設定安全且可擴展的多帳戶 AWS 環境

AWS 方案指引

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

AWS 方案指引: 設定安全且可擴展的多帳戶 AWS 環境

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

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

Table of Contents

簡介 1
什麼是登陸區域？ 2
多帳戶架構 2
建置登陸區域 3
AWS Control Tower 4
自訂建置的登陸區域 6
建議方法 6
後續步驟 7
影片 7
文件 7
文件歷史紀錄 8
..... ix

設定安全且可擴展的多帳戶 AWS 環境

Nivas Durairaj 和 Jan Hertsens，Amazon Web Services

2024 年 7 月 (文件歷史記錄)

組織必須平衡建置者的需求，才能保持敏捷，同時提供大規模的控管。建立基礎標準可讓您啟用、佈建和操作您的環境，以實現業務敏捷性和大規模控管。

成功的雲端採用從安全的雲端型環境開始，其中包括：

- 具有多帳戶架構 AWS 的環境
- 初始安全性基準
- 身分與存取管理
- 控管
- 資料安全
- 網路設計
- 日誌

我們是指具有這些功能的環境，做為登陸區域。本指南可協助您設定安全且可擴展的登陸區域，以支援遷移的生產實作。

什麼是登陸區域？

登陸區域是架構良好的多帳戶 AWS 環境，可擴展且安全。這是您的組織可以放心地快速啟動和部署工作負載和應用程式的起點。建置登陸區域涉及根據組織的未來成長和業務目標，跨帳戶結構、聯網、安全和存取管理做出技術和業務決策。

當您開始 AWS 大規模使用 時，您可以查看 AWS 以取得規範性指導，以及建立環境的方法。此區域中心的 AWS 最佳實務是關於將資源和工作負載隔離到多個 AWS 帳戶 （資源容器） 以降低隔離和影響範圍的需求。下一節說明為什麼要使用多個帳戶。

多帳戶架構

雖然您應該沒有帳戶的標準數量 AWS ，但我們建議您建立多個 AWS 帳戶。多個帳戶提供最高層級的資源和安全隔離。如果您對下列任何問題回答是，請考慮建立其他 AWS 帳戶：

- 您的企業是否需要工作負載之間的管理隔離？
- 您的企業是否需要工作負載的有限可見性和可探索性？
- 您的企業是否需要隔離，以將影響範圍降至最低？
- 您的企業是否需要強烈隔離復原或稽核資料？

以下是單一帳戶可能不夠的其他原因：

- 安全控制 – 不同的應用程式可能有不同的安全設定檔，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更為容易。
- 隔離 – 帳戶是安全保護的單位。帳戶中應包含潛在風險和安全威脅，而不會影響其他帳戶。由於多個團隊或不同的安全設定檔，不同的安全需求可能需要您隔離一個帳戶與另一個帳戶。
- 資料隔離 – 將資料存放區隔離到帳戶會限制可存取和管理該資料存放區的人數。這可限制對高度私有資料的暴露，並有助於符合一般資料保護法規 (GDPR)。
- 許多團隊 – 不同的團隊有不同的責任和資源需求。他們不應該在同一個帳戶中以彼此的方式進入。
- 業務流程：不同的業務單位或產品可能有不同的目的和流程。您應該建立不同的帳戶，以滿足業務特定的需求。
- 帳單 – 帳戶是在帳單層級分隔項目的唯一真實方式，包括分隔轉移費用。多個帳戶可協助跨業務單位、職能團隊或個別使用者的帳單層級分隔項目。
- 限制配置 – 限制是以每個帳戶為單位。將工作負載分成不同的帳戶，可防止它們消耗限制或可能過度佈建資源，然後防止其他應用程式如預期般運作。

