

實驗室 1：Amazon Simple Storage Service (Amazon S3) 簡介

實驗室概觀和目標

此實驗室使用 AWS Management Console 讓您了解 Amazon Simple Storage Service (Amazon S3) 的基本功能。

Amazon S3 是物件儲存服務，提供領先業界的可擴展性、資料可用性、安全和效能。這表示來自各種產業及所有規模的客戶，可在各種使用案例中利用此服務來存放和保護任意數量的資料，例如網站、行動應用程式、備份和還原、封存、企業應用程式、物聯網 (IoT) 裝置及大數據分析。Amazon S3 提供易於使用的管理功能，讓您可以組織資料和設定微調的存取控制，以符合特定的商業、組織和合規要求。Amazon S3 的設計可達到 99.999999999% (11 個 9) 的耐久性，並可為全世界的公司存放數百萬個應用程式的資料。

完成此實驗室之後，您將了解如何執行以下作業：

- 在 Amazon S3 建立儲存貯體
- 將物件新增至儲存貯體
- 管理物件和儲存貯體的存取許可
- 建立儲存貯體政策
- 使用儲存貯體版本控制

持續時間

此實驗室需要大約 **60 分鐘** 的時間來完成。

AWS 服務限制

在此實驗室環境中，AWS 服務和服務動作的存取可能會限定於完成實驗室指示所需的範圍內。如果您嘗試存取其他服務，或執行本實驗室中所述動作以外的動作，則可能會遇到錯誤。

存取 AWS Management Console

1. 在這些指示的上方，選擇 **Start Lab** (啟動實驗室) 來啟動實驗室。

Start Lab (啟動實驗室) 面板會隨即開啟，並顯示實驗室狀態。

提示：如果您需要更多時間來完成實驗室，請再次選擇 **Start Lab** (啟動實驗室) 按鈕，以重新啟動環境的計時器。

2. 等到您看到 **Lab status: ready** (實驗室狀態：就緒) 的訊息，即可選擇 **X** 來關閉 **Start Lab** (啟動實驗室) 面板。

3. 在這些指示的上方，選擇 **AWS**

這會在新的瀏覽器標籤中開啟 AWS Management Console。系統會自動將您登入。

提示：如果新的瀏覽器標籤未開啟，瀏覽器頂端通常會顯示橫幅或圖示，並顯示瀏覽器阻止網站開啟快顯視窗的訊息。選擇橫幅或圖示，然後選擇 **** Allow pop ups**** (允許快顯視窗)。

4. 排列 **AWS Management Console** 標籤，使其顯示在這些指示旁邊。在理想情況下，您可以同時看到兩個瀏覽器標籤，以便您可以更輕鬆地遵循實驗室的步驟。

任務 1：建立儲存貯體

您剛開始接觸 Amazon S3，並且想在設定存放 Amazon Elastic Compute Cloud (Amazon EC2) 報告資料的環境時，測試 Amazon S3 的功能和安全性。您知道 Amazon S3 中的每個物件都儲存在儲存貯體中，因此任務清單中的第一件事就是建立新儲存貯體以存放報告。

在此任務中，您會建立儲存貯體來存放 Amazon EC2 報告資料，然後檢查不同的儲存貯體組態選項。

5. 在 AWS Management Console 左上方的 **Services** (服務) 選單上，選擇 **S3**。
6. 選擇 **Create bucket** (建立儲存貯體)

i 儲存貯體名稱的長度必須是 3-63 個字元，且只能包含小寫字母、數字或連字號。無論帳戶或區域為何，儲存貯體名稱在 Amazon S3 中必須為全域唯一，而且您在建立儲存貯體之後無法變更儲存貯體名稱。當您輸入儲存貯體名稱時，若有違反命名規則的話，會出現對應的說明方塊。如需詳細資訊，請參閱此實驗室最後**其他資源**部分的 Amazon S3 儲存貯體命名規則。

7. 在 **General configuration** (一般組態) 區段中，輸入以下做為 **Bucket name** (儲存貯體名稱)：`reportbucket(NUMBER)`

在儲存貯體名稱中，將 **(NUMBER)** 取代為隨機數字，使您的儲存主體具有唯一的名稱。

- 範例儲存貯體名稱：`reportbucket987987`

讓 **Region** (區域) 保留預設值。

藉由選取一個特定區域，您可以最佳化延遲、將成本降至最低或遵守法規要求。除非您明確將存放在區域中的物件傳輸到其他區域，否則它們絕不會離開該區域。

8. 選擇 **Create bucket** (建立儲存貯體)

任務 2：將物件上傳到儲存貯體

現在您已為報告資料建立儲存貯體，可以開始處理物件。物件可以是任何類型的檔案：文字檔、相片、影片、.zip 檔等等。當您將物件新增到 Amazon S3，可以選擇包括物件的中繼資料，以及設定控制物件存取的許可。

