使用租戶帳戶
StorageGRID 11.7

NetApp
April 12, 2024

目錄

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。

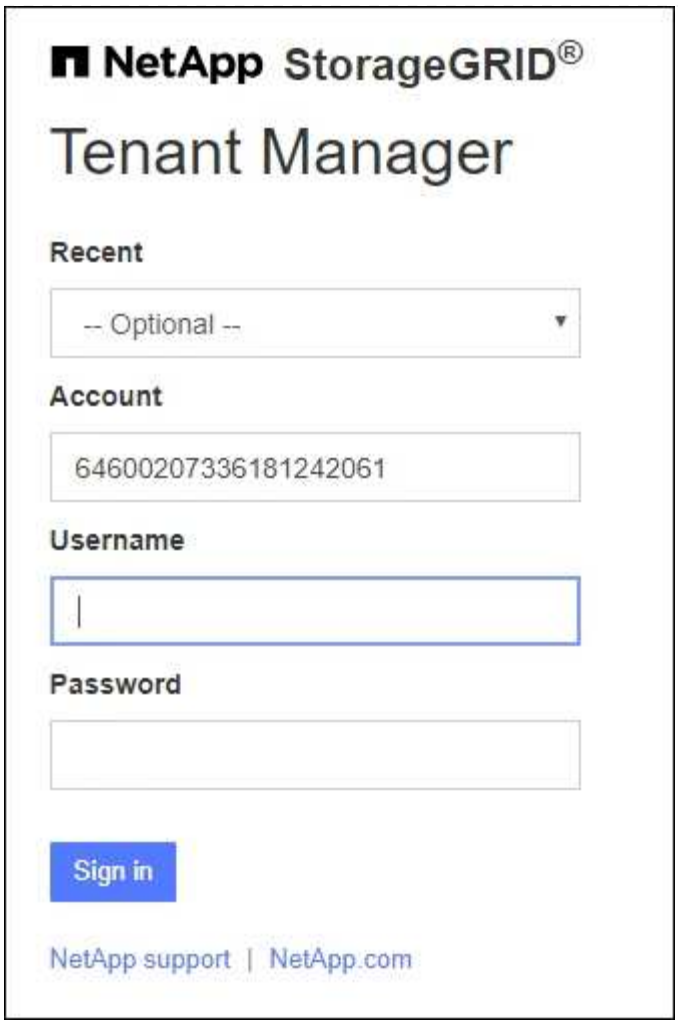
   顯示的登入畫面取決於您輸入的 URL 、以及是否已針對 StorageGRID 設定單一登入（ SSO ）。