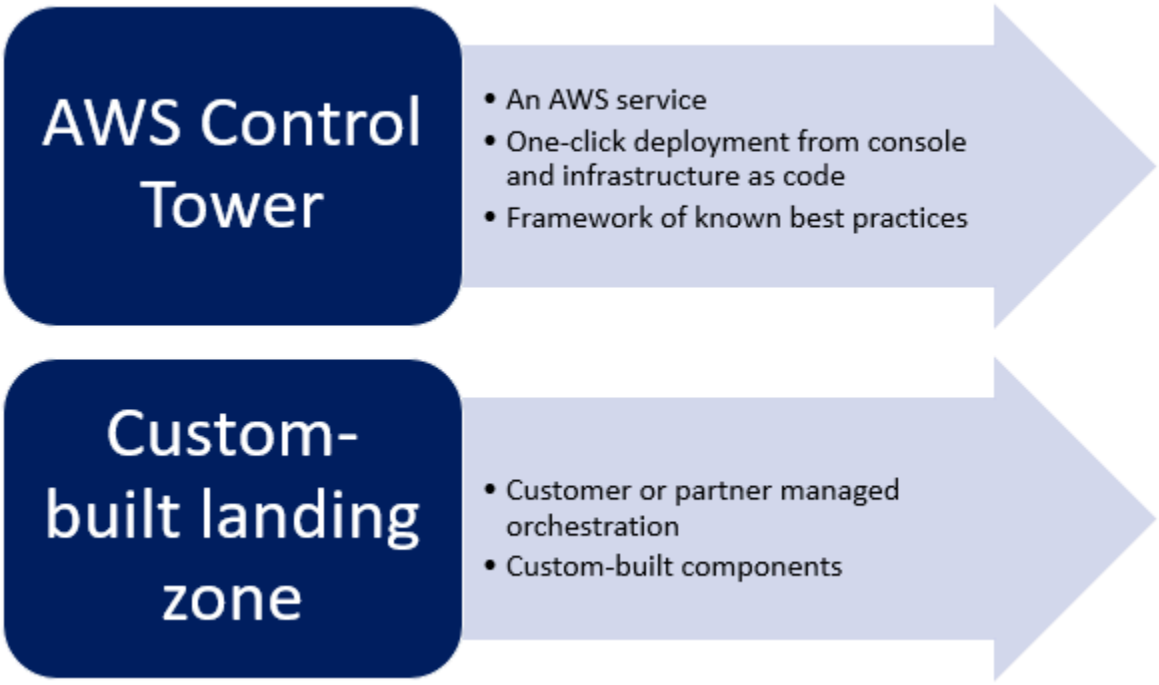
建置登陸區域

您有一些建立登陸區域的選項 AWS。您可以選擇受管服務來協調您的環境，或與合作夥伴合作來建置您自己的 受管服務。 AWS 提供 AWS Control Tower。我們建議所有使用者從 開始 AWS Control Tower。不過，請務必了解每種方法的差異和功能，以便為組織做出最佳決策。

