使用 AWS 備份與復原的方法

2016 年 6 月

注意

本文件資訊僅供參考。其內容為文件發佈當日時，AWS 最新的產品內容及實務，如有變更，恕不另行通知。客戶需自行獨立評估本文件資訊，任何 AWS 產品或服務皆以「現狀」提供，不包含任何明示或暗示之保證。本文並不構成 AWS、其附屬公司、供應商或授權人所做出的任何保證、表示、契約承諾、條件或擔保。AWS 對其客戶的責任與義務應由 AWS 協議管轄，本文並非 AWS 與其客戶之間的任何協議的一部分，也並非上述協議的修改。

目錄

摘要

本白皮書適用於負責在公司 IT 環境下保護資料的企業解決方案架構師、備份架構師及 IT 管理人員。其內容將討論可使用 AWS 實作的生產工作負載及架構，以強化或取代備份與復原解決方案。這些方法提供較低的成本、更高的擴展能力與耐用性，以符合復原時間目標 (RTO)、復原點目標 (RPO) 以及合規要求。

簡介

隨著企業資料成長的速度加快，保護資料的工作變得更具有挑戰性。有關備份方法的耐用性與擴展能力的問題已經變成理所當然，包括以下這個問題：雲端如何協助滿足我的備份與封存的需求？

本白皮書將說明多種備份架構 (雲端原生應用程式、混合式及現場部署環境) 與相關的 AWS 服務，可用於建立可擴展且可靠的資料保護解決方案。

為何要使用 AWS 做為資料保護平台？

Amazon Web Services (AWS) 是安全、高效能、彈性、符合成本效益且容易使用的雲端運算平台。AWS 可處理各種繁重的作業，並提供工具與支援以協助使用者建立可擴展的備份與復原解決方案。

使用 AWS 做為資料保護策略的一部分可帶來許多優點：

- **耐用性：**Amazon Simple Storage Service (Amazon S3) 與 Amazon Glacier 可為所存放的物件提供 99.999999999% (11 個 9) 的耐用性。以上兩個平台皆提供可靠的備份資料據點。
- **安全性：**AWS 針對傳輸中或靜態的資料提供多種存取控制與加密的選項。
- **全球基礎設施：**AWS 服務在全球各地皆有提供，您可以將資料備份及存放至符合法規要求的地區。
- **合規：**AWS 基礎設施已通過多項標準認證，例如服務組織控制 (SOC)、鑑證業務準則公告 (SSAE) 第 16 條、國際標準組織 (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 (HIPPA)、SEC[1]，以及聯邦風險與授權管理計劃 (FedRAMP)，讓您可輕易將此備份解決方案納入現有的合規計畫。

- **擴展能力**：使用 AWS，您無需擔心容量的問題。您可以依據需求的變動而增加或減少使用量，不會增加管理的間接成本。
- **更低的總持有成本 (TCO)**：AWS 的營運規模可降低服務成本，並協助降低儲存服務的總持有成本 (TCO)。AWS 以降價的方式，將上述節省的成本提供給客戶。
- **依用量計費的定價**：您可以針對有需要以及計畫使用的期間購買 AWS 服務。AWS 的定價沒有前期費用、終止罰金或長期合約。

AWS 儲存服務提供資料保護

Amazon S3 與 Amazon Glacier 是理想的備份與封存服務，兩者皆為耐用、低成本的儲存平台，兩者皆提供無限容量，而且當備份資料增加時，無須進行磁碟區或媒體的管理。用多少付多少的模式與較低的每月單位 GB 成本，使這兩項服務非常適合資料保護使用案例。

Amazon S3

Amazon S3 提供具有高安全性與擴展能力的物件儲存空間。

您可以使用 Amazon S3 存放與取回任何數量的資料，這些操作隨時可從 Web 上的任何位置執行。Amazon S3 將資料以物件的形式存放於名為*儲存貯體* 的資源中。AWS Storage Gateway 與許多第三方備份解決方案皆可代您管理 Amazon S3 物件。您可以在儲存貯體中存放任意數量的物件，而且可以寫入、讀取及刪除儲存貯體中的物件。單一物件的大小最大可達 5 TB。

[1] https://aws.amazon.com/about-aws/whats-new/2015/09/amazon-glacier-receives-third-party-compliance-assessment-for-sec-rule-17a-4f-from-cohasset-associates-inc/

Amazon S3 針對不同的使用案例提供多種儲存方案。包括：

- **Amazon S3 標準**為一般用途的儲存，適用於經常存取的資料。
- **Amazon S3 標準 — 不常存取**適用於長期存放但不常存取的資料。
- **Amazon Glacier** 適用於長期封存。

Amazon S3 亦提供生命週期政策，可供您設定以管理資料的生命週期。在設定政策之後，您的資料將移轉至適當的儲存方案，您的應用程式無須進行任何變更。如需詳細資訊，請參閱「S3 儲存方案」。

Amazon Glacier

Amazon Glacier 是成本極低的雲端封存儲存服務，提供安全且耐用的儲存空間以供資料封存及線上備份。為保持成本低廉，Amazon Glacier 已針對不常存取以及可接受擷取時間為數小時的資料進行最佳化。使用 Amazon Glacier，您可以安心存放大量或少量的資料，每月每 GB 的成本最低可至 0.007 USD，相較於現場部署解決方案，可大幅節省成本。Amazon Glacier 非常適合長期或不確定保留期間的備份資料儲存，以及長期的資料封存。如需詳細資訊，請參閱「Amazon Glacier」。

AWS Storage Gateway

AWS Storage Gateway 可連接現場部署軟體裝置與雲端型儲存裝置，在您的現場部署 IT 環境與 AWS 儲存基礎設施之間提供無縫及高安全性的整合。如需詳細資訊，請參閱「AWS Storage Gateway」。

AWS 傳輸服務

除了第三方閘道與連接器之外，您可以使用 AWS 選項如 AWS Direct Connect、AWS Snowball、AWS Storage Gateway 及 Amazon S3 Transfer Acceleration 以快速傳輸資料。如需詳細資訊，請參閱「雲端資料遷移」。

設計備份與復原解決方案

當您在訂定完整的策略以備份與復原資料時，首先必須找出可能發生的故障或災難情況及其對事業的潛在影響。在部分產業中，您必須考量法規對於資料安全性、隱私及記錄保留的要求。