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*。

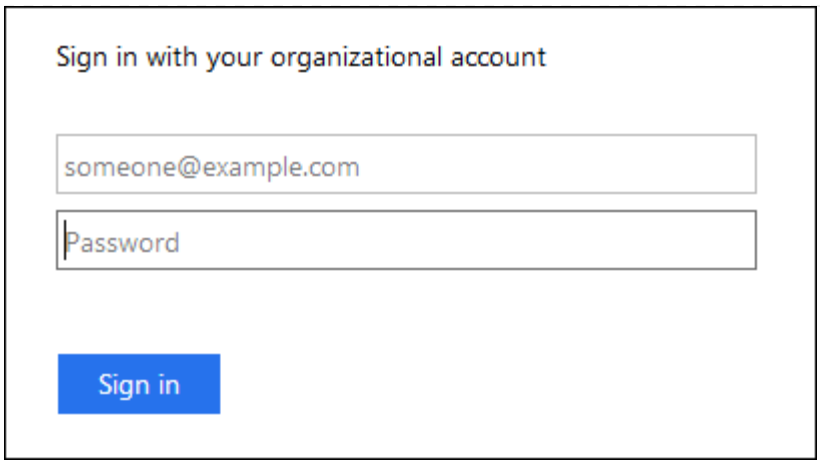
租戶管理器儀表板即會出現。

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。

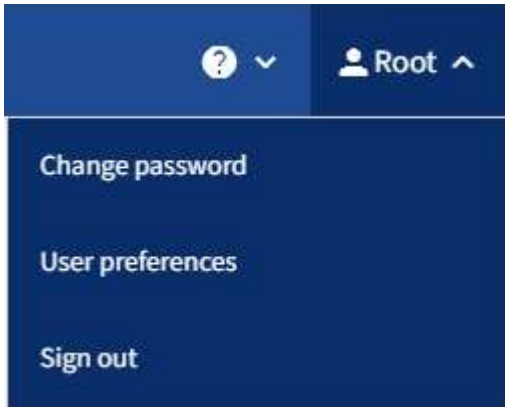
登出租戶管理程式

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*。

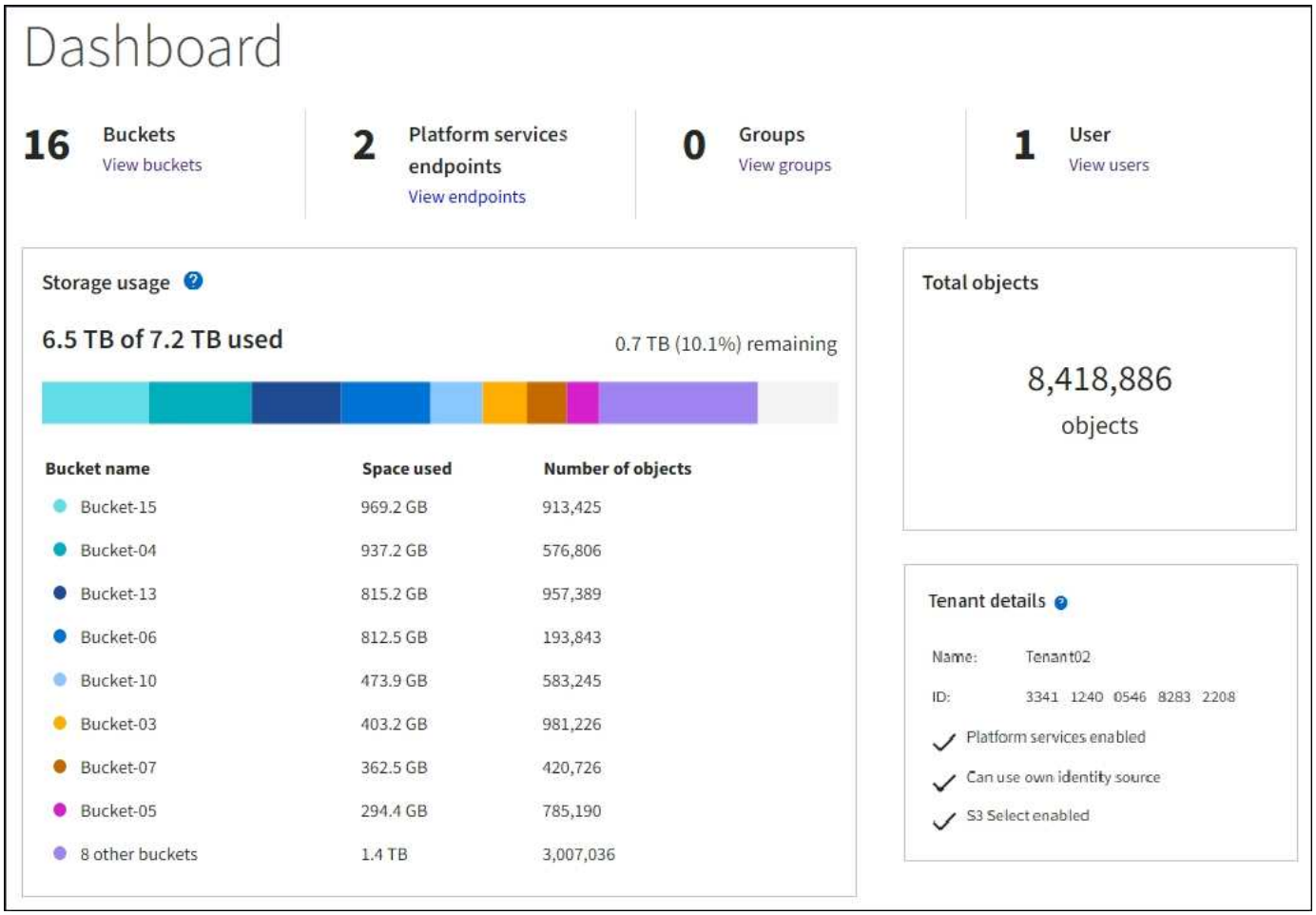
如果已啟用SSO、而且您也已登入Grid Manager、您也必須登出Grid Manager以登出SSO。

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。

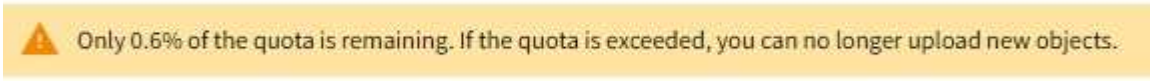
若要變更租戶管理程式中顯示的儲存值單位、請選取租戶管理程式右上角的使用者下拉式清單、然後選取 * 使用者偏好 * 。

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：

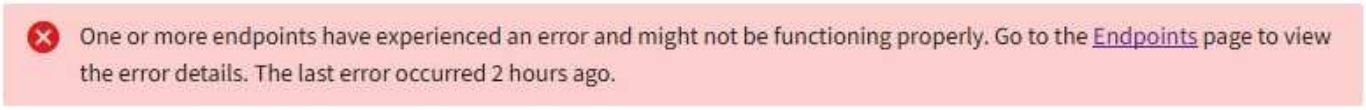
如果已使用90%以上的租戶配額、則會觸發*租戶配額使用量高*警示。執行警示的建議動作。