在這個任務中，您會測試將物件上傳到 reportbucket。您擁有每日報告的螢幕擷取畫面，並希望將此影像上傳到 S3 儲存貯體。

9. 以滑鼠右鍵按一下下面連結：[new-report.png](#)。選擇 **Save link as** (另存連結)，並將檔案儲存到您的桌面。
10. 在 **S3 Management Console** (S3 管理主控台) 中，尋找並選取開頭為 **reportbucket** 的儲存貯體名稱。
11. 選擇 **Upload** (上傳)

此步驟會啟動上傳精靈。使用這個精靈上傳檔案，從檔案選擇器選取檔案，或將檔案拖曳至 Amazon S3 視窗。

12. 選擇 **Add files** (新增檔案)
13. 瀏覽並選取您先前下載的 **new-report.png** 檔案。
14. 選擇頁面底部的 **Upload** (上傳)

顯示代表 **Upload succeeded** (上傳成功) 的綠色長條時，表示您的檔案已成功上傳。

15. 在右上方的 **Upload: status** (上傳：狀態) 區段中，選擇 **Close** (關閉)

任務 3：將物件公開

安全是 Amazon S3 的首要考量。在您設定將 EC2 執行個體連線到 reportbucket 之前，您想要針對安全性測試儲存貯體和物件設定。

在此任務中，您會設定儲存貯體和物件的許可，以測試可存取性。

首先，您嘗試存取物件，確認物件預設為私有。

16. 在 **reportbucket** 概觀頁面的 **Objects** (物件) 標籤上，找到 **new-report.png** 物件，然後選擇 **new-report.png** 檔案名稱。

new-report.png 概觀頁面隨即開啟。左上方的導覽會更新為連結，可返回儲存貯體概觀頁面。

17. 在 **Object overview** (物件概觀) 區段中，找到並複製 **Object URL** (物件 URL) 連結。

連結看起來應該類似如下：<https://reportbucket987987.s3-us-west-2.amazonaws.com/new-report.png>

18. 開啟新的瀏覽器標籤，並將物件 URL 連結貼到網址列中，然後按下 **Enter** 鍵。

您會收到 **Access Denied** (存取遭拒) 錯誤，因為 Amazon S3 中的物件預設為私有物件。

現在您已確認 Amazon S3 的安全性預設為私有，您要測試如何將物件設定為可公開存取。

19. 讓瀏覽器的 Access Denied (存取遭拒) 錯誤保持開啟狀態，然後使用 **S3 Management Console** (S3 管理主控台) 返回 Web 瀏覽器標籤。
20. 您應該仍在 **new-report.png Object overview** (物件概觀) 標籤上。
21. 在右上方選擇 **Object actions** (物件動作) 下拉式選單，您將注意到 **Make public via ACL** (透過 ACL 設為公開) 呈反灰。
22. 在頁面的左上方，選擇導覽中的 **reportbucket** 名稱以返回主要 **reportbucket** 概觀頁面。
23. 選擇 **Permissions** (許可) 標籤。
24. 我們需要先允許使用 ACL。在 **Object Ownership** (物件擁有權) 底下，選擇 **Edit** (編輯)。
25. 選擇 **ACLs enabled** (已啟用 ACL)。
26. 選擇 **Bucket owner preferred** (儲存貯體擁有者優先)。
27. 選擇 **Save changes** (儲存變更)。
28. 在 **Block public access (bucket settings)** (封鎖公開存取 (儲存貯體設定)) 底下，選擇 **Edit** (編輯) 來變更設定。
29. 清除 **Block all public access** (封鎖所有公開存取) 選項，然後讓所有其他選項保留清除狀態。

請注意，所有個別選項都會保持清除狀態。清除所有公開存取的選項時，必須選取適用於本身情況和安全目標的個別選項。您稍後在實驗室中使用存取控制清單 (ACL) 和儲存貯體政策，因此這些選項在本任務中會保持清除狀態。在生產環境中，建議使用可能的最低權限設定。如需詳細資訊，請參閱此實驗室最後**其他資源**部分的 Amazon S3 封鎖公開存取連結。

28. 選擇 **Save changes** (儲存變更)
29. 對話方塊隨即開啟，要求您確認變更。在欄位中輸入 `confirm`，然後選擇 **Confirm** (確認)

Successfully edited bucket settings for Block Public Access (已成功編輯封鎖公開存取的儲存貯體設定) 的訊息會顯示在視窗頂端。

30. 選擇 **Objects** (物件) 標籤。
31. 選擇 **new-report.png** 檔案名稱。
32. 在 **new-report.png** 概觀頁面上，選擇 **Object actions** (物件動作) 下拉式選單，然後選取 **Make public** (設為公開)。

請注意以下警告：**When public read access is enabled and not blocked by Block Public Access settings, anyone in the world can access the specified objects** (當公開讀取存取權已啟用且未遭 Block Public Access (封鎖公開存取) 設定封鎖時，全球所有人皆可存取指定的物件)。這是為了提醒您，如果您將物件設為公開，則全球所有人皆可讀取物件。

