歡迎學習模組 3：添加存儲層。

模組概覽

章節

1. 最簡單的架構
2. 使用 Amazon S3
3. 在 Amazon S3 中存儲資料
4. 將數據移入和移出 Amazon S3
5. 為您的架構選擇區域

演示

- Amazon S3 版本控制
- Amazon S3 Transfer Acceleration

實驗

- 指導實驗：託管靜態網站
- 挑戰實驗：為咖啡館創建靜態網站

知識考核

aws

本模組包括以下章節：

1. 最簡單的架構
2. 使用 Amazon S3
3. 在 Amazon S3 中存儲資料
4. 將數據移入和移出 Amazon S3
5. 為您的架構選擇區域

本模組還包括：

- 一個講師主導的演示，向您展示 Amazon S3 版本控制功能的工作原理。
- 一個講師主導的演示，向您展示如何配置 Amazon S3 Transfer Acceleration。
- 一個動手指導實驗，詳細的分步說明介紹了如何創建 Amazon S3 存儲桶並將其配置為託管簡單網站。
- 一個動手挑戰實驗，您將部署一個靜態網站來支援咖啡館場景。僅提供有限的指導，因為所涉及的任務與您在本模組中之前完成的指導實驗活動非常相似。

最後，您需要完成一個知識考核，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：

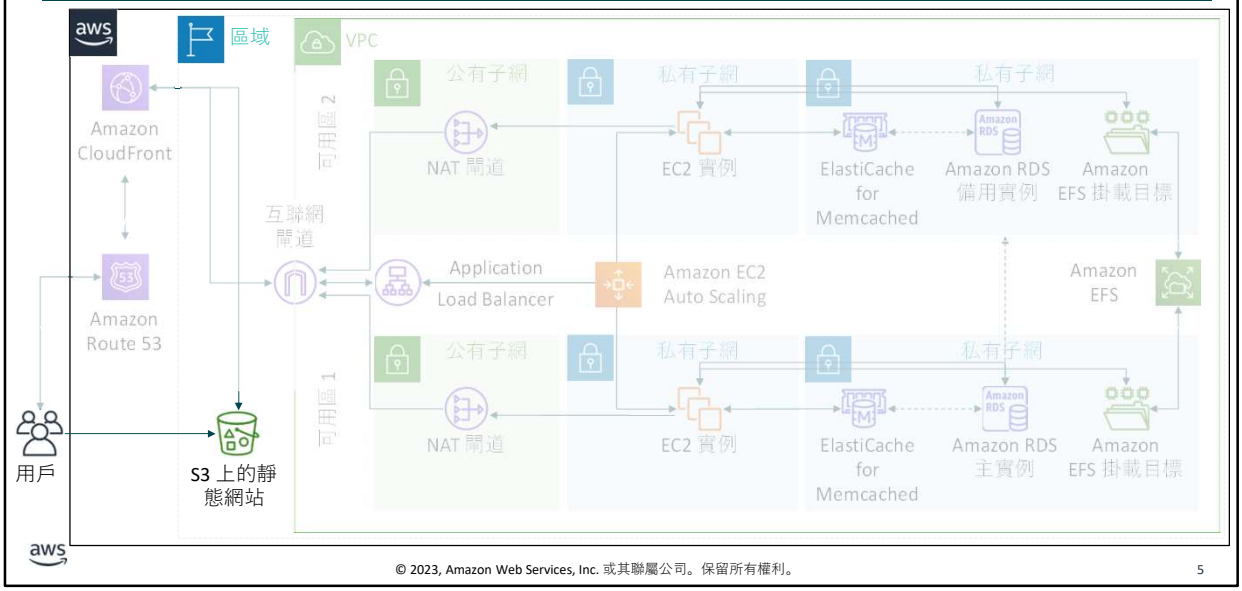
- 識別 Amazon Simple Storage Service (Amazon S3) 可以解決的問題
- 描述如何使用 Amazon S3 高效存儲內容
- 瞭解各種 Amazon S3 存儲類和成本注意事項
- 描述如何將資料移入和移出 Amazon S3
- 描述如何選擇區域
- 創建靜態網站

aws

學完本模組後，您應該能夠：
- 識別 Amazon Simple Storage Service (Amazon S3) 可以解決的問題
- 描述如何使用 Amazon S3 高效存儲內容
- 瞭解各種 Amazon S3 存儲類和成本注意事項
- 描述如何將資料移入和移出 Amazon S3
- 描述如何選擇區域
- 創建靜態網站

介紹第 1 節：最簡單的架構。

存儲是更大架構的一部分



在每個模組介紹新功能時，這張大圖中的相應部分便會顯示出來。

在本模組中，您首先要學習的是在 AWS 上實施最簡單的架構之一，即通過完全在 Amazon S3 上託管該架構來創建靜態網站。您還將瞭解各種 Amazon S3 存儲選項以及在 AWS 上選擇區域時的一些關鍵注意事項。

咖啡館業務需求

咖啡館剛剛開始運營。他們希望建立一個簡單的靜態網站，為顧客提供咖啡館的基本資訊（包括功能表、營業時間、位置等）。

這家咖啡館在這個大城市裡只開了一家店，他們在那裡出售甜點和咖啡。這家咖啡館由 Frank 和 Martha 擁有，這是一家夫妻店。他們的女兒 Sofía 和一位名叫 Nikhil 的中學生也在咖啡館工作。

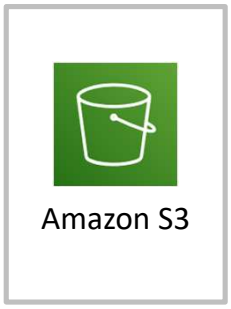
這家咖啡館目前還沒有行銷策略。有人路過，注意到咖啡館，然後決定試一試，這便是他們獲得新顧客的唯一方式。咖啡館供應的優質甜點和咖啡有著不錯的口碑，但如果不是熟客或者有人推薦的話，口碑的傳播還是比較有限的。

Sofía 建議，他們應該擴大社區對咖啡館所提供的服務的認識。Frank 和 Martha 同意了。咖啡館還沒有網路服務，他們目前也沒有使用任何雲計算服務。不過，這一現狀即將發生改變。第一個挑戰是為咖啡館創建一個基本的網站。

在本模組中，您將詳細瞭解業務要求以及如何使用 Amazon Web Services 滿足這些業務要求。

介紹第 2 節：使用 Amazon S3。

Amazon S3



對象存儲服務：

- 存儲大量（無限）非結構化資料
- 數據文件作為物件存儲在您定義的存儲桶中
- 單個物件的最大檔大小為 5 TB
- 所有物件都包含一個 REST 可訪問的全域唯一 URL（通用命名空間）
- 所有物件都包含一個鍵、版本 ID、值、中繼資料和子資源

Amazon S3 是一項*對象存儲服務*。它可讓您存儲幾乎任意數量的資料。資料檔案存儲為物件。您將物件放置在自己定義的存儲桶中。每個存儲桶的名稱必須在區域之間具有全域唯一性。這意味著存儲桶名稱在所有 AWS 客戶帳戶中必須是唯一的。

