30 分鐘。

步驟 4：確認 Terraform 環境是否可用於部署

此步驟假設您具有使用 Terraform 的經驗，並具有執行 Terraform 的程序。如需詳細資訊，請參閱 HashiCorp 開發人員網站上的命令：init。

> **Note**
>
> AFT 支援地形版本或更高版本`1.2.0`。

步驟 5：呼叫地形模組的 Account Factory 以部署 AFT

使用您為具有AdministratorAccess登入資料的 AWS Control Tower 管理帳戶建立的角色呼叫 AFT 模組。AWS Control Tower 會透過 AWS Control Tower 管理帳戶佈建 Terraform 模組，以建立協調 AWS Control Tower Account Factory 請求所需的所有基礎設施。

您可以在上檢視 AFT 儲存庫中的 AFT 模組。 GitHub整個 GitHub 存儲庫被認為是 AFT 模塊。如需執行 AFT 模組和部署 AFT 所需輸入的詳細資訊，請參閱 README 檔案。或者，您也可以在 Terra form 登錄中檢視 AFT 模組。

AFT 模組包含一個`aft_enable_vpc`參數，用於指定 AWS Control Tower 是否在中央 AFT 管理帳戶的虛擬私有雲 (VPC) 內佈建帳戶資源。依預設，參數設定為`true`。如果將此參數設定為`false`，則 AWS Control Tower 會在不使用 VPC 和私有網路資源 (例如 NAT 閘道或 VPC 端點) 的情況下部署 AFT。停用`aft_enable_vpc`可能有助於降低某些使用模式的 AFT 運作成本。

> **Note**
>
> 重新啟用`aft_enable_vpc`參數 (將值從切換`false`為`true`) 可能需要您連續執行兩次`terraform apply`指令。

如果您的環境中已建立管道來管理 Terraform，則可以將 AFT 模組整合到現有的工作流程中。否則，請從使用所需認證進行驗證的任何環境中執行 AFT 模組。

逾時會導致部署失敗。我們建議您使用 AWS Security Token Service (STS) 認證，以確保您的逾時足以進行完整部署。 AWS STS 認證的逾時時間下限為 60 分鐘。如需詳細資訊，請參閱AWS Identity and Access Management 使用指南中 IAM 中的臨時安全登入資料。

> **Note**
>
> 您最多可能需要等待 30 分鐘，讓 AFT 透過 Terraform 模組完成部署。

步驟 6：管理地形狀態檔案

部署 AFT 時，會產生地形狀態檔案。此成品描述了 Terraform 所建立之資源的狀態。如果您打算更新 AFT 版本，請務必預先設定地形狀態檔案，或使用 Amazon S3 和 DynamoDB 設定地形後端。AFT 模組不會管理後端地形狀態。

> **Note**
>
> 您有責任保護地形狀態檔案。某些輸入變數可能包含敏感值，例如私ssh密金鑰或 Terraform 權杖。視您的部署方法而定，這些值可在 Terraform 狀態檔案中以純文字的形式檢視。如需詳細資訊，請參閱 HashiCorp 網站上的「州/省」中的敏感資料。

部署後步驟

AFT 基礎結構部署完成後，請依照下列額外步驟完成設定程序，並準備好佈建帳戶。

步驟 1：（可選）CodeConnections 與所需的 VCS 提供商完成

如果您選擇第三方 VCS 提供商，AFT 會建立 CodeConnections並確認它們。請參閱AFT 中源代碼版本控制的替代方案以瞭解如何使用您偏好的 VCS 設定 AFT。

建立 AWS CodeStar 連接的初始步驟由 AFT 完成。您必須確認連接。

步驟 2：(必要) 填入每個儲存庫

AFT 要求您管理四個存儲庫：

1. 帳戶請求 — 此存儲庫處理放置或更新帳戶請求。可用的例子。如需 AFT 帳戶要求的詳細資訊，請參閱在 AFT 提供新帳戶。
2. AFT 帳戶佈建自訂 — 此儲存庫會在開始全域自訂階段之前，管理套用至由 AFT 建立和管理之所有帳戶的自訂。可用的例子。若要建立 AFT 帳戶佈建自訂，請參閱建立您的 AFT 帳戶佈建自訂狀態機器。
3. 全域自訂 — 此儲存庫會管理套用至由 AFT 建立及管理之所有帳戶的自訂。可用的例子。若要建立 AFT 全域自訂，請參閱套用全域自訂。
4. 帳戶自訂 — 此存放庫管理僅套用至由 AFT 建立和管理之特定帳戶的自訂。可用的例子。若要建立 AFT 帳戶自訂，請參閱套用帳戶自訂。

AFT 預期這些儲存庫都遵循特定的目錄結構。用來填入儲存庫的範本，以及說明如何填入範本的指示，可在 AFT github 儲存庫的 Terraform Account Factory 模組中取得。

適用於地形的 AWS Control Tower Account Factory (AFT) 概觀

地形 Account Factory (AFT) 會設定 Terraform 管道，以協助您在 AWS Control Tower 中佈建和自訂帳戶。AFT 為您提供基於地形的帳戶佈建的優勢，同時允許您使用 AWS Control Tower 管理帳戶。

透過 AFT，您可以建立帳戶要求 Terraform 檔案，以取得觸發帳戶佈建之 AFT 工作流程的輸入。帳戶佈建階段完成後，AFT 會在帳戶自訂階段開始之前自動執行一系列步驟。如需詳細資訊，請參閱 AFT 帳戶佈建管線。

AFT 支持地形雲，地形企業和地形社區版。使用 AFT，您可以使用輸入文件和簡單的`git push`命令啟動帳戶創建，並自定義新帳戶或現有帳戶。帳戶建立包括所有 AWS Control Tower 管理權益和帳戶自訂項目，可協助您符合組織的標準安全程序和合規準則。

AFT 支援帳戶自訂要求追蹤。每次您提交帳戶自訂要求時，AFT 都會產生一個唯一的追蹤權杖，該 Token 會通過 AFT 自訂 AWS Step Functions 狀態機器進行記錄，並將權杖記錄為其執行的一部分。然後，您可以使用 Amazon CloudWatch Logs 深入解析查詢來搜尋時間戳記範圍並擷取請求權杖。因此，您可以看到令牌隨附的有效載荷，因此您可以在整個 AFT 工作流程中跟踪帳戶自定義請求。如需 CloudWatch 記錄檔和 Step Functions 的相關資訊，請參閱下列內容：

- 什麼是 Amazon CloudWatch 日誌？ 在 Amazon CloudWatch 日誌用戶指南
- 什麼是 AWS Step Functions？ 在AWS Step Functions 開發人員指南中

AFT 結合了其他 AWS 服務的功能組件服務，以構建框架，以及部署 Terraform 基礎結構即代碼（IaC）的管道。AFT 讓您能夠：

- 在 GitOps 模型中提交帳戶佈建和更新請求
- 儲存帳戶中繼資料和稽核記錄
- 套用帳戶層級標記
- 將自訂新增至所有帳戶、一組帳戶或個別帳戶
- 啟用功能選項

AFT 會建立另一個帳戶 (稱為 AFT 管理帳戶) 來部署 AFT 功能。在設定 AFT 之前，您必須先擁有現有的 AWS Control Tower landing zone。AFT 管理帳戶與 AWS Control Tower 管理帳戶不同。

AFT 提供靈活性

- 為您的平台提供靈活性：AFT 支持任何 Terraform 分發以進行初始部署和正在進行的操作：社區版，雲和企業版。
- 版本控制系統的靈活性：AFT 本身依賴 AWS CodeCommit，但它支持. CodeConnections

AFT 提供功能選項

您可以根據最佳做法啟用數個功能選項：

- 建立 CloudTrail 用於記錄資料事件的組織層級
- 刪除帳戶的 AWS 預設 VPC
- 將佈建帳戶註冊至 AWS 企業 Support 方案

> **Note**
>
> AFT 管道不適用於部署帳戶執行應用程式所需的資源 (例如 Amazon EC2 執行個體)。它僅用於 AWS Control Tower 帳戶的自動佈建和自訂。

影片演練

本影片 (7:33) 說明如何使用適用於地形的 AWS Control Tower Account Factory 部署帳戶。若要獲得更佳的觀賞效果，請選取影片右下角的圖示，將影片放大至全螢幕。並提供字幕。

AWS Control Tower 中自動化帳戶佈建的影片逐步解說。

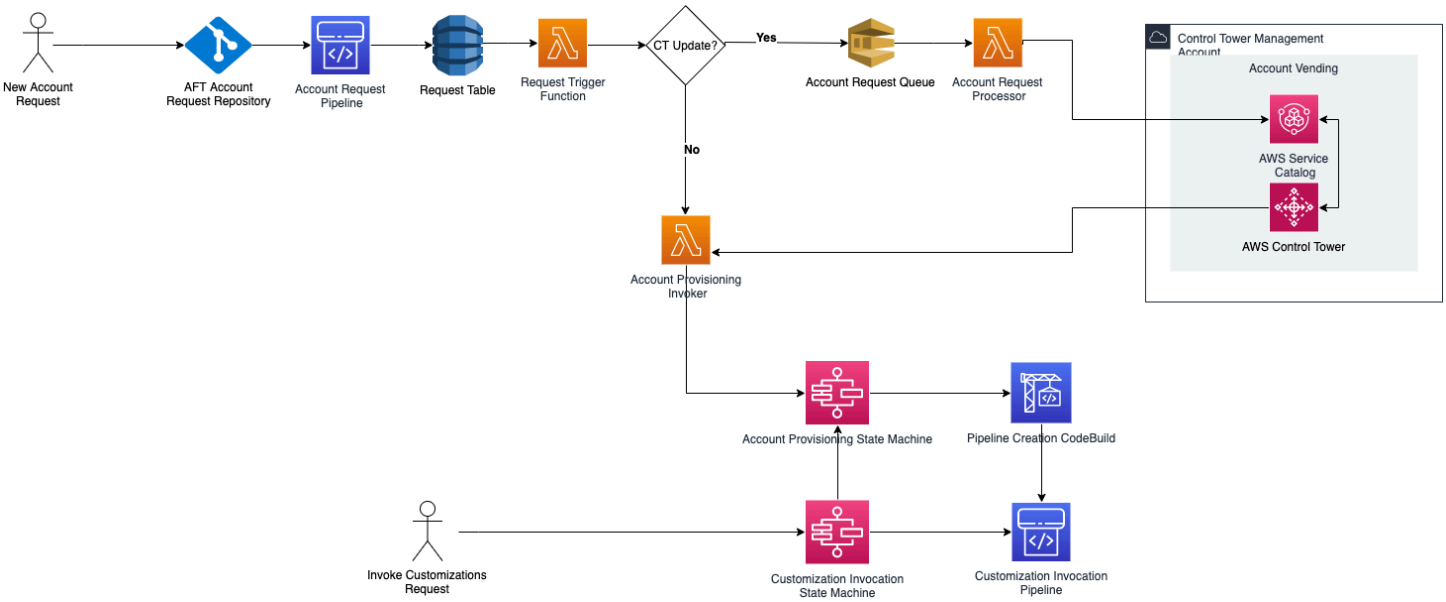
船尾架構

操作順序

您在 AFT 管理帳戶中執行 AFT 作業。對於完整的帳戶佈建工作流程，圖表中階段從左到右的順序如下：

1. 帳戶請求已建立並提交至管道。您一次可以創建並提交多個帳戶請求。Account Factory 會以 first-in-first-out 訂單處理要求。如需詳細資訊，請參閱提交多個帳戶請求。
2. 每個帳戶都已佈建。此階段會在 AWS Control Tower 管理帳戶中執行。
3. 全域自訂會在針對每個付費帳戶建立的管道中執行。
4. 如果在初始帳戶佈建請求中指定了自訂，則自訂只會在目標帳戶上執行。如果您擁有已佈建的帳戶，則必須在帳戶的管道中手動啟動進一步的自訂。

適用於地形的 AWS Control Tower Account Factory — 帳戶佈建工作流程



費用

AFT 不會收取額外費用。您只需為 AFT 部署的資源、AFT 啟用的 AWS 服務，以及您在 AFT 環境中部署的資源付費。

預設 AFT 組態包括 AWS PrivateLink 端點的配置、增強的資料保護和安全性，以及支援 AWS CodeBuild所需的 NAT 閘道。如需此基礎設施定價的詳細資訊，請參閱 NAT 閘道的定AWS PrivateLink 價和 Amazon VPC 定價。如需管理這些成本的詳細資訊，請連絡您的 AWS 客戶代表。您可以變更 AFT 的這些預設設定。

地形和 AFT 版本

地形（AFT）的 Account Factory 支持地形版本或更高版本。`1.2.0`您必須提供 Terraform 版本做為 AFT 部署程序的輸入參數，如下列範例所示。

```
terraform_version = "1.2.0"
```

地形分佈

AFT 支持三種地形分佈：

- 地形社區版
- 地形雲
- 地形企業

這些發行版將在以下各節中進行說明。在 AFT 引導過程中，提供您選擇的 Terraform 分佈作為輸入參數。如需 AFT 部署和輸入參數的詳細資訊，請參閱部署適用於地形 (AFT) 的 AWS Control Tower Account Factory。

如果您選擇 Terraform 雲端或 Terraform 企業發行版，則您指定的 API 權杖`terraform_token` 必須是使用者或團隊 API 權杖。並非所有必要的 API 都支援組織權杖。基於安全性考量，您必須透過指定 terraform 變數來避免將此權杖的值簽入版本控制系統 (VCS)，如下列範例所示。

```
# Sensitive variable managed in Terraform Cloud:
terraform_token = var.terraform_cloud_token
```

地形社區版

當您選擇 Terraform 社區版作為您的發行版時，AFT 會在 AFT 管理帳戶中為您管理 Terraform 後端。AFT 會下載您指定`terraform-cli`的 Terraform 版本，以便在 AFT 部署和 AFT 管道階段執行。產生的 Terraform 狀態組態會存放在 Amazon S3 儲存貯體中，以下列格式命名：

```
aft-backend-[account_id]-primary-region
```

AFT 還會建立一個 Amazon S3 儲存貯體，將您的 Terraform 狀態組態複製到另一個儲存貯體中 AWS 區域，以災難復原目的，並以下列格式命名：

```
aft-backend-[account_id]-secondary-region
```

我們建議您針對這些 Terraform 狀態 Amazon S3 儲存貯體上的刪除功能啟用多因素身份驗證 (MFA)。要了解有關地形社區版的更多信息，請參閱地形文檔。

若要選取 Terraform OSS 作為您的發行版本，請提供下列輸入參數：

```
terraform_distribution = "oss"
```

地形雲

當您選取 Terraform 雲端作為發佈時，AFT 會在 Terraform Cloud 組織中為下列元件建立工作區，以啟動 API 導向的工作流程。

- 帳戶請求
- AFT 規定之帳戶的 AFT 自訂
- AFT 規定之帳戶的帳戶自訂
- AFT 佈建之帳戶的全域自訂

地形雲管理產生的地形狀態配置。

當您選取 Terraform 雲端作為您的發佈時，請提供下列輸入參數：

- `terraform_distribution = "tfc"`
- `terraform_token`— 此參數包含地形雲端權杖的值。AFT 會將值標記為機密，並將值儲存為 AFT 管理帳戶的 SSM 參數存放區中的安全字串。我們建議您根據公司的安全性原則和合規性準則，定期輪換 Terraform 權杖的值。地形令牌應該是用戶或團隊級別的 API 令牌。不支援組織權杖。
- `terraform_org_name`— 此參數包含您的地形雲端組織的名稱。

> **Note**
>
> 不支援單一 Terraform 雲端組織中的多個 AFT 部署。

如需如何設定地形雲端的詳細資訊，請參閱地形文件。

地形企業

當您選取 Terraform 企業版作為您的發佈時，AFT 會為您的 Terraform 企業組織中的下列元件建立工作區，並觸發 API 導向的工作流程，以便產生的 Terraform 執行。

- 帳戶請求
- AFT 佈建之帳戶的 AFT 帳戶佈建自訂
- AFT 佈建之帳戶的帳戶自訂
- AFT 佈建之帳戶的全域自訂

產生的地形表單狀態配置由您的地形企業安裝管理。

若要選取 Terraform 企業作為您的發行版，請提供下列輸入參數：

- `terraform_distribution = "tfe"`
- `terraform_token`— 此參數包含您的地形企業權杖的值。AFT 會將其值標記為機密值，並將其儲存為安全字串在 SSM 參數存放區的 AFT 管理帳戶中。我們建議您根據貴公司的安全性原則和合規性準則，定期輪換 Terraform 權杖的值。
- `terraform_org_name`— 此參數包含您的 Terraform 企業組織的名稱。
- `terraform_api_endpoint`— 此參數包含您的地形企業環境的 URL。此參數的值必須是格式：

```
https://{fqdn}/api/v2/
```

請參閱 Terraform 文件以進一步了解如何設定地形企業版。

檢查船尾版本

您可以透過查詢 AWS SSM 參數存放區金鑰來檢查已部署的 AFT 版本：

```
/aft/config/aft/version
```

如果您使用登錄方法，您可以釘選版本。

```
module "control_tower_account_factory" {
  source  = "aws-ia/control_tower_account_factory/aws"
  version = "1.3.2"
  # insert the 6 required variables here
```

```
}
```

您可以在 AFT 儲存庫中檢視有關 AFT 版本的詳細資訊。

更新船尾版本

您可以通過從main存儲庫分支中提取部署的 AFT 版本來更新它：

```
terraform get -update
```

提取完成後，您可以重新執行 Terraform 計劃或執行套用，以使用最新的變更更新 AFT 基礎結構。

啟用功能選項

AFT 根據最佳實務提供功能選項。在 AFT 部署期間，您可以透過功能旗標選擇加入這些功能。如需有關 AFT 輸入組態參數在 AFT 提供新帳戶的詳細資訊，請參閱。

依預設，這些功能不會啟用。您必須在您的環境中明確啟用每個項目。

主題

- AWS CloudTrail 資料事件
- AWS 企業 Support 計劃
- 刪除預 AWS 設 VPC

AWS CloudTrail 資料事件

啟用時， AWS CloudTrail 資料事件選項會設定這些功能。

- 在 AWS Control Tower 管理帳戶中建立組織追蹤 CloudTrail
- 開啟 Amazon S3 和 Lambda 資料事件的記錄
- 使 AWS KMS 用加密功能，將所有 CloudTrail 資料事件加密並匯出到 AWS Control 塔日誌存檔帳戶中的 `aws-aft-logs-*` S3 儲存貯體
- 開啟記錄檔驗證設定

若要啟用此選項，請在 AFT 部署輸入組態中將下列功能旗標設定為 True。

```
aft_feature_cloudtrail_data_events
```

必要條件

啟用此功能選項之前，請確定組織中已啟用 AWS CloudTrail 的受信任存取權。

若要檢查受信任存取權的狀態 CloudTrail ：

1. 導覽至主 AWS Organizations 控台。
2. 選擇「服務」> CloudTrail。
3. 如有需要，請選取右上角的「啟用受信任存取」。

您可能會收到警告訊息，建議您使用 AWS CloudTrail 主控台，但在此情況下，請忽略警告。在您允許受信任的存取之後，AFT 會建立追蹤，做為啟用此功能選項的一部分。如果未啟用受信任的存取，當 AFT 嘗試建立資料事件的追蹤時，您會收到錯誤訊息。

> **Note**
>
> 此設定適用於組織層級。啟用此設定會影響中的所有帳號 AWS Organizations，不論這些帳號是否由 AFT 管理。啟用時 AWS Control Tower 日誌存檔帳戶中的所有儲存貯體都會從 Amazon S3 資料事件中排除。請參閱使用 AWS CloudTrail 者指南以進一步瞭解相關資訊 CloudTrail。

AWS 企業 Support 計劃

啟用此選項時，AFT 管道會針對 AFT 佈建的帳戶開啟 AWS 企業 Support 計劃。

AWS 根據預設，帳戶會啟用 AWS 基本 Support 方案。AFT 針對 AFT 佈建的帳戶，提供企業支援層級的自動註冊。佈建程序會開啟帳戶的 Support 票證，要求將其新增至 AWS 企業支援方案。

若要啟用「企業 Support」選項，請在 AFT 部署輸入組態中將下列功能旗標設定為 True。

```
aft_feature_enterprise_support=false
```

請參閱比較 Sup AWS port 方案以深入瞭解 Sup AWS port 方案。

> **Note**
>
> 若要允許此功能運作，您必須將付款人帳戶註冊至企業 Support 計劃。

刪除預 AWS 設 VPC

啟用此選項時，AFT 會刪除管理帳戶中的所有 AWS 預設 VPC，並刪除所有預設 VPC AWS 區域，即使這些 VPC 中尚未部署 AWS Control Tower 資源也一樣。 AWS 區域

AFT 不會針對 AFT 佈建的任何 AWS Control Tower 帳戶或透過 AFT 在 AWS Control Tower 註冊的現有 AWS 帳戶自動刪除 AWS 預設 VPC。

根據預設 AWS 區域，每個 AWS 帳戶中都會設定 VPC 來建立新帳戶。您的企業可能具有建立 VPC 的標準做法，因此您必須刪除 AWS 預設 VPC 並避免啟用它，尤其是 AFT 管理帳戶。

若要啟用此選項，請在 AFT 部署輸入組態中將下列功能旗標設定為 True。

```
aft_feature_delete_default_vpcs_enabled
```

如需有關預設 VPC 的詳細資訊，請參閱預設 VPC 和預設子網路。

適用於地形的 AWS Control Tower Account Factory 的資源考量

當您使用適用於 Terraform 的 AWS Control Tower Account Factory 設定 landing zone 時，會在您 AWS 的帳戶中建立數種類型的 AWS 資源。

搜尋資源

- 您可以使用標籤來搜尋最新的 AFT 資源清單。搜尋的索引鍵值配對為：

  ```
  Key: managed_by | Value: AFT
  ```

- 對於不支援標籤的元件服務，您可以在資源名稱`aft`中尋找具有搜尋功能的資源。

最初建立的資源表格 (依帳戶分類)

適用於地形管理帳戶的 AWS Control Tower Account Factory

AWS 服務	Resource Type (資源類型)	資源名稱
AWS Identity and Access Management	角色	AWSAFTAdministrator AWSAFTExecution AWSAFTService

AWS 服務	Resource Type (資源類型)	資源名稱
		aws-ct-aft-*
AWS Identity and Access Management	政策	aws-ct-aft-*
CodeCommit	儲存庫	aws-ct-aft-*
CodeBuild	組建專案	aws-ct-aft-*
代碼管道	管道	*-baseline-*
Amazon S3	儲存貯體	*-aws-ct-aft-* aws-ct-aft-*
Lambda	函數	aws-ct-aft-*
Lambda	圖層	aws-ct-aft-common-layer
DynamoDB	資料表	aws-ct-aft-request aws-ct-aft-request-audit aws-ct-aft-request-metadata aws-ct-aft-controltower-events
Step Functions	狀態機	aws-ct-aft-prebaseline aws-ct-aft-prebaseline-customizations aws-ct-aft-trigger-baseline aws-ct-aft-features
VPC	VPC	aws-ct-aft-vpc

AWS 服務	Resource Type (資源類型)	資源名稱
Amazon SNS	主題	aws-ct-aft-notifications aws-ct-aft-failure-notifications
Amazon EventBridge	事件匯流排	aws-ct-aft-events-from-ct-management
Amazon EventBridge	活動規則	aws-ct-aft-capture-ct-events aws-ct-aft-lambda-account-request-processor
金鑰管理服務	客戶管理的金鑰	*-aws-ct-aft-* aws-ct-aft-*
AWS Systems Manager	參數存放區	/aws-ct-aft/account/* /aws/ct-aft/config/*
Amazon SQS	佇列	aws-ct-aft-account-request.fifo aws-ct-aft-account-request-dlg.fifo
CloudWatch	日誌群組	/aws/*/aws-ct-aft-* aws-ct-aft-*
AWS Support 中心（可選）	Support 方案	Enterprise

AWS 透過 AWS Control Tower Account Factory 為地形佈建的帳戶

AWS 服務	Resource Type (資源類型)	資源名稱
AWS Identity and Access Management	角色	AWSAFTExecution
AWS Support 中心（可選）	Support 方案	Enterprise

AWS Control Tower 管理帳戶

AWS 服務	Resource Type (資源類型)	資源名稱
AWS Identity and Access Management	角色	AWSAFTExecutionRole AWSAFTExecution aws-ct-aft-controltower-events-rule
AWS Systems Manager	參數存放區	/aws-ct-aft/account/aws-ct-aft-management/account-id
AWS Organizations (選擇性)	服務控制政策	aws-ct-aft-protect-resources
CloudTrail (選擇性)	線索	aws-ct-aft-BaselineCloudTrail
AWS Support 中心 (選用)	Support 方案	Enterprise

AWS Control Tower 日誌存檔帳戶

AWS 服務	Resource Type (資源類型)	資源名稱
AWS Identity and Access Management	角色	AWSAFTExecutionRole AWSAFTExecution aws-ct-aft-cloudtrail-data-events-role
金鑰管理服務	客戶管理的金鑰	*-aws-ct-aft-kms-gd-findings
Amazon S3	儲存貯體	*-aws-ct-aft-logs* aws-ct-aft-s3-access-logs*
AWS Support 中心（可選）	Support 方案	Enterprise

AWS Control Tower 稽核帳戶

AWS 服務	Resource Type (資源類型)	資源名稱
AWS Identity and Access Management	角色	AWSAFTExecutionRole AWSAFTExecution
AWS Support 中心（可選）	Support 方案	Enterprise

必要角色

一般而言，角色和政策是中身分識別與存取管理 (IAM) 的一部分 AWS。如需詳細資訊，請參閱 AWS IAM 使用者指南。

AFT 會在 AFT 管理和 AWS Control Tower 管理帳戶中建立多個 IAM 角色和政策，以支援 AFT 管道的操作。這些角色是根據最低權限存取模型建立的，該模型會限制每個角色和原則的最低需要動作和資源集的權限。這些角色和策略被分配一個 AWS 標籤`key:value`配對，作 `managed_by:AFT`為識別。

除了這些 IAM 角色之外，AFT 還建立了三個基本角色：

- 該`AWSAFTAdmin`角色
- 該`AWSAFTExecution`角色
- 該`AWSAFTService`角色

這些角色將在以下各節中說明。

AWSAFTAdmin 角色，解釋

部署 AFT 時，會在 AFT 管理帳戶中建立`AWSAFTAdmin`角色。此角色允許 AFT 管道擔任 AWS Control Tower 和 AFT 佈建帳戶中的`AWSAFTExecution`角色，從而執行與帳戶佈建和自訂相關的動作。

以下是附加至`AWSAFTAdmin`角色的內嵌政策 (JSON 成品)：

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

```
            "Resource": [
                "arn:aws:iam::*:role/AWSAFTExecution",
                "arn:aws:iam::*:role/AWSAFTService"
            ]
        }
    ]
}
```

下列 JSON 成品會顯示AWSAFTAdmin角色的信任關係。預留位置編號012345678901由 AFT 管理帳戶 ID 號碼取代。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

AWSAFTExecution 角色，解釋

部署 AFT 時，會在 AFT 管理和 AWS Control Tower 管理帳戶中建立AWSAFTExecution角色。稍後，AFT 管線會在 AFT 帳戶佈建階段期間，在每個 AFT 佈建的帳戶中建立AWSAFTExecution角色。

AFT 一開始會利用AWSControlTowerExecution角色，在指定的帳戶中建立AWSAFTExecution角色。此AWSAFTExecution角色可讓 AFT 管線執行在 AFT 架構佈建和佈建自訂階段、AFT 佈建帳戶和共用帳戶期間執行的步驟。

> **不同的角色可協助您限制範圍**
>
> 最佳做法是將自訂權限與初始部署資源期間允許的權限分開。請記住，該AWSAFTService角色是用於帳戶佈建，而該AWSAFTExecution角色是用於帳戶自訂。此分隔會限制管線每個階段所允許的權限範圍。如果您要自訂 AWS Control Tower 共用帳戶，此區別特別重要，因為共用帳戶可能包含敏感資訊，例如帳單詳細資訊或使用者資訊。

AWSAFTExecution角色許可：AdministratorAccess— AWS 受管政策

下列 JSON 成品顯示附加至該AWSAFTExecution角色的 IAM 政策 (信任關係)。預留位置編號012345678901由 AFT 管理帳戶 ID 號碼取代。

信任政策 AWSAFTExecution

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/AWSAFTAdmin"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

AWSAFTService 角色，解釋

此AWSAFTService角色會在所有已註冊和受管理的帳戶 (包括共用帳戶和管理帳戶) 中部署 AFT 資源。資源先前僅由AWSAFTExecution角色部署。

此AWSAFTService角色適用於服務基礎結構，以在佈建階段部署資源，而AWSAFTExecution角色僅用於部署自訂項目。通過以這種方式假設角色，您可以在每個階段保持更精細的訪問控制。

AWSAFTService角色許可：AdministratorAccess— AWS 受管政策

下列 JSON 成品顯示附加至該AWSAFTService角色的 IAM 政策 (信任關係)。預留位置編號012345678901由 AFT 管理帳戶 ID 號碼取代。

信任政策 AWSAFTService

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/AWSAFTAdmin"
```

```
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

組件服務

當您部署 AFT 時，元件會從這些 AWS 服務新增至您的 AWS 環境中。

- AWS Control Tower — AFT 使用 AWS Control Tower 管理帳戶中的 AWS Control Tower Account Factory 佈建帳戶。
- Amazon DynamoDB — AFT 會在後端管理帳戶中建立 Amazon DynamoDB 表格，用於存放帳戶請求、帳戶更新的稽核歷史記錄、帳戶中繼資料和 AWS Control Tower 生命週期事件。AFT 也會建立 DynamoDB Lambda 觸發程序來啟動下游程序，例如啟動 AFT 帳戶佈建工作流程。
- 亞馬遜簡單儲存服務 — AFT 在 AFT 管理帳戶和 AWS Control Tower 日誌存檔帳戶中建立 Amazon 簡易儲存服務 (S3) 儲存貯體，這些帳戶會存放由 AFT 管道所需的 AWS 服務產生的日誌。AFT 也會在主要和次要 AWS 區域建立 Terraform 後端 S3 儲存貯體，以存放在 AFT 管道工作流程期間產生的 Terraform 狀態。
- Amazon 簡易通知服務 — AFT 會在 AFT 管理帳戶中建立 Amazon Simple Notification Service (SNS) 主題，該主題會在處理每個 AFT 帳戶請求後儲存成功和失敗通知。您可以使用您選擇的協議收到這些消息。
- Amazon 簡單排隊服務 — AFT 在 AFT 管理帳戶中創建一個 Amazon 簡單排隊服務（Amazon SQS）FIFO 隊列。佇列可讓您 parallel 提交多個帳戶請求，但會一次傳送一個請求至 AWS Control Tower Account Factory，以進行順序處理。
- AWS CodeBuild — AFT 在 AFT 管理帳戶中 CodeBuild 建立 AWS 建置專案，以便在各個建置階段針對 AFT 原始程式碼初始化、編譯、測試和套用 Terraform 計劃。
- AWS CodePipeline — AFT 在 AFT 管理帳戶中建立 AWS 管 CodePipeline 道，以與您選定且受支援的 AWS CodeStar 連線供應商整合 AFT 原始程式碼，並在 AWS 中觸發建置任務。 CodeBuild
- AWS Lambda — AFT 會在後端管理帳戶中建立 AWS Lambda 函數和層，以便在帳戶請求、AFT 帳戶佈建和帳戶自訂程序期間執行步驟。
- AWS Systems Manager Parameter Store — AFT 在 AFT 管理帳戶中設定 AWS Systems Manager Parameter Store，以存放 AFT 管道程序所需的組態參數。
- Amazon CloudWatch — AFT 在 AFT 管理帳戶中建立 Amazon 日 CloudWatch 誌群組，以存放 AFT 管道使用的 AWS 服務所產生的日誌。 CloudWatch 記錄檔的保留期間設定為`Never Expire`。

- Amazon VPC — AFT 建立 Amazon Virtual Private Cloud (VPC)，將 AFT 管理帳戶中的服務和資源隔離到單獨的網路環境中，以增強安全性。
- AWS KMS — AFT 在 AFT 管理帳戶和 AWS Control Tower 日誌存檔帳戶中使用 AWS Key Management Service (KMS) (KMS)。AFT 會建立金鑰來加密地形狀態、DynamoDB 資料表中儲存的資料，以及 SNS 主題。AFT 部署 AWS 資源和服務時，會產生這些日誌和成品。AFT 建立的 KMS 金鑰預設會啟用每年輪替。
- AWS Identity and Access Management (IAM) — AFT 遵循建議的最低權限模型。它會在 AFT 管理帳戶、AWS Control Tower 帳戶和 AFT 佈建帳戶中建立 AWS Identity and Access Management (IAM) 角色和政策，視需要在 AFT 管道工作流程期間執行所需的動作。
- AWS Step Functions — AFT 會在 AFT 管理帳戶中建立 AWS Step Functions 狀態機器。這些狀態機器可協調並自動化 AFT 帳戶佈建架構和自訂的程序和步驟。
- Amazon EventBridge — AFT 在 AFT 和 AWS Control Tower 管理帳戶中建立 Amazon EventBridge 事件匯流排，以便在後端管理帳戶的 DynamoDB 表中長期擷取和存放 AWS Control Tower 生命週期事件。AFT 會在 AFT 管理和 AWS 控制塔管理帳戶中建立 AWS CloudWatch 事件規則，這會觸發執行 AFT 管道工作流程期間所需的多個步驟
- AWS CloudTrail (選用) — 啟用此功能時，AFT 會在 AWS 控制塔管理帳戶中建立 AWS CloudTrail 組織追蹤，以記錄 Amazon S3 儲存貯體和 AWS Lambda 函數的資料事件。AFT 會將這些日誌傳送到 AWS Control Tower 日誌存檔帳戶中的中央 S3 儲存貯體。
- AWS Support (選用) — 啟用此功能時，AFT 會為 AFT 佈建的帳戶開啟 AWS 企業 Support 計劃。根據預設，AWS 帳戶是在啟用 AWS 基本 Support 計劃的情況下建立的。

AFT 帳戶佈建管道

管道的帳戶佈建階段完成後，AFT 架構會繼續進行。它會自動執行一系列步驟，以確保新佈建的帳戶在帳戶自訂階段開始之前具有適當的詳細資料。

以下是 AFT 管線執行的後續步驟。

1. 驗證帳戶請求輸入。
2. 擷取已佈建之帳戶的相關資訊，例如帳號 ID。
3. 將帳戶中繼資料儲存在 AFT 管理帳戶的 DynamoDB 表格中。
4. 在新佈建的帳戶中建立 AWSAFTExecutionIAM 角色。AFT 會假設此角色來執行帳戶自訂階段，因為此角色會授與帳戶工廠組合的存取權。
5. 套用您提供的帳戶標籤作為帳戶請求輸入參數的一部分。

6. 套用您在 AFT 部署時選擇的 AFT 功能選項。
7. 套用您提供的 AFT 帳戶佈建自訂。下一節將詳細說明如何使用`git`儲存庫中的 AWS Step Functions 狀態機設定這些自訂。此階段有時稱為帳戶佈建架構階段。這是核心佈建程序的一部分，但是您先前已設定一個架構，該架構會在帳戶佈建工作流程中提供自訂整合，然後再將額外的自訂項目新增至下一階段的帳戶。
8. 對於佈建的每個帳戶，它會 AWS CodePipeline 在 AFT 管理帳戶中建立一個帳戶，該帳戶將執行以執行（下一個全域）帳戶自訂階段。
9. 針對每個佈建 (以及目標) 的帳戶叫用帳戶自訂管道。
10. 傳送成功或失敗通知至 SNS 主題，您可以從中擷取訊息。

使用狀態機器設定帳戶佈建架構自訂

如果您在佈建帳戶之前設定了自訂的非 TerraForm 整合，這些自訂會包含在 AFT 帳戶佈建工作流程中。例如，您可能需要特定的自訂，以確保 AFT 建立的所有帳戶都符合組織的標準和策略 (例如安全性標準)，而且這些標準可能會在其他自訂之前新增至帳戶。在全域帳戶自訂階段下一步開始之前，會在每個佈建的帳戶上實作這些帳戶佈建架構自訂。

> **Note**
>
> 本節中描述的 AFT 功能適用於了解 AWS Step Functions 的進階使用者。或者，我們建議您在帳戶自訂階段使用全域助手。

AFT 帳戶佈建架構會呼叫您定義的 AWS Step Functions 狀態機器來實作您的自訂。請參閱 AWS Step Functions 文件，進一步了解可能的狀態機器整合。

以下是一些常見的集成。

- 使用您選擇的語言提供 AWS Lambda 函數
- AWS ECS 或 AWS Fargate 任務，使用碼頭容器
- 使用在 AWS 或現場部署託管的自訂工作者的 AWS Step Functions 活動
- Amazon SNS 或 SQS 整合

如果未定義任何 AWS Step Functions 狀態機器，則階段會以無操作狀態通過。若要建立 AFT 帳戶佈建自訂狀態機器，請遵循中建立您的 AFT 帳戶佈建自訂狀態機器的指示。在新增自訂之前，請確定您已具備必要條件。

這些類型的整合不屬於 AWS Control Tower，且無法在 AFT 帳戶自訂的全球 API 前階段新增。AFT 管線可讓您將這些自訂設定為佈建程序的一部分，並在佈建工作流程中執行這些自訂。您必須在開始 AFT 帳戶佈建階段之前提前建立狀態機器來實作這些自訂，如下列各節所述。

建立狀態機的先決條件

- 一個完全部署的船尾。部署適用於地形 (AFT) 的 AWS Control Tower Account Factory如需 AFT 部署的詳細資訊，請參閱。
- 在您的環境中設定 AFT 帳戶佈建自訂的`git`存放庫。如需更多資訊，請參閱部署後步驟。

建立您的 AFT 帳戶佈建自訂狀態機器

步驟 1：修改狀態機定義

修改範例`customizations.asl.json`狀態機器定義。此範例可在您設定用來儲存 AFT 帳戶佈建自訂的儲存`git`庫中，在部署後的步驟中取得。請參閱 AWS Step Functions 開發人員指南，進一步了解狀態機器定義。

步驟 2：包含對應的地形組態

將具有`.tf`副檔名的 Terraform 檔案包含在同一個`git`儲存庫中，以及自訂整合的狀態機器定義。例如，如果您選擇在狀態機器工作定義中呼叫 Lambda 函數，則會將該`lambda.tf`檔案包含在相同的目錄中。確保為自訂組態包含必要的 IAM 角色和許可。

當您提供適當的輸入時，AFT 管道會自動叫用您的狀態機器，並將您的自訂部署為 AFT 帳戶佈建架構階段的一部分。

若要重新啟動 AFT 帳戶佈建架構和自訂

AFT 會針對每個透過 AFT 管道供應的帳戶執行帳戶佈建架構和自訂步驟。若要重新啟動帳戶佈建自訂，您可以使用下列兩種方法之一：

1. 對帳戶請求存儲庫中的現有帳戶進行任何更改。
2. 在 AFT 提供新帳戶。

帳戶自訂

AFT 可以在佈建的帳戶中部署標準或自訂組態。在 AFT 管理帳戶中，AFT 為每個帳戶提供一個管道。透過此管道，您可以在所有帳戶、一組帳戶或個別帳戶中實作自訂。您可以執行 Python 指令碼、bash 指令碼和 Terraform 組態，也可以在帳戶自訂階段中與 AWS CLI 互動。

概要

在您選擇的儲存庫 (儲存全域自訂的git儲存庫) 中指定自訂之後，或是儲存帳戶自訂的儲存庫中，帳戶自訂階段就會由 AFT 管道自動完成。若要追溯自訂帳戶，請參閱重新叫用自訂。

全域自訂 (選用)

您可以選擇將某些自訂套用至 AFT 佈建的所有帳戶。例如，如果您需要建立特定的 IAM 角色，或在每個帳戶中部署自訂控制項，則 AFT 管道中的全域自訂階段可讓您自動執行此操作。

帳戶自訂 (選用)

若要自訂個別帳戶或一組帳戶 (與其他 AFT 佈建帳戶不同)，您可以利用 AFT 管道的帳戶自訂部分來實作帳戶特定組態。例如，只有特定帳戶可能需要存取網際網路閘道。

自訂先決條

開始自訂帳戶之前，請確定這些先決條件已經到位。

- 一個完全部署的船尾。若要取得有關如何部署的資訊，請參閱設定和啟動適用於地形的 AWS Control Tower Account Factory。
- 預先填入的git儲存庫，用於您環境中的全域自訂和帳戶自訂。如需詳細資訊，請參閱中部署後步驟的步驟 3：填入每個儲存庫。

套用全域自訂

若要套用全域自訂，您必須將特定資料夾結構推送至您選擇的存放庫。

- 如果您的自定義配置是 Python 程序或腳本的形式，請將這些配置放在存儲庫中的 api_helpers/python 文件夾下。
- 如果您的自定義配置是 Bash 腳本的形式，請將它們放在存儲庫中的 api_helpers 文件夾下。
- 如果您的自定義配置是 Terraform 的形式，請將這些配置放在存儲庫的 Terraform 文件夾下。
- 如需有關建立自訂組態的詳細資訊，請參閱全域自訂 README 檔案。

> **Note**
>
> 在 AFT 管線中的 AFT 帳戶佈建架構階段之後，會自動套用全域自訂。

套用帳戶自訂

您可以透過將特定資料夾結構推送到您選擇的儲存庫來套用帳戶自訂。帳戶自訂會自動套用至 AFT 管線中，並在全域自訂階段之後套用。您也可以在帳戶自訂存放庫中建立包含不同帳戶自訂的多個資料夾。針對您需要的每個帳戶自訂，請使用下列步驟。

若要套用帳戶自訂

1. 步驟 1：為帳戶自訂建立資料夾

   在您選擇的儲存庫中，將 AFT 提供的ACCOUNT_TEMPLATE資料夾複製到新資料夾。新資料夾的名稱應與您在account_customizations_name帳戶要求中提供的名稱相符。

2. 將設定新增至您的特定帳戶自訂資料夾

   您可以根據設定的格式，將設定新增至帳戶自訂資料夾。

   - 如果您的自定義配置是 Python 程序或腳本的形式，請將它們放在存儲庫中的 ***[######] / api_*** helpers/ python 文件夾下。
   - 如果您的自定義配置是 Bash 腳本的形式，請將它們放在存儲庫中的 ***[######] /api_*** 幫手文件夾下。
   - 如果您的自定義配置是以 Terraform 的形式，請將它們放置在存儲庫中的 ***[####] / terraform ##***夾下。

   如需有關建立自訂組態的詳細資訊，請參閱帳戶自訂 README 檔案。

3. 請**account_customizations_name**參閱帳戶請求文件中的特定參數

   AFT 帳戶請求檔案包含輸入參數account_customizations_name。輸入您的帳戶自訂名稱作為此參數的值。

> **Note**
>
> 您可以針對環境中的帳戶提交多個帳戶請求。當您要套用不同或類似的帳戶自訂項目時，請使用帳戶請求中的account_customizations_name輸入參數指定帳戶自訂。如需詳細資訊，請參閱提交多個帳戶請求。

重新叫用自訂

AFT 提供了一種在 AFT 管線中重新叫用自訂的方法。當您已新增新的自訂步驟，或對現有自訂進行變更時，此方法非常有用。當您重新呼叫時，AFT 會啟動自訂管線，以對 AFT 佈建的帳戶進行變更。event-source-based 重新叫用可讓您將自訂套用至個別帳戶、所有帳戶、根據其 OU 的帳戶，或套用至根據標籤選取的帳戶。

請遵循以下三個步驟，重新叫用 AFT 佈建帳戶的自訂項目。

步驟 1：將變更推送至全域或帳戶自訂**git**儲存庫

您可以視需要更新全域和帳戶自訂項目，並將變更推送回儲git存庫。在這一點上，沒有任何反應，自訂管道必須由事件來源叫用，如接下來的兩個步驟所述。

步驟 2：啟動 AWS 步驟函數執行以重新叫用自訂

AFT 提供在 AFT 管理帳戶aft-invoke-customizations中呼叫的 AWS 步驟函數。該函數的目的是重新叫用 AFT 佈建帳戶的自訂管道。

以下是您可以建立的事件結構描述 (JSON 格式) 範例，以將輸入傳遞至 aft-invoke-customizations AWS 步驟函數。

```
{
  "include": [
    {
      "type": "all"
    },
    {
      "type": "ous",
      "target_value": [ "ou1","ou2"]
    },
    {
      "type": "tags",
      "target_value": [ {"key1": "value1"}, {"key2": "value2"}]
    },
    {
      "type": "accounts",
      "target_value": [ "acc1_ID","acc2_ID"]
    }
  ],
```

```
  "exclude": [
    {
      "type": "ous",
      "target_value": [ "ou1","ou2"]
    },
    {
      "type": "tags",
      "target_value": [ {"key1": "value1"}, {"key2": "value2"}]
    },
    {
      "type": "accounts",
      "target_value": [ "acc1_ID","acc2_ID"]
    }
  ]
}
```

範例事件結構描述顯示您可以選擇要在重新呼叫程序中包含或排除的帳戶。您可以依組織單位 (OU)、帳號標籤和帳號 ID 進行篩選。如果您未套用任何篩選器並包含陳述式`"type":"all"`，則會重新叫用所有 AFT 佈建帳戶的自訂。

> **Note**
>
> 如果您的 AWS Control Tower 版本為 1.6.5 或更新版本，您可以使用語法鎖定巢狀 OU0U Name (ou-id-1234)。如需詳細資訊，請參閱下列主題（詳見）GitHub。

填寫事件參數之後，「Step Functions 數」會執行並叫用對應的自訂項目。AFT 一次最多可以叫用 5 個自訂。Step Functions 會等待並迴圈，直到符合事件條件的所有帳戶都完成為止。

步驟 3：監控 AWS 步驟函數輸出並觀察 AWS CodePipeline 執行中

- 產生的「步驟函數」輸出包含符合「步驟函數」輸入事件來源的帳戶 ID。
- 導覽至開發人員工具 CodePipeline 下的 AWS，並檢視帳戶 ID 的對應自訂管道。

使用 AFT 帳戶自訂要求追蹤疑難排解

以包含目標帳戶和自訂要求 ID 的 AWS Lambda 發出記錄為基礎的帳戶自訂工作流程。AFT 可讓您透過 Amazon CloudWatch Logs 追蹤並疑難排解自訂請求，方法是提供 CloudWatch 日誌見解查詢，您可以使用這些查詢來篩選目標帳戶或自訂請求 ID 與自訂請求相關的 CloudWatch 日誌。如需詳細資訊，請參閱 Amazon CloudWatch 日誌使用者指南中的使用 Amazon CloudWatch 日誌分析日誌資料。

若要使用 AFT 的 CloudWatch 日誌深入解析

1. 請在以下位置開啟 CloudWatch 主控台。 https://console.aws.amazon.com/cloudwatch/
2. 在瀏覽窗格中，選擇 [記錄檔]，然後選擇 [記錄深入解析]。
3. 選擇「查詢」。
4. 在 [範例查詢] 下，選擇 [Terraform 的 Account Factory]，然後選取下列其中一個查詢：
   - 依帳戶 ID 分類的自訂記錄

     > **Note**
     >
     > 確保將 *##### ID########## ID*。

     ```
     fields @timestamp, log_message.account_id as target_account_id,
      log_message.customization_request_id as customization_request_id,
      log_message.detail as detail, @logStream
     | sort @timestamp desc
     | filter log_message.account_id == "YOUR-ACCOUNT-ID" and @message like /
     customization_request_id/
     ```

   - 依自訂要求識別碼的自訂記錄

     > **Note**
     >
     > 確保將 *######## ID########### ID*。您可以在 AFT 帳戶佈建架構 AWS Step Functions 狀態機器的輸出中找到您的自訂要求 ID。如需 AFT 帳戶佈建架構的詳細資訊，請參閱 AFT 帳戶佈建管線

     ```
     fields @timestamp, log_message.account_id as target_account_id,
      log_message.customization_request_id as customization_request_id,
      log_message.detail as detail, @logStream
     | sort @timestamp desc
     | filter log_message.customization_request_id == "YOUR-CUSTOMIZATION-REQUEST-ID"
     ```

5. 選取查詢之後，請務必選取時間間隔，然後選擇 [執行查詢]。

AFT 中源代碼版本控制的替代方案

AFT 原生地用 AWS CodeCommit 於源代碼版本控制系統（VCS），但它允許其他滿足您CodeConnections的業務需求或現有架構。您可以指定協力廠商 VCS 做為 AFT 部署先決條件的一部分。

AFT 支持以下源代碼控制替代方案：

- GitHub
- GitHub 企業伺服器
- BitBucket

如果您選擇 AWS CodeCommit 作為 VCS，則不需要執行其他步驟。根據預設，AFT 會使用預設名稱在您的環境中建立必要的`git`儲存庫。但是，您可以視需要覆寫的預設存放庫名稱，以符合您的組織標準。 CodeCommit

使用 AFT 設置替代源代碼版本控制系統（自定義 VCS）

若要為 AFT 部署設定替代原始程式碼版本控制系統，請依照下列步驟執行。

步驟 1：在支援的第三方版本控制系統 (VCS) 中建立**`git`**儲存庫。

如果您未使用 AWS CodeCommit，則必須在 AFT 支援的第三方 VCS 提供者環境中為下列項目建立`git`儲存庫。

- AFT 帳戶請求。示例代碼可用。如需 AFT 帳戶要求的詳細資訊，請參閱在 AFT 提供新帳戶。
- AFT 帳戶佈建自訂。示例代碼可用。如需 AFT 帳戶佈建自訂的詳細資訊，請參閱建立您的 AFT 帳戶佈建自訂狀態機器。
- AFT 全球定制。示例代碼可用。如需 AFT 全域自訂的詳細資訊，請參閱帳戶自訂。
- AFT 帳戶自訂功能。示例代碼可用。如需 AFT 帳戶自訂的詳細資訊，請參閱帳戶自訂。

步驟 2：指定 AFT 部署所需的 VCS 組態參數

將 VCS 提供者設定為 AFT 部署的一部分，需要下列輸入參數。

- vcs_provider：如果您未使用 AWS CodeCommit，請根據您的使用案例將 VCS 提供者指定為`"bitbucket""github""githubenterprise"`、或。
- 網址：僅適用於 GitHub 企業客戶，請指定網址。 GitHub

- 帳戶請求名稱：根據預設，此值會針對使用者設定為。`aft-account-request` AWS CodeCommit 如果您在 CodeCommit AFT 支援的第三方 VCS 提供者環境中使用新名稱建立存放庫，請使用實際存放庫名稱更新此輸入值。對於 BitBucket Github 和 GitHub 企業，存儲庫名稱必須具有格式`[Org]/[Repo]`。
- 帳戶自訂名稱：依預設，此值會針對使用者設定為。`aft-account-customizations` AWS CodeCommit 如果您在 CodeCommit AFT 支援的第三方 VCS 提供者環境中使用新名稱建立存放庫，請使用您的存放庫名稱更新此輸入值。對於 BitBucket Github 和 GitHub 企業，存儲庫名稱必須具有格式`[Org]/[Repo]`。
- 帳戶佈建 _ 自訂 _ repo_name: 依預設，此值會針對使用者設定為。`aft-account-provisioning-customizations` AWS CodeCommit 如果您在 AWS CodeCommit 支援 AFT 的第三方 VCS 提供者環境中使用新名稱建立存放庫，請使用您的存放庫名稱更新此輸入值。對於 BitBucket Github 和 GitHub 企業，存儲庫名稱必須具有格式`[Org]/[Repo]`。
- 全域自訂名稱：依預設，此值會針對使用者設定為。`aft-global-customizations` AWS CodeCommit 如果您在 CodeCommit AFT 支援的第三方 VCS 提供者環境中使用新名稱建立存放庫，請使用您的存放庫名稱更新此輸入值。對於 BitBucket Github 和 GitHub 企業，存儲庫名稱必須具有格式`[Org]/[Repo]`。
- 分支：默認情況下是分支，但該值可以**`main`**被覆蓋。

依預設，來自每個`git`儲存庫`main`分支的 AFT 來源。您可以使用額外的輸入參數覆寫分支名稱值。如需有關輸入參數的詳細資訊，請參閱 AFT 地形模組中的讀我檔案。

步驟 3：完成第三方 VCS 提供商的 AWS CodeStar 連接

當您的部署執行時，AFT 會建立必要的 AWS CodeCommit 儲存庫，或為您選擇的第三方 VCS 提供者建立 AWS CodeStar 連線。如果是後者，您必須手動登錄 AFT 管理帳戶的控制台以完成掛起的 AWS CodeStar 連接。如需完成 AWS CodeStar 連線的進一步指示，請參閱AWS CodeStar 文件。

資料保護

AWS 共同責任模式適用於 AFT 中的資料保護。基於資料保護的目的，我們建議您採用下列最佳作法，以確保安全

- 遵循 AWS Control Tower 提供的資料保護準則。如需詳細資訊，請參閱 AWS Control Tower 的資料保護。
- 保留 AFT 部署時產生的地形狀態組態。如需詳細資訊，請參閱 部署適用於地形 (AFT) 的 AWS Control Tower Account Factory。
- 依照組織安全性原則的指示，定期輪換機密認證。秘密的例子是地形令牌，`git`令牌等。

靜態加密

AFT 會建立 Amazon S3 儲存貯體、Amazon SNS 主題、Amazon SQS 佇列，以及使用金鑰管理服務 AWS 金鑰進行靜態加密的 Amazon DynamoDB 資料庫。AFT 建立的 KMS 金鑰預設會啟用每年輪替。如果您選擇 Terraform 雲端或地形企業發行版，AFT 會包含一個 AWS Systems Manager SecureString 參數來儲存敏感的 Terraform 權杖值。

AFT 使用中所述組件服務的 AWS 服務，依預設，靜態加密。有關詳細信息，請參閱 AFT 每個組件 AWS 服務的 AWS 文檔，並了解每個服務遵循的數據保護實踐。

傳輸中加密

AFT 依賴於預設情況下組件服務，在傳輸過程中使用加密的 AWS 服務。有關詳細信息，請參閱 AFT 每個組件 AWS 服務的 AWS 文檔，並了解每個服務遵循的數據保護實踐。

對於地形雲端或地形企業發行版，AFT 會呼叫 HTTPS 端點 API 來存取您的 Terraform 組織。如果您選擇 AWS CodeStar 連線支援的第三方 VCS 提供者，AFT 會呼叫 HTTPS 端點 API 以存取您的 VCS 提供者組織。

從 AFT 移除帳戶

本主題說明如何從 AFT 移除帳戶，以便 AFT 管線停止部署和更新帳戶。

> **Important**
>
> 從 AFT 管線移除帳戶是不可逆轉的，可能會導致狀態喪失。

當您想要關閉已淘汰應用程式的帳戶、隔離遭入侵的帳戶，或是將帳戶從某個組織移至另一個組織時，可以從 AFT 移除帳戶。

> **Note**
>
> 從 AFT 移除帳戶與刪除 AWS Control Tower 帳戶或 AWS 帳戶不同。當您從 AFT 移除帳戶時，AWS Control Tower 仍會管理該帳戶。要刪除 AWS Control Tower 帳戶 AWS 帳戶，或請參閱以下內容：
>
> - 在 AWS Control Tower 使用者指南中取消管理帳戶。
> - 關閉使AWS Billing 用者指南中的帳號。

若要從 AFT 管線中移除帳戶

下列程序說明如何從 AFT 移除帳戶。

1. 從**git**儲存帳號要求的儲存庫移除帳號

   在git儲存帳戶要求的儲存庫中，刪除要從 AFT 移除之帳戶的帳戶要求。

   當您從帳戶要求儲存庫移除帳戶要求時，AFT 會刪除自訂管道和帳戶中繼資料。如需詳細資訊，請參閱上的 AFT 1.8.0 版本說明。 GitHub
2. 刪除地形工作區（僅適用於地形雲和地形企業客戶）

   刪除您要從 AFT 移除之帳戶的全域自訂和帳戶自訂工作區。
3. 從 Amazon S3 後端刪除地形狀態

   在 AFT 管理帳戶中，針對您要從 AFT 移除的帳戶刪除 Amazon S3 儲存貯體內的所有相關資料夾。

   > **Tip**
   >
   > 在下列範例中，請以 AFT 管理帳戶 ID 號碼取*012345678901*代。

   範例：地形 OSS

   當您選擇 Terraform OSS 時，您會在 aft-backend-*012345678901*-secondary-region Amazon S3 儲存貯體中找到每個帳戶的 aft-backend-*012345678901*-primary-region 3 個資料夾。這些資料夾與帳戶自訂狀態、自訂管道狀態和全域自訂狀態相關

   範例：地形雲或地形企業

   當您選擇 Terraform 雲端或 Terraform 企業版時，您會在aft-backend-*012345678901*-primary-region和 aft-backend-*012345678901*-secondary-region Amazon S3 儲存貯體中找到每個帳戶的資料夾。這些資料夾與自訂管線狀態相關。

操作指標

依預設，地形表單 (AFT) 的 Account Factory 會將匿名作業指標傳送至。 AWS我們使用這些數據來了解客戶如何使用 AFT，以便我們可以改善解決方案的質量和功能。您可以在 AFT 部署期間變更參數，選擇退出資料收集。啟用收集時，會將下列資料傳送至 AWS：

- 解決方案：AFT 特定識別碼
- 版本：AFT 的版本
- 通用唯一識別碼 (UUID)：為每個 AFT 部署隨機產生的唯一識別碼
- 時間戳記：資料收集時間戳記
- 資料：AFT 組態與客戶採取的行動

AWS 擁有收集的數據。數據收集受AWS 隱私政策的約束。

> **Note**
>
> 1.6.0 之前的 AFT 版本不會將使用量度報告給。 AWS

若要選擇退出報告指標：

- `aft_metrics_reporting`將 Terraform 輸入組態檔案`false`中的輸入值設定為，如下列範例所示，然後重新部署 AFT。如果您未明確設定此值，則`true`依預設會設定為。

如果您複製範例，請記得將實際 ID 和 Region 值替換為字串中指定的項目x。

```
module "control_tower_account_factory" {
source = "aws-ia/control_tower_account_factory/aws"

# Required Vars
ct_management_account_id    = "xxxxxxxxxxx"
log_archive_account_id      = "xxxxxxxxxxx"
audit_account_id            = "xxxxxxxxxxx"
aft_management_account_id   = "xxxxxxxxxxx"
ct_home_region              = "xx-xxxx-x"
tf_backend_secondary_region = "xx-xxxx-x"
```

```
    # Optional Vars
    aft_metrics_reporting = false    # to opt out, set this value to false
    }
```

