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 提供簡單的方法來設定和管理 AWS 多帳戶環境，並遵循規範性最佳實務。AWS Control Tower 會協調數個AWS 其他服務的功能，包括 AWS Organizations AWS Service Catalog、和 AWS IAM Identity Center，以在不到一小時的時間內建置登陸區域。資源會代表您設定和管理。

AWS Control Tower 協同運作擴展了 的功能 AWS Organizations。為了協助避免您的組織和帳戶偏離，這與最佳實務不同，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安全日誌和必要的跨帳戶存取許可已建立，而不會變更。

如果您託管多個帳戶，則擁有協調層有助於帳戶部署和帳戶控管。您可以採用 AWS Control Tower 做為佈建帳戶和基礎設施的主要方式。透過 AWS Control Tower，您可以更輕鬆地遵守公司標準、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 AWS Account Factory 中的可設定帳戶範本，快速佈建新帳戶。同時，您的中央雲端管理員可以監控所有帳戶是否符合整個公司的既定合規政策。

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

功能

AWS Control Tower 具有下列功能：

- 登陸區域 – 登陸區域是一種架構良好的多帳戶環境，以安全和合規最佳實務為基礎。這是整個企業的容器，可存放所有組織單位 (OUs)、帳戶、使用者和其他您希望受合規法規規範的資源。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 環境提供持續的控管。其表示的方式是普通語言。有三種類型的控制：預防性、偵測性和主動性。三類指引適用於控制項：強制性、強烈建議或選擇性。如需控制項的詳細資訊，請參閱 控制的運作方式。
- Account Factory – Account Factory 是一種可設定的帳戶範本，可協助使用預先核准的帳戶組態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 – 儀表板可為中央雲端管理員團隊持續監控您的登陸區域。使用儀表板查看整個企業的佈建帳戶、啟用政策強制執行的控制項、啟用持續偵測政策不一致性的控制項，以及由帳戶和 OUs 整理的不合規資源。

AWS Control Tower 如何與其他 AWS 服務互動

AWS Control Tower 建置在信任且可靠的 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 服務整合到可協助您將現有工作負載遷移到其中的解決方案中 AWS。如需詳細資訊，請參閱如何利用 AWS Control Tower 和 CloudEndure 將工作負載遷移至 AWS。

組態、控管和可擴展性

- 自動化帳戶組態：AWS Control Tower 會透過 Account Factory （或「自動販賣機」）自動執行帳戶部署和註冊，其建置為佈建產品上的抽象概念 AWS Service Catalog。Account Factory 可以建立和註冊 AWS 帳戶，並自動將控制項和政策套用至這些帳戶的程序。如需建立和佈建帳戶的詳細資訊，請參閱佈建方法。
- 集中式控管：透過採用 的功能 AWS Organizations，AWS Control Tower 會設定架構，確保跨多帳戶環境的一致性合規和管理。 AWS Organizations 此服務提供管理多帳戶環境的基本功能，包括帳戶的集中控管和管理、從 AWS Organizations APIs建立帳戶、服務控制政策 (SCPs)，以及資源控制政策 RCPs)。

- 可擴展性：您可以直接在 和 AWS Control Tower 主控台中工作 AWS Organizations，以建置或擴展您自己的 AWS Control Tower 環境。您可以在註冊現有組織並將現有帳戶註冊到 AWS Control Tower 之後，看到 AWS Control Tower 中反映的變更。您可以更新 AWS Control Tower 登陸區域，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 合作夥伴解決方案搭配 AWS Control Tower。

您是第一次使用 AWS Control Tower 嗎？

若您是第一次使用此服務，我們建議您閱讀以下內容：

1. 如果您需要如何規劃和組織登陸區域的詳細資訊，請參閱 規劃您的 AWS Control Tower 登陸區域和 AWS AWS Control Tower 登陸區域的多帳戶策略。
2. 若您已準備好建立第一個登陸區，請參閱AWS Control Tower 入門。
3. 如需漂移偵測和預防的資訊，請參閱在 AWS Control Tower 中偵測並解決偏離。
4. 如需安全詳細資訊，請參閱AWS Control Tower 的安全性。
5. 如需更新登陸區域和成員帳戶的資訊，請參閱 AWS Control Tower 中的組態更新管理。

AWS Control Tower 的運作方式

本節在高階說明 AWS Control Tower 的運作方式。您的登陸區域是所有 AWS 資源的架構良好的多帳戶環境。您可以使用此環境，對所有 AWS 帳戶強制執行合規法規。

AWS Control Tower 登陸區域的結構

AWS Control Tower 中登陸區域的結構如下：

- 根 — 包含登陸區域中所有其他 OUs父系。
- 安全性 OU – 此 OU 包含日誌封存和稽核帳戶。這些帳戶通常稱為共用帳戶。當您啟動登陸區域時，您可以選擇這些共用帳戶的自訂名稱，而且您可以選擇將現有 AWS 帳戶帶入 AWS Control Tower 以進行安全性和記錄。不過，這些帳戶稍後無法重新命名，而且無法在初始啟動後為安全性和記錄新增現有帳戶。
- 沙盒 OU – 如果您啟用沙盒 OU，則會在您啟動登陸區域時建立沙盒 OU。此和其他已註冊OUs 包含您的使用者用來執行工作負載 AWS 的註冊帳戶。
- IAM Identity Center 目錄 – 根據預設，此目錄會存放您的 IAM Identity Center 使用者。它定義了每個 IAM Identity Center 使用者的許可範圍。或者，您可以選擇自行管理您的身分和存取控制。如需詳細資訊，請參閱使用 AWS IAM Identity Center 和 AWS Control Tower。
- IAM Identity Center 使用者 – 這些是使用者可以擔任的身分，以在登陸區域中執行 AWS 工作負載。

設定登陸區域時會發生什麼情況

當您設定登陸區域時，AWS Control Tower 會在您的管理帳戶中代表您執行下列動作：

- 建立組織根結構中包含的兩個 AWS Organizations 組織單位 (OUs)：安全性和沙盒 （選用）。
- 在安全性 OU 中建立或新增兩個共用帳戶：日誌封存帳戶和稽核帳戶。
- 如果您選擇預設 AWS Control Tower 組態，或允許您自行管理身分提供者，即可在 IAM Identity Center 中建立雲端原生目錄，其中包含預先設定的群組和單一登入存取。
- 套用所有必要的預防性控制，以強制執行政策。
- 套用所有必要的偵測性控制項來偵測組態違規。
- 預防性控制不會套用至管理帳戶。
- 除了 管理帳戶之外，控制項會套用至整個組織。

安全地管理 AWS Control Tower 登陸區域和帳戶中的資源

- 當您建立登陸區域時，會建立許多 AWS 資源。若要使用 AWS Control Tower，您不得在本指南所述的支援方法之外修改或刪除這些 AWS Control Tower 受管資源。刪除或修改這些資源會導致您的登陸區域進入未知狀態。如需詳細資訊，請參閱建立和修改 AWS Control Tower 資源的指引
- 當您啟用選用控制項（具有強烈建議或選擇性指引的控制項）時，AWS Control Tower 會建立它在帳戶中管理 AWS 的資源。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狀態。

什麼是共用帳戶？

在 AWS Control Tower 中，您登陸區域中的共用帳戶會在設定期間佈建：管理帳戶、日誌封存帳戶和稽核帳戶。

什麼是管理帳戶？

這是您專為登陸區域建立的帳戶。此帳戶用於支付登陸區域中所有項目的帳單。它也用於帳戶的帳戶工廠佈建，以及管理 OUs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。

什麼是日誌封存帳戶？

此帳戶可做為登陸區域中所有帳戶之 API 活動和資源組態日誌的儲存庫。

如需詳細資訊，請參閱日誌封存帳戶。

什麼是稽核帳戶？

稽核帳戶是受限制的帳戶，旨在讓您的安全與合規團隊讀取和寫入您登陸區域中所有帳戶的存取權。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。

控制的運作方式

控制項是為整體 AWS 環境提供持續控管的高階規則。每個控制項都會強制執行單一規則，並以純語言表示。您可以隨時從 AWS Control Tower 主控台或 AWS Control Tower APIs 變更有效選擇性或強烈建議使用的控制項。強制控制項一律會套用，而且無法變更。

預防性控制可防止動作發生。例如，名為不允許對 Amazon S3 儲存貯體的儲存貯體政策進行變更的選擇性控制（先前稱為不允許對日誌封存進行政策變更）可防止日誌封存共用帳戶中的任何 IAM 政策變更。任何執行阻止動作的嘗試都會遭到拒絕，並記錄在 CloudTrail 中。資源也會登入 AWS Config。

Detective 控制項會在特定事件發生時偵測，並在 CloudTrail 中記錄動作。例如，針對連接至 Amazon EC2 執行個體的 Amazon EBS 磁碟區啟用加密時， 強烈建議的控制項會偵測未加密的 Amazon EBS 磁碟區是否連接至登陸區域中的 EC2 執行個體。

在帳戶中佈建資源之前，主動控制會檢查資源是否符合您的公司政策和目標。如果資源不合規，則不會佈建這些資源。主動控制會監控透過 CloudFormation 範本部署在帳戶中的資源。

對於熟悉的人 AWS：在 AWS Control Tower 中，預防性控制會使用服務控制政策 SCPs) 和資源控制政策 RCPs) 實作。Detective 控制項會使用 AWS Config 規則實作。主動控制會使用 CloudFormation 勾點實作。

相關主題

- 在 AWS Control Tower 中偵測並解決偏離

AWS Control Tower 如何與 StackSets 搭配使用

AWS Control Tower 預設會使用 CloudFormation StackSets 來設定您帳戶中的資源。每個堆疊集都有對應至帳戶和 AWS 區域 每個帳戶的 StackInstances。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 會根據 CloudFormation 參數， AWS 區域 選擇性地將更新套用至特定帳戶。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 CloudFormation 更新期間指定的參數，預期行為的快速摘要：

如果堆疊集更新包含範本的變更（即指定 `TemplateBody`或 `TemplateURL` 屬性），或者指定 `Parameters` 屬性，則在更新指定帳戶中的堆疊執行個體之前， 會 CloudFormation 標記狀態為過期的所有堆疊執行個體，以及 AWS 區域。如果堆疊集更新不包含範本或參數的變更， 會 CloudFormation 更新指定帳戶和區域中的堆疊執行個體，同時讓所有其他堆疊執行個體保持其現有的堆疊執行個體狀態。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 CloudFormation 《 使用者指南》中的更新您的堆疊集。

術語

以下是您將在 AWS Control Tower 文件中看到的一些術語的快速檢閱。

首先，最好知道 AWS Control Tower 與 AWS Organizations 服務共用許多術語，包括出現在本文件中的組織和組織單位 (OU) 一詞。

- 如需組織和 OUs 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，該術語是一個很好的開始。
- AWS Organizations 是一項 AWS 服務，可協助您在工作負載成長和擴展時，集中管理環境 AWS。AWS Control Tower 依賴 AWS Organizations 來建立帳戶、在 OU 層級強制執行預防性控制，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 AWS 的帳戶。有時候，帳戶工廠會以非正式方式稱為帳戶的「販賣機」。
- 您的 AWS Control Tower 主區域是 AWS 部署 AWS Control Tower 登陸區域的區域。您可以在登陸區域設定中檢視您的主要區域。
- AWS Service Catalog 可讓您集中管理經常部署的 IT 服務。在本文件的內容中，Account Factory 會使用 AWS Service Catalog 來佈建新 AWS 帳戶，包括自訂藍圖中的帳戶。
- AWS CloudFormation StackSets 是一種延伸堆疊功能的資源類型，可讓您使用單一操作和單一 CloudFormation 範本，跨多個帳戶和區域建立、更新或刪除堆疊。
- Astack 執行個體是區域內目標帳戶中堆疊的參考。
- Astack 是您可以單一單位管理的一組 AWS 資源。
- 彙整工具是一種 AWS Config 資源類型，可從組織內的多個帳戶和區域收集 AWS Config 組態和合規資料，讓您可以在單一帳戶中檢視和查詢此合規資料。
- 一致性套件是 AWS Config 規則和修補動作的集合，可部署為帳戶和區域中的單一實體，或 中的整個組織 AWS Organizations。您可以使用一致性套件來協助自訂 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 中的基準是一組資源和特定組態，您可以套用至目標。最常見的基準目標可能是組織單位 (OU)。例如，名為 的基準`AWSControlTowerBaseline`可協助您向 AWS Control Tower 註冊 OUs。在登陸區域設定和更新期間，基準目標可能是共用帳戶，或整個登陸區域的特定設定。
- 藍圖：藍圖是封裝一些中繼資料的成品，描述在帳戶中部署的基礎設施元件。例如，CloudFormation 範本可以做為 AWS Control Tower 帳戶的藍圖。

- 偏離：由 AWS Control Tower 安裝和設定的資源變更。沒有偏離的資源可讓 AWS Control Tower 正常運作。
- 不合規資源：違反規則的資源，該 AWS Config 規則定義了特定的偵測控制。
- 共用帳戶：設定登陸區域時，AWS Control Tower 會自動建立的三個帳戶之一：管理帳戶、日誌封存帳戶和稽核帳戶。您可以在設定期間選擇日誌封存帳戶和稽核帳戶的自訂名稱。
- 成員帳戶：成員帳戶屬於 AWS Control Tower 組織。您可以在 AWS Control Tower 中註冊或取消註冊成員帳戶。當已註冊的 OU 包含已註冊和未註冊帳戶的混合時：
  - 在 OU 上啟用（或繼承）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 層級使用 SCPs、RCPS 或宣告政策強制執行，而不是帳戶層級。如需詳細資訊，請參閱 文件中的 AWS Organizations 服務控制政策繼承。
  - 在 OU 上啟用的偵測控制不適用於未註冊的帳戶。
  - 主動控制由 AWS CloudFormation 勾點實作。這些控制項不適用於 OU 中的未註冊帳戶。

  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。成員帳戶可以移至組織的根容器。
- AWS 帳戶： AWS 帳戶充當資源容器和資源隔離界限。 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為 AWS account. AWS accounts。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（也稱為護欄) 是高階規則，可為整體 AWS Control Tower 環境提供持續的控管。每個控制項都會強制執行單一規則。預防性控制是使用 SCPs。Detective 控制項是使用 AWS Config 規則實作。主動控制會使用 CloudFormation 勾點實作。如需詳細資訊，請參閱控制的運作方式。
- Control Catalog：AWS Control Tower 控制目錄是可透過 AWS Control Tower 在主控台和 APIs 中取得的所有控制項的摘要。它先前稱為 Control Library。我們將術語與命名空間 controlcatalog 的名稱進行比對。
- 登陸區域：登陸區域是一種提供建議起點的雲端環境，包括預設帳戶、帳戶結構、網路和安全配置等。從登陸區域，您可以部署利用解決方案和應用程式的工作負載。
- 架構：架構是特定的法規標準或產業需求。在 Control Catalog 上下文中，架構由標準控制項表示。如需詳細資訊，請參閱 Control Catalog Ontology 概觀。
- 巢狀 OU：AWS Control Tower 中的巢狀 OU 是包含在另一個 OU 中的 OU。巢狀 OU 可以只有一個父 OU，而且每個帳戶可以是一個 OU 的成員。巢狀 OUs會建立階層。當您將政策連接到階層中的其中一個 OUs 時，政策會向下流動，並影響其下的所有 OUs和帳戶。AWS Control Tower 中的巢狀 OU 階層最多可深度五個層級。
- 父 OU：OU 緊接在階層中目前 OU 的上方。每個 OU 只能有一個父 OU。

- 子 OU：階層中低於目前 OU 的任何 OU。OU 可以有許多子 OUs。
- OU 階層：在 AWS Control Tower 中，巢狀 OUs 的階層最多可以有五個層級。巢狀的順序稱為關卡。階層的頂端會指定為層級 1。
- 最上層 OU：最上層 OU 是直接在根下的任何 OU，而不是根本身。根不會被視為 OU。
- 受管：受管區域由 AWS Control Tower 根據您的組織設定的控管政策，在您的環境中管理和控制。這些 AWS 區域 都會受到監控，以遵守最佳實務和組織政策。當您啟用 AWS Control Tower 控制項時，這些區域中的資源會受到保護。
- 未受管：顯示未受管狀態的區域不受 AWS Control Tower 控制或監控。這些政策 AWS 區域 通常不遵守 AWS Control Tower 強制執行的相同控管政策。您可以在這些區域中建立資源，但這些資源不受 AWS Control Tower 控制項保護。
- 拒絕：AWS Control Tower 特別封鎖拒絕的區域。在 AWS Control Tower 環境中，您無法在這些 中佈建資源 AWS 區域。

定價

使用 AWS Control Tower 無需額外費用。您只需支付 AWS Control Tower 啟用 AWS 的服務，以及您在登陸區域中使用的服務。例如，您需為向 Account Factory 佈建帳戶的 Service Catalog 以及在您的登陸區域中追蹤 AWS CloudTrail 的事件付費。如需 AWS Control Tower 定價和相關費用的相關資訊，請參閱 AWS Control Tower 定價。

如果您從 AWS Control Tower 的帳戶執行暫時性工作負載，您可能會看到與 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，請聯絡您的 AWS 客戶代表。若要進一步了解 如何搭配 AWS Control Tower AWS Config 運作，請參閱 使用 監控資源變更 AWS Config。

如果您在 AWS Control Tower 外部實作 AWS CloudTrail 線索，您可以將它們與 AWS Control Tower 搭配使用。不過，如果您也選擇加入 AWS Control Tower 管理的線索，則可能會產生重複的費用。我們不建議設定外部線索，除非您有特定需求。如果您選擇在登陸區域設定或更新期間加入，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 成本的資訊，請參閱管理 CloudTrail 成本。

設定

AWS Control Tower 第一次使用 之前，請遵循本節中的步驟來建立 AWS 帳戶並保護您的 AWS Control Tower 管理帳戶。如需專門針對 的其他設定任務的資訊 AWS Control Tower，請參閱 AWS Control Tower 入門。

註冊 AWS

當您註冊 Amazon Web Services (AWS) 時， AWS 您的帳戶會自動註冊所有 服務 AWS，包括 AWS Control Tower。如果您已經有 AWS 帳戶，請跳到下一個任務。如果您沒有 AWS 帳戶，請使用下列程序來建立帳戶。

請記下您的 AWS 帳戶號碼，因為您需要用於其他任務。

註冊 AWS 帳戶

如果您沒有 AWS 帳戶，請完成下列步驟來建立一個。

註冊 AWS 帳戶

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

   部分註冊程序需接收來電或簡訊，並在電話鍵盤輸入驗證碼。

   當您註冊 時 AWS 帳戶，AWS 帳戶根使用者會建立 。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。作為安全最佳實務，請將管理存取權指派給使用者，並且僅使用根使用者來執行需要根使用者存取權的任務。

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

建立具有管理存取權的使用者

註冊 後 AWS 帳戶，請保護 AWS 帳戶根使用者、啟用 AWS IAM Identity Center和建立管理使用者，以免將根使用者用於日常任務。

保護您的 AWS 帳戶根使用者

1. 選擇根使用者並輸入 AWS 帳戶 您的電子郵件地址，以帳戶擁有者AWS 管理主控台身分登入 。在下一頁中，輸入您的密碼。

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

2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

   如需說明，請參閱《IAM 使用者指南》中的為您的 AWS 帳戶 根使用者 （主控台） 啟用虛擬 MFA 裝置。

建立具有管理存取權的使用者

1. 啟用 IAM Identity Center。

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

2. 在 IAM Identity Center 中，將管理存取權授予使用者。

   如需使用 IAM Identity Center 目錄 做為身分來源的教學課程，請參閱AWS IAM Identity Center 《 使用者指南》中的使用預設值設定使用者存取 IAM Identity Center 目錄。

以具有管理存取權的使用者身分登入

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

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

指派存取權給其他使用者

1. 在 IAM Identity Center 中，建立一個許可集來遵循套用最低權限的最佳實務。

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的建立許可集。

2. 將使用者指派至群組，然後對該群組指派單一登入存取權。

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的新增群組。

您帳戶的安全性

您可以在 AWS Organizations 文件中找到有關如何設定保護 AWS Control Tower 帳戶安全之最佳實務的其他指導。

- 管理帳戶的最佳實務
- 成員帳戶的最佳實務

下一步驟

AWS Control Tower 入門

AWS Control Tower 入門

此入門程序適用於 AWS Control Tower 管理員。當您準備好使用 AWS Control Tower 主控台或 APIs 設定登陸區域時，請遵循此程序。

如果您目前是 AWS 客戶，但剛加入 AWS Control Tower，建議您檢閱名為 的 區段規劃您的 AWS Control Tower 登陸區域，然後再繼續。

主題

- AWS Control Tower 快速入門指南
- 先決條件：管理帳戶的自動化啟動前檢查
- 設定控制項專用環境
- 從主控台開始使用 AWS Control Tower
- 使用 APIs 開始使用 AWS Control Tower
- 後續步驟

AWS Control Tower 快速入門指南

如果您是初次使用 AWS，您可以依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. 設定和啟動您的登陸區域。

> **Note**
>
> AWS Control Tower 會設定付費服務 AWS CloudTrail AWS Config，例如 Amazon CloudWatch、Amazon S3 和 Amazon VPC。使用時，這些服務可能會產生費用，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 本身不會建立額外費用。

開始之前

在開始設定程序之前要做出的最重要決策是選擇您的主要區域。您的主要區域是您將在其中執行大部分工作負載或存放大部分資料 AWS 的區域。在您設定 AWS Control Tower 登陸區域之後，就無法變更。如需如何選擇主要區域的詳細資訊，請參閱 登陸區域設定的管理秘訣。

> **Note**
>
> 根據預設，AWS Control Tower 會選擇您的帳戶目前運作的區域做為您的主要區域。您可以在管理主控台畫面的 AWS 右上角看到目前的區域。

快速入門程序假設您會接受 AWS Control Tower 環境中資源的預設值。其中許多選項稍後都可以變更。在名為 的區段中，會列出幾個一次性選項對登陸區域組態的期望。

如果您已建立新 AWS 帳戶，它會自動符合設定 AWS Control Tower 所需的先決條件。您可以繼續執行下列步驟。

快速入門步驟

1. 使用您的管理員使用者登入資料登入 AWS 管理主控台。
2. 導覽至位於 https：//https://console.aws.amazon.com/controltower 的 AWS Control Tower 主控台。
3. 確認您是在所需的主要區域中工作。
4. 選擇設定登陸區域。
5. 遵循 主控台中的指示，接受所有預設值。您需要輸入帳戶的電子郵件地址、日誌封存帳戶和稽核帳戶。
6. 確認您的選擇，然後選擇設定登陸區域。
7. AWS Control Tower 大約需要 30 分鐘的時間來設定登陸區域中的所有資源。

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

> **Note**
>
> 如果您是第一次遇到設定問題，請聯絡 AWS Support 以取得診斷協助。

先決條件：管理帳戶的自動化啟動前檢查

在 AWS Control Tower 設定登陸區域之前，它會自動在您的帳戶中執行一系列啟動前檢查。這些檢查不需要採取任何動作，以確保您的管理帳戶已準備好進行建立登陸區域的變更。以下是 AWS Control Tower 在設定登陸區域之前執行的檢查：

- 的現有服務限制 AWS 帳戶 必須足以讓 AWS Control Tower 啟動。如需詳細資訊，請參閱AWS Control Tower 中的限制和配額。
- AWS 帳戶 必須訂閱下列 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 Identity Center) 客戶的考量事項

- 如果已設定 AWS IAM Identity Center (IAM Identity Center)，AWS Control Tower 主區域必須與 IAM Identity Center 區域相同。
- IAM Identity Center 只能安裝在組織的管理帳戶中。
- 根據您選擇的身分來源，三個選項適用於您的 IAM Identity Center 目錄：
  - IAM Identity Center 使用者商店：如果 AWS Control Tower 是使用 IAM Identity Center 設定，AWS Control Tower 會在 IAM Identity Center 目錄中建立群組，並為您選取的使用者佈建對這些群組的存取權。
  - Active Directory：如果使用 Active Directory 設定 AWS Control Tower 的 IAM Identity Center，AWS Control Tower 不會管理 IAM Identity Center 目錄。它不會將使用者或群組指派給新 AWS 帳戶。
  - 外部身分提供者：如果使用外部身分提供者 (IdP) 設定 AWS Control Tower 的 IAM Identity Center，AWS Control Tower 會在 IAM Identity Center 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。您可以在帳戶建立期間，從帳戶工廠的外部 IdP 指定現有使

用者，而 AWS Control Tower 會在 IAM Identity Center 與外部 IdP 之間同步相同名稱的使用者時，提供該使用者新付費帳戶的存取權。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，這些使用者將可存取您已註冊的帳戶。

如需使用 IAM Identity Center 和 AWS Control Tower 的詳細資訊，請參閱 IAM Identity Center 帳戶和 AWS Control Tower 的須知事項

AWS Config 和 AWS CloudTrail 客戶的考量事項

- AWS 帳戶 無法在組織管理帳戶中啟用受信任存取 AWS Config。如需有關如何停用受信任存取的資訊，請參閱如何啟用或停用受信任存取 AWS Organizations 的文件。
- 如果您計劃在 AWS Control Tower 註冊的任何現有帳戶中有現有的 AWS Config 記錄器、交付管道或彙總設定，您必須在設定登陸區域之後，先修改或移除這些組態，才能開始註冊帳戶。此預先檢查不適用於登陸區域啟動期間的 AWS Control Tower 管理帳戶。如需詳細資訊，請參閱註冊具有現有 AWS Config 資源的帳戶。
- 如果您從 AWS Control Tower 的帳戶執行暫時性工作負載，您可能會看到與 Config AWS 相關的成本增加。如需管理這些成本的詳細資訊，請聯絡您的 AWS 客戶代表。
- 當您向 AWS Control Tower 註冊帳戶時，您的帳戶會受 AWS Control Tower 組織的 AWS CloudTrail 追蹤所管理。如果您在帳戶中已有 CloudTrail 追蹤的現有部署，除非您在 AWS Control Tower 中註冊帳戶之前刪除該帳戶的現有追蹤，否則可能會看到重複費用。如需組織層級追蹤和 AWS Control Tower 的資訊，請參閱 定價。

> **Note**
>
> 啟動時，必須在管理帳戶中啟用 AWS Control Tower 管理的所有區域 AWS 的安全字符服務 (STS) 端點。否則，啟動可能會在組態過程中途發生失敗。

設定控制項專用環境

使用 AWS Control Tower 登陸區域 4.0，您現在可以建立僅限控制的環境，而無需實作完整的登陸區域。此部署選項專為擁有已建立的 AWS Organizations 設定，並希望透過 AWS Control Tower 控制目錄專注於採用受管控制的客戶而設計。

主題

開始使用

首先從首頁檢閱 AWS Control Tower Control Catalog，以了解可用的受管控制項、其相關聯的合規架構，以及控制中繼資料。若要在 AWS Control Tower 上啟用此體驗，請選取我有現有環境，並想要在主控台上啟用 AWS 受管控制項。然後，您將確認您的主要區域，並選擇性地選取其他受管區域。在設定期間，您可以啟用自動帳戶註冊，以確保帳戶在 OU 之間移動時自動繼承其父組織單位 (OUs) 的控制項和組態。

AWS Config 考量事項

您可以選擇在初始設定 AWS Config 期間或之後視需要啟用 。 AWS Config 如果您計劃在環境中使用偵測性控制項，則需要 。如果您選擇啟用 AWS Config，則需要指定彙總器帳戶來收集組態和合規資料。您可以在設定期間選取現有帳戶或建立新的帳戶。其他選項包括設定 AWS KMS 金鑰加密，以及指定記錄的 Amazon S3 日誌保留期間。

實作程序

如果您不使用 AWS Config繼續，您的環境將立即準備好在 Control Catalog 中進行預防性和主動性控制。

不過，當您準備好啟用第一個偵測控制時，您需要透過`ConfigBaseline`在目標 OUs 上啟用的新 來啟用 AWS Config 記錄。這是每個 OU 的一次性設定程序，並根據每個 AWS 區域每個 OU 的帳戶數量和每個帳戶的資源產生 AWS Config 定價。

重要說明

建立 AWS Control Tower 環境會與 建立信任關係 AWS Organizations、啟用預防性控制的偏離偵測，以及追蹤帳戶和 OU 變更。在設定期間，AWS Control Tower 會建立登陸區域組態，做為受管控制環境的基礎。

若要透過 APIs 建立控制項專用環境，請參閱：使用 APIs 開始使用 AWS Control Tower。請注意，資訊清單欄位現在在登陸區域 4.0 為選用。

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 Tower 主控台設定登陸區域時，請遵循此程序。從開始到結束，大約需要半小時。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 客戶，但剛加入 AWS Control Tower，建議您檢閱名為 的 區段規劃您的 AWS Control Tower 登陸區域，然後再繼續。

主題

對登陸區域組態的期望

設定 AWS Control Tower 登陸區域的程序有多個步驟。AWS Control Tower 登陸區域的某些層面是可設定的。其他選項無法在設定後變更。

設定期間要設定的關鍵項目

- 您可以在設定期間選取最上層 OU 名稱，也可以在設定登陸區域之後變更 OU 名稱。根據預設，最上層OUs 會命名為安全性和沙盒。如需詳細資訊，請參閱設定架構良好的環境的指導方針。
- 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，預設稱為日誌封存和稽核，但您無法在設定後變更這些名稱。（這是一次性選擇。）
- 在設定期間，您可以選擇指定 AWS Control Tower 的現有 AWS 帳戶，以用作稽核和日誌封存帳戶。如果您打算指定現有的 AWS 帳戶，而且這些帳戶有現有的 AWS Config 資源，您必須先刪除現有的 AWS Config 資源，才能將帳戶註冊到 AWS Control Tower。（這是一次性選擇。）
- 如果您是第一次設定 ，或者要升級到登陸區域 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 AWS CloudTrail 追蹤，也可以選擇退出由 AWS Control Tower 管理的追蹤，以及管理您自己的 CloudTrail 追蹤。您可以隨時更新登陸區域，選擇加入或退出由 AWS Control Tower 管理的組織層級追蹤。
- 當您設定或更新登陸區域時，您可以選擇為 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。
- 您可以選擇指定先前定義的藍圖，用於從 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 使用帳戶工廠自訂 (AFC) 自訂帳戶。

無法復原的組態選項

- 設定登陸區域之後，您就無法變更主要區域。
- 如果您要使用 VPCs 佈建帳戶工廠帳戶，則無法在建立 VPC CIDRs 之後對其進行變更。

步驟 1：建立您的共用帳戶電子郵件地址

如果您要在新的 中設定登陸區域 AWS 帳戶，請參閱 設定。

- 若要使用新的共用帳戶設定登陸區域，AWS Control Tower 需要兩個尚未與 相關聯的唯一電子郵件地址 AWS 帳戶。這些電子郵件地址將做為協作收件匣 -- 共用電子郵件帳戶 -- 用於您企業中將執行與 AWS Control Tower 相關特定工作的各種使用者。
- 如果您是第一次設定 AWS Control Tower，而且要將現有的安全性和日誌封存帳戶帶入 AWS Control Tower，則可以輸入現有 AWS 帳戶的目前電子郵件地址。

以下項目需要電子郵件地址：

- 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群組。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 – 此帳戶適用於需要存取登陸區域中已註冊 OUs 內所有已註冊帳戶的所有記錄資訊的使用者團隊。

當您建立登陸區域時，這些帳戶會在安全 OU 中設定。根據最佳實務，我們建議您在這些帳戶中執行動作時，應使用具有適當範圍許可的 IAM Identity Center 使用者。

> **Note**
>
> 如果您將現有 AWS 帳戶指定為稽核和日誌封存帳戶，則現有帳戶必須通過一些啟動前檢查，以確保沒有任何資源與 AWS Control Tower 要求衝突。如果這些檢查未成功，您的登陸區域設定可能無法成功。特別是，帳戶不得有現有的 AWS Config 資源。如需詳細資訊，請參閱引進現有安全或記錄帳戶的考量事項。

為了清楚起見，本使用者指南一律會參考共用帳戶的預設名稱：日誌封存和稽核。當您閱讀本文件時，如果您選擇自訂名稱，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檢視具有自訂名稱的帳戶。

> **Note**
>
> 我們正在變更一些 AWS Control Tower 組織單位 (OUs) 預設名稱的術語，以符合 AWS 多帳戶策略。在我們進行轉換以改善這些名稱的清晰度時，您可能會注意到一些不一致。安全 OU 先前稱為核心 OU。沙盒 OU 先前稱為自訂 OU。

步驟 2. 設定和啟動您的登陸區域

啟動 AWS Control Tower 登陸區域之前，請先判斷最適合的主區域。如需詳細資訊，請參閱登陸區域設定的管理秘訣。

> **Important**
>
> 在部署 AWS Control Tower 登陸區域之後變更您的主要區域需要解除委任以及 AWS Support 的協助。不建議此做法。

了解如何使用 AWS CLI 中的 來設定和啟動您的登陸區域使用 APIs 開始使用 AWS Control Tower。

若要在主控台中設定和啟動登陸區域，請執行下列一系列步驟。

準備：導覽至 AWS Control Tower 主控台

1. 開啟 Web 瀏覽器，然後導覽至位於 https：//https://console.aws.amazon.com/controltower 的 AWS Control Tower 主控台。
2. 在 主控台中，確認您是在 AWS Control Tower 所需的主區域中工作。然後選擇設定您的登陸區域。

步驟 2a。檢閱並選取您的 AWS 區域

請確定您已正確指定您為主要 AWS 區域選取的區域。部署 AWS Control Tower 之後，您就無法變更主要區域。

在設定程序的本節中，您可以新增所需的任何其他 AWS 區域。您可以視需要在稍後新增更多區域，也可以從控管中移除區域。

選取要管理的其他 AWS 區域

1. 面板會顯示目前的區域選擇。開啟下拉式選單以查看可用於控管的其他區域清單。
2. 勾選每個區域旁的方塊，讓 AWS Control Tower 進行控管。您的主要區域選擇無法編輯。

拒絕存取特定區域

若要拒絕存取特定 AWS 區域中 AWS 的資源和工作負載，請在區域拒絕控制區段中選取已啟用。根據預設，此控制項的設定未啟用。

步驟 2b. 設定您的組織單位 OUs)

如果您接受這些 OUs 的預設名稱，則不需要採取任何動作即可繼續設定。若要變更 OUs 的名稱，請直接在表單欄位中輸入新名稱。

- 基礎 OU – AWS Control Tower 倚賴最初名為 Security OU 的基礎 OU。 您可以在初始設定期間和之後，從 OU 詳細資訊頁面變更此 OU 的名稱。此安全 OU 包含兩個共用帳戶，預設情況下稱為日誌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 OUs。除了安全 OU 之外，我們建議您在登陸區域中佈建至少一個額外的 OU。如果此額外 OU 適用於開發專案，建議您將其命名為沙盒 OU，如 中所述設定架構良好的環境的指導方針。如果您已有現有的 OU AWS Organizations，您可能會看到略過在 AWS Control Tower 中設定其他 OU 的選項。

步驟 2c：設定共用帳戶、記錄和加密

在設定程序的本節中，面板會顯示共用 AWS Control Tower 帳戶名稱的預設選擇。這些帳戶是您登陸區域的重要部分。請勿移動或刪除這些共用帳戶。您可以在設定期間選擇稽核和日誌封存帳戶的自訂名稱。或者，您也可以選擇將現有 AWS 帳戶指定為共用帳戶。

您必須為日誌封存和稽核帳戶提供唯一的電子郵件地址，而且您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。

關於共用帳戶

- 管理帳戶 – AWS Control Tower 管理帳戶是根層級的一部分。管理帳戶允許 AWS Control Tower 計費。帳戶也具有登陸區域的管理員許可。您無法在 AWS Control Tower 中為帳單和管理員許可建立個別帳戶。

管理帳戶顯示的電子郵件地址在此設定階段無法編輯。它會顯示為確認，因此您可以檢查您是否正在編輯正確的管理帳戶，以防您有多個帳戶。

- 兩個共用帳戶 – 您可以為這兩個帳戶選擇自訂名稱，或自備自己的帳戶，而且您必須為每個帳戶提供唯一的電子郵件地址，無論是新帳戶或現有帳戶。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相關聯的 AWS 帳戶。

若要設定共用帳戶，請填寫請求的資訊。

1. 在 主控台中，輸入最初稱為日誌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之帳戶的名稱。許多客戶選擇將其稱為安全帳戶。
4. 為此帳戶提供唯一的電子郵件地址。

選擇性地設定日誌保留

在此設定階段，您可以自訂 Amazon S3 儲存貯體的日誌保留政策，將 AWS CloudTrail 日誌存放在 AWS Control Tower 中，以天數或年為單位遞增，最長可達 15 年。如果您選擇不自訂您的日誌保留，則標準帳戶記錄的預設設定為一年，存取記錄的預設設定為 10 年。當您更新或重設登陸區域時，也可以使用此功能。

選擇性自我管理 AWS 帳戶 存取

您可以選取 AWS Control Tower 是否使用 AWS Identity and Access Management (IAM) 設定 AWS 帳戶 存取權，還是使用您可以自行設定和自訂的 AWS 帳戶 AWS IAM Identity Center 使用者、角色和許可，或是使用其他方法，例如外部 IdP，透過 IAM Identity Center 直接聯合帳戶或聯合多個帳戶。您可以稍後變更此選項。

根據預設，AWS Control Tower AWS 會為您的登陸區域設定 IAM Identity Center，以符合使用多個帳戶整理 AWS 環境時所定義的最佳實務指引。大多數客戶都會選擇預設值。有時需要替代的存取方法，才能在特定產業或國家/地區，或是無法使用 IAM Identity Center AWS AWS 區域 的法規合規。

不支援在帳戶層級選擇身分提供者。此選項僅適用於整個登陸區域。

如需詳細資訊，請參閱IAM Identity Center 指引。

選擇性地設定 AWS CloudTrail 線索

最佳實務是建議您設定記錄。如果您想要允許 AWS Control Tower 設定組織層級 CloudTrail 追蹤並為您管理，請選擇加入。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，請選擇選擇退出。在主控台中要求時確認您的選擇。您可以在更新登陸區域時變更選擇，以及選擇加入或退出組織層級追蹤。

您可以隨時設定和管理自己的 CloudTrail 追蹤，包括組織層級和帳戶層級追蹤。如果您設定重複的 CloudTrail 追蹤，則在記錄 CloudTrail 事件時，可能會產生重複的成本。

選擇性設定 AWS KMS keys

如果您想要使用加密金鑰 AWS KMS 來加密和解密資源，請選取核取方塊。如果您有現有的金鑰，您可以從下拉式選單中顯示的識別符中選取它們。您可以選擇建立金鑰來產生新的金鑰。您可以在更新登陸區域時新增或變更 KMS 金鑰。

當您選取設定登陸區域時，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
- 已將正確的許可新增至政策
- 金鑰位於管理帳戶中

如果金鑰不符合這些要求，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。請務必編輯金鑰的許可政策，如下節所述。

更新 KMS 金鑰政策

您必須先建立 KMS 金鑰，才能更新 KMS 金鑰政策。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。

若要搭配 AWS Control Tower 使用 KMS 金鑰，您必須新增 AWS Config 和 所需的最低許可，以更新預設 KMS 金鑰政策 AWS CloudTrail。根據最佳實務，建議您在任何政策中包含最低必要許可。更新 KMS 金鑰政策時，您可以在單一 JSON 陳述式或逐行新增群組的許可。

此程序說明如何透過新增允許 AWS Config 和 CloudTrail AWS KMS 用於加密的政策陳述式，在 AWS KMS 主控台中更新預設 KMS 金鑰政策。政策陳述式要求您包含下列資訊：

- **YOUR-MANAGEMENT-ACCOUNT-ID** – 要在其中設定 AWS Control Tower 的管理帳戶 ID。
- **YOUR-HOME-REGION** – 您在設定 AWS Control Tower 時要選取的主要區域。
- **YOUR-KMS-KEY-ID** – 將與政策搭配使用的 KMS 金鑰 ID。

更新 KMS 金鑰政策

1. 在 開啟 AWS KMS 主控台 https://console.aws.amazon.com//kms
2. 從導覽窗格中，選擇客戶受管金鑰。
3. 在表格中，選取您要編輯的金鑰。
4. 在金鑰政策索引標籤中，確定您可以檢視金鑰政策。如果您無法檢視金鑰政策，請選擇切換到政策檢視。
5. 選擇編輯，並透過為 和 CloudTrail 新增下列政策陳述式來更新預設 KMS AWS Config 金鑰政策。

   AWS Config 政策陳述式

```
{
    "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 政策陳述式

```
{
    "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。

範例 KMS 金鑰政策

以下範例政策顯示在您新增授予 AWS Config 和 CloudTrail 最低必要許可的政策陳述式之後，您的 KMS 金鑰政策可能是什麼樣子。範例政策不包含您的預設 KMS 金鑰政策。

```
{
    "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:PARTITION: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:PARTITION:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-
ID:key/YOUR-KMS-KEY-ID",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn": "arn:PARTITION:cloudtrail:YOUR-HOME-REGION:YOUR-
MANAGEMENT-ACCOUNT-ID:trail/aws-controltower-BaselineCloudTrail"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:PARTITION:cloudtrail:*:YOUR-MANAGEMENT-ACCOUNT-ID:trail/*"
                }
            }
        }
    ]
}
```

若要檢視其他範例政策，請參閱下列頁面：

- AWS CloudTrail 《 使用者指南》中的授予加密許可。
- 《 AWS Config 開發人員指南》中的使用服務連結RolesS3儲存貯體交付時 KMS 金鑰的必要許可）。

> **防範攻擊者**
>
> 透過將特定條件新增至政策，您可以協助防止特定類型的攻擊，稱為混淆代理人攻擊，如果實體強制更特權的實體執行動作，例如跨服務模擬。如需政策條件的一般資訊，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 會執行現有金鑰的預先檢查。如果您選擇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 的詳細資訊 AWS KMS，請參閱 AWS KMS 開發人員指南。

請注意，根據預設，AWS Control Tower 中的客戶資料會使用 SSE-S3 進行靜態加密。

選擇性地設定帳戶的自動註冊

當您在設定期間或之後啟用此功能時，在兩個已註冊OUs 之間移動或第一次移入 AWS Control Tower 環境的帳戶不會再顯示繼承偏離的狀態。帳戶會自動繼承在新 OU 上啟用的基準和控制項。會移除先前 OU 的控制項和基準。

若要在設定後隨時選擇加入自動註冊，請導覽至登陸區域設定頁面，然後選擇更新登陸區域，或呼叫 AWS Control Tower `UpdateLandingZone` API。

您可以透過 AWS Organizations API 或 AWS Control Tower 主控台在 OUs 之間移動帳戶。如果您將帳戶移出已註冊的 OU，AWS Control Tower 會自動移除所有部署的基準和控制項。它基本上會從 AWS Control Tower 取消註冊帳戶。

> **Note**
>
> 如果您選擇在初始設定登陸區域後啟用自動註冊功能，AWS Control Tower 不會追溯性地解決在啟用自動註冊功能之前在 OUs 之間移動帳戶所造成的繼承偏離。對於啟用此設定後移動的帳戶，自動偏離解析度會生效。

選擇性地設定和建立自訂成員帳戶

當您遵循建立帳戶工作流程來新增成員帳戶時，您可以選擇指定先前定義的藍圖，以用於從 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 使用帳戶工廠自訂 (AFC) 自訂帳戶。

步驟 3。檢閱並設定登陸區域

設定中的下一節會顯示 AWS Control Tower 為您的登陸區域所需的許可。選擇核取方塊以展開每個主題。系統會要求您同意這些許可，這可能會影響多個帳戶，並且同意整體服務條款。

若要完成

1. 在 主控台檢閱服務許可，當您準備好時，選擇我了解 AWS Control Tower 將用來管理 AWS 資源並代表我強制執行規則的許可。
2. 若要完成您的選擇並初始化啟動，請選擇設定登陸區域。

這一系列步驟會開始設定登陸區域的程序，可能需要大約 30 分鐘才能完成。在設定期間，AWS Control Tower 會建立您的根層級、安全 OU 和共用帳戶。系統會建立、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會收到來自 AWS Control Tower 支援之每個 AWS 區域的AWS 通知 – 訂閱確認電子郵件。若要在您的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 區域選擇每封電子郵件中的確認訂閱連結。

使用 APIs 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，並包含兩個主要步驟。

在此程序中，您將使用 AWS Control Tower 和其他 APIs 來設定和啟動登陸區域。 AWS 這些 APIs 可讓您透過 CloudFormation 主控台或透過 ，以程式設計方式建立 AWS Control Tower 環境 AWS CLI。

啟動 AWS Control Tower 登陸區域之前，請執行下列必要任務：

- 判斷最適合的主區域。如需詳細資訊，請參閱登陸區域設定的管理秘訣。
- 檢閱先決條件：管理帳戶的自動化啟動前檢查以了解自動化啟動前檢查，以確保您的管理帳戶已準備好進行建立登陸區域的變更。

主題

- 檢視登陸區域資訊清單檔案的詳細資訊
- 檢視登陸區域操作的狀態
- 範例：僅使用 APIs 設定 AWS Control Tower 登陸區域
- 登陸區域結構描述
- 使用 啟動登陸區域 CloudFormation

使用 APIs 登陸區域組態的期望

設定 AWS Control Tower 登陸區域的程序有多個步驟。AWS Control Tower 登陸區域的某些層面是可設定的。其他選項無法在設定後變更。

設定期間要設定的關鍵項目

- 您可以在設定期間選取基礎 OU 名稱，也可以在設定登陸區域之後變更 OU 名稱。根據預設，基礎 OUs會命名為安全和沙盒。如需詳細資訊，請參閱設定架構良好的環境的指導方針。
- 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，預設稱為日誌封存和稽核，但您無法在設定後變更這些名稱。（這是一次性選擇。）
- 使用 APIs設定期間，您必須指定 AWS Control Tower 的現有 AWS 帳戶，以用作稽核和日誌封存帳戶。若要指定現有的 AWS 帳戶，如果這些帳戶有現有的 AWS Config 資源，您必須先刪除或修改現有的 AWS Config 資源，才能將帳戶註冊到 AWS Control Tower。（這是一次性選擇。）
- 如果您是第一次設定 ，或是升級到登陸區域 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 AWS CloudTrail 追蹤，也可以選擇退出由 AWS Control Tower 管理的追蹤，以及管理您自己的 CloudTrail 追蹤。您可以隨時更新登陸區域，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登陸區域時，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。

無法復原的組態選項

- 設定登陸區域之後，就無法變更主區域。
- 如果您使用 VPCs 佈建帳戶，則無法在建立 VPC CIDRs 之後對其進行變更。

下一節會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 APIs 設定 AWS Control Tower 登陸區域。

步驟 1：設定您的登陸區域

設定 AWS Control Tower 登陸區域的程序有多個步驟。AWS Control Tower 登陸區域的某些層面是可設定的，但在設定後無法變更其他選擇。若要在啟動登陸區域之前進一步了解這些重要考量，請檢閱登陸區域組態的預期。

在使用 AWS Control Tower 登陸區域 APIs之前，您必須先從其他 AWS 服務呼叫 APIs，以在啟動之前設定您的登陸區域。此程序包含三個主要步驟：

1. 建立新的 AWS Organizations 組織、
2. 設定您的服務整合帳戶、
3. 和 建立具有呼叫登陸區域 APIs 所需許可的 IAM 角色或 IAM Identity Center 使用者。

步驟 1. 建立將包含您的登陸區域的組織：

呼叫 AWS Organizations `CreateOrganization` API 並啟用所有功能來建立基礎 OU。AWS Control Tower 也建議建立指定的安全 OU。此安全 OU 應包含您的所有服務整合帳戶。這些是日誌封存帳戶和先前登陸區域版本的稽核帳戶。

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

AWS Control Tower 可以設定一或多個其他 OUs。除了安全 OU 之外，建議您在登陸區域中佈建至少一個其他 OU。如果此額外 OU 適用於開發專案，建議您將其命名為沙盒 OU，如 AWS Control Tower 登陸區域的 AWS 多帳戶策略中所述。

步驟 2. 視需要佈建服務整合帳戶：

若要設定您的登陸區域，AWS Control Tower 可讓客戶設定 AWS 服務整合。每個這些服務整合可能需要一或多個服務整合中央帳戶。如果您是第一次使用登陸區域 APIs 來設定 AWS Control Tower，則必須為每個啟用的 AWS 服務整合提供中央整合帳戶。您可以使用現有的 AWS 帳戶，或透過 AWS Control Tower 主控台或 AWS Organizations APIs 佈建這些帳戶。確保這些服務整合帳戶位於組織中根層級的指定安全 OU 中。

1. 呼叫 AWS Organizations `CreateAccount` API，以在安全 OU 中建立日誌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"
```

（選用）使用 AWS Organizations `DescribeAccount` API 檢查`CreateAccount`操作的狀態。

2. 將佈建的服務整合帳戶移至指定的安全 OU

```
                            aws organizations move-account --account-id 0123456789012
 --source-parent-id r-examplerootid111 --destination-parent-id ou-examplerootid111-
security
```

步驟 3。建立所需的服務角色

在 IAM 路徑中建立下列 IAM `/service-role/` 服務角色，讓 AWS Control Tower 能夠執行設定登陸區域所需的 API 呼叫：

- AWSControlTowerAdmin
- AWSControlTowerCloudTrailRole
- AWSControlTowerStackSetRole
- AWSControlTowerConfigAggregatorRoleForOrganizations

如需這些角色及其政策的詳細資訊，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：

建立具有呼叫所有登陸區域 APIs IAM 角色。或者，您可以建立 IAM Identity Center 使用者並指派必要的許可。

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

```
                "backup:UpdateGlobalSettings",
                "controltower:CreateLandingZone",
                "controltower:UpdateLandingZone",
                "controltower:ResetLandingZone",
                "controltower:DeleteLandingZone",
                "controltower:GetLandingZoneOperation",
                "controltower:GetLandingZone",
                "controltower:ListLandingZones",
                "controltower:ListLandingZoneOperations",
                "controltower:ListTagsForResource",
                "controltower:TagResource",
                "controltower:UntagResource",
                "servicecatalog:*",
                "organizations:*",
                "organizations:RegisterDelegatedAdministrator",
                "organizations:EnableAWSServiceAccess",
                "organizations:DeregisterDelegatedAdministrator",
                "organizations:ListDelegatedAdministrators",
                "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": "*"
        }
    ]
}
```

> **Note**
>
> 在啟用 Config AWS 整合的情況下升級至登陸區域 4.0 版時，客戶需要擁有 `organizations:ListDelegatedAdministrators` 許可。

步驟 2：使用 AWS Control Tower APIs啟動登陸區域

您可以使用 AWS Control Tower APIs來啟動您的登陸區域。本節說明如何建立所需的登陸區域資訊清單檔案，並將其與 `CreateLandingZone` API 操作搭配使用。

建立資訊清單檔案

資訊清單檔案是 JSON 文件，可指定您的登陸區域組態。使用登陸區域 4.0 版，許多元件現在是選用的，允許更靈活的部署。

資訊清單結構

以下是具有所有可用組態的資訊清單檔案的完整結構：

```
{
    "accessManagement": {
        "enabled": true    // Required - Controls IAM Identity Center integration
    },
    "backup": {
        "enabled": true,   // Required - Controls AWS Backup integration
        "configurations": {
            "backupAdmin": {
                "accountId": "111122223333"    // Backup administrator account
            },
            "centralBackup": {
                "accountId": "111122224444"    // Central backup account
            },
            "kmsKeyArn": "arn:aws:kms:region:account-id:key/key-id"
        }
    },
    "centralizedLogging": {
        "accountId": "111122225555",    // Log archive account
        "enabled": true,                // Required - Controls centralized logging
        "configurations": {
            "accessLoggingBucket": {
```

```
                "retentionDays": 365    // Minimum value: 1
            },
            "loggingBucket": {
                "retentionDays": 365    // Minimum value: 1
            },
            "kmsKeyArn": "arn:aws:kms:region:account-id:key/key-id"
        }
    },
    "config": {
        "accountId": "111122226666",    // Config aggregator account
        "enabled": true,                // Required - Controls AWS Config integration
        "configurations": {
            "accessLoggingBucket": {
                "retentionDays": 365    // Minimum value: 1
            },
            "loggingBucket": {
                "retentionDays": 365    // Minimum value: 1
            },
            "kmsKeyArn": "arn:aws:kms:region:account-id:key/key-id"
        }
    },
    "governedRegions": [               // Optional - List of regions to govern
        "us-east-1",
        "us-west-2"
    ],
    "securityRoles": {
        "enabled": true,               // Required - Controls security roles creation
        "accountId": ""111122226666"    // Security/Audit account
    }
}
```

重要說明

- 資訊清單中需要所有`enabled`旗標。
- 如果您停用 AWS Config 整合 (`"config.enabled": false`)，您還必須停用下列整合：
  - 安全角色 (`"securityRoles.enabled": false`)
  - 存取管理 (`"accessManagement.enabled": false`)
  - 備份 (`"backup.enabled": false`)
- 帳戶 IDs必須是有效的 12 位數 AWS 帳戶 IDs。
- KMS 金鑰 ARNs 必須是有效的 AWS KMS 金鑰 ARNs。

- 保留天數必須至少為 1。

使用 CreateLandingZone API

若要使用 API 建立登陸區域：

```
                    aws controltower create-landing-zone --landing-zone-version 4.0 --
manifest file://manifest.json
```

API 會傳回登陸區域操作 ID，您可用來追蹤登陸區域建立的進度。回應範例：

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

您可以使用傳回狀態為 SUCCEEDED、 FAILED或 的 GetLandingZoneOperation API 來監控操作狀態IN_PROGRESS：

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

登陸區域 4.0 版中的變更內容

資訊清單結構和要求的重要變更：

- 組織結構
  - organizationStructure 定義已從資訊清單中移除
  - 客戶現在可以定義自己的組織結構
  - 僅限需求：服務整合帳戶必須直接在根目錄下的相同 OU 中
- 啟用的旗標
  - 所有服務整合組態都有 enabled旗標，現在是必要欄位。

- 客戶需要一律提供布林值。未提供預設值。
- 客戶需要明確啟用/停用資訊清單中的每個服務整合組態：
  - accessManagement
  - backup
  - centralizedLogging
  - config
  - securityRoles
- 安全角色
  - 安全角色整合現在是選用的
  - 引入用於管理securityRoles部署的新enabled旗標
  - 停用時，將不會實作相關的安全功能
- AWS 組態整合
  - 新增 AWS Config 服務整合區段至資訊清單，config如下列欄位所示：
    - enabled：管理 AWS Config 整合部署所需的布林值旗標
    - accountId：AWS Config 彙總工具的 AWS 帳戶 ID
    - 組態：
      - accessLoggingBucket.retentionDays：存取日誌的保留期間
      - loggingBucket.retentionDays：AWS Config 日誌的保留期間
      - kmsKeyArn：用於加密的 KMS 金鑰

識別您的登陸區域

呼叫ListLandingZones可協助您判斷您的帳戶是否已使用 AWS Control Tower 設定。此 API 會在任何商業區域傳回一個登陸區域識別符 (ARN)，無論登陸區域的主要區域為何。登陸區域 ARNs是唯一的。

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

對於選擇加入區域，如果您在與 ListLandingZones API 主要區域相同的區域中呼叫 API，則 API 只會傳回登陸區域識別符。 例如，如果您的登陸區域是在 af-south-1 中設定，而您在 af-south-1 ListLandingZones中呼叫 ，則 API 會傳回登陸區域識別符。 如果您的登陸區域是在 af-south-1 中設定，且您在 ap-east-1 ListLandingZones中呼叫 ，則 API 不會傳回登陸區域識別符。

輸出：

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

更新您的登陸區域

當新的登陸區域版本可用時，或若要對登陸區域組態進行其他更新，您可以呼叫 UpdateLandingZone API 並參考更新的登陸區域資訊清單檔案。此 API 會傳回 OperationIdentifier，然後您可以在呼叫 GetLandingZoneOperation API 時用來檢查更新操作的狀態。

更新登陸區域

1. 呼叫 AWS Control Tower UpdateLandingZone API，並參考更新的登陸區域版本或更新的登陸區域資訊清單檔案。

   ```
   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
   ```

包含區域和集中式記錄的範例 LandingZoneManifest.json 檔案：

```
{
   "governedRegions": ["us-west-2","us-west-1"],
   "organizationStructure": {
       "security": {
           "name": "Security"
       },
       "sandbox": {
           "name": "Sandbox"
       }
   },
   "centralizedLogging": {
        "accountId": "LOG ARCHIVE ACCOUNT ID",
        "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": "SECURITY ACCOUNT ID"
   },
   "accessManagement": {
        "enabled": true
   }
}
```

輸出：

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

> **選擇性地重新註冊 OU 以更新帳戶**
>
> 對於帳戶少於 1000 OUs，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。

重設登陸區域以解決偏離

當您建立登陸區域時，登陸區域和所有組織單位 (OUs)、帳戶和資源都符合您選擇的控制項強制執行的控管規則。當您和您的組織成員使用登陸區域時，可能會發生此合規狀態的變更。這些變更稱為偏離。

若要識別您的登陸區域是否偏離，您可以呼叫 `GetLandingZone` API。此 API 會傳回登陸區域的偏離狀態 `DRIFTED`或 `IN_SYNC`。

若要解決登陸區域內的偏離，您可以使用 `ResetLandingZone` API 將登陸區域重設回原始組態。例如，AWS Control Tower 預設會啟用 IAM Identity Center 來協助您管理 AWS 帳戶--，但如果您在停

用 IAM Identity Center 的情況下設定原始登陸區域參數，呼叫會ResetLandingZone維護停用的 IAM Identity Center 組態。

只有在您使用最新的可用登陸區域版本時，才能使用 ResetLandingZone API。您可以呼叫 GetLandingZone API，並將登陸區域版本與最新的可用版本進行比較。如有必要，您可以更新您的登陸區域讓登陸區域使用最新的可用版本。在這些範例中，我們使用 3.3 版做為最新版本。

1. 呼叫 GetLandingZone API。如果 API 傳回 的偏離狀態DRIFTED，您的登陸區域會處於偏離狀態。
2. 呼叫 ResetLandingZone API 將登陸區域重設為其原始組態。

```
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**
>
> 重設登陸區域不會更新登陸區域版本。更新您的登陸區域 檢閱有關更新登陸區域版本的詳細資訊。

檢視登陸區域資訊清單檔案的詳細資訊

AWS Control Tower 登陸區域資訊清單檔案是描述 AWS Control Tower 資源的文字檔案。下列各節顯示登陸區域資訊清單檔案中項目的詳細定義。

若要查看完整的登陸區域結構描述範例，請參閱登陸區域結構描述。

governedRegions – 在控管下放置的區域

- 類型：字串清單
- 必要：否

- 範例：

```
"governedRegions": ["us-west-2","us-west-1"]
```

organizationStructure – 選取要在您的組織中建立的安全和沙盒 OUs名稱

- 類型：物件
- 必要：是
- 屬性：
- 範例：
  - security - 具有一個必要屬性的物件，name需要 String
  - sandbox - 具有一個必要屬性的物件，name需要 String

```
"organizationStructure": {
       "security": {
           "name": "CORE"
       },
       "sandbox": {
           "name": "Sandbox"
       }
   }
```

centralizedLogging – 的組態 AWS CloudTrail

- 類型：物件
- 必要：是
- 屬性：
  - accountId - String 代表應部署記錄資源 AWS 的帳戶
  - 組態 - Object具有三個屬性的
    - loggingBucket - 具有一個屬性 的物件retentionDays，需要 Number
    - accessLoggingBucket - 具有一個屬性 的物件retentionDays，需要 Number
    - kmsKeyArn - 選用 String
  - 已啟用 - 選用 Boolean
- 範例：

```
"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 – 選擇在何處部署記錄資源

- 類型：物件
- 必要：是
- 屬性：accountId - String代表記錄資源應部署至其中 AWS 的帳戶
- 範例：

```
"securityRoles": {
        "accountId": "333333333333"
   }
```

accessManagement – 選擇 以啟用存取管理

- 類型：物件
- 必要：否
- 屬性：已啟用 - 布林值
- 範例：

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

備份 – 使用 AWS Control Tower AWS 備份的組態

- 類型：物件
- 必要：否
- 屬性：
  - 組態 - Object具有三個屬性的
    - centralBackup - 具有一個屬性 的物件accountId，需要 String
    - backupAdmin - 具有一個屬性 的物件accountId，需要 String
    - kmsKeyArn - 選用 String
  - 已啟用 - Boolean
- 範例：

```
"backup": {
    "configurations": {
        "centralBackup": {
            "accountId": "CENTRAL BACKUP ACCOUNT ID"
        },
        "backupAdmin": {
            "accountId": "BACKUP MANAGER ACCOUNT ID"
        },
        "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/e84XXXXX-6bXX-49XX-9eXX-
ecfXXXXXXXXX"
    },
    "enabled": true
}
```

檢視登陸區域操作的狀態

ListLandingZoneOperations API 可讓您檢視在登陸區域上執行動作的 AWS Control Tower 操作狀態。

如需此 API 操作的詳細資訊，請參閱 ListLandingZoneOperations。

ListLandingZoneOperations

的範例輸入和輸出ListLandingZoneOperations。

此範例說明如何在沒有參數的情況下呼叫 API。

```
aws controltower --region us-east-1 list-landing-zone-operations

{
    "landingZoneOperations": [
        {
            "operationIdentifier": "873fe98d-1ecc-4154-b593-86e4a95ebfXX",
            "operationType": "CREATE",
            "status": "FAILED"
        },
        {
            "operationIdentifier": "0016d43d-a307-4ad8-a2a2-b427b8eb1cXX",
            "operationType": "DELETE",
            "status": "SUCCEEDED"
        },
        {
            "operationIdentifier": "002b8b5a-6bb7-4c40-89cd-5822a73d13XX",
            "operationType": "CREATE",
            "status": "SUCCEEDED"
        },
        {
            "operationIdentifier": "008886a0-f7a2-4df3-90e8-6e9f936507XX",
            "operationType": "CREATE",
            "status": "FAILED"
        }
    ]
}
```

此範例示範如何呼叫 API 並指定結果數量上限。

```
aws controltower --region us-east-1 list-landing-zone-operations --max-results 1

{
    "landingZoneOperations": [
        {
            "operationIdentifier": "873fe98d-1ecc-4154-b593-86e4a95ebfXX",
            "operationType": "CREATE",
            "status": "FAILED"
        }
    ],
    "nextToken": "AAMAATFMzwP0QysYY8npWgstfcHGQBj-
XCC18ISyd9mkQmzLR7ZFMket4F0aWv8tUTtnsTWOnfblUp_Q9U-
nX9_6lEsLHs0RlhceDKskHr0_3fm8KdPTa6ofxMt5SPw8WF7-Jsvw2rJVvhj4DHDipo-y1HVK_eZ__Z3-
OzInm403cIHxhbjGPgqCX6FeKr8lwgTDKOejkLYZ9w7J5aqPAKLfVP8KKNda5g0VfMj1wdl4J2nwnHI-
```

```
UuCTIZ5nUEgXgUHaFq6Ma1pLDfGefZQJn5HmDhhgd5yvqzSRH1BtrHpdV_N1EVP8u3JJr3eWQHe9jNB02lihD4Mdcbm3SJg
VXRwTUIBInrit4HslNtPE8-IC1gxCjGoYPGtuWBPumK-pUPE="
}
```

此範例示範如何使用 呼叫 API 並取得分頁結果nextToken。

```
aws controltower --region us-east-1 list-landing-zone-operations --next-token
 AAMAATFMzwP0QysYY8npWgstfcHGQBj-XCC18ISyd9mkQmzLR7ZFMket4F0aWv8tUTtnsTWOnfblUp_Q9U-
nX9_6lEsLHs0RlhceDKskHr0_3fm8KdPTa6ofxMt5SPw8WF7-Jsvw2rJVvhj4DHDipo-y1HVK_eZ__Z3-
OzInm403cIHxhbjGPgqCX6FeKr8lwgTDKOejkLYZ9w7J5aqPAKLfVP8KKNda5g0VfMj1wdl4J2nwnHI-
UuCTIZ5nUEgXgUHaFq6Ma1pLDfGefZQJn5HmDhhgd5yvqzSRH1BtrHpdV_N1EVP8u3JJr3eWQHe9jNB02lihD4Mdcbm3SJg
VXRwTUIBInrit4HslNtPE8-IC1gxCjGoYPGtuWBPumK-pUPE=

{
    "landingZoneOperations": [
        {
            "operationIdentifier": "0016d43d-a307-4ad8-a2a2-b427b8eb1cXX",
            "operationType": "DELETE",
            "status": "SUCCEEDED"
        },
        {
            "operationIdentifier": "002b8b5a-6bb7-4c40-89cd-5822a73d13XX",
            "operationType": "CREATE",
            "status": "SUCCEEDED"
        },
        {
            "operationIdentifier": "008886a0-f7a2-4df3-90e8-6e9f936507XX",
            "operationType": "CREATE",
            "status": "FAILED"
        }
    ]
}
```

此範例說明如何使用篩選條件呼叫 API。

```
aws controltower --region us-east-1 list-landing-zone-operations --filter '{"types":
["CREATE"],"statuses":["FAILED"]}'

{
    "landingZoneOperations": [
        {
            "operationIdentifier": "873fe98d-1ecc-4154-b593-86e4a95ebfXX",
            "operationType": "CREATE",
```

```
            "status": "FAILED"
        },
        {
            "operationIdentifier": "008886a0-f7a2-4df3-90e8-6e9f936507XX",
            "operationType": "CREATE",
            "status": "FAILED"
        }
    ]
}
```

範例：僅使用 APIs 設定 AWS Control Tower 登陸區域

此範例演練是配套文件。如需說明、注意事項和詳細資訊，請參閱使用 APIs 的 AWS Control Tower 入門。

先決條件

在建立 AWS Control Tower 登陸區域之前，您必須建立組織、兩個共用帳戶和一些 IAM 角色。本演練教學包含這些步驟，其中包含範例 CLI 命令和輸出。

步驟 1. 建立組織和兩個必要的帳戶。

```
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. 建立所需的 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 >cloudtrail_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. 取得帳戶 IDs並產生登陸區域資訊清單檔案。

下列範例中的前兩個命令會將您在步驟 1 中建立之帳戶的帳戶 IDs 存放到變數中。這些變數接著有助於產生登陸區域資訊清單檔案。

```
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. 使用最新版本建立登陸區域。

您必須使用資訊清單檔案和最新版本來設定登陸區域。此範例顯示 3.3 版。

```
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 operationIdentifier，如以下範例所示。

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

步驟 5.（選用）透過設定迴圈來追蹤登陸區域建立操作的狀態。

若要追蹤狀態，請使用上一個`create-landing-zone`命令輸出中的 operationIdentifier。

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

狀態輸出範例：

```
{
    "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，該迴圈會依序報告操作的狀態，例如日誌檔案。然後，您不需要繼續輸入命令。

```
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
```

顯示登陸區域的詳細資訊

步驟 1. 尋找登陸區域的 ARN

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

輸出將包含登陸區域的識別符，如下列輸出範例所示。

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

步驟 2. 取得資訊

```
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範例：

```
{
    "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"
    }
}
```

步驟 6：（選用）呼叫 **ListLandingZoneOperations** API 以檢視變更登陸區域的任何操作的狀態。

若要追蹤任何登陸區域操作的狀態，您可以呼叫 ListLandingZoneOperations API。

登陸區域結構描述

登陸區域是一種透過結構描述建立 AWS 的資源。每個 AWS Control Tower 登陸區域版本都有唯一的結構描述。

AWS Control Tower 登陸區域的結構描述，3.1 版及更新版本，會發佈在此參考區段中，以協助您選擇相容的版本。

> **Note**
>
> 登陸區域 3.0 版中存在有關不必要的存取記錄的已知問題。問題會在登陸區域 3.1 版中解決。如需變更的詳細資訊，請參閱 AWS Control Tower 登陸區域 3.1 版。

登陸區域 4.0 結構描述

```
{
    "type": "object",
```

```
    "required": [],
    "properties": {
        "accessManagement": {
            "$ref": "#/definitions/AccessManagement"
        },
        "backup": {
            "$ref": "#/definitions/Backup"
        },
        "centralizedLogging": {
            "$ref": "#/definitions/CentralizedLogging"
        },
        "governedRegions": {
            "type": "array",
            "items": {
                "type": "string",
                "maxLength": 24,
                "minLength": 1,
                "pattern": "^[a-z]{2}-[a-z\\-]*-[0-9]{1}$",
                "additionalProperties": false
            },
            "additionalProperties": false
        },
        "securityRoles": {
            "$ref": "#/definitions/SecurityRoles"
        },
        "config": {
            "$ref": "#/definitions/Config"
        }
    },
    "additionalProperties": false,
    "definitions": {
        "AccessManagement": {
            "type": "object",
            "required": [
                "enabled"
            ],
            "properties": {
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
```

```
        "Backup": {
            "type": "object",
            "required": [
                "enabled"
            ],
            "properties": {
                "configurations": {
                    "$ref": "#/definitions/BackupConfigurations"
                },
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false,
            "if": {
                "properties": {
                    "enabled": {
                        "const": true
                    }
                }
            },
            "then": {
                "required": [
                    "configurations"
                ]
            }
        },
        "BackupAdminConfigurations": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
```

```
        "BackupConfigurations": {
            "type": "object",
            "required": [
                "backupAdmin",
                "centralBackup",
                "kmsKeyArn"
            ],
            "properties": {
                "backupAdmin": {
                    "$ref": "#/definitions/BackupAdminConfigurations"
                },
                "centralBackup": {
                    "$ref": "#/definitions/CentralBackupConfigurations"
                },
                "kmsKeyArn": {
                    "type": "string",
                    "maxLength": 2048,
                    "minLength": 1,
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "CentralBackupConfigurations": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "CentralizedLogging": {
            "type": "object",
            "required": [
                "enabled"
            ],
```

```
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                },
                "configurations": {
                    "$ref": "#/definitions/LoggingConfigurations"
                },
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false,
            "if": {
                "properties": {
                    "enabled": {
                        "const": true
                    }
                }
            },
            "then": {
                "required": [
                    "accountId"
                ]
            }
        },
        "LoggingConfigurations": {
            "type": "object",
            "properties": {
                "accessLoggingBucket": {
                    "$ref": "#/definitions/S3BucketConfiguration"
                },
                "kmsKeyArn": {
                    "type": "string",
                    "maxLength": 2048,
                    "minLength": 1,
                    "additionalProperties": false
                },
                "loggingBucket": {
                    "$ref": "#/definitions/S3BucketConfiguration"
```

```
                }
            },
            "additionalProperties": false
        },
        "S3BucketConfiguration": {
            "type": "object",
            "properties": {
                "retentionDays": {
                    "type": "number",
                    "minimum": 1,
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "SecurityRoles": {
            "type": "object",
            "required": [
                "enabled"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                },
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false,
            "if": {
                "properties": {
                    "enabled": {
                        "const": true
                    }
                }
            },
            "then": {
                "required": [
                    "accountId"
```

```
                ]
            }
        },
        "Config": {
            "type": "object",
            "required": [
                "enabled"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                },
                "configurations": {
                    "$ref": "#/definitions/ConfigConfiguration"
                },
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false,
            "if": {
                "properties": {
                    "enabled": {
                        "const": true
                    }
                }
            },
            "then": {
                "required": [
                    "accountId"
                ]
            }
        },
        "ConfigConfiguration": {
            "type": "object",
            "required": [],
            "properties": {
                "loggingBucket": {
                    "$ref": "#/definitions/S3BucketConfiguration"
```

```
                },
                "accessLoggingBucket": {
                    "$ref": "#/definitions/S3BucketConfiguration"
                },
                "kmsKeyArn": {
                    "type": "string",
                    "maxLength": 2048,
                    "minLength": 1,
                    "additionalProperties": false
                }
            }
        }
    }
}
```

登陸區域 3.3 結構描述

```
{
    "type": "object",
    "required": [
        "centralizedLogging",
        "organizationStructure",
        "securityRoles"
    ],
    "properties": {
        "accessManagement": {
            "$ref": "#/definitions/AccessManagement"
        },
        "backup": {
            "$ref": "#/definitions/Backup"
        },
        "centralizedLogging": {
            "$ref": "#/definitions/CentralizedLogging"
        },
        "governedRegions": {
            "type": "array",
            "items": {
                "type": "string",
                "maxLength": 24,
                "minLength": 1,
                "pattern": "^[a-z]{2}-[a-z\\-]*-[0-9]{1}$",
                "additionalProperties": false
            },
```

```
            "additionalProperties": false
        },
        "organizationStructure": {
            "$ref": "#/definitions/OrganizationStructure"
        },
        "securityRoles": {
            "$ref": "#/definitions/SecurityRoles"
        }
    },
    "additionalProperties": false,
    "definitions": {
        "AccessManagement": {
            "type": "object",
            "required": [
                "enabled"
            ],
            "properties": {
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false,
                    "default": true
                }
            },
            "additionalProperties": false
        },
        "Backup": {
            "type": "object",
            "properties": {
                "configurations": {
                    "$ref": "#/definitions/BackupConfigurations"
                },
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false,
                    "default": false
                }
            },
            "additionalProperties": false,
            "if": {
                "properties": {
                    "enabled": {
                        "const": true
                    }
                }
```

```
            },
            "then": {
                "required": [
                    "configurations"
                ]
            }
        },
        "BackupAdminConfigurations": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "BackupConfigurations": {
            "type": "object",
            "required": [
                "backupAdmin",
                "centralBackup",
                "kmsKeyArn"
            ],
            "properties": {
                "backupAdmin": {
                    "$ref": "#/definitions/BackupAdminConfigurations"
                },
                "centralBackup": {
                    "$ref": "#/definitions/CentralBackupConfigurations"
                },
                "kmsKeyArn": {
                    "type": "string",
                    "maxLength": 2048,
                    "minLength": 1,
                    "additionalProperties": false
                }
            },
```

```
            "additionalProperties": false
        },
        "CentralBackupConfigurations": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "CentralizedLogging": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                },
                "configurations": {
                    "$ref": "#/definitions/LoggingConfigurations"
                },
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false,
                    "default": true
                }
            },
            "additionalProperties": false
        },
        "LoggingConfigurations": {
            "type": "object",
```

```
            "properties": {
                "accessLoggingBucket": {
                    "$ref": "#/definitions/S3BucketConfiguration"
                },
                "kmsKeyArn": {
                    "type": "string",
                    "maxLength": 2048,
                    "minLength": 1,
                    "additionalProperties": false
                },
                "loggingBucket": {
                    "$ref": "#/definitions/S3BucketConfiguration"
                }
            },
            "additionalProperties": false
        },
        "OrganizationalUnit": {
            "type": "object",
            "required": [
                "name"
            ],
            "properties": {
                "name": {
                    "type": "string",
                    "maxLength": 120,
                    "minLength": 1,
                    "pattern": "^[\\s\\S]*$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "OrganizationStructure": {
            "type": "object",
            "required": [
                "security"
            ],
            "properties": {
                "sandbox": {
                    "$ref": "#/definitions/OrganizationalUnit"
                },
                "security": {
                    "$ref": "#/definitions/OrganizationalUnit"
                }
```

```
            },
            "additionalProperties": false
        },
        "S3BucketConfiguration": {
            "type": "object",
            "properties": {
                "retentionDays": {
                    "type": "number",
                    "minimum": 1,
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "SecurityRoles": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        }
    }
}
```

登陸區域 3.2 結構描述

```
{
    "type": "object",
    "required": [
        "centralizedLogging",
        "organizationStructure",
        "securityRoles"
    ],
    "properties": {
```

```
        "accessManagement": {
            "$ref": "#/definitions/AccessManagement"
        },
        "backup": {
            "$ref": "#/definitions/Backup"
        },
        "centralizedLogging": {
            "$ref": "#/definitions/CentralizedLogging"
        },
        "governedRegions": {
            "type": "array",
            "items": {
                "type": "string",
                "maxLength": 24,
                "minLength": 1,
                "pattern": "^[a-z]{2}-[a-z\\-]*-[0-9]{1}$",
                "additionalProperties": false
            },
            "additionalProperties": false
        },
        "organizationStructure": {
            "$ref": "#/definitions/OrganizationStructure"
        },
        "securityRoles": {
            "$ref": "#/definitions/SecurityRoles"
        }
    },
    "additionalProperties": false,
    "definitions": {
        "AccessManagement": {
            "type": "object",
            "required": [
                "enabled"
            ],
            "properties": {
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false,
                    "default": true
                }
            },
            "additionalProperties": false
        },
        "Backup": {
```

```
            "type": "object",
            "properties": {
                "configurations": {
                    "$ref": "#/definitions/BackupConfigurations"
                },
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false,
                    "default": false
                }
            },
            "additionalProperties": false,
            "if": {
                "properties": {
                    "enabled": {
                        "const": true
                    }
                }
            },
            "then": {
                "required": [
                    "configurations"
                ]
            }
        },
        "BackupAdminConfigurations": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "BackupConfigurations": {
            "type": "object",
            "required": [
```

```
                "backupAdmin",
                "centralBackup",
                "kmsKeyArn"
            ],
            "properties": {
                "backupAdmin": {
                    "$ref": "#/definitions/BackupAdminConfigurations"
                },
                "centralBackup": {
                    "$ref": "#/definitions/CentralBackupConfigurations"
                },
                "kmsKeyArn": {
                    "type": "string",
                    "maxLength": 2048,
                    "minLength": 1,
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "CentralBackupConfigurations": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "CentralizedLogging": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
```

```
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                },
                "configurations": {
                    "$ref": "#/definitions/LoggingConfigurations"
                },
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false,
                    "default": true
                }
            },
            "additionalProperties": false
        },
        "LoggingConfigurations": {
            "type": "object",
            "properties": {
                "accessLoggingBucket": {
                    "$ref": "#/definitions/S3BucketConfiguration"
                },
                "kmsKeyArn": {
                    "type": "string",
                    "maxLength": 2048,
                    "minLength": 1,
                    "additionalProperties": false
                },
                "loggingBucket": {
                    "$ref": "#/definitions/S3BucketConfiguration"
                }
            },
            "additionalProperties": false
        },
        "OrganizationalUnit": {
            "type": "object",
            "required": [
                "name"
            ],
            "properties": {
                "name": {
                    "type": "string",
                    "maxLength": 120,
                    "minLength": 1,
```

```
                "pattern": "^[\\s\\S]*$",
                "additionalProperties": false
            }
        },
        "additionalProperties": false
    },
    "OrganizationStructure": {
        "type": "object",
        "required": [
            "security"
        ],
        "properties": {
            "sandbox": {
                "$ref": "#/definitions/OrganizationalUnit"
            },
            "security": {
                "$ref": "#/definitions/OrganizationalUnit"
            }
        },
        "additionalProperties": false
    },
    "S3BucketConfiguration": {
        "type": "object",
        "properties": {
            "retentionDays": {
                "type": "number",
                "minimum": 1,
                "additionalProperties": false
            }
        },
        "additionalProperties": false
    },
    "SecurityRoles": {
        "type": "object",
        "required": [
            "accountId"
        ],
        "properties": {
            "accountId": {
                "type": "string",
                "maxLength": 12,
                "minLength": 12,
                "pattern": "^\\d{12}$",
                "additionalProperties": false
```

```
                }
            },
            "additionalProperties": false
        }
    }
}
```

登陸區域 3.1 結構描述

```
{
    "type": "object",
    "required": [
        "centralizedLogging",
        "organizationStructure",
        "securityRoles"
    ],
    "properties": {
        "accessManagement": {
            "$ref": "#/definitions/AccessManagement"
        },
        "backup": {
            "$ref": "#/definitions/Backup"
        },
        "centralizedLogging": {
            "$ref": "#/definitions/CentralizedLogging"
        },
        "governedRegions": {
            "type": "array",
            "items": {
                "type": "string",
                "maxLength": 24,
                "minLength": 1,
                "pattern": "^[a-z]{2}-[a-z\\-]*-[0-9]{1}$",
                "additionalProperties": false
            },
            "additionalProperties": false
        },
        "organizationStructure": {
            "$ref": "#/definitions/OrganizationStructure"
        },
        "securityRoles": {
            "$ref": "#/definitions/SecurityRoles"
        }
```

```
    },
    "additionalProperties": false,
    "definitions": {
        "AccessManagement": {
            "type": "object",
            "required": [
                "enabled"
            ],
            "properties": {
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false,
                    "default": true
                }
            },
            "additionalProperties": false
        },
        "Backup": {
            "type": "object",
            "properties": {
                "configurations": {
                    "$ref": "#/definitions/BackupConfigurations"
                },
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false,
                    "default": false
                }
            },
            "additionalProperties": false,
            "if": {
                "properties": {
                    "enabled": {
                        "const": true
                    }
                }
            },
            "then": {
                "required": [
                    "configurations"
                ]
            }
        },
        "BackupAdminConfigurations": {
```

```
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "BackupConfigurations": {
            "type": "object",
            "required": [
                "backupAdmin",
                "centralBackup",
                "kmsKeyArn"
            ],
            "properties": {
                "backupAdmin": {
                    "$ref": "#/definitions/BackupAdminConfigurations"
                },
                "centralBackup": {
                    "$ref": "#/definitions/CentralBackupConfigurations"
                },
                "kmsKeyArn": {
                    "type": "string",
                    "maxLength": 2048,
                    "minLength": 1,
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "CentralBackupConfigurations": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
```

```
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "CentralizedLogging": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                },
                "configurations": {
                    "$ref": "#/definitions/LoggingConfigurations"
                },
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false,
                    "default": true
                }
            },
            "additionalProperties": false
        },
        "LoggingConfigurations": {
            "type": "object",
            "properties": {
                "accessLoggingBucket": {
                    "$ref": "#/definitions/S3BucketConfiguration"
                },
                "kmsKeyArn": {
                    "type": "string",
                    "maxLength": 2048,
                    "minLength": 1,
```

```
                    "additionalProperties": false
                },
                "loggingBucket": {
                    "$ref": "#/definitions/S3BucketConfiguration"
                }
            },
            "additionalProperties": false
        },
        "OrganizationalUnit": {
            "type": "object",
            "required": [
                "name"
            ],
            "properties": {
                "name": {
                    "type": "string",
                    "maxLength": 120,
                    "minLength": 1,
                    "pattern": "^[\\s\\S]*$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "OrganizationStructure": {
            "type": "object",
            "required": [
                "security"
            ],
            "properties": {
                "sandbox": {
                    "$ref": "#/definitions/OrganizationalUnit"
                },
                "security": {
                    "$ref": "#/definitions/OrganizationalUnit"
                }
            },
            "additionalProperties": false
        },
        "S3BucketConfiguration": {
            "type": "object",
            "properties": {
                "retentionDays": {
                    "type": "number",
```

```
                    "minimum": 1,
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "SecurityRoles": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        }
    }
}
```

使用 啟動登陸區域 CloudFormation

您可以透過 CloudFormation 主控台 CloudFormation 或透過 設定和啟動登陸區域 AWS CLI。本節提供使用 APIs啟動登陸區域的指示和範例 CloudFormation。

主題

- 使用 啟動登陸區域的先決條件 CloudFormation
- 使用 建立新的登陸區域 CloudFormation
- 使用 管理現有的登陸區域 CloudFormation

使用 啟動登陸區域的先決條件 CloudFormation

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

   如需更詳細的說明，請參閱 步驟 1：設定您的登陸區域。

2. 從 CloudFormation 主控台或使用 部署 CloudFormation 範本 AWS CLI，以在 管理帳戶中建立下列資源：

   - Log Archive 帳戶 （有時稱為「記錄」帳戶）
   - 稽核帳戶 （有時稱為「安全性」帳戶）
   - AWSControlTowerAdmin、AWSControlTowerCloudTrailRole、AWSControlTowerConfigAggregatorRole 和 AWSControlTowerStackSetRole 服務角色。

     如需 AWS Control Tower 如何使用這些角色來執行登陸區域 API 呼叫的資訊，請參閱步驟 1：設定您的登陸區域。

```
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 建立新的登陸區域 CloudFormation

從 CloudFormation 主控台或使用 AWS CLI部署下列 CloudFormation 範本，以建立登陸區域。

```
Parameters:
  Version:
    Type: String
    Description: The version number of Landing Zone
  GovernedRegions:
    Type: Array
    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 管理現有的登陸區域 CloudFormation

您可以使用 在新的或現有的 CloudFormation 堆疊中匯入登陸區域，藉此 CloudFormation 管理已啟動的登陸區域。如需詳細資訊和指示，請參閱將現有資源帶入 CloudFormation 管理。

若要偵測和解決登陸區域內的偏離，您可以使用 AWS Control Tower 主控台 AWS CLI、 或 ResetLandingZone API。

後續步驟

現在您的登陸區域已設定完畢，即可使用。

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 Identity Center 使用者和群組。如需建議，請參閱設定群組、角色和政策的建議。
- 若要開始從您的 AWS Organizations 部署註冊組織和帳戶，請參閱管理現有的組織和帳戶。
- 您的最終使用者可以使用 AWS 帳戶工廠在您的登陸區域中佈建自己的帳戶。如需詳細資訊，請參閱設定和佈建帳戶的許可。
- 為了確保 AWS Control Tower 的合規驗證，您的中央雲端管理員可以檢閱 Log Archive 帳戶中的日誌封存，而指定的第三方稽核人員可以檢閱 Audit （共用） 帳戶中的稽核資訊，這是 Security OU 的成員。
- 若要進一步了解 AWS Control Tower 的功能，請參閱相關資訊。
- 有時候，您可能需要更新登陸區域，以取得最新的後端更新、最新的控制項，並讓您的登陸區域保持在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 疑難排解。

> **Important**
>
> 如果您尚未為帳戶的根使用者啟用 MFA，請現在執行此操作。如需根使用者最佳實務的詳細資訊，請參閱保護您帳戶的根使用者的最佳實務。

AWS Control Tower 中的限制和配額

本章涵蓋使用 AWS Control Tower 時應謹記 AWS 的服務限制和配額。如果您因為服務配額問題而無法設定登陸區域，請聯絡 AWS 支援。

如需控制項特定限制的詳細資訊，請參閱 控制限制。

> **控制項參考指南**
>
> AWS Control Tower 控制項的詳細資訊已移至 AWS Control Tower 控制項參考指南。

AWS Control Tower 中的已知限制

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，允許一次一個操作。允許此限制的兩個例外狀況：
  - 選用控制項可以透過非同步程序同時啟用和停用。一次最多可以進行一百 (100) 個控制相關操作，無論它們是從主控台還是 API 呼叫。
  - 帳戶可以透過非同步程序在 Account Factory 中同時佈建、更新和註冊，同時進行最多五 (5) 個帳戶相關操作。取消管理帳戶必須一次執行一個帳戶。
  - Account Factory for Terraform (AFT) 在部署期間設定了額外的並行參數。AWS 已使用下列預設值測試 AFT：
    - `concurrent_account_factory_actions`：5（帳戶佈建）
    - `maximum_concurrent_customizations`：5（自訂管道）

    提高這些限制超過測試的預設值可能會降低穩定性。
- 安全 OU 中共用帳戶的電子郵件地址可以變更，但您必須更新登陸區域，才能在 AWS Control Tower 主控台中查看這些變更。
- 每個 OU 限制五 (5) SCPs 適用於 AWS Control Tower 登陸區域中OUs。
- AWS Control Tower 支援登陸區域組織中最多 10，000 個帳戶，除以所有 OUs。
- 具有超過 1000 個直接巢狀帳戶的現有 OUs 無法在 AWS Control Tower 中註冊或重新註冊。如需註冊 OUs 限制的詳細資訊，請參閱 以基礎 AWS 服務為基礎的限制。
- AWS Control Tower (CfCT) 的自訂無法用於這些項目 AWS 區域，因為某些相依性無法使用：

- 歐洲（蘇黎世）、eu-central-2
- 歐洲（西班牙）、eu-south-2
- 加拿大西部（卡加利）ca-west-1
- 亞太區域（墨爾本）、ap-southeast-4
- 亞太區域（馬來西亞）、ap-southeast-5
- 亞太區域（泰國），ap-southeast-7
- 墨西哥（中部）、mx-central-1

如果您將 CfCT 部署 CfCT 到 AWS Control Tower 主區域，但您無法在這些區域中建置 CfCT，則可以使用 CfCT 在這些區域中部署和管理資源。

- 下列無法使用 AWS Control Tower Account Factory for Terraform (AFT) AWS 區域，因為某些相依性無法使用：
  - 歐洲（蘇黎世）、eu-central-2
  - 歐洲（西班牙）、eu-south-2
  - 加拿大西部（卡加利），ca-west-1
  - 亞太區域（墨爾本）、ap-southeast-4
  - 亞太區域（馬來西亞）、ap-southeast-5
  - 亞太區域（泰國），ap-southeast-7
  - 墨西哥（中部）、mx-central-1
- 下列區域中的新 AFT 客戶無法部署適用於 Terraform 的 AWS Control Tower 帳戶工廠 (AFT)，因為 AWS CodeConnections 無法連線至第三方版本控制系統 (VCS)：
  - 亞太區域（香港）、非洲（開普敦）、中東（巴林）、歐洲（蘇黎世）、亞太區域（雅加達）、亞太區域（海德拉巴）、亞太區域（大阪）、亞太區域（墨爾本）、以色列（特拉維夫）、歐洲（西班牙）、中東（阿拉伯聯合大公國）、亞太區域（泰國）、墨西哥（中部）
- 下列區域不支援 AWS Service Catalog。
  - 加拿大西部（卡加利），ca-west-1
  - 亞太區域（馬來西亞）、ap-southeast-5
  - 亞太區域（泰國），ap-southeast-7
  - 墨西哥（中部）、mx-central-1

> **Note**
>
> 不支援 Service Catalog 的區域不支援 AWS Control Tower (AFC) 的 Account Factory Customizations。

如需不支援 區域中 AWS Control Tower 功能的詳細資訊 AWS Service Catalog，請參閱 AWS Control Tower 可在 AWS 加拿大西部（卡加利）使用。

- 呼叫控制項 API 來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。十個操作 (10) 可以同時進行，剩餘操作已排入佇列。您可能需要調整程式碼以等待完成。
- 當您透過 Account Factory Customizations (AFC) 佈建帳戶時，如果藍圖是以 Terraform 為基礎，則只能將這些藍圖部署到一個 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 AWS Control Tower 配額的相關資訊。您可以使用 Service Quotas 主控台來檢視預設的服務配額，或請求增加可調整配額的配額。

> **Note**
>
> 新建立的帳戶和組織可能會遇到低於預設值 10 個帳戶的配額。

您可以透過 Service Quotas 主控台檢視下列配額

- 並行帳戶操作配額 ：可同時執行的並行帳戶操作數目上限。預設：5，上限：10，可調整
- 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。如果您新增超過此限制的帳戶，則無法執行 AWS Control Tower 中的 OU 註冊程序。若要進一步了解每個 OU 的帳戶數量，請參閱 AWS Control Tower 文件以基礎 AWS 服務為基礎的限制。預設：1000，不可調整。
- 組織單位 (OUs) 的並行操作：可同時執行的並行 OU 相關操作數目上限。預設：1，不可調整。

例如，您可以請求從最多 10 個並行帳戶相關操作中的 5 個提高配額。配額增加後，某些 AWS Control Tower 效能特性可能會變更。例如，當您擁有更多帳戶時，更新 OU 可能需要更長的時間。或者，在具有五個 SCPs OU 上完成動作可能需要更長的時間，而不是使用三個 SCPs。

> **Note**
>
> 增加服務配額請求可能需要最多兩天的時間才會生效。請務必向 AWS Control Tower 主區域請求增加配額。

或者，您可以聯絡 AWS Support，請求提高 AWS Control Tower 中某些資源的配額。或者，您可以檢視以下影片，並了解如何自動提高特定服務配額。

影片：在與 AWS Control Tower 相關的服務中，自動化提高服務配額的請求

此影片 (7：24) 說明如何根據 AWS Control Tower 中的部署，自動提高相關整合式 AWS 服務的服務配額。它還顯示如何自動將新帳戶註冊到您組織的 AWS Enterprise 支援。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來觸發指定 中服務配額增加的自動請求 AWS 區域。

如需 AWS 配額的詳細資訊，請參閱 AWS 一般參考。

控制限制

AWS Control Tower AWS 透過以各種形式實作的控制，例如服務控制政策 (SCPs)、 AWS Config 規則和 CloudFormation 勾點，協助您在 上維護安全的多帳戶環境。

> **控制項參考指南**
>
> AWS Control Tower 控制項的詳細資訊已移至 AWS Control Tower 控制項參考指南。

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 無法再保證控制項如設計般運作。因此，多帳戶環境的安全性可能會受到影響。安全性 AWS 的共同責任模型適用於您可能進行的任何此類變更。

> **Note**
>
> 當您更新登陸區域時，AWS Control Tower 會將預防性控制的 SCPs 重設為其標準組態，以協助維護您環境的完整性。您對 SCPs 所做的變更將由標準版本的控制項依設計取代。

區域限制

AWS Control Tower 中的某些控制項無法在可使用 AWS Control Tower AWS 區域 的特定 中運作，因為這些區域不支援所需的基礎功能。因此，當您部署該控制項時，它可能不會在您使用 AWS Control Tower 管理的所有區域中運作。此限制會影響 Security Hub CSPM 服務受管標準：AWS Control Tower 中的特定偵測控制、特定主動控制和特定控制。如需區域可用性的詳細資訊，請參閱 Security Hub 控制項。另請參閱區域服務清單文件和 Security Hub CSPM 控制參考文件。

在混合控管的情況下，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項限制的詳細資訊，請參閱 啟用 AWS 選擇加入區域的考量事項。

> **Note**
>
> 如需控制和區域支援的最新資訊，建議您呼叫 `GetControl`和 `ListControls` API 操作。

尋找可用的控制項和區域

您可以在 AWS Control Tower 主控台中檢視每個控制項的可用區域。您可以使用 AWS Control Catalog 中的 `GetControl`和 `ListControls` APIs，以程式設計方式檢視可用的區域。

如需特定 中不支援之服務受管標準：AWS Control Tower AWS Security Hub CSPM 控制的相關資訊 AWS 區域，請參閱 Security Hub CSPM 標準中的「不支援的區域」。

以基礎 AWS 服務為基礎的限制

此頁面說明由於其他服務的限制 AWS ，以及 AWS Control Tower 如何與這些服務搭配使用而可能遇到的限制。

一般準則

一般而言，我們預期註冊 OU 時支援的帳戶數量會隨著您增加該 OU 的受管區域數量和啟用的控制項數量而減少。這些一般準則假設您已啟用 15 個選用控制項。如果您的 OU 已啟用更多或更少的控制項，註冊時每個 OU 的帳戶限制會有所不同。

- 透過 15 個受管區域，支援最多 1000 個帳戶的 OUs。
- 使用 16 到 21 個受管區域，支援的最大 OU 大小範圍為 600-1000 個帳戶。
- 透過 22 個受管區域，支援最多 680 個帳戶的 OUs。
- 對於 23 個以上的受管區域，支援的最大 OU 大小小於 680 個帳戶。

如果發生錯誤

如果註冊失敗，您可以嘗試重新註冊 OU。此外，您可以使用巢狀 OU 或將帳戶移至另一個 OU，讓 OU 變小。

> **Note**
>
> 基於註冊目的，AWS Control Tower 一律強制執行的強制性控制項不會計入您在 OU 上啟用的控制項數量。

CloudFormation 堆疊集限制

如果您計劃跨多個帳戶註冊大量帳戶 AWS 區域，您可能會遇到 CloudFormation 堆疊集針對組織整體大小所建立的限制。您可以使用此公式估計限制：

組織中的受管帳戶數目 x 受管區域數目 <= 150，000

此限制在 OU 註冊程序期間變得明顯。例如，如果 15 個區域受管，並啟用 15 個選用控制項，則註冊 OU 的限制為 1000 個帳戶。不過，如果您需要向超過 1000 個帳戶註冊 OUs，或者如果您已啟用大量選用控制項，則必須將受管區域的數量減少到 15 以下。此減少是由於堆疊集限制所致。

AWS Config 限制

如果您計劃向大量帳戶註冊 OUs，您可能會遇到帳戶數量上限的限制， AWS Config 允許 每週在所有彙總工具之間建立或刪除。已註冊帳戶不計入此限制：您每週最多可以在 AWS Control Tower 中註冊 1000 個新帳戶。

帳戶和選擇加入區域的第一次限制

如果您計劃第一次向多個選擇加入區域的大量帳戶註冊 OUs，您可能會因為帳戶管理配額而遇到限制，這可能會導致延遲延長。由於延遲，OU 註冊期間可能會發生錯誤。

AWS Control Tower 功能的區域差異

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

- AWS Service Catalog 不適用於 AWS Control Tower 提供的所有 AWS 區域 ，這會變更這些區域中帳戶工廠的行為。
- 在某些區域中，帳戶工廠自訂 (AFC) 無法使用，因為 Service Catalog 無法支援藍圖的基礎功能。
- AWS 區域 由於缺少基礎功能，某些控制項無法在所有 中使用。
- AWS 區域 由於缺少基礎功能，所有 都無法使用 AFT 和 CfCT。

若要為您的 AWS Control Tower 環境做出行為的最佳判斷，請確認您的所在區域。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。

- 您所需的主要區域是否 AWS Service Catalog 可用？
- 您需要的控制項是否可用？ 請參閱控制限制。
- IAM Identity Center 是否可在您想要的主區域中使用？

控制項的可部署區域

由於缺少基礎相依性，AWS Control Tower 無法在特定區域中部署特定控制項。您可以呼叫 `ListControls`和 `GetControl` APIs，找到任何控制項可部署區域的最新資訊。您也可以在 AWS Control Tower 主控台中檢視可部署的區域。

當您在由 AWS Control Tower 管理的 OU 上啟用控制項時，控制項的有效區域是 AWS Control Tower 受管區域與控制項可部署區域的交集。

