



適用於 SAP on AWS 綠地實作的最佳實務

# AWS 方案指引



# AWS 方案指引: 適用於 SAP on AWS 綠地實作的最佳實務

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

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

# Table of Contents

簡介 .....	1
概觀 .....	2
目標對象 .....	2
規劃階段的最佳實務 .....	3
建置 RACI 矩陣 .....	3
檢閱 SoW .....	4
建立團隊組織結構圖和聯絡人清單 .....	5
與內部雲端團隊一起建立參與模型 .....	5
記錄雲端建置和部署程序 .....	7
專案藍圖和里程碑追蹤器 .....	7
設計階段的最佳實務 .....	11
建立交付時間表和景觀圖 .....	11
了解區域服務和文件決策 .....	12
建立命名慣例 .....	13
記錄所有決策 .....	13
建置階段的最佳實務 .....	15
主持每日站立會議 .....	15
使用統一的建置規格表 .....	15
請注意 AWS 服務配額 .....	16
制定安全金鑰輪換策略 .....	16
停用未使用的伺服器 .....	17
資源 .....	18
文件歷史紀錄 .....	19
詞彙表 .....	20
# .....	20
A .....	20
B .....	23
C .....	24
D .....	27
E .....	30
F .....	32
G .....	33
H .....	34
I .....	35

---

L .....	37
M .....	38
O .....	42
P .....	44
Q .....	46
R .....	46
S .....	49
T .....	52
U .....	53
V .....	54
W .....	54
Z .....	55
.....	lvi

# SAP on AWS greenfield 實作的最佳實務

Almaz Thornton、Johnny Frye 和 Raveendra Voore , Amazon Web Services (AWS)

2024 年 7 月 ([文件歷史記錄](#))

綠地 SAP 實作通常是大規模業務轉型專案的一部分，其中包括 SAP 企業資源規劃 (ERP) 應用程式的新安裝。Amazon Web Services (AWS) 上的 Greenfield SAP 實作與 AWS 遷移上的 SAP 不同，因為內部部署或雲端中沒有要遷移的現有伺服器足跡，而是調整新伺服器的大小和佈建。此外，綠地專案在技術和功能上往往具有更廣泛的範圍。由於綠地實作不如遷移常見，因此通常很難找到這些專案的指南。

本指南針對參與綠地 SAP 實作的 IT 領導者和專案經理提供建議和最佳實務。這些準則也與 SAP 遷移專案相關，可協助您避免在管理遷移或綠地實作時遇到的問題。這些準則分為三個章節，以遷移或實作專案的三個主要階段為基礎：

- [規劃階段](#) – 初步規劃、建立團隊、需求收集
- [設計階段](#) – 將需求轉化為架構圖、構建規範以及設計文檔
- [建置階段](#) – 開發、設定和測試綠地 SAP 實作

本指南假設您擁有 AWS 和 SAP 服務的 100 級知識、對 IT 專案管理的高度熟悉，以及對[遷移 AWS 方法](#)和[遷移 SAP AWS HANA 模式的 SAP](#) 的認識。

## 概觀

本文件重點介紹了在 SAP on AWS 的綠地實作過程中吸取的經驗教訓。這些建議大多也可以套用至 AWS 遷移專案上的標準 SAP。本文分享了有關專案規劃、設計和建置階段的建議。它包括有關專案維護或操作階段的課程，但該階段並不是本指南的重點。您可以使用瀑布方法，或者反覆式、靈活或混合方法來套用這些最佳實務。

以下是本指南中引用的基礎架構團隊的主要利益相關者：

- AWS 實作合作夥伴 – 這可能是 AWS 專業服務或 AWS 合作夥伴。其角色是建置 SAP 應用程式將在其中執行的 AWS 基礎設施。
- SAP Basis 團隊 – 此團隊可由系統整合商 (SI) 或廠商公司提供，由您組織內部的員工或混合人員組成。他們的工作是安裝 SAP 軟體，在技術層面對其進行設定，升級並經常進行維護。
- SI 基礎設施負責人 – 此人是產品所有者。他們提供來自更大專案團隊的技術要求，並為基礎設施團隊提供總體領導。
- 客戶基礎設施負責人 – 此人也是產品所有者。他們提供來自更大專案團隊的技術要求，並為基礎設施團隊提供總體領導。SI 和客戶基礎設施負責人可以在聯合領導模式中平等運作，或者您可決定指派單一基礎設施負責人。

此規範性指引的重點，特別著重於綠地 SAP 專案的 AWS 層面。

在上部署 SAP 環境時 AWS，基礎設施團隊通常比正在設定和自訂 SAP 以滿足業務需求的職能和開發團隊提前幾個月。由於兩個團隊的交付時間表不同，因此基礎設施團隊的建置階段可能是功能團隊的規劃階段。此外，建置 SAP 環境的工作非常反覆和重複。例如，在 N+2 方案中，您可能會建置三種不同的開發環境。視您建構專案的方式以及何時需要環境而定，除非環境都在同一日期到期，否則可能會有三個建置階段。將本指引套用到專案的特定階段時，請記住這些差異，以便您可以更有效地與功能團隊和開發團隊進行溝通和合作。

## 目標對象

本文件的撰寫考量為專案經理、做為專案實作的指南，以及做為在 SAP AWS 實作期間設定期望並提供強大 IT 領導的工具。在大規模 SAP 實作中，基礎架構團隊的所有成員很可能會與自己的專案經理一起參與，以管理他們的工作。建議您找出單一、首要的基礎架構專案經理，以管理整體雲端之旅，並負責確保遵循這些最佳實務。

## 規劃階段的最佳實務

在綠地 SAP 實作的規劃階段，專案通常會遇到各種挑戰和機會。本節討論以 SAP 為基礎的五個關鍵學習，了解 AWS 專業服務團隊已參與的 AWS 綠地實作。甚至可以在專案開始或諮詢團隊參與之前實作其中一些建議。提供文件草稿，例如角色和職責矩陣或團隊聯絡人清單，有助於加速提升程序。

## 建置 RACI 矩陣

為基礎設施團隊建置責任指派矩陣對於任何實作專案來說都很重要。該矩陣採用綜合負責者、當責者、事先諮詢者和事後告知者 (RACI) 圖表的形式。RACI 用於闡明複雜團隊結構中的角色、工作分派和任務。它應該與 AWS SAP Cloud 團隊、SAP Basis 團隊、SAP 系統整合商 (SI) 和客戶合作開發。這可以由這些群組中的任何一個或由專案經理驅動。在沒有這些利益相關者參與的情況下建置 RACI 會產生矛盾和分歧，有時甚至是衝突。考慮專案的所有階段至關重要。提前設立 RACI 可加強所有參與方之間的合作夥伴關係，並提高透明度。理想情況下，RACI 應在專案啟動前完成。

以下是綠地 SAP 實作專案的範例 RACI 矩陣摘錄。

---

[下載完整的 RACI 矩陣](#)

Topic: Program Governance	SAP Basis	AWS Professional Services or AWS Partner	SAP Systems Integrator	Customer
AWS project management and governance	I	R	I	A
SAP AWS team staffing	C	R	C	A
Onboarding	I	I	I	RA
Access	I	I	I	RA
Engagement security	-	RA	-	I
Collaboration tools - access	I	I	I	RA
Financials	-	R	-	A
Status reporting	I	RA	I	I
Program reporting	C	R	C	A
Advisory of AWS services for SAP throughout project phase	I	R	C	A
Topic: AWS Platform and Architecture				
Architecture of target AWS SAP environment, including HA/DR capabilities	I	R	C	A
Design of backup/restore strategies on AWS infrastructure	I	R	C	A
Provide host names and ports for SAP	R	C	I	A
Open firewall	C	I	I	R
AWS infrastructure design per SAP sizing requirements provided by Basis	C	R	C	A
Automating and provisioning of AWS infrastructure	I	R	C	A
Post-infrastructure build steps (e.g., request domain join)	I	R	I	A
Review of AWS infrastructure security	I	R	I	A
AWS infrastructure issues resolution before system handover to Basis	I	R	I	A
Project team infrastructure support, Level 1 (project team always goes through Basis; no direct contact to AWS)	R	C	I	A
AWS support ticket (involves TAM)	C	R	I	A
Identify HA relevant SAP application	C	I	R	A
AWS go-live check, including SAP AWS requirements - infrastructure	I	C	R	A
SAP cutover to production	I	C	R	A