地形 (AFT) Account Factory 疑難排解指南

本節可協助您疑難排解使用 Terraform Account Factory (AFT) 時可能遇到的常見問題。

主題

一般問題

- 超出 AWS 資源配額

  如果您的記錄群組指出您超過 AWS 資源配額，請連絡 Sup AWS port 部門。Account Factory 使 AWS 服務 用的資源配額包括 AWS CodeBuild AWS Organizations、和 AWS Systems Manager。如需詳細資訊，請參閱下列內容：

  - 什麼是 AWS CodeBuild？ 在《CodeBuild 使用者指南》中。
  - 什麼是 AWS Organizations？ 在《Organ izations 使用指南》中。
  - 什麼是 AWS Systems Manager？ 在「Sy stems Manager 使用指南」中。
- Account Factory 的過時版本

  如果您遇到問題並認為問題是錯誤，請確保您擁有最新版本的 Account Factory。如需詳細資訊，請參閱更新 Account Factory 版本。
- 對 Account Factory 原始程式碼進行了本機變更

  Account Factory 是一個開源項目。AWS Control Tower 支援 Account Factory 核心代碼。如果您對 Account Factory 核心程式碼進行本機變更，AWS Control Tower 僅會盡力支援您的 Account Factory 部署。
- Account Factory 角色權限不足

  Account Factory 建立 IAM 角色和政策，以管理付費帳戶部署和自訂項目。如果您變更這些角色或原則，Account Factory 管線可能無法執行某些動作。如需詳細資訊，請參閱必要角色。

- 未正確填入帳號儲存庫

  在佈建帳戶之前，請務必遵循部署後的步驟。

- 手動變更 OU 後未偵測漂移

  > **Note**
  >
  > AWS Control Tower 會自動偵測漂移。如需解決漂移的相關資訊，請參閱在 AWS Control Tower 中偵測和解決漂移。

  手動變更組織單位 (OU) 時，不會偵測到漂移。這是由於 Account Factory 的事件驅動的性質。提交帳戶請求時，Terraform 管理的資源是 Amazon DynamoDB 項目，而不是直接帳戶。項目變更後，請求會放入佇列中，AWS Control Tower 會透過 Service Catalog (管理帳戶詳細資訊的服務) 處理這些要求。如果您手動變更 OU，則不會偵測到漂移，因為帳戶要求未變更。

與帳戶佈置/註冊相關問題

- 帳戶請求（電子郵件地址/姓名）已存在

  此問題通常會導致 Service Catalog 產品在佈建期間或作為失敗`ConditionalCheckFailedException`。

  您可以執行下列其中一個動作，找到有關此問題的詳細資訊：

  - 檢閱您的地形表單或 CloudWatch 記錄檔群組。
  - 檢閱傳送至 Amazon SNS 主題`aft-failure-notifications`的失敗情形。

- 格式錯誤的帳戶請求

  請確定您的帳戶要求遵循預期的結構描述。有關示例，請參閱 terraform-aws-control（詳見）。GitHub

- 超出 Or AWS ganizations 資源配額

  請確定您的帳號要求未超過 AWS Organizations 資源配額。如需詳細資訊，請參閱 Organ AWS izations 的配額。

與自訂呼叫相關的問題

- 未登入 Account Factory 的目標帳戶

  確定自訂要求中包含的所有帳戶都已登入 Account Factory。如需詳細資訊，請參閱更新現有帳戶。
- 自訂請求目標存在於 DynamoDB 表格中**aft-request-metadata**，但不存在於帳戶請求儲存庫中的帳戶

  請執行下列其中一項動作，格式化您的自訂叫用要求，以排除違規帳戶：
  - 在 DynamoDB 表格中`aft-request-metadata`，刪除參照帳戶請求儲存庫中不再存在之帳戶的帳戶的項目。
  - 不使用「全部」作為目標。
  - 不鎖定帳戶所屬的 OU。
  - 不直接針對帳戶。
- 對於地形雲使用了不正確的令牌

  請確定您設定了正確的權杖。Terraform 雲僅支持基於團隊的令牌，而不支持基於組織的令牌。
- 無法在建立帳戶自訂管道之前建立帳戶；無法自訂帳戶

  變更帳戶要求儲存庫中的帳戶規格。當您進行變更 (例如變更帳戶的標籤值) 時，即使管線不存在，Account Factory 仍會遵循嘗試建立管線的路徑。

與帳戶自訂工作流程相關的問題

如果您遇到與帳戶自訂工作流程相關的問題，請確定您的 AFT 版本為 1.8.0 或更高版本，並從 DynamoDB 請求表中刪除帳戶相關中繼資料的所有執行個體。

如需 AFT 版本 1.8.0 的相關資訊，請參閱上的版本 1. 8.0。 GitHub

如需如何檢查及更新 AFT 版本的詳細資訊，請參閱下列內容：

- 檢查船尾版本
- 更新船尾版本

您也可以使用 Amazon CloudWatch Logs Insights 查詢來篩選包含目標帳戶和自訂請求 ID 的日誌，來追蹤和疑難排解自訂請求。如需詳細資訊，請參閱使用 AFT 帳戶自訂要求追蹤進行疑難排解。

偵測並解決 AWS Control Tower 中的漂移

識別和解決漂移是 AWS Control Tower 管理帳戶管理員的常規操作任務。解決漂移有助於確保您遵守治理要求。

當您建立 landing zone 域時，landing zone 域及所有組織單位 (OU)、帳戶和資源都符合您選擇的控制項強制執行的治理規則。當您和您的組織成員使用 landing zone 時，此規範狀態可能會發生變更。有些變更可能是意外，有些則是為了回應時間急迫性運作事件而刻意為之。

偏離偵測可協助您找出需要變更或組態更新的資源，以解決偏離。

偵測漂移

AWS Control Tower 會自動偵測漂移。若要偵測漂移，該`AWSControlTowerAdmin`角色需要持續存取您的管理帳戶，以便 AWS Control Tower 可以對其進行唯讀 API 呼叫 AWS Organizations。這些 API 呼叫會顯示為 AWS CloudTrail 事件。

漂移在亞馬遜簡單通知服務 (Amazon SNS) 通知中浮出水面，這些通知彙總在稽核帳戶中。每個成員帳戶中的通知會傳送警示至本機 Amazon SNS 主題和 Lambda 函數。

對於屬於 AWS Security Hub 服務管理標準：AWS Control Tower 一部分的控制項，漂移會顯示在 AWS Control Twer 主控台的帳戶和帳戶詳細資訊頁面上，以及 Amazon SNS 通知。

成員帳戶管理員 (根據最佳實務，他們應該) 可訂閱特定帳戶的 SNS 偏離通知。例如，`aws-controltower-AggregateSecurityNotifications`SNS 主題提供漂移通知。AWS Control 塔主控台會在發生漂移時向管理帳戶管理員指示。如需有關漂移偵測和通知的 SNS 主題的詳細資訊，請參閱漂移預防和通知。

漂移通知重複刪除

如果同一組資源多次發生相同類型的漂移，AWS Control Tower 只會針對初始漂移執行個體傳送 SNS 通知。如果 AWS Control Tower 偵測到此漂移執行個體已修復，則只有在這些相同資源重新發生漂移時，才會傳送另一個通知。

示例：帳戶漂移和 SCP 漂移按以下方式處理

- 如果您多次修改相同的受管理 SCP，您會在第一次修改時收到通知。
- 如果您修改託管 SCP，然後修復漂移，然後再次修改，您將收到兩個通知。

- 如果帳戶在相同來源和目的地 OU 之間移動多次，但未先修復漂移，則會傳送單一通知，即使該帳戶在這些 OU 之間移動一次以上。

帳戶漂移類型

- 帳戶在 OU 之間移動
- 已從組織移除的帳號

> **Note**
>
> 當您將帳戶從一個 OU 移至另一個 OU 時，不會移除先前 OU 中的控制項。如果您在目的地 OU 上啟用任何新的掛接式控制項，舊的 系統會從帳戶中移除以掛接為基礎的控制項，而新的控制項則會取代它。當帳戶變更 OU 時，必須手動移除使用 SCP 和 AWS Config 規則實作的控制項。

政策漂移的類型

- SCP 已更新
- 附加至 OU 的 SCP
- 從 OU 中分離的 SCP
- SCP 附加至帳戶

如需詳細資訊，請參閱治理漂移的類型。

解決漂移

雖然偵測是自動的，但解決偏離的步驟必須透過主控台完成。

- 許多類型的漂移可以通過著陸區設置頁面解決。您可以選擇「版本」部分中的「重置」按鈕來解決這些類型的漂移問題。
- 如果您的 OU 帳戶少於 300 個，您可以在 [組織] 頁面或 [OU 詳細資料] 頁面上選取 [重新註冊 OU]，解決 Account Factory 佈建帳戶中的漂移問題或 SCP 漂移問題。
- 您可以解決帳戶漂移問題，例如移動成員帳戶後更新個人帳戶。如需詳細資訊，請參閱 更新主控台中的帳戶。

⚠ 當您採取行動解決 landing zone 版本上的漂移問題時，有兩種行為可能。

- 如果您使用的是最新的登陸區域版本，當您選擇「重設」然後選擇「確認」時，漂移的 landing zone 域資源會重設為儲存的 AWS Control Tower 組態。landing zone 版本保持不變。
- 如果您不是使用最新版本，則必須選擇「更新」。landing zone 已升級至最新的 landing zone 版本。漂移已作為此過程的一部分解決。

關於漂移和 SCP 掃描的注意事項

AWS Control Tower 每天掃描您的受管 SCP，以確認對應的控制項已正確套用，以及它們沒有漂移。若要擷取 SCP 並對其執行檢查，AWS Control Tower 會使用管理帳戶中的角色代表您呼叫 AWS Organizations 。

如果 AWS Control Tower 掃描發現漂移，您會收到通知。AWS Control Tower 每個漂移問題只會傳送一個通知，因此，如果您的 landing zone 已處於漂移狀態，除非找到新的漂移項目，否則您將不會收到其他通知。

AWS Organizations 限制每個 API 可以調用的頻率。此限制以每秒交易數 (TPS) 表示，稱為 TPS 限制、節流率或 API 要求率。當 AWS Control Tower 透過呼叫稽核 SCP 時 AWS Organizations，AWS Control Tower 發出的 API 呼叫會計入您的 TPS 限制，因為 AWS Control Tower 使用管理帳戶進行呼叫。

在極少數情況下，當您重複呼叫相同的 API 時，無論是透過協力廠商解決方案還是您撰寫的自訂指令碼，都可以達到此限制。例如，如果您和 AWS Control Tower 在同一時間 (1 秒內) 呼叫相同的 AWS Organizations API，且達到 TPS 限制，則後續呼叫會被限制。也就是說，這些調用返回一個錯誤，例如`Rate exceeded`。

如果超過 API 請求率

- 如果 AWS Control Tower 達到限制且受到限制，我們會暫停稽核的執行，稍後再繼續執行。
- 如果您的工作負載達到限制並受到限制，則結果的範圍可能從輕微的延遲到工作負載中的嚴重錯誤，具體取決於工作負載的設定方式。這種邊緣情況是需要注意的。

每日 SCP 掃描包含

1. 擷取您最近作用中的 OU。

2. 針對每個已註冊的 OU，擷取由 AWS Control Tower 管理且連接至 OU 的所有 SCP。受管理的 SCP 具有以`aws-guardrails`開頭的識別碼。
3. 針對 OU 上啟用的每個預防性控制項，驗證控制項的原則陳述式是否存在於 OU 的受管理 SCP 中。

OU 可能有一或多個受管理的 SCP。

要立即解決的漂移類型

系統管理員可以解決大多數類型的偏離。必須立即解決幾種類型的漂移問題，包括刪除 AWS Control Tower landing zone 所需的組織單位。以下是您可能希望避免的一些主要漂移示例：

- 請勿刪除安全 OU：不應刪除 AWS Control Tower 設定 landing zone 期間原本命名為 Security 的組織單位。如果您將其刪除，您會看到錯誤訊息，指示您立即重設 landing zone 域。在重設完成之前，您將無法在 AWS Control Tower 中採取任何其他動作。
- 不要刪除必要的角色：當您登入主控台以取得 IAM 角色漂移時，AWS Control Tower 會檢查特定 AWS Identity and Access Management (IAM) 角色。如果這些角色遺失或無法存取，您會看到錯誤頁面，指示您重設 landing zone。這些角色是 `AWSControlTowerAdmin` `AWSControlTowerCloudTrailRoleAWSControlTowerStackSetRole`.

  如需這些角色的詳細資訊，請參閱使用 AWS Control Tower 主控台所需的許可。
- 不要刪除所有其他 OU：如果您在 AWS Control Tower 設定的登陸區域期間刪除原本名為 Sandbox 的組織單位，您的 landing zone 域將處於漂移狀態，但您仍然可以使用 AWS Control Tower。AWS Control Tower 至少需要一個額外的 OU 才能運作，但不一定是沙箱 OU。
- 不要移除共用帳戶：如果您從基礎 OU 移除共用帳戶 (例如從安全性 OU 移除記錄帳戶)，您的 landing zone 將處於漂移狀態。您必須先重設 landing zone，才能繼續使用 AWS Control Tower 主控台。

資源的可修復變更

以下是允許的 AWS Control Tower 資源變更清單，但這些資源會建立可解析的漂移。雖然可能需要重新整理，但可在 AWS Control Tower 主控台中檢視這些允許操作的結果。

如需如何解決產生的偏移問題的詳細資訊，請參閱管理 AWS Control Tower 以外的資源。

AWS Control Tower 主控台外允許的變更

- 變更已註冊 OU 的名稱。
- 變更安全性 OU 的名稱。
- 變更非基礎 OU 中成員帳戶的名稱。
- 變更安全 OU 中 AWS Control Tower 共用帳戶的名稱。
- 刪除非基礎 OU。
- 從非基礎 OU 刪除已註冊的帳戶。
- 在安全性 OU 中變更共用帳戶的電子郵件地址。
- 在註冊的 OU 中變更會員帳號的電子郵件地址。

> **Note**
>
> 在 OU 之間移動帳戶被認為是漂移，並且必須解決。

偏離和新帳戶佈建

如果您的 landing zone 域處於漂移狀態，AWS Control Tower 中的註冊帳戶功能將無法運作。在這種情況下，您必須透過 AWS Service Catalog 佈建新帳戶。如需說明，請參閱使用 AWS Service Catalog Account Factory 佈建帳戶 。

特別是，如果您透過 Service Catalog 對帳戶進行了某些變更，例如變更產品組合的名稱，則註冊帳戶功能將無法運作。

管控偏離的類型

當 OU、SCP 和成員帳戶變更或更新時，就會發生治理偏移，也稱為組織偏移。可在 AWS Control Tower 中偵測到的控管偏移類型如下：

- 移動成員帳戶後
- 移除成員帳戶後
- 未計劃的受管 SCP 更新
- 連接到成員帳戶的 SCP

- 連接到受管 OU 的 SCP
- 從受管 OU 分離的 SCP
- 已刪除的基礎 OU
- Security Hub 控制漂移
- 信任存取已停用

另一種漂移類型是 landing zone 漂移，可以通過管理帳戶找到。著陸區域漂移包含 IAM 角色漂移，或特別影響基礎 OU 和共用帳戶的任何類型的組織漂移。

landing zone 漂移的一個特殊情況是角色漂移，當所需的角色不可用時會被檢測到。如果發生這種類型的漂移，控制台會顯示警告頁面以及有關如何還原角色的一些說明。在角色漂移解決之前，您的 landing zone 將無法使用。有關漂移的更多信息，請參閱名為的部分中的不刪除必要角色要立即解決的漂移類型。

AWS Control Tower 不會尋找與管理帳戶搭配使用的其他服務相關的漂移 CloudTrail CloudWatch AWS CloudFormation AWS Config，包括 IAM 身分中心等。兒童帳戶不可用漂移偵測，因為這些帳戶受到預防性強制性控制的保護。

但是，它會報告與AWS Security Hub 服務管理標準：AWS Control Tower 一部分的控制有關的漂移。

移動成員帳戶後

這種類型的漂移發生在帳戶上，而不是 OU 上。當 AWS Control Tower 成員帳戶、稽核帳戶或日誌存檔帳戶從註冊的 AWS Control Tower OU 移至任何其他 OU 時，可能會發生這種類型的漂移。以下是偵測到此類漂移時 Amazon SNS 通知的範例。

```
{
  "Message" : "AWS Control Tower has detected that your member account 'account-
email@amazon.com (012345678909)' has been moved from organizational unit 'Sandbox
 (ou-0123-eEXAMPLE)' to 'Security (ou-3210-1EXAMPLE)'. For more information, including
 steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/
move-account'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "ACCOUNT_MOVED_BETWEEN_OUS",
  "RemediationStep" : "Re-register this organizational unit (OU), or if the OU has more
 than 300 accounts, you must update the provisioned product in Account Factory.",
  "AccountId" : "012345678909",
```

```
  "SourceId" : "012345678909",
  "DestinationId" : "ou-3210-1EXAMPLE"
}
```

解決方案

在具有多達 300 個帳戶的 OU 中，Account Factory 佈建的帳戶發生這種類型的漂移時，您可以透過以下方式解決此問題：

- 導覽至 AWS Control Tower 主控台中的組織頁面，選取帳戶，然後選擇右上角的 [更新帳戶] (個別帳戶最快的選項)。
- 導覽至 AWS Control Tower 主控台中的組織頁面，然後針對包含該帳戶的 OU 選擇重新註冊 (多個帳戶最快的選項)。如需詳細資訊，請參閱 向 AWS Control Tower 註冊現有的組織單位。
- 更新 Account Factory 中佈建的產品。如需詳細資訊，請參閱 使用 AWS Control Tower 或使用更新和移動帳戶工廠帳戶 AWS Service Catalog。

  > **Note**
  >
  > 如果您有數個要更新的個別帳戶，請參閱此方法以使用指令碼進行更新：使用自動化佈建和更新帳戶。

- 在擁有 300 個帳戶以上的 OU 中發生此類漂移時，漂移解析度可能取決於已移動的帳戶類型，如下段所述。如需詳細資訊，請參閱 更新您的登陸區域。
  - 如果移動了 Account Factory 佈建的帳戶 — 在帳戶少於 300 個的 OU 中，您可以透過更新 Account Factory 中佈建的產品、重新註冊 OU 或更新您的 landing zone 來解決帳戶偏移問題。

    在擁有 300 個帳戶以上的 OU 中，您必須透過 AWS Control Tower 主控台或佈建的產品對每個移動的帳戶進行更新來解決此問題，因為重新註冊 OU 不會執行更新。如需詳細資訊，請參閱 使用 AWS Control Tower 或使用更新和移動帳戶工廠帳戶 AWS Service Catalog。
  - 如果共用帳戶已移動 — 您可以透過更新您的 landing zone 來解決移動稽核或記錄封存帳戶的問題。如需詳細資訊，請參閱 更新您的登陸區域。

> **已停用的欄位名**
>
> 欄位名稱`MasterAccountID`已變更為符`ManagementAccountID`合 AWS 指導方針。舊名稱已棄用。從 2022 年開始，包含已取代欄位名稱的指令碼將不再起作用。

移除成員帳戶後

從註冊的 AWS Control Tower 組織單位中移除成員帳戶時，可能會發生這種類型的漂移。下列範例顯示偵測到此類漂移時的 Amazon SNS 通知。

```
{
  "Message" : "AWS Control Tower has detected that the member account 012345678909 has
 been removed from organization o-123EXAMPLE. For more information, including steps
 to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/remove-
account'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "ACCOUNT_REMOVED_FROM_ORGANIZATION",
  "RemediationStep" : "Add account to Organization and update Account Factory
 provisioned product",
  "AccountId" : "012345678909"
}
```

解析度

- 當成員帳戶中發生這種類型的漂移時，您可以在 AWS Control Tower 主控台或 Account Factory 中更新帳戶來解決此問題。例如，您可以從 Account Factory 更新精靈將帳戶新增至另一個已註冊的 OU。如需詳細資訊，請參閱 使用 AWS Control Tower 或使用更新和移動帳戶工廠帳戶 AWS Service Catalog。
- 如果共用帳戶已從基礎 OU 中移除，您必須透過重設 landing zone 來解決此問題。在解決此漂移之前，您將無法使用 AWS Control 塔主控台。
- 如需解決帳戶和 OU 偏離的詳細資訊，請參閱如果您管理 AWS Control Tower 以外的資源。

> **Note**
>
> 在 Service Catalog 中，不會更新代表該帳戶的 Account Factory 佈建產品以移除帳戶。相反地，佈建的產品會顯示為 TAINTED 和錯誤狀態。若要清除，請移至 Service Catalog，選擇佈建的產品，然後選擇 [終止]。

未計劃的受管 SCP 更新

在 AWS Organizations 主控台中更新控制項的 SCP 或以程式設計方式使用或其中一個 AWS 開發套件時，可能會發生這種類型的漂移。 AWS CLI 以下是偵測到此類漂移時 Amazon SNS 通知的範例。

```
{
  "Message" : "AWS Control Tower has detected that the managed service control policy
 'aws-guardrails-012345 (p-tEXAMPLE)', attached to the registered organizational unit
 'Security (ou-0123-1EXAMPLE)', has been modified. For more information, including
 steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/
update-scp'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "SCP_UPDATED",
  "RemediationStep" : "Update Control Tower Setup",
  "OrganizationalUnitId" : "ou-0123-1EXAMPLE",
  "PolicyId" : "p-tEXAMPLE"
}
```

解析度

當此類型的漂移發生在具有多達 300 個帳戶的 OU 中時，您可以透過下列方式解決此問題：

- 導覽至 AWS Control 塔主控台中的組織頁面，以重新註冊 OU (最快的選項)。如需詳細資訊，請參閱 向 AWS Control Tower 註冊現有的組織單位。
- 更新您的 landing zone（較慢的選項）。如需詳細資訊，請參閱 更新您的登陸區域。

在擁有 300 個帳戶以上的 OU 中發生此類漂移時，請透過更新您的 landing zone 來解決此問題。如需詳細資訊，請參閱 更新您的登陸區域。

連接到受管 OU 的 SCP

當控制項的 SCP 連接至任何其他 OU 時，就會發生這種類型的漂移。當您從 AWS Control 塔主控台外部處理 OU 時，這種情況尤其常見。以下是偵測到此類漂移時 Amazon SNS 通知的範例。

```
{
  "Message" : "AWS Control Tower has detected that the managed service control
 policy 'aws-guardrails-012345 (p-tEXAMPLE)' has been attached to the registered
```

```
 organizational unit 'Sandbox (ou-0123-1EXAMPLE)'. For more information, including
 steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/
scp-detached-ou'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "SCP_ATTACHED_TO_OU",
  "RemediationStep" : "Update Control Tower Setup",
  "OrganizationalUnitId" : "ou-0123-1EXAMPLE",
  "PolicyId" : "p-tEXAMPLE"
}
```

解析度

當此類型的漂移發生在具有多達 300 個帳戶的 OU 中時，您可以透過下列方式解決此問題：

- 導覽至 AWS Control 塔主控台中的組織頁面，以重新註冊 OU (最快的選項)。如需詳細資訊，請參閱 向 AWS Control Tower 註冊現有的組織單位。
- 更新您的 landing zone（較慢的選項）。如需詳細資訊，請參閱 更新您的登陸區域。

在擁有 300 個帳戶以上的 OU 中發生此類漂移時，請透過更新您的 landing zone 來解決此問題。如需詳細資訊，請參閱 更新您的登陸區域。

從受管 OU 分離的 SCP

當控制項的 SCP 已從 AWS Control Tower 管理的 OU 中分離時，可能會發生這種類型的漂移。當您在 AWS Control 塔主控台外部工作時，這種情況尤其常見。以下是偵測到此類漂移時 Amazon SNS 通知的範例。

```
{
  "Message" : "AWS Control Tower has detected that the managed service control
 policy 'aws-guardrails-012345 (p-tEXAMPLE)' has been detached from the registered
 organizational unit 'Sandbox (ou-0123-1EXAMPLE)'. For more information, including
 steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/
scp-detached'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "SCP_DETACHED_FROM_OU",
  "RemediationStep" : "Update Control Tower Setup",
  "OrganizationalUnitId" : "ou-0123-1EXAMPLE",
  "PolicyId" : "p-tEXAMPLE"
```

```
}
```

解析度

當此類型的漂移發生在具有多達 300 個帳戶的 OU 中時，您可以透過下列方式解決此問題：

- 導覽至 AWS Control Tower 主控台中的 OU 以重新註冊 OU (最快的選項)。如需詳細資訊，請參閱向 AWS Control Tower 註冊現有的組織單位。
- 更新您的 landing zone（較慢的選項）。如果漂移影響強制控制項，則更新程序會建立新的服務控制原則 (SCP)，並將其附加至 OU 以解決漂移問題。如需如何更新 landing zone 域的詳細資訊，請參閱更新您的登陸區域。

在擁有 300 個帳戶以上的 OU 中發生此類漂移時，請透過更新您的 landing zone 來解決此問題。如果漂移影響強制控制項，則更新程序會建立新的服務控制原則 (SCP)，並將其附加至 OU 以解決漂移問題。如需如何更新 landing zone 域的詳細資訊，請參閱更新您的登陸區域。

連接到成員帳戶的 SCP

當控制項的 SCP 附加至 Organizations 主控台中的帳戶時，可能會發生這種類型的漂移。您可以透過 AWS Control 塔主控台在 OU 上啟用護欄及其 SCP (因此套用至所有 OU 的註冊帳戶)。以下是偵測到此類漂移時 Amazon SNS 通知的範例。

```
{
  "Message" : "AWS Control Tower has detected that the managed service control policy
 'aws-guardrails-012345 (p-tEXAMPLE)' has been attached to the member account 'account-
email@amazon.com (012345678909)'. For more information, including steps to resolve this
 issue, see 'https://docs.aws.amazon.com/console/controltower/scp-detached-account'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "SCP_ATTACHED_TO_ACCOUNT",
  "RemediationStep" : "Re-register this organizational unit (OU)",
  "AccountId" : "012345678909",
  "PolicyId" : "p-tEXAMPLE"
}
```

解析度

這種類型的漂移發生在帳戶上，而不是 OU 上。

當基礎 OU (例如安全性 OU) 中的帳戶發生這種類型的偏移時，解決方案是更新您的 landing zone。如需詳細資訊，請參閱 更新您的登陸區域。

當此類型的漂移發生在具有多達 300 個帳戶的非基礎 OU 中時，您可以透過以下方式解決此問題：

- 將 AWS Control Tower SCP 與帳戶原廠帳戶分離。
- 導覽至 AWS Control Tower 主控台中的 OU 以重新註冊 OU (最快的選項)。如需詳細資訊，請參閱向 AWS Control Tower 註冊現有的組織單位。

當此類型的偏移發生在擁有 300 個以上帳戶的 OU 中時，您可以嘗試透過更新帳戶的帳戶原廠設定來解決此問題。可能無法成功解決它。如需詳細資訊，請參閱 更新您的登陸區域。

已刪除的基礎 OU

此類型的漂移僅適用於 AWS Control Tower 基礎 OU，例如安全 OU。如果在 AWS Control 塔主控台外部刪除基礎 OU，就可能會發生這種情況。如果不建立此類型漂移，就無法移動基礎 OU，因為移動 OU 與刪除 OU，然後將其新增到其他位置相同。當您透過更新 landing zone 來解決偏移問題時，AWS Control Tower 會取代原始位置的基礎 OU。下列範例顯示偵測到此類漂移時，您可能會收到的 Amazon SNS 通知。

```
{
  "Message" : "AWS Control Tower has detected that the registered organizational unit
 'Security (ou-0123-1EXAMPLE)' has been deleted. For more information, including steps
 to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/delete-
ou'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "ORGANIZATIONAL_UNIT_DELETED",
  "RemediationStep" : "Delete organizational unit in Control Tower",
  "OrganizationalUnitId" : "ou-0123-1EXAMPLE"
}
```

解析度

由於此漂移僅適用於基礎 OU，因此解析度是更新 landing zone 域。刪除其他類型的 OU 時，AWS Control Tower 會自動更新。

如需解決帳戶和 OU 偏離的詳細資訊，請參閱如果您管理 AWS Control Tower 以外的資源。

Security Hub 控制漂移

當屬於AWS Security Hub 服務管理標準的一部分的控制項時，就會發生這種類型的漂移：AWS Control Tower 報告漂移狀態。 AWS Security Hub 服務本身不會報告這些控制項的漂移狀態。相反地，服務會將其發現傳送到 AWS Control Tower。

如果 AWS Control Tower 在 24 小時內未收到來自 Security Hub 的狀態更新，也可以偵測到安全中心控制漂移。如果未如預期般收到這些發現，AWS Control Tower 會驗證控制項是否處於偏移狀態。下列範例顯示偵測到此類漂移時，您可能會收到的 Amazon SNS 通知。

```
{
"Message" : "AWS Control Tower has detected that an AWS Security Hub control
 was removed in your account example-account@amazon.com <mailto:example-
account@amazon.com>. The artifact deployed on the target OU and accounts does not match
 the expected template and configuration for the control. This mismatch indicates that
 configuration changes were made outside of AWS Control Tower. For more information,
 view Security Hub standard",
"MasterAccountId" : "123456789XXX",
"ManagementAccountId" : "123456789XXX",
"OrganizationId" : "o-123EXAMPLE",
"DriftType" : "SECURITY_HUB_CONTROL_DISABLED",
"RemediationStep" : "To remediate the issue, Re-register the OU, or remove the control
 and enable it again. If the problem persists, contact AWS support.",
"AccountId" : "7876543219XXX",
"ControlId" : "PYBETSAGNUZB",
"ControlName" : "EBS snapshots should not be publicly restorable",
"ApiControlIdentifier" : "arn:aws:controltower:us-east-1::control/PYBETSAGNUZB",
"Region" : "us-east-1"
}
```

解析度

對於具有少於 300 個帳戶的 OU，解決方案是重新註冊 OU，如此可將控制項重設為原始狀態。對於任何 OU，您都可以透過主控台或 AWS Control 塔 API 移除和重新啟用控制，這也會重設控制。

如需解決帳戶和 OU 偏離的詳細資訊，請參閱如果您管理 AWS Control Tower 以外的資源。

信任存取已停用

此類型的漂移適用於 AWS Control Tower 登陸區域。當您在設定 AWS Control Tower landing zone AWS Organizations 後停用對 AWS Control Tower 的受信任存取權限時，就會發生這種情況。

停用受信任存取時，AWS Control Tower 不再接收來自的變更事件 AWS Organizations。AWS Control Tower 依賴這些變更事件與之保持同步 AWS Organizations。因此，AWS Control Tower 可能會遺漏帳戶和 OU 中的組織變更。這就是為什麼每次更新 landing zone 域時，重新註冊每個 OU 很重要的原因。

範例：Amazon SNS 通知

以下是發生此類漂移時收到的 Amazon SNS 通知範例。

```
{
  "Message" : "AWS Control Tower has detected that trusted access has been disabled in
 AWS Organizations. For more information, including steps to resolve this issue, see
 https://docs.aws.amazon.com/controltower/latest/userguide/drift.html#drift-trusted-
access-disabled",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "TRUSTED_ACCESS_DISABLED",
  "RemediationStep" : "Reset Control Tower landing zone."
}
```

解析度

AWS Control Tower 會在 AWS Control Tower 主控台中發生此類漂移時通知您。解決方案是重設您的 AWS Control Tower landing zone。有關詳情，請參閱解決漂移。

如果您管理 AWS Control Tower 以外的資源

AWS Control Tower 會代您設定帳戶、組織單位和其他資源，但您是這些資源的擁有者。您可以在 AWS Control Tower 內或外部變更這些資源。在 AWS Control Tower 外部變更資源最常見的地方是主控 AWS Organizations 台。本主題說明在 AWS Control Tower 外部進行變更時，如何協調 AWS Control Tower 資源的變更。

在 AWS Control Tower 主控台之外重新命名、刪除和移動資源會導致主控台不同步。許多變更都可以自動協調。某些變更需要重設您的 landing zone，才能更新 AWS Control Tall 主控台中顯示的資訊。

一般而言，您在 AWS Control Twer 主控台外部對 AWS Control Tower 資源進行的變更會在您的 landing zone 域建立可解析的漂移狀態。如需這些變更的詳細資訊，請參閱資源的可修復變更。

需要重設 landing zone 域的工作

- 刪除安全 OU（一種特殊情況，不要輕心完成。）

- 從安全性 OU 移除共用帳戶 (不建議使用)。
- 更新、附加或卸離與安全性 OU 相關聯的 SCP。

AWS Control Tower 自動更新的變更

- 變更已註冊帳戶的電子郵件地址
- 重新命名已註冊的帳戶
- 建立新的頂層組織單位 (OU)
- 重新命名註冊的 OU
- 刪除已登錄的 OU (安全性 OU 除外，需要更新)。
- 刪除已註冊的帳戶 (安全性 OU 中的共用帳戶除外)。

> **Note**
>
> AWS Service Catalog 與 AWS Control Tower 以不同的方式處理變更。 AWS Service Catalog 在調和您的變更時，可能會造成治理狀態的變更。如需更新已佈建產品的詳細資訊，請參閱 AWS Service Catalog 說明文件中的更新已佈建產品。

參考 AWS Control Tower 外的資源

當您在 AWS Control Tower 外建立新的 OU 和帳戶時，即使可能會顯示這些帳戶，它們也不會受 AWS Control Tower 管理。

建立 OU

在 AWS Control Tower 外建立的組織單位 (OU) 稱為「未註冊」。它們會顯示在組織頁面中，但不受 AWS Control Tower 控制管理。

創建一個帳戶

在 AWS Control Tower 外建立的帳戶稱為「取消註冊」。屬於 AWS Control Tower 註冊之 OU 的已註冊和取消註冊帳戶會顯示在組織頁面中。不屬於已註冊 OU 的帳戶可以使用 AWS Organizations 主控台來邀請。此加入邀請不會在 AWS Control Tower 中註冊帳戶，也不會將 AWS Control Tower 管理延伸到該帳戶。若要透過註冊帳戶來擴展管理，請前往組織頁面或 AWS Control Tower 中的帳戶詳細資料頁面，然後選擇註冊帳戶。

從外部變更 AWS Control Tower 資源名稱

您可以在 AWS Control Tower 主控台外部變更組織單位 (OU) 和帳戶的名稱，主控台會自動更新以反映這些變更。

重新命名 OU

在中 AWS Organizations，您可以使用 AWS Organizations API 或主控台來變更 OU 的名稱。當您在 AWS Control Tower 外部變更 OU 名稱時，AWS Control 塔主控台會自動反映名稱變更。不過，如果您使用佈建帳戶 AWS Service Catalog，也必須重設 landing zone，以確保 AWS Control Tower 與之保持一致 AWS Organizations。重設工作流程可確保基礎和其他 OU 的服務之間的一致性。您可以從「著陸區設定」 頁面解決此類漂移問題。請參閱中的「解決漂移」一節偵測並解決 AWS Control Tower 中的漂移。

AWS Control Tower 會在 AWS Control Tower 儀表板的組織頁面上顯示 OU 的名稱。您可以查看 landing zone 重設作業何時成功。

重新命名已註冊的帳戶

每個 AWS 帳戶都有一個顯示名稱，該名稱可由 AWS Billing and Cost Management 控制台中帳戶的 root 用戶進行更改。當您重新命名已註冊 AWS Control Tower 的帳戶時，名稱變更會自動反映在 AWS Control Tower 中。如需有關變更帳戶名稱的詳細資訊，請參閱AWS 帳AWS 單使用手冊中的管理帳戶。

刪除安全性 OU

這種類型的偏離是一種特殊情況。如果您刪除安全性 OU，您會看到錯誤訊息頁面，提示您重設 landing zone。您必須先重設 landing zone，才能在 AWS Control Tower 中採取任何其他動作。

- 您將無法在 AWS Control Tower 主控台中執行任何動作，而且在重設完成 AWS Service Catalog 之前，您將無法在中建立任何新帳戶。
- 您將無法檢視「著陸區設定」 頁面，以便在該處看到「重設」按鈕。

在此情況下，landing zone 重設程序會建立新的安全性 OU，並將這兩個共用帳戶移至新的安全性 OU。AWS Control Tower 會將日誌存檔和稽核帳戶標記為已漂移。相同的過程解決了這些帳戶中的漂移。

如果您決定必須刪除安全性 OU，以下是您必須知道的事項：

刪除安全性 OU 之前，您必須確定它不包含任何帳戶。具體而言，您必須從 OU 移除記錄封存和稽核帳戶。我們建議您將這些帳戶移至另一個 OU。

> **Note**
>
> 刪除您的安全性 OU 的動作不會在沒有適當考量的情況下執行。如果暫時暫停記錄，並且可能無法強制執行某些控制項，此動作可能會造成符合性問題。

如需有關偏離的一般資訊，請參閱 偵測並解決 AWS Control Tower 中的漂移 中的「解決偏離」。

從安全性 OU 移除帳戶

我們不建議您從組織中移除任何共用帳戶，或將其移出 [安全性 OU]。如果您意外移除了共用帳戶，您可以依照本節中的修復步驟來還原帳戶。

- 從 AWS Control Tower 主控台內部：若要啟動修復程序，請按照半手動修復步驟操作。確保您用來存取 AWS Control 塔主控台的使用者或角色具有執行許可`organizations:InviteAccountToOrganization`。如果您沒有這些許可，請按照手動修復步驟操作，這些步驟同時使用 AWS Control Tower 主控台和 AWS Organizations 主控台。
- 從 AWS Organizations 主控台開始：此修復程序需要稍長、完全手動的程序。按照手動修復步驟操作時，您將在主控 AWS Organizations 台和 AWS Control Tower 台之間切換。在中工作時 AWS Organizations，您需要具有`AWSOrganizationsFullAccess`受管理策略或同等策略的使用者或角色。在 AWS Control Tower 主控台中工作時，您需要具有`AWSControlTowerServiceRolePolicy`受管政策或同等政策的使用者或角色，以及執行所有 AWS Control Tall 動作 (控制塔：*) 的許可。
- 如果補救步驟無法還原帳戶，請聯絡 AWS Support。

通過以下方式刪除共享帳戶的結果 AWS Organizations：

- 該帳戶不再受到具有服務控制政策 (SCP) 的 AWS Control Tower 強制性控制措施的保護。結果：AWS Control Tower 在帳戶中建立的資源可能會遭到修改或刪除。
- 該帳戶不再位於 AWS Organizations 管理帳戶下。結果： AWS Organizations 管理帳戶的管理員不再能看到帳戶的支出。
- 該帳戶不再保證受到監控 AWS Config。結果： AWS Organizations 管理帳號的管理員可能無法偵測資源變更。
- 該帳戶不再在組織中。結果：AWS Control Tower 更新和重設將失敗。

使用 AWS Control 塔主控台還原共用帳戶 (半手動程序)

1. 登入 AWS Control Tower 主控台主控台，網址為 https://console.aws.amazon.com/controltower。您必須以 IAM 使用者、IAM 身分中心的使用者身分或具有權限的角色登入才能執行`organizations:InviteAccountToOrganization`。如果您沒有此類權限，請使用本主題稍後所述的手動修復程序。
2. 在 [偵測到的登陸區域漂移] 頁面上，選擇 [重新邀請]，藉由重新邀請共用帳戶加入組織，以修復共用帳戶的移除問題。系統會將自動產生的電子郵件傳送至帳戶的電子郵件地址。
3. 接受邀請，將共用帳戶帶回組織。執行以下任意一項：
   - 登入已移除的共用帳戶，然後前往 https://console.aws.amazon.com/organizations/home#/invites
   - 如果您可以存取重新邀請帳戶時傳送的電子郵件訊息，請登入已移除的帳戶，然後按一下訊息中的連結，直接瀏覽至帳戶邀請。
   - 如果已移除的共用帳戶不在其他組織中，請登入該帳戶，開啟 AWS Organizations 主控台並瀏覽至 [邀請]。
4. 再次登入管理帳戶，或重新載入 AWS Control Tower 主控台 (如果已開啟)。您將看到著陸區漂移頁面。選擇「重設」以修復 landing zone 域。
5. 等待重置過程完成。

如果修復成功，共用帳戶會以正常狀態和符合性顯示。

如果補救步驟無法還原帳戶，請聯絡 AWS Support。

使用 AWS Control Tower 和 AWS Organizations 主控台還原共用帳戶 (手動修復)

1. 請在以下位置登入 AWS Organizations 主控台https://console.aws.amazon.com/organizations/。您必須以 IAM 使用者、IAM 身分中心的使用者身分登入，或使用`AWSOrganizationsFullAccess`受管政策或同等政策的角色登入。
2. 邀請共用帳戶回到組織。如需邀請帳戶的需求、先決條件和程序的詳細資訊 AWS Organizations，請參閱AWS Organizations 使用者指南中的邀請 AWS 帳戶加入您的組織。
3. 登入已移除的共用帳戶，然後前往 https://console.aws.amazon.com/organizations/home#/invites 接受邀請。
4. 再次登入管理帳戶。
5. 使用`AWSControlTowerServiceRolePolicy`受管政策或同等政策以使用者或角色身分登入 AWS Control Tower 主控台，以及執行所有 AWS Control Tall 動作 (控制塔：*) 的許可。

6. 您將看到 landing zone 漂移頁面，其中包含重置著陸區的選項。選擇「重設」以修復 landing zone 域。
7. 等待重置過程完成。

如果修復成功，共用帳戶會以正常狀態和符合性顯示。

如果補救步驟無法還原帳戶，請聯絡 AWS Support。

自動更新的外部變更

AWS Control Tower 會自動更新您對帳戶電子郵件地址所做的變更，但 Account Factory 不會自動更新這些變更。

變更受控管帳戶的電子郵件地址

AWS Control Tower 會根據主控台體驗的要求擷取和顯示電子郵件地址。因此，共用和其他帳戶的電子郵件地址會在您變更後更新並一致地顯示在 AWS Control Tower 中。

> **Note**
>
> 在中 AWS Service Catalog，Account Factory 會顯示您建立已佈建產品時，在主控台中指定的參數。不過，當帳戶電子郵件地址變更時，不會自動更新原始的帳戶電子郵件地址。這是因為帳戶在概念上包含在佈建的產品中；它與佈建的產品不同。若要更新此數值，您必須更新佈建的產品，而這可能導致控管狀態發生變更。

套用外部 AWS Config 規則

AWS Control Tower 顯示部署到 AWS Control Tower 註冊組織單位的所有 AWS Config 規則的合規狀態，包括在 AWS Control Twer 主控台外部啟用的規則。

刪除 AWS Control Tower 外部的 AWS Control Tower 資源

您可以刪除 AWS Control Tower 中的 OU 和帳戶，而且不需要採取任何進一步的動作即可查看更新。刪除 OU 時，Account Factory 會自動更新，但刪除帳戶時則不會更新。

刪除已登錄的 OU (安全性 OU 除外)

在中 AWS Organizations，您可以使用 API 或主控台移除空的組織單位 (OU)。無法刪除包含帳戶的 OU。

刪除 OU AWS Organizations 時，AWS Control Tower 會收到來自的通知。它會更新 Account Factory 中的 OU 清單，以便註冊 OU 的清單保持一致。

> **Note**
>
> 在中 AWS Service Catalog，Account Factory 已更新，以從您可以佈建帳戶的可用 OU 清單中移除已刪除的 OU。

從 OU 刪除註冊的帳戶

刪除註冊帳戶時，AWS Control Tower 會收到通知並進行更新，以便資訊保持一致。

> **Note**
>
> 在中 AWS Service Catalog，不會更新代表受管理帳戶的 Account Factory 佈建產品以刪除帳戶。相反地，佈建的產品會顯示為 TAINTED 和錯誤狀態。若要清理，請移至 AWS Service Catalog，選擇已佈建的產品，然後選擇 Terminate (終止)。

使用 AWS Control Tower 管理組織和帳戶

您在 AWS Control Tower 中建立的所有組織單位 (OU) 和帳戶都會由 AWS Control Tower 自動管理。此外，如果您擁有現有的 OU 和在 AWS Control Tower 以外建立的帳戶，則可以將其納入 AWS Control Tower 管理。

對於現有 AWS 帳戶 AWS Organizations 和帳戶，大多數客戶偏好註冊包含帳戶的整個組織單位 (OU) 來註冊帳戶群組。您也可以個別註冊帳戶。如需註冊個別帳戶的詳細資訊，請參閱註冊現有的 AWS 帳戶。

術語

- 當您將現有組織帶入 AWS Control Tower 時，稱為註冊組織，或將管理擴展到組織。
- 將 AWS 帳戶帶入 AWS Control Tower 時，稱為註冊帳戶。

檢視您的 OU 和帳戶

在 AWS Control Tower 組織頁面上，您可以檢視您的所有 OU AWS Organizations，包括在 AWS Control Tower 註冊的 OU 以及未註冊的 OU。您可以在階層中檢視巢狀 OU。在 [組織] 頁面上檢視組織單位的簡單方法是從右上角的下拉式清單中選取 [僅限組織單位]。

組織頁面會列出組織中的所有帳戶，無論 AWS Control Tower 的 OU 或註冊狀態為何。在「組織」頁面上查看帳戶的一種簡單方法是從右上角的下拉菜單中選擇「僅帳戶」。如果帳戶符合註冊的先決條件，您可以在 OU 中個別檢視、更新和註冊帳戶。

如果您未選取任何篩選，[組織] 頁面會以階層顯示您的帳戶和 OU。這是監控所有 AWS Control Tower 資源和採取動作的中心位置。如需有關「組織」頁面的詳細資訊，您可以檢視視訊逐步解說。

影片演練

此影片 (4:01) 說明如何使用 AWS Control Tower 中的組織頁面。若要獲得更佳的觀賞效果，請選取影片右下角的圖示，將影片放大至全螢幕。並提供字幕。

AWS Control Tower 中使用組織頁面的影片逐步解說。

主題

- 向 AWS Control Tower 註冊現有的組織單位

- 註冊現有的 AWS 帳戶

將治理擴展到現有組織

您可以按照入門步驟 2 中 AWS Control Tower 使用者指南中所述設定 landing zone (LZ)，將 AWS Control Tower 管理新增至現有組織。

以下是在現有組織中設定 AWS Control Tower landing zone 時的預期情況。

- 每個 AWS Organizations 組織可以有一個 landing zone 域。
- AWS Control Tower 使用現有 AWS Organizations 組織的管理帳戶做為其管理帳戶。不需要新的管理帳戶。
- AWS Control Tower 在已註冊的 OU 中設定兩個新帳戶：稽核帳戶和記錄帳戶。
- 貴組織的 Service Limits 必須允許建立這兩個額外的帳戶。
- 啟動 landing zone 域或註冊 OU 後，AWS Control Tower 控制會自動套用至該 OU 中所有註冊的帳戶。
- 您可以將其他現有 AWS 帳戶註冊到由 AWS Control Tower 管理的 OU 中，以便控制適用於這些帳戶。
- 您可以在 AWS Control Tower 新增更多 OU，也可以註冊現有的 OU。

若要查看註冊和註冊的其他先決條件，請參閱 AWS Control Tower 入門。

以下詳細說明 AWS Control Tower 控制如何不適用於未設定 AWS Control 塔登陸區域的 AWS 組織中的 OU：

- 在 AWS Control Tower Account Factory 以外建立的新帳戶不受已註冊 OU 的控制的約束。
- 除非您特別將這些帳戶註冊到 AWS Control Tower，否則在 OU 中建立且未在 AWS Control Tower 註冊的新帳戶不受控制的約束。請參閱註冊現有的 AWS 帳戶以取得註冊帳戶的詳細資訊。
- 除非您另行註冊 OU 或註冊帳戶，否則其他現有組織、現有帳戶以及任何新 OU 或您在 AWS Control Tower 外建立的任何帳戶都不受 AWS Control Tower 控制的約束。

如需如何將 AWS Control Tower 套用至現有 OU 和帳戶的詳細資訊，請參閱向 AWS Control Tower 註冊現有的組織單位。

如需在現有組織中設定 AWS Control 塔 landing zone 的程序概觀，請參閱下一節中的影片。

> **Note**
>
> 在設定期間，AWS Control Tower 會執行預先檢查以避免常見問題。但是，如果您目前正在使用 AWS landing zone 解決 AWS 方案 AWS Organizations，請在嘗試在組織中啟用 AWS Control Tower 之前諮詢您的解決方案架構師，以確定 AWS Control Tower 是否會干擾您目前的登陸區域部署。另請參閱以取得有如果帳戶不符合先決條件怎麼辦？關將帳戶從一個登陸區域移至另一個登陸區域的資訊

影片：啟用現有的著陸區 AWS Organizations

本影片 (7:48) 說明如何在現有 AWS Organizations 結構中設定和啟用 AWS Control Tower landing zone。若要獲得更佳的觀賞效果，請選取影片右下角的圖示，將影片放大至全螢幕。並提供字幕。

為現有組織啟用 AWS Control Tower

IAM 身分中心和現有組織的注意事項

- 如果已設定 AWS IAM Identity Center (IAM 身分中心)，則 AWS Control Tower 的本地區域必須與 IAM 身分中心區域相同。
- AWS Control Tower 不會刪除現有組態。
- 如果 IAM 身分中心已啟用，而且您正在使用 IAM 身分中心目錄，則 AWS Control Tower 會新增許可集、群組等資源，並照常進行。
- 如果設定了其他目錄 (外部、AD、受管 AD)，AWS Control Tower 不會變更現有組態。如需詳細資訊，請參閱AWS IAM Identity Center (IAM 身分中心) 客戶的注意事項。

使用其他 AWS 服務

在您將組織納入 AWS Control Tower 管控之後，您仍然可以透過 AWS Organizations主控 AWS Organizations 台和 API 存取任何可用的 AWS 服務。如需更多詳細資訊，請參閱 相關 AWS 服務。

AWS Control Tower 中的巢狀 OU

本章列出在 AWS Control Tower 中使用巢狀 OU 時，您需要注意的期望和考量事項。在大多數方面，使用巢狀 OU 與使用扁平 OU 結構相同。「註冊」與「重新註冊」功能可與巢狀 OU 搭配使用，但本章所述的變更行為除外。

影片演練

此影片 (4:46) 說明如何在 AWS Control Tower 中管理巢狀 OU 部署。若要獲得更佳的觀賞效果，請選取影片右下角的圖示，將影片放大至全螢幕。並提供字幕。

AWS Control Tower 中管理巢狀 OU 的影片逐步解說。

如需巢狀 OU 和 landing zone 域的最佳實務指引，請參閱部落格文章使用巢狀 OU 組織 AWS Control Tower landing zone。

從平面 OU 結構展開為巢狀 OU 結構

如果您使用扁平 OU 結構建立 AWS Control Tower landing zone，則可以將其擴展為巢狀 OU 結構。

此過程有四個主要步驟：

1. 在 AWS Control Tower 中建立所需的巢狀 OU 結構。
2. 移至 AWS Organizations 主控台並使用其大量移動功能，將帳戶從來源 OU (平面) 移至目的地 OU (巢狀)。這裡是如何：
   a. 移至您要從中移動帳戶的 OU。
   b. 選取 OU 中的所有帳戶。
   c. 選擇「移動」。

   > **Note**
   >
   > 必須在主控 AWS Organizations 台中完成此步驟，因為 AWS Control Tower 沒有移動功能。

3. 前往 AWS Control Tower 中的巢狀 OU，然後註冊或重新註冊。巢狀 OU 中的所有帳戶都會註冊。
   - 如果您在 AWS Control Tower 中建立 OU，請重新註冊 OU。
   - 如果您在中建立 OU AWS Organizations，請第一次登錄 OU。
4. 移動並註冊帳戶後，請從主控 AWS Organizations 台或 AWS Control Tower 主控台刪除空白的頂層 OU。

巢狀 OU 登錄預先檢查

為了支援成功註冊巢狀 OU 及其成員帳戶，AWS Control Tower 會執行一系列的預先檢查。這些相同的預先檢查會在註冊任何頂層 OU 或巢狀 OU 時執行。如需詳細資訊，請參閱註冊或重新註冊期間失敗的常見原因。

- 如果所有預先檢查都通過，AWS Control Tower 會自動開始註冊您的 OU。
- 如果任何預先檢查失敗，AWS Control Tower 會停止註冊程序，並提供您必須修正的項目清單，然後才能註冊 OU。

巢狀 OU 和角色

AWS Control Tower 會將AWSControlTowerExecution角色部署到目標 OU 下的帳戶，以及嵌套在目標 OU 下的所有 OU 帳戶，即使您只想註冊目標 OU 也一樣。此角色會為管理帳戶的任何使用者授予任何具有該AWSControlTowerExecution角色之帳戶的管理員權限。角色可用來執行 AWS Control Tower 控制通常不允許的動作。

您可以從不打算註冊的未註冊帳戶中刪除此角色。如果刪除此角色，除非您將角色還原到帳戶，否則無法在 AWS Control Tower 註冊帳戶或註冊直屬父 OU。若要刪除帳戶中的AWSControlTowerExecution角色，您必須以該AWSControlTowerExecution角色登入，因為不允許其他 IAM 主體刪除 AWS Control Tower 所管理的角色。

如需如何限制角色存取權的詳細資訊，請參閱角色信任關係的選用條件。

巢狀 OU 和帳戶的註冊和重新註冊期間會發生什麼情況

當您註冊或重新註冊巢狀 OU 時，AWS Control Tower 會註冊目標 OU 的所有未註冊帳戶，並更新所有註冊帳戶。以下是可以期待的。

AWS Control Tower 執行下列任務

- 將AWSControlTowerExecution角色新增至此 OU 下的所有未註冊帳戶，以及其巢狀 OU 中的所有未註冊帳戶。
- 註冊未註冊的會員帳戶。
- 重新註冊註冊的會員帳戶。
- 為新註冊的成員帳戶建立 IAM 身分中心登入。
- 更新現有的註冊成員帳戶，以反映您的 landing zone 變更。

- 更新針對此 OU 及其成員帳戶設定的控制項。

巢狀 OU 註冊的考量事項

- 您無法在核心 OU (安全性 OU) 下註冊 OU。
- 巢狀 OU 必須個別註冊。
- 除非 OU 的父 OU 已註冊，否則您無法註冊 OU。
- 您無法註冊 OU，除非樹狀結構中較高層級的所有 OU 在某些時間都已成功註冊 (有些可能已刪除)。
- 您可以註冊位於漂移較高 OU 下的 OU，但該動作不會修復漂移。

巢狀 OU 限制

- OU 最多可以嵌套根深度為 5 個層級。
- 目標 OU 下的巢狀 OU 必須個別註冊或重新註冊。
- 如果目標 OU 位於階層中的層級 2 或以下，也就是說，如果它不是最上層 OU，則會自動在此 OU 及其下方的所有 OU 上強制執行在較高 OU 上啟用的預防性控制。
- OU 註冊失敗不會向上傳播階層樹狀結構。您可以在父項的 OU 詳細資料頁面上查看巢狀 OU 狀態的詳細資訊。
- OU 註冊失敗不會向下傳播階層樹狀結構。
- AWS Control Tower 不會修改任何新帳戶或現有帳戶的 VPC 設定。

巢狀 OU 與合規性

您可以從 AWS Control Tower 主控台檢視組織頁面中不合規的 OU 和帳戶，以便更大規模了解合規。

巢狀 OU 和帳戶符合性的考量

- OU 的相容性並不是根據巢狀在其下方的 OU 符合性來決定。
- 系統會針對啟用控制項的所有 OU (包括巢狀 OU) 計算控制項的相容性狀態。請參閱 OU 和帳戶的 AWS Control Tower 合規狀態。
- 只有當 OU 具有不相容的帳戶時，不論 OU 位於 OU 階層中的哪個位置，OU 才會顯示為不相容。
- 如果巢狀 OU 不相容，就不會自動將其父 OU 視為不相容。
- 在 OU 詳細資料或帳戶詳細資料頁面上，您可以檢視可能造成 OU 或帳號顯示不符合標準狀態的不相容資源清單。

巢狀 OU 和漂移

在某些情況下，漂移可能會阻止巢狀 OU 的註冊。

對漂移和巢狀 OU 的期望

- 您可以對具有漂移父母的 OU 啟用控制，但不能直接在漂移的 OU 上啟用控制。
- 您可以在漂移的 OU 下啟用偵探控制項，只要它不是最上層的漂移 OU 即可。
- 僅在頂層 OU 上啟用強制控制項。註冊巢狀 OU 時，會略過必要的控制項。
- 一個強制控制項可保護 AWS Config 資源；因此，該控制項必須處於非漂移狀態，才能登錄巢狀 OU。如果已移轉，AWS Control Tower 會封鎖巢狀 OU 的註冊。
- 如果頂層 OU 處於漂移狀態，則保護 AWS Config 資源的控制項可能處於漂移狀態。在此情況下，AWS Control Tower 會封鎖任何需要建立或更新 AWS Config 資源的動作，包括偵探控制的應用程式。

巢狀 OU 和控制項

當您在已註冊 OU 上啟用控制項時，預防性和偵測控制項會有不同的行為。對於巢狀 OU，主動式控制項的行為與偵測控制項類似。

預防性控制

- 預防性控制會在巢狀 OU 上強制執行。
- 強制性預防控制會對 OU 及其巢狀 OU 下的所有帳戶強制執行。
- 預防性控制會影響目標 OU 下巢狀的所有帳戶和 OU，即使這些帳戶和 OU 未註冊也一樣。

Detective 和主動控制

- 巢狀 OU 不會自動繼承偵測或主動控制；這些控制項必須個別啟用。
- Detective 和主動式控制功能只會部署至您登陸區營運區域中的註冊帳號。

啟用的控制狀態和繼承

您可以在 OU 詳細資料頁面上檢視每個 OU 的繼承控制項。

> **Tip**
>
> 您可以利用控制繼承來協助維持在 OU 的 SCP 配額內。例如，您可以在 OU 階層的頂層 OU 上啟用控制項，而不是直接為巢狀 OU 啟用。

繼承狀態

- [繼承] 狀態表示控制項僅透過繼承啟用，而且尚未直接套用至 OU。
- 狀態「已啟用」表示控制項會在此 OU 上強制執行，而不論其在其他 OU 上的狀態為何。
- 狀態「失敗」表示不會在此 OU 上強制執行控制項，無論其在其他 OU 上的狀態為何。

> **Note**
>
> [繼承] 狀態表示控制項已套用至樹狀結構中較高層級的 OU，而且它會在此 OU 上強制執行，但並未直接新增至此 OU。

> **如果您的 landing zone 不是當前版本**
>
> [已啟用] 控制項表格中的每一個資料列都代表一個個別 OU 上啟用的控制項。

巢狀 OU 與根

根不是 OU，無法註冊或重新註冊。您也無法直接在根目錄中建立帳號。根不能不相容或具有生命週期狀態，例如已註冊或處於漂移狀態。

不過，根目錄是所有帳戶和 OU 的最上層容器。在巢狀 OU 的環境中，它是所有其他 OU 都嵌套在其下的節點。

向 AWS Control Tower 註冊現有的組織單位

將多個現有 AWS 帳戶引入 AWS Control Tower 的有效方法是將 AWS Control Tower 的管理擴展到整個組織單位 (OU)。

若要對使 AWS Organizations用建立的現有 OU 及其帳戶啟用 AWS Control Tower 管理，請向 AWS Control Tower landing zone 註冊該 OU。您可以註冊最多包含 300 個帳戶的 OU。如果 OU 包含 300 個以上的帳戶，則無法在 AWS Control Tower 註冊該帳戶。

