AWS 決策指南

選擇 AWS 雲端控管服務

選擇 AWS 雲端控管服務: AWS 決策指南

Table of Contents

決策指南 1
AWS 雲端控管簡介 1
了解 2
考慮 3
選擇 4
使用 6
探索 10
文件歷史紀錄 11
..... xii

選擇 AWS 雲端控管服務

採取第一步

用途	協助判斷哪些 AWS 雲端控管服務最適合您的組織。
上次更新	2024 年 12 月 23 日
涵蓋的服務	• AWS Artifact • AWS Audit Manager • CloudFormation • AWS CloudTrail • AWS Config • AWS Control Tower • AWS Organizations • AWS Security Hub CSPM • AWS Service Catalog • AWS Systems Manager • AWS Trusted Advisor

AWS 雲端控管簡介

雲端控管是一組規則、程序和報告，可協助您根據業務目標調整 AWS 雲端 使用方式。

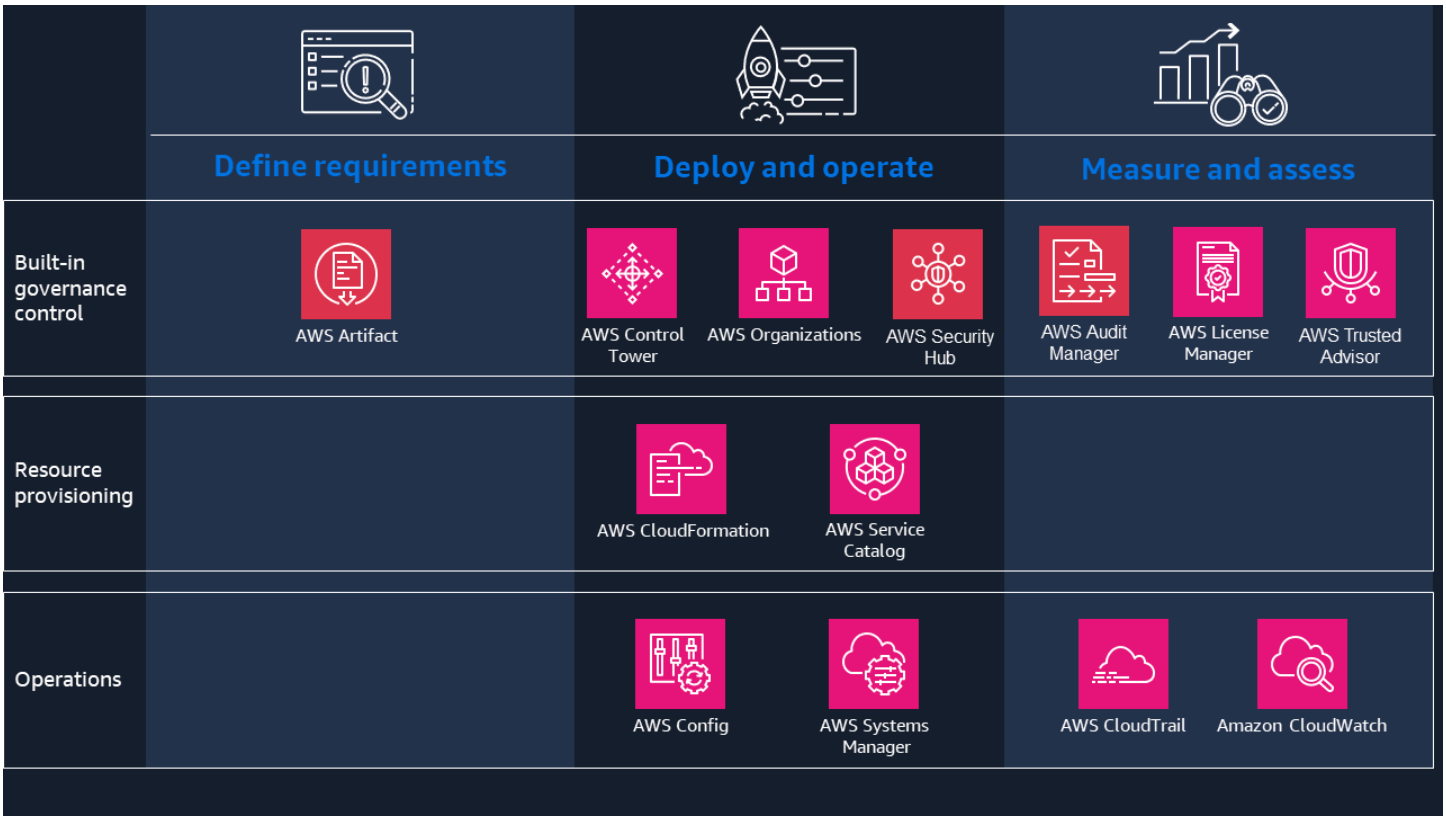
這透過啟用多帳戶策略、持續監控和控制政策來涵蓋安全性。它透過自動化檢查、報告和修復來涵蓋合規。它透過在企業範圍內套用控制項來涵蓋操作。它透過大規模集中身分和存取管理來涵蓋身分。它透過促進用量報告和政策強制執行來涵蓋成本。它涵蓋了彈性，透過協助將評估和測試整合到 CI/CD 管道以進行驗證。