## 檢閱 SoW

了解 AWS 諮詢和顧問服務的工作陳述式 (SoW) 的所有元素，並與主要利益相關者共同檢閱 SoW，以便所有人清楚地了解交付項目。如果基礎設施團隊打算執行超過 SoW 定義的作業，請務必在風險、假設、動作、問題、相依性和決策 (RAAIDD) 日誌中記錄。在綠地 SAP 實作專案中，保持靈活和敏捷至關重要，因此偏離 SoW 是常見的案例。不過，如果 AWS 實作合作夥伴開始交付超出記錄的內容，預期可能會變得模糊。發生變更時，應保留新工作範圍以及可能必須進行權衡的執行清單。對於瀑布式專案方法，必須定義和實作範圍變更管理程序。對於敏捷專案，積壓工作優先級排序程序更適合管理範圍。

考量：

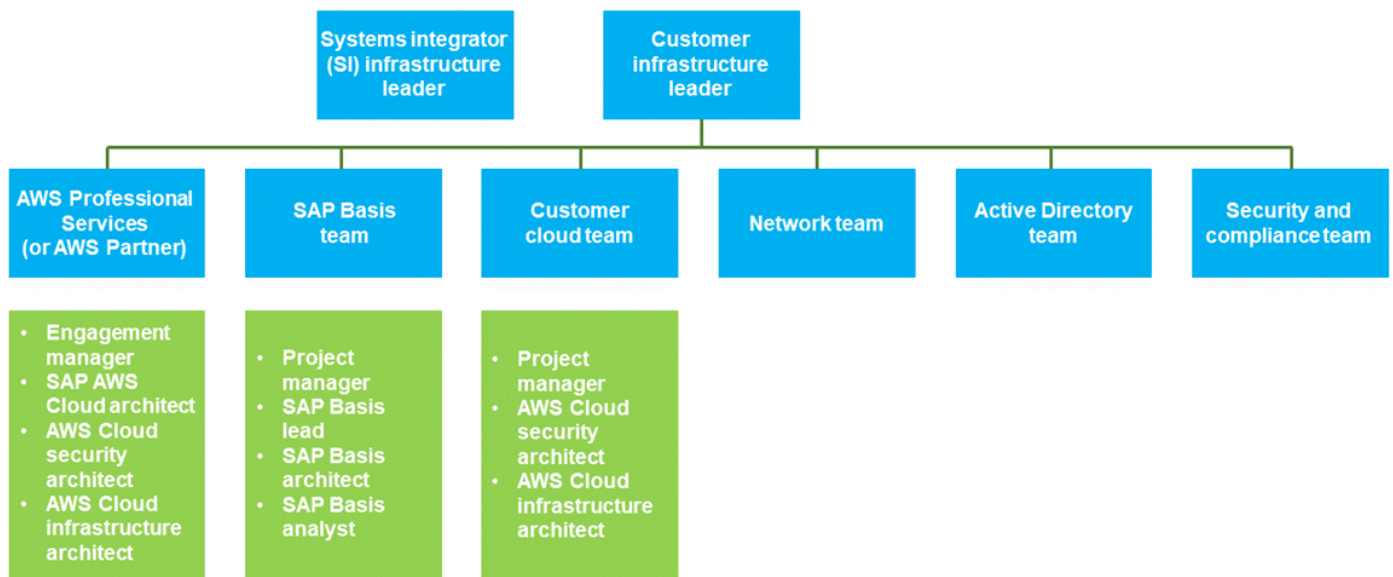
- 隨著專案的進展，請務必擷取新範圍並定義任何新的可交付成果。這將協助您管理期望，並在確定積壓工作的優先級時尋求協助。

- 識別文件變更和任務以及現有的交付積壓，並確定其優先順序，以便可在專案的整個生命週期內生成文件，而不是延遲到結束。
- 在整個專案中定期進行 SoW 演練，以與交付項目和優先順序保持一致。
- 對於生產切換，請務必至少提前 12 個月核准具有唯讀存取權的 SoW，以協助 Hypercare 支援。

## 建立團隊組織結構圖和聯絡人清單

構建可描繪團隊和領導結構的高層級組織結構圖。開發跨團隊聯絡人清單進行更深入的了解，它包括基礎設施團隊中每個人的姓名、職稱和角色，以及各種功能的關鍵聯絡點，例如安全性、網路和防火牆操作、Microsoft Active Directory、內部雲端操作和伺服器操作。每個人都應該知道專案的參與者是誰以及他們扮演的角色。當團隊沒有掌握此資訊時，不可避免地會發生延遲和溝通不當。了解利益相關者的頭銜也很重要。例如，您不希望邀請董事級別的利益相關者參加設計會議或每日站立會議，除非他們是討論的主要貢獻者。了解頭銜和角色可讓您邀請合適的人員參加相關會議。能夠在組織結構圖中可視化團隊可以協助您了解團隊的結構以及在專案中的合作方式。

下圖提供 AWS 基礎設施組織圖表上典型 SAP 的範例。



## 與內部雲端團隊一起建立參與模型

如果您的 IT 組織有內部 AWS 雲端團隊，您應該與該團隊建立互動模式，並釐清他們將執行的工作，與 AWS 實作合作夥伴（例如 AWS，專業服務或 AWS 合作夥伴）的任務相比。需要考慮的一個關鍵責任是在建置和移交環境之後的支援情況。例如，如果只有兩位 SAP 雲端架構師正在為數十個 AWS SAP 應用程式建置多景觀和多環境基礎設施，則他們沒有頻寬來支援同時完成建置和建置新環境

的環境。一種選擇是請求內部雲端團隊接管已完成環境的支援。這使內部團隊有機會學習並獲得環境的所有權。當專案有所進展並確定新的工作範圍時，他們最終將負責維護和擴展這些環境。

內部雲端基礎設施和雲端 DevOps 團隊也應該同意要使用的自動化軟體類型，例如，是否使用 AWS CloudFormation 或 Terraform 做為基礎設施做為程式碼 (IaC) 工具。同樣地，他們可能會決定將 AWS Systems Manager 或 Ansible 用於組態任務，例如引導磁碟區和可能的 SAP 安裝。這些決定應記錄在案。此外，如果需要第三方監控和可觀測性儀表板，但這不是 SoW 中的可交付項目，請考慮在此期間使用 Amazon CloudWatch 和 Amazon Simple Notification Service (Amazon SNS) 放置監控和記錄掛鉤。內部雲端團隊可以在以後使用第三方監控解決方案進行整合。

參與模型或支援協議也應該是 RACI 矩陣的一部分，並在 SoW 中表達。使用 AWS 服務可以實現顯著程度的自動化。SoW 和 RACI 矩陣應識別在綠地 SAP 實作專案中需要達成的項目，以及可委派給營運團隊的項目。