當您註冊 OU 時，其成員帳戶會註冊到 AWS Control Tower landing zone。它們是由套用至其 OU 的控制項所控制。

> **Note**
>
> 如果您還沒有 AWS Control 塔 landing zone，請先在 AWS Control Twer 建立的新組織或現有組 AWS Organizations 織中設定 landing zone 域。如需如何設定 landing zone 域的更多詳細資訊，請參閱開始使用 AWS Control Tower。

當我註冊 OU 時，我的帳戶會發生什麼情況？

AWS Control Tower 需要獲得許可，才能 AWS Organizations 在您之間 AWS CloudFormation 和代表您建立受信任的存取權限， AWS CloudFormation 以便自動將堆疊部署到組織中的帳戶。

- `AWSControlTowerExecution`角色會新增至所有狀態為「未註冊」的帳號。
- 當您註冊 OU 時，OU 及其所有帳戶預設會啟用必要控制項。

OU 註冊後部分註冊帳戶

您可以成功註冊 OU，但某些帳戶可能仍未註冊。如果是這樣，則這些帳戶不符合註冊的某些先決條件。如果作為註冊 OU 程序一部分的帳戶註冊未成功，帳戶頁面上的帳戶狀態會顯示註冊失敗。您也可以在 OU 頁面上看到帳戶資訊，例如帳戶欄位中的第 4 個，共 5 個。

例如，如果您看到 5 個中的 4 個，則表示您的 OU 總共有 5 個帳戶，其中 4 個帳戶註冊成功，但是有一個帳戶無法在註冊 OU 程序期間註冊。確定帳戶符合註冊必要條件之後，您可以選擇「重新註冊 OU」，將帳戶納入註冊。

註冊 OU 的 IAM 使用者先決條件

當您 AWS Identity and Access Management 執行註冊 OU 作業時，您的 (IAM) 身分識別 (使用者或角色) 或 IAM 身分中心使用者身分必須包含在適當的 Account Factory 產品組合中，即使您已經擁有`Admin`許可也是如此。否則，建立佈建的產品將會在註冊期間失敗。發生失敗的原因是 AWS Control Tower 在註冊 OU 時依賴 IAM 使用者或 IAM 身分中心使用者身分的登入資料。

相關產品組合由 AWS Control Tower 建立，稱為 AWS Control Tower Account Factory 產品組合。選擇 Service Catalog > Account Factory > AWS Control Tower Account Factory 產品組合，以瀏覽至該服務。然後選取名為群組、角色和使用者的索引標籤，以檢視您的 IAM 或 IAM 身分中心身分識別。如需如何授與存取權的詳細資訊，請參閱的文件 AWS Service Catalog。

註冊現有的 OU

在 AWS Control Tower 主控台的組織頁面上，您可以在階層中檢視組織的所有 OU 和帳戶，包括在 AWS Control Tower 註冊的 OU，以及未註冊的 OU。

一般而言，未註冊的 OU 是在中建立的 AWS Organizations，且不受任何其他 landing zone 管理。您可以註冊最多包含 300 個帳戶的現有 OU。如果 OU 包含 300 個以上的帳戶，則無法在 AWS Control Tower 註冊該帳戶。

若要註冊現有的 OU

1. 登入 AWS Control Tower 主控台主控台，網址為 https://console.aws.amazon.com/controltower。
2. 在左窗格導覽功能表中，選擇 [組織]。
3. 在 [組織] 頁面上，選取您要註冊之 OU 旁的圓鈕，然後從右上角的 [動作] 下拉式功能表中選取 [註冊組織單位]，或者選取 OU 的名稱，以便檢視該 OU 的 OU 詳細資訊頁面。
4. 在 OU 詳細資料頁面的右上角，您可以從 [動作] 下拉式功能表中選取 [註冊 OU]。

註冊程序至少需要 10 分鐘才能將管理延伸至 OU，而每增加一個帳戶最多需要 2 分鐘的時間。

註冊現有 OU 的結果

註冊現有 OU 之後，該AWSControlTowerExecution角色可讓 AWS Control Tower 將管理擴展到其個別帳戶。護欄會強制執行，而有關帳戶活動的資訊會報告給您的稽核和記錄帳戶。

其他結果包括以下內容：

- AWSControlTowerExecution 允許 AWS Control Tower 稽核帳戶進行稽核。
- AWSControlTowerExecution幫助您配置組織的日誌記錄，以便將每個帳戶的所有日誌都發送到日誌記錄帳戶。
- AWSControlTowerExecution確保您選取的 AWS Control Tower 控制會自動套用到 OU 中的每個個別帳戶，以及您在 AWS Control Tower 中建立的每個新帳戶。

對於已註冊的 OU，您可以根據 AWS Control Tower 控制所包含的稽核和記錄功能，提供合規和安全報告。您的安全及合規團隊可以確認所有要求都符合，而且沒有發生任何組織偏離。如需漂移的更多資訊，請參閱偵測並解決 AWS Control Tower 中的漂移。

> **Note**
>
> AWS Control Tower 顯示 OU 及其帳戶時，可能會發生一種異常情況。如果您已在已註冊的 OU 中建立帳戶，然後將該註冊帳戶移至另一個尚未註冊的 OU，特別是如果您使用 AWS Organizations 移動帳戶，則可以在 OU 詳細資料頁面中看到結果「0 分之 1」帳戶。此外，您可能已在該未註冊的 OU 中建立另一個未註冊的帳戶。如果有未註冊的帳戶，主控台可能會讀取 OU 的「1 之 1」。似乎單個（新創建的）帳戶已註冊，但實際上並非如此。您必須註冊新帳戶。

建立新的 OU

在 AWS Control Tower 中建立新的 OU

1. 切換作業選項至「組織」頁。
2. 從右上角的 [建立資源] 下拉式功能表中選取 [建立組織單位]。
3. 在 OU 名稱欄位中指定名稱。
4. 在父 OU 下拉式清單中，您可以看到已註冊 OU 的階層。為您要建立的新 OU 選取父系 OU。
5. 選擇新增。

> **Tip**
>
> 若要以較少的步驟新增巢狀 OU，請選取 [組織] 頁面上表格中顯示的父 OU 名稱，檢視該父 OU 的 OU 頁面，然後從右上角的 [動作] 下拉式功能表中選擇 [新增 OU]。新 OU 會自動在您選取的 OU 下建立為巢狀 OU。

> **Note**
>
> 如果您的 landing zone 域不是最新版本，您會在下拉式選單中看到一個平面清單，而不是階層。即使您的 landing zone 域包含巢狀 OU，您也不會在下拉式清單中看到 L5 OU，因為您無

法在 L5 OU 下建立新的 OU。如需 AWS Control Tower 中巢狀 OU 的詳細資訊，請參閱AWS Control Tower 中的巢狀 OU。

註冊或重新註冊時失敗的常見原因

如果 OU 或其任何成員帳戶的註冊（或重新註冊）失敗，您可以下載包含詳細報告的文件，其中顯示哪些預先檢查未通過。您可以選擇出現在註冊區域右上方的 [下載] 按鈕來完成下載。

本節列出預先檢查失敗時可能會收到的錯誤類型，以及如何更正錯誤。

一般而言，當您註冊或重新註冊 OU 時，該 OU 內的所有帳戶都會在 AWS Control Tower 中註冊。不過，即使整個 OU 已成功註冊，部分帳戶也可能無法註冊。在這些情況下，您必須解決與帳戶相關的預先檢查失敗，然後嘗試重新註冊該帳戶或 OU。

著陸區錯誤

- 著陸區尚未準備好

  重設您目前的 landing zone，或將其更新為最新版本。

OU 錯誤

- 超過 SCP 的最大數目

  您可能超過每個 OU 的服務控制原則 (SCP) 限制，或者您可能已達到另一個配額。每個 OU 的限制為 5 個 SCP，適用於 AWS Control Tower landing zone 中的所有 OU。如果您擁有的 SCP 數量超過配額允許的數量，則必須刪除或合併 SCP。
- 衝突的 SCP

  現有的 SCP 可套用至 OU 或帳戶，這會導致 AWS Control Tower 無法註冊帳戶。查看已套用的 SCP，瞭解任何可能導致 AWS Control Tower 無法運作的政策。請務必檢查階層中較高層級 OU 繼承的 SCP。
- 超過堆疊設定配額

  堆疊集配額可能已超過。如果您的執行個體數量超過配額允許的數量，則必須刪除一些堆疊執行個體。如需詳細資訊，請參閱AWS CloudFormation 使用者指南中的AWS CloudFormation 配額。
- 超過帳戶限制

AWS Control Tower 在註冊期間將每個 OU 限制為 300 個帳戶。

帳戶錯誤

- 帳戶防止預先檢查

  OU 上現有的 SCP 可防止 AWS Control Tower 對您的 OU 成員帳戶進行預先檢查。若要解決此預先檢查失敗，請從 OU 更新或移除 SCP。

- 電郵地址錯誤

  您為帳號指定的電子郵件地址不符合命名標準。以下是指定允許哪些字符的正則表達式（regex）：`[A-Z0-9a-z._%+-]+@[A-Za-z0-9.-]+[.]+[A-Za-z]+`

- Config 記錄器或交付通道已啟用

  該帳戶可能具有現有的 AWS Config 組態記錄器或傳遞通道。您必須 AWS CLI 在 AWS Control Tower 管理帳戶管理資源的所有 AWS 區域中刪除或修改這些資源，然後才能註冊帳戶。

- 停用 STS

  AWS Security Token Service (AWS STS) 可能會在帳戶中停用。 AWS 必須在 AWS Control Tower 支援的所有區域的帳戶中啟用 STS 端點。

- IAM 身分識別中心衝突

  AWS Control Tower 的本地區域與 AWS IAM Identity Center (IAM 身分中心) 區域不同。如果已設定 IAM 身分中心，則 AWS Control Tower 的本地區域必須與 IAM 身分中心區域相同。

- 衝突的 SNS 主題

  該帳戶具有 AWS Control Tower 需要使用的亞馬遜簡單通知服務 (Amazon SNS) 主題名稱。AWS Control Tower 會建立具有特定名稱的資源 (例如 SNS 主題)。如果已使用這些名稱，則 AWS Control Tower 安裝會失敗。如果您重複使用先前在 AWS Control Tower 註冊的帳戶，可能會發生這種情況。

- 偵測到暫停帳號

  此帳戶已被暫停使用。無法註冊 AWS Control Tower。請從這個 OU 移除帳戶，然後再試一次。

- IAM 使用者不在產品組合中

  註冊 OU 之前，請先將 AWS Identity and Access Management (IAM) 使用者新增至 Service Catalog 產品組合。此錯誤僅適用於管理帳戶。

- 帳戶不符合先決條件

  帳戶不符合帳戶註冊的先決條件。例如，帳戶可能缺少在 AWS Control Tower 中註冊所需的角色和許可。有關添加角色的說明可在中找到手動將所需的 IAM 角色新增至現有角色 AWS 帳戶 並註冊。

提醒您，當您在 AWS Control Tower 註冊 AWS 帳戶時，所有帳戶都會自動啟用 AWS CloudTrail 這些帳戶。如果 CloudTrail 在註冊之前的帳戶啟用，除非您在開始註冊程序 CloudTrail 之前停用，否則您可能會遇到雙重計費的情況。

更新組織

在 OU 中更新組織單位 (OU) 或更新多個帳戶的最快方法是重新註冊 OU。

何時更新 AWS Control Tower OU 和帳戶

執行 landing zone 更新時，您必須更新註冊的帳戶，才能將新的控制項套用至這些帳戶。

- 您可以使用 [重新註冊] 選項對 OU 下的所有帳戶執行更新。
- 如果您的 landing zone 中有多個註冊 OU，請重新註冊所有 OU 以更新您的所有帳戶。
- 若要更新單一帳戶，您可以從 AWS Control Tower 主控台進行更新，也可以在中選取更新佈建的產品選項 AWS Service Catalog。請參閱 更新主控台中的帳戶。

更新相同 OU 中的多個帳戶

使用一個動作更新單一 OU 中的多個帳戶

1. 登入 AWS Control Tower 主控台主控台，網址為 https://console.aws.amazon.com/controltower。
2. 在左窗格導覽功能表中，選擇 [組織]。
3. 在 [組織] 頁面上，選擇任何 OU 以檢視 OU 詳細資訊頁面。
4. 在右上角的「動作」下，選取「重新註冊 OU」。

如果您需要更新所有帳戶和 OU，請針對 AWS Control Tower 組織中的每個 OU 重複這些步驟。

或者，您可以選取任何顯示 [可用更新] 狀態的帳戶，然後根據需要選擇 [更新帳戶]。

重新註冊期間會發生什麼

當您重新註冊 OU 時：

- [州/省] 欄位會指出帳戶目前是否向 AWS Control Tower (已註冊) 註冊、該帳戶是否從未註冊 (未註冊)，或是先前註冊失敗 (註冊失敗)。
- 當您重新註冊 OU 時，`AWSControlTowerExecution`角色會新增至所有狀態為 [未註冊] 或 [註冊失敗] 的帳戶。
- AWS Control Tower 會為這些新註冊的帳戶建立單一登入 (IAM 身分中心) 登入。
- 註冊的帳戶會重新註冊到 AWS Control Tower。
- 套用至 OU 的任何預防性控制項上的偏移都是固定的，因為 SCP 會傳回其預設定義。
- 所有帳號都會更新，以反映最新的 landing zone 變更。

如需詳細資訊，請參閱 註冊現有的 AWS 帳戶。

> **Tip**
>
> 當您重新註冊 OU 時，或是當您更新您的 landing zone 版本和多個會員帳戶時，您可能會看到提及-的失敗訊息。StackSet AWSControlTowerExecutionRole管理帳戶 StackSet 中的此操作可能會失敗，因為 AWSControlTowerExecutionIAM 角色已存在於所有註冊的成員帳戶中。此錯誤訊息為預期行為，可忽略此錯誤訊息。

更新單一帳戶

您可以在 AWS Control Tower 台或 Service Catalog 主控台中更新個別的 AWS Control 塔帳戶。

若要在 AWS Control Tower 主控台中更新單一帳戶，請參閱更新主控台中的帳戶。

若要更新中的單一帳號 AWS Service Catalog

1. 前往 AWS Service Catalog。
2. 在左窗格導覽功能表中，選擇已佈建的產品。
3. 在「已佈建的產品」頁面上，選取您要更新之已佈建產品旁邊的圓鈕。
4. 在右上角，選擇「操作」 下拉列表以更新。

若要深入瞭解中的更新 AWS Service Catalog，請參閱更新佈建的產品《Service Catalog 管理員指南》中的〈更新產品〉。

整合服務

AWS Control Tower 是建立在其他服務之上的 AWS 服務，可協助您設定架構良好的環境。本章提供這些服務的簡要概觀，包括基礎服務及其在 AWS Control Tower 中運作方式的組態資訊。

如需有關如何測量 Well-Architected 環境的詳細資訊，請瞭解架構AWS 良好的工具。另請參閱管理和治理雲端環境指南。

主題

- 部署環境 AWS CloudFormation
- 監視事件 CloudTrail
- 監控資源和服務 CloudWatch
- 控管資源組態 AWS Config
- 使用 IAM 管理實體的許可
- AWS Key Management Service
- 使用 Lambda 執行無伺服器運算函數
- 透過管理帳戶 AWS Organizations
- 使用 Amazon S3 存放物件
- 使用 Security Hub 監控您的環境
- 通過佈建帳戶 AWS Service Catalog
- 通過 Amazon 簡單通知服務跟踪警報
- 建置分散式應用程式 AWS Step Functions

部署環境 AWS CloudFormation

AWS CloudFormation 可讓您以預測和重複的方式建立和佈建 AWS 基礎結構部署。它可協助您運用 AWS 產品在雲端中建置高度可靠、可高度擴充、具成本效益的應用程式，而不必擔心建立和設定基 AWS 礎架構。 AWS CloudFormation 可讓您使用範本檔案，以單一單元 (堆疊) 的形式一起建立和刪除資源集合。如需詳細資訊，請參閱 AWS CloudFormation 使用者指南。

AWS Control Tower 使用 AWS CloudFormation 堆疊集對帳戶套用控制。如需 AWS Control Tower 如何 AWS CloudFormation 協同運作的詳細資訊，請參閱 建立 AWS Control Tower 資源 AWS CloudFormation。

監視事件 CloudTrail

AWS Control Tower 設定 AWS CloudTrail 為啟用集中式記錄和稽核。使用 CloudTrail管理帳戶可以檢閱成員帳戶的管理動作和生命週期事件。

CloudTrail 保留帳戶 AWS API 呼叫歷史記錄，協助您監控雲端 AWS 環境。例如，您可以識別針對支援服務呼叫 AWS API 的使用者和帳戶 CloudTrail、進行呼叫的來源 IP 位址，以及發生呼叫的時間。您可以使用 API 整合 CloudTrail 到應用程式中、為您的組織自動建立追蹤、檢查追蹤的狀態，以及控制系統管理員開啟和關閉 CloudTrail 登入的方式。如需詳細資訊，請參閱 AWS CloudTrail 使用者指南。

監控資源和服務 CloudWatch

Amazon CloudWatch 提供可靠、可擴展且靈活的監控解決方案，您可以在幾分鐘內開始使用。您再也不需要設定、管理及擴展自己的監控系統和基礎設施。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南。

如需 Amazon 如何與 AWS Control Tower CloudWatch 搭配使用的詳細資訊，請參閱監控。

控管資源組態 AWS Config

AWS Config 提供與您 AWS 帳戶相關聯的資源的詳細檢視，包括如何設定這些資源、彼此之間的關聯性，以及組態及其關係在一段時間內如何變更。如需詳細資訊，請參閱《AWS Config 開發人員指南》。

AWS Config AWS Control Tower 佈建的資源會自動標記，`aws-control-tower`且值為`managed-by-control-tower`。

如需 AWS Control Tower 中 AWS Config 監控和記錄資源方式的詳細資訊，以及如何向您收取費用，請參閱監視資源變更 AWS Config。

AWS Control Tower 用 AWS Config 規則 於實作偵探控制。如需詳細資訊，請參閱關於 AWS Control Tower 中的控制。

使用 IAM 管理實體的許可

AWS Identity and Access Management (IAM) 是用來控制其他 AWS 服務存取的 AWS 服務。透過 IAM，您可以集中管理使用者、安全登入資料 (例如存取金鑰和權限)，以指定授與使用者和應用程式存取權的 AWS 資源。

當您設定 landing zone 域時，如果您選取 IAM 做為身分提供者，則可以 AWS IAM Identity Center 自動為其建立多個群組。這些群組具有來自 IAM 預先定義的許可政策的權限集。您的最終使用者也可以使用 IAM 定義 IAM 使用者和成員帳戶內其他實體的許可範圍。

AWS Identity and Access Management (IAM) 可簡化您管理 AWS 帳戶和商業應用程式存取權的方式。您可以在 AWS Control Tower 中控制所有 AWS 帳戶的 IAM 身分中心存取權和使用者許可。

如需詳細資訊，請參閱 AWS IAM Identity Center 使用者指南。

如果您所在的位置不支援 IAM，您可以使用其他身分提供者來手動設定和維護自己的使用者和群組。
AWS 區域

AWS Key Management Service

AWS Key Management Service (AWS KMS) 可讓您建立和控制保護資料的金鑰。AWS Control Tower 可選擇性地允許您使用 AWS KMS 加密金鑰加密資料。如需相關資訊 AWS KMS，請參閱 AWS KMS 開發人員指南。

如需如何使用 AWS Control Tower 設定 AWS KMS 金鑰的詳細資訊，請參閱選擇性設定 AWS KMS 金鑰。

使用 Lambda 執行無伺服器運算函數

使用 AWS Lambda，您無需佈建或管理伺服器即可執行程式碼。您可以針對許多類型的應用程式或後端服務執行程式碼，而不需要額外的管理額外負荷。當您上傳程式碼時，Lambda 可以以高可用性執行和擴展程式碼。您可以將程式碼設定為自動從其他 AWS 服務觸發，也可以直接從任何 Web 或行動應用程式呼叫程式碼。

例如，可以透過程式設計方式假設 AWS Control Tower 稽核帳戶中的某些角色，以便您可以使用 Lambda 檢閱其他帳戶。此外，您也可以使用 AWS Control Tower 生命週期事件觸發 Lambda 函數。

透過管理帳戶 AWS Organizations

AWS Organizations 是一項帳戶管理服務，可讓您將多個 AWS 帳戶整合到您建立並集中管理的組織中。透過「組 Organizations」，您可以建立成員帳戶，並邀請現有帳戶加入您的組織。您可以將這些帳戶分組，並連接以政策為基礎的控制。如需詳細資訊，請參閱 AWS Organizations 使用者指南。

在 AWS Control Tower 中，Organizations 可協助集中管理帳單、控制存取、合規和安全性，以及跨成員 AWS 帳戶共用資源。帳戶會分組成邏輯群組，稱為組織單位 (OU)。如需「Organizations」的詳細資訊，請參閱AWS Organizations 使用者指南。

AWS Control Tower 使用下列 OU：

- 根 — landing zone 中所有帳戶和所有其他 OU 的上層容器。
- 安全性 — 此 OU 包含記錄封存帳戶、稽核帳戶及其擁有的資源。
- 沙箱 — 此 OU 會在您設定 landing zone 域時建立。您 landing zone 中的其他子系 OU 包含您的會員帳戶。這些是您的最終使用者存取以執行 AWS 資源工作的帳戶。

> **Note**
>
> 您可以透過組織單位頁面上的 AWS Control 塔主控台，在您的 landing zone 域新增其他 OU。

考量事項

透過 AWS Control Tower 建立的 OU 可以套用控制。依預設，無法在 AWS Control Tower 外建立的 OU。不過，您可以註冊此類 OU。註冊 OU 之後，您可以對其及其帳戶套用控制權。如需註冊 OU 的相關資訊，請參閱向 AWS Control Tower 註冊現有的組織單位。

使用 Amazon S3 存放物件

Amazon Simple Storage Service (Amazon S3) 是網際網路儲存服務。您可以使用 Amazon S3 隨時從 Web 任何地方存放和擷取任意資料量。您可以使用 AWS Management Console簡單且直覺的 web 界面，來完成這些任務。如需詳細資訊，請參閱 Amazon 簡易儲存服務使用者指南。

設定 landing zone 時，系統會在您的日誌存檔帳戶中建立 Amazon S3 儲存貯體，以包含 landing zone 中所有帳戶的所有日誌。

使用 Security Hub 監控您的環境

AWS Control Tower 透過稱為服務管理標準：AWS Control Tower 的 Security Hub 標準與 AWS 安全中心整合。如需詳細資訊，請參閱 Security Hub 標準。

通過佈建帳戶 AWS Service Catalog

AWS Service Catalog 讓 IT 管理員能夠建立、管理及分發已核准產品的產品組合給終端使用者，讓他們在個人化入口網站中存取所需的產品。典型產品包括使用資源部署的伺服器、 AWS 資料庫、網站或應用程式。

您可以控制具有特定產品存取權的使用者，這可讓您強制遵循組織業務標準、管理產品生命週期，以及協助使用者自信地尋找和推出產品。如需詳細資訊，請參閱 Service Catalog 管理員指南。

在 AWS Control Tower 中，您的中央雲端管理員和最終使用者可以使用稱為「自訂藍圖」的 AWS Service Catalog 產品在 landing zone 域佈建自訂帳戶。如需詳細資訊，請參閱步驟 2。建立 AWS Service Catalog 產品。

AWS Control Tower 還可以使用 Service Catalog API 進一步自動化帳戶佈建和更新。如需詳細資訊，請參閱開 AWS Service Catalog 發人員指南。

轉換至 AWS Service Catalog 外部產品類型

AWS Service Catalog 將對 Terraform 開放原始碼產品和佈建產品的支援變更為新的產品類型，稱為「外部」。若要深入了解此轉換，請參閱《AWS Service Catalog 管理員指南》中的「將現有的 Terraform 開放原始碼產品和佈建的產品更新為外部產品類型」。

這項變更會影響您透過 AWS Control 塔帳戶原廠自訂建立或註冊的現有帳戶。若要將這些帳戶轉換為外部產品類型，您需要在 AWS Service Catalog 和 AWS Control Tower 中進行變更。

若要轉換至外部產品類型

1. 升級您現有的 Terraform 參考引擎， AWS Service Catalog 以包含對外部和 Terraform 開放原始碼產品類型的支援。如需有關更新 Terraform 參考引擎的指示，請檢閱儲存AWS Service Catalog GitHub 庫。
2. 在中 AWS Service Catalog，複製任何現有的 Terraform 開放原始碼產品 (藍圖)，並使用新的外部產品類型複製這些產品。請勿終止現有的 Terraform 開放原始碼藍圖。
3. 在 AWS Control Tower 中，使用 Terraform 開放原始碼藍圖更新每個帳戶，以使用新的外部藍圖。
    a. 若要更新藍圖，您必須先完全移除 Terraform 開放原始碼藍圖。如需詳細資訊，請檢閱從帳戶移除藍圖。
    b. 將新的外部藍圖新增至相同的帳戶。如需詳細資訊，請參閱將藍圖新增至 AWS Control Tower 帳戶。
4. 使用 Terraform 開放原始碼藍圖的所有帳戶都更新為外部藍圖後，請返回 AWS Service Catalog 並終止使用 Terraform 開放原始碼作為產品類型的所有產品。
5. 未來，所有使用 AWS Control Tower 帳戶工廠自訂建立或註冊的帳戶都必須參考使用AWS CloudFormation或外部產品類型的藍圖。

對於使用外部產品類型建立的藍圖，AWS Control Tower 僅支援使用 Terraform 範本和 Terraform 參考引擎的帳戶自訂。若要深入了解，請檢閱設定以進行自訂。

> **Note**
>
> 建立新帳戶時，AWS Control Tower 不支援 Terraform 開放原始碼做為產品類型。若要深入瞭解這些變更，請參閱AWS Service Catalog 管理員指南中的「將現有的 Terraform 開放原始碼產品和佈建的產品更新為外部產品類型」。 AWS Service Catalog 將視需要透過此產品類型轉換為客戶提供支援。請連絡您的客戶代表以請求協助。

通過 Amazon 簡單通知服務跟踪警報

Amazon Simple Notification Service (Amazon SNS) 是一種 Web 服務，可讓應用程式、最終使用者和裝置立即從雲端傳送和接收通知。如需詳細資訊，請參閱《Amazon Simple Notification Service 開發人員指南》。

AWS Control Tower 使用 Amazon SNS 向管理帳戶和稽核帳戶的電子郵件地址傳送程式化提醒。這些警示可協助您防止在 landing zone 內漂移。如需詳細資訊，請參閱 偵測並解決 AWS Control Tower 中的漂移。

我們也使用 Amazon 簡易通知服務從中傳送合規通知 AWS Config。

> **Tip**
>
> 接收 AWS Control Tower 控制合規通知 (在您的稽核帳戶中) 的最佳方式之一就是訂閱`AggregateConfigurationNotifications`。這項服務可協助您檢查合規性。它為您提供有關超出合 AWS Config 規規則的真實數據。 AWS Config 自動維護 OU 中的帳戶清單。您必須使用電子郵件或 SNS 允許的任何類型的訂閱手動訂閱。該聲明`arn:aws:sns:`*`homeregion`*`:`*`account`*`:aws-controltower-AggregateSecurityNotifications`會導致您的審計帳戶。

建置分散式應用程式 AWS Step Functions

AWS Step Functions 可讓您輕鬆地將分散式應用程式的元件作為視覺化工作流程中的一系列步驟進行協調。您可以快速建立和執行狀態機器，以可靠和可擴展的方式執行應用程式的步驟。如需詳細資訊，請參閱 AWS Step Functions 開發人員指南。

AWS Control Tower 中的身分和存取管理

若要在您的 landing zone 執行任何操作，例如在 Account Factory 中佈建帳戶，或在 AWS Control Twer 主控台 (IAM) 中建立新的組織單位 AWS Identity and Access Management (OU)，或 AWS IAM Identity Center 要求您驗證您是核准的 AWS 使用者。例如，如果您使用 AWS Control Tower 主控台，您可以按照管理員提供的 AWS 登入資料來驗證身分。

驗證身分後，IAM 會在特定作業和資源上使 AWS 用一組已定義的許可來控制您的存取。如果您是帳戶管理員，則可以使用 IAM 控制其他 IAM 使用者對與您帳戶相關聯之資源的存取。

主題

身分驗證

您可以存取 AWS 下列任何類型的身分識別：

- AWS 帳號 root 使用者 — 當您第一次建立 AWS 帳號時，您會以一個可完整存取帳號中所有 AWS 服務和資源的身分開始。此身份稱為 AWS 帳號根使用者。當您使用建立帳戶時使用的電子郵件地址和密碼登入時，您就可以存取此身分。強烈建議您不要以根使用者處理日常作業，即使是管理作業。相反地，請遵循最佳做法，即僅使用 root 使用者來建立您的第一個 IAM 身分中心使用者 (建議使用) 或 IAM 使用者 (在大多數使用案例中不是最佳做法)。接著請妥善鎖定根使用者憑證，只用來執行少數的帳戶與服務管理任務。如需詳細資訊，請參閱 何時以 root 使用者身分登入。
- IAM 使用者 — IAM 使用者是您 AWS 帳戶中具有特定自訂許可的身分。您可以使用 IAM 使用者登入資料登入以保護 AWS 網頁，例如 AWS 管理主控台、 AWS 論壇或 Sup AWS port 中心。 AWS 最佳實務建議您建立 IAM 身分中心使用者而非 IAM 使用者，因為當您建立具有長期登入資料的 IAM 使用者時，會存在較大的安全風險。

  如果您必須為特定目的建立 IAM 使用者，除了登入認證外，您還可以為每個 IAM 使用者產生存取金鑰。當您透過數個 SDK 之一或使用 AWS 命令列介面 (CLI) 以程式設計方式呼叫 AWS 服務時，您

可以使用這些金鑰。此 SDK 和 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，則必須自行簽署要求。AWS Control Tower 支援簽章版本 4，這是一種驗證傳入 API 請求的協定。如需驗證要求的詳細資訊，請參閱 AWS 一般參考中的簽章版本 4 簽署程序。

- 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。IAM 角色與 IAM 使用者類似，因為它是一個 AWS 身分，而且具有許可政策，可決定身分可以執行和不能在其中執行的操作 AWS。但是，角色的目的是讓需要它的任何人可代入，而不是單獨地與某個人員關聯。此外，角色沒有與之關聯的標準長期憑證，例如密碼或存取金鑰。反之，當您擔任角色時，其會為您的角色工作階段提供臨時安全性登入資料。使用臨時登入資料的 IAM 角色在下列情況中非常有用：
  - 聯合使用者存取 — 您可以使用企業使用者目錄或 Web 身分提供者的現有身分，而不是建立 IAM 使用者。 AWS Directory Service這些稱為聯合使用者。 AWS 透過身分識別提供者要求存取時，會將角色指派給聯合身分使用者。如需有關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。
  - AWS 服務存取 — 服務角色是一種 IAM 角色，服務會代表您在帳戶中執行動作。當您設定某些 AWS 服務環境時，您必須定義要擔任的服務角色。此服務角色必須包含服務存取所需 AWS 資源所需的所有權限。各個服務的服務角色不同，但許多都可讓您選擇許可，只要您符合該服務所記錄的需求。服務角色提供的存取權僅限在您的帳戶內，不能用來授予存取其他帳戶中的服務。您可以從 IAM 內建立、修改和刪除服務角色。例如，您可以建立一個角色，允許 Amazon RedShift 代表您存取 Amazon S3 儲存貯體，然後將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將權限委派給 AWS 服務。
  - 在 Amazon EC2 上執行的應用程式 — 您可以使用 IAM 角色管理在 Amazon EC2 執行個體上執行的應用程式的臨時登入資料，以及提出 AWS CLI 或 AWS API 請求。這比在 Amazon EC2 執行個體中存放存取金鑰更可取。若要將 AWS 角色指派給 Amazon EC2 執行個體並讓其所有應用程式都可以使用，請建立連接至執行個體的執行個體設定檔。執行個體設定檔包含該角色，並且可讓 Amazon EC2 執行個體上執行的程式取得臨時憑證。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM 角色為在 Amazon EC2 執行個體上執行的應用程式授予許可。
- IAM 身分中心使用者入口網站的 IAM 身分識別中心使用者身分驗證是由您連線到 IAM 身分中心的目錄所控制。不過，終端使用者可從使用者入口網站中使用的 AWS 帳戶授權是由兩個因素決定：
  - 誰已在 AWS IAM 身分中心主控台中被指派存取這些 AWS 帳戶。如需詳細資訊，請參閱AWS IAM Identity Center 使用指南中的單一登入存取。
  - AWS IAM Identity Center 主控台中已授予最終使用者的權限層級，以允許使用者適當存取這些 AWS 帳戶。如需詳細資訊，請參閱《AWS IAM Identity Center 使用指南》中的〈權限集〉。

存取控制

若要在您的 landing zone 建立、更新、刪除或列出 AWS Control Tower AWS 資源或其他資源，您需要許可才能執行操作，而且您需要存取對應資源的許可。此外，若要以程式設計方式執行操作，您需要有效的存取金鑰。

以下各節說明如何管理 AWS Control Tower 的許可：

主題

- 管理 AWS Control Tower 資源存取許可的概觀
- 針對 AWS Control Tower 使用身分型政策 (IAM 政策)

使用 AWS IAM 身分中心和 AWS Control Tower

在 AWS Control Tower 中，IAM 身分中心可讓中央雲端管理員和終端使用者管理對多個 AWS 帳戶和商業應用程式的存取。根據預設，AWS Control Tower 會使用此服務來設定和管理透過 Account Factory 建立之帳戶的存取權，除非您已選取自行管理身分和存取控制的選項。

如需有關選取身分識別提供者的詳細資訊，請參閱。IAM 身分識別中心指引

如需有關如何在 AWS Control Tower 中設定 IAM 身分中心使用者和許可的簡短教學課程，您可以觀看此影片 (6:23)。若要獲得更佳的觀賞效果，請選取影片右下角的圖示，將影片放大至全螢幕。並提供字幕。

在 AWS Control Tower 中設定 AWS IAM 身分中心的影片逐步解說。

關於使用 IAM 身分中心設定 AWS Control Tower

最初設定 AWS Control Tower 時，只有根使用者和任何具有正確許可的 IAM 使用者可以新增 IAM 身分中心使用者。不過，在AWSAccountFactory群組中新增使用者之後，他們可以從 Account Factory 精靈建立新的 IAM 身分中心使用者。如需詳細資訊，請參閱 使用 Account Factory 佈建和管理帳戶。

如果您選擇建議的預設值，AWS Control Tower 會使用預先設定的目錄來設定您的登 landing zone，以協助您管理使用者身分和單一登入，以便您的使用者擁有跨帳戶的聯合存取權。當您設定 landing zone 域時，會建立此預設目錄以包含使用者群組和權限集。

> **Note**
>
> 您可以使用 IAM Identity Center AWS IAM Identity Center 的委派系統管理員功能，將組織中的管理委派給管理帳戶以外的帳戶。如果您選擇使用此功能，請注意，具有管理群組成員資格存取權的管理員也可以管理指派給管理帳戶的群組。如需詳細資訊，請參閱此部落格文章，標題為，開始使用 AWS SSO 委派系統管理

使用者群組、角色和權限集

使用者群組可管理共用帳戶中定義的特殊角色。角色會建立屬於同一組的許可集。群組的所有成員都會繼承與群組相關聯的許可集合或角色。您可以為成員帳戶的使用者建立新群組，以便針對群組執行特定工作自訂指派所需的角色。

可用的權限集涵蓋各種不同的使用者許可需求，例如唯讀存取、AWS Control Tower 管理存取權限和 Service Catalog 存取。這些權限集可讓您的使用者在您的 landing zone 快速佈建自己的 AWS 帳戶，並符合您企業的準則。

如需規劃使用者、群組和許可配置的秘訣，請參閱 設定群組、角色和原則的建議

如需有關如何在 AWS Control Tower 中使用此服務的詳細資訊，請參閱使用AWS IAM Identity Center者指南中的以下主題。

- 若要新增使用者，請參閱新增使用者。
- 若要將使用者新增到群組，請參閱將使用者新增到群組。
- 若要編輯使用者屬性，請參閱編輯使用者屬性。
- 若要新增群組，請參閱新增群組。

> **Warning**
>
> AWS Control Tower 會在您的主區域中設定您的 IAM 身分中心目錄。如果您在其他區域設定 landing zone 域，然後導覽至 IAM 身分中心主控台，則必須將該區域變更為您的本地區域。請勿刪除您本地區域中的 IAM 身分中心組態。

IAM 身分中心帳戶和 AWS Control Tower 的注意事項

以下是在 AWS Control Tower 中使用 IAM 身分中心使用者帳戶時需要注意的事項。

- 如果您的 AWS IAM 身分中心使用者帳戶已停用，您會在嘗試在 Account Factory 中佈建新帳戶時收到錯誤訊息。您可以在 IAM 身分中心主控台中重新啟用 IAM 身分中心使用者。
- 如果您在更新與 Account Factory 提供的帳戶相關聯的已佈建產品時指定新的 IAM 身分中心使用者電子郵件地址，AWS Control Tower 會建立新的 IAM 身分中心使用者帳戶。之前建立的使用者帳戶不會移除。如果您想要從 AWS IAM 身分中心移除先前的 IAM 身分中心使用者電子郵件地址，請參閱停用使用者。
- AWS IAM 身分中心已與 Azure 作用中目錄整合，您可以將現有的 Azure 作用中目錄連線到 AWS Control Tower。
- 如需 AWS Control Tower 行為如何與 AWS IAM 身分中心和不同身分來源互動的詳細資訊，請參閱 AWS IAM 身分中心文件中的變更身分來源的注意事項。

適用於 AWS Control Tower 的 IAM 身分中心群組

AWS Control Tower 提供預先設定的群組，以組織在帳戶中執行特定任務的使用者。您可以直接在 IAM 身分中心新增使用者，並將其指派給這些群組。執行此作業會將許可集與您帳戶內群組中的使用者進行比對。當您設置 landing zone 域時，會建立下列群組。

AWSAccountFactory

帳戶	許可集	描述
管理帳戶	AWSServiceCatalogEndUserAccess	此群組僅用於此帳戶，以使用 Account Factory 佈建新帳戶。

AWSServiceCatalogAdmins

帳戶	許可集	描述
管理帳戶	AWSServiceCatalogAdminFullAccess	此群組僅用於此帳戶，以對 Account Factory 進行系統管理變更。除非此群組中的使用者也在AWSAccountFactory群組中，否則無法佈建新帳戶。

AWSControlTowerAdmins

帳戶	許可集	描述
管理帳戶	AWSAdministratorAccess	此帳戶中此群組的使用者是唯一可存取 AWS Control 塔主控台的使用者。
日誌存檔帳戶	AWSAdministratorAccess	此帳戶中的使用者將具備管理存取權限。
稽核帳戶	AWSAdministratorAccess	此帳戶中的使用者將具備管理存取權限。
成員帳戶	AWSOrganizationsFullAccess	使用者擁有此帳戶中「Organizations」的完整存取權。

AWSSecurityAuditPowerUsers

帳戶	許可集	描述
管理帳戶	AWSPowerUserAccess	使用者可以執行應用程式開發工作，並可建立和設定支援 AWS 感知應用程式開發的資源和服務。
日誌存檔帳戶	AWSPowerUserAccess	使用者可以執行應用程式開發工作，並可建立和設定支援 AWS 感知應用程式開發的資源和服務。
稽核帳戶	AWSPowerUserAccess	使用者可以執行應用程式開發工作，並可建立和設定支援 AWS 感知應用程式開發的資源和服務。
成員帳戶	AWSPowerUserAccess	使用者可以執行應用程式開發工作，並可建立和設定支援

帳戶	許可集	描述
		AWS 感知應用程式開發的資源和服務。

AWSSecurityAuditors

帳戶	許可集	描述
管理帳戶	AWSReadOnlyAccess	使用者擁有此帳戶中所有 AWS 服務和資源的唯讀存取權。
日誌存檔帳戶	AWSReadOnlyAccess	使用者擁有此帳戶中所有 AWS 服務和資源的唯讀存取權。
稽核帳戶	AWSReadOnlyAccess	使用者擁有此帳戶中所有 AWS 服務和資源的唯讀存取權。
成員帳戶	AWSReadOnlyAccess	使用者擁有此帳戶中所有 AWS 服務和資源的唯讀存取權。

AWSLogArchiveAdmins

帳戶	許可集	描述
日誌存檔帳戶	AWSAdministratorAccess	此帳戶中的使用者將具備管理存取權限。

AWSLogArchiveViewers

帳戶	許可集	描述
日誌存檔帳戶	AWSReadOnlyAccess	使用者擁有此帳戶中所有 AWS 服務和資源的唯讀存取權。

AWSAuditAccountAdmins

帳戶	許可集	描述
稽核帳戶	AWSAdministratorAccess	此帳戶中的使用者將具備管理存取權限。

管理 AWS Control Tower 資源存取許可的概觀

每個 AWS 資源都擁有 AWS 帳戶，建立或取得資源存取權的權限由權限原則控制。帳戶管理員可以將許可政策連接到 IAM 身分 (即使用者、群組和角色)。某些服務 (例如 AWS Lambda) 也支援將權限原則附加至資源。

> **Note**
>
> 「帳戶管理員」 (或管理員) 是具有管理員權限的使用者。如需詳細資訊，請參《IAM 使用者指南》中的 IAM 最佳實務。

當您負責將權限授與使用者或角色時，您必須知道並追蹤需要權限的使用者和角色、每個使用者和角色需要權限的資源，以及操作這些資源所必須允許的特定動作。

主題

- AWS Control Tower 資源和操作
- 關於資源擁有權
- 管理資源存取
- 指定策略元素：動作、效果和主參與者
- 在政策中指定條件

AWS Control Tower 資源和操作

在 AWS Control Tower 中，主要資源是 landing zone。AWS Control Tower 也支援額外的資源類型、控制項，有時也稱為護欄。但是，對於 AWS Control Tower，您只能在現有 landing zone 的環境中管理控制。控制項可稱為子資源。

中的資源和子資源具 AWS 有與其關聯的唯一 Amazon 資源名稱 (ARN)，如以下範例所示。

AWS Control Tower 提供一組 API 操作，可與 AWS Control Tower 資源搭配使用。如需可用操作的清單，請參閱 AWS Control Tower API 參考中的 AWS Control Tower。

如需 AWS Control Tower 中 AWS CloudFormation 資源的詳細資訊，請參閱AWS CloudFormation 使用者指南。

關於資源擁有權

AWS 帳號擁有在帳號中建立的資源，無論是誰建立資源。具體而言，資源擁有者是驗證資源建立請求的主體實體 (即 AWS 帳戶 根使用者、IAM 身分中心使用者、IAM 使用者或 IAM 角色) 的 AWS 帳戶。下列範例說明其如何運作：

- 如果您使用 AWS 帳戶的 AWS 帳戶根使用者認證來設定 landing zone，則您的 AWS 帳戶就是資源的擁有者。
- 如果您在 AWS 帳戶中建立 IAM 使用者，並授與設定 landing zone 的權限給該使用者，只要使用者的帳戶符合先決條件，就可以設定 landing zone。不過，您的 AWS 帳號 (使用者所屬) 擁有 landing zone 域資源。
- 如果您在 AWS 帳戶中建立具有設定 landing zone 權限的 IAM 角色，則任何可以擔任該角色的人都可以設定 landing zone。您的 AWS 帳號 (角色所屬) 擁有 landing zone 域資源。

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**
>
> 本節討論在 AWS Control Tower 的內容中使用 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 使用者指南中的什麼是 IAM。如需有關 IAM 政策語法和說明的資訊，請參閱IAM 使用者指南中的 AWS IAM 政策參考。

附加至 IAM 身分的政策稱為以身分為基礎的政策 (IAM 政策)。連接到資源的政策稱為資源型政策。

> **Note**
>
> AWS Control Tower 僅支援以身分識別為基礎的政策 (IAM 政策)。

主題

關於以身分識別為基礎的政策 (IAM 政策)

您可以將政策連接到 IAM 身分。例如，您可以執行下列動作：

- 將許可政策附加到帳戶中的使用者或群組 — 若要授與使用者建立 AWS Control Tower 資源 (例如設定 landing zone) 的許可，您可以將許可政策附加到該使用者所屬的使用者或群組。
- 將許可政策連接至角色 (授予跨帳戶許可)：您可以將身分識別型許可政策連接至 IAM 角色，藉此授予跨帳戶許可。例如，一個 AWS 帳戶 (帳戶 A) 的系統管理員可以建立將跨帳戶權限授與另一個帳 AWS 戶 (帳戶 B) 的角色，或者管理員可以建立授與其他 AWS 服務權限的角色。
  1. 帳戶 A 管理員會建立 IAM 角色，並將許可政策附加至授與管理帳戶 A 中資源之權限的角色。
  2. 帳戶 A 系統管理員會將信任原則附加至角色。策略會將帳戶 B 識別為可擔任該角色的主參與者。
  3. 身為主體，帳戶 B 管理員可以授與帳戶 B 中的任何使用者擔任該角色的權限。透過假設該角色，帳戶 B 中的使用者可以建立或取得帳戶 A 中的資源存取權。
  4. 若要授與 AWS 服務擔任角色的能力 (權限)，您在信任原則中指定的主體可以是 AWS 服務。

建立角色並指派權限

角色和許可可讓您存取 AWS Control Tower 和其他 AWS 服務中的資源，包括以程式設計方式存取資源。

若要提供存取權，請新增權限至您的使用者、群組或角色：

- 使用者和群組位於 AWS IAM Identity Center：

  建立權限合集。請按照 AWS IAM Identity Center 使用者指南 中的 建立權限合集 說明進行操作。
- 透過身分提供者在 IAM 中管理的使用者：

  建立聯合身分的角色。請按照 IAM 使用者指南 的 為第三方身分提供者 (聯合) 建立角色 中的指示進行操作。
- IAM 使用者：

- 建立您的使用者可擔任的角色。請按照 IAM 使用者指南 的 為 IAM 使用者建立角色 中的指示進行操作。
- (不建議) 將政策直接附加至使用者，或將使用者新增至使用者群組。請遵循 IAM 使用者指南的新增許可到使用者 (主控台)中的指示。

如需使用 IAM 來委派許可的相關資訊，請參閱《IAM 使用者指南》中的存取管理。

> **Note**
>
> 設定 AWS Control Tower landing zone 時，您需要使用AdministratorAccess受管政策的使用者或角色。 （ARN：AW：IAM：：aws：策略/）AdministratorAccess

若要建立 AWS 服務 (IAM 主控台) 的角色

1. 登入 AWS Management Console 並開啟身分與存取權管理主控台，網址為 https://console.aws.amazon.com/iam/。
2. 在 IAM 主控台的導覽窗格中，選擇角色，然後選擇建立角色。
3. 對於 Trusted entity type (信任的實體類型)，請選擇 AWS 服務。
4. 對於服務或使用案例，請選擇服務，然後選擇使用案例。服務會定義使用案例，以包含服務所需的信任政策。
5. 選擇下一步。
6. 對於權限原則，選項取決於您選取的使用案例：
   - 如果服務定義了角色的權限，您就無法選取權限原則。
   - 從一組有限的權限原則中進行選取。
   - 從所有權限原則中選取。
   - 選取 [無權限原則]，建立角色後建立原則，然後將原則附加至角色。
7. (選用) 設定許可界限。這是進階功能，可用於服務角色，而不是服務連結的角色。
   a. 開啟 [設定權限界限] 區段，然後選擇 [使用權限界限] 控制最大角色權限。

      IAM 在您的帳戶中包含受 AWS 管政策和客戶管理政策的清單。

   b. 選取用於許可界限的政策。
8. 選擇下一步。

9. 對於角色名稱，選項取決於服務：

   - 如果服務定義了角色名稱，您就無法編輯角色名稱。
   - 如果服務定義了角色名稱的前置詞，您可以輸入選擇性的尾碼。
   - 如果服務未定義角色名稱，您可以命名角色。

   > **Important**
   >
   > 命名角色時，請注意下列事項：
   >
   > - 角色名稱在您的內部必須是唯一的 AWS 帳戶，並且不能根據大小寫將其唯一。
   >
   >   例如，請勿建立同時命名為**PRODROLE**和的角色**prodrole**。當角色名稱用於策略中或作為 ARN 的一部分時，角色名稱會區分大小寫，但是當主控台中的客戶 (例如在登入程序期間) 顯示角色名稱時，角色名稱不區分大小寫。
   > - 您無法在建立角色之後編輯該角色的名稱，因為其他實體可能會參照該角色。

10. (選擇性) 在說明中，輸入角色的說明。
11. (選擇性) 若要編輯角色的使用案例和權限，請在步驟 1：選取信任的實體或步驟 2：新增權限區段中，選擇編輯。
12. (選擇性) 若要協助識別、組織或搜尋角色，請將標籤新增為鍵值配對。如需有關在 IAM 中使用標籤的詳細資訊，請參閱《IAM 使用者指南》中的標記 IAM 資源。
13. 檢閱角色，然後選擇 Create role (建立角色)。

若要使用 JSON 政策編輯器來建立政策

1. 登入 AWS Management Console 並開啟身分與存取權管理主控台，網址為 https://console.aws.amazon.com/iam/。
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。
6. 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 Next (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. (選擇性) 在中建立或編輯原則時 AWS Management Console，您可以產生可在 AWS CloudFormation 範本中使用的 JSON 或 YAML 原則範本。

   若要這麼做，請在 [原則編輯器] 中選擇 [動作]，然後選擇 [產生 CloudFormation範本]。若要進一步了解 AWS CloudFormation，請參閱《AWS CloudFormation 使用指南》中的AWS Identity and Access Management 資源類型參考。
8. 將許可新增至政策後，請選擇下一步。
9. 在檢視與建立頁面上，為您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。
10. (選用) 藉由連接標籤作為鍵值組，將中繼資料新增至政策。如需有關在 IAM 中使用標籤的詳細資訊，請參閱《IAM 使用者指南》中的標記 IAM 資源。
11. 選擇 Create policy (建立政策) 儲存您的新政策。

若要使用視覺化編輯器來建立政策

1. 登入 AWS Management Console 並開啟身分與存取權管理主控台，網址為 https://console.aws.amazon.com/iam/。
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. 選擇 Create policy (建立政策)。
4. 在 [原則編輯器] 區段中，找到 [選取服務] 區段，然後選擇 AWS 服務。您可用上方的搜尋框來限制服務清單中的結果。您僅可以選擇一項視覺化編輯器許可區塊中的服務。若要授予存取一個以上服務的許可，請選擇新增更多許可，來新增多個許可區塊。
5. 在動作中，選擇要新增至政策的動作。您可採用以下方式來選擇動作：

   - 選取所有動作的核取方塊。
   - 選擇「新增動作」 以輸入特定動作的名稱。您可以使用萬用字元 (*) 來指定多個動作。

- 選取其中一個 Access level (存取層級) 群組，以選擇存取層級的所有動作 (例如，Read (讀取)、Write (寫入) 或 List (列出))。
- 展開各個 Access level (存取級別) 群組來選擇個別動作。

預設情況下，您建立的政策允許執行選擇的操作。若要拒絕選擇的動作，請選擇 Switch to deny permissions (切換為拒絕許可)。由於 IAM 會根據預設拒絕，作為安全最佳實務，我們建議您僅允許使用者所需的操作和資源的許可。建立 JSON 陳述式，只有在您想要覆寫另一個陳述式或原則所允許的權限時，才拒絕權限。我們建議您將拒絕許可數限制為最低，因為它們可能會增加解決許可問題的難度。

6. 對於 Resources (資源)，如果您在先前步驟中選取的服務和動作不支援選擇特定資源，則會允許所有資源，而且您無法編輯此區段。

   如果選擇一或多個支援資源等級許可的動作，視覺化編輯器將列出這些資源。然後，您可以展開 Resources (資源) 來為您的政策指定資源。

   您可採用以下方式來指定資源：

   - 選擇新增 ARN，可根據它們的 Amazon Resource Name (ARN) 來指定資源。您可以使用視覺化 ARN 編輯器或手動列出 ARN。如需 ARN 語法的詳細資訊，請參閱 IAM 使用者指南中的 Amazon 資源名稱 (ARN)。如需在政策`Resource`元素中使用 ARN 的詳細資訊，請參閱 IAM JSON 政策元素：IAM 使用者指南中的資源。
   - 選擇資源旁的此帳戶中的任何，將許可授予該類型的任何資源。
   - 選擇所有，可為服務選擇所有資源。

7. (選用) 選擇請求條件 - (選用)，為您正在建立的政策新增條件。條件可限制 JSON 政策陳述式的效果。例如，您可以指定只有在使用者的請求於特定時間範圍內發生時，使用者才能對資源執行動作。您也可以使用常用的條件來限制是否必須使用多重要素驗證 (MFA) 裝置來驗證使用者。或者，您可以要求請求必須源自於特定 IP 地址範圍。如需可在原則條件中使用之所有內容索引鍵的清單，請參閱服務授權參考中服AWS 務的動作、資源和條件金鑰。

   您可採用以下方式來選擇條件：

   - 使用核取方塊來選擇常用條件。
   - 選擇新增另一個條件，可指定其他條件。選擇條件的「條件索引鍵」、「限定元」 及「運算子」，然後輸入「值」。若要新增超過一個值，請選擇新增。您可以將這些值視為由邏輯OR運算符連接。完成時，請選擇新增條件。

若要新增超過一個條件，請再次選擇新增另一個條件。視需要重複執行。每項條件僅適用於這一個視覺化編輯器許可區塊。所有條件的許可區塊皆須為 true 才會被視為符合。換句話說，考慮要由邏輯AND運算符連接的條件。

如需有關「條件」元素的詳細資訊，請參閱 IAM JSON 政策元素：IAM 使用者指南中的條件。

8. 若要新增更多許可區塊，請選擇新增更多許可。針對每個區塊皆重複步驟 2 到 5。

> **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。

9. (選擇性) 在中建立或編輯原則時 AWS Management Console，您可以產生可在 AWS CloudFormation 範本中使用的 JSON 或 YAML 原則範本。

   若要這麼做，請在 [原則編輯器] 中選擇 [動作]，然後選擇 [產生 CloudFormation範本]。若要進一步了解 AWS CloudFormation，請參閱《AWS CloudFormation 使用指南》中的AWS Identity and Access Management 資源類型參考。

10. 將許可新增至政策後，請選擇下一步。
11. 在檢視與建立頁面上，為您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，可確認您已授予想要的許可。
12. (選用) 藉由連接標籤作為鍵值組，將中繼資料新增至政策。如需有關在 IAM 中使用標籤的詳細資訊，請參閱《IAM 使用者指南》中的標記 IAM 資源。
13. 選擇 Create policy (建立政策) 儲存您的新政策。

若要授與程式設計存取

如果使用者想要與 AWS 之外的 AWS Management Console. 授與程式設計存 AWS取權的方式取決於正在存取的使用者類型。

若要授與使用者程式設計存取權，請選擇下列其中一個選項。

哪個使用者需要程式設計存取權？	到	By
人力身分 (IAM Identity Center 中管理的使用者)	使用臨時登入資料來簽署對 AWS CLI、 AWS SDK 或 AWS API 的程式設計要求。	請依照您要使用的介面所提供的指示操作。 • 如需詳細資訊 AWS CLI，請參閱《使 AWS CLI 用AWS Command Line Interface者指南》 AWS IAM Identity Center中的〈配置使用〉。 • 如需 AWS SDK、工具和 AWS API，請參閱 AWS SDK 和工具參考指南中的 IAM 身分中心身分驗證。
IAM	使用臨時登入資料來簽署對 AWS CLI、 AWS SDK 或 AWS API 的程式設計要求。	遵循《IAM 使用者指南》中的〈將臨時登入資料搭配 AWS 資源使用〉中的指示
IAM	(不建議使用) 使用長期認證簽署對 AWS CLI、 AWS SDK 或 AWS API 的程式設計要求。	請依照您要使用的介面所提供的指示操作。 • 如需相關資訊 AWS CLI，請參閱使用指南中的使用 IAM 使用者登入資料進行驗證。AWS Command Line Interface • 對於 AWS SDK 和工具，請參閱 AWS SDK 和工具參考指南中的使用長期憑據進行身份驗證。 • 如需 AWS API，請參閱 IAM 使用者指南中的管理 IAM 使用者的存取金鑰。

防止攻擊者

如需在授與其他 AWS 服務主體權限時如何協助防範攻擊者的詳細資訊，請參閱角色信任關係的選用條件。透過將某些條件新增至您的原則，您可以協助防止特定類型的攻擊 (稱為混淆的副攻擊)，如果實體強制授權較多的實體執行動作 (例如跨服務模擬)，就會發生這種攻擊。如需有關策略條件的一般資訊，另請參閱在政策中指定條件。

如需將身分型政策與 AWS Control Tower 搭配使用的詳細資訊，請參閱。針對 AWS Control Tower 使用身分型政策 (IAM 政策)如需使用者、群組、角色和許可的詳細資訊，請參閱《IAM 使用者指南》中的身分 (使用者、群組和角色)。

資源型政策

其他服務 (例如 Amazon S3) 也支援以資源為基礎的許可政策。例如，您可以將政策連接至 S3 儲存貯體，以管理該儲存貯體的存取許可。AWS Control Tower 不支援以資源為基礎的政策。

指定策略元素：動作、效果和主參與者

您可以透過 AWS Control 塔主控台或 landing zone API 來設定和管理您的 landing zone。若要設定 landing zone，您必須是 IAM 政策中所定義具有管理許可的 IAM 使用者。

以下是您可以在策略中識別的最基本元素：

- 資源 – 在政策中，您可以使用 Amazon Resource Name (ARN) 來識別要套用政策的資源。如需詳細資訊，請參閱 AWS Control Tower 資源和操作。
- 動作：使用動作關鍵字識別您要允許或拒絕的資源操作。如需可執行之動作類型的相關資訊，請參閱 AWS Control Tower 定義的動作。
- 效果 - 您可以指定使用者要求特定動作時會有什麼效果；可為允許或拒絕。如果您未明確授予存取 (允許) 資源，則隱含地拒絕存取。您也可以明確拒絕資源存取，這樣做可確保使用者無法存取資源，即使不同政策授予存取也是一樣。
- 主體 — 在以身分為基礎的政策 (IAM 政策) 中，附加該政策的使用者是隱含的主體。對於資源型政策，您可以指定想要收到許可的使用者、帳戶、服務或其他實體 (僅適用於資源型政策)。AWS Control Tower 不支援以資源為基礎的政策。

