歡迎學習模組 14：災難規劃。

模組概覽

aws academy

小節目錄

1. 架構需求
2. 災難規劃策略
3. 災難復原模式

實驗

- 指導實驗：使用 AWS Storage Gateway 檔閘道進行混合存儲和資料移轉

知識測驗

本模組包含以下章節：

1. 架構需求
2. 災難規劃策略
3. 災難復原模式

該模組還包括一個指導實驗，您將在實驗中啟用 Amazon S3 跨區域複製。您將設定檔閘道並將檔共用掛載到 Amazon Elastic Compute Cloud (Amazon EC2) 實例上。

最後，您需要完成一份知識測驗，以測試您對本模組中涵蓋的關鍵概念的理解程度。

模組目標

學完本模組後，您應該能夠：

- 確定災難規劃策略
- 定義復原點目標 (RPO) 和恢復時間目標 (RTO)
- 描述備份和災難恢復的四種常見模式以及實施方法
- 使用 AWS Storage Gateway 實現本地到雲備份解決方案

學完本模組後，您應該能夠：

- 確定災難規劃策略
- 定義復原點目標 (RPO) 和恢復時間目標 (RTO)
- 描述備份和災難恢復的四種常見模式以及實施方法
- 使用 AWS Storage Gateway 實現本地到雲備份解決方案

模組 14：災難規劃

第 1 節：架構需求

介紹第 1 節：架構需求。

咖啡館業務要求

如果咖啡館的基礎設施不可用，員工必須能夠在企業可以接受的時間內讓應用程式重新運行。他們需要一種支援災難恢復計畫的架構，同時也能優化成本。

到目前為止，咖啡館已經實施了幾個可在 AWS 上運行的應用程式。他們還在 AWS 雲中存儲大量業務關鍵型資料。Sofía 意識到如果咖啡館的基礎設施不可用，則他們必須能夠在企業可以接受的時間內讓應用程式重新運行和可訪問。目前，該咖啡館的員工尚未制定任何全面的災難恢復計畫。

Sofía 向 Frank 和 Martha 提出了這種擔憂。他們都同意，將備份和災難恢復計畫落實到位非常重要。他們的目標是實施一種支援災難恢復時間目標的架構，同時還能優化成本。他們還同意，隨著收入的增長，他們將能夠負擔得起支援較短恢復時間目標的解決方案。

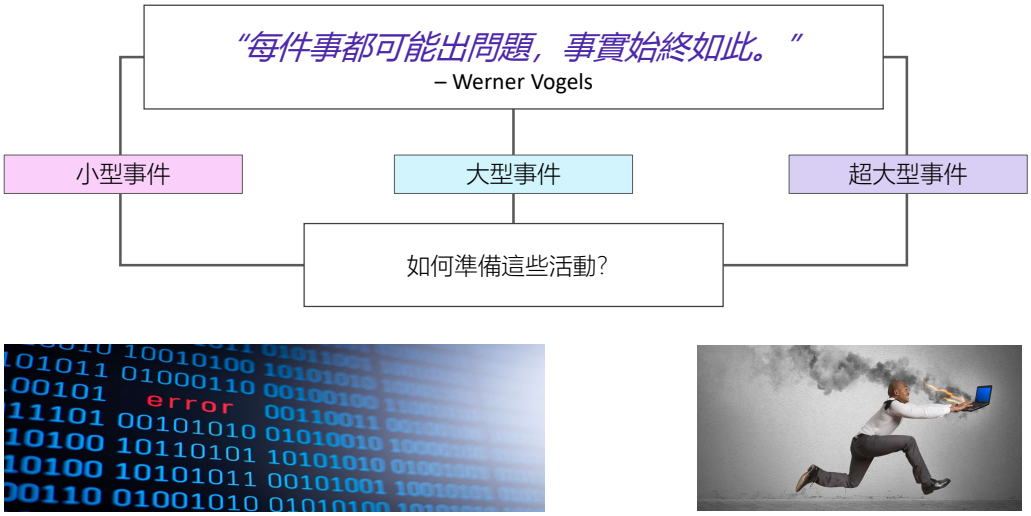
在本模組中，您將瞭解支持資料備份和災難恢復的主要 AWS 服務功能。瞭解這些功能後，您應該能夠幫助咖啡廳滿足這一基本業務要求。

模組 14：災難規劃

第 2 節：災難規劃策略

介紹第 2 節：災難規劃策略。

針對故障的規劃



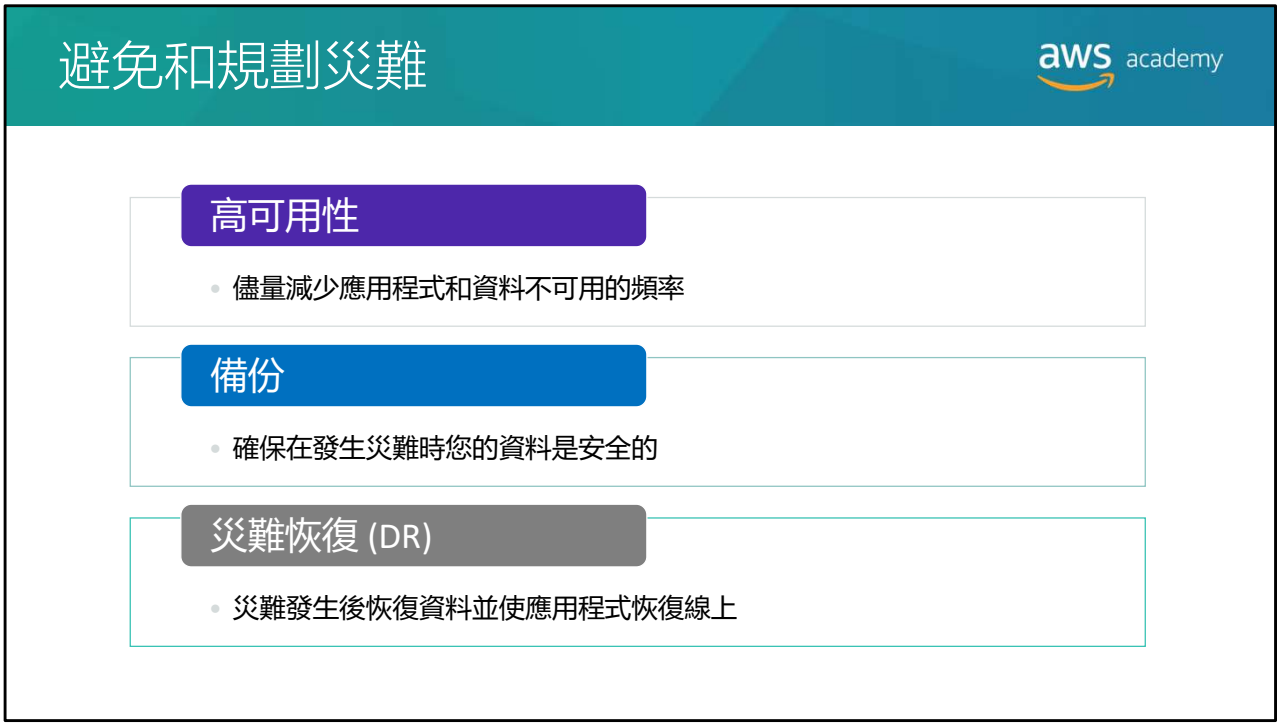
AWS 的首席技術官 (CTO) Werner Vogels 在不止一次場合中曾著重指出： "一直以來，所有事情都在失敗。" 他的這句發聲多年來一直影響著雲計算架構設計，因為這是一個真實的說法。

不應將失敗視為不太可能出現的異常情況。相反，應該假設失敗，無論大小，都可能會發生，也將會發生。如何準備這些活動?

故障可以歸類為以下三種類型之一：

- 小*規模事件* – 例如，單台伺服器停止回應或離線
- 大*規模事件* – 在這種情況下，多種資源將受到影響，甚至可能是一個區域內的多個可用區
- 超大*規模事件* – 在這種情況下，故障很普遍，會影響到大量使用者和系統

為了最大限度地減少災難造成的影響，企業必須投入大量的時間和資源為災難做前期的規劃和準備，並培訓員工、記錄和更新流程。特定系統的災難計畫的投資額可能會因潛在服務中斷的成本而有很大差異。



您可以通過三種方式努力避免災難並進行規劃：

- *高可用性*提供了冗余和容錯能力。當系統能夠承受單個或多個元件（例如，硬碟、伺服器或網路連結等）的故障時，這個系統即為高度可用的。生產系統通常已定義了正常執行時間要求

- *備份*對保護資料和確保業務連續性來說至關重要。但是，要實施也是一個挑戰。資料的生成速度呈指數級增長，同時，本地磁片的密度和持久性沒有同樣的增長率。即便如此，在發生災難時，保持關鍵資料已備份至關重要。

- *災難恢復 (DR)* 是指為災難做好預防準備以及從災難中恢復。災難*是所有會對公司的業務連續性或財務帶來負面影響的事件*。此類事件包括硬體或軟體故障、網路中斷、停電、建築物的物理性損壞（如火災或洪水）。原因可能是人為錯誤或其他重大事件。災難恢復是一套策略和程式，可在發生任何災難後恢復或延續至關重要的技術基礎設施和系統。

相關的 AWS 架構完善框架的設計原則

aws academy

卓越運營支柱

- 預見故障
- 經常優化運行程式

可靠性支柱

- 測試恢復流程
- 自動從故障中恢復

考慮一些與災難恢復主題相關的設計原則。

AWS 架構完善的框架的*卓越運營*支柱指出了*預測失敗*的重要性。它建議您執行預先練習，以識別潛在的故障源，從而消除或緩解故障。您必須測試您的故障情況，並驗證您對故障影響的理解。AWS 架構完善的框架還描述了經常改進操作程式的好處，以便您可以尋找改進它們的機會。然後，隨著工作負載的增加，您可以相應地改進您的程式。

可靠性*支柱描述了*設計系統的重要性。您必須能夠從基礎設施或服務中斷中恢復，以及減少中斷（例如配置錯誤或短暫的網路問題）。

它提到的設計原則之一是*測試恢復程式*。測試系統的故障情況，驗證您的恢復過程。您可以使用自動化功能來類比不同的故障或重新創建先前導致故障的場景。此測試可以在實際故障場景出現之前暴露故障路徑，以便您進行測試和修復。它降低了在元件出現故障之前未經過測試的風險。

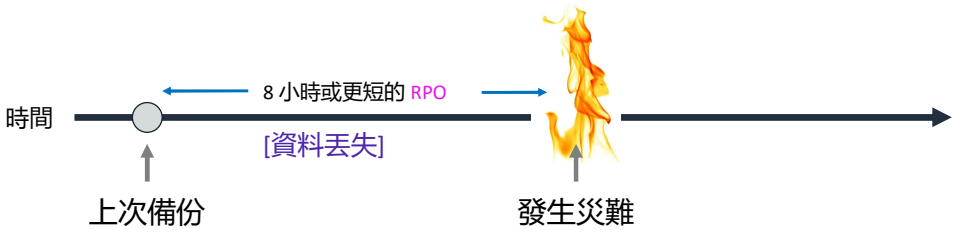
另一個設計原則是*自動從故障中恢復*。通過監控系統的關鍵性能指標 (KPI)，您可以在超出閾值時觸發自動化。這些 KPI 應衡量商業價值，而不是服務運營方式的技術方面。您的自動化可以提供通知和跟蹤故障，並自動執行可解決故障或修復故障的恢復過程。

復原點目標 (RPO)

復原點目標 (RPO) 是按時間衡量的可接受的最大資料丟失量。

您的資料必須多久備份一次?