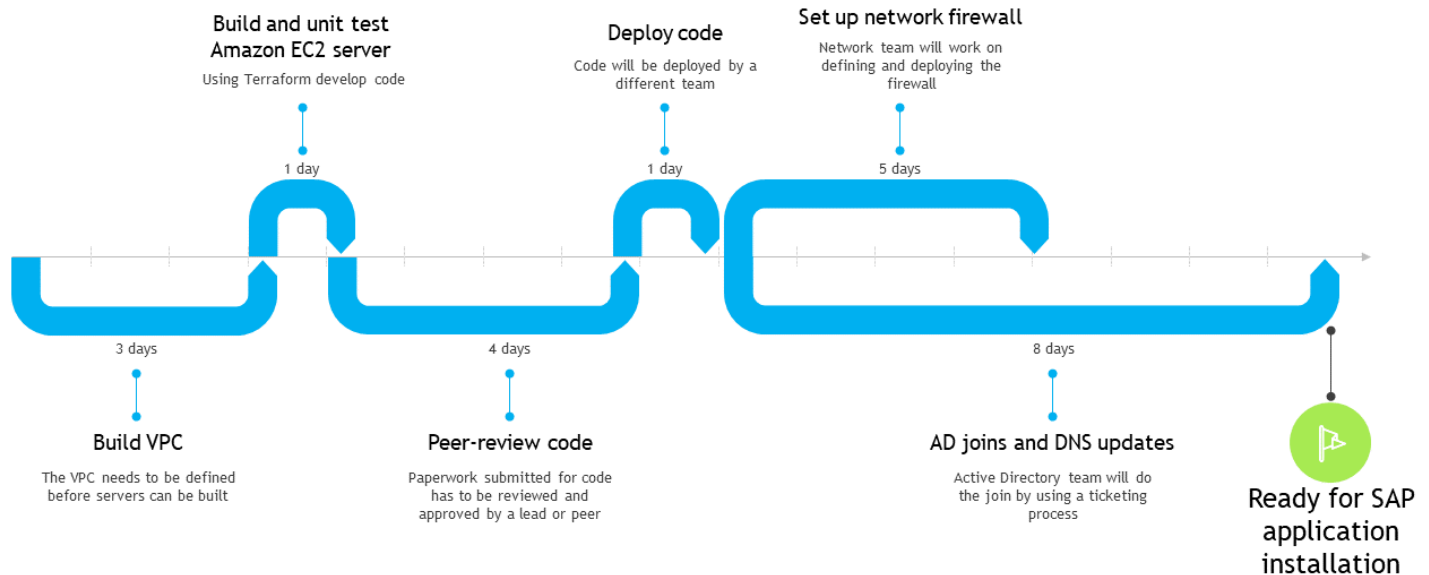
當您建立參與模型時，請判斷瀑布式、敏捷式或混合式方法是否會是向前邁進的關鍵方法。AWS 與瀑布式方法相比，專業服務觀察到任務完成增加 300%，並在實作敏捷式或混合式方法的參與中縮短 94% 的規劃時間。在規劃階段，您也應該在客戶的協助下，選取溝通計畫和工具方法。下表顯示通訊計畫範例。

Communication plan					
Meeting	Duration	Frequency	Notes	Deliverables	Stakeholders
Scrum meetings (for each worksteam)	15–30 minutes	Daily or twice weekly	Daily: Monday – Friday Twice weekly: Monday, Thursday	<ul style="list-style-type: none"> <li>What did I do yesterday to advance the sprint goal?</li> <li>What will I do today to advance the sprint goal?</li> <li>Are there any impediments that will prevent us from meeting the sprint goal?</li> </ul>	All project team members are invited
Internal scrum meeting	15–30 minutes	Weekly	Tuesday	<ul style="list-style-type: none"> <li>Like scrum but internal only</li> </ul>	Internal scrum team
Sprint review and retrospective	1.5 hours	Every 3 weeks on Fridays	Fridays at 9:00 AM PST	<ul style="list-style-type: none"> <li>Review sprint goals.</li> <li>Demo and solicit feedback for each story.</li> <li>Discuss stories not completed and identify the blockers.</li> <li>Identify risks and impediments. Revise team backlog.</li> </ul>	All project team members are invited
Sprint planning and backlog grooming	1.0 hours	Every 3 weeks on Mondays after review	Mondays at 1:00PM PST		All project team members are invited
Leadership status meeting	30 minutes	Weekly	Thursdays at 1:00PM PST	<ul style="list-style-type: none"> <li>Meet with customer champion</li> </ul>	EM/customer champion
Internal account team and AWS Professional Services calls	30 minutes	Bi-weekly	Fridays at 1:00PM PST	<ul style="list-style-type: none"> <li>CSM to make agenda or team members to bring agenda items/concerns</li> </ul>	Account team and AWS Professional Services team
External account team, AWS Professional Services, and customer	1 hour	Bi-weekly	Dependent on customer	<ul style="list-style-type: none"> <li>Discuss budget, issues, accomplishment, goals.</li> </ul>	Account team, AWS Professional Services team, customer leadership
Quarterly business review	1–2 hours	Quarterly	Dependent on customer	<ul style="list-style-type: none"> <li>Discuss high-level accomplishments and milestones</li> </ul>	Account team, AWS Professional Services team, customer executive leadership

最後，請務必識別將及早支援專案的客戶和 SAP Basis 團隊。在您實作和遷移新解決方案時對其進行訓練，是儘早開始知識轉移工作階段的關鍵。

## 記錄雲端建置和部署程序

如果您的 IT 組織擁有內部雲端團隊，該團隊應該使用程序流程圖來記錄雲端建置和部署程序，並與整個團隊共用這些圖表。您希望主要利益相關者能夠輕鬆發現程序中的任何瓶頸或低效，並了解現有內部程序在造成低效或延遲方面所起的作用。在下列範例中，您可以看到 Active Directory 加入和網域名稱系統 (DNS) 更新程序如何花費最長的時間才能完成。這種視覺效果可能會激勵團隊進行協作，並想辦法減少該程序步驟中涉及的時間。