如需進一步了解有關 IAM 政策語法和說明的詳細資訊，請參閱《IAM 使用者指南》 中的 AWS IAM 政策參考。

在政策中指定條件

當您授與許可時，您可以使用 IAM 政策語言指定政策生效時間的條件。例如，建議只在特定日期之後套用政策。如需使用政策語言指定條件的詳細資訊，請參閱IAM 使用者指南中的條件。

若要表示條件，您可以使用預先定義的條件索引鍵。AWS Control Tower 沒有特定條件金鑰。但是，您可以根據需要使用 AWS寬條件鍵。如需完整的 AWS全金鑰清單，請參閱《IAM 使用者指南》中的條件可用金鑰。

防止跨服務模擬

在中 AWS，跨服務模擬可能會導致混淆的副問題。當一個服務呼叫另一個服務時，如果某個服務操縱另一個服務，使用其權限以不允許的方式對客戶的資源採取行動，就會發生跨服務模擬。為了防止此攻擊，請 AWS 提供協助您保護資料的工具，以便只有具有合法權限的服務才能存取您帳戶中的資源。

我們建議您使用政策中的`aws:SourceArn`和`aws:SourceAccount`條件，以限制 AWS Control Tower 授予其他服務以存取資源的許可。

- 如`aws:SourceArn`果您只希望一個資源與跨服務存取相關聯，請使用此選項。
- 如`aws:SourceAccount`果您要允許該帳號中的任何資源與跨服務使用相關聯，請使用此選項。
- 如果`aws:SourceArn`值不包含帳戶 ID (例如 Amazon S3 儲存貯體的 ARN)，您必須使用這兩種條件來限制許可。
- 如果您同時同時使用這兩種條件，並且該`aws:SourceArn`值包含帳戶 ID，則該`aws:SourceAccount`值和帳戶在`aws:SourceArn`同一保單聲明中使用時必須顯示相同的帳戶 ID

如需詳細資訊和範例，請參閱 https://docs.aws.amazon.com/controltower/latest/userguide/conditions-for-role-trust.html。

針對 AWS Control Tower 使用身分型政策 (IAM 政策)

本主題提供以身分為基礎的政策範例，這些政策示範帳戶管理員如何將許可政策附加到 IAM 身分 (亦即使用者、群組和角色)，進而授予對 AWS Control Tower 資源執行操作的許可。

> **Important**
>
> 我們建議您先檢閱介紹性主題，其中說明可用於管理 AWS Control Tower 資源存取權的基本概念和選項。如需詳細資訊，請參閱 管理 AWS Control Tower 資源存取許可的概觀。

使用 AWS Control Tower 主控台所需的許可

當您設定 landing zone 時，AWS Control Tower 會自動建立三個角色。所有三個角色都需要允許主控台存取。AWS Control Tower 將許可分為三個角色，做為限制對最少動作和資源集的存取權限的最佳實務。

三個必要角色

- AWS ControlTowerAdmin 角色
- AWS ControlTowerStackSetRole
- AWS ControlTowerCloudTrailRole

我們建議您限制這些角色的角色信任原則的存取權。如需詳細資訊，請參閱角色信任關係的選用條件。

AWS ControlTowerAdmin 角色

這個角色為 AWS Control Tower 提供了維護 landing zone 域至關重要的基礎設施的存取權。該AWS ControlTowerAdmin角色需要附加的受管政策和 IAM 角色的角色信任政策。角色信任原則是以資源為基礎的原則，可指定哪些主體可以擔任該角色。

以下是此角色信任政策的範例程式碼片段：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "controltower.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
```

```
}
```

要從 AWS CLI 創建此角色，並將其放入名為的文件中`trust.json`，以下是 CLI 命令的示例：

```
aws iam create-role --role-name AWSControlTowerAdmin --path /service-role/ --assume-
role-policy-document file://trust.json
```

此角色需要兩個 IAM 政策。

1. 內嵌政策，例如：

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

2. 接下來的受管理策略，也就是`AWS ControlTowerServiceRolePolicy`.

AWS ControlTowerServiceRolePolicy

這AWS ControlTowerServiceRolePolicy是一項受 AWS管政策，用於定義建立和管理 AWS Control Tower 資源的許可，例如 AWS CloudFormation 堆疊集和堆疊執行個體、 AWS CloudTrail 日誌檔、AWS Control Tower 的組態彙總器，以及由 AWS Control Tower 管理的 AWS Organizations 帳戶和組織單位 (OU)。

此受管理策略的更新摘要列於表格中AWS Control Tower 的受管政策。

如需詳細資訊，請參閱 AWS 受管政策參考指南*AWSControlTowerServiceRolePolicy*中的。

受管理的策略名稱：`AWS ControlTowerServiceRolePolicy`

的 JSON 加工品如`AWS ControlTowerServiceRolePolicy`下：

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

```
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:CreateStackInstances",
                "cloudformation:CreateStackSet",
                "cloudformation:DeleteStack",
                "cloudformation:DeleteStackInstances",
                "cloudformation:DeleteStackSet",
                "cloudformation:DescribeStackInstance",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackSet",
                "cloudformation:DescribeStackSetOperation",
                "cloudformation:ListStackInstances",
                "cloudformation:UpdateStack",
                "cloudformation:UpdateStackInstances",
                "cloudformation:UpdateStackSet"
            ],
            "Resource": [
                "arn:aws:cloudformation:*:*:type/resource/AWS-IAM-Role"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "account:EnableRegion",
                "account:ListRegions",
                "account:GetRegionOptStatus"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:CreateStackInstances",
                "cloudformation:CreateStackSet",
                "cloudformation:DeleteStack",
                "cloudformation:DeleteStackInstances",
                "cloudformation:DeleteStackSet",
                "cloudformation:DescribeStackInstance",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackSet",
                "cloudformation:DescribeStackSetOperation",
```

```
                "cloudformation:GetTemplate",
                "cloudformation:ListStackInstances",
                "cloudformation:UpdateStack",
                "cloudformation:UpdateStackInstances",
                "cloudformation:UpdateStackSet"
            ],
            "Resource": [
                "arn:aws:cloudformation:*:*:stack/AWSControlTower*/*",
                "arn:aws:cloudformation:*:*:stack/StackSet-AWSControlTower*/*",
                "arn:aws:cloudformation:*:*:stackset/AWSControlTower*:*",
                "arn:aws:cloudformation:*:*:stackset-target/AWSControlTower*/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:CreateTrail",
                "cloudtrail:DeleteTrail",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:StartLogging",
                "cloudtrail:StopLogging",
                "cloudtrail:UpdateTrail",
                "cloudtrail:PutEventSelectors",
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:PutRetentionPolicy"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
                "arn:aws:cloudtrail:*:*:trail/aws-controltower*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::aws-controltower*/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/AWSControlTowerExecution",
                "arn:aws:iam::*:role/AWSControlTowerBlueprintAccess"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "ec2:DescribeAvailabilityZones",
                "iam:ListRoles",
                "logs:CreateLogGroup",
                "logs:DescribeLogGroups",
                "organizations:CreateAccount",
                "organizations:DescribeAccount",
                "organizations:DescribeCreateAccountStatus",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribePolicy",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListChildren",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListPoliciesForTarget",
                "organizations:ListTargetsForPolicy",
                "organizations:ListRoots",
                "organizations:MoveAccount",
                "servicecatalog:AssociatePrincipalWithPortfolio"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetRole",
                "iam:GetUser",
                "iam:ListAttachedRolePolicies",
                "iam:GetRolePolicy"
            ],
            "Resource": "*"
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/service-role/AWSControlTowerStackSetRole",
                "arn:aws:iam::*:role/service-role/AWSControlTowerCloudTrailRole",
                "arn:aws:iam::*:role/service-role/
AWSControlTowerConfigAggregatorRoleForOrganizations"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "config:DeleteConfigurationAggregator",
                "config:PutConfigurationAggregator",
                "config:TagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/aws-control-tower": "managed-by-control-tower"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "organizations:ServicePrincipal": [
                        "config.amazonaws.com",
                        "cloudtrail.amazonaws.com"
                    ]
                }
            }
        },
        {
```

```
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "cloudtrail.amazonaws.com"
                }
            }
        }
    ]
}
```

角色信任政策：

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "controltower.amazonaws.com"
         ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

內嵌政策是AWSControlTowerAdminPolicy：

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

AWS ControlTowerStackSetRole

AWS CloudFormation 擔任此角色在 AWS Control Tower 建立的帳戶中部署堆疊集。內嵌政策

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/AWSControlTowerExecution"
            ],
            "Effect": "Allow"
        }
    ]
}
```

信任政策

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudformation.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

AWS ControlTowerCloudTrailRole

AWS Control Tower 可 CloudTrail 作為最佳實務，並將此角色提供給 CloudTrail。 CloudTrail假設此角色可建立和發佈 CloudTrail 記錄檔。內嵌政策

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

```
        {
            "Action": "logs:CreateLogStream",
            "Resource": "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
            "Effect": "Allow"
        },
        {
            "Action": "logs:PutLogEvents",
            "Resource": "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
            "Effect": "Allow"
        }
    ]
}
```

信任政策

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

AWSControlTowerBlueprintAccess 角色需求

AWS Control Tower 要求您在相同組織內的指定藍圖中樞帳戶中建立`AWSControlTowerBlueprintAccess`角色。

Role name (角色名稱)

角色名稱必須是`AWSControlTowerBlueprintAccess`。

角色信任原則

角色必須設定為信任下列主參與者：

- 在管理帳戶中使用 AWS Control Tower 的主體。
- 管理帳戶中的`AWSControlTowerAdmin`角色。

下列範例顯示最低權限信任原則。當您制定自己的政策時，請使*YourManagementAccountId*用 AWS Control Tower 管理帳戶的實際會員 ID 取代該術語，並以管理帳戶*YourControlTowerUserRole*的 IAM 角色識別碼取代該術語。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::YourManagementAccountId:role/service-role/
AWSControlTowerAdmin",

 "arn:aws:iam::YourManagementAccountId:role/YourControlTowerUserRole"
                ]
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```

角色權限

您必須將受管理的策略附加AWSServiceCatalogAdminFullAccess至角色。

AWSServiceRoleForAWSControlTower

這個角色可讓 AWS Control Tower 存取日誌存取帳戶、稽核帳戶和成員帳戶，以執行維護 landing zone 域至關重要的操作，例如通知您資源漂移。

該AWSServiceRoleForAWSControlTower角色需要附加的受管政策和 IAM 角色的角色信任政策。

此角色的受管理策略：AWSControlTowerAccountServiceRolePolicy

角色信任政策：

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

```
            "Principal": {
                "Service": "controltower.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

AWSControlTowerAccountServiceRolePolicy

這項 AWS受管政策可讓 AWS Control Tower 呼叫代表您 AWS 提供自動化帳戶組態和集中控管的服務。

該政策包含 AWS Control Tower 的最低許可，可針對屬於 Security Hub 服務管理標準：AWS Control Twer 的一部分的 Security Hub 控制項所管理的資源實作 AWS Security Hub 發現項目轉送，並防止變更限制管理客戶帳戶的能力。它是後台 AWS Security Hub 漂移檢測過程的一部分，不是由客戶直接啟動的。

該政策授予在每個成員帳戶中建立 Amazon EventBridge 規則的許可，特別是針對 Security Hub 控制項，而且這些規則必須指定精確的規則 EventPattern。此外，規則只能在由我們的服務主體管理的規則上運作。

服務主體：`controltower.amazonaws.com`

的 JSON 加工品如`AWSControlTowerAccountServiceRolePolicy`下：

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
  //For creating the managed rule
   "Sid": "AllowPutRuleOnSpecificSourcesAndDetailTypes",
   "Effect": "Allow",
   "Action": "events:PutRule",
   "Resource": "arn:aws:events:*:*:rule/*ControlTower*",
   "Condition": {
    "ForAnyValue:StringEquals": {
     "events:source": "aws.securityhub"
    },
    "Null": {
     "events:detail-type": "false"
    },
    "StringEquals": {
```

```
      "events:ManagedBy": "controltower.amazonaws.com",
      "events:detail-type": "Security Hub Findings - Imported"
     }
    }
   },
   // Other operations to manage the managed rule
   {
    "Sid": "AllowOtherOperationsOnRulesManagedByControlTower",
    "Effect": "Allow",
    "Action": [
     "events:DeleteRule",
     "events:EnableRule",
     "events:DisableRule",
     "events:PutTargets",
     "events:RemoveTargets"
    ],
    "Resource": "arn:aws:events:*:*:rule/*ControlTower*",
    "Condition": {
     "StringEquals": {
      "events:ManagedBy": "controltower.amazonaws.com"
     }
    }
   },
   // More managed rule permissions
   {
    "Sid": "AllowDescribeOperationsOnRulesManagedByControlTower",
    "Effect": "Allow",
    "Action": [
     "events:DescribeRule",
     "events:ListTargetsByRule"
    ],
    "Resource": "arn:aws:events:*:*:rule/*ControlTower*"
   },
   // Add permission to publish the security notifications to SNS
   {
    "Sid": "AllowControlTowerToPublishSecurityNotifications",
    "Effect": "Allow",
    "Action": "sns:publish",
    "Resource": "arn:aws:sns:*:*:aws-controltower-AggregateSecurityNotifications",
    "Condition": {
     "StringEquals": {
      "aws:PrincipalAccount": "${aws:ResourceAccount}"
     }
    }
```

```
  },
  // For drift verification
  {
   "Sid": "AllowActionsForSecurityHubIntegration",
   "Effect": "Allow",
   "Action": [
    "securityhub:DescribeStandardsControls",
    "securityhub:GetEnabledStandards"
   ],
   "Resource": "arn:aws:securityhub:*:*:hub/default"
  }
 ]
}
```

此受管理策略的更新摘要列於表格中AWS Control Tower 的受管政策。

AWS Control Tower 的受管政策

AWS 透過提供由建立和管理的獨立 IAM 政策來解決許多常見使用案例 AWS。受管政策授與常見使用案例中必要的許可，讓您免於查詢需要哪些許可。如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

變更	描述	日期
AWSControlTowerAccountServiceRolePolicy— 新政策	AWS Control Tower 新增了一個新的服務連結角色，可讓 AWS Control Tower 建立和管理事件規則，並根據這些規則管理與 Security Hub 相關控制的漂移偵測。 當這些資源與屬於 Security Hub 服務管理標準：AWS Control Tower 一部分的 Security Hub 控制項相關時，客戶可以在主控台中檢視漂移的資源，這些資源需要進行此變更。	2023 年 5 月 22 日

變更	描述	日期
AWS ControlTowerServiceRolePolicy – 更新現有政策	AWS Control Tower 新增了允許 AWS Control Tower 對 AWS 帳戶管理服務實作的`EnableRegion` `ListRegions` 、和 `GetRegionOptStatus` API 撥打電話的新許 AWS 區域 可，讓 landing zone 中的客戶帳戶 (管理帳戶、日誌存檔帳戶、稽核帳戶、OU 成員帳戶) 可以選擇加入。 需要進行此變更，以便客戶可以選擇將 AWS Control Tower 的區域管理擴展到選擇加入的區域。	2023 年 4 月 6 日

變更	描述	日期
AWS ControlTowerServiceRolePolicy – 更新現有政策	AWS Control Tower 新增了新許可，允許 AWS Control Tower 擔任藍圖 (Hub) 帳戶中的`AWSControlTowerBlueprintAccess` 角色，該帳戶是組織中的專用帳戶，其中包含儲存在一或多個 Service Catalog 產品中的預先定義藍圖。AWS Control Tower 擔任執行三項任務的`AWSControlTowerBlueprintAccess` 角色：建立 Service Catalog 產品組合、新增要求的藍圖產品，以及在帳戶佈建時將產品組合共用至要求的成員帳戶。 需要進行此變更，以便客戶可以透過 AWS Control Tower Account Factory 佈建自訂帳戶。	2022 年 10 月 28 日
AWS ControlTowerServiceRolePolicy – 更新現有政策	AWS Control Tower 新增了新的許可，允許客戶設定組織層級 AWS CloudTrail 追蹤，從 3.0 版起。 組織型 CloudTrail 功能要求客戶啟用該 CloudTrail 服務的受信任存取權，而 IAM 使用者或角色必須具有在管理帳戶中建立組織層級追蹤的權限。	2022 年 6 月 20 日

變更	描述	日期
AWS ControlTowerServiceRolePolicy – 更新現有政策	AWS Control Tower 新增了允許客戶使用 KMS 金鑰加密的新許可。 KMS 功能可讓客戶提供自己的 KMS 金鑰來加密其 CloudTrail 記錄。客戶也可以在 landing zone 更新或修復期間變更 KMS 金鑰。更新 KMS 金鑰時，AWS CloudFormation 需要呼叫 AWS CloudTrail `PutEventSelector` API 的權限。政策的變更是允許AWS ControlTowerAdmin角色呼叫 AWS CloudTrail `PutEventSelector` API。	2021 年 7 月 28 日
AWS Control Tower 開始追蹤變更	AWS Control Tower 開始追蹤其 AWS 受管政策的變更。	2021 年 5 月 27 日

AWS Control Tower 中的安全性

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 與您之間共同的責任。共同責任模型將此描述為雲端本身的安全和雲端內部的安全：

- 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。第三方稽核人員定期檢測及驗證安全的效率也是我們 AWS 合規計劃的一部分。要了解適用於 AWS Control Tower 的合規計劃，請參閱合規計劃的範圍AWS 服務。
- 雲端安全性 — 您的責任取決於您使用的 AWS 服務。您也必須對其他因素負責，包括資料的敏感度、您組織的需求和適用的法律及法規。

本文件可協助您了解如何在使用 AWS Control Tower 時套用共同的責任模型。以下主題說明如何設定 AWS Control Tower 以符合安全和合規目標。您也會學到如何使用其他可 AWS 協助您監控和保護 AWS Control Tower 資源的服務。

AWS Control Tower 的資料保護

AWS 共同責任模型適用於 AWS Control Tower 中的資料保護。如此模型中所述， AWS 負責保護執行所有 AWS 雲端. 您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務 的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱資料隱私權常見問答集。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 AWS 共同的責任模型和 GDPR 部落格文章。

基於資料保護目的，我們建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 登入資料並設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源進行通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用設定 API 和使用者活動記錄 AWS CloudTrail。
- 使用 AWS 加密解決方案以及其中的所有默認安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在透過命令列介面或 API 存取時需要經 AWS 過 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-2 概觀。

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

> **Note**
>
> 當您設定 landing zone AWS CloudTrail 時，AWS Control Tower 會自動處理使用者活動記錄。

如需關於資料保護的詳細資訊，請參閱 AWS 安全部落格上的 AWS 共同責任模型和歐盟《一般資料保護規範》(GDPR) 部落格文章。AWS Control Tower 提供下列選項，您可以使用這些選項來協助保護 landing zone 域中的內容：

主題

- 靜態加密
- 傳輸中加密
- 限制存取內容

靜態加密

AWS Control Tower 使用 Amazon S3 儲存貯體和 Amazon DynamoDB 資料庫，這些資料庫透過使用 Amazon S3 受管金鑰 (SSE-S3) 支援您的 landing zone 進行加密。當您設定 landing zone 時，依預設會設定此加密。或者，您可以將 landing zone 域設定為使用 KMS 加密金鑰來加密資源。您也可以為您在 landing zone 中使用的服務建立靜態加密，以便為支援該服務的服務建立靜態加密。如需詳細資訊，請參閱該服務線上文件的安全性章節。

傳輸中加密

AWS Control Tower 使用傳輸層安全性 (TLS) 和用戶端加密進行傳輸中的加密，以支援您的 landing zone。此外，存取 AWS Control Tower 需要使用主控台，主控台只能透過 HTTPS 端點存取。當您設定 landing zone 時，依預設會設定此加密。

限制存取內容

做為最佳實務，您應該限制存取適當的使用者子集。使用 AWS Control Tower，您可以確保中央雲端管理員和最終使用者擁有正確的 IAM 許可，或者如果是 IAM 身分中心使用者，他們位於正確的群組中，即可執行此操作。

- 如需 IAM 實體角色和政策的詳細資訊，請參閱 IAM 使用者指南。
- 如需設定 landing zone 域時建立的 IAM 身分中心群組的詳細資訊，請參閱適用於 AWS Control Tower 的 IAM 身分中心群組。

AWS Control Tower 的合規驗證

AWS Control Tower 是架構良好的服務，可協助您的組織透過控制和最佳實務滿足您的合規需求。此外，協力廠商稽核人員會評估您可在 landing zone 中使用的多項服務的安全性與合規性，做為多項 AWS 合規計畫的一部分。這些計劃包括 SOC、PCI、FedRAMP、HIPAA 等等。

如需特定合規方案範圍內的 AWS 服務清單，請參閱合規方案範圍內的AWS 服務。如需一般資訊，請參閱 AWS 合規計劃。

您可以使用下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱AWS Artifact 使用指南中的在 AWS Artifact 中下載報表。

使用 AWS Control Tower 時的合規責任取決於資料的敏感度、公司的合規目標以及適用的法律和法規。 AWS 提供下列資源以協助遵循法規：

- 安全性與合規性快速入門指南 — 這些部署指南討論架構考量，並提供在上部署以安全性和法規遵循為重點的基準環境的步驟。 AWS
- 在 Amazon Web Services 上架構 HIPAA 安全性與合規性 — 本白皮書說明公司如何使用建立符合 HIPAA 標準的應 AWS 用程式。
- AWS 合規資源 — 此工作簿和指南集合可能適用於您的產業和所在地。
- AWS Config— 此 AWS 服務評估您的資源配置是否符合內部實踐，行業準則和法規。
- AWS Security Hub— 此 AWS 服務提供安全狀態的全面檢視，協助您檢查您 AWS 是否符合安全性產業標準和最佳做法。

AWS Control Tower 的彈性

AWS 全球基礎架構是圍繞區 AWS 域和可用區域建立的。

AWS 區域提供多個實體分離和隔離的可用區域，這些可用區域透過低延遲、高輸送量和高度備援的網路進行連接。可用區域允許您設計與操作在可用區域之間自動容錯移轉的應用程式和資料庫，而不會發生中斷。可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS Control Tower 可供使用的 AWS 區域 清單，請參閱AWS 區域如何與 AWS Control Tower 搭配使用。

您的居住地 AWS 區定義為設定 landing zone 的地區。

如需區域和可用區域的相關 AWS 資訊，請參閱AWS 全域基礎結構。

AWS Control Tower 中的基礎設施安全

AWS Control Tower 受到 Amazon Web Services：安 AWS 全程序概觀白皮書中所述的全球網路安全程序保護。

您可以使用 AWS 已發佈的 API 呼叫，透過網路存取 landing zone 域內的 AWS 服務和資源。我們需要傳輸層安全性 (TLS) 1.2，並建議使用傳輸層安全性 (TLS) 1.3 或更新版本。用戶端也必須支援具備完美轉送私密 (PFS) 的密碼套件，例如臨時 Diffie-Hellman (DHE) 或橢圓曲線臨時 Diffie-Hellman (ECDHE)。現代系統 (如 Java 7 和更新版本) 大多會支援這些模式。

此外，請求必須使用存取金鑰 ID 和與 IAM 主體相關聯的私密存取金鑰來簽署。或者，您可以透過 AWS Security Token Service (AWS STS) 來產生暫時安全憑證來簽署請求。

您可以設定安全群組，為 AWS Control Tower landing zone 工作負載提供額外的網路基礎設施安全性。如需更多詳細資訊，請參閱 逐步解說：使用 AWS Firewall Manager 在 AWS Control Tower 中設定安全群組。

AWS Control Tower 中的記錄和監控

監控可讓您針對潛在的事件做規劃並加以回應。監視活動的結果儲存在記錄檔中。因此，記錄和監控是密切相關的概念，它們是 AWS Control Tower 架構良好本質的重要組成部分。

當您設定 landing zone 時，其中一個建立的共用帳戶就是記錄封存帳戶。它致力於集中收集所有日誌，包括所有共享帳戶和成員帳戶的日誌。日誌檔案存放在 Amazon S3 儲存貯體中。這些日誌檔案可讓管理員和稽核員檢閱已發生的動作和事件。

最佳作法是，您應該將 AWS 設定的所有部分的監視資料收集到記錄檔中，以便在發生多點失敗時更輕鬆地偵錯。 AWS 提供數種工具，用於監控您在 landing zone 的資源和活動。

例如，系統會持續監控控制項的狀態。您可以在 AWS Control 塔主控台中一目了然地查看其狀態，或透過 AWS Control Tower API 以程式設計方式查看。您在 Account Factory 中佈建之帳戶的健全狀況和狀態也會持續監控。

從「活動」頁面檢視記錄的動作

在 AWS Control Tower 主控台中，活動頁面提供 AWS Control Tower 管理帳戶動作的概觀。若要導覽至 AWS Control Tower 活動頁面，請從左側導覽選取活動。

活動頁面中顯示的活動與 AWS Control Tower AWS CloudTrail 事件日誌中報告的活動相同，但會以表格格式顯示。若要深入瞭解特定活動，請從表格中選取活動，然後選擇 View details (檢視詳細資料)。

您可以檢視記錄封存檔案中的成員帳號動作和事件。

以下各節將詳細說明 AWS Control Tower 中的監控和記錄：

主題

- 用於監控的集成工具
- 使用記錄 AWS Control Tower 動作 AWS CloudTrail
- AWS Control Tower 的生命週期事件
- 使用使用 AWS 者通知 AWS Control Tower

關於 AWS Control Tower 的登入

AWS Control Tower 透過與和的整合，自動完成動作和事件的記錄 AWS Config， AWS CloudTrail 並將其記錄在中 CloudWatch。所有動作都會記錄下來，包括來自 AWS Control Tower 管理帳戶和組織

成員帳戶的動作。您可以在主控台的 [活動] 頁面上檢視管理帳戶動作和事件。您可以檢視記錄封存檔案中的成員帳號動作和事件。

組織層級的追蹤

當您設定 landing zone 域時，AWS Control Tower 會設定新的 CloudTrail 追蹤。這是組織層級追蹤，也就是說，它會記錄組織中管理帳戶和所有成員帳戶的所有事件。此功能依賴受信任的存取權限授予管理帳戶在每個成員帳戶上建立追蹤的權限。

如需 AWS Control Tower 和 CloudTrail 組織追蹤的詳細資訊，請參閱為組織建立追蹤。

> **Note**
>
> 在 landing zone 3.0 版之前發行的 AWS Control Tower 中，AWS Control Tower 會在每個帳戶中建立一個成員帳戶追蹤。當您更新至 3.0 版時，您的 CloudTrail 追蹤就會變成組織追蹤。若要取得在系統線之間移動時的最佳作法，請參閱《CloudTrail 使用指南》中有關變更系統線的最佳

當您在 AWS Control Tower 註冊帳戶時，您的帳戶受 AWS Control Tower 組織的 AWS CloudTrail 追蹤管理。如果該帳戶中現有的 CloudTrail 追蹤部署，您可能會看到重複的費用，除非您在 AWS Control Tower 註冊帳戶之前刪除該帳戶的現有追蹤。

> **Note**
>
> 當您更新至 landing zone 3.0 版時，AWS Control Tower 會代表您刪除註冊帳戶中的帳戶層級追蹤 (該 AWS Control Tower 已建立)。您現有的帳戶層級日誌檔會保留在其 Amazon S3 儲存貯體中。

稽核帳戶中的 Amazon S3 儲存貯體政策

在 AWS Control Tower 中，只有當請求來自您的組織或組織單位 (OU) 時， AWS 服務才能存取您的資源。必須符合任何寫入權限的`aws:SourceOrgID`條件。

您可以使用`aws:SourceOrgID`條件金鑰，並在 Amazon S3 儲存貯體政策的條件元素中將值設定為組織 ID。這種情況可確保 CloudTrail 只能代表組織內的帳戶將日誌寫入 S3 儲存貯體；它可防止組織外部的 CloudTrail 日誌寫入 AWS Control Tower S3 儲存貯體。

此原則不會影響現有工作負載的功能。該策略顯示在以下範例中。

```
S3AuditBucketPolicy:
    Type: AWS::S3::BucketPolicy
    Properties:
      Bucket: !Ref S3AuditBucket
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Sid: AllowSSLRequestsOnly
            Effect: Deny
            Principal: '*'
            Action: s3:*
            Resource:
             - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}"
             - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/*"
            Condition:
              Bool:
                aws:SecureTransport: false
          - Sid: AWSBucketPermissionsCheck
            Effect: Allow
            Principal:
              Service:
                - cloudtrail.amazonaws.com
                - config.amazonaws.com
            Action: s3:GetBucketAcl
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}"
          - Sid: AWSConfigBucketExistenceCheck
            Effect: Allow
            Principal:
              Service:
                - cloudtrail.amazonaws.com
                - config.amazonaws.com
            Action: s3:ListBucket
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}"
          - Sid: AWSBucketDeliveryForConfig
            Effect: Allow
            Principal:
              Service:
                - config.amazonaws.com
            Action: s3:PutObject
            Resource:
```

```
              - Fn::Join:
                  - ""
                  -
                    - !Sub "arn:${AWS::Partition}:s3:::"
                    - !Ref "S3AuditBucket"
                    - !Sub "/${AWSLogsS3KeyPrefix}/AWSLogs/*/*"
            Condition:
              StringEquals:
                aws:SourceOrgID: !Ref OrganizationId
          - Sid: AWSBucketDeliveryForOrganizationTrail
            Effect: Allow
            Principal:
              Service:
                - cloudtrail.amazonaws.com
            Action: s3:PutObject
            Resource: !If [IsAccountLevelBucketPermissionRequiredForCloudTrail,
                [!Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/
${AWSLogsS3KeyPrefix}/AWSLogs/${Namespace}/*", !Sub "arn:${AWS::Partition}:s3:::
${S3AuditBucket}/${AWSLogsS3KeyPrefix}/AWSLogs/${OrganizationId}/*"],
                !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/
${AWSLogsS3KeyPrefix}/AWSLogs/*/*"]
            Condition:
              StringEquals:
            aws:SourceOrgID: !Ref OrganizationId
```

如需有關此條件金鑰的詳細資訊，請參閱 IAM 文件和標題為「針對存取資源的 AWS 服務使用可擴展控制項」的 IAM 部落格文章。

用於監控的集成工具

監控是維護 AWS Control Tower 和其他 AWS 解決方案的可靠性、可用性和效能的重要組成部分。AWS 提供下列監控工具來觀看 AWS Control Tower、在發生錯誤時報告，並在適當時採取自動動作：

- Amazon 會即時 CloudWatch監控您的 AWS 資源和執行 AWS 的應用程式。您可以收集和追蹤指標、建立自訂儀板表，以及設定警示，在特定指標達到您指定的閾值時通知您或採取動作。例如，您可以 CloudWatch 追蹤 Amazon EC2 執行個體的 CPU 使用率或其他指標，並在需要時自動啟動新執行個體。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南。
- Amazon E CloudWatch vents 提供近乎即時的系統事件串流，用於描述 AWS 資源變更。CloudWatch 事件可啟用自動化事件驅動計算，因為您可以撰寫規則來監視特定事件，並在其他 AWS 服務發生時觸發自動化動作。如需詳細資訊，請參閱 Amazon CloudWatch 事件使用者指南。

- Amazon CloudWatch 日誌可讓您從 Amazon EC2 執行個體和其他來源監控 CloudTrail、存放和存取日誌檔。 CloudWatch 記錄檔可以監控記錄檔中的資訊，並在符合特定臨界值時通知您。您也可以將日誌資料存檔在高耐用性的儲存空間。如需詳細資訊，請參閱 Amazon CloudWatch 日誌使用者指南。
- AWS CloudTrail擷取您帳戶或代表您 AWS 帳戶發出的 API 呼叫和相關事件，並將日誌檔傳送到您指定的 Amazon S3 儲存貯體。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。

提示：您可以透過 CloudWatch 記錄和日 CloudWatch 誌深入解析來檢視和查詢帳戶的 CloudTrail 活動。此活動包括 AWS Control Tower 生命週期事件。 CloudWatch日誌的功能使您可以執行比通常能夠使用 CloudTrail的更精細和更精確的查詢。

如需更多詳細資訊，請參閱 使用記錄 AWS Control Tower 動作 AWS CloudTrail。

使用記錄 AWS Control Tower 動作 AWS CloudTrail

AWS Control Tower 與 AWS Control Tower 中的使用者 AWS CloudTrail、角色或服務所採取的動作記錄提供 AWS 服務整合的服務。 CloudTrail 以事件形式擷取 AWS Control Tower 的動作。如果您建立追蹤，您可以啟用持續交付 CloudTrail 事件到 Amazon S3 儲存貯體，包括 AWS Control Tower 的事件。

如果您未設定追蹤，您仍然可以在 [事件歷程記錄] 中檢視 CloudTrail 主控台中最近的事件。使用收集的資訊 CloudTrail，您可以判斷向 AWS Control Tower 發出的請求、提出請求的 IP 地址、提出請求的人員、提出請求的時間以及其他詳細資訊。

若要進一步了解 CloudTrail，包括如何設定和啟用它，請參閱AWS CloudTrail 使用者指南。

AWS Control Tower 資訊，請參閱 CloudTrail

CloudTrail 在您創建 AWS 帳戶時，您的帳戶已啟用。當 AWS Control Tower 中發生受支援的事件活動時，該活動會與 CloudTrail 事件歷史記錄中的其他 AWS 服務事件一起記錄在事件中。您可以在帳戶中查看，搜索和下載最近的事 AWS 件。如需詳細資訊，請參閱檢視具有事 CloudTrail 件記錄的事件。

> **Note**
>
> 在 landing zone 3.0 版之前發行的 AWS Control Tower 中，AWS Control Tower 建立了一個成員帳戶追蹤。當您更新至 3.0 版時，您的 CloudTrail 追蹤就會更新為組織追蹤。如需在追蹤之間移動時的最佳作法，請參閱《 CloudTrail 使用指南》中的「建立組織追蹤」。

建議：建立追蹤

如需 AWS 帳戶中持續的事件記錄 (包括 AWS Control Tower 的事件)，請建立追蹤。追蹤可 CloudTrail 將日誌檔交付到 Amazon S3 儲存貯體。根據預設，當您在主控台建立線索時，線索會套用到所有 AWS 區域。追蹤記錄來自 AWS 分區中所有區域的事件，並將日誌檔傳送到您指定的 Amazon S3 儲存貯體。此外，您還可以設定其他 AWS 服務，以進一步分析 CloudTrail 記錄中收集的事件資料並採取行動。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- 準備建立系統線
- 管理 CloudTrail 成本
- CloudTrail 支援的服務與整合
- 設定的 Amazon SNS 通知 CloudTrail
- 從多個區域接收 CloudTrail 記錄檔並從多個帳戶接收 CloudTrail記錄檔

AWS Control Tower 會將下列動作記錄為日 CloudTrail 誌檔中的事件：

公用 API

- DisableControl
- EnableControl
- GetControlOperation
- ListEnabledControls

其他 API

- SetupLandingZone
- UpdateAccountFactoryConfig
- ManageOrganizationalUnit
- CreateManagedAccount
- EnableGuardrail
- GetLandingZoneStatus
- GetHomeRegion
- ListManagedAccounts

- DescribeManagedAccount
- DescribeAccountFactoryConfig
- DescribeGuardrailForTarget
- DescribeManagedOrganizationalUnit
- ListEnabledGuardrails
- ListGuardrailViolations
- ListGuardrails
- ListGuardrailsForTarget
- ListManagedAccountsForGuardrail
- ListManagedAccountsForParent
- ListManagedOrganizationalUnits
- ListManagedOrganizationalUnitsForGuardrail
- GetGuardrailComplianceStatus
- DescribeGuardrail
- ListDirectoryGroups
- DescribeSingleSignOn
- DescribeCoreService
- GetAvailableUpdates

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

- 要求是使用根使用者登入資料還是 AWS Identity and Access Management (IAM) 使用者登入資料提出。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 請求是否由其他 AWS 服務提出。
- 請求是因為訪問被拒絕而被拒絕還是成功處理。

如需詳細資訊，請參閱 CloudTrail 使用者身分元素。

範例：AWS Control Tower 日誌檔項目

追蹤是一種組態，可讓事件以日誌檔的形式傳遞到您指定的 Amazon S3 儲存貯體。 CloudTrail 記錄檔包含一或多個記錄項目。事件代表來自任何來源的單一請求，包括有關請求的操作，動作的日期和時間，請求參數等信息。 CloudTrail 事件不會以任何特定順序出現在記錄檔中。

下列範例顯示一個記 CloudTrail 錄項目，其中顯示 SetupLandingZone AWS Control Tower 事件的典型日誌檔項目結構，包括啟動動作的使用者身分記錄。

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE:backend-test-assume-role-session",
    "arn": "arn:aws:sts::76543EXAMPLE;:assumed-role/AWSControlTowerTestAdmin/backend-
test-assume-role-session",
    "accountId": "76543EXAMPLE",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-11-20T19:36:11Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::AKIAIOSFODNN7EXAMPLE:role/AWSControlTowerTestAdmin",
        "accountId": "AIDACKCEVSQ6C2EXAMPLE",
        "userName": "AWSControlTowerTestAdmin"
      }
    }
  },
  "eventTime": "2018-11-20T19:36:15Z",
  "eventSource": "controltower.amazonaws.com",
  "eventName": "SetupLandingZone",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "Coral/Netty4",
  "errorCode": "InvalidParametersException",
  "errorMessage": "Home region EU_CENTRAL_1 is unsupported",
  "requestParameters": {
    "homeRegion": "EU_CENTRAL_1",
    "logAccountEmail": "HIDDEN_DUE_TO_SECURITY_REASONS",
```

```
    "sharedServiceAccountEmail": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "securityAccountEmail": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "securityNotificationEmail": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "responseElements": null,
  "requestID": "96f47b68-ed5f-4268-931c-807cd1f89a96",
  "eventID": "4ef5cf08-39e5-4fdf-9ea2-b07ced506851",
  "eventType": "AwsApiCall",
  "recipientAccountId": "76543EXAMPLE"
}
```

監視資源變更 AWS Config

AWS Control Tower 可 AWS Config 在所有註冊帳戶上啟用，以便透過偵探控制監控合規、記錄資源變更，以及將資源變更日誌傳遞到日誌存檔帳戶。

如果您的 landing zone 域版本早於 3.0：對於您註冊的帳號，會 AWS Config 記錄帳戶運作所有區域的資源變更。每項變更都會建模為組態項目 (CI)，其中包含資源識別元、區域、記錄每個變更的日期，以及變更是否與已知資源或新發現的資源有關。

如果您的 landing zone 域版本為 3.0 或更新版本：AWS Control Tower 會將全球資源 (例如 IAM 使用者、群組、角色和客戶受管政策) 的記錄限制在您的本地區域。全域資源變更的副本不會儲存在每個區域中。資源記錄的這種限制符合 AWS Config 最佳做法。 AWS Config 文件中提供全域資源的完整清單。

- 若要深入瞭解 AWS Config，請參閱AWS Config 運作方式。
- 如需 AWS Config 可支援的資源清單，請參閱支援的資源類型。
- 要了解如何在 AWS Control Tall 環境中自訂資源追蹤，請參閱標題為 AWS Control Tower 中的自訂 AWS Config 資源追蹤的部落格文章。

AWS Control Tower 會在所有註冊帳戶中設定 AWS Config 交付管道。透過此交付管道，它會將記錄在日誌存檔帳戶 AWS Config 中記錄的所有變更，並將其存放到 Amazon Simple Simple Storage Service 儲存貯體中的資料夾中。

管理 AWS Config AWS Control Tower 中的成本

本節說明如何 AWS Config 記錄和收取 AWS Control Tower 帳戶中資源變更的帳單。這些資訊可協助您了解如何在使用 AWS Control Tower 時管理相關成本。 AWS ConfigAWS Control Tower 不會增加額外費用。

> **Note**
>
> 如果您的 landing zone 域版本為 3.0 或更新版本：AWS Control Tower 會將全球資源 (例如 IAM 使用者、群組、角色和客戶管理政策) 的 AWS Config 記錄限制在您的本地區域。因此，本節中的某些資訊可能不適用於您的 landing zone。

AWS Config 旨在將每個資源的每個更改記錄在帳戶運行的每個區域中，作為配置項目（CI）。 AWS Config 針對其產生的每個組態項目，向您開立帳單。

如何 AWS Config 運作

AWS Config 分別記錄每個「區域」中的資源。某些全球資源 (例如 IAM 角色) 會在每個區域記錄一次。例如，如果您在註冊帳戶中建立新的 IAM 角色，且該帳戶在五個區域中運作，則 AWS Config 會產生五個 CI，每個區域各一個 CI。其他全球資源 (例如 Route 53 託管區域) 只會在所有區域中記錄一次。例如，如果您在註冊的帳戶中建立新的 Route 53 託管區域，則 AWS Config 會產生一個 CI，無論該帳戶選取了多少個區域。如需有助於區分這些資源類型的清單，請參閱多次記錄相同的資源。

> **Note**
>
> 與 AWS Control Tower 合作時 AWS Config，某個區域可能受到 AWS Control Tower 管理，或不受管理，如果帳戶在該區域運作， AWS Config 仍會記錄變更。

AWS Config 偵測資源中的兩種關係

AWS Config 區分資源之間的直接和間接關係。如果在其他資源的「描述 API」呼叫中傳回資源，則這些資源會記錄為直接關係。當您在與另一個資源的直接關係中更改資源時， AWS Config 不會為這兩種資源創建 CI。

例如，如果您建立 Amazon EC2 執行個體，而 API 需要您建立網路界面，則 AWS Config 會考慮 Amazon EC2 執行個體與網路界面有直接關係。因此，只 AWS Config 會產生一個 CI。

AWS Config 記錄屬於間接關係之資源關係的個別變更。例如，如果您建立安全群組並新增屬於安全群組一部分的關聯 Amazon EC2 執行個體，則 AWS Config 會產生兩個 CI。

如需有關直接和間接關係的詳細資訊，請參閱什麼是資源的直接和間接關係？

您可以在 AWS Config 文件中找到資源關係的清單。

檢視已註冊帳戶上的記 AWS Config 錄器資料

AWS Config 與整合，以 CloudWatch 便您可以在儀表板中檢視 AWS Config CI。如需詳細資訊，請參閱標題為AWS Config 支援 Amazon CloudWatch 指標的部落格文章。

以程式設計方式，若要檢視 AWS Config 資料，您可以使用 AWS CLI，或者您可以利用其他 AWS 工具。

查詢特定資源上的 AWS Config 記錄器資料

您可以使用 AWS CLI 擷取資源最近變更的清單。

資源歷程記錄命令：

- `aws configservice get-resource-config-history --resource-type RESOURCE-TYPE --resource-id RESOURCE-ID --region REGION`

若要進一步了解，請參閱的 API 文件`get-config-history`。

使用 AWS Config Amazon 視覺化資 QuickSight

您可以視覺化並查詢整個組織 AWS Config 中記錄的資源。如需詳細資訊，請參閱使用 Amazon 雅典娜和亞馬遜將資 AWS Config 料視覺化。 QuickSight

AWS Control Tower AWS Config 中的疑難排解

本節提供 AWS Config 與 AWS Control Tower 搭配使用時可能遇到的一些問題的相關資訊。

AWS Config 成本高

如果您的工作流程包含經常建立、更新或刪除資源的程序，或處理大量資源，則該工作流程可能會產生大量 CI。如果您在非生產科目中執行這些處理，請考慮取消註冊該科目。您可能需要手動停用該帳戶的 AWS Config 記錄器。

> **Note**
>
> 取消註冊帳戶後，AWS Control Tower 無法針對該帳戶中的資源強制執行偵探控制或記錄帳戶事件 (例如 AWS Config 活動)。

如需詳細資訊，請參閱取消管理已註冊帳戶。若要瞭解如何停用 AWS Config 記錄器，請參閱管理組態錄製程式。

多次記錄相同的資源

檢查資源是否為全域資源。對於 3.0 版之前的 AWS Control Tower 登陸區域，每個操作區域 AWS Config 可能會記錄某些全球資源一次。 AWS Config 例如，如果在八 AWS Config 個區域上啟用，則每個角色都會記錄八次。

下列資源會針對每個作業中的「區域」記錄一次： AWS Config

- `AWS::IAM::Group`
- `AWS::IAM::Policy`
- `AWS::IAM::Role`
- `AWS::IAM::User`

其他全球資源只會記錄一次。以下是記錄一次資源的一些示例：

- `AWS::Route53::HostedZone`
- `AWS::Route53::HealthCheck`
- `AWS::ECR::PublicRepository`
- `AWS::GlobalAccelerator::Listener`
- `AWS::GlobalAccelerator::EndpointGroup`
- `AWS::GlobalAccelerator::Accelerator`

AWS Config 沒有記錄資源

某些資源與其他資源具有相依性關係。這些關係可能是直接或間接的。您可以在AWS Config 常見問題集中找到已取代間接關係的清單。

AWS Control Tower 的生命週期事件

AWS Control Tower 記錄的一些事件是生命週期事件。生命週期事件的目的是標記變更資源狀態的某些 AWS Control Tower 動作已完成。生命週期事件適用於 AWS Control Tower 建立或管理的資源，例如組織單位 (OU)、帳戶和控制項。

AWS Control Tower 生命週期事件的特性

- 對於每個生命週期事件，事件日誌會顯示原始 Control Tower 動作是否順利完成或失敗。
- AWS CloudTrail 會自動將每個生命週期事件記錄為非 API AWS 服務事件。若要取得更多資訊，請參閱 AWS CloudTrail 使用者指南。
- 每個生命週期事件也會傳送到 Amazon EventBridge 和 Amazon CloudWatch 活動服務。

AWS Control Tower 的生命週期事件提供兩個主要優點：

- 由於生命週期事件會註冊 AWS Control Tower 動作的完成情況，因此您可以建立 Amazon EventBridge 規則或 Amazon E CloudWatch vents 規則，以根據生命週期事件的狀態觸發自動化工作流程中的後續步驟。
- 日誌提供額外的詳細資訊，以協助管理員和稽核員檢閱組織中特定類型的活動。

生命週期事件的運作方式

AWS Control Tower 仰賴多種服務來實作其動作。因此，只有在一系列動作完成後，才會記錄每個生命週期事件。例如，當您在 OU 上啟用控制項時，AWS Control Tower 會啟動一系列實作請求的子步驟。整個系列子步驟的最終結果會在日誌中記錄為生命週期事件的狀態。

- 如果每個基礎子步驟都已成功完成，則生命週期事件狀態會記錄為 Succeeded (成功)。
- 如果有任何基礎子步驟未成功完成，則生命週期事件狀態會記錄為 Failed (失敗)。

每個生命週期事件都包含一個記錄的時間戳記，顯示 AWS Control Tower 動作啟動的時間，以及另一個時間戳記，顯示生命週期事件何時完成，標示成功或失敗。

檢視 Control Tower 中的生命週期事件

您可以從 AWS Control Tower 儀表板的活動頁面檢視生命週期事件。

- 若要瀏覽至 Activities (活動) 頁面，請從左側導覽窗格選擇 Activities (活動)。
- 若要取得特定事件的詳細資訊，請選取事件，然後選擇右上角的 View details (檢視詳細資料) 按鈕。

有關如何將 AWS Control Tower 生命週期事件整合到工作流程中的詳細資訊，請參閱此部落格文章：使用生命週期事件追蹤 AWS Control Tower 動作並觸發自動化工作流程。

預期的行為 CreateManagedAccount 和生 UpdateManagedAccount命週期事件

在 AWS Control Tower 建立帳戶或註冊帳戶時，這兩個動作會呼叫相同的內部 API。如果在此程序期間發生錯誤，通常會在帳戶建立但未完全佈建之後發生。當您在錯誤發生後重試建立帳戶，或嘗試更新佈建的產品時，AWS Control Tower 會看到該帳戶已存在。

由於帳戶存在，AWS Control Tower 會在重試請求結束時記錄`CreateManagedAccount`生命週期事件，而不是生命週期事件。`UpdateManagedAccount`由於錯誤，您可能預期會看到另一個`CreateManagedAccount`事件。但是，`UpdateManagedAccount`生命週期事件是預期和所需的行為。

如果您計劃使用自動化方法在 AWS Control Tower 建立帳戶或註冊帳戶，請對 Lambda 函數進行程式設計，以尋找UpdateManagedAccount生命週期事件和CreateManagedAccount生命週期事件。

生命週期事件名稱

每個生命週期事件的命名方式都會與原始 AWS Control Tower 動作相對應，AWS 也會記錄這個動作 CloudTrail。因此，例如，AWS Control Tower 事件所產生的生命週期`CreateManagedAccount` CloudTrail 事件會被命名為`CreateManagedAccount`。

清單中每個名稱後面都會有個連結，連至以 `JSON` 格式記錄的詳細資訊範例。這些範例中顯示的其他詳細資訊取自 Amazon CloudWatch 事件日誌。

雖然 `JSON` 不支援註解，但是為了用於解釋，已在範例中加入一些註解。註釋前面有 “//”，並且會出現在範例的右側。

在這些範例中，已隱蔽某些帳戶名稱和組織名稱。`accountId` 始終是一個 12 個數字的序列，它在範例中已取代為 “xxxxxxxxxxx”。`organizationalUnitID` 為唯一字串，由字母和數字組成。其形式保留在範例中。

- `CreateManagedAccount`：日誌記錄 AWS Control Tower 是否成功完成使用帳戶工廠建立和佈建新帳戶的每個動作。
- `UpdateManagedAccount`：日誌記錄 AWS Control Tower 是否成功完成每個動作，以更新與先前使用帳戶工廠建立的帳戶相關聯的佈建產品。
- `EnableGuardrail`：日誌記錄 AWS Control Tower 是否成功完成每個動作，以對 AWS Control Tower 建立的 OU 啟用控制。

- DisableGuardrail：日誌記錄 AWS Control Tower 是否成功完成了對 AWS Control Tower 建立的 OU 停用控制的每個動作。
- SetupLandingZone：記錄會記錄 AWS Control Tower 是否成功完成設定 landing zone 域的每個動作。
- UpdateLandingZone：日誌記錄 AWS Control Tower 是否成功完成每個動作以更新現有 landing zone。
- RegisterOrganizationalUnit：日誌記錄 AWS Control Tower 是否成功完成每個動作，以便在 OU 上啟用其控管功能。
- DeregisterOrganizationalUnit：記錄會記錄 AWS Control Teck 是否成功完成所有動作，以停用 OU 上的控管功能。
- PrecheckOrganizationalUnit：日誌記錄 AWS Control Tower 是否偵測到任何可能導致延伸控管操作無法成功完成的資源。

以下各節提供 AWS Control Tower 生命週期事件清單，以及針對每種生命週期事件類型記錄的詳細資訊範例。

CreateManagedAccount

此生命週期事件記錄 AWS Control Tower 是否使用帳戶工廠成功建立和佈建新帳戶。此事件對應於 AWS Control Tower CreateManagedAccount CloudTrail 事件。生命週期事件日誌包含新建立帳戶的 accountName 和 accountId，以及放置帳戶之 OU 的 organizationalUnitName 和 organizationalUnitId。

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",                                    // Management account
 ID.
    "time": "2018-08-30T21:42:18Z",                               // Format: yyyy-MM-
dd'T'hh:mm:ssZ
    "region": "us-east-1",                                        // AWS Control Tower
 home region.
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
```

```
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",                    // Timestamp when call
 was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
        "eventName": "CreateManagedAccount",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "createManagedAccountStatus": {
                "organizationalUnit":{
                    "organizationalUnitName":"Custom",
                    "organizationalUnitId":"ou-XXXX-l3zc8b3h"

                    },
                "account":{
                    "accountName":"LifeCycle1",
                    "accountId":"XXXXXXXXXXXX"
                    },
                "state":"SUCCEEDED",
                "message":"AWS Control Tower successfully created a managed account.",
                "requestedTimestamp":"2019-11-15T11:45:18+0000",
                "completedTimestamp":"2019-11-16T12:09:32+0000"}
        }
    }
}
```

UpdateManagedAccount

此生命週期事件記錄 AWS Control Tower 是否成功更新與先前使用帳戶工廠建立的帳戶相關聯的佈建產品。此事件對應於 AWS Control Tower UpdateManagedAccount CloudTrail 事件。生命週期事件日誌包含相關聯帳戶的 organizationalUnitId 和 organizationalUnitName，以及放置更新帳戶之 OU 的 accountName 和 accountId。

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
```

```
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",                                    // AWS Control Tower
 organization management account.
    "time": "2018-08-30T21:42:18Z",                               // Format: yyyy-MM-
dd'T'hh:mm:ssZ
    "region": "us-east-1",                                        // AWS Control Tower
 home region.
    "resources": [],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",                      // Timestamp when call
 was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
        "eventName": "UpdateManagedAccount",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "updateManagedAccountStatus": {
                "organizationalUnit":{
                    "organizationalUnitName":"Custom",
                    "organizationalUnitId":"ou-XXXX-l3zc8b3h"
                    },
                "account":{
                    "accountName":"LifeCycle1",
                    "accountId":"624281831893"
                    },
                "state":"SUCCEEDED",
                "message":"AWS Control Tower successfully updated a managed account.",
                "requestedTimestamp":"2019-11-15T11:45:18+0000",
                "completedTimestamp":"2019-11-16T12:09:32+0000"}
        }
    }
}
```

EnableGuardrail

此生命週期事件記錄 AWS Control Tower 是否成功啟用由 AWS Control Tower 管理的 OU 上的控制。此事件對應於 AWS Control Tower EnableGuardrail CloudTrail 事件。生命週期事件記錄檔包括控制項organizationalUnitId的organizationalUnitName和，以及啟用控制項之 OU 的和。guardrailId guardrailBehavior

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",
    "time": "2018-08-30T21:42:18Z",                                    // End-time of action.
 Format: yyyy-MM-dd'T'hh:mm:ssZ
    "region": "us-east-1",                                             // AWS Control Tower
 home region.
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",
        "eventSource": "controltower.amazonaws.com",
        "eventName": "EnableGuardrail",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "enableGuardrailStatus": {
                "organizationalUnits": [
                    {
                      "organizationalUnitName": "Custom",
                      "organizationalUnitId": "ou-vwxy-18vy4yro"
                    }
                  ],
                  "guardrails": [
                    {
```

```
                    "guardrailId": "AWS-GR_RDS_INSTANCE_PUBLIC_ACCESS_CHECK",
                    "guardrailBehavior": "DETECTIVE"
                  }
                ],
                "state": "SUCCEEDED",
                "message": "AWS Control Tower successfully enabled a guardrail on an
 organizational unit.",
                "requestTimestamp": "2019-11-12T09:01:07+0000",
                "completedTimestamp": "2019-11-12T09:01:54+0000"
              }
        }
    }
}
```

DisableGuardrail

此生命週期事件記錄 AWS Control Tower 是否成功停用由 AWS Control Tower 管理的 OU 上的控制。此事件對應於 AWS Control Tower DisableGuardrail CloudTrail 事件。生命週期事件記錄檔包括控制項organizationalUnitId的和，以organizationalUnitName及已停用控制項之 OU 的和。guardrailId guardrailBehavior

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",
    "time": "2018-08-30T21:42:18Z",
    "region": "us-east-1",
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",
        "eventSource": "controltower.amazonaws.com",
        "eventName": "DisableGuardrail",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
```

```
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "disableGuardrailStatus": {
                   "organizationalUnits": [
                    {
                      "organizationalUnitName": "Custom",
                      "organizationalUnitId": "ou-vwxy-18vy4yro"
                    }
                  ],
                  "guardrails": [
                    {
                      "guardrailId": "AWS-GR_RDS_INSTANCE_PUBLIC_ACCESS_CHECK",
                      "guardrailBehavior": "DETECTIVE"
                    }
                  ],
                  "state": "SUCCEEDED",
                  "message": "AWS Control Tower successfully disabled a guardrail on an
 organizational unit.",
                  "requestTimestamp": "2019-11-12T09:01:07+0000",
                  "completedTimestamp": "2019-11-12T09:01:54+0000"
                }
            }
        }
    }
```

SetupLandingZone

此生命週期事件記錄 AWS Control Tower 是否成功設定 landing zone 域。此事件對應於 AWS Control Tower SetupLandingZone CloudTrail 事件。生命週期事件日誌包括rootOrganizationalId，這是 AWS Control Tower 從管理帳戶建立的組織 ID。記錄項目還包括 AWS Control Tower 設定 landing zone 時所建立accountId的每個 OU 的accountName和，以及每個帳戶的和。organizationalUnitName organizationalUnitId

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",                // Request ID.
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",                                  // Management account
 ID.
```

```
   "time": "2018-08-30T21:42:18Z",                                  // Event time from
CloudTrail.
   "region": "us-east-1",                                           // Management account
CloudTrail region.
   "resources": [ ],
   "detail": {
       "eventVersion": "1.05",
       "userIdentity": {
           "accountId": "XXXXXXXXXXXX",                             // Management-account
ID.
           "invokedBy": "AWS Internal"
       },
       "eventTime": "2018-08-30T21:42:18Z",                         // Timestamp when call
was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
       "eventSource": "controltower.amazonaws.com",
       "eventName": "SetupLandingZone",
       "awsRegion": "us-east-1",                                    // AWS Control Tower
home region.
       "sourceIPAddress": "AWS Internal",
       "userAgent": "AWS Internal",
       "eventID": "CloudTrail_event_ID",                            // This value is
generated by CloudTrail.
       "readOnly": false,
       "eventType": "AwsServiceEvent",
       "serviceEventDetails": {
           "setupLandingZoneStatus": {
               "state": "SUCCEEDED",                                 // Status of entire
lifecycle operation.
               "message": "AWS Control Tower successfully set up a new landing zone.",

               "rootOrganizationalId" : "r-1234",
               "organizationalUnits" : [                             // Use a list.
                 {
                   "organizationalUnitName": "Security",             // Security OU
name.
                   "organizationalUnitId": "ou-adpf-302pk332"        // Security OU ID.
                 },
                 {
                   "organizationalUnitName": "Custom",               // Custom OU name.
                   "organizationalUnitId": "ou-adpf-302pk332"        // Custom OU ID.
                 },
               ],
              "accounts": [                                          // All created
accounts are here. Use a list of "account" objects.
```

```
                {
                  "accountName": "Audit",
                  "accountId": "XXXXXXXXXXXX"
                },
                {
                  "accountName": "Log archive",
                  "accountId": "XXXXXXXXXXXX"
                }
            ],
            "requestedTimestamp": "2018-08-30T21:42:18Z",
            "completedTimestamp": "2018-08-30T21:42:18Z"
          }
        }
    }
}
```

UpdateLandingZone

此生命週期事件記錄 AWS Control Tower 是否成功更新您現有的 landing zone。此事件對應於 AWS Control Tower UpdateLandingZone CloudTrail 事件。生命週期事件日誌包括rootOrganizationalId，這是由 AWS Control Tower 管理的 (已更新) 組織的 ID。記錄項目還包括organizationalUnitName之organizationalUnitId前 AWS Control Tower 最初設定 landing zone 時所建立的每個 OU 的accountName和accountId，以及每個帳戶的和。

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",                // Request ID.
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",                                   // Management account
 ID.
    "time": "2018-08-30T21:42:18Z",                              // Event time from
 CloudTrail.
    "region": "us-east-1",                                       // Management account
 CloudTrail region.
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",                         // Management account
 ID.
```

```
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",                    // Timestamp when call
was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
        "eventName": "UpdateLandingZone",
        "awsRegion": "us-east-1",                               // AWS Control Tower
home region.
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "CloudTrail_event_ID",                       // This value is
generated by CloudTrail.