33. 選擇 **Make public** (設為公開)，您就會看到視窗頂端的 **Successfully edited public access** (已成功編輯公開存取權) 綠色橫幅。
34. 在右上方，選擇 **Close** (關閉) 以返回 **new-report.png** 物件概觀。
35. 返回針對 new-report.png 物件顯示 **Access Denied** (存取遭拒) 的瀏覽器標籤，然後重新整理頁面。

new-report.png 物件現在會正確顯示，因為它可以公開存取。

36. 關閉顯示新 new-report.png 影像的 Web 瀏覽器標籤，然後返回 Amazon S3 管理主控台的標籤。

在此範例中，您只將讀取存取權授與特定物件。如果您想要將存取權授與整個儲存貯體，則需要使用儲存貯體政策，本實驗室稍後會涵蓋該政策。


在下一個任務中，您會使用 EC2 執行個體來確認與 S3 儲存貯體的連線。

任務 4：從 EC2 執行個體測試連線

在此任務中，您會連線到 EC2 執行個體，以測試 Amazon S3 reportbucket 的連線和安全性。

您應該已經登入到 AWS S3 Management Console。如果沒有，請依照開始實驗室部分中的步驟登入 AWS S3 Management Console。

37. 在 **Services** (服務) 選單上，選擇 **EC2**。
38. 在 **EC2 Dashboard** (EC2 儀表板) 上的 **Resources** (資源) 區段底下，選擇 **Instances (running)** (執行個體 (執行中))。
39. 選取 **Bastion Host** (堡壘主機) 的 ☒ 核取方塊，並選擇 **Connect** (連線)
40. 在 **Connect to instance** (連接執行個體) 視窗中，選取 **Session Manager** (工作階段管理員) 標籤做為連線方法。

 透過 AWS Systems Manager Session Manager，您可連線到堡壘主機執行個體，而不需要在防火牆或 Amazon Virtual Private Cloud (Amazon VPC) 安全群組開啟特定連接埠。如需詳細資訊，請參閱此實驗室結尾其他資源部分的 **AWS Systems Manager Session Manager**。

41. 選擇 **Connect** (連線)

包含與堡壘主機執行個體連線的新瀏覽器標籤或視窗隨即開啟。

您現在已連線到存放報告應用程式的 EC2 執行個體。由於工作階段管理員使用 HTTPS 連接埠 443，因此不需要您開啟 SSH 連接埠 22 給外部使用。您滿意這個安全性功能。現在您想了解 EC2 如何與 S3 儲存貯體互動。

42. 在堡壘主機工作階段中輸入以下命令，變更為主目錄 (/home/ssm-user/)：

```
cd ~
```

輸出會帶您回到命令提示字元。

43. 輸入以下命令，確認您位於主目錄中：

```
pwd
```

輸出應如下所示：

```
/home/ssm-user
```

您現在位於 ssm-user 的主目錄，您將在此位置執行此實驗室中的所有命令。

44. 輸入以下命令來列出所有 S3 儲存貯體。

```
aws s3 ls
```

輸出內容應該會如下所示：

```
2020-11-11 22:34:46 reportbucket987987
```

您會看到自己建立的 reportbucket 和實驗室自動產生的儲存貯體。

注意：在建立實驗室環境期間，系統會自動為 EC2 執行個體新增執行個體描述檔 (定義您的身分，用於身份驗證) 和角色 (定義身份驗證後您可以執行的動作)，讓 EC2 執行個體可以列出 S3 儲存貯體和物件。

45. 在以下命令中，將 reportbucket 名稱末端的 (NUMBER) 變更為您建立的儲存貯體名稱。輸入您調整過的命令來列出 reportbucket 中的所有物件。

```
aws s3 ls s3://reportbucket(NUMBER)
```

該命令看起來類似如下：**aws s3 ls s3://reportbucket987987**

輸出看起來應如下所示：

```
2020-11-11 15:46:34      86065 new-report.png
```

您的儲存貯體中目前只有一個物件。該物件稱為 new-report.png。

46. 輸入下列命令，將目錄變更至報告目錄。

```
cd reports
```

輸出會帶您回到命令提示字元。

47. 輸入下列命令來列出目錄的內容。

```
ls
```

輸出會顯示報告目錄中所建立的一些檔案，以測試應用程式。

```
dolphins.jpg files.zip report-test.txt  report-test1.txt report-test2.txt report-test3.txt  
whale.jpg
```

48. 在以下命令中，將 reportbucket 名稱末端的 (NUMBER) 變更為您建立的儲存貯體名稱。輸入您調整過的命令來查看是否可以將檔案複製到 S3 儲存貯體。


```
aws s3 cp report-test1.txt s3://reportbucket(NUMBER)
```