存儲的物件的大小可以從 0 位元組到 5 TB 不等。雖然單個物件不能大於 5 TB，但是您可以存儲的資料總量沒有限制。

每個物件都有五個一致的特性。

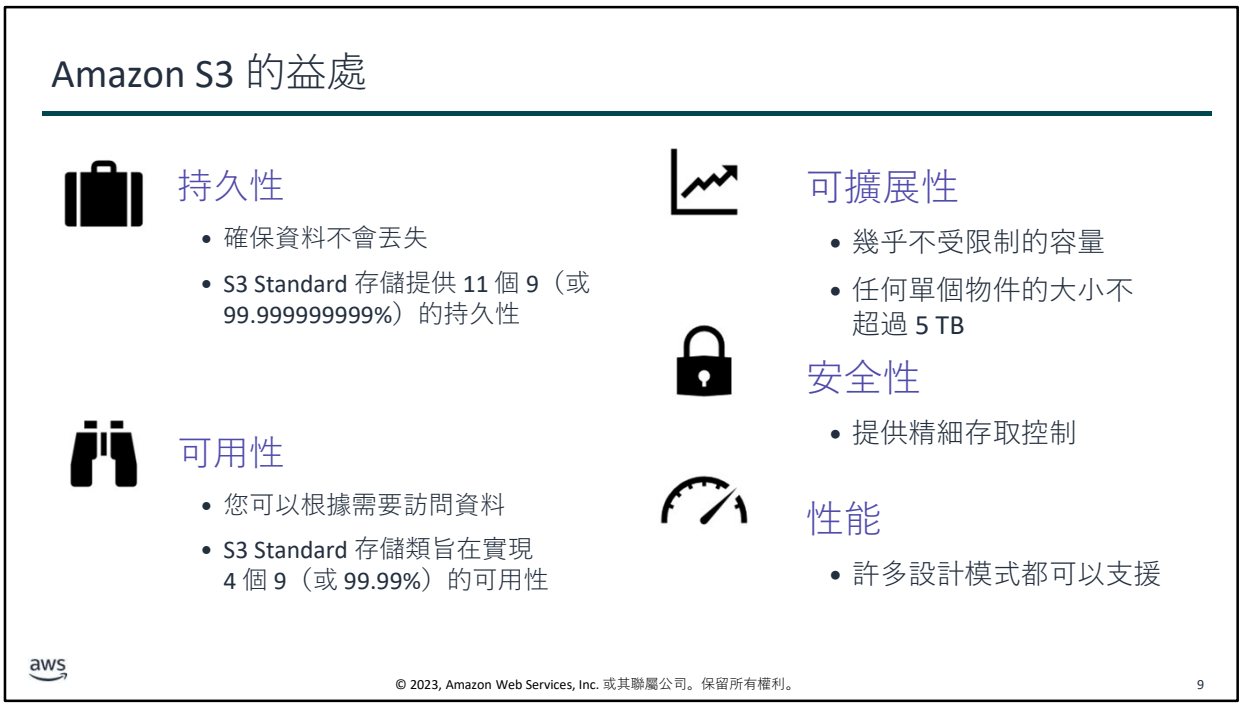
首先，它擁有一個鍵，這是您分配給物件的名稱。您可以使用物件鍵檢索該物件。
在 AWS 管理主控台中，您可以在存儲桶內創建目錄，然後將物件上傳到該目錄。但實際上，Amazon S3 並不知道目錄，因此鍵值包括相對於存儲桶根目錄的完整路徑。

對象還包括版本 ID。在存儲桶中，鍵和版本 ID 可以唯一地標識物件。稍後您將在本模組中瞭解有關版本控制的更多資訊。

對象的*值*是您存儲的實際內容。它可以是任意序列的位元組。物件值是不可變的，這意味著在上傳物件之後，您無法修改該值。如果要修改物件，則必須在 Amazon S3 之外進行更改，然後重新上傳物件。

物件還包括中繼資料，它是一組名稱值對，可用來存儲有關物件的資訊。您可以將中繼資料（稱為*用戶定義的中繼資料*）分配給 Amazon S3 中的物件。Amazon S3 也可以將系統中繼資料分配給這些物件，用於管理物件。

最後，Amazon S3 還使用子資源來存儲其他物件特定的資訊。



Amazon S3 提供了許多功能，使其成為基於 AWS 構建的許多解決方案的重要組成部分。

首先，它提供*持久性*，以物件平均年度預計損失來衡量。11 個 9 的持久性意味著每年丟失對象的幾率為 0.000000001 個百分點。例如，如果您在 Amazon S3 上存儲 10,000 個物件，則預期平均每 10,000,000 年發生一次物件丟失。Amazon S3 將您的物件冗餘地存儲在您所指定的 Amazon S3 區域內多個設施的多台設備上。Amazon S3 可以快速檢測和修復任何丟失冗餘，從而抵禦同時發生的設備故障。Amazon S3 還定期使用校驗和來驗證您的資料完整性。

Amazon S3 還提供 4 個 9（或 99.99%）的*可用性*。可用性是指您在需要時快速訪問資料的能力。它還提供了幾乎無限的容量來存儲資料，因此它具有*可擴展性*。Amazon S3 具有強大的*安全設置*。它提供了多種方法來控制對所存儲資料的訪問，還允許您對資料進行加密。

最後，Amazon S3 *具有很高的性能*，對於大多數存儲類，第一個位元組的延遲以毫秒為單位。有關 S3 性能設計模式的更多資訊，請參閱 Amazon S3 文檔。常見的方法包括：對頻繁訪問的內容使用緩存；對在短時間內接收大量請求流量的物件使用可配置的重試和超時邏輯；以及在整個網路中橫向擴展和請求並行化以實現高輸送量。

Amazon S3 常見使用模式

Amazon S3

使用 Amazon S3 可以解決哪些問題？
現在，您將考慮一些使用案例。

既然您已經瞭解了 Amazon S3 的許多功能，那麼，如何使用這些功能來滿足您的需求？

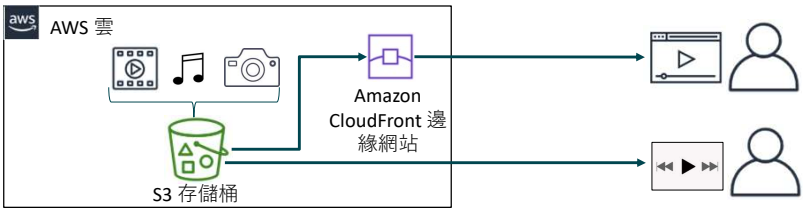
在本模組的這節內容中，您將瞭解四種使用 Amazon S3 作為強大架構解決方案重要組成部分的常見使用案例。

Amazon S3 使用案例 1：
存儲和分發 Web 內容和媒體

構建冗餘、可擴展且高度可用的基礎設施，以便託管要上傳和下載的視頻、照片或音樂。

https://<bucket-name>.s3.amazonaws.com

https://<bucket-name>.s3.amazonaws.com/video.mp4



Amazon S3 的常見使用場景是將其用於*媒體託管*。在此使用案例中，Amazon S3 用於存儲和分發視頻、照片、音樂檔和其他媒體。此內容可以直接從 Amazon S3 交付，因為 Amazon S3 中的每個物件都有唯一的 HTTP URL。

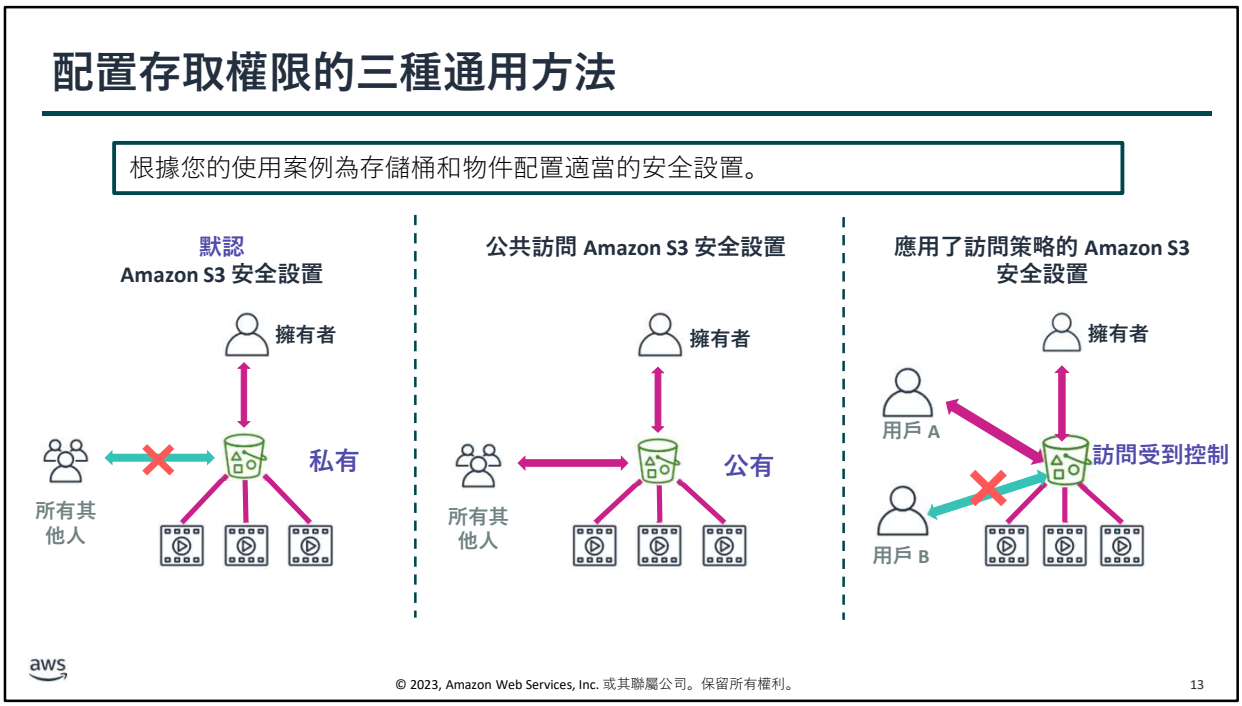
或者，Amazon S3 可以作為內容分發網路 (CDN) 的源存儲，例如 *Amazon CloudFront*。Amazon S3 的彈性使其非常適合託管需要頻寬來應對極端需求峰值的 Web 內容。此外，由於您不需要為 Amazon S3 預置存儲，因此它非常適合託管使用者生成的資料密集型內容（如視頻和照片共用網站）的快速增長的網站。

