Backup 和恢復方法 AWS

AWS 規定指引

AWS 規定指引: Backup 和恢復方法 AWS

Table of Contents

備份和恢復方法AWS

尼扎米, 亞馬遜 Web 服務 (AWS)

二零二三年四月(文件記錄)

本指南討論如何使用 Amazon Web 服務實作備份和復原方法 (AWS) 內部部署、雲端原生和混合式架構的服務。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) 和合規性要求。

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、混合式和內部部署環境)。它還涵蓋相關的 Amazon Web Services (AWS) 服務，這些服務可用於為架構的不可變元件建立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架構，從而減少對元件備份和復原的需求。AWS提供許多實作不可變架構的服務，並減少備份與復原的需求，包括：

- 無伺服器搭配AWS Lambda
- 具有亞馬遜彈性容器服務 (亞馬遜 ECS) 的容器、亞馬遜彈性 Kubernetes 服務 (亞馬遜 EKS) 和AWS Fargate
- 亞馬遜機器映像（AMI）與亞馬遜彈性計算雲（亞馬遜 EC2）

隨著企業資料的成長加速，保護資料的任務也變得更具挑戰性。有關備份方法的耐久性和可擴展性的問題很普遍，其中包括：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：

- 選擇適合 AWS 資料保護的服務
- 設計備份與復原解決方案
- 使用 Backup 和恢復AWS Backup
- 使用 Amazon S3 和 Amazon S3 冰川進行 Backup 和恢復
- 使用 EBS 磁碟區的 Amazon EC2 Backup 和復原
- 從內部部署基礎結構備份及復原至AWS
- Backup 與復原AWS到您的數據中心
- 雲端原生AWS服務的 Backup 與復原

- 混合架構 Backup 與恢復
- 使用災難復原AWS
- 清理備份

為什麼使用AWS作為數據保護平台？

AWS 是安全、高效能、彈性、省錢的產品，而且easy-to-use雲計算平台。AWS負責建立、實作及管理可擴充備份與復原解決方案所需的無差別繁重工作。

使用有很多優點AWS作為數據保護策略的一部分：

- 耐用性：亞馬遜簡單儲存服務 (亞馬遜 S3)、亞馬遜 S3 冰川和 S3 冰川深度存檔的設計可達 99.999999999 百分比 (11 個九) 的耐久性。這兩個平台都提供可靠的資料備份，並在至少三個分散各地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，亞馬遜彈性區塊存放區 (亞馬遜 EBS) 使用 Amazon S3 進行快照儲存。
- 安全性:AWS在傳輸中和靜態時，提供了許多存取控制和資料加密的選項。
- 全球基建:AWS服務遍布全球，因此您可以在符合合規性和工作負載要求的區域中備份和儲存資料。
- 合規性:AWS基礎架構已通過認證，符合以下標準，因此您可以輕鬆地將備份解決方案納入您現有的合規性方案中：
  - 服務組織控制 (SOC)
  - 關於證明參與標準的聲明 16
  - 國際標準化組織
  - 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)
  - 第一節
  - 聯邦風險與授權管理計劃 (FedRAMP)
- 擴充性：同AWS，您不必擔心容量。隨著需求的變化，您可以擴展或減少使用量，而不需要管理開銷。
- 降低總體擁有成本 (TCO)：的規模AWS作業可降低服務成本，並協助降低整體擁有成本 (TCO)AWS服務。AWS通過價格下降將這些節省的成本傳遞給客戶。
- Pay-as-you-go價錢: 購買AWS根據您需要的服務，並且僅在您計劃使用它們的期間內提供服務。AWS定價沒有預付費用，終止罰款或長期合同。

目標業務成果

本指南的目標是提供以下內容的概述：AWS您可以用來支援下列項目的備份和復原方法的服務：

- 本地架構
- 雲端原生架構
- 混合式架構
- AWS 原生服務
- 災難復原 (DR)

涵蓋了最佳做法和考量事項，以及服務概觀。本指南還為您提供了使用一種方法進行備份和恢復之間的權衡。

選擇適合 AWS 資料保護的服務

AWS 提供許多儲存與補充服務，可作為備份與復原方法的一部分使用。這些服務可以同時支援雲端原生和混合式架構。不同的服務對於不同的使用案例更有效。

- Amazon S3 和 Amazon S3 冰川和 S3 Glacier Deep Archive 適用於混合和雲端原生使用案例。這些服務提供高耐用性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是混合使用案例的理想選擇。Storage Gateway 使用 Amazon S3 的強大功能來處理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通訊協定，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
  - 伺服器訊息區塊 (SMB)
  - 網際網路小型電腦系統介面 (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，例如：
  - Amazon S3
  - Amazon S3 Glacier
  - S3 Glacier Deep Archive
  - Amazon EBS

  Storage Gateway 可讓您更輕鬆地為中的檔案、磁碟區、快照和虛擬磁帶提供彈性、高效能的儲存裝置 AWS。
- AWS Backup是一項全受管備份服務，用於集中和自動化跨 AWS 服務的資料備份。您可以使用 AWS Backup集中設定備份原則，並監視資 AWS 源的備份活動，例如：
  - EBS 磁碟區
  - EC2 執行個體 (包括視窗應用程式)
  - Amazon RDS 和 Amazon Aurora 數據庫
  - DynamoDB 資料表
  - Amazon Neptune 資
  - Amazon DocumentDB (with MongoDB compatibility) 資料庫
  - Amazon EFS 檔案系統
  - Amazon FSx for Lustre 檔案系統的 Amazon FSx 和適用於 Windows 檔案伺服器檔案系統的亞馬遜 FSx

  - 內部部署和 VMware 雲端上的 VMware 工作負載 AWS
  - 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。如需詳細資訊，請參閱定AWS Backup 價。
- AWS Elastic Disaster Recovery持續將您的機器複製到目標 AWS 帳戶和首選區域中的低成本暫存區域。您可以在 premises-to-cloud DR 和跨區域 DR 上使用彈性災難復原。
- AWS Config提供您 AWS 帳戶中 AWS 資源組態的詳細檢視。這包括資源如何彼此之間的關聯，以及它們在過去的配置方式。在此檢視中，您可以看到資源組態和關係在一段時間內如何變更。

  當您開啟 AWS 資源的AWS Config 組態記錄時，會隨著時間的推移維護資源關係的歷史記錄。這有助於識別和追蹤長達七年的 AWS 資源關係 (包括已刪除的資源)。例如， AWS Config 可以追蹤 Amazon EBS 快照磁碟區和磁碟區連接的 EC2 執行個體之間的關係。
- AWS Lambda可用於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 SDK 與 AWS 服務及其資料互動。您也可以使用 Amazon CloudWatch 活動按排程執行 Lambda 函數。

AWS 服務提供備份和還原的特定功能。針對您使用的每項 AWS 服務，請參閱 AWS 文件，以判斷服務所提供的備份、還原和資料保護功能。您可以使用 AWS Command Line Interface (AWS CLI)、AWS SDK 和 API 作業將 AWS 服務特定功能自動化，以進行資料備份和復原。

設計備份與復原解決方案

在制定備份和還原資料的全方位策略時，您必須先找出可能發生的故障或災難情況，以及其潛在的業務影響。在某些產業中，您必須考慮資料安全性、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資料粒度層級，以符合工作負載及其支援業務程序的復原時間目標 (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)
- 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)
- 亞馬遜 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)
- 受管理的服務復原 (例如，DynamoDB 資料表)

請務必考慮解決方案的所有復原需求，以及架構中各個元件之間的資料相依性。為了促進成功的還原程序，請協調架構中各個元件之間的備份和復原。

下列主題說明以基礎結構組織為基礎的備份與復原方法。IT 基礎架構大致可分類為內部部署、混合式或雲端原生。

使用 Backup 和恢復AWS Backup

AWS Backup是一項完全託管的備份服務，可以集中和自動執行跨AWS服務。AWS Backup提供了一個業務流程層，該層集成了 Amazon CloudWatch、AWS CloudTrail、AWS Identity and Access Management(IAM),AWS Organizations和其他服務。這種集中,AWS雲原生解決方案提供全球備份功能，可幫助您滿足災難恢復和合規性要求。使用AWS Backup，您可以透過集中方式，設定備份策略和監控AWS的費用。

AWS Backup是實施標準備份計劃的理想解決方案AWS資源AWS帳户和區域。由於AWS Backup支持多個AWS資源類型，它可以更輕鬆地維護和實施工作負載的備份策略，使用多個AWS需要集體備份的資源。AWS Backup還使您能夠共同監視包含多個AWS的費用。

如果您有合規性和審核要求，您可以使用AWS Backup稽核管理員功能創建審計框架和報告以支持您的合規性要求。所以此AWS Backup保存庫鎖功能還通過對存儲在備份保管庫中的所有備份強制執行一次性寫入多讀 (WORM) 配置來支持合規性要求AWS Backup。

一個關鍵的區別因素AWS Backup是對 Organizations 的支持。使用此支持，您可以在組織或組織單位級別定義和管理備份策略，並自動為每個相關的AWS帳户和區域。當您登載新的AWS帳户和地區，則無需單獨定義和管理備份計劃。

AWS Backup可以使用標籤更輕鬆地實施組織範圍的備份策略。您可以創建單獨的備份計劃，每個備份計劃都具有唯一的頻率和保留設置，然後創建唯一的鍵值對標籤，以選擇要包括的資源以供備份。

例如，您可以創建每日備份計劃，該計劃每天在 UTC 05:00 啟動備份，並具有 35 天的保留策略。此備份計劃可以包括備份資源分配，它指定任何受支持的AWS具有標籤鍵的資源備份和標籤值每天將根據此計劃進行備份。此外，您可以創建一個月度備份計劃，該計劃從每月的第一天 05:00 UTC 開始，並具有 366 天的保留策略。此備份計劃可以包括一個備份資源分配，指定任何受支持的AWS具有標籤鍵的資源備份和標籤值每月將根據此計劃進行備份。

然後，您可以使用標記策略和required-tags AWS Config規則來確保您的所有AWS支持的資源具有此標籤鍵和其中一個標記值。此方法可以幫助您始終如一地實施和維護AWS支援AWS Backup的費用。您可以擴展此方法來標準化具有不同恢復點目標 (RPO) 要求的應用程序和體繫結構層的備份。

我們建議採取措施來保護您的備份保管庫。例如，您可以實施 Organizations 服務控制策略 (SCP)，以防止您的備份文件庫被刪除或與意外共享AWS帳户。有關詳細信息和其他重要的安全注意事項，請查看保護備份安全的 10 大最佳安全最佳實務AWS博客文章。

AWS Backup可以簡化災難恢復 (DR) 計劃的實施AWS因為它支持多個AWS可以集體解決的資源。例如，您可以將跨區域和跨帳戶備份的大多數AWS支援的資源類型AWS Backup。跨賬户備份提高了備

份安全性，因為副本可在單獨的帳戶中使用。跨區域備份提高了可用性，因為備份在多個區域可用。有關支援的詳細信息AWS資源類型，請參閱資源分列的功能可用性表。

您可使用範例Backup 與恢復AWS Backup開源碼解決方案實施基礎架構即代碼 (iAC) 和持續集成和持續交付 (CI/CD) 方法來管理AWS Organizations組織。此解決方案包括自定義功能，例如自動重新應用AWS已恢復的標籤AWS資源，以及在單獨的帳戶和區域中為災難恢復目的建立輔助備份文件庫。

使用 Amazon S3 和 Amazon S3 冰川進行 Backup 和恢復

Amazon S3 和 Amazon S3 Glacier 是在現場部署、混合式和雲端原生架構中使用的理想儲存服務。這些服務提供耐用、低成本的儲存平台，提供可擴充的容量，而且隨著備份資料集的成長，無需進行磁碟區或媒體管 pay-for-what-you-use 模式和每月低成本，因此這些服務非常適合各種資料保護使用案例。

> **Note**
>
> 某些儲存類別會收取最低持續時間費用。如需詳細資訊，請參閱 Amazon S3 定價，並使用網頁搜尋尋找`duration`。

主題

Amazon S3

您可以隨時使用 Amazon S3 存放和擷取任意數量的資料。您可以使用 Amazon S3 做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 SDK 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 提供高耐用性和可靠的儲存，如下列範例所示：

- Amazon EC2 使用 Amazon S3 為 EBS 磁碟區和 EC2 執行個體存放區存放 Amazon EBS 快照存放區。
- Storage Gateway 與 Amazon S3 整合，為現場部署環境提供 Amazon S3 支援的檔案共用、磁碟區和磁帶庫。
- Amazon RDS 使用 Amazon S3 進行數據庫快照。

許多第三方備份解決方案也使用 Amazon S3。例如，Arcserve 統一資料保護支援 Amazon S3，為現場部署和雲端原生伺服器提供持久備份。

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

Amazon S3 將資料作為物件存放在稱為儲存貯體的資源中。您可以在值區中儲存任意數量的物件。您可以透過精細的存取控制來寫入、讀取和刪除值區中的物件。單一物件的大小最多可達 5 TB。

Amazon S3 提供各種專為不同使用案例設計的儲存類別，包括下列類別：

- S3 標準，適用於經常存取之資料的一般用途儲存 (例如組態檔案、意外備份、每日備份)。
- S3 標準 — IA 適用於長期存取但存取頻率較低的資料 (例如，每月備份)。IA 代表不常訪問。

Amazon S3 提供生命週期政策，您可以設定這些政策來管理資料的整個生命週期。設定原則後，您的資料將移轉至適當的儲存區類別，而不會對應用程式進行任何變更。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，請根據復原時間目標 (RTO) 和復原點目標 (RPO)，使用階層式儲存類別方法，如下列範例所示：

- 使用 S3 標準版進行過去 2 週的每日備份
- 過去 3 個月使用 S3 標準 — IA 進行每週備份
- S3 冰川彈性擷取過去一年的季度備份
- S3 Glacier Deep Archive 中過去 5 年的每年備份
- 備份從 S3 Glacier Deep Archive 刪除後 5 年標記

您可以使用物件生命週期管理來自動化備份的轉換。

> **Note**
>
> 某些儲存類別會收取最低持續時間費用。如需詳細資訊，請參閱 Amazon S3 定價，並使用網頁搜尋尋找`duration`。

建立用於備份和存檔的標準 S3 儲存貯體

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，建立標準 S3 儲存貯體進行備份和存檔。 AWS 帳單的成本配置標記和報告是根據在時段層次指定的標籤而定。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存檔 S3 儲存貯體，以便相應地分配成本。

您的備份指令碼和應用程式可以使用您建立的備份和存檔 S3 儲存貯體，以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 前置詞來協助您組織 point-in-time 資料快照。例

如，如果您建立每小時備份，請考慮使用備份前置詞，例如YYYY/MM/DD/HH/<WorkloadName>/<files...>。這樣，您可以手動或以編程方式快速檢索 point-in-time 備份。