該命令看起來與此類似：**aws s3 cp report-test1.txt s3://reportbucket987987**

輸出會表示 **upload failed** (上傳失敗) 錯誤。發生此錯誤是因為您擁有儲存貯體的唯讀權限，但沒有執行 PutObject 動作的許可。

49. 讓此視窗保持開啟狀態，然後返回 AWS 主控台的瀏覽器標籤。

在下一個任務中，您會建立儲存貯體政策來新增 PutObject 許可。

任務 5：建立儲存貯體政策

儲存貯體政策是與 S3 儲存貯體關聯的一組許可。它可用於控制整個儲存貯體的存取權，或儲存貯體內特定目錄的存取權。

在此任務中，您會使用 AWS 政策產生器建立儲存貯體政策，以啟用從 EC2 執行個體到儲存貯體的讀取和寫入存取權，以確保您的報告應用程式能夠成功寫入 Amazon S3。

50. 以滑鼠右鍵按一下以下連結：[sample-file.txt](#)。選擇 **Save link as** (另存連結)，並將檔案儲存到您的桌面。
51. 返回 AWS S3 Management Console，移至 **Services** (服務) 選單，然後選取 **S3**。
52. 在 **S3 Management Console** (S3 管理主控台) 標籤中，選取儲存貯體的名稱。
53. 若要上傳 **sample-file.txt** 檔案，選擇 **Upload** (上傳)，並使用在任務 2 中相同的上傳程序。
54. 在 **reportbucket** 概觀頁面上，選擇 **sample-file.txt** 檔案名稱。**sample-file.txt** 概觀頁面隨即開啟。
55. 在 **Object overview** (物件概觀) 區段底下，找到並複製 **Object URL** (物件 URL) 連結。
56. 在新的瀏覽器標籤，將連結貼到網址列，然後按 Enter 鍵。

您的瀏覽器會再次顯示 **Access Denied** (存取遭拒) 訊息。您需要設定儲存貯體政策，以便將存取權限授與儲存貯體中的所有物件，無須個別在每一個物件指定許可。

57. 將此瀏覽器標籤保持開啟，但返回 **S3 管理主控台** 的標籤。
58. 選取 **Services** (服務)，並選取 **IAM**。在左側導覽中，選擇 **Roles** (角色)。
59. 在 **Search** (搜尋) 欄位中，輸入 `EC2InstanceProfileRole`。

這是 EC2 執行個體連線到 Amazon S3 時所使用的角色。

60. 選取 **EC2InstanceProfileRole**。在 **Summary** (摘要) 區段中，將 **Role ARN** (角色 ARN) 複製到文字檔案，以便在稍後的步驟中使用。


它看起來應該類似如下：**arn:aws:iam::596123517671:role/EC2InstanceProfileRole**

61. 依序選擇 **Services** (服務)、**S3**，然後返回 **S3 Management Console** (S3 管理主控台)。
62. 選擇 **reportbucket**。

您應該會看到自己上傳的兩個物件。如果沒有看到，請回到您的儲存貯體，就會看到已上傳的物件清單。

63. 選擇 **Permissions** (許可) 標籤。
64. 在 **Permissions** (許可) 標籤中，捲動至 **Bucket Policy** (儲存貯體政策) 區段，然後選擇 **Edit** (編輯)

空白的儲存貯體政策編輯器隨即顯示。您可以手動建立儲存貯體政策，也可以借助 **AWS 政策產生器** 來建立。

 Amazon 資源名稱 (ARN) 可在所有 AWS 中唯一識別 AWS 資源。ARN 的每個部分都以冒號 (:) 區隔，而且每個部分都代表指定資源的路徑特定部分。根據參考的服務，這些部分可能略有不同，但格式通常如下：

arn:*partition:service:region:account-id:resource*

Amazon S3 不需要 ARN 中的 Region 或 account-id 參數，所以這些部分保留空白。但是，仍然使用冒號 (:) 區隔每一個部分，因此看起來類似於 `arn:aws:s3:::reportbucket987987`

如需詳細資訊，請參閱此實驗室最後其他資源部分的 **Amazon 資源名稱 (ARN)** 和 **AWS 服務命名空間文件連結**。

65. 在 **Policy examples** (政策範例) 和 **Policy generator** (政策產生器) 按鈕下方，找到 **Bucket ARN** (儲存貯體 ARN)。將儲存貯體 ARN 複製到文字檔案，以便在稍後的步驟中使用。

看起來如下：

```
Bucket ARN
arn:aws:s3:::reportbucket987987
```

66. 選擇政策產生器

會在新的 Web 瀏覽器標籤開啟 AWS 政策產生器。

i AWS 政策會使用 JSON 格式，用來為 AWS 服務設定精細許可。您可以使用 JSON 手動寫入政策，也可以使用 AWS 政策產生器以方便使用的 Web 界面來建立政策。