保護 Amazon S3 存儲桶和物件

- 預設情況下，新創建的 S3 存儲桶和物件均為私有並受保護
- 當使用案例必須共用 Amazon S3 資料時–
  - 管理和控制資料訪問
  - 遵循最低許可權原則
- 用於控制 Amazon S3 資料訪問的工具和選項包括–
  - 阻止公共訪問功能：在新存儲桶上預設啟用，易於管理
  - IAM 策略：用戶可以使用 IAM 進行身份驗證時的理想之選
  - 存儲桶策略：您可以定義對特定物件或存儲桶的訪問
  - 訪問控制列表 (ACL)：傳統存取控制機制
  - S3 接入點：您可以使用特定于每個應用程式的名稱和許可權來配置訪問
  - 預簽名 URL：您可以通過臨時 URL 向其他人授予有時限的存取權限
  - AWS Trusted Advisor 存儲桶許可權檢查：免費功能

預設情況下，所有 S3 存儲桶都是私有的，只能由獲得顯式訪問授權的用戶訪問。管理和控制對 Amazon S3 資料的訪問至關重要。AWS 提供了許多工具和選項，用於控制對 S3 存儲桶或物件的訪問，例如：

- 使用 Amazon S3 阻止公共訪問。這些設置會覆蓋任何其他策略或物件使用權限。為您不希望提供公開存取權限的所有存儲桶啟用阻止公共訪問。此功能提供了一個直接方法來避免意外洩露 Amazon S3 資料。
- 編寫 AWS Identity and Access Management (IAM) 用戶策略，以指定可以訪問特定存儲桶和物件的使用者或角色。
- 編寫存儲桶策略，以確定對特定存儲桶或物件的存取權限。此選項通常在使用者或系統無法使用 IAM 進行身份驗證時使用。存儲桶策略可以配置為授予跨 AWS 帳戶的存取權限，或授予對 Amazon S3 資料的公開或匿名存取權限。如果使用存儲桶策略，應對其進行仔細編寫並全面測試。您可以在存儲桶策略中指定一個拒絕語句來限制訪問。即使用戶具有附加到用戶、基於身份的策略中授予的許可權，訪問也將受到限制。
- 創建 S3 接入點。接入點是唯一的主機名稱，對通過它發出的請求強制執行不同的許可權和網路控制。擁有共用資料集的客戶可以通過創建個性化的接入點，並為每個應用程式定制名稱和許可權，從而擴展對許多應用程式的訪問。
- 針對存儲桶和對象設置存取控制清單 (ACL)。ACL 並不常用（ACL 早於 IAM）。如果您使用 ACL，請勿將存取權限設置得太開放或太寬鬆。
- AWS Trusted Advisor 提供存儲桶許可權檢查功能。這是一款非常實用的工具，可用於發現帳戶中是否有任何存儲桶具有授予全域訪問的許可權。



以下是配置 S3 存儲桶中物件存取權限的三種不同的常見方法。

*左側的場景*顯示了 Amazon S3 的默認安全設置。預設情況下，所有 Amazon S3 存儲桶及其中存儲的物件都是私有（*受保護*）的。只有帳戶管理員和 AWS 根用戶才有權訪問新創建且未經修改的存儲桶。 資源擁有者可以向其他人授予特定的存取權限，但未被授予這些許可權的任何人都將無法訪問。

*中間的場景*顯示了 S3 安全設置已被禁用，任何人都可以公開訪問存儲桶中存儲的物件的情況。

注意！使用 Amazon S3 存儲桶託管靜態網站是快速設置 AWS 架構的一個示例。但是，對於大多數 Amazon S3 使用案例，您不想授予對 Amazon S3 的公共存取權限。 大多數使用案例不需要公共存取權限。 更常見的情況是，您在 Amazon S3 之外運行應用程式，而使用 Amazon S3 來存儲該應用程式所使用的資料，或備份敏感性資料。對於這些常見的使用案例，永遠不應該授予對存儲資料的存儲桶的公共存取權限。

*右側的場景*顯示了 Amazon S3 配置為提供*受控訪問*的情況。使用者 A 被授予了對存儲桶中物件的存取權限，但使用者 B 被拒絕訪問。受控訪問場景很常見。存儲桶擁有者可以通過本模組前面討論過的一個或多個工具或選項來配置這些場景，控制對 Amazon S3 資料的存取權限。

考慮在 Amazon S3 中加密對象

- 加密將使用密鑰對數據進行編碼，使其不可讀
  - 只有具有金鑰的使用者才可對資料解碼
  - 或者，使用 AWS Key Management Service (AWS KMS) 來管理金鑰

- *伺服器端*加密
  - 在存儲桶上，通過選擇 Default encryption（預設加密）選項啟用此功能
  - Amazon S3 會在將物件保存到磁片之前加密物件，並在您下載物件時解密物件

- *用戶端*加密
  - 在用戶端加密資料並將加密的數據上傳到 Amazon S3
  - 在這種情況下，您負責管理加密過程

aws

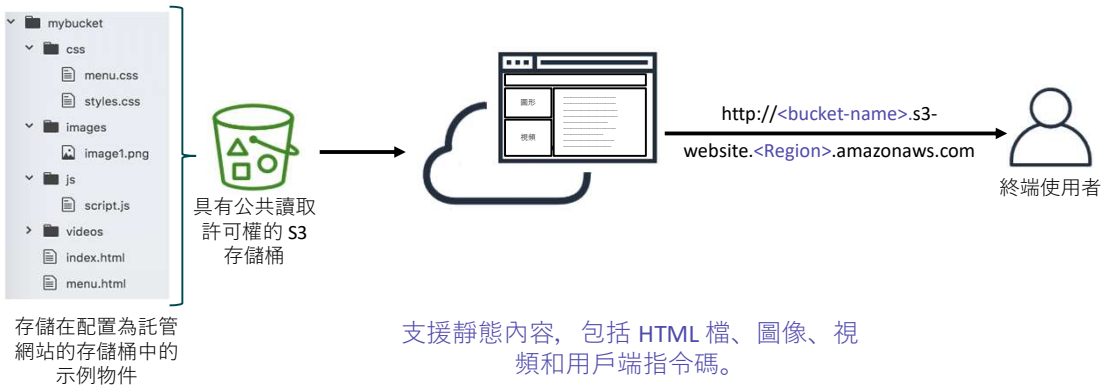
當您的目標是保護數位資料時，資料加密是必不可少的工具。資料加密是對可讀數據進行編碼。如果用戶沒有許可權訪問用於解碼加密資料的金鑰，則無法訪問相關資料。因此，即使攻擊者獲得了對資料的存取權限，他們也無法獲取有價值的資訊。

對於存儲在 Amazon S3 中的資料，您有兩種主要的加密選項。

當您在存儲桶上設置預設加密選項時，它會啟用伺服器端加密。使用此功能，Amazon S3 會在將物件保存到磁片之前加密該物件。然後，Amazon S3 將在您下載物件時對其進行解密。

另一個選項是用戶端加密。使用此方法時，在您將資料上傳到 Amazon S3 之前，您需要先在用戶端對資料進行加密。在這種情況下，您需要管理加密過程、加密金鑰和相關工具。如伺服器端加密一樣，用戶端加密可以幫助減少面臨的風險：通過使用存儲在一個不同機制（而不是存儲資料本身的機制）中的金鑰來加密資料。

