



上的備份和復原方法 AWS

AWS 方案指引



AWS 方案指引: 上的備份和復原方法 AWS

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

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

Table of Contents

簡介	1
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	10
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	12
Amazon EC2 備份和復原	13
AMIs 或快照	13
伺服器磁碟區	14
個別伺服器磁碟區	15
執行個體儲存體磁碟區	15
標記和強制執行標準	16
建立 EBS 磁碟區備份	17
準備 EBS 磁碟區	17
從主控台建立快照	18
建立 AMIs	18
Amazon Data Lifecycle Manager	19
AWS Backup	20
多磁碟區備份	20
保護備份	22
封存快照	22
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	36
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
我是否需要在開發帳戶中建立備份？	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
Resources	44
文件歷史紀錄	45
.....	xlvi

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）。它還涵蓋相關的 Amazon Web Services (AWS) 服務，可用於為架構的非可變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 提供多種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
- 搭配 Amazon Elastic Compute Cloud (Amazon EC2) 的 Amazon Machine Image (AMIs)

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 是一種安全、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 作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。這兩個平台提供可靠的資料備份，在至少三個地理位置分散的可用區域中進行物件複寫。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 服務可在全球各地使用，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)
 - 認證業務標準聲明 (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。隨著需求的變化，您可以向上或向下擴展消耗量，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，並協助降低 AWS 服務的總擁有成本。會透過價格下降將這些節省成本 AWS 傳遞給客戶。
- Pay-as-you-go定價：根據需要購買 AWS 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 AWS 服務的概觀，您可以用來支援下列項目的備份和復原方法：

- 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

的成本 AWS Backup 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 彈性災難復原](#) 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。您可以從現場部署到雲端和跨區域 DR 使用 Elastic Disaster Recovery for 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](#) 安排程執行 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) 來存放和擷取任意數量的資料。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 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，為內部部署環境提供 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存放任意數量的物件。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，不需要隨著備份資料集的增長進行磁碟區或媒體管理。pay-for-what-you-use 模型和每月每 GB 的成本低，使得 Amazon S3 儲存類別適用於廣泛的資料保護使用案例。Amazon S3 儲存類別是專為不同的使用案例所設計，包括下列類別：

- [經常存取儲存類別](#)，用於經常存取資料的一般用途儲存（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。
- [不常存取長期資料的儲存體方案](#)，但不常存取的資料（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期資料（例如，每年備份）。這包括 S3 Glacier Deep Archive，可提供最低成本的儲存 AWS。

對於存取模式不明或變更的備份，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

某些儲存類別有最低的持續時間費用。如需詳細資訊，請參閱 [Amazon S3 定價](#)，並使用網頁搜尋尋找 duration。

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 週內使用 S3 Standard 的每日備份
- 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
- S3 Glacier Deep Archive 上過去 5 年的年度備份
- 在 5 年後從 S3 Glacier Deep Archive 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，建立用於備份和封存的標準 S3 儲存貯體。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 版本控制自動維護轉返歷史記錄

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能力。這對於組態檔案和其他可能比 point-in-time 備份排程更頻繁變更的物件很有用。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，您不需要自訂並重新建立 AMI 即可使用更新版本。

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，您可以快速整合至現有的自訂備份程序。您可以使用 AWS CLI、AWS SDKs 和 API 操作來整合使用 Amazon S3 的備份和還原指令碼和程序。例如，您可能有一個執行夜間資料庫匯出的資料庫備份指令碼。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

資料安全性是普遍的考量，AWS 非常重視安全性。安全性是每個的基礎 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 來加密傳輸中的資料。您可以執行下列動作來設定靜態物件的加密：

