使用StorageGRID

StorageGRID

NetApp
November 04, 2025

目錄

使用StorageGRID

使用租戶帳戶

使用租戶帳戶：總覽

租戶帳戶可讓您使用簡易儲存服務（S3）REST API或Swift REST API、在StorageGRID一個無法恢復的系統中儲存及擷取物件。

什麼是租戶帳戶？

每個租戶帳戶都有自己的聯盟或本機群組、使用者、S3儲存區或Swift容器、以及物件。

租戶帳戶可用來分隔不同實體所儲存的物件。例如、多個租戶帳戶可用於下列任一使用案例：

- 企業使用案例： StorageGRID 如果在企業內部使用此功能、則網格的物件儲存設備可能會由組織內的不同部門加以分隔。例如、行銷部門、客戶支援部門、人力資源部門等可能有租戶帳戶。

  如果您使用S3用戶端傳輸協定、也可以使用S3儲存區和儲存區原則來分隔企業部門之間的物件。您不需要建立個別的租戶帳戶。請參閱實作說明 "S3 貯體和貯體原則" 以取得更多資訊。

- 服務供應商使用案例： StorageGRID 如果服務供應商正在使用此功能、則網格的物件儲存設備可能會由租用儲存設備的不同實體加以分隔。例如、公司A、公司B、公司C等可能有租戶帳戶。

如何建立租戶帳戶

租戶帳戶是由所建立 "使用Grid Manager的網格管理員StorageGRID"。建立租戶帳戶時、網格管理員會指定下列項目：

- 基本資訊、包括租戶名稱、用戶端類型（ S3 或 Swift ）和選用的儲存配額。
- 租戶帳戶的權限、例如租戶帳戶是否可以使用 S3 平台服務、設定自己的身分識別來源、使用 S3 Select 或使用網格同盟連線。
- 租戶的初始根存取權、取決於 StorageGRID 系統是使用本機群組和使用者、身分識別聯盟或單一登入（ SSO ）。

此外、如果StorageGRID S3租戶帳戶需要符合法規要求、網格管理員也可以針對該系統啟用S3物件鎖定設定。啟用S3物件鎖定時、所有S3租戶帳戶都能建立及管理相容的儲存區。

設定**S3**租戶

之後是 "S3租戶帳戶已建立"、您可以存取租戶管理程式來執行下列工作：

- 設定身分識別聯盟（除非身分識別來源與網格共用）
- 管理群組和使用者
- 使用網格同盟進行帳戶複製和跨網格複寫
- 管理S3存取金鑰

- 建立及管理 S3 儲存區
- 使用 S3 平台服務
- 使用S3 Select
- 監控儲存使用量

> 雖然您可以使用租戶管理器來建立和管理 S3 貯體、但您必須使用 S3 用戶端來擷取和管理物件。請參閱 "使用S3 REST API" 以取得詳細資料。

設定**Swift**租戶

之後 "Swift租戶帳戶已建立"、您可以存取租戶管理程式來執行下列工作：

- 設定身分識別聯盟（除非身分識別來源與網格共用）
- 管理群組和使用者
- 監控儲存使用量

> Swift使用者必須擁有root存取權限、才能存取租戶管理程式。不過、根存取權限不允許使用者驗證進入 "Swift REST API" 以建立容器和擷取物件。使用者必須具有Swift Administrator權限、才能驗證到Swift REST API。

如何登入及登出

登入租戶管理程式

若要存取租戶管理程式、請在的網址列中輸入租戶的URL "支援的網頁瀏覽器"。

開始之前

- 您擁有登入認證資料。
- 您可以使用網格管理員提供的 URL 來存取租戶管理程式。此URL的範例如下所示：

  ```
  https://FQDN_or_Admin_Node_IP/

  https://FQDN_or_Admin_Node_IP:port/

  https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id

  https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id
  ```

  URL 一律包含完整網域名稱（ FQDN ）、管理節點的 IP 位址、或管理節點 HA 群組的虛擬 IP 位址。也可能包括連接埠號碼、 20 位數的租戶帳戶 ID 、或兩者。

- 如果 URL 不包含租戶的 20 位數帳戶 ID 、則您擁有此帳戶 ID 。
- 您使用的是 "支援的網頁瀏覽器"。
- Cookie會在您的網頁瀏覽器中啟用。
- 您屬於具有的使用者群組 "特定存取權限"。

步驟

1. 啟動A "支援的網頁瀏覽器"。
2. 在瀏覽器的網址列中、輸入存取租戶管理程式的URL。
3. 如果系統提示您輸入安全性警示、請使用瀏覽器的安裝精靈來安裝憑證。
4. 登入租戶管理程式。

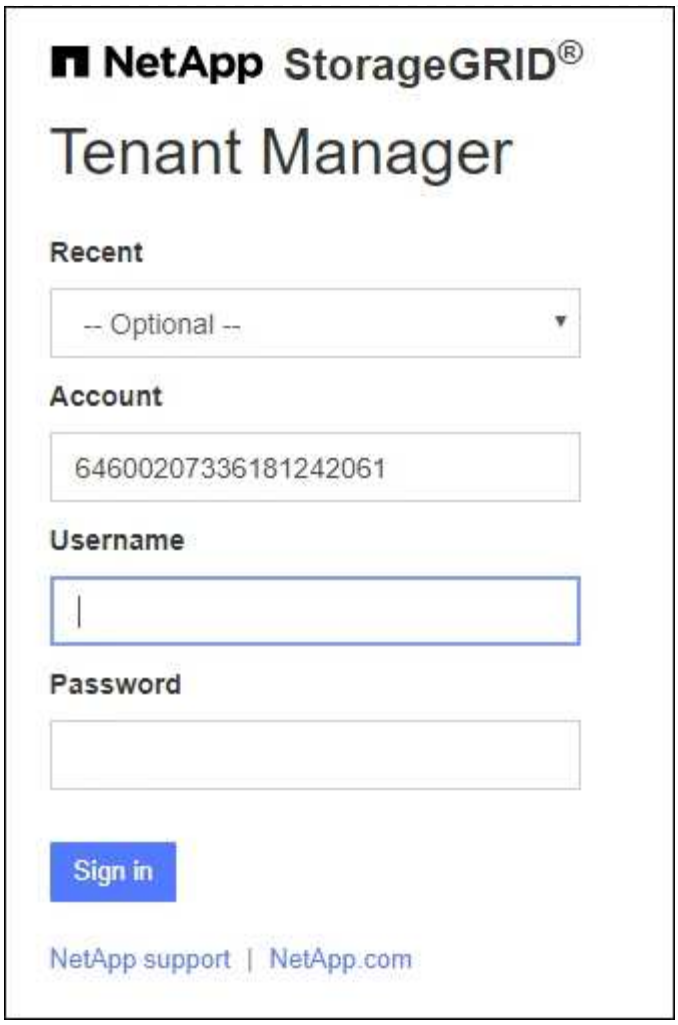
   顯示的登入畫面取決於您輸入的 URL 、以及是否已針對 StorageGRID 設定單一登入（ SSO ）。

未使用 **SSO**

如果 StorageGRID 未使用 SSO 、則會出現下列其中一個畫面：

- Grid Manager登入頁面。選取 * 租戶登入 * 連結。

- 租戶管理程式登入頁面。* 帳戶 * 欄位可能已完成、如下所示。



i. 如果租戶的20位數帳戶ID未顯示、請選取租戶帳戶名稱（如果出現在最近帳戶清單中）、或輸入帳戶ID。

ii. 輸入您的使用者名稱和密碼。

iii. 選擇*登入*。

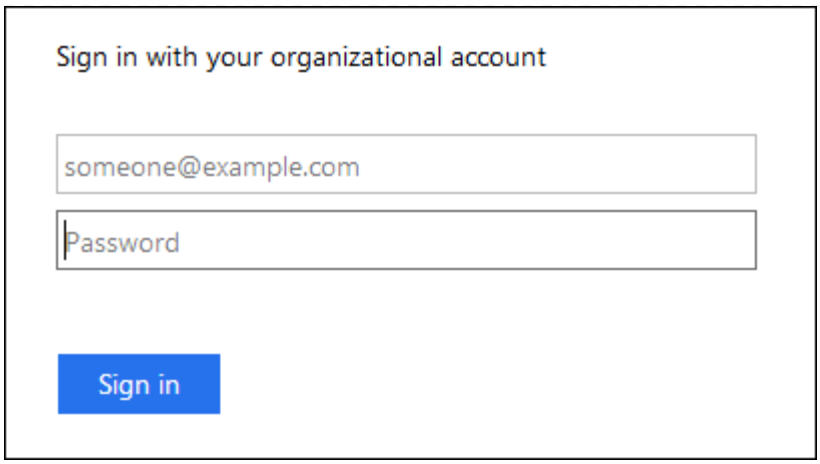
租戶管理器儀表板即會出現。

iv. 如果您收到其他人的初始密碼、請選擇 * _ 使用者名稱 _ * > * 變更密碼 * 來保護您的帳戶安全。

使用 **SSO**

如果 StorageGRID 使用 SSO 、則會出現下列其中一個畫面：

- 貴組織的 SSO 頁面。例如：



輸入您的標準 SSO 認證、然後選取 * 登入 * 。

- 租戶管理程式SSO登入頁面。

i. 如果租戶的20位數帳戶ID未顯示、請選取租戶帳戶名稱（如果出現在最近帳戶清單中）、或輸入帳戶ID。

ii. 選擇*登入*。

iii. 在組織的SSO登入頁面上、以標準SSO認證登入。

租戶管理器儀表板即會出現。

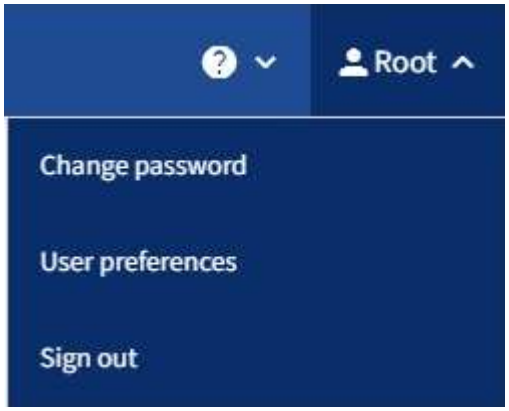
登出租戶管理程式

完成租戶管理程式的使用後、您必須登出、以確保未經授權的使用者無法存取

StorageGRID 系統。根據瀏覽器Cookie設定、關閉瀏覽器可能不會將您登出系統。

步驟

1. 在使用者介面的右上角找到使用者名稱下拉式清單。



2. 選取使用者名稱、然後選取 * 登出 * 。

   - 如果未使用SSO：

     您已登出管理節點。隨即顯示「租戶管理程式」登入頁面。

     如果您登入多個管理節點、則必須登出每個節點。

   - 如果啟用SSO：

     您已登出您正在存取的所有管理節點。畫面會顯示「此功能的登入」頁面。StorageGRID您剛存取的租戶帳戶名稱會在「最近的帳戶」下拉式清單中列為預設名稱、並顯示租戶的*帳戶ID*。

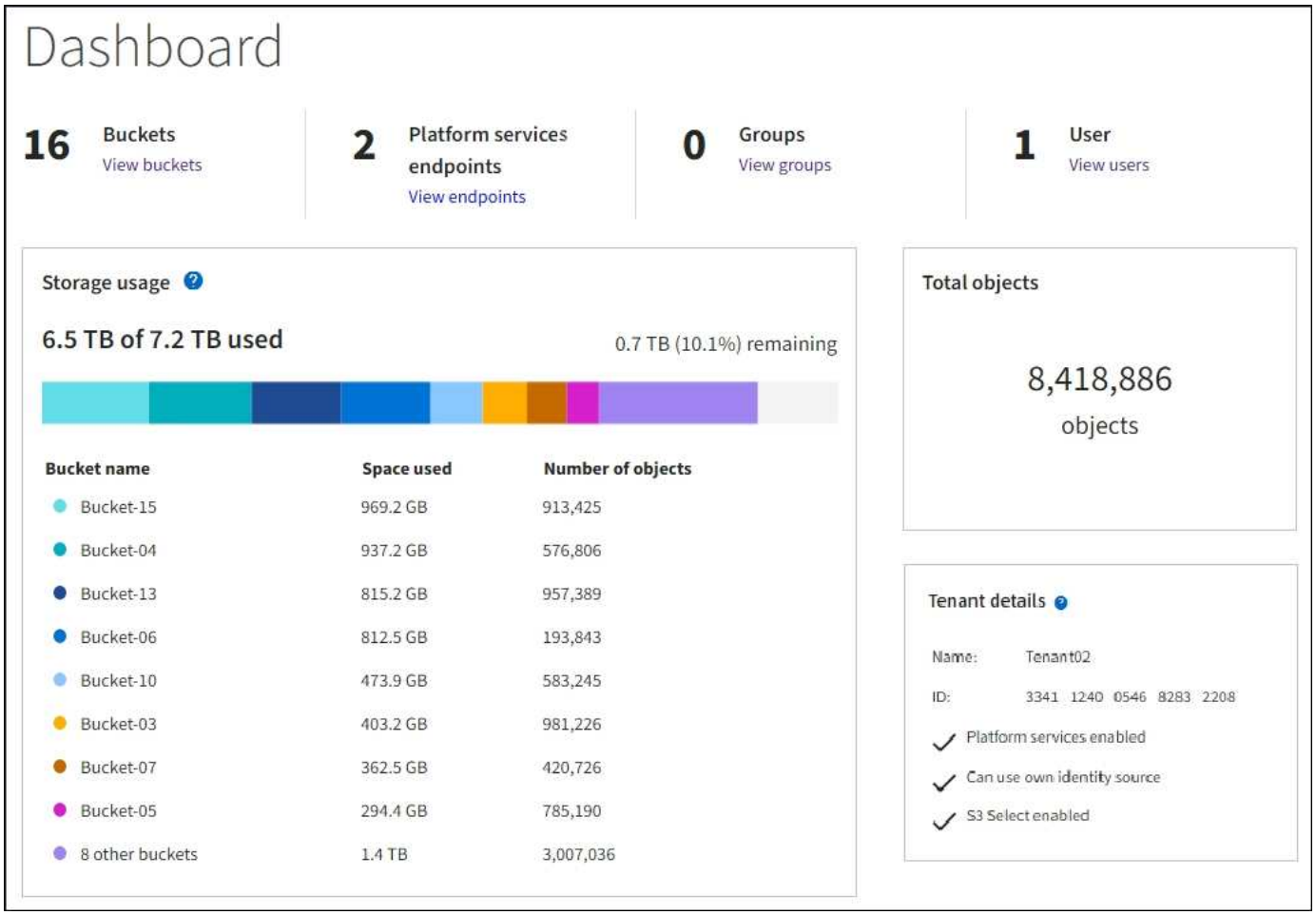
     如果已啟用SSO、而且您也已登入Grid Manager、您也必須登出Grid Manager以登出SSO。

瞭解 **Tenant Manager** 儀表板

租戶管理員儀表板提供租戶帳戶組態的概觀、以及租戶桶（ S3 ）或容器（ Swift ）中物件所使用的空間量。如果租戶有配額、儀表板會顯示使用多少配額、以及剩餘多少配額。如果有任何與租戶帳戶相關的錯誤、這些錯誤會顯示在儀表板上。

「已用空間」值為預估值。這些預估值會受到擷取時間、網路連線能力和節點狀態的影響。

物件上傳後、儀表板看起來像以下範例：



租戶帳戶摘要

儀表板頂端包含下列資訊：

- 已設定的儲存區或容器、群組和使用者數量
- 平台服務端點的數量（若有）

您可以選取連結來檢視詳細資料。

儀表板右側包含下列資訊：

- 租戶的物件總數。

  對於 S3 帳戶、如果沒有擷取任何物件、而且您具有「根目錄」存取權限、則會顯示「入門指南」、而非物件總數。

- 租戶詳細資料、包括租戶帳戶名稱和ID、以及租戶是否可以使用 "平台服務"、 "其本身的身分識別來源"、 "網格同盟"或 "S3 Select" （僅列出已啟用的權限）。

儲存設備與配額使用量

「儲存設備」使用面板包含下列資訊：

- 租戶的物件資料量。

此值表示上傳的物件資料總數量、不代表用來儲存這些物件複本及其中繼資料的空間。

- 如果已設定配額、則為物件資料可用的空間總量、以及剩餘空間的數量和百分比。配額會限制可擷取的物件資料量。

配額使用量是根據內部預估、在某些情況下可能會超過。例如StorageGRID 、當租戶開始上傳物件時、會檢查配額、如果租戶超過配額、則會拒絕新的擷取。不過StorageGRID 、判斷是否超過配額時、不考慮目前上傳的大小。如果刪除物件、可能會暫時禁止租戶上傳新物件、直到重新計算配額使用量為止。配額使用量計算可能需要 10 分鐘或更長時間。

- 代表最大桶或容器之相對大小的長條圖。

  您可以將游標放在任何圖表區段上、以檢視該區段或容器所耗用的總空間。

- 若要對應長條圖、請列出最大的貯體或容器清單、包括物件資料的總數量、以及每個貯體或容器的物件數目。

Bucket name	Space used	Number of objects
Bucket-02	944.7 GB	7,575
Bucket-09	899.6 GB	589,677
Bucket-15	889.6 GB	623,542
Bucket-06	846.4 GB	648,619
Bucket-07	730.8 GB	808,655
Bucket-04	700.8 GB	420,493
Bucket-11	663.5 GB	993,729
Bucket-03	656.9 GB	379,329
9 other buckets	2.3 TB	5,171,588

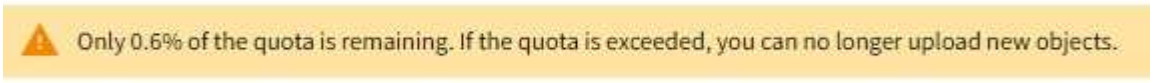
如果租戶擁有超過九個貯體或容器、則所有其他貯體或容器都會合併成清單底部的單一項目。

若要變更租戶管理程式中顯示的儲存值單位、請選取租戶管理程式右上角的使用者下拉式清單、然後選取 * 使用者偏好 * 。

配額使用量警示

如果已在Grid Manager中啟用配額使用量警示、則當配額不足或超出時、這些警示會出現在Tenant Manager中、如下所示：

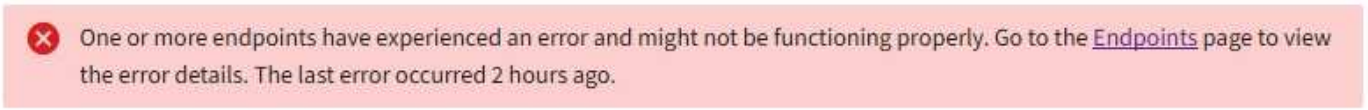
如果已使用90%以上的租戶配額、則會觸發*租戶配額使用量高*警示。執行警示的建議動作。



如果超過配額、就無法上傳新物件。

端點錯誤

如果您使用 Grid Manager 來設定一個或多個端點以搭配平台服務使用、租戶管理程式儀表板會在過去七天內發生任何端點錯誤時、顯示警示。



以查看詳細資訊 "平台服務端點錯誤"，選擇 * 端點 * 以顯示端點頁面。

租戶管理API

瞭解租戶管理API

您可以使用租戶管理REST API（而非租戶管理程式使用者介面）來執行系統管理工作。例如、您可能想要使用API來自動化作業、或更快建立多個實體、例如使用者。

租戶管理API：

- 使用Swagger開放原始碼API平台。Swagger提供直覺式使用者介面、可讓開發人員和非開發人員與API互動。Swagger使用者介面提供每個API作業的完整詳細資料和文件。
- 用途 "支援不中斷營運升級的版本管理"。

若要存取租戶管理API的Swagger文件：

1. 登入租戶管理程式。
2. 從租戶管理器的頂端、選取說明圖示、然後選取 * API 文件 * 。

API作業

租戶管理API會將可用的API作業組織成下列區段：

- * 帳戶 * ：目前租戶帳戶的作業、包括取得儲存使用資訊。
- * 驗證 * ：執行使用者工作階段驗證的作業。

  租戶管理API支援承載權杖驗證方案。對於租戶登入、您可以在驗證要求的Json實體中提供使用者名稱、密碼和帳戶ID（也就是 `POST /api/v3/authorize`）。如果使用者已成功驗證、則會傳回安全性權杖。此

權杖必須在後續API要求（「授權：承載權杖」）的標頭中提供。

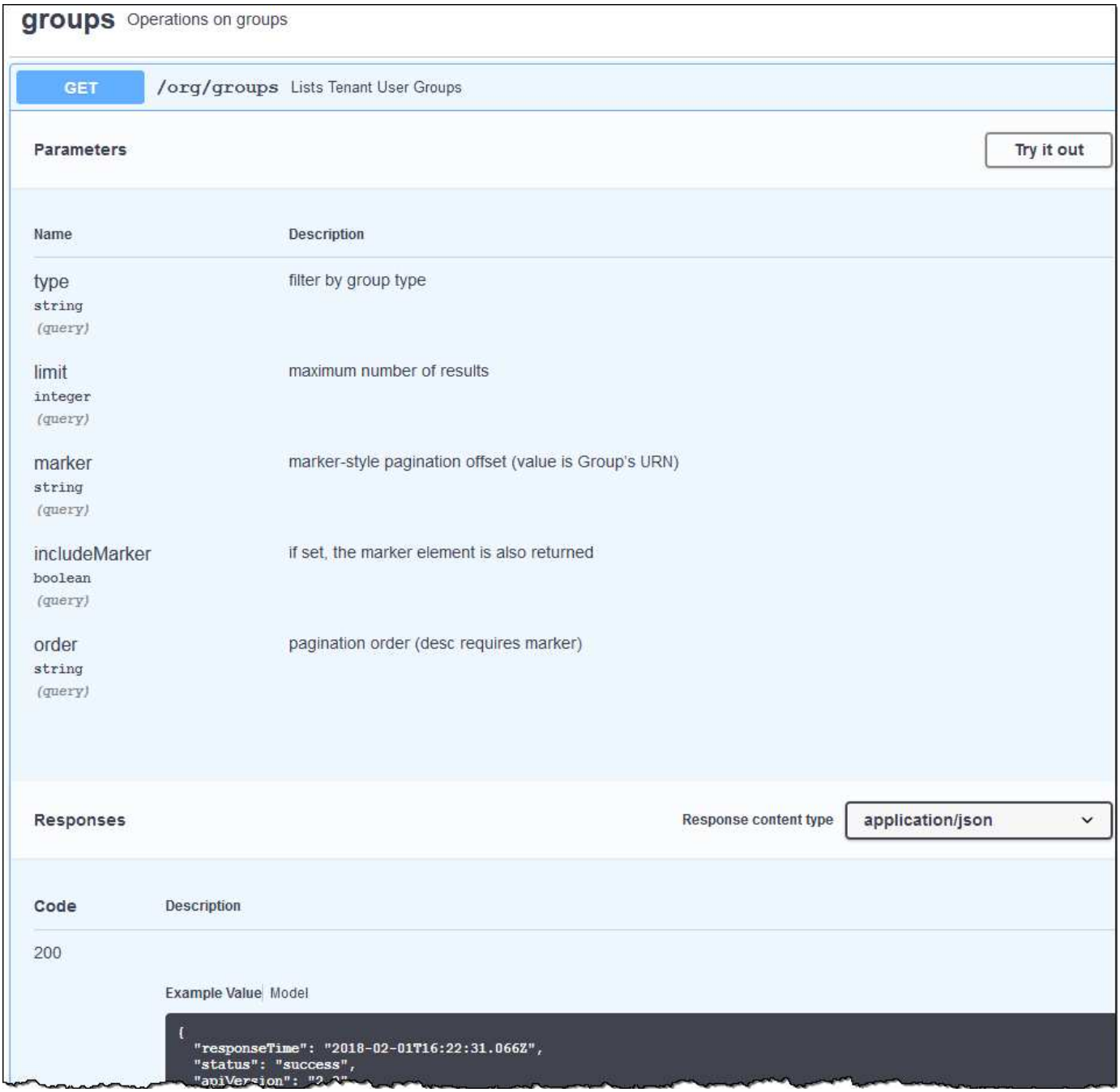
如需改善驗證安全性的資訊、請參閱 "防止跨網站要求偽造"。

> 如果StorageGRID 啟用了單一登入（SSO）功能、您必須執行不同的驗證步驟。請參閱 "網格管理API的使用說明"。

- * 組態 * ：與租戶管理 API 產品版本和版本相關的作業。您可以列出該版本所支援的產品版本和主要API版本。
- * 容器 * ：在 S3 貯體或 Swift 容器上執行作業。
- * 停用功能 * ：檢視可能已停用功能的作業。
- * 端點 * ：管理端點的作業。端點可讓S3儲存區使用外部服務StorageGRID 來進行CloudMirror複寫、通知或搜尋整合。
- * 網格聯合連線 * ：網格聯合連線和跨網格複寫的作業。
- * 群組 * ：管理本機租戶群組及從外部身分識別來源擷取同盟租戶群組的作業。
- * 身分識別來源 * ：設定外部身分識別來源及手動同步同盟群組與使用者資訊的作業。
- * 地區 * ：用於確定已爲 StorageGRID 系統配置哪些區域的操作。
- **S1** ：管理租戶使用者 S3 存取金鑰的作業。
- **S3-object-lock** ：在全域 S3 物件鎖定設定上的作業、用於支援法規遵循。
- * 使用者 * ：檢視及管理租戶使用者的作業。

營運詳細資料

展開每個API作業時、您可以看到其HTTP動作、端點URL、任何必要或選用參數的清單、要求本文的範例（視需要）、以及可能的回應。



發出**API**要求

您使用API文件網頁執行的任何API作業都是即時作業。請小心不要錯誤地建立、更新或刪除組態資料或其他資料。

步驟

1. 選取HTTP動作以查看要求詳細資料。
2. 判斷要求是否需要其他參數、例如群組或使用者ID。然後取得這些值。您可能需要先發出不同的API要求、才能取得所需的資訊。
3. 判斷您是否需要修改範例要求本文。如果是、您可以選取*模型*來瞭解每個欄位的需求。
4. 選擇*試用*。

5. 提供任何必要的參數、或視需要修改申請本文。
6. 選擇*執行*。
7. 檢閱回應代碼以判斷要求是否成功。

租戶管理**API**版本管理

租戶管理API使用版本管理來支援不中斷營運的升級。

例如、此Request URL會指定API版本3。

```
https://hostname_or_ip_address/api/v3/authorize
```

當進行與舊版不相容的變更時、會增加租戶管理 API 的主要版本。當進行與舊版相容的變更時、會增加租戶管理 API 的次要版本。相容的變更包括新增端點或新屬性。下列範例說明如何根據所做的變更類型來提高API版本。

API變更類型	舊版本	新版本
與舊版相容	2.1	2.2
與舊版不相容	2.1	3.0

第一次安裝時、只會啟用最新版本的租戶管理API。StorageGRID不過StorageGRID 、當將支援功能升級至新功能版本時、您仍可繼續存取舊版的API、以取得至少一個StorageGRID 版本的支援功能。

過時的要求會以下列方式標示為已過時：

- 回應標頭為「deprecated：true」
- Json回應本文包含「deprecated」：true

判斷目前版本支援哪些**API**版本

使用下列API要求傳回支援的API主要版本清單：

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

您可以使用路徑參數來指定API版本 (`/api/v3`）或標頭 (`Api-Version: 3`）。如果您同時提供這兩個值、則標頭值會覆寫路徑值。

```
curl https://<IP-Address>/api/v3/grid/accounts
```

```
curl -H "Api-Version: 3" https://<IP-Address>/api/grid/accounts
```

防範跨網站要求偽造（**CSRF**）

您StorageGRID 可以使用CSRF權杖來強化使用Cookie的驗證功能、協助防範跨網站要求偽造（CSRF）攻擊。Grid Manager與租戶管理程式會自動啟用此安全功能、其他API用戶端則可選擇是否在登入時啟用。

攻擊者若能觸發要求至不同網站（例如HTTP表單POST）、可能會導致使用登入使用者的Cookie發出特定要求。

利用CSRF權杖協助防範CSRF攻擊。StorageGRID啟用時、特定Cookie的內容必須符合特定標頭或特定POST本文參數的內容。

若要啟用此功能、請設定 `csrfToken` 參數至 `true` 驗證期間。預設值為 `false`。

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

如果正確、則為A `GridCsrfToken` Cookie是以隨機值設定、用於登入Grid Manager和 `AccountCsrfToken` Cookie是以隨機值設定、用於登入租戶管理程式。

如果Cookie存在、則所有可修改系統狀態的要求（POST、PUT、PATCH、DELETE）都必須包含下列其中一項：

- 。 `X-Csrf-Token` 標頭、並將標頭值設為CSRF權杖Cookie的值。
- 對於接受格式編碼實體的端點：a `csrfToken` 表單編碼要求本文參數。

若要設定CSRF保護、請使用 "網格管理API" 或 "租戶管理API"。

> 具有CSRF權杖Cookie集的要求也會強制執行 `"Content-Type: application/json"` 任何要求的標頭、如果要求Json要求實體做為額外的CSRF攻擊防護、

使用網格同盟連線

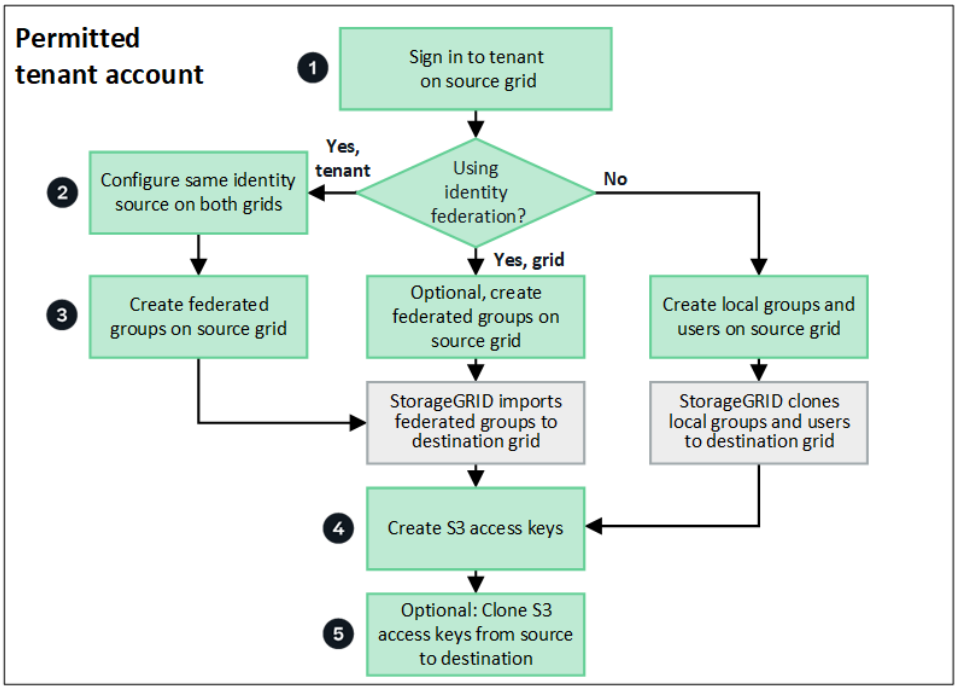
如果新租戶有使用網格同盟連線的權限、則該租戶在建立時會從一個 StorageGRID 系統複寫到另一個 StorageGRID 系統。複寫租戶之後、任何新增至來源租戶的群組和使用者都會複製到目的地租戶。

最初建立租戶的 StorageGRID 系統是租戶的 _ 來源網格 _ 。複寫租戶的 StorageGRID 系統是租戶的 _ 目的地網格 _ 。兩個租戶帳戶都有相同的帳戶 ID 、名稱、說明、儲存配額和指派的權限、 但目的地租戶最初並沒有 root 使用者密碼。如需詳細資訊、請參閱 "什麼是帳戶複製" 和 "管理允許的租戶"。

需要複製租戶帳戶資訊 "跨網格複寫" 的目標。在兩個網格上擁有相同的租戶群組和使用者、可確保您存取任一網格上對應的貯體和物件。

帳戶複製的租戶工作流程

如果您的租戶帳戶具有 * 使用網格同盟連線 * 權限、請檢閱工作流程圖、查看您將執行哪些步驟來複製群組、使用者和 S3 存取金鑰。



以下是工作流程的主要步驟：

1 登入租戶

登入來源網格（最初建立租戶的網格）上的租戶帳戶。

2 您也可以選擇設定身分識別聯盟

如果您的租戶帳戶具有 * 使用自己的身分識別來源 * 權限、可以使用同盟群組和使用者、請為來源和目的地租戶帳戶設定相同的身分識別來源（使用相同的設定）。除非兩個網格使用相同的身分識別來源、否則無法複製同盟群組和使用者。如需相關指示、請參閱 "使用身分識別聯盟"。

3 建立群組和使用者

建立群組和使用者時、請務必從租戶的來源網格開始。當您新增群組時、 StorageGRID 會自動將其複製到目的地網格。

- 如果身分識別聯盟是針對整個 StorageGRID 系統或您的租戶帳戶而設定、 "建立新的租戶群組" 從身分識別來源匯入同盟群組。
- 如果您不使用身分識別聯盟、 "建立新的本機群組" 然後 "建立本機使用者"。

4 建立 **S3** 存取金鑰

您可以 "建立您自己的存取金鑰" 或至 "建立其他使用者的存取金鑰" 在來源網格或目的地網格上存取該網格上的貯體。

5 您也可以選擇複製 **S3** 存取金鑰

如果您需要在兩個網格上存取具有相同存取金鑰的貯體、請在來源網格上建立存取金鑰、然後使用 Tenant Manager API 將它們手動複製到目的地網格。如需相關指示、請參閱 "使用 API 複製 S3 存取金鑰"。

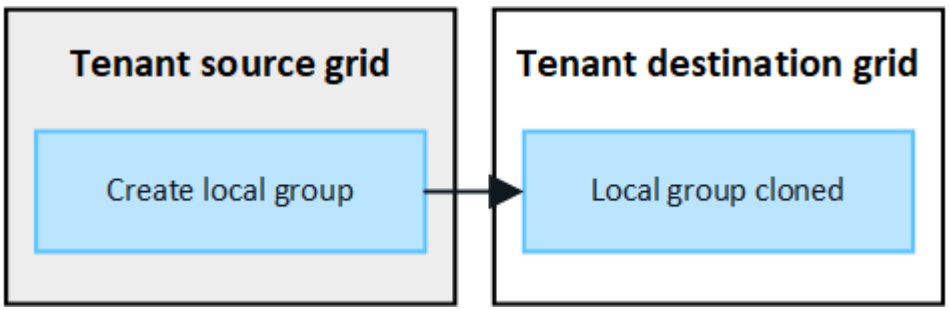
如何複製群組、使用者和 **S3** 存取金鑰？

請參閱本節、瞭解如何在租戶來源網格和租戶目的地網格之間複製群組、使用者和 S3 存取金鑰。

複製在來源網格上建立的本機群組

建立租戶帳戶並複寫到目的地網格之後、 StorageGRID 會自動將您新增至租戶來源網格的任何本機群組、複製到租戶的目的地網格。

原始群組及其複本具有相同的存取模式、群組權限和 S3 群組原則。如需相關指示、請參閱 "為S3租戶建立群組"。

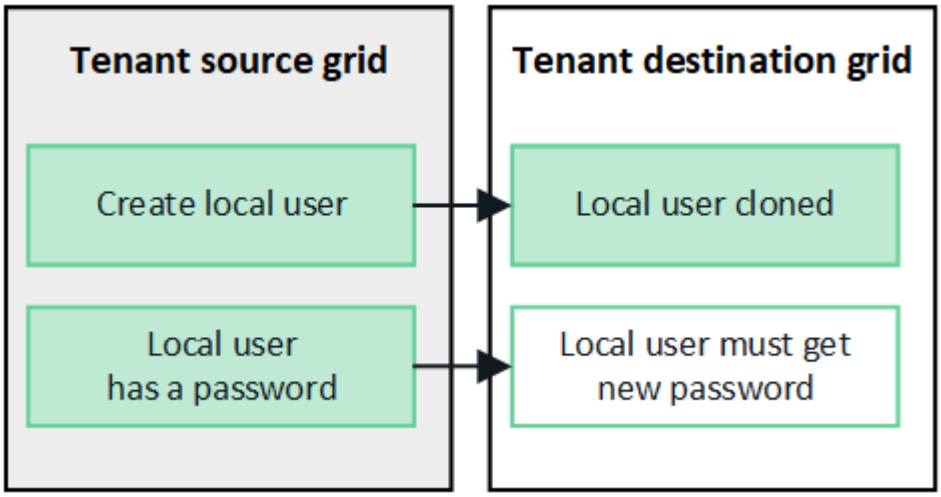


當您在來源網格上建立本機群組時所選取的任何使用者、都不會被複製到目的地網格時納入其中。因此、建立群組時請勿選取使用者。而是在建立使用者時選取群組。

複製在來源網格上建立的本機使用者

當您在來源網格上建立新的本機使用者時、 StorageGRID 會自動將該使用者複製到目的地網格。原始使用者及其複本具有相同的全名、使用者名稱及 * 拒絕存取 * 設定。兩個使用者也屬於同一個群組。如需相關指示、請參閱 "管理本機使用者"。

基於安全考量、本機使用者密碼不會複製到目的地網格。如果本機使用者需要存取目的地網格上的 Tenant Manager 、則租戶帳戶的根使用者必須在目的地網格上新增該使用者的密碼。如需相關指示、請參閱 "管理本機使用者"。

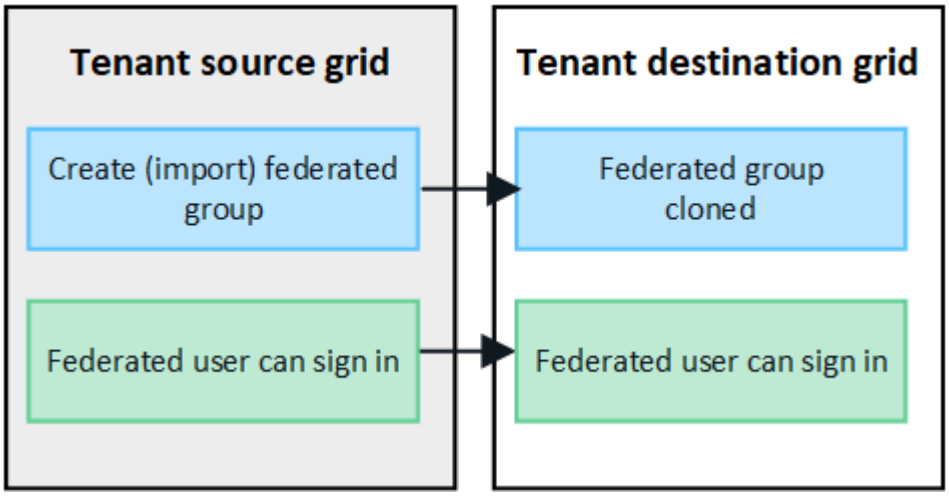


複製在來源網格上建立的同盟群組

假設使用帳戶複製的需求 "單一登入" 和 "身分識別聯盟" 已符合、您在來源網格上為租用戶建立（匯入）的聯盟群組會自動複製到目的地網格上的租用戶。

這兩個群組都有相同的存取模式、群組權限和 S3 群組原則。

為來源租戶建立同盟群組並複製到目的地租戶之後、同盟使用者可以在任一網格上登入租戶。



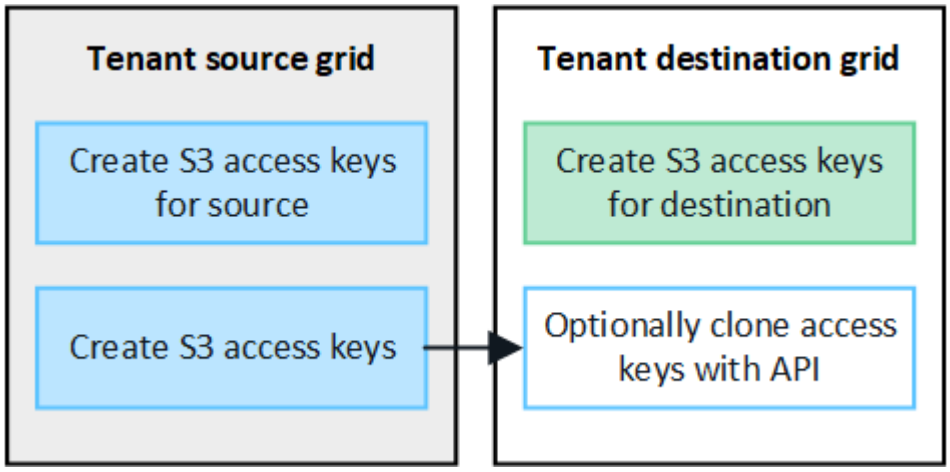
S3 存取金鑰可以手動複製

StorageGRID 不會自動複製 S3 存取金鑰、因為每個網格上都有不同的金鑰、因此安全性得到改善。

若要管理兩個網格上的存取金鑰、您可以執行下列其中一項：

- 如果您不需要對每個網格使用相同的按鍵、您可以 "建立您自己的存取金鑰" 或 "建立其他使用者的存取金鑰" 在每個網格上。
- 如果您需要在兩個網格上使用相同的金鑰、您可以在來源網格上建立金鑰、然後使用 Tenant Manager API

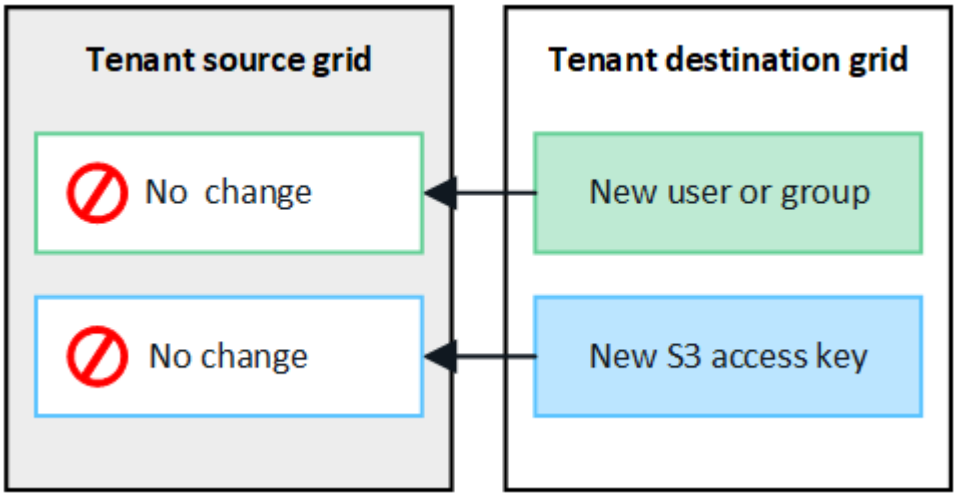
手動建立金鑰 "複製金鑰" 至目的地網格。



當您複製同盟使用者的 S3 存取金鑰時、使用者和 S3 存取金鑰都會複製到目的地租戶。

不會複製新增至目的地網格的群組和使用者

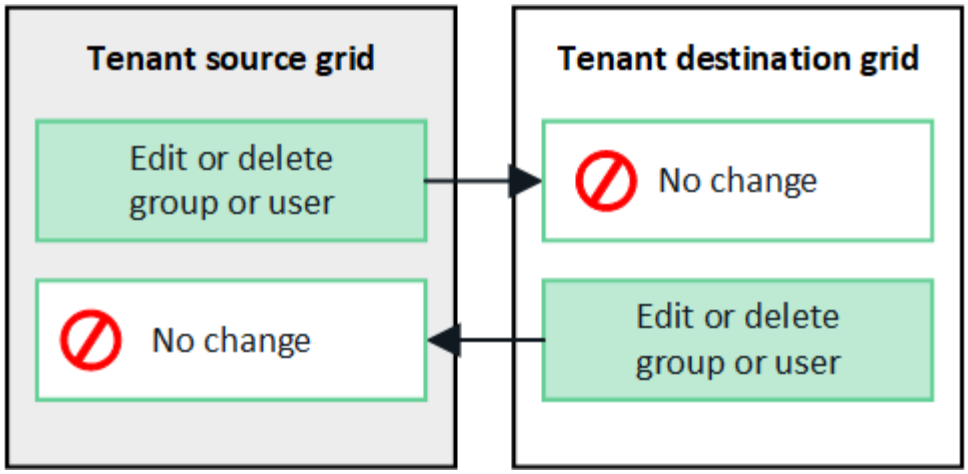
只會從租戶的來源網格到租戶的目的地網格進行複製。如果您在租戶的目的地網格上建立或匯入群組和使用者、StorageGRID 將不會將這些項目複製回租戶的來源網格。



編輯或刪除的群組、使用者和存取金鑰不會複製

只有在您建立新群組和使用者時、才會進行複製。

如果您在任一網格上編輯或刪除群組、使用者或存取金鑰、您的變更將不會複製到其他網格。



使用 **API** 複製 **S3** 存取金鑰

如果您的租戶帳戶具有 * 使用網格同盟連線 * 權限、您可以使用租戶管理 API 、將 S3 存取金鑰從來源網格上的租戶手動複製到目的地網格上的租戶。

開始之前

- 租戶帳戶具有 * 使用網格同盟連線 * 權限。
- 網格聯盟連線的 * 連線狀態 * 為 * 已連線 * 。
- 您可以使用登入租戶來源網格上的租戶管理員 "支援的網頁瀏覽器"。
- 您屬於具有的使用者群組 "管理您自己的 S3 認證或根存取權限"。
- 如果您要複製本機使用者的存取金鑰、則該使用者已存在於兩個網格上。

> 當您複製同盟使用者的 S3 存取金鑰時、使用者和 S3 存取金鑰都會新增至目的地租戶。

複製您自己的存取金鑰

如果您需要存取兩個網格上的相同儲存格、則可以複製自己的存取金鑰。

步驟

1. 在來源網格上使用租戶管理器、 "建立您自己的存取金鑰" 並下載 `.csv` 檔案：
2. 從租戶管理器的頂端、選取說明圖示、然後選取 * API 文件 * 。
3. 在 **S2** 區段中、選取下列端點：

   ```
   POST /org/users/current-user/replicate-s3-access-key
   ```

4. 選擇*試用*。
5. 在 * 本文 * 文字方塊中、將 **AccessKey** 和 **secretAccessKey** 的範例項目取代為您下載的 * 。 csv* 檔案中的值。

   請務必保留每個字串的雙引號。

6. 如果金鑰即將過期、請以 ISO 8601 資料時間格式的字串形式、將 * Expires* 的範例項目取代為過期日期和時間（例如、 `2024-02-28T22:46:33-08:00`）。如果金鑰不會過期、請輸入 * null * 作為 * Expires* 項目的值（或移除 * Expires* 行及前面的逗號）。
7. 選擇*執行*。
8. 確認伺服器回應碼為 **204** 、表示金鑰已成功複製到目的地網格。

複製其他使用者的存取金鑰

如果其他使用者需要存取兩個網格上的相同儲存格、您可以複製該使用者的存取金鑰。

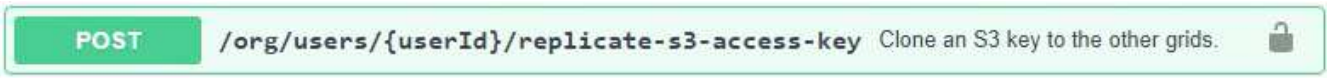
步驟

1. 在來源網格上使用租戶管理器、 "建立其他使用者的 S3 存取金鑰" 並下載 `.csv` 檔案：
2. 從租戶管理器的頂端、選取說明圖示、然後選取 * API 文件 * 。
3. 取得使用者 ID 。您需要此值來複製其他使用者的存取金鑰。
   a. 從 * 使用者 * 區段中、選取下列端點：

      `GET /org/users`

   b. 選擇*試用*。
   c. 指定在查找用戶時要使用的任何參數。
   d. 選擇*執行*。
   e. 尋找您要複製金鑰的使用者、然後在 * id* 欄位中複製該數字。
4. 在 **S2** 區段中、選取下列端點：

   `POST /org/users/{userId}/replicate-s3-access-key`



5. 選擇*試用*。
6. 在 * 使用者 ID* 文字方塊中、貼上您複製的使用者 ID 。
7. 在 * 本文 * 文字方塊中、將 * 範例存取金鑰 * 和 * 秘密存取金鑰 * 的範例項目、取代為該使用者的 * 。 csv* 檔案中的值。

   請務必保留字串周圍的雙引號。

8. 如果金鑰即將過期、請以 ISO 8601 資料時間格式的字串形式、將 * Expires* 的範例項目取代為過期日期和

時間（例如、 `2023-02-28T22:46:33-08:00`）。如果金鑰不會過期、請輸入 * null * 作為 * Expires* 項目的值（或移除 * Expires* 行及前面的逗號）。

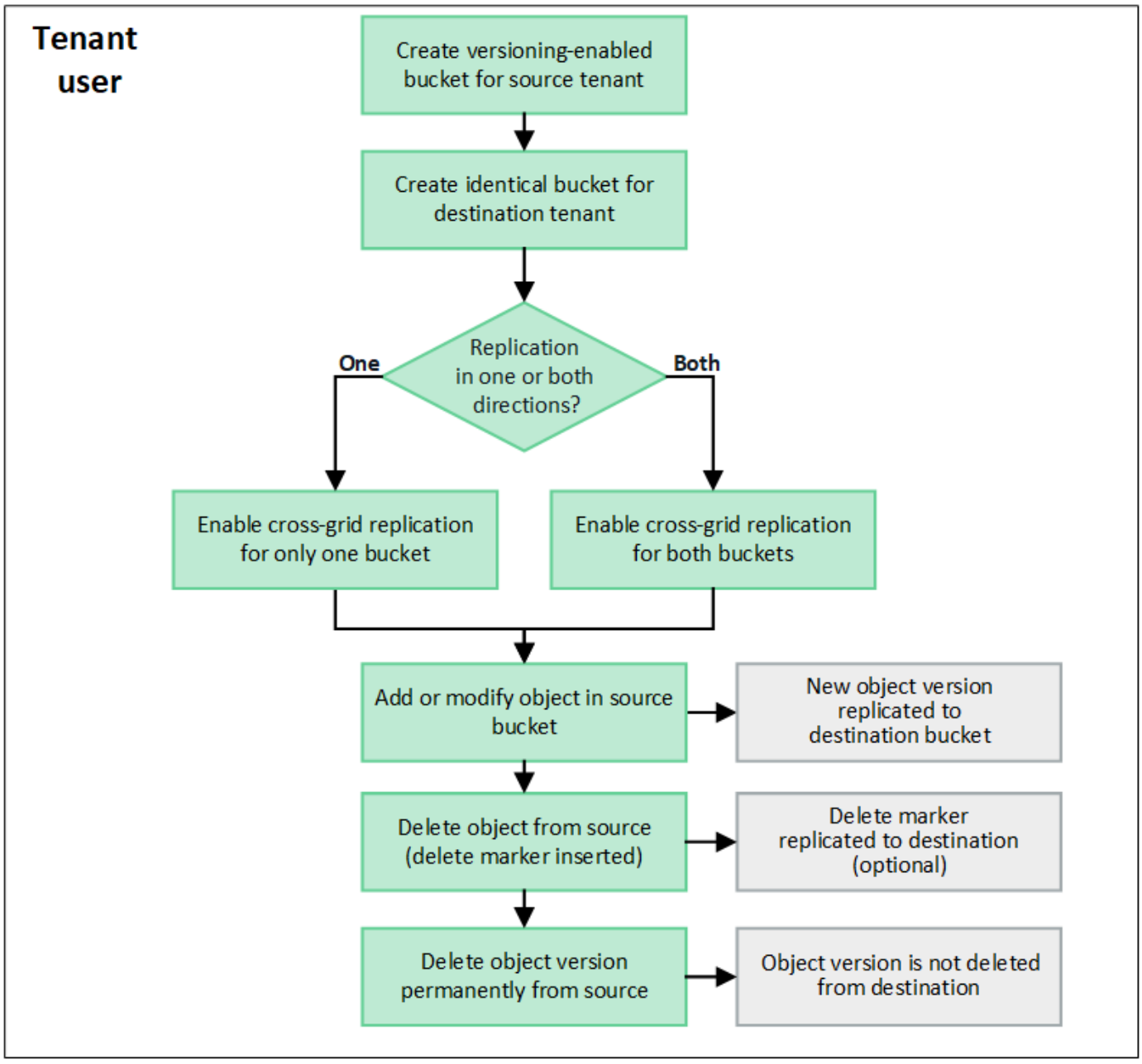
9. 選擇*執行*。
10. 確認伺服器回應碼為 **204** 、表示金鑰已成功複製到目的地網格。

管理跨網格複寫

如果您的租戶帳戶在建立時已獲指派 * 使用網格同盟連線 * 權限、您可以使用跨網格複寫、在租戶來源網格上的貯體和租戶目的地網格上的貯體之間自動複寫物件。跨網格複寫可在一個或兩個方向進行。

跨網格複寫的工作流程

工作流程圖概述了在兩個網格上的貯體之間設定跨網格複寫的步驟。以下將詳細說明這些步驟。



在使用跨網格複寫之前、您必須先登入每個網格上對應的租戶帳戶、然後建立相同的工作區。然後、您可以在任一或兩個貯體上啟用跨網格複寫。

開始之前

- 您已檢閱跨網格複寫的需求。請參閱 "什麼是跨網格複寫"。
- 您使用的是 "支援的網頁瀏覽器"。
- 租戶帳戶具有 * 使用網格同盟連線 * 權限、而且兩個網格上都有相同的租戶帳戶。請參閱 "管理網格同盟連線的允許租戶"。
- 您要登入的租戶使用者已存在於兩個網格上、且屬於具有的使用者群組 "root 存取權限"。
- 如果您將以本機使用者身分登入租戶的目的地網格、則租戶帳戶的 root 使用者已在該網格上為您的使用者帳戶設定密碼。

建立兩個相同的貯體

第一步是登入每個網格上對應的租戶帳戶、然後建立相同的貯體。

步驟

1. 從網格聯盟連線的任一網格開始、建立新的儲存格：
   a. 使用位於兩個網格上的租戶使用者身分證明登入租戶帳戶。

      如果您無法以本機使用者身分登入租戶的目的地網格、請確認租戶帳戶的根使用者已設定您的使用者帳戶密碼。

   b. 請依照的指示進行 "建立 S3 儲存貯體"。
   c. 在 * 管理物件設定 * 索引標籤上、選取 * 啟用物件版本設定 * 。
   d. 如果您的 StorageGRID 系統已啟用 S3 物件鎖定、請勿啟用儲存貯體的 S3 物件鎖定。
   e. 選取*建立桶*。
   f. 選擇*完成*。
2. 重複這些步驟、在 Grid Federation 連線的其他網格上、為相同的租戶帳戶建立相同的貯體。

啟用跨網格複寫

您必須先執行這些步驟、才能將任何物件新增至任一貯體。

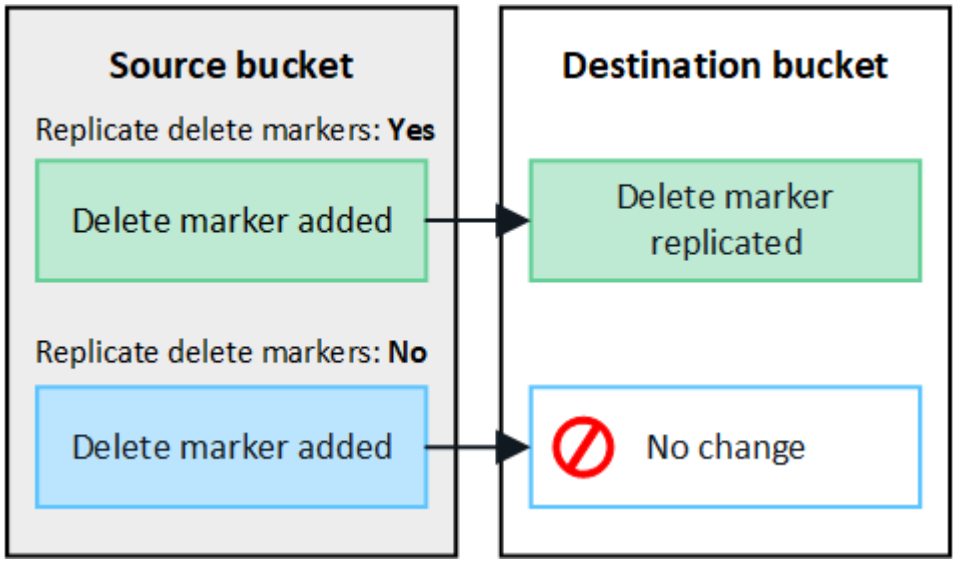
步驟

1. 從您要複寫物件的網格開始、請啟用 "單向跨網格複寫"：
   a. 登入貯體的租戶帳戶。
   b. 從儀表板選取 * 檢視貯體 * 、或選取 * 儲存空間（ S3 ） * > * 鏟斗 * 。
   c. 從表格中選取貯體名稱、以存取貯體詳細資料頁面。
   d. 選取 * 跨網格複寫 * 標籤。
   e. 選取 * 啟用 * 、然後檢閱要求清單。

f. 如果符合所有需求、請選取您要使用的網格同盟連線。

g. 您也可以變更 * 複寫刪除標記 * 的設定、以判斷如果 S3 用戶端向不含版本 ID 的來源網格發出刪除要求、目的地網格上會發生什麼情況：

- 如果 * 是 * （預設）、則會將刪除標記新增至來源貯體、並複寫至目的地貯體。
- 如果 * 否 * 、則會將刪除標記新增至來源貯體、但不會複寫至目的地貯體。



如果刪除要求包含版本 ID 、則該物件版本會從來源貯體中永久移除。StorageGRID 不會複寫包含版本 ID 的刪除要求、因此不會從目的地刪除相同的物件版本。

請參閱 "什麼是跨網格複寫" 以取得詳細資料。

a. 檢閱您的選擇。除非兩個貯體都是空的、否則您無法變更這些設定。

b. 選取 * 啟用和測試 * 。

稍後會出現成功訊息。新增至此貯體的物件現在會自動複寫到其他網格。* 交叉網格複寫 * 會在貯體詳細資料頁面上顯示為啟用的功能。

2. 或者、前往其他網格和上的對應儲存格 "雙向啟用跨網格複寫"。

測試網格之間的複寫

如果已為貯體啟用跨網格複寫、您可能需要驗證連線和跨網格複寫是否正常運作、以及來源和目的地貯體是否仍符合所有需求（例如、版本設定仍為啟用狀態）。

開始之前

- 您使用的是 "支援的網頁瀏覽器"。
- 您屬於具有的使用者群組 "root 存取權限"。

步驟

1. 登入貯體的租戶帳戶。
2. 從儀表板選取 * 檢視貯體 * 、或選取 * 儲存空間（ S3 ） * > * 鏟斗 * 。

3. 從表格中選取貯體名稱、以存取貯體詳細資料頁面。
4. 選取 * 跨網格複寫 * 標籤。
5. 選擇*測試連線*。

   如果連線正常、就會出現成功橫幅。否則會出現錯誤訊息、您和網格管理員可以使用該訊息來解決問題。如需詳細資訊、請參閱 "疑難排解網格同盟錯誤"。

6. 如果跨網格複寫設定為雙向進行、請前往另一個網格上的對應儲存格、然後選取 * 測試連線 * 、確認跨網格複寫在另一個方向上運作。

停用跨網格複寫

如果您不想再將物件複製到其他網格、可以永久停止跨網格複寫。

停用跨網格複寫之前、請注意下列事項：

- 停用跨網格複寫並不會移除已在網格之間複製的任何物件。例如、中的物件 `my-bucket` 已複製到的 On Grid 1 `my-bucket` 如果您停用該貯體的跨網格複寫、則不會移除 On Grid 2 。如果您要刪除這些物件、必須手動移除它們。
- 如果已為每個貯體啟用跨網格複寫（也就是說、如果雙向進行複寫）、您可以停用其中一個或兩個貯體的跨網格複寫。例如、您可能想要停用的複寫物件 `my-bucket` 在網格 1 到 `my-bucket` 在 Grid 2 上、同時繼續從複寫物件 `my-bucket` 在網格 2 到 `my-bucket` 在網格 1 上。
- 您必須先停用跨網格複寫、才能移除租用戶使用網格同盟連線的權限。請參閱 "管理允許的租戶"。
- 如果您停用包含物件之貯體的跨網格複寫、則除非您同時刪除來源和目的地貯體中的所有物件、否則將無法重新啟用跨網格複寫。

> ! 除非兩個儲存區都是空的、否則無法重新啟用複寫。

開始之前

- 您使用的是 "支援的網頁瀏覽器"。
- 您屬於具有的使用者群組 "root 存取權限"。

步驟

1. 從您不再想複寫物件的網格開始、停止貯體的跨網格複寫：
   a. 登入貯體的租戶帳戶。
   b. 從儀表板選取 * 檢視貯體 * 、或選取 * 儲存空間（ S3 ） * > * 鏟斗 * 。
   c. 從表格中選取貯體名稱、以存取貯體詳細資料頁面。
   d. 選取 * 跨網格複寫 * 標籤。
   e. 選取 * 停用複寫 * 。
   f. 如果您確定要停用此貯體的跨網格複寫、請在文字方塊中鍵入 * 是 * 、然後選取 * 停用 * 。

      稍後會出現成功訊息。新增至此貯體的物件無法再自動複寫到其他網格。* 跨網格複寫 * 不再顯示為「已啟用」功能。

2. 如果跨網格複寫設定為雙向進行、請移至另一個網格上的對應儲存格、並在另一個方向停止跨網格複寫。

檢視網格同盟連線

如果您的租戶帳戶具有 * 使用網格同盟連線 * 權限、您可以檢視允許的連線。

開始之前

- 租戶帳戶具有 * 使用網格同盟連線 * 權限。
- 您將使用登入租戶管理程式 "支援的網頁瀏覽器"。
- 您屬於具有的使用者群組 "root 存取權限"。

步驟

1. 選擇 * 儲存設備（ S3 ） * > * 網格聯盟連線 * 。

   此時會出現 Grid Federation 連線頁面、其中包含摘要下列資訊的表格：

欄位	說明
連線名稱	此租用戶有權使用的網格同盟連線。
具有跨網格複寫的貯體	對於每個網格同盟連線、已啟用跨網格複寫的租戶區。新增至這些貯體的物件將會複寫至連線中的其他網格。
上次錯誤	對於每個網格聯盟連線、資料複寫到其他網格時、最新發生的錯誤（如果有）。請參閱 清除最後一個錯誤。

2. 您也可以選擇儲存區名稱 "檢視貯體詳細資料"。

[[Clear-last 錯誤 **]]** 清除最後一個錯誤

下列其中一個原因可能會在 * 最後一個錯誤 * 欄中出現錯誤：

- 找不到來源物件版本。
- 找不到來源貯體。
- 目的地貯體已刪除。
- 目的地貯體是由不同的帳戶重新建立。
- 目的地貯體已暫停版本設定。
- 目的地貯體是由相同的帳戶重新建立、但現在已取消版本管理。

> 此欄只會顯示最後發生的跨網格複寫錯誤、不會顯示先前可能發生的錯誤。

步驟

1. 如果訊息出現在 * 最後一個錯誤 * 欄中、請檢視訊息文字。

   例如、此錯誤表示跨網格複寫的目的地儲存格處於無效狀態、可能是因為版本設定已暫停或啟用 S3 物件鎖

定。

2. 執行任何建議的動作。例如、如果目的地貯體上的版本設定已暫停進行跨網格複寫、請重新啟用該貯體的版本設定。
3. 從表格中選取連線。
4. 選取 * 清除錯誤 * 。
5. 選擇 * 是 * 以清除訊息並更新系統狀態。
6. 等待 5-6 分鐘、然後將新物件擷取到貯體中。確認錯誤訊息不會再次出現。