Amazon S3 使用案例 2：託管靜態網站



第二個 Amazon S3 使用案例是使用該服務託管靜態網站。在靜態網站上，各個網頁都包含靜態內容，還可能包含用戶端指令碼。

相比之下，*動態*網站依賴伺服器端處理，這可能涉及為回應伺服器端腳本（例如 PHP, JSP 或 ASP.NET）而運行的資料庫查詢。Amazon S3 不支援伺服器端腳本編寫。但是，AWS 還提供其他服務，使您能夠託管動態網站。

要託管*靜態*網站，請為網站託管配置 S3 存儲桶。然後，將您的網站內容上傳到存儲桶。

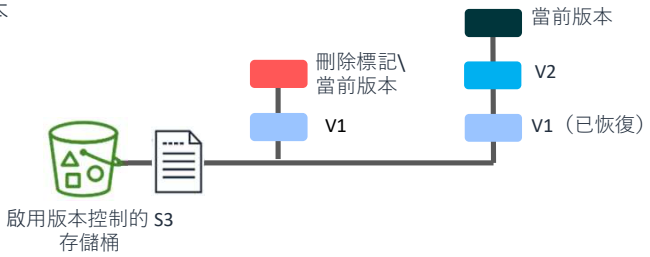
該示例顯示靜態網站可能包含 HTML 檔、圖像、視頻和 JavaScript 等格式的用戶端指令碼。

使用這種方法，您無需運行託管 Web 伺服器的虛擬機器。事實上，您不需要運行伺服器。但是，您仍然可以託管網站。Amazon S3 推出了低成本的 Web 託管解決方案，其中包括高性能、可擴展性和可用性。

Amazon S3 最佳實踐：版本控制

- 防止意外覆蓋和刪除，不會造成任何性能損失
- 每次上傳生成一個新版本
- 允許輕鬆檢索已刪除的對象或回滾到早期版本
- S3 存儲桶的三種可能狀態–

1. *默認*：未啟用版本控制
2. 啟用版本控制
3. 暫停版本控制



Amazon S3 為客戶提供具有高安全性和持久性的存儲基礎設施。版本控制進一步提高了保護等級。它提供了一種在應用程式發生故障或客戶意外覆蓋或刪除物件時恢復資料的方法。

*版本控制*是在相同的存儲桶中保留物件的多個變體的方法。對於 S3 存儲桶中存儲的每個物件，您可以使用版本控制功能來保留、檢索和還原它們的各個版本。

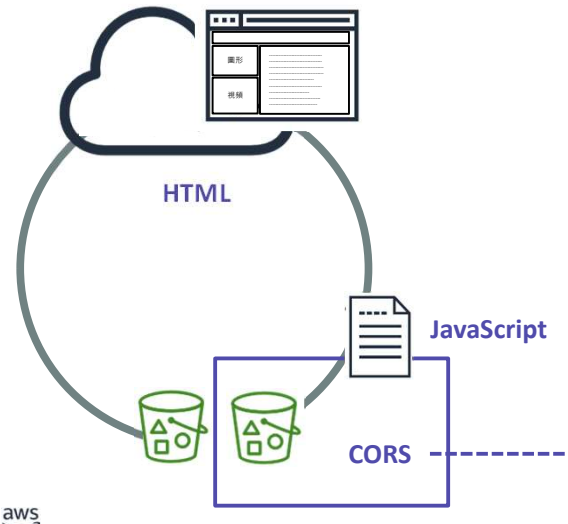
- 如果刪除（而不是永久移除）物件，Amazon S3 會插入一個刪除標記，該標記將成為當前物件的版本。您始終可以還原以前的版本。
- 覆蓋物件會導致在存儲桶中產生一個新的物件版本。您始終可以還原以前的版本。

存儲桶可處於以下三種狀態之一：未啟用版本控制（默認）、啟用版本控制或暫停版本控制。為存儲桶啟用版本控制後，將無法將其更改為未啟用版本控制狀態。但是，您可以暫停該存儲桶的版本控制。

演示：Amazon S3 版本控制

現在，講師可能會選擇使用 AWS 管理主控台演示 Amazon S3 版本控制。

支援跨源資源分享 (CORS)



示例 CORS 配置

```
<CORSConfiguration>
 <CORSRule>

<AllowedOrigin>http://www.example.com</AllowedOrigin>
 <AllowedMethod>PUT</AllowedMethod>
 <AllowedMethod>POST</AllowedMethod>
 <AllowedMethod>DELETE</AllowedMethod>
 <AllowedHeader>*</AllowedHeader>
 <MaxAgeSeconds>3000</MaxAgeSeconds>
 <ExposeHeader>x-amz-server-side-
encryption</ExposeHeader>
 <ExposeHeader>x-amz-request-id</ExposeHeader>
 <ExposeHeader>x-amz-id-2</ExposeHeader>
 </CORSRule>
</CORSConfiguration>
```

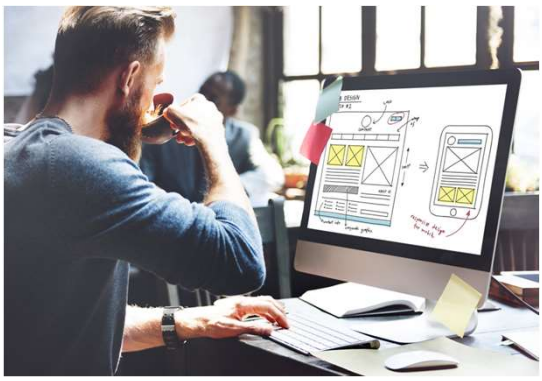

跨源資源分享 (CORS) 為在一個域中載入的用戶端 Web 應用程式定義了一種與另一個域中的資源進行交互的方法。借助 CORS 支援，您可以使用 Amazon S3 構建豐富的用戶端 Web 應用程式，並有選擇地允許跨源訪問 Amazon S3 資源。

要將您的存儲桶配置為允許跨源請求，您可以創建 CORS 配置。CORS 配置是一個 XML 文檔，其中包含識別以下內容的規則：

- 允許訪問您的存儲桶的源。
- 每個源支援的操作（HTTP 方法）。在本例中，PUT、POST 和 DELETE 請求來自 http://www.example.com，可以使用 Amazon Route 53 將其配置到另一個 S3 存儲桶。
- 其他特定於操作的資訊。

有關 CORS 的更多資訊，請參閱跨源資源分享 (CORS) AWS 文檔。

模組 3 – 指導實驗：託管靜態網站



您現在將完成模塊 3 – 指導實驗：託管靜態網站。

指導實驗：任務

1. 在 Amazon S3 中創建存儲桶
2. 將內容上傳到存儲桶
3. 允許訪問對象
4. 更新網站

在本指導實驗中，您將完成以下任務：

1. 在 Amazon S3 中創建存儲桶
2. 將內容上傳到存儲桶
3. 允許訪問對象
4. 更新網站

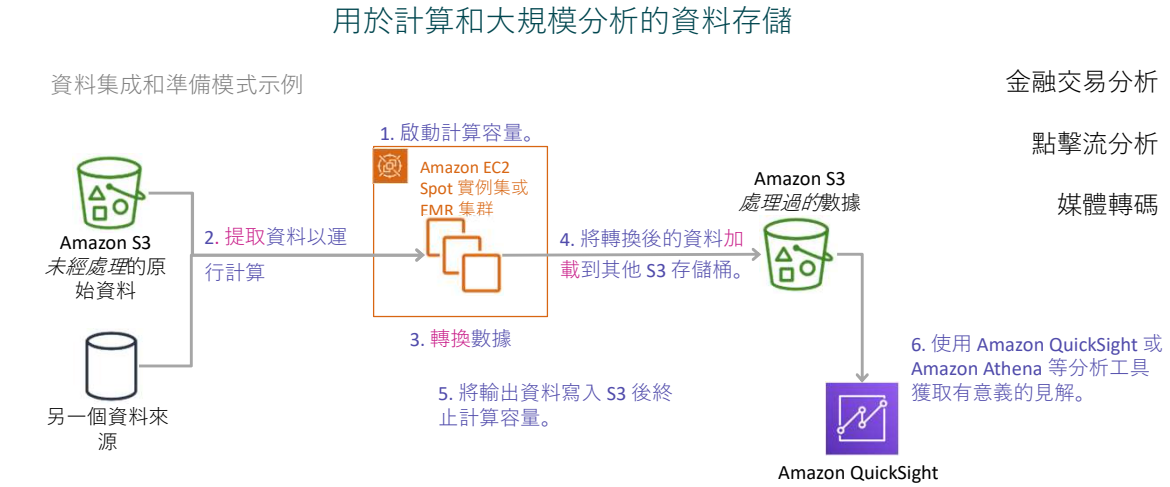
大約 20 分鐘

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。

Amazon S3 使用案例 3：
用於計算和分析的資料存儲



您還可以將 Amazon S3 用作資料存儲進行計算或大規模分析，如金融交易分析、點擊流分析和媒體轉碼。Amazon S3 可以支援這些工作負載，因為它可以橫向擴展，從而實現多個併發事務。