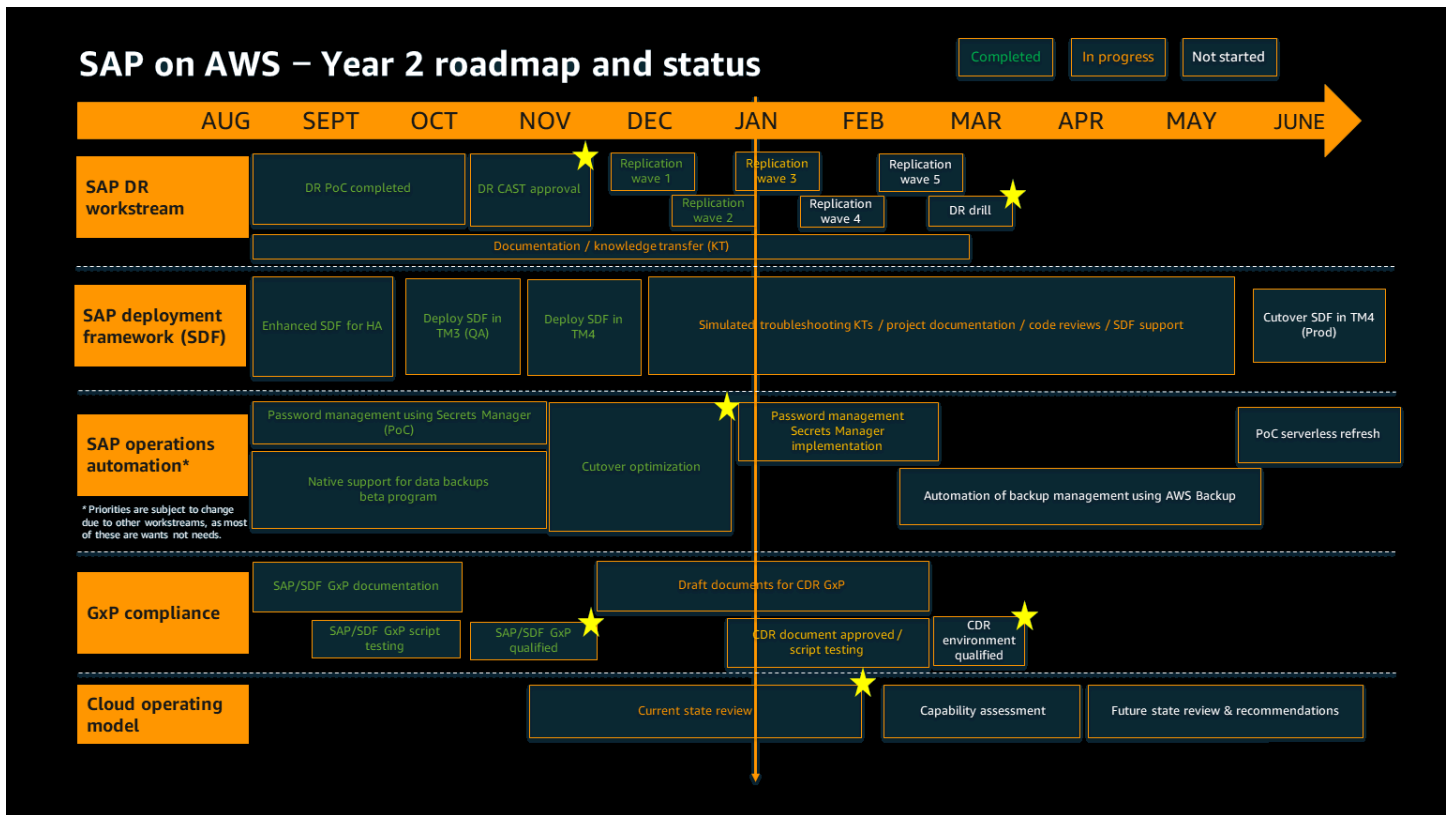
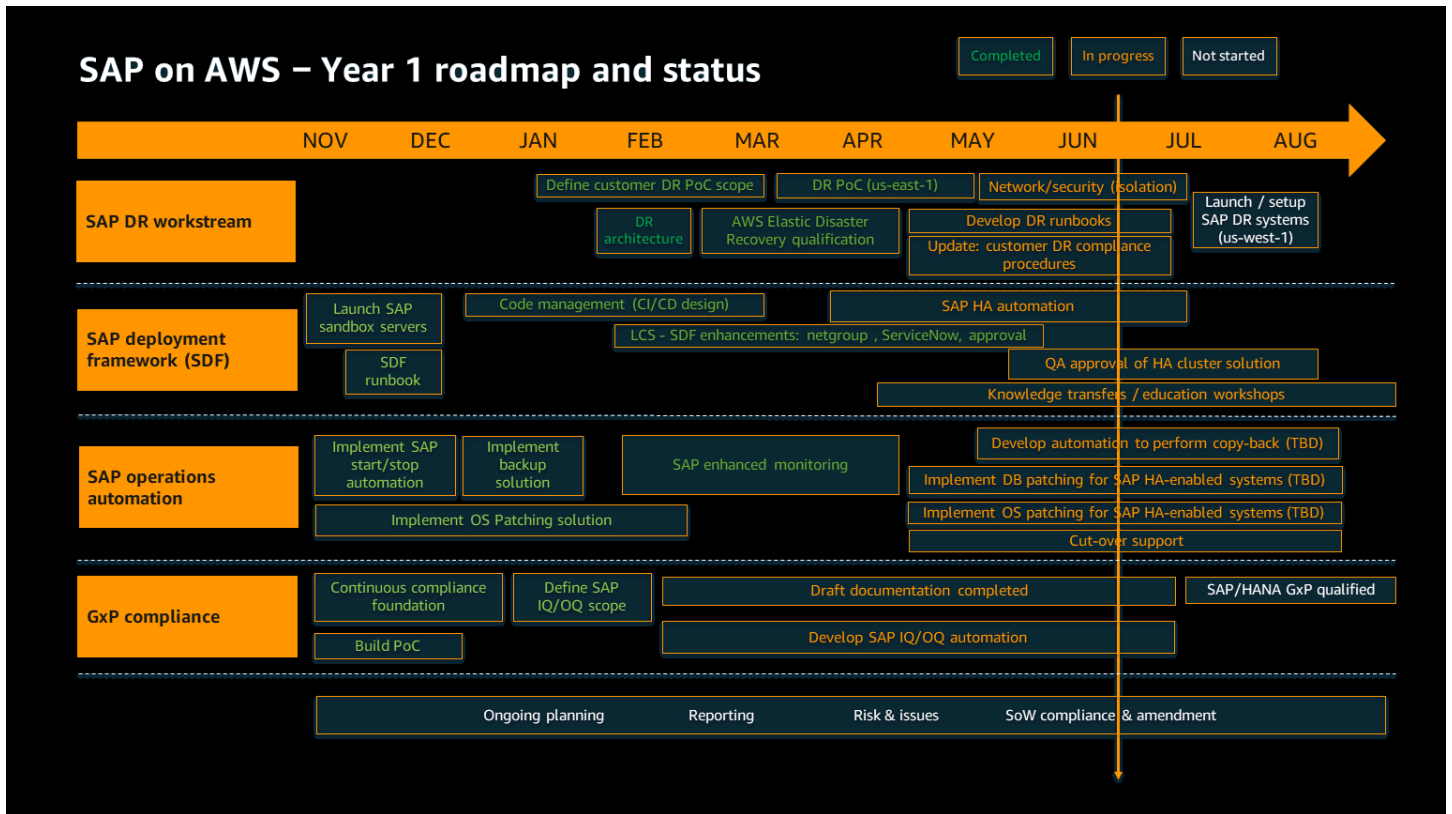


