管制 AWS 登陸區域中的 OU 結構：來自製藥產業的範例

AWS 方案指引

AWS 方案指引: 管制 AWS 登陸區域中的 OU 結構：來自製藥產業的範例

Table of Contents

管制 AWS 登陸區域中的 OU 結構：製藥產業的範例

Katja Mueller、Petar Forai 和 Keval Sheth，Amazon Web Services (AWS)

2023 年 3 月 (文件歷史記錄)

AWS 提供多種 Landing Zone Accelerator 組態，支援特定產業，包括醫療保健。Landing Zone Accelerator for Healthcare 與 搭配使用 AWS Control Tower ，以簡化多帳戶環境的管理和管控，此環境符合 AWS 最佳實務和多個全球合規架構。協調控管的一個重要方面是使用組織單位 (OUs AWS 帳戶 分組在一起，以便您可以將它們作為單一單位進行管理。

本指南討論重新設計現有 OU 結構的最佳實務和考量事項，因為貴公司的雲端成熟度不斷增加。它介紹了一個以大型製藥公司的 AWS Control Tower 實作為基礎的實際範例，並討論從該實作中學到的經驗。 AWS 登陸區域設計不是一次性的工作。它可以且應該允許發展。透過套用本指南中強調的 AWS 最佳實務和秘訣，即可成功且有效率地實現此演變。

概觀

我們與一家多國製藥公司合作，在 上執行proof-of-concept(PoC) 活動 AWS ，以探索他們如何將其應用程式從現場部署遷移到 AWS 雲端。當他們開始擴展和加速遷移工作流程以包含生產工作負載時，很明顯地，他們需要受管制且合規的 AWS 登陸區域來支援他們的目標。我們曾經AWS Control Tower設計和實作新的 AWS 登陸區域。

新 AWS 登陸區域及其組織的重要層面是其組織單位 (OUs的結構。OU 是使用 AWS 帳戶 建立的邏輯群組AWS Organizations。您可以使用 OUs AWS 帳戶 組織階層，並一致且更輕鬆地套用管理和控管控制。

您可以將政策型控制項連接到 OU 和 AWS 帳戶。OUs 中的子 OU 會自動繼承這些控制項。因此，OUs 中管理安全與控管方面扮演重要角色 AWS Organizations。

政策是 JSON 文件，其中包含一或多個陳述式，定義您要套用至 群組的控制項 AWS 帳戶。 AWS Organizations 目前支援四種類型的政策，也稱為服務控制政策 SCPs)。SCP 定義可用於不同 的 AWS 服務 和 動作 AWS 帳戶。例如，您可以使用 SCP 要求 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體啟動以使用特定執行個體類型。

政策類型

SCP 政策類型包括下列項目：

- 允許清單和拒絕清單是補充策略，可用來套用 SCPs 來篩選帳戶可用的許可。
- 標籤政策可協助您維持一致的標籤，包括跨帳戶的標籤索引鍵和標籤值的偏好大小寫處理。
- 備份政策會為支援的資源類型設定備份，例如備份的時間範圍和備份的目的地保存庫 AWS 區域。
- AI 服務選擇退出政策可啟用或停用全球 AWS 人工智慧 (AI) 服務的持續改善。

政策繼承行為：當您將政策連接至特定 OU 時，直接在該 OU 或任何子 OU 下的帳戶會繼承政策。當您將政策連接到特定帳戶時，政策只會影響該帳戶。您可以透過引入例外狀況政策來覆寫繼承的政策。繼承明確允許所有許可從根 (OU) 向下流到該 OU 和子 OU AWS 帳戶 中的每個 ，除非您明確拒絕許可。若要拒絕許可，您可以建立額外的政策，並將其連接到適當的 OU 或 AWS 帳戶。如需政策繼承和例外狀況的詳細資訊，請參閱 AWS Organizations 文件。

AWS Control Tower 也會使用 OU 結構提供自己的一組偵測和預防性控制 （ 也稱為護欄)。 AWS Control Tower 預防性控制會使用 中的 SCPs 防止動作 AWS Organizations。使用 對控制項進行組態