在此示例中，當 Spot 實例的出價較低時，或當 Amazon EMR 集群啟動時，Amazon Elastic Compute Cloud (Amazon EC2) Spot 實例集就會啟動。無論如何，在計算容量可用之後，將從 Amazon S3 以及從另一個資料來源中提取*未經處理的原始*數據。資料通過集成和轉換資料的計算演算法運行。生成的*處理*資料將載入到其他 Amazon S3 存儲桶中。現在資料已處理完畢，計算容量將終止以節省成本。最後，可能會使用 Amazon QuickSight 等分析工具從處理的資料中獲取有意義的見解。這只是 Amazon S3 如何在大規模分析解決方案架構中為資料存儲發揮重要作用的示例場景之一。

Amazon S3 使用案例 4：備份和歸檔關鍵資料

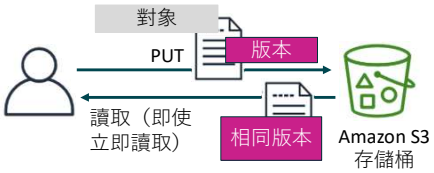
在本模組討論的第四個也是最後一個使用案例中，Amazon S3 被用作資料備份解決方案。由于具備高持久性和可擴展性，Amazon S3 適合作為資料備份和歸檔工具。

在這種情況下，資料是從本地部署企業資料中心以及大量 Amazon EC2 伺服器備份的。這些伺服器運行生成資料的應用程式。

此外，您可以將長期資料從 Amazon S3 Standard 存儲移動到 Amazon Simple Storage Service Glacier。本模組稍後將進一步詳細討論此過程。您可以在存儲桶上配置另一個 Amazon S3 選項以實現更高的持久性，這就是*跨區域複製*。在跨區域複製中，上傳到一個區域中的存儲桶的物件將自動複製到其他區域中的其他 S3 存儲桶。

Amazon S3 資料一致性模型

- Amazon S3 對所有區域中的所有新的和現有的*對象*都具有**強一致性**
  - 為 S3 存儲桶中物件的所有 GET、LIST 和 PUT 操作提供先寫後讀一致性
  - 一致性模型為大資料工作負載提供了優勢
- 存儲桶配置具有最終一致的模型



許多客戶開發的大資料分析應用程式都使用 Amazon S3 進行物件存儲。這些應用程式通常需要在寫操作之後立即訪問物件。在 2020 年 12 月之前，Amazon S3 在所有區域為覆蓋 PUTS 和 DELETES 提供最終一致性。不過，Amazon S3 現在對所有 AWS 區域的所有新的和現有的 S3 物件都具有很強的一致性。

Amazon S3 通過在 AWS 資料中心的多台伺服器之間複製資料來實現高可用性。如果 PUT 請求成功，資料將被安全存儲。在 PUT 回應成功後啟動的任何讀取（GET 或 LIST）都將返回 PUT 寫入的資料。這種先寫後讀強一致性自動存在于所有應用程式中，不會影響性能或可用性。

借助強一致性，無需為支援應用程式而進行更改，從而簡化了本地部署分析工作負載的遷移。也無需額外的基礎設施（如 S3Guard）來提供強一致性。

雖然物件具有強一致性，但 Amazon S3 存儲桶配置具有最終一致性模型。例如，如果刪除一個存儲桶並立即列出所有存儲桶，則已刪除的存儲桶可能仍會出現在列表中。不過，在短時間內，如果再次運行 list bucket 命令，已刪除的存儲桶將不再出現在 list buckets 結果中。

有關詳細資訊，請閱讀 Amazon S3 強一致性文檔。

第 2 節要點

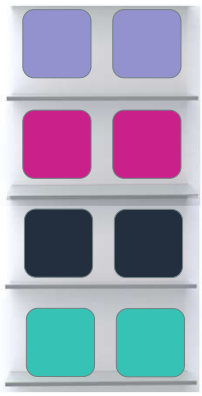
- 存儲桶必須具有全域唯一名稱，並在區域級別定義
- 存儲桶默認是私有的，處於受保護狀態
- Amazon S3 安全性可以通過 IAM 策略、存儲桶策略、存取控制清單、S3 接入點和預簽名 URL 進行配置
- Amazon S3 對所有區域中的所有新物件和現有物件都具有很強的一致性
- 單個對象的最大大小為 5 TB
- Amazon S3 通常用作計算和分析的資料存儲，以及關鍵資料的備份和歸檔服務

本模組中這節內容的要點包括：

- 存儲桶必須具有全域唯一名稱，並在區域級別定義
- 存儲桶預設是私有的，處於受保護狀態
- Amazon S3 安全性可以通過 IAM 策略、存儲桶策略、存取控制清單、S3 接入點和預簽名 URL 進行配置
- Amazon S3 對所有區域中的所有新物件和現有物件都具有很強的一致性
- 5 TB 是單個對象的最大大小，但是您可以存儲幾乎無限的物件
- Amazon S3 通常用作計算和分析的資料存儲，以及關鍵資料的備份和歸檔服務

介紹第 3 節：在 Amazon S3 中存儲資料。

Amazon S3 和 Amazon S3 Glacier 存儲類



S3 Standard：
經常訪問的資料

S3 Standard IA：
長時間存在的、不經常訪問的資料

S3 One Zone IA：
長時間存在的、不經常訪問的、非關鍵資料

Amazon S3 Glacier 或 Deep Archive：
很少訪問的歸檔資料

Amazon S3 Intelligent Tiering
根據資料訪問模式，自動在存儲類之間移動物件。

有關 Amazon S3 存儲類的詳細資訊，請參閱 https://aws.amazon.com/s3/storage-classes/。

現在您已經使用 Amazon S3 構建了網站，下面是不同 Amazon S3 存儲類及其特性的比較。

S3 Standard 為頻繁訪問的資料提供高持久性、可用性和高性能的物件存儲。S3 Standard 提供較低的延遲和較高的輸送量，因此非常適合各種使用案例，包括雲應用程式、動態網站、內容分發、移動和遊戲應用程式以及大資料分析。它提供了至少三個可用區的持久性。

S3 標準 - 不頻繁訪問存儲 (S3 Standard-IA) 具有 Amazon S3 Standard 的所有優勢，但它在不同的成本模型上運行以存儲不經常訪問的資料，例如較舊的數位圖像或較舊的日誌檔。對於放置在其中的任何資料，都需要收取 30 天的最低存儲費，而且從 S3 Standard-IA 檢索資料的成本也高於從 S3 Standard 存儲中檢索資料的成本。

S3 One Zone-IA 將資料存儲在單個可用區內。它非常適合想要使用較低費用選項並且不需要 S3 Standard 或 S3 Standard-IA 的可用性和彈性的客戶。如果用於存儲本地部署資料的輔助備份副本或可輕鬆重新創建的資料，它是一個很好的選擇。您還可以將其用作從另一個 AWS 區域複製的資料的經濟高效存儲。

S3 Intelligent-Tiering 旨在通過自動將資料轉移到最經濟高效的訪問層來優化成本，而不會影響性能，也不會產生運營開銷。只需針對每個對象收取小額月度監控和自動化費用，Amazon S3 會監控 S3 Intelligent-Tiering 中物件的訪問模式。它將連續 30 天未訪問的對象移動到不頻繁訪問層。如果不頻繁訪問層中的某個物件被訪問，即會自動將該對象移回頻繁訪問層。在使用 S3 Intelligent-Tiering 時不收取檢索費用，並且在各層之間移動物件時不收取額外的分層費用。

Amazon S3 Glacier 是一種安全、持久且成本低的存儲類，可用於資料歸檔。您可以放心存儲任意數量的資料，成本與本地部署解決方案相當，甚至更低。為了保持低成本，但適合不同的需求，您有三種檢索資料的選擇，存取時間和成本各不相同：

