



使用 建置企業藍圖工廠 AWS Service Catalog

AWS 方案指引



AWS 方案指引: 使用 建置企業藍圖工廠 AWS Service Catalog

Copyright © 2025 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
業務概觀	1
解決方案概觀	1
目標對象	2
目標	2
架構	3
元件	4
產品儲存庫	4
組態儲存庫	5
組態檔案	5
設定管道	6
發行管道	9
藍圖生命週期	11
藍圖建立	12
藍圖更新	12
藍圖刪除	13
設定	15
先決條件	15
最佳實務	16
建立儲存庫	16
設定工廠	17
刪除工廠	24
使用原廠	25
先決條件	25
建立藍圖	25
更新藍圖	27
刪除藍圖	29
故障診斷	30
相關資源	32
AWS 文件	32
AWS 部落格文章	32
貢獻者	33
編寫	33
檢閱	33

技術寫入 33

文件歷史紀錄 34

詞彙表 35

..... 35

A 35

B 38

C 39

D 42

E 45

F 47

G 48

H 49

I 50

L 52

M 53

O 57

P 59

Q 61

R 62

S 64

T 67

U 68

V 69

W 69

Z 70

..... lxxi

使用 建置企業藍圖工廠 AWS Service Catalog

Amazon Web Services ([貢獻者](#))

2024 年 10 月 ([文件歷史記錄](#))

業務概觀

許多企業在雲端中擴展工作負載時面臨挑戰。這些組織挑戰包括下列項目：

- 建立基礎設施做為程式碼 (IaC) 範本，這些範本可以針對多個 大規模重複使用 AWS 服務
- 驗證 IaC 範本遵循安全最佳實務
- 減少[未區分](#)或重複的任務，可大幅降低開發人員生產力並延長上市時間
- 建立 IaC 範本的一致性
- 降低資源使用率，尤其是安全團隊，以避免可重複的手動檢閱

建立遵循安全最佳實務的 IaC 範本需要您建立護欄和安全控制。傳統上，雲端平台團隊或安全團隊會手動檢閱每個 IaC 範本中的程式碼。或者，開發人員會在非生產環境中部署 IaC 範本，並依賴[偵測性控制](#)來尋找任何安全問題。這兩種方法都需要反覆的意見回饋週期、減緩開發程序，以及增加手動工程工作。

因此，許多企業想要簡化 IaC 範本的建立、驗證和發行。他們也想要在發行後管理這些範本。適當的管理和控管機制可協助您更新範本，並確保開發人員可以存取最新版本。這些機制也可協助您監督和稽核整個組織中範本的使用。

解決方案概觀

本指南說明企業藍圖工廠解決方案，可協助您簡化整個組織的基礎設施即程式碼 (IaC) 範本的建立、驗證、發佈、分發和使用。這些 IaC 範本也稱為藍圖。此解決方案支援 AWS CloudFormation [範本](#) 或 AWS Cloud Development Kit (AWS CDK) [建構的](#) 藍圖檔案。

企業藍圖工廠使用組態導向方法來自動化藍圖的共用、發佈和分發。開發人員將藍圖新增至產品儲存庫，然後將藍圖資訊新增至組態檔案。這會自動啟動持續整合和持續交付 (CI/CD) 發行管道。此管道會驗證藍圖是否遵循 AWS 安全最佳實務。這有助於確保您組織的藍圖在設計上是安全的。安全性設計是一種系統工程方法，可透過整個開發程序將安全性納入考量。

企業藍圖工廠將藍圖發佈為 中的產品[AWS Service Catalog](#)。透過使用 Service Catalog，最終使用者可以快速部署您提供的已核准藍圖。Service Catalog 也旨在提供管理和管理功能，以便管理員可以定義[精細存取控制](#)並監督藍圖使用情況。

目標對象

[企業藍圖工廠架構](#)區段可協助架構師、經理和技術負責人評估此解決方案，並判斷其是否適合其組織。本節說明什麼是藍圖、如何使用 Service Catalog 來管理藍圖，以及企業藍圖工廠的架構。

[設定企業藍圖工廠](#)一節可協助 DevOps 工程師在您的 AWS 環境中部署企業藍圖工廠。它包含設定所需儲存庫和組態管道的詳細說明。

[使用企業藍圖工廠](#)區段可協助藍圖開發人員在您的環境中建立、更新或刪除藍圖。它提供在其整個生命週期中管理藍圖的詳細說明。若要建立藍圖，開發人員必須了解如何建立 IaC 範本，例如 CloudFormation 範本。本指南不包含有關如何定義這些藍圖的資訊或指示。

目標

Enterprise 藍圖工廠可協助您的組織實現下列優勢：

- 驗證藍圖是否遵循 AWS 安全最佳實務
- 自動化和標準化藍圖的發行和驗證程序
- 透過減少開發人員必須執行的手動任務數量來提高開發人員生產力
- 使用精細存取控制來判斷最終使用者可以存取哪些藍圖
- 使用版本控制來管理藍圖更新，並與最終使用者共用
- 協助最終使用者自助探索和啟動藍圖
- 監督和稽核整個組織的藍圖使用

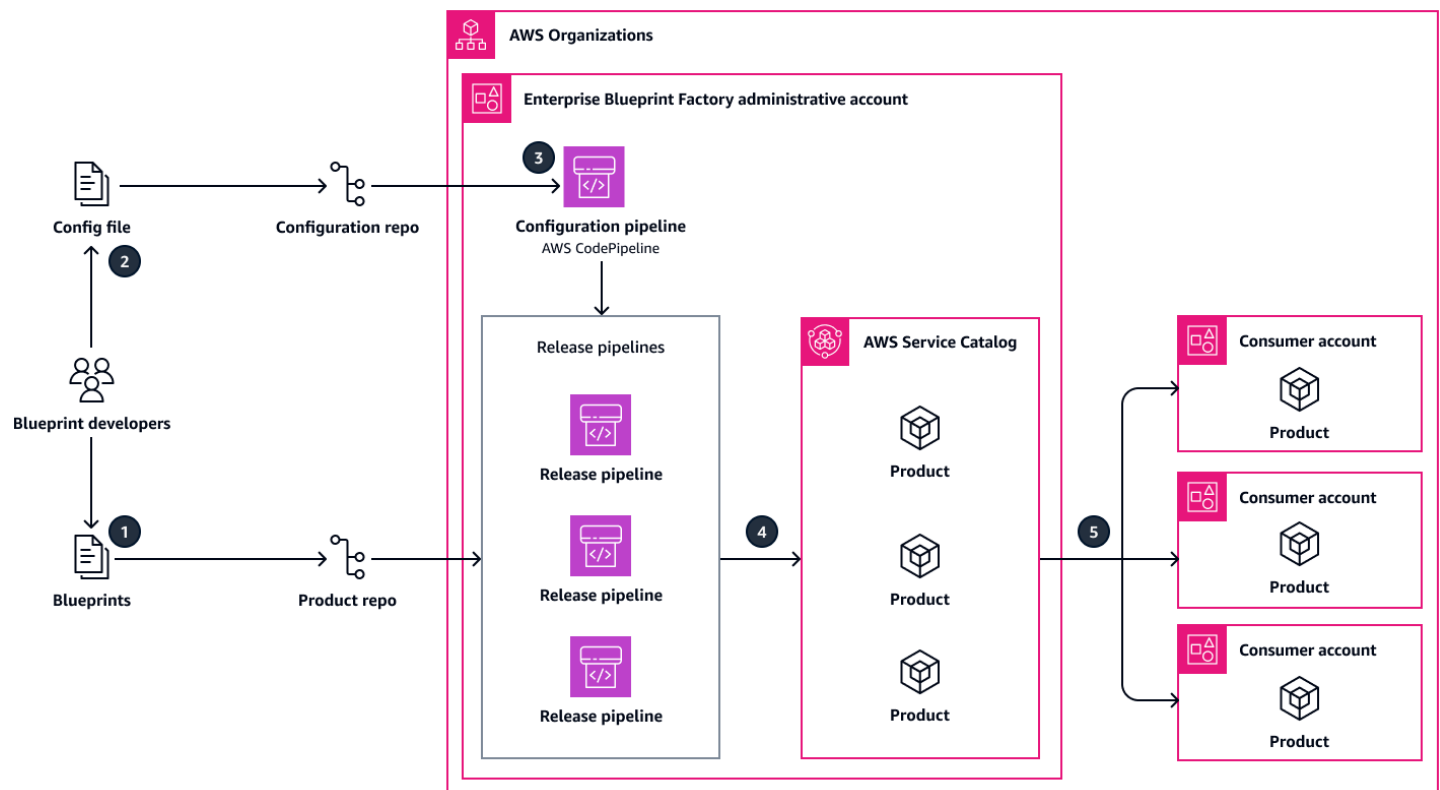
企業藍圖工廠架構

基礎設施即程式碼 (IaC) 範本也稱為藍圖，是一種組態檔案，可協助您佈建和管理雲端資源。藍圖可能會佈建單一資源，也可能為複雜的多層應用程式佈建架構。IaC 旨在協助您集中管理基礎設施、標準化資源並快速擴展。