使用 Amazon S3 版本控制自動維護回滾歷史記錄

您可以啟用 S3 物件版本控制來維護物件變更歷程記錄，包括還原到先前版本的功能。這對於可能比 point-in-time 備份排程更頻繁變更的組態檔和其他物件非常有用。這對於必須單獨還原的文件也很有用。

使用 Amazon S3 備份和復原 AMI 的自訂組態檔

具有物件版本控制的 Amazon S3 可成為工作負載組態和選項檔的記錄系統。例如，您可以使用由 ISV 維護的標準 AWS Marketplace Amazon EC2 映像檔。此影像可能包含一些組態檔案中維護其組態的軟體。您可以在 Amazon S3 中維護自訂的組態檔案。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，您不需要自訂並重新建立 AMI 即可使用更新的版本。

在您的自訂備份和還原程序中使用 Amazon S3

Amazon S3 提供一般用途的備份存放區，您可以快速整合到現有的自訂備份程序中。您可以使用 AWS CLI、 AWS 開發套件和 API 操作來整合使用 Amazon S3 的備份和還原指令碼和程序。例如，您可能有一個資料庫備份指令碼，可以執行每晚資料庫匯出。您可以自訂此指令碼，將每晚備份複製到 Amazon S3 以進行異地儲存。有關如何執行此操作的概述，請參閱 Batch 上傳檔案至雲端教學課程。

您可以採用類似的方法，根據個別的 RPO 匯出和備份不同應用程式的資料。此外，您也可以使用 AWS 系統管理員在受控執行個體上執行備份指令碼。Systems Manager 可為您的個別備份程序提供自動化、存取控制、排程、記錄和通知。

Amazon S3 Glacier

Amazon S3 Glacier 是一種低成本的雲端存檔儲存服務，可為資料存檔和線上備份提供安全耐用的儲存。為了保持低成本，S3 Glacier 提供三種儲存類別，範圍從數毫秒到數小時不等。S3 Glacier 彈性擷取和 S3 Glacier Deep Archive 會根據您需要還原資料的速度提供其他選項。使用 S3 Glacier，與現場部署解決方案相比，您可以可靠地存放大量或少量資料，節省大量成本。S3 Glacier 非常適合儲存有長期或無限期保留需求的備份資料，以及長期資料存檔。S3 冰川提供下列儲存類別：

- S3 Glacier 即時擷取，用於存檔每季可能需要一次的資料，且需要快速還原 (毫秒)
- S3 Glacier 彈性擷取適用於存檔可能不常需要在數小時內每年恢復一次或兩次的資料
- S3 Glacier 深度存檔，用於存檔可能不常需要在 12 小時內還原的長期備份週期資料

下表摘要說明封存擷取選項。

儲存方案	快速	標準	大批
S3 Glacier Instant Retrieval	不適用	不適用	不適用
S3 Glacier Flexible Retrieval	1 - 5 分鐘	3 - 5 小時	5 - 12 小時
S3 Glacier Deep Archive	無	12 小時內	48 小時內

使用 Amazon S3，您可以在建立 S3 儲存貯體時為 S3 儲存貯體中的每個物件設定儲存類別。建立物件之後，您可以將物件複製到具有不同儲存區類別的新物件，以變更儲存類別。或者，您可以啟用生命週期配置，該配置將根據您指定的規則自動更改對象的存儲類別。

若要將備份和還原程序自動化，您可以透過、和 AWS 開發套件存取 Amazon S3 Glacier 和 S3 Glacier Deep Archive。 AWS Management Console AWS CLI如需詳細資訊，請參閱 Amazon S3 冰川。

> **Note**
>
> S3 Glacier 儲存類別有最低持續時間費用。如需詳細資訊，請參閱 Amazon S3 定價，並使用網頁搜尋尋找`duration`。

使用 Amazon S3 生命週期物件轉換到 Amazon S3 冰川與管理 Amazon S3 冰川存檔相比

Amazon S3 可讓您方便地將 S3 物件轉換為 Amazon S3 Glacier 儲存類別，因此您可以管理備份的生命週期和成本。不過，根據物件的大小，以及是否必須還原架構中不同元件的物件集合，您可能會想要自行管理此程序。

如果您有大量必須共同還原的小型物件，請考慮下列選項的成本影響：

- 使用生命週期政策自動將物件個別轉移到 Amazon S3 冰川
- 將物件壓縮到單一檔案中，並將它們存放在 Amazon S3 冰川

Amazon S3 Glacier 會根據您使用的儲存類別，針對每個物件收取最低容量費用。例如，S3 冰川即時擷取的每個物件的最低容量費用為 128 KB。如需最多 up-to-date 資訊，請參閱效能圖表。

對於存檔到 S3 Glacier 彈性擷取或 S3 Glacier 深度存檔的每個物件，Amazon S3 會針對物件名稱和其他中繼資料使用 8 KB 的儲存空間。Amazon S3 會存於此中繼資料，以便於可利用 Amazon S3 API 取得封存物件的即時清單。將就這項額外的儲存體向您收取 S3 Standard 費率。

Amazon S3 也會為存檔到 S3 Glacier 彈性擷取或 S3 Glacier 深度存檔儲存類別的每個物件新增 32 KB 的索引和相關中繼資料儲存空間。為了能識別及還原您的物件，將需要這項額外的資料。此額外儲存需支付 Amazon S3 冰川或 S3 Glacier Deep Archive 費率。

透過將物件壓縮到單一檔案中，您可以減少 Amazon S3 Glacier 使用的額外儲存空間，並避免許多小型物件的最低容量費用。

另一個重要的考量因素是，生命週期原則會個別套用至物件。如果必須從特定時間點集合還原物件集合，這可能會影響備份的完整性。無法保證所有物件都會同時轉移，即使跨物件設定了相同的到期時間和生命週期轉移時間。在滿足生命週期規則到規則的動作完成之間，可能會有延遲。如需詳細資訊，請參閱 AWS 知識中心。

最後，考慮使用生命週期原則的歸檔和管理您建立的個別歸檔之間的還原工作。您必須分別從 Amazon S3 冰川啟動每個物件的還原作業。這需要您撰寫指令碼或使用工具，以便共同啟動許多物件的還原。您可以使用 S3 Batch 操作來協助減少個別請求的數量，也可以使用 Amazon S3 主控台。

保護 Amazon S3 和 Amazon S3 冰川中的備份資料

數據安全是普遍關注的問題，並且 AWS 非常重視安全性。安全性是每項 AWS 服務的基礎。Amazon S3 等儲存服務為靜態和傳輸中的存取控制和加密提供強大的功能。所有 Amazon S3 和 Amazon S3 Glacier API 端點都支援安全通訊端層/傳輸層安全性 (SSL/TLS)，以加密傳輸中的資料。Amazon S3 冰川預設會加密所有靜態資料。使用 Amazon S3，您可以執行下列動作，為靜態物件選擇伺服器端加密：

- 搭配 Amazon S3 受管加密金鑰使用伺服器端加密
- 使用儲存於 AWS Key Management Service (AWS KMS) 金鑰的伺服器端加密 AWS KMS

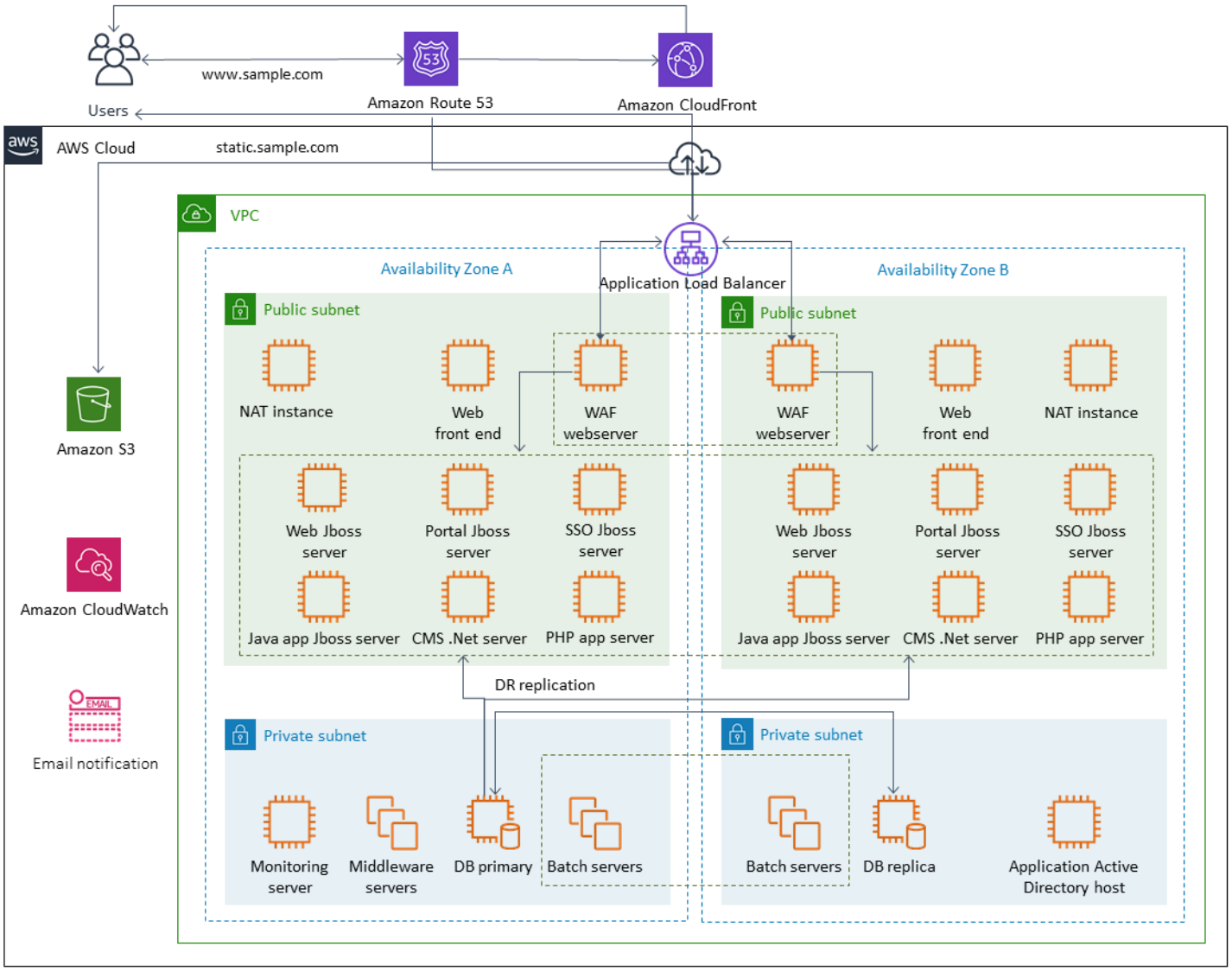
或者，您可以在將數據上傳到之前加密數據 AWS。如需詳細資訊，請參閱用戶端加密文件。

您可以使用 AWS Identity and Access Management (IAM 來控制 S3 物件的存取。IAM 可控制 S3 儲存貯體中個別物件和特定前置碼路徑的許可。您可以使用物件層級記錄功能來稽核 S3 物件的存取 AWS CloudTrail。

使用 EBS 磁碟區的 Amazon EC2 Backup 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) 磁碟區或執行個體存放磁碟區以進行儲存的不同層面。 AWS 如果它符合您的要求，請考慮 AWS Backup 作為管理備份的首選。請記住，只有當備份可以恢復到預期的功能時，它們才是好的。應定期測試還原和恢復功能以確認這一點。

下圖中的解決方案架構描述了完全存在於 AWS 大多數基於 Amazon EC2 架構的工作負載環境。如下圖所示，案例包括網頁伺服器、應用程式伺服器、監視伺服器、資料庫和 Active Directory。



AWS 為此架構中代表的許多 Amazon EC2 伺服器提供許多功能齊全的服務，以執行建立、佈建、備份、還原和最佳化執行個體和儲存的無差異化工作。考慮這些服務是否適用於您的架構，以降低複雜性和管理。 AWS 此外，還提供服務以改善 Amazon EC2 架構的可用性。特別是，請考慮使用 Amazon

EC2 Auto Scaling 和 Elastic Load Balancing 來補充您在 Amazon EC2 上的工作負載。使用這些服務可以提高架構的可用性和容錯能力，並幫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 磁碟區做為持久性儲存。Amazon EBS 提供了許多備份和復原功能，本節將詳細介紹這些功能。

主題

使用快照和 AMI 進行 Amazon EC2 備份和復原

考慮是否需要使用 Amazon 機器映像 (AMI) 建立 EC2 執行個體的完整備份，還是需要拍攝個別磁碟區的快照。

使用 AMI 或 Amazon EBS 快照進行備份

AMI 包括下列項目：

- 一或多個快照。I nstance-store-backed AMI 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)。
- 控制哪些 AWS 帳戶可以使用 AMI 啟動執行個體的啟動權限。
- 區塊裝置對應，指定啟動執行個體時要連接至執行個體的磁碟區。

您可以使用 AMI 透過預先設定的軟體和資料來啟動新執行個體。當您想要建立基準線時，可以建立 AMI，這是啟動更多實例的可重複使用組態。當您建立現有 EC2 執行個體的 AMI 時，會為連接至執行個體的所有磁碟區建立快照。快照包括裝置對映。

您無法使用快照來啟動新的執行個體，但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，您可以從已建立的快照建立磁碟區並取代舊磁碟區。您也可以使用快照佈建新磁碟區，並在新執行個體啟動期間連接它們。

如果您使用的是由 AWS 或發佈的平台和應用程式 AMI AWS Marketplace，請考慮為您的資料維護個別磁碟區。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，搭配由 AWS 或發佈的最新更新 AMI。 AWS Marketplace此方法需要仔細測試和規劃，以備份和還原新發佈的 AMI 上的所有自訂資料 (包括組態資訊)。

還原程序受 AMI 備份或快照備份之間的選擇影響。如果您建立 AMI 做為執行個體備份，則必須從 AMI 啟動 EC2 執行個體，做為還原程序的一部分。您可能還需要關閉現有實例以避免潛在的衝突。可能發生衝突的範例是加入網域的 Windows 執行個體的安全性識別碼 (SID)。快照的還原程序可能需要您卸離現有磁碟區並連接新還原的磁碟區。或者，您可能需要變更設定，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 AMI) 和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，請建立在 Linux 或 Windows 上執行的 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建立執行個體。在執行個體啟動精靈中，選擇 [我的 AMI]。
- 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，但不是中繼資料。EBS 快照的成本為個別磁碟區的儲存。如需有關磁碟區儲存成本的詳細資訊，請參閱 Amazon EBS 定價頁面。

服務器卷

EBS 磁碟區是 Amazon EC2 的主要持續性儲存選項。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 (例如磁碟區上檔案系統中的檔案)。

EBS 磁碟區會放置在特定的可用區域中。磁碟區會在多個伺服器之間複製，以防止因任何單一元件故障而遺失資料。故障是指磁碟區完全或部分遺失，視磁碟區的大小和效能而定。