- 加速檢索通常在 1 到 5 分鐘內完成

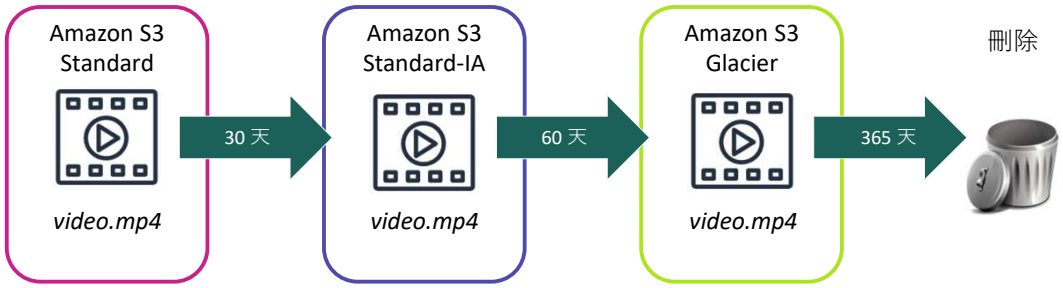
- 標准檢索通常在 3 到 5 小時內完成
- 批量檢索通常在 5 到 12 小時內完成

Amazon S3 Glacier Deep Archive 是 Amazon S3 最低成本的存儲類。它支持長期保留和數位化保存一年中可能被訪問一兩次的資料。資料至少存儲在三個地理位置分散的可用區中，受到 11 個 9（99.999999999%）的持久性保護，可在 12 小時內恢復。

有關 Amazon S3 存儲類的更多詳細資訊，請參閱 AWS 文檔。

Amazon S3 **生命週期策略**

配置 **Amazon S3 生命週期策略**可根據時間來刪除或移動物件。



您可以配置物件的生命週期，以管理物件在整個生命週期中的存儲方式。**生命週期配置**是一組規則，用於定義 Amazon S3 對一組物件應用的操作。

設置 S3 生命週期策略之後，無需更改您的應用程式，*您的資料將自動傳輸到不同存儲類*。

利用生命週期策略，您可以讓資料在不同的 Amazon S3 存儲類型之間定期迴圈。這種迴圈可降低總體成本，因為隨著時間的推移，資料的重要性會降低，因此支付的資料費用也會減少。除了可以針對物件設置生命週期規則外，您還可以針對存儲桶設置生命週期規則。

有關物件生命週期管理的更多詳細資訊，請參閱對象生命週期管理 AWS 文檔。

Amazon S3 成本

僅按實際用量付費，包括：
存儲的物件的 GB（每月）。每個*區域*和每個*存儲類*的定價不同。
傳出到其他區域或互聯網。
PUT、COPY、POST、LIST、GET、SELECT、生命週期轉換、資料檢索請求。

以下服務免費：
資料從互聯網傳入到 Amazon S3。
在同一 AWS 區域內的 S3 存儲桶之間或從 Amazon S3 傳輸到同一 AWS 區域內的任何服務。
傳出到 Amazon CloudFront。
DELETE 和 CANCEL 請求。

使用 Amazon S3 時，您只需為實際使用量付費。沒有最低收費。選擇最適合您資料資料的 Amazon S3 存儲類時，您需要考慮四項：存儲定價、請求和資料檢索定價、資料傳輸和傳輸加速定價以及資料管理功能定價。

有關 Amazon S3 定價的詳細資訊，可以在 Amazon S3 定價中找到。

第 3 節要點

- Amazon S3 存儲類包括–
  - S3 Standard
  - S3 Standard-IA
  - S3 One Zone-IA
  - S3 Intelligent-Tiering
  - S3 Glacier
  - S3 Glacier Deep Archive
- Amazon S3 生命週期策略可以根據時間刪除物件或將物件移動到較便宜的存儲類
- 資料傳輸從互聯網傳入 Amazon S3 是免費的，但是傳輸到其他區域或互聯網需要付費

本模組中這節內容的要點包括：

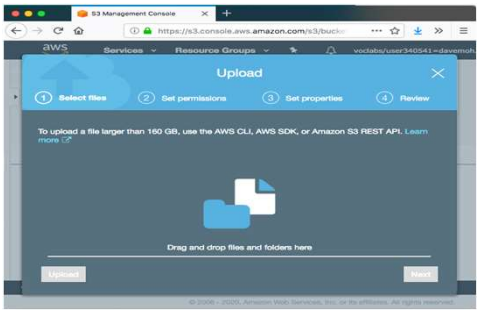
- Amazon S3 存儲類包括 – S3 Standard、S3 標準 - 不頻繁訪問存儲、S3 One Zone-不頻繁訪問存儲、S3 Intelligent-Tiering、S3 Glacier 和 S3 Glacier Deep Archive
- Amazon S3 生命週期策略可以根據時間刪除物件或將物件移動到較便宜的存儲類
- 數據傳輸從互聯網傳入 Amazon S3 是免費的，但是傳輸到其他區域或互聯網需要付費

介紹第 4 節：將數據移入和移出 Amazon S3。

將對象移動到 Amazon S3

AWS 管理主控台

使用流覽器上傳或下載。



AWS 命令列介面

從終端命令提示符或腳本的調用中上傳或下載。

- 上傳命令示例：

```
$aws s3 cp test.txt \
s3://AWSDOC-EXAMPLE-BUCKET/test.txt
```

AWS 工具和 SDK

使用 AWS 工具或 SDK 以程式設計方式移動物件。

在本模組前面的指導實驗中，您使用 AWS 管理主控台提供的 Web 流覽器介面將文件上傳到 Amazon S3。這是將數據移入或移出 Amazon S3 的最簡單方法。它提供了一種基於嚮導的方法，其中包括將要複製的檔拖放到存儲桶中的選項。

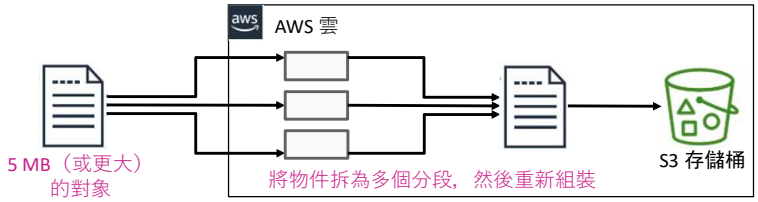
在模組的這節內容中，您將瞭解一些其他選項，這些選項可用於將資料移入和移出 Amazon S3。

其中兩個選項包括使用 AWS 命令列介面 (AWS CLI) 或 AWS SDK。

下面的示例顯示了 AWS CLI 上傳命令。在命令中，您指定 *aws* 調用 AWS CLI，然後指定服務，即 *S3*。接下來，您發出一個 *cp*（或 copy）子命令，後跟 *test.txt*，這是要複製的本地檔（存在於您的電腦上）。最後，*s3://AWSDOC-EXAMPLE-BUCKET/test.txt* 參數指示應上傳檔的存儲桶，以及應存儲物件值（內容）的鍵 (*AWSDOC-EXAMPLE-BUCKET/test.txt*)。

S3 AWS CLI 命令參考提供了更多詳細資訊。

分段上傳



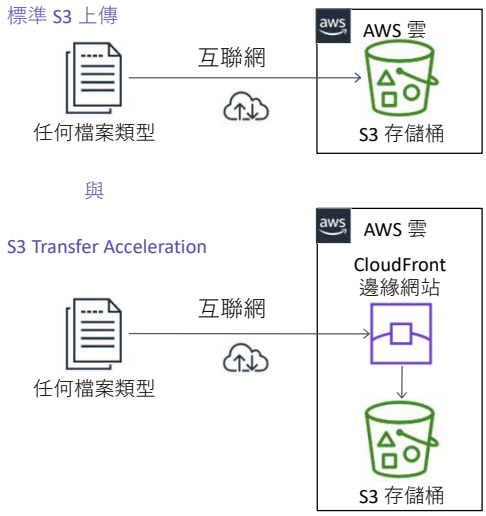
- 檔可以使用分段上傳 API 進行上傳
  - 您可以將單個物件分段進行上傳
  - 每個分段都是物件資料的連續部分
  - 上傳完物件的所有分段後，Amazon S3 將彙集這些分段並創建物件
- 通常只用於大於 100 MB 的文件
- 優點–
  - 快速從網路問題中恢復：如果任何分段傳輸失敗，只需重新傳輸該分段
  - 能夠暫停和恢復對象上傳
  - 提高輸送量：並行上傳分段以提高輸送量