   若要確保清除錯誤訊息、請在訊息中的時間戳記之後至少等待 5 分鐘、然後再擷取新物件。

7. 若要判斷是否有任何物件因儲存區錯誤而無法複寫、請參閱 "識別並重試失敗的複寫作業"。

管理群組和使用者

使用身分識別聯盟

使用身分識別聯盟可更快設定租戶群組和使用者、並可讓租戶使用者使用熟悉的認證登入租戶帳戶。

設定租戶管理程式的身分識別聯盟

如果您想要在其他系統（例如Active Directory、Azure Active Directory（Azure AD）、OpenLDAP或Oracle Directory Server）中管理租戶群組和使用者、可以為租戶管理程式設定身分識別聯盟。

開始之前

- 您將使用登入租戶管理程式 "支援的網頁瀏覽器"。
- 您屬於具有的使用者群組 "root 存取權限"。
- 您使用Active Directory、Azure AD、OpenLDAP或Oracle Directory Server做為身分識別供應商。

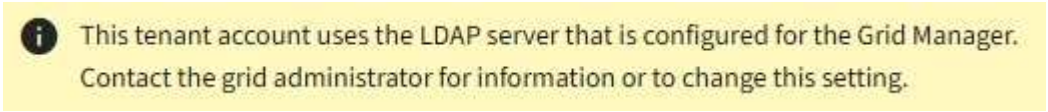
  如果您想使用未列出的LDAP v3服務、請聯絡技術支援部門。

- 如果您打算使用OpenLDAP、則必須設定OpenLDAP伺服器。請參閱 設定OpenLDAP伺服器的準則。

- 如果您打算使用傳輸層安全性（TLS）與LDAP伺服器進行通訊、則身分識別供應商必須使用TLS 1.2或1.3。請參閱 "用於傳出TLS連線的支援密碼"。

關於這項工作

您是否可以為租戶設定身分識別聯盟服務、取決於租戶帳戶的設定方式。您的租戶可能會共用為Grid Manager設定的身分識別聯盟服務。如果您在存取「身分識別聯盟」頁面時看到此訊息、則無法為此租用戶設定個別的同盟身分識別來源。

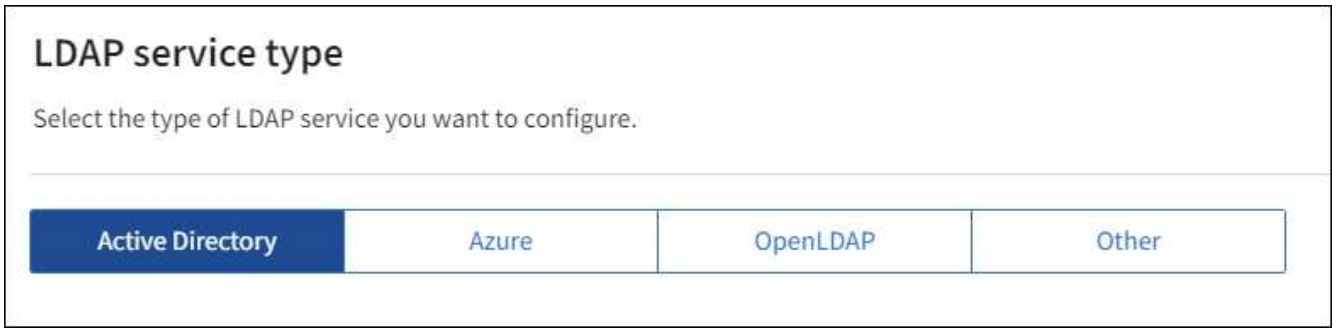


輸入組態

當您設定識別聯盟時、您會提供 StorageGRID 連線至 LDAP 服務所需的值。

步驟

1. 選擇*存取管理*>*身分識別聯盟*。
2. 選取*啟用身分識別聯盟*。
3. 在LDAP服務類型區段中、選取您要設定的LDAP服務類型。



選擇*其他*以設定使用Oracle Directory Server的LDAP伺服器值。

4. 如果選擇*其他*、請填寫「LDAP屬性」區段中的欄位。否則、請前往下一步。
   - 使用者唯一名稱：含有LDAP使用者唯一識別碼的屬性名稱。此屬性相當於 `sAMAccountName` 適用於Active Directory和 `uid` 適用於OpenLDAP。如果您要設定Oracle Directory Server、請輸入 `uid`。
   - *使用者UUID *：含有LDAP使用者永久唯一識別碼的屬性名稱。此屬性相當於 `objectGUID` 適用於Active Directory和 `entryUUID` 適用於OpenLDAP。如果您要設定Oracle Directory Server、請輸入 `nsuniqueid`。指定屬性的每個使用者值必須是16位元組或字串格式的32位數十六進位數字、連字號會被忽略。
   - 群組唯一名稱：包含LDAP群組唯一識別碼的屬性名稱。此屬性相當於 `sAMAccountName` 適用於Active Directory和 `cn` 適用於OpenLDAP。如果您要設定Oracle Directory Server、請輸入 `cn`。
   - *群組UUID *：包含LDAP群組永久唯一識別碼的屬性名稱。此屬性相當於 `objectGUID` 適用於Active Directory和 `entryUUID` 適用於OpenLDAP。如果您要設定Oracle Directory Server、請輸入 `nsuniqueid`。指定屬性的每個群組值必須是16位元組或字串格式的32位數十六進位數字、連字號會被忽略。
5. 對於所有LDAP服務類型、請在「設定LDAP伺服器」區段中輸入所需的LDAP伺服器和網路連線資訊。

- 主機名稱：LDAP伺服器的完整網域名稱（FQDN）或IP位址。
- 連接埠：用於連接LDAP伺服器的連接埠。

  STARTTLS的預設連接埠為389、LDAPS的預設連接埠為636。不過、只要防火牆設定正確、您就可以使用任何連接埠。

- 使用者名稱：將連線至LDAP伺服器之使用者的辨別名稱（DN）完整路徑。

  對於Active Directory、您也可以指定低層級的登入名稱或使用者主要名稱。

  指定的使用者必須擁有列出群組和使用者的權限、並可存取下列屬性：

  - `sAMAccountName` 或 `uid`
  - `objectGUID`、 `entryUUID`或 `nsuniqueid`
  - `cn`
  - `memberOf` 或 `isMemberOf`
  - * Active Directory* ： `objectSid`、 `primaryGroupID`、 `userAccountControl`和 `userPrincipalName`
  - * Azure * ： `accountEnabled` 和 `userPrincipalName`
- 密碼：與使用者名稱相關的密碼。
- 群組基礎**DN**：您要搜尋群組之LDAP子樹狀結構的辨別名稱（DN）完整路徑。在Active Directory範例（如下）中、識別名稱相對於基礎DN（DC=storagegRID、DC=example、DC=com）的所有群組均可做為聯盟群組使用。

  「群組唯一名稱*」值必須在所屬的*群組基礎DN*中是唯一的。

- 使用者基礎**DN**：您要搜尋使用者之LDAP子樹狀目錄的辨別名稱（DN）完整路徑。

  *使用者唯一名稱*值必須在其所屬的*使用者基礎DN*內是唯一的。

- * 連結使用者名稱格式 * （選用）：如果無法自動判斷模式、則應使用預設的使用者名稱模式StorageGRID 。

  建議提供*連結使用者名稱格式*、因為StorageGRID 如果無法連結服務帳戶、使用者可以登入。

  輸入下列其中一種模式：

  - * UserPrincipalName 模式（ Active Directory 和 Azure ） * ： `[USERNAME]@example.com`
  - * 低階登入名稱模式（ Active Directory 和 Azure ） * ： `example\[USERNAME]`
  - * 辨別名稱模式 * ： `CN=[USERNAME],CN=Users,DC=example,DC=com`

    請準確附上所寫的*（使用者名稱）*。

6. 在傳輸層安全性（TLS）區段中、選取安全性設定。

- 使用**ARTTLS**：使用ARTTLS來保護與LDAP伺服器的通訊安全。這是Active Directory、OpenLDAP或其他的建議選項、但Azure不支援此選項。
- 使用**LDAPS**：LDAPS（LDAP over SSL）選項使用TLS建立與LDAP伺服器的連線。您必須為Azure選取此選項。
- 請勿使用**TLS**：StorageGRID 不保護介於整個系統與LDAP伺服器之間的網路流量。Azure不支援此選項。

> 如果Active Directory伺服器強制執行LDAP簽署、則不支援使用*「不使用TLS*」選項。您必須使用ARTTLS或LDAPS。

7. 如果您選取了ARTTLS或LDAPS、請選擇用來保護連線安全的憑證。
   - 使用作業系統**CA**憑證：使用作業系統上安裝的預設Grid CA憑證來保護連線安全。
   - 使用自訂**CA**憑證：使用自訂安全性憑證。

     如果選取此設定、請將自訂安全性憑證複製並貼到CA憑證文字方塊中。

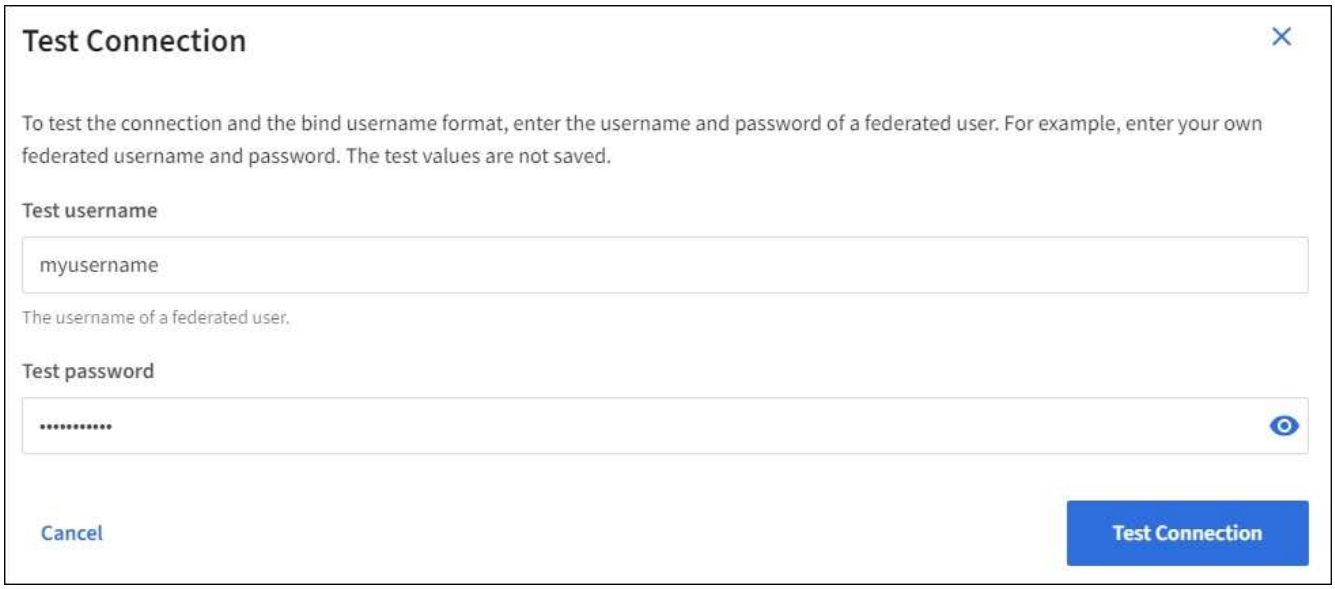
測試連線並儲存組態

輸入所有值之後、您必須先測試連線、才能儲存組態。如果您提供LDAP伺服器的連線設定和連結使用者名稱格式、則可透過此驗證。StorageGRID

步驟

1. 選擇*測試連線*。
2. 如果您未提供連結使用者名稱格式：
   - 如果連線設定有效、則會出現「Test connection Successful（測試連線成功）」訊息。選取*「Save（儲存）」*以儲存組態。
   - 如果連線設定無效、則會出現「test connection Could not be connection…（無法建立測試連線）」訊息。選擇*關閉*。然後、解決所有問題、並再次測試連線。
3. 如果您提供連結使用者名稱格式、請輸入有效同盟使用者的使用者名稱和密碼。

   例如、輸入您自己的使用者名稱和密碼。請勿在使用者名稱中包含任何特殊字元、例如 @ 或 / 。



- 如果連線設定有效、則會出現「Test connection Successful（測試連線成功）」訊息。選取*「Save（儲存）」*以儲存組態。
- 如果連線設定、連結使用者名稱格式或測試使用者名稱和密碼無效、則會出現錯誤訊息。解決所有問題、然後再次測試連線。

強制與身分識別來源同步

此系統會定期同步來自身分識別來源的聯盟群組和使用者。StorageGRID如果您想要盡快啟用或限制使用者權限、可以強制啟動同步。

步驟

1. 前往「身分識別聯盟」頁面。
2. 選取頁面頂端的*同步伺服器*。

   視您的環境而定、同步處理程序可能需要一些時間。

   如果同步處理來自身分識別來源的聯盟群組和使用者時發生問題、則會觸發*身分識別聯盟同步處理失敗*警示。

停用身分識別聯盟

您可以暫時或永久停用群組和使用者的身分識別聯盟。停用身分識別聯盟時StorageGRID 、不會在驗證和身分識別來源之間進行通訊。不過、您已設定的任何設定都會保留下來、讓您日後可以輕鬆重新啟用身分識別聯盟。

關於這項工作

在停用身分識別聯盟之前、您應注意下列事項：

- 聯盟使用者將無法登入。
- 目前已登入的聯盟使用者將在StorageGRID 其工作階段過期之前保留對此系統的存取權、但在工作階段過期後仍無法登入。
- 不會在不同步系統與身分識別來源之間進行同步、StorageGRID 也不會針對尚未同步的帳戶發出警示或警示。

- 如果將單點登錄 (SSO) 設置爲 **Enabled** 或 **Sandbox Mode** ，則禁用 **Enable identity Federation** （啓用身份聯合） * 複選框。「單一登入」頁面的**SSO**狀態必須為*停用、才能停用身分識別聯盟。請參閱 "停用單一登入"。

步驟

1. 前往「身分識別聯盟」頁面。
2. 取消勾選 * 啟用身分識別聯盟 * 核取方塊。

設定**OpenLDAP**伺服器的準則

如果您要使用OpenLDAP伺服器進行身分識別聯盟、則必須在OpenLDAP伺服器上設定特定設定。

> 對於非 ActiveDirectory 或 Azure 的身分識別來源、 StorageGRID 不會自動封鎖 S3 對外部停用使用者的存取。若要封鎖 S3 存取、請刪除使用者的任何 S3 金鑰、或將使用者從所有群組中移除。

memberOf和**refert**覆疊

應啟用memberof和refert覆疊。如需詳細資訊、請參閱中的反轉群組成員資格維護指示http://www.openldap.org/doc/admin24/index.html["OpenLDAP文件：2.4版管理員指南"^]。

索引

您必須使用指定的索引關鍵字來設定下列OpenLDAP屬性：

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

此外、請確定使用者名稱說明中所述的欄位已建立索引、以獲得最佳效能。

請參閱中有關反轉群組成員資格維護的資訊http://www.openldap.org/doc/admin24/index.html["OpenLDAP文件：2.4版管理員指南"^]。

管理租戶群組

為**S3**租戶建立群組

您可以匯入同盟群組或建立本機群組、來管理S3使用者群組的權限。

開始之前

- 您將使用登入租戶管理程式 "支援的網頁瀏覽器"。
- 您屬於具有的使用者群組 "root 存取權限"。
- 如果您計畫匯入同盟群組、您就擁有了 "已設定的身分識別聯盟"，且已設定的身分識別來源中已存在同盟群組。
- 如果您的租戶帳戶具有 * 使用網格同盟連線 * 權限、您已檢閱的工作流程和考量事項 "複製租戶群組和使用

者"，您將登入租戶的來源網格。

存取建立群組精靈

第一步是存取「建立群組」精靈。

步驟

1. 選擇*存取管理*>*群組*。
2. 如果您的租戶帳戶具有 * 使用網格同盟連線 * 權限、請確認出現藍色橫幅、表示在此網格上建立的新群組將會複製到連線中其他網格上的同一個租戶。如果未顯示此橫幅、您可能會登入租戶的目的地網格。

3. 選取*建立群組*。

選擇群組類型

您可以建立本機群組或匯入同盟群組。

步驟

1. 選取*本機群組*索引標籤以建立本機群組、或選取*聯盟群組*索引標籤、從先前設定的身分識別來源匯入群組。

   如果StorageGRID 您的系統啟用單一登入（SSO）、屬於本機群組的使用者將無法登入租戶管理程式、不過他們可以根據群組權限、使用用戶端應用程式來管理租戶的資源。

2. 輸入群組名稱。
   - 本機群組：輸入顯示名稱和唯一名稱。您可以稍後再編輯顯示名稱。

     如果您的租戶帳戶具有 * 使用網格同盟連線 * 權限、則如果目的地網格上的租戶已經存在相同的 * 唯一名稱 * 、就會發生複製錯誤。

   - 聯盟群組：輸入唯一名稱。對於Active Directory、唯一名稱是與相關聯的名稱 `sAMAccountName` 屬性。對於OpenLDAP、唯一名稱是與相關聯的名稱 `uid` 屬性。
3. 選擇*繼續*。

管理群組權限

群組權限可控制使用者可在租戶管理器和租戶管理 API 中執行的工作。

步驟

1. 對於 * 存取模式 * 、請選取下列其中一項：
   - * 讀寫 *（預設）：使用者可以登入租戶管理員並管理租戶組態。
   - 唯讀：使用者只能檢視設定和功能。他們無法在租戶管理員或租戶管理 API 中進行任何變更或執行任何作業。本機唯讀使用者可以變更自己的密碼。

   如果使用者屬於多個群組、且任何群組設定為唯讀、則使用者將擁有所有選取設定和功能的唯讀存取權。

2. 為此群組選取一或多個權限。

   請參閱 "租戶管理權限"。

3. 選擇*繼續*。

設定 **S3** 群組原則

群組原則決定使用者將擁有哪些 S3 存取權限。

步驟

1. 選取您要用於此群組的原則。

群組原則	說明
無 S3 存取權	預設。此群組中的使用者無法存取 S3 資源、除非已透過貯體原則授予存取權限。如果選取此選項、預設只有root使用者可以存取S3資源。
唯讀存取	此群組中的使用者擁有 S3 資源的唯讀存取權。例如、此群組中的使用者可以列出物件並讀取物件資料、中繼資料和標記。選取此選項時、唯讀群組原則的Json字串會出現在文字方塊中。您無法編輯此字串。
完整存取	此群組中的使用者可完全存取 S3 資源、包括貯體。選取此選項時、會在文字方塊中顯示完整存取群組原則的Json字串。您無法編輯此字串。
勒索軟體緩解	此範例原則適用於此租戶的所有貯體。此群組中的使用者可以執行一般動作、但無法從已啟用物件版本設定的儲存區中永久刪除物件。 擁有「 * 管理所有儲存區 * 」權限的租戶管理員使用者可以覆寫此群組原則。將「管理所有貯體」權限限制於信任的使用者、並在可行的情況下使用「多因素驗證」（ MFA ）。
自訂	群組中的使用者會獲得您在文字方塊中指定的權限。

2. 如果您選取*自訂*、請輸入群組原則。每個群組原則的大小上限為5、120位元組。您必須輸入有效的Json格式字串。

   如需群組原則的詳細資訊、包括語言語法和範例、請參閱 "群組原則範例"。

3. 如果您要建立本機群組、請選取*繼續*。如果您要建立聯盟群組、請選取*建立群組*和*完成*。

新增使用者（僅限本機群組）

您可以儲存群組而不新增使用者、也可以選擇性地新增已存在的任何本機使用者。

> 如果您的租戶帳戶具有 * 使用網格同盟連線 * 權限、則當您在來源網格上建立本機群組時、所選取的任何使用者、都不會被複製到目的地網格時納入。因此、建立群組時請勿選取使用者。而是在建立使用者時選取群組。

步驟

1. 您也可以為此群組選取一或多個本機使用者。
2. 選擇* Create group（創建組）和 Finish（完成）*。

   您建立的群組會出現在群組清單中。

   如果您的租戶帳戶具有 * 使用網格同盟連線 * 權限、且您位於租戶的來源網格上、則新群組會複製到租戶的目的地網格。* 成功 * 會在群組詳細資料頁面的「概述」區段中顯示為 * 複製狀態 * 。

為**Swift**租戶建立群組

您可以匯入聯盟群組或建立本機群組、來管理Swift租戶帳戶的存取權限。至少一個群組必須具有Swift Administrator權限、這是管理Swift租戶帳戶的容器和物件所需的權限。

> Swift 用戶端應用程式的支援已過時、未來版本將會移除。

開始之前

- 您將使用登入租戶管理程式 "支援的網頁瀏覽器"。
- 您屬於具有的使用者群組 "root 存取權限"。
- 如果您計畫匯入同盟群組、您就擁有了 "已設定的身分識別聯盟"，且已設定的身分識別來源中已存在同盟群組。

存取建立群組精靈

步驟

第一步是存取「建立群組」精靈。

1. 選擇*存取管理*>*群組*。
2. 選取*建立群組*。

選擇群組類型

您可以建立本機群組或匯入同盟群組。

步驟

1. 選取*本機群組*索引標籤以建立本機群組、或選取*聯盟群組*索引標籤、從先前設定的身分識別來源匯入群組。

   如果StorageGRID 您的系統啟用單一登入（SSO）、屬於本機群組的使用者將無法登入租戶管理程式、不過他們可以根據群組權限、使用用戶端應用程式來管理租戶的資源。

2. 輸入群組名稱。
   - 本機群組：輸入顯示名稱和唯一名稱。您可以稍後再編輯顯示名稱。
   - 聯盟群組：輸入唯一名稱。對於Active Directory、唯一名稱是與相關聯的名稱 `sAMAccountName` 屬性。對於OpenLDAP、唯一名稱是與相關聯的名稱 `uid` 屬性。
3. 選擇*繼續*。

管理群組權限

群組權限可控制使用者可在租戶管理器和租戶管理 API 中執行的工作。

步驟

1. 對於 * 存取模式 * 、請選取下列其中一項：
   - * 讀寫 *（預設）：使用者可以登入租戶管理員並管理租戶組態。
   - 唯讀：使用者只能檢視設定和功能。他們無法在租戶管理員或租戶管理 API 中進行任何變更或執行任何作業。本機唯讀使用者可以變更自己的密碼。

   > ⓘ 如果使用者屬於多個群組、且任何群組設定為唯讀、則使用者將擁有所有選取設定和功能的唯讀存取權。

2. 如果群組使用者需要登入租戶管理員或租戶管理 API 、請選取 * 根存取 * 核取方塊。
3. 選擇*繼續*。

設定 **Swift** 群組原則

Swift 使用者需要系統管理員權限才能驗證 Swift REST API 、以建立容器和擷取物件。

1. 如果群組使用者需要使用 Swift REST API 來管理容器和物件、請選取 * Swift 管理員 * 核取方塊。
2. 如果您要建立本機群組、請選取*繼續*。如果您要建立聯盟群組、請選取*建立群組*和*完成*。

新增使用者（僅限本機群組）

您可以儲存群組而不新增使用者、也可以選擇性地新增已存在的任何本機使用者。

步驟

1. 您也可以為此群組選取一或多個本機使用者。

如果您尚未建立本機使用者、可以在「使用者」頁面上將此群組新增至使用者。請參閱 "管理本機使用者"。

2. 選擇* Create group（創建組）和 Finish（完成）*。

   您建立的群組會出現在群組清單中。

租戶管理權限

建立租戶群組之前、請先考量您要指派給該群組的權限。租戶管理權限可決定使用者可以使用租戶管理程式或租戶管理API執行哪些工作。使用者可以屬於一或多個群組。如果使用者屬於多個群組、則權限是累積性的。

若要登入租戶管理程式或使用租戶管理API、使用者必須屬於至少擁有一項權限的群組。所有可以登入的使用者都可以執行下列工作：

- 檢視儀表板
- 變更自己的密碼（適用於本機使用者）

對於所有權限、群組的存取模式設定會決定使用者是否可以變更設定及執行作業、或是只能檢視相關設定和功能。

> 如果使用者屬於多個群組、且任何群組設定為唯讀、則使用者將擁有所有選取設定和功能的唯讀存取權。

您可以將下列權限指派給群組。請注意、S3租戶和Swift租戶擁有不同的群組權限。

權限	說明
root存取權	提供租戶管理程式和租戶管理API的完整存取權限。 • 附註： * Swift 使用者必須擁有 root 存取權限、才能登入租戶帳戶。
系統管理員	僅限Swift租戶。提供此租戶帳戶的Swift容器和物件的完整存取權 附註： Swift使用者必須擁有Swift管理員權限、才能使用Swift REST API執行任何作業。
管理您自己的 S3 認證	可讓使用者建立及移除自己的S3存取金鑰。沒有此權限的使用者不會看到 * 儲存設備（ S3 ） * > * My S3 存取鍵 * 功能表選項。

權限	說明
管理所有貯體	• S3租戶：可讓使用者使用租戶管理程式和租戶管理API來建立及刪除S3桶、並管理租戶帳戶中所有S3桶的設定、無論S3桶或群組原則為何。 沒有此權限的使用者不會看到 * 「鏟斗」 * 功能表選項。 • Swift租戶：可讓Swift使用者使用租戶管理API來控制Swift Container的一致性層級。 • 注意： * 您只能從租戶管理 API 將「管理所有貯體」權限指派給 Swift 群組。您無法使用 Tenant Manager 將此權限指派給 Swift 群組。
管理端點	可讓使用者使用租戶管理器或租戶管理 API 來建立或編輯平台服務端點、這些端點是 StorageGRID 平台服務的目的地。 沒有此權限的使用者不會看到 * 平台服務端點 * 功能表選項。
使用 S3 主控台管理物件	結合「管理所有貯體」權限、可讓使用者從「貯體」頁面存取實驗 S3 主控台。擁有此權限但沒有「管理所有儲存區」權限的使用者仍可直接瀏覽至實驗 S3 主控台。

管理群組

您可以檢視群組、編輯群組的名稱、權限、原則和使用者、複製群組； 或刪除群組。

開始之前

- 您將使用登入租戶管理程式 "支援的網頁瀏覽器"。
- 您屬於具有的使用者群組 "root 存取權限"。

檢視或編輯群組

您可以檢視和編輯每個群組的基本資訊和詳細資料。

步驟

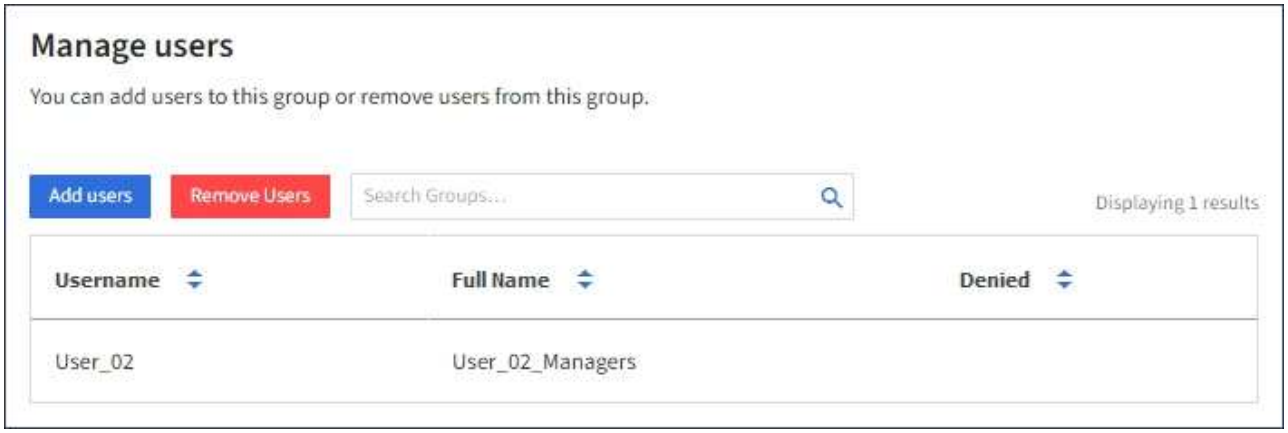
1. 選擇*存取管理*>*群組*。
2. 檢閱「群組」頁面上提供的資訊、其中列出此租戶帳戶所有本機和同盟群組的基本資訊。

   如果租戶帳戶具有 * 使用網格同盟連線 * 權限、且您正在租戶來源網格上檢視群組、則藍色橫幅會指出、如果您編輯或移除群組、您的變更將不會同步到其他網格。請參閱 "複製租戶群組和使用者"。

3. 如果您要變更群組名稱：
   a. 選取群組的核取方塊。
   b. 選擇*操作*>*編輯群組名稱*。
   c. 輸入新名稱。
   d. 選取 * 儲存變更 *
4. 如果您想要檢視更多詳細資料或進行其他編輯、請執行下列其中一項：

- 選取群組名稱。
- 選取群組的核取方塊、然後選取 * 動作 * > * 檢視群組詳細資料 * 。

5. 檢閱「總覽」一節、其中顯示每個群組的下列資訊：
   - 顯示名稱
   - 唯一名稱
   - 類型
   - 存取模式
   - 權限
   - S3 原則
   - 此群組中的使用者數目
   - 如果租戶帳戶具有「 * 使用網格同盟連線 * 」權限、且您正在租戶來源網格上檢視群組、則會顯示其他欄位：
     - 克隆狀態，可以是 * 成功 * 或 * 失敗 *
     - 藍色橫幅表示如果您編輯或刪除此群組、您的變更將不會同步至其他網格。
6. 視需要編輯群組設定。請參閱 "為S3租戶建立群組" 和 "為Swift租戶建立群組" 以取得有關輸入內容的詳細資訊。
   a. 在「總覽」區段中、選取名稱或編輯圖示以變更顯示名稱 。
   b. 在 * 群組權限 * 索引標籤上、更新權限、然後選取 * 儲存變更 * 。
   c. 在 * 群組原則 * 索引標籤上、進行任何變更、然後選取 * 儲存變更 * 。
      - 如果您正在編輯 S3 群組、請視需要選擇不同的 S3 群組原則、或輸入自訂原則的 JSON 字串。
      - 如果您正在編輯 Swift 群組、請選擇或清除 **Swift Administrator** 核取方塊。
7. 若要將一或多個現有的本機使用者新增至群組：
   a. 選取使用者索引標籤。



   b. 選取 * 新增使用者 * 。
   c. 選取您要新增的現有使用者、然後選取 * 新增使用者 * 。

      右上角會出現成功訊息。

8. 若要從群組中移除本機使用者：
   a. 選取使用者索引標籤。
   b. 選取 * 移除使用者 * 。
   c. 選取您要移除的使用者、然後選取 * 移除使用者 * 。

      右上角會出現成功訊息。
9. 確認您為變更的每個區段選擇了 * 儲存變更 * 。

複製群組

您可以複製現有群組、以更快建立新群組。

> 如果您的租戶帳戶具有 * 使用網格同盟連線 * 權限、而且您從租戶的來源網格複製群組、則複製的群組將會複製到租戶的目的地網格。

步驟

1. 選擇*存取管理*>*群組*。
2. 選取您要複製之群組的核取方塊。
3. 選取*「動作*」>*「重複群組*」。
4. 請參閱 "為S3租戶建立群組" 或 "為Swift租戶建立群組" 以取得有關輸入內容的詳細資訊。
5. 選取*建立群組*。

刪除一或多個群組

您可以刪除一或多個群組。只屬於已刪除群組的任何使用者將無法再登入租戶管理員或使用租戶帳戶。

> 如果您的租戶帳戶具有 * 使用網格同盟連線 * 權限、而且您刪除了群組、 StorageGRID 將不會刪除其他網格上的對應群組。如果您需要保持此資訊同步、您必須從兩個方格中刪除相同的群組。

步驟

1. 選擇*存取管理*>*群組*。
2. 選取您要刪除的每個群組的核取方塊。
3. 選擇 * 行動 * > * 刪除群組 * 或 * 行動 * > * 刪除群組 * 。

   隨即顯示確認對話方塊。
4. 選取 * 刪除群組 * 或 * 刪除群組 * 。

管理本機使用者

您可以建立本機使用者並將其指派給本機群組、以決定這些使用者可以存取哪些功能。租戶管理程式包含一個預先定義的本機使用者、名為「 root 」。 雖然您可以新增及移除本機使用者、但無法移除根使用者。

如果您的 StorageGRID 系統啟用單一登入（ SSO ）、本機使用者將無法登入租戶管理員或租戶管理 API 、不過他們可以根據群組權限使用用戶端應用程式來存取租戶的資源。

開始之前

- 您將使用登入租戶管理程式 "支援的網頁瀏覽器"。
- 您屬於具有的使用者群組 "root 存取權限"。
- 如果您的租戶帳戶具有 * 使用網格同盟連線 * 權限、您已檢閱的工作流程和考量事項 "複製租戶群組和使用者"，您將登入租戶的來源網格。

建立本機使用者

您可以建立本機使用者並將其指派給一或多個本機群組、以控制其存取權限。

不屬於任何群組的 S3 使用者沒有管理權限或 S3 群組原則套用到他們。這些使用者可能會透過儲存區原則授予S3儲存區存取權。

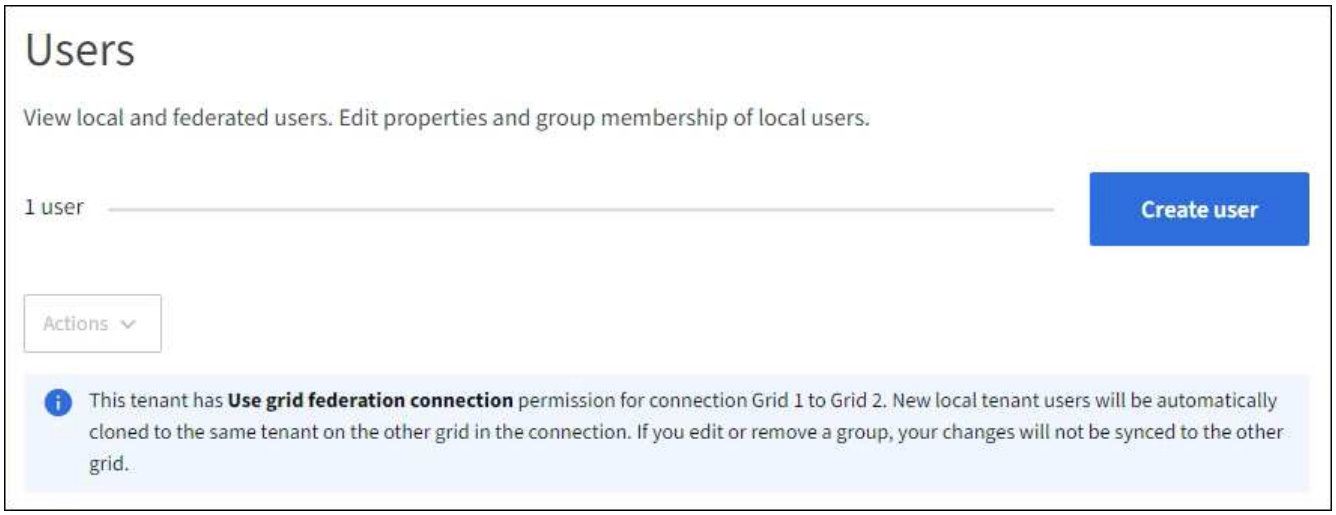
不屬於任何群組的 Swift 使用者沒有管理權限或 Swift Container 存取權。

存取建立使用者精靈

步驟

1. 選擇*存取管理*>*使用者*。

   如果您的租戶帳戶具有 * 使用網格同盟連線 * 權限、則藍色橫幅會指出這是租戶的來源網格。您在此網格上建立的任何本機使用者都會複製到連線中的其他網格。



2. 選取*建立使用者*。

輸入認證

步驟

1. 對於 * 輸入使用者認證 * 步驟、請填寫下列欄位。

欄位	說明
全名	此使用者的全名、例如人員的名字和姓氏、或應用程式的名稱。
使用者名稱	此使用者將用來登入的名稱。使用者名稱必須是唯一的、而且無法變更。 • 附註 * ：如果您的租戶帳戶具有 * 使用網格同盟連線 * 權限、則如果目的地網格上的租戶已經存在相同的 * 使用者名稱 * 、就會發生複製錯誤。
密碼和確認密碼	使用者在登入時最初使用的密碼。
拒絕存取	選取 * 是 * 可防止此使用者登入租戶帳戶、即使他們仍屬於一個或多個群組。 例如、選取 * 是 * 可暫時暫停使用者登入的能力。

2. 選擇*繼續*。

指派給群組

步驟

1. 將使用者指派給一或多個本機群組、以判斷他們可以執行哪些工作。

   將使用者指派給群組是選擇性的。如果您願意、可以在建立或編輯群組時選取使用者。

   不屬於任何群組的使用者將沒有管理權限。權限是累積性的。使用者將擁有所屬所有群組的所有權限。請參閱 "租戶管理權限"。

2. 選取*建立使用者*。

   如果您的租戶帳戶具有 * 使用網格同盟連線 * 權限、且您位於租戶的來源網格上、則新的本機使用者會複製到租戶的目的地網格。* 成功 * 會在使用者詳細資料頁面的「概述」區段中顯示為 * 複製狀態 * 。

3. 選擇 * 完成 * 返回「使用者」頁面。

檢視或編輯本機使用者

步驟

1. 選擇*存取管理*>*使用者*。
2. 檢閱「使用者」頁面上提供的資訊、其中列出此租戶帳戶所有本機和同盟使用者的基本資訊。

   如果租戶帳戶具有 * 使用網格同盟連線 * 權限、且您正在租戶來源網格上檢視使用者、則藍色橫幅會指出、如果您編輯或移除使用者、您的變更將不會同步到其他網格。

3. 若要變更使用者的全名：
   a. 選取使用者的核取方塊。
   b. 選擇* Actions > Edit full name*（操作>*編輯全名*）。
   c. 輸入新名稱。

d. 選取 * 儲存變更 *

4. 如果您想要檢視更多詳細資料或進行其他編輯、請執行下列其中一項：
   - 選取使用者名稱。
   - 選取使用者的核取方塊、然後選取 * 動作 * > * 檢視使用者詳細資料 * 。
5. 檢閱「總覽」一節、其中顯示每位使用者的下列資訊：
   - 全名
   - 使用者名稱
   - 使用者類型
   - 拒絕存取
   - 存取模式
   - 群組成員資格
   - 如果租戶帳戶具有「 * 使用網格同盟連線 * 」權限、且您正在租戶來源網格上檢視使用者、則會顯示其他欄位：
     - 克隆狀態，可以是 * 成功 * 或 * 失敗 *
     - 藍色橫幅表示如果您編輯此使用者、您的變更將不會同步至其他網格。
6. 視需要編輯使用者設定。請參閱 建立本機使用者 以取得有關輸入內容的詳細資訊。
   a. 在「總覽」區段中、選取名稱或編輯圖示以變更全名 。

      您無法變更使用者名稱。

   b. 在 * 密碼 * 標籤上、變更使用者的密碼、然後選取 * 儲存變更 * 。
   c. 在 * 存取 * 索引標籤上、選取 * 否 * 以允許使用者登入、或選取 * 是 * 以防止使用者登入。然後選取 * 儲存變更 * 。
   d. 在 * 存取金鑰 * 索引標籤上、選取 * 建立金鑰 * 、然後依照的指示進行 "建立其他使用者的 S3 存取金鑰 "。
   e. 在 * 群組 * 索引標籤上、選取 * 編輯群組 * 、將使用者新增至群組或從群組中移除使用者。然後選取 * 儲存變更 * 。
7. 確認您為變更的每個區段選擇了 * 儲存變更 * 。

重複的本機使用者

您可以複製本機使用者、以更快建立新使用者。

> 如果您的租戶帳戶具有 * 使用網格同盟連線 * 權限、且您從租戶的來源網格複製使用者、則複製的使用者將會複製到租戶的目的地網格。

步驟

1. 選擇*存取管理*>*使用者*。
2. 選取您要複製之使用者的核取方塊。
3. 選取*「動作*」>*「重複使用者*」。

4. 請參閱 建立本機使用者 以取得有關輸入內容的詳細資訊。
5. 選取*建立使用者*。

刪除一或多個本機使用者

您可以永久刪除不再需要存取 StorageGRID 租戶帳戶的一或多個本機使用者。

如果您的租戶帳戶具有 * 使用網格同盟連線 * 權限、且您刪除了本機使用者、 StorageGRID 將不會刪除其他網格上的對應使用者。如果您需要保持此資訊同步、則必須從兩個方格中刪除相同的使用者。

您必須使用同盟識別來源來刪除同盟使用者。

步驟

1. 選擇*存取管理*>*使用者*。
2. 選取您要刪除的每個使用者的核取方塊。
3. 選擇 * 行動 * > * 刪除使用者 * 或 * 行動 * > * 刪除使用者 * 。

   隨即顯示確認對話方塊。

4. 選取 * 刪除使用者 * 或 * 刪除使用者 * 。

管理S3存取金鑰

管理 **S3** 存取金鑰：總覽

S3租戶帳戶的每位使用者都必須擁有存取金鑰、才能在StorageGRID 這個系統中儲存及擷取物件。存取金鑰包含存取金鑰ID和秘密存取金鑰。

S3存取金鑰的管理方式如下：

- 擁有 * 管理您自己的 S3 認證 * 權限的使用者可以建立或移除自己的 S3 存取金鑰。
- 擁有 * 根存取 * 權限的使用者可以管理 S3 根帳戶和所有其他使用者的存取金鑰。根存取金鑰可讓租戶完整存取所有的貯體和物件、除非已明確停用貯體原則。

支援簽名版本2和簽名版本4驗證。StorageGRID除非庫位原則明確啟用、否則不允許跨帳戶存取。

建立自己的**S3**存取金鑰

如果您使用的是S3租戶、而且您擁有適當的權限、則可以建立自己的S3存取金鑰。您必須擁有存取金鑰才能存取您的貯體和物件。

開始之前

- 您將使用登入租戶管理程式 "支援的網頁瀏覽器"。
- 您屬於具有的使用者群組 "管理您自己的 S3 認證或根存取權限"。

關於這項工作

您可以建立一或多個S3存取金鑰、以便為租戶帳戶建立及管理貯體。建立新的存取金鑰之後、請使用新的存取金鑰ID和秘密存取金鑰來更新應用程式。為了安全起見、請勿建立超出您所需的金鑰、並刪除您未使用的金鑰。如果您只有一個金鑰即將過期、請在舊金鑰過期之前建立新金鑰、然後刪除舊金鑰。

每個金鑰都可以有特定的到期時間、或是沒有到期時間。請遵循下列到期時間準則：

- 設定金鑰的到期時間、將存取限制在特定時間段內。如果您的存取金鑰ID和秘密存取金鑰意外暴露、設定短的到期時間有助於降低風險。過期的金鑰會自動移除。
- 如果環境中的安全風險較低、而且您不需要定期建立新金鑰、就不需要設定金鑰的到期時間。如果您決定稍後再建立新金鑰、請手動刪除舊金鑰。

> 您可以使用租戶管理程式中顯示的帳戶存取金鑰ID和秘密存取金鑰、來存取屬於您帳戶的S3儲存區和物件。因此、請像保護密碼一樣保護存取金鑰。定期旋轉存取金鑰、從帳戶中移除任何未使用的金鑰、而且切勿與其他使用者共用。

步驟

1. 選擇*儲存設備（S3）>*我的存取金鑰。

   「我的存取金鑰」頁面隨即出現、並列出任何現有的存取金鑰。

2. 選取*建立金鑰*。
3. 執行下列其中一項：
   - 選取*不要設定到期時間*以建立不會過期的金鑰。（預設）
   - 選取*設定到期時間*、然後設定到期日和時間。

     > 到期日最長可為從目前日期算起的五年。到期時間最短可從目前時間開始一分鐘。

4. 選取*建立存取金鑰*。

   此時會出現「下載存取金鑰」對話方塊、列出您的存取金鑰ID和秘密存取金鑰。

5. 將存取金鑰ID和秘密存取金鑰複製到安全位置、或選取*下載.csv*以儲存內含存取金鑰ID和秘密存取金鑰的試算表檔案。

   > 在複製或下載此資訊之前、請勿關閉此對話方塊。對話方塊關閉後、您無法複製或下載金鑰。

6. 選擇*完成*。

   新金鑰會列在「我的存取金鑰」頁面上。

7. 如果您的租戶帳戶具有 * 使用網格同盟連線 * 權限、請選擇性使用租戶管理 API 、將 S3 存取金鑰從來源網格上的租戶手動複製到目的地網格上的租戶。請參閱 "使用 API 複製 S3 存取金鑰"。

檢視您的**S3**存取金鑰

如果您使用的是S3租戶、而且您擁有適當的權限、則可以檢視S3存取金鑰的清單。您可以依到期時間排序清單、以便判斷哪些金鑰即將到期。如有需要、您可以 "建立新金鑰" 或 "

刪除金鑰" 不再使用。

> 您可以使用租戶管理程式中顯示的帳戶存取金鑰ID和秘密存取金鑰、來存取屬於您帳戶的S3儲存區和物件。因此、請像保護密碼一樣保護存取金鑰。定期旋轉存取金鑰、從帳戶中移除任何未使用的金鑰、而且切勿與其他使用者共用。

開始之前

- 您將使用登入租戶管理程式 "支援的網頁瀏覽器"。
- 您屬於擁有「管理您自己的 S3 認證」的使用者群組 "權限"。

步驟

1. 選擇*儲存設備（S3）>*我的存取金鑰。
2. 從「我的存取金鑰」頁面、依 * 到期時間 * 或 * 存取金鑰 ID* 來排序任何現有的存取金鑰。
3. 視需要建立新金鑰或刪除不再使用的任何金鑰。

   如果您在現有金鑰過期之前建立新金鑰、您可以開始使用新金鑰、而不會暫時失去帳戶中物件的存取權。

   過期的金鑰會自動移除。

刪除您自己的**S3**存取金鑰

如果您使用的是S3租戶、而且您擁有適當的權限、則可以刪除自己的S3存取金鑰。刪除存取金鑰之後、就無法再使用它來存取租戶帳戶中的物件和儲存區。

開始之前

- 您將使用登入租戶管理程式 "支援的網頁瀏覽器"。
- 您擁有「管理自己的S3認證」權限。請參閱 "租戶管理權限"。

> 您可以使用租戶管理程式中顯示的帳戶存取金鑰ID和秘密存取金鑰、來存取屬於您帳戶的S3儲存區和物件。因此、請像保護密碼一樣保護存取金鑰。定期旋轉存取金鑰、從帳戶中移除任何未使用的金鑰、而且切勿與其他使用者共用。

步驟

1. 選擇*儲存設備（S3）>*我的存取金鑰。
2. 從「我的存取金鑰」頁面、選取您要移除的每個存取金鑰核取方塊。
3. 選取*刪除機碼*。
4. 從確認對話方塊中、選取 * 刪除機碼 * 。

   頁面右上角會出現確認訊息。

建立其他使用者的**S3**存取金鑰

如果您使用的是S3租戶、而且您擁有適當的權限、則可以為其他使用者建立S3存取金鑰、例如需要存取儲存區和物件的應用程式。

開始之前

- 您將使用登入租戶管理程式 "支援的網頁瀏覽器"。
- 您屬於具有的使用者群組 "root 存取權限"。

關於這項工作

您可以為其他使用者建立一或多個S3存取金鑰、以便他們為租戶帳戶建立及管理貯體。建立新的存取金鑰之後、請使用新的存取金鑰ID和秘密存取金鑰來更新應用程式。為了安全起見、請勿建立超出使用者需求的金鑰、並刪除未使用的金鑰。如果您只有一個金鑰即將過期、請在舊金鑰過期之前建立新金鑰、然後刪除舊金鑰。

每個金鑰都可以有特定的到期時間、或是沒有到期時間。請遵循下列到期時間準則：

- 設定金鑰的到期時間、以限制使用者存取特定時間段。如果存取金鑰ID和秘密存取金鑰意外暴露、設定短的過期時間有助於降低風險。過期的金鑰會自動移除。
- 如果環境中的安全風險較低、而且您不需要定期建立新金鑰、就不需要設定金鑰的到期時間。如果您決定稍後再建立新金鑰、請手動刪除舊金鑰。

> ⓘ 您可以使用租戶管理程式中顯示的該使用者存取金鑰ID和秘密存取金鑰、來存取屬於該使用者的S3儲存區和物件。因此、請像保護密碼一樣保護存取金鑰。定期旋轉存取金鑰、從帳戶中移除任何未使用的金鑰、而且切勿與其他使用者共用。

步驟

1. 選擇*存取管理*>*使用者*。
2. 選取您要管理其S3存取金鑰的使用者。

   使用者詳細資料頁面隨即出現。
3. 選取*存取金鑰*、然後選取*建立金鑰*。
4. 執行下列其中一項：
   - 選取 * 不要設定到期時間 * 來建立不會過期的金鑰。（預設）
   - 選取*設定到期時間*、然後設定到期日和時間。

     > ⓘ 到期日最長可為從目前日期算起的五年。到期時間最短可從目前時間開始一分鐘。
5. 選取*建立存取金鑰*。

   此時會出現「下載存取金鑰」對話方塊、列出存取金鑰ID和秘密存取金鑰。
6. 將存取金鑰ID和秘密存取金鑰複製到安全位置、或選取*下載.csv*以儲存內含存取金鑰ID和秘密存取金鑰的試算表檔案。

   > ⓘ 在複製或下載此資訊之前、請勿關閉此對話方塊。對話方塊關閉後、您無法複製或下載金鑰。
7. 選擇*完成*。

   新金鑰會列在使用者詳細資料頁面的「存取金鑰」索引標籤上。

8. 如果您的租戶帳戶具有 * 使用網格同盟連線 * 權限、請選擇性使用租戶管理 API 、將 S3 存取金鑰從來源網格上的租戶手動複製到目的地網格上的租戶。請參閱 "使用 API 複製 S3 存取金鑰"。

檢視其他使用者的**S3**存取金鑰

如果您使用的是S3租戶、而且您擁有適當的權限、則可以檢視其他使用者的S3存取金鑰。您可以依到期時間排序清單、以便判斷哪些金鑰即將到期。您可以視需要建立新的金鑰、並刪除不再使用的金鑰。

開始之前

- 您將使用登入租戶管理程式 "支援的網頁瀏覽器"。
- 您擁有root存取權限。

> 您可以使用租戶管理程式中顯示的該使用者存取金鑰ID和秘密存取金鑰、來存取屬於該使用者的S3儲存區和物件。因此、請像保護密碼一樣保護存取金鑰。定期旋轉存取金鑰、從帳戶中移除任何未使用的金鑰、而且切勿與其他使用者共用。

步驟

1. 選擇*存取管理*>*使用者*。
2. 從「使用者」頁面中、選取您要檢視其 S3 存取金鑰的使用者。
3. 從「使用者詳細資料」頁面、選取 * 存取金鑰 * 。
4. 按*過期時間*或*存取金鑰ID*來排序金鑰。
5. 視需要建立新金鑰、並手動刪除不再使用的金鑰。

   如果您在現有金鑰過期之前建立新金鑰、使用者可以開始使用新金鑰、而不會暫時失去帳戶中物件的存取權。

   過期的金鑰會自動移除。

相關資訊

"建立另一個使用者的S3存取金鑰"

"刪除其他使用者的S3存取金鑰"

刪除其他使用者的**S3**存取金鑰

如果您使用的是S3租戶、而且您擁有適當的權限、則可以刪除其他使用者的S3存取金鑰。刪除存取金鑰之後、就無法再使用它來存取租戶帳戶中的物件和儲存區。

開始之前

- 您將使用登入租戶管理程式 "支援的網頁瀏覽器"。
- 您擁有root存取權限。請參閱 "租戶管理權限"。

您可以使用租戶管理程式中顯示的該使用者存取金鑰ID和秘密存取金鑰、來存取屬於該使用者的S3儲存區和物件。因此、請像保護密碼一樣保護存取金鑰。定期旋轉存取金鑰、從帳戶中移除任何未使用的金鑰、而且切勿與其他使用者共用。

步驟

1. 選擇*存取管理*>*使用者*。
2. 從「使用者」頁面中、選取您要管理其 S3 存取金鑰的使用者。
3. 從「使用者詳細資料」頁面選取 * 存取金鑰 * 、然後選取您要刪除的每個存取金鑰的核取方塊。
4. 選取*「動作*」>*「刪除選取的金鑰*」。
5. 從確認對話方塊中、選取 * 刪除機碼 * 。

   頁面右上角會出現確認訊息。

管理S3儲存區

建立S3儲存區

您可以使用租戶管理程式來建立S3儲存區以供物件資料使用。

開始之前

- 您將使用登入租戶管理程式 "支援的網頁瀏覽器"。
- 您屬於具有「根目錄」存取權或「管理所有儲存區」的使用者群組 "權限"。這些權限會覆寫群組或儲存區原則中的權限設定。

  可以授予設定或修改區段或物件之S3物件鎖定內容的權限 "庫位原則或群組原則"。

- 如果您計畫為貯體啟用 S3 物件鎖定、則網格管理員已為 StorageGRID 系統啟用全域 S3 物件鎖定設定、而且您已檢閱 S3 物件鎖定貯體和物件的需求。請參閱 "使用 S3 物件鎖定來保留物件"。

存取精靈

步驟

1. 從儀表板選取 * 檢視貯體 * 、或選取 * 儲存空間（ S3 ） * > * 鏟斗 * 。
2. 選取*建立桶*。

輸入詳細資料

步驟

1. 輸入貯體的詳細資料。

欄位	說明
儲存區名稱	符合以下規則的貯體名稱： • 必須在各個StorageGRID 方面都是獨一無二的（不只是租戶帳戶內的獨特功能）。 • 必須符合DNS規範。 • 必須包含至少3個字元、且不得超過63個字元。 • 每個標籤都必須以英文字母或數字開頭和結尾、而且只能使用英文字母、數字和連字號。 • 不應在虛擬託管樣式要求中使用期間。期間會導致伺服器萬用字元憑證驗證發生問題。 如需詳細資訊、請參閱 "Amazon Web Services（AWS）儲存區命名規則文件"。 • 附註 * ：建立貯體後、您無法變更貯體名稱。
區域	貯體的區域。 您的系統管理員負責管理可用的區域。StorageGRID儲存區的區域可能會影響套用至物件的資料保護原則。依預設、所有的儲存區都會在中建立 `us-east-1` 區域。 • 附註 * ：建立貯體後、您無法變更區域。

2. 選擇*繼續*。

管理物件設定

步驟

1. 或者、為儲存區啟用物件版本管理。

   如果您要儲存此儲存區中每個物件的每個版本、請啟用物件版本管理。然後您可以視需要擷取物件的舊版。如果儲存區將用於跨網格複寫、則必須啟用物件版本管理。

2. 如果啟用全域 S3 物件鎖定設定、則可選擇性啟用儲存區的 S3 物件鎖定、以使用一次寫入多讀（ WORM ）模式來儲存物件。

   只有當您需要保留物件一段固定時間（例如、為了符合特定法規要求）時、才需要為貯體啟用 S3 物件鎖定。S3 物件鎖定是一項永久性設定、可協助您防止物件在固定的時間內或無限期地遭到刪除或覆寫。

   > 為貯體啟用 S3 物件鎖定設定之後、就無法停用該設定。擁有正確權限的任何人都可以將無法變更的物件新增至此貯體。您可能無法刪除這些物件或貯體本身。

   如果您為儲存區啟用S3物件鎖定、則會自動啟用儲存區版本設定。

3. 如果您選取 * 啟用 S3 物件鎖定 * 、則可選擇性啟用此貯體的 * 預設保留 * 。

啟用 * 預設保留 * 時、新增至貯體的新物件將會自動受到保護、不被刪除或覆寫。「 * 預設保留 * 」設定不會套用至具有其本身保留期間的物件。

a. 如果啟用 * 預設保留 * 、請為貯體指定 * 預設保留模式 * 。

預設保留模式	說明
法規遵循	• 直到達到物件的保留日期、才能刪除物件。 • 物件的保留日期可以增加、但不能減少。 • 直到達到該日期為止、才能移除物件的保留日期。
治理	• 的使用者 `s3:BypassGovernanceRetention` 權限可以使用 `x-amz-bypass-governance-retention: true` 要求標頭略過保留設定。 • 這些使用者可以在達到物件版本的保留截止日期之前刪除物件版本。 • 這些使用者可以增加、減少或移除物件的保留到目前為止。

b. 如果啟用 * 預設保留 * 、請指定貯體的 * 預設保留期間 * 。

「 * 預設保留期間 * 」表示新增至此貯體的物件應保留多久、從擷取開始算起。指定 1 至 36500 天或 1 至 100 年（含）之間的值。

4. 選取*建立桶*。

此庫位會建立並新增至「庫位」頁面上的表格。

5. 您也可以選擇 * 前往儲存庫詳細資料頁面 * "檢視貯體詳細資料" 並執行其他組態。

檢視貯體詳細資料

您可以檢視租戶帳戶中的貯體。

開始之前

- 您將使用登入租戶管理程式 "支援的網頁瀏覽器"。

步驟

1. 從儀表板選取 * 檢視貯體 * 、或選取 * 儲存空間（ S3 ） * > * 鏟斗 * 。

此時會出現「鏟斗」頁面。

2. 檢閱每個貯體的摘要資訊。

視需要、您可以依任何欄排序資訊、也可以在清單中前後翻頁。

所顯示的「物件數」和「已用空間」值為預估值。這些預估值會受到擷取時間、網路連線能力和節點狀態的影響。如果儲存區已啟用版本管理、則刪除的物件版本會包含在物件數中。

欄位	說明
名稱	貯體的獨特名稱、無法變更。
啟用的功能	已啟用貯體功能的清單。
S3物件鎖定	儲存區是否啟用 S3 物件鎖定。 只有在網格啟用 S3 物件鎖定時、才會顯示此欄。此欄也會顯示任何舊版相容桶的資訊。
區域	庫位的區域、無法變更。
物件數	此貯體中的物件數目。新增或刪除物件時、此值可能不會立即更新。如果已啟用版本設定功能、則此值會包含非目前物件版本。
已用空間	貯體中所有物件的邏輯大小。邏輯大小不包含複寫或銷毀編碼複本或物件中繼資料所需的實際空間。
建立日期	建立庫位的日期與時間。

3. 若要檢視特定貯體的詳細資料、請從表格中選取貯體名稱。

   此時會顯示「庫位詳細資料」頁面。在此頁面中、您可以執行下列工作：

   - 設定及管理貯體選項、例如 "一致性層級"、 "上次存取時間更新"、 "物件版本管理"、 "S3物件鎖定" 和 "預設貯體保留"
   - 設定貯體存取、例如 "跨來源資源共享（ CORS ）"
   - 管理 "平台服務" （如果租戶允許）、包括複寫、事件通知和搜尋整合
   - 啟用和 "管理跨網格複寫" （如果租戶允許）將擷取至此貯體的物件複寫到另一個 StorageGRID 系統
   - 存取 "試驗性 S3 主控台" 管理貯體中的物件
   - "刪除貯體中的所有物件"
   - "刪除貯體" 那已經是空的

變更貯體的一致性層級

如果您使用的是 S3 租戶、您可以變更 S3 儲存區中物件上執行作業的一致性層級。

開始之前

- 您將使用登入租戶管理程式 "支援的網頁瀏覽器"。
- 您屬於具有的使用者群組 "管理所有貯體或根目錄存取權限"。這些權限會覆寫群組或儲存區原則中的權限設定。

關於這項工作

一致性控制可在物件的可用度與這些物件在不同儲存節點和站台之間的一致性之間取得平衡。一般而言、您應該

使用庫存箱的*新寫入後讀取*一致性層級。

如果*新寫入後讀取*一致性層級不符合用戶端應用程式的需求、您可以設定儲存區一致性層級或使用來變更一致性層級 `Consistency-Control` 標頭。。 `Consistency-Control` 標頭會覆寫貯體一致性層級。

> 當您變更桶的一致性層級時、只有變更後擷取的物件才保證符合修訂的層級。

步驟

1. 從儀表板選取 * 檢視貯體 * 、或選取 * 儲存空間（ S3 ） * > * 鏟斗 * 。
2. 從表格中選取貯體名稱。

   此時會顯示「庫位詳細資料」頁面。

3. 從 **Bucket options** 標籤中、選取 **Consistency Level** 折疊。
4. 針對此儲存區中的物件執行的作業、選取一致性層級。
   - * 全部 * ：提供最高等級的一致性。所有節點都會立即接收資料、否則要求將會失敗。
   - **Strong-globall** ：保證所有網站上所有用戶端要求的寫入後讀取一致性。
   - **Strong-site** ：保證網站內所有用戶端要求的寫入後讀取一致性。
   - * 新寫入後讀取 * （預設）：提供新物件的寫入後讀取一致性、以及物件更新的最終一致性。提供高可用度與資料保護保證。建議大多數情況下使用。
   - * 可用 * ：提供新物件和物件更新的最終一致性。對於 S3 貯體、請僅視需要使用（例如、包含很少讀取的記錄值之貯體、或用於對不存在的金鑰執行 head 或 Get 作業）。S3 FabricPool 儲存區不支援。
5. 選取*儲存變更*。

啟用或停用上次存取時間更新

當網格管理員為StorageGRID 某個系統建立資訊生命週期管理（ILM）規則時、他們可以選擇性地指定物件的上次存取時間、以決定是否要將該物件移到不同的儲存位置。如果您使用的是S3租戶、您可以針對S3儲存區中的物件啟用上次存取時間更新、藉此充分利用這類規則。

這些指示僅適用於至少包含一個 ILM 規則的 StorageGRID 系統、該規則使用 * 上次存取時間 * 選項作為進階篩選器或參考時間。如果您的支援系統不包含此類規則、您可以忽略這些指示StorageGRID 。請參閱 "在 ILM 規則中使用上次存取時間" 以取得詳細資料。

開始之前

- 您將使用登入租戶管理程式 "支援的網頁瀏覽器"。
- 您屬於具有的使用者群組 "管理所有貯體或根目錄存取權限"。這些權限會覆寫群組或儲存區原則中的權限設定。

關於這項工作

- 上次存取時間 * 是 ILM 規則的 * 參考時間 * 放置指示可用的選項之一。將規則的參考時間設為上次存取時間、可讓網格管理員根據上次擷取（讀取或檢視）物件的時間、指定物件放置在特定儲存位置。

例如、為了確保最近檢視的物件仍保留在較快的儲存空間、網格管理員可以建立ILM規則、指定下列項目：

- 過去一個月擷取的物件應保留在本機儲存節點上。
- 過去一個月未擷取的物件應移至異地位置。

根據預設、上次存取時間的更新會停用。如果您的 StorageGRID 系統包含使用 * 上次存取時間 * 選項的 ILM 規則、且您想要將此選項套用至此儲存庫中的物件、則必須針對該規則中指定的 S3 儲存區、啟用更新至上次存取時間。

更新上次擷取物件的存取時間、可能會降低StorageGRID 功能性、尤其是小型物件的效能。

上次存取時間更新會影響效能、因為StorageGRID 每次擷取物件時、VMware都必須執行下列額外步驟：

- 使用新的時間戳記更新物件
- 將物件新增至ILM佇列、以便根據目前的ILM規則和原則重新評估

下表摘要說明上次存取時間停用或啟用時、套用至儲存區中所有物件的行為。

申請類型	停用上次存取時間時的行為（預設）		啟用上次存取時間時的行為	
	上次存取時間已更新？	新增至ILM評估佇列的物件？	上次存取時間已更新？	新增至ILM評估佇列的物件？
要求擷取物件、其存取控制清單或其中繼資料	否	否	是的	是的
要求更新物件的中繼資料	是的	是的	是的	是的
要求將物件從一個儲存區複製到另一個儲存區	• 否、來源複本 • 是、適用於目的地複本	• 否、來源複本 • 是、適用於目的地複本	• 是、來源複本 • 是、適用於目的地複本	• 是、來源複本 • 是、適用於目的地複本
要求完成多部分上傳	是的、適用於組裝好的物件	是的、適用於組裝好的物件	是的、適用於組裝好的物件	是的、適用於組裝好的物件