EBS 磁碟區的設計年故障率 (AFR) 為 0.1-0.2 百分比。這使得 EBS 磁碟區的可靠性是一般商用磁碟機的 20 倍，因為 AFR 的故障率約為 4%。例如，如果您有 1,000 個 EBS 磁碟區執行 1 年，您應該預期一或兩個磁碟區會發生故障。

Amazon EBS 也支援用於 point-in-time 備份資料的快照功能。所有 EBS 磁碟區類型都提供耐用的快照功能，而且專為 99.999 百分比的可用性而設計。如需詳細資訊，請參閱 Amazon 運算服務級別協議。

Amazon EBS 能夠為任何 EBS 磁碟區建立快照 (備份)。快照是建立 EBS 磁碟區備份的基本功能。快照會拍攝 EBS 磁碟區的副本，並將其放置在 Amazon S3 中，並以冗餘方式存放在多個可用區域中。初始快照是磁碟區的完整副本；進行中的快照只會儲存增量區塊層級的變更。如需如何建立 Amazon EBS 快照的詳細資訊，請參閱 Amazon EC2 文件。

您可以執行還原操作、刪除快照或更新快照中繼資料 (例如標籤)，與拍攝快照的同一區域中 Amazon EC2 主控台中的快照相關聯。

還原快照會建立具有完整磁碟區資料的新 Amazon EBS 磁碟區。如果您只需要部分還原，您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。然後掛載它，並使用作業系統複製命令將備份磁碟區中的資料複製到生產磁碟區。

您也可以使用 Amazon EBS 快照複製功能在不同 AWS 區域之間複製 Amazon EBS 快照，如 Amazon EC2 文件所述。您可以使用此功能將備份儲存在其他區域，而不必管理基礎複寫技術。

建立獨立伺服器磁碟

您可能已經為作業系統、記錄檔、應用程式和資料使用了一組標準的獨立磁碟區。透過建立個別的伺服器磁碟區，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。物理硬盤驅動器的風險通常更大，因為您沒有快速擴展卷的靈活性。使用實體磁碟機時，您必須購買新磁碟機、備份資料，然後還原新磁碟機上的資料。有了 AWS，因為您可以使用 Amazon EBS 擴充佈建的磁碟區，因此可大幅降低此風險。如需詳細資訊，請參閱 AWS 文件。

為應用程式資料、使用者資料、記錄檔和交換檔案維護個別磁碟區，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，使用不同的磁碟區類型。然後，您可以針對不同的工作負載最佳化和微調成本。

執行個體儲存磁碟區考量

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暫時儲存經常變更的資訊，例如緩衝區、快取、暫存資料和其他暫存內容。對於跨執行個體叢集進行複製的資料，例如 Web 伺服器的負載平衡集區，這些資料也比較適合。

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。但是，在下列任一情況下，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來獲取有價值的長期資料。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)，視需要定期將必要的資料保存到 Amazon S3。然後，您可以在啟動新執行個體時，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到 Amazon S3。如需持續性，請建立 EBS 磁碟

區，將其連接至執行個體，然後定期將資料從執行個體存放區磁碟區複製到 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 AMI 的標準

標記所有資 AWS 源是成本分配、稽核、疑難排解和通知的重要作法。標記對於 EBS 磁碟區來說很重要，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 AMI 或從來源磁碟區複製到快照。請確定您的備份程序包含這些來源的相關標籤。這可協助您設定快照中繼資料 (例如存取原則、附件資訊和成本配置)，以便 future 使用這些備份。如需標記 AWS 資源的詳細資訊，請參閱標籤最佳實務技術 paper。

除了用於所有 AWS 資源的標籤之外，請使用以下備份特定標籤：

- 來源執行環境 ID
- 來源磁碟區 ID (適用於快照)
- 復原點說明

您可以使用 AWS Config 規則和 IAM 許可強制執行標記政策。IAM 支援強制使用標籤，因此您可以撰寫 IAM 政策，以便在 Amazon EBS 快照上執行動作時，強制使用特定標籤。如果在未授予權限的 IAM 許可政策中定義的標籤的情況下嘗試`CreateSnapshot`執行操作，則快照建立會失敗，並拒絕存取。如需詳細資訊，請參閱有關在建立和實作更強安全政策時標記 Amazon EBS 快照的部落格文章。

您可以使用 AWS Config 規則自動評估 AWS 資源的組態設定。為協助您開始使用，請 AWS Config 提供稱為 Managed 規則的可自訂預先定義規則。您也可以建立自己的自訂規則。在持 AWS Config 續追蹤資源之間的組態變更時，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 標記為不相容。請注意，必要的標籤受管理規則目前不支援快照和 AMI。

使用 AMI 和 EBS 快照建立 EBS 磁碟區備份

AWS 為建立和管理 AMI 和快照提供了豐富的選項。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，並依據用途、保留原則等明確對齊快照。如果沒有適當的標記，就有可能會意外刪除快照，或是做為自動清理程序的一部分而遭到刪除。您最終可能還需要支付保留的過時快照，因為沒有清楚的瞭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

在拍攝快照或建立 AMI 之前，請對 EBS 磁碟區進行必要的準備工作。建立 AMI 會為連接至執行個體的每個 EBS 磁碟區建立新的快照，因此這些準備工作也適用於 AMI。

您可以拍攝已開啟電源的 EC2 執行個體正在使用的連接 EBS 磁碟區的快照。不過，快照只會擷取發出快照指令時已寫入 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。最佳做法是讓系統處於未執行任何 I/O 的狀態。理想情況下，機器不接受流量且處於停止狀態，但這種情況很少，因為全年無休的 IT 作業成為常態。如果您可以將系統記憶體中的任何資料清除到應用程式正在使用的磁碟，並暫停對磁碟區的任何檔案寫入時間足以拍攝快照，您的快照就應該已完成。

若要進行全新備份，您必須靜止資料庫或檔案系統。執行此操作的方式取決於您的資料庫或檔案系統。

數據庫的過程如下：

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. 將資料庫退出熱備份模式，或者如果使用僅供讀取複本，則終止僅供讀取複本執行個體。

對於一個文件系統的過程是相似的，但它取決於操作系統或文件系統的能力。例如，XFS 是一種檔案系統，可以清除其資料以進行一致的備份。如需詳細資訊，請參閱 xfs_ 凍結。或者，您也可以使用支援凍結 I/O 的邏輯磁碟區管理員來簡化此程序。

不過，如果您無法清除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. 發出快照指令。
3. 重新掛接磁碟區以獲得一致且完整的快照。當快照狀態處於擱置狀態時，您可以重新掛接並使用磁碟區。

快照程序會在背景中繼續執行，而且快照建立速度很快，可擷取某個時間點。您要備份的磁碟區只需幾秒鐘即可卸載。您可以排程小型備份視窗，在此時間預期會中斷，並由用戶端妥善處理。

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，然後再建立快照。Windows 提供磁碟區陰影複製服務 (VSS) 來協助建立應用程式一致的快照集。 AWS 提供 Systems Manager 文件，您可以執行此文件，以便對 VSS 感知應用程式進行映像層級備份。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，您不必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 來系統執行您的執行個體。然後從停止的實例創建 AMI。Sysprep 會移除 Amazon

EC2 視窗執行個體的唯一資訊，包括 SID、電腦名稱和驅動程式。重複的 SID 可能會導致活動目錄，Windows 服務器更新服務（WSUS），登錄問題，Windows 卷密鑰激活，Microsoft Office 和協力廠商產品的問題。如果您的 AMI 用於備份目的，而且您想要還原相同的執行個體，且其所有唯一資訊都完整無缺，請勿搭配執行個體使用 Sysprep。

從主控台手動建立 EBS 磁碟區快照

請先建立適當磁碟區或整個執行個體的快照，然後再進行任何未在執行個體上完整測試的重大變更。例如，您可能想要先建立快照，然後再升級或修補執行個體上的應用程式或系統軟體。

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，選取要備份的磁碟區。然後在 [動作] 功能表上選擇 [建立快照]。您可以在篩選方塊中輸入執行個體 ID，以搜尋附加至特定執行個體的磁碟區。

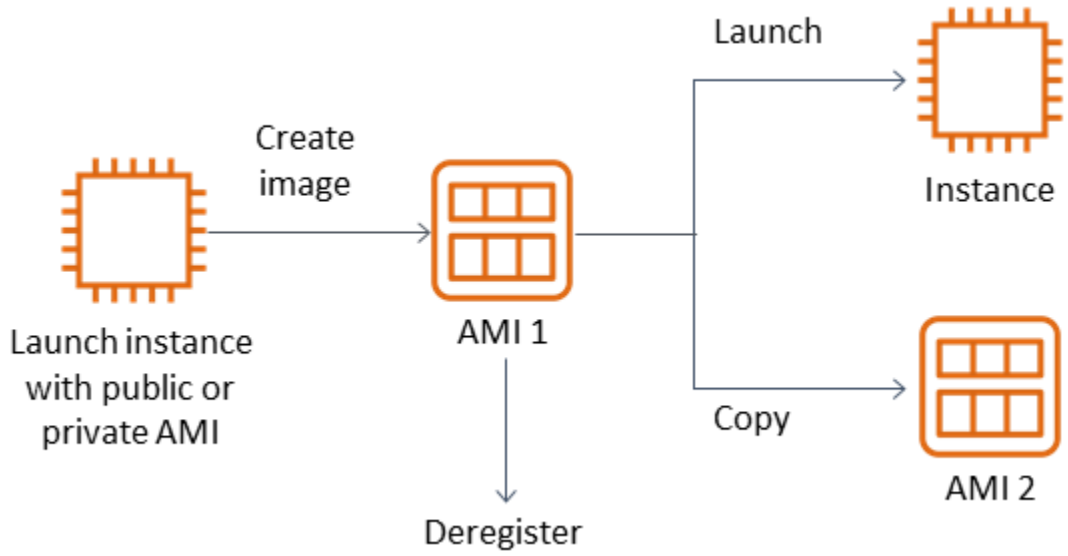
輸入描述並加入適當的標籤。新增標Name籤，以便日後更容易尋找磁碟區。根據您的標記策略新增任何其他適當的標籤。

建立 AMI

AMI 提供啟動執行個體所需的資訊。AMI 包括建立映像檔時連接至執行個體的根磁碟區和 EBS 磁碟區的快照。您無法僅從 EBS 快照啟動新執行個體；您必須從 AMI 啟動新執行個體。

建立 AMI 時，會在您使用的帳戶和區域中建立該 AMI。AMI 建立程序會為連接到執行個體的每個磁碟區建立 Amazon EBS 快照，而 AMI 則參照這些 Amazon EBS 快照。這些快照存放在 Amazon S3 中，且非常耐用。

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 AMI 從一個區域複製到另一個區域以進行應用程式移轉或 DR。



必須從 EC2 執行個體建立 AMI，除非您要將虛擬機器 (例如 VMWARE 虛擬機器) 移轉到 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作業：

- 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 資料生命週期管理員，您可以自動執行 EC2 執行個體 (及其連接的 EBS 磁碟區) 或獨立 EBS 磁碟區的快照管理程序。它支援跨區域複製等選項，因此您可以自動將快照複製到其他區 AWS 域。將快照複製到替代區域是在替代區域中支援 DR 工作和還原選項的一種方法。您也可以使用 Amazon Data Lifecycle Manager 建立支援快照還原的快照生命週期政策。

Amazon Data Lifecycle Manager 管理器是 Amazon EC2 和 Amazon EBS 的一項功能。Amazon Data Lifecycle Manager 不收取任何費用。

AWS Backup

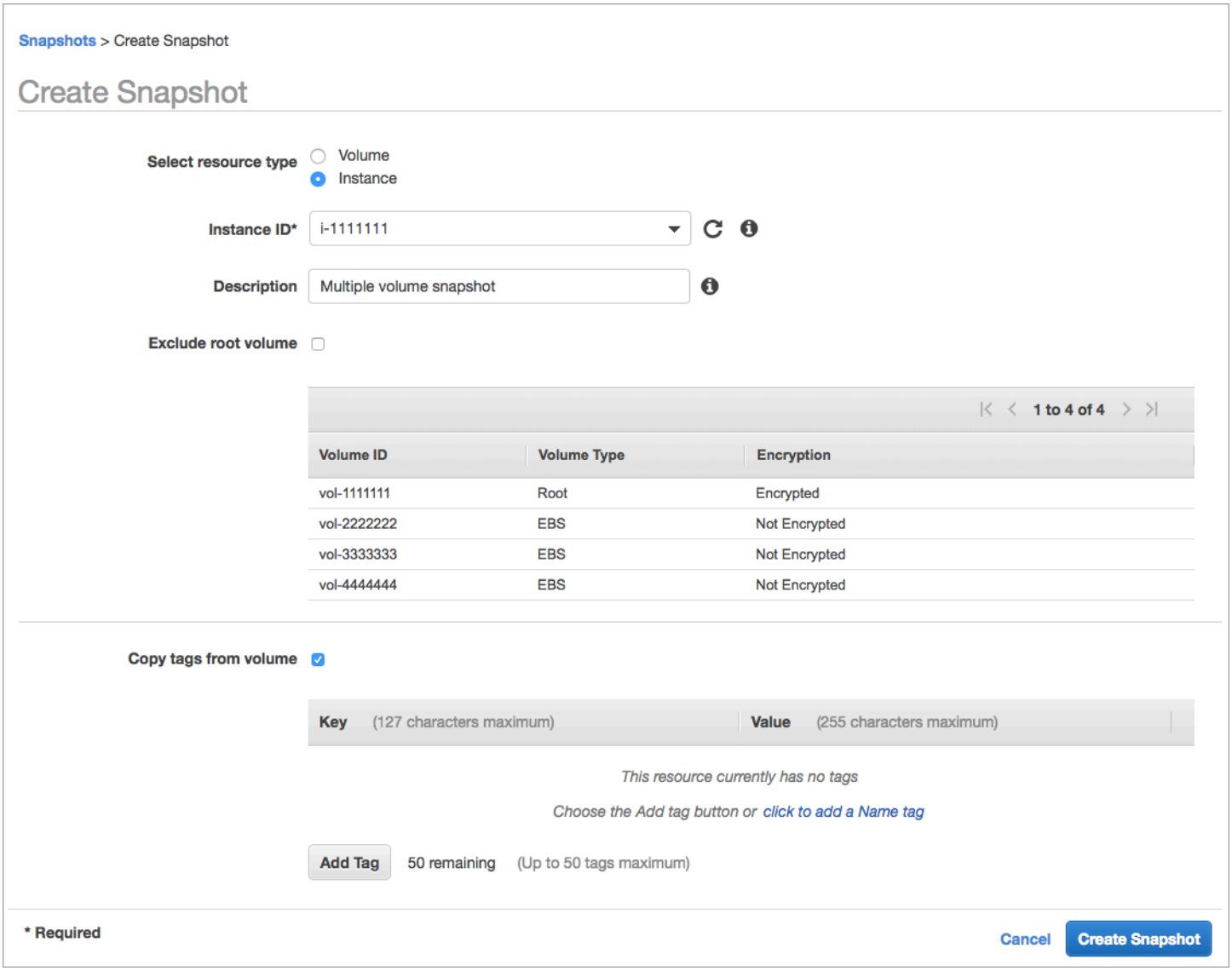
AWS Backup Amazon Data Lifecycle Manager 是獨一無二的，因為您可以建立包含多個 AWS 服務資源的備份計劃。您可以協調備份以涵蓋一起使用的資源，而不是個別協調資源的備份。