例如，可以在在受管區域 X、Y 和 Z 中操作的 OU 上啟用控制項。但在啟用之後，相同的控制項只會部署在區域 X 和 Z 上，因為控制項本身不支援區域 Y。

請務必監控您部署的控制項與在 AWS Control Tower 中操作工作負載的 區域之間的關係，以免您遇到 AWS 資源保護漏洞。

如何檢查您的受保護區域

- 在 AWS Control Tower 主控台中，您可以在已啟用控制項區段中檢視已啟用的控制項和區域。
- 如果您呼叫 `GetEnabledControl` API，targetRegions 參數只會顯示您可以有效部署控制項的區域，而不是無法部署的區域。

AWS Control Tower 控制項參考指南

AWS Control Tower 中控制項的詳細資訊已移至 AWS Control Tower 控制項參考指南。

AWS Control Tower 管理員的最佳實務

本主題主要適用於管理帳戶管理員。

管理帳戶管理員負責解釋 AWS Control Tower 控制阻止其成員帳戶管理員執行的一些任務。本主題說明一些傳輸此知識的最佳實務和程序，並提供其他秘訣，讓您有效率地設定和維護 AWS Control Tower 環境。

向使用者說明存取權

AWS Control Tower 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登陸區域內執行管理工作。根據最佳實務，這表示您的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，您有責任視需要向您成員帳戶的使用者和管理員解釋以下資訊。

- 說明使用者和管理員可以在登陸區域內存取哪些 AWS 資源。
- 列出適用於每個組織單位 (OU) 的預防性控制，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

有些管理員和其他使用者可能需要說明他們在登陸區域中可存取 AWS 的資源。此存取可以包括程式設計存取和以主控台為基礎的存取。一般而言，允許 AWS 資源的讀取存取和寫入存取。若要在 內執行工作 AWS，您的使用者需要某種層級的存取權才能執行其任務所需的特定服務。

有些使用者，例如您的 AWS 開發人員，可能需要了解他們可存取的資源，以便他們可以建立工程解決方案。其他使用者，例如在 AWS 服務上執行的應用程式最終使用者，不需要知道登陸區域中 AWS 的資源。

AWS 提供工具來識別使用者 AWS 資源存取的範圍。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 存取建議程式 – AWS Identity and Access Management (IAM) 存取建議程式工具可讓您在 IAM 實體，例如使用者、角色或群組，稱為 AWS 服務時，透過分析上次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 – 透過 IAM 政策模擬器，您可以測試和疑難排解 IAM 型和資源型政策。如需詳細資訊，請參閱使用 IAM 政策模擬器測試 IAM 政策。
- AWS CloudTrail 日誌 – 您可以檢閱 AWS CloudTrail 日誌，以查看使用者、角色或 採取的動作 AWS 服務。如需有關 CloudTrail 的相關資訊，請參閱 AWS CloudTrail 使用者指南。

  AWS Control Tower 登陸區域管理員採取的動作可在登陸區域管理帳戶中檢視。您可以在共用日誌封存帳戶中檢視成員帳戶管理員和使用者採取的動作。

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

說明預防性控制

預防性控制可確保組織的帳戶持續遵守您的公司政策。預防性控制的狀態為強制執行或未啟用。預防性控制使用服務控制政策 (SCPs)、資源控制政策 (RCPs) 或宣告政策來防止政策違規。相比之下，偵測性控制會透過定義的 AWS Config 規則通知您存在的各種事件或狀態。

您的一些使用者，例如 AWS 開發人員，可能需要了解適用於他們使用的任何帳戶和 OUs預防性控制，以便他們可以建立工程解決方案。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**
>
> 此程序假設您已在登陸區域內建立至少一個子 OU，以及至少一個 AWS IAM Identity Center 使用者。

範例：為需要知道的使用者顯示預防性控制

1. 登入 AWS Control Tower 主控台，網址為 https：//https://console.aws.amazon.com/controltower/。
2. 從左側導覽中，選擇組織。
3. 從表格中，選擇您的使用者需要適用控制項相關資訊的其中一個 OUs 名稱。
4. 請注意 OU 的名稱和適用於此 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。

如需控制項及其函數的詳細資訊，請參閱 AWS Control Tower 中的關於控制項。

規劃您的 AWS Control Tower 登陸區域

當您完成設定程序時，AWS Control Tower 會啟動與您的帳戶相關聯的金鑰資源，稱為登陸區域，做為您組織及其帳戶的首頁。

> **Note**
>
> 每個組織可以有一個登陸區域。

如需規劃和設定登陸區域時應遵循的一些最佳實務的相關資訊，請參閱 AWS AWS Control Tower 登陸區域的多帳戶策略。

設定 AWS Control Tower 的方法

您可以在現有組織中設定 AWS Control Tower 登陸區域，也可以從建立包含 AWS Control Tower 登陸區域的新組織開始。

- 在現有組織中啟動 AWS Control Tower：本節適用於已經 AWS Organizations 準備好讓 AWS Control Tower 進行控管的客戶。
- 在新組織中啟動 AWS Control Tower：本節適用於沒有現有 AWS Organizations、OUs 和帳戶的客戶。

> **Note**
>
> 如果您已有 AWS Organizations 登陸區域，您可以將 AWS Control Tower 管控從現有登陸區域擴展到組織內的部分或全部現有 OUs 和帳戶。請參閱管理現有的組織和帳戶。

比較功能

以下是將 AWS Control Tower 新增至現有組織或將 AWS Control Tower 控管延伸至 OUs 和帳戶之間的差異的簡短比較。此外，如果您要從 AWS 登陸區域解決方案移至 AWS Control Tower，也會有一些特殊考量。

關於將 新增至現有組織：將 AWS Control Tower 新增至現有組織是您可以在 主控台中 AWS 完成的任務。在此情況下，您已經擁有已在 AWS Organizations 服務中建立的組織、該組織目前尚未向 AWS Control Tower 註冊，而且之後想要新增登陸區域。

當您將登陸區域新增至現有組織時，AWS Control Tower 會在 AWS Organizations 層級設定平行結構。它不會變更現有組織中OUs 和帳戶。

關於擴展控管：擴展控管適用於已向 AWS Control Tower 註冊的單一組織中的特定 OUs 和帳戶，這表示該組織已存在登陸區域。擴展控管意味著擴展 AWS Control Tower 控制項，以便其限制條件適用於該註冊組織中的特定 OUs 和帳戶。在此情況下，您不會啟動新的登陸區域，只會擴展組織的目前登陸區域。

> **Important**
>
> 特殊考量：如果您目前使用適用於 的AWS 登陸區域解決方案 (ALZ) AWS Organizations，請先向您的 AWS 解決方案架構師確認，再嘗試在組織中啟用 AWS Control Tower。AWS Control Tower 無法執行預先檢查，以判斷 AWS Control Tower 是否可能干擾您目前的登陸區域部署。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

在現有組織中啟動 AWS Control Tower

透過在現有組織中設定 AWS Control Tower 登陸區域，您可以立即開始與現有 AWS Organizations 環境平行運作。您在 中建立的其他 OUs AWS Organizations 保持不變，因為它們並未向 AWS Control Tower 註冊。您可以繼續依現狀使用該些 OU 和帳戶。

AWS Control Tower 會使用現有組織的管理帳戶做為其管理帳戶來進行合併。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 登陸區域。

> **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的帳戶。

將 AWS Control Tower 新增至現有組織的效果

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。這些帳戶會記錄您的團隊在其個別最終使用者帳戶中所採取的動作。稽核和日誌封存帳戶會顯示在 AWS Control Tower 登陸區域內的安全 OU 中。

當您設定登陸區域時，AWS Control Tower 新增的帳戶會成為您現有組織的一部分 AWS Organizations，因此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。

- 它允許跨組織的群組統一計費，因為 AWS Control Tower 新增的帳戶將成為現有組織的一部分。
- 它可讓您從 OU 中的一個管理帳戶管理所有帳戶。
- 它簡化了如何套用和強制執行控制，以涵蓋現有和新帳戶的安全性和合規性。

> **Important**
>
> 在現有 AWS Organizations 組織中啟動 AWS Control Tower 登陸區域，無法讓您將 AWS Control Tower 管控從該組織擴展到未向 AWS Control Tower 註冊的其他 OUs 或帳戶。

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

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

如果您是初次使用 AWS Control Tower 且尚未使用 AWS Organizations，最好的起點是使用 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 AWS Control Tower 登陸區域的多帳戶策略

AWS Control Tower 客戶通常會尋求有關如何設定 AWS 環境和帳戶以獲得最佳結果的指導。 AWS 已建立一組統一的建議，稱為多帳戶策略，以協助您充分利用 AWS 資源，包括 AWS Control Tower 登陸區域。

基本上，AWS Control Tower 可做為與其他 AWS 服務搭配使用的協同運作層，協助您針對 AWS 帳戶和 實作 AWS 多帳戶建議 AWS Organizations。設定登陸區域之後，AWS Control Tower 會繼續協助您在多個帳戶和工作負載中維護公司政策和安全實務。

大多數登陸區域會隨著時間發展。隨著 AWS Control Tower 登陸區域中的組織單位 (OUs) 和帳戶數量增加，您可以透過有助於有效組織工作負載的方式擴展 AWS Control Tower 部署。本章提供如何規劃和設定 AWS Control Tower 登陸區域的規範性指導，以符合 AWS 多帳戶策略，並隨時間擴展。

如需組織單位最佳實務的一般討論，請參閱搭配 的組織單位最佳實務 AWS Organizations。

AWS 多帳戶策略：最佳實務指引

AWS 架構良好的環境最佳實務建議您將資源和工作負載分隔為多個 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，並在發生錯誤時減少爆量半徑。

AWS 帳戶的定義

AWS 帳戶充當 資源容器和資源隔離界限。

> **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。

AWS 帳戶詳細資訊

AWS 帳戶可讓您隔離資源，並包含 AWS 工作負載的安全威脅。帳戶也提供用於計費和管理工作負載環境的機制。

AWS 帳戶是為您的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，您可以有效管理多個 AWS 帳戶，進而管理多個工作負載和環境。

AWS Control Tower 會設定架構良好的環境。它依賴 AWS 帳戶以及 AWS Organizations，這有助於控管可跨多個帳戶擴展的環境變更。

架構良好的環境定義

AWS 將架構良好的環境定義為以 登陸區域開頭的環境。

AWS Control Tower 提供自動設定的登陸區域。它強制執行控制，以確保在您環境中的多個帳戶中符合您的公司準則。

登陸區域的定義

登陸區域是提供建議起點的雲端環境，包括預設帳戶、帳戶結構、網路和安全配置等。從登陸區域，您可以部署利用解決方案和應用程式的工作負載。

設定架構良好的環境的指導方針

建構良好的環境的三個關鍵元件，如以下章節所述：

- 多個 AWS 帳戶
- 多個組織單位 OUs)
- 妥善規劃的結構

使用多個 AWS 帳戶

一個帳戶不足以設定架構良好的環境。透過使用多個帳戶，您可以最佳地支援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：

- 安全控制 – 應用程式有不同的安全設定檔，因此需要不同的控制政策和機制。例如，與稽核人員交談並指向託管支付卡產業 (PCI) 工作負載的單一帳戶會更為容易。
- 隔離 – 帳戶是安全保護的單位。帳戶中可以包含潛在風險和安全威脅，而不會影響其他人。因此，安全需求可能會要求您將帳戶彼此隔離。例如，您可能擁有具有不同安全性設定檔的團隊。
- 許多團隊 – 團隊有不同的責任和資源需求。透過設定多個帳戶，團隊無法互相干擾，因為他們在使用相同帳戶時可能會相互干擾。
- 資料隔離 – 將資料存放區隔離到帳戶有助於限制可存取資料並可管理資料存放區的人數。此隔離有助於防止高度私有資料的未經授權暴露。例如，資料隔離有助於支援遵循一般資料保護法規 (GDPR)。
- 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。您可以建立個別帳戶，以滿足業務特定需求。
- 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、職能團隊或個別使用者建立個別的計費項目。
- 配額配置 – AWS 配額是根據每個帳戶設定。將工作負載分成不同的帳戶，可讓每個帳戶 （例如專案） 獲得明確定義的個別配額。

使用多個組織單位

AWS Control Tower 和其他帳戶協同運作架構可以進行跨帳戶界限的變更。因此， AWS 最佳實務可處理跨帳戶變更，這可能會破壞環境或破壞其安全性。在某些情況下，除了政策之外，變更可能會影響整體環境。因此，我們建議您至少設定兩個強制性帳戶：生產和預備。

此外，基於控管和控制目的， AWS 帳戶通常會分組為組織單位 (OUs)。OUs旨在處理多個帳戶間政策的強制執行。

我們建議至少建立生產前 （或預備） 環境，該環境與您的生產環境不同，並具有不同的控制和政策。生產和預備環境可以建立和管理為單獨的 OUs，並以單獨的帳戶計費。此外，您可能想要設定沙盒 OU 進行程式碼測試。

為登陸區域中OUs 使用妥善規劃的結構

AWS Control Tower 會自動為您設定一些 OUs。隨著工作負載和需求隨時間擴展，您可以擴展原始登陸區域組態以符合您的需求。

> **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。您可以在設定登陸區域之後，透過在 OUs 詳細資訊頁面上選取編輯來重新命名 OU。

建議

AWS Control Tower 為您設定第一個必要的 OU 之後，我們建議您在登陸區域中建立一些額外的 OUs。

我們建議您允許 AWS Control Tower 建立至少一個額外的 OU，稱為沙盒 OU。此 OU 適用於您的軟體開發環境。如果您選取沙盒 OU，AWS Control Tower 可以在登陸區域建立期間為您設定沙盒 OU。

您可以自行設定的兩個建議其他 OUs：基礎設施 OU 包含共用服務和聯網帳戶，以及 OU 包含生產工作負載，稱為工作負載 OU。您可以透過組織單位頁面上的 AWS Control Tower 主控台，在登陸區域中新增其他 OUs。

除了自動設定的 OU 之外的建議 OUs

- 基礎設施 OU – 包含您的共用服務和聯網帳戶。

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

- 沙盒 OU – 軟體開發 OU。例如，它可能有固定的花費限制，也可能未連線到生產網路。

> **Note**
>
> AWS Control Tower 建議您設定沙盒 OU，但這是選用的。它可以在設定登陸區域時自動設定。

- 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 OU 結構。您可以建置 AWS Control Tower 環境以符合 AWS 多帳戶策略指引。

您也可以建置更簡單、平坦的 OU 結構，其效能良好，並符合 AWS 多帳戶指引。只是因為您可以建置階層式 OU 結構，並不表示您必須這麼做。

- 若要檢視圖表，其中顯示 OUs 擴展、平面 AWS Control Tower 環境中具有 AWS 多帳戶指引的一組 OU 範例，請參閱範例：平面 OU 結構中的工作負載。
- 如需 AWS Control Tower 如何搭配巢狀 OU 結構運作的詳細資訊，請參閱 AWS Control Tower 中的巢狀 OUs。
- 如需 AWS Control Tower 如何符合 AWS 指引的詳細資訊，請參閱 AWS 白皮書：使用多個帳戶組織您的 AWS 環境。

連結頁面上的圖表顯示已建立更多基礎 OUs和更多其他 OUs。這些 OUs 可滿足大型部署的其他需求。

在基礎 OUs欄中，有兩個 OUs已新增至基本結構：

- Security_Prod OU – 提供安全政策的唯讀區域，以及碎片安全稽核區域。
- 基礎設施 OU – 您可能希望將先前建議的基礎設施 OU 分成兩個 OUs，即 Infrastructure_Test （適用於生產前基礎設施） 和 Infrastructure_Prod （適用於生產基礎設施）。

在其他 OUs區域中，已將多數個 OUs新增至基本結構。以下是隨著環境成長而建立的下一個建議 OUs：

- 工作負載 OU – 先前建議但選用的工作負載 OU 已分成兩個 OUs：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 – 允許系統管理員在完全套用控制項和政策之前測試其變更。
- 暫停的 OU – 為可能暫時停用的帳戶提供位置。

關於根目錄

根不是 OU。這是管理帳戶以及組織中所有 OUs和帳戶的容器。概念上，根包含所有 OUs。無法刪除。您無法在 AWS Control Tower 的根層級管理已註冊的帳戶。反之， 會控管您 OUs 中的註冊帳戶。如需實用圖表，請參閱 AWS Organizations 文件。

登陸區域設定的管理秘訣

以下是設定和設定登陸區域的一些秘訣。

- 您執行最多工作 AWS 的區域應該是您的主區域。
- 設定您的登陸區域，並從主區域部署您的 Account Factory 帳戶。
- 如果您要投資多個 AWS 區域，請確定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中。
- 透過將您的工作負載和日誌保留在同一個 AWS 區域中，您可以降低與跨區域移動和擷取日誌資訊相關聯的成本。
- 稽核和其他 Amazon S3 儲存貯體會在您啟動 AWS Control Tower 的相同 AWS 區域中建立。建議不要移動這些儲存貯體。
- 您可以在 Log Archive 帳戶中建立自己的日誌儲存貯體，但不建議這麼做。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，必須在管理帳戶中針對 AWS Control Tower 支援的所有區域啟用 AWS 安全性字符服務 (STS) 端點。否則，啟動可能會在組態過程中途發生失敗。
- AWS Control Tower 僅支援已啟用控制項的標記。如需詳細資訊，請參閱AWS Control Tower 控制標記 APIs。
- 我們建議為 AWS Control Tower 管理的每個帳戶啟用多重驗證 (MFA)。

- 或者，您可以使用 AWS 根存取管理功能，允許對成員帳戶執行根動作，並不需要為每個帳戶啟用 MFA。如需詳細資訊，請參閱使用 為客戶集中管理根存取權 AWS Organizations。

VPCs的考量

- AWS Control Tower 建立的 VPC 僅限於可使用 AWS Control Tower AWS 區域 的 。有些工作負載在不支援的區域中執行的客戶可能想要停用以您的 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，或建立只在所需區域中執行的自訂 VPC。
- AWS Control Tower 建立的 VPC 與為所有 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。
- 如果您在主要區域中刪除預設 VPC AWS ，最好在所有其他 AWS 區域中將其刪除。

登陸區域 v4.0 遷移指南

AWS Control Tower 登陸區域 4.0 引入了登陸區域架構的主要大修，提供靈活的專用控制體驗和完全可選的服務整合。主要增強功能包括選擇性地啟用 AWS Config、AWS CloudTrail、SecurityRoles 和 AWS Backup 整合，以及 AWS Config 和 AWS CloudTrail 的專用資源，以改善隔離。

版本會移除強制性的組織結構需求，讓客戶能夠定義自己的組織結構需求，同時引進新的`ConfigBaseline`偵測性控制支援，而不需要完整的 `AWSControlTowerBaseline`。服務連結的 Config 彙總工具會取代先前的彙總方法，簡化合規資料收集。

此外，資訊清單欄位會變成選用，讓最少的登陸區域部署僅 AWS Organizations 專注於整合和控制啟用。這些變更提供更大的自訂選項，同時維持強大的控管功能，讓客戶更有效地根據其特定需求量身打造 AWS Control Tower。

主題

- 金鑰變更
- AWS Config 更新

金鑰變更

> **Note**
>
> - 「已註冊」和「已註冊」的定義已隨著 AWS Control Tower 的新版本而轉移。當您的帳戶/OU 已啟用任何 AWS Control Tower 資源時（例如控制項或基準），它將被視為受管資源。定義將不再由`AWSControlTowerBaseline`基準的存在所驅動。
> - 服務連結角色會保留在所有登陸區域版本中，並且在 OUs 變成「未註冊」時不再刪除
> - 只有在登陸區域解除委任後，客戶才能手動刪除服務連結角色

- 登陸區域 4.0 的先決條件：透過 API 升級至 4.0 版時，請確定`AWSControlTowerCloudTrailRole`服務角色使用新的受管政策，`AWSControlTowerCloudTrailRolePolicy`而非現有的內嵌政策。分離目前的內嵌政策並連接新的受管政策，如 文件所述。
- 選用資訊清單：登陸區域 API 中的資訊清單欄位現在為選用。客戶可以建立登陸區域，而不需要任何服務整合。對於已經使用資訊清單欄位的現有客戶沒有影響。
- 選用的組織結構：AWS Control Tower 不再強制執行或管理安全 OU 建立，讓客戶可以定義和管理自己的組織結構。不過，AWS Control Tower 會要求針對每個 AWS 服務整合設定的所有帳戶都位於相同的父 OU 下。對於已設定 AWS Control Tower 且具有安全 OU 的客戶，沒有影響。AWS Control Tower 會自動部署在 Security OU 中管理服務整合帳戶所需的資源和控制項。例如，啟用 AWS Config 整合時，會在所有服務整合帳戶中啟用 AWS Config 記錄。AWS Control Tower 基準和 AWS Config 基準不適用於安全 OU 和整合帳戶。若要變更服務整合，請更新登陸區域設定。

  > **Note**
  >
  > - AWS Control Tower 登陸區域 4.0 的組織結構設定已從先前的登陸區域版本變更。AWS Control Tower 將不再建立指定的安全 OU。具有服務整合帳戶的 OU 將是指定的安全 OU。
  > - 如果成員帳戶移至每個整合帳戶所在的 OU，則無論開啟或關閉自動註冊，都會漂移在該 OU 上啟用的控制項。

- 偏離通知：AWS Control Tower 將在未`AWSControlTowerBaseline`啟用 的情況下，停止向登陸區域 4.0 的所有客戶傳送偏離通知至 SNS 主題，並改為開始將偏離通知傳送至管理帳戶中的 EventBridge。若要檢閱如何透過 EventBridge 接收偏離通知的範例事件和指引，請參閱本指南。

- 選用的服務整合：您現在可以啟用/停用所有 AWS Control Tower 整合 AWS Config，包括 AWS CloudTrail、SecurityRoles 和 AWS Backup。這些整合現在在 API 中也有選用的必要enabled旗標。可能適用於您的登陸區域或共用帳戶的基準現在彼此具有相依性。整合的特定相依性為：
  - 啟用：
    - CentralSecurityRolesBaseline → CentralConfigBaseline 需要啟用
    - IdentityCenterBaseline → CentralSecurityRolesBaseline 需要啟用
    - BackupCentralVaultBaseline → CentralSecurityRolesBaseline 需要啟用
    - BackupAdminBaseline → CentralSecurityRolesBaseline 需要啟用
    - LogArchiveBaseline → 獨立 （無相依性）
    - CentralConfigBaseline → 獨立 （無相依性）
  - 停用：
    - CentralConfigBaseline 只有在先停用 CentralSecurityRolesBaseline、BackupAdminBaseline和 BackupCentralVaultBaseline基準時IdentityCenterBaseline，才能停用。
    - CentralSecurityRolesBaseline 只有在 IdentityCenterBaseline、BackupAdminBaseline和 BackupCentralVaultBaseline基準先停用時，才能停用。
    - IdentityCenterBaseline 可以獨立停用。
    - BackupAdminBaseline 和 BackupCentralVaultBaseline基準可以獨立停用
    - LogArchiveBaseline 可以獨立停用

AWS Config 更新

- AWS Config 和 AWS CloudTrail 的專用資源： AWS Config 和 AWS CloudTrail 現在使用單獨的專用 S3 儲存貯體和 SNS 主題，而不是共用資源。客戶在多個整合中使用單一或個別帳戶的彈性受到限制。
  - 升級到 AWS Control Tower 登陸區域 4.0 版時，不會移動現有的資料和 S3 儲存貯體。AWS CloudTrail 整合會繼續使用字首為 的現有 S3 儲存貯體aws-controltower-logs。更新操作後的新 AWS Config 資料將存放在新的 S3 儲存貯體中aws-controltower-config，並加上 AWS Control Tower 在為 CentralConfigBaseline 指定的帳戶中建立的字首。

> **Note**
>
> 第一次在登陸區域 4.0 上啟用 AWS CloudTrail 整合時，每次都會使用字首建立新的 S3 儲存貯體 `aws-controltower-cloudtrail`

- 資料位置變更：從先前共用的現有客戶升級至專用資源時，會在不同的 S3 儲存貯體中擁有 AWS Config 和 AWS CloudTrail 資料。建立的客戶工作流程和工具可能需要更新，才能從新的儲存貯體位置存取資料。
- AWS CloudTrail 將繼續保留在相同的現有儲存貯體中，但 AWS Config 資料將保留在 AWS Control Tower 建立的新 S3 儲存貯體中。
- 如果客戶想要將不同的日誌集中到單一儲存貯體，則可以設定跨儲存貯體複寫。如需詳細資訊，請參閱 S3 文件。
- 如果您已在 AWS Config Control Tower 管理的區域中使用 AWS Control Tower 未建立的預先存在 AWS Config 交付通道註冊帳戶，請將交付通道的 S3 儲存貯體名稱更新為 AWS Config 整合帳戶中具有字首的新 S3 儲存貯`aws-controltower-config-logs-`體，以符合登陸區域 4.0 上的 AWS Control Tower 組態。如需詳細資訊，請參閱註冊具有現有 AWS Config 資源的帳戶。

- AWS Config 登陸區域 4.0 版上的整合：在啟用 AWS Config 整合的情況下遷移至登陸區域 4.0 時，客戶會看到下列變更 -

  1. 現有的 Audit 帳戶會註冊為 的委派管理員 AWS Config。
  2. 服務連結 Config 彙整工具會部署到 Audit 帳戶 （新客戶的AWS Config 中央彙整工具帳戶和現有客戶的 Audit 帳戶）。新的彙總工具可以從組織中的任何 AWS Config 記錄器彙總資料，包括非 Control Tower 受管帳戶。
  3. 現有的彙總工具將被刪除 - 管理帳戶 (`aws-controltower-ConfigAggregatorForOrganizations`) 中的組織彙總器和稽核帳戶 (`aws-controltower-GuardRailsComplianceAggregator`) 中的帳戶彙總器將被刪除。
  4. 由於組態彙總工具是服務連結，因此與已刪除彙總工具相關聯的控制項會自動移除。
     a. 不允許變更 AWS Control Tower for AWS Config 資源建立的標籤
     b. 不允許刪除 AWS Control Tower 建立的 AWS Config 彙總授權

- 新的**`ConfigBaseline`**基準：OU `ConfigBaseline` 層級現在有一個單獨的偵測控制支援，而不需要全面的 `AWSControlTowerBaseline`。如需詳細資訊，請參閱 OU 層級的基準類型清單。對於使用預設登陸區域的現有客戶，所有服務整合現在都是選用的，並具有 中概述的相依性要求警告金鑰變更。
- 服務連結組態彙總工具：取代 AWS Config 中央彙總工具帳戶中的組織和帳戶彙總工具。

- 在啟用 AWS Config 整合的情況下升級至登陸區域 4.0 時，客戶需要具有 `organizations:ListDelegatedAdministrators` 許可

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
           "backup:UpdateGlobalSettings",
           "controltower:CreateLandingZone",
           "controltower:UpdateLandingZone",
           "controltower:ResetLandingZone",
           "controltower:DeleteLandingZone",
           "controltower:GetLandingZoneOperation",
           "controltower:GetLandingZone",
           "controltower:ListLandingZones",
           "controltower:ListLandingZoneOperations",
           "controltower:ListTagsForResource",
           "controltower:TagResource",
           "controltower:UntagResource",
            "servicecatalog:*",
            "organizations:*",
            "organizations:RegisterDelegatedAdministrator",
            "organizations:EnableAWSServiceAccess",
            "organizations:DeregisterDelegatedAdministrator",
            "organizations:ListDelegatedAdministrators",
            "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": "*"
    }
  ]
}
```

設定群組、角色和政策的建議

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，安全帳戶應只能由安全團隊存取，管理帳戶應只能由雲端管理員的團隊存取，以此類推。

如需此主題的詳細資訊，請參閱 AWS Control Tower 中的身分和存取管理。

建議限制

您可以設定 IAM 角色或政策，允許管理員僅管理 AWS Control Tower 動作，以限制組織的管理存取範圍。建議的方法為使用 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 AWS Organizations ，以管理您的預防性控制和 SCPs AWS Config，以及 存取權，以管理偵測性控制。

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強加條件，以限制與 AWS Control Tower 中特定角色互動的帳戶和資源。我們強烈建議您限制對`AWSControlTowerAdmin`角色的存取，因為它允許廣泛的存取許可。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 資源的指引

當您在 AWS Control Tower 中建立和修改資源時，我們建議您採用下列最佳實務。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，您可能需要更新登陸區域或重新註冊 OU，而修改可能會導致合規報告不準確。

  特別是：

  - 保留作用中 AWS Config 的記錄器。如果您刪除 Config 記錄器，偵測控制項將無法偵測和報告偏離。由於資訊不足，不合規資源可能會報告為合規。
  - 請勿修改或刪除在安全組織單位 AWS Identity and Access Management (OU) 中共用帳戶內建立的 (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刪除`AWSControlTowerExecution`角色，即使是在未註冊的帳戶中也一樣。如果您這麼做，您將無法向 AWS Control Tower 註冊這些帳戶，或註冊其直接父系 OUs。
- 請勿禁止 AWS 區域 透過 SCPs或 AWS Security Token Service () 使用任何AWS STS。這樣做會導致 AWS Control Tower 進入未定義狀態。如果您不允許使用 的區域 AWS STS，您的功能會在這些區域中失敗，因為在這些區域中無法使用身分驗證。相反地，依賴 AWS Control Tower 區域拒絕功能，如控制項所示，AWS 根據請求拒絕對 的存取 AWS 區域，其在登陸區域層級運作，或控制區域拒絕套用至 OU 的控制，其在 OU 層級運作以限制對區域的存取。
- 必須 AWS Organizations `FullAWSAccess`套用 SCP，且不應與其他 SCPs 合併。此 SCP 的變更不會報告為偏離；不過，如果拒絕存取特定資源，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 分離或修改，帳戶可能會失去對記錄器的 AWS Config 存取權或在 CloudTrail 日誌中建立間隙。
- 請勿使用 AWS Organizations `DisableAWSServiceAccess` API 關閉您設定登陸區域之組織的 AWS Control Tower 服務存取權。如果您這樣做，某些 AWS Control Tower 偏離偵測功能可能無法正常運作，如果沒有來自 的訊息支援 AWS Organizations。這些偏離偵測功能有助於保證 AWS Control Tower 可以準確報告組織中組織單位、帳戶和控制項的合規狀態。如需詳細資訊，請參閱《API_DisableAWSServiceAccessAWS Organizations API 參考》中的 。
- 一般而言，AWS Control Tower 會一次執行單一動作，必須先完成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在操作時佈建帳戶，帳戶佈建將會失敗。

  例外狀況：

  - AWS Control Tower 允許並行動作來部署選用的控制項。如需詳細資訊，請參閱選用控制項的並行部署。
  - AWS Control Tower 允許帳戶工廠最多十個並行建立、更新或註冊動作。

> **Note**
>
> 如需 AWS Control Tower 所建立資源的詳細資訊，請參閱 什麼是共用帳戶？。

有關帳戶和 OUs提示

- 我們建議您將每個已註冊的 OU 保留為最多 1000 個帳戶，以便在需要帳戶更新時，使用重新註冊 OU 功能來更新這些帳戶，例如設定新的 區域進行控管。
- 若要縮短註冊 OU 所需的時間，建議您將每個 OU 的帳戶數量保留在大約 680 個，即使限制為每個 OU 1000 個帳戶。一般而言，註冊 OU 所需的時間會根據您 OU 操作的區域數量增加，乘以 OU 中的帳戶數量。
- 根據預估，擁有 680 個帳戶的 OU 最多可能需要 2 小時才能註冊和啟用控制項，最多可能需要 1 小時才能重新註冊。此外，具有許多控制項的 OU 比具有少量控制項的 OU 需要更長的時間進行註冊。
- 允許較長的 OU 註冊時間範圍的其中一個考量是此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，因為他們偏好在每個 OU 中允許更多帳戶。

以根使用者身分登入的時機

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

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 更新和移動帳戶。
- 關閉 AWS 帳戶。
- 如需需要根使用者登入憑證之動作的詳細資訊，請參閱《 AWS 帳戶管理 參考指南》中的需要根使用者登入憑證的任務。

> **Note**
>
> 若要變更或啟用AWS 支援計劃，您必須以根使用者身分登入，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 AWS 帳戶 您需要存取的 的電子郵件地址，您可以從 AWS Control Tower 取得。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 AWS 帳戶 您需要存取的 的電子郵件地址，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。

或者，您可以使用 AWS 根存取管理功能，允許在成員帳戶上執行根動作，而不需要以根身分登入。如需詳細資訊，請參閱使用 為客戶集中管理根存取權 AWS Organizations。

AWS Organizations 指引

AWS Control Tower 與 密切相關 AWS Organizations。以下是一些具體指引，說明它們如何以最佳方式協同運作來保護您的 AWS 環境。

- 您可以在 AWS Organizations 文件中找到保護 AWS Control Tower 管理帳戶和成員帳戶安全的最佳實務相關指導。
  - 管理帳戶的最佳實務
  - 成員帳戶的最佳實務
- 請勿更新連接至向 AWS Control Tower 註冊之 OU 的現有服務控制政策 (SCPs)。這樣做可能會導致控制項進入未知狀態，這將會要求您在 AWS Control Tower 中重設登陸區域或重新註冊 OU。反之，您可以使用 AWS Organizations 建立新的 SCPs，並將它們連接到 OUs，而不是編輯 AWS Control Tower 已建立SCPs。
- 將已註冊的個人帳戶從已註冊的 OU 外部移至 AWS Control Tower，會導致必須解決的偏離。請參閱 控管偏離的類型。
- 如果您使用 AWS Organizations 在向 AWS Control Tower 註冊的組織中建立、邀請或移動帳戶，AWS Control Tower 不會註冊這些帳戶，也不會記錄這些變更。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 AWS Organizations 將 OU 移至 AWS Control Tower 建立的組織，則 AWS Control Tower 不會註冊外部 OU。

- AWS Control Tower 處理許可篩選的方式與 AWS Organizations 處理方式不同。如果使用 AWS Control Tower 帳戶工廠佈建您的帳戶，最終使用者可以在 AWS Control Tower 主控台中查看所有 OUs 的名稱和父項，即使他們沒有 AWS Organizations 直接從 擷取這些名稱和父項的許可。
- AWS Control Tower 不支援組織混合許可，例如檢視 OU 父項但不支援檢視 OU 名稱的許可。因此，AWS Control Tower 管理員應擁有完整許可。
- 必須 AWS Organizations `FullAWSAccess`套用 SCP，且不應與其他 SCPs 合併。此 SCP 的變更不會報告為偏離；不過，如果拒絕存取特定資源，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 分離或修改，帳戶可能會失去對記錄器的 AWS Config 存取權或在 CloudTrail 日誌中建立間隙。
- 請勿使用 AWS Organizations `DisableAWSServiceAccess` API 關閉您設定登陸區域之組織的 AWS Control Tower 服務存取權。如果您這樣做，某些 AWS Control Tower 偏離偵測功能可能無法正常運作，如果沒有來自 的訊息支援 AWS Organizations。這些偏離偵測功能有助於保證 AWS Control Tower 可以準確報告組織中組織單位、帳戶和控制項的合規狀態。如需詳細資訊，請參閱《API_DisableAWSServiceAccessAWS Organizations API 參考》中的 。

IAM Identity Center 指引

AWS Control Tower 建議您使用 AWS Identity and Access Management (IAM) 來規範對 的存取 AWS 帳戶。不過，您可以選擇 AWS Control Tower 是否為您設定 IAM Identity Center、您是否以最符合您業務需求的方式為自己設定 IAM Identity Center，還是選擇其他帳戶存取方法。

> **Note**
>
> SSO 是技術產業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身分驗證服務。它允許某人使用一組登入憑證來存取許多應用程式。參考 中的單一登入功能時 AWS，我們指的是名為 AWS 的服務AWS Identity and Access Management，並縮寫為 IAM 或 IAM Identity Center。

根據預設，AWS Control Tower AWS 會為您的登陸區域設定 IAM Identity Center，以符合使用多個帳戶整理 AWS 環境時所定義的最佳實務指引。大多數客戶都會選擇預設值。有時需要替代的存取方法，才能在特定產業或國家/地區的法規合規，或是無法使用 AWS IAM Identity Center AWS 區域 的 。

選擇選項

從主控台，您可以選擇在登陸區域設定程序中自我管理 IAM Identity Center，而不是允許 AWS Control Tower 為您設定。稍後，您可以在登陸區域設定頁面上修改登陸區域設定並更新登陸區域，以選擇變更此選項。

若要停止 AWS Control Tower AWS 中的 IAM Identity Center，或開始使用 AWS IAM Identity Center

1. 導覽至登陸區域設定頁面
2. 選取組態索引標籤
3. 然後選擇適當的選項按鈕，以變更 IAM Identity Center AWS 的選擇。

在您選擇自行管理 AWS IAM Identity Center 做為 IdP 之後，AWS Control Tower 只會建立管理 AWS Control Tower 所需的這些角色和政策，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 角色和群組，而不是在登陸區域設定程序期間，或在帳戶工廠的帳戶佈建期間。

> **Note**
>
> 如果您從 AWS Control Tower AWS 登陸區域移除 IAM Identity Center，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。

具有替代身分提供者 IdPs) 的帳戶工廠客戶，例如 Azure AD、Ping 或 Okta，可以遵循 AWS IAM Identity Center 程序連線到外部身分提供者並加入其 IdP。您可以隨時修改登陸區域設定，讓 AWS Control Tower 產生您的群組和角色。

- 如需 AWS Control Tower 如何根據您的身分來源與 IAM Identity Center 搭配使用的特定資訊，請參閱《 使用者指南》入門頁面的啟動前檢查一節中的 AWS IAM Identity Center 客戶考量事項。
- 如需 AWS Control Tower 行為如何與 IAM Identity Center 和不同身分來源互動的其他資訊，請參閱《IAM Identity Center 使用者指南》中的變更身分來源的考量。
- 如需使用 AWS Control Tower 和 IAM Identity Center 的詳細資訊使用 AWS IAM Identity Center 和 AWS Control Tower，請參閱 。

帳戶工廠指引

> **Note**
>
> 單一帳戶佈建、更新和自訂必須以啟用 AWSControlTowerBaseline 的組織單位 (OU) 為目標。如果 OU 未啟用 AWSControlTowerBaseline，您可以啟用帳戶自動註冊，或在 EnabledBaselines 上使用 ResetEnabledBaseline 和 ResetEnabledControl APIs並在該 OU 上使用 EnabledControls 來註冊帳戶。如需 AWSControlTowerBaseline 的詳細資訊，請參閱：在 OU 層級套用的基準類型。

使用 Account Factory 在 AWS Control Tower 中佈建新帳戶時，您可能會遇到問題。如需有關如何對這些問題進行故障診斷的資訊，請參閱《AWS Control Tower 使用者指南》的故障診斷新帳戶佈建失敗一節。

我們建議您建立聯合身分使用者或 IAM 角色，而不是 IAM 使用者。聯合身分使用者和 IAM 角色為您提供暫時登入資料。IAM 使用者具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）。

如果您在 Account Factory 中佈建新帳戶或使用註冊帳戶功能 AWS Control Tower 時，已驗證為 IAM 使用者或 IAM Identity Center 使用者，請確認您的使用者可存取您的 AWS Service Catalog 產品組合。否則，您可能會收到來自 Service Catalog 的錯誤訊息。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》中的故障診斷一節。

> **Note**
>
> 一次最多可佈建五個帳戶。

訂閱 SNS 主題的指引

訂閱 SNS 主題以取得 AWS Control Tower 環境的相關資訊。

> **Note**
>
> AWS Control Tower 會停止為所有 LZ4.0+ 上的客戶傳送偏離通知至 SNS 主題。

- `aws-controltower-AllConfigNotifications` SNS 主題會接收 發佈的所有事件 AWS Config，包括合規通知和 Amazon CloudWatch 事件通知。例如，如果發生控制違規，本主題會通知您。它也會提供有關其他類型事件的資訊。(AWS Config進一步了解設定此主題時發佈的內容。)
- 來自`aws-controltower-BaselineCloudTrail`追蹤的資料事件也會設定為發佈至 `aws-controltower-AllConfigNotifications` SNS 主題。
- 若要接收詳細的合規通知，建議您訂閱 `aws-controltower-AllConfigNotifications` SNS 主題。本主題彙總所有子帳戶的合規通知。
- 若要接收偏離通知和其他通知以及合規通知，但整體而言較少通知，建議您訂閱 `aws-controltower-AggregateSecurityNotifications` SNS 主題。
- 若要接收有關 AWS Control Tower Account Factory for Terraform (AFT) 錯誤的通知，您可以訂閱名為 的 SNS 主題aft_failure_notifications，如 AFT 儲存庫所示。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 主題和合規的詳細資訊，請參閱預防和通知。

KMS 金鑰的指引

AWS Control Tower 可與 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。您可以在更新登陸區域時新增或變更 KMS 金鑰。最佳實務是建議您使用自己的 KMS 金鑰，並隨時變更它們。

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 會執行現有金鑰的預先檢查。如果您選擇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 叢集相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，才能使用 AWS Control Tower。如需詳細資訊，請參閱名為 的章節更新 KMS 金鑰政策。

登陸區域更新的最佳實務

當您考慮在 AWS Control Tower 中升級登陸區域版本時，本節提供一些考量和最佳實務。從 2.0 登陸區域版本系列變更為 3.0 登陸區域版本系列尤其重要。升級登陸區域時，AWS Control Tower 會自動將您移至最新的可用版本。

> **Note**
>
> 最佳實務是更新至最新版本的登陸區域。

本節中說明的最佳實務摘要

- 最佳實務：基於安全和稽核原因，強烈建議您為所有帳戶啟用整個電路板的記錄，並將記錄資訊傳送至集中位置。在 AWS Control Tower 中，此集中位置是日誌封存帳戶，可提供 Amazon S3 記錄儲存貯體。
- 最佳實務：如果您選擇退出 AWS Control Tower 中的組織層級 CloudTrail 追蹤，請設定和管理您自己的追蹤。
- 最佳實務：操作 AWS Control Tower 環境時，請設定測試環境。

從 2.x 登陸區域版本移至 3.x 登陸區域版本的優勢

- 僅在主區域中記錄 AWS Config 資源，這可在您管理全域資源時節省成本
- 使用您自己的 KMS 金鑰加密您的 AWS CloudTrail 線索
- 自訂您的日誌保留時間範圍
- 增強型強制性控制
- 可用的控制項數量增加
- 與 整合 AWS Security Hub CSPM
- Python 執行期更新

從 2.x 登陸區域版本移至 3.x 登陸區域版本的注意事項

- 在登陸區域 3.0 及更新版本中，AWS Control Tower 不再支援 AWS 管理的帳戶層級 AWS CloudTrail 追蹤。
- 您可以選擇由 AWS Control Tower 管理的組織層級追蹤，或選擇退出它並管理您自己的 CloudTrail 追蹤。
- 有些潛在的雙成本存在，特別是如果 OU 中的某些帳戶未註冊 AWS Control Tower，並且有自己想要保留的帳戶層級追蹤。

選擇組織層級 CloudTrail 追蹤的考量

- 當您升級至 3.0 或更新版本時，AWS Control Tower 會在 24 小時後刪除其最初建立的帳戶層級追蹤。【例外狀況】
- 不會遺失來自這些線索的資料。即使移除線索，您現有的日誌也會保留。
- AWS Control Tower 會在追蹤的相同 Amazon S3 儲存貯體中建立新的路徑，以區分帳戶層級追蹤與組織層級追蹤。
  - 帳戶追蹤日誌路徑的格式如下：`/orgId/AWSLogs/...`
  - 組織追蹤日誌路徑的格式如下：`/orgId/AWSLogs/orgId/...`
- 您已部署的其他 CloudTrail 線索，AWS Control Tower 未部署的線索不會碰觸到。
- 如果未註冊的帳戶是已註冊 OU 的一部分，則所有帳戶都會包含在組織層級追蹤中，包括未在 AWS Control Tower 註冊的帳戶。
- 連結帳戶中的 Amazon CloudWatch 警示不會觸發。
- 如果您選擇退出組織層級追蹤，AWS Control Tower 仍會建立追蹤，但將其狀態設定為關閉。
- 最佳實務是，如果您選擇退出 AWS Control Tower 中的組織層級追蹤，您應該設定和管理自己的 CloudTrail 追蹤，

組織層級追蹤的優勢

- 組織追蹤適用於 OU 中的所有帳戶。
- 記錄的項目是標準化的，帳戶使用者無法修改。

考慮測試環境

升級登陸區域時，AWS Control Tower 只會對共用帳戶和基礎 OU 進行變更。它不會對工作負載帳戶或 OUs 進行變更。不過，根據最佳實務，在操作 AWS Control Tower 環境時，建議您設定測試環

境。在隔離的測試環境中，您可以測試 AWS Control Tower 登陸區域升級，以及您對服務控制政策 (SCPs) 所做的任何變更，也可以測試您想要套用至環境的控制。如果您在受管制的產業中操作，此建議特別有用。

更新時常見錯誤的檢查清單

以下是您可以執行的簡短任務清單，以避免將 AWS Control Tower 登陸區域從 2.x 版本更新為 3.x 版本時發生常見錯誤。

基本更新檢查清單

- 檢查您的登陸區域：

  – 前往 AWS Control Tower 服務，檢閱組織單位和帳戶頁面，然後確認您的帳戶狀態設定為已註冊和已註冊。

  – 如適用，請驗證並確認自訂管道的上次執行是否成功。

  – 檢查稽核帳戶中的 Amazon S3 集中式記錄儲存貯體，因為先前對儲存貯體政策所做的任何變更都會遭到覆寫。
- 驗證 AWS Control Tower 未擁有的任何 SCPs 不會限制`AWSControlTowerExecution`角色在成員帳戶中執行動作，或在管理帳戶中對執行更新的管理角色執行動作。

AI 型服務和 AWS Control Tower

您可以建立服務控制政策 (SCPs)，讓您選擇退出 AI 型服務儲存資料 AWS。這些 SCP 政策指定 AI 型服務，例如 Amazon Rekognition 或 Amazon CodeWhisperer，無法存放和使用您的資料來改善其他 AI 型 AWS 服務。

這些 AI 選擇不接收 SCP 政策可以套用至整個組織、OU 或特定帳戶。這些政策是全域生效的。您可以在 AWS Organizations 文件中找到 AI 服務選擇退出政策中這些政策的詳細資訊。

如需使用 AI AWS 的服務清單，以及政策範例，請參閱AWS Organizations 《 使用者指南》中的 AI 服務選擇退出政策語法和範例。

AWS Control Tower 中的組態更新管理

中央雲端管理員團隊的成員必須負責更新您的登陸區域。更新您的登陸區域可確保 AWS Control Tower 已修補和更新。此外，為了保護您的登陸區域免於潛在的合規問題，中央雲端管理員團隊的成員應在偵測到和報告偏離問題時立即解決。

> **Note**
>
> AWS Control Tower 主控台會指出何時需要更新登陸區域。如果您沒有看到更新選項，您的登陸區域已經是最新的。

下表包含 AWS Control Tower 登陸區域更新版本的清單，其中包含每個版本的說明連結。

版本	版本日期	Description
4.0	11-17-2025	登陸區域 4.0 版
3.3	12-12-2023	登陸區域 3.3 版
3.2	6-09-2023	登陸區域 3.2 版
3.1	2-09-2023	登陸區域 3.1 版
3.0	7-26-2022	登陸區域 3.0 版
2.9	4-22-2022	登陸區域 2.9 版
2.8	2-10-2022	登陸區域 2.8 版
2.7	4-8-2021	登陸區域 2.7 版
2.6	12-29-2020	登陸區域 2.6 版
2.5	11-18-2020	登陸區域 2.5 版
2.4	無	無
2.3	3-5-2020	登陸區域 2.3 版

版本	版本日期	Description
2.2	11-13-19	登陸區域 2.2 版
2.1	6-24-19	登陸區域 2.1 版

每次更新登陸區域時，您都有機會修改登陸區域設定。

更新的優點

- 您可以變更受管區域
- 您可以變更日誌保留政策
- 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的 CloudTrail 追蹤。
- 您可以解決登陸區域偏離

當您更新登陸區域時，您會自動收到 AWS Control Tower 的最新功能。在登陸區域設定頁面上檢視您目前的登陸區域版本。

如果更新失敗，AWS Control Tower 不會轉返至先前的登陸區域版本。您可能會發現您的登陸區域處於不確定狀態。若是如此，請聯絡 AWS 支援。如需故障診斷更新失敗的詳細資訊，請參閱 無法更新登陸區域。

當您更新登陸區域時，有機會清除未使用的 AWS 身分中心 （ 先前稱為 AWS SSO) 映射。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 Identity Center 映射。

> 更新和重設的先決條件 – 關閉申請者付款
>
> 更新或重設登陸區域之前，請確定 Log Archive 帳戶的 Amazon S3 記錄儲存貯體未啟用申請者付款功能。您必須先關閉此功能，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，只有不當啟用申請者付款功能的客戶必須將其關閉。如需詳細資訊，請參閱 CloudTrail 的 Amazon S3 儲存貯體政策和使用申請者付款儲存貯體。

關於登陸區域更新

需要更新才能修正控管偏離，或移至 AWS Control Tower 的新版本。若要執行 AWS Control Tower 的完整更新，您必須先更新登陸區域，然後個別更新已註冊的帳戶。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：通常透過選擇登陸區域設定頁面上的更新來執行這種類型的更新。您可能需要執行登陸區域更新來解決特定類型的偏離，而且您可以視需要選擇重設。
- 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，請導覽至帳戶詳細資訊頁面，然後選取更新帳戶。也可以透過手動程序、選擇重新註冊 OU 或使用自動化指令碼方法更新帳戶，如本頁稍後章節所述。
- 完整更新：完整更新包含登陸區域的更新，接著更新已註冊 OUs 中的所有已註冊帳戶。AWS Control Tower 的新版本需要完整更新，例如 3.0、3.2 等。若要簡化完整更新程序，對於 1000 個或更少帳戶的 OUs，您可以選擇重新註冊 OU 以更新該 OU 中的所有帳戶，並為每個 OU 重複重新註冊 OU 命令。

如需登陸區域更新的詳細資訊，請參閱登陸區域更新的最佳實務。

> **Note**
>
> 完成登陸區域更新後，您無法復原更新或降級至先前的版本。

更新您的登陸區域

更新 AWS Control Tower 登陸區域最簡單的方式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到達。

登陸區域設定頁面會顯示登陸區域的目前版本，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。

標準更新程序

下列程序會逐步解說從主控台完整更新 AWS Control Tower 的步驟。若要更新個別帳戶，請參閱 在 主控台中更新帳戶。

若要更新您的登陸區域，每個 OU 可使用任意數量的帳戶

1. 開啟 Web 瀏覽器，然後導覽至位於 https：//https://console.aws.amazon.com/controltower/home/update 的 AWS Control Tower 主控台。
2. 在精靈中檢閱資訊，然後選擇 Update (更新)。這會更新登陸區域的後端以及您的共用帳戶。此程序可能需要稍微超過半小時。
3. 更新您的成員帳戶 （ 若 OU 包含超過 1000 個帳戶，必須遵循此程序 ）。
4. 從左側導覽窗格中，選擇組織。
5. 若要更新每個帳戶，請遵循 中提供的步驟在 主控台中更新帳戶。

> **選擇性地重新註冊 OU 以更新帳戶**
>
> 對於帳戶少於 1000 OUs，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。

選取登陸區域版本

如果您執行的是 AWS Control Tower 登陸區域 3.1 版及更高版本，您可以選擇保留目前的版本，也可以在登陸區域組態上執行更新或重設操作時升級至較新的版本。在大多數情況下，重設操作是修復偏離的最佳方式。

您可以在 AWS Control Tower 主控台或透過 AWS Control Tower APIs 來選擇登陸區域版本。

> **Note**
>
> 如果您選擇部署略過中繼版本的登陸區域版本，例如，如果您從 3.1 移至 3.3，AWS Control Tower 會自動部署中繼版本作為更新操作的一部分。
> 在對話中，移至較新版本通常稱為升級，而不只是更新。這兩個概念不同，因為您可以在不升級至新版本的情況下更新登陸區域設定，例如，變更您管理的區域。在 主控台中，更新按鈕會根據您目前的登陸區域版本和您選取要部署的版本，執行就地更新或升級操作。

選擇您的登陸區域版本 – 主控台程序

1. 從 AWS Control Tower 主控台，導覽至登陸區域設定頁面。在可用登陸區域的表格中，選取新版本。請記住，您可以選取 3.1 版或更新版本。3.1 之前的版本與此功能不相容。
2. 當您從資料表中選取版本時，您可以看到可用的動作。如果您目前的版本早於選取的版本，則可使用更新。如果您目前的版本是 3.1 或更新版本，則可以重設。
3. 選擇版本後，請選取畫面右上角的更新按鈕或重設按鈕。
4. 您會看到確認顯示，顯示您為部署選取的登陸區域版本。若要繼續，請選擇右下角的下一步。您的更新操作可能需要幾分鐘或更久的時間。
5. 更新登陸區域之後，您可能需要更新帳戶。執行帳戶更新最簡單的方法是重新註冊每個已註冊 OU 的 OUs 程序。

帳戶更新、登陸區域版本和基準

AWS Control Tower 登陸區域是對應於一組基準組態 AWS 的資源。基準和登陸區域版本沒有one-to-one的映射。您可以檢視顯示 的資料表OU 基準和登陸區域版本的相容性。

當您跳躍基準版本時，您必須在登陸區域更新後更新帳戶。例如，從 3.1 升級到 3.2 時，您不需要更新帳戶，因為這些登陸區域版本具有相同的基準。

相反地，如果您從 3.1 升級到 3.3，您必須更新帳戶，因為基準版本是 4.0，其中包含 3.2 到 3.3。

如需登陸區域版本與基準之間的關係詳細資訊，請參閱 OU 基準和登陸區域版本的相容性。

在登陸區域更新期間保留 AWS CloudTrail 線索

您可以選擇在升級 AWS Control Tower 登陸區域版本時保留帳戶層級 AWS CloudTrail 追蹤。

先決條件

- 您的登陸區域版本低於 3.0。
- 您最新的建立或更新操作已成功。

保留帳戶層級追蹤並選擇加入組織層級 CloudTrail 追蹤

1. 聯絡 AWS Support 要求允許列出您的帳戶。

2. 支援團隊會確認允許列出目標帳戶的時間。
3. 確認後，將您的登陸區域更新至 3.1 版或更新版本，然後選擇AWS CloudTrail 組態 - 已啟用。

保留帳戶層級追蹤，並選擇退出 AWS Control Tower 管理的 CloudTrail 追蹤

1. 聯絡 AWS Support 要求允許列出您的帳戶。
2. 支援團隊會確認允許列出目標帳戶的時間。
3. 確認後，將您的登陸區域更新至 3.1 版或更新版本，然後選擇AWS CloudTrail 組態 - 未啟用。

> **Important**
>
> 保留帳戶層級 CloudTrail 追蹤之後，我們無法從允許清單中移除追蹤或移除您的帳戶。

如何提出支援請求以保留您的帳戶層級追蹤

如果您需要在登陸區域更新期間保留帳戶層級追蹤，您必須聯絡 AWS Support，將您的帳戶新增至 AWS Control Tower 允許清單。請依照下列步驟提交支援票證：

1. 登入 AWS 管理主控台。
2. 導覽至 AWS 支援中心。
3. 選擇建立案例。
4. 針對案例類型，選取技術支援。
5. 針對服務，選擇 AWS Control Tower。
6. 針對類別，選取一般指引。
7. 在主旨列中，包含下列片語：

```
Allow retention of account-level trails during Landing Zone update
```

8. 在描述欄位中，提供下列詳細資訊：
   - 您的 AWS 管理帳戶號碼
   - 為您的 AWS Control Tower 環境選取的主要區域
9. 填寫支援案例表單中的任何其他必要欄位。
10選擇提交以建立支援案例。

提交票證後， AWS Support 會檢閱您的請求，並在適當時將您的帳戶新增至允許清單。您將會透過支援案例通訊管道收到進一步的指示和確認。

> **Note**
>
> 若要在允許清單之後刪除帳戶層級追蹤，請使用 管理帳戶來刪除 CloudFormation 堆疊集或特定堆疊執行個體。堆疊中的所有資源都會遭到刪除。

使用重設並重新註冊來解決偏離

當您和您的組織成員使用登陸區域時，通常會發生偏離。

AWS Control Tower 中會自動偵測偏離。自動掃描 SCPs 可協助您識別需要變更或組態更新的資源，這些資源必須進行才能解決偏離。

若要修復許多類型的偏離，請在主控台的登陸區域設定頁面上選擇重設。此外，您可以選擇在主控台中重新註冊 OU，以解決某些類型的偏離。對於控制項，您可以呼叫 ResetEnabledControl API，以程式設計方式解決偏離。如需偏離類型以及如何解決它們的詳細資訊，請參閱 控管偏離的類型和 在 AWS Control Tower 中偵測並解決偏離。

角色偏離發生漂移解析度的一個特殊情況。如果無法使用必要的角色，主控台會顯示警告頁面，以及如何還原角色的一些指示。在角色偏離解決之前，您的登陸區域無法使用。此偏離重設與完整登陸區域重設不同。如需詳細資訊，請參閱名為 的 區段中的不要刪除必要角色要立即解決的偏離類型。

> **⚠** 當您採取動作來解決登陸區域版本的偏離時，有兩種行為是可能的。
>
> - 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，偏離的登陸區域資源會重設為儲存的 AWS Control Tower 組態。登陸區域版本保持不變。
> - 如果您不是最新版本，則必須選擇更新。登陸區域已升級至最新的登陸區域版本。漂移會在此程序中解決。

使用自動化佈建和更新帳戶

> **Note**
>
> 單一帳戶佈建、更新和自訂必須以啟用 AWSControlTowerBaseline 的組織單位 (OU) 為目標。如果 OU 未啟用 AWSControlTowerBaseline，您可以啟用帳戶自動註冊，或在 EnabledBaselines 上使用 ResetEnabledBaseline 和 ResetEnabledControl APIs並在該 OU 上使用 EnabledControls 來註冊帳戶。如需 AWSControlTowerBaseline 的詳細資訊，請參閱：在 OU 層級套用的基準類型。

您可以透過數種方法在 AWS Control Tower 中佈建或更新個別帳戶：

- 您可以使用 AWS Control Tower Account Factory for Terraform (AFT) 佈建和自訂帳戶。如需詳細資訊，請參閱適用於 Terraform (AFT) 的 AWS Control Tower 帳戶工廠概觀。
- 您可以使用 AWS Control Tower (CfCT) 的自訂更新帳戶。 CfCT 如需詳細資訊，請參閱AWS Control Tower (CfCT) 的自訂概觀。
- 指令碼自動化：如果您偏好使用 API 方法，您可以使用 Service Catalog 的 API 架構和更新帳戶 AWS CLI ，以批次程序更新帳戶。您將為每個帳戶呼叫 Service Catalog 的 `UpdateProvisionedProduct` API。您可以使用此 API，編寫指令碼來逐一更新帳戶。新增區域進行控管時，有關此方法的詳細資訊，請參閱部落格文章：在新 AWS 區域中啟用護欄。

  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，請參閱透過 Service Catalog APIs 自動化 AWS Control Tower 中的帳戶佈建。

> **影片演練**
>
> 專為使用指令碼自動佈建帳戶影片演練而設計，但步驟也適用於帳戶更新。使用 `UpdateProvisionedProduct` API 而非 `ProvisionProduct` API。

自動化的另一個步驟是檢查 AWS Control Tower `UpdateLandingZone`生命週期事件是否成功。使用它做為觸發，開始更新影片中所述的個別帳戶。生命週期事件會標記一系列活動的完成，因此此事件的出現表示登陸區域更新已完成。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.
- 自動化 AWS Control Tower 中的任務.

自動化 AWS Control Tower 中的任務

許多客戶偏好自動化 AWS Control Tower 中的任務，例如帳戶佈建、控制指派和稽核。您可以使用呼叫 來設定這些自動化動作：

- AWS Service Catalog API
- AWS Organizations API
- AWS Control Tower APIs
- AWS CLI

其他資訊和連結 此頁面包含許多卓越技術部落格文章的連結，可協助您自動化 AWS Control Tower 中的任務。以下各節提供本 AWS Control Tower 使用者指南中區域的連結，可協助您自動化任務。

自動化控制任務

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

如需如何使用 AWS Control Tower APIs 執行控制操作的詳細資訊，請參閱部落格文章 AWS Control Tower 發行 API，這是您組織單位的預先定義控制項。

自動化登陸區域任務

AWS Control Tower 登陸區域 APIs 可協助您自動化與登陸區域相關的特定任務。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 APIs 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。

自動化帳戶關閉

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 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 Customization (AFC) 可協助您從 AWS Control Tower 主控台建立帳戶，其中包含我們稱為藍圖的自訂 CloudFormation 範本。此程序會在設定單一藍圖後自動執行，因為您可以在不維護管道的情況下，重複建立新帳戶和更新帳戶。

AWS Control Tower Account Factory for Terraform (AFT) 遵循 GitOps 模型，以在 AWS Control Tower 中自動化帳戶佈建和帳戶更新的程序。如需詳細資訊，請參閱使用 AWS Control Tower Account Factory for Terraform (AFT) 佈建帳戶。

AWS Control Tower (CfCT) 的自訂可協助您自訂 AWS Control Tower 登陸區域，並保持符合 AWS 最佳實務。 CfCT 自訂是使用 AWS CloudFormation 範本、服務控制政策 (SCPs) 和資源控制政策 (RCPs實作。如需詳細資訊，請參閱AWS Control Tower (CfCT) 的自訂概觀。

如需自動化帳戶佈建的詳細資訊和影片，請參閱演練：AWS Control Tower 中的自動化帳戶佈建和 IAM 角色的自動化佈建。

另請參閱依指令碼更新帳戶。

帳戶的程式設計稽核

如需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。

自動化其他任務

如需有關如何使用自動化請求方法增加特定 AWS Control Tower 服務配額的資訊，請檢視此影片：自動化服務限制增加。

如需涵蓋自動化和整合使用案例的技術部落格，請參閱自動化和整合。

GitHub 上提供兩個開放原始碼範例，協助您處理與安全性相關的特定自動化任務。

- 名為 aws-control-tower-org-setup-sample 的範例說明如何自動將 Audit 帳戶設定為安全相關服務的委派管理員。
- 名為 aws-control-tower-account-setup-using-step-functions 的範例說明如何在佈建和設定新帳戶時，使用 Step Functions 自動化安全最佳實務。此範例包括將主體新增至組織共用的 AWS Service Catalog 產品組合，以及自動將整個組織的 AWS IAM Identity Center 群組與新帳戶建立關聯。它還說明如何刪除每個區域中的預設 VPC。

AWS 安全參考架構包含程式碼範例，用於自動化與 AWS Control Tower 相關的任務。如需詳細資訊，請參閱 AWS 規範指引頁面和相關聯的 GitHub 儲存庫。

如需將 AWS Control Tower 與 AWS CloudShell 搭配使用的相關資訊，CloudShell 是一種有助於在 CLI AWS 中運作 AWS 的服務，請參閱 AWS CloudShell 和 AWS CLI。

由於 AWS Control Tower 是 的協同運作層 AWS Organizations，因此許多 AWS 其他服務可透過 APIs 和 CLI AWS 使用。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 是一種有助於在 CLI AWS 中工作的 AWS 服務，它是瀏覽器型、預先驗證的 Shell，您可以直接從 啟動 AWS 管理主控台。您不需要下載或安裝命令列工具。您可以從您偏好的 shell (Bash、PowerShell 或 Z shell) 執行 AWS Control Tower 和其他 AWS 服務的 AWS CLI 命令。

當您從 啟動 AWS CloudShellAWS 管理主控台時，您用來登入主控台的 AWS 登入資料可在新的 shell 工作階段中使用。您可以在與 AWS Control Tower 和其他 AWS 服務互動時，略過輸入設定登入資料，而且您將使用預先安裝在 shell 運算環境的第 2 AWS CLI 版。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，可讓管理員將存取許可授予 IAM 使用者和 IAM Identity Center 使用者 AWS CloudShell。

管理員授予使用者存取權的最快速方法是透過 AWS 受管政策。AWS 受管政策是由 AWS建立並管理的獨立政策。下列適用於 CloudShell 的 AWS 受管政策可以連接到 IAM 身分：

- `AWSCloudShellFullAccess`：授予許可，以 AWS CloudShell 使用 並完整存取所有功能。

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。如需限制 CloudShell 中使用者可用的動作的詳細資訊，請參閱AWS CloudShell 《 使用者指南》中的使用 IAM 政策管理 AWS CloudShell 存取和用量。

> **Note**
>
> 您的 IAM 身分也需要政策，授予對 進行呼叫的許可 AWS Control Tower。如需詳細資訊，請參閱使用 AWS Control Tower 主控台所需的許可。

啟動 AWS CloudShell

從 中 AWS 管理主控台，您可以選擇導覽列上可用的下列選項來啟動 CloudShell：

- 選擇 CloudShell 圖示。
- 開始在搜尋方塊中輸入「cloudshell」，然後選擇 CloudShell 選項。

現在您已啟動 CloudShell，您可以輸入需要使用的任何 AWS CLI 命令 AWS Control Tower。例如，您可以檢查 AWS Config 狀態。

透過 與 互動 AWS Control Tower AWS CloudShell

AWS CloudShell 從 啟動後 AWS 管理主控台，您可以立即從命令列 interface. AWS CLI commands AWS Control Tower 開始與 互動，在 CloudShell 中以標準方式運作。

> **Note**
>
> 在 AWS CLI 中使用 時 AWS CloudShell，您不需要下載或安裝任何其他資源。您已在 shell 中驗證，因此在進行呼叫之前不需要設定登入資料。

使用 AWS CloudShell 協助設定 AWS Control Tower

在執行這些程序之前，除非另有說明，否則您必須登入您登陸區域的 AWS 管理主控台 主區域中的 ，而且您必須以 IAM Identity Center 使用者或 IAM 使用者身分登入，並具有包含您登陸區域的管理帳戶管理許可。

1. 以下是在開始設定 AWS Control Tower 登陸區域之前，您可以在 中使用 AWS Config CLI 命令 AWS CloudShell 來判斷組態記錄器和交付管道的狀態。

   範例：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`
   - 正常回應類似 `"name": "default"`
2. 如果您有在設定 AWS Control Tower 登陸區域之前需要刪除的現有 AWS Config 記錄器或交付管道，您可以輸入以下命令：

   範例：管理您預先存在 AWS Config 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 Control Tower 的資源 AWS Config。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. 此範例顯示您要從 輸入的 AWS CLI 命令 AWS CloudShell ，以啟用或停用受信任的存取 AWS Organizations。對於 AWS Control Tower 您不需要啟用或停用 的受信任存取 AWS Organizations，這只是範例。不過， AWS 如果您要在其中自動化或自訂動作，您可能需要啟用或停用其他服務的受信任存取 AWS Control Tower。

   範例：啟用或停用受信任的服務存取

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

範例：使用 建立 Amazon S3 儲存貯體 AWS CloudShell

在下列範例中，您可以使用 AWS CloudShell 建立 Amazon S3 儲存貯體，然後使用 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 AWS 區域中建立儲存貯體，請在 CloudShell 命令列中輸入下列命令：

```
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**
>
> 如果您未遵守命名儲存貯體的規則（例如，僅使用小寫字母），則會顯示下列錯誤：呼叫 CreateBucket 操作時發生錯誤 (InvalidBucketName)：指定的儲存貯體無效。

2. 若要上傳檔案並將其新增為物件至剛建立的儲存貯體，請呼叫 PutObject方法：

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

如果物件成功上傳至 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 是存放物件的雜湊。它可用來檢查上傳至 Amazon S3 之物件的完整性。

使用 建立 AWS Control Tower 資源 AWS CloudFormation

AWS Control Tower 已與 整合 AWS CloudFormation，此服務可協助您模型化和設定 AWS 資源，以減少建立和管理資源和基礎設施的時間。您可以建立範本來描述您想要的所有 AWS 資源，例如 `AWS::ControlTower::EnabledControl` for control. CloudFormation provisions 和 為您設定這些資源。

使用 時 CloudFormation，您可以重複使用範本來一致且重複地設定 AWS Control Tower 資源。描述您的資源一次，然後在多個 AWS 帳戶 和 區域中逐一佈建相同的資源。

AWS Control Tower 和 CloudFormation 範本

若要佈建和設定 AWS Control Tower 和相關服務的資源，您必須了解 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 CloudFormation 堆疊中佈建的資源。如果您不熟悉 JSON 或 YAML，您可以使用 CloudFormation 設計工具來協助您開始使用 CloudFormation 範本。如需詳細資訊，請參閱《AWS CloudFormation 使用者指南》 中的什麼是 CloudFormation 設計器？。

AWS Control Tower 支援在其中建立 `AWS::ControlTower::EnabledControl`（控制資源）、 `AWS::ControlTower::LandingZone`（登陸區域） 和 `AWS::ControlTower::EnabledBaseline`（基準線） 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 `EnableControl`和 `DisableControl`更新限制 AWS Control Tower 為 100 個並行操作。

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 CloudFormation。

進一步了解 CloudFormation

若要進一步了解 CloudFormation，請參閱下列資源：

- AWS CloudFormation
- AWS CloudFormation 使用者指南
- CloudFormation API 參考
- AWS CloudFormation 命令列界面使用者指南

自訂您的 AWS Control Tower 登陸區域

AWS Control Tower 登陸區域的某些層面可在 主控台中設定，例如選擇區域和選用控制項。其他變更可能會透過自動化在 主控台外部進行。

例如，您可以使用適用於 AWS Control Tower 的 Customizations 功能為您的登陸區域建立更廣泛的自訂，這是 GitOps 樣式的自訂架構，可與 AWS CloudFormation 範本和 AWS Control Tower 生命週期事件搭配使用。

從 AWS Control Tower 主控台自訂

若要對登陸區域進行這些自訂，請遵循 AWS Control Tower 主控台提供的步驟。

在設定期間選取自訂名稱

- 您可以在設定期間選取最上層的 OU 名稱。您可以隨時使用 AWS Organizations 主控台重新命名 OUs，但在 中變更 OUs AWS Organizations 可能會導致可修復的偏離。
- 您可以選取共用稽核和日誌封存帳戶的名稱，但您無法在設定後變更名稱。（這是一次性選擇。）

> **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（並避免偏離），您必須透過 AWS Control Tower 執行 OU 操作，包括建立、刪除或重新註冊 OU。

選取 AWS 區域

- 您可以透過選取特定區域進行控管來自訂登陸 AWS 區域。請遵循 AWS Control Tower 主控台中的步驟。
- 您可以在更新登陸 AWS 區域時選取和取消選取控管的區域。
- 您可以將區域拒絕控制設定為已啟用或未啟用，並控制使用者對未受管區域中大多數 AWS 服務的存取 AWS 。

如需 CfCT 具有部署限制 AWS 區域 之處的詳細資訊，請參閱 控制限制。

透過新增選用控制項來自訂

- 強烈建議且選擇性的控制是選用的，這表示您可以透過選擇要啟用哪些控制來自訂登陸區域的強制執行層級。預設不會啟用選用控制項。
- 選用的資料駐留控制可讓您自訂存放區域，並允許存取您的資料。
- 屬於整合式 Security Hub CSPM 標準一部分的選用控制項可讓您掃描 AWS Control Tower 環境，以檢查安全風險。
- 選用的主動控制可讓您在佈建 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 線索

- 當您將登陸區域更新至 3.0 版或更新版本時，您可以選擇加入或退出由 AWS Control Tower 管理的組織層級 CloudTrail 追蹤。您可以在更新登陸區域時變更此選項。AWS Control Tower 會在您的管理帳戶中建立組織層級追蹤，該追蹤會根據您的選擇進入作用中或非作用中狀態。登陸區域 3.0 不支援帳戶層級的 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。重複的線索可能會產生額外費用。

在主控台中建立自訂成員帳戶

- 您可以建立自訂的 AWS Control Tower 成員帳戶，也可以從 AWS Control Tower 主控台更新現有的成員帳戶以新增自訂。如需詳細資訊，請參閱使用帳戶工廠自訂 (AFC) 自訂帳戶。

在 AWS Control Tower 主控台外自動化自訂

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

- 您可以在 GitOps 樣式的工作流程中，使用 Account Factory for Terraform (AFT) 在佈建期間自訂帳戶。

  AFT 使用 Terraform 模組部署，可在 AFT 儲存庫中取得。
- 您可以使用 Customizations for AWS Control Tower (CfCT) 自訂 AWS Control Tower 登陸區域，這是以 AWS CloudFormation 範本和服務控制政策 (SCPs) 建置的功能套件。 CfCT 您可以將自訂範本和政策部署到組織中的個別帳戶和組織單位 (OUs)。

  CfCT 的原始碼可在 GitHub 儲存庫中使用。

- 您可以在開啟登陸區域加速器 (LZA) 的情況下自訂 AWS Control Tower 登陸區域 AWS。LZA 解決方案的架構符合 AWS 最佳實務，並符合多個全球合規架構。我們建議您部署 AWS Control Tower 做為基礎登陸區域，然後視需要使用 LZA 增強登陸區域功能。如需詳細資訊，請參閱 AWS Control Tower 和登陸區域加速器。

AWS Control Tower 和登陸區域加速器

本節說明使用 AWS Control Tower 和登陸區域加速器 (LZA) 解決方案的優勢。

您可以在開啟登陸區域加速器 (LZA) 的情況下自訂 AWS Control Tower 登陸區域 AWS 。

LZA 是部署一組基本功能的解決方案，旨在符合 AWS 最佳實務和多個全球合規架構，以協助您管理和管理多帳戶環境。LZA 是使用 AWS 雲端開發套件 (CDK) 建置。

LZA 會自動設定適合託管安全工作負載的雲端環境。此解決方案可以部署在所有 中 AWS 區域，以協助您維持操作和控管的一致性。LZA 解決方案的架構符合 AWS 最佳實務，並符合多個全球合規架構。

我們建議您部署 AWS Control Tower 做為基礎登陸區域，然後視需要使用 LZA 增強登陸區域功能。LZA 和 AWS Control Tower 的組合提供全方位的無程式碼解決方案，可協助您管理和管理多帳戶環境，其專為支援高度受規範的工作負載和複雜的合規要求而打造。AWS Control Tower 和 Landing Zone Accelerator 共同協助您建立平台準備，包括安全、合規和操作功能。

LZA 的原始碼可在 GitHub 儲存庫中使用。

如需如何結合 LZA 和 AWS Control Tower 的詳細資訊，請參閱 LZA 實作指南。

AWS Control Tower (CfCT) 自訂的優點

我們稱為 AWS Control Tower 自訂 (CfCT) 的功能套件可協助您為登陸區域建立比 AWS Control Tower 主控台中建立更廣泛的自訂。它提供 GitOps 樣式的自動化程序。您可以重塑登陸區域，以符合您的業務需求。

此infrastructure-as-code自訂程序整合 AWS CloudFormation 範本 AWS 與服務控制政策 (SCPs) 和 AWS Control Tower 生命週期事件，讓您的資源部署與您的登陸區域保持同步。例如，當您使用 Account Factory 建立新帳戶時，可以自動部署連接至帳戶和 OU 的資源。

> **Note**
>
> 與 Account Factory 和 AFT 不同，CfCT 並非專門用來建立新帳戶，而是透過部署您指定的資源來自訂登陸區域中的帳戶和 OUs。

> **Note**
>
> 在 CfCT 中設定的目標組織單位 (OU) 必須在 AWS Control Tower 中啟用 AWSControlTowerBaseline。如需 AWSControlTowerBaseline 的詳細資訊，請參閱：在 OU 層級套用的基準類型。

優勢

- 擴展自訂且安全 AWS 的環境 – 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。
- 執行個體化您的需求 – 您可以使用範本 AWS CloudFormation 和服務控制政策來表達您的政策意圖，為您的業務需求自訂 AWS Control Tower 登陸區域。
- 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。您可以依賴生命週期事件來協助您自動將資源部署到帳戶和 OUs。
- 擴展您的網路架構 – 您可以部署自訂的網路架構，以改善和保護您的連線，例如傳輸閘道。

其他 CfCT 範例

- AWS 架構部落格文章提供使用 Customizations for AWS Control Tower (CfCT) 的範例聯網使用案例，並使用 Service Catalog 和 AWS Control Tower 自訂部署一致的 DNS。
- 與 CfCT 和 Amazon GuardDuty 相關的特定範例可在 `aws-samples`儲存庫的 GitHub 上取得。
- 有關 CfCT 的其他程式碼範例作為 儲存`aws-samples`庫中安全參考架構的一部分 AWS 提供。其中許多範例在名為 的目錄中包含範例`manifest.yaml`檔案`customizations_for_aws_control_tower`。

如需 AWS 安全參考架構的詳細資訊，請參閱 AWS 規範指引頁面。

AWS Control Tower (CfCT) 的自訂概觀

AWS Control Tower (CfCT) 的自訂可協助您自訂 AWS Control Tower 登陸區域，並保持符合 AWS 最佳實務。 CfCT 自訂是使用 AWS CloudFormation 範本和服務控制政策 (SCPs實作。

此 CfCT 功能與 AWS Control Tower 生命週期事件整合，因此您的資源部署會與您的登陸區域保持同步。例如，當透過帳戶工廠建立新帳戶時，連接至帳戶的所有資源都會自動部署。您可以將自訂範本和政策部署到組織中的個別帳戶和組織單位 (OUs)。

> **Note**
>
> 在 CfCT 中設定的目標組織單位 (OU) 必須在 AWS Control Tower 中啟用 AWSControlTowerBaseline。如需 AWSControlTowerBaseline 的詳細資訊，請參閱：在 OU 層級套用的基準類型。

下列影片說明部署可擴展 CfCT 管道和常見 CfCT 自訂的最佳實務。

下一節提供部署 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、設定和執行所需的 AWS 服務，以符合安全性和可用性的 AWS 最佳實務。

本主題適用於在 雲端中具有實際架構經驗的 AWS IT 基礎設施架構師和開發人員。

如需有關 AWS Control Tower (CfCT) 自訂的最新更新和變更的資訊，請參閱 GitHub 儲存庫中的 CHANGELOG.md 檔案。

架構概觀

部署 CfCT 會在 AWS 雲端中建置下列環境，並以 Amazon S3 儲存貯體做為組態來源。

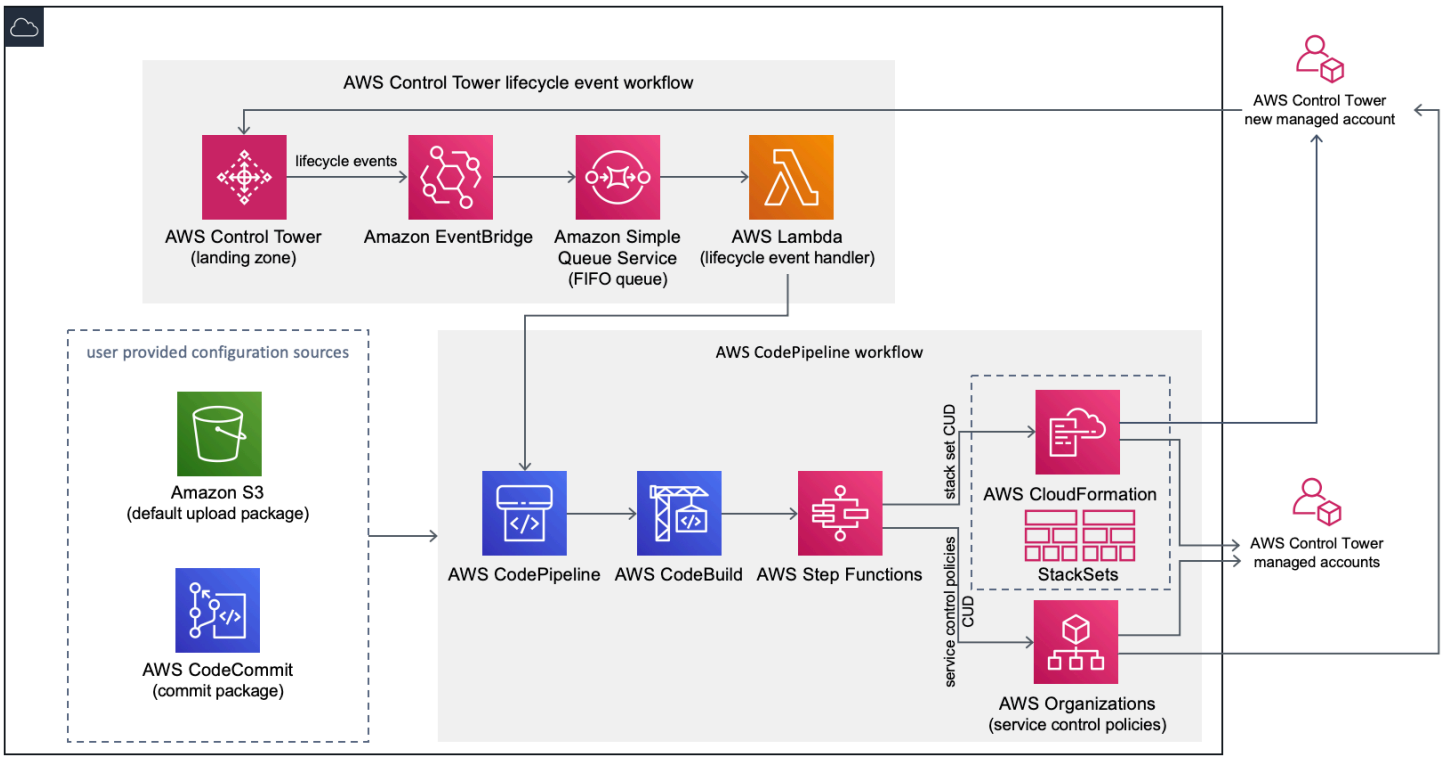

圖 1：AWS Control Tower 架構的自訂

CfCT 包含您在 AWS Control Tower 管理帳戶中部署的 AWS CloudFormation 範本。範本會啟動建置工作流程所需的所有元件，讓您可以自訂 AWS Control Tower 登陸區域。

> **注意**
>
> CfCT 必須部署在 AWS Control Tower 主區域和 AWS Control Tower 管理帳戶中，因為這是您的 AWS Control Tower 登陸區域部署的位置。如需設定 AWS Control Tower 登陸區域的資訊，請參閱 開始使用。

當您部署 CfCT 時，它會透過 Amazon Simple Storage Service (Amazon S3) 封裝自訂資源並將其上傳至程式碼管道來源。上傳程序會自動叫用服務控制政策 (SCPs) 狀態機器和 AWS CloudFormation StackSets 狀態機器，以在 OU 層級部署 SCPs，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。如果您有現有的 AWS CodeCommit 儲存庫，您可以將位置變更為 CodeCommit 儲存庫。如需詳細資訊，請參閱將 Amazon S3 設定為組態來源。

CfCT 部署兩個工作流程：

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

AWS CodePipeline 工作流程

AWS CodePipeline 工作流程會設定、 AWS CodePipelineAWS CodeBuild專案AWS Step Functions，以及協調組織中 AWS CloudFormation StackSets 和 SCPs的管理。

當您上傳組態套件時，CfCT 會叫用程式碼管道來執行三個階段。

- 組建階段 – 使用 AWS CodeBuild 驗證組態套件的內容。
- SCP 階段 – 叫用服務控制政策狀態機器，其會呼叫 AWS Organizations API 來建立 SCPs。
- CloudFormation 階段 – 調用堆疊集狀態機器來部署您在資訊清單檔案中提供的帳戶或 OUs 清單中指定的資源。

在每個階段，程式碼管道會叫用堆疊集和 SCP 步驟函數，將自訂堆疊集和 SCPs 部署到目標個別帳戶，或整個組織單位。

> **注意**
>
> 如需自訂組態套件的詳細資訊，請參閱 CfCT 自訂指南。

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，其中包含 Amazon EventBridge 事件規則、Amazon Simple Queue Service (Amazon SQS) 先進先出 (FIFO) 佇列和 AWS Lambda函數。

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

Cost

執行 CfCT 的成本取決於 AWS CodePipeline 執行次數、 AWS CodeBuild 執行持續時間、 AWS Lambda 函數數量和持續時間，以及發佈的 Amazon EventBridge 事件數量。例如，如果您在一個月內

使用 build.general1.small 執行 100 個組建，其中每個組建執行五分鐘，則執行 CfCT 的大約成本為每月 3.00 美元。如需完整詳細資訊，您可以檢閱執行中每個 AWS 服務的定價網頁。

Amazon Simple Storage Service (Amazon S3) 儲存貯體和 AWS CodeCommit Git 型儲存庫資源會在您刪除範本後保留，以保護組態資訊。根據您選取的選項，系統會根據存放在 Amazon S3 儲存貯體中的資料量和 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。

元件服務

下列 AWS 服務是適用於 AWS Control Tower (CfCT) 的 Customizations 元件。 CfCT

AWS CodeCommit

如果您有現有的 AWS CodeCommit 儲存庫，您可以將它設定為管道的來源，作為 Amazon S3 的替代方案。

根據您對 CloudFormation 範本的輸入，CfCT 可以建立具有相同範例組態的AWS CodeCommit儲存庫，如 Amazon Simple Storage Service 一節所述。

若要將 CfCT AWS CodeCommit 儲存庫複製到本機電腦，您必須建立可讓您暫時存取儲存庫的登入資料，如 AWS CodeCommit 使用者指南所述。如需版本相容性的相關資訊，請參閱設定 AWS CodeCommit。

> **Note**
>
> 如果您尚未使用 CodeCommit，唯一的選項是將 Amazon S3 儲存貯體設定為組態套件的儲存位置。如果您是第一次部署 CfCT，則無法使用 CodeCommit。

AWS CodePipeline

AWS CodePipeline 根據組態套件的更新來驗證、測試和實作變更，您將在預設 Amazon S3 儲存貯體或儲存 AWS CodeCommit 庫中進行這些更新。如需組態來源控制的詳細資訊，請參閱使用 Amazon S3 做為組態來源。管道包含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 AWS CloudFormation StackSets 的階段。如需管道階段的詳細資訊，請參閱 CfCT 自訂指南

AWS Key Management Service

CfCT 會建立 AWS Key Management Service(AWS KMS) `CustomControlTowerKMSKey`加密金鑰。此金鑰用於加密 AWS Systems Manager 參數存放區中 Amazon S3 組態儲存貯體、Amazon SQS 佇列和敏感參數中的物件。根據預設，只有由 CfCT 佈建的角色具有使用此金鑰執行加密或解密操作的許可。若要存取組態檔案、FIFO 佇列或參數存放區`SecureString`值，必須將管理員新增至`CustomControlTowerKMSKey`政策。預設會啟用自動金鑰輪換。

AWS Lambda

CfCT 會在 AWS Control Tower 生命週期事件的 AWS CloudFormation StackSets 或 AWS Organizations SCPs 初始安裝和部署期間，使用 AWS Lambda 函數來叫用安裝元件。

Amazon Simple Notification Service

CfCT 可能會在工作流程期間發佈通知，例如管道核准至 Amazon Simple Notification Service (Amazon SNS) 主題。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

部署 CfCT 時，CfCT 會建立具有唯一名稱的 Amazon Simple Storage Service (Amazon S3) 儲存貯體：

範例：Amazon S3 儲存貯體名稱

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

儲存貯體包含名為 的範例組態檔案 `_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，以自訂您的 AWS Control Tower 登陸區域。範例資訊清單會識別實作自訂時所需的堆疊集和服務控制政策 (SCPs) 所需的組態。

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，以自動觸發 CfCT 組態管道。

如需自訂組態檔案的資訊，請參閱 CfCT 自訂指南。

Amazon Simple Queue Service

CfCT 使用 Amazon Simple Queue Service (Amazon SQS) FIFO 佇列從 Amazon EventBridge 擷取生命週期事件。它會觸發 AWS Lambda 函數，叫 AWS CodePipeline 用 來部署 AWS CloudFormation StackSets 或 SCPs。如需 SCPs的詳細資訊，請參閱 AWS Organizations。

AWS Step Functions

CfCT 會建立 Step Functions 來協調自訂部署。這些 Step Functions 會轉譯組態檔案，以視需要跨環境部署自訂項目。

AWS Systems Manager 參數存放區

AWS Systems Manager 參數存放區會存放 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 參數存放區提供集中的位置，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 登陸區域的相同帳戶和區域中啟動 AWS Control Tower (CfCT) 的自訂；也就是說，您必須在 AWS Control Tower 主區域的 AWS Control Tower 管理帳戶中部署它。CfCT 根據預設，CfCT 透過在該帳戶和區域中設定組態管道來建立和執行登陸區域組態套件。

準備部署

當您準備 CloudFormation 範本進行初始部署時，有一些選項。您可以選擇組態來源，也可以允許手動核准管道部署。接下來的兩個章節會進一步說明這些選項。

選擇您的組態來源

根據預設，範本會建立 Amazon Simple Storage Service (Amazon S3) 儲存貯體，將範例組態套件儲存為名為 `.zip`的檔案`_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。如需有關更新組態套件的資訊，請參閱使用 Amazon S3 做為組態來源。

> **請記得移除底線**
>
> 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。當您完成自訂組態套件時，請務必上傳`custom-control-tower-configuration.zip`不含底線 (_) 的 ，以開始部署 AWS CodePipeline。

如果您有現有的 AWS CodeCommit Git 儲存庫，您可以將組態套件的儲存位置從 Amazon S3 儲存貯體變更為 AWS CodeCommit Git 儲存庫。若要這樣做，請在 CloudFormation 參數中選取`CodeCommit`選項。

> **是否要壓縮？**
>
> 當您使用預設 S3 儲存貯體時，請確定組態套件以`.zip`檔案形式提供。如果您使用的是 AWS CodeCommit 儲存庫，請務必將組態套件放在儲存庫中，而不壓縮檔案。如需在 中建立和存放組態套件的詳細資訊 AWS CodeCommit，請參閱 CfCT 自訂指南。

您可以使用範例組態套件來建立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至 Amazon S3 儲存貯體或儲存 AWS CodeCommit 庫。當您上傳組態檔案時，管道會自動開始。

選擇管道組態核准參數

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

啟用手動核准時，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，直到授予手動核准為止。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) 的自訂功能。 CfCT

您可以使用手動核准參數，透過拒絕第一次嘗試透過管道執行，來防止 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，做為實作前的最終控制項。

更新 AWS Control Tower 的自訂

如果您先前已部署 CfCT，則必須更新 CloudFormation 堆疊以取得 CfCT 架構的最新版本。如需詳細資訊，請參閱更新堆疊。

範本和原始程式碼

啟動 AWS CloudFormation 範本後，您的管理帳戶中會部署 AWS Control Tower (CfCT) 的自訂。您可以從 GitHub 下載範本，然後從 啟動範本AWS CloudFormation。

customizations-for-aws-control-tower.template 會部署下列項目：

- AWS CodeBuild 專案
- AWS CodePipeline 專案
- Amazon EventBridge 規則
- AWS Lambda 函數
- Amazon Simple Queue Service 佇列
- 具有範例組態套件的 Amazon Simple Storage Service 儲存貯體
- AWS Step Functions

> **Note**
> 您可以根據您的特定需求自訂範本。

原始程式碼儲存庫

您可以造訪我們的 GitHub 儲存庫，下載 CfCT 的範本和指令碼，並與他人共用您的登陸區域自訂。

自動化部署

啟動自動化部署之前，請檢閱考量事項。遵循本節中的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

先決條件

CfCT 必須部署在您的 AWS Control Tower 管理帳戶，以及您的 AWS Control Tower 主區域。如果您沒有設定登陸區域，請參閱 開始使用。

部署步驟

部署 CfCT 的程序包含兩個主要步驟。如需詳細說明，請點選各項步驟連結。

步驟 1. 啟動 堆疊

- 在您的管理帳戶中啟動 CloudFormation 範本。
- 檢閱範本參數，並視需要調整。

步驟 2. 建立自訂套件

- 建立自訂組態套件。

> **Important**
>
> 若要下載正確的 AWS CloudFormation 範本並啟動 CfCT，請遵循本節中提供的 GitHub 連結。請勿遵循先前指定之任何 S3 儲存貯體的舊連結。

步驟 1. 啟動 堆疊

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

> **注意**
>
> 您需負責支付執行 CfCT 時所使用的 AWS 服務成本。如需詳細資訊，請參閱Cost。

1. 若要啟動 AWS Control Tower 的自訂，請從 GitHub 下載範本，然後從 啟動範本AWS CloudFormation。
2. 根據預設，範本會在美國東部 （維吉尼亞北部） 區域啟動。若要在不同區域中啟動 CfCT AWS ，請使用主控台導覽列中的區域選擇器。

   > **Note**
   >
   > CfCT 必須在您部署 AWS Control Tower 登陸區域的相同區域和帳戶中啟動，這是您的主要區域。

3. 在建立堆疊頁面上，驗證 URL 文字方塊中顯示的範本 URL 是否正確，然後選擇下一步。
4. 在指定堆疊詳細資訊頁面上，為您的 CfCT 堆疊指派名稱。
5. 在參數下，檢閱下列參數，並視需要在範本中修改它們。

管道組態		
參數	預設	描述
管道核准階段	No	選擇是否要將管道組態從預設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 自訂指南”。
管道核准電子郵件地址	< 選用輸入 >	核准通知的電子郵件地址。若要使用此參數，您必須將管道核准階段參數設定為 Yes。
AWS CodePipeline 來源	Amazon S3	AWS CodePipeline 的來源，可協助您選取要存放和設定 CfCT 自訂的位置。
AWS CodeCommit 設定		
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 Source 參數設定為 AWS CodeCommit 。
CodeCommit 儲存庫名稱	custom-control-tower-configuration	如果您提供現有 Git 儲存庫的名稱，則必須將現有 CodeCommit Repository？參數設定為 ，Yes然後輸入該儲存庫的確切名稱。

AWS CodeCommit 設定		
參數	預設	描述
CodeCommit 分支名稱	`main`	存放自訂套件的 Git 分支。若要使用此參數，您必須將 CodePipeline Source 參數設定為 `AWS CodeCommit` 。
CloudFormation StackSets 組態		
參數	預設	描述
區域並行類型	`PARALLEL`	選取在 區域中部署 StackSets 操作的並行類型。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` 。
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。允許的值上限為 100。如需詳細資訊，請參閱堆疊集操作選項。
容錯率百分比	`10`	AWS CloudFormation 停止該區域的操作前，此堆疊操作在每個區域失敗的帳戶百分比。允許值下限為 0，允許值上限為 100。如需詳細資訊，請參閱堆疊集操作選項。

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) 资源的核取方塊。
9. 選擇 Create stack (建立堆疊) 以部署堆疊。

您可以在狀態欄的 CloudFormation 主控台中檢視堆疊的狀態。您應該會在大約 15 分鐘內看到 CREATE_COMPLETE 狀態。

步驟 2. 建立自訂套件

透過啟動的堆疊，您可以自訂包含的組態套件，將自訂新增至 AWS Control Tower 登陸區域和服務控制政策 (SCPs)。如需建立自訂套件的詳細說明，請參閱 CfCT 自訂指南。

> **注意**
>
> 管道不會在沒有上傳自訂組態套件的情況下執行。

更新堆疊

如果您先前已部署 AWS Control Tower (CfCT) 的自訂，請依照程序更新 CfCT 架構最新版本的 AWS CloudFormation 堆疊。 CfCT

> **Important**
>
> 您必須先將最新的範本從 GitHub 上傳至 Amazon Simple Storage Service (Amazon S3) 儲存貯體，才能完成下列程序。如需如何開始使用 Amazon S3 的說明，請參閱《Amazon Simple Storage Service 使用者指南》中的 Amazon S3 入門。

1. 登入 AWS CloudFormation 主控台。
2. 選取您現有的 AWS Control Tower (CfCT) CloudFormation 堆疊自訂，然後選取更新。 CfCT CloudFormation
3. 在先決條件 — 準備範本下，選取取代目前範本。
4. 在指定範本下，執行下列動作：
   a. 對於範本來源，選取取代目前範本。
   b. 針對 Amazon S3 URL，輸入您先前從 GitHub 上傳到 Amazon S3 之範本的範本 URL，然後選擇下一步。
   c. 驗證範本 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。請參閱步驟 1。如需參數的詳細資訊，請啟動 堆疊。

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. 在檢視 頁面上，檢視和確認的設定。請務必勾選確認範本可能會建立 AWS Identity and Access Management (IAM) 資源的核取方塊。
9. 選擇檢視變更集並驗證變更。
10. 選擇更新堆疊以部署堆疊。

    您可以在狀態欄的 AWS CloudFormation 主控台中檢視堆疊的狀態。您應該會在大約 15 分鐘內看到 UPDATE_COMPLETE 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，則可以刪除堆疊集。依預設，`enable_stack_set_deletion` 參數設為 `false`。在此組態中，從 CfCT 資訊清單檔案移除資源時，不會採取任何動作來刪除相關聯的堆疊集。

如果您將資訊清單檔案中的 `enable_stack_set_deletion` 值變更為 `true` ，當您從資訊清單檔案移除相關聯的資源時，CfCT 會刪除堆疊集及其所有資源。

資訊清單檔案的 v2 支援此功能。

> **Important**
>
> 當您最初將 的值設定為 `enable_stack_set_deletion` `true`時，下次叫用 CfCT 時，所有以字首 開頭`CustomControlTower-`、具有關聯索引鍵標籤 `Key:AWS_Solutions, Value: CustomControlTowerStackSet`且未在資訊清單檔案中宣告的資源都會暫存以供刪除。

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 設定為組態來源

當您設定 AWS Control Tower 的自訂時，它會將名為 `_custom-control-tower-configuration.zip` 檔案的初始組態檔案存放在名為 的 Amazon Simple Storage Service (Amazon S3) 儲存貯體中`custom-control-tower-configuration-`*`account-ID`*`-`*`region`*。

> **注意**
>
> 如果您選擇下載和修改此檔案，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。預設設定到位時，將檔案名稱中沒有底線字首的組態 zip 檔案上傳至 S3 儲存貯體時，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) 的保護，並拒絕使用 KMS 金鑰。若要存取 zip 檔案，您必須更新 KMS 金鑰政策，以指定應授予存取權的角色 （這些角色）。角色可以是管理員角色、使用者或兩者。請遵循下列程序：