您應實作可提供適當精細分級程度的備份程序，以符合事業的 RTO 與 PRO，包括：

- 檔案層級復原
- 磁碟區層級復原
- 應用程式層級復原 (例如資料庫)
- 影像層級復原

以下章節依據您的基礎設施組織，說明備份、復原及封存的方法。IT 基礎設施可大致分類為雲端原生、現場部署及混合式。

雲端原生基礎設施

此方案描述完全存在於 AWS 的工作負載環境。如下圖所示，包括 Web 伺服器、應用程式伺服器、監控伺服器、資料庫及 Active Directory。

如果您從 AWS 執行所有的服務，即可運用許多內建的功能以滿足資料保護與復原的需求。

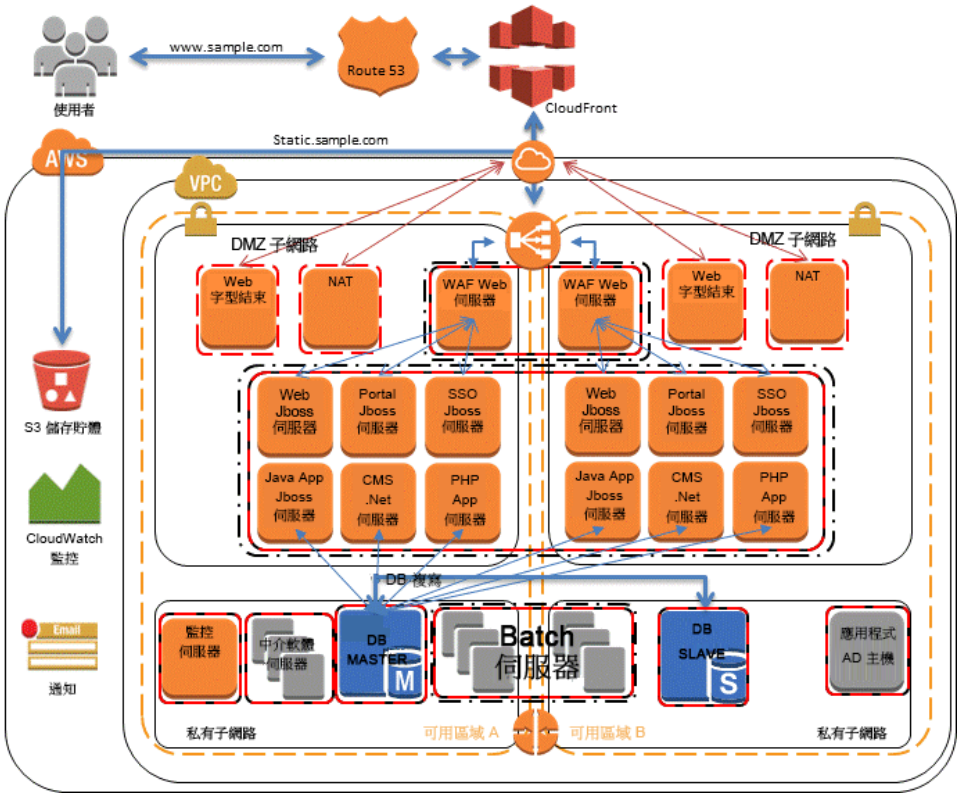

圖 1：AWS 原生案例

EBS 快照式保護

當服務執行於 Amazon Elastic Compute Cloud[2] (Amazon EC2) 時，運算執行個體可使用 Amazon Elastic Block Store (Amazon EBS) 磁碟區來存放及存取主要資料。您可以使用此區塊儲存空間存放結構化資料 (例如資料庫)，或非結構化資料 (例如磁碟區檔案系統中的檔案)。

Amazon EBS 提供為任何 Amazon EBS 磁碟區建立快照 (備份) 的功能。它會建立磁碟區的備份並放置於 Amazon S3，並存放於多個可用區域以提供備援。第一個快照是磁碟區的完整副本，後續的快照則僅存放增量的區塊層級變更。

這個方法可快速且可靠地復原完整磁碟區資料。如果您僅需部分復原，可將磁碟區連接至不同裝置名稱下的執行中執行個體，掛載磁碟區，然後使用作業系統複製命令，將資料從備份磁碟區複製至生產磁碟區。

使用主控台的 Amazon EBS 快照複製功能或命令列，亦可在 AWS 區域之間複製 Amazon EBS 快照，操作方法如「Amazon Elastic Cloud Compute 使用者指南」所述。[3]您可以使用此功能將備份存放於其他區域，無須管理底層的複寫技術。

[2] http://aws.amazon.com/ec2/

[3] http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-copy-snapshot.html

建立 EBS 快照

當您建立快照時，即可直接在耐用的磁碟式儲存裝置中保護您的資料。您可以使用 AWS 管理主控台、命令列介面 (CLI) 或 API 建立 Amazon EBS 快照。

在 Amazon EC2 主控台的 **Elastic Block Store Volumes** 頁面中，選擇 **Actions** 功能表中的 **Create Snapshot**。在 **Create Snapshot** 對話方塊中選擇 **Create**，建立快照存放於 Amazon S3。