AWS Backup 也包括備份儲存庫的概念，可限制對已完成備份之復原點的存取。還原作業可以從啟動， AWS Backup 而不是繼續到每個個別資源並還原建立的備份。 AWS Backup 還包括許多其他功能，例如稽核管理和報告。如需詳細資訊，請參閱本指南的 使用 Backup 和恢復AWS Backup 一節。

執行多重磁碟區備份

如果要使用快照備份 RAID 陣列中 EBS 磁碟區上的資料，快照必須保持一致。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 RAID 陣列建立一組一致的快照集，請使用 CreateSnapshotsAPI 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 組態中連接了多個磁碟區的執行個體快照，會統稱為多磁碟區快照。多磁碟區快照可在連接至 EC2 執行個體的多個 EBS 磁碟區之間提供 point-in-time資料協調和當機一致的快照。您不必停止執行

個體來協調磁碟區之間，以達到一致性，因為會在多個 EBS 磁碟區自動擷取快照。啟動磁碟區的快照 (通常是第二個或兩個) 之後，檔案系統可以繼續其作業。

建立快照後，每個快照視為個別快照。您可以執行所有快照作業，例如還原、刪除、跨區域和帳戶複製，就像使用單一磁碟區快照一樣。您也可以標記多磁碟區快照，就像建立單一磁碟區快照一樣。建議您標記多磁碟區快照，以便在還原、複製或保留期間進行統一管理。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，使用傳統的備份代理程式可以透過網路備份資料。網際網路和中提供了許多以代理程式為基礎的備份解決方案。AWS Marketplace

另一種方法是建立存在於單一大型磁碟區上之主要系統磁碟區的複本。這樣可簡化備份程序，因為只需備份一個大型磁碟區，而且主要系統上不會進行備份。不過，請先判斷單一磁碟區是否能夠在備份期間執行充分，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

請務必考慮備份的安全性，並防止意外或惡意刪除備份。您可以使用許多方法集體來實現這一目標。為了避免因安全漏洞而遺失重要備份，建議您將備份複製到其他 AWS 帳戶。如果您有多個 AWS 帳戶，您可以指定一個不同的帳戶做為您的存檔帳戶，其他所有帳戶都可以將備份複製到該帳戶。例如，您可以使用中 AWS Backup的跨帳戶備份來完成此操作。

如果發生區域故障，您的災難復原計劃也可能要求您能夠在另一個 AWS 區域重現 EC2 執行個體。您可以將備份複製到同一帳戶內的其他區域，以支援此目標。這可以提供額外的意外刪除保護層，以及支援災難復原 (DR) 目標。AWS Backup 提供跨區域備份的支援。

考慮阻止 EC2：DeleteSnapshot和 ec2：DeregisterImage操作的 IAM 許可。相反地，您可以讓保留政策和方法管理 EBS 快照和 Amazon EC2 AMI 的生命週期。封鎖刪除動作是為 EBS 快照實作一次寫入多讀 (WORM) 策略的一種方式。您也可以使用文件AWS Backup 庫鎖定，它為 EBS 快照和其他 AWS 資源提供支援。

此外，請考慮封鎖 ec2: 和 ec2: ModifySnapshotAttribute IAM 動作來封鎖使用者共用 AMI ModifyImageAttribute 和 EBS 快照的能力。這樣可防止您的 AMI 和快照與組織外部的 AWS 帳戶共用。如果您正在使用 AWS Backup，請限制使用者對備份儲存庫執行類似作業。如需詳細資訊，請參閱本指南的 AWS Backup 一節。

Amazon EC2 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。使用者應特別小心刪除多個快照，因為 Amazon EC2 主控台可讓您選取多個快照並在一次操作中刪除快照。此外，當您使用清理指令碼和自動化操作

時，請務必小心，這樣您就不會意外刪除所需的快照。資源回收筒功能可協助提供防護，避免這些類型的情況發生。

封存 EBS 快照

封存 EBS 快照是一種經濟實惠的方法，可以用來保留磁碟區副本以供參考，而且您不打算還原 90 天或更長時間。在永久刪除 EBS 磁碟區的所有相關快照之前，這是一個很好的中繼步驟。例如，您可以考慮將快照封存為不再使用的 EBS 磁碟區的 end-of-lifecycle 步驟。封存而非刪除也可能是一種更具成本效益的刪除保留方式，而不是使用資源回收筒。

使用 Systems Manager、和 SDK 自動化快照和 AMI 建立 AWS CLIAWS

您的備份方法可能需要在建立快照或 AMI 之前和之後進行操作。例如，您可能需要停止和啟動服務以靜止檔案系統。或者，您可能需要在 AMI 建立期間停止並啟動執行個體。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確認備份程序是否一致套用，以減少備份的維護時間。若要自動化您的自訂建立前和建立後作業，請使用 AWS CLI 和 SDK 編寫備份程序指令碼。

您的自動化可以在 Systems Manager 手冊中定義，該手冊可以根據需求或在 Systems Manager 維護期間執行。您可以授予使用者執行 Systems Manager 工作流程手冊的存取權，而不需要授予他們權限給 Amazon EC2 顛覆性命令。這也可協助您確認您的備份程序和標籤是否一致地套用您的使用者。您可以使用 AWS CreateSnapshot 和 AWS CreateImage 執行手冊來建立快照和 AMI，也可以授予其他使用者使用它們的許可。Systems Manager 還包括 AWS UpdateLinuxAmi 和 AWS 工作 UpdateWindowsAmi流程手冊，可自動化 AMI 修補和 AMI 建立。

您也可以使用 AWS CLI 和AWS Tools for Windows PowerShell來自動化您的快照和 AMI 建立程序。您可以使用 aws ec2 創建快照 AWS CLI 命令來創建 EBS 磁碟區的快照，作為自動化的一個步驟。您可以使用 aws ec2 創建快照命令為連接到 EC2 實例的所有卷創建崩潰一致的同步快照。

您可以使用 AWS CLI 建立新的 AMI。您可以使用 aws ec2 註冊映像命令為 EC2 實例創建新映像。若要自動執行個體的關閉、映像建立和重新啟動，請將此命令與 aws ec2 停止執行個體和 aws ec2 啟動執行個體命令結合使用。

還原 Amazon EBS 磁碟區或 EC2 執行個體

如果您只需要還原連接到 EC2 執行個體的單一磁碟區，則可以分別還原該磁碟區、分離現有磁碟區，然後將還原的磁碟區附加到 EC2 執行個體。如果您需要還原整個 EC2 執行個體 (包括所有關聯的磁碟區)，則必須使用執行個體的 Amazon 機器映像 (AMI) 備份。

為了減少復原時間以及對相依應用程式和程序的影響，您的還原程序必須考量其取代的資源。為獲得最佳結果，請定期在較低環境 (例如非生產環境) 中測試還原程序，以確認您的程序是否符合復原點目標 (RPO) 和復原時間目標 (RTO)，以及還原程序是否如預期般運作。考慮還原程序會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作業。嘗試盡可能自動化並測試還原程序，以降低還原程序失敗或不一致地實作的風險。

如果您使用 Elastic Load Balancing，讓多個執行個體為流量提供服務，則可以將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以取代它，而其他執行個體會繼續為流量提供服務，而不會中斷使用者。

下列所述的還原程序適用於未使用 Elastic Load Balancing 的執行處理：

- 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 快照提供用來建立快照之原始磁碟區的 point-in-time 精確複本。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. 將磁碟區附加到要還原檔案的 EC2 執行個體。
3. 將檔案從還原的磁碟區複製到 EC2 執行個體磁碟區。
4. 分離並刪除還原的磁碟區。

從 Amazon EBS 快照還原 EBS 磁碟區

您可以從現有 EC2 執行個體建立磁碟區並將其附加到執行個體，藉此還原連接到現有 EC2 執行個體的磁碟區。您可以使用控制台 AWS CLI、或 API 操作從現有快照建立磁碟區。然後，您可以使用作業系統將磁碟區掛接到執行個體。

請注意，來自 Amazon EBS 快照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，延遲會比正常情況高。若要避免對延遲敏感的應用程式產生這種影響，您有兩種選擇：

- 您可以初始化 EBS 磁碟區。
- Amazon EBS 只需支付額外費用，即可支援快速快照還原，無需初始化磁碟區。

如果您要更換必須使用相同掛接點的磁碟區，請卸載該磁碟區，以便在其位置掛接新的磁碟區。若要卸載磁碟區，請先停止任何正在使用該磁碟區的程序。如果要取代根磁碟區，您必須先停止執行個體，才能卸離根磁碟區。

例如，請依照下列步驟，使用主控台將磁碟區還原為先前的 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，然後加以選取。
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. 在執行個體詳細資料中，記下您要取代的裝置名稱，在根裝置項目或封鎖裝置項目中。
7. 附加磁碟區。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 彈性區塊存放磁碟區功能表上，選取要取代的根磁碟區。
   c. 選擇 [動作]，然後選擇 [分離磁碟區]。
   d. 在 EC2 彈性區塊存放磁碟區功能表上，選取新磁碟區。
   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，然後使用您先前提到的相同裝置名稱。

   對於非根磁碟區：

   a. 在 EC2 彈性區塊存放磁碟區功能表上，選取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上選擇新磁碟區，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，然後將新磁碟區掛接到其位置。

      在 Linux 中，您可以使用該`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 彈性區塊存放區磁碟區功能表上選擇該磁碟區，然後選擇 [動作] > [卸離磁碟區]，以卸離您可能要取代的任何先前磁碟區

您也可以結合使用 AWS CLI 作業系統指令來自動執行這些步驟。

從 EBS 快照建立或還原 EC2 執行個體

若要建立用於還原整個 EC2 執行個體的備份，建議您建立 Amazon 機器映像 (AMI)。AMI 會擷取機器資訊，例如虛擬化類型。他們還會為連接到 EC2 執行個體的每個磁碟區 (包括其裝置對映) 建立快照，以便在相同的組態中還原它們。

但是，如果您必須使用 EBS 快照還原執行個體，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，然後加以選取。
3. 選擇 [動作]，然後選擇 [從快照建立影像]。
4. 輸入影像的名稱 (例如，YYYYMMDD-restore-for-i-012345678998765de)，然後為新影像選擇適當的選項。

建立映像並可用之後，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 備份啟動新執行個體，以取代現有的執行中執行個體。一種方法是停止現有的執行個體，在您從 AMI 啟動新執行個體時將其保持離線狀態，並執行任何必要的更新。這種方法可降低兩個執行個體同時執行的衝突風險。如果執行個體提供的服務已關閉，或者您正在維護時段執行還原作業，這是可以接受的方法。測試新執行個體之後，您可以重新指派配置給舊執行個體的任何彈性 IP 位址。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。

但是，如果在還原期間必須將服務中執行個體的停機時間降至最低，請考慮從 AMI 備份啟動和測試新執行個體。然後使用新例證取代現有的執行個體。

當這兩個執行個體都在執行時，您必須防止新執行個體造成任何平台層級或應用程式層級衝突。例如，您可能會遇到使用相同 SID 和電腦名稱執行的網域 Windows 執行個體的問題。您可能會遇到需要唯一識別碼的網路應用程式和服務類似的問題。

為了防止其他伺服器和服務在新執行個體準備就緒之前連線至您的新執行個體，請使用安全性群組暫時封鎖新執行個體的所有輸入連線，但您自己的 IP 位址進行存取和測試除外。您也可以暫時封鎖新執行個體的輸出連線，以防止服務和應用程式啟動對其他資源的任何連線或更新。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，然後解除封鎖您實作的任何輸入或輸出網路連線。

從內部部署基礎結構備份及復原至AWS

您可以使用AWS為您的內部部署基礎結構備份提供持久的異地儲存空間。通過使用AWS在此案例中，您可以專注於備份和封存工作的儲存服務。您不必擔心備份工作的儲存基礎結構佈建、擴展或基礎架構容量。

Amazon S3 和 Amazon S3 Glacier 提供廣泛的 API 操作和開發套件，可將這些服務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的方式AWS儲存解決方案。

在此案例中，您在內部部署基礎結構中使用的備份和封存軟體會直接介面AWS通過 API 操作。因為備份軟件是AWS-意識到，它會將資料從現場部署伺服器直接備份到 Amazon S3 或亞馬遜 S3 冰川。

如果您現有的備份軟體本身不支援AWS雲，您可以使用存儲網關。Storage Gateway 是雲端儲存服務，可讓您的內部部署系統存取可擴充的雲端儲存。它支援與現有應用程式搭配使用的開放標準儲存協定，同時將加密的資料安全地存放在 Amazon S3 或 Amazon S3 Glacier 中。您可以使用 Storage Gateway 做為內部部署區塊式儲存工作負載的備份和復原方法的一部分。

在您想要轉換為雲端儲存以進行備份的混合式案例中，儲存閘道非常有用。儲存閘道也可協助您減少內部部署儲存裝置的資本投資。您可以將儲存閘道部署為虛擬機器或專用硬體應用裝置。本指南著重說明儲存閘道如何套用至備份與復原。

儲存閘道提供三種不同的選項來滿足不同的需求：

- 一種檔案閘道，可使用 SMB 型或 NFS 型存取，在 Amazon S3 雲端儲存上以耐久物件形式存放應用程式資料檔案和備份映像。
- 一種磁碟區閘道，可將雲端式 iSCSI 區塊儲存磁碟區呈現給內部部署應用程 磁碟區閘道可在內部部署提供本機快取或完整磁碟區，同時將磁碟區的完整複本儲存在AWS雲端。
- 用於將受信任備份軟體指向現場部署儲存閘道的磁帶閘道，然後連接到 Amazon S3 和 Amazon S3 Glacier。此選項可提供雲端的規模和耐久性，以便在不中斷現有投資或流程的情況下安全、長期保留。