企業藍圖工廠可協助您簡化整個組織的藍圖建立、驗證、發佈、分發和使用。除了提供架構概觀之外，本節還會檢閱解決方案的[架構元件](#)和[藍圖生命週期](#)。

當您透過企業藍圖工廠發佈藍圖時，藍圖會成為 [產品AWS Service Catalog](#)。您可以將產品收集到一或多個[產品組合](#)中，然後授予許可，以允許最終使用者存取該產品組合中的產品。您可以使用[產品組合共用](#)，允許另一個的 Service Catalog 管理員 AWS 帳戶 將您的產品分發給最終使用者。

下圖顯示 Enterprise Blueprint Factory 架構的高階概觀。此工作流程會將藍圖發佈為 Service Catalog 中的產品。它也會建立或更新產品組合和產品組合共用，以便將藍圖提供給目標最終使用者。



此圖表顯示下列工作流程：

1. 開發人員會建置藍圖。它們會在產品儲存庫中建立功能分支，將藍圖推送至分支，然後建立提取請求。藍圖管理團隊和安全團隊會檢閱提取請求，以確保藍圖符合組織和安全需求。這些團隊會核准提取請求。開發人員會將功能分支合併到主分支。如需詳細資訊，請參閱本指南中的[產品儲存庫](#)。
2. 開發人員會在位於組態儲存庫的組態檔案中新增或更新藍圖資訊。如需詳細資訊，請參閱本指南中的[組態儲存庫](#)和[組態檔案](#)。
3. 組態檔案的更新會叫用組態管道。此管道使用 [AWS CodePipeline](#)和 [AWS CodeBuild](#)專案來建立或更新 Service Catalog 產品組合和產品組合共用。它也會建立藍圖的發行管道。如需詳細資訊，請參閱本指南中的[組態管道](#)。
4. 發行管道會在藍圖上執行各種安全檢查。如果藍圖通過，發行管道會將藍圖部署為 Service Catalog 中的產品。如需詳細資訊，請參閱本指南中的[發行管道](#)。
5. 透過產品組合和產品組合共用存取產品，最終使用者會在其目標消費者帳戶中部署藍圖。

企業藍圖工廠元件

企業藍圖工廠包含下列元件：

- [產品儲存庫](#) – 您存放藍圖的儲存庫。
- [組態儲存庫](#) – 儲存組態檔案的儲存庫，用於定義 AWS Service Catalog 產品組合和產品。
- [組態檔案](#) - 定義可用的藍圖、誰可以使用它們，以及如何使用它們的組態檔案。
- [組態管道](#) – DevOps CI/CD 管道，可設定 Service Catalog 產品組合和產品組合共用，並為每個產品建立發行管道。
- [發行管道](#) – DevOps CI/CD 管道，將藍圖發行為 Service Catalog 產品。

雲端基礎設施團隊通常會管理整個企業藍圖工廠，因為他們必須核准每個藍圖。不過，DevOps 程式碼團隊通常負責組態管道和發行管道。為了發佈新的藍圖，開發人員只會與產品儲存庫、組態儲存庫和組態檔案互動。

產品儲存庫

產品儲存庫是您存放組織核准藍圖的集中位置。藍圖管理團隊和安全團隊會檢閱對此儲存庫的提取請求，以確保每個藍圖都符合組織和安全需求。在本指南中，我們使用 GitHub 做為儲存庫，但您可以使用替代方法。

組態儲存庫

組態儲存庫（組態儲存庫）是組織存放 Service Catalog 產品組合組態檔案的位置，以及透過 Enterprise Blueprint Factory 發行的產品。在本指南中，我們使用 GitHub 做為儲存庫，但您可以使用替代方法。

組態檔案

企業藍圖工廠組態檔案（組態檔案）存放在組態儲存庫中，該儲存庫由藍圖管理團隊所擁有。此檔案名稱為 bp_config.yml。當開發人員更新此檔案時，藍圖管理團隊會檢閱變更。將變更合併到主分支會啟動組態管道。組態檔案會協調發佈、共用和分發透過企業藍圖工廠管理的所有藍圖。

組態檔案是 YAML 檔案，由兩個主要物件組成：portfolios和 products。以下是範例組態檔案的範例：

```
portfolios:
  - portfolio_name: blueprint-portfolio
    owner: Blueprint-team
    provider_name: AWS
    description: "Blueprint portfolio"
    portfolio_access_role:
      - arn:aws:iam::123456789012:role/examplerole
      - arn:aws:iam::123456789012:user/exampleuser
    share_to_ou:
      - org_id: "o-exampleOrgID"
    stack_tags:
      DataClassification: Confidential
      Organization: AWS
products:
  - name: BP-S3-Product
    description: "Blueprint for BP-S3 product"
    product_config_file: 'BP-S3/product_config.json'
    owner: Blueprint-team
    stack_tags:
      DataClassification: Confidential
      Organization: AWS
    portfolio_associations:
      - blueprint-portfolio
    launch_constraint_role: arn:aws:iam::123456789012:role/examplelaunchrole
```

在 portfolios 物件中，您可以定義目標 Service Catalog 產品組合。對於每個產品組合，您提供下列屬性：

- `portfolio_name` 是產品組合的名稱。此為必要屬性。
- `owner` 是擁有產品組合的團隊名稱。此屬性是選用的。
- `provider_name` 是管理產品組合的團隊或組織的名稱。預設值為 AWS。此為必要屬性。
- `description` 是產品組合的簡短描述。此屬性是選用的。
- `portfolio_access_roles` 是允許存取產品組合及其相關聯產品的 AWS Identity and Access Management (IAM) [身分](#) (使用者、角色或群組)。此屬性是選用的。
- `share_to_ou` 是與產品組合共用[的組織單位](#) AWS Organizations (OU)。最終使用者可以在 AWS 帳戶目標 OU 成員的 中部署此產品組合的產品。此屬性是選用的。
- `stack_tags` 是套用至產品組合的[標籤](#)。此屬性是選用的。

在 `products` 物件中，您會定義要發佈為 Service Catalog 中產品的每個藍圖。對於每個產品，您提供下列屬性：

- `name` 是 Service Catalog 中產品的名稱。此為必要屬性。
- `description` 是產品的簡短描述。此為必要屬性。
- `product_config_file` 是存放在產品儲存庫中的藍圖產品組態檔案的名稱。此為必要屬性。
- `owner` 是擁有產品的團隊名稱。此為必要屬性。
- `stack_tags` 是套用至產品的標籤。此屬性是選用的。
- `portfolio_associations` 是包含產品的目標產品組合。此屬性是選用的。

Note

我們建議您僅將產品新增至透過 Enterprise Blueprint Factory 管理的產品組合。如果您想要將產品新增至非透過企業藍圖工廠管理的產品組合，使用者的 IAM 政策必須允許 [AssociateProductWithPortfolio](#) 動作。不過，根據安全最佳實務，建議您只針對 Enterprise Blueprint Factory 組態管道允許此動作。

