上的備份和復原方法 AWS

AWS 方案指引

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS 方案指引: 上的備份和復原方法 AWS

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
為什麼使用 AWS 做為資料保護平台？ ... 2
目標業務成果 ... 3
選擇 AWS 服務 ... 4
設計備份和復原解決方案 ... 6
AWS Backup ... 7
Amazon S3 ... 9
使用 Amazon S3 儲存體方案 ... 9
建立標準 S3 儲存貯體 ... 10
使用 Amazon S3 版本控制 ... 11
備份和復原 AMIs的自訂組態檔案 ... 11
自訂備份和還原 ... 11
保護備份資料 ... 11
具有 EBS 磁碟區的 Amazon EC2 ... 13
Amazon EC2 備份和復原 ... 14
AMIs或快照 ... 14
伺服器磁碟區 ... 15
個別伺服器磁碟區 ... 16
執行個體儲存體磁碟區 ... 16
標記和強制執行標準 ... 17
建立 EBS 磁碟區備份 ... 18
準備 EBS 磁碟區 ... 18
從主控台建立快照 ... 19
建立 AMIs ... 19
Amazon Data Lifecycle Manager ... 20
AWS Backup ... 20
多磁碟區備份 ... 21
保護備份 ... 22
封存快照 ... 23
自動化快照和 AMI 建立 ... 23
還原磁碟區或執行個體 ... 23
從 EBS 快照還原檔案和目錄 ... 24
從 Amazon EBS 快照還原 EBS 磁碟區 ... 24
從 EBS 快照建立或還原 EC2 執行個體 ... 26

從 AMI 還原執行中的執行個體 26
從內部部署備份和復原 28
檔案閘道 28
磁碟區閘道 29
磁帶閘道 29
備份和復原應用程式 31
雲端原生 AWS 服務 32
Amazon RDS 32
使用 DNS CNAME 33
DynamoDB 34
混合架構 35
移動集中式備份管理解決方案 35
災難復原 37
內部部署 DR 至 AWS 37
雲端原生工作負載的 DR 39
單一可用區域中的 DR 39
區域故障中的 DR 40
清除備份 41
常見問答集 42
我應該選取哪些備份排程？ 42
我需要在開發帳戶中建立備份嗎？ 42
在建立快照時，是否可以升級應用程式並繼續使用 EBS 磁碟區，而不會有任何影響？ 42
後續步驟 43
資源 44
文件歷史紀錄 45
詞彙表 47
..... 47
A 47
B 50
C 51
D 54
E 57
F 59
G 60
H 61
I 62

L 64
M 65
O 69
P 71
Q 73
R 73
S 76
T 79
U 80
V 81
W 81
Z 82
..... lxxxiii

上的備份和復原方法 AWS

Khurram Nizami，Amazon Web Services (AWS)

2024 年 6 月 (文件歷史記錄)

本指南討論如何使用內部部署、雲端原生和混合架構的 Amazon Web Services (AWS) 服務實作備份和復原方法。這些方法提供更低的成本、更高的可擴展性和更高的耐用性，以滿足復原時間目標 (RTO)、復原點目標 (RPO) 和合規要求。

本指南適用於負責保護公司 IT 和雲端環境中資料的技術領導者。

本指南涵蓋不同的備份架構（雲端原生應用程式、混合和內部部署環境）。它也涵蓋相關的 Amazon Web Services (AWS) 服務，可用於為架構中不可變的元件建置可擴展且可靠的資料保護解決方案。

另一種方法是將工作負載現代化，以使用不可變的架構，減少對備份和復原元件的需求。 AWS 提供許多服務來實作不可變的架構，並減少備份和復原的需求，包括：

- 使用 的無伺服器 AWS Lambda
- 使用 Amazon Elastic Container Service (Amazon ECS)、Amazon Elastic Kubernetes Service (Amazon EKS) 和 的容器 AWS Fargate
- Amazon Machine Image AMIs) 搭配 Amazon Elastic Compute Cloud (Amazon EC2)

隨著企業資料的成長加速，保護資料的任務會變得更具挑戰性。有關備份方法的耐久性和可擴展性的問題很常見，包括以下問題：雲端如何協助滿足我的備份和還原需求？

本指南包含下列主題：

- 選擇資料保護 AWS 的服務
- 設計備份和復原解決方案
- 使用 備份和復原 AWS Backup
- 使用 Amazon S3 進行備份和復原
- 使用 EBS 磁碟區的 Amazon EC2 備份和復原
- 從內部部署基礎設施備份和復原至 AWS
- 從 備份和復原應用程式 AWS 至您的資料中心
- 雲端原生 AWS 服務的備份和復原

- 混合架構的備份和復原
- 使用 進行災難復原 AWS
- 清除備份

為什麼使用 AWS 做為資料保護平台？

AWS 是安全、高效能、彈性、節省成本且easy-to-use雲端運算平台。 AWS 負責建立、實作和管理可擴展備份和復原解決方案所需的無差異繁重工作。

使用 AWS 做為資料保護策略的一部分有許多優點：

- 耐用性：Amazon Simple Storage Service (Amazon S3) 和 S3 Glacier Deep Archive 專為 99.999999999% (11 個九） 的耐用性而設計。這兩個平台都提供可靠的資料備份，並跨至少三個分散地理的可用區域進行物件複寫。許多 AWS 服務使用 Amazon S3 進行儲存和匯出/匯入操作。例如，Amazon Elastic Block Store (Amazon EBS) 使用 Amazon S3 進行快照儲存。
- Security：在傳輸中和靜態時 AWS ，提供許多存取控制和資料加密的選項。
- 全球基礎設施： AWS 服務可在全球使用，因此您可以在符合合規和工作負載需求的區域中備份和存放資料。
- Compliance： AWS infrastructure 已通過認證，符合下列標準，因此您可以輕鬆地將備份解決方案納入現有的合規方案：
  - 服務組織控制 (SOC)
  - 認證參與標準聲明 (SSAE) 16
  - 國際標準化組織 (ISO) 27001
  - 支付卡產業資料安全標準 (PCI DSS)
  - 美國健康保險流通與責任法案 (HIPAA)
  - SEC1
  - 聯邦風險與授權管理計劃 (FedRAMP)
- 可擴展性：使用 AWS，您不必擔心容量。隨著您的需求變更，您可以向上或向下擴展您的消耗量，而無需管理開銷。
- 降低總擁有成本 (TCO)： AWS 營運規模可降低服務成本，並有助於降低 AWS 服務的 TCO。 會透過價格下降將這些節省的成本 AWS 傳遞給客戶。
- Pay-as-you-go定價：購買您需要 AWS 的服務，並且僅在您計劃使用服務的期間內購買。 AWS 定價沒有預付費用、終止處罰或長期合約。

目標業務成果

本指南的目標是提供您可以用來支援下列備份和復原方法 AWS 的服務概觀：

- 內部部署架構
- 雲端原生架構
- 混合架構
- AWS 原生服務
- 災難復原 (DR)

涵蓋最佳實務和考量事項，以及服務概觀。本指南也提供使用一種方法與另一種方法進行備份和復原之間的權衡。

選擇資料保護 AWS 的服務

AWS 提供多種儲存和補充服務，可作為備份和復原方法的一部分。這些服務可以同時支援雲端原生和混合架構。對於不同的使用案例，不同的服務更有效。

- Amazon S3 適用於混合和雲端原生使用案例。它提供高度耐用的一般用途物件儲存解決方案，適合備份個別檔案、伺服器或整個資料中心。
- AWS Storage Gateway 非常適合混合使用案例。Storage Gateway 使用 Amazon S3 的強大功能來滿足常見的現場部署備份和儲存需求。您的應用程式會使用下列標準儲存協定，透過虛擬機器 (VM) 或硬體閘道設備連線至服務：
  - 網路檔案系統 (NFS)
  - 伺服器訊息區塊 (SMB)
  - 網路小型電腦系統界面 (iSCSI)

  閘道會將這些常見的內部部署通訊協定橋接至 AWS 儲存服務，如下所示：
  - Amazon S3
  - S3 Glacier Deep Archive
  - Amazon EBS

  Storage Gateway 可讓您更輕鬆地為檔案、磁碟區、快照和虛擬磁帶提供彈性、高效能的儲存 AWS 體。
- AWS Backup 是一種全受管備份服務，可集中和自動化跨 AWS 服務的資料備份。使用 AWS Backup，您可以集中設定備份政策並監控資源的 AWS 備份活動，例如：
  - EBS 磁碟區
  - EC2 執行個體（包括 Windows 應用程式）
  - Amazon RDS 和 Amazon Aurora 資料庫
  - DynamoDB 資料表
  - Amazon Neptune 資料庫
  - Amazon DocumentDB (with MongoDB compatibility) 資料庫
  - Amazon EFS 檔案系統
  - Amazon FSx for Lustre 檔案系統和 Amazon FSx for Windows File Server 檔案系統
  - Storage Gateway 磁碟區

AWS Backup 的成本取決於您在一個月內使用、還原和傳輸的儲存體。如需詳細資訊，請參閱 AWS Backup 定價。

- AWS Elastic Disaster Recovery 會將您的機器複寫到目標 AWS 帳戶 和偏好區域中的暫存區域子網路。預備區域設計使用經濟實惠的儲存體和最少的運算資源來維持持續複寫，進而降低成本。您可以將 Elastic Disaster Recovery for DR 從現場部署到雲端，以及用於跨區域 DR。
- AWS Config 提供您 AWS 帳戶中 AWS 資源組態的詳細檢視。這包括資源彼此的關係，以及過去的設定方式。在此檢視中，您可以查看資源組態和關係隨著時間的變化。

  當您開啟 AWS 資源的AWS Config 組態記錄時，您會隨著時間保留資源關係的歷史記錄。這有助於識別和追蹤 AWS 資源關係 （包括已刪除的資源） 長達七年。例如， AWS Config 可以追蹤 Amazon EBS 快照磁碟區與磁碟區連接的 EC2 執行個體之間的關係。
- AWS Lambda 可用來以程式設計方式定義和自動化工作負載的備份和復原程序。您可以使用 AWS SDKs 與服務 AWS 及其資料互動。您也可以使用 Amazon EventBridge 定期執行 Lambda 函數。

AWS 服務提供用於備份和還原的特定功能。對於您使用的每個 AWS 服務，請參閱 AWS 文件，以判斷服務提供的備份、還原和資料保護功能。您可以使用 AWS Command Line Interface (AWS CLI)、AWS SDKs和 API 操作來自動化資料備份和復原 AWS 的服務特定功能。

設計備份和復原解決方案

在開發備份和還原資料的全方位策略時，您必須先識別可能的故障或災難情況及其潛在的業務影響。在某些產業中，您必須考慮資料安全、隱私權和記錄保留的法規要求。

備份和復原程序應包含適當的精細程度，以符合工作負載及其支援業務流程的復原時間目標 (RTO) 和復原點目標 (RPO)，包括下列項目：

- 檔案層級復原（例如，應用程式的組態檔案）
- 應用程式資料層級復原（例如，MySQL 中的特定資料庫）
- 應用程式層級復原（例如，特定的 Web 伺服器應用程式版本）
- Amazon EC2 磁碟區層級復原（例如 EBS 磁碟區）
- EC2 執行個體層級復原。（例如 EC2 執行個體）
- 受管服務復原（例如 DynamoDB 資料表）

請務必考慮解決方案的所有復原需求，以及架構中各種元件之間的資料相依性。為了促進成功的還原程序，請在架構中的各種元件之間協調備份和復原。

下列主題說明以基礎設施組織為基礎的備份和復原方法。IT 基礎設施可以廣泛分類為內部部署、混合或雲端原生。

使用 備份和復原 AWS Backup

AWS Backup 是一種全受管備份服務，可集中和自動化跨 AWS 服務的資料備份。 AWS Backup 提供整合 Amazon CloudWatch、、 AWS CloudTrail AWS Identity and Access Management (IAM) AWS Organizations和其他服務的協調層。此集中式 AWS 雲端原生解決方案提供全域備份功能，可協助您達成災難復原和合規要求。您可以使用 AWS Backup集中設定備份政策，並監控 AWS 資源的備份活動。

AWS Backup 是跨 AWS 帳戶和區域為您的 AWS 資源實作標準備份計劃的理想解決方案。因為 AWS Backup 支援多種 AWS 資源類型，因此可讓您更輕鬆地維護和實作工作負載的備份策略，而這些備份策略使用需要一起備份的多個 AWS 資源。 AWS Backup 也可讓您共同監控涉及多個 AWS 資源的備份和還原操作。

如果您有合規和稽核要求，您可以使用 AWS Backup Audit Manager 功能來建立稽核架構和報告，以支援您的合規要求。AWS Backup 保存庫鎖定功能也支援合規要求，方法是針對存放在備份保存庫中的所有備份強制執行一次寫入、多讀 (WORM) 組態 AWS Backup。

的主要區別 AWS Backup 是支援 Organizations。使用此支援，您可以在組織或組織單位層級定義和管理備份政策，並自動為每個相關 AWS 帳戶和區域實作這些政策。當您加入新 AWS 帳戶和區域時，您不需要分別定義和管理備份計劃。

AWS Backup 可讓您更輕鬆地使用標籤來實作全組織的備份政策。您可以建立個別的備份計劃，每個計劃都有唯一的頻率和保留設定，然後建立唯一的鍵值對標籤，以選擇要包含的資源進行備份。

例如，您可以建立每日備份計劃，在 UTC 每天 05：00 開始備份，並具有 35 天的保留政策。此備份計劃可以包含備份資源指派，指定具有標籤金鑰備份和標籤值的任何支援 AWS 資源都會根據此計劃備份。此外，您可以建立每月備份計畫，該計畫從每月第一天 UTC 的 05：00 開始，並具有 366 天的保留政策。此備份計劃可以包含備份資源指派，指定任何具有標籤金鑰備份和標籤值的支援 AWS 資源都會根據此計劃每月備份。

然後，您可以使用標籤政策和必要的標籤 AWS Config 規則，以確保所有 AWS 支援的資源都具有此標籤金鑰和其中一個標籤值。此方法可協助您在 AWS 中持續實作和維護支援 AWS Backup 資源的標準備份方法。您可以擴展此方法，以標準化具有不同復原點目標 (RPO) 需求的應用程式和架構層的備份。

建議您採取步驟來保護備份保存庫。例如，您可以實作 Organizations 服務控制政策 (SCP)，以防止備份文件庫遭到刪除或與非預期 AWS 的帳戶共用。如需更多詳細資訊和其他重要的安全考量，請參閱部落格文章中保護備份的前 10 大安全最佳實務 AWS。

AWS Backup 可以簡化 的災難復原 (DR) 計劃的實作， AWS 因為它支援多個可以共同解決 AWS 的資源。例如，您可以為 支援的大多數 AWS 資源類型實作跨區域和跨帳戶備份 AWS Backup。跨帳戶備

份可提高備份安全性，因為可在個別帳戶中取得複本。跨區域備份可提高可用性，因為備份可在多個區域中使用。如需支援 AWS 資源類型的詳細資訊，請參閱依資源區分的功能可用性資料表。

您可以使用範例 Backup and Recovery with AWS Backup open-source 解決方案來實作基礎設施做為程式碼 (IaC)，以及持續整合和持續交付 (CI/CD) 方法來管理 AWS Organizations 組織的備份。此解決方案包含自訂功能，例如在還原 AWS 的資源上自動重新套用 AWS 標籤，以及在單獨的帳戶和區域中建立次要備份保存庫，以供 DR 使用。