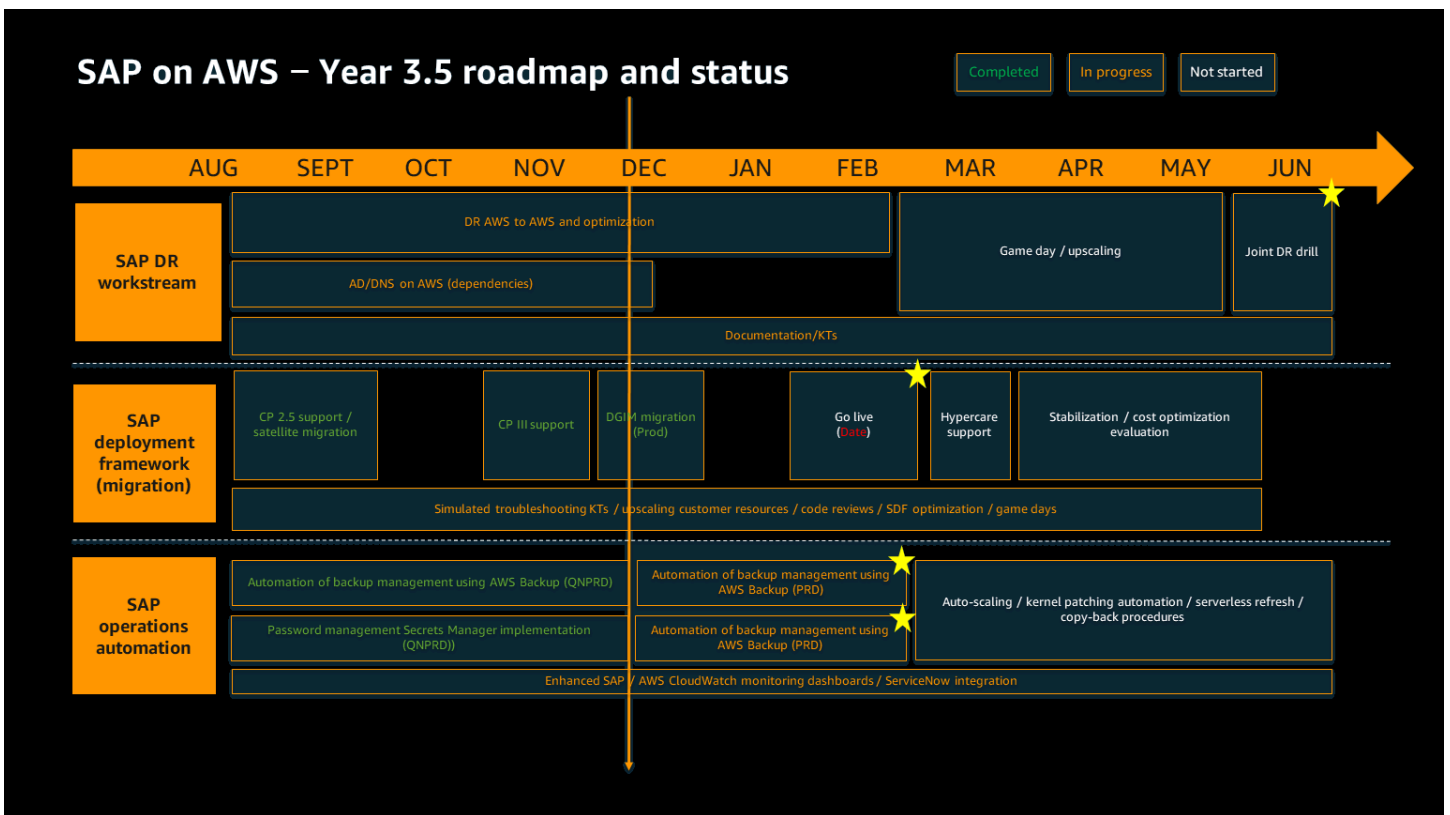
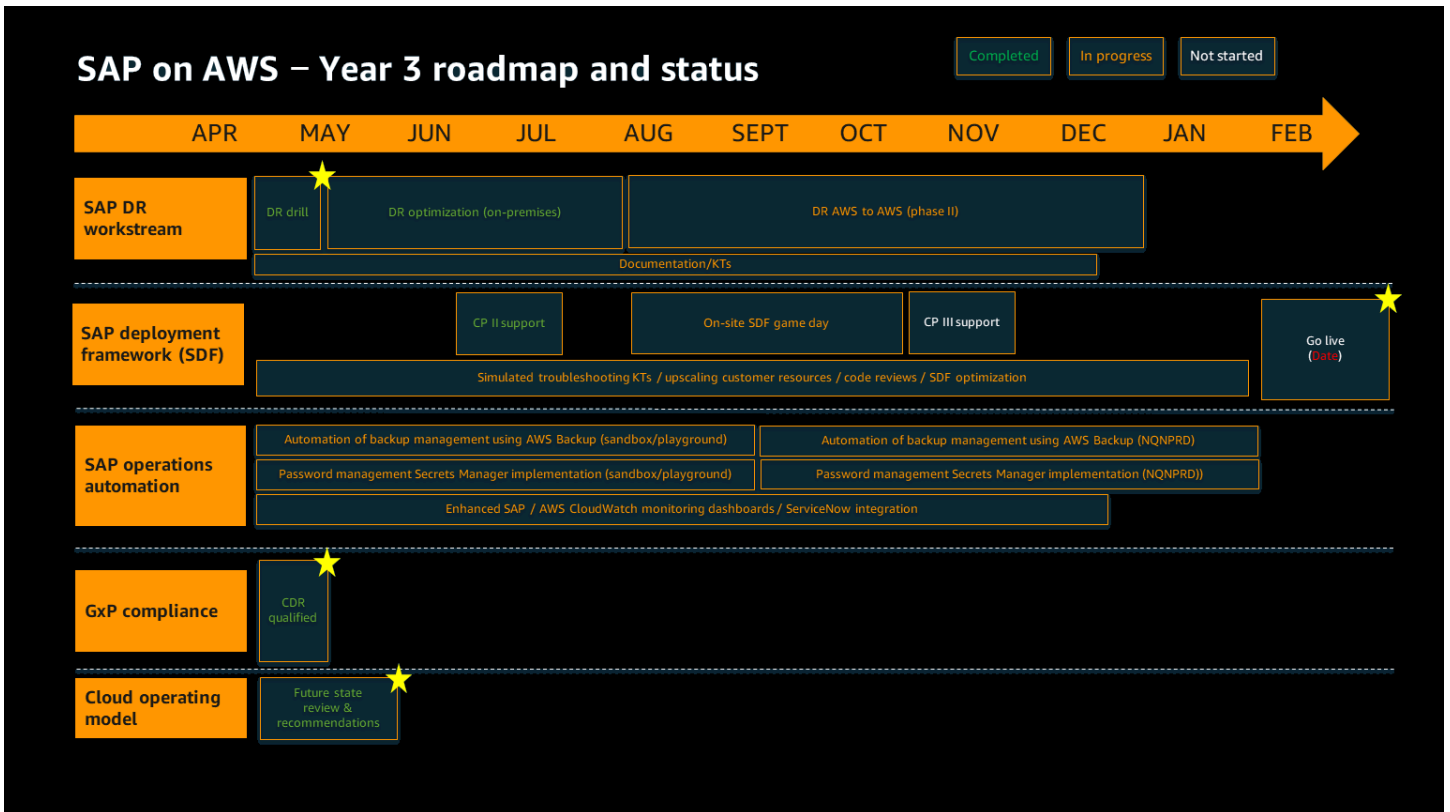
### 考量：

- 分別記錄服務台程序和 workflows，與基礎設施團隊共用此資訊，並確保每個人都可以存取服務台工具，以免依賴某個人。通常情況下，執行 Active Directory 加入、DNS 更新、開放防火牆和請求加密金鑰時，可能會有一個複雜且耗時的票證程序。記錄這些程序並在專案規劃階段考慮每個團隊的服務水準協議 (SLA) 至關重要。它還有助於解釋需要特別注意才能消除的延遲或瓶頸的原因。
- 為 Active Directory 和防火牆或聯網任務指派具名聯絡點。這些專用資源應該是專案的一部分。如果必須依賴服務票證，則無法控制服務 SLA。