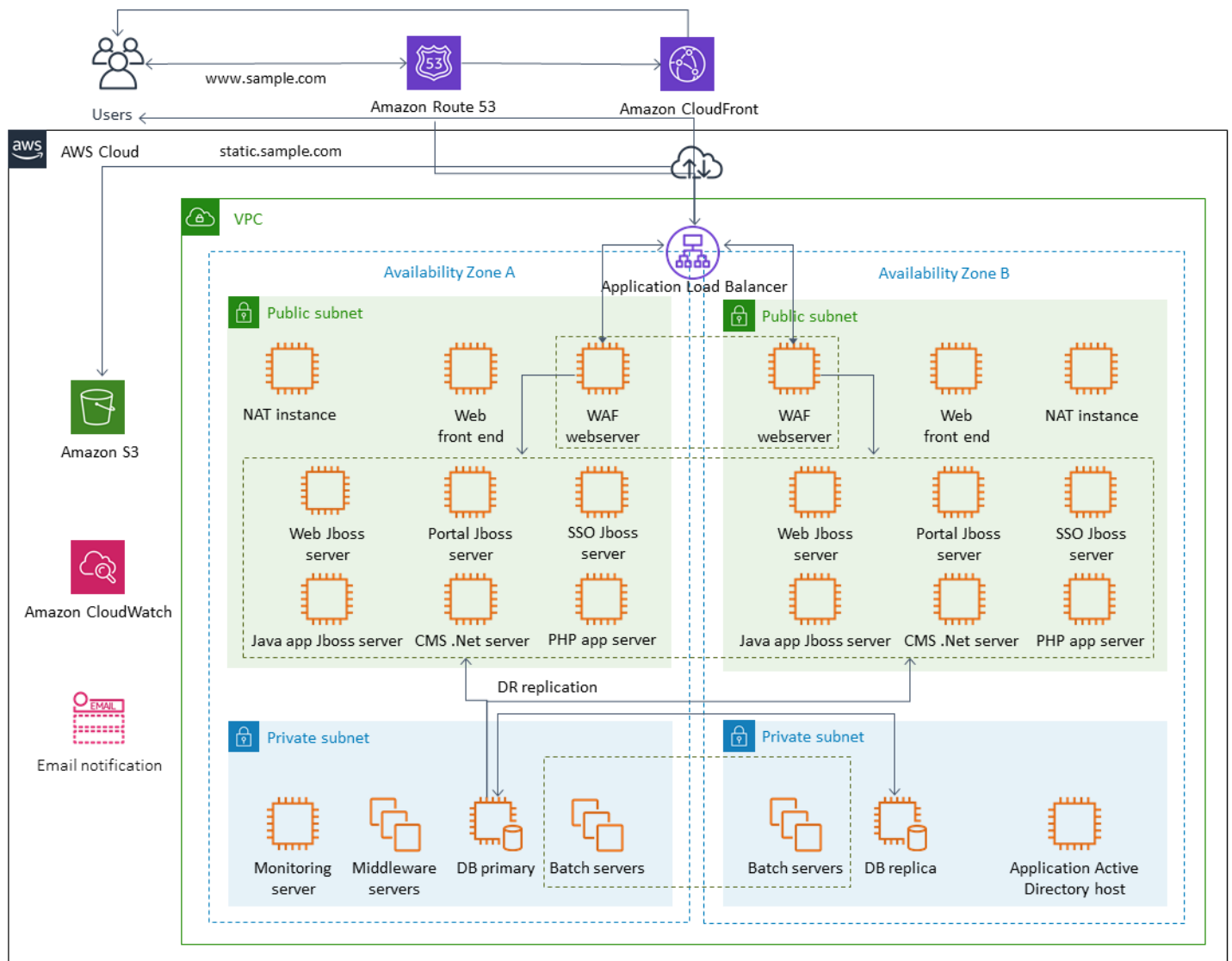
- [搭配 Amazon S3 受管加密金鑰使用伺服器端加密](#)（預設）
- [搭配中存放的 AWS Key Management Service \(AWS KMS\) 金鑰使用伺服器端加密 AWS KMS](#)
- 使用[用戶端加密](#)

您可以使用 AWS Identity and Access Management (IAM) 來控制對 S3 物件的存取。IAM 提供控制 S3 儲存貯體中個別物件和特定字首路徑的許可。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) 磁碟區或執行個體存放區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至其預定的 函數時，備份才有效。還原和復原函數應定期測試以確認這一點。

下圖中的解決方案架構說明以 Amazon EC2 為基礎的 AWS 大多數架構完全存在於 上的工作負載環境。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無差別工作。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 也提供服務來改善以 Amazon EC2 為基礎的架構可用性。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 提供本節中詳細說明的多種備份和復原功能。

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 and 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。
- 區塊型設備映射，指定啟動時要連接至執行個體的磁碟區。

Note

在多數情況，適用於 Windows、Red Hat、SUSE 和 SQL Server 的 AMI 需要 AMI 具正確授權資訊。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，會為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，搭配由 AWS 發佈或從中發佈的新更新 AMIs AWS Marketplace。此方法需要仔細測試和規劃，以在新發佈 AMIs 上備份和還原所有自訂資料，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 管理主控台 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，而不是中繼資料。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。磁碟區會複寫到多個伺服器，以防止資料因任何單一元件故障而遺失。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 磁碟區比典型的商用磁碟機更可靠 20 倍，AFR 失敗約 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 關卡協議](#)。

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，以備援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；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](#)。

您可以在您拍攝快照的相同區域中，[從 Amazon EC2 主控台](#) 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。

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，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，將資料從備份磁碟區複製到生產磁碟區。

您也可以使用 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，而無需管理基礎複寫技術。

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，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。

執行個體存放區磁碟區的考量事項

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。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 下載到您的執行個體存放區。您也可以執行個體停止之前，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

標記您的所有 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。標籤不會從 EC2 執行個體自動複製到 AMIs 或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 快照上執行動作時強制使用特定標籤。如果在 IAM 許可政策授予權限中未定義標籤的情況下嘗試 CreateSnapshot 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，則可能會意外刪除快照，或在自動清除程序中刪除快照的風險。您最終可能會支付保留過時的快照費用，因為沒有明確了解它們是否仍然需要。