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。

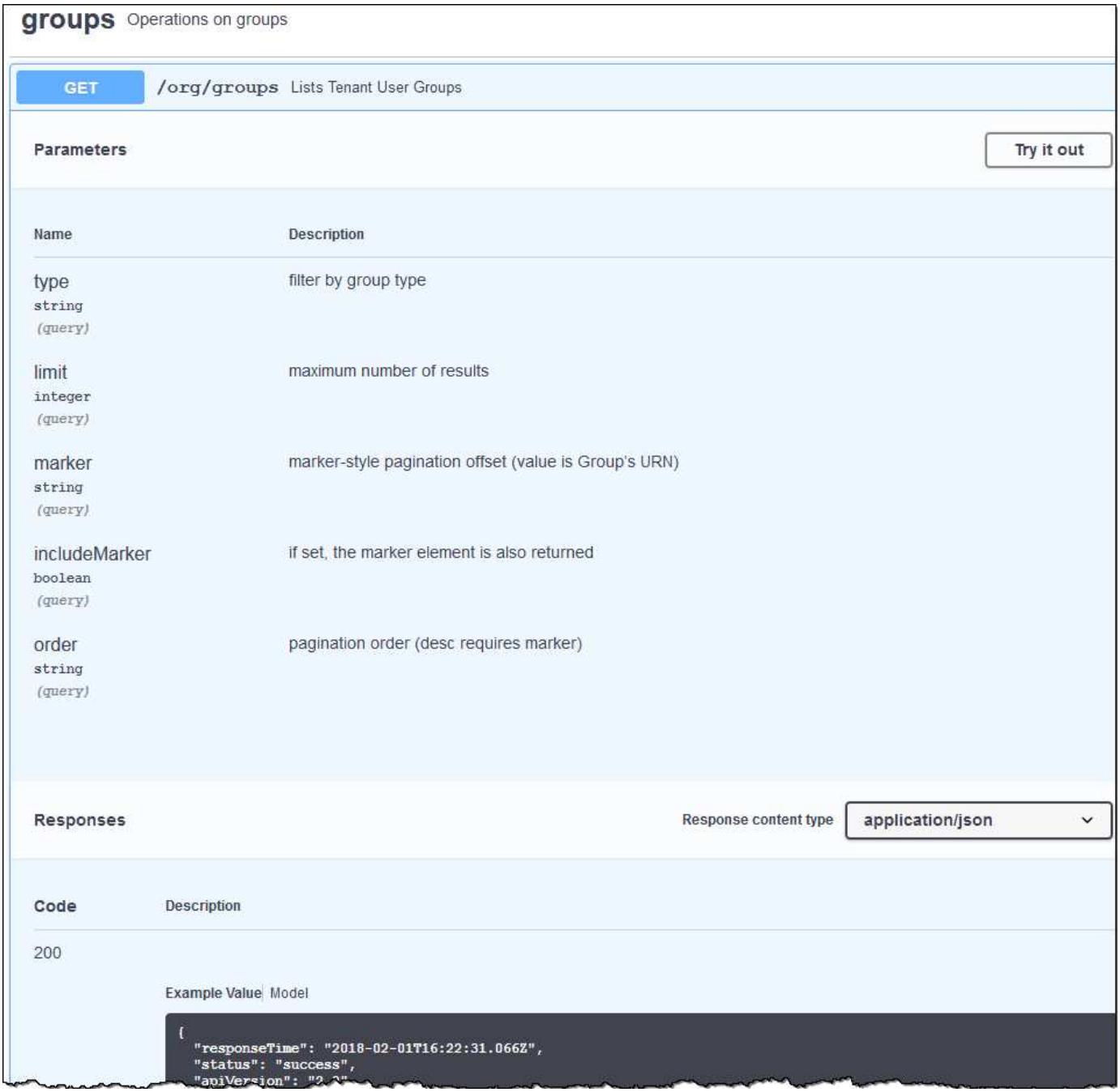
如需改善驗證安全性的資訊、請參閱 "防止跨網站要求偽造"。

> 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
  ]
}
```

指定要申請的**API**版本

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

複製租戶群組和使用者

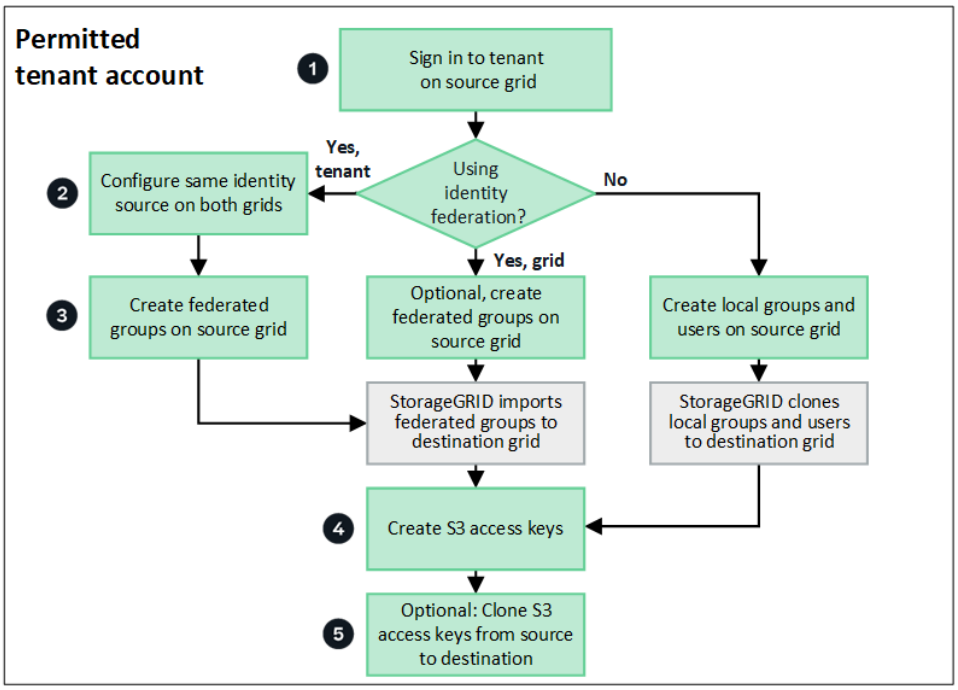
如果新租戶有使用網格同盟連線的權限、則該租戶在建立時會從一個 StorageGRID 系統複寫到另一個 StorageGRID 系統。複寫租戶之後、任何新增至來源租戶的群組和使用者都會複製到目的地租戶。