- `launch_constraint_role` 是 Service Catalog 在最終使用者啟動產品時擔任的啟動[角色](#)。此為必要屬性。

組態管道

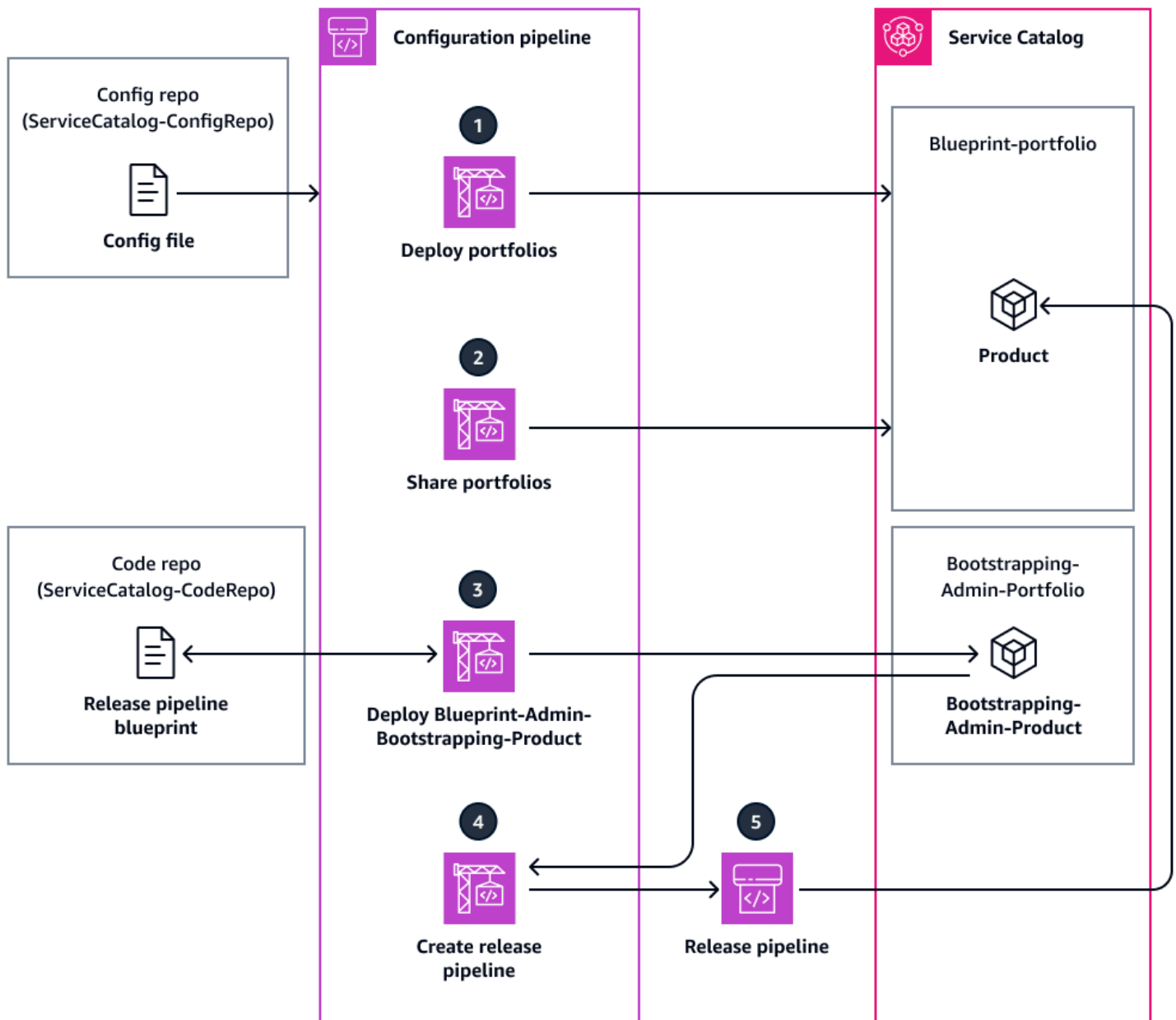
組態管道（組態管道）會自動化 Service Catalog 產品組合和產品組合共用的組態。它也會為每個產品建立發行管道。此管道是 [AWS CodePipeline](#) 資源。組態檔案的更新會叫用組態管道。

第一次叫用組態管道時，它會建立組態檔案中未定義的兩個額外產品組合：

- **Blueprint-portfolio** – 您透過企業藍圖工廠部署的每個產品都會新增至此產品組合。此產品組合可供您在組態檔案中指定的 IAM 主體和組織單位使用。
- **Bootstrapping-Admin-Portfolio** – **Bootstrapping-Admin-Product** 產品與此產品組合相關聯。此產品是發行管道的 CloudFormation 範本。僅允許藍圖管理團隊存取此產品組合，以便他們可以管理管理產品。

組態管道階段

下圖顯示組態管道中的階段，以及管道與之互動的資源。管道中的每個階段都是一個 [AWS CodeBuild](#) 專案。



以下是組態管道的階段：

1. 部署產品組合 – 組態管道會部署任何已新增至組態檔案的產品組合，或刪除已從組態檔案移除的任何產品組合。如果產品組合沒有變更，則管道會略過此階段。
2. 共用產品組合 – 組態管道會與目標組織單位 (OUs) 共用產品組合。如果產品組合共用沒有變更，則管道會略過此階段。
3. 部署Blueprint-Admin-Bootstrapping-Product – 組態管道會從ServiceCatalog-CodeRepo儲存庫擷取bp-pipeline 藍圖，並將其以 的形式部署至 Service CatalogBootstrapping-Admin-

Product。此產品是用來建立發行管道的 CloudFormation 範本。將此範本部署 為 Service Catalog 產品有助於維持版本控制。如果bp-pipeline 藍圖沒有變更，則管道會略過此階段。

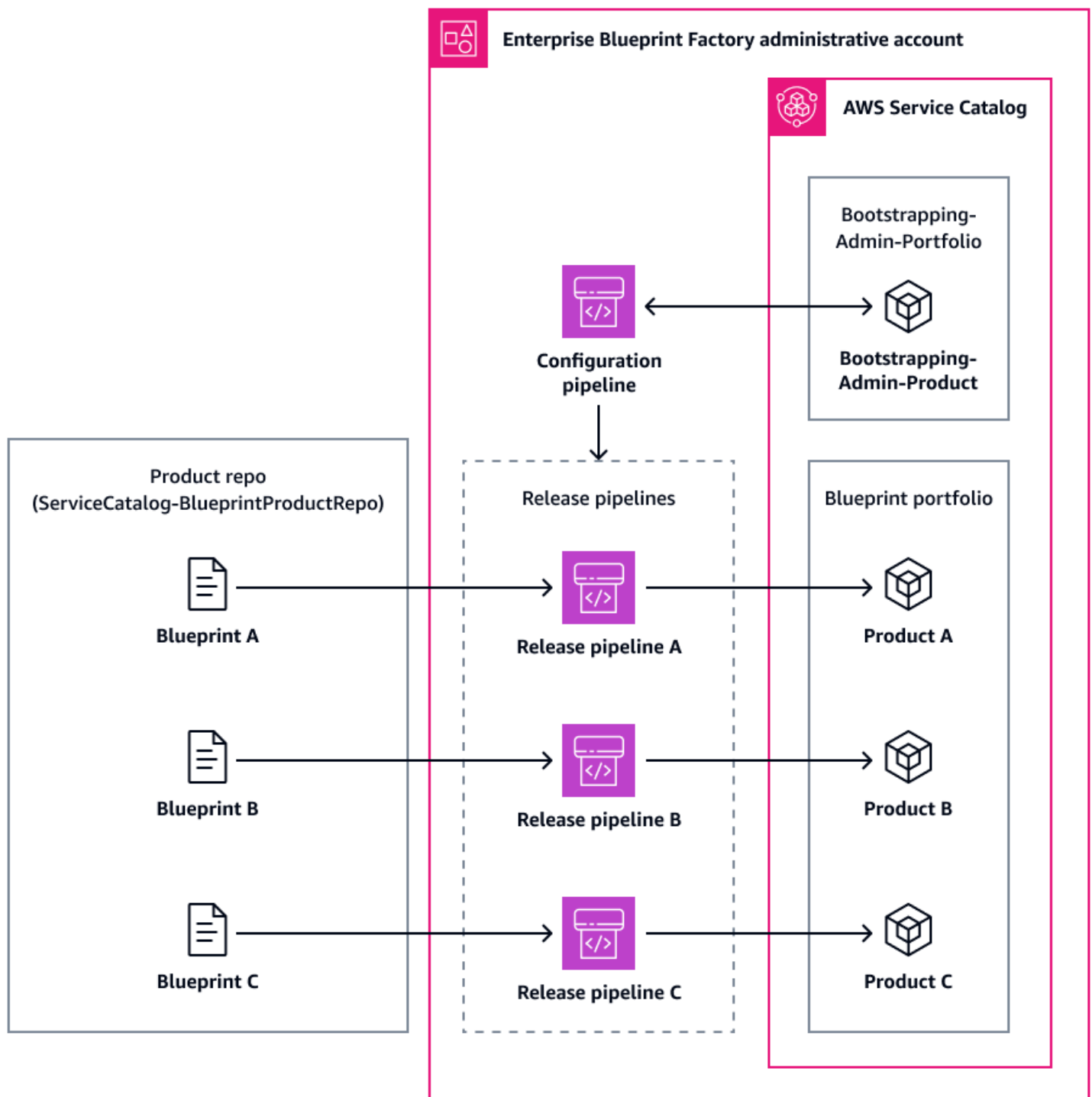
4. 建立發行管道 – 根據組態檔案中的產品屬性，組態管道會準備堆疊參數並啟動 CloudFormation 堆疊，以建立產品的發行管道。如需詳細資訊，請參閱本指南中的[發行管道](#)。
5. 部署產品 – 發行管道會將藍圖部署為 Service Catalog 產品，並將其與目標產品組合建立關聯。最終使用者可以在 中部署 AWS 帳戶 屬於目標 OU 成員的產品。