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 會對連接至執行個體的每個 EBS 磁碟區產生新的快照，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，該磁碟區由已開機的 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，但由於全年無休的 IT 操作成為常態，這種情況很少見。如果您可以將任何資料從系統記憶體排清到應用程式正在使用的磁碟，並將任何檔案寫入磁碟區暫停到足以拍攝快照的時間，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。您執行此操作的方式取決於您的資料庫或檔案系統。

資料庫的程序如下：

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，可以排清其資料以進行一致的備份。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. 重新掛載磁碟區以達到一致且完整的快照。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，其中預期會發生中斷，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，請在拍攝快照之前停止執行個體。Windows 提供磁碟區陰影複製服務 (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 以便部署另一個類似的執行個體，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所有完整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

請先建立適當磁碟區或整個執行個體的快照，再對執行個體進行尚未完整測試的任何主要變更。例如，您可能想要先建立快照，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。然後在動作功能表中，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。

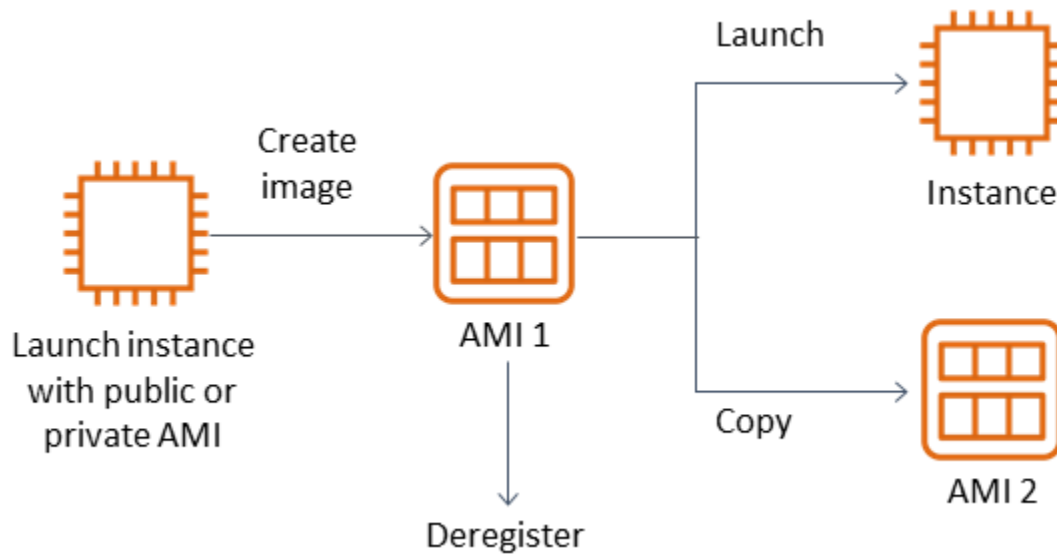
輸入描述並新增適當的標籤。新增 Name 標籤，以便稍後更容易找到磁碟區。根據您的標記策略新增任何其他適當的標籤。

建立 AMIs

AMI 提供啟動執行個體所需的資訊。AMI 包含建立映像時連接至執行個體之 EBS 磁碟區的根磁碟區和快照。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，它會在您正在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 會參考這些 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 的包含功能。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，這會限制對已完成備份之復原點的存取。還原操作可以從 啟動，AWS Backup 而不是繼續進行每個個別資源，並還原建立的備份。AWS Backup 也包含許多額外的功能，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，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。

[Snapshots](#) > Create Snapshot

Create Snapshot

Select resource type ☐ Volume ☒ Instance

Instance ID*  

Description 

Exclude root volume ☐

Volume ID	Volume Type	Encryption
vol-1111111	Root	Encrypted
vol-2222222	EBS	Not Encrypted
vol-3333333	EBS	Not Encrypted
vol-4444444	EBS	Not Encrypted

Copy tags from volume ☒

Key	Value
(127 characters maximum)	(255 characters maximum)

This resource currently has no tags

Choose the Add tag button or [click to add a Name tag](#)

50 remaining (Up to 50 tags maximum)

* Required

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的快照。您不需要停止執行個體，就能在磁碟區之間協調以達到一致性，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，以便在還原、複製或保留期間進行集體管理。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。許多代理程式型備份解決方案可在網際網路和 [AWS Marketplace](#) 中使用。

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，而且不會在主要系統上進行備份。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

請務必考慮備份的安全性，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。為避免因安全性漏洞而遺失重要備份，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 [中的跨帳戶備份 AWS Backup](#) 來完成此操作。

如果 AWS 區域發生區域故障，您的災難復原計劃也可能要求您能夠在另一個中重現 EC2 執行個體。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。這可以提供額外的一層意外刪除保護，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 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。資源回收筒功能有助於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，可讓您將磁碟區複本保留 90 天或更長時間，以供您不想還原的參考之用。在永久刪除 EBS 磁碟區的所有相關快照之前，這可能是很好的中繼步驟。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快照或 AMI 建立前後的操作。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，以減少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使用者是否一致地套用備份程序和標籤。您可以使用 [AWS-CreateSnapshot](#) 和 [AWS-CreatImage](#) Runbook 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，在自動化中建立 EBS 磁碟區的快照。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 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