1. 導覽至 AWS Key Management Service 主控台。
2. 在客戶受管金鑰中，選取 CustomControlTowerKMSKey。
3. 選取金鑰政策索引標籤。然後，選取編輯。
4. 在編輯金鑰政策頁面中，尋找程式碼中的允許使用金鑰區段，並新增下列其中一個許可：
   - 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 zip 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。如需自訂資訊清單和範本檔案的資訊，請參閱 the section called “CfCT 自訂指南”。
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. 使用主 AWS KMS 金鑰 SSE 將檔案上傳至 Amazon S3：`CustomControlTowerKMSKey`。

將 GitHub 設定為組態來源

本節說明如何使用 GitHub 做為來源來部署 AWS Control Tower (CfCT) 的自訂。程序有三個主要步驟：

- 準備 GitHub 儲存庫
- 建立 GitHub 程式碼連線
- 部署 CloudFormation 堆疊

準備 GitHub 儲存庫

在 GitHub 帳戶中建立儲存庫，範本中使用的預設名稱為 `custom-control-tower-configuration`。考慮將目標儲存庫設為私有。您將在 CfCT 儲存庫`manifest.yaml`的部署資料夾中名為 的`yaml`檔案中定義自訂項目。

CfCT 自訂指南提供有關建立 `manifest.yaml`以設定自訂的詳細指導。

建立 GitHub 對流

從適用於 Github 的開發人員工具 --Connections 執行個體中，執行下列步驟：

1. 選取建立連線，然後選擇 GitHub 做為提供者
2. 選擇建立 GitHub 應用程式連線，然後在連線名稱欄位中輸入 GitHub CfCT 或您選擇的任何名稱
3. 選取連線至 GitHub，然後選擇安裝新的應用程式
4. 為您的儲存庫選取 GitHub 使用者或組織
5. 在儲存庫存取下，選擇僅選取儲存庫，然後選取您先前建立的儲存庫，然後儲存您的工作。
6. 請注意程式碼連線 ARN - 部署 CloudFormation 堆疊時需要它。

部署 CloudFormation 堆疊

- 從儲存庫下載 `custom-control-tower-initiation.template` 檔案。
- 使用 `custom-control-tower-initiation.template` 檔案建立新的 CloudFormation 堆疊。
- 在 AWS CodePipeline Source 下，選擇 GitHub （透過 Code Connection)。
- 在 GitHub 設定下，指定下列欄位：
  - 對於程式碼連線的 ARN，請提供程式碼連線 ARN
  - 對於 GitHub 使用者或組織，請提供您建立儲存庫的 GitHub 使用者或組織的名稱
  - 針對 GitHub 儲存庫名稱，輸入儲存庫名稱 （預設為 `custom-control-tower-configuration`)
  - 對於 GitHub 分支名稱，輸入分支名稱 （預設為 `main`)

操作指標的集合

AWS Control Tower (CfCT) 的自訂包含傳送匿名操作指標的選項 AWS。 AWS 使用此資料來了解客戶如何使用 CfCT，以及其他相關的服務和產品。 CfCT 啟用資料收集時，會將下列資訊傳送至 AWS：

- 解決方案 ID： AWS 解決方案識別符
- 唯一 ID (UUID)：每次部署隨機產生的唯一識別符
- 時間戳記：資料收集時間戳記
- 狀態機器執行計數：遞增計數此狀態機器執行的次數
- 資訊清單版本：組態中使用的資訊清單版本

> **Note**
>
> AWS 擁有其收集的資料。資料收集受 AWS 隱私權政策約束。

若要選擇不傳送匿名操作指標給 AWS，請完成下列其中一個任務：

- 更新 AWS CloudFormation 範本映射區段，如下所示：

  從

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

  至

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

- 部署 CfCT 之後，請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 自訂指南

AWS Control Tower (CfCT) 的自訂指南適用於管理員、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，他們想要為其公司和客戶自訂和擴展其 AWS Control Tower 環境。 CfCT 它提供使用 CfCT 自訂套件自訂和擴展 AWS Control Tower 環境的相關資訊。

> **Note**
>
> 若要部署和設定 (CfCT)，您必須透過 部署和處理組態套件 AWS CodePipeline。下列各節會詳細說明程序。

程式碼管道概觀

組態套件需要 Amazon Simple Storage Service (Amazon S3) 和 AWS CodePipeline。組態套件包含下列項目：

- 資訊清單檔案
- 隨附的範本集
- 用於描述和實作 AWS Control Tower 環境自訂的其他 JSON 檔案

根據預設，`_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：

`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。大多數客戶都會保留此預設值。如果您有現有的 AWS CodeCommit 儲存庫，您可以將來源位置變更為儲存 AWS CodeCommit 庫。如需詳細資訊，請參閱AWS CodePipeline 《 使用者指南》中的在 CodePipeline 中編輯管道。

資訊清單檔案是一種文字檔案，描述您可以部署以自訂登陸區域 AWS 的資源。CodePipeline 會執行這些任務：

- 會擷取資訊清單檔案、隨附的範本集，以及其他 JSON 檔案
- 執行資訊清單和範本驗證
- 調用 CfCT 資訊清單檔案中的區段，以執行特定的管道階段。

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

> **記住底線**
>
> 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。當您完成組態套件的自訂時，請上傳`custom-control-tower-configuration.zip`不含底線 (_) 的檔案，以觸發其中的部署 AWS CodePipeline。

AWS CodePipeline 階段

CfCT 管道需要多個 AWS CodePipeline 階段來實作和更新 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道階段。的來源 AWS CodePipeline 可以是 Amazon S3 儲存貯體或可託管組態套件的 AWS CodeCommit 儲存庫。

2. 建置階段

   建置階段需要 AWS CodeBuild 驗證組態套件的內容。這些檢查包括使用 和 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 CloudFormation 範本 CloudFormation `validate-template`。`cfn_nag`如果資訊清單檔案和 CloudFormation 範本通過測試，管道會繼續進入下一個階段。如果測試失敗，您可以檢閱 CodeBuild 日誌以識別問題，並視需要編輯組態來源檔案。

3. 手動核准階段 （選用）

   手動核准階段是選用的。如果您啟用此階段，它會提供額外的組態管道控制。它會在部署期間暫停管道，直到獲得核准為止。您可以在啟動堆疊時，將管道核准階段參數編輯為是，以選擇加入手動核准。

4. 政策階段

   政策階段會呼叫服務控制政策 (SCP) 或資源控制政策 (RCP) 狀態機器，以呼叫建立 SCPs AWS Organizations APIs。 RCPs

5. CloudFormation 資源階段

   CloudFormation 資源階段會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組織單位 (OUs) 清單中指定的資源。狀態機器會依資訊清單檔案中指定的順序建立 CloudFormation 資源。若要指定資源相依性，請排列清單檔案中指定資源的順序。資訊清單檔案中的資源順序是指定相依性的唯一方法。

定義自訂組態

您將使用 CfCT 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。您可以將這些檔案封裝成資料夾結構，並將其放在 Amazon S3 儲存貯體中做為`.zip`檔案，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 或 AWS CodeCommit 儲存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為`custom-control-tower-configuration.zip`檔案，然後僅將`.zip`檔案上傳至指定的 Amazon S3 儲存貯體。

> **Note**
>
> 如果您使用的是 AWS CodeCommit，請將檔案放在儲存庫中，而不壓縮檔案。

CfCT 資訊清單檔案

CfCT `manifest.yaml` 檔案是描述 AWS 資源的文字檔案。下列範例顯示 CfCT 資訊清單檔案的結構。

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

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

如先前程式碼範例所示，資訊清單檔案的前兩行會指定區域值和版本關鍵字。以下是這些關鍵字的定義。

region – 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`)。建立自訂 AWS Control Tower 資源 （例如 CloudFormation StackSets) 時，除非指定更特定於資源的區域，否則 AWS Control Tower 主區域為預設值。

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

版本 – 資訊清單結構描述版本編號。最新的支援版本為 2021-03-15。

```
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 CfCT 資訊清單的版本升級。

上一個範例中顯示的下一個關鍵字是資源關鍵字。資訊清單檔案的資源區段具有高度結構化。它包含 AWS 資源的詳細清單，由 CfCT 管道自動部署。資源及其可用參數的這些描述會在下一節中提供。

CfCT 資訊清單檔案的資源區段

本主題說明 CfCT 資訊清單檔案的資源區段，您可以在其中定義自訂所需的資源。CfCT 資訊清單檔案的這個區段從關鍵字資源開始，並繼續到檔案的結尾。

資訊清單檔案的資源區段指定 CloudFormation StackSets、 AWS Organizations SCPs和 RCPs，CfCT 會透過程式碼管道自動部署。您可以列出要部署堆疊執行個體OUs、帳戶和區域。

堆疊執行個體部署在帳戶層級，而不是 OU 層級。SCPs和 RCPs會部署在 OU 層級。如需詳細資訊，請參閱建置您自己的自訂。

下列範例範本說明資訊清單檔案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 | rcp
    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]
```

本主題的其餘部分提供先前程式碼範例中所示關鍵字的詳細定義。

name – 與 CloudFormation StackSets 相關聯的名稱。
您提供的字串會為堆疊集指派更易於使用的名稱。

- 類型：字串
- 必要：是
- 有效值：a-z、A-Z、0-9 和連字號 (-)。名稱必須以字母字元開頭。

description – 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、指向 JSON 中 CloudFormation 範本 AWS Organizations 或服務控制政策的 Amazon S3 URI 或 URL，以建立 CloudFormation 資源、SCPs 或 RCPs。

- 類型：字串
- 必要：是

1. 下列範例顯示 `resource_file`，做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. 下列範例顯示指定為 Amazon S3 URI 的資源檔案

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

3. 下列範例顯示以 Amazon S3 HTTPS URL 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允許從中部署 CfCT 之 AWS Control Tower 管理帳戶的讀取存取權。如果您提供 Amazon S3 HTTPS URL，請確認路徑使用點表示法。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. 下列範例顯示儲存資源的 Amazon S3 儲存貯體政策和 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 Simple Storage Service 使用者指南》中的儲存貯體政策範例。

參數 – 指定 CloudFormation 參數的名稱和值。

- 類型：MapList
- 必要：否

參數區段包含金鑰/值參數對。下列虛擬範本概述參數區段。

```
parameters:
```

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

- parameter_key – 與 參數相關聯的金鑰。
  - 類型：字串
  - 必要：是（在參數屬性下）
  - 有效值：a-z、A-Z 和 0-9
- parameter_value – 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 `stack_set`選項透過 CloudFormation StackSets 部署資源、部署 SCPs 時為 `scp`選項，或者部署 RCPs 時為 `rcp`選項。

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

deployment_targets – 帳戶或組織單位 OUs) 的清單，CfCT 會將 CloudFormation 資源部署到其中，指定為帳戶或 organization_units。

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

- 類型：字串清單 `account number` `account name`或 表示此資源將部署到指定的帳戶清單中，或 `0U names` 表示此資源將部署到指定的 OU 清單中。
- 必要：至少一個帳戶或 organization_units
  - 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戶清單中。
  - organization_units：

類型：字串清單，0U names指出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。根據預設，CfCT 不支援將堆疊執行個體部署到組織的管理帳戶中。如果您有特殊使用案例，請參閱根 OU。

export_outputs – 表示 SSM 參數索引鍵的名稱/值對清單。這些 SSM 參數金鑰可讓您將範本輸出儲存到 SSM 參數存放區。輸出旨在供資訊清單檔案中稍早定義的其他資源參考。

```
export_outputs: # List of SSM parameters
  - name: [String]
    value: [String]
```

- 類型：名稱和值金鑰對的清單。名稱包含 SSM 參數存放區索引鍵的name字串，而值包含參數的value字串。
- 有效值：*CfnOutput-Logical-ID* 對應至範本輸出$[output_*CfnOutput-Logical-ID*]變數的任何字串或變數。如需 CloudFormation 範本中輸出區段的詳細資訊，請參閱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輸出變數存放到名為 的 SSM 參數金鑰/org/member/audit/vpc_id。

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

> **Note**
>
> export_outputs 金鑰名稱可能包含 以外的值output。例如，如果名稱為 /org/environment-name，則值可能是 production。

區域 – CfCT 將在其中部署 CloudFormation 堆疊執行個體的區域清單。

- 類型： AWS 商業區域名稱的任何清單，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要區域中。
- 必要：否

根 OU

CfCT 支援清單檔案 V2 版本) `organizational_units` 下組織單位 (OU) 的根值。 V2 (2021-03-15

- 如果您選擇 `scp`或 的部署方法`rcp`，當您在 下新增根時`organizational_units`，AWS Control Tower 會將政策套用至根下的所有 OUs。如果您選擇 的部署方法`stack_set`，當您在 下新增根時`organizational_units`，CfCT 會在在 AWS Control Tower 中註冊的根帳戶下的所有帳戶中部署堆疊集，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用於計費目的。請勿在 AWS Control Tower 管理帳戶中執行生產工作負載。

  根據最佳實務指引，AWS Control Tower 部署會將管理帳戶放在根 OU 下，使其具有完整存取權，且不會執行其他資源。因此，AWSControlTowerExecution 角色不會部署到管理帳戶。
- 我們建議您遵循管理帳戶的這些最佳實務。如果您有特定的使用案例，要求您在管理帳戶中部署堆疊集，請包含帳戶做為部署目標，並指定管理帳戶。否則，請勿將帳戶納入部署目標。您必須在管理帳戶中建立缺少的資源，包括必要的 IAM 角色。

若要在管理帳戶中部署堆疊集，請將 納入`accounts`為部署目標，並指定管理帳戶。否則，請勿將帳戶納入部署目標。

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

resources:

  …truncated…

    deployment_targets:
      organizational_units:
        - Root
```

> **Note**
>
> 根 OU 功能僅支援資訊清單檔案 (2021-03-15 的 V2 版本）。如果您在 下將根新增為 OUorganizational_units，請勿新增任何其他 OUs。

巢狀 OU

CfCT 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 OUs)。

巢狀 OU 需要完整的路徑 （根除外），使用冒號做為 OUs 之間的分隔符號。對於部署方法scp或 rcp，AWS Control Tower 會將 SCPs 或 RCPs 部署到巢狀 OU 路徑中的最後一個 OU。對於部署方法 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，請考慮路徑 OUName1:OUName2:OUName3。路徑中的最後一個 OU 為 OUName3。CfCT 只會將 SCPs 或 RCPs 部署至 OUName3，OUName3並將堆疊集直接部署至 下的所有帳戶。

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

resources:

  …truncated…

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

> **Note**
>
> 巢狀 OU 功能僅支援資訊清單檔案 (2021-03-15 的 V2 版本）。

建置您自己的自訂項目

若要建置自己的自訂，您可以透過新增或更新服務控制政策 (SCPs)、資源控制政策 (RCPs) CloudFormation 和資源來修改 CfCT manifest.yaml 檔案。對於必須部署的資源，您可以新

增或移除帳戶和 OUs。您可以在套件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。

本節說明建置自訂項目的兩個主要部分：

- 如何為服務控制政策設定自己的組態套件
- 如何為 AWS CloudFormation 堆疊集設定自己的組態套件

設定 SCPs或 RCPs 的組態套件

本節說明如何建立服務控制政策 SCPs) 或資源控制政策 (RCPs組態套件。此程序的兩個主要部分是 (1) 準備 CfCT 資訊清單檔案，以及 (2) 準備您的資料夾結構。

步驟 1：編輯 manifest.yaml 檔案

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。

下列程式碼片段顯示預設資訊清單檔案。

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

resources: []
```

部署期間會自動`region`新增 的值。它必須符合您部署 CfCT 的區域。此區域必須與 AWS Control Tower 區域相同。

若要在存放在 Amazon S3 儲存貯體之 zip 套件的 `example-configuration` 資料夾中新增自訂 SCP 或 RCP，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 | rcp
```

```
    #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。您可以在單一變更中新增多個政策。

```
---
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 | rcp
    #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

如果您使用資源檔案的 Amazon S3 URL，以及搭配金鑰/值對使用參數，則可以略過此步驟。

您必須包含 JSON 格式的 SCP 政策或 RCP 政策以支援資訊清單，因為資訊清單檔案參考 JSON 檔案。確定檔案路徑符合資訊清單檔案中提供的路徑資訊。

- 政策 JSON 檔案包含要部署到 OUs SCPs 或 RCPs。

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`政策檔案的範例。

JSON

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

設定 CloudFormation StackSets 的組態套件

本節說明如何設定 CloudFormation StackSets 的組態套件。此程序的兩個主要部分是：(1) 準備資訊清單檔案，以及 (2) 更新資料夾結構。

步驟 1：編輯現有的資訊清單檔案

將新的 CloudFormation StackSets 資訊新增至您先前編輯的資訊清單檔案。

僅供檢閱，下列程式碼片段包含先前顯示的相同自訂資訊清單檔案，用於設定 SCPs或 RCPs 的組態套件。現在您可以進一步編輯此檔案，以包含 資源的詳細資訊。

```
---
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 | rcp
    #Apply to the following OU(s)
    deployment_targets:
    organizational_units: #array of strings
    - OUName1
    - OUName2
```

下列程式碼片段顯示已編輯的範例資訊清單檔案，其中包含resources詳細資訊。的順序會resources決定建立resources相依性的執行順序。您可以根據您的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 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 | rcp
    #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：更新資料夾結構

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 CloudFormation 範本檔案和 SCP 或 RCP 政策檔案。確認檔案路徑符合資訊清單檔案中提供的路徑。

- 範本檔案包含要在 OUs 和帳戶中部署 AWS 的資源。
- 政策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
```

「fred」協助程式和 CloudFormation 參數檔案

CfCT 為您提供稱為預製協助程式的機制，以取得 CloudFormation 範本中定義的 SSM 參數存放區金鑰值。使用預製協助程式，您可以使用存放在 SSM 參數存放區中的值，無需更新 CloudFormation 範本。如需詳細資訊，請參閱CloudFormation 《 使用者指南》中的什麼是 CloudFormation 範本？。

> **Important**
>
> 預製協助程式有兩個限制。參數僅適用於 AWS Control Tower 管理帳戶的主區域。最佳實務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 'alfred' 協助程式擷取參數時，會從匯出變數的堆疊集選擇隨機堆疊執行個體。

範例

假設您有兩個 CloudFormation 堆疊集。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，且 `VPC ID`和 `subnet ID` 必須傳遞至堆疊集 2 做為參數值。在將 `VPC ID`和 `subnet ID` 傳遞至堆疊集 2 之前，`subnet ID`必須使用 將 `VPC ID`和存放在堆疊集 1 中`AWS:::SSM::Parameter`。如需詳細資訊，請參閱《CloudFormation 使用者指南》中的 `AWS:::SSM::Parameter`。

CloudFormation 堆疊集 1：

在下列程式碼片段中，原始協助程式可以從參數存放區取得 `VPC ID`和 的值`subnet ID`，並將其做為輸入傳遞至 StackSet 狀態機器。

```
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
```

CloudFormation 堆疊集 2：

程式碼片段顯示 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]
```

CloudFormation 堆疊集 2.1：

程式碼片段顯示您可以列出`alfred_ssm`屬性，以支援 CommaDelimitedList 類型的參數。如需詳細資訊，請參閱《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 結構描述

CfCT 自訂套件的 JSON 結構描述位於 GitHub 的原始程式碼儲存庫中。您可以搭配許多您最愛的開發工具使用結構描述，而且您可能會發現在建置自己的 CfCT `manifest.yaml` 檔案時減少錯誤很有幫助。

CfCT 資訊清單的版本升級

如需 AWS Control Tower (CfCT) 最新版本自訂的相關資訊，請參閱 GitHub 儲存庫中的 CHANGELOG.md 檔案。 CfCT

> **Warning**
>
> AWS Control Tower (CfCT) 自訂的 2.2.0 版引入了 CfCT 資訊清單結構描述 (2021-03-15 版），以與相關 AWS 服務 APIs保持一致。 CfCT 資訊清單結構描述允許單一 manifest.yaml 檔案透過解耦的 DevOps 工作流程管理支援的資源 (CloudFormation 範本、SCPs 和 RCPs)。強烈建議您將 CfCT 資訊清單結構描述從 2020-01-01 版更新為 2021-03-15 版或更新版本。CfCT 繼續支援 `manifest.yaml` 檔案的 2021-03-15 和 2020-01-01 版。您現有的組態不需要變更。不過，2020-01-01 版已終止支援。我們不再提供更新或新增增強功能至 2020-01-01 版。2020-01-01 版不支援根 OU 和巢狀 OU 功能。

CfCT 資訊清單版本 2021-03-15 中的已棄用屬性：

```
organization_policies
policy_file
apply_to_accounts_in_ou

cloudformation_resources
template_file
deploy_to_account
deploy_to_ou
ssm_parameters
```

強制性 CfCT 升級步驟

當您升級至 CfCT 資訊清單結構描述 2021-03-15 版時，您必須進行下列變更，才能更新檔案。下一節概述轉換的必要和建議變更。

Organizations 政策

1. 在新屬性資源下移動 organization_policies 下的 SCPs RCPs。
2. 將 policy_file 屬性變更為新的 屬性 resource_file。
3. 將 apply_to_accounts_in_ou 變更為新的屬性 deployment_targets。OU 清單應在 sub-property organization_units 下定義。組織政策不支援帳戶子屬性。

4. 使用值 scp 或 rcp 新增屬性 deploy_method。

CloudFormation 資源

1. 在新屬性資源下，將 CloudFormation 資源移至 cloudformation_resources 下。
2. 將 template_file 屬性變更為新的 屬性 resource_file。
3. 將 deploy_to_ou 變更為新的屬性 deployment_targets。OU 清單應在 sub-property organization_units 下定義。
4. 將 deploy_to_accounts 變更為新的屬性 deployment_targets。帳戶清單應在子屬性帳戶下定義。
5. 將 ssm_parameters 屬性變更為新的 屬性 export_outputs。

強烈建議的 CfCT 升級步驟

CloudFormation 參數

1. 將 parameter_file 屬性變更為新的屬性參數。
2. 移除 parameter_file 屬性值中的檔案路徑。
3. 將參數索引鍵和參數值從現有參數 JSON 檔案複製到參數屬性的新格式。這可協助您在資訊清單檔案中管理它們。

> **Note**
>
> CfCT 資訊清單版本 2021-03-15 支援 parameter_file 屬性。

AWS Control Tower 中的聯網

AWS Control Tower 提供透過 VPCs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 VPCs和 AWS Control Tower 的詳細資訊，請參閱建置可擴展且安全的多 VPC AWS 網路基礎設施。

AWS Control Tower 透過雙堆疊 IP 地址支援 IPv4 和 IPv6 通訊協定。如需詳細資訊，請參閱 AWS Control Catalog 端點和配額，以及 AWS Control Tower 端點和配額。

相關主題

- 如需有關當您註冊具有現有 VPCs 的帳戶時 AWS Control Tower 如何運作的資訊，請參閱 使用 VPCs 註冊現有帳戶。
- 透過 Account Factory，您可以佈建包含 AWS Control Tower VPC 的帳戶，也可以在沒有 VPC 的情況下佈建帳戶。如需如何刪除 AWS Control Tower VPC 或設定不含 VPC 的 AWS Control Tower 帳戶的詳細資訊，請參閱 逐步解說：設定沒有 VPC 的 AWS Control Tower。
- 如需有關如何變更 VPCs 帳戶設定的資訊，請參閱更新帳戶的帳戶工廠文件。
- 如需在 AWS Control Tower 中使用聯網和 VPCs 的詳細資訊，請參閱本使用者指南相關資訊頁面上的聯網一節。

AWS Control Tower 中的 VPCs 和 AWS 區域

作為帳戶建立的標準部分， 會在每個區域中 AWS 建立 AWS預設 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，但非受管區域中 AWS 的預設 VPC 可供 IAM 使用者存取。

管理員可以啟用區域拒絕控制，因此您的最終使用者沒有許可，無法連線到 AWS Control Tower 支援但受管區域以外的區域中的 VPC。若要設定區域拒絕控制項，請前往登陸區域設定頁面，然後選取修改設定。

區域拒絕控制會封鎖對非受管 中大多數 服務的 API 呼叫 AWS 區域。如需詳細資訊，請參閱AWS 根據請求拒絕對 的存取 AWS 區域。

> **Note**
>
> 區域拒絕控制可能不會阻止 IAM 使用者連線到 AWS 不支援 AWS Control Tower 的區域中的預設 VPC。

或者，您可以移除非受管區域中 AWS 的預設 VPCs。若要列出區域中的預設 VPC，您可以使用類似此範例的 CLI 命令：

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

AWS Control Tower 和 VPCs概觀

以下是有關 AWS Control Tower VPCs的一些基本事實：

- 當您在帳戶工廠中佈建帳戶時，AWS Control Tower 建立的 VPC 與 AWS 預設 VPC 不同。
- 當 AWS Control Tower 在支援 AWS 的區域設定新帳戶時，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 帳戶都可以有一個由 AWS Control Tower 建立的 VPC。帳戶可以在帳戶限制內擁有額外的 AWS VPCs。
- 每個 AWS Control Tower VPC 在所有區域中都有三個可用區域，美國西部（加利佛尼亞北部）區域除外`us-west-1`，以及 中的兩個可用區域`us-west-1`。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 預設包含九個子網路，分為三個可用區域。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等的唯一範圍。
- 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 內的六個或九個子網路可以不受限制的方式互相通訊。

使用 VPCs 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

如果您設定帳戶工廠 VPC 組態，以便在佈建新帳戶時啟用公有子網路，帳戶工廠會將 VPC 設定為建立 NAT 閘道。Amazon VPC 將向您收取您的使用費用。

VPC 和控制設定

如果您在啟用 VPC 網際網路存取設定的情況下佈建 Account Factory 帳戶，該 Account Factory 設定會覆寫控制項 不允許客戶管理之 Amazon VPC 執行個體的網際網路存取。若要避免啟用新佈建帳戶的網際網路存取，您必須在 Account Factory 中變更 設定。如需詳細資訊，請參閱逐步解說：不使用 VPC 設定 AWS Control Tower。

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您的 AWS Control Tower 組織選取整體 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 區塊高達 ，範圍/16為：

- `10.0.0.0/8`
- `172.16.0.0/12`
- `192.168.0.0/16`
- `100.64.0.0/10`（只有當您的網際網路供應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，它會針對您在組織單位 (OU) 內建立的每個帳戶，將相同的 CIDR 範圍指派給每個 VPC。由於 IP 地址的預設重疊，此實作最初不允許在 OU 中的任何 AWS Control Tower VPCs 之間對等互連。

子網路

在每個 VPC 中，AWS Control Tower 會將您指定的 CIDR 範圍平均分成九個子網路（美國西部（加利佛尼亞北部）除外，其中六個子網路）。VPC 內沒有任何子網路重疊。因此，它們都可以在 VPC 中互相通訊。

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 在 AWS Control Tower 中設定安全群組。

對等互連

AWS Control Tower 不會限制多個 VPC-to-VPC VPCs對等互連。不過，根據預設，所有 AWS Control Tower VPCs都有相同的預設 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 地址不會重疊。

如果您在 Account Factory 的設定中變更 CIDR 範圍，則後續由 AWS Control Tower 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。

使用介面端點存取 AWS Control Tower (AWS PrivateLink)

您可以使用 在 VPC 和 AWS Control Tower 之間 AWS PrivateLink 建立私有連線。您可以像在 VPC 中一樣存取 AWS Control Tower，無需使用網際網路閘道、NAT 裝置、VPN 連接或 Direct Connect 連線。VPC 中的執行個體不需要公有 IP 地址即可存取 AWS Control Tower。

您可以建立由 AWS PrivateLink提供支援的介面端點來建立此私有連線。我們會在您為介面端點啟用的每個子網中建立端點網路介面。這些是請求者管理的網路介面，可做為目的地為 AWS Control Tower 之流量的進入點。

如需詳細資訊，請參閱《AWS PrivateLink 指南》中的AWS 服務 透過 存取 AWS PrivateLink 。

AWS Control Tower 的考量事項

在您設定 AWS Control Tower 的介面端點之前，請檢閱 AWS PrivateLink 指南中的考量事項。

AWS Control Tower 支援透過介面端點呼叫其所有 API 動作。

建立 AWS Control Tower 的介面端點

您可以使用 Amazon VPC 主控台或 AWS Command Line Interface () 為 AWS Control Tower 建立介面端點AWS CLI。如需詳細資訊，請參閱《AWS PrivateLink 指南》中的「建立介面端點」。

使用下列服務名稱建立 AWS Control Tower 的介面端點：

```
com.amazonaws.region.controltower
com.amazonaws.region.controltower-fips
```

如果您為介面端點啟用私有 DNS，您可以使用其預設的區域 DNS 名稱向 AWS Control Tower 提出 API 請求。例如 `controltower.us-east-1.amazonaws.com`。

為您的介面端點建立端點政策

端點政策為 IAM 資源，您可將其連接至介面端點。預設端點政策允許透過介面端點完整存取 AWS Control Tower。若要控制允許從您的 VPC 存取 AWS Control Tower，請將自訂端點政策連接至介面端點。

端點政策會指定以下資訊：

- 可執行動作 (AWS 帳戶、IAM 使用者和 IAM 角色) 的主體。
- 可執行的動作。
- 可供執行動作的資源。

如需詳細資訊，請參閱《AWS PrivateLink 指南》中的「使用端點政策控制對服務的存取」。

範例：AWS Control Tower 動作的 VPC 端點政策

以下是自訂端點政策的範例。當您將此政策連接到介面端點時，它會授予所有資源上所有主體的所列 AWS Control Tower 動作的存取權。

```
{
```

```
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "controltower:ListEnabledControls",
            "controltower:ListLandingZones"
         ],
         "Resource":"*"
      }
   ]
}
```

> **Note**
>
> 如需 AWS Control Tower API 操作的完整清單，請參閱 AWS Control Tower API 參考。

必要的角色和許可

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

如需角色的一般資訊，請參閱使用者群組、角色和許可集。

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 Identity Center 群組。
- 如需佈建帳戶所需的許可資訊，請參閱帳戶所需的許可。
- 如需 AWS Control Tower 所需的主控台許可資訊，請參閱使用 AWS Control Tower 主控台所需的許可。

關於角色

- 如需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 稽核帳戶的程式設計角色和信任關係。
- 如需有關 AWS Control Tower 用來管理帳戶的其他角色的資訊，請參閱使用 AWS Control Tower 的身分型政策 (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 AWS Config 資訊的角色資訊，請參閱 AWS Control Tower 如何在未受管OUs 和帳戶中彙總 AWS Config 規則。
- 如需有關如何在指派角色和許可時保護 資源的資訊，請參閱角色信任關係的選用條件、選擇性設定 AWS KMS 金鑰，以及防止跨服務模擬。
- 如需使用 IAM 角色在 AWS Control Tower 中自動佈建帳戶的特定資訊，請參閱使用 IAM 角色自動佈建帳戶。
- 若要檢視保護 AWS Config SNS 主題的政策，請參閱 AWS Config SNS 主題政策。

AWS Control Tower 如何與角色搭配使用來建立和管理帳戶

一般而言，角色是 中身分和存取管理 (IAM) 的一部分 AWS。如需 IAM 和 中角色的一般資訊 AWS，請參閱《IAM AWS 使用者指南》中的 IAM 角色主題。

角色和帳戶建立

AWS Control Tower 會透過呼叫 的 `CreateAccount` API 來建立客戶的帳戶 AWS Organizations。當 AWS Organizations 建立此帳戶時，它會在該帳戶中建立角色，透過將參數傳遞至 API 來讓 AWS Control Tower 命名。角色的名稱是 `AWSControlTowerExecution`。

AWS Control Tower 接管 Account Factory 建立的所有帳戶`AWSControlTowerExecution`的角色。使用此角色時，AWS Control Tower 會為帳戶建立基準，並套用強制性 （ 和任何其他啟用的 ） 控制項，這會導致建立其他角色。這些角色會由其他服務使用，例如 AWS Config。

> **Note**
>
> 若要基準化帳戶，請設定其資源，其中包含 Account Factory 範本，有時稱為藍圖和控制項。基本程序也會在 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已註冊帳戶的角色中。

如需帳戶和資源的詳細資訊，請參閱 關於 AWS Control Tower AWS 帳戶 中的。

AWSControlTowerExecution 角色說明

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您的 Audit and Log Archive 帳戶。

角色`AWSControlTowerExecution`可以透過多種方式新增至 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 Tower 主控台建立的帳戶工廠帳戶，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 中註冊帳戶。
- 將控管延伸至 OU 時，AWS Control Tower 會使用 StackSet-AWSControlTowerExecutionRole 在該 OU 中的所有帳戶中建立角色。

> **Note**
>
> 當您取消註冊帳戶時，無論角色是手動建立還是由 AWS Control Tower 本身建立，AWS Control Tower 都會移除該AWSControlTowerExecution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 手動將必要的 IAM 角色新增至現有 AWS 帳戶 並註冊。

AWSControlTowerExecution 角色如何與 OUs 搭配使用：

此AWSControlTowerExecution角色可確保您選擇的 AWS Control Tower 控制項會自動套用至組織中每個 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。因此：

- 您可以根據 AWS Control Tower 控制項所體現的稽核和記錄功能，更輕鬆地提供合規和安全性報告。
- 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。

如需偏離的詳細資訊，請參閱在 AWS Control Tower 中偵測和解決偏離。

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，安全性或通訊協定的違規不太可能發生。

角色信任關係的選用條件

若要為 AWS Control Tower 環境新增額外的安全層，您可以在角色信任政策中強加條件，以限制與 AWS Control Tower 中特定角色互動的帳戶和資源。例如，您可以進一步限制對AWSControlTowerAdmin角色的存取，因為它允許廣泛的存取許可。

為了協助防止威脅行為者存取您的資源，請手動編輯您的 AWS Control Tower 信任政策，將至少一個aws:SourceArn或aws:SourceAccount條件式新增至政策陳述式。作為額外的安全最佳實務，您可

以新增 aws:SourceArn條件，因為它比 更具體aws:SourceAccount，限制對特定帳戶和特定資源的存取。

如果您不知道資源的完整 ARN，或如果您指定多個資源，則可以針對 ARN 的未知部分使用具有萬用字元 (*) aws:SourceArn的條件。例如，如果您不想指定區域，arn:aws:controltower:*:123456789012:*就會運作。

下列範例示範搭配 IAM aws:SourceArn 角色信任政策使用 IAM 條件。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 格式如下：arn:aws:controltower:*${HOME_REGION}*:*${CUSTOMER_AWSACCOUNT_id}*:*

將字串 ${HOME_REGION}和 取代${CUSTOMER_AWSACCOUNT_id}為您自己的主區域和呼叫帳戶的帳戶 ID。

JSON

```
{
  "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sts:AssumeRole動作的 ARN。換句話說，只有可在 012345678901us-west-2區域中

登入帳戶 ID 的使用者，才能執行需要此特定角色的動作，以及指定為 的 AWS Control Tower 服務的信任關係`controltower.amazonaws.com`。

下一個範例顯示套用至角色信任政策的 `aws:SourceAccount`和 `aws:SourceArn`條件。

JSON

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

此範例說明 `aws:SourceArn`條件陳述式，以及新增`aws:SourceAccount`的條件陳述式。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 管理對 資源的存取。

建議：

我們建議您將條件新增至 AWS Control Tower 建立的角色，因為這些角色直接由其他 AWS 服務擔任。如需詳細資訊，請參閱本節先前所示的 AWSControlTowerAdmin 範例。對於 AWS Config 記錄器角色，我們建議新增 `aws:SourceArn`條件，將 Config 記錄器 ARN 指定為允許的來源 ARN。

對於 AWSControlTowerExecution 等角色或所有受管帳戶中 AWS Control Tower Audit 帳戶可擔任的其他程式設計角色，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**
>
> 如果發生偏離，在某些情況下可能會重設 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 如何彙總未受管 OUs和帳戶中的 AWS Config 規則

- AWS Control Tower 管理帳戶會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 不需要存取未受管帳戶。AWS Control Tower 主控台會顯示您為指定帳戶建立的外部 AWS Config 規則數量。您可以在帳戶詳細資訊頁面的外部 Config 規則合規索引標籤中檢視這些外部規則的詳細資訊。
- 若要建立彙總工具，AWS Control Tower 會新增具有描述組織和列出其下帳戶所需許可的角色。此AWSControlTowerConfigAggregatorRoleForOrganizations角色需要 AWSConfigRoleForOrganizations受管政策和與 的信任關係config.amazonaws.com。

> **Note**
>
> 使用登陸區域 4.0 版的客戶不需要此角色，因為 AWS Control Tower 已從現有的組織層級組態彙總工具遷移至服務連結組態彙總工具

> **Note**
>
> 當您在包含登陸區域的組織中啟用受信任存取時，AWS Control Tower 可以為組織中的所有帳戶建立角色、管理資源和讀取資料。透過受信任的存取，AWS Control Tower 可以使用組織中的任何帳戶或 OU，無論已註冊和已註冊或未註冊。

以下是連接到角色的 IAM 政策 (JSON 成品）：

JSON

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

以下是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，下列許可會新增至 受管政策 中AWSControlTowerServiceRolePolicy，該政策會在AWSControlTowerAdmin角色建立 AWS Config 彙總工具時使用：

JSON

```
{
```

```
  "Version":"2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
          "config:PutConfigurationAggregator",
          "config:DeleteConfigurationAggregator",
          "iam:PassRole"
          ],
        "Resource": [
          "arn:aws:iam::123456789012:role/service-role/
AWSControlTowerConfigAggregatorRoleForOrganizations",
          "arn:aws:config:us-east-1:123456789012:config-aggregator/"
          ]
        },
      {
        "Effect": "Allow",
        "Action": "organizations:EnableAWSServiceAccess",
        "Resource": "*"
      }
    ]
}
```

新建立的資源： AWSControlTowerConfigAggregatorRoleForOrganizations和 aws-controltower-ConfigAggregatorForOrganizations

當您準備好時，您可以個別註冊帳戶，或透過註冊 OU 將其註冊為群組。當您註冊帳戶後，如果您在中建立規則 AWS Config，AWS Control Tower 會偵測新的規則。彙整工具會顯示外部規則的數量，並提供 AWS Config 主控台的連結，您可以在其中檢視您帳戶的每個外部規則的詳細資訊。使用 主控台和 AWS Control Tower 主控台中 AWS Config 的資訊，判斷您是否為帳戶啟用適當的控制項。

AWS Control Tower 稽核帳戶的程式設計角色和信任關係

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

稽核帳戶可讓您透過僅授予 AWS Lambda 函數的某些角色，以程式設計方式存取其他帳戶。基於安全考量，這些角色與其他角色具有信任關係，這表示嚴格定義可使用角色的條件。

AWS Control Tower 堆疊會在稽核帳戶中StackSet-AWSControlTowerBP-BASELINE-ROLES建立這些僅限程式設計的跨帳戶 IAM 角色：

- aws-controltower-AdministratorExecutionRole
- aws-controltower-ReadOnlyExecutionRole

AWS Control Tower 堆疊會在稽核帳戶中`StackSet-AWSControlTowerSecurityResources`建立這些僅限程式設計的跨帳戶 IAM 角色：

- aws-controltower-AuditAdministratorRole
- aws-controltower-AuditReadOnlyRole

`ReadOnlyExecutionRole`: 請注意，此角色允許稽核帳戶在整個組織中讀取 Amazon S3 儲存貯體中的物件（與僅允許中繼資料存取`SecurityAudit`的政策相反）。

aws-controltower-AdministratorExecutionRole：

- 具有管理員許可
- 無法從主控台擔任
- 只能由稽核帳戶中的角色擔任 – `aws-controltower-AuditAdministratorRole`

下列成品顯示 的信任關係`aws-controltower-AdministratorExecutionRole`。預留位置號碼`012345678901`將由您稽核帳戶的`Audit_acct_ID`號碼取代。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/aws-controltower-AuditAdministratorRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

aws-controltower-AuditAdministratorRole：

- 只能由 AWS Lambda 服務擔任
- 具有許可，可在名稱開頭為字串日誌的 Amazon S3 物件上執行讀取（取得）和寫入（提取）操作

連接的政策：

1. AWSLambdaExecute – AWS 受管政策

2. AssumeRole-aws-controltower-AuditAdministratorRole – 內嵌政策 – 由 AWS Control Tower 建立，成品如下。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
 {
 "Action": [
   "sts:AssumeRole"
   ],
 "Resource": [
   "arn:aws:iam::*:role/aws-controltower-AdministratorExecutionRole"
   ],
 "Effect": "Allow"
 }
   ]
}
```

下列成品顯示 的信任關係`aws-controltower-AuditAdministratorRole`：

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

aws-controltower-ReadOnlyExecutionRole：

- 無法從主控台擔任
- 只能由稽核帳戶中的另一個角色擔任 – AuditReadOnlyRole

下列成品顯示 的信任關係aws-controltower-ReadOnlyExecutionRole。預留位置號碼012345678901將由您稽核帳戶的Audit_acct_ID號碼取代。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/aws-controltower-AuditReadOnlyRole "
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

aws-controltower-AuditReadOnlyRole：

- 只能由 AWS Lambda 服務擔任
- 具有在名稱開頭為字串日誌的 Amazon S3 物件上執行讀取（取得）和寫入（提取）操作的許可

連接的政策：

1. AWSLambdaExecute – AWS 受管政策

2. AssumeRole-aws-controltower-AuditReadOnlyRole – 內嵌政策 – 由 AWS Control Tower 建立，成品如下。

JSON

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

```
    "sts:AssumeRole"
   ],
   "Resource": [
    "arn:aws:iam::*:role/aws-controltower-ReadOnlyExecutionRole"
   ],
   "Effect": "Allow"
     }
    ]
}
```

下列成品顯示 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 管理帳戶中建立 Lambda 函數，該帳戶會在成員帳戶中擔任 AWSControlTowerExecution 角色。然後，使用 角色，管理帳戶會在每個成員帳戶中執行所需的組態步驟。

如果您使用 Lambda 函數佈建帳戶，則將執行此工作的身分除了 之外，還必須具有下列 IAM 許可政策AWSServiceCatalogEndUserFullAccess。

JSON

```
{
    "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: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 帳戶工廠`sso:ProvisionSAMLProvide`需要`sso:GetPeregrineStatussso:ProvisionApplicationInstanceForAWSAccount`、`sso:Provisio`和 許可，才能與 IAM Identity Center AWS 互動。

AWS Control Tower 中的資源

- 如需 AWS Control Tower 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 在共用帳戶中建立之資源的相關資訊，請參閱 關於共用帳戶。
- 如需 AWS Control Tower 透過 Account Factory 佈建帳戶時所建立資源的相關資訊，請參閱 Account Factory 的資源考量事項。
- 若要檢視 AWS Control Tower 定義之 AWS 資源類型的詳細資訊，以便與 AWS Control Tower APIs 搭配使用，請參閱AWS CloudFormation 《 使用者指南》中的 AWS Control Tower 資源類型參考。

AWS 區域如何使用 AWS Control Tower

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)
- 亞太地區 (悉尼)
- 亞太地區 (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)
- 亞太地區 (孟買)
- 亞太地區 (首爾)
- 亞太地區 (東京)
- Europe (Paris)
- 南美洲 (聖保羅)
- 美國西部 (加利佛尼亞北部)
- 亞太地區 (香港)
- 亞太地區 (雅加達)
- 亞太地區 (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)
- 亞太地區 (海德拉巴)
- 歐洲 (蘇黎世)

- 亞太地區 (墨爾本)
- 加拿大西部 (卡加利)
- 馬來西亞 (Kuala Lumpur)
- 亞太區域 (泰國)
- 墨西哥 (中部)
- 亞太區域 (台北)

關於您的主要區域

當您建立登陸區域時，您用於存取 AWS 管理主控台的區域會成為 AWS Control Tower 的主 AWS 區域。在建立過程中，某些資源會在主要區域中佈建。其他資源，例如 OUs和 AWS 帳戶，都是全域資源。

選取主要區域之後，就無法進行變更。

控制項和區域

目前，所有預防性控制都適用於全球。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 Tower 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

本節說明當您將 AWS Control Tower 登陸區域擴展到新的 AWS 區域，或從登陸區域組態中移除區域時，您可以預期的行為。一般而言，此動作是透過 AWS Control Tower 主控台的更新函數執行。

> **Note**
>
> 建議您避免將 AWS Control Tower 登陸區域擴展到 AWS 不需要工作負載執行的區域。選擇退出某個區域並不會阻止您在該區域中部署資源，但這些資源將保留在 AWS Control Tower 控管範圍之外。

在新區域的組態期間，AWS Control Tower 會更新登陸區域，這表示它會為您的登陸區域建立基準：

- 在所有新選取的區域中主動運作，以及
- 停止管理取消選取區域中的資源。

組織單位 (OUs) 中由 AWS Control Tower 管理的個別帳戶不會在此登陸區域更新程序中更新。因此，您必須重新註冊 OUs 來更新帳戶。

設定 AWS Control Tower 區域時，請注意下列建議和限制：

- 選取您計劃託管 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中部署資源，但這些資源將保留在 AWS Control Tower 控管範圍之外。

當您為新區域設定登陸區域時，AWS Control Tower 偵測控制會遵循下列規則：

- 已存在的項目保持不變。在現有區域的現有 OUs 中，現有帳戶的控制行為、偵測和預防行為保持不變。
- 您無法將新的偵測性控制套用至包含未更新帳戶的現有 OUs。當您將 AWS Control Tower 登陸區域設定為新區域（透過更新登陸區域）時，您必須先更新現有 OUs 中的現有帳戶，才能對這些 OUs 和帳戶啟用新的偵測控制。
- 一旦更新帳戶，您現有的偵測控制就會開始在新設定的區域中運作。當您更新 AWS Control Tower 登陸區域以設定新區域，然後更新帳戶時，已在 OU 上啟用的偵測性控制項將開始在新設定的區域中使用該帳戶。

設定 AWS Control Tower 區域

1. 在 登入 AWS Control Tower 主控台 https://console.aws.amazon.com//controltower
2. 在左側窗格導覽功能表中，選擇登陸區域設定。
3. 在登陸區域設定頁面的詳細資訊區段中，選擇右上角的修改設定按鈕。系統會將您導向至更新登陸區域工作流程，因為管理新區域或從管控中移除區域需要您更新至最新的登陸區域版本。
4. 在用於控管的其他 AWS 區域下，搜尋您要控管（或停止管理）的區域。狀態欄指出您目前管理的區域，以及您未管理的區域。
5. 選取要管理的每個額外區域的核取方塊。取消選取您要移除控管的每個區域的核取方塊。

> **Note**
>
> 如果您選擇不管理區域，您仍然可以在該區域中部署資源，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，然後選擇更新登陸區域。

7. 當登陸區域設定完成時，重新註冊 OUs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 OUs和帳戶。

設定新區域後佈建或更新個別帳戶的替代方法是使用 Service Catalog 的 API 架構和 在 AWS CLI批次程序中更新帳戶。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 管控擴展至新的區域，以及從區域移除 AWS Control Tower 管控之後 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 內每個帳戶的控制項不完全相符，則可能會發生混合控管的不良情況。如果在 AWS Control Tower 將管控延伸至新的 或移除管控之後，帳戶未更新 AWS 區域，則混合管控會在 OU 中發生。

在這種情況下，與 OU 中的其他帳戶相比，或與登陸區域的整體控管狀態相比，OU 中的某些帳戶可能會在不同區域中套用不同的控制。

在具有混合控管的 OU 中，如果您佈建新帳戶，該新帳戶會收到與登陸區域相同的 （更新） 區域和 OU 控管狀態。不過，尚未更新的現有帳戶不會收到更新的區域控管狀態。

一般而言，混合控管可能會在 AWS Control Tower 主控台中建立矛盾或不準確的狀態指示燈。例如，在混合控管期間，對於尚未更新的 帳戶，選擇加入區域會在已註冊OUs 中以「未控管」狀態顯示。

> **Note**
>
> AWS Control Tower 不允許在混合控管狀態期間啟用控制項。

混合控管期間的控制行為

- 在混合控管期間，AWS Control Tower 無法一致地在 OU 已顯示為受管的區域中部署基於 AWS Config 規則 （即偵測性控制） 的控制項，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。
- 在混合控管期間，如果您在 OU 中的任何帳戶尚未更新時，將登陸區域的控管延伸至選擇加入區域，則 OU 上的 `EnableControl` API 操作會針對偵測和主動控制失敗。您會收到`FAILED_TO_ENABLE`錯誤訊息，因為 OU 中的未更新成員帳戶尚未選擇加入這些區域。
- 在混合控管期間，屬於 Security Hub CSPM 服務受管標準的控制項：AWS Control Tower 無法在登陸區域組態與未更新的帳戶之間不相符的區域中準確報告合規。

- 混合控管不會變更 SCP 型控制（預防性控制）的行為，其會統一套用至每個受管區域中 OU 中的每個帳戶。

> **Note**
>
> 混合控管與漂移不同，也不會回報為漂移。

修復混合控管

- 客戶現在可以透過重設區域控制項來修復混合控管。任何非全域控制項都是區域性（偵測和主動控制）。系統會透過警示橫幅提醒您的 OU 處於混合控管中。

啟用 AWS 選擇加入區域的考量事項

雖然您的 預設為 AWS 區域 作用中 AWS 帳戶，但只有在您手動選取特定區域時，才會啟用這些區域。本文件將那些區域稱為選擇加入區域。相反地，當您 AWS 帳戶 建立 時，預設處於作用中狀態的區域即稱為商業區域、預設區域，或簡稱為區域。

選擇加入一詞具有歷史基礎。2019 年 3 月 20 日之後 AWS 區域 推出的任何 都會部署為選擇加入區域。在選擇加入的區域中，您的帳戶不會在該區域內啟用，而且您的身分也不會複寫到該區域，除非您選擇使用該區域。透過 IAM 服務管理的所有資料均視為身分資料，包括使用者、群組、角色、政策、身分提供者、其相關資料（例如 X.509 簽署憑證或內容特定憑證），以及其他帳戶層級設定，例如密碼政策和帳戶別名。

您可以選取登入區域設定期間自動啟用選擇加入區域。您的登陸區域會在所有選取的區域中變成作用中。

如果您選擇選擇加入區域做為 AWS Control Tower 主區域，請先依照啟用區域中的步驟，在登入 管理主控台時啟用該區域。 AWS 若要從選擇加入的區域使用您自己的現有日誌封存和稽核帳戶，請先手動啟用該區域。

AWS 選擇加入的區域包括數個可使用 AWS Control Tower 的區域：

- 亞太區域（香港）區域，ap-east-1
- 亞太區域（雅加達）區域，ap-southeast-3
- 歐洲（米蘭）區域，eu-south-1
- 非洲（開普敦）區域，af-south-1

- 中東（巴林）區域，me-south-1
- 以色列（特拉維夫），il-central-1
- 中東（阿拉伯聯合大公國）區域，me-central-1
- 歐洲（西班牙）區域，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）區域，ap-southeast-4
- 加拿大西部（卡加利）區域，ca-west-1
- 亞太區域（泰國），ap-southeast-7
- 墨西哥（中部）、mx-central-1
- 亞太區域（台北），ap-east-2
- 亞太區域（紐西蘭），ap-southeast-6

AWS Control Tower 有一些控制項在選擇加入區域與預設區域（其他商業區域）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，請注意下列事項。

> **管理或啟用？**
>
> 請記住，管理區域是您可以從 AWS Control Tower 主控台選取的動作，因此可以在區域中套用控制項。啟用或停用選擇加入區域是您可以在 主控台中選擇 AWS 的不同動作，這會將區域開啟至您的帳戶，讓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，建議您不要停用（選擇退出）任何受管選擇加入區域，因為這可能會導致工作負載失敗。AWS Control Tower 不允許從 AWS Control Tower 主控台內停用受管區域，但請務必不要從 AWS Control Tower 外部的來源停用受管區域，例如 AWS Billing 主控台或 AWS SDK。
- 當 AWS Control Tower 將管控擴展到選擇加入區域時，它會啟用（選擇加入）到所有成員帳戶中的區域。當您從控管中移除區域時，AWS Control Tower 不會停用（選擇退出）成員帳戶中的區域。
- 在區域取消選取期間，如果已從 AWS Control Tower 外部來源手動停用帳戶的資源，例如 AWS 帳單主控台或 AWS SDK，則 AWS Control Tower 會略過從選擇加入區域移除資源。我們建議您從已停用的區域移除資源，否則您可能會收到這些資源的意外帳單費用。

- 如果您的登陸區域已停用，AWS Control Tower 會清除所有受管區域中的資源，包括選擇加入區域。不過，AWS Control Tower 不會停用選擇加入區域。您可以停用選擇加入區域，做為停用後的額外步驟。
- 如果您的主要區域是選擇加入區域，而且如果您想要將現有帳戶註冊為日誌封存和稽核帳戶，您必須先手動啟用選擇加入區域，才能選取該區域做為登陸區域的主要區域。請參閱啟用區域。
- 如果 AWS Control Tower 已設定選擇加入區域做為您的主要區域，而且如果您從任何其他區域的 AWS 主控台造訪 AWS Control Tower 服務，則主控台不會自動將您重新導向至主要區域。
- 基礎 API 具有容量限制，這可能會根據區域、帳戶和服務負載的數量，將延遲從幾分鐘增加到數小時。最佳實務是僅選擇加入您將執行工作負載 AWS 區域 的 ，並一次選擇加入一個區域。

控管和帳戶的重要限制

- 如果 16 個以上可使用 AWS Control Tower 的商業區域受管，包括選擇加入區域，則在註冊 OU 時，每個組織單位 (OU) 的帳戶數量上限會減少。如需詳細資訊，請參閱以基礎 AWS 服務為基礎的限制。

設定區域拒絕控制

AWS Control Tower 提供兩個區域拒絕控制。啟用GRREGIONDENY時，一個控制項 會套用至整個登陸區域。啟用CTMULTISERVICEPV1時，另一個控制項 可以套用到您指定的特定 OUs。如需詳細資訊，請參閱 AWS 根據請求拒絕存取 ， AWS 區域以及套用到 OU 的區域拒絕控制。

登陸區域的區域拒絕控制考量

區域拒絕控制GRREGIONDENY是唯一的，因為它適用於整個登陸區域，而不是任何特定的 OU。若要設定區域拒絕控制，請前往登陸區域設定頁面，然後選取修改設定。

- 稍後可以變更此設定。
- 啟用時，此控制項會套用至所有已註冊OUs。
- 無法針對個別 OUs 設定此控制項。

> **Note**
>
> 啟用區域拒絕控制項之前，請確定您在這些區域中沒有現有資源，因為您套用控制項後將無法存取您的資源。啟用控制項時，您將無法在遭拒的區域中部署資源。

當您啟用控制項時，它會套用到階層中所有已註冊的頂層 OUs，並且由鏈結中較低的 OUs 繼承。當您移除 控制項時，它會在所有已註冊OUs 上移除它，AWS Control Tower 中的所有非受管區域都會保持 未受管 狀態， 而且您可以在 AWS Control Tower 可用性之外的區域中 部署資源。

> **例外狀況**
>
> 您無法拒絕存取您的主要區域。某些全域 AWS 服務，例如 IAM 和 AWS Organizations，不受區域拒絕控制。若要進一步了解，請參閱AWS 根據請求拒絕存取 AWS 區域。

- 完整控制名稱： AWS 根據請求 AWS 的區域拒絕對 的存取
- 控制描述：不允許在指定區域外的全域和區域服務中存取未列出的操作。
- 這是具有預防性指導的選擇性控制。

若要檢視區域拒絕控制 SCP 的範本，請參閱 AWS Control Tower 控制參考中的根據請求拒絕對 AWS 的存取 AWS 區域。AWS Control Tower SCP 類似於 的 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。

OU 層級區域拒絕控制的考量事項

OU 層級區域拒絕控制的主要考量是判斷如果兩者都啟用，它將如何與登陸區域區域拒絕控制互動。如需詳細資訊，請參閱套用至 OU 的區域拒絕控制。

您也可以檢閱設定區域拒絕控制。

關於 AWS Control Tower AWS 帳戶 中的

AWS 帳戶 是您擁有的所有資源的容器。這些資源包括帳戶接受的 AWS Identity and Access Management (IAM) 身分，這會決定誰可以存取該帳戶。IAM 身分可以包含使用者、群組、角色等。如需在 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。

資源和帳戶建立時間

當 AWS Control Tower 建立或註冊帳戶時，它會部署帳戶所需的最低資源組態。例如，它可能包含 Account Factory 範本形式的資源，以及登陸區域中的其他資源，例如 IAM 角色、 AWS CloudTrail 通道、Service Catalog 佈建產品，以及 IAM Identity Center 使用者。AWS Control Tower 也會根據控制組態的要求，針對新帳戶目的地為成員帳戶的組織單位 (OU) 部署資源。

AWS Control Tower 會代表您協調這些資源的部署。每個資源可能需要幾分鐘才能完成部署，因此請在建立或註冊帳戶之前考慮總時間。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 資源的指引。

AWS Control Tower 建立帳戶時會發生什麼情況

AWS Control Tower 中的新帳戶是透過 AWS Control Tower 之間的互動建立並佈建 AWS Organizations，以及 AWS Service Catalog。您可以從 AWS Control Tower 主控台建立帳戶並註冊現有帳戶。如需 AWS 帳戶 使用 AWS Control Tower 主控台註冊現有 的詳細步驟，請參閱 從 AWS Control Tower 主控台註冊現有帳戶。

帳戶建立的幕後

1. 例如，您可以從 AWS Control Tower 帳戶工廠頁面，或直接從 AWS Service Catalog 主控台，或呼叫 Service Catalog `ProvisionProduct` API 來啟動請求。
2. AWS Service Catalog 呼叫 AWS Control Tower。
3. AWS Control Tower 會開始工作流程，第一步是呼叫 AWS Organizations `CreateAccount` API。
4. AWS Organizations 建立帳戶後，AWS Control Tower 會透過套用藍圖和控制項來完成佈建程序。
5. Service Catalog 會繼續輪詢 AWS Control Tower，以檢查佈建程序是否完成。
6. 當 AWS Control Tower 中的工作流程完成時，Service Catalog 會完成帳戶的狀態，並通知您 （ 申請者 ） 結果。

引進現有安全或記錄帳戶的考量事項

接受 AWS 帳戶 做為安全 （預設名稱：稽核) 或記錄 （預設名稱：日誌封存) 帳戶之前，AWS Control Tower 會檢查帳戶是否有與 AWS Control Tower 需求衝突的資源。例如，您可能有一個記錄儲存貯體，其名稱與 AWS Control Tower 要求的名稱相同。此外，AWS Control Tower 會驗證帳戶是否可以佈建資源；例如，確保已啟用 AWS Security Token Service (AWS STS)、帳戶未暫停，以及 AWS Control Tower 具有在帳戶中佈建資源的許可。

AWS Control Tower 不會移除您提供的日誌和安全性帳戶中的任何現有資源。不過，如果您選擇啟用它，AWS Control Tower 區域拒絕控制會防止存取遭拒區域中的資源。

> **您帳戶的安全性**
>
> 您可以在 文件中找到 AWS Organizations 保護 AWS Control Tower 管理帳戶和成員帳戶安全的最佳實務相關指導。
>
> - 管理帳戶的最佳實務
> - 成員帳戶的最佳實務

關於共用帳戶

三個特殊項目與 AWS Control Tower AWS 帳戶 相關聯；管理帳戶、稽核帳戶和日誌封存帳戶。這些帳戶通常稱為共用帳戶，有時稱為核心帳戶。

- 您可以在設定登陸區域時，選取稽核和日誌封存帳戶的自訂名稱。如需變更帳戶名稱的資訊，請參閱外部變更 AWS Control Tower 資源名稱。
- 您也可以在初始登陸區域設定程序期間，將現有的 指定 AWS 帳戶 為 AWS Control Tower 安全或記錄帳戶。此選項消除了 AWS Control Tower 建立新的共用帳戶的需求。（這是一次性選擇。）

如需共用帳戶及其相關資源的詳細資訊，請參閱 在共用帳戶中建立的資源。

管理帳戶

這會 AWS 帳戶 啟動 AWS Control Tower。根據預設，此帳戶的根使用者和此帳戶的 IAM 使用者或 IAM 管理員使用者具有登陸區域內所有資源的完整存取權。

> **Note**
>
> 最佳實務是，我們建議在 AWS Control Tower 主控台內執行管理功能時，以具有管理員權限的 IAM Identity Center 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 在共用帳戶中建立的資源。

日誌封存帳戶

如果您未特別攜帶另一個帳戶，日誌封存共用 AWS 帳戶會在您建立登陸區域時自動設定。

此帳戶包含中央 Amazon S3 儲存貯體，用於儲存登陸區域中所有其他帳戶的所有 AWS CloudTrail 和 AWS Config 日誌檔案副本。根據最佳實務，我們建議將日誌封存帳戶存取權限制在負責合規和調查的團隊，以及其相關的安全或稽核工具。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 儲存貯體政策**
>
> 對於 AWS Control Tower 登陸區域 3.3 版及更新版本，帳戶必須符合對稽核儲存貯體的任何寫入許可`aws:SourceOrgID`條件。此條件可確保 CloudTrail 只能代表您組織內的帳戶將日誌寫入 S3 儲存貯體；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 登陸區域 3.3 版。

如需日誌封存帳戶中可用角色和資源的詳細資訊，請參閱 日誌封存帳戶資源

> **Note**
>
> 這些日誌無法變更。所有日誌都會儲存，以用於與帳戶活動相關的稽核和合規調查。

稽核帳戶

如果您未特別攜帶另一個帳戶，則會在您建立登陸區域時自動設定此共用帳戶。

稽核帳戶應僅限於具有稽核員（唯讀）和管理員（完整存取）跨帳戶角色的安全和合規團隊，以及登陸區域中所有帳戶。這些角色旨在供安全與合規團隊使用，以：

- 透過 AWS 機制執行稽核，例如託管自訂 AWS Config 規則 Lambda 函數。
- 執行自動化安全操作，例如修復動作。

稽核帳戶也會透過 Amazon Simple Notification Service (Amazon SNS) 服務接收通知。可接收三種類型的通知：

- 所有組態事件 – 此主題會彙總登陸區域中所有帳戶的所有 CloudTrail 和 AWS Config 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 合規狀態變更事件和 GuardDuty 調查結果的所有安全性通知。
- 偏離通知 – 此主題彙總了在您登陸區域中所有帳戶、使用者、OUs 和 SCPs 中發現的所有偏離警告。如需有關偏離的詳細資訊，請參閱在 AWS Control Tower 中偵測並解決偏離。

在成員帳戶中觸發的稽核通知也可以傳送提醒到本機 Amazon SNS 主題。此功能可讓帳戶管理員訂閱個別成員帳戶特有的稽核通知。因此，管理員可以解決影響個別帳戶的問題，同時仍然將所有帳戶通知彙總到集中式稽核帳戶。如需詳細資訊，請參閱《Amazon Simple Notification Service 開發人員指南》。

如需稽核帳戶中可用角色和資源的詳細資訊，請參閱 稽核帳戶資源。

如需程式設計稽核的詳細資訊，請參閱 AWS Control Tower 稽核帳戶的程式設計角色和信任關係。

> **Important**
>
> 您為稽核帳戶提供的電子郵件地址會從 AWS Control Tower AWS 區域 支援的每個 接收AWS 通知 - 訂閱確認電子郵件。若要在您的稽核帳戶中接收合規電子郵件，您必須從 AWS Control Tower AWS 區域 支援的每個電子郵件中選擇確認訂閱連結。

在共用帳戶中建立的資源

本節顯示當您設定登陸區域時，AWS Control Tower 在共用帳戶中建立的資源。

如需成員帳戶資源的資訊，請參閱 Account Factory 的資源考量事項。

管理帳戶資源

當您設定登陸區域時，會在您的管理帳戶中建立下列 AWS 資源。

AWS 服務	Resource Type (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 版和更新版本中）
AWS CloudFormation	StackSets	AWSControlTowerBP-BASELINE-CLOUDTRAIL（未在 3.0 和更新版本中部署） AWSControlTowerBP_BASELINE_SERVICE_LINKED_ROLE (Deployed in 3.2 and later) AWSControlTowerBP-BASELINE-CLOUDWATCH AWSControlTowerBP-BASELINE-CONFIG AWSControlTowerBP-BASELINE-ROLES

AWS 服務	Resource Type (資源類型)	資源名稱
		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 Service Catalog	產品	AWS Control Tower 帳戶工廠
AWS Config	彙整工具	aws-controltower-ConfigAggregatorForOrganizations
AWS CloudTrail	追蹤	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch Logs	aws-controltower/CloudTrailLogs

AWS 服務	Resource Type (資源類型)	資源名稱
AWS Identity and Access Management	角色	AWSControlTowerAdmin AWSControlTowerStackSetRole AWSControlTowerCloudTrailRolePolicy
AWS Identity and Access Management	政策	AWSControlTowerServiceRolePolicy AWSControlTowerAdminPolicy AWSControlTowerCloudTrailRolePolicy AWSControlTowerStackSetRolePolicy
AWS IAM Identity Center	目錄群組	AWSAccountFactory AWSAuditAccountAdmins AWSControlTowerAdmins AWSLogArchiveAdmins AWSLogArchiveViewers AWSSecurityAuditors AWSSecurityAuditPowerUsers AWSServiceCatalogAdmins

AWS 服務	Resource Type (資源類型)	資源名稱
AWS IAM Identity Center	許可集	AWSAdministratorAccess AWSPowerUserAccess AWSServiceCatalogAdminFullAccess AWSServiceCatalogEndUserAccess AWSReadOnlyAccess AWSOrganizationsFullAccess

> **Note**
>
> The CloudFormation StackSet `BP_BASELINE_CLOUDTRAIL` 不會部署在登陸區域 3.0 版或更新版本中。不過，它會持續存在於舊版的登陸區域，直到您更新登陸區域為止。

日誌封存帳戶資源

當您設定登陸區域時，日誌封存帳戶中會建立下列 AWS 資源。

AWS 服務	Resource Type (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	Resource Type (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-BASELINE-ROLES- 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

AWS 服務	Resource Type (資源類型)	資源名稱
Amazon CloudWatch	CloudWatch 事件規則	aws-controltower-ConfigComplianceChangeEventRule
Amazon CloudWatch	CloudWatch Logs	/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 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

AWS 服務	Resource Type (資源類型)	資源名稱
Amazon Simple Storage Service	儲存貯體	aws-controltower-logs-* aws-controltower-s3-access-logs-*

稽核帳戶資源

當您設定登陸區域時，會在您的稽核帳戶中建立下列 AWS 資源。

AWS 服務	Resource Type (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-

AWS 服務	Resource Type (資源類型)	資源名稱
		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 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 事件規則	aws-controltower-ConfigComplianceChangeEventRule
Amazon CloudWatch	CloudWatch Logs	/aws/lambda/aws-controltower-NotificationForwarder

AWS 服務	Resource Type (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

關於成員帳戶

成員帳戶是您的使用者執行 AWS 工作負載的帳戶。AWS Control Tower 成員帳戶可以透過各種方法建立和自訂，包括自動化方法。在某些情況下，您可以將現有的 帶 AWS 帳戶 入 AWS Control Tower。建立或註冊成員帳戶時，這些帳戶必須存在於 AWS Control Tower 主控台中建立的組織單位 (OU) 內，或向 AWS Control Tower 註冊。如需詳細資訊，請參閱下列相關主題：

- 佈建方法
- 使用 Account Factory 佈建和管理帳戶
- 自動化 AWS Control Tower 中的任務
- 使用自動註冊來移動和註冊帳戶
- 使用 AWS Control Tower Account Factory for Terraform (AFT) 佈建帳戶
- AWS Organizations 《 使用者指南AWS 》中的 Organizations 術語和概念。

> **帳戶和控制項**
>
> 成員帳戶可以在 AWS Control Tower 中註冊，也可以取消註冊。控制項適用於已註冊和未註冊的帳戶，並且控制項可能會根據繼承套用至巢狀 OUs 中的帳戶。

如需 AWS Control Tower 配置的成員帳戶資源資訊，請參閱 Account Factory 的資源考量事項。

與來自 的 AWS Control Tower 帳戶互動 AWS Service Catalog

本節說明如何使用 功能處理您的 AWS Control Tower 帳戶 AWS Service Catalog。

主題

- 在 Service Catalog 主控台中使用 Account Factory 佈建帳戶
- 透過 Service Catalog APIs 自動化 AWS Control Tower 中的帳戶佈建
- 更新 Service Catalog 中的佈建產品
- 在 Service Catalog 中取消註冊帳戶

在 Service Catalog 主控台中使用 Account Factory 佈建帳戶

下列程序說明如何透過 在 IAM Identity Center 中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戶佈建。或者，您可以使用 AWS CLI、Service Catalog APIs 或 AWS Control Tower Account Factory for Terraform (AFT)，以程式設計方式佈建 AWS Control Tower 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。如需自訂的詳細資訊，請參閱 使用帳戶工廠自訂 (AFC) 自訂帳戶。

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，選擇您管理帳戶的帳戶 ID。此 ID 也可能有標籤，例如 （管理）。
4. 從 AWSServiceCatalogEndUserAccess，選擇 Management console (管理主控台)。這會 AWS 管理主控台 開啟此帳戶中此使用者的 。
5. 請確定您已選取 AWS 區域 正確的佈建帳戶，該帳戶應該是您的 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 帳戶工廠，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：
   - SSOUserEmail 可以是新的電子郵件地址，或與現有 IAM Identity Center 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。
   - AccountEmail 必須是尚未與 建立關聯的電子郵件地址 AWS 帳戶。如果您在 SSOUserEmail 中使用了新的電子郵件，您就可以在此使用該電子郵件地址。
10. 不要定義 TagOptions，也不要啟用通知，否則帳戶可能無法佈建。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，否則帳戶將無法佈建。
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**
>
> 一次最多可佈建五個帳戶。

透過 Service Catalog APIs 自動化 AWS Control Tower 中的帳戶佈建

AWS Control Tower 已與數個其他服務整合 AWS ，例如 AWS Service Catalog。您可以使用 APIs 在 AWS Control Tower 中建立和佈建您的成員帳戶，或註冊現有的成員帳戶。

> **Note**
>
> 如果您已在登陸區域設定中選擇退出 IAM Identity Center，則不會使用您在使用 AWS Service Catalog APIs或主控台佈建帳戶期間提供的值。

影片說明如何透過呼叫 AWS Service Catalog APIs，以自動化的批次方式佈建帳戶。對於佈建，您將從 AWS 命令列界面 (CLI) 呼叫 `ProvisionProduct` API，並指定 JSON 檔案，其中包含您要設定的每個帳戶的參數。影片說明安裝和使用 AWS Cloud9 開發環境來執行此工作。如果您使用 AWS Cloudshell 而非 AWS Cloud9，CLI 命令會相同。

> **Note**
>
> 您也可以呼叫 AWS Service Catalog 每個帳戶的 `UpdateProvisionedProduct` API 來調整此方法來自動化帳戶更新。您可以編寫指令碼來逐一更新帳戶。

作為完全不同的自動化方法，如果您熟悉 Terraform，您可以向 AWS Control Tower Account Factory for Terraform (AFT) 佈建帳戶。

自動化管理角色範例

以下是範例範本，您可以用來協助在 管理帳戶中設定自動化管理角色。您會在管理帳戶中設定此角色，以便在目標帳戶中使用管理員存取權來執行自動化。

```
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"
```

自動化執行角色範例

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 APIs來執行自動化任務。CLI 命令會在影片中提供。

Service Catalog API 的範例佈建輸入

如果您使用 `ProvisionProduct` API 佈建新的 AWS Control Tower 帳戶或註冊現有的成員帳戶，以下是您可以提供給 Service Catalog API 的輸入範例：

> **Note**
>
> 若要使用 `ProvisionProduct` API 註冊現有的成員帳戶，在您呼叫 API 之前，IAM `AWSControlTowerExecution` 角色必須存在於目標帳戶上。您可以針對新帳戶佈建和現有帳戶註冊，使用下列範例中顯示的相同輸入參數。

```
{
  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 變更為 OU_NAME OU_NAME (OU_ID)。以下影片並未提及此變更。

影片演練

此影片 (6：58) 說明如何自動化 AWS Control Tower 中的帳戶部署。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 自動化帳戶佈建的影片逐步解說。

更新 Service Catalog 中的佈建產品

下列程序會引導您如何更新 Account Factory 中的帳戶，或在 Service Catalog 中更新帳戶的佈建產品，將其移至新的 OU。

> **Note**
>
> 如果您已在登陸區域設定中選擇退出 IAM Identity Center，則不會使用您在使用 AWS Service Catalog APIs或主控台佈建帳戶期間提供的值。

透過 Service Catalog 更新 Account Factory 帳戶或變更其 OU

1. 登入 AWS 管理主控台，並在 https：//https://console.aws.amazon.com/servicecatalog/ 開啟 AWS Service Catalog 主控台。

   > **Note**
   >
   > 您必須以具有在 Service Catalog 中佈建新產品許可的使用者身分登入（例如，`AWSAccountFactory`或 `AWSServiceCatalogAdmins`群組中的 IAM Identity Center 使用者）。

2. 在導覽窗格中，選擇佈建，然後選擇佈建產品。
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. 選取成員帳戶。系統會將您導向該帳戶的佈建產品詳細資訊頁面。
   b. 在佈建產品詳細資訊頁面上，選擇事件索引標籤。
   c. 記下以下參數：

      - SSOUserEmail (可用於已佈建的產品詳細資訊)
      - AccountEmail (可用於已佈建的產品詳細資訊)
      - SSOUserFirstName（可在 IAM Identity Center 中使用）
      - SSOUSerLastName（可在 IAM Identity Center 中使用）
      - AccountName（可在 IAM Identity Center 中使用）

   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，請針對 ManagedOrganizationalUnit，選擇帳戶已經存在其中的 OU。
- 如果您要將帳戶遷移至新的 OU，請針對 ManagedOrganizationalUnit，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。

在 Service Catalog 中取消註冊帳戶

`AWSAccountFactory` 群組中的 IAM Identity Center 使用者可以透過終止佈建產品，在 Service Catalog 主控台中完成帳戶取消註冊。如需 IAM Identity Center 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。下列程序說明如何在 Service Catalog 中取消註冊成員帳戶。

透過 Service Catalog 取消註冊已註冊的帳戶

1. 在 Web 瀏覽器中開啟 Service Catalog 主控台，網址為 https://console.aws.amazon.com/servicecatalog。
2. 在左側導覽窗格中，選擇佈建產品清單。
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**
>
> 字詞終止專屬於 Service Catalog。當您在 Service Catalog Account Factory 中終止帳戶時，帳戶不會關閉。此動作會從其 OU 和您的登陸區域移除帳戶。

6. 帳戶取消註冊後，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

> **Note**
>
> 等待帳戶狀態顯示未註冊。

在 AWS Control Tower 中佈建和管理帳戶

本章包含：

- 在 AWS Control Tower 中佈建和管理新成員帳戶的概觀和程序。
- 將現有 AWS 帳戶註冊到 AWS Control Tower 的概觀和程序。

如需 AWS Control Tower 中帳戶的一般資訊，請參閱 關於 AWS Control Tower AWS 帳戶 中的。如需在 AWS Control Tower 中註冊多個帳戶的資訊，請參閱 向 AWS Control Tower 註冊現有的組織單位。

> **Note**
>
> 單一帳戶佈建、更新和自訂必須以啟用 AWSControlTowerBaseline 的組織單位 (OU) 為目標。如果 OU 未啟用 AWSControlTowerBaseline，您可以啟用帳戶自動註冊，或在 EnabledBaselines 上使用 ResetEnabledBaseline 和 ResetEnabledControl APIs並在該 OU 上使用 EnabledControls 來註冊帳戶。如需 AWSControlTowerBaseline 的詳細資訊，請參閱：在 OU 層級套用的基準類型。

> **Note**
>
> 您可以同時執行最多五 (5) 個與帳戶相關的操作，包括佈建、更新和註冊。

佈建帳戶所需的許可

使用適當的使用者群組許可，佈建器可以為其組織中的任何帳戶指定標準化基準和網路組態。

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，而且您無法以根使用者身分登入。

> **Note**
>
> 佈建帳戶時，帳戶請求者一律必須擁有 `CreateAccount`和 `DescribeCreateAccountStatus`許可。此許可集是 Admin 角色的一部分，當申請者擔任

Admin 角色時會自動提供。如果您委派佈建帳戶的許可，您可能需要直接為帳戶請求者新增這些許可。

如需 AWS Control Tower 中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。

在 AWS Control Tower 內佈建帳戶

AWS Control Tower 提供多種方法來建立和更新成員帳戶。有些方法主要以主控台為基礎，有些方法主要是自動化的。

概觀

在 AWS Control Tower 中建立成員帳戶的一種標準方法是透過 Account Factory，這是一種屬於 Service Catalog 的主控台型產品。此外，在 AWS Control Tower 主控台中，如果您的登陸區域未處於偏離狀態，您可以使用建立帳戶作為佈建新帳戶的方法，以及註冊帳戶以將現有 AWS 帳戶註冊到 AWS Control Tower。

透過 Account Factory，您可以根據 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 Customization (AFC) 是一種從 AWS Control Tower 主控台佈建自訂帳戶的方式，可自動化帳戶的自訂和部署。它允許在一些一次性設定步驟之後以主控台為基礎的自動佈建，這樣就不需要編寫指令碼或設定管道。如需詳細資訊，請參閱使用帳戶工廠自訂 (AFC) 自訂帳戶。

> **自動註冊**
>
> 如果您選擇加入登陸區域設定的自動帳戶註冊功能，您也可以在 AWS Control Tower AWS 帳戶 外部建立 AWS Control Tower，並將它們移至向 AWS Control Tower 註冊的 OU，而無需建立繼承偏離。如需詳細資訊，請參閱使用自動註冊來移動和註冊帳戶。

主控台型方法：

- 透過屬於基本或自訂帳戶一部分的 Account Factory AWS Service Catalog主控台。檢閱 使用 Account Factory 佈建和管理帳戶 以取得詳細資訊和指示。
- 透過自動註冊，將帳戶從主控台移至 OU。請參閱 使用自動註冊來移動和註冊帳戶

- 如果您的登陸區域未處於偏離狀態，請透過 AWS Control Tower 中的註冊帳戶功能。請參閱 從 AWS Control Tower 主控台註冊現有帳戶。
- 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 角色的自動化帳戶佈建。
- Terraform：來自 AWS Control Tower Account Factory for Terraform (AFT)，這倚賴 Account Factory 和 GitOps 模型來允許帳戶佈建和更新自動化。請參閱 使用 AWS Control Tower Account Factory for Terraform (AFT) 佈建帳戶。
- 透過自動註冊，使用 APIs 將現有帳戶移至 OU。請參閱 使用自動註冊來移動和註冊帳戶
- AWS Control Tower 主控台中的 Account Factory 自訂：設定步驟之後，自訂帳戶的未來佈建不需要額外的組態或管道維護。帳戶是透過稱為藍圖 AWS Service Catalog 的產品來佈建。藍圖可以使用 CloudFormation 範本或 Terraform 範本。

> **Note**
>
> CloudFormation 藍圖可以將資源部署到多個區域。Terraform 藍圖只能將資源部署到單一區域。根據預設，這是主要區域。

在 AWS Control Tower 主控台中佈建帳戶

下列程序說明如何透過 AWS Control Tower 主控台，在 IAM Identity Center 中以使用者身分建立和佈建帳戶。此程序也稱為手動帳戶佈建。或者，您可以使用 AWS CLI、Service Catalog APIs 或 AWS Control Tower Account Factory for Terraform (AFT) 以程式設計方式佈建 AWS Control Tower 帳戶，或自動將現有帳戶註冊到已註冊的 OU。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。如需自訂的詳細資訊，請參閱 使用帳戶工廠自訂 (AFC) 自訂帳戶。

以使用者身分在 AWS Control Tower 主控台中個別佈建帳戶

1. 登入 AWS 並導覽至 AWS Control Tower 主控台。
2. 從左側導覽中，選擇組織以檢視組織頁面。
3. 從右上角，選擇建立資源。

4. 在下拉式選單中，選擇建立帳戶。
5. 填寫頁面上的資訊，並謹記下列事項：
   - 帳戶電子郵件必須是尚未與 建立關聯的電子郵件地址 AWS 帳戶。
   - 顯示名稱是您想要為此帳戶查看的名稱。
6. 使用 IAM Identity Center 電子郵件地址和使用者名稱，填寫欄位以定義您的存取組態。
7. 從下拉式清單中選取已註冊的 OU，以指出您要佈建帳戶的 OU。
8. 選擇性地使用預先定義的藍圖，以自訂資源佈建您的帳戶。您可以稍後執行此任務。
9. 檢閱您的帳戶選擇，然後選擇右下角的建立帳戶。
10. 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**
>
> 一次最多可佈建五個帳戶。

檢視您的帳戶

組織頁面列出組織中的所有 OUs 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，您可以個別或依 OU 群組檢視和註冊成員帳戶到 AWS Control Tower。

檢視特定帳戶

- 導覽至組織頁面。
- 您只能從右上角的下拉式選單中選擇帳戶。
- 然後，從資料表中選取您帳戶的名稱。
- 或者，您可以從資料表中選取父 OU 的名稱，並在該 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訊頁面上，您可以查看帳戶的狀態，這是下列其中一項：

- 未註冊 – 帳戶是父 OU 的成員，但不是由 AWS Control Tower 完全管理。如果父 OU 已註冊，帳戶會受到為其註冊父 OU 設定的預防性控制所管理，但 OU 的偵測性控制不適用於此帳戶。如果父 OU 未註冊，則不會套用任何控制項到此帳戶。

- 註冊 – 帳戶正由 AWS Control Tower 進行控管。我們將帳戶與父 OU 的控制組態保持一致。此程序每個帳戶資源可能需要幾分鐘的時間。
- 已註冊 – 帳戶由為其父 OU 設定的控制項管理。它由 AWS Control Tower 完全管理。
- 註冊失敗 – 帳戶無法在 AWS Control Tower 中註冊。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會註冊，但帳戶必須更新以反映最近對您環境所做的變更。若要更新單一帳戶，請導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 並一起更新這些帳戶。

關於註冊現有帳戶

當您將 AWS Control Tower 註冊到已受 AWS Control Tower 管理的組織單位 (OU) AWS 帳戶 時，您可以將 AWS Control Tower 管控擴展到現有的個人。合格帳戶存在於與 AWS Control Tower OUs 屬於相同 AWS Organizations 組織的未註冊 OU 中。

有數種方法可將帳戶註冊到 AWS Control Tower。此頁面上的資訊適用於所有註冊方法。

> **Note**
>
> 除非在初始登陸區域設定期間，否則您無法註冊現有 AWS 帳戶做為稽核或日誌封存帳戶。

帳戶註冊期間會發生什麼情況

在註冊過程中，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。
- 透過套用至整個所選 OU SCPs，將強制性控制項套用至帳戶。
- 啟用 AWS Config 並設定它來記錄帳戶中的所有資源。
- 新增將 AWS Control Tower 偵測控制項套用至帳戶的 AWS Config 規則。

帳戶和組織層級 CloudTrail 追蹤

對於登陸區域 3.1 版及更高版本，如果您已在登陸區域設定中選擇選用 AWS CloudTrail 整合：

- OU 中的所有成員帳戶都受 OU 的 AWS CloudTrail 線索管理，無論是否已註冊。
- 當您在 AWS Control Tower 中註冊帳戶時，您的帳戶會受到新組織的 AWS CloudTrail 追蹤管理。如果您有現有的 CloudTrail 追蹤部署，除非您在 AWS Control Tower 中註冊帳戶之前刪除該帳戶的現有追蹤，否則可能會看到重複費用。
- 如果您將帳戶移至已註冊的 OU，例如透過 AWS Organizations 主控台或 APIs，您可能想要移除帳戶的任何剩餘帳戶層級追蹤。如果您有現有的 CloudTrail 追蹤部署，則會產生重複的 CloudTrail 費用。

如果您更新登陸區域並選擇不接收組織層級追蹤，或您的登陸區域比 3.0 版舊，則組織層級 CloudTrail 追蹤不適用於您的帳戶。

使用 VPCs 註冊現有帳戶

當您在 Account Factory 中佈建新帳戶時，AWS Control Tower 處理 VPCs 的方式與註冊現有帳戶時不同。

- 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。
- 當您註冊現有帳戶時，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**
>
> 您可以設定 Account Factory 來變更新帳戶的預設行為，因此預設不會在 AWS Control Tower 下為組織中的帳戶設定 VPC。如需詳細資訊，請參閱在 AWS Control Tower 中建立沒有 VPC 的帳戶。

使用 AWS Config 資源註冊帳戶

要註冊的帳戶不得有現有 AWS Config 資源。請參閱註冊具有現有 AWS Config 資源的帳戶。

以下是一些範例 AWS Config CLI 命令，您可以用來判斷現有帳戶 AWS Config 資源的狀態，例如組態記錄器和交付管道。

檢視命令：

- `aws configservice describe-delivery-channels`
- `aws configservice describe-delivery-channel-status`
- `aws configservice describe-configuration-recorders`

正常回應類似 `"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`*

註冊的先決條件

本節說明如何在登陸區域設定頁面上未選取選用的自動註冊功能，或是您使用 3.1 之前的登陸區域版本操作時，在 AWS Control Tower 中註冊現有 AWS 帳戶。

在您可以註冊 AWS Control Tower AWS 帳戶 中現有的 之前，需要這些先決條件：

> **Note**
>
> 如果您已在登陸區域設定頁面中啟用 AWS Control Tower 自動註冊功能，或者您正在註冊帳戶作為註冊 OU 程序的一部分，則不需要新增`AWSControlTowerExecution`角色的先決條件。不過，在所有情況下，要註冊的帳戶可能沒有現有的 AWS Config 資源。請參閱註冊具有現有 AWS Config 資源的帳戶

1. 若要註冊現有的 AWS 帳戶，`AWSControlTowerExecution`角色必須存在於您要註冊的帳戶中。您可以檢閱註冊帳戶以取得詳細資訊和指示。
2. 除了 `AWSControlTowerExecution`角色之外， AWS 帳戶 您要註冊的現有 必須具有下列許可和信任關係。否則，註冊將會失敗。

   角色許可： `AdministratorAccess` (AWS 受管政策)

   角色信任關係：

   JSON

   ```
   {
       "Version":"2012-10-17",
       "Statement": [
           {
               "Effect": "Allow",
               "Principal": {
                   "AWS": "arn:aws:iam::111122223333:root"
               },
               "Action": "sts:AssumeRole"
           }
       ]
   }
   ```

3. 我們建議帳戶不應有 AWS Config 組態記錄器或交付管道。您可以透過 AWS CLI 刪除或修改這些項目，然後才能註冊 帳戶。否則，請檢閱註冊具有現有 AWS Config 資源的帳戶，以取得如何修改現有資源的指示。
4. 您要註冊的帳戶必須存在於與 AWS Control Tower 管理帳戶相同的 AWS Organizations 組織中。已存在的帳戶只能在已向 AWS Control Tower 註冊的 OU 中，註冊到與 AWS Control Tower 管理帳戶相同的組織。

若要檢查其他註冊先決條件，請參閱 AWS Control Tower 入門。

> **Note**
>
> 當您向 AWS Control Tower 註冊帳戶時，您的帳戶會受 AWS CloudTrail AWS Control Tower 組織的追蹤所管理。如果您有現有的 CloudTrail 追蹤部署，除非您在 AWS Control Tower 中註冊帳戶之前刪除該帳戶的現有追蹤，否則可能會看到重複費用。

關於使用 **AWSControToweRExecution**角色的受信任存取

在將現有的 註冊 AWS 帳戶 到 AWS Control Tower 之前，您必須授予 AWS Control Tower 管理或控管帳戶的許可。具體而言，AWS Control Tower 需要許可，才能 AWS Organizations 代表您在 AWS CloudFormation 和 之間建立受信任的存取，以便 CloudFormation 可以自動將堆疊部署到所選組織中的帳戶。透過此受信任的存取，`AWSControlTowerExecution`角色會執行管理每個帳戶所需的活動。因此，您必須先將此角色新增至每個帳戶，才能註冊。

啟用受信任存取時， CloudFormation 可以透過 AWS 區域 單一操作跨多個帳戶建立、更新或刪除堆疊。AWS Control Tower 依賴此信任功能，因此在將角色和許可移至已註冊的組織單位之前，可以先將角色和許可套用至現有帳戶，進而使其受到控管。

若要進一步了解受信任存取和 AWS CloudFormation StackSets，請參閱 AWS CloudFormationStackSets和 AWS Organizations 。

使用自動註冊來移動和註冊帳戶

帳戶自動註冊功能適用於 3.1 版及更高版本的登陸區域。

如果您選擇性地啟用此功能，您可以使用 AWS Organizations APIs和主控台將帳戶移至 AWS Control Tower，而無需建立繼承偏離。帳戶會自動從 AWS Control Tower 中的目的地組織單位 (OU) 接收基準資源和控制組態。如果兩個 OUs 具有相同的基準組態並啟用相同的控制項，則此選用功能也可讓您在 AWS Control Tower 內的 OUs 之間移動帳戶，而無需建立繼承偏離。

若要啟用自動註冊：您可以在 AWS Control Tower 主控台的登陸區域設定頁面上選取帳戶自動註冊，或呼叫 AWS Control Tower `CreateLandingZone`或 `UpdateLandingZone` APIs，並將 `RemediationType` 參數的值設定為繼承偏離。

若要套用自動註冊：在設定頁面中選取此選項後，您可以透過 AWS Organizations 主控台、 API AWS Organizations `MoveAccount`或 AWS Control Tower 主控台來移動帳戶。

若要使用自動註冊取消註冊帳戶：如果您將帳戶移出已註冊的 OU，AWS Control Tower 會自動移除所有部署的基準資源和控制項。

> **Note**
>
> 如果 AWS Control Tower 中的來源和目的地 OUs 已移動的成員帳戶 具有不同的組態，帳戶可能會顯示偏離。

先決條件：設定 進行自動註冊

- 您必須執行 AWS Control Tower 登陸區域 3.1 版或更新版本。
- 透過主控台中的登陸區域設定頁面或透過 AWS Control Tower 登陸區域 APIs，將 `RemediationTypes` 參數的值設定為 ，選擇加入 AWS Control Tower 自動註冊功能`Inheritance Drift`。當您選擇加入時，AWS Control Tower 會針對 `move account`的事件做出反應 AWS Organizations，並代表您立即修復已移動帳戶的繼承偏離。

所需的許可

您需要特定角色和許可才能使用 `CreateAccount` API AWS Organizations 和 `MoveAccount` API。如需 AWS Organizations 搭配 AWS Control Tower 使用 的詳細資訊，請參閱 AWS Control Tower 和 AWS Organizations 。

API 用量範例

如需這些 APIs的詳細資訊和範例，請參閱AWS Organizations 《 API 參考`MoveAccount`》中的 `CreateAccount`和 。

考量事項

- 註冊時間表：移至向 AWS Control Tower 註冊的 OU 的帳戶會使用最終一致性模型註冊。此程序通常需要幾分鐘的時間，最多幾個小時，取決於要移動的帳戶數目。
- 取消註冊程序：您可以使用相同的程序，將帳戶移至 AWS Control Tower 外部的 OU，從 AWS Control Tower 取消註冊帳戶。此程序會移除 AWS Control Tower 部署的任何角色和資源，以及 AWS Control Tower 中啟用的任何控制項。

從 AWS Control Tower 主控台註冊現有帳戶

有兩種常見方式可將個人註冊 AWS 帳戶 到 AWS Control Tower。

1. 在設定頁面中選取自動註冊功能後，您可以在 AWS Control Tower AWS 帳戶 外部建立 ，並將其直接移入已註冊的 OU。如需詳細資訊，請參閱自動移動和註冊帳戶。此選項適用於登陸區域 3.1 版和更新版本。
2. 您可以從 AWS Control Tower 主控台手動註冊現有帳戶。

下列各節說明第二個選項，不需要 AWS Control Tower 環境的先前組態。 AWS 帳戶 必須符合必要的先決條件。

在 主控台中檢視您的合格帳戶：

1. 導覽至 AWS Control Tower 中的組織頁面。
2. 尋找您要註冊的帳戶名稱。若要尋找，請從右上角的下拉式選單中選擇帳戶，然後在篩選的表格中找到帳戶名稱。

接著，請遵循註冊個別帳戶的步驟，如 手動註冊帳戶的步驟一節所示。

從主控台註冊的考量事項

- AWS Control Tower 主控台中提供的註冊帳戶功能旨在註冊現有的 ， AWS 帳戶 以便它們由 AWS Control Tower 管理。如需詳細資訊，請參閱註冊現有的 AWS 帳戶。
- 當您的登陸區域未處於偏離狀態時，可以使用主控台型註冊帳戶功能。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 或其他方法佈建新帳戶，直到您的登陸區域偏離解決為止。
- 當您從 AWS Control Tower 主控台註冊帳戶時，您必須使用已啟用`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許可，而且您無法以根使用者身分登入。
- 您註冊的帳戶可能會透過 AWS Control Tower 帳戶工廠更新，就像您更新任何其他帳戶一樣。稱為使用 AWS Control Tower 更新和移動帳戶的小節會提供更新程序。

> **Note**
>
> 當您註冊現有的 時 AWS 帳戶，請務必驗證現有的電子郵件地址。否則，可能會建立新帳戶。

手動註冊帳戶的步驟

在現有 AWS 帳戶 帳戶中具備 AdministratorAccess 存取許可 （ 政策 ） 之後，請依照下列步驟註冊帳戶：

從主控台在 AWS Control Tower 中註冊個別帳戶

- 導覽至 AWS Control Tower Organization 頁面。
- 在組織頁面上，有資格註冊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。當您在帳戶詳細資訊頁面上檢視帳戶時，這些帳戶也會顯示註冊帳戶按鈕。
- 選擇註冊帳戶時，您會看到註冊帳戶頁面，提示您將`AWSControlTowerExecution`角色新增至帳戶。如需一些說明，請參閱 手動將必要的 IAM 角色新增至現有 AWS 帳戶 並註冊。
- 接著，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)。
- 您會看到新增`AWSControlTowerExecution`角色並確認動作的模態提醒。
- 選擇註冊。
- AWS Control Tower 會開始註冊程序，系統會將您導向至帳戶詳細資訊頁面。

註冊失敗的常見原因

- 若要註冊現有帳戶，`AWSControlTowerExecution`角色必須存在於您要註冊的帳戶中。
- 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) 在您的 AWS 帳戶 主區域或 AWS Control Tower 支援的任何區域中已停用。
- 您可能會登入需要新增至帳戶工廠產品組合的帳戶 AWS Service Catalog。您必須先新增帳戶，才能存取 Account Factory，才能在 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，當您嘗試新增帳戶時，會收到錯誤。如需如何授予 AWS Service Catalog 產品組合存取權的指示，請參閱授予使用者存取權。
- 您可以 root 身分登入。
- 您嘗試註冊的帳戶可能會有剩餘的 AWS Config 設定。特別是，帳戶可能具有組態記錄器或交付管道。您必須先透過 刪除或修改這些項目， AWS CLI 才能註冊 帳戶。如需詳細資訊，請參閱註冊具有現有 AWS Config 資源的帳戶及透過 與 互動 AWS Control Tower AWS CloudShell。
- 如果帳戶屬於另一個具有管理帳戶的 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。

- 如果您的目的地 OU 的 SCPs 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 不支援資源標記。如需協助，請聯絡您的客戶代表，或 支援。

如需在建立新帳戶或註冊現有帳戶時，AWS Control Tower 如何使用角色的詳細資訊，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。如果註冊發生失敗，則不會有其他帳戶或 OUs 受到失敗的影響。

如果您不確定現有帳戶及其組態是否與 AWS Control Tower 相容，您可以遵循下一節建議的最佳實務。

建議：您可以為帳戶註冊設定雙步驟方法

- 首先，使用 AWS Config 一致性套件來評估您的帳戶可能如何受到某些 AWS Control Tower 控制項的影響。若要判斷註冊 AWS Control Tower 如何影響您的帳戶，請參閱使用一致性套件擴展 AWS Control Tower AWS Config 控管。
- 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 登陸區域，您可能需要移除為評估建立的 AWS Config 交付管道和組態記錄器。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 註冊OUs 中的情況，但工作負載會在沒有 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 AWS Control Tower 未部署區域中現有的帳戶中的資源。

如果帳戶不符合先決條件

請記住，作為先決條件，符合 AWS Control Tower 控管資格的帳戶必須屬於相同的整體組織。若要滿足帳戶註冊的此先決條件，您可以遵循這些準備步驟，將帳戶移至與 AWS Control Tower 相同的組織。

將帳戶帶入與 AWS Control Tower 相同的組織的準備步驟

1. 從現有組織捨棄帳戶。如果您使用此方法，則必須提供單獨的付款方式。
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。帳戶會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。 會建立 SCPs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。

滿足其餘先決條件的步驟：

1. 建立必要的`AWSControlTowerExecution`角色。
2. 清除預設 VPC。（此部分為選用。 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 組態記錄器或交付管道 AWS CLI AWS CloudShell。如需詳細資訊，請參閱 使用 AWS Config 資源註冊帳戶 和 註冊具有現有 AWS Config 資源的帳戶

完成這些準備步驟後，您可以將帳戶註冊到 AWS Control Tower。如需詳細資訊，請參閱手動註冊帳戶的步驟。此步驟會將帳戶納入完整的 AWS Control Tower 控管。

取消佈建帳戶的選用步驟，以便註冊並保留其堆疊

1. 若要保留套用的 CloudFormation 堆疊，請從堆疊集中刪除堆疊執行個體，然後選擇保留執行個體的堆疊。
2. 終止帳戶工廠中的 AWS Service Catalog 帳戶佈建產品。（此步驟只會從 AWS Control Tower 移除佈建的產品。 它不會刪除帳戶。）

3. 視需要為不屬於組織的任何帳戶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。（您這樣做，因此帳戶不會計入 AWS Organizations 配額中的總計。）
4. 如果資源仍然存在，請清除帳戶，然後遵循中的帳戶關閉步驟將其關閉取消註冊 帳戶。
5. 如果您有已定義控制項的暫停 OU，您可以在該處移動帳戶，而不是執行步驟 1。

手動將必要的 IAM 角色新增至現有 AWS 帳戶 並註冊

如果您已設定 AWS Control Tower 登陸區域，您可以開始將組織的帳戶註冊到向 AWS Control Tower 註冊的 OU。如果您尚未設定登陸區域，請遵循《 入門》中的 AWS Control Tower 使用者指南，步驟 2 中所述的步驟。 https://docs.aws.amazon.com/controltower/latest/userguide/getting-started-with-control-tower.html#step-two登陸區域準備就緒後，請完成下列步驟，以手動方式將現有帳戶納入 AWS Control Tower 的控管。

請務必檢閱本章先前註冊的先決條件記下的 。

向 AWS Control Tower 註冊帳戶之前，您必須授予 AWS Control Tower 管理該帳戶的許可。若要這樣做，您將新增具有帳戶完整存取權的角色，如以下步驟所示。您必須為您註冊的每個帳戶執行這些步驟。

對於每個帳戶：

步驟 1：使用管理員存取權登入目前包含您要註冊之帳戶的組織的管理帳戶。

例如，如果您從 建立此帳戶， AWS Organizations 並使用跨帳戶 IAM 角色登入，則可以遵循下列步驟：

1. 登入組織的管理帳戶。
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. 開啟頂端導覽列上的帳戶下拉式選單，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戶時定義的。如果您在建立帳戶時未指定角色名稱，請輸入預設角色名稱 `OrganizationAccountAccessRole`。

6. 選擇 Switch Role (切換角色)。
7. 您現在應該以子帳戶 AWS 管理主控台 身分登入 。
8. 完成後，請保留在子帳戶中以進行程序的下一個部分。
9. 請記下管理帳戶 ID，因為您需要在下一個步驟中輸入它。

步驟 2：授予 AWS Control Tower 管理帳戶的許可。

1. 前往 IAM。
2. 前往 角色。
3. 選擇建立角色。
4. 當系統要求選取角色適用的服務時，請選擇自訂信任政策。
5. 複製此處顯示的程式碼範例，並貼到政策文件中。將字串取代*Management Account ID*為您管理帳戶的實際管理帳戶 ID。以下是要貼上的政策：

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```

6. 當系統要求連接政策時，請選擇 AdministratorAccess。
7. 選擇 Next: Add Tags (下一步：新增標籤)。
8. 您可能會看到名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. 在檢閱畫面上的角色名稱欄位中，輸入 AWSControlTowerExecution。
10. 在描述方塊中輸入簡短描述，例如允許註冊的完整帳戶存取權。
11. 選擇建立角色。

步驟 3：將帳戶移至已註冊的 OU 來註冊帳戶，並驗證註冊。

建立角色以設定必要的許可之後，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選單中選擇註冊。
   - 請遵循註冊個別帳戶的步驟，如 手動註冊帳戶的步驟 頁面所示。
3. 驗證註冊。
   - 從 AWS Control Tower，選擇左側導覽中的組織。
   - 尋找您最近註冊的帳戶。其初始狀態會顯示註冊狀態。
   - 當狀態變更為已註冊時，移動成功。

若要繼續此程序，請登入組織中您要在 AWS Control Tower 註冊的每個帳戶。為每個帳戶重複先決條件步驟和註冊步驟。

新增**AWSControlTowerExecution**角色的範例

下列 YAML 範本可協助您在帳戶中建立所需的角色，以便以程式設計方式註冊。