發行管道

發行管道會將藍圖的發行自動化為 Service Catalog 產品。此管道是 [AWS CodePipeline](#) 資源。當您的組織想要發佈新的藍圖時，開發人員會將 IaC 範本及其產品組態檔案上傳至產品儲存庫。將產品詳細資訊新增至組態檔案會觸發組態管道。組態管道會為此藍圖建立發行管道。藍圖的任何後續更新都會觸發此發行管道，以使用新版本更新 Service Catalog 中的產品。

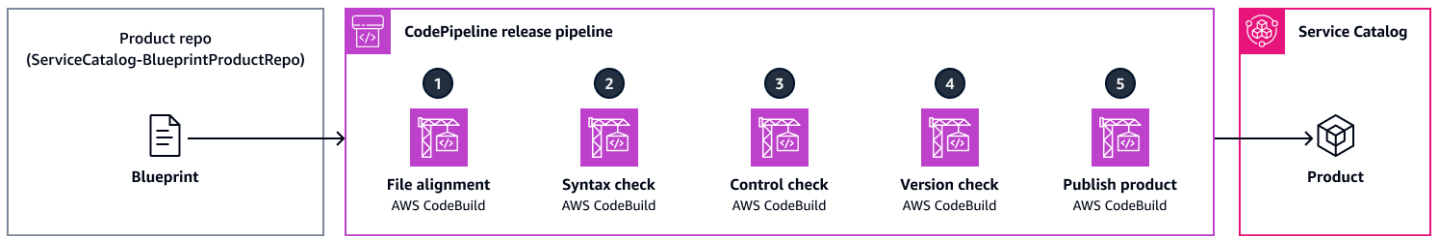
發行管道包含[主動控制](#)，可自動化藍圖的安全與合規檢查。主動控制旨在防止建立不合規的資源。這些控制可以減少其他類型的安全[控制](#)所處理的安全事件數量，例如回應和偵測性控制。由於主動控制可確保部署的資源在部署之前符合規範，因此沒有需要回應或修復的偵測事件。

第一次叫用組態管道時，它會建立名為 的 Service Catalog 產品Bootstrapping-Admin-Product。此產品是發行管道的 CloudFormation 範本。如下圖所示，組態管道使用 Bootstrapping-Admin-Product產品為每個新藍圖建立專用發行管道。藍圖和發行管道之間有 one-to-one的關係。



發行管道階段

下圖顯示發行管道中的預設階段，以及管道與之互動的資源。管道中的每個階段都是 CodeBuild 專案。



以下是發行管道的階段：

1. 檔案對齊 – 此階段會驗證藍圖是 CloudFormation [範本](#) 或 AWS Cloud Development Kit (AWS CDK) [建構](#)。如果藍圖是 AWS CDK 建構模組，此階段會將 AWS CDK 建構模組成為 CloudFormation 範本。此程序會透過 CloudFormation 自動化和標準化部署。如果發現任何錯誤，管道會失敗。
2. 語法檢查 – 語法錯誤是 CloudFormation 部署錯誤的常見原因。在此階段中，[AWS CloudFormation Linter \(cfn-lint\)](#) 會比較範本與 [AWS CloudFormation 資源規格](#)，以檢查語法錯誤。它也會執行其他檢查，例如檢查資源屬性的有效值，以及是否遵守最佳實務。如果發現任何錯誤，管道會失敗，而 cfn-lint 會傳回建議。
3. 控制檢查 – 在此階段中，[cfn_nag](#) 透過搜尋模式來檢查潛在安全問題。例如，它會檢查是否有過度寬鬆的安全群組和 AWS Identity and Access Management (IAM) 政策、缺少加密和密碼常值。如果發現任何錯誤，管道會失敗，而 cfn_nag 會傳回建議。
4. 版本檢查 – 發行管道會根據產品組態檔案中定義的版本策略執行版本控制。如果產品版本定義為 [不可變](#)，Service Catalog 會停用先前的產品版本。
5. 發佈產品 – 發行管道會在 Service Catalog 中發行產品。

Note

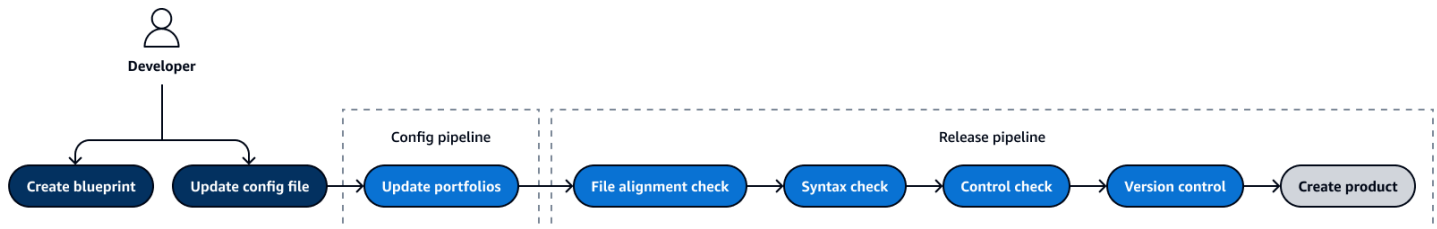
發行管道是可自訂的。例如，您可以移除任何不適用於您的使用案例的階段。如果您想要新增其他控制項檢查、其他驗證或手動核准步驟，也可以新增更多階段。本指南不包含修改發行管道的指示。如需詳細資訊，請參閱 [CodePipeline](#) 和 [CodeBuild](#) 文件。

企業藍圖工廠中的藍圖生命週期

企業藍圖工廠藍圖的生命週期包含三個典型階段：建立、更新和刪除。生命週期階段會影響組態管道和發行管道執行的動作。

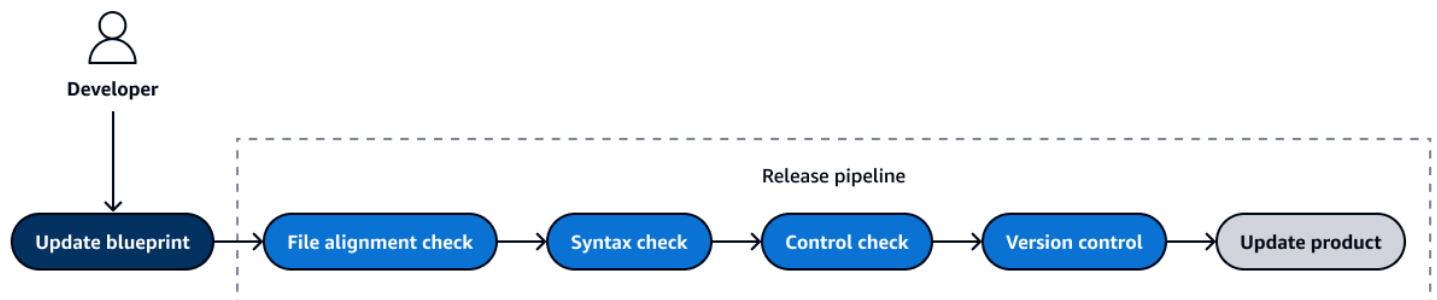
藍圖建立

若要在 中發佈新的藍圖做為產品 AWS Service Catalog，開發人員會將藍圖合併至產品儲存庫、更新組態檔案中的產品組合，並將新產品新增至組態檔案。這會叫用組態管道。組態管道會建立產品的發行管道。在發行管道中，藍圖會進行多次安全檢查。然後，發行管道會將藍圖部署為 Service Catalog 產品。