使用 Amazon S3 進行備份和復原

您可以隨時使用 Amazon Simple Storage Service (Amazon S3) 來存放和擷取任何數量的資料。您可以使用 Amazon S3 作為應用程式資料和檔案層級備份和還原程序的耐用存放區。例如，您可以使用 AWS CLI 或 AWS SDKs，使用備份指令碼將資料庫備份從資料庫執行個體複製到 Amazon S3。

AWS 服務 使用 Amazon S3 進行高度耐用且可靠的儲存，如下列範例所示：

- Amazon EC2 使用 Amazon S3 來存放 EBS 磁碟區和 EC2 執行個體存放區的 Amazon EBS 快照。
- Storage Gateway 與 Amazon S3 整合，提供內部部署環境搭配 Amazon S3 支援的檔案共用、磁碟區和磁帶程式庫。
- Amazon RDS 使用 Amazon S3 進行資料庫快照。

許多第三方備份解決方案也使用 Amazon S3。例如，Arcserve Unified Data Protection 支援 Amazon S3 以長期備份內部部署和雲端原生伺服器。

您可以使用這些服務的 Amazon S3 整合功能來簡化備份和復原方法。同時，您可以受益於 Amazon S3 提供的高耐用性和可用性。

Amazon S3 會將資料儲存為稱為儲存貯體的資源中的物件。您可以在儲存貯體中儲存任意數量的物件。您可以使用精細存取控制來寫入、讀取和刪除儲存貯體中的物件。單一物件的大小上限為 5 TB。

使用 Amazon S3 儲存類別來降低備份資料儲存成本

Amazon S3 提供多種儲存類別，可用於內部部署、混合和雲端原生架構。所有儲存類別都提供可擴展的容量，隨著備份資料集的增長，不需要磁碟區或媒體管理。pay-for-what-you-use模型和每月每 GB 的低成本，讓 Amazon S3 儲存類別適合各種資料保護使用案例。Amazon S3 儲存類別專為不同的使用案例而設計，包括下列類別：

- 經常存取儲存體類別，用於經常存取的資料的一般用途儲存體 （例如，組態檔案、意外備份、每日備份）。這包括 S3 標準儲存類別，這是所有 Amazon S3 物件的預設值。
- 長時間存取儲存類別不常，但存取資料不常 （例如每月備份）。這包括 S3 Standard-IA 儲存類別。IA 表示不常存取。
- S3 Glacier 儲存類別，適用於很少需要存取的極長時間資料 （例如，每年備份）。這包括 S3 Glacier Deep Archive，可提供最低成本的儲存 AWS。

對於具有未知或變更存取模式的備份，您可以使用 S3 Intelligent-Tiering 儲存類別。S3 Intelligent-Tiering 會根據上次存取物件的天數，自動將物件轉換為最具成本效益的層。

> **Note**
>
> 某些儲存類別的持續時間費用下限。如需詳細資訊，請參閱Amazon S3 定價，並使用網頁搜尋尋找 `duration`。

Amazon S3 提供生命週期政策，您可以設定這些政策來管理整個生命週期的資料。設定政策後，您的資料會自動遷移至適當的儲存類別，而不會變更您的應用程式。如需詳細資訊，請參閱 Amazon S3 物件生命週期管理文件。

若要降低備份成本，請根據您的復原時間目標 (RTO) 和復原點目標 (RPO)，使用分層儲存類別方法，如下列範例所示：

- 過去 2 週的每日備份使用 S3 Standard
- 過去 3 個月內使用 S3 Standard-IA 的每週備份
- S3 Glacier Flexible Retrieval 上過去一年的每季備份
- 過去 5 年的 S3 Glacier Deep Archive 年度備份
- 在 5 年後從 S3 Glacier Deep Archive 中刪除的備份

建立標準 S3 儲存貯體以進行備份和封存

您可以使用透過 S3 生命週期政策實作的公司備份和保留政策，來建立標準 S3 儲存貯體以進行備份和封存。成本分配標記和 AWS 計費報告是以儲存貯體層級指派的標籤為基礎。如果成本分配很重要，請為每個專案或業務單位建立單獨的備份並封存 S3 儲存貯體，以便您可以相應地分配成本。

您的備份指令碼和應用程式可以使用您建立的備份和封存 S3 儲存貯體來存放應用程式和工作負載資料的point-in-time快照。您可以建立標準 S3 字首，協助您組織point-in-time資料快照。例如，如果您建立每小時備份，請考慮使用備份字首，例如 `YYYY/MM/DD/HH/<WorkloadName>/<files...>`。透過這樣做，您可以手動或以程式設計方式快速擷取point-in-time備份。

使用 Amazon S3 版本控制自動維護復原歷史記錄

您可以啟用 S3 物件版本控制來維護物件變更的歷史記錄，包括還原至先前版本的功能。這對於組態檔案和其他物件非常有用，這些物件可能比point-in-time備份排程更頻繁地變更。它也適用於必須個別還原的檔案。

使用 Amazon S3 備份和復原 AMIs的自訂組態檔案

具有物件版本控制的 Amazon S3 可以成為工作負載組態和選項檔案的記錄系統。例如，您可以使用 ISV 維護的標準 AWS Marketplace Amazon EC2 映像。此映像可能包含軟體，其組態會維護在多個組態檔案中。您可以在 Amazon S3 中維護自訂組態檔案。啟動執行個體時，您可以將這些組態檔案複製到執行個體，做為執行個體使用者資料的一部分。當您套用此方法時，您不需要自訂和重新建立 AMI，即可使用更新的版本。

在自訂備份和還原程序中使用 Amazon S3

Amazon S3 提供一般用途備份存放區，您可以快速整合到現有的自訂備份程序。您可以使用 AWS CLI、 AWS SDKs和 API 操作來整合備份和還原使用 Amazon S3 的指令碼和程序。例如，您可能有一個資料庫備份指令碼，執行每晚資料庫匯出。您可以自訂此指令碼，將夜間備份複製到 Amazon S3 以進行異地儲存。如需如何執行此操作的概觀，請參閱批次上傳檔案至雲端教學課程。

您可以採取類似的方法，根據其個別 RPO 匯出和備份不同應用程式的資料。此外，您可以使用 在受管執行個體上執行 AWS Systems Manager 備份指令碼。Systems Manager 為個別備份程序提供自動化、存取控制、排程、記錄和通知。

保護 Amazon S3 中的備份資料

資料安全是普遍的考量， AWS 而且非常重視安全性。安全是每個 的基礎 AWS 服務。Amazon S3 提供靜態和傳輸中存取控制和加密的功能。所有 Amazon S3 端點都支援 SSL/TLS 加密傳輸中的資料。您可以執行下列動作來設定靜態物件的加密：

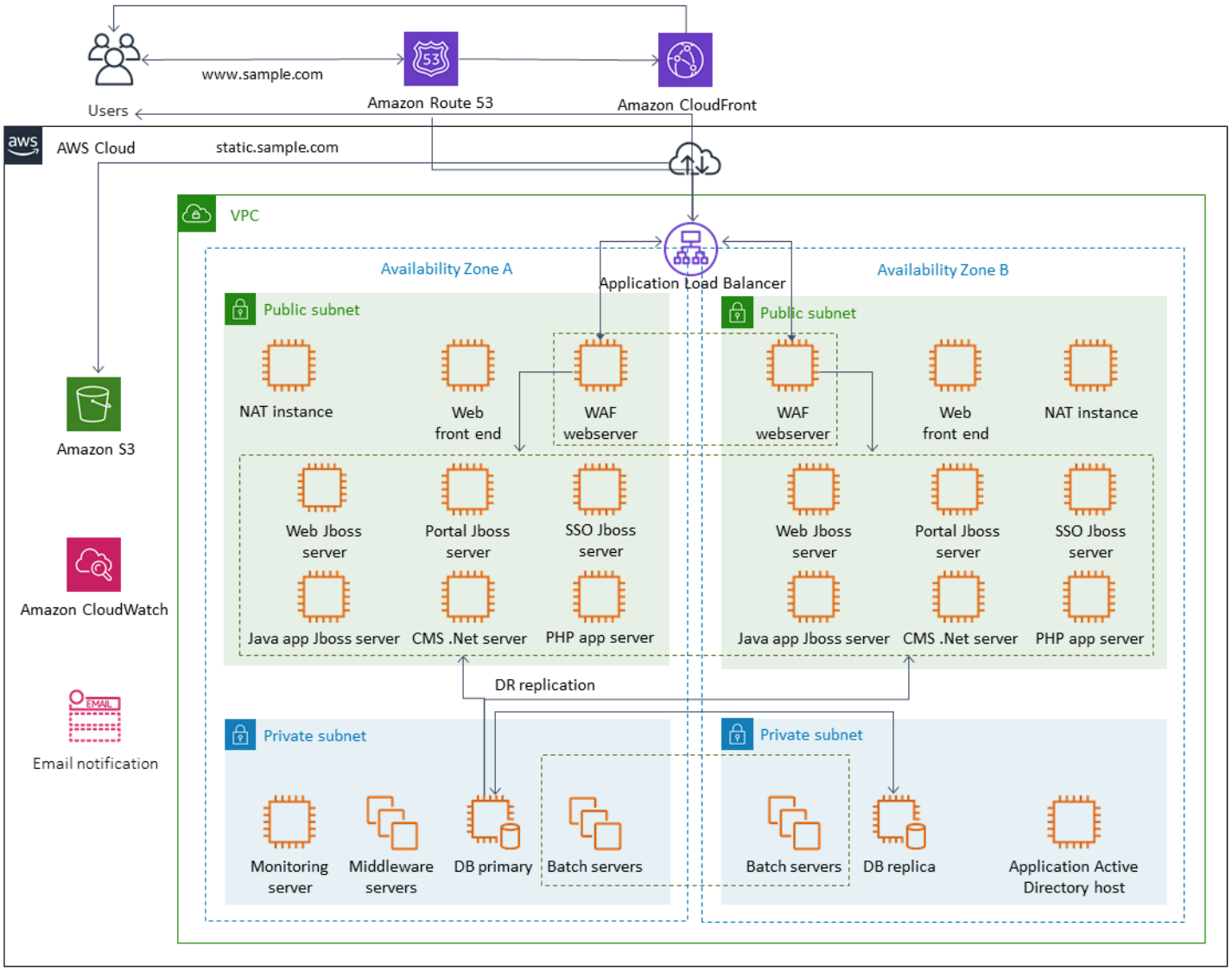
- 搭配 Amazon S3 受管加密金鑰使用伺服器端加密（預設）
- 使用伺服器端加密搭配 中存放的 AWS Key Management Service (AWS KMS) 金鑰 AWS KMS
- 使用用戶端加密

您可以使用 AWS Identity and Access Management (IAM) 來控制對 S3 物件的存取。IAM 提供對 S3 儲存貯體中個別物件和特定字首路徑許可的控制。您可以使用物件層級記錄搭配 來稽核對 S3 物件的存取。 AWS CloudTrail

使用 EBS 磁碟區的 Amazon EC2 備份和復原

AWS 提供多種方法來備份您的 Amazon EC2 執行個體。本節涵蓋備份 Amazon Elastic Block Store (Amazon EBS) 磁碟區或執行個體儲存磁碟區以進行儲存的不同層面。 AWS 如果備份符合您的需求，請考慮 AWS Backup 在 上管理備份的首選。請記住，只有在備份可以還原到其預定的 函數時，備份才有效。應定期測試還原和復原函數以確認這一點。

下圖中的解決方案架構描述了完全存在於 上的工作負載環境， AWS 其中大多數架構是以 Amazon EC2 為基礎。如下圖所示，此案例包括 Web 伺服器、應用程式伺服器、監控伺服器、資料庫、Active Directory 和災難復原 (DR) 複寫。



AWS 為此架構中呈現的許多 Amazon EC2 伺服器提供許多全功能服務，以執行建立、佈建、備份、還原和最佳化執行個體和儲存體的未區分工作。考慮這些服務在您的架構中是否合理，以降低複雜性和

管理。 AWS 也提供可改善 Amazon EC2 架構可用性的服務。特別是，請考慮使用 Amazon EC2 Auto Scaling 和 Elastic Load Balancing 來補充 Amazon EC2 上的工作負載。使用這些服務可以改善架構的可用性和容錯能力，並協助您在使用者影響最小的情況下還原受損的執行個體。

EC2 執行個體主要使用 Amazon EBS 磁碟區進行持久性儲存。Amazon EBS 提供多種備份和復原功能，本節詳細說明。

主題

- 使用快照和 AMIs Amazon EC2 備份和復原
- 使用 AMIs 和 EBS 快照建立 EBS 磁碟區備份
- 還原 Amazon EBS 磁碟區或 EC2 執行個體

使用快照和 AMIs Amazon EC2 備份和復原

考慮您是否需要使用 Amazon Machine Image (AMI) 建立 EC2 執行個體的完整備份，或拍攝個別磁碟區的快照。

使用 AMIs 或 Amazon EBS 快照進行備份

AMI 包括下列項目：

- 一或多個快照。Instance-store-backed AMIs 包含執行個體根磁碟區的範本（例如，作業系統、應用程式伺服器和應用程式）。
- 啟動許可，控制哪些 AWS 帳戶可以使用 AMI 啟動執行個體。
- 區塊型裝置映射，指定啟動時要連接至執行個體的磁碟區。

> **Note**
>
> 在大多數情況下，適用於 Windows、Red Hat、SUSE 和 SQL Server AMIs 需要正確的授權資訊，才能出現在 AMI 上。如需詳細資訊，請參閱了解 AMI 帳單資訊。當從快照建立 AMI 時，`RegisterImage` 操作會從快照的中繼資料衍生出正確帳單資訊，但這需要有適當的中繼資料。若要驗證是否已套用正確帳單資訊，請參閱新 AMI 的平台詳細資料欄位。如果欄位空白或不符合預期的作業系統程式碼（例如 Windows、Red Hat、SUSE 或 SQL)，則 AMI 建立失敗，您應該捨棄 AMI，並遵循從執行個體建立 AMI 中的指示。

您可以使用 AMIs來啟動具有預先設定軟體和資料的新執行個體。當您想要建立基準時，您可以建立 AMIs，這是用於啟動更多執行個體的可重複使用組態。當您建立現有 EC2 執行個體的 AMI 時，會針對連接至執行個體的所有磁碟區拍攝快照。快照包含裝置映射。

您無法使用快照來啟動新的執行個體，但您可以使用它們來取代現有執行個體上的磁碟區。如果您遇到資料損毀或磁碟區故障，您可以從已拍攝的快照建立磁碟區，並取代舊磁碟區。您也可以使用快照來佈建新的磁碟區，並在新的執行個體啟動期間連接它們。

如果您使用的是 AWS 維護和發佈的平台和應用程式 AMIs AWS Marketplace，請考慮為資料維護不同的磁碟區。您可以將資料磁碟區備份為與作業系統和應用程式磁碟區分開的快照。然後使用資料磁碟區快照，搭配 AWS 或 發佈的新更新 AMIs AWS Marketplace。此方法需要仔細測試和規劃，以備份和還原新發佈AMIs 上的所有自訂資料，包括組態資訊。

還原程序會受到您在 AMI 備份或快照備份之間的選擇所影響。如果您建立 AMIs 做為執行個體備份，則必須在還原程序中從 AMI 啟動 EC2 執行個體。您可能還需要關閉現有的執行個體，以避免潛在的衝突。潛在衝突的範例是加入網域之 Windows 執行個體的安全識別符 (SIDs)。快照的還原程序可能需要分離現有的磁碟區，並連接新還原的磁碟區。或者，您可能需要進行組態變更，將應用程式指向新連接的磁碟區。