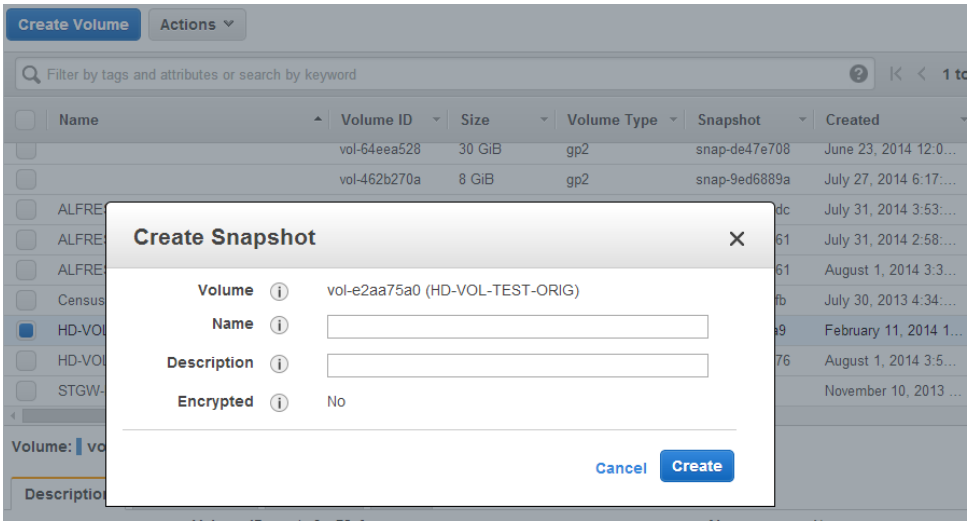

圖 2：使用 EC2 主控台建立快照

若要使用 CLI 命令建立快照，請執行以下命令：

```
➢ aws ec2 create-snapshot
```

您可以排程並定期執行 `aws ec2 create-snapshot` 命令以備份 EBS 資料。Amazon S3 經濟的定價讓您可以保留多個不同時間版本的資料。由於快照是以區塊為基礎，您使用的空間只有在初次建立快照之後發生變更的資料。

從 EBS 快照進行復原

若要從快照復原資料，您可以使用 AWS 管理主控台、CLI 或 API，從現有的快照建立磁碟區。

例如，依照以下步驟，將磁碟區復原至先前的時間點備份：

1. 使用以下命令從備份快照建立磁碟區：

```
➢ aws ec2 create-volume --region us-west-1b --snapshot-
  id mysnapshot-id
```

2. 在 Amazon EC2 執行個體上，卸載現有的磁碟區。

   在 Linux 中，使用 umount。在 Windows 中，請使用邏輯磁碟管理工具 (LVM)。

3. 使用以下命令，從執行個體中斷連接現有的磁碟區：

```
➢ aws ec2 detach-volume --volume-id oldvolume-id –
  instance-id myec2instance-id
```

4. 使用以下命令以連接先前從快照建立的磁碟區：

```
➢ aws ec2 attach-volume --volume-id newvolume-id
  --instance-id myec2instance-id --device /dev/sdf
```

5. 將磁碟區重新掛載於執行中的執行個體。

建立一致備份或線上備份

執行備份時，系統最好能處於未執行 I/O 的狀態。在理想的情況下，機器不接受流量，但隨著全年無休的 IT 運作成為常態，此種情況越來越罕見。

因此，您必須使檔案系統或資料庫靜止，才能建立乾淨的備份。您執行此作業的方式需依據資料庫或檔案系統而定。

資料庫的程序如下：

- 如果可能，請讓資料庫進入線上備份模式。
- 執行 Amazon EBS 快照命令。
- 結束資料庫的線上備份模式，如果使用的是讀取複寫方式，則請終止讀取複寫執行個體。

檔案系統的程序與資料庫類似，但必須依據作業系統或檔案系統的功能而定。例如，XFS 檔案系統可排清資料以建立一致備份。如需詳細資訊，請參閱「xfs_freeze」。[4]

如果您的檔案系統不支援凍結功能，您應卸載檔案系統，發出快照命令，然後重新掛載檔案系統。或者，您可以使用支援 I/O 凍結的邏輯磁碟區管理工具來執行此程序。

由於快照程序會在背景持續進行，而且快照會快速執行並擷取特定時間點，因此您備份的磁碟區僅需卸載幾秒鐘的時間。由於備份時間非常短，因此停機時間可預測且可排程。

[4] https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Storage_Administration_Guide/xfsfreeze.html

執行多磁碟區備份

在部分案例中，您可以使用邏輯磁碟區管理工具，分割跨多個 Amazon EBS 磁碟區的資料以提高潛在的傳輸量。當您使用邏輯磁碟區管理工具 (例如 mdadm 或 LVM) 時，很重要的是，必須從磁碟區管理工具層執行備份，而非從底層的 EBS 磁碟區。如此可確保所有中繼資料一致，以及子元件磁碟區相連貫。

有幾種方法可以達成上述目標。例如，您可以使用 alestic.com[5] 建立的指令碼。記憶體緩衝區應排清至磁碟，存取磁碟的檔案系統 I/O 應予以停止，所有組成 RAID 磁碟組的磁碟區皆應同時開始建立快照。磁碟區的快照開始建立之後 (通常是一秒或兩秒)，檔案系統即可繼續運作。快照應加上標籤，以便在復原時集中管理。

您亦可從邏輯磁碟區管理工具或檔案系統層級執行這些備份。在這類情況下，使用傳統備份代理程式可讓資料經由網路進行備份。在網際網路與 AWS Marketplace 上有多種以代理程式為基礎的備份解決方案。[6]請記住，以代理程式為基礎的備份軟體需要一致的伺服器名稱與 IP 位址。因此，使用上述工具搭配部署於 Amazon 虛擬私有雲端 (VPC)[7] 中的執行個體，是確保可靠性的最佳方式。

有一個替代方法是建立位於單一大型磁碟區中的主要系統磁碟區複寫。如此可簡化備份程序，因為只有一個大型磁碟區需要備份，而且備份不是在主要系統中進行。但是，您必須先確認此單一磁碟區在備份過程中是否能夠展現足夠效能，以及最大的磁碟區大小對於應用程式而言是否適當。

---

[5] https://github.com/alestic/ec2-consistent-snapshot

[6] https://aws.amazon.com/marketplace/

[7] http://aws.amazon.com/vpc/

資料庫備份方法

AWS 有多種資料庫選項。您可以在 EC2 執行個體上執行自己的資料庫，或使用 Amazon Relational Database Service [8](Amazon RDS) 提供的託管服務資料庫選項。如果您在 EC2 執行個體上執行自己的資料庫，您可以使用原生工具 (例如 MySQL[9]、Oracle[10]、MSSQL[11]、PostgreSQL[12]) 將資料備份至檔案，或使用「EBS 快照式保護」中描述的程序，為包含資料的磁碟區建立快照。

使用資料庫複寫備份

如果是建立於 Amazon EBS 磁碟區的 RAID 磁碟組的資料庫，您可以建立資料庫的讀取複寫以消除主要資料庫的備份負擔。它是執行於另一個 Amazon EC2 執行個體的資料庫最新副本。使用類似來源的多個磁碟，即可建立複寫資料庫執行個體，或者可將資料合併至單一 EBS 磁碟區。然後您就可以使用「EBS 快照式保護」中描述的程序，建立 EBS 磁碟區的快照。此方法通常用於需要全天候運行的大型資料庫。在此情況下，需要的備份時間過長，而生產資料庫無法停機如此長的時間。