示例 RPO: *企業（最多）可以從丟失過去 8 個小時的資料中恢復。*



各種規模的組織，無論大小，通常都有業務連續性計畫 (BCP)。BCP 的一個典型部分是提供 IT 服務連續性，包括 IT 災難恢復計畫。

災難恢復計畫最重要的措施之一是定義*恢複點目標 (RPO)*。要計算 RPO，首先根據您的 BCP 確定可接受的資料丟失量。然後，作為時間衡量標準，找出資料丟失可能發生的速度。

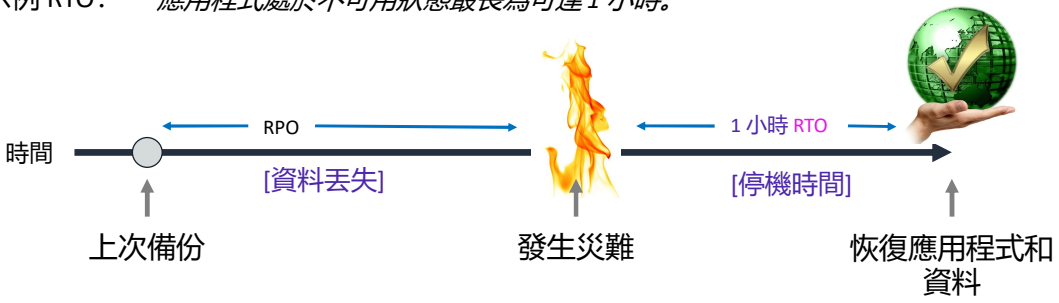
例如，假設您確定應用程式生成的資料很重要但不關鍵，因此丟失 800 條記錄是可以接受的。您進一步計算出，即使在高峰時段，一小時內創建的記錄也不超過 100 條。在這種情況下，您決定 8 小時的 RPO 足以滿足您的需求。如果隨後實施了符合此 RPO 的災難恢復計畫，則必須至少每 8 小時進行一次資料備份。然後，如果在 22:00 發生災難，系統應該能夠在下午 14:00 之前恢復系統中的所有資料。

恢復時間目標 (RTO)

恢復時間目標 (RTO) 是在發生災難後，業務流程可以保持失效的最大可接受時間。

應用程式和資料必須以多快的速度恢復？

示例 RTO：　*應用程式處於不可用狀態最長為可達 1 小時。*

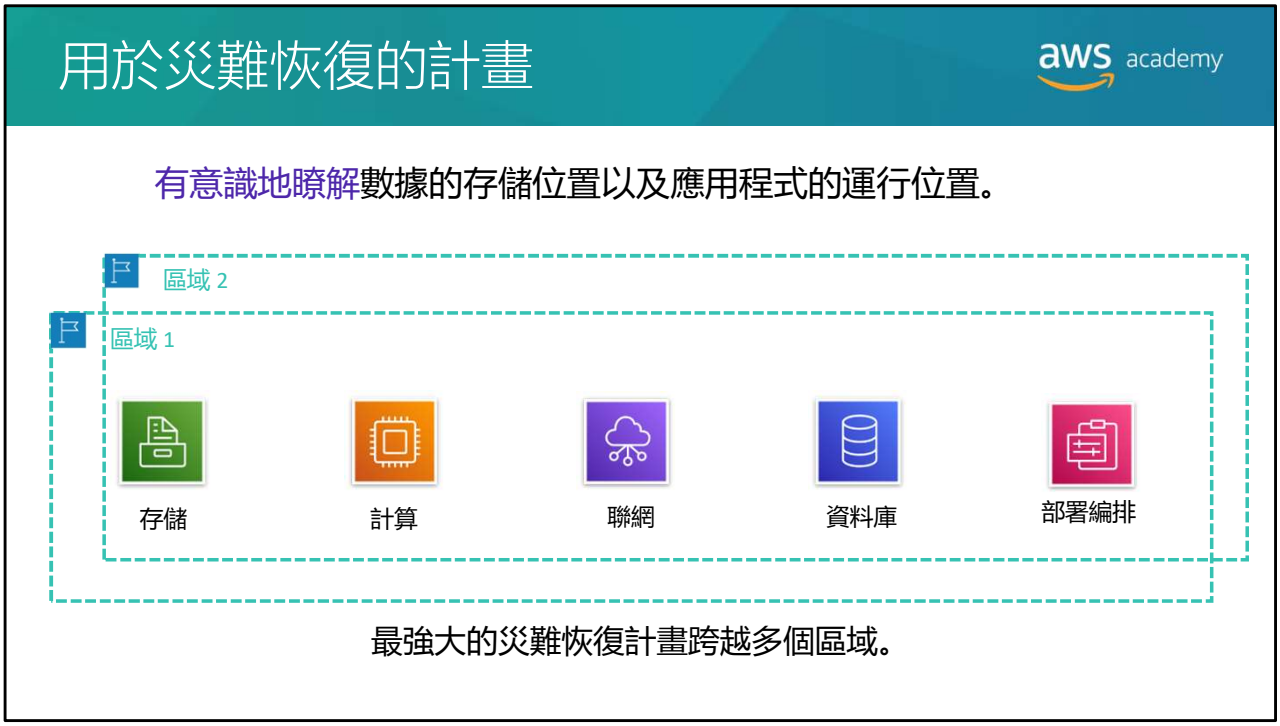


災難恢復計畫的另一個重要措施是定義*恢複時間目標* (RTO)。RTO 是中斷*後*恢複應用程式和恢復資料所需的時間。要繼續上一個示例，假設災難發生在 22:00，RTO 為 1 小時。在這種情況下，災難恢復過程應在 23:00 之前將業務流程恢復到可接受的服務級別。

當系統不可用時，公司通常會根據對業務造成的財務影響的決策來決定可接受的 RPO 和 RTO。該公司通過考慮許多因素來確定財務影響。這些因素包括因停機和缺乏系統可用性導致的業務損失和聲譽損害。

然後，IT 組織計畫解決方案，以提供經濟高效的系統恢復。這些解決方案基於時間表內的 RPO 和 RTO 確定的服務級別。

用於災難恢復的計畫



要正確確定災難恢復計畫的範圍，您必須全面審視 AWS 的使用情況。大多數組織使用的服務組合可以廣泛歸類為包含以下五大服務分類領域：

- 存儲
- 計算
- 聯網
- 數據庫
- 部署編排服務

如果發生災難，您的 RPO 和 RTO 將在這些服務領域指導您的備份和恢復計畫和程式。它們還可能會影響您的生產部署架構。

同樣重要的是要記住，儘管整個區域都不可用是不太可能的，但它是在可能性範圍內。如果某些大規模事件影響某個區域（例如，隕石撞擊），您的資料是否仍可用？您的應用程式仍然可以訪問嗎？AWS 在世界各地提供了多個區域。因此，除了完全部署系統的網站外，您還可以為災難恢復網站選擇最合適的位置。

圖中引用了以下服務：

- Amazon Elastic Block Store (Amazon EBS)
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Elastic File System (Amazon EFS)
- Amazon Simple Storage Service (Amazon S3)
- Amazon Simple Storage Service Glacier (Amazon S3 Glacier)

要開始制定詳細的災難計畫，請查看資料存儲層（暫時推遲對資料庫層的討論）。

您的 AWS 雲存儲可以由資料塊存儲、檔案系統存儲和物件存儲的組合組成。同時，您的組織也可能使用將本地資料中心連接到 AWS 雲的 AWS 服務。

在接下來的幾張幻燈片中，您將瞭解這三個領域中每個領域的高級別最佳實踐。

您可能不熟悉的一項服務是 *AWS DataSync*。使用 AWS DataSync，可以在本機存放區與 Amazon S3、Amazon EFS 或 Amazon FSx for Windows File Server 之間移動大量線上資料。它支援從本地網路檔案系統 (NFS) 和伺服器訊息區 (SMB) 存儲傳輸腳本複製作業和計畫資料傳輸。它還可以選擇性地使用 AWS Direct Connect 連結。

最佳實踐：Amazon S3 跨區域複製

- 大多數 S3 存儲類在單個區域內的可用區中複製資料
- 配置 S3 跨區域複製以實現更高級別的資料安全
  - 自動非同步複製您添加複製配置後創建的物件
  - 還可以說明滿足合規性要求並減少訪問物件的使用者的延遲

對於許多組織來說，他們存儲在 AWS 上的大部分數據都在提供物件存儲的 Amazon S3 中。

回想一下，S3 存儲桶存在於特定的 AWS 區域中。您在創建存儲桶時選擇區域。Amazon S3 為 S3 標準、S3 標準 – IA、S3 單區 – IA 和 Amazon S3 Glacier 存儲類提供了 11 個 9 (99.999999999%) 的持久性。Amazon S3 標準、S3 標準 – IA 和 Amazon S3 Glacier 的設計還可在整個 Amazon S3 可用區丟失的情況下保留資料。它們通過在*單個* AWS 區域中自動將物件存儲在至少三個相隔數英里的可用區中，從而提供這種穩定性。

對於希望獲得更高級別資料安全性的關鍵應用程式和資料場景，最佳做法是配置 S3 跨區域複製。要啟用複製，請將複製配置添加到*源存儲桶*。最低配置必須指明您希望 Amazon S3 複製所有物件或所有物件的子集的目標存儲桶。它還必須包含 AWS Identity and Access Management (IAM) 角色，該角色授予 Amazon S3 將物件複製到目標存儲桶的許可權。