```
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 資源的帳戶

本主題提供step-by-step方法，說明如何註冊具有現有 AWS Config 資源的帳戶。如需如何檢查現有資源的範例，請參閱 使用 AWS Config 資源註冊帳戶。

AWS Config 資源的範例

以下是您的帳戶可能已有的一些 AWS Config 資源類型。您可能需要修改這些資源，才能將您的帳戶註冊到 AWS Control Tower。

- AWS Config 記錄器
- AWS Config 交付管道
- AWS Config 彙總授權

限制

- 登陸區域中設定的管理帳戶或服務整合帳戶不支援使用現有的 AWS Config 資源註冊帳戶 (AWS Config)。
- 只能使用啟用 的 OU 註冊或重新註冊工作流程來註冊帳戶`AWSControlTowerBaseline`。無法透過啟用或停用 來註冊帳戶`ConfigBaseline`。
- 不支援具有現有 AWS Config 資源的帳戶使用自動註冊來移動和註冊帳戶。
- 如果修改資源並在帳戶上建立偏離，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。

前提

- 您已部署 AWS Control Tower 登陸區域。
- 您的帳戶尚未向 AWS Control Tower 註冊。

- 您的帳戶在至少一個由 AWS Control Tower 管理的區域中至少有一個預先存在 AWS Config 的資源。
- 您的帳戶未處於控管偏離狀態。

> **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，則註冊將會失敗。之後，如果您隨後嘗試將相同帳戶新增至允許清單，AWS Control Tower 就無法驗證帳戶是否已正確佈建。您必須從 AWS Control Tower 取消佈建帳戶，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，則會導致控管偏離，這也會防止帳戶新增至允許清單。

如需描述使用現有 AWS Config 資源註冊帳戶的自動化方法的部落格，請參閱將具有現有 AWS Config 資源的帳戶註冊自動化到 AWS Control Tower。

此程序有 5 個主要步驟。

1. 將帳戶新增至 AWS Control Tower 允許清單 (AWS Control Tower)。
2. 在帳戶中建立新的 IAM 角色。
3. 修改預先存在 AWS Config 的資源。
4. 在資源不存在的 AWS 區域中建立 AWS Config 資源。
5. 向 AWS Control Tower 註冊帳戶。

在繼續之前，請考慮下列有關此程序的期望。

- 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 AWS Config 的資源，包括新的 IAM 角色。
- 如果在註冊後對 AWS Config 資源進行任何變更，則必須更新這些資源以符合 AWS Control Tower 設定，才能重新註冊帳戶。

步驟 1：聯絡支援，將 account（帳戶）新增至允許清單

在票證主旨行中包含此片語：

將具有現有 AWS Config 資源的帳戶註冊至 AWS Control Tower

在票證內文中包含下列詳細資訊：

- 管理帳戶號碼
- 具有現有 AWS Config 資源的成員帳戶的帳號。您可以為要註冊的所有帳戶建立支援案例。
- 您為 AWS Control Tower 設定選取的主區域

> **Note**
>
> 將您的帳戶新增至允許清單所需的時間為 2 個工作天。

步驟 2：在成員帳戶中建立新的 IAM 角色

1. 開啟成員帳戶的 CloudFormation 主控台。
2. 使用下列範本建立新的堆疊

```
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. 將堆疊的名稱提供為 CustomerCreatedConfigRecorderRoleForControlTower
4. 建立堆疊。

> **Note**
>
> 您建立的任何 SCPs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許可。
> 請遵循這些準則，以便在您擁有`aws-controltower-ConfigRecorderRole*`封鎖呼叫 Config SCPs `AccessDeniedException`時，不會收到 。

步驟 3：使用預先存在的資源識別 AWS 區域

對於帳戶中的每個受管區域 (AWS Control Tower 受管），識別並記下至少具有先前顯示之其中一個現有 AWS Config 資源範例類型的區域。

步驟 4：識別沒有任何 AWS Config 資源 AWS 的區域

對於帳戶中的每個受管區域 (AWS Control Tower 受管），識別並記下先前顯示的範例類型沒有 AWS Config 資源的區域。

步驟 5：修改每個區域中的現有資源 AWS

在此步驟中，需要有關 AWS Control Tower 設定的下列資訊。

- `AUDIT_ACCOUNT` - AWS Config 服務整合帳戶 （先前稱為稽核帳戶） ID
- `CONFIG_BUCKET` - AWS Config 交付組態快照和組態歷史記錄檔案的 AWS S3 儲存貯體。找到並確認 AWS S3 儲存貯體存在，然後再繼續進行後續步驟。
  - 對於登陸區域 3.3 版或更低版本，AWS S3 儲存貯體名為 `aws-controltower-logs-LOGGING_ACCOUNT-HOME_REGION`，位於記錄帳戶中。
  - 對於登陸區域 4.0 版或更新版本，AWS S3 儲存貯體名為 `aws-controltower-config-logs-AUDIT_ACCOUNT-<REGION_STRING>-<SUFFIX_STRING>`，位於 AWS Config 服務整合帳戶（先前稱為稽核帳戶）。
- `IAM_ROLE_ARN` - 在步驟 2 中建立的 IAM 角色 ARN
- `ORGANIZATION_ID` - 管理帳戶的組織 ID
- `MEMBER_ACCOUNT_NUMBER` - 正在修改的成員帳戶
- `HOME_REGION` - AWS Control Tower 設定的主區域。

按照以下第 5a 至 5c 節中的指示修改每個現有資源。

步驟 5a. AWS Config recorder 資源

每個 AWS 區域只能存在一個 AWS Config 記錄器。如果存在，請修改設定，如下所示。在主區域中將項目取代GLOBAL_RESOURCE_RECORDING為 true。對於存在 AWS Config 記錄器的其他區域，以 false 取代項目。

- 名稱：請勿變更
- RoleARN： IAM_ROLE_ARN
  - RecordingGroup：
  - AllSupported： true
  - IncludeGlobalResourceTypes： GLOBAL_RESOURCE_RECORDING
  - ResourceTypes：空

您可以使用下列命令，透過 AWS CLI 進行此修改。將字串取代RECORDER_NAME為現有的 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 5b。修改 AWS Config 交付管道資源

每個區域只能有一個 AWS Config 交付管道。如果存在另一個設定，請修改設定，如下所示。

- 名稱：請勿變更
- ConfigSnapshotDeliveryProperties：TwentyFour_Hours
- S3BucketName：*CONFIG_BUCKET*
- S3KeyPrefix：*ORGANIZATION_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

您可以使用下列命令，透過 AWS CLI 進行此修改。將字串取代*DELIVERY_CHANNEL_NAME*為現有的 AWS Config 記錄器名稱。

```
aws configservice put-delivery-channel --delivery-channel
 name=DELIVERY_CHANNEL_NAME,s3BucketName=CONFIG_BUCKET,s3KeyPrefix="ORGANIZATION_ID",configSnap
controltower-AllConfigNotifications --region CURRENT_REGION
```

步驟 5c：修改 AWS Config 彙總授權資源

> **Note**
>
> 登陸區域 4.0 版或更新版本不需要此步驟。

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 的主區域指定為授權區域。如果不存在，請使用下列設定建立新的設定：

- AuthorizedAccountId：稽核帳戶 ID
- AuthorizedAwsRegion：AWS Control Tower 設定的主區域

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

修訂 CloudFormation 範本，以便在您的主區域中，IncludeGlobalResourcesTypes 參數具有值 GLOBAL_RESOURCE_RECORDING，如以下範例所示。另請更新範本中的必要欄位，如本節所指定。

將主區域中的項目取代GLOBAL_RESOURCE_RECORDING為 true。對於 AWS Config 記錄器不存在的其他區域，以 false 取代項目。

1. 導覽至管理帳戶的 CloudFormation 主控台。
2. 使用名稱 CustomerCreatedConfigResourcesForControlTower 建立新的 StackSet。
3. 複製並更新下列範本：

> **Note**
>
> 登陸區域 4.0 版或更新版本不需要範本中的CustomerCreatedAggregationAuthorization資源。

```
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::${AWS::AccountId}:role/aws-controltower-
ConfigRecorderRole-customer-created
      RecordingGroup:
        AllSupported: true
        IncludeGlobalResourceTypes: GLOBAL_RESOURCE_RECORDING
        ResourceTypes: []
  CustomerCreatedConfigDeliveryChannel:
    Type: AWS::Config::DeliveryChannel
    Properties:
      Name: aws-controltower-BaselineConfigDeliveryChannel-customer-created
      ConfigSnapshotDeliveryProperties:
        DeliveryFrequency: TwentyFour_Hours
      S3BucketName: CONFIG_BUCKET
      S3KeyPrefix: ORGANIZATION_ID
      SnsTopicARN: !Sub arn:aws:sns:${AWS::Region}:AUDIT_ACCOUNT:aws-controltower-
AllConfigNotifications
  CustomerCreatedAggregationAuthorization:
    Type: "AWS::Config::AggregationAuthorization"
    Properties:
      AuthorizedAccountId: AUDIT_ACCOUNT
      AuthorizedAwsRegion: HOME_REGION
```

使用必要欄位更新範本：

a. 在 S3BucketName 欄位中，取代 *CONFIG_BUCKET*

b. 在 S3KeyPrefix 欄位中，取代 *ORGANIZATION_ID*

c. 在 SnsTopicARN 欄位中，取代 *AUDIT_ACCOUNT*

d. 在 AuthorizedAccountId 欄位中，取代 *AUDIT_ACCOUNT*

e. 在 AuthorizedAwsRegion 欄位中，取代 *HOME_REGION*

4. 在 CloudFormation 主控台上部署期間，新增成員帳戶號碼。
5. 新增步驟 4 中識別 AWS 的區域。
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**
>
> 此任務的註冊帳戶工作流程將不會成功。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

> **Note**
>
> 單一帳戶佈建、更新和自訂必須以啟用 AWSControlTowerBaseline 的組織單位 (OU) 為目標。如果 OU 未啟用 AWSControlTowerBaseline，您可以啟用帳戶自動註冊，或在 EnabledBaselines 上使用 ResetEnabledBaseline 和 ResetEnabledControl APIs並在該 OU 上使用 EnabledControls 來註冊帳戶。如需 AWSControlTowerBaseline 的詳細資訊，請參閱：在 OU 層級套用的基準類型。

本章包含使用 Account Factory 在 AWS Control Tower 登陸區域中佈建新成員帳戶的概觀和程序。

設定和佈建帳戶的許可

AWS Control Tower 帳戶工廠可讓 中的雲端管理員和使用者在您的登陸區域中 AWS IAM Identity Center 佈建帳戶。根據預設，佈建帳戶的 IAM Identity Center 使用者必須位於 `AWSAccountFactory`群組或 管理群組中。

> **Note**
>
> 從管理帳戶工作時，請小心謹慎，就像使用整個組織中具有許可的任何帳戶一樣。

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，包括一些自動帳戶設定。如需`AWSControlTowerExecution`角色的詳細資訊，請參閱角色和帳戶。

> **Note**
>
> 若要在 AWS Control Tower AWS 帳戶 中註冊現有的 ，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，請參閱關於註冊現有帳戶。

如需許可的詳細資訊，請參閱「佈建帳戶所需的許可」。

在 Account Factory 中管理帳戶的考量事項

您可以更新、取消註冊和關閉透過 Account Factory 建立和佈建的帳戶。您可以透過更新要重新利用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 提供的帳戶相關聯的佈建產品時，如果您指定新的使用者電子郵件地址 AWS IAM Identity Center，AWS Control Tower 會在 IAM Identity Center 中建立新的使用者。先前建立的帳戶不會移除。如需有關從 IAM Identity Center 移除先前 IAM Identity Center 使用者電子郵件地址的資訊，請參閱停用使用者。

使用 AWS Control Tower 更新和移動帳戶

更新已註冊帳戶的最簡單方法是透過 AWS Control Tower 主控台。個別帳戶更新有助於解決偏離，例如 已移動的成員帳戶。帳戶更新也是完整登陸區域更新的一部分。

在 主控台中更新帳戶

在 AWS Control Tower 主控台中更新帳戶

1. 登入 AWS Control Tower 時，導覽至組織頁面。
2. 在 OUs和帳戶清單中，選取您要更新的帳戶名稱。可供更新的帳戶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資訊頁面。
4. 在右上角，選擇更新帳戶。

如果您將帳戶從一個組織單位 (OU) 移至另一個組織單位，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 中的控制項符合您帳戶的政策需求。

AWS Control Tower 帳戶修改方式不同，取決於您是否已選擇加入帳戶自動註冊。如需自動註冊的詳細資訊，請參閱 選擇性地設定帳戶的自動註冊。

在帳戶之間移動時的控制行為
OUs啟用自動註冊

當您將帳戶移至新的 OU 時，AWS Control Tower 會將 OU 啟用的基準和控制項套用至帳戶。會移除先前 OU 的控制項和基準。如果您將帳戶移出已註冊的 OU，AWS Control Tower 會移除所有部署的基準和控制項。

在帳戶之間移動時的控制行為
OUs，不含自動註冊

當您在 OUs 之間移動帳戶時，目的地 OU 的控制項會套用至
帳戶。不過，從先前 OU 套用到帳戶的控制項不是
已移除。控制項的確切行為專屬於 的實作
控制項在先前的 OU 和目的地 OU 上處於作用中狀態。

- 對於使用 AWS Config 規則實作的控制項：先前 OU 的控制項
  不會移除。這些控制項必須手動移除。
- 對於使用 SCPs控制項：先前 OU 的 SCP 型控制項為
  已移除。目的地 OU 的 SCP 型控制項會在此帳戶上生效。
- 對於使用 CloudFormation 勾點實作的控制項：此行為
  取決於新 OU 中控制項的狀態。
  - 如果目的地 OU 沒有作用中的勾點型控制項：舊的

控制項會保持移動帳戶的作用中狀態，除非您移除它們手動。

- 如果目的地 OU 已啟用勾點控制：舊控制項為已移除，且目的地 OU 中的控制項會套用至帳戶。

變更已註冊帳戶的電子郵件地址

若要變更 AWS Control Tower 中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、日誌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 AWS 帳戶相關聯的電子郵件地址？或聯絡 AWS Support。

變更 AWS Control Tower 建立之帳戶的電子郵件地址

1. 復原帳戶的根使用者密碼。您可以遵循文章中的步驟，如何復原遺失或忘記 AWS 的密碼？
2. 使用根使用者密碼登入帳戶。
3. 像對任何其他地址一樣變更電子郵件地址 AWS 帳戶，並等待變更反映 AWS Organizations。當電子郵件地址變更完成更新時，您可能會遇到延遲。
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。更新佈建產品的程序包括將新電子郵件地址與佈建產品建立關聯。如此一來，電子郵件地址變更就會在 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。

若要變更您使用 建立之成員帳戶的密碼或電子郵件地址 AWS Organizations，請參閱AWS Organizations 《 使用者指南》中的以根使用者的身分存取成員帳戶。

或者，您可以從 AWS Organizations 主控台更新 Account Factory 或其他成員帳戶的電子郵件地址，而無需以根使用者身分登入。如需詳細資訊，請參閱AWS Organizations 《 使用者指南》中的使用 更新成員帳戶的根使用者電子郵件地址 AWS Organizations。

變更已註冊帳戶的名稱

請依照本節中的程序，變更已註冊 AWS Control Tower 帳戶的名稱。

> **Note**
>
> 若要變更 AWS 管理員帳戶的名稱，您必須擁有管理員許可，並以帳戶的根使用者身分登入。

使用 AWS Organizations 主控台或 APIs 變更 AWS Control Tower 建立的帳戶名稱

- 遵循 AWS 帳戶管理參考指南中的指示。

變更 AWS Control Tower 所建立帳戶名稱的替代方法

1. 復原帳戶的根密碼。您可以遵循本文概述的步驟，如何復原遺失或忘記 AWS 的密碼？
2. 使用根密碼登入 帳戶。
3. 在 AWS Billing 主控台中，導覽至帳戶設定頁面。
4. 變更帳戶設定中的名稱，就像對任何其他設定一樣 AWS 帳戶。
5. AWS Control Tower 會自動自我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 Virtual Private Cloud 設定帳戶工廠

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。

在帳戶工廠頁面上，您可以看到組織單位 (OUs及其允許清單狀態的清單。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。您可以停用透過 進行帳戶佈建的特定 OUs AWS Service Catalog。

您可以檢視最終使用者在佈建新帳戶時可用的 Amazon VPC 組態選項。

在 Account Factory 中設定 Amazon VPC 設定

1. 身為中央雲端管理員，請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，請選取編輯並檢視您 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 中的私有子網路數量上限。根據預設，選取 1。每個可用區域允許的私有子網路數量上限為 2。
- 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 區塊提供 Account Factory 為您的帳戶建立之 VPC 的整體子網路 IP 地址範圍。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。

取消註冊 帳戶

如果您在 Account Factory 中建立帳戶或註冊 AWS 帳戶，而且您不再希望帳戶由登陸區域中的 AWS Control Tower 管理，您可以從 AWS Control Tower 主控台取消註冊帳戶。

當您取消註冊 AWS Control Tower 帳戶時，會移除 AWS Control Tower 佈建的所有資源，包括任何控制項和藍圖。帳戶會從任何 AWS Control Tower OU 移至根區域。帳戶不再是已註冊 OU 的一部分，也不再受 AWS Control Tower SCPs的約束。您可以透過 關閉帳戶 AWS Organizations。

從 AWS Control Tower 主控台取消註冊已註冊的帳戶

1. 在 的網頁瀏覽器中開啟 AWS Control Tower 主控台 https://console.aws.amazon.com/controltower
2. 在左側導覽窗格中，選擇組織。
3. 在組織頁面中，選取 OU 附近的 + 按鈕，展開包含帳戶的 OU。
4. 選取帳戶，然後選擇取消管理。

> **Note**
>
> 等待帳戶的狀態顯示未註冊。

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

> **自動註冊處於作用中狀態時取消註冊帳戶**
>
> 如果您的設定頁面中的自動註冊功能處於作用中狀態，您也可以將帳戶移至未在 AWS Control Tower 中註冊的 OU 來取消註冊帳戶。所有 AWS Control Tower 資源都會移除。請注意，您不會以這種方式意外取消註冊帳戶。不過，您可以透過將其傳回 OU 來重新註冊帳戶。

當您取消註冊自訂帳戶時，AWS Control Tower 會移除登陸區域已部署的資源，以及 AWS Control Tower 在帳戶中建立的任何其他資源。AWS Control Tower 也會移除 AWSControlTowerExecution 角色，即使已手動新增。移除此角色符合最低權限原則，因為服務執行角色不應保留在未受管帳戶中。

取消註冊帳戶後，您可以透過 關閉帳戶 AWS Organizations。

> **Note**
>
> 未註冊的帳戶不會關閉或刪除。取消註冊帳戶後，您在 Account Factory 中建立帳戶時選取的 IAM Identity Center 使用者仍然具有帳戶的管理存取權。如果您不希望此使用者具有管理存取權，則必須更新帳戶工廠中的帳戶並變更帳戶的 IAM Identity Center 使用者電子郵件地址，以在 IAM Identity Center 中變更此設定。如需詳細資訊，請參閱使用 AWS Control Tower 更新和移動帳戶。

影片演練

此影片 (3：25) 說明如何從 AWS Control Tower 移除帳戶、取得帳戶的根存取權，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。

您可以檢視說明 AWS Control Tower 中常見任務的 AWS YouTube 影片清單。

關閉在 Account Factory 中建立的帳戶

在 Account Factory 中建立的帳戶為 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 AWS 帳戶 與從 AWS Control Tower 取消註冊帳戶不同，這些是個別的動作。您必須先取消註冊帳戶，才能將其關閉。

透過 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，而無需使用根登入資料個別登入每個成員帳戶 AWS Organizations。不過，您無法以這種方式關閉管理帳戶。

當您呼叫 AWS Organizations CloseAccount API 或在 AWS Organizations 主控台中關閉帳戶時，成員帳戶會隔離 90 天，如同任何 AWS 帳戶 一樣。帳戶會在 AWS Control Tower 和 中顯示暫停狀態 AWS Organizations。如果您在該 90 天內嘗試使用帳戶，AWS Control Tower 會提供錯誤訊息。

> **Note**
>
> 如果 OU 已暫停帳戶，則目標上的區域控制項的 EnabledControl 操作將會失敗。

在 90 天過期之前，您可以還原成員帳戶，就像使用任何 一樣 AWS 帳戶。在 90 天之後，會移除帳戶的記錄。

根據最佳實務，建議您先取消註冊成員帳戶，再關閉該帳戶。如果您在未先取消管理的情況下關閉成員帳戶，AWS Control Tower 會將帳戶的狀態顯示為已暫停，但也顯示為已註冊。因此，如果您嘗試在該 90 天時間內重新註冊帳戶的 OU，AWS Control Tower 會產生錯誤訊息。暫停的帳戶基本上會封鎖重新註冊動作並發生預先檢查失敗。如果您從 OU 移除帳戶，您可以重新註冊 OU，但 AWS 可能會產生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**
>
> 如果您在關閉帳戶之前未取消註冊帳戶，您必須在 AWS Service Catalog 這 90 天完成後刪除中的帳戶佈建產品。

如需詳細資訊，請參閱 CloseAccount API AWS Organizations 的文件。

Account Factory 的資源考量事項

使用 Account Factory 佈建帳戶時，會在帳戶內建立下列 AWS 資源。

AWS 服務	Resource Type (資源類型)	資源名稱
AWS CloudFormation	堆疊	StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL-* StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-* StackSet-AWSControlTowerBP-BASELINE-CONFIG-* StackSet-AWSControlTowerBP-BASELINE-ROLES-* StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES-*
AWS CloudTrail	追蹤	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch 事件規則	aws-controltower-ConfigComplianceChangeEventRule
Amazon CloudWatch	CloudWatch Logs	aws-controltower/CloudTrailLogs /aws/lambda/aws-controltower-NotificationForwarder

AWS 服務	Resource Type (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
Amazon EventBridge	規則	AWSControlTowerManagedRule
Amazon EventBridge	規則	aws-controltower-ConfigComplianceChangeEventRule

使用帳戶工廠自訂 (AFC) 自訂帳戶

> **Note**
>
> 單一帳戶佈建、更新和自訂必須以啟用 AWSControlTowerBaseline 的組織單位 (OU) 為目標。如果 OU 未啟用 AWSControlTowerBaseline，您可以啟用帳戶自動註冊，或在 EnabledBaselines 上使用 ResetEnabledBaseline 和 ResetEnabledControl APIs並在該 OU 上使用 EnabledControls 來註冊帳戶。如需 AWSControlTowerBaseline 的詳細資訊，請參閱：在 OU 層級套用的基準類型。

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 Account Factory 自訂後，AWS Control Tower 會自動執行此程序以供未來佈建，因此您不需要維護任何管道。自訂帳戶可在佈建資源後立即使用。

使用藍圖佈建新帳戶

您的自訂帳戶是在 AWS Control Tower 帳戶工廠、透過 CloudFormation 範本或使用 Terraform 佈建。您將定義做為自訂帳戶藍圖的範本。您的藍圖說明您在佈建帳戶時所需的特定資源和組態。也提供由 AWS 合作夥伴建置和管理的預先定義藍圖。如需合作夥伴管理藍圖的詳細資訊，請參閱 AWS Service Catalog 入門程式庫。

將藍圖套用至現有帳戶

您也可以遵循 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，請參閱在 主控台中更新帳戶。

定義：您的中樞帳戶

您的帳戶藍圖會存放在 中 AWS 帳戶，基於我們的目的稱為中樞帳戶。藍圖會以 Service Catalog 產品的形式儲存。我們將此產品稱為藍圖，以區分它與任何其他 Service Catalog 產品。若要進一步了解如何建立 Service Catalog 產品，請參閱《 AWS Service Catalog 管理員指南》中的建立產品。

> **Note**
>
> AWS Control Tower 包含主動控制，可監控 AWS Control Tower 中的 CloudFormation 資源。或者，您可以在登陸區域中啟用這些控制項。當您套用主動控制時，他們會檢查以確保您要部署到帳戶的資源符合組織的政策和程序。如需主動控制的詳細資訊，請參閱主動控制。

如需使用 AFC 的詳細資訊，請參閱使用 AWS Control Tower 中的帳戶工廠自訂自動化帳戶自訂。

> **先決條件**
>
> 開始使用 AWS Control Tower 帳戶工廠建立自訂帳戶之前，您必須部署 AWS Control Tower 登陸區域環境，而且必須擁有向 AWS Control Tower 註冊的組織單位 (OU)，其中將放置新建立的帳戶。

自訂的準備

- 指定中樞帳戶：您可以建立新的帳戶做為中樞帳戶，也可以使用現有的 AWS 帳戶。我們強烈建議您不要使用 AWS Control Tower 管理帳戶做為藍圖中樞帳戶。
- 新增必要的角色：如果您計劃 AWS 帳戶 註冊 AWS Control Tower 並自訂這些角色，您必須先將`AWSControlTowerExecution`角色新增至這些帳戶，就像註冊 AWS Control Tower 的任何其他帳戶一樣。
- 設定合作夥伴藍圖 （選用）：如果您計劃使用具有市場訂閱需求的合作夥伴藍圖，您必須先從 AWS Control Tower 管理帳戶設定這些藍圖，才能將合作夥伴藍圖部署為帳戶原廠自訂藍圖。

主題

設定自訂

下一節提供為自訂程序設定 Account Factory 的步驟。建議您在開始這些步驟之前，先設定中樞帳戶的委派管理員。

摘要

- 步驟 1. 建立必要的角色。建立 IAM 角色，授予 AWS Control Tower 存取（中樞）帳戶的許可，其中存放 Service Catalog 產品，也稱為藍圖。
- 步驟 2. 建立 AWS Service Catalog 產品。建立自訂帳戶基礎所需的 AWS Service Catalog 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 AWS Service Catalog 的產品（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 中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

開始自訂帳戶之前，您必須設定包含 AWS Control Tower 與中樞帳戶之間信任關係的角色。擔任 時，該角色會授予 AWS Control Tower 管理中樞帳戶中資源的存取權。角色必須命名為 AWSControlTowerBlueprintAccess。

AWS Control Tower 會擔任此角色來代表您在 中建立產品組合資源 AWS Service Catalog，然後將您的藍圖做為服務型錄產品新增至此產品組合，然後在帳戶佈建期間與成員帳戶共用此產品組合和藍圖。

您將建立`AWSControlTowerBlueprintAccess`角色，如以下各節所述。您可以在已註冊或未註冊帳戶中設定角色。

> 導覽至 IAM 主控台以設定所需的角色。

在已註冊的 AWS Control Tower 帳戶中設定 AWSControlTowerBlueprintAccess 角色

1. 聯合或以 AWS Control Tower 管理帳戶中的委託人身分登入。
2. 從管理帳戶中的聯合委託人，擔任或切換角色到您選擇做為藍圖中樞帳戶的已註冊 AWS Control Tower 帳戶中`AWSControlTowerExecution`的角色。
3. 從已註冊 AWS Control Tower 帳戶中`AWSControlTowerExecution`的角色，建立具有適當許可和信任關係`AWSControlTowerBlueprintAccess`的角色。

> **Important**
>
> 為了遵循 AWS 最佳實務指引，請務必在建立AWSControlTowerExecution角色後立即登出AWSControlTowerBlueprintAccess角色。
> 為避免意外變更資源，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角色將不會存在於帳戶中，而且在您繼續設定角色之前，不需要擔任該AWSControlTowerBlueprintAccess角色。

在未註冊的成員帳戶中設定 AWSControlTowerBlueprintAccess 角色

1. 透過您偏好的方法，聯合或登入為您要指定為中樞帳戶之帳戶中的委託人。
2. 以帳戶中的委託人身分登入時，請建立具有適當許可和信任關係AWSControlTowerBlueprintAccess的角色。

必須設定 AWSControlTowerBlueprintAccess 角色，才能將信任授予兩個委託人：

- 在 AWS Control Tower 管理帳戶中執行 AWS Control Tower 的委託人（使用者）。
- AWS Control Tower 管理帳戶中名為 AWSControlTowerAdmin 的角色。

以下是信任政策範例，類似於您需要為角色包含的政策。此政策示範授予最低權限存取權的最佳實務。當您制定自己的政策時，請將該術語取代為 AWS Control Tower 管理帳戶*YourManagementAccountId*的實際帳戶 ID，並將該術語取代*YourControlTowerUserRole*為管理帳戶的 IAM 角色識別符。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
```

```
                    "arn:aws:iam::111122223333:role/service-role/
AWSControlTowerAdmin",
                    "arn:aws:iam::111122223333:role/YourControlTowerUserRole"
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

必要的許可政策

AWS Control Tower 要求名為 的受管政策AWSServiceCatalogAdminFullAccess必須連接到AWSControlTowerBlueprintAccess角色。此政策提供許可，在允許 AWS Control Tower 管理您的產品組合和 AWS Service Catalog 產品資源 AWS Service Catalog 時尋找 。您可以在 IAM 主控台中建立角色時連接此政策。

可能需要其他許可

- 如果您在 Amazon S3 中存放藍圖，AWS Control Tower 也需要該AWSControlTowerBlueprintAccess角色的AmazonS3ReadOnlyAccess許可政策。
- 如果您不使用預設的管理員政策， AWS Service Catalog Terraform 產品類型會要求您將一些額外的許可新增至 AFC 自訂 IAM 政策。除了建立您在 terraform 範本中定義的資源所需的許可之外，還需要這些許可。

步驟 2. 建立 AWS Service Catalog 產品

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的步驟。建立 AWS Service Catalog 產品時，您會將帳戶藍圖新增為範本。

Important

由於 HashiCorp 更新的 Terraform 授權，將對 Terraform Open Source 產品和佈建產品的支援 AWS Service Catalog 變更為新的產品類型，稱為 External。若要進一步了解此變更如何影響 AFC，包括如何將現有帳戶藍圖更新為外部產品類型，請檢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 CloudFormation 範本或 Terraform tar.gz 組態檔案。本節稍後會提供一些範本範例。
- 登入您存放 Account Factory 藍圖的 AWS 帳戶 （有時稱為中樞帳戶）。
- 導覽至 AWS Service Catalog 主控台。選擇產品清單，然後選擇上傳新產品。
- 在產品詳細資訊窗格中，輸入藍圖產品的詳細資訊，例如名稱和描述。
- 選取使用範本檔案，然後選取選擇檔案。選取或貼上您開發或下載以用作藍圖的範本或組態檔案。
- 選擇主控台頁面底部的建立產品。

您可以從 AWS Service Catalog 參考架構儲存庫下載 CloudFormation 範本。該儲存庫的一個範例有助於為您的 資源設定備份計劃。

以下是一個範例範本，適用於名為 Best Pets 的虛構公司。它有助於設定與其寵物資料庫的連線。

```
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: nodejs22.x
      Handler: index.handler
      Timeout: 5
      Code:
```

```
        ZipFile: >
           export const handler = async (event, context) => {
             const awsAccountId = context.invokedFunctionArn.split(":")[4]
             const connectionString= "fake connection for account " + awsAccountId;
             const response = {
               statusCode: 200,
               body: connectionString
             };
            return response;
           };

  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 主控台中檢視您的藍圖。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

當您遵循 AWS Control Tower 主控台中的建立帳戶工作流程時，您會看到一個選用區段，您可以在其中輸入要用於自訂帳戶之藍圖的相關資訊。

> **先決條件**
>
> 您必須設定自訂中樞帳戶並新增至少一個藍圖 (Service Catalog 產品），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. 輸入包含您的藍圖之帳戶的帳戶 ID。
2. 從該帳戶選取現有的 Service Catalog 產品 （ 現有的藍圖 ）。
3. 如果您有多個版本，請選取藍圖的正確版本 (Service Catalog 產品 ）。
4. （選用 ） 您可以在程序的這個時間點新增或變更藍圖佈建政策。藍圖佈建政策是以 JSON 撰寫並連接到 IAM 角色，因此可以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，以便 Service Catalog 可以使用 CloudFormation 堆疊集部署資源。角色已命名 `AWSControlTower-BlueprintExecution-bp-xxxx`。根據預設，`AdministratorAccess`政策會在此處套用。
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. 如果您的藍圖包含參數，您可以將參數的值輸入 AWS Control Tower 工作流程中的其他欄位。其他值可能包括：GitHub 儲存庫名稱、GitHub 分支、Amazon ECS 叢集名稱，以及儲存庫擁有者的 GitHub 身分。
7. 如果您的中樞帳戶或藍圖尚未準備好，您可以稍後遵循帳戶更新程序來自訂帳戶。

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

建立自訂藍圖後，您可以在 AWS Control Tower 帳戶工廠中開始建立自訂帳戶。

當您建立新 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 管理主控台。
2. 選取帳戶工廠和建立帳戶。
3. 輸入帳戶詳細資訊，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 Identity Center 詳細資訊。
5. 選取將新增您帳戶的已註冊 OU。
6. 展開帳戶原廠自訂區段。
7. 輸入包含 Service Catalog 產品的藍圖中樞帳戶的帳戶 ID，然後選擇驗證。如需藍圖中樞帳戶的詳細資訊，請參閱 使用帳戶工廠自訂 (AFC) 自訂帳戶。
8. 從 Service Catalog 產品清單中選取包含所有藍圖的下拉式選單 （ 所有自訂和合作夥伴藍圖 ）。選擇要部署的藍圖和對應的版本。

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管區域。Route 53 或 IAM 等全域資源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，可以部署到所有受管區域
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，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。當您的帳戶佈建完成時，藍圖指定的資源已在其中部署。若要檢視帳戶的詳細資訊和藍圖，請前往帳戶詳細資訊頁面。

在您註冊帳戶時，使用 AFC 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 Tower 主控台，然後從左側導覽中選取組織。
2. 您將看到可用帳戶的清單。識別您想要使用自訂藍圖註冊的帳戶。該帳戶的狀態欄應反映為未註冊狀態的帳戶。
3. 選取帳戶左側的選項按鈕，然後選擇畫面右上角的動作下拉式功能表。在這裡，您將選取註冊選項。
4. 使用帳戶的 IAM Identity Center 資訊完成存取組態區段。
5. 選取您的帳戶將成為成員的已註冊 OU。
6. 使用與建立帳戶程序 7-12 相同的步驟，完成帳戶原廠自訂區段。如需詳細資訊，請參閱使用佈建帳戶工廠帳戶 AWS Service Catalog。

您可以在組織頁面上檢視帳戶進度的狀態。當您的帳戶註冊完成時，藍圖指定的資源已在其中部署。

將藍圖新增至 AWS Control Tower 帳戶

若要將藍圖新增至現有的 AWS Control Tower 成員帳戶，請遵循 AWS Control Tower 主控台中的更新帳戶工作流程，然後選擇要新增至帳戶的新藍圖。如需詳細資訊，請參閱使用 AWS Control Tower 或使用 更新和移動帳戶工廠帳戶 AWS Service Catalog。

> **Note**
>
> 如果您將新的藍圖新增至帳戶，則會覆寫現有的藍圖。

> **Note**
>
> 每個 AWS Control Tower 帳戶可以部署一個藍圖。

更新藍圖

下列程序說明如何更新自訂藍圖，以及如何部署這些藍圖。

更新您的自訂藍圖

1. 使用新組態更新您的 CloudFormation 範本或 Terraform tar.gz 檔案（藍圖）。
2. 將更新的藍圖儲存為新的版本 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。

如果藍圖更新失敗

當佈建產品處於 AVAILABLE 狀態時，AWS Control Tower 允許藍圖更新。如果您的佈建產品處於 TAINTED 狀態，更新將會失敗。我們建議採取以下解決方法：

1. 在 AWS Service Catalog 主控台中，手動更新TAINTED佈建的產品，將狀態變更為 AVAILABLE。如需詳細資訊，請參閱更新佈建的產品。
2. 然後，遵循 AWS Control Tower 的更新帳戶程序來修正藍圖部署錯誤。

我們建議您使用此手動步驟，因為：當您移除藍圖時，可能會導致移除成員帳戶中的資源。移除資源可能會影響您現有的工作負載。因此，我們建議您使用此方法，而不是更新藍圖的替代方式，特別是如果您正在執行生產工作負載，即移除和取代原始藍圖。

從帳戶移除藍圖

若要從帳戶移除藍圖，請遵循更新帳戶工作流程移除藍圖，並將帳戶傳回 AWS Control Tower 預設組態。

當您在主控台中輸入更新帳戶工作流程時，您會看到所有帳戶詳細資訊都會填入，而且自訂詳細資訊也不會填入。如果您將這些 AFC 詳細資訊保留空白，AWS Control Tower 會從帳戶移除藍圖。您會在動作開始之前看到警告訊息。

> **Note**
>
> 只有當您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 帳戶工廠自訂 (AFC) 可讓您存取由 AWS 合作夥伴建置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置自訂帳戶，這些帳戶已預先設定為與該特定合作夥伴的產品方案搭配使用。

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 Customizations (AFC) 的考量事項

- AFC 僅支援使用單一 AWS Service Catalog 藍圖產品的自訂。
- AWS Service Catalog 藍圖產品必須在中樞帳戶中建立，並在與 AWS Control Tower 登陸區域主區域相同的區域中建立。
- IAM `AWSControlTowerBlueprintAccess` 角色必須以適當的名稱、許可和信任政策建立。
- AWS Control Tower 支援兩種藍圖部署選項：僅部署到主區域，或部署到由 AWS Control Tower 管理的所有區域。區域選擇不可用。
- 當您更新成員帳戶中的藍圖時，藍圖中樞帳戶 ID 和 AWS Service Catalog 藍圖產品無法變更。
- AWS Control Tower 不支援移除現有的藍圖，並在單一藍圖更新操作中新增新的藍圖。您可以移除藍圖，然後在個別操作中新增藍圖。
- AWS Control Tower 會根據您是建立還是註冊自訂帳戶或非自訂帳戶，來變更行為。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的過程中發生錯誤，無論是新帳戶或您註冊 AWS Control Tower 的現有帳戶，復原程序都相同。帳戶將存在，但不會自訂，也不會註冊到 AWS Control Tower。若要繼續，請依照步驟將帳戶註冊到 AWS Control Tower，並在註冊時新增藍圖。

建立**AWSControlTowerBlueprintAccess**角色時發生錯誤，以及解決方法

當您從 AWS Control Tower 帳戶建立`AWSControlTowerBlueprintAccess`角色時，您必須使用該`AWSControlTowerExecution`角色以委託人身分登入。如果您以任何其他身分登入，SCP 會阻止`CreateRole`操作，如以下成品所示：

```
{
            "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"
        }
```

可用的解決方法如下：

- （最佳建議）擔任AWSControlTowerExecution角色並建立AWSControlTowerBlueprintAccess角色。如果您選擇此解決方法，請務必在之後立即登出該AWSControlTowerExecution角色，以防止意外變更資源。
- 登入未在 AWS Control Tower 註冊的帳戶，因此不受此 SCP 約束。
- 暫時編輯此 SCP 以允許 操作。
- （強烈建議不要）使用您的 AWS Control Tower 管理帳戶做為您的中樞帳戶，因此不受 SCP 約束。

根據 CloudFormation 自訂 AFC 藍圖的政策文件

當您透過帳戶工廠啟用藍圖時，AWS Control Tower CloudFormation 會指示 代表您建立 StackSet。CloudFormation 需要存取您的受管帳戶，才能在 StackSet 中建立 CloudFormation 堆疊。雖然 CloudFormation 已透過 AWSControlTowerExecution角色在受管帳戶中具有管理員權限，但此角色無法擔任 CloudFormation。

在啟用藍圖的過程中，AWS Control Tower 會在成員帳戶中建立角色， CloudFormation 可能擔任該角色來完成 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全部允許政策，因為這些政策與任何藍圖範本相容。

不過，最佳實務建議您必須限制 CloudFormation 目標帳戶中的 許可。您可以提供自訂政策，AWS Control Tower 會套用到其建立 CloudFormation 供 使用的角色。例如，如果您的藍圖建立稱為重要事項的 SSM 參數，您可以提供下列政策：

JSON

```
{
    "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 自訂政策都需要 `AllowCloudFormationActionsOnStacks`陳述式； CloudFormation 使用此角色來建立堆疊執行個體，因此需要在堆疊上執行 CloudFormation 動作的許可。`AllowSsmParameterActions` 區段專屬於要啟用的範本。

解決許可問題

當您啟用具有限制政策的藍圖時，您可能會發現沒有足夠的許可來啟用藍圖。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，以使用更正的政策。若要檢查政策是否足以啟用藍圖，請確定已授予 CloudFormation 許可，而且您可以直接使用該角色建立堆疊。

建立 Terraform 型 Service Catalog 產品所需的其他許可

當您使用適用於 AFC 的 Terraform 組態檔案建立 AWS Service Catalog 外部產品時，除了建立範本中定義資源所需的許可之外， AWS Service Catalog 還需要將特定許可新增至您的 AFC 自訂 IAM 政策。如果您選擇預設的完整管理員政策，則不需要新增這些額外的許可。

JSON

```
{
    "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"
                }
            }
        }
    ]
}
```

如需使用 中的外部產品類型建立 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。

轉換為 AWS Service Catalog 外部產品類型

AWS Service Catalog 將 Terraform Open Source 產品和佈建產品的支援變更為新的產品類型，稱為外部。若要進一步了解此轉換，請參閱 AWS Service Catalog 管理員指南中的將現有的 Terraform Open Source 產品和佈建產品更新為外部產品類型。

此變更會影響您透過 AWS Control Tower 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。

轉換為外部產品類型

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 參考引擎的說明，請檢閱 AWS Service Catalog GitHub 儲存庫。
2. 在 中 AWS Service Catalog，使用新的外部產品類型複製任何現有的 Terraform Open Source 產品 （藍圖） 和複本。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，請參閱從帳戶移除藍圖。

   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 Open Source 藍圖的所有帳戶更新為外部藍圖後，請返回 AWS Service Catalog 並終止使用 Terraform Open Source 作為產品類型的任何產品。
5. 接下來，使用 AWS Control Tower 帳戶原廠自訂建立或註冊的所有帳戶，都必須使用 CloudFormation或 外部產品類型參考藍圖。

   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。若要進一步了解，請檢閱設定以進行自訂。

> **Note**
>
> 建立新帳戶時，AWS Control Tower 不支援 Terraform Open Source 做為產品類型。若要進一步了解這些變更，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產品更新為外部產品類型。 AWS Service Catalog 將視需要支援客戶完成此產品類型轉換。請聯絡您的 帳戶代表以請求協助。

使用 AWS Control Tower Account Factory for Terraform (AFT) 佈建帳戶

AWS Control Tower Account Factory for Terraform (AFT) 採用 GitOps 模型，可自動化 AWS Control Tower 中的帳戶佈建和更新程序。

使用 AFT，您可以建立帳戶請求 Terraform 檔案，其中包含叫用 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。

AFT 不會影響 AWS Control Tower 中的工作流程效能。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。

先決條件

> **Note**
>
> AFT 帳戶佈建必須以 AWS Control Tower 中啟用 AWSControlTowerBaseline 的組織單位 (OU) 為目標。如需 AWSControlTowerBaseline 的詳細資訊，請參閱：在 OU 層級套用的基準類型。

當您開始使用 AFT 時，您將建立下列項目：

- 在 AWS Control Tower 中，為您的 AFT 環境建立 OU，然後建立 AFT 管理帳戶。請記下帳戶 ID，以便您稍後使用 Terraform 模組部署 AFT 時，可以在 `main.tf` 檔案中輸入帳戶 ID。您可以在 AWS Control Tower Control 詳細資訊頁面上檢視此帳戶 ID。如需詳細資訊，請參閱 Terraform 文件。
- 完整部署 AFT 環境的一或多個`git`儲存庫。如需詳細資訊，請參閱 AFT 的部署後步驟。
- 完全部署的 AFT 環境。如需詳細資訊，請參閱適用於 Terraform 的 AWS Control Tower 帳戶工廠概觀 (AFT) 和適用於 Terraform 的部署 AWS Control Tower 帳戶工廠 (AFT)。另請參閱 Terraform 文件。

> **Tip**
>
> 您可以從 AWS Control Tower 主控台使用建立帳戶建立 AFT 管理帳戶。如需詳細資訊，請參閱佈建方法。
> 此外，您可以選擇在 aft-account-customizations 儲存庫中建立帳戶範本資料夾，以協助定義其他帳戶。

對於透過自動註冊註冊的帳戶：

- 透過 AFT 建立新帳戶會繼續正常運作。
- 現有的帳戶匯入需要額外的步驟：

- 註冊 OU 以在匯入之前建立必要的佈建產品。
- 註冊 OU 將發出 `CreateManagedAccount`和 `UpdateManagedAccount`事件，啟用 AFT 自訂。

如需 AFT 具有部署限制 AWS 區域 之處的詳細資訊，請參閱 AWS Control Tower 中的限制和配額和控制限制。

Terraform 文件包含如何為 Terraform 設定 AWS Control Tower 帳戶工廠 (AFT) 的良好概觀。

適用於 Terraform (AFT) 的 AWS Control Tower 帳戶工廠概觀

Account Factory for Terraform (AFT) 會設定 Terraform 管道，協助您在 AWS Control Tower 中佈建和自訂帳戶。AFT 為您提供 Terraform 型帳戶佈建的優勢，同時允許您使用 AWS Control Tower 管理您的帳戶。

使用 AFT，您可以建立帳戶請求 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 會自動在帳戶自訂階段開始之前執行一系列步驟。如需詳細資訊，請參閱 AFT 帳戶佈建管道。

AFT 支援 Terraform Cloud、Terraform Enterprise 和 Terraform Community Edition。使用 AFT，您可以使用輸入檔案和簡單的`git push`命令來啟動帳戶建立，並自訂新的或現有的帳戶。帳戶建立包括所有 AWS Control Tower 控管優勢和帳戶自訂，可協助您符合組織的標準安全程序和合規準則。

AFT 支援帳戶自訂請求追蹤。每次您提交帳戶自訂請求時，AFT 都會產生唯一的追蹤字符，透過 AFT 自訂 AWS Step Functions 狀態機器傳遞，該機器會將字符記錄為執行的一部分。然後，您可以使用 Amazon CloudWatch Logs 洞見查詢來搜尋時間戳記範圍並擷取請求字符。因此，您可以看到字符隨附的承載，以便在整個 AFT 工作流程中追蹤您的帳戶自訂請求。如需 CloudWatch Logs 和 Step Functions 的相關資訊，請參閱下列內容：

- 《Amazon CloudWatch Logs 使用者指南》中的什麼是 Amazon CloudWatch Logs？
- 《AWS Step Functions 開發人員指南》中的什麼是 AWS Step Functions？

AFT 結合了其他 AWS 服務的功能，以元件服務建置架構，以及部署 Terraform Infrastructure as Code (IaC) 的管道。AFT 可讓您：

- 在 GitOps 模型中提交帳戶佈建和更新請求
- 存放帳戶中繼資料和稽核歷史記錄

- 套用帳戶層級標籤
- 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 會建立稱為 AFT 管理帳戶的獨立帳戶，以部署 AFT 功能。您必須先擁有現有的 AWS Control Tower 登陸區域，才能設定 AFT。AFT 管理帳戶與 AWS Control Tower 管理帳戶不同。

AFT 提供彈性

- 平台彈性：AFT 支援任何 Terraform Distribution 進行初始部署和持續操作：Community Edition、Cloud 和 Enterprise。
- 版本控制系統的彈性：AFT 支援 AWS CodeCommit，以及透過 的替代版本控制來源 AWS CodeConnections。

AFT 提供功能選項

您可以根據最佳實務啟用數個功能選項：

- 建立用於記錄資料事件的組織層級 CloudTrail
- 刪除帳戶 AWS 的預設 VPC
- 將佈建帳戶註冊至 AWS 企業支援計劃

> **Note**
>
> AFT 管道不適用於部署您帳戶執行應用程式所需的資源，例如 Amazon EC2 執行個體。它僅用於自動佈建和自訂 AWS Control Tower 帳戶。

影片演練

此影片 (7：33) 說明如何使用 AWS Control Tower Account Factory for Terraform 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 自動化帳戶佈建的影片逐步解說。

AFT 架構

操作順序

您可以在 AFT 管理帳戶中執行 AFT 操作。對於完整的帳戶佈建工作流程，圖表中從左到右的階段順序如下：

1. 帳戶請求會建立並提交至管道。您可以一次建立和提交多個帳戶請求。Account Factory first-in-first-out順序處理請求。如需詳細資訊，請參閱提交多個帳戶請求。
2. 每個帳戶都會佈建。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自訂，則自訂只會在目標帳戶上執行。如果您有已佈建的帳戶，則必須在帳戶的管道中手動啟動進一步的自訂。

適用於 Terraform 的 AWS Control Tower 帳戶工廠 – 帳戶佈建工作流程

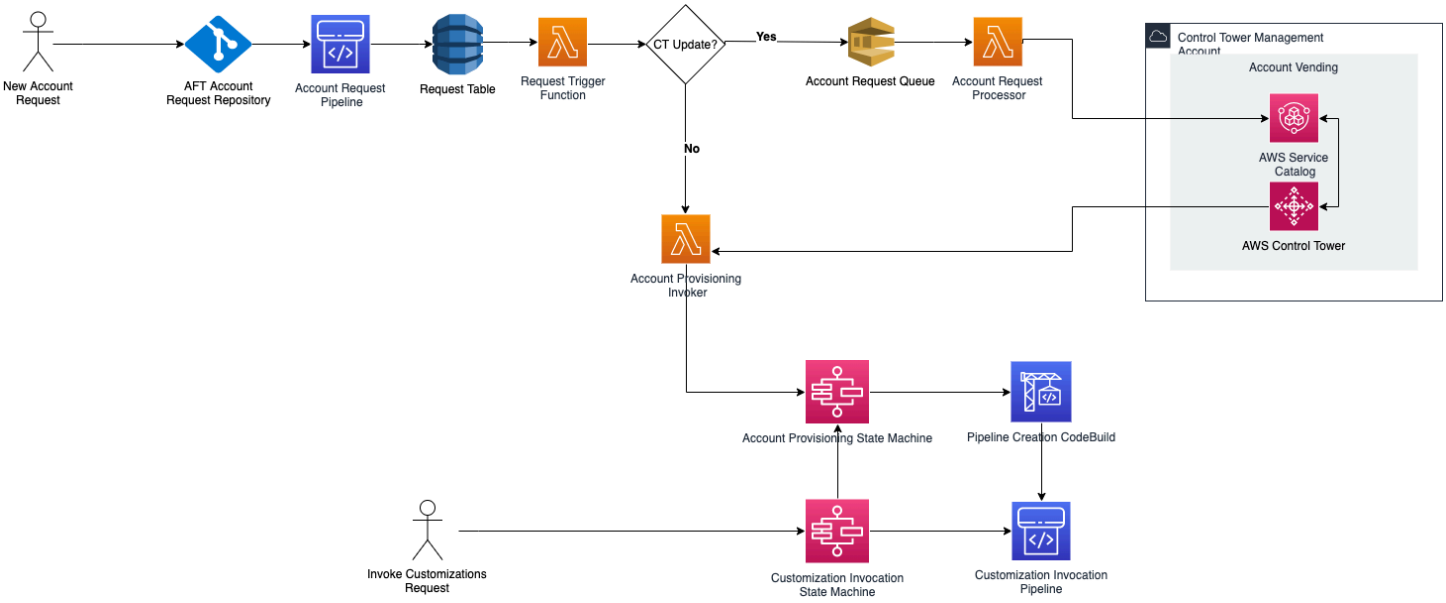

圖 1：適用於 Terraform 的 AWS Control Tower 帳戶工廠

Cost

AFT 沒有額外費用。您只需為 AFT 部署的資源、AFT 啟用 AWS 的服務，以及您在 AFT 環境中部署的資源付費。

預設 AFT 組態包含 AWS PrivateLink 端點的配置，以增強資料保護和安全性，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 Gateway 的AWS

PrivateLink 定價和 Amazon VPC 定價。 https://aws.amazon.com//vpc/pricing/如需管理這些成本的詳細資訊，請聯絡您的 AWS 客戶代表。您可以變更 AFT 的這些預設設定。

部署適用於 Terraform (AFT) 的 AWS Control Tower 帳戶工廠

本節適用於想要在現有環境中設定 Account Factory for Terraform (AFT) 的 AWS Control Tower 環境管理員。它說明如何使用新的專用 AFT 管理帳戶設定 Account Factory for Terraform (AFT) 環境。

> **Note**
>
> Terraform 模組會部署 AFT。此模組可在 GitHub 上的 AFT 儲存庫中使用，而且整個 AFT 儲存庫都視為模組。
> 我們建議您參考 GitHub 上的 AFT 模組，而不是複製 AFT 儲存庫。如此一來，您就可以在模組可用時控制和使用更新。

如需 AWS Control Tower Account Factory for Terraform (AFT) 功能最新版本的詳細資訊，請參閱此 GitHub 儲存庫的版本檔案。

部署先決條件

在設定和啟動 AFT 環境之前，您必須擁有下列資源：

- AWS Control Tower 登陸區域的主區域。如需詳細資訊，請參閱如何使用 AWS 區域 AWS Control Tower。
- AWS Control Tower 登陸區域。如需詳細資訊，請參閱規劃您的 AWS Control Tower 登陸區域。
- AFT 管理帳戶，您可以在 AWS Control Tower 中佈建，或透過其他方式佈建並註冊 AWS Control Tower。
- Terraform 版本和分佈。如需詳細資訊，請參閱 Terraform 和 AFT 版本。
- 用於追蹤和管理程式碼和其他檔案變更的 VCS 提供者。根據預設，AFT 會使用 AWS CodeCommit。如需詳細資訊，請參閱AWS CodeCommit 《 使用者指南》中的什麼是 AWS CodeCommit？。

  如果您是第一次部署 AFT，而且沒有現有的 CodeCommit 儲存庫，則必須選擇外部 VCS 供應商，例如 GitHub 或 BitBucket。如需詳細資訊，請參閱 AFT 中原始程式碼版本控制的替代方案。
- 執行期環境，您可以在其中執行安裝 AFT 的 Terraform 模組。
- AFT 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 Terraform 的 AWS Control Tower 帳戶工廠

下列步驟假設您熟悉 Terraform 工作流程。您也可以遵循 AWS Workshop Studio 網站上的 AFT 實驗室簡介，進一步了解部署 AFT。

步驟 1：啟動您的 AWS Control Tower 登陸區域

完成 AWS Control Tower 入門中的步驟。您可以在此處建立 AWS Control Tower 管理帳戶，並設定 AWS Control Tower 登陸區域。

> **Note**
>
> 請務必為具有 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：
>
> - AWS Identity and Access Management 《使用者指南》中的 IAM 身分（使用者、使用者群組和角色）
> - 《AWS 受管政策參考指南》中的 AdministratorAccess

步驟 2：為 AFT 建立新的組織單位（強烈建議）

我們建議您在 AWS Control Tower 登陸區域 中建立個別的 OU。此 OU 是您佈建 AFT 管理帳戶的地方。從 AWS Control Tower 管理帳戶建立新的 OU 和 AFT 管理帳戶。如需詳細資訊，請參閱建立新的 OU。

步驟 3：佈建 AFT 管理帳戶

AFT 要求您佈建專用於 AFT 管理操作 AWS 的帳戶。當您登入與您的 AWS Control Tower 登陸區域相關聯的 AWS Control Tower 管理帳戶時，請建立 AFT 管理帳戶。您可以在組織頁面上選取建立帳戶，或透過其他方式，從 AWS Control Tower 主控台佈建 AFT 管理帳戶。如需詳細資訊，請參閱使用 Account Factory 佈建 AWS Service Catalog 帳戶。

> **Note**
>
> 如果您為 AFT 建立單獨的 OU，請務必在建立 AFT 管理帳戶時選取此 OU。

完整佈建 AFT 管理帳戶最多可能需要 30 分鐘。

步驟 4：確認 Terraform 環境可供部署

此步驟假設您有使用 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 Command： init。

> **Note**
>
> AFT 支援 Terraform 版本 `1.6.0` 或更新版本。

步驟 5：選用組態

- 選擇性地設定虛擬私有雲端 (VPC) 組態

  AFT 模組包含 `aft_enable_vpc` 參數，指定 AWS Control Tower 是否在中央 AFT 管理帳戶中的 VPC 內佈建帳戶資源。根據預設， 參數會設定為 `true`。如果您將此參數設定為 `false`，AWS Control Tower 會在不使用 VPC 和私有聯網資源的情況下部署 AFT，例如 NAT Gateways 或 VPC 端點。停用`aft_enable_vpc`可能有助於降低某些使用模式的 AFT 操作成本。新增任何 VPC 組態會覆寫設定為 的`aft_enable_vpc`參數`false`。

  > **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`terraform apply`命令兩次。

  您可以設定 AFT 以使用帳戶中現有的 VPC，而不是佈建新的 VPC。若要使用您自己的 VPC，請提供下列 VPC 組態參數：

  - `aft_customer_vpc_id` - 現有 VPC 的 ID
  - `aft_customer_private_subnets` - VPC 中的私有子網路 IDs清單

  範例組態：

```
module "aft" {
  source = "github.com/aws-ia/terraform-aws-control_tower_account_factory"

  # VPC configuration
  aft_customer_vpc_id = "vpc-0123456789abcdef0"
```

```
  aft_customer_private_subnets = ["subnet-0123456789abcdef0",
 "subnet-0123456789abcdef1"]

  # Other AFT parameters...
}
```

> **Important**
>
> 如果您有現有的 AFT 部署，我們不建議您使用自訂 VPC 選項。您可能對 Lambda 函數或 CodePipeline 有相依性，這些相依性取決於基礎現有 VPC 中的資源。

- 選擇性地設定 Terraform 專案名稱

  您可以設定 `terraform_project_name` 參數來自訂 AFT 使用的 Terraform 專案名稱。根據預設，AFT 會將部署置於 Terraform Cloud 或 Terraform Enterprise 的「預設」專案中。

  範例組態：

```
module "aft" {
  source = "github.com/aws-ia/terraform-aws-control_tower_account_factory"

  # Project name configuration
  terraform_project_name = "my-organization-aft"

  # Other AFT parameters...
}
```

> **Note**
>
> 此參數僅適用於 Terraform Enterprise 或 Terraform Cloud 部署。

- 選擇性地將自訂標籤套用至 AFT 資源

  您可以使用 `tags` 參數，將自訂標籤套用至所有 AFT 資源。這些標籤可協助進行資源組織、成本分配和存取控制。

  範例組態：

```
module "aft" {
  source = "github.com/aws-ia/terraform-aws-control_tower_account_factory"

  # Custom tags configuration
  tags = {
    Environment = "Production"
    CostCenter = "IT-12345"
    Project = "AFT-Deployment"
    Owner = "platform-team@example.com"
  }

  # Other AFT parameters...
}
```

這些標籤會套用至 AFT 模組建立的所有資源。AFT 會自動將`managed_by = "AFT"`標籤新增至所有資源，這些資源無法被自訂標籤覆寫。

> **Note**
>
> 您可以隨時新增自訂標籤，而不只是在初始部署期間。

- 選擇性地將 AWS KMS 客戶受管加密金鑰 (CMK) 套用至 CloudWatch 日誌群組和 SNS 主題

  若要啟用日誌群組和 SNS 主題的 KMS CMK 加密，請設定`cloudwatch_log_group_enable_cmk_encryption`和`sns_topic_enable_cmk_encryption`變數。

  如果您選擇加入這些設定，AFT 會使用現有的 CMK、別名/後置來加密 CloudWatch 日誌和 SNS 主題。在 AFT 管理帳戶中部署 AFT 時，會建立此 CMK，並可套用至日誌群組和 SNS 主題。

  - 如果變數`cloudwatch_log_group_enable_cmk_encryption`設為 true，則 AFT 的 CloudWatch 日誌群組會使用 CMK 加密。如果變數設定為 false，這是預設值，則會使用伺服器端加密來加密日誌，並預設使用 CloudWatch 日誌。
  - 如果變數`sns_topic_enable_cmk_encryption`設為 true，傳送至 AFT SNS 主題的通知 (後置通知和aft-failure-notifications) 會使用 CMK 加密。如果變數設定為 false，這是預設值，SNS 訊息會使用 AWS 受管金鑰加密：alias/aws/sns。如需詳細資訊，請參閱 SSE 金鑰術語。
- 選擇性地變更 CodeBuild 運算類型

在部署期間，若要變更 AFT 用於 CodeBuild 的運算類型，請設定變數 `aft_codebuild_compute_type`。

如需已接受運算類型的資訊，請參閱關於隨需環境類型。預設運算類型為 `BUILD_GENERAL1_MEDIUM`。

- 選擇性地為 Terraform 設定 OpenID Connect (OIDC)

使用 Terraform Enterprise 或 HCP Terraform （先前稱為 Terraform Cloud) 的客戶可以使用建立在 OIDC 通訊協定上的 Terraform 工作負載身分字符 （或動態提供者憑證），以使用 AFT 安全地連接和驗證工作區。

您可以將 `terraform_oidc_integration` 參數設定為 ，以啟用 AFT 工作區的 OIDC 整合`true`。根據預設，此參數會設定為 `false`。啟用此參數時，如果預設值 (`aws.workload.identity` `terraform_oidc_aws_audience`和 分別為) 不符合您的環境`app.terraform.io`，則應檢閱和設定 和 `terraform_oidc_hostname` 參數。

範例組態：

```
module "aft" {
  source = "github.com/aws-ia/terraform-aws-control_tower_account_factory"

  # Terraform distribution must be "tfc" or "tfe" for OIDC
  terraform_distribution = "tfc"

  # Terraform OIDC Configuration
  terraform_oidc_integration  = true
  terraform_oidc_aws_audience = "aws.workload.identity"  # default
  terraform_oidc_hostname     = "app.terraform.io"       # default; set to your TFE
 hostname if applicable

  # Other AFT parameters...
}
```

> **Note**
>
> 此參數僅適用於 Terraform Enterprise 或 HCP Terraform 部署。

> **Note**
>
> 如果您目前正在 AFT 管理帳戶中利用 Terraform 的 OIDC 提供者，您必須先刪除該提供者，才能選擇加入此整合。AFT 會在部署時為您重新建立該提供者。

步驟 6：呼叫 Account Factory for Terraform 模組以部署 AFT

使用您為具有 AdministratorAccess 憑證的 AWS Control Tower 管理帳戶建立的角色來呼叫 AFT 模組。AWS Control Tower 透過 AWS Control Tower 管理帳戶佈建 Terraform 模組，這會建立協調 AWS Control Tower 帳戶工廠請求所需的所有基礎設施。

您可以在 GitHub 的 AFT 儲存庫中檢視 AFT 模組。整個 GitHub 儲存庫會被視為 AFT 模組。如需執行 AFT 模組和部署 AFT 所需的輸入相關資訊，請參閱 README 檔案。或者，您可以在 Terraform 登錄檔中檢視 AFT 模組。

如果您在環境中建立了用於管理 Terraform 的管道，您可以將 AFT 模組整合到現有的工作流程中。否則，請從使用所需登入資料進行身分驗證的任何環境執行 AFT 模組。

逾時會導致部署失敗。我們建議您使用 AWS Security Token Service (STS) 登入資料，以確保您的逾時足以進行完整部署。 AWS STS 登入資料的最短逾時為 60 分鐘。如需詳細資訊，請參閱AWS Identity and Access Management 《使用者指南》中的 IAM 中的臨時安全登入資料。

> **Note**
>
> 您可以等待最多 30 分鐘讓 AFT 透過 Terraform 模組完成部署。

步驟 7：管理 Terraform 狀態檔案

部署 AFT 時會產生 Terraform 狀態檔案。此成品說明 Terraform 建立的資源狀態。如果您打算更新 AFT 版本，請務必預先保存 Terraform 狀態檔案，或使用 Amazon S3 和 DynamoDB 設定 Terraform 後端。AFT 模組不會管理後端 Terraform 狀態。

> **Note**
>
> 您有責任保護 Terraform 狀態檔案。某些輸入變數可能包含敏感值，例如私有ssh金鑰或 Terraform 字符。根據您的部署方法，這些值可以在 Terraform 狀態檔案中以純文字形式檢視。如需詳細資訊，請參閱 HashiCorp 網站上的狀態敏感資料。

部署後步驟

AFT 基礎設施部署完成後，請依照這些額外步驟完成設定程序，並準備好佈建帳戶。

步驟 1：使用所需的 VCS 供應商完成 CodeConnections

如果您選擇第三方 VCS 提供者，AFT 會建立 CodeConnections，然後進行確認。請參閱 ，AFT 中原始程式碼版本控制的替代方案了解如何使用您偏好的 VCS 設定 AFT。

建立 AWS CodeStar 連線的初始步驟是由 AFT 完成。您必須確認連線。

步驟 2：填入每個儲存庫

AFT 要求您管理四個儲存庫：

1. 帳戶請求 – 此儲存庫會處理提出或更新帳戶請求。可用的範例 。如需 AFT 帳戶請求的詳細資訊，請參閱 使用 AFT 佈建新帳戶。
2. AFT 帳戶佈建自訂 – 此儲存庫會在開始全域自訂階段之前，管理套用到由 AFT 建立和使用 AFT 管理的所有帳戶的自訂。可用的範例 。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 建立和使用 AFT 管理的所有帳戶的自訂。可用的範例 。若要建立 AFT 全域自訂，請參閱 套用全域自訂。
4. 帳戶自訂 – 此儲存庫會管理僅套用至由 AFT 建立和使用 AFT 管理的特定帳戶的自訂。可用的範例 。若要建立 AFT 帳戶自訂，請參閱 套用帳戶自訂。

AFT 預期每個儲存庫都遵循特定的目錄結構。用於填入儲存庫的範本和描述如何填入範本的指示，可在 AFT github 儲存庫的 Account Factory for Terraform 模組中使用。

使用 AFT 佈建新帳戶

本節假設您已設定 AFT 和 AFT 管理帳戶，而且您正在佈建其他帳戶。

若要使用 AFT 佈建新帳戶，請建立帳戶請求 Terraform 檔案。此檔案包含 aft-account-request 儲存庫中參數的輸入。建立帳戶請求 Terraform 檔案之後，請執行 開始處理您的帳戶請求`git push`。此命令會在 中叫用 操作 AWS CodePipeline，該`ct-aft-account-request`操作會在帳戶佈建完成後在 AFT 管理帳戶中建立。如需詳細資訊，請參閱 AFT 帳戶佈建管道。

帳戶請求 Terraform 檔案參數

您必須在帳戶請求 Terraform 檔案中包含下列參數。您可以在 GitHub 上檢視範例帳戶請求 Terraform 檔案。

- 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 提供之帳戶請求 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。此值包含下列輸入欄位：
  - `AccountEmail`
  - `AccountName`
  - `ManagedOrganizationalUnit`
  - `SSOUserEmail`
  - `SSOUserFirstName`
  - `SSOUserLastName`

> **Note**
>
> 您無法在帳戶佈建期間`control_tower_parameters`變更您為 提供的輸入。
> 在 aft-account-request 儲存庫`ManagedOrganizationalUnit`中指定 支援的格式包括 `OUName`和 `OUName (OU-ID)`。

- `account_tags` 會擷取使用者定義的金鑰和值，這些金鑰和值可根據業務準則 AWS 帳戶 進行標記。如需詳細資訊，請參閱AWS Organizations 《 使用者指南》中的標記 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。此值包含下列輸入欄位：
  - `change_reason`
  - `change_requested_by`

- `custom_fields` 在 /aft/account-request/custom-fields/ 下的付費帳戶中，使用部署為 SSM 參數的索引鍵和值擷取其他中繼資料。您可以在帳戶自訂期間參考此中繼資料，以部署適當的控制項。例如，受法規合規約束的帳戶可能會部署額外的 AWS Config 規則。您使用 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。如果從帳戶請求中移除自訂欄位，則自訂欄位會從佈建帳戶的 SSM 參數存放區中移除。
- （選用）會`account_customizations_name`擷取 aft-account-customizations 儲存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，但您可以將多個帳戶請求提交至 AFT 管道。當您向 AFT 管道提交多個帳戶請求時，AFT 會排入佇列，並以先進先出順序處理帳戶請求。

> **Note**
>
> 您可以為您希望 AFT 在單一帳戶請求 Terraform 檔案中佈建或串聯多個帳戶請求的每個帳戶建立帳戶請求 Terraform 檔案。

更新現有帳戶

> **⚠ 自動註冊相容性**
>
> 如果您的組織使用自動註冊進行自動帳戶註冊，請注意，AFT 對匯入這些帳戶有限制。透過自動註冊註冊的帳戶缺少 AFT 匯入工作流程所需的 Service Catalog 佈建產品。
> 解決方法：使用註冊 OU 功能為自動註冊的帳戶建立佈建產品。這可為 AFT 自訂啟用必要的生命週期事件。

您可以編輯先前提交的帳戶請求並執行 ，以更新 AFT 佈建的帳戶`git push`。此命令會叫用帳戶佈建工作流程，並可處理帳戶更新請求。您可以更新 的輸入`ManagedOrganizationalUnit`，這是 所需值的一部分`control_tower_parameters`。

`ManagedOrganizationalUnit` 是可在所有 中更新的唯一參數`control_tower_parameters`。不過，屬於帳戶請求 Terraform 檔案的其他參數可以更新，例如 `custom_fields`。如需詳細資訊，請參閱使用 AFT 佈建新帳戶。

例如，若要更新 AFT 帳戶的名稱或電子郵件地址，您可以定義帳戶custom_fields請求檔案中的詳細資訊。透過這樣做，您可以建立 SSM 參數，您可以在全域自訂期間傳入aws_account_alternate_contact資源。

```
resource "aws_account_alternate_contact" "operations" {

  alternate_contact_type = "OPERATIONS"

  name          = "Example"
  title         = "Example"
  email_address = "someone@example.com"
  phone_number  = "+1234567890"
}
```

您可以為其他聯絡類型新增類似的欄位，例如操作和安全性。在全球自訂中，為每個自訂欄位新增資料查詢，以確保您查詢在帳戶請求中建立的所有欄位：

```
data "aws_ssm_parameter" "billing_name" {
            name = "/aft/account-request/custom-fields/billing_name"
            }

            data "aws_ssm_parameter" "billing_title" {
            name = "/aft/account-request/custom-fields/billing_title"
            }

            data "aws_ssm_parameter" "billing_email_address" {
            name = "/aft/account-request/custom-fields/billing_email_address"
            }

            data "aws_ssm_parameter" "billing_phone_number" {
            name = "/aft/account-request/custom-fields/billing_phone_number"
            }
```

最後，在全球自訂檔案中，建立替代聯絡人資源。您需要為您在帳戶請求中建立的每個聯絡類型定義其中一個區塊：

```
resource "aws_account_alternate_contact" "billing" {

            alternate_contact_type = "BILLING"

            name          = data.aws_ssm_parameter.billing_name.value
            title         = data.aws_ssm_parameter.billing_title.value
```

```
email_address = data.aws_ssm_parameter.billing_email_address.value
phone_number  = data.aws_ssm_parameter.billing_phone_number.value
}
```

> **Note**
>
> 您無法在帳戶佈建期間control_tower_parameters變更您為 提供的輸入。
> 在 aft-account-request 儲存庫ManagedOrganizationalUnit中指定 支援的格式包括 OUName和 OUName (OU-ID)。

更新 AFT 未佈建的帳戶

您可以在 aft-account-request 儲存庫中指定帳戶，以更新在 AFT 外部建立的 AWS Control Tower 帳戶。

> **Note**
>
> 確保所有帳戶詳細資訊皆正確且符合 AWS Control Tower 組織和個別 AWS Service Catalog 佈建的產品。

AWS 帳戶 使用 AFT 更新現有 的先決條件

- AWS 帳戶 必須在 AWS Control Tower 中註冊。
- AWS 帳戶 必須是 AWS Control Tower 組織的一部分。

Terraform 和 AFT 版本

Account Factory for Terraform (AFT) 支援 Terraform 版本 1.6.0 或更新版本。您必須提供 Terraform 版本做為 AFT 部署程序的輸入參數，如以下範例所示。

```
terraform_version = "1.6.0"
```

Terraform 分佈

AFT 支援三種 Terraform 分佈：

- Terraform Community Edition
- Terraform 雲端
- Terraform Enterprise

這些分佈會在以下各節中說明。在 AFT 引導程序期間，提供您選擇的 Terraform 分佈做為輸入參數。如需 AFT 部署和輸入參數的詳細資訊，請參閱 部署適用於 Terraform (AFT) 的 AWS Control Tower 帳戶工廠 。

如果您選擇 Terraform Cloud 或 Terraform Enterprise 分佈，您為 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 APIs都支援 Organization 權杖。基於安全考量，您必須藉由指派 terraform 變數，避免將此權杖的值簽入版本控制系統 (VCS)，如以下範例所示。

```
# Sensitive variable managed in Terraform Cloud:
terraform_token = var.terraform_cloud_token
```

Terraform Community Edition

當您選取 Terraform Community Edition 做為分佈時，AFT 會在 AFT 管理帳戶中為您管理 Terraform 後端。AFT 會下載`terraform-cli`指定 Terraform 版本的 ，以在 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，並以下列格式命名：

```
aft-backend-[account_id]-primary-region
```

AFT 也會建立 Amazon S3 儲存貯體，在另一個儲存貯體中複寫您的 Terraform 狀態組態 AWS 區域，用於災難復原，名稱為 ，格式如下：

```
aft-backend-[account_id]-secondary-region
```

建議您為這些 Terraform 狀態 Amazon S3 儲存貯體上的刪除函數啟用多重驗證 (MFA)。若要進一步了解 Terraform Community Edition，請參閱 Terraform 文件。

若要選取 Terraform OSS 做為分佈，請提供下列輸入參數：

```
terraform_distribution = "oss"
```

Terraform 雲端

當您選取 Terraform Cloud 做為分佈時，AFT 會在 Terraform Cloud 組織中為下列元件建立工作區，這會啟動 API 驅動的工作流程。

- 帳戶請求
- AFT 佈建之帳戶的 AFT 自訂
- AFT 佈建之帳戶的帳戶自訂
- AFT 佈建之帳戶的全域自訂

Terraform Cloud 會管理產生的 Terraform 狀態組態。

當您選取 Terraform Cloud 做為分佈時，請提供下列輸入參數：

- `terraform_distribution = "tfc"`
- `terraform_token` – 此參數包含 Terraform Cloud 字符的值。AFT 會將 標記為敏感，並將值儲存為 AFT 管理帳戶中 SSM 參數存放區中的安全字串。我們建議您根據公司的安全政策和合規準則定期輪換 Terraform 字符的值。Terraform 權杖應該是使用者或團隊層級 API 權杖。不支援組織字符。
- `terraform_org_name` – 此參數包含 Terraform Cloud 組織的名稱。

> **Note**
>
> 不支援單一 Terraform Cloud 組織中的多個 AFT 部署。

如需有關如何設定 Terraform Cloud 的資訊，請參閱 Terraform 文件。

Terraform Enterprise

當您選取 Terraform Enterprise 做為分佈時，AFT 會在 Terraform Enterprise 組織中為下列元件建立工作區，並觸發產生 Terraform 執行的 API 驅動工作流程。

- 帳戶請求
- 由 AFT 佈建之帳戶的 AFT 帳戶佈建自訂
- AFT 佈建的帳戶的帳戶自訂
- AFT 佈建之帳戶的全域自訂

產生的 Terraform 狀態組態是由您的 Terraform Enterprise 設定管理。

若要選取 Terraform Enterprise 做為分佈，請提供下列輸入參數：

- `terraform_distribution = "tfe"`
- `terraform_token` – 此參數包含 Terraform Enterprise 字符的值。AFT 將其值標記為敏感，並將其儲存為 SSM 參數存放區 AFT 管理帳戶中的安全字串。我們建議您根據公司的安全政策和合規準則，定期輪換 Terraform 字符的值。
- `terraform_org_name` – 此參數包含 Terraform Enterprise 組織的名稱。
- `terraform_api_endpoint` – 此參數包含 Terraform Enterprise 環境的 URL。此參數的值格式必須為：

```
https://{fqdn}/api/v2/
```

請參閱 Terraform 文件以進一步了解如何設定 Terraform Enterprise。

檢查 AFT 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
```

如果您使用登錄檔方法，則可以鎖定版本。

```
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 AFT 版本的詳細資訊。

更新 AFT 版本

登入 AWS Control Tower 管理帳戶以啟動此 AFT 更新。

您可以從`main`儲存庫分支中提取已部署的 AFT 版本，以更新該版本：

```
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 基礎設施。

啟用功能選項

AFT 會根據最佳實務提供功能選項。您可以在 AFT 部署期間，透過功能旗標選擇加入這些功能。如需 AFT 輸入組態參數的詳細資訊使用 AFT 佈建新帳戶，請參閱。

預設不會啟用這些功能。您必須明確啟用環境中的每個項目。

主題

- AWS CloudTrail 資料事件
- AWS 企業支援計劃
- 刪除 AWS 預設 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。

- 在適用於 CloudTrail 的 AWS Control Tower 管理帳戶中建立 Organization Trail
- 開啟 Amazon S3 和 Lambda 資料事件的記錄
- 使用加密將所有 CloudTrail 資料事件加密並匯出至 AWS Control Tower Log Archive 帳戶中的 `aws-aft-logs-*` S3 儲存貯體 AWS KMS
- 開啟日誌檔案驗證設定

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為 True。

```
aft_feature_cloudtrail_data_events
```

必要條件

啟用此功能選項之前，請確定您的組織中 AWS CloudTrail 已啟用 的受信任存取。

若要檢查 CloudTrail 的受信任存取狀態：

1. 導覽至 AWS Organizations 主控台。
2. 選擇服務 > CloudTrail。
3. 然後視需要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，但在這種情況下，請忽略警告。在您允許受信任存取之後，AFT 會建立線索做為啟用此功能選項的一部分。如果未啟用受信任存取，當 AFT 嘗試為資料事件建立追蹤時，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 中的所有帳戶 AWS Organizations，無論它們是否由 AFT 管理。Amazon S3 資料事件會排除啟用時 AWS Control Tower Log Archive 帳戶中的所有儲存貯體。請參閱 AWS CloudTrail 使用者指南以進一步了解 CloudTrail。

AWS 企業支援計劃

啟用此選項時，AFT 管道會為 AFT 佈建的帳戶開啟 AWS 企業支援計劃。

AWS 帳戶預設會啟用 AWS 基本支援計劃。AFT 為 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支援票證，請求將其新增至 AWS 企業支援計劃。

若要啟用企業支援選項，請在 AFT 部署輸入組態中將下列功能旗標設為 True。

```
aft_feature_enterprise_support=false
```

請參閱比較 AWS 支援計劃以進一步了解 AWS 支援計劃。

> **Note**
>
> 若要允許此功能運作，您必須將付款人帳戶註冊到企業支援計劃中。

刪除 AWS 預設 VPC

當您啟用此選項時，即使尚未在這些 中部署 AWS Control Tower 資源 AWS 區域，AFT 仍會刪除 AFT 管理帳戶和 中的所有 AWS 預設 VPCs AWS 區域。

AFT 不會自動刪除 AFT 佈建的任何 AWS Control Tower 帳戶或您透過 AFT 註冊 AWS Control Tower 的現有 AWS 帳戶 AWS 的預設 VPCs。

根據預設 AWS 區域，會在每個 中設定 VPC 來建立新 AWS 帳戶。您的企業可能有建立 VPCs的標準實務，這需要您刪除 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為 True。

```
aft_feature_delete_default_vpcs_enabled
```

以下是 AFT 部署輸入組態的範例。

```
module "aft" {
  source = "github.com/aws-ia/terraform-aws-control_tower_account_factory"
  ct_management_account_id    = var.ct_management_account_id
  log_archive_account_id      = var.log_archive_account_id
  audit_account_id            = var.audit_account_id
  aft_management_account_id   = var.aft_management_account_id
  ct_home_region              = var.ct_home_region
  tf_backend_secondary_region = var.tf_backend_secondary_region

  vcs_provider                                = "github"
  account_request_repo_name                   = "${var.github_username}/learn-
terraform-aft-account-request"
  account_provisioning_customizations_repo_name = "${var.github_username}/learn-
terraform-aft-account-provisioning-customizations"
  global_customizations_repo_name             = "${var.github_username}/learn-
terraform-aft-global-customizations"
  account_customizations_repo_name            = "${var.github_username}/learn-
terraform-aft-account-customizations"

  # Optional Feature Flags
  aft_feature_delete_default_vpcs_enabled = true
  aft_feature_cloudtrail_data_events      = false
  aft_feature_enterprise_support          = false
}
```

請參閱預設 VPC 和預設子網路，進一步了解預設 VPCs。

適用於 Terraform 的 AWS Control Tower 帳戶工廠的資源考量事項

當您使用 AWS Control Tower Account Factory for Terraform 設定登陸區域時，會在 AWS 您的帳戶內建立數種類型的 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。您搜尋的鍵/值對為：

```
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中找到搜尋 的資源。

> **Note**
>
> AFT 不會在管理帳戶中建立任何 AWS Backup 資源。

帳戶最初建立的資源資料表

適用於 Terraform 管理帳戶的 AWS Control Tower 帳戶工廠

AWS 服務	Resource Type (資源類型)	資源名稱
AWS Identity and Access Management	角色	AWSAFTAdmin AWSAFTExecution AWSAFTService ct-aft-* aft-* codebuild_trigger_role python-layer-builder-aft-common-*
AWS Identity and Access Management	政策	aft-*
CodeCommit：	儲存庫	aft-*
CodeBuild：	組建專案	aft-* ct-aft-* python-layer-builder-aft-common-*

AWS 服務	Resource Type (資源類型)	資源名稱
程式碼管道	管道	*YourAccountId* -customizations-pipeline
Amazon S3	儲存貯體	aft-*
Lambda	函數	aft-*
Lambda	層	aft-common-*
DynamoDB	表格	aft-request aft-request-audit aft-request-metadata aft-controltower-events
步驟函數	狀態機器	aft-account-provisioning-customizations aft-account-provisioning-framework aft-feature-options aft-invoke-customizations
VPC	VPC	aft-management-vpc
Amazon SNS	主題	aft-notifications aft-failure-notifications
Amazon EventBridge	事件匯流排	aft-events-from-ct-management

AWS 服務	Resource Type (資源類型)	資源名稱
Amazon EventBridge	事件規則	aft-account-provisioning-customizations-trigger aft-account-request-codepipeline-trigger aft-lambda-account-request-processor aft-controltower-event-logger
Key Management Service (KMS)	客戶受管金鑰	aft-backend-*-kms-key aft
AWS Systems Manager	參數存放區	/aft/*
Amazon SQS	佇列	aft-account-request.fifo aft-account-request-dlg.fifo
CloudWatch	日誌群組	/aws/*/ct-aft-* /aws/*/aft-* /aws/codebuild/python-layer-builder-aft-common-*
AWS 備份	保存庫	aft-controltower-backup-vault
AWS 備份	計劃	aft-controltower-backup-plan
AWS 支援中心（選用）	支援計劃	Enterprise

AWS 透過 AWS Control Tower Account Factory for Terraform 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 支援中心（選用）	支援計劃	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	AWSAFTExecution AWSAFTService aft-controltower-events-rule
AWS Systems Manager	參數存放區	/aft/*
EventBridge	事件規則	aft-capture-ct-events
CloudTrail（選用）	線索	aws-aft-CustomizationsCloudTrail
AWS Support Center（選用）	支援計劃	Enterprise

AWS Control Tower 日誌封存帳戶

AWS 服務	Resource Type (資源類型)	資源名稱
AWS Identity and Access Management	角色	AWSAFTExecution AWSAFTService
Key Management Service (KMS)	客戶受管金鑰	aft
Amazon S3	儲存貯體	aws-aft-logs-*

AWS 服務	Resource Type (資源類型)	資源名稱
		aws-aft-s3-access-logs-*
AWS 支援中心（選用）	支援計劃	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	AWSAFTExecution AWSAFTService
AWS 支援中心（選用）	支援計劃	Enterprise

必要角色

一般而言，角色和政策是 中身分和存取管理 (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，這會限制對每個角色和政策的最低必要動作和資源集的許可。這些角色和政策會獲指派 AWS 標籤`key:value`對， `managed_by:AFT`用於識別。

除了這些 IAM 角色之外，AFT 還會建立三個基本角色：

- `AWSAFTAdmin` 角色
- `AWSAFTExecution` 角色
- `AWSAFTService` 角色

以下各節會說明這些角色。

AWSAFTAdmin 角色，說明

當您部署 AFT 時，`AWSAFTAdmin`角色會在 AFT 管理帳戶中建立。此角色允許 AFT 管道擔任 AWS Control Tower 和 AFT 佈建帳戶中`AWSAFTExecution`的角色，藉此執行與帳戶佈建和自訂相關的動作。

以下是連接到AWSAFTAdmin角色的內嵌政策 (JSON 成品）：

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": [
                "arn:aws:iam::*:role/AWSAFTExecution",
                "arn:aws:iam::*:role/AWSAFTService"
            ]
        }
    ]
}
```

下列 JSON 成品顯示AWSAFTAdmin角色的信任關係。預留位置號碼012345678901會由 AFT 管理帳戶 ID 號碼取代。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

AWSAFTExecution 角色，說明

部署 AFT 時，AWSAFTExecution角色會在 AFT 管理和 AWS Control Tower 管理帳戶中建立。稍後，AFT 管道會在 AFT 帳戶佈建階段期間，在每個 AFT 佈建帳戶中建立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 管道針對 AFT 佈建帳戶和共用帳戶，執行在 AFT 架構佈建和佈建自訂階段期間執行的步驟。

> **不同的角色可協助您限制範圍**
>
> 最佳實務是將自訂許可與 資源初始部署期間允許的許可分開。請記住，AWSAFTService角色適用於帳戶佈建，而AWSAFTExecution角色適用於帳戶自訂。此分隔會限制管道每個階段期間允許的許可範圍。如果您自訂 AWS Control Tower 共用帳戶，此區別尤其重要，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 角色的許可： AdministratorAccess – AWS 受管政策

下列 JSON 成品顯示連接至AWSAFTExecution角色的 IAM 政策 （信任關係）。預留位置號碼012345678901會由 AFT 管理帳戶 ID 號碼取代。

的信任政策 AWSAFTExecution

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/AWSAFTAdmin"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

AWSAFTService 角色，說明

此AWSAFTService角色會在所有已註冊和受管帳戶中部署 AFT 資源，包括共用帳戶和管理帳戶。先前僅由 AWSAFTExecution角色部署的資源。

該AWSAFTService角色旨在供服務基礎設施在佈建階段期間部署資源，而該AWSAFTExecution角色僅用於部署自訂。透過以此方式擔任角色，您可以在每個階段維持更精細的存取控制。

AWSAFTService 角色的許可： AdministratorAccess – AWS 受管政策

下列 JSON 成品顯示連接至AWSAFTService角色的 IAM 政策（信任關係）。預留位置號碼012345678901會由 AFT 管理帳戶 ID 號碼取代。

的信任政策 AWSAFTService

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/AWSAFTAdmin"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

元件服務

當您部署 AFT 時，元件會從每個 AWS 服務新增至您的 AWS 環境。

- AWS Control Tower – AFT 使用 AWS Control Tower 管理帳戶中的 AWS Control Tower 帳戶工廠來佈建帳戶。
- Amazon DynamoDB – AFT 會在 AFT 管理帳戶中建立 Amazon DynamoDB 資料表，以存放帳戶請求、帳戶更新稽核歷史記錄、帳戶中繼資料和 AWS Control Tower 生命週期事件。AFT 也會建立 DynamoDB Lambda 觸發來啟動下游程序，例如啟動 AFT 帳戶佈建工作流程。
- Amazon Simple Storage Service – AFT 會在 AFT 管理帳戶和 AWS Control Tower 日誌封存帳戶中建立 Amazon Simple Storage Service (S3) 儲存貯體，以存放 AFT 管道所需的 AWS 服務所產生的

日誌。AFT 也會在主要和次要 中建立 Terraform 後端 S3 儲存貯體 AWS 區域，以存放 AFT 管道工作流程期間產生的 Terraform 狀態。

- Amazon Simple Notification Service – 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。您可能會使用您選擇的通訊協定來接收這些訊息。
- Amazon Simple Queuing Service – AFT 在 AFT 管理帳戶中建立 Amazon Simple Queuing Service (Amazon SQS) FIFO 佇列。佇列可讓您平行提交多個帳戶請求，但一次傳送一個請求給 AWS Control Tower 帳戶工廠，以進行循序處理。
- AWS CodeBuild – AFT 在 AFT 管理帳戶中建立 AWS CodeBuild 組建專案，以在各種組建階段初始化、編譯、測試和套用 AFT 原始程式碼的 Terraform 計劃。
- AWS CodePipeline – AFT 在 AFT 管理帳戶中建立 AWS CodePipeline 管道，以與您所選、支援的 AFT 原始碼 AWS CodeStar 連線供應商整合，並在 AWS CodeBuild 中觸發建置任務。
- AWS Lambda – AFT 在 AFT 管理帳戶中建立 AWS Lambda 函數和層，以在帳戶請求、AFT 帳戶佈建和帳戶自訂程序期間執行步驟。
- AWS Systems Manager 參數存放區 – AFT 會在 AFT 管理帳戶中設定 AWS Systems Manager 參數存放區，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 CloudWatch 日誌群組，以存放由 AFT 管道使用之 AWS 服務產生的日誌。CloudWatch 日誌的保留期間設定為 `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聯網環境中，以提高安全性。
- AWS KMS – AFT 在 AWS Key Management Service (KMS)。AFT 會建立金鑰來加密 Terraform 狀態、存放在 DynamoDB 資料表中的資料，以及 SNS 主題。這些日誌和成品會在 AFT 部署 AWS 資源和服務時產生。AFT 建立的 KMS 金鑰預設會啟用每年輪換。
- AWS Identity and Access Management (IAM) – AFT 遵循建議的最低權限模型。它會視需要在 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，以在 AFT 管道工作流程期間執行所需的動作。
- AWS Step Functions – AFT 在 AFT 管理帳戶中建立 AWS Step Functions 狀態機器。這些狀態機器會協調和自動化 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，以在 AFT 管理帳戶的 DynamoDB 資料表中長期擷取和存放 AWS Control Tower 生命週期事件。AFT 在 AFT 管理和 AWS Control Tower 管理帳戶中建立 Amazon 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 Control Tower 管理帳戶中建立 AWS CloudTrail 組織追蹤，用於記錄 Amazon S3 儲存貯體和 AWS Lambda 函數的資料事件。AFT 會將這些日誌傳送至 AWS Control Tower 日誌封存帳戶中的中央 S3 儲存貯體。
- AWS 支援 （選用） – 啟用此功能時，AFT 會為 AFT 佈建的帳戶開啟 AWS 企業支援計劃。根據預設， AWS 帳戶會在基本 AWS 支援計劃啟用的情況下建立。

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。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擁有詳細資訊。

以下是 AFT 管道執行的後續步驟。

1. 驗證帳戶請求輸入。
2. 擷取已佈建帳戶的相關資訊，例如帳戶 ID。
3. 將帳戶中繼資料存放在 AFT 管理帳戶中的 DynamoDB 資料表中。
4. 在新佈建的帳戶中建立 AWSAFTExecution IAM 角色。AFT 會擔任此角色來執行帳戶自訂階段，因為此角色會授予帳戶工廠產品組合的存取權。
5. 套用您在帳戶請求輸入參數中提供的帳戶標籤。
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。下一節說明如何在`git`儲存庫中使用 AWS Step Functions 狀態機器設定這些自訂。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，但您先前已設定架構，在帳戶佈建工作流程中提供自訂整合，然後再將其他自訂新增至下一個階段的帳戶。
8. 對於每個佈建的帳戶，它會 AWS CodePipeline 在 AFT 管理帳戶中建立 ，該帳戶將執行以執行（下一個、全域）帳戶自訂階段。
9. 叫用每個佈建（和目標）帳戶的帳戶自訂管道。
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自訂、非 Terraform 整合，這些自訂會包含在 AFT 帳戶佈建工作流程中。例如，您可能需要特定自訂，以確保 AFT 建立的所有帳戶都符合組織的標準和政策，例如安全標準，而且這些標準可能會在其他自訂之前新增至帳戶。這些帳戶佈建架構自訂會在每個佈建帳戶上實作，之後才開始全球帳戶自訂階段。

> **Note**
>
> 本節所述的 AFT 功能適用於了解 AWS Step Functions 功能的進階使用者。或者，我們建議您在帳戶自訂階段與全球協助程式合作。

AFT 帳戶佈建架構會呼叫您定義的 AWS Step Functions 狀態機器，以實作您的自訂。請參閱 AWS Step Functions 文件，進一步了解可能的 狀態機器整合。

以下是一些常見的整合。

- 您選擇的語言 AWS Lambda 函數
- AWS ECS 或 AWS Fargate 任務，使用 Docker 容器
- 使用自訂工作者的 AWS Step Functions 活動，託管於 AWS 或內部部署
- Amazon SNS 或 SQS 整合

如果未定義 AWS Step Functions 狀態機器，則階段會通過無操作。若要建立 AFT 帳戶佈建自訂狀態機器，請遵循 中的指示建立您的 AFT 帳戶佈建自訂狀態機器。新增自訂之前，請確定您已備妥先決條件。

這些類型的整合不屬於 AWS Control Tower，而且無法在 AFT 帳戶自訂的全域預先 API 階段期間新增。反之，AFT 管道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。您必須在啟動 AFT 帳戶佈建階段之前，事先建立您的狀態機器來實作這些自訂，如以下各節所述。

建立狀態機器的先決條件

- 完全部署的 AFT。如需 AFT 部署的詳細資訊部署適用於 Terraform (AFT) 的 AWS Control Tower 帳戶工廠，請參閱 。
- 在您的環境中設定儲存`git`庫以進行 AFT 帳戶佈建自訂。如需詳細資訊，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：修改狀態機器定義

修改範例`customizations.asl.json`狀態機器定義。此範例在您為儲存 AFT 帳戶佈建自訂而設定的儲存`git`庫中可用，位於部署後步驟中。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 Terraform 組態

在具有自訂整合狀態機器定義的相同`git`儲存庫中包含`.tf`副檔名的 Terraform 檔案。例如，如果您選擇在狀態機器任務定義中呼叫 Lambda 函數，您會在相同的目錄中包含 `lambda.tf` 檔案。請務必包含自訂組態所需的 IAM 角色和許可。

當您提供適當的輸入時，AFT 管道會自動調用您的狀態機器，並將您的自訂部署為 AFT 帳戶佈建架構階段的一部分。

重新啟動 AFT 帳戶佈建架構和自訂

AFT 會針對透過 AFT 管道提供的每個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. 對帳戶請求儲存庫中的現有帳戶進行任何變更。
2. 使用 AFT 佈建新帳戶。