如果您只需要還原連接至 EC2 執行個體的單一磁碟區，您可以個別還原該磁碟區、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，您的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（例如非生產環境）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取決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，搭配多個為流量提供服務的執行個體，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為流量提供服務，而不會中斷使用者。

以下說明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，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，延遲會比平常高。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](#)。
- 額外付費，Amazon EBS 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，請先停止使用該磁碟區的任何程序。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 彈性區塊存放區磁碟區功能表中，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上選擇，然後選擇動作、連接磁碟區，以連接新的磁碟區。選取您要連接至其中的執行個體，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 功能表上選擇磁碟區，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

若要建立將用於還原整個 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，以便它們可以在相同的組態中還原。

Note

在多數情況，適用於 Windows、Red Hat、SUSE 和 SQL Server 的 AMI 需要 AMI 具正確授權資訊。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 快照還原執行個體，請先從將成為新 EC2 執行個體根磁碟區的 EBS 快照建立 AMI：

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帳單資訊，請檢查新 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 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的執行個體，讓它在您從 AMI 啟動新執行個體時保持離線，並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發生衝突的風險。如果您的執行個體提供的服務關閉，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。然後將現有的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 和電腦名稱執行之加入網域的 Windows 執行個體的問題。對於需要唯一識別符的網路應用程式和服務，您可能會遇到類似問題。

若要防止其他伺服器和服务在新執行個體就緒之前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，以供存取和測試。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 進行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，可整合至新的和現有的備份和復原方法。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，您在現場部署基礎設施中使用的備份和封存軟體 AWS 會透過 API 操作直接與 連接。由於備份軟體已 AWS 察覺，因此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，可與您現有的應用程式搭配使用，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型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，將應用程式資料檔案和備份映像儲存為 Amazon S3 雲端儲存上耐用物件的檔案閘道。
- 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。磁碟區閘道會在內部部署提供本機快取或完整磁碟區，同時將 AWS 磁碟區的完整複本存放在 雲端。
- 磁帶閘道，用於在內部部署儲存閘道指向可信任的備份軟體，進而連接到 Amazon S3。此選項提供雲端的擴展和耐久性，以實現安全、長期的保留，而不會中斷現有的投資或程序。

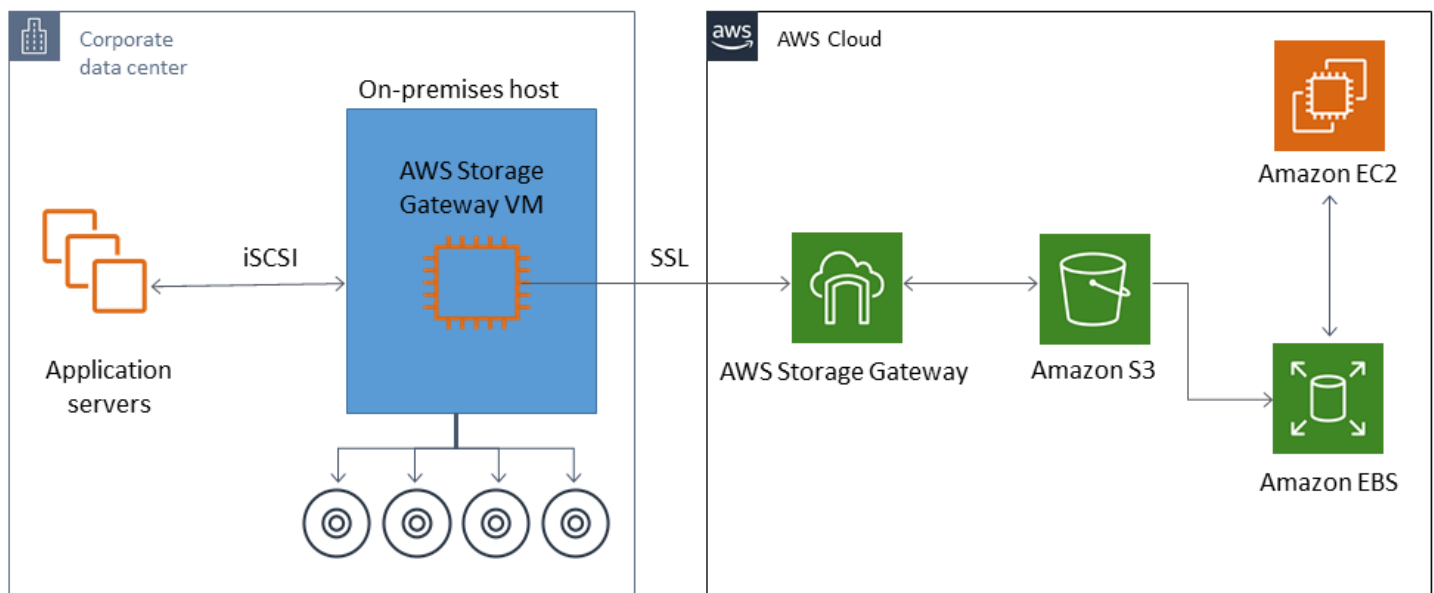
檔案閘道

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至雲端。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 Amazon 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，以進行高耐用性的異地備份。對於最近備份的檔案必須快速還原的情況特別有用。由於檔案閘道支援 SMB 和 NFS 通訊協定，因此使用者可以像存取網路檔案共享一樣存取檔案。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。磁碟區閘道會將磁碟區資料存放至 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，並將其存放於雲端做為 Amazon EBS 快照。儲存為快照之後，整個磁碟區可以還原為 EBS 磁碟區並連接到 EC2 執行個體，以加速雲端型 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。磁碟區閘道為您提供了耐用、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](#)。