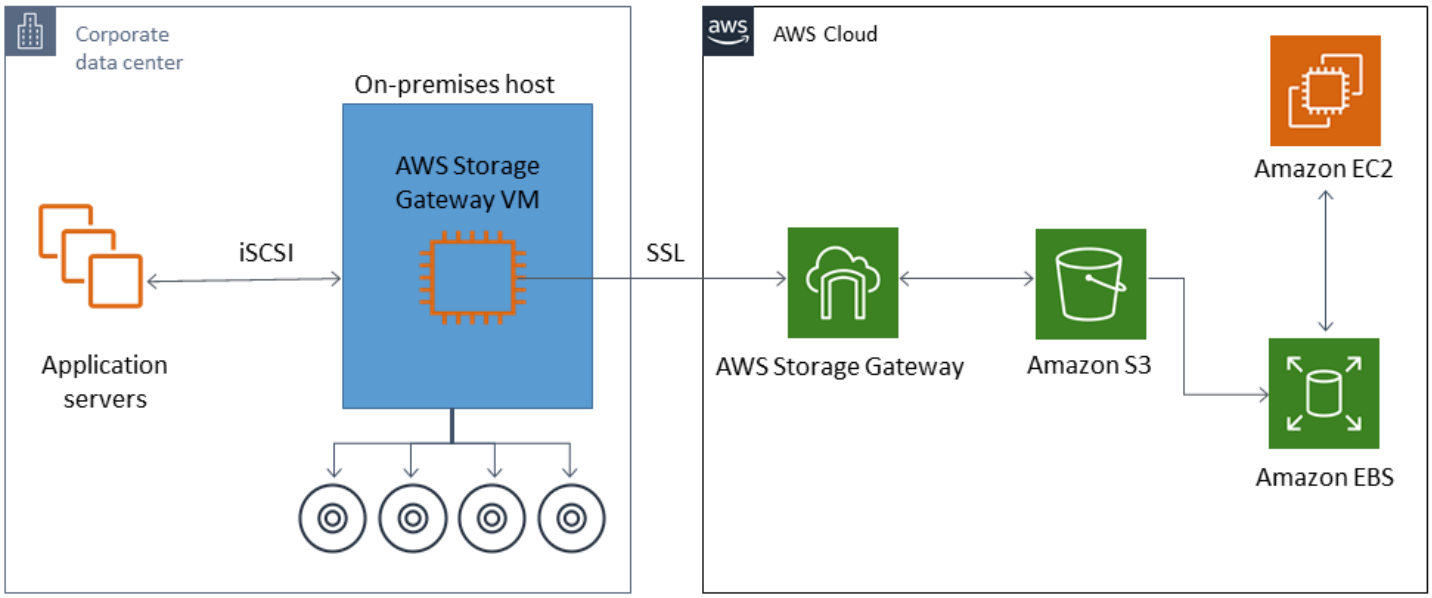
檔案閘道

許多組織透過將次要和第三級資料 (例如備份) 移至雲端，開始他們的雲端旅程。檔案閘道的 SMB 和 NFS 介面支援可讓 IT 群組將備份工作從現有的內部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，都可以寫入檔案閘道。檔案閘道會將備份存放為最大 5 TiB 的 Amazon S3 物件。使用適當大小的本機快取，最近的備份可用於快速的現場復原。透過將備份分層到低成本的 S3 標準-不常存取和 Amazon S3 Glacier 儲存層，可解決長期保留需求。

檔案閘道為您的區塊式儲存提供快速到 Amazon S3，以實現高耐用性的異地備份。對於必須快速還原最近備份的檔案的情況而言，此功能特別有用。由於檔案閘道支援 SMB 和 NFS 通訊協定，因此使用者可以使用與存取網路檔案共用相同的方式存取檔案。您也可以利用 Amazon S3 物件版本控制功能。使用物件版本控制，您可以還原檔案的先前物件版本，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 iSCSI 區塊儲存磁碟區。磁碟區閘道將您的磁碟區資料存放到 Amazon S3，以提供耐用、可擴展的雲端異地儲存。磁碟區閘道有助於充分取得point-in-time磁碟區的快照，並以 Amazon EBS 快照的形式存放在雲端。將它們儲存為快照後，整個磁碟區可以還原為 EBS 磁碟區並連接至 EC2 執行個體，以加速雲端型 DR 解決方案。磁碟區也可以還原至 Storage Gateway，讓您的內部部署應用程式能夠還原至先前的狀態。



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自動化並排程您的快照程序。磁碟區閘道為您提供耐用且支援 Amazon S3 的 Amazon EBS 快照和標記功能的額外優勢。如需詳細資訊，請參閱亞馬遜 EBS 快照文檔。

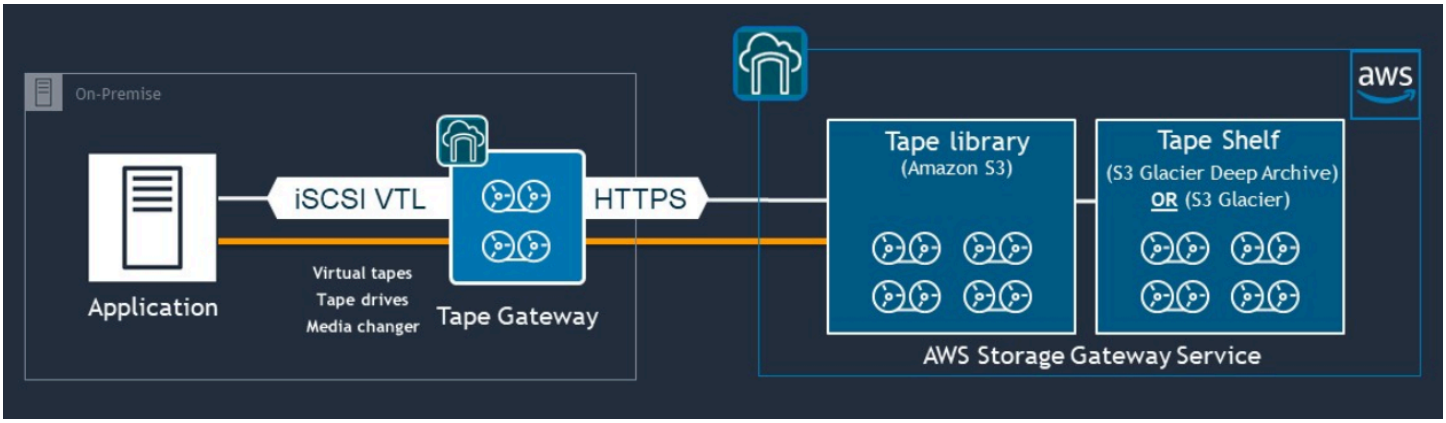
磁帶閘道

磁帶閘道為您的異地虛擬磁帶備份存放區提供 Amazon S3 和 Amazon S3 Glacier 的高耐用性、低成本的分層儲存以及廣泛的功能。您存放在 Amazon S3 和 Amazon S3 Glacier 中的所有虛擬磁帶都會在至少三個分散各地的可用區域中進行複寫和存放。您的虛擬磁帶受到 11 個九的耐用性保護。

AWS還會定期執行固定性檢查，以確認您的資料是否可以讀取，並且沒有引入任何錯誤。Amazon S3中存放的所有磁帶都受到伺服器端加密的保護，使用預設金鑰或AWS KMS鑰匙。此外，您還可以避免

與磁帶可攜性相關的實體安全性風險。與磁帶的異地倉儲相比，您可以使用磁帶閘道獲得正確的資料，在還原期間您可能會收到不正確或損壞的磁帶。

將資料存放在 Amazon S3 時，可以節省每月儲存成本。您可以使用 S3 Glacier 深度存檔，為您的長期存檔需求節省更多成本。



磁帶閘道充當虛擬磁帶櫃 (VTL)，從您的現場部署環境擴展到高度可擴展、備援和耐用的儲存服務：Amazon S3、S3 Glacier 彈性擷取和 S3 Glacier 深度存檔。

磁帶閘道將儲存閘道以開放標準 ISCSI 為基礎的 VTL 呈現給您現有的備份應用程式，並配備虛擬媒體轉換器和虛擬磁帶機。您可以繼續使用現有的備份應用程式和工作流程，同時寫入存放在可大規模擴展 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，您的備份應用程式可將其存檔到 S3 Glacier 彈性擷取或 S3 Glacier 深層存檔，進一步降低儲存成本。

您可以擷取存檔在 S3 Glacier 彈性擷取或 S3 Glacier 深度存檔中的磁帶，通常分別需要 3 到 5 小時或 12 小時。磁帶閘道可搭配與 ISCSI 型磁帶櫃介面相容的備份應用程式搭配使用，以存取虛擬磁帶。另外，請考慮每個磁帶的最小 100 GB 儲存大小。有關更多信息，請查看列表第三方備份應用支援磁帶閘道。

Backup 與復原AWS到您的數據中心

您可能有一個策略要求您為基於雲的工作負載和本地基礎架構實施災難恢復或業務連續性等方案。如果您已經擁有現場部署伺服器的資料備份框架，您可以將其擴展至AWS資源通過 VPN 連接或通過AWS Direct Connect。您可以在 EC2 實例上安裝備份代理，並根據您的數據保護策略備份數據和應用程序。您還可以使用 Amazon S3 作為中間服務來存儲您的應用程序級別備份。然後，您可以使用 API 操作、軟件開發工具包或AWS CLI將數據還原到您的本地環境。

若要備份AWS服務，Amazon EC2 使用AWS CLI、軟件開發工具包和 API 操作，將數據提取為您所需的格式。然後複製檔案到 Amazon S3，從 Amazon S3 複製檔案到現場部署環境。某些服務可直接匯出至 Amazon S3。例如，Amazon RDS 支援原生備份複製檔案到 Amazon S3。

雲端原生AWS服務的 Backup 與復原

您的備份和復原方法應涵蓋工作負載中使用的AWS服務。 AWS提供服務特定功能和選項，以管理您的資料並與之互動。您可以使用主控台AWS CLI、SDK 和 API 作業，為您正在使用的AWS服務實作備份和復原。本指南涵蓋了亞馬遜 RDS 和 Amazon DynamoDB 作為示例。 AWS Backup同時支援 DynamoDB 和 Amazon RDS，如果符合您的需求，就應該使用它。

適用於 Amazon RDS 的 Backup 與復原

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體磁碟區快照，因此會備份整個資料庫執行個體，而不只是個別的資料庫。您可以使用 Amazon RDS 建立自動備份的備份視窗、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您的資料庫執行個體：

- 自動備份可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，依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，執行完整的每日資料備份。您最多可以將保留期間設定最長 35 天的自動備份。Amazon RDS 還每 5 分鐘會將資料庫執行個體的交易日誌上傳至 Amazon S3。Amazon RDS 會使用您的每日備份和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到任何一秒鐘，最多可將執行個體還原到`LatestRestorableTime` (通常是最近五分鐘)。

  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。或者，在 Amazon RDS 主控台上查看資料庫的「描述」索引標籤。

  當您啟動 PITR 時，交易記錄會與最適當的每日備份結合使用，將資料庫執行個體還原到要求的時間。
- 資料庫快照是您啟動的備份，可將您的資料庫執行個體還原至您喜歡的已知狀態。然後，您可以隨時恢復到該狀態。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 呼叫明確刪除它們為止。

Amazon RDS 中支援這兩個備份選項AWS Backup，也提供其他功能。考慮使AWS Backup用為 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候，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。這也可防止您將 RDS 資料庫執行個體上的資料庫直接匯出到其本機磁碟。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功能。例如，您可以將 mysqldump 命令與 Amazon RDS MySQL 資料庫搭配使用，將資料庫匯出到本機用戶端電腦。在某些情況下，Amazon RDS 還提供用於執行資料庫原生備份和還原的增強選項。例如，亞馬遜 RDS 提供用於匯出和匯入 SQL 伺服器資料庫 RDS 資料庫備份的預存程序。

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

使用 DNS CNAME 記錄來減少資料庫復原期間的用戶端影響

使用 PITR 或 RDS 資料庫執行個體快照還原資料庫時，會建立具有新端點的新資料庫執行個體。如此一來，您就可以從特定的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，需要特別考量。例如，您必須決定如何將現有的資料庫用戶端重新導向至新的執行個體，以最少的中斷和修改。您還必須考慮還原的資料時間和新執行個體開始接收寫入時的復原時間，以確保資料庫中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 以指向新的還原端點，而無需更新資料庫用戶端。

將您的 CNAME 記錄的存留時間 (TTL) 設定至適當的值。您指定的 TTL 會決定 DNS 解析器快取記錄的時間長度，然後再發出另一個要求。請務必注意，某些 DNS 解析器或應用程式可能不遵守 TTL，而且它們可能會快取記錄的時間超過 TTL。對於 Amazon Route 53，如果您指定較長的值 (例如 172800 秒或兩天)，您會降低 DNS 遞迴解析程式對 Route 53 進行的呼叫數。這樣可以減少延遲並減少 Route 53 服務的費用。如需詳細資訊，請參閱 Amazon Route 53 如何為您的網域路由流量。

應用程式和用戶端作業系統也可能會快取您必須清除或重新啟動的 DNS 資訊，才能起始新的 DNS 解析要求並擷取更新的 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，請確認所有用戶端都寫入已還原的執行個體，而非先前的執行個體。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，然後修復仍可能寫入您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，所有訪問都來自新恢復的實例。這可能會暫時導致某些您可以單獨處理的資料庫用戶端發生連線問題。若要減少對用戶端的影響，您可以在維護時段期間執行資料庫還原。

撰寫您的應用程式，以利用指數輪詢重試，妥善處理資料庫連線失敗。這可讓您的應用程式在還原期間無法使用資料庫連線時復原，而不會造成應用程式意外損毀。

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，您也可以使用安全性群組規則來限制前一個執行個體的流量，直到您滿意不再需要該執行個體為止。若要逐步解除委任的方法，請先限制

安全性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予以停止。最後，建立資料庫執行個體的快照，並予以刪除。

Backup 與 DynamoDB 原

DynamoDB 資料庫提供 PITR，因此會備份 DynamoDB 資料資料表的資料。啟用後，DynamoDB 資料庫會保留最近 35 天的資料表的增量備份，直到您明確表格關閉。

您也可以使用 DynamoDB 主控台、或 DynamoDB API 來建立動態資料表的隨選備份。AWS CLI如需詳細資訊，請參閱備份 DynamoDB 資料表。您可以使用排程定期或 future 備份方法AWS Backup，或使用 Lambda 函數來自訂和自動化備份方法。如需使用 Lambda 函數進行 DynamoDB Backup 的詳細資訊，請參閱無伺服器解決方案以排定 Amazon DynamoDB 資料隨需備份。如果您不希望建立排程指令碼和清理任務，可以使AWS Backup用建立備份計畫。備份計劃包括 DynamoDB 表的排程和保留政策。 AWS Backup建立備份，並根據您的保留排程刪除先前的備份。 AWS Backup此外，還包括 DynamoDB 服務無法使用的進階 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副本。如需詳細資訊，請參閱進階 DynamoDB 備份。

您必須在還原的 DynamoDB 表格上手動設定下列項目：

- 自動調整規模政
- IAM 政策
- Amazon CloudWatch 指標和警示
- Tags (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。