在 AWS 政策產生器視窗中，設定以下各項：

- 為 **Select Type of Policy** (選取政策類型) 選取 **S3 Bucket Policy** (S3 儲存貯體政策)。
- 為 **Effect** (效果) 選取 **Allow** (允許)。
- 在 **Principal** (主體)，貼上您在先前步驟中複製到文字檔案的 **EC2 Role ARN** (EC2 角色 ARN)。
- 在 **AWS Service** (AWS 服務)，保留 **Amazon S3** 的預設設定。
- 為 **Actions** (動作) 選取 **GetObject** 和 **PutObject**。

i **GetObject** 動作會為要從 Amazon S3 擷取的物件授與許可。請參閱實驗室最後的其他資源部分，透過該處的連結取得關於可在 Amazon S3 政策中使用之動作的詳細資訊。

- **Amazon Resource Name (ARN)** (Amazon 資源名稱 (ARN))，貼上您先前複製的儲存貯體 ARN。
- 在 ARN 最後，輸入 `/*`

ARN 看起來應該類似如下：`arn:aws:s3:::reportbucket987987/*`

67. 選擇 **Add Statement** (新增陳述式)。您設定的陳述式詳細資訊會新增至按鈕下方的表格。您可以將多個陳述式新增至政策。
68. 選擇 **Generate Policy** (產生政策)。

會開啟新視窗並顯示產生的政策 (JSON 格式)。看起來應類似於以下內容：

```
{
  "Version": "2012-10-17",
  "Id": "Policy1604361694227",
  "Statement": [
    {
      "Sid": "Stmt1604361692117",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::416159072693:role/EC2InstanceProfileRole"
      },
      "Action": [
```

```

        "s3:GetObject",
        "s3:PutObject"
    ],
    "Resource": "arn:aws:s3:::reportbucket987987/*"
}
]
}

```

⚠ 確認儲存貯體名稱後面有 **/***，如這個範例中的 Resource 行所示。

69. 將您建立的政策複製到剪貼簿。
70. 關閉 Web 瀏覽器標籤，並返回**儲存貯體政策編輯器**的 S3 管理主控台標籤。
71. 將您建立的儲存貯體政策貼到**儲存貯體政策編輯器**中。
72. 選擇 **Save changes** (儲存變更)
73. 返回 AWS Systems Manager (Systems Manager) 視窗。如果您的工作階段逾時，請使用實驗室中先前的步驟重新連接到 Systems Manager。
74. 輸入以下命令，確認您位於 `/home/ssm-user/reports` 目錄中。

```
pwd
```

輸出應如下所示：

```
/home/ssm-user/reports
```

75. 在以下命令中，以您建立儲存貯體時所使用的號碼取代 (*NUMBER*)。輸入調整過的命令來列出 reportbucket 中的所有物件。

```
aws s3 ls s3://reportbucket(NUMBER)
```

該命令看起來應該類似如下：**aws s3 ls s3://reportbucket987987**

輸出內容應該會如下所示：

```
sh-4.2$ aws s3 ls s3://reportbucket987987
2020-11-02 23:20:27      86065 new-report.png
2020-11-02 23:57:03       90 sample-file.txt
```

76. 輸入下列命令來列出報告目錄的內容。

```
ls
```

輸出會傳回檔案清單。

77. 在以下命令中，以您建立儲存貯體時所使用的號碼取代 (*NUMBER*)。輸入您調整過的命令，嘗試將 report-test1.txt 檔案複製到 S3 儲存貯體。

```
aws s3 cp report-test1.txt s3://reportbucket(NUMBER)
```

該命令看起來應該如下所示：**aws s3 cp report-test1.txt s3://reportbucket987987**

輸出會傳回以下內容：

```
upload: ./report-test1.txt to s3://reportbucket987987/report-test1.txt
```

78. 在以下命令中，以您建立儲存貯體時所使用的號碼取代 (*NUMBER*)。輸入您調整過的命令，查看檔案是否已成功上傳至 Amazon S3。

```
aws s3 ls s3://reportbucket(NUMBER)
```

輸出內容應該會如下所示：

```
2020-11-11 18:20:23      86065 new-report.png
2020-11-11 18:32:18         31 report-test1.txt
2020-11-11 18:20:22         90 sample-file.txt
```

您已成功將檔案從 EC2 執行個體上傳 (PutObject) 到 S3 儲存貯體。

79. 在以下命令中，以您建立儲存貯體時所使用的號碼取代 (*NUMBER*)。輸入您調整過的命令，將檔案從 Amazon S3 擷取 (GetObject) 到 EC2 執行個體。

```
aws s3 cp s3://reportbucket(NUMBER)/sample-file.txt sample-file.txt
```

輸出內容應該會如下所示：

```
download: s3://reportbucket987987/sample-file.txt to ./sample-file.txt
```


80. 輸入下列命令，查看檔案現在是否位於 /reports 目錄中。

```
ls
```

輸出內容應該會如下所示：

```
dolphins.jpg  files.zip  report-test1.txt  report-test2.txt  report-test3.txt  sample-
file.txt
```