[8] https://aws.amazon.com/rds/

[9] http://dev.mysql.com/doc/refman/5.7/en/backup-and-recovery.html

[10] http://docs.oracle.com/cd/E11882_01/backup.112/e10642/rcmbckba.htm#BRADV8003

[11] http://msdn.microsoft.com/en-us/library/ms187510.aspx

[12] http://www.postgresql.org/docs/9.3/static/backup.html

使用 Amazon RDS 進行備份

Amazon RDS 包含自動資料庫備份功能。Amazon RDS 可建立資料庫執行個體的儲存裝置磁碟區快照，因此會備份整個 DB 執行個體，而不只是個別的資料庫。

Amazon RDS 提供兩種方法來備份與復原 DB 執行個體：

- **自動備份**可進行 DB 資料庫的時間點復原。依據預設，當您建立新的 DB 執行個體時，將會開啟自動備份。Amazon RDS 會在您建立 DB 執行個體時定義的時段中，為您的資料執行完整的每日備份。您可以針對自動備份設定最長 35 天的保留期間。Amazon RDS 利用上述定期資料備份並搭配您的交易日誌，讓您可以在保留期間內隨時復原您的 DB 執行個體，可復原的最新資料為 `LatestRestorableTime` (通常為最後五分鐘)。若要找出您的 DB 執行個體的最新可復原時間，可使用 `DescribeDBInstances` API 呼叫或到 AWS 管理主控台查看該資料庫的 **Description** 索引標籤。

  當您啟動時間點復原時，交易日誌將套用至最適當的每日備份，將 DB 執行個體復原至您要求的時間。

- **DB 快照**是使用者啟動的備份，可讓您隨時間 DB 執行個體備份至已知的狀態，之後亦可隨時復原至該狀態。您可以使用 AWS 管理主控台或 `CreateDBSnapshot` API 呼叫以建立 DB 執行個體。這些快照的保留期間沒有限制，可保留到您使用主控台或 `DeleteDBSnapshot` API 呼叫予以刪除為止。

當您將資料庫復原至某個時間點，或從 DB 執行個體復原資料庫時，將會建立一個帶有新的終端節點的資料庫執行個體。如此一來，您即可從特定 DB 快照或時間點建立多個資料庫執行個體。

您可以使用 AWS 管理主控台或 `DeleteDBInstance` 呼叫以刪除舊的資料庫執行個體。

使用 AMI 備份 EC2 執行個體

AWS 將系統映像存放於 Amazon Machine Images (AMI)。這些映像包含啟動執行個體時所需的根磁碟區的範本。您可以使用 AWS 管理主控台或 `aws ec2 create-image` CLI 命令，將根磁碟區備份為 AMI。

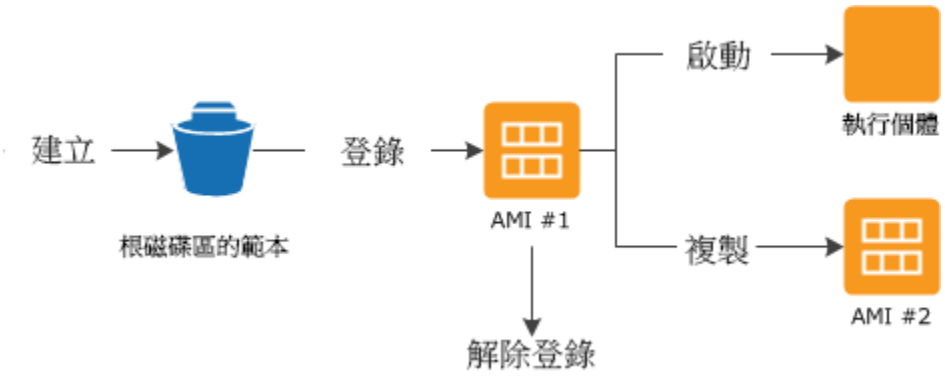

圖 3：使用 AMI 備份與啟動執行個體

當您登錄一個 AMI 時，它會使用 Amazon EBS 快照存放於您的帳戶中。這些存放於 Amazon S3 的快照皆具有高耐用性。

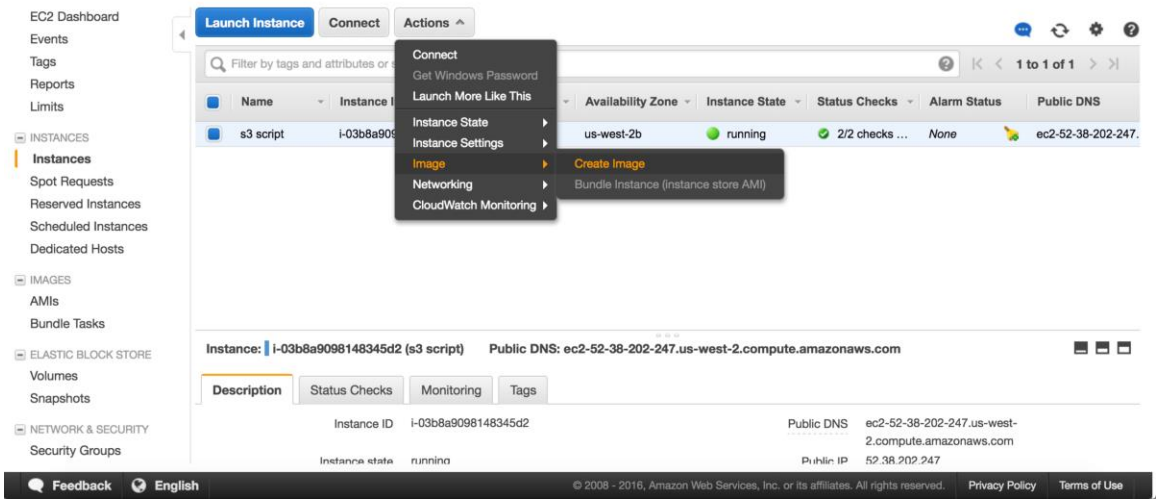

圖 4：使用 EC2 主控台建立機器映像

在您為自己的 Amazon EC2 執行個體建立 AMI 之後，即可使用 AMI 重新建立該執行個體或啟動更多的執行個體副本。您亦可將 AMI 從一個區域複製至另一個區域，以進行應用程式遷移或災難復原。