步驟

1. 從儀表板選取 * 檢視貯體 * 、或選取 * 儲存空間（ S3 ） * > * 鏟斗 * 。
2. 從表格中選取貯體名稱。

   此時會顯示「庫位詳細資料」頁面。

3. 從 **Bucket options** 標籤中、選取 * 上次存取時間更新 * 手風琴。
4. 啟用或停用上次存取時間更新。
5. 選取*儲存變更*。

變更儲存區的物件版本設定

如果您使用的是 S3 租戶、則可以變更 S3 儲存區的版本設定狀態。

開始之前

- 您將使用登入租戶管理程式 "支援的網頁瀏覽器"。
- 您屬於具有的使用者群組 "管理所有貯體或根目錄存取權限"。這些權限會覆寫群組或儲存區原則中的權限設定。

關於這項工作

您可以啟用或暫停儲存區的物件版本管理。在您啟用貯體的版本設定之後、它就無法恢復至未版本化狀態。不過、您可以暫停儲存區的版本管理。

- 停用：從未啟用版本管理
- 已啟用：已啟用版本管理
- 已暫停：先前已啟用版本管理、並已暫停

如需詳細資訊、請參閱下列內容：

- "物件版本管理"
- "S3版本化物件的ILM規則和原則（範例4）"
- "如何刪除物件"

步驟

1. 從儀表板選取 * 檢視貯體 * 、或選取 * 儲存空間（ S3 ） * > * 鏟斗 * 。
2. 從表格中選取貯體名稱。

   此時會顯示「庫位詳細資料」頁面。

3. 從 * 儲存庫選項 * 標籤中、選取 * 物件版本設定 * 折疊器。
4. 選取此儲存區中物件的版本管理狀態。

   物件版本設定功能必須保持啟用、才能用於跨網格複寫的儲存區。如果啟用S3物件鎖定或舊版規範、則會停用*物件版本管理*選項。

選項	說明
啟用版本管理	如果您要儲存此儲存區中每個物件的每個版本、請啟用物件版本管理。然後您可以視需要擷取物件的舊版。 使用者修改儲存庫中已有的物件時、將會對其進行版本控制。
暫停版本管理	如果您不想再建立新的物件版本、請暫停物件版本管理。您仍然可以擷取任何現有的物件版本。

5. 選取*儲存變更*。

如果貯體和物件必須符合保留法規要求、您可以使用 S3 物件鎖定。

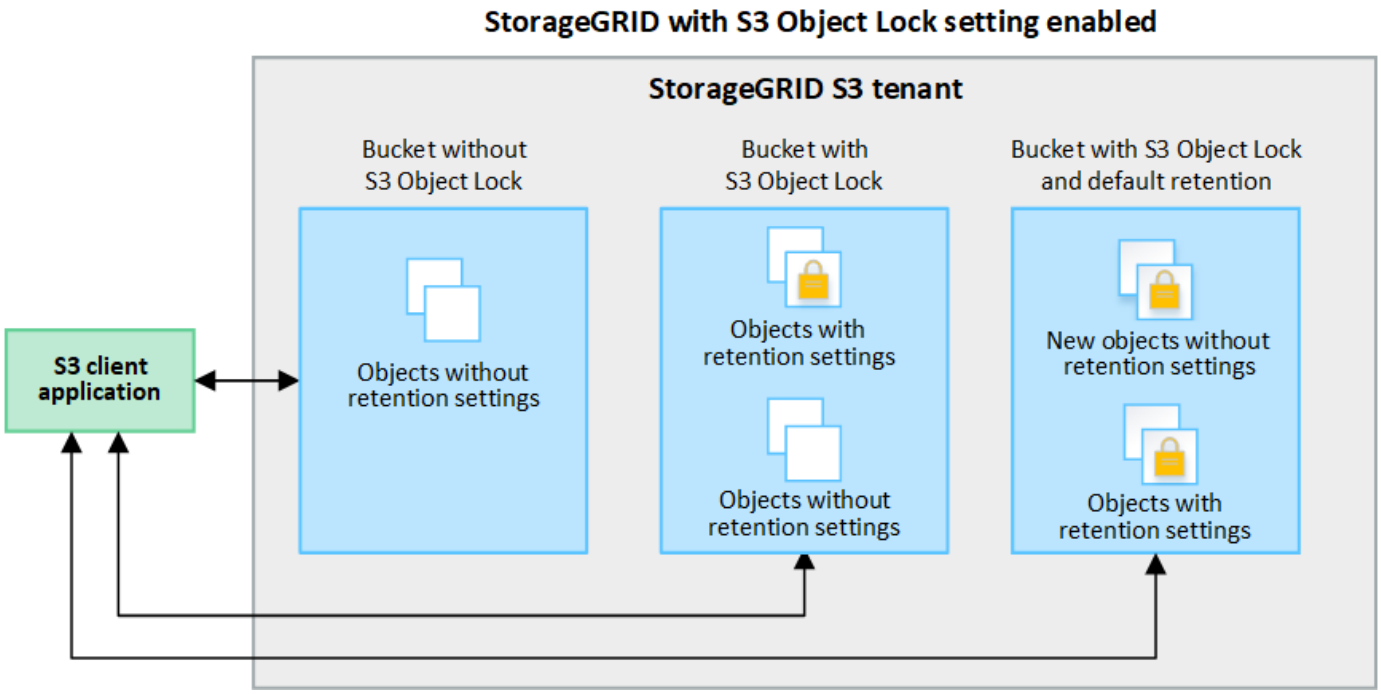
什麼是S3物件鎖定？

「物件鎖定」功能是物件保護解決方案、StorageGRID 相當於Amazon Simple Storage Service（Amazon S3）中的S3物件鎖定。

如圖所示、當啟用StorageGRID 全域S3物件鎖定設定以供支援某個功能時、S3租戶帳戶可以建立啟用或不啟用S3物件鎖定的儲存區。如果貯體已啟用 S3 物件鎖定、則需要設定貯體版本、而且會自動啟用。

如果某個貯體已啟用 S3 物件鎖定、 S3 用戶端應用程式可以選擇性地指定儲存至該貯體的任何物件版本的保留設定。

此外、已啟用 S3 物件鎖定的貯體、也可以選用預設保留模式和保留期間。預設設定只會套用至新增至貯體的物件、而不會套用其本身的保留設定。



保留模式

StorageGRID S3 物件鎖定功能支援兩種保留模式、可將不同層級的保護套用至物件。這些模式相當於 Amazon S3 保留模式。

- 在法規遵循模式中：
  - 直到達到物件的保留日期、才能刪除物件。
  - 物件的保留日期可以增加、但不能減少。
  - 直到達到該日期為止、才能移除物件的保留日期。
- 在治理模式中：
  - 具有特殊權限的使用者可以在修改特定保留設定的要求中使用略過標頭。

- 這些使用者可以在達到物件版本的保留截止日期之前刪除物件版本。
- 這些使用者可以增加、減少或移除物件的保留到目前為止。

物件版本的保留設定

如果在啟用 S3 物件鎖定的情況下建立貯體、使用者可以使用 S3 用戶端應用程式、針對新增至貯體的每個物件、選擇性地指定下列保留設定：

- * 保留模式 * ：法規遵循或治理。
- * 保留至日期 * ：如果物件版本的保留至未來日期、則可以擷取物件、但無法刪除。
- 合法持有：將合法持有套用至物件版本、會立即鎖定該物件。例如、您可能需要對與調查或法律爭議相關的物件保留法律。合法持有沒有到期日、但在明確移除之前、仍會保留到位。合法持有不受保留至日期的限制。

  如果物件處於合法保留狀態、則無論物件的保留模式為何、任何人都無法刪除該物件。

  如需物件設定的詳細資訊、請參閱 "使用 S3 REST API 來設定 S3 物件鎖定"。

貯體的預設保留設定

如果在啟用 S3 物件鎖定的情況下建立貯體、使用者可以選擇性地指定貯體的下列預設設定：

- * 預設保留模式 * ：法規遵循或治理。
- * 預設保留期間 * ：新增至此貯體的物件版本應保留多久、從新增物件之日起算。

預設的貯體設定僅適用於沒有自己保留設定的新物件。當您新增或變更這些預設設定時、現有的貯體物件不會受到影響。

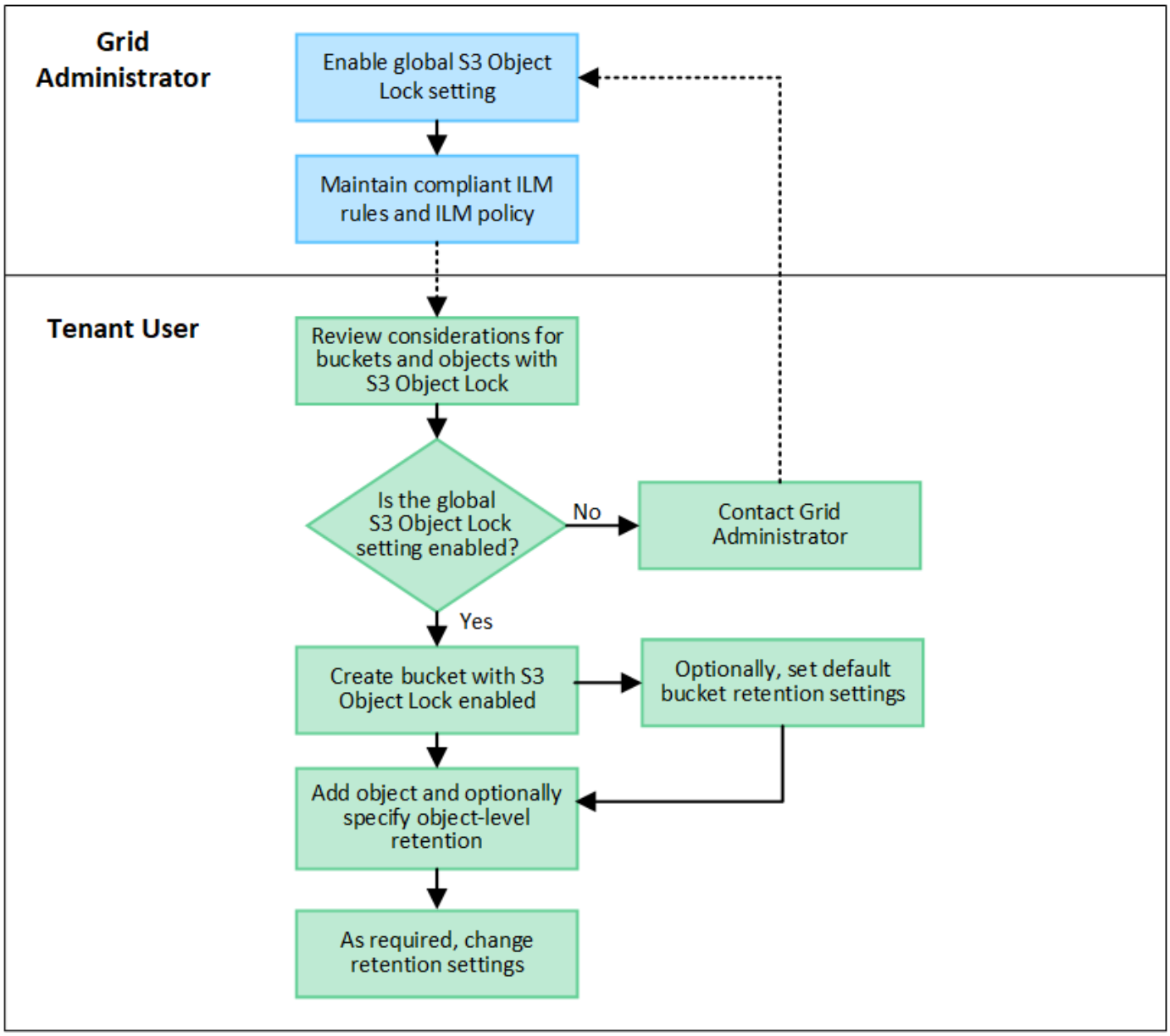
請參閱 "建立S3儲存區" 和 "更新 S3 物件鎖定預設保留"。

S3物件鎖定工作流程

工作流程圖顯示StorageGRID 使用S3物件鎖定功能的高階步驟。

在啟用S3物件鎖定功能的情況下建立儲存區之前、網格管理員必須先為整個StorageGRID 支援整個系統啟用全域S3物件鎖定設定。網格管理員也必須確保資訊生命週期管理（ILM）原則符合「法規遵循」、而且必須符合啟用S3物件鎖定的儲存區需求。如需詳細資訊、請聯絡您的網格管理員、或參閱的指示 "使用 S3 物件鎖定來管理物件"。

啟用全域 S3 物件鎖定設定後、您可以建立啟用 S3 物件鎖定的儲存區、並選擇性地為每個儲存區指定預設保留設定。此外、您可以使用 S3 用戶端應用程式、選擇性地指定每個物件版本的保留設定。



啟用**S3**物件鎖定的儲存區需求

- 如果StorageGRID 已針對整個S3物件鎖定設定啟用for the S廳 系統、您可以使用租戶管理程式、租戶管理API或S3 REST API來建立啟用S3物件鎖定的儲存區。
- 如果您打算使用S3物件鎖定、則必須在建立儲存區時啟用S3物件鎖定。您無法為現有貯體啟用 S3 物件鎖定。
- 當「S3物件鎖定」已啟用時、StorageGRID 即可自動啟用該儲存區的版本管理功能。您無法停用儲存區的 S3 物件鎖定或暫停版本設定。
- 您也可以選擇使用租戶管理員、租戶管理 API 或 S3 REST API 、為每個貯體指定預設保留模式和保留期間。貯體的預設保留設定僅適用於新增至貯體但沒有其本身保留設定的新物件。您可以指定保留模式來覆寫這些預設設定、並在上傳每個物件版本時保留至日期。
- 啟用 S3 物件鎖定的貯體支援貯體生命週期組態。
- 啟用S3物件鎖定的儲存區不支援CloudMirror複寫。

啟用**S3**物件鎖定之儲存區中的物件需求

- 若要保護物件版本、您可以指定貯體的預設保留設定、或是指定每個物件版本的保留設定。可以使用 S3 用戶端應用程式或 S3 REST API 來指定物件層級保留設定。
- 保留設定適用於個別物件版本。物件版本可以同時具有「保留直到日期」和「合法保留」設定、但不能有另一個設定、或兩者都沒有。指定物件的保留截止日期或合法保留設定、只會保護要求中指定的版本。您可以建立物件的新版本、而舊版物件仍會保持鎖定狀態。

啟用**S3**物件鎖定的儲存區物件生命週期

儲存在已啟用 S3 物件鎖定的儲存貯體中的每個物件都會經過下列階段：

1. 物件擷取

   當物件版本新增至啟用 S3 物件鎖定的儲存區時、保留設定會套用如下：

   - 如果為物件指定保留設定、則會套用物件層級的設定。任何預設貯體設定都會被忽略。
   - 如果未指定物件的保留設定、則會套用預設貯體設定（如果存在）。
   - 如果未指定物件或貯體的保留設定、則 S3 物件鎖定不會保護該物件。

   如果套用保留設定、則物件和任何 S3 使用者定義的中繼資料都會受到保護。

2. * 物件保留與刪除 *

   StorageGRID 會在指定的保留期間內儲存每個受保護物件的多個複本。物件複本和儲存位置的確切數量和類型取決於主動式 ILM 原則中的相容規則。受保護物件是否能在達到保留截止日期之前刪除、取決於其保留模式。

   - 如果物件處於合法保留狀態、則無論物件的保留模式為何、任何人都無法刪除該物件。

我是否仍能管理舊有的法規遵循貯體？

S3物件鎖定功能取代先前StorageGRID 版本的Compliance功能。如果您使用StorageGRID 舊版的《不規則》建立了相容的儲存桶、您可以繼續管理這些儲存桶的設定、但是您無法再建立新的相容儲存桶。如需相關指示、請參閱https://kb.netapp.com/Advice_and_Troubleshooting/Hybrid_Cloud_Infrastructure/StorageGRID/How_to_manage_legacy_Compliant_buckets_in_StorageGRID_11.5["NetApp知識庫：如何管理StorageGRID 支援老舊的知識庫、請參閱《知識庫文章"^]。

更新 **S3** 物件鎖定預設保留

如果您在建立貯體時啟用 S3 物件鎖定、則可以編輯貯體以變更預設保留設定。您可以啟用（或停用）預設保留、並設定預設保留模式和保留期間。

開始之前

- 您將使用登入租戶管理程式 "支援的網頁瀏覽器"。
- 您屬於具有的使用者群組 "管理所有貯體或根目錄存取權限"。這些權限會覆寫群組或儲存區原則中的權限設定。
- S3 物件鎖定已在 StorageGRID 系統中全域啟用、您在建立儲存貯體時啟用 S3 物件鎖定。請參閱 "使用 S3 物件鎖定來保留物件"。

步驟

1. 從儀表板選取 * 檢視貯體 * 、或選取 * 儲存空間（ S3 ） * > * 鏟斗 * 。
2. 從表格中選取貯體名稱。

   此時會顯示「庫位詳細資料」頁面。

3. 從 **Bucket options** 標籤中、選取 **S3 Object Lock** 折疊式。
4. 或者、啟用或停用此貯體的 * 預設保留 * 。

   對此設定所做的變更不適用於已在貯體中的物件、也不適用於可能有其本身保留期間的任何物件。

5. 如果啟用 * 預設保留 * 、請為貯體指定 * 預設保留模式 * 。

預設保留模式	說明
法規遵循	• 直到達到物件的保留日期、才能刪除物件。 • 物件的保留日期可以增加、但不能減少。 • 直到達到該日期為止、才能移除物件的保留日期。
治理	• 的使用者 `s3:BypassGovernanceRetention` 權限可以使用 `x-amz-bypass-governance-retention: true` 要求標頭略過保留設定。 • 這些使用者可以在達到物件版本的保留截止日期之前刪除物件版本。 • 這些使用者可以增加、減少或移除物件的保留到目前為止。

6. 如果啟用 * 預設保留 * 、請指定貯體的 * 預設保留期間 * 。

   「 * 預設保留期間 * 」表示新增至此貯體的物件應保留多久、從擷取開始算起。指定 1 至 36500 天或 1 至 100 年（含）之間的值。

7. 選取*儲存變更*。

設定跨來源資源共用（**CORS**）

如果您想讓其他網域中的 Web 應用程式能夠存取 S3 貯體中的貯體和物件、則可以為 S3 貯體設定跨來源資源共享（ CORS ）。

開始之前

- 您將使用登入租戶管理程式 "支援的網頁瀏覽器"。
- 您屬於具有的使用者群組 "管理所有貯體或根目錄存取權限"。這些權限會覆寫群組或儲存區原則中的權限設定。

關於這項工作

跨來源資源共用（CORS）是一種安全機制、可讓單一網域中的用戶端Web應用程式存取不同網域中的資源。例如、假設您使用名為的S3儲存區 `Images` 儲存圖形。設定的CORS `Images` 儲存庫、您可以讓該儲存庫中的影像顯示在網站上 `http://www.example.com`。

為貯體啟用 CORS

步驟

1. 使用文字編輯器建立必要的 XML 。

   此範例顯示用於啟用S3儲存區的CORS的XML。此XML可讓任何網域將GET要求傳送至儲存區、但僅允許 `http://www.example.com` 要傳送貼文和刪除要求的網域。允許所有要求標頭。

   ```
   <CORSConfiguration
       xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
       <CORSRule>
           <AllowedOrigin>*</AllowedOrigin>
           <AllowedMethod>GET</AllowedMethod>
           <AllowedHeader>*</AllowedHeader>
       </CORSRule>
       <CORSRule>
           <AllowedOrigin>http://www.example.com</AllowedOrigin>
           <AllowedMethod>GET</AllowedMethod>
           <AllowedMethod>POST</AllowedMethod>
           <AllowedMethod>DELETE</AllowedMethod>
           <AllowedHeader>*</AllowedHeader>
       </CORSRule>
   </CORSConfiguration>
   ```

   如需CORS組態XML的詳細資訊、請參閱 "Amazon Web Services（AWS）文件：Amazon Simple Storage Service開發人員指南"。

2. 從儀表板選取 * 檢視貯體 * 、或選取 * 儲存空間 （ S3 ） * > * 鏟斗 * 。
3. 從表格中選取貯體名稱。

   此時會顯示「庫位詳細資料」頁面。

4. 從 **Bucket access** （庫存取 * ）標籤中、選取 * 跨來源資源共用（ CORS ） * 折疊。
5. 選中 * 啓用 CORS* 複選框。
6. 將 CORS 組態 XML 貼到文字方塊中。
7. 選取*儲存變更*。

修改 CORS 設定

步驟

1. 在文字方塊中更新 CORS 組態 XML 、或選取 * 清除 * 重新開始。
2. 選取*儲存變更*。

停用 CORS 設定

步驟

1. 清除 **Enable CORS** （啓用 CORS* ）複選框。
2. 選取*儲存變更*。

刪除貯體中的物件

您可以使用 Tenant Manager 刪除一個或多個貯體中的物件。

考量與要求

執行這些步驟之前、請注意下列事項：

- 當您刪除貯體中的物件時、 StorageGRID 會從 StorageGRID 系統中的所有節點和站台、永久移除每個所選貯體中的所有物件和所有物件版本。StorageGRID 也會移除任何相關的物件中繼資料。您將無法恢復此資訊。
- 根據物件數量、物件複本和並行作業、刪除貯體中的所有物件可能需要數分鐘、數天甚至數週的時間。
- 如果貯體有 "S3 物件鎖定已啟用"，它可能會保留在 * 刪除物件：唯讀 * 狀態中，時間 _ 年 _ 。

  使用 S3 物件鎖定的貯體將保留在 * 刪除物件：唯讀 * 狀態、直到達到所有物件的保留日期、並移除任何合法保留為止。

- 刪除物件時、貯體的狀態為 * 刪除物件：唯讀 * 。在此狀態下、您無法將新物件新增至貯體。
- 刪除所有物件後、貯體仍保持唯讀狀態。您可以執行下列其中一項：
  - 將貯體恢復為寫入模式、並將其重複用於新物件
  - 刪除貯體
  - 將貯體保持在唯讀模式、以保留其名稱供未來使用
- 如果某個貯體已啟用物件版本設定、則在您開始這些步驟時、任何在該貯體中的刪除標記都不會被刪除物件作業移除。如果您想要在刪除所有物件之後刪除版本化的儲存庫、則必須移除任何預先存在的刪除標記。
- 如果您使用 "跨網格複寫"，請注意以下事項：
  - 使用此選項不會刪除其他網格上的貯體中的任何物件。
  - 如果您為來源貯體選取此選項、當您將物件新增至其他網格上的目的地貯體時、就會觸發 * 跨網格複寫失敗 * 警示。如果您無法保證沒有人會將物件新增至另一個網格上的貯體、 "停用跨網格複寫" 刪除所有貯體物件之前、請先刪除該貯體的所有物件。

開始之前

- 您將使用登入租戶管理程式 "支援的網頁瀏覽器"。
- 您屬於具有的使用者群組 "root 存取權限"。此權限會覆寫群組或儲存區原則中的權限設定。

步驟

1. 從儀表板選取 * 檢視貯體 * 、或選取 * 儲存空間（ S3 ） * > * 鏟斗 * 。

   此時會顯示「庫位」頁面、並顯示所有現有的S3庫位。

2. 使用 * 動作 * 功能表或特定儲存庫的詳細資料頁面。

「行動」功能表

a. 選取您要從中刪除物件的每個貯體的核取方塊。

b. 選取 * 動作 * > * 刪除貯體中的物件 * 。

詳細資料頁面

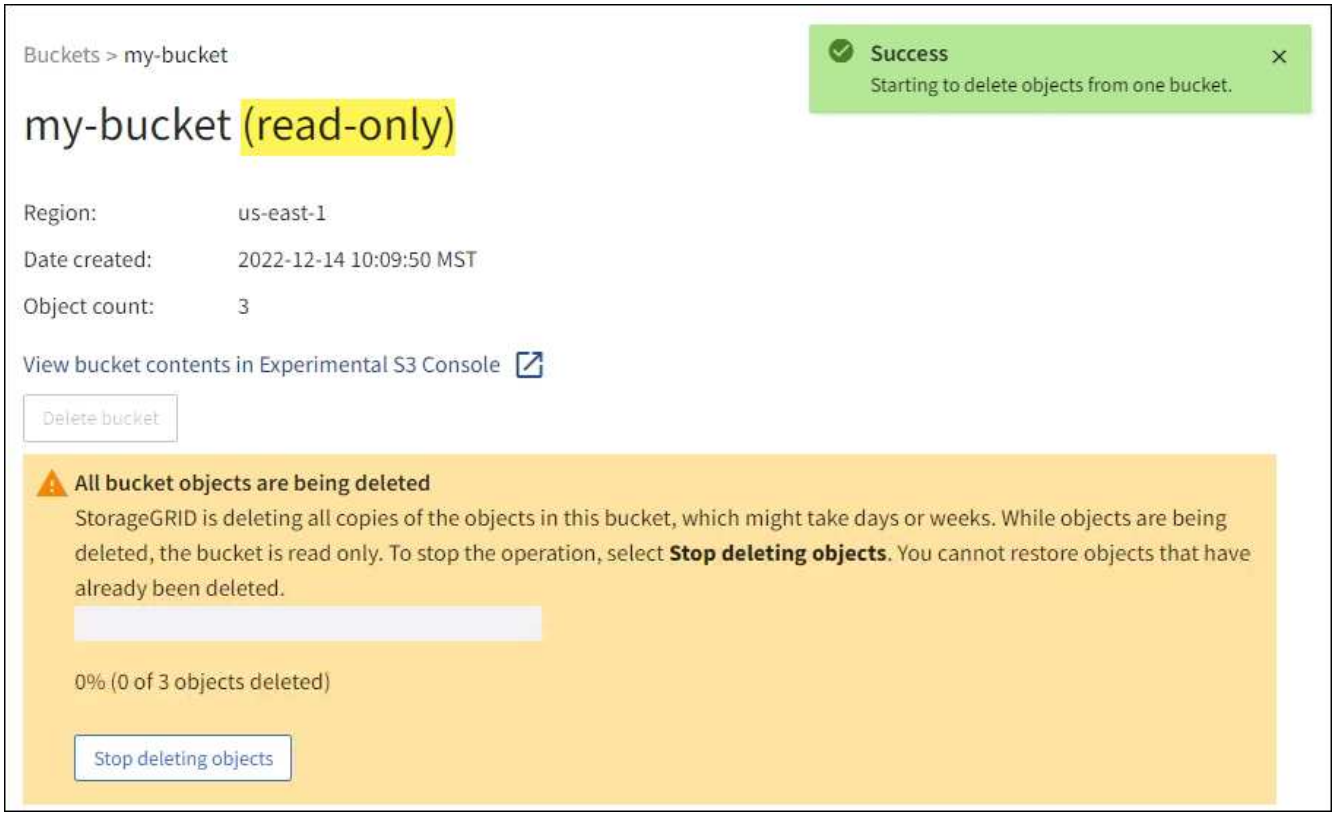
a. 選取貯體名稱以顯示其詳細資料。

b. 選取 * 刪除貯體中的物件 * 。

3. 當確認對話方塊出現時、請檢閱詳細資料、輸入 * 是 * 、然後選取 * 確定 * 。
4. 等待刪除作業開始。

   幾分鐘後：

   - 貯體詳細資料頁面上會出現黃色狀態橫幅。進度列代表已刪除物件的百分比。
   - * （唯讀） * 會出現在貯體詳細資料頁面上的貯體名稱之後。
   - * （刪除物件：唯讀） * 會出現在「 Bucket 」頁面上的 Bucket 名稱旁邊。

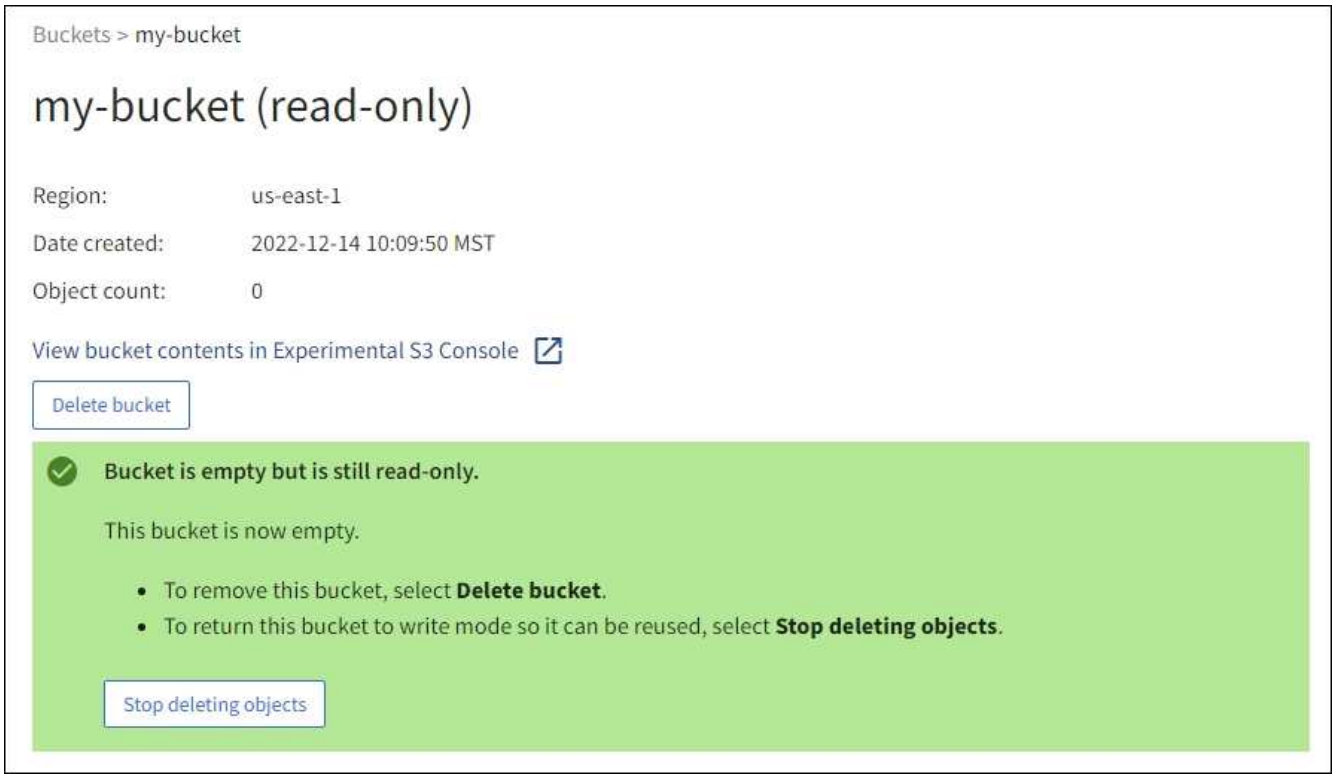


5. 在作業執行時視需要選取 * 停止刪除物件 * 以停止處理程序。然後、您也可以選擇 * 刪除貯體中的物件 * 來恢復處理程序。

   當您選取 * 停止刪除物件 * 時、貯體會返回寫入模式、但您無法存取或還原任何已刪除的物件。

6. 等待作業完成。

當貯體為空時、狀態橫幅會更新、但貯體仍為唯讀。



7. 執行下列其中一項：
   - 離開頁面以保持貯體處於唯讀模式。例如、您可以將空貯體保留為唯讀模式、以保留貯體名稱供未來使用。
   - 刪除儲存庫。您可以選擇 * 刪除貯體 * 來刪除單一貯體、或是退回 " 鏟斗 " 頁面、然後選取 * 動作 * > * 刪除 * 貯體來移除多個貯體。

     如果在刪除所有物件之後、無法刪除版本化的貯體、則刪除標記可能會保留。若要刪除貯體、您必須移除所有剩餘的刪除標記。

   - 將貯體恢復為寫入模式、並選擇性地將其重複用於新物件。您可以選擇 * 停止刪除單一貯體的物件 * 、或返回至鏟斗頁面、然後針對多個貯體選取 * 操作 * > * 停止刪除物件 * 。

刪除**S3**儲存區

您可以使用租戶管理程式刪除一或多個空的S3儲存區。

開始之前

- 您將使用登入租戶管理程式 "支援的網頁瀏覽器"。
- 您屬於具有的使用者群組 "管理所有貯體或根目錄存取權限"。這些權限會覆寫群組或儲存區原則中的權限設定。
- 您要刪除的儲存區是空的。

關於這項工作

這些指示說明如何使用租戶管理程式刪除S3儲存區。您也可以使用刪除S3儲存區 "租戶管理API" 或 "S3 REST API"。

如果 S3 儲存區包含物件、非目前物件版本或刪除標記、則無法刪除該儲存區。如需如何刪除 S3 版本化物件的相關資訊、請參閱 "如何刪除物件"。

步驟

1. 從儀表板選取 * 檢視貯體 * 、或選取 * 儲存空間（ S3 ） * > * 鏟斗 * 。

   此時會顯示「庫位」頁面、並顯示所有現有的S3庫位。

2. 使用 * 動作 * 功能表或特定儲存庫的詳細資料頁面。

   「行動」功能表

   a. 選取您要刪除的每個貯體的核取方塊。

   b. 選取 * 動作 * > * 刪除儲存區 * 。

   詳細資料頁面

   a. 選取貯體名稱以顯示其詳細資料。

   b. 選取 * 刪除儲存庫 * 。

3. 當確認對話方塊出現時、請選取 * 是 * 。

   確認每個儲存區都是空的、然後刪除每個儲存區。StorageGRID此作業可能需要幾分鐘的時間。

   如果儲存區不是空的、就會出現錯誤訊息。您必須先刪除貯體中的所有物件和任何刪除標記、才能刪除該貯體。

使用實驗性**S3**主控台

您可以使用S3主控台檢視S3儲存區中的物件。

您也可以使用S3主控台執行下列動作：

- 新增及刪除物件、物件版本及資料夾
- 重新命名物件
- 在儲存區和資料夾之間移動和複製物件
- 管理物件標記
- 檢視物件中繼資料
- 下載物件

S3 Console 標示為「實驗性」、因為尚未完成或核准用於正式作業環境。租戶只能在執行少量物件的功能時使用S3主控台、例如上傳物件以模擬新的ILM原則、疑難排解擷取問題、或使用概念驗證或非正式作業網格時。

開始之前

- 您將使用登入租戶管理程式 "支援的網頁瀏覽器"。

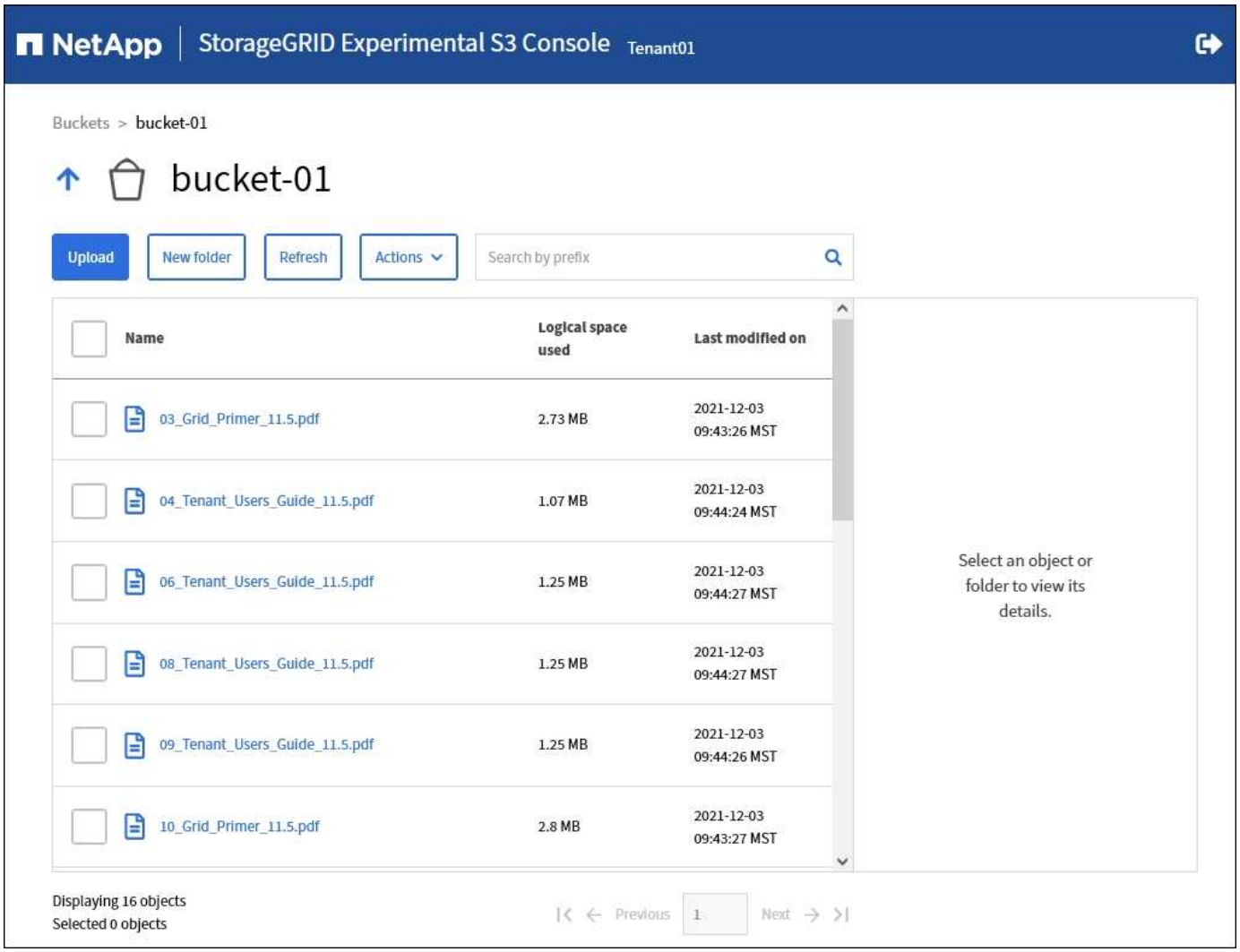
- 您屬於具有「根目錄」存取權限的使用者群組、或是擁有「使用 S3 主控台管理所有儲存區」和「管理物件」的使用者群組 "權限"。

> 擁有「管理具有 S3 主控台權限的物件」、但沒有「管理所有儲存區」權限的使用者、仍可直接瀏覽至實驗 S3 主控台。

- 您已經建立了一個儲存庫。
- 已為使用者設定 S3 群組或儲存區原則。
- 您知道使用者的存取金鑰ID和秘密存取金鑰。或者、您也可以選擇 `.csv` 包含此資訊的檔案。請參閱 "建立存取金鑰的說明"。

步驟

1. 選擇*桶*。
2. 選取 Experimental S3 Console 。您也可以從「庫位詳細資料」頁面存取此連結。
3. 在「實驗S3主控台登入」頁面上、將存取金鑰ID和秘密存取金鑰貼到欄位中。否則、請選取 * 上傳存取金鑰 * 、然後選取您的 `.csv` 檔案：
4. 選擇*登入*。
5. 視需要管理物件。



管理S3平台服務

什麼是平台服務？

StorageGRID 平台服務可讓您將 S3 物件和物件中繼資料的事件通知和複本傳送至外部目的地、協助您實作混合雲策略。

如果您的租戶帳戶允許使用平台服務、您可以針對任何S3儲存區設定下列服務：

- * CloudMirror 複寫 * ：使用 "CloudMirror複寫服務StorageGRID" 將特定物件從 StorageGRID 貯體鏡射到指定的外部目的地。

  例如、您可以使用CloudMirror複寫將特定的客戶記錄鏡射到Amazon S3、然後利用AWS服務對資料執行分析。

  > 如果來源儲存區已啟用S3物件鎖定、則不支援CloudMirror複寫。

- * 通知 * ：使用 "每桶事件通知" 可向指定的外部 Amazon Simple Notification Service ™ （ SNS ） 發送有關對對象執行的特定操作的通知。

  例如、您可以設定要傳送警示給系統管理員、以通知新增至儲存區的每個物件、其中物件代表與重大系統事件相關的記錄檔。

  > 雖然事件通知可在已啟用S3物件鎖定的儲存區上設定、但通知訊息中不會包含物件的S3物件鎖定中繼資料（包括「保留直到日期」和「法定保留」狀態）。

- * 搜尋整合服務 * ：使用 "搜尋整合服務" 將 S3 物件中繼資料傳送至指定的彈性搜尋索引、以便使用外部服務搜尋或分析中繼資料。

  例如、您可以設定儲存區、將S3物件中繼資料傳送至遠端Elasticsearch服務。然後您可以使用Elasticsearch來執行跨儲存區的搜尋、並對物件中繼資料中的模式進行精密分析。

  > 雖然可在啟用S3物件鎖定的儲存區上設定Elasticsearch整合、但通知訊息中不會包含物件的S3物件鎖定中繼資料（包括「保留直到日期」和「法定保留」狀態）。

由於平台服務的目標位置通常是StorageGRID 不受您的支援、因此平台服務可讓您靈活運用外部儲存資源、通知服務、以及搜尋或分析資料服務。

任何平台服務組合都可設定為單一S3儲存區。例如、您可以在StorageGRID S3儲存區上設定CloudMirror服務和通知、以便將特定物件鏡射至Amazon Simple Storage Service、同時將每個物件的通知傳送至協力廠商監控應用程式、以協助您追蹤AWS費用。

> 每個租戶帳戶必須由StorageGRID 使用Grid Manager或Grid Management API的管理員啟用平台服務的使用。

平台服務的設定方式

平台服務會與您使用設定的外部端點通訊 "租戶管理程式" 或 "租戶管理API"。每個端點都代表一個外部目的地、例如StorageGRID 一個不支援的S3儲存區、一個Amazon Web Services儲存區、一個簡單通知服務（SNS）主題、或是在本機、AWS或其他地方代管的Elasticsearch叢集。

建立外部端點之後、您可以將 XML 組態新增至貯體、為某個貯體啟用平台服務。XML組態可識別儲存區應執行的物件、儲存區應採取的動作、以及儲存區應用於服務的端點。

您必須為每個要設定的平台服務新增個別的XML組態。例如：

- 如果您想要所有以金鑰開頭的物件 `/images` 若要複寫至Amazon S3儲存區、您必須將複寫組態新增至來源儲存區。
- 如果您也想要在這些物件儲存至儲存區時傳送通知、則必須新增通知組態。
- 最後、如果您要為這些物件的中繼資料建立索引、則必須新增用於實作搜尋整合的中繼資料通知組態。

組態XML的格式受用於實作StorageGRID 支援功能的S3 REST API所規範：

平台服務	**S3 REST API**
"CloudMirror複寫"	• 取得庫位複寫 • 放入資源桶複寫
"通知"	• 取得庫存箱通知 • 放置時段通知
"搜尋整合"	• 取得Bucket中繼資料通知組態 • 放置時段中繼資料通知組態 這些作業是根據StorageGRID 需求量身打造的。

相關資訊

"平台服務的考量"

"使用S3 REST API"

CloudMirror複寫服務

如果您想StorageGRID 要將新增至儲存區的指定物件複寫到一或多個目的地儲存區、則可以針對S3儲存區啟用CloudMirror複寫。

CloudMirror複寫作業獨立於網格的作用中ILM原則。CloudMirror服務會在物件儲存到來源儲存區時複寫物件、並盡快將物件傳送到目的地儲存區。物件擷取成功時、會觸發複寫物件的交付。

CloudMirror 複寫與跨網格複寫功能有重要的相似之處和差異。若要深入瞭解、請參閱 "比較跨網格複寫和 CloudMirror 複寫"。

如果您為現有的儲存區啟用CloudMirror複寫、則只會複寫新增至該儲存區的新物件。貯體中的任何現有物件都不會複寫。若要強制複寫現有物件、您可以執行物件複本來更新現有物件的中繼資料。

如果您使用 CloudMirror 複寫功能將物件複製到 Amazon S3 目的地、請注意 Amazon S3 會將每個 Put 要求標頭內使用者定義的中繼資料大小限制在 2 KB 。如果物件的使用者定義中繼資料大於2 KB、則不會複寫該物件。

在這個功能中、您可以將單一儲存區中的物件複寫到多個目的地儲存區。StorageGRID若要這麼做、請在複寫組態XML中指定每個規則的目的地。您無法同時將物件複寫到多個儲存庫。

此外、您可以在版本控制或未版本控制的儲存區上設定CloudMirror複寫、也可以將版本控制或未版本控制的儲存區指定為目的地。您可以使用任何版本控制和未版本控制的儲存區組合。例如、您可以將版本控制的儲存區指定為未版本化來源儲存區的目的地、反之亦然。您也可以在未版本化的儲存區之間進行複寫。

CloudMirror複寫服務的刪除行為與Amazon S3提供的跨區域複寫（CRR）服務的刪除行為相同、刪除來源儲存區中的物件時、永遠不會刪除目的地中的複寫物件。如果來源和目的地儲存區都有版本、則會複寫刪除標記。如果目的地庫位沒有版本化、刪除來源庫位中的物件不會將刪除標記複寫到目的地庫位、也不會刪除目的地物件。

物件複寫到目的地庫位時StorageGRID 、將其標示為「plicas」。 目的地StorageGRID 循環庫不會再次複寫標示為複本的物件、可防止意外的複寫迴圈。此複本標記為StorageGRID 內部的物件、並不妨礙您在使用Amazon S3儲存區作為目的地時、運用AWS CRR。

用於標記複本的自訂標頭為 `x-ntap-sg-replica`。此標記可防止串聯鏡射。StorageGRID 確實支援兩個網格之間的雙向 CloudMirror 。

目的地貯體中事件的獨特性和順序不受保證。為了保證交付成功、可能會將多個相同的來源物件複本傳送至目的地。在極少數情況下、當同一個物件同時從兩StorageGRID 個或更多不同的站台更新時、目的地庫位上的作業順序可能與來源庫位上的事件順序不符。

CloudMirror複寫通常設定為使用外部S3儲存區作為目的地。不過、您也可以將複寫設定為使用其他StorageGRID 的支援功能或任何S3相容服務。

瞭解庫存箱通知

如果您想StorageGRID 要將有關特定事件的通知傳送至目的地Amazon Simple Notification Service（SNS）、您可以啟用S3儲存區的事件通知。

您可以 "設定事件通知" 將通知組態XML與來源儲存區建立關聯。通知組態XML遵循S3慣例來設定儲存區通知、目的地SNS主題則指定為端點的URN。

事件通知會在通知組態中指定的來源儲存區建立、並傳送至目的地。如果與物件相關聯的事件成功、就會建立該事件的通知並排入傳送佇列。

無法保證通知的唯一性和順序。由於為了確保交付成功而採取的作業、可能會將多個事件通知傳送到目的地。由於交付方式非同步、因此無法保證目的地的通知時間順序與來源庫位事件的順序相符、尤其是來自不同StorageGRID 的站台的作業。您可以使用 `sequencer` 請輸入事件訊息、以判斷特定物件的事件順序、如Amazon S3文件所述。

支援的通知和訊息

StorageGRID 事件通知遵循 Amazon S3 API 、但有一些限制：

- 支援下列事件類型：
  - S3 ： ObjectCreated ： *

- S3 ： ObjectCreated ： Put
- S3 ： ObjectCreated ： Post
- S3 ： ObjectCreated ：複製
- S3 ： ObjectCreated ： CompleteMultpartUpload
- S3 ： ObjectRemoved ： *
- S3:ObjectRemoved ：刪除
- S3 ： ObjectRemoved ：刪除 MarkerCreated
- S3 ： ObjectRestore ： Post

- 從 StorageGRID 傳送的事件通知使用標準 JSON 格式、但不包含某些金鑰、也不為其他金鑰使用特定值、如下表所示：

金鑰名稱	價值**StorageGRID**
事件來源	`sgws:s3`
awsRegion	不含
X-amz-id-2	不含
不需要	`urn:sgws:s3:::bucket_name`

瞭解搜尋整合服務

如果您想要使用外部搜尋與資料分析服務來取得物件中繼資料、可以啟用S3儲存區的搜尋整合。

搜尋整合服務是一StorageGRID 項自訂的功能、可在物件或其中繼資料更新時、自動且非同步地將S3物件中繼資料傳送至目的地端點。然後、您可以使用目的地服務所提供的精密搜尋、資料分析、視覺化或機器學習工具、來搜尋、分析物件資料、並從中獲得深入見解。

您可以針對任何版本控制或未版本控制的儲存區啟用搜尋整合服務。搜尋整合是透過將中繼資料通知組態XML與儲存區建立關聯來設定、此儲存區會指定要在哪些物件上執行動作、以及物件中繼資料的目的地。

以Json文件的形式產生通知、其名稱為儲存區名稱、物件名稱及版本ID（如果有）。每個中繼資料通知都包含物件的標準系統中繼資料集、以及物件的所有標記和使用者中繼資料。

針對標記和使用者中繼資料StorageGRID 、將日期和數字以字串或S3事件通知的形式傳送至Elasticsearch。若要設定Elasticsearch將這些字串解譯為日期或數字、請遵循Elasticsearch指示進行動態欄位對應、以及對應日期格式。您必須先在索引上啟用動態欄位對應、才能設定搜尋整合服務。建立文件索引後、您就無法編輯索引中文件的欄位類型。

在下列情況下、系統會產生通知並排入傳送佇列：

- 隨即建立物件。
- 刪除物件、包括因網格ILM原則運作而刪除物件的時間。

- 物件中繼資料或標記會新增、更新或刪除。一律會在更新時傳送完整的中繼資料和標記集、而不只是變更的值。

將中繼資料通知組態XML新增至儲存區之後、系統會針對您所建立的任何新物件、以及您透過更新其資料、使用者中繼資料或標記來修改的任何物件、傳送通知。然而、對於已在貯體中的任何物件、則不會傳送通知。若要確保儲存區中所有物件的物件中繼資料都會傳送到目的地、您應該執行下列其中一項：

- 在建立儲存區之後、以及新增任何物件之前、請立即設定搜尋整合服務。
- 對儲存庫中已有的所有物件執行動作、以觸發將中繼資料通知訊息傳送至目的地。

支援以Elasticsearch叢集作為目的地的支援。StorageGRID如同其他平台服務、目的地是在端點中指定、而其URN則用於服務的組態XML中。使用 "NetApp 互通性對照表工具" 以判斷受支援版本的Elasticsearch。

相關資訊

"搜尋整合的組態XML"

"中繼資料通知中包含的物件中繼資料"

"由搜尋整合服務產生的JSON"

"設定搜尋整合服務"

平台服務的考量

在實作平台服務之前、請先檢閱使用這些服務的建議與考量事項。

如需S3的相關資訊、請參閱 "使用S3 REST API"。

使用平台服務的考量

考量	詳細資料
目的地端點監控	您必須監控每個目的地端點的可用度。如果連線到目的地端點的時間過長、而且有大量的要求待處理、那麼額外的用戶端要求StorageGRID （例如提出要求）將會失敗。當端點可連線時、您必須重試這些失敗的要求。
目的地端點節流	如果傳送要求的速度超過目的地端點接收要求的速度、則支援使用此軟體來限制傳入S3的貯體要求。StorageGRID節流只會在有待傳送至目的地端點的要求待處理項目時發生。 唯一的可見效果是傳入S3要求執行時間較長。如果您開始偵測到效能大幅降低、應該降低擷取速度、或是使用容量較大的端點。如果要求的待處理項目持續增加、用戶端S3作業（例如PUT要求）最終將會失敗。 CloudMirror要求較容易受到目的地端點效能的影響、因為這些要求通常比搜尋整合或事件通知要求涉及更多資料傳輸。

考量	詳細資料
訂購保證	可保證站台內物件的作業順序。StorageGRID只要物件的所有作業都在同一個站台內、最終的物件狀態（用於複寫）就會永遠等於StorageGRID 該站台的狀態。 在整個景點進行作業時、盡力訂購申請。StorageGRID StorageGRID例如、如果您一開始將物件寫入站台A、然後在站台B覆寫相同的物件、則CloudMirror複寫到目的地儲存區的最終物件將無法保證為較新的物件。
ILM導向物件刪除	為了符合 AWS CRR 和 SNS 服務的刪除行為、當來源儲存區中的物件因 StorageGRID ILM 規則而遭到刪除時、 CloudMirror 和事件通知要求不會傳送。例如、如果ILM規則在14天後刪除物件、則不會傳送CloudMirror或事件通知要求。 相反地、因為ILM而刪除物件時、會傳送搜尋整合要求。

使用**CloudMirror**複寫服務的考量

考量	詳細資料
複寫狀態	不支援StorageGRID `x-amz-replication-status` 標頭。
物件大小	CloudMirror複寫服務可複寫至目的地儲存區的物件大小上限為5 TiB、與最大_supported物件大小相同。 附註：單一放置物件作業的最大_Recommended大小為5 GiB（5、368、709、120位元組）。如果您的物件大於5 GiB、請改用多部份上傳。
儲存區版本管理和版本ID	如果StorageGRID 支援版本管理功能的來源S3儲存區、您也應該啟用目的地儲存區的版本管理功能。 使用版本管理時、請注意、由於S3傳輸協定的限制、CloudMirror服務無法保證目的地儲存庫中物件版本的順序順序。 • 附註 * ： StorageGRID 中來源貯體的版本 ID 與目的地貯體的版本 ID 無關。
標記物件版本	由於S3傳輸協定的限制、CloudMirror服務不會複寫提供版本ID的任何「放置物件」標記或刪除物件標記要求。由於來源和目的地的版本識別碼不相關、因此無法確保將標記更新複寫到特定版本識別碼。 相反地、 CloudMirror 服務會複寫「放置物件」標記要求、或刪除未指定版本 ID 的「物件」標記要求。這些要求會更新最新金鑰的標記（如果儲存庫版本已有版本、則會更新最新版本）。也會複寫含有標記的一般擷取（非標記更新）。
多部份上傳和 `ETag` 價值	鏡射使用多重上傳的物件時、CloudMirror服務不會保留這些部分。因此 `ETag` 鏡射物件的值將與不同 `ETag` 原始物件的值。
使用SSE-C加密的物件（使用客戶提供的金鑰進行伺服器端加密）	CloudMirror服務不支援以SSE-C加密的物件如果您嘗試將物件擷取至來源儲存區以進行CloudMirror複寫、且要求中包含SSE-C要求標頭、則作業會失敗。

考量	詳細資料
啟用S3物件鎖定的儲存區	如果用於CloudMirror複寫的目的地S3儲存區已啟用S3物件鎖定、則設定儲存區複寫（放置儲存區複寫）的嘗試將會失敗、並顯示AccessDenied錯誤。

設定平台服務端點

您必須先將至少一個端點設定為平台服務的目的地、才能為某個服務區段設定平台服務。

平台服務的存取是StorageGRID 由NetApp管理員以每個租戶為單位來啟用。若要建立或使用平台服務端點、您必須是具有管理端點或根存取權限的租戶使用者、位於網路已設定為允許儲存節點存取外部端點資源的網格中。如StorageGRID 需詳細資訊、請聯絡您的管理員。

什麼是平台服務端點？

當您建立平台服務端點時、請指定StorageGRID 存取外部目的地所需的資訊。

例如、如果您想要將物件從 StorageGRID 儲存庫複寫到 Amazon S3 儲存區、您可以建立平台服務端點、其中包含 StorageGRID 存取 Amazon 上目的地儲存區所需的資訊和認證。

每種類型的平台服務都需要自己的端點、因此您必須為每個打算使用的平台服務至少設定一個端點。在定義平台服務端點之後、您可以在用來啟用服務的組態XML中、使用端點的URN作為目的地。

您可以將同一個端點作為多個來源儲存區的目的地。例如、您可以設定多個來源儲存區、將物件中繼資料傳送至同一個搜尋整合端點、以便在多個儲存區之間執行搜尋。您也可以將來源儲存區設定為使用多個端點做為目標、以便將有關物件建立的通知傳送至單一SNS主題、並將物件刪除的通知傳送至第二個SNS主題。

用於**CloudMirror**複寫的端點

支援代表S3儲存區的複寫端點。StorageGRID這些儲存庫可能託管在Amazon Web Services、相同或遠端StorageGRID 的功能或其他服務上。

通知的端點

支援Simple Notification Service（SNS）端點。StorageGRID不支援 Simple Queue Service （ SQS ）或 AWS Lambda 端點。

搜尋整合服務的端點

支援代表Elasticsearch叢集的搜尋整合端點。StorageGRID這些彈性搜尋叢集可以位於本機資料中心、也可以存放在 AWS 雲端或其他地方。

搜尋整合端點是指特定的彈性搜尋索引和類型。您必須先在Elasticsearch中建立索引、才能在StorageGRID 其中建立端點、否則端點建立將會失敗。建立端點之前、您不需要建立類型。如果需要、當將物件中繼資料傳送至端點時、將會建立類型。StorageGRID

相關資訊

"管理StorageGRID"

當您建立平台服務端點時、必須指定唯一的資源名稱（URN）。當您為平台服務建立組態XML時、將會使用URN來參考端點。每個端點的URN必須是唯一的。

當您建立平台服務端點時、此功能會驗證它們。StorageGRID在建立平台服務端點之前、請先確認端點中指定的資源是否存在、以及是否可以到達該端點。

urnElements

平台服務端點的URN必須從任一端開始 `arn:aws` 或 `urn:mysite`如下所示：

- 如果服務是在 Amazon Web Services （ AWS ）上代管、請使用 `arn:aws`。
- 如果服務是在 Google Cloud Platform （ GCP ）上代管、請使用 `arn:aws`。
- 如果服務是在本機代管、請使用 `urn:mysite`

例如、如果您要為StorageGRID 位於VMware上的CloudMirror端點指定URN、則可能會以開頭 `urn:sgws`。

URN的下一個元素會指定平台服務的類型、如下所示：

服務	類型
CloudMirror複寫	S3
通知	SnS
搜尋整合	ES

例如、若要繼續為StorageGRID 位於支援的CloudMirror端點指定URN、您可以新增 `s3` 以取得 `urn:sgws:s3`。

URN的最後一個元素會在目的地URI上識別特定的目標資源。

服務	特定資源
CloudMirror複寫	儲存庫名稱
通知	SnS-topic-name
搜尋整合	`domain-name/index-name/type-name` *注意：*如果Elasticsearch叢集*未*設定為自動建立索引、則必須在建立端點之前手動建立索引。

提供**AWS**和**GCP**上的服務

對於AWS和GCP實體而言、完整的URN是有效的AWS ARN。例如：

- CloudMirror複寫：

```
arn:aws:s3:::bucket-name
```

- 通知：

```
arn:aws:sns:region:account-id:topic-name
```

- 搜尋整合：

```
arn:aws:es:region:account-id:domain/domain-name/index-name/type-name
```

> 如需AWS搜尋整合端點、請使用 `domain-name` 必須包含文字字串 `domain/`、如下所示。

適用於本機代管服務

使用本機代管服務而非雲端服務時、只要URN在第三和最後的位置中包含必要的元素、您就可以以任何方式指定URN、以建立有效且獨特的URN。您可以將選用的元素保留空白、也可以以任何方式指定這些元素、協助您識別資源並使URN成為唯一的。例如：

- CloudMirror複寫：

```
urn:mysite:s3:optional:optional:bucket-name
```

若為StorageGRID 以支援此功能的CloudMirror端點、您可以指定以開頭的有效URN `urn:sgws`：

```
urn:sgws:s3:optional:optional:bucket-name
```

- 通知：

```
urn:mysite:sns:optional:optional:sns-topic-name
```

- 搜尋整合：

```
urn:mysite:es:optional:optional:domain-name/index-name/type-name
```

> 對於本機代管的搜尋整合端點 `domain-name` 元素可以是任何字串、只要端點的URN是唯一的。

您必須至少建立一個正確類型的端點、才能啟用平台服務。

開始之前

- 您將使用登入租戶管理程式 "支援的網頁瀏覽器"。
- StorageGRID 管理員已為您的租戶帳戶啟用平台服務。
- 您屬於具有的使用者群組 "管理端點或根存取權限"。
- 已建立平台服務端點所參照的資源：
  - CloudMirror複寫：S3儲存區
  - 事件通知：SnS主題
  - 搜尋通知：彈性搜尋索引、如果目的地叢集未設定為自動建立索引。
- 您有關於目的地資源的資訊：
  - 統一資源識別元（URI）的主機和連接埠

    如果您計畫將裝載在StorageGRID 某個SnapMirror系統上的儲存庫當作CloudMirror複寫的端點、請聯絡網格管理員、以判斷您需要輸入的值。

  - 獨特資源名稱（URN）

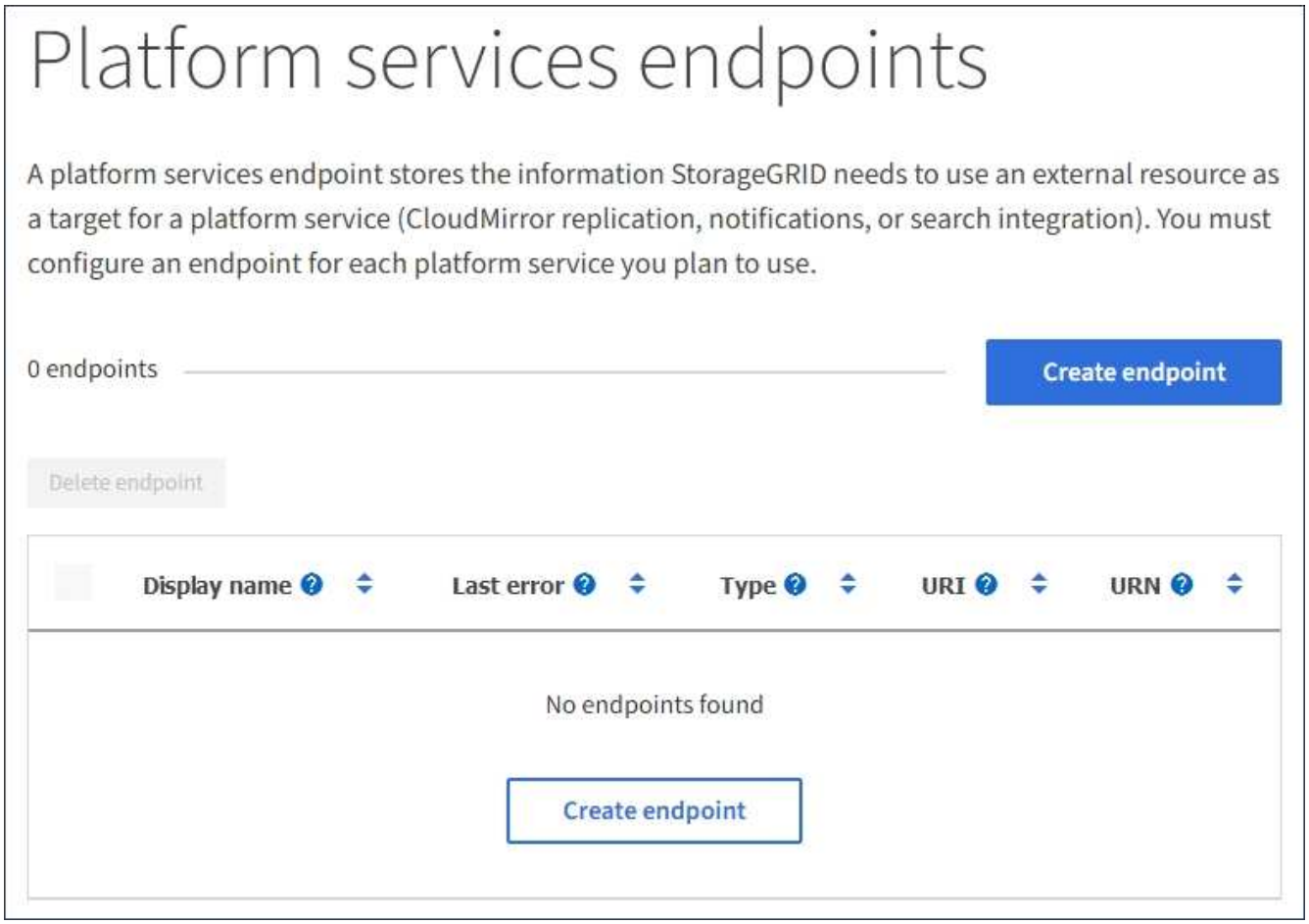
    "指定平台服務端點的URN"