我們提供各種服務，協助您設定、管理、監控和控制雲端中帳戶、服務和資源的使用，進而實作雲端控管最佳實務。

本指南旨在協助您決定哪些 AWS 雲端控管服務最適合您的組織、強化營運彈性、最佳化成本，以及建置控制以協助遵守法規或公司標準，同時維持開發速度並加速創新。

此影片是簡報的六分鐘區段，介紹雲端控管的最佳實務。

了解 AWS 雲端控管



上圖顯示雲端控管如何利用多個 AWS 服務，可讓您定義控管需求、部署和操作系統，以及測量和評估其效能。服務提供內建的控管控制、符合控管政策的資源佈建，以及可協助您監控和管理環境的操作工具。

利用 AWS 雲端控管服務可協助您確保雲端使用可支援您的業務目標。具體而言，它們可讓您改善開發人員的速度和敏捷性、在動態法規環境中運作、簡化合併和收購，以及強化營運恢復能力：

- 改善開發人員的速度和敏捷性 — 透過 APIs 快速旋轉新環境，確保您的開發人員不會等待數週的佈建週期，並加速佈建 CI/CD 管道。使用預先建置的控制項和規則，以及infrastructure-as-code範本，在軟體交付過程中及早發現並防止瑕疵，以有效率地佈建常見資源。
- 在動態法規環境中操作 - 建立永遠在線的界限，以保護和控制對跨 資料的存取 AWS、編纂您的合規要求，以及自動化整個組織的資源組態評估。
- 簡化合併和收購：透過建置安全、架構良好的多帳戶環境，更快速地遷移工作負載。集中帳戶建立、配置資源、群組帳戶，以及輕鬆快速地套用控管政策和控制項。採用程式設計方法來大規模管理多帳戶。

- 強化營運彈性：快速設定安全、架構完善且具彈性的多帳戶環境。執行工作負載的評估，以發現潛在的彈性相關弱點。針對成本最佳化、效能、安全性、容錯能力和服務限制等五個關鍵領域進行自動化檢查，並接收可讓您遵循已知最佳實務的建議。
- 最佳化成本：視覺化、了解和管理一段時間內的成本和用量。持續分析資源使用率、識別未充分利用的資源，以及終止閒置資源。

當您設定和操作工作負載時，可以有效地內建雲端控管最佳實務 AWS。互通性服務可協助您實現對 IT 資產的一致、集中式控管，包括 AWS 和第三方產品。跨 控制的範圍和深度 AWS 服務 可協助您滿足不斷變化的法規要求，並將安全風險降至最低。