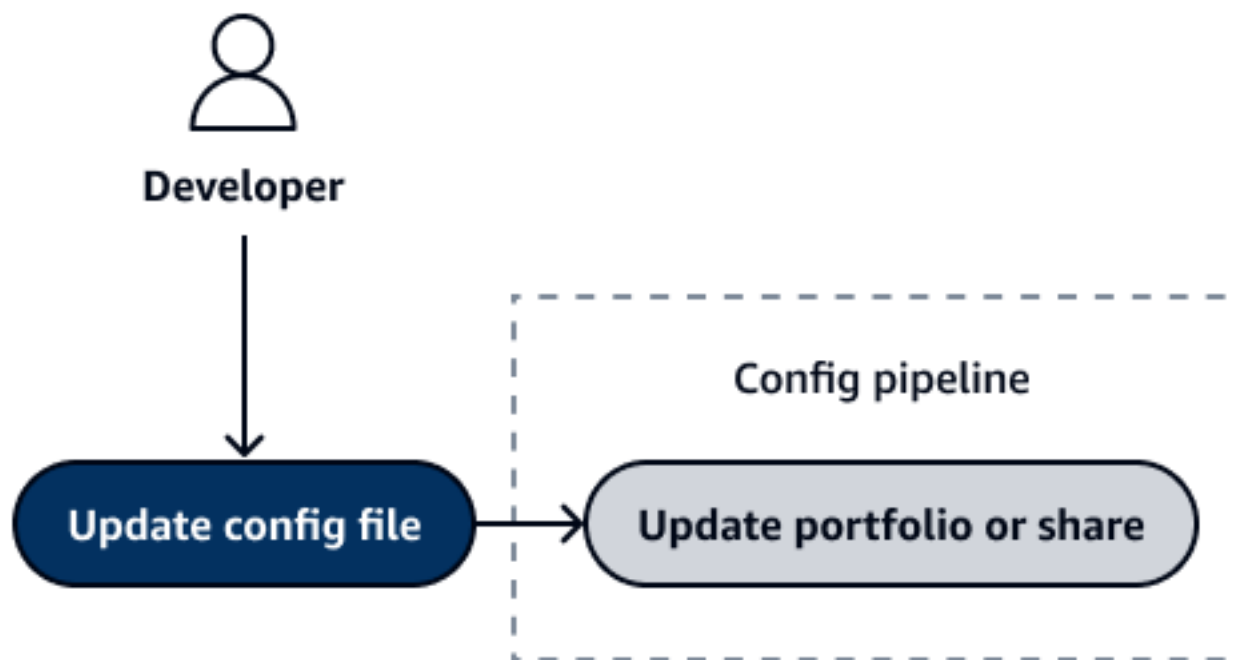


藍圖更新

開發人員可以透過將更新的藍圖版本合併至產品儲存庫來更新 Service Catalog 中的產品。此更新會叫用產品的發行管道。更新後的範本會進行發行管道中的安全檢查。發行管道會部署 Service Catalog 產品的新版本。如需 Service Catalog 如何更新產品版本的詳細資訊，請參閱 Service Catalog 文件中的[管理版本](#)。



或者，您可以更新藍圖相關聯的 Service Catalog 產品組合，也可以變更這些產品組合的共用組態。在這種情況下，開發人員會更新組態儲存庫中的組態檔案。組態管道會更新產品組合或產品組合共用。在這種情況下，Service Catalog 中的產品保持不變，但現在可能會包含在不同的產品組合中。



藍圖刪除

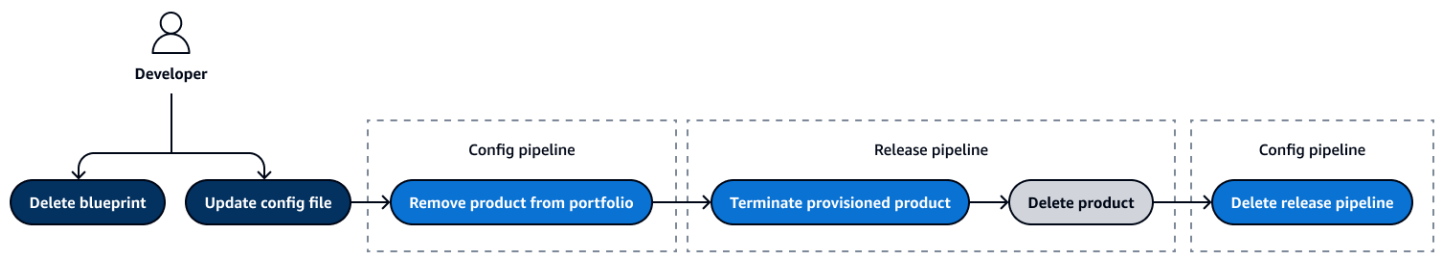
Important

您無法在 Service Catalog 產品遭到刪除後將其復原。不過，您可以將藍圖重新部署為新產品。

當您刪除產品時，Service Catalog 會從包含產品的每個產品組合中移除所有產品版本。如需詳細資訊，請參閱 Service Catalog 文件中的[刪除產品](#)。

若要在 Service Catalog 中部署藍圖之後刪除藍圖，開發人員會刪除產品儲存庫中的藍圖。然後，他們從組態檔中移除產品。組態管道會將產品與包含產品的產品組合取消關聯，並刪除所有產品關聯。發行管道會終止 Service Catalog 產品和[佈建的產品](#)。然後，組態管道會刪除產品的發行管道。

如果組態管道無法取消所有產品資源的關聯，則不會刪除產品，且管道會失敗。您必須解決失敗的資源取消關聯，然後重新啟動管道。如需詳細資訊，請參閱[解決刪除產品時失敗的資源取消關聯](#)。



設定企業藍圖工廠

本節可協助您在 AWS 環境中設定企業藍圖工廠。它包含設定企業藍圖工廠所需儲存庫和資源 AWS 的詳細說明。

先決條件

以下是在您的 AWS 環境中設定企業藍圖工廠的先決條件：

- 下列項目 AWS 帳戶：
 - 用來管理企業藍圖工廠和發行產品的帳戶
 - 一或多個使用已發行產品的帳戶
- 所有帳戶皆為：
 - 在 中以組織身分受管 [AWS Organizations](#)
 - 位於相同的[組織單位 \(OU\)](#)
 - 組織遵循[account-per-tenant模型](#)
- AWS Command Line Interface (AWS CLI) , [已安裝並設定](#)
- 部署可建立下列 AWS 資源之 AWS CloudFormation 堆疊的許可：
 - Amazon CloudWatch Logs 日誌群組
 - AWS CodePipeline 管道
 - AWS CodeBuild 專案
 - Amazon EventBridge 事件匯流排政策和規則
 - AWS Identity and Access Management (IAM) 角色和政策
 - AWS Key Management Service (AWS KMS) 金鑰和金鑰政策
 - AWS Service Catalog 產品組合、產品和佈建產品
 - Amazon Simple Notification Service (Amazon SNS) 主題、主題政策和訂閱
 - Amazon Simple Storage Service (Amazon S3) 儲存貯體
 - AWS Systems Manager 參數存放區參數

如需設定這些許可的詳細資訊，請參閱 [CloudFormation 文件](#)和[實作最低權限許可的政策 AWS CloudFormation](#)。

- [GitHub 帳戶](#)
- 先決條件

最佳實務

建議您在 AWS 環境中設定企業藍圖工廠時，遵循下列最佳實務：

- 設定部署企業藍圖工廠所需的許可時，請遵循最低權限原則，並授予所需的最低許可。如需詳細資訊，請參閱 IAM 文件中的[授予最低權限](#)和[安全最佳實務](#)。
- 設定 Service Catalog 產品組合的存取權時，請遵循最低權限原則，並僅將存取權授予特定角色、使用者或管理員。遵循 Service Catalog [的安全最佳實務](#)。

建立儲存庫

本節可協助您設定 企業藍圖工廠的[組態儲存庫](#)和[產品儲存庫](#)。若要設定儲存庫，您可以在 GitHub 中[放棄](#)提供的儲存庫。然後，您可以使用 建立 GitHub 儲存庫 AWS CodeConnections 的[連線](#)。然後，您將 GitHub 儲存庫複製到本機電腦。