偏離的 Detective 控制報告 AWS Config。如需這些控制項的詳細資訊，請參閱 AWS Control Tower 文件。

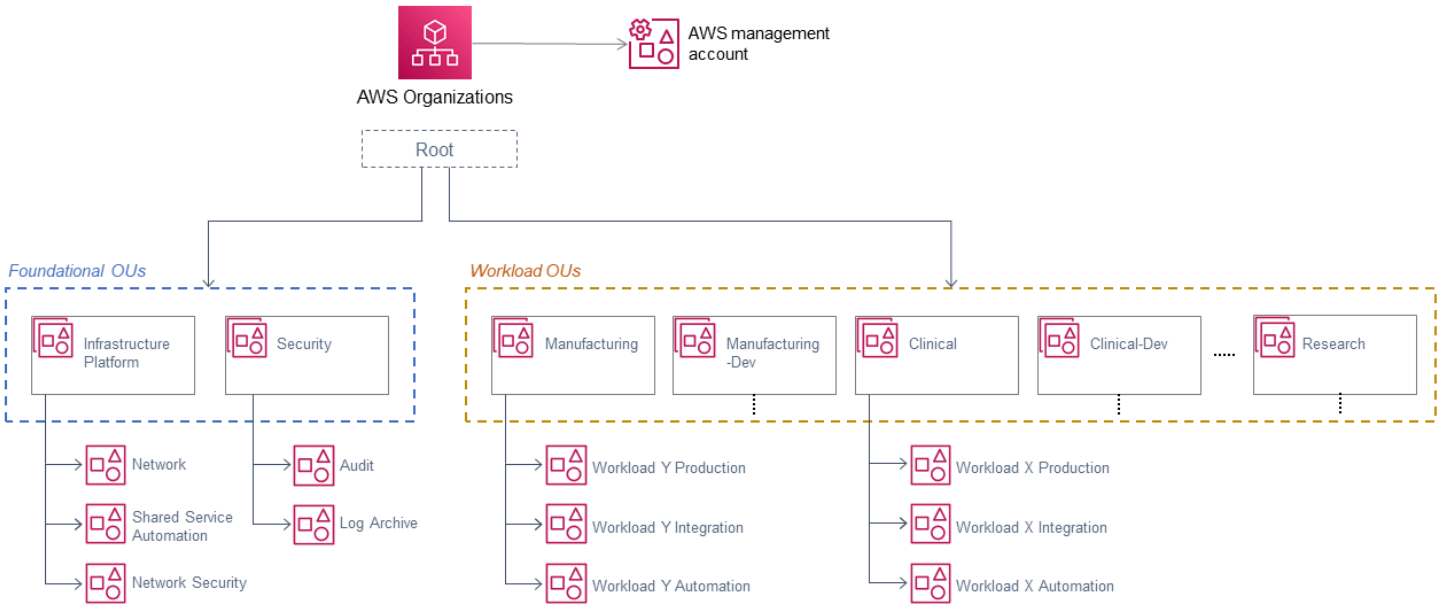
您也可以讓 AWS Security Hub CSPM 自動執行安全最佳實務檢查、將安全提醒彙總為單一位置和格式，以及了解所有 的整體安全狀態 AWS 帳戶。

OU 設計：階段 1

對於我們範例中的跨國製藥公司， 中組織和 OUs 的初始設計 AWS Organizations 嚴格遵循設定 AWS 建議 AWS Control Tower。如需範例，請參閱 AWS for Healthcare. AWS Control Tower initially provisioned a simple OU structure with common baseal OUs，如部落格文章 組織單位最佳實務 AWS Organizations中所述，包括 Security OU、 Platform Infrastructure OU 和 company-specific OUs。

架構設計

下圖顯示初始 OU 架構。



安全 OU

安全 OU 廣泛地將與安全功能 AWS 帳戶 相關的群組結合在一起，並使用兩個帳戶 (Audit 和 Log Archive) 來存放安全操作資料，以便集中記錄和稽核對環境的存取。 AWS 核心安全服務，例如 Amazon GuardDuty，並 AWS Security Hub CSPM 位於稽核帳戶中。

基礎設施平台 OU

AWS 帳戶 提供基礎設施基礎的基礎設施平台 OU 群組。最初部署在此 OU 中的 是中央聯網元件 （ 閘道、防火牆、中央聯網中樞和類似服務 ） AWS 帳戶 的 。