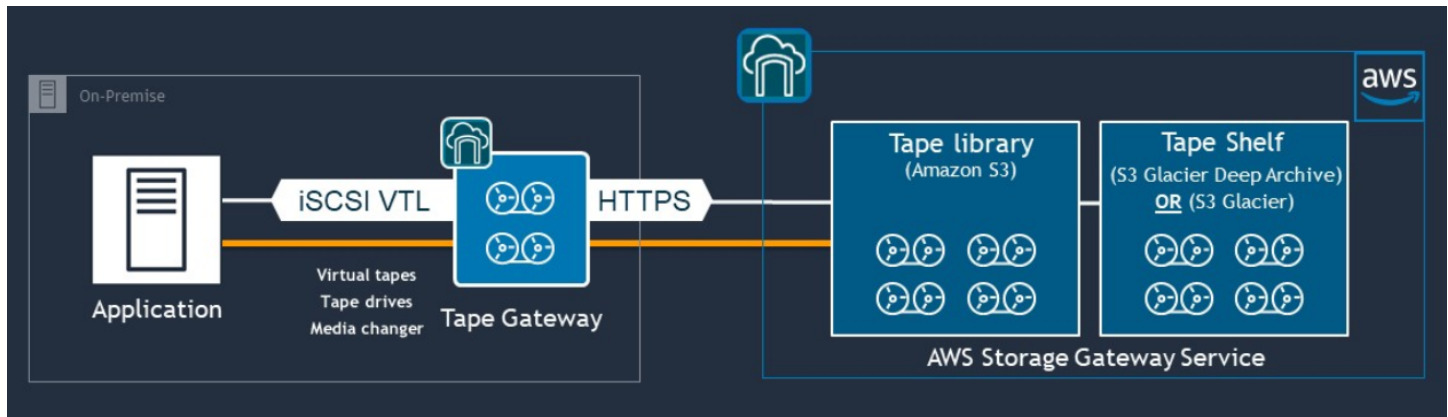
磁帶閘道

磁帶閘道為離站虛擬磁帶備份存放區提供了 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儲存在至少三個分散地理的可用區域中。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 中的所有磁帶都受到使用預設金鑰或 AWS KMS 金鑰的伺服器端加密保護。此外，您可以避免與磁帶

可攜性相關的實體安全風險。與磁帶的異地倉儲相比，使用磁帶閘道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庫 (VTL)，從現場部署環境到高度可擴展、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 提供給現有的備份應用程式，其中包含虛擬媒體變更器和虛擬磁帶機。您可以在寫入大量可擴展性 Amazon S3 上存放的虛擬磁帶集合時，繼續使用現有的備份應用程式和工作流程。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其封存至 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。磁帶閘道可搭配與 iSCSI 型磁帶庫介面相容的備份應用程式使用，以存取虛擬磁帶。另請考慮每個磁帶至少 100-GB 的儲存大小。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 提供用於管理和與資料互動的服務特定功能和選項。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所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 會使用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。或者，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畫，並在特定資料庫的備份計畫是唯一的時，使用使用者起始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。這也可防止您將 RDS 資料庫執行個體上的資料庫直接匯出至其本機磁碟。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 記錄來減少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執行個體，並將中斷和修改降至最低。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持續性和一致性。

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 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，使用 DNS 解析程式快取記錄的時間長度。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，使用指數退避來正常處理重試的資料庫連線失敗。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。對於逐步解除委任方法，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將其刪除。

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 AWS CLI、或 DynamoDB API，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 排程定期或未來的備份 AWS Backup，也可以使用 Lambda 函數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 [排程 Amazon DynamoDB 隨需備份的無伺服器解決方案](#)。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製。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
- 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。只有在還原的資料表變成作用中之後，您才能寫入該資料表。