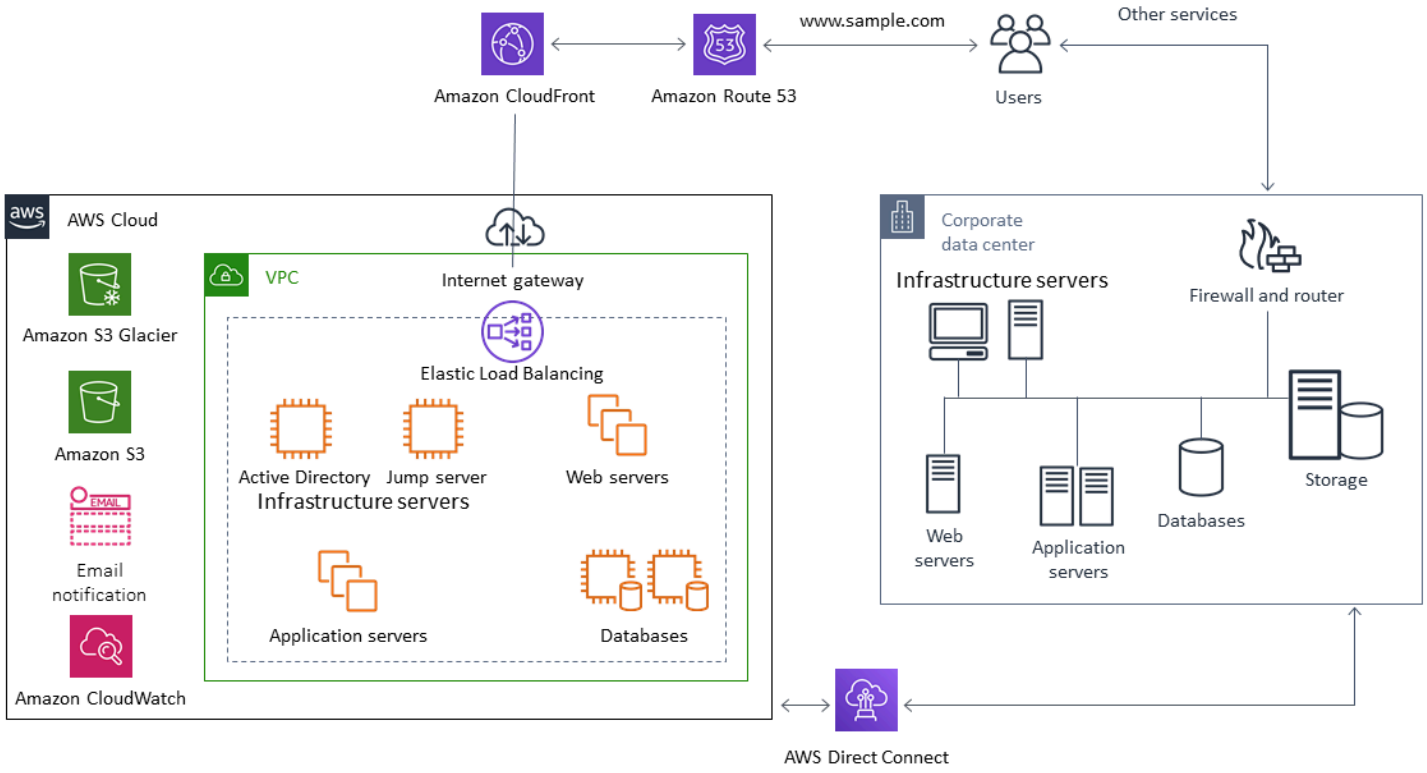
您的還原程序必須考慮如何將用戶端導向至使用新還原的表格名稱。您可以將應用程式和用戶端設定為從組態檔、AWS Systems Manager參數存放區值或其他可動態更新以反映用戶端應使用的表名稱的參考擷取 DynamoDB 表名稱。

作為還原過程的一部分，您應該仔細考慮切換過程。您可以選擇透過 IAM 許可拒絕存取現有 DynamoDB 表格，並允許存取新表格。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 表與新還原的 DynamoDB 表之間的差異。

混合架構 Backup 與恢復

本指南中討論的雲原生部署和本地部署可以組合到混合方案中，其中工作負載環境具有本地部署和AWS基礎設施組件。資源（包括 Web 服務器、應用程序服務器、監視服務器、數據庫和 Microsoft 活動目錄）託管在客户數據中心或AWS。運行的應用程序AWS雲連接到本地運行的應用程序。

這正在成為企業工作負載的常見情況。許多企業擁有自己的數據中心，並使用AWS以增強能力. 這些客户數據中心通常連接到AWS網絡通過高容量網絡鏈路。例如，使用AWS Direct Connect，您可以建立從現場部署資料中心至AWS。這提供了帶寬和一致的延遲，以便將數據上傳到雲以實現數據保護。它還為混合工作負載提供一致的性能和延遲。下圖提供了混合環境方法的一個示例。



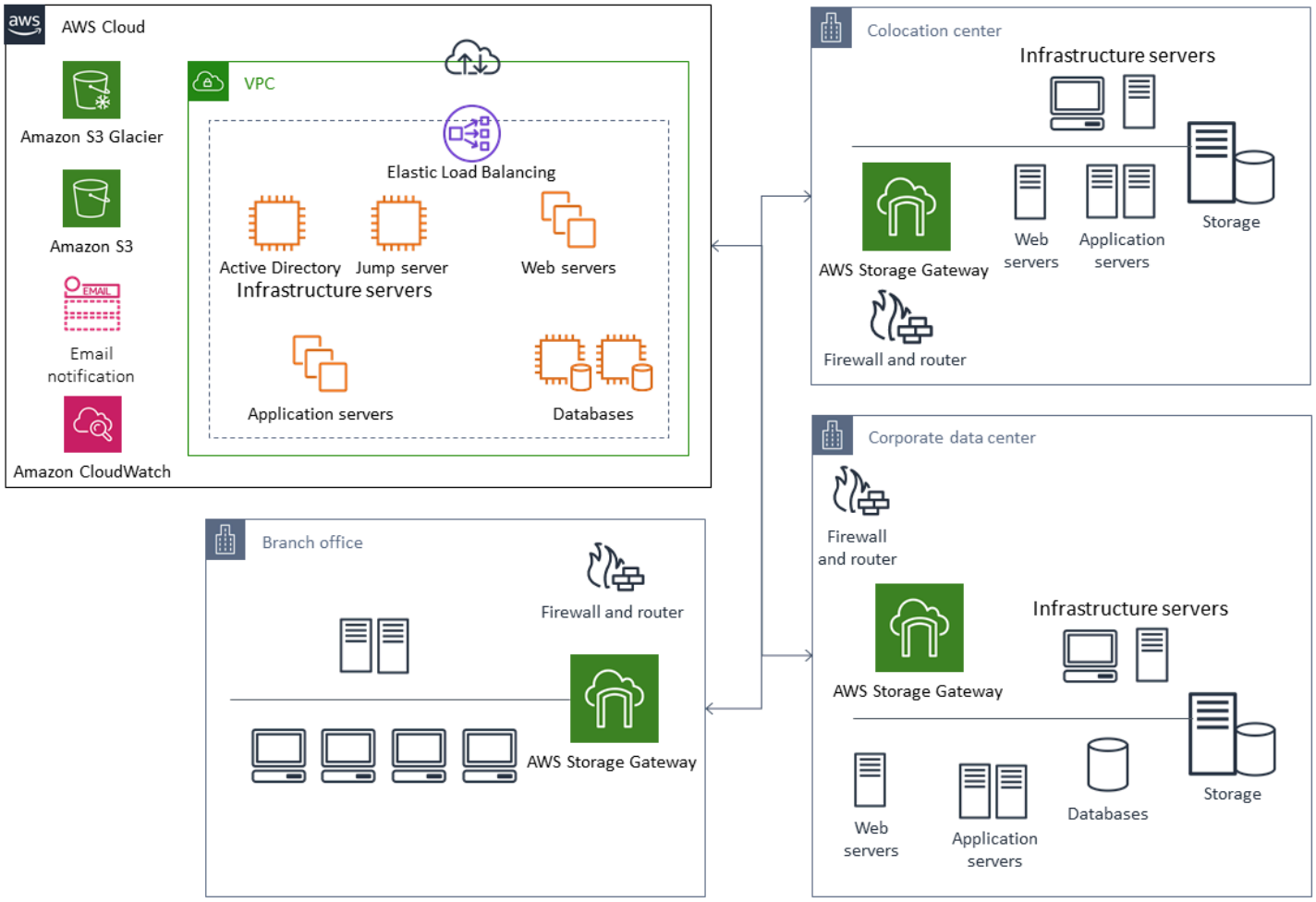
精心設計的數據保護解決方案通常使用本指南中的雲原生解決方案和本地解決方案中描述的選項的組合。許多 ISV 為本地基礎架構提供了市場領先的備份和恢復解決方案，並擴展了他們的解決方案以支持混合方法。

將集中式備份管理解決方案遷移到雲中以提高可用性

通過使用現有的備份管理解決方案投資AWS，您可以改進方法的恢復能力和體繫結構。您可能有一個主備份服務器和一個或多個介質或存儲服務器位於本地的多個位置，靠近它們所保護的服務器和服務。在這種情況下，請考慮將主備份服務器移動到 EC2 實例，以保護其免受本地災難和高可用性。

要管理備份數據流，您可以在 EC2 實例上創建一個或多個媒體服務器將保護的服務器位於同一區域。EC2 實例附近的媒體服務器可為您節省互聯網傳輸資金。當您備份到 Amazon S3 或 Amazon S3 Glacier 時，媒體服務器會提高整體備份和恢復性能。

您還可以使用 Storage Gateway 提供集中式雲訪問來自地理位置分散的數據中心和辦公室的數據。例如，通過文件網關，您可以按需、低延遲地訪問存儲在AWS，瞭解可以跨越全球的應用程序工作流。您可以使用緩存刷新等功能刷新地理位置中的數據，以便在您的辦公室之間輕鬆共享內容。



使用災難復原AWS

備份和還原方法以及支援服務和技術可用於實作災難復原 (DR) 解決方案。許多企業都在使用AWS用於備份和還原以及作為 DR 站點的雲端。AWS提供許多支援災難復原 (DR) 和業務持續性的服務和功能。

主題

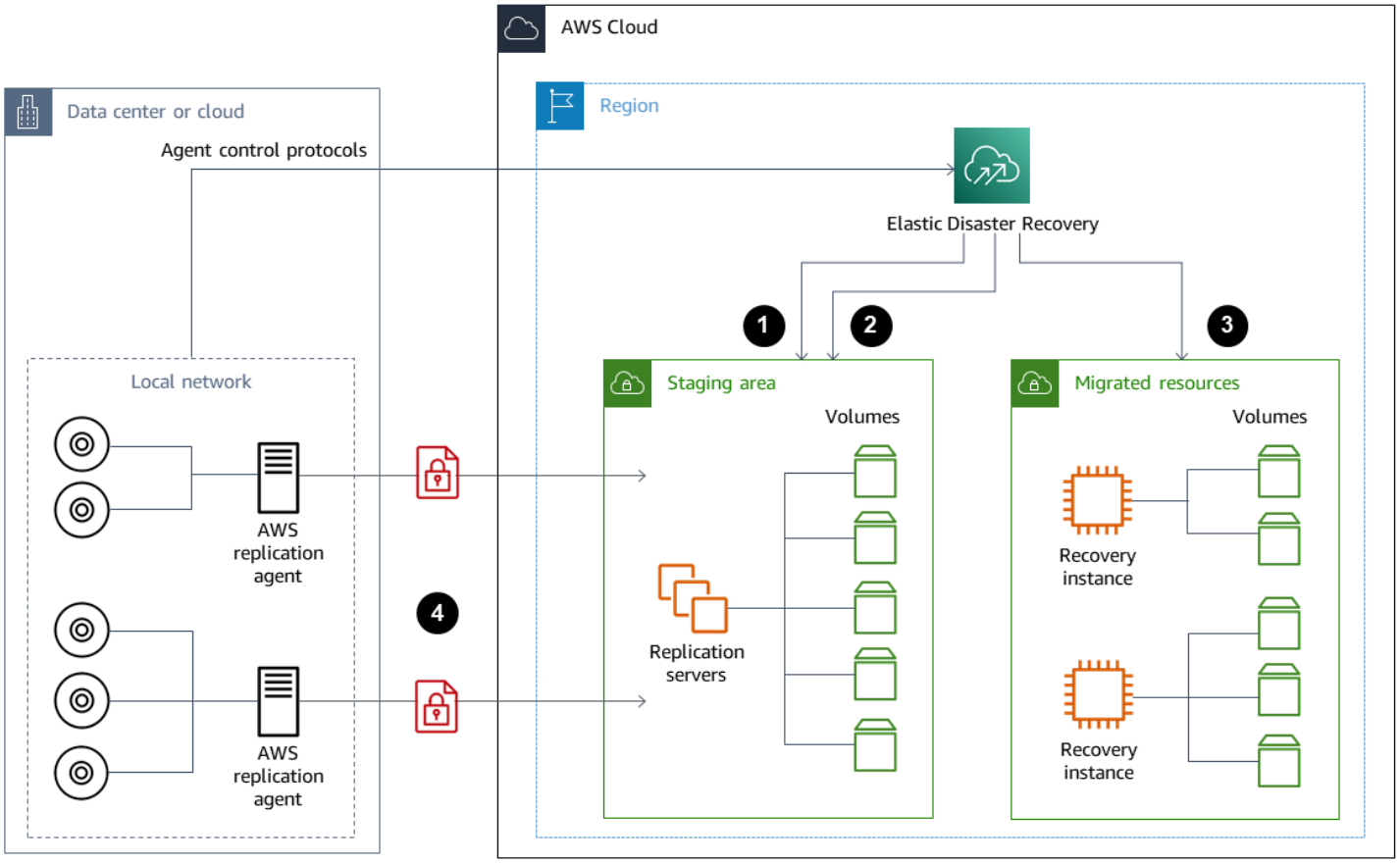
內部部署 DR 至AWS

使用AWS作為內部部署工作負載的異地災難復原 (DR) 環境是常見的混合案例。在選擇要使用的技術之前，先定義災難復原目標，包括所需的復原時間和復原點目標。若要協助定義，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。請務必將所有工作負載相依性納入考量，並徹底定期測試 DR 計劃和解決方案，以驗證其完整性。

AWS提供AWS Elastic Disaster Recovery用於在上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。彈性災難復原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，且偏好 AWS 區域。區塊層級複寫是伺服器儲存空間的精確複本，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，您可以指示彈性災難復原在幾分鐘內以完全佈建的狀態快速啟動數千台機器。

彈性災難復原會使用安裝在每個內部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在上執行的低功率 Amazon EC2 等效項目同步化AWS。您也可以使用彈性災難復原將 DR 容錯移轉和容錯回復程序自動化。自動化容錯移轉和容錯回復程序可協助您達成更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資源
3. 以 RTO 啟動的復原執行個體 (分鐘) 和 RPO (秒)
4. 連續區塊層級複寫 (壓縮和加密)

請務必測試 DR 程序，並確認即時測試環境不會與內部部署環境產生衝突。例如，確認適當的授權可在內部部署、預備和起始的 DR 環境中使用且正常運作。同時確認任何可能從中央資料庫輪詢和提取工作的 Worker 類型處理序都已適當配置，以避免重疊或衝突。在 DR 程序中，請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。此外，還包括復原伺服器執行處理上線且可用之後要執行的步驟。您可以使用解決方案AWS Elastic Disaster Recovery計劃自動化方案或另一種協助您自動化 DR 計劃的方法。