  - 驗證認證資料（若有需要）：
    - 存取金鑰：存取金鑰ID和秘密存取金鑰
    - 基本HTTP：使用者名稱和密碼
    - CAP（C2S存取入口網站）：暫用認證URL、伺服器與用戶端認證、用戶端金鑰、以及選用的用戶端私密金鑰複雜密碼。
  - 安全性憑證（如果使用自訂CA憑證）
- 如果啟用彈性搜尋安全功能、您就擁有監控叢集權限來進行連線測試、以及寫入索引權限、或是索引和刪除文件更新的索引權限。

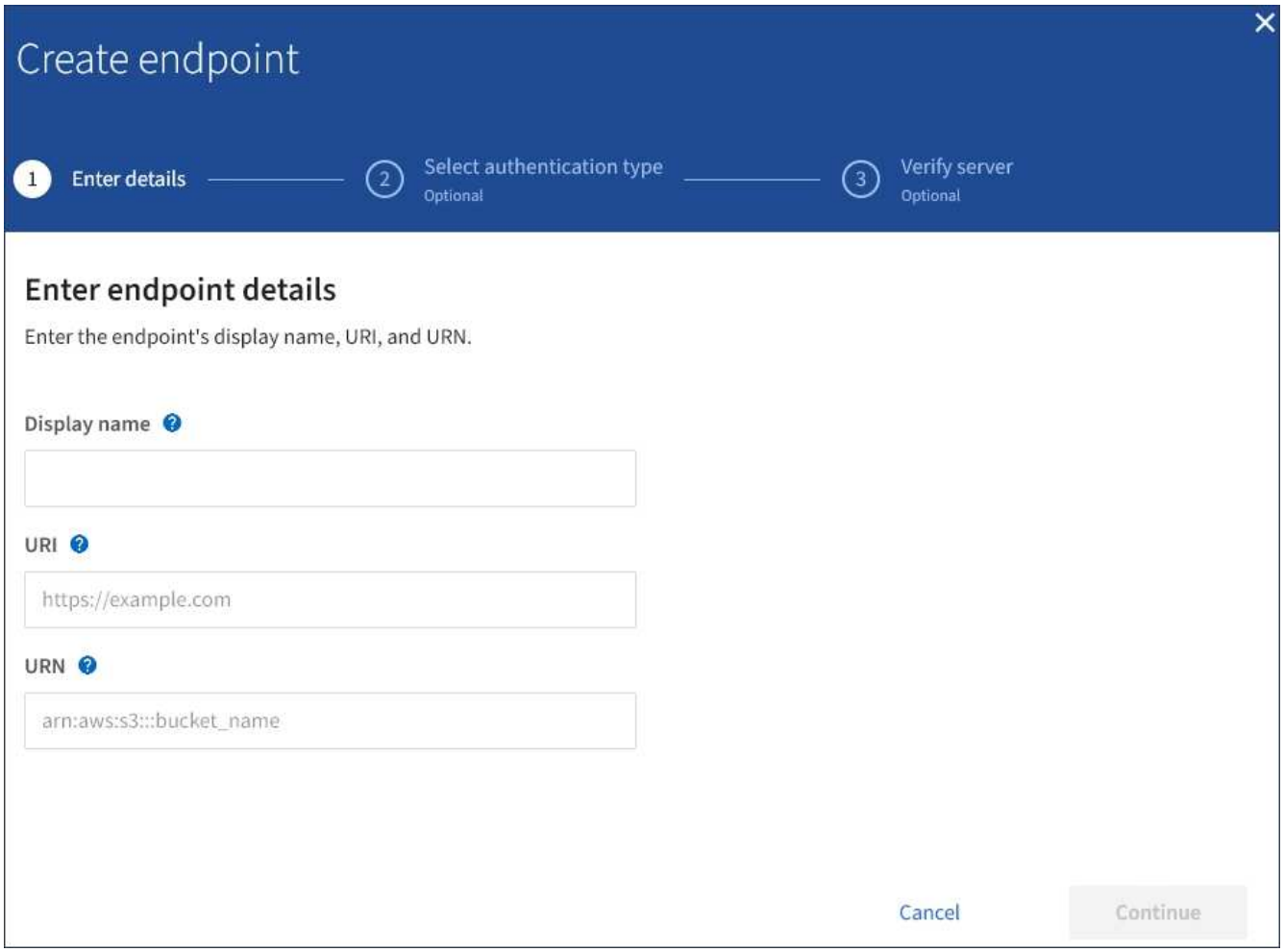
步驟

1. 選擇*儲存設備（S3）>*平台服務端點。

   「平台服務端點」頁面隨即出現。


Platform services endpoints
A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.
0 endpoints
Create endpoint
Delete endpoint
Display name
Last error
Type
URI
URN
No endpoints found
Create endpoint

2. 選取*建立端點*。



3. 輸入顯示名稱、簡短說明端點及其用途。

   端點支援的平台服務類型會顯示在端點名稱旁邊、端點名稱會列在端點頁面上、因此您不需要在名稱中包含該資訊。

4. 在「* URI *」欄位中、指定端點的唯一資源識別元（URI）。

   請使用下列其中一種格式：

   ```
   https://host:port
   http://host:port
   ```

   如果您未指定連接埠、則會將連接埠 443 用於 HTTPS URI 、並將連接埠 80 用於 HTTP URI 。

   例如StorageGRID 、裝載於列舉在整個基礎上的儲存區的URI可能是：

   ```
   https://s3.example.com:10443
   ```

   在此範例中、 `s3.example.com` 表示StorageGRID 支援虛擬IP（VIP）的DNS項目、以及 `10443` 表示負載平衡器端點中定義的連接埠。

您應該盡可能連線到 HA 群組的負載平衡節點、以避免單點故障。

同樣地、AWS上裝載的儲存區URI可能是：

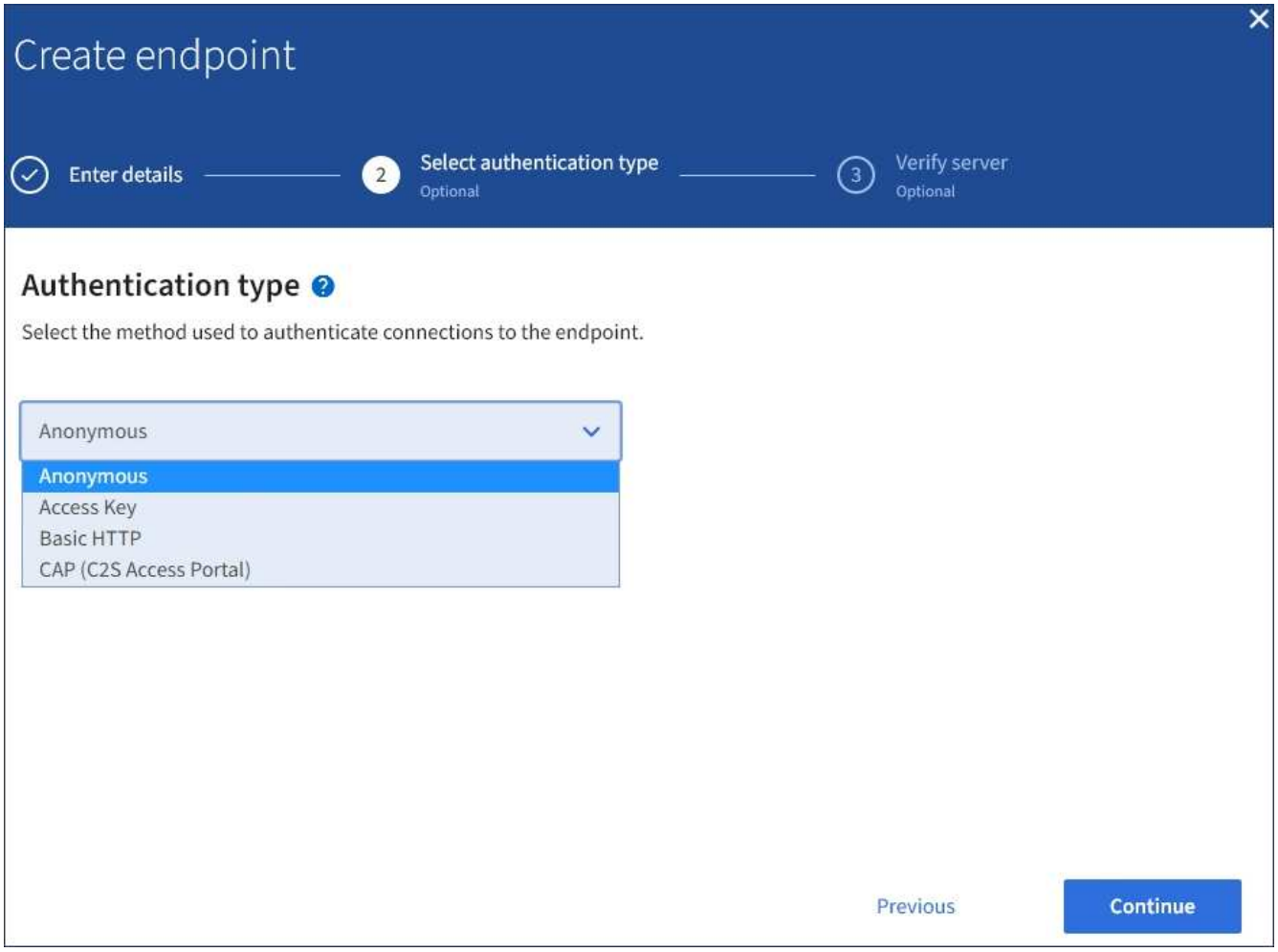
```
https://s3-aws-region.amazonaws.com
```

如果端點用於 CloudMirror 複寫服務、請勿在 URI 中包含貯體名稱。您可以在「* URN*」欄位中加入貯體名稱。

5. 輸入端點的唯一資源名稱（URN）。

建立端點後、您無法變更端點的 URN 。

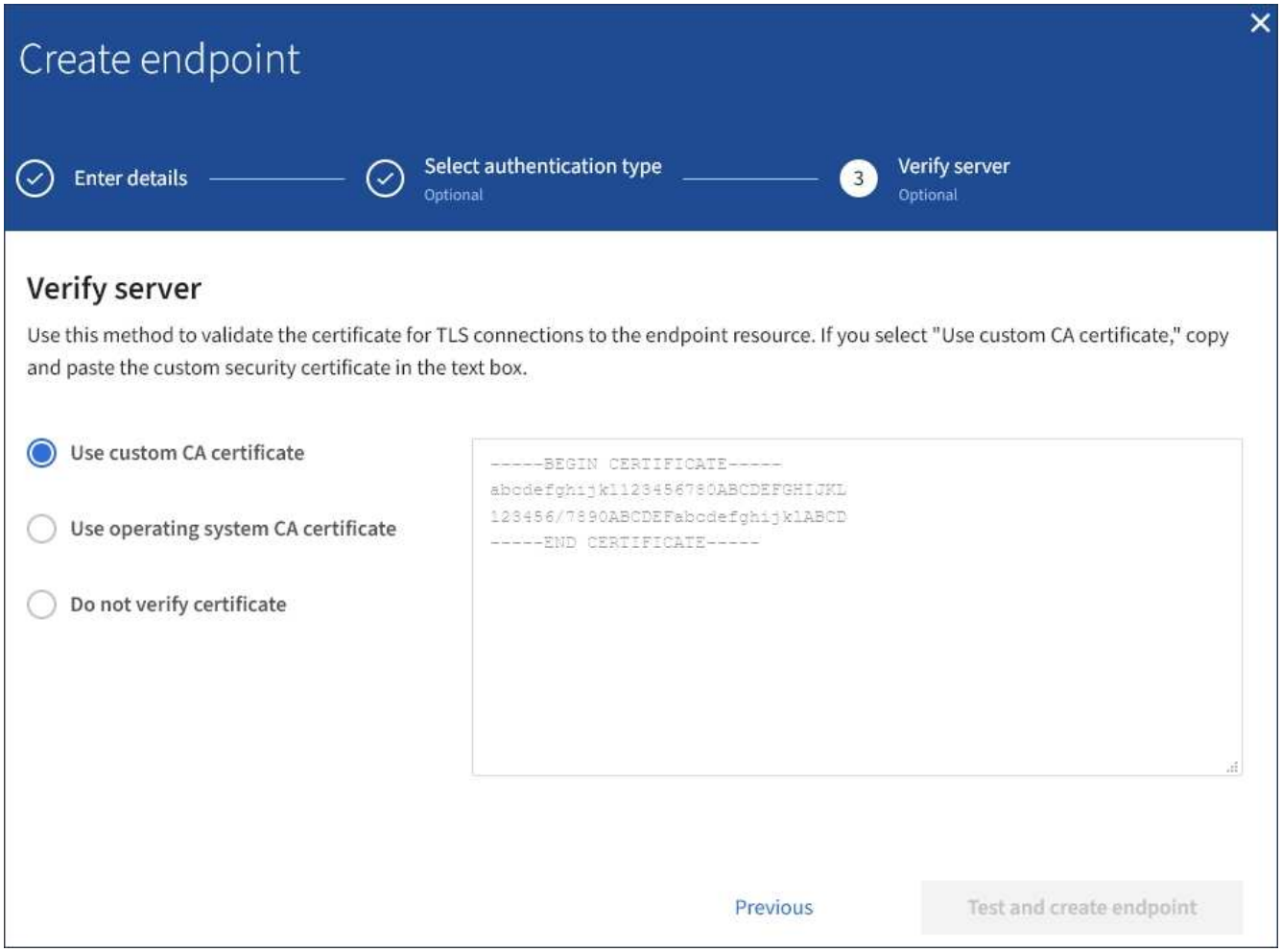
6. 選擇*繼續*。
7. 選取*驗證類型*的值、然後輸入或上傳所需的認證資料。



您提供的認證必須具有目的地資源的寫入權限。

驗證類型	說明	認證資料
匿名	提供對目的地的匿名存取。僅適用於停用安全性的端點。	無驗證。
存取金鑰	使用AWS型認證來驗證與目的地的連線。	• 存取金鑰ID • 機密存取金鑰
基本HTTP	使用使用者名稱和密碼來驗證目的地的連線。	• 使用者名稱 • 密碼
CAP（C2S存取入口網站）	使用憑證和金鑰來驗證與目的地的連線。	• 暫用認證URL • 伺服器CA憑證（PEE檔案上傳） • 用戶端憑證（PEE檔案上傳） • 用戶端私密金鑰（上傳PEE檔案、OpenSSL加密格式或未加密的私密金鑰格式） • 用戶端私密金鑰複雜密碼（選用）

8. 選擇*繼續*。
9. 選取*驗證伺服器*的選項按鈕、以選擇驗證TLS與端點的連線方式。



憑證驗證類型	說明
使用自訂CA憑證	使用自訂安全性憑證。如果您選取此設定、請複製並貼上「* CA認證 *」文字方塊中的自訂安全性認證。
使用作業系統CA憑證	使用作業系統上安裝的預設Grid CA憑證來保護連線安全。
請勿驗證憑證	用於TLS連線的憑證尚未驗證。此選項不安全。

10. 選擇*測試並建立端點*。
    - 如果可以使用指定的認證資料來連線至端點、則會出現一則成功訊息。端點的連線會從每個站台的一個節點驗證。
    - 當端點驗證失敗時、會出現錯誤訊息。如果您需要修改端點以修正錯誤、請選取*返回端點詳細資料*並更新資訊。然後選取*測試並建立端點*。

> 如果您的租戶帳戶未啟用平台服務、端點建立將會失敗。請聯絡StorageGRID 您的系統管理員。

設定端點之後、您可以使用其URN來設定平台服務。

相關資訊

"指定平台服務端點的URN"

"設定CloudMirror複寫"

"設定事件通知"

"設定搜尋整合服務"

測試平台服務端點的連線

如果平台服務的連線已變更、您可以測試端點的連線、以驗證目的地資源是否存在、以及是否可以使用您指定的認證來連線。

開始之前

- 您將使用登入租戶管理程式 "支援的網頁瀏覽器"。
- 您屬於具有的使用者群組 "管理端點或根存取權限"。

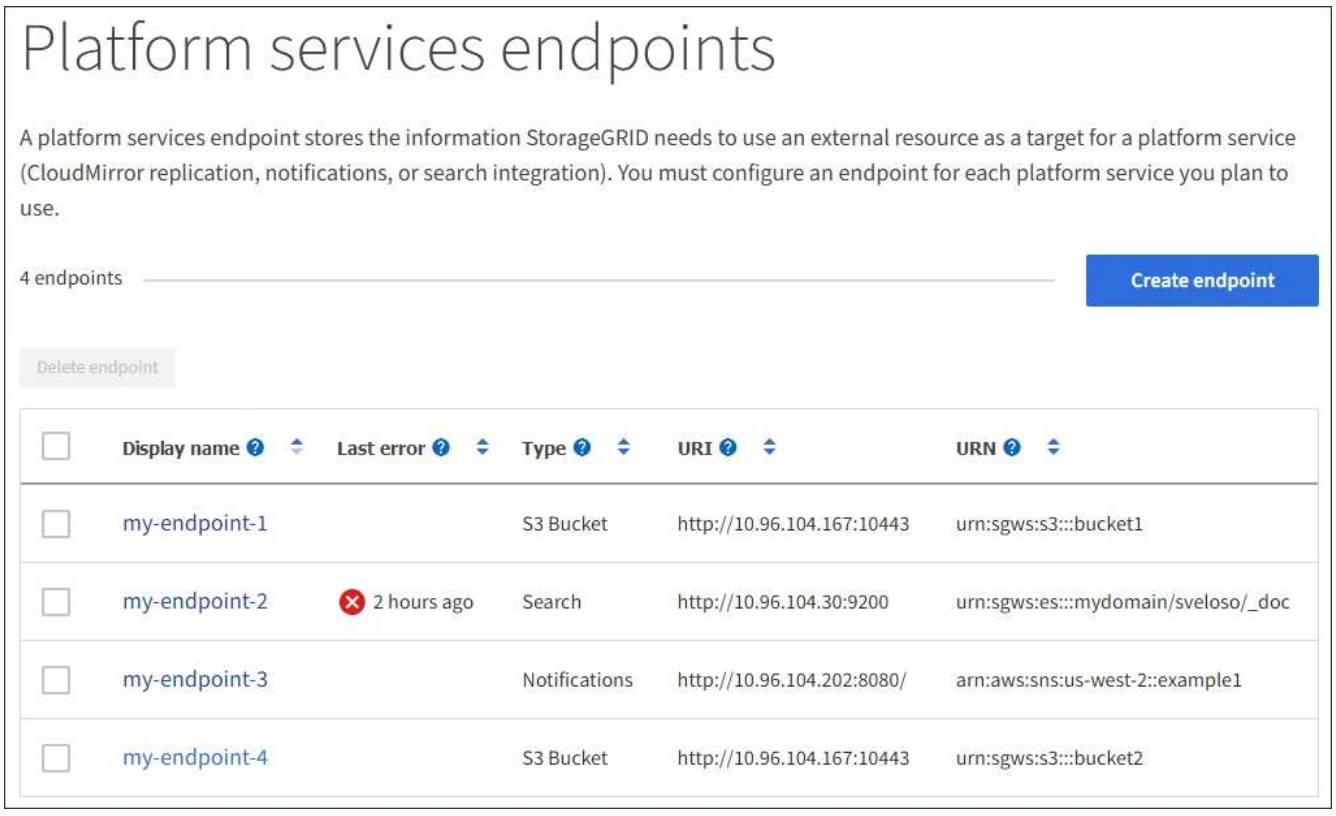
關於這項工作

無法驗證認證資料是否擁有正確的權限。StorageGRID

步驟

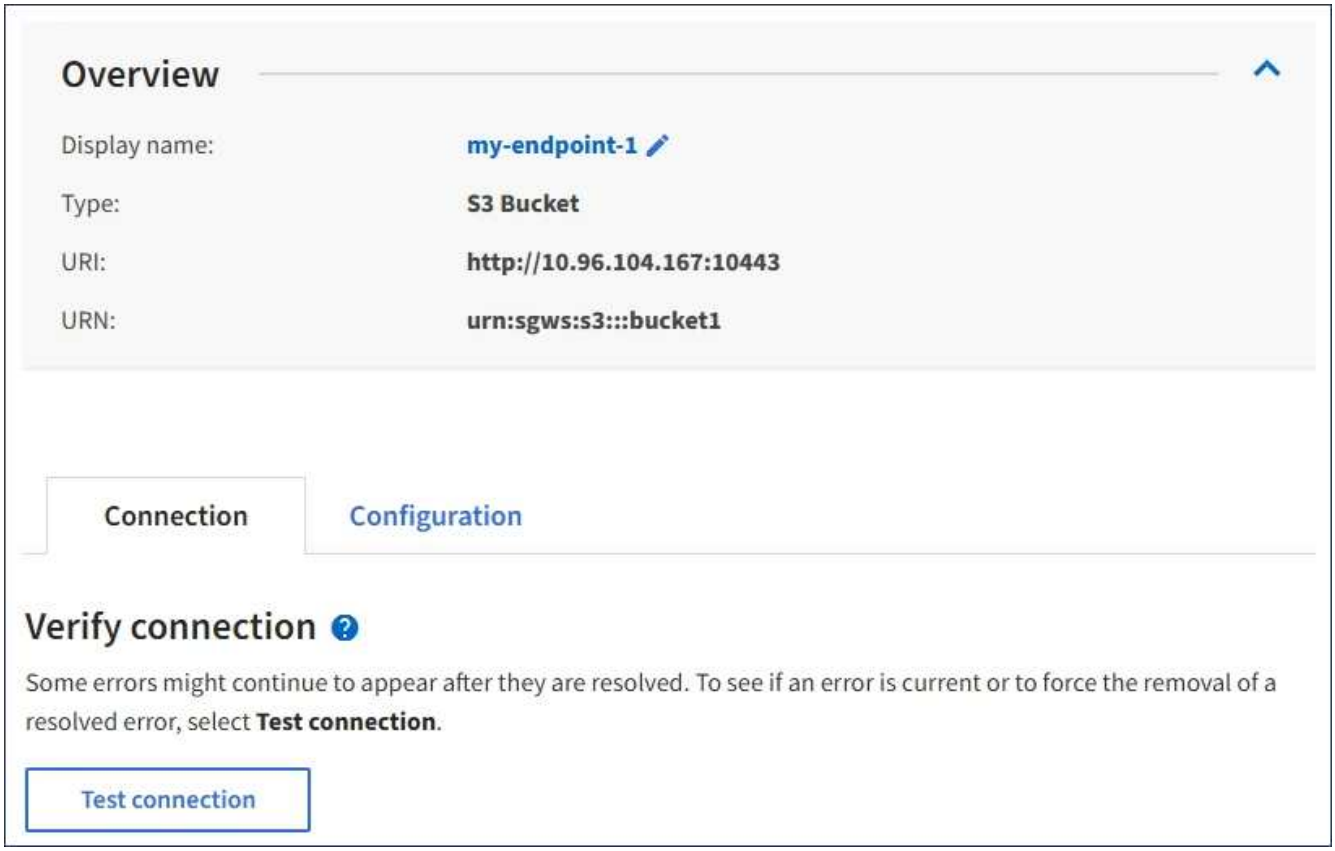
1. 選擇*儲存設備（S3）>*平台服務端點。

   「平台服務端點」頁面隨即出現、並顯示已設定的平台服務端點清單。



2. 選取您要測試其連線的端點。

端點詳細資料頁面隨即出現。



3. 選擇*測試連線*。
   - 如果可以使用指定的認證資料來連線至端點、則會出現一則成功訊息。端點的連線會從每個站台的一個節點驗證。
   - 當端點驗證失敗時、會出現錯誤訊息。如果您需要修改端點以修正錯誤、請選取*組態*並更新資訊。然後選取*測試並儲存變更*。

編輯平台服務端點

您可以編輯平台服務端點的組態、以變更其名稱、URI或其他詳細資料。例如、您可能需要更新過期的認證資料、或是變更URI以指向備份Elasticsearch索引以進行容錯移轉。您無法變更平台服務端點的 URN 。

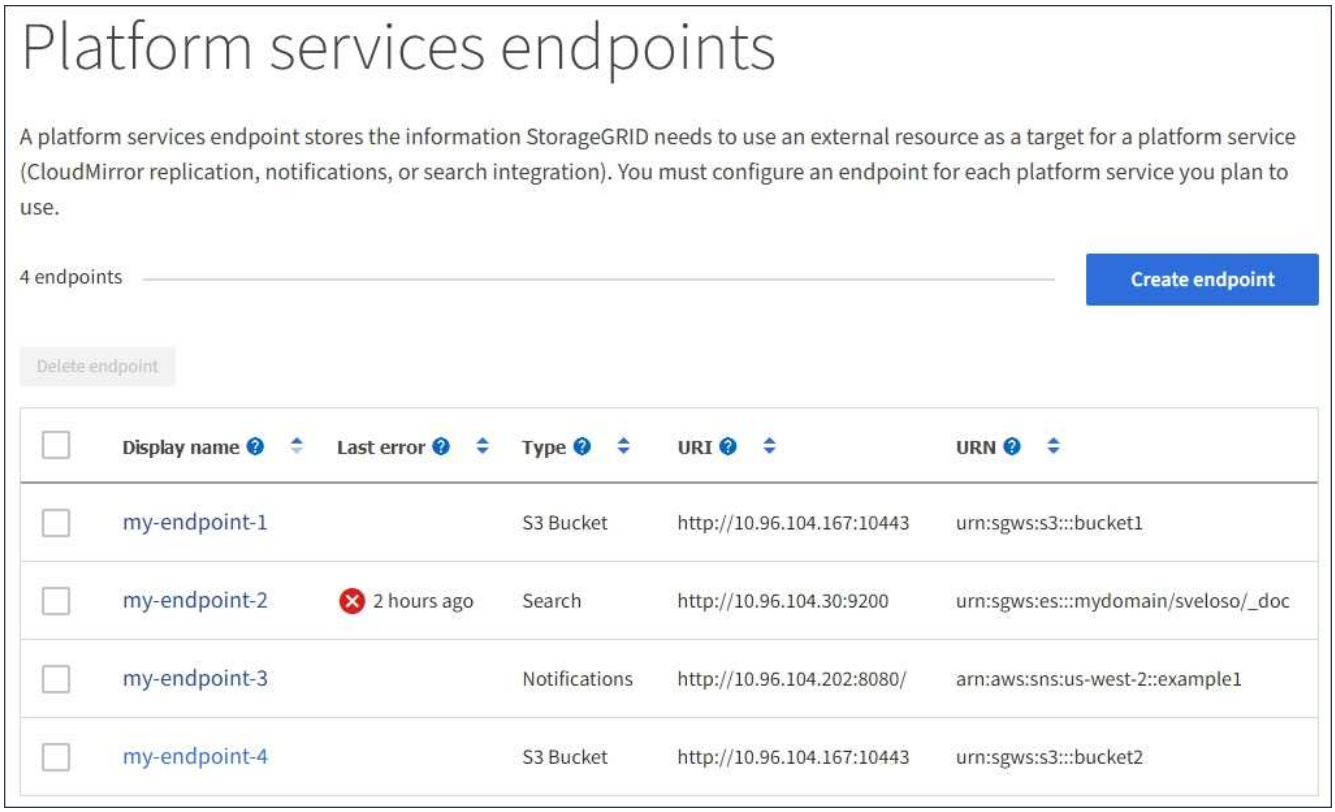
開始之前

- 您將使用登入租戶管理程式 "支援的網頁瀏覽器"。
- 您屬於具有的使用者群組 "管理端點或根存取權限"。

步驟

1. 選擇*儲存設備（S3）>*平台服務端點。

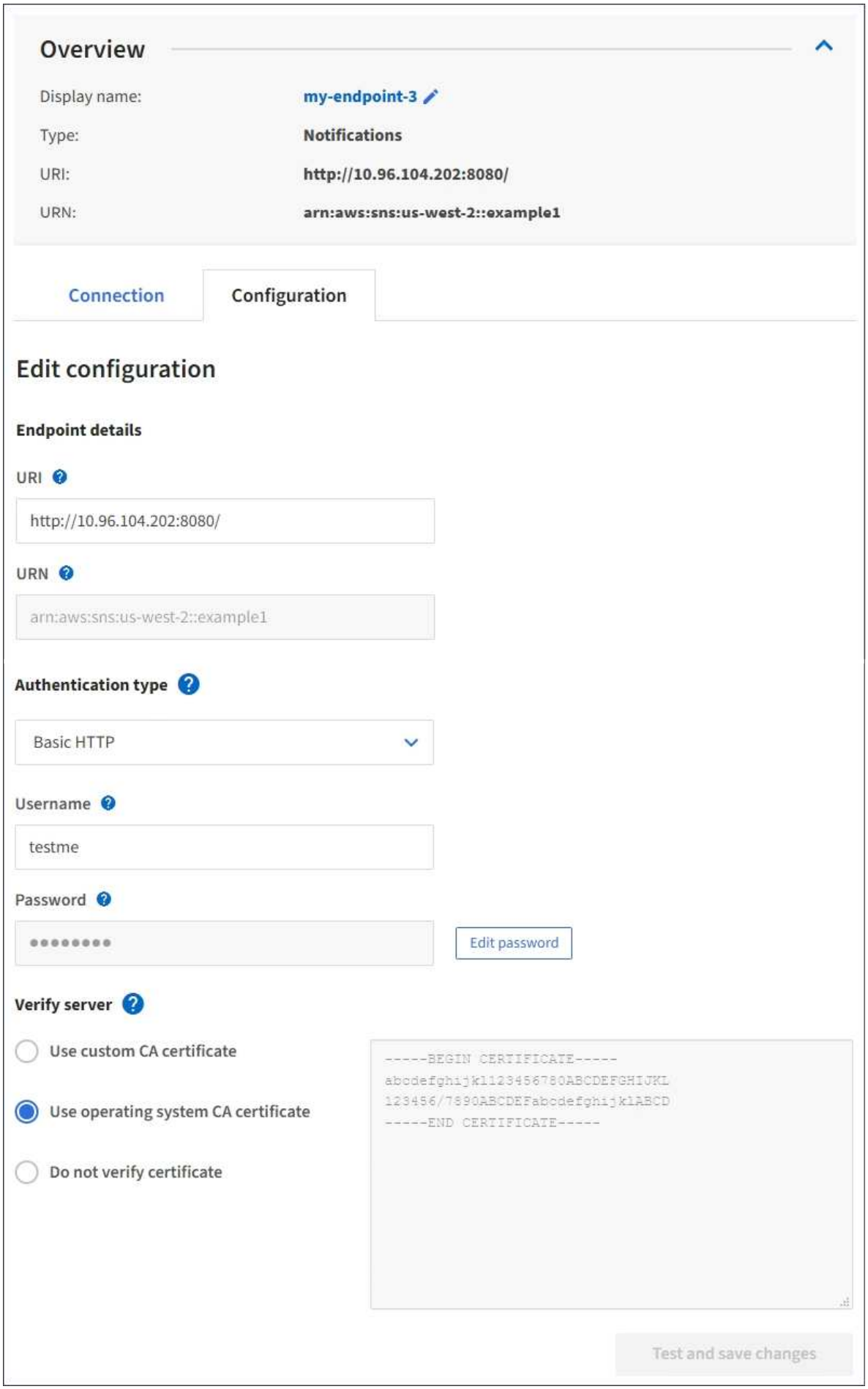
   「平台服務端點」頁面隨即出現、並顯示已設定的平台服務端點清單。



2. 選取您要編輯的端點。

   端點詳細資料頁面隨即出現。

3. 選擇*組態*。


Overview
Display name:
my-endpoint-3
Type:
Notifications
URI:
http://10.96.104.202:8080/
URN:
arn:aws:sns:us-west-2::example1
Connection
Configuration
Edit configuration
Endpoint details
URI
http://10.96.104.202:8080/
URN
arn:aws:sns:us-west-2::example1
Authentication type
Basic HTTP
Username
testme
Password
Edit password
Verify server
Use custom CA certificate
Use operating system CA certificate
Do not verify certificate
-----BEGIN CERTIFICATE-----
abcdefghijkl123456780ABCDEFGHIJKL
123456/7890ABCDEFabcdefghijklABCD
-----END CERTIFICATE-----
Test and save changes

4. 視需要變更端點的組態。

   建立端點後、您無法變更端點的 URN 。

   a. 若要變更端點的顯示名稱、請選取編輯圖示 。

   b. 視需要變更URI。

   c. 視需要變更驗證類型。

      - 若要進行存取金鑰驗證、請視需要變更金鑰、方法是選取*編輯S3金鑰*、然後貼上新的存取金鑰ID和秘密存取金鑰。如果您需要取消變更、請選取*恢復S3金鑰編輯*。
      - 如需基本HTTP驗證、請視需要變更使用者名稱。選取*編輯密碼*並輸入新密碼、即可視需要變更密碼。如果您需要取消變更、請選取*恢復密碼編輯*。
      - 若要進行CAP（C2S存取入口網站）驗證、請變更暫用認證URL或選用的用戶端私密金鑰通關密碼、並視需要上傳新的憑證和金鑰檔案。

        用戶端私密金鑰必須為OpenSSL加密格式或未加密的私密金鑰格式。

   d. 視需要變更驗證伺服器的方法。

5. 選擇*測試並儲存變更*。

   ◦ 如果可以使用指定的認證資料來連線至端點、則會出現一則成功訊息。端點的連線會從每個站台的一個節點進行驗證。

   ◦ 當端點驗證失敗時、會出現錯誤訊息。修改端點以修正錯誤、然後選取*測試並儲存變更*。

刪除平台服務端點

如果您不想再使用相關的平台服務、可以刪除端點。

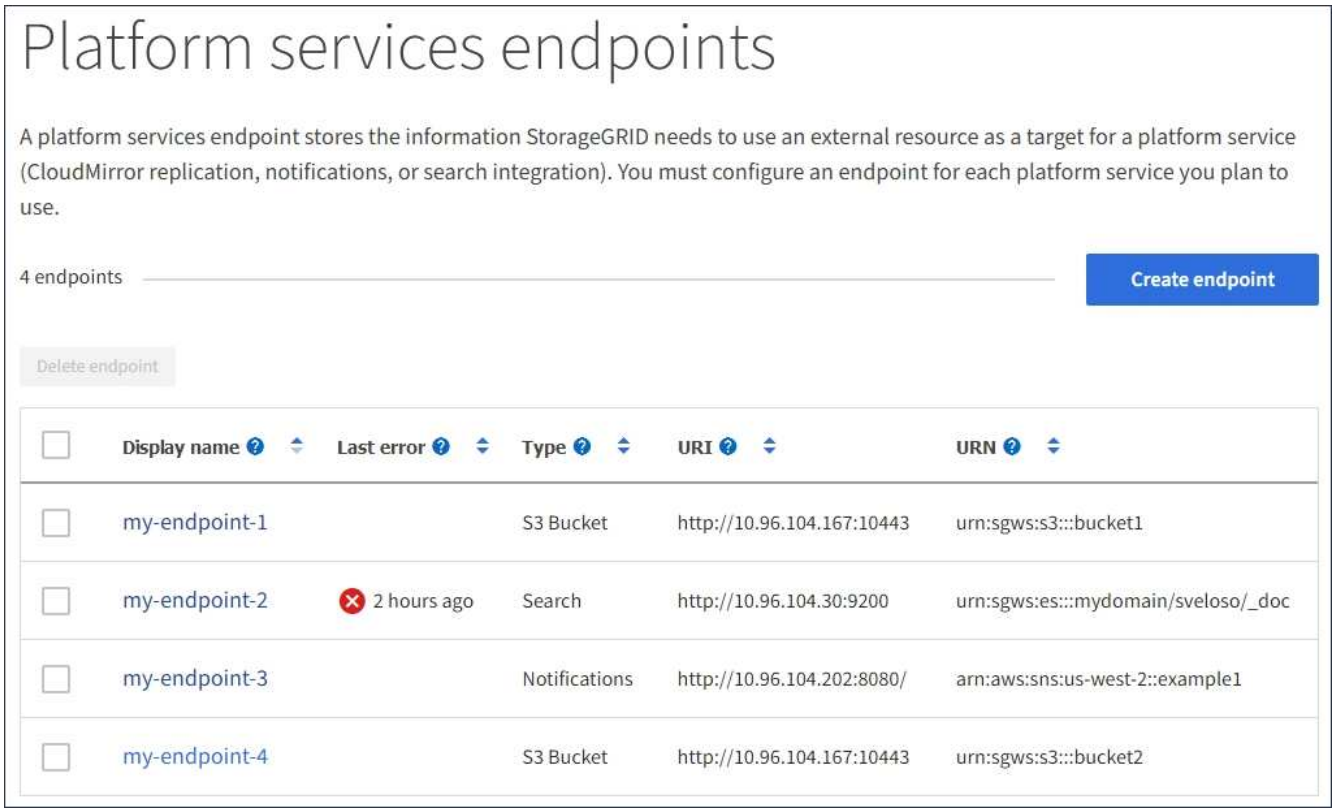
開始之前

- 您將使用登入租戶管理程式 "支援的網頁瀏覽器"。
- 您屬於具有的使用者群組 "管理端點或根存取權限"。

步驟

1. 選擇*儲存設備（S3）>*平台服務端點。

   「平台服務端點」頁面隨即出現、並顯示已設定的平台服務端點清單。

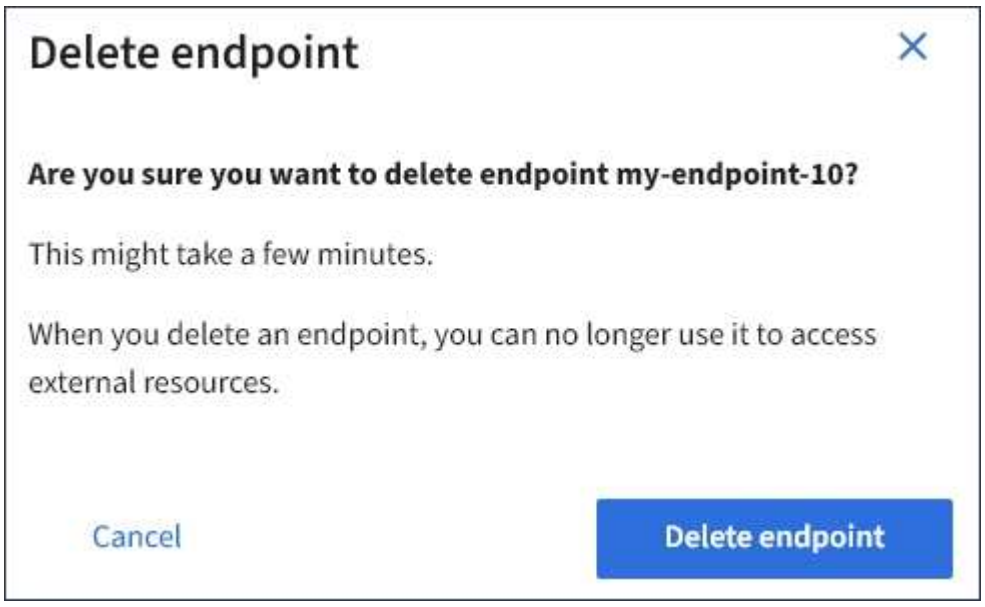


2. 選取您要刪除的每個端點的核取方塊。

> 如果您刪除使用中的平台服務端點、則使用端點的任何貯體都會停用相關的平台服務。任何尚未完成的要求都會被捨棄。在您將庫位組態變更為不再參照已刪除的URN之前、將會繼續產生任何新的要求。將這些要求報告為不可恢復的錯誤。StorageGRID

3. 選取*「動作*」>*「刪除端點*」。

隨即顯示確認訊息。

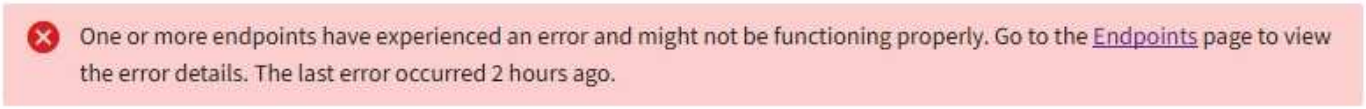


4. 選擇*刪除端點*。

如果 StorageGRID 嘗試與平台服務端點通訊時發生錯誤、儀表板上會顯示訊息。在「Platform Services Endives」（平台服務端點）頁面上、最後一個錯誤欄位會指出錯誤發生的時間已過多久。如果端點認證的相關權限不正確、則不會顯示錯誤。

判斷是否發生錯誤

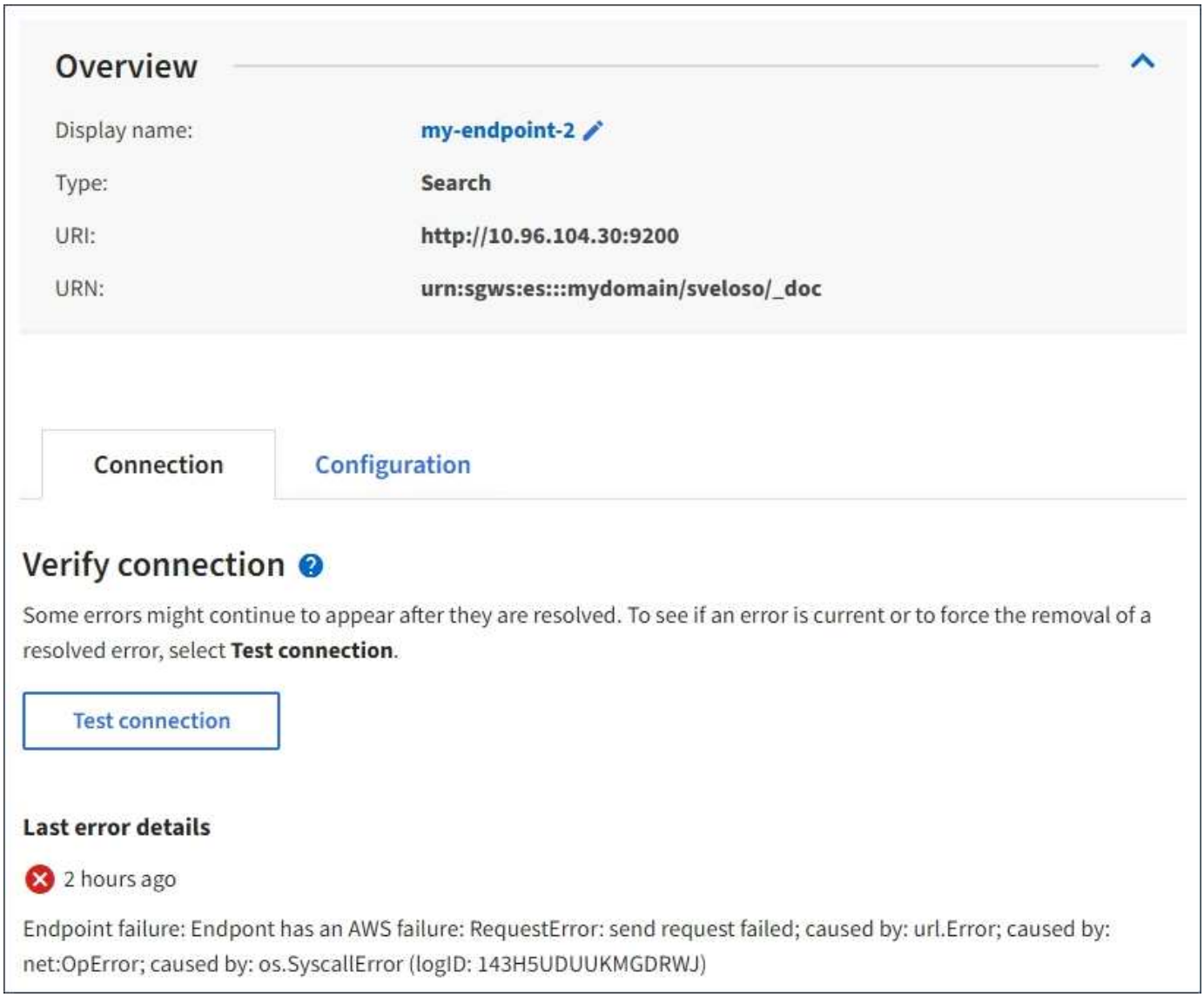
如果過去 7 天內發生任何平台服務端點錯誤、租戶管理器儀表板會顯示警示訊息。您可以移至「平台服務端點」頁面、查看錯誤的詳細資料。



儀表板上出現的相同錯誤也會出現在「平台服務端點」頁面頂端。若要檢視更詳細的錯誤訊息：

步驟

1. 從端點清單中、選取有錯誤的端點。
2. 在端點詳細資料頁面上、選取*連線*。此索引標籤只會顯示端點最近發生的錯誤、並指出錯誤發生的時間已過多久。包含紅色X圖示的錯誤 過去7天內發生。



檢查錯誤是否仍為最新狀態

有些錯誤可能會繼續顯示在「最後一個錯誤」欄中、即使這些錯誤已解決。若要查看錯誤是否為目前錯誤、或強制從表格中移除已解決的錯誤：

步驟

1. 選取端點。

   端點詳細資料頁面隨即出現。

2. 選擇*連線*>*測試連線*。

選擇*測試連線*會使StorageGRID Sexing驗證平台服務端點是否存在、以及是否能以目前的認證資料來連線。端點的連線會從每個站台的一個節點驗證。

解決端點錯誤

您可以使用端點詳細資料頁面上的*上次錯誤*訊息來協助判斷造成錯誤的原因。有些錯誤可能需要您編輯端點才能解決問題。例如StorageGRID 、如果由於沒有正確的存取權限或存取金鑰已過期、所以無法存取目的地S3儲

存區、就會發生CloudMirroring錯誤。訊息為「端點認證或目的地存取需要更新」、詳細資料為「'AccessDenied」或「'InvalidAccessKeyId'」。

如果您需要編輯端點來解決錯誤、請選取*測試並儲存變更*、以StorageGRID 驗證更新的端點、並確認可以使用目前的認證來達到該端點。端點的連線會從每個站台的一個節點驗證。

步驟

1. 選取端點。
2. 在端點詳細資料頁面上、選取*組態*。
3. 視需要編輯端點組態。
4. 選擇*連線*>*測試連線*。

權限不足的端點認證

當驗證平台服務端點時、會確認端點的認證資料可用於聯絡目的地資源、並執行基本權限檢查。StorageGRID不過StorageGRID 、不驗證特定平台服務作業所需的所有權限。因此、如果您在嘗試使用平台服務時收到錯誤訊息（例如「"4003 Forbidbididbididbide"）、請檢查與端點認證相關的權限。

相關資訊

- 管理 **StorageGRID** › 疑難排解平台服務
- "建立平台服務端點"
- "測試平台服務端點的連線"
- "編輯平台服務端點"

設定**CloudMirror**複寫

。 "CloudMirror複寫服務" 是StorageGRID 三種支援的平台服務之一。您可以使用CloudMirror複寫、將物件自動複寫到外部S3儲存區。

開始之前

- StorageGRID 管理員已為您的租戶帳戶啟用平台服務。
- 您已建立一個儲存區作為複寫來源。
- 您打算用作 CloudMirror 複寫目的地的端點已經存在、而且您有它的 URN 。
- 您屬於具有的使用者群組 "管理所有貯體或根目錄存取權限"。這些權限會在使用租戶管理程式設定儲存區時、覆寫群組或儲存區原則中的權限設定。

關於這項工作

CloudMirror複寫會將物件從來源儲存區複製到端點中指定的目的地儲存區。

CloudMirror 複寫與跨網格複寫功能有重要的相似之處和差異。若要深入瞭解、請參閱 "比較跨網格複寫和 CloudMirror 複寫"。

若要為儲存區啟用CloudMirror複寫、您必須建立並套用有效的儲存區複寫組態XML。複寫組態XML必須針對每個目的地使用S3儲存區端點的URN。

啟用S3物件鎖定的來源或目的地桶不支援複寫。

如需有關貯體複寫及如何設定的一般資訊、請參閱 "Amazon Simple Storage Service （ S3 ）文件：複寫物件"。如需 StorageGRID 如何實作 GetBucketReplication 、 DeleteBucketReplication 和 PuttBucketReplication 的相關資訊、請參閱 "在貯體上作業"。

如果您在包含物件的貯體上啟用 CloudMirror 複寫、則會複寫新增至該貯體的物件、但不會複寫該貯體中的現有物件。您必須更新現有物件、才能觸發複寫。

如果您在複寫組態XML中指定儲存類別、StorageGRID 則當針對目的地S3端點執行作業時、會使用該類別。目的地端點也必須支援指定的儲存類別。請務必遵循目的地系統廠商所提供的任何建議。

步驟

1. 啟用來源儲存區的複寫：

   使用文字編輯器建立所需的複寫組態XML、以啟用S3複寫API中指定的複寫。設定XML時：

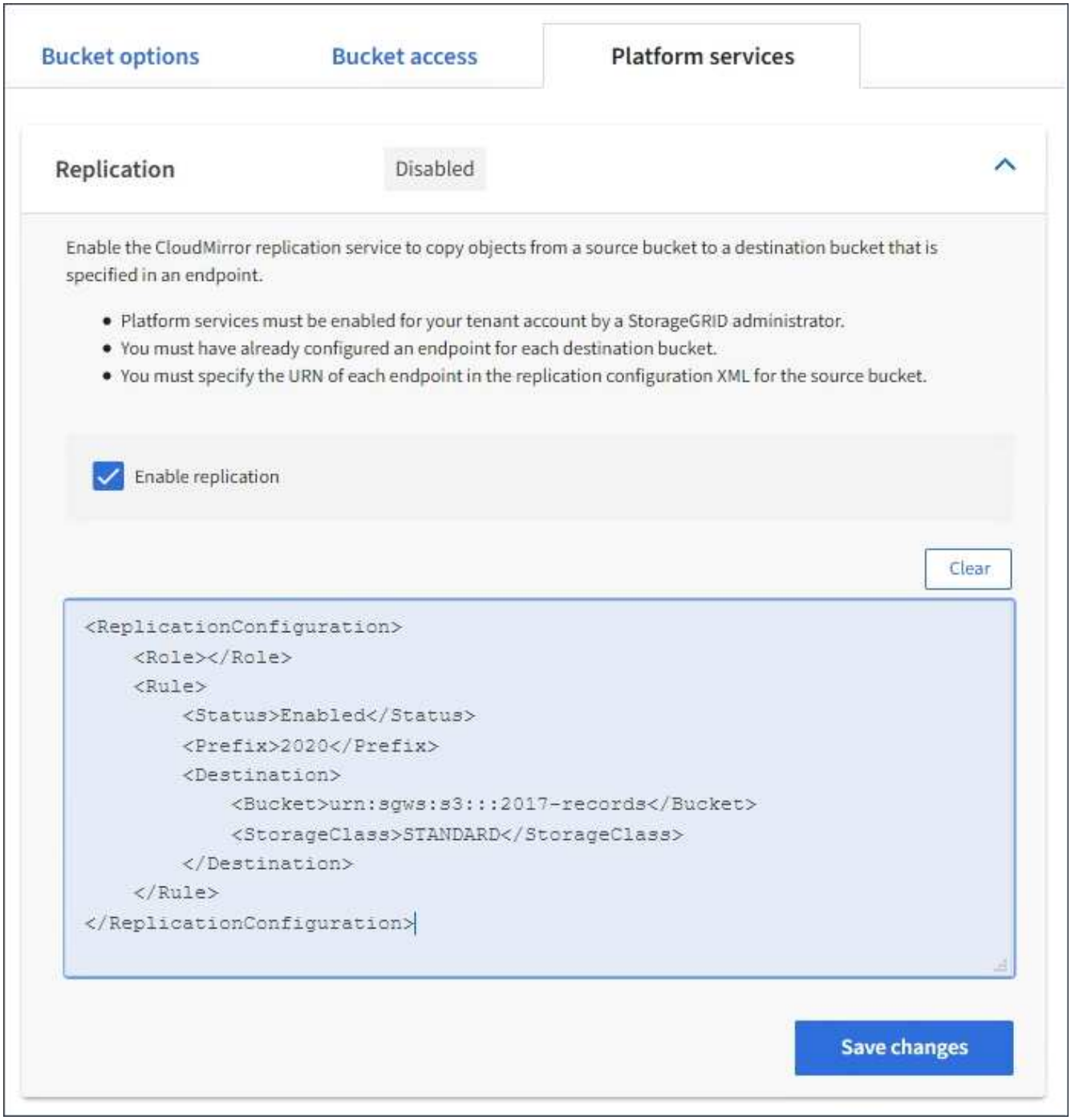
   - 請注意StorageGRID 、僅支援V1複寫組態。這表示StorageGRID 、不支援使用 `Filter` 規則元素、並遵循刪除物件版本的V1慣例。如需詳細資訊、請參閱Amazon複寫組態文件。
   - 使用S3貯體端點的URN作為目的地。
   - 選擇性地新增 `<StorageClass>` 元素、並指定下列其中一項：
     - `STANDARD`：預設儲存類別。如果您在上傳物件時未指定儲存類別、請使用 `STANDARD` 已使用儲存類別。
     - `STANDARD_IA`：（標準-非常用存取）此儲存類別適用於存取頻率較低、但仍需在需要時快速存取的資料。
     - `REDUCED_REDUNDANCY`：此儲存類別適用於非關鍵且可重複產生的資料、其備援能力可低於 `STANDARD` 儲存類別：
   - 如果您指定 `Role` 在組態XML中、將會忽略此項目。此值不供StorageGRID 下列項目使用：

```
<ReplicationConfiguration>
    <Role></Role>
    <Rule>
        <Status>Enabled</Status>
        <Prefix>2020</Prefix>
        <Destination>
           <Bucket>urn:sgws:s3:::2017-records</Bucket>
           <StorageClass>STANDARD</StorageClass>
         </Destination>
     </Rule>
</ReplicationConfiguration>
```

2. 從儀表板選取 * 檢視貯體 * 、或選取 * 儲存空間（ S3 ） * > * 鏟斗 * 。
3. 選取來源儲存區的名稱。

   此時會顯示「庫位詳細資料」頁面。

4. 選擇*平台服務*>*複寫*。
5. 選中 * 啓用複製 * 複選框。
6. 將複寫組態XML貼到文字方塊中、然後選取*儲存變更*。



每個租戶帳戶都必須由StorageGRID 使用Grid Manager或Grid Management API的管理員啟用平台服務。如果您儲存組態XML時發生錯誤、請聯絡StorageGRID 您的管理員。

7. 確認複寫設定正確：
   a. 將符合複寫組態中所指定之複寫需求的物件新增至來源儲存區。

在前面所示的範例中、會複寫與前置詞「'2020」相符的物件。

b. 確認物件已複寫至目的地儲存區。

對於小型物件、複寫作業很快就會完成。

相關資訊

"建立平台服務端點"

設定事件通知

通知服務是StorageGRID 三種支援的平台服務之一。您可以啟用儲存區通知、將指定事件的相關資訊傳送至支援AWS Simple Notification Service™（SNS）的目的地服務。

開始之前

- StorageGRID 管理員已為您的租戶帳戶啟用平台服務。
- 您已建立一個儲存庫做為通知來源。
- 您打算用作事件通知目的地的端點已經存在、而且您擁有它的 URN 。
- 您屬於具有的使用者群組 "管理所有貯體或根目錄存取權限"。這些權限會在使用租戶管理程式設定儲存區時、覆寫群組或儲存區原則中的權限設定。

關於這項工作

設定事件通知之後、每當來源儲存區中的物件發生指定事件時、就會產生通知、並傳送至作為目的地端點的Simple Notification Service（SNS）主題。若要啟用儲存區通知、您必須建立並套用有效的通知組態XML。通知組態XML必須針對每個目的地使用事件通知端點的URN。

如需事件通知及如何設定的一般資訊、請參閱 Amazon 文件。如需 StorageGRID 如何實作 S3 儲存區通知組態 API 的相關資訊、請參閱實作 S3 用戶端應用程式的指示。

如果您為包含物件的儲存區啟用事件通知、則通知僅會針對儲存通知組態後所執行的動作傳送。

步驟

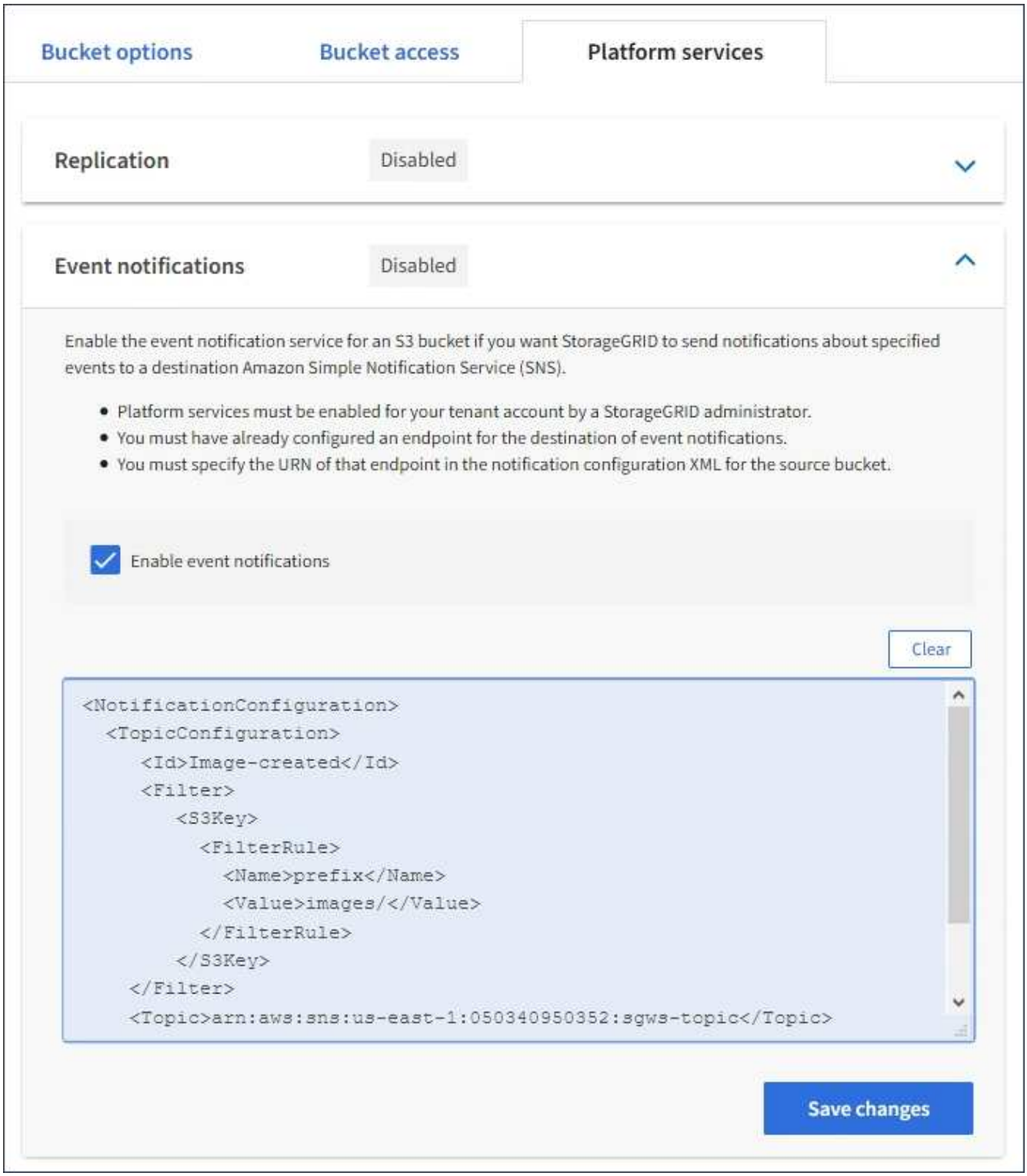
1. 啟用來源儲存區的通知：
   - 使用文字編輯器建立啟用事件通知所需的通知組態XML、如S3通知API所指定。
   - 設定XML時、請使用事件通知端點的URN作為目的地主題。

```
<NotificationConfiguration>
  <TopicConfiguration>
     <Id>Image-created</Id>
     <Filter>
        <S3Key>
          <FilterRule>
            <Name>prefix</Name>
            <Value>images/</Value>
          </FilterRule>
        </S3Key>
    </Filter>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
    <Event>s3:ObjectCreated:*</Event>
   </TopicConfiguration>
 </NotificationConfiguration>
```

2. 在租戶管理程式中、選取*儲存設備（S3）>*桶。
3. 選取來源儲存區的名稱。

   此時會顯示「庫位詳細資料」頁面。

4. 選擇*平台服務*>*事件通知*。
5. 選中 * 啓用事件通知 * 複選框。
6. 將通知組態XML貼到文字方塊中、然後選取*儲存變更*。



每個租戶帳戶都必須由StorageGRID 使用Grid Manager或Grid Management API的管理員啟用平台服務。如果您儲存組態XML時發生錯誤、請聯絡StorageGRID 您的管理員。

7. 確認事件通知設定正確：

   a. 對來源儲存區中符合觸發通知要求的物件執行動作、如組態XML中所設定。

      在範例中、每當使用建立物件時、就會傳送事件通知 `images/` 前置碼：

b. 確認已將通知傳送至目的地SNS主題。

例如、如果您的目的地主題是裝載在AWS Simple Notification Service（SNS）上、您可以設定服務在通知送達時傳送電子郵件給您。

```
{
   "Records":[
      {
         "eventVersion":"2.0",
         "eventSource":"sgws:s3",
         "eventTime":"2017-08-08T23:52:38Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"11111111111111111"
         },
         "requestParameters":{
            "sourceIPAddress":"193.51.100.20"
         },
         "responseElements":{
            "x-amz-request-id":"122047343"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"Image-created",
            "bucket":{
               "name":"test1",
               "ownerIdentity":{
                  "principalId":"11111111111111111"
               },
               "arn":"arn:sgws:s3:::test1"
            },
            "object":{
               "key":"images/cat.jpg",
               "size":0,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
               "sequencer":"14D90402421461C7"
            }
         }
      }
   ]
}
```

如果在目的地主題收到通知、表示您已成功設定來源庫位以供StorageGRID 發出資訊通知。

相關資訊

"瞭解庫存箱通知"

"使用S3 REST API"

"建立平台服務端點"

使用搜尋整合服務

搜尋整合服務是StorageGRID 三項功能完善的平台服務之一。您可以啟用此服務、在物件建立、刪除或更新中繼資料或標記時、將物件中繼資料傳送至目的地搜尋索引。

您可以使用租戶管理程式來設定搜尋整合功能、將自訂StorageGRID 的靜態組態XML套用至儲存庫。

> 由於搜尋整合服務會將物件中繼資料傳送至目的地、因此其組態XML稱為中繼資料通知組態XML。此組態XML不同於用來啟用事件通知的_notification組態XML。

請參閱 "實作S3用戶端應用程式的指示" 如需下列自訂StorageGRID 的Sfor Rest API作業的詳細資料：

- 刪除時段中繼資料通知組態
- 取得Bucket中繼資料通知組態
- 放置時段中繼資料通知組態

相關資訊

"搜尋整合的組態XML"

"中繼資料通知中包含的物件中繼資料"

"由搜尋整合服務產生的JSON"

"設定搜尋整合服務"

"使用S3 REST API"

搜尋整合的組態**XML**

搜尋整合服務是使用中包含的一組規則來設定 `<MetadataNotificationConfiguration>` 和 `</MetadataNotificationConfiguration>` 標記。每個規則都會指定規則適用的物件、StorageGRID 以及應將這些物件中繼資料傳送到哪個目的地。