AWS Backup 同時支援執行個體層級備份做為 AMIs，以及磁碟區層級備份做為個別快照：

- 如需執行個體上所有 EBS 磁碟區的完整備份，請建立 EC2 執行個體的 AMI。當您想要復原時，請使用啟動執行個體精靈來建立執行個體。在執行個體啟動精靈中，選擇我的 AMIs。
- 若要備份個別磁碟區，請建立快照。若要還原快照，請參閱從快照建立磁碟區。您可以使用 AWS Management Console 或 AWS Command Line Interface (AWS CLI)。

執行個體 AMI 的成本是執行個體上所有磁碟區的儲存體，但不是中繼資料。EBS 快照的成本是個別磁碟區的儲存體。如需磁碟區儲存成本的詳細資訊，請參閱 Amazon EBS 定價頁面。

伺服器磁碟區

EBS 磁碟區是 Amazon EC2 的主要持久性儲存選項。您可以將此區塊儲存用於結構化資料，例如資料庫或非結構化資料，例如磁碟區檔案系統中的檔案。

EBS 磁碟區會放置在特定的可用區域中。磁碟區會複寫到多個伺服器，以防止任何單一元件故障而導致資料遺失。失敗是指磁碟區完全或部分遺失，取決於磁碟區的大小和效能。

EBS 磁碟區的設計年失敗率 (AFR) 為 0.1-0.2%。這使得 EBS 磁碟區比典型商品磁碟機更可靠 20 倍，AFR 故障率約為 4%。例如，如果您有 1，000 個執行 1 年的 EBS 磁碟區，您應該預期一或兩個磁碟區將會失敗。

Amazon EBS 也支援快照功能，以擷取資料的point-in-time備份。所有 EBS 磁碟區類型都提供耐用的快照功能，專為 99.999% 的可用性而設計。如需詳細資訊，請參閱 Amazon Compute Service Level Agreement。

Amazon EBS 可讓您建立任何 EBS 磁碟區的快照（備份）。快照是建立 EBS 磁碟區備份的基本功能。快照會取得 EBS 磁碟區的副本，並將其放在 Amazon S3 中，在多個可用區域中以備援方式存放。初始快照是磁碟區的完整複本；持續快照只會儲存增量區塊層級變更。如需如何建立 Amazon EBS 快照的詳細資訊，請參閱 Amazon EBS 文件。

您可以執行還原操作、刪除快照，或更新快照中繼資料，例如與快照相關聯的標籤，這些中繼資料來自您拍攝快照的相同區域中的 Amazon EC2 主控台。

還原快照會建立新的 Amazon EBS 磁碟區，其中包含完整的磁碟區資料。如果您只需要部分還原，則可以使用不同的裝置名稱將磁碟區連接至執行中的執行個體。然後掛載，並使用作業系統複製命令，將資料從備份磁碟區複製到生產磁碟區。

也可以使用 Amazon EBS 快照複製功能，在 AWS 區域之間複製 Amazon EBS 快照，如 Amazon EBS 文件所述。您可以使用此功能將備份存放在另一個區域，而不必管理基礎複寫技術。

建立個別的伺服器磁碟區

您可能已經為作業系統、日誌、應用程式和資料使用一組標準的個別磁碟區。透過建立單獨的伺服器磁碟區，您可以減少因磁碟空間耗盡而導致應用程式或平台故障時的影響範圍。實體硬碟的風險通常更大，因為您沒有快速擴展磁碟區的彈性。使用實體磁碟機時，您必須購買新的磁碟機、備份資料，然後還原新磁碟機上的資料。透過 AWS，此風險會大幅降低，因為您可以使用 Amazon EBS 來擴展佈建的磁碟區。如需詳細資訊，請參閱 AWS 文件。

維護應用程式資料、使用者資料、日誌和交換檔案的個別磁碟區，以便您可以針對這些資源使用個別的備份和還原政策。透過分隔資料的磁碟區，您也可以根據資料的效能和儲存需求來使用不同的磁碟區類型。然後，您可以最佳化和微調不同工作負載的成本。

執行個體存放磁碟區的考量事項

執行個體存放區為執行個體提供暫時的區塊層級儲存空間。這個儲存空間位於實際連接到主機電腦的磁碟上。執行個體存放區非常適合用於臨時儲存經常變更的資訊，例如緩衝區、快取、暫存資料和其他臨時內容。對於跨執行個體機群複寫的資料，例如負載平衡的 Web 伺服器集區，它們也是較適合的。

執行個體存放區中的資料，只會在相關執行個體的生命週期期間存在。如果執行個體重新啟動 (刻意或無意)，執行個體存放區中的資料仍會持續存在。不過，在下列任何情況下，執行個體存放區中的資料都會遺失。

- 基礎磁碟機失敗。
- 執行個體停止。
- 執行個體終止。

因此，請勿依賴執行個體存放區以取得寶貴的長期資料。而是使用更持久的資料儲存體，例如 Amazon S3、Amazon EBS 或 Amazon EFS。

執行個體存放區磁碟區的常見策略是，根據復原點目標 (RPO) 和復原時間目標 (RTO)，視需要定期將必要資料保留至 Amazon S3。然後，您可以在啟動新的執行個體時，將資料從 Amazon S3 下載到執行個體存放區。您也可以在執行個體停止之前，將資料上傳至 Amazon S3。為了持久性，請建立 EBS 磁碟區，將其連接至您的執行個體，並定期將執行個體存放磁碟區中的資料複製到 EBS 磁碟區。如需詳細資訊，請參閱 AWS 知識中心。

標記和強制執行 EBS 快照和 AMIs 的標準

標記所有 AWS 資源是成本分配、稽核、疑難排解和通知的重要實務。標記對於 EBS 磁碟區很重要，因此存在管理和還原磁碟區所需的相關資訊。標籤不會自動從 EC2 執行個體複製到 AMIs也不會從來源磁碟區複製到快照。請確定您的備份程序包含來自這些來源的相關標籤。這可協助您設定快照中繼資料，例如存取政策、附件資訊和成本分配，以在未來使用這些備份。如需標記 AWS 資源的詳細資訊，請參閱標記最佳實務技術論文。

除了您用於所有 AWS 資源的標籤之外，還請使用下列備份特定標籤：

- 來源執行個體 ID
- 來源磁碟區 ID （適用於快照）
- 復原點描述

您可以使用 AWS Config 規則和 IAM 許可來強制執行標記政策。IAM 支援強制執行的標籤用量，因此您可以撰寫 IAM 政策，在 Amazon EBS 快照上操作時強制使用特定標籤。如果嘗試`CreateSnapshot`操作時沒有在 IAM 許可政策授予許可許可中定義的標籤，快照建立會失敗，但存取遭拒。如需詳細資訊，請參閱有關在建立和實作更強大的安全政策時標記 Amazon EBS 快照的部落格文章。

您可以使用 AWS Config 規則來自動評估資源 AWS 的組態設定。為了協助您開始使用， AWS Config 提供可自訂的預先定義規則，稱為 受管規則。您也可以建立自己的自訂規則。雖然 AWS Config 會持續追蹤 資源之間的組態變更，但它會檢查這些變更是否違反規則中的任何條件。如果資源違反規則，會將資源和規則 AWS Config 標記為不合規。請注意，必要的標籤受管規則目前不支援快照和 AMIs。

使用 AMIs 和 EBS 快照建立 EBS 磁碟區備份

AWS 提供建立和管理 AMIs和快照的豐富選項。您可以使用符合您需求的方法。許多客戶面臨的常見問題是管理快照生命週期，並依用途、保留政策等明確對齊快照。如果沒有適當的標記，則快照可能會意外刪除，或作為自動清除程序的一部分。您最終可能要為保留的過時快照付費，因為沒有明確了解是否仍然需要這些快照。

在建立快照或 AMI 之前準備 EBS 磁碟區

在您拍攝快照或建立 AMI 之前，請先為您的 EBS 磁碟區進行必要的準備。建立 AMI 會產生連接到執行個體的每個 EBS 磁碟區的新快照，因此這些準備也適用於 AMIs。

您可以拍攝已連接之 EBS 磁碟區的快照，該磁碟區正由開啟電源的 EC2 執行個體使用。不過，快照只會擷取在發出快照命令時寫入 EBS 磁碟區的資料。這可能會排除應用程式或作業系統快取的任何資料。最佳實務是讓系統處於未執行任何 I/O 的狀態。 在理想情況下，機器不接受流量且處於停止狀態，但這很少，因為全年無休的 IT 操作會成為常態。如果您可以將任何資料從系統記憶體排清到應用程式使用的磁碟，並暫停任何寫入磁碟區的檔案，以便拍攝快照，您的快照應該會完成。

若要進行乾淨的備份，您必須查詢資料庫或檔案系統。執行此作業的方式取決於資料庫或檔案系統。

資料庫的程序如下所示：

1. 如果可能，請將資料庫置於熱備份模式。
2. 執行 Amazon EBS 快照命令。
3. 將資料庫移出熱備份模式，或者，如果使用僅供讀取複本，請終止僅供讀取複本執行個體。

檔案系統的程序類似，但取決於作業系統或檔案系統的功能。例如，XFS 是一種檔案系統，可以排清其資料，以取得一致的備份。如需詳細資訊，請參閱 xfs_freeze。或者，您可以使用支援凍結 I/O 的邏輯磁碟區管理員來促進此程序。

不過，如果您無法排清或暫停磁碟區的所有檔案寫入，請執行下列動作：

1. 從作業系統卸載磁碟區。
2. 發出快照命令。
3. 重新掛載磁碟區以實現一致且完整的快照。您可以在快照狀態為待定時重新掛載和使用磁碟區。

快照程序會在背景繼續，快照建立速度很快，並擷取時間點。您備份的磁碟區只會卸載幾秒鐘。您可以排程小型備份時段，其中預期中斷，並由用戶端正常處理。

當您為做為根裝置的 EBS 磁碟區建立快照時，請先停止執行個體，再擷取快照。Windows 提供磁碟區影子複製服務 (VSS)，以協助建立應用程式一致性快照。 AWS 提供 Systems Manager 文件，您可以執行該文件來取得 VSS 感知應用程式的映像層級備份。快照包括來自這些應用程式和磁碟之間擱置中交易的資料。備份所有連接的磁碟區時，您不需要關閉執行個體或中斷連線。如需詳細資訊，請參閱 AWS 文件。

> **Note**
>
> 如果您要建立 Windows AMI 以便部署其他類似的執行個體，請使用 EC2Config 或 EC2Launch 來 Sysprep 執行個體。然後從已停止的執行個體建立 AMI。Sysprep 會從 Amazon EC2 Windows 執行個體移除唯一資訊，包括 SIDs、電腦名稱和驅動程式。重複 SIDs 可能會導致 Active Directory、Windows Server Update Services (WSUS)、登入問題、Windows 磁碟區金鑰啟用、Microsoft Office 和第三方產品的問題。如果您的 AMI 用於備份目的，而且您想要還原具有完整所有唯一資訊的相同執行個體，請勿將 Sysprep 與執行個體搭配使用。

從主控台手動建立 EBS 磁碟區快照

在您進行任何尚未在執行個體上完整測試的主要變更之前，請建立適當磁碟區或整個執行個體的快照。例如，您可能想要在升級或修補執行個體上的應用程式或系統軟體之前建立快照。

您可以從主控台手動建立快照。在 Amazon EC2 主控台的彈性區塊存放磁碟區頁面上，選取您要備份的磁碟區。然後在動作功能表中，選擇建立快照。您可以在篩選條件方塊中輸入執行個體 ID，以搜尋連接至特定執行個體的磁碟區。

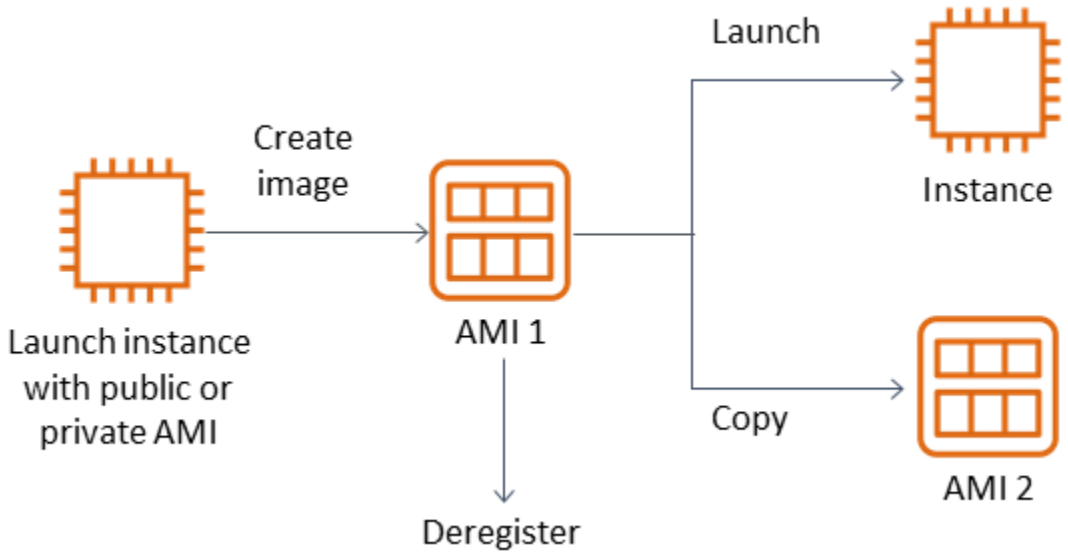
輸入描述並新增適當的標籤。新增`Name`標籤，以便稍後更容易找到磁碟區。根據您的標記策略新增任何其他適當的標籤。

建立 AMIs

AMI 提供啟動執行個體所需的資訊。AMI 包含根磁碟區和建立映像時連接至執行個體的 EBS 磁碟區的快照。您無法單獨從 EBS 快照啟動新的執行個體；您必須從 AMI 啟動新的執行個體。

當您建立 AMI 時，它會在您所使用的帳戶和區域中建立。AMI 建立程序會為每個連接至執行個體的磁碟區建立 Amazon EBS 快照，而 AMI 則參考這些 Amazon EBS 快照。這些快照位於 Amazon S3 中，非常耐用。

建立 EC2 執行個體的 AMI 之後，您可以使用 AMI 重新建立執行個體或啟動更多執行個體複本。您也可以將 AMIs 從一個區域複製到另一個區域，以進行應用程式遷移或 DR。



除非您要將虛擬機器遷移至 VMWARE 虛擬機器，否則必須從 EC2 執行個體建立 AMI AWS。若要從 Amazon EC2 主控台建立 AMI，請選取執行個體、選擇動作、選擇映像，然後選擇建立映像。

Amazon Data Lifecycle Manager

若要自動建立、保留和刪除 Amazon EBS 快照，您可以使用 Amazon Data Lifecycle Manager。自動化快照管理可協助您執行下列動作：

- 強制執行定期備份排程來保護重要資料。
- 依稽核人員或內部合規的要求來保留備份。
- 刪除過時的備份以降低儲存成本。

使用 Amazon Data Lifecycle Manager，您可以自動化 EC2 執行個體（及其連接的 EBS 磁碟區）或個別 EBS 磁碟區的快照管理程序。它支援跨區域複製等選項，因此您可以將快照自動複製到其他 AWS 區域。將快照複製到替代區域是支援替代區域中 DR 工作和還原選項的一種方法。您也可以使用 Amazon Data Lifecycle Manager 建立支援快速快照還原的快照生命週期政策。