複製的物件保留其中繼資料。目標存儲桶*可以屬於另一個存儲類*。例如，S3 標準存儲桶的內容可能會複製到 Amazon S3 Glacier 存儲桶。您可以為目標存儲桶中的物件分配不同的所有權。您還可以使用 S3 複製時間控制 (S3 RTC) 在可預測的時間範圍內跨不同區域複製您的資料。S3 RTC 可以在 15 分鐘內複製存儲在 Amazon S3 中的 4 個 9 (99.99%) 的新對象。

最佳實踐：EBS 卷快照

- 創建 EBS 卷的時間點快照
  - 快照提供增量備份（它們備份自上一個快照以來更改的資料塊）
- 快照使您能夠將資料還原到新的 EBS 卷
- 使用 Amazon Data Lifecycle Manager 自動創建、保留和刪除快照
- 您無法快照實例存儲

關於資料塊存儲，您可以通過創建時間點*快照*將 EBS 卷上的資料備份到 Amazon S3。快照是*增量*備份，這意味著僅保存設備上在最新快照之後更改的資料塊。由於無需複製資料，此架構將最大限度縮短創建快照所需的時間和增加存儲成本節省。

每個快照都包含將資料（拍攝快照時存在的資料）還原到新 EBS 卷所需的所有資訊。當您基於快照創建 EBS 卷時，新卷將開始作為原始卷的精確副本。該原始卷用於創建快照。複製的卷將在後臺載入資料，讓您可以立即開始使用資料。如果您訪問尚未載入的資料，卷會立即從 Amazon S3 下載請求的資料。然後，它將繼續在後臺載入該卷的其餘資料。

Amazon EBS 卷可提供脫離實例的存儲，該存儲獨立於實例的生命週期，並在可用區中的多個伺服器之間進行複製。卷可以防止任何單個元件發生故障造成資料丟失。創建快照後，快照將完成複製到 Amazon S3（快照狀態完成後）。然後，您可以將其從一個 AWS 區域複製到另一個，或在同一區域內複製。

您可以*使用 Amazon Data Lifecycle Manager* 來自動創建、保留和刪除為備份 EBS 卷而拍攝的快照。通過自動執行快照管理，您可以：

- 通過實施定期備份計畫來保護重要資料
- 按照審計員的要求或內部合規性保留備份
- 通過刪除過時的備份來降低存儲成本

您無法創建 EC2 實例存儲卷的快照但是，如果必須備份實例存儲中的資料，則可以創建一個新的 EBS 卷並對其進行格式化。然後，將新卷掛載到 EC2 實例用戶端作業系統，然後將實例存儲卷上的資料複製到 EBS 卷。回想一下，*實例存儲*卷提供了臨時資料塊級存儲，該存儲非常適合頻繁更改的資訊，例如緩衝區、緩存和臨時資料。您可能會發現必須備份實例存儲中的資料。如果是，您可能需要重新考慮為什麼首先將這些資料存儲在實例存儲卷上。

複製檔存儲也是最佳實踐。

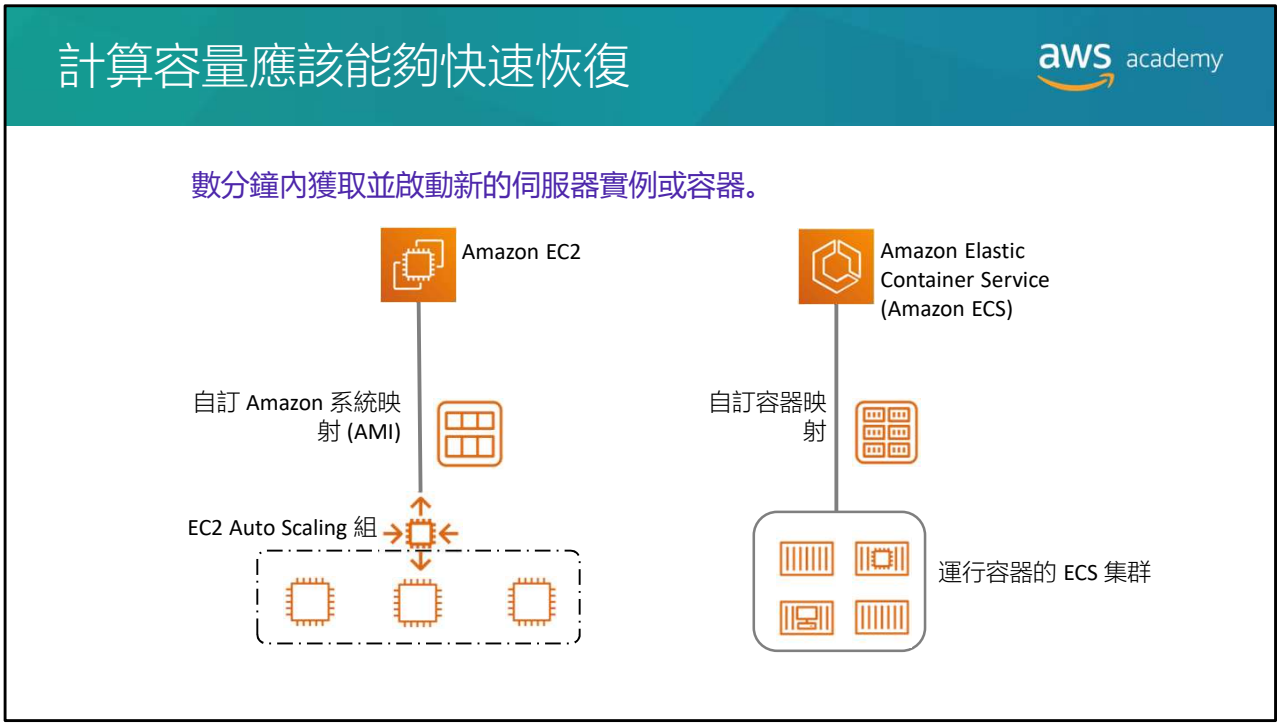
AWS DataSync 使資料在兩個 EFS 或 Amazon FSx Windows File Server 檔案系統之間，或者在本機存放區和 AWS 檔存儲之間更快地移動資料。您可以使用 DataSync 通過 DX 或互聯網傳輸資料集。使用該服務用於一次性資料移轉或持續工作流以進行資料保護和恢復。

您可以瞭解有關如何使用 *AWS Backup* 管理 EBS 卷備份和自動化 EFS 檔案系統備份的更多資訊。有關詳細資訊，請參閱使用 Amazon EFS 和 AWS Backup 計畫自動備份博客。

FSx for Windows File Server 會每天自動備份檔案系統，使您能夠隨時進行更多備份。Amazon FSx 將備份存儲在 Amazon S3 中。每日備份時段是您在創建檔案系統時指定的 30 分鐘時段。為檔案系統指定的每日備份保留期，決定了每日自動備份的保留天數。（預設情況下為 7 天。）

與大多數 Amazon S3 存儲類一樣，跨可用區複製資料同樣適用於 Amazon EFS 和 FSx for Windows File Server 檔案系統。您的災難恢復要求可能會指定您需要多區域恢復解決方案。在這種情況下，最佳實踐是將 Amazon EFS 和 FSx for Windows File Server 檔案系統複製到第二個區域。您可以使用 AWS DataSync 獲取此複製。要使用 DataSync 簡化在兩個 EFS 檔案系統之間傳輸檔的過程，您可以使用 AWS DataSync 雲端快速入門和計畫程式。

計算容量應該能夠快速恢復



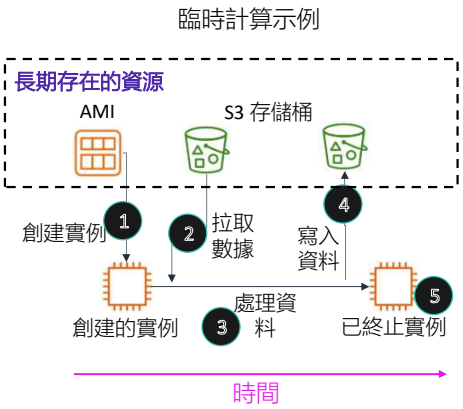
在災難恢復環境下，能夠快速創建您可控制的虛擬機器至關重要。通過在單獨的可用區中啟動實例，可以保護應用程式免受單個網站故障的影響。

當底層硬體的系統狀態檢查出現故障時，您可以安排自動恢復 EC2 實例。該實例已重新開機（必要時在新硬體上啟動），但將保留其實例 ID、IP 位址、EBS 卷附件和其他配置詳細資訊。為了完成恢復，請確保實例配置為在其初始化過程中自動啟動任何服務或應用程式。

Amazon 系統映射 (AMI) 已預先配置了作業系統，而且一些預配置的 AMI 可能還包括應用程式堆疊。您還可以配置自己的自訂 AMI。在進行災難恢復時，AWS 強烈建議您配置和標識自己的 AMI，以便它們可以作為恢復過程的一部分啟動。此類 AMI 應預配置您選擇的作業系統以及應用程式堆疊的相應部分。

計算資源的災難恢復策略

- 使用 Amazon EC2 快照功能進行備份
  - 快照可以手動執行，也可以計畫執行（例如，使用 AWS Lambda）
- 不經常使用系統或實例級系統備份，並且作為不得已的手段
  - 提高了快速使用的存儲成本
  - 改為更喜歡從配置或代碼存儲庫進行自動重建
- 跨區域 AMI 複製
- 跨區域快照複製
- 考慮臨時計算架構
  - 將基本資料存儲在實例之外

