轉換為多個 AWS 帳戶

AWS 方案指引

AWS 方案指引: 轉換為多個 AWS 帳戶

Table of Contents

轉換至多個 AWS 帳戶

Amazon Web Services （貢獻者）

2024 年 11 月 (文件歷史記錄)

許多公司透過使用單個 Amazon Web Services (AWS) 帳戶來開始他們的旅程。公司內有多個角色使用此帳戶來運營業務。工程師可開發程式碼、部署至開發和測試環境以及促進生產變更。產品經理會查詢資料來源，以收集業務績效的見解。銷售團隊正在生產環境中進行演示，以吸引新客戶。財務團隊正在從 AWS Billing 主控台監控雲端支出。

當所有這些不同的角色都使用單一角色時 AWS 帳戶，可能會難以強制執行套用最低權限許可的安全性最佳實務，這表示您只授予執行任務所需的最低許可。在新創公司發展的某個階段，會有人提出這個問題全部工程師都需要存取生產嗎？ 答案幾乎永遠是否定，但是許多公司總是在不減緩業務的情況下如何將現有的單一帳戶環境轉換為多帳戶環境而苦苦掙扎。

本指南包含協助您從單一帳戶環境轉換為多帳戶環境的最佳實務。它討論了您需要做出的有關帳戶遷移、使用者管理、聯網、安全性和架構的決策。它旨在協助您在最少或沒有停機時間的業務和日常營運中獲得成功。當您從單一 AWS 帳戶 轉換為多帳戶環境時，本指南著重於下列功能：

- 身分管理與存取控制
- 管理許可和存取
- 網路連線能力
- 安全事件回應
- 備份
- 帳戶遷移
- 資源遷移
- 帳單考量

如需功能的詳細資訊，請參閱 上的雲端基礎 AWS。

本指南與與本主題相關的現有資源保持一致，包括AWS 啟動安全基準 (AWS SSB)、使用多個帳戶組織 AWS 您的環境白皮書、AWS 安全參考架構 (AWS SRA) 和在白皮書上建立您的雲端基礎 AWS。您應該繼續使用這些資源，以獲取本指南未涵蓋的更具體指引。

目標對象

本指南最適合想要或需要轉換為 AWS 帳戶的公司。對於新創公司而言，當發現產品適合市場、籌集了一輪資金並開始聘用不同的工程學科 (例如基礎設施、開發操作 (DevOps) 或安全性) 人才時通常會產生這種需求。

即使您的公司還沒有準備好進行此轉換，仍然可以使用本指南來了解在轉換期間需要做出的決定並開始做好準備。

轉換為多帳戶架構的目標

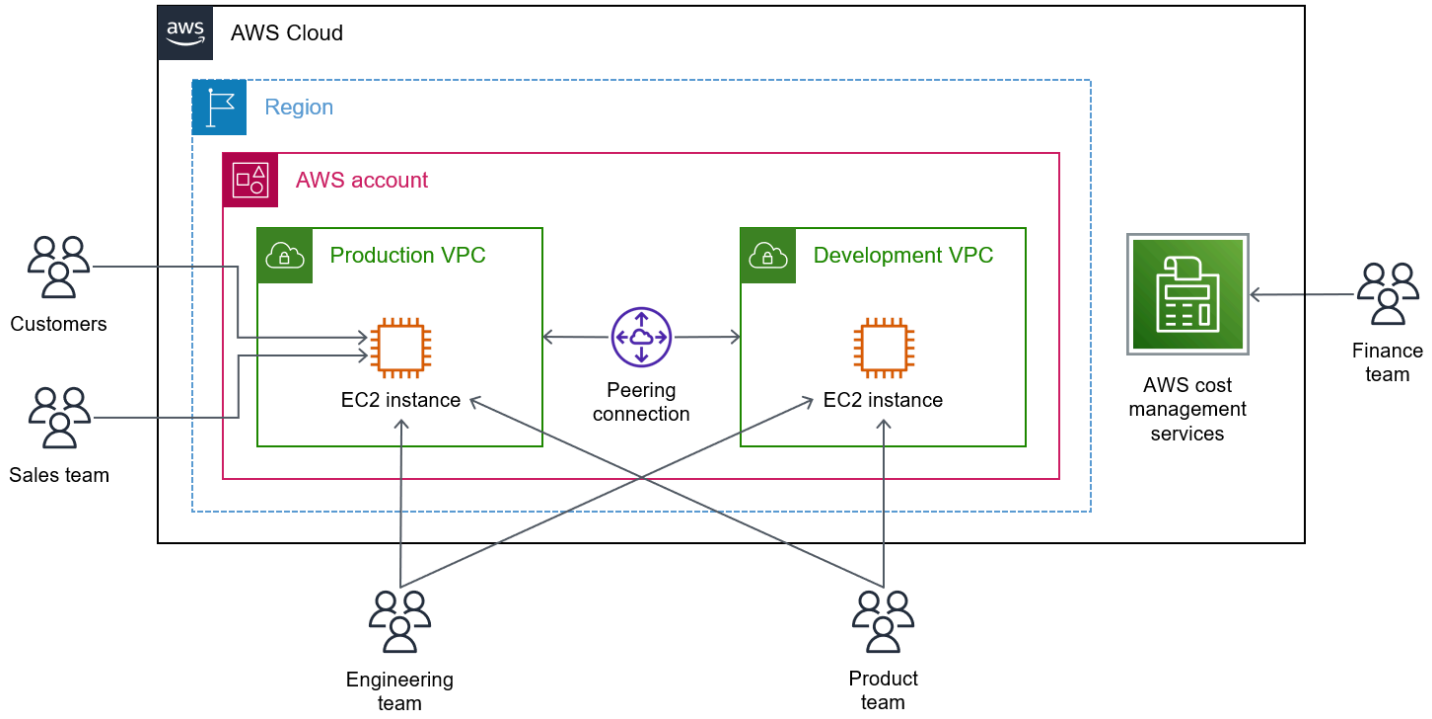
轉換為多帳戶架構通常由業務需求所驅動，具有下列一個或多個優點：

- 根據業務目的或擁有權將工作負載分組
- 依環境套用不同的安全控制
- 限制對敏感資料的存取
- 促進創新和敏捷性
- 限制不良事件所造成的影響範圍
- 支援多種 IT 操作模式
- 管理成本
- 分佈配額和 API AWS 服務 請求率限制

如需使用多帳戶架構之許多優點的詳細資訊，請參閱使用多個帳戶組織您的 AWS 環境 (AWS 白皮書）和設定良好架構環境的指導方針 (AWS Control Tower 文件）。

單一帳戶架構範例

新創公司或小公司最初通常會使用單一 AWS 區域 並具有兩個透過 VPC 對等互連進行連接的虛擬私有雲端 (VPC)。每個 VPC 都包含運算資源，例如 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體。工程團隊直接在開發 VPC 中開發程式碼。產品團隊會審核變更，然後工程團隊手動將變更推進至生產 VPC。財務團隊可以存取 ， AWS 帳戶 以便他們可以檢閱 AWS 帳單與成本管理 主控台。



以下是公司在此環境下可能會遇到的幾個挑戰範例：

- 工程師認為他們正在存取開發資料庫時，錯誤地刪除了生產資料。
- 當生產部署所花費的時間超過預期時，銷售演示會受到影響。
- 當開發程式碼正在進行負載測試時，生產 VPC 變得緩慢並產生有關限流的錯誤消息。
- 財務團隊無法區分生產和開發環境的成本。
- CEO 擔心一些新聘用的離岸承包商可以透過生產 VPC 來存取客戶資料。
- 財務團隊無法禁止存取 AWS 服務 可能會產生高成本的特定 。

採用多帳戶策略可解決所有這些挑戰，方法是使用分隔化 AWS 帳戶 來分隔工作負載和存取。

轉換為多帳戶架構的基礎框架和安全責任

本指南中的資訊和最佳實務旨在補充基礎設施和安全性的現有 AWS 建議。當您從單一 AWS 帳戶 轉換到多個 時 AWS 帳戶，請務必確保您的新多帳戶架構符合 AWS Well-Architected Framework 和 Cloud Foundation 原則。這可協助您建置和操作專為安全性、效能和彈性而設計的環境，同時遵守控管要求和 AWS 最佳實務。

AWS Well-Architected 架構

AWS Well-Architected Framework 可協助您為應用程式和工作負載建置安全、高效能、彈性且高效率的基礎設施。本指南與此框架的卓越運營、安全性以及可靠性要件保持一致。這可協助您遵循目前的 AWS 建議，滿足您的業務和法規要求。

您可以使用 AWS 帳戶中的 AWS Well-Architected Tool 來評估您對良好架構的最佳實務的遵守情況。

上的雲端基礎 AWS

在 （白皮書） 上建立您的雲端基礎 AWS提供指引，協助您量身打造 AWS 環境，以滿足業務需求。AWS 您可以使用以功能為基礎的方法來建立環境，以部署、操作和管理工作負載。您還可以隨著需求的發展和向雲端部署額外的工作負載來增強擴展環境的能力。如需 定義的 30 項功能的詳細資訊 AWS，請參閱功能。本指南包含按預期順序實作初始功能的最佳實務。

您可以根據自己的操作和控管需求來採用和實作功能。隨著業務需求成熟，基於功能的方法可用作一種機制，以驗證您的雲端環境是否已準備好支援工作負載並視需要進行擴展。這種方法可讓您自信地為建置者和業務建立雲端環境。

轉換為多帳戶架構的身分管理與存取控制

轉換為多帳戶架構時，第一步是在組織內設定新帳戶架構。然後，可以新增使用者並設定他們對帳戶的存取權。本節介紹了在多個 AWS 帳戶中管理存取權的方法。

本節包含下列任務：

- 設定組織
- 建立登陸區域
- 新增組織單位
- 新增初始使用者
- 管理成員帳戶

設定組織

當您有多個 時 AWS 帳戶，您可以透過 中的組織以邏輯方式管理這些帳戶AWS Organizations。中的帳戶 AWS Organizations 是標準 AWS 帳戶 ，其中包含您的 AWS 資源和可存取這些資源的身分。組織是合併 的實體 AWS 帳戶 ，讓您可以以單一單位管理它們。

當您使用帳戶建立組織時，該帳戶會變為組織的管理帳戶 (也稱為付款人帳戶或者根帳戶)。一個組織只能有一個管理帳戶。當您將其他 AWS 帳戶 新增至組織時，它們會成為成員帳戶。

> **Note**
>
> 每個 AWS 帳戶 也具有稱為根使用者的單一身分。可以使用用來建立帳戶的電子郵件地址和密碼，以根使用者的身分登入。不過，強烈建議您不要以根使用者身分處理日常任務，即使是管理任務。如需詳細資訊，請參閱 AWS 帳戶 根使用者。
> 我們也建議集中成員帳戶的根存取權，並從組織中的成員帳戶移除根使用者憑證。

在階層式樹狀結構中組織帳戶，該結構包含組織根、組織單位 (OU) 以及成員帳戶。根是組織中所有帳戶的父級容器。組織單位 (OU) 是根中帳戶的容器。OU 可以包含其他 OU 或成員帳戶。OU 可以僅有一個父級，並且每個帳戶只能是一個 OU 的成員。如需詳細資訊，請參閱術語和概念 (AWS Organizations 文件) 。

服務控制政策 (SCP) 會指定使用者和角色可以使用的服務和動作。SCPs類似於 AWS Identity and Access Management (IAM) 許可政策，但不授予許可。相反，SCP 會定義最大許可。當您將政策附接

至階層中的其中一個節點時，它會套用至該節點內的所有 OU 和帳戶。例如，如果將政策套用至根，則它將套用至組織中的所有 OU 和帳戶，如果將政策套用至 OU，則它將僅套用至 OU 以及目標 OU 中的帳戶。

資源控制政策 (RCP) 可讓您集中控制組織中資源的可用許可上限。RCPs可協助您確保帳戶中的資源保持在組織的存取控制準則內。

您可以使用 AWS Organizations 主控台集中檢視和管理組織中的所有帳戶。使用組織的其中一個好處是您可以收到合併帳單，其中顯示與管理帳戶和成員帳戶相關的所有費用。如需詳細資訊，請參閱合併帳單 (AWS Organizations 文件）。

最佳實務

- 請勿使用現有的 AWS 帳戶 來建立組織。從新帳戶開始，它會成為組織的管理帳戶。特殊權限操作可以在組織的管理帳戶中執行，而 SCPs和 RCPs 不適用於管理帳戶。這就是為什麼您應該將管理帳戶中包含的雲端資源和資料限制為只能在管理帳戶中管理的資源和資料。
- 限制只有需要佈建新 AWS 帳戶 和管理組織的個人才能存取 管理帳戶。
- 使用 SCP 來定義根、組織單位和成員帳戶的最大許可。SCP 無法直接套用至管理帳戶。
- 使用 RCPs定義成員帳戶中資源的最大許可。RCPs無法直接套用至管理帳戶。
- 遵守 (AWS Organizations 文件） 的最佳實務 AWS Organizations。

建立登陸區域

登陸區域是架構良好的多帳戶 AWS 環境，是您部署工作負載和應用程式的起點。它會提供一種基準，以便開始使用多帳戶架構、身分管理和存取管理、控管、資料安全、網路設計和日誌。AWS Control Tower 是一項服務，它透過提供自動化防護機制來簡化多帳戶環境的維護和控管。一般而言，您會佈建單一 AWS Control Tower 登陸區域，透過在 AWS 服務 帳戶中協調其他 來管理您在 all AWS 區域. AWS Control Tower works 的環境。如需詳細資訊，請參閱設定登陸區域（文件）時會發生的情況。AWS Control Tower

當您使用 設定登陸區域時 AWS Control Tower，您可以識別三個共用帳戶：管理帳戶、日誌封存帳戶和稽核帳戶。如需詳細資訊，請參閱什麼是共用帳戶 (AWS Control Tower 文件）。對於管理帳戶，必須使用未託管任何工作負載的現有帳戶來設定登陸區域。對於日誌封存和稽核帳戶，您可以選擇重複使用現有帳戶 AWS 帳戶，也可以為您 AWS Control Tower 建立這些帳戶。

如需如何設定 AWS Control Tower 登陸區域的指示，請參閱入門 (AWS Control Tower 文件）。

最佳實務

- 遵守多帳戶策略的設計原則 (AWS 白皮書） 中的最佳實務。
- 遵守管理員的 AWS Control Tower 最佳實務 (AWS Control Tower 文件）。
- 在 AWS 區域 託管大部分工作負載的 中建立登陸區域。

> **Important**
>
> 如果您在部署登陸區域之後決定變更此區域，您需要 的協助 AWS 支援，而且必須停用登陸區域。不建議採用這種做法。

- 判斷 AWS Control Tower 要管理的區域時，請僅選取您預期立即部署工作負載的區域。可以變更這些區域或稍後新增更多區域。如果 AWS Control Tower 管理某個區域，則會將其偵測護欄部署到該區域中，做為 AWS Config 規則。
- 決定 AWS Control Tower 要管理哪些區域之後， 會拒絕存取所有未受管區域。這有助於確保您的工作負載和開發人員只能使用已批准的 AWS 區域。這在組織中將實作為服務控制政策 (SCP)。如需詳細資訊，請參閱設定 AWS 區域 拒絕控制 (AWS Control Tower 文件）。
- 在 中設定登陸區域時 AWS Control Tower，我們建議您重新命名下列 OUs和帳戶：
  - 建議您將 Security OU 重新命名為 Security_Prod，表明此 OU 將用於生產安全相關 AWS 帳戶。
  - 我們建議您允許 AWS Control Tower 建立額外的 OU，然後從沙盒重新命名為工作負載。在下一節中，您可以在工作負載 OU 中建立其他 OU，用來組織您的 AWS 帳戶。
  - 建議您將 Log Archive AWS 帳戶 的集中式記錄重新命名為 log-archive-prod。
  - 建議將稽核帳戶從稽核重新命名為為 security-tooling-prod。
- 為了協助防止詐騙， AWS 需要 AWS 帳戶 具有使用歷史記錄，才能將其新增至 AWS Control Tower 登陸區域。如果您使用的是 AWS 帳戶 不含任何用量歷史記錄的新 ，您可以在新帳戶中啟動不在 AWS 免費方案中的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體。讓執行個體執行幾分鐘，然後將其終止。

新增組織單位

建立適當的組織結構對於設定多帳戶環境至關重要。因為您使用服務控制政策 (SCP) 來定義 OU 及其中帳戶的最大許可，因此從管理、許可和財務報告的角度來看，您的組織結構必須是合乎邏輯的。如需組織結構的詳細資訊，包括組織單位 OUs)，請參閱術語和概念 (AWS Organizations 文件）。

在本節中，可以透過建立巢狀 OU 來自訂登陸區域，以協助您對環境進行分割和結構化，例如生產和非生產。這些建議的最佳實務設計用來將登陸區域劃分為生產資源和非生產資源，並將基礎設施與工作負載分開。

如需如何建立 OUs的詳細資訊，請參閱管理組織單位 (AWS Organizations 文件）。

最佳實務

- 在您在 建立登陸區域 中建立的工作負載中，建立下列巢狀 OU：
  - Prod – 針對儲存和存取生產資料的 AWS 帳戶 使用此 OU，包括客戶資料。
  - NonProd – 針對儲存非生產資料的 AWS 帳戶 使用此 OU，例如開發、預備或測試環境

在組織根下，建立一個 Infrastructure_Prod OU。使用此 OU 來託管集中式網路帳戶。

新增初始使用者

有兩種方法可以授予人員存取 AWS 帳戶：

- IAM 身分，例如使用者、群組和角色
- 聯合身分，例如使用 AWS IAM Identity Center

在小型公司和單一帳戶環境中，在新人員加入公司時，管理員通常會建立 IAM 使用者。與 IAM 使用者相關聯的存取金鑰和秘密金鑰憑證稱為長期憑證，因為其不會過期。不過，這並不是建議的安全最佳實務，因為如果攻擊者威脅到這些憑證，您必須為使用者產生一組新的憑證。另一種存取方法是 AWS 帳戶 透過 IAM 角色。您也可以使用 AWS Security Token Service (AWS STS) 暫時請求短期憑證，它會在可設定的時間後過期。

您可以透過 IAM Identity Center AWS 帳戶 管理人員存取 。您可以為每位員工或承包商建立個別使用者帳戶，他們可以管理自己的密碼和多重要素驗證 (MFA) 解決方案，也可以將他們分組以管理存取權。設定 MFA 時，可以使用軟體權杖，例如驗證器應用程式，也可以使用硬體權杖，例如 YubiKey 裝置。

IAM Identity Center 也支援來自外部身分提供者 (IdP) 的聯合，例如 Okta、JumpCloud 和 Ping Identity。如需詳細資訊，請參閱支援的身分提供者 (IAM Identity Center 文件)。透過與外部 IdP 聯合，您可以跨應用程式管理使用者身分驗證，然後使用 IAM Identity Center 授權存取特定 AWS 帳戶。

最佳實務

- 遵循安全最佳實務 (IAM 文件) 以設定使用者存取權。
- 依群組而非個別使用者管理帳戶存取權。在 IAM Identity Center 中，建立代表每個業務職能的新群組。例如，可以建立工程、財務、銷售和產品管理群組。
- 通常，透過將需要存取所有 AWS 帳戶 的人 (通常為唯讀存取) 和需要存取單個 AWS 帳戶的人分開來定義群組。建議您針對群組使用以下命名慣例，以便輕鬆識別與群組相關聯的 AWS 帳戶 和 許可。