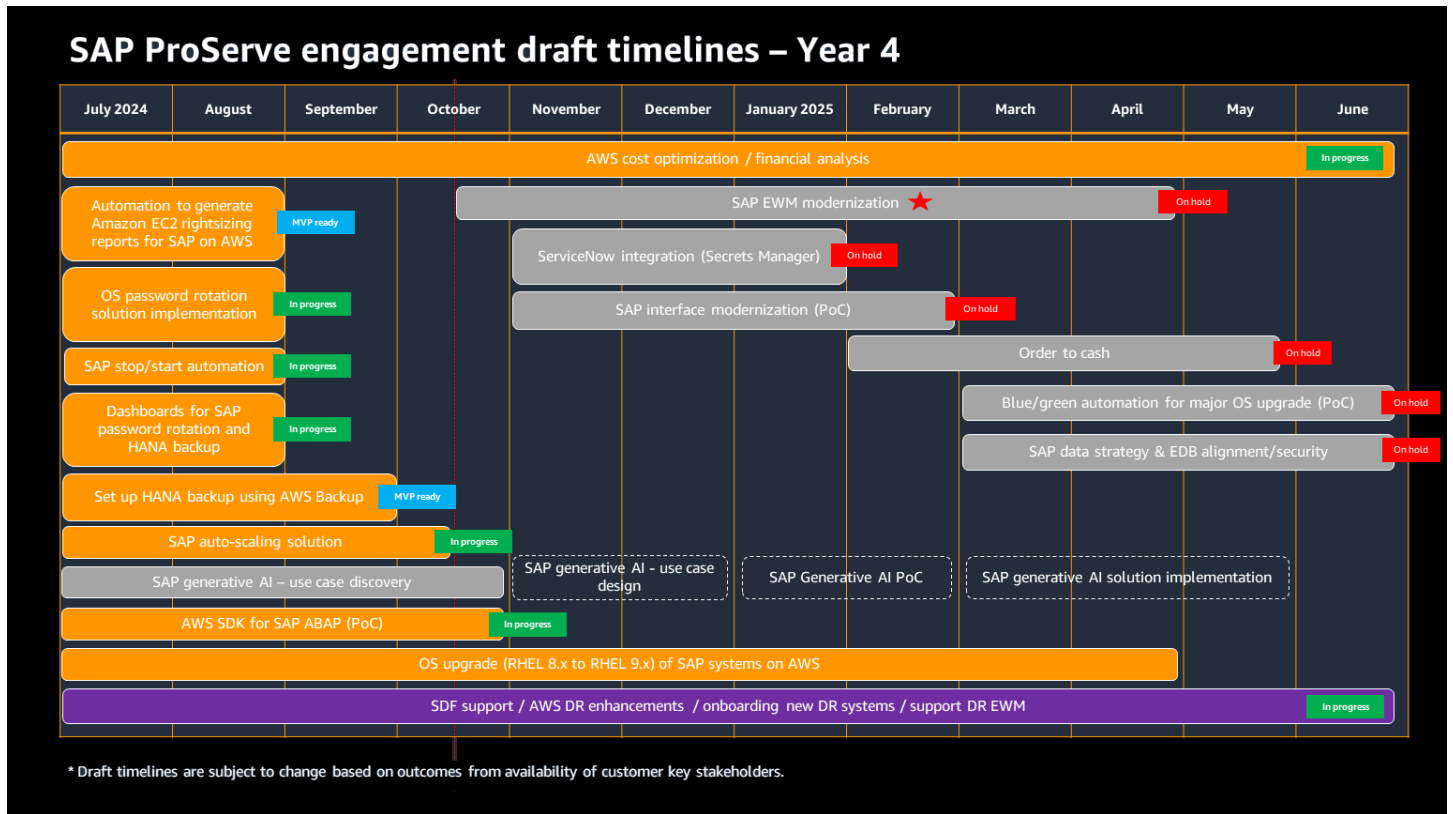
## 專案藍圖和里程碑追蹤器

下列圖表提供 AWS 綠地專案上多年 SAP 的範例藍圖。





下表顯示相同專案的 AWS Professional Services 參與時間表範例。



下圖顯示此專案的上線里程碑追蹤器。

### Go-live milestone tracker

Milestone	Projected start	Projected end	Start	End	Notes
Shutdown	Day 1 – 6 PM	Day 1 – 8:30 PM			
Snapshot	Day 1 – 8:30 PM	Day 1 – 10:30 PM			
Pre-data migration	Day 1 – 10:30 PM	Day 1 – 12 AM			
Data migration (go/no-go #1)	Day 2 – 12 AM	Day 2 – 10 PM			
Data verification (go/no-go #2)	Day 3 – 12 AM	Day 3 – 10 AM			
Basis OV	Day 3 – 5 PM	Day 3 – 11 PM			
Function OV	Day 3 – 5 PM	Day 3 – 11 PM			
Production (go/no-go #3)	Day 3 – 11 PM	Day 3 – 11:30 PM			

## 設計階段的最佳實務

綠地 SAP 實作的設計階段是建置階段成功的基礎。在此階段中，您會與基礎設施利益相關者合作，收集需求並記錄架構。您還必須考慮其他事項。必須確保各種專案利益相關者就時間表、總體策略和 SAP on AWS 架構達成共識，包括高可用性 (HA) 和災難復原 (DR) 環境。本節提供了解決專案設計階段可能遇到的一些挑戰的建議。

## 建立交付時間表和景觀圖

與您共用業務轉型專案時間表後，應立即建立基礎設施交付時間表。這有助於您提前規劃並在基礎設施團隊內保持一致。用於建置時間表的主要輸入來自 SAP 專案團隊的系統整合商 (SI)。回溯以取得 SAP Basis 團隊應該完成其工作的日期，以及基礎設施應準備好讓 SAP Basis 團隊安裝 SAP 應用程式的日期。

考量：

- 交付時間表的可視化展示可讓團隊快速了解正在建置的內容、需求日期以及可能的資源衝突。它還允許關鍵利益相關者以易於理解的方式視覺化正在建置的環境、專案的持續時間，以及 AWS 和 SAP Basis 團隊之間的交接。

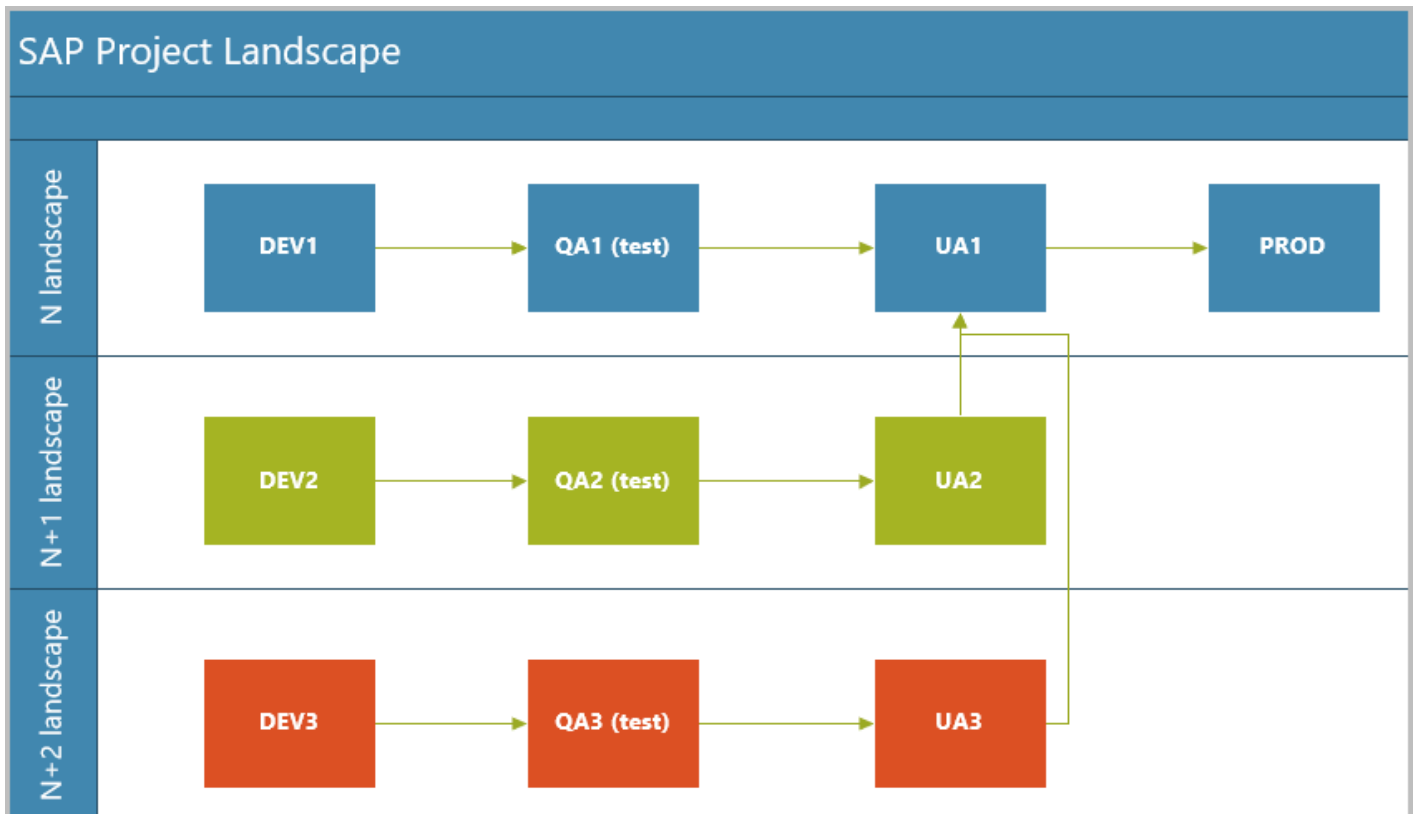
		January	February				March				April				May										
Week Beginning		January	2/1/2021	2/8/2021	2/15/2021	2/22/2021	3/1/2021	3/8/2021	3/15/2021	3/22/2021	3/29/2021	4/5/2021	4/12/2021	4/19/2021	4/26/2021	5/3/2021	5/10/2021	5/17/2021	5/24/2021						
Week ending		January	2/5/2021	2/12/2021	2/19/2021	2/26/2021	3/5/2021	3/12/2021	3/19/2021	3/26/2021	4/2/2021	4/9/2021	4/16/2021	4/23/2021	4/30/2021	5/7/2021	5/14/2021	5/21/2021	5/28/2021						
N Landscape	SBX Environment	SBX AWS Infra	SBX SAP Basis Build																						
	QA1 Environment					Requirements Gathering				QA1 Design				QA1 AWS Infra Build				QA1 Basis Build							
	UA1 Environment													UA1 Design				UA1 AWS Infra Build							
	PROD Environment																								
N+1 Landscape	DV2 Environment													DEV2 Design				DEV2 AWS Infra Build				Automation &			
	QA2 Environment																								
	UA2 Environment																								
N+2 Landscape	DV3 Environment																								
	QA3 Environment																								
	UA3 Environment																								