Amazon Data Lifecycle Manager 是 Amazon EC2 和 Amazon EBS 的隨附功能。Amazon Data Lifecycle Manager 不收取任何費用。

AWS Backup

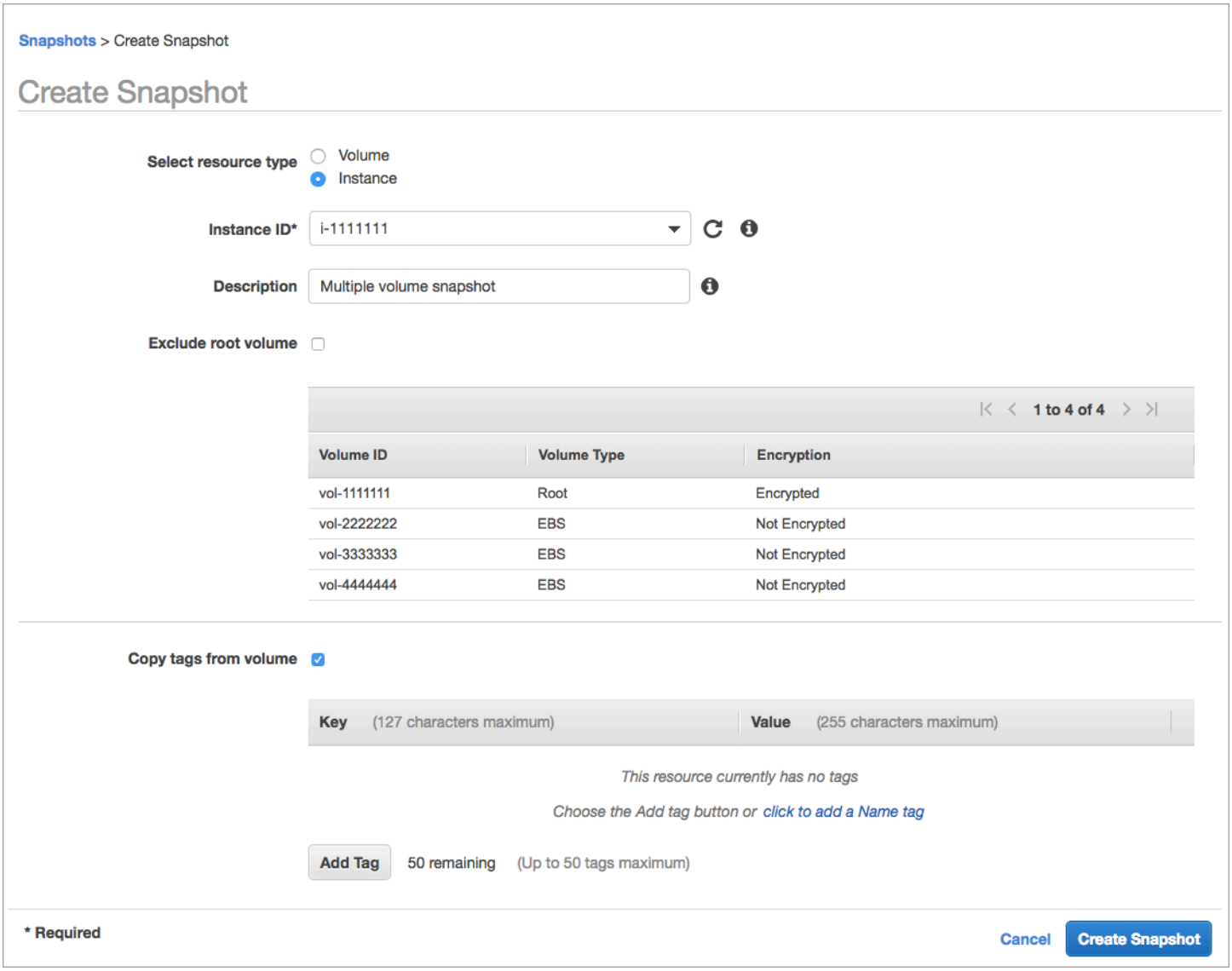
AWS Backup 是 Amazon Data Lifecycle Manager 獨有的，因為您可以建立備份計劃，其中包含跨多個 AWS 服務的資源。您可以協調備份，以涵蓋您同時使用的資源，而不是個別協調資源的備份。

AWS Backup 也包含備份保存庫的概念，這可以限制對已完成備份的復原點的存取。還原操作可以從開始， AWS Backup 而不是繼續每個個別資源，並還原建立的備份。 AWS Backup 也包含許多其他功能，例如稽核管理和報告。如需詳細資訊，請參閱本指南的 使用 備份和復原 AWS Backup 一節。

執行多磁碟區備份

如果您想要使用快照備份 RAID 陣列中 EBS 磁碟區上的資料，則快照必須一致。因為這些磁碟區的快照是個別建立的。從不同步的快照還原 RAID 陣列中的 EBS 磁碟區會降低陣列的完整性。

若要為您的 RAID 陣列建立一致的快照集，請使用 CreateSnapshots API 操作，或登入 Amazon EC2 主控台，然後選擇彈性區塊存放區、快照、建立快照。



在 RAID 組態中連接多個磁碟區的執行個體快照，會合稱為多磁碟區快照。多磁碟區快照可在連接到 EC2 執行個體的多個 EBS 磁碟區間提供point-in-time、資料協調和損毀一致性快照。您不需要停止執

行個體在磁碟區之間進行協調，即可達到一致性，因為快照會自動跨多個 EBS 磁碟區擷取。磁碟區的快照啟動後（通常是一到兩個），檔案系統可以繼續其操作。

建立快照後，每個快照視為個別快照。您可以執行所有快照操作，例如還原、刪除和跨區域和帳戶複製，就像使用單一磁碟區快照一樣。您也可以像單一磁碟區快照一樣標記多磁碟區快照。我們建議您標記多磁碟區快照，以在還原、複製或保留期間進行整體管理。如需詳細資訊，請參閱 AWS 文件。

您也可以從邏輯磁碟區管理員或檔案系統層級備份執行這些備份。在這些情況下，使用傳統備份代理程式可讓資料透過網路進行備份。網際網路和 提供許多代理程式型備份解決方案AWS Marketplace。

另一種方法是建立存在於單一大型磁碟區上主要系統磁碟區的複本。這可簡化備份程序，因為只需要備份一個大型磁碟區，而且備份不會發生在主要系統上。不過，請先判斷單一磁碟區在備份期間是否可以充分執行，以及最大磁碟區大小是否適合應用程式。

保護您的 Amazon EC2 備份

請務必考量備份的安全性，並防止意外或惡意刪除備份。您可以共同使用多種方法來完成此操作。為了防止因安全性漏洞而遺失關鍵備份，我們建議您將備份複製到另一個 AWS 帳戶。如果您有多個 AWS 帳戶，您可以將個別帳戶指定為封存帳戶，讓所有其他帳戶可以複製備份。例如，您可以使用跨帳戶備份來完成 AWS Backup此操作。

您的災難復原計劃也可能要求您能夠在其他 AWS 區域中重現 EC2 執行個體，以防發生區域故障。您可以將備份複製到相同帳戶中的另一個區域，以支援此目標。這可提供額外一層的意外刪除保護，並支援災難復原 (DR) 目標。AWS Backup 支援跨區域備份。

考慮封鎖 ec2：DeleteSnapshot 和 ec2：DeregisterImage 動作的 IAM 許可。反之，您可以讓保留政策和方法管理 EBS 快照和 Amazon EC2 AMIs 的生命週期。封鎖刪除動作是為您的 EBS 快照實作一次寫入、多讀 (WORM) 策略的一種方式。您也可以使用 AWS Backup Vault Lock，其可支援 EBS 快照和其他 AWS 資源。

此外，請考慮封鎖 ec2：ModifyImageAttribute 和 ec2：ModifySnapshotAttribute IAM 動作，以封鎖使用者共用 AMIs 和 EBS 快照的能力。這將防止您的 AMIs 和快照與組織外部 AWS 的帳戶共用。如果您使用的是 AWS Backup，請限制使用者在備份保存庫上執行類似的操作。如需詳細資訊，請參閱本指南的 AWS Backup 一節。

Amazon EBS 包含資源回收筒功能，可協助您還原意外刪除的 EBS 快照。如果您允許使用者刪除快照，請開啟此功能，以便不會永久刪除所需的快照。使用者在刪除多個快照時應特別小心，因為 Amazon EC2 主控台可讓您在一個操作中選取多個快照並將其刪除。此外，使用清除指令碼和自動化時請小心，以免意外刪除您需要的快照。資源回收筒功能可協助提供這類情況的保護。

封存 EBS 快照

封存 EBS 快照可以是經濟實惠的方法，可讓您保留磁碟區複本以供參考，而您不打算還原 90 天或更多天。在永久刪除 EBS 磁碟區的所有相關快照之前，這可能是一個良好的中繼步驟。例如，您可能會考慮將快照封存為不再使用的 EBS 磁碟區的end-of-lifecycle步驟。封存而不是刪除也可以是更符合成本效益的刪除保留方法，而不是使用資源回收筒。

使用 Systems Manager、 和 AWS SDKs 自動化快照 AWS CLI和 AMI 建立

您的備份方法可能需要建立快照或 AMI 之前和之後的操作。例如，您可能需要停止和啟動 服務，才能查詢檔案系統。或者，您可能需要在 AMI 建立期間停止和啟動執行個體。您可能還需要在架構中共同建立多個元件的備份，每個元件都有自己的建立前和建立後步驟。

您可以透過自動化程序並驗證備份程序是否一致套用，來縮短備份的維護時段時間。若要自動化您的自訂建立前和建立後操作，請使用 AWS CLI 和 SDK 編寫備份程序的指令碼。

您可以在 Systems Manager 執行手冊中定義自動化，該手冊可隨需執行或在 Systems Manager 維護時段期間執行。您可以授予使用者執行 Systems Manager Runbook 的存取權，而不需要授予 Amazon EC2 破壞性命令的許可。這也可以協助您驗證備份程序和標籤是否由使用者一致套用。您可以使用 AWS-CreateSnapshot 和 AWS-CreateImage 執行手冊來建立快照和 AMIs，也可以授予其他使用者使用它們的許可。Systems Manager 也包含 AWS-UpdateLinuxAmi 和 AWS-UpdateWindowsAmi Runbook，以自動化 AMI 修補和 AMI 建立。

您也可以使用 AWS CLI 和 AWS Tools for Windows PowerShell來自動化快照和 AMI 建立程序。您可以使用 aws ec2 create-snapshot AWS CLI 命令來建立 EBS 磁碟區的快照，做為自動化中的一個步驟。您可以使用 aws ec2 create-snapshots 命令來建立連接到 EC2 執行個體之所有磁碟區的損毀一致性同步快照。

您可以使用 AWS CLI 建立新的 AMIs。您可以使用 aws ec2 register-image 命令來為您的 EC2 執行個體建立新的映像。若要自動關閉、建立映像和重新啟動執行個體，請將此命令與 aws ec2 stop-instances 和 aws ec2 start-instances 命令結合。

還原 Amazon EBS 磁碟區或 EC2 執行個體

如果您需要僅還原連接至 EC2 執行個體的單一磁碟區，您可以分別還原該磁碟區、分離現有的磁碟區，並將還原的磁碟區連接至您的 EC2 執行個體。如果您需要還原整個 EC2 執行個體，包括其所有相關聯的磁碟區，您必須使用執行個體的 Amazon Machine Image (AMI) 備份。

為了減少復原時間和對相依應用程式和程序的影響，還原程序必須考慮要取代的資源。為了獲得最佳結果，請在較低的環境（例如，非生產）中定期測試還原程序，以確認您的程序符合復原點目標 (RPO)

和復原時間目標 (RTO)，以及還原程序如預期般運作。考慮還原程序將如何影響依賴於您要還原之執行個體的應用程式和服務，然後視需要協調還原。嘗試盡可能自動化和測試還原程序，以降低還原程序失敗或實作不一致的風險。

如果您使用 Elastic Load Balancing，搭配多個執行個體為流量提供服務，則可以讓故障或受損的執行個體停止服務。然後，您可以還原新的執行個體來取代它，而其他執行個體繼續服務流量，而不會中斷使用者。

以下所述的還原程序適用於未使用 Elastic Load Balancing 的執行個體：

- 從 EBS 快照還原個別檔案和目錄
- 從 Amazon EBS 快照還原 EBS 磁碟區
- 從 EBS 快照建立或還原 EC2 執行個體
- 從 AMI 還原執行中的執行個體

從 EBS 快照還原檔案和目錄

EBS 快照提供用於建立快照之原始磁碟區的point-in-time確切複本。若要還原個別檔案或目錄，您必須執行下列動作：

1. 首先，從包含檔案或目錄的 EBS 快照還原磁碟區。
2. 將磁碟區連接至您要還原檔案的 EC2 執行個體。
3. 將檔案從還原的磁碟區複製到您的 EC2 執行個體磁碟區。
4. 分離和刪除還原的磁碟區。

從 Amazon EBS 快照還原 EBS 磁碟區

您可以從現有 EC2 執行個體的快照建立磁碟區並將其連接至執行個體，以還原連接至現有 EC2 執行個體的磁碟區。您可以使用 主控台 AWS CLI、 或 API 操作，從現有的快照建立磁碟區。然後，您可以使用作業系統將磁碟區掛載到執行個體。

請注意，Amazon EBS 快照中的資料會以非同步方式載入 EBS 磁碟區。如果應用程式存取未載入資料的磁碟區，則從 Amazon S3 載入資料時，延遲會比平常更高。為了避免對延遲敏感的應用程式造成此影響，您有兩個選項：

- 您可以初始化 EBS 磁碟區。

- Amazon EBS 需要額外付費，可支援快速快照還原，無需初始化您的磁碟區。

如果您要取代必須使用相同掛載點的磁碟區，請卸載該磁碟區，以便掛載新的磁碟區。若要卸載磁碟區，請先停止任何使用磁碟區的程序。如果您要取代根磁碟區，您必須先停止執行個體，才能分離根磁碟區。

例如，請依照下列步驟，使用主控台將磁碟區還原至較早point-in-time備份：

1. 在 Amazon EC2 主控台的彈性區塊存放區功能表上，選擇快照。
2. 搜尋您要還原的快照，然後選取它。
3. 選擇動作，然後選擇建立磁碟區。
4. 在與 EC2 執行個體相同的可用區域中建立新的磁碟區。
5. 在 Amazon EC2 主控台上，選取執行個體。
6. 在執行個體詳細資訊中，記下您要在根裝置項目或封鎖裝置項目中取代的裝置名稱。
7. 連接磁碟區。根磁碟區和非根磁碟區的程序不同。

   對於根磁碟區：

   a. 停止 EC2 執行個體。
   b. 在 EC2 Elastic Block Store Volumes 功能表中，選取您要取代的根磁碟區。
   c. 選擇動作，然後選擇分離磁碟區。
   d. 在 EC2 Elastic Block Store Volumes 功能表中，選取新的磁碟區。
   e. 選擇動作，然後選擇連接磁碟區。
   f. 選取您要連接磁碟區的執行個體，並使用您先前記下的相同裝置名稱。