現場部署 AWS 基礎設施

此方案描述雲端中無元件的工作負載環境。包括 Web 伺服器、應用程式伺服器、監控伺服器、資料庫、Active Directory 等所有資源皆託管於客戶資料中心或透過主機代管方式託管。

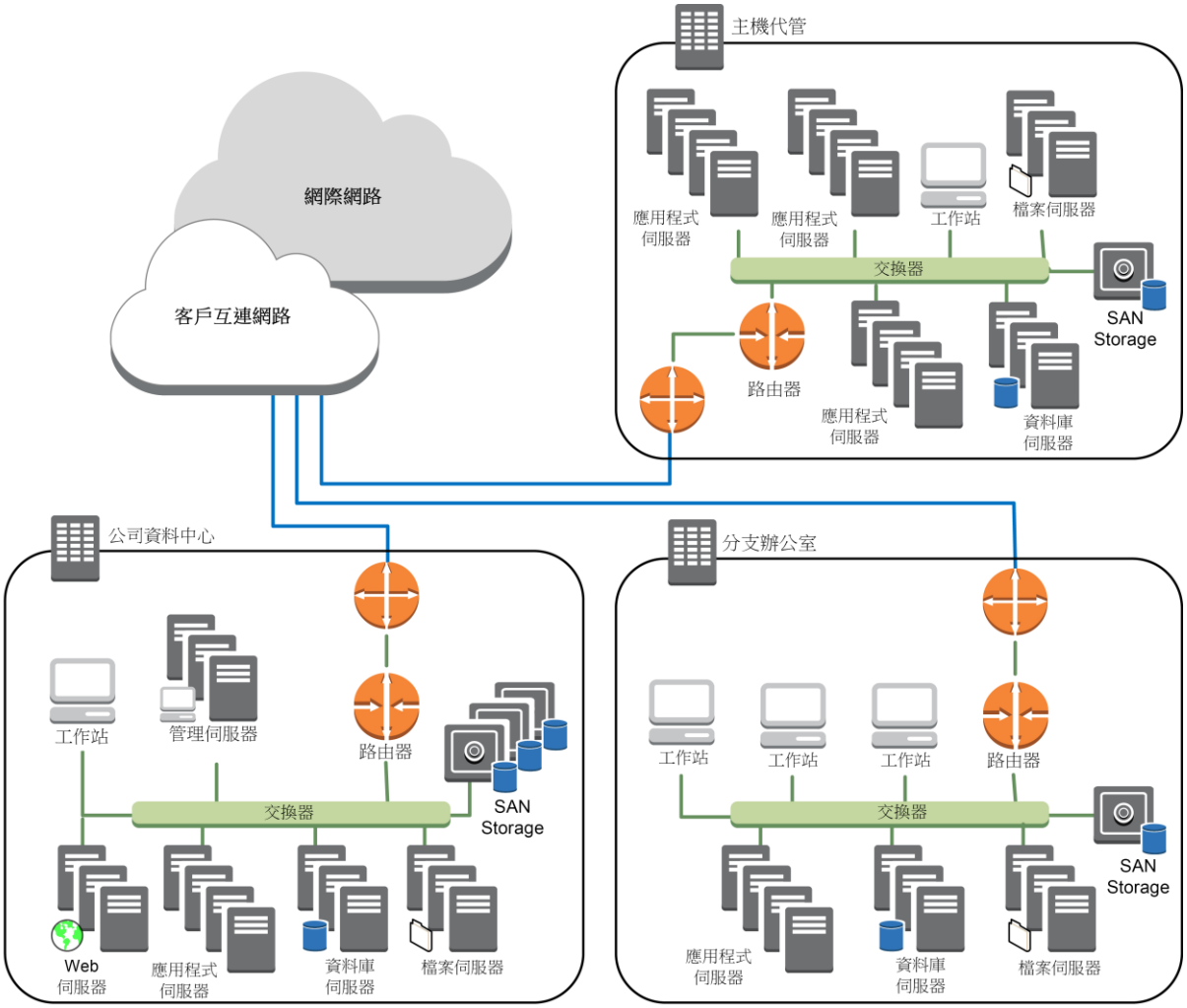

圖 5：現場部署環境

利用此方案中的 AWS 儲存服務，您可以專注於備份與封存工作，無須擔心儲存裝置擴展或基礎設施容量是否能完成備份工作。

Amazon S3 與 Amazon Glacier 以原生 API 為基礎，並可透過網際網路取得。如此可讓備份軟體廠商將應用程式直接整合至 AWS 儲存解決方案，如下圖所示。

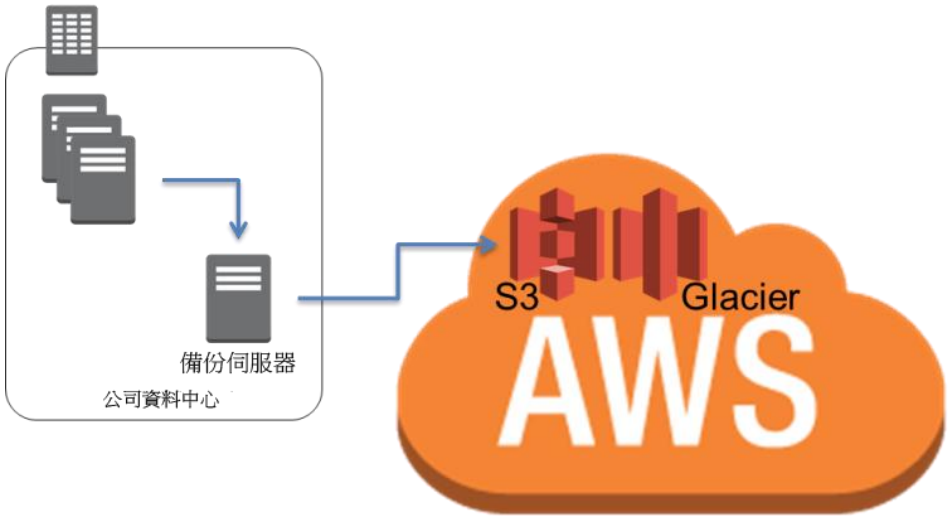

圖 6：與 Amazon S3 或 Amazon Glacier 連接的備份連接器

在此方案中，備份與封存軟體可直接透過 API 連接 AWS。由於這些備份軟體可連結 AWS 功能，因此可將資料從現場部署伺服器直接備份至 Amazon S3 或 Amazon Glacier。