分段上傳 API 可讓您通過可控的分段來持續上傳大型對象。優勢包括：

- 提高輸送量 – 您可以並行上傳各個分段以提高輸送量。
- 從任何網路問題快速恢復 – 較小的各個分段可以最大限度地減少因網路錯誤而重新開機失敗上傳的影響。
- 暫停和恢復物件上傳 – 您可以用一段時間來上傳物件分段。啟動分段上傳後，就不會過期。您必須明確完成或停止分段上傳。
- 在您知道物件的最終大小前開始上傳 – 您可以在創建物件時就將其上傳。
- 上傳大型物件 – 您可以使用分段上傳 API 來上傳高達 5 TB 的大型對象。

請注意，檔的大小必須至少為 5 MB 才能使用分段上傳功能。

Amazon S3 Transfer Acceleration



- 加快 Amazon S3 資料傳輸
- 使用優化的網路通訊協定和 AWS 邊緣基礎設施
- 典型的速度改善：
  - 跨國傳輸較大物件的速度可提高 50-500%
  - 在某些情況下可以更高
- Amazon S3 Transfer Acceleration 速度比較工具*
  - 顯示獲得的速度優勢（按區域）

* 有關更多資訊，請參閱 http://s3-accelerate-speedtest.s3-accelerate.amazonaws.com/en/accelerate-speed-comparsion.html。

Amazon S3 Transfer Acceleration 利用分佈在全球的 Amazon CloudFront 和 AWS 邊緣網站，快速、輕鬆地將資料傳輸到 S3 存儲桶。隨後資料將通過經過優化的網路路徑路由至 Amazon S3。

適合使用 Transfer Acceleration 的場景：
- 您位於全球各地的客戶需要上傳到一個集中的存儲桶
- 您定期跨大洲傳輸 GB 或 TB 級的資料
- 通過互聯網將文件上傳到 Amazon S3 時對可用頻寬的利用率不足

演示：
S3 Transfer Acceleration

現在，講師可能會選擇演示 S3 Transfer Acceleration 工具。

將大量資料移動到 Amazon S3：AWS Snowball

AWS Snowball

AWS Snowball
PB 級資料傳輸

- 可以將數 TB 的數據傳入或傳出 Amazon S3
  - 可以使用多個設備來傳輸 PB 級數據
- 解決了對大型資料傳輸的擔憂（網路成本、傳輸時間、安全性）
  - *示例*：要以 10 Gbps 的上傳速度在互聯網上傳輸 10 PB（1000 萬 GB）資料，將需要 100 天以上的時間
- 使用方法–
  - 在 AWS 管理主控台中創建一項任務，然後等待 Snowball 設備送達。
  - 連接到本地網路，然後下載並運行 Snowball 用戶端
  - 選擇要傳輸（加密）到設備的檔目錄
  - 運回設備並跟蹤狀態

AWS Snowball 是一種 PB 級資料傳輸方案，您無需編寫任何代碼或購買任何硬體即可傳輸資料。您只需在 AWS 管理主控台中創建一個任務，我們就會將 Snowball 設備運送給您。只需將設備接入您的本地網路，然後直接將檔案傳輸到設備上。然後，將設備運回並跟蹤貨物狀態。資料到達安全的 Amazon 設施後，資料將被傳輸到您的 AWS 帳戶中。

將大量資料移動到 Amazon S3：AWS Snowmobile

AWS Snowmobile
EB 級資料傳輸

AWS Snowmobile

- 一個 45 英尺長（13.7 米）的運輸集裝箱，由半掛卡車牽引
- 每個 Snowmobile 最多可以傳輸 100 PB
- 提供多層安全保護–
  - 專門的安保人員
  - GPS 跟蹤、警報監控、全天候視頻監控
  - 運輸過程中可選配護送安保車
  - 數據采用 256 位加密金鑰進行加密

AWS Snowmobile 是更大的資料傳輸方案，可傳輸 EB 級的資料。1 EB 相當於 100 萬 TB 或 10 億 GB。它只用於將極大量的資料移轉到 AWS。Snowmobile 是一種堅固的運輸容器，長達 45 英尺（13.7 米），由半掛式卡車牽引。每個 Snowmobile 可以傳輸 100 PB 資料。

如果嘗試在互聯網上傳輸 100 PB 的資料，上傳速度為 10 Gbps（假設 TCP/IP 開銷為 10%），則需要大約 1018 天（近三年）才能完成資料上傳。這不切實際。在這種情況下，使用 AWS Snowmobile 傳輸資料將是更好的選擇。

Snowmobile 採用多層安全防護措施，力保您的資料安全，這些措施包括：專門的安保人員、GPS 跟蹤、警報監控、全天候視頻監控，並且在運輸過程中可選配護送安保車。所有資料都使用 256 位加密金鑰進行加密，金鑰可通過 AWS Key Management Service (AWS KMS) 管理，這樣可確保您的資料安全並形成完整的監管鏈。

第 4 節要點

- 對於大於 100 MB 的檔以及網路連接可能不穩定的情況，S3 分段上傳選項是一個不錯的選擇
- Amazon S3 Transfer Acceleration 使用邊緣網站，可以顯著提高上傳速度
- AWS Snowball 提供了一種傳輸 *PB 級*數據的方法，AWS Snowmobile 提供了一種將 *EB 級*數據傳輸到 AWS 的方法

本模組中這節內容的要點包括：

- 對於大於 100 MB 的檔以及網路連接可能不穩定的情況，S3 分段上傳選項是一個不錯的選擇
- Amazon S3 Transfer Acceleration 使用邊緣網站，可以顯著提高上傳速度
- AWS Snowball 提供了一種傳輸 PB 級數據的方法，而 AWS Snowmobile 提供了一種將 EB 級資料傳輸到 AWS 的方法

介紹第 5 節：為您的架構選擇區域。

選擇區域：合規性和延遲注意事項

- 數據屬地和監管合規
  - 是否有相關的區域數據隱私法？
  - 客戶資料可以存儲在該國家/地區之外嗎？
  - 您能否滿足監管要求？

- 使用者與資料之間的距離
  - 延遲方面的細微差異可能會影響客戶體驗
  - 選擇離用戶最近的區域

在決定將資料託管到哪個區域時，需要考慮很多因素。

首先，您應該考慮*數據隱私法*和監管合規要求。您在 AWS 上存儲的資料需要遵守資料存儲地的國家/地區法律和地方性法規。此外，一些法律規定，如果您在其司法管轄區內經營業務，則不得將相關資料存儲到其他地方。與此類似的是，*合規性標準*（例如《美國健康保險流通與責任法案》(HIPAA)）也對資料的存儲方式和位置提出了嚴格要求。

其次，*距離*是在選擇區域時的一個重要因素，尤其是當*延遲*對您來說非常重要時，更是如此。大多數情況下，選擇最近的區域和選擇最遠的區域，這兩者之間的延遲差異是相對較小的，但即使是細微的延遲差異，也會影響客戶體驗。客戶需要回應迅捷的環境，而且隨著時間推移，技術變得越來越強大，客戶的這種期望也越來越強烈。

選擇區域：服務可用性和成本注意事項

- 服務和功能可用性
  - 並非所有的 AWS 服務都能在任何區域中提供
    - 請參閱 AWS 區域表瞭解詳細信息
    - 服務會定期擴展到新的區域
  - 可以跨區域使用某些服務，但會增加延遲

- 成本效益
  - 成本因區域而異
  - 某些服務（如 Amazon S3）針對傳出資料收費
  - 考慮在其他區域內複製整個環境的成本效益

選擇區域時，第三個重要的考慮因素是 AWS 服務和功能的可用性。雖然 AWS 一直努力讓其服務和功能在所有區域可用，但由於業務遍佈全球而導致的複雜性使得實現這個目標非常困難。我們的服務在準備就緒時會先在部分區域發佈，然後儘快推向其他區域，而不是等到所有區域都可用才發佈。

選擇區域時的第四個考慮因素是成本。服務費用因使用服務的區域不同而異。例如，在 us-east-1 區域中運行 Amazon EC2 實例的費用可能與在 eu-west-1 區域中運行的費用不同。通常，成本差異可能不足以取代其他三個考慮因素。然而，如果區域之間在延遲、合規性或服務可用性方面的差異很小，則可以通過為您的環境使用成本較低的區域來節省資金。