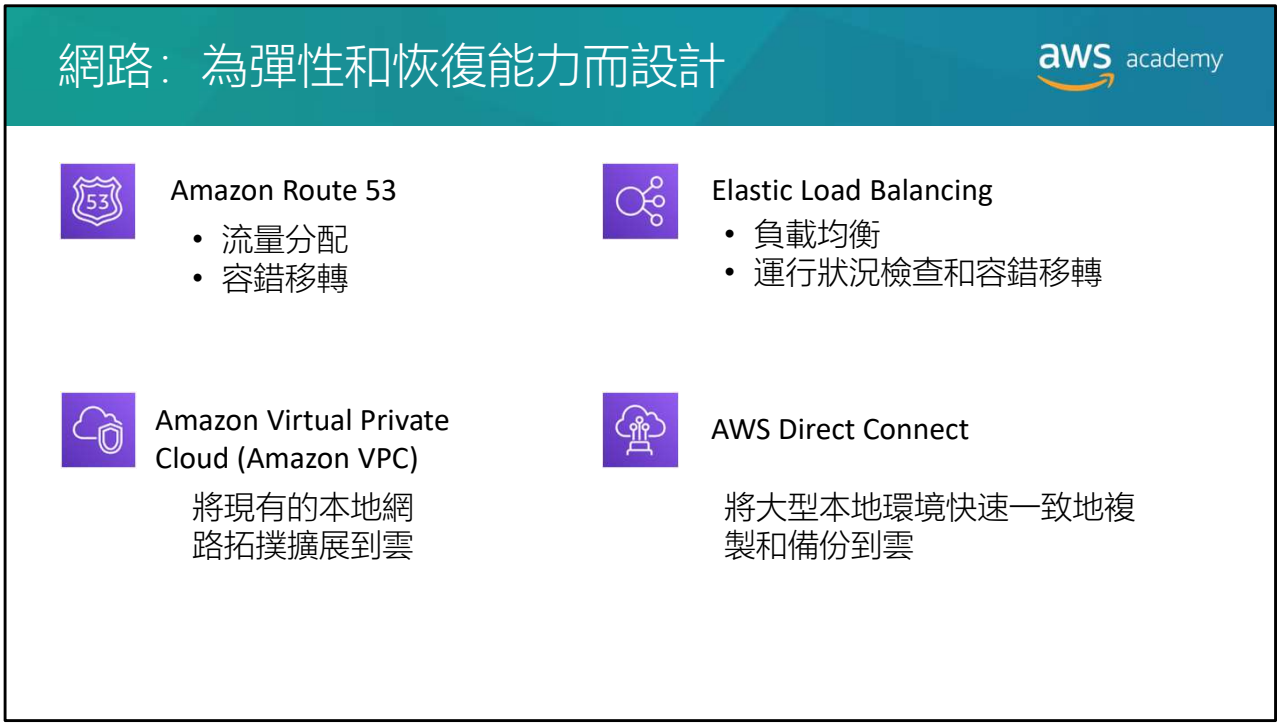


對於計算資源的災難恢復，您可能需要使用 Amazon EC2 快照功能。快照可以手動拍攝，也可以定時拍攝。

儘管您可以創建系統或實例級系統備份，但廣泛使用此方法會增加存儲成本。更好的方法是配置自動重建過程，將原始程式碼存儲在存儲庫中。

您可能希望跨區域複製 Amazon S3，並且可能還希望跨區域複製最關鍵的 AMI 和快照。

最後，考慮架構設計計算資源的使用，將基本資料存儲在實例之外。正如您在示例中看到的那樣，您的資料可以存儲在 S3 存儲桶中。當您必須處理資料時，您可以從使用應用程式軟體預配置的自訂 AMI 啟動一個或多個 EC2 實例。實例啟動後，它就可以從 S3 存儲桶中提取所需的資料並處理資料。然後，它可以將輸出資料寫回 Amazon S3（也許寫入另一個 S3 存儲桶）。實例在完成計算任務後，實例可以終止。這種架構（當它仍然可以滿足您的業務需求時）可以更輕鬆地設計災難恢復策略。它還可以節省成本，因為不常用的伺服器可以被終止，然後在需要時重新創建。



當您努力從災難中恢復時，很可能必須修改網路設置才能將系統故障切換到另一個網站。AWS 可提供多種讓您能夠管理和修改網路設置的服務和功能，在下方將突出顯示其中的幾種服務和功能。

Amazon Route 53 提供負載均衡和網路路由功能，以便您分配網路流量。它還提供了在多個終端節點之間進行故障切換的功能，甚至可以容錯移轉到 Amazon S3 中託管的靜態網站。

Elastic Load Balancing *服務可以在多個 EC2 實例間自動分配傳入的應用程式流量*。它可以提供回應應用程式傳入流量所需要的負載均衡容量，讓您實現應用程式容錯性能。您可以預先分配負載等化器，以便其網域名稱系統 (DNS) 名稱已知，這可以簡化災難恢復計畫的實施。

您可以使用 *Amazon Virtual Private Cloud (Amazon VPC)* 將現有本地網路拓撲擴展到雲。當您恢復可能託管在內部網路上的企業應用程式時，此擴展尤為適合。

最後，*AWS Direct Connect* 可以簡化從本地資料中心到 AWS 的私人網路絡連接設置。使用 DX 可以減少網路花費、增加頻寬輸送量，同時提供優於 Internet 連接的穩定網路體驗。

資料庫：支持恢復的功能

Amazon Relational Database Service (Amazon RDS)

- 創建資料快照並將其保存在一個單獨的區域
- 將只讀副本與多可用區部署相結合，構建彈性災難恢復策略
- 保留自動備份

Amazon DynamoDB

- 數秒內備份整個表
- 使用時間點恢復，持續備份表的時間可長達 35 天
- 只需在控制台中按一下一下滑鼠或調用一次應用程式設計發展介面 (API) 即可啟動備份
- 使用全域表構建多區域、多主要資料庫，為大規模擴展的全球分散式應用程式提供快速的本地性能

AWS 提供了許多資料庫服務。下面將介紹 Amazon RDS 和 Amazon DynamoDB 的一些與災難恢復方案相關的關鍵功能。

考慮在災難恢復*准備階段*使用 *Amazon RDS*，將關鍵資料的副本存儲在已運行的資料庫中。然後，在災難恢復的*恢複階段*使用 Amazon RDS 來運行生產資料庫。

如果您實施多區域災難恢復計畫，通過 Amazon RDS，您可以將從一個區域捕獲的快照資料存儲到另一個區域。您最多可以與其他 20 個 AWS 帳戶共用手動快照。

將唯讀副本與多可用區部署相結合，您可以構建彈性災難恢復策略並簡化資料庫引擎升級過程。通過使用 Amazon RDS 唯讀副本，您可以創建資料庫實例的一個或多個唯讀副本。您可以在同一 AWS 區域或另一個 AWS 區域中創建這些副本。然後，對來源資料庫所做的更新將非同步複製到唯讀副本。唯讀副本在需要時也能升級成獨立的資料庫實例。

在準備階段使用*Amazon DynamoDB* 將資料複製到另一個區域的 DynamoDB 或複製到 Amazon S3。在災難恢復的恢復階段，您可以在幾分鐘內擴展。DynamoDB 全域表會在您選擇的 AWS 區域中自動複製您的 DynamoDB 表。它們可以解決更新衝突並使應用程式保持高度可用，即使在整個區域被隔離或受到降級影響這些不太可能發生的情況下也是如此。

自動化服務：快速複製或重新部署環境

AWS CloudFormation

- 按需使用範本快速部署資源集合
- 在幾分鐘內在新區域或 VPC 中重複生產環境

AWS Elastic Beanstalk

- 只需按一下幾下即可快速重新部署整個堆疊

AWS OpsWorks

- 自動主機更換
- 在恢復階段將其與 AWS CloudFormation 結合使用
- 預置支援已定義 RTO 的新堆疊

使用自動化服務時，可以快速複製或重新部署環境。

AWS CloudFormation 使您可以在文字檔中為整個基礎設施建模和部署。此範本可成為您的基礎設施的唯一可信來源。當您使用 AWS CloudFormation 管理整個基礎設施時，它也成為災難恢復規劃工具包中的強大工具。例如，它使您能夠在幾分鐘內將複雜的生產環境複製到新區域或新 VPC。

AWS CloudFormation 以可重複的方式預置資源，這使您能夠構建和重建基礎設施和應用程式。您無需執行手動操作或編寫自訂腳本。

如果您使用 *AWS Elastic Beanstalk* 託管您的應用程式，您可以上傳更新後的應用程式來源資料包並將其部署到您的 AWS Elastic Beanstalk 環境。或者，您可以重新部署以前上傳的應用程式版本。您還可以將之前上傳的應用程式版本部署到其任意環境。

最後一點，*AWS OpsWorks* 是一種應用程式管理服務，可以輕鬆部署和運行各種類型和規模的應用程式。您可以將環境定義為一系列層，並將每一層配置為應用程式的一個層。AWS OpsWorks 具有自動主機替換功能，因此如果實例發生故障，會自動進行替換。您可以在災難恢復*准備階段*使用 AWS OpsWorks 來模擬您的環境，並且在恢復恢復的災難階段將其與 AWS CloudFormation 結合使用。

第 2 節要點

- 要選擇正確的災難恢複策略，首先確定復原點目標 (RPO) 和恢復時間目標 (RTO)
- 使用 S3 跨區域複製、 EBS 卷快照和 Amazon RDS 快照等功能來保護資料
- 使用聯網功能（如 Route 53 容錯移轉和 Elastic Load Balancing ）來提高應用程式可用性
- 使用自動化服務作為災難恢復策略的一部分（例如 AWS CloudFormation），在需要時快速部署重複環境

本模組中這節內容的要點包括：

- 要選擇正確的*災難恢複*策略，首先確定復原點目標 (RPO) 和恢復時間目標 (RTO)
- 使用 S3 跨區域複製、EBS 卷快照*和* RDS 快照等功能來保護資料
- 使用聯網功能（如 *Route 53 容錯移轉*和 *Elastic Load Balancing*）來提高應用程式可用性
- 使用自動化服務作為災難恢復策略的一部分（例如 *AWS CloudFormation*），*在需要時*快速部署重複環境