考慮 AWS 雲端控管條件

下一節概述選擇雲端控管策略時需要考慮的一些關鍵條件。特別是討論不同類型的雲端環境、控制機制和開發人員支援可能適用於您組織和業務目標的機會。

Multi-account strategy

它是什麼：實作雲端環境最佳實務取決於採用安全的多帳戶策略。使用帳戶做為建置區塊，並將其分組到組織單位 (OUs)，例如安全性和基礎設施的基礎 OUs，以及沙盒和工作負載的其他 OUs。

為什麼重要：多帳戶策略可在您的雲端環境中提供自然界限和隔離。這反過來可讓您管理配額和帳戶限制、自動化帳戶的佈建和自訂，以及透過限制對管理帳戶的存取來套用最低權限原則。它可讓可見性追蹤整個環境的使用者活動和風險。您的多帳戶策略是您可以為遷移專案或合併和收購等組織變更建立的基礎。

使用 AWS Organizations 將多個 合併 AWS 帳戶 到組織，您可以使用它來配置資源、群組帳戶和套用控管政策。

使用 AWS Control Tower做為協同運作服務，疊加在上面 AWS Organizations，以協助建構您的 AWS 資產，並擴展對 OUs和多帳戶環境的控管。

Controls management best practices

它是什麼：實作控制管理最佳實務可以包含各種方法。Detective 控制項會擷取違反已定義安全政策的資源。預防性控制會封鎖特定動作來保護安全基準。在佈建之前主動控制掃描資源、停止部署不合規的程式碼，並指示開發人員修復這些資源。當您進入新市場時，可互通可讓您 AWS 服務 集中管理和控制整個 IT 資產，包括 AWS 和第三方產品。

為什麼重要：控制管理最佳實務可讓您以程式設計方式大規模實作控制，並自動設定合規或修復不合規。如果您的組織在受監管的產業中營運，例如醫療保健、生命科學、金融服務或公有部門，適用或遵循特定公司標準，或資料落地和數位主權要求，則這一點尤其重要。

考慮協調多個 的機會 AWS 服務 ，以確保您組織的安全和合規需求、使用 AWS Control Tower定義組態設定並偵測偏離情況、使用 AWS Config，以及使用 來稽核 AWS 使用情況以及是否符合法規和業界標準AWS Audit Manager。

Cloud governance for developers

它是什麼：為開發人員實作雲端控管最佳實務可以包括使用基礎設施做為程式碼 (IaC)，以確保其工作中的可重複性和一致性，以及建立偵測安全漏洞的程序。

為什麼重要：這有助於團隊快速行動，同時對其控管程序有信心。它為開發人員提供了單一的事實來源，可以部署到整個堆疊、他們可以複寫、重新部署和重新利用的基礎設施、一起控制基礎設施和應用程式版本控制的能力，以及自助服務動作的選擇。

開發人員的雲端控管也可以涉及偵測程式碼中的安全漏洞。這有助於他們改善程式碼品質、識別關鍵問題、確保一致的發行管道，以及使用藍圖啟動專案。

考慮如何為建置器提供預先核准的infrastructure-as-code範本，以及對應的 IAM 政策，這些政策規定了使用 AWS 服務 類似 Service Catalog 的人員、位置和方式。

Scalability and flexibility

內容：選擇 AWS 服務 可協助雲端控管措施與您的基礎設施無縫成長，並適應不斷變化的需求。考慮您的組織將如何成長，以及速度有多快。

為什麼重要：考慮可擴展性和靈活性有助於確保您的雲端控管安排強大、回應能力高，並且能夠支援動態商業環境。

為了協助您快速擴展， AWS Control Tower 會協調數個其他 的功能AWS 服務，包括 AWS Organizations 和 AWS IAM Identity Center，以在不到一小時的時間內建置登陸區域。Control Tower 會代表您設定和管理資源。