其他 OUs

其他公司特定的 OUs（例如臨床 OU) 會在低階階層中擴增基礎 OUs。工作負載會使用多帳戶結構和這些 OUs 中的個別環境來實作。

有幾個考量因素推動了此初始設計：

- 巢狀 OUs 目前無法在 中使用 AWS Control Tower ，且需要廣泛的自訂。
- 為雲端指定的初始工作負載著重於公司的特定層面，例如臨床試驗或製造設備分析（功能檢視）。
- 公司區分五個工作負載環境（開發、驗證、整合、訓練和生產）。公司需要遊樂場來開發應用程式，而不需透過 AWS 控制生產工作負載的嚴格控管。例如 Manufacturing-Dev OUs 等開發 OU 已為此目的指派。
- 工作負載自動化是每個應用程式生態系統的一部分，不需要分離。
- 基礎設施資格 (IQ) 和 GxP 合規程序不需要區分 OU 層級的 AWS 控制項。

OU 設計：第 2 階段

範例中的製藥公司透過將合格的生產工作負載部署到現有的 OUs，加速進入雲端成熟的新階段。這啟動了初始設計的審查，並挑戰了階段 1 結構，因為更多工作負載遷移到受管制的 AWS 登陸區域。

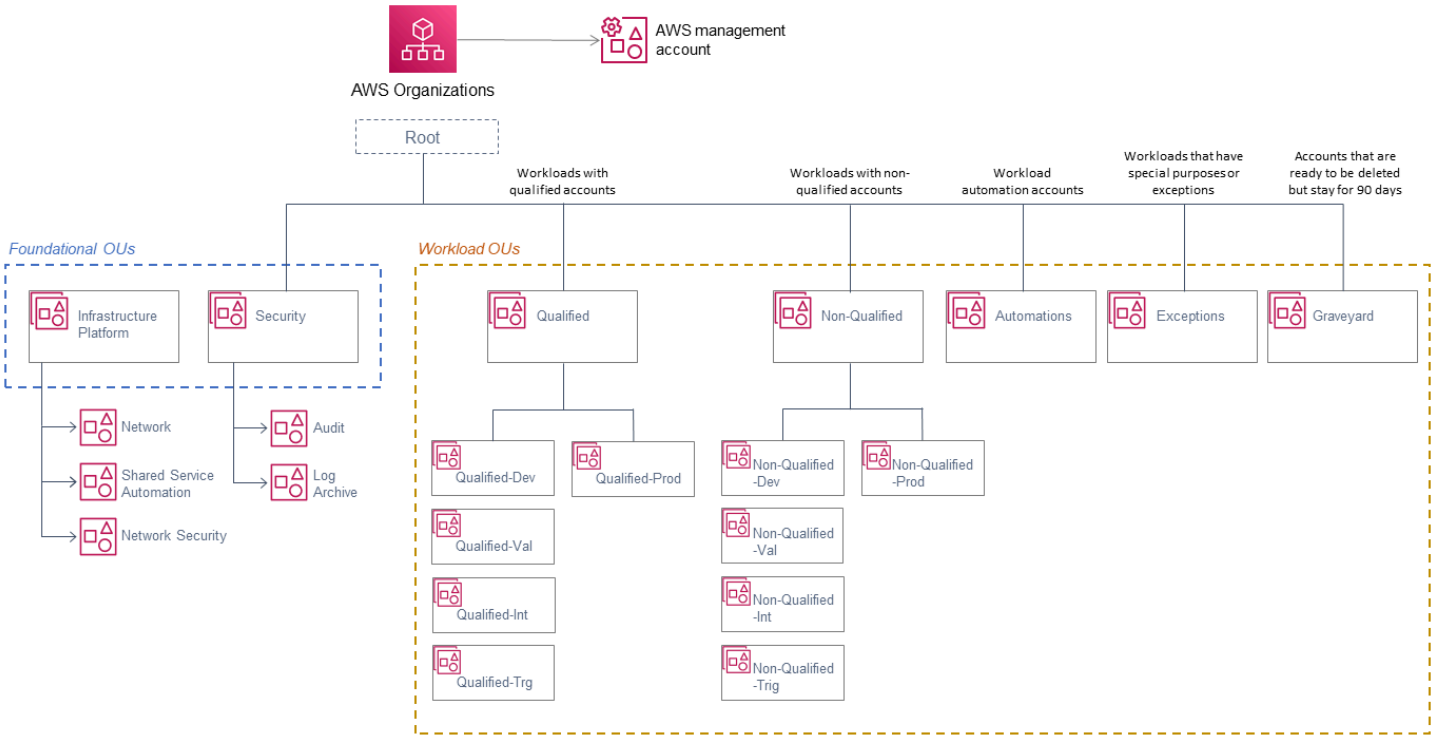
下列新要求和洞見變得重要：

- 公司實作了資料共用模型工作負載，因此應用程式取得了無法再指派給個別 OUs多用途性質，例如臨床或製造。
- 資格（特別是持續資格）成為許多工作負載的重要層面。這些工作負載必須整合到操作程序中，以便更輕鬆地遵循安全最佳實務。合格的工作負載需要更嚴格的 AWS 控制，這些控制是在階段 1 中的 OU 層級設定。
- 巢狀 OU 功能可在 中使用 AWS Control Tower。
- 提升技能和經驗可更深入了解哪些特定政策與工作負載相關。
- 公司根據責任一致性定義並商定了營運模型。
- 工作負載分割和結構化藍圖已成熟，並已用於工作負載遷移。

因此，在階段 2 中實作了新設計，並 AWS 帳戶 遷移至該新結構。此新結構包含以下各節所述OUs。

架構設計

下圖顯示階段 2 的 OU 架構。



安全 OU

安全 OU 包含與安全功能廣泛 AWS 帳戶 相關的 ，並使用兩個帳戶 (Audit 和 Log Archive) 來存放安全操作資料，以集中記錄和稽核對 environment. AWS core 安全服務的存取權，例如 Amazon GuardDuty，並 AWS Security Hub CSPM 位於稽核帳戶中。此 OU 與原始設計保持不變。