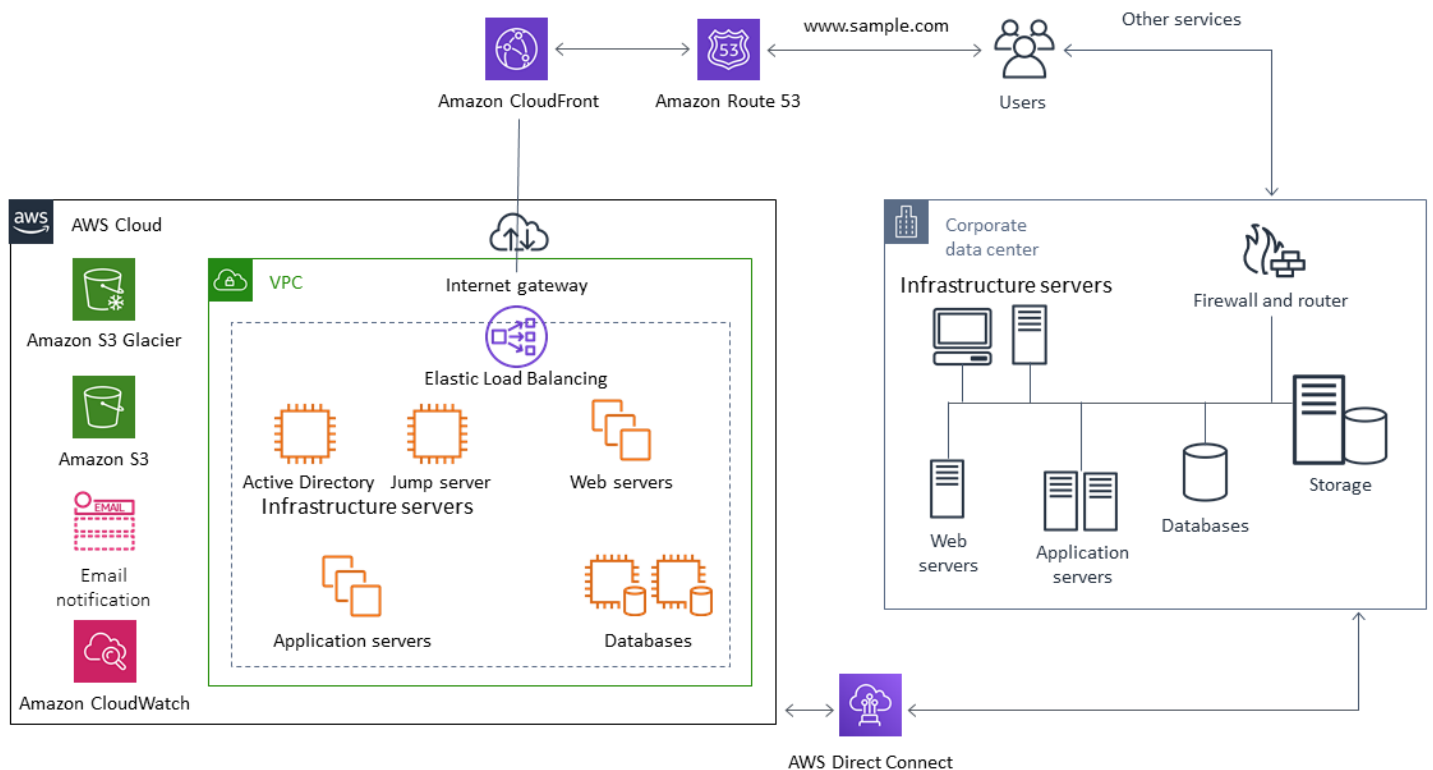
您的還原程序必須考慮如何引導用戶端使用新還原的資料表名稱。您可以設定應用程式和用戶端，從組態檔案、AWS Systems Manager 參數存放區值或其他可動態更新的參考擷取 DynamoDB 資料表名稱，以反映用戶端應使用的資料表名稱。

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，都會託管在客戶資料中心或上 AWS。在 AWS 雲端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，並使用 AWS 來增強容量。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 [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，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。