分支 GitHub 儲存庫

1. 登入 [GitHub](#)。
2. 導覽至[組態儲存庫](#) GitHub 儲存庫。
3. 選擇分叉。
4. 在建立新的分支頁面上的儲存庫名稱方塊中，輸入 ServiceCatalog-ConfigRepo。
5. (選用) 輸入描述。
6. 選取僅複製主要分支。
7. 選擇建立分支。
8. 重複這些步驟來分支[程式碼儲存庫](#) GitHub 儲存庫。輸入ServiceCatalog-CodeRepo此儲存庫的名稱。
9. 重複這些步驟來分支[產品儲存庫](#) GitHub 儲存庫。輸入ServiceCatalog-BlueprintProductRepo此儲存庫的名稱。

建立 CodeConnections 連線

1. 在 AWS CLI 中，輸入下列命令來建立與 GitHub 的 CodeConnections 連線：

```
aws codeconnections create-connection --provider-type GitHub --connection-name  
<MyConnection>
```

2. 使用 AWS 開發人員工具主控台來完成連線。如需詳細資訊，請參閱[更新待定連線](#)。

複製分叉儲存庫

- 輸入下列命令，將 GitHub 儲存庫複製到您的本機工作站：

```
git clone git@github.com:<user>/aws-enterprise-blueprint-factory-config-repo
ServiceCatalog-ConfigRepo
git clone git@github.com:<user>/aws-enterprise-blueprint-factory-blueprint-repo
ServiceCatalog-BlueprintProductRepo
git clone git@github.com:<user>/aws-enterprise-blueprint-factory-code-repo
ServiceCatalog-CodeRepo
```

設定企業藍圖工廠

本節中的指示說明如何在目標帳戶中設定企業藍圖工廠。您從 GitHub 複製的產品儲存庫包含兩個範例 CloudFormation 範本，BP-S3 以及 BP-SNS。遵循這些指示，即可將這兩個範例藍圖部署為 Service Catalog 中的產品。

設定角色

1. 在藍圖開發人員的帳戶中，建立下列信任政策，然後將其儲存為 `sc-enduserrole-trust-policy.json`：

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::123456789012:role/ServiceCatalogEndUserRole"
    },
    "Action": "sts:AssumeRole"
  }
}
```

2. 輸入下列命令來建立 IAM `ServiceCatalogEndUserRole` 角色：

```
aws iam create-role \
--role-name ServiceCatalogEndUserRole \
--assume-role-policy-document file://sc-enduserrole-trust-policy.json
```

```
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AWSServiceCatalogEndUserFullAccess \
-- role-name ServiceCatalogEndUserRole
```

Note

開發人員使用 ServiceCatalogEndUserRole 角色來佈建 Service Catalog 產品。此角色不需要許可即可建立藍圖中定義的資源。這遵循最低權限許可和職責分離的最佳實務。

3. 建立下列信任政策，然後將其儲存為 `sc-launchconstraintrole-trust-policy.json`：

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

4. 輸入下列命令來建立 IAM ServiceCataloglogLaunchConstraintRole 角色：

```
aws iam create-role \
--role-name ServiceCataloglogLaunchConstraintRole \
--assume-role-policy-document file://sc-launchconstraintrole-trust-policy.json
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AmazonSNSFullAccess \
--role-name ServiceCataloglogLaunchConstraintRole
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AWSCloudFormationFullAccess \
--role-name ServiceCataloglogLaunchConstraintRole
```

5. 將下列政策新增至 IAM ServiceCataloglogLaunchConstraintRole 角色。如 Service Catalog 文件中的 [設定啟動角色](#) 所述，包含產品資源所需的任何其他許可：

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
```

```

        "s3:GetObject"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "s3:ExistingObjectTag/servicecatalog:provisioning": "true"
        }
      }
    ]
  }
}

```

Note

Service Catalog 使用此角色將 CloudFormation 堆疊部署為 Service Catalog 中的產品。此角色的信任政策可確保只有 Service Catalog 可以擔任該角色。其他使用者或服務無法擔任此角色。這遵循職責分離的最佳實務。

6. 建立下列信任政策，然後將其儲存為 `sc-codebuild-trust-policy.json`：

```

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

```

7. 輸入下列命令來建立 IAM `codebuild-servicecatalog-admin-role` 角色：

```

aws iam create-role \
--role-name codebuild-servicecatalog-admin-role \
--assume-role-policy-document file://sc-codebuild-trust-policy.json
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AWSCodeBuildAdminAccess \
--role-name codebuild-servicecatalog-admin-role

```

Note

組態管道中的 CodeBuild 任務使用此角色。

設定 Amazon S3 儲存貯體

- 若要建立用於存放 CodePipeline 成品的 Amazon Simple Storage Service (Amazon S3) 儲存貯體，請遵循 Amazon S3 文件中[建立儲存貯體](#)的指示。請遵循 [Amazon S3 的安全最佳實務](#)。

設定 AWS Systems Manager 參數

- 請依照 [Systems Manager 中建立參數存放區參數](#) 的指示，在下表中建立 Systems Manager 參數。這些參數用於部署組態管道的 CloudFormation 範本。

參數名稱	Type	描述
/blueprints/resources/vpc_id	字串	存放目標虛擬私有雲端 (VPC) ID 的參數。
/blueprints/resources/subnets	StringList	存放目標子網路 IDs 參數。
/blueprints/resources/securitygroups	StringList	存放目標安全群組 IDs 的參數。
/blueprints/resources/artifacts-bucket-name	字串	存放用於 CodePipeline 成品之 Amazon S3 儲存貯體名稱的參數。
/blueprints/resources/BlueprintRepo	字串	存放儲存企業藍圖工廠藍圖之 GitHub 儲存庫的參數。預設值為 <user>/aws-enterprise-blueprint-factory-blueprint-repo。

參數名稱	Type	描述
/blueprints/resources/CodeRepo	字串	存放 GitHub 儲存庫的參數，用於存放企業藍圖工廠組態管道程式碼和Bootstrapping-Admin-Product 程式碼。預設值為 <user>/aws-enterprise-blueprint-factory-code-repo。
/blueprints/resources/ConfigRepo	字串	存放儲存企業藍圖工廠組態檔案之 GitHub 儲存庫的參數。預設值為 <user>/aws-enterprise-blueprint-factory-config-repo。

更新 CloudFormation 範本

1. 在程式碼儲存庫 (ServiceCatalog-CodeRepo) 中，開啟 ServiceCatalog-Pipeline.yml 檔案。
2. 編輯此檔案中下列參數的預設值：
 - ConfigRepositoryName 是 Systems Manager 參數，存放儲存企業藍圖工廠組態檔案的 GitHub 儲存庫。預設值為 /blueprints/resources/ConfigRepo。
 - CodeRepositoryName 是 Systems Manager 參數，用於存放 GitHub 儲存庫，其中存放 Enterprise Blueprint Factory 組態管道程式碼和Bootstrapping-Admin-Product程式碼。預設值為 /blueprints/resources/CodeRepo。
 - BlueprintRepositoryName 是 Systems Manager 參數，存放儲存企業藍圖工廠藍圖的 GitHub 儲存庫。預設值為 /blueprints/resources/BlueprintRepo。
 - BranchName 是存放組態檔案之組態儲存庫的分支。預設值為 main。
 - VPCID 是 Systems Manager 參數，存放目標 VPC 的 ID。預設值為 /blueprints/resources/vpc_id。

- Subnets 是 Systems Manager 參數，可存放目標子網路IDs。預設值為 /blueprints/resources/subnets。
 - SecurityGroupIds 是 Systems Manager 參數，存放目標安全群組IDs。預設值為 /blueprints/resources/securitygroups。
 - IamRoleName 是 CodeBuild 任務使用的 IAM 角色名稱。預設值為 codebuild-servicecatalog-admin-role。
 - EnvironmentType 是您部署企業藍圖工廠的環境。預設值為 DEV。
 - ArtifactBucket 是 Systems Manager 參數，存放 CodePipeline 存放成品的 Amazon S3 儲存貯體。預設值為 /blueprints/resources/artifacts-bucket-name。
 - CodeConnectionArn 是 CodeConnections 連線至 GitHub 的 Amazon Resource Name (ARN)。
3. 儲存並關閉 ServiceCatalog-Pipeline.yml 檔案。
 4. 輸入下列命令，將變更合併到程式碼儲存庫：

```
cd ServiceCatalog-CodeRepo
git add ServiceCatalog-Pipeline.yml
git commit -m "<description of change>"
git push origin main
```