  `<prefix>-<account name>-<permission set>`
- 例如，對於群組 `AWS-A-dev-nonprod-DeveloperAccess`，`AWS-A` 是一個字首，它表示可存取單個帳戶，`dev-nonprod` 是帳戶名稱，`DeveloperAccess` 是指派給群組的許可集。對於群組 `AWS-O-BillingAccess`，`AWS-O` 字首表示對整個組織的存取，`BillingAccess` 表示群組的許可集。在此範例中，由於群組擁有對整個組織的存取權，所以群組名稱中不會顯示帳戶名稱。
- 如果您將 IAM Identity Center 與外部 SAML 型 IdP 搭配使用，並且想要使用 MFA，則可以使用屬性型存取控制 (ABAC) 將驗證方法從 IdP 傳遞至 IAM Identity Center。透過 SAML 宣告來傳送屬性。如需詳細資訊，請參閱啟用和設定存取控制屬性 (IAM Identity Center 文件)。

  諸如 Microsoft Azure Active Directory 和 Okta 等許多 IdP 可使用 SAML 宣告中的 Authentication Method Reference (`amr`) 聲明將使用者的 MFA 狀態傳遞至 IAM Identity Center。用來宣告 MFA 狀態及其格式的聲明因 IdP 而異。如需詳細資訊，請參閱您的 IdP 文件。

  在 IAM Identity Center 中，您可以建立許可集政策，以決定誰可以存取您的 AWS 資源。啟用 ABAC 並指定屬性時，IAM Identity Center 會將已驗證使用者的屬性值傳遞至 IAM，以便用於政策評估。如需詳細資訊，請參閱建立 ABAC 的許可政策 (IAM Identity Center 文件)。如下列範例所示，使用 `aws:PrincipalTag` 條件金鑰為 MFA 建立存取控制規則。

```
"Condition": {
  "StringLike": { "aws:PrincipalTag/amr": "mfa" }
}
```

管理成員帳戶

在本節中，邀請先前存在的帳戶加入組織，並開始在組織內建立新帳戶。此過程的一個重要部分是定義條件，用於確定是否需要佈建新帳戶。

本節包含下列任務：

- 邀請先前存在的帳戶
- 在 中自訂 VPC 設定 AWS Control Tower
- 定義範圍標準

邀請先前存在的帳戶

在其中 AWS Organizations，您可以邀請貴公司的預先存在帳戶加入您的新組織。只有組織中的管理帳戶可以邀請其他帳戶加入。當受邀帳戶的管理員接受邀請時，帳戶可立即加入組織，並且組織的管理帳戶將負責新成員帳戶累積的所有費用。如需詳細資訊，請參閱邀請 AWS 帳戶 加入組織和接受或拒絕來自組織的邀請 (AWS Organizations 文件)。

> **Note**
>
> 只有當該帳戶目前不在其他組織時，您才可以邀請該帳戶加入組織。如果帳戶是現有組織的成員，必須將其從組織中移除。如果帳戶是錯誤建立的其他組織的管理帳戶，則必須刪除該組織。

> **Important**
>
> 如果您需要從預先存在的帳戶存取任何歷史成本或使用資訊，您可以使用 AWS Cost and Usage Report 將該資訊匯出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體。在接受邀請加入組織之前執行此操作。當帳戶加入組織時，您將無法存取該帳戶的此歷史資料。如需詳細資訊，請參閱設定成本和用量報告的 Amazon S3 儲存貯體 (AWS Cost and Usage Report 文件)。

最佳實務

- 建議您將先前存在的帳戶 (它可能包含生產工作負載) 新增至您在 新增組織單位 中建立的工作負載 > 生產組織單位。
- 依預設，組織的管理帳戶沒有對受邀加入組織之成員帳戶的管理存取權。如果您希望管理帳戶擁有管理控制權，則必須在成員帳戶中建立 OrganizationAccountAccessRole IAM 角色，並對管理帳戶授予擔任該角色的許可。如需詳細資訊，請參閱在受邀成員帳戶中建立 OrganizationAccountAccessRole (AWS Organizations 文件）。
- 對於您邀請加入組織的既有帳戶，請檢閱成員帳戶的最佳實務 (AWS Organizations 文件），並確認帳戶遵守這些建議。

在 中自訂 VPC 設定 AWS Control Tower

建議您 AWS 帳戶 透過 中的 Account Factory 佈建新的 AWS Control Tower。透過使用 Account Factory，您可以在帳戶建立 AWS 帳戶 後立即使用與 Amazon EventBridge 的 AWS Control Tower 整合，在新的 中佈建資源。

當您設定新的 時 AWS 帳戶，會自動佈建預設虛擬私有雲端 (VPC)。但是，當您透過 Account Factory 設定新帳戶時， AWS Control Tower 會自動佈建額外的 VPC。如需詳細資訊，請參閱 AWS Control Tower 和 VPCs(AWS Control Tower 文件）。這意味著，預設情況下， AWS Control Tower 會在每個新帳戶中佈建兩個預設 VPC。

公司通常希望對其帳戶中的 VPC 進行更多控制。許多人偏好使用其他 服務 AWS CloudFormation，例如 Hashicorp Terraform 或 Pulumi，來設定和管理其 VPCs。您應該自訂 Account Factory 設定，以防止建立由 AWS Control Tower佈建的其他 VPC。如需說明，請參閱設定 Amazon VPC 設定 (AWS Control Tower 文件），並套用下列設定：

1. 停用網際網路可存取的子網路選項。
2. 在私有子網路上限中，選擇 0。
3. 在 VPC 建立的區域中，清除所有區域。
4. 在可用區域中，選擇 3。

最佳實務

- 刪除在每個新帳戶中自動佈建的預設 VPC。這可防止使用者在未明確建立專用 VPC 的情況下，在帳戶中啟動公有 EC2 執行個體。如需詳細資訊，請參閱刪除您的預設子網路和預設 VPC (Amazon Virtual Private Cloud 文件)。您也可以設定 AWS Control Tower Account Factory for Terraform (AFT) 以自動刪除新建立帳戶中的預設 VPC。
- 將 AWS 帳戶 稱為 dev-nonprod 的新 佈建至工作負載 > NonProd 組織單位。在開發環境中使用此帳戶。如需說明，請參閱使用 佈建帳戶工廠帳戶 AWS Service Catalog (AWS Control Tower 文件）。

定義範圍標準

您需要選取貴公司在決定是否佈建新 時將使用的條件 AWS 帳戶。您可以決定為每個業務單位佈建帳戶，或者決定根據環境來佈建帳戶，例如生產、測試或 QA。每家公司都有自己的需求，要求其 AWS 帳戶 大小應該多大。通常，在決定如何調整帳戶大小時，會評估以下三個因素：

- 平衡服務配額 – 服務配額是 AWS 服務 中每個資源、動作和項目數量的最大值 AWS 帳戶。如果許多工作負載共用相同帳戶，而一個工作負載取用了大部分或全部服務配額，則可能會對同一帳戶中的另一個工作負載產生負面影響。如果這樣，則您可能需要將這些工作負載分隔到不同的帳戶中。如需詳細資訊，請參閱 AWS 服務 配額 (AWS 一般參考)。
- 成本報告 – 將工作負載隔離到單獨的帳戶中，可讓您在成本和用量報告中查看帳戶層級的成本。當您將相同帳戶用於多個工作負載時，可以使用標籤來協助您管理和識別資源。如需標記的詳細資訊，請參閱標記 AWS 資源 (AWS 一般參考)。
- 控制存取 – 當工作負載共用帳戶時，需要考慮如何設定 IAM 政策以限制對帳戶資源的存取，以便使用者無法存取不需要的工作負載。作為替代方案，您可以在 IAM Identity Center 中使用多個帳戶和許可集來管理對個別帳戶的存取。

最佳實務

- 遵守AWSAWS Control Tower 登陸區域多帳戶策略的最佳實務 (AWS Control Tower 文件）。
- 建立有效的標記策略，協助您識別和管理 AWS 資源。可使用標籤依照用途、業務單位、環境或其他條件對資源進行分類。如需詳細資訊，請參閱標記的最佳實務 (AWS 一般參考 文件）。
- 不要因過多的工作負載讓帳戶不堪重負。如果工作負載的需求超過服務配額，則可能會造成效能問題。您可以將競爭的工作負載分成不同的工作負載， AWS 帳戶 也可以請求提高服務配額。如需詳細資訊，請參閱請求增加配額 (Service Quotas 文件)。

管理多帳戶架構的許可和存取

本節包含下列主題：

工程文化考量事項

AWS Well-Architected Framework 的其中一個支柱是卓越營運。團隊必須了解運作模式以及他們在實現業務成果方面的作用。當團隊了解自己的責任、可以取得擁有權並知道如何制定決策時，他們就可以專注於實現共同目標。

對於正在快速發展的初期公司，團隊中的每個人都扮演多個角色。這些使用者對整個 AWS 帳戶擁有高度特權存取並不罕見。隨著公司的成長，公司往往希望遵循最低權限原則並僅授予使用者執行其工作所需的許可。為了協助您限制範圍，可以使用 AWS Identity and Access Management Access Analyzer 查看使用者或 IAM 角色實際使用的許可，以便移除任何多餘許可。

決定公司中誰有權建立 IAM 角色非常有挑戰性。這通常是提升權限。提升權限是指使用者可以擴展自己的許可或存取範圍。例如，如果使用者擁有的許可有限，但可以建立新的 IAM 角色，則該使用者可以透過建立並承擔已套用 `AdministratorAccess` 受管政策的新 IAM 角色來提升其權限。

有些公司將 IAM 角色佈建限制給由受信任的個人組成的集中式團隊。此方法的缺點是，此團隊可以快速成為瓶頸，因為幾乎所有人員 AWS 服務 都需要 IAM 角色才能運作。作為替代方案，您可以使用許可界限，將 IAM 存取權僅委派給正在開發、測試、啟動和管理雲端基礎設施的使用者。如需政策範例，請參閱許可界限範例 (GitHub)。

開發營運 (DevOps) 團隊，也稱為平台團隊，通常需要平衡多個內部開發團隊的自助服務能力與應用程式操作穩定性。培養在工作場所具有自主性、掌控力和目標明確的工程文化有助於激勵團隊。工程師希望自主完成自己的工作，而不需要依賴別人為他們做事情。如果 DevOps 團隊可以實作自助式解決方案，這也可以減少其他人依賴他們完成工作的時間。

建立許可集

您可以使用 中的許可集來管理 AWS 帳戶 存取權 AWS IAM Identity Center。許可集是一個範本，可協助您將一個或多個 IAM 政策部署至多個 AWS 帳戶。當您將許可集指派給 AWS 帳戶時，IAM Identity

Center 會建立 IAM 角色，並將您的 IAM 政策附接到該角色。如需詳細資訊，請參閱建立和管理許可集 (IAM Identity Center 文件)。

AWS 建議建立對應到您業務中不同角色的許可集。

例如，可以建立下列許可集：

- 帳單許可集
- 開發人員許可集
- 生產許可集

下列許可集是 AWS CloudFormation 範本的程式碼片段。應該使用此代碼作為起點，並為您的業務進行自訂。如需 CloudFormation 範本的詳細資訊，請參閱了解範本基本知識 (CloudFormation 文件)。

帳單許可集

財務團隊使用 BillingAccessPermissionSet 來檢視 AWS Billing 主控台儀表板和每個帳戶中 AWS Cost Explorer 的 。

```
BillingAccessPermissionSet:
  Type: "AWS::SSO::PermissionSet"
  Properties:
    Description: Access to Billing and Cost Explorer
    InstanceArn: !Sub "arn:${AWS::Partition}:sso:::instance/ssoins-instanceId"
    ManagedPolicies:
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/job-function/Billing"
    Name: BillingAccess
    SessionDuration: PT8H
    RelayStateType: https://console.aws.amazon.com/billing/home
```

開發人員許可集

工程團隊使用 DeveloperAccessPermissionSet 來存取非生產帳戶。

```
DeveloperAccessPermissionSet:
  Type: "AWS::SSO::PermissionSet"
  Properties:
    Description: Access to provision resources through CloudFormation
    InlinePolicy: !Sub |-
      {
        "Version": "2012-10-17",
```

```
        "Statement": [
          {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:${AWS::Partition}:iam::*:role/CloudFormationRole",
            "Condition": {
              "StringEquals": {
                "aws:ResourceAccount": "${!aws:PrincipalAccount}",
                "iam:PassedToService": "cloudformation.${AWS::URLSuffix}"
              }
            }
          },
          {
            "Effect": "Allow",
            "Action": [
              "cloudformation:ContinueUpdateRollback",
              "cloudformation:CreateChangeSet",
              "cloudformation:CreateStack",
              "cloudformation:DeleteStack",
              "cloudformation:RollbackStack",
              "cloudformation:UpdateStack"
            ],
            "Resource": "arn:${AWS::Partition}:cloudformation:*:*:stack/app-*",
            "Condition": {
              "ArnLike": {
                "cloudformation:RoleArn": "arn:${AWS::Partition}:iam::${!
aws:PrincipalAccount}:role/CloudFormationRole"
              },
              "Null": {
                "cloudformation:ImportResourceTypes": true
              }
            }
          },
          {
            "Effect": "Allow",
            "Action": [
              "cloudformation:CancelUpdateStack",
              "cloudformation:DeleteChangeSet",
              "cloudformation:DetectStackDrift",
              "cloudformation:DetectStackResourceDrift",
              "cloudformation:ExecuteChangeSet",
              "cloudformation:TagResource",
              "cloudformation:UntagResource",
              "cloudformation:UpdateTerminationProtection"
```

```
            ],
            "Resource": "arn:${AWS::Partition}:cloudformation:*:*:stack/app-*"
          },
          {
           "Effect": "Allow",
            "Action": [
              "cloudformation:CreateUploadBucket",
              "cloudformation:ValidateTemplate",
              "cloudformation:EstimateTemplateCost"
            ],
            "Resource": "*"
          }
        ]
      }
    InstanceArn: !Sub "arn:${AWS::Partition}:sso:::instance/ssoins-instanceId"
    ManagedPolicies:
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSServiceCatalogEndUserFullAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSProtonDeveloperAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSBillingReadOnlyAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSSupportAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/ReadOnlyAccess"
    Name: DeveloperAccess
    SessionDuration: PT8H
```

生產許可集

工程團隊使用 ProductionPermissionSet 來存取生產帳戶。此許可集具有有限、僅供檢視的存取權。

```
ProductionPermissionSet:
  Type: "AWS::SSO::PermissionSet"
  Properties:
    Description: Access to production accounts
    InlinePolicy: !Sub |-
      {
        "Version": "2012-10-17",
        "Statement": [
          {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:${AWS::Partition}:iam::*:role/CloudFormationRole",
            "Condition": {
              "StringEquals": {
                "aws:ResourceAccount": "${!aws:PrincipalAccount}",
```

```
                "iam:PassedToService": "cloudformation.${AWS::URLSuffix}"
              }
            }
          },
          {
            "Effect": "Allow",
            "Action": "cloudformation:ContinueUpdateRollback",
            "Resource": "arn:${AWS::Partition}:cloudformation:*:*:stack/app-*",
            "Condition": {
              "ArnLike": {
                "cloudformation:RoleArn": "arn:${AWS::Partition}:iam::${!
aws:PrincipalAccount}:role/CloudFormationRole"
              }
            }
          },
          {
            "Effect": "Allow",
            "Action": "cloudformation:CancelUpdateStack",
            "Resource": "arn:${AWS::Partition}:cloudformation:*:*:stack/app-*"
          }
        ]
      }
    InstanceArn: !Sub "arn:${AWS::Partition}:sso:::instance/ssoins-instanceId"
    ManagedPolicies:
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSBillingReadOnlyAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSSupportAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/job-function/ViewOnlyAccess"
    Name: ProductionAccess
    SessionDuration: PT2H
```

建立許可界限

部署許可集之後，您會建立許可界限。此許可界限是一種機制，它將 IAM 存取權僅委派給正在開發、測試、啟動和管理雲端基礎設施的使用者。這些使用者只能執行政策和許可界限允許的動作。

您可以在 AWS CloudFormation 範本中定義許可界限，然後使用 CloudFormation StackSets 將範本部署到多個帳戶。這可協助您透過單一操作在整個組織中建立和維護標準化政策。如需詳細資訊和指示，請參閱使用 AWS CloudFormation StackSets (CloudFormation 文件)。

下列 CloudFormation 範本會佈建 IAM 角色，並建立作為許可界限的 IAM 政策。使用堆疊集，可以將此範本部署到組織中的所有成員帳戶。

```
CloudFormationRole:
  Type: "AWS::IAM::Role"
  Properties:
    AssumeRolePolicyDocument:
      Version: "2012-10-17"
      Statement:
        Effect: Allow
        Principal:
          Service: !Sub "cloudformation.${AWS::URLSuffix}"
        Action: "sts:AssumeRole"
        Condition:
          StringEquals:
            "aws:SourceAccount": !Ref "AWS::AccountId"
    Description: !Sub "DO NOT DELETE - Used by CloudFormation. Created by
 CloudFormation ${AWS::StackId}"
    ManagedPolicyArns:
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AdministratorAccess"
    PermissionsBoundary: !Ref DeveloperBoundary
    RoleName: CloudFormationRole

DeveloperBoundary:
  Type: "AWS::IAM::ManagedPolicy"
  Properties:
    Description: Permission boundary for developers
    ManagedPolicyName: PermissionsBoundary
    PolicyDocument:
      Version: "2012-10-17"
      Statement:
        - Sid: AllowModifyIamRolesWithBoundary
          Effect: Allow
          Action:
            - "iam:AttachRolePolicy"
            - "iam:CreateRole"
            - "iam:DeleteRolePolicy"
            - "iam:DetachRolePolicy"
            - "iam:PutRolePermissionsBoundary"
            - "iam:PutRolePolicy"
          Resource: !Sub "arn:${AWS::Partition}:iam::${AWS::AccountId}:role/app/*"
          Condition:
            ArnEquals:
              "iam:PermissionsBoundary": !Sub "arn:${AWS::Partition}:iam::
${AWS::AccountId}:policy/PermissionsBoundary"
        - Sid: AllowModifyIamRoles
```