   對於非根磁碟區：

   a. 在 EC2 Elastic Block Store Volumes 功能表中，選取您要取代的非根磁碟區。
   b. 選擇動作，然後選擇分離磁碟區。
   c. 在 EC2 彈性區塊存放磁碟區功能表中選擇新磁碟區，然後選擇動作、連接磁碟區，以連接新磁碟區。選取您要附加的執行個體，然後選取可用的裝置名稱。
   d. 使用執行個體的作業系統，卸載現有的磁碟區，然後將新的磁碟區掛載到其位置。

      在 Linux 中，您可以使用 `umount`命令。在 Windows 中，您可以使用邏輯磁碟區管理員 (LVM)，例如磁碟管理系統公用程式。
   e. 在 EC2 Elastic Block Store Volumes 功能表中選擇磁碟區，然後選擇動作、分離磁碟區，以分離您可能要取代的任何先前磁碟區。

您也可以使用 AWS CLI 搭配作業系統命令來自動化這些步驟。

從 EBS 快照建立或還原 EC2 執行個體

若要建立用來還原整個 EC2 執行個體的備份，建議您建立 Amazon Machine Image (AMI)。AMIs會擷取機器資訊，例如虛擬化類型。它們也會為每個連接到 EC2 執行個體的磁碟區建立快照，包括其裝置映射，以便可在相同的組態中還原這些磁碟區。

> **Note**
>
> 在大多數情況下，適用於 Windows、Red Hat、SUSE 和 SQL Server AMIs 需要正確的授權資訊，才能出現在 AMI 上。如需詳細資訊，請參閱了解 AMI 帳單資訊。當從快照建立 AMI 時，`RegisterImage` 操作會從快照的中繼資料衍生出正確帳單資訊，但這需要有適當的中繼資料。若要驗證是否已套用正確帳單資訊，請參閱新 AMI 的平台詳細資料欄位。如果欄位空白或不符合預期的作業系統程式碼（例如 Windows、Red Hat、SUSE 或 SQL)，則 AMI 建立失敗，您應該捨棄 AMI，並遵循從執行個體建立 AMI 中的指示。

如果您必須使用 EBS 快照來還原執行個體，請先從 EBS 快照建立 AMI，該快照將成為新 EC2 執行個體的根磁碟區：

1. 在 Amazon EC2 主控台的彈性區塊存放區功能表上，選擇快照。
2. 搜尋將用於為新 EC2 執行個體建立根磁碟區的快照，並加以選取。
3. 選擇動作，然後選擇從快照建立映像。
4. 輸入映像的名稱（例如 `YYYYMMDD-restore-for-i-012345678998765de`)，並為新映像選擇適當的選項。
5. （僅限 Windows、Red Hat、SUSE 和 SQL Server) 若要驗證是否已套用正確的帳單資訊，請檢查新 AMI 上的平台詳細資訊欄位。如果欄位空白或不符合預期的作業系統程式碼（例如 Windows 或 Red Hat)，則 AMI 建立失敗，您應該捨棄 AMI，並遵循從執行個體建立 AMI 中的指示。

建立映像並可供使用之後，您可以啟動新的 EC2 執行個體，該執行個體將使用根磁碟區的 EBS 快照。

從 AMI 還原執行中的執行個體

您可以從 AMI 備份中提取新的執行個體，以取代現有的執行中執行個體。其中一種方法是停止現有執行個體、讓它在您從 AMI 啟動新執行個體時保持離線，以及執行任何必要的更新。此方法可降低兩個

執行個體同時執行時產生衝突的風險。如果您的執行個體提供的服務已關閉，或是您在維護時段執行還原，這是可接受的方法。測試新執行個體之後，您可以重新指派任何配置給舊執行個體的彈性 IP 地址。然後，您可以更新任何網域名稱服務 (DNS) 記錄，以指向新的執行個體。

不過，如果在還原期間，您必須將服務中執行個體的停機時間降至最低，請考慮從 AMI 備份啟動和測試新的執行個體。然後將現有執行個體取代為新的執行個體。

當兩個執行個體都在執行時，您必須防止新的執行個體造成任何平台層級或應用程式層級的衝突。例如，您可能會遇到使用相同 SIDs和電腦名稱執行的網域加入 Windows 執行個體問題。您可能會遇到類似需要唯一識別符的網路應用程式和服務問題。

若要防止其他伺服器和服務在新執行個體準備就緒之前就連線到您的新執行個體，請使用安全群組暫時封鎖新執行個體的所有傳入連線，但您自己的 IP 地址除外，以便存取和測試。您也可以暫時封鎖新執行個體的傳出連線，以防止服務和應用程式啟動任何連線或更新其他資源。當新執行個體準備就緒時，請停止現有執行個體、在新執行個體上啟動服務和程序，然後取消封鎖您實作的任何傳入或傳出網路連線。

從內部部署基礎設施備份和復原至 AWS

您可以使用 AWS 來儲存現場部署基礎設施備份的耐用、異地儲存。在此案例中使用 AWS 儲存服務，您可以專注於備份和封存任務。您不需要擔心備份任務的儲存基礎設施佈建、擴展或基礎設施容量。

Amazon S3 提供廣泛的 API 操作和SDKs可整合到新的和現有的備份和復原方法中。這也為備份軟體供應商提供了直接整合其應用程式與 AWS 儲存解決方案的方法。

在此案例中，備份和封存您在內部部署基礎設施中使用的軟體， AWS 會透過 API 操作直接與 互動。因為備份軟體很 AWS清楚，所以會將現場部署伺服器的資料直接備份到 Amazon S3。

如果您現有的備份軟體原生不支援 AWS 雲端，您可以使用 Storage Gateway。Storage Gateway 是一種雲端儲存服務，可讓您的內部部署系統存取可擴展的雲端儲存。它支援開放式標準儲存協定，可搭配您現有的應用程式使用，同時安全地將加密的資料儲存在 Amazon S3 中。您可以使用 Storage Gateway 做為內部部署區塊型儲存工作負載備份和復原方法的一部分。

Storage Gateway 在您想要轉換至雲端儲存以進行備份的混合式案例中很有用。Storage Gateway 也可協助您減少內部部署儲存的資本投資。您可以將 Storage Gateway 部署為 VM 或專用硬體設備。本指南著重於 Storage Gateway 如何套用至備份和復原。

Storage Gateway 提供三種不同的選項以滿足不同的需求：

- 使用 SMB 型或 NFS 型存取，在 Amazon S3 雲端儲存上將應用程式資料檔案和備份映像儲存為耐久物件的檔案閘道。
- 將雲端型 iSCSI 區塊儲存磁碟區呈現至內部部署應用程式的磁碟區閘道。磁碟區閘道提供本機快取或內部部署的完整磁碟區，同時將 AWS 磁碟區的完整複本儲存在 雲端。
- 磁帶閘道，用於指向內部部署儲存閘道的受信任備份軟體，進而連接到 Amazon S3。此選項提供雲端的擴展和耐久性，以安全、長期保留，而不會中斷現有的投資或程序。

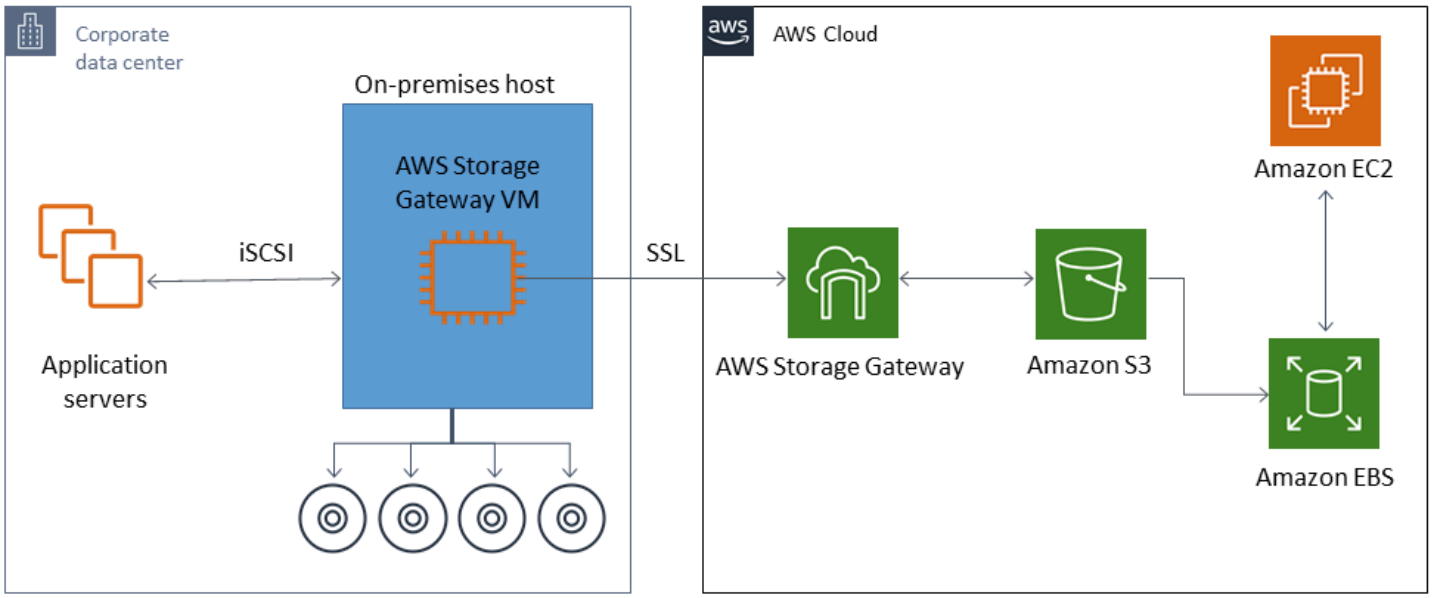
檔案閘道

許多組織透過將備份等次要和第三級資料移至雲端，開始其雲端之旅。檔案閘道的 SMB 和 NFS 介面支援，可讓 IT 群組將備份任務從現有的現場部署備份系統轉移到雲端。可以寫入 SMB 或 NFS 的備份應用程式、原生資料庫工具或指令碼可以寫入檔案閘道。檔案閘道會將備份儲存為大小上限為 5 TiB 的 Amazon S3 物件。透過大小適中的本機快取，最近的備份可用於快速現場復原。長期保留需求是透過將備份分層為低成本 S3 標準不常存取和 S3 Glacier 儲存類別來解決。

檔案閘道為 Amazon S3 提供區塊型儲存的 on ramp 功能，以進行高度耐用的異地備份。對於必須快速還原最近備份檔案的情況特別有用。由於檔案閘道支援 SMB 和 NFS 通訊協定，因此使用者可以以存取網路檔案共用的方式存取檔案。您也可以利用 Amazon S3 物件版本控制功能。使用物件版本控制，您可以還原檔案的舊物件版本，然後使用 SMB 或 NFS 輕鬆存取它們。

磁碟區閘道

磁碟區閘道可讓您為內部部署伺服器佈建雲端型 iSCSI 區塊儲存磁碟區。磁碟區閘道會將您的磁碟區資料存放到 Amazon S3，以提供持久、可擴展的雲端型異地儲存。磁碟區閘道有助於擷取磁碟區的完整point-in-time快照，並將其以 Amazon EBS 快照的形式存放在雲端。儲存為快照後，整個磁碟區可以還原為 EBS 磁碟區並連接到 EC2 執行個體，以加速雲端 DR 解決方案。磁碟區也可以還原至 Storage Gateway，讓您的現場部署應用程式還原至先前的狀態。



由於磁碟區閘道與 Amazon EC2 的 Amazon EBS 磁碟區功能整合，因此您可以使用 AWS Backup 來自動化和排程快照程序。磁碟區閘道可為您提供耐用、Amazon S3 支援的 Amazon EBS 快照和標記功能的額外優勢。如需詳細資訊，請參閱 Amazon EBS 快照文件。

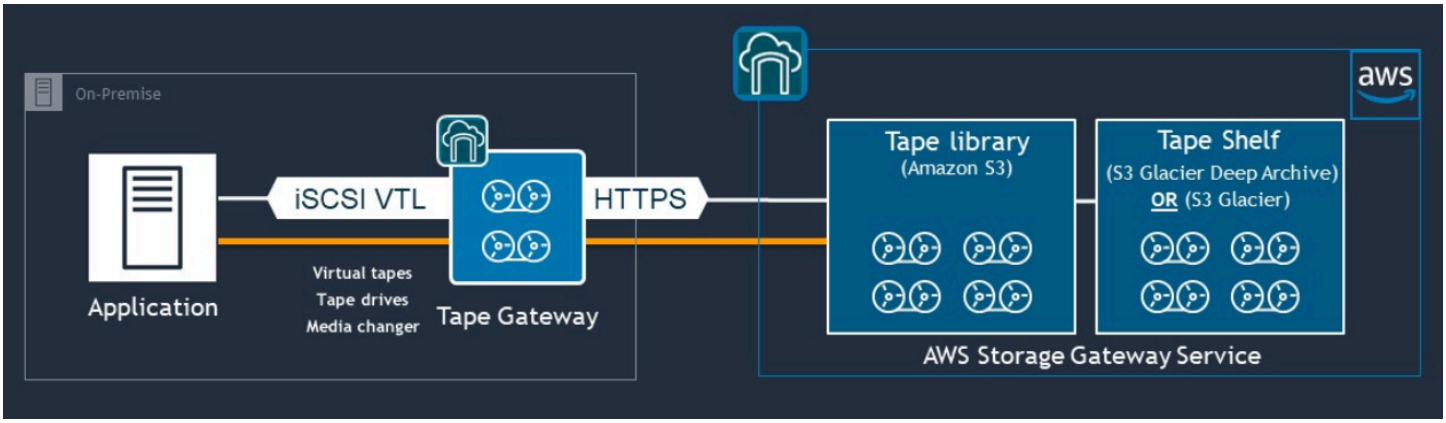
磁帶閘道

磁帶閘道為您的異地虛擬磁帶備份存放區提供 Amazon S3 的高耐用性、低成本分層儲存和廣泛的功能。存放在 Amazon S3 中的所有虛擬磁帶都會複寫並存放在至少三個分散地理的可用區域。您的虛擬磁帶受到 11 九個耐用性的保護。

AWS 也會定期執行修正性檢查，以確認您的資料可以讀取，而且沒有發生錯誤。存放在 Amazon S3 中的所有磁帶都會使用預設金鑰或您的 AWS KMS 金鑰，受到伺服器端加密的保護。此外，您可以避

免與磁帶可攜性相關的實體安全風險。使用磁帶閘道時，相較於磁帶的異地倉儲，您可以取得正確的資料，在還原期間，您可能會收到不正確或損壞的磁帶。

在 Amazon S3 中儲存資料時，您可以節省每月儲存成本。您可以使用 S3 Glacier Deep Archive，為您的長期封存需求省下更多。



磁帶閘道可做為虛擬磁帶程式庫 (VTL)，從現場部署環境延伸至高度可擴展、備援且耐用的儲存服務：Amazon S3、S3 Glacier Flexible Retrieval 和 S3 Glacier Deep Archive。

磁帶閘道會將 Storage Gateway 做為開放標準 iSCSI 型 VTL 呈現給現有的備份應用程式，並搭配虛擬媒體變更器和虛擬磁帶機。您可以繼續使用現有的備份應用程式和工作流程，同時寫入存放在大規模可擴展 Amazon S3 上的虛擬磁帶集合。當您不再需要立即或頻繁存取虛擬磁帶上的資料時，備份應用程式可以將資料封存到 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive，進一步降低儲存成本。