如果您現有的備份軟體並未原生支援 AWS 雲端，那麼您可以使用 AWS Storage Gateway 產品。AWS Storage Gateway[13] 是一種虛擬裝置，可順暢安全地整合您的資料中心與 AWS 儲存基礎設施。此服務可讓您安全地將資料存放至 AWS 雲端，以獲得可擴展且具有成本效益的儲存空間。Storage Gateway 支援業界標準儲存通訊協定，可搭配您現有的應用程式使用，同時將您的所有資料安全地加密存放於 Amazon S3 或 Amazon Glacier。

[13] http://aws.amazon.com/storagegateway/

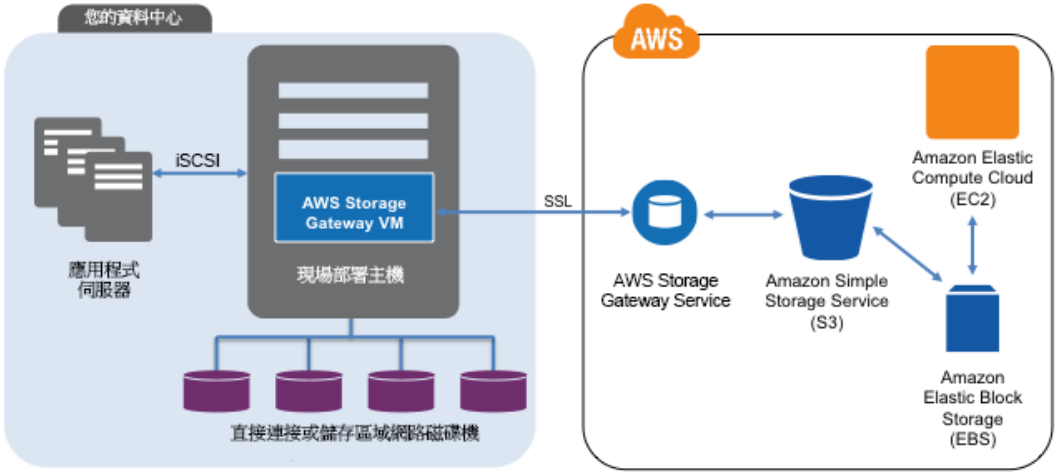

圖 7：將現場部署裝置連接至 AWS 儲存

AWS Storage Gateway 支援以下配置：

- **磁碟區閘道**：磁碟區閘道提供雲端儲存磁碟區，您可以將它從現場部署應用程式伺服器以 Internet Small Computer System Interface (iSCSI) 裝置掛載。閘道支援以下磁碟區配置：
  - **閘道快取磁碟區**：您可以將主要資料存放至 Amazon S3，然後將經常存取的資料保留在本機。閘道快取磁碟區可為主要儲存裝置節省大量成本，減低擴展現場部署儲存裝置的需求，同時維持低延遲存取經常存取的資料。
  - **閘道存放磁碟區**：如果您需要低延遲存取整個資料集，您可以設定現場部署資料閘道將主要資料存放在本機，然後以非同步方式將資料的時間點快照備份至 Amazon S3。閘道存放磁碟區提供耐用且價廉的離站備份，讓您可以從本機或從 Amazon EC2 進行復原。
- **閘道虛擬磁帶庫 (gateway-VTL)**：使用 gateway-VTL，您可以無限制地收藏虛擬磁帶。每個虛擬磁帶皆可存放於 Amazon S3 提供的虛擬磁帶庫，或 Amazon Glacier 提供的虛擬磁帶架。虛擬磁帶庫提供產業標準 iSCSI 介面，可讓您的備份應用程式線上存取虛擬磁帶。當您不再需要立即或經常存取虛擬磁帶中的資料時，即可使用您的備份應用程式，將磁帶從虛擬磁帶庫移至您的虛擬磁帶架，以進一步減少您的儲存成本。

這些閘道具有隨插即用裝置的功能以提供標準 iSCSI 裝置，並可整合至您的備份或封存框架中。您可以使用 iSCSI 裝置做為您的備份軟體或 gateway-VTL 的儲存集區，以減輕磁帶式備份的作業負擔，或直接封存至 Amazon S3 或 Amazon Glacier。

利用此方法，您的備份與封存將會自動離站 (以達到合規目的)，並存放於耐用的媒體，免除離站磁帶管理作業的複雜性與安全風險。

混合式環境

目前已討論雲端原生與現場部署兩種基礎設施部署方式，兩者可結合成為混合式方案，其工作負載環境包含現場部署與 AWS 基礎設施元件。包括 Web 伺服器、應用程式伺服器、監控伺服器、資料庫、Active Directory 等所有資源皆託管於客戶資料中心或透過 AWS 託管。執行於 AWS 雲端的應用程式將連接至執行於現場部署的應用程式。

這將成為企業工作負載的常見方案。許多企業擁有自己的資料中心，同時使用 AWS 擴大容量。這些客戶資料中心通常透過高容量網路連結以連接至 AWS 網路。例如，利用 AWS Direct Connect[14]，您可以在現場部署環境與 AWS 之間建立私有的專屬連線。如此可提供頻寬與一致的延遲以上傳資料至雲端，藉此達到保護資料的目的，並使混合式工作負載獲得一致的效能與延遲。