您可以使用儲存閘道磁碟區閘道為您的內部部署伺服器提供雲端磁碟區。您也可以使用 Amazon EBS 快照快照快速佈建這些磁碟區，以便與 Amazon EC2 搭配使用。特別是，儲存磁碟區閘道為您的內部部署應用程式提供對其整個資料集的低延遲存取。磁碟區閘道也提供耐用的快照型備份，可還原以供內

部部署使用或搭配 Amazon EC2 使用。您可以安排point-in-time以工作負載的復原點目標 (RPO) 為基礎的快照。

> **Important**
>
> 磁碟區閘道磁碟區的目的是做為資料磁碟區使用，而非開機磁碟區。

您可以將 Amazon EC2 Amazon 機器映像 (AMI) 搭配與現場部署伺服器相符的組態搭配使用，並分別指定資料磁碟區。設定並測試 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。此方法要求您徹底測試環境，以驗證 EC2 執行個體是否正常運作，尤其是 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符合 DR 目標。AWS在全球各地的區域提供多個可用區域。許多企業使用AWS雲端會調整其工作負載架構和災難復原目標，以承受可用區域的損失。該可靠性支柱在AWS架構良好的框架支持這種最佳實踐。您可以架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，您可以將 DR 自動化並實現災難復原目標，而且只需最少甚至不需要干預。

但實際上，您可能會發現無法為所有元件建立冗餘、使用中和自動化的架構。檢查架構的每一層，以判斷達成目標所需的災難復原程序。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AWS服務，您可以參考AWS文件以決定高可用性和 DR 選項。

適用於單一可用區域中的亞馬遜 EC2 DR

嘗試架構您的工作負載，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 自動擴展和彈性負載平衡來實現適用於 Amazon EC2 和其他服務的異地同步備份伺服器架構。

如果您的架構具有無法進行負載平衡的 EC2 執行個體，且在任何特定時刻只能執行單一執行個體，則可以使用下列任一選項。

- 建立 Auto Scaling 群組，其大小下限、最大和所需大小為 1，並針對多個可用區域進行設定。創建一個 AMI，如果實例失敗，可用於替換實例。請務必定義適當的自動化和設定，以便 AMI 新佈建的執行個體可以自動設定並提供服務。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。您也可以選擇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，並讓用戶端使用此記錄連線。建立指令碼以建立作用中執行個體的新 AMI，並使用 AMI 在單獨的可用區域中佈建處於停止狀態的新 EC2 執行個體。設定指

令碼定期執行，並終止先前停止的執行個體。如果可用區域發生故障，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。

模擬解決方案設計用來防範的故障，徹底測試您的解決方案。此外，也請考慮您的 DR 解決方案隨著工作負載架構的變更而需要的更新。

區域故障中亞馬遜 EC2 的 DR

雖然AWS區域故障是罕見的，這是可能的AWS地區可能會在未來的某個時候失敗。客戶必須仔細權衡建立和維護多區域災難復原計劃所需的複雜性、成本和精力，以及效益。AWS提供支援全球可用性、容錯移轉和 DR 的多區域架構的功能本指南涵蓋 Amazon EC2 備份和復原專用的一些可用功能。

AWSAMI 和 Amazon EBS 快照是區域資源，可用於在單一區域內佈建新執行個體。但是，您可以將快照和 AMI 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。若要支援區域故障災難復原計劃，您可以將 AMI 和快照複製到其他區域的程序自動化。AWS BackupAmazon 資料生命週期管理員支援跨區域複製作為備份組態的一部分。

AWS Elastic Disaster Recovery可用於自動化並持續將一個區域中的 Amazon EC2 伺服器複寫到另一個 DR 區域。彈性災難復原可簡化您的多區域災難復原方法，並協助您使用演習定期測試跨區域 Amazon EC2 DR 計劃。當備份和復原無法達到 RTO 和 RPO 目標時，彈性災難復原可以提供協助。彈性災難復原可以幫助您將 RTO 降低到幾分鐘，並將 RPO 降低到低於一秒的範圍。

無論您使用哪種解決方案，都必須判斷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

清理備份

若要降低成本，請清除復原或保留不再需要的備份。您可以使用AWS Backup和 Amazon 資料生命週期管理員，自動化部分備份的保留政策。但是，即使使用了這些工具，您仍然需要對單獨進行的備份採取清理方法。

標籤策略是清理策略的先決條件。使用標籤來識別應清理的資源、適當地通知擁有者，以及自動化您的清理程序。備份建立者AWS建立日期與其對齊，但標記對於將備份與工作負載、保留需求和還原點識別相互關聯非常重要。

您可以使用自動化來實作快照的清理程序。例如，您可以掃描帳戶中的快照，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臨界值進一步篩選結果。使用附加至磁碟區的標籤，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程刪除。此自動補救可透過使用AWS Config規則，腳本使用AWS CLI，或使用AWSSDK。

系統管理員提供AWS-代表VolumeSnapshots和AWS-DeleteSnapshot可協助您啟動和自動清理 Amazon EBS 快照的文件。您也可以使用AWS CLI和AWSSDK 自動清理其他AWS資源，例如亞馬遜 RDS 快照。

備份與復原常見問題

我應該選擇什麼備份排程？

定義與復原點目標 (RPO) 保持一致的備份排程頻率。定義當您的工作負載處於最少負載量時以及何時可以減少使用者影響的備份時間。創建一個point-in-time每當您要對工作負載進行重大變更時，都可以進行快照。

我是否需要在開發帳戶中建立備份？

在執行重大變更之前，測試開發帳戶中可能發生的重大變更，並建立備份。你可能還有更多point-in-time開發和測試活動的開發和非生產帳戶中的復原 (PITR) 備份。

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

快照以非同步方式發生；point-in-time快照會立即建立，但快照的狀態仍處於擱置狀態，直到所有修改後的區塊都傳輸到 Amazon S3 為止。對於大型初始快照或許多區塊已變更的後續快照，傳輸可能需要數小時。正在傳輸時，進行中的快照不會受到磁碟區的持續讀取和寫入影響。如需詳細資訊，請參閱 AWS 文件。

後續步驟

首先，在非生產環境中評估、實作和測試您的備份和復原方法。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非常重要。

除了架構中的所有元件之外，還可測試架構中單一元件的還原程序。驗證每個項目的復原時間。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，並確認下游對備份的影響。

其他資源

AWS 資源

- AWS規定指引
- AWS 文件集
- AWS 一般參考資料
- AWS 詞彙表

AWS 服務

- AWS Backup
- Amazon CloudWatch
- 亞馬遜CloudWatch活動
- AWS Config
- Amazon DynamoDB
- Amazon EBS
- Amazon EC2
- IAM
- Amazon RDS
- Amazon Simple Storage Service (Amazon S3)
- Amazon S3 Glacier
- 儲存閘道
- AWS Systems Manager

其他資源

- 備份與復原AWS Backup（解決方案）
- 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)
- DR 計劃檢查清單
- 備份和復原方法使用AWS(技術文件 — 已封存)

- AWS Backup 入門
- AWS市場 — 備份和還原

文件歷史紀錄

下表說明本指南的重大變更。如果您想收到有關 future 更新的通知，您可以訂閱 RSS 摘要。

變更	描述	日期
更新資訊	已更新內部部署 DR 目標AWS區段中的資訊。	2023 年 4 月 13 日
增加了一個部分	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
新增有關彈性災難復原的資訊，並新增說明	在災難復原使用AWS和選擇資料保護AWS服務區段中，新增了關於AWS Elastic Disaster Recovery. 在具有快照和 AMI 的 Amazon EC2 備份和復原中，在建立快照或 AMI 之前準備一個 EBS 磁碟區，以及從 Amazon EBS 快照或 AMI 區段還原，新增說明。已新增至 Backup 與復原常見問題集。	2023 年 1 月 19 日
添加了一個鏈接	在 Amazon Data Lifecycle Manager 區段中新增 Amazon Data Lifecycle Manager 文件的連結。	2022 年 10 月 31 日
更新資訊	更新了還原磁碟區的相關資訊。	2022 年 8 月 30 日
更新信息，並添加了新的部分	在 [選擇用於資料保護的AWS服務] 區段中，新增服務。新增使用 AWS Backup Backup 備份和復原部分。在使用 Amazon S3 和 Amazon S3 冰川進行 Backup 和復原部分，新增了有關新的 Amazon S3	2022 年 1 月 28 日

	冰川儲存類別的資訊。在使用 EBS 磁碟區的 Amazon EC2 Backup 和復原區段中，新增了文件和其他資訊的連結。在「Backup 與復原雲端原生AWS服務」區段中，新增要使用的建議AWS Backup。在「其他資源」區段中，新增資源。	
更新資訊	已新增有關設定儲存類別至 S3 Glacier 彈性擷取區段的資訊。已新增有關擷取快照至 Amazon EC2 備份和使用快照和 AMI 進行復原的相關資訊。	2021 年 9 月 9 日
更新資訊	在此AWS Backup區段中，已新增AWS Backup支援AWS服務的相關資訊。	2021 年 6 月 1 日
初始出版	—	2020 年 7 月 29 日

《AWS 方案指引》詞彙表

以下是由《AWS 方案指引》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：將您的內部部署 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：將您的內部部署 Oracle 資料庫遷移至 AWS 雲端中的 Amazon Relational Database Service (Amazon RDS) for Oracle。
- 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：將您的內部部署 Oracle 資料庫遷移至 AWS 雲端中 EC2 執行個體上的 Oracle。
- 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。此遷移案例特定於 VMware Cloud on AWS，它支援內部部署環境與 AWS 之間的虛擬機器 (VM) 相容性和工作負載可移植性。在將基礎設施遷移至 VMware Cloud on AWS 時，您可以使用內部部署資料中心的 VMware Cloud Foundation 技術。範例：將託管 Oracle 資料庫的虛擬機器監視器重新放置到 VMware Cloud on 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

請參閱以屬性為基礎的存取控制。

抽象的服務

請參閱受管理服務。

酸

請參閱原子性、一致性、隔離性、耐用性。

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。它比主動-被動遷移更具彈性，但需要更多的工作。

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。

聚合函數

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

AI

請參閱人工智慧。

艾奧運

請參閱人工智慧作業。

匿名化

永久刪除資料集中個人資訊的程序。匿名化可以幫助保護個人隱私。匿名資料不再被視為個人資料。

反模式

一種經常使用的解決方案，用於解決方案的生產力適得其反，效果不佳或效果低於替代方案。

應用控制

一種安全性方法，只允許使用核准的應用程式，以協助保護系統免受惡意軟體的攻擊。

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) 文件中的適用於 AWS 的 ABAC。

授權資料來源

儲存資料主要版本的位置，被認為是最可靠的資訊來源。您可以將授權資料來源中的資料複製到其他位置，以便處理或修改資料，例如匿名化、編輯或將其化名化。

可用區域

AWS 區域 內一個有所區別的位置，隔離了其他可用區域的故障，並對同區域內的其他可用區域提供低成本、低延遲的網路連線。

AWS 雲端採用架構 (AWS CAF)

AWS 的指導方針和最佳實務架構，可協助組織制定高效且有效的計畫以成功移至雲端。AWSCAF 將指引分為六個焦點區域 (稱為層面)：業務、人員、控管、平台、安全和操作。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。對於此層面，AWS CAF 為人員發展、培訓和通訊提供指引，以協助組織為成功採用雲端做好準備。如需詳細資訊，請參閱 AWS CAF 網站和 AWS CAF 白皮書。

AWS Workload Qualification Framework (AWS WQF)

一種評估資料庫遷移工作負載、建議遷移策略並提供工作預估的工具。AWSWQF 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

BCP

請參閱業務連續性規劃。

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「位元順序」。

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。

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)。

防碎玻璃訪問

在特殊情況下，並透過核准的程序，使用者可以快速取得他AWS 帳戶們通常沒有存取權限的存取權。如需詳細資訊，請參閱 AWS Well-Architected 指南中的實作防破玻璃程序指標。

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

咖啡

請參閱AWS雲端採用架構。

CCoE

請參閱雲端卓越中心。

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來測試系統的彈性。您可以使用 AWS Fault Injection Service(AWS FIS) 執行實驗來 stress 您的AWS工作負載並評估其回應。

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，在本機對資料進行加密。

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。雲計算通常連接到邊緣計算技術。

雲端運作模式

在 IT 組織中，這是用來建置、成熟和最佳化一或多個雲端環境的作業模型。如需詳細資訊，請參閱建立您的雲端作業模型。

採用雲端階段

組織遷移至 AWS 雲端時通常會經歷以下四個階段：

- 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 在 AWS 雲端企業策略部落格上的部落格文章邁向雲端優先之旅和採用階段中定義。如需有關其與 AWS 遷移策略如何相關的資訊，請參閱遷移準備程度指南。

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。常見的雲存儲庫包括 GitHub 或AWS CodeCommit。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。查詢此類資料時，通常可以接受慢速查詢。將此資料移至效能較低且成本較低的儲存層或類別可降低成本。

電腦視覺

機器使用的 AI 領域，可以準確識別圖像中的人，地點和事物，在人類水平或以上。它通常使用深度學習模型構建，可以自動從單個圖像或一系列圖像中提取，分析，分類和理解有用的信息。

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

AWS Config 規則和補救措施的集合，您可以將其組合起來以自訂合規和安全檢查。使用 YAML 範本，您可以在 AWS 帳戶 和區域中將一致性套件部署為單一實體，或者跨組織部署。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。

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 中安全支柱的一個組成部分。如需詳細資訊，請參閱資料分類。

資料漂移

生產資料與用來訓練 ML 模型的資料之間有意義的變化，或輸入資料隨著時間的推移有意義的變化。資料漂移可降低 ML 模型預測中的整體品質、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。

資料最小化

僅收集和處理絕對必要的數據的原則。在中執行資料最小化AWS 雲端可降低隱私權風險、成本和分析碳足跡。

資料周長

您AWS環境中的一組預防性護欄，可協助確保只有受信任的身分正在存取來自預期網路的受信任資源。若要取得更多資訊，請參閱〈在上建置資料周長〉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。

數據來源

在整個生命週期中追蹤資料來源和歷史記錄的程序，例如資料的產生、傳輸和儲存方式。

資料主體

正在收集和處理資料的個人。

資料倉儲

支援商業智慧 (例如分析) 的資料管理系統。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。

defense-in-depth

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。在 AWS 上採用此策略時，可以在 AWS Organizations 結構的不同層上新增多個控制，以協助保護資源。例如，一 defense-in-depth 種方法可能會結合多因素驗證、網路分段和加密。

委派的管理員

在 AWS Organizations 中，相容的服務可以註冊 AWS 成員帳戶，用於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。