上登陸區域的選項 AWS：

- AWS Control Tower
- 自訂建置的登陸區域

交付機制：



每種方法的優點和權衡：

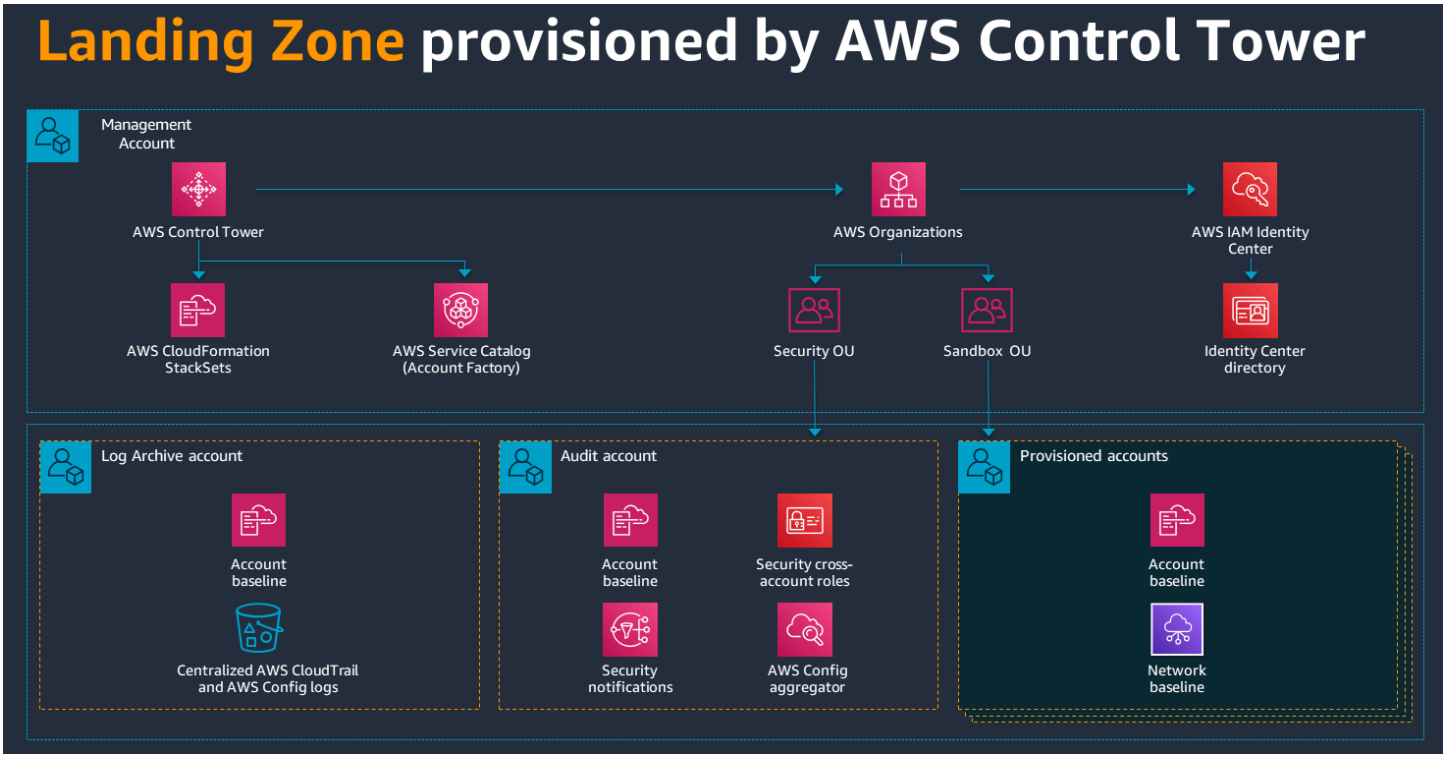
解決方案	優勢	取捨
AWS Control Tower	• 全受管服務。 • AWS依預設會套用 提供的控制項和合規政策。	• 自訂 for AWS Control Tower (CfCT) 和帳戶工廠 for Terraform (AFT) 提供額外的擴充性和自訂功能。

解決方案	優勢	取捨
	• 提供監控和合規狀態的中央儀表板。 • 提供帳戶工廠以佈建新帳戶。 • 某些自訂項目 （例如區域選擇和選用控制項） 可在 主控台中使用。	• AWS Control Tower 區域AWS 服務清單中顯示的 AWS 區域支援 。
AWS Organizations 使用客戶或合作夥伴建置的自訂解決方案	• 自訂建置的解決方案。	• 客戶或合作夥伴擁有所有開發和編碼。 • 客戶或合作夥伴負責整合和實作。

所有多帳戶環境產品均採用 技術 AWS Organizations。 AWS Organizations 提供基礎基礎設施和功能，供您建置和管理 AWS 環境。使用 AWS Organizations，您可以採用 提供的多帳戶策略指引 AWS ，並自行自訂您的環境，以符合您的業務需求。如果您是現有客戶，並且對目前的 AWS Organizations 實作感到滿意，您應該繼續操作目前的 AWS 環境。