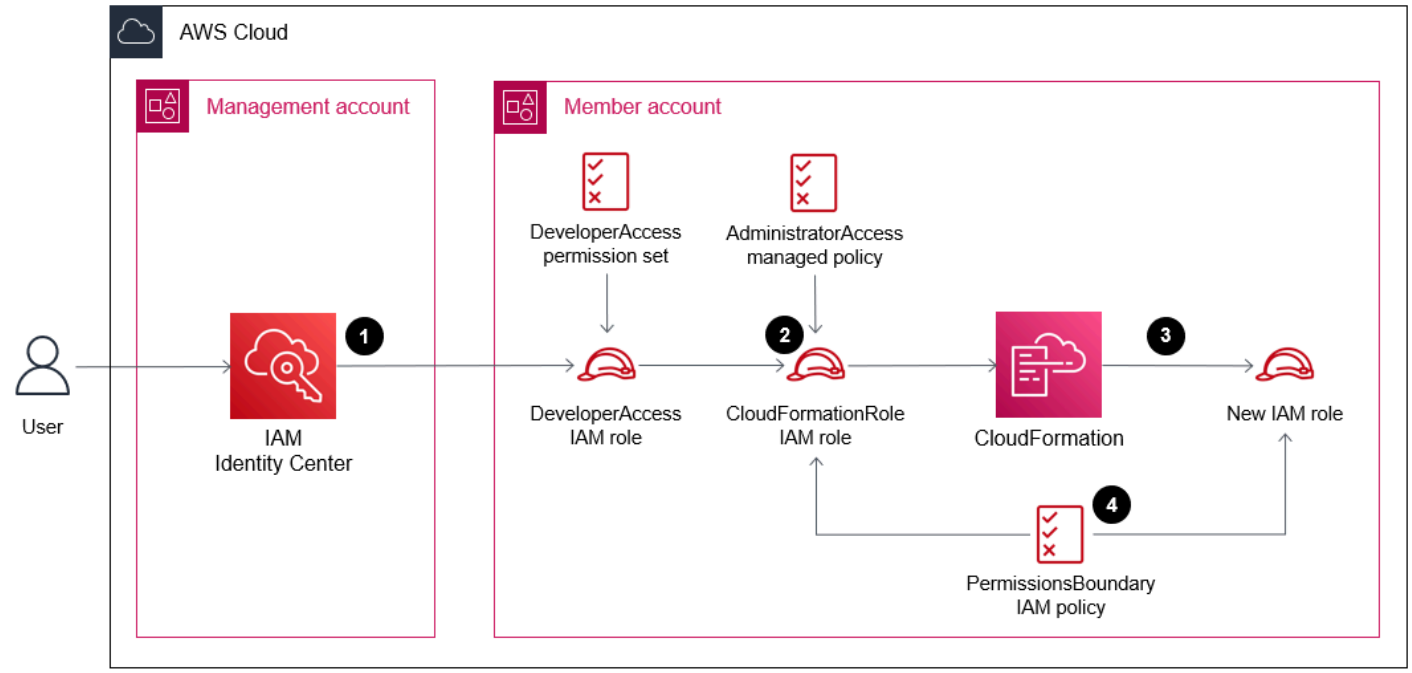
```
        Effect: Allow
        Action:
          - "iam:DeleteRole"
          - "iam:TagRole"
          - "iam:UntagRole"
          - "iam:UpdateAssumeRolePolicy"
          - "iam:UpdateRole"
          - "iam:UpdateRoleDescription"
        Resource: !Sub "arn:${AWS::Partition}:iam::${AWS::AccountId}:role/app/*"
      - Sid: OverlyPermissiveAllowedServices
        Effect: Allow
        Action:
          - "lambda:*"
          - "apigateway:*"
          - "events:*"
          - "s3:*"
          - "logs:*"
        Resource: "*"
```

CloudFormationRole 角色、PermissionsBoundary 政策以及 DeveloperAccess 許可集共同運作以授與下列許可：

- 使用者 AWS 服務可透過 ReadOnlyAccess AWS 受管政策，對大多數使用者進行唯讀存取。
- 使用者可透過 AWSSupportAccess AWS 受管政策存取開放支援案例。
- 使用者可透過 AWSBillingReadOnlyAccess AWS 受管政策，以唯讀方式存取 AWS Billing 主控台儀表板。
- 使用者可以透過 AWSProtonDeveloperAccess AWS 受管政策 AWS Proton，從 佈建新的環境。
- 使用者可以透過 AWSServiceCatalogEndUserFullAccess AWS 受管政策，從 Service Catalog 佈建產品。
- 使用者可以透過內嵌政策來驗證和估算任何 CloudFormation 範本的成本。
- 透過使用 CloudFormationRole IAM 角色，使用者可以建立、更新或刪除任何以 app/ 開始的 CloudFormation 堆疊。
- 使用者可以使用 CloudFormation 來建立、更新或刪除以 app/ 開頭的 IAM 角色 。PermissionsBoundary IAM 政策可防止使用者提升其權限。
- 使用者只能使用 CloudFormation 佈建 AWS Lambda Amazon EventBridge、Amazon CloudWatch、Amazon Simple Storage Service (Amazon S3) 和 Amazon API Gateway 資源。

下圖顯示了授權使用者 (例如開發人員) 如何使用本指南中所描述的許可集、IAM 角色和許可界限，在成員帳戶中建立新的 IAM 角色：

1. 使用者會在 IAM Identity Center 進行驗證，並承擔 DeveloperAccess IAM 角色。
2. 使用者會啟動 `cloudformation:CreateStack` 動作，並承擔 CloudFormationRole IAM 角色。
3. 使用者會啟動 `iam:CreateRole` 動作並使用 CloudFormation 建立新的 IAM 角色。
4. PermissionsBoundary IAM 政策會套用至新的 IAM 角色。



CloudFormationRole 角色已附接 AdministratorAccess 受管政策，但由於 PermissionsBoundary IAM 政策，CloudFormationRole 角色的有效許可等同於 PermissionsBoundary 政策。PermissionsBoundary 政策在允許 `iam:CreateRole` 動作時會參照本身，這可確保只有在套用許可界限時才能建立角色。

管理個人許可

透過使用許可集、許可界限和 CloudFormationRole IAM 角色，您可以限制需要直接指派給個別主體的許可數量。這有助於您在公司成長時管理存取權，並協助您套用授與最低權限的安全最佳實務。

您也可以使用服務連結角色，它會向 AWS 服務授予許可，以代表您佈建資源。您可以向服務授予許可，而不是將許可授予給 IAM 主體 (使用者、使用者群組或角色)。例如，AWS Proton 和 AWS

Service Catalog 的服務連結角色可讓您佈建自己的範本、資源和環境，而無需將許可指派給 IAM 主體。如需詳細資訊，請參閱可搭配 IAM 運作的AWS 服務和使用服務連結角色 (IAM 文件)。

另一個最佳實務是限制個人對 AWS Management Console的存取量。透過限制主控台的存取權，您可以要求個人使用基礎設施即程式碼 (IaC) 技術來佈建資源，例如 AWS CloudFormation、HashiCorp Terraform 或 Pulumi。透過 IaC 來管理基礎設施可以追蹤一段時間內資源的變更，並引入核准變更的機制，例如 GitHub 提取請求。

多帳戶架構的網路連線能力

與 VPC 連線

許多公司在 Amazon Virtual Private Cloud (Amazon VPC) 中使用 VPC 對等互連，以連接開發和生產 VPC。使用 VPC 對等互連，您可以使用私有 IP 地址在兩個 VPC 之間路由流量。連線VPCs 可以位於不同的 AWS 帳戶 和不同的 AWS 區域。如需詳細資訊，請參閱 VPC 對等互連是什麼 (Amazon VPC 文件)。隨著公司的成長和 VPC 數量的增加，維護所有 VPC 之間的對等互連可能會成為維護負擔。您也可能受到每個 VPC 的 VPC 對等互連數目上限的限制。如需詳細資訊，請參閱 VPC 對等互連配額 (Amazon VPC 文件)。

如果您有多個開發、測試和預備環境來託管多個非生產資料 AWS 帳戶，建議您在所有這些 VPCs之間提供網路連線，但不允許存取生產環境。您可以使用 AWS Transit Gateway 在多個帳戶間連接多個 VPC。您可以分隔路由表，以防止開發 VPC 透過傳輸閘道 (充當集中式路由器) 與生產 VPC 通訊。如需詳細資訊，請參閱集中式路由器 (Transit Gateway 文件)。

Transit Gateway 還支援與其他傳輸閘道的對等互連，包括其他 AWS 帳戶 或 AWS 區域中的閘道。由於 Transit Gateway 是一項全受管、高可用性服務，因此您只需要為每個區域佈建一個傳輸閘道。

如需詳細資訊和詳細的網路架構，請參閱建置可擴展且安全的多 VPC AWS 網路基礎設施 (AWS 白皮書）。

連接應用程式

如果您需要在相同環境 （ 例如生產 ） AWS 帳戶 中不同 的應用程式之間建立通訊，您可以使用下列其中一個選項：

- 如果您想要開放對多個 IP 地址和連接埠的廣泛存取，VPC 對等互連或者 AWS Transit Gateway 可在網路層級提供連線。
- AWS PrivateLink 在 VPC 的私有子網路中建立端點，並在 Amazon Route 53 Resolver 中將這些端點註冊為 DNS 項目。透過使用 DNS，應用程式可以解析端點並連線到已註冊的服務，而不需要 VPC 中的 NAT 閘道或網際網路閘道。
- Amazon VPC Lattice 會在多個帳戶和 VPC 中關聯服務 (例如應用程式)，並將其收集到服務網路中。與服務網路相關聯之 VPC 中的用戶端可以將請求傳送到與服務網路相關聯的所有其他服務，無論其是否位於同一帳戶中。VPC Lattice 與 AWS Resource Access Manager (AWS RAM) 整合，以便您可以與其他帳戶或透過 共用資源 AWS Organizations。您只能將 VPC 與一個服務網路相關聯。此解決方案不需要使用 VPC 對等互連或 AWS Transit Gateway 進行跨帳戶通訊。

網路連線的最佳實務

- 建立 AWS 帳戶 您用於集中式聯網的 。命名此帳戶網路生產者，並將其用於 AWS Transit Gateway 和 Amazon VPC IP Address Manager (IPAM)。將此帳戶新增至 Infrastructure_Prod 組織單位。
- 使用 AWS Resource Access Manager (AWS RAM) 與組織的其他成員共用傳輸閘道、VPC Lattice 服務網路和 IPAM 集區。這可讓 AWS 帳戶 組織內的任何 與這些服務互動。
- 透過使用 IPAM 集區集中管理 IPv4 和 IPv6 地址配置，可以允許最終使用者透過使用 AWS Service Catalog 自行佈建 VPC。這可協助您適當調整 VPC 的大小，並防止 IP 地址空間重疊。
- 針對連接到網際網路的流量使用集中式輸出方法，並針對從網際網路進入環境的流量使用分散式輸入方法。如需詳細資訊，請參閱 集中式輸出 和 分散式輸入。

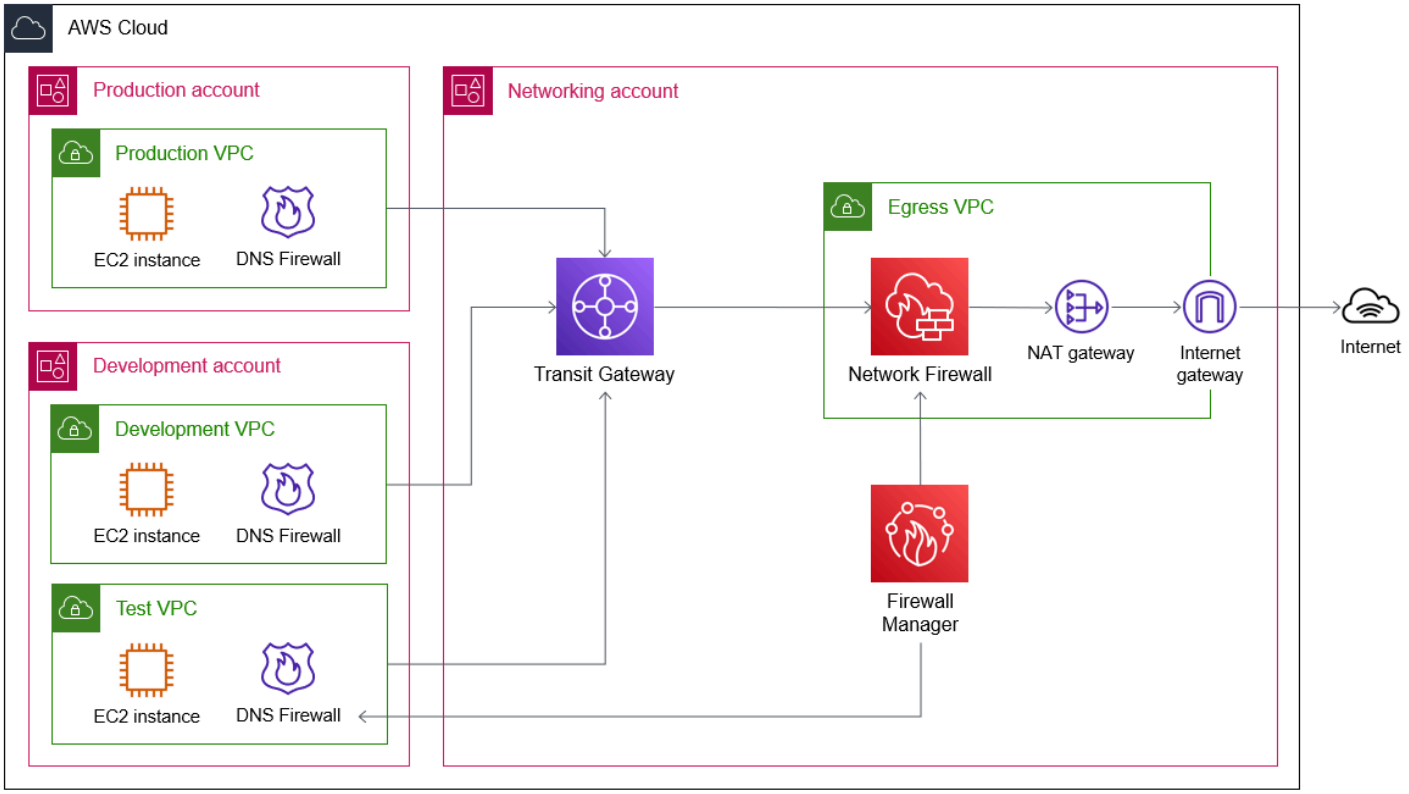
集中式輸出

集中式輸出的原則是針對傳輸到網際網路的所有網路流量使用單一的通用檢查點。在此檢查點，只允許流量傳輸到指定的域，或僅通過指定連接埠或通訊協定。集中式輸出也可協助您降低成本，不需要在每個 VPC 中部署 NAT 閘道以連線至網際網路。從安全角度來看，這是有益的，因為它限制了暴露於外部可存取的惡意資源，例如惡意軟體命令和控制 (C&C) 基礎設施。如需集中輸出的詳細資訊和架構選項，請參閱集中輸出至網際網路 (AWS 白皮書）。

您可以使用 AWS Network Firewall，它是一個具有狀態、受管的網路防火牆和入侵偵測與防護服務，作為輸出流量的中央檢查點。您可以在專用 VPC 中為輸出流量設定此防火牆。Network Firewall 支援有狀態規則，可用於限制特定域的網際網路存取。如需詳細資訊，請參閱域篩選 (Network Firewall 文件)。

您也可以使用 Amazon Route 53 Resolver DNS 防火牆以限制流量輸出至特定域名稱，主要是為了防止未經授權的資料外洩。在 DNS 防火牆規則中，可以套用域清單 (Route 53 文件)，允許或拒絕存取指定域。您可以使用受 AWS 管網域清單，其中包含與惡意活動或其他潛在威脅相關聯的網域名稱，也可以建立自訂網域清單。可以建立 DNS 防火牆規則群組，然後將其套用至 VPC。傳出 DNS 請求會透過 VPC 中的解析器進行路由以解析域名，而 DNS 防火牆會根據套用至 VPC 的規則群組篩選請求。傳送至解析器的遞迴 DNS 請求不會通過傳輸閘道和網路防火牆路徑。Route 53 Resolver 和 DNS Firewall 應被視為 VPC 外的單獨輸出路徑。

下圖顯示集中式輸出的範例架構。在網路通訊開始之前，DNS 請求會傳送至 Route 53 Resolver，DNS 防火牆會允許或拒絕用於通訊的 IP 地址解析。傳送至網際網路的流量會路由至集中式網路帳戶中的傳輸閘道。傳輸閘道會將流量轉送至 Network Firewall 以進行檢查。如果防火牆政策允許輸出流量，則流量會透過 NAT 閘道、網際網路閘道和網際網路進行路由。您可以使用 AWS Firewall Manager 跨多帳戶基礎設施集中管理 DNS 防火牆規則群組和網路防火牆政策。



保護輸出流量的最佳實務

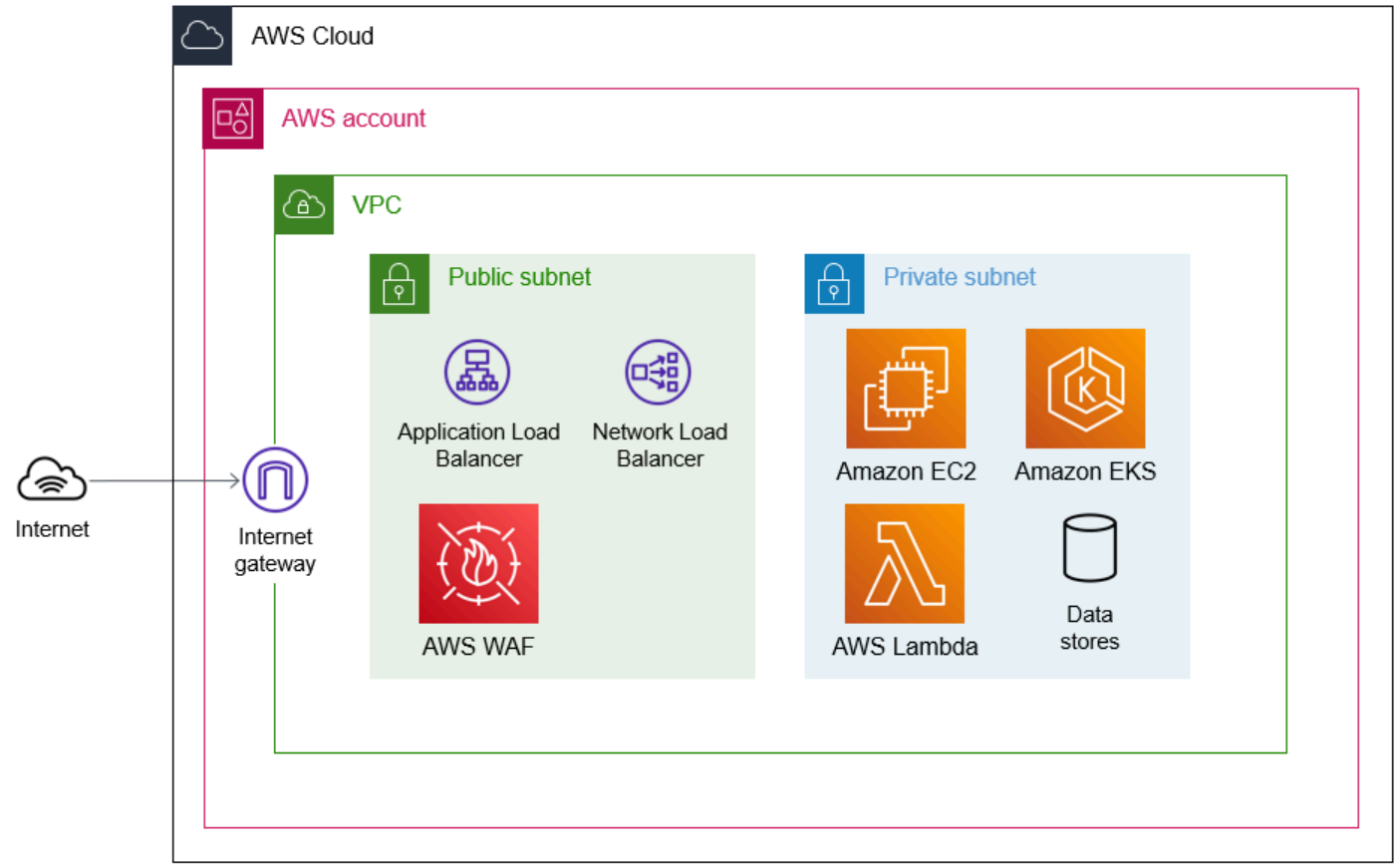
- 在僅登入模式中開始 (Route 53 文件)。驗證合法流量不受影響後，請變更為封鎖模式。
- 使用AWS Firewall Manager 網路存取控制清單的政策或使用 來封鎖流向網際網路的 DNS 流量 AWS Network Firewall。所有 DNS 查詢都應透過 Route 53 Resolver 路由，您可以在其中使用 Amazon GuardDuty （如果啟用）監控它們，並使用 Route 53 Resolver DNS Firewall （如果啟用）篩選它們。如需詳細資訊，請參閱解析 VPC 與網路之間的 DNS 查詢 (Route 53 文件)。
- 使用 DNS Firewall 和 Network Firewall 中的 AWS 受管域清單 (Route 53 文件)。
- 請考慮封鎖高風險、未使用的頂層域，例如 .info、.top、.xyz 或一些國家/地區代碼域。
- 請考慮封鎖高風險且未使用的連接埠，例如連接埠 1389、4444、3333、445、135、139 或 53。
- 一開始，您可以使用包含 AWS 受管規則的拒絕清單。然後，您可以逐步實作允許清單模型。例如，不是在允許清單中只包含完整網域名稱的嚴格清單，而是使用一些萬用字元，例如 *.example.com。您甚至只能允許您預期的頂層網域，並封鎖所有其他網域。然後，隨著時間的推移，也要縮小範圍。
- 使用 Route 53 Profiles (Route 53 文件）將 DNS 相關的 Route 53 組態套用至許多 VPCs和不同的 AWS 帳戶。
- 定義處理這些最佳實務例外狀況的程序。