模組 14：災難規劃

第 3 節：災難復原模式

介紹第 3 節：災難復原模式。

AWS 上的常用災難復原模式

aws academy

四種災難復原模式

- 備份與還原
- "Pilot light"式
- 熱備份
- 多網站

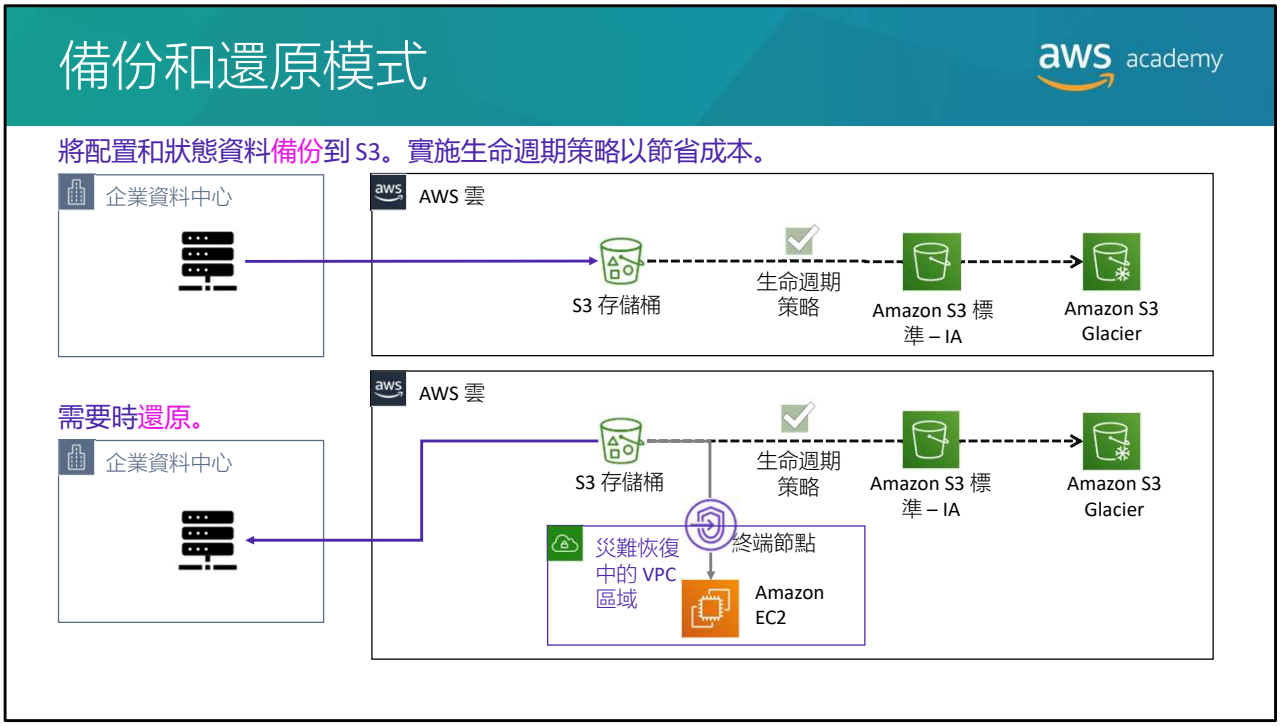
每種模式都適合以下不同的組合：

- 復原點目標
- 恢複時間目標
- 成本效益

組織經常使用以下四種常見的災難復原模式：

- 備份與還原
- "Pilot light" 式
- 熱備份
- 多網站

正如您將在下面的細節中發現的那樣，每種模式都非常適合不同的要求。其中一些模式提供了更好的成本效益。其他一些模式則提供更快的 RPO 和更快的 RTO，但維護成本更高。



第一種災難恢復方法是*備份和還原模式*。

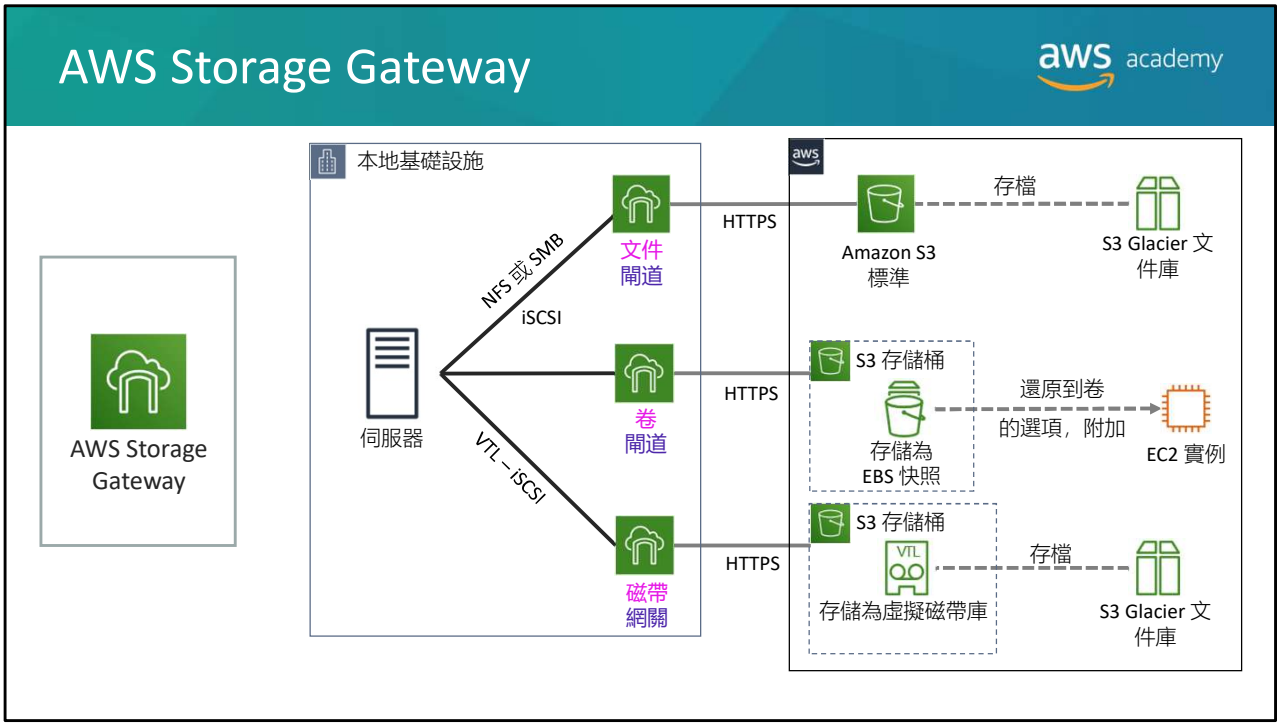
大多數傳統環境中都會將資料備份到磁帶並定期發送到異地。如果使用此方法，則在發生災難時恢復系統可能需要很長時間。

Amazon S3 為執行恢復亟需的備份資料提供了一個更容易訪問的目標。數據傳入和傳出 Amazon S3 通常都通過網路完成，因此可以從任意位置訪問。

在示例備份場景中，資料從本地資料中心複製到 Amazon S3。AWS DataSync 或 Amazon S3 Transfer Acceleration 可以選擇用作此配置的一部分，以自動化或提高資料傳輸速度。然後，應用於存儲桶的 S3 生命週期配置稍後會將備份資料移動到成本較低的 Amazon S3 存儲類中。備份資料移動到 Amazon S3 Glacier 或 Amazon S3 標準 – IA，隨著資料老化而且不經常訪問，可節省成本。

在示例還原方案中，本地資料可能會暫時或永久丟失。然後，備份資料可以從 Amazon S3 下載回本機伺服器。

如果您的公司資料中心仍處於離線狀態，您可以進一步確保將資料還原到伺服器的功能。您可以在指定災難恢復區域的 VPC 中使用 Amazon EC2 伺服器。此區域可以連接到包含備份應用程式資料的 S3 存儲桶。它可以讀取這些資料，也許可以在恢復資料中心的同時臨時託管應用程式。



作為備份和還原模式的一部分，您可能會發現使用 AWS Storage Gateway 意義重大。

AWS Storage Gateway 是一種混合存儲服務，您的本地應用程式可以借助它來使用 AWS 雲存儲。您可以使用該服務進行備份、存檔、災難恢復、雲資料處理、存儲分層和遷移。

您的應用程式可以使用標準存儲協定通過虛擬機器或硬體閘道設備連接到該服務。這些協定包括 NFS、SMB、虛擬磁帶庫 (VTL) 和互聯網小型電腦系統介面 (iSCSI)。閘道會連接到 Amazon S3、Amazon S3 Glacier、Amazon EBS 等 AWS 存儲服務，這些服務為檔、卷和虛擬磁帶提供存儲。該服務包括優化的資料傳輸機制。它提供頻寬管理、自動實現網路彈性、高效傳輸資料以及本地緩存，讓您能夠對最活躍的資料進行低延遲本地訪問。

使用*文件閘道*，您可以在 Amazon S3 中存儲和檢索物件（通過使用 NFS 或 SMB 協議）。您可以使用本地緩存實現低延遲對您最近使用的資料訪問。當您將檔案傳輸到 Amazon S3 之後，它們將作為物件存儲，並允許通過 NFS 掛載點進行訪問。

Storage Gateway *卷*介面為您的應用程式提供了資料塊存儲磁片卷，可以使用 iSCSI 協定訪問這些卷。這些卷上的資料將作為時間點 EBS 快照進行備份，因此您可以在必要時通過 Amazon EC2 對其進行訪問。

Storage Gateway *磁帶*接口 以虛擬磁帶庫的形式將 Storage Gateway 呈現給您的現有備份應用程式。此庫由虛擬介質轉換器和虛擬磁帶驅動器組成。您可以繼續使用現有的備份應用程式，同時寫入虛擬磁帶集。每個虛擬磁帶均存儲在 Amazon S3 中。當您不再需要訪問虛擬磁帶上的資料時，您的備份應用程式可以將其從虛擬磁帶庫存檔到 Amazon S3 Glacier。

備份與還原：檢查清單

aws academy

準備階段

- 創建當前系統備份
- 將備份存儲在 Amazon S3 中
- 記錄從備份還原的過程
- 瞭解：
  - 根據需要使用和構建哪些 AMI
  - 如何從備份中還原系統
  - 如何將流量路由到新系統
  - 如何配置部署

發生災難時

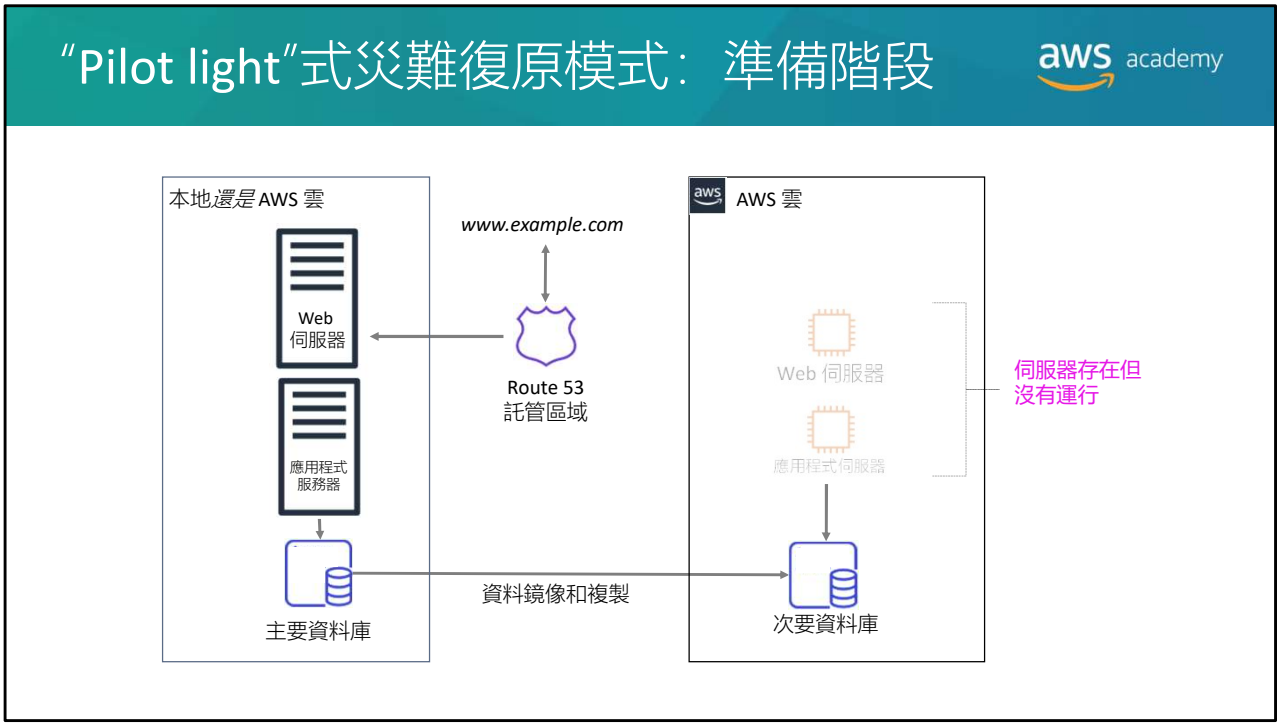
- 從 Amazon S3 中檢索備份
- 恢復所需的基礎設施
  - 來自準備好的 AMI 的 EC2 實例
  - Elastic Load Balancing 負載等化器
  - 由 AWS CloudFormation 堆疊創建的 AWS 資源 – 自動部署以恢復或複製環境
- 從備份中恢復系統
- 將流量路由到新系統
  - 相應地調整網域名稱系統 (DNS) 記錄