AWS Organizations 可讓您跨多個帳戶管理超過 40 個 服務的資源。這為個別應用程式團隊提供彈性和可見性，以管理工作負載特有的雲端控管需求，同時為集中式團隊提供可見性。

選擇 AWS 雲端控管服務

現在您知道要評估雲端控管選項的條件，您已準備好選擇最適合您組織需求的 AWS 雲端控管服務。下表重點介紹針對哪些情況最佳化哪些服務。使用它來協助判斷最適合您組織和使用案例的服務。

使用案例類型	您會何時使用它？	建議的服務
定義需求	提供隨需下載 AWS 的安全與合規文件。	AWS Artifact
部署和操作	使用基礎設施做為程式碼來加速雲端佈建。	AWS CloudFormation
	代表您的理想組態設定，並偵測 AWS 資源是否偏離。	AWS Config
	AWS 服務 代表您設定和協調多個 ，同時協助您滿足組織的安全和合規需求。	AWS Control Tower
	若要將多個 合併 AWS 帳戶 到組織，您可以使用它來配置資源、分組帳戶、套用控管政策，以及集中和大規模管理。	AWS Organizations
	對一組支援的安全標準中的規則執行自動化和持續檢查。	AWS Security Hub CSPM
	為了向建置器提供預先核准的infrastructure-as-code範本，以及對應的 IAM 政策，這些政策會決定誰、在哪裡以及如何使用它們。	Service Catalog
	提供多雲端和混合環境中和 上 AWS 資源的安全end-to-end管理。	AWS Systems Manager
測量和評估	稽核 AWS 用量，並評估風險和是否符合法規和業界標準。	AWS Audit Manager
	啟用您 的操作和風險稽核、控管和合規 AWS 帳戶。	AWS CloudTrail

使用案例類型	您會何時使用它？	建議的服務
	AWS 即時監控您的 AWS 資源和您在 上執行的應用程式。	Amazon CloudWatch
	集中管理來自跨 AWS 和您內部部署環境之廠商的軟體授權。	AWS License Manager
	根據最佳實務評估用量和組態。	AWS Trusted Advisor

使用 AWS 雲端控管服務

您現在應該清楚了解每個 AWS 雲端控管服務的功能，以及哪些可能適合您。

為了探索如何使用和進一步了解每個可用的 AWS 雲端控管服務，我們提供了途徑來探索每個服務的運作方式。下列各節提供深入文件、實作教學課程和其他資源的連結，協助您開始使用。

AWS Artifact

- 入門 AWS Artifact

  下載安全與合規報告、管理法律協議和管理通知。

  探索指南 »
- 在 中管理協議 AWS Artifact

  使用 AWS 管理主控台 來檢閱、接受和管理您帳戶或組織的協議。

  探索指南 »
- 準備第 1 AWS 部分 – AWS Audit Manager AWS Config、 和 中的稽核 AWS Artifact

  使用 AWS 服務 服務來協助您自動化稽核中使用的證據集合。

  閱讀部落格 »

AWS Audit Manager

- 入門 AWS Audit Manager

  使用 AWS 管理主控台、Audit Manager API 或 啟用 Audit Manager AWS CLI。

  探索指南 »
- 稽核擁有者教學課程：建立評估

  使用 Audit Manager 範例架構建立評估。

  教學課程入門 »
- 委派代表的教學課程：檢閱控制集

  檢閱 Audit Manager 中稽核擁有者與您共用的控制集。

  開始使用教學課程 »

AWS CloudTrail

- 檢視事件歷史記錄

  檢閱 中支援 CloudTrail AWS 帳戶 之服務的 AWS API 活動。

  開始使用教學課程 »
- 建立追蹤以記錄管理事件

  建立追蹤以記錄所有區域中的管理事件。

  開始使用教學課程 »

AWS Config

- AWS Config features

  探索 的資源追蹤功能 AWS Config，從組態歷史記錄和快照到可自訂的規則和一致性套件。

  探索指引 »
- 運作 AWS Config 方式

深入了解 AWS Config，並了解服務如何探索和追蹤資源，並透過各種管道交付組態項目。

探索指南 »