[14] http://aws.amazon.com/directconnect/

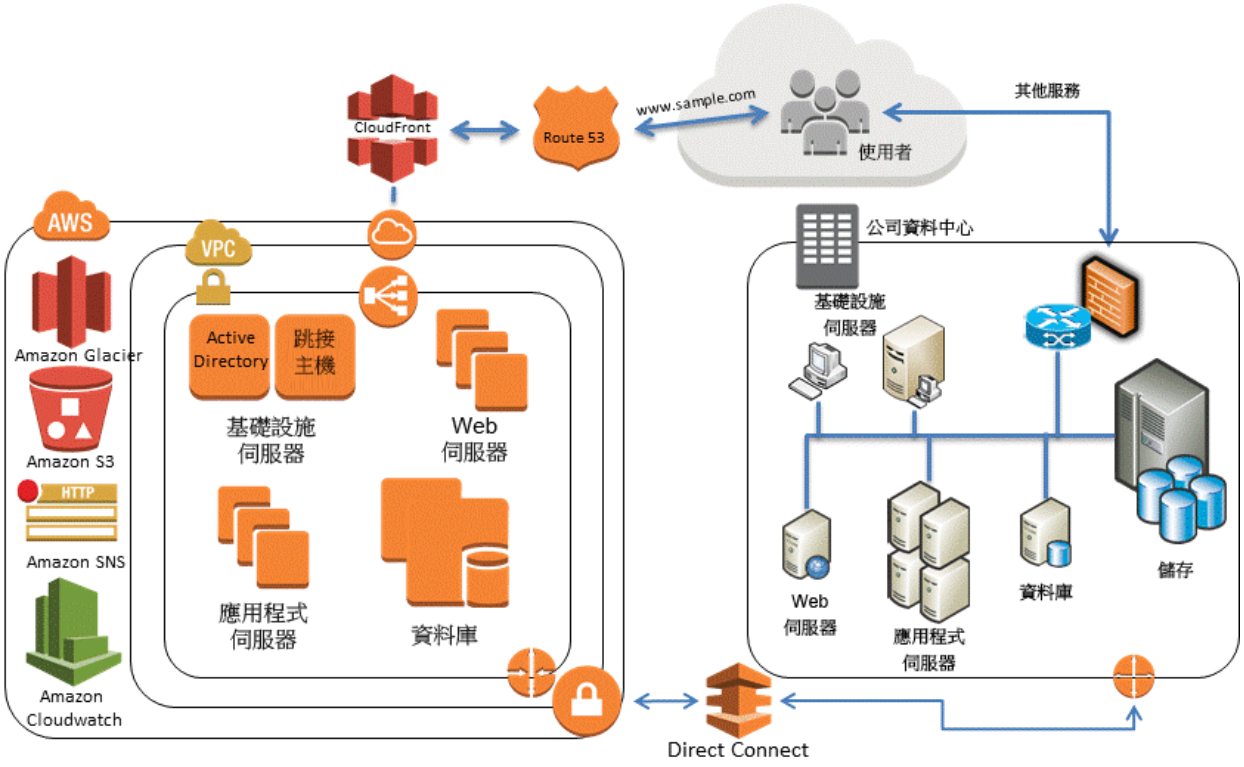

圖 8：混合式基礎設施方案

設計完善的資料保護解決方案通常結合使用雲端原生與現場部署解決方案中描述的方法。

將以 AWS 為基礎的應用程式備份至您的資料中心

如果您的現場部署伺服器已有備份資料的框架，那麼您可以輕鬆地透過 VPN 連接或 AWS Direct Connect，將它延伸至您的 AWS 資源。您可以在 Amazon EC2 執行個體上安裝備份代理程式，然後依據您的資料保護政策備份資料。

將備份管理遷移至雲端以提升可用性

依據您的備份架構而定，您或許在現場部署環境中擁有主要備份伺服器以及一或多個媒體或儲存伺服器，以及受到保護的各種服務。在此情況下，您或許會想要將主要備份伺服器遷移至 Amazon EC2 執行個體，為其提供保護以避免收到現場部署環境災難的影響，並獲得具有高可用性的備份基礎設施。

為了管理備份資料流程，您或許也會想要在 Amazon EC2 執行個體上建立一或多個媒體伺服器。接近 Amazon EC2 執行個體的媒體伺服器將可節省網際網路資料傳輸費用，而且在備份至 S3 或 Amazon Glacier 時，可提高整體備份與復原效能。