您可以擷取存檔在 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 中的磁帶，通常分別在 3-5 小時或 12 小時內。磁帶閘道可與備份應用程式搭配使用，該備份應用程式與存取虛擬磁帶的 iSCSI 型磁帶程式庫介面相容。另請考慮每個磁帶的最小 100-GB儲存大小。如需詳細資訊，請檢閱支援磁帶閘道的第三方備份應用程式清單。

從 備份和復原應用程式 AWS 至您的資料中心

您可能有一項政策，要求您為雲端工作負載和內部部署基礎設施實作 DR 或業務連續性等案例。如果您已經有現場部署伺服器的資料備份架構，您可以透過 VPN 連線或透過 將其擴展到您的 AWS 資源 AWS Direct Connect。您可以在 EC2 執行個體上安裝備份代理程式，並根據資料保護政策備份您的資料和應用程式。您也可以使用 Amazon S3 作為中繼服務來存放應用程式層級備份。然後，您可以使用 API 操作、SDKs或 AWS CLI ，將資料還原至您的內部部署環境。

若要備份 Amazon EC2 以外的 AWS 服務中的資料，請使用 、 AWS CLI SDKs和 API 操作，以您想要的格式擷取資料。然後將資料複製到 Amazon S3，然後從 Amazon S3 複製到您的內部部署環境。有些 服務提供直接匯出至 Amazon S3。例如，Amazon RDS 支援將 Microsoft SQL Server 資料庫原生備份至 Amazon S3。

雲端原生 AWS 服務的備份和復原

您的備份和復原方法應涵蓋工作負載中使用的 AWS 服務。 AWS 提供服務特定的功能和選項，用於管理和與資料互動。您可以使用 主控台、 AWS CLI、 SDKs和 API 操作，為您正在使用 AWS 的服務實作備份和復原。本指南涵蓋 Amazon RDS 和 Amazon DynamoDB 作為範例。 同時 AWS Backup 支援 DynamoDB 和 Amazon RDS，如果符合您的需求，則應使用 。

Amazon RDS 的備份和復原

Amazon RDS 包含自動化資料庫備份的功能。Amazon RDS 會建立資料庫執行個體的儲存磁碟區快照，備份整個資料庫執行個體，而非僅限個別資料庫。使用 Amazon RDS，您可以建立自動備份的備份時段、建立資料庫執行個體快照，以及跨區域和帳戶共用和複製快照。

Amazon RDS 提供兩種不同的選項來備份和還原資料庫執行個體：

- 自動化備份提供資料庫執行個體的point-in-time復原 (PITR)。當您建立新的資料庫執行個體時，預設會開啟自動備份。

  Amazon RDS 會在您建立資料庫執行個體時定義的備份時段期間執行資料的每日備份。您可以為自動備份設定最長 35 天的保留期。Amazon RDS 也會每 5 分鐘將資料庫執行個體的交易日誌上傳至 Amazon S3。Amazon RDS 使用您的每日備份以及資料庫交易日誌來還原資料庫執行個體。您可以在保留期間將執行個體還原至任何秒，最多可還原至 `LatestRestorableTime`（通常為最後五分鐘）。

  若要尋找資料庫執行個體的最新可還原時間，請使用 `DescribeDBInstances` API 呼叫。或查看 Amazon RDS 主控台上資料庫的描述索引標籤。

  當您啟動 PITR 時，交易日誌會與最適當的每日備份結合，以將資料庫執行個體還原至請求的時間。
- 資料庫快照是使用者啟動的備份，您可以視需要頻繁地將資料庫執行個體還原至已知狀態。然後，您可以隨時還原到該狀態。您可以使用 Amazon RDS 主控台或 `CreateDBSnapshot` API 呼叫來建立資料庫快照。這些快照會保留，直到您使用 主控台或 `DeleteDBSnapshot` API 呼叫來明確刪除為止。

中的 Amazon RDS 支援這兩種備份選項 AWS Backup，這也提供其他功能。請考慮使用 AWS Backup 為您的 Amazon RDS 資料庫設定標準備份計劃，並在特定資料庫的備份計劃是唯一的時，使用使用者啟動的執行個體備份選項。

Amazon RDS 可防止直接存取資料庫執行個體所使用的基礎儲存體。這也可讓您直接將 RDS 資料庫執行個體上的資料庫匯出至其本機磁碟。在某些情況下，您可以使用用戶端公用程式來使用原生備份和還原函數。例如，您可以使用 mysqldump 命令搭配 Amazon RDS MySQL 資料庫，將資料庫匯出至本機用戶端機器。在某些情況下，Amazon RDS 也提供增強型選項，以執行資料庫的原生備份和還原。例如，Amazon RDS 提供預存程序來匯出和匯入 SQL Server 資料庫的 RDS 資料庫備份。

作為整體備份和還原方法的一部分，請務必徹底測試資料庫還原程序及其對資料庫用戶端的影響。

使用 DNS CNAME 記錄來降低資料庫復原期間的用戶端影響

當您使用 PITR 或 RDS 資料庫執行個體快照還原資料庫時，會建立新的資料庫執行個體與新的端點。如此一來，您可以從特定資料庫快照或時間點建立多個資料庫執行個體。當您還原 RDS 資料庫執行個體以取代即時 RDS 資料庫執行個體時，有特殊考量。例如，您必須判斷如何將現有資料庫用戶端重新導向至新的執行個體，且中斷和修改最少。您也必須在新執行個體開始接收寫入時，考慮還原的資料時間和復原時間，以確保資料庫內資料的連續性和一致性。

您可以建立指向資料庫執行個體端點的個別 DNS CNAME 記錄，並讓用戶端使用此 DNS 名稱。然後，您可以更新 CNAME 以指向新的已還原端點，而無需更新資料庫用戶端。

將 CNAME 記錄的存留時間 (TTL) 設定為適當的值。您指定的 TTL 會決定在發出另一個請求之前，記錄會與 DNS 解析程式一起快取多久。請務必注意，某些 DNS 解析程式或應用程式可能無法遵守 TTL，而且快取記錄的時間可能會超過 TTL。對於 Amazon Route 53，如果您指定較長的值（例如 172800 秒或兩天），您可以減少 DNS 遞迴解析程式必須對 Route 53 進行的呼叫數量，以取得此記錄中的最新資訊。這可減少延遲，並減少 Route 53 服務的帳單。如需詳細資訊，請參閱 Amazon Route 53 如何路由網域的流量。

應用程式和用戶端作業系統也可能快取您必須排清或重新啟動的 DNS 資訊，以啟動新的 DNS 解析請求，並擷取更新的 CNAME 記錄。

當您啟動資料庫還原並將流量轉移到還原的執行個體時，請確認您的所有用戶端正在寫入還原的執行個體，而不是先前的執行個體。您的資料架構可能支援還原資料庫、更新 DNS 以將流量轉移到還原的執行個體，然後修復可能仍會寫入先前執行個體的任何資料。如果不是這種情況，您可以在更新 DNS CNAME 記錄之前停止現有的執行個體。然後，所有存取都是來自新還原的執行個體。這可能會對您可以個別處理的某些資料庫用戶端暫時造成連線問題。若要降低用戶端影響，您可以在維護時段期間執行資料庫還原。

編寫您的應用程式，以使用指數退避來正常處理資料庫連線失敗。這可讓應用程式在還原期間無法使用資料庫連線時復原，而不會導致應用程式意外當機。

完成還原程序後，您可以將先前的執行個體保持在停止狀態。或者，您可以使用安全群組規則來限制先前執行個體的流量，直到您滿意不再需要為止。對於漸進停用方法，請先限制安全群組對執行中資料庫的存取。您最終可以在不再需要執行個體時停止執行個體。最後，拍攝資料庫執行個體的快照並刪除它。

DynamoDB 的備份和復原

DynamoDB 提供 PITR，可幾乎持續備份 DynamoDB 資料表資料。啟用時，DynamoDB 會維護資料表過去 35 天的增量備份，直到您明確將其關閉為止。

您也可以使用 DynamoDB 主控台、 或 DynamoDB API AWS CLI，建立 DynamoDB 資料表的隨需備份。如需詳細資訊，請參閱備份 DynamoDB 資料表。您可以使用 來排程定期或未來的備份 AWS Backup，也可以使用 Lambda 函數來自訂和自動化備份方法。如需使用 Lambda 函數備份 DynamoDB 的詳細資訊，請參閱部落格文章 無伺服器解決方案，以排程您的 Amazon DynamoDB 隨需備份。如果您不想建立排程指令碼和清除任務，您可以使用 AWS Backup 來建立備份計劃。備份計劃包含 DynamoDB 資料表的排程和保留政策。 會根據保留排程 AWS Backup 建立備份並刪除先前的備份。 AWS Backup 也包含 DynamoDB 服務中無法使用的進階 DynamoDB 備份選項，包括成本較低的分層儲存，以及跨帳戶和跨區域複本。如需詳細資訊，請參閱進階 DynamoDB 備份。

您必須在還原的 DynamoDB 資料表上手動設定下列項目：

- 自動擴展政策
- IAM 政策
- Amazon CloudWatch 指標和警示
- 標籤
- 串流設定
- TTL 設定

您只能從備份將整個資料表資料還原至新資料表。您只能在還原的資料表變為作用中之後，才可寫入資料表。

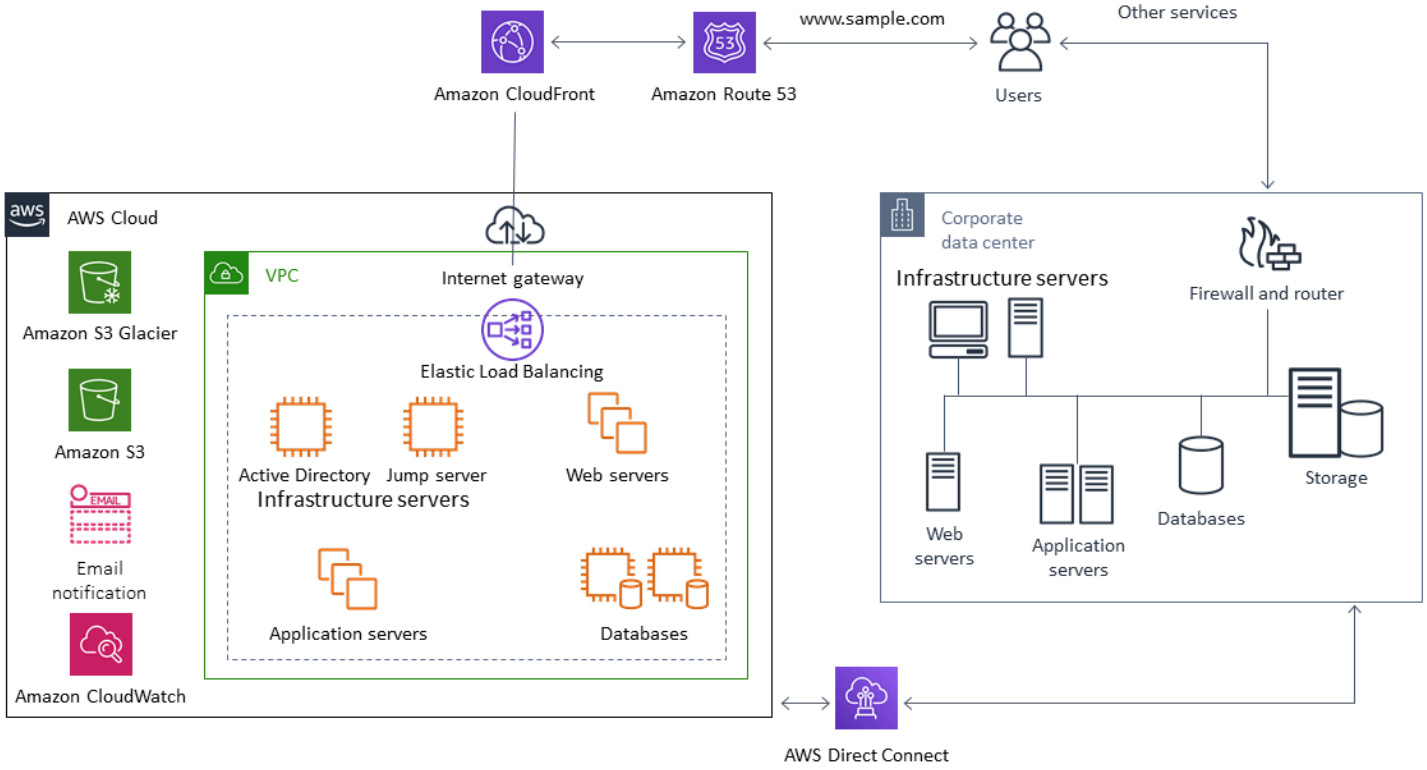
您的還原程序必須考慮用戶端將如何被引導使用新還原的資料表名稱。您可以設定應用程式和用戶端，從組態檔案、 AWS Systems Manager 參數存放區值或其他可動態更新的參考擷取 DynamoDB 資料表名稱，以反映用戶端應使用的資料表名稱。

作為還原程序的一部分，您應該仔細考慮切換程序。您可以選擇拒絕透過 IAM 許可存取現有的 DynamoDB 資料表，並允許存取您的新資料表。然後，您可以更新應用程式和用戶端組態，以使用新的資料表。您可能還需要協調現有 DynamoDB 資料表和新還原的 DynamoDB 資料表之間的差異。

混合架構的備份和復原

本指南中討論的雲端原生和內部部署可以合併為工作負載環境具有內部部署和 AWS 基礎設施元件的混合式案例。資源，包括 Web 伺服器、應用程式伺服器、監控伺服器、資料庫和 Microsoft Active Directory，都託管在客戶資料中心或 上 AWS。在 AWS Cloud 中執行的應用程式會連接到在內部部署中執行的應用程式。

這已成為企業工作負載的常見案例。許多企業都有自己的資料中心，並用來 AWS 增加容量。這些客戶資料中心通常透過高容量 AWS 網路連結連接到網路。例如，使用 AWS Direct Connect，您可以從現場部署資料中心建立私有的專用連線 AWS。這可提供頻寬和一致的延遲，以將資料上傳到雲端，以用於資料保護。它也為混合工作負載提供一致的效能和延遲。下圖提供混合環境方法的一個範例。



設計良好的資料保護解決方案通常使用本指南中雲端原生和內部部署解決方案中所述的選項組合。許多 ISVs為內部部署基礎設施提供市場領先的備份和還原解決方案，並已擴展其解決方案以支援混合方法。