        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "updateLandingZoneStatus": {
                "state": "SUCCEEDED",                           // Status of entire
operation.
                "message": "AWS Control Tower successfully updated a landing zone.",


                "rootOrganizationalId" : "r-1234",
                "organizationalUnits" : [                        // Use a list.
                  {
                    "organizationalUnitName": "Security",            // Security OU
name.
                    "organizationalUnitId": "ou-adpf-302pk332"    // Security OU ID.
                  },
                  {
                    "organizationalUnitName": "Custom",           // Custom OU name.
                    "organizationalUnitId": "ou-adpf-302pk332"     // Custom OU ID.
                  },
                ],
               "accounts": [                                     // All created
accounts are here. Use a list of "account" objects.

                  {
                    "accountName": "Audit",
                    "accountId": "XXXXXXXXXXXX"
                  },
                  {
                    "accountName": "Log archive",
                    "accountId": "XXXXXXXXXX"
```

```
                }
            ],
            "requestedTimestamp": "2018-08-30T21:42:18Z",
            "completedTimestamp": "2018-08-30T21:42:18Z"
        }
    }
  }
}
```

RegisterOrganizationalUnit

此生命週期事件記錄 AWS Control Tower 是否在 OU 上成功啟用其控管功能。此事件對應於 AWS Control Tower RegisterOrganizationalUnit CloudTrail 事件。生命週期事件日誌包括 AWS Control Tower 在其管理下帶來organizationalUnitId的 OU organizationalUnitName 和。

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "123456789012",
    "time": "2018-08-30T21:42:18Z",
    "region": "us-east-1",
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",
        "eventSource": "controltower.amazonaws.com",
        "eventName": "RegisterOrganizationalUnit",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "registerOrganizationalUnitStatus": {
                "state": "SUCCEEDED",
```

```
                "message": "AWS Control Tower successfully registered an organizational
 unit.",

                "organizationalUnit" :
                  {
                    "organizationalUnitName": "Test",
                    "organizationalUnitId": "ou-adpf-302pk332"
                  }
                "requestedTimestamp": "2018-08-30T21:42:18Z",
                "completedTimestamp": "2018-08-30T21:42:18Z"
            }
        }
    }
}
```

DeregisterOrganizationalUnit

此生命週期事件記錄 AWS Control Tower 是否成功停用 OU 上的管理功能。此事件對應於 AWS Control Tower `DeregisterOrganizationalUnit` CloudTrail 事件。生命週期事件日誌包括 AWS Control Tower 已停用其控管功能`organizationalUnitId`之 OU 的`organizationalUnitName`和。

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",
    "time": "2018-08-30T21:42:18Z",
    "region": "us-east-1",
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",
        "eventSource": "controltower.amazonaws.com",
        "eventName": "DeregisterOrganizationalUnit",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
```

```
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "deregisterOrganizationalUnitStatus": {
                "state": "SUCCEEDED",
                "message": "AWS Control Tower successfully deregistered an
organizational unit, and enabled mandatory guardrails on the new organizational
unit.",
                "organizationalUnit" :
                  {
                    "organizationalUnitName": "Test",                    // Foundational
OU name.
                    "organizationalUnitId": "ou-adpf-302pk332"           // Foundational
OU ID.
                  },
                "requestedTimestamp": "2018-08-30T21:42:18Z",
                "completedTimestamp": "2018-08-30T21:42:18Z"
            }
            }
        }
    }
```

PrecheckOrganizationalUnit

此生命週期事件記錄 AWS Control Tower 是否成功對 OU 執行預先檢查。此事件對應於 AWS Control Tower PrecheckOrganizationalUnit CloudTrail 事件。生命週期事件日誌包含 AWS Control Tower 在 OU 註冊程序期間執行預先檢查的每個資源的、和failedPrechecks值的欄位。Id Name

事件記錄檔也包含執行預先檢查之巢狀帳戶的相關資訊，包括accountNameaccountId、和failedPrechecks欄位。

如果該failedPrechecks值為空，則表示該資源的所有預先檢查成功通過。

- 只有在發生預先檢查失敗時，才會發出此事件。
- 如果您正在註冊空 OU，則不會發出此事件。

事件示例：

```
{
  "eventVersion": "1.08",
  "userIdentity": {
```

```
    "accountId": "XXXXXXXXXXXX",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2021-09-20T22:45:43Z",
  "eventSource": "controltower.amazonaws.com",
  "eventName": "PrecheckOrganizationalUnit",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "eventID": "b41a9d67-0da4-4dc5-a87a-25fa19dc5305",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "XXXXXXXXXXXX",
  "serviceEventDetails": {
    "precheckOrganizationalUnitStatus": {
      "organizationalUnit": {
        "organizationalUnitName": "Ou-123",
        "organizationalUnitId": "ou-abcd-123456",
        "failedPrechecks": [
            "SCP_CONFLICT"
          ]
      },
      "accounts": [
        {
          "accountName": "Child Account 1",
          "accountId": "XXXXXXXXXXXX",
          "failedPrechecks": [
            "FAILED_TO_ASSUME_ROLE"
          ]
        },
        {
          "accountName": "Child Account 2",
          "accountId": "XXXXXXXXXXXX",
          "failedPrechecks": [
            "FAILED_TO_ASSUME_ROLE"
          ]
        },
        {
          "accountName": "Management Account",
          "accountId": "XXXXXXXXXXXX",
          "failedPrechecks": [
            "MISSING_PERMISSIONS_AF_PRODUCT"
          ]
```

```
        },
        {
          "accountName": "Child Account 3",
          "accountId": "XXXXXXXXXXXX",
          "failedPrechecks": []
        },
        ...
      ],
      "state": "FAILED",
      "message": "AWS Control Tower failed to register an organizational unit due to
 pre-check failures. Go to the OU details page to download a list of failed pre-checks
 for the OU and accounts within.",
      "requestedTimestamp": "2021-09-20T22:44:02+0000",
      "completedTimestamp": "2021-09-20T22:45:43+0000"
    }
  },
  "eventCategory": "Management"
}
```

使用使用 AWS 者通知 AWS Control Tower

您可以使用「使用AWS 者通知」 來設定傳送管道，以接收 AWS Control Tower 事件通知。當事件符合您指定的規則時，便會收到通知。您可以透過多個管道接收事件通知，包括電子郵件、AWS Chatbot聊天通知或AWS 主控台行動應用程式推播通知。您也可以在主控台通知中心查看通知。

AWS 使用者通知支援彙總，可減少您在特定事件期間收到的通知數目。通知也會顯示在「主控台通知中心」中。

透過 AWS 使用者通知訂閱通知的優點，而不是 EventBridge 包括：

- 一個更友好的用戶界面（UI）。
- 與 AWS 控制台集成，位於全局導航欄上的鈴聲/通知區域中。
- 原生支援電子郵件通知，不需要設定 Amazon SNS。
- 最值得注意的是，支持移動推送通知，專用於用 AWS 戶通知。

例如，您可能希望收到的一種通知類型是發現 Security Hub 嚴重和高嚴重性的情況下。JSON 中用於設置通知訂閱的代碼片段可能如下所示：

```
{
  "detail": {
```

```
    "findings": {
      "Compliance": {
        "Status": ["FAILED", "WARNING", "NOT_AVAILABLE"]
      },
      "RecordState": ["ACTIVE"],
      "Severity": {
        "Label": ["CRITICAL", "HIGH"]
      },
      "Workflow": {
        "Status": ["NEW", "NOTIFIED"]
      }
    }
  }
}
```

事件篩選

- 您可以使用 [使用 AWS 者通知] 主控台上提供的篩選器，依服務和名稱篩選事件。
- 如果您從 JSON 代碼創建自己的過濾器，則可以按特定屬性 EventBridge 過濾事件。

示例 AWS Control Tower 事件

下面是一個通用的示例 AWS Control Tower事件.

- 這是一個 EventBridge 事件。
- 您可以使用「使用 AWS 者通知」來訂閱 EventBridge 事件 (例如此事件)。

```
{
    "version": "0",
    "id": "<id>", // alphanumeric string
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "<account ID>", // Management account ID.
    "time": "<date>", // Format: yyyy-MM-dd'T'hh:mm:ssZ
    "region": "<region>", // AWS Control Tower home region.
    "resources": [],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "121212121212",
            "invokedBy": "AWS Internal"
```

```
        },
        "eventTime": "2018-08-30T21:42:18Z", // Timestamp when call was made. Format:
 yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
        "eventName": "<event name>", // one of the 9 event names in https://
docs.aws.amazon.com/controltower/latest/userguide/lifecycle-events.html
        "awsRegion": "<region>",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "<id>",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            // the contents of this object vary depending on the event subtype and
 event state
        }
    }
}
```

逐步解說

本章包含逐步解說程序，可協助您使用 AWS Control Tower。

主題

逐步解說：從 ALZ 移至 AWS Control Tower

許多 AWS 客戶已採用 AWS 登陸區域解決方案 (ALZ) 來設定安全、合規的多帳戶環 AWS 境。為了減輕管理 landing zone 域的負擔，請 AWS 建立名為 AWS Control Tower 的受管服務。

ALZ 沒有安排其他功能；它僅提供長期支持。因此，我們建議您從 ALZ 移至 AWS Control Tower 服務。本章所連結的部落格會引導您瞭解該次移動的不同考量事項，並說明如何規劃從 ALZ 到 AWS Control Tower 的成功移轉。

部落格：將 AWS 著陸區解決方案遷移到 AWS Control Tower

AWS 規範指導提供更廣泛的文件，包括從 ALZ 轉換到 AWS Control Tower 的步驟。基本上，您將根據一些先決條件，在執行 ALZ 的現有組織中啟用 AWS Control Tower 管控。如需相關資訊，請參閱從 AWS 著陸區轉換到 AWS Control Tower。

逐步解說：依 Service Catalog API 在 AWS Control Tower 中自動佈建帳戶

AWS Control Tower 已與其他多項 AWS 服務整合，例如 AWS Service Catalog. 您可以使用 API 在 AWS Control Tower 中建立和佈建您的成員帳戶。

影片說明如何透過呼叫 AWS Service Catalog API，以自動化的批次方式佈建帳戶。對於佈建，您將從 AWS 命令列介面 (CLI) 呼叫 `ProvisionProduct`API，並指定一個 JSON 檔案，其中包含您要設定

的每個帳戶的參數。影片說明如何安裝並使用 AWS Cloud9 開發環境來執行這項工作。如果您使用雲 AWS 殼而不是 Cloud9，則 CLI 命令將是相同的 AWS 。

> **Note**
>
> 您也可以調整此方法以自動化帳戶更新，方法是呼叫每個帳戶 AWS Service Catalog 的 `UpdateProvisionedProduct`API。您可以編寫指令碼來逐一更新帳戶。

這是一種完全不同的自動化方法，如果您熟悉 Terraform，可以使用適用於 Terraform (AFT) 的 AWS Control Tower Account Factory 佈建帳戶。

範例自動化管理角色

以下範例範本可用來協助設定管理帳戶中的自動化管理角色。您可以在管理帳戶中設定此角色，以便它可以透過目標帳戶中的系統管理員存取權執行自動化。

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure the SampleAutoAdminRole

Resources:
  AdministrationRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: SampleAutoAdminRole
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: cloudformation.amazonaws.com
            Action:
              - sts:AssumeRole
      Path: /
      Policies:
        - PolicyName: AssumeSampleAutoAdminRole
          PolicyDocument:
            Version: 2012-10-17
            Statement:
              - Effect: Allow
                Action:
                  - sts:AssumeRole
```

```
                Resource:
                  - "arn:aws:iam::*:role/SampleAutomationExecutionRole"
```

範例自動化執行角色

以下是範例範本，可用來協助您設定自動化執行角色。您可以在目標帳戶中設定此角色。

```
AWSTemplateFormatVersion: "2010-09-09"
Description: "Create automation execution role for creating Sample Additional Role."

Parameters:
  AdminAccountId:
    Type: "String"
    Description: "Account ID for the administrator account (typically management,
 security or shared services)."
  AdminRoleName:
    Type: "String"
    Description: "Role name for automation administrator access."
    Default: "SampleAutomationAdministrationRole"
  ExecutionRoleName:
    Type: "String"
    Description: "Role name for automation execution."
    Default: "SampleAutomationExecutionRole"
  SessionDurationInSecs:
    Type: "Number"
    Description: "Maximum session duration in seconds."
    Default: 14400

Resources:
  # This needs to run after AdminRoleName exists.
  ExecutionRole:
    Type: "AWS::IAM::Role"
    Properties:
      RoleName: !Ref ExecutionRoleName
      MaxSessionDuration: !Ref SessionDurationInSecs
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: "Allow"
            Principal:
              AWS:
                - !Sub "arn:aws:iam::${AdminAccountId}:role/${AdminRoleName}"
            Action:
              - "sts:AssumeRole"
```

```
      Path: "/"
      ManagedPolicyArns:
        - "arn:aws:iam::aws:policy/AdministratorAccess"
```

設定這些角色之後，您可以呼叫 AWS Service Catalog API 來執行自動化工作。CLI 命令在視頻中給出。

Service Catalog API 的範例佈建輸入

如果您使用 API 佈建 AWS Control Tower 帳戶，以下是您可以提供給 Service Catalog `ProvisionProduct` API 的輸入範例：

```
{
  pathId: "lpv2-7n2o3nudljh4e",
  productId: "prod-y422ydgjge2rs",
  provisionedProductName: "Example product 1",
  provisioningArtifactId: "pa-2mmz36cfpj2p4",
  provisioningParameters: [
    {
      key: "AccountEmail",
      value: "abc@amazon.com"
    },
    {
      key: "AccountName",
      value: "ABC"
    },
    {
      key: "ManagedOrganizationalUnit",
      value: "Custom (ou-xfe5-a8hb8ml8)"
    },
    {
      key: "SSOUserEmail",
      value: "abc@amazon.com"
    },
    {
      key: "SSOUserFirstName",
      value: "John"
    },
    {
      key: "SSOUserLastName",
      value: "Smith"
    }
  ],
```

```
  provisionToken: "c3c795a1-9824-4fb2-a4c2-4b1841be4068"
}
```

如需詳細資訊，請參閱 Service Catalog 的 API 參考。

> **Note**
>
> 請注意，值的輸入字串格式ManagedOrganizationalUnit已從變更OU_NAME為OU_NAME (OU_ID)。接下來的視頻沒有提及此更改。

影片演練

此影片 (6:58) 說明如何在 AWS Control Tower 中自動化帳戶部署。若要獲得更佳的觀賞效果，請選取影片右下角的圖示，將影片放大至全螢幕。並提供字幕。

AWS Control Tower 中自動化帳戶佈建的影片逐步解說。

逐步解說：在沒有 VPC 的情況下設定 AWS Control Tower

本主題將逐步介紹如何在沒有 VPC 的情況下設定 AWS Control Tower 帳戶。

如果您的工作負載不需要 VPC，您可以執行下列動作：

- 您可以刪除 AWS Control Tower 虛擬私有雲端 (VPC)。此 VPC 是在您設定登陸區域時建立。
- 您可以變更 Account Factory 設定，以便在沒有關聯 VPC 的情況下建立新的 AWS Control Tower Tall 帳戶。

> **Important**
>
> 如果在啟用 VPC 網際網路存取設定的情況下佈建 Account Factory 帳戶，則該 Account Factory 設定會覆寫客戶管理之 Amazon VPC 執行個體的「禁止網際網路存取」控制項。若要避免為新佈建的帳戶啟用網際網路存取，您必須變更 Account Factory 中的設定。

刪除 AWS Control Tower VPC

在 AWS Control Tower 外，每個 AWS 客戶都有一個預設的 VPC，您可以在 Amazon Virtual Private Cloud 端 (Amazon VPC) 主控台上查看，網址為 https://console.aws.amazon.com/vpc/。由於其名稱總是在名稱結尾包括此字詞 (預設)，因此您將可辨識出預設 VPC。

當您設定 AWS Control Tower landing zone 時，AWS Control Tower 會刪除您的 AWS 預設 VPC，並建立新的 AWS Control Tower 預設 VPC。新的 VPC 與您的 AWS Control Tower 管理帳戶相關聯。本主題將該新 VPC 稱為 Control Tower V PC。

當您在 Amazon VPC 主控台中檢視 AWS Control Tower VPC 時，名稱末尾不會看到這個字 (預設值)。如果您有多個 VPC，則必須使用指派的 CIDR 範圍來識別正確的 AWS Control Tower VPC。

您可以刪除 AWS Control Tower VPC，但是如果稍後需要 AWS Control Tower 中的 VPC，則必須自行建立 VPC。

若要刪除 AWS Control Tower VPC

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 從 Service Catalog 選項中搜尋**VPC**或選取 VPC。您之後就會看到 VPC Dashboard (VPC 儀表板)。
3. 從左側功能表中，選擇 Your VPCs (您的 VPC)。接著則可看到所有 VPC 的清單。
4. 按照其 CIDR 範圍識別 AWS Control Tower VPC 人雲端。
5. 若要刪除 VPC，並選擇 Actions (動作)，然後選擇 Delete VPC (刪除 VPC)。

AWS Control Tower 管理帳戶的每個區域都已存在 AWS (預設) VPC。若要遵循安全最佳實務，如果您選擇刪除 AWS Control Tower VPC，最好也從所有 AWS 區域刪除與管理帳戶關聯的 AWS 預設 VPC。因此，若要保護管理帳戶，請從每個區域移除預設 VPC，並移除由 Control Tower 在 AWS Control Tower Control Twer 本地區域中建立的 VPC。

在沒有 VPC 的 AWS Control Tower 中建立帳戶

如果您的使用者工作負載不需要 VPC，您可以使用此方法來設定沒有自動為其建立 VPC 的使用者帳戶。

您可以從 AWS Control Tower 儀表板檢視和編輯網路組態設定。變更設定以便在沒有關聯 VPC 的情況下建立 AWS Control Tower 帳戶後，會在沒有 VPC 的情況下建立所有新帳戶，直到您再次變更設定為止。

若要設定 Account Factory 理站以建立沒有 VPC 的帳戶

1. 開啟網頁瀏覽器，然後瀏覽至 AWS Control Tower 主控台，網址為 https://console.aws.amazon.com/controltower。
2. 從左側選單中選擇「Account Factory」。
3. 接著您會看到 [Account Factory] 頁面，其中包含 [網路組態] 區段
4. 如果您之後想要還原目前的設定，請記下目前的設定。
5. 選擇「網路組態」段落中的 「編輯」按鈕。
6. 在 Edit account factory network configuration (編輯帳戶團隊網路組態) 頁面中，前往 VPC Configuration options for new accounts (新帳戶的 VPC 組態選項) 區段。

   您可以遵循選項 1 或選項 2 或兩者，以確保 AWS Control Tower 在佈建帳戶時不會建立 VPC。

   a. 選項 1-刪除子網

      - 關閉 Internet-accessible subnet (可從網際網路存取的子網路) 切換開關。
      - 將 Maximum number of private subnets (私有子網路上限) 的值設為 0。

   b. 選項 2 — 移除 AWS 區域

      - 清除 Regions for VPC creation (VPC 建立的區域) 欄中的每個核取方塊。
7. 選擇儲存。

可能的錯誤

請注意刪除 AWS Control Tower VPC 或重新設定 Account Factory 以建立沒有 VPC 的帳戶時，可能發生的錯誤。

- 您現有的管理帳戶可能在 AWS Control Tower VPC 中具有相依性或資源，這可能會導致刪除失敗錯誤。
- 如果您在設為啟動沒有 VPC 的新帳戶時，沿用預設的 CIDR，您的請求則會失敗，並出現 CIDR 無效的錯誤。

逐步解說：使用 AWS Firewall Manager 在 AWS Control Tower 中設定安全群組

影片說明如何使用 AWS Firewall Manager 員服務改善 AWS Control Tower 的網路安全性。您可以指定已啟用的安全管理員帳戶來設定安全群組。您將瞭解如何為 AWS Control Tower 組織設定安全政策和強制執行安全規則，以及如何透過自動套用政策來修復不合規的資源。您可以檢視組織中每個帳戶和資源 (例如 Amazon EC2 執行個體) 生效的安全群組。

您可以建立自己的防火牆原則，也可以訂閱信任廠商的規則。

使用 AWS Firewall Manager 員設定安全群組

本影片 (8:02) 說明如何在 AWS Control Tower 中為資源和工作負載設定更好的網路基礎設施安全性。若要獲得更佳的觀賞效果，請選取影片右下角的圖示，將影片放大至全螢幕。並提供字幕。

AWS Control Tower 中防火牆設定的影片逐步解說。

如需詳細資訊，請參閱有關如何設定 AWS WAF 的文件。

逐步解說：解除委任 AWS Control Tower 登陸區

AWS Control Tower 可讓您設定和管理安全的多帳戶 AWS 環境 (稱為登陸區域)。清理 AWS Control Tower 分配的所有資源的程序稱為停用 landing zone。

如果您不想再使用 AWS Control Tower，則自動解除委任工具會清除 AWS Control Tower 分配的資源。若要開始自動化解除委任程序，請導覽至「landing zone 設定」頁面，選取「解除委任」索引標籤，然後選擇「解除使用登陸區域」。

如需解除委任期間執行的動作清單，請參閱解除委任程序概觀。

> **Warning**
>
> 手動刪除所有 AWS Control Tower 資源與解除委任不同。它將不允許您設置新的 landing zone。

您的數據和現 AWS Organizations 有數據不會通過以下方式更改退役過程。

- AWS Control Tower 不會移除您的資料，只會移除其建立的登陸區域部分。
- 解除委任程序完成後，仍會保留一些資源成品，例如 Amazon S3 儲存貯體和 Amazon CloudWatch 日誌日誌群組。在設定其他登陸區域之前，必須手動刪除這些資源，以避免產生維護特定資源的相關可能成本。
- 您無法使用自動解除委任來移除部分設定的登陸區域。如果您的登陸區域設定程序失敗，您必須解決失敗狀態並將其設定為能夠自動解除委任，否則就必須個別手動刪除資源。

解除委任登陸區域是具有重大後果的程序，且無法復原。以下各節說明 AWS Control Tower 採取的解除委任動作，以及停用後保留的成品。

> **Important**
>
> 強烈建議您只有在想要停止使用登陸區域時，才執行此解除委任程序。解除委任後，將無法重新建立現有的登陸區域。

解除委任程序概觀

當您要求停用 landing zone 時，AWS Control Tower 會執行下列動作。

- 停用在 landing zone 域中啟用的每個偵探控制。AWS Control Tower 會刪除支援控制的 AWS CloudFormation 資源。
- 透過從中移除服務控制策略 (SCP) 來 AWS Organizations停用每個預防性控制。如果政策為空白 (在移除由 AWS Control Tower 管理的所有 SCP 之後應該是空白的)，AWS Control Tower 會分離並完全刪除政策。
- 刪除部署為 AWS CloudFormation StackSets的所有藍圖。
- 刪除所有區域中部署為 CloudFormation 堆疊的所有藍圖。
- AWS Control Tower 會針對每個佈建的帳戶在解除委任程序期間執行下列動作。
  - 刪除每個帳戶團隊帳戶的記錄。
  - 移除 AWS Control Tower 建立的 IAM 角色 (除非已新增其他政策)，以撤銷帳戶的 AWS Control Tower 許可，然後重新建立標準 `OrganizationsFullAccessRole` IAM 角色。
  - 從中移除帳戶的記錄 AWS Service Catalog。
  - 從 AWS Service Catalog中移除帳戶團隊產品和產品組合。
- 刪除共用 (稽核和記錄封存) 帳戶的藍圖。

- 移除 AWS Control Tower 建立的 IAM 角色 (除非已新增其他政策)，以撤銷共用帳戶的 AWS Control Tower 許可，然後重新建立 `OrganizationsFullAccessRole` IAM 角色。
- 刪除與共用帳戶相關的記錄。
- 刪除與客戶建立 OU 相關的記錄。
- 刪除識別主區域的內部記錄。

> **Note**
>
> 解除委任後，如果您的 VPC 不是空的，您可能會想要移除帳戶團隊 VPC 藍圖 (`BP_ACCOUNT_FACTORY_VPC`) 以清理路由和 NAT 閘道。

解除委任期間未移除的資源

停用 landing zone 並不會完全顛倒 AWS Control Tower 的設定程序。某些資源仍然存在，可以手動移除。

AWS Organizations

對於沒有現有組 AWS Organizations 織的客戶，AWS Control Tower 會設定一個組織，其中包含兩個組織單位 (OU)，分別為安全和沙箱。當您解除委任登陸區域時，會保留組織的階層，如下所示：

- 您從 AWS Control Tower 主控台建立的組織單位 (OU) 不會移除。
- 不會移除安全性和沙箱 OU。
- 不會從中刪除組織 AWS Organizations。
- 不會移動或移除 AWS Organizations (共用、佈建或管理) 中的帳戶。

AWS IAM Identity Center (單一登入)

對於沒有現有 IAM 身分中心目錄的客戶，AWS Control Tower 會設定 IAM 身分中心並設定初始目錄。解除使用 landing zone 時，AWS Control Tower 不會對 IAM 身分中心進行任何變更。如有需要，您可以手動刪除儲存在管理帳戶中的 IAM 身分中心資訊。特別是，解除委任不會變更這些區域：

- 使用帳戶團隊建立的使用者不會被移除。
- 不會移除 AWS Control Tower 設定所建立的群組。
- AWS Control Tower 建立的許可集不會移除。

- 不會移除 AWS 帳戶和 IAM 身分中心權限集之間的關聯。
- IAM 身分中心目錄不會變更。

角色

在設定期間，如果您使用主控台，AWS Control Tower 會為您建立特定角色，或者如果您透過 API 設定 landing zone 域，則會要求您建立這些角色。當您解除使用 landing zone 時，不會移除下列角色：

- `AWSControlTowerAdmin`
- `AWSControlTowerCloudTrailRole`
- `AWSControlTowerStackSetRole`
- `AWSControlTowerConfigAggregatorRoleForOrganizations`

Amazon S3 儲存貯體

在安裝期間，AWS Control Tower 會在記錄帳戶中建立值區以進行記錄和記錄存取。當您解除委任登陸區域時，不會移除下列資源：

- 不會移除日誌帳戶中的日誌和日誌記錄存取 S3 儲存貯體。
- 不會移除日誌和日誌記錄存取儲存貯體的內容。

共享帳戶

在 AWS Control Tower 設定期間，會在安全 OU 中建立兩個共用帳戶 (稽核和日誌存檔)。當您解除委任登陸區域時：

- 在 AWS Control Tower 設定期間建立的共用帳戶不會關閉。
- `OrganizationAccountAccessRole`IAM 角色會重新建立，以與標準 AWS Organizations 組態保持一致。
- 會移除 `AWSControlTowerExecution` 角色。

佈建的帳戶

AWS Control Tower 客戶可以使用帳戶工廠建立新的 AWS 帳戶。當您解除委任登陸區域時：

- 您使用帳戶團隊建立的佈建帳戶不會關閉。

- 中佈建的產品 AWS Service Catalog 不會移除。如果您透過終止這些項目來清除它們，其帳戶就會移至根 OU。
- AWS Control Tower 建立的 VPC 不會移除，而且不會移除關聯的 AWS CloudFormation 堆疊集 (BP_ACCOUNT_FACTORY_VPC)。
- OrganizationAccountAccessRoleIAM 角色會重新建立，以與標準 AWS Organizations 組態保持一致。
- 會移除 AWSControlTowerExecution 角色。

CloudWatch 記錄檔記錄群組

記 CloudWatch 錄記錄群組會建立為名為之藍圖的一部分AWSControlTowerBP-BASELINE-CLOUDTRAIL-MANAGEMENT。aws-controltower/CloudTrailLogs不會移除此日誌群組。而是刪除藍圖並保留資源。

- 在您設定其他登陸區域之前，必須先手動刪除此日誌群組。

> **Note**
>
> landing zone 3.0 及更新版本的客戶不需要刪除其個別註冊帳戶的 CloudTrail 記錄檔和記 CloudTrail 錄角色，因為這些角色僅在管理帳戶中建立，適用於組織層級追蹤。
> 從 3.2 版 landing zone 開始，AWS Control Tower 會建立一個叫做的 Amazon EventBridge 規則AWSControlTowerManagedRule。此規則會在每個成員帳戶中建立，適用於所有受控管的區域。在解除委任期間不會自動刪除規則，因此您必須先從所有受控管區域的共用帳戶和成員帳戶中手動刪除該規則，然後才能在新區域中設定 landing zone 域。

有關如何刪除 AWS Control Tower 資源的程序，請參閱管理 AWS Control Tower 資源。

管理 AWS Control Tower 資源

本文件提供如何在定期維護和管理任務中個別移除 AWS Control Tower 資源的指示。本章中提供的程序僅用於在需要時移除個別資源或一些資源。它與退役您的 landing zone 不一樣。

有兩種類型的工作可能需要您移除資源：

- 在一般情況下管理登陸區域時刪除資源。
- 清理自動解除委任後剩餘的資源。

> **Warning**
>
> 手動移除資源將不允許您設定新的 landing zone。它與退役不一樣。如果您打算取消 AWS Control Tower landing zone 的委任，請在採取本章所述的任何動作逐步解說：解除委任 AWS Control Tower 登陸區之前，遵循上述的指示。本章中的指示可協助您清理完成自動化解除委任後剩餘的資源。即使您手動刪除所有 landing zone 資源，這與解除使用 landing zone 域並不相同，而且可能會產生非預期費用。

如果您需要從 AWS Control Tower 移除帳戶，請參閱以下各節以關閉帳戶：

- 取消管理帳戶
- 關閉在 Account Factory 中創建的帳戶

我是否需要解除委任而不是刪除？

如果您不想再為企業使用 AWS Control Tower，或者您需要重新部署組織資源，則可能需要解除最初設定 landing zone 時所建立的資源的委任。

- 解除委任程序完成後，仍會保留一些資源成品，例如 Amazon S3 儲存貯體和 Amazon CloudWatch 日誌日誌群組。
- 您必須先手動清理帳號中剩餘的資源，才能設定其他 landing zone，並避免產生意外費用的可能性。如需詳細資訊，請參閱 解除委任期間未移除的資源。

> **Warning**
>
> 我們強烈建議您只有在打算停止使用 landing zone 時才執行解除委任程序。此程序無法復原。

關於移除 AWS Control Tower 資源

本章中的個別程序會引導您完成移除 AWS Control Tower 資源的手動方法。當您需要從 landing zone 域刪除特定資源時，可以遵循這些程序。

執行這些程序之前，除非另有說明，否則您必須登入登陸區域中的主區域，而且您必須在 IAM Identity Center 中以 IAM 使用者或使用者身分登入，並且具有您 landing zone 域之管理帳戶的管理許可。AWS Management Console

> **Warning**
>
> 這些是破壞性的動作，可能會導入 AWS Control Tower 設定中的管理偏差。這些動作無法復原。

主題

刪除 SCP

AWS Control Tower 使用服務控制政策 (SCP) 做為其控制。此程序逐步說明如何刪除與 AWS Control Tower 特別相關的 SCP。

若要刪除 AWS Organizations SCP

1. 開啟「Organizations」主控台，位於 https://console.aws.amazon.com/organizations/。
2. 開啟 Policies (政策) 標籤，尋找具有 aws-guardrails- 前綴的服務控制政策 (SCP)，並針對每個 SCP 執行以下作業：
   a. 將 SCP 從相關聯的 OU 分離。
   b. 刪除 SCP。

刪除 StackSets 和堆疊

AWS Control Tower 會使用 StackSets 和堆疊在您的 landing zone 部署 AWS Config 規則 與控制相關的控制項。以下程序會帶您演練如何刪除這些特定資源。

若要刪除 AWS CloudFormation StackSets

1. 請在以下位置開啟 AWS CloudFormation 主控台。 https://console.aws.amazon.com/cloudformation

2. 從左側導覽功能表中選擇StackSets。
3. 對於每個 StackSet 具有前綴的前綴 AWSControlTower，請執行以下操作。如果您有許多帳戶 StackSet，這可能需要一些時間。

   a. 從儀表板 StackSet 中的表格中選擇特定項目。這將打開屬性頁面 StackSet。

   b. 在頁面底部的「堆疊」表格中，記錄表格中所有帳 AWS 戶的帳號 ID。複製所有帳戶的清單。

   c. 從「動作」 中選擇「刪除堆疊自」 StackSet。

   d. 在 [設定部署選項] 上，從 [部署位置] 選擇 [在帳戶中部署堆疊]。

   e. 在文字欄位中，輸入您在步驟 3.b 中記錄的 AWS 帳號 ID，並以逗號分隔。例如：「*123456789012*, *098765431098*」等。

   f. 從 Specify regions (指定區域)，選擇 Add all (全部新增)，並保留頁面上其餘參數的預設值，然後選擇 Next (下一步)。

   g. 在 Review (檢閱) 頁面上，檢閱您的選擇，然後選擇 Delete stacks (刪除堆疊)。

   h. 在StackSet 屬性頁面上，您可以為另一個重新開始此程序 StackSets。
4. 當不同StackSets 屬性頁面的「堆疊」表格中的記錄為空白時，此程序即完成。
5. 當「堆疊」表格中的記錄為空白時，請選擇「刪除」 StackSet。

刪除 AWS CloudFormation 堆疊

1. 請在以下位置開啟 AWS CloudFormation 主控台。 https://console.aws.amazon.com/cloudformation
2. 在「堆疊」儀表板中，搜尋具有前置字元的所有堆疊AWSControlTower。
3. 針對表格中的每個堆疊，執行以下作業：

   a. 選擇堆疊名稱旁的核取方塊。

   b. 從 Actions (動作) 選單中，選擇 Delete Stack (刪除堆疊)。

   c. 在開啟的對話方塊中，檢閱資訊並確認其正確無誤，然後選擇 Yes, Delete (是，刪除)。

刪除日誌存檔帳戶中的 Amazon S3 儲存貯體

下列程序會引導您如何以AWSControlTowerExecution群組中的 IAM 身分中心使用者身分登入日誌存檔帳戶，然後刪除日誌存檔帳戶中的 Amazon S3 儲存貯體。

使用正確許可登入您的日誌存檔帳戶

1. 開啟「Organizations」主控台，位於 https://console.aws.amazon.com/organizations/。
2. 從 Accounts (帳戶) 標籤，尋找 Log archive (日誌存檔) 帳戶。
3. 從開啟的右側窗格記下日誌存檔帳戶號碼。
4. 從導覽列選擇您的帳戶名稱以開啟您的帳戶選單。
5. 選擇 Switch Role (切換角色)。
6. 在開啟的頁面上，於 Account (帳戶) 中提供日誌存檔帳戶的帳戶號碼。
7. 對於「角色」，輸入AWSControlTowerExecution。
8. Display Name (顯示名稱) 接著便會以文字填入。
9. 選擇您喜愛的 Color (顏色)。
10. 選擇 Switch Role (切換角色)。

刪除 Amazon S3 存儲桶

1. 前往 https://console.aws.amazon.com/s3/ 開啟的 Amazon Simple Storage Service (Amazon S3) 主控台。
2. 搜尋包含 aws-controltower 的儲存貯體名稱。
3. 針對表格中的每個儲存貯體，執行以下作業：
   a. 選擇表格中儲存貯體的核取方塊。
   b. 選擇刪除。
   c. 在開啟的對話方塊中，檢閱資訊並確認其正確無誤，輸入儲存貯體的名稱以確認，然後選擇 Confirm (確認)。

移除 Account Factory 產品組合與產品

下列程序會引導您如何以AWSServiceCatalogAdmins群組中的 IAM 身分中心使用者身分登入，然後清理您的 Account Factory 產品組合和產品。

使用正確的權限登入您的管理帳戶

1. 前往您位於 *directory-id*.awsapps.com/start 的使用者入口網站 URL。
2. 從AWS 帳戶中，找到管理帳戶。

3. 從AWSServiceCatalogAdminFullAccess中選擇管理主控台以此角色 AWS Management Console 身分登入。

若要清理 Account Factory

1. 在 https://console.aws.amazon.com/servicecatalog/ 開啟 Service Catalog 主控台。
2. 從左側導覽選單選擇 Portfolios list (組合清單)。
3. 在「本地產品組合」表中，搜尋名為「AWS Control Tower Account Factory 產品組合」的產品組合
4. 選擇該組合的名稱，然後前往其詳細資訊頁面。
5. 展開頁面的「限制條件」段落，然後選擇產品名稱為 Con AWS trol Tower Account Factory 的限制條件圓鈕。
6. 選擇 REMOVE CONSTRAINTS (移除條件約束)。
7. 在開啟的對話方塊中，檢閱資訊並確認其正確無誤，然後選擇 CONTINUE (繼續)。
8. 從頁面的「產品」區段中，選擇名為「AWS Control Tower Account Factory」之產品的圓鈕。
9. 選擇 REMOVE PRODUCT (移除產品)。
10. 在開啟的對話方塊中，檢閱資訊並確認其正確無誤，然後選擇 CONTINUE (繼續)。
11. 展開頁面的 Users, Groups, and Roles (使用者、群組和角色) 區段，然後選擇此表格中所有記錄的核取方塊。
12. 選擇 REMOVE USERS, GROUP OR ROLE (移除使用者、群組或角色)。
13. 在開啟的對話方塊中，檢閱資訊並確認其正確無誤，然後選擇 CONTINUE (繼續)。
14. 從左側導覽選單選擇 Portfolios list (組合清單)。
15. 在「本地產品組合」表中，搜尋名為「AWS Control Tower Account Factory 產品組合」的產品組合
16. 選擇該組合的圓形按鈕，然後選擇 DELETE PORTFOLIO (刪除組合)。
17. 在開啟的對話方塊中，檢閱資訊並確認其正確無誤，然後選擇 CONTINUE (繼續)。
18. 從左側導覽選單選擇 Product list (產品清單)。
19. 在「管理產品」頁面上，搜尋名為「Con AWS trol Tower Account Factory」的產品。
20. 選擇產品來開啟 Admin product details (管理產品詳細資訊) 頁面。
21. 從 Actions (動作)，選擇 Delete product (刪除產品)。
22. 在開啟的對話方塊中，檢閱資訊並確認其正確無誤，然後選擇 CONTINUE (繼續)。

移除 AWS Control Tower 角色和政策

這些程序會引導您如何清理 AWS Control Tower 在設定 landing zone 時或稍後建立的角色和政策。

若要刪除 IAM 身分中心 AWSServiceCatalogEndUserAccess 角色

1. 請在以下位置開啟 AWS IAM Identity Center 主控台。 https://console.aws.amazon.com/singlesignon/
2. 將 AWS 區域變更為主要區域，也就是您最初設定 AWS Control Tower 的區域。
3. 從左側導覽選單中選擇AWS 帳戶。
4. 選擇您的管理帳戶連結。
5. 選擇 [權限集] 下拉式清單，選取 AWSServiceCatalogEndUserAccess，然後選擇 [移除]。
6. 從左側面板中選擇AWS 帳戶。
7. 開啟 Permission sets (許可集) 標籤。
8. 選擇AWSServiceCatalogEndUserAccess並刪除它。

若要刪除 IAM 角色

1. 開啟位於 https://console.aws.amazon.com/iam/ 的 IAM 主控台。
2. 從左側導覽選單選擇 Roles (角色)。
3. 從表格中搜尋具有名稱的角色AWSControlTower。
4. 針對表格中的每個角色，執行以下作業：
   a. 選擇角色的核取方塊。
   b. 選擇 Delete role (刪除角色)。
   c. 在開啟的對話方塊中，檢閱資訊並確認其正確無誤，然後選擇 Yes, delete (是，刪除)。

若要刪除 IAM 政策

1. 開啟位於 https://console.aws.amazon.com/iam/ 的 IAM 主控台。
2. 從左側導覽選單選擇 Policies (政策)。
3. 從表格中搜尋具有名稱的策略AWSControlTower。
4. 針對表格中的每個政策，執行以下作業：
   a. 選擇政策的核取方塊。

b. 選擇 Policy actions (政策動作)，然後從下拉式選單選擇 Delete (刪除)。

c. 在開啟的對話方塊中，檢閱資訊並確認其正確無誤，然後選擇 Delete (刪除)。

AWS Control Tower 資源說明

如果您在移除 AWS Control Tower 資源時遇到無法解決的問題，請聯絡 Sup AWS port 部門。

如何解除使用 landing zone

若要解除使用 AWS Control 塔 landing zone 的委任，請按照此處提供的程序進行操作。

> **Note**
> 我們建議您在解除委任前取消管理已註冊帳戶。

1. 導覽至 AWS Control 塔主控台中的「登陸區域設定」 頁面。
2. 在 Decommission your landing zone (解除委任您的登陸區域) 區段中，選擇 Decommission your landing zone (解除委任您的登陸區域)。
3. 隨即出現一個對話方塊，說明您即將執行的動作，以及必要的確認程序。若要確認您打算解除委任，您必須選取每個方塊並依要求鍵入確認。

> **Important**
> 解除委任程序無法復原。

4. 如果您確認想要解除使用 landing zone，系統會在解除委任期間將您重新導向至 AWS Control Tower 首頁。此程序最多可能需要兩個小時。
5. 解除委任成功後，您必須手動刪除剩餘的資源，然後再從 AWS Control Tower 主控台設定新的 landing zone。這些剩餘資源包括一些特定的 Amazon S3 儲存貯體、組織和 CloudWatch 日誌日誌群組。

> **Note**
> 這些行動可能會對您的帳單和合規活動造成重大後果。例如，無法刪除這些資源可能會導致非預期的費用。

如需如何手動刪除資源的詳細資訊，請參閱關於移除 AWS Control Tower 資源。

6. 如果您打算在新區 AWS 域中設置新的 landing zone，請執行此額外步驟。透過 CLI 輸入下列指令：

```
aws organizations disable-aws-service-access --service-principal
 controltower.amazonaws.com
```

解除委任後所需的手動清除工作

- 如果您在解除委任後建立新的 landing zone，或遵循使用您自己現有的記錄封存或稽核帳戶的程序，則必須為記錄封存和稽核帳戶指定不同的電子郵件地址。
- 必須先手動刪除「 CloudWatch 記錄」記錄群組`aws-controltower/CloudTrailLogs`，才能設置其他 landing zone 域。
- 必須手動移除或重新命名兩個具有日誌保留名稱的 Amazon S3 儲存貯體。
- 您必須手動刪除或重新命名現有的安全性和沙箱組織單位。

> **Note**
>
> 您必須先刪除記錄和稽核帳戶，但不要刪除管理帳戶，才能刪除 AWS Control Tower 安全 OU 組織。若要刪除這些帳戶，您必須何時以 root 使用者身分登入稽核帳戶和日誌帳戶，並個別刪除它們。

- 您可能希望手動刪除 AWS Control Tower 的 AWS IAM Identity Center (IAM 身分中心) 組態，但可以繼續使用現有的 IAM 身分中心組態。
- 您可能希望移除 AWS Control Tower 建立的 VPC，並移除關聯的 AWS CloudFormation 堆疊集。
- 您必須遵循下列其他步驟，才能在新 AWS 區域中設置新的 landing zone 域。
  - 透過 CLI 輸入下列指令：

```
aws organizations disable-aws-service-access --service-principal
 controltower.amazonaws.com
```

- 從所有受控管區域的共用帳戶和成員帳戶中刪除其餘的受管理規則 (稱為AWSControlTowerManagedRule)。 AWSControlTowerManagedRule是一個 Amazon 的 EventBridge 規則。

解除 landing zone 後的設置

解除委任登陸區域之後，在手動清理完成之前，您無法再次成功執行安裝程式。此外，如果沒有手動清理這些剩餘資源，您可能會產生意外的帳單費用。您必須注意以下問題：

- AWS Control Tower 管理帳戶是 AWS Control Tower 根 OU 的一部分。請確定這些 IAM 角色和 IAM 政策已從管理帳戶中移除：
  - 角色：
    - AWSControlTowerAdmin
    - AWSControlTowerCloudTrailRole
    - AWSControlTowerStackSetRole
  - 政策：
    - AWSControlTowerAdminPolicy
    - AWSControlTowerCloudTrailRolePolicy
    - AWSControlTowerStackSetRolePolicy
- 您可能希望先刪除或更新 AWS Control Tower 的現有 IAM 身分中心組態，然後再次 landing zone，但不需要將其刪除。
- 您可能希望移除 AWS Control Tower 建立的 VPC。
- 如果為記錄或稽核帳 AWS 戶指定的電子郵件地址與現有帳戶相關聯，則安裝程式會失敗。您可以關閉 AWS 帳戶，或使用不同的電子郵件地址重新設定 landing zone。或者，您可以重複使用這些現有的共享帳戶，並具有允許您攜帶自己的日誌記錄和審計帳戶的功能。如需詳細資訊，請參閱 使用現有安全性或記錄帳戶的考量。
- 如果記錄帳戶中已存在具有下列保留名稱的 Amazon S3 儲存貯體，則安裝失敗：
  - aws-controltower-logs-*{accountId}*-*{region}* (用於日誌儲存貯體)。
  - aws-controltower-s3-access-logs-*{accountId}*-*{region}* (用於日誌記錄存取儲存貯體)。

您必須重新命名或移除這些儲存貯體，或為日誌帳戶使用不同的帳戶。

- 如果管理帳戶在記錄檔中具有現有的 CloudWatch 記錄群組`aws-controltower/CloudTrailLogs`，安裝程式會失敗。您必須重新命名或移除日誌群組。

在您設置一個新的 AWS 區域

如果您打算在新區 AWS 域中設置新的 landing zone，請遵循以下其他步驟。

- 透過 CLI 輸入下列指令：

```
aws organizations disable-aws-service-access --service-principal
 controltower.amazonaws.com
```

- 從所有受控管區域的共用帳戶和成員帳戶中刪除其餘的受管理規則 (稱為`AWSControlTowerManagedRule`)。

> **Note**
>
> 您無法在具有名為「安全性」或「沙箱」的頂層 OU 的組織中設定新的 landing zone。您必須重新命名或移除這些 OU，才能再次設定登陸區域。

故障診斷

如果您在使用 AWS Control Tower 時遇到問題，可以使用下列資訊根據我們的最佳實務解決問題。如果您遇到的問題超出了下列資訊的範圍，或者在您嘗試解決問題後仍然存在，請連絡 Sup AWS port 部門。

登陸區域啟動失敗

登陸區域啟動失敗的常見原因：

- 沒有回應確認電子郵件訊息。
- AWS CloudFormation StackSet 失敗。

確認電子郵件訊息：如果您的管理帳戶使用時間不到一小時，您可能會在建立其他帳戶時遇到問題。

採取動作

如果您遭遇此問題，請查看您的電子郵件。您可能已經收到正在等候回應的確認電子郵件。或者，若您發生此問題，我們建議您等待一個小時，然後再試一次。如果問題仍然存在，請聯絡 Sup AWS port 部門。

失敗 StackSets：導致 landing zone 啟動失敗的另一個可能原因是失 AWS CloudFormation StackSet 敗。 AWS 必須在 AWS Control Tower 管理的所有區域的管理帳戶中啟用安全性權杖服務 (STS) AWS 區域，才能成功佈建；否則，堆疊集將無法啟動。

採取動作

在啟動 AWS Control Tower 之前，請務必啟用所有必要的 AWS 安全性權杖服務 (STS) 端點區域。

若要檢視 AWS Control Tower 支援的 AWS 區域 清單，請參閱AWS 區域如何與 AWS Control Tower 搭配使用。

著陸區域不是最新的錯誤

如果您最近沒有更新 landing zone 域，嘗試重新獲得 AWS Control Tower 的存取權時可能會收到錯誤訊息。您可能會看到類似下列的錯誤訊息：

```
Unable to access Control Tower
```

您的帳戶已停用時間過長。由於閒置狀態，您必須更新 landing zone 才能存取 AWS Control Tower。

不過，您的 landing zone 更新可能會失敗。

採取的步驟

登入組織的管理帳戶，然後以 root 使用者身分登入。IAM 身分中心中的 IAM 使用者或使用者必須擁有 AWS Control Tower 管理員許可，並且是AWSControlTowerAdmins群組的一部分。然後再次嘗試更新。

新帳戶佈建失敗

如果您遇到這個問題，請檢查這些常見的原因。

填寫帳戶佈建表單時，您可能會有：

- 指定的 tagOptions、
- 啟用的 SNS 通知、
- 啟用的佈建產品通知。

再試一次佈建您的帳戶，而不指定這些選項中的任何選項。如需詳細資訊，請參閱 使用 AWS Service Catalog Account Factory 佈建帳戶 。

失敗的其他常見原因：

- 如果您已建立佈建產品計劃 (以檢視資源變更)，您的帳戶佈建可能會無限期地保持為 In progress (進行中) 狀態。
- 在 Account Factory 建立新帳戶將會失敗，而其他 AWS Control Tower 組態變更正在進行中。例如，當處理序正在執行以將控制項新增至 OU 時，如果您嘗試佈建帳戶，Account Factory 將會顯示錯誤訊息。

在 AWS Control Tower 中查看先前動作的狀態

- 導覽至 AWS CloudFormation > StackSets
- 檢查與 AWS Control Tower 相關的每個堆疊集 (前綴:"AWSControlTower「)
- 尋找仍在 AWS CloudFormation StackSets 執行中的作業。

如果您的帳戶佈建時間超過一小時，建議您終止佈建程序，然後再試一次。

註冊現有帳戶失敗

如果您嘗試註冊現有 AWS 帳戶一次，但該註冊失敗，則當您再次嘗試時，錯誤訊息可能會告訴您堆疊集存在。若要繼續，您必須在帳戶團隊中移除已佈建的產品。

如果第一次註冊失敗的原因是您忘記事先在帳戶中建立 `AWSControlTowerExecution` 角色，您會收到正確地告訴您建立角色的錯誤訊息。但是，當您嘗試建立角色時，您可能會收到另一個錯誤訊息，指出 AWS Control Tower 無法建立該角色。發生此錯誤是因為處理程序已部分完成。

在這種情況下，您必須採取兩個復原步驟，才能繼續註冊現有的帳戶。首先，您必須透過 AWS Service Catalog 主控台終止 Account Factory 佈建的產品。接下來，您必須使用 AWS Organizations 主控台手動將帳戶移出 OU，然後再移回根目錄。完成之後，請在帳戶中建立 `AWSControlTowerExecution` 角色，然後再次填寫 Enroll account (註冊帳戶) 表單。

註冊失敗的另一個可能原因是帳戶具有現有的 AWS Config 資源。在這種情況下，請參閱註冊具有現有 AWS Config 資源的帳戶，以取得如何修改現有資源的指示。

無法更新帳戶團隊帳戶

當帳戶處於不一致狀態時，無法從 Account Factory 或 AWS Service Catalog.

案例 1：您可能會遇到類似下列錯誤訊息：

```
AWS Control Tower could not baseline VPC in the managed account because of existing resource dependencies.
```

常見原因：AWS Control Tower 在初始佈建期間一律移除 AWS 預設 VPC。若要在帳戶中使用 AWS 預設 VPC，您必須在帳戶建立後新增它。AWS Control Tower 擁有自己的預設 VPC 來取代 AWS 預設 VPC，除非您按照逐步解說的方式設定 Account Factory，因此 AWS Control Tower 完全不會佈建 VPC。那麼該帳戶就沒有 VPC。如果要使用 AWS 預設 VPC，則必須重新新增預設 VPC。

不過，AWS Control Tower 不支援 AWS 預設 VPC。部署預設 VPC 的話，會導致帳戶進入 `Tainted` 狀態。處於該狀態時，您無法透過更新帳戶 AWS Service Catalog。

要採取的動作：您必須刪除新增的預設 VPC，然後才能更新帳戶。

> **Note**
>
> 狀`Tainted`態會導致後續問題：未更新的帳戶可能會阻止在其所屬 OU 上啟用控制項。

案例 2：您可能會看到類似下列錯誤訊息：

```
AWS Control Tower detects that your enrolled account has been moved to a
new organizational unit.
```

常見原因：您嘗試將帳戶從一個已註冊的 OU 移到另一個 OU，但舊的 AWS Config 規則仍然存在。帳戶處於不一致的狀態。

要採取的行動：

如果帳戶移動的目的是：

- 終止 Service Catalog 中的帳戶。
- 再次註冊。
- 內容/影響：部署的組 AWS Config 規則與目的地 OU 指定的組態不符。
- AWS Config 規則可能會保留在先前的 OU 中，導致非預期的支出。
- 由於資源命名衝突，嘗試重新註冊或更新帳號將失敗。

如果帳戶移動意外：

- 將帳戶返回其原始 OU。
- 從 Service Catalog 更新帳戶。
- 在啟動參數中，輸入帳戶原本所在的 OU。
- 內容/影響：如果帳戶未返回原始 OU，其狀態將與其所在的新 OU 指定的控制項不一致。
- 更新帳戶不是有效的補救措施，因為它不會刪除與其先前 OU 相關聯的 AWS Config 規則。

無法更新著陸區

如果更新失敗，AWS Control Tower 不會復原至先前的 landing zone 版本。您可能會發現您的 landing zone 處於不確定狀態。如果是這樣，請聯繫 AWS 支持。

著陸區更新可能會因為幾個原因而失敗。

- 不符合先決條件
- AWS Config 特定帳號中存在資源
- 存在關閉的帳戶

不符合先決條件

landing zone 更新必須符合與 landing zone 設置相同的先決條件。更新之前，請先檢閱啟動前檢查。

AWS Config 資源存在於安全性 OU 帳戶中

請勿在稽核和記錄封存帳戶中新增 AWS Config 資源。出現這些資源時，無法完成 landing zone 域更新程序。這些限制類似於第一次註冊帳戶或設置 landing zone 的限制。如需詳細資訊，請參閱註冊具有現有 AWS Config 資源的帳戶。

存在關閉的帳戶

當帳戶處於「已關閉」或「暫停」狀態時，您可能會在嘗試更新 landing zone 時遇到問題。您必須先刪除每個已關閉帳戶上佈建的產品，然後才能對 landing zone 域執行更新。

在 AWS Service Catalog 佈建的產品頁面上，您可能會看到類似下列錯誤訊息：

```
AWSControlTowerExecution role can't be assumed on the account.
```

常見原因：您已暫停帳戶，但未刪除已佈建的產品。

要採取的動作：如果您看到此錯誤，您有兩種選擇：

1. 聯絡 Sup AWS port 部門並重新開啟帳戶、刪除佈建的產品，然後再次關閉帳戶。
2. 移除因為帳號關閉而被遺棄的資源。 StackSets (只 StackSets 有在您未移除的「目前」狀態的實例時，才能使用此選項。)

若要從中移除資源 StackSets，請針對每個已關閉的帳號執行此動作：

- 進入每個 AWS Control Tower， StackSets 並針對已關閉的帳戶 StackInstances 從每個區域中移除。
- 重要事項：選擇「保留堆疊」選項，以便只 StackSet 移除堆疊執行個體。 StackSet 不能承擔來自已關閉帳戶的角色，因此如果嘗試擔任該`AWSControlTowerExecution`角色，它將失敗，從而導致您收到的錯誤消息。

提及的失敗錯誤 AWS Config

如果 AWS Config 在 AWS Control Tower 支援的任何 AWS 區域啟用，您可能會收到錯誤訊息，因為預先檢查失敗。由於某些基本行為，該消息似乎無法充分解釋問題。 AWS Config

您可能會收到如下的錯誤訊息：

- `AWS Control Tower cannot create an AWS Config delivery channel because one already exists. To continue, delete the existing delivery channel and try again .`
- `AWS Control Tower cannot create an AWS Config configuration recorder because one already exists. To continue, delete the existing delivery channel and try again .`

常見原因：在 AWS 帳戶上啟用 AWS Config 服務時，會使用預設命名建立組態記錄程式和傳遞通道。如果您透過主控台停用 AWS Config 服務，則不會刪除組態錄製程式或傳遞通道。您必須透過 CLI 刪除它們，或修改它們以供 AWS Control Tower 使用。如果在 AWS Control Tower 支援的任何一個區域中啟用 AWS Config 服務，則可能導致此失敗。

如果帳戶具有現有的 AWS Config 資源，請參閱註冊具有現有 AWS Config 資源的帳戶，以取得如何修改現有資源的指示。

採取動作：在所有支援的區域中，刪除組態記錄器和交付通路。禁用 AWS Config 是不夠的，配置記錄器和交付通道必須通過 CLI 來刪除。從 CLI 刪除組態記錄器和交付通道後，您可以再次嘗試啟動 AWS Control Tower 並註冊該帳戶。

如果您正在部署已佈建產品，則必須先刪除已佈建的產品，然後再重試。否則，您可能會看到類似下列錯誤訊息：

- `An error occurred (InvalidParametersException) when calling the ProvisionProduct operation: A stack named Stackname already exists.`

在訊息中，*Stackname*指定堆疊的名稱。

以下是一些可用來判斷組態記錄程式和傳遞通道狀態的 AWS Config CLI 命令範例。

檢視命令：

- `aws configservice describe-delivery-channels`
- `aws configservice describe-delivery-channel-status`
- `aws configservice describe-configuration-recorders`

- The normal response is something like "name": "default"

刪除命令：

- aws configservice stop-configuration-recorder --configuration-recorder-name *NAME-FROM-DESCRIBE-OUTPUT*
- aws configservice delete-delivery-channel --delivery-channel-name *NAME-FROM-DESCRIBE-OUTPUT*
- aws configservice delete-configuration-recorder --configuration-recorder-name *NAME-FROM-DESCRIBE-OUTPUT*

如需詳細資訊，請參閱 AWS Config 文件

- 管理組態錄製AWS 程式 (CLI)
- 管理交付通路

找不到啟動路徑錯誤

當您嘗試建立新帳戶時，可能會看到類似如下的錯誤訊息：

```
No launch paths found for resource: prod-dpqqfywxxxx
```

此錯誤訊息由產生 AWS Service Catalog，這是可協助在 AWS Control Tower 中佈建帳戶的整合服務。

常見原因：

- 您可能會以 root 身份登入。當您以 root 使用者身分登入時，AWS Control Tower 不支援建立帳戶。
- 您的 IAM 身分中心使用者尚未新增至適當的權限群組。您可能需要將您的 IAM Identity Center 使用者新增至下列其中一個權限群組：AWSAccountFactory(用於使用者存取) 或 AWSServiceCatalogAdmins(用於管理員存取權)。
- 如果您以 IAM 使用者身分驗證，則必須將其新增至 AWS Service Catalog 產品組合，以使其具有正確的許可。
- 如果您擁有正確的許可，但偵測到 AWS Control Tower 漂移，並且需要進行漂移修復，也會發生此問題。若要修復大多數類型的漂移，請在「著陸區設定」頁面上選擇「重設」。

收到權限不足錯誤

您的帳戶可能沒有執行某些工作的必要權限 AWS Organizations。如果遇到以下類型的錯誤，請檢查所有許可區域 (例如 IAM 或 IAM Identity Center 許可)，以確保不會從這些位置拒絕您的許可：

```
You have insufficient permissions to perform AWS Organizations API actions.
```

如果您認為自己的工作需要您嘗試採取的動作，而且找不到任何相關限制，請聯絡您的系統管理員或 Sup AWS port 部門。

Detective 控制項未對帳戶生效

如果您最近已將 AWS Control Tower 部署擴展到新 AWS 區域，則新套用的偵探控制不會對您在任何區域建立的新帳戶生效，直到更新 AWS Control Tower 管理的 OU 中的個別帳戶為止。現有帳戶上的現有偵測控制仍然有效。

如果您嘗試在更新帳戶之前啟用偵測控制項，您可能會看到類似下列錯誤訊息：

```
AWS Control Tower can't enable the selected control on this OU. AWS Control
Tower cannot apply the control on the OU ou-xxx-xxxxxxxx, because child
accounts have dependencies that are missing. Update all child accounts
under the OU, then try again.
```

要採取的動作：更新帳戶。

若要從 AWS Control Tower 主控台更新帳戶，請參閱何時更新 AWS Control Tower OU 和帳戶。

若要以程式設計方式更新多個個別帳戶，您可以使用來自 AWS Service Catalog 和 AWS CLI 的 API 來自動執行更新。如需如何處理更新程序的詳細資訊，請參閱此影片演練。 您可以將 UpdateProvisionedProductAPI 替換為視頻中顯示的 ProvisionProductAPI。

如果您在帳戶上啟用偵探控制時遇到進一步的困難，請聯絡 Sup AWS port 部門。

AWS Organizations API 傳回的速率超過錯誤

可能的原因

當 AWS Control Tower 執行每日掃描時，您的工作負載正在執行，以檢查您的 SCP 是否已漂移。

要遵循的步驟

如果遇到 API 節流或`rate exceeded`錯誤，請嘗試以下步驟：

- 在不同的時間執行您的工作負載。(請參閱 AWS Control Tower SCP 不變動掃描排程 (依區域)，瞭解 AWS Control Tower 何時執行稽核掃描。)
- 如果您直接透過 HTTP 呼叫 API：請使用 AWS SDK，該 SDK 會自動重試失敗的動作
- 透過 Service Quotas 與 Sup AWS port 要求提高限制

您可以在這裡找到 Elastic Beanstalk 中 API 節流的疑難排解說明的範例：`https://aws.amazon.com/premiumsupport/knowledge-center/elastic-beanstalk-api-throttling-errors/`

無法將 Account Factory 帳戶直接從一個 AWS Control Tower landing zone 移至另一個 AWS Control Tower landing zone

> **Warning**
>
> 此做法不符合符合資格帳戶註冊的先決條件，因為符合資格的帳戶必須屬於同一整個 AWS 組織，而且每個組織只能有一個 landing zone。如果您嘗試執行此動作，並且發現自己收到多個錯誤訊息，以下是一些可能會有所幫助的資訊。

若要將透過 Account Factory 佈建的帳戶移到另一個由 AWS Control Tower 管理的 landing zone，您必須從原始 OU 中移除所有 IAM 角色以及與該帳戶相關聯的堆疊。從部署帳號的每個區域移除這些資源。

> **Note**
>
> 移除資源的最佳方法是在嘗試移動帳戶之前，先取消佈建原始 OU 中的帳戶。

如果您不移除資源，新 OU 的註冊將會失敗，有點驚人。您可能會遇到一或多個錯誤訊息，而且您會繼續收到類似的錯誤訊息，直到從部署帳戶的每個區域移除剩餘的角色和堆疊為止。

每次收到錯誤訊息時，您都必須從新的 OU 移除帳號、刪除錯誤訊息主旨的舊資源，然後嘗試將帳號移回新的 OU。對於部署帳號的每個區域 (可能是 10 或 20 次)，每個剩餘資源都 removing-and-

deleting 必須重複此程序。發生這些重複錯誤的原因是帳戶已佈建到具有 SCP 防止 IAM 角色刪除的 OU 中。您可以在重試之前刪除帳號的所有資源，以縮短復原程序。

以下範例說明如果仍保留未刪除的角色和堆疊，您可能會收到的失敗訊息類型。只要保留舊資源，每次嘗試註冊帳戶時，您很可能會一次看到其中一個訊息。

範例中已修改資源 ID 字串的值。在您可能收到的錯誤消息中，它們的值不會相同。您可能會看到類似下列範例的訊息：

- AWS Control Tower cannot create the IAM role *aws-controltower-AdministratorExecutionRole* because the role already exists. To continue, delete the existing IAM role and try again.
- AWS Control Tower cannot create the IAM role *aws-controltower-ConfigRecorderRole* because the role already exists. To continue, delete the existing IAM role and try again.
- AWS Control Tower cannot create the IAM role *aws-controltower-ForwardSnsNotificationRole* because the role already exists. To continue, delete the existing IAM role and try again.