帳戶自訂

AFT 可以在佈建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。使用此管道，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。

概觀

在您選擇的`git`儲存庫中指定自訂之後，無論是存放全域自訂的儲存庫，或是存放帳戶自訂的儲存庫，帳戶自訂階段都會由 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）

您可以選擇將特定自訂套用至 AFT 佈建的所有帳戶。例如，如果您需要建立特定 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的組態。例如，只有特定帳戶可能需要存取網際網路閘道。

自訂先決條件

開始自訂帳戶之前，請確定已備妥這些先決條件。

- 完全部署的 AFT。如需如何部署的資訊，請參閱 設定和啟動適用於 Terraform 的 AWS Control Tower 帳戶工廠。
- 預先填入git的儲存庫，用於您環境中的全域自訂和帳戶自訂。如需詳細資訊部署後步驟，請參閱中的步驟 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儲存庫。

- 如果您的自訂組態採用 Python 程式或指令碼的形式，請將這些組態放在儲存庫的 api_helpers/python 資料夾下。
- 如果您的自訂組態採用 Bash 指令碼形式，請將這些組態放在儲存庫的 api_helpers 資料夾下。
- 如果您的自訂組態採用 Terraform 格式，請將它們放在儲存庫中的 terraform 資料夾下。
- 如需建立自訂組態的詳細資訊，請參閱全域自訂 README 檔案。

> **Note**
>
> 在 AFT 管道的 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

您可以將特定資料夾結構推送至您選擇的儲存庫，以套用帳戶自訂。帳戶自訂會在 AFT 管道和全域自訂階段之後自動套用。您也可以在帳戶自訂儲存庫中建立多個資料夾，其中包含不同的帳戶自訂。對於您需要的每個帳戶自訂，請使用下列步驟。

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account_customizations_name您在帳戶請求中提供的 相符。
2. 將組態新增至您的特定帳戶自訂資料夾

   您可以根據組態的格式，將組態新增至您的帳戶自訂資料夾。

- 如果您的自訂組態採用 Python 程式或指令碼的形式，請將它們放在儲存庫中的 ***#account_customizations_name#***/api_helpers/python 資料夾下。
- 如果您的自訂組態是 Bash 指令碼的形式，請將它們放在儲存庫中的 ***#account_customizations_name#***/api_helpers 資料夾下。
- 如果您的自訂組態採用 Terraform 格式，請將它們放在儲存庫中的 ***#account_customizations_name#***/terraform 資料夾下。

如需建立自訂組態的詳細資訊，請參閱帳戶自訂 README 檔案。

3. 請參閱帳戶請求檔案中的特定**account_customizations_name**參數

   AFT 帳戶請求檔案包含輸入參數 `account_customizations_name`。輸入您帳戶自訂的名稱做為此參數的值。

> **Note**
>
> 您可以為環境中的帳戶提交多個帳戶請求。當您想要套用不同或類似的帳戶自訂時，請在帳戶請求中使用`account_customizations_name`輸入參數來指定帳戶自訂。如需詳細資訊，請參閱提交多個帳戶請求。

重新叫用自訂

AFT 提供在 AFT 管道中重新叫用自訂項目的方法。當您新增新的自訂步驟，或變更現有的自訂時，此方法非常有用。當您重新叫用 時，AFT 會啟動自訂管道，以對 AFT 佈建帳戶進行變更。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，或根據標籤選取的帳戶。

請依照這三個步驟，為 AFT 佈建的帳戶重新叫用自訂。

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，並將變更推回`git`儲存庫。此時，不會發生任何情況。自訂管道必須由事件來源調用，如接下來兩個步驟所述。

步驟 2：啟動 AWS Step Function 執行以重新叫用自訂

AFT 提供在 AFT 管理帳戶中呼叫`aft-invoke-customizations`的 AWS Step Function。該函數的目的是為 AFT 佈建的帳戶重新調用自訂管道。

以下是您可以建立以將輸入傳遞至 aft-invoke-customizations AWS Step Function 的事件結構描述 (JSON 格式) 範例。

```
{
  "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包含在重新叫用程序中或從中排除的帳戶。您可以依組織單位 (OU)、帳戶標籤和帳戶 ID 進行篩選。如果您未套用任何篩選條件並包含陳述式 "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 Account Factory for Terraform (AFT) 版本為 1.6.5 或更新版本，您可以使用語法 鎖定巢狀 OUs`0U Name (ou-id-1234)`。如需詳細資訊，請參閱 GitHub 上的下列主題。

在您填寫事件參數之後，Step Functions 會執行並叫用對應的自訂。AFT 一次最多可以叫用 5 個自訂項目。Step Functions 會等待 和 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 Step Function 輸出並監看執行中的 AWS CodePipeline

- 產生的 Step Function 輸出包含符合 Step Function 輸入事件來源的帳戶 IDs。
- 導覽至開發人員工具下的 AWS CodePipeline，並檢視帳戶 ID 對應的自訂管道。

使用 AFT 帳戶自訂請求追蹤進行故障診斷

基於 AWS Lambda 的帳戶自訂工作流程會發出包含目標帳戶和自訂請求 IDs日誌。AFT 可讓您使用 Amazon CloudWatch Logs 追蹤和疑難排解自訂請求，方法是提供 CloudWatch Logs Insights 查詢，您可以使用這些查詢來依目標帳戶或自訂請求 ID 篩選與自訂請求相關的 CloudWatch Logs。如需詳細資訊，請參閱《Amazon CloudWatch Logs 使用者指南》中的使用 Amazon CloudWatch Logs 分析日誌資料。 Amazon CloudWatch

使用適用於 AFT 的 CloudWatch Logs Insights

1. 透過 https://console.aws.amazon.com/cloudwatch/ 開啟 CloudWatch 主控台。
2. 從導覽窗格中，選擇日誌，然後選擇日誌洞察。
3. 選擇查詢。
4. 在範例查詢下，選擇適用於 Terraform 的帳戶工廠，然後選取下列其中一個查詢：
   - 依帳戶 ID 的自訂日誌

     > **Note**
     >
     > 請務必將 *"YOUR-ACCOUNT-ID"* 取代為您的目標帳戶 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/
```

- 依自訂請求 ID 的自訂日誌

> **Note**
>
> 請務必使用自訂請求 ID 取代 *"YOUR-CUSTOMIZATION-REQUEST-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自訂請求 ID。如需 AFT 帳戶佈建架構的詳細資訊，請參閱 AFT 帳戶佈建管道

```
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 中原始程式碼版本控制的替代方案

AFT AWS CodeCommit 用於原始程式碼版本控制系統 (VCS)，並允許其他 CodeConnections 符合您業務需求或現有架構。

如果您是第一次部署 AFT，而且沒有現有的 CodeCommit 儲存庫，則必須指定外部 VCS 供應商，做為 AFT 部署先決條件的一部分。

AFT 支援下列原始程式碼控制替代方案：

- GitHub
- GitHub Enterprise Server
- BitBucket
- GitLab

- GitLab 自我管理

> **Note**
>
> 如果您將 指定 AWS CodeCommit 為 VCS，則不需要其他步驟。AFT 會在您的環境中使用預設名稱建立必要的`git`儲存庫。不過，您可以視需要覆寫 CodeCommit 的預設儲存庫名稱，以符合您的組織標準。

使用 AFT 設定替代原始程式碼版本控制系統 （ 自訂 VCS)

若要為您的 AFT 部署設定替代原始程式碼版本控制系統，請遵循下列步驟。

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。可用的範本程式碼 。如需 AFT 帳戶請求的詳細資訊，請參閱 使用 AFT 佈建新帳戶。
- AFT 帳戶佈建自訂。可用的範本程式碼 。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 全域自訂。可用的範本程式碼 。如需 AFT 全域自訂的詳細資訊，請參閱 帳戶自訂。
- AFT 帳戶自訂。可用的範本程式碼 。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

需要下列輸入參數，才能將 VCS 提供者設定為 AFT 部署的一部分。

- vcs_provider：如果您未使用 AWS CodeCommit，`"gitlab"`請根據您的使用案例將 VCS 提供者指定為 `"bitbucket"`、`"githubenterprise"`、 `"github"`或 。
- github_enterprise_url：僅限 GitHub Enterprise 客戶，請指定 GitHub URL。
- account_request_repo_name：對於 AWS CodeCommit 使用者，此值設定為 `aft-account-request`。在 AFT 支援的第三方 VCS 提供者環境中，使用實際儲存庫名稱更新此輸入值。對於 BitBucket、Github、GitHub Enterprise、GitLab 和 GitLab 自我管理，儲存庫名稱的格式必須是 `[Org]/[Repo]`。

- account_customizations_repo_name：對於 AWS CodeCommit 使用者，此值設定為 `aft-account-customizations`。在 AFT 支援的第三方 VCS 提供者環境中，使用儲存庫名稱更新此輸入值。對於 BitBucket、Github、GitHub Enterprise、GitLab 和 GitLab 自我管理，儲存庫名稱的格式必須是 `[Org]/[Repo]`。
- account_provisioning_customizations_repo_name：對於 AWS CodeCommit 使用者，此值設定為 `aft-account-provisioning-customizations`。在 AFT 支援的第三方 VCS 提供者環境中，使用儲存庫名稱更新此輸入值。對於 BitBucket、Github、GitHub Enterprise、GitLab 和 GitLab 自我管理，儲存庫名稱的格式必須是 `[Org]/[Repo]`。
- global_customizations_repo_name：對於 AWS CodeCommit 使用者，此值設定為 `aft-global-customizations`。在 AFT 支援的第三方 VCS 提供者環境中，使用儲存庫名稱更新此輸入值。對於 BitBucket、Github、GitHub Enterprise、GitLab 和 GitLab 自我管理，儲存庫名稱的格式必須是 `[Org]/[Repo]`。
- account_request_repo_branch：分支`main`預設為 ，但值可以覆寫。

根據預設，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。如需輸入參數的詳細資訊，請參閱 AFT Terraform 模組中的 README 檔案。

> **對於現有 AWS CodeCommit 客戶**
>
> 如果您使用 AFT 的新名稱建立 CodeCommit 儲存庫，您可以透過更新這些輸入參數的值來更新儲存庫名稱。

步驟 3：完成第三方 VCS 提供者的 AWS CodeCommit 連線

當您的部署執行時，AFT 會建立所需的 AWS CodeCommit 儲存庫，或者為您選擇的第三方 VCS 提供者建立 AWS CodeCommit 連線。如果是後者，您必須手動登入 AFT 管理帳戶的主控台，以完成待定的 CodeCommit 連線。如需AWS CodeCommit 完成 CodeCommit 連線的進一步說明，請參閱 文件。CodeCommit

將 AFT 從 AWS CodeCommit 移至另一個 VCS 供應商

本節提供如何將 AWS Control Tower Account Factory for Terraform (AFT) 從 AWS CodeCommit 做為版本控制系統 (VCS) 移至另一個 VCS 供應商的概觀。

步驟 1. 在您選擇的 VCS 中設定新的儲存庫。

步驟 2. 在 中將這些儲存庫新增為新的遠端`git`。

步驟 3. 執行`git push`至新的 VCS 提供者。

> **Note**
>
> 您建立的儲存庫結構應與 in AWS CodeCommit 相同。變更結構會阻礙 AFT 執行所需程式碼的能力。
>
> 儲存庫結構：
>
> - aft-account-request
> - aft-account-customizations
> - aft-global-customizations
> - aft-account-provisioning-customizations

步驟 4. 在您的 AWS Control Tower 管理帳戶中，更新 Terraform 模組（引導）以指向您的 VCS 供應商，如下列範例所示：

範例：GitLab 搭配 Terraform OSS

– 執行 `terraform plan`以預覽變更，然後執行 `terraform apply`。

步驟 5. 完成步驟以完成 CodeConnection（先前稱為 CodeStar) 的設定：

1. 登入您的 AFT 管理帳戶
2. 找到並完成新 VCS 供應商的 pending AWS CodeConnections，如更新待定連線或 AWS 主控台 【`https://us-east-1.console.aws.amazon.com/codesuite/settings/connections`】 所述。
3. 參考：部署後步驟

> **Note**
>
> 帳戶管道會保留先前的來源，直到叫用 `aft-invoke-customizations` Step Functions 為止。此調用可以作為升級的一部分或作為下一次自訂調用的一部分來完成。

如需詳細資訊，請參閱此部落格：如何將 AWS CodeCommit 儲存庫遷移至另一個 Git 供應商。

資料保護

AWS 共同責任模型適用於 AFT 中的資料保護。基於資料保護目的，我們建議採用下列安全性最佳實務。

- 遵循 AWS Control Tower 提供的資料保護指導方針。如需詳細資訊，請參閱AWS Control Tower 中的資料保護。
- 保留在 AFT 部署時產生的 Terraform 狀態組態。如需詳細資訊，請參閱部署適用於 Terraform (AFT) 的 AWS Control Tower 帳戶工廠。
- 根據您組織的安全政策，定期輪換敏感憑證。秘密的範例包括 Terraform 字符、`git`字符等。

靜態加密

AFT 會建立使用 AWS Key Management Service 金鑰靜態加密的 Amazon S3 儲存貯體、Amazon SNS 主題、Amazon SQS 佇列和 Amazon DynamoDB 資料庫。AFT 建立的 KMS 金鑰預設會啟用每年輪換。如果您選擇 Terraform 的 Terraform Cloud 或 Terraform Enterprise 分佈，AFT 會包含 AWS Systems Manager SecureString 參數來存放敏感的 Terraform 字符值。

AFT 使用中所述的服務，元件服務該 AWS 服務預設為靜態加密。如需詳細資訊，請參閱每個 AFT 元件 AWS 服務 AWS 的文件，並了解每個服務後面的資料保護實務。

傳輸中加密

根據預設，AFT 倚賴 中所述元件服務使用傳輸中加密 AWS 的服務。如需詳細資訊，請參閱每個 AFT 元件 AWS 服務 AWS 的文件，並了解每個服務後面的資料保護實務。

對於 Terraform Cloud 或 Terraform Enterprise 分佈，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 來存取您的 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，因此 AFT 管道會停止部署和更新帳戶。

> **Important**
>
> 從 AFT 管道移除帳戶是無法復原的，可能會導致狀態遺失。

當您想要關閉已淘汰應用程式的帳戶、隔離遭入侵的帳戶，或將帳戶從一個組織移至另一個組織時，您可以從 AFT 中移除帳戶。

> **Note**
>
> 從 AFT 移除帳戶不同於刪除 AWS Control Tower 帳戶或 AWS 帳戶。當您從 AFT 移除帳戶時，AWS Control Tower 仍會管理該帳戶。若要刪除 AWS Control Tower 帳戶或 AWS 帳戶，請參閱下列內容：
>
> - 《AWS Control Tower 使用者指南》中的取消管理帳戶。
> - AWS Billing 《 使用者指南》中的關閉帳戶。

從 AFT 管道移除帳戶

下列程序說明如何從 AFT 移除帳戶。

1. 從儲存帳戶請求的儲存**git**庫移除帳戶

   在您存放帳戶請求的儲存`git`庫中，刪除您要從 AFT 中移除之帳戶的 帳戶請求。

   當您從帳戶請求儲存庫移除帳戶請求時，AFT 會刪除自訂管道和帳戶中繼資料。如需詳細資訊，請參閱 GitHub 上 AFT 的 1.8.0 版本備註。

2. 刪除 Terraform 工作區 （ 僅適用於 Terraform Cloud 和 Terraform Enterprise 客戶 ）

   刪除您要從 AFT 中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 Terraform 狀態

   在 AFT 管理帳戶中，刪除您要從 AFT 中移除之帳戶的 Amazon S3 儲存貯體內的所有相關資料夾。

   > **Tip**
   >
   > 在下列範例中，將 取代*012345678901*為 AFT 管理帳戶 ID 號碼。

   範例：Terraform OSS

當您選擇 Terraform OSS 時，您會在 `aft-backend-012345678901-primary-region`和 Amazon S3 儲存貯體中找到每個帳戶的 `aft-backend-012345678901-secondary-region` 3 個資料夾。 Amazon S3 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：Terraform Cloud 或 Terraform Enterprise

當您選擇 Terraform Cloud 或 Terraform Enterprise 時，您會在 `aft-backend-012345678901-primary-region`和 Amazon S3 `aft-backend-012345678901-secondary-region` 儲存貯體中找到每個帳戶的資料夾。這些資料夾與自訂管道狀態相關。

操作指標

根據預設，Account Factory for Terraform (AFT) 會傳送匿名操作指標至 AWS。我們使用此資料來了解客戶如何使用 AFT，以便改善解決方案的品質和功能。您可以在 AFT 部署期間變更參數，以選擇退出資料收集。啟用收集時，會將下列資料傳送至 AWS：

- 解決方案：AFT 特定的識別符
- 版本：AFT 的版本
- 全域唯一識別符 (UUID)：每個 AFT 部署隨機產生的唯一識別符
- 時間戳記：資料收集時間戳記
- 資料：客戶採取的 AFT 組態和動作

AWS 擁有收集的資料。資料收集受 AWS 隱私權政策的約束。

> **Note**
>
> 1.6.0 之前的 AFT 版本不會向 報告用量指標。 AWS

若要選擇退出報告指標：

- `aft_metrics_reporting false` 將 Terraform 輸入組態檔案中的輸入值設定為 ，如以下範例所示，然後重新部署 AFT。如果您未明確設定，則此值`true`預設為 。

如果您複製範例，請記得以 取代字串中給定項目的實際 ID 和區域值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
}
```

Account Factory for Terraform (AFT) 疑難排解指南

本節可協助您針對使用 Account Factory for Terraform (AFT) 時可能遇到的常見問題進行疑難排解。

主題

一般問題

- 超過 AWS 資源配額

  如果您的日誌群組指出您超過 AWS 資源配額，請聯絡 AWS Support。Account Factory 使用 AWS 服務 與包含 AWS CodeBuild AWS Organizations和 的資源配額 AWS Systems Manager。如需詳細資訊，請參閱下列內容：

  - CodeBuild 使用者指南中的什麼是 AWS CodeBuild？。
  - 《 Organizations 使用者指南》中的什麼是 AWS Organizations？。
  - Systems Manager 使用者指南中的什麼是 AWS Systems Manager？。
- Account Factory 的過時版本

如果您遇到問題，且認為問題是錯誤，請確定您擁有最新版的 Account Factory。如需詳細資訊，請參閱更新 Account Factory 版本。

- 已對 Account Factory 原始程式碼進行本機變更

  Account Factory 是開放原始碼專案。AWS Control Tower 支援 Account Factory 核心程式碼。如果您對 Account Factory 核心程式碼進行本機變更，AWS Control Tower 只會盡力支援您的 Account Factory 部署。

- Account Factory 角色許可不足

  Account Factory 會建立 IAM 角色和政策來管理付費帳戶部署和自訂。如果您變更這些角色或政策，Account Factory 管道可能無法執行特定動作。如需詳細資訊，請參閱必要角色。

- 帳戶儲存庫未正確填入

  在佈建帳戶之前，請務必遵循部署後步驟。

- 手動變更 OU 後未偵測偏離

> **Note**
>
> AWS Control Tower 會自動偵測漂移。如需解決偏離的資訊，請參閱偵測和解決 AWS Control Tower 中的偏離。

手動變更組織單位 (OU) 時，不會偵測到偏離。這是因為 Account Factory 的事件驅動性質所致。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。變更項目後，請求會放入佇列中，AWS Control Tower 會在佇列中透過 Service Catalog（管理帳戶詳細資訊的服務）處理它們。如果您手動變更 OU，則不會偵測到偏離，因為帳戶請求未變更。

與帳戶佈建/註冊相關的問題

- 帳戶請求（電子郵件地址/名稱）已存在

  此問題通常會在佈建期間或作為 時導致 Service Catalog 產品故障`ConditionalCheckFailedException`。

  您可以執行下列其中一項操作，找到有關問題的詳細資訊：

  - 檢閱您的 Terraform 或 CloudWatch Logs 日誌群組。

  - 檢閱傳送到 Amazon SNS 主題 的失敗`aft-failure-notifications`。
- 格式不正確的帳戶請求

  請確定您的帳戶請求遵循預期的結構描述。如需範例，請參閱 GitHub 上的 terraform-aws-control_tower_account_factory。
- 超過 AWS Organizations 資源配額

  請確定您的帳戶請求不超過 AWS Organizations 資源配額。如需詳細資訊，請參閱 AWS Organizations 的配額。

與自訂調用相關的問題

- 未加入 Account Factory 的目標帳戶

  確定自訂請求中包含的所有帳戶都已加入 Account Factory。如需詳細資訊，請參閱更新現有帳戶。
- 自訂請求目標的帳戶存在於 DynamoDB 資料表 中**`aft-request-metadata`**，但不存在於帳戶請求儲存庫中

  執行下列其中一項操作來格式化您的自訂調用請求，以排除違規帳戶：
  - 在 DynamoDB 資料表 中`aft-request-metadata`，刪除參考不再位於您帳戶請求儲存庫中帳戶的項目。
  - 不使用「全部」作為目標。
  - 未鎖定帳戶所屬的 OU。
  - 未直接鎖定帳戶。
- 對 Terraform Cloud 使用不正確的字符

  請確定您已設定正確的字符。Terraform Cloud 僅支援以團隊為基礎的權杖，不支援以組織為基礎的權杖。
- 無法在建立帳戶自訂管道之前建立帳戶；無法自訂帳戶

  變更帳戶請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，即使管道不存在，Account Factory 仍會遵循嘗試建立管道的路徑。

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 版本是 1.8.0 或更高版本，而且已從 DynamoDB 請求資料表刪除帳戶相關中繼資料的所有執行個體。

如需 AFT 1.8.0 版的相關資訊，請參閱 GitHub 上的 1.8.0 版。

如需有關如何檢查和更新 AFT 版本的資訊，請參閱下列內容：

- 檢查 AFT 版本
- 更新 AFT 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 IDs日誌，以追蹤自訂請求並進行疑難排解。如需詳細資訊，請參閱使用 AFT 帳戶自訂請求追蹤進行故障診斷。

在 AWS Control Tower 中偵測並解決偏離

識別和解決偏離是 AWS Control Tower 管理帳戶管理員的常規操作任務。解決偏離有助於確保您符合控管要求。

當您建立登陸區域時，登陸區域和所有組織單位 (OUs)、帳戶和資源都符合您選擇的控制項強制執行的控管規則。當您和您的組織成員使用登陸區域時，可能會發生此合規狀態的變更。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。

偵測偏離

AWS Control Tower 會自動偵測漂移。若要偵測偏離，該`AWSControlTowerAdmin`角色需要持續存取您的管理帳戶，以便 AWS Control Tower 可以對 進行唯讀 API 呼叫 AWS Organizations。這些 API 呼叫會顯示為 AWS CloudTrail 事件。

成員帳戶的偏離會呈現在稽核帳戶中彙總的 Amazon Simple Notification Service (Amazon SNS) 通知中。每個成員帳戶中的通知都會將提醒傳送至本機 Amazon SNS 主題和 Lambda 函數。

> **Note**
>
> 在設定中啟用帳戶的自動註冊功能時，這些 SNS 通知無法使用。

對於屬於 AWS Security Hub CSPM 服務受管標準的控制項：AWS Control Tower，偏離會顯示在 AWS Control Tower 主控台的帳戶和帳戶詳細資訊頁面上，以及透過 Amazon SNS 通知顯示。

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 主題會提供偏離通知。AWS Control Tower 主控台會在發生偏離時向管理帳戶管理員指示 。如需偏離偵測和通知 SNS 主題的詳細資訊，請參閱偏離預防和通知。

偏離通知刪除重複

如果同一組資源多次發生相同類型的偏離，AWS Control Tower 只會針對初始偏離執行個體傳送 SNS 通知。如果 AWS Control Tower 偵測到此漂移執行個體已修復，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。

範例：SCP 偏離的處理方式如下

- 如果您多次修改相同的受管 SCP，您會在第一次修改時收到通知。
- 如果您修改受管 SCP，然後修復偏離，然後再次修改，您將收到兩個通知。

帳戶偏離的類型

- 帳戶在 OUs之間移動 （請參閱 啟用基準的繼承偏離和 啟用控制項上的繼承偏離)
- 帳戶已從組織中移除

> **Note**
>
> 當您將帳戶從一個 OU 移至另一個 OU 時，不會移除先前 OU 的控制項。如果您在目的地 OU 上啟用任何新的勾點型控制，舊的
> 掛鉤型控制項會從帳戶移除，而新的控制項會取代它。當帳戶變更 OUs 時，一律必須手動移除使用 SCPs 和 AWS Config 規則實作的控制項。

政策偏離的範例

- SCP 已更新
- SCP 從 OU 分離

如需詳細資訊，請參閱控管偏離的類型。

檢視偏離

您可以透過主控台或 APIs 檢視帳戶和 OUs 的偏離狀態，並識別帳戶和 OU 組態何時偏離或不同步。偏離狀態也會與 SNS 訊息通訊。如需接收這些 SNS 訊息的詳細資訊，請參閱訂閱 SNS 主題的相關指導。

若要在主控台中檢視 OU 和帳戶偏離狀態，請導覽至組織頁面，然後選取您要檢查OUs 或帳戶。

若要以程式設計方式檢視 OUs 和帳戶的偏離狀態，請呼叫 `ListEnabledBaselines` API 來檢視已啟用基準的狀態。若要使用 `ListEnabledBaselines` API 以程式設計方式檢視個別帳戶的狀態，請使用 `includeChildren`旗標。您可以依這些狀態進行篩選，並只查看需要您注意的帳戶和 OUs。

> **Note**
>
> AWS Control Tower 會在每個偏離修復操作完成時產生生命週期事件。

解決偏離

雖然偵測是自動的，但解決偏離的步驟必須透過主控台或使用 APIs手動完成。（除非在某些情況下，已為移動的帳戶啟用自動註冊。）

例如，您可以透過呼叫 `ResetEnabledControl` API，以程式設計方式解決控制項的政策偏離。

若要解決 OU 的組態基準偏離，您可以在 主控台中選擇重新註冊 OU。如果偏離是由單一帳戶造成，您可以在 主控台中選擇更新帳戶。若要使用 APIs 解決基準偏離，您可以在 OU 上呼叫 `ResetEnabledBaseline` API。

摘要

- 許多類型的偏離可以透過登陸區域設定頁面解決。您可以在版本區段中選擇重設按鈕，以解決這些類型的偏離。
- 如果您的 OU 帳戶少於 1000 個，您可以在組織頁面或 OU 詳細資訊頁面上選取重新註冊 OU，以解決帳戶工廠佈建帳戶中的偏離或 SCP 偏離。
- 您可以透過更新個別帳戶來解決帳戶偏離已移動的成員帳戶，例如 。如需詳細資訊，請參閱在 主控台中更新帳戶。
- 對於控制項，您可以透過呼叫 `ResetEnabledControl` API 來解決許多類型的偏離。
- OUs 和帳戶的基準偏離可以透過呼叫 `ResetEnabledBaseline` API，或在 AWS Control Tower 主控台中選擇重新註冊 OU 或更新帳戶來解決。
- 若要解決帳戶在 OUs 之間移動時發生的繼承偏離，您可以啟用自動註冊功能。啟用自動註冊時，AWS Control Tower 會自動修復繼承偏離，方法是將基準資源和控制組態從目的地 OU 套用至移動的帳戶。您可以在 主控台的登陸區域設定頁面上啟用自動註冊，或呼叫 `RemediationType` 參數設定為繼承偏離的 `UpdateLandingZone` API。如需詳細資訊，請參閱使用自動註冊來移動和註冊帳戶。

> **⚠ 當您採取行動來解決登陸區域版本的偏離時，有兩種行為是可能的。**
>
> - 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，偏離的登陸區域資源會重設為儲存的 AWS Control Tower 組態。登陸區域版本保持不變。

- 如果您不是最新版本，則必須選擇更新。登陸區域已升級至最新的登陸區域版本。漂移會在此程序中解決。

偏離和政策掃描的考量

AWS Control Tower 會每天掃描您的受管 SCPs、RCPs 和宣告政策，以確認對應的控制項已正確套用，且尚未漂移。為了擷取這些資源並對其執行檢查，AWS Control Tower 會使用管理帳戶中的角色 AWS Organizations 代表您呼叫 。

如果 AWS Control Tower 掃描發現偏離，您將會收到通知。AWS Control Tower 每個偏離問題只會傳送一個通知，因此如果您的登陸區域已經處於偏離狀態，除非找到新的偏離項目，否則您不會收到其他通知。

AWS Organizations 會限制呼叫其每個 APIs的頻率。此限制以每秒交易數 (TPS) 表示，稱為 TPS 限制、限流率或 API 請求率。當 AWS Control Tower 透過呼叫 來稽核您的 SCPs、RCPs 和宣告政策時 AWS Organizations，AWS Control Tower 發出的 API 呼叫會計入您的 TPS 限制，因為 AWS Control Tower 會使用 管理帳戶來進行呼叫。

在極少數情況下，無論您透過第三方解決方案或您撰寫的自訂指令碼，重複呼叫相同的 APIs 時都可以達到此限制。例如，如果您和 AWS Control Tower 在同一時間 (1 秒內） 呼叫相同的 AWS Organizations APIs，並達到 TPS 限制，則會調節後續呼叫。也就是說，這些呼叫會傳回錯誤，例如 `Rate exceeded`。

如果超過 API 請求率

- 如果 AWS Control Tower 達到限制並受到調節，我們會暫停稽核的執行，並在稍後繼續執行。
- 如果您的工作負載達到限制並受到調節，結果可能從輕微延遲到工作負載中的嚴重錯誤，取決於工作負載的設定方式。此邊緣案例需要注意。

每日 SCP 掃描包含

1. 擷取您最近作用中OUs。
2. 對於每個已註冊的 OU，擷取由 AWS Control Tower 管理且連接至 OU 的所有 SCPs。受管 SCPs 具有以 開頭的識別符`aws-guardrails`。
3. 對於在 OU 上啟用的每個預防性控制項，驗證控制項的政策陳述式是否存在於 OU 的受管 SCPs 中。

OU 可能有一或多個受管 SCPs。

要立即解決的偏離類型

系統管理員可以解決大多數類型的偏離。您必須立即解決幾種類型的偏離，包括刪除 AWS Control Tower 登陸區域所需的組織單位。以下是一些您可能想要避免的主要偏離範例：

- 請勿刪除安全 OU：在 AWS Control Tower 設定登陸區域期間，不應刪除原本名為安全的組織單位。如果您刪除它，您會看到錯誤訊息，指示您立即重設登陸區域。在重設完成之前，您將無法在 AWS Control Tower 中採取任何其他動作。
- 請勿刪除必要角色：當您登入主控台進行 IAM 角色偏離時，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，指示您重設登陸區域。這些角色為 `AWSControlTowerAdmin` `AWSControlTowerCloudTrailRole` `AWSControlTowerStackSetRole`。

  如需使用者角色的詳細資訊，請參閱 使用 AWS Control Tower 主控台所需的許可。
- 請勿刪除所有額外的 OUs：AWS Control Tower 至少需要一個額外的 OU 才能運作，但它不必是沙盒 OU。
- 請勿移除共用帳戶：如果您使用 AWS Organizations 主控台或 APIs 從基礎 OUs 移除共用帳戶，例如從安全 OU 移除記錄帳戶。移動這些帳戶會建立必須修復的移動帳戶偏離類型。若要修復此類型的偏離，您必須更新登陸區域。

> **Note**
>
> 根據最佳實務，請勿將這些共用帳戶移出基礎 OU。

資源的可修復變更

以下是允許的 AWS Control Tower 資源變更清單，雖然它們會建立可解決的偏離。這些允許操作的結果可在 AWS Control Tower 主控台中檢視，但可能需要重新整理。

如需如何解決產生的偏離的詳細資訊，請參閱在 AWS Control Tower 外部管理資源。

AWS Control Tower 主控台以外允許的變更

- 變更已註冊 OU 的名稱。

- 變更安全 OU 的名稱。
- 變更非實體 OUs 中成員帳戶的名稱。
- 在安全 OU 中變更 AWS Control Tower 共用帳戶的名稱。
- 刪除非實體 OU。
- 從非實體 OU 刪除已註冊的帳戶。
- 在安全 OU 中變更共用帳戶的電子郵件地址。
- 變更已註冊 OU 中成員帳戶的電子郵件地址。

> **Note**
>
> 在 OUs 之間移動帳戶會被視為偏離，必須加以解決。

偏離和新帳戶佈建

如果您的登陸區域處於偏離狀態，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 佈建新帳戶 AWS Service Catalog。如需說明，請參閱在 Service Catalog 主控台中使用 Account Factory 佈建帳戶。

特別是，如果您已透過 Service Catalog 對帳戶進行特定變更，例如變更產品組合的名稱，則註冊帳戶功能將無法運作。

控管偏離的類型

當 OUs、SCPs 和成員帳戶變更或更新時，就會發生治理偏離，也稱為組織偏離。可在 AWS Control Tower 中偵測到的控管偏離類型如下：

- 帳戶和 OU 控管偏離
- 登陸區域偏離
- 非 SCP 控制項的控制項偏離
- 基準和控制項的繼承偏離

以下各節提供 AWS Control Tower 報告之此類偏離的詳細資訊，以及如何解決這些偏離。

> **Note**
>
> AWS Control Tower 將停止向 LZ4.0+ 客戶的 SNS 主題傳送偏離通知，並改為開始將偏離通知傳送至管理帳戶中的 EventBridge。若要查看如何透過 EventBridge 接收偏離通知的範例事件和指引，請參閱 EventBridge 建立的下列章節。

帳戶和 OU 控管偏離

- 已移動的成員帳戶
- 已移除成員帳戶
- 非計劃的受管 SCP 更新
- SCP 從受管 OU 分離

登陸區域偏離

另一種偏離類型是登陸區域偏離，可透過 管理帳戶找到。登陸區域偏離包含 IAM 角色偏離，或任何特別影響基礎 OUs 和共用帳戶的組織偏離類型。

- 刪除的基礎 OU
- 已停用信任的存取

登陸區域偏離的特殊情況是角色偏離，當所需的角色不可用時偵測到。如果發生此類偏離，主控台會顯示警告頁面，以及如何還原角色的一些指示。在角色偏離解決之前，您的登陸區域無法使用。如需角色偏離的詳細資訊，請參閱名為 的章節中的不要刪除必要角色要立即解決的偏離類型。

非 SCP 控制項的控制偏離

AWS Control Tower 會報告使用資源控制政策 (RCP)、宣告政策和屬於服務受管標準 AWS Control Tower 一部分的控制項的控制偏離。 RCPs AWS Security Hub CSPM

- Security Hub CSPM 控制偏離
- 控制政策偏離

基準和控制項的繼承偏離

- 啟用基準偏離

當成員帳戶的基準組態與套用至父 OU 的基準組態不同時，AWS Control Tower 會針對這些 OUs 和帳戶上已啟用的基準（資源組態）報告繼承偏離。如需基準的詳細資訊，請參閱基準類型。

- 啟用基準的繼承偏離

- 啟用的控制偏離

當成員帳戶上啟用的控制組態與套用至父 OU 的控制組態不同時，AWS Control Tower 會針對這些 OUs和帳戶上啟用的控制項報告繼承偏離。

- 啟用控制項上的繼承偏離

> **未報告的偏離**
>
> - AWS Control Tower 不會尋找與使用管理帳戶的其他服務相關的偏離 AWS CloudTrail，包括 Amazon CloudWatch CloudFormation AWS Config、IAM Identity Center 等。
> - 如果您修改基準中包含的資源，AWS Control Tower 不會偵測可能發生的資源偏離或其他類型的偏離。

已移動的成員帳戶

> **Note**
>
> 對於使用 LZ 4.0+ 的客戶，AWS Control Tower 不會為沒有 AWSControlTowerBaseline 的帳戶工廠帳戶傳送移動帳戶偏離通知。

這種類型的偏離發生在帳戶上，而不是 OU。當 AWS Control Tower 成員帳戶、稽核帳戶或日誌封存帳戶從已註冊的 AWS Control Tower OU 移至任何其他 OU 時，可能會發生這種偏離。在許多情況下，如果您在設定頁面上啟用帳戶的自動註冊功能，您可以避免此類偏離。如需詳細資訊，請參閱使用自動註冊來移動和註冊帳戶。

以下是偵測到這種偏離時，偏離通知的範例。

```
{
  "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 1000 accounts, you must update the provisioned product in Account Factory.",
  "AccountId" : "012345678909",
  "SourceId" : "012345678909",
  "DestinationId" : "ou-3210-1EXAMPLE"
}
```

解決方案

當 OU 中具有最多 1000 個帳戶的 Account Factory 佈建帳戶發生此類偏離時，您可以透過下列方式加以解決：

- 在 AWS Control Tower 主控台中導覽至組織頁面，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）。
- 在 AWS Control Tower 主控台中導覽至組織頁面，然後選擇重新註冊包含帳戶的 OU （多個帳戶的最快選項）。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 中的佈建產品。如需詳細資訊，請參閱使用 AWS Control Tower 更新和移動帳戶。

> **Note**
>
> 如果您有數個個別帳戶要更新，也請參閱使用此方法來使用指令碼進行更新：使用自動化佈建和更新帳戶。

- 當這種類型的偏離發生在具有超過 1000 個帳戶的 OU 中時，偏離解析度可能取決於已移動的帳戶類型，如下一段所述。如需詳細資訊，請參閱更新您的登陸區域。
  - 如果已移動 Account Factory 佈建帳戶 – 在少於 1000 個帳戶的 OU 中，您可以透過更新 Account Factory 中的佈建產品、重新註冊 OU 或更新您的登陸區域來解決帳戶偏離。

    在超過 1000 個帳戶的 OU 中，您必須透過 AWS Control Tower 主控台或佈建產品對每個移動的帳戶進行更新，以解決偏離，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 更新和移動帳戶。

- 如果已移動共用帳戶 – 您可以透過更新登陸區域來解決移動稽核或日誌封存帳戶的偏離。如需詳細資訊，請參閱更新您的登陸區域。

> ⚠ 已棄用的欄位名稱
>
> 欄位名稱MasterAccountID已變更為 ManagementAccountID以符合 AWS 準則。舊名稱已棄用。自 2022 年起，包含已棄用欄位名稱的指令碼將無法再運作。

已移除成員帳戶

當成員帳戶從已註冊的 AWS Control Tower 組織單位中移除時，可能會發生這種類型的偏離。下列範例顯示偵測到此類偏離時的偏離通知。

```
{
  "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"
}
```

Resolution

- 當成員帳戶中發生此類偏離時，您可以透過在 AWS Control Tower 主控台或 Account Factory 中更新帳戶來解決偏離。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 更新和移動帳戶。
- 如果從基礎 OU 移除共用帳戶，您必須重設登陸區域來解決偏離。在此偏離解決之前，您將無法使用 AWS Control Tower 主控台。
- 如需解決帳戶和 OU 偏離的詳細資訊，請參閱如果您在 AWS Control Tower 外部管理資源。

> **Note**
>
> 在 Service Catalog 中，代表帳戶的 Account Factory 佈建產品不會更新以移除帳戶。相反地，佈建的產品會顯示為 TAINTED 和錯誤狀態。若要清除，請前往 Service Catalog，選擇佈建的產品，然後選擇終止。

非計劃的受管 SCP 更新

在主控台中 AWS Organizations 更新控制項的 SCP，或使用 AWS CLI 或其中一個 AWS SDKs以程式設計方式更新時，可能會發生這種類型的偏離。以下是偵測到這種偏離時，偏離通知的範例。

```
{
  "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"
}
```

Resolution

當這種類型的偏離發生在具有最多 1000 個帳戶的 OU 中時，您可以透過下列方式解決：

- 導覽至 AWS Control Tower 主控台中的組織頁面，以重新註冊 OU （最快選項）。如需詳細資訊，請參閱向 AWS Control Tower 註冊現有的組織單位。
- 更新您的登陸區域 （較慢選項）。如需詳細資訊，請參閱更新您的登陸區域。

當這種類型的偏離發生在具有超過 1000 個帳戶的 OU 中時，請透過更新您的登陸區域來解決此問題。如需詳細資訊，請參閱更新您的登陸區域。

SCP 從受管 OU 分離

當控制項的 SCP 從 AWS Control Tower 管理的 OU 分離時，可能會發生這種偏離。當您從 AWS Control Tower 主控台外部工作時，這種情況特別常見。以下是偵測到這種偏離時，偏離通知的範例。

```
{
  "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"
}
```

Resolution

當這種類型的偏離發生在具有最多 1000 個帳戶的 OU 中時，您可以透過下列方式解決：

- 在 AWS Control Tower 主控台中導覽至 OU，以重新註冊 OU（最快選項）。如需詳細資訊，請參閱向 AWS Control Tower 註冊現有的組織單位。
- 更新您的登陸區域（較慢選項）。如果偏離影響強制性控制，更新程序會建立新的服務控制政策 (SCP)，並將其連接到 OU 以解決偏離。如需如何更新登陸區域的詳細資訊，請參閱 更新您的登陸區域。

當這種類型的偏離發生在具有超過 1000 個帳戶的 OU 中時，請透過更新您的登陸區域來解決此問題。如果偏離影響強制性控制，更新程序會建立新的服務控制政策 (SCP)，並將其連接到 OU 以解決偏離。如需如何更新登陸區域的詳細資訊，請參閱 更新您的登陸區域。

刪除的基礎 OU

這種偏離類型僅適用於 AWS Control Tower Foundational OUs，例如 Security OU。如果在 AWS Control Tower 主控台之外刪除基礎 OU，就可能發生這種情況。基礎 OUs 無法在未建立這種偏離的情況下移動，因為移動 OU 與刪除 OU 並將其新增到其他地方相同。當您透過更新登陸區域來解決偏離

時，AWS Control Tower 會取代原始位置的基礎 OU。下列範例顯示偵測到這類偏離時，您可能會收到的偏離通知。

```
{
  "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"
}
```

Resolution

由於此偏離僅適用於基礎 OUs，因此解決方法是更新登陸區域。刪除其他類型的 OUs時，AWS Control Tower 會自動更新。

如需解決帳戶和 OU 偏離的詳細資訊，請參閱如果您在 AWS Control Tower 外部管理資源。

Security Hub CSPM 控制偏離

當屬於AWS Security Hub CSPM 服務受管標準：AWS Control Tower 的控制項報告偏離狀態時，就會發生這種類型的偏離。 AWS Security Hub CSPM 服務本身不會報告這些控制項的偏離狀態。反之，服務會將其調查結果傳送至 AWS Control Tower。

如果 AWS Control Tower 在超過 24 小時內未收到來自 Security Hub CSPM 的狀態更新，也可以偵測到 Security Hub CSPM 控制偏離。如果未如預期收到這些調查結果，AWS Control Tower 會驗證控制項是否偏離。下列範例顯示偵測到這類偏離時，您可能會收到的偏離通知。

```
{
"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" : "SH.XXXXXXX.1",
"ControlName" : "EBS snapshots should not be publicly restorable",
"ApiControlIdentifier" : "arn:aws:controltower:us-east-1::control/PYBETSAGNUZB",
"EnabledControlIdentifier": "arn:aws:controltower:us-
east-1::enabledcontrol/<UNIQUE_ID>".
"Region" : "us-east-1"
}
```

Resolution

對於帳戶少於 1000 OUs，建議的解決方案是呼叫 ResetEnabledControl API 進行漂移控制。在主控台中，您可以選取重新註冊 OU，將控制項重設為原始狀態。或者，對於任何 OU，您可以透過主控台或 AWS Control Tower APIs 移除並重新啟用控制項，該 API 也會重設控制項。

如需解決帳戶和 OU 偏離的詳細資訊，請參閱[如果您在 AWS Control Tower 外部管理資源](#)。

控制政策偏離

當使用資源控制政策 (RCPs) 或宣告性政策實作的控制項報告偏離狀態時，就會發生這種類型的偏離。它會傳回狀態 CONTROL_INEFFECTIVE，您可以在 AWS Control Tower 主控台和偏離訊息中檢視此狀態。此類偏離的偏離訊息也包含受影響控制項`EnabledControlIdentifier`的 。

對於以 SCP 為基礎的控制項，不會報告這種類型的偏離。

下列範例顯示偵測到這類偏離時，您可能會收到的偏離通知。

```
{
    "Message": "AWS Control Tower detects that a policy it owns was updated
 unexpectedly. This mismatch indicates that configuration changes were made outside of
 AWS Control Tower.",
    "MasterAccountId": "123456789XXX",
    "ManagementAccountId": "123456789XXX",
    "OrganizationId": "o-123EXAMPLE",
    "DriftType": "CONTROL_INEFFECTIVE",
    "RemediationStep": "To remediate the issue, Reset the DRIFTED enabled control if
 permitted or Re-register the OU. If the problem persists, contact AWS support.",
    "TargetIdentifier": "arn:aws:::organizations/o-123456/ou-1234-4567",
    "ControlId": "CT.XXXXXXX.PV.1",
```

```
    "ControlName": "EBS snapshots should not be publicly restorable",
    "ApiControlIdentifier": "arn:aws:controlcatalog:::control/<UNIQUE_ID>",
    "EnabledControlIdentifier": "arn:aws:controltower:us-
east-1::enabledcontrol/<UNIQUE_ID>"
}
```

Resolution

在 AWS Control Tower 中啟用的 RCP 控制、宣告政策控制和 Security Hub CSPM 控制上控制政策偏離的最簡單解析度是呼叫 `ResetEnabledControl` API。

對於少於 1000 個帳戶的 OUs，主控台或 API 的另一個解決方案是重新註冊 OU，這會將控制項重設為原始狀態。

對於任何個別 OU，您可以透過主控台或 AWS Control Tower APIs 移除並重新啟用控制項，該 API 也會重設控制項。

如需解決帳戶和 OU 偏離的詳細資訊，請參閱如果您在 AWS Control Tower 外部管理資源。

已停用信任的存取

這種偏離類型適用於 AWS Control Tower 登陸區域。當您在設定 AWS Control Tower 登陸區域 AWS Organizations 之後，在 中停用對 AWS Control Tower 的受信任存取時，就會發生這種情況。

停用受信任存取時，AWS Control Tower 不會再收到來自 的變更事件 AWS Organizations。AWS Control Tower 依賴這些變更事件來保持同步 AWS Organizations。因此，AWS Control Tower 可能會遺漏帳戶和 OUs 中的組織變更。因此，每次更新登陸區域時，重新註冊每個 OU 非常重要。

範例：偏離通知

以下是發生此類偏離時，您收到的偏離通知範例。

```
{
  "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."
}
```

Resolution

AWS Control Tower 會在 AWS Control Tower 主控台中發生此類偏離時通知您。解決方法是重設您的 AWS Control Tower 登陸區域。如需詳細資訊，請參閱解決偏離。

啟用基準的繼承偏離

AWS Control Tower OUs 和帳戶可能會發生這種類型的偏離。

Resolution

AWS Control Tower 會在發生此類偏離時通知您。對於幾乎所有繼承偏離的情況，您將收到移動成員帳戶偏離的偏離通知。這是因為這種偏離類型通常發生在帳戶移動或帳戶註冊失敗時。

在主控台中檢視和解決偏離

在 AWS Control Tower 主控台中，您可以在 Organizations 頁面上的基準狀態欄中檢視此繼承的偏離狀態。主控台的解決方法是重新註冊您的 OU 或更新您的帳戶。

以程式設計方式檢視和解決偏離

若要以程式設計方式檢視偏離狀態，您可以呼叫 `ListEnabledBaselines` API 來檢視 OUs 上已啟用基準的狀態。若要使用 `ListEnabledBaselines` API 以程式設計方式檢視個別帳戶的狀態，請使用 `includeChildren`旗標。

您可以呼叫 `ResetEnabledBaseline` API，以程式設計方式解決此類偏離。

啟用控制項上的繼承偏離

AWS Control Tower OUs 和帳戶可能會發生這種類型的偏離。

Resolution

AWS Control Tower 會在發生此類偏離時通知您。對於幾乎所有繼承偏離的情況，您將收到移動成員帳戶偏離的偏離通知。這是因為這種偏離類型通常發生在帳戶移動或帳戶註冊失敗時。

在主控台中檢視和解決偏離

在 AWS Control Tower 主控台中，您可以在組織頁面、啟用的控制頁面和帳戶詳細資訊頁面中檢視此繼承的偏離狀態。主控台的解決方法是重新註冊您的 OU 或更新您的帳戶。

以程式設計方式檢視和解決偏離

若要以程式設計方式檢視已啟用控制項的繼承偏離狀態，您可以呼叫 ListEnabledControls API 來檢視 OUs 上已啟用控制項的狀態。若要使用 ListEnabledControls API 以程式設計方式檢視個別帳戶的狀態，請使用 includeChildren旗標。

您可以呼叫 ResetEnabledControl API，以程式設計方式解決這種類型的繼承偏離。

EventBridge 建立

> **Note**
>
> EventBridge 僅適用於 LZ4.0+ 客戶。

AWS Control Tower 的 EventBridge 格式範例

```
{
   "version": "0",
   "id": "cd4d811e-ab12-322b-8255-872ce65b1bc8",
   "detail-type": "Drift Detected",
   "source": "aws.controltower",
   "account": "111122223333",
   "time": "2018-03-22T00:38:11Z",
   "region": "us-east-1",
   "resources": [],
   "detail": {
       "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 1000 accounts, you must update the provisioned product in Account Factory.",

       "accountId" : "012345678909",
       "sourceId" : "012345678909",
       "destinationId" : "ou-3210-1EXAMPLE"
   }
}
```

建立 EventBridge 規則以接收偏離通知的指引：

建立偏離通知的 EventBridge 規則

1. 開啟 Amazon EventBridge 主控台：
2. 在導覽窗格中，選擇規則。
3. 選擇建立規則。
4. 輸入規則的名稱和描述。
5. 針對規則類型，選擇具有事件模式的規則。
6. 定義事件來源：
   - 針對「事件來源」，選取 AWS 服務做為事件來源。
   - 針對「AWS 服務名稱」，選取 AWS Control Tower。
   - 針對「事件類型」，選取偵測到的偏離
7. 選取目標：
   - 對於目標類型，請選擇AWS 服務，對於選取目標，選擇偏離通知主題或 Lambda 函數等目標。當接收到符合規則中定義之事件模式的事件時，就會觸發目標。
   - 根據您選取的目標，提供必要的組態詳細資訊，例如 Lambda 函數名稱或偏離通知主題 ARN。
8. 檢閱和建立規則：
   - 檢閱規則的詳細資訊，並進行任何必要的變更。
   - 滿意之後，請按一下建立規則以儲存新的 EventBridge 規則。

建立規則後，它會開始監控指定的 AWS Control Tower 事件，並在發生偏離事件時觸發選取的目標動作。

如果您在 AWS Control Tower 外部管理資源

AWS Control Tower 會代表您設定帳戶、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 內外變更這些資源。在 AWS Control Tower 之外變更資源的最常見位置是 AWS Organizations 主控台。本主題說明如何在 AWS Control Tower 外部進行變更時，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對帳。某些變更需要重設您的登陸區域，才能更新 AWS Control Tower 主控台中顯示的資訊。

一般而言，您在 AWS Control Tower 主控台外對 AWS Control Tower 資源所做的變更，會在您的登陸區域中建立可解決的偏離狀態。如需這些變更的詳細資訊，請參閱資源的可修復變更。

需要重設登陸區域的任務

- 刪除安全 OU （特殊情況，不可略微完成。）
- 從安全 OU 移除共用帳戶 （不建議）。
- 更新、連接或分離與安全 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
- 建立新的最上層組織單位 (OU)
- 重新命名已註冊的 OU
- 刪除已註冊的 OU （安全 OU 除外，這需要更新。）
- 刪除已註冊的帳戶 （安全性 OU 中的共用帳戶除外）。

> **Note**
>
> AWS Service Catalog 處理變更的方式與 AWS Control Tower 不同。在協調變更時， AWS Service Catalog 可能會在控管狀態中建立變更。如需更新佈建產品的詳細資訊，請參閱 AWS Service Catalog 文件中的更新佈建產品。

參考 AWS Control Tower 以外的資源

當您在 AWS Control Tower 外部建立新的 OUs 和帳戶時，它們不受 AWS Control Tower 管理，即使它們可能顯示。

建立 OU

在 AWS Control Tower 外部建立的組織單位 (OUs) 稱為未註冊。它們會顯示在組織頁面中，但不受 AWS Control Tower 控制。

建立 帳戶

在 AWS Control Tower 外部建立的帳戶稱為未註冊。屬於向 AWS Control Tower 註冊之 OU 的已註冊和未註冊帳戶會顯示在組織頁面中。您可以使用 主控台來邀請 AWS Organizations 不屬於已註冊 OU 的帳戶。此加入邀請不會在 AWS Control Tower 中註冊帳戶，也不會將 AWS Control Tower 控管延伸至帳戶。若要透過註冊帳戶來擴展控管，請前往 AWS Control Tower 中的組織頁面或帳戶詳細資訊頁面，然後選擇註冊帳戶。

外部變更 AWS Control Tower 資源名稱

您可以在 AWS Control Tower 主控台之外變更組織單位 (OUs) 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 主控台變更 OU 的名稱。當您在 AWS Control Tower 外部變更 OU 名稱時，AWS Control Tower 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，您也必須重設登陸區域，以確保 AWS Control Tower 與保持一致 AWS Organizations。重設工作流程可確保基礎和其他 OUs 服務之間的一致性。您可以從登陸區域設定頁面解決此類偏離。請參閱 中的「解決偏離」一節在 AWS Control Tower 中偵測並解決偏離。

AWS Control Tower 會在 AWS Control Tower 儀表板的組織頁面上顯示 OUs 的名稱。您可以查看登陸區域重設操作何時成功。

重新命名已註冊的帳戶

每個 AWS 帳戶都有一個顯示名稱，可在 AWS 帳單與成本管理 主控台中由帳戶的根使用者變更。當您重新命名已在 AWS Control Tower 註冊的帳戶時，名稱變更會自動反映在 AWS Control Tower 中。如需變更帳戶名稱的詳細資訊，請參閱 AWS 帳單使用者指南中的管理 AWS 帳戶。

刪除安全 OU

這種類型的偏離是一種特殊情況。如果您刪除安全 OU，您會看到錯誤訊息頁面，提示您重設登陸區域。您必須先重設登陸區域，才能在 AWS Control Tower 中採取任何其他動作。

- 在重設完成 AWS Service Catalog 之前，您將無法在 AWS Control Tower 主控台中執行任何動作，也無法在 中建立任何新帳戶。
- 您將無法檢視登陸區域設定頁面，以查看該頁面的重設按鈕。

在這種情況下，登陸區域重設程序會建立新的安全 OU，並將兩個共用帳戶移至新的安全 OU。AWS Control Tower 會將日誌封存和稽核帳戶標記為偏離。相同的程序會解決這些帳戶中的偏離。

如果您確定必須刪除安全 OU，以下是您需要知道的事項：

您必須先確定安全 OU 不包含任何帳戶，才能刪除安全 OU。具體而言，您必須從 OU 移除日誌封存和稽核帳戶。我們建議您將這些帳戶移至另一個 OU。

> **Note**
>
> 在沒有適當考量的情況下，不會執行刪除安全 OU 的動作。如果暫時暫停記錄，且因為某些控制項可能無法強制執行，則此動作可能會引發合規問題。

如需有關偏離的一般資訊，請參閱 在 AWS Control Tower 中偵測並解決偏離 中的「解決偏離」。

從安全 OU 移除帳戶

我們不建議您從組織移除任何共用帳戶，或將其移出安全 OU。如果您不小心移除了共用帳戶，您可以遵循本節中的修復步驟來還原帳戶。

- 從 AWS Control Tower 主控台內：若要開始修復程序，請遵循半手動修復步驟。確保您用來存取 AWS Control Tower 主控台的使用者或角色具有執行 的許可`organizations:InviteAccountToOrganization`。如果您沒有此類許可，請遵循同時使用 AWS Control Tower 主控台和 AWS Organizations 主控台的手動修復步驟。
- 從 AWS Organizations 主控台開始：此修復程序是稍微較長、完全手動的程序。遵循手動修復步驟時，您將在 AWS Organizations 主控台和 AWS Control Tower 主控台之間切換。使用 時 AWS Organizations，您將需要具有 `AWSOrganizationsFullAccess`受管政策或同等政策的使用者或角色。在 AWS Control Tower 主控台中工作時，您將需要具有`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 Tower 動作的許可 (controltower：*)。
- 如果修復步驟未還原帳戶，請聯絡 AWS 支援。

透過下列方式移除共用帳戶的結果 AWS Organizations：

- 帳戶不再受到 AWS Control Tower 強制控制與服務控制政策 (SCPs保護。結果：帳戶中 AWS Control Tower 建立的資源可能會修改或刪除。

- 帳戶不再位於 AWS Organizations 管理帳戶下。結果： AWS Organizations 管理帳戶的管理員無法再查看帳戶的支出。
- 帳戶不再保證由 監控 AWS Config。結果： AWS Organizations 管理帳戶的管理員可能無法偵測資源變更。
- 帳戶不再位於組織中。結果：AWS Control Tower 更新和重設將會失敗。

使用 AWS Control Tower 主控台還原共用帳戶 （半手動程序）

1. 登入 AWS Control Tower 主控台，網址為 https：//https://console.aws.amazon.com/controltower。您必須以 IAM 使用者、IAM Identity Center 中的使用者或具有執行 許可的角色身分登入`organizations:InviteAccountToOrganization`。如果您沒有這類許可，請使用本主題稍後所述的手動修復程序。
2. 在已偵測到的登陸區域偏離頁面上，選擇重新邀請，透過將共用帳戶重新邀請至組織來修復共用帳戶移除。自動產生的電子郵件會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：//https://console.aws.amazon.com/organizations/home#/invites
   - 如果您有權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以直接導覽至帳戶邀請。
   - 如果移除的共用帳戶不在另一個組織中，請登入帳戶，開啟 AWS Organizations 主控台並導覽至邀請。
4. 再次登入管理帳戶，或重新載入已開啟的 AWS Control Tower 主控台。您將看到登陸區域偏離頁面。選擇重設以修復登陸區域。
5. 等待重設程序完成。

如果修復成功，共用帳戶會顯示為正常狀態和合規。

如果修復步驟未還原帳戶，請聯絡 AWS 支援。

使用 AWS Control Tower 和 AWS Organizations 主控台還原共用帳戶 （手動修復）

1. 在 登入 AWS Organizations 主控台https://console.aws.amazon.com/organizations/。您必須以 IAM 使用者、IAM Identity Center 中的使用者，或具有 `AWSOrganizationsFullAccess` 受管政策或同等身分的角色登入。

2. 邀請共用帳戶回到組織。如需邀請 帳戶之需求、先決條件和程序的相關資訊 AWS Organizations，請參閱AWS Organizations 《 使用者指南》中的邀請 AWS 帳戶到您的組織。
3. 登入已移除的共用帳戶，然後前往 https：//https://console.aws.amazon.com/organizations/home#/invites 接受邀請。
4. 再次登入管理帳戶。
5. 以 AWSControlTowerServiceRolePolicy受管政策或同等政策的使用者或角色身分登入 AWS Control Tower 主控台，以及執行所有 AWS Control Tower 動作的許可 (controltower：*)。
6. 您將看到登陸區域偏離頁面，其中包含重設登陸區域的選項。選擇重設以修復登陸區域。
7. 等待重設程序完成。

如果修復成功，共用帳戶會顯示為正常狀態和合規。

如果修復步驟未還原帳戶，請聯絡 AWS 支援。

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。

變更受控管帳戶的電子郵件地址

AWS Control Tower 會擷取並顯示主控台體驗所需的電子郵件地址。因此，共用和其他帳戶電子郵件地址會在您變更後更新，並在 AWS Control Tower 中一致顯示。

> **Note**
>
> 在 中 AWS Service Catalog，帳戶工廠會顯示您建立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 會顯示部署到向 AWS Control Tower 註冊之組織單位的所有 AWS Config 規則的合規狀態，包括在 AWS Control Tower 主控台外部啟動的規則。

刪除 AWS Control Tower 外部的 AWS Control Tower 資源

您可以在 AWS Control Tower 中刪除 OUs和帳戶，而且不需要採取任何進一步的動作來查看更新。刪除 OU 時會自動更新帳戶工廠，但刪除帳戶時不會自動更新。

刪除已註冊的 OU （安全 OU 除外）

AWS Organizations您可以在其中使用 API 或主控台移除空的組織單位 (OUs)。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。它會更新帳戶工廠中的 OU 清單，以便註冊的 OUs 清單保持一致。

> **Note**
>
> 在 中 AWS Service Catalog，帳戶工廠已更新，從您可以佈建帳戶的可用 OU 清單中移除已刪除的 OUs。

從 OU 刪除註冊的帳戶

當您刪除已註冊的帳戶時，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，代表受管帳戶的帳戶工廠佈建產品不會更新為刪除帳戶。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 (OUs) 和帳戶都由 AWS Control Tower 自動管理。此外，如果您有在 AWS Control Tower 外部建立的現有 OUs 和帳戶，您可以將它們帶入 AWS Control Tower 管控。

對於現有 AWS Organizations 和 AWS 帳戶，大多數客戶偏好透過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 關於註冊現有帳戶。

術語

- 當您將現有組織帶入 AWS Control Tower 時，稱為註冊組織，或將控管延伸至組織。
- 當您將 AWS 帳戶帶入 AWS Control Tower 時，稱為註冊帳戶。

檢視您的 OUs和帳戶

在 AWS Control Tower Organization 頁面上，您可以檢視 中的所有 OUs AWS Organizations，包括向 AWS Control Tower 註冊的 OUs，以及未註冊的 OU。您可以在階層中檢視巢狀 OUs。在組織頁面上檢視組織單位的簡單方法是僅從右上角的下拉式清單中選取組織單位。

組織頁面會列出組織中的所有帳戶，無論 AWS Control Tower 中的 OU 或註冊狀態為何。在組織頁面上檢視帳戶的簡單方法是僅從右上角的下拉式清單中選取帳戶。如果帳戶符合註冊的先決條件，您可以在 OUs 中個別檢視、更新和註冊帳戶。

如果您未選取任何篩選，組織頁面會在階層中顯示您的帳戶和 OUs。這是監控所有 AWS Control Tower 資源並對其採取動作的集中位置。如需組織頁面的詳細資訊，您可以檢視影片逐步解說。

> **Note**
>
> 當您在包含登陸區域的組織中啟用受信任存取時，AWS Control Tower 可以為組織中的所有帳戶建立角色、管理資源和讀取資料。透過受信任的存取，AWS Control Tower 可以使用組織中的任何帳戶或 OU，無論已註冊和已註冊或未註冊。

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

將控管延伸至現有的組織

您可以透過設定登陸區域 (LZ) 將 AWS Control Tower 控管新增至現有組織，如入門中的 AWS Control Tower 使用者指南步驟 2 中所述。

以下是在現有組織中設定 AWS Control Tower 登陸區域時預期會發生的情況。

- 每個 AWS Organizations 組織可以有一個登陸區域。
- AWS Control Tower 會使用現有 AWS Organizations 組織的管理帳戶作為其管理帳戶。不需要新的管理帳戶。
- AWS Control Tower 會在已註冊的 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。
- 在您啟動登陸區域或註冊 OU 之後，AWS Control Tower 控制項會自動套用至該 OU 中的所有註冊帳戶。
- 您可以將其他現有 AWS 帳戶註冊到由 AWS Control Tower 管理的 OU，以便控制適用於這些帳戶。
- 您可以在 AWS Control Tower 中新增更多 OUs，也可以註冊現有的 OUs。

若要檢查註冊和註冊的其他先決條件，請參閱 AWS Control Tower 入門。

以下是有關 AWS Control Tower 控制如何不適用於未設定 AWS Control Tower 登陸區域的 AWS 組織中 OUs 的詳細資訊：

- 在 AWS Control Tower 帳戶工廠外部建立的新帳戶不受已註冊 OU 控制項的約束。
- 在 OUs 中建立但未向 AWS Control Tower 註冊的新帳戶不受控制項約束，除非您特別將這些帳戶註冊到 AWS Control Tower。請參閱關於註冊現有帳戶以取得註冊帳戶的詳細資訊。
- 除非您單獨註冊 OUs 或註冊帳戶，否則其他現有組織、現有帳戶以及您在 AWS Control Tower 外部建立的任何新 OU 或任何帳戶不受 AWS Control Tower 控制約束。

如需如何將 AWS Control Tower 套用至現有 OUs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 Tower 登陸區域的程序概觀，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。不過，如果您目前使用的是 AWS 登陸區域解決方案 AWS Organizations，請在嘗試在組織中啟用 AWS Control Tower 以判斷 AWS Control Tower 是否可能干擾您目前的登陸區域部署之前，先向您的 AWS 解決方案架構師確認。此外，如果帳戶不符合先決條件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 。

影片：在現有 中啟用登陸區域 AWS Organizations

此影片 (7：48) 說明如何在現有 AWS Organizations 結構中設定和啟用 AWS Control Tower 登陸區域。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 Identity Center 和現有組織的考量事項

- 如果已設定 AWS IAM Identity Center (IAM Identity Center)，AWS Control Tower 主區域必須與 IAM Identity Center 區域相同。
- AWS Control Tower 不會刪除現有的組態。
- 如果已啟用 IAM Identity Center，且如果您使用 IAM Identity Center Directory，AWS Control Tower 會新增許可集、群組等資源，並照常繼續進行。
- 如果設定了另一個目錄 （外部、AD、受管 AD)，AWS Control Tower 不會變更現有的組態。如需詳細資訊，請參閱AWS IAM Identity Center (IAM Identity Center) 客戶的考量事項。

存取其他 AWS 服務

將組織帶入 AWS Control Tower 控管之後，您仍可透過 AWS Organizations 主控台和 APIs AWS Organizations存取任何可透過 AWS 提供的服務。如需詳細資訊，請參閱相關 AWS 服務。

AWS Control Tower 中的巢狀 OUs

本章列出在 AWS Control Tower 中使用巢狀 OUs 時，您要注意的期望和考量事項。在大多數情況下，使用巢狀 OUs 與使用平面 OU 結構相同。註冊和重新註冊功能可與巢狀 OUs 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) 說明如何管理 AWS Control Tower 中的巢狀 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 OUs的影片逐步解說。

如需巢狀 OUs 和登陸區域的最佳實務指引，請參閱部落格文章使用巢狀 OUs 組織 AWS Control Tower 登陸區域。

從平面 OU 結構擴展到巢狀 OU 結構

如果您使用平面 OU 結構建立 AWS Control Tower 登陸區域，您可以將它擴展到巢狀 OU 結構。

此程序有四個主要步驟：

1. 在 AWS Control Tower 中建立所需的巢狀 OU 結構。
2. 前往 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）。以下是方法：
   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**
   > 此步驟必須在 AWS Organizations 主控台的 中完成，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。
   - 如果您已在 中建立 OU AWS Organizations，請第一次註冊 OU。

4. 移動並註冊帳戶後，請從 AWS Organizations 主控台或從 AWS Control Tower 主控台刪除空的頂層 OU。

巢狀 OU 註冊預先檢查

為了支援成功註冊您的巢狀 OUs 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，並提供您必須先修正的項目清單，才能註冊 OU。

巢狀 OUs和角色

AWS Control Tower 會將`AWSControlTowerExecution`角色部署到目標 OU 下的帳戶，以及巢狀到目標 OUs 下所有 OU 中的帳戶，即使您的意圖是只註冊目標 OU。此角色會針對具有`AWSControlTowerExecution`角色的任何帳戶，授予管理帳戶管理員許可的任何使用者。角色可用來執行 AWS Control Tower 控制項通常不允許的動作。

您可以從不打算註冊的未註冊帳戶中刪除此角色。如果您刪除此角色，則無法向 AWS Control Tower 註冊帳戶，或註冊直接父系 OUs，除非您將角色還原到帳戶。若要從帳戶刪除`AWSControlTowerExecution`角色，您必須在`AWSControlTowerExecution`角色下登入，因為不允許其他 IAM 主體刪除 AWS Control Tower 管理的角色。

如需如何限制角色存取的資訊，請參閱角色信任關係的選用條件。

巢狀 OUs 和帳戶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，並更新所有已註冊的帳戶。以下是預期事項。

AWS Control Tower 會執行下列任務

- 將`AWSControlTowerExecution`角色新增至此 OU 下的所有未註冊帳戶，以及其巢狀 OUs 中的所有未註冊帳戶。
- 註冊未註冊的成員帳戶。
- 重新註冊已註冊的成員帳戶。

- 為新註冊的成員帳戶建立 IAM Identity Center 登入。
- 更新現有的已註冊成員帳戶，以反映您的登陸區域變更。
- 更新為此 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 OU) 下註冊 OU。
- 巢狀 OUs 必須分別註冊。
- 除非其父 OU 已註冊，否則您無法註冊 OU。
- 您無法註冊 OU，除非樹狀結構中所有較高的 OUs 都已成功註冊 （有些可能已刪除）。
- 您可以註冊處於偏離較高 OU 下的 OU，但該動作無法修復偏離。

巢狀 OU 限制

- OUs最多可巢狀至根目錄深處 5 個層級。
- 目標 OUs 下的巢狀 OU 必須分別註冊或重新註冊。
- 如果目標 OU 位於階層中的層級 2 或以下，也就是說，如果不是頂層 OU，則在此 OU 及其下的所有 OUs 上會自動強制執行在較高 OUs 上啟用的預防性控制。
- OU 註冊失敗不會傳播階層樹狀結構。您可以在父系的 OUs 詳細資訊頁面上查看巢狀 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 OUs和合規

從 AWS Control Tower 主控台，您可以在組織頁面中檢視不合規OUs 和帳戶，以便大規模了解合規。

巢狀 OUs 和帳戶的合規考量

- OU 的合規不是根據其下巢狀 OUs 的合規來確定的。
- 控制項的合規狀態是根據啟用控制項的所有 OUs 來計算，包括巢狀 OUs。請參閱 OUs和帳戶的 AWS Control Tower 合規狀態。
- OU 只有在帳戶不合規時才會顯示為不合規，無論 OU 在 OU 階層中的位置為何。

- 如果巢狀 OU 不合規，其父 OU 不會自動視為不合規。
- 在 OU 詳細資訊或帳戶詳細資訊頁面上，您可以檢視可能導致您的 OUs或帳戶顯示不合規狀態的不合規資源清單。

巢狀 OUs和漂移

在某些情況下，偏離可能會阻止巢狀 OUs 的註冊。

漂移和巢狀 OUs 的預期

- 您可以在具有漂移父OUs 上啟用控制項，但不能直接在漂移OUs 上啟用控制項。
- 您可以啟用偏離 OU 下的偵測性控制，只要它不是頂層偏離 OU。
- 強制控制項僅在頂層 OUs 上啟用。當您註冊巢狀 OU 時，會略過強制性控制項。
- 一項強制性控制可保護 AWS Config 資源；因此，該控制必須處於非偏離狀態，才能註冊巢狀 OUs。如果漂移，AWS Control Tower 會封鎖巢狀 OUs 的註冊。
- 如果頂層 OU 處於偏離中，則保護 AWS Config 資源的控制項可能處於偏離中。在這種情況下，AWS Control Tower 會封鎖任何需要建立或更新 AWS Config 資源的動作，包括偵測控制項的應用。

巢狀 OUs和控制項

當您在已註冊的 OU 上啟用控制項時，預防性和偵測性控制項有不同的行為。對於巢狀 OUs，主動控制的行為類似於偵測性控制。

預防性控制

- 在巢狀 OUs 上強制執行預防性控制。
- 強制預防性控制會在 OU 及其巢狀 OUs 下的所有帳戶上執行。
- 預防性控制會影響目標 OUs 下巢狀化的所有帳戶和 OU，即使這些帳戶和 OUs 未註冊也一樣。

Detective 和主動控制

- 巢狀 OUs不會自動繼承偵測或主動控制；這些控制必須單獨啟用。
- Detective 和主動控制只會部署到登陸區域操作區域中的註冊帳戶。

啟用的控制狀態和繼承

您可以在 OU 詳細資訊頁面上檢視每個 OU 的繼承控制項。

> **Tip**
>
> 您可以使用控制繼承來協助保持在 OU 的 SCP 配額內。例如，您可以在 OU 階層的最上層 OU 啟用控制項，而不是直接為巢狀 OU 啟用 。

繼承狀態

- 狀態繼承表示控制項僅由繼承啟用，且尚未直接套用至 OU。
- 狀態已啟用表示此 OU 上強制執行控制項，無論其在其他 OUs 上的狀態為何。
- 狀態失敗表示不在此 OU 上強制執行控制項，無論其在其他 OUs 上的狀態為何。

> **Note**
>
> 狀態繼承表示控制項已套用至樹狀目錄中較高的 OU，並且在此 OU 上強制執行，但未直接新增至此 OU。

> **如果您的登陸區域不是目前版本**
>
> 啟用控制項表格中的每一列代表一個個別 OU 上已啟用的控制項。

巢狀 OUs和根目錄

根不是 OU，而且無法註冊或重新註冊。您也無法直接在根目錄中建立帳戶。根不能不合規或具有生命週期狀態，例如已註冊或偏離。

不過，根是所有帳戶和 OUs 的最上層容器。在巢狀 OUs 的內容中，它是所有其他 OUs 巢狀化所在的節點。

向 AWS Control Tower 註冊現有的組織單位

將多個現有 AWS 帳戶帶入 AWS Control Tower 的有效方法是將 AWS Control Tower 的管控擴展到整個組織單位 (OU)。

若要透過使用 建立的現有 OU AWS Organizations及其帳戶啟用 AWS Control Tower 管控，請向您的 AWS Control Tower 登陸區域註冊 OU。您可以註冊最多包含 1000 個帳戶的 OUs。如果 OU 包含超過 1000 個帳戶，您無法在 AWS Control Tower 中註冊該帳戶。

當您註冊 OU 時，其成員帳戶會註冊到 AWS Control Tower 登陸區域。它們由適用於其 OU 的控制項管理。

從登陸區域 4.0 版開始，您可以直接在 OU 上啟用控制項。Detective 控制項需要 AWS Config 記錄，可透過註冊 OU 或在 OU 上啟用 AWS Config 記錄來啟用。註冊 OU 將啟用 `AWSControlTowerBaseline`。啟用 AWS Config 記錄將啟用 `ConfigBaseline`。如需詳細資訊，請參閱 基準類型 和 AWS Control Tower 控制項參考指南

> **Note**
>
> 如果您還沒有 AWS Control Tower 登陸區域，請先在 AWS Control Tower 建立的新組織中或在現有 AWS Organizations 組織中設定登陸區域。如需如何設定登陸區域的詳細資訊，請參閱 AWS Control Tower 入門。

當我註冊 OU 時，我的帳戶會發生什麼情況？

AWS Control Tower 需要許可，才能 AWS Organizations 代表您在 AWS CloudFormation 和 之間建立受信任的存取，以便 AWS CloudFormation 可以自動將堆疊部署到組織中的帳戶。

- `AWSControlTowerExecution` 角色會新增至狀態為未註冊的所有帳戶。
- 註冊 OU 時，預設會啟用 OU 及其所有帳戶的強制性控制。

OU 註冊後的部分帳戶註冊

您可以成功註冊 OU，但某些帳戶可能會保持未註冊狀態。若是如此，這些帳戶不符合某些註冊的先決條件。如果註冊 OU 程序中的帳戶註冊未成功，帳戶頁面上的帳戶狀態會顯示註冊失敗。您也可以在帳戶欄位中看到 OU 頁面上的帳戶資訊，例如 5 的 4。

例如，如果您看到 5 個中的 4 個，這表示您的 OU 總共有 5 個帳戶，其中 4 個註冊成功，但一個帳戶無法在註冊 OU 程序期間註冊。在確定帳戶符合註冊先決條件之後，您可以選擇重新註冊 OU 讓帳戶加入註冊。

註冊 OU 的 IAM 使用者先決條件

執行註冊 OU 操作時，您的 AWS Identity and Access Management (IAM) 身分 （使用者或角色） 或 IAM Identity Center 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。否則，佈建產品的建立會在註冊期間失敗。由於 AWS Control Tower 在註冊 OU 時依賴 IAM 使用者或 IAM Identity Center 使用者身分的登入資料，因此發生失敗。

相關產品組合是由 AWS Control Tower 建立，稱為 AWS Control Tower 帳戶工廠產品組合。選擇服務目錄 > 帳戶工廠 > AWS Control Tower 帳戶工廠產品組合，導覽至其中。然後選取稱為群組、角色和使用者的標籤，以檢視您的 IAM 或 IAM Identity Center 身分。如需如何授予存取權的詳細資訊，請參閱 文件 AWS Service Catalog。

註冊現有的 OU

在 AWS Control Tower 主控台的組織頁面上，您可以檢視階層中組織的所有 OUs 和帳戶，包括向 AWS Control Tower 註冊的 OUs，以及未註冊的 OU。

一般而言，在 中建立未註冊OUs AWS Organizations，而且它們不受任何其他登陸區域的管理。您可以註冊包含最多 1000 個帳戶的現有 OUs。如果 OU 包含超過 1000 個帳戶，您無法在 AWS Control Tower 中註冊該帳戶。

從主控台註冊現有的 OU

1. 登入 AWS Control Tower 主控台，網址為 https：//https://console.aws.amazon.com/controltower。
2. 在左側窗格導覽功能表中，選擇組織。
3. 在組織頁面上，選取您要註冊的 OU 旁的選項按鈕，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，以便您可以檢視該 OU 的 OU 詳細資訊頁面。
4. 在 OU 詳細資訊頁面上，您可以在動作下拉式功能表中選取註冊 OU。

註冊程序至少需要 10 分鐘才能將控管延伸至 OU，每個額外帳戶最多需要額外 2 分鐘。

向 APIs 註冊現有的 OU

若要向 AWS Control Tower APIs 註冊現有的 OU，您可以在 AWSControlTowerBaseline baselineIdentifier 欄位中使用 呼叫 EnableBaseline API。如需詳細資訊，請參閱僅向 APIs 註冊 AWS Control Tower OU。

註冊現有 OU 的結果

在您註冊現有的 OU 之後，該AWSControlTowerExecution角色可讓 AWS Control Tower 將控管延伸至其個別帳戶。系統會強制執行護欄，並將帳戶活動的相關資訊回報給您的稽核和記錄帳戶。

其他結果包括下列項目：

- `AWSControlTowerExecution` 允許 AWS Control Tower 稽核帳戶進行稽核。
- `AWSControlTowerExecution` 可協助您設定組織的記錄，以便將每個帳戶的所有記錄傳送到記錄帳戶。
- `AWSControlTowerExecution` 確保您選取的 AWS Control Tower 控制項會自動套用至 OUs 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 控制項所體現的稽核和記錄功能，提供合規和安全性報告。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。如需漂移的詳細資訊，請參閱 在 AWS Control Tower 中偵測並解決偏離。

> **Note**
>
> 當 AWS Control Tower 顯示 OUs及其帳戶時，可能會發生一個不尋常的情況。如果您已在已註冊的 OU 中建立帳戶，然後又將該已註冊帳戶移至另一個未註冊的 OU，特別是如果您使用 AWS Organizations 來移動帳戶，您可以在 OU 詳細資訊頁面中看到「0 之 1」帳戶的結果。此外，您可能已在未註冊的 OU 中建立另一個未註冊帳戶。如果有未註冊的帳戶，主控台可能會讀取 OU 的「1/1」。似乎已註冊單一（新建立）帳戶，但事實上並未註冊。您必須註冊新帳戶。

建立新的 OU

以下是如何在 AWS Control Tower 中建立 OU 或巢狀 OU。

在 AWS Control Tower 中建立新的 OU

1. 導覽至組織頁面。
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，您可以查看已註冊 OUs 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系 OU 名稱、檢視該父系 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。新的 OU 會自動在您選取的 OU 下建立為巢狀 OU。

> **Note**
>
> 如果您的登陸區域不是最新的，您會在下拉式功能表中看到一般清單，而不是階層。即使您的登陸區域包含巢狀 OUs，您也無法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 OUs 的詳細資訊，請參閱 AWS Control Tower 中的巢狀 OUs。

移除 OU

AWS Control Tower 支援取消註冊 OU 和刪除 OU 的個別主控台動作。

刪除 OU 是最終的。無法撤銷。

考量事項

- OU 必須清空帳戶，刪除和取消註冊操作才能成功。
- 必須從 OU 中移除所有選用控制項。
- 您必須先取消註冊 OU，才能將其刪除。
- 您可以取消註冊 OU 來從 AWS Control Tower 移除 OU，無需將其刪除。

從 AWS Control Tower 移除 OU

1. 登入 AWS Control Tower 主控台，網址為 https：//https://console.aws.amazon.com/controltower。
2. 導覽至組織頁面。
3. 選取 OU 的名稱以檢視 OU 詳細資訊頁面，並確定已從 OU 移除所有帳戶。
4. 此外，在 OU 詳細資訊頁面上，請確定已從 OU 中移除所有選用控制項。
5. 返回組織頁面，然後選取 OU 旁的選項按鈕。
6. 從右上角的動作下拉式功能表中選取取消註冊組織單位。

7. 如果您不想完全刪除 OU，請在此停止，只要從 AWS Control Tower 取消註冊即可。若要完全刪除 OU，請繼續下一個步驟。
8. 若要繼續，請從右上角的動作下拉式功能表中選取刪除。

您必須等到取消註冊程序完成，才能取消註冊另一個 OU。

> **Note**
>
> 若要移除由 AWS Control Tower 管理的帳戶，您可以從 AWS Control Tower 主控台的左側導覽窗格中導覽至帳戶工廠。若要移除 OU 中非由 AWS Control Tower 管理的帳戶，請前往 AWS Organizations 主控台。

若要以程式設計方式取消註冊 OU，請呼叫 `DisableBaseline` API。

註冊或重新註冊期間失敗的常見原因

一般而言，當您註冊或重新註冊 OU 時，該 OU 中的所有帳戶都會在 AWS Control Tower 中註冊。不過，即使整體 OU 註冊成功，某些帳戶仍可能無法註冊。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。

如果 OU 或其任何成員帳戶的註冊（或重新註冊）失敗，AWS Control Tower 會傳回受影響成員帳戶的錯誤訊息。您可以在 OU 詳細資訊頁面上檢視錯誤訊息，其中資料表會彙總預先檢查和帳戶錯誤訊息。如果註冊 OU 操作失敗，資料表會顯示 OU 下所有帳戶的所有錯誤訊息。如有需要，您也可以在帳戶詳細資訊頁面上檢視每個帳戶的錯誤訊息。

或者，您可以下載包含詳細報告的檔案，其中顯示哪些預先檢查未通過，以進行離線分析。您可以選擇位於註冊區域右上角的下載按鈕來完成下載。

本節列出預先檢查失敗時可能收到的錯誤類型，以及如何修正錯誤。

登陸區域錯誤

- 登陸區域尚未就緒

  重設您目前的登陸區域，或將其更新至最新版本。

OU 錯誤

- 超過 SCPs 數量上限

您可能超過每個 OU 的服務控制政策 (SCPs) 限制，或者您可能已達到另一個配額。每個 OU 的 5 個 SCPs 限制適用於 AWS Control Tower 登陸區域中的所有 OUs。如果您有比配額允許的更多 SCPs，則必須刪除或合併 SCPs。

- 衝突SCPs

  現有的 SCPs 可以套用到 OU 或帳戶，以防止 AWS Control Tower 註冊帳戶。檢查套用SCPs 是否有任何政策可能使 AWS Control Tower 無法運作。請務必檢查從階層中較高 OUs 繼承的 SCPs。

- 超過堆疊集配額

  堆疊集配額可能已超過。如果您有超過配額允許的執行個體，您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 1000 個帳戶。

帳戶錯誤

- 帳戶已防止預先檢查

  OU 上的現有 SCP 可防止 AWS Control Tower 對您的 OU 成員帳戶執行預先檢查。若要解決此預先檢查失敗，請從 OU 更新或移除 SCP。

- 電子郵件地址錯誤

  您為帳戶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元的規則表達式 (regex)：`[A-Z0-9a-z._%+-]+@[A-Za-z0-9.-]+[.]+[A-Za-z]+`

- 已啟用組態記錄器或交付管道

  帳戶可能有現有的 AWS Config 組態記錄器或交付管道。您必須先 AWS CLI 在 AWS Control Tower 管理帳戶受管資源的所有 AWS 區域中，透過 刪除或修改這些資源，才能註冊帳戶。

- STS 已停用

  AWS Security Token Service (AWS STS) 可能會在帳戶中停用。必須針對 AWS Control Tower 支援的所有區域，在帳戶中啟用 AWS STS 端點。

- IAM Identity Center 衝突

  AWS Control Tower 主區域與 AWS IAM Identity Center (IAM Identity Center) 區域不同。如果已設定 IAM Identity Center，AWS Control Tower 主區域必須與 IAM Identity Center 區域相同。

- 衝突 SNS 主題

  帳戶具有 AWS Control Tower 需要使用的 Amazon Simple Notification Service (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，AWS Control Tower 設定會失敗。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。

- 偵測到暫停的帳戶

  此帳戶已暫停。它無法註冊到 AWS Control Tower。從此 OU 移除帳戶，然後再試一次。

- 不在產品組合中的 IAM 使用者

  在註冊 OU 之前，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 中註冊帳戶所需的角色和許可。新增角色的說明可在 中找到手動將必要的 IAM 角色新增至現有 AWS 帳戶 並註冊。

提醒您，當您在 AWS Control Tower 中註冊所有 AWS 帳戶時， AWS CloudTrail 會自動啟用。如果 CloudTrail 在註冊之前已在 帳戶上啟用，除非您在開始註冊程序之前停用 CloudTrail，否則您可能會遇到重複計費。

更新組織

更新組織單位 (OU) 或更新 OU 內多個帳戶的最快方法是執行下列其中一個動作：

- 如果`AWSControlTowerBaseline`已啟用，請重新註冊 OU。
- 如果 未啟用，則重設啟用的基準或重設啟用`AWSControlTowerBaseline`的控制項。

何時更新 AWS Control Tower OUs和帳戶

當您執行登陸區域更新時，您必須更新已註冊的帳戶，才能將新的控制項套用至這些帳戶。

- 您可以使用重新註冊或重設選項，對 OU 下的所有帳戶執行更新。
- 如果您的登陸區域中有多個已註冊的 OU，請重新註冊或重設所有 OUs 以更新所有帳戶。

- 若要更新單一帳戶，您可以從 AWS Control Tower 主控台更新，或者， AWS Service Catalog 如果帳戶已啟用 AWSControlTowerBaseline，您可以在 中選擇更新佈建產品選項。請參閱 在 主控台中更新帳戶。

更新相同 OU 中的多個帳戶

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 OUs 重複這些步驟。

以一個動作更新一個 OU 中的多個帳戶

1. 登入 AWS Control Tower 主控台，網址為 https：//https://console.aws.amazon.com/controltower。
2. 在左側窗格導覽功能表中，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. 如果在 OU 上啟用 AWSControlTowerBaseline，請選取動作下的重新註冊 OU。如果未在 OU 上啟用 AWSControlTowerBaseline，請在動作下選取重設 AWS Config 基準以重設啟用的基準，並在「啟用的控制項」下選取啟用的控制項和重設控制項區段以重設啟用的控制項。

或者，您可以選取任何顯示可用更新狀態的帳戶，然後視需要為多個帳戶選擇更新帳戶。

重新註冊期間會發生什麼情況

當您重新註冊 OU 時：

- 狀態欄位指出帳戶目前是否已向 AWS Control Tower 註冊 （ 已註冊)、帳戶從未註冊 (尚未註冊)，或先前註冊是否失敗 (註冊失敗)。
- 當您重新註冊 OU 時，`AWSControlTowerExecution`角色會新增至狀態為未註冊或註冊失敗的所有帳戶。
- AWS Control Tower 會為這些新的註冊帳戶建立單一登入 (IAM Identity Center) 登入。
- 已註冊的帳戶會重新註冊至 AWS Control Tower。
- 套用至 OU 的任何預防性控制項上的偏離是固定的，因為 SCPs 會傳回至其預設定義。
- 所有帳戶都會更新，以反映最新的登陸區域變更。

如需詳細資訊，請參閱關於註冊現有帳戶。

> **Tip**
>
> 當您重新註冊 OU 或更新登陸區域版本和多個成員帳戶時，您可能會看到提及 StackSet-AWSControlTowerExecutionRole 的失敗訊息。管理帳戶中的此 StackSet 可能會失敗，因為 AWSControlTowerExecution IAM 角色已存在於所有註冊的成員帳戶中。此錯誤訊息是預期的行為，可以忽略。

更新單一帳戶

> **Note**
>
> 單一帳戶佈建、更新和自訂必須以啟用 AWSControlTowerBaseline 的組織單位 (OU) 為目標。如果 OU 未啟用 AWSControlTowerBaseline，您可以啟用帳戶自動註冊，或在 EnabledBaselines 上使用 ResetEnabledBaseline 和 ResetEnabledControl APIs並在該 OU 上使用 EnabledControls 來註冊帳戶。如需 AWSControlTowerBaseline 的詳細資訊，請參閱：在 OU 層級套用的基準類型。

您可以在 AWS Control Tower 主控台或 Service Catalog 主控台中更新個別 AWS Control Tower 帳戶。

若要在 AWS Control Tower 主控台中更新單一帳戶，請參閱 在 主控台中更新帳戶。

在 中更新單一帳戶 AWS Service Catalog

1. 前往 AWS Service Catalog。
2. 在左側窗格導覽功能表中，選擇佈建產品。
3. 在佈建產品頁面上，選取您要更新之佈建產品旁邊的選項按鈕。
4. 在右上角，選擇動作下拉式清單以更新。

若要進一步了解如何更新 AWS Service Catalog，請參閱 Service Catalog 管理員指南中的 更新 Service Catalog 中的佈建產品和更新產品。

整合服務

AWS Control Tower 是一項在其他服務的基礎上建置 AWS 的服務，可協助您設定架構良好的環境。本章提供這些服務的簡短概觀，包括基礎服務的組態資訊，以及它們在 AWS Control Tower 中的運作方式。

如需如何測量架構良好的環境的詳細資訊，請參閱 AWS Well-Architected 工具。另請參閱 管理與控管雲端環境指南。

主題

AWS 可用的備份選項

AWS 備份可讓您為 AWS Control Tower 登陸區域建立備份計劃。您可以將資料備份和復原工作流程直接併入您的登陸區域。備份計畫包含預先定義的規則，例如保留天數、備份頻率，以及進行備份的時段。如需詳細資訊，請參閱 AWS Backup and AWS Control Tower。

使用 部署環境 CloudFormation

CloudFormation 可讓您以可預測且重複的方式建立和佈建 AWS 基礎設施部署。它可協助您利用 AWS 產品在雲端中建置高度可靠、高度可擴展且符合成本效益的應用程式，而不必擔心建立和設定基礎 AWS 基礎設施。 CloudFormation 可讓您使用範本檔案，以單一單位 （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 CloudFormation 堆疊集對帳戶套用控制項。如需 CloudFormation 和 AWS Control Tower 如何搭配運作的詳細資訊，請參閱 使用 建立 AWS Control Tower 資源 AWS CloudFormation。

使用 CloudTrail 監控事件

AWS Control Tower 會設定 AWS CloudTrail 以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 透過保留帳戶的 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 CloudTrail 的服務呼叫 AWS APIs的使用者和帳戶、進行呼叫的來源 IP 地址，以及呼叫發生的時間。您可以使用 API 將 CloudTrail 整合至應用程式，以自動建立組織的追蹤記錄、查看追蹤記錄的狀態，並控制管理員開啟和關閉 CloudTrail 記錄功能的方式。如需詳細資訊，請參閱 AWS CloudTrail 使用者指南。

使用 CloudWatch 監控資源和服務

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 CloudWatch 如何搭配 AWS Control Tower 運作的詳細資訊，請參閱監控。

使用 管理資源組態 AWS Config

AWS Config 提供與您 AWS 帳戶相關聯資源的詳細檢視，包括它們的設定方式、它們彼此的關係，以及組態及其關係如何隨時間變化。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`和 值`managed-by-control-tower`。

如需如何在 AWS Control Tower 中 AWS Config 監控和記錄資源及其如何向您收取費用的詳細資訊，請參閱 使用 監控資源變更 AWS Config。

AWS Control Tower 使用 AWS Config 規則 實作偵測性控制。如需詳細資訊，請參閱關於 AWS Control Tower 中的控制項。

Control Tower 登陸區域 4.0 中的 AWS Config 整合

服務連結組態彙總工具 (SLCA)

AWS Control Tower 現在會在登陸區域 4.0+ 實作服務連結組態彙總工具 (SLCA)。此變更可大幅改善 AWS Config 資料在組織中的彙總和管理方式。

重要變更

新的服務連結組態彙整工具部署

- 服務連結組態彙整工具會部署在您指定的 AWS Config 整合帳戶中。
- 對於現有客戶，這將是您的稽核帳戶
- 對於新客戶，這將是資訊清單`config.accountId`欄位中指定的帳戶

委派的管理員

- AWS Config 彙總工具帳戶會成為 AWS Config 的委派管理員
- AWS Control Tower 會自動設定委派的管理員設定
- 這可讓您在整個組織中集中管理 AWS Config

從舊版彙總工具遷移

在升級至登陸區域 4.0 期間：

- 管理帳戶中的組織彙整工具將被移除。
- 稽核帳戶中的帳戶彙整工具將被移除。
- 這些會由 AWS Config 整合彙整工具帳戶中的新服務連結 Config 彙整工具取代。

增強型資料彙總

服務連結的 Config 彙總工具可改善 Config 資料彙總的功能：

- 可以從組織中的任何 AWS Config 記錄器彙總資料
- 包含來自非 Control Tower 管理之帳戶的資料
- 提供整個組織的組態項目完整檢視
- 支援增強型資料周邊控制

重要考量

委派的管理員組態

- AWS Control Tower 將使用資訊清單中指定的帳戶進行 AWS Config 整合
- 此帳戶將自動設定為委派管理員
- 此組態不需要客戶採取其他動作
- 對於現有客戶，先前的安全角色整合帳戶（稽核帳戶）將在登陸區域 4.0 升級期間設定為 AWS Config 中央彙整工具帳戶

資料彙總範圍

- 服務連結組態彙總工具可以從下列位置彙總組態資料：
  - Control Tower 受管帳戶
  - 非控制塔受管帳戶
  - 組織中具有作用中 Config 記錄器的任何帳戶

存取控制

- 透過 IAM 政策管理對彙總資料的存取
- AWS Config 中央彙總工具帳戶可集中存取所有彙總資料
- 成員帳戶維護其個別 AWS Config 記錄器

最佳實務

Config Central 彙整工具帳戶選擇

- 選擇專用於安全和合規監控的帳戶
- 確保有適當的存取控制

- 考慮使用現有的稽核或安全帳戶

資料管理

- 定期檢閱彙總的組態資料
- 實作適當的保留政策
- 跨帳戶監控 AWS Config 記錄器狀態

遷移影響

升級到登陸區域 4.0 時：

遷移之前

- 記錄現有的 AWS Config 規則和彙總工具
- 檢閱目前的 AWS Config 資料存取模式
- 規劃任何必要的 IAM 政策更新

在遷移期間

- 舊版 AWS Config 彙總工具會自動移除
- 將部署服務連結組態彙總工具
- 將設定委派管理員

遷移後

- 驗證服務連結組態彙整工具是否正常運作
- 從成員帳戶確認資料彙總
- 視需要更新監控和報告工具

使用 IAM 管理實體的許可

AWS Identity and Access Management (IAM) 是一種 AWS 服務，用於控制對其他 AWS 服務的存取。透過 IAM，您可以集中管理使用者、安全登入資料，例如存取金鑰和許可，這些登入資料會指定授予使用者和應用程式存取 AWS 的資源。

當您設定登陸區域時，如果您選取 IAM 做為身分提供者，則可以為 AWS IAM Identity Center 自動建立多個群組。這些群組具有來自 IAM 的預先定義許可政策的許可集。您的最終使用者也可以使用 IAM 來定義成員帳戶中 IAM 使用者和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的方式。您可以在 AWS Control Tower 中控制所有 AWS 帳戶的 IAM Identity Center 存取和使用者許可。

如需詳細資訊，請參閱 AWS IAM Identity Center 使用者指南。

如果您位於不支援 IAM AWS 區域 的 中，您可以攜帶另一個身分提供者，以手動設定和維護您自己的使用者和群組。

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 可讓您選用加密金鑰 AWS KMS 來加密資料。如需 的詳細資訊 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

您可以使用 執行程式碼 AWS Lambda，而無需佈建或管理伺服器。您可以為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開銷。當您上傳程式碼時，Lambda 可以使用高可用性執行和擴展程式碼。您可以設定程式碼以自動從其他 AWS 服務觸發，也可以直接從任何 Web 或行動應用程式呼叫它。

例如，AWS Control Tower 稽核帳戶中的某些角色可以透過程式設計方式擔任，因此您可以使用 Lambda 檢閱其他帳戶。此外，您可以使用 AWS Control Tower 生命週期事件來觸發 Lambda 函數。

透過 管理帳戶 AWS Organizations

AWS Organizations 是一種帳戶管理服務，可讓您將多個 AWS 帳戶合併到您建立並集中管理的組織。透過 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 使用以下 OUs：

- 根 – 登陸區域中所有帳戶和所有其他 OUs的父容器。
- 安全性 – 此 OU 包含日誌封存帳戶、稽核帳戶及其擁有的資源。
- 沙盒 – 當您設定登陸區域時，會建立此 OU。它和登陸區域中的其他子 OUs包含您的成員帳戶。這些是您的最終使用者用來對 AWS 資源執行工作的帳戶。

> **Note**
>
> 您可以透過組織單位頁面上的 AWS Control Tower 主控台，在登陸區域中新增其他 OUs。

考量事項

透過 AWS Control Tower 建立OUs 可以套用控制項。根據預設，在 AWS Control Tower 外部建立的 OUs 無法。不過，您可以註冊這類 OUs。註冊 OU 後，您可以將控制項套用至它及其帳戶。如需註冊 OU 的資訊，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 管理主控台簡單且直覺的 web 界面，來完成這些任務。如需詳細資訊，請參閱 Amazon Simple Storage Service 使用者指南。