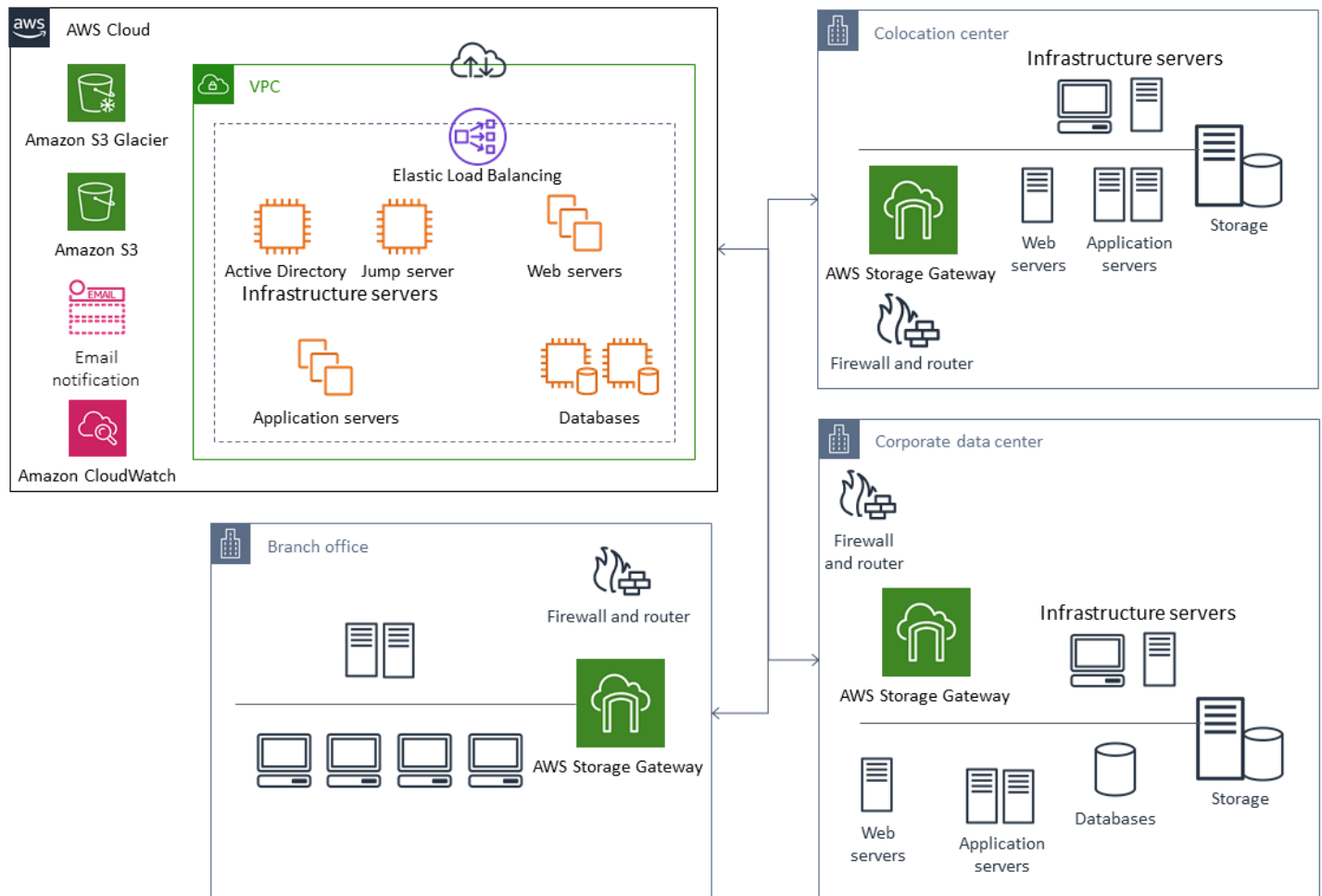
精心設計的資料保護解決方案通常使用本指南中雲端原生和內部部署解決方案中所述的選項組合。許多 ISVs 為內部部署基礎設施提供市場領先的備份和還原解決方案，並已擴展其解決方案以支援混合方法。

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，以及位於多個位置的一或多個媒體或儲存伺服器，這些位置靠近他們保護的伺服器和服务。在這種情況下，請考慮將主要備份伺服器移至 EC2 執行個體，以防止內部部署災難和高可用性。

若要管理備份資料流程，您可以在與要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費用。當您備份到 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 從分散各地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地理分佈位置中的資料，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，並做為 DR 網站。AWS 提供多種支援 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](#)