物件可依物件名稱的前置詞進行篩選。例如、您可以傳送具有前置碼之物件的中繼資料 `images` 至一個目的地、以及具有前置碼之物件的中繼資料 `videos` 到另一個。有重疊前置字元的組態無效、提交時會遭到拒絕。例如、含有一個前置字元物件規則的組態 `test` 和第二個規則、用於具有前置碼的物件 `test2` 不允許。

目的地必須使用StorageGRID 已為搜尋整合服務建立的一個端點的URN來指定。這些端點是指在ElasticSearch叢集上定義的索引和類型。

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

下表說明中繼資料通知組態XML中的元素。

名稱	說明	必要
Metadata NotifyationConfiguration	用於指定中繼資料通知物件和目的地之規則的容器標籤。 包含一或多個規則元素。	是的
規則	規則的容器標記、用於識別應將中繼資料新增至指定索引的物件。 會拒絕具有重疊前置碼的規則。 包括在Metadata NotifyationConfiguration元素中。	是的
ID	規則的唯一識別碼。 包含在Rule元素中。	否
狀態	狀態可以是「已啟用」或「已停用」。不針對停用的規則採取任何行動。 包含在Rule元素中。	是的

名稱	說明	必要
前置碼	符合前置碼的物件會受到規則影響、其中繼資料會傳送到指定的目的地。 若要符合所有物件、請指定一個空白首碼。 包含在Rule元素中。	是的
目的地	規則目的地的容器標記。 包含在Rule元素中。	是的
urn	傳送物件中繼資料的目的地之一。必須是StorageGRID 具有下列屬性的不景端點的URN： • `es` 必須是第三個元素。 • URN必須以索引結尾、並在表單中輸入中繼資料的儲存位置 `domain-name/myindex/mytype`。 端點是使用租戶管理程式或租戶管理API來設定。它們採用下列形式： • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` 端點必須在提交組態XML之前進行設定、否則組態將會失敗並顯示404錯誤。 目標元素中包含urn.	是的

使用範例中繼資料通知組態XML來瞭解如何建構您自己的XML。

適用於所有物件的中繼資料通知組態

在此範例中、所有物件的物件中繼資料都會傳送到相同的目的地。

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:myes:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

中繼資料通知組態有兩條規則

在此範例中、物件的中繼資料會與前置詞相符 `/images` 會傳送至一個目的地、而物件中繼資料則會與前置詞相符 `/videos` 傳送至第二個目的地。

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

相關資訊

"使用S3 REST API"

"中繼資料通知中包含的物件中繼資料"

"由搜尋整合服務產生的JSON"

"設定搜尋整合服務"

每當建立、刪除物件、或更新其中繼資料或標記時、搜尋整合服務會將物件中繼資料傳送至目的地搜尋索引。

開始之前

- StorageGRID 管理員已為您的租戶帳戶啟用平台服務。
- 您已經建立了要索引其內容的 S3 儲存貯體。
- 您打算用作搜尋整合服務目的地的端點已經存在、而且您有其 URN 。
- 您屬於具有的使用者群組 "管理所有貯體或根目錄存取權限"。這些權限會在使用租戶管理程式設定儲存區時、覆寫群組或儲存區原則中的權限設定。

關於這項工作

在您設定來源儲存區的搜尋整合服務之後、建立物件或更新物件的中繼資料或標記、會觸發物件中繼資料傳送到目的地端點。如果您為已包含物件的貯體啟用搜尋整合服務、則不會自動傳送現有物件的中繼資料通知。您必須更新這些現有物件、以確保其中繼資料已新增至目的地搜尋索引。

步驟

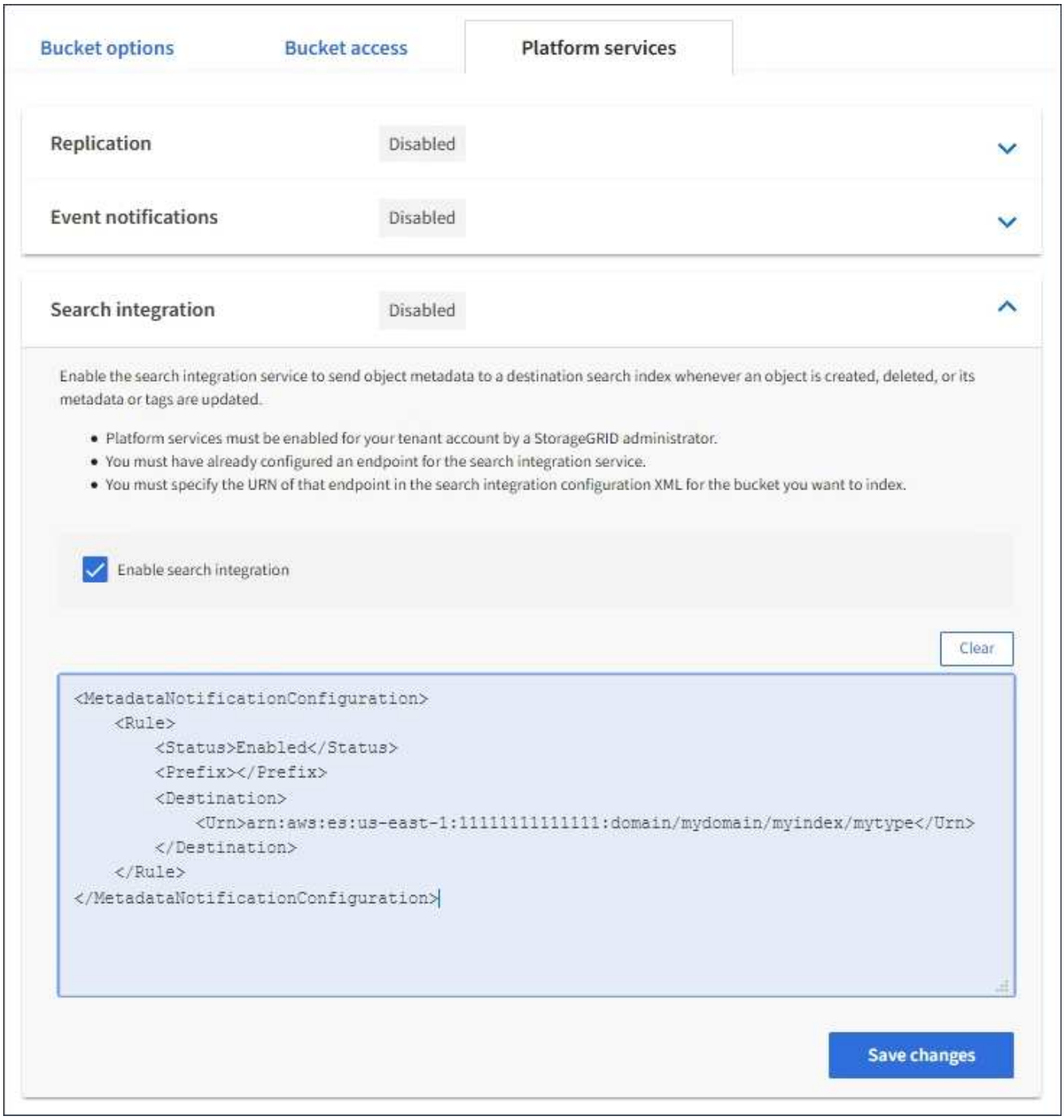
1. 使用文字編輯器建立啟用搜尋整合所需的中繼資料通知XML。
   - 請參閱組態XML的相關資訊以進行搜尋整合。
   - 設定XML時、請使用搜尋整合端點的URN作為目的地。

```
<MetadataNotificationConfiguration>
 <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
       <Urn>arn:aws:es:us-east-
1:11111111111111:domain/mydomain/myindex/mytype</Urn>
       </Destination>
 </Rule>
</MetadataNotificationConfiguration>
```

2. 在租戶管理程式中、選取*儲存設備（S3）>*桶。
3. 選取來源儲存區的名稱。

   此時會顯示「庫位詳細資料」頁面。

4. 選擇*平台服務*>*搜尋整合*
5. 選中 * 啓用搜索集成 * 複選框。
6. 將中繼資料通知組態貼到文字方塊中、然後選取*儲存變更*。



每個租戶帳戶都必須由StorageGRID 使用Grid Manager或Management API的管理員為其啟用平台服務。如果您儲存組態XML時發生錯誤、請聯絡StorageGRID 您的管理員。

7. 確認搜尋整合服務的設定正確：
   a. 將符合觸發組態XML中指定中繼資料通知要求的物件新增至來源儲存區。

      在先前所示的範例中、新增至儲存區的所有物件都會觸發中繼資料通知。

   b. 確認包含物件中繼資料和標記的Json文件已新增至端點中指定的搜尋索引。

完成後

如有必要、您可以使用下列任一方法來停用儲存區的搜尋整合：

- 選取 * 儲存（ S3 ） * > * 儲存容量 * 、然後清除 * 啟用搜尋整合 * 核取方塊。
- 如果您直接使用S3 API、請使用刪除時段中繼資料通知要求。請參閱實作S3用戶端應用程式的指示。

相關資訊

"瞭解搜尋整合服務"

"搜尋整合的組態XML"

"使用S3 REST API"

"建立平台服務端點"

由搜尋整合服務產生的**JSON**

當您啟用儲存區的搜尋整合服務時、每次新增、更新或刪除物件中繼資料或標記時、都會產生Json文件並傳送至目的地端點。

此範例顯示Json範例、該範例可在具有金鑰的物件產生時產生 `SGWS/Tagging.txt` 在名為的儲存區中建立 `test`。。 `test` 儲存區沒有版本、因此 `versionId` 標記為空白。

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1"
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

中繼資料通知中包含的物件中繼資料

此表格列出JSON文件中所有欄位、這些欄位會在啟用搜尋整合時傳送至目的地端點。

文件名稱包含儲存區名稱、物件名稱及版本ID（若有）。

類型	項目名稱與說明
儲存區和物件資訊	`bucket`：桶的名稱

類型	項目名稱與說明
`key`：物件金鑰名稱	`versionID`：對象版本，用於版本控制桶中的對象
`region`例如：`Bucket`區域 `us-east-1`	系統中繼資料
`size`：HTTP用戶端可見的物件大小（以位元組為單位）	`md5`：物件雜湊
使用者中繼資料	`metadata`：對象的所有用戶元數據（作爲鍵值對） `key:value`
標記	`tags`：所有為物件定義的物件標記、做為金鑰值配對 `key:value`

針對標記和使用者中繼資料StorageGRID 、將日期和數字以字串或S3事件通知的形式傳送至Elasticsearch。若要設定Elasticsearch將這些字串解譯為日期或數字、請遵循Elasticsearch指示進行動態欄位對應、以及對應日期格式。您必須先在索引上啟用動態欄位對應、才能設定搜尋整合服務。建立文件索引後、您就無法編輯索引中文件的欄位類型。

使用S3 REST API

S3 REST API 支援的版本與更新

支援簡單儲存服務（S3）API、此API是以代表狀態傳輸（REST）網路服務的形式實作。StorageGRID

S3 REST API 的支援可讓您將專為 S3 Web 服務開發的服務導向應用程式、與使用 StorageGRID 系統的內部部署物件儲存設備連線。用戶端應用程式目前使用 S3 REST API 呼叫的變更最少。

支援的版本

支援下列S3和HTTP的特定版本。StorageGRID

項目	版本
S3規格	*Simple Storage Service API*參考資料 2006年3月1日

項目	版本
HTTP	1.1 如需HTTP的詳細資訊、請參閱HTTP / 1.1（RFC 7230-35）。 附註 StorageGRID ：不支援HTTP / 1.1鋪管。

相關資訊

"IETF RFC 2616：超文字傳輸傳輸協定（HTTP / 1.1）"

"Amazon Web Services（AWS）文件：Amazon Simple Storage Service API Reference"

S3 REST API 支援的更新

版本	註解
11.7	• 新增 "快速參考：支援的 S3 API 要求"。 • 新增對使用 S3 物件鎖定的治理模式的支援。 • 新增支援 StorageGRID 專屬 `x-ntap-sg-cgr-replication-status` GET 物件和 HEAD 物件要求的回應標頭。此標頭提供物件的跨網格複寫狀態。 • SelectObjectContent 要求現在支援 Parquet 物件。
11.6%	• 新增使用的支援 `partNumber` 取得物件和標頭物件要求中的要求參數。 • 新增S3物件鎖定的預設保留模式支援、以及儲存區層級的預設保留期間。 • 新增對的支援 `s3:object-lock-remaining-retention-days` 原則條件金鑰、可設定物件的允許保留期間範圍。 • 將單一「放置物件」作業的最大大小 _ 建議 _ 變更為 5 GiB （ 5 、 368,709,120 位元組）。如果您的物件大於5 GiB、請改用多部份上傳。
11.5	• 新增對管理儲存區加密的支援。 • 新增了對S3物件鎖定和過時舊版規範要求的支援。 • 新增使用刪除版本型儲存區上的多個物件的支援。 • 。 `Content-MD5` 現在已正確支援要求標頭。

版本	註解
11.4	• 新增刪除庫位標記、取得庫位標記及置入庫位標記的支援。不支援成本分攤標記。 • 對於StorageGRID 在VMware 11.4中建立的儲存區、不再需要限制物件金鑰名稱以符合效能最佳實務做法。 • 新增了對上的儲存區通知的支援 `s3:ObjectRestore:Post` 事件類型。 • 現在已強制多部分零件的AWS大小限制。多部分上傳中的每個部分必須介於5個mib和5 GiB之間。最後一個部分可能小於5個mib。 • 新增 TLS 1.3 支援
11.3	• 新增支援使用客戶提供的金鑰（SSE-C）進行物件資料的伺服器端加密。 • 新增刪除、取得及置放資源庫生命週期作業（僅限到期行動）和的支援 `x-amz-expiration` 回應標頭： • 更新的「放置物件」、「放置物件」-「複製」和「多重成分上傳」、說明ILM規則在擷取時使用同步放置的影響。 • 不再支援TLS 1.1密碼。
11.2	新增後物件還原支援、可搭配雲端儲存資源池使用。新增了使用AWS語法的支援、可用於ARN、原則條件金鑰、以及群組和儲存區原則中的原則變數。我們StorageGRID 將繼續支援使用此功能的現有群組和儲存區原則。 *附註：*在其他組態JSON/XML中使用ARN/URN StorageGRID （包括用於自訂的版本功能）並未變更。
11.1.	新增支援跨來源資源共享（ CORS ）、 HTTP for S3 用戶端連線至網格節點、以及儲存區的法規遵循設定。
11.0	新增支援、可設定適用於儲存區的平台服務（CloudMirror複寫、通知及Elasticsearch整合）。此外、也新增了對儲存區物件標記位置限制的支援、以及可用的一致性控制設定。
10.4	新增對ILM掃描版本設定、端點網域名稱頁面更新、原則、原則範例及PuttoverwriteObject權限中的條件和變數的支援。
10.3.1	新增版本管理支援。
10.2	新增對群組和庫位存取原則的支援、以及多部份複本（上傳零件-複本）的支援。
10.1	新增多部分上傳、虛擬託管樣式要求及v4驗證的支援。
10.0%	由整個系統初始支援S3 REST API StorageGRID 。目前支援的_Simple Storage Service API Reference版本為2009-03-01。

快速參考：支援的 **S3 API** 要求

本頁概述 StorageGRID 如何支援 Amazon Simple Storage Service （ S3 ） API 。

本頁僅包含 StorageGRID 支援的 S3 作業。

若要查看每項作業的 AWS 文件、請選取標題中的連結。

通用 **URI** 查詢參數和要求標頭

除非另有說明、否則支援下列常見的 URI 查詢參數：

- `versionId` （視物件作業需求而定）

除非另有說明、否則支援下列常見的要求標頭：

- `Authorization`
- `Connection`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Date`
- `Expect`
- `Host`
- `x-amz-date`

相關資訊

- "S3 REST API 實作詳細資料"
- "Amazon Simple Storage Service API 參考：一般要求標頭"

"AbortMultiPart上 傳"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求、加上此額外的 URI 查詢參數：

- `uploadId`

申請本文

無

本文檔**StorageGRID**

"多部份上傳作業"

"完成多個部分上傳"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求、加上此額外的 URI 查詢參數：

- `uploadId`

要求內文 **XML** 標記

StorageGRID 支援這些要求本文 XML 標記：

- `CompleteMultipartUpload`
- `Part`
- `ETag`
- `PartNumber`

本文檔**StorageGRID**

"完成多部份上傳"

"CopyObject"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求、加上下列額外標頭：

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-modified-since`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-server-side-encryption-customer-algorithm`
- `x-amz-copy-source-server-side-encryption-customer-key`
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`
- `x-amz-metadata-directive`
- `x-amz-object-lock-legal-hold`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-server-side-encryption`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-storage-class`

- `x-amz-tagging`
- `x-amz-tagging-directive`
- `x-amz-meta-<metadata-name>`

申請本文

無

本文檔**StorageGRID**

"放置物件複本"

"建立庫位"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求、加上下列額外標頭：

- `x-amz-bucket-object-lock-enabled`

申請本文

StorageGRID 支援 Amazon S3 REST API 在實作時所定義的所有要求主體參數。

本文檔**StorageGRID**

"在貯體上作業"

"建立多個部分上傳"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求、加上下列額外標頭：

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-server-side-encryption`
- `x-amz-storage-class`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-tagging`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`

- `x-amz-meta-<metadata-name>`

申請本文

無

本文檔**StorageGRID**

"啟動多部份上傳"

"刪除**Bucket**"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求。

本文檔**StorageGRID**

"在貯體上作業"

"刪除 **BucketCors**"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求。

申請本文

無

本文檔**StorageGRID**

"在貯體上作業"

"刪除 **BucketEncryption**"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求。

申請本文

無

本文檔**StorageGRID**

"在貯體上作業"

"刪除 **BucketLifecycle**"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求。

申請本文

無

本文檔**StorageGRID**

- "在貯體上作業"

- "建立S3生命週期組態"

"刪除BucketPolicy"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求。

申請本文

無

本文檔**StorageGRID**

"在貯體上作業"

"刪除 BucketReplication"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求。

申請本文

無

本文檔**StorageGRID**

"在貯體上作業"

"刪除 Bucketagging"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求。

申請本文

無

本文檔**StorageGRID**

"在貯體上作業"

"刪除物件"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求、加上此額外的要求標頭：

- `x-amz-bypass-governance-retention`

申請本文

無

本文檔**StorageGRID**

"物件上的作業"

"刪除物件"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求、加上此額外的要求標頭：

- `x-amz-bypass-governance-retention`

申請本文

StorageGRID 支援 Amazon S3 REST API 在實作時所定義的所有要求主體參數。

本文檔**StorageGRID**

"物件上的作業" （刪除多個物件）

"刪除ObjectTagging"

StorageGRID 支援所有功能 通用參數和標頭 針對此要求。

申請本文

無

本文檔**StorageGRID**

"物件上的作業"

"GetBucketAcl"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求。

申請本文

無

本文檔**StorageGRID**

"在貯體上作業"

"GetBucketCors"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求。

申請本文

無

本文檔**StorageGRID**

"在貯體上作業"

"GetBucketEncryption"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求。

申請本文

無

本文檔**StorageGRID**

"在貯體上作業"

"GetBucketLifecycleConfiguration"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求。

申請本文

無

本文檔**StorageGRID**

- "在貯體上作業" （ Get Bucket 生命週期）
- "建立S3生命週期組態"

"GetBucketLocation"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求。

申請本文

無

本文檔**StorageGRID**

"在貯體上作業"

"GetBucketNotificationConfiguration"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求。

申請本文

無

本文檔**StorageGRID**

"在貯體上作業" （取得庫存箱通知）

"GetBucketPolicy"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求。

申請本文

無

本文檔**StorageGRID**

"在貯體上作業"

"GetBucketReplication"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求。

申請本文

無

本文檔**StorageGRID**

"在貯體上作業"

"GetBucketTagging"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求。

申請本文

無

本文檔**StorageGRID**

"在貯體上作業"

"GetBucketVersion"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求。

申請本文

無

本文檔**StorageGRID**

"在貯體上作業"

"GetObject"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求、加上下列其他 URI 查詢參數：

- `partNumber`
- `response-cache-control`
- `response-content-disposition`
- `response-content-encoding`
- `response-content-language`

- response-content-type
- response-expires

以及這些額外的要求標頭：

- Range
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- If-Match
- If-Modified-Since
- If-None-Match
- If-Unmodified-Since

申請本文

無

本文檔**StorageGRID**

"取得物件"

"GetObjectAcl"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求。

申請本文

無

本文檔**StorageGRID**

"物件上的作業"

"GetObjectLegalHold"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求。

申請本文

無

本文檔**StorageGRID**

"使用 S3 REST API 來設定 S3 物件鎖定"

"GetObjectLockConfiguration"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求。

申請本文

無

本文檔**StorageGRID**

"使用 S3 REST API 來設定 S3 物件鎖定"

"GetObjectRetention"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求。

申請本文

無

本文檔**StorageGRID**

"使用 S3 REST API 來設定 S3 物件鎖定"

"GetObjectTagging"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求。

申請本文

無

本文檔**StorageGRID**

"物件上的作業"

"標題庫"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求。

申請本文

無

本文檔**StorageGRID**

"在貯體上作業"

"標題物件"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求、加上下列額外標頭：

- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`
- `Range`

申請本文

無

本文檔**StorageGRID**

"標頭物件"

"列表桶"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求。

申請本文

無

本文檔**StorageGRID**

"服務的作業 gt; 取得服務"

"ListMultipartUploads"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求、加上下列額外參數：

- `delimiter`
- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`

申請本文

無

本文檔**StorageGRID**

"列出多個部分上傳"

"清單物件"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求、加上下列額外參數：

- `delimiter`
- `encoding-type`
- `marker`
- `max-keys`
- `prefix`

申請本文

無

本文檔**StorageGRID**

"在貯體上作業" （ Get Bucket ）

"清單對象V2."

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求、加上下列額外參數：

- `continuation-token`
- `delimiter`
- `encoding-type`
- `fetch-owner`
- `max-keys`
- `prefix`
- `start-after`

申請本文

無

本文檔**StorageGRID**

"在貯體上作業" （ Get Bucket ）

"ListObjectVerions"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求、加上下列額外參數：

- `delimiter`
- `encoding-type`

- `key-marker`
- `max-keys`
- `prefix`
- `version-id-marker`

申請本文

無

本文檔**StorageGRID**

"在貯體上作業" （ Get Bucket 物件版本）

"清單零件"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求、加上下列額外參數：

- `max-parts`
- `part-number-marker`
- `uploadId`

申請本文

無

本文檔**StorageGRID**

"列出多個部分上傳"

"PuttBucketCors"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求。

申請本文

StorageGRID 支援 Amazon S3 REST API 在實作時所定義的所有要求主體參數。

本文檔**StorageGRID**

"在貯體上作業"

"PuttBucketEncryption"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求。

要求內文 **XML** 標記

StorageGRID 支援這些要求本文 XML 標記：

- `ServerSideEncryptionConfiguration`

- `Rule`
- `ApplyServerSideEncryptionByDefault`
- `SSEAlgorithm`

本文檔**StorageGRID**

"在貯體上作業"

"PuttBucketLifecycleConfiguration"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求。

要求內文 **XML** 標記

StorageGRID 支援這些要求本文 XML 標記：

- `NewerNoncurrentVersions`
- `LifecycleConfiguration`
- `Rule`
- `Expiration`
- `Days`
- `Filter`
- `And`
- `Prefix`
- `Tag`
- `Key`
- `Value`
- `Prefix`
- `Tag`
- `Key`
- `Value`
- `ID`
- `NoncurrentVersionExpiration`
- `NoncurrentDays`
- `Prefix`
- `Status`

本文檔**StorageGRID**

- "在貯體上作業" （ Put Bucket 生命週期）

- "建立S3生命週期組態"

"PutBucketNotificationConfiguration"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求。

要求內文 **XML** 標記

StorageGRID 支援這些要求本文 XML 標記：

- `Prefix`
- `Suffix`
- `NotificationConfiguration`
- `TopicConfiguration`
- `Event`
- `Filter`
- `S3Key`
- `FilterRule`
- `Name`
- `Value`
- `Id`
- `Topic`

本文檔**StorageGRID**

"在貯體上作業" （ Put Bucket 通知）

"PuttBucketPolicy"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求。

申請本文

如需受支援 JSON 本文欄位的詳細資訊、請參閱"使用貯體和群組存取原則"。

"PutBucketReplication"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求。

要求內文 **XML** 標記

- `ReplicationConfiguration`
- `Status`
- `Prefix`

- `Destination`
- `Bucket`
- `StorageClass`
- `Rule`

本文檔**StorageGRID**

"在貯體上作業"

"PuttBucketTagging"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求。

申請本文

StorageGRID 支援 Amazon S3 REST API 在實作時所定義的所有要求主體參數。

本文檔**StorageGRID**

"在貯體上作業"

"PuttBucketVersion"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求。

要求主體參數

StorageGRID 支援下列要求主體參數：

- `VersioningConfiguration`
- `Status`

本文檔**StorageGRID**

"在貯體上作業"

"PuttObject"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求、加上下列額外標頭：

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `x-amz-server-side-encryption`
- `x-amz-storage-class`

- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-tagging`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`
- `x-amz-meta-<metadata-name>`

申請本文

- 物件的二進位資料

本文檔**StorageGRID**

"放置物件"

"PutObjectLegalHold"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求。

申請本文

StorageGRID 支援 Amazon S3 REST API 在實作時所定義的所有要求主體參數。

本文檔**StorageGRID**

"使用 S3 REST API 來設定 S3 物件鎖定"

"PutObjectLockConfiguration"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求。

申請本文

StorageGRID 支援 Amazon S3 REST API 在實作時所定義的所有要求主體參數。

本文檔**StorageGRID**

"使用 S3 REST API 來設定 S3 物件鎖定"

"PutObjectRetention"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求、加上此額外標頭：

- `x-amz-bypass-governance-retention`

申請本文

StorageGRID 支援 Amazon S3 REST API 在實作時所定義的所有要求主體參數。

本文檔**StorageGRID**

"使用 S3 REST API 來設定 S3 物件鎖定"

"PuttObjectTagging"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求。

申請本文

StorageGRID 支援 Amazon S3 REST API 在實作時所定義的所有要求主體參數。

本文檔**StorageGRID**

"物件上的作業"

"選取物件內容"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求。

申請本文

如需受支援實體欄位的詳細資訊、請參閱下列內容：

- "使用S3 Select"
- "選取物件內容"

"上傳零件"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求、加上下列其他 URI 查詢參數：

- `partNumber`
- `uploadId`

以及這些額外的要求標頭：

- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`

申請本文

- 零件的二進位資料

本文檔**StorageGRID**

"上傳零件"

"上傳PartCopy"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 通用參數和標頭 針對此要求、加上下列其他 URI 查詢參數：

- partNumber
- uploadId

以及這些額外的要求標頭：

- x-amz-copy-source
- x-amz-copy-source-if-match
- x-amz-copy-source-if-modified-since
- x-amz-copy-source-if-none-match
- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-range
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-copy-source-server-side-encryption-customer-algorithm
- x-amz-copy-source-server-side-encryption-customer-key
- x-amz-copy-source-server-side-encryption-customer-key-MD5

申請本文

無

本文檔StorageGRID

"上傳零件-複製"

設定租戶帳戶和連線

若要設定StorageGRID 從用戶端應用程式接受連線、需要建立一或多個租戶帳戶並設定連線。

建立及設定S3租戶帳戶

S3 API用戶端必須先有S3租戶帳戶、才能將物件儲存及擷取StorageGRID 到支援區。每個租戶帳戶都有自己的帳戶 ID 、群組、使用者、貯體和物件。

S3租戶帳戶是StorageGRID 由使用Grid Manager或Grid Management API的資訊網管理員所建立。請參閱 "管理租戶" 以取得詳細資料。建立 S3 租戶帳戶後、租戶使用者即可存取租戶管理器、以管理群組、使用者、存取金鑰和貯體。請參閱 "使用租戶帳戶" 以取得詳細資料。

雖然 S3 租戶使用者可以使用 Tenant Manager 來建立和管理 S3 存取金鑰和貯體、但他們必須使用 S3 用戶端應用程式來擷取和管理物件。請參閱 "使用S3 REST API" 以取得詳細資料。

如何設定用戶端連線

網格管理員會做出組態選擇、影響S3用戶端連線StorageGRID 至以儲存及擷取資料的方式。將 StorageGRID 連線至任何 S3 應用程式有四個基本步驟：

- 根據用戶端應用程式與 StorageGRID 的連線方式、在 StorageGRID 中執行必要工作。
- 使用 StorageGRID 取得應用程式連線至網格所需的值。您也可以 "使用 S3 設定精靈" 或手動設定每個 StorageGRID 實體。
- 使用 S3 應用程式完成與 StorageGRID 的連線。建立 DNS 項目、將 IP 位址與您打算使用的任何網域名稱建立關聯。
- 在應用程式和 StorageGRID 中執行持續的工作、以隨時間而管理和監控物件儲存。

如需這些步驟的詳細資訊、請參閱 "設定用戶端連線"。

用戶端連線所需的資訊

若要儲存或擷取物件、 S3 用戶端應用程式會連線到負載平衡器服務（包含在所有管理節點和閘道節點上）、或是連接到所有儲存節點上的本機分配路由器（ LDR ）服務。

用戶端應用程式可以使用網格節點的 IP 位址和該節點上服務的連接埠號碼、來連線至 StorageGRID 。您也可以建立高可用度（ HA ）負載平衡節點群組、以提供使用虛擬 IP （ VIP ）位址的高可用度連線。如果您想要使用完整網域名稱（ FQDN ）而非 IP 或 VIP 位址連線至 StorageGRID 、您可以設定 DNS 項目。

請參閱 "摘要：用於用戶端連線的IP位址和連接埠" 以取得更多資訊。

決定使用**HTTPS**或**HTTP**連線

使用負載平衡器端點進行用戶端連線時、必須使用為該端點指定的傳輸協定（HTTP或HTTPS）來建立連線。若要將 HTTP 用於用戶端連線至儲存節點、您必須啟用 HTTP 。

根據預設、當用戶端應用程式連線至儲存節點時、它們必須使用加密的 HTTPS 進行所有連線。或者、您也可以在 Grid Manager 中選取 * 組態 * > * 安全性設定 * > * 網路和物件 * > * 啟用儲存節點連線的 HTTP * 、以啟用不安全的 HTTP 連線。例如、用戶端應用程式在非正式作業環境中測試與儲存節點的連線時、可能會使用HTTP。

為正式作業網格啟用 HTTP 時請務必小心、因為要求和回應將以未加密的方式傳送。

相關資訊

"管理StorageGRID"

"作用中、閒置及並行HTTP連線的優點"

S3 要求的 **S3** 端點網域名稱

StorageGRID 系統管理員必須先將系統設定為接受在 S3 路徑樣式和 S3 虛擬代管樣式要求中使用 S3 端點網域名稱的連線、才能將 S3 端點網域名稱用於用戶端要求。

關於這項工作

若要使用S3虛擬託管樣式要求、網格管理員必須執行下列工作：

- 使用Grid Manager將S3端點網域名稱新增StorageGRID 至整個系統。
- 請確認用戶端用於HTTPS連線StorageGRID 的驗證書已針對用戶端所需的所有網域名稱簽署。

  例如、如果 S3 API 服務端點網域端點是 `s3.company.com`，網格管理員必須確保用於 HTTPS 連線的憑證具有 `s3.company.com` 做為主體一般名稱和主體替代名稱、以及 `*.s3.company.com` 在主旨替代名稱中。

- "設定 DNS 伺服器" 用戶端用來包含符合 S3 端點網域名稱的 DNS 記錄、包括任何必要的萬用字元記錄。

如果用戶端使用負載平衡器服務連線、則網格管理員設定的憑證是用戶端使用的負載平衡器端點的憑證。

每個負載平衡器端點都有自己的憑證、而且每個端點都可以設定為辨識不同的 S3 端點網域名稱。

如果用戶端連線至儲存節點、則網格管理員所設定的憑證是用於網格的單一自訂伺服器憑證。

請參閱的說明 "管理StorageGRID" 以取得更多資訊。

完成這些步驟之後、您可以使用虛擬託管式要求。

測試**S3 REST API**組態

您可以使用Amazon Web Services命令列介面（AWS CLI）來測試您與系統的連線、並確認您可以讀取物件並將物件寫入系統。

開始之前

- 您已從下載並安裝AWS CLI "aws.amazon.com/cli"。
- 您已在StorageGRID 整個系統上建立S3租戶帳戶。
- 您已在租戶帳戶中建立存取金鑰。

步驟

1. 設定 AWS CLI 設定以使用您在 StorageGRID 系統中建立的帳戶：
   a. 進入組態模式： `aws configure`
   b. 輸入您所建立帳戶的存取金鑰 ID 。
   c. 輸入您所建立帳戶的秘密存取金鑰。
   d. 輸入要使用的預設區域、例如us-east-1。
   e. 輸入要使用的預設輸出格式、或按* Enter *選取Json。
2. 建立儲存庫。

   本範例假設您已將負載平衡器端點設定為使用 IP 位址 10.96.101.17 和連接埠 10443 。

```
aws s3api --endpoint-url https://10.96.101.17:10443
--no-verify-ssl create-bucket --bucket testbucket
```

如果成功建立了儲存區、則會傳回儲存區的位置、如下列範例所示：

```
"Location": "/testbucket"
```

3. 上傳物件。

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
put-object --bucket testbucket --key s3.pdf --body C:\s3-
test\upload\s3.pdf
```

如果物件上傳成功、則會傳回Etag、這是物件資料的雜湊。

4. 列出儲存區的內容、以驗證物件是否已上傳。

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
list-objects --bucket testbucket
```

5. 刪除物件。

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-object --bucket testbucket --key s3.pdf
```

6. 刪除儲存庫。

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-bucket --bucket testbucket
```

支援**StorageGRID** 支援功能

透過支援此平台的服務、非重租戶帳戶可利用遠端S3儲存區、簡易通知服務（SNS）端點或彈性搜尋叢集等外部服務來擴充網格所提供的服務。StorageGRID StorageGRID

下表摘要說明可用的平台服務和用來設定的S3 API。

平台服務	目的	用來設定服務的**S3 API**
CloudMirror複寫	將物件從來源StorageGRID 的靜止庫複寫到設定的遠端S3庫位。	Put Bucket 複寫（請參閱"在貯體上作業"）
通知	將來源StorageGRID 資訊庫中的事件通知傳送至設定的簡易通知服務（SNS）端點。	Put Bucket 通知（請參閱"在貯體上作業"）

平台服務	目的	用來設定服務的**S3 API**
搜尋整合	將StorageGRID 儲存在物件庫的物件中繼資料傳送至已設定的彈性搜尋索引。	"放置時段中繼資料通知組態" *附註：*這是StorageGRID 一套由人自訂的S3 API。

網格管理員必須先啟用租戶帳戶的平台服務、才能使用這些服務。請參閱 "管理StorageGRID"。然後、租戶管理員必須在租戶帳戶中建立代表遠端服務的端點。必須先執行此步驟、才能設定服務。請參閱 "使用租戶帳戶"。

使用平台服務的建議

在使用平台服務之前、您必須瞭解下列建議：

- NetApp建議您允許不超過100個主動租戶、且S3要求需要CloudMirror複寫、通知及搜尋整合。擁有超過100個作用中租戶可能會導致S3用戶端效能變慢。
- 如果 StorageGRID 系統中的 S3 儲存區同時啟用版本設定和 CloudMirror 複寫功能、 NetApp 建議目的地端點也啟用 S3 儲存區版本設定功能。這可讓CloudMirror複寫在端點上產生類似的物件版本。
- 如果來源儲存區已啟用S3物件鎖定、則不支援CloudMirror複寫。
- 如果目的地儲存區已啟用舊版法規遵循、CloudMirror複寫將會失敗並顯示「AccessDenied」錯誤。

如何實作**S3 REST API StorageGRID**

衝突的用戶端要求

衝突的用戶端要求（例如兩個寫入同一個金鑰的用戶端）會以「最新致勝」的方式解決。

「最新致勝」評估的時間取決於StorageGRID 何時由VMware系統完成指定的要求、而非S3用戶端開始作業的時間。

一致性控管

一致性控制功能可根據應用程式的需求、在物件的可用度與不同儲存節點和站台之間的物件一致性之間取得平衡。

根據預設StorageGRID 、此功能可確保新建立物件的寫入後讀取一致性。任何「Get」追蹤成功完成的「PUT」、都能讀取新寫入的資料。覆寫現有物件、更新中繼資料及刪除的動作最終一致。覆寫通常需要幾秒鐘或幾分鐘才能傳播、但可能需要15天的時間。

如果您想要在不同的一致性層級執行物件作業、可以為每個儲存區或每個API作業指定一致性控制。

一致性控管

一致性控制項會影響StorageGRID 到物件所用的中繼資料如何在節點之間分佈、進而影響物件對用戶端要求的可用度。

您可以將桶或API作業的一致性控制設定為下列其中一個值：

- * 全部 * ：所有節點都會立即接收資料、否則要求將會失敗。
- 強式全域：保證所有站台所有用戶端要求的寫入後讀取一致性。
- * Strong站台*：保證站台內所有用戶端要求的寫入後讀取一致性。
- * 新寫入後讀取 * ：（預設）提供新物件的寫入後讀取一致性、以及物件更新的最終一致性。提供高可用度與資料保護保證。建議大多數情況下使用。
- * 可用 * ：提供新物件和物件更新的最終一致性。對於 S3 貯體、請僅視需要使用（例如、包含很少讀取的記錄值之貯體、或用於對不存在的金鑰執行 head 或 Get 作業）。S3 FabricPool 儲存區不支援。

使用「全新寫入後的準備」和「可用」一致性控制

當執行者或Get作業時、StorageGRID 若使用「全新寫入後的讀取」一致性控制、則由下列多個步驟執行查詢：

- 它會先使用低一致性來查詢物件。
- 如果該查詢失敗、它會在下一個一致性層級重複查詢、直到達到等同於 Strong-global 行為的一致性層級為止。

如果 HEAD 或 GET 作業使用「讀取新寫入後」一致性控制項、但物件不存在、則物件查詢一律會達到等同於 Strong-global 行為的一致性層級。由於此一致性層級需要在每個站台上提供多個物件中繼資料複本、因此如果同一個站台上有兩個或多個儲存節點無法使用、您可能會收到大量 500 個內部伺服器錯誤。

除非您需要與Amazon S3類似的一致性保證、否則您可以將一致性控制設定為「可用」、以防止這些錯誤發生、並取得作業。 當使用「可用的」一致性控制時StorageGRID 、只有提供最終一致性的功能、它不會在增加一致性層級的情況下重試失敗的作業、因此不需要物件中繼資料的多個複本。

指定**API**作業的一致性控制

若要設定個別API作業的一致性控制、作業必須支援一致性控制、而且您必須在要求標頭中指定一致性控制。此範例將Get物件作業的一致性控制設為「站台」。

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Consistency-Control: strong-site
```

您必須對「放置物件」和「取得物件」作業使用相同的一致性控制。

指定桶的一致性控制

若要設定桶的一致性控制、您可以使用StorageGRID 「用作桶」一致性要求和「取得桶」一致性要求。您也可以使用租戶管理程式或租戶管理API。

設定桶的一致性控制時、請注意下列事項：

- 設定區段的一致性控制可決定哪些一致性控制用於在區段或區段組態中的物件上執行S3作業。它不會影響儲存庫本身的作業。
- 個別API作業的一致性控制會覆寫貯體的一致性控制。

- 一般而言、貯體應使用預設的一致性控制「讀取新寫入後」。 如果要求無法正常運作、請盡可能變更應用程式用戶端行為。或者、將用戶端設定為針對每個API要求指定一致性控制。只能將貯體層級的一致性控制設定為最後的方法。

[[how — consistency — controls — and — ILM — rules — hender]] 一致性控制和 **ILM** 規則如何交互以影響數據保護

您選擇的一致性控制和ILM規則都會影響物件的保護方式。這些設定可以互動。

例如、儲存物件時所使用的一致性控制項會影響物件中繼資料的初始放置位置、而針對ILM規則所選取的擷取行為則會影響物件複本的初始放置位置。由於支援對象的中繼資料及其資料、因此需要同時存取才能滿足用戶端要求、因此針對一致性層級和擷取行為選擇相符的保護層級、可提供更好的初始資料保護、並提供更可預測的系統回應。StorageGRID

下列擷取行為適用於ILM規則：

- * 雙重承諾 * ： StorageGRID 會立即製作物件的臨時複本、並將成功傳回用戶端。在ILM規則中指定的複本會盡可能製作。
- 嚴格：ILM規則中指定的所有複本都必須在成功傳回用戶端之前完成。
- 平衡：StorageGRID 在擷取時、會嘗試製作ILM規則中指定的所有複本；如果不可能、則會製作過渡複本、並將成功傳回給用戶端。ILM規則中指定的複本會盡可能製作。

> ⓘ 在選擇ILM規則的擷取行為之前、請先閱讀資訊生命週期管理物件管理說明中有關這些設定的完整說明。

一致性控制和**ILM**規則如何互動的範例

假設您有一個雙站台網格、其中包含下列ILM規則和下列一致性層級設定：

- * ILM規則*：建立兩個物件複本、一個在本機站台、一個在遠端站台。選取嚴格的擷取行為。
- 一致性層級：「'trong-globat'（物件中繼資料會立即發佈至所有站台）。

當用戶端將物件儲存到網格時、StorageGRID 在成功傳回用戶端之前、功能區會同時複製物件並將中繼資料散佈到兩個站台。

在擷取最成功的訊息時、物件會受到完整保護、不會遺失。例如、如果在擷取後不久即遺失本機站台、則物件資料和物件中繼資料的複本仍存在於遠端站台。物件可完全擷取。

如果您改用相同的ILM規則和「站台」一致性層級、則用戶端可能會在物件資料複寫到遠端站台之後、收到成功訊息、但物件中繼資料才會散佈到該站台。在此情況下、物件中繼資料的保護層級與物件資料的保護層級不符。如果在擷取後不久本機站台便會遺失、則物件中繼資料將會遺失。無法擷取物件。

一致性層級與ILM規則之間的相互關係可能相當複雜。如需協助、請聯絡NetApp。

相關資訊

"使用ILM管理物件"

"取得庫位一致性"

"實現庫位一致性"

網格管理員會建立資訊生命週期管理（ILM）規則、以管理StorageGRID 從S3 REST API用戶端應用程式擷取到整個系統的物件資料。然後將這些規則新增至ILM原則、以決定物件資料的儲存方式和位置。

ILM設定決定物件的下列層面：

- 地理

  物件資料的位置、無論是StorageGRID 在更新系統（儲存資源池）或雲端儲存資源池中。

- 儲存等級

  用於儲存物件資料的儲存類型：例如Flash或旋轉式磁碟。

- 損失保護

  製作了多少份複本、以及建立的複本類型：複寫、銷毀編碼或兩者。

- 保留

  物件資料的管理方式、儲存位置、以及保護資料不受遺失的方式、都會隨時間而改變。

- 擷取期間的保護

  用於在擷取期間保護物件資料的方法：同步放置（使用擷取行為的平衡或嚴格選項）、或製作過渡複本（使用雙重提交選項）。

ILM規則可篩選及選取物件。對於使用S3擷取的物件、ILM規則可根據下列中繼資料來篩選物件：

- 租戶帳戶
- 儲存區名稱
- 擷取時間
- 金鑰
- 上次存取時間

> 根據預設、所有S3儲存區的上次存取時間更新都會停用。如果您的 StorageGRID 系統包含使用上次存取時間選項的 ILM 規則、則必須針對該規則中指定的 S3 儲存區、啟用更新、使其能在最後存取時間內完成。請使用「放置庫位上次存取時間」要求、租戶管理程式（請參閱 "啟用或停用上次存取時間更新"）、或租戶管理 API 。啟用上次存取時間更新時、請注意StorageGRID 、可能會降低不佳效能、尤其是在使用小型物件的系統中。

- 位置限制
- 物件大小
- 使用者中繼資料
- 物件標籤

相關資訊

"使用租戶帳戶"

"使用ILM管理物件"

"將資源桶放在最後存取時間"

物件版本管理

您可以使用版本管理功能來保留物件的多個版本、避免意外刪除物件、並可讓您擷取及還原物件的舊版。

支援大部分功能的支援功能、以及部分限制、可讓整個系統執行版本管理。StorageGRID支援多達1、000個版本的每個物件。StorageGRID

物件版本管理可與StorageGRID 資訊的生命週期管理（ILM）或S3生命週期組態結合使用。您必須明確啟用每個儲存區的版本管理、才能開啟此儲存區功能。您儲存庫中的每個物件都會指派一個版本ID、由StorageGRID該系統產生。

不支援使用MFA（多因素驗證）刪除。

> 版本管理只能在StorageGRID 以不含更新版本的版本資訊版本10.3所建立的儲存庫上啟用。

ILM與版本管理

ILM原則會套用至物件的每個版本。ILM掃描程序會持續掃描所有物件、並根據目前的ILM原則重新評估這些物件。您對ILM原則所做的任何變更、都會套用至所有先前擷取的物件。如果啟用版本管理、則包括先前擷取的版本。ILM掃描會將新的ILM變更套用至先前擷取的物件。

對於啟用版本設定的儲存區中的 S3 物件、版本設定支援可讓您建立使用「非目前時間」做為參考時間的 ILM 規則（請針對問題選取 * 是 * 「僅將此規則套用至舊版物件？」 在中 "建立 ILM 規則精靈的步驟 1"）。更新物件時、其舊版本會變成非最新版本。使用「非目前時間」篩選器可建立原則、以降低舊版物件的儲存影響。

> 當您使用多部分上傳作業上傳物件的新版本時、原始版本物件的非目前時間會反映新版本的多部分上傳時間、而非多部分上傳完成時。在有限的情況下、原始版本的非目前時間可能比目前版本的時間早上幾小時或幾天。

請參閱 "S3版本化物件的ILM規則和原則（範例4）"。

使用 **S3 REST API** 來設定 **S3** 物件鎖定

如果 StorageGRID 系統已啟用全域 S3 物件鎖定設定、您可以在啟用 S3 物件鎖定的情況下建立儲存區。您可以針對每個物件版本、指定每個儲存區或保留設定的預設保留。

如何為貯體啟用 **S3** 物件鎖定

如果StorageGRID 您的整個S3物件鎖定設定已啟用、則您可以在建立每個儲存區時、選擇性地啟用S3物件鎖定。

S3 物件鎖定是永久性設定、只有在建立貯體時才能啟用。建立貯體後、您無法新增或停用 S3 物件鎖定。

若要為貯體啟用 S3 物件鎖定、請使用下列其中一種方法：

- 使用租戶管理程式建立桶。請參閱 "建立S3儲存區"。
- 使用「放入庫位」要求與一起建立庫位 `x-amz-bucket-object-lock-enabled` 要求標頭：請參閱 "在貯體上作業"。

S3 物件鎖定需要儲存區版本設定、此功能會在建立儲存區時自動啟用。您無法暫停儲存區的版本設定。請參閱 "物件版本管理"。

貯體的預設保留設定

為貯體啟用 S3 物件鎖定時、您可以選擇性地啟用貯體的預設保留、並指定預設保留模式和預設保留期間。

預設保留模式

- 在法規遵循模式中：
  - 直到達到物件的保留日期、才能刪除物件。
  - 物件的保留日期可以增加、但不能減少。
  - 直到達到該日期為止、才能移除物件的保留日期。
- 在治理模式中：
  - 的使用者 `s3:BypassGovernanceRetention` 權限可以使用 `x-amz-bypass-governance-retention: true` 要求標頭略過保留設定。
  - 這些使用者可以在達到物件版本的保留截止日期之前刪除物件版本。
  - 這些使用者可以增加、減少或移除物件的保留到目前為止。

預設保留期間

每個貯體都可以有一段以年或日為單位指定的預設保留期間。

如何設定貯體的預設保留

若要設定貯體的預設保留、請使用下列其中一種方法：

- 從 Tenant Manager 管理貯體設定。請參閱 "建立S3儲存區" 和 "更新 S3 物件鎖定預設保留"。
- 針對貯體發出「放置物件鎖定組態」要求、以指定預設模式和預設天數或年數。

放置物件鎖定組態

「放置物件鎖定組態」要求可讓您設定及修改已啟用 S3 物件鎖定的儲存區的預設保留模式和預設保留期間。您也可以移除先前設定的預設保留設定。

將新物件版本擷取至貯體時、會套用預設保留模式 `x-amz-object-lock-mode` 和 `x-amz-object-lock-retain-until-date` 未指定。預設保留期間用於計算截止日期 IF `x-amz-object-lock-retain-until-date` 未指定。

如果在擷取物件版本之後修改預設保留期間、則物件版本的保留截止日期將維持不變、且不會使用新的預設保留期間重新計算。

您必須擁有 `s3:PutBucketObjectLockConfiguration` 完成此作業的權限、或是帳戶根目錄。

。 `Content-MD5` 必須在 PUT 要求中指定要求標頭。

申請範例

此範例可為貯體啟用 S3 物件鎖定、並將預設保留模式設為符合法規、並將預設保留期間設為 6 年。

```
PUT /bucket?object-lock HTTP/1.1
Accept-Encoding: identity
Content-Length: 308
Host: host
Content-MD5: request header
User-Agent: s3sign/1.0.0 requests/2.24.0 python/3.8.2
X-Amz-Date: date
X-Amz-Content-SHA256: authorization-string
Authorization: authorization-string

<ObjectLockConfiguration>
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

如何決定貯體的預設保留

若要判斷儲存區是否啟用 S3 物件鎖定、並查看預設保留模式和保留期間、請使用下列其中一種方法：

- 在租戶管理器中檢視貯體。請參閱 "檢視 S3 儲存區"。
- 發出「取得物件鎖定組態」要求。

取得物件鎖定組態

「取得物件鎖定組態」要求可讓您判斷儲存區是否已啟用 S3 物件鎖定、如果已啟用、請查看儲存區是否已設定預設保留模式和保留期間。

將新物件版本擷取至貯體時、會套用預設保留模式 `x-amz-object-lock-mode` 未指定。預設保留期間用於計算截止日期 IF `x-amz-object-lock-retain-until-date` 未指定。

您必須擁有 `s3:GetBucketObjectLockConfiguration` 完成此作業的權限、或是帳戶根目錄。

申請範例

```
GET /bucket?object-lock HTTP/1.1
Host: host
Accept-Encoding: identity
User-Agent: aws-cli/1.18.106 Python/3.8.2 Linux/4.4.0-18362-Microsoft
botocore/1.17.29
x-amz-date: date
x-amz-content-sha256: authorization-string
Authorization: authorization-string
```

回應範例

```
HTTP/1.1 200 OK
x-amz-id-2:
iVmcB7OXXJRkRH1FiVq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpXlknabA0LTvBYJpSIX
k=
x-amz-request-id: B34E94CACB2CEF6D
Date: Fri, 04 Sep 2020 22:47:09 GMT
Transfer-Encoding: chunked
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<ObjectLockConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

如何指定物件的保留設定

啟用 S3 物件鎖定的貯體可包含物件組合、並具有或不含 S3 物件鎖定保留設定。

物件層級保留設定是使用 S3 REST API 指定的。物件的保留設定會覆寫貯體的任何預設保留設定。

您可以為每個物件指定下列設定：

- * 保留模式 * ：法規遵循或治理。
- * 截止日期 * ：指定 StorageGRID 必須保留物件版本多久的日期。
  - 在規範模式中、如果保留截止日期是未來、則可以擷取物件、但無法修改或刪除物件。保留截止日期可以增加、但無法減少或移除此日期。

- 在治理模式中、具有特殊權限的使用者可以略過保留到最新的設定。他們可以在物件版本的保留期間結束之前刪除物件版本。他們也可以增加、減少或甚至移除截止日期的保留。

- 合法持有：將合法持有套用至物件版本、會立即鎖定該物件。例如、您可能需要對與調查或法律爭議相關的物件保留法律。合法持有沒有到期日、但在明確移除之前、仍會保留到位。

  物件的合法保留設定不受保留模式和保留截止日期的影響。如果物件版本處於合法保留狀態、則沒有人可以刪除該版本。

若要在將物件版本新增至貯體時指定 S3 物件鎖定設定、請發出 "放置物件"、 "放置物件-複製"或 "啟動多部份上傳" 申請。

您可以使用下列項目：

- `x-amz-object-lock-mode`，可以是法規遵循或治理（區分大小寫）。

  > 如果您指定 `x-amz-object-lock-mode`，您也必須指定 `x-amz-object-lock-retain-until-date`。

- `x-amz-object-lock-retain-until-date`
  - 保留截止日期值必須採用格式 `2020-08-10T21:46:00Z`。允許分數秒、但只保留3個小數位數（毫秒精度）。不允許其他 ISO 8601 格式。
  - 保留截止日期必須為未來日期。
- `x-amz-object-lock-legal-hold`

  如果已開啟合法持有（區分大小寫）、則物件將置於合法持有之下。如果法律保留已關閉、則不會保留任何合法的保留。任何其他值都會導致400個錯誤要求（InvalidArgument）錯誤。

如果您使用上述任一要求標頭、請注意下列限制：

- 。 `Content-MD5` 如有任何要求、則要求標頭為必填欄位 `x-amz-object-lock-*` 要求標頭出現在「放置物件」要求中。 `Content-MD5` 不需要「放置物件-複製」或「啟動多重成分上傳」。
- 如果儲存區未啟用S3物件鎖定和 `x-amz-object-lock-*` 出現要求標頭、傳回400個錯誤要求（InvalidRequest）錯誤。
- 「放置物件」要求支援使用 `x-amz-storage-class: REDUCED_REDUNDANCY` 以符合AWS行為。然而、當物件被擷取至啟用S3物件鎖定的儲存區時StorageGRID 、則會一律執行雙重認可擷取。
- 後續的Get或HeadObject版本回應將包含標頭 `x-amz-object-lock-mode`、 `x-amz-object-lock-retain-until-date`和 `x-amz-object-lock-legal-hold`（如果已設定）以及要求傳送者是否正確 `s3:Get*` 權限：

您可以使用 `s3:object-lock-remaining-retention-days` 原則條件金鑰、可限制物件的最小和最大允許保留期間。

如何更新物件的保留設定

如果您需要更新現有物件版本的合法保留或保留設定、可以執行下列物件子資源作業：

- `PUT Object legal-hold`

如果新的合法持有值已開啟、則物件將置於合法持有之下。如果合法持有值為「關」、則合法持有將被解除。

- `PUT Object retention`
  - 模式值可以是法規遵循或治理（區分大小寫）。
  - 保留截止日期值必須採用格式 `2020-08-10T21:46:00Z`。允許分數秒、但只保留3個小數位數（毫秒精度）。不允許其他 ISO 8601 格式。
  - 如果物件版本有現有的截至日期保留、您只能增加。新的價值必須是未來的價值。

如何使用治理模式

擁有的使用者 `s3:BypassGovernanceRetention` 權限可以略過使用治理模式之物件的作用中保留設定。任何刪除或放置物件保留作業都必須包含 `x-amz-bypass-governance-retention:true` 要求標頭：這些使用者可以執行這些額外作業：

- 執行刪除物件或刪除多個物件作業、以在物件版本的保留期間結束之前刪除物件版本。

  合法持有的物件無法刪除。合法持有必須關閉。

- 在物件的保留期間結束之前、執行「放置物件」保留作業、將物件版本的模式從治理變更為符合性。

  永遠不允許將模式從法規遵循變更為治理。

- 執行「放置物件」保留作業、以增加、減少或移除物件版本的保留期間。

相關資訊

- "使用S3物件鎖定來管理物件"
- "使用 S3 物件鎖定來保留物件"
- "Amazon簡易儲存服務使用者指南：使用S3物件鎖定"

建立**S3**生命週期組態

您可以建立S3生命週期組態、以控制何時從StorageGRID 作業系統刪除特定物件。

本節的簡單範例說明S3生命週期組態如何控制從特定S3儲存區刪除（過期）特定物件的時間。本節範例僅供說明用途。如需建立S3生命週期組態的完整詳細資料、請參閱 "Amazon Simple Storage Service開發人員指南：物件生命週期管理"。請注意StorageGRID 、僅支援過期行動、不支援轉換行動。

什麼是生命週期組態

生命週期組態是套用至特定S3儲存區中物件的一組規則。每個規則都會指定受影響的物件、以及這些物件何時到期（在特定日期或幾天之後）。

在生命週期組態中、支援多達1、000個生命週期規則。StorageGRID每個規則可包含下列XML元素：

- 過期：在達到指定日期或達到指定天數時刪除物件、從擷取物件開始算起。
- 非目前版本過期：在達到指定天數時刪除物件、從物件變成非目前的開始算起。
- 篩選器（前置、標記）

- 狀態
- ID

如果您將生命週期組態套用至貯體、則該貯體的生命週期設定一律會覆寫StorageGRID 「ILM」設定。使用儲存區的到期設定、而非ILM來決定是否要刪除或保留特定物件。StorageGRID

因此、即使ILM規則中的放置指示仍套用至物件、也可能從網格中移除物件。或者、即使物件的任何ILM放置指示失效、物件仍可能保留在網格上。如需詳細資訊、請參閱 "ILM在物件生命週期內的運作方式"。

> 庫位生命週期組態可搭配已啟用S3物件鎖定的庫位使用、但庫位生命週期組態不支援舊型符合標準的庫位。

支援使用下列庫位作業來管理生命週期組態：StorageGRID

- 刪除時段生命週期
- 取得生命週期
- 放入鏟斗生命週期

建立生命週期組態

建立生命週期組態的第一步、就是建立一個包含一或多個規則的Json檔案。例如、此Json檔案包含三個規則、如下所示：

1. 規則1僅適用於符合前置碼的物件 `category1/`而且有 `key2` 的價值 `tag2`。。 `Expiration` 參數指定符合篩選條件的物件將於2020年8月22日午夜到期。
2. 規則2僅適用於符合前置碼的物件 `category2/`。。 `Expiration` 參數指定符合篩選條件的物件在擷取後100天過期。

   > 指定天數的規則是相對於擷取物件的時間。如果目前日期超過擷取日期加上天數、則在套用生命週期組態後、部分物件可能會立即從儲存庫中移除。

3. 規則3僅適用於符合前置碼的物件 `category3/`。。 `Expiration` 參數指定任何非目前版本的相符物件在變成非目前物件50天後過期。

```
{
    "Rules": [
        {
            "ID": "rule1",
            "Filter": {
                "And": {
                    "Prefix": "category1/",
                    "Tags": [
                        {
                            "Key": "key2",
                            "Value": "tag2"
                        }
                    ]
                }
            },
            "Expiration": {
                "Date": "2020-08-22T00:00:00Z"
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule2",
            "Filter": {
                "Prefix": "category2/"
            },
            "Expiration": {
                "Days": 100
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule3",
            "Filter": {
                "Prefix": "category3/"
            },
            "NoncurrentVersionExpiration": {
                "NoncurrentDays": 50
            },
            "Status": "Enabled"
        }
    ]
}
```

將生命週期組態套用至貯體

建立生命週期組態檔案之後、您可以發出「放入庫位」生命週期要求、將其套用至庫位。

此要求會將範例檔案中的生命週期組態套用至名為的儲存區中的物件 `testbucket`。

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-
configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

若要驗證生命週期組態是否已成功套用至儲存庫、請發出「Get Bucket生命週期」要求。例如：

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-
configuration
 --bucket testbucket
```

成功的回應會列出您剛套用的生命週期組態。

驗證目標是否適用庫位生命週期到期

您可以在發出「放置物件」、「標頭物件」或「取得物件」要求時、判斷生命週期組態中的到期規則是否適用於特定物件。如果適用規則、回應會包含 `Expiration` 指出物件到期時間及符合到期規則的參數。

> 因為儲存區生命週期會取代ILM `expiry-date` 顯示的是物件刪除的實際日期。如需詳細資訊、請參閱 "如何判斷物件保留"。

例如、此Put物件要求是在2020年6月22日發出、並在中放置物件 `testbucket` 鏟斗。

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

成功回應表示物件將在100天（2020年10月1日）後過期、且符合生命週期組態的規則2。

```
{
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:49 GMT\", rule-
id=\"rule2\"",
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
}
```

例如、此「標頭物件」要求是用來取得同一個物件在testBucket儲存區中的中繼資料。

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object
--bucket testbucket --key obj2test2
```

成功回應包括物件的中繼資料、指出物件將在100天內過期、且符合規則2。