AWS Control Tower

AWS Control Tower 會以 AWS 受管服務的形式執行。當您正在尋找開箱即用的預先封裝環境解決方案時，您可以使用 AWS Control Tower 進行規範指引和全受管環境。服務會根據多帳戶最佳實務來設定登陸區域、集中身分和存取管理，以及建立預先設定的安全和合規控管規則。



AWS Control Tower 使用最佳實務、身分藍圖、聯合存取和帳戶結構，自動設定新的登陸區域。在 上實作的一些藍圖 AWS Control Tower 包括：

- 使用 的多帳戶環境 AWS Organizations
- 使用 AWS Identity and Access Management (IAM) 和 的跨帳戶安全稽核 AWS IAM Identity Center
- 使用 Identity Center 預設目錄進行身分管理
- 從 AWS CloudTrail Amazon Simple Storage Service (Amazon S3) 中集中記錄和 AWS Config 存放

控制項是為整體 AWS 環境提供持續控管的高階規則。控制項可以是預防性或偵測性。預防性控制是使用服務控制政策 (SCPs) 實作的，這是其中的一部分 AWS Organizations。Detective 控制項是使用 實作 AWS Config。 AWS Control Tower 控制項的範例包括：

- 不允許為根使用者建立存取金鑰
- 不允許透過 RDP 進行網際網路連線
- 不允許公開寫入存取 S3 儲存貯體
- 不允許未連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store (Amazon EBS) 磁碟區

> **Note**
>
> AWS Control Tower 是登陸區域的起點。您需要在建置登陸區域時，根據獨特需求來決定聯網、存取管理和安全性的策略。

自訂建置的登陸區域

您可以選擇建置自己的自訂登陸區域解決方案。在此情況下，您會實作基準環境，以開始使用身分和存取管理、控管、資料安全、網路設計和記錄。如果您想要從頭開始建置所有環境元件，或是只有自訂解決方案可以支援的需求，建議您使用此方法。您必須在 部署解決方案後，擁有足夠的專業知識 AWS 來管理、升級、維護和操作解決方案。

建議方法

我們建議您從 開始 AWS Control Tower 建置登陸區域。 AWS Control Tower 可協助您建置初始的規範性登陸區域組態、使用out-of-the-box控制項和藍圖，以及使用 AWS Control Tower Account Factory 建立新帳戶。

在設定期間，您可以從 AWS Control Tower 主控台自訂登陸區域。如需詳細資訊，請參閱 AWS Control Tower 文件。設定基礎登陸區域之後，請使用下列其中一個選項來進一步增強和自訂它：

- 使用 Customizations for AWS Control Tower (CfCT)，透過 CloudFormation 範本和服務控制政策 (SCPs) 提供廣泛的自訂選項。如需詳細資訊，請參閱 AWS Control Tower 文件。
- 使用登陸區域加速器 (LZA) 增強您的登陸區域，以符合合規架構。如需詳細資訊，請參閱 LZA 實作指南。

後續步驟

您現在應該更了解登陸區域 AWS。如果您有更多問題或想要開始建置您的登陸區域，請聯絡您的 AWS 客戶團隊尋求協助。

如需其他檢閱和詳細資訊，請參閱下列各節中連結的一些文件和影片。

影片

- 建構整個登陸區域的安全性和管理
- 什麼是 AWS Control Tower？

文件

- 雲端治理
- AWS Control Tower
- AWS Control Tower 控制項程式庫
- 自訂您的 AWS Control Tower 登陸區域
- 自訂 for AWS Control Tower (CfCT)
- AWS Organizations
- 服務控制政策 (SCP)
- 使用 Account Factory 佈建和管理帳戶
- 使用 Account Factory for Terraform (AFT) 佈建 AWS Control Tower 帳戶
- CloudFormation
- AWS Service Catalog

文件歷史紀錄

下表描述了本指南的重大變更。如果您想收到有關未來更新的通知，可以訂閱 RSS 摘要。

變更	描述	日期
更新資訊	更新自訂登陸區域的相關資訊。	2024 年 7 月 30 日
初次出版	—	2020 年 3 月 16 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。