如果實施備份和還原災難復原模式，則在*准備階段*應完成的關鍵步驟是：

- 創建當前系統備份
- 將備份存儲在 Amazon S3 中
- 記錄從備份還原的過程

如果實施此模式，在發生*災難時要完成的*關鍵步驟是：

- 從 Amazon S3 中檢索備份
- 開始所需的基礎設施
- 從備份中還原系統
- 最後，將流量路由到新系統



第二種災難恢復方法是 *"Pilot light" 式災難復原模式*。

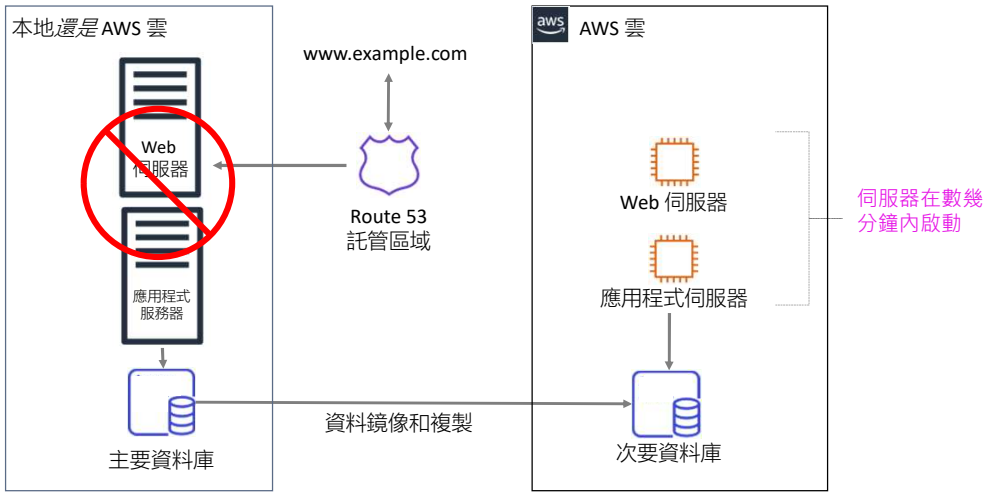
*"Pilot light" 式災難復原模式*描述了一種災難復原模式，*其中環境的*最低*備份版本*始終在運行。標燈類比源於燃氣取暖器：即使在加熱器關閉的情況下，小火焰（或標燈）始終燃起。標燈可以迅速點燃整個爐灶，讓房間變暖。在示例模式中，標燈是始終在運行的次要資料庫。

標燈方案類似於備份和恢復方案。但是，恢復時間通常會更快，因為系統的核心部分已經在運行並持續保持最新狀態。恢復時，您可以快速預置關鍵核心周圍的完整生產環境。

標燈本身的基礎設施要素通常包括您的資料庫伺服器。這種分組是該系統的關鍵核心（標燈）。可以快速預置所有其他基礎設施部件，以恢復整個系統。要預置基礎設施的其餘部分，您通常將預置的伺服器捆綁為可立即啟動的 AMI。（或者它們可能是處於停止狀態的實例。）恢復開始時，這些實例將以其預定義的角色快速啟動，從而使它們能夠連接到資料庫。

此模式實施起來相對經濟實惠。必須將定期更改的資料複製到標燈中，即整個環境在恢復階段啟動的小核心。作業系統和應用程式等不經常更新的資料可以定期更新並存儲為 AMI。

“Pilot light”式災難復原模式：在發生災難的情況下



假設發生災難，主應用程式將離線。在這種情況下，您可以快速委託計算資源運行應用程式或編排容錯移轉以在 AWS 中標記資源。在此示例中，次要資料庫用於存儲關鍵資料。如果發生災難，新的 Web 伺服器和應用程式伺服器將啟動並連接到次要資料庫。Amazon Route 53 配置為然後將流量路由到新的 Web 伺服器。

主環境可以存在於本地資料中心，也可以存在於 AWS 上的另一個區域或可用區中。無論哪種方式，您都可以使用標燈模式來滿足恢復時間目標 (RTO)。

“Pilot light”式災難復原模式：檢查清單

準備階段

- 配置 EC2 實例以複製或鏡像伺服器
- 確保您擁有 AWS 中提供的所有支援性自訂套裝軟體
- 創建並維護需要快速恢復的主要伺服器的 AMI
- 定期運行這些伺服器，對其進行測試，並且應用所有軟體更新和配置更改
- 考慮自動預置 AWS 資源

發生災難時

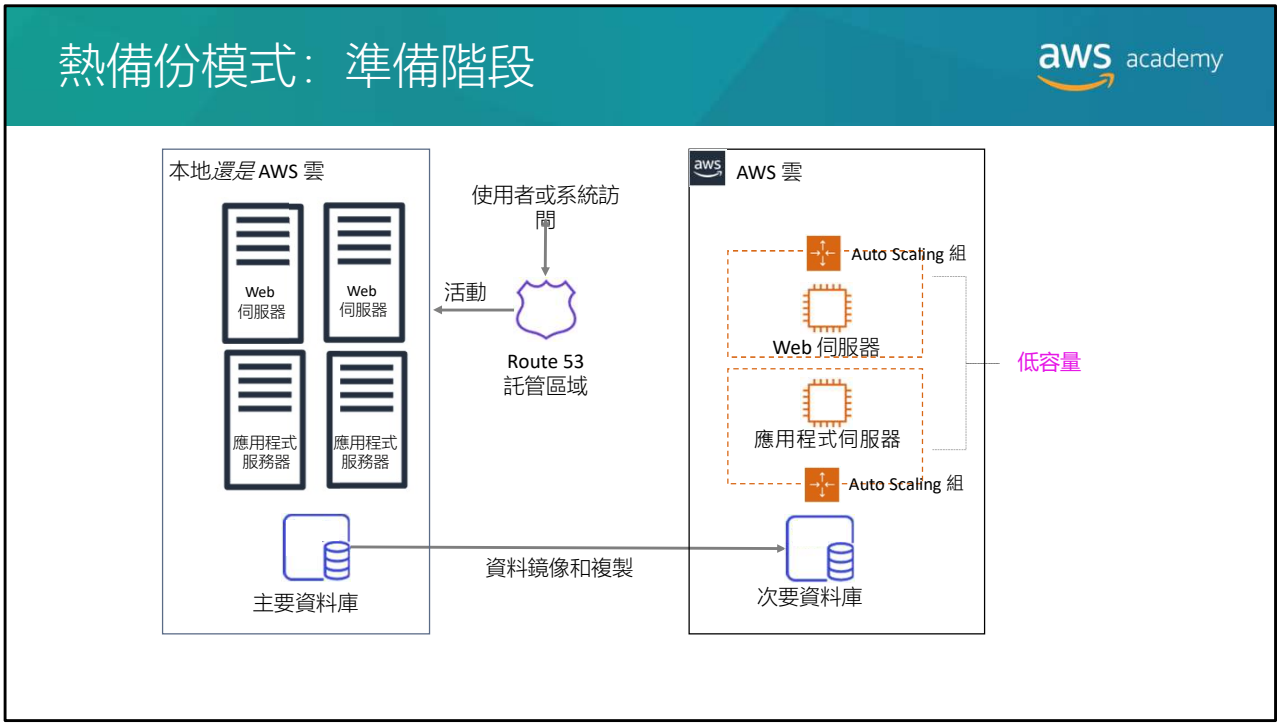
- 自動調出已複製核心資料集周圍的資源
- 根據需要擴展系統以處理當前的生產流量
- 切換到新系統
  - 調整 DNS 記錄以指向 AWS

如果實施標燈災難復原模式，則在*准備階段*應完成的關鍵步驟是：

- 配置 EC2 實例
- 確保您擁有提供的所有支援性自訂套裝軟體
- 創建並維護需要快速恢復的必要 AMI。
- 定期運行並測試這些伺服器，並且應用軟體更新和配置更新
- 考慮自動預置 AWS 資源