您現在可以在檔案清單中看到 sample-file.txt。恭喜您！您已成功將檔案從 Amazon EC2 上傳到 S3 儲存貯體並進行擷取。

81. 返回針對 **sample-file.txt** 顯示 **Access Denied** (存取遭拒) 錯誤的瀏覽器標籤，然後重新整理  頁面。

頁面仍然顯示錯誤訊息，因為儲存貯體政策僅將權限授予名為 EC2InstanceProfileRole 的主體。

82. 前往 AWS 政策產生器，並將另一個允許每個人 (*) 讀取存取權 (GetObject) 的陳述式新增至儲存貯體政策。產生此政策需要一些時間。這個政策讓 EC2InstanceProfileRole 能夠存取儲存貯體，同時還讓每個人都能透過瀏覽器讀取物件。

以下是上述的範例：

```
{
  "Sid": "Stmt1604428842806",
  "Effect": "Allow",
  "Principal": "*",
  "Action": "s3:GetObject",
  "Resource": "arn:aws:s3:::reportbucket987987/*"
}
```

83. 若要測試您的政策是否有效，請前往顯示 **Access Denied** (存取遭拒) 錯誤的瀏覽器，然後重新整理。如果您可以閱讀文字，那麼恭喜您！您的政策成功了。

如果不行，看一下以下政策以取得協助。修改後的政策應如下列政策所示。請注意，陳述式有兩個：其中一個是包含 EC2InstanceProfileRole 的陳述式，另一個是主體為 "*" (表示每個人) 的陳述式。

如果您無法自行產生政策，您可以複製下列政策並貼到 BucketPolicy 編輯器中。請務必使用您在前一步驟中複製的 EC2InstanceProfileRole ARN 取代下列政策中現有的 EC2InstanceProfileRole ARN。確保用您建立的儲存貯體取代 reportbucket 範例 ARN，而且 /* 顯示在儲存貯體 ARN 的末端。請以政策的最後一行當作範例。

```
{
  "Version": "2012-10-17",
  "Id": "Policy1604428844058",
  "Statement": [
    {
      "Sid": "Stmt1604428821481",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::285058481724:role/EC2InstanceProfileRole"
      },
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::reportbucket987987/*"
    },
    {
      "Sid": "Stmt1604428842806",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::reportbucket987987/*"
    }
  ]
}
```

84. 讓標籤保持開啟狀態並顯示 sample-file.txt。您在下一個任務中返回此標籤。

在此任務中，您建立了儲存貯體政策，以允許儲存貯體的特定存取權限。在下一節中，您將探索如何保留檔案複本，以防止意外刪除。

任務 6：探索版本控制

版本控制是在相同儲存貯體中保持一個物件的多個不同版本。您可以使用版本控制功能來保留、擷取和恢復在 S3 儲存貯體中存放的每個物件的每個版本。有了版本控制，您即可從使用者動作失誤和應用程式故障中輕鬆恢復。

基於稽核與合規性原因，您需要在 reportbucket 上啟用版本控制。版本控制應保護 reportbucket 中的報告，避免遭意外刪除。您有興趣了解這是否如廣告所說的那樣有效。在此任務中，您可以上傳先前任務中 sample-file.txt 檔案的修訂版本，藉此啟用版本控制並測試功能。

85. 您應該在上一個任務的 S3 儲存貯體 **Permissions** (許可) 標籤上。如果不是，請選擇畫面左上方的儲存貯體連結，返回儲存貯體概觀頁面。
86. 在 **reportbucket** 概觀頁面上，選擇 **Properties** (屬性) 標籤。
87. 在 **Bucket Versioning** (儲存貯體版本控制) 區段底下，按一下 **Edit** (編輯)，選取 **Enable** (啟用)，然後按一下 **Save changes** (儲存變更)。

版本控制會對整個儲存貯體和儲存貯體中的所有物件啟用。無法為個別物件啟用。


 啟用版本控制時，也需考量成本因素。請參閱實驗室最後的**其他資源**部分，透過該處的連結取得詳細資訊。

88. 以滑鼠右鍵按一下此連結，並使用您在上一個任務中的文字檔案名稱，將文字檔案儲存到您的電腦：[sample-file.txt](#)

此檔案雖然具有與先前的檔案相同的名稱，但包含新的文字。

89. 在 Amazon S3 管理主控台的 reportbucket 上，選擇 **Objects** (物件) 標籤。

在 **Objects** (物件) 區段底下尋找  **Show versions** (顯示版本)。

90. 選擇 **Upload** 檔案，並使用在任務 2 到 5 中的相同上傳程序來上傳新的 **sample-file.txt** 檔案。
91. 移至內有 sample-file.txt 檔案內容的瀏覽器標籤。
92. 記下頁面上的內容，然後重新整理  頁面。