分散式輸入

分散式輸入的原則是在個人帳戶層級定義來自網際網路的流量如何到達該帳戶中的工作負載。在多帳戶架構中，分散式輸入的優點之一是每個帳戶都可以針對其工作負載使用最合適的輸入服務或資源，例如 Application Load Balancer、Amazon API Gateway 或 Network Load Balancer。

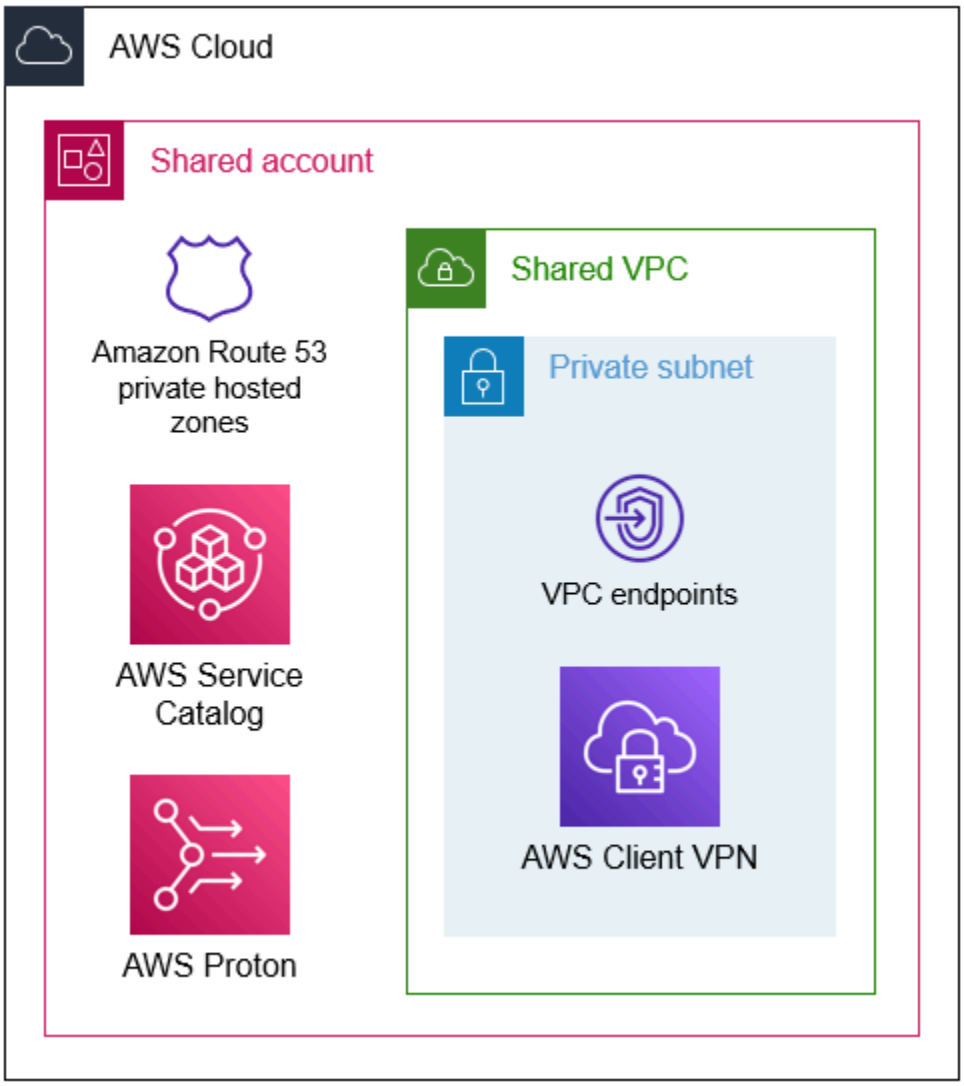
雖然分散式輸入意味著您必須單獨管理每個帳戶，但您可以透過 AWS Firewall Manager 集中管理和維護組態。Firewall Manager 支援保護，例如 AWS WAF 和 Amazon VPC 安全群組。您可以 AWS WAF 與 Application Load Balancer、Amazon CloudFront、API Gateway 或 建立關聯 AWS AppSync。如果您使用的是輸出 VPC 和傳輸閘道 (如 集中式輸出 中所述)，則每個分支 VPC 包含公有和私有子網路。不過，不需要部署 NAT 閘道，因為流量會經過網路帳戶中的輸出 VPC 路由。

下圖顯示具有單一 VPC AWS 帳戶 的個人範例，其中包含可存取網際網路的工作負載。來自網際網路的流量透過網際網路閘道存取 VPC，並達到公有子網路中託管的負載平衡和安全服務。(公有子網路包含目的地為網際網路閘道的預設路由。) 將負載平衡器部署到公有子網路，並連接 AWS WAF 存取控制清單 (ACLs)，以協助防範惡意流量，例如跨網站指令碼。將託管應用程式的工作負載部署到私有子網路中，這些子網路不能直接存取網際網路。



如果您的組織中有很多 VPC，您可能想透過在專用和共用的 AWS 帳戶中建立介面 VPC 端點或私有託管區域，來共用常見的 AWS 服務 。如需詳細資訊，請參閱AWS 服務 使用介面 VPC 端點 (AWS PrivateLink 文件） 存取 和使用私有託管區域 (Route 53 文件）。

下圖顯示 的範例 AWS 帳戶 ，該 託管可在組織中共用的資源。透過在專用 VPC 中建立 VPC 端點，可以在多個帳戶之間共用 VPC 端點。建立 VPC 端點時，您可以選擇讓 AWS 管理端點的 DNS 項目。若要共用端點，請清除此選項，然後在單獨的 Route 53 私有託管區域 (PHZ) 中建立 DNS 項目。然後，可以將 PHZ 與組織中的所有 VPC 產生關聯，以便對 VPC 端點進行集中的 DNS 解析。還需要確保傳輸閘道路由表包含共用 VPC 到其他 VPC 的路由。如需詳細資訊，請參閱介面 VPC 端點的集中存取 (AWS 白皮書）。



共用 AWS 帳戶 也是託管 AWS Service Catalog 產品組合的好地方。產品組合是您要提供部署的一組 IT 服務 AWS，而產品組合包含這些服務的組態資訊。您可以在共用帳戶中建立產品組合，將其分享給

組織，然後每個成員帳戶將產品組合匯入自己的區域 Service Catalog 執行個體。如需詳細資訊，請參閱與 AWS Organizations共用 (Service Catalog 文件)。

同樣地，使用 AWS Proton，您可以使用共用帳戶集中管理您的環境和服務範本，然後設定與組織成員帳戶的帳戶連線。如需詳細資訊，請參閱環境帳戶連線 (AWS Proton 文件）。

多帳戶架構的安全事件回應

當您轉換到多個 時 AWS 帳戶，請務必保持組織內部可能發生的安全事件的可見性。在 身分管理與存取控制 中，您使用 AWS Control Tower 來設定登陸區域。在該設定程序期間， 會 AWS 帳戶 為安全性 AWS Control Tower 指定 。應該將安全服務的管理委派給 security-tooling-prod 帳戶並使用此帳戶集中管理這些服務。

本指南會檢閱下列項目的使用 AWS 服務 ，以協助保護您的 AWS 帳戶 和組織：

- Amazon GuardDuty
- Amazon Macie
- AWS Security Hub

Amazon GuardDuty

Amazon GuardDuty 是一種持續的安全監控服務，可分析資料來源，例如 AWS CloudTrail 事件日誌。如需受支援資料來源的完整清單，請參閱 Amazon GuardDuty 如何使用其資料來源 (GuardDuty 文件)。它使用威脅智慧饋送 (例如惡意 IP 地址和域清單以及機器學習) 以在您的 AWS 環境中識別意外和可能未經授權且惡意的活動。

當您搭配 GuardDuty 使用 時 AWS Organizations，組織中的管理帳戶可以將組織中的任何帳戶指定為 GuardDuty 委派管理員。委派的管理員會成為該區域的 GuardDuty 管理員帳戶。GuardDuty 會在該 中自動啟用：AWS 區域，委派的管理員帳戶具有許可，可針對該區域內組織中的所有帳戶啟用和管理 GuardDuty。如需詳細資訊，請參閱使用 AWS Organizations管理 GuardDuty 帳戶 (GuardDuty 文件)。

GuardDuty 是一項區域性服務。這表示您必須在要監控的每個區域中啟用 GuardDuty。

最佳實務

- 在所有支援的 中啟用 GuardDuty AWS 區域。GuardDuty 可產生有關未授權或不尋常的活動問題清單，甚至在未使用中的區域中也一樣。GuardDuty 的定價基於分析的事件數。即使在您沒有操作工作負載的區域，啟用 GuardDuty 也是一種有效且具成本效益的偵測工具，可提醒您潛在惡意活動。如需有關可提供 GuardDuty 的區域詳細資訊，請參閱 Amazon GuardDuty 服務端點 (AWS 一般參考)。
- 在每個區域內，為您的組織委派 security-tooling-prod 帳戶以管理 GuardDuty。如需詳細資訊，請參閱指定 GuardDuty 委派的管理員 (GuardDuty 文件)。

- 將 GuardDuty 設定為在新增至組織 AWS 帳戶 時自動註冊新的 。如需詳細資訊，請參閱使用 AWS Organizations管理帳戶中的步驟 3 - 以成員身分自動新增組織帳戶 (GuardDuty 文件)。

Amazon Macie

Amazon Macie 是一種全受管資料安全和資料隱私權服務，該服務使用機器學習和模式比對來協助您探索、監控和保護 Amazon Simple Storage Service (Amazon S3) 中的敏感資料。可以將資料從 Amazon Relational Database Service (Amazon RDS) 和 Amazon DynamoDB 匯出到 S3 儲存貯體，然後使用 Macie 掃描資料。

當您搭配 Macie 使用 時 AWS Organizations，組織中的管理帳戶可以將組織中的任何帳戶指定為 Macie 管理員帳戶。管理員帳戶可以為組織中的成員帳戶啟用和管理 Macie、存取 Amazon S3 庫存清單資料以及執行帳戶的敏感資料探索作業。如需詳細資訊，請參閱使用 AWS Organizations管理帳戶 (Macie 文件)。

Macie 是一項區域性服務。這表示您必須在要監控的每個區域中啟用 Macie，而且 Macie 管理員帳戶只能在同一區域內管理成員帳戶。

最佳實務

- 遵守搭配使用 Macie 與 AWS Organizations的考量事項和建議 (Macie 文件)。
- 在每個區域內，為您的組織委派 security-tooling-prod 帳戶以管理 Macie。若要集中管理多個 Macie 帳戶 AWS 區域，管理帳戶必須登入組織目前使用或將使用 Macie 的每個區域，然後在每個區域中指定 Macie 管理員帳戶。然後，Macie 管理員帳戶就可以在這些區域中設定組織。如需詳細資訊，請參閱整合並設定組織 (Macie 文件)。
- Macie 為敏感資料探索作業提供每月免費方案。如果您在 Amazon S3 中儲存了敏感資料，請使用 Macie 來分析 S3 儲存貯體，作為每月免費方案的一部分。如果超出免費方案範圍，就會開始向您的帳戶收取敏感資料探索費用。

AWS Security Hub

AWS Security Hub 可讓您全面檢視 的安全狀態 AWS。可使用它來檢查環境是否符合安全業界標準和最佳實務。Security Hub 會從您所有 AWS 帳戶服務 （ 包括 GuardDuty 和 Macie) 和支援的第三方合作夥伴產品收集安全資料。Security Hub 可協助您分析安全趨勢，並識別最高優先級的安全問題。Security Hub 提供各種安全標準，讓您可以在每個 AWS 帳戶中執行合規檢查。

當您搭配 Security Hub 使用 時 AWS Organizations，組織中的管理帳戶可以將組織中的任何帳戶指定為 Security Hub 管理員帳戶。然後，Security Hub 管理員帳戶就可以啟用和管理組織中的其他成員帳戶。如需詳細資訊，請參閱使用 AWS Organizations 管理帳戶 (Security Hub 文件）。

Security Hub 是一項區域性服務。這表示您必須在要分析的每個區域中啟用 Security Hub AWS Organizations，而且您必須為每個區域定義委派管理員。

最佳實務

- 遵循先決條件和建議 (Security Hub 文件)。
- 在每個區域內，為您的組織委派 security-tooling-prod 帳戶以管理 Security Hub。如需詳細資訊，請參閱指定 Security Hub 管理員帳戶 (Security Hub 文件)。
- 將 Security Hub 設定為在新增至組織 AWS 帳戶 時自動註冊新的 。
- 啟用 AWS 基礎安全最佳實務標準 (Security Hub 文件)，偵測資源何時偏離安全最佳實務。
- 啟用跨區域彙總 (Security Hub 文件)，從單一區域檢視和管理所有 Security Hub 調查結果。

設定多帳戶架構的備份

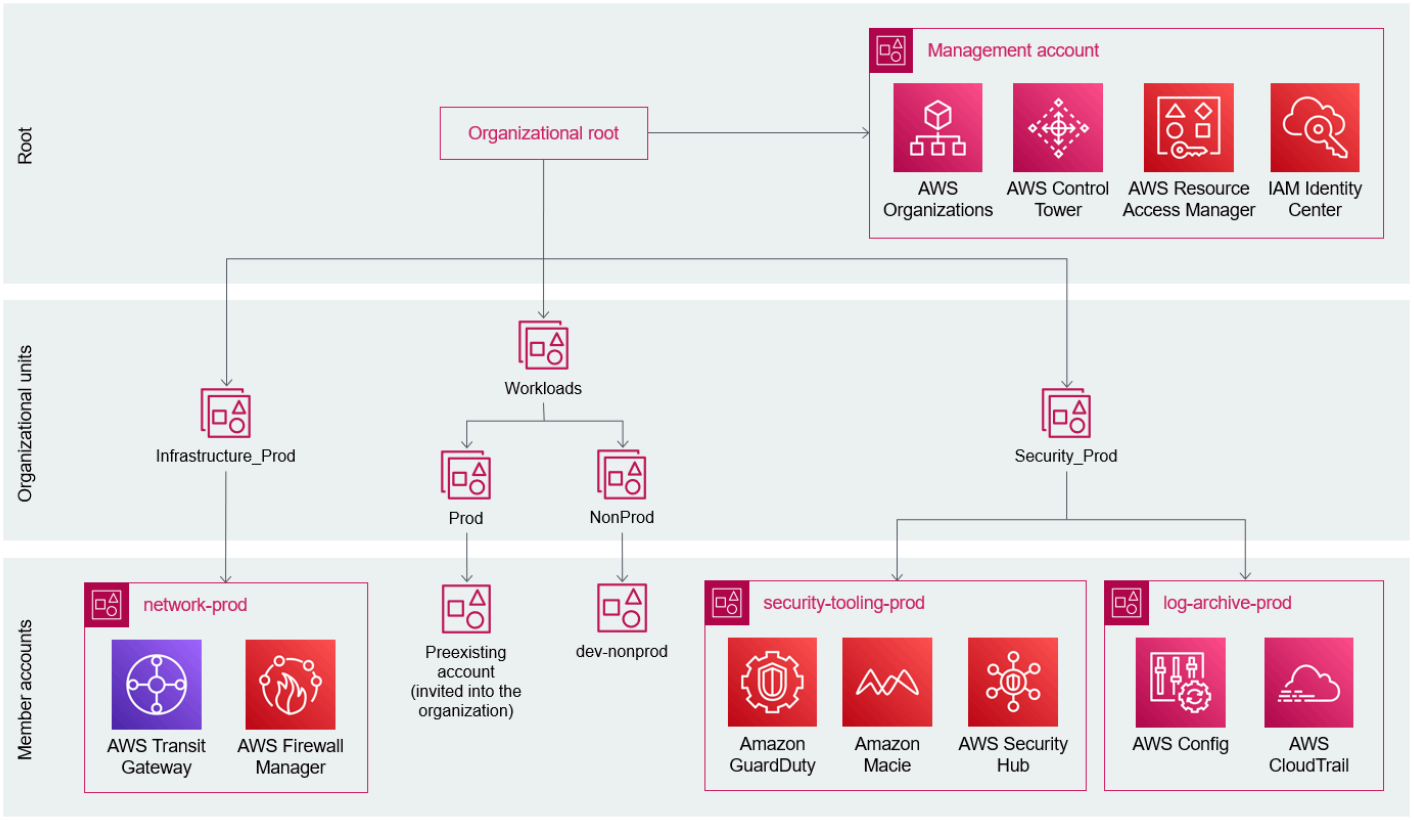
全面的備份策略是公司資料保護計畫的重要組成部分，可以抵禦、復原和減少因安全事件而可能持續存在的任何影響。備份政策可協助您將組織中所有帳戶的資源標準化及實作備份政策。在備份政策中，您可以為您的資源設定和部署備份計劃。如需詳細資訊，請參閱備份政策 (AWS Organizations 文件）。如需詳細資訊，請參閱 中保護備份安全的十大安全最佳實務 AWS(AWS 規範指南）。

轉換至多帳戶架構時的帳戶遷移

在 邀請先前存在的帳戶 中，您已邀請先前存在的帳戶加入工作負載 > 生產組織單位。現在此帳戶作為您組織的一部分進行管理。

您還在工作負載 > 非生產組織單位中佈建了一個新的開發-非生產帳戶。團隊成員現在應能夠透過 存取適當的帳戶 AWS IAM Identity Center。在 AWS Identity and Access Management (IAM) 中移除任何個別使用者帳戶。