或者，您可能會看到有關堆疊集失敗的錯誤訊息，類似於以下內容：

```
"Error\":\"StackSetFailState\",
\"Cause\":\"StackSetOperation on AWSControlTowerBP-BASELINE-CLOUDWATCH
with id 8aXXXXf5-e0XX-4XXa-bc4XX-dXXXXXee31
has reached SUCCEEDED state but has 1 NON-CURRENT stack instances;
here is the summary :{ StackSet Id:
AWSControlTowerBP-BASELINE-CLOUDWATCH:40XXXbf2-Xead-46a1-XXXa-eXXXXecb2ee2,
Stack instance Id:
arn:aws:cloudformation:eu-west-1:1X23456789XX:
            stack/StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-4feXXXXXX-ecXX-XXc6-
bXXX-4ae678/4feXXXXXX-ecX-4ae123458,
Status: OUTDATED,
Status Reason: ResourceLogicalId:ForwardSnsNotification,
ResourceType:AWS::Lambda::Function,
ResourceStatusReason:aws-controltower-NotificationForwarder already exists in stack
arn:aws:cloudformation:eu-west-1:1X23456789XX:
            stack/StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-4feXXXXXX-ecXX-XXc6-
bXXX-4ae678/4feXXXXXX-ecX-4ae123458.
```

從第一個 OU 移除所有剩餘的資源之後，您就可以成功邀請、佈建或註冊帳戶到新的 OU。

AWS Support

如果您想要將現有的成員帳戶移至不同的支援方案，您可以使用根帳戶登入資料登入每個帳戶、比較方案以及設定您偏好的支援層級。

我們建議您在變更支援方案時，更新 MFA 和帳戶安全聯絡人。

基準線的類型

AWS Control Tower 中的基準是一組可套用至目標的資源和特定組態。最常見的基準目標可能是組織單位 (OU)。例如，您可以啟用選取作為目標的 OU 的基準，將該 OU 註冊到 AWS Control Tower。

在 landing zone 設定期間，基準目標可能是共用帳戶或整個 landing zone。根據您的 landing zone 域設定和規劃，可能會啟用和更新某些基準線。AWS Control Tower 會依照基準指定的方式，建立資源並將其部署到目標。

當您啟用目標的基準線時，基準線會顯示為 AWS CloudFormation 資源 (稱為`EnabledBaseline`資源)。

AWS Control Tower 包括四種基本類型的基準：

- 一種類型可以套用至已在 AWS Control Tower 註冊的 OU，或套用基準來註冊的 OU。
- 在初始設定期間或在 landing zone 域更新期間，三種基準類型可套用至 landing zone 域或共用帳戶。

在 OU 層級套用的基準類型，用於註冊和更新 OU

- 名稱: `AWSControlTowerBaseline`

  說明：為目標 OU 內的成員帳戶設定資源和強制控制，AWS Control Tower 管理所需。

  考量：此基準線會保留 landing zone 域「區域」拒絕控制的設定。換句話說，如果在 landing zone 層級不允許使用某個區域，則當您呼叫 `EnableBaseline` API 註冊 OU 時，該 OU 將不允許該區域進行該區域。

  > **Note**
  >
  > OU 層級的區域拒絕控制無法允許 landing zone 域拒絕控制的區域。

  如需詳細資訊，請參閱 AWS Organizations 說明文件中的 SCP 如何處理拒絕。

  建議：建議您在呼叫 OU 的 API 之前，先確認目標 OU 可能執行工作負載的區域，並對照 landing zone 域區域拒絕控制檢查結果，然後再呼叫 OU 的 `EnableBaseline` API，或者您可能無法存取特定區域中的資源。

> **Note**
>
> 連字線區域基準線的行為與 U 層級基準線不同。

AWS Control Tower 會在 landing zone 域設定和更新程序中自動啟用在 landing zone 層級套用的基準。您的 landing zone 域的基準線可能會隨著您變更 landing zone 域設定而變更。例如，如果您選擇使用 IAM 身分中心，AWS Control Tower 可以在您的 landing zone 啟用最新版本的`IdentityCenterBaseline`基準。

您可以透過 `ListEnabledBaselines` API 呼叫檢視您的 landing zone 域已啟用的基準。

可能適用於您的 landing zone 或共享帳戶的基準類型

- 名稱: `AuditBaseline`

  描述：設定資源以監視組織中帳號的安全性與合規性。您無法變更此基準，因為它是由 AWS Control Tower 部署。
- 名稱: `LogArchiveBaseline`

  描述：針對組織中帳號的 API 活動和資源組態設定記錄，設定中央儲存庫。您無法變更此基準，因為它是由 AWS Control Tower 部署。
- 名稱: `IdentityCenterBaseline`

  描述：為 IAM 身分中心設定共用資源，`AWSControlTowerBaseline`以準備為帳戶設定身分中心存取權限。

  注意事項：只有在您最初設定 landing zone 時選取 IAM 身分中心做為身分提供者，或者您隨後變更登陸區域設定以為 landing zone 域啟用 IAM 身分中心時，此基準才有效。如果您使用不同的身分識別提供者，您將無法存取啟用此基準。

部分註冊帳戶

當您使用基準時，可以將帳戶置於稱為「部分已註冊」的狀態。

如果您透過呼叫 `ResetEnabledBaseline` API 重新註冊 OU，就會發生此狀態，因為 AWS Control Tower 僅將必要資源套用至目標 OU 中的帳戶。缺少其父 OU 的選擇性資源 (控制項) 的帳戶會標示為部分已註冊。

如果您將未註冊的帳戶移到已註冊的 OU，然後呼叫 OU 上的 ResetEnabledBaseline API 來註冊該帳戶，AWS Control Tower 會將與該帳戶相關聯的資源套用到AWSControlTowerBaseline新註冊的帳戶。不過，針對此 OU 啟用的選擇性控制項不會套用至帳戶。帳戶會維持「部分註冊」狀態。

若要完全註冊帳戶，請在主控台中選擇 [重新註冊] 或 [更新帳戶]。當您從主控台選取這些操作時，AWS Control Tower 會將該 OU 的所有資源套用到新註冊的帳戶，包括為該 OU 啟用的選用控制項。

AWS Control Tower 主控台和基準 API 之間的操作差異

當您變更 OU 的管理狀態時，AWS Control Tower 主控台會自動為您執行更多操作，相較於透過基準的 API 變更管理。

差異

- 註冊和佈建產品

  當您透過主控台註冊 OU 時，AWS Control Tower 會為 OU 的成員帳戶建立 Service Catalog 產品，作為註冊每個帳戶的一部分。當您透過 EnableBaseline API 註冊 OU 時AWSControlTowerBaseline，AWS Control Tower 不會為 OU 中的成員帳戶建立佈建的產品。
- 取消註冊 OU

  每當您取消註冊 OU 時，都必須先移除所有成員帳戶和巢狀 OU。然後，AWS Control Tower 會移除套用至 OU 的所有控制。

  - 如果您選取從主控台刪除 OU 的 OU，AWS Control Tower 會繼續取消註冊，然後從組織中刪除 OU。
  - 不過，如果您透過呼叫 DisableBaseline API AWSControlTowerBaseline 從 OU 移除來取消註冊 OU，AWS Control Tower 不會從您的組織刪除 OU，則組織中仍未註冊 OU。

基準線和版本預設值

如果您的 AWS Control Tower landing zone 已設定，然後您選擇啟用 landing zone 基準，則 AWS Control Tower 會啟用與您的 landing zone 版本相容的最新版本基準。如果您選擇為尚未向 AWS Control Tower 註冊的 OU 啟用基準，AWS Control Tower 會自動為該 OU 提供最新的相容基準版本。

OU 基準和 landing zone 版本的相容性

如果您的企業需要，AWS Control Tower 基準可讓您在 OU 層級設定管理標準，而不是在 landing zone 層級設定。呼叫AWSControlTowerBaseline的基準可協助您向 AWS Control Tower 註冊 OU。

> **Note**
>
> 基準是一組控制項和資源，可共同運作，在您的 landing zone 內建立穩定的治理環境。

當您在 OU 上啟用基準時，透過呼叫 AWS Control Tower 中的 EnableBaseline API，您必須指定與目前 AWS Control Tower landing zone 版本相容的基準版本。指定基準之後，OU 中的所有成員帳戶都會遵循針對 OU 指定的基準。換句話說，新帳戶隨著更新的基準佈建，現有的成員帳戶會根據新的基準進行管理。

如果您未為現有 OU 和帳戶選取基準，landing zone 版本預設會決定整個控管狀態。不過，您 landing zone 中的每個註冊 OU 都會指派一個基準版本，這是與您目前 landing zone 版本相容的最新基準。因此，每個 OU 和已註冊的成員帳戶都有相關聯的基準，即使您從未特別指派基準線。

對於 OU 層級基準AWSControlTowerBaseline，下表顯示基準與 AWS Control Tower landing zone 版本的相容性。

基準版本	著陸區版本	包括藍圖	包含的控制	從上一個基準線變更	
1.0	2 至 2	基礎線路, 基礎線程, 雲觀察, BP 基線配置, 基礎線角色, 基礎線角色, 基本服務角色, IAM 資源	所有強制性控制	無	
2.0	2 至 2 分鐘	基礎線路, BP 基線雲觀察, BP 基線	所有強制性控制	新增 AWS Config 服務連結角色 (SLR)	

基準版本	著陸區版本	包括藍圖	包含的控制	從上一個基準線變更	
		Config, 基線角色, 基礎線角色, 角色, 組態 SLR, IAM 資源		和新的 Config 藍圖以使用 SLR	
3.0	3 至 3 分鐘	基線雲觀察, BP 基線 Config, 基線角色, 基線角色, 配置單反, IAM 資源	所有強制性控制	新 AWS Config 藍圖。更改為僅在本地區記錄全球資源。已移除 CloudTrail 藍圖	
4.0	三點二至三點三	基線雲觀察, BP 基線 Config, BP 基線角色, 基礎線角色, 基本服務鏈接角色, BP_ 基線服務角色, 配置 SLR, IAM 資源	所有強制性控制	全新單反藍圖	

如需設定 landing zone 域時在帳號中建立之特定資源的詳細資訊，請參閱共用帳戶中建立的資源。

如果您將 landing zone 域更新為支援較新`AWSControlTowerBaseline`基準版本的版本，且新的 landing zone 版本與您現有的基準版本相容，則您的 OU 狀態會變更為「可用的更新」。

- 您可以繼續使用帳戶工廠和其他功能，而不立即更新 OU 基準，但從 2.x 更新到 3.x 的 landing zone 域除外。
- 在此 OU 中註冊的新帳戶會根據現有的基準版本接收資源，直到基準版本更新為止 (使用主控台中的延伸控管功能，或透過 `UpdateEnabledBaseline` API)。

- 更新基準版本之後，該 OU 內的所有帳戶都會根據新的基準版本接收資源。

> **Note**
>
> 如果您將 AWS Control Tower landing zone 從任何 2.X 版本更新為任何版本 3.X，則由於帳戶層級追蹤變更為組織層級追蹤，您也必須更新 OU 上的基準版本。 AWS CloudTrail 在主控台中，您的 OU 會顯示 [需要更新] 狀態。

基準線的考量

- 如果您的 OU 需要基準更新，則無法佈建新帳戶或將現有帳戶註冊到該 OU。
- 在 landing zone 更新之後，如果您還計劃更新 OU 基準，則必須以程式設計方式重新註冊 OU 或更新 OU 基準版本。
- 我們建議您將所使用的 landing zone 版本更新為最高相容基準，以便獲得 landing zone 和基準線合併的所有優點。例如，如果您更新為 3.3 版的 landing zone 域，您可以繼續使用基線 3.0，但除非您同時更新至基線 4.0，否則您將無法獲得 3.3 版 landing zone 域的所有好處。
- 無法復原基準更新。
- 基準啟用一次以一個 OU 為目標。因此，當父 OU 更新時，巢狀 OU 不會自動更新。我們建議您在更新巢狀 OU 之前，先更新父 OU。
- 當您從主控台呼叫 `UpdateEnabledBaseline` API 或重新註冊 OU 時，OU 會保留基準更新之前啟用的所有控制項。
- 當多個基準版本與您的 landing zone 版本相容時，如果您在未受管理的 OU 上啟用基準，則必須使用最新的基準版本。

範例：僅使用 API 註冊 AWS Control Tower OU

此範例逐步解說是隨附文件。如需說明、注意事項和更多資訊，請參閱。基準線的類型

先決條件

您必須擁有尚未在 AWS Control Tower 註冊且想要註冊的現有 OU。或者，您必須擁有已註冊的 OU，您想要重新註冊以進行更新。

註冊 OU

1. 檢查IdentityCenterBaseline是否已啟用平 landing zone。如果是這樣，請取得已啟用識別中心的基準識別碼。

```
aws controltower list-baselines --query 'baselines[?name==`IdentityCenterBaseline`].
[arn]'
```

```
aws controltower list-enabled-baselines --query 'enabledBaselines[?
baselineIdentifier==`<Identity Center Baseline Arn>`].[arn]'
```

2. 取得目標 OU 的 ARN。

```
aws organizations describe-organizational-unit --organizational-unit-id
 <Organizational Unit ID> --query 'OrganizationalUnit.[Arn]'
```

3. 取得AWSControlTowerBaseline基準線的 ARN。

```
aws controltower list-baselines --query 'baselines[?name==`AWSControlTowerBaseline`].
[arn]'
```

4. 在目標 OU 上建立AWSControlTowerBaseline基準。

   如果已啟用身分識別中心基準：

```
aws controltower enable-baseline --baseline-identifier <AWSControlTowerBaseline ARN>
 --baseline-version <BASELINE VERSION> --target-identifier <OU ARN> --parameters
 '[{"key":"IdentityCenterEnabledBaselineArn","value":"<Identity Center Enabled
 Baseline ARN>"}]'
```

   如果未啟用身分識別中心基準，請忽略*parameters*旗標，如下所示：

```

aws controltower enable-baseline --baseline-identifier <AWSControlTowerBaseline ARN>
 --baseline-version <BASELINE VERSION> --target-identifier <OU ARN>
```

重新註冊 OU

在您更新 landing zone 域設定或更新 landing zone 域版本之後，您必須重新註冊 OU 以提供最新的變更。請依照下列步驟重設關聯的EnabledBaseline資源，以程式設計方式重新註冊 OU。

1. 取得要重新註冊之目標 OU 的 ARN。

```
aws organizations describe-organizational-unit --organizational-unit-id <OU ID> --
query 'OrganizationalUnit.[Arn]'
```

2. 取得目標 OU 之EnabledBaseline資源的 ARN。

```
aws controltower list-enabled-baselines --query 'enabledBaselines[?
targetIdentifier==`<OUARN>`].[arn]'
```

3. 重設啟用的基準線。

```
aws controltower reset-enabled-baseline --enabled-baseline-
identifier <EnabledBaselineArn>
```

基準 API 用法的範例

本節包含 AWS Control Tower 基準 API 的輸入和輸出參數範例。

DisableBaseline

如需此 API 作業的詳細資訊，請參閱DisableBaseline。

DisableBaseline輸入：

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/AB12CD34EF56GH789"
}
```

DisableBaseline輸出：

```
{
    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
}
```

DisableBaselineCLI 範例：

```
aws controltower disable-baseline \
    --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/AB12CD34EF56GH789 \
```

```
    --region us-west-2
```

EnableBaseline

如需此 API 作業的詳細資訊，請參閱EnableBaseline。

EnableBaseline輸入：

```
{
    "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline:17BSJV3IGJ2QSGA2",
    "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-kgj0txdhpa/ou-
r9mj-4j3mzjql",
    "baselineVersion": "3.0",
    "parameters": [
        {
            "key": "IdentityCenterEnabledBaselineArn",
            "value": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ"
        }
    ]
}
```

EnableBaseline輸出：

```
{
    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f",
    "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ"
}
```

EnableBaselineCLI 範例：

此範例顯示啟用由 AWS Control Tower 管 AWS Organizations 理的 landing zone 選擇加入 AWS IAM 身分中心存取權的組織的基準。若要擷取您的身分中心EnabledBaseline識別碼，您可以呼叫 ListEnabledBaselines API，並根據身分中心基準進行篩選：(arn:aws:controltower:*Region*::baseline/LN25R72TTG6IGPTQ)

```
aws controltower list-enabled-baselines \
    --filter baselineIdentifiers=arn:aws:controltower:us-west-2::baseline/
LN25R72TTG6IGPTQ \
    --region us-west-2
```

響應將顯示EnabledBaseline詳細信息，顯示其標識符。

```
{
    "enabledBaselines": [
        {
            "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHXS7P6C4I453EZC",
            "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/
LN25R72TTG6IGPTQ",
            "targetIdentifier": "arn:aws:organizations::123456789012:account/o-
aq21sw43de5/123456789012",
            "statusSummary": {
                "status": "SUCCEEDED"
            }
        }
    ]
}
```

> **Note**
>
> 記下回應中的 ARN 值，並將此值作為參數傳遞，以啟用預設基準線。

```
aws controltower enable-baseline \
    --baseline-identifier arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2 \
    --baseline-version 3.0 \
    --target-identifier arn:aws:organizations::123456789012:ou/o-aq21sw43de5/ou-po90-
lk87jh65 \
    --parameters
 '[{"key":"IdentityCenterEnabledBaselineArn","value":"arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC"}]' \
    --region us-west-2
```

對於已選擇退出 IAM 身分中心 AWS Control Tower 管理的 landing zone 的組織，請啟用不含參數的基準。

```
aws controltower enable-baseline \
    --baseline-identifier arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2 \
    --baseline-version 3.0 \
    --target-identifier arn:aws:organizations::123456789012:ou/o-aq21sw43de5/ou-po90-
lk87jh65 \
```

```
    --region us-west-2
```

GetBaseline

如需此 API 作業的詳細資訊，請參閱GetBaseline。

GetBaseline輸入：

```
{
    "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2"
}
```

GetBaseline輸出：

```
{
    "arn": "arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2",
    "name": "AWSControlTowerBaseline",
    "description": "Sets up resources and mandatory controls for member accounts within
 the target OU, required for AWS Control Tower governance.",
}
```

GetBaselineCLI 範例：

```
aws controltower get-baseline \
    --baseline-identifier arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2 \
    --region us-west-2
```

GetBaselineOperation

如需此 API 作業的詳細資訊，請參閱GetBaselineOperation。

GetBaselineOperation輸入：

```
{
    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
}
```

GetBaselineOperation輸出：

```
{
```

```
    "baselineOperation": {
        "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f",
        "operationType": "DISABLE_BASELINE",
        "status": "FAILED",
        "startTime": "2023-01-12T19:05:00Z",
        "endTime": "2023-01-12T19:45:00Z",
        "statusMessage": "Can't perform DisableBaseline on a parent target with
 governed child OUs"
    }
}
```

GetBaselineOperationCLI 範例：

```
aws controltower get-baseline-operation \
    --operation-identifier 58f12232-26be-4735-a3e9-dd30d90f021f \
    --region us-west-2
```

GetEnabledBaseline

如需此 API 作業的詳細資訊，請參閱GetEnabledBaseline。

GetEnabledBaseline輸入：

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHCR4CJTSI4W07MZ"
}
```

GetEnabledBaseline輸出：

```
{
    "enabledBaselineDetails": {
        "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ",
        "baselineIdentifier": "arn:aws:controltower:us-
west-2::baseline:17BSJV3IGJ2QSGA2",
        "baselineVersion": "3.0",
        "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-kgj0txdhpa/ou-
r9mj-4j3mzjql",
        "statusSummary": {
            "status": "SUCCEEDED",
```

```
            "lastOperationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
        },
        "parameters": [
            {
                "key": "IdentityCenterEnabledBaselineArn",
                "value": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ"
            }
        ]
    }
}
```

GetEnabledBaselineCLI 範例：

```
aws controltower get-enabled-baseline \
    --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC \
    --region us-west-2
```

ListBaselines

如需此 API 作業的詳細資訊，請參閱ListBaselines。

ListBaselines輸入（使用可選輸入）：

```
{
    "nextToken": "AbCd1234",
    "maxResults": "4"
}
```

ListBaselines輸出：

```
{
    "baselines": [
        {
            "arn": "arn:aws:controltower:us-west-1::baseline/4T4HA1KMO10S6311",
            "name": "AuditBaseline",
            "description": "Sets up resources to monitor security and compliance of
 accounts in your organization."
        },
        {
            "arn": "arn:aws:controltower:us-west-1::baseline/J8HX46AHS5MIKQPD",
```

```
            "name": "LogArchiveBaseline",
            "description": "Sets up a central repository for logs of API activities and
 resource configurations from accounts in your organization."
        },
        {
            "arn": "arn:aws:controltower:us-west-1::baseline/LN25R72TTG6IGPTQ",
            "name": "IdentityCenterBaseline",
            "description": "Sets up shared resources for AWS Identity Center, which
 prepares the AWSControlTowerBaseline to set up Identity Center access for accounts."
        },
        {
            "arn": "arn:aws:controltower:us-west-1::baseline/17BSJV3IGJ2QSGA2",
            "name": "AWSControlTowerBaseline",
            "description": "Sets up resources and mandatory controls for member
 accounts within the target OU, required for AWS Control Tower governance."
        }
    ]
}
```

ListBaselinesCLI 範例：

```
aws controltower list-baselines \
    --region us-west-2
```

ListEnabledBaselines

如需此 API 作業的詳細資訊，請參閱ListEnabledBaselines。

ListEnabledBaselines輸入（無過濾器）：

```
{
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 5
}
```

ListEnabledBaselines輸入（僅限baselineIdentifiers過濾器）：

```
{
    "filter": {
        "baselineIdentifiers": ['arn:aws:controltower:us-
east-1::baseline/17BSJV3IGJ2QSGA2', 'arn:aws:controltower:us-
east-1::baseline/12GZU8CKZKVMS2AW']
```

```
    },
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 5
}
```

ListEnabledBaselines輸入（僅限targetIdentifiers過濾器）：

```
{
    "filter": {
        "targetIdentifiers": ['arn:aws:organizations::123456789012:ou/o-s9511vn103/ou-
xqj7-fex1u317', 'arn:aws:organizations::123456789012:ou/o-s9511vn103/ou-xqj7-11q6n2cf']
    },
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 2
}
```

ListEnabledBaselines輸入（baselineIdentifiers和targetIdentifiers過濾器）：

```
{
    "filter": {
        "baselineIdentifiers": ['arn:aws:controltower:us-
east-1::baseline/17BSJV3IGJ2QSGA2']
        "targetIdentifiers": ['arn:aws:organizations::123456789012:ou/o-s9511vn103/ou-
xqj7-fex1u317']
    },
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 5
}
```

ListEnabledBaselines輸出：

```
{
    "enabledBaselines": [
        {
            "arn": "arn:aws:controltower:us-east-1:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ",
            "baselineIdentifier": "arn:aws:controltower:us-
east-1::baseline:17BSJV3IGJ2QSGA2",
            "baselineVersion": "3.0",
            "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-kgj0txdhpa/
ou-r9mj-4j3mzjql",
            "statusSummary": {
```

```
                "status": "SUCCEEDED",
                "lastOperationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
            }
        },
        {
            "arn": "arn:aws:controltower:us-east-1:123456789012:enabledbaseline/
XAJ9NKW88AA4W9CLL",
            "baselineIdentifier": "arn:aws:controltower:us-
east-1::baseline:17BSJV3IGJ2QSGA2",
            "baselineVersion": "4.0",
            "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-s9511vn103/
ou-xqj7-fex1u317",
            "statusSummary": {
            "status": "FAILED",
                "lastOperationIdentifier": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"
            }
        }
    ],
    "nextToken": "e2bXXXXX6cab"
}
```

帶有一種過濾器類型的 CLI 示例（baselineIdentifiers過濾器）：

```
aws controltower list-enabled-baselines \
    --filter baselineIdentifiers=arn:aws:controltower:us-
west-2::baseline/17BSJV3IGJ2QSGA2,arn:aws:controltower:us-west-2::baseline/
LN25R72TTG6IGPTQ \
    --region us-west-2
```

使用多個過濾器（baselineIdentifiers和過濾targetIdentifiers器）的 CLI 示例：

```
aws controltower list-enabled-baselines \
    --filter targetIdentifiers=arn:aws:organizations::123456789012:ou/o-
aq21sw43de5/ou-po90-lk87jh65,baselineIdentifiers=arn:aws:controltower:us-
west-2::baseline/17BSJV3IGJ2QSGA2 \
    --region us-west-2
```

ResetEnabledBaseline

如需此 API 作業的詳細資訊，請參閱ResetEnabledBaseline。

ResetEnabledbaseline輸入：

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAJ9NKW88AA4W9CLL"
}
```

ResetEnabledBaseline輸出：

```
{
    "operationIdentifier": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"
}
```

ResetEnabledBaselineCLI 範例：

```
aws controltower reset-enabled-baseline \
    --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC \
    --region us-west-2
```

UpdateEnabledBaseline

如需此 API 作業的詳細資訊，請參閱UpdateEnabledBaseline。

UpdateEnabledBaseline輸入：

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
east-1:123456789012:enabledbaseline/XAJ9NKW88AA4W9CLL",
    "baselineVersion": "4.0",
    "parameters": [
        {
            "key": "IdentityCenterEnabledBaselineArn",
            "value": "arn:aws:controltower:us-east-1:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ"
        }
    ]
}
```

UpdateEnabledBaseline輸出：

```
{
```

```
    "operationIdentifier": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"
}
```

UpdateEnabledBaselineCLI 範例：

```
aws controltower update-enabled-baseline \
    --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC \
    --baseline-version 4.0
    --parameters
 '[{"key":"IdentityCenterEnabledBaselineArn","value":"arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC"}]' \
    --region us-west-2
```

相關資訊

本主題列出 AWS Control Tower 功能和其他增強功能的常見使用案例和最佳實務。本主題也包含相關部落格文章、技術文件和相關資源的連結，這些資源可協助您在使用 AWS Control Tower 時提供協助。

教程和實驗室

- AWS Control Tower 實驗室 — 這些實驗室提供與 AWS Control Tower 相關的常見任務的高階概觀。
- 如果您有使用案例，但不確定從何開始，請在 AWS Control Tower 儀表板上選擇取得個人化指導。
- 嘗試瀏覽精選 YouTube 影片清單，其中詳細說明如何使用 AWS Control Tower 功能。

聯網

為中 AWS的網路設定可重複且可管理的模式。進一步瞭解客戶常用的設計、自動化和設備。

- AWS 快速入門 VPC 人雲端架構 — 本快速入門指南根據 AWS 雲端基礎架構的 AWS 最佳做法，提供網路基礎架構。它會建立具有公用和私有子網路的 AWS Virtual Private Network 環境，讓您可以在其中啟動 AWS 服務和其他資源。
- AWS Control Tower 中使用 AWS 服務目錄的自助服務 VPC — 此部落格文章說明設定 Account Factory 的方法，讓您可以使用自訂 VPC 佈建帳戶。
- 在 AWS Control Tower 中實作無伺服器傳輸網路控制器 (STNO) — 此部落格文章示範如何自動化跨帳戶的網路連線存取。此部落格適用於 AWS Control Tower 管理員，或負責在其 AWS 環境中管理網路的管理員。

安全性、身分識別和記錄

延伸您的安全狀態、與外部或現有的身分識別提供者整合，並集中記錄系統。

安全性

- 使用 AWS Control Tower 生命週期事件自動化 AWS Security Hub 提醒 — 此部落格文章說明如何在現有和新帳戶的 AWS Control Tower 多帳戶環境中自動啟用和設定 Security Hub。

- 啟用 AWS Identity and Access Management — 此部落格文章說明如何透過啟用和集中化 IAM Access Analyzer 發現項目來增強組織的安全可見度。
- AWS Systems Manager Parameter Store 為組態資料管理和機密管理提供安全的階層式儲存。您可以使用它在安全位置共用組態資訊，以供 AWS Systems Manager 和 AWS 使用 CloudFormation。例如，您可以儲存要在其中部署一致性套件的區域清單。

身份

- 將 Azure AD 使用者身分連結至 AWS 帳戶和應用程式以進行單一登入 — 此部落格文章說明如何將 Azure AD 與 IAM 身分中心和 AWS Control Tower 搭配使用。
- 透過以下方式集中管理 Okta 使用者對 AWS 的存取 AWS IAM Identity Center— 此部落格文章說明如何將 Okta 與 IAM 身分中心和 AWS Control Tower 搭配使用。

日誌

- AWS 集中式記錄解決方案 — 此解決方案文章描述了集中式記錄解決方案，該解決方案使組織能夠 AWS 跨多個帳戶和 AWS 區域收集，分析和顯示日誌。

部署資源和管理工作負載

部署和管理資源和工作負載。

- 入門庫集成-這篇博客文章描述入門投資組合，你可以使用。
- 將雲端託管人持續部署到 AWS Control Tower

使用現有組織和帳戶

使用現有的 AWS 組織和帳戶。

- 註冊帳戶 — 此使用者指南主題說明如何在 AWS Control Tower 中註冊現有 AWS 帳戶。
- 將帳戶帶到 AWS Control Tower 下 — 此部落格文章說明如何將 AWS Control Tower 部署到您現有的 AWS 組織。
- 使用 AWS Config 一致性套件擴展 AWS Control Tower 管理 — 此部落格文章說明如何部署一 AWS Config 致性套件，以協助將現有帳戶和組織納入 AWS Control Tower 的管理中。

- 如何使用 AWS Control Tower 偵測和緩解護欄違規 — 此部落格文章說明如何新增控制項以及如何訂閱 SNS 通知，以便透過電子郵件收到控制合規違規情況的通知。

自動化與整合

使用 AWS Control Tower 自動化帳戶建立並整合生命週期事件。

- 生命週期事件 — 此部落格文章說明如何搭配 AWS Control Tower 使用生命週期事件。
- 自動化帳戶建立 — 此部落格文章說明如何在 AWS Control Tower 中設定自動化帳戶建立。
- Amazon VPC 流程日誌自動化 — 此部落格文章說明如何在多帳戶環境中自動化和集中管理 Amazon VPC 流程日誌。
- 使用 AWS Control Tower 生命週期事件自動化 VPC 標記 — 此部落格文章說明如何透過 AWS Control Tower 中的生命週期事件自動化 VPC 的資源標記。
- 自動化帳戶管理 — 此部落格文章說明如何在 AWS Control Tower 環境設定完成後自動化帳戶管理任務。

移轉工作量

搭配 AWS Control Tower 使用其他 AWS 服務來協助工作負載移轉。

- CloudEndure 遷移 — 此部落格文章說明如何將 CloudEndure 其他 AWS 服務與 AWS Control Tower 結合使用，以協助進行工作負載移轉。

相關 AWS 服務

AWS Control Tower 充當的 AWS Organizations協調層。因此，透過 AWS Organizations 主控台和 API，您可以存取與 AWS 控制塔搭配使用的其他 20 多種 AWS 服務。這些額外的服務無法直接透過 AWS Control 塔主控台存取。

- 如需 AWS Control Tower 透過 AWS Organizations 提供的完整服務清單，請參閱可與 AWS 組織搭配使用的 AWS Organizations 服務。
- 若要為這些相關 AWS 服務啟用多帳戶功能，您必須啟用受信任的存取權。如需詳細資訊，請參閱將 AWS Organizations 與其他 AWS 服務搭配使用。

> **Note**
>
> 請記住 AWS Config， AWS IAM 身分中心和 AWS CloudTrail 已在 AWS Control Tower 中為您設置並完全集成。您不需要修改這些服務的信任存取或委派管理設定。

- 透過提供的某些 AWS 服務 AWS Organizations 可以使用委派管理，包括 AWS Systems Manager 和 AWS Firewall Manager。如需詳細資訊，請參閱設定委派的系統管理員和啟用 Firewall Manager 員的委派系統管理員帳戶。另請參閱此影片：使用 AWS Firewall Manager 設定安全群組。

AWS Marketplace 解決方

探索來自 AWS Marketplace.

- AWS Control Tower Marketplace — 為 AWS Control Tower AWS Marketplace 提供廣泛的解決方案，協助您整合第三方軟體。這些解決方案有助於解決關鍵基礎架構和作業使用案例，包括身分識別管理、多帳戶環境的安全性、集中式網路、營運智慧，以及安全性資訊與事件管理 (SIEM)。

AWS Control Tower 版本注意事項

以下各節顯示需要更新 AWS Control 塔 landing zone 的 AWS Control Tower 版本的詳細資訊，以及自動整合到服務中的版本。

功能和版本會依照正式向公眾宣布的日期，依時間順序反向排列 (最新的優先順序)。由於在記錄功能或版本的記錄與正式宣布之間可能存在延遲，因此此處列出的功能或發行日期可能會與中的日期略有不同文件歷史記錄。

2024 年發行的功能

2023 年發布的功能

2022 年發行的功能

2021 年發布的功能

2020 年發布的功能

2019 年發布的功能

二零二四年一月至今

自 2024 年 1 月起，AWS Control Tower 已發佈下列更新：

- AWS Control Tower 最多支援 100 個同時控制操作
- AWS Control Tower 於 AWS 加拿大西部 (卡加立) 提供
- AWS Control Tower 支援自助配額調整
- AWS Control Tower 發行控制參考指南
- AWS Control Tower 更新和重新命名兩個主動控制
- 已淘汰的控制項不再可用
- AWS Control Tower 支援標記`EnabledControl`資源 AWS CloudFormation
- AWS Control Tower 支援使用基準進行 OU 註冊和組態的 API

AWS Control Tower 最多支援 100 個同時控制操作

2024年5月20日

AWS Control Tower landing zone 不需要更新。)

AWS Control Tower 現在支援具有更高並行性的多重控制操作。您可以從主控台或使用 API 同時跨多個組織單位 (OU) 提交多達 100 個 AWS Control Tower 控制操作。最多可同時執行十 (10) 個作業，而其他作業則會排入佇列。如此一來，您就可以跨多個設定更標準化的組態 AWS 帳戶，而不會產生重複控制作業的作業負擔。

若要監控進行中和排入佇列的控制操作的狀態，您可以瀏覽至 AWS Control Tower 主控台中新的最近操作頁面，或者呼叫新的 `ListControlOperations`API。

AWS Control Tower 程式庫包含 500 多個控制項，可對應到不同的控制目標、架構和服務。對於特定控制目標 (例如靜態加密資料)，您可以透過單一控制作業啟用多個控制項，以協助您達成目標。此功能有助於加速開發、更快地採用最佳實務控制項，並減少營運複雜性。

AWS Control Tower 於 AWS 加拿大西部 (卡加立) 提供

2024年5月3日

AWS Control Tower landing zone 不需要更新。)

從今天開始，您可以在加拿大西部 (卡加立) 區域啟用 AWS Control Tower。如果您已部署 AWS Control Tower，並且想要將其控管功能擴展到此區域，則可以使用 AWS Control 塔 landing zone 域 API 來完成。或者從主控台前往 AWS Control Tower 儀表板中的「設定」頁面，選取您的區域，然後更新您的 landing zone 域。

加拿大西部 (卡加利) 地區不支援 AWS Service Catalog。因此，AWS Control Tower 的某些功能不同。最顯著的功能變化是 Account Factory 不可用。如果您選擇加拿大西部 (卡加立) 作為您的本地區域，則更新帳戶、設定帳戶自動化，以及任何其他涉及 Service Catalog 的程序會與其他區域不同。

佈建帳戶

若要在加拿大西部 (卡加利) 區域建立和佈建新帳戶，建議您在 AWS Control Tower 以外建立帳戶，然後將其註冊到已註冊的 OU。如需詳細資訊，請參閱註冊現有帳戶和註冊帳戶的步驟。

加拿大西部 (卡加利) 地區不提供 Service Catalog API。在 AWS Control Tower (依 Service Catalog API) 自動化帳戶佈建中顯示的範例指令碼無法運作。

由於 AWS Control Tower 缺少其他基本相依性，加拿大西部 (卡加利) 無法使用 Account Factory 自訂 (AFC)、Terraform Account Factory (AFT) 和 AWS Control Tower (CFCT) 的自訂項目。如果您將管理擴展到加拿大西部 (卡加利) 區域，只要您的本地區域提供 Service Catalog，就可以在 AWS Control Tower 支援的所有區域繼續管理 AFC 藍圖。

控制

AWS Security Hub 服務管理標準的主動控制和控制：加拿大西部 (卡加利) 區域不提供 AWS Control Tower。加拿大西部（卡爾加里）不提供預防控制CT.CLOUDFORMATION.PR.1，因為僅在激活基於鉤子的主動控件時才需要此控制。某些基於的偵探控制 AWS Config 項無法使用。如需詳細資訊，請參閱控制限制。

身份提供者

加拿大西部 (卡加立) 不提供 IAM 身分中心。最佳做法建議是在提供 IAM 身分中心的區域中設定您的登陸區域。或者，如果您在加拿大西部 (卡爾加里) 使用外部身分提供者，則可以選擇自行管理帳戶存取設定。

加拿大西部 (卡加利) 區域的 Service Catalog 不會對 AWS Control Tower 支援的其他區域造成影響。這些差異僅適用於您的所在地區是加拿大西部（卡爾加里）。

如需提供 AWS Control Tower 的完整區域清單，請參閱AWS 區域表。

AWS Control Tower 支援自助配額調整

2024年4月25日

AWS Control Tower landing zone 不需要更新。)

AWS Control Tower 現在可透過 Service Quotas 主控台支援自助配額調整。如需詳細資訊，請參閱 請求提高配額。

AWS Control Tower 發行控制參考指南

2024年4月21 日

AWS Control Tower landing zone 不需要更新。)

AWS Control Tower 發行了《控制參考指南》，這是一份新文件，您可以在其中找到 AWS Control 塔環境專屬控制的詳細資訊。此資料之前已包含在 AWS Control Tower 使用者指南中。控制項參考指南涵蓋了展開格式的控制項。如需詳細資訊，請參閱 AWS Control Tower 控制參考指南。

AWS Control Tower 更新和重新命名兩個主動控制

2024年3月26日

AWS Control Tower landing zone 不需要更新。)

AWS Control Tower 已重新命名兩個主動控制，以配合 Amazon OpenSearch 服務的更新。

- [CT.OPENSEARCH.PR.8] 需要彈性搜索服務域才能使用 TLSv1.2
- [CT.OPENSEARCH.PR.16] 需要 Amazon OpenSearch 服務域才能使用 TLSv1.2

我們更新了這兩個控制項的控制名稱和成品，以與 Amazon OpenSearch 服務的最新版本保持一致，該服務現在支援傳輸層安全性 (TLS) 1.3 版，在其網域端點安全性的傳輸安全性選項中支援傳輸層安全性 (TLS) 1.3 版。

若要為這些控制項新增 TLSv1.3 的支援，我們已更新控制項的成品和名稱，以反映控制項的意圖。他們現在會評估服務網域的最低 TLS 版本。若要在您的環境中進行此更新，您必須停用和啟用控制項，才能部署最新的成品。

此變更不會影響其他主動控制項。我們建議您檢閱這些控制項，以確保這些控制項符合您的控制目標。

如有問題或疑慮，請聯絡 Sup AWS port 部門。

已淘汰的控制項不再可用

2024年3月12日

AWS Control Tower landing zone 不需要更新。)

AWS Control Tower 已棄用某些控制項。這些控制項已不再可用。

- CT.ATHENA.PR.1
- CT.CODEBUILD.PR.4
- CT.AUTOSCALING.PR.3
- SH.Athena.1
- SH.Codebuild.5
- SH.AutoScaling.4
- SH.SNS.1
- SH.SNS.2

AWS Control Tower 支援標記**EnabledControl**資源 AWS CloudFormation

2024年2月22 日

AWS Control Tower landing zone 不需要更新。)

此 AWS Control Tower 發行版本更新EnabledControl資源的行為，以更好地與可設定的控制項保持一致，並透過自動化提升管理 AWS Control Tower 環境的能力。在此版本中，您可以透過 AWS CloudFormation 範本將標籤新增至可設定的EnabledControl資源。之前，您只能透過 AWS Control Tower 主控台和 API 新增標籤。

AWS Control Tower GetEnabledControl 和 ListTagsforResource API 操作會隨此版本進行更新，因為它們仰賴資EnabledControl源功能。EnableControl

如需詳細資訊，請參閱 AWS Control Tower 和AWS CloudFormation 使用者指南*EnabledControl*中的標記EnabledControl資源。

AWS Control Tower 支援使用基準進行 OU 註冊和組態的 API

2024年2月14日

AWS Control Tower landing zone 不需要更新。)

這些 API 支援透過EnableBaseline呼叫進行程式設計 OU 註冊。當您在 OU 上啟用基準時，OU 內的成員帳戶就會註冊到 AWS Control Tower 管理。某些警告可能適用。例如，透過 AWS Control 塔主控台註冊 OU 可啟用選擇性控制項以及強制性控制。呼叫 API 時，您可能需要完成額外的步驟，以便啟用選用的控制項。

AWS Control Tower 基準體現了 OU 和成員帳戶 AWS Control Tower 管理的最佳實務。例如，當您在 OU 上啟用基準時，OU 內的成員帳戶會收到已定義的資源群組 AWS CloudTrail AWS Config，包括 IAM 身分中心和必要的 AWS IAM 角色。

特定基準與特定 AWS Control Tower landing zone 版本相容。當您變更 landing zone 域設定時，AWS Control Tower 可以將最新的相容基準套用至您的 landing zone 域。如需詳細資訊，請參閱 OU 基準和 landing zone 版本的相容性。

此版本包括四個基本 基準線的類型

- AWSControlTowerBaseline
- AuditBaseline
- LogArchiveBaseline
- IdentityCenterBaseline

使用新的 API 和定義的基準，您可以註冊 OU 並自動化您的 OU 佈建工作流程。這些 API 也可以管理已受 AWS Control Tower 管理的 OU，因此您可以在 landing zone 更新後重新註冊 OU。這些 API 包含對 AWS CloudFormation `EnabledBaseline`資源的支援，可讓您使用基礎結構即程式碼 (IaC) 來管理 OU。

基準線 API

- EnableBaseline、UpdateEnabledBaseline、DisableBaseline：對 OU 的基準採取動作。
- GetEnabledBaseline、ListEnabledBaselines：探索已啟用基準的組態。
- GetBaselineOperation：檢視特定基準線作業的狀態。
- ResetEnabledBaseline：使用啟用的基準線 (包括巢狀 OU 和強制控制偏移) 修正 OU 上的資源漂移。還修復了區 landing-zone-level 域拒絕控制的漂移
- GetBaseline、ListBaselines：探索 AWS Control Tower 基準的內容。

若要進一步了解這些 API，請參閱 AWS Control Tower 使用者指南中的基準和 API 參考。提供 AWS Control Tower 的新 API AWS 區域 可供使用，但 GovCloud (美國) 區域除外。如需 AWS Control Tower 可供使用的 AWS 區域 清單，請參閱 AWS 區域 表格。

二零二三年一月至今

自 2023 年 1 月起，AWS Control Tower 已發佈下列更新：

- 轉換為新的 AWS Service Catalog 外部產品類型（第 3 階段）
- AWS Control Tower landing zone 3.3 版
- 轉換為新的 AWS Service Catalog 外部產品類型（第二階段）
- AWS Control Tower 宣佈針對數位主權提供協助的控制
- AWS Control Tower 支援 landing zone 域 API
- AWS Control Tower 支援已啟用控制的標記
- AWS Control Tower 於亞太區域 (墨爾本) 區域提供
- 轉換為新的 AWS Service Catalog 外部產品類型（第一階段）
- 提供新的控制 API
- AWS Control Tower 新增其他控制
- 報告的新漂移類型：受信任存取已停用
- 四個額外 AWS 區域

- AWS Control Tower 於特拉維夫區域提供
- AWS Control Tower 推出 28 個新的主動式控制
- AWS Control Tower 棄用兩個控制
- AWS Control Tower landing zone 3.2 版
- AWS Control Tower 根據 ID 處理帳戶
- AWS Control Tower 控制程式庫提供的其他 Security Hub 偵測控制
- AWS Control Tower 發佈控制中繼資料表
- Account Factory 定制的地形支持
- AWS 適用於 landing zone 的 IAM 身分中心自我管理
- AWS Control Tower 處理 OU 的混合式管控問題
- 提供其他主動式控制
- 更新的 Amazon EC2 主動控制
- 7 個額外 AWS 區域 可用
- 地形表單 (AFT) 帳戶自訂要求追蹤的 Account Factory
- AWS Control Tower landing zone 3.1 版
- 一般提供主動式控制

轉換為新的 AWS Service Catalog 外部產品類型（第 3 階段）

2023年12月14日

AWS Control Tower landing zone 不需要更新。）

建立新產品時，AWS Control Tower 不再支援 Terraform 開放原始碼做為產品類型 (藍圖)。 AWS 帳戶如需更新帳戶藍圖的詳細資訊和指示，請參閱轉換為 AWS Service Catalog 外部產品類型。

如果您未更新帳戶藍圖以使用外部產品類型，則只能更新或終止您使用 Terraform 開放原始碼藍圖佈建的帳戶。

AWS Control Tower landing zone 3.3 版

2023年12月14日

AWS Control Tower landing zone 需要更新至 3.3 版。 若要取得資訊，請參閱〈更新您的登陸區域〉。

AWS Control Tower 稽核帳戶中 S3 儲存貯體政策的更新

我們已修改 AWS Control Tower 在帳戶中部署的 Amazon S3 稽核儲存貯體政策，因此任何寫入許可都必須符合`aws:SourceOrgID`條件。在此版本中，只有當要求來自您的組織或組織單位 (OU) 時，AWS 服務才能存取您的資源。

您可以使用`aws:SourceOrgID`條件金鑰，並在 S3 儲存貯體政策的條件元素中將值設定為組織 ID。這種情況可確保 CloudTrail 只能代表組織內的帳戶將日誌寫入 S3 儲存貯體；它可防止組織外部的 CloudTrail 日誌寫入 AWS Control Tower S3 儲存貯體。

我們進行此變更是為了修復潛在的安全性弱點，而不會影響現有工作負載的功能。若要檢視更新的策略，請參閱稽核帳戶中的 Amazon S3 儲存貯體政策。

如需有關新條件金鑰的詳細資訊，請參閱 IAM 文件和標題為「針對存取資源的 AWS 服務使用可擴展控制項」的 IAM 部落格文章。

AWS Config SNS 主題中的政策更新

我們已將新的`aws:SourceOrgID`條件金鑰新增至 AWS Config SNS 主題的原則。若要檢視更新的原則，請參閱 AWS Config SNS 主題原則。

landing zone 域「區域拒絕」控制的更新

- 已移除`discovery-marketplace:`。這項行動受`aws-marketplace:*`豁免所涵蓋。
- 已新增 `quicksight:DescribeAccountSubscription`

更新的 AWS CloudFormation 模板

我們更新了名為堆棧的 AWS CloudFormation 模板，`BASELINE-CLOUDTRAIL-MASTER`以便在不使用 AWS KMS 加密時不顯示漂移。

轉換為新的 AWS Service Catalog 外部產品類型（第二階段）

2023年12月7日

AWS Control Tower landing zone 不需要更新。）

HashiCorp 更新了他們的地形版授權。因此，將對 Terraform 開放原始碼產品和佈建產品的支援 AWS Service Catalog 變更為新的產品類型，稱為「外部」。

為避免帳戶中現有的工作負載和 AWS 資源受到干擾，請在 2023 年 12 月 14 日之前，依照轉換為 AWS Service Catalog 外部產品類型中的 AWS Control Tower 轉換步驟進行操作。

AWS Control Tower 宣佈針對數位主權提供協助的控制

2023年11月27日

AWS Control Tower landing zone 不需要更新。)

AWS Control Tower 宣布推出 65 個新的 AWS受管控制項，協助您符合數位主權要求。在此版本中，您可以在 AWS Control Tower 主控台的新數位主權群組下探索這些控制項。您可以使用這些控制項來協助防止有關資料存放區、細微存取限制、加密和恢復能力的資源變更，並偵測資源變更。這些控制項的設計目的是讓您能夠更輕鬆地處理大規模需求。如需有關數位主權控制的詳細資訊，請參閱加強數位主權保護的控制項。

例如，您可以選擇啟用有助於強制執行加密和恢復策略的控制項，例如需要 AWS AppSync API 快取以啟用傳輸過程中的加密或需要跨多個可用區域部署 AWS Network Firewall。您也可以自訂 AWS Control Tower 區域拒絕控制，套用最符合您獨特業務需求的區域限制。

此版本帶來強化的 AWS Control Tower 區域拒絕功能。您可以在 OU 層級套用新的參數化 Region 拒絕控制，以提高治理的細微性，同時在 landing zone 層級維持其他區域治理。這個可自訂的區域拒絕控制可協助您套用最符合您獨特業務需求的區域限制。如需新的可設定區域拒絕控制項的相關資訊，請參閱套用至 OU 的區域拒絕控制。

作為新區域拒絕增強功能的新工具，此版本包含新的 APIUpdateEnabledControl，可讓您將已啟用的控制項重設為預設設定。在需要快速解決漂移問題或以程式設計方式保證控制項不處於漂移狀態的使用案例時，此 API 特別有用。如需有關新 API 的詳細資訊，請參閱 AWS Control Tower API 參考

全新的主動控制

- CT.APIGATEWAY.PR.6：要求 Amazon API Gateway REST 網域使用安全政策，以指定 TLSv1.2 的最低 TLS 通訊協定版本
- CT.APPSYNC.PR.2：需要使用私有可見性來設定 AWS AppSync GraphQL API
- CT.APPSYNC.PR.3：要求未使用 API 金鑰驗證 AWS AppSync GraphQL API
- CT.APPSYNC.PR.4：需要 AWS AppSync GraphQL API 快取才能啟用傳輸中的加密功能。
- CT.APPSYNC.PR.5：需要 AWS AppSync GraphQL API 快取才能啟用靜態加密。
- CT.AUTOSCALING.PR.9：需要透過 Amazon EC2 自動擴展啟動組態設定的 Amazon EBS 磁碟區，才能加密靜態資料
- CT.AUTOSCALING.PR.10：覆寫啟動範本時，要求 Amazon EC2 自動擴展群組僅使用 AWS Nitro 執行個體類型

- CT.AUTOSCALING.PR.11：覆寫啟動範本時，僅需要將支援執行個體之間網路流量加密的 AWS Nitro 執行個體類型新增至 Amazon EC2 Auto Scaling 群組
- CT.DAX.PR.3：需要 DynamoDB 加速器叢集使用傳輸層安全性 (TLS) 來加密傳輸中的資料
- CT.DMS.PR.2：需要 AWS Database Migration Service (DMS) 端點來加密來源和目標端點的連線
- CT.EC2.PR.15：從`AWS::EC2::LaunchTemplate`資源類型建立時，要求 Amazon EC2 執行個體使用 AWS Nitro 執行個體類型
- CT.EC2.PR.16：使用`AWS::EC2::Instance`資源類型建立時，要求 Amazon EC2 執行個體使用 AWS Nitro 執行個體類型
- CT.EC2.PR.17：需要 Amazon EC2 專用主機才能使用 AWS 硝基執行個體類型
- CT.EC2.PR.18：要求 Amazon EC2 叢集僅覆寫具有 AWS Nitro 執行個體類型的啟動範本
- CT.EC2.PR.19：使用資源類型建立時，要求 Amazon EC2 執行個體使用硝基執行個體類型，該類型支援執行個體之間的傳輸中加密 `AWS::EC2::Instance`
- CT.EC2.PR.20：要求 Amazon EC2 叢集僅覆寫具有支援在執行個體之間傳輸加密的 AWS Nitro 執行個體類型的啟動範本
- CT.ELASTICACHE.PR.8：需要使用較新 Redis 版本的 Amazon ElastiCache 複寫群組，才能啟用 RBAC 身份驗證
- CT.MQ.PR.1：要求 Amazon MQ ActiveMQ 代理程式使用主動/待命部署模式以獲得高可用性
- CT.MQ.PR.2：需要 Amazon MQ 兔子 MQ 代理程式使用異地同步備份叢集模式以獲得高可用性
- CT.MSK.PR.1：需要適用於 Apache Kafka (MSK) 叢集的 Amazon 受管串流，才能在叢集代理程式節點之間強制執行傳輸過程中的加密
- CT.MSK.PR.2：需要將 Apache 卡夫卡 (MSK) 叢集的 Amazon 受管串流設定為停用狀態 PublicAccess
- CT.NETWORK-FIREWALL.PR.5：需要跨多個可用區域部署 AWS Network Firewall 防火牆
- CT.RDS.PR.26：需要 Amazon RDS 資料庫代理才能要求傳輸層安全性 (TLS) 連線
- CT.RDS.PR.27：要求 Amazon RDS 資料庫叢集參數群組需要支援的引擎類型的傳輸層安全性 (TLS) 連線
- CT.RDS.PR.28：要求 Amazon RDS 資料庫參數群組需要支援的引擎類型的傳輸層安全性 (TLS) 連線
- CT.RDS.PR.29：要求 Amazon RDS 叢集未設定為可透過 'PubliclyAccessible' 內容公開存取
- CT.RDS.PR.30：要求 Amazon RDS 資料庫執行個體已設定靜態加密，以使用您為支援的引擎類型指定的 KMS 金鑰
- CT.S3.PR.12：要求 Amazon S3 存取點具有區塊公用存取 (BPA) 組態，且所有選項都設定為 true

新的預防性控制

- CT.APPSYNC.PV.1需要使用私有可見性來設定 AWS AppSync GraphQL API
- CT.EC2.PV.1需要從加密的 EC2 磁碟區建立 Amazon EBS 快照
- CT.EC2.PV.2需要將連接的 Amazon EBS 磁碟區設定為加密靜態資料
- CT.EC2.PV.3要求 Amazon EBS 快照無法公開還原
- CT.EC2.PV.4要求 Amazon EBS 直接 API 不被調用
- CT.EC2.PV.5不允許使用 Amazon EC2 虛擬機器導入和導出
- CT.EC2.PV.6不允許使用已淘汰的 Amazon EC2 RequestSpotFleet 和 RequestSpotInstances API 操作
- CT.KMS.PV.1要求一個 AWS KMS 關鍵策略有一個限制對 AWS 服務 AWS KMS 授予創建的聲明
- CT.KMS.PV.2要求具有用於加密的 RSA 金鑰材料的 AWS KMS 非對稱金鑰不具有 2048 位元的金鑰長度
- CT.KMS.PV.3要求在 AWS KMS 啟用略過原則鎖定安全檢查的情況下設定金鑰
- CT.KMS.PV.4需要使用源自 CloudHSM 的金鑰材料來設定 AWS KMS 客戶管理金鑰 (CMK) AWS
- CT.KMS.PV.5要求使用匯入的金鑰材料設定 AWS KMS 客戶管理金鑰 (CMK)
- CT.KMS.PV.6要求 AWS KMS 客戶管理金鑰 (CMK) 設定使用源自外部金鑰存放區 (XKS) 的金鑰材料
- CT.LAMBDA.PV.1需要 AWS Lambda 函數 URL 才能使用基於 AWS IAM 的身份驗證
- CT.LAMBDA.PV.2需要將 AWS Lambda 函數 URL 配置為僅由內部的主參與者訪問 AWS 帳戶
- 根據組織單位的要求 AWS 拒絕存取 AWS 區域

新的偵測控制可增強您的數位主權治理態勢，是 AWS Security Hub 服務管理的標準 AWS Control Tower 的一部分。

全新偵探控制

- SH.ACM.2：ACM 管理的 RSA 憑證應使用至少 2,048 位元的金鑰長度
- SH.AppSync.5：不應使用 API 金鑰驗證 AWS AppSync GraphQL API
- SH.CloudTrail.6：確保用於存放 CloudTrail 日誌的 S3 儲存貯體無法公開存取：
- SH.DMS.9：DMS 端點應使用 SSL
- SH.DocumentDB.3: Amazon DocumentDB 手動叢集快照不應該是公開的
- SH.DynamoDB.3：DynamoDB 加速器 (DAX) 叢集應在靜態時加密

- SH.EC2.23：EC2 傳輸閘道不應自動接受 VPC 附件請求
- SH.EKS.1: EKS 叢集端點不應可公開存取
- SH.ElastiCache.3： ElastiCache 複寫群組應啟用自動容錯移轉
- SH.ElastiCache.4： ElastiCache 複製群組應該已 encryption-at-rest 啟用
- SH.ElastiCache.5： ElastiCache 複製群組應該已 encryption-in-transit 啟用
- SH.ElastiCache.6：舊版 Redis 的 ElastiCache 複寫群組應啟用 Redis 的 AUTH
- SH.EventBridge.3: EventBridge 自訂事件匯流排應附有以資源為基礎的政策
- SH.KMS.4： AWS KMS 鍵旋轉應該啟用
- SH.Lambda.3：Lambda 函數應該位於 VPC 中
- SH.MQ.5: ActiveMQ 代理程式應該使用主動/待命部署模式
- SH.MQ.6: RabbitMQ 代理程式應該使用叢集部署模式
- SH.MSK.1：MSK 叢集應在代理程式節點之間的傳輸過程中加密
- SH.RDS.12：應為 RDS 叢集設定 IAM 身分驗證
- SH.RDS.15：應針對多個可用區域設定 RDS 資料庫叢集
- SH.S3.17：S3 儲存貯體應使用 AWS KMS 金鑰進行靜態加密

如需新增至 AWS Security Hub 服務管理標準 AWS Control Teck 塔的控制的詳細資訊，請參閱文件中適用於服務管理標準的控制：AWS Control Tower。 AWS Security Hub

如需不支援 AWS Security Hub 服務管理標準 AWS Control 塔一部分之某些控制項的清單，請參閱不支援的區域。 AWS 區域

OU 層級的區域拒絕的新可設定控制項

CT.MULTIPERVE.PV.1：此控制項接受參數，以指定在 OU 層級 (而非整個 AWS Control Tower 登陸區域) 允許的豁免區域、IAM 主體和動作。這是一種預防性控制，由服務控制策略（SCP）實施。

如需詳細資訊，請參閱套用至 OU 的區域拒絕控制。

`UpdateEnabledControl` API

此 AWS Control Tower 版本為控制新增了以下 API 支援：

- 更新後的 `EnableControl` API 可以設定可設定的控制項。
- 更新的 `GetEnabledControl` API 會顯示已啟用控制項上的已設定參數。
- 新的 `UpdateEnabledControl` API 可以在已啟用的控制項上變更參數。

如需詳細資訊，請參閱 AWS Control Tower API 參考。

AWS Control Tower 支援 landing zone 域 API

2023 年 11 月 26 日

AWS Control Tower landing zone 不需要更新。)

AWS Control Tower 現在支援 landing zone 域組態和使用 API 啟動。您可以使用 API 建立、更新、取得、列出、重設和刪除登陸區域。

下列 API 可讓您使用 AWS CloudFormation 或以程式設計方式設定和管理 landing zone 域。 AWS CLI

AWS Control Tower 支援下列登陸區域的 API：

- `CreateLandingZone`— 此 API 呼叫會使用 landing zone 版本和資訊清單檔案建立 landing zone。
- `GetLandingZoneOperation`此 API 呼叫會傳回指定 landing zone 作業的狀態。
- `GetLandingZone`此 API 呼叫會傳回有關指定 landing zone 的詳細資訊，包括版本、資訊清單檔案和狀態。
- `UpdateLandingZone`— 此 API 呼叫會更新 landing zone 版本或資訊清單檔案。
- `ListLandingZone`— 此 API 呼叫會針對管理帳戶中的 landing zone 設定傳回一個 landing zone 識別碼 (ARN)。
- `ResetLandingZone`— 此 API 呼叫會將 landing zone 重設為最新更新時指定的參數，以修復漂移。如果尚未更新 landing zone 域，此呼叫會將 landing zone 域重置為建立時指定的參數。
- `DeleteLandingZone`— 此 API 呼叫會取消對 landing zone 域的委任。

若要開始使用 landing zone API，請參閱使用 API 開始使用 AWS Control Tower.