當您設定登陸區域時，日誌封存帳戶中會建立 Amazon S3 儲存貯體，以包含登陸區域中所有帳戶的所有日誌。

使用 Security Hub CSPM 監控您的環境

AWS Control Tower 透過稱為服務受管標準 AWS AWS Control Tower 的 Security Hub CSPM 標準與 Security Hub CSPM 整合。 如需詳細資訊，請參閱 Security Hub 標準。

透過 佈建帳戶 AWS Service Catalog

AWS Service Catalog 可讓 IT 管理員建立、管理和分發核准產品組合給最終使用者，這些使用者接著可以在個人化入口網站中存取他們所需的產品。典型的產品包括使用 AWS 資源部署的伺服器、資料庫、網站或應用程式。

您可以控制有權存取特定產品的使用者，這可讓您強制執行組織商業標準的合規性、管理產品生命週期，並協助使用者放心地尋找和啟動產品。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 AWS Service Catalog 產品在您的登陸區域中佈建自訂帳戶，稱為自訂藍圖。如需詳細資訊，請參閱Step2。建立 AWS Service Catalog 產品。

您可以透過 AWS Service Catalog 主控台和 APIs 與 AWS Control Tower 帳戶互動。如需詳細資訊，請參閱與來自 的 AWS Control Tower 帳戶互動 AWS Service Catalog

AWS Control Tower 也可以利用 Service Catalog APIs進一步自動化帳戶佈建和更新。如需詳細資訊，請參閱 AWS Service Catalog 開發人員指南。

透過 Amazon Simple Notification Service 追蹤提醒

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 將程式設計提醒傳送到您管理帳戶和稽核帳戶的電子郵件地址。這些提醒可協助您防止登陸區域內的漂移。如需詳細資訊，請參閱在 AWS Control Tower 中偵測並解決偏離。

我們也使用 Amazon Simple Notification Service 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）的最佳方式之一是訂閱 `AggregateConfigurationNotifications`。此服務可協助您檢查合規性。它為您提供有關 AWS Config 不合規規則的真實資料。 AWS Config 會自動維護 OU 中的帳戶清單。
> 您必須使用電子郵件或 SNS 允許的任何訂閱類型來手動訂閱。陳述式`arn:aws:sns:`*`homeregion`*`:`*`account`*`:aws-controltower-AggregateSecurityNotifications`會導致您的稽核帳戶。

使用 建置分散式應用程式 AWS Step Functions

AWS Step Functions 可讓您輕鬆地協調分散式應用程式的元件，做為視覺化工作流程中的一系列步驟。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

若要在您的登陸區域中執行任何操作，例如在 Account Factory 中佈建帳戶，或在 AWS Control Tower 主控台中建立新的組織單位 (OUs)，請執行 AWS Identity and Access Management (IAM)，或 AWS IAM Identity Center 要求您驗證您是核准的 AWS 使用者。例如，如果您使用的是 AWS Control Tower 主控台，您可以依照 AWS 管理員提供的登入資料來驗證您的身分。

驗證您的身分後，IAM AWS 會使用一組特定操作和資源的已定義許可來控制您對 的存取。如果您是帳戶管理員，您可以使用 IAM 來控制其他 IAM 使用者存取與您帳戶相關聯的資源。

主題

身分驗證

您可以使用下列 AWS 任一類型的身分來存取 ：

- AWS 帳戶根使用者 – 當您第一次建立 AWS 帳戶時，您會從對帳戶中所有 AWS 服務和資源具有完整存取權的身分開始。此身分稱為 AWS 帳戶根使用者。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。反之，請遵守僅使用根使用者的最佳實務，以建立您的第一個 IAM Identity Center 使用者（建議）或 IAM 使用者（在大多數使用案例中不是最佳實務）。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，請參閱以根使用者身分登入的時機。
- 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 使用者登入資料來登入安全 AWS 網頁，例如 AWS 管理主控台、 AWS 討論論壇或 AWS 支援中心。 AWS 最佳實務建議您建立 IAM Identity Center 使用者，而不是 IAM 使用者，因為當您建立具有長期登入資料的 IAM 使用者時，會有更高的安全風險。

  如果您必須為特定用途建立 IAM 使用者，除了登入憑證之外，您還可以為每個 IAM 使用者產生存取金鑰。當您透過其中一個 SDKs 或使用 AWS 命令列界面 (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，則必須自行簽署請求。AWS Control Tower 支援 Signature 第 4 版，這是用於驗證傳入 API 請求的通訊協定。如需驗證請求的詳細資訊，請參閱《 AWS 一般參考》中的 Signature 第 4 版簽署程序。

- 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 角色類似於中的 IAM 使用者，因為它是 AWS 身分，並且具有許可政策來決定身分在 中可以和不能執行的操作 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：
  - 聯合身分使用者存取 – 您可以使用來自 Directory Service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。這些稱為聯合身分使用者。當透過身分提供者請求存取時， 會將角色 AWS 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 – 服務角色是服務擔任的 IAM 角色，可代表您在帳戶中執行動作。當您設定某些 AWS 服務環境時，您必須定義服務要擔任的角色。此服務角色必須包含服務存取所需 AWS 資源所需的所有許可。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》中的建立角色以將許可委派給 AWS 服務。
  - 在 Amazon EC2 上執行的應用程式 – 您可以使用 IAM 角色來管理在 Amazon EC2 執行個體上執行之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適合。若要將 AWS 角色指派給 Amazon EC2 執行個體並將其提供給其所有應用程式，您可以建立連接至執行個體的執行個體描述檔。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 Identity Center 使用者對 IAM Identity Center 使用者入口網站的身分驗證是由您已連線至 IAM Identity Center 的目錄所控制。不過，使用者入口網站內可供最終使用者使用的 AWS 帳戶授權取決於兩個因素：
  - 在 IAM Identity Center 主控台中 AWS ，誰已被指派存取這些 AWS 帳戶。如需詳細資訊，請參閱AWS IAM Identity Center 《 使用者指南》中的單一登入存取。
  - AWS IAM Identity Center 主控台中授予最終使用者何種層級的許可，以允許他們適當存取這些 AWS 帳戶。如需詳細資訊，請參閱AWS IAM Identity Center 《 使用者指南》中的許可集。

存取控制

若要建立、更新、刪除或列出登陸區域中的 AWS Control Tower 資源或其他 AWS 資源，您需要許可才能執行操作，而且需要許可才能存取對應的資源。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。

下列各節說明如何管理 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 Identity Center 和 AWS Control Tower

在 AWS Control Tower 中，IAM Identity Center 允許中央雲端管理員和最終使用者管理對多個 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，除非您已選取自我管理身分和存取控制的選項。

如需選取身分提供者的詳細資訊，請參閱 IAM Identity Center 指引。

如需如何在 AWS Control Tower 中設定 IAM Identity Center 使用者和許可的簡短教學課程，您可以檢視此影片 (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 Identity Center 的影片逐步解說。

關於使用 IAM Identity Center 設定 AWS Control Tower

當您最初設定 AWS Control Tower 時，只有根使用者和具有正確許可的任何 IAM 使用者才能新增 IAM Identity Center 使用者。不過，在 AWSAccountFactory 群組中新增最終使用者之後，他們可以從 Account Factory 精靈建立新的 IAM Identity Center 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登陸區域，協助您管理使用者身分和單一登入，以便您的使用者跨帳戶擁有聯合存取。當您設定登陸區域時，系統會建立此預設目錄，以包含使用者群組和許可集。

> **Note**
>
> 您可以使用 IAM Identity Center 的委派管理員功能，將 AWS IAM Identity Center 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 AWS SSO 委派管理入門

使用者群組、角色和許可集

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。

可用的許可集涵蓋各種不同的使用者許可要求，例如唯讀存取、AWS Control Tower 管理存取和 Service Catalog 存取。這些許可集可讓您的最終使用者快速在您的登陸區域中佈建自己的 AWS 帳戶，並符合您的企業準則。

如需規劃使用者、群組和許可配置的秘訣，請參閱設定群組、角色和政策的建議

如需如何在 AWS Control Tower 內容中使用此服務的詳細資訊，請參閱AWS IAM Identity Center《 使用者指南》中的下列主題。

- 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 會在您的主要區域中設定您的 IAM Identity Center 目錄。如果您在另一個區域中設定登陸區域，然後導覽至 IAM Identity Center 主控台，則必須將該區域變更為您所在區域。請勿刪除您主要區域中的 IAM Identity Center 組態。

IAM Identity Center 帳戶和 AWS Control Tower 的須知事項

以下是在 AWS Control Tower 中使用 IAM Identity Center 使用者帳戶時需要了解的一些好事項。

- 如果您的 AWS IAM Identity Center 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 Identity Center 主控台中重新啟用 IAM Identity Center 使用者。
- 如果您在更新與帳戶工廠提供的帳戶相關聯的佈建產品時指定新的 IAM Identity Center 使用者電子郵件地址，AWS Control Tower 會建立新的 IAM Identity Center 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 IAM Identity Center 移除先前的 AWS IAM Identity Center 使用者電子郵件地址，請參閱停用使用者。
- AWS IAM Identity Center 已與 Azure Active Directory 整合，您可以將現有的 Azure Active Directory 連線至 AWS Control Tower。
- 如需 AWS Control Tower 行為如何與 AWS IAM Identity Center 和不同身分來源互動的詳細資訊，請參閱 AWS IAM Identity Center 文件中的變更身分來源注意事項。

AWS Control Tower 的 IAM Identity Center 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 Identity Center 中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。如需設定 群組的最新指引和最佳實務，請參閱《IAM Identity Center 使用者指南》中的最佳實務。

當您設定登陸區域時，會建立下列群組。

AWSAccountFactory

帳戶	許可集	Description
管理帳戶	AWSServiceCatalogEndUserAccess	此群組僅用於此帳戶中，以使用 Account Factory 佈建新帳戶。

AWSServiceCatalogAdmins

帳戶	許可集	Description
管理帳戶	AWSServiceCatalogAdminFullAccess	此群組僅用於此帳戶，以對帳戶工廠進行管理變更。除非同時位於 AWSAccountFactory 群組中，否則此群組中的使用者無法佈建新帳戶。

AWSControlTowerAdmins

帳戶	許可集	Description
管理帳戶	AWSAdministratorAccess	此帳戶中此群組的使用者是唯一可存取 AWS Control Tower 主控台的使用者。
日誌封存帳戶	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	使用者可完整存取此帳戶中的 Organizations。

AWSSecurityAuditPowerUsers

帳戶	許可集	Description
管理帳戶	AWSPowerUserAccess	使用者可以執行應用程式開發任務，也可以建立和設定支援 AWS 感知應用程式開發的資源和服務。
日誌封存帳戶	AWSPowerUserAccess	使用者可以執行應用程式開發任務，也可以建立和設定支援 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任務，也可以建立和設定支援 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任務，也可以建立和設定支援

帳戶	許可集	Description
		AWS 感知應用程式開發的資源和服務。

AWSSecurityAuditors

帳戶	許可集	Description
管理帳戶	AWSReadOnlyAccess	使用者可唯讀存取此帳戶中的所有 AWS 服務和資源。
日誌封存帳戶	AWSReadOnlyAccess	使用者可唯讀存取此帳戶中的所有 AWS 服務和資源。
稽核帳戶	AWSReadOnlyAccess	使用者可唯讀存取此帳戶中的所有 AWS 服務和資源。
成員帳戶	AWSReadOnlyAccess	使用者可唯讀存取此帳戶中的所有 AWS 服務和資源。

AWSLogArchiveAdmins

帳戶	許可集	Description
日誌封存帳戶	AWSAdministratorAccess	此帳戶中的使用者將具備管理存取權限。

AWSLogArchiveViewers

帳戶	許可集	Description
日誌封存帳戶	AWSReadOnlyAccess	使用者可唯讀存取此帳戶中的所有 AWS 服務和資源。

AWSAuditAccountAdmins

帳戶	許可集	Description
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 資源都由 擁有 AWS 帳戶，而建立或取得資源存取權的許可是由許可政策管理。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)。有些 服務 （ 例如 AWS Lambda) 也支援將許可政策連接至 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。

當您負責將許可授予使用者或角色時，您必須知道並追蹤需要許可的使用者和角色、每個使用者和角色需要許可的資源，以及操作這些資源時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
- 管理對 資源的存取
- 指定政策元素：動作、效果和委託人
- 在政策中指定條件

AWS Control Tower 資源和操作

在 AWS Control Tower 中，主要資源是登陸區域。AWS Control Tower 也支援其他資源類型、控制項，有時稱為護欄。不過，對於 AWS Control Tower，您只能在現有登陸區域的內容中管理控制項。控制項可以稱為子資源。

中的資源和子資源 AWS 具有與其相關聯的唯一 Amazon Resource Name (ARNs)，如下列範例所示。

AWS Control Tower 提供一組 API 操作，以使用 AWS Control Tower 資源。如需可用操作的清單，請參閱 AWS Control Tower the AWS Control Tower API Reference。

如需 AWS Control Tower 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

無論誰建立資源， AWS 帳戶都會擁有在帳戶中建立的資源。具體而言，資源擁有者是驗證資源建立請求之主體實體（即 AWS 帳戶 根使用者、IAM Identity Center 使用者、IAM 使用者或 IAM 角色）AWS 的帳戶。下列範例說明其如何運作：

- 如果您使用 AWS 帳戶的 AWS 帳戶根使用者登入資料來設定登陸區域， AWS 您的帳戶即為資源的擁有者。
- 如果您在 AWS 帳戶中建立 IAM 使用者，並將設定登陸區域的許可授予該使用者，只要其帳戶符合先決條件，該使用者就可以設定登陸區域。不過，使用者所屬 AWS 的帳戶擁有登陸區域資源。
- 如果您在 AWS 帳戶中建立具有設定登陸區域許可的 IAM 角色，則任何可以擔任該角色的人都可以設定登陸區域。該角色所屬 AWS 的帳戶擁有登陸區域資源。

管理對 資源的存取

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。

連接至 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 僅支援以身分為基礎的政策 (IAM 政策）。

主題

- 關於以身分為基礎的政策 (IAM 政策)
- 建立角色並指派許可
- 資源型政策

關於以身分為基礎的政策 (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：

- 將許可政策連接至您帳戶中的使用者或群組 – 若要授予使用者建立 AWS Control Tower 資源的許可，例如設定登陸區域，您可以將許可政策連接至使用者或使用者所屬的群組。
- 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 帳戶的管理員 (帳戶 A) 可以建立將跨帳戶許可授予另一個 AWS 帳戶 (帳戶 B) 的角色，或者管理員可以建立將許可授予另一個 AWS 服務的角色。
  1. 帳戶 A 管理員會建立 IAM 角色，並將許可政策連接至角色，以授予許可來管理帳戶 A 中的資源。
  2. 帳戶 A 管理員會將信任政策連接至角色。此政策會將帳戶 B 識別為可擔任該角色的委託人。
  3. 身為委託人，帳戶 B 管理員可以授予帳戶 B 中的任何使用者擔任該角色的許可。透過擔任角色，帳戶 B 中的使用者可以建立或存取帳戶 A 中的資源。
  4. 若要授予 AWS 服務擔任角色的能力 （許可），您在信任政策中指定的委託人可以是 AWS 服務。

建立角色並指派許可

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：

- 中的使用者和群組 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。遵循《IAM 使用者指南》的為第三方身分提供者 (聯合) 建立角色中的指示。
- IAM 使用者：
  - 建立您的使用者可擔任的角色。請按照《IAM 使用者指南》的為 IAM 使用者建立角色中的指示。

- (不建議) 將政策直接附加至使用者，或將使用者新增至使用者群組。請遵循《IAM 使用者指南》的新增許可到使用者 (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 登陸區域時，您需要具有 AdministratorAccess 受管政策的使用者或角色。(arn：aws：iam：：aws：policy/AdministratorAccess)

為 AWS 服務 (IAM 主控台） 建立角色

1. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
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. 針對服務或使用案例，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. 對於許可政策，選項取決於您選取的使用案例：
   - 如果服務定義了角色的許可，則您無法選取許可政策。
   - 從一組有限的許可政策中選取。
   - 從所有許可政策中選取。
   - 選取無許可政策，在建立角色之後建立政策，然後將政策連接到角色。
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. 開啟設定許可界限區段，然後選擇使用許可界限來控制角色許可上限。

      IAM 包含您帳戶中 AWS 受管和客戶受管政策的清單。

   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，則無法編輯角色名稱。

- 如果服務定義了角色名稱的字首，則可以輸入選用字尾。
- 如果服務未定義角色名稱，則可以為角色命名。

> **Important**
>
> 當您命名角色時，請注意下列事項：
>
> - 角色名稱在您的 中必須是唯一的 AWS 帳戶，而且無法依大小寫設為唯一。
>
> 例如，不要同時建立名為 **PRODROLE** 和 **prodrole** 的角色。當角色名稱用於政策或 ARN 的一部分時，角色名稱會區分大小寫，但是當角色名稱在主控台中顯示給客戶時，例如在登入過程中，角色名稱不會區分大小寫。
> - 因為其他實體可能會參考角色，所以在建立角色之後，就無法編輯其名稱。

10. (選用) 在說明中，輸入角色的說明。
11. (選用) 若要編輯使用案例和角色許可，請在步驟 1：選取受信任的實體或者步驟 2：新增許可區段中選擇編輯。
12. (選用) 若要協助識別、組織或搜尋角色，請將標籤新增為索引鍵值對。如需在 IAM 中使用標籤的詳細資訊，請參閱《IAM 使用者指南》中的AWS Identity and Access Management 資源的標籤。
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 管理主控台 ，並在 https：//https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
2. 在左側的導覽窗格中，選擇 Policies (政策)。

   如果這是您第一次選擇 Policies (政策)，將會顯示 Welcome to Managed Policies (歡迎使用受管政策) 頁面。選擇 Get Started (開始使用)。
3. 在頁面頂端，選擇 Create policy (建立政策)。
4. 在政策編輯器中，選擇 JSON 選項。
5. 輸入或貼上 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. （選用）當您在 中建立或編輯政策時 AWS 管理主控台，您可以產生可在 範本中使用的 JSON 或 YAML 政策 CloudFormation 範本。

   若要執行此動作，請在政策編輯器中選擇動作，然後選擇產生 CloudFormation 範本。若要進一步了解 CloudFormation，請參閱AWS CloudFormation 《 使用者指南》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。如需在 IAM 中使用標籤的詳細資訊，請參閱《IAM 使用者指南》中的AWS Identity and Access Management 資源的標籤。
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 管理主控台 ，並在 https：//https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
2. 在左側的導覽窗格中，選擇 Policies (政策)。

   如果這是您第一次選擇 Policies (政策)，將會顯示 Welcome to Managed Policies (歡迎使用受管政策) 頁面。選擇 Get Started (開始使用)。

3. 選擇建立政策。
4. 在政策編輯器區段中，尋找選取服務區段，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政策個別允許的許可時，才會拒絕許可。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 Resource Name (ARNs)。如需有關在政策的 `Resource`元素中使用 ARNs 的資訊，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素：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使用者是否必須使用多重要素驗證 (MFA) 裝置進行身分驗證。或者，您可以要求請求必須源自於特定 IP 地址範圍。如需您可以在政策條件中使用的所有內容金鑰清單，請參閱《服務授權參考》中的 AWS 服務的動作、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、限定詞和運算子，然後輸入值。若要新增超過一個值，請選擇新增。您可以將值視為由邏輯OR運算子連線。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，請考慮邏輯AND運算子要連線的條件。

如需 條件元素的詳細資訊，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素：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. （選用）當您在 中建立或編輯政策時 AWS 管理主控台，您可以產生可在 範本中使用的 JSON 或 YAML 政策 CloudFormation 範本。

   若要執行此動作，請在政策編輯器中選擇動作，然後選擇產生 CloudFormation 範本。若要進一步了解 CloudFormation，請參閱AWS CloudFormation 《 使用者指南》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。如需在 IAM 中使用標籤的詳細資訊，請參閱《IAM 使用者指南》中的AWS Identity and Access Management 資源的標籤。
13. 選擇 Create policy (建立政策) 儲存您的新政策。

授予程式設計存取權

如果使用者想要與 AWS 外部互動，則需要程式設計存取 AWS 管理主控台。授予程式設計存取權的方式取決於正在存取的使用者類型 AWS。

若要授予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	根據
IAM	（建議）使用主控台登入資料做為臨時登入資料，以簽署對 AWS CLI、 AWS SDKs程式設計請求。 AWS APIs	請依照您要使用的介面所提供的指示操作。 • 如需 AWS CLI，請參閱AWS Command Line Interface 《使用者指南》中的登入以進行 AWS 本機開發。 • AWS SDKs請參閱 AWS SDKs和工具參考指南中的登入以進行 AWS 本機開發。
人力資源身分 (IAM Identity Center 中管理的使用者)	使用暫時登入資料簽署對 AWS CLI、 AWS SDKs程式設計請求。 AWS APIs	請依照您要使用的介面所提供的指示操作。 • 如需 AWS CLI，請參閱AWS Command Line Interface 《使用者指南》中的設定 AWS CLI 要使用 AWS IAM Identity Center的 。 • AWS SDKs、工具和 AWS APIs，請參閱 AWS SDKs 和工具參考指南中的 IAM Identity Center 身分驗證。
IAM	使用暫時登入資料簽署對 AWS CLI、 AWS SDKs程式設計請求。 AWS APIs	遵循《IAM 使用者指南》中將臨時登入資料與 AWS 資源搭配使用的指示。
IAM	(不建議使用) 使用長期憑證簽署對 AWS CLI、 AWS SDKs 或 AWS APIs程式設計請求。	請依照您要使用的介面所提供的指示操作。 • 如需 AWS CLI，請參閱AWS Command Line Interface 《使用者指南》中的使用

哪個使用者需要程式設計存取權？	到	根據
		IAM 使用者憑證進行身分驗證。 • AWS SDKs和工具，請參閱 AWS SDKs和工具參考指南中的使用長期憑證進行身分驗證。 • 對於 AWS APIs，請參閱《IAM 使用者指南》中的管理 IAM 使用者的存取金鑰。

防範攻擊者

如需如何在將許可授予其他服務 AWS 委託人時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。透過將特定條件新增至您的政策，您可以協助防止特定類型的攻擊，稱為混淆代理人攻擊，如果實體強制更特權的實體執行動作，例如跨服務模擬。如需政策條件的一般資訊，另請參閱 在政策中指定條件。

如需搭配 AWS Control Tower 使用身分型政策的詳細資訊，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。

指定政策元素：動作、效果和委託人

您可以透過 AWS Control Tower 主控台或登陸區域 APIs 來設定和管理登陸區域。若要設定登陸區域，您必須是具有 IAM 政策所定義管理許可的 IAM 使用者。

以下是您可以在政策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。如需有關可執行之動作類型的資訊，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。
- 委託人 – 在以身分為基礎的政策 (IAM 政策） 中，附加政策的使用者是隱含委託人。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。

若要表達條件，您可以使用預先定義的條件索引鍵。AWS Control Tower 沒有特定的條件索引鍵。不過，您可以視需要使用 AWS全局條件索引鍵。如需 AWS全系列金鑰的完整清單，請參閱《IAM 使用者指南》中的條件的可用金鑰。

防止跨服務模擬

在 中 AWS，跨服務模擬可能會導致混淆代理人問題。當一個服務呼叫另一個服務時，如果一個服務操縱另一個服務來使用其許可，以以其他方式不允許的方式處理客戶的資源，則會發生跨服務模擬。為了防止此攻擊， AWS 提供工具來協助您保護資料，因此只有具有合法許可的服務才能存取您帳戶中的資源。

我們建議您在政策中使用 `aws:SourceArn`和 `aws:SourceAccount`條件，以限制 AWS Control Tower 提供給其他服務的許可，以存取您的 資源。

- `aws:SourceArn` 如果您希望只有一個資源與跨服務存取相關聯，請使用 。
- `aws:SourceAccount` 如果您想要允許該帳戶中的任何資源與跨服務使用相關聯，請使用 。
- 如果`aws:SourceArn`值不包含帳戶 ID，例如 Amazon S3 儲存貯體的 ARN，您必須使用這兩個條件來限制許可。

- 如果您同時使用這兩個條件，而且該`aws:SourceArn`值包含帳戶 ID，則值中的`aws:SourceAccount`值和帳戶`aws:SourceArn`必須在相同的政策陳述式中使用時顯示相同的帳戶 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，示範帳戶管理員如何將許可政策連接至 IAM 身分 （即使用者、群組和角色），並藉此授予在 AWS Control Tower 資源上執行操作的許可。

> **Important**
>
> 我們建議您先檢閱簡介主題，這些主題說明可用於管理 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

當您設定登陸區域時，AWS Control Tower 會自動建立三個角色。需要這三個角色才能允許主控台存取。AWS Control Tower 將許可分割為三個角色作為最佳實務，以限制對最少動作和資源的存取。

登陸區域存取的三個必要角色

- AWS ControlTowerAdmin 角色
- AWS ControlTowerStackSetRole

我們建議您限制存取這些角色的角色信任政策。如需詳細資訊，請參閱角色信任關係的選用條件。

在主控台中檢視 Control Catalog

若要在 AWS Control Tower 主控台中檢視控制項資訊，您必須將其他`controlcatalog`許可新增至 IAM 政策。這些許可如下所示：

- `controlcatalog:GetControl`
- `controlcatalog:ListControls`

- controlcatalog:ListControlMappings
- controlcatalog:ListCommonControls

以下是顯示政策中已更新許可的範例。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "controlcatalog:GetControl",
                "controlcatalog:ListControls",
                "controlcatalog:ListControlMappings",
                "controlcatalog:ListCommonControls"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

您必須新增這些許可，因為 AWS Control Tower 會呼叫 controlcatalog APIs來擷取特定控制中繼資料，因此 AWS Control Tower 許可不足。

若要尋找如何更新許可的詳細資訊，請參閱建立角色和指派許可。

若要尋找 IAM controlcatalog 動作的詳細資訊，請參閱 Control Catalog 的動作、資源和條件索引鍵。

> **Note**
>
> 控制資訊可透過 Control Catalog APIs取得。

AWS ControlTowerAdmin 角色

此角色可讓 AWS Control Tower 存取對維護登陸區域至關重要的基礎設施。此AWS ControlTowerAdmin角色需要附加的 受管政策和 IAM 角色的角色信任政策。角色信任政策是以資源為基礎的政策，指定哪些委託人可以擔任該角色。

以下是此角色信任政策的範例程式碼片段：

JSON

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

若要從 CLI AWS 建立此角色，並將其放入名為 的檔案trust.json，以下是 CLI 命令範例：

```
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：

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeAvailabilityZones",
```

```
            "Resource": "*"
        }
    ]
}
```

2. 接下來的受管政策，即 `AWS ControlTowerServiceRolePolicy`。

AWS ControlTowerServiceRolePolicy

AWS ControlTowerServiceRolePolicy 是一種 AWS受管政策，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 日誌檔案、AWS Control Tower 的組態彙總器，以及受 AWS Control Tower 管理 AWS Organizations 的帳戶和組織單位 (OUs)。

此受管政策的更新摘要於 資料表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》中的 AWS ControlTowerServiceRolePolicy。

角色信任政策：

JSON

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

內嵌政策為 `AWS ControlTowerAdminPolicy`：

JSON

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

AWS ControlTowerIdentityCenterManagementPolicy

此政策提供在註冊 AWS Control Tower 的成員帳戶中設定 IAM Identity Center (IdC) 資源的許可。當您在 AWS Control Tower 的登陸區域設定 （或更新） 期間選取 IAM Identity Center 做為身分提供者時，此政策會連接至`AWS ControlTowerAdmin`角色。

若要檢視政策的詳細資訊，包括最新版本的 JSON 政策文件，請參閱《 AWS 受管政策參考指南》中的 AWS ControlTowerIdentityCenterManagementPolicy。

AWS ControlTowerStackSetRole

CloudFormation 會擔任此角色，在 AWS Control Tower 建立的帳戶中部署堆疊集。內嵌政策

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/AWSControlTowerExecution"
            ],
            "Effect": "Allow"
        }
```

```
    ]
}
```

信任政策

JSON

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

AWS ControlTowerCloudTrailRolePolicy

AWS Control Tower 可讓 CloudTrail 成為最佳實務，並將此角色提供給 CloudTrail。CloudTrail 會擔任此角色來建立和發佈 CloudTrail 日誌。

受管政策： `AWS ControlTowerCloudTrailRolePolicy`

此角色使用 AWS受管政策 `AWS ControlTowerCloudTrailRolePolicy`，授予 CloudTrail 代表 AWS Control Tower 將稽核日誌發佈至 Amazon CloudWatch Logs 所需的許可。此受管政策會取代先前用於此角色的內嵌政策，讓 AWS 無需客戶介入即可更新政策。

如需詳細資訊，請參閱《 AWS 受管政策參考指南》中的 AWS ControlTowerCloudTrailRolePolicy。

此受管政策的更新摘要於 資料表AWS Control Tower 的受管政策。

> **Note**
>
> 在引進 受管政策之前，此角色使用具有同等許可的內嵌政策。內嵌政策已由 受管政策取代，以啟用無縫更新。

先前的內嵌政策（以供參考）：

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"
        }
    ]
}
```

信任政策

JSON

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

AWS ControlTowerBlueprintAccess 角色需求

AWS Control Tower 要求您在同一組織內，在指定的藍圖中樞帳戶中建立AWS ControlTowerBlueprintAccess角色。

Role name (角色名稱)

角色名稱必須是 AWS ControlTowerBlueprintAccess。

角色信任政策

必須設定 角色以信任下列委託人：

- 管理帳戶中使用 AWS Control Tower 的委託人。
- 管理帳戶中AWS ControlTowerAdmin的角色。

下列範例顯示最低權限的信任政策。當您制定自己的政策時，請將 *YourManagementAccountId* 一詞取代為 AWS Control Tower 管理帳戶的實際帳戶 ID，並將 *YourControlTowerUserRole* 一詞取代為管理帳戶的 IAM 角色識別符。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:role/service-role/
AWSControlTowerAdmin",
                    "arn:aws:iam::111122223333:role/YourControlTowerUserRole"
                ]
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```

角色許可

您必須將 受管政策 AWSServiceCatalogAdminFullAccess 連接至角色。

AWSServiceRoleForAWSControlTower

此角色可讓 AWS Control Tower 存取 Log Archive 帳戶、稽核帳戶和成員帳戶，以進行維護登陸區域至關重要的操作，例如通知您資源漂移。

此AWS ServiceRoleFor AWS ControlTower角色需要附加的 受管政策和 IAM 角色的角色信任政策。

此角色的受管政策： AWS ControlTowerAccountServiceRolePolicy

角色信任政策：

JSON

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

AWS ControlTowerAccountServiceRolePolicy

此 AWS受管政策可讓 AWS Control Tower 代您呼叫提供自動化帳戶組態和集中式控管 AWS 的服務。

此政策包含 AWS Control Tower 的最低許可，以針對 Security Hub CSPM 控制項管理的資源實作 AWS Security Hub CSPM 調查結果轉送，這些資源屬於 Security Hub CSPM 服務受管標準：AWS Control Tower，並可防止限制管理客戶帳戶能力的變更。這是背景 AWS Security Hub CSPM 偏離偵測程序的一部分，並非由客戶直接啟動。

此政策提供許可來建立 Amazon EventBridge 規則，特別是針對每個成員帳戶中的 Security Hub CSPM 控制項，而且這些規則必須指定確切的 EventPattern。此外，規則只能操作於由我們的服務委託人管理的規則。

服務主體： `controltower.amazonaws.com`

如需詳細資訊，請參閱《 AWS 受管政策參考指南》中的 AWS ControlTowerAccountServiceRolePolicy。

此受管政策的更新摘要於 資料表AWS Control Tower 的受管政策。

AWS Control Tower 的受管政策

AWS 提供由 建立和管理的獨立 IAM 政策，以解決許多常見的使用案例 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	Date
AWS ControlTowerAccountServiceRolePolicy – 更新現有政策	AWS Control Tower 新增了新的許可，允許 AWS Control Tower 呼叫 AWS CloudFormation 服務 API，`BatchDescribeTypeConfigurations` 以內部改善服務連結勾點。	2026 年 3 月 23 日
AWS ControlTowerAccountServiceRolePolicy – 更新現有政策	AWS Control Tower 已更新現有政策，以改善 Amazon EventBridge 規則條件的驗證精確度。更新會將`events:detail-type` 條件從 `StringEquals` 移至 `ForAllValues:StringEquals` ，以獲得更好的事件模式比對控制，同時維持相同的功能許可。	2025 年 12 月 30 日

變更	描述	Date
AWS ControlTowerAccountServiceRolePolicy – 更新現有政策	AWS Control Tower 新增了延伸下列許可的新政策： • AWS Config 建立、標記、刪除、管理和讀取服務連結組態彙總器的許可 • AWS Config 描述所有組態彙總器的許可 • AWS Organizations 列出委派管理員的許可 AWS Config • AWS Organizations 描述組織的許可 • CloudFormation 管理服務連結勾點的許可	2025 年 11 月 10 日

變更	描述	Date
AWS ControlTowerServiceRolePolicy – 更新 受管政策	AWS Control Tower 已更新 AWS ControlTowerServiceRolePolicy 中的 Amazon CloudWatch Logs 資源模式，以支援登陸區域 4.0 的選用 AWS CloudTrail 整合。模式從 變更為 `aws-controltower/CloudTrailLogs:*` `aws-controltower/CloudTrailLogs*:*` ，在 之後新增萬用字元`CloudTrailLogs` ，以允許管理具有任何尾碼的日誌群組。 此更新會啟用登陸區域 4.0 的選用 AWS CloudTrail 整合，讓客戶能夠多次啟用和停用 AWS CloudTrail 整合。每次啟用整合時，都會使用唯一的尾碼重新建立 Amazon CloudWatch Logs 日誌群組，以避免命名衝突。更新與現有部署回溯相容。	2025 年 10 月 31 日

變更	描述	Date
AWS ControlTowerCloudTrailRolePolicy – 新的 受管政策	AWS Control Tower 推出 AWS ControlTowerCloudTrailRolePolicy 受管政策，允許 CloudTrail 建立日誌串流並將日誌事件發佈至 Control Tower 受管 Amazon CloudWatch Logs 日誌群組。 此受管政策會取代 AWS ControlTowerCloudTrailRole 先前使用的內嵌政策，讓 AWS 無需客戶介入即可更新政策。此政策的範圍是使用符合模式的名稱來記錄群組`aws-controltower/CloudTrailLogs*` 。	2025 年 10 月 31 日
AWS ControlTowerIdentityCenterManagementPolicy – 新政策	AWS Control Tower 新增了一項新政策，允許客戶在已註冊 AWS Control Tower 的帳戶中設定 IAM Identity Center 資源，並允許 AWS Control Tower 在自動註冊帳戶時修復某些類型的偏離。 需要此變更，客戶才能在 AWS Control Tower 中設定 IAM Identity Center，讓 AWS Control Tower 可以修復自動註冊偏離。	2025 年 10 月 10 日

變更	描述	Date
AWS ControlTowerServiceRolePolicy – 更新現有政策	AWS Control Tower 新增了新的 CloudFormation 許可，允許 AWS Control Tower 在自動將帳戶註冊到 AWS Control Tower 時，查詢堆疊集資源並將其部署到成員帳戶。	2025 年 10 月 10 日
AWS ControlTowerServiceRolePolicy – 更新現有政策	AWS Control Tower 新增了允許客戶啟用和停用服務連結 AWS Config 規則的新許可。 需要此變更，客戶才能管理由 Config 規則部署的控制項。	2025 年 6 月 5 日
AWS ControlTowerServiceRolePolicy – 更新現有政策	AWS Control Tower 新增了新的許可，允許 AWS Control Tower 在 上呼叫 AWS CloudFormation 服務 APIs `SetTypeConfiguration` 、 `ActivateType` `DeactivateType` 和 `AWS::ControlTower types`。 此變更可讓客戶佈建主動控制，而無需部署私有 CloudFormation 勾點類型。	2024 年 12 月 10 日

變更	描述	Date
AWS ControlTowerAccountServiceRolePolicy – 新政策	AWS Control Tower 新增了新的服務連結角色，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 CSPM 相關的控制項的偏離偵測。 需要進行此變更，以便當這些資源與 Security Hub CSPM 控制相關時，客戶可以在主控台中檢視漂移的資源，這些控制屬於 Security Hub CSPM 服務受管標準：AWS Control Tower 的一部分。	2023 年 5 月 22 日
AWS ControlTowerServiceRolePolicy – 更新現有政策	AWS Control Tower 新增了新的許可，允許 AWS Control Tower 呼叫帳戶管理服務實作的 AWS `EnableRegion` 、 `ListRegions` 和 `GetRegionOptStatus` APIs，讓登陸區域中的客戶帳戶（管理帳戶、日誌封存帳戶、稽核帳戶、OU 成員帳戶）可選擇加入 AWS 區域。 需要此變更，以便客戶可以選擇將 AWS Control Tower 的區域控管擴展到選擇加入區域。	2023 年 4 月 6 日

變更	描述	Date
AWS ControlTowerServiceRolePolicy – 更新現有政策	AWS Control Tower 新增了新的許可，允許 AWS Control Tower 在藍圖（中樞）帳戶中擔任`AWSControlTowerBlueprintAccess` 角色，這是組織中的專用帳戶，其中包含存放在一或多個 Service Catalog 產品中的預先定義藍圖。AWS Control Tower 會擔任執行三個任務`AWSControlTowerBlueprintAccess` 的角色：建立 Service Catalog 產品組合、新增請求的藍圖產品，並在帳戶佈建時將產品組合分享至請求的成員帳戶。 需要此變更，客戶才能透過 AWS Control Tower 帳戶工廠佈建自訂帳戶。	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，從登陸區域 3.0 版開始。 以組織為基礎的 CloudTrail 功能要求客戶為 CloudTrail 服務啟用信任存取，且 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許可。	2022 年 6 月 20 日

變更	描述	Date
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 日誌。客戶也可以在登陸區域更新或修復期間變更 KMS 金鑰。更新 KMS 金鑰時，AWS CloudFormation AWS CloudTrail 需要許可才能呼叫 `PutEventSelector` API。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 的安全性

的雲端安全性 AWS 是最高優先順序。身為 AWS 客戶，您可以受益於資料中心和網路架構，這些架構專為滿足最安全敏感組織的需求而建置。

安全性是 AWS 與您之間的共同責任。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 Cloud 中執行 AWS 服務的基礎設施。 AWS 也為您提供可安全使用的服務。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。若要了解適用於 AWS Control Tower 的合規計劃，請參閱AWS 合規計劃範圍內的服務。
- 雲端的安全性 – 您的責任取決於您使用 AWS 的服務。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 時套用共同責任模型。下列主題說明如何設定 AWS Control Tower 以符合您的安全與合規目標。您也會了解如何使用其他 AWS 服務來協助您監控和保護 AWS Control Tower 資源。

AWS Control Tower 中的資料保護

AWS 共同責任模型適用於 AWS Control Tower 中的資料保護。如此模型所述， AWS 負責保護執行所有 的全域基礎設施 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 共同責任模型和 GDPR 部落格文章。

基於資料保護目的，我們建議您保護 AWS 帳戶 登入資料，並使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 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。如需有關使用 CloudTrail 追蹤擷取 AWS 活動的資訊，請參閱AWS CloudTrail 《 使用者指南》中的使用 CloudTrail 追蹤。
- 使用 AWS 加密解決方案，以及其中的所有預設安全控制 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 AWS 透過命令列界面或 API 存取 時需要 FIPS 140-3 驗證的密碼編譯模組，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) 140-3。

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 AWS Control Tower 或使用主控台、API AWS CLI或其他 AWS 服務 AWS SDKs 時。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**
>
> 當您設定登陸區域時， AWS CloudTrail AWS Control Tower 會自動處理 的使用者活動記錄。

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，可讓您用來協助保護登陸區域中存在的內容：

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，這些資料庫使用 Amazon S3-Managed管金鑰 (SSE-S3) 進行靜態加密，以支援您的登陸區域。當您設定登陸區域時，預設會設定此加密。或者，您可以設定登陸區域，以使用 KMS 加密金鑰加密資源。您也可以為支援此服務的登陸區域中所使用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章節。

傳輸中加密

AWS Control Tower 使用 Transport Layer Security (TLS) 和用戶端加密進行傳輸中加密，以支援您的登陸區域。此外，存取 AWS Control Tower 需要使用 主控台，只能透過 HTTPS 端點存取。當您設定登陸區域時，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。透過 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，或在 IAM Identity Center 使用者的情況下，確保他們位於正確的群組中。

- 如需 IAM 實體角色和政策的詳細資訊，請參閱 IAM 使用者指南。
- 如需設定登陸區域時所建立 IAM Identity Center 群組的詳細資訊，請參閱 AWS Control Tower 的 IAM Identity Center 群組。

AWS Control Tower 的合規驗證

AWS Control Tower 是架構完善的服務，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，第三方稽核人員會評估您可以在登陸區域中使用的許多服務的安全性和合規性，做為多個 AWS 合規計劃的一部分。這些計劃包括 SOC、PCI、FedRAMP、HIPAA 等等。

如需特定合規計劃範圍內 AWS 的服務清單，請參閱AWS 合規計劃範圍內的服務。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 《 使用者指南》中的在 AWS 成品中下載報告。

您在使用 AWS Control Tower 時的合規責任取決於資料的敏感度、您公司的合規目標，以及適用的法律和法規。 AWS 提供下列資源以協助合規：

- 安全與合規快速入門指南 – 這些部署指南討論架構考量，並提供在其中部署以安全與合規為重心的基準環境的步驟 AWS。
- Amazon Web Services 上的 HIPAA 安全與合規架構 – 本白皮書說明公司如何使用 AWS 來建立符合 HIPAA 規範的應用程式。
- AWS 合規資源 – 此工作手冊和指南集合可能適用於您的產業和位置。
- AWS Config – AWS 此服務會評估資源組態符合內部實務、產業準則和法規的程度。
- AWS Security Hub CSPM – AWS 此服務提供 內安全狀態的完整檢視 AWS ，協助您檢查是否符合安全產業標準和最佳實務。

AWS Control Tower 中的彈性

AWS 全球基礎設施是以 AWS 區域和可用區域為基礎建置。

AWS 區域提供多個實體隔離和隔離的可用區域，這些可用區域透過低延遲、高輸送量和高備援聯網進行連接。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 可用 AWS 區域 位置的清單，請參閱 AWS 區域如何使用 AWS Control Tower。

您的主要區域定義為您的登陸區域設定所在的 AWS 區域。

如需 AWS 區域和可用區域的詳細資訊，請參閱 AWS 全球基礎設施。

AWS Control Tower 中的基礎設施安全

AWS Control Tower 受到 Amazon Web Services：安全程序概觀白皮書中所述 AWS 的全球網路安全程序所保護。

您可以使用 AWS 發佈的 API 呼叫，透過網路存取登陸區域內 AWS 的服務和資源。我們需要 Transport Layer Security (TLS) 1.2，並建議 Transport Layer Security (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，為您的 AWS Control Tower 登陸區域工作負載提供額外的網路基礎設施安全性。如需詳細資訊，請參閱逐步解說：使用 在 AWS Control Tower 中設定安全群組 AWS Firewall Manager。

在 AWS Control Tower 中記錄和監控

監控可讓您針對潛在的事件做規劃並加以回應。監控活動的結果會存放在日誌檔案中。因此，記錄和監控是密切相關的概念，它們是 AWS Control Tower 架構良好的本質的重要部分。

當您設定登陸區域時，建立的其中一個共用帳戶是日誌封存帳戶。它專用於集中收集所有日誌，包括所有共用和成員帳戶的日誌。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。

最佳實務是，您應該從設定的所有部分 AWS 收集監控資料到日誌中，以便在發生多點失敗時更輕鬆地偵錯。 AWS 提供數種工具來監控登陸區域中的資源和活動。

例如，會持續監控控制項的狀態。您可以在 AWS Control Tower 主控台中快速查看其狀態，或透過 AWS Control Tower APIs 以程式設計方式查看。您在 Account Factory 中佈建之帳戶的運作狀態和狀態也會持續受到監控。

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，請從左側導覽中選取活動。

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，但會以資料表格式顯示。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)。

您可以在日誌封存檔案中檢視成員帳戶動作和事件。

下列各節說明在 AWS Control Tower 中監控和記錄的詳細資訊：

主題

- 用於監控的整合式工具
- 使用 記錄 AWS Control Tower 動作 AWS CloudTrail
- AWS Control Tower 中的生命週期事件
- 搭配 使用 AWS 使用者通知 AWS Control Tower

關於在 AWS Control Tower 中記錄

AWS Control Tower 透過與 和 的整合，自動完成動作 AWS CloudTrail 和事件的記錄 AWS Config，並將其記錄在 CloudWatch 中。系統會記錄所有動作，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。您可以在日誌封存檔案中檢視成員帳戶動作和事件。

組織層級追蹤

當您設定登陸區域時，AWS Control Tower 會設定新的 CloudTrail 追蹤。這是組織層級追蹤，這表示它會記錄管理帳戶和組織中的所有成員帳戶的所有事件。此功能倚賴受信任的存取，授予管理帳戶在每個成員帳戶上建立追蹤的許可。

如需 AWS Control Tower 和 CloudTrail 組織線索的詳細資訊，請參閱為組織建立線索。

> **Note**
>
> 在登陸區域 3.0 版之前的 AWS Control Tower 版本中，AWS Control Tower 在每個帳戶中建立成員帳戶追蹤。當您更新至 3.0 版時，您的 CloudTrail 追蹤會成為組織追蹤。如需在線索之間移動時的最佳實務，請參閱 CloudTrail 使用者指南中的變更線索的最佳實務。

當您向 AWS Control Tower 註冊帳戶時，您的帳戶會受 AWS Control Tower 組織的 AWS CloudTrail 追蹤所管理。如果您在該帳戶中已有 CloudTrail 追蹤的現有部署，除非您在 AWS Control Tower 中註冊帳戶之前刪除該帳戶的現有追蹤，否則可能會看到重複費用。

> **Note**
>
> 當您更新至登陸區域 3.0 版時，AWS Control Tower 會代表您刪除已註冊帳戶中的帳戶層級追蹤 (AWS Control Tower 已建立的追蹤）。您現有的帳戶層級日誌檔案會保留在其 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，只有在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。任何寫入許可都必須符合`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 值設定為您的組織 ID。此條件可確保 CloudTrail 只能代表您組織內的帳戶將日誌寫入 S3 儲存貯體；可防止組織外的 CloudTrail 日誌寫入 AWS Control Tower S3 儲存貯體。

此政策不會影響您現有工作負載的功能。此政策會顯示在下列範例中。

```
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
```

如需此條件索引鍵的詳細資訊，請參閱 IAM 文件和名為「使用可擴展性控制來存取 資源 AWS 的服務」的 IAM 部落格文章。

用於監控的整合式工具

監控是維護 AWS Control Tower 及其他 AWS 解決方案可靠性、可用性和效能的重要部分。 AWS 提供下列監控工具來監看 AWS Control Tower、在發生錯誤時回報，以及適時採取自動動作：

- Amazon CloudWatch AWS 會即時監控您的 AWS 資源和您在 上執行的應用程式。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，您可以讓 CloudWatch 追蹤 CPU 使用量或其他 Amazon EC2 執行個體指標，並在需要時自動啟動新的執行個體。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南。

- Amazon CloudWatch Events 提供近乎即時的系統事件串流，描述 AWS 資源的變更。CloudWatch Events 啟用自動的事件驅動運算，因為您可以在這些事件發生時，編寫監看特定事件與在其他 AWS 服務內觸發自動化動作的規則。如需詳細資訊，請參閱 Amazon CloudWatch Events 使用者指南。
- Amazon CloudWatch Logs 可讓您監控、存放和存取來自 Amazon EC2 執行個體、CloudTrail 及其他來源的日誌檔案。CloudWatch Logs 可監控日誌檔案中的資訊，並在達到特定閾值時通知您。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 Logs 使用者指南。
- AWS CloudTrail 會擷取由 AWS 您的帳戶發出或代表發出的 API 呼叫和相關事件，並將日誌檔案交付至您指定的 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 地址，以及呼叫的時間。

秘訣：您可以透過 CloudWatch Logs 和 CloudWatch Logs Insights 檢視和查詢帳戶上的 CloudTrail 活動。 CloudWatch 此活動包含 AWS Control Tower 生命週期事件。CloudWatch Logs 的功能可讓您執行比平常使用 CloudTrail 更精細且精確的查詢。

如需詳細資訊，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 已與 整合 AWS CloudTrail，此服務提供由使用者、角色或 AWS Control Tower 中的 AWS 服務所採取之動作的記錄。CloudTrail 會將 AWS Control Tower 的動作擷取為事件。如果您建立線索，則可以將 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 AWS Control Tower 的事件。

即使您未設定追蹤，依然可以透過 CloudTrail 主控台中的事件歷史記錄檢視最新事件。您可以使用 CloudTrail 所收集的資訊，判斷對 AWS Control Tower 提出的請求、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，包括如何設定及啟用，請參閱《AWS CloudTrail 使用者指南》。

CloudTrail 中的 AWS Control Tower 資訊

當您建立 AWS 帳戶時，會在您的帳戶上啟用 CloudTrail。當 AWS Control Tower 中發生支援的事件活動時，該活動會與事件歷史記錄中的其他 AWS 服務事件一起記錄在 CloudTrail 事件中。您可以在 AWS 帳戶中檢視、搜尋和下載最近的事件。如需詳細資訊，請參閱《使用 CloudTrail 事件歷史記錄檢視事件》https://docs.aws.amazon.com/awscloudtrail/latest/userguide/view-cloudtrail-events.html。

> **Note**
>
> 在登陸區域 3.0 版之前的 AWS Control Tower 版本中，AWS Control Tower 建立了成員帳戶追蹤。當您更新至 3.0 版時，您的 CloudTrail 追蹤會更新為組織追蹤。如需在線索之間移動時的最佳實務，請參閱 CloudTrail 使用者指南中的建立組織線索。

建議：建立線索

若要持續記錄您 AWS 帳戶中的事件，包括 AWS Control Tower 的事件，請建立追蹤。線索能讓 CloudTrail 將日誌檔案交付至 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。線索會記錄 AWS 分割區中所有區域的事件，並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析和處理 CloudTrail 日誌中所收集的事件資料。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- 準備建立線索
- 管理 CloudTrail 成本
- CloudTrail 支援的服務和整合
- 設定 CloudTrail 的 Amazon SNS 通知
- 從多個區域接收 CloudTrail 日誌檔案，以及從多個帳戶接收 CloudTrail 日誌檔案

AWS Control Tower 會將下列動作記錄為 CloudTrail 日誌檔案中的事件：

公APIs

- 如需 AWS Control Tower 公有 APIs 的完整清單和每個 API 的詳細資訊，請參閱 AWS Control Tower API 參考。會記錄對這些公有 APIs呼叫 AWS CloudTrail。

其他 API

- `SetupLandingZone`
- `UpdateAccountFactoryConfig`
- `ManageOrganizationalUnit`
- `CreateManagedAccount`

- GetLandingZoneStatus
- GetHomeRegion
- ListManagedAccounts
- DescribeManagedAccount
- DescribeAccountFactoryConfig
- DescribeGuardrailForTarget
- DescribeManagedOrganizationalUnit
- ListEnabledGuardrails
- ListGuardrailViolations
- ListGuardrails
- ListGuardrailsForTarget
- ListManagedAccountsForGuardrail
- ListManagedAccountsForParent
- ListManagedOrganizationalUnits
- ListManagedOrganizationalUnitsForGuardrail
- GetGuardrailComplianceStatus
- DescribeGuardrail
- ListDirectoryGroups
- DescribeSingleSignOn
- DescribeCoreService
- GetAvailableUpdates

每一筆事件或日誌專案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：

- 是否使用根或 AWS Identity and Access Management (IAM) 使用者登入資料提出請求。
- 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。
- 請求是否因存取遭拒或處理成功而遭到拒絕。

如需詳細資訊，請參閱 CloudTrail userIdentity 元素。

範例：AWS Control Tower 日誌檔案項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一或多個日誌專案。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時間、請求參數等資訊。CloudTrail 事件不會以任何特定順序出現在日誌檔案中。

下列範例顯示 CloudTrail 日誌項目，其中顯示 SetupLandingZone AWS Control Tower 事件的典型日誌檔案項目結構，包括啟動動作之使用者的身分記錄。

```
{
  "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"
}
```

使用 監控資源變更 AWS Config

AWS Control Tower 會在所有註冊帳戶 AWS Config 上啟用 ，以便透過偵測控制、記錄資源變更，以及將資源變更日誌交付至日誌封存帳戶，來監控合規性。

如果您的登陸區域版本早於 3.0：對於已註冊的帳戶， 會針對帳戶運作的所有區域 AWS Config 記錄資源的所有變更。每個變更都會建模為組態項目 (CI)，其中包含資源識別符、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相關。

如果您的登陸區域版本是 3.0 或更新版本：AWS Control Tower 只會將 IAM 使用者、群組、角色和客戶受管政策等全球資源的記錄限制在您所在區域。全域資源變更的副本不會儲存在每個區域中。此資源記錄限制符合 AWS Config 最佳實務。全球資源的完整清單可在 AWS Config 文件中取得。

- 若要進一步了解 AWS Config，請參閱 如何 AWS Config 運作。
- 如需 AWS Config 可支援的資源清單，請參閱支援的資源類型。
- 若要了解如何在 AWS Control Tower 環境中自訂資源追蹤，請參閱名為在 AWS Control Tower 中自訂 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，它會記錄 AWS Config 日誌封存帳戶中 記錄的所有變更，這些變更會存放在 Amazon Simple Storage Service 儲存貯體中的資料夾。

在 AWS Control Tower 中管理 AWS Config 成本

本節說明 如何 AWS Config 記錄 AWS Control Tower 帳戶中資源的變更，並向您收費。當您使用 AWS Control Tower 時 AWS Config，此資訊可協助您了解如何管理相關的成本。AWS Control Tower 無需額外費用。

> **Note**
>
> 如果您的登陸區域版本為 3.0 或更新版本：AWS Control Tower 只會將 IAM 使用者、群組、角色和客戶受管政策等全球資源 AWS Config 的記錄限制在您所在區域。因此，本節中的部分資訊可能不適用於您的登陸區域。

AWS Config 旨在將帳戶運作的每個區域中每個資源的變更記錄為組態項目 (CI)。 會針對其產生的每個組態項目向您 AWS Config 收費。

如何 AWS Config 運作

AWS Config 會分別記錄每個區域中的資源。有些全域資源，例如 IAM 角色，每個區域都會記錄一次。例如，如果您在五個區域中運作的註冊帳戶中建立新的 IAM 角色，則 AWS Config 會產生五個 CIs，每個區域一個。其他全域資源，例如 Route 53 託管區域，在所有區域中只會記錄一次。例如，如果您在已註冊帳戶中建立新的 Route 53 託管區域， AWS Config 無論為該帳戶選取多少區域， 都會產生一個 CI。如需可協助您區分這些資源類型的清單，請參閱 系統會多次記錄相同的資源。

> **Note**
>
> 當 AWS Control Tower 使用 時 AWS Config，區域可能由 AWS Control Tower 管理，或不受管理，如果帳戶在該區域中操作，則 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。如果在另一個資源的描述 API 呼叫中傳回資源，這些資源會記錄為直接關係。當您變更與其他資源直接關係中的資源時， AWS Config 不會為這兩個資源建立 CI。

例如，如果您建立 Amazon EC2 執行個體，且 API 要求您建立網路介面， AWS Config 請考慮讓 Amazon EC2 執行個體與網路介面有直接關係。因此， 只會 AWS Config 產生一個 CI。

AWS Config 會針對屬於間接關係的資源關係記錄個別變更。例如，如果您建立安全群組並新增屬於安全群組的相關聯 Amazon EC2 執行個體， AWS Config 會產生兩個 CIs。

如需直接和間接關係的詳細資訊，請參閱什麼是與資源相關的直接和間接關係？

您可以在 AWS Config 文件中找到資源關係的清單。

檢視已註冊帳戶的 AWS Config 記錄器資料

AWS Config 已與 CloudWatch 整合，因此您可以在儀表板中檢視 AWS Config CIs。如需詳細資訊，請參閱名為 的部落格文章AWS Config 支援 Amazon CloudWatch 指標。

若要以程式設計方式檢視 AWS Config 資料，您可以使用 AWS CLI，也可以使用其他 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 來擷取資源的最新變更清單。

資源歷史記錄命令：

- `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 Quick 視覺化 AWS Config 資料

您可以視覺化和查詢 AWS Config 整個組織中由 記錄的資源。如需詳細資訊，請參閱 Config Resource Compliance Dashboard 和使用 Amazon Athena 和 Quick 視覺化 AWS Config 資料。

在 AWS Control Tower AWS Config 中進行故障診斷

本節提供使用 AWS Config 搭配 AWS Control Tower 時可能遇到的一些問題的相關資訊。

高 AWS Config 成本

如果您的工作流程包含經常建立、更新或刪除資源的程序，或是處理大量資源，該工作流程可能會產生大量 CIs。如果您在非生產帳戶中執行這些程序，請考慮取消註冊帳戶。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 就無法針對該帳戶中的資源強制執行偵測性控制或日誌帳戶事件，例如 AWS Config 活動。

如需詳細資訊，請參閱取消管理已註冊的帳戶。若要了解如何停用 AWS Config 記錄器，請參閱管理組態記錄器。

系統會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， AWS Config 可以記錄操作中每個區域的特定全域資源一次。 AWS Config 例如，如果 AWS Config 在八個區域啟用 ，則會記錄每個角色八次。

下列資源會針對 AWS Config 運作中的每個區域記錄一次：

- `AWS::IAM::Group`
- `AWS::IAM::Policy`
- `AWS::IAM::Role`
- `AWS::IAM::User`

其他全域資源只會記錄一次。以下是記錄一次的資源範例：

- `AWS::Route53::HostedZone`
- `AWS::Route53::HealthCheck`
- `AWS::ECR::PublicRepository`
- `AWS::GlobalAccelerator::Listener`
- `AWS::GlobalAccelerator::EndpointGroup`
- `AWS::GlobalAccelerator::Accelerator`

AWS Config 未記錄資源

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 常見問答集中找到已棄用間接關係的清單。

AWS Control Tower 中的生命週期事件

AWS Control Tower 記錄的某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特定 AWS Control Tower 動作是否完成。生命週期事件適用於 AWS Control Tower 建立或管理的資源，例如與組織單位 (OU) 或帳戶相關的登陸區域、基準或控制。

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。如需詳細資訊，請參閱 AWS CloudTrail 使用者指南。
- 每個生命週期事件也會交付給 Amazon EventBridge 和 Amazon CloudWatch Events 服務。注意：若要在 EventBridge 中接收生命週期事件，您必須具有啟用記錄的作用中 AWS CloudTrail 線索。如需透過 傳遞 AWS 之服務事件的詳細資訊 AWS CloudTrail，請參閱《Amazon EventBridge 使用者指南》中的透過 AWS CloudTrail 傳遞的 AWS 服務事件。

AWS Control Tower 中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完成 AWS Control Tower 動作，因此您可以建立 Amazon EventBridge 規則或 Amazon CloudWatch Events 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 依賴多個 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，顯示何時啟動 AWS Control Tower 動作，另一個時間戳記則顯示生命週期事件何時完成、標記成功或失敗。

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。

如需如何將 AWS Control Tower 生命週期事件整合至工作流程的詳細資訊，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。

CreateManagedAccount 和 UpdateManagedAccount 生命週期事件的預期行為

當您在 AWS Control Tower 中建立帳戶或註冊帳戶時，這兩個動作會呼叫相同的內部 API。如果程序期間發生錯誤，通常是在建立帳戶但未完全佈建之後發生。當您在錯誤後重試建立帳戶，或嘗試更新佈建產品時，AWS Control Tower 會看到帳戶已存在。

由於帳戶存在，AWS Control Tower 會記錄`UpdateManagedAccount`生命週期事件，而不是重試請求結束時的`CreateManagedAccount`生命週期事件。您可能因為錯誤而預期會看到另一個`CreateManagedAccount`事件。不過，`UpdateManagedAccount`生命週期事件是預期和所需的行為。

如果您打算使用自動化方法在 AWS Control Tower 中建立或註冊帳戶，請編寫 Lambda 函數的程式來尋找 UpdateManagedAccount 生命週期事件以及 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會與原始 AWS Control Tower 動作相對應，AWS CloudTrail 也會加以記錄。因此，例如，AWS Control Tower `CreateManagedAccount` CloudTrail 事件所產生的生命週期事件名為 `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 Events 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`：日誌會記錄 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`：日誌會記錄 AWS Control Tower 是否成功完成每個動作，以更新與您之前使用帳戶工廠建立的帳戶相關聯的佈建產品。
- `EnableGuardrail`：日誌會記錄 AWS Control Tower 是否成功完成每個動作，以在 OU 上啟用控制項。
- `DisableGuardrail`：日誌會記錄 AWS Control Tower 是否成功完成每個動作，以停用 OU 上的控制項。
- `SetupLandingZone`：日誌會記錄 AWS Control Tower 是否成功完成設定登陸區域的每個動作。
- `UpdateLandingZone`：日誌會記錄 AWS Control Tower 是否成功完成每個動作，以更新現有的登陸區域。

- RegisterOrganizationalUnit：日誌會記錄 AWS Control Tower 是否成功完成每個動作，以在 OU 上啟用其控管功能。
- DeregisterOrganizationalUnit：日誌會記錄 AWS Control Tower 是否成功完成每個動作，以停用 OU 上的控管功能。
- PrecheckOrganizationalUnit：日誌會記錄 AWS Control Tower 是否偵測到任何會阻止擴展控管操作成功完成的資源。
- EnableBaseline：日誌會記錄 AWS Control Tower 是否成功完成每個動作，以啟用 OU 下目標成員帳戶的新基準。您可以使用 EnableBaseline API 或 主控台啟動啟用操作。
- ResetEnabledBaseline：日誌會記錄 AWS Control Tower 是否成功完成每個動作，以重設 OU 下目標成員帳戶上已啟用的現有基準。您可以使用 ResetEnabledBaseline API 或 主控台啟動重設操作。
- UpdateEnabledBaseline：日誌會記錄 AWS Control Tower 是否成功完成每個動作，以更新 OU 下目標成員帳戶上已啟用的現有基準。您可以使用 UpdateEnabledBaseline API 或 主控台啟動更新操作。
- DisableBaseline：日誌會記錄 AWS Control Tower 是否成功完成每個動作，以停用 OU 下目標成員帳戶上已啟用的現有基準。停用操作可以使用 DisableBaseline API 或 主控台啟動。

以下各節提供 AWS Control Tower 生命週期事件清單，其中包含針對每種生命週期事件類型記錄的詳細資訊範例。

CreateManagedAccount

此生命週期事件會記錄 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

此生命週期事件會記錄 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":"XXXXXXXXXXXX"
                    },
                "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

此生命週期事件會記錄 AWS Control Tower 是否成功在由 AWS Control Tower 管理的 OU 上啟用控制項。此事件對應於 AWS Control Tower `EnableGuardrail` CloudTrail 事件。生命週期事件日誌包含控制項`guardrailBehavior`的 `guardrailId`和 ，以及啟用控制項之 OU `organizationalUnitId` 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",                                  // 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

此生命週期事件會記錄 AWS Control Tower 是否成功停用由 AWS Control Tower 管理之 OU 上的控制項。此事件對應於 AWS Control Tower `DisableGuardrail` CloudTrail 事件。生命週期事件日誌包含控制項`guardrailBehavior`的 `guardrailId`和 ，以及停用控制項之 OU `organizationalUnitId` 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": "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

此生命週期事件會記錄 AWS Control Tower 是否成功設定登陸區域。此事件對應於 AWS Control Tower SetupLandingZone CloudTrail 事件。生命週期事件日誌包含 rootOrganizationalId，這是 AWS Control Tower 從管理帳戶建立之組織的 ID。日誌項目也包含organizationalUnitId每個 OUs的 organizationalUnitName和 ，以及每個帳戶accountId在 AWS Control Tower 設定登陸區域時建立的 accountName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": "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

此生命週期事件會記錄 AWS Control Tower 是否成功更新您現有的登陸區域。此事件對應於 AWS Control Tower UpdateLandingZone CloudTrail 事件。生命週期事件日誌包含 `rootOrganizationalId`，這是由 AWS Control Tower 管理的（已更新）組織的 ID。當 AWS Control Tower 最初設定登陸區域時，日誌項目也包含`organizationalUnitName`和`organizationalUnitId`每個 OUs的 和 ，以及`accountId`每個帳戶先前建立的 `accountName`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

此生命週期事件會記錄 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含 AWS Control Tower `organizationalUnitId` 在其控管下提供的 OU 的 `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

此生命週期事件會記錄 AWS Control Tower 是否成功停用 OU 上的控管功能。此事件對應於 AWS Control Tower `DeregisterOrganizationalUnit` CloudTrail 事件。生命週期事件日誌包含 AWS Control Tower 已停用其控管功能的 `organizationalUnitId` 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

此生命週期事件會記錄 AWS Control Tower 是否在 OU 上成功執行預先檢查。此事件對應於 AWS Control Tower `PrecheckOrganizationalUnit` CloudTrail 事件。生命週期事件日誌包含 `Id`、`Name`和 `failedPrechecks`值的欄位，適用於 AWS Control Tower 在 OU 註冊程序期間執行預先檢查的每個資源。

事件日誌也包含執行預先檢查之巢狀帳戶的相關資訊，包括 `accountName`、 `accountId`和 `failedPrechecks` 欄位。

如果`failedPrechecks`值為空，表示該資源的所有預先檢查都已成功傳遞。

- 只有在發生預先檢查失敗時，才會發出此事件。

- 如果您要註冊空的 OU，則不會發出此事件。

事件範例：

```
{
  "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"
}
```

EnableBaseline

此生命週期事件會記錄 AWS Control Tower 是否成功啟用 OU 下目標成員帳戶的基準。此事件對應至 AWS Control Tower `RegisterOrganizationalUnit`或 `EnableBaseline` CloudTrail 事件。生命週期事件日誌包含已啟用的基準及其版本、已啟用基準`targetIdentifier`的 、父 OU 上已啟用基準`parentIdentifier`的 ，以及`statusSummary`顯示 SUCCEEDED 或 FAILED 狀態的 ，以及操作的其他參數和時間戳記。

```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "accountId": "XXXXXXXXXXXX",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2025-02-10T17:14:57Z",
```

```
    "eventSource": "controltower.amazonaws.com",
    "eventName": "EnableBaseline",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "366911a2-4fa6-4e4a-ac2b-280f627e0027",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "XXXXXXXXXXXX",
    "serviceEventDetails": {
        "enableBaselineStatus": {
            "enabledBaselineDetails": {
                "arn": "arn:aws:controltower:us-east-2:XXXXXXXXXXXX:enabledbaseline/
XXXXXXXXXXXXXXXX",
                "parentIdentifier": "arn:aws:controltower:us-
east-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXX",
                "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/o-
ern76xmzvf/XXXXXXXXXXXX",
                "baselineIdentifier": "arn:aws:controltower:us-east-2::baseline/
XXXXXXXXXXXXXXX",
                "baselineVersion": "4.0",
                "statusSummary": {
                    "lastOperationIdentifier": "37f5eb68-e5b9-4c70-ae76-4ca15f6b16de",
                    "status": "SUCCEEDED"
                },
                "parameters": [
                    {
                        "key": "IdentityCenterEnabledBaselineArn",
                        "value": {
                            "untyped": {
                                "object": "arn:aws:controltower:us-
east-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXX"                          }
                        }
                    }
                ]
            },
            "requestedTimestamp": "2025-02-10T17:07:09+0000",
            "completedTimestamp": "2025-02-10T17:14:57+0000"
        }
    },
    "eventCategory": "Management"
```

```
}
```

ResetEnabledBaseline

此生命週期事件會記錄 AWS Control Tower 是否成功重設 OU 下目標成員帳戶上已啟用的現有基準。此事件對應至 AWS Control Tower RegisterOrganizationalUnit或 ResetEnabledBaseline CloudTrail 事件。生命週期事件日誌包含已啟用的基準及其版本、已啟用基準targetIdentifier的 、父 OU 上已啟用基準parentIdentifier的 ，以及statusSummary顯示 SUCCEEDED 或 FAILED 狀態的 ，以及操作的其他參數和時間戳記。

```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "accountId": "XXXXXXXXXXXX",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2025-02-10T21:17:55Z",
    "eventSource": "controltower.amazonaws.com",
    "eventName": "ResetEnabledBaseline",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "c01a32e1-13ab-4b46-8f1b-00699ef6f989",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "XXXXXXXXXXXX",
    "serviceEventDetails": {
        "resetEnabledBaselineStatus": {
            "enabledBaselineDetails": {
                "arn": "arn:aws:controltower:us-west-2:XXXXXXXXXXXX:enabledbaseline/
XXXXXXXXXXXXXXXX",
                "parentIdentifier": "arn:aws:controltower:us-
west-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXX",
                "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/
o-0uh2kplf6d/XXXXXXXXXXXX",
                "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/
XXXXXXXXXXXXXXX",
                "baselineVersion": "1.0",
                "statusSummary": {
```

```
                    "lastOperationIdentifier": "3e364c89-89fa-42b8-9776-9f7cc47ba1fa",
                    "status": "SUCCEEDED"
                },
                "parameters": []
            },
            "requestedTimestamp": "2025-02-10T21:14:24Z",
            "completedTimestamp": "2025-02-10T21:17:54+0000"
        }
    },
    "eventCategory": "Management"
}
```

UpdateEnabledBaseline

此生命週期事件會記錄 AWS Control Tower 是否成功更新 OU 下目標成員帳戶上已啟用的現有基準。此事件對應至 AWS Control Tower RegisterOrganizationalUnit或 UpdateEnabledBaseline CloudTrail 事件。生命週期事件日誌包含已啟用的基準及其版本、已啟用基準targetIdentifier的 、父 OU 上已啟用基準parentIdentifier的 ，以及statusSummary顯示 SUCCEEDED 或 FAILED 狀態的 ，以及操作的其他參數和時間戳記。

```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "accountId": "XXXXXXXXXXXX",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2025-02-10T19:45:28Z",
    "eventSource": "controltower.amazonaws.com",
    "eventName": "UpdateEnabledBaseline",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "514f2aff-1a99-4912-bda1-0d4d6662c96e",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "XXXXXXXXXXXX",
    "serviceEventDetails": {
        "updateEnabledBaselineStatus": {
            "enabledBaselineDetails": {
```

```
                "arn": "arn:aws:controltower:us-east-2:XXXXXXXXXXXX:enabledbaseline/
XXXXXXXXXXXXXXXX",
                "parentIdentifier": "arn:aws:controltower:us-
east-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXX",
                "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/o-
ern76xmzvf/XXXXXXXXXXXX",
                "baselineIdentifier": "arn:aws:controltower:us-east-2::baseline/
XXXXXXXXXXXXXXX",
                "baselineVersion": "4.0",
                "statusSummary": {
                    "lastOperationIdentifier": "ba3de28f-83fb-4c9a-8a8c-a4e15fac2c41",
                    "status": "SUCCEEDED"
                },
                "parameters": [
                    {
                        "key": "IdentityCenterEnabledBaselineArn",
                        "value": {
                            "untyped": {
                                "object": "arn:aws:controltower:us-
east-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXX"                          }
                        }
                    }
                ]
            },
            "requestedTimestamp": "2025-02-10T19:39:35+0000",
            "completedTimestamp": "2025-02-10T19:45:28+0000"
        }
    },
    "eventCategory": "Management"
}
```


DisableBaseline

此生命週期事件會記錄 AWS Control Tower 是否成功停用 OU 下目標成員帳戶上已啟用的現有基準。此事件對應於 AWS Control Tower `DisableBaseline` CloudTrail 事件。生命週期事件日誌包含已啟用的基準及其版本、已啟用基準`targetIdentifier`的 、在父 OU 上啟用`parentIdentifier`基準的 ，以及`statusSummary`顯示 SUCCEEDED 或 FAILED 狀態的 ，以及操作的其他參數和時間戳記。


```
{
    "eventVersion": "1.11",
    "userIdentity": {
```

```
        "accountId": "XXXXXXXXXXXX",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2025-03-14T00:50:58Z",
    "eventSource": "controltower.amazonaws.com",
    "eventName": "DisableBaseline",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "704794c4-a32e-4960-8386-c7efaa5a22a1",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "XXXXXXXXXXXX",
    "serviceEventDetails": {
        "disableBaselineStatus": {
            "enabledBaselineDetails": {
                "arn": "arn:aws:controltower:us-west-2:XXXXXXXXXXXX:enabledbaseline/
XXXXXXXXXXXXXXXX",
                "parentIdentifier": "arn:aws:controltower:us-
west-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXX",
                "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/
o-0uh2kplf6d/XXXXXXXXXXXX",
                "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/
XXXXXXXXXXXXXXX",
                "baselineVersion": "1.0",
                "statusSummary": {
                    "lastOperationIdentifier": "7b895594-0edb-48bc-9f3d-d88c2ad618df",
                    "status": "SUCCEEDED"
                },
                "parameters": []
            },
            "baselineDetails": {
                "arn": "arn:aws:controltower:us-west-2:XXXXXXXXXXXX:enabledbaseline/
XXXXXXXXXXXXXXXX",
                "parentIdentifier": "arn:aws:controltower:us-
west-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXX",
                "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/
o-0uh2kplf6d/XXXXXXXXXXXX",
                "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/
XXXXXXXXXXXXXXX",
                "baselineVersion": "1.0",
```

```
                "statusSummary": {
                    "lastOperationIdentifier": "7b895594-0edb-48bc-9f3d-d88c2ad618df",
                    "status": "SUCCEEDED"
                },
                "parameters": []
            },
            "requestedTimestamp": "2025-03-14T00:49:13Z",
            "completedTimestamp": "2025-03-14T00:50:58+0000"
        }
    },
    "eventCategory": "Management"
}
```

搭配 使用 AWS 使用者通知 AWS Control Tower

您可以使用AWS 使用者通知來設定交付管道，以接收事件的 AWS Control Tower 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的通知，包括電子郵件、聊天應用程式中的 Amazon Q Developer 聊天通知，或AWS 主控台行動應用程式推送通知。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量。通知也會顯示在主控台通知中心。

透過 AWS 使用者通知而非 EventBridge 訂閱通知的優點包括：

- 友善的使用者介面 (UI)。
- 與 AWS 主控台整合，位於全域導覽列的鈴鐺/通知區域。
- 原生支援電子郵件通知，不需要設定 Amazon SNS。
- 最值得注意的是，支援行動推播通知， AWS 使用者通知獨有。

例如，在 Security Hub CSPM 嚴重和高嚴重性問題清單的情況下，您可能希望收到的通知類型之一。JSON 中用來設定通知訂閱的程式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 AWS 使用者通知主控台上提供的篩選條件，依服務和名稱篩選事件。
- 如果您從 JSON 程式碼建立自己的 EventBridge 篩選條件，您可以依特定屬性篩選事件。

範例 AWS Control Tower 事件

以下是 的廣義範例事件 AWS Control Tower。

- 這是 EventBridge 事件。
- 您可以使用 AWS 使用者通知訂閱 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
        }
    }
}
```

AWS 備份和 AWS Control Tower

AWS Backup 是一項服務，可讓您建立自動備份 AWS 資源的計劃。若要設定 AWS Control Tower 資源的備份，您必須遵循四個主要步驟：

1. AWS Backup 為您的登陸區域啟用 。您可以在 AWS Control Tower 主控台的登陸區域設定頁面上執行此操作。當您開啟 時 AWS Backup，資源會在多個帳戶中建立。如需詳細資訊，請參閱為 建立的資源 AWS Backup。
2. 在 AWS Backup 主控台中選擇加入 AWS Control Tower 的備份。如需詳細資訊，請參閱《 AWS Backup 開發人員指南》中的使用支援的服務。
3. 在您想要包含的個別 OUs AWS Backup 上啟用 。在登陸區域層級啟用 AWS Backup 之後，您可以在 主控台的 OU 詳細資訊頁面上執行此任務。當您 AWS Backup 在 OU 上啟用 時，該 OU 中的帳戶會收到本機保存 AWS Backup 庫。
4. 標記要包含在備份中的所選資源。標籤表示該資源的備份頻率。您的備份計畫遵循每個資源上資源標籤指定的排程。

如需詳細資訊，請參閱 AWS Backup 開發人員指南。當您設定 AWS Backup with AWS Control Tower 時，不會產生任何費用。您將從中產生成本 AWS Backup。如需定價的詳細資訊，請參閱 AWS Backup 定價。

如需 AWS Control Tower 在您的 AWS Control Tower 登陸區域中建立 AWS Backup 之資源的詳細資訊，請參閱 為 建立的資源 AWS Backup

> **Note**
>
> AWS Control Tower 不支援透過 AWS Backup 服務直接設定 AWS Control Tower 資源的備份計劃，如果沒有也在 AWS Control Tower 服務中啟用它。

先決條件

您必須先有現有的 AWS Organizations 組織，才能 AWS Backup 設定 AWS Control Tower 資源。如果您已經設定 AWS Control Tower 登陸區域，做為現有的組織。

您必須配置或建立未在 AWS Control Tower 中註冊的兩個其他 AWS 帳戶。這些帳戶會成為中央備份帳戶和備份管理員帳戶。使用這些名稱命名這些帳戶。

此外，您必須選取或建立多區域 AWS Key Management Service (KMS) AWS 金鑰，特別是備份。

定義您的先決條件

- 中央備份帳戶 — 中央備份帳戶會存放您的 AWS Control Tower 備份文件庫和備份。此保存庫建立在此帳戶內 AWS 區域 AWS Control Tower 管理的所有 中。跨帳戶複本會存放在此帳戶中，以防帳戶遭到入侵且需要資料還原。
- 備份管理員帳戶 - 備份管理員帳戶是 AWS Control Tower 中 AWS Backup 服務的委派管理員帳戶。它存放 Backup Audit Manager (BAM) 報告計劃。此帳戶會彙總所有備份監控資料，例如還原任務和複製任務。資料會存放在 Amazon S3 儲存貯體中。如需詳細資訊，請參閱《 AWS Backup 開發人員指南》中的使用 AWS Backup 主控台建立報告計劃。
- 多區域 AWS KMS 金鑰的政策需求

  您的 AWS KMS 金鑰需要金鑰政策。請考慮類似此政策的金鑰政策，這會限制具有與組織管理帳戶相關聯許可的委託人（使用者和角色）存取：

  JSON

```
{
    "Version":"2012-10-17",
    "Id": "KMS key policy",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow use of the KMS key for organization",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Action": [
                "kms:Decrypt",
                "kms:DescribeKey",
                "kms:GenerateDataKey*",
                "kms:Encrypt",
```

```
                "kms:ReEncrypt*",
                "kms:GetKeyPolicy",
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "ORGANIZATION-ID"
                }
            }
        }
    ]
}
```

此範例政策可讓組織中的所有帳戶存取其加密的備份資料。使用AWS 全域條件索引鍵和AWS KMS 條件索引鍵來精簡許可，取決於哪些委託人需要存取您的備份。

> **Note**
>
> 您的多區域 AWS KMS 金鑰必須針對 AWS 區域 您計劃使用 AWS Control Tower 管理的每個進行複寫。

啟用備份

您可以在登陸區域設定期間或更新登陸區域時，為在 AWS Control Tower 中註冊的帳戶中的資源啟用備份。

身為 先決條件，您必須提供下列項目

- AWS 帳戶 做為 AWS Backup 管理員帳戶的
- AWS 帳戶 做為 AWS Backup 中央備份帳戶的
- 您為跨帳戶備份管理的多區域 AWS KMS 金鑰

如何啟用備份

啟用程序有兩個主要部分：首先，為您的登陸區域啟用備份；然後，為需要備份的每個已註冊 OU 啟用備份。

第一部分：為您的登陸區域設定備份

主控台：您可以在 AWS Control Tower 主控台的登陸區域設定頁面上設定登陸區域的備份。您會在初始登陸區域設定操作期間看到此選項，稍後可以透過更新登陸區域來重新檢視。

API：如果您已經有 AWS Control Tower 登陸區域，您可以呼叫 `UpdateLandingZone` API 來啟用 AWS Control Tower APIs 的備份，或者如果您是第一次設定 AWS Control Tower，則可以啟用 `CreateLandingZone` API。（提示：在此之後，請呼叫 `EnableBaseline` API 來為您需要的每個 OU 建立備份。）

AWS Control Tower 主控台外部

為您的登陸區域啟用備份的一部分包括 AWS Control Tower 主控台以外的步驟。您必須導覽至 AWS Backup 主控台，才能檢閱您的 資源。

檢閱您的選擇加入資源類型或選擇加入其他資源類型

1. 在 開啟 AWS Backup 主控台https://console.aws.amazon.com/backup。
2. 在導覽窗格中，選擇設定。
3. 在 Service opt-in (選擇加入服務) 頁面上，選擇 Configure resources (設定資源)。
4. 使用切換開關來啟用或停用您要包含的服務 AWS Backup。請確定已選取您要備份的資源，例如 RDS、EC2、DDB 等，無論它們是否屬於您的 AWS Control Tower 環境。

如需詳細資訊，請參閱選擇使用 管理服務 AWS Backup。

> **新資源類型的考量事項**
>
> 在依賴 AWS Backup 來管理任何 AWS 服務資源的資料保護之前，您必須執行先前的程序並選擇加入 AWS Backup 該服務。此外，當 AWS Backup 服務在未來新增對其他服務及其資源類型的支援時，您必須先重複此程序，並使用 選擇加入每個額外的資源類型， AWS Backup 才能在 AWS Control Tower 中備份該資源類型。標記不支援的資源類型可能會導致備份失敗。

當您啟用登陸區域的備份時，AWS Control Tower 會分別建立您提供的兩個帳戶，做為中央備份帳戶和備份管理員帳戶。AWS Control Tower 會在這些帳戶和其他帳戶中建立資源。

> **Important**
>
> 若要啟用 AWS Control Tower Audit 和 Log Archive 帳戶的備份，您必須呼叫 `EnableBaseline` API 來設定安全 OU 的備份。建議您這樣做。

建議的計劃和保留庫如下所示：

- 每小時備份 = 在本機保存庫中保留 2 週，中央備份保存庫中沒有副本
- 每日備份 = 在本機文件庫中保留 2 週，在中央備份文件庫中保留 1 個月
- 每週備份 = 在本機保存庫中保留 1 個月，在中央保存庫中保留 3 個月
- 每月備份 = 在本機保存庫中保留 3 個月，在中央備份保存庫中保留 3 個月

如需如何建立備份計劃的資訊，請參閱使用 AWS Backup 主控台建立報告計劃。

下一部分：在 OUs 上啟用備份

在登陸區域設定 AWS Backup 中啟用 之後，您必須採取額外的步驟，以對您要備份的特定 OUs 啟用備份。如果您已 AWS Backup 為登陸區域啟用 ，您會在 主控台的 OU 詳細資訊頁面上看到 區段，可讓您選擇啟用 OU 的備份。如果未在登陸區域層級啟用備份，您將無法在 OU 詳細資訊頁面上看到本節。

若要在 OU `BackupBaseline`上啟用 ，該 OU 必須`AWSControlTowerBaseline`已啟用 。每個 OU 中的註冊帳戶都`AWSControlTowerBaseline`已啟用 。

在您選取的帳戶和 OUs 中，AWS Control Tower 會設定其他資源

- 本機備份保存庫

  AWS Control Tower 會在您的帳戶中建立本機備份保存庫，並將四種可能的備份計畫類型連接到保存庫。透過 AWS Control Tower 建立的備份計劃會以字首標記。

  ```
  BackupPlanTags:
          aws-control-tower: 'managed-by-control-tower'
  ```

- 四種類型的備份計畫：每小時、每日、每週、每月。

  每個計劃都與標籤型資源指派相關聯。例如，任何以 aws-control-tower-backuphourly 標記的資源：true 會受到每小時備份計劃的保護。

- 帳戶中的本機備份角色

  AWS Control Tower 會建立用於備份的 IAM 角色。此角色需要四個特定許可。

  ```
  "backup:UpdateGlobalSettings","organizations:RegisterDelegatedAdministrator","organizations:E
  ```

  該角色與 的服務主體具有信任關係 AWS Backup 。該角色名為 `aws-controltower-backup-role`，並具有與其連接的下列受管許可：

  - AWSBackupServiceRolePolicyForBackup
  - AWSBackupServiceRolePolicyForRestores
  - AWSBackupServiceRolePolicyForS3Backup
  - AWSBackupServiceRolePolicyForS3Restore

標記資源以進行備份

在 AWS Control Tower 中設定備份程序的一部分是標記您要包含在備份計畫中的資源。這些標籤會指定備份的頻率。這些是可能的標籤。

- `aws-control-tower-backuphourly : true`
- `aws-control-tower-backupdaily: true`
- `aws-control-tower-backupweekly: true`
- `aws-control-tower-backupmonthly: true`

考量

- 當 在 OU 上 AWS Backup 處於作用中狀態時，您會在 AWS Control Tower 主控台的 OU 詳細資訊頁面上的狀態欄位中看到已啟用的值。狀態欄位的一些其他可能值包括未啟用、進行中和失敗。如果您看到失敗狀態，請選擇重新註冊 OU，將您的 AWS Backup 組態重新套用至 OU。
- 如果您已在 OU 上 AWS Backup 啟用 ，則透過帳戶工廠佈建的新帳戶會包含在 OU 下 AWS Backup。

關閉備份

您可以在登陸區域設定期間或更新登陸區域時，關閉在 AWS Control Tower 註冊帳戶中資源的備份。

關閉備份需要兩個主要步驟：首先，關閉每個已啟用備份之 OU 的 AWS Backup 基準，然後關閉登陸區域的備份。

第一步：關閉 OUs 上的備份

如果 AWS Backup 已啟用 ，您必須先停用所有 OUs的 AWS Backup 基準，才能 AWS Backup 關閉登陸區域的 。

若要停用 OU 的 AWS Backup 基準，您可以呼叫 `DisableBaseline` API。巢狀 OUs 會繼承此狀態，因此也會為其停用 AWS Backup 基準。

範例命令：

```
aws controltower disable-baseline --enabled-baseline-identifier Enabled-baseline-ARN
```

當您停用 AWS Backup 基準時，AWS Control Tower 會清除下列資源：

- 所有與 相關的堆疊集 AWS Backup
- 所有與 相關的控制項 AWS Backup

> **Note**
>
> 即使刪除堆疊集，也會保留本機保存庫，因為本機保存庫上的保留政策設定為 `Retain`。它會保留您的資料。

下一步： AWS Backup 關閉您的登陸區域

透過關閉 OUs備份來滿足先決條件後，若要從 AWS Control Tower 主控台關閉備份，請導覽至登陸區域設定頁面。選擇停用備份。

當您關閉時 AWS Backup，AWS Control Tower 會變更下列資源：

- 移除所有與 相關的堆疊集 AWS Backup
- 在安全 OU AWS Backup 中停用與 相關的所有控制項
- 取消註冊委派管理員帳戶以進行 AWS Backup 管理
- 從管理員和中央備份帳戶移除 AWS Control Tower 控管 AWS Backup （適用於 CloudTrail AWS Config等）

- AWS Control Tower AWS Backup 會保留保存庫和包含資料的 Amazon S3 儲存貯體資源

停用備份之後，不會建立新的備份，但不會移除現有的備份。

在移動的帳戶上啟用備份

如果您將帳戶移至 AWS Backup 已啟用 的 AWS Control Tower OU，且帳戶未註冊 AWS Control Tower，則您的備份計劃不會自動套用至帳戶。

主控台：若要從 AWS Control Tower 主控台 AWS Backup 為個別帳戶啟用 ，您可以在帳戶詳細資訊頁面上選擇更新帳戶，或在 OU 詳細資訊頁面上選擇重新註冊 OU，以同時更新多個帳戶。

API：從 API，如果您將帳戶移至已啟用備份基準的 OU，您可以呼叫該 OU 上的 `ResetEnabledBaseline` API，將 OU `EnabledBaseline` 的資源指定為目標，以透過從 OU 繼承來觸發帳戶上的備份。

範例命令：

```
aws controltower reset-enabled-baseline --enabled-baseline-identifier
 arn:aws:controltower:REGION:NAMESPACE:enabledbaseline/XOSDORW8HDB5ZNWEE --region us-
east-1
```

回應範例：

```
{
        "operationIdentifier": "0bbdb587-c849-4152-95c6-7afa7664ee71"
}
```

AWS Control Tower 中的備份漂移

AWS Control Tower 中的 AWS Backup 組態不會報告偏離。如需 AWS Control Tower 中漂移的詳細資訊，請參閱偵測和解決 AWS Control Tower 中的漂移。

如果您刪除或修改 AWS Backup 計劃，您的計劃可能會進入偏離狀態。以下是要避免的一些修改。

- 請勿從安全 OU 移動 Backup Administrator 帳戶。
- 請勿從安全 OU 移動中央備份帳戶。
- 請勿從組織中移除 Backup Administrator 帳戶。
- 請勿從組織中移除中央備份帳戶。

- 請勿分離、連接或更新套用至安全 OU 的 AWS Backup SCP。
- 請勿分離、連接或更新套用至其他 OUs AWS Backup SCP。
- 請勿移除 Backup Administrator 帳戶的 許可 AWS Backup。
- 請勿更新您的跨帳戶備份設定，以關閉跨帳戶備份。如需跨帳戶備份的詳細資訊，請參閱《 AWS Backup API 參考`UpdateGlobalSettings`》中的 。
- 請勿刪除您的 AWS KMS 金鑰。
- 請勿在設定 AWS KMS 金鑰政策後對其進行修改。
- 請勿停用服務的受信任存取 AWS Backup。

> **Note**
>
> 系統會針對保護 AWS Control Tower 中 AWS Backup 資源的 SCP 型控制項狀態報告偏離。

為 建立的資源 AWS Backup

此頁面上的資料表會顯示啟用時在 AWS Control Tower 帳戶中建立的資源 AWS Backup。

下表顯示當您 AWS Backup 為登陸區域組織啟用 時，AWS Control Tower 在 AWS Control Tower Central Backup 帳戶中建立的資源。

Description	中央備份帳戶的資源
哪個 OU 包含帳戶？	安全 OU
哪些動作建立了 資源？	登陸區域建立或更新
會建立哪些資源？	中央備份保存庫 —`aws-controltower-central-backupvault-*`
包含哪些區域？	所有受管區域
與這些資源相關的控制項有哪些？	`CT.BACKUP.PV.3`

下表顯示當您 AWS Backup 為登陸區域組織啟用 時，AWS Control Tower 在 AWS Control Tower Backup Administrator 帳戶中建立的資源。

Description	備份管理員帳戶的資源：這是 的委派管理員帳戶 AWS Backup
哪個 OU 包含帳戶？	安全 OU
哪些動作建立了資源？	登陸區域建立或更新
會建立哪些資源？	備份稽核管理員 (BAM) • aws_controltower_copy_report • aws_controltower_backup_report • aws_controltower_restore_report 用於存放 BAM 日誌的 Amazon S3 儲存貯體—aws-controltower-backup-reports- *{accountId}* -* Amazon S3 存取記錄儲存貯體 —aws-controltower-backup-reports-log- *{accountId}* -*
包含哪些區域？	主要區域
與這些資源相關的控制項有哪些？	• CT.BACKUP.PV.2 • CT.S3.PV.1 • CT.S3.PV.1

下表顯示當您 AWS Backup 為安全 OU 啟用 時，AWS Control Tower 在 AWS Control Tower 稽核帳戶和 AWS Control Tower Log Archive 帳戶中建立的資源。

Description	稽核和日誌封存帳戶的資源
哪個 OU 包含帳戶？	安全 OU
哪些動作建立了 資源？	啟用 BackupBaseline

Description	稽核和日誌封存帳戶的資源

會建立哪些資源？	• 本機備份保存庫 `-aws-controltower-local-backupvault-*`
	• 本機備份角色 —`aws-controltower-BackupRole`
	• 四個本機備份計劃（每小時、每週、每月、每日）
	  • `aws-controltower-hourly-backup-plan`
	  • `aws-controltower-daily-backup-plan`
	  • `aws-controltower-weekly-backup-plan`
	  • `aws-controltower-monthly-backup-plan`
	• IAM 角色 —`aws-controltower-BackupRole`

包含哪些區域？	所有受管區域
與這些資源相關的控制項有哪些？	• `CT.BACKUP.PV.3` • `CT.IAM.PV.1` • `CT.BACKUP.PV.3` • `CT.BACKUP.PV.1`

> **Note**
>
> 當您將 `BackupBaseline` 套用至安全 OU 時，該 OU 中的所有成員帳戶都會接收 AWS Backup 資源，而不只是 Audit and Log Archive 帳戶。

下表顯示當您 AWS Backup 在目標 OU 上啟用 時，AWS Control Tower 在 AWS Control Tower OU 成員帳戶中建立的資源。

Description	其他 OUs 中成員帳戶的資源
哪個 OU 包含帳戶？	安全 OU 以外的任何 OU
哪些動作建立了 資源？	啟用 BackupBaseline

會建立哪些資源？	• 本機備份保存庫 -aws-controltower-local-backupvault-*
	• 本機備份角色 —aws-controltower-BackupRole
	• 四個本機備份計劃 （每小時、每週、每月、每日）
	  • aws-controltower-hourly-backup-plan
	  • aws-controltower-daily-backup-plan
	  • aws-controltower-weekly-backup-plan
	  • aws-controltower-monthly-backup-plan
	• IAM 角色 —aws-controltower-BackupRole

包含哪些區域？	所有受管區域
與這些資源相關的控制項有哪些？	• CT.BACKUP.PV.3 • CT.IAM.PV.1 • CT.BACKUP.PV.3 • CT.BACKUP.PV.1

AWS 備份的控制項

當您 AWS Backup 在 AWS Control Tower 登陸區域中啟用 時，某些預防性控制會在您的環境中啟用。這些控制項會保護使用 AWS Control Tower 操作 AWS Backup 所需的資源。如果您的登陸區域 AWS Backup 未啟用 ，則您無法啟用這些控制項。

如需詳細資訊，請參閱 的控制項 AWS Backup。

停用 AWS Control Tower 登陸區域

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。清除 AWS Control Tower 配置的所有資源的程序稱為解除委任登陸區域。

如果您不想再使用 AWS Control Tower，自動除役工具會清除 AWS Control Tower 配置的資源。若要開始自動解除委任程序，請導覽至登陸區域設定頁面，選取解除委任索引標籤，然後選擇解除委任登陸區域。

如需停用期間執行的動作清單，請參閱 停用程序概觀。

> **Warning**
>
> 手動刪除所有 AWS Control Tower 資源與停用不同。它不允許您設定新的登陸區域。

停用程序 AWS Organizations 不會以下列方式變更您的資料和現有資料。

- 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。
- 停用程序完成後，會保留一些資源成品，例如 Amazon S3 儲存貯體和 Amazon CloudWatch Logs 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。AWS Control Tower 採取的除役動作和除役後剩餘的成品會在下列各節中說明。

> **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。

停用程序概觀

當您請求解除委任登陸區域時，AWS Control Tower 會執行下列動作。

- 停用登陸區域中啟用的每個偵測控制。AWS Control Tower 會刪除支援控制項 CloudFormation 的資源。
- 從中移除服務控制政策 SCPs)，以停用每個預防性控制 AWS Organizations。如果政策是空的 （應該是在移除 AWS Control Tower 管理的所有 SCPs 之後），AWS Control Tower 會分離並完全刪除政策。
- 刪除所有部署為 CloudFormation StackSets 的藍圖。
- 刪除所有區域中部署為 CloudFormation 堆疊的所有藍圖。
- 對於每個佈建帳戶，AWS Control Tower 會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。
  - 透過移除 AWS Control Tower 建立的 IAM 角色 （除非已新增其他政策） 來撤銷帳戶的 AWS Control Tower 許可，並重新建立標準 IAM `OrganizationsFullAccessRole` 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 （稽核和日誌存檔） 帳戶的藍圖。
- 透過移除 AWS Control Tower 建立的 IAM 角色 （除非已新增其他政策） 並重新建立 IAM 角色，從共用帳戶撤銷 AWS Control Tower `OrganizationsFullAccessRole` 許可。
- 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。

如何解除委任登陸區域

若要從主控台解除委任您的 AWS Control Tower 登陸區域，請遵循此處提供的程序。

> **Note**
>
> 建議您在停用之前取消管理已註冊的帳戶。

1. 導覽至 AWS Control Tower 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. 如果您確認要解除委任登陸區域的意圖，則在解除委任進行時，系統會將您重新導向至 AWS Control Tower 首頁。此程序最多可能需要兩個小時。
5. 當停用成功時，您必須先手動刪除剩餘的資源，才能從 AWS Control Tower 主控台設定新的登陸區域。這些剩餘的資源包括一些特定的 Amazon S3 儲存貯體、組織和 CloudWatch Logs 日誌群組。

> **Note**
>
> 這些動作可能會對您的帳單和合規活動造成重大影響。例如，無法刪除這些資源可能會導致意外費用。

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. 如果您想要在新區域中設定新的登陸區域 AWS ，請遵循此額外步驟。透過 CLI 輸入下列命令：

```
aws organizations disable-aws-service-access --service-principal
 controltower.amazonaws.com
```

使用 APIs 停用您的登陸區域

清除所有登陸區域資源的程序稱為解除委任登陸區域。

> **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。

如需解除委任登陸區域的詳細資訊，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 停用 AWS Control Tower 登陸區域。

若要解除委任登陸區域，請呼叫 `DeleteLandingZone` API。此 API 會傳回 `OperationIdentifier`，然後您可以在呼叫 `GetLandingZoneOperation` API 時用來檢查刪除操作的狀態。