- 風險與合規研討會

  使用 AWS Config 和 AWS 受管 Config 規則來自動化控制項。

  探索研討會 »

- AWS Config 規則開發套件程式庫：大規模建置和操作規則

  使用規則開發套件 (RDK) 來建置自訂 AWS Config 規則，並使用 RDKLib 部署它。

  閱讀部落格 »

AWS Control Tower

- 入門 AWS Control Tower

  了解如何使用 AWS Control Tower 主控台或 APIs設定您的登陸區域。

  探索指南 »

- AWS Control Tower 控制管理研討會

  了解如何在您的多帳戶環境中設定控管，以符合 AWS 最佳實務和常見合規架構。

  探索研討會 »

- 使用 Amazon Bedrock 和 現代化帳戶管理 AWS Control Tower

  佈建安全工具帳戶，並利用生成式 AI 來加速 AWS 帳戶 設定和管理程序。

  閱讀部落格 »

- 使用 建置架構良好的 AWS GovCloud (US) 環境 AWS Control Tower

  在 AWS GovCloud (US) 區域中設定您的管理，包括使用組織單位 (OUs) 和 來管理 AWS 工作負載 AWS 帳戶。

  閱讀部落格 »

AWS Organizations

- 入門 AWS Organizations

  了解如何開始使用 AWS Organizations，包括檢閱術語和概念、使用合併帳單，以及套用組織政策。

  探索指南 »

- 建立和設定組織

  建立您的組織，並使用兩個 AWS 成員帳戶進行設定。

  開始使用教學課程 »

- 使用多個帳戶組織您的 AWS 環境

  了解使用多個 AWS 帳戶 如何協助隔離和管理業務應用程式和資料，並跨 AWS Well-Architected Framework 支柱進行最佳化。

  閱讀白皮書 »

- 使用 的服務 AWS Organizations

  了解您可以搭配哪些 AWS 服務 服務使用， AWS Organizations 以及在全組織層級使用每項服務的優點。

  探索指南 »

- 組織單位的 AWS Organizations最佳實務

  在建置組織時深入探索建議的 AWS 最佳實務架構，以取得 OU 結構和特定實作範例。

  閱讀部落格 »

- 使用 AWS Organizations SCPs 的設計考量來實現卓越營運

  了解 SCPs如何協助控制在組織內建立的多個帳戶之間佈建對 AWS 服務 和 資源的存取。

  閱讀部落格 »

AWS Security Hub CSPM

- 啟用 AWS Security Hub CSPM

在獨立帳戶中 AWS Security Hub CSPM 啟用 AWS Organizations 或 。

探索指南 »

- 跨區域彙總

  將 AWS Security Hub CSPM 問題清單從多個彙總 AWS 區域 到單一彙總區域。

  探索指南 »

- AWS Security Hub CSPM 研討會

  了解如何使用 AWS Security Hub CSPM 和 來管理和改善 AWS 環境的安全狀態。

  探索研討會 »

- 三種重複的 Security Hub 使用模式，以及如何部署它們

  了解三種最常見的 AWS Security Hub CSPM 使用模式，以及如何改善識別和管理問題清單的策略。

  閱讀部落格 »

探索 AWS 雲端控管資源

架構圖

探索參考架構圖，以協助您開發安全性、身分和控管策略。

探索架構圖

白皮書

探索白皮書，進一步了解選擇、實作和使用最適合您組織的安全性、身分和控管服務方面的洞見和最佳實務。

探索白皮書

解決方案

使用這些解決方案進一步開發和完善您的安全、身分和控管策略。

探索解決方案

文件歷史紀錄

下表說明此決策指南的重要變更。如需有關本指南更新的通知，您可以訂閱 RSS 摘要。

變更	描述	日期
初次出版	指南首先發佈。	2024 年 10 月 4 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。