```
{
      "AcceptRanges": "bytes",
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:48 GMT\", rule-
id=\"rule2\"",
      "LastModified": "2020-06-23T09:07:48+00:00",
      "ContentLength": 921,
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
      "ContentType": "binary/octet-stream",
      "Metadata": {}
}
```

實作**S3 REST API**的建議

實作S3 REST API以搭配StorageGRID 使用時、請遵循以下建議。

針對不存在物件的使用者提出建議

如果您的應用程式會定期檢查某個物件是否存在於您不希望該物件實際存在的路徑、則應使用「可用」一致性控制項。例如、如果您的應用程式在放入之前就先前往某個位置、則應該使用「可用」一致性控制。

否則、如果執行頭作業找不到物件、當一個或多個儲存節點無法使用時、您可能會收到大量500個內部伺服器錯誤。

您可以使用「放置時段一致性」要求、為每個時段設定「可用」一致性控制、也可以在個別API作業的要求標頭中指定一致性控制。

物件金鑰建議

請根據第一次建立貯體的時間、遵循下列物件金鑰名稱建議。

在 **StorageGRID 11.4** 或更早版本中建立的貯體

- 請勿使用隨機值做為物件金鑰的前四個字元。這與前AWS關於金鑰前置碼的建議不同。請改用非隨機、非唯一的前置字元、例如 `image`。
- 如果您遵循前 AWS 的建議、在金鑰首碼中使用隨機和唯一字元、請在物件金鑰前加上目錄名稱。也就是使用此格式：

  `mybucket/mydir/f8e3-image3132.jpg`

  而非此格式：

  `mybucket/f8e3-image3132.jpg`

在 **StorageGRID 11.4** 或更新版本中建立的貯體

不需要限制物件金鑰名稱以符合效能最佳實務做法。在大多數情況下、您可以對物件金鑰名稱的前四個字元使用隨機值。

S3 工作負載的例外情況是、它會在一段短時間後持續移除所有物件。為了將此使用案例的效能影響降至最低、請將金鑰名稱的前置部分變更為每數千個物件、例如日期。例如、假設 S3 用戶端通常每秒寫入 2 、 000 個物件、而 ILM 或儲存庫生命週期原則則會在三天後移除所有物件。若要將效能影響降至最低、您可以使用如下模式命名金鑰： `/mybucket/mydir/yyyymmddhhmmss-random_UUID.jpg`

「range Reads」建議

如果是 "用於壓縮儲存物件的全域選項" 啟用後、 S3 用戶端應用程式應避免執行指定傳回位元組範圍的 Get Object 作業。這些「範圍讀取」作業效率不彰、因為StorageGRID 必須有效解壓縮物件才能存取所要求的位元組。從非常大的物件要求少量位元組的「Get Object」（取得物件）作業效率特別低；例如、從50 GB壓縮物件讀取10 MB範圍的效率不彰。

如果從壓縮物件讀取範圍、用戶端要求可能會逾時。

如果您需要壓縮物件、而用戶端應用程式必須使用範圍讀取、請增加應用程式的讀取逾時。

相關資訊

- "一致性控管"
- "實現庫位一致性"
- "管理StorageGRID"

支援 **Amazon S3 REST API**

S3 REST API 實作詳細資料

此系統實作簡單儲存服務API（API版本2002-03）、支援大部分作業、並有一些限制。StorageGRID整合S3 REST API用戶端應用程式時、您必須瞭解實作詳細資料。

支援虛擬託管型要求和路徑型要求的支援。StorageGRID

日期處理

S3 REST API的支援僅支援有效的HTTP日期格式。StorageGRID

支援此功能的僅支援接受日期值的任何標頭的有效HTTP日期格式。StorageGRID日期的時間部分可以格林尼治標準時間（GMT）格式指定、或以通用協調時間（UTC）格式指定、且無時區偏移（必須指定+0000）。如果您包含 `x-amz-date` 標頭在您的要求中、會覆寫在「日期」要求標頭中指定的任何值。使用AWS簽名版本4時 `x-amz-date` 由於不支援日期標頭、因此標頭必須存在於簽署的要求中。

一般要求標頭

StorageGRID 系統支援定義的一般要求標頭 "Amazon Simple Storage Service API 參考：一般要求標頭"、但有一項例外。

要求標頭	實作
授權	完整支援AWS簽名版本2 支援AWS簽名版本4、但有下列例外： • SHA256值不會針對申請本文進行計算。使用者提交的值會在未經驗證的情況下接受、如同值一樣 `UNSIGNED-PAYLOAD` 已提供給 `x-amz-content-sha256` 標頭。
X-amz-security-token	未實作。退貨 `XNotImplemented`。

通用回應標頭

支援所有由_Simple Storage Service API Reference（簡易儲存服務API參考）定義的通用回應標頭、但有一項例外。StorageGRID

回應標頭	實作
X-amz-id-2	未使用

驗證要求

支援使用S3 API驗證和匿名存取物件的功能。StorageGRID

S3 API支援驗證S3 API要求的簽名版本2和簽名版本4。

驗證的要求必須使用您的存取金鑰ID和秘密存取金鑰來簽署。

支援兩種驗證方法：HTTP StorageGRID `Authorization` 標頭及使用查詢參數。

使用**HTTP**授權標頭

HTTP `Authorization` 標頭會被所有S3 API作業使用、但資源庫原則允許的匿名要求除外。。 `Authorization` 標頭包含驗證要求所需的所有簽署資訊。

使用查詢參數

您可以使用查詢參數將驗證資訊新增至URL。這稱為URL預先簽署、可用來授予特定資源的暫時存取權。具有預先簽署 URL 的使用者不需要知道密碼存取金鑰即可存取資源、這可讓您提供第三方受限存取資源。

服務營運

支援下列服務作業的支援。StorageGRID

營運	實作
取得服務 `(ListBuckets)`	以所有Amazon S3 REST API行為來實作。如有變更、恕不另行通知。
取得儲存使用量	「Get Storage使用量」要求會告訴您某個帳戶所使用的總儲存容量、以及與該帳戶相關聯的每個儲存區容量。這是服務上的作業、其路徑為/和自訂查詢參數 (`?x-ntap-sg-usage`）新增。
選項/	用戶端應用程式可能會發生問題 `OPTIONS /` 要求儲存節點上的S3連接埠、但不提供S3驗證認證、以判斷儲存節點是否可用。您可以使用此要求進行監控、或允許外部負載平衡器識別儲存節點何時當機。

相關資訊

"取得儲存使用量"

在貯體上作業

這個系統最多可為每個S3租戶帳戶支援1、000個貯體。StorageGRID

貯體名稱限制遵循 AWS 美國標準地區限制、但您應進一步將它們限制在 DNS 命名慣例、以支援 S3 虛擬託管式要求。

如需詳細資訊、請參閱下列內容：

- "Amazon Web Services（AWS）文件：儲存區限制與限制"
- "設定 S3 端點網域名稱"

Get Bucket（列出物件）和Get Bucket版本作業支援StorageGRID 一致性控管。

您可以檢查是否為個別的儲存區啟用或停用上次存取時間的更新。

下表說明StorageGRID 了為什麼由Ss哪些 人執行S3 REST API貯體作業。若要執行上述任何作業、必須為帳戶提供必要的存取認證資料。

營運	實作
刪除時段	此作業會刪除貯體。
刪除庫位檢查	此作業會刪除儲存區的CORS組態。
刪除時段加密	此作業會從儲存區刪除預設加密。現有的加密物件會保持加密狀態、但新增至儲存庫的任何新物件都不會加密。
刪除時段生命週期	此作業會從儲存庫中刪除生命週期組態。請參閱 "建立S3生命週期組態"。

營運	實作
刪除庫位原則	此作業會刪除附加至儲存貯體的原則。
刪除時段複寫	此作業會刪除附加至儲存區的複寫組態。
刪除庫位標記	此作業使用 `tagging` SubResource可移除庫位中的所有標記。
取得 Bucket （ ListObjects ） （ ListObjectsV2 ）	此作業會傳回某個儲存區中的部分或全部（最多1、000個）物件。物件的儲存類別可以有兩個值之一、即使物件是使用擷取的 `REDUCED_REDUNDANCY` 儲存類別選項： • `STANDARD`（表示物件儲存在儲存節點所組成的儲存資源池中）。 • `GLACIER`、表示物件已移至Cloud Storage Pool指定的外部儲存區。 如果儲存區包含大量具有相同前置碼的刪除金鑰、回應可能會包含部分金鑰 `CommonPrefixes` 不包含金鑰。
取得Bucket物件版本 （ ListObjectVerions ）	此作業可透過鏟斗的讀取存取權限 `versions` 子資源會列出儲存區中所有物件版本的中繼資料。
取得Bucket ACL	此作業會傳回正面回應、並傳回貯體擁有者的ID、顯示名稱和權限、表示擁有者對該貯體具有完整存取權。
獲取庫位檢查器	此作業會傳回 `cors` 鏟斗組態。
取得Bucket加密	此作業會傳回儲存區的預設加密組態。
取得生命週期 （ GetBucketLifecycleConfiguration ）	此作業會傳回該儲存庫的生命週期組態。請參閱 "建立S3生命週期組態"。
取得理想位置	此作業會傳回使用設定的區域 `LocationConstraint` 置入庫位要求中的元素。如果庫位所在的區域是 `us-east-1`，則會傳回區域的空白字串。
取得庫存箱通知 （ GetBucketNotificationConfiguration ）	此作業會傳回附加至儲存貯體的通知組態。
取得庫存管理政策	此作業會傳回附加至庫位的原則。

營運	實作
取得庫位複寫	此作業會傳回附加至儲存區的複寫組態。
取得庫位標記	此作業使用 `tagging` SubResource可傳回某個儲存區的所有標記。
取得版本管理	此實作使用 `versioning` SubResource可傳回儲存區的版本管理狀態。 • *blank*：從未啟用版本管理（儲存庫為「未版本管理」） • 已啟用：已啟用版本管理 • 已暫停：先前已啟用版本管理、並已暫停
取得物件鎖定組態	此作業會傳回儲存區預設保留模式和預設保留期間（若已設定）。 請參閱 "使用 S3 REST API 來設定 S3 物件鎖定"。
鏟斗	此作業會判斷儲存區是否存在、且您是否有權存取它。 此作業會傳回： • `x-ntap-sg-bucket-id`： UUID 格式的儲存區 UUID 。 • `x-ntap-sg-trace-id`：關聯請求的唯一跟蹤 ID 。

營運	實作
放入鏟斗	此作業會建立新的儲存桶。建立貯體後、您就成為了貯體的擁有者。 • 庫位名稱必須符合下列規則： ◦ 必須在各個StorageGRID 方面都是獨一無二的（不只是租戶帳戶內的獨特功能）。 ◦ 必須符合DNS規範。 ◦ 必須包含至少3個字元、且不得超過63個字元。 ◦ 可以是一或多個標籤的系列、相鄰的標籤以句點分隔。每個標籤都必須以英文字母或數字開頭和結尾、而且只能使用英文字母、數字和連字號。 ◦ 不得看起來像是文字格式的IP位址。 ◦ 不應在虛擬託管樣式要求中使用期間。期間會導致伺服器萬用字元憑證驗證發生問題。 • 根據預設、會在中建立儲存區 `us-east-1` 區域；不過、您可以使用 `LocationConstraint` 要求主體中的要求元素、以指定不同的區域。使用時 `LocationConstraint` 元素、您必須指定已使用Grid Manager或Grid Management API定義的區域確切名稱。如果您不知道應該使用的地區名稱、請聯絡您的系統管理員。 附註：如果您的Pet Bucket要求使用StorageGRID 未在功能區中定義的區域、就會發生錯誤。 • 您可以加入 `x-amz-bucket-object-lock-enabled` 要求標頭以建立啟用S3物件鎖定的儲存區。請參閱 "使用 S3 REST API 來設定 S3 物件鎖定"。 建立儲存區時、您必須啟用S3物件鎖定。建立貯體後、您無法新增或停用 S3 物件鎖定。S3物件鎖定需要儲存區版本管理、這會在您建立儲存區時自動啟用。
放入庫位	此作業會設定儲存區的CORS組態、以便儲存區能夠處理跨來源要求。跨來源資源共用（CORS）是一種安全機制、可讓單一網域中的用戶端Web應用程式存取不同網域中的資源。例如、假設您使用名為的S3儲存區 `images` 儲存圖形。設定的CORS組態 `images` 儲存庫、您可以讓該儲存庫中的影像顯示在網站上 `http://www.example.com`。
使用資源桶加密	此作業會設定現有儲存區的預設加密狀態。啟用桶層級加密時、任何新增至桶的新物件都會加密。StorageGRID支援使用StorageGRID管理的金鑰進行伺服器端加密。指定伺服器端加密組態規則時、請設定 `SSEAlgorithm` 參數至 `AES256`、請勿使用 `KMSMasterKeyID` 參數。 如果物件上傳要求已指定加密（亦即、如果要求包含、則會忽略儲存區預設加密組態 `x-amz-server-side-encryption-*` 要求標頭）。

營運	實作
放入鏟斗生命週期 （PuttBucketLifecycleConfiguration ）	此作業會為儲存庫建立新的生命週期組態、或取代現有的生命週期組態。在生命週期組態中、支援多達1、000個生命週期規則。StorageGRID每個規則可包含下列XML元素： • 到期日（天數、日期） • 非目前版本過期（非目前日期） • 篩選器（前置、標記） • 狀態 • ID 不支援下列動作：StorageGRID • AbortIncompleteMultiPart上 傳 • ExpiredObjectDelete標記 • 移轉 請參閱 "建立S3生命週期組態"。若要瞭解貯體生命週期中的到期動作如何與 ILM 放置指示互動、請參閱 "ILM如何在整個物件生命週期內運作"。 附註：鏟斗生命週期組態可搭配已啟用S3物件鎖定的鏟斗使用、但舊型符合標準的鏟斗不支援鏟斗生命週期組態。

營運	實作

放置時段通知
 	
（ PuttBucketNotificationConfiguration ）
	此作業會使用要求內文所含的通知組態XML來設定儲存區的通知。您應該瞭解下列實作詳細資料：
	
	• 支援簡單通知服務（SNS）主題作為目的地。StorageGRID不支援 Simple Queue Service （ SQS ）或 Amazon Lambda 端點。
	• 通知的目的地必須指定為StorageGRID 一個端點的URN。端點可以使用租戶管理程式或租戶管理API來建立。
	
	端點必須存在、通知組態才能成功。如果端點不存在、則為 `400 Bad Request` 程式碼傳回錯誤 `InvalidArgument`。
	
	• 您無法設定下列事件類型的通知。這些事件類型*不支援*。
	
	◦ `s3:ReducedRedundancyLostObject`
	
	◦ `s3:ObjectRestore:Completed`
	
	• 從 StorageGRID 傳送的事件通知使用標準 JSON 格式、但不包含某些金鑰、也不為其他金鑰使用特定值、如下表所示：
	
	◦ 事件來源
	
	`sgws:s3`
	
	◦ * awsRegion *
	
	不含
	
	◦ * X-amz-id-2*
	
	不含
	
	◦ * arn*
	
	`urn:sgws:s3:::bucket_name`

資源桶政策	此作業會設定附加至庫位的原則。

營運	實作
放入資源桶複寫	此作業會進行設定 "StorageGRID CloudMirror 複寫" 適用於要求主體中所提供的複寫組態 XML 的貯體。對於CloudMirror複寫、您應該瞭解下列實作詳細資料： • 僅支援複寫組態的V1。StorageGRID這表示StorageGRID 、不支援使用 `Filter` 規則元素、並遵循刪除物件版本的V1慣例。如需詳細資訊、請參閱 "有關複寫組態的Amazon S3文件"。 • 儲存區複寫可在版本控制或未版本控制的儲存區上進行設定。 • 您可以在複寫組態XML的每個規則中指定不同的目的地儲存區。來源儲存區可複寫至多個目的地儲存區。 • 目的地貯體必須指定為StorageGRID 租戶管理程式或租戶管理API中指定的非功能性端點的URN。請參閱 "設定CloudMirror複寫"。 複寫組態必須存在端點才能成功。如果端點不存在、則要求會以的形式失敗 `400 Bad Request`。錯誤訊息指出： `Unable to save the replication policy. The specified endpoint URN does not exist: URN.` • 您不需要指定 `Role` 在組態XML中。此值不供StorageGRID Some使用、如果提交、將會忽略此值。 • 如果您從組態XML中省略儲存類別、StorageGRID 則無法使用 `STANDARD` 預設為儲存類別。 • 如果您從來源儲存區刪除物件、或是刪除來源儲存區本身、跨區域複寫行為如下： ◦ 如果您在物件或貯體複寫之前刪除該物件或貯體、則不會複寫該物件 / 貯體、也不會通知您。 ◦ 如果您在複寫物件或儲存區之後將其刪除、StorageGRID 則針對跨區域複寫的V1、執行標準Amazon S3刪除行為。
置入庫位標記	此作業使用 `tagging` 子資源：新增或更新一組庫位的標記。新增庫位標記時、請注意下列限制： • 支援每個儲存區最多50個標籤的支援功能包括：StorageGRID • 與庫位關聯的標記必須具有唯一的標記金鑰。標籤金鑰長度最多可達128個UNICODE字元。 • 標記值長度最多可達256個UNICODE字元。 • 金鑰和值區分大小寫。

營運	實作
放入資源桶版本管理	此實作使用 `versioning` SubResource可設定現有儲存區的版本管理狀態。您可以使用下列其中一個值來設定版本設定狀態： • 已啟用：啟用儲存區中物件的版本管理。新增至儲存庫的所有物件都會收到唯一的版本ID。 • 暫停：停用儲存區中物件的版本設定。新增至儲存庫的所有物件都會收到版本ID `null`。
放置物件鎖定組態	此作業會設定或移除庫位預設保留模式和預設保留期間。 如果修改了預設保留期間、現有物件版本的保留截止日期將維持不變、且不會使用新的預設保留期間重新計算。 請參閱 "使用 S3 REST API 來設定 S3 物件鎖定" 以取得詳細資訊。

相關資訊

"一致性控管"

"取得時段上次存取時間"

"使用貯體和群組存取原則"

"在稽核記錄中追蹤S3作業"

在貯體上進行自訂作業

支援將自訂儲存區作業新增至S3 REST API、並專供系統使用。StorageGRID

下表列出StorageGRID 支援的自訂儲存區作業。

營運	說明	以取得更多資訊
取得庫位一致性	傳回套用至特定儲存庫的一致性層級。	"取得庫位一致性"
實現庫位一致性	設定套用至特定儲存庫的一致性層級。	"實現庫位一致性"
取得時段上次存取時間	傳回是否為特定儲存區啟用或停用上次存取時間更新。	"取得時段上次存取時間"
將資源桶放在最後存取時間	可讓您啟用或停用特定儲存區的上次存取時間更新。	"將資源桶放在最後存取時間"
刪除時段中繼資料通知組態	刪除與特定儲存區相關聯的中繼資料通知組態XML。	"刪除時段中繼資料通知組態"

營運	說明	以取得更多資訊
取得Bucket中繼資料通知組態	傳回與特定儲存區相關聯的中繼資料通知組態XML。	"取得Bucket中繼資料通知組態"
放置時段中繼資料通知組態	設定區段的中繼資料通知服務。	"放置時段中繼資料通知組態"
運用法規遵循設定來滿足需求	已過時且不受支援：您無法再建立啟用「符合性」的新儲存區。	"已過時：將資源桶放在符合法規的設定中"
取得符合需求的產品	已過時但受支援：傳回現有舊版相容儲存區目前有效的法規遵循設定。	"已過時：取得 Bucket 法規遵循"
符合資源需求	已過時但受支援：可讓您修改現有舊版相容儲存區的法規遵循設定。	"已過時：符合 Put Bucket 規範"

相關資訊

"稽核記錄中追蹤的S3作業"

物件上的作業

本節說明StorageGRID 此「物件」的「物件」功能如何執行S3 REST API作業。

下列條件適用於所有物件作業：

- StorageGRID "一致性控管" 受物件上的所有作業支援、但下列項目除外：
  - 取得物件ACL
  - `OPTIONS /`
  - 將物件保留為合法
  - 保留物件
  - 選取「物件內容」
- 衝突的用戶端要求（例如兩個寫入同一個金鑰的用戶端）會以「最新致勝」的方式解決。「最新致勝」評估的時間、是根據StorageGRID 下列條件而定：當系統完成特定要求時、S3用戶端開始作業時、不會開啟。
- 所有物件均由庫位擁有者擁有、包括匿名使用者或其他帳戶所建立的物件。StorageGRID
- 透過 Swift 擷取至 StorageGRID 系統的資料物件無法透過 S3 存取。

下表說明StorageGRID 了Ss哪些 物件是由S3 REST API物件執行。

營運	實作
刪除物件	多因素驗證（MFA）和回應標頭 `x-amz-mfa` 不受支援。 處理刪除物件要求時StorageGRID 、功能區會嘗試立即從所有儲存位置移除物件的所有複本。如果成功、StorageGRID 則會立即將回應傳回給用戶端。如果無法在 30 秒內移除所有複本（例如、因為某個位置暫時無法使用）、 StorageGRID 會將複本排入佇列以供移除、然後表示用戶端成功。 版本管理 若要移除特定版本、申請者必須是貯體擁有者、並使用 `versionId` 子資源：使用此子資源會永久刪除版本。如果是 `versionId` 對應於刪除標記、即回應標頭 `x-amz-delete-marker` 傳回設定為 `true`。 • 如果刪除的物件不含 `versionId` 子資源在啟用版本的儲存區上、會產生刪除標記。。 `versionId` 刪除標記會使用傳回 `x-amz-version-id` 回應標頭和 `x-amz-delete-marker` 回應標頭會傳回設定為 `true`。 • 如果刪除的物件不含 `versionId` 子資源在版本暫停的儲存區上、會永久刪除現有的'null '版本或'null '刪除標記、並產生新的'null '刪除標記。。 `x-amz-delete-marker` 回應標頭會傳回設定為 `true`。 附註：在某些情況下、物件可能會有多個刪除標記。 請參閱 "使用 S3 REST API 來設定 S3 物件鎖定" 以瞭解如何在治理模式中刪除物件版本。
刪除多個物件 （刪除物件）	多因素驗證（MFA）和回應標頭 `x-amz-mfa` 不受支援。 您可以在同一個要求訊息中刪除多個物件。 請參閱 "使用 S3 REST API 來設定 S3 物件鎖定" 以瞭解如何在治理模式中刪除物件版本。
刪除物件標記	使用 `tagging` SubResource可移除物件的所有標記。 版本管理 如果是 `versionId` 查詢參數未在要求中指定、此作業會刪除版本控制儲存區中物件最新版本的所有標記。如果物件的目前版本是刪除標記、則會傳回「MethodNotSupported」狀態 `x-amz-delete-marker` 回應標頭設定為 `true`。
取得物件	"取得物件"
取得物件ACL	如果提供帳戶所需的存取認證資料、則作業會傳回正面回應、並傳回物件擁有者的ID、顯示名稱和權限、表示擁有者擁有物件的完整存取權。

營運	實作
取得物件合法持有	"使用 S3 REST API 來設定 S3 物件鎖定"
取得物件保留	"使用 S3 REST API 來設定 S3 物件鎖定"
取得物件標記	使用 `tagging` SubResource可傳回物件的所有標記。 版本管理 如果是 `versionId` 查詢參數未在要求中指定、此作業會傳回版本控制儲存區中物件最新版本的所有標記。如果物件的目前版本是刪除標記、則會傳回「MethodNotSupported」狀態 `x-amz-delete-marker` 回應標頭設定為 `true`。
標頭物件	"標頭物件"
POST物件還原	"POST物件還原"
放置物件	"放置物件"
放置物件-複製	"放置物件-複製"
將物件保留為合法	"使用 S3 REST API 來設定 S3 物件鎖定"
保留物件	"使用 S3 REST API 來設定 S3 物件鎖定"

營運	實作
放置物件標記	使用 `tagging` SubResource可將一組標記新增至現有物件。 物件標籤限制 您可以在上傳新物件時新增標記、也可以將標記新增至現有物件。每個物件最多可支援10個標記的支援功能。StorageGRID與物件相關聯的標記必須具有唯一的標記金鑰。標籤金鑰長度最多可達128個UNICODE字元、標籤值長度最多可達256個UNICODE字元。金鑰和值區分大小寫。 標記更新和擷取行為 當您使用「放置物件」標記來更新物件的標記時、StorageGRID 無法重新擷取物件。這表示不會使用相符ILM規則中指定的擷取行為選項。當ILM由正常背景ILM程序重新評估時、會對更新所觸發的物件放置位置進行任何變更。 這表示、如果 ILM 規則使用嚴格選項來擷取行為、則無法在無法進行所需物件放置時（例如、因為新要求的位置無法使用）、就不會採取任何行動。更新後的物件會保留其目前的放置位置、直到能夠放置所需的位置為止。 解決衝突 相互衝突的用戶端要求（例如兩個寫入同一個金鑰的用戶端）會以「最新致勝」的方式解決。「最新致勝」評估的時間、是根據StorageGRID 下列條件而定：當系統完成特定要求時、S3用戶端開始作業時、不會開啟。 版本管理 如果是 `versionId` 查詢參數未在要求中指定、該作業會將標記新增至版本控制儲存區中物件的最新版本。如果物件的目前版本是刪除標記、則會傳回「MethodNotSupported」狀態 `x-amz-delete-marker` 回應標頭設定為 `true`。
選取物件內容	"選取物件內容"

相關資訊

"在稽核記錄中追蹤S3作業"

使用S3 Select

StorageGRID 支援下列的 Amazon S3 Select 子句、資料類型和運算子 "SelectObjectContent命令"。

不支援任何未列出的項目。

如需語法、請參閱 "選取物件內容"。如需S3 Select的詳細資訊、請參閱 "S3 Select的AWS文件"。

只有啟用S3 Select的租戶帳戶才能發出SelectObjectContent查詢。請參閱 "使用S3 Select的考量與要求"。

條款

- 選取清單
- from子句
- where子句
- 限制條款

資料類型

- 布爾
- 整數
- 字串
- 浮動
- 十進位、數字
- 時間戳記

運算子

邏輯運算子

- 和
- 不是
- 或

比較運算子

- <
- >
- &l;=
- >=
- =
- =
- <>
- ！=
- 兩者之間
- 在中

模式比對運算子

- 喜歡
- _
- %

單一運算子

- 為空值
- 不是空值

數學運算子

- +
- -
- *
- /
- %

StorageGRID 遵循 Amazon S3 Select 運算子的優先順序。

Aggregate函數

- 平均（）
- 計數（*）
- 最大（）
- 最小（）
- 總計（）

條件式函數

- 案例
- 合併
- NULLIF

轉換功能

- CAST（適用於支援的資料類型）

日期函數

- 日期新增
- 日期_差異
- 擷取
- 至字串
- 目標時間戳記
- UTCNOW

字串函數

- char_length、字元長度
- 降低
- 子字串
- 修剪
- 上

使用伺服器端加密

伺服器端加密可讓您保護閒置的物件資料。當資料寫入物件時、系統會加密資料、並在您存取物件時解密資料。StorageGRID

如果您想要使用伺服器端加密、您可以根據加密金鑰的管理方式、選擇兩個互不相容的選項之一：

- * SSE（使用StorageGRID管理金鑰的伺服器端加密）*：當您發出S3要求以儲存物件時StorageGRID 、用唯一的金鑰來加密物件。當您發出S3要求以擷取物件時StorageGRID 、則會使用儲存的金鑰來解密物件。
- * SSE-C（使用客戶提供的金鑰進行伺服器端加密）*：當您發出S3要求以儲存物件時、您會提供自己的加密金鑰。擷取物件時、您提供的加密金鑰與要求的一部分相同。如果兩個加密金鑰相符、則會解密物件並傳回物件資料。

  雖然此功能可管理所有物件加密與解密作業、但您必須管理所提供的加密金鑰。StorageGRID

  您提供的加密金鑰永遠不會儲存。如果您遺失加密金鑰、就會遺失對應的物件。

  如果物件是以SSE或SSE-C加密、則會忽略任何儲存區層級或網格層級的加密設定。

使用**SS**

若要使用StorageGRID 由支援此功能的唯一金鑰來加密物件、請使用下列要求標頭：

```
x-amz-server-side-encryption
```

下列物件作業可支援SSe要求標頭：

- "放置物件"
- "放置物件-複製"
- "啟動多部份上傳"

使用**SSE-C**

若要使用您管理的唯一金鑰來加密物件、請使用三個要求標頭：

要求標頭	說明
`x-amz-server-side-encryption-customer-algorithm`	指定加密演算法。標頭值必須是 `AES256`。
`x-amz-server-side-encryption-customer-key`	指定將用於加密或解密物件的加密金鑰。金鑰的值必須是256位元、已編碼的base64。
`x-amz-server-side-encryption-customer-key-MD5`	根據RFC 1321指定加密金鑰的md5摘要、以確保傳輸加密金鑰時不會發生錯誤。md5摘要的值必須是以64編碼的128位元。

下列物件作業可支援SSE-C要求標頭：

- "取得物件"
- "標頭物件"
- "放置物件"
- "放置物件-複製"
- "啟動多部份上傳"
- "上傳零件"
- "上傳零件-複製"

使用伺服器端加密搭配客戶提供的金鑰（**SSE-C**）時的考量

使用SSE-C之前、請注意下列考量事項：

- 您必須使用https。

> 使用SSE-C時、不接受透過http提出的任何要求StorageGRID基於安全考量、您應該考慮使用http意外傳送的任何金鑰是否會遭到入侵。捨棄按鍵、然後視需要旋轉。

- 回應中的ETag不是物件資料的MD5。
- 您必須管理加密金鑰與物件之間的對應關係。不儲存加密金鑰。StorageGRID您必須負責追蹤為每個物件提供的加密金鑰。
- 如果您的儲存區已啟用版本管理功能、則每個物件版本都應該擁有自己的加密金鑰。您負責追蹤每個物件版本所使用的加密金鑰。
- 由於您管理用戶端的加密金鑰、因此也必須管理用戶端上的任何其他安全防護措施、例如金鑰輪替。

> 您提供的加密金鑰永遠不會儲存。如果您遺失加密金鑰、就會遺失對應的物件。

- 如果為貯體設定了跨網格複寫或 CloudMirror 複寫、您就無法擷取 SSE-C 物件。擷取作業將會失敗。

相關資訊

"Amazon S3開發人員指南：使用客戶提供的加密金鑰（SSE-C）、使用伺服器端加密來保護資料"

取得物件

您可以使用S3取得物件要求、從S3儲存區擷取物件。

取得物件和多個部分物件

您可以使用 `partNumber` 要求參數以擷取多部分或分割物件的特定部分。。 `x-amz-mp-parts-count` 回應元素指出物件有多少部分。

您可以設定 `partNumber` 對於分割 / 多個零件物件和非分割 / 非多個零件物件、則為 1 ；不過、 `x-amz-mp-parts-count` 只會針對分割或多個零件物件傳回回應元素。

使用者中繼資料中的**UTF-8**字元

在使用者定義的中繼資料中、無法剖析或解譯轉義的utf-8字元。StorageGRID取得使用者定義中繼資料中含有轉義式 UTF-8 字元的物件要求、並不會傳回 `x-amz-missing-meta` 如果金鑰名稱或值包含不可列印的字元、則為標頭。

不支援的要求標頭

不支援並傳回下列要求標頭 `XNotImplemented`：

- `x-amz-website-redirect-location`

版本管理

如果是 `versionId` 未指定SubResource、此作業會擷取版本控制儲存區中最新版本的物件。如果物件的目前版本是刪除標記、則會傳回「未找到」狀態 `x-amz-delete-marker` 回應標頭設定為 `true`。

使用客戶提供的加密金鑰（**SSE-C**）要求伺服器端加密標頭

如果物件是以您提供的唯一金鑰加密、請使用所有三個標頭。

- `x-amz-server-side-encryption-customer-algorithm`：指定 `AES256`。
- `x-amz-server-side-encryption-customer-key`：指定物件的加密金鑰。
- `x-amz-server-side-encryption-customer-key-MD5`：指定對象加密密鑰的md5摘要。

> 您提供的加密金鑰永遠不會儲存。如果您遺失加密金鑰、就會遺失對應的物件。在使用客戶提供的金鑰來保護物件資料之前、請先檢閱中的考量事項 "使用伺服器端加密"。

取得雲端儲存池物件的行為

如果物件已儲存在中 "雲端儲存資源池"、「取得物件」要求的行為取決於物件的狀態。請參閱 "標頭物件" 以取得更多詳細資料。

> 如果物件儲存在雲端儲存資源池中、而且網格上也有一個或多個物件複本、則「Get Object（取得物件）」要求會先嘗試從網格擷取資料、然後再從雲端儲存資源池擷取資料。

物件狀態	**Get**物件的行為
物件擷取到StorageGRID 不經ILM評估、或儲存在傳統儲存資源池中的物件、或使用銷毀編碼	`200 OK` 系統會擷取物件複本。
Cloud Storage Pool中的物件、但尚未轉換為無法擷取的狀態	`200 OK` 系統會擷取物件複本。
物件移轉至無法擷取的狀態	`403 Forbidden、 InvalidObjectState` 使用 "POST物件還原" 要求將物件還原至可擷取狀態。
正在從無法擷取的狀態還原的物件	`403 Forbidden、 InvalidObjectState` 等待POST物件還原要求完成。
物件已完全還原至雲端儲存資源池	`200 OK` 系統會擷取物件複本。

雲端儲存資源池中的多部份或分段物件

如果您上傳了多個部分的物件、或StorageGRID 是將一個大型物件分割成多個區段、StorageGRID 則透過取樣物件的一部分或區段、決定該物件是否可在Cloud Storage Pool中使用。在某些情況下、可能會錯誤傳回「Get物件」要求 `200 OK` 當物件的某些部分已轉換為無法擷取的狀態、或物件的某些部分尚未還原時。

在這些情況下：

- Get Object要求可能會傳回部分資料、但會在傳輸中途停止。
- 隨後可能會傳回「Get Object」（取得物件）要求 `403 Forbidden`。

取得物件和跨網格複寫

如果您使用 "網格同盟" 和 "跨網格複寫" 已啟用貯體、 S3 用戶端可藉由發出「 Get Object 」（取得物件）要求來驗證物件的複寫狀態。回應包括 StorageGRID 專屬 `x-ntap-sg-cgr-replication-status` 回應標頭會有下列其中一個值：

網格	複寫狀態
來源	• * 成功 * ：複寫成功。 • * 擱置 * ：物件尚未複寫。 • * 失敗 * ：複寫失敗且持續失敗。使用者必須解決此錯誤。
目的地	• 複本 * ：物件已從來源網格複寫。

不支援StorageGRID `x-amz-replication-status` 標頭。

相關資訊

"在稽核記錄中追蹤S3作業"

標頭物件

您可以使用S3頭物件要求從物件擷取中繼資料、而不傳回物件本身。如果物件儲存在Cloud Storage Pool中、您可以使用「標頭物件」來判斷物件的轉換狀態。

標頭物件和多個部分物件

您可以使用 `partNumber` 要求參數以擷取多部分或分割物件特定部分的中繼資料。。 `x-amz-mp-parts-count` 回應元素指出物件有多少部分。

您可以設定 `partNumber` 對於分割 / 多個零件物件和非分割 / 非多個零件物件、則為 1 ；不過、 `x-amz-mp-parts-count` 只會針對分割或多個零件物件傳回回應元素。

使用者中繼資料中的**UTF-8**字元

在使用者定義的中繼資料中、無法剖析或解譯轉義的utf-8字元。StorageGRID使用者定義中繼資料中的轉義式 UTF-8 字元物件的標頭要求不會傳回 `x-amz-missing-meta` 如果金鑰名稱或值包含不可列印的字元、則為標頭。

不支援的要求標頭

不支援並傳回下列要求標頭 `XNotImplemented`：

- `x-amz-website-redirect-location`

版本管理

如果是 `versionId` 未指定SubResource、此作業會擷取版本控制儲存區中最新版本的物件。如果物件的目前版本是刪除標記、則會傳回「未找到」狀態 `x-amz-delete-marker` 回應標頭設定為 `true`。

使用客戶提供的加密金鑰（**SSE-C**）要求伺服器端加密標頭

如果物件使用您提供的唯一金鑰加密、請使用這三個標頭。

- `x-amz-server-side-encryption-customer-algorithm`：指定 `AES256`。
- `x-amz-server-side-encryption-customer-key`：指定物件的加密金鑰。
- `x-amz-server-side-encryption-customer-key-MD5`：指定對象加密密鑰的md5摘要。

您提供的加密金鑰永遠不會儲存。如果您遺失加密金鑰、就會遺失對應的物件。在使用客戶提供的金鑰來保護物件資料之前、請先檢閱中的考量事項 "使用伺服器端加密"。

Cloud Storage Pool 物件的 head 物件回應

如果物件儲存在中 "雲端儲存資源池"，會傳回下列回應標頭：

- `x-amz-storage-class: GLACIER`
- `x-amz-restore`

回應標頭會提供物件移至雲端儲存集區時的狀態資訊、並選擇性地移轉至無法擷取的狀態、然後還原。

物件狀態	回應標頭物件
物件擷取到StorageGRID 不經ILM評估、或儲存在傳統儲存資源池中的物件、或使用銷毀編碼	`200 OK` （未傳回特殊回應標頭。）

Cloud Storage Pool中的物件、但尚未轉換為無法擷取的狀態	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	在物件轉換為無法擷取的狀態之前、其值為 `expiry-date` 設定為未來的某段時間。確切的轉換時間不受StorageGRID 此功能的控制。

物件已轉換為無法擷取的狀態、但網格上至少也有一個複本	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	的價值 `expiry-date` 設定為未來的某段時間。
	
	• 注意 * ：如果網格上的複本不可用（例如、儲存節點停機）、您必須發出 "POST物件還原" 要求從雲端儲存池還原複本、然後才能成功擷取物件。

物件移轉至無法擷取的狀態、而且網格上不存在複本	`200 OK`
	
	`x-amz-storage-class: GLACIER`

正在從無法擷取的狀態還原的物件	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="true"`

物件狀態	回應標頭物件

物件已完全還原至雲端儲存資源池	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT"`
	
	。 `expiry-date` 指出Cloud Storage Pool中的物件何時會傳回無法擷取的狀態。

Cloud Storage Pool中的多部份或分段物件

如果您上傳了多個部分的物件、或StorageGRID 是將一個大型物件分割成多個區段、StorageGRID 則透過取樣物件的一部分或區段、決定該物件是否可在Cloud Storage Pool中使用。在某些情況下、可能會錯誤傳回物件要求 `x-amz-restore: ongoing-request="false"` 當物件的某些部分已轉換為無法擷取的狀態、或物件的某些部分尚未還原時。

標頭物件和跨網格複寫

如果您使用 "網格同盟" 和 "跨網格複寫" 已啟用貯體、 S3 用戶端可透過發出 head Object 要求來驗證物件的複寫狀態。回應包括 StorageGRID 專屬 `x-ntap-sg-cgr-replication-status` 回應標頭會有下列其中一個值：

網格	複寫狀態
來源	• * 成功 * ：複寫成功。 • * 擱置 * ：物件尚未複寫。 • * 失敗 * ：複寫失敗且持續失敗。使用者必須解決此錯誤。
目的地	• 複本 * ：物件已從來源網格複寫。

不支援StorageGRID `x-amz-replication-status` 標頭。

相關資訊

"在稽核記錄中追蹤S3作業"

POST物件還原

您可以使用S3 POST物件還原要求來還原儲存在雲端儲存池中的物件。

支援的要求類型

僅支援POST物件還原要求以還原物件。StorageGRID它不支援 `SELECT` 還原類型。選取「要求傳回」 `XNotImplemented`。

版本管理

或者、請指定 `versionId` 還原版本化儲存區中物件的特定版本。如果您沒有指定 `versionId`，則會還原物件的最新版本

在**Cloud Storage Pool**物件上進行物件後還原的行為

如果物件儲存在Cloud Storage Pool中（請參閱使用資訊生命週期管理來管理物件的指示）、則根據物件的狀態、POST物件還原要求會出現下列行為。如需詳細資訊、請參閱「標頭物件」。

> 如果物件儲存在雲端儲存資源池中、而且網格上也存在物件的一或多個複本、就不需要發出物件後還原要求來還原物件。相反地、您可以使用「取得物件」要求、直接擷取本機複本。

物件狀態	**POST**物件還原的行為
物件擷取至StorageGRID 不受ILM評估、或物件不在雲端儲存資源池中	`403 Forbidden`、 `InvalidObjectState`
Cloud Storage Pool中的物件、但尚未轉換為無法擷取的狀態	`200 OK` 不會進行任何變更。 • 注意 * ：在物件轉換為不可擷取的狀態之前、您無法變更物件 `expiry-date`。
物件移轉至無法擷取的狀態	`202 Accepted` 將物件的可擷取複本還原至Cloud Storage Pool、直到要求本文指定的天數。在此期間結束時、物件會返回無法擷取的狀態。 您也可以選擇使用 `Tier` 要求元素以決定還原工作完成所需的時間（`Expedited`、 `Standard`或 `Bulk`）。如果您沒有指定 `Tier`、 `Standard` 使用階層。 • 重要 * ：如果物件已移轉至 S3 Glacier Deep Archive 、或雲端儲存池使用 Azure Blob 儲存設備、則無法使用還原 `Expedited` 層級。傳回下列錯誤 `403 Forbidden`、 `InvalidTier`： `Retrieval option is not supported by this storage class`。
正在從無法擷取的狀態還原的物件	`409 Conflict`、 `RestoreAlreadyInProgress`
物件已完全還原至雲端儲存資源池	`200 OK` *附註：*如果物件已還原為可擷取的狀態、您可以變更物件 `expiry-date` 以新的值重新發出POST物件還原要求 `Days`。還原日期會根據申請時間而更新。

相關資訊

"使用ILM管理物件"

"標頭物件"

"在稽核記錄中追蹤S3作業"

放置物件

您可以使用S3放置物件要求、將物件新增至儲存區。

解決衝突

衝突的用戶端要求（例如兩個寫入同一個金鑰的用戶端）會以「最新致勝」的方式解決。「最新致勝」評估的時間取決於StorageGRID 何時由VMware系統完成指定的要求、而非S3用戶端開始作業的時間。

物件大小

單一放置物件作業的最大_Recommended大小為5 GiB（5、368、709、120位元組）。如果您的物件大於5 GiB、請改用多部份上傳。

單一放置物件作業的最大 _ 支援 _ 大小為 5 TiB （ 5 、 497 、 558 、 138 、 880 位元組）。但是、如果您嘗試上傳超過5 GiB的物件、則會觸發* S3「Pure Object size too large （將物件大小設為太大）」警示。

使用者中繼資料大小

Amazon S3會將每個PUT要求標頭內使用者定義的中繼資料大小限制為2 KB。支援範圍將使用者中繼資料限制為24 KiB。StorageGRID使用者定義的中繼資料大小是以每個金鑰和值的utf-8編碼方式、計算出位元組數的總和。

使用者中繼資料中的**UTF-8**字元

如果要求在使用者定義的中繼資料金鑰名稱或值中包含（未轉義）utf-8值、StorageGRID 則無法定義任何不正常的行為。

不剖析或解譯使用者定義之中繼資料的金鑰名稱或值中包含的轉義式utf-8字元。StorageGRID轉義的UTF-8字元會視為Ascii字元：

- 如果使用者定義的中繼資料包含轉義的UTF-8字元、則放置、放置物件複製、取得和標頭要求都會成功。
- 無法歸還StorageGRID `x-amz-missing-meta` 標頭：金鑰名稱或值的解譯值包含不可列印的字元。

物件標籤限制

您可以在上傳新物件時新增標記、也可以將標記新增至現有物件。每個物件最多可支援10個標記的支援功能。StorageGRID與物件相關聯的標記必須具有唯一的標記金鑰。標籤金鑰長度最多可達128個UNICODE字元、標籤值長度最多可達256個UNICODE字元。金鑰和值區分大小寫。

物件擁有權

在功能區中StorageGRID 、所有物件均歸庫位擁有者帳戶所有、包括非擁有者帳戶或匿名使用者所建立的物件。

支援的要求標頭

支援下列要求標頭：

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`

  當您指定時 `aws-chunked` 適用於 `Content-Encoding`無法驗證下列項目StorageGRID ：

  - 無法驗證StorageGRID `chunk-signature` 根據區塊資料。
  - 無法驗證您提供的價值StorageGRID `x-amz-decoded-content-length` 針對物件。
- `Content-Language`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Expires`
- `Transfer-Encoding`

  如果支援Chunked傳輸編碼 `aws-chunked` 也會使用有效負載簽署。
- `x-amz-meta-`，然後是包含使用者定義中繼資料的名稱值配對。

  為使用者定義的中繼資料指定名稱值配對時、請使用以下一般格式：

  ```
  x-amz-meta-name: value
  ```

  如果您要使用 * 使用者定義的建立時間 * 選項做為 ILM 規則的參考時間、則必須使用 `creation-time` 做為建立物件時記錄的中繼資料名稱。例如：

  ```
  x-amz-meta-creation-time: 1443399726
  ```

  的價值 `creation-time` 自1970年1月1日起算為秒數。

  > ILM 規則不能同時使用 * 使用者定義的建立時間 * 作為參考時間、也不能同時使用「擷取」行為的平衡或嚴格選項。建立ILM規則時會傳回錯誤。
- `x-amz-tagging`
- S3物件鎖定要求標頭
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    如果要求是在沒有這些標頭的情況下提出、則貯體預設保留設定會用於計算物件版本模式並保留至最新日期。請參閱 "使用 S3 REST API 來設定 S3 物件鎖定"。

- SSe要求標頭：
  - x-amz-server-side-encryption
  - x-amz-server-side-encryption-customer-key-MD5
  - x-amz-server-side-encryption-customer-key
  - x-amz-server-side-encryption-customer-algorithm

    請參閱 [要求伺服器端加密的標頭]

不支援的要求標頭

不支援下列要求標頭：

- 。 x-amz-acl 不支援要求標頭。
- 。 x-amz-website-redirect-location 不支援要求標頭並傳回 XNotImplemented。

儲存類別選項

。 x-amz-storage-class 支援要求標頭。提交的值 x-amz-storage-class 影響StorageGRID 到在擷取期間、如何保護物件資料、而非StorageGRID 物件的持續複本儲存在整個系統（由ILM決定）中。

如果符合擷取物件的ILM規則使用「擷取行為」的「嚴格」選項、則會使用 x-amz-storage-class 標頭沒有作用。

下列值可用於 x-amz-storage-class：

- STANDARD （預設）
  - 雙重提交：如果ILM規則指定「內嵌行為」的「雙重提交」選項、則只要物件擷取到另一個物件複本、就會建立該物件的第二個複本、並將其分散到不同的儲存節點（雙重提交）。評估 ILM 時、 StorageGRID 會判斷這些初始過渡複本是否符合規則中的放置指示。如果沒有、則可能需要在不同位置製作新的物件複本、而且可能需要刪除初始過渡複本。
  - *Balanced * ：如果 ILM 規則指定 Balanced 選項、而 StorageGRID 無法立即製作規則中指定的所有複本、 StorageGRID 會在不同的儲存節點上製作兩個臨時複本。

    如果StorageGRID 能夠立即建立ILM規則中指定的所有物件複本（同步放置） x-amz-storage-class 標頭沒有作用。
- REDUCED_REDUNDANCY
  - 雙重提交：如果ILM規則指定擷取行為的雙重提交選項、StorageGRID 則會在擷取物件時建立單一的過渡複本（單一提交）。
  - *Balanced * ：如果 ILM 規則指定 Balanced 選項、則 StorageGRID 只會在系統無法立即製作規則中指定的所有複本時、才製作單一的臨時複本。如果能夠執行同步放置、則此標頭不會有任何影響。StorageGRID。 REDUCED_REDUNDANCY 當符合物件的ILM規則建立單一複寫複本時、最適合使用此選項。在此案例中、請使用 REDUCED_REDUNDANCY 免除在每次擷取作業中不必要地建立和刪除額外的物件複本。

  使用 REDUCED_REDUNDANCY 在其他情況下不建議使用此選項。 REDUCED_REDUNDANCY 增加擷取期間物件資料遺失的風險。例如、如果單一複本一開始儲存在無法進行ILM評估的儲存節點上、則可能會遺失資

料。

> 在任何時間段只複寫一個複本、會使資料面臨永久遺失的風險。如果只有一個物件複寫複本存在、則當儲存節點故障或發生重大錯誤時、該物件就會遺失。在升級等維護程序期間、您也會暫時失去物件的存取權。

指定 `REDUCED_REDUNDANCY` 只會影響第一次擷取物件時所建立的複本數量。它不會影響使用中ILM原則評估物件時所製作的物件複本數量、也不會導致資料儲存在StorageGRID 較低層級的資料冗餘環境中。

> 如果您將物件擷取至啟用S3物件鎖定的儲存區、則會顯示 `REDUCED_REDUNDANCY` 選項會被忽略。如果您要將物件擷取至舊版相容的儲存區、請使用 `REDUCED_REDUNDANCY` 選項會傳回錯誤。執行「雙重承諾」的程序時、務必確保符合法規遵循要求。StorageGRID

要求伺服器端加密的標頭

您可以使用下列要求標頭、以伺服器端加密來加密物件。「SSE」和「SSE-C」選項互不相關。

- * SSE-*：如果您想使用StorageGRID 由支援的唯一金鑰來加密物件、請使用下列標頭。
  - `x-amz-server-side-encryption`
- * SSE-C*：如果您想使用您提供及管理的唯一金鑰來加密物件、請使用這三個標頭。
  - `x-amz-server-side-encryption-customer-algorithm`：指定 `AES256`。
  - `x-amz-server-side-encryption-customer-key`：指定新物件的加密金鑰。
  - `x-amz-server-side-encryption-customer-key-MD5`：指定新對象加密密鑰的md5摘要。

> 您提供的加密金鑰永遠不會儲存。如果您遺失加密金鑰、就會遺失對應的物件。在使用客戶提供的金鑰來保護物件資料之前、請先檢閱的考量事項 "使用伺服器端加密"。

> 如果物件是以SSE或SSE-C加密、則會忽略任何儲存區層級或網格層級的加密設定。

版本管理

如果已啟用儲存區的版本管理功能、則為唯一的 `versionId` 會針對儲存的物件版本自動產生。這 `versionId` 也會使用傳回回應 `x-amz-version-id` 回應標頭：

如果版本控制暫停、則物件版本會以null儲存 `versionId` 如果空版本已經存在、則會覆寫。

授權標頭的簽名計算

使用時 `Authorization` 用於驗證要求的標頭、 StorageGRID 與 AWS 有下列不同：

- StorageGRID 不需要 `host` 要包含的標頭 `CanonicalHeaders`。
- StorageGRID 不需要 `Content-Type` 包括在內 `CanonicalHeaders`。
- StorageGRID 不需要 `x-amz-*` 要包含的標頭 `CanonicalHeaders`。

一般最佳實務做法是一律將這些標頭包含在內 `CanonicalHeaders` 為了確保這些標頭已通過驗證、但如果您排除這些標頭、 StorageGRID 不會傳回錯誤。

如需詳細資訊、請參閱 "授權標頭的簽名計算：在單一區塊中傳輸有效負載（ AWS 簽名版本 4 ）"。

相關資訊

"使用ILM管理物件"

"在貯體上作業"

"在稽核記錄中追蹤S3作業"

"如何設定用戶端連線"

放置物件-複製

您可以使用「S3放置物件-複製」要求來建立S3中已儲存物件的複本。「放置物件」-「複製」作業與執行「取得」和「放置」相同。

解決衝突

衝突的用戶端要求（例如兩個寫入同一個金鑰的用戶端）會以「最新致勝」的方式解決。「最新致勝」評估的時間取決於StorageGRID 何時由VMware系統完成指定的要求、而非S3用戶端開始作業的時間。

物件大小

單一放置物件作業的最大_Recommended大小為5 GiB（5、368、709、120位元組）。如果您的物件大於5 GiB、請改用多部份上傳。

單一放置物件作業的最大 _ 支援 _ 大小為 5 TiB （ 5 、 497 、 558 、 138 、 880 位元組）。但是、如果您嘗試上傳超過5 GiB的物件、則會觸發* S3「Pure Object size too large （將物件大小設為太大）」警示。

使用者中繼資料中的**UTF-8**字元

如果要求在使用者定義的中繼資料金鑰名稱或值中包含（未轉義）utf-8值、StorageGRID 則無法定義任何不正常的行為。

不剖析或解譯使用者定義之中繼資料的金鑰名稱或值中包含的轉義式utf-8字元。StorageGRID轉義的UTF-8字元會視為Ascii字元：

- 如果使用者定義的中繼資料包含轉義的utf-8字元、則要求會成功。
- 無法歸還StorageGRID `x-amz-missing-meta` 標頭：金鑰名稱或值的解譯值包含不可列印的字元。

支援的要求標頭

支援下列要求標頭：

- `Content-Type`
- `x-amz-copy-source`

- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`
- `x-amz-meta-`，然後是包含使用者定義中繼資料的名稱值配對
- `x-amz-metadata-directive`：預設值為 `COPY`可讓您複製物件及相關的中繼資料。

  您可以指定 `REPLACE` 可在複製物件時覆寫現有的中繼資料、或更新物件中繼資料。

- `x-amz-storage-class`
- `x-amz-tagging-directive`：預設值為 `COPY`可讓您複製物件和所有標記。

  您可以指定 `REPLACE` 覆寫複製物件時的現有標記、或更新標記。

- S3物件鎖定要求標頭：
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    如果要求是在沒有這些標頭的情況下提出、則貯體預設保留設定會用於計算物件版本模式並保留至最新日期。請參閱 "使用 S3 REST API 來設定 S3 物件鎖定"。

- SSe要求標頭：
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`
  - `x-amz-copy-source-server-side-encryption-customer-key`
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    請參閱 [要求伺服器端加密的標頭]

不支援的要求標頭

不支援下列要求標頭：

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`

- `Expires`
- `x-amz-website-redirect-location`

儲存類別選項

。 `x-amz-storage-class` 如果StorageGRID 相符的ILM規則指定「雙重認可」或「平衡」的擷取行為、則會支援要求標頭、並影響到所建立的物件複本數量。

- `STANDARD`

  （預設）當ILM規則使用雙重提交選項、或平衡選項回到建立臨時複本時、指定雙重提交擷取作業。

- `REDUCED_REDUNDANCY`

  當ILM規則使用雙重提交選項、或平衡選項回到建立過渡複本時、指定單一提交擷取作業。

> 如果您將物件擷取至啟用S3物件鎖定的儲存區、則會顯示 `REDUCED_REDUNDANCY` 選項會被忽略。如果您要將物件擷取至舊版相容的儲存區、請使用 `REDUCED_REDUNDANCY` 選項會傳回錯誤。執行「雙重承諾」的程序時、務必確保符合法規遵循要求。StorageGRID

在「放置物件**-**複製」中使用**x-amz-copy-**來源

如果來源儲存區和金鑰、請在中指定 `x-amz-copy-source` 標頭與目的地桶和金鑰不同、來源物件資料的複本會寫入目的地。

如果來源和目的地相符、則會顯示和 `x-amz-metadata-directive` 標頭指定為 `REPLACE`、會以要求中提供的中繼資料值來更新物件的中繼資料。在這種情況StorageGRID 下、無法重新擷取物件。這有兩個重要後果：

- 您無法使用「放置物件 - 複製」來加密現有的物件、或變更現有物件的加密。如果您提供 `x-amz-server-side-encryption` 標頭或 `x-amz-server-side-encryption-customer-algorithm` 標頭StorageGRID 、不接受要求並退貨 `XNotImplemented`。
- 不會使用相符ILM規則中指定的擷取行為選項。當ILM由正常背景ILM程序重新評估時、會對更新所觸發的物件放置位置進行任何變更。

  這表示、如果 ILM 規則使用嚴格選項來擷取行為、則無法在無法進行所需物件放置時（例如、因為新要求的位置無法使用）、就不會採取任何行動。更新後的物件會保留其目前的放置位置、直到能夠放置所需的位置為止。

要求伺服器端加密的標頭

如果您使用伺服器端加密、所提供的要求標頭取決於來源物件是否加密、以及您是否打算加密目標物件。

- 如果來源物件是使用客戶提供的金鑰（SSE-C）加密、您必須在「放置物件-複製」要求中包含下列三個標頭、以便解密物件、然後複製：
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`：指定 `AES256`。
  - `x-amz-copy-source-server-side-encryption-customer-key`：指定在創建源對象時提供的加密密鑰。
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`：指定在創建源對象時提

供的md5摘要。

- 如果您要使用您提供及管理的唯一金鑰來加密目標物件（複本）、請包含下列三個標頭：
  - `x-amz-server-side-encryption-customer-algorithm`：指定 `AES256`。
  - `x-amz-server-side-encryption-customer-key`：指定目標物件的新加密金鑰。
  - `x-amz-server-side-encryption-customer-key-MD5`：指定新加密金鑰的md5摘要。

> 您提供的加密金鑰永遠不會儲存。如果您遺失加密金鑰、就會遺失對應的物件。在使用客戶提供的金鑰來保護物件資料之前、請先檢閱的考量事項 "使用伺服器端加密"。

- 如果您想要使用StorageGRID 由支援對象（複本）的獨特金鑰來加密目標物件（複本）、請在「放置物件-複製」要求中加入此標頭：
  - `x-amz-server-side-encryption`

> `server-side-encryption` 物件的值無法更新。改用新的複本 `server-side-encryption` 使用價值 `x-amz-metadata-directive`： `REPLACE`。

版本管理

如果來源儲存區已版本化、您可以使用 `x-amz-copy-source` 標頭以複製物件的最新版本。若要複製物件的特定版本、您必須使用明確指定要複製的版本 `versionId` 子資源：如果目標儲存區已版本化、則會在中傳回所產生的版本 `x-amz-version-id` 回應標頭：如果目標儲存區的版本設定已暫停、則 `x-amz-version-id` 傳回「'null」值。

相關資訊

"使用ILM管理物件"

"在稽核記錄中追蹤S3作業"

"放置物件"

選取物件內容

您可以使用S3 SelectObjectContent要求、根據簡單的SQL陳述來篩選S3物件的內容。

如需詳細資訊、請參閱 "SelectObjectContent的AWS文件"。

開始之前

- 租戶帳戶具有S3 Select權限。
- 您有 `s3:GetObject` 您要查詢之物件的權限。
- 您要查詢的物件必須採用下列其中一種格式：
  - * CSV* 。可依原樣使用、也可壓縮至 GZIP 或 bzip2 歸檔。
  - * 硬地板 * 。硬地板物件的其他需求：
    - S3 Select 僅支援使用 GZIP 或 Snappy 進行柱式壓縮。S3 Select 不支援 Parquet 物件的全物件壓縮。

- S3 Select 不支援硬地板輸出。您必須將輸出格式指定為 CSV 或 JSON 。
- 最大未壓縮列群組大小為 512 MB 。
- 您必須使用物件架構中指定的資料類型。
- 您無法使用時間間隔、 JSON 、清單、時間或 UUID 邏輯類型。

- SQL運算式的最大長度為256 KB。
- 輸入或結果中的任何記錄最大長度為1個mib。

不支援使用 ScanRange 。

CSV 要求語法範例

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns="http://s3.amazonaws.com/doc/2006-03-
01/">
   <Expression>string</Expression>
   <ExpressionType>string</ExpressionType>
   <RequestProgress>
      <Enabled>boolean</Enabled>
   </RequestProgress>
   <InputSerialization>
      <CompressionType>GZIP</CompressionType>
      <CSV>
         <AllowQuotedRecordDelimiter>boolean</AllowQuotedRecordDelimiter>
         <Comments>#</Comments>
         <FieldDelimiter>\t</FieldDelimiter>
         <FileHeaderInfo>USE</FileHeaderInfo>
         <QuoteCharacter>'</QuoteCharacter>
         <QuoteEscapeCharacter>\\</QuoteEscapeCharacter>
         <RecordDelimiter>\n</RecordDelimiter>
      </CSV>
   </InputSerialization>
   <OutputSerialization>
      <CSV>
         <FieldDelimiter>string</FieldDelimiter>
         <QuoteCharacter>string</QuoteCharacter>
         <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
         <QuoteFields>string</QuoteFields>
         <RecordDelimiter>string</RecordDelimiter>
      </CSV>
   </OutputSerialization>
   <ScanRange>
      <End>long</End>
      <Start>long</Start>
   </ScanRange>
</SelectObjectContentRequest>
```

拼花地板要求語法範例

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns=http://s3.amazonaws.com/doc/2006-03-01/>
   <Expression>string</Expression>
   <ExpressionType>string</ExpressionType>
   <RequestProgress>
      <Enabled>boolean</Enabled>
   </RequestProgress>
   <InputSerialization>
      <CompressionType>GZIP</CompressionType>
      <PARQUET>
      </PARQUET>
   </InputSerialization>
   <OutputSerialization>
      <CSV>
         <FieldDelimiter>string</FieldDelimiter>
         <QuoteCharacter>string</QuoteCharacter>
         <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
         <QuoteFields>string</QuoteFields>
         <RecordDelimiter>string</RecordDelimiter>
      </CSV>
   </OutputSerialization>
   <ScanRange>
      <End>long</End>
      <Start>long</Start>
   </ScanRange>
</SelectObjectContentRequest>
```

SQL查詢範例

此查詢會取得州名、2010年人口、2015年估計人口、以及美國統計資料的變更百分比。檔案中非狀態的記錄會被忽略。

```
SELECT STNAME, CENSUS2010POP, POPESTIMATE2015, CAST((POPESTIMATE2015 -
CENSUS2010POP) AS DECIMAL) / CENSUS2010POP * 100.0 FROM S3Object WHERE
NAME = STNAME
```

要查詢的檔案前幾行： `SUB-EST2020_ALL.csv`、如下所示：

```
SUMLEV,STATE,COUNTY,PLACE,COUSUB,CONCIT,PRIMGEO_FLAG,FUNCSTAT,NAME,STNAME,
CENSUS2010POP,
ESTIMATESBASE2010,POPESTIMATE2010,POPESTIMATE2011,POPESTIMATE2012,POPESTIM
ATE2013,POPESTIMATE2014,
POPESTIMATE2015,POPESTIMATE2016,POPESTIMATE2017,POPESTIMATE2018,POPESTIMAT
E2019,POPESTIMATE042020,
POPESTIMATE2020
040,01,000,00000,00000,00000,0,A,Alabama,Alabama,4779736,4780118,4785514,4
799642,4816632,4831586,
4843737,4854803,4866824,4877989,4891628,4907965,4920706,4921532
162,01,000,00124,00000,00000,0,A,Abbeville
city,Alabama,2688,2705,2699,2694,2645,2629,2610,2602,
2587,2578,2565,2555,2555,2553
162,01,000,00460,00000,00000,0,A,Adamsville
city,Alabama,4522,4487,4481,4474,4453,4430,4399,4371,
4335,4304,4285,4254,4224,4211
162,01,000,00484,00000,00000,0,A,Addison
town,Alabama,758,754,751,750,745,744,742,734,734,728,
725,723,719,717
```

AWS-CLI 使用範例（ CSV ）

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--no-verify-ssl  --bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.csv --expression-type SQL --input-serialization '{"CSV":
{"FileHeaderInfo": "USE", "Comments": "#", "QuoteEscapeCharacter": "\"",
"RecordDelimiter": "\n", "FieldDelimiter": ",", "QuoteCharacter": "\"",
"AllowQuotedRecordDelimiter": false}, "CompressionType": "NONE"}' --output
-serialization '{"CSV": {"QuoteFields": "ASNEEDED",
"QuoteEscapeCharacter": "#", "RecordDelimiter": "\n", "FieldDelimiter":
",", "QuoteCharacter": "\""}}' --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" changes.csv
```

輸出檔案的前幾行、 `changes.csv`、如下所示：

```
Alabama,4779736,4854803,1.570526070895965802295356898372629785 4
Alaska,710231,738430,3.970398363349389142405780654463125377 5
Arizona,6392017,6832810,6.895992297892824753125656580700583243 1
Arkansas,2915918,2979732,2.188470320495981025529524492801237894 9
California,37253956,38904296,4.429972483996062055798852610444914897 1
Colorado,5029196,5454328,8.453279609703022113276157859029554624 6
```

AWS-CLI 使用範例（ Parquet ）

```
aws s3api select-object-content  -endpoint-url https://10.224.7.44:10443
--bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.parquet --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" --expression-type
'SQL' --input-serialization '{"Parquet":{}}'  --output-serialization
'{"CSV": {}}' changes.csv
```

輸出檔案的前幾行： changes .csv 、如下所示：

```
Alabama,4779736,4854803,1.5705260708959658022953568983726297854
Alaska,710231,738430,3.9703983633493891424057806544631253775
Arizona,6392017,6832810,6.8959922978928247531256565807005832431
Arkansas,2915918,2979732,2.1884703204959810255295244928012378949
California,37253956,38904296,4.4299724839960620557988526104449148971
Colorado,5029196,5454328,8.4532796097030221132761578590295546246
```

多部份上傳作業

本節說明StorageGRID 此功能如何支援多部份上傳作業。

下列條件與附註適用於所有多重部分上傳作業：

- 您不應超過1、000次同時將多個部分上傳至單一儲存庫、因為針對該儲存庫列出多個部分上傳查詢的結果可能會傳回不完整的結果。
- 針對多個零件執行AWS大小限制。StorageGRIDS3用戶端必須遵循下列準則：
  - 多部份上傳的每個部分必須介於5個mib（5、242,880位元組）和5 GiB（5、368,709,120位元組）之間。
  - 最後一部分可小於5個mib（5、242,880位元組）。
  - 一般而言、零件尺寸應盡量大。例如、對於100 GiB物件使用5 GiB的零件大小。因為每個零件都被視為唯一的物件、所以使用較大的零件大小可降低 StorageGRID 中繼資料的負荷。
  - 對於小於5 GiB的物件、請考慮改用非多部份上傳。
- 如果 ILM 規則使用平衡或嚴格的擷取行為、則會在擷取時針對多個部分物件的每個部分進行 ILM 評估、並在多個部分上傳完成時針對整個物件進行 ILM 評估。您應該瞭解這會如何影響物件和零件放置：
  - 如果在S3多部份上傳進行期間ILM發生變更、則當多部份上傳完成物件的部分時、可能無法符合目前的ILM需求。未正確放置的任何零件都會排入ILM重新評估佇列、稍後會移至正確位置。
  - 評估零件的ILM時StorageGRID 、會根據零件大小而非物件大小來篩選。這表示物件的部分可以儲存在不符合整體物件 ILM 需求的位置。例如、如果規則指定所有10 GB或更大的物件都儲存在DC1、而所有較小的物件則儲存在DC2、則在10部分多部分上傳的每1 GB擷取部分、都會儲存在DC2。當針對整個物件評估ILM時、物件的所有部分都會移至DC1。
- 所有的多部份上傳作業都支援StorageGRID 不一致的控管功能。

- 視需要、您可以使用伺服器端加密來上傳多個部分。若要使用SSe（伺服器端加密搭配StorageGRID管理金鑰）、請加入 `x-amz-server-side-encryption` 僅在「初始化多重成分上傳」要求中顯示要求標頭。若要使用SSE-C（使用客戶提供的金鑰進行伺服器端加密）、您可以在「初始化多部份上傳」要求和後續每個「上傳零件」要求中、指定相同的三個加密金鑰要求標頭。