如果已遵循本指南中的建議，則您的組織現在具有下列結構。



如果先前存在的帳戶內有工作負載正在執行，您現在可以根據 定義範圍標準 中建立的準則將這些工作負載遷移到獨立帳戶。將任何非生產工作負載遷移至新的工作開發-非生產組織單位，並將生產工作負載遷移至網路-生產帳戶。如需遷移常見 AWS 資源的詳細資訊，請參閱本指南的下一節：資源遷移。

AWS 帳戶之間的資源複製或遷移

從單一帳戶遷移 AWS 帳戶 到多帳戶架構之後，在預先存在的帳戶中執行生產和非生產工作負載是很常見的。將這些資源遷移到專用的生產和非生產帳戶或組織單位，可協助您管理這些工作負載的存取和聯網。以下是將常見 AWS 資源遷移到另一個資源的一些選項 AWS 帳戶。

本節重點介紹在 AWS 帳戶之間複製資料的策略。您應該努力讓工作負載盡可能無狀態，以避免需要在帳戶之間複寫運算資源。透過基礎設施即程式碼 (IaC) 來管理您的資源也是有益的，以便您可以在單獨 AWS 帳戶中重新佈建環境。

本節檢閱遷移下列資料資源的選項：

- AWS AppConfig 組態和環境
- AWS Certificate Manager 憑證
- Amazon CloudFront 分佈
- AWS CodeArtifact 網域和儲存庫
- Amazon DynamoDB 資料表
- Amazon EBS 磁碟區
- Amazon EC2 執行個體或 AMI
- Amazon ECR 登錄檔
- Amazon EFS 檔案系統
- Amazon ElastiCache (Redis OSS) 叢集
- AWS Elastic Beanstalk 環境
- 彈性 IP 位址
- AWS Lambda 層
- Amazon Lightsail 執行個體
- Amazon Neptune 叢集
- Amazon OpenSearch Service 域
- Amazon RDS 快照
- Amazon Redshift 叢集
- Amazon Route 53 域和託管區域
- Amazon S3 儲存貯體

- Amazon SageMaker AI 模型
- AWS WAF Web ACLs

AWS AppConfig 組態和環境

AWS AppConfig 不支援將其組態直接複製到另一個組態 AWS 帳戶。不過，最佳實務是與託管環境 AWS 帳戶 的 分開管理 AWS AppConfig 組態和環境。如需詳細資訊，請參閱使用 的跨帳戶組態 AWS AppConfig (AWS 部落格文章）。

AWS Certificate Manager 憑證

您無法將 AWS Certificate Manager (ACM) 憑證從一個帳戶直接匯出到另一個帳戶，因為用來加密憑證私有金鑰的 AWS Key Management Service (AWS KMS) 金鑰對於每個 AWS 區域 和帳戶都是唯一的。但是，您可以在多個帳戶和區域中同時佈建具有相同域名的多個憑證。ACM 支援使用 DNS (建議) 或電子郵件驗證域擁有權。當您使用 DNS 驗證並建立新憑證時，ACM 會為憑證上每個域產生唯一的 CNAME 記錄。CNAME 記錄對於每個帳戶都是唯一的，必須在 72 小時內將其新增至 Amazon Route 53 託管區域或 DNS 提供商，才能正確驗證憑證。

Amazon CloudFront 分佈

Amazon CloudFront 不支援將分佈從一個 遷移 AWS 帳戶 到另一個 AWS 帳戶。不過，CloudFront 確實支援將替代域名從一個分發遷移到另一個分發，也稱為 CNAME。如需詳細資訊，請參閱如何在為 CloudFront 分佈設定 CNAME 別名時解決 CNAMEAlreadyExists 錯誤 (AWS 知識中心）。

AWS CodeArtifact 網域和儲存庫

雖然組織可以有多個域，但建議您擁有一個包含所有已發行成品的單一生產域。這有助於開發團隊在整個組織中尋找和共用套件。 AWS 帳戶 擁有網域的 可能與擁有與網域關聯之任何儲存庫的帳戶不同。您可以在儲存庫之間複製套件，但其必須屬於同一個域。如需詳細資訊，請參閱在儲存庫間複製套件 (CodeArtifact 文件)。

Amazon DynamoDB 資料表

可以使用下列其中一項服務將 Amazon DynamoDB 表遷移至其他 AWS 帳戶：

- AWS Backup

- DynamoDB 匯入和匯出至 Amazon S3
- Amazon S3 和 AWS Glue
- AWS Data Pipeline
- Amazon EMR

如需詳細資訊，請參閱如何將 Amazon DynamoDB 資料表從一個遷移 AWS 帳戶 到另一個 (AWS 知識中心）。

Amazon EBS 磁碟區

您可以建立現有 Amazon Elastic Block Store (Amazon EBS) 磁碟區的快照，與目標帳戶共用快照，然後在目標帳戶中建立磁碟區複本。這會有效地將磁碟區從一個帳戶遷移到另一個帳戶。如需詳細資訊，請參閱如何與另一個（知識中心）共用加密的 Amazon EBS 快照或磁碟區 AWS 帳戶。AWS

Amazon EC2 執行個體或 AMI

無法將現有 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或 Amazon Machine Image (AMI) 直接遷移到其他 AWS 帳戶。相反，您可以在來源帳戶中建立自訂 AMI、與目標帳戶共用 AMI、從目標帳戶中的共用 AMI 啟動新 EC2 執行個體，然後取消註冊共用 AMI。

Amazon ECR 登錄檔

Amazon Elastic Container Registry (Amazon ECR) 支援跨帳戶和跨區域複寫。可以在來源登錄檔中設定複寫，並在目標登錄檔中設定登錄檔許可政策。如需詳細資訊，請參閱設定跨帳戶複寫 (Amazon ECR 文件) 和允許來源帳戶的根使用者複製所有儲存庫 (Amazon ECR 文件)。

Amazon EFS 檔案系統

Amazon Elastic File System (Amazon EFS) 支援跨帳戶和跨區域複寫。您可以在來源檔案系統上設定複寫。如需詳細資訊，請參閱複寫檔案系統 (Amazon EFS 文件）。

Amazon ElastiCache (Redis OSS) 叢集

您可以使用 Amazon ElastiCache (Redis OSS) 資料庫叢集的備份，將其遷移至不同的 帳戶。如需詳細資訊，請參閱遷移 ElastiCache (Redis OSS) 叢集的最佳實務 (AWS 知識中心）。

AWS Elastic Beanstalk 環境

對於 AWS Elastic Beanstalk，您可以使用已儲存的組態 (Elastic Beanstalk 文件） 將環境遷移至不同的 AWS 帳戶。如需詳細資訊，請參閱如何將 Elastic Beanstalk 環境從一個環境遷移 AWS 帳戶 到另一個 AWS 帳戶環境 (AWS 知識中心）。

彈性 IP 位址

您可以在 AWS 帳戶 位於相同 的 之間轉移彈性 IP 地址 AWS 區域。如需詳細資訊，請參閱傳輸彈性 IP 地址 (Amazon VPC 文件)。

AWS Lambda 層

根據預設，您建立的 AWS Lambda layer 是您的私有 layer AWS 帳戶。不過，您可以選擇與其他 共用 layer AWS 帳戶 或使其公開。若要複製圖層，請在另一個圖層中重新佈建。 AWS 帳戶如需詳細資訊，請參閱設定圖層許可 (Lambda 文件)。

Amazon Lightsail 執行個體

您可以建立 Amazon Lightsail 執行個體的快照，然後將快照匯出至 Amazon Machine Image (AMI) 和 Amazon EBS 磁碟區的加密快照。如需詳細資訊，請參閱將 Amazon Lightsail 快照匯出至 Amazon EC2 (Lightsail 文件)。根據預設，快照會使用在 AWS Key Management Service () 中建立的 AWS 受管金鑰加密AWS KMS。不過，此類型的 KMS 金鑰無法在兩者之間共用 AWS 帳戶。相反，您可以透過可從目標帳戶中使用的客戶受管金鑰來手動加密 AMI 的複本。如需詳細資訊，請參閱允許其他帳戶中的使用者使用 KMS 金鑰 (AWS KMS 文件）。然後，您可以與目標共用複製的 AMI， AWS 帳戶 並從複製Lightsail的 AMI 為 啟動新的 EC2 執行個體。如需詳細資訊，請參閱使用新的啟動執行個體精靈啟動執行個體 (Amazon EC2 文件)。

Amazon Neptune 叢集

您可以將 Amazon Neptune 資料庫叢集的自動化快照複製到另一個 AWS 帳戶。如需詳細資訊，請參閱複製資料庫 (DB) 叢集快照 (Neptune 文件)。

您也可以與最多 20 個AWS 帳戶 共用手動快照，其可以直接從快照中還原資料庫叢集。如需詳細資訊，請參閱共用資料庫叢集快照 (Neptune 文件)。

Amazon OpenSearch Service 域

若要在 Amazon OpenSearch Service 域之間複製資料，您可以使用 Amazon S3 建立來源域的快照，然後將快照還原到不同 AWS 帳戶中的目標域。如需詳細資訊，請參閱如何從另一個（知識中心）中的 Amazon OpenSearch Service 網域還原資料 AWS 帳戶。AWS

如果您在 之間有網路連線 AWS 帳戶，您也可以使用 OpenSearch Service 中的跨叢集複寫 (OpenSearch Service 文件） 功能。 OpenSearch

Amazon RDS 快照

對於 Amazon Relational Database Service (Amazon RDS)，您最多可與 20 個AWS 帳戶共用資料庫執行個體或叢集的手動快照。然後，可從共用快照中還原資料庫執行個體或資料庫叢集。如需詳細資訊，請參閱如何與其他（知識中心）共用手動 Amazon RDS 資料庫快照或 Aurora 資料庫叢集快照 AWS 帳戶。AWS

您也可以使用 AWS Database Migration Service (AWS DMS) 來設定不同帳戶中資料庫執行個體之間的連續複寫。但是，這需要帳戶之間的網路連線，例如 VPC 對等互連或傳輸閘道。

Amazon Redshift 叢集

若要將 Amazon Redshift 叢集遷移至不同的叢集 AWS 帳戶，您可以在來源帳戶中建立叢集的手動快照、與目標共用快照 AWS 帳戶，然後從快照還原叢集。如需詳細資訊，請參閱如何將 Amazon Redshift 佈建叢集複製到不同的 AWS 帳戶 (AWS 知識中心）。

Amazon Route 53 域和託管區域

您可以在 AWS 帳戶之間傳輸 Amazon Route 53 域。如需詳細資訊，請參閱將域傳送到其他 AWS 帳戶 (Route 53 文件)。

您也可以將 Route 53 託管區域遷移至不同的 AWS 帳戶。如需有關何時建議或要求這麼做的詳細資訊，請參閱將託管區域遷移至其他 AWS 帳戶 (Route 53 文件)。遷移託管區域時，會在目標 AWS 帳戶中重新建立它。如需指示，請參閱將託管區域遷移至其他 AWS 帳戶 (Route 53 文件)。

Amazon S3 儲存貯體

您可以使用 Amazon Simple Storage Service (Amazon S3) 相同區域複寫功能在相同 AWS 區域的 S3 儲存貯體之間複製物件。如需詳細資訊，請參閱複製物件 (Amazon S3 文件)。注意下列事項：

- 將複本擁有權變更為 AWS 帳戶 擁有目的地儲存貯體的 。如需指示，請參閱變更複本擁有者 (Amazon S3 文件)。
- 更新儲存貯體擁有者條件，以反映目標儲存貯體的 AWS 帳戶 ID。如需詳細資訊，請參閱使用儲存貯體擁有者條件驗證儲存貯體擁有權 (Amazon S3 文件)。
- 截至 2023 年 4 月，會針對新建立的儲存貯體啟用儲存貯體擁有者強制設定，儲存貯體存取控制清單 (ACL) 和物件 ACL 會失效。如需詳細資訊，請參閱即將推出的 Amazon S3 安全變更 (AWS 部落格文章）。
- 可以使用 S3 批次複寫 (Amazon S3 文件) 來複寫在設定複寫之前已存在的物件。

Amazon SageMaker AI 模型

SageMaker AI 模型在訓練期間存放在 Amazon S3 儲存貯體中。透過從目標帳戶授與 S3 儲存貯體的存取權，您可以將儲存在來源帳戶中的模型部署到目標帳戶。如需詳細資訊，請參閱如何將 Amazon SageMaker AI 模型部署到不同的 AWS 帳戶(AWS 知識中心）。

AWS WAF Web ACLs

AWS WAF Web 存取控制清單 (Web ACLs) 必須與其相關聯的資源位於相同的帳戶中，例如 Amazon CloudFront 分佈、Application Load Balancer、Amazon API Gateway REST APIs 和 AWS AppSync GraphQL APIs。您可以使用 AWS Firewall Manager 來集中管理 區域中整個組織的 AWS WAF Web ACLs AWS Organizations 。如需詳細資訊，請參閱 AWS Firewall Manager AWS WAF 政策入門 (Firewall Manager 文件)。

轉換為多帳戶架構時的帳單考量

如果您使用 AWS Organizations 轉換到多個 AWS 帳戶，您可以使用合併帳單功能 (AWS Organizations 文件）。此功能提供單一合併帳單，顯示多個帳戶的費用。

以下是轉換到多個帳戶的帳單最佳實務和建議：

- 如果您需要存取歷史帳單資料，請在接受加入組織的邀請之前，建立成本和用量報告 (AWS Cost and Usage Report 文件），將帳戶的歷史帳單資料匯出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體。在您接受加入組織的邀請後，帳戶的歷史帳單資料將無法再存取。
- 如果您需要合併兩個組織，例如合併或收購，您可以使用 (AWS 解決方案庫） 的帳戶評估 AWS Organizations來評估每個組織中以資源為基礎的政策，並在合併之前識別任何潛在問題。

結論

如果沒有採用策略，從單一帳戶轉換 AWS 帳戶 到多個帳戶一開始可能會感到不堪負荷。透過實作多帳戶策略，可以解決公司在使用單一 AWS 帳戶時面臨的許多挑戰：

- 錯用開發資料的生產資料 – 您可以使用 AWS IAM Identity Center 搭配單獨的許可集生產和非生產組織單位，來授予不同的許可和存取權。只有高權限使用者才能存取生產資料庫，而且該存取應在有限的時間內進行並經過審核。
- 影響其他業務運作的生產部署 – 您可以使用多個帳戶和多個環境來分隔利益相關者。例如，您可以在非生產帳戶中建立專用的銷售演示環境，以便在未進行演示時規劃部署和發行。
- 測試開發工作負載時，生產工作負載效能緩慢 – 每個 AWS 帳戶 都有獨立的服務配額來管理每個服務。透過使用多個帳戶，您可以限制一個環境對另一個環境的影響範圍。
- 區分生產成本與開發成本 – 組織的合併帳單匯總了 AWS 帳戶 級別的所有成本，以便財務團隊可以了解與非生產環境 (例如開發、測試和演示環境) 相比的生產成本有多少。也可以使用標籤和標記策略來區分帳戶內的成本。
- 限制對敏感資料的存取 – IAM Identity Center 允許您針對特定帳戶相關聯的一組人員制定單獨的存取政策。
- 控制成本 – 透過在多帳戶架構中使用服務控制政策 (SCP)，可以禁止存取會為您的組織帶來高昂成本的特定 AWS 服務 。SCP 可以拒絕對特定服務的所有存取，也可以將服務的使用方式限制為特定類型，例如限制可建立之 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的類型。

貢獻者

本文件的貢獻者包括：

- Justin Plock，首席解決方案架構師， AWS （首席作者）
- Emily Arnautovic，首席架構師， AWS
- Jason DiDomenico，資深解決方案架構師， AWS
- Michael Leighty，資深安全專家解決方案架構師， AWS
- Jesse Lepich，資深安全專家解決方案架構師， AWS
- Rodney Lester，首席解決方案架構師， AWS
- Israel Lopez Moriano，解決方案架構師， AWS
- George Rolston，資深解決方案架構師， AWS
- Alex Torres，資深解決方案架構師 AWS
- Dave Walker，首席解決方案架構師， AWS

資源

AWS 規範性指導

- AWS 啟動安全基準 (AWS SSB)
- AWS 安全參考架構 (AWS SRA)
- 在 中保護備份安全的十大安全最佳實務 AWS

AWS 部落格文章

- 設定 IAM 使用者和 IAM 角色如何協助確保啟動安全
- 如何讓建置人員建立 IAM 資源，同時提升組織的安全性和靈活性

AWS 白皮書

- 使用多個帳戶組織您的 AWS 環境
- 在 上建立您的雲端基礎 AWS
- 建置可擴展且安全的多 VPC AWS 網路基礎設施

AWS 程式碼範例

- 使用 AWS Control Tower 自動化安全服務設定 (GitHub)

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
資源控制政策	我們已將資源控制政策的相關資訊新增至設定組織區段。	2024 年 11 月 20 日
集中式輸出最佳實務	我們更新了保護輸出流量的最佳實務。	2024 年 5 月 6 日
組織最佳實務	我們更新了在 AWS Organizations中建立組織的最佳實務。	2023 年 12 月 4 日
帳單考量	我們新增了帳單考量部分。	2023 年 9 月 20 日
資源遷移、應用程式連線能力和 Amazon VPC Lattice	我們新增了資源遷移和連接應用程式章節。還新增了有關新的 AWS 服務 Amazon Virtual Private Cloud (Amazon VPC) Lattice 的資訊。	2023 年 4 月 27 日
帳戶歷史記錄和 ABAC	我們修訂了建立登陸區域區段，以新增有關如何確保新 AWS 帳戶 具有使用歷史記錄的資訊，以便您可以將它們 AWS Control Tower 新增至登陸區域。我們還修訂了新增初始使用者部分，新增有關如何使用屬性型存取控制 (ABAC) 將驗證方法從外部 SAML 型 IdP 傳遞給 AWS IAM Identity Center的資訊。	2023 年 1 月 6 日
輸出流量網路	我們修訂了集中輸出區段，以新增有關使用 Amazon Route 53 Resolver DNS 防火	2022 年 10 月 13 日

	牆將輸出流量限制為特定網域名稱的資訊。	
輸出流量的安全性	新增了保護輸出流量的最佳實務。	2022 年 10 月 6 日
許可界限	我們改進了許可界限的定義，在資源部分中，新增有關此主題詳細資訊的新連結。	2022 年 9 月 22 日
初次出版	—	2022 年 9 月 6 日

AWS 規範性指引詞彙表

以下是 AWS Prescriptive Guidance 提供的策略、指南和模式中常用的術語。若要建議項目，請使用詞彙表末尾的提供意見回饋連結。

數字

7 R

將應用程式移至雲端的七種常見遷移策略。這些策略以 Gartner 在 2011 年確定的 5 R 為基礎，包括以下內容：

- 重構/重新架構 – 充分利用雲端原生功能來移動應用程式並修改其架構，以提高敏捷性、效能和可擴展性。這通常涉及移植作業系統和資料庫。範例：將您的現場部署 Oracle 資料庫遷移至 Amazon Aurora PostgreSQL 相容版本。
- 平台轉換 (隨即重塑) – 將應用程式移至雲端，並引入一定程度的優化以利用雲端功能。範例：將您的現場部署 Oracle 資料庫遷移至 中的 Amazon Relational Database Service (Amazon RDS) for Oracle AWS 雲端。
- 重新購買 (捨棄再購買) – 切換至不同的產品，通常從傳統授權移至 SaaS 模型。範例：將您的客戶關係管理 (CRM) 系統遷移至 Salesforce.com。
- 主機轉換 (隨即轉移) – 將應用程式移至雲端，而不進行任何變更以利用雲端功能。範例：將您的現場部署 Oracle 資料庫遷移至 中 EC2 執行個體上的 Oracle AWS 雲端。
- 重新放置 (虛擬機器監視器等級隨即轉移) – 將基礎設施移至雲端，無需購買新硬體、重寫應用程式或修改現有操作。您可以將伺服器從內部部署平台遷移到相同平台的雲端服務。範例：將 Microsoft Hyper-V應用程式遷移至 AWS。
- 保留 (重新檢視) – 將應用程式保留在來源環境中。其中可能包括需要重要重構的應用程式，且您希望將該工作延遲到以後，以及您想要保留的舊版應用程式，因為沒有業務理由來進行遷移。
- 淘汰 – 解除委任或移除來源環境中不再需要的應用程式。