AWS Control Tower 支援已啟用控制的標記

2023年11月10日

AWS Control Tower landing zone 不需要更新。)

AWS Control Tower 現在可透過 AWS Control Tower 主控台或透過 API 支援已啟用控制的資源標記。您可以新增、移除或列出已啟用控制項的標籤。

隨著下列 API 的發行版本，您可以為在 AWS Control Tower 中啟用的控制設定標籤。標籤可協助您管理、識別、組織、搜尋和篩選資源。您可建立標籤，依照用途、擁有者、環境或其他條件分類資源。

AWS Control Tower 支援下列 API 進行控制標記：

- `TagResource`— 此 API 呼叫會將標籤新增至 AWS Control Tower 中啟用的控制項。
- `UntagResource`— 此 API 呼叫會從 AWS Control Tower 中啟用的控制移除標籤。
- `ListTagsForResource`— 此 API 呼叫會傳回 AWS Control Tower 中啟用之控制項的標籤。

AWS Control Tower 控制 API 可在 AWS 區域 其中使用 AWS Control Tower 控制塔控制 API。如需提供 AWS Control Tower 的 AWS 區域 完整清單，請參閱AWS 區域表。如需 AWS Control Tower API 的完整清單，請參閱 API 參考。

AWS Control Tower 於亞太區域 (墨爾本) 區域提供

2023年11月3日

AWS Control Tower landing zone 不需要更新。)

AWS Control Tower 在亞太區域 (墨爾本) 區域提供。

如果您已經在使用 AWS Control Tower，而且想要將其管理功能擴展到帳戶中的這個區域，請前往 AWS Control Tower 儀表板中的「設定」頁面，選取區域，然後更新您的 landing zone 域。在 landing zone 域更新之後，您必須更新受 AWS Control Tower 管理的所有帳戶，以便在新區域中管理您的帳戶和 OU。如需詳細資訊，請參閱關於更新。

如需 AWS Control Tower 可使用的區域完整清單，請參閱AWS 區域 表格。

轉換為新的 AWS Service Catalog 外部產品類型（第一階段）

2023年10月31 日

AWS Control Tower landing zone 不需要更新。)

HashiCorp 更新了他們的地形版授權。因此，Terraform 開放原始碼產品和已佈建產品的支援 AWS Service Catalog 更新為新產品類型 (稱為「外部」)。

AWS Control Tower 不支援依賴於 AWS Service Catalog 外部產品類型的 Account Factory 自訂。為避免帳戶中現有的工作負載和 AWS 資源受到干擾，請在 2023 年 12 月 14 日之前按照以下建議順序執行 AWS Control Tower 轉換步驟：

1. 升級您現有的 Terraform 參考引擎， AWS Service Catalog 以包含對外部和 Terraform 開放原始碼產品類型的支援。如需有關更新 Terraform 參考引擎的指示，請檢閱儲存AWS Service Catalog GitHub 庫。

2. 移至 AWS Service Catalog 並複製任何現有的 Terraform 開放原始碼藍圖，以使用新的外部產品類型。請勿終止現有的 Terraform 開放原始碼藍圖。
3. 繼續使用現有的 Terraform 開放原始碼藍圖在 AWS Control Tower 中建立或更新帳戶。

提供新的控制 API

2023年10月14日

AWS Control Tower landing zone 不需要更新。)

AWS Control Tower 現在支援額外的 API，您可以用來大規模部署和管理 AWS Control Tower 控制。如需 AWS Control Tower 控制 API 的詳細資訊，請參閱 API 參考。

AWS Control Tower 新增了新的控制 API。

- `GetEnabledControl`API 呼叫提供有關已啟用控制項的詳細資訊。

我們也更新了這個 API：

`ListEnabledControls`— 此 API 呼叫會列出 AWS Control Tower 在指定組織單位上啟用的控制項及其包含的帳戶。它現在會傳回`EnabledControlSummary`物件中的其他資訊。

使用這些 API，您可以透過程式設計方式執行多項常見作業 例如：

- 從 AWS Control Tower 控制程式庫取得您已啟用的所有控制清單。
- 對於任何已啟用的控制項，您都可以取得有關支援控制項的區域、控制項的識別碼 (ARN)、控制項的漂移狀態，以及控制項狀態摘要的相關資訊。

AWS Control Tower 控制 API 可在 AWS 區域 其中使用 AWS Control Tower 控制塔控制 API。如需提供 AWS Control Tower 的 AWS 區域 完整清單，請參閱AWS 區域表。如需 AWS Control Tower API 的完整清單，請參閱 API 參考。

AWS Control Tower 新增其他控制

2023年10月5 日

AWS Control Tower landing zone 不需要更新。)

AWS Control Tower 宣布推出新的主動式和偵探控制。

AWS Control Tower 中的主動控制是透過 AWS CloudFormation Hook 來實作，可在佈建不合 AWS CloudFormation 規資源之前識別並封鎖這些資源。主動式控制可補充 AWS Control 塔中現有的預防和偵測控制功能。

全新的主動控制

- [CT.ATHENA.PR.1] 要求亞馬遜 Athena 工作組在靜態時加密雅典娜查詢結果
- [CT.ATHENA.PR.2] 要求亞馬遜 Athena 工作群組使用 AWS Key Management Service (KMS) 金鑰加密雅典娜靜態查詢結果
- [CT.CLOUDTRAIL.PR.4] 需要 AWS CloudTrail Lake 事件數據存儲才能使用密 AWS KMS 鑰啟用靜態加密
- [CT.DAX.PR.2] 要求 Amazon DAX 叢集將節點部署到至少三個可用區域
- [CT.EC2.PR.14] 需要透過 Amazon EC2 啟動範本設定的 Amazon EBS 磁碟區來加密靜態資料
- [CT.EKS.PR.2] 要求使用金 AWS 鑰管理服務 (KMS) 金鑰使用秘密加密來設定 Amazon EKS 叢集
- [CT.ELASTICLOADBALANCING.PR.14] 要求 Network Load Balancer 啟用跨區域負載平衡
- [CT.ELASTICLOADBALANCING.PR.15] 要求 Elastic Load Balancing v2 目標群組未明確停用跨區域負載平衡
- [CT.EMR.PR.1] 要求將 Amazon EMR (EMR) 安全組態設定設定為加密 Amazon S3 中的靜態資料
- [CT.EMR.PR.2] 要求將 Amazon EMR (EMR) 安全組態設定設定為使用金鑰加密 Amazon S3 中的靜態資料 AWS KMS
- [CT.EMR.PR.3] 要求使用密鑰使用 EBS 卷本地磁盤加密配置 Amazon EMR（EMR）安全組態 AWS KMS
- [CT.EMR.PR.4] 要求將 Amazon EMR (EMR) 安全組態設定設定為加密傳輸中的資料
- [CT.GLUE.PR.1] 要求 AWS Glue 作業具有關聯的安全配置
- [CT.GLUE.PR.2] 需要 AWS Glue 安全組態才能使用 AWS KMS 金鑰加密 Amazon S3 目標中的資料
- [CT.KMS.PR.2] 要求具有用於加密的 RSA 密鑰材料的 AWS KMS 非對稱密鑰的密鑰長度大於 2048 位
- [CT.KMS.PR.3] 要求一個 AWS KMS 關鍵策略有一個限制對 AWS 服務 AWS KMS 授予創建的聲明
- [CT.LAMBDA.PR.4] 需要 AWS Lambda 層權限才能授予對 AWS 組織或特定 AWS 帳戶的訪問權限
- [CT.LAMBDA.PR.5] 需要 AWS Lambda 函數 URL 才能使用 AWS 基於 IAM 的身份驗證
- [CT.LAMBDA.PR.6] 需要 AWS Lambda 函數 URL CORS 策略來限制對特定來源的訪問
- [CT.NEPTUNE.PR.4] 需要 Amazon Neptune 資料庫叢集才能為稽核日誌啟用 Amazon CloudWatch 日誌匯出

- [CT.NEPTUNE.PR.5] 要求 Amazon Neptune 資料庫叢集將備份保留期設定為大於或等於 7 天
- [CT.REDSHIFT.PR.9] 要求 Amazon Redshift 叢集參數群組設定為使用安全通訊端層 (SSL) 來加密傳輸中的資料

這些新的主動式控制可用於提供 AWS Control Tower 的商業 AWS 區域 用途。如需這些控制項的詳細資訊，請參閱主動式控制。如需控制項可用位置的詳細資訊，請參閱控制項限制。

全新偵探控制

Security Hub 服務管理標準：AWS Control Tower 新增了新的控制項。這些控制項可協助您強化您的治理狀態。在您在任何特定 OU 上啟用它們之後，它們就是 Security Hub 服務管理標準：AWS Control Tower 的一部分。

- [SH.Athena.1] Athena 工作組應在靜態時進行加密
- [SH.Neptune.1] Neptune 數據庫集群應在靜態時進行加密
- [SH.Neptune.2] Neptune DB 叢集應將審核日誌發佈到 CloudWatch 日誌
- [SH.Neptune.3] Neptune 資料庫叢集快照不應該是公開的
- [SH.Neptune.4] Neptune 資料庫叢集應啟用刪除保護
- [SH.Neptune.5] Neptune 資料庫叢集應啟用自動備份
- [SH.Neptune.6] Neptune 數據庫集群快照應在靜態時進行加密
- [SH.Neptune.7] Neptune 數據庫集群應啟用 IAM 數據庫身份驗證
- [SH.Neptune.8] 應將 Neptune DB 叢集設定為將標籤複製到快照
- [SH.RDS.27] RDS 數據庫集群應在靜態時進行加密

在 AWS Control Tower 提供的大多數情 AWS 區域 況下，都可以使用新的 AWS Security Hub 偵探控制項。如需有關這些控制的詳細資訊，請參閱適用於服務管理標準的控制：AWS Control Tower。如需控制項可用位置的詳細資訊，請參閱控制限制。

報告的新漂移類型：受信任存取已停用

2023年9月21 日

AWS Control Tower landing zone 不需要更新。)

在您設定 AWS Control Tower landing zone 之後，您可以在中停用對 AWS Control Tower 的受信任存取 AWS Organizations。但是，這樣做會導致漂移。

使用受信任的存取禁用漂移類型，AWS Control Tower 會在發生此類漂移時通知您，以便您修復 AWS Control Tower landing zone。如需詳細資訊，請參閱治理漂移的類型。

四個額外 AWS 區域

2023年9月13 日

AWS Control Tower landing zone 不需要更新。)

AWS Control Tower 現已在亞太區域 (海德拉巴)、歐洲 (西班牙和蘇黎世) 和中東 (阿拉伯聯合大公國) 推出。

如果您已經在使用 AWS Control Tower，而且想要將其管理功能擴展到帳戶中的這個區域，請前往 AWS Control Tower 儀表板中的「設定」頁面，選取區域，然後更新您的 landing zone 域。在 landing zone 域更新之後，您必須更新受 AWS Control Tower 管理的所有帳戶，以便在新區域中管理您的帳戶和 OU。如需詳細資訊，請參閱關於更新。

如需 AWS Control Tower 可使用的區域完整清單，請參閱AWS 區域 表格。

AWS Control Tower 於特拉維夫區域提供

2023年8月28日

AWS Control Tower landing zone 不需要更新。)

AWS Control Tower 宣布在以色列 (特拉維夫) 區域推出。

如果您已經在使用 AWS Control Tower，而且想要將其管理功能擴展到帳戶中的這個區域，請前往 AWS Control Tower 儀表板中的「設定」頁面，選取區域，然後更新您的 landing zone 域。在 landing zone 域更新之後，您必須更新受 AWS Control Tower 管理的所有帳戶，以便在新區域中管理您的帳戶和 OU。如需詳細資訊，請參閱關於更新。

如需 AWS Control Tower 可使用的區域完整清單，請參閱AWS 區域 表格。

AWS Control Tower 推出 28 個新的主動式控制

2023年7月24日

AWS Control Tower landing zone 不需要更新。)

AWS Control Tower 新增了 28 個新的主動控制項，協助您管理 AWS 環境。

主動式控制可在佈建不合規資源之前封鎖不合規的資源，藉此在您的多帳戶 AWS 環境中強化 AWS Control Tower 的管理功能。這些控制項有助於管 AWS 理 Amazon CloudWatch、亞 Amazon Neptune ElastiCache AWS Step Functions、Amazon 和 Amazon DocumentDB 等服務。這些新的控制項可協助您達成控制目標，例如建立記錄和監控、加密靜態資料或改善彈性。

以下是新控件的完整列表：

- 需要使用 GraphQL API 才能啟用記錄功能 AWS AppSync
- [CLOUDWATCH.PR.1] 要求 Amazon CloudWatch 警報為警報狀態設定動作
- 要求 Amazon CloudWatch 日誌群組保留至少一年
- 需要使用 KMS 金鑰在靜態時對 Amazon CloudWatch 日誌群組進行加密 AWS
- 需要啟動 Amazon 警報動作 CloudWatch
- 需要在靜態時對 Amazon DocumentDB 集群進行加密
- 要求 Amazon DocumentDB 群集啟用自動備份
- 需要使用金鑰在靜態時加密亞馬遜動態資料表 AWS KMS
- 要求 Amazon EC2 執行個體啟用詳細的監控功能
- [CT.EKS.PR.1] 要求將 Amazon EKS 叢集設定為停用叢集 Kubernetes API 伺服器端點的公開存取權
- 要求 Amazon ElastiCache 用於 Redis 的群集啟動自動備份
- 要求 Amazon ElastiCache 適用於 Redis 的叢集啟用次要版本的自動升級
- 需要 ElastiCache 針對 Redis 複寫群組的 Amazon 啟動自動容錯移轉
- 要求 Amazon 複寫群組啟動靜態加密 ElastiCache
- 要求 Amazon 的 Redis 複寫群組啟 ElastiCache 用傳輸過程中的加密
- 需要 Amazon 快取叢集才能使用自訂子網路群組 ElastiCache
- 要求較早版本的 Amazon ElastiCache 複寫群組具有 Redis 身份驗證
- 需要 Elastic Beanstalk 環境才能擁 AWS 有日誌記錄配置
- 需要在客戶管理的亞馬遜虛擬私有雲 (VPC) 中使用一個 AWS Lambda 功能
- 要求 Amazon Neptune 王星資料庫叢集具有 (IAM) 資料庫身份驗證 AWS Identity and Access Management
- 要求 Amazon Neptune 王星資料庫叢集啟用刪除保護
- 要求 Amazon Neptune 王星資料庫叢集啟用儲存加密
- 需要加密 Amazon Redshift 叢集
- 要求 Amazon S3 儲存貯體啟用 S3 物件鎖定

- [CT.S3.PR.10] 要求 Amazon S3 儲存貯體使用金鑰設定伺服器端加密 AWS KMS
- 要求 Amazon S3 儲存貯體啟用版本控制
- [步驟功能 .PR.1] 要求狀態機啟動日誌記錄 AWS Step Functions
- [步驟功能 .PR.2] 要求狀態機啟動追蹤 AWS Step Functions AWS X-Ray

AWS Control Tower 中的主動控制是透過 AWS CloudFormation Hook 來實作，可在佈建不合 AWS CloudFormation 規資源之前識別並封鎖這些資源。主動式控制可補充 AWS Control 塔中現有的預防和偵測控制功能。

這些新的主動式控制可 AWS 區域 在所有 AWS Control Tower 提供服務的地方使用。如需這些控制項的詳細資訊，請參閱主動式控制。

AWS Control Tower 棄用兩個控制

2023年7月18日

AWS Control Tower landing zone 無需更新。)

AWS Control Tower 會定期檢閱其安全控制，以確保它們是最新的，而且仍被視為最佳實務。下列兩個控制項已被棄用，自 2023 年 7 月 18 日起生效，而且它們將從控制項程式庫中移除，自 2023 年 8 月 18 日起生效。您無法再對任何組織單位啟用這些控制項。您可以選擇在移除日期之前停用這些控制項。

- [SH.S3.4] S3 儲存貯體應啟用伺服器端加密
- [CT.S3.PR.7] 要求 Amazon S3 儲存貯體設定伺服器端加密

棄用原因

自 2023 年 1 月起，Amazon S3 在所有新的和現有的未加密儲存貯體上設定了預設加密，以使用 S3 受管金鑰 (SSE-S3) 套用伺服器端加密作為上傳到這些儲存貯體的新物件的基礎加密層級。對於已設定 SSE-S3 或已設定金鑰管理服務 (AWS KMS) 金鑰 (SSE-KMS) 的伺服器端加密的現有儲存貯體，未對預設加密組態進行任何變更。 AWS

AWS Control Tower landing zone 3.2 版

2023 年 6 月 16 日

AWS Control Tower landing zone 需要更新至 3.2 版。 若要取得資訊，請參閱〈更新您的登陸區域〉。

AWS Control 塔 landing zone 3.2 版將屬於 AWS Security Hub 服務管理標準：AWS Control Tower 一部分的控制項納入正式推出。它引入了在 AWS Control 塔主控台中檢視屬於此標準一部分的控制項漂移狀態的功能。

此更新包含新的服務連結角色 (SLR)，稱為. AWSServiceRoleForAWSControlTower 此角色透過AWSControlTowerManagedRule在每個成員帳戶中建立稱為「」的 EventBridge 受管規則，協助 AWS Control Tower。此受管規則會收集 AWS Security Hub 尋找事件，使用 AWS Control Tower 可以判斷控制偏移。

此規則是 AWS Control Tower 要建立的第一個受管規則。規則不是由堆疊部署，而是直接從 EventBridge API 部署。您可以在 EventBridge 主控台或透過 EventBridge API 檢視規則。如果`managed-by`欄位已填入，則會顯示 AWS Control Tower 服務主體。

之前，AWS Control Tower 擔任在成員帳戶中執行操作的AWSControlTowerExecution角色。這項新角色和規則與在多帳戶 AWS 環境中執行作業時允許最少權限的最佳實務原則更加一致。新角色提供的限制權限特別允許：在成員帳戶中建立受管規則、維護受管規則、透過 SNS 發佈安全性通知，以及驗證漂移。如需詳細資訊，請參閱 AWSServiceRoleForAWSControlTower。

landing zone 3.2 更新也包含管理帳戶中的新 StackSet 資源`BP_BASELINE_SERVICE_LINKED_ROLE`，該資源最初會部署服務連結的角色。

報告 Security Hub 控制漂移 (在 landing zone 3.2 及更新版本) 時，AWS Control Tower 會從 Security Hub 收到每日狀態更新。雖然每個受管轄區域的控制都有效，但 AWS Control 塔只會將 AWS Security Hub 尋找事件傳送到 AWS Control Tower 本地區域。如需詳細資訊，請參閱資訊 Security Hub 控制漂移報告。

區域拒絕控制項的更新

此 landing zone 版本也包含「區域拒絕」控制項的更新。

新增全球服務和 API

- AWS Billing and Cost Management (`billing:*`)
- AWS CloudTrail （`cloudtrail:LookupEvents`）允許成員帳戶中的全局事件的可見性。
- AWS 合併帳單 (`consolidatedbilling:*`)
- AWS 管理 Console Mobile Application (`consoleapp:*`)
- AWS 免費方案 (`freetier:*`)
- AWS Invoicing (`invoicing:*`)
- AWS IQ（`iq:*`）

- AWS 使用者通知 (notifications:*)
- AWS 用戶通知聯系人 (notifications-contacts:*)
- Amazon Payments (payments:*)
- AWS 稅金設定 (tax:*)

全域服務和 API 已移除

- 已移除，s3:GetAccountPublic因為它不是有效的動作。
- 已移除，s3:PutAccountPublic因為它不是有效的動作。

AWS Control Tower 根據 ID 處理帳戶

2023年6月14日

AWS Control Tower landing zone 無需更新。)

AWS Control Tower 現在透過追蹤帳戶 ID 而非帳戶的電子郵件地址，來建立和管理您在 AWS Account Factory 中建立的帳戶。

佈建帳戶時，帳戶請求者一律必須具有CreateAccount和DescribeCreateAccountStatus權限。此權限集是管理員角色的一部分，當請求者擔任管理員角色時，會自動提供此權限集。如果您委派佈建帳戶的權限，您可能需要直接為帳戶要求者新增這些權限。

AWS Control Tower 控制程式庫提供的其他 Security Hub 偵測控制

2023年6月12日

AWS Control Tower landing zone 無需更新。)

AWS Control Tower 已在 AWS Control Tower 控制程式庫中新增了十個新的 AWS Security Hub 偵探控制項。這些新控制項的目標是服務，例如 API Gateway AWS CodeBuild、Amazon Elastic Compute Cloud (EC2)、Amazon Elastic Load Balancer、Amazon Redshift SageMaker、Amazon 和 AWS WAF. 這些新的控制項可協助您達成控制目標，例如建立記錄和監控、限制網路存取，以及加密靜態資料等，藉此增強您的治理狀態。

在您在任何特定 OU 上啟用這些控制後，這些控制是 Security Hub 服務管理標準：AWS Control 塔的一部分。

- [sh.Account。1] 應提供安全聯繫信息 AWS 帳戶

- [8] API Gateway 路由應指定授權類型
- [9] 應該為 API Gateway V2 階段配置訪問日誌
- [SH. CodeBuild.3] CodeBuild S3 日誌應加密
- [SH.EC2.25] EC2 啟動範本不應將公有 IP 指派給網路介面
- [SH.ELB.1] 應設定應 Application Load Balancer，以將所有 HTTP 要求重新導向至 HTTPS
- [紅移 .10] Redshift 叢集應該在靜態時加密
- [SH. SageMaker.2] SageMaker 筆記型電腦執行個體應該在自訂 VPC 中啟動
- [SH. SageMaker.3] 用戶不應該擁有對 SageMaker 筆記本實例的 root 訪問權限
- WAFV2 網頁 ACL 應該至少有一個規則或規則群組

所有 AWS Control Tower 均提供新 AWS 區域 的 AWS Security Hub 偵探控制項。如需有關這些控制的詳細資訊，請參閱適用於服務管理標準的控制：AWS Control Tower。

AWS Control Tower 發佈控制中繼資料表

2023年6月7日

AWS Control Tower landing zone 無需更新。)

AWS Control Tower 現在提供完整的控制中繼資料表，做為已發佈文件的一部分。使用控制項 API 時，您可以查詢每個控制項的 API 控制識別器，這是與每個控制項相關聯的唯一 ARN。 AWS 區域這些表格包括每個控制項涵蓋的架構和控制目標。之前，此資訊只能在主控台中使用。

這些表格也包含 Security Hub 控制項的中繼資料，這些控制項屬於AWS Security Hub 服務管理標準：AWS Control Tower 的一部分。如需完整詳細資訊，請參閱控制項中繼資料表。

如需控制項識別碼的縮寫清單，以及一些使用範例，請參閱 API 和控制項的資源識別碼。

Account Factory 定制的地形支持

2023年6月6日

AWS Control Tower landing zone 無需更新。)

AWS Control Tower 透過 Account Factory 自訂 (AFC) 為地形提供單一區域支援。從此版本開始，您可以一起使用 AWS Control Tower 和 Service Catalog，在 Terraform 開放原始碼中定義 AFC 帳戶藍圖。在 AWS Control Tower 中佈建資源之前 AWS 帳戶，您可以自訂新的和現有的資源。根據預設，此功能可讓您使用 Terraform 在 AWS Control Tower 本地區域部署和更新帳戶。

帳戶藍圖描述佈建時所需的特定資源和組態。 AWS 帳戶 您可以使用藍圖做為範本，以大規模建立多個 AWS 帳戶 。

若要開始使用，請在上使用地形參考引擎。 GitHub參考引擎會定義 Terraform 開放原始碼引擎與 Service Catalog 搭配使用所需的程式碼和基礎結構。這個一次性的設置過程需要幾分鐘的時間。之後，您可以在 Terraform 中定義自訂帳戶需求，然後使用定義明確的 AWS Control Tower 帳戶工廠工作流程部署您的帳戶。喜歡使用 Terraform 的客戶可以透過 AFC 大規模利用 AWS Control Tower 帳戶自訂，並在佈建後立即存取每個帳戶。

若要了解如何建立這些自訂，請參閱 Service Catalog 文件中的建立產品和 Terraform 開放原始碼入門。此功能適用於所有 AWS Control Tower 的 AWS 區域 地方。

AWS 適用於 landing zone 的 IAM 身分中心自我管理

2023年6月6日

AWS Control Tower landing zone 無需更新。)

AWS Control Tower 現在支援 AWS Control Tower landing zone 的選擇性身分供應商選擇，您可以在安裝或更新期間進行設定。根據預設，landing zone 會選擇使用 AWS IAM 身分中心，並與使用多個帳戶組織 AWS 環境中定義的最佳實務指引一致。您現在有三種選擇：

- 您可以接受預設值，並允許 AWS Control Tower 為您設定和管理 AWS IAM 身分中心。
- 您可以選擇自行管理 AWS IAM 身分中心，以反映您的特定業務需求。
- 如有需要，您可以透過 IAM 身分中心連接第三方身分識別提供者，選擇性地引入和自我管理。如果您的法規環境要求您使用特定的供應商，或者您在無法使用 AWS IAM Identity Center 的 AWS 區域 地方進行操作，則應使用身分提供者選擇性。

如需詳細資訊，請參閱 IAM 身分識別中心指引。

不支援在帳戶層級選取身分識別提供者。此功能僅適用於整個 landing zone 域。AWS Control Tower 的所有提供 AWS Control Tower 的 AWS 區域 地方均提供 AWS 控制塔身分供應商選擇性。

AWS Control Tower 處理 OU 的混合式管控問題

2023年6月1日

AWS Control Tower landing zone 無需更新。)

在此版本中，如果 OU 處於混合管理狀態，則 AWS Control Tower 可防止控制項部署到組織單位 (OU)。如果 AWS Control Tower 將管理擴展到新的管理或移除管理之後，帳戶未更新 AWS 區域，則

會在 OU 中發生混合控管。此版本可協助您使該 OU 的成員帳戶保持一致的合規性。如需詳細資訊，請參閱 設定區域時避免混合控管。

提供其他主動式控制

2023年5月19日

AWS Control Tower landing zone 無需更新。)

AWS Control Tower 新增了 28 個新的主動控制功能，協助您管理多帳戶環境並達成特定控制目標，例如靜態資料加密或限制網路存取。主動式控制是透過 AWS CloudFormation 掛接來實作，可在佈建資源之前先檢查資源。這些新的控制項可協助治理 AWS 服務，例如 Amazon OpenSearch 服務、Amazon EC2 Auto Scaling SageMaker、Amazon API Gateway 和 Amazon Relational Database Service (RDS)。

提供 AWS Control Tower 的所有商業廣告 AWS 區域 都支援主動式控制。

Amazon OpenSearch 服務

- 需要一個彈性搜索域來加密靜態數據
- 需要在使用者指定的 Amazon VPC 中建立彈性搜尋網域
- 需要使用彈性搜尋網域來加密節點之間傳送的資料
- 需要一個彈性搜索域才能將錯誤日誌發送到 Amazon 日誌 CloudWatch
- 需要彈性搜尋網域才能將稽核日誌傳送至 Amazon 日誌 CloudWatch
- 要求彈性搜索域具有區域感知功能和至少三個數據節點
- 要求一個彈性搜索域至少有三個專用的主節點
- 需要彈性搜尋服務網域才能使用 TLSv1.2
- 需要使用 Amazon OpenSearch 服務網域來加密靜態資料
- 需要在使用者指定的 Amazon VPC 中建立 Amazon OpenSearch 服務網域
- 要求 Amazon OpenSearch 服務網域加密節點之間傳送的資料
- [CT.OPENSEARCH.PR.12] 要求 Amazon OpenSearch 服務域將錯誤日誌發送到 Amazon 日誌 CloudWatch
- [CT.OPENSEARCH.PR.13] 要求 Amazon OpenSearch 服務網域將稽核日誌傳送到 Amazon 日誌 CloudWatch
- [CT.OPENSEARCH.PR.14] 要求 Amazon OpenSearch 服務域具有區域感知功能和至少三個數據節點

- 要求 Amazon OpenSearch 服務網域使用精細的存取控制
- 需要一個 Amazon 服務域才能使用 TLSv1.2 OpenSearch

Amazon EC2 Auto Scaling

- [CT 自動擴展 .PR.1] 要求 Amazon EC2 自 Auto Scaling 群組具有多個可用區域
- [CT.自動擴展 .PR.2] 需要使用 Amazon EC2 Auto Scaling 群組啟動組態，才能為 IMDSv2 設定 Amazon EC2 執行個體
- [CT.自動擴展 .PR.3] 要求 Amazon EC2 自動擴展啟動組態具有單一躍點中繼資料回應限制
- [CT.自動擴展 .PR.4] 需要與 Amazon Elastic Load Balancing (ELB) 關聯的 Amazon EC2 Auto Scaling 群組才能啟動 ELB 運作狀態檢查
- [CT.自動擴展 .PR.5] 要求 Amazon EC2 自動擴展群組啟動組態沒有具有公有 IP 地址的 Amazon EC2 執行個體
- [CT 自動擴展 .PR.6] 要求任何 Amazon EC2 自 Auto Scaling 群組使用多個執行個體類型
- [CT 自動擴展 .PR.8] 要求 Amazon EC2 自 Auto Scaling 群組設定 EC2 啟動範本

Amazon SageMaker

- [CT.SAGEMAKER.PR.1] 需要一個 Amazon SageMaker 筆記本執行個體，以防止直接存取網際網路
- 需要在自訂的 Amazon VPC 中部署 Amazon SageMaker 筆記型電腦執行個體
- [CT.SAGEMAKER.PR3] 要求 Amazon SageMaker 筆記本執行個體具有不允許根訪問權限

Amazon API Gateway

- 需要 Amazon API Gateway V2 網路通訊端和 HTTP 路由來指定授權類型

Amazon Relational Database Service (RDS)

- 要求 Amazon RDS 資料庫叢集必須設定日誌記錄

如需詳細資訊，請參閱主動式控制。

更新的 Amazon EC2 主動控制

2023年5月2日

AWS Control Tower landing zone 無需更新。)

AWS Control Tower 已更新兩項主動控制：CT.EC2.PR.3和CT.EC2.PR.4。

對於更新的CT.EC2.PR.3控制項，任何參考安全性群組資源前置詞清單的部 AWS CloudFormation 署都會遭到封鎖，無法部署，除非用於連接埠 80 或 443。

針對更新的CT.EC2.PR.4控制 AWS CloudFormation 項，如果連接埠是
3389、20、23、110、3306、8080、1433、1433、9200、9300、25、445、135、1434、5432、5500、143

7 個額外 AWS 區域 可用

2023年4月19 日

AWS Control Tower landing zone 無需更新。)

AWS Control Tower 現在另外提供七個服務 AWS 區域：北加州 (舊金山)、亞太區域 (香港、雅加達和大阪)、歐洲 (米蘭)、中東 (巴林) 和非洲 (開普敦)。AWS Control Tower 的這些其他區域 (稱為選擇加入區域) 預設為作用中狀態，除了美國西部 (加利佛尼亞北部) 區域 (預設為作用中) 之外。

AWS Control Teck Teck 中的某些控制項無法在提供 AWS Control Tower 的 AWS 區域 其他部分控制中運作，因為這些區域不支援所需的基礎功能。如需詳細資訊，請參閱 控制限制。

在這些新地區中，CFCT 不在亞太地區（雅加達和大阪）提供。在其他可用性 AWS 區域 是不變的。

如需 AWS Control Tower 如何管理區域和控制限制的詳細資訊，請參閱啟用 AWS 選擇加入區域的注意事項。

中東 (巴林) 區域不提供 AFT 所需的 VPCE 端點。在此區域部署 AFT 的客戶必須使用參數`aft_vpc_endpoints=false`進行部署。如需詳細資訊，請參閱 README 檔案中的參數。

由於 Amazon EC2 的限制，`us-west-1`AWS Control Tower VPC 在美國西部 (加利佛尼亞北部) 區域有兩個可用區域。在美國西部 (加利佛尼亞北部)，六個子網路分為兩個可用區域。如需詳細資訊，請參閱 AWS Control Tower 和虛擬私人雲端概觀。

AWS Control Tower 已新增許 AWS 區域 可`AWSControlTowerServiceRolePolicy`，讓 AWS Control Tower 可以呼叫 AWS 帳戶管理服務實作的`EnableRegionListRegions`、和 `GetRegionOptStatus` API，讓您在 landing zone (管理帳戶、記錄存檔帳戶、稽核帳戶) 和 OU 成員帳戶的共用帳戶可以使用這些額外的權限。如需詳細資訊，請參閱 AWS Control Tower 的受管政策。

地形表單 (AFT) 帳戶自訂要求追蹤的 Account Factory

2023年2月16日

AFT 支援帳戶自訂要求追蹤。每次您提交帳戶自訂要求時，AFT 都會產生一個唯一的追蹤 Token，該 Token 會通過 AFT 自訂 AWS Step Functions 狀態機器進行記錄，並將權杖記錄為其執行的一部分。您可以使用 Amazon CloudWatch Logs 深入解析查詢來搜尋時間戳記範圍並擷取請求權杖。因此，您可以看到令牌隨附的有效載荷，因此您可以在整個 AFT 工作流程中跟踪帳戶自定義請求。如需 AFT 的詳細資訊，請參閱地形 AWS Control Tower Account Factory 概觀。如需 CloudWatch 記錄檔和 Step Functions 的相關資訊，請參閱下列內容：

- 什麼是 Amazon CloudWatch 日誌？ 在 Amazon CloudWatch 日誌用戶指南
- 什麼是 AWS Step Functions？ 在AWS Step Functions 開發人員指南

AWS Control Tower landing zone 3.1 版

2023 年 2 月 9 日

AWS Control Tower landing zone 需要更新至 3.1 版。 若要取得資訊，請參閱更新您的登陸區域)

AWS Control Tower landing zone 3.1 版包含下列更新：

- 在此版本中，AWS Control Tower 會停用存取日誌儲存貯體 (存取日誌存放在日誌存檔帳戶的 Amazon S3 儲存貯體) 不必要的存取日誌記錄，同時繼續為 S3 儲存貯體啟用伺服器存取日誌。此版本也包含「區域拒絕」控制項的更新，可針對全域服務執行其他動作，例如 AWS Support Plans 和 AWS Artifact。
- 停用 AWS Control Tower 存取記錄儲存貯體的伺服器存取記錄會導致 Security Hub 為日誌存檔帳戶的存取記錄儲存貯體建立發現項目，因為有 AWS Security Hub 規則，應啟用 [S3.9] S3 儲存貯體伺服器存取記錄。與安全中心一致，我們建議您隱藏此特定發現項目，如此規則的 Security Hub 說明所述。如需其他資訊，請參閱有關隱藏發現項目的資訊
- 在 3.1 版中，記錄封存帳戶中 (一般) 記錄值區的存取記錄不會變更。根據最佳做法，該值區的存取事件會記錄為存取記錄值區中的記錄項目。如需有關存取記錄的詳細資訊，請參閱 Amazon S3 文件中的使用伺服器存取日誌記錄請求。
- 我們更新了「區域拒絕」控制項。此更新允許更多全球服務執行動作。如需此 SCP 的詳細資訊，請參閱拒絕 AWS 根據要求的存取 AWS 區域和增強資料駐留保護的控制項。

  全球服務新增：

  - AWS Account Management (`account:*`)
  - AWS 啟動 (`activate:*`)
  - AWS Artifact (`artifact:*`)
  - AWS Billing Conductor (`billingconductor:*`)

- AWS Compute Optimizer (`compute-optimizer:*`)
- AWS Data Pipeline (`datapipeline:GetAccountLimits`)
- AWS Device Farm(`devicefarm:*`)
- AWS Marketplace (`discovery-marketplace:*`)
- Amazon ECR () `ecr-public:*`
- AWS License Manager (`license-manager:ListReceivedLicenses`)
- AWS Lightsail () `lightsail:Get*`
- AWS 資源總管 (`resource-explorer-2:*`)
- Amazon S3 (`s3:CreateMultiRegionAccessPoint`，`s3:GetBucketPolicyStatus`，`s3:PutMultiRegi`
- AWS Savings Plans (`savingsplans:*`)
- IAM 身分識別中心 (`sso:*`)
- AWS Support App (`supportapp:*`)
- AWS Support 計劃 (`supportplans:*`)
- AWS 可持續發展 (`sustainability:*`)
- AWS Resource Groups Tagging API (`tag:GetResources`)
- AWS Marketplace 供應商洞察 (`vendor-insights:ListEntitledSecurityProfiles`)

一般提供主動式控制

2023年1月24日

AWS Control Tower landing zone 無需更新。)

先前以預覽狀態宣佈的選用主動式控制項，現已正式推出。這些控制項稱為主動式控制項，因為它們會在資源部署之前先檢查您的資源，以判斷新資源是否符合在您環境中啟動的控制項。如需詳細資訊，請參閱 全面的控制有助於 AWS 資源佈建和管理。

二零二二年一月至

在 2022 年，AWS Control Tower 發布了以下更新：

- 並行帳戶作業
- 客 Account Factory 定制

- 全面的控制有助於 AWS 資源佈建和管理
- 可檢視所有 AWS Config 規則的符合性狀態
- 控制項和新資 AWS CloudFormation 源的 API
- CFCT 支持堆棧集刪除
- 自訂記錄保留
- 提供角色漂移修復
- AWS Control Tower landing zone 3.0 版
- 「組織」頁面結合了 OU 和帳戶的檢視
- 更輕鬆地註冊和更新個別會員帳戶
- AFT 支援共用 AWS Control Tower 帳戶的自動化自訂
- 所有選擇性控制項的並行作業
- 現有的安全性和記錄帳戶
- AWS Control Tower landing zone 2.9 版
- AWS Control Tower landing zone 2.8 版

並行帳戶作業

2022年12月16日

AWS Control Tower landing zone 無需更新。)

AWS Control Tower 現在支援帳戶工廠中同時執行動作。您一次最多可以建立、更新或註冊五 (5) 個帳戶。最多可連續提交五個動作，並檢視每個請求的完成狀態，同時您的帳戶會在背景完成建置。例如，您不再需要等待每個程序完成後才能更新其他帳戶，或重新註冊整個組織單位 (OU) 之前。

客 Account Factory 定制

2022年11月28日

AWS Control Tower landing zone 無需更新。)

帳戶工廠自訂可讓您在 AWS Control Tower 主控台內自訂新帳戶和現有帳戶。這些新的自訂功能可讓您彈性定義帳戶藍圖，這些藍圖是包含在專門 Service Catalog 產品中的 AWS CloudFormation 範本。藍圖佈建完全自訂的資源和組態。您也可以選擇使用由 AWS 合作夥伴建置和管理的預先定義藍圖，以協助您針對特定使用案例自訂帳戶。

過去，AWS Control Tower 帳戶工廠不支援主控台中的帳戶自訂。透過此帳戶工廠更新，您可以預先定義帳戶需求，並將其作為定義明確的工作流程的一部分來實作。您可以套用藍圖來建立新帳戶、將其他 AWS 帳戶註冊到 AWS Control Tower，以及更新現有的 AWS Control Tower 帳戶。

在帳戶 Factory 中佈建、註冊或更新帳戶時，您將選取要部署的藍圖。藍圖中指定的那些資源會佈建在您的帳戶中。當您的帳戶完成構建後，所有自定義配置都可以立即使用。

若要開始自訂帳戶，您可以在 Service Catalog 產品中針對預定使用案例定義資源。您也可以從 AWS 入門程式庫中選取合作夥伴管理的解決方案。如需詳細資訊，請參閱 使用 Account Factory 定制（AFC）自定義帳戶。

全面的控制有助於 AWS 資源佈建和管理

2022年11月28日

AWS Control Tower landing zone 無需更新。)

AWS Control Tower 現在支援全面的控制管理，包括透過 AWS CloudFormation 掛接實作的新選用主動式控制。這些控制項稱為主動式控制項，因為它們會在資源部署之前先檢查您的資源，以判斷新資源是否符合在您環境中啟動的控制項。

超過 130 種全新的主動式控制可協助您達成 AWS Control Tower 環境的特定政策目標；符合業界標準合規架構的要求，以及管理 AWS Control Tower 在其他二十多個 AWS 服務之間的互動。

AWS Control Tower 控制程式庫會根據相關的 AWS 服務和資源對這些控制進行分類。如需詳細資訊，請參閱主動式控制。

在此版本中，AWS Control Tower 也透過新的 AWS Security Hub Security Hub 服務管理標準：AWS Control Tower 整合，該標準支援 AWS 基礎安全最佳實務 (FSBP) 標準。您可以在主控台中檢視超過 160 個安全中心控制以及 AWS Control 塔控制項，也可以取得 AWS Control Tower 環境的安全中 Security Hub 安全分數。如需詳細資訊，請參閱 Security Hub 控制項。

可檢視所有 AWS Config 規則的符合性狀態

2022年11月18日

AWS Control Tower landing zone 無需更新。)

AWS Control Tower 現在會顯示部署到 AWS Control Tower 註冊組織單位的所有 AWS Config 規則的合規狀態。您可以在 AWS Control Tower (已註冊或未註冊) 中檢視影響帳戶的所有 AWS Config 規則的合規狀態，而無需在 AWS Control Tower 主控台之外瀏覽。客戶可以選擇在 AWS Control Tower 中

設定 Config 規則 (稱為偵探控制)，或直接透過 AWS Config 服務進行設定。部署的規則 AWS Config 會顯示，以及 AWS Control Tower 部署的規則。

之前，透過 AWS Config 服務部署的 AWS Config 規則在 AWS Control 塔主控台中看不到。客戶必須瀏覽至 AWS Config 服務，才能識別不合 AWS Config 規的規則。現在，您可以在 AWS Control 塔主控台中識別任何不合 AWS Config 規的規則。若要檢視所有 Config 規則的合規狀態，請導覽至 AWS Control 塔主控台中的帳戶詳細資訊頁面。您會看到一份清單，顯示 AWS Control Tower 管理的控制的合規狀態，以及在 AWS Control Tower 外部部署的 Config 規則。

控制項和新資 AWS CloudFormation 源的 API

2022年9月1日

AWS Control Tower landing zone 無需更新。)

AWS Control Tower 現在支援透過一組 API 呼叫對控制進行程式設計管理 (也稱為護欄)。新 AWS CloudFormation 資源支援控制項的 API 功能。如需詳細資訊，請參閱 AWS Control Tower 中的自動化任務 和 建立 AWS Control Tower 資源 AWS CloudFormation。

這些 API 可讓您在 AWS Control Tower 程式庫中啟用、停用和檢視控制的應用程式狀態。這些 API 包括支援 AWS CloudFormation，因此您可以將 AWS 資源管理為 infrastructure-as-code (IaC)。AWS Control Tower 提供選用的預防性和偵測控制，可表達您對整個組織單位 (OU) 以及 OU 內每個 AWS 帳戶的政策意向。當您建立新帳戶或變更現有帳戶時，這些規則仍然有效。

此發行版本中包含的 API

- EnableControl— 此 API 呼叫會啟動控制項。它會啟動非同步作業，在指定的組織單位及其包含的帳號上建立 AWS 資源。
- DisableControl— 此 API 呼叫會關閉控制項。它會啟動非同步作業，刪除指定組織單位上的 AWS 資源及其包含的帳號。
- GetControlOperation— 傳回特定EnableControl或DisableControl作業的狀態。
- ListEnabledControls— 列出 AWS Control Tower 在指定組織單位上啟用的控制項及其包含的帳戶。

若要檢視選用控制項的控制名稱清單，請參閱 AWS Control 塔使用者指南中的 API 和控制項的資源識別碼。

CFCT 支持堆棧集刪除

2022年8月26日

AWS Control Tower landing zone 無需更新。)

AWS Control Tower (CFCT) 的自訂現在可透過在manifest.yaml檔案中設定參數，支援刪除堆疊集。如需詳細資訊，請參閱 刪除堆疊集。

> **Important**
>
> 當您初始enable_stack_set_deletion將的值設定為時true，下次呼叫 CFCT 時，會暫存以前置詞開頭的所有資源CustomControlTower-，這些資源具有相關聯的索引鍵標記Key:AWS_Solutions, Value: CustomControlTowerStackSet，且未在資訊清單檔案中宣告，以供刪除。

自訂記錄保留

2022年8月15日

AWS Control Tower landing zone 需要更新。 若要取得資訊，請參閱更新您的登陸區域)

AWS Control Tower 現在可為存放 AWS Control Tower CloudTrail 日誌的 Amazon S3 儲存貯體自訂保留政策。您可以自訂 Amazon S3 日誌保留政策，以天數或年為增量，最長可達 15 年。

如果您選擇不自訂記錄保留，則預設設定為標準帳戶記錄 1 年，存取記錄的預設設定為 10 年。

當您更新或修復您的 landing zone 時，現有客戶可透過 AWS Control Tower 使用此功能，以及透過 AWS Control Tower 設定程序的新客戶使用。

提供角色漂移修復

2022年8月11日

AWS Control Tower landing zone 無需更新。)

AWS Control Tower 現在支援角色漂移的修復。您可以恢復必要的角色，而無需完整修復您的 landing zone。如果需要此類漂移修復，主控台錯誤頁面會提供還原角色的步驟，以便再次使用您的 landing zone。

AWS Control Tower landing zone 3.0 版

2022年7月29日

AWS Control Tower landing zone 需要更新至 3.0 版。 若要取得資訊，請參閱更新您的登陸區域)

AWS Control Tower landing zone 3.0 版包含下列更新：

- 可選擇組織層級 AWS CloudTrail 追蹤，或選擇退出由 AWS Control Tower 管理的 CloudTrail 追蹤。
- 兩個新的偵探控制項可判斷 AWS CloudTrail 是否在您的帳戶中記錄活動。
- 此選項僅能彙總您所在地區的全域資源相關資 AWS Config 訊。
- 區域拒絕控制的更新。
- 受管理策略的更新AWSControlTowerServiceRolePolicy。
- 我們不再`aws-controltower/CloudTrailLogs`在每個註冊帳戶中建立 IAM 角色`aws-controltower-CloudWatchLogsRole`和 CloudWatch 日誌群組。之前，我們在每個帳戶中為其帳戶跟踪創建了這些內容。透過組織追蹤，我們只會在管理帳戶中建立一個。

以下各節提供有關每個新功能的詳細資訊。

AWS Control Tower 中的組織層級 CloudTrail 追蹤

使用 3.0 版的 landing zone，AWS Control Tower 現在支援組織層級 AWS CloudTrail 追蹤。

將 AWS Control Tower landing zone 更新為 3.0 版時，您可以選擇選擇組織層級 AWS CloudTrail 追蹤作為記錄偏好設定，或選擇退出由 AWS Control Tower 管理的 CloudTrail 追蹤。當您更新至 3.0 版時，AWS Control Tower 會在 24 小時等待期後刪除已註冊帳戶的現有帳戶層級追蹤。AWS Control Tower 不會刪除未註冊帳戶的帳戶層級追蹤。在不太可能的情況下，您的 landing zone 域更新無法成功，但是在 AWS Control Tower 已建立組織層級追蹤後發生失敗，您可能會對組織層級和帳戶層級追蹤產生重複費用，直到您的更新作業能夠順利完成為止。

從 landing zone 3.0 開始，AWS Control Tower 不再支援管理的帳戶層級追蹤。 AWS 相反地，AWS Control Tower 會根據您的選擇建立組織層級的追蹤，該追蹤為作用中或非作用中狀態。

> **Note**
>
> 更新至 3.0 版或更新版本後，您無法選擇繼續使用 AWS Control Tower 管理的帳戶層級 CloudTrail 追蹤。

彙總帳戶日誌中不會遺失任何記錄資料，因為日誌會保留在存放日誌的現有 Amazon S3 儲存貯體中。只會刪除追蹤，而不會刪除現有的記錄。如果您選取新增組織層級追蹤的選項，AWS Control Tower

會在 Amazon S3 儲存貯體中開啟新資料夾的新路徑，並繼續將記錄資訊傳送到該位置。如果您選擇退出由 AWS Control Tower 管理的追蹤，您現有的記錄會保留在值區中，不變。

記錄檔儲存的路徑命名慣例

- 帳戶追蹤記錄會以下列格式的路徑儲存：*/org id*/AWSLogs/…
- 組織追蹤記錄會以下列格式的路徑儲存：*/org id*/AWSLogs/*org id*/…

AWS Control Tower 為組織層級 CloudTrail 追蹤建立的路徑與手動建立的組織層級追蹤的預設路徑不同，其格式如下：

- /AWSLogs/*org id*/…

如需 CloudTrail 路徑命名的詳細資訊，請參閱尋找 CloudTrail 記錄檔。

> **Tip**
>
> 如果您打算建立和管理自己的帳戶層級追蹤，建議您在完成 AWS Control Tower landing zone 3.0 版本的更新之前建立新追蹤，以立即開始記錄。

您可以隨時選擇建立新的帳戶層級或組織層級 CloudTrail追蹤，並自行管理。在任何 landing zone 更新至 3.0 版或更新版本期間，都可以選擇由 AWS Control Tower 管理的組織層級 CloudTrail追蹤選項。每當您更新 landing zone 域時，您都可以選擇加入和選擇退出組織層級的追蹤。

如果您的記錄檔是由協力廠商服務管理，請務必提供服務的新路徑名稱。

> **Note**
>
> 對於 3.0 版或更新版本的登陸區域，AWS Control Tower 不支援帳戶層級 AWS CloudTrail 追蹤。您可以隨時建立和維護自己的帳戶層級追蹤，也可以選擇加入 AWS Control Tower 管理的組織層級追蹤。

僅在本地區記錄 AWS Config 資源

在 3.0 版的 landing zone 域中，AWS Control Tower 已更新的基準組態， AWS Config 以便僅在本地區域記錄全球資源。在您更新至 3.0 版之後，全域資源的資源記錄只會在您的本地區域中啟用。

此組態被視為最佳作法。建議使用 AWS Security Hub 和 AWS Config，它會減少建立、修改或刪除全域資源時所建立的組態項目數，藉此節省成本。以前，每次建立、更新或刪除全域資源 (無論是由客戶或 AWS 服務) 時，都會為每個受控區域中的每個項目建立組態項目。

兩個用於 AWS CloudTrail 記錄的新偵探控件

作為組織層級 AWS CloudTrail 追蹤變更的一部分，AWS Control Tower 推出兩個新的偵探控制項，以檢查 CloudTrail 是否已啟用。第一個控制項具有強制性指引，並且在 3.0 及更新版本的安裝或 landing zone 更新期間，會在安全性 OU 上啟用。第二個控制項具有強烈建議的指導方針，並選擇性地套用至安全性 OU 以外的任何 OU，此 OU 已強制執行強制控制保護。

強制控制：偵測安全性組織單位下的共用帳戶是否已啟用 AWS CloudTrail 或啟用 CloudTrail Lake

強烈建議控制項：偵測帳戶是否已啟用 AWS CloudTrail 或啟用 CloudTrail Lake

如需有關新控制的詳細資訊，請參閱 AWS Control Tower 控制程式庫。

區域拒絕控制的更新

我們更新了「地區拒絕控制」中的NotAction清單，以包含一些其他服務的動作，列出如下：

```
        “chatbot:*”,
        "s3:GetAccountPublic",
        "s3:DeleteMultiRegionAccessPoint",
        "s3:DescribeMultiRegionAccessPointOperation",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:ListMultiRegionAccessPoints",
        "s3:GetStorageLensConfiguration",
        “s3:GetStorageLensDashboard",
        “s3:ListStorageLensConfigurations”
        “s3:GetAccountPublicAccessBlock“,,
        “s3:PutAccountPublic",
        “s3:PutAccountPublicAccessBlock“,
```

影片演練

本影片 (3:07) 說明如何將現有的 AWS Control Tower landing zone 更新為第 3 版。若要獲得更佳的觀賞效果，請選取影片右下角的圖示，將影片放大至全螢幕。並提供字幕。

將現有 AWS Control Tower 登陸區更新為著陸區 3 的視頻演練。

「組織」頁面結合了 OU 和帳戶的檢視

2022年7月18日

(AWS Control Tower landing zone 無需更新)

AWS Control Tower 中的新組織頁面會顯示所有組織單位 (OU) 和帳戶的階層檢視。它結合了先前存在的 OU 和帳戶頁面中的資訊。

在新頁面上，您可以看到父 OU 與其巢狀 OU 與帳戶之間的關係。您可以對資源群組採取動作。您可以設定頁面檢視。例如，您可以展開或收合階層式檢視、篩選檢視以查看帳戶或僅 OU、選擇僅檢視已註冊的帳戶和已註冊的 OU，或者您可以檢視相關資源群組。這是更容易確保您的整個組織正確更新。