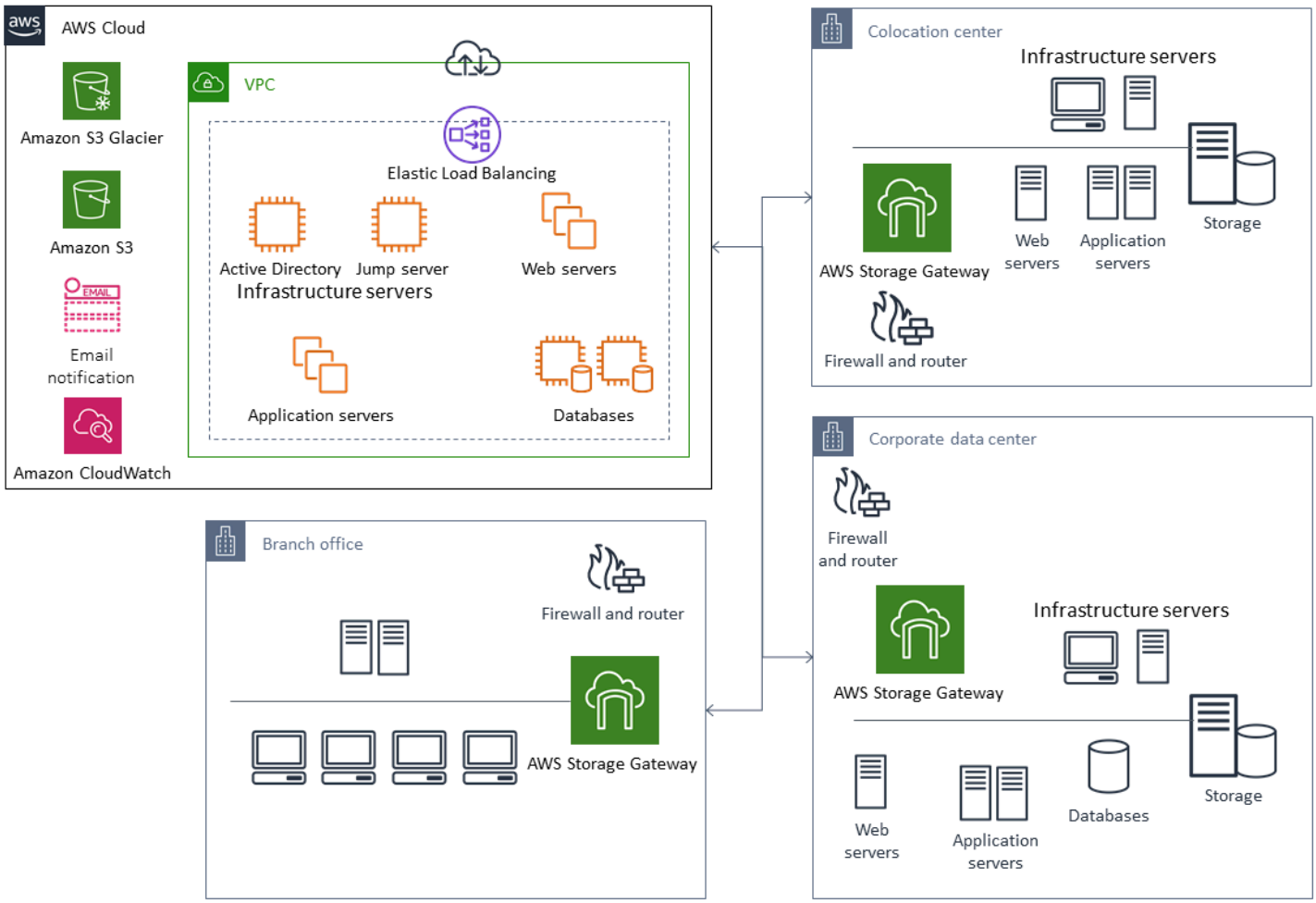
將集中式備份管理解決方案移至雲端，以提高可用性

透過使用現有的備份管理解決方案投資 AWS，您可以改善方法的彈性和架構。您可能有一個主要備份伺服器，以及一個或多個媒體或儲存伺服器，位於多個位置的內部部署，靠近他們保護的伺服器和服

務。在這種情況下，請考慮將主要備份伺服器移至 EC2 執行個體，以保護其免受內部部署災難和高可用性的影響。

若要管理備份資料流程，您可以在與其將保護的伺服器相同的區域中，在 EC2 執行個體上建立一或多個媒體伺服器。EC2 執行個體附近的媒體伺服器可節省網際網路傳輸的成本。當您備份至 Amazon S3 時，媒體伺服器會提高整體備份和復原效能。

您也可以使用 Storage Gateway，從分散地理的資料中心和辦公室提供資料的集中式雲端存取。例如，檔案閘道可讓您隨需、低延遲地存取儲存在 中的資料， AWS 以供跨全球的應用程式工作流程使用。您可以使用快取重新整理等功能來重新整理分散地理位置中的資料，以便在辦公室之間輕鬆共用內容。



使用 進行災難復原 AWS

備份和還原方法以及支援服務和技術可用來實作您的災難復原 (DR) 解決方案。許多企業使用 AWS 雲端進行備份和還原，並以 DR 網站的形式進行。 AWS 提供許多支援 DR 和業務連續性的服務和功能。

主題

- 內部部署 DR 至 AWS
- 雲端原生工作負載的 DR

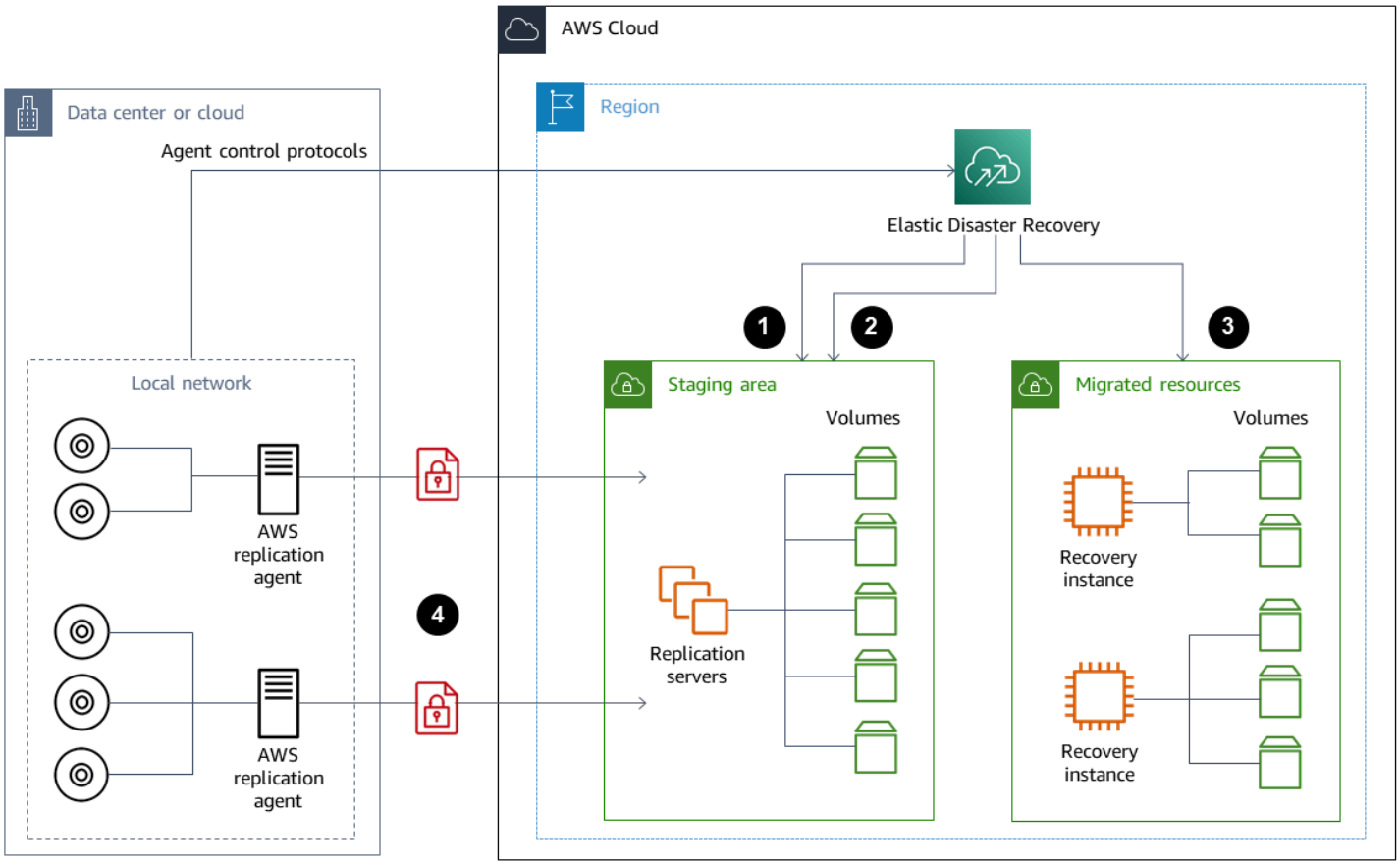
內部部署 DR 至 AWS

使用 AWS 做為現場部署工作負載的異地災難復原 (DR) 環境是常見的混合情況。在選取要使用的技術之前，定義您的 DR 目標，包括必要的復原時間和復原點目標。若要協助處理此定義，您可以使用 DR 計劃檢查清單。

有許多選項可協助您快速設定和佈建 DR 環境 AWS。請務必考慮所有工作負載相依性，並徹底定期測試 DR 計畫和解決方案，以確認其完整性。

AWS AWS Elastic Disaster Recovery提供建立內部部署伺服器的完整複本，包括根磁碟區和作業系統 AWS。Elastic Disaster Recovery 會持續將您的機器複寫到目標 AWS 帳戶中的低成本暫存區域，並且是首選 AWS 區域。區塊層級複寫是伺服器儲存體的確切複本，包括作業系統、系統狀態組態、資料庫、應用程式和檔案。如果發生災難，您可以指示 Elastic Disaster Recovery 在幾分鐘內快速啟動數千部機器，處於完全佈建的狀態。

Elastic Disaster Recovery 會使用安裝在您每個現場部署伺服器上的代理程式。代理程式會將現場部署伺服器的狀態與執行於 的低功率 Amazon EC2 對等同步 AWS。您也可以使用 Elastic Disaster Recovery 自動化 DR 容錯移轉和容錯回復程序。自動化容錯移轉和容錯回復程序，可協助您達成較低且更一致的復原時間目標 (RTO)。



1. 複寫伺服器狀態報告
2. 自動建立和終止暫存區域資源
3. 啟動的復原執行個體 RTO 為 分鐘，RPO 為 秒
4. 持續區塊層級複寫（壓縮和加密）

請務必測試 DR 程序，並確認即時預備環境不會與內部部署環境產生衝突。例如，確認您的內部部署、預備和起始的 DR 環境中有適當的授權可用且正常運作。同時確認可能輪詢並從中央資料庫提取工作的任何工作者類型程序已適當設定，以避免重疊或衝突。在您的 DR 程序中，包含復原伺服器執行個體上線之前必須執行的任何必要步驟。也包含復原伺服器執行個體上線且可供使用後執行的步驟。您可以使用AWS Elastic Disaster Recovery 計劃自動化解決方案或其他方法來協助您自動化 DR 計劃。

您可以使用 Storage Gateway 磁碟區閘道，為內部部署伺服器提供雲端磁碟區。這些磁碟區也可以使用 Amazon EBS 快照快速佈建，以與 Amazon EC2 搭配使用。特別是，儲存的磁碟區閘道可讓您的現場部署應用程式低延遲存取其整個資料集。磁碟區閘道也提供持久的快照型備份，可還原供內部部署使用或與 Amazon EC2 搭配使用。您可以根據工作負載的復原point-in-time快照。

> **Important**
>
> 磁碟區閘道磁碟區旨在用作資料磁碟區，而不是開機磁碟區。

您可以使用 Amazon EC2 Amazon Machine Image (AMI) 搭配符合現場部署伺服器的組態，並分別指定您的資料磁碟區。在您設定和測試 AMI 之後，請根據磁碟區閘道快照，從 AMI 佈建 EC2 執行個體以及資料磁碟區。此方法需要您徹底測試您的環境，以確認 EC2 執行個體是否正常運作，特別是 Windows 工作負載。

雲端原生工作負載的 DR

考慮您的雲端原生工作負載如何與您的 DR 目標保持一致。 在全球區域 AWS 提供多個可用區域。許多使用 AWS 雲端的企業會調整工作負載架構和 DR 目標，以承受可用區域的損失。 AWS Well-Architected Framework 中的可靠性支柱支援此最佳實務。您可以建構工作負載及其服務和應用程式相依性，以使用多個可用區域。然後，您可以自動化您的 DR 並實現您的 DR 目標，而只需最少或無需介入。

不過，實際上，您可能會發現您無法為所有元件建立備援、作用中和自動化的架構。檢查架構的每一層，以判斷實現目標所需的 DR 程序。這可能因工作負載而異，具有不同的架構和服務需求。本指南涵蓋 Amazon EC2 的考量事項和選項。對於其他服務 AWS ，您可以參考 AWS 文件來判斷高可用性和 DR 選項。

單一可用區域中 Amazon EC2 的 DR

嘗試建構您的工作負載，以主動支援和服務來自多個可用區域的用戶端。您可以使用 Amazon EC2 Auto Scaling 和 Elastic Load Balancing 來實現 Amazon EC2 和其他服務的多可用區域伺服器架構。

如果您的架構具有無法平衡負載的 EC2 執行個體，且在任何指定時間只能執行單一執行個體，您可以使用下列其中一個選項。

- 建立 Auto Scaling 群組，其大小下限、上限和所需大小為 1，並針對多個可用區域進行設定。建立 AMI，以便在執行個體失敗時用來取代執行個體。請務必定義適當的自動化和組態，以便自動設定 AMI 的新佈建執行個體並提供服務。建立指向 Auto Scaling 群組並針對多個可用區域設定的負載平衡器。或者，建立指向負載平衡器端點的 Amazon Route 53 別名。
- 為您的作用中執行個體建立 Route 53 記錄，並讓您的用戶端使用此記錄進行連線。建立指令碼，以建立作用中執行個體的新 AMI，並使用 AMI 在個別可用區域中，以停止狀態佈建新的 EC2 執行個

體。將指令碼設定為定期執行，並終止先前停止的執行個體。如果發生可用區域故障，請在替代可用區域中啟動備份執行個體。然後更新 Route 53 記錄以指向此新執行個體。

透過模擬解決方案旨在防範的失敗，徹底測試您的解決方案。另請考慮 DR 解決方案在工作負載架構變更時所需的更新。

區域故障時 Amazon EC2 的 DR

具有極高可用性需求（例如，任務關鍵型應用程式無法容忍任何停機時間）的客戶可以在多個區域 AWS 使用 ，以進一步恢復區域層級的問題。客戶必須仔細權衡建立和維護多區域 DR 計劃與 利益所需的複雜性、成本和工作量。 AWS 提供支援多區域架構的功能，以用於全域可用性、容錯移轉和 DR。 本指南涵蓋一些 Amazon EC2 備份和復原特定的可用功能。

AWS AMIs 和 Amazon EBS 快照是區域資源，可用於在單一區域中佈建新的執行個體。不過，您可以將快照和 AMIs 複製到另一個區域，並使用它們在該區域中佈建新的執行個體。若要支援區域故障 DR 計畫，您可以將 AMIs和快照複製到其他區域的程序自動化。 AWS Backup Amazon Data Lifecycle Manager 支援跨區域複製，做為備份組態的一部分。

AWS Elastic Disaster Recovery 可用來自動化並持續將您的 Amazon EC2 伺服器複寫至其他 DR 區域。Elastic Disaster Recovery 可以簡化多區域 DR 方法，並協助您使用演練定期測試跨區域 Amazon EC2 DR 計劃。當備份和復原無法滿足您的 RTO 和 RPO 目標時，Elastic Disaster Recovery 可以提供協助。Elastic Disaster Recovery 可協助您將 RTO 降至 分鐘，並將 RPO 降至次秒範圍。

無論您使用哪種解決方案，都必須判斷在發生中斷時要使用的佈建、容錯移轉和容錯回復程序。您可以使用 Route 53 搭配運作狀態檢查和網域名稱系統容錯移轉，以協助支援您的解決方案。

清除備份

若要降低成本，請清除復原或保留目的不再需要的備份。您可以使用 AWS Backup 和 Amazon Data Lifecycle Manager 來自動化部分備份的保留政策。不過，即使已備妥這些工具，您仍需要針對個別取得的備份進行清理方法。