5. 在組態儲存庫 (ServiceCatalog-ConfigRepo) 中，開啟 bp_config.yml 檔案。
6. 視需要為您的組織更新產品組合區段中的值。例如，更新 portfolio_access_roles 和 share_to_ou 屬性。如需詳細資訊，請參閱本指南中的[組態檔案](#)。
7. 儲存並關閉 bp_config.yml 檔案。
8. 輸入下列命令，將變更合併到程式碼儲存庫：

```
cd ServiceCatalog-ConfigRepo
git add bp_config.yml
git commit -m "<description of change>"
git push origin main
```

部署 CloudFormation 堆疊

1. 登入 Enterprise Blueprint Factory 管理帳戶。
2. 切換到具有[管理許可](#)的 IAM 角色。
3. 開啟 [CloudFormation 主控台](#)。

4. 在畫面頂端的導覽列上，選擇目標 AWS 區域。
5. 在堆疊頁面上，選擇右上角的建立堆疊，然後選擇使用新資源（標準）。
6. 針對 Prepare template (準備範本)，選擇 Template is ready (範本已就緒)。
7. 在指定範本下，選擇上傳範本檔案。
8. 選擇選擇檔案，導覽至 ServiceCatalog-CodeRepo 資料夾，然後選擇 ServiceCatalog-Pipeline.yml。
9. 選擇下一步以繼續並驗證範本。
10. 針對堆疊名稱，輸入堆疊的名稱。
11. 在參數區段中，請勿變更預設值。
12. 選擇下一步。
13. 在設定堆疊選項頁面上，請勿變更預設值，然後選擇下一步。
14. 在檢閱和建立頁面上，驗證範本和堆疊詳細資訊，然後選擇提交。
15. 監控堆疊部署的進度。如需詳細資訊，請參閱 [CloudFormation 文件](#)。
16. 等待狀態變更為 CREATE_COMPLETE。

驗證部署

1. 開啟 [AWS Service Catalog 主控台](#)。
2. 在導覽窗格中，選擇產品。
3. 確認 ServiceCatalog-Pipeline 可在產品清單中使用。
4. 開啟 [AWS CodePipeline 主控台](#)。
5. 在名稱中，選擇組態管道。根據預設，管道名稱為 ServiceCatalog-Pipeline。
6. 選擇 View history (檢視歷程記錄)。
7. 檢視管道和階段執行的狀態。如需狀態的詳細資訊，請參閱 CodePipeline 文件中的 [檢視執行狀態](#)。
8. 等到組態管道狀態為 Succeeded。
9. 開啟 [Service Catalog 主控台](#)。
10. 在導覽窗格中，選擇產品。
11. 確認 BP-S3-Product 和 BP-SNS-Product 產品可用。這表示範例藍圖的產品發行管道已成功完成。
12. 如果您想要刪除在設定企業藍圖工廠時部署的範例藍圖，請遵循 [刪除藍圖](#) 中的指示。

刪除企業藍圖工廠

如果您不是使用企業藍圖工廠，則可以將其刪除，以停止產生與其 AWS 資源相關的成本。

刪除 資源

1. 輸入下列命令來刪除部署在 Enterprise Blueprint Factory 管理帳戶中的 IAM 角色：

```
aws iam detach-role-policy \  
--policy-arn arn:aws:iam::aws:policy/AWSServiceCatalogEndUserFullAccess \  
--role-name ServiceCatalogEndUserRole  
aws iam delete-role --role-name ServiceCatalogEndUserRole  
aws iam detach-role-policy \  
--policy-arn arn:aws:iam::aws:policy/AmazonSNSFullAccess \  
--role-name ServiceCataloglogLaunchConstraintRole  
aws iam delete-role --role-name ServiceCataloglogLaunchConstraintRole
```

2. 刪除企業藍圖工廠的 CloudFormation 堆疊。如需說明，請參閱[從 CloudFormation 主控台刪除堆疊](#)或從 [刪除堆疊 AWS CLI](#)。
3. 刪除用於存放 CodePipeline 成品的 Amazon S3 儲存貯體。如需說明，請參閱 Amazon S3 文件中的[刪除儲存貯體](#)。
4. 從參數存放區刪除下列 Systems Manager 參數：
 - /blueprints/resources/vpc_id
 - /blueprints/resources/subnets
 - /blueprints/resources/securitygroups
 - /blueprints/resources/artifacts-bucket-name
 - /blueprints/resources/BlueprintRepo
 - /blueprints/resources/CodeRepo
 - /blueprints/resources/ConfigRepo

如需說明，請參閱 Systems Manager 文件中的[從參數存放區刪除參數](#)。

使用企業藍圖工廠

本節可協助您在環境中建立、更新或刪除藍圖。它提供在其整個[生命週期](#)中管理藍圖的詳細說明。

若要建立或更新自訂藍圖，您必須了解如何建立 IaC 範本，例如 AWS CloudFormation [範本](#) 或 AWS Cloud Development Kit (AWS CDK) [建構](#)。本指南不包含有關如何定義透過企業藍圖工廠發行之藍圖的資訊或指示。

先決條件

以下是在您的 AWS 環境中使用 Enterprise Blueprint Factory 的先決條件：

- AWS Command Line Interface (AWS CLI)，[已安裝](#)和[設定](#)
- 擔任 ServiceCatalogEndUserRole AWS Identity and Access Management (IAM) 角色的許可
- CloudFormation 範本或 AWS CDK 建構

建立藍圖

企業藍圖工廠管道會部署您在組態檔案中定義的藍圖。開發人員透過將組態檔案合併到組態儲存庫來啟動組態管道。然後，企業藍圖工廠會使用 ServiceCatalogLaunchConstraintRole 將藍圖部署為 Service Catalog 中的產品。如需組態管道和發行管道在建立藍圖時所執行動作的詳細資訊，請參閱本指南中的[藍圖建立](#)。

將藍圖新增至產品儲存庫

1. 請確定您已根據本指南中設定企業藍圖工廠的指示[來設定您的企業藍圖工廠](#)。
2. 確認 ServiceCatalogLaunchConstraintRole 角色的政策可讓您佈建藍圖中定義的資源。
3. 在產品儲存庫 (ServiceCatalog-BlueprintProductRepo) 中，為新藍圖建立資料夾。
4. 將 IaC 範本 AWS CDK (CloudFormation 範本或建構) 貼到您建立的資料夾中。
5. 在您建立的資料夾中建立名為 product_config.json 的檔案。
6. 開啟 product_config.json 檔案，並將以下內容貼到檔案中：

```
{  
  "SchemaVersion": "1.0",
```

```
"ProductVersionName": "1.0.1",
"Deprecated_Versions" : [],
"ProductVersionDescription": "<description>",
"ProductType": "CLOUD_FORMATION_TEMPLATE",
"Properties": {
  "TemplateFilePath": "./<folder name>/<file name>"
}
}
```

其中：

- <description> 是藍圖版本的簡短描述
- <folder name> 是您在產品儲存庫中建立的資料夾名稱
- <file name> 是 IaC 範本的名稱

Note

您可以更新結構描述版本或產品版本名稱，以符合組織的政策。

7. 儲存並關閉 product_config.json 檔案。
8. 輸入下列命令，將變更合併到產品儲存庫：

```
cd ServiceCatalog-BlueprintProductRepo
git add <folder name>/<file name> <folder name>\product_config.json
git commit -m "The first version of <file name> blueprint"
git push origin main
```

更新組態檔案

1. 在組態儲存庫 (ServiceCatalog-ConfigRepo) 中，開啟 config.yml 檔案。
2. 視需要編輯新藍圖的 portfolios 區段和 products 區段。如需詳細資訊，請參閱本指南中的[組態檔案](#)。
3. 儲存並關閉 config.yml 檔案。
4. 輸入下列命令，將變更合併到組態儲存庫：

```
cd ServiceCatalog-ConfigRepo
git add config.yml
```

```
git commit -m "<description of change>"
git push origin main
```