A

ABAC

請參閱屬性型存取控制。

抽象服務

請參閱 受管服務。

ACID

請參閱原子性、一致性、隔離性、耐久性。

主動-主動式遷移

一種資料庫遷移方法，其中來源和目標資料庫保持同步 (透過使用雙向複寫工具或雙重寫入操作)，且兩個資料庫都在遷移期間處理來自連接應用程式的交易。此方法支援小型、受控制批次的遷移，而不需要一次性切換。它更靈活，但比主動-被動遷移需要更多的工作。

主動-被動式遷移

一種資料庫遷移方法，其中來源和目標資料庫保持同步，但只有來源資料庫處理來自連接應用程式的交易，同時將資料複寫至目標資料庫。目標資料庫在遷移期間不接受任何交易。

彙總函數

在一組資料列上運作的 SQL 函數，會計算群組的單一傳回值。彙總函數的範例包括 SUM和 MAX。

AI

請參閱人工智慧。

AIOps

請參閱人工智慧操作。

匿名化

在資料集中永久刪除個人資訊的程序。匿名化有助於保護個人隱私權。匿名資料不再被視為個人資料。

反模式

經常用於重複性問題的解決方案，其中解決方案具有反生產力、無效或比替代解決方案更有效。

應用程式控制

一種安全方法，僅允許使用核准的應用程式，以協助保護系統免受惡意軟體攻擊。

應用程式組合

有關組織使用的每個應用程式的詳細資訊的集合，包括建置和維護應用程式的成本及其商業價值。此資訊是產品組合探索和分析程序的關鍵，有助於識別要遷移、現代化和優化的應用程式並排定其優先順序。

人工智慧 (AI)

電腦科學領域，致力於使用運算技術來執行通常與人類相關的認知功能，例如學習、解決問題和識別模式。如需詳細資訊，請參閱什麼是人工智慧？

人工智慧操作 (AIOps)

使用機器學習技術解決操作問題、減少操作事件和人工干預以及提高服務品質的程序。如需有關如何在 AWS 遷移策略中使用 AIOps 的詳細資訊，請參閱操作整合指南。

非對稱加密

一種加密演算法，它使用一對金鑰：一個用於加密的公有金鑰和一個用於解密的私有金鑰。您可以共用公有金鑰，因為它不用於解密，但對私有金鑰存取應受到高度限制。

原子性、一致性、隔離性、耐久性 (ACID)

一組軟體屬性，即使在出現錯誤、電源故障或其他問題的情況下，也能確保資料庫的資料有效性和操作可靠性。

屬性型存取控制 (ABAC)

根據使用者屬性 (例如部門、工作職責和團隊名稱) 建立精細許可的實務。如需詳細資訊，請參閱《 AWS Identity and Access Management (IAM) 文件》中的 ABAC for AWS。

授權資料來源

您存放主要版本資料的位置，被視為最可靠的資訊來源。您可以將授權資料來源中的資料複製到其他位置，以處理或修改資料，例如匿名、修訂或假名化資料。

可用區域

中的不同位置 AWS 區域 ，可隔離其他可用區域中的故障，並提供相同區域中其他可用區域的低成本、低延遲網路連線。

AWS 雲端採用架構 (AWS CAF)

的指導方針和最佳實務架構 AWS ，可協助組織制定高效且有效的計劃，以成功地移至雲端。 AWS CAF 將指導方針組織到六個重點領域：業務、人員、治理、平台、安全和營運。業務、人員和控管層面著重於業務技能和程序；平台、安全和操作層面著重於技術技能和程序。例如，人員層面針對處理人力資源 (HR)、人員配備功能和人員管理的利害關係人。因此， AWS CAF 為人員開發、訓練和通訊提供指引，協助組織做好成功採用雲端的準備。如需詳細資訊，請參閱 AWS CAF 網站和 AWS CAF 白皮書。

AWS 工作負載資格架構 (AWS WQF)

一種工具，可評估資料庫遷移工作負載、建議遷移策略，並提供工作預估值。 AWS WQF 隨附於 AWS Schema Conversion Tool (AWS SCT)。它會分析資料庫結構描述和程式碼物件、應用程式程式碼、相依性和效能特性，並提供評估報告。

B

錯誤的機器人

旨在中斷或傷害個人或組織的機器人。

BCP

請參閱業務持續性規劃。

行為圖

資源行為的統一互動式檢視，以及一段時間後的互動。您可以將行為圖與 Amazon Detective 搭配使用來檢查失敗的登入嘗試、可疑的 API 呼叫和類似動作。如需詳細資訊，請參閱偵測文件中的行為圖中的資料。

大端序系統

首先儲存最高有效位元組的系統。另請參閱 Endianness。

二進制分類

預測二進制結果的過程 (兩個可能的類別之一)。例如，ML 模型可能需要預測諸如「此電子郵件是否是垃圾郵件？」等問題 或「產品是書還是汽車？」

Bloom 篩選條件

一種機率性、記憶體高效的資料結構，用於測試元素是否為集的成員。

藍/綠部署

一種部署策略，您可以在其中建立兩個不同但相同的環境。您可以在一個環境 （藍色） 中執行目前的應用程式版本，並在另一個環境 （綠色） 中執行新的應用程式版本。此策略可協助您快速復原，並將影響降至最低。

機器人

透過網際網路執行自動化任務並模擬人類活動或互動的軟體應用程式。有些機器人有用或有益，例如在網際網路上為資訊編製索引的 Web 爬蟲程式。有些其他機器人稱為惡意機器人，旨在中斷或傷害個人或組織。

殭屍網路

受到惡意軟體感染且受單一方控制之機器人的網路，稱為機器人繼承器或機器人運算子。殭屍網路是擴展機器人及其影響的最佳已知機制。

分支

程式碼儲存庫包含的區域。儲存庫中建立的第一個分支是主要分支。您可以從現有分支建立新分支，然後在新分支中開發功能或修正錯誤。您建立用來建立功能的分支通常稱為功能分支。當準備好發佈功能時，可以將功能分支合併回主要分支。如需詳細資訊，請參閱關於分支 (GitHub 文件)。

碎片存取

在特殊情況下，以及透過核准的程序，讓使用者能夠快速存取他們通常無權存取 AWS 帳戶 的 。如需詳細資訊，請參閱 Well-Architected 指南中的 AWS 實作打破玻璃程序指標。

棕地策略

環境中的現有基礎設施。對系統架構採用棕地策略時，可以根據目前系統和基礎設施的限制來設計架構。如果正在擴展現有基礎設施，則可能會混合棕地和綠地策略。

緩衝快取

儲存最常存取資料的記憶體區域。

業務能力

業務如何創造價值 (例如，銷售、客戶服務或營銷)。業務能力可驅動微服務架構和開發決策。如需詳細資訊，請參閱在 AWS上執行容器化微服務白皮書的圍繞業務能力進行組織部分。

業務連續性規劃 (BCP)

一種解決破壞性事件 (如大規模遷移) 對營運的潛在影響並使業務能夠快速恢復營運的計畫。

C

CAF

請參閱AWS 雲端採用架構。

Canary 部署

版本對最終使用者的緩慢和增量版本。當您有信心時，您可以部署新版本並完全取代目前的版本。

CCoE

請參閱 Cloud Center of Excellence。

CDC

請參閱變更資料擷取。

變更資料擷取 (CDC)

追蹤對資料來源 (例如資料庫表格) 的變更並記錄有關變更的中繼資料的程序。您可以將 CDC 用於各種用途，例如稽核或複寫目標系統中的變更以保持同步。

混沌工程

故意引入故障或破壞性事件，以測試系統的彈性。您可以使用 AWS Fault Injection Service (AWS FIS) 執行實驗，為您的 AWS 工作負載帶來壓力，並評估其回應。

CI/CD

請參閱持續整合和持續交付。

分類

有助於產生預測的分類程序。用於分類問題的 ML 模型可預測離散值。離散值永遠彼此不同。例如，模型可能需要評估影像中是否有汽車。

用戶端加密

在目標 AWS 服務 接收資料之前，在本機加密資料。

雲端卓越中心 (CCoE)

一個多學科團隊，可推動整個組織的雲端採用工作，包括開發雲端最佳實務、調動資源、制定遷移時間表以及領導組織進行大規模轉型。如需詳細資訊，請參閱 AWS 雲端 企業策略部落格上的 CCoE 文章。

雲端運算

通常用於遠端資料儲存和 IoT 裝置管理的雲端技術。雲端運算通常連接到邊緣運算技術。

雲端操作模型

在 IT 組織中，用於建置、成熟和最佳化一或多個雲端環境的操作模型。如需詳細資訊，請參閱建置您的雲端操作模型。

採用雲端階段

組織在遷移至 時通常會經歷的四個階段 AWS 雲端：

- 專案 – 執行一些與雲端相關的專案以進行概念驗證和學習用途
- 基礎 – 進行基礎投資以擴展雲端採用 (例如，建立登陸區域、定義 CCoE、建立營運模型)

- 遷移 – 遷移個別應用程式
- 重塑 – 優化產品和服務，並在雲端中創新

這些階段由 Stephen Orban 於部落格文章 The Journey Toward Cloud-First 和 Enterprise Strategy 部落格上的採用階段中定義。 AWS 雲端 如需有關它們如何與 AWS 遷移策略相關的詳細資訊，請參閱遷移整備指南。

CMDB

請參閱組態管理資料庫。

程式碼儲存庫

透過版本控制程序來儲存及更新原始程式碼和其他資產 (例如文件、範例和指令碼) 的位置。常見的雲端儲存庫包括 GitHub或 Bitbucket Cloud。程式碼的每個版本都稱為分支。在微服務結構中，每個儲存庫都專用於單個功能。單一 CI/CD 管道可以使用多個儲存庫。

冷快取

一種緩衝快取，它是空的、未填充的，或者包含過時或不相關的資料。這會影響效能，因為資料庫執行個體必須從主記憶體或磁碟讀取，這比從緩衝快取讀取更慢。

冷資料

很少存取且通常是歷史資料的資料。查詢這類資料時，通常可接受慢查詢。將此資料移至效能較低且成本較低的儲存層或類別，可以降低成本。

電腦視覺 (CV)

使用機器學習從數位影像和影片等視覺化格式分析和擷取資訊的 AI 欄位。例如，Amazon SageMaker AI 提供 CV 的影像處理演算法。

組態偏離

對於工作負載，組態會從預期狀態變更。這可能會導致工作負載變得不合規，而且通常是漸進和無意的。

組態管理資料庫 (CMDB)

儲存和管理有關資料庫及其 IT 環境的資訊的儲存庫，同時包括硬體和軟體元件及其組態。您通常在遷移的產品組合探索和分析階段使用 CMDB 中的資料。

一致性套件

您可以組合的 AWS Config 規則和修補動作集合，以自訂您的合規和安全檢查。您可以使用 YAML 範本，將一致性套件部署為 AWS 帳戶 和 區域中或整個組織的單一實體。如需詳細資訊，請參閱 AWS Config 文件中的一致性套件。

持續整合和持續交付 (CI/CD)

自動化軟體發行程序的來源、建置、測試、暫存和生產階段的程序。CI/CD 通常被描述為管道。CI/CD 可協助您將程序自動化、提升生產力、改善程式碼品質以及加快交付速度。如需詳細資訊，請參閱持續交付的優點。CD 也可表示持續部署。如需詳細資訊，請參閱持續交付與持續部署。

CV

請參閱電腦視覺。

D

靜態資料

網路中靜止的資料，例如儲存中的資料。

資料分類

根據重要性和敏感性來識別和分類網路資料的程序。它是所有網路安全風險管理策略的關鍵組成部分，因為它可以協助您確定適當的資料保護和保留控制。資料分類是 AWS Well-Architected Framework 中安全支柱的元件。如需詳細資訊，請參閱資料分類。

資料偏離

生產資料與用於訓練 ML 模型的資料之間有意義的變化，或輸入資料隨時間有意義的變更。資料偏離可以降低 ML 模型預測的整體品質、準確性和公平性。

傳輸中的資料

在您的網路中主動移動的資料，例如在網路資源之間移動。

資料網格

架構架構，提供分散式、分散式資料擁有權與集中式管理。

資料最小化

僅收集和處理嚴格必要資料的原則。在 中實作資料最小化 AWS 雲端 可以降低隱私權風險、成本和分析碳足跡。

資料周邊

AWS 環境中的一組預防性防護機制，可協助確保只有信任的身分才能從預期的網路存取信任的資源。如需詳細資訊，請參閱在 上建置資料周邊 AWS。

資料預先處理

將原始資料轉換成 ML 模型可輕鬆剖析的格式。預處理資料可能意味著移除某些欄或列，並解決遺失、不一致或重複的值。

資料來源

在整個生命週期中追蹤資料的原始伺服器和歷史記錄的程序，例如資料的產生、傳輸和儲存方式。

資料主體

正在收集和處理其資料的個人。

資料倉儲

支援商業智慧的資料管理系統，例如 分析。資料倉儲通常包含大量歷史資料，通常用於查詢和分析。

資料庫定義語言 (DDL)

用於建立或修改資料庫中資料表和物件之結構的陳述式或命令。

資料庫處理語言 (DML)

用於修改 (插入、更新和刪除) 資料庫中資訊的陳述式或命令。

DDL

請參閱資料庫定義語言。

深度整體

結合多個深度學習模型進行預測。可以使用深度整體來獲得更準確的預測或估計預測中的不確定性。

深度學習

一個機器學習子領域，它使用多層人工神經網路來識別感興趣的輸入資料與目標變數之間的對應關係。

深度防禦

這是一種資訊安全方法，其中一系列的安全機制和控制項會在整個電腦網路中精心分層，以保護網路和其中資料的機密性、完整性和可用性。當您在 上採用此策略時 AWS，您可以在 AWS Organizations 結構的不同層新增多個控制項，以協助保護資源。例如，defense-in-depth方法可能會結合多重要素驗證、網路分割和加密。

委派的管理員

在 中 AWS Organizations，相容的服務可以註冊 AWS 成員帳戶來管理組織的帳戶，並管理該服務的許可。此帳戶稱為該服務的委派管理員。如需詳細資訊和相容服務清單，請參閱 AWS Organizations 文件中的可搭配 AWS Organizations運作的服務。

部署

在目標環境中提供應用程式、新功能或程式碼修正的程序。部署涉及在程式碼庫中實作變更，然後在應用程式環境中建置和執行該程式碼庫。

開發環境

請參閱 環境。

偵測性控制

一種安全控制，用於在事件發生後偵測、記錄和提醒。這些控制是第二道防線，提醒您注意繞過現有預防性控制的安全事件。如需詳細資訊，請參閱在 AWS上實作安全控制中的偵測性控制。

開發值串流映射 (DVSM)

一種程序，用於識別對軟體開發生命週期中的速度和品質造成負面影響的限制並排定優先順序。DVSM 擴展了最初專為精簡製造實務設計的價值串流映射程序。它著重於透過軟體開發程序建立和移動價值所需的步驟和團隊。

數位分身

真實世界系統的虛擬呈現，例如建築物、工廠、工業設備或生產線。數位分身支援預測性維護、遠端監控和生產最佳化。

維度資料表

在星星結構描述中，較小的資料表包含有關事實資料表中量化資料的資料屬性。維度資料表屬性通常是文字欄位或離散數字，其行為類似於文字。這些屬性通常用於查詢限制、篩選和結果集標記。

災難

防止工作負載或系統在其主要部署位置實現其業務目標的事件。這些事件可能是自然災難、技術故障或人為動作的結果，例如意外設定錯誤或惡意軟體攻擊。

災難復原 (DR)

您用來將災難造成的停機時間和資料遺失降至最低的策略和程序。如需詳細資訊，請參閱 AWS Well-Architected Framework 中的 上工作負載災難復原 AWS：雲端中的復原。

DML

請參閱資料庫處理語言。

領域驅動的設計

一種開發複雜軟體系統的方法，它會將其元件與每個元件所服務的不斷發展的領域或核心業務目標相關聯。Eric Evans 在其著作 Domain-Driven Design: Tackling Complexity in the Heart of Software (Boston: Addison-Wesley Professional, 2003) 中介紹了這一概念。如需有關如何將領域驅動的設計與 strangler fig 模式搭配使用的資訊，請參閱使用容器和 Amazon API Gateway 逐步現代化舊版 Microsoft ASP.NET (ASMX) Web 服務。

DR

請參閱災難復原。

偏離偵測

追蹤與基準組態的偏差。例如，您可以使用 AWS CloudFormation 來偵測系統資源中的偏離，也可以使用 AWS Control Tower 來偵測登陸區域中可能影響控管要求合規性的變更。 https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-stack-drift.html

DVSM

請參閱開發值串流映射。

E

EDA

請參閱探索性資料分析。

EDI

請參閱電子資料交換。

邊緣運算

提升 IoT 網路邊緣智慧型裝置運算能力的技術。與雲端運算相比，邊緣運算可以減少通訊延遲並改善回應時間。

電子資料交換 (EDI)

組織之間商業文件的自動交換。如需詳細資訊，請參閱什麼是電子資料交換。

加密

一種運算程序，可將人類可讀取的純文字資料轉換為加密文字。

加密金鑰

由加密演算法產生的隨機位元的加密字串。金鑰長度可能有所不同，每個金鑰的設計都是不可預測且唯一的。

端序

位元組在電腦記憶體中的儲存順序。大端序系統首先儲存最高有效位元組。小端序系統首先儲存最低有效位元組。

端點

請參閱 服務端點。

端點服務

您可以在虛擬私有雲端 (VPC) 中託管以與其他使用者共用的服務。您可以使用 建立端點服務，AWS PrivateLink 並將許可授予其他 AWS 帳戶 或 AWS Identity and Access Management (IAM) 委託人。這些帳戶或主體可以透過建立介面 VPC 端點私下連接至您的端點服務。如需詳細資訊，請參閱 Amazon Virtual Private Cloud (Amazon VPC) 文件中的建立端點服務。

企業資源規劃 (ERP)

一種系統，可自動化和管理企業的關鍵業務流程 （例如會計、MES 和專案管理）。

信封加密

使用另一個加密金鑰對某個加密金鑰進行加密的程序。如需詳細資訊，請參閱 AWS Key Management Service (AWS KMS) 文件中的信封加密。