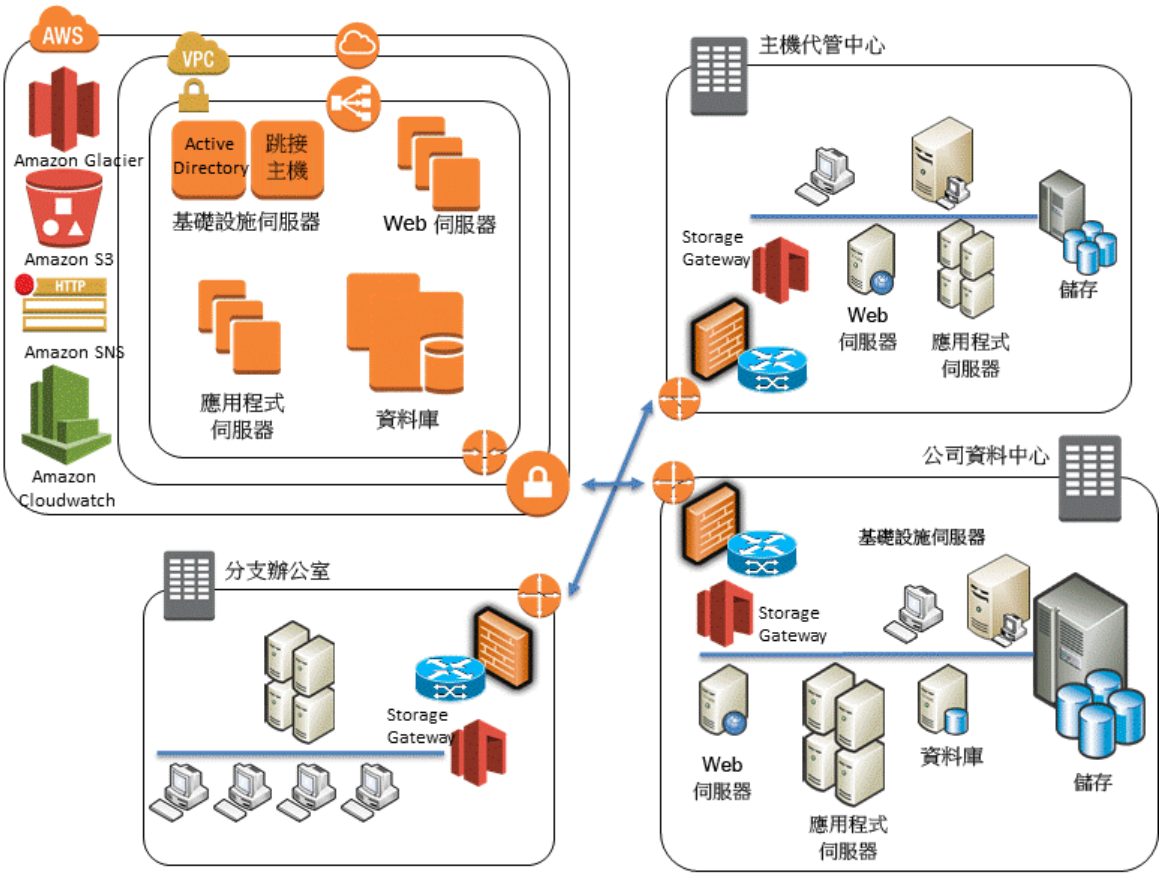

圖 9：在混合式方案中使用閘道

範例混合式方案

假設您負責管理的環境中，需要備份 Amazon EC2 執行個體、獨立伺服器、虛擬機器及資料庫。此環境有 1,000 個伺服器，而且您需要備份作業系統、檔案資料、虛擬機器映像以及資料庫。需要備份的資料庫有 20 個 (包括 MySQL、Microsoft SQL Server 及 Oracle)。

您的備份軟體包含代理程式，可備份作業系統、虛擬機器映像、資料磁碟區、SQL Server 資料庫以及 Oracle 資料庫 (使用 RMAN)。如果您的備份軟體沒有適用於 MySQL 等應用程式的代理程式，您可以使用 mysqldump 用戶端應用程式在磁碟上建立資料庫傾印檔案，即可由標準備份代理程式保護資料。

為了保護此環境，您的第三方備份軟體通常會有通用類別目錄伺服器或主要伺服器，以控制備份、封存及復原作業，另外也可能會有多個媒體伺服器，以連接磁碟式儲存裝置、Linear Tape-Open (LTO) 磁碟機，以及 AWS 儲存服務。

若要利用 AWS 儲存服務來強化您的備份解決方案，最簡單的方式是利用您的備份廠商對 Amazon S3 或 Amazon Glacier 的支援。我們建議您向廠商洽詢有關整合與連接器的選項。如需與 AWS 合作的備份軟體廠商清單，請參閱我們的「合作夥伴目錄[15]」。

如果您現有的備份軟體並未原生支援雲端儲存以進行備份或封存，那麼您可以在備份軟體與 Amazon S3 或 Amazon Glacier 之間使用儲存閘道裝置，例如橋接器。

目前有許多第三方閘道解決方案。您亦可使用 AWS Storage Gateway 虛擬裝置來連接兩端，因為它使用通用技術，例如以 iSCSI 為基礎的磁碟區與虛擬磁帶庫 (VTL)。此組態需要支援的 Hypervisor (VMware 或 Microsoft Hyper-V) 與本機儲存裝置以代管裝置。

使用 AWS 封存資料

當您需要為了合規與公司的目的而保存資料時，您可以予以封存。不同於通常是為了短期保留生產資料副本，以便在資料損毀或資料遺失時進行復原而執行的備份，封存則是存放所有資料副本，直到保留政策到期為止。

---

[15] http://www.aws-partner-directory.com/PartnerDirectory/PartnerSearch?type=ISV

良好的封存需符合以下條件：

- 具備資料耐用性以提供長期完整性
- 資料安全性
- 容易復原
- 低成本

不可變動的資料存放區可能是另一項法規或合規要求。

Amazon Glacier 以低成本、靜態資料原生加密、11 個 9 的耐用性以及無限容量提供封存。

Amazon S3 標準 — 不常存取對於需要快速取回資料的使用案例而言是理想的選擇。對於資料不常存取並可接受數小時取回時間的使用案例而言，Amazon Glacier 是不錯的選擇。

透過 S3 的生命週期規則或 Amazon Glacier API，物件可分層存放至 Amazon Glacier。Amazon Glacier Vault Lock 功能可讓您透過保存庫鎖定政策，針對個別 Amazon Glacier 保存庫輕鬆部署並強制執行合規控制。您可以在保存庫政策中指定控制功能，例如「寫入一次、讀取多次」(WORM)，並鎖定該政策以禁止編輯。如需詳細資訊，請參閱「Amazon Glacier」。

保護 AWS 的備份資料

資料安全性是共同的關注焦點。AWS 非常重視安全性，它是我們推出的每一項服務的基礎。儲存服務如 Amazon S3 提供強大的功能，可針對靜態與傳輸中的資料進行存取控制與加密。所有 Amazon S3 與 Amazon Glacier API 終端節點皆支援傳送中資料的 SSL 加密。Amazon Glacier 預設會對所有靜態資料進行加密。使用 Amazon S3，客戶可選擇讓 AWS 管理加密金鑰，以便為靜態物件進行伺服器端加密，當客戶上傳物件時則提供自己的金鑰，或者使用 AWS Key Management Service (AWS KMS) [16]以整合加密金鑰。或者，客戶可在將資料上傳至 AWS 之前進行加密。如需詳細資訊，請參閱「Amazon Web Services：安全程序概觀」。

[16] http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingKMSEncryption.html

結論

Gartner 已認定 AWS 為公有雲端儲存服務的領導業者[17]。AWS 目前處於有利的地位，可協助企業組織將工作負載轉移至新一代雲端備份平台。AWS 提供具有成本效益且可擴展的解決方案，協助企業組織在備份與封存需求之間達到平衡。相關服務皆以您目前使用的技術進行完善的整合。

作者群

協力完成這份白皮書的個人如下：

- Pawan Agnihotri，Amazon Web Services 解決方案架構師
- Lee Kear，Amazon Web Services 解決方案架構師
- Peter Levett，Amazon Web Services 解決方案架構師

文件校訂

2016 年 6 月更新

[17] http://www.gartner.com/technology/reprints.do?id=1-1WWKTQ3&ct=140709&st=sb