此提取請求的核准會啟動組態管道。組態管道會建立產品的發行管道。

若要檢閱部署日誌

1. 登入企業藍圖工廠管理帳戶。
2. 開啟 [AWS CodePipeline 主控台](#)。
3. 在名稱中，選擇產品的發行管道。根據預設，管道名稱為 Blueprint_<Product-Name>-<CloudFormation-Stack-Name>。
4. 選擇 View history (檢視歷程記錄)。
5. 檢視管道和階段執行的狀態。如需狀態的詳細資訊，請參閱 CodePipeline 文件中的[檢視執行狀態](#)。
6. 如果管道失敗，請檢閱失敗的原因。如需如何設定管道監控的指示，請參閱 CodePipeline 文件中的[監控管道](#)。如果發行管道因為 cfn-lint 或 cfn_nag 檢查而失敗，請更正範本中的錯誤。將另一個提取請求提交至產品儲存庫。這會重新啟動發行管道。如需修正範本錯誤的詳細資訊，請參閱本指南中的[故障診斷](#)一節。
7. 等到發行管道狀態為 Succeeded。

驗證部署

1. 登入組織中的消費者帳戶。
2. 擔任 ServiceCatalogEndUserRole IAM 角色。
3. 開啟 [Service Catalog 主控台](#)。
4. 在導覽窗格中，選擇產品。
5. 確認新產品可在產品清單中取得。

更新藍圖

如需組態管道和發行管道在建立藍圖時所執行動作的詳細資訊，請參閱本指南中的[藍圖更新](#)。

更新藍圖

1. 在產品儲存庫中，導覽至產品的 資料夾。

2. 貼上更新的 IaC 範本。請確定檔案名稱與先前的版本相同。
3. 開啟 product_config.json 檔案。
4. 對於 ProductVersionName，請更新版本編號。
5. 如果您想要防止未來部署先前的產品版本，請在逗號分隔清單中Deprecated_Versions輸入先前的版本號碼。
6. 輸入下列命令，將變更合併到產品儲存庫：

```
cd ServiceCatalog-BlueprintProductRepo
git add <folder name>/<file name> <folder name>\product_config.json
git commit -m "Version <number> of <file name> blueprint"
git push origin main
```

此提取請求的核准會啟動產品的發行管道。

若要檢閱部署日誌

1. 登入企業藍圖工廠管理帳戶。
2. 開啟 [AWS CodePipeline 主控台](#)。
3. 在名稱中，選擇發行管道。根據預設，管道名稱為 BluePrint_<Product-Name>-<CloudFormation-Stack-Name>。
4. 選擇 View history (檢視歷程記錄)。
5. 檢視管道和階段執行的狀態。如需狀態的詳細資訊，請參閱 CodePipeline 文件中的[檢視執行狀態](#)。
6. 如果管道失敗，請檢閱失敗的原因。如需如何設定管道監控的指示，請參閱 CodePipeline 文件中的[監控管道](#)。如果發行管道因為 cfn-lint 或 cfn_nag 檢查而失敗，請更正範本中的錯誤。將另一個提取請求提交至產品儲存庫。這會重新啟動發行管道。如需修正範本錯誤的詳細資訊，請參閱本指南中的[故障診斷](#)一節。
7. 等到發行管道狀態為 Succeeded。

驗證更新

1. 登入組織中的消費者帳戶。
2. 擔任 ServiceCatalogEndUserRole IAM 角色。
3. 開啟 [Service Catalog 主控台](#)。

4. 在導覽窗格中，選擇產品。
5. 確認新的產品版本可在產品清單中取得。

刪除藍圖

當您刪除產品時，Service Catalog 會從包含產品的每個產品組合中移除所有產品版本。如需詳細資訊，請參閱 Service Catalog 文件中的[刪除產品](#)。如需組態管道和發行管道在建立藍圖時所執行動作的詳細資訊，請參閱本指南中的[藍圖刪除](#)。

刪除藍圖

1. 在組態儲存庫中，開啟 config.yml 檔案。
2. 編輯產品區段，移除或評論您要刪除的產品。
3. 儲存並關閉 config.yml 檔案。
4. 輸入下列命令，將變更合併到組態儲存庫：

```
cd ServiceCatalog-ConfigRepo
git add config.yml
git commit -m "<description of change>"
git push origin main
```

此提取請求的核准會啟動組態管道。組態管道會刪除產品及其發行管道。

5. 在產品儲存庫中，刪除產品的資料夾，包括其內容。
6. 輸入下列命令，將變更合併到產品儲存庫：

```
cd ServiceCatalog-BlueprintProductRepo
git add .
git commit -m "Delete <file name> blueprint"
git push origin main
```

驗證刪除

1. 登入組織中的消費者帳戶。
2. 擔任 ServiceCatalogEndUserRole IAM 角色。
3. 開啟 [Service Catalog 主控台](#)。
4. 在導覽窗格中，選擇產品。

5. 確認已刪除的產品不再可用。

故障診斷

當您建立或更新藍圖時，cfn-lint 和 cfn-nag 工具會驗證藍圖。如需發行管道中驗證的詳細資訊，請參閱本指南中的[發行管道](#)。任何報告的語法或安全錯誤都會導致管道失敗。若要透過發行管道成功部署藍圖，您必須更正藍圖中的錯誤。

以下是顯示兩個安全相關錯誤的範例輸出：失敗和警告。

```
BP-SNS.yml
-----
BP-SNS.yml
-----
| WARN W47
|
| Resource: ["ExampleTopic"]
| Line numbers: [5]
|
| SNS Topic should specify KmsMasterKeyId property
-----
| FAIL F18
|
| Resource: ["ExampleTopicPolicy"]
| Line numbers: [10]
|
| SNS topic policy should not allow * principal

Failures count: 1
Warnings count: 1
```

若要更正這些錯誤，請在藍圖檔案中取代 Amazon Simple Notification Service (Amazon SNS) 主題政策中的 *主體，並將 AWS Key Management Service (AWS KMS) 金鑰與主題建立關聯。下列程式碼範例示範這些更新。

```
ExampleTopic:
  Type: AWS::SNS::Topic
  Properties:
    TopicName: ExampleTopic
ExampleTopicPolicy:
  Type: AWS::SNS::TopicPolicy
```

Properties:

KmsMasterKeyId: alias/aws/sns # Added KMS key

PolicyDocument:

Id: Id1

Version: '2012-10-17'

Statement:

- Sid: Sid2

Effect: Allow

Principal:

"Service" : "s3.amazonaws.com" # Replaced "AWS": '*'

Action: 'sns:Publish'

Resource: !Ref ExampleTopic

Topics:

- !Ref ExampleTopic

相關資源

AWS 文件

- [教學課程：建立部署至 Service Catalog 的管道](#) (AWS CodePipeline 文件)
- [AWS CodePipeline 文件](#)
- [AWS CodeBuild 文件](#)
- [AWS Service Catalog 管理員指南](#)
- [AWS Service Catalog 使用者指南](#)

AWS 部落格文章

- [報告和視覺化 AWS Service Catalog 您的 Estate](#) (AWS 部落格文章)
- [實作警示以自動偵測堆疊中的 AWS CloudFormation 偏離](#) (AWS 部落格文章)

貢獻者

下列個人對本指南有所貢獻。

編寫

- Haofei Feng，資深雲端架構師，AWS
- Cam Maxwell，首席安全顧問，AWS
- Joe Guo，雲端支援工程師，AWS
- Shreejesh MV，資深雲端架構師，AWS

檢閱

- Joseph Dominic，雲端架構師，AWS
- Naresh Rajaram，諮詢合作夥伴解決方案架構師，AWS

技術寫入

- 資深技術作者，Lilly AbouHarb AWS

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	—	2024 年 10 月 10 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、持久性](#)。

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](#)。

AI Ops

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 and 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，以管理組織的帳戶和管理該服務的許可。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 延伸了原本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中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)

在組織之間自動交換商業文件。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邊界會限制故障的影響，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[機器學習模型可解釋性 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，少量的提示非常有效。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，以及以自然語言交談。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，以及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。

|

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

[Klaus 於](#) 2016 年引進的術語，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 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釋性 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、特洛伊木馬程式、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，請參閱本詞彙表中的 [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[不可變的基礎設施](#)作為最佳實務。

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[開啟程序通訊 - 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)

問題及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。

設計隱私權

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[擷取增強生成](#)。

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 Rs](#)。

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)

服務中斷和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。

重新放置

請參閱 [7 Rs](#)。

Replatform

請參閱 [7 Rs](#)。

回購

請參閱 [7 Rs](#)。

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

定義所有涉及遷移活動和雲端操作之各方的角色和責任的矩陣。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 Rs](#)。

淘汰

請參閱 [7 個 R](#)。

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。此功能可啟用聯合單一登入 (SSO)，讓使用者可以登入 AWS Management Console 或呼叫 AWS API 操作，而無需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 and 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。