環境

執行中應用程式的執行個體。以下是雲端運算中常見的環境類型：

- 開發環境 – 執行中應用程式的執行個體，只有負責維護應用程式的核心團隊才能使用。開發環境用來測試變更，然後再將開發環境提升到較高的環境。此類型的環境有時稱為測試環境。
- 較低的環境 – 應用程式的所有開發環境，例如用於初始建置和測試的開發環境。
- 生產環境 – 最終使用者可以存取的執行中應用程式的執行個體。在 CI/CD 管道中，生產環境是最後一個部署環境。
- 較高的環境 – 核心開發團隊以外的使用者可存取的所有環境。這可能包括生產環境、生產前環境以及用於使用者接受度測試的環境。

epic

在敏捷方法中，有助於組織工作並排定工作優先順序的功能類別。epic 提供要求和實作任務的高層級描述。例如， AWS CAF 安全概念包括身分和存取管理、偵測控制、基礎設施安全、資料保護和事件回應。如需有關 AWS 遷移策略中的 Epic 的詳細資訊，請參閱計畫實作指南。

ERP

請參閱企業資源規劃。

探索性資料分析 (EDA)

分析資料集以了解其主要特性的過程。您收集或彙總資料，然後執行初步調查以尋找模式、偵測異常並檢查假設。透過計算摘要統計並建立資料可視化來執行 EDA。

F

事實資料表

星狀結構描述中的中央資料表。它存放有關業務操作的量化資料。一般而言，事實資料表包含兩種類型的資料欄：包含度量的資料，以及包含維度資料表外部索引鍵的資料欄。

快速失敗

一種使用頻繁和增量測試來縮短開發生命週期的理念。這是敏捷方法的關鍵部分。

故障隔離界限

在 中 AWS 雲端，像是可用區域 AWS 區域、控制平面或資料平面等界限會限制故障的影響，並有助於改善工作負載的彈性。如需詳細資訊，請參閱AWS 故障隔離界限。

功能分支

請參閱分支。

特徵

用來進行預測的輸入資料。例如，在製造環境中，特徵可能是定期從製造生產線擷取的影像。

功能重要性

特徵對於模型的預測有多重要。這通常表示為可以透過各種技術來計算的數值得分，例如 Shapley Additive Explanations (SHAP) 和積分梯度。如需詳細資訊，請參閱 的機器學習模型可解譯性 AWS。

特徵轉換

優化 ML 程序的資料，包括使用其他來源豐富資料、調整值、或從單一資料欄位擷取多組資訊。這可讓 ML 模型從資料中受益。例如，如果將「2021-05-27 00:15:37」日期劃分為「2021」、「五月」、「週四」和「15」，則可以協助學習演算法學習與不同資料元件相關聯的細微模式。

少量擷取提示

在要求 LLM 執行類似的任務之前，提供少量示範任務和所需輸出的範例。此技術是內容內學習的應用程式，其中模型會從內嵌在提示中的範例 (快照) 中學習。對於需要特定格式、推理或網域知識的任務，少量的提示可以有效。另請參閱零鏡頭提示。

FGAC

請參閱精細存取控制。

精細存取控制 (FGAC)

使用多個條件來允許或拒絕存取請求。

閃切遷移

一種資料庫遷移方法，透過變更資料擷取使用連續資料複寫，以盡可能在最短的時間內遷移資料，而不是使用分階段方法。目標是將停機時間降至最低。

FM

請參閱基礎模型。

基礎模型 (FM)

大型深度學習神經網路，已針對廣義和未標記資料的大量資料集進行訓練。FMs 能夠執行各種一般任務，例如了解語言、產生文字和影像，以及自然語言的交談。如需詳細資訊，請參閱什麼是基礎模型。

G

生成式 AI

已針對大量資料進行訓練的 AI 模型子集，可使用簡單的文字提示建立新的內容和成品，例如影像、影片、文字和音訊。如需詳細資訊，請參閱什麼是生成式 AI。

地理封鎖

請參閱地理限制。

地理限制 (地理封鎖)

Amazon CloudFront 中的選項，可防止特定國家/地區的使用者存取內容分發。您可以使用允許清單或封鎖清單來指定核准和禁止的國家/地區。如需詳細資訊，請參閱 CloudFront 文件中的限制內容的地理分佈。

Gitflow 工作流程

這是一種方法，其中較低和較高環境在原始碼儲存庫中使用不同分支。Gitflow 工作流程會被視為舊版，而以幹線為基礎的工作流程是現代、偏好的方法。

黃金影像

系統或軟體的快照，做為部署該系統或軟體新執行個體的範本。例如，在製造中，黃金映像可用於在多個裝置上佈建軟體，並有助於提高裝置製造操作的速度、可擴展性和生產力。

綠地策略

新環境中缺乏現有基礎設施。對系統架構採用綠地策略時，可以選擇所有新技術，而不會限制與現有基礎設施的相容性，也稱為棕地。如果正在擴展現有基礎設施，則可能會混合棕地和綠地策略。

防護機制

有助於跨組織單位 (OU) 來管控資源、政策和合規的高層級規則。預防性防護機制會強制執行政策，以確保符合合規標準。透過使用服務控制政策和 IAM 許可界限來將其實作。偵測性防護機制可偵測政策違規和合規問題，並產生提醒以便修正。它們是透過使用 AWS Config AWS Security Hub、Amazon GuardDuty、、Amazon Inspector AWS Trusted Advisor和自訂 AWS Lambda 檢查來實作。

H

HA

請參閱高可用性。

異質資料庫遷移

將來源資料庫遷移至使用不同資料庫引擎的目標資料庫 (例如，Oracle 至 Amazon Aurora)。異質遷移通常是重新架構工作的一部分，而轉換結構描述可能是一項複雜任務。AWS 提供有助於結構描述轉換的 AWS SCT。

高可用性 (HA)

在遇到挑戰或災難時，工作負載能夠在不介入的情況下持續運作。HA 系統的設計目的是自動容錯移轉、持續提供高品質的效能，並處理不同的負載和故障，並將效能影響降至最低。

歷史現代化

一種方法，用於現代化和升級操作技術 (OT) 系統，以更好地滿足製造業的需求。歷史資料是一種資料庫，用於從工廠中的各種來源收集和存放資料。

保留資料

從用於訓練機器學習模型的資料集中保留的部分歷史標記資料。您可以使用保留資料，透過比較模型預測與保留資料來評估模型效能。

異質資料庫遷移

將您的來源資料庫遷移至共用相同資料庫引擎的目標資料庫 (例如，Microsoft SQL Server 至 Amazon RDS for SQL Server)。同質遷移通常是主機轉換或平台轉換工作的一部分。您可以使用原生資料庫公用程式來遷移結構描述。

熱資料

經常存取的資料，例如即時資料或最近的轉譯資料。此資料通常需要高效能儲存層或類別，才能提供快速的查詢回應。

修補程序

緊急修正生產環境中的關鍵問題。由於其緊迫性，通常會在典型 DevOps 發行工作流程之外執行修補程式。

超級護理期間

在切換後，遷移團隊在雲端管理和監控遷移的應用程式以解決任何問題的時段。通常，此期間的長度為 1-4 天。在超級護理期間結束時，遷移團隊通常會將應用程式的責任轉移給雲端營運團隊。

I

IaC

將基礎設施視為程式碼。

身分型政策

連接至一或多個 IAM 主體的政策，可定義其在 AWS 雲端 環境中的許可。

閒置應用程式

90 天期間 CPU 和記憶體平均使用率在 5% 至 20% 之間的應用程式。在遷移專案中，通常會淘汰這些應用程式或將其保留在內部部署。

IIoT

請參閱工業物聯網。

不可變的基礎設施

為生產工作負載部署新基礎設施的模型，而不是更新、修補或修改現有的基礎設施。不可變基礎設施本質上比可變基礎設施更一致、可靠且可預測。如需詳細資訊，請參閱 AWS Well-Architected Framework 中的使用不可變基礎設施部署最佳實務。

傳入 (輸入) VPC

在 AWS 多帳戶架構中，接受、檢查和路由來自應用程式外部之網路連線的 VPC。AWS 安全參考架構建議您使用傳入、傳出和檢查 VPC 來設定網路帳戶，以保護應用程式與更廣泛的網際網路之間的雙向介面。

增量遷移

一種切換策略，您可以在其中將應用程式分成小部分遷移，而不是執行單一、完整的切換。例如，您最初可能只將一些微服務或使用者移至新系統。確認所有項目都正常運作之後，您可以逐步移動其他微服務或使用者，直到可以解除委任舊式系統。此策略可降低與大型遷移關聯的風險。

工業 4.0

2016 年 Klaus Schwab 推出的術語，透過連線能力、即時資料、自動化、分析和 AI/ML 的進展，指製造程序的現代化。

基礎設施

應用程式環境中包含的所有資源和資產。

基礎設施即程式碼 (IaC)

透過一組組態檔案來佈建和管理應用程式基礎設施的程序。IaC 旨在協助您集中管理基礎設施，標準化資源並快速擴展，以便新環境可重複、可靠且一致。

工業物聯網 (IIoT)

在製造業、能源、汽車、醫療保健、生命科學和農業等產業領域使用網際網路連線的感測器和裝置。如需詳細資訊，請參閱建立工業物聯網 (IIoT) 數位轉型策略。

檢查 VPC

在 AWS 多帳戶架構中，集中式 VPC 可管理 VPCs 之間 （在相同或不同的 中 AWS 區域)、網際網路和內部部署網路之間的網路流量檢查。AWS 安全參考架構建議您使用傳入、傳出和檢查 VPC 來設定網路帳戶，以保護應用程式與更廣泛的網際網路之間的雙向介面。

物聯網 (IoT)

具有內嵌式感測器或處理器的相連實體物體網路，其透過網際網路或本地通訊網路與其他裝置和系統進行通訊。如需詳細資訊，請參閱什麼是 IoT？

可解釋性

機器學習模型的一個特徵，描述了人類能夠理解模型的預測如何依賴於其輸入的程度。如需詳細資訊，請參閱 的機器學習模型可解譯性 AWS。

IoT

請參閱物聯網。

IT 資訊庫 (ITIL)

一組用於交付 IT 服務並使這些服務與業務需求保持一致的最佳實務。ITIL 為 ITSM 提供了基礎。

IT 服務管理 (ITSM)

與組織的設計、實作、管理和支援 IT 服務關聯的活動。如需有關將雲端操作與 ITSM 工具整合的資訊，請參閱操作整合指南。

ITIL

請參閱 IT 資訊庫。

ITSM

請參閱 IT 服務管理。

L

標籤型存取控制 (LBAC)

強制存取控制 (MAC) 的實作，其中使用者和資料本身都會獲得明確指派的安全標籤值。使用者安全標籤和資料安全標籤之間的交集會決定使用者可以看到哪些資料列和資料欄。

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。這是一個起點，您的組織可以從此起點快速啟動和部署工作負載與應用程式，並對其安全和基礎設施環境充滿信心。如需有關登陸區域的詳細資訊，請參閱設定安全且可擴展的多帳戶 AWS 環境。

大型語言模型 (LLM)

預先訓練大量資料的深度學習 AI 模型。LLM 可以執行多個任務，例如回答問題、摘要文件、將文字翻譯成其他語言，以及完成句子。如需詳細資訊，請參閱什麼是 LLMs。

大型遷移

遷移 300 部或更多伺服器。

LBAC

請參閱標籤型存取控制。

最低權限

授予執行任務所需之最低許可的安全最佳實務。如需詳細資訊，請參閱 IAM 文件中的套用最低權限許可。

隨即轉移

請參閱 7 個 R。

小端序系統

首先儲存最低有效位元組的系統。另請參閱 Endianness。

LLM

請參閱大型語言模型。

較低的環境

請參閱 環境。

M

機器學習 (ML)

一種使用演算法和技術進行模式識別和學習的人工智慧。機器學習會進行分析並從記錄的資料 (例如物聯網 (IoT) 資料) 中學習，以根據模式產生統計模型。如需詳細資訊，請參閱機器學習。

主要分支

請參閱分支。

惡意軟體

旨在危及電腦安全或隱私權的軟體。惡意軟體可能會中斷電腦系統、洩露敏感資訊，或取得未經授權的存取。惡意軟體的範例包括病毒、蠕蟲、勒索軟體、特洛伊木馬、間諜軟體和鍵盤記錄器。

受管服務

AWS 服務 會 AWS 操作基礎設施層、作業系統和平台，而您會存取端點來存放和擷取資料。Amazon Simple Storage Service (Amazon S3) 和 Amazon DynamoDB 是受管服務的範例。這些也稱為抽象服務。

製造執行系統 (MES)

一種軟體系統，用於追蹤、監控、記錄和控制生產程序，將原物料轉換為現場成品。

MAP

請參閱遷移加速計劃。

機制

建立工具、推動工具採用，然後檢查結果以進行調整的完整程序。機制是在操作時強化和改善自身的循環。如需詳細資訊，請參閱 AWS Well-Architected Framework 中的建置機制。

成員帳戶

除了屬於組織一部分的管理帳戶 AWS 帳戶 之外的所有 AWS Organizations。一個帳戶一次只能是一個組織的成員。

製造執行系統

請參閱製造執行系統。

訊息佇列遙測傳輸 (MQTT)

根據發佈/訂閱模式的輕量型machine-to-machine(M2M) 通訊協定，適用於資源受限的 IoT 裝置。

微服務

一種小型的獨立服務，它可透過定義明確的 API 進行通訊，通常由小型獨立團隊擁有。例如，保險系統可能包含對應至業務能力 (例如銷售或行銷) 或子領域 (例如購買、索賠或分析) 的微服務。微服務的優點包括靈活性、彈性擴展、輕鬆部署、可重複使用的程式碼和適應力。如需詳細資訊，請參閱使用無 AWS 伺服器服務整合微服務。

微服務架構

一種使用獨立元件來建置應用程式的方法，這些元件會以微服務形式執行每個應用程式程序。這些微服務會使用輕量型 API，透過明確定義的介面進行通訊。此架構中的每個微服務都可以進行

更新、部署和擴展，以滿足應用程式特定功能的需求。如需詳細資訊，請參閱在 上實作微服務 AWS。

Migration Acceleration Program (MAP)

一種 AWS 計畫，提供諮詢支援、訓練和服務，協助組織建立強大的營運基礎，以移至雲端，並協助抵銷遷移的初始成本。MAP 包括用於有條不紊地執行舊式遷移的遷移方法以及一組用於自動化和加速常見遷移案例的工具。

大規模遷移

將大部分應用程式組合依波次移至雲端的程序，在每個波次中，都會以更快的速度移動更多應用程式。此階段使用從早期階段學到的最佳實務和經驗教訓來實作團隊、工具和流程的遷移工廠，以透過自動化和敏捷交付簡化工作負載的遷移。這是 AWS 遷移策略的第三階段。

遷移工廠

可透過自動化、敏捷的方法簡化工作負載遷移的跨職能團隊。遷移工廠團隊通常包括營運、業務分析師和擁有者、遷移工程師、開發人員以及從事 Sprint 工作的 DevOps 專業人員。20% 至 50% 之間的企業應用程式組合包含可透過工廠方法優化的重複模式。如需詳細資訊，請參閱此內容集中的遷移工廠的討論和雲端遷移工廠指南。

遷移中繼資料

有關完成遷移所需的應用程式和伺服器的資訊。每種遷移模式都需要一組不同的遷移中繼資料。遷移中繼資料的範例包括目標子網路、安全群組和 AWS 帳戶。

遷移模式

可重複的遷移任務，詳細描述遷移策略、遷移目的地以及所使用的遷移應用程式或服務。範例：使用 AWS Application Migration Service 重新託管遷移至 Amazon EC2。

遷移組合評定 (MPA)

線上工具，提供驗證商業案例以遷移至 的資訊 AWS 雲端。MPA 提供詳細的組合評定 (伺服器適當規模、定價、總體擁有成本比較、遷移成本分析) 以及遷移規劃 (應用程式資料分析和資料收集、應用程式分組、遷移優先順序，以及波次規劃)。MPA 工具 （需要登入） 可供所有 AWS 顧問和 APN 合作夥伴顧問免費使用。

遷移準備程度評定 (MRA)

使用 AWS CAF 取得組織雲端整備狀態的洞見、識別優缺點，以及建立行動計劃以消除已識別差距的程序。如需詳細資訊，請參閱遷移準備程度指南。MRA 是 AWS 遷移策略的第一階段。

遷移策略

用來將工作負載遷移至 的方法 AWS 雲端。如需詳細資訊，請參閱此詞彙表中的 7 個 Rs 項目，並請參閱動員您的組織以加速大規模遷移。

機器學習 (ML)

請參閱機器學習。

現代化

將過時的 (舊版或單一) 應用程式及其基礎架構轉換為雲端中靈活、富有彈性且高度可用的系統，以降低成本、提高效率並充分利用創新。如需詳細資訊，請參閱《》中的現代化應用程式的策略 AWS 雲端。

現代化準備程度評定

這項評估可協助判斷組織應用程式的現代化準備程度；識別優點、風險和相依性；並確定組織能夠在多大程度上支援這些應用程式的未來狀態。評定的結果就是目標架構的藍圖、詳細說明現代化程序的開發階段和里程碑的路線圖、以及解決已發現的差距之行動計畫。如需詳細資訊，請參閱《》中的評估應用程式的現代化準備 AWS 雲端程度。

單一應用程式 (單一)

透過緊密結合的程序作為單一服務執行的應用程式。單一應用程式有幾個缺點。如果一個應用程式功能遇到需求激增，則必須擴展整個架構。當程式碼庫增長時，新增或改進單一應用程式的功能也會變得更加複雜。若要解決這些問題，可以使用微服務架構。如需詳細資訊，請參閱將單一體系分解為微服務。

MPA

請參閱遷移產品組合評估。

MQTT

請參閱訊息佇列遙測傳輸。

多類別分類

一個有助於產生多類別預測的過程 (預測兩個以上的結果之一)。例如，機器學習模型可能會詢問「此產品是書籍、汽車還是電話？」 或者「這個客戶對哪種產品類別最感興趣？」

可變基礎設施

更新和修改生產工作負載現有基礎設施的模型。為了提高一致性、可靠性和可預測性， AWS Well-Architected Framework 建議使用不可變基礎設施做為最佳實務。

O

OAC

請參閱原始存取控制。

OAI

請參閱原始存取身分。

OCM

請參閱組織變更管理。

離線遷移

一種遷移方法，可在遷移過程中刪除來源工作負載。此方法涉及延長停機時間，通常用於小型非關鍵工作負載。

OI

請參閱 操作整合。

OLA

請參閱操作層級協議。

線上遷移

一種遷移方法，無需離線即可將來源工作負載複製到目標系統。連接至工作負載的應用程式可在遷移期間繼續運作。此方法涉及零至最短停機時間，通常用於關鍵的生產工作負載。

OPC-UA

請參閱開放程序通訊 - 統一架構。

開放程序通訊 - 統一架構 (OPC-UA)

用於工業自動化的machine-to-machine(M2M) 通訊協定。OPC-UA 提供資料加密、身分驗證和授權機制的互通性標準。

操作水準協議 (OLA)

一份協議，闡明 IT 職能群組承諾向彼此提供的內容，以支援服務水準協議 (SLA)。

操作整備審查 (ORR)

問題和相關最佳實務的檢查清單，可協助您了解、評估、預防或減少事件和可能失敗的範圍。如需詳細資訊，請參閱 AWS Well-Architected Framework 中的操作準備度審查 (ORR)。

操作技術 (OT)

使用實體環境控制工業操作、設備和基礎設施的硬體和軟體系統。在製造業中，整合 OT 和資訊技術 (IT) 系統是工業 4.0 轉型的關鍵重點。

操作整合 (OI)