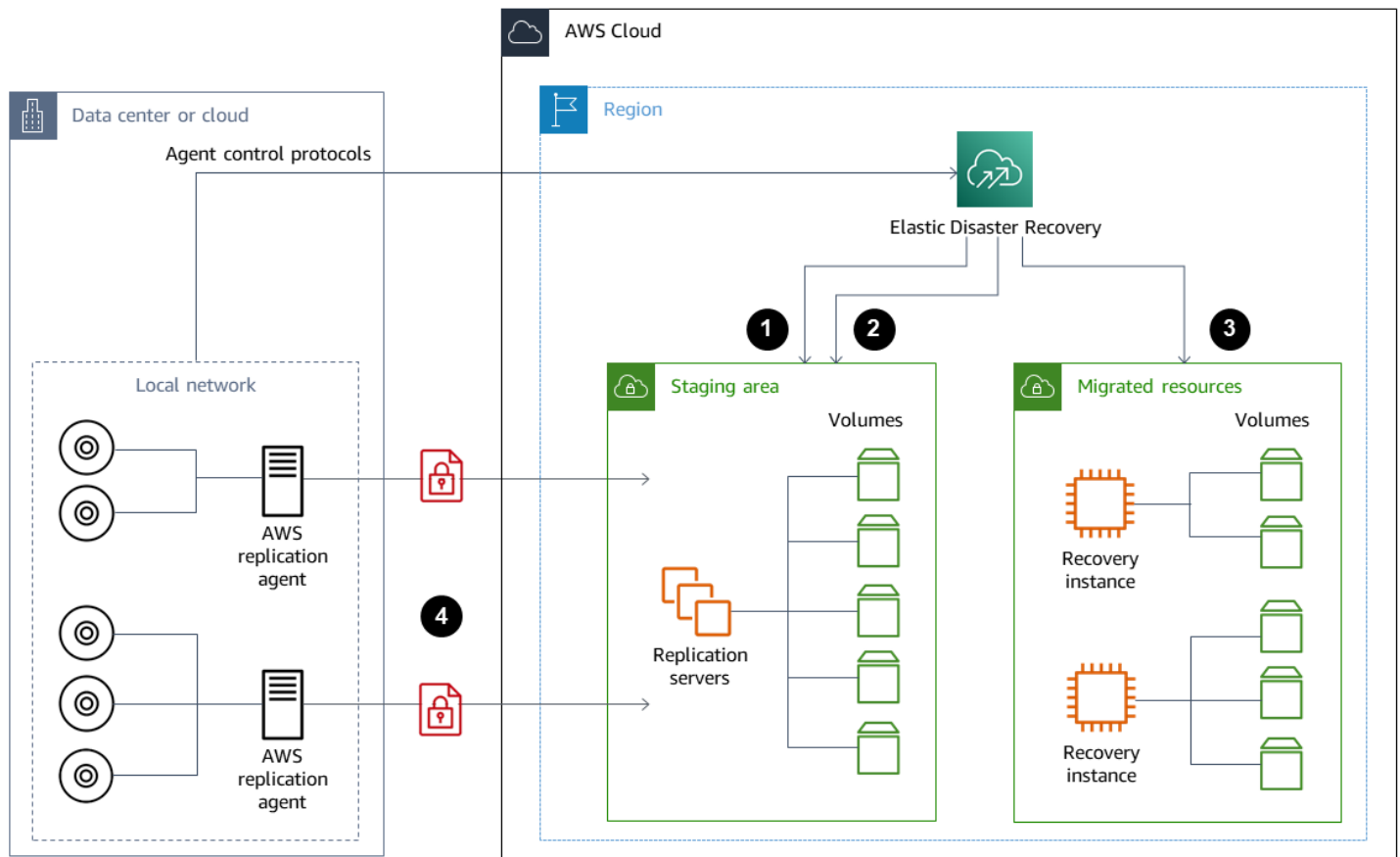
內部部署 DR 至 AWS

使用 AWS 做為現場部署工作負載的異地災難復原 (DR) 環境是常見的混合案例。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 計畫檢查清單](#)。

有多種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，以驗證其完整性。

AWS [AWS 彈性災難復原](#) 可讓您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，並優先使用 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處於完全佈建狀態的機器。

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的低功率 Amazon EC2 同等項目同步 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. 使用 RTO 啟動的復原執行個體為 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，確認您的現場部署、預備和啟動的 DR 環境中有可用的適當授權並正常運作。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之後要執行的步驟。您可以使用[AWS 彈性災難復原 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型磁碟區。也可以使用 Amazon EBS 快照快速佈建這些磁碟區，以便與 Amazon EC2 搭配使用。特別是，儲存的磁碟區閘道可為您的現場部署應用程式提供對整個資料集的低延遲存取。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。此方法要求您徹底測試環境，以確認 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與您的 DR 目標保持一致。在世界各地的區域中 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，只需最少或無需干預。

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，以確定實現目標所需的 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 AWS 服務，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負載平衡的 EC2 執行個體，而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。建立可在執行個體失敗時用來取代執行個體的 AMI。請務必定義適當的自動化和組態，以便自動設定來自 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，並讓用戶端使用此記錄進行連線。建立指令碼來建立新的作用中執行個體 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故障，徹底測試您的解決方案。另請考慮 DR 解決方案隨著工作負載架構變更而需要的更新。

區域故障時 Amazon EC2 的 DR

具有非常高可用性需求（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 AWS 多個區域使用，以針對區域層級的問題提供進一步的彈性。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，以實現全域可用性、容錯移轉和 DR。本指南涵蓋一些 Amazon EC2 備份和復原特有的可用功能。

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 彈性災難復原](#) 可用來將某個區域中的 Amazon EC2 伺服器自動化並持續複寫至替代 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 降至幾分鐘，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，請清除不再需要用於復原或保留目的的備份。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。

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，以及自動化清除程序。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非常重要。

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。您可以根據您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，以及可降低使用者影響時的備份時間。每當您要對工作負載進行重大變更時，請建立point-in-time快照。

我是否需要在開發帳戶中建立備份？

為您的工作負載測試開發帳戶中可能中斷的變更，並在執行中斷變更之前建立備份。您可能在開發和非生產帳戶中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傳輸至 Amazon S3 為止。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，進行中的快照不會受到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 resources

- [AWS 方案指引](#)
- [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 S3](#)
- [Storage Gateway](#)
- [AWS Systems Manager](#)

其他資源

- [使用 備份和復原 AWS Backup](#) (解決方案)
- [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](#)
- [使用的備份和復原方法 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	已將 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 使用 進行災難復原 AWS 並選擇 資料保護 AWS 服務 區段中，新增了有關的資訊 AWS 彈性災難復原。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 ，新增說明。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 有關還原磁碟區 的資訊。	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。新增使用 備份和復原 AWS Backup 一節。在使用 Amazon S3 和 Amazon Glacier 的備份和	2022 年 1 月 28 日

復原區段中，新增了有關新 Amazon 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。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 AWS Backup 支援 AWS 之服務的相關資訊。

2021 年 6 月 1 日

[初次出版](#)

—

2020 年 7 月 29 日

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。