更輕鬆地註冊和更新個別會員帳戶

2022年5月31日

(AWS Control Tower landing zone 無需更新)

AWS Control Tower 現在提供您個別更新和註冊成員帳戶的改良功能。每個帳戶都會顯示何時可用更新，因此您可以更輕鬆地確保您的成員帳戶包含最新的設定。您可以透過幾個簡化的步驟，更新您的 landing zone、修復帳戶偏移，或將帳戶註冊到已註冊的 OU。

當您更新帳戶時，不需要在每個更新動作中包含帳戶的整個組織單位 (OU)。因此，更新個人帳戶所需的時間大大縮短。

您可以透過 AWS Control Tower 主控台提供的更多協助，將帳戶註冊到 AWS Control Tower OU。您在 AWS Control Tower 註冊的現有帳戶仍然必須符合帳戶先決條件，而且您必須新增`AWSControlTowerExecution`角色。然後，您可以選擇任何已註冊的 OU，並透過選取 [註冊] 按鈕將帳戶註冊到其中。

我們已將「註冊帳戶」功能與「在帳戶工廠中建立帳戶」工作流程分開，以便在這些類似程序之間建立更多區別，並協助避免在輸入帳戶資訊時發生設定錯誤。

AFT 支援共用 AWS Control Tower 帳戶的自動化自訂

2022年5月27日

(AWS Control Tower landing zone 無需更新)

Terraform Account Factory (AFT) 現在可以透過程式設計方式自訂和更新由 AWS Control Tower 管理的任何帳戶，包括管理帳戶、稽核帳戶和記錄存檔帳戶，以及您註冊的帳戶。您可以集中管理帳戶自訂和更新管理，同時保護帳戶設定的安全性，因為您可以限定執行工作的角色範圍。

現有AWSAFTExecution角色現在會在所有帳戶中部署自訂項目。您可以使用界限設定 IAM 許可，以根據您的業務和安全需求限制AWSAFTExecution角色的存取權限。您也可以透過程式設計方式將該角色中核准的自訂權限委派給信任的使用者。最佳作法是，建議您將權限限制為部署所需自訂所需的權限。

AFT 現在會建立新AWSAFTService角色，在所有受管理帳戶 (包括共用帳戶和管理帳戶) 中部署 AFT 資源。資源先前是由AWSAFTExecution角色部署的。

AWS Control Tower 共用和管理帳戶不是透過帳戶工廠佈建，因此中沒有對應的佈建產品 AWS Service Catalog。因此，您無法更新 Service Catalog 中的共用和管理帳戶。

所有選擇性控制項的並行作業

2022年5月18日

(AWS Control Tower landing zone 無需更新)

AWS Control Tower 現在支援預防性控制和偵探控制的同時操作。

有了這項新功能，現在可以同時套用或移除任何選用的控制項，進而改善所有選用控制項的易用性和效能。您可以啟用多個選擇性控制項，而無需等待個別控制項作業完成。唯一受到限制的時間是 AWS Control Tower 正在設定 landing zone，或將管理擴展到新組織。

支援的預防性控制功能：

- 在相同 OU 上套用及移除不同的預防性控制。
- 同時在不同 OU 上套用並移除不同的預防性控制。
- 同時在多個 OU 上套用並移除相同的預防控制。
- 您可以同時套用並移除任何預防性和偵探控制項。

您可以在所有發行版本的 AWS Control Tower 中體驗這些控制並行改進功能。

當您對巢狀 OU 套用預防控制時，預防性控制會影響目標 OU 下巢狀的所有帳戶和 OU，即使這些帳戶和 OU 未向 AWS Control Tower 註冊也一樣。預防性控制是使用服務控制策略（SCP）來實現的，這些策略屬於的一部 AWS Organizations分。Detective 控制項是使用 AWS Config 規則來實作。當您建

立新帳戶或變更現有帳戶時，Guardrails 仍然有效，而 AWS Control Tower 會提供每個帳戶如何符合您已啟用政策的摘要報告。如需可用控制項的完整清單，請參閱 AWS Control Tower 控制程式庫。

現有的安全性和記錄帳戶

2022年5月16日

（在初始設置期間可用。）

AWS Control Tower 現在可讓您在初始 landing zone 設定程序期間，將現有 AWS 帳戶指定為 AWS Control Tower 安全或記錄帳戶的選項。此選項無需 AWS Control Tower 建立新的共用帳戶。安全性帳戶 (依預設稱為稽核帳戶) 是受限制的帳戶，可讓您的安全性和規範遵循團隊存取您 landing zone 中所有帳戶的權限。記錄帳戶 (依預設稱為記錄封存帳戶) 可當做儲存庫使用。它會儲存您 landing zone 中所有帳號的 API 活動和資源設定記錄。

透過使用現有的安全和記錄帳戶，可以更輕鬆地將 AWS Control Tower 管理擴展到現有組織，或從替代的 landing zone 移至 AWS Control Tower。在初始 landing zone 域設置期間，會顯示您使用既有帳戶的選項。它包括安裝程序期間的檢查，以確保部署成功。AWS Control Tower 在您現有的帳戶上實作必要的角色和控制。它不會移除或合併這些帳戶中存在的任何現有資源或資料。

限制：如果您計劃將現有 AWS 帳戶帶入 AWS Control Tower 作為稽核和日誌存檔帳戶，而且這些帳戶具有現有 AWS Config 資源，則必須先刪除現有 AWS Config 資源，然後才能將帳戶註冊到 AWS Control Tower。

AWS Control Tower landing zone 2.9 版

2022年4月22日

AWS Control Tower landing zone 需要更新至 2.9 版。 若要取得資訊，請參閱更新您的登陸區域)

AWS Control Tower landing zone 2.9 版更新了通知轉發器 Lambda，以使用 Python 版本 3.9 執行階段。此更新解決了計劃於 2022 年 7 月進行的 Python 3.6 版本的棄用問題。有關最新信息，請參閱 Python 棄用頁面。

AWS Control Tower landing zone 2.8 版

2022年2月10日

AWS Control Tower landing zone 需要更新至 2.8 版。 若要取得資訊，請參閱更新您的登陸區域)

AWS Control Tower landing zone 2.8 版新增了與AWS 基礎安全最佳實務的最新更新保持一致的功能。

在此版本中：

- 針對日誌封存帳戶中的存取日誌儲存貯體設定存取記錄，以追蹤現有 S3 存取日誌儲存貯體的存取。
- 已新增 Support 生命週期原則的支援。現有 S3 存取日誌儲存貯體的存取日誌設定為預設保留時間為 10 年。
- 此外，此版本更新 AWS Control Tower 以使用所有受管帳戶 (不包括管理帳戶) 中提供的 AWS 服務連結角色 (SLR)，以便您可以設定和管理 Config 規則以符合 AWS Config 最佳實務。 AWS Config 未升級的客戶將繼續使用其現有角色。
- 此版本簡化了加密 AWS Config 資料的 AWS Control Tower KMS 組態程序，並改善中的相關狀態訊息。 CloudTrail
- 此版本包含區域拒絕控制項的更新，以允許中的`route53-application-recovery`功能`us-west-2`。
- 更新：2022 年 2 月 15 日，我們移除了 AWS Lambda 函數的無效字母佇列。

其他詳細資訊：

- 如果您解除 landing zone 的委任，AWS Control Tower 不會移除 AWS Config 服務連結角色。
- 如果您取消佈建 Account Factory 帳戶，AWS Control Tower 不會移除 AWS Config 服務連結角色。

若要將 landing zone 域更新為 2.8，請瀏覽至「登陸區域設定」頁面，選取 2.8 版本，然後選擇「更新」。更新 landing zone 域之後，您必須更新受 AWS Control Tower 管理的所有帳戶，如中所述AWS Control Tower 中的組態更新管理。

二零二一年一月至十

AWS Control Tower 在 2021 年發布了以下更新：

- 區域拒絕功能
- 資料駐留功能
- AWS Control Tower 介紹 Terraform 帳戶佈建和自訂
- 有新的生命週期事件
- AWS Control Tower 啟用巢狀 OU

- Detective 控制並發
- 提供兩個新區域
- 區域取消選擇
- AWS Control Tower 可與 AWS 金鑰管理系統搭配使用
- 控制項已重新命名，功能
- AWS Control Tower 每天掃描 SCP 以檢查漂移
- OU 和帳戶的自訂名稱
- AWS Control Tower landing zone 2.7 版
- 提供三個新 AWS 區域
- 僅控制選取的區域
- AWS Control Tower 現在將管理擴展到 AWS 組織中的現有 OU
- AWS Control Tower 提供大量帳戶更新

區域拒絕功能

2021年11月30日

AWS Control Tower landing zone 無需更新。)

AWS Control Tower 現在提供區域拒絕功能，可協助您限 AWS Control Tower 環境中已註冊帳戶的 AWS 服務和操作的存取。區域拒絕功能可補充 AWS Control Tower 中現有的區域選擇和區域取消選擇功能。這些功能可協助您解決合規性和法規問題，同時平衡擴展至其他區域的相關成本。

例如，德國的 AWS 客戶可以拒絕法蘭克福地區以外的區域存取 AWS 服務。您可以在 AWS Control Tower 設定程序期間或在登陸區域設定頁面中選取受限區域。當您更新 AWS Control Tower 登陸區域版本時，即可使用區域拒絕功能。特定 AWS 服務不受區域拒絕功能的限制。若要深入了解，請參閱設定區域拒絕控制。

資料駐留功能

2021年11月30日

(AWS Control Tower landing zone 無需更新)

AWS Control Tower 現在提供專門建置的控制，協助確保您上傳到 AWS 服務的任何客戶資料僅位於您指定的 AWS 區域。您可以選擇存儲和處理客戶數據的地 AWS 區。如需提供 AWS Control Tower 的完整區 AWS 域清單，請參閱AWS 區域表。

對於精細控制，您可以套用其他控制項，例如「不允許 Amazon 虛擬私人網路 (VPN) 連線」或「禁止 Amazon VPC 執行個體存取網際網路」。您可以在 AWS Control 塔主控台中檢視控制的合規狀態。如需可用控制項的完整清單，請參閱 AWS Control Tower 控制程式庫。

AWS Control Tower 介紹 Terraform 帳戶佈建和自訂

2021年11月29 日

(AWS Control Tower landing zone 的選用更新)

您現在可以使用 Terraform 透過 AWS Control Tower Account Factory (AFT)，透過 AWS Control Tower 帳戶工廠佈建和更新自訂帳戶。

AFT 提供單一 Terraform 基礎設施即程式碼 (IaC) 管道，可佈建由 AWS Control Tower 管理的帳戶。在您將帳戶提供給使用者之前，佈建期間的自訂有助於符合您的業務和安全性原則。

AFT 自動化帳戶創建管道會監控，直到帳戶佈建完成為止，然後繼續進行，從而觸發其他 Terraform 模塊，以使用任何必要的自定義來增強帳戶。作為自訂程序的其他部分，您可以將管線設定為安裝您自己的自訂 Terraform 模組，並且可以選擇新增任何 AFT 功能選項，這些選項由 AWS 一般自訂提供。

按照 AWS Control Tower 使用者指南中提供的步驟開始使用 Terraform 的 AWS Control Tower Account Factory部署適用於地形 (AFT) 的 AWS Control Tower Account Factory，並下載 Terraform 執行個體的 AFT。AFT 支持地形雲，地形企業和地形開源分發。

有新的生命週期事件

2021年11月18日

(AWS Control Tower landing zone 無需更新)

`PrecheckOrganizationalUnit`事件會記錄是否有任何資源封鎖延伸控管工作成功，包括巢狀 OU 中的資源。如需詳細資訊，請參閱 `PrecheckOrganizationalUnit`。

AWS Control Tower 啟用巢狀 OU

2021年11月16 日

(AWS Control Tower landing zone 無需更新)

AWS Control Tower 現在可讓您將巢狀 OU 納入您的 landing zone 域中。

AWS Control Tower 提供巢狀組織單位 (OU) 的支援，可讓您將帳戶組織成多個階層層級，並以階層方式強制執行預防性控制。您可以註冊包含巢狀 OU 的 OU、在父 OU 下建立和註冊 OU，以及在任何已註冊 OU 上啟用控制項，無論深度為何。為了支援此功能，主控台會顯示受控帳戶和 OU 的數目。

使用巢狀 OU，您可以將 AWS Control Tower OU 與 AWS 多帳戶策略配合，並且可以在父 OU 層級強制執行控制，縮短在多個 OU 上啟用控制所需的時間。

關鍵考量

1. 您可以一次向一個 OU 註冊現有的多 AWS Control Tower 級 OU，從頂層 OU 開始，然後向下移動樹狀結構。如需詳細資訊，請參閱 從平面 OU 結構展開為巢狀 OU 結構。
2. 直接在註冊 OU 下的帳戶會自動註冊。樹狀結構下方的帳戶可透過註冊其直屬父系 OU 來註冊。
3. 預防性控制項 (SCP) 會自動向下繼承階層；套用至父項的 SCP 會由所有巢狀 OU 繼承。
4. Detective 控制項 (AWS Config 規則) 不會自動繼承。
5. 每個 OU 都會報告偵測控制的符合性。
6. OU 上的 SCP 漂移會影響其下的所有帳戶和 OU。
7. 您無法在安全性 OU (核心 OU) 底下建立新的巢狀 OU。

Detective 控制並發

2021年11月5 日

(AWS Control Tower landing zone 的選用更新)

AWS Control Tower 偵測控制現在支援偵測控制的同時作業，進而改善易用性和效能。您可以啟用多個偵測控制項，而無需等待個別控制項作業完成。

支援的功能：

- 在相同 OU 上啟用不同的偵測控制 (例如，偵測根使用者的 MFA 是否已啟用，以及偵測是否允許對 Amazon S3 儲存貯體的公用寫入存取權)。
- 同時在不同 OU 上啟用不同的偵測控制項。
- Guardrail 錯誤訊息已改進，為支援的控制項並行作業提供額外的指引。

此版本不支援：

- 不支援在多個 OU 上同時啟用相同的偵測控制。

- 不支援預防性控制並行。

您可以在所有版本的 AWS Control Tower 中體驗偵探控制並行改進。建議您目前未使用 2.7 版的客戶執行 landing zone 域更新，以利用最新版本提供的其他功能，例如區域選擇和取消選擇。

提供兩個新區域

2021年7月29 日

(AWS Control Tower landing zone 需要更新)

AWS Control Tower 現在在另外兩個 AWS 區域提供：南美洲 (聖保羅) 和歐洲 (巴黎)。此更新將 AWS Control Tower 的可用性擴展到 15 個 AWS 區域。

如果您是 AWS Control Tower 的新手，可以立即在任何支援的區域啟動它。在啟動期間，您可以選取希望 AWS Control Tower 建立和管理多帳戶環境的區域。

如果您已經擁有 AWS Control Tower 環境，而且想要在一或多個支援的區域中擴充或移除 AWS Control Tower 管理功能，請前往 AWS Control Tower Teck Teck 儀表板中的「登陸區域設定」頁面，然後選取區域。更新您的 landing zone 之後，您必須更新受 AWS Control Tower 管理的所有帳戶。

區域取消選擇

2021年7月29 日

(AWS Control Tower landing zone 的選用更新)

取消選擇 AWS Control Tower 區域可增強您管理 AWS Control Tower 資源地理佔用空間的能力。您可以取消選取不再希望 AWS Control Tower 管理的區域。此功能可讓您解決合規性和法規問題，同時在擴展至其他區域的相關成本之間取得平衡。

當您更新 AWS Control Tower 登陸區域版本時，即可使用區域取消選取。

當您使用 Account Factory 建立新帳戶或註冊預先存在的成員帳戶，或選取「延伸管理」在現有的組織單位中註冊帳戶時，AWS Control Tower 會在帳戶中選擇的區域中部署其管理功能 (包括集中式記錄、監控和控制)。選擇取消選取某個區域，然後從該區域移除 AWS Control Tower 管理會移除該控管功能，但不會妨礙使用者將 AWS 資源或工作負載部署到這些區域的能力。

AWS Control Tower 可與 AWS 金鑰管理系統搭配使用

2021年7月28日

(AWS Control Tower landing zone 的選用更新)

AWS Control Tower 提供您使用金 AWS 鑰管理服務 (AWS KMS) 金鑰的選項。您可以提供和管理金鑰，以保護 AWS Control Tower 部署的服務 AWS CloudTrail AWS Config，包括和相關的 Amazon S3 資料。 AWS KMS 加密是 AWS Control Tower 預設使用的 SSE-S3 加密增強的加密層級。

將 AWS KMS 支援整合到 AWS Control Tower 與AWS 基礎安全最佳實務保持一致，該實務會為您的敏感日誌檔建議額外一層的安全性。您應該使用 AWS KMS 受管金鑰 (SSE-KMS) 進行靜態加密。AWS 當您設定新的登陸區域或更新現有 AWS Control Tower 登陸區域時，都可以使用 KMS 加密支援。

若要設定此功能，您可以在初始 landing zone 設定期間選取 KMS 金鑰組態。您可以選擇現有的 KMS 金鑰，也可以選取將您導向至 AWS KMS 主控台以建立新的 KMS 金鑰的按鈕。您也可以彈性地從預設加密變更為 SSE-KMS，或變更為不同的 SSE-KMS 金鑰。

對於現有的 AWS Control Tower landing zone，您可以執行更新以開始使用 AWS KMS 金鑰。

控制項已重新命名，功能

2021年7月26日

(AWS Control Tower landing zone 無需更新)

AWS Control Tower 正在修訂某些控制名稱和說明，以更好地反映控制項的政策意圖。修改後的名稱和說明可協助您更直覺地瞭解控制項體現帳戶政策的方式。例如，我們將偵測控制項的一部分名稱從「不允許」變更為「偵測」，因為偵測控制項本身不會停止特定動作，只會偵測原則違規，並透過儀表板提供警示。

控制功能、指導和實作保持不變。僅對控制項名稱和描述進行了修訂。

AWS Control Tower 每天掃描 SCP 以檢查漂移

2021年5月11日

(AWS Control Tower landing zone 無需更新)

AWS Control Tower 現在會對受管 SCP 執行每日自動掃描，以確認對應的控制項是否正確套用，以及它們沒有漂移。如果掃描發現漂移，您將收到通知。AWS Control Tower 每個漂移問題只會傳送一個通知，因此，如果您的 landing zone 已處於漂移狀態，除非找到新的漂移項目，否則您將不會收到其他通知。

OU 和帳戶的自訂名稱

2021年4月16日

(AWS Control Tower landing zone 無需更新)

AWS Control Tower 現在可讓您自訂 landing zone 命名。您可以保留 AWS Control Tower 為組織單位 (OU) 和核心帳戶建議的名稱，也可以在初始 landing zone 設定程序期間修改這些名稱。

AWS Control Tower 為 OU 和核心帳戶提供的預設名稱與 AWS 多帳戶最佳實務指導相符。 不過，如果您的公司具有特定的命名原則，或者您已經擁有相同建議名稱的現有 OU 或帳戶，則新的 OU 和帳戶命名功能可讓您彈性解決這些限制。

與安裝期間的工作流程變更不同，先前稱為核心 OU 的 OU 現在稱為安全性 OU，而先前稱為自訂 OU 的 OU 現在稱為沙箱 OU。我們做了這項變更，是為了改善我們與命名整體 AWS 最佳實務指引的一致性。

新客戶會看到這些新的 OU 名稱。現有客戶將繼續看到這些 OU 的原始名稱。當我們將文件更新為新名稱時，您可能會在 OU 命名中遇到一些不一致的情況。

若要從 AWS 管理主控台開始使用 AWS Control Twer，請前往 AWS Control 塔主控台，然後選取右上角的 [設定 landing zone]。如需其他資訊，您可以閱讀有關規劃 AWS Control Tower landing zone 的相關資訊。

AWS Control Tower landing zone 2.7 版

二 ○ 二一年四月八日

AWS Control Tower landing zone 需要更新至 2.7 版。 若要取得資訊，請參閱更新您的登陸區域)

使用 AWS Control Tower 2.7 版，AWS Control Tower 引入了四個新的強制性預防性日誌存檔控制，這些控制項僅在 AWS Control Tower 資源上實作政策。我們已將四個現有日誌存檔控制的指導從強制性調整為選修，因為它們為 AWS Control Tower 以外的資源設定政策。這項控制變更和擴充可讓您將 AWS Control Tower 內資源的日誌存檔管理與 AWS Control 塔外部的資源管理分開。

這四個變更的控制項可與新的強制控制項搭配使用，為更廣泛的 AWS 記錄檔檔案集提供治理功能。現有的 AWS Control Tower 環境會自動啟用這四個變更的控制項，以保持環境一致性；不過，這些選擇性控制現在可以停用。新的 AWS Control Tower 環境必須啟用所有選擇性控制。現有環境必須先停用先前的強制控制，然後才能將加密新增至未由 AWS Control Tower 部署的 Amazon S3 儲存貯體。

新的強制性控制：

- 不允許變更 AWS Control Tower 在日誌存檔中建立的 S3 儲存貯體的加密組態
- 不允許變更 AWS Control Tower 在日誌存檔中建立 S3 儲存貯體的日誌組態
- 不允許變更 AWS Control Tower 在日誌存檔中建立的 S3 儲存貯體的儲存貯體政策
- 不允許變更 AWS Control Tower 在日誌存檔中建立的 S3 儲存貯體的生命週期組態

指引從強制性變更為選修科目：

- 不允許變更所有 Amazon S3 儲存貯體的加密組態 [先前：針對日誌存檔啟用靜態加密]
- 不允許變更所有 Amazon S3 儲存貯體的日誌組態 [先前：啟用日誌存檔的存取日誌記錄]
- 不允許變更所有 Amazon S3 儲存貯體的儲存貯體政策 [先前：不允許對日誌存檔進行政策變更]
- 不允許變更所有 Amazon S3 儲存貯體的生命週期組態 [先前：設定日誌存檔的保留政策]

AWS Control Tower 2.7 版包含對 AWS Control Tower landing zone 藍圖的變更，升級到 2.7 後可能會導致與舊版不相容。

- 特別是，AWS Control Tower 2.7 版會在 AWS Control Tower 部署的 S3 儲存貯體上`BlockPublicAccess`自動啟用。如果您的工作負載需要跨帳戶存取權，您可以關閉此預設值。如需`BlockPublicaccess`啟用後會發生什麼情況的詳細資訊，請參閱封鎖 Amazon S3 儲存的公開存取。
- AWS Control Tower 版本 2.7 包含 HTTPS 的要求。AWS Control Tower 部署到 S3 儲存貯體的所有請求都必須使用安全通訊端層 (SSL)。只允許 HTTPS 要求傳遞。如果您使用 HTTP (不含 SSL) 作為傳送要求的端點，則此變更會顯示拒絕存取錯誤，這可能會中斷您的工作流程。在 2.7 版更新到您的 landing zone 後，無法還原此變更。

  我們建議您將要求變更為使用 TLS 而非 HTTP。

提供三個新 AWS 區域

二 ○ 二一年四月八日

(AWS Control Tower landing zone 需要更新)

AWS Control Tower 在三個其他區 AWS 域提供：亞太區域 (東京) 區域、亞太區域 (首爾) 區域和亞太區域 (孟買) 區域。若要將管理擴展至這些區域，必須進行 2.7 版的登陸區域更新。

當您執行 2.7 版更新時，您的 landing zone 域不會自動展開到這些區域，您必須在「區域」(Region) 表格中檢視並選取它們以加入。

僅控制選取的區域

2021年2月19日

(AWS Control Tower landing zone 無需更新)

AWS Control Tower 區域選擇可讓您更好地管理 AWS Control Tower 資源的地理佔用空間。若要擴充託管 AWS 資源或工作負載的區域數目 (基於合規性、法規、成本或其他原因)，您現在可以選取要管理的其他區域。

您可以在設定新的登陸區域或更新 AWS Control Tower landing zone 域版本時使用 landing zone 域選擇。當您使用 Account Factory 建立新帳戶或註冊預先存在的成員帳戶，或者當您使用延伸管理在現有的組織單位中註冊帳戶時，AWS Control Tower 會在帳戶中選擇的區域中部署集中式記錄、監控和控制等控管功能。如需選取「區域」的更多資訊，請參閱設定您的 AWS Control Tower 區域。

AWS Control Tower 現在將管理擴展到 AWS 組織中的現有 OU

2021年1月28日

(AWS Control Tower landing zone 無需更新)

從 AWS Control Tower 主控台將管理擴展到現有組織單位 (OU) (非 AWS Control Tower 中的組織單位)。使用此功能，您可以將頂層 OU 和內含帳戶納入 AWS Control Tower 管理。如需將控管擴充至整個 OU 的相關資訊，請參閱向 AWS Control Tower 註冊現有的組織單位。

當您註冊 OU 時，AWS Control Tower 會執行一系列檢查，以確保在 OU 內成功擴展管理和註冊帳戶。如需 OU 初始註冊相關的常見問題的詳細資訊，請參閱註冊或重新註冊時失敗的常見原因。

您也可以造訪 AWS Control Tower 產品網頁或瀏覽 YouTube 觀看此影片，了解 AWS Control Tower 入門的相關影片 AWS Organizations。

AWS Control Tower 提供大量帳戶更新

2021年1月28日

(AWS Control Tower landing zone 無需更新)

透過大量更新功能，您現在可以從 AWS Control Tower 儀表板更新已註冊 AWS Organizations 組織單位 (OU) 中的所有帳戶，其中包含多達 300 個帳戶，只要按一下即可。這在您更新 AWS Control Tower 登陸區域時特別有用，並且還必須更新註冊的帳戶以使其與目前的 landing zone 域版本對齊。

此功能也可協助您在更新 AWS Control Tower 登陸區域以擴展到新區域時，或是當您想要重新註冊 OU 以確保該 OU 中的所有帳戶都套用最新控制時，讓帳戶保持在最新狀態。大量帳戶更新不需要一次更新一個帳戶，或使用外部指令碼在多個帳號上執行更新。

若要取得有關更新 landing zone 域的資訊，請參閱更新您的登陸區域。

如需註冊或重新註冊 OU 的相關資訊，請參閱向 AWS Control Tower 註冊現有的組織單位。

二零二零年一月至十

在 2020 年，AWS Control Tower 發布了以下更新：

- AWS Control Tower 主控台現在可連結至外部 AWS Config 規則
- AWS Control Tower 現已在其他區域提供
- 護欄更新
- AWS Control Tower 主控台顯示有關 OU 和帳戶的更多詳細資訊
- 使用 AWS Control Tower 設定新的多帳戶 AWS 環境 AWS Organizations
- AWS Control Tower 解決方案的自訂
- AWS Control Tower 2.3 版正式推出
- AWS Control Tower 中的單一步驟帳戶佈建
- AWS Control Tower 解除委任工具
- AWS Control Tower 生命週期事件通知

AWS Control Tower 主控台現在可連結至外部 AWS Config 規則

2020年12月29 日

AWS Control Tower landing zone 需要更新至 2.6 版。 若要取得資訊，請參閱更新您的登陸區域)

AWS Control Tower 現在包含組織層級彙總工具，可協助偵測外部 AWS Config 規則。除了 AWS AWS Control Tower 建立的 Config 規則之外，您還可以在 AWS Control Tower 主控台中查看外部建立的 AWS Config 規則是否存在。彙總器可讓 AWS Control Tower 偵測外部規則，並提供 Con AWS fig 主控台的連結，而無需 AWS Control Tower 即可存取未受管帳戶。

透過此功能，您現在可以將偵探控制套用至帳戶的整合檢視，以便追蹤合規性並判斷是否需要額外的帳戶控制項。如需詳細資訊，請參閱 AWS Control Tower 如何彙總非受管 OU 和帳戶中的 AWS Config 規則。

AWS Control Tower 現已在其他區域提供

2020年11月18日

AWS Control Tower landing zone 需要更新至 2.5 版。 若要取得資訊，請參閱更新您的登陸區域)

AWS Control Tower 現在可在 5 個其他 AWS 區域使用：

- 亞太 (新加坡) 區域
- 歐洲 (法蘭克福) 區域
- 歐洲 (倫敦) 區域
- 歐洲 (斯德哥爾摩) 區域
- 加拿大 (中部) 區域

這 5 個 AWS 區域的新增是 AWS Control Tower 2.5 版推出的唯一變更。

AWS Control Tower 也在美國東部 (維吉尼亞北部) 區域、美國東部 (俄亥俄) 區域、美國西部 (奧勒岡) 區域、歐洲 (愛爾蘭) 區域和亞太區域 (雪梨) 區域提供。此次推出後，AWS Control Tower 現在可在 10 個 AWS 區域使用。

此 landing zone 域更新包含列示的所有區域，且無法復原。將 landing zone 域更新為 2.5 版後，您必須手動更新 AWS Control Tower 的所有註冊帳戶，以便在 10 個支援的區 AWS 域中進行管理。如需相關資訊，請參閱設定您的 AWS Control Tower 區域。

護欄更新

二 ○ 二 ○ 年十月八日

(AWS Control Tower landing zone 無需更新)

已針對強制性控制項發行更新版本`AWS-GR_IAM_ROLE_CHANGE_PROHIBITED`。

需要對控制進行此項變更，因為自動註冊到 AWS Control Tower 的帳戶必須啟用`AWSControlTowerExecution`角色。先前版本的控制項會防止建立此角色。

如需詳細資訊，請參閱不允許變更 AWS Control Tower 設定的 AWS IAM 角色和 AWS Control Tower 控制參考指南 AWS CloudFormation中的。

AWS Control Tower 主控台顯示有關 OU 和帳戶的更多詳細資訊

2020年7月22日

(AWS Control Tower landing zone 無需更新)

您可以檢視未在 AWS Control Tower 註冊的組織和帳戶，以及已註冊的組織和帳戶。

在 AWS Control 塔主控台中，您可以檢視有關 AWS 帳戶和組織單位 (OU) 的更多詳細資訊。[帳戶] 頁面現在會列出組織中的所有帳戶，無論 AWS Control Tower 的 OU 或註冊狀態為何。您現在可以搜尋、排序和篩選所有表格。

使用 AWS Control Tower 設定新的多帳戶 AWS 環境 AWS Organizations

二零二零年四月廿二

(AWS Control Tower landing zone 無需更新)

AWS Organizations 客戶現在可以利用以下新功能，使用 AWS Control Tower 來管理新建立的組織單位 (OU) 和帳戶：

- 現有 AWS Organizations 客戶現在可以在其現有管理帳戶中為新的組織單位 (OU) 設定新的 landing zone。您可以在 AWS Control Tower 中建立新的 OU，並使用 AWS Control Tower 管理在這些 OU 中建立新帳戶。
- AWS Organizations 客戶可以使用帳戶註冊程序或透過指令碼註冊現有帳戶。

AWS Control Tower 提供使用其他服務的協調 AWS 服務。它專為擁有多個帳戶和團隊的組織而設計，他們正在尋找最簡單的方法來設置新的或現有的多帳戶 AWS 環境並大規模管理。透過由 AWS Control Tower 管理的組織，雲端管理員知道組織中的帳戶符合既定政策。建築商可以從中受益，因為他們可以快速佈建新 AWS 帳戶，而不必擔心合規性。

若要取得有關設置 landing zone 的資訊，請參閱〈〉規劃您的 AWS Control Tower landing zone。您也可以造訪 AWS Control Tower 產品網頁或瀏覽 YouTube 觀看此影片，了解 AWS Control Tower 入門的相關影片 AWS Organizations。

除了這項變更之外，AWS Control Tower 中的快速帳戶佈建功能已重新命名為註冊帳戶。現在，它允許註冊現有 AWS 帳戶以及創建新帳戶。如需詳細資訊，請參閱 註冊現有帳戶。

AWS Control Tower 解決方案的自訂

二零二零年三月十七

(AWS Control Tower landing zone 無需更新)

AWS Control Tower 現在包含新的參考實作，可讓您輕鬆地將自訂範本和政策套用到 AWS Control Tower landing zone。

透過 AWS Control Tower 的自訂功能，您可以使用 AWS CloudFormation 範本將新資源部署到組織內的現有帳戶和新帳戶。除了 AWS Control Tower 已提供的 SCP 之外，您還可以將自訂服務控制政策 (SCP) 套用至這些帳戶。AWS Control Tower 管道的自訂項目與 AWS Control Tower 生命週期事件和通知 (AWS Control Tower 的生命週期事件) 整合，以確保資源部署與您的 landing zone 保持同步。

此 AWS Control Tower 解決方案架構的部署文件可透過解決方AWS 案網頁取得。

AWS Control Tower 2.3 版正式推出

二零二零年三月五日

AWS Control Tower landing zone 需要更新。 如需詳細資訊，請參閱更新您的登陸區域。)

除了美國東部 (俄亥俄)、美國東部 (維吉尼亞北部)、美國西部 (奧勒岡) 和歐洲 (愛爾蘭) AWS 區域外，AWS Control Tower 現已在亞太區域 (雪梨) 提供。新增的亞太區域 (雪梨) 區域是 AWS Control Tower 2.3 版推出的唯一變更。

如果您之前尚未使用過 AWS Control Tower Teck，您可以立即在任何支援的區域啟動它。如果您已在使用 AWS Control Tower，並且想要將其管理功能擴展到帳戶中的亞太區域 (雪梨) 區域，請前往 AWS Control Tower 儀表板中的 「設定」 頁面。從那裡，將您的 landing zone 更新為最新版本。然後，單獨更新您的帳戶。

> **Note**
>
> 更新您的 landing zone 不會自動更新您的帳戶。如果您有幾個以上的帳戶，則所需的更新可能很耗時。因此，我們建議您避免將 AWS Control Tower landing zone 域擴展到不需要執行工作負載的區域。

如需部署到新區域時偵探控制預期行為的相關資訊，請參閱設定 AWS Control Tower Tall 區域。

AWS Control Tower 中的單一步驟帳戶佈建

二零二零年三月二日

(AWS Control Tower landing zone 無需更新)

AWS Control Tower 現在支援透過 AWS Control Tower 主控台進行單一步驟帳戶佈建。此功能可讓您從 AWS Control 塔主控台內佈建新帳戶。

若要使用簡化表單，請導覽至 AWS Control Tower 主控台中的 Account Factory，然後選擇快速帳戶佈建。AWS Control Tower 會將相同的電子郵件地址指派給已佈建帳戶，以及為該帳戶建立的單一登入 (IAM 身分中心) 使用者。如果您需要這兩個電子郵件地址不同，則必須透過 Service Catalog 佈建您的帳戶。

使用 Service Catalog 和 AWS Control Tower 帳戶工廠，透過快速帳戶佈建來更新您建立的帳戶，就像對任何其他帳戶的更新一樣。

> **Note**
>
> 2020 年 4 月，快速帳戶佈建功能已重新命名為註冊帳戶。2022 年 6 月，在 AWS Control 塔主控台中建立和更新帳戶的能力與註冊 AWS 帳戶的能力分開。如需詳細資訊，請參閱 註冊現有帳戶。

AWS Control Tower 解除委任工具

二零二零年二月28日

(AWS Control Tower landing zone 無需更新)

AWS Control Tower 現在支援自動化解除委任工具，協助您清理 AWS Control Tower 分配的資源。如果您不想再為企業使用 AWS Control Tower，或者您需要重新部署組織資源，則可能需要清理最初設定 landing zone 時建立的資源。

若要使用主要是自動化的程序來解除使用 landing zone 域的使用，請聯絡 AWS Support 以取得所需其他步驟的協助。如需解除委任的更多資訊，請參閱逐步解說：解除委任 AWS Control Tower 登陸區。

AWS Control Tower 生命週期事件通知

二零二零年一月二十

(AWS Control Tower landing zone 無需更新)

AWS Control Tower 宣布生命週期事件通知的可用性。生命週期事件標誌著 AWS Control Tower 動作的完成，該動作可以變更資源狀態，例如組織單位 (OU)、帳戶和由 AWS Control Tower 建立和管理的控制項。生命週期事件會記錄為 AWS CloudTrail 事件，並以事件 EventBridge 形式傳送給 Amazon。

AWS Control Tower 會記錄下列可使用服務執行的動作完成後的生命週期事件：建立或更新 landing zone、建立或刪除 OU、啟用或停用 OU 的控制；以及使用帳戶工廠建立新帳戶或將帳戶移至其他 OU。

AWS Control Tower 使用多種 AWS 服務來建立和管理多帳戶 AWS 環境的最佳實務。AWS Control Tower 動作可能需要幾分鐘的時間才能完成。您可以在 CloudTrail 日誌中追蹤生命週期事件，以確認原始 AWS Control Tower 動作是否成功完成。您可以建立 EventBridge 規則，在 CloudTrail 記錄生命週期事件時通知您，或自動觸發自動化工作流程中的下一個步驟。

二零一九年一月至十

從 2019 年 1 月 1 日到 12 月 31 日，AWS Control Tower 發布了以下更新：

- AWS Control Tower 2.2 版的正式推出
- AWS Control Tower 中的新選擇性控制
- AWS Control Tower 中的新偵探控制
- AWS Control Tower 接受與管理帳戶不同網域的共用帳戶的電子郵件地址
- AWS Control Tower 2.1 版的正式推出

AWS Control Tower 2.2 版的正式推出

二零一九年11月13日

AWS Control Tower landing zone 需要更新。 如需詳細資訊，請參閱更新您的登陸區域。)

AWS Control Tower 2.2 版提供三種新的預防性控制，可防止帳戶出現漂移：

- 不允許變更 AWS Control Tower 設定的 Amazon CloudWatch 日誌日誌群組
- 不允許刪除 AWS Control To AWS Config wer 建立的彙總授權
- 不允許刪除記錄存檔

控制項是一項高階規則，可為您的整體 AWS 環境提供持續的治理。當您建立 AWS Control Tower 登陸區域時，landing zone 域和所有組織單位 (OU)、帳戶和資源都符合您選擇的控制項強制執行的管理規則。當您和您的組織成員使用 landing zone 時，可能會發生此合規狀態的變更 (意外或故意)。漂移檢測可幫助您識別需要更改或配置更新以解決漂移的資源。如需詳細資訊，請參閱 偵測並解決 AWS Control Tower 中的漂移。

AWS Control Tower 中的新選擇性控制

二零一九年九月五日

(AWS Control Tower landing zone 無需更新)

AWS Control Tower 現在包含下列四個新的選擇性控制：

- 不允許在沒有 MFA 的 Amazon S3 儲存貯體上執行刪除動作
- 不允許變更 Amazon S3 儲存貯體的複寫組態
- 不允許以根使用者身分執行動作
- 不允許為根使用者建立存取金鑰

控制項是一項高階規則，可為您的整體 AWS 環境提供持續的治理。護欄可讓您表達政策目的。如需詳細資訊，請參閱關於 AWS Control Tower 中的控制。

AWS Control Tower 中的新偵探控制

二零一九年八月25日

(AWS Control Tower landing zone 無需更新)

AWS Control Tower 現在包含以下八個新偵探控制項：

- 偵測是否已啟用 Amazon S3 儲存貯體的版本控制
- 偵測主控台的 IAM 使用者是否已啟用 MFA AWS
- 偵測 IAM 使用者是否已啟用 MFA
- 偵測 Amazon EC2 執行個體是否已啟用亞馬遜 EBS 優化
- 偵測 Amazon EBS 磁碟區是否已連接至 Amazon EC2 執行個體
- 偵測是否已啟用 Amazon RDS 資料庫執行個體的公開存取
- 偵測是否已啟用對 Amazon RDS 資料庫快照的公開存取

- 偵測 Amazon RDS 資料庫執行個體是否已啟用儲存加密

控制項是一項高階規則，可為您的整體 AWS 環境提供持續的治理。偵測控制項可偵測帳號內資源的不符合性 (例如原則違規)，並透過儀表板提供警示。如需詳細資訊，請參閱關於 AWS Control Tower 中的控制。

AWS Control Tower 接受與管理帳戶不同網域的共用帳戶的電子郵件地址

二零一九年八月一日

(AWS Control Tower landing zone 無需更新)

在 AWS Control Tower 中，您現在可以為網域與管理帳戶的電子郵件地址不同的共用帳戶 (記錄存檔和稽核成員) 和子帳戶 (使用帳戶工廠出售) 提交電子郵件地址的電子郵件地址。只有在您建立新的 landing zone 以及佈建新的兒童帳戶時，才能使用此功能。

AWS Control Tower 2.1 版的正式推出

二零一九年6月24日

AWS Control Tower landing zone 需要更新。 如需詳細資訊，請參閱更新您的著陸區。)

AWS Control Tower 現已正式推出，並支援生產使用。AWS Control Tower 適用於擁有多個帳戶和團隊的組織，他們正在尋求設定新的多帳戶 AWS 環境和大規模管理的最簡單方法。使用 AWS Control Tower，您可以協助確保組織中的帳戶符合既定政策。分散式團隊的終端使用者可以快速佈建新 AWS 帳戶。

使用 AWS Control Tower，您可以設定使用最佳實務的 landing zone，例如使用設定多帳戶結構 AWS Organizations、管理使用者身分和聯合存取、透過 Service Catalog 啟用帳戶佈建 AWS IAM Identity Center，以及使用和建立集中式記錄存檔。 AWS CloudTrail AWS Config

對於持續的治理，您可以啟用預先設定的控制項，這些控制項是明確定義的安全性、作業和合規性規則。護欄有助於防止部署不符合策略的資源，並持續監控已部署的資源是否不符合。AWS Control Tower 儀表板可讓您集中掌握 AWS 環境，包括佈建的帳戶、啟用控制項以及帳戶的合規狀態。

只要在 AWS Control Twer 主控台按一下，即可設定新的多帳戶環境。使用 AWS Control Tower 不需支付額外費用或預先承諾。您只需為已啟用設定 landing zone 域和實作選取控制項的 AWS 服務付費。

文件歷史記錄

- 最新文件更新：2024 年 5 月 20 日

下表說明 AWS Control Tower 使用者指南的重要變更。如需有關文件更新的通知，您可以訂閱 RSS 摘要。

變更	描述	日期
AWS Control Tower 最多支援 100 個同時控制操作	並行控制作業配額增加至 100。	2024年5月20日
AWS Control Tower 於 AWS 卡加利西部 (加拿大) 區域提供	加拿大西部 (卡加利) 區域提供 AWS Control Tower。	2024年5月3日
AWS Control Tower 支援自助配額調整	AWS Control Tower 已與主控台中的 AWS Service Quotas 整合。	2024年4月25日
將控制項的文件移至新的指南	AWS Control Tower 發佈了控制參考指南。	2024年4月21 日
標記`EnabledControl` 資源 AWS CloudFormation	AWS Control Tower 支援透過 AWS CloudFormation 範本向`EnabledControl` 資源新增標籤。	2024年2月22 日
可用的基準 API	AWS Control Tower 發布了用於以程式設計方式註冊 OU 的新 API	2024年2月14日
AWS Control Tower landing zone 3.3 版	提供 AWS Control Tower landing zone 3.3 版本。	2023 年 12 月 14 日
AWS Control Tower 宣佈針對數位主權提供協助的控制	AWS Control Tower 發布了一組控制，以協助滿足數位主權要求的客戶。	2023 年 11 月 27 日

AWS Control Tower 支援 landing zone 域 API	AWS Control Tower 支援使用新 API 設定和啟動登陸區域。	2023 年 11 月 26 日
AWS Control Tower 支援啟用標記的控制	AWS Control Tower 支援在主控台和新 API 中標記啟用的控制項。	2023 年 11 月 10 日
AWS Control Tower 於亞太區域 (墨爾本) 提供 AWS 區域	僅適用於亞太區域 (墨爾本) 區域。	2023 年 11 月 3 日
提供新的控制 API	AWS Control Tower 發布了新的控制 API。	2023年10月14日
AWS Control Tower 推出新的控制	AWS Control Tower 發布了新的主動和偵探控制。	2023 年 10 月 5 日
AWS Control Tower 報告偏離停用受信任存取	如果客戶在中關閉受信任的 AWS Control Tower 存取，AWS Control Tower 會在發生漂移時通知客戶 AWS Organizations。	2023 年 9 月 21 日
另外提供四個 AWS Control Tower AWS 區域	適用於亞太區域 (海德拉巴)、歐洲 (西班牙和蘇黎世) 和中東 (阿拉伯聯合大公國)。	2023 年 9 月 13 日
AWS Control Tower 於特拉維夫區域提供	AWS Control Tower 在特拉維夫區域 il-central-1 提供。	2023 年 8 月 28 日
AWS Control Tower 推出 28 個新的主動式控制	AWS Control Tower 發布了 28 個新的主動控制。	2023 年 7 月 24 日
AWS Control Tower 棄用 2 個控制	AWS Control Tower 將從控制程式庫中移除兩個控制，自 2023 年 8 月 18 日起生效。	2023 年 7 月 18 日
提供 AWS Control Tower landing zone 3.2	提供 AWS Control Tower landing zone 3.2 版。	2023 年 6 月 16 日

AWS Control Tower 根據 ID 處理帳戶	AWS Control Tower 會追蹤 AWS 帳戶 ID，而非帳戶的電子郵件地址。	2023 年 6 月 14 日
提供額外的 Security Hub 偵測控制	AWS Control Tower 針對 Security Hub 服務管理標準：AWS Control Tower 新增了十個控制項程式庫。	2023 年 6 月 12 日
AWS Control Tower 發佈控制中繼資料表	AWS Control Tower 現在提供控制中繼資料表，做為已發佈文件的一部分。	2023 年 6 月 7 日
Account Factory 定制的地形支持	AFC 中地形開放原始碼藍圖的單一區域支援。	2023 年 6 月 6 日
AWS 適用於 landing zone 域的 IAM 自我管理	AWS Control Tower 現在支援客戶選擇 landing zone 的身分供應商。	2023 年 6 月 6 日
已新增角色	AWS Control Tower 新增了新的服務連結角AWSServiceRoleForAWSControlTower色和相關政策。AWSControlTowerAccountServiceRolePolicy	2023 年 6 月 1 日
混合治理更新	更新以向客戶提供混合治理的建議。	2023 年 6 月 1 日
提供其他主動式控制	全新的主動式控制可協助您管理多帳戶環境，並達成特定控制目標。	2023 年 5 月 19 日

提供七個額外區域	AWS Control Tower 現在另外提供七個服務 AWS 區域：北加州 (舊金山)、亞太區域 (香港、雅加達和大阪)、歐洲 (米蘭)、中東 (巴林) 和非洲 (開普敦)。	2023 年 4 月 19 日
變更為受管理策略	我們變更了，AWSControlTowerServiceRolePolicy讓 AWS Control Tower 可以呼叫 AWS 帳戶管理服務實作的 `ListRegions` 、`GetRegionOptStatus` API。`EnableRegion`	2023 年 4 月 6 日
一般提供帳戶自訂要求追蹤	AWS Control Tower 現在支援使用 Terraform Account Factory (AFT) 工作流程追蹤帳戶自訂請求的功能。	2023 年 2 月 16 日
IAM 最佳做法更新	更新指南以符合 IAM 最佳實務建議。如需更多詳細資訊，請參閱 IAM 中的安全最佳實務。	2023 年 2 月 15 日
提供 AWS Control Tower landing zone 3.1	提供 AWS Control Tower landing zone 3.1。	2023 年 2 月 9 日
一般提供主動式控制	主動式控制功能會從預覽狀態啟動到正式上市。	2023 年 1 月 24 日
並行帳戶作業	AWS Control Tower 現在可在帳戶工廠支援最多五 (5) 個同時動作。您一次最多可以建立、更新或註冊五個帳戶。	2022 年 12 月 16 日
主動式控制可協助資源佈建	AWS Control Tower 現在支援透過 AWS CloudFormation 掛接實作的主動式控制。	2022 年 11 月 28 日

客戶工廠定制可用	AWS Control Tower 現在可直接從 AWS Control Tower 台支援使用可自訂帳戶範本 (稱為藍圖) 佈建帳戶。	2022 年 11 月 28 日
可檢視所有 AWS Config 規則的符合性狀態	AWS Control Tower 現在會顯示部署到 AWS Control Tower 註冊組織單位的所有 AWS Config 規則的合規狀態。	2022 年 11 月 18 日
變更為受管理策略	我們變更了，以AWSControlTowerServiceRolePolicy便 AWS Control Tower 可以擔任該AWSControlTowerBlueprintAccess 角色，這是 Account Factory 自訂所需的角色。	2022 年 10 月 28 日
用於控制項、 AWS CloudFormation 資源的 API	AWS Control Tower 現在支援透過一組 API 呼叫和新 AWS CloudFormation 資源啟用和停用控制。	2022 年 9 月 1 日
CFCT 支持堆棧集刪除	CFCT 通過在清單文件中設置參數來支持堆棧集刪除。	2022 年 8 月 26 日
自訂記錄保留	您可以針對存放 AWS Control Tower CloudTrail 日誌的 Amazon S3 儲存貯體自訂保留政策，以天數或年為單位，最長可達 15 年。	2022 年 8 月 15 日
提供角色漂移修復	AWS Control Tower 支援角色漂移的修復，無需完整修復 landing zone。	2022 年 8 月 11 日

版本 3.0 可用	AWS Control Tower landing zone 3.0 版從帳戶型 AWS CloudTrail 追蹤變更為組織型追蹤，並更新受管政策以啟用組織層級追蹤。它可讓您僅彙總您所在地區的 AWS Config 資訊。3.0 版還包括區域拒絕控制的更新，以及兩個新的偵探控制。	2022 年 7 月 29 日
「組織」頁面結合了 OU 和帳戶的檢視	AWS Control Tower 中的新組織頁面會顯示所有組織單位 (OU) 和帳戶的階層式檢視。	2022 年 7 月 18 日
變更為受管理策略	我們變更了，以AWSControlTowerServiceRolePolicy便客戶可以擁有組織層級的 AWS CloudTrail 追蹤來彙總 AWS CloudTrail 記錄檔。	2022 年 6 月 20 日
更輕鬆地註冊和更新會員帳戶	AWS Control Tower 現在可讓您從 landing zone 個別註冊和更新成員帳戶。每個帳戶都會顯示何時可用更新。我們將 [註冊帳戶] 按鈕與 [Account Factory] 中的 [建立帳戶] 工作流程中	2022 年 5 月 31 日
AFT 支援共用帳戶的自訂功能	適用於 Terraform 的 AWS Control Tower Account Factory 現在支援 AWS Control Tower 管理帳戶、日誌存檔和稽核帳戶的自訂功能。	2022 年 5 月 27 日
所有選擇性控制項的並行作業	AWS Control Tower 現在可讓您同時套用和移除選用的預防性防護，以及偵探控制。	2022 年 5 月 18 日

現有的安全性和記錄帳戶	AWS Control Tower 現在支援使用現有安全和記錄帳戶的功能，而不是在 landing zone 設定期間建立新帳戶。	2022 年 5 月 16 日
2.9 版本可供選擇	AWS Control Tower landing zone 2.9 版更新了通知轉發器 Lambda，以使用 Python 版本 3.9 執行階段。	2022 年 4 月 22 日
對於 AWS 最佳實踐更新的支持，2.8 版可用	AWS Control Tower landing zone 2.8 版提供額外的支援，以確保您的工作負載和 AWS 帳戶符合 AWS 最佳實務。	2022 年 2 月 10 日
區域拒絕控制	AWS Control Tower 現在包含一個控制項，可協助您限制對 AWS 區域的存取，以解決合規和法規問題。	2021 年 11 月 30 日
資料駐留控制	AWS Control Tower 現在支援控制項，協助您透過精細控制來管理資料駐留。	2021 年 11 月 30 日
適用於地形的 AWS Control Tower 帳戶工廠	AWS Control Tower 現在支援用於自動化帳戶佈建和更新的 Terraform。	2021 年 11 月 29 日
有新的生命週期事件	`PrecheckOrganizationalUnit` 事件會記錄是否有任何資源封鎖延伸控管工作成功，包括巢狀 OU 中的資源。	2021 年 11 月 18 日
提供巢狀 OU	AWS Control Tower 現在可讓您的 landing zone 域包含巢狀 OU 結構。	2021 年 11 月 16 日

Detective 控制並發	AWS Control Tower 偵測控制現在支援並行啟用和停用操作。	2021 年 11 月 5 日
提供兩個新區域	AWS Control Tower 現已在兩個新區 AWS 域推出：歐洲 (巴黎) 區域和南美洲 (聖保羅) 區域。	2021 年 7 月 29 日
區域取消選擇	您可以透過 AWS Control Tower 取消選取不再需要管理的 AWS 區域。	2021 年 7 月 29 日
可用的 KMS 金鑰	您可以選擇性地建立或選擇您管理的 KMS 金鑰，以加密資料和資源。	2021 年 7 月 28 日
變更為受管理策略	我們變更了，以AWSControlTowerServiceRolePolicy便客戶可以將自己的 KMS 加密金鑰用於 AWS CloudTrail 記錄檔。	2021 年 7 月 28 日
控制項名稱已變更，功能不變	某些控制項名稱和說明已更新，以更好地反映控制項的原則意圖，而不會變更功能。	2021 年 7 月 26 日
自動掃描受管理的 SCP	AWS Control Tower 對受管 SCP 執行每日自動掃描，以檢查漂移情況。	2021 年 5 月 11 日
OU 和帳戶的自訂名稱	AWS Control Tower 可讓您在 landing zone 設定程序期間為基本 OU 和帳戶提供自訂名稱，而不會產生漂移。	2021 年 4 月 16 日

停用 landing zone 是自助服務	AWS Control Tower 現在可讓您解除 landing zone 的委任，而無需聯絡 Sup AWS port 部門。退役是一種無法復原的半自動化程序。這與手動刪除所有 AWS Control Tower 資源不同。	2021 年 4 月 9 日
三個額外的區域	AWS Control Tower 現已在三個額外區 AWS 域提供：亞太區域 (東京) 區域、亞太區域 (首爾) 區域和亞太區域 (孟買) 區域。	2021 年 4 月 8 日
新的日誌存檔控制項，提供 2.7 版 landing zone	四個新的日誌存檔控制提供 AWS Control Town 資源的日誌存檔管理，與 AWS Control Tower 外部的資源管理分開。有關現行四項管制的指引，已由強制性改為選修科目。AWS Control Tower landing zone 2.7 版包含 HTTPS 的要求，在您更新之後無法還原。	2021 年 4 月 8 日
區域選擇	AWS Control Tower 區域選擇可讓您更好地管理 AWS Control Tower 資源的地理佔用空間。若要擴充託管 AWS 資源或工作負載的區域數目 (基於合規性、法規、成本或其他原因)，您現在可以選取要管理的其他區域。	2021 年 2 月 19 日
在 AWS Control Tower 一次註冊 OU 並管理其所有帳戶	AWS Control Tower 新增了註冊 OU 的功能，這是讓多個帳戶同時進行管理的一種方式。	2021 年 1 月 28 日

已註冊 OU 中的多個帳戶更新	您現在可以從 AWS Control Tower 儀表板按一下，更新任何已註冊 AWS Organizations 組織單位 (OU) 中包含最多 300 個帳戶的所有帳戶。多帳戶更新功能也稱為大量更新，無需一次更新一個帳戶，或使用外部指令碼一起對多個帳戶執行更新。	2021 年 1 月 28 日
彙總未受管 OU 和帳戶的新角色	新角色可協助偵測外部 AWS Config 規則，因此 AWS Control Tower 不需要取得未受管帳戶的存取權。	2020 年 12 月 29 日
AWS Control Tower 在更多區 AWS 域提供。	AWS Control Tower 現在可部署在亞太區域 (新加坡) 區域、歐洲 (法蘭克福) 區域、歐洲 (倫敦) 區域、歐洲 (斯德哥爾摩) 區域和加拿大 (中部) 區域。此次推出後，AWS Control Tower 現在可在 10 個 AWS 區域使用。此 landing zone 域更新包含列出的所有區域，且無法復原。將 landing zone 域更新為 2.5 版後，您必須手動更新 AWS Control Tower 的所有註冊帳戶，以便在 10 個支援的區 AWS 域中進行管理。	2020 年 11 月 18 日
控制項更新	已針對強制控制項發行更新版本`AWS-GR_IAM_ROLE_CHANGE_PROHIBITED` 。更新的控制項可讓您更輕鬆地自動註冊帳戶。	2020 年 10 月 8 日

AWS Control Tower 現已提供相關資訊頁面	相關資訊頁面可讓您更輕鬆地找到在設定 AWS Control Tower landing zone 後可能會有所幫助的常見任務。	2020 年 9 月 18 日
AWS Control Tower 主控台顯示有關 OU 和帳戶的更多詳細資訊。	在 AWS Control 塔主控台中，您可以檢視有關 AWS 帳戶和組織單位 (OU) 的更多詳細資訊。「帳戶」頁面現在會列出組織中的所有帳戶，無論 AWS Control Tower 的 OU 或註冊狀態為何。您現在可以搜尋、排序和篩選所有表格。	2020 年 7 月 22 日
AWS Control Tower 可讓現有組織設定 landing zone	您現在可以在現有組織中為 AWS Control Tower 啟動 landing zone，以將組織納入治理中。AWS Control Tower 中的快速帳戶佈建功能已重新命名為註冊帳戶，現在允許註冊現有 AWS 帳戶以及建立新帳戶。	2020 年 4 月 16 日
AWS Control Tower 現已在亞太地區推出	AWS Control Tower 現在可在亞太區域 (雪梨) AWS 區域部署。此版本需要手動更新付款帳戶，只有在您打算在亞太區域 (雪梨) 執行工作負載時才更新。	2020 年 3 月 3 日
可以停用 AWS Control Tower landing zone	AWS Support 務可以透過大部分自動化程序來協助您永久解除 landing zone 的委任，不過需要進行一些手動清理作業。	2020 年 2 月 27 日

AWS Control Tower 提供快速帳戶佈建	當您的登陸區域處於最新狀態時，搭配 Enroll account (註冊帳戶) 功能，快速帳戶佈建可讓您更輕鬆地啟動新的成員帳戶。	2020 年 2 月 20 日
AWS Control Tower 會追蹤生命週期事件	生命週期事件提供特定 AWS Control Tower 事件的其他詳細資訊，讓某些工作流程自動化更容易。	2019 年 12 月 12 日
AWS Control Tower 提供設定和活動頁面	[設定] 和 [活動] 頁面可讓您更輕鬆地更新登陸區域和檢視記錄事件。	二○一九年十一月三
AWS Control Tower 還提供其他預防性控制	AWS Control Tower 中的預防性控制可讓您的組織和資源與您的環境保持一致。	2019 年 9 月 6 日
AWS Control Tower 提供其他偵探控制	AWS Control Tower 中的 Detective 控制可提供組織狀態和資源的相關資訊。	2019 年 8 月 27 日
AWS Control Tower 現已正式推出	AWS Control Tower 是一項服務，提供大規模設定和管理多帳戶 AWS 環境的最簡單方法。	2019 年 6 月 24 日

AWS 詞彙表

有關最新 AWS 術語，請參閱AWS 詞彙表 參考文獻中的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。