基礎設施平台 OU

基礎設施平台 OU 包含基礎基礎設施帳戶，例如整個 AWS 登陸區域的聯網和共用自動化。此 OU 與原始設計保持不變。

合格的 OU

合格 OU 包含需要合格基礎設施的工作負載，例如嚴格的變更管理、資格和驗證。

不合格的 OU

不合格的 OU 包含的工作負載沒有 GxP 要求或不具業務關鍵性的工作負載。

自動化 OU

Automations OU 包含工作負載自動化的共用資源，例如用於基礎設施管理的持續整合和持續交付 (CI/CD) 管道。根據需求，自動化可以跨環境分割或以單一 託管 AWS 帳戶。

例外狀況 OU

例外狀況 OU 包含需要特殊處理的工作負載，否則政策會阻止這些工作負載。例如，廣泛存取且可讀取的 Amazon Simple Storage Service (Amazon S3) 儲存貯體會屬於例外狀況 OU。

Graveyard OU

Graveyard OU 包含將刪除的 AWS 帳戶 工作負載。應移除這些帳戶中的政策，以取得有效且簡單的管理存取權，直到帳戶過期或刪除為止。

OU 遷移和驗證

對於我們範例中的跨國製藥公司，雲端平台工程和變更管理團隊同意遷移計畫和排程。 AWS 帳戶 我們已根據業務影響和重要性進行審核和排名，作為規劃的一部分。

新的 OU 結構與現有的 OU 結構並排部署，以允許新政策和增量遷移的預備。我們建立了具有子 OUs 的新空白 OUs並將 AWS Organizations 政策和 AWS Control Tower 控制項指派給這些子 OUs。

AWS Organizations 政策是透過在新結構上套用所需的政策來手動遷移。我們使用手動 Spot 檢查來驗證 AWS Organizations 政策和自動化機制來驗證 AWS Control Tower 控制項。只有在這些檢查成功之後， AWS 帳戶 才會移至新的 OUs。

帳戶遷移是半自動化的，並遵循交錯或批次方法。視為較不重要的初始遷移 AWS 帳戶 目標， AWS 帳戶 每次遷移執行使用批次 5。遷移批次不超過 10 個帳戶。遷移帳戶時，檢閱者和測試人員會使用 AWS Control Tower 主控台來驗證這些帳戶是否已移至正確的 OU，並監控 AWS CloudTrail 日誌是否有錯誤。檢閱者也會檢查 AWS Service Catalog 和 AWS Control Tower 主控台是否有任何漂移或處於污點或未知狀態的帳戶。