如果實施此標燈模式，在發生*災難時要完成的*關鍵步驟是：

- 自動調出已複製核心資料集周圍的資源
- 根據需要擴展系統以處理當前的生產流量
- 通過調整 DNS 記錄以指向備份部署，切換到新系統



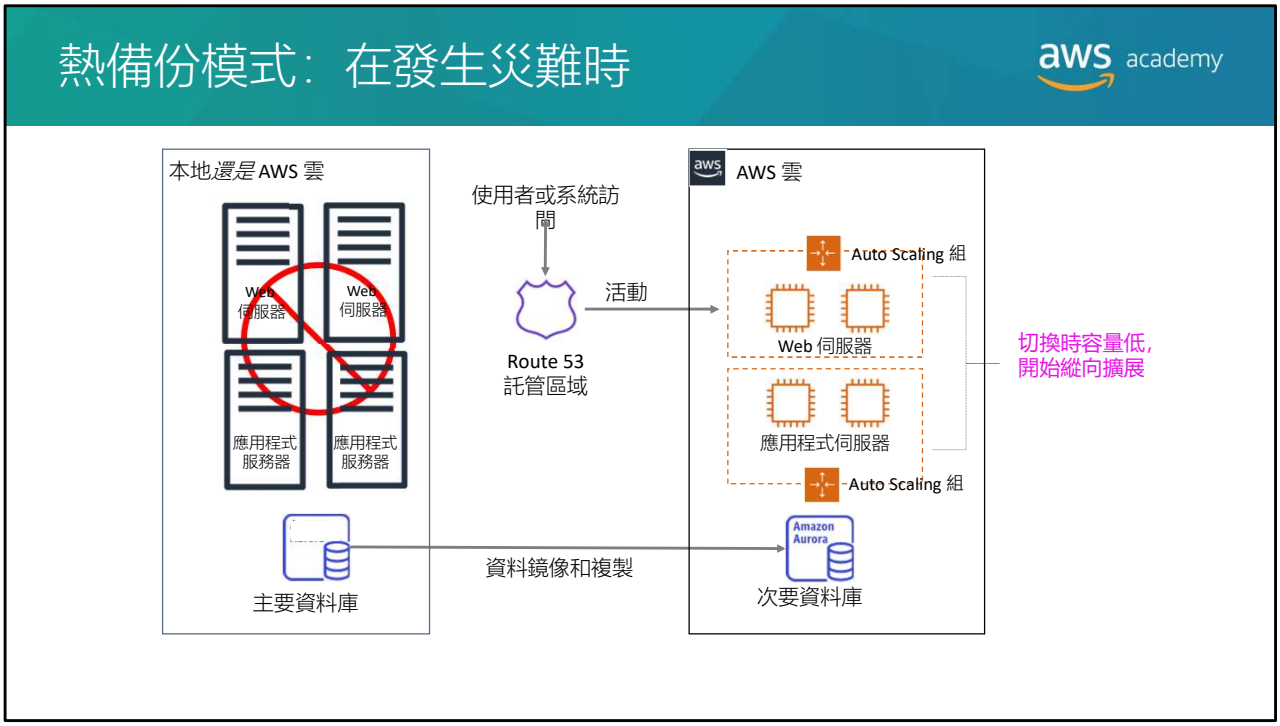
第三種災難恢復方法是*熱備份災難復原模式*。

熱備份災難復原模式與“Pilot light”式災難復原模式一樣，但更多的資源已經在運行。“*熱備份*”一詞用於描述災難恢復場景，在此場景下，功能完備的縮小版環境始終在雲中運行。熱備份解決方案擴充了“Pilot light”式災難恢復的元素和準備工作，進一步縮短了恢復時間，因為某些服務一直在運行。通過識別您的業務關鍵型系統，您可以完全複製這些系統並讓它們始終保持運行。

這些伺服器可以在佇列規模最小，實例大小最小的 EC2 實例佇列上運行。此解決方案並未經過擴展，無法承擔全部生產負載，但它的功能完備。儘管它用於災難恢復目的，但您也可以將其用於非生產性工作，例如測試、品質保證和內部使用。

在示例中，兩個系統正在運行。主系統可能在本地資料中心或 AWS 區域中運行，並且 AWS 上運行的是低容量系統。使用 Amazon Route 53 在主系統和備份系統之間分發請求。

熱備份模式：在發生災難時



在災難中，如果主環境不可用，Amazon Route 53 會切換到輔助系統。

然後，輔助系統可以迅速開始向上擴展以便處理生產負載。您可以通過向負載等化器添加更多 EC2 實例來實現這此增長。或者，您可以調整小容量伺服器的大小，以便在較大的 EC2 實例類型上運行。 橫向擴展（創建更多 EC2 實例）優先於縱向擴展（增加現有實例的大小）。

熱備份模式：檢查清單

準備工作

- 與"Pilot Light"式類似
- 所有必要組件全天候運行，但不因生產流量而擴展
- 最佳實踐：持續測試
  - 促使生產流量的統計子集慢慢移動到災難恢復網站

發生災難時

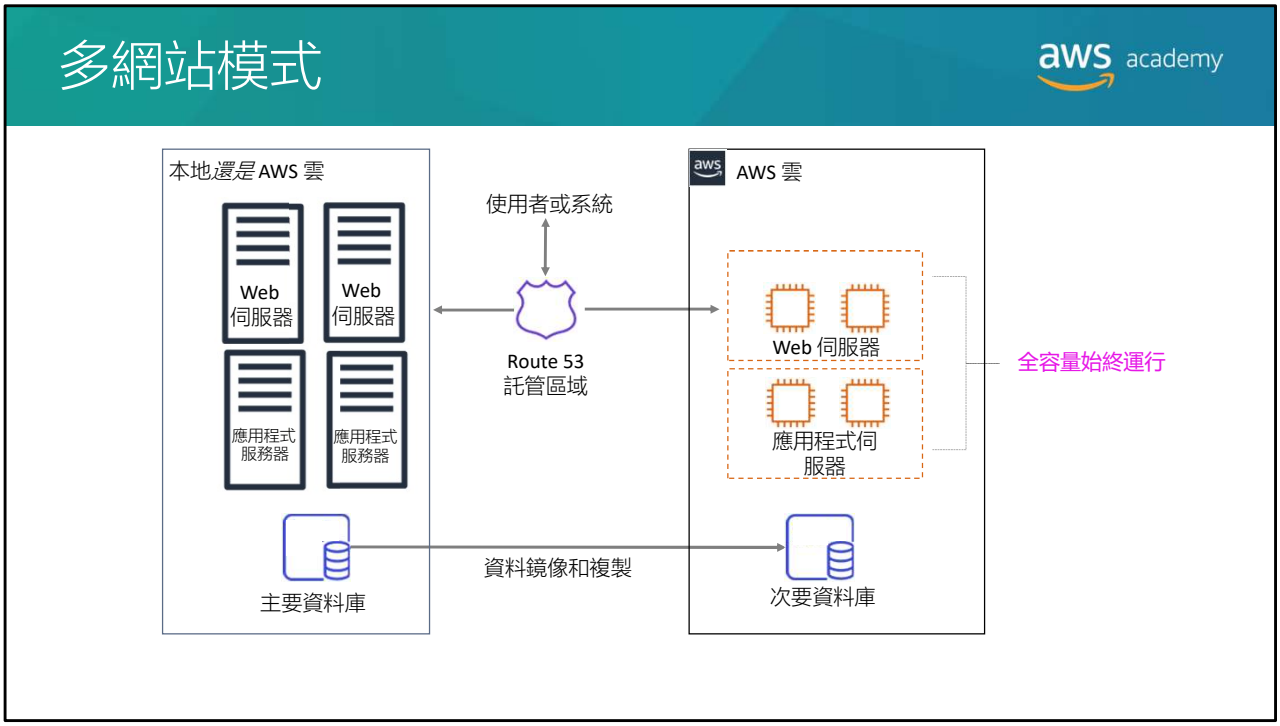
- 立即對關鍵生產負載進行容錯移轉
  - 調整 DNS 記錄以指向 AWS
- 進一步（自動）擴展系統以處理所有生產負載

如果實施熱備份災難復原模式，那麼*準備階段*至關重要。在準備階段，您應該完成的關鍵步驟與為“Pilot light”式災難復原模式完成的步驟類似。最顯著的區別是，所有必要的元件都應保持全天候運行，但不能根據生產流量進行擴展。

作為最佳實踐，進行持續測試。您還可能會促使生產流量的統計子集慢慢移動到災難恢復網站因此，您可以驗證它是否與主系統一樣可無縫用於使用者和系統。

使用熱備份模式，*在發生災難時*，要完成的關鍵步驟是：

- 立即對最關鍵的生產負載進行容錯移轉
- 調整 DNS 記錄以指向 AWS
- 進一步（自動）擴展系統以處理所有生產負載



第四種也是最後一種災難恢復方法是*多網站模式*。使用這種模式，您將擁有一個功能齊全的系統，其在第二個 AWS 區域運行。它與本地系統或在其他 AWS 區域中運行的系統同時運行。

多網站解決方案在*雙活配置*中運行。您使用的資料複製方法由您選擇的復原點決定。

由於兩個網站都可以支援全部生產容量，因此您可以選擇使用支援加權路由的 DNS 服務。Amazon Route 53 就是一個例子，它將生產流量路由到交付相同應用程式或服務的兩個網站。在這種情況下，一部分流量會流入 AWS 中的基礎設施，其餘流量會流入您的現場基礎設施。（或者，如果這兩個環境存在於不同的 AWS 區域中，則流量在這兩個區域之間按比例分佈。）

如果現場或主要 AWS 區域出現災難，您可以調整 DNS 權重並將*所有*流量發送到第二個部署。然後，第二個部署的容量可以快速提高以按需處理整個生產負載。您可以使用 Amazon EC2 Auto Scaling 自動執行這一流程。您可能需要使用某種應用程式邏輯來檢測主要資料庫服務的故障，然後切換到已運行的並行資料庫服務。

此場景的成本取決於正常操作期間的生產流量總量。在恢復階段，您只需支付整個災難恢復環境持續時間內您所使用的內容。您可以為始終運行的 AWS 伺服器購買 Amazon EC2 預留實例，以進一步降低成本。

多網站：檢查清單

準備工作

- 類似於熱備份
- 配置為完全向內擴展或向外擴展以實現生產負載

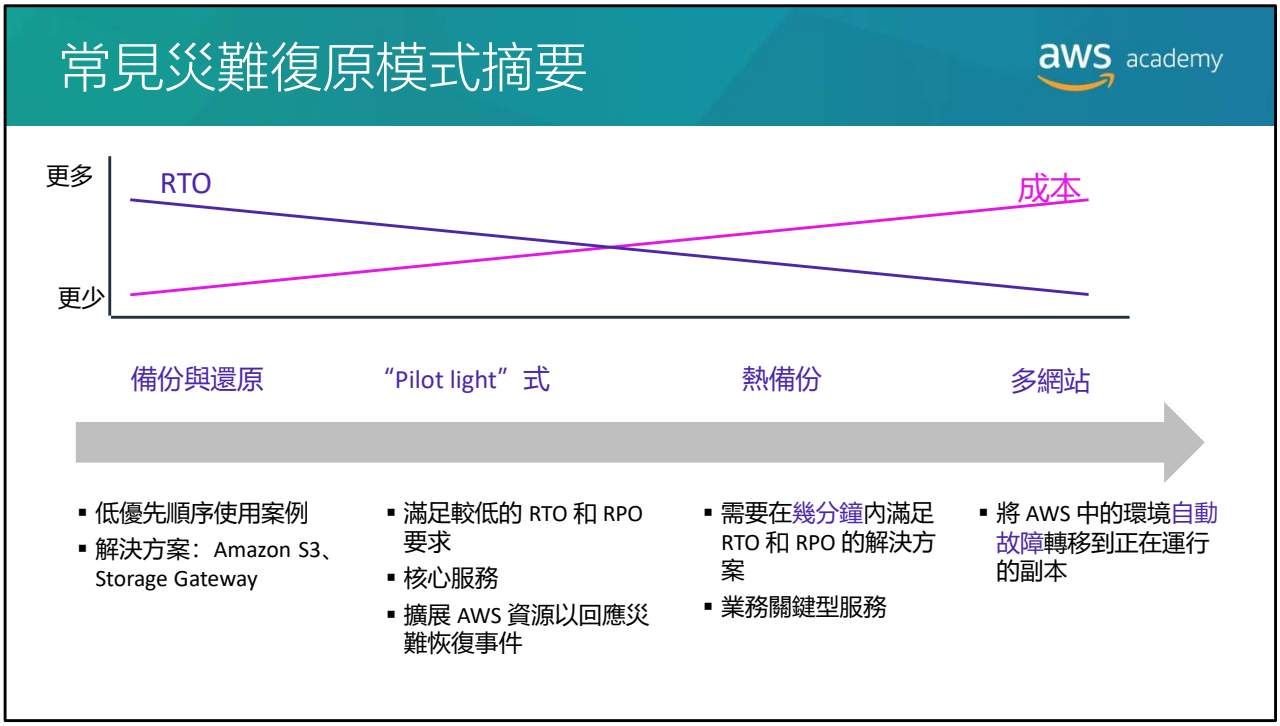
發生災難時

- 立即對所有生產負載進行容錯移轉

如果您正在實施多網站災難復原模式，則*准備階段*要完成的關鍵步驟與熱備份模式類似。您必須將備份部署配置為完全擴展和縮減生產負載。您應該讓伺服器運行並準備好接收流量。