請注意隨即顯示的新文字行。

如果未另行指定版本，Amazon S3 一律會傳回物件的最新版本。

您也可以在 Amazon S3 管理主控台取得可用的版本清單。

93. 關閉內含文字檔內容的 Web 瀏覽器標籤。
94. 在 Amazon S3 管理主控台中，選擇 **sample-file.txt** 檔案名稱。**sample-file.txt** 概觀頁面隨即開啟。
95. 選擇 **Versions** (版本) 標籤，然後選取最底下顯示為 **null** 的版本。(這不是最新版本)。
96. 按一下 **Open** (開啟)。

您現在應該可以使用 Amazon S3 管理主控台查看檔案的原始版本。

不過，如果您嘗試使用物件 URL 連結存取較舊版本的 sample-file.txt 檔案，將會收到拒絕存取訊息。這是預期的訊息，因為您在上一個任務中建立的儲存貯體政策，只允許存取最新版本的物件。若要存取物件的舊版本，您必須更新儲存貯體政策，以納入 **s3:GetObjectVersion** 許可。以下儲存貯體政策範例包含額外的 **s3:GetObjectVersion** 動作，可讓您使用連結存取較舊的版本。您無須使用此範例更新儲存貯體政策即可完成此實驗室。您可以在完成任務後自行嘗試執行此操作。

```
{
  "Id": "Policy1557511288767",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1557511286634",
```

```
    "Action": [
      "s3:GetObject",
      "s3:GetObjectVersion"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:s3:::reportbucket987987/*",
    "Principal": "*"
  }
}
```

97. 返回 **AWS Management Console** 標籤，然後選擇左上方的儲存貯體名稱連結，返回儲存貯體概觀標籤。

98. 找到 **Show versions** (顯示版本) 選項，並將按鈕切換為開啟 **Show versions** 以顯示版本。

現在，您可以檢視每個物件的可用版本，並識別哪個版本為最新版本。注意 **new-report.png** 物件只有一個版本。版本 ID 是 **null**，因為這個儲存貯體啟用版本控制功能之前，已經上傳了物件。

另請注意，您現在可以選擇版本名稱連結，直接瀏覽至主控台中的該物件版本。

99. 將 **Show versions** (顯示版本) 旁的按鈕切換為關閉 **Show versions**，返回預設物件檢視。

100. 選取 **sample-file.txt** 左側的核取方塊。

101. 選取物件後，選擇 **Delete** (刪除)

102. **Delete objects** (刪除物件) 頁面隨即顯示。

103. 在底部的 **Delete objects?** (刪除物件?) 區段中，輸入 **delete** 並選擇 **Delete objects** (刪除物件) 來確認刪除物件。

104. 在頁面的右上方，選擇 **Close** (關閉) 以返回儲存貯體概觀。

儲存貯體中不會再顯示 **sample-file.txt** 物件。不過，如果不小心刪除物件，您可以使用版本控制進行復原。

105. 找到 **Show versions** (顯示版本) 選項，並將按鈕切換為開啟 **Show versions** 以顯示版本。

請注意，**sample-file.txt** 物件會再次顯示，但最新版本是 **刪除標記**。也會列出兩個之前的版本。如果已啟用儲存貯體版本控制功能，則不會立即刪除物件。Amazon S3 會插入刪除標記，該標記變成最新的物件版本。該物件的舊版本不會移除。請參閱實驗室最後的**其他資源**部分，透過該處的連結取得關於版本控制的詳細資訊。

106. 使用刪除標記選取 **sample-file.txt** 物件版本左側的核取記號。

107. 選取物件後，選擇 **Delete** (刪除)

108. **Delete objects** (刪除物件) 視窗隨即顯示。

109. 在 **Permanently delete objects?** (永久刪除物件?) 區段的底部，輸入 **permanently delete** 並選擇 **Delete objects** (刪除物件) 按鈕來確認刪除物件。

110. 在頁面的右上方，選擇 **Close** (關閉) 以返回儲存貯體概觀。

111. 將 **Show versions** (顯示版本) 旁的按鈕切換為關閉 **Show versions**，返回預設物件檢視。

請注意，**sample-file.txt** 物件已還原至儲存貯體。移除刪除標記已有效地將物件還原至其先前的狀態。請參閱實驗室最後的**其他資源**部分，透過該處的連結取得關於取消刪除 S3 物件的詳細資訊。

接下來，刪除物件的特定版本。

112. 若要刪除物件的特定版本，請找出 **Show versions** (顯示版本) 選項，並將按鈕切換為開啟 **Show versions** 以顯示版本。

您應該會看到 **sample-file.txt** 物件的兩個版本。

113. 選取 **sample-file.txt** 物件最新版本的核取方塊。

114. 選取物件後，選擇 **Delete** (刪除)

115. **Delete objects** (刪除物件) 視窗隨即顯示。

116. 在 **Permanently delete objects?** (永久刪除物件?) 區段的底部，輸入 `permanently delete`，然後選擇 **Delete objects** (刪除物件) 按鈕。