帳戶 OU 放置的變更不會影響 資源的連線能力或可存取性。生產應用程式中未報告中斷。

經驗教訓和最佳實務

- OU 結構設計並非一次性工作。隨著公司提高雲端採用率並將其他工作負載遷移到 AWS 登陸區域，其 OU 設計（隱含其政策概念）也會自然發展。
- 不要誤認為資料夾OUs；將它們視為政策的目標。OUs 及其階層提供 的結構元素， AWS 帳戶 應一律視為 政策的容器。建議您將需要相同政策集的所有 AWS 帳戶 放入相同的 OU。本指南也延伸至巢狀 OUs(OUs內的 OUs)。

  AWS 需要集中共用功能和跨工作負載資料共用功能（在企業資料平台中經常出現）的環境，較容易容納在非以業務單位 (LOB) 函數分類為基礎的 OU 結構中。例如，在 中的政策方面，製造應用程式的生產環境與臨床試驗分析應用程式的生產環境並無不同 AWS Organizations。
- 遵守並使用繼承。當您將政策連接到特定 OU 時， AWS 帳戶 這些 OU 會直接在該 OU 下方或任何子 OU 下繼承政策。當您將政策連接至特定 時 AWS 帳戶，政策只會影響該 AWS 帳戶。

  從一個 OU 結構到另一個 OU 結構的遷移工作取決於在 OU 或 AWS 帳戶 層級設定現有政策的廣泛程度。另一個重要因素是現有 OU 階層中使用多少政策繼承，或繼承是否中斷。遷移的複雜性會隨著不規則或偏離繼承路徑的實作而增加。例如，如果您在個別 AWS 帳戶 層級套用政策，或經常發生政策例外狀況（中斷繼承），將這些政策遷移到新結構將花費更多精力。在這種情況下，在遷移規劃期間，我們建議您花時間檢閱和重新設計政策繼承。
- 同時負責 AWS Organizations 政策和 AWS Control Tower 控制。OU 結構在 AWS Control Tower 和之間共用 AWS Organizations。 AWS Control Tower 提供自己的一組偵測和預防性控制。這些控制項適用於 AWS 帳戶 或 OU 層級。 AWS Organizations 會協調 OU 層級上的政策。在 OU 遷移中，我們建議您先遷移 AWS Organizations 政策，因為這些政策具有更多合規性權重。我們建議您在第二個遷移步驟中將 AWS Control Tower 控制項套用至新的 OU 結構。
- 更新需要一些時間 AWS 帳戶。您必須使用 將現有的 AWS 帳戶 個別重新註冊到新的 OU 結構 AWS Control Tower。這需要一些時間。如果您有大量帳戶，建議您透過自動化簡化此工作，以控制和自動化 的 OU 放置 AWS 帳戶。以下是兩個範例案例：
  - 小型遷移的手動變更：遷移潛在客戶會將每個 AWS 帳戶 從其舊 OU 重新指派給 中的新 OU AWS 管理主控台。當所有 的重新指派完成時 AWS 帳戶，遷移潛在客戶會 AWS 帳戶 分別 AWS Control Tower 為每個 或所有 OUs 開啟。重新註冊 AWS 帳戶 每個 AWS Control Tower 需要 10-15 分鐘， AWS 帳戶 具體取決於帳戶 AWS 區域 中使用的數量。 AWS Control Tower 最多允許此類並行操作平行執行。
  - 自訂變更自動化：自動化簡化並節省工作量。例如，您可以自動管理從建立到遷移和終止的 AWS 帳戶 生命週期。您可以使用 AWS Control Tower Account Factory 來變更 的 OU 指派， AWS 帳戶 並執行重新註冊程序。此自動化支援數百個的大規模遷移 AWS 帳戶。

資源

- AWS Organizations 使用者指南 (AWS 文件）
- AWS Organizations 術語和概念 (AWS 文件）
- 服務控制政策 SCPs) (AWS 文件）
- AWS Organizations API 參考 (AWS 文件）
- AWS Control Tower 使用者指南 (AWS 文件）
- 醫療保健登陸區域加速器簡介 (AWS 部落格文章）
- 使用 AWS Organizations 和 管理多帳戶環境 AWS Control Tower (AWS 部落格文章）
- 使用 的組織單位最佳實務 AWS Organizations(AWS 部落格文章）
- AWS 安全參考架構 (AWS SRA) (AWS 方案指引）
- 在 上建立您的雲端基礎 AWS (AWS 白皮書）
- 使用多個帳戶組織您的 AWS 環境 (AWS 白皮書）

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
初次出版	—	2023 年 3 月 28 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。