在雲端中將操作現代化的程序，其中包括準備程度規劃、自動化和整合。如需詳細資訊，請參閱操作整合指南。

組織追蹤

由 建立的線索 AWS CloudTrail 會記錄 AWS 帳戶 組織中所有 的所有事件 AWS Organizations。在屬於組織的每個 AWS 帳戶 中建立此追蹤，它會跟蹤每個帳戶中的活動。如需詳細資訊，請參閱 CloudTrail 文件中的建立組織追蹤。

組織變更管理 (OCM)

用於從人員、文化和領導力層面管理重大、顛覆性業務轉型的架構。OCM 透過加速變更採用、解決過渡問題，以及推動文化和組織變更，協助組織為新系統和策略做好準備，並轉移至新系統和策略。在 AWS 遷移策略中，此架構稱為人員加速，因為雲端採用專案所需的變更速度。如需詳細資訊，請參閱 OCM 指南。

原始存取控制 (OAC)

CloudFront 中的增強型選項，用於限制存取以保護 Amazon Simple Storage Service (Amazon S3) 內容。OAC 支援所有 S3 儲存貯體中的所有伺服器端加密 AWS KMS (SSE-KMS) AWS 區域，以及對 S3 儲存貯體的動態PUT和DELETE請求。

原始存取身分 (OAI)

CloudFront 中的一個選項，用於限制存取以保護 Amazon S3 內容。當您使用 OAI 時，CloudFront 會建立一個可供 Amazon S3 進行驗證的主體。經驗證的主體只能透過特定 CloudFront 分發來存取 S3 儲存貯體中的內容。另請參閱 OAC，它可提供更精細且增強的存取控制。

ORR

請參閱操作整備審核。

OT

請參閱操作技術。

傳出 (輸出) VPC

在 AWS 多帳戶架構中，處理從應用程式內啟動之網路連線的 VPC。AWS 安全參考架構建議您使用傳入、傳出和檢查 VPC 來設定網路帳戶，以保護應用程式與更廣泛的網際網路之間的雙向介面。

P

許可界限

附接至 IAM 主體的 IAM 管理政策，可設定使用者或角色擁有的最大許可。如需詳細資訊，請參閱 IAM 文件中的許可界限。

個人身分識別資訊 (PII)

直接檢視或與其他相關資料配對時，可用來合理推斷個人身分的資訊。PII 的範例包括名稱、地址和聯絡資訊。

PII

請參閱個人身分識別資訊。

手冊

一組預先定義的步驟，可擷取與遷移關聯的工作，例如在雲端中提供核心操作功能。手冊可以採用指令碼、自動化執行手冊或操作現代化環境所需的程序或步驟摘要的形式。

PLC

請參閱可程式設計邏輯控制器。

PLM

請參閱產品生命週期管理。

政策

可定義許可的物件（請參閱身分型政策）、指定存取條件（請參閱資源型政策），或定義組織中所有帳戶的最大許可 AWS Organizations（請參閱服務控制政策）。

混合持久性

根據資料存取模式和其他需求，獨立選擇微服務的資料儲存技術。如果您的微服務具有相同的資料儲存技術，則其可能會遇到實作挑戰或效能不佳。如果微服務使用最適合其需求的資料儲存，則

可以更輕鬆地實作並達到更好的效能和可擴展性。如需詳細資訊，請參閱在微服務中啟用資料持久性。

組合評定

探索、分析應用程式組合並排定其優先順序以規劃遷移的程序。如需詳細資訊，請參閱評估遷移準備程度。

述詞

傳回 `true`或 的查詢條件`false`，通常位於 `WHERE`子句中。

述詞下推

一種資料庫查詢最佳化技術，可在傳輸前篩選查詢中的資料。這可減少必須從關聯式資料庫擷取和處理的資料量，並改善查詢效能。

預防性控制

旨在防止事件發生的安全控制。這些控制是第一道防線，可協助防止對網路的未經授權存取或不必要變更。如需詳細資訊，請參閱在 AWS上實作安全控制中的預防性控制。

委託人

中可執行動作和存取資源 AWS 的實體。此實體通常是 AWS 帳戶、IAM 角色或使用者的根使用者。如需詳細資訊，請參閱 IAM 文件中角色術語和概念中的主體。

依設計的隱私權

透過整個開發程序將隱私權納入考量的系統工程方法。

私有託管區域

一種容器，它包含有關您希望 Amazon Route 53 如何回應一個或多個 VPC 內的域及其子域之 DNS 查詢的資訊。如需詳細資訊，請參閱 Route 53 文件中的使用私有託管區域。

主動控制

旨在防止部署不合規資源的安全控制。這些控制項會在佈建資源之前對其進行掃描。如果資源不符合控制項，則不會佈建。如需詳細資訊，請參閱 AWS Control Tower 文件中的控制項參考指南，並參閱實作安全控制項中的主動控制項。 AWS

產品生命週期管理 (PLM)

管理產品整個生命週期的資料和程序，從設計、開發和啟動，到成長和成熟，再到拒絕和移除。

生產環境

請參閱 環境。

可程式設計邏輯控制器 (PLC)

在製造中，高度可靠、可調整的電腦，可監控機器並自動化製造程序。

提示鏈結

使用一個 LLM 提示的輸出做為下一個提示的輸入，以產生更好的回應。此技術用於將複雜任務分解為子任務，或反覆精簡或展開初步回應。它有助於提高模型回應的準確性和相關性，並允許更精細、個人化的結果。

擬匿名化

將資料集中的個人識別符取代為預留位置值的程序。假名化有助於保護個人隱私權。假名化資料仍被視為個人資料。

發佈/訂閱 (pub/sub)

一種模式，可啟用微服務之間的非同步通訊，以提高可擴展性和回應能力。例如，在微服務型 MES 中，微服務可以將事件訊息發佈到其他微服務可訂閱的頻道。系統可以新增新的微服務，而無需變更發佈服務。

Q

查詢計劃

一系列步驟，如指示，用於存取 SQL 關聯式資料庫系統中的資料。

查詢計劃迴歸

在資料庫服務優化工具選擇的計畫比對資料庫環境進行指定的變更之前的計畫不太理想時。這可能因為對統計資料、限制條件、環境設定、查詢參數繫結的變更以及資料庫引擎的更新所導致。

R

RACI 矩陣

請參閱負責、負責、諮詢、告知 (RACI)。

RAG

請參閱擷取增強產生。

勒索軟體

一種惡意軟體，旨在阻止對計算機系統或資料的存取，直到付款為止。

RASCI 矩陣

請參閱負責、負責、諮詢、告知 (RACI)。

RCAC

請參閱資料列和資料欄存取控制。

僅供讀取複本

用於唯讀用途的資料庫複本。您可以將查詢路由至僅供讀取複本以減少主資料庫的負載。

重新架構師

請參閱 7 個 R。

復原點目標 (RPO)

自上次資料復原點以來可接受的時間上限。這會決定最後一個復原點與服務中斷之間可接受的資料遺失。

復原時間目標 (RTO)

服務中斷與服務還原之間的可接受延遲上限。

重構

請參閱 7 個 R。

區域

地理區域中的 AWS 資源集合。每個 AWS 區域 都獨立於其他 ，以提供容錯能力、穩定性和彈性。如需詳細資訊，請參閱指定 AWS 區域 您的帳戶可以使用哪些 。

迴歸

預測數值的 ML 技術。例如，為了解決「這房子會賣什麼價格？」的問題 ML 模型可以使用線性迴歸模型，根據已知的房屋事實 (例如，平方英尺) 來預測房屋的銷售價格。

重新託管

請參閱 7 個 R。

版本

在部署程序中，它是將變更提升至生產環境的動作。

重新定位

請參閱 7 個 R。

Replatform

請參閱 7 個 R。

回購

請參閱 7 個 R。

彈性

應用程式抵禦中斷或從中斷中復原的能力。在 中規劃彈性時，高可用性和災難復原是常見的考量 AWS 雲端。如需詳細資訊，請參閱AWS 雲端 彈性。

資源型政策

附接至資源的政策，例如 Amazon S3 儲存貯體、端點或加密金鑰。這種類型的政策會指定允許存取哪些主體、支援的動作以及必須滿足的任何其他條件。

負責者、當責者、事先諮詢者和事後告知者 (RACI) 矩陣

矩陣，定義所有涉及遷移活動和雲端操作之各方的角色和責任。矩陣名稱衍生自矩陣中定義的責任類型：負責人 (R)、責任 (A)、已諮詢 (C) 和知情 (I)。支援 (S) 類型為選用。如果您包含支援，則矩陣稱為 RASCI 矩陣，如果您排除它，則稱為 RACI 矩陣。

回應性控制

一種安全控制，旨在驅動不良事件或偏離安全基準的補救措施。如需詳細資訊，請參閱在 AWS上實作安全控制中的回應性控制。

保留

請參閱 7 個 R。

淘汰

請參閱 7 Rs。

檢索增強生成 (RAG)

一種生成式 AI 技術，其中 LLM 會在產生回應之前參考訓練資料來源以外的授權資料來源。例如，RAG 模型可能會對組織的知識庫或自訂資料執行語意搜尋。如需詳細資訊，請參閱什麼是 RAG。

輪換

定期更新秘密的程序，讓攻擊者更難存取登入資料。

資料列和資料欄存取控制 (RCAC)

使用已定義存取規則的基本、彈性 SQL 表達式。RCAC 包含資料列許可和資料欄遮罩。

RPO

請參閱復原點目標。

RTO

請參閱復原時間目標。

執行手冊

執行特定任務所需的一組手動或自動程序。這些通常是為了簡化重複性操作或錯誤率較高的程序而建置。

S

SAML 2.0

許多身分提供者 (IdP) 使用的開放標準。此功能會啟用聯合單一登入 (SSO)，讓使用者可以登入 AWS Management Console 或呼叫 AWS API 操作，而不必為您組織中的每個人在 IAM 中建立使用者。如需有關以 SAML 2.0 為基礎的聯合詳細資訊，請參閱 IAM 文件中的關於以 SAML 2.0 為基礎的聯合。

SCADA

請參閱監督控制和資料擷取。

SCP

請參閱服務控制政策。

秘密

您以加密形式存放的 AWS Secrets Manager機密或限制資訊，例如密碼或使用者登入資料。它由秘密值及其中繼資料組成。秘密值可以是二進位、單一字串或多個字串。如需詳細資訊，請參閱 Secrets Manager 文件中的 Secrets Manager 秘密中的什麼內容？。

設計安全性

透過整個開發程序將安全性納入考量的系統工程方法。

安全控制

一種技術或管理防護機制，它可預防、偵測或降低威脅行為者利用安全漏洞的能力。安全控制有四種主要類型：預防性、偵測性、回應性和主動性。

安全強化

減少受攻擊面以使其更能抵抗攻擊的過程。這可能包括一些動作，例如移除不再需要的資源、實作授予最低權限的安全最佳實務、或停用組態檔案中不必要的功能。

安全資訊與事件管理 (SIEM) 系統

結合安全資訊管理 (SIM) 和安全事件管理 (SEM) 系統的工具與服務。SIEM 系統會收集、監控和分析來自伺服器、網路、裝置和其他來源的資料，以偵測威脅和安全漏洞，並產生提醒。

安全回應自動化

預先定義和程式設計的動作，旨在自動回應或修復安全事件。這些自動化可做為偵測或回應式安全控制，協助您實作 AWS 安全最佳實務。自動化回應動作的範例包括修改 VPC 安全群組、修補 Amazon EC2 執行個體或輪換登入資料。

伺服器端加密

由 AWS 服務 接收資料的 在其目的地加密資料。

服務控制政策 (SCP)

為 AWS Organizations中的組織的所有帳戶提供集中控制許可的政策。SCP 會定義防護機制或設定管理員可委派給使用者或角色的動作限制。您可以使用 SCP 作為允許清單或拒絕清單，以指定允許或禁止哪些服務或動作。如需詳細資訊，請參閱 AWS Organizations 文件中的服務控制政策。

服務端點

的進入點 URL AWS 服務。您可以使用端點，透過程式設計方式連接至目標服務。如需詳細資訊，請參閱 AWS 一般參考 中的 AWS 服務 端點。

服務水準協議 (SLA)

一份協議，闡明 IT 團隊承諾向客戶提供的服務，例如服務正常執行時間和效能。

服務層級指標 (SLI)

服務效能層面的測量，例如其錯誤率、可用性或輸送量。

服務層級目標 (SLO)

代表服務運作狀態的目標指標，由服務層級指標測量。

共同責任模式

描述您與 共同 AWS 承擔雲端安全與合規責任的模型。 AWS 負責雲端的安全，而 負責雲端的安全。如需詳細資訊，請參閱共同責任模式。

SIEM

請參閱安全資訊和事件管理系統。

單一故障點 (SPOF)

應用程式的單一關鍵元件故障，可能會中斷系統。

SLA

請參閱服務層級協議。

SLI

請參閱服務層級指標。

SLO

請參閱服務層級目標。

先拆分後播種模型

擴展和加速現代化專案的模式。定義新功能和產品版本時，核心團隊會進行拆分以建立新的產品團隊。這有助於擴展組織的能力和服務，提高開發人員生產力，並支援快速創新。如需詳細資訊，請參閱 中的階段式應用程式現代化方法 AWS 雲端。

SPOF

請參閱單一故障點。

星狀結構描述

使用一個大型事實資料表來存放交易或測量資料的資料庫組織結構，並使用一或多個較小的維度資料表來存放資料屬性。此結構旨在用於資料倉儲或商業智慧用途。

Strangler Fig 模式

一種現代化單一系統的方法，它會逐步重寫和取代系統功能，直到舊式系統停止使用為止。此模式源自無花果藤，它長成一棵馴化樹並最終戰勝且取代了其宿主。該模式由 Martin Fowler 引入，作

為重寫單一系統時管理風險的方式。如需有關如何套用此模式的範例，請參閱使用容器和 Amazon API Gateway 逐步現代化舊版 Microsoft ASP.NET (ASMX) Web 服務。

子網

您 VPC 中的 IP 地址範圍。子網必須位於單一可用區域。

監控控制和資料擷取 (SCADA)

在製造中，使用硬體和軟體來監控實體資產和生產操作的系統。

對稱加密

使用相同金鑰來加密及解密資料的加密演算法。

合成測試

以模擬使用者互動的方式測試系統，以偵測潛在問題或監控效能。您可以使用 Amazon CloudWatch Synthetics 來建立這些測試。

系統提示

一種向 LLM 提供內容、指示或指導方針以指示其行為的技術。系統提示有助於設定內容，並建立與使用者互動的規則。

T

標籤

做為中繼資料以組織 AWS 資源的鍵值對。標籤可協助您管理、識別、組織、搜尋及篩選資源。如需詳細資訊，請參閱標記您的 AWS 資源。

目標變數

您嘗試在受監督的 ML 中預測的值。這也被稱為結果變數。例如，在製造設定中，目標變數可能是產品瑕疵。

任務清單

用於透過執行手冊追蹤進度的工具。任務清單包含執行手冊的概觀以及要完成的一般任務清單。對於每個一般任務，它包括所需的預估時間量、擁有者和進度。

測試環境

請參閱 環境。

訓練

為 ML 模型提供資料以供學習。訓練資料必須包含正確答案。學習演算法會在訓練資料中尋找將輸入資料屬性映射至目標的模式 (您想要預測的答案)。它會輸出擷取這些模式的 ML 模型。可以使用 ML 模型，來預測您不知道的目標新資料。

傳輸閘道

可以用於互連 VPC 和內部部署網路的網路傳輸中樞。如需詳細資訊，請參閱 AWS Transit Gateway 文件中的什麼是傳輸閘道。

主幹型工作流程

這是一種方法，開發人員可在功能分支中本地建置和測試功能，然後將這些變更合併到主要分支中。然後，主要分支會依序建置到開發環境、生產前環境和生產環境中。

受信任的存取權

將許可授予您指定的服務，以代表您在組織中 AWS Organizations 及其帳戶中執行任務。受信任的服務會在需要該角色時，在每個帳戶中建立服務連結角色，以便為您執行管理工作。如需詳細資訊，請參閱 文件中的 AWS Organizations 搭配使用 AWS Organizations 與其他 AWS 服務。

調校

變更訓練程序的各個層面，以提高 ML 模型的準確性。例如，可以透過產生標籤集、新增標籤、然後在不同的設定下多次重複這些步驟來訓練 ML 模型，以優化模型。

雙比薩團隊

兩個比薩就能吃飽的小型 DevOps 團隊。雙披薩團隊規模可確保軟體開發中的最佳協作。

U

不確定性

這是一個概念，指的是不精確、不完整或未知的資訊，其可能會破壞預測性 ML 模型的可靠性。有兩種類型的不確定性：認知不確定性是由有限的、不完整的資料引起的，而隨機不確定性是由資料中固有的噪聲和隨機性引起的。如需詳細資訊，請參閱量化深度學習系統的不確定性指南。

未區分的任務

也稱為繁重工作，這是建立和操作應用程式的必要工作，但不為最終使用者提供直接價值或提供競爭優勢。未區分任務的範例包括採購、維護和容量規劃。

較高的環境

請參閱 環境。

V

清空

一種資料庫維護操作，涉及增量更新後的清理工作，以回收儲存並提升效能。

版本控制

追蹤變更的程序和工具，例如儲存庫中原始程式碼的變更。

VPC 對等互連

兩個 VPC 之間的連線，可讓您使用私有 IP 地址路由流量。如需詳細資訊，請參閱 Amazon VPC 文件中的什麼是 VPC 對等互連。

漏洞

危害系統安全性的軟體或硬體瑕疵。

W

暖快取

包含經常存取的目前相關資料的緩衝快取。資料庫執行個體可以從緩衝快取讀取，這比從主記憶體或磁碟讀取更快。

暖資料

不常存取的資料。查詢這類資料時，通常可接受中等速度的查詢。

視窗函數

SQL 函數，對與目前記錄有某種程度關聯的資料列群組執行計算。視窗函數適用於處理任務，例如根據目前資料列的相對位置計算移動平均值或存取資料列的值。

工作負載

提供商業價值的資源和程式碼集合，例如面向客戶的應用程式或後端流程。

工作串流

遷移專案中負責一組特定任務的功能群組。每個工作串流都是獨立的，但支援專案中的其他工作串流。例如，組合工作串流負責排定應用程式、波次規劃和收集遷移中繼資料的優先順序。組合工作串流將這些資產交付至遷移工作串流，然後再遷移伺服器和應用程式。

WORM

請參閱寫入一次，讀取許多。

WQF

請參閱AWS 工作負載資格架構。

寫入一次，讀取許多 (WORM)

儲存模型，可一次性寫入資料，並防止刪除或修改資料。授權使用者可以視需要多次讀取資料，但無法變更資料。此資料儲存基礎設施被視為不可變。

Z

零時差入侵

利用零時差漏洞的攻擊，通常是惡意軟體。

零時差漏洞

生產系統中未緩解的缺陷或漏洞。威脅行為者可以使用這種類型的漏洞來攻擊系統。開發人員經常因為攻擊而意識到漏洞。

零鏡頭提示

提供 LLM 執行任務的指示，但沒有可協助引導任務的範例 (快照)。LLM 必須使用其預先訓練的知識來處理任務。零鏡頭提示的有效性取決於任務的複雜性和提示的品質。另請參閱少量擷取提示。

殭屍應用程式

CPU 和記憶體平均使用率低於 5% 的應用程式。在遷移專案中，通常會淘汰這些應用程式。

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。