最後，如果您的客戶位於全球的不同地區，可以考慮將您的環境複製到多個離他們較近的區域，以優化客戶體驗。因為，這樣您就可以將負載分配到多個環境中，每個環境中的元件成本就會降低，即使您添加更多基礎設施也沒問題。例如，添加第二個應用程式環境可能會讓您在每個環境中的處理和存儲容量要求都降低一半。AWS 旨在為您提供這種靈活性，而且您只需按實際用量付費，因此您可以將現有環境縮減，用節約下來的費用來添加另一個環境。

這種方法的缺點是，您現在需要管理兩個環境。此外，並非所有組件都能縮減，並且縮減量足以彌補新組件的所有成本。此外，您可能需要在一個區域中維護一個單一存儲“真實資料來源”，例如主 Amazon Relational Database Service (Amazon RDS) 實例。您的輔助區域需要與存儲實例進行通信，這可能會增加這些操作的延遲和成本。

模組 3 – 挑戰實驗：為咖啡館創建靜態網站

您現在將完成模塊 3 – 挑戰實驗：為咖啡館創建靜態網站。

業務需求：一個簡單的網站

Sofía 曾向 Nikhil 提到過，她想要的網站能夠以圖片展示咖啡館的氛圍，並為顧客提供詳細的業務資訊。

Frank 喜歡網站的想法。他一直在拍照，可以用來突出咖啡館的功能表項目目。

Sofía 向 Nikhil 提到過，她想要的網站能夠以圖片展示咖啡館的氛圍。該網站還應向客戶提供業務詳細資訊，例如商店的位置、營業時間和電話號碼。

Nikhil 很高興為咖啡館創建第一個網站。在本活動中，您將扮演 Nikhil，努力打造出咖啡館的每個人都期待您能帶來的結果。也許您還能超出他們的預期！

挑戰實驗：任務

1. 提取此實驗所需的檔
2. 創建 S3 存儲桶來託管靜態網站
3. 將內容上傳到 S3 存儲桶
4. 創建存儲桶策略以授予公共讀取存取權限
5. 為 S3 存儲桶啟用版本控制
6. 設置生命週期策略
7. 啟用跨區域複製

在本挑戰實驗中，您將完成以下任務：

1. 提取此實驗所需的檔
2. 創建 S3 存儲桶來託管靜態網站
3. 將內容上傳到 S3 存儲桶
4. 創建存儲桶策略以授予公共讀取存取權限
5. 為 S3 存儲桶啟用版本控制
6. 設置生命週期策略
7. 啟用跨區域複製

挑戰實驗：最終產品

http://<bucket-name>.s3-website-<region>.amazonaws.com

在本挑戰實驗中，您將為咖啡館創建一個靜態網站。該網站將託管在 Amazon S3 上。創建 S3 存儲桶並正確配置用於託管網站後，Web 流覽器應該能夠使用指定的 Amazon S3 終端節點 URL 直接訪問網站。

內容說明：架構圖顯示了兩個區域，每個區域都有一個 S3 存儲桶。一個 S3 存儲桶指向咖啡館的網站。http://<bucket-name>.s3-website-<region>.amazonaws.com。**內容說明結束。**

大約 60 分鐘

現在可以開始挑戰實驗了。

挑戰實驗總結：要點

完成這個挑戰實驗之後，您的講師現在可能會帶您討論此挑戰實驗的要點。

現在該複習本模組，並完成最後的知識考核和對實踐認證考試問題的討論了。

模組總結

總的來說，在本模組中，您學習了如何：

- 識別 Amazon Simple Storage Service (Amazon S3) 可以解決的問題
- 描述如何使用 Amazon S3 高效存儲內容
- 瞭解各種 Amazon S3 存儲類和成本注意事項
- 描述如何將資料移入和移出 Amazon S3
- 描述如何選擇區域
- 創建靜態網站

總的來說，在本模組中，您學習了如何：
- 識別 Amazon Simple Storage Service (Amazon S3) 可以解決的問題
- 描述如何使用 Amazon S3 高效存儲內容
- 瞭解各種 Amazon S3 存儲類和成本注意事項
- 描述如何將資料移入和移出 Amazon S3
- 描述如何選擇區域
- 創建靜態網站

完成知識考核

現在該完成本模組的知識考核了。

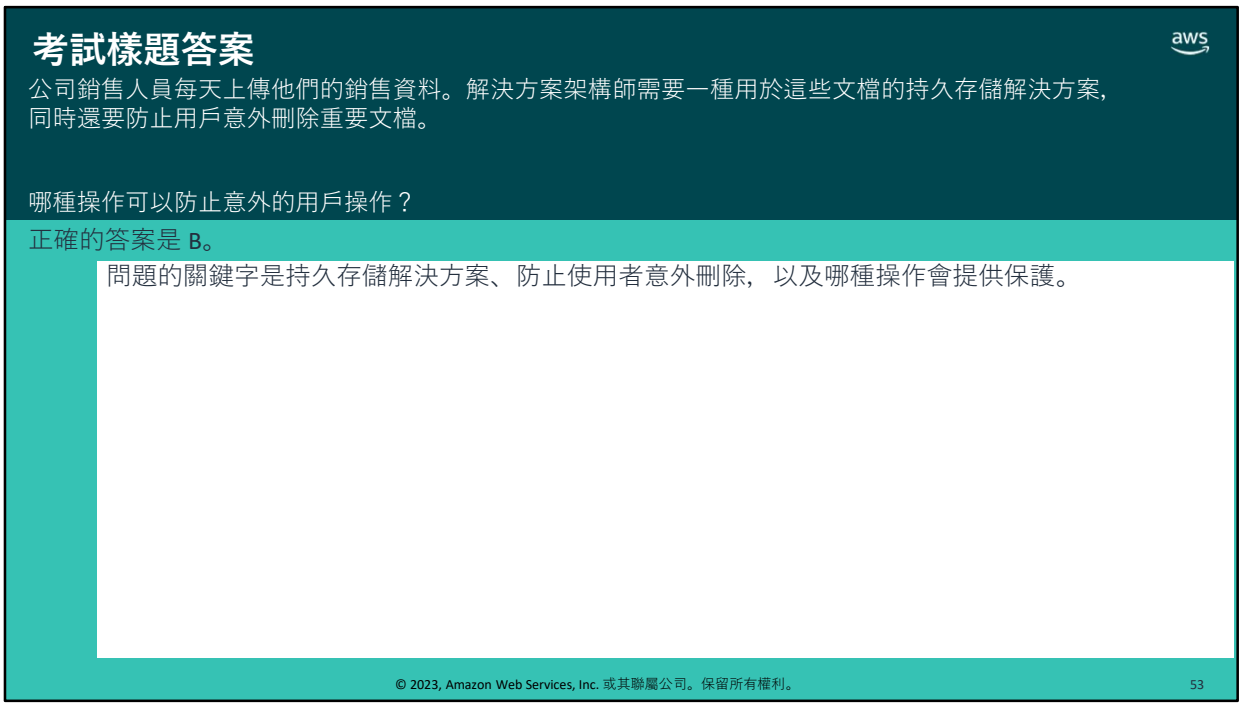
考試樣題

公司銷售人員每天上傳他們的銷售資料。解決方案架構師需要一種用於這些文檔的持久存儲解決方案，同時還要防止用戶意外刪除重要文檔。

哪種操作可以防止意外的用戶操作？

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

思考答案選項，並根據關鍵字排除錯誤選項。



以下是要識別的關鍵字：持久存儲解決方案、防止使用者意外刪除，以及哪種操作會提供保護。

正確答案是 B。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。

錯誤的答案：
選項 A 將丟失自上一個快照以來提交的任何更改。將資料存儲在兩個 S3 存儲桶中（選項 C）提供的保護稍好一些，但用戶仍然可以從兩個存儲桶中刪除物件。EC2 實例存儲（選項 D）是臨時存儲，永遠不應用于需要持久性的資料。

其他資源

- Amazon S3 開發人員指南
- Amazon S3 常見問題
- Amazon S3 常見使用場景
- AWS 存儲服務白皮書
- Amazon S3 存儲類比較
- Amazon S3 阻止公開訪問

如果您想進一步瞭解本模組中涵蓋的主題，以下額外資源可能會對您有所幫助：

- Amazon S3 開發人員指南
- Amazon S3 常見問題
- Amazon S3 常見使用場景
- AWS 存儲服務白皮書
- Amazon S3 存儲類比較
- Amazon S3 阻止公開訪問

感謝您完成本模組的學習。