```
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"
}
```

解除委任後所需的手動清除任務

本節列出在初始停用步驟之後，您必須執行的手動清除任務。

- 如果您在停用日誌封存和稽核帳戶之後建立新的登陸區域，或遵循自備現有日誌封存或稽核帳戶的程序，您必須為日誌封存和稽核帳戶指定不同的電子郵件地址。
- 您必須先手動刪除 CloudWatch Logs 日誌群組 `aws-controltower/CloudTrailLogs`，才能設定另一個登陸區域。
- 必須手動移除或重新命名具有日誌預留名稱的兩個 Amazon S3 儲存貯體。
- 您必須手動刪除或重新命名現有的安全和沙盒組織單位。

> **Note**
>
> 您必須先刪除記錄和稽核帳戶，而不是管理帳戶，才能刪除 AWS Control Tower Security OU 組織。若要刪除這些帳戶，您必須以根使用者身分登入的時機稽核帳戶和日誌帳戶，並個別刪除它們。

- 您可能想要手動刪除 AWS Control Tower 的 AWS IAM Identity Center (IAM Identity Center) 組態，但您可以繼續現有的 IAM Identity Center 組態。
- 您可能想要移除 AWS Control Tower 建立的 VPC，並移除相關聯的 AWS CloudFormation 堆疊集。
- 您必須先遵循這些額外步驟，才能在新區域中設定新的登陸 AWS 區域。
  - 透過 CLI 輸入下列命令：

```
aws organizations disable-aws-service-access --service-principal
 controltower.amazonaws.com
```

  - 從所有受管區域的`AWSControlTowerManagedRule`共用和成員帳戶刪除剩餘的受管規則，稱為 。 `AWSControlTowerManagedRule` 是 Amazon EventBridge 規則。

解除委任期間未移除的資源

解除委任登陸區域並不會完全反轉 AWS Control Tower 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 AWS Organizations 組織的客戶，AWS Control Tower 會設定具有一或多個組織單位 (OUs的組織。指定的安全 OU 和選用建立的沙盒 OU。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 (OUs) 不會移除。
- 安全與沙盒 OUs不會移除。
- 組織不會從中刪除 AWS Organizations。
- AWS Organizations （ 共用、佈建或管理 ） 中的任何帳戶都不會移動或移除。

AWS IAM Identity Center (SSO)

對於沒有現有 IAM Identity Center 目錄的客戶，AWS Control Tower 會設定 IAM Identity Center 並設定初始目錄。當您停用登陸區域時，AWS Control Tower 不會對 IAM Identity Center 進行任何變更。如有需要，您可以手動刪除存放在管理帳戶中的 IAM Identity Center 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。
- AWS Control Tower 設定建立的群組不會移除。
- AWS Control Tower 建立的許可集不會移除。
- AWS 帳戶與 IAM Identity Center 許可集之間的關聯不會移除。
- IAM Identity Center 目錄不會變更。
- AWS Control Tower 的這些 IAM Identity Center 政策不會移除：
  - `AWSControlTowerAdminPolicy`
  - `AWSControlTowerCloudTrailRolePolicy`
  - `AWSControlTowerStackSetRolePolicy`

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 APIs 設定登陸區域，則會要求您建立這些角色。當您停用登陸區域時，不會移除下列角色：

- `AWSControlTowerAdmin`
- `AWSControlTowerCloudTrailRole`
- `AWSControlTowerStackSetRole`
- `AWSControlTowerConfigAggregatorRoleForOrganizations`

> **Note**
>
> 刪除登陸區域時，無論是 AWS Control Tower 代表您建立角色，還是手動建立角色，`AWSControlTowerExecution`成員帳戶中的角色都會遭到刪除。不過，如果您已將其他政策附加至此角色，或修改附加至此角色的政策，AWS Control Tower 可能無法在刪除登陸區域期間刪除此角色。在這種情況下，登陸區域刪除會成功，但角色會保留在您的成員帳戶中。

Amazon S3 儲存貯體

在設定期間，AWS Control Tower 會在 AWS CloudTrail 的日誌封存帳戶中建立儲存貯體，並在 AWS Config 整合的組態中央彙總器帳戶中建立儲存貯體。AWS Control Tower 會建立用於記錄和記錄每個帳戶中存取的儲存貯體。當您解除委任登陸區域時，不會移除下列資源：

- 不會移除日誌封存帳戶中的日誌和記錄存取 S3 儲存貯體。
- 不會移除組態中央彙整工具帳戶中的記錄和記錄存取 S3 儲存貯體。
- 不會移除每個帳戶中記錄和記錄存取儲存貯體的內容。

服務整合帳戶

AWS Control Tower 要求每個服務整合組態都有一個中央帳戶。此帳戶不一定會在根據登陸區域版本的 AWS Control Tower 設定期間建立。當您解除委任登陸區域時：

- 在 AWS Control Tower 設定期間建立的服務整合帳戶不會關閉。
- IAM `OrganizationAccountAccessRole` 角色會重新建立以符合標準 AWS Organizations 組態。
- 會移除 `AWSControlTowerExecution` 角色。

佈建的帳戶

AWS Control Tower 客戶可以使用帳戶工廠來建立新 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。
- 中的佈建產品 AWS Service Catalog 不會移除。如果您透過終止這些帳戶來清除這些帳戶，其帳戶會移至根 OU。
- 不會移除 AWS Control Tower 建立的 VPC，也不會移除相關聯的 AWS CloudFormation 堆疊集 (`BP_ACCOUNT_FACTORY_VPC`)。
- IAM `OrganizationAccountAccessRole` 角色會重新建立以符合標準 AWS Organizations 組態。
- 會移除 `AWSControlTowerExecution` 角色。

CloudWatch Logs 日誌群組

- CloudWatch Logs 日誌群組 `aws-controltower/CloudTrailLogs`會建立為名為 的藍圖的一部分`AWSControlTowerBP-BASELINE-CLOUDTRAIL-MASTER`。不會移除此日誌群組。而是刪除藍圖並保留資源。

> **Note**
>
> 登陸區域 3.0 和更新版本的客戶不需要刪除其個別註冊帳戶的 CloudTrail 日誌和 CloudTrail 日誌角色，因為這些角色僅在管理帳戶中針對組織層級追蹤建立。
> 從登陸區域 3.2 版開始，AWS Control Tower 會建立稱為 的 Amazon EventBridge 規則`AWSControlTowerManagedRule`。此規則會針對所有受管區域，在每個成員帳戶中建立。解除委任期間不會自動刪除規則，因此您必須先從服務整合帳戶和所有受管區域的成員帳戶手動刪除規則，才能在新區域中設定登陸區域。

有關如何刪除 AWS Control Tower 資源的程序，請參閱 移除 AWS Control Tower 資源。

移除 AWS Control Tower 資源

本文件提供如何個別移除 AWS Control Tower 資源的指示，做為定期維護和管理任務的一部分。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。這與停用您的登陸區域不同。

兩種類型的任務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。
- 清除自動停用後剩餘的資源。

> **Warning**
>
> 手動移除資源將不允許您設定新的登陸區域。這與停用不同。如果您想要停用 AWS Control Tower 登陸區域，請在採取本章所述的任何動作停用 AWS Control Tower 登陸區域之前遵循上的指示。本章中的指示可協助您清除自動除役完成後剩餘的資源。即使您手動刪除所有登陸區域資源，它與解除委任登陸區域不同，而且可能會產生非預期的費用。

如果您需要從 AWS Control Tower 移除帳戶，請參閱下列各節以關閉帳戶：

- 取消管理 帳戶
- 關閉在 Account Factory 中建立的帳戶

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，或者需要主要重新部署組織資源，建議您取消委任最初設定登陸區域時建立的資源。

- 停用程序完成後，會保留一些資源成品，例如 Amazon S3 儲存貯體和 Amazon CloudWatch Logs 日誌群組。
- 您必須先手動清除帳戶中的剩餘資源，才能設定另一個登陸區域，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**
>
> 強烈建議您只有在想要停止使用登陸區域時，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手動移除 AWS Control Tower 資源。當您需要從登陸區域刪除特定資源時，可以遵循這些程序。

在執行這些程序之前，除非另有說明，否則您必須登入您登陸區域的 AWS 管理主控台 主區域中的 ，而且您必須以 IAM 使用者或 IAM Identity Center 中的使用者身分登入，並具有包含您登陸區域的管理帳戶的管理許可。

> **Warning**
>
> 這些是破壞性動作，可將控管偏離引入您的 AWS Control Tower 設定。這些動作無法復原。

主題

- 刪除 SCP
- 刪除 StackSet 和堆疊。
- 刪除日誌存檔帳戶中的 Amazon S3 儲存貯體

- 移除帳戶工廠產品組合和產品
- 移除 AWS Control Tower 角色和政策
- AWS Control Tower 資源說明

刪除 SCP

AWS Control Tower 使用服務控制政策 SCPs) 進行控制。此程序會逐步解說如何刪除與 AWS Control Tower 特別相關的 SCPs。

刪除 AWS Organizations SCPs

1. 在 https：//https://console.aws.amazon.com/organizations/ 開啟 Organizations 主控台。
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 StackSet 和堆疊。

AWS Control Tower 使用 StackSets 和堆疊來部署與登陸區域中控制項 AWS Config 規則 相關的 。以下程序會帶您演練如何刪除這些特定資源。

刪除 CloudFormation StackSets

1. 在 https：//https://console.aws.amazon.com/cloudformation 開啟 CloudFormation 主控台。
2. 從左側導覽選單選擇 StackSets。
3. 針對每個具備 AWSControlTower 前綴的 StackSet，執行以下作業。若 StackSet 中有許多帳戶，這可能會需要一些時間。
   a. 從儀表板中的表格選擇特定 StackSet。這會開啟該 StackSet 的屬性頁面。
   b. 在頁面底部，在 Stacks 資料表中，記錄資料表中所有帳戶的帳戶 AWS IDs。複製所有帳戶的清單。
   c. 在動作中，選擇從 StackSet 刪除堆疊。
   d. 在設定部署選項中，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 AWS 的帳戶 IDs，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 properties (StackSet 屬性) 頁面上，您可以為其他 StackSet 再度啟動此程序。

4. 當不同 StackSets StackSets 資料表中的記錄為空白時，程序即完成。
5. 當 Stacks (堆疊) 資料表中的記錄為空白時，請選擇 Delete StackSet (刪除 StackSet)。

刪除 CloudFormation 堆疊

1. 在 https：//https://console.aws.amazon.com/cloudformation 開啟 CloudFormation 主控台。
2. 從 Stacks (堆疊) 儀表板，搜尋所有具備 AWSControlTower 前綴的堆疊。
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

下列程序引導您如何以 AWSControlTowerExecution 群組中的 IAM Identity Center 使用者身分登入日誌封存帳戶，然後刪除日誌封存帳戶中的 Amazon S3 儲存貯體。

使用正確許可登入您的日誌存檔帳戶

1. 在 https：//https://console.aws.amazon.com/organizations/ 開啟 Organizations 主控台。
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. 針對 Role (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 儲存貯體

1. 開啟位於 https://console.aws.amazon.com/s3/ 的 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)。

移除帳戶工廠產品組合和產品

下列程序會引導您如何以 AWSServiceCatalogAdmins 群組中的 IAM Identity Center 使用者身分登入，然後清除您的 Account Factory 產品組合和產品。

使用適當的許可登入您的管理帳戶

1. 前往您位於 *directory-id*.awsapps.com/start 的使用者入口網站 URL。
2. 在 AWS 帳戶中，尋找 管理帳戶。
3. 從 AWSServiceCatalogAdminFullAccess 中，選擇管理主控台以此角色 AWS 管理主控台 身分登入 。

清除帳戶工廠

1. 在 https：//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. 在本機產品組合表格中，搜尋名為 AWS Control Tower 帳戶工廠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. 展開頁面的限制區段，然後使用產品名稱 AWS Control Tower Account Factory 選擇限制條件的選項按鈕。
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 之產品的選項按鈕。
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. 在本機產品組合表格中，搜尋名為 AWS Control Tower 帳戶工廠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 AWS Control 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

這些程序會逐步解說如何清除 AWS Control Tower 在設定登陸區域時或之後建立的角色和政策。

刪除 IAM Identity Center AWSServiceCatalogEndUserAccess 角色

1. 在 https：//https://console.aws.amazon.com/singlesignon/ 開啟 AWS IAM Identity Center 主控台。
2. 將您的 AWS 區域變更為主區域，這是您最初設定 AWS Control Tower 的區域。
3. 從左側導覽功能表中，選擇AWS 帳戶。
4. 選擇您的管理帳戶連結。
5. 選擇 Permission sets (許可集) 的下拉式選單、選取 AWSServiceCatalogEndUserAccess，然後選擇 Remove (移除)。

6. 從左側面板選擇AWS 帳戶。
7. 開啟 Permission sets (許可集) 標籤。
8. 選取 AWSServiceCatalogEndUserAccess，然後將其刪除。

刪除 IAM 角色

1. 前往 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
2. 從左側導覽選單選擇 Roles (角色)。
3. 從表格搜尋名為 AWSControlTower 的角色。
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)。

刪除 IAM 政策

1. 前往 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
2. 從左側導覽選單選擇 Policies (政策)。
3. 從表格搜尋名為 AWSControlTower 的政策。
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 資源時遇到任何無法解決的問題，請聯絡 AWS Support。

解除委任登陸區域後的設定

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。請確定已從管理帳戶移除這些 IAM 角色和 IAM 政策：
  - 角色：
    - `AWSControlTowerAdmin`
    - `AWSControlTowerCloudTrailRole`
    - `AWSControlTowerStackSetRole`
  - 政策：
    - `AWSControlTowerAdminPolicy`
    - `AWSControlTowerCloudTrailRolePolicy`
    - `AWSControlTowerStackSetRolePolicy`
- 在再次設定登陸區域之前，您可能想要刪除或更新 AWS Control Tower 的現有 IAM Identity Center 組態，但不需要將其刪除。
- 您可能想要移除 AWS Control Tower 建立的 VPC。
- 如果為記錄或稽核帳戶指定的電子郵件地址與現有 AWS 帳戶相關聯，則設定會失敗。您可以關閉 AWS 帳戶，或使用不同的電子郵件地址再次設定登陸區域。或者，您可以重複使用這些現有的共用帳戶，搭配可讓您使用自己的記錄和稽核帳戶的功能。如需詳細資訊，請參閱引進現有安全或記錄帳戶的考量事項。
- 如果記錄帳戶中已存在具有下列預留名稱的 Amazon S3 儲存貯體，則設定失敗：
  - `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 CloudWatch Logs 中有現有的日誌群組 `aws-controltower/CloudTrailLogs`，則設定會失敗。您必須重新命名或移除日誌群組。

在新的 中設定 之前 AWS 區域

如果您想要在新區域中設定新的登陸區域 AWS ，請遵循這些額外步驟。

- 透過 CLI 輸入下列命令：

```
aws organizations disable-aws-service-access --service-principal
 controltower.amazonaws.com
```

- 從所有受管區域的共用和成員帳戶刪除剩餘的受管規則AWSControlTowerManagedRule，稱為 。

> **Note**
>
> 您無法在名為 Security 或 Sandbox 的頂層 OUs組織中設定新的登陸區域。您必須重新命名或移除這些 OU，才能再次設定登陸區域。

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 AWS 環境。為了減輕管理登陸區域的負擔， AWS 建立了稱為 AWS Control Tower 的受管服務。

ALZ 沒有排程其他功能；它僅處於長期支援狀態。因此，我們建議您從 ALZ 移至 AWS Control Tower 服務。本章中連結的部落格會逐步解說該移動的不同考量，並說明如何規劃從 ALZ 成功遷移至 AWS Control Tower。

部落格：將 AWS 登陸區域解決方案遷移至 AWS Control Tower

AWS 方案指引提供更廣泛的文件，包括從 ALZ 轉換至 AWS Control Tower 的步驟。基本上，您將根據多項先決條件，在執行 ALZ 的現有組織中啟用 AWS Control Tower 控管。如需詳細資訊，請參閱從 AWS 登陸區域轉換至 AWS Control Tower。

逐步解說：設定沒有 VPC 的 AWS Control Tower

本主題會逐步解說如何在不使用 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。
- 您可以變更您的 Account Factory 設定，以便在沒有相關聯 VPC 的情況下建立新的 AWS Control Tower 帳戶。

> **Important**
>
> 如果您在啟用 VPC 網際網路存取設定的情況下佈建 Account Factory 帳戶，則該 Account Factory 設定會覆寫控制項 不允許客戶管理之 Amazon VPC 執行個體的網際網路存取。若要避免啟用新佈建帳戶的網際網路存取，您必須在 Account Factory 中變更 設定。

刪除 AWS Control Tower VPC

在 AWS Control Tower 之外，每個 AWS 客戶都有預設 VPC，您可以在 Amazon Virtual Private Cloud (Amazon VPC) 主控台上檢視，網址為 https：//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 登陸區域時，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。本主題將新的 VPC 稱為 Control Tower VPC。

當您在 Amazon VPC 主控台中檢視 AWS Control Tower VPC 時，名稱結尾不會看到單字 （預設）。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，但如果稍後需要 AWS Control Tower 中的 VPC，則必須自行建立。

刪除 AWS Control Tower VPC

1. 在 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. 依其 CIDR 範圍識別 AWS Control Tower VPC。
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中已存在 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相關聯的 AWS 預設 VPC。因此，為了保護管理帳戶，請移除每個區域的預設 VPC，以及移除您 AWS Control Tower 主區域中 Control Tower 建立的 VPC。

選擇性地清除帳戶中的 VPC 資源

或者，若要從現有帳戶清除 AWS Control Tower VPC 資源 `aws-controltower-VPC`，您可以在確認 VPC 中沒有現有資源或資源相依性之後`AWSControlTowerBP-VPC-ACCOUNT-FACTORY-V1`，從 AWS CloudFormation StackSet 中移除堆疊執行個體。

在 AWS Control Tower 中建立沒有 VPC 的帳戶

如果您的最終使用者工作負載不需要 VPCs，您可以使用此方法來設定沒有自動為其建立 VPCs的最終使用者帳戶。

從 AWS Control Tower 儀表板，您可以檢視和編輯網路組態設定。在您變更設定，讓 AWS Control Tower 帳戶在沒有相關聯的 VPC 的情況下建立之後，所有新帳戶都會在沒有 VPC 的情況下建立，直到您再次變更設定為止。

設定 Account Factory 以建立沒有 VPCs的帳戶

1. 開啟 Web 瀏覽器，然後導覽至位於 https：//https://console.aws.amazon.com/controltower 的 AWS Control Tower 主控台。
2. 從左側的選單中選擇 Account Factory。
3. 然後，您會看到帳戶工廠頁面與網路組態區段。
4. 如果您之後想要還原目前的設定，請記下目前的設定。
5. 選擇網路組態區段中的編輯按鈕。
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 – 移除子網路

      - 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，當您刪除 AWS Control Tower VPC 或重新設定 Account Factory 來建立沒有 VPCs的帳戶時，可能會發生這些錯誤。

- 您現有的管理帳戶在 AWS Control Tower VPC 中可能有相依性或資源，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 在 AWS Control Tower 中設定安全群組 AWS Firewall Manager

此影片說明如何使用 AWS Firewall Manager 服務來改善 AWS Control Tower 的網路安全。您可以指定已啟用的安全管理員帳戶來設定安全群組。您將了解如何為 AWS Control Tower 組織設定安全政策並強制執行安全規則，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 ） 有效的安全群組。

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 設定安全群組

此影片 (8：02) 說明如何為 AWS Control Tower 中的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，請參閱如何設定 AWS WAF 的文件。

疑難排解

如果您在使用 AWS Control Tower 時遇到問題，您可以根據我們的最佳實務使用下列資訊來解決這些問題。如果您遇到的問題超出下列資訊的範圍，或在您嘗試解決這些問題後仍持續存在，請聯絡 AWS Support。

主題

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。
- CloudFormation StackSet 失敗。

確認電子郵件訊息：如果您的管理帳戶少於一小時，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 AWS Support。

失敗的 StackSets：登陸區域的另一個可能原因是 CloudFormation StackSet 失敗。必須在 AWS Control Tower 管理的所有區域的管理帳戶中啟用 AWS 安全字符服務 (STS) AWS 區域，以便佈建成功；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 AWS 的安全字符服務 (STS) 端點區域。

修復失敗的堆疊集，然後重試設定

1. 在適當的 中導覽至 CloudFormation 主控台 AWS 區域。
2. 使用名稱 AWSControlTowerBP-BASELINE-CLOUDTRAIL-MASTER 清除失敗的堆疊。
3. 等待堆疊刪除完成。
4. 返回 AWS Control Tower 頁面。
5. 再次選取設定登陸區域。

若要檢視 AWS 區域 AWS Control Tower 支援的清單，請參閱 AWS 區域如何使用 AWS Control Tower。

登陸區域更新失敗，出現 KMS 錯誤

登陸區域更新失敗的最常見原因是無效的 AWS KMS 金鑰政策。

非有效 KMS 金鑰政策的常見原因：

- 政策中的 Typo。
- 忘記新增必要的政策陳述式。
- AWS 分割區不正確。
- 政策中的帳戶號碼不正確。
- 忘記移除範例政策中的預留位置。

採取動作

檢閱您的政策以檢查這些錯誤。

如需 AWS KMS 金鑰政策的詳細資訊，請參閱設定 KMS 金鑰和備份先決條件。

無法更新登陸區域

如果更新失敗，AWS Control Tower 不會轉返至先前的登陸區域版本。您可能會發現您的登陸區域處於不確定狀態。若是如此，請聯絡 AWS 支援。

登陸區域更新可能會失敗，原因有幾個。

- 不符合先決條件
- AWS Config 資源存在於特定帳戶中
- 存在已關閉的帳戶

不符合先決條件

登陸區域更新必須符合與登陸區域設定相同的先決條件。更新之前，請檢閱啟動前檢查。

AWS Config 安全 OU 帳戶中存在的資源

請勿在稽核和日誌封存帳戶中新增 AWS Config 資源。登陸區域更新程序無法在這些資源存在的情況下完成。這些限制類似於第一次註冊帳戶或設定登陸區域的限制。如需詳細資訊，請參閱註冊具有現有 AWS Config 資源的帳戶。

存在已關閉的帳戶

當帳戶處於關閉或暫停狀態時，當您嘗試更新登陸區域時，可能會遇到問題。您必須先刪除每個已關閉帳戶上的佈建產品，才能對登陸區域執行更新。

在 AWS Service Catalog 佈建產品頁面上，您可能會看到類似以下的錯誤訊息：

```
AWSControlTowerExecution role can't be assumed on the account.
```

常見原因：您已暫停帳戶，但不刪除佈建的產品。

要採取的動作：如果您看到此錯誤，您有兩個選項：

1. 聯絡 AWS Support 並重新開啟帳戶、刪除佈建的產品，然後再次關閉帳戶。
2. 從因為帳戶關閉而遭到孤立的 StackSets 中移除資源。（只有在 StackSets 具有您未移除的目前狀態執行個體時，才能使用此選項。）

若要從 StackSets 移除資源，請為每個已關閉的帳戶執行此操作：

- 針對已關閉的帳戶，前往每個 AWS Control Tower StackSets 並從每個區域移除 StackInstances。
- 重要：選擇保留堆疊選項，讓 StackSet 僅移除堆疊執行個體。StackSet 無法從已關閉的帳戶擔任角色，因此如果嘗試擔任該`AWSControlTowerExecution`角色，將會失敗，這會導致您收到的錯誤訊息。

登陸區域不是最新的錯誤

如果您最近尚未更新登陸區域，當您嘗試重新取得 AWS Control Tower 的存取權時，可能會收到錯誤。您可能會看到類似以下的錯誤訊息：

```
Unable to access Control Tower
```

您的帳戶已閒置太久。由於處於非作用中狀態，您必須更新登陸區域才能存取 AWS Control Tower。

不過，您的登陸區域更新可能會失敗。

要採取的步驟

登入組織的管理帳戶，並以根使用者身分登入。您的 IAM 使用者或 IAM Identity Center 中的使用者必須具有 AWS Control Tower 管理員許可，且屬於 AWSControlTowerAdmins 群組。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，請參閱在 Service Catalog 主控台中使用 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。
- 當其他 AWS Control Tower 組態變更正在進行時，在 Account Factory 中建立新帳戶將會失敗。例如，當程序正在執行將控制項新增至 OU 時，如果您嘗試佈建帳戶，帳戶工廠會顯示錯誤訊息。

檢查 AWS Control Tower 中先前動作的狀態

- 導覽至 AWS CloudFormation > StackSets
- 檢查與 AWS Control Tower 相關的每個堆疊集 （ 字首："AWSControlTower")
- 尋找仍在執行中的 CloudFormation StackSets 操作。

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，且該註冊失敗，當您嘗試第二次時，錯誤訊息可能會通知您堆疊集存在。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。接著，您必須使用 AWS Organizations 主控台手動將帳戶移出 OU 並移回根目錄。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說明。

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 成功更新 AWS Service Catalog。

案例 1：您可能會遇到類似以下的錯誤訊息：

`AWS Control Tower could not baseline VPC in the managed account because of existing resource dependencies.`

常見原因：AWS Control Tower 一律會在初始佈建期間移除 AWS 預設 VPC。若要在帳戶中擁有 AWS 預設 VPC，您必須在帳戶建立後新增它。AWS Control Tower 有自己的預設 VPC 來取代 AWS 預設 VPC，除非您按照演練顯示的方式設定 Account Factory，否則 AWS Control Tower 完全不會佈建 VPC。那麼該帳戶就沒有 VPC。如果您想要使用該 VPC，則必須重新新增 AWS 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。當它處於該狀態時，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**
>
> `Tainted` 狀態會導致後續問題：未更新的 帳戶可能會阻止對其所屬的 OU 啟用控制項。

案例 2：您可能會看到類似以下的錯誤訊息：

`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註冊的 OU 移至另一個，但保留舊 AWS 的 Config 規則。帳戶處於不一致狀態。

要採取的動作：

如果打算移動帳戶：

- 在 Service Catalog 中終止帳戶。
- 再次註冊。
- 內容/影響：部署的 AWS Config 規則與目的地 OU 指定的組態不相符。
- AWS 組態規則可能會從先前的 OU 保留，導致意外支出。
- 由於資源命名衝突，嘗試重新註冊或更新帳戶將會失敗。

如果帳戶意外移動：

- 將帳戶傳回其原始 OU。
- 從 Service Catalog 更新帳戶。

- 在啟動參數中，輸入帳戶原先所在的 OU。
- 內容/影響：如果帳戶未傳回至其原始 OU，其狀態將與其所在新 OU 指定的控制項不一致。
- 更新帳戶不是有效的修補，因為它不會刪除與其先前 OU 相關聯的 AWS Config 規則。

提及的失敗錯誤 AWS Config

如果在 AWS Control Tower 支援的任何 AWS 區域中啟用 AWS Config ，您可能會因為預先檢查失敗而收到錯誤訊息。由於 的一些基礎行為，訊息可能無法充分解釋問題 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，它會建立具有預設命名的組態記錄器和交付管道。如果您透過主控台停用 AWS Config 服務，則不會刪除組態記錄器或交付管道。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 支援的任何區域中啟用 AWS Config 服務，可能會導致此失敗。

如果帳戶有現有的 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說明。

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。停用 AWS Config 不夠，必須透過 CLI 刪除組態記錄器和交付管道。從 CLI 刪除組態記錄器和交付管道之後，您可以再次嘗試啟動 AWS Control Tower 並註冊帳戶。

如果您正在部署佈建產品，您必須在重試之前刪除佈建產品。否則，您可能會看到類似以下的錯誤訊息：

- `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。

以下是一些範例 AWS Config CLI 命令，您可以用來判斷組態記錄器和交付管道的狀態。

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"`

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

- 管理組態記錄器 (AWS 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
```

此錯誤訊息是由 產生 AWS Service Catalog，這是協助在 AWS Control Tower 中佈建帳戶的整合服務。

常見原因：

- 您可能會以根登入。當您以根使用者身分登入時，AWS Control Tower 不支援建立帳戶。

- 您的 IAM Identity Center 使用者尚未新增至適當的許可群組。您可能需要將 IAM Identity Center 使用者新增至下列其中一個許可群組：AWSAccountFactory（適用於最終使用者存取）或 AWSServiceCatalogAdmins（適用於管理員存取）。
- 如果您以 IAM 使用者身分進行身分驗證，則必須將其新增至 AWS Service Catalog 產品組合，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 偏離，且需要偏離修復，也會發生此問題。若要修復大多數類型的偏離，請在登陸區域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特定工作所需的許可 AWS Organizations。如果您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，以確保您的許可不會遭到這些位置拒絕：

```
You have insufficient permissions to perform AWS Organizations API actions.
```

如果您認為您的工作需要您嘗試的動作，但找不到任何相關限制，請聯絡您的系統管理員或 AWS Support。

Detective 控制項未對帳戶生效

如果您最近已將 AWS Control Tower 部署擴展到新的 AWS 區域，新套用的偵測性控制不會對您在任何區域中建立的新帳戶生效，直到更新由 AWS Control Tower 管理OUs 中的個別帳戶為止。現有帳戶的現有偵測性控制仍然有效。

如果您在更新帳戶之前嘗試啟用偵測性控制，您可能會看到類似以下的錯誤訊息：

```
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 主控台更新您的帳戶，請參閱 何時更新 AWS Control Tower OUs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 APIs AWS Service Catalog 和 AWS CLI 來自動更新。如需如何處理更新程序的詳細資訊，請參閱此影片演練。 您可以用 UpdateProvisionedProduct API 取代影片中顯示的 ProvisionProduct API。

如果您在帳戶上啟用偵測性控制時遇到進一步困難，請聯絡 AWS Support。

AWS Organizations API 傳回超出速率的錯誤

可能的原因

在 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 SCPs 是否已漂移。

要遵循的步驟

如果您遇到 API 限流或`rate exceeded`錯誤，請嘗試下列步驟：

- 在不同時間執行工作負載。（請參閱各區域的 AWS Control Tower SCP 變異數掃描排程，以了解 AWS Control Tower 何時執行其稽核掃描。）
- 如果您直接透過 HTTP 呼叫 APIs：使用 AWS SDK，會自動重試失敗的動作
- 透過 Service Quotas 和 AWS Support 請求提高限制

如需 Elastic Beanstalk 中 API 限流的疑難排解指示範例，請參閱： `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 登陸區域移至另一個 AWS Control Tower 登陸區域

> **Warning**
>
> 此實務不符合合格帳戶註冊的先決條件，因為合格帳戶必須屬於相同的整體 AWS 組織，而且每個組織可能只有一個登陸區域。如果您已嘗試執行此動作，且發現自己收到多個錯誤訊息，以下是一些可能有幫助的資訊。

若要將您透過 Account Factory 佈建的帳戶移至另一個 AWS Control Tower 管理的登陸區域，在另一個管理帳戶下，您必須從原始 OU 中移除與該帳戶相關聯的所有 IAM 角色和堆疊。從部署帳戶的每個區域移除這些資源。

> **Note**
>
> 移除資源的最佳方法是先取消佈建原始 OU 中的帳戶，然後再嘗試移動該帳戶。

如果您不移除資源，新 OU 的註冊將會失敗，有些令人驚嘆。您可能會遇到一或多個錯誤訊息，而且會持續收到類似的錯誤訊息，直到從部署帳戶的每個區域中移除剩餘的角色和堆疊為止。

每次收到錯誤訊息時，您必須從新的 OU 中移除帳戶、刪除作為錯誤訊息主旨的舊資源，然後嘗試將帳戶移回新的 OU。必須針對部署帳戶的每個區域，為每個剩餘的資源重複removing-and-deleting此程序，可能為 10 或 20 次。這些重複錯誤是因為帳戶已佈建至具有 SCP 的 OU，以防止 IAM 角色刪除。您可以在重試之前刪除帳戶的所有資源，以縮短復原程序。

以下範例代表如果保留未刪除的角色和堆疊，您可能會收到的失敗訊息類型。每當您嘗試註冊帳戶時，只要舊資源仍然存在，您最有可能一次看到其中一個訊息。

已針對範例修改資源 ID 字串的值。它們的值在您可能收到的錯誤訊息中不會相同。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，類似如下：

```
"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後，您就可以成功邀請、佈建或註冊帳戶到新的 OU。

AWS 支援

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。

基準類型

AWS Control Tower 中的基準是一組資源和特定組態，您可以套用至目標。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 OU 做為目標的基準，將該 OU 註冊到 AWS Control Tower。

在登陸區域設定期間，可能會在共用帳戶上自動啟用某些基準。根據您的登陸區域設定和組態，可能會啟用和更新特定基準。AWS Control Tower 會以基準指定的方式，建立資源並將其部署到目標。

當您在目標上啟用基準時，基準會以稱為 資源的 AWS `EnabledBaseline` 資源表示。

AWS Control Tower 包含兩種一般類型的基準：

- 可以在 OU 上啟用的基準。
- 在登陸區域設定期間，可在共用帳戶上啟用的基準。

在 OU 層級套用的基準類型

> **Note**
>
> 只有適用於 OU 層級的基準可以使用 `EnableBaseline` API 直接啟用。

- 名稱: `AWSControlTowerBaseline`

  描述：此基準會為目標 OU 內的成員帳戶設定資源和控制項，這是合規監控、稽核、安全監控以及選擇性存取管理的必要項目。當您在 AWS Control Tower 中註冊 OU 時，會啟用此基準。

  先決條件：必須在 AWS Control Tower 登陸區域中啟用 AWS Config 整合。

  考量：此基準會保留登陸區域區域拒絕控制的設定。換句話說，如果登陸區域層級不允許某個區域，當您呼叫 `EnableBaseline` API 註冊 OU 時，該 OU 不允許該區域。

  > **Note**
  >
  > OU 層級區域拒絕控制無法允許登陸區域區域拒絕控制不允許的區域。

  如需詳細資訊，請參閱 AWS Organizations 文件中的 SCPs 如何使用拒絕。

建議：建議您確認目標 OU 可能正在執行工作負載的區域，並在呼叫 OU 的 EnableBaseline API 之前，針對登陸區域區域拒絕控制檢查結果，否則您可能會失去對特定區域中資源的存取權。

- 名稱: ConfigBaseline

  描述：此基準會在 Detective 控制項啟用所需的目標 OU 內為成員帳戶設定 AWS Config 相關資源。設定的資源是 AWSControlTowerBaseline 資源的子集。

  先決條件：必須在 AWS Control Tower 登陸區域中啟用 AWS Config 整合。

  考量：此基準不會保留登陸區域區域拒絕控制的設定。在啟用 ConfigBaseline 的過程中，不會啟用區域拒絕控制。

  限制：無法在相同的 OU 上啟用 AWSControlTowerBaseline 和 ConfigBaseline。OU 上只允許其中一個。

- 名稱: BackupBaseline

  描述：此基準會設定目標 OU 內成員帳戶的資源和控制項。這些是必要的，以便與 整合 AWS Backup 可以自動化跨 的資料備份 AWS 服務，並集中備份政策管理。

  先決條件：

  - AWS Backup 整合必須在 AWS Control Tower 登陸區域中啟用。
  - AWS Config 整合必須在 AWS Control Tower 登陸區域中啟用。
  - AWSControlTowerBaseline 必須在目標 OU 上啟用 。

  考量：在目標 OU BackupBaseline上啟用 之前，請確定AWSControlTowerBaseline已在目標 OU 上啟用 。也就是說，目標 OU 必須在 AWS Control Tower 中註冊。

  - 您可以選擇在建立 AWS Control Tower 登陸區域 AWS Backup 的過程中或在登陸區域更新程序中啟用 。
  - 與登陸區域 3.1 版及更新版本BackupBaseline相容。
  - BackupBaseline 不會套用至管理帳戶。

在登陸區域設定期間，可能套用至共用帳戶的基準類型

AWS Control Tower 會在共用帳戶上啟用特定基準，做為登陸區域設定和更新程序的一部分。當您變更登陸區域設定時，登陸區域的基準可能會變更。例如，如果您選擇加入 IAM Identity Center，AWS Control Tower 可以在您的登陸區域啟用最新版本的IdentityCenterBaseline基準。

您可以使用 ListEnabledBaselines API 呼叫來檢視登陸區域的已啟用基準。

> **Note**
>
> 從登陸區域 4.0 版開始，AuditBaseline 會取代為兩個不同的基準：CentralSecurityRolesBaseline和 CentralConfigBaseline。

- 名稱: CentralConfigBaseline

  描述：使用 AWS Config 設定組織中合規監控和稽核的中央資源。
- 名稱: CentralSecurityRolesBaseline

  描述：設定組織中安全監控的中央資源。
- 名稱: AuditBaseline

  描述：設定資源來監控組織中帳戶的安全性和合規性。
- 名稱: LogArchiveBaseline

  描述：為組織中帳戶 API 活動和資源組態的日誌設定中央儲存庫。
- 名稱: IdentityCenterBaseline

  描述：設定 IAM Identity Center 的共用資源，這會準備 AWSControlTowerBaseline 來設定帳戶的 Identity Center 存取權。

  考量：只有在您最初設定登陸區域時已選取 IAM Identity Center 做為身分提供者，或隨後變更登陸區域設定以啟用登陸區域的 IAM Identity Center 時，此基準才有效。如果您使用的是不同的身分提供者，您將無法啟用此基準。
- 名稱: BackupCentralVaultBaseline

  描述：在組織中設定中央 AWS Backup 保存庫。
- 名稱: BackupAdminBaseline

  描述：設定委派的管理員和 AWS Backup Audit Manager。

部分註冊帳戶

當您使用基準時，帳戶可以置於稱為部分註冊的狀態。

如果您透過呼叫 ResetEnabledBaseline API 重新註冊 OU，則可能會發生此狀態，因為 AWS Control Tower 只會將強制性資源套用至目標 OU 中的帳戶。缺少其父 OU 選用資源 （控制項） 的帳戶會標示為已部分註冊。

如果您將未註冊的帳戶移至已註冊的 OU，然後呼叫 OU 上的 ResetEnabledBaseline API 來註冊該帳戶，AWS Control Tower AWSControlTowerBaseline會將與 相關聯的資源套用至新註冊的帳戶。不過，針對此 OU 啟用的選用控制項不會套用至帳戶。帳戶保持部分註冊狀態。

若要完整註冊帳戶，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 的所有資源套用至新註冊的帳戶，包括針對該 OU 啟用的選用控制項。

AWS Control Tower 主控台與基準 APIs 之間的操作變化

當您變更 OU 的控管狀態時，相較於透過基準APIs 變更控管，AWS Control Tower 主控台會自動為您執行更多操作。

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，做為註冊每個帳戶的一部分。當您透過 EnableBaseline API 和 註冊 OU 時AWSControlTowerBaseline，AWS Control Tower 不會為 OU 中的成員帳戶建立佈建產品。
- 取消註冊 OU

  每當您取消註冊 OU 時，您必須先移除所有成員帳戶和巢狀 OUs。然後，AWS Control Tower 會移除套用至 OU 的所有控制項。
  - 如果您從主控台選取刪除 OU，AWS Control Tower 會繼續取消註冊，然後從組織刪除 OU。
  - 不過，如果您透過呼叫 DisableBaseline API 從 OU AWSControlTowerBaseline 中移除 來取消註冊 OU，AWS Control Tower 不會從您的組織刪除 OU，則 OU 仍存在於組織中，且已取消註冊。

已啟用基準和成員帳戶

當您在 OU 上啟用基準時，該組態會由 OU 的成員帳戶繼承。由於繼承的事實，當我們參考帳戶時，會將其稱為子啟用基準。套用至 OU 的基準稱為已啟用父基準。父系啟用基準控制其子系啟用基準的組態。這類似於在 OU 上啟用的控制項如何套用至 OU 中的每個帳戶。

檢視帳戶的基準狀態

AWS Control Tower 不允許您使用基準直接鎖定帳戶。不過，您可以透過每個成員帳戶的繼承子啟用基準來追蹤其啟用和偏離狀態。若要檢視帳戶的狀態，您可以使用 `includeChildren`功能旗標呼叫 `ListEnabledBaselines` API。

停用帳戶的基準

AWS Control Tower 不允許您停用連結至父系啟用基準的子系啟用基準。如果子系啟用的基準偏離且不再連結至父系啟用的基準，則可以停用子系啟用的基準。

基準和版本控制預設值

如果您的 AWS Control Tower 登陸區域已設定，然後選擇啟用登陸區域基準，則 AWS Control Tower 會啟用與您的登陸區域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 會自動提供該 OU 基準的最新相容版本。

OU 基準和登陸區域版本的相容性

如果您的業務需要，AWS Control Tower 基準可讓您在 OU 層級設定控管標準，而不是在登陸區域層級設定控管標準。稱為 的基準`AWSControlTowerBaseline`可協助您向 AWS Control Tower 註冊 OUs。

> **Note**
>
> 基準是一組控制項和資源，共同在您的登陸區域內建立穩定的控管環境。

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 登陸區域版本相容的基準版本。指定基準後，OU 中的所有成員帳戶都會遵循針對 OU 提供的基準。換言之，新帳戶會以更新的基準進行佈建，現有成員帳戶會根據新基準進行管理。

如果您未選取現有 OUs 和帳戶的基準，則登陸區域版本預設會決定整個控管狀態。不過，您登陸區域中的每個已註冊 OU 都會指派一個基準版本，這是與您目前登陸區域版本相容的最新基準。因此，即使您從未特別指派基準，每個 OU 和註冊成員帳戶都有相關聯的基準。

對於 OU 層級基準 `AWSControlTowerBaseline`，下表顯示基準與 AWS Control Tower 登陸區域版本的相容性。

基準版本	登陸區域版本	包含的藍圖	與上一個基準相比的變化		
1.0	2.0 到 2.7	BP_BASELINE_CLOUDTRAIL、BP_BASELINE_CLOUDWATCH、BP_BASELINE_CONFIG、BP_BASELINE_ROLES、BP_BASELINE_SERVICE_ROLES、IAM 資源	無		
2.0	2.8 到 2.9	BP_BASELINE_CLOUDTRAIL、BP_BASELINE_CLOUDWATCH、BP_BASELINE_CONFIG、BP_BASELINE_ROLES、BP_BASELINE_SERVICE_ROLES、Config SLR、IAM 資源	新增使用 SLR AWS Config 的服務連結角色 (SLR) 和新的 Config 藍圖		
3.0	3.0 到 3.1	BP_BASELINE_CLOUDWATCH、BP_BASELINE_C	新的 AWS Config 藍圖。變更為僅在主區域中記錄全		

基準版本	登陸區域版本	包含的藍圖	與上一個基準相比的變化		
		ONFIG、BP_BASELINE_ROLES、BP_BASELINE_SERVICE_ROLES、Config SLR、IAM 資源	域資源。已移除 CloudTrail 藍圖		
4.0	3.2 到 3.3	BP_BASELINE_CLOUDWATCH、BP_BASELINE_CONFIG、BP_BASELINE_ROLES、BP_BASELINE_SERVICE_LINKED_ROLE、BP_BASELINE_SERVICE_ROLES、Config SLR、IAM 資源	新的 SLR 藍圖		

基準版本	登陸區域版本	包含的藍圖	與上一個基準相比的變化		
5.0	4.0	BP_BASELINE_CLOUDWATCH、BP_BASELINE_CONFIG、BP_BASELINE_ROLES、BP_BASELINE_SERVICE_LINKED_ROLE、BP_BASELINE_SERVICE_ROLES、Config SLR、IAM 資源	已移除 AWS Config 彙總授權 (s)。不需要每個成員帳戶的 AWS Config 彙總授權，因為 LandingZone 4.0 版採用的 AWS Organizations Config 彙總工具可存取組織中的所有成員帳戶。		

如需設定登陸區域時在帳戶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。

如果您將登陸區域更新為支援較新AWSControlTowerBaseline基準版本的版本，且新的登陸區域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，而無需立即更新 OU 基準，但登陸區域從 2.x 更新到 3.x 的情況除外。
- 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 （ 在 主控台中使用擴展控管功能，或透過 UpdateEnabledBaseline API)。
- 更新基準版本後，該 OU 中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 登陸區域從任何 2.X 版更新至任何 3.X 版，您也必須在 OUs 上更新基準版本，因為從帳戶層級變更為組織層級 AWS CloudTrail 追蹤。在 主控台中，您的 OU 會顯示需要更新的狀態。

基準的考量事項

- 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。
- 更新登陸區域後，如果您也計劃更新 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。
- 我們建議您更新到所使用登陸區域版本的最高相容基準，以便獲得登陸區域和基準組合的所有優點。例如，如果您更新到登陸區域 3.3 版，您可以繼續使用基準 3.0，但除非您也更新到基準 4.0，否則無法獲得登陸區域 3.3 版的所有好處。
- 基準更新無法復原。
- 基準啟用一次以一個 OU 為目標。因此，在父 OUs 更新時，不會自動更新巢狀 OU。建議您先更新父 OU，再更新巢狀 OUs。
- 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登陸區域版本相容時，如果您在未受管 OU 上啟用基準，則必須使用最新的基準版本。

範例：僅向 APIs 註冊 AWS Control Tower OU

此範例演練是配套文件。如需說明、注意事項和詳細資訊，請參閱 基準類型。

先決條件

您必須擁有尚未向 AWS Control Tower 註冊的現有 OU，而且您想要註冊。或者，您必須擁有要為更新目的重新註冊的已註冊 OU。

註冊 OU

1. 檢查是否已為登陸區域`IdentityCenterBaseline`啟用 。若是如此，請取得 Identity Center Enabled Baseline 識別符。

```
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基準的 ARN。

```
aws controltower list-baselines --query 'baselines[?name==`AWSControlTowerBaseline`].
[arn]'
```

4. 在目標 OU 上建立AWSControlTowerBaseline基準。

   如果身分中心基準已啟用：

```
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 Identity Center Baseline，請省略 *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

更新登陸區域設定或更新您的登陸區域版本後，您必須重新註冊 OUs才能提供最新的變更。請依照下列步驟，重設相關聯的EnabledBaseline資源和任何相關聯的EnabledControl資源，以程式設計方式重新註冊 OU。

> **Important**
>
> 如果 OU 已啟用選用控制項，則在重設基準之後，您還必須為每個已啟用的選用控制項呼叫 ResetEnabledControl API。此步驟可確保選用控制項與最新的登陸區域組態保持一致。如果您略過此步驟，OU 上的選用控制項可能不會反映最新的登陸區域變更。如果您沒有啟用任何選用的控制項，則不需要此步驟。

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 EnabledBaseline 資源的 ARN。

```
aws controltower list-enabled-baselines --query 'enabledBaselines[?
targetIdentifier==`<OUARN>`].[arn]'
```

3. 重設已啟用基準。

```
aws controltower reset-enabled-baseline --enabled-baseline-
identifier <EnabledBaselineArn>
```

4. 如果 OU 已啟用選用控制項，請列出 OU 的已啟用控制項，並重設每個控制項，使其與最新的登陸區域組態保持一致。

   列出目標 OU 上已啟用的控制項：

```
aws controltower list-enabled-controls --target-identifier <OU ARN>
```

   對於傳回的每個已啟用的選用控制項，請呼叫 來重設它：

```
aws controltower reset-enabled-control --enabled-control-
identifier <EnabledControlArn>
```

   如需詳細資訊，請參閱 AWS Control Tower API 參考中的 ResetEnabledControl。

基準 API 用量的範例

本節包含 AWS Control Tower 基準 APIs 的輸入和輸出參數範例。

DisableBaseline

如需此 API 操作的詳細資訊，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"
}
```

DisableBaseline CLI 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 操作的詳細資訊，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，傳回新資源：

```
{
    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f",
    "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAGF7TNOHRD7ES5VV"
}
```

EnableBaseline CLI 範例：

此範例顯示為已選擇加入 IAM Identity Center AWS 存取權 AWS Organizations 的組織啟用基準，該組織由 AWS Control Tower 管理。若要擷取 Identity Center EnabledBaseline識別符，您可以呼叫 ListEnabledBaselines API，在 Identity Center 基準上進行篩選：(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
```

回應會顯示EnabledBaseline詳細資訊，顯示其識別符。

```
{
    "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，並將此值做為參數傳遞，以啟用預設基準。

```
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 \
    --parameters
 '[{"key":"IdentityCenterEnabledBaselineArn","value":"arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC"}]' \
    --region us-west-2
```

對於登陸區域已從 IAM Identity Center 的 AWS Control Tower 管理選擇退出的組織，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 操作的詳細資訊，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.",
}
```

GetBaseline CLI 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 操作的詳細資訊，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"
    }
}
```

GetBaselineOperation CLI 範例：

```
aws controltower get-baseline-operation \
```

```
    --operation-identifier 58f12232-26be-4735-a3e9-dd30d90f021f \
    --region us-west-2
```

GetEnabledBaseline

如需此 API 操作的詳細資訊，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"
            }
        ]
    }
}
```

GetEnabledBaseline CLI 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 操作的詳細資訊，請參閱 ListBaselines。

ListBaselines input（使用選用輸入）：

```
{
    "nextToken": "AbCd1234",
    "maxResults": "4"
}
```

ListBaselines 輸出：

```
{
    "baselines": [
        {
            "arn": "arn:aws:controltower:us-east-1::baseline/4T4HA1KMO10S6311",
            "name": "AuditBaseline",
            "description": "Sets up resources to monitor security and compliance of
 accounts in your organization."
        },
        {
            "arn": "arn:aws:controltower:us-east-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-east-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-east-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."
        },
```

```
        {
            "arn": "arn:aws:controltower:us-east-1::baseline/3WPD0NA6TJ9AOMU2",
            "name": "BackupCentralVaultBaseline",
            "description": "Sets up central AWS Backup vault in your organization."
        },
        {
            "arn": "arn:aws:controltower:us-east-1::baseline/H6C5JFCJJ3CPU3J5",
            "name": "BackupManagerBaseline",
            "description": "Sets up delegated admin and AWS Backup Audit Manager."
        },
        {
            "arn": "arn:aws:controltower:us-east-1::baseline/APO9ATVPBKFRRGLK",
            "name": "BackupBaseline",
            "description": "Sets up local Backup vault and attach Backup policy."
        }
    ]
}
```

ListBaselines CLI 範例：

```
aws controltower list-baselines \
    --region us-west-2
```

ListEnabledBaselines

ListEnabledBaselines API 具有選用參數，可讓您檢視套用到屬於 OU 成員之帳戶的基準。以下範例顯示一些 CLI 命令，您可以用來檢視帳戶的基準。AWS Control Tower 是指在 OU 上啟用的這些基準，但會套用到 OU 中的每個帳戶，做為子啟用的基準，因為它們從在 OU 上套用的基準衍生其控管組態。

如需此 API 操作的詳細資訊，請參閱 ListEnabledBaselines。

ListEnabledBaselines 輸入以顯示子啟用的基準：

```
aws controltower list-enabled-baselines --include-children
```

ListEnabledBaselines 輸出以檢視子啟用的基準：

```
{
    "enabledBaselines": [
        {
```

```
            "arn": "arn:aws:controltower:us-east-1:666355521292:enabledbaseline/
XO2UQ1PC6BB5085S5",
            "baselineIdentifier": "arn:aws:controltower:us-east-1::baseline/
APO9ATVPBKFRRGLK",
            "baselineVersion": "1.0",
            "statusSummary": {
                "lastOperationIdentifier": "07d6d2b8-e357-4f96-ba00-98ea88143445",
                "status": "SUCCEEDED"
            },
            "targetIdentifier": "arn:aws:organizations::666355521292:ou/o-vaex10vaey/
ou-k86y-ld9k8vpu"
        },
        {
            "arn": "arn:aws:controltower:us-east-1:666355521292:enabledbaseline/
XAFPKQQXOJB50ZWQH",
            "baselineIdentifier": "arn:aws:controltower:us-east-1::baseline/
APO9ATVPBKFRRGLK",
            "baselineVersion": "1.0",
            "parentIdentifier": "arn:aws:controltower:us-
east-1:666355521292:enabledbaseline/XOIZ4G08CWB50ZWON",
            "statusSummary": {
                "lastOperationIdentifier": "3508793e-48c8-4895-965b-3dc6abd52b6b",
                "status": "SUCCEEDED"
            },
            "targetIdentifier": "arn:aws:organizations::666355521292:account/o-
vaex10vaey/183295447314"
        }
]
```

> **Note**
>
> 在上述範例中，parentIdentifier 欄位會顯示此子系已啟用基準的父系 OU 已啟用基準。

檢視套用至特定目標 (OU 或帳戶） 的所有基準：

```
aws controltower list-enabled-baselines \
    --filter '{
        "targetIdentifiers": ["TARGET_ARN"]
    }
```

檢視具有特定基準的所有 OUs：

```
aws controltower list-enabled-baselines \
    --filter '{
        "baselineIdentifiers": ["BASELINE_ARN"]
    }'
```

檢視具有特定基準的所有 OUs和帳戶：

```
aws controltower list-enabled-baselines \
    --filter '{
        "baselineIdentifiers": ["BASELINE_ARN"]
    }'  \
    --include-children
```

檢視 OU 中已啟用基準 B 的所有帳戶：

```
### First fetch the enabled baseline record for Baseline B on the OU
 aws controltower list-enabled-baselines \
    --filter '{
        "targetIdentifiers": ["OU_TARGET_ARN"],
        "baselineIdentifiers": ["BASELINE_ARN_FOR_BASELINE_B"]
    }'

### Call ListEnabled baseline to fetch all accounts that have their parent as the
 enabled baseline record on the OU
aws controltower list-enabled-baselines \
    --filter '{
        "parentIdentifiers": ["ENABLED_BASELINE_ARN_FOR_OU"]
    }' \
    --include-children
```

有關子系啟用基準的更多資訊

- 您可以使用 GetEnabledBaseline API 來檢視已啟用特定子系基準的詳細資訊
- 您可以使用 GetBaselineOperation API 來檢視在子已啟用基準上執行的操作
- 您無法在已啟用子基準上直接呼叫任何寫入 APIsDisableBaseline，例如 UpdateEnabledBaseline、 EnableBaselineResetEnabledBaseline或 。
- 子系啟用的基準資源只能透過 AWS Control Tower 服務、在父系 OU 上執行的操作，或透過 Account Factory 進行修改。

使用篩選條件的範例：

ListEnabledBaselines input（無篩選條件）：

```
{
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 5
}
```

ListEnabledBaselines input (baselineIdentifiers 僅限篩選條件）：

```
{
    "filter": {
        "baselineIdentifiers": ['arn:aws:controltower:us-
east-1::baseline/17BSJV3IGJ2QSGA2', 'arn:aws:controltower:us-
east-1::baseline/12GZU8CKZKVMS2AW']
    },
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 5
}
```

ListEnabledBaselines input (targetIdentifiers 僅限篩選條件）：

```
{
    "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篩選條件）：

```
{
    "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"
}
```

具有一種篩選條件 (baselineIdentifiers 篩選條件） 的 CLI 範例：

```
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
```

使用多個篩選條件 (baselineIdentifiers 和 targetIdentifiers 篩選條件） 的 CLI 範例：

```
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 操作的詳細資訊，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"
}
```

ResetEnabledBaseline CLI 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 操作的詳細資訊，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"
}
```

UpdateEnabledBaseline CLI 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
```

其他資訊和連結

本主題包含相關部落格文章的連結、技術文件和相關資訊，可協助您使用 AWS Control Tower。這些來源涵蓋 AWS Control Tower 功能的一些常見使用案例和最佳實務，以及一些額外的增強功能。

教學課程和實驗室

- AWS Control Tower 實驗室 – 這些實驗室提供 AWS Control Tower 相關常見任務的高階概觀。
- 在 AWS Control Tower 儀表板上，如果您有使用案例，但不確定從何處開始，請選擇取得個人化指引。
- 請嘗試造訪此 AWS Cloud Operations YouTube 播放清單並搜尋 AWS Control Tower 以尋找影片，以進一步了解如何使用 AWS Control Tower 功能。

聯網

為 中的網路設定可重複且可管理的模式 AWS。進一步了解客戶常用的設計、自動化和設備。

- AWS Quick Start VPC 架構 – 此 Quick Start 指南根據 AWS 雲端基礎設施的 AWS 最佳實務提供聯網基礎。它使用公有和私有子網路建置 AWS Virtual Private Network 環境，您可以在其中啟動 AWS 服務和其他資源。
- 使用 AWS Service Catalog 的 AWS Control Tower 自助VPCs – 此部落格文章描述了設定 Account Factory 的方式，讓您可以使用自訂 VPCs佈建帳戶。
- 在 AWS Control Tower 中實作 Serverless Transit Network Orchestrator (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 環境中管理網路的人員。

安全性、身分和記錄

擴展您的安全狀態、與外部或現有身分提供者整合，以及集中記錄系統。

安全性

- 使用 AWS Control Tower 生命週期事件自動化 AWS Security Hub CSPM 提醒 – 此部落格文章說明如何在現有和新帳戶的 AWS Control Tower 多帳戶環境中自動化 Security Hub CSPM 啟用和組態。

- 啟用 AWS Identity and Access Management – 此部落格文章說明如何啟用和集中 IAM Access Analyzer 調查結果，以增強您的組織安全可見性。
- AWS Systems Manager 參數存放區為組態資料管理和秘密管理提供安全的階層式儲存。您可以使用它在安全的位置共用組態資訊，以供 AWS Systems Manager 和 AWS CloudFormation 使用。例如，您可以存放您要部署一致性套件的區域清單。

身分

- 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搭配 IAM Identity Center 和 AWS Control Tower 使用 Azure AD。
- 使用 集中管理 Okta 使用者的 AWS 存取權 AWS IAM Identity Center – 此部落格文章說明如何搭配 IAM Identity Center 和 AWS Control Tower 使用 Okta。

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，可讓組織 AWS 跨多個帳戶和區域收集、分析和 AWS 顯示日誌。
- 如需檢視 AWS Config 資源的相關資訊，請參閱 Config Resource Compliance Dashboard。

部署資源和管理工作負載

部署和管理資源和工作負載。

- 入門程式庫整合 – 此部落格文章說明您可以使用的入門產品組合。
- 持續將雲端託管人部署至 AWS Control Tower

使用現有的組織和帳戶

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。
- 在 AWS Control Tower 下擁有 帳戶 – 此部落格文章說明如何將 AWS Control Tower 部署到現有的 AWS 組織。
- 使用 AWS Config 一致性套件擴展 AWS Control Tower 控管 – 此部落格文章說明如何部署 AWS Config 一致性套件，以協助將現有帳戶和組織納入 AWS Control Tower 的控管。

- 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，以便您透過電子郵件收到控制合規違規的通知。

自動化與整合

自動化帳戶建立，並將生命週期事件與 AWS Control Tower 整合。

- 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 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 VPCs 的資源標記。
- 自動化帳戶管理 – 此部落格文章說明如何在設定 AWS Control Tower 環境後自動化帳戶管理任務。

遷移工作負載

使用其他 AWS 服務搭配 AWS Control Tower，以協助工作負載遷移。

- CloudEndure 遷移 – 此部落格文章說明如何將 CloudEndure 和其他 AWS 服務與 AWS Control Tower 結合，以協助工作負載遷移。

相關 AWS 服務

AWS Control Tower 可做為 的協同運作層 AWS Organizations。因此，透過 AWS Organizations 主控台和 APIs，您可以存取其他超過 20 個與 AWS Control Tower 搭配使用的 AWS 服務。這些額外服務無法直接透過 AWS Control Tower 主控台存取。

- 如需透過 AWS Organizations 提供給 AWS Control Tower 的服務完整清單，請參閱可與 AWS Organizations 搭配使用的 AWS 服務。
- 若要為這些相關的 AWS 服務啟用多帳戶功能，您必須啟用受信任的存取。如需詳細資訊，請參閱搭配其他 AWS 服務使用 AWS Organizations。

> **Note**
>
> 請記住，IAM Identity Center AWS Config、 AWS 和 AWS CloudTrail 是在 AWS Control Tower 中為您設定並完全整合。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 可以使用委派的管理，包括 AWS Systems Manager 和 AWS Firewall Manager。如需詳細資訊，請參閱設定委派管理員和啟用 Firewall Manager 的委派管理員帳戶。另請參閱此影片，使用 AWS Firewall Manager 設定安全群組。

AWS Marketplace 解決方案

探索來自 的解決方案 AWS Marketplace。

- AWS Control Tower Marketplace – 為 AWS Control Tower AWS Marketplace 提供各種解決方案，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設施和操作使用案例，包括身分管理、多帳戶環境的安全性、集中式聯網、操作智慧，以及安全資訊和事件管理 (SIEM)。

AWS Control Tower 版本備註

下列各節顯示自服務啟動以來，AWS Control Tower 版本的詳細資訊。有些版本需要更新 AWS Control Tower 登陸區域，而其他版本會自動併入服務中。

功能和版本會根據正式向公眾宣布的日期，以反向時間順序（最新先到）列出。

主題

2026 年 1 月 - 目前

自 2026 年 1 月起，AWS Control Tower 已發佈下列更新：

- 歐洲主權雲端提供 AWS Control Tower

歐洲主權雲端提供 AWS Control Tower

2026 年 1 月 13 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 現已在歐洲主權雲端提供。如需歐洲主權雲端中 AWS Control Tower 的詳細資訊，請參閱歐洲主權雲端的 AWS Control Tower 使用者指南。

2025 年 1 月 – 2025 年 12 月

自 2025 年 1 月起，AWS Control Tower 已發佈下列更新：

- AWS Control Tower 登陸區域 4.0 版
- AWS Control Tower 會將其他 279 個 AWS Config 控制項新增至 Control Catalog
- 亞太區域 （ 紐西蘭 ） 區域提供 AWS Control Tower
- AWS Control Tower 支援自動帳戶註冊
- AWS Control Tower 更新 Python 版本
- AWS Control Tower 支援 IPv6 地址
- AWS Control Tower 減少偏離

  提供適用於 Terraform 的 Account Factory 1.15.0 版
- 使用 Nitro 執行個體類型更新控制項
- 亞太區域 （ 台北 ） 區域提供 AWS Control Tower
- AWS Control Tower 支援 PrivateLink
- 支援其他產業架構、更新的中繼資料
- 服務連結 AWS Config 控制項
- 啟用的控制項主控台檢視可提供集中式可見性
- the section called “Account Factory for Terraform (AFT) 在部署時支援新組態”
- AWS Control Tower 推出基準 APIs的帳戶層級報告
- the section called “AWS Control Tower 適用於 AWS 亞太區域 （ 泰國 ） 和墨西哥 （ 中部 ） 區域”
- 其他可用的 AWS Config 控制項
- 取消註冊和刪除 OUs 的動作
- the section called “Control Catalog 支援 IPv6 地址”

AWS Control Tower 登陸區域 4.0 版

2025 年 11 月 17 日

(AWS Control Tower 登陸區域需要更新至 4.0 版。 如需詳細資訊，請參閱 更新您的登陸區域)。

AWS Control Tower 登陸區域 4.0 是一項主要更新，引進了靈活的僅限控制體驗，讓客戶能夠自訂如何實作和管理其 AWS 多帳戶環境。此版本會大幅改變 AWS Control Tower 與 AWS 服務整合和管理組織資源的方式。如需金鑰變更的資訊，請參閱 登陸區域 v4.0 遷移指南。

主要變更和功能

- 選用的服務整合 - 登陸區域 4.0 可讓您選擇要在環境中啟用的服務整合。停用整合將清除 AWS Control Tower 在受管帳戶和服務整合中央帳戶中針對該整合部署的資源。您現在可以選擇性地啟用或停用服務整合：
  - AWS Config
  - AWS CloudTrail
  - 安全角色
  - AWS Backup

重要：如果您想要停用 AWS Config 整合，您還必須停用安全角色、IAM Identity Center 和 AWS Backup 整合。

- 專用資源，而不是使用共用資源 - 登陸區域 4.0 現在會為金鑰服務建立專用資源。此區隔可提供更好的資源隔離，並更精細地控制服務特定的資源：
  - AWS Config 的個別 S3 儲存貯體
  - AWS CloudTrail 的個別 S3 儲存貯體
  - 每個服務的個別 SNS 主題

- 彈性組織結構 - 登陸區域 4.0 會移除先前的組織結構需求：
  - 您不再需要使用安全 OU
  - 您可以定義自己的組織結構
  - 唯一的要求是所有中樞帳戶都必須位於相同的 OU
- 專用控制項體驗 - 您現在可以建立最小的登陸區域設定，其中包含：
  - 基本 AWS Organizations 整合
  - 能夠在不啟用`AWSControlTowerBaseline`基準的情況下啟用控制項
  - 根據您的需求自訂控管組態
- AWS Config 變更 - 登陸區域 4.0 引入了 AWS Config 整合實作的多項改進：
  - 專門用於偵測控制項的新 Config 輔條基準
  - Config 中樞帳戶中的服務連結 Config 彙總工具 (SLCA)
  - 取代傳統組織和帳戶彙總工具
- 選用資訊清單：

- 資訊清單欄位現在為選用，可讓您：
  - 建立無需任何服務整合的登陸區域
  - 初始設定時更具彈性
  - 自訂部署選項

AWS Control Tower 會將其他 279 個 AWS Config 控制項新增至 Control Catalog

2025 年 11 月 14 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 現在包含額外的 279 個 AWS Config 控制項做為 Control Catalog 的一部分。您可以在 AWS Control Tower 主控台中或透過 APIs 檢視控制項。

某些控制項與其他控制項有關係。這些關係也會在 AWS Control Tower 主控台和 APIs中表示。關係類型包括補充、互斥和替代。

亞太區域（紐西蘭）區域提供 AWS Control Tower

2025 年 10 月 28 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 現已在亞太區域（紐西蘭）區域提供。

如需 AWS Control Tower 可用區域的完整清單，請參閱AWS 區域表。

AWS Control Tower 支援自動帳戶註冊

2025 年 10 月 15 日

(AWS Control Tower 登陸區域不需要更新。)

對於操作 AWS Control Tower 登陸區域 3.1 版或更新版本的客戶，AWS Control Tower 現在允許在 OUs 中自動註冊帳戶。如果您選擇自動註冊帳戶，AWS Control Tower 會在您將帳戶移至新的 OU 時，將 OU 啟用的基準資源和控制項套用至帳戶。會移除先前 OU 的控制項和基準。在大多數情況下，此動作不會建立偏離。

若要啟用自動註冊：您可以在 AWS Control Tower 主控台的登陸區域設定頁面上選取帳戶自動註冊，或呼叫 AWS Control Tower `CreateLandingZone`或 `UpdateLandingZone` APIs，並將 `RemediationType` 參數的值設定為繼承偏離。

若要套用自動註冊：在設定頁面中選取此選項後，您可以透過 AWS Organizations 主控台、API AWS Organizations `MoveAccount`或 AWS Control Tower 主控台來移動帳戶。

若要透過自動註冊取消註冊帳戶：如果您將帳戶移出已註冊的 OU，AWS Control Tower 會自動移除所有部署的基準資源和控制項。

如需自動註冊的詳細資訊，請參閱 選擇性地設定帳戶的自動註冊。

此版本也包含受管政策和新受管政策的更新。我們更新了 AWS ControlTowerServiceRolePolicy，並新增了新的 AWS ControlTowerIdentityCenterManagementPolicy。

我們更新了 AWS Control Tower `CreateLandingZone`和 `UpdateLandingZone` API，以新增`RemediationType`名為 的新 `Inheritance Drift`。 APIs

AWS Control Tower 更新 Python 版本

2025 年 9 月 3 日

(AWS Control Tower 登陸區域不需要更新。)

Python 3.9 版已棄用。AWS Control Tower 已更新 AWS Control Tower 環境中的 Python 版本。不需要任何動作，而且此更新不會影響您現有的工作負載。

AWS Control Tower 減少偏離

2025 年 8 月 20 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 已更新服務控制政策 (SCP) 偏離的功能。在此版本中，AWS Control Tower 會直接處理兩種類型的控管偏離，不會再在您的環境中造成偏離。

已移除兩種類型的控管偏離

- 連接到受管 OU 的 SCP – 當控制項的 SCP 連接到任何其他 OU 時，會發生這種偏離。當您從 AWS Control Tower 主控台外部更新 OUs時，這種情況特別常見。

- 連接至成員帳戶的 SCP – 當控制項的 SCP 從 AWS Control Tower 主控台外部連接至帳戶時，通常會發生這種偏離。

如需偏離的詳細資訊，請參閱在 AWS Control Tower 中偵測和解決偏離。

AWS Control Tower 支援 IPv6 地址

2025 年 8 月 18 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower API 現在透過新的雙堆疊端點支援網際網路通訊協定第 6 版 (IPv6) 地址。支援 IPv4 的現有端點仍可回溯相容。新的雙堆疊網域可從網際網路或使用 AWS PrivateLink 從 Amazon Virtual Private Cloud (VPC) 中取得。

提供適用於 Terraform 的 Account Factory 1.15.0 版

2025 年 7 月 28 日

(AWS Control Tower 登陸區域不需要更新。)

1.15.0 版的 AWS Control Tower Account Factory for Terraform (AFT) 已推出。如需詳細資訊，請參閱 AFT GitHub 儲存庫。

使用 Nitro 執行個體類型更新控制項

2025 年 7 月 24 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 已更新 Control Catalog （ 先前稱為 Control Library) 中的八個主動控制，以強制執行 Amazon EC2 初始化類型。此更新可讓您執行個體化一些新的 Nitro 執行個體類型，並移除一些已取代的 u 系列執行個體類型。

已更新控制項

- CT.AUTOSCALING.PR.10
- CT.AUTOSCALING.PR.11
- CT.EC2.PR.15

- CT.EC2.PR.16
- CT.EC2.PR.17
- CT.EC2.PR.18
- CT.EC2.PR.19
- CT.EC2.PR.20

可用的新執行個體類型

- c8gd
- c8gn
- i7i
- m8gd
- p6-b200
- r8gd

已移除執行個體類型

- u-12tb1
- u-18tb1
- u-24tb1
- u-9tb1

更新後的控制項可在 AWS Control Tower 可用的所有 AWS 區域 中使用。如需可使用 AWS Control Tower 的區域清單，請參閱 AWS 區域 表格。

亞太區域（台北）區域提供 AWS Control Tower

2025 年 7 月 23 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 現已在亞太區域（台北）區域提供：

如需 AWS Control Tower 可用區域的完整清單，請參閱AWS 區域表。

AWS Control Tower 支援 PrivateLink

2025 年 6 月 30 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 現在支援 AWS PrivateLink。您可以從 Amazon Virtual Private Cloud (VPC) 內叫用 AWS Control Tower 和 Control Catalog APIs，而無需周遊公有網際網路。 可在虛擬私有雲端 (VPCs)、支援的服務和資源，以及內部部署網路之間 AWS PrivateLink 提供私有連線。AWS Control Tower 的 AWS PrivateLink 支援可在 AWS Control Tower 提供的所有 AWS 區域 中使用。

支援其他產業架構、更新的中繼資料

2025 年 6 月 12 日

(AWS Control Tower 登陸區域不需要更新。)

在此版本中，AWS Control Tower 擴展以包含 10 個產業架構的支援。如需架構清單，請參閱支援的架構。

例如，您可以開始導覽至 AWS Control Tower 主控台的 Control Catalog 頁面，並搜尋 PCI-DSS-v4.0 等架構，以檢視與該架構相關的所有控制項。或者，您可以透過呼叫新的 `ListControlMappings` API，以程式設計方式檢查控制項和架構。

與控制項相關聯的中繼資料定義正在變更，以更好地支援這些額外的產業影格。中繼資料的變更可能會影響您評估啟用控制項的方式。例如，NIST、PCI 和 CIS 中繼資料的值可能已變更。建議您在 主控台的控制詳細資訊頁面上，檢視已啟用控制項的映射。

在 主控台和 API 中，我們推出了 3 個新的中繼資料欄位。這些欄位整體描述了一個階層，協助您了解如何分類和啟用控制項。欄位為：網域、目標和常見控制項。我們已重新定義控制目標，以更符合更廣泛的產業架構可用範圍。如需此階層的詳細資訊，請參閱腫瘤學概觀。

- 這些中繼資料變更會反映在 AWS Control Tower 主控台中，而且主控台體驗在 AWS Control Tower 和 AWS Config 主控台之間是一致的。
- 若要在 AWS Control Tower 主控台中檢視控制項資訊，您必須將其他`controlcatalog`許可新增至 IAM 政策。如需詳細資訊，請參閱使用 AWS Control Tower 主控台所需的許可。
- 每個控制項現在都有一個名為 的新欄位`GovernedResources`，顯示控制項管理的資源類型。在某些情況下，此欄位會顯示資源的服務字首，在其他執行個體中，可以是空白的。如需詳細資訊，請參閱`GetControl`及`ListControls`。

在此版本中，我們已將 Controls Library 重新命名為 Control Catalog，以與其他術語保持一致。

服務連結 AWS Config 控制項

2025 年 6 月 12 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 宣布支援將 AWS Control Tower 偵測控制部署為服務連結 AWS Config 規則。

在此版本中，AWS Control Tower 現在會直接在您的註冊帳戶中部署服務連結 Config 規則，以 AWS CloudFormation 堆疊集取代先前的部署方法。此變更可大幅改善部署速度。此外，這些服務連結 Config 規則有助於確保資源的一致控管，因為它們可防止可能因手動變更 CloudFormation 堆疊集或 Config 規則而導致的意外組態偏離。

接下來，所有由 AWS Config 規則實作的 AWS Control Tower 控制項都會使用此機制部署，此機制會直接呼叫 AWS Config APIs。

> **Important**
>
> 在您採用服務連結 Config 規則之前，請檢閱您在 AWS Control Tower 外部對 Config 規則所做的現有自訂，例如修復，因為這些自訂會在轉換期間移除。 AWS Config APIs 不支援為服務連結 AWS Config 規則新增修復組態。請參閱 PutRemediationConfigurations。

所需的詳細資訊和動作

- 當您更新或重設登陸區域時，AWS Control Tower 會更新管理安全 OU 的強制性控制。若要完成升級，您也必須重設以 AWS Config 規則內嵌的每個偵測性控制項，或重新註冊 OU。
- 如果您的 AWS Control Tower 登陸區域版本為 3.2 或更新版本，則此升級的完整範圍適用於您。當您套用此更新時，現有的 AWS Config 規則會變更為服務管理的 Config 規則，以及新的部署方法。
- 如果您的登陸區域是 3.1 版或以下版本，則會使用新方法部署任何新的 Config 規則，而不再使用堆疊集。您現有的 Config 規則不會更新為服務管理的 Config 規則。它們將保留為標準類型。
- 您可以依其資源 ARN 來識別服務連結組態規則，其格式為：

```
arn:aws:config:*:*:config-rule/aws-service-rule/controltower.*/*
```

由服務連結 AWS Config 規則實作時，控制項的預期功能並未變更。AWS Control Tower 中的偵測性服務連結 Config 規則可以識別您帳戶中的不合規資源，例如政策違規，並透過儀表板提供提醒。為了

保持一致性、防止組態偏離並簡化您的整體使用者體驗，現在只能透過 AWS Control Tower 修改這些規則。

在此版本中，我們為服務連結角色 (SLR) 的政策新增了四個新許可[AWSServiceRoleForAWSControlTower](#)，以便您可以啟用和停用已註冊帳戶的服務連結 AWS Config 規則。