使用多網站模式，*在發生災難*時，您只需完成一個關鍵步驟。這一步是立即將所有生產負載容錯移轉到備份網站。

多網站模式的停機時間可能最少。但是，由於需要運行的系統更多，它的成本確實更高。



總而言之，四種災難復原模式中的每種模式都提供了不同的優勢組合。

此圖顯示了四種場景的圖譜，按照災難恢復事件發生後系統可重新供使用者使用的速度排列。

備份和還原模式通常可以最低的成本完成任務，但它的 RTO 較長。因此，您的系統的恢復速度可能比選擇其他模式更慢。

熱備份模式和多網站模式支援快得多的 RTO，但是由於需要一直運行的額外系統，因此成本會更高。

您能夠使用 AWS 經濟高效地執行每種災難恢復策略。重要的是要注意，這裡列舉的只是一些可行的模式示例，您也可以有多種模式變體或將其組合使用。如果您的應用程式在 AWS 上運行，則可以使用多個區域，同樣的災難恢復策略仍然適用。

災難恢復準備：最佳實踐

簡單開始

檢查軟體許可問題

方案演練
練習

制定全面的災難恢復計畫可能是一項複雜的任務。但是，大多數組織都認識到（可能是從過去的事件中吸取經驗教訓），這值得付出努力。

儘管制定和實施完整計畫需要時間，但這不應阻止您邁出簡單的第一步。簡單開始，然後再自行擴展。例如，作為第一步，創建資料存儲、資料庫和關鍵伺服器的備份。然後，作為持續努力的一部分，努力逐步改善 RTO 和 RPO。

軟體許可證是創建備份網站時可能會出現的問題。查看您必須獲得的軟體許可證，以確定當前的許可證合同是否支持您的災難恢復計畫。根據需要升級許可證或以其他方式進行調整。

最後，始終如一地運用災難恢復解決方案是一種最佳做法，以確保其按預期工作。一些建議的步驟包括：

- 方案演練。這些練習可測試關鍵系統離線的場景，甚至整個區域。如果整個佇列崩潰，該怎麼辦？
- 確保正在創建備份、快照和 AMI，並且可以使用它們成功恢復資料。
- 監控您的監控系統。

測試您的回應程式，確保它們有效且團隊熟知如何將其付諸實踐。設置定期的實際試用，以測試工作負載和團隊對類比事件的反應。

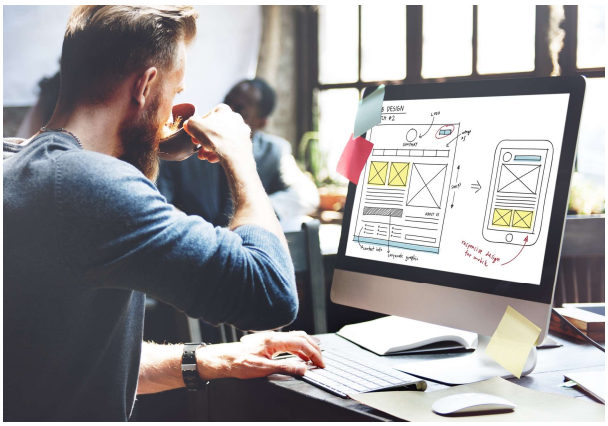
第 3 節要點

- AWS 上常見的災難恢複模式包括備份和恢復、“Pilot light”式、熱備份模式和多網站。
- 備份和恢復是最具成本效益的方法。但是，它擁有最高的 RTO。
- 多網站提供了最快的 RTO。但是，它的成本最高是因為它提供了一個完全運行的生產就緒副本。
- AWS Storage Gateway 提供三個介面（檔閘道、卷閘道和磁帶閘道），用於本地和 AWS 雲之間的資料備份和恢復。

本模組中這節內容的要點包括：

- AWS 上常見的*災難恢複模式*包括備份和恢復、“Pilot light”式、熱備份模式和多網站。
- *備份和恢復*是最經濟高效的方法，但它具有最高的 RTO。
- *多網站*提供了最快的 RTO，但其成本最高，因為它提供了一個完全運行的生產就緒副本。
- *AWS Storage Gateway* 提供三個介面（檔閘道、卷閘道和磁帶閘道），用於本地和 AWS 雲之間的資料備份和恢復。

模組 14 – 指導實驗：使用 AWS Storage Gateway 檔閘道進行混合存儲和資料移轉



現在，您將完成開始模組 14 – 指導實驗：使用 AWS Storage Gateway 檔閘道進行混合存儲和資料移轉

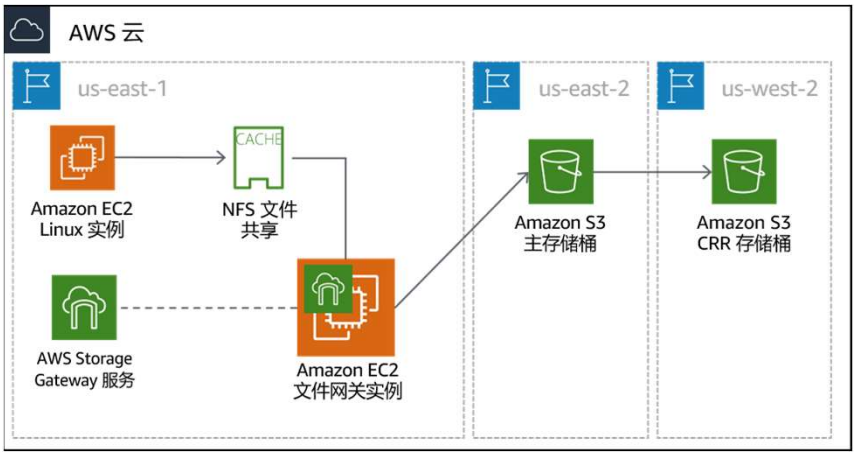
指導實驗：任務

1. 查看實驗架構
2. 創建主 S3 存儲桶和輔助 S3 存儲桶
3. 啟用跨區域複製
4. 設定檔閘道並創建 NFS 檔共用
5. 將檔共用掛載到 Linux 實例並遷移資料
6. 驗證資料是否已遷移

在本指導實驗中，您將完成以下任務：

1. 查看實驗架構
2. 創建主 S3 存儲桶和輔助 S3 存儲桶
3. 啟用跨區域複製
4. 配置檔閘道並創建 NFS 檔共用
5. 將文件共用掛載到 Linux 實例並遷移資料
6. 驗證數據是否已遷移

指導實驗：最終產品



該圖總結了您完成指導實驗後將會構建的內容。您將使用 AWS Storage Gateway 中的檔閘道選項成功將資料移轉到 Amazon S3。

大約 45 分鐘

現在可以開始指導實驗了。

指導實驗總結：要點

完成這個指導實驗之後，您的講師可能會帶您討論此指導實驗的要點。

模組 14：災難規劃

模組總結

現在來回顧下本模組，並對知識測驗和對實踐認證考試問題的討論進行總結。

模組總結

aws academy

總體來說，您在本模組中學習了如何：

- 確定災難規劃策略
- 定義 RPO 和 RTO
- 描述備份和災難恢復的四種常見模式以及實施方法
- 使用 AWS Storage Gateway 實現本地到雲備份解決方案

總體來說，您在本模組中學習了如何：

- 確定災難規劃策略
- 定義 RPO 和 RTO
- 描述備份和災難恢復的四種常見模式以及實施方法
- 使用 AWS Storage Gateway 實現本地到雲備份解決方案

完成知識測驗

現在可以完成本模組的知識測驗。

樣題

aws academy

公司銷售人員每天上傳銷售資料。解決方案架構師需要為這些文檔提供持久存儲解決方案，以防止用戶意外刪除重要文檔。

哪項操作可以防止用戶意外操作？

A. 將資料存儲在 EBS 卷中，並每週創建一次快照。
B. 將數據存儲在 S3 存儲桶中並啟用版本控制。
C. 將數據存儲在不同 AWS 區域的兩個 S3 存儲桶中。
D. 將數據存儲在 EC2 實例存儲中。

請查看答案選項，並根據之前突出顯示的關鍵字排除錯誤選項。

正確答案是 B： "將資料存儲在 S3 存儲桶中並啟用版本控制。" 使用這種方法，如果刪除了某個受版本控制的物件，仍然可以通過檢索最終版本來恢復該物件。

選項 A 將丟失自上一個快照以來提交的任何更改。選項 C 將資料存儲在兩個 S3 存儲桶中，它提供的保護比選項 A 稍大一些。但是，使用者仍然可以從兩個存儲桶中刪除物件。選項 D 不是一種好方法，因為 EC2 實例存儲是短暫的，並且永遠不要應用於需要持久性的數據。

其他資源

- Amazon S3 複製
- Amazon S3 物件生命週期管理
- Amazon EBS 快照
- 將 AWS Lambda 用於計畫的事件
- 備份和還原資源中心
- 借助 AWS 實現災難恢復（視頻）

如果您想瞭解本模組所涵蓋主題的更多資訊，下面這些資源可能會有所幫助：

- Amazon S3 複製
- Amazon S3 物件生命週期管理
- Amazon EBS 快照
- 將 AWS Lambda 用於計畫的事件
- 備份和還原資源中心
- 借助 AWS 實現災難恢復（視頻）

感謝您完成本模組的學習。