**Legend**

- Basis & AWS Design
- Basis Deliverable
- AWS Deliverable
- ★ Milestone: SAP application delivered to project team

- 典型的綠地 SAP 實作需要一年或更長時間。它包括基礎設施團隊沒有主動建置基礎設施元件的時間，因此請務必考慮這段時間的活動和可交付成果。要對應的活動範例包括 HA 設定和測試、DR 設定和測試、效能測試以及樓宇自動化指令碼。
- 在綠地實作中，景觀和環境的概念可能會令人困惑，難以理解。區分環境與景觀 (N、N+1、N+2) 的彩色編碼時間表可協助利益相關者快速了解此資訊矩陣。

以下是典型的高層級 SAP 景觀圖範例。這些方塊代表環境，它們是應用程式的集合 (例如，SAP S/4HANA)，而景觀則是用於特定版本的環境集合。



- 當您建立藍圖時，我們建議您重新瀏覽高階藍圖，並每季執行長期規劃，直到團隊建立為止。除了遷移之外，還包含其他藍圖項目，例如雲端卓越中心 (CCoE) 的工作流、操作自動化、安全性和合規性，以及雲端災難復原。

## 了解區域服務和文件決策

在設計階段開始時，我們建議您花時間了解和討論特定提供的服務，AWS 區域 以便正確選擇主要區域。具體而言，SAP 通常需要高效能執行個體，因此必須確保這些資源可在主要或次要區域中使用。選擇一個 [已通過認證可用於 SAP 應用程式的執行個體類型](#)。確定執行個體類型在選擇的 AWS 區域中可用。確定這一點的快速簡便方法是使用 [適用於執行個體類型方案的 AWS Command Line Interface \(AWS CLI\) 命令](#)。如果要用於實作的區域目前無法使用服務，請考慮為該區域訂購基礎設施的交付週期。

確認、再確認及記錄地區相關決策。在更大的專案團隊中公佈這些決策，以便關鍵利益相關者知悉。如果專案有架構審查委員會，請務必提出此主題，讓每個人都有機會在制定決策之前發表意見。

考量：

- 一個關鍵的考量事項是與 SAP 整合的邊界系統。如果您要在上託管邊界或衛星應用程式 AWS，最好在同一主要區域託管 SAP，以防止任何不必要的延遲討論。即使您確認延遲不是問題，也很難向利益相關者解釋為什麼邊界應用程式建置在與 SAP 應用程式不同的區域中。
- 對於 SAP 和與 SAP 整合的系統，災難復原 (DR) 網站也應該相同，以便能夠實際地協調 DR 測試。不同的系統可能需要不同的解決方案。例如，BusinessObjects 或 Winshuttle 等大型 SAP 系統可能無法使用，AWS 彈性災難復原 並且可能需要使用 Amazon Relational Database Service (Amazon RDS) 資料庫的不同解決方案。

## 建立命名慣例

徹底審核和記錄主機、SAP 環境、虛擬私有雲端 (VPC) 和 AWS 帳戶的命名慣例。請務必遵循現有的標準或慣例。在綠地實作中，可能必須從頭開始定義命名慣例。保持一致。例如，如果您呼叫 VPC Pre-Prod、SAP 環境 UAT 和 AWS 帳戶 TST，從支援角度建立這三個名稱的關聯將會很困難。確保獲得共識並分配每個角色都有意義的名稱，但要保持靈活性。例如，請勿將區域名稱硬編碼為伺服器名稱，以防將來必須切換為其他區域。避免使用內部部署伺服器所使用的命名慣例。相反地，如果您的組織還沒有一個靈活的雲端命名慣例，建議使用它。

考量：

- 對於可變更的資訊使用 [AWS 標記](#)。
- 請勿將非生產環境置於生產 VPC 中。如果這是一個要求，請確保在同意之前有合理的理由。

## 記錄所有決策

建議您徹底記錄每個決策的每個變化，誰做出決策，在什麼日期，以及誰在場。將決策儲存在公共場所，例如 Atlassian Confluence 或試算表，並確保正確簽署決策。利益相關者或團隊成員可能會忘記達成的共識，並在稍後的設計或建置階段對決策提出質疑。如果發生這種情況，您會希望有現成的資料來解決任何問題。以下是要記錄的關鍵決策範例：

- 區域決策
- HA 相關的應用程式
- 災難復原選項
- 專案階段中的環境支援模型
- 備份和還原方法以及工具
- VPC 結構

- AWS 帳戶決策
- 安全決策

此外，追蹤所有產品功能請求，並記錄團隊實作變更所需的時間。

## 建置階段的最佳實務

本節中的建議有助於確保專案的建置階段更順暢。建置階段包括程式碼、開發、部署和實作活動。它通常包含一個設計審查和核准工作階段，一次啟動會議，以確定正在建置的內容、時間表和退出標準。這是為所有 AWS 服務編寫、對等審查和部署程式碼的階段。

以下建議也涵蓋測試或驗證活動。

## 主持每日站立會議

無論使用哪種專案方法，請務必主持每日站立會議。儘管每日站立會議與敏捷方法論相關聯，但對於其他方法 (包括瀑布模型)，其也是非常有用的團隊連接機制。甚至可以使用混合專案架構，它採用各種方法的最佳實務。

考量：

- 使用諸如 Jira 看板這類輕量級產品，建立每個任務的說明。這些看板將成為每日站立會議的指南。如果您的團隊擁有足夠的能力和專業知識，那麼也可以使用 Scaled Agile Framework (SAFe) 方法論並創造壯舉。但是，大多數基礎設施團隊不希望管理複雜的 Scrum 看板而帶來管理開銷，因此建議使用輕量級工具。擁有看板還可以讓您生成有關團隊正在進行的工作報告，並為您提供控制範圍的機制。
- 在綠地 SAP 專案中，在鎖定範圍之後新增許多 SAP 或邊界應用程式並不罕見。如果您沒有良好的機制來控制、排定優先順序並提供專案範圍的可見性，則很難請求額外的資源或重新排定工作的優先順序，以保持專案的正常進行。

## 使用統一的建置規格表

針對所有環境和情形使用單一建置規格試算表。這將建立一個可以很容易尋找和搜尋的文件。建議您啟用版本管理，以輕鬆地從事故中復原。與 SAP Basis 團隊合作制定一種格式。Basis 團隊會追蹤 SAP 系統的詳細資訊，並擁有單一規格，可確保內部雲端團隊能夠在專案完成後快速取得所有權並在一處查看所有中繼資料。