標記策略是清除策略的先決條件。使用標記來識別應該清除的資源、適當地通知擁有者，並自動化清除程序。建立的備份 AWS 具有與其一致的建立日期，但標記對於將備份與工作負載、保留要求和還原點識別相關聯很重要。

您可以使用自動化實作快照的清除程序。例如，您可以掃描帳戶是否有快照，並判斷對應的磁碟區是否處於連接狀態或可用狀態。您可以根據指定的時間閾值進一步篩選結果。使用連接到磁碟區的標籤，您可以自動傳送電子郵件給快照擁有者，並警告他們其快照已排定刪除。此自動化修復可以透過使用 AWS Config 規則、使用 的指令碼 AWS CLI，或使用 AWS SDK 的 Lambda 函數來實作。

Systems Manager 提供 AWS-DeleteEBSVolumeSnapshots和 AWS-DeleteSnapshot 文件，協助您啟動和自動化 Amazon EBS 快照的清除。您也可以使用 AWS CLI 和 AWS SDK 自動清除其他 AWS 資源，例如 Amazon RDS 快照。

備份和復原常見問答集

我應該選取哪些備份排程？

定義符合您復原點目標 (RPO) 的備份排程頻率。定義工作負載低於最低負載量的備份時間，以及可降低使用者影響的時間。每當您要對工作負載進行重大變更時，請建立point-in-time快照。

我需要在開發帳戶中建立備份嗎？

在執行重大變更之前，先測試開發帳戶中的可能重大變更，並建立備份。您的開發和非生產帳戶中，可能還有更多來自開發和測試活動的point-in-time復原 (PITR) 備份。

在建立快照時，是否可以升級應用程式並繼續使用 EBS 磁碟區，而不會有任何影響？

快照會以非同步方式發生；point-in-time快照會立即建立，但快照的狀態會待定，直到所有修改過的區塊都已傳輸至 Amazon S3。對於變更許多區塊的大型初始快照或後續快照，傳輸可能需要幾個小時。傳輸時，進行中的快照不受持續讀取和寫入磁碟區的影響。如需詳細資訊，請參閱 AWS 文件。

後續步驟

首先評估、實作和測試非生產環境中的備份和復原方法。請務必徹底測試復原程序，並驗證還原的工作負載是否如預期般運作。

測試架構中單一元件的還原程序，以及架構中的所有元件。驗證每個 的復原時間。同時驗證備份和還原程序對上游和下游相依性的影響。確認任何服務中斷對上游相依性的影響，並確認對備份的下游影響。

其他資源

AWS 資源

- AWS 規範性指導
- AWS 文件
- AWS 一般參考
- AWS 詞彙表

AWS 服務

- AWS Backup
- Amazon CloudWatch
- AWS Config
- Amazon DynamoDB
- Amazon EBS
- Amazon EC2
- Amazon EventBridge
- IAM
- Amazon RDS
- Amazon Simple Storage Service (Amazon S3)
- Storage Gateway
- AWS Systems Manager

其他資源

- 使用（解決方案）備份和復原 AWS Backup
- 上工作負載的災難復原 AWS：雲端中的復原（白皮書）
- 災難復原系列 (AWS 架構部落格文章）
- IT 災難復原計劃檢查清單
- 使用 備份和復原方法 AWS（技術論文 – 封存）
- 入門 AWS Backup

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
更新資訊	已更新 Amazon S3 章節中的指引。	2024 年 6 月 28 日
更新資訊	將內部部署 DR 中的資訊更新為 AWS 區段。	2023 年 4 月 13 日
新增章節	新增從快照建立或還原執行個體的指引和步驟。	2023 年 3 月 7 日
新增 Elastic Disaster Recovery 的相關資訊並新增說明	在 災難復原 AWS和選擇資料保護 AWS 服務區段中，新增了有關 的資訊 AWS Elastic Disaster Recovery。在具有快照和 AMIs Amazon EC2 備份和復原中，在建立快照或 AMI 之前準備 EBS 磁碟區，以及從 Amazon EBS 快照或 AMI 區段還原，新增了釐清。已新增至備份和復原常見問答集。	2023 年 1 月 19 日
新增連結	在 Amazon Data Lifecycle Manager 區段中新增了 Amazon Data Lifecycle Manager 文件的連結。	2022 年 10 月 31 日
更新資訊	更新還原磁碟區的相關資訊。	2022 年 8 月 30 日
更新資訊和新增章節	在選擇資料保護 AWS 服務區段中，新增了 服務。已新增使用 AWS Backup 進行備份和復原一節。在使用 Amazon S3 和 Amazon S3 Glacier 的備份	2022 年 1 月 28 日

	和復原區段中，新增了有關新 Amazon S3 Glacier 儲存類別的資訊。在具有 EBS 磁碟區的 Amazon EC2 備份和復原區段中，新增文件和其他資訊的連結。在雲端原生 AWS 服務的備份和復原區段中，新增了要使用的建議 AWS Backup。在其他資源區段中，新增了資源。	
更新資訊	已將有關設定儲存類別的資訊新增至 S3 Glacier Flexible Retrieval 區段。已新增有關使用快照和 AMIs 擷取快照至 Amazon EC2 備份和復原的資訊。	2021 年 9 月 9 日
更新資訊	在 AWS Backup區段中，新增了有關 AWS Backup 支援 AWS 服務的資訊。	2021 年 6 月 1 日
初次出版	—	2020 年 7 月 29 日

AWS 規範性指引詞彙表

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

數字

7 R

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

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

A

ABAC

請參閱屬性型存取控制。

抽象服務

請參閱 受管服務。

ACID

請參閱原子性、一致性、隔離性、耐久性。

主動-主動式遷移

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

主動-被動式遷移

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

彙總函數

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

AI

請參閱人工智慧。

AIOps

請參閱人工智慧操作。

匿名化

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

反模式

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

應用程式控制

一種安全方法，僅允許使用核准的應用程式，以協助保護系統免受惡意軟體攻擊。

應用程式組合

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

人工智慧 (AI)

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

人工智慧操作 (AIOps)

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

非對稱加密

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

原子性、一致性、隔離性、耐久性 (ACID)

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

屬性型存取控制 (ABAC)

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

授權資料來源

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

可用區域

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

AWS 雲端採用架構 (AWS CAF)

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

AWS 工作負載資格架構 (AWS WQF)

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

B

錯誤的機器人

旨在中斷或傷害個人或組織的機器人。

BCP

請參閱業務持續性規劃。

行為圖

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

大端序系統

首先儲存最高有效位元組的系統。另請參閱 Endianness。

二進制分類

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

Bloom 篩選條件

一種機率性、記憶體高效的資料結構，用於測試元素是否為集的成員。

藍/綠部署

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

機器人

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

殭屍網路

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

分支

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

碎片存取

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

棕地策略

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

緩衝快取

儲存最常存取資料的記憶體區域。

業務能力

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

業務連續性規劃 (BCP)

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

C

CAF

請參閱AWS 雲端採用架構。

Canary 部署

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

CCoE

請參閱 Cloud Center of Excellence。

CDC

請參閱變更資料擷取。

變更資料擷取 (CDC)

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

混沌工程

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

CI/CD

請參閱持續整合和持續交付。

分類

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

用戶端加密

在目標 AWS 服務 接收資料之前，在本機加密資料。

雲端卓越中心 (CCoE)

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

雲端運算

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

雲端操作模型

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

採用雲端階段

組織在遷移至 時通常會經歷的四個階段 AWS 雲端：

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

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

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

CMDB

請參閱組態管理資料庫。

程式碼儲存庫

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

冷快取

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

冷資料

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

電腦視覺 (CV)

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

組態偏離

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

組態管理資料庫 (CMDB)

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

一致性套件

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

持續整合和持續交付 (CI/CD)

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

CV

請參閱電腦視覺。

D

靜態資料

網路中靜止的資料，例如儲存中的資料。

資料分類

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

資料偏離

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

傳輸中的資料

在您的網路中主動移動的資料，例如在網路資源之間移動。

資料網格

架構架構，提供分散式、分散式資料擁有權與集中式管理。

資料最小化

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

資料周邊

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

資料預先處理

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

資料來源

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

資料主體

正在收集和處理其資料的個人。

資料倉儲

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

資料庫定義語言 (DDL)

用於建立或修改資料庫中資料表和物件之結構的陳述式或命令。

資料庫處理語言 (DML)

用於修改 (插入、更新和刪除) 資料庫中資訊的陳述式或命令。

DDL

請參閱資料庫定義語言。

深度整體

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

深度學習

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

深度防禦

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

委派的管理員

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

部署

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

開發環境

請參閱 環境。

偵測性控制

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

開發值串流映射 (DVSM)

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

數位分身

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

維度資料表

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

災難

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

災難復原 (DR)

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

DML

請參閱資料庫處理語言。

領域驅動的設計

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

DR

請參閱災難復原。

偏離偵測

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

DVSM

請參閱開發值串流映射。

E

EDA

請參閱探索性資料分析。

EDI

請參閱電子資料交換。

邊緣運算

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

電子資料交換 (EDI)

組織之間商業文件的自動交換。如需詳細資訊，請參閱什麼是電子資料交換。

加密

一種運算程序，可將人類可讀取的純文字資料轉換為加密文字。

加密金鑰

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

端序

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

端點

請參閱 服務端點。

端點服務

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

企業資源規劃 (ERP)

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

信封加密

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

環境

執行中應用程式的執行個體。以下是雲端運算中常見的環境類型：

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

epic

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

ERP

請參閱企業資源規劃。

探索性資料分析 (EDA)

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

F

事實資料表

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

快速失敗

一種使用頻繁和增量測試來縮短開發生命週期的理念。這是敏捷方法的關鍵部分。

故障隔離界限

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

功能分支

請參閱分支。

特徵

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

功能重要性

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

特徵轉換

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

少量擷取提示

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

FGAC

請參閱精細存取控制。

精細存取控制 (FGAC)

使用多個條件來允許或拒絕存取請求。

閃切遷移

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

FM

請參閱基礎模型。

基礎模型 (FM)

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

G

生成式 AI

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

地理封鎖

請參閱地理限制。

地理限制 (地理封鎖)

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

Gitflow 工作流程

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

黃金影像

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

綠地策略

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

防護機制

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

H

HA

請參閱高可用性。

異質資料庫遷移

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

高可用性 (HA)

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

歷史現代化

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

保留資料

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

異質資料庫遷移

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

熱資料

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

修補程序

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

超級護理期間

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

I

IaC

將基礎設施視為程式碼。

身分型政策

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

閒置應用程式

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

IIoT

請參閱工業物聯網。

不可變的基礎設施

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

傳入 (輸入) VPC

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

增量遷移

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

工業 4.0

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

基礎設施

應用程式環境中包含的所有資源和資產。

基礎設施即程式碼 (IaC)

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

工業物聯網 (IIoT)

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

檢查 VPC

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

物聯網 (IoT)

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

可解釋性

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

IoT

請參閱物聯網。

IT 資訊庫 (ITIL)

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

IT 服務管理 (ITSM)

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

ITIL

請參閱 IT 資訊庫。

ITSM

請參閱 IT 服務管理。

L

標籤型存取控制 (LBAC)

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

登陸區域

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

大型語言模型 (LLM)

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

大型遷移

遷移 300 部或更多伺服器。

LBAC

請參閱標籤型存取控制。

最低權限

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

隨即轉移

請參閱 7 個 R。

小端序系統

首先儲存最低有效位元組的系統。另請參閱 Endianness。

LLM

請參閱大型語言模型。

較低的環境

請參閱 環境。

M

機器學習 (ML)

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

主要分支

請參閱分支。

惡意軟體

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

受管服務

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

製造執行系統 (MES)

一種軟體系統，用於追蹤、監控、記錄和控制生產程序，將原物料轉換為現場成品。

MAP

請參閱遷移加速計劃。

機制

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

成員帳戶

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

製造執行系統

請參閱製造執行系統。

訊息佇列遙測傳輸 (MQTT)

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

微服務

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

微服務架構

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

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

Migration Acceleration Program (MAP)

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

大規模遷移

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

遷移工廠

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

遷移中繼資料

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

遷移模式

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

遷移組合評定 (MPA)

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

遷移準備程度評定 (MRA)

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

遷移策略

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

機器學習 (ML)

請參閱機器學習。

現代化

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

現代化準備程度評定

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

單一應用程式 (單一)

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

MPA

請參閱遷移產品組合評估。

MQTT

請參閱訊息佇列遙測傳輸。

多類別分類

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

可變基礎設施

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

O

OAC

請參閱原始存取控制。

OAI

請參閱原始存取身分。

OCM

請參閱組織變更管理。

離線遷移

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

OI

請參閱 操作整合。

OLA

請參閱操作層級協議。

線上遷移

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

OPC-UA

請參閱開放程序通訊 - 統一架構。

開放程序通訊 - 統一架構 (OPC-UA)

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

操作水準協議 (OLA)

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

操作整備審查 (ORR)

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

操作技術 (OT)

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

操作整合 (OI)

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

組織追蹤

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

組織變更管理 (OCM)

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

原始存取控制 (OAC)

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

原始存取身分 (OAI)

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

ORR

請參閱操作整備審核。

OT

請參閱操作技術。

傳出 (輸出) VPC

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

P

許可界限

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

個人身分識別資訊 (PII)

當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。

可程式設計邏輯控制器 (PLC)

在製造中，高度可靠、可調整的電腦，可監控機器並自動化製造程序。

提示鏈結

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

擬匿名化

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

發佈/訂閱 (pub/sub)

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

Q

查詢計劃

一系列步驟，如指示，用於存取 SQL 關聯式資料庫系統中的資料。

查詢計劃迴歸

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

R

RACI 矩陣

請參閱負責、負責、諮詢、告知 (RACI)。

RAG

請參閱擷取增強產生。

勒索軟體

一種惡意軟體，旨在阻止對計算機系統或資料的存取，直到付款為止。

RASCI 矩陣

請參閱負責、負責、諮詢、告知 (RACI)。

RCAC

請參閱資料列和資料欄存取控制。

僅供讀取複本

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

重新架構師

請參閱 7 個 R。

復原點目標 (RPO)

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

復原時間目標 (RTO)

服務中斷與服務還原之間的可接受延遲上限。

重構

請參閱 7 個 R。

區域

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

迴歸

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

重新託管

請參閱 7 個 R。

版本

在部署程序中，它是將變更提升至生產環境的動作。

重新定位

請參閱 7 個 R。

Replatform

請參閱 7 個 R。

回購

請參閱 7 個 R。

彈性

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

資源型政策

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

負責者、當責者、事先諮詢者和事後告知者 (RACI) 矩陣

矩陣，定義所有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)，讓使用者可以登入 AWS Management Console 或呼叫 AWS API 操作，而不必為您組織中的每個人在 IAM 中建立使用者。如需有關以 SAML 2.0 為基礎的聯合詳細資訊，請參閱 IAM 文件中的關於以 SAML 2.0 為基礎的聯合。

SCADA

請參閱監督控制和資料擷取。

SCP

請參閱服務控制政策。

秘密

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

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

由接收資料的 AWS 服務 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)

服務效能方面的測量，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，然後再遷移伺服器和應用程式。

WORM

請參閱寫入一次，讀取許多。

WQF

請參閱AWS 工作負載資格架構。

寫入一次，讀取許多 (WORM)

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

Z

零時差入侵

利用零時差漏洞的攻擊，通常是惡意軟體。

零時差漏洞

生產系統中未緩解的瑕疵或漏洞。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。