117. 在頁面的右上方，選擇 **Close** (關閉) 以返回儲存貯體概觀。

請注意，現在 **sample-file.txt** 檔案只有一個版本。當刪除物件的特定版本時，不會建立刪除標記。物件會永久刪除。請參閱實驗室最後的**其他資源**部分，透過該處的連結取得關於刪除 Amazon S3 物件版本的詳細資訊。

118. 將 **Show versions** (顯示版本) 旁的按鈕切換為關閉 **Off**，返回預設物件檢視。

119. 選擇 **sample-file.txt** 檔案名稱。sample-file.txt 概觀頁面隨即開啟。

120. 複製視窗底部顯示的 **Object URL** (物件 URL) 連結。

121. 在新的瀏覽器標籤，將連結貼到網址列，然後按 Enter 鍵。

瀏覽器頁面會顯示 **sample-file.txt** 物件的原始版本文字。

摘要

您已成功建立 S3 儲存貯體，可供貴公司從 EC2 執行個體存放報告資料。您已建立允許 EC2 執行個體從 reportbucket 執行 PutObjects 和 GetObject 的儲存貯體政策，而且您已成功測試從 EC2 執行個體上傳和下載檔案，藉此測試儲存貯體政策。您已在 S3 儲存貯體上啟用版本控制功能，以防止意外刪除物件。您已成功完成 EC2 reportbucket 的組態。恭喜您！

提交您的作品

122. 在這些指示的上方，選擇 **Submit** (提交) 以記錄您的進度，並且在收到提示時，選擇 **Yes** (是)。

提示：如果您先前在瀏覽器面板中已隱藏終端機，請勾選右上方的終端機 ☐ 核取方塊以再次顯示它。這將確保實驗室指示在您選擇 Submit (提交) 後仍舊可見。

123. 如果幾分鐘後未顯示結果，請返回這些指示的上方，並選擇 **Grades** (成績)

提示：您可以多次提交作品。在變更作品後，再次選擇 **Submit** (提交)。這個實驗室將記錄您最後一次的提交。

實驗室完成

 恭喜！您已經完成此實驗室。

124. 在此頁面頂端選擇 **End Lab** (結束實驗室)，然後選取 **Yes** (是) 以確認您要結束實驗室。

面板顯示 *DELETE has been initiated...You may close this message box now.* (刪除已啟動... 您現在可以關閉此訊息方塊。)

125. 選取右上角的 **X** 以關閉此面板。

其他資源

- Amazon S3，網址 <http://aws.amazon.com/s3>
- Amazon S3 訓練，網址 https://www.aws.training/LearningLibrary?&search=Amazon%20Simple%20Storage%20Service&tab=view_all
- 編輯物件許可，網址 <http://docs.aws.amazon.com/AmazonS3/latest/UG/EditingPermissionsonanObject.html>
- Amazon S3 儲存貯體命名規則，網址 <https://docs.aws.amazon.com/AmazonS3/latest/dev//BucketRestrictions.html#bucketnamingrules>
- Amazon S3 封鎖公開存取，網址 <https://docs.aws.amazon.com/AmazonS3/latest/user-guide/block-public->

[access.html](#)

- Amazon Resource Names (ARN) 和 AWS 服務命名空間文件，網址 <https://docs.aws.amazon.com/general/latest/gr/aws-arns-and-namespaces.html>
- AWS JSON 政策元素文件，網址 https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_principal.html
- Amazon S3 的動作、資源和條件金鑰，網址 https://docs.aws.amazon.com/IAM/latest/UserGuide/list_amazons3.html
- Amazon S3 版本控制，網址 <https://docs.aws.amazon.com/AmazonS3/latest/dev/Versioning.html>
- 在 Amazon S3 中取消刪除物件，網址 <https://docs.aws.amazon.com/AmazonS3/latest/user-guide/undelete-objects.html>
- 在 Amazon S3 中刪除物件版本，網址 <https://docs.aws.amazon.com/AmazonS3/latest/dev/DeletingObjectVersions.html>
- Amazon S3 版本控制成本考量，網址 <https://aws.amazon.com/s3/faqs/>
- AWS Systems Manager Session Manager，網址 <https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager.html>

如需 AWS Training and Certification 的詳細資訊，請參閱 <https://aws.amazon.com/training/>。

歡迎並感謝您提供的意見回饋。

如果您想要分享任何建議或更正，請在 [AWS Training and Certification 聯絡表格](#) 中提供詳細資訊，網址 <https://support.aws.amazon.com/#/contacts/aws-training>。

© 2021 Amazon Web Services, Inc. 及其關係企業。保留所有權利。在未事先獲得 Amazon Web Services, Inc 書面許可的情況下，不得重製或轉散佈本文件的全部或部分內容。禁止商業用途的複製、出借或銷售。