營運	實作
列出多個部分上傳	請參閱 "列出多個部分上傳"
啟動多部份上傳	請參閱 "啟動多部份上傳"
上傳零件	請參閱 "上傳零件"
上傳零件-複製	請參閱 "上傳零件-複製"
完成多部份上傳	請參閱 "完成多部份上傳"
中止多部份上傳	以所有Amazon S3 REST API行為來實作。如有變更、恕不另行通知。
列出零件	以所有Amazon S3 REST API行為來實作。如有變更、恕不另行通知。

相關資訊

- "一致性控管"
- "使用伺服器端加密"

列出多個部分上傳

「列出多部份上傳」作業會列出某個儲存庫正在進行的多部份上傳。

支援下列要求參數：

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`
- `Host`
- `Date`
- `Authorization`

版本管理

多部分上傳包含不同的作業、可用於初始化上傳、列出上傳內容、上傳零件、組裝上傳的零件、以及完成上傳。當執行完整的「多部份上傳」作業時、即為建立物件的時間點（若適用、則為版本控制）。

啟動多部份上傳

「初始多部分上傳（ CreateMultpartUpload ）」（ CreateMultpartupload ）作業會啟動物件的多部分上傳、並傳回上傳 ID 。

。 `x-amz-storage-class` 支援要求標頭。提交的值 `x-amz-storage-class` 影響StorageGRID 到在擷取期間、如何保護物件資料、而非StorageGRID 物件的持續複本儲存在整個系統（由ILM決定）中。

如果符合擷取物件的ILM規則使用「擷取行為」的「嚴格」選項、則會使用 `x-amz-storage-class` 標頭沒有作用。

下列值可用於 `x-amz-storage-class`：

- `STANDARD` （預設）
  - 雙重提交：如果ILM規則指定「內嵌行為」的「雙重提交」選項、則只要物件擷取到另一個物件複本、就會建立該物件的第二個複本、並將其分散到不同的儲存節點（雙重提交）。評估 ILM 時、 StorageGRID 會判斷這些初始過渡複本是否符合規則中的放置指示。如果沒有、則可能需要在不同位置製作新的物件複本、而且可能需要刪除初始過渡複本。
  - *Balanced * ：如果 ILM 規則指定 Balanced 選項、而 StorageGRID 無法立即製作規則中指定的所有複本、 StorageGRID 會在不同的儲存節點上製作兩個臨時複本。

    如果StorageGRID 能夠立即建立ILM規則中指定的所有物件複本（同步放置） `x-amz-storage-class` 標頭沒有作用。

- `REDUCED_REDUNDANCY`
  - 雙重提交：如果ILM規則指定擷取行為的雙重提交選項、StorageGRID 則會在擷取物件時建立單一的過渡複本（單一提交）。
  - *Balanced * ：如果 ILM 規則指定 Balanced 選項、則 StorageGRID 只會在系統無法立即製作規則中指定的所有複本時、才製作單一的臨時複本。如果能夠執行同步放置、則此標頭不會有任何影響。StorageGRID。 `REDUCED_REDUNDANCY` 當符合物件的ILM規則建立單一複寫複本時、最適合使用此選項。在此案例中、請使用 `REDUCED_REDUNDANCY` 免除在每次擷取作業中不必要地建立和刪除額外的物件複本。

  使用 `REDUCED_REDUNDANCY` 在其他情況下不建議使用此選項。 `REDUCED_REDUNDANCY` 增加擷取期間物件資料遺失的風險。例如、如果單一複本一開始儲存在無法進行ILM評估的儲存節點上、則可能會遺失資料。

> ⓘ 在任何時間段只複寫一個複本、會使資料面臨永久遺失的風險。如果只有一個物件複寫複本存在、則當儲存節點故障或發生重大錯誤時、該物件就會遺失。在升級等維護程序期間、您也會暫時失去物件的存取權。

指定 `REDUCED_REDUNDANCY` 只會影響第一次擷取物件時所建立的複本數量。它不會影響使用中ILM原則評估物件時所製作的物件複本數量、也不會導致資料儲存在StorageGRID 較低層級的資料冗餘環境中。

如果您將物件擷取至啟用S3物件鎖定的儲存區、則會顯示 `REDUCED_REDUNDANCY` 選項會被忽略。如果您要將物件擷取至舊版相容的儲存區、請使用 `REDUCED_REDUNDANCY` 選項會傳回錯誤。執行「雙重承諾」的程序時、務必確保符合法規遵循要求。StorageGRID

支援下列要求標頭：

- `Content-Type`
- `x-amz-meta-`，然後是包含使用者定義中繼資料的名稱值配對

  為使用者定義的中繼資料指定名稱值配對時、請使用以下一般格式：

  ```
  x-amz-meta-_name_: `value`
  ```

  如果您要使用 * 使用者定義的建立時間 * 選項做為 ILM 規則的參考時間、則必須使用 `creation-time` 做為建立物件時記錄的中繼資料名稱。例如：

  ```
  x-amz-meta-creation-time: 1443399726
  ```

  的價值 `creation-time` 自1970年1月1日起算為秒數。

  新增 `creation-time` 如果您要將物件新增至已啟用舊版規範的儲存區、則不允許使用者定義的中繼資料。將傳回錯誤。

- S3物件鎖定要求標頭：
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    如果提出的要求沒有這些標頭、則會使用儲存庫預設保留設定來計算物件版本的保留日期。

  "使用 S3 REST API 來設定 S3 物件鎖定"

- SSe要求標頭：
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    [要求伺服器端加密的標頭]

    如需 StorageGRID 如何處理 UTF-8 字元的相關資訊、請參閱 Put Object 的文件。

要求伺服器端加密的標頭

您可以使用下列要求標頭、以伺服器端加密來加密多部份物件。「SSE」和「SSE-C」選項互不相關。

- * SSE-*：如果您想要使用StorageGRID 由支援的唯一金鑰來加密物件、請在「初始化多部份上傳」要求中使用下列標頭。請勿在任何上傳零件要求中指定此標頭。
  - `x-amz-server-side-encryption`
- * SSE-C*：如果您想要使用您提供及管理的唯一金鑰來加密物件、請在「初始化多部份上傳」要求（以及後續的每個「上傳零件」要求）中使用這三個標頭。
  - `x-amz-server-side-encryption-customer-algorithm`：指定 `AES256`。
  - `x-amz-server-side-encryption-customer-key`：指定新物件的加密金鑰。
  - `x-amz-server-side-encryption-customer-key-MD5`：指定新對象加密密鑰的md5摘要。

> 您提供的加密金鑰永遠不會儲存。如果您遺失加密金鑰、就會遺失對應的物件。在使用客戶提供的金鑰來保護物件資料之前、請先檢閱的考量事項 "使用伺服器端加密"。

不支援的要求標頭

不支援並傳回下列要求標頭 `XNotImplemented`

- `x-amz-website-redirect-location`

版本管理

多部分上傳包含不同的作業、可用於初始化上傳、列出上傳內容、上傳零件、組裝上傳的零件、以及完成上傳。執行完整的「多重組件上傳」作業時、會建立物件（並在適用情況下建立版本）。

相關資訊

"使用ILM管理物件"

"放置物件"

上傳零件

「上傳零件」作業會上傳物件的多部份上傳中的零件。

支援的要求標頭

支援下列要求標頭：

- `Content-Length`
- `Content-MD5`

要求伺服器端加密的標頭

如果您為「初始化多重組件上傳」要求指定SSE-C加密、則您也必須在每個「上傳零件」要求中包含下列要求標頭：

- `x-amz-server-side-encryption-customer-algorithm`：指定 `AES256`。
- `x-amz-server-side-encryption-customer-key`：指定您在「初始化多部份上傳」要求中提供的相同加密金鑰。
- `x-amz-server-side-encryption-customer-key-MD5`：指定您在「初始化多部份上傳」要求中提供的相同的MD5摘要。

> 您提供的加密金鑰永遠不會儲存。如果您遺失加密金鑰、就會遺失對應的物件。在使用客戶提供的金鑰來保護物件資料之前、請先檢閱「使用伺服器端加密」中的考量事項。

版本管理

多部分上傳包含不同的作業、可用於初始化上傳、列出上傳內容、上傳零件、組裝上傳的零件、以及完成上傳。執行完整的「多重組件上傳」作業時、會建立物件（並在適用情況下建立版本）。

相關資訊

"使用伺服器端加密"

上傳零件-複製

「上傳零件-複製」作業會將現有物件的資料複製為資料來源、藉此上傳物件的一部分。

「上傳零件-複製」作業會在所有Amazon S3 REST API行為下執行。如有變更、恕不另行通知。

此要求會讀取及寫入中指定的物件資料 `x-amz-copy-source-range` 在整個系統中StorageGRID 。

支援下列要求標頭：

- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`

要求伺服器端加密的標頭

如果您為「初始化多重成分上傳」要求指定SSE-C加密、則您也必須在每個「上傳成分-複製」要求中包含下列要求標頭：

- `x-amz-server-side-encryption-customer-algorithm`：指定 `AES256`。
- `x-amz-server-side-encryption-customer-key`：指定您在「初始化多部份上傳」要求中提供的相同加密金鑰。
- `x-amz-server-side-encryption-customer-key-MD5`：指定您在「初始化多部份上傳」要求中提供的相同的MD5摘要。

如果來源物件是使用客戶提供的金鑰（SSE-C）加密、您必須在「上傳零件-複製」要求中包含下列三個標頭、以便解密物件、然後複製：

- `x-amz-copy-source-server-side-encryption-customer-algorithm`：指定 `AES256`。

- `x-amz-copy-source-server-side-encryption-customer-key`：指定在創建源對象時提供的加密密鑰。
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`：指定在創建源對象時提供的md5摘要。

> 您提供的加密金鑰永遠不會儲存。如果您遺失加密金鑰、就會遺失對應的物件。在使用客戶提供的金鑰來保護物件資料之前、請先檢閱「使用伺服器端加密」中的考量事項。

版本管理

多部分上傳包含不同的作業、可用於初始化上傳、列出上傳內容、上傳零件、組裝上傳的零件、以及完成上傳。執行完整的「多重組件上傳」作業時、會建立物件（並在適用情況下建立版本）。

完成多部份上傳

完整的「多重零件上傳」作業會透過組裝先前上傳的零件、完成物件的多重部分上傳。

解決衝突

衝突的用戶端要求（例如兩個寫入同一個金鑰的用戶端）會以「最新致勝」的方式解決。「最新致勝」評估的時間取決於StorageGRID 何時由VMware系統完成指定的要求、而非S3用戶端開始作業的時間。

要求標頭

。 `x-amz-storage-class` 如果StorageGRID 相符的ILM規則指定「雙重認可」或「平衡」的擷取行為、則會支援要求標頭、並影響到所建立的物件複本數量。

- `STANDARD`

  （預設）當ILM規則使用雙重提交選項、或平衡選項回到建立臨時複本時、指定雙重提交擷取作業。

- `REDUCED_REDUNDANCY`

  當ILM規則使用雙重提交選項、或平衡選項回到建立過渡複本時、指定單一提交擷取作業。

> 如果您將物件擷取至啟用S3物件鎖定的儲存區、則會顯示 `REDUCED_REDUNDANCY` 選項會被忽略。如果您要將物件擷取至舊版相容的儲存區、請使用 `REDUCED_REDUNDANCY` 選項會傳回錯誤。執行「雙重承諾」的程序時、務必確保符合法規遵循要求。StorageGRID

> 如果多部分上傳未在15天內完成、則該作業會標示為非作用中、且所有相關資料都會從系統中刪除。

> 。 `ETag` 傳回的值不是資料的MD5總和、而是在的Amazon S3 API實作之後 `ETag` 多部分物件的值。

版本管理

此作業會完成多部份上傳。如果已啟用貯體的版本設定功能、則物件版本會在完成多重部分上傳後建立。

如果已啟用儲存區的版本管理功能、則為唯一的 `versionId` 會針對儲存的物件版本自動產生。這 `versionId` 也會使用傳回回應 `x-amz-version-id` 回應標頭：

如果版本控制暫停、則物件版本會以null儲存 `versionId` 如果空版本已經存在、則會覆寫。

> 當某個儲存區啟用版本管理時、完成多部份上傳會一律建立新版本、即使在同一個物件金鑰上同時完成多部份上傳也一樣。如果未針對某個儲存區啟用版本管理、則可以啟動多重部分上傳、然後在同一個物件金鑰上啟動並完成另一個多重部分上傳。在非版本的儲存區上、完成最後一次的多部分上傳優先。

複寫失敗、通知或中繼資料通知

如果平台服務已設定多重零件上傳的儲存區、即使相關的複寫或通知動作失敗、多重零件上傳仍會成功。

如果發生這種情況、則會在Grid Manager中針對Total事件（SMT）發出警示。最後一個事件訊息會針對通知失敗的最後一個物件、顯示「無法發佈Bucket名稱物件金鑰的通知」。（要查看此訊息、請選取*節點*>*儲存節點_*>*事件*。檢視表格頂端的最後一個事件。）中也會列出事件訊息 `/var/local/log/bycast-err.log`。

租戶可透過更新物件的中繼資料或標記來觸發失敗的複寫或通知。租戶可以重新提交現有的值、以避免進行不必要的變更。

相關資訊

"使用ILM管理物件"

錯誤回應

支援所有適用的標準S3 REST API錯誤回應。StorageGRID此外、此功能還會加入數個自訂回應。StorageGRID

支援的**S3 API**錯誤代碼

名稱	**HTTP**狀態
ACCESSDENIED	403禁止
《標誌摘要》	400個錯誤要求
BuckketAlreadyEx分子	衝突
BucketNotEmpty	衝突
不完整正文	400個錯誤要求
內部錯誤	500內部伺服器錯誤
InvalidAccessKeyId	403禁止

名稱	**HTTP**狀態
InvalidArgument	400個錯誤要求
InvalidBucketName	400個錯誤要求
InvalidBucketState	衝突
InvalidDigest	400個錯誤要求
InvalidEncryptionAlgorithm錯誤	400個錯誤要求
InvalidPart	400個錯誤要求
InvalidPartOrder	400個錯誤要求
InvalidRang	無法滿足416個要求的範圍
InvalidRequest	400個錯誤要求
InvalidStorageClass	400個錯誤要求
InvalidTag	400個錯誤要求
InvalidURI	400個錯誤要求
KeyTooLong	400個錯誤要求
MalformedXML	400個錯誤要求
Metadata TooLarg	400個錯誤要求
方法未允許	不允許使用405方法
內容長度	需要411長度
MissingRequestBodyError	400個錯誤要求
MISingSecurityHeader	400個錯誤要求
NoSuchBucket	找不到404
NoSuchKey	找不到404

名稱	**HTTP**狀態
NoSuchUpload	找不到404
未實作	501未實作
NoSuchBucketPolicy	找不到404
ObjectLockConfiguration未找到錯誤	找不到404
預先條件失敗	412先決條件失敗
要求時間TooSkewed	403禁止
服務無法使用	503服務無法使用
簽名DoesNotMatch	403禁止
TooManyboo	400個錯誤要求
使用者KeyMustBeSpecified	400個錯誤要求

零點自訂錯誤代碼**StorageGRID**

名稱	說明	**HTTP**狀態
XBucketLifecycleNotSupported	不允許在符合舊版規範的儲存庫中進行貯體生命週期組態	400個錯誤要求
XBucketPolicyParseException	無法剖析收到的儲存區原則Json。	400個錯誤要求
XComplianceConflict	因為舊版規範設定而拒絕作業。	403禁止
XComplianceReducedRedundancyForbidded	舊型符合標準的儲存區不允許減少備援	400個錯誤要求
XMaxBucketPolicyLengthExceed	您的原則超過允許的儲存區原則長度上限。	400個錯誤要求
XMissingInternalRequestHeader	缺少內部要求的標頭。	400個錯誤要求
XNoSuchBucketCompliance	指定的儲存庫未啟用舊版法規遵循。	找不到404
XNotAcceptable	要求包含一或多個無法滿足的Accept標頭。	無法接受的406

名稱	說明	HTTP狀態
XNotImplemed	您提供的要求暗示功能尚未實作。	501未實作

StorageGRID S3 要求

取得庫位一致性

「Get Bucket一致性」要求可讓您決定套用至特定Bucket的一致性層級。

預設的一致性控制項設定為保證新建立物件的寫入後讀取。

您有S3：GetBucketConsistency權限、或是帳戶root權限、才能完成此作業。

申請範例

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

回應

在回應XML中、 `<Consistency>` 會傳回下列其中一個值：

一致性控制	說明
全部	所有節點都會立即接收資料、否則要求將會失敗。
強大的全球化技術	保證所有站台所有用戶端要求的寫入後讀取一致性。
強式網站	保證站台內所有用戶端要求的寫入後讀取一致性。
全新寫入後讀取	（預設）為新物件提供寫入後讀取一致性、並最終確保物件更新一致。提供高可用度與資料保護保證。建議大多數情況下使用。
可用	提供新物件和物件更新的最終一致性。對於 S3 貯體、請僅視需要使用（例如、包含很少讀取的記錄值之貯體、或用於對不存在的金鑰執行 head 或 Get 作業）。S3 FabricPool 儲存區不支援。

回應範例

```
HTTP/1.1 200 OK
Date: Fri, 18 Sep 2020 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/11.5.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<Consistency xmlns="http://s3.storagegrid.com/doc/2015-02-01/">read-after-
new-write</Consistency>
```

相關資訊

"一致性控管"

實現庫位一致性

「放入庫位一致性」要求可讓您指定要套用至庫位執行作業的一致性層級。

預設的一致性控制項設定為保證新建立物件的寫入後讀取。

開始之前

您有S3：PuttBucketConsistency權限、或是帳戶root、才能完成此作業。

申請

。 `x-ntap-sg-consistency` 參數必須包含下列其中一個值：

一致性控制	說明
全部	所有節點都會立即接收資料、否則要求將會失敗。
強大的全球化技術	保證所有站台所有用戶端要求的寫入後讀取一致性。
強式網站	保證站台內所有用戶端要求的寫入後讀取一致性。
全新寫入後讀取	（預設）為新物件提供寫入後讀取一致性、並最終確保物件更新一致。提供高可用度與資料保護保證。建議大多數情況下使用。
可用	提供新物件和物件更新的最終一致性。對於 S3 貯體、請僅視需要使用（例如、包含很少讀取的記錄值之貯體、或用於對不存在的金鑰執行 head 或 Get 作業）。S3 FabricPool 儲存區不支援。

*附註：*一般而言、您應該使用「全新寫入後的讀取」一致性控制值。如果要求無法正常運作、請盡可能變更應用程式用戶端行為。或者、將用戶端設定為針對每個API要求指定一致性控制。只能將貯體層級的一致性控制設定為最後的方法。

申請範例

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

相關資訊

"一致性控管"

取得時段上次存取時間

「取得時段上次存取時間」要求可讓您決定是否為個別的時區啟用或停用上次存取時間更新。

您有S3：GetBucketLastAccessTime權限、或是帳戶root權限、才能完成此作業。

申請範例

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

回應範例

此範例顯示已針對儲存庫啟用上次存取時間更新。

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/10.3.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<LastAccessTime xmlns="http://s3.storagegrid.com/doc/2015-02-01/">enabled
</LastAccessTime>
```

將資源桶放在最後存取時間

「放置時段上次存取時間」要求可讓您針對個別的時段啟用或停用上次存取時間更新。停用上次存取時間更新可改善效能、是所有以10.3.0版或更新版本建立之儲存區的預設設

定。

您擁有儲存區的S3：PuttBucketLastAccessTime權限、或是帳戶root權限、即可完成此作業。

> 從版本10.3開始StorageGRID 、所有新的儲存庫預設都會停用上次存取時間的更新。如果您有使用StorageGRID 舊版的更新程式建立的儲存區、而且想要符合新的預設行為、則必須明確停用這些舊版儲存區的上次存取時間更新。您可以使用「浮動授權管理員」中的「放置儲存庫上次存取時間」要求、「 **S2** > * 儲存庫 * > * 變更上次存取設定 * 」核取方塊、或「浮動授權管理 API 」、來啟用或停用上次存取時間的更新。

如果某個儲存區的上次存取時間更新已停用、則會將下列行為套用至儲存區上的作業：

- 取得物件、取得物件 ACL 、取得物件標籤和頭端物件要求不會更新上次存取時間。不會將物件新增至佇列、以進行資訊生命週期管理（ILM）評估。
- 放置物件：只更新中繼資料的複製和放置物件標記要求、也會更新上次存取時間。物件會新增至佇列以進行ILM評估。
- 如果來源貯體的上次存取時間更新已停用、則「放置物件 - 複製要求」不會更新來源貯體的上次存取時間。複製的物件不會新增至來源儲存區的ILM評估佇列。但是、對於目的地、「放置物件」-「複製要求」一律會更新上次存取時間。物件複本會新增至佇列以進行ILM評估。
- 完成多重成分上傳要求更新上次存取時間。完成的物件會新增至佇列以進行ILM評估。

申請範例

此範例可讓儲存區的上次存取時間達到。

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

此範例會停用儲存區的上次存取時間。

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

相關資訊

"使用租戶帳戶"

刪除時段中繼資料通知組態

刪除庫位中繼資料通知組態要求可讓您刪除組態XML、以停用個別庫位的搜尋整合服務。

您擁有儲存區的S3：刪除BucketMetadata通知權限、或是帳戶根權限、即可完成此作業。

申請範例

此範例顯示停用區段的搜尋整合服務。

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

取得**Bucket**中繼資料通知組態

「Get Bucket中繼資料」通知組態要求可讓您擷取組態XML、以設定個別儲存區的搜尋整合。

您有S3：GetBucketMetadata通知權限、或是帳戶root、才能完成此作業。

申請範例

此要求會擷取名為的儲存區之中繼資料通知組態 `bucket`。

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

回應

回應本文包含儲存區的中繼資料通知組態。中繼資料通知組態可讓您決定儲存區的搜尋整合設定方式。也就是、它可讓您決定要建立索引的物件、以及要將物件中繼資料傳送至哪個端點。

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:_region:account-
ID_:domain/_mydomain/myindex/mytype_</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

每個中繼資料通知組態都包含一或多個規則。每個規則都會指定套用的物件、StorageGRID 以及應將物件中繼資料傳送到哪個目的地。目的地必須使用StorageGRID 不實端點的URN來指定。

名稱	說明	必要
Metadata NotifyationConfiguration	用於指定中繼資料通知物件和目的地之規則的容器標籤。 包含一或多個規則元素。	是的
規則	規則的容器標記、用於識別應將中繼資料新增至指定索引的物件。 會拒絕具有重疊前置碼的規則。 包括在Metadata NotifyationConfiguration元素中。	是的
ID	規則的唯一識別碼。 包含在Rule元素中。	否
狀態	狀態可以是「已啟用」或「已停用」。不針對停用的規則採取任何行動。 包含在Rule元素中。	是的

名稱	說明	必要
前置碼	符合前置碼的物件會受到規則影響、其中繼資料會傳送到指定的目的地。 若要符合所有物件、請指定一個空白首碼。 包含在Rule元素中。	是的
目的地	規則目的地的容器標記。 包含在Rule元素中。	是的
urn	傳送物件中繼資料的目的地之一。必須是StorageGRID 具有下列屬性的不景端點的URN： • `es` 必須是第三個元素。 • URN必須以索引結尾、並在表單中輸入中繼資料的儲存位置 `domain-name/myindex/mytype`。 端點是使用租戶管理程式或租戶管理API來設定。它們採用下列形式： • `arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` 端點必須在提交組態XML之前進行設定、否則組態將會失敗並顯示404錯誤。 目標元素中包含urn.	是的

回應範例

之間包含的XML `<MetadataNotificationConfiguration></MetadataNotificationConfiguration>` 標記顯示如何為儲存區設定與搜尋整合端點的整合。在此範例中、物件中繼資料會傳送至名為的Elasticsearch索引 `current` 並輸入named `2017` 這是以AWS網域命名的 `records`。

```
HTTP/1.1 200 OK
Date: Thu, 20 Jul 2017 18:24:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/11.0.0
x-amz-request-id: 3832973499
Content-Length: 264
Content-Type: application/xml

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix>2017</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-
1:3333333:domain/records/current/2017</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

相關資訊

"使用租戶帳戶"

放置時段中繼資料通知組態

「置入庫位元資料」通知組態要求可讓您針對個別的庫位啟用搜尋整合服務。您在要求本文中提供的中繼資料通知組態XML、會指定將中繼資料傳送至目的地搜尋索引的物件。

您擁有儲存區的S3：PuttBucketMetadata通知權限、或是帳戶根權限、即可完成此作業。

申請

要求必須在要求本文中包含中繼資料通知組態。每個中繼資料通知組態都包含一或多個規則。每個規則都會指定要套用的物件、StorageGRID 以及應將物件中繼資料傳送到哪個目的地。

物件可依物件名稱的前置詞進行篩選。例如、您可以傳送具有前置碼之物件的中繼資料 `/images` 至一個目的地、以及具有前置碼的物件 `/videos` 到另一個。

有重疊前置字元的組態無效、提交時會遭到拒絕。例如、含有前置字元物件規則的組態 `test` 和第二個規則、用於具有前置碼的物件 `test2` 不允許。

目的地必須使用StorageGRID 不實端點的URN來指定。當中繼資料通知組態已提交、或要求以失敗的方式提交時、端點必須存在 `400 Bad Request`。錯誤訊息指出： `Unable to save the metadata notification (search) policy. The specified endpoint URN does not exist: URN.`

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

下表說明中繼資料通知組態XML中的元素。

名稱	說明	必要
Metadata NotifyationConfiguration	用於指定中繼資料通知物件和目的地之規則的容器標籤。 包含一或多個規則元素。	是的
規則	規則的容器標記、用於識別應將中繼資料新增至指定索引的物件。 會拒絕具有重疊前置碼的規則。 包括在Metadata NotifyationConfiguration元素中。	是的
ID	規則的唯一識別碼。 包含在Rule元素中。	否
狀態	狀態可以是「已啟用」或「已停用」。不針對停用的規則採取任何行動。 包含在Rule元素中。	是的

名稱	說明	必要
前置碼	符合前置碼的物件會受到規則影響、其中繼資料會傳送到指定的目的地。 若要符合所有物件、請指定一個空白首碼。 包含在Rule元素中。	是的
目的地	規則目的地的容器標記。 包含在Rule元素中。	是的
urn	傳送物件中繼資料的目的地之一。必須是StorageGRID 具有下列屬性的不景端點的URN： • `es` 必須是第三個元素。 • URN必須以索引結尾、並在表單中輸入中繼資料的儲存位置 `domain-name/myindex/mytype`。 端點是使用租戶管理程式或租戶管理API來設定。它們採用下列形式： • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` 端點必須在提交組態XML之前進行設定、否則組態將會失敗並顯示404錯誤。 目標元素中包含urn.	是的

申請範例

此範例顯示啟用儲存庫的搜尋整合功能。在此範例中、所有物件的物件中繼資料都會傳送到相同的目的地。

```
PUT /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:sgws:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

在此範例中、物件的中繼資料會與前置詞相符 `/images` 會傳送至一個目的地、而物件中繼資料則會與前置詞相符 `/videos` 傳送至第二個目的地。

```
PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

由搜尋整合服務產生的**JSON**

當您啟用儲存區的搜尋整合服務時、每次新增、更新或刪除物件中繼資料或標記時、都會產生Json文件並傳送至目的地端點。

此範例顯示Json範例、該範例可在具有金鑰的物件產生時產生 `SGWS/Tagging.txt` 在名為的儲存區中建立 `test`。。 `test` 儲存區沒有版本、因此 `versionId` 標記為空白。

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1"
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

中繼資料通知中包含的物件中繼資料

此表格列出JSON文件中所有欄位、這些欄位會在啟用搜尋整合時傳送至目的地端點。

文件名稱包含儲存區名稱、物件名稱及版本ID（若有）。

類型	項目名稱	說明
儲存區和物件資訊	鏟斗	庫位名稱
儲存區和物件資訊	金鑰	物件金鑰名稱
儲存區和物件資訊	版本ID	物件版本、適用於版本控制的儲存區中的物件
儲存區和物件資訊	區域	例如、儲存區 `us-east-1`
系統中繼資料	尺寸	HTTP用戶端可見的物件大小（以位元組為單位）
系統中繼資料	md5	物件雜湊

類型	項目名稱	說明
使用者中繼資料	中繼資料 *key:value*	物件的所有使用者中繼資料、做為金鑰值配對
標記	標記 *key:value*	為物件定義的所有物件標記、做為金鑰值配對

針對標記和使用者中繼資料StorageGRID 、將日期和數字以字串或S3事件通知的形式傳送至Elasticsearch。若要設定Elasticsearch將這些字串解譯為日期或數字、請遵循Elasticsearch指示進行動態欄位對應、以及對應日期格式。您必須先在索引上啟用動態欄位對應、才能設定搜尋整合服務。建立文件索引後、您就無法編輯索引中文件的欄位類型。

相關資訊

"使用租戶帳戶"

取得儲存使用量要求

「Get Storage使用量」要求會告訴您某個帳戶所使用的總儲存容量、以及與該帳戶相關聯的每個儲存區容量。

帳戶使用的儲存容量及其儲存桶、可透過修改後的Get Service（取得服務）要求取得 `x-ntap-sg-usage` 查詢參數。儲存區的使用量會與系統處理的PUT和DELETE要求分開追蹤。使用值可能會在處理要求時延遲、使其符合預期值、尤其是系統負載過重時。

根據預設StorageGRID 、功能區會嘗試使用強大的全域一致性來擷取使用資訊。如果無法達成強大的全球一致性、 StorageGRID 會嘗試以強大的站台一致性來擷取使用資訊。

您有S3：listAllMybops權限、或是帳戶root、可以完成此作業。

申請範例

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

回應範例

此範例顯示一個帳戶、其中兩個儲存區中有四個物件和12個位元組的資料。每個儲存區包含兩個物件和六個位元組的資料。

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 00:49:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/10.2.0
x-amz-request-id: 727237123
Content-Length: 427
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<UsageResult xmlns="http://s3.storagegrid.com/doc/2015-02-01">
<CalculationTime>2014-11-19T05:30:11.000000Z</CalculationTime>
<ObjectCount>4</ObjectCount>
<DataBytes>12</DataBytes>
<Buckets>
<Bucket>
<Name>bucket1</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
<Bucket>
<Name>bucket2</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
</Buckets>
</UsageResult>
```

版本管理

儲存的每個物件版本都有助於 `ObjectCount` 和 `DataBytes` 回應中的值。刪除標記不會新增至 `ObjectCount` 總計。

相關資訊

"一致性控管"

已過時的資源桶要求、適用於舊版法規遵循

您可能需要使用StorageGRID Sfs3 REST API來管理使用舊版Compliance功能所建立的儲存區。

法規遵循功能已過時

先前版本的不支援《支援不符合要求》功能、現已由S3物件鎖定取代。StorageGRID StorageGRID

如果您先前已啟用「全域符合性」設定、StorageGRID 則會在「支援物件鎖定」中啟用「全域S3物件鎖定」設定。您不再能夠在啟用「法規遵循」的情況下建立新的儲存庫、不過、您可以視需要使用StorageGRID 「S3 REST API」來管理任何現有的符合舊規範的儲存庫。

- "使用 S3 REST API 來設定 S3 物件鎖定"
- "使用ILM管理物件"
- "NetApp知識庫：如何管理StorageGRID 支援老舊的知識庫、請參閱《知識庫文章"

過時的法規遵循要求：

- "已過時-將資源桶要求修改以符合法規要求"

  SGCompliance XML元素已過時。先前、您可以將StorageGRID 此等不必要的自訂元素納入可選的XML要求內容中、以建立符合法規的儲存庫要求。

- "已過時 - 取得 Bucket 法規遵循"

  Get Bucket法規遵循要求已過時。不過、您可以繼續使用此要求來判斷現有舊版相容儲存區目前有效的法規遵循設定。

- "已過時 - 符合 Put Bucket 規範"

  「放入時段」法規遵循要求已過時。不過、您可以繼續使用此要求來修改現有舊版相容桶的法規遵循設定。例如、您可以將現有的貯體置於合法持有狀態、或是延長保留期間。

已過時：將資源桶要求修改以符合法規要求

SGCompliance XML元素已過時。先前、您可以將StorageGRID 此等不必要的自訂元素納入可選的XML要求內容中、以建立符合法規的儲存庫要求。

> 先前版本的不支援《支援不符合要求》功能、現已由S3物件鎖定取代。StorageGRID StorageGRID

"使用 S3 REST API 來設定 S3 物件鎖定"

"使用ILM管理物件"

"NetApp知識庫：如何管理StorageGRID 支援老舊的知識庫、請參閱《知識庫文章"

您無法再建立啟用「法規遵循」的新庫位。如果您嘗試使用「置放桶」要求修改以符合法規要求、以建立新的「符合法規」桶、則會傳回下列錯誤訊息：

```
The Compliance feature is deprecated.
Contact your StorageGRID administrator if you need to create new Compliant
buckets.
```

已過時：**Get Bucket Compliance**要求

Get Bucket法規遵循要求已過時。不過、您可以繼續使用此要求來判斷現有舊版相容儲存區目前有效的法規遵循設定。

先前版本的不支援《支援不符合要求》功能、現已由S3物件鎖定取代。StorageGRID StorageGRID

"使用 S3 REST API 來設定 S3 物件鎖定"

"使用ILM管理物件"

"NetApp知識庫：如何管理StorageGRID 支援老舊的知識庫、請參閱《知識庫文章"

您有S3：GetBucketCompliance權限、或是帳戶root、可以完成此作業。

申請範例

此範例要求可讓您決定名為的儲存區的法規遵循設定 `mybucket`。

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

回應範例

在回應XML中、 `<SGCompliance>` 列出庫位有效的法規遵循設定。此回應範例顯示儲存區的法規遵循設定、其中每個物件將保留一年（525600分鐘）、從物件擷取到網格開始算起。此庫位目前沒有合法持有。每個物件將在一年後自動刪除。

```
HTTP/1.1 200 OK
Date: date
Connection: connection
Server: StorageGRID/11.1.0
x-amz-request-id: request ID
Content-Length: length
Content-Type: application/xml

<SGCompliance>
  <RetentionPeriodMinutes>525600</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

名稱	說明
RetentionPeriodMinutes	新增至此儲存區之物件的保留期間長度（以分鐘為單位）。保留期間是從物件擷取至網格時開始。

名稱	說明
LegalHold	• 是：此儲存庫目前處於合法持有狀態。除非取消合法保留、否則無法刪除此貯體中的物件、即使保留期間已過期。 • 假：此庫位目前未合法持有。此儲存區中的物件可在保留期間到期時刪除。
自動刪除	• 是：此儲存區中的物件會在保留期間到期時自動刪除、除非儲存區處於合法持有狀態。 • 否：保留期間到期時、此儲存區中的物件不會自動刪除。如果需要刪除這些物件、您必須手動刪除這些物件。

錯誤回應

如果儲存區建立不符合法規要求、則回應的HTTP狀態代碼為 `404 Not Found`的S3錯誤代碼 `XNoSuchBucketCompliance`。

已過時：提出資源桶法規遵循要求

「放入時段」法規遵循要求已過時。不過、您可以繼續使用此要求來修改現有舊版相容桶的法規遵循設定。例如、您可以將現有的貯體置於合法持有狀態、或是延長保留期間。

先前版本的不支援《支援不符合要求》功能、現已由S3物件鎖定取代。StorageGRID StorageGRID

"使用 S3 REST API 來設定 S3 物件鎖定"

"使用ILM管理物件"

"NetApp知識庫：如何管理StorageGRID 支援老舊的知識庫、請參閱《知識庫文章"

您有S3：PuttBucketCompliance權限、或是帳戶root、才能完成此作業。

在發出「放入庫位」法規遵循要求時、您必須為法規遵循設定的每個欄位指定一個值。

申請範例

此範例要求會修改名為的儲存區的規範設定 `mybucket`。在此範例中、物件位於 `mybucket` 現在將保留兩年（1、051、200分鐘）、而非一年、從物件進入網格開始算起。此庫位沒有合法持有。每個物件將在兩年後自動刪除。

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Content-Length: 152

<SGCompliance>
  <RetentionPeriodMinutes>1051200</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

名稱	說明
RetentionPeriodMinutes	新增至此儲存區之物件的保留期間長度（以分鐘為單位）。保留期間是從物件擷取至網格時開始。 • 重要 * 為 RetentionPeriodMinutes 指定新值時、您必須指定一個值、該值等於或大於該貯體目前的保留期間。設定貯體保留期間之後、您就無法減少該值、只能增加該值。
LegalHold	• 是：此儲存庫目前處於合法持有狀態。除非取消合法保留、否則無法刪除此貯體中的物件、即使保留期間已過期。 • 假：此庫位目前未合法持有。此儲存區中的物件可在保留期間到期時刪除。
自動刪除	• 是：此儲存區中的物件會在保留期間到期時自動刪除、除非儲存區處於合法持有狀態。 • 否：保留期間到期時、此儲存區中的物件不會自動刪除。如果需要刪除這些物件、您必須手動刪除這些物件。

法規遵循設定的一致性層級

當您更新S3儲存區的法規遵循設定、並提出「置放儲存區法規遵循」要求時StorageGRID 、即可嘗試更新整個網格的儲存區中繼資料。根據預設、StorageGRID 支援使用*強式全域*一致性層級、以保證所有資料中心站台及包含儲存庫中繼資料的所有儲存節點、在變更的法規遵循設定中、具有寫入後讀取一致性。

如果 StorageGRID 無法達到 * 強式全域 * 一致性層級、因為某個站台的資料中心站台或多個儲存節點無法使用、則回應的 HTTP 狀態代碼為 `503 Service Unavailable.`

如果您收到此回應、則必須聯絡網格管理員、以確保所需的儲存服務能夠儘快提供。如果網格管理員無法在每個站台上提供足夠的儲存節點、技術支援可能會強制*強站台*一致性層級、引導您重試失敗的要求。

除非您是技術支援人員的指示、而且您不瞭解使用此層級可能造成的後果、否則請勿強迫*強站台*一致性層級以符合放置桶規範。

當一致性層級降至*強站台*時StorageGRID 、更新的法規遵循設定只有在站台內的用戶端要求才具有寫入後讀取一致性。這表示StorageGRID 在所有站台和儲存節點都可用之前、此儲存區的設定可能會暫時有多個不一致的設定。不一致的設定可能會導致非預期和非預期的行為。例如、如果您將儲存庫置於合法持有之下、而強制降低一致性層級、則儲存庫先前的法規遵循設定（即合法暫停）可能會繼續在某些資料中心站台上生效。因此、您認為合法保留的物件、可能會在保留期間到期時遭到刪除、使用者或自動刪除（如果已啟用）。

若要強制使用*強站台*一致性層級、請重新發出「Put Bucket Compliance」（放入儲存庫）要求、並附上 `Consistency-Control` HTTP要求標頭、如下所示：

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

錯誤回應

- 如果儲存區建立不符合法規要求、則回應的HTTP狀態代碼為 `404 Not Found`。
- 如果 `RetentionPeriodMinutes` 在要求中、HTTP狀態代碼小於儲存區目前的保留期間 `400 Bad Request`。

相關資訊

"已過時：將資源桶要求修改以符合法規要求"

儲存庫和群組存取原則

使用貯體和群組存取原則

支援使用Amazon Web Services（AWS）原則語言、讓S3租戶能夠控制對這些儲存區內的儲存區和物件的存取。StorageGRID此系統實作S3 REST API原則語言的子集。StorageGRIDS3 API的存取原則是以Json撰寫。

存取原則總覽

支援的存取原則有兩種。StorageGRID

- 資源庫原則、使用「取得資源庫」原則設定、「放入資源庫」原則、以及刪除資源庫原則S3 API作業。庫位原則會附加至庫位、因此這些原則可設定為控制庫位擁有者帳戶或其他帳戶中的使用者對庫位及其中物件的存取。庫位原則僅適用於一個庫位、可能也適用於多個群組。
- 群組原則、使用租戶管理程式或租戶管理API進行設定。群組原則會附加至帳戶中的群組、因此這些原則會設定為允許該群組存取該帳戶所擁有的特定資源。群組原則僅適用於一個群組、可能也適用於多個儲存區。

> 群組原則和儲存庫原則之間的優先順序沒有差異。

根據Amazon定義的特定語法、執行庫位和群組原則。StorageGRID每個原則內部都有一組原則聲明、每個陳述都包含下列元素：

- 對帳單ID（Sid）（選用）
- 效果

- 委託人/未委託人
- 資源/未資源
- 行動/未行動
- 條件（選用）

原則陳述是使用此結構來指定權限：在套用<condition>時，授與<effect>允許/拒絕<Principe>執行<Action"。

每個原則元素都用於特定功能：

元素	說明
SID	Sid元素為選用項目。Sid僅供使用者說明使用。它會儲存、但StorageGRID 不會被作業系統解讀。
效果	使用effect元素來確定是否允許或拒絕指定的作業。您必須使用支援的Action元素關鍵字、識別您允許（或拒絕）的貯體或物件作業。
委託人/未委託人	您可以允許使用者、群組和帳戶存取特定資源並執行特定動作。如果要求中未包含S3簽名、則可指定萬用字元（*）做為主體、以匿名存取。根據預設、只有root帳戶可以存取該帳戶擁有的資源。 您只需要在庫位原則中指定主要元素。對於群組原則而言、附加原則的群組是內含的主體元素。
資源/未資源	資源元素可識別儲存區和物件。您可以使用Amazon資源名稱（ARN）來允許或拒絕貯體和物件的權限、以識別資源。
行動/未行動	「行動」和「效果」元素是權限的兩個元件。當群組要求資源時、系統會將資源的存取權限授予或拒絕。除非您特別指派權限、否則存取會遭拒、但您可以使用明確拒絕來覆寫其他原則所授予的權限。
條件	條件元素為選用項目。條件可讓您建置運算式、以判斷何時應套用原則。

在Action元素中、您可以使用萬用字元（*）來指定所有作業或作業子集。例如、此動作會比對S3：GetObject、S3：PuttObject和S3：Delete物件等權限。

```
s3:*Object
```

在資源元素中、您可以使用萬用字元（*）和（？）。星號（*）與0個以上的字元相符、但問號（？） 符合任何單一字元。

在 Principal 元素中、除了設定匿名存取外、不支援萬用字元、這會將權限授予每個人。例如、您將萬用字元（*）設為主要值。

```
"Principal":"*"
```

在下列範例中、陳述式使用的是「效果」、「主要」、「行動」和「資源」元素。此範例顯示完整的Bucket原則聲明、其使用「允許」的效果來賦予主體（即管理群組） `federated-group/admin` 以及財務團隊 `federated-group/finance`的權限 `s3:ListBucket` 在名為的儲存區上 `mybucket` 和行動 `s3:GetObject` 儲存區內的所有物件。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:iam:s3:::mybucket",
        "arn:aws:iam:s3:::mybucket/*"
      ]
    }
  ]
}
```

儲存區原則的大小上限為20、480個位元組、而且群組原則的大小上限為5、120個位元組。

原則的一致性控制設定

根據預設、您對群組原則所做的任何更新最終都是一致的。一旦群組原則一致、因為原則快取、變更可能需要額外15分鐘才能生效。根據預設、您對庫位原則所做的任何更新、最終也會保持一致。

您可以視需要變更庫位原則更新的一致性保證。例如、基於安全考量、您可能希望變更庫位原則、使其儘快生效。

在此情況下、您可以設定 `Consistency-Control` 請參閱「放入庫位」原則要求中的標頭、或使用「放入庫位一致性」要求。變更此要求的一致性控制時、您必須使用* all *值、以提供寫入後讀取一致性的最高保證。如果您在「放置時段一致性要求」的標頭中指定任何其他一致性控制值、則該要求將被拒絕。如果您為「放入庫位」原則要求指定任何其他值、則會忽略該值。當儲存區原則一致之後、由於原則快取、變更可能需要額外8秒的時間才能生效。

> 如果您將一致性層級設為*全部*、以強制新的儲存庫原則更快生效、請務必在完成時將儲存庫層級控制權設回其原始值。否則、所有未來的貯體要求都會使用* all*設定。

在原則聲明中使用**ARN**

在原則聲明中、ARN用於主要和資源元素。

- 使用此語法來指定S3資源ARN：

```
arn:aws:s3:::bucket-name
arn:aws:s3:::bucket-name/object_key
```

- 使用此語法來指定身分識別資源ARN（使用者和群組）：

```
arn:aws:iam::account_id:root
arn:aws:iam::account_id:user/user_name
arn:aws:iam::account_id:group/group_name
arn:aws:iam::account_id:federated-user/user_name
arn:aws:iam::account_id:federated-group/group_name
```

其他考量事項：

- 您可以使用星號（*）做為萬用字元、以比對物件金鑰內的零個或多個字元。
- 可以在物件金鑰中指定的國際字元、應使用Json utf-8或Json \u轉義序列進行編碼。不支援百分比編碼。

  "RFC 2141 URN語法"

  PPUT Bucket原則作業的HTTP要求本文必須以charset=utf-8進行編碼。

在原則中指定資源

在原則聲明中、您可以使用資源元素來指定允許或拒絕權限的儲存區或物件。

- 每個原則聲明都需要資源元素。在原則中、資源會以元素表示 `Resource`或是 `NotResource` 排除。
- 您可以使用S3資源ARN來指定資源。例如：

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- 您也可以在物件機碼內使用原則變數。例如：

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- 資源值可以指定在建立群組原則時尚未存在的儲存區。

使用主體元素來識別原則聲明允許/拒絕存取資源的使用者、群組或租戶帳戶。

- 庫位原則中的每個原則聲明都必須包含主要元素。群組原則中的原則聲明不需要 Principal 元素、因為群組被理解為主體。
- 在原則中、原則會以「主體」或「NotPrincipal」等元素表示、以排除原則。
- 帳戶型身分識別必須使用ID或ARN來指定：

```
"Principal": { "AWS": "account_id"}
"Principal": { "AWS": "identity_arn" }
```

- 此範例使用租戶帳戶ID 27233906934684427525、其中包含帳戶root和帳戶中的所有使用者：

```
 "Principal": { "AWS": "27233906934684427525" }
```

- 您只能指定帳戶根目錄：

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- 您可以指定特定的聯盟使用者（「Alex」）：

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
user/Alex" }
```

- 您可以指定特定的聯盟群組（「經理」）：

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
group/Managers"  }
```

- 您可以指定匿名主體：

```
"Principal": "*"
```

- 為了避免混淆、您可以使用使用者UUID、而非使用者名稱：

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-
eb6b9e546013
```

例如、假設Alex離開組織和使用者名稱 `Alex` 已刪除。如果有新的Alex加入組織、則指派給他們的任務相同 `Alex` 使用者名稱、新使用者可能會不小心繼承授予原始使用者的權限。

- 主要值可以指定建立儲存區原則時尚未存在的群組/使用者名稱。

在原則中指定權限

在原則中、會使用Action元素來允許/拒絕資源的權限。您可以在原則中指定一組權限、以元素「Action」表示、或是以「NotAction」表示排除權限。每個元素都對應到特定的S3 REST API作業。

這些表格列出套用至儲存區的權限、以及套用至物件的權限。

Amazon S3現在使用S3：PuttReplicationConfiguration權限來執行PPUT和DELETE Bucket複寫動作。針對每個行動使用不同的權限、這與原始的Amazon S3規格相符。StorageGRID

使用PUT覆寫現有值時、會執行刪除。

套用至貯體的權限

權限	**S3 REST API**作業	客製**StorageGRID**化以供選擇
S3：建立桶	放入鏟斗	
S3：刪除資源桶	刪除時段	
S3：刪除BucketMetadata通知	刪除時段中繼資料通知組態	是的
S3：刪除BucketPolicy	刪除庫位原則	
S3：刪除複製組態	刪除時段複寫	是的、請針對「放置」和「刪除」*分別設定權限
S3：GetBucketAcl	取得Bucket ACL	
S3：GetBucketCompliance	取得資源桶法規遵循（已過時）	是的
S3：GetBucketConsistency	取得庫位一致性	是的
S3：GetBucketCORS	獲取庫位檢查器	
S3：GetEncryptionConfiguration	取得Bucket加密	
S3：GetBucketLastAccessTime	取得時段上次存取時間	是的

權限	**S3 REST API**作業	客製**StorageGRID**化以供選擇
S3：GetBucketLocation	取得理想位置	
S3：GetBucketMetadata通知	取得Bucket中繼資料通知組態	是的
S3：GetBucketNotification	取得庫存箱通知	
S3：GetBucketObjectLockConfiguration	取得物件鎖定組態	
S3：GetBucketPolicy	取得庫存管理政策	
S3：GetBucketting	取得庫位標記	
S3：GetBucketVersion	取得版本管理	
S3：Get生命 週期組態	取得生命週期	
S3：GetReplicationConfiguration	取得庫位複寫	
S3：ListAllMyb桶	• 取得服務 • 取得儲存使用量	是的、適用於取得儲存設備使用量
S3：清單庫	• Get Bucket（列出物件） • 鏟斗 • POST物件還原	
S3：listBucketMultiPartUploads	• 列出多個部分上傳 • POST物件還原	
S3：listBucketVerions	取得Bucket版本	
S3：PuttBucketCompliance	符合資源桶規範（已過時）	是的
S3：PuttBucketConsistency	實現庫位一致性	是的
S3：PuttBucketCORS	• 刪除庫位檢查 • 放入庫位	
S3：PuttEncryptionConfiguration	• 刪除時段加密 • 使用資源桶加密	

權限	**S3 REST API**作業	客製**StorageGRID**化以供選擇
S3：PuttBucketLastAccessTime	將資源桶放在最後存取時間	是的
S3：PuttBucketMetadata通知	放置時段中繼資料通知組態	是的
S3：PuttBucketNotification	放置時段通知	
S3：PuttBucketObjectLockConfiguration	• 將鏟斗放在一起 `x-amz-bucket-object-lock-enabled: true` 要求標頭（也需要S3：建立桶權限） • 放置物件鎖定組態	
S3：PuttBucketPolicy	資源桶政策	
S3：PuttBucketting	• 刪除庫位標記 • 置入庫位標記	
S3：PuttBucketVersion	放入資源桶版本管理	
S3：Putt升降 器組態	• 刪除時段生命週期 • 放入鏟斗生命週期	
S3：PuttReplicationConfiguration	放入資源桶複寫	是的、請針對「放置」和「刪除」*分別設定權限

套用至物件的權限

權限	**S3 REST API**作業	客製**StorageGRID**化以供選擇
S3：中止多重角色上傳	• 中止多部份上傳 • POST物件還原	
S3：BypassGovernanceRetention	• 刪除物件 • 刪除多個物件 • 保留物件	

權限	S3 REST API作業	客製StorageGRID化以供選擇
S3：刪除物件	• 刪除物件 • 刪除多個物件 • POST物件還原	
S3：刪除ObjectTagging	刪除物件標記	
S3：刪除ObjectVersion標記	刪除物件標記（物件的特定版本）	
S3：刪除ObjectVersion	刪除物件（物件的特定版本）	
S3：GetObject	• 取得物件 • 標頭物件 • POST物件還原 • 選取「物件內容」	
S3：GetObjectAcl	取得物件ACL	
S3：GetObjectLegalHold	取得物件合法持有	
S3：GetObjectRetention	取得物件保留	
S3：GetObjectTagging	取得物件標記	
S3：GetObjectVersion標記	取得物件標記（物件的特定版本）	
S3：GetObjectVersion	Get物件（物件的特定版本）	
S3：列出多個零件上傳零件	列出零件、POST物件還原	
S3：PuttObject	• 放置物件 • 放置物件-複製 • POST物件還原 • 啟動多部份上傳 • 完成多部份上傳 • 上傳零件 • 上傳零件-複製	

權限	**S3 REST API**作業	客製**StorageGRID**化以供選擇
S3：PuttObjectLegalHold	將物件保留為合法	
S3：PuttObjectRetention	保留物件	
S3：PuttObjectTagging	放置物件標記	
S3：PuttObjectVersion標記	放置物件標記（物件的特定版本）	
S3：PuttOverwriteObject	• 放置物件 • 放置物件-複製 • 放置物件標記 • 刪除物件標記 • 完成多部份上傳	是的
S3：恢復物件	POST物件還原	

使用**PuttOverwriteObject**權限

S3：PuttOverwriteObject權限是套StorageGRID 用至建立或更新物件之作業的自訂功能。此權限的設定決定用戶端是否可以覆寫物件的資料、使用者定義的中繼資料或S3物件標記。

此權限的可能設定包括：

- 允許：用戶端可以覆寫物件。這是預設設定。
- * 拒絕 * ：用戶端無法覆寫物件。設為「拒絕」時、PuttOverwriteObject權限的運作方式如下：
  - 如果在同一路徑找到現有物件：
    - 物件的資料、使用者定義的中繼資料或 S3 物件標記無法覆寫。
    - 任何進行中的擷取作業都會取消、並傳回錯誤。
    - 如果啟用S3版本管理、則「拒絕」設定可防止「放置物件標記」或「刪除物件標記」作業修改物件及其非目前版本的TagSet。
  - 如果找不到現有的物件、此權限將不會生效。
- 當此權限不存在時、效果與「允許」設定相同。

> 如果目前的 S3 原則允許覆寫、而 PutOverwriteObject 權限設定為拒絕、則用戶端無法覆寫物件的資料、使用者定義的中繼資料或物件標記。此外、如果選取 * 禁止用戶端修改 * 核取方塊（ * 組態 * > * 安全性設定 * > * 網路和物件 * ）、則該設定會覆寫 PutOverwriteObject 權限的設定。

在原則中指定條件

條件會定義原則的生效時間。條件包括運算子和金鑰值配對。

條件使用金鑰值配對進行評估。條件元素可以包含多個條件、而且每個條件可以包含多個金鑰值配對。條件區塊使用下列格式：

```
Condition: {
     condition_type: {
          condition_key: condition_values
```

在下列範例中、ipAddress條件使用SourceIp條件金鑰。

```
"Condition": {
    "IpAddress": {
      "aws:SourceIp": "54.240.143.0/24"
        ...
},
        ...
```

支援的條件運算子

條件運算子的分類如下：

- 字串
- 數字
- 布林值
- IP 位址
- null檢查

條件運算子	說明
擷取等量資料	根據完全相符（區分大小寫）、將金鑰與字串值進行比較。
擷取NotEquals	根據否定比對（區分大小寫）、將金鑰與字串值進行比較。
StringEqualsIgnoreCase	根據完全相符的結果（忽略大小寫）、將金鑰與字串值進行比較。
StringNotEqualsIgnoreCase	根據否定比對（忽略大小寫）、將金鑰與字串值進行比較。
StringLike	根據完全相符（區分大小寫）、將金鑰與字串值進行比較。可以包括*和？萬用字元。
StringNotLike	根據否定比對（區分大小寫）、將金鑰與字串值進行比較。可以包括*和？萬用字元。

條件運算子	說明
分子等量	根據完全相符的結果、將金鑰與數值進行比較。
NumericNotEquals	根據已否定的比對、將金鑰與數值進行比較。
數值資料	根據「大於」比對、將金鑰與數值進行比較。
NumericGreaterThang Equals	根據「大於或等於」比對、將金鑰與數值進行比較。
數字LessThan	根據「小於」比對、將金鑰與數值進行比較。
NumericLessThang Equals	根據「小於或等於」比對、將金鑰與數值進行比較。
布爾	根據「'true or假'」比對、將金鑰與布林值進行比較。
IP地址	比較金鑰與IP位址或IP位址範圍。
NotIppAddress	根據已否定的比對、將金鑰與IP位址或IP位址範圍進行比較。
null	檢查條件金鑰是否存在於目前的要求內容中。

支援的條件金鑰

類別	適用的條件金鑰	說明
IP營運者	AWS：來源Ip	將會與傳送要求的IP位址進行比較。可用於庫位或物件作業。 *附註：*如果S3要求是透過管理節點和閘道節點上的負載平衡器服務傳送、則這會與負載平衡器服務上游的IP位址進行比較。 附註：如果使用第三方、不透明的負載平衡器、則會比較該負載平衡器的IP位址。任何 `X-Forwarded-For` 標頭將會被忽略、因為無法確定其有效性。
資源/身分識別	AWS：使用者名稱	將會比較傳送者的使用者名稱、以從中傳送要求。可用於庫位或物件作業。
S3：清單儲存庫和 S3：listBucketVerions權限	S3：分隔符號	會比較「Get Bucket」或「Get Bucket Object versions」要求中指定的分隔符號參數。

類別	適用的條件金鑰	說明
S3：清單儲存庫和 S3：listBucketVerions權限	S3：金鑰上限	會比較「Get Bucket」或「Get Bucket Object版本」要求中指定的最大金鑰參數。
S3：清單儲存庫和 S3：listBucketVerions權限	S3：前置碼	會比較「Get Bucket」或「Get Bucket Object versions」要求中指定的前置字元參數。
S3：PuttObject	S3：物件鎖定剩餘保留天數	與中指定的保留截止日期比較 `x-amz-object-lock-retain-until-date` 要求標頭或從貯體預設保留期間計算、以確保這些值在下列要求的允許範圍內： • 放置物件 • 放置物件-複製 • 啟動多部份上傳
S3：PuttObjectRetention	S3：物件鎖定剩餘保留天數	與「放置物件保留」要求中指定的保留截止日期進行比較、以確保其在允許的範圍內。

在原則中指定變數

您可以在原則中使用變數、在原則可用時填入原則資訊。您可以在中使用原則變數 `Resource` 中的元素和字串比較 `Condition` 元素。

在此範例中、變數 `${aws:username}` 是資源元素的一部分：

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

在此範例中、變數 `${aws:username}` 是條件區塊中條件值的一部分：

```
"Condition": {
    "StringLike": {
      "s3:prefix": "${aws:username}/*"
        ...
},
        ...
```

變動	說明
`${aws:SourceIp}`	使用來源Ip金鑰作為提供的變數。

變動	說明
`${aws:username}`	使用UserName金鑰做為提供的變數。
`${s3:prefix}`	使用服務專屬的前置碼作為提供的變數。
`${s3:max-keys}`	使用服務專屬的最大金鑰作為提供的變數。
`${*}`	特殊字元。使用字元做為文字*字元。
`${?}`	特殊字元。使用字元做為字型？字元。
`${$}`	特殊字元。使用字元做為文字$字元。

建立需要特殊處理的原則

有時候原則可能會授與安全性危險或危險的權限、以便繼續執行作業、例如封鎖帳戶的root使用者。在原則驗證期間、不像Amazon、StorageGRID 執行「支援S3 REST API」的限制較少、但在原則評估期間同樣嚴格。

原則說明	原則類型	**Amazon**行為	運作方式**StorageGRID**
拒絕root帳戶的任何權限	鏟斗	有效且強制、但root使用者帳戶保留所有S3儲存區原則作業的權限	相同
拒絕對使用者/群組擁有任何權限	群組	有效且強制	相同
允許外部帳戶群組擁有任何權限	鏟斗	無效的主體	有效、但原則允許時、所有S3儲存區原則作業的權限都會傳回「不允許使用405方法」錯誤
允許外部帳戶root或使用者擁有任何權限	鏟斗	有效、但原則允許時、所有S3儲存區原則作業的權限都會傳回「不允許使用405方法」錯誤	相同
允許每個人都有權執行所有動作	鏟斗	有效、但所有S3儲存區原則作業的權限都會傳回異帳戶根目錄和使用者不允許的「405方法」錯誤	相同
拒絕所有人對所有動作的權限	鏟斗	有效且強制、但root使用者帳戶保留所有S3儲存區原則作業的權限	相同

原則說明	原則類型	**Amazon**行為	運作方式**StorageGRID**
主體是不存在的使用者或群組	鏟斗	無效的主體	有效
資源是不存在的S3儲存區	群組	有效	相同
主體是本機群組	鏟斗	無效的主體	有效
原則授予非擁有者帳戶（包括匿名帳戶）放置物件的權限	鏟斗	有效。物件由建立者帳戶擁有、且庫位原則不適用。建立者帳戶必須使用物件ACL來授與物件的存取權限。	有效。物件由庫位擁有者帳戶擁有。適用庫位政策。

一次寫入多讀（**WORM**）保護

您可以建立一次寫入多次讀取（WORM）儲存區、以保護資料、使用者定義的物件中繼資料、以及S3物件標記。您可以設定WORM儲存區、以允許建立新物件、並防止覆寫或刪除現有內容。請使用本文所述的其中一種方法。

為了確保覆寫永遠被拒絕、您可以：

- 從 Grid Manager 移至 * 組態 * > * 安全性 * > * 安全性設定 * > * 網路和物件 * 、然後選取 * 禁止用戶端修改 * 核取方塊。
- 套用下列規則和S3原則：
  - 將PuttOverwriteObject拒絕作業新增至S3原則。
  - 將刪除物件拒絕作業新增至S3原則。
  - 新增「允許放置物件」作業至S3原則。

若在S3原則中將刪除物件設為拒絕、則不會在存在「30天後歸零複本」等規則時、防止ILM刪除物件。

即使套用了所有這些規則和原則、也無法防範並行寫入（請參閱情況 A ）。它們確實能防止連續完成的覆寫（請參閱情況B）。

情況**A**：並行寫入（不受保護）

```
/mybucket/important.doc
PUT#1 ---> OK
PUT#2 -------> OK
```

情況**B**：連續完成覆寫（防範）

```
/mybucket/important.doc
PUT#1 -------> PUT#2 ---X (denied)
```

相關資訊

- "如何利用ILM規則來管理物件StorageGRID"
- "貯體原則範例"
- "群組原則範例"
- "使用ILM管理物件"
- "使用租戶帳戶"

貯體原則範例

使用本節中的範例、為貯體建立 StorageGRID 存取原則。

儲存區原則會指定原則附加的儲存區存取權限。儲存區原則是使用S3 PuttBucketPolicy API進行設定。請參閱 "在貯體上作業"。

根據下列命令、可使用AWS CLI設定儲存區原則：

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
file://policy.json
```

範例：允許每個人只讀存取儲存區

在此範例中、每個人（包括匿名）都可以列出儲存區中的物件、並對儲存區中的所有物件執行「Get Object」（取得物件）作業。所有其他作業都將遭拒。請注意、這項原則可能並不特別有用、因為除了帳戶根目錄之外、沒有其他人擁有寫入貯體的權限。

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"]
    }
  ]
}
```

範例：允許同一個帳戶中的每個人都擁有完整存取權、以及其他帳戶中的每個人只讀存取庫位

在此範例中、某個指定帳戶中的每個人都可以完整存取某個儲存區、而另一個指定帳戶中的每個人只能列出該儲存區、並從開始對儲存區中的物件執行GetObject作業 `shared/` 物件金鑰前置碼。

> 在功能區中StorageGRID 、非擁有者帳戶所建立的物件（包括匿名帳戶）、均由庫位擁有者帳戶擁有。庫位原則適用於這些物件。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "95390887230002558202"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/shared/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::examplebucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "shared/*"
        }
      }
    }
  ]
}
```

範例：允許每個人只讀存取儲存區、並由指定群組進行完整存取

在此範例中、每個人（包括匿名）都可以列出儲存區、並在儲存區中的所有物件上執行「Get Object」（取得物件）作業、而只有屬於群組的使用者 `Marketing` 在指定的帳戶中、允許完整存取。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/Marketing"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3:ListBucket","s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

範例：如果用戶端位於**IP**範圍、則允許每個人讀取及寫入儲存區的存取權

在此範例中、每個人（包括匿名）都可以列出儲存區、並在儲存區中的所有物件上執行任何物件作業、前提是要求來自指定的IP範圍（54.240.143.0至54.240.143.255、但54.240.143.188除外）。所有其他作業都會遭到拒絕、而且IP範圍以外的所有要求都會遭到拒絕。

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadWriteAccessIfInSourceIpRange",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:*Object", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"],
      "Condition": {
        "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
        "NotIpAddress": {"aws:SourceIp": "54.240.143.188"}
      }
    }
  ]
}
```

範例：允許特定同盟使用者專屬完整存取儲存區

在此範例中、聯盟使用者Alex可以完整存取 `examplebucket` 儲存區及其物件。所有其他使用者、包括「root」、都會明確拒絕所有作業。不過請注意、「root」永遠不會被拒絕存取權限來放置/取得/刪除BucketPolicy。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