下面是一個範本範例，用來擷取具有一個範例伺服器需求的金鑰伺服器建置中繼資料。

Landscape	Environment	SAP SID	Application Name	Application ID	Instance Role / Component	Hostname (AWS)	Domain Name	User-Friendly Hostname (CNAME)	IP Address	HA Cluster (Yes/No)	OS Type	OS	Build Status
N	DV1	DS4	SAP S/4 HANA	S4H	ASCS/ERS Server	AWSS4HDV101	xx.xxxx.com	SAPS4.xx.xxxx.com	12.345.678.901	Yes	RHEL	Red Hat Enterprise Linux for SAP	AD Join in progress

## 請注意 AWS 服務配額

您可以為 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體佈建的虛擬 CPU (vCPU) 數目有配額。部署 EC2 執行個體時，需要特定數量的 vCPU，具體取決於 EC2 執行個體類型。每個 AWS 帳戶都有可以為其佈建 vCPUs 數量的軟性限制。當您部署 EC2 執行個體時，軟性限制會自動增加約 100-150 個 vCPU。不過，如果嘗試同時部署多個 (例如 20 個) EC2 執行個體，則可能會超過軟性限制。如果您認為可能會遇到此限制，請在部署 EC2 執行個體之前[提交請求以增加配額](#)。這可避免在部署過程中達到服務配額限制。

## 制定安全金鑰輪換策略

AWS Key Management Service (AWS KMS) 可讓客戶輕鬆建立和管理密碼編譯金鑰，並控制其在各種 AWS 服務和各種應用程式中的使用。對於 SAP 實作，AWS KMS 金鑰用於加密存放在 Amazon Elastic Block Store (Amazon EBS) 磁碟區中的靜態資料，並用於 SAP 二進位檔和 SAP HANA 檔案系統。KMS 金鑰也用於存放在 Amazon Simple Storage Service (Amazon S3) 儲存貯體中的資料，以存放軟體媒體和備份，以及 `/usr/sap/trans` 和 `/sapmnt` 的 Amazon Elastic File System (Amazon EFS) 檔案系統。AWS KMS 可讓您靈活地使用 AWS 受管金鑰或客戶受管金鑰。建議您在建置階段開始時記錄並共用安全金鑰管理策略和決策。專案中間的安全政策變更，例如從客戶受管金鑰切換到 AWS 受管金鑰，可能需要 SAP 環境的完整重建，這可能會影響您的專案時間表。

獲得所有安全利益相關者對金鑰使用和輪換的認可。考慮雲端或內部部署環境的現有金鑰輪換政策，並修改這些政策以便在 AWS 上使用。如果在金鑰管理策略上難以達成共識，請為決策者提供培訓，協助他們了解安全基線和級別設定方面的考量事項。在建置環境之前制定金鑰輪換決策至關重要。例如，如果您要從客戶受管金鑰變更為 AWS 受管金鑰，您可能會遇到 Amazon EBS 問題，這不允許線上變更加密金鑰。必須使用新金鑰重建 EBS 磁碟區。需要重建 SAP 執行個體，這不是理想情況。

同樣地，如果您的專案使用 Vormetric 等外部金鑰管理解決方案，並將金鑰材料匯入其中 AWS KMS，請確定您的安全決策者知道外部 KMS 金鑰和 AWS KMS 金鑰之間的金鑰輪換差異（自動輪換）。當根據安全政策使用和輪換外部 KMS 金鑰時，不僅金鑰材料發生變更，而且金鑰的 Amazon Resource Name (ARN) 也會變更，這表示必須重新建立 EBS 磁碟區，而且整個 SAP 系統必須進行少量遷移。另一方面，如果您啟用客戶受管金鑰或 AWS 受管金鑰的自動輪換 AWS KMS，則金鑰材料會變更，但金鑰 ARN 會保持不變，這表示 EBS 磁碟區不會受到影響。如需金鑰輪換的詳細資訊，請參閱 AWS KMS 文件中的[輪換 AWS KMS 金鑰](#)。

另一個安全方法是使用 AWS Secrets Manager 進行資料庫和作業系統密碼輪換，這可透過標準儀表板取得。此外，請確保災難復原環境的 AWS Identity and Access Management (IAM) 角色與生產環境隔離，以協助保護環境免受惡意活動的影響。

## 停用未使用的伺服器

我們建議您在概念驗證 (PoC) 伺服器用盡後立即將其停用。執行未使用的伺服器可能成本高昂。請務必追蹤為綠地 SAP 實作所建置的所有伺服器，並在建置階段停止和停用未使用的伺服器。在停用伺服器之前，可以對 EC2 執行個體進行 Amazon Machine Image (AMI) 備份。如果未來需要啟動完全相同的伺服器，則可以還原備份。

停用伺服器不應該是您為結束實作專案而保留的操作。應該在專案的整個生命週期內以及完成實作後的維護或操作階段監控使用情況，停止並最終銷毀未使用的伺服器。請務必在開始時設定程序，以教導 SAP Basis 團隊成員停用這些伺服器，因為費用會快速累積。

# 資源

## 參考

- [輪換 AWS KMS 金鑰](#)
- [SAP HANA on AWS](#)
- [介紹 AWS Well-Architected Framework 的 SAP Lens](#) ( 部落格文章 )

## 工具

- [使用 Infrastructure as Code with 自動化 CloudFormation](#)
- [最佳實務 2.7 – 自動化測試、整合和部署變更](#) (AWS Well-Architected Framework ; 、 SAP Lens)
- [最佳實務 2.5 – 測試和驗證變更](#) (AWS Well-Architected Framework、SAP Lens)

## 指南和模式

- [SAP on AWS 遷移方法](#)
- [SAP HANA 至 AWS : AWS 遷移的模式](#)

# 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
<a href="#">已新增範例</a>	更新了指南，以新增範例 <a href="#">通訊計劃</a> 、 <a href="#">專案藍圖</a> 和里程碑追蹤器。	2024 年 7 月 18 日
<a href="#">初次出版</a>	—	2022 年 4 月 12 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：將內部部署 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，但只有來源資料庫會在資料複寫至目標資料庫時處理來自連線應用程式的交易。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

永久刪除資料集中個人資訊的程序。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

經常用於經常性問題的解決方案，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、持久性 (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

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、低延遲網路連線能力。

## 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，例如在網際網路上編製資訊索引的 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，並透過核准的程序，讓使用者快速取得他們通常無權存取 AWS 帳戶 之 的存取權。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改的中繼資料的程序。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 \(AWS FIS\)](#) 執行試驗，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

部落格文章中的 Stephen Orban 定義了這些階段：AWS 雲端 企業策略部落格上的[邁向雲端優先之旅和採用階段](#)。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](#)。

## deployment

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[上工作負載的災難復原 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

將人類可讀取的純文字資料轉換為加密文字的運算程序。

### 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 [\(\) 文件中的信封加密](#)。AWS Key Management Service AWS KMS

### 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給 LLM。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，已在廣義和未標記資料的大量資料集上進行訓練。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 CSPM、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 系統旨在自動容錯移轉、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。

## 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。

## IloT

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的部署](#)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

由 [Klaus Schwab](#) 於 2016 年推出的術語，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 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。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)

此 AWS 計畫提供諮詢支援、訓練和服務，以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

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 支援使用 S3 AWS KMS (SSE-KMS) 的所有伺服器端加密中的所有 S3 儲存貯體 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。

## 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 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。

## 重新放置

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，定義所有參與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 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。此功能會啟用聯合單一登入 (SSO)，AWS 管理主控台 讓使用者可以登入 或呼叫 AWS API 操作，而不必為組織中的每個人在 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](#)。

## 斯卡達

請參閱[監督控制和資料擷取](#)。

## SCP

請參閱[服務控制政策](#)。

## 秘密

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 秘密中的內容？](#) 在 Secrets Manager 文件中。

## 依設計的安全性

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。

## 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，通常可接受中等緩慢的查詢。

### 視窗函數

SQL 函數，對與目前記錄在某種程度上相關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，多次讀取](#)。

## 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。