發展價值流映射

用於識別限制並排定優先順序，對軟體開發生命週期中的速度和品質產生不利影響的程序。DVSM 擴展了最初為精益生產實踐而設計的價值流映射流程。它著重於創造和通過軟件開發過程中移動價值所需的步驟和團隊。

數字雙胞胎

真實世界系統的虛擬表現法，例如建築物、工廠、工業設備或生產線。數位雙胞胎支援預測性維護、遠端監控和生產最佳化。

維度表

在 star 結構描述中，較小的資料表包含事實資料表中定量資料的相關資料屬性。維度表格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、篩選和結果集標籤。

災難

防止工作負載或系統在其主要部署位置達成其業務目標的事件。這些事件可能是自然災害、技術故障或人為行為造成的結果，例如意外設定錯誤或惡意軟體攻擊。

災難復原 (DR)

您使用的策略和程序，將因災難造成的停機時間和資料遺失降到最低。如需詳細資訊，請參閱 AWS Well-Architected 的架構中的雲端中的工作負載的災難復原AWS：雲端復原。

DML

請參閱資料庫操作語言。

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。

博士

請參閱災難復原。

漂移檢測

追蹤基線組態的偏差。例如，您可以用AWS CloudFormation來偵測系統資源中的漂移，也可以用AWS Control Tower來偵測 landing zone 中可能會影響法規遵循治理要求的變更。

DVSM

請參閱開發價值流映射。

E

EDA

請參閱探索性資料分析。

邊緣運算

提升 IoT 網路邊緣智慧型裝置運算能力的技術。與雲計算相比，邊緣計算可以減少通信延遲並縮短響應時間。

加密

一種計算過程，將純文本數據（這是人類可讀的）轉換為密文。

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 AWS PrivateLink 建立端點服務並向其他 AWS 帳戶 或 AWS Identity and Access Management (IAM) 主體授予許可。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。

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) 文件中的封套加密。

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 Epic 包括身分和存取管理、偵測性控制、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。

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

事實表

星型架構中的中央表格。它存儲有關業務運營的定量數據。事實資料表通常包含兩種類型的資料欄：包含計量的資料欄，以及包含維度表格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減少開發生命週期的理念。這是敏捷方法的關鍵組成部分。

故障隔離邊界

在中AWS 雲端，可用區域、AWS 區域控制平面或資料平面等界限，可限制故障的影響，並協助改善工作負載的彈性。如需詳細資訊，請參閱AWS錯誤隔離邊界。

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。有關詳情，請參閱機器學習模型可解釋性：AWS。

特徵轉換

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

FGAC

請參閱精細的存取控制。

精細的存取控制 (FGAC)

使用多個條件來允許或拒絕訪問請求。

閃切遷移

一種資料庫移轉方法，透過變更資料擷取使用連續資料複寫，在最短的時間內移轉資料，而不是使用階段化方法。目標是將停機時間降至最低。

G

地理阻塞

請參閱地理限制。

地理限制 (地理封鎖)

在 Amazon 中 CloudFront，防止特定國家/地區的使用者存取內容分發的選項。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 工作流程被認為是遺留的，基於主幹的工作流程是現代的首選方法。

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。它們是通過使用AWS Config，Amazon AWS Security Hub GuardDuty，AWS Trusted Advisor亞馬遜檢查 Amazon Inspector 和自定義AWS Lambda檢查來實現的。

H

公頃

查看高可用性。

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)

工作負載在遇到挑戰或災難時持續運作的能力，無需干預。HA 系統的設計可自動容錯移轉、持續提供高品質的效能，以及處理不同的負載和故障，並將效能影響降到最低。

歷史學家現代化

一種用於現代化和升級操作技術 (OT) 系統的方法，以更好地滿足製造業的需求。歷史學家是一種類型的數據庫，用於收集和存儲工廠中的各種來源的數據。

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。

熱數據

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的儲存層或類別，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，hotfix 通常是在典型的 DevOps 發行工作流程之外進行。

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

查看基礎結構即程式碼。

身分型政策

附接至一個或多個 IAM 主體的政策，可在 AWS 雲端 環境內部定義其許可。

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。

不可變基礎設施

為生產工作負載部署新基礎結構的模型，而不是更新、修補或修改現有基礎結構。不可變的基礎架構本質上比可變基礎架構更加一致、可靠且可預測。如需詳細資訊，請參閱 Well-Architected 的架構中的使用不可變基礎結AWS構進行部署最佳作法。

傳入 (輸入) VPC

AWS 多帳戶架構中的 VPC，可接受、檢查和路由來自應用程式外部的網路連線。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。

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

AWS 多帳戶架構中的集中式 VPC，可管理 VPC (在相同或不同 AWS 區域 中)、網際網路和內部部署網路之間的網路流量的檢查。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 AWS 的機器學習模型可解釋性。

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

以標籤為基礎的存取控制 (LBAC)

強制存取控制 (MAC) 的實作，其中每個使用者和資料本身都明確指派一個安全性標籤值。使用者安全性標籤與資料安全性標籤之間的交集決定了使用者可以看到哪些列與欄。

登陸區域

登陸區域是一個可擴展且安全的、架構良好的多帳戶 AWS 環境。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。

大型遷移

遷移 300 部或更多伺服器。

LBAC

請參閱以標示為基礎的存取控制。

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

見 7 盧比

小端序系統

首先儲存最低有效位元組的系統。另請參閱 「位元順序」。

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。

受管理服務

AWS 服務用於AWS操作基礎架構層、作業系統和平台，並且您可以存取端點以儲存和擷取資料。Amazon Simple Storage Service (Amazon S3) 和 Amazon DynamoDB 是受管服務的範例。這些也被稱為抽象的服務。

MAP

請參閱 Migration Acceleration Program。

機制

一個完整的過程，您可以在其中創建工具，推動工具的採用，然後檢查結果以進行調整。機制是一個循環，它加強和改善自己，因為它運行。如需詳細資訊，請參閱 AWS Well-Architected 的架構中建置機制。

成員帳戶

管理帳戶之外的所有 AWS 帳戶，屬於 AWS Organizations 中組織的一部分。一個帳戶一次只能是一個組織的成員。

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 AWS 無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 AWS 上實作微服務。

Migration Acceleration Program (MAP)

一個提供諮詢支援、培訓和服務的 AWS 計畫，以協助組織為移至雲端建置強大的營運基礎，並協助抵消遷移的初始成本。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。移轉工廠團隊通常包括營運、業務分析師和擁有者、移轉工程師、開發人員和 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 將遷移重新託管至 Amazon EC2。

遷移組合評定 (MPA)

一種線上工具，提供用於驗證遷移至 AWS 雲端的業務案例的資訊。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) 免費提供給所有 AWS 顧問和 APN 合作夥伴顧問。

遷移準備程度評定 (MRA)

使用 AWS CAF 深入了解組織的雲端準備狀態、識別優缺點並制定動作計畫來彌補已識別差距的程序。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

用於將工作負載遷移至 AWS 雲端的方法。如需詳細資訊，請參閱本詞彙表中的 7 Rs 項目，並參閱動員您的組織以加速大規模移轉。

ML

請參閱機器學習。

MPA

請參閱移轉組合評估。

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 AWS 雲端中應用程式現代化策略。

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，請參閱評估 AWS 雲端中應用程式的現代化準備情況。

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。

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？」

可變的基礎

更新和修改生產工作負載現有基礎結構的模型。為了提高一致性，可靠性和可預測性，AWSWell-Architected 框架建議使用不可變的基礎結構作為最佳實踐。

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

請參閱作業整合。

OLA

請參閱作業層級協定。

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。

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)。

操作準備程度檢討 (ORR)

問題和相關最佳做法的檢查清單，可協助您瞭解、評估、預防或減少事件和可能的故障範圍。如需詳細資訊，請參閱 AWS Well-Architected 的架構中的作業準備檢閱 (ORR)。

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 AWS CloudTrail 建立的追蹤，它會記錄 AWS Organizations 中某個組織的所有 AWS 帳戶 的所有事件。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文件中的為組織建立追蹤。

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)

在中 CloudFront，限制存取權限以保護 Amazon Simple Storage Service (Amazon S3) 內容的增強選項。OAC 支援 AWS 區域 中的所有 S3 儲存貯體、具有 AWS KMS (SS-KMS) 的伺服器端加密以及對 S3 儲存貯體的動態 PUT 和 DELETE 請求。

原始存取身分 (OAI)

在中 CloudFront，用於限制存取以保護 Amazon S3 內容的選項。當您使用 OAI 時， CloudFront 會建立 Amazon S3 可用來進行驗證的主體。經驗證的主體只能透過特定散發存取 S3 儲存 CloudFront 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

請參閱作業整備檢閱。

傳出 (輸出) VPC

AWS 多帳戶架構中的 VPC，它可處理從應用程式內部啟動的網路連線。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。

個人識別資訊 (PII)

直接查看或與其他相關數據配對時，可用於合理推斷個人身份的信息。PII 的範例包括姓名、地址和聯絡資訊。

PII

請參閱個人識別資訊。

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。

政策

可以定義權限 (請參閱以身分識別為基礎的策略)、指定存取條件 (請參閱以資源為基礎的策略) 或定義組織中所有帳戶的最大權限的物件 AWS Organizations (請參閱服務控制策略)。

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`，通常位於子`WHERE`句中。

謂詞下推

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。這樣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

AWS 中的實體，可以執行動作和存取資源。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。

隱私設計

一種系統工程方法，在整個工程過程中將隱私權納入考量。

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。這些控制項會在資源佈建之前進行掃描。如果資源不符合控制項，則不會佈建該資源。如需詳細資訊，請參閱AWS Control Tower文件中的控制項參考指南，並參閱實作安全性控制中的主動控制AWS。

生產環境

請參閱環境。

化名化

以預留位置值取代資料集中的個人識別碼的程序。假名化可以幫助保護個人隱私。假名化數據仍被認為是個人數據。

Q

查詢計劃

一系列步驟，如指示，用來存取 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

拉齊矩陣

請參閱負責任，負責，諮詢，通知（RACI）。

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。

拉西矩陣

請參閱負責任，負責，諮詢，通知（RACI）。

RCAC

請參閱列與欄存取控制。

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。

重新建築師

見 7 盧比

復原點目標 (RPO)

自上次資料復原點以來可接受的時間上限。這決定了最後一個恢復點和服務中斷之間可接受的數據丟失。

復原時間目標 (RTO)

服務中斷與恢復服務之間的最大可接受延遲。

重構

見 7 盧比

區域

地理區域中 AWS 資源的集合。每個 AWS 區域 都是獨立的且獨立於其他區域，以提供容錯能力、穩定性和恢復能力。如需詳細資訊，請參閱 AWS 一般參考 中的管理 AWS 區域。

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。

重新主持

見 7 盧比

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

見 7 盧比

再平台

見 7 盧比

買回

見 7 盧比

資源型政策

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

負責者、當責者、事先諮詢者和事後告知者 (RACI) 矩陣

定義移轉活動和雲端作業所有相關方的角色和職責的矩陣。矩陣名稱衍生自矩陣中定義的責任類型：負責 (R)、負責 (A)、諮詢 (C)，以及通知 (I)。支撐（S）類型是可選的。如果您包含支援，則該矩陣稱為 RASCI 矩陣，如果您將其排除，則稱為 R ACI 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

見 7 盧比

退休

見 7 盧比

旋轉

定期更新密碼以使攻擊者更難以存取認證的程序。

資料列與資料行存取控制 (RCAC)

使用已定義存取規則的基本、彈性 SQL 運算式。RCAC 由資料列權限和資料行遮罩所組成。

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

許多身份提供者（IdPs）使用的開放標準。此功能可啟用聯合單一登入 (SSO)，因此使用者可以登入 AWS Management Console 或呼叫 AWS API 操作，而不必為組織中的每個人都建立一個 IAM 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。

SCP

請參閱服務控制策略。

秘密

您以加密形式儲存的機密或受限制資訊，例如密碼或使用者認證。AWS Secrets Manager它由秘密值及其中繼資料組成。密碼值可以是二進位、單一字串或多個字串。如需詳細資訊，請參閱秘密管理員說明文件中的秘密。

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。安全性控制有四種主要類型：預防性、偵測、回應式和主動式。

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

預先定義且程式化的動作，其設計用來自動回應或修復安全性事件。這些自動化作業可做為偵探或回應式安全控制項，協助您實作AWS安全性最佳實務。自動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 對其目的地的資料進行加密。

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

AWS 服務 的進入點 URL。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。

服務等級指示器 (SLI)

對服務效能層面的測量，例如錯誤率、可用性或輸送量。

服務層級目標 (SLO)

代表服務狀況的目標測量結果，由服務層次指示器測量。

共同責任模式

描述您與 AWS 共同承擔責任以確保雲端安全和合規的模型。AWS 負責雲端的安全，而您負責雲端中的安全。如需詳細資訊，請參閱共同責任模式。

暹

請參閱安全性資訊和事件管理系統。

單一故障點 (SPF)

應用程式的單一重要元件發生故障，可能會中斷系統。

SLA

請參閱服務等級協議。

SLI

請參閱服務層級指示器。

SLO

請參閱服務等級目標。

split-and-seed 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. AWS 雲端

抽

請參閱單一故障點。

星型綱要

使用一個大型事實資料表來儲存交易或測量資料，並使用一或多個較小的維度表格來儲存資料屬性的資料庫組織結構。這種結構是專為在數據倉庫中使用或用於商業智能目的。

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。

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

以模擬使用者互動以偵測潛在問題或監控效能的方式測試系統。您可以使用 Amazon CloudWatch Synthetics 來創建這些測試。

T

標籤

作為組織AWS資源的中繼資料的索引鍵值配對。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 文件中的傳輸閘道是什麼。

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

准許您指定的服務在 AWS Organizations 中的組織中以及其帳戶中代表您執行任務。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 AWS Organizations 文件中的搭配使用 AWS Organizations 和其他 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

一個小 DevOps 團隊，你可以餵兩個比薩餅。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。

無差別的任務

也稱為繁重工作，是創建和操作應用程序所必需的工作，但不能為最終用戶提供直接價值或提供競爭優勢。無差異化作業的範例包括採購、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

會危及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。

溫暖的數據

不常存取的資料。查詢此類資料時，通常可以接受中度緩慢的查詢。

視窗功能

一種 SQL 函數，可對以某種方式與當前記錄相關的一組行執行計算。視窗函數對於處理工作非常有用，例如計算移動平均值或根據目前列的相對位置存取列的值。

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。

蠕蟲

看到寫一次，多讀。

WQF

請參閱 AWS 工作負載資格架構。

寫一次，多讀（WORM）

一種儲存模型，可單次寫入資料並防止資料遭到刪除或修改。授權用戶可以根據需要多次讀取數據，但無法更改數據。這種數據存儲基礎設施被認為是不可變的。

Z

零日漏洞

一種利用零時差漏洞的攻擊，通常是惡意軟件。

零時差漏洞

生產系統中未緩解的瑕疵或弱點。威脅參與者可以利用這種類型的漏洞攻擊系統。由於攻擊，開發人員經常意識到該漏洞。

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。