範例：**PuttOverwriteObject**權限

在此範例中 `Deny` PuttoverwriteObject和Delete物件的效果可確保任何人都無法覆寫或刪除物件的資料、使用者定義的中繼資料和S3物件標記。

```
{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutOverwriteObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::wormbucket/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}
```

群組原則範例

使用本節中的範例、為群組建置 StorageGRID 存取原則。

群組原則會指定原則所附加之群組的存取權限。沒有 `Principal` 原則中的元素、因為它是隱含的。群組原則是使用租戶管理程式或API來設定。

範例：使用租戶管理程式設定群組原則

當您在租戶管理器中新增或編輯群組時、可以選取群組原則、以判斷此群組成員將擁有哪些 S3 存取權限。請參閱 "為S3租戶建立群組"。

- 無**S3**存取：預設選項。此群組中的使用者無法存取 S3 資源、除非已透過貯體原則授予存取權限。如果選取此選項、預設只有root使用者可以存取S3資源。
- 唯讀存取：此群組中的使用者擁有S3資源的唯讀存取權。例如、此群組中的使用者可以列出物件並讀取物件資料、中繼資料和標記。選取此選項時、唯讀群組原則的Json字串會出現在文字方塊中。您無法編輯此字串。
- 完整存取：此群組中的使用者可完整存取S3資源、包括儲存區。選取此選項時、會在文字方塊中顯示完整存取群組原則的Json字串。您無法編輯此字串。
- * 勒索軟體緩解 * ：此範例原則適用於此租戶的所有貯體。此群組中的使用者可以執行一般動作、但無法從已啟用物件版本設定的儲存區中永久刪除物件。

  擁有「管理所有貯體」權限的租戶管理員使用者可以覆寫此群組原則。將「管理所有貯體」權限限制於信任的使用者、並在可行的情況下使用「多因素驗證」（ MFA ）。

- 自訂：群組中的使用者會被授予您在文字方塊中指定的權限。

範例：允許群組完整存取所有儲存區

在此範例中、除非庫位原則明確拒絕、否則群組的所有成員都可以完整存取租戶帳戶擁有的所有庫位。

```
{
  "Statement": [
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

範例：允許群組唯讀存取所有儲存區

在此範例中、除非資源庫原則明確拒絕、否則群組的所有成員都擁有S3資源的唯讀存取權。例如、此群組中的使用者可以列出物件並讀取物件資料、中繼資料和標記。

```
{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

範例：允許群組成員只能完整存取儲存庫中的「**'folder"**」

在此範例中、群組成員只能在指定的儲存區中列出及存取其特定資料夾（金鑰首碼）。請注意、在決定這些資料夾的隱私權時、應考慮其他群組原則和儲存區原則的存取權限。

```
{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}
```

設定**REST API**的安全性

您應該檢閱針對REST API實作的安全措施、並瞭解如何保護系統安全。

如何為**REST API**提供安全性**StorageGRID**

您應該瞭解StorageGRID 什麼是讓此系統為REST API實作安全性、驗證和授權。

使用下列安全措施。StorageGRID

- 如果已針對負載平衡器端點設定HTTPS、則用戶端與負載平衡器服務的通訊會使用HTTPS。

  當您設定負載平衡器端點時、可以選擇啟用HTTP。例如、您可能想要使用HTTP進行測試或其他非正式作業用途。如StorageGRID 需詳細資訊、請參閱《關於管理功能的說明》。

- 根據預設、 StorageGRID 會使用 HTTPS 與儲存節點進行用戶端通訊。

  您可以選擇性地為這些連線啟用HTTP。例如、您可能想要使用HTTP進行測試或其他非正式作業用途。如StorageGRID 需詳細資訊、請參閱《關於管理功能的說明》。

- 支援使用TLS加密支援不支援的客戶端與StorageGRID 之通訊。
- 無論負載平衡器端點是設定為接受HTTP或HTTPS連線、網格內負載平衡器服務與儲存節點之間的通訊都會加密。
- 用戶端必須提供HTTP驗證標頭StorageGRID 給才能執行REST API作業。

用戶端可以直接連線至 Gateway 節點或管理節點上的負載平衡器服務、並直接連線至 Storage Node 。

在任何情況下、用戶端應用程式都可以使用網格管理員上傳的自訂伺服器憑證或StorageGRID 由該系統產生的憑證來建立TLS連線：

- 當用戶端應用程式連線至負載平衡器服務時、應用程式會使用針對用於建立連線的特定負載平衡器端點所設定的憑證來執行此作業。每個端點都有自己的憑證、可以是由網格管理員上傳的自訂伺服器憑證、也可以是網格管理員StorageGRID 在設定端點時產生的憑證。
- 當用戶端應用程式直接連線至儲存節點時、它們會使用安裝 StorageGRID 系統（由系統憑證授權單位簽署）時為儲存節點產生的系統產生的伺服器憑證、 或是由網格管理員提供給網格的單一自訂伺服器憑證。

用戶端應設定為信任已簽署其用於建立TLS連線之任何憑證的憑證授權單位。

如需設定負載平衡器端點的相關資訊、請參閱管理 StorageGRID 的指示、以及直接將單一自訂伺服器憑證新增至儲存節點的說明。

摘要

下表顯示S3和Swift REST API如何實作安全性問題：

安全問題	**REST API**的實作
連線安全性	TLS
伺服器驗證	由系統CA或系統管理員提供的自訂伺服器憑證簽署的X．509伺服器憑證
用戶端驗證	• S3：S3帳戶（存取金鑰ID和秘密存取金鑰） • Swift：Swift帳戶（使用者名稱和密碼）
用戶端授權	• S3：貯體所有權及所有適用的存取控制原則 • Swift：系統管理員角色存取

相關資訊

"管理StorageGRID"

TLS程式庫支援的雜湊和加密演算法

支援一套有限的加密套件、用戶端應用程式可在建立傳輸層安全性（TLS）工作階段時使用。StorageGRID要配置加密算法，請轉至 * 配置 * > * 安全性 * > * 安全性設置 * ，然後選擇 *TLS 和 SSH 策略 * 。

支援的**TLS**版本

支援TLS 1.2和TLS 1.3。StorageGRID

不再支援SSLv3和TLS 1.1（或更早版本）。

相關資訊

"設定租戶帳戶和連線"

監控與稽核作業

監控物件擷取和擷取速率

您可以監控物件擷取和擷取速率、以及物件計數、查詢和驗證的度量。您可以檢視用戶端應用程式在StorageGRID 讀取、寫入及修改物件時、成功和失敗的嘗試次數。

步驟

1. 使用登入Grid Manager "支援的網頁瀏覽器"。
2. 在儀表板上、選取 * 效能 * > * S3 作業 * 或 * 效能 * > * Swift 作業 * 。

   本節概述StorageGRID 您的一套系統執行的用戶端作業數量。在過去兩分鐘內平均傳輸協定速率。

3. 選擇*節點*。
4. 在節點首頁（部署層級）中、按一下*負載平衡器*索引標籤。

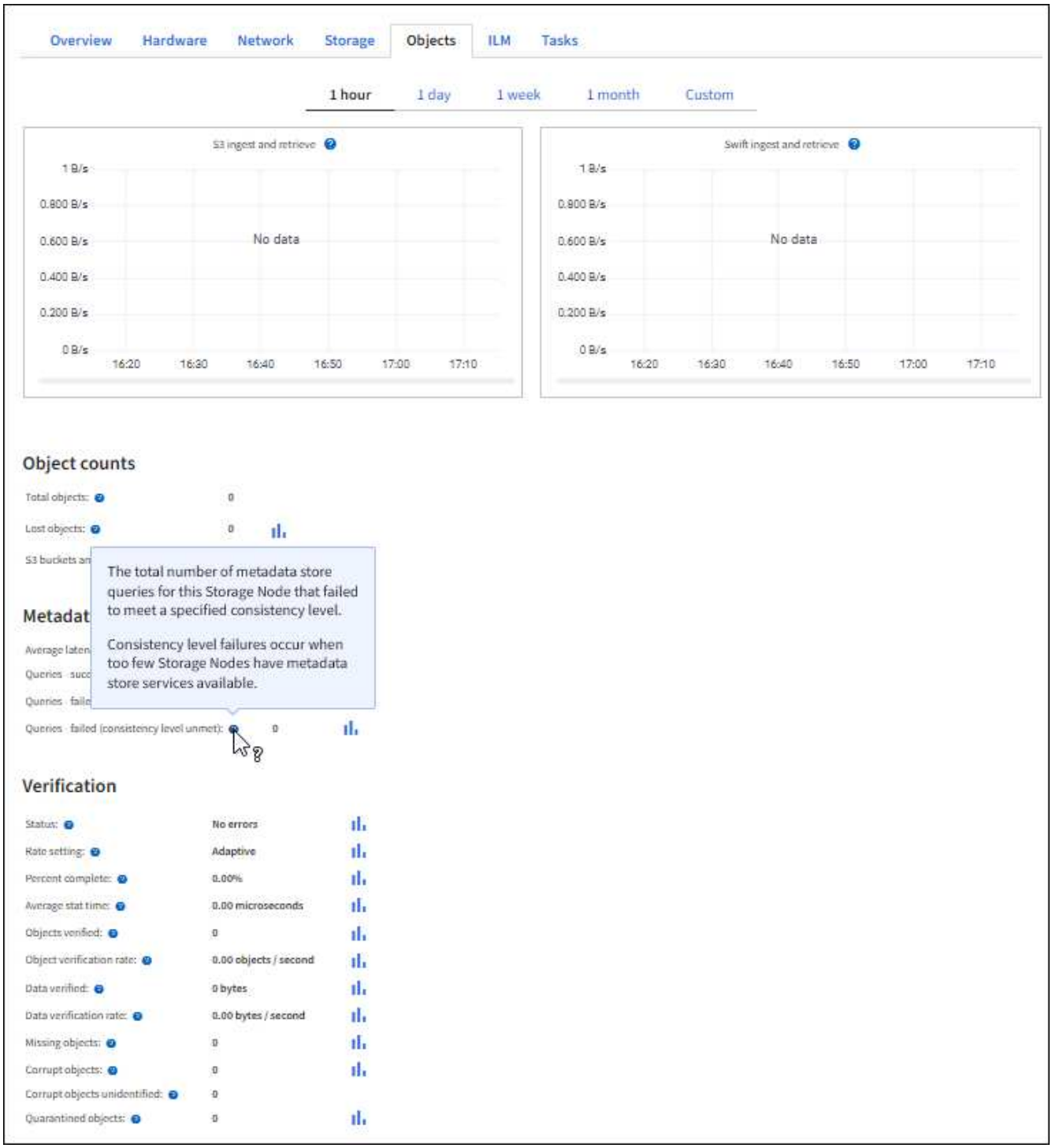
   這些圖表顯示了導向至網格內負載平衡器端點的所有用戶端流量趨勢。您可以選擇以小時、天、週、月或年為單位的時間間隔、 您也可以套用自訂時間間隔。

5. 在節點首頁（部署層級）中、按一下*物件*索引標籤。

   此圖表以StorageGRID 每秒位元組數和總位元組數顯示整個系統的擷取和擷取速率。您可以選擇以小時、天、週、月或年為單位的時間間隔、 您也可以套用自訂時間間隔。

6. 若要查看特定儲存節點的資訊、請從左側清單中選取節點、然後按一下「物件」索引標籤。

   此圖表顯示此儲存節點的物件擷取和擷取速率。此索引標籤也包含物件計數、查詢和驗證的度量。您可以按一下標籤來查看這些度量的定義。



7. 如果您想要更詳細的資料：
   a. 選取*支援*>*工具*>*網格拓撲*。
   b. 選擇*站台_*>*總覽*>*主選項*。

      「API作業」區段會顯示整個網格的摘要資訊。

   c. 選擇「儲存節點_」>「最大」>「用戶端應用程式_」>「總覽」>「主要」

      「作業」區段會顯示所選儲存節點的摘要資訊。

稽核訊息是StorageGRID 由支援服務產生、並儲存在文字記錄檔中。稽核日誌中的API專屬稽核訊息可提供關鍵的安全性、作業和效能監控資料、協助您評估系統的健全狀況。

開始之前

- 您擁有特定的存取權限。
- 您擁有 `Passwords.txt` 檔案：
- 您知道管理節點的IP位址。

關於這項工作

作用中的稽核記錄檔會命名為 `audit.log`和儲存在管理節點上。

一天只要儲存一次作用中的audit.log檔案、就會儲存一個新檔案 `audit.log` 檔案已啟動。儲存檔案的名稱會以格式指出儲存時間 *`yyyy-mm-dd.txt`*。

一天後、儲存的檔案會以壓縮格式重新命名 *`yyyy-mm-dd.txt.gz`*，保留原始日期。

此範例顯示使用中的 `audit.log` 檔案、前一天的檔案 (`2018-04-15.txt`）、以及前一天的壓縮檔案 (`2018-04-14.txt.gz`）。

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

步驟

1. 登入管理節點：
   a. 輸入下列命令： `ssh admin@primary_Admin_Node_IP`
   b. 輸入中所列的密碼 `Passwords.txt` 檔案：
   c. 輸入下列命令以切換至root： `su -`
   d. 輸入中所列的密碼 `Passwords.txt` 檔案：

      當您以root登入時、提示會從變更 `$` 至 `#`。
2. 移至包含稽核記錄檔的目錄：

   ```
   cd /var/local/audit/export
   ```
3. 視需要檢視目前或已儲存的稽核記錄檔。

稽核記錄中追蹤的**S3**作業

在不完整的稽核記錄中、會追蹤多項庫位作業和物件作業StorageGRID 。

稽核記錄中追蹤的庫位作業

- 刪除時段
- 刪除庫位標記
- 刪除多個物件
- Get Bucket（列出物件）
- 取得Bucket物件版本
- 取得庫位標記
- 鏟斗
- 放入鏟斗
- 符合資源需求
- 置入庫位標記
- 放入資源桶版本管理

稽核記錄中追蹤的物件作業

- 完成多部份上傳
- 上傳零件（當 ILM 規則使用平衡或嚴格的擷取行為時）
- 上傳零件 - 複製（當 ILM 規則使用平衡或嚴格的擷取行為時）
- 刪除物件
- 取得物件
- 標頭物件
- POST物件還原
- 放置物件
- 放置物件-複製

相關資訊

"在貯體上作業"

"物件上的作業"

作用中、閒置及並行**HTTP**連線的優點

如何設定HTTP連線、可能會影響StorageGRID 到整個系統的效能。組態會因HTTP連線為作用中或閒置狀態、或是您同時有多個連線而有所不同。

您可以找出下列類型HTTP連線的效能優勢：

- 閒置HTTP連線
- 作用中HTTP連線
- 並行HTTP連線

保持閒置**HTTP**連線開啟的優點

即使用戶端應用程式閒置、您仍應保持HTTP連線開啟、以允許用戶端應用程式透過開放式連線執行後續交易。根據系統測量與整合體驗、您應將閒置的HTTP連線保持開啟狀態最長10分鐘。可能會自動關閉持續開啟和閒置超過10分鐘的HTTP連線。StorageGRID

開放式和閒置的HTTP連線提供下列優點：

- 縮短延遲時間、從StorageGRID 由整個過程中、由整個過程中的資訊系統判斷它必須執行HTTP交易到StorageGRID 整個系統能夠執行交易的時間

  縮短延遲是主要優勢、尤其是在建立TCP/IP和TLS連線所需的時間內。

- 使用先前執行的傳輸來初始化TCP/IP慢速啟動演算法、藉此提高資料傳輸率
- 即時通知多種故障情況、可中斷用戶端應用程式與StorageGRID 該系統之間的連線

判斷閒置連線開啟的時間長度、是在與現有連線相關的慢速啟動優點與內部系統資源連線的理想分配之間取得平衡。

作用中**HTTP**連線的優點

對於直接連線至儲存節點的連線、即使 HTTP 連線持續執行交易、您仍應將作用中 HTTP 連線的持續時間限制為最多 10 分鐘。

判斷連線應保持開啟的最長時間、是在連線持續性的優點與連線至內部系統資源的理想分配之間取得平衡。

對於用戶端連線至儲存節點、限制作用中的 HTTP 連線有下列優點：

- 在StorageGRID 整個支援過程中實現最佳負載平衡。

  隨著時間推移、隨著負載平衡需求的變更、HTTP連線可能不再是最佳狀態。當用戶端應用程式為每筆交易建立獨立的HTTP連線時、系統會執行最佳負載平衡、但這會使持續連線所帶來的更多寶貴成果喪失價值。

- 允許用戶端應用程式將HTTP交易導向具有可用空間的LDR服務。
- 可啟動維護程序。

  部分維護程序只會在所有進行中的HTTP連線完成後才會開始。

對於連接到負載平衡器服務的用戶端連線、限制開放連線的持續時間、有助於讓部分維護程序立即啟動。如果用戶端連線的持續時間不受限制、則自動終止作用中連線可能需要幾分鐘的時間。

並行**HTTP**連線的優點

您應該StorageGRID 將多個TCP/IP連線保持開放狀態、以允許平行處理、進而提升效能。最佳的平行連線數量取決於各種因素。

並行HTTP連線提供下列優點：

- 縮短延遲時間

  交易可以立即開始、而非等待其他交易完成。

- 提高處理量

  此系統可執行平行交易、並提高集合交易處理量。StorageGRID

用戶端應用程式應建立多個HTTP連線。當用戶端應用程式必須執行交易時、它可以選取並立即使用任何目前未處理交易的已建立連線。

在StorageGRID 效能開始降級之前、每個支援系統的拓撲在並行交易和連線方面都有不同的尖峰處理量。尖峰處理量取決於運算資源、網路資源、儲存資源和WAN連結等因素。此外、伺服器和服務的數量、StorageGRID 以及支援哪些應用程式、也是因素。

支援多種用戶端應用程式的系統。StorageGRID當您決定用戶端應用程式所使用的並行連線數目上限時、請謹記這一點。如果用戶端應用程式包含多個軟體實體、每個實體都會建立StorageGRID 與該系統的連線、您應該新增整個實體之間的所有連線。在下列情況下、您可能必須調整並行連線的最大數量：

- 此系統的拓撲會影響系統可支援的並行交易和連線數量上限。StorageGRID
- 在StorageGRID 頻寬有限的網路上與該系統互動的用戶端應用程式、可能必須降低並行度、以確保在合理的時間內完成個別交易。
- 當許多用戶端應用程式共用StorageGRID 該系統時、您可能必須減少並行處理的程度、以避免超出系統限制。

分隔**HTTP**連線集區以進行讀取和寫入作業

您可以使用不同的HTTP連線集區進行讀取和寫入作業、並控制每個集區的使用量。獨立的HTTP連線集區可讓您更有效地控制交易並平衡負載。

用戶端應用程式可建立擷取主導（讀取）或儲存主導（寫入）的負載。有了個別的HTTP連線集區、即可針對讀寫交易調整每個集區的專屬容量、以處理讀寫交易。

使用 **Swift REST API** （已過時）

使用 **Swift REST API** ：概述

用戶端應用程式可以使用OpenStack Swift API與StorageGRID 該系統進行介面。

Swift 用戶端應用程式的支援已過時、未來版本將會移除。

支援下列Swift和HTTP的特定版本。StorageGRID

項目	版本
Swift規格	OpenStack Swift Object Storage API v1（截至2015年11月）
HTTP	1.1如需HTTP的詳細資訊、請參閱HTTP / 1.1（RFC 7230-35）。 附註 StorageGRID ：不支援HTTP / 1.1鋪管。

相關資訊

"OpenStack：物件儲存API"

Swift API支援的歷史StorageGRID 記錄

您應該注意StorageGRID 到支援Swift REST API的功能有所變更。

版本	註解
11.7	Swift 用戶端應用程式的支援已過時、未來版本將會移除。
11.6%	略有編輯變更。
11.5	移除弱一致性控制。將改用可用的一致性層級。
11.4	新增 TLS 1.3 支援。新增ILM與一致性設定之間相互關係的說明。
11.3	更新的「放置物件」作業、說明ILM規則在擷取時使用同步放置的影響（擷取行為的平衡和嚴格選項）。新增使用負載平衡器端點或高可用度群組的用戶端連線說明。不再支援TLS 1.1密碼。
11.2	文件的編輯略有變更。
11.1.	新增使用HTTP的支援、可將Swift用戶端連線至網格節點。更新一致性控制的定義。
11.0	新增每個租戶帳戶的1、000個容器支援。
10.3.1	文件的管理更新與修正。移除設定自訂伺服器憑證的區段。
10.2	Swift API的初始支援StorageGRID 、由整個系統提供。目前支援的版本為OpenStack Swift Object Storage API v1。

如何實作Swift REST API StorageGRID

用戶端應用程式可以使用Swift REST API呼叫來連線至儲存節點和閘道節點、以建立容器、以及儲存和擷取物件。如此一來、專為OpenStack Swift開發的服務導向應用程式就能與StorageGRID 由該系統提供的內部部署物件儲存設備連線。

Swift物件管理

在StorageGRID Swift物件被擷取到整個物件系統之後、這些物件會由系統作用中ILM原則中的資訊生命週期管理（ILM）規則來管理。。 "ILM規則" 和 "ILM原則" 判斷 StorageGRID 如何建立及散佈物件資料複本、以及如何隨著時間管理這些複本。例如、ILM規則可能會套用至特定Swift容器中的物件、並可能指定將多個物件複本儲存至數個資料中心、保留一段時間。

如果您需要瞭解網格的 ILM 規則和原則如何影響 Swift 租戶帳戶中的物件、請聯絡您的 NetApp 專業服務顧問或

StorageGRID 管理員。

衝突的用戶端要求

衝突的用戶端要求（例如兩個寫入同一個金鑰的用戶端）會以「最新致勝」的方式解決。「最新致勝」評估的時間取決於StorageGRID VMware系統何時完成指定的要求、而非Swift用戶端何時開始作業。

一致性保證與控管

根據預設、StorageGRID 針對新建立的物件、提供寫入後讀取一致性、並在物件更新和執行前置作業時提供最終一致性。任何 "取得" 在成功完成之後 "放入" 將能夠讀取新寫入的資料。覆寫現有物件、更新中繼資料及刪除的動作最終一致。覆寫通常需要幾秒鐘或幾分鐘才能傳播、但可能需要15天的時間。

利用此功能、您也可以控制每個容器的一致性。StorageGRID一致性控制功能可根據應用程式的需求、在物件的可用度與不同儲存節點和站台之間的物件一致性之間取得平衡。

實作**Swift REST API**的建議

實作Swift REST API以搭配StorageGRID 使用時、請遵循以下建議。

針對不存在物件的使用者提出建議

如果您的應用程式會定期檢查某個物件是否存在於您不希望該物件實際存在的路徑、則應使用「可用」一致性控制項。例如、如果您的應用程式在執行放置作業之前、先對某個位置執行頭作業、則應使用「可用」一致性控制。

否則、如果執行頭作業找不到物件、當一個或多個儲存節點無法使用時、您可能會收到大量500個內部伺服器錯誤。

您可以使用設定每個容器的「可用」一致性控制 "放置容器一致性要求"。您可以使用設定每個容器的「可用」一致性控制 "取得Container一致性要求"。

物件名稱建議

對於StorageGRID 以VMware 11.4或更新版本建立的容器、不再需要限制物件名稱以符合效能最佳實務做法。例如、您現在可以將隨機值用於物件名稱的前四個字元。

若容器是在StorageGRID 版本早於物件名稱的版本中建立、請繼續遵循以下建議：

- 您不應使用隨機值做為物件名稱的前四個字元。這與前AWS關於名稱前置詞的建議不同。您應該改用非隨機、非唯一的前置詞、例如 `image`。
- 如果您遵循前一項AWS建議、在名稱前置字元中使用隨機和獨特的字元、則應該在物件名稱前置一個目錄名稱。也就是使用此格式：

  ```
  mycontainer/mydir/f8e3-image3132.jpg
  ```

  而非此格式：

  ```
  mycontainer/f8e3-image3132.jpg
  ```

「**range Reads**」建議

如果是 "用於壓縮儲存物件的全域選項" 啟用時、 Swift 用戶端應用程式應避免執行指定傳回位元組範圍的 Get 物件作業。這些「範圍讀取」作業效率不彰、因為StorageGRID 必須有效解壓縮物件才能存取所要求的位元組。從非常大的物件要求少量位元組的「Get Object」（取得物件）作業效率特別低；例如、從50 GB壓縮物件讀取10 MB範圍的效率非常低。

如果從壓縮物件讀取範圍、用戶端要求可能會逾時。

如果您需要壓縮物件、而用戶端應用程式必須使用範圍讀取、請增加應用程式的讀取逾時。

設定租戶帳戶和連線

若要設定StorageGRID 從用戶端應用程式接受連線、需要建立一或多個租戶帳戶並設定連線。

建立及設定**Swift**租戶帳戶

Swift API用戶端必須先有Swift租戶帳戶、才能將物件儲存及擷取StorageGRID 到靜止不動的地方。每個租戶帳戶都有自己的帳戶ID、群組和使用者、以及容器和物件。

Swift租戶帳戶是StorageGRID 由使用Grid Manager或Grid Management API的資訊網管理員所建立。

何時 "建立 Swift 租戶帳戶"，網格管理員會指定下列資訊：

- "租戶的顯示名稱"（租戶的帳戶 ID 會自動指派、無法變更）
- （可選） a "租戶帳戶的儲存配額" — 租戶物件可用的最大 GB 、 TB 或 PB 數。租戶的儲存配額代表邏輯容量（物件大小）、而非實體容量（磁碟大小）。
- 如果 "單一登入（ SSO ）" 不適用於 StorageGRID 系統、無論租戶帳戶是使用自己的身分識別來源、還是共用網格的身分識別來源、以及租戶本機根使用者的初始密碼。
- 如果啟用 SSO 、則哪個聯盟群組具有「根」存取權限、可設定租戶帳戶。

建立 Swift 租戶帳戶之後、擁有「根」存取權限的使用者可以存取租戶管理員、以執行下列工作：

- 設定身分識別聯盟（除非身分識別來源與網格共用）、以及建立本機群組和使用者
- 監控儲存使用量

Swift 使用者必須具有的「根」存取權限 "存取租戶管理程式"。不過、「根」存取權限不允許使用者驗證Swift REST API、以建立容器和擷取物件。使用者必須具有Swift Administrator權限、才能驗證到Swift REST API。

如何設定用戶端連線

網格管理員會做出組態選擇、影響Swift用戶端連線StorageGRID 至以儲存及擷取資料的方式。建立連線所需的特定資訊取決於所選的組態。

用戶端應用程式可在管理節點或閘道節點上連線至負載平衡器服務、或選擇性地連線至管理節點或閘道節點的高可用度（ HA ）群組的虛擬 IP 位址、以儲存或擷取物件。

所有仰賴 StorageGRID 來提供負載平衡的應用程式都應該使用負載平衡器服務進行連線。

- 儲存節點、無論是否有外部負載平衡器

設定StorageGRID 功能時、網格管理員可以使用Grid Manager或Grid Management API來執行下列步驟、這些步驟都是選用的：

1. 設定負載平衡器服務的端點。

   您必須設定端點以使用負載平衡器服務。管理節點或閘道節點上的負載平衡器服務會將傳入的網路連線從用戶端應用程式分散到儲存節點。建立負載平衡器端點時StorageGRID 、系統管理員會指定連接埠號碼、端點是否接受HTTP或HTTPS連線、使用端點的用戶端類型（S3或Swift）、以及用於HTTPS連線的憑證（若適用）。Swift 支援這些功能 "端點類型"。

2. 設定不受信任的用戶端網路。

   如果StorageGRID 某個節點的用戶端網路設定為不受信任、則該節點僅接受用戶端網路上明確設定為負載平衡器端點之連接埠的傳入連線。

3. 設定高可用度群組。

   如果系統管理員建立HA群組、則多個管理節點或閘道節點的網路介面會置於主動備份組態中。用戶端連線是使用HA群組的虛擬IP位址進行。

請參閱 "HA群組的組態選項" 以取得更多資訊。

摘要：用於用戶端連線的**IP**位址和連接埠

用戶端應用程式StorageGRID 會使用網格節點的IP位址和該節點上服務的連接埠號碼來連線至功能區。如果已設定高可用度（HA）群組、用戶端應用程式就可以使用HA群組的虛擬IP位址進行連線。

建立用戶端連線所需的資訊

下表摘要說明用戶端連線StorageGRID 至靜態的不同方式、以及每種連線類型所使用的IP位址和連接埠。請參閱 "用戶端連線的 IP 位址和連接埠" 或聯絡您的 StorageGRID 管理員以取得更多資訊。

連線位置	用戶端連線的服務	**IP** 位址	連接埠
HA群組	負載平衡器	HA群組的虛擬IP位址	• 負載平衡器端點連接埠
管理節點	負載平衡器	管理節點的IP位址	• 負載平衡器端點連接埠
閘道節點	負載平衡器	閘道節點的IP位址	• 負載平衡器端點連接埠

連線位置	用戶端連線的服務	IP 位址	連接埠
儲存節點	LdR	儲存節點的IP位址	預設Swift連接埠： • HTTPS：18083 • HTTP：18085

範例

若要將Swift用戶端連線至閘道節點HA群組的負載平衡器端點、請使用結構如下所示的URL：

- `https://VIP-of-HA-group:LB-endpoint-port`

例如、如果HA群組的虛擬IP位址為192.0.2.6、而Swift負載平衡器端點的連接埠號碼為104444、則Swift用戶端可使用下列URL連線StorageGRID 到Sender:

- `https://192.0.2.6:10444`

您可以為用戶端用來連線StorageGRID 到靜態的IP位址設定DNS名稱。請聯絡您的本機網路管理員。

決定使用**HTTPS**或**HTTP**連線

使用負載平衡器端點進行用戶端連線時、必須使用為該端點指定的傳輸協定（HTTP或HTTPS）來建立連線。若要將 HTTP 用於用戶端連線至儲存節點、您必須啟用 HTTP 。

根據預設、當用戶端應用程式連線至儲存節點時、它們必須使用加密的 HTTPS 進行所有連線。您也可以選取、以啟用不太安全的 HTTP 連線 "啟用 HTTP 以進行儲存節點連線" Grid Manager 中的選項。例如、用戶端應用程式在非正式作業環境中測試與儲存節點的連線時、可能會使用HTTP。

> 為正式作業網格啟用 HTTP 時請務必小心、因為要求和回應將以未加密的方式傳送。

如果選擇了 *Enable HTTP for Storage Node connections （爲存儲節點連接啓用 HTTP ）選項，則客戶端必須使用不同於 HTTPS 使用的端口。

在**Swift API**組態中測試連線

您可以使用Swift CLI來測試與StorageGRID 該系統的連線、並驗證您是否可以讀取物件並將物件寫入系統。

開始之前

- 您必須下載並安裝python swiftClient、Swift命令列用戶端。

  "SwiftStack：Python-swiftClient"

- 您必須在StorageGRID 整個作業系統中擁有Swift租戶帳戶。

關於這項工作

如果您尚未設定安全性、則必須新增 `--insecure` 標記至每個命令。

步驟

1. 查詢StorageGRID 資訊URL以進行您的NetApp Swift部署：

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/info
capabilities
```

這足以測試您的Swift部署是否正常運作。若要儲存物件以進一步測試帳戶組態、請繼續執行其他步驟。

2. 將物件放入容器：

```
touch test_object
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
upload test_container test_object
--object-name test_object
```

3. 取得容器以驗證物件：

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
list test_container
```

4. 刪除物件：

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
delete test_container test_object
```

5. 刪除容器：

```
swift
-U `<_Tenant_Account_ID:Account_User_Name_>`
-K `<_User_Password_>`
-A `\https://<_FQDN_ | _IP_>:<_Port_>/auth/v1.0'
delete test_container
```

相關資訊

"建立及設定Swift租戶帳戶"

"設定REST API的安全性"

Swift REST API支援的作業

此系統支援OpenStack Swift API的大部分作業。StorageGRID在將Swift REST API用戶端與StorageGRID NetApp整合之前、請先檢閱帳戶、容器和物件作業的實作詳細資料。

支援的作業StorageGRID

支援下列Swift API作業：

- "帳戶營運"
- "容器作業"
- "物件作業"

所有作業的通用回應標頭

根據OpenStack Swift Object Storage API v1的定義、此系統可實作所有支援作業的通用標頭。StorageGRID

相關資訊

"OpenStack：物件儲存API"

支援的Swift API端點

支援下列Swift API端點：資訊URL、驗證URL及儲存URL。StorageGRID

資訊URL

您可以StorageGRID 使用/info路徑、向Swift基礎URL發出Get要求、藉此判斷執行過程的功能和限制。

`https://FQDN | Node IP:Swift Port/info/`

在要求中：

- *FQDN* 為完整網域名稱。
- *Node IP* 是StorageGRID 指儲存節點的IP位址、或是指位於該網路上的閘道節點。

- *Swift Port* 是儲存節點或閘道節點上用於Swift API連線的連接埠編號。

例如、下列資訊URL會向IP位址為10.99.106.103且使用連接埠18083的儲存節點要求資訊。

```
https://10.99.106.103:18083/info/
```

回應內容包括Swift實作的功能、即Json字典。用戶端工具可剖析Json回應、判斷實作的功能、並將其作為後續儲存作業的限制。

Swift的支援功能可未經驗證存取資訊URL。StorageGRID

驗證URL

用戶端可以使用Swift驗證URL來驗證租戶帳戶使用者身分。

```
https://FQDN | Node IP:Swift Port/auth/v1.0/
```

您必須在中提供租戶帳戶ID、使用者名稱和密碼作為參數 `X-Auth-User` 和 `X-Auth-Key` 要求標頭、如下所示：

```
X-Auth-User: Tenant_Account_ID:Username

X-Auth-Key: Password
```

在要求標頭中：

- *Tenant_Account_ID* 是StorageGRID 建立Swift租戶時由支援人員指派的帳戶ID。這是租戶管理員登入頁面上使用的相同租戶帳戶ID。
- *Username* 是租戶管理程式中建立的租戶使用者名稱。此使用者必須屬於具有Swift Administrator權限的群組。租戶的根使用者無法設定為使用 Swift REST API 。

  如果租戶帳戶已啟用Identity Federation、請提供LDAP伺服器的聯盟使用者名稱和密碼。或者、提供LDAP使用者的網域名稱。例如：

  ```
  X-Auth-User: Tenant_Account_ID:Username@Domain_Name
  ```

- *Password* 是租戶使用者的密碼。使用者密碼是在租戶管理程式中建立及管理的。

成功驗證要求的回應會傳回儲存URL和驗證權杖、如下所示：

```
X-Storage-Url: https://FQDN | Node_IP:Swift_Port/v1/Tenant_Account_ID

X-Auth-Token: token

X-Storage-Token: token
```

根據預設、權杖自產生時間起24小時內有效。

會針對特定租戶帳戶產生權杖。一個帳戶的有效權杖並未授權使用者存取另一個帳戶。

儲存URL

用戶端應用程式可以發出Swift REST API呼叫、以便針對閘道節點或儲存節點執行支援的帳戶、容器和物件作業。儲存要求會被定址至驗證回應中傳回的儲存URL。要求也必須包含從驗證要求傳回的X-auth-Token標頭和值。

```
https://FQDN | IP:Swift_Port/v1/Tenant_Account_ID

[/container][/object]

X-Auth-Token: token
```

有些儲存回應標頭包含使用量統計資料、可能無法反映最近修改物件的準確數字。這些標頭可能需要幾分鐘的時間才能顯示準確的數字。

下列帳戶和容器作業的回應標頭是包含使用統計資料的範例：

- `X-Account-Bytes-Used`
- `X-Account-Object-Count`
- `X-Container-Bytes-Used`
- `X-Container-Object-Count`

相關資訊

"設定租戶帳戶和連線"

"帳戶營運"

"容器作業"

"物件作業"

帳戶營運

下列Swift API作業會在帳戶上執行。

取得帳戶

此作業會擷取與帳戶和帳戶使用量統計資料相關的容器清單。

需要下列要求參數：

- `Account`

需要下列要求標頭：

- `X-Auth-Token`

下列支援的要求查詢參數為選用項目：

- `Delimiter`

- End_marker
- Format
- Limit
- Marker
- Prefix

如果找到帳戶且沒有容器或容器清單為空白、成功執行會傳回下列標頭「HTTP / 1.1 204無內容」回應；如果找到帳戶且容器清單為非空白、則會傳回「HTTP / 1.1 200 OK」回應：

- Accept-Ranges
- Content-Length
- Content-Type
- Date
- X-Account-Bytes-Used
- X-Account-Container-Count
- X-Account-Object-Count
- X-Timestamp
- X-Trans-Id

總公司帳戶

此作業會從Swift帳戶擷取帳戶資訊和統計資料。

需要下列要求參數：

- Account

需要下列要求標頭：

- X-Auth-Token

成功執行會傳回下列標頭、並顯示「HTTP / 1.1 204無內容」回應：

- Accept-Ranges
- Content-Length
- Date
- X-Account-Bytes-Used
- X-Account-Container-Count
- X-Account-Object-Count
- X-Timestamp
- X-Trans-Id

相關資訊

"監控與稽核作業"

容器作業

每個Swift帳戶最多可支援1、000個容器。StorageGRID下列Swift API作業會在Container上執行。

刪除容器

此作業會從StorageGRID Swift帳戶的一個空容器中移除一個位在整個系統中的容器。

需要下列要求參數：

- `Account`
- `Container`

需要下列要求標頭：

- `X-Auth-Token`

成功執行會傳回下列標頭、並顯示「HTTP / 1.1 204無內容」回應：

- `Content-Length`
- `Content-Type`
- `Date`
- `X-Trans-Id`

取得**Container**

此作業會擷取與容器相關聯的物件清單、以及StorageGRID 物件統計資料和元資料在一個作業系統中。

需要下列要求參數：

- `Account`
- `Container`

需要下列要求標頭：

- `X-Auth-Token`

下列支援的要求查詢參數為選用項目：

- `Delimiter`
- `End_marker`
- `Format`
- `Limit`

- Marker
- Path
- Prefix

成功執行會傳回下列標頭、並顯示「HTTP / 1.1 200成功」或「HTTP / 1.1 204無內容」回應：

- Accept-Ranges
- Content-Length
- Content-Type
- Date
- X-Container-Bytes-Used
- X-Container-Object-Count
- X-Timestamp
- X-Trans-Id

頭端容器

此作業會從StorageGRID 作業系統擷取Container統計資料和中繼資料。

需要下列要求參數：

- Account
- Container

需要下列要求標頭：

- X-Auth-Token

成功執行會傳回下列標頭、並顯示「HTTP / 1.1 204無內容」回應：

- Accept-Ranges
- Content-Length
- Date
- X-Container-Bytes-Used
- X-Container-Object-Count
- X-Timestamp
- X-Trans-Id

放入容器

此作業會在StorageGRID 一個不穩定系統中建立帳戶的容器。

需要下列要求參數：

- `Account`
- `Container`

需要下列要求標頭：

- `X-Auth-Token`

成功執行會傳回下列標頭、並顯示「HTTP / 1.1 201已建立」或「HTTP / 1.1 2已接受」（如果此帳戶下已存在該容器）回應：

- `Content-Length`
- `Date`
- `X-Timestamp`
- `X-Trans-Id`

Container名稱必須在StorageGRID lsname命名空間中是唯一的。如果該容器存在於其他帳戶下、則會傳回下列標頭：「HTTP / 1.1 409衝突」。

相關資訊

"監控與稽核作業"

物件作業

下列Swift API作業會在物件上執行。您可以在中追蹤這些作業 "StorageGRID 稽核記錄"。

刪除物件

此作業會從StorageGRID 作業系統刪除物件的內容和中繼資料。

需要下列要求參數：

- `Account`
- `Container`
- `Object`

需要下列要求標頭：

- `X-Auth-Token`

成功執行會傳回下列回應標頭與 `HTTP/1.1 204 No Content` 回應：

- `Content-Length`
- `Content-Type`
- `Date`
- `X-Trans-Id`

處理刪除物件要求時StorageGRID 、功能區會嘗試立即從所有儲存位置移除物件的所有複本。如果成

功、StorageGRID 則會立即將回應傳回給用戶端。如果無法在 30 秒內移除所有複本（例如、因為某個位置暫時無法使用）、 StorageGRID 會將複本排入佇列以供移除、然後表示用戶端成功。

如需詳細資訊、請參閱 "如何刪除物件"。

Get物件

此作業會擷取物件內容、並從StorageGRID 一套系統取得物件中繼資料。

需要下列要求參數：

- `Account`
- `Container`
- `Object`

需要下列要求標頭：

- `X-Auth-Token`

以下是選用的要求標頭：

- `Accept-Encoding`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`
- `Range`

成功執行會傳回下列標頭與 `HTTP/1.1 200 OK` 回應：

- `Accept-Ranges`
- `Content-Disposition`、僅在發生時傳回 `Content-Disposition` 已設定中繼資料
- `Content-Encoding`、僅在發生時傳回 `Content-Encoding` 已設定中繼資料
- `Content-Length`
- `Content-Type`
- `Date`
- `ETag`
- `Last-Modified`
- `X-Timestamp`
- `X-Trans-Id`

標頭物件

此作業會從StorageGRID 作業系統擷取擷取物件的中繼資料和屬性。

需要下列要求參數：

- `Account`
- `Container`
- `Object`

需要下列要求標頭：

- `X-Auth-Token`

成功執行會傳回下列標頭、並顯示「HTTP / 1.1 200 OK」回應：

- `Accept-Ranges`
- `Content-Disposition`、僅在發生時傳回 `Content-Disposition` 已設定中繼資料
- `Content-Encoding`、僅在發生時傳回 `Content-Encoding` 已設定中繼資料
- `Content-Length`
- `Content-Type`
- `Date`
- `ETag`
- `Last-Modified`
- `X-Timestamp`
- `X-Trans-Id`

放置物件

此作業會以資料和中繼資料建立新物件、或以StorageGRID 資料和中繼資料取代現有物件。

支援最多5 TiB（5、497、558、13880位元組）的物件。StorageGRID

> 衝突的用戶端要求（例如兩個寫入同一個金鑰的用戶端）會以「最新致勝」的方式解決。「最新致勝」評估的時間取決於StorageGRID VMware系統何時完成指定的要求、而非Swift用戶端何時開始作業。

需要下列要求參數：

- `Account`
- `Container`
- `Object`

需要下列要求標頭：

- `X-Auth-Token`

以下是選用的要求標頭：

- `Content-Disposition`
- `Content-Encoding`

  請勿使用分塊 `Content-Encoding` 如果套用至物件的ILM規則會根據大小來篩選物件、並在擷取時使用同步放置（擷取行為的平衡或嚴格選項）。

- `Transfer-Encoding`

  請勿使用壓縮或分塊的方式 `Transfer-Encoding` 如果套用至物件的ILM規則會根據大小來篩選物件、並在擷取時使用同步放置（擷取行為的平衡或嚴格選項）。

- `Content-Length`

  如果ILM規則會根據大小篩選物件、並在擷取時使用同步位置、則必須指定 `Content-Length`。

  > 如果您未遵循下列準則 `Content-Encoding`、 `Transfer-Encoding`和 `Content-Length`、StorageGRID 必須先儲存物件、才能判斷物件大小並套用ILM規則。換句話說StorageGRID 、在擷取時、必須預設使用功能來建立物件的過渡複本。也就是StorageGRID 、對於內嵌行為、必須使用雙重認可選項。

  如需同步放置和 ILM 規則的詳細資訊、請參閱 "用於擷取的資料保護選項"。

- `Content-Type`
- `ETag`
- `X-Object-Meta-<name\>` （物件相關中繼資料）

  如果您要使用 * 使用者定義的建立時間 * 選項做為 ILM 規則的參考時間、則必須將該值儲存在名為的使用者定義標頭中 `X-Object-Meta-Creation-Time`。例如：

  ```
  X-Object-Meta-Creation-Time: 1443399726
  ```

  此欄位自1970年1月1日起計算為秒數。

- `X-Storage-Class: reduced_redundancy`

  如果符合擷取物件的ILM規則指定「雙重認可」或「平衡」的擷取行為、則此標頭會影響StorageGRID 到所建立的物件複本數量。

  - 雙重提交：如果ILM規則指定擷取行為的雙重提交選項、StorageGRID 則會在擷取物件時建立單一的過渡複本（單一提交）。
  - *Balanced * ：如果 ILM 規則指定 Balanced 選項、則 StorageGRID 只會在系統無法立即製作規則中指定的所有複本時、才製作單一的臨時複本。如果能夠執行同步放置、則此標頭不會有任何影響。StorageGRID

。 `reduced_redundancy` 當符合物件的ILM規則建立單一複寫複本時、最好使用標頭。在此案例中、請使用 `reduced_redundancy` 免除在每次擷取作業中不必要地建立和刪除額外的物件複本。

使用 `reduced_redundancy` 在其他情況下不建議使用標頭、因為它會增加擷取期間物件資料遺失的風險。例如、如果單一複本一開始儲存在無法進行ILM評估的儲存節點上、則可能會遺失資料。

> 在任何時間段只複寫一個複本、會使資料面臨永久遺失的風險。如果只有一個物件複寫複本存在、則當儲存節點故障或發生重大錯誤時、該物件就會遺失。在升級等維護程序期間、您也會暫時失去物件的存取權。

請注意、指定 `reduced_redundancy` 只會影響第一次擷取物件時所建立的複本數量。當物件由作用中的ILM原則評估時、不會影響物件的複本份數、也不會導致資料儲存在StorageGRID 較低層級的資料冗餘環境中。

成功執行會傳回下列標頭、並顯示「已建立的HTTP/1.1 201」回應：

- `Content-Length`
- `Content-Type`
- `Date`
- `ETag`
- `Last-Modified`
- `X-Trans-Id`

選項要求

選項要求會檢查個別Swift服務的可用度。選項要求由URL中指定的儲存節點或閘道節點處理。

選項方法

例如、用戶端應用程式可以在儲存節點上向Swift連接埠發出選項要求、而無需提供Swift驗證認證、以判斷儲存節點是否可用。您可以使用此要求來監控或允許外部負載平衡器識別儲存節點何時當機。

搭配資訊URL或儲存URL使用時、options方法會傳回指定URL所支援的動詞清單（例如、標頭、Get、選項及PUT）。選項方法無法與驗證 URL 搭配使用。

需要下列要求參數：

- `Account`

下列要求參數為選用項目：

- `Container`
- `Object`

成功執行會傳回下列標頭、並顯示「HTTP / 1.1 204無內容」回應。儲存URL的選項要求不需要目標存在。

- `Allow` （特定URL支援的動詞清單、例如：標頭、GET、選項、並投入）

- `Content-Length`
- `Content-Type`
- `Date`
- `X-Trans-Id`

相關資訊

"支援的Swift API端點"

Swift API作業的錯誤回應

瞭解可能的錯誤回應有助於疑難排解作業。

當作業期間發生錯誤時、可能會傳回下列HTTP狀態代碼：

Swift錯誤名稱	**HTTP**狀態
AccountNameTooLong、ContainerNameTooLong、HeaderTooBig、InvalidContainerName、InvalidRequest、 InvalidURI、Metadata NameTooLong、Metadata ValueTooBig、MISingSecurityHeader、ObjectNameTooLong、 TooManyContainers,TooManyMetadata項目,TotalMetadata TooLarg	400個錯誤要求
ACCESSDENIED	403禁止
ContainerNotEmpty、ContainerAlreadyExiss	衝突
內部錯誤	500內部伺服器錯誤
InvalidRang	無法滿足416個要求的範圍
方法未允許	不允許使用405方法
內容長度	需要411長度
NotFound	找不到404
未實作	501未實作
預先條件失敗	412先決條件失敗
資源NotFound	找不到404
未獲授權	401未獲授權

Swift錯誤名稱	HTTP狀態
UnprocessableEntity	無法處理的實體

Swift REST API作業StorageGRID

Swift REST API上新增了特定StorageGRID 於該系統的作業。

取得Container一致性要求

"一致性控管" 在物件的可用度與這些物件在不同儲存節點和站台之間的一致性之間取得平衡。「Get Container一致性」要求可讓您判斷要套用至特定容器的一致性層級。

申請

要求HTTP標頭	說明
X-AUTH-Token	指定要用於要求的帳戶Swift驗證權杖。
X-ntap-sg- 一致性	指定要求類型、其中 `true` =取得容器一致性、以及 `false` =取得容器。
主機	要求導向的主機名稱。

申請範例

```
GET /v1/28544923908243208806/Swift container
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29
x-ntap-sg-consistency: true
Host: test.com
```

回應

回應HTTP標頭	說明
日期	回應的日期和時間。
連線	是否開啟或關閉與伺服器的連線。
X-trans-ID	要求的唯一交易識別碼。
內容長度	回應本文的長度。

回應**HTTP**標頭	說明
X-ntap-sg- 一致性	套用至容器的一致性控制層級。支援下列值： 全部：所有節點都會立即接收資料、否則要求將會失敗。 強式全域：保證所有站台所有用戶端要求的寫入後讀取一致性。 • Strong站台*：保證站台內所有用戶端要求的寫入後讀取一致性。 • 新寫入後讀取 * ：（預設）提供新物件的寫入後讀取一致性、以及物件更新的最終一致性。提供高可用度與資料保護保證。建議大多數情況下使用。 • 可用 * ：提供新物件和物件更新的最終一致性。對於 S3 貯體、請僅視需要使用（例如、包含很少讀取的記錄值之貯體、或用於對不存在的金鑰執行 head 或 Get 作業）。S3 FabricPool 儲存區不支援。

回應範例

```
HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
x-ntap-sg-consistency: strong-site
```

放置容器一致性要求

放置容器一致性要求可讓您指定要套用至容器上執行之作業的一致性層級。根據預設、新的容器是使用「全新寫入後的讀取」一致性層級來建立。

申請

要求**HTTP**標頭	說明
X-AUTH-Token	用於要求的帳戶Swift驗證權杖。

要求**HTTP**標頭	說明
X-ntap-sg- 一致性	套用至容器作業的一致性控制層級。支援下列值： 全部：所有節點都會立即接收資料、否則要求將會失敗。 強式全域：保證所有站台所有用戶端要求的寫入後讀取一致性。 • Strong站台*：保證站台內所有用戶端要求的寫入後讀取一致性。 • 新寫入後讀取 * ：（預設）提供新物件的寫入後讀取一致性、以及物件更新的最終一致性。提供高可用度與資料保護保證。建議大多數情況下使用。 • 可用 * ：提供新物件和物件更新的最終一致性。對於 S3 貯體、請僅視需要使用（例如、包含很少讀取的記錄值之貯體、或用於對不存在的金鑰執行 head 或 Get 作業）。S3 FabricPool 儲存區不支援。
`Host`	要求導向的主機名稱。

一致性控制與**ILM**規則如何互動、以影響資料保護

任您選擇 "一致性控制" 而且您的 ILM 規則會影響物件的保護方式。這些設定可以互動。

例如、儲存物件時使用的一致性控制項會影響物件中繼資料的初始放置、而 "擷取行為" 為 ILM 規則選取會影響物件複本的初始放置位置。由於支援對象的中繼資料及其資料、因此需要同時存取才能滿足用戶端要求、因此針對一致性層級和擷取行為選擇相符的保護層級、可提供更好的初始資料保護、並提供更可預測的系統回應。StorageGRID

一致性控制和**ILM**規則如何互動的範例

假設您有一個雙站台網格、其中包含下列ILM規則和下列一致性層級設定：

- * ILM規則*：建立兩個物件複本、一個在本機站台、一個在遠端站台。選取嚴格的擷取行為。
- 一致性層級：「'trong-globat'（物件中繼資料會立即發佈至所有站台）。

當用戶端將物件儲存到網格時、StorageGRID 在成功傳回用戶端之前、功能區會同時複製物件並將中繼資料散佈到兩個站台。

在擷取最成功的訊息時、物件會受到完整保護、不會遺失。例如、如果在擷取後不久即遺失本機站台、則物件資料和物件中繼資料的複本仍存在於遠端站台。物件可完全擷取。

如果您改用相同的ILM規則和「站台」一致性層級、則用戶端可能會在物件資料複寫到遠端站台之後、收到成功訊息、但物件中繼資料才會散佈到該站台。在此情況下、物件中繼資料的保護層級與物件資料的保護層級不符。如果在擷取後不久本機站台便會遺失、則物件中繼資料將會遺失。無法擷取物件。

一致性層級與ILM規則之間的相互關係可能相當複雜。如需協助、請聯絡NetApp。

申請範例

```
PUT /v1/28544923908243208806/_Swift container_
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29
x-ntap-sg-consistency: strong-site
Host: test.com
```

回應

回應**HTTP**標頭	說明
`Date`	回應的日期和時間。
`Connection`	是否開啟或關閉與伺服器的連線。
`X-Trans-Id`	要求的唯一交易識別碼。
`Content-Length`	回應本文的長度。

回應範例

```
HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
```

設定**REST API**的安全性

您應該檢閱針對REST API實作的安全措施、並瞭解如何保護系統安全。

如何為**REST API**提供安全性**StorageGRID**

您應該瞭解StorageGRID 什麼是讓此系統為REST API實作安全性、驗證和授權。

使用下列安全措施。StorageGRID

- 如果已針對負載平衡器端點設定HTTPS、則用戶端與負載平衡器服務的通訊會使用HTTPS。

  當您 "設定負載平衡器端點"， HTTP 也可以選擇啟用。例如、您可能想要使用HTTP進行測試或其他非正式作業用途。

- 根據預設、 StorageGRID 會使用 HTTPS 與儲存節點進行用戶端通訊。

  （可選） "為這些連線啟用 HTTP"。例如、您可能想要使用HTTP進行測試或其他非正式作業用途。

- 支援使用TLS加密支援不支援的客戶端與StorageGRID 之通訊。

- 無論負載平衡器端點是設定為接受HTTP或HTTPS連線、網格內負載平衡器服務與儲存節點之間的通訊都會加密。
- 用戶端必須提供HTTP驗證標頭StorageGRID 給才能執行REST API作業。

安全性憑證與用戶端應用程式

用戶端可以直接連線至 Gateway 節點或管理節點上的負載平衡器服務、並直接連線至 Storage Node 。

在任何情況下、用戶端應用程式都可以使用網格管理員上傳的自訂伺服器憑證或StorageGRID 由該系統產生的憑證來建立TLS連線：

- 當用戶端應用程式連線至負載平衡器服務時、應用程式會使用針對用於建立連線的特定負載平衡器端點所設定的憑證來執行此作業。每個端點都有自己的憑證、可以是由網格管理員上傳的自訂伺服器憑證、也可以是網格管理員StorageGRID 在設定端點時產生的憑證。
- 當用戶端應用程式直接連線至儲存節點時、它們會使用安裝 StorageGRID 系統（由系統憑證授權單位簽署）時為儲存節點產生的系統產生的伺服器憑證、 或是由網格管理員提供給網格的單一自訂伺服器憑證。

用戶端應設定為信任已簽署其用於建立TLS連線之任何憑證的憑證授權單位。

請參閱 "設定負載平衡器端點" 和 "新增單一自訂伺服器憑證" 適用於直接連線至儲存節點的 TLS 連線。

摘要

下表顯示S3和Swift REST API如何實作安全性問題：

安全問題	**REST API**的實作
連線安全性	TLS
伺服器驗證	由系統CA或系統管理員提供的自訂伺服器憑證簽署的X・509伺服器憑證
用戶端驗證	• S3：S3帳戶（存取金鑰ID和秘密存取金鑰） • Swift：Swift帳戶（使用者名稱和密碼）
用戶端授權	• S3：貯體所有權及所有適用的存取控制原則 • Swift：系統管理員角色存取

TLS程式庫支援的雜湊和加密演算法

支援一套有限的加密套件、用戶端應用程式可在建立傳輸層安全性（TLS）工作階段時使用。StorageGRID要配置加密算法，請轉至 * 配置 * > * 安全性 * > * 安全性設置 * ，然後選擇 *TLS 和 SSH 策略 * 。

支援的**TLS**版本

支援TLS 1.2和TLS 1.3。StorageGRID

不再支援SSLv3和TLS 1.1（或更早版本）。

相關資訊

"設定租戶帳戶和連線"

監控與稽核作業

您可以檢視整個網格或特定節點的交易趨勢、來監控用戶端作業的工作負載和效率。您可以使用稽核訊息來監控用戶端作業和交易。

監控物件擷取和擷取速率

您可以監控物件擷取和擷取速率、以及物件計數、查詢和驗證的度量。您可以檢視用戶端應用程式在StorageGRID 讀取、寫入及修改物件時、成功和失敗的嘗試次數。

步驟

1. 使用登入Grid Manager "支援的網頁瀏覽器"。
2. 在儀表板上、選取 * 效能 * > * S3 作業 * 或 * 效能 * > * Swift 作業 * 。

   本節概述StorageGRID 您的一套系統執行的用戶端作業數量。在過去兩分鐘內平均傳輸協定速率。

3. 選擇*節點*。
4. 在節點首頁（部署層級）中、按一下*負載平衡器*索引標籤。

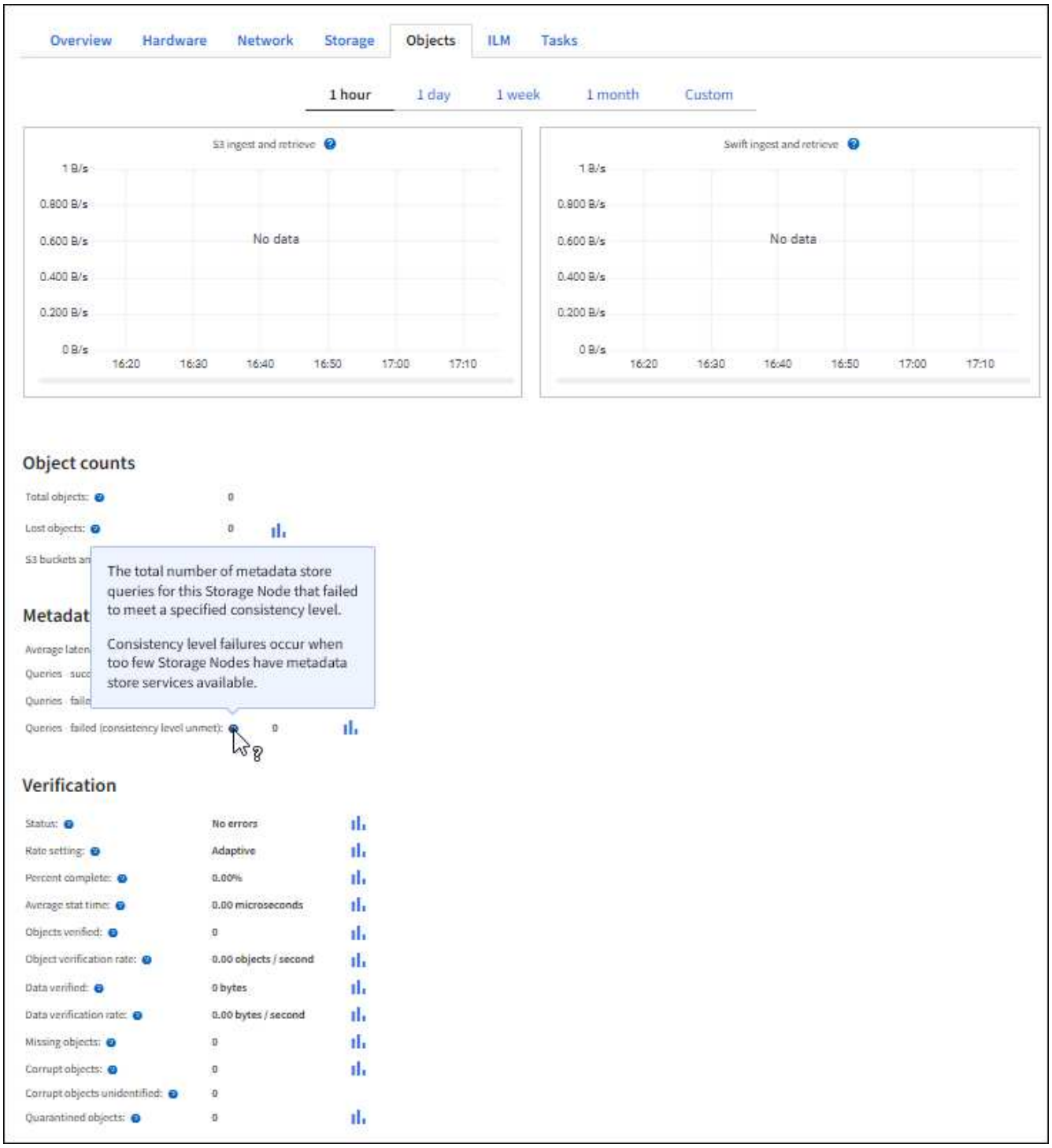
   這些圖表顯示了導向至網格內負載平衡器端點的所有用戶端流量趨勢。您可以選擇以小時、天、週、月或年為單位的時間間隔、 您也可以套用自訂時間間隔。

5. 在節點首頁（部署層級）中、按一下*物件*索引標籤。

   此圖表以StorageGRID 每秒位元組數和總位元組數顯示整個系統的擷取和擷取速率。您可以選擇以小時、天、週、月或年為單位的時間間隔、 您也可以套用自訂時間間隔。

6. 若要查看特定儲存節點的資訊、請從左側清單中選取節點、然後按一下「物件」索引標籤。

   此圖表顯示此儲存節點的物件擷取和擷取速率。此索引標籤也包含物件計數、查詢和驗證的度量。您可以按一下標籤來查看這些度量的定義。



7. 如果您想要更詳細的資料：
   a. 選取*支援*>*工具*>*網格拓撲*。
   b. 選擇*站台_*>*總覽*>*主選項*。

      「API作業」區段會顯示整個網格的摘要資訊。

   c. 選擇「儲存節點_」>「最大」>「用戶端應用程式_」>「總覽」>「主要」

      「作業」區段會顯示所選儲存節點的摘要資訊。

存取及檢閱稽核記錄

稽核訊息是StorageGRID 由支援服務產生、並儲存在文字記錄檔中。稽核日誌中的API專屬稽核訊息可提供關鍵的安全性、作業和效能監控資料、協助您評估系統的健全狀況。

開始之前

- 您必須擁有特定的存取權限。
- 您必須擁有 `Passwords.txt` 檔案：
- 您必須知道管理節點的IP位址。

關於這項工作

。 "作用中稽核記錄檔" 名稱 `audit.log`和儲存在管理節點上。

一天只要儲存一次作用中的audit.log檔案、就會啟動新的audit.log檔案。儲存檔案的名稱會以格式指出儲存時間 `yyyy-mm-dd.txt`。

一天後、儲存的檔案會以壓縮格式重新命名 `yyyy-mm-dd.txt.gz`，保留原始日期。

此範例顯示使用中的audit.log檔案、前一天的檔案（2018-04-15.TXT）、以及前一天的壓縮檔案 (`2018-04-14.txt.gz`) 。

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

步驟

1. 登入管理節點：
   a. 輸入下列命令： `ssh admin@primary_Admin_Node_IP`
   b. 輸入中所列的密碼 `Passwords.txt` 檔案：
   c. 輸入下列命令以切換至root： `su -`
   d. 輸入中所列的密碼 `Passwords.txt` 檔案：

      當您以root登入時、提示會從變更 `$` 至 `#`。
2. 移至包含稽核記錄檔的目錄：`cd /var/local/audit/export`
3. 視需要檢視目前或已儲存的稽核記錄檔。

在稽核記錄中追蹤的**Swift**作業

所有成功的儲存刪除、取得、主管、張貼和放置作業都會在中追蹤 "StorageGRID 稽核記錄"。不會記錄故障、也不會記錄資訊、驗證或選項要求。

系統會追蹤下列 Swift 作業的資訊。

帳戶營運

- "取得帳戶"
- "總公司帳戶"

容器作業

- "刪除容器"
- "取得Container"
- "頭端容器"
- "放入容器"

物件作業

- "刪除物件"
- "Get物件"
- "標頭物件"
- "放置物件"