```
config:DescribeConfigRules
config:TagResource
config:PutConfigRule
config:DeleteConfigRule
```

啟用的控制項主控台檢視可提供集中式可見性

2025 年 5 月 21 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 在主控台中新增了新頁面，可在單一集中式檢視中顯示所有已啟用的控制項。先前，只有啟用控制項的帳戶或 OU 才能檢視控制項。合併檢視可讓您更輕鬆地大規模識別控制控管中的差距。

在已啟用控制項頁面上，您可以根據行為篩選控制項：Deventive、Detective 或 Proactive。您也可以根據控制實作進行篩選，例如 SCP。對於每個控制項，您可以查看啟用此控制項OUs 數量。

若要查看已啟用控制項頁面，請導覽至 AWS Control Tower 主控台中的控制項區段。

Account Factory for Terraform (AFT) 在部署時支援新組態

2025 年 5 月 13 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 帳戶自訂架構 Account Factory for Terraform (AFT) 現在在部署時支援三個額外的選用組態。您可以將 AFT 部署到自訂虛擬私有雲端 (VPC)，指定 AFT 部署的 Terraform 專案名稱，並標記 AFT 建立的資源。

如需詳細資訊，請參閱[部署適用於 Terraform (AFT) 的 AWS Control Tower 帳戶工廠](#)。

AWS Control Tower 推出基準 APIs的帳戶層級報告

2025 年 5 月 12 日

(AWS Control Tower 登陸區域不需要更新。)

您現在可以透過呼叫基準 APIs，以程式設計方式檢視受管帳戶的偏離和帳戶註冊狀態。透過此功能，您可以識別帳戶和 OU 基準組態何時漂移或不同步。若要以程式設計方式檢視偏離狀態，您可以針對已啟用的基準呼叫 `ListEnabledBaselines` API。若要使用 `ListEnabledBaselines` API 以程式設計方式檢視個別帳戶的狀態，請使用 `includeChildren`旗標。您可以依這些狀態進行篩選，並只查看需要您注意的帳戶和 OUs。

`AWS_ControlTowerBaseline` 會設定控管所需的最佳實務組態、控制項和資源。當您在組織單位 (OU) 上啟用此基準時，OU 內的成員帳戶會自動註冊到 AWS Control Tower。AWS Control Tower 基準 APIs 包含 CloudFormation 支援，可讓您建置自動化，以使用基礎設施即程式碼 (IaC) 來管理 OUs 和帳戶。

若要進一步了解這些 APIs，請參閱《AWS Control Tower 使用者指南》中的基準。AWS Control Tower 提供的所有 都提供偏離和帳戶註冊狀態的基準 APIs AWS 區域 和新啟動的報告功能。如需 AWS Control Tower 可用 AWS 區域 位置的清單，請參閱 AWS 區域 表格。

AWS Control Tower 適用於 AWS 亞太區域 （泰國） 和墨西哥 （中部） 區域

2025 年 5 月 9 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 現已在下列 AWS 區域提供：

- 亞太區域 (泰國)
- 墨西哥 (中部)

如需 AWS Control Tower 可用區域的完整清單，請參閱AWS 區域表。

其他可用的 AWS Config 控制項

2025 年 4 月 11 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 現在支援適用於各種使用案例的額外 223 個受管 AWS Config 規則，例如安全性、成本、耐用性和操作。透過此啟動，您現在可以使用 AWS Control Tower 來搜尋和探索管理多帳戶環境所需的 AWS Config 規則；然後直接從 AWS Control Tower 啟用和管理控制項。

若要從 AWS Control Tower 主控台開始使用，請前往 Control Catalog，並使用實作篩選條件搜尋控制項 AWS Config。您可以直接從 AWS Control Tower 主控台啟用控制項。

如需詳細資訊，請參閱 AWS Control Tower 中可用的整合式 AWS Config 控制項。

此次啟動後，我們更新了 `ListControls`和 `GetControl` APIs，以支援三個新欄位：CreateTime、嚴重性和實作，您可以在 Control Catalog 中搜尋控制項時使用。例如，您現在可以以程式設計方式找到上次評估後建立的高嚴重性 AWS Config 規則。

您可以在可使用 AWS Control Tower 的所有 AWS 區域 中搜尋新 AWS Config 規則。若要部署規則，請參閱該規則 AWS 區域 支援的 清單，以查看可啟用該規則的位置。

取消註冊和刪除 OUs 的動作

2025 年 4 月 8 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 現在支援個別主控台動作來取消註冊 OU 和刪除 OU。您必須先取消註冊 OU，才能將其刪除。您可以取消註冊 OU，從 AWS Control Tower 移除 OU。

如需詳細資訊，請參閱移除 OU。

Control Catalog 支援 IPv6 地址

2025 年 4 月 2 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower Control Catalog API 現在透過新的雙堆疊端點支援網際網路通訊協定第 6 版 (IPv6) 地址。支援 IPv4 的現有 Control Catalog 端點仍可回溯相容。新的雙堆疊網域可從網際網路或使用 AWS PrivateLink 從 Amazon Virtual Private Cloud (VPC) 中取得。

2024 年 1 月至 12 月

2024 年，AWS Control Tower 發佈了下列更新：

- AWS Control Tower CfCT 支援 GitHub 和 RCPs
- AWS Control Tower 使用宣告式政策新增預防性控制
- AWS Control Tower 新增規範備份計劃選項
- AWS Control Tower 整合 AWS Config 控制項
- AWS Control Tower 改善勾點管理並新增主動控制區域
- AWS Control Tower 啟動受管資源控制政策
- AWS Control Tower 報告控制政策偏離
- 新的 `ResetEnabledControl` API
- 控制目錄更新 `GetControl` API
- AWS Control Tower AFT 支援 GitLab
- AWS 亞太區域 （馬來西亞） 區域提供 AWS Control Tower
- AWS Control Tower 每個 OU 最多支援 1000 個帳戶
- AWS Control Tower 新增登陸區域版本選擇
- 可用的描述性控制 API，擴展對區域和控制項的存取
- AWS Control Tower 在選擇加入區域中支援 AFT 和 CfCT
- AWS Control Tower 新增 `ListLandingZoneOperations` API
- AWS Control Tower 最多支援 100 個並行控制操作
- AWS Control Tower 可在 AWS 加拿大西部 （卡加利） 使用
- AWS Control Tower 支援自助式配額調整
- AWS Control Tower 發佈控制項參考指南
- AWS Control Tower 會更新和重新命名兩個主動控制
- 已棄用的控制項不再可用
- AWS Control Tower 支援在 中標記`EnabledControl`資源 CloudFormation
- AWS Control Tower 支援具有基準的 OU 註冊和組態 APIs

AWS Control Tower CfCT 支援 GitHub 和 RCPs

2024 年 12 月 9 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 現在支援 GitHub™ TM作為第三方版本控制系統 (VCS) 和 AWS Control Tower 自訂組態來源 (CFCT) 的選項。如需詳細資訊，請參閱 將 GitHub 設定為組態來源。

AWS Control Tower 現在支援 AWS Control Tower (CFCT) 自訂的資源控制政策 (RCPs)。如需詳細資訊，請參閱CfCT 自訂指南。

AWS Control Tower 使用宣告式政策新增預防性控制

2024 年 12 月 1 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 現在支援宣告政策從中實作的預防性控制 AWS Organizations。宣告政策會直接套用在服務層級。此方法可確保強制執行指定的組態，即使服務引入了新功能或 APIs。如需詳細資訊，請參閱使用宣告政策實作的控制項。

AWS Control Tower 新增規範備份計劃選項

2024 年 11 月 25 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 現在支援方案 AWS Backup ，可讓您將資料備份和復原工作流程直接整合到您的登陸區域。備份計畫包含預先定義的規則，例如保留天數、備份頻率，以及進行備份的時段。這些規則定義如何在所有受管成員帳戶中備份 AWS 資源。當您將備份計劃套用至登陸區域時，AWS Control Tower 會確保所有成員帳戶的計劃一致，並符合 AWS Backup 的最佳實務建議。

如需詳細資訊，請參閱 AWS Backup and AWS Control Tower。

AWS Control Tower 整合 AWS Config 控制項

2024 年 11 月 21 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 已整合選取的 AWS Config 控制項，因此可以由 AWS Control Tower 檢視和管理。

如需詳細資訊，請參閱 AWS Control Tower 中可用的整合式 AWS Config 控制項

AWS Control Tower 改善勾點管理並新增主動控制區域

2024 年 11 月 20 日

(AWS Control Tower 登陸區域不需要更新。)

在此版本中，您可以利用 CloudFormation 勾點的完整容量，不受 AWS Control Tower 限制。此外，加拿大西部 （卡加利） 區域和亞太區域 （馬來西亞） 區域也提供主動控制。

先前，您環境中的所有 CloudFormation 勾點都需要受到 CT.CLOUDFORMATION.PR.1 控制項的保護，因此只有 AWS Control Tower 可以修改它們。在此版本中，您可以部署 CloudFormation 掛鉤並修改這些掛鉤，而不需要 AWS Control Tower 服務先前所需的限制。

如果您目前部署主動控制，您可以移至此改進的勾點功能。若要重設 OU 上的所有主動控制，請重設該 OU 上作用中的任何單一主動控制。您可以透過呼叫 `ResetEnabledControl` API，或從主控台使用重設功能更新控制項來執行重設。當您針對任何主動控制完成此重設任務時，AWS Control Tower 會將 OU 上的所有主動控制勾點移至新功能。針對部署主動控制的每個 OU 重複此程序。

重設任何主動控制後，請移除 AWS Control Tower OUs上的 CT.CLOUDFORMATION.PR.1 控制，除非您針對其他用途啟用該控制。如果您不關閉 CT.CLOUDFORMATION.PR.1 控制項，您將無法建立和修改其他勾 CloudFormation 點。

如需詳細資訊，請參閱更新主動控制勾點。

AWS Control Tower 啟動受管資源控制政策

2024 年 11 月 15 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 提供新類型的預防性控制，以資源控制政策 (RCPs實作。這些控制項可協助您在 AWS Control Tower 環境中建立資料周邊，保護您的資源免於意外存取。

例如，您可以為 Amazon S3、 AWS Security Token Service、Amazon SQS AWS Secrets Manager 和服務啟用 RCP AWS Key Management Service型控制。以 RCP 為基礎的控制項可以強制執行需求，例如「要求組織的 Amazon S3 資源只能由屬於組織的 IAM 主體或 AWS 服務存取」，無論個別儲存貯體政策授予的許可為何。

您可以設定新的 RCP 型控制項和某些現有的 SCP 型預防性控制項，以指定主體和資源的 AWS IAM 豁免。如果您不希望委託人或資源受控制項管理，您可以設定 豁免。

透過在 AWS Control Tower 中結合預防性、主動性和偵測性控制，您可以根據最佳實務監控多帳戶 AWS 環境是否安全和管理，例如AWS 基礎安全最佳實務標準。

這些新的 RCP 型預防性控制可在提供 AWS Control Tower AWS 區域 的 中使用。如需 AWS Control Tower 可用 AWS 區域 位置的完整清單，請參閱 AWS 區域 表格。

AWS Control Tower 報告控制政策偏離

2024 年 11 月 15 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 現在會報告控制政策偏離，適用於使用資源控制政策 (RCPs) 實作的控制，以及屬於 Security Hub CSPM 服務受管標準 AWS Control Tower 的控制。這種類型的偏離可以透過新的 `ResetEnabledControl` API 修復。如需詳細資訊，請參閱控管偏離的類型。

新的 **`ResetEnabledControl`** API

2024 年 11 月 14 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 推出新的 API，協助您以程式設計方式管理控制偏離。您可以修復控制項偏離，並將控制項重設為其預期的組態。`ResetEnabledControl` API 可與選用的 AWS Control Tower 控制項搭配使用，包括強烈建議和選擇性控制項。

控制例外狀況

- 使用此 API 無法重設使用服務控制政策 (SCPs) 實作的控制項。如需詳細資訊，請參閱`ResetEnabledControl`。
- 無法重設強制性控制，因為它們會保護 AWS Control Tower 資源。
- 登陸區域的區域拒絕控制必須透過 主控台重設。

控制偏離會在 AWS Control Tower 外部修改 AWS Control Tower 控制時發生，例如從 AWS Organizations 主控台。解決偏離有助於確保您符合控管要求。

控制目錄更新 **`GetControl`** API

2024 年 11 月 8 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 現在支援更新的 `GetControl` API，其中包含兩個新欄位：所有控制項`Parameters`的`Implementation`類型，以及可設定的特定控制項。

`GetControl` API 是 AWS Control Tower `controlcatalog`命名空間的一部分。

如需詳細資訊，請參閱 Control Catalog `GetControl API` 參考中的 API。

此版本包含 AWS Control Tower 主控台中顯示的相關變更。

- 所有現有的 AWS Security Hub CSPM 控制項都會將其`Implementation`參數值從 AWS Config 規則變更為 AWS Security Hub CSPM。修改對應的主控台說明面板以反映此變更。
- 所有現有的勾點控制項都會將其`Implementation`參數值從 CloudFormation 防護規則變更為 CloudFormation 勾點。修改對應的主控台說明面板以反映此變更。

AWS Control Tower AFT 支援 GitLab

2024 年 10 月 23 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 現在支援 GitLab™ TM和 GitLab 自我管理作為第三方版本控制系統 (VCS) 的選項，以及 Account Factory for Terraform (AFT) 的組態來源。

AWS 亞太區域 （馬來西亞） 區域提供 AWS Control Tower

2024 年 10 月 21 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 可在 AWS 亞太區域 （馬來西亞） 區域使用。

如需 AWS Control Tower 可用區域的完整清單，請參閱AWS 區域表。

AWS Control Tower 每個 OU 最多支援 1000 個帳戶

2024 年 8 月 30 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 已將每個組織單位 (OU) 允許的帳戶數目上限從 300 個增加到 1000 個。現在，您可以一次註冊最多 1000 AWS 帳戶 個 AWS Control Tower 控管，而無需變更您的 OU 結構。OU 註冊

和重新註冊程序也更有效率，因此將 AWS Control Tower 基準資源部署到您的帳戶所需的時間會明顯減少。

由於可用堆疊集數量 CloudFormation 的限制，某些帳戶限制仍然適用。具體而言，您可以註冊到 OU 的帳戶數量上限可能會有所不同，具體取決於您在控管下擁有的區域數量。若要進一步了解，請參閱《AWS Control Tower 使用者指南》中的以基礎 AWS 服務為基礎的限制。如需 AWS Control Tower 可用 AWS 區域 位置的完整清單，請參閱 AWS 區域 表格。

AWS Control Tower 新增登陸區域版本選擇

2024 年 8 月 15 日

(AWS Control Tower 登陸區域不需要更新。)

如果您執行的是 AWS Control Tower 登陸區域 3.1 版及更高版本，則可以更新或修復目前版本上的登陸區域，也可以升級至您選擇的版本。先前，任何登陸區域更新或修復都需要升級至最新的登陸區域版本。

透過選擇登陸區域版本，您可以在評估環境的潛在變更時，更靈活地規劃版本升級。您不需要選擇修復偏離以保持合規、更新您的登陸區域組態，或升級至最新的登陸區域版本。如果您執行的是登陸區域 3.1 版或更新版本，您可以選擇在更新或重設登陸區域組態時保持目前版本，或升級至較新版本。

可用的描述性控制 API，擴展對區域和控制項的存取

2024 年 8 月 6 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 新增了兩項新的 API 操作，可協助您以程式設計方式找到可用控制項的詳細資訊。此功能可讓您更輕鬆地透過自動化部署控制項。

- `GetControl` API 會傳回已啟用控制項的詳細資訊，包括目標識別符、控制項資訊摘要、目標區域清單，以及偏離狀態。
- `ListControls` API 會傳回 AWS Control Tower 控制庫中所有可用控制項的分頁清單。

這些 APIs 可透過 AWS Control Catalog 命名空間來存取。 AWS Control Catalog 是 AWS Control Tower 的一部分，其中包含可協助您管理其他服務的控制項 AWS ，而不只是 AWS Control Tower。此擴展的目錄會合併來自數個 AWS 服務的控制項，讓您可以根據一些常見的使用案例來檢視 AWS 控制項，例如：安全性、成本、耐用性和操作。如需詳細資訊，請參閱 Control Catalog API 參考。

擴充區域可用性

從此版本開始，您可以將 AWS Control Tower 控管 AWS 區域 延伸至某些已啟用 （ 已 ） 的控制項無法使用的地方。此外，您現在可以在更多區域中啟用特定控制項，即使並非所有受管區域都支援該控制項。

先前，當 AWS Control Tower 未在所有已啟用的控制項和受管區域中提供一致性時，AWS Control Tower 會阻止您將管控擴展到 區域或啟用控制。在此版本中，您擁有更多彈性，以及更多責任來確保您的組態適用於所有已啟用的控制項和所有受管區域。AWS Control Tower 控制項 APIs 和控制項目錄 APIs 可協助您取得受已啟用控制項保護 AWS 之區域的相關資訊，以及可能部署其他控制項的區域。區域和控制資訊也可在 AWS Control Tower 主控台中取得。

AWS Control Tower 在選擇加入區域中支援 AFT 和 CfCT

2024 年 7 月 18 日

(AWS Control Tower 登陸區域不需要更新。)

今天，AWS Control Tower 自訂架構 Account Factory for Terraform (AFT) 和 Customizations for AWS Control Tower (CfCT) 提供五個額外服務 AWS 區域：亞太區域 （ 海德拉巴、雅加達和大阪 ）、以色列 （ 特拉維夫 ） 和中東 （ 阿拉伯聯合大公國 ）。

Account Factory for Terraform (AFT) 會設定 Terraform 管道，協助您在 AWS Control Tower 中佈建和自訂帳戶。AWS Control Tower (CfCT) 的自訂功能可協助您使用 CloudFormation 範本和服務控制政策 (SCPs) 自訂 AWS Control Tower 登陸區域和帳戶。

若要進一步了解，請造訪 AWS Control Tower 使用者指南中的 Account Factory for Terraform and Customizations for AWS Control Tower 頁面。您也可以檢閱 AFT Github 頁面和 CfCT Github 頁面上的版本備註。所有 AWS 區域都支援 AFT 和 CfCT，但有一些例外狀況。如需詳細資訊，請參閱區域限制。

AWS Control Tower 新增 `ListLandingZoneOperations` API

2024 年 6 月 26 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 已新增 API，可讓您擷取最近套用至登陸區域的操作清單，以及目前進行中的操作。API 最多可以傳回登陸區域操作的歷史記錄及其識別符 90 天。如需使用範例，請參閱檢視登陸區域操作的狀態。

如需 ListLandingZoneOperations API 的詳細資訊，請參閱《AWS Control Tower API 參考ListLandingZoneOperations》中的 。

AWS Control Tower 最多支援 100 個並行控制操作

2024 年 5 月 20 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 現在支援具有較高並行的多個控制操作。您可以同時從主控台或使用 APIs 跨多個組織單位 (OUs) 提交最多 100 個 AWS Control Tower 控制操作。最多可同時執行十 (10) 個操作，其他操作則會排入佇列。透過這種方式，您可以跨多個 設定更標準化的組態 AWS 帳戶，而不需要重複控制操作的操作負擔。

若要監控進行中和佇列控制操作的狀態，您可以導覽至 AWS Control Tower 主控台中的新最近操作頁面，也可以呼叫新的 ListControlOperations API。

AWS Control Tower 程式庫包含超過 500 個控制項，對應至不同的控制目標、架構和服務。對於特定控制目標，例如靜態加密資料，您可以使用單一控制操作啟用多個控制項，以協助您實現目標。此功能有助於加速開發、更快速採用最佳實務控制，並減輕操作複雜性。

AWS Control Tower 可在 AWS 加拿大西部 （卡加利） 使用

2024 年 5 月 3 日

(AWS Control Tower 登陸區域不需要更新。)

從今天開始，您可以在加拿大西部 （卡加利） 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，您可以使用 AWS Control Tower 登陸區域 APIs 來執行此操作。或者，從主控台前往 AWS Control Tower 儀表板的設定頁面，選取您的區域，然後更新您的登陸區域。

加拿大西部 （卡加利） 區域不支援 AWS Service Catalog。因此，AWS Control Tower 的某些功能不同。最值得注意的功能變更是 Account Factory 無法使用。如果您選擇加拿大西部 （卡加利） 做為您的主要區域，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，都會與其他 區域中的程序不同。

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 外部建立帳戶，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。

Service Catalog APIs 不適用於加拿大西部（卡加利）區域。在 AWS Control Tower by Service Catalog APIs中自動化帳戶佈建中顯示的範例指令碼無法運作。

由於缺少 AWS Control Tower 的其他基礎相依性，Account Factory Customizations (AFC)、Account Factory for Terraform (AFT) 和 Customizations for AWS Control Tower (CfCT) 不適用於加拿大西部（卡加利）。如果您將控管延伸至加拿大西部（卡加利）區域，只要您的所在區域可使用 Service Catalog，您就可以繼續管理 AWS Control Tower 支援的所有區域中的 AFC 藍圖。

控制項

AWS Security Hub CSPM 服務受管標準的主動控制和控制：AWS Control Tower 不適用於加拿大西部（卡加利）區域。加拿大西部（卡加利）`CT.CLOUDFORMATION.PR.1` 無法使用預防性控制，因為只有在啟用以勾點為基礎的主動控制時才需要預防性控制。無法使用以 為基礎的某些偵測性控制項 AWS Config 。如需詳細資訊，請參閱控制限制。

身分提供者

IAM Identity Center 不適用於加拿大西部（卡加利）。最佳實務建議是在可使用 IAM Identity Center 的區域中設定登陸區域。或者，如果您在加拿大西部（卡加利）使用外部身分提供者，您可以選擇自行管理帳戶存取組態。

在加拿大西部（卡加利）區域無法使用 Service Catalog 不會影響 AWS Control Tower 支援的其他區域。這些差異僅適用於您的主要區域是加拿大西部（卡加利）。

如需 AWS Control Tower 可用區域的完整清單，請參閱AWS 區域表。

AWS Control Tower 支援自助式配額調整

2024 年 4 月 25 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 現在支援透過 Service Quotas 主控台進行自助式配額調整。如需詳細資訊，請參閱請求提高配額。

AWS Control Tower 發佈控制項參考指南

2024 年 4 月 21 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 發佈了控制項參考指南，這是一份新文件，您可以在其中找到 AWS Control Tower 環境特定控制項的詳細資訊。先前，此資料包含在 AWS Control Tower 使用者指南中。控制項參考指南涵蓋擴展格式的控制項。如需詳細資訊，請參閱 AWS Control Tower 控制項參考指南。

AWS Control Tower 會更新和重新命名兩個主動控制

2024 年 3 月 26 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 已重新命名兩個主動控制，以符合 Amazon OpenSearch Service 的更新。

- 【CT.OPENSEARCH.PR.8】 需要 Elasticsearch Service 網域才能使用 TLSv1.2
- 【CT.OPENSEARCH.PR.16 】 要求 Amazon OpenSearch Service 網域使用 TLSv1.2

我們更新了這兩個控制項的控制項名稱和成品，以符合 Amazon OpenSearch Service 的最新版本，現在支援 Transport Layer Security (TLS) 1.3 版的網域端點安全性傳輸安全選項。

為了新增對這些控制項的 TLSv1.3 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，您必須停用並啟用控制項以部署最新的成品。

此變更不會影響其他主動控制。我們建議您檢閱這些控制項，以確保它們符合您的控制目標。

如有問題或疑慮，請聯絡 AWS Support。

已棄用的控制項不再可用

2024 年 3 月 12 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 已棄用一些控制項。這些控制項不再可用。

- 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 支援在 中標記**EnabledControl**資源 CloudFormation

2024 年 2 月 22 日

(AWS Control Tower 登陸區域不需要更新。)

此 AWS Control Tower 版本會更新EnabledControl資源的行為，以更符合可設定的控制項，並改善透過自動化管理 AWS Control Tower 環境的能力。在此版本中，您可以透過 範本將標籤新增至可設定EnabledControl的資源 CloudFormation 。先前，您只能透過 AWS Control Tower 主控台和 APIs 新增標籤。

AWS Control Tower GetEnabledControl、 EnableControl和 ListTagsforResource API 操作會隨著此版本更新，因為它們依賴 EnabledControl 資源功能。

如需詳細資訊，請參閱CloudFormation 《 使用者指南》中的在 AWS Control Tower 中標記EnabledControl資源。 EnabledControl

AWS Control Tower 支援具有基準的 OU 註冊和組態 APIs

2024 年 2 月 14 日

(AWS Control Tower 登陸區域不需要更新。)

這些 APIs 支援使用 EnableBaseline呼叫進行程式設計 OU 註冊。當您在 OU 上啟用基準時，OU 中的成員帳戶會註冊到 AWS Control Tower 管控。某些注意事項可能適用。例如，透過 AWS Control Tower 主控台的 OU 註冊可啟用選用控制項以及強制性控制項。呼叫 APIs 時，您可能需要完成額外的步驟，才能啟用選用控制項。

AWS Control Tower 基準體現了 OU 和成員帳戶的 AWS Control Tower 控管最佳實務。例如，當您在 OU 上啟用基準時，OU 中的成員帳戶會收到定義的資源群組，包括 AWS CloudTrail、 AWS Config、IAM Identity Center 和必要的 AWS IAM 角色。

特定基準與特定 AWS Control Tower 登陸區域版本相容。當您變更登陸區域設定時，AWS Control Tower 可以將最新的相容基準套用至您的登陸區域。如需詳細資訊，請參閱OU 基準和登陸區域版本的相容性。

此版本包含四個必要的 基準類型

- `AWSControlTowerBaseline`
- `AuditBaseline`
- `LogArchiveBaseline`
- `IdentityCenterBaseline`

使用新的 APIs和定義的基準，您可以註冊 OUs並自動化 OU 佈建工作流程。APIs 也可以管理已在 AWS Control Tower 控管下的 OUs，因此您可以在登陸區域更新後重新註冊 OUs。APIs 包含 資源 CloudFormation `EnabledBaseline`的支援，可讓您使用基礎設施即程式碼 (IaC) 來管理 OUs。

基準 APIs

- 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：檢視特定基準操作的狀態。
- ResetEnabledBaseline：修復已啟用基準之 OU 上的資源偏離 （包括巢狀 OUs和強制控制偏離）。也修復landing-zone-level區域拒絕控制的偏離
- GetBaseline、ListBaselines：探索 AWS Control Tower 基準的內容。

若要進一步了解這些 APIs，請檢閱 AWS Control Tower 使用者指南中的基準，以及 API 參考。新的 APIs 可在提供 AWS Control Tower AWS 區域 的 中使用，但 GovCloud (US) 區域除外。如需 AWS Control Tower 可用 AWS 區域 位置的清單，請參閱 AWS 區域 表格。

2023 年 1 月至 12 月

2023 年，AWS Control Tower 發佈了下列更新：

- 轉換為新的 AWS Service Catalog 外部產品類型 （階段 3)
- AWS Control Tower 登陸區域 3.3 版
- 轉換為新的 AWS Service Catalog 外部產品類型 （階段 2)
- AWS Control Tower 宣布控制以協助數位主權
- AWS Control Tower 登陸區域 APIs
- AWS Control Tower 控制標記 APIs
- AWS 亞太區域 （墨爾本） 提供 AWS Control Tower

- 轉換為新的 AWS Service Catalog 外部產品類型 （階段 1)
- AWS Control Tower 新增新的控制 API
- AWS Control Tower 新增控制項
- AWS Control Tower 偵測受信任的存取偏離
- AWS Control Tower 提供四個額外的 AWS 區域
- AWS 以色列 （特拉維夫） 提供 AWS Control Tower
- AWS Control Tower 新增了 28 個新的主動控制
- AWS Control Tower 取代了兩個控制項
- AWS Control Tower 登陸區域 3.2 版
- AWS Control Tower 新增 IAM Identity Center email-to-ID 映射
- AWS Control Tower 新增更多 AWS Security Hub CSPM 控制項
- AWS Control Tower 發佈 AWS Security Hub CSPM 控制項的中繼資料
- AWS Control Tower 新增 Terraform 的帳戶工廠自訂 (AFC)
- AWS Control Tower 新增自我管理的 IAM 身分中心
- AWS Control Tower 新增混合控管備註
- AWS Control Tower 新增了新的主動控制
- AWS Control Tower 會更新 Amazon EC2 控制項
- AWS Control Tower 提供七種額外功能 AWS 區域
- AWS Control Tower 帳戶工廠自訂 (AFC) 和請求追蹤已全面推出
- AWS Control Tower 登陸區域 3.1 版
- AWS Control Tower 主動控制已全面推出

轉換為新的 AWS Service Catalog 外部產品類型 （階段 3)

2023 年 12 月 14 日

(AWS Control Tower 登陸區域不需要更新。)

在建立新的 時，AWS Control Tower 不再支援 Terraform Open Source 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，您只能更新或終止使用 Terraform 開放原始碼藍圖佈建的帳戶。

AWS Control Tower 登陸區域 3.3 版

2023 年 12 月 14 日

(AWS Control Tower 登陸區域需要更新至 3.3 版。 如需詳細資訊，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 部署在帳戶中的 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，只有在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。

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 值設定為您的組織 ID。此條件可確保 CloudTrail 只能代表您組織內的帳戶將日誌寫入 S3 儲存貯體；可防止組織外的 CloudTrail 日誌寫入 AWS Control Tower S3 儲存貯體。

我們進行了這項變更，以修復潛在的安全漏洞，而不會影響您現有工作負載的功能。若要檢視更新的政策，請參閱 稽核帳戶中的 Amazon S3 儲存貯體政策。

如需新條件索引鍵的詳細資訊，請參閱 IAM 文件和名為「使用可擴展控制項存取 資源 AWS 的服務」的 IAM 部落格文章。

AWS Config SNS 主題中的政策更新

我們已將新aws:SourceOrgID條件金鑰新增至 AWS Config SNS https：//topic.To 檢視更新政策的政策，請參閱 AWS Config SNS 主題政策。

對登陸區域區域拒絕控制的更新

- 已移除 discovery-marketplace:。此動作由aws-marketplace:*豁免涵蓋。
- 已新增 quicksight:DescribeAccountSubscription

更新 CloudFormation 範本

我們已更新名為 之堆疊的 CloudFormation 範本，BASELINE-CLOUDTRAIL-MASTER因此未使用 AWS KMS 加密時， 不會顯示偏離。

轉換為新的 AWS Service Catalog 外部產品類型 （ 階段 2)

2023 年 12 月 7 日

(AWS Control Tower 登陸區域不需要更新。)

HashiCorp 已更新其 Terraform 授權。因此，將對 Terraform Open Source 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。

若要避免中斷帳戶中的現有工作負載 AWS 和資源，請遵循 2023 年 12 月 14 日之前轉換為 AWS Service Catalog 外部產品類型的 AWS Control Tower 轉換步驟。

AWS Control Tower 宣布控制以協助數位主權

2023 年 11 月 27 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 宣布推出 65 項新 AWS受管控制項，協助您滿足數位主權需求。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動作，並偵測有關資料駐留、精細存取限制、加密和彈性功能的資源變更。這些控制項旨在讓您更輕鬆地大規模處理需求。如需數位主權控制的詳細資訊，請參閱增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彈性策略的控制項，例如需要 an AWS AppSync API 快取才能啟用傳輸中加密，或需要 AWS 跨多個可用區域部署 Network Firewall。您也可以自訂 AWS Control Tower 區域拒絕控制，以套用最符合您獨特業務需求的區域限制。

此版本帶來增強良好的 AWS Control Tower 區域拒絕功能。您可以在 OU 層級套用新的參數化區域拒絕控制，以提高控管的精細程度，同時在登陸區域層級維持額外的區域控管。此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的詳細資訊，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，可讓您將啟用的控制項重設為預設設定。此 API 在您需要快速解決偏離的使用案例中特別有用，或以程式設計方式保證控制項未處於偏離狀態。如需新 API 的詳細資訊，請參閱 AWS Control Tower API 參考

新的主動控制

- CT.APIGATEWAY.PR.6：要求 Amazon API Gateway REST 網域使用指定最低 TLS 通訊協定版本 TLSv1.2 的安全政策
- CT.APPSYNC.PR.2：要求以私有可見性設定 AWS AppSync GraphQL API
- CT.APPSYNC.PR.3：要求使用 API 金鑰來驗證 AWS AppSync GraphQL API
- CT.APPSYNC.PR.4：需要 AWS AppSync GraphQL API 快取才能啟用傳輸中加密。
- 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 Auto Scaling 啟動組態設定的 Amazon EBS 磁碟區，才能加密靜態資料 Auto Scaling
- CT.AUTOSCALING.PR.10：需要 Amazon EC2 Auto Scaling 群組在覆寫啟動範本時僅使用 AWS Nitro 執行個體類型
- CT.AUTOSCALING.PR.11：在覆寫啟動範本時，只需要支援執行個體之間網路流量加密的 AWS Nitro 執行個體類型，即可新增至 Amazon EC2 Auto Scaling 群組
- CT.DAX.PR.3：要求 DynamoDB Accelerator 叢集使用 Transport Layer Security (TLS) 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，需要 Amazon EC2 執行個體使用 AWS Nitro 執行個體類型
- CT.EC2.PR.16：使用 AWS `AWS::EC2::Instance` 資源類型建立時，需要 Amazon EC2 執行個體使用 Nitro 執行個體類型
- CT.EC2.PR.17：需要 Amazon EC2 專用主機才能使用 AWS Nitro 執行個體類型
- CT.EC2.PR.18：要求 Amazon EC2 機群僅使用 AWS Nitro 執行個體類型覆寫這些啟動範本
- CT.EC2.PR.19：要求 Amazon EC2 執行個體使用 nitro 執行個體類型，以便在使用 `AWS::EC2::Instance` 資源類型建立時支援執行個體之間的傳輸中加密
- CT.EC2.PR.20：要求 Amazon EC2 機群僅使用支援執行個體之間傳輸中加密的 AWS Nitro 執行個體類型來覆寫這些啟動範本
- CT.ELASTICACHE.PR.8：需要較新 Redis 版本的 Amazon ElastiCache 複寫群組，才能啟用 RBAC 身分驗證
- CT.MQ.PR.1：要求 Amazon MQ ActiveMQ 代理程式使用作用中/待命部署模式以獲得高可用性
- CT.MQ.PR.2：需要 Amazon MQ Rabbit MQ 代理程式使用多可用區域叢集模式以獲得高可用性
- CT.MSK.PR.1：需要 Amazon Managed Streaming for Apache Kafka (MSK) 叢集，才能強制執行叢集代理程式節點之間的傳輸中加密
- CT.MSK.PR.2：需要將 Amazon Managed Streaming for Apache Kafka (MSK) 叢集設定為已停用 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 Transport Layer Security (TLS) 連線
- CT.RDS.PR.27：要求 Amazon RDS 資料庫叢集參數群組針對支援的引擎類型要求 Transport Layer Security (TLS) 連線
- CT.RDS.PR.28：要求 Amazon RDS 資料庫參數群組針對支援的引擎類型要求 Transport Layer Security (TLS) 連線

- CT.RDS.PR.29：需要未將 Amazon RDS 叢集設定為可透過 'PubliclyAccessible' 屬性公開存取
- CT.RDS.PR.30：要求 Amazon RDS 資料庫執行個體已將靜態加密設定為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 存取點具有封鎖公開存取 (BPA) 組態，且所有選項都設為 true

新的預防性控制

- CT.APPSYNC.PV.1 需要以私有可見性設定 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 要求不呼叫 Amazon EBS APIs
- CT.EC2.PV.5 不允許使用 Amazon EC2 VM 匯入和匯出
- CT.EC2.PV.6 不允許使用已棄用的 Amazon EC2 RequestSpotFleet 和 RequestSpotInstances API 動作
- CT.KMS.PV.1 需要 AWS KMS 金鑰政策，才能擁有將 AWS KMS 授予建立限制為 AWS 服務的陳述式
- CT.KMS.PV.2 要求具有用於加密之 RSA 金鑰材料 AWS KMS 的非對稱金鑰的金鑰長度不為 2048 位元
- CT.KMS.PV.3 要求在啟用略過政策鎖定安全檢查的情況下設定 AWS KMS 金鑰
- CT.KMS.PV.4 要求使用源自 AWS CloudHSM 的金鑰材料來設定 AWS KMS 客戶受管金鑰 (CMK)
- CT.KMS.PV.5 要求使用匯入的金鑰材料設定 AWS KMS 客戶受管金鑰 (CMK)
- CT.KMS.PV.6 要求使用源自外部金鑰存放區 (XKS) 的金鑰材料來設定 AWS KMS 客戶受管金鑰 (CMK)
- CT.LAMBDA.PV.1 需要 AWS Lambda 函數 URL 才能使用 AWS IAM 型身分驗證
- CT.LAMBDA.PV.2 需要將 AWS Lambda 函數 URL 設定為僅供 中的主體存取 AWS 帳戶

AWS Control Tower 登陸區域 APIs

2023 年 11 月 26 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 現在提供 APIs，可協助您以程式設計方式管理登陸區域。這些 APIs 可讓您建立、更新和重設登陸區域，以及擷取登陸區域組態和操作的相關資訊。如需詳細資訊，請參閱登陸區域 API 範例。

登陸區域 APIs 可在 AWS Control Tower 提供的所有 AWS 區域 中使用，但 GovCloud (US) 區域除外。如需 AWS Control Tower 可用 AWS 區域 位置的清單，請參閱 AWS 區域 表格。

AWS Control Tower 控制標記 APIs

2023 年 11 月 10 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 現在提供 APIs，可協助您以程式設計方式標記已啟用的控制項。這些 APIs 可讓您新增、移除和列出已啟用控制項的標籤。如需詳細資訊，請參閱標記 AWS Control Tower 資源。

除了 GovCloud (US) 區域外，控制項標記 APIs 可在 AWS Control Tower AWS 區域 提供的所有 中使用。如需 AWS Control Tower 可用 AWS 區域 位置的清單，請參閱 AWS 區域 表格。

AWS 亞太區域 （墨爾本） 提供 AWS Control Tower

2023 年 11 月 3 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 可在亞太區域 （墨爾本） 使用。如需 AWS Control Tower 可用區域的完整清單，請參閱 AWS 區域 表格。

轉換為新的 AWS Service Catalog 外部產品類型 （階段 1)

2023 年 10 月 31 日

(AWS Control Tower 登陸區域不需要更新。)

HashiCorp 已更新其 Terraform 授權。因此，將對 Terraform Open Source 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。

為避免中斷您帳戶中的現有工作負載 AWS 和資源，請遵循 2023 年 12 月 14 日之前轉移至 AWS Service Catalog 外部產品類型的 AWS Control Tower 轉換步驟。

AWS Control Tower 新增新的控制 API

2023 年 10 月 27 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 現在提供新的 API `UpdateEnabledControl`，可讓您更新已啟用的控制項。此 API 在您需要快速解決偏離的使用案例中特別有用，或以程式設計方式保證控制項未處於偏離狀態。如需新 API 的詳細資訊，請參閱 AWS Control Tower API 參考。

除了 GovCloud (US) 區域外，`UpdateEnabledControl`API 可在 AWS Control Tower AWS 區域 提供的所有 中使用。如需 AWS Control Tower 可用位置的 AWS 區域 清單，請參閱 AWS 區域 表格。

AWS Control Tower 新增控制項

2023 年 10 月 20 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 已將 22 個新控制項新增至 AWS Control Tower 控制項程式庫。這些控制項可協助您強制執行 AWS 資源的最佳實務。如需新控制項的詳細資訊，請參閱控制類別。

新的控制項可在 AWS Control Tower 提供的所有 AWS 區域 中使用。如需 AWS Control Tower 可用 AWS 區域 位置的清單，請參閱 AWS 區域 表格。

AWS Control Tower 偵測受信任的存取偏離

2023 年 10 月 13 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 現在可偵測並報告受信任存取設定的偏離。信任的存取設定可讓 AWS Control Tower 代表您與其他 AWS 服務互動。如果在 AWS Control Tower 之外變更這些設定，AWS Control Tower 會偵測偏離，並在 AWS Control Tower 主控台中回報。如需受信任存取偏離的詳細資訊，請參閱控管偏離的類型。

信任的存取偏離偵測可在 AWS Control Tower 提供的所有 AWS 區域 中使用。如需 AWS Control Tower 可用 AWS 區域 位置的清單，請參閱 AWS 區域 表格。

AWS Control Tower 提供四個額外的 AWS 區域

2023 年 9 月 29 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 提供四個額外服務 AWS 區域：亞太區域（海德拉巴）、亞太區域（雅加達）、歐洲（西班牙）和歐洲（蘇黎世）。如需 AWS Control Tower 可用區域的完整清單，請參閱 AWS 區域 表格。

AWS 以色列（特拉維夫）提供 AWS Control Tower

2023 年 8 月 1 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 可在以色列（特拉維夫）使用。如需 AWS Control Tower 可用區域的完整清單，請參閱 AWS 區域 表格。

AWS Control Tower 新增了 28 個新的主動控制

2023 年 7 月 27 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 已將 28 個新的主動控制新增至 AWS Control Tower 控制庫。這些控制項可協助您強制執行 AWS 資源的最佳實務。如需新控制項的詳細資訊，請參閱控制項類別。

新的控制項可在 AWS Control Tower 提供的所有 AWS 區域 中使用。如需 AWS Control Tower 可用 AWS 區域 位置的清單，請參閱 AWS 區域 表格。

AWS Control Tower 取代了兩個控制項

2023 年 7 月 27 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 已棄用兩個控制項： CT.CLOUDFORMATION.PR.2和 CT.CLOUDFORMATION.PR.3。這些控制項不再可在 AWS Control Tower 控制項程式庫中使用。如需已棄用控制項的詳細資訊，請參閱控制項類別。

已棄用的控制項不再可用於任何 AWS 區域。

AWS Control Tower 登陸區域 3.2 版

2023 年 6 月 16 日

(AWS Control Tower 登陸區域需要更新至 3.2 版。 如需詳細資訊，請參閱 更新您的登陸區域)。

AWS Control Tower 登陸區域 3.2 版將屬於 AWS Security Hub CSPM 服務受管標準：AWS Control Tower 的控制項帶入一般可用性。它引入了在 AWS Control Tower 主控台中檢視屬於此標準一部分之控制項偏離狀態的功能。

此更新包含新的服務連結角色 (SLR)，稱為 AWSServiceRoleForAWSControlTower。此角色透過在每個成員帳戶中建立名為 AWSControlTowerManagedRule 的 EventBridge 受管規則來協助 AWS Control Tower。 AWSControlTowerManagedRule 此受管規則會從 使用 AWS Control Tower 收集 AWS Security Hub CSPM 尋找事件，以判斷控制偏離。

此規則是 AWS Control Tower 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 APIs 部署。您可以在 EventBridge 主控台中或透過 EventBridge APIs來檢視規則。如果已填入 `managed-by` 欄位，則會顯示 AWS Control Tower 服務主體。

先前，AWS Control Tower 擔任 AWSControlTowerExecution 角色，以在成員帳戶中執行操作。這個新角色和規則更符合在多帳戶 AWS 環境中執行操作時允許最低權限的最佳實務原則。新角色提供明確允許的縮小範圍許可：在成員帳戶中建立受管規則、維護受管規則、透過 SNS 發佈安全通知，以及驗證偏離。如需詳細資訊，請參閱AWSServiceRoleForAWSControlTower。

登陸區域 3.2 更新也包含管理帳戶中的新 StackSet 資源，`BP_BASELINE_SERVICE_LINKED_ROLE`最初會部署服務連結角色。

報告 Security Hub CSPM 控制偏離時（在登陸區域 3.2 和更新版本中），AWS Control Tower 會收到 Security Hub CSPM 的每日狀態更新。雖然控制在每個受管區域中都是作用中的，但 AWS Control Tower 只會將 AWS Security Hub CSPM 尋找事件傳送至 AWS Control Tower 主區域。如需詳細資訊，請參閱 Security Hub 控制偏離報告。

區域拒絕控制項的更新

此登陸區域版本也包含區域拒絕控制的更新。

已新增全域服務和 APIs

- AWS 帳單與成本管理 (`billing:*`)
- AWS CloudTrail (`cloudtrail:LookupEvents`) 以允許成員帳戶中全域事件的可見性。
- AWS 合併帳單 (`consolidatedbilling:*`)
- AWS 管理主控台行動應用程式 (`consoleapp:*`)
- AWS 免費方案 (`freetier:*`)
- AWS Invoicing (`invoicing:*`)
- AWS IQ (`iq:*`)

- AWS 使用者通知 (`notifications:*`)
- AWS 使用者通知聯絡人 (`notifications-contacts:*`)
- Amazon Payments (`payments:*`)
- AWS 稅務設定 (`tax:*`)

已移除全域服務和 APIs

- 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 新增 IAM Identity Center email-to-ID 映射

2023 年 7 月 13 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 現在支援 IAM Identity Center email-to-ID 映射。此功能可讓您將電子郵件地址映射至 IAM Identity Center 使用者 IDs，讓您更輕鬆地管理使用者存取您的 AWS Control Tower 環境。如需email-to-ID映射的詳細資訊，請參閱與 IAM Identity Center 整合。

Email-to-ID映射可在 AWS Control Tower 提供的所有 AWS 區域 中使用。如需 AWS Control Tower 可用 AWS 區域 位置的清單，請參閱 AWS 區域 表格。

AWS Control Tower 新增更多 AWS Security Hub CSPM 控制項

2023 年 6 月 29 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 已將更多 AWS Security Hub CSPM 控制項新增至 AWS Control Tower 控制項程式庫。這些控制項可協助您強制執行 AWS 資源的最佳實務。如需新控制項的詳細資訊，請參閱控制項類別。

新的控制項可在 AWS Control Tower 可用的所有 AWS 區域 中使用。如需 AWS Control Tower 可用 AWS 區域 位置的清單，請參閱 AWS 區域 表格。

AWS Control Tower 發佈 AWS Security Hub CSPM 控制項的中繼資料

2023 年 6 月 22 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 現在會發佈 AWS Security Hub CSPM 控制項的中繼資料。此中繼資料包含控制項的相關資訊，例如控制項 ID、控制項標題和控制項描述。如需中繼資料的詳細資訊，請參閱控制中繼資料。

控制中繼資料可在 AWS Control Tower 提供的所有 AWS 區域 中使用。如需 AWS Control Tower 可用 AWS 區域 位置的清單，請參閱 AWS 區域 表格。

AWS Control Tower 新增 Terraform 的帳戶工廠自訂 (AFC)

2023 年 6 月 15 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 現在支援 Terraform 的帳戶工廠自訂 (AFC)。此功能可讓您使用 Terraform 來自訂 AWS Control Tower 帳戶。如需適用於 Terraform 的 AFC 的詳細資訊，請參閱適用於 Terraform 的帳戶工廠自訂。

AWS Control Tower 提供的所有 都提供適用於 Terraform 的 AWS 區域 AFC。如需 AWS Control Tower 可用 AWS 區域 位置的清單，請參閱 AWS 區域 表格。

AWS Control Tower 新增自我管理的 IAM 身分中心

2023 年 6 月 8 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 現在支援自我管理的 IAM 身分中心。此功能可讓您將自己的身分提供者與 AWS Control Tower 搭配使用。如需自我管理 IAM 身分中心的詳細資訊，請參閱 IAM 身分中心。

自我管理的 IAM 身分中心可在 AWS Control Tower 提供的所有 AWS 區域 中使用。如需 AWS Control Tower 可用 AWS 區域 位置的清單，請參閱 AWS 區域 表格。

AWS Control Tower 新增混合控管備註

2023 年 6 月 1 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 現在包含混合控管的注意事項。此備註說明 AWS Control Tower 如何與其他 AWS 服務搭配使用，為您的 AWS 資源提供控管。如需混合控管的詳細資訊，請參閱混合控管。

混合控管備註可在 AWS Control Tower 提供的所有 AWS 區域 中使用。如需 AWS Control Tower 可用 AWS 區域 位置的清單，請參閱 AWS 區域 表格。

AWS Control Tower 新增了新的主動控制

2023 年 5 月 25 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 已將新的主動控制新增至 AWS Control Tower 控制庫。這些控制項可協助您強制執行 AWS 資源的最佳實務。如需新控制項的詳細資訊，請參閱控制項類別。

新的控制項可在 AWS Control Tower 可用的所有 AWS 區域 中使用。如需 AWS Control Tower 可用 AWS 區域 位置的清單，請參閱 AWS 區域 表格。

AWS Control Tower 會更新 Amazon EC2 控制項

2023 年 5 月 18 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 已更新 AWS Control Tower 控制庫中的 Amazon EC2 控制。這些更新可改善 AWS Control Tower 環境的安全性和可靠性。如需更新控制項的詳細資訊，請參閱控制項類別。

更新後的控制項可在 AWS Control Tower 可用的所有 AWS 區域 中使用。如需 AWS Control Tower 可用 AWS 區域 位置的清單，請參閱 AWS 區域 表格。

AWS Control Tower 提供七種額外功能 AWS 區域

2023 年 5 月 11 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 提供七種額外服務 AWS 區域：亞太區域 （大阪）、加拿大 （中部）、歐洲 （米蘭）、歐洲 （斯德哥爾摩）、中東 （巴林）、中東 （阿拉伯聯合大公國） 和南美洲 （聖保羅）。如需 AWS Control Tower 可用區域的完整清單，請參閱 AWS 區域 表格。

AWS Control Tower 帳戶工廠自訂 (AFC) 和請求追蹤已全面推出

2023 年 4 月 27 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 帳戶工廠自訂 (AFC) 和請求追蹤現已正式推出。AFC 可讓您自訂 AWS Control Tower 帳戶，而請求追蹤可讓您追蹤 AWS Control Tower 請求的狀態。如需 AFC 和請求追蹤的詳細資訊，請參閱帳戶工廠自訂和請求追蹤。

AFC 和請求追蹤可在 AWS Control Tower 提供的所有 AWS 區域 中使用。如需 AWS Control Tower 可用 AWS 區域 位置的清單，請參閱 AWS 區域 表格。

AWS Control Tower 登陸區域 3.1 版

2023 年 2 月 9 日

(AWS Control Tower 登陸區域需要更新至 3.1 版。 如需詳細資訊，請參閱 更新您的登陸區域)

AWS Control Tower 登陸區域 3.1 版包含下列更新：

- 在此版本中，AWS Control Tower 會停用存取記錄儲存貯體的不必要存取記錄，這是 Amazon S3 儲存貯體，其中存取日誌存放在日誌封存帳戶中，同時繼續啟用 S3 儲存貯體的伺服器存取記錄。此版本也包含區域拒絕控制項的更新，允許對 全域服務執行其他動作，例如 支援 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 CSPM 為日誌封存帳戶的存取記錄儲存貯體建立調查結果，因為 AWS Security Hub CSPM 規則，所以應該啟用【S3.9】 S3 儲存貯體伺服器存取記錄。為了與 Security Hub CSPM 保持一致，我們建議您隱藏此特定調查結果，如此規則的 Security Hub CSPM 描述中所述。如需詳細資訊，請參閱隱藏問題清單的相關資訊。
- Log Archive 帳戶中 （ 一般 ） 記錄儲存貯體的存取記錄在 3.1 版中保持不變。為了符合最佳實務，該儲存貯體的存取事件會記錄為存取記錄儲存貯體中的日誌項目。如需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記錄來記錄請求。
- 我們已更新區域拒絕控制。此更新允許更多全域服務執行動作。如需此 SCP 的詳細資訊，請參閱AWS 根據請求拒絕存取 AWS 區域和增強資料駐留保護的控制項。

  已新增全域服務：

  - AWS 帳戶管理 (`account:*`)
  - AWS 啟用 (`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:PutMultiRegionA`
- AWS Savings Plans (`savingsplans:*`)
- IAM Identity Center (`sso:*`)
- AWS Support App (`supportapp:*`)
- 支援 計劃 (`supportplans:*`)
- AWS 永續性 (`sustainability:*`)
- AWS Resource Groups Tagging API (`tag:GetResources`)
- AWS Marketplace Vendor Insights (`vendor-insights:ListEntitledSecurityProfiles`)

AWS Control Tower 主動控制已全面推出

2023 年 4 月 13 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 主動控制現已全面推出。主動式控制可協助您強制執行 AWS 資源的最佳實務。如需主動控制的詳細資訊，請參閱主動控制。

主動控制可在 AWS Control Tower 提供的所有 AWS 區域 中使用。如需 AWS Control Tower 可用 AWS 區域 位置的清單，請參閱 AWS 區域 表格。

2022 年 1 月至 12 月

在 2022 年，AWS Control Tower 發佈了下列更新：

- 並行帳戶操作
- 帳戶工廠自訂 (AFC)

- 全方位控制可協助 AWS 資源佈建和管理
- 所有 AWS Config 規則都可檢視的合規狀態
- 用於控制項和新 CloudFormation 資源的 API
- CfCT 支援堆疊集刪除
- 自訂日誌保留
- 角色偏離修復可用
- AWS Control Tower 登陸區域 3.0 版
- 組織頁面結合 OUs和帳戶的檢視
- 簡化帳戶建立和註冊
- AFT 支援共用 AWS Control Tower 帳戶的自動自訂
- 所有選用控制項的並行操作
- 現有的安全性和記錄帳戶
- AWS Control Tower 登陸區域 2.9 版
- AWS Control Tower 登陸區域 2.8 版

並行帳戶操作

2022 年 12 月 16 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 現在支援帳戶工廠中的並行動作。您一次最多可以建立、更新或註冊五 (5) 個帳戶。連續提交最多五個動作，並檢視每個請求的完成狀態，同時您的帳戶在背景完成建置。例如，在更新另一個帳戶之前，或重新註冊整個組織單位 (OU) 之前，您不再需要等待每個程序完成。

帳戶工廠自訂 (AFC)

2022 年 11 月 28 日

(AWS Control Tower 登陸區域不需要更新。)

帳戶原廠自訂可讓您從 AWS Control Tower 主控台自訂新的和現有的帳戶。這些新的自訂功能可讓您靈活地定義帳戶藍圖，這些藍圖是包含在專業 Service Catalog 產品中的 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。

先前，AWS Control Tower 帳戶工廠不支援在 主控台中自訂帳戶。透過此帳戶工廠的更新，您可以預先定義帳戶需求，並將其實作為明確定義工作流程的一部分。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。

當您在帳戶工廠中佈建、註冊或更新帳戶時，您將選取要部署的藍圖。藍圖中指定的資源會在您的帳戶中佈建。當您的帳戶完成建置時，所有自訂組態都可以立即使用。

若要開始使用自訂帳戶，您可以在 Service Catalog 產品中定義預期使用案例的資源。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，請參閱使用帳戶工廠自訂 (AFC) 自訂帳戶。

全方位控制可協助 AWS 資源佈建和管理

2022 年 11 月 28 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 現在支援全面的控制管理，包括透過 CloudFormation 勾點實作的全新選用主動控制。這些控制項稱為主動，因為它們會在部署資源之前檢查您的資源，以判斷新資源是否符合您環境中啟用的控制項。

超過 130 種新的主動控制可協助您達成 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，以及管理超過 20 種其他 AWS 服務的 AWS Control Tower 互動。

AWS Control Tower 控制程式庫會根據相關聯的 AWS 服務和資源來分類這些控制。如需詳細資訊，請參閱主動控制。

在此版本中，AWS Control Tower 也 AWS Security Hub CSPM透過支援 AWS 基礎安全最佳實務 (FSBP) 標準的新 Security Hub CSPM 服務受管標準整合：AWS Control Tower。您可以在主控台中檢視超過 160 個 Security Hub CSPM 控制項以及 AWS Control Tower 控制項，而且您可以取得 AWS Control Tower 環境的 Security Hub CSPM 安全分數。如需詳細資訊，請參閱 Security Hub 控制項。

所有 AWS Config 規則都可檢視的合規狀態

2022 年 11 月 18 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 現在會顯示部署到向 AWS Control Tower 註冊之組織單位的所有 AWS Config 規則的合規狀態。您可以在 AWS Control Tower 中檢視影響您帳戶的所有 AWS Config 規則的合規狀態、已註冊或未註冊，而無需在 AWS Control Tower 主控台外部導覽。客戶可以選擇在 AWS Control

Tower 中設定稱為偵測控制項的 Config 規則，或透過 AWS Config 服務直接設定規則。 AWS Config 隨即顯示 所部署的規則，以及 AWS Control Tower 所部署的規則。

先前，透過 AWS Config 服務部署的 AWS Config 規則在 AWS Control Tower 主控台中看不到。客戶必須導覽至 AWS Config 服務，才能識別不合規的 AWS Config 規則。現在，您可以在 AWS Control Tower 主控台中識別任何不合規的 AWS Config 規則。若要檢視所有 Config 規則的合規狀態，請導覽至 AWS Control Tower 主控台中的帳戶詳細資訊頁面。您將看到清單，其中顯示 AWS Control Tower 管理的控制項合規狀態，以及部署在 AWS Control Tower 外部的 Config 規則。

用於控制項和新 CloudFormation 資源的 API

2022 年 9 月 1 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 現在支援透過一組 API 呼叫對控制項進行程式設計管理，也稱為護欄。新 CloudFormation 資源支援 控制項的 API 功能。如需詳細資訊，請參閱自動化 AWS Control Tower 中的任務和使用 建立 AWS Control Tower 資源 AWS CloudFormation。

這些 APIs 可讓您在 AWS Control Tower 程式庫中啟用、停用和檢視控制項的應用程式狀態。APIs 包含 的支援 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性控制，可表達您對整個組織單位 (OU) 和 OU 內每個 AWS 帳戶的政策意圖。當您建立新帳戶或變更現有帳戶時，這些規則仍然有效。

此版本中包含APIs

- EnableControl – 此 API 呼叫會啟用控制項。它會啟動非同步操作，在指定的組織單位及其包含的帳戶上建立 AWS 資源。
- DisableControl – 此 API 呼叫會關閉控制項。它會啟動非同步操作，刪除 AWS 指定組織單位及其包含的帳戶上的資源。
- GetControlOperation – 傳回特定 EnableControl 或 DisableControl 操作的狀態。
- ListEnabledControls – 列出 AWS Control Tower 在指定組織單位及其包含的帳戶上啟用的控制項。

若要檢視選用控制項的控制項名稱清單，請參閱《AWS Control Tower 使用者指南》中的 APIs 和控制項的資源識別符。

CfCT 支援堆疊集刪除

2022 年 8 月 26 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower (CfCT) 的自訂現在支援堆疊集刪除，方法是在 `manifest.yaml` 檔案中設定 參數。如需詳細資訊，請參閱刪除堆疊集。

> **Important**
>
> 當您最初將 的值設定為 `enable_stack_set_deletion` `true`時，下次叫用 CfCT 時，所有以字首 開頭`CustomControlTower-`、具有關聯索引鍵標籤 `Key:AWS_Solutions, Value: CustomControlTowerStackSet`且未在資訊清單檔案中宣告的資源都會暫存以供刪除。

自訂日誌保留

2022 年 8 月 15 日

(AWS Control Tower 登陸區域需要更新。 如需詳細資訊，請參閱 更新您的登陸區域)

AWS Control Tower 現在能夠為存放 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，以天數或年為單位遞增，最長可達 15 年。

如果您選擇不自訂日誌保留，則標準帳戶記錄的預設設定為 1 年，存取記錄的預設設定為 10 年。

當您更新或修復登陸區域時，此功能可透過 AWS Control Tower 提供給現有客戶，並透過 AWS Control Tower 設定提供給新客戶使用

角色偏離修復可用

2022 年 8 月 11 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 現在支援角色偏離的修復。您可以還原必要的角色，而無需完全修復您的登陸區域。如果需要這種類型的偏離修復，主控台錯誤頁面會提供還原角色的步驟，讓您的登陸區域再次可用。

AWS Control Tower 登陸區域 3.0 版

2022 年 7 月 29 日

(AWS Control Tower 登陸區域需要更新至 3.0 版。 如需詳細資訊，請參閱 更新您的登陸區域)

AWS Control Tower 登陸區域 3.0 版包含下列更新：

- 選擇組織層級 AWS CloudTrail 追蹤的選項，或選擇退出 AWS Control Tower 管理的 CloudTrail 追蹤。
- 兩個新的偵測性控制，用於判斷 AWS CloudTrail 是否在帳戶中記錄活動。
- 僅彙總您主要區域中全域資源 AWS Config 相關資訊的選項。
- 區域拒絕控制的更新。
- 受管政策 AWSControlTowerServiceRolePolicy 的更新。
- 我們不再在每個註冊`aws-controltower/CloudTrailLogs`帳戶中建立 IAM 角色`aws-controltower-CloudWatchLogsRole`和 CloudWatch 日誌群組。先前，我們在每個帳戶中為其帳戶追蹤建立這些項目。使用組織追蹤，我們只會在管理帳戶中建立一個。

下列各節提供每個新功能的詳細資訊。

AWS Control Tower 中的組織層級 CloudTrail 追蹤

使用登陸區域 3.0 版，AWS Control Tower 現在支援組織層級 AWS CloudTrail 追蹤。

當您將 AWS Control Tower 登陸區域更新至 3.0 版時，您可以選擇組織層級 AWS CloudTrail 追蹤做為您的記錄偏好設定，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 小時等待期間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。在極少數情況下，您的登陸區域更新未成功，但失敗發生在 AWS Control Tower 已建立組織層級追蹤之後，您可能需要支付組織層級和帳戶層級追蹤的重複費用，直到更新操作能夠成功完成為止。

從登陸區域 3.0 開始，AWS Control Tower 不再支援 AWS 管理的帳戶層級追蹤。反之，AWS Control Tower 會根據您的選擇，建立處於作用中或非作用中的組織層級追蹤。

> **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。

您的彙總帳戶日誌不會遺失記錄資料，因為日誌會保留在存放它們的現有 Amazon S3 儲存貯體中。只會刪除線索，不會刪除現有的日誌。如果您選擇新增組織層級追蹤的選項，AWS Control Tower 會開

啟您 Amazon S3 儲存貯體中新資料夾的新路徑，並繼續將記錄資訊傳送至該位置。如果您選擇退出 AWS Control Tower 管理的線索，您現有的日誌會保留在儲存貯體中，保持不變。

日誌儲存的路徑命名慣例

- 帳戶追蹤日誌的儲存路徑如下：`/org id/AWSLogs/…`
- 組織追蹤日誌的儲存路徑如下：`/org id/AWSLogs/org id/…`

AWS Control Tower 為您的組織層級 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，請參閱尋找您的 CloudTrail 日誌檔案。

> **Tip**
>
> 如果您打算建立和管理自己的帳戶層級線索，建議您先建立新的線索，然後再完成 AWS Control Tower 登陸區域 3.0 版的更新，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，並自行管理它們。在 3.0 版或更新版本的任何登陸區域更新期間，可以選擇由 AWS Control Tower 管理的組織層級 CloudTrail 追蹤。每當您更新登陸區域時，您可以選擇加入和退出組織層級的線索。

如果您的日誌是由第三方服務管理，請務必為您的服務提供新的路徑名稱。

> **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，也可以選擇加入由 AWS Control Tower 管理的組織層級追蹤。

僅記錄主要區域中 AWS Config 的資源

在登陸區域 3.0 版中，AWS Control Tower 已更新 的基準組態， AWS Config 以便只記錄主要區域中的全域資源。更新至 3.0 版之後，僅在您的主區域中啟用全域資源的資源記錄。

此組態視為最佳實務。它由 AWS Security Hub CSPM 和 建議 AWS Config，並透過減少建立、修改或刪除全域資源時建立的組態項目數量來節省成本。先前，每次建立、更新或刪除全域資源時，無論是由客戶還是由 AWS 服務，都會為每個受管區域中的每個項目建立組態項目。

記錄的 AWS CloudTrail 兩個新偵測控制項

作為組織層級 AWS CloudTrail 追蹤變更的一部分，AWS Control Tower 正在引入兩個新的偵測性控制項，以檢查 CloudTrail 是否已啟用。第一個控制項具有強制性指導，並在 3.0 和更新版本的設定或登陸區域更新期間，在安全 OU 上啟用。第二個控制項具有強烈建議的指導，並且可選擇性地套用到安全 OUs 以外的任何 OU，該安全 OU 已強制執行強制性控制保護。

強制性控制：偵測安全組織單位下的共用帳戶是否已啟用 AWS CloudTrail 或 CloudTrail Lake

強烈建議的控制：偵測帳戶是否已啟用 AWS CloudTrail 或 CloudTrail Lake

如需新控制項的詳細資訊，請參閱 AWS Control Tower 控制項程式庫。

區域拒絕控制的更新

我們更新了區域拒絕控制中的 NotAction 清單，以包含一些其他服務的動作，如下所示：

```
        "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

此影片 (3：07) 說明如何將現有的 AWS Control Tower 登陸區域更新為第 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 登陸區域更新為登陸區域 3 的影片逐步解說。

組織頁面結合 OUs和帳戶的檢視

2022 年 7 月 18 日

(AWS Control Tower 登陸區域不需要更新）

AWS Control Tower 中的新組織頁面會顯示所有組織單位 (OUs) 和帳戶的階層（樹）檢視。它結合了來自先前存在OUs 和帳戶頁面的資訊。

在新頁面上，您可以看到父 OUs 與其巢狀 OUs 和帳戶之間的關係，您可以對資源分組採取動作。您可以設定頁面檢視。例如，您可以展開或摺疊階層檢視、篩選檢視以僅查看帳戶或 OUs、選擇僅檢視已註冊帳戶和已註冊OUs，或者您可以檢視相關資源的群組。更容易確保整個組織正確更新。

簡化帳戶建立和註冊

2022 年 6 月 30 日

(AWS Control Tower 登陸區域不需要更新。)

AWS Control Tower 現在提供建立和註冊帳戶的簡化工作流程。您可以在單一工作流程中建立新帳戶或註冊現有帳戶，而無需導覽至 Service Catalog 主控台。如需詳細資訊，請參閱從 AWS Control Tower 主控台註冊現有帳戶。

AFT 支援共用 AWS Control Tower 帳戶的自動自訂

2022 年 5 月 27 日

(AWS Control Tower 登陸區域不需要更新）

Account Factory for Terraform (AFT) 現在能以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、稽核帳戶和日誌封存帳戶，以及您註冊的帳戶。您可以集中帳戶自訂和更新管理，同時保護帳戶組態的安全性，因為您限制了執行工作的角色。

現有的 AWSAFTExecution 角色現在會在所有帳戶中部署自訂。您可以使用邊界來設定 IAM 許可，以根據您的業務和安全性需求限制 AWSAFTExecution 角色的存取。您也可以以程式設計方式委派該角色中已核准的自訂許可給信任的使用者。根據最佳實務，建議您將許可限制為部署所需自訂所需的許可。

AFT 現在會建立新的 AWSAFTService 角色，在所有受管帳戶中部署 AFT 資源，包括共用帳戶和管理帳戶。先前由 AWSAFTExecution 角色部署的資源。

AWS Control Tower 共用和管理帳戶不是透過帳戶工廠佈建，因此它們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。

所有選用控制項的並行操作

2022 年 5 月 18 日

(AWS Control Tower 登陸區域不需要更新）

AWS Control Tower 現在支援預防性控制以及偵測性控制的並行操作。

使用此新功能，現在可同時套用或移除任何選用控制項，從而改善所有選用控制項的易用性和效能。您可以啟用多個選用控制項，而無需等待個別控制操作完成。唯一的限制時間是 AWS Control Tower 正在登陸區域設定過程中，或將控管延伸至新組織時。

預防性控制支援的 功能：

- 在相同的 OU 上套用和移除不同的預防性控制項。
- 在不同的 OUs 上同時套用和移除不同的預防性控制。
- 在多個 OUs 上同時套用和移除相同的預防性控制。
- 您可以同時套用和移除任何預防性和偵測性控制項。

您可以在所有發行的 AWS Control Tower 版本中體驗這些控制並行改進。

當您將預防性控制套用至巢狀 OUs 時，預防性控制會影響目標 OUs 下的所有帳戶和 OU，即使這些帳戶和 OUs 未向 AWS Control Tower 註冊。預防性控制是使用屬於其中的服務控制政策 SCPs) 實作 AWS Organizations。Detective 控制項是使用 AWS Config 規則實作。當您建立新帳戶或變更現有帳戶時，護欄仍然有效，AWS Control Tower 會提供每個帳戶如何符合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 控制項程式庫。

現有的安全性和記錄帳戶

2022 年 5 月 16 日

（在初始設定期間可用。）

AWS Control Tower 現在可讓您在初始登陸區域設定程序期間，將現有 AWS 帳戶指定為 AWS Control Tower 安全或記錄帳戶。此選項不需要 AWS Control Tower 建立新的共用帳戶。根據預設，安全帳戶稱為稽核帳戶，是限制帳戶，可讓安全與合規團隊存取登陸區域中的所有帳戶。根據預設，記錄帳戶稱

為 Log Archive 帳戶，可做為儲存庫運作。它會儲存來自登陸區域中所有帳戶的 API 活動和資源組態日誌。

透過將您現有的安全性和記錄帳戶，您可以更輕鬆地將 AWS Control Tower 管控擴展到現有的組織，或從替代登陸區域移至 AWS Control Tower。在初始登陸區域設定期間，會顯示讓您使用現有帳戶的選項。它包括在設定程序期間的檢查，以確保成功部署。AWS Control Tower 會在您現有的帳戶中實作必要的角色和控制項。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 帳戶作為稽核和日誌封存帳戶帶入 AWS Control Tower，而且這些帳戶有現有 AWS Config 資源，您必須先刪除現有 AWS Config 資源，才能將帳戶註冊到 AWS Control Tower。

AWS Control Tower 登陸區域 2.9 版

2022 年 4 月 22 日

(AWS Control Tower 登陸區域需要更新至 2.9 版。 如需詳細資訊，請參閱 更新您的登陸區域)

AWS Control Tower 登陸區域 2.9 版會將通知轉寄站 Lambda 更新為使用 Python 3.9 版執行時間。此更新說明 Python 3.6 版的棄用，預計於 2022 年 7 月推出。如需最新資訊，請參閱 Python 棄用頁面。

AWS Control Tower 登陸區域 2.8 版

2022 年 2 月 10 日

(AWS Control Tower 登陸區域需要更新至 2.8 版。 如需詳細資訊，請參閱 更新您的登陸區域)

AWS Control Tower 登陸區域 2.8 版新增的功能符合AWS 基礎安全最佳實務的最新更新。

在此版本中：

- 存取日誌已針對日誌封存帳戶中的存取日誌儲存貯體設定，以追蹤對現有 S3 存取日誌儲存貯體的存取。
- 新增生命週期政策的支援。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，此版本會將 AWS Control Tower 更新為在所有受管帳戶 （不包括 管理帳戶） 中使用 提供的服務 AWS 連結角色 (SLR) AWS Config，以便您可以設定和管理 Config 規則以符合 AWS Config 最佳實務。未升級的客戶將繼續使用其現有角色。
- 此版本可簡化加密 AWS Config 資料的 AWS Control Tower KMS 組態程序，並改善 CloudTrail 中的相關狀態訊息。

- 版本包含區域拒絕控制的更新，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 Lambda 函數的 AWS 無效字母佇列。

其他詳細資訊：

- 如果您停用登陸區域，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。

若要將登陸區域更新為 2.8，請導覽至登陸區域設定頁面，選取 2.8 版本，然後選擇更新。更新登陸區域之後，您必須更新由 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。

2021 年 1 月至 12 月

2021 年，AWS Control Tower 發佈了下列更新：

- 區域拒絕功能
- 資料駐留功能
- AWS Control Tower 推出 Terraform 帳戶佈建和自訂
- 可用的新生命週期事件
- AWS Control Tower 啟用巢狀 OUs
- Detective 控制並行
- 兩個可用的新區域
- 區域取消選取
- AWS Control Tower 可與 AWS Key Management Systems 搭配使用
- 控制項已重新命名，功能不變
- AWS Control Tower 每天掃描 SCPs 以檢查漂移
- OUs 和帳戶的自訂名稱
- AWS Control Tower 登陸區域 2.7 版
- 三個可用的新 AWS 區域
- 僅管理選取的區域
- AWS Control Tower 現在可將管控擴展到 AWS 組織中現有的 OUs

- 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 登陸區域不需要更新。)

AWS Control Tower 現在提供區域拒絕功能，協助您限制存取 AWS Control Tower 環境中已註冊帳戶的 AWS 服務和操作。區域拒絕功能補充了 AWS Control Tower 中現有的區域選擇和區域取消選擇功能。這些功能共同協助您解決合規和法規問題，同時平衡與擴展到其他區域相關的成本。

例如，德國 AWS 的客戶可以拒絕存取法蘭克福區域以外區域中 AWS 的服務。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，可以使用區域拒絕功能。選取 AWS 服務不受區域拒絕功能限制。若要進一步了解，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 登陸區域不需要更新)

AWS Control Tower 現在提供專門建置的控制項，協助確保您上傳至 AWS 服務的任何客戶資料僅位於您指定的 AWS 區域。您可以選取存放和處理客戶資料的 AWS 區域。如需 AWS Control Tower 可用 AWS 區域的完整清單，請參閱AWS 區域表。

對於精細控制，您可以套用其他控制，例如不允許 Amazon Virtual Private Network (VPN) 連線，或不允許 Amazon VPC 執行個體的網際網路存取。您可以在 AWS Control Tower 主控台中檢視控制項的合規狀態。如需可用控制項的完整清單，請參閱 AWS Control Tower 控制項程式庫。

AWS Control Tower 推出 Terraform 帳戶佈建和自訂

2021 年 11 月 29 日

(AWS Control Tower 登陸區域的選用更新)

您現在可以使用 Terraform 透過 AWS Control Tower 搭配 AWS Control Tower Account Factory for Terraform (AFT) 來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。在您將帳戶提供給最終使用者之前，佈建期間的自訂有助於滿足您的業務和安全性政策。

AFT 自動化帳戶建立管道會持續監控，直到帳戶佈建完成，然後觸發其他 Terraform 模組，以任何必要的自訂來增強帳戶。作為自訂程序的另一個部分，您可以設定管道來安裝自己的自訂 Terraform 模組，也可以選擇新增任何 AFT 功能選項，這些選項由 AWS 為常見自訂提供。

按照 AWS Control Tower 使用者指南、 和下載 Terraform 執行個體的 AFT 中提供的步驟，開始使用適用於 Terraform 的 AWS Control Tower 帳戶工廠。 部署適用於 Terraform (AFT) 的 AWS Control Tower 帳戶工廠AFT 支援 Terraform Cloud、Terraform Enterprise 和 Terraform Open Source 分佈。

可用的新生命週期事件

2021 年 11 月 18 日

(AWS Control Tower 登陸區域不需要更新）

`PrecheckOrganizationalUnit` 事件會記錄是否有任何資源阻止擴展控管任務成功，包括巢狀 OUs 中的資源。如需詳細資訊，請參閱`PrecheckOrganizationalUnit`。

AWS Control Tower 啟用巢狀 OUs

2021 年 11 月 16 日

(AWS Control Tower 登陸區域不需要更新）

AWS Control Tower 現在可讓您將巢狀 OUs 包含在登陸區域中。

AWS Control Tower 支援巢狀組織單位 (OUs)，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 OUs 的 OU、在父 OUs 下建立和註冊 OUs，並在任何已註冊的 OU 上啟用控制項，無論深度為何。為了支援此功能，主控台會顯示受管帳戶和 OUs 的數量。

使用巢狀 OUs，您可以將 AWS Control Tower OUs 與 AWS 多帳戶策略保持一致，而且您可以透過在父 OUs 層級強制執行控制項，以減少在多個 OU 上啟用控制項所需的時間。

關鍵考量

1. 您可以向 AWS Control Tower 註冊現有的多層級 OUs，一次一個 OU，從最上層 OU 開始，然後向下處理樹狀結構。如需詳細資訊，請參閱從平面 OU 結構擴展到巢狀 OU 結構。
2. 直接在已註冊 OU 下的帳戶會自動註冊。可以透過註冊其直接父系 OU 來進一步註冊樹狀目錄的帳戶。

3. 預防性控制 SCPs) 會自動繼承至階層；套用至父系的 SCPs 會繼承所有巢狀 OUs。
4. Detective 控制項 (AWS Config 規則） 不會自動繼承。
5. 每個 OU 都會報告對偵測性控制的合規性。
6. OU 上的 SCP 偏離會影響其下的所有帳戶和 OUs。
7. 您無法在安全 OUs （核心 OU) 下建立新的巢狀 OU。

Detective 控制並行

2021 年 11 月 5 日

(AWS Control Tower 登陸區域的選用更新）

AWS Control Tower 偵測控制現在支援偵測控制的並行操作，可提高易用性和效能。您可以啟用多個偵測性控制，而無需等待個別控制操作完成。

支援的功能：

- 在相同的 OU 上啟用不同的偵測性控制 （例如，偵測是否啟用根使用者的 MFA，以及偵測是否允許公開寫入存取 Amazon S3 儲存貯體)。
- 同時對不同的 OUs 啟用不同的偵測性控制。
- 已改善護欄錯誤訊息，為支援的控制並行操作提供額外的指引。

此版本不支援：

- 不支援同時在多個 OUs 上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 中體驗偵測性控制並行改進。建議目前不在 2.7 版上的客戶執行登陸區域更新，以利用其他功能，例如區域選擇和取消選擇，這些功能可在最新版本中使用。

兩個可用的新區域

2021 年 7 月 29 日

(AWS Control Tower 登陸區域需要更新）

AWS Control Tower 現已在兩個其他 AWS 區域提供：南美洲 （聖保羅） 和歐洲 （巴黎）。此更新將 AWS Control Tower 可用性擴展至 15 AWS 個區域。

如果您是初次使用 AWS Control Tower，您可以立即在任何支援的區域中啟動它。在啟動期間，您可以選取您希望 AWS Control Tower 在其中建置和管理多帳戶環境的區域。

如果您已有 AWS Control Tower 環境，而且想要在一或多個支援的區域中擴展或移除 AWS Control Tower 控管功能，請前往 AWS Control Tower 儀表板中的登陸區域設定頁面，然後選取區域。更新登陸區域之後，您必須更新由 AWS Control Tower 管理的所有帳戶。

區域取消選取

2021 年 7 月 29 日

(AWS Control Tower 登陸區域的選用更新）

AWS Control Tower 區域取消選取可增強您管理 AWS Control Tower 資源地理足跡的能力。您可以取消選取您不再希望 AWS Control Tower 管理的區域。此功能可讓您解決合規和法規問題，同時平衡與擴展到其他區域相關的成本。

當您更新 AWS Control Tower 登陸區域版本時，可以使用區域取消選取。

當您使用 Account Factory 建立新帳戶或註冊預先存在的成員帳戶，或選取擴展控管以註冊預先存在組織單位的帳戶時，AWS Control Tower 會在帳戶中的所選區域中部署其控管功能，包括集中式記錄、監控和控制。選擇取消選取區域並從該區域移除 AWS Control Tower 控管會移除該控管功能，但不會阻礙使用者將 AWS 資源或工作負載部署到這些區域。

AWS Control Tower 可與 AWS Key Management Systems 搭配使用

2021 年 7 月 28 日

(AWS Control Tower 登陸區域的選用更新）

AWS Control Tower 可讓您選擇使用 AWS Key Management Service (AWS KMS) 金鑰。金鑰由您提供和管理，以保護 AWS Control Tower 部署的服務 AWS CloudTrail AWS Config，包括 和相關聯的 Amazon S3 資料。 AWS KMS 加密是 AWS Control Tower 預設使用的 SSE-S3 加密的增強加密層級。

將 AWS KMS 支援整合至 AWS Control Tower 與AWS 基礎安全最佳實務保持一致，該最佳實務建議為您的敏感日誌檔案增加一層安全性。您應該使用 AWS KMS 受管金鑰 (SSE-KMS) 進行靜態加密。當您設定新的登陸區域或更新現有的 AWS Control Tower 登陸區域時，可使用 AWS KMS 加密支援。

若要設定此功能，您可以在初始登陸區域設定期間選取 KMS 金鑰組態。您可以選擇現有的 KMS 金鑰，也可以選取按鈕，將您導向 AWS KMS 主控台以建立新的金鑰。您也可以靈活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 登陸區域，您可以執行更新以開始使用 AWS KMS 金鑰。

控制項已重新命名，功能不變

2021 年 7 月 26 日

(AWS Control Tower 登陸區域不需要更新）

AWS Control Tower 正在修訂特定控制項名稱和描述，以更好地反映控制項的政策意圖。修訂的名稱和描述可協助您更直覺地了解 控制體現您帳戶政策的方式。例如，我們將部分偵測性控制的名稱從「不允許」變更為「偵測」，因為偵測性控制本身不會停止特定動作，只會偵測政策違規，並透過儀表板提供提醒。

控制功能、指引和實作保持不變。只有控制項名稱和描述已修訂。

AWS Control Tower 每天掃描 SCPs 以檢查漂移

2021 年 5 月 11 日

(AWS Control Tower 登陸區域不需要更新）

AWS Control Tower 現在會執行受管 SCPs 的每日自動化掃描，以確認對應的控制項已正確套用，且尚未漂移。如果掃描發現偏離，您會收到通知。AWS Control Tower 只會為每個偏離問題傳送一個通知，因此如果您的登陸區域已經處於偏離狀態，除非找到新的偏離項目，否則您不會收到其他通知。

OUs 和帳戶的自訂名稱

2021 年 4 月 16 日

(AWS Control Tower 登陸區域不需要更新）

AWS Control Tower 現在可讓您自訂登陸區域命名。您可以保留 AWS Control Tower 為組織單位 (OUs) 和核心帳戶建議的名稱，也可以在初始登陸區域設定程序期間修改這些名稱。

AWS Control Tower 為 OUs 和核心帳戶提供的預設名稱符合 AWS 多帳戶最佳實務指引。 不過，如果您的公司有特定的命名政策，或者您已擁有具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靈活地解決這些限制。

與設定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 OU，而先前稱為自訂 OU 的 OU 現在稱為沙盒 OU。我們進行了這項變更，以改善與命名整體 AWS 最佳實務指引的一致性。

新客戶將看到這些新的 OU 名稱。現有客戶將繼續看到這些 OUs 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。

若要從 AWS 管理主控台開始使用 AWS Control Tower，請前往 AWS Control Tower 主控台，然後選取右上角的設定登陸區域。如需詳細資訊，請參閱如何規劃 AWS Control Tower 登陸區域。

AWS Control Tower 登陸區域 2.7 版

2021 年 4 月 8 日

(AWS Control Tower 登陸區域需要更新至 2.7 版。 如需詳細資訊，請參閱 更新您的登陸區域)

使用 AWS Control Tower 2.7 版，AWS Control Tower 推出了四個新的強制性預防性日誌封存控制項，僅對 AWS Control Tower 資源實作政策。我們已將四個現有 Log Archive 控制項的指引從強制性調整為選擇性，因為它們為 AWS Control Tower 外部的資源設定政策。此控制變更和擴展可讓您將 AWS Control Tower 內資源的 Log Archive 控管與 AWS Control Tower 外部資源的控管分開。

四個已變更的控制項可以與新的強制性控制項搭配使用，為更廣泛的 AWS 日誌封存集提供控管。為了環境一致性，現有的 AWS Control Tower 環境會自動啟用這四個變更的控制項；不過，這些選擇性控制項現在可以停用。新的 AWS Control Tower 環境必須啟用所有選擇性控制。將加密新增至 AWS Control Tower 未部署的 Amazon S3 儲存貯體之前，現有的環境必須停用先前的強制性控制。

新的強制性控制項：

- 不允許在日誌存檔中變更 AWS Control Tower 建立的 S3 儲存貯體的加密組態
- 不允許變更日誌存檔中 AWS Control Tower 建立的 S3 儲存貯體的日誌組態
- 不允許變更日誌存檔中 AWS Control Tower 建立的 S3 儲存貯體的儲存貯體政策
- 不允許在日誌存檔中變更 AWS Control Tower 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擇性：

- 不允許變更所有 Amazon S3 儲存貯體的加密組態 【先前：為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：啟用日誌封存的存取日誌】
- 不允許變更所有 Amazon S3 儲存貯體的儲存貯體政策 【先前：不允許變更日誌存檔的政策】
- 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 登陸區域藍圖的變更，這可能會導致您升級至 2.7 之後與舊版不相容。

- 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，您可以關閉此預設。如

需BlockPublicaccess啟用 時會發生哪些情況的詳細資訊，請參閱封鎖對 Amazon S3 儲存體的公開存取。

- AWS Control Tower 2.7 版包含 HTTPS 的需求。傳送至 AWS Control Tower 部署之 S3 儲存貯體的所有請求都必須使用安全通訊端層 (SSL)。僅允許 HTTPS 請求傳遞。如果您使用 HTTP （不含 SSL) 做為端點來傳送請求，此變更會為您提供存取遭拒的錯誤，這可能會破壞您的工作流程。此變更無法在 2.7 更新至您的登陸區域後還原。

  建議您將請求變更為使用 TLS 而非 HTTP。

三個可用的新 AWS 區域

2021 年 4 月 8 日

(AWS Control Tower 登陸區域需要更新）

AWS Control Tower 可在其他三個 AWS 區域使用：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。需要更新 2.7 版的登陸區域，才能將管控擴展到這些區域。

當您執行 2.7 版的更新時，您的登陸區域不會自動擴展到這些區域，您必須在區域資料表中檢視和選取它們以進行包含。

僅管理選取的區域

2021 年 2 月 19 日

(AWS Control Tower 登陸區域不需要更新）

AWS Control Tower 區域選擇可讓您更妥善地管理 AWS Control Tower 資源的地理足跡。若要擴展託管 AWS 資源或工作負載的區域數量，基於合規、法規、成本或其他原因，您現在可以選取要管理的其他區域。

當您設定新的登陸區域或更新 AWS Control Tower 登陸區域版本時，即可選擇區域。當您使用 Account Factory 建立新帳戶或註冊預先存在的成員帳戶，或當您使用擴展控管在預先存在的組織單位中註冊帳戶時，AWS Control Tower 會在帳戶中的所選區域中部署集中式記錄、監控和控制的控管功能。如需選取區域的詳細資訊，請參閱 設定您的 AWS Control Tower 區域。

AWS Control Tower 現在可將管控擴展到 AWS 組織中現有的 OUs

2021 年 1 月 28 日

(AWS Control Tower 登陸區域不需要更新）

從 AWS Control Tower 主控台將控管延伸至現有的組織單位 (OUs)（不在 AWS Control Tower 中的單位）。透過此功能，您可以在 AWS Control Tower 控管下提供最上層的 OUs 和包含的帳戶。如需將控管延伸至整個 OU 的資訊，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 內成功延伸控管和註冊帳戶。如需 OU 初始註冊相關常見問題的詳細資訊，請參閱 註冊或重新註冊期間失敗的常見原因。

您也可以造訪 AWS Control Tower 產品網頁或前往 YouTube 觀看此影片，了解 AWS Control Tower 的入門 AWS Organizations。

AWS Control Tower 提供大量帳戶更新

2021 年 1 月 28 日

(AWS Control Tower 登陸區域不需要更新)

使用大量更新功能，您現在可以從 AWS Control Tower 儀表板，一鍵更新最多包含 300 個帳戶的已註冊 AWS Organizations 組織單位 (OU) 中的所有帳戶。當您更新 AWS Control Tower 登陸區域，並且還必須更新已註冊的帳戶，使其與目前的登陸區域版本保持一致時，這特別有用。

當您更新 AWS Control Tower 登陸區域以擴展至新區域，或您想要重新註冊 OU 以確保該 OU 中的所有帳戶都套用了最新的控制項時，此功能也可協助您將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戶上執行更新。

如需更新登陸區域的資訊，請參閱 更新您的登陸區域。

如需註冊或重新註冊 OU 的資訊，請參閱 向 AWS Control Tower 註冊現有的組織單位。

2020 年 1 月至 12 月

2020 年，AWS Control Tower 發佈了下列更新：

- AWS Control Tower 主控台現在連結至外部 Config AWS 規則
- AWS Control Tower 現已在其他區域提供
- 護欄更新
- AWS Control Tower 主控台會顯示有關 OUs和帳戶的詳細資訊
- 使用 AWS Control Tower 在 中設定新的多帳戶 AWS 環境 AWS Organizations
- AWS Control Tower 解決方案的自訂
- AWS Control Tower 2.3 版的一般可用性

- AWS Control Tower 中的單一步驟帳戶佈建
- AWS Control Tower 停用工具
- AWS Control Tower 生命週期事件通知

AWS Control Tower 主控台現在連結至外部 Config AWS 規則

2020 年 12 月 29 日

(AWS Control Tower 登陸區域需要更新至 2.6 版。 如需詳細資訊，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。這可讓您在 AWS Control Tower 主控台中查看外部建立的 AWS Config 規則，以及 AWS Control Tower 建立的 AWS Config 規則。彙整工具可讓 AWS Control Tower 偵測外部規則並提供 Config AWS 主控台的連結，而不需要 AWS Control Tower 存取未受管帳戶。

使用此功能，您現在可以將偵測性控制項的合併檢視套用至您的帳戶，以便您可以追蹤合規性，並判斷您是否需要帳戶的其他控制項。如需詳細資訊，請參閱 AWS Control Tower 如何彙總未受管 OUs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 登陸區域需要更新至 2.5 版。 如需詳細資訊，請參閱 更新您的登陸區域)

AWS Control Tower 現已在 5 個其他 AWS 區域提供：

- 亞太地區 (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

新增這些 5 AWS Regions 是針對 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。透過此啟動，AWS Control Tower 現在可在 10 AWS 區域使用。

此登陸區域更新包含列出的所有區域，且無法復原。將登陸區域更新至 2.5 版之後，您必須手動更新 AWS Control Tower 的所有註冊帳戶，以在 10 個支援的區域中進行管理。 AWS 如需相關資訊，請參閱設定您的 AWS Control Tower 區域。

護欄更新

2020 年 10 月 8 日

(AWS Control Tower 登陸區域不需要更新）

已針對強制性控制項 發行更新版本`AWS-GR_IAM_ROLE_CHANGE_PROHIBITED`。

需要對控制項進行此變更，因為自動註冊到 AWS Control Tower 的帳戶必須啟用 `AWSControlTowerExecution`角色。舊版控制項可防止建立此角色。

如需詳細資訊，請參閱《AWS Control Tower AWS 控制項參考指南》中的不允許對 AWS Control Tower 設定的 IAM 角色進行變更 CloudFormation。

AWS Control Tower 主控台會顯示有關 OUs和帳戶的詳細資訊

2020 年 7 月 22 日

(AWS Control Tower 登陸區域不需要更新）

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 Tower 主控台中，您可以檢視有關 AWS 帳戶和組織單位 (OUs的詳細資訊。帳戶頁面現在會列出組織中的所有帳戶，無論 AWS Control Tower 中的 OU 或註冊狀態為何。您現在可以搜尋、排序和篩選所有資料表。

使用 AWS Control Tower 在 中設定新的多帳戶 AWS 環境 AWS Organizations

2020 年 4 月 22 日

(AWS Control Tower 登陸區域不需要更新）

AWS Organizations 客戶現在可以利用這些新功能，使用 AWS Control Tower 來管理新建立的組織單位 (OUs) 和帳戶：

- 現有 AWS Organizations 客戶現在可以為其現有管理帳戶中的新組織單位 (OUs) 設定新的登陸區域。您可以在 AWS Control Tower 中建立新的 OUs，並在這些具有 AWS Control Tower 管控OUs 中建立新的帳戶。
- 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同運作 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定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已建立的政策。建置器可受益於 ，因為他們可以快速佈建新 AWS 帳戶，而不會過度擔心合規性。

如需設定登陸區域的資訊，請參閱 規劃您的 AWS Control Tower 登陸區域。您也可以造訪 AWS Control Tower 產品網頁或前往 YouTube 觀看此影片，了解 AWS Control Tower 的入門 AWS Organizations。

除了此變更之外，AWS Control Tower 中的快速帳戶佈建功能已重新命名為註冊帳戶。它現在允許註冊現有 AWS 帳戶以及建立新帳戶。如需詳細資訊，請參閱從 AWS Control Tower 主控台註冊現有帳戶。

AWS Control Tower 解決方案的自訂

2020 年 3 月 17 日

(AWS Control Tower 登陸區域不需要更新)

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至 AWS Control Tower 登陸區域。

透過 AWS Control Tower 的自訂功能，您可以使用 CloudFormation 範本，將新資源部署到組織內的現有和新帳戶。除了 AWS Control Tower 提供的 SCP 之外，您也可以將自訂服務控制政策 (SCPs) 套用至這些帳戶。 SCPs AWS Control Tower 管道的自訂與 AWS Control Tower 生命週期事件和通知 (AWS Control Tower 中的生命週期事件) 整合，以確保資源部署與您的登陸區域保持同步。

此 AWS Control Tower 解決方案架構的部署文件可透過 AWS 解決方案網頁取得。

AWS Control Tower 2.3 版的一般可用性

2020 年 3 月 5 日

(AWS Control Tower 登陸區域需要更新。 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）AWS、美國東部（維吉尼亞北部）、美國西部（奧勒岡）和歐洲（愛爾蘭）區域外，AWS Control Tower 現已在亞太區域（雪梨）區域提供。新增亞太區域（雪梨）區域是針對 AWS Control Tower 2.3 版推出的唯一變更。

如果您先前尚未使用 AWS Control Tower，則可以立即在任何支援的區域中啟動它。如果您已經在使用 AWS Control Tower，並想要將其控管功能擴展到帳戶中的亞太區域（雪梨）區域，請前往 AWS Control Tower 儀表板的設定頁面。從那裡，將您的登陸區域更新為最新版本。然後，個別更新您的帳戶。

> **Note**
>
> 更新登陸區域不會自動更新您的帳戶。如果您有多個帳戶，則所需的更新可能會很耗時。因此，建議您避免將您的 AWS Control Tower 登陸區域擴展到您不需要執行工作負載的區域。

如需因部署到新區域而導致偵測性控制預期行為的資訊，請參閱設定您的 AWS Control Tower 區域。

AWS Control Tower 中的單一步驟帳戶佈建

2020 年 3 月 2 日

(AWS Control Tower 登陸區域不需要更新）

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 Tower 主控台佈建新帳戶。

若要使用簡化表單，請在 AWS Control Tower 主控台中導覽至 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佈建帳戶，以及為帳戶建立的單一登入 (IAM Identity Center) 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，更新您透過快速帳戶佈建建立的帳戶，就像更新任何其他帳戶一樣。

> **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 Tower 主控台中建立和更新帳戶的能力與註冊 AWS 帳戶的能力不同。如需詳細資訊，請參閱從 AWS Control Tower 主控台註冊現有帳戶。

AWS Control Tower 停用工具

2020 年 2 月 28 日

(AWS Control Tower 登陸區域不需要更新)

AWS Control Tower 現在支援自動除役工具，協助您清理 AWS Control Tower 配置的資源。如果您不想再為企業使用 AWS Control Tower，或者需要主要重新部署組織資源，建議您清除最初設定登陸區域時建立的資源。

若要使用大部分自動化的程序來解除委任您的登陸區域，請聯絡 AWS 支援 以取得所需額外步驟的協助。如需停用的詳細資訊，請參閱 停用 AWS Control Tower 登陸區域。

AWS Control Tower 生命週期事件通知

2020 年 1 月 22 日

(AWS Control Tower 登陸區域不需要更新)

AWS Control Tower 宣布生命週期事件通知的可用性。生命週期事件表示 AWS Control Tower 動作已完成，可變更組織單位 (OUs)、帳戶和由 AWS Control Tower 建立和管理之控制項等資源的狀態。生命週期事件會記錄為 AWS CloudTrail 事件，並以事件形式傳送至 Amazon EventBridge。

AWS Control Tower 會在完成下列可使用 服務執行的動作時記錄生命週期事件：建立或更新登陸區域；建立或刪除 OU；啟用或停用 OU 上的控制項；以及使用帳戶工廠建立新帳戶或將帳戶移至另一個 OU。

AWS Control Tower 使用多項 AWS 服務來建置和控管多帳戶 AWS 環境最佳實務。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，以驗證原始 AWS Control Tower 動作是否成功完成。您可以建立 EventBridge 規則，以便在 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。

2019 年 6 月至 12 月

從 2019 年 6 月 24 日至 12 月 31 日，AWS Control Tower 發佈了下列更新：

- AWS Control Tower 2.2 版的一般可用性
- AWS Control Tower 中新的選擇性控制
- AWS Control Tower 中的新偵測控制

- AWS Control Tower 接受具有與管理帳戶不同網域之共用帳戶的電子郵件地址
- AWS Control Tower 2.1 版的一般可用性

AWS Control Tower 2.2 版的一般可用性

2019 年 11 月 13 日

(AWS Control Tower 登陸區域需要更新。 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，可防止帳戶偏離：

- 不允許變更 AWS Control Tower 設定的 Amazon CloudWatch Logs 日誌群組
- 不允許刪除 AWS Control Tower AWS Config 建立的彙總授權
- 不允許刪除日誌存檔

控制項是為整體 AWS 環境提供持續控管的高階規則。當您建立 AWS Control Tower 登陸區域時，登陸區域和所有組織單位 (OUs)、帳戶和資源都符合您選擇的控制項強制執行的控管規則。當您和您的組織成員使用登陸區域時，可能會發生此合規狀態的變更（意外或有意）。偏離偵測可協助您識別需要變更或組態更新來解決偏離的資源。如需詳細資訊，請參閱在 AWS Control Tower 中偵測並解決偏離。

AWS Control Tower 中新的選擇性控制

2019 年 9 月 5 日

(AWS Control Tower 登陸區域不需要更新）

AWS Control Tower 現在包含以下四個新的選擇性控制：

- 不允許在沒有 MFA 的情況下對 Amazon S3 儲存貯體執行刪除動作
- 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

控制項是為整體 AWS 環境提供持續控管的高階規則。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 中的控制項。

AWS Control Tower 中的新偵測控制

2019 年 8 月 25 日

(AWS Control Tower 登陸區域不需要更新）

AWS Control Tower 現在包含以下八個新的偵測控制：

- 偵測是否啟用 Amazon S3 儲存貯體的版本控制
- 偵測 AWS 主控台的 IAM 使用者是否啟用 MFA
- 偵測 IAM 使用者是否已啟用 MFA
- 偵測 Amazon EC2 執行個體是否啟用 Amazon EBS 最佳化
- 偵測 Amazon EBS 磁碟區是否連接至 Amazon EC2 執行個體
- 偵測是否啟用對 Amazon RDS 資料庫執行個體的公開存取
- 偵測是否啟用對 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

控制項是為整體 AWS 環境提供持續控管的高階規則。偵測性控制可偵測您帳戶中資源的不合規情況，例如政策違規，並透過儀表板提供提醒。如需詳細資訊，請參閱關於 AWS Control Tower 中的控制項。

AWS Control Tower 接受具有與管理帳戶不同網域之共用帳戶的電子郵件地址

2019 年 8 月 1 日

(AWS Control Tower 登陸區域不需要更新）

在 AWS Control Tower 中，您現在可以提交共用帳戶（日誌封存和稽核成員）和子帳戶（使用帳戶工廠提供）的電子郵件地址，其網域與管理帳戶的電子郵件地址不同。只有在建立新的登陸區域以及佈建新的子帳戶時，才能使用此功能。

AWS Control Tower 2.1 版的一般可用性

2019 年 6 月 24 日

(AWS Control Tower 登陸區域需要更新。 如需詳細資訊，請參閱更新您的登陸區域。）

AWS Control Tower 現已正式推出並支援生產用途。AWS Control Tower 適用於擁有多個帳戶和團隊的組織，他們正在尋找最簡單的方法來設定其新的多帳戶 AWS 環境並大規模管理。透過 AWS Control Tower，您可以協助確保組織中的帳戶符合已建立的政策。分散式團隊的最終使用者可以快速佈建新 AWS 帳戶。

使用 AWS Control Tower，您可以設定登陸區域，採用最佳實務，例如使用 設定多帳戶結構 AWS Organizations、使用 管理使用者身分和聯合存取 AWS IAM Identity Center、透過 Service Catalog 啟用帳戶佈建，以及使用 AWS CloudTrail 和 建立集中式日誌封存 AWS Config。

為了持續控管，您可以啟用預先設定的控制項，這些控制項是安全、操作和合規的明確定義規則。護欄有助於防止部署不符合政策的資源，並持續監控已部署的資源是否有不一致性。AWS Control Tower 儀表板提供 AWS 環境的集中可見性，包括佈建的帳戶、啟用的控制項，以及帳戶的合規狀態。

您可以在 AWS Control Tower 主控台中按一下來設定新的多帳戶環境。使用 AWS Control Tower 無需額外費用或預付承諾。您只需為您啟用的 AWS 這些服務付費，即可設定登陸區域並實作選取的控制項。

文件歷史記錄

- 文件最近更新時間：2025 年 12 月 30 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
受管政策的更新	已更新 AWS ControlTowerAccountServiceRolePolicy。	2025 年 12 月 30 日
AWS Control Tower 登陸區域版本 4.0，具有專用控制環境	AWS Control Tower 登陸區域 4.0 版現已提供選用的服務整合和專用控制環境	2025 年 11 月 17 日
AWS Control Tower 包含額外的 279 個 AWS Config 控制項	更新 Control Catalog 以包含其他 279 個 AWS Config 控制項。	2025 年 11 月 14 日
受管政策的更新	已更新 AWS ControlTowerAccountServiceRolePolicy。	2025 年 11 月 10 日
已更新受管政策	更新 AWS ControlTowerServiceRolePolicy，以支援登陸區域 4.0 的選用 AWS CloudTrail 整合。Amazon CloudWatch Logs 資源模式從 變更為 `aws-controltower/CloudTrailLogs:*` `aws-controltower/CloudTrailLogs*:*` ，以允許管理具有唯一尾碼的日誌群組。此回溯相容性更新可讓客戶多次啟用	2025 年 11 月 5 日

	和停用 AWS CloudTrail 整合，每次使用唯一尾碼重新建立日誌群組，以避免命名衝突。	
新的 受管政策	新增 AWS ControlTowerCloudTrailRolePolicy 受管政策的文件。此受管政策會取代 AWS ControlTowerCloudTrailRole 先前使用的內嵌政策，讓 AWS 無需客戶介入即可更新政策。	2025 年 11 月 5 日
亞太區域（紐西蘭）區域提供 AWS Control Tower	AWS Control Tower 可在紐西蘭的奧克蘭使用。	2025 年 10 月 28 日
AWS Control Tower 支援自動帳戶註冊	自動註冊帳戶並在 OUs 之間移動。	2025 年 10 月 15 日
更新 受管政策、新的 受管政策	更新 AWS ControlTowerServiceRolePolicy 並新增 AWS ControlTowerIdentityCenterManagementPolicy。	2025 年 10 月 14 日
AWS Control Tower 更新 Python 版本	已更新 AWS Control Tower 環境中的 Python 版本	2025 年 9 月 3 日
AWS Control Tower 支援 IPv6	AWS Control Tower 新增對 IPv6 端點的支援。	2025 年 8 月 18 日
Terraform 1.15.0 版的 Account Factory	AFT 1.15.0 版已推出。	2025 年 7 月 28 日
使用 Nitro 執行個體類型更新控制項	已更新八個主動控制，以新增新的執行個體類型。	2025 年 7 月 24 日
亞太區域（台北）提供 AWS Control Tower	AWS Control Tower 新增對亞太區域（台北）的支援。	2025 年 7 月 23 日

AWS Control Tower 支援 AWS PrivateLink	AWS Control Tower 新增對 的支援 AWS PrivateLink。	2025 年 6 月 30 日
服務連結 AWS Config 控制項	AWS Control Tower 部署服務連結 AWS Config 控制項。	2025 年 6 月 12 日
增強型中繼資料。其他控制項、新架構	AWS Control Tower 推出來自 的其他整合控制項 AWS Config，具有控制目錄中所有控制項的增強型中繼資料，並支援更多產業架構。	2025 年 6 月 12 日
啟用的控制項檢視	AWS Control Tower 推出已啟用控制項的完整主控台檢視。	2025 年 5 月 21 日
AFT 支援新組態	AWS Control Tower AFT 在部署時支援三個額外的選用組態。	2025 年 5 月 13 日
增強型基準	AWS Control Tower 現在報告基準偏離。	2025 年 5 月 12 日
AWS Control Tower 適用於 AWS 亞太區域（泰國）和墨西哥（中部）區域	下列區域可供使用：亞太區域（泰國）和墨西哥（中部）。	2025 年 5 月 9 日
AWS Control Tower 新增 233 個 AWS Config 控制項	新增了 Config 控制項、修訂的中繼資料表、區域表、全域識別符頁面。	2025 年 4 月 11 日
AWS Control Tower 會更新服務連結角色	更新至 `AWSControlTowerAccountServiceRolePolicy` 。	2024 年 12 月 10 日
AWS Control Tower CfCT 支援 GitHub	第三方組態來源的新選項。	2024 年 12 月 9 日
具有宣告政策的 AWS Control Tower 預防性控制	新類型的政策會實作新類型的預防性控制。	2024 年 12 月 1 日

AWS Control Tower 與 AWS Backup 整合	您可以設定計劃來備份 AWS Control Tower 資源。	2024 年 11 月 25 日
AWS Control Tower 整合 AWS Config 控制項	AWS Control Tower 整合選取的 AWS Config 控制項。	2024 年 11 月 21 日
AWS Control Tower 改善勾點管理	AWS Control Tower 現在可管理主動控制的勾點。	2024 年 11 月 20 日
已回報控制政策偏離	AWS Control Tower 會報告一種新的漂移類型。	2024 年 11 月 15 日
AWS Control Tower 啟動受管資源控制政策	一種新的預防性控制類型，使用 RCPs實作。	2024 年 11 月 15 日
AWS Control Tower 新增 ResetEnabledControl API	用於管理控制偏離的新 API。	2024 年 11 月 14 日
更新的 `GetControl` API	的兩個新控制欄位`GetControl` 。	2024 年 11 月 8 日
AWS Control Tower AFT 支援 Gitlab	第三方組態來源的新選項。	2024 年 10 月 23 日
AWS Control Tower 適用於 AWS 亞太區域 （馬來西亞） 區域	馬來西亞 (Kuala Lumpur) 已推出新區域。	2024 年 10 月 21 日
AWS Control Tower 每個 OU 最多支援 1000 個帳戶	增加每個 OU 的帳戶限制。	2024 年 8 月 30 日
AWS Control Tower 新增登陸區域版本選擇	如果您執行 3.1 或更新版本，請更新或修復您的登陸區域，而不移至最新版本。	2024 年 8 月 15 日
GetControl 和 ListControls API 操作可用	兩個新的 Control Catalog 操作可協助您找到控制項的詳細資訊。	2024 年 8 月 6 日

AWS Control Tower 在選擇加入區域中支援 AFT 和 CfCT	AFT 和 CfCT 可在其他 中使用 AWS 區域。	2024 年 7 月 18 日
AWS Control Tower 新增 `ListLandingZoneOperations` API	可讓您擷取登陸區域最近操作的新 API。	2024 年 6 月 26 日
AWS Control Tower 最多支援 100 個並行控制操作	並行控制操作配額增加到 100。	2024 年 5 月 20 日
AWS 卡加利西部 （加拿大） 區域提供 AWS Control Tower	AWS Control Tower 可在加拿大西部 （卡加利） 區域使用。	2024 年 5 月 3 日
AWS Control Tower 支援自助式配額調整	AWS Control Tower 在 主控台中與 AWS Service Quotas 整合。	2024 年 4 月 25 日
將控制項的文件移至新指南	AWS Control Tower 發佈了控制項參考指南。	2024 年 4 月 21 日
在 中標記`EnabledControl` 資源 CloudFormation	AWS Control Tower 支援透過 CloudFormation 範本將標籤新增至`EnabledControl` 資源。	2024 年 2 月 22 日
可用的基準 APIs	AWS Control Tower 發佈了用於以程式設計方式註冊 OUs的新 APIs。	2024 年 2 月 14 日
AWS Control Tower 登陸區域 3.3 版	提供 AWS Control Tower 登陸區域 3.3 版。	2023 年 12 月 14 日
AWS Control Tower 宣布控制以協助數位主權	AWS Control Tower 發佈了一組控制項，協助客戶滿足數位主權要求。	2023 年 11 月 27 日
AWS Control Tower 支援登陸區域 APIs	AWS Control Tower 支援使用新的 APIs設定和啟動登陸區域。	2023 年 11 月 26 日

AWS Control Tower 支援標記啟用的控制項	AWS Control Tower 支援在主控台和新 APIs控制項。	2023 年 11 月 10 日
亞太區域（墨爾本）提供 AWS Control Tower AWS 區域	適用於亞太區域（墨爾本）區域。	2023 年 11 月 3 日
可用的新控制項 API	AWS Control Tower 發佈了新的控制 API。	2023 年 10 月 14 日
AWS Control Tower 啟動新的控制項	AWS Control Tower 發佈了新的主動和偵測性控制項。	2023 年 10 月 5 日
AWS Control Tower 報告無法停用受信任存取	如果客戶關閉對 AWS Control Tower 的信任存取，AWS Control Tower 會在發生偏離時通知客戶 AWS Organizations。	2023 年 9 月 21 日
AWS Control Tower 提供四個額外的 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
特拉維夫區域提供 AWS Control Tower	AWS Control Tower 可在特拉維夫區域 il-central-1 中使用。	2023 年 8 月 28 日
AWS Control Tower 推出 28 個新的主動控制	AWS Control Tower 發佈了 28 個新的主動控制。	2023 年 7 月 24 日
AWS Control Tower 取代了 2 個控制項	AWS Control Tower 將從控制項程式庫中移除兩個控制項，自 2023 年 8 月 18 日開始生效。	2023 年 7 月 18 日
可使用 AWS Control Tower 登陸區域 3.2	AWS Control Tower 登陸區域版本 3.2 已推出。	2023 年 6 月 16 日

AWS Control Tower 會根據 ID 處理帳戶	AWS Control Tower 會追蹤 AWS 帳戶 ID，而不是帳戶的電子郵件地址。	2023 年 6 月 14 日
其他可用的 Security Hub CSPM 偵測控制	AWS Control Tower 為 Security Hub CSPM 服務受管標準：AWS Control Tower 新增了 10 個控制項至控制項程式庫。	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的資料表，做為已發佈文件的一部分。	2023 年 6 月 7 日
帳戶工廠自訂的 Terraform 支援	AFC 中對 Terraform 開放原始碼藍圖的單一區域支援。	2023 年 6 月 6 日
AWS IAM 自我管理可用於登陸區域	AWS Control Tower 現在支援客戶為登陸區域選擇其身分提供者。	2023 年 6 月 6 日
已新增新角色	AWS Control Tower 新增了新的服務連結角色 AWSServiceRoleForAWSControlTower，以及相關聯的政策 AWSControlTowerAccountServiceRolePolicy。	2023 年 6 月 1 日
混合控管更新	更新以建議客戶混合控管。	2023 年 6 月 1 日
可用的其他主動控制	新的主動控制可協助您管理多帳戶環境，並達成特定的控制目標。	2023 年 5 月 19 日

七個其他可用區域	AWS Control Tower 現已提供七種額外服務 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
變更為受管政策	我們變更了 AWSControlTowerServiceRolePolicy，讓 AWS Control Tower 可以呼叫帳戶 AWS 管理服務實作的 `EnableRegion`、`ListRegions`、`GetRegionOptStatus` APIs。	2023 年 4 月 6 日
帳戶自訂請求追蹤已全面推出	AWS Control Tower 現在支援使用 Account Factory for Terraform (AFT) 工作流程追蹤帳戶自訂請求。	2023 年 2 月 16 日
IAM 最佳實務更新	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
AWS Control Tower 登陸區域 3.1 可用	AWS Control Tower 登陸區域 3.1 可供使用。	2023 年 2 月 9 日
普遍可用的主動控制	主動控制會從預覽狀態啟動到一般可用性。	2023 年 1 月 24 日
並行帳戶操作	AWS Control Tower 現在支援帳戶工廠中最多五 (5) 個並行動作。您一次最多可以建立、更新或註冊五個帳戶。	2022 年 12 月 16 日

主動控制可協助資源佈建	AWS Control Tower 現在支援透過 CloudFormation 勾點實作的主動控制。	2022 年 11 月 28 日
提供帳戶原廠自訂	AWS Control Tower 現在支援直接從 AWS Control Tower 主控台使用稱為藍圖的可自訂帳戶範本進行帳戶佈建。	2022 年 11 月 28 日
所有 AWS Config 規則都可檢視的合規狀態	AWS Control Tower 現在會顯示部署到向 AWS Control Tower 註冊之組織單位的所有 AWS Config 規則的合規狀態。	2022 年 11 月 18 日
變更為受管政策	我們變更了 AWSControlTowerServiceRolePolicy，以便 AWS Control Tower 可以擔任角色，這是帳戶工廠自訂所需的`AWSControlTowerBlueprintAccess` 角色。	2022 年 10 月 28 日
控制項、 CloudFormation 資源 APIs	AWS Control Tower 現在支援透過一組 API 呼叫和新 CloudFormation 資源來啟用和停用控制項。	2022 年 9 月 1 日
CfCT 支援堆疊集刪除	CfCT 透過在資訊清單檔案中設定參數來支援堆疊集刪除。	2022 年 8 月 26 日
自訂日誌保留	您可以自訂存放 AWS Control Tower CloudTrail 日誌的 Amazon S3 儲存貯體的保留政策，以天數或年為單位，最長可達 15 年。	2022 年 8 月 15 日
角色偏離修復可用	AWS Control Tower 支援角色偏離的修復，無需完全修復登陸區域。	2022 年 8 月 11 日

提供 3.0 版	AWS Control Tower 登陸區域版本 3.0 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。它可讓您僅彙總主要區域中 AWS Config 的資訊。3.0 版也包含區域拒絕控制的更新，以及兩個新的偵測性控制。	2022 年 7 月 29 日
組織頁面結合 OUs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 (OUs) 和帳戶的階層檢視。	2022 年 7 月 18 日
變更為受管政策	我們變更了 AWSControlTowerServiceRolePolicy，讓客戶可以擁有組織層級 AWS CloudTrail 追蹤來彙總 AWS CloudTrail 日誌。	2022 年 6 月 20 日
更輕鬆地註冊和更新成員帳戶	AWS Control Tower 現在可讓您從登陸區域個別註冊和更新成員帳戶。每個帳戶會顯示何時可用於更新。我們已將註冊帳戶按鈕與 Account Factory 中的建立帳戶工作流程分開。	2022 年 5 月 31 日
AFT 支援共用帳戶的自訂	適用於 Terraform 的 AWS Control Tower 帳戶工廠現在支援 AWS Control Tower 管理帳戶、日誌封存和稽核帳戶的自訂。	2022 年 5 月 27 日
所有選用控制項的並行操作	AWS Control Tower 現在可讓您同時套用和移除選用的預防性護欄，以及偵測控制。	2022 年 5 月 18 日

現有的安全性和記錄帳戶	AWS Control Tower 現在支援使用現有的安全和記錄帳戶，而不是在登陸區域設定期間建立新的帳戶。	2022 年 5 月 16 日
提供 2.9 版	AWS Control Tower 登陸區域 2.9 版會將通知轉寄站 Lambda 更新為使用 Python 3.9 版執行時間。	2022 年 4 月 22 日
更新 AWS 了對最佳實務的支援，提供 2.8 版	AWS Control Tower 登陸區域 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 現在包含一項控制項，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，可協助您使用精細控制來管理資料駐留。	2021 年 11 月 30 日
Terraform 的 AWS Control Tower 帳戶工廠	AWS Control Tower 現在支援 Terraform 來自動佈建和更新帳戶。	2021 年 11 月 29 日
可用的新生命週期事件	`PrecheckOrganizationalUnit` 事件會記錄是否有任何資源阻止擴展控管任務成功，包括巢狀 OUs 中的資源。	2021 年 11 月 18 日
可用的巢狀 OUs	AWS Control Tower 現在可讓您的登陸區域包含巢狀 OU 結構。	2021 年 11 月 16 日

Detective 控制並行	AWS Control Tower 偵測控制項現在支援並行啟用和停用操作。	2021 年 11 月 5 日
兩個可用的新區域	AWS Control Tower 現已在兩個新 AWS 區域提供：歐洲（巴黎）區域和南美洲（聖保羅）區域。	2021 年 7 月 29 日
區域取消選取	您可以取消選取您不想再透過 AWS Control Tower 管理 AWS 的區域。	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，以加密您的資料和資源。	2021 年 7 月 28 日
變更為受管政策	我們變更了 AWSControlTowerServiceRolePolicy，讓客戶可以針對 AWS CloudTrail 日誌使用自己的 KMS 加密金鑰。	2021 年 7 月 28 日
控制項名稱已變更，功能不變	已更新某些控制項名稱和描述，以更好地反映控制項的政策意圖，而不會變更功能。	2021 年 7 月 26 日
受管 SCPs的自動化掃描	AWS Control Tower 會執行受管 SCPs 的每日自動化掃描，以檢查是否有偏離。	2021 年 5 月 11 日
OUs 和帳戶的自訂名稱	AWS Control Tower 可讓您在登陸區域設定程序期間為基本 OUs 和帳戶提供自訂名稱，而無需建立偏離。	2021 年 4 月 16 日

停用登陸區域是自助式	AWS Control Tower 現在可讓您解除委任登陸區域，而無需聯絡 AWS Support。解除委任是無法復原的半自動程序。這與手動刪除所有 AWS Control Tower 資源不同。	2021 年 4 月 9 日
三個額外區域	AWS Control Tower 現已在三個額外 AWS 區域提供：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
新的日誌封存控制項，提供登陸區域 2.7 版	四個新的 Log Archive 控制項透過 AWS Control Tower 資源提供日誌封存控管，與 AWS Control Tower 外部資源的控管分開。四個現有控制項的指引已從強制性變更為選擇性。AWS Control Tower 登陸區域的 2.7 版包含 HTTPS 的需求，更新後將無法復原。	2021 年 4 月 8 日
區域選擇	AWS Control Tower 區域選擇可讓您更妥善地管理 AWS Control Tower 資源的地理足跡。若要擴展託管 AWS 資源或工作負載的區域數量，基於合規、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
同時向 AWS Control Tower 註冊 OU 並控管其所有帳戶	AWS Control Tower 新增了註冊 OU 的功能，這是同時將多個帳戶引入控管的一種方式。	2021 年 1 月 28 日

已註冊 OUs中的多個帳戶更新	您現在可以從 AWS Control Tower 儀表板，一鍵更新任何包含最多 300 個帳戶之已註冊 AWS Organizations 組織單位 (OU) 中的所有帳戶。多個帳戶更新功能也稱為大量更新，不需要一次更新一個帳戶，或使用外部指令碼在多個帳戶上執行更新。	2021 年 1 月 28 日
用於彙總未受管 OUs 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 不需要存取未受管帳戶。	2020 年 12 月 29 日
AWS Control Tower 可在更多 AWS 區域使用。	AWS Control Tower 現已可在亞太區域（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）區域部署。透過此啟動，AWS Control Tower 現已在 10 AWS 區域提供。此登陸區域更新包含所有列出的區域，且無法復原。將登陸區域更新至 2.5 版之後，您必須手動更新 AWS Control Tower 的所有註冊帳戶，以在 10 個支援的區域中進行管理。 AWS	2020 年 10 月 8 日
控制更新	已針對強制性控制項 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。	

AWS Control Tower 現在提供相關資訊頁面	相關資訊頁面可讓您更輕鬆地找到設定 AWS Control Tower 登陸區域後可能有幫助的常見任務。	2020 年 9 月 18 日
AWS Control Tower 主控台會顯示有關 OUs和帳戶的詳細資訊。	在 AWS Control Tower 主控台中，您可以檢視有關 AWS 帳戶和組織單位 (OUs的詳細資訊。「帳戶」頁面現在會列出組織中的所有帳戶，無論 AWS Control Tower 中的 OU 或註冊狀態為何。您現在可以搜尋、排序和篩選所有資料表。	2020 年 7 月 22 日
AWS Control Tower 允許現有組織設定登陸區域	您現在可以在現有組織中啟動 AWS Control Tower 的登陸區域，讓組織受到控管。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 現已在亞太區域提供	AWS Control Tower 現已可在亞太區域（雪梨）AWS 區域部署。此版本需要手動更新付費帳戶，只有在您計劃在亞太區域（雪梨）執行工作負載時才會更新。	2020 年 3 月 3 日
可以停用 AWS Control Tower 登陸區域	AWS 支援可協助您透過保留組織的大多數自動化程序永久停用登陸區域，但需要一些手動清除。	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
設定和活動頁面適用於 AWS Control Tower	[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。	2019 年 11 月 30 日
AWS Control Tower 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 提供其他偵測性控制	AWS Control Tower 中的 Detective 控制項會提供組織和資源狀態的相關資訊。	2019 年 8 月 27 日
AWS Control Tower 現已正式推出	AWS Control Tower 是一項服務，提供最簡單的方法來大規模設定和管理您的多帳戶 AWS 環境。	2019 年 6 月 24 日

AWS 詞彙表

如需最新的 AWS 術語，請參閱 AWS 詞彙表 參考中的AWS 詞彙表。

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。