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"。

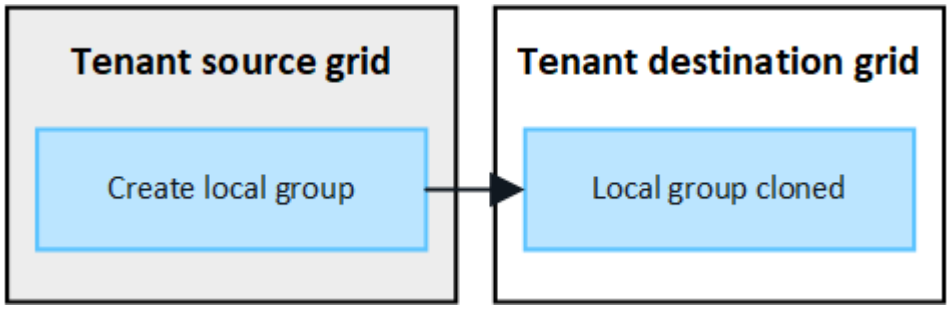
如何複製群組、使用者和 **S3** 存取金鑰？

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"。

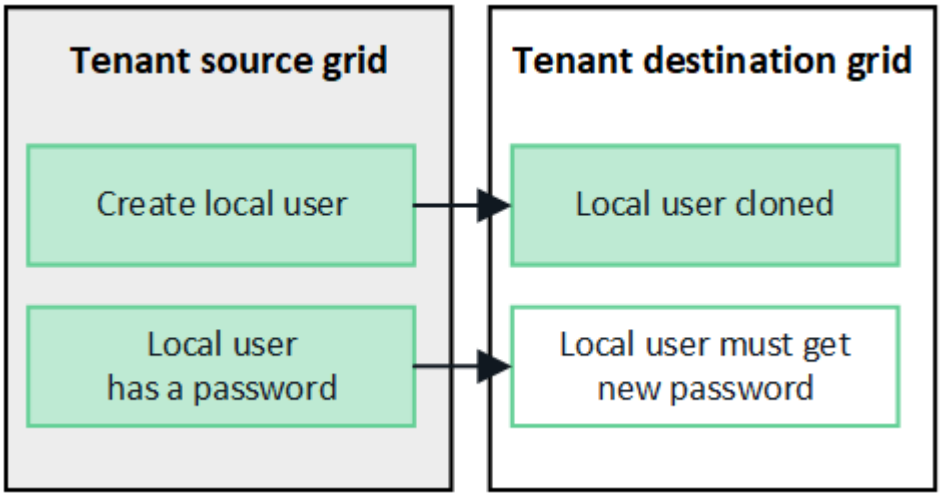


當您在來源網格上建立本機群組時所選取的任何使用者、都不會被複製到目的地網格時納入其中。因此、建立群組時請勿選取使用者。而是在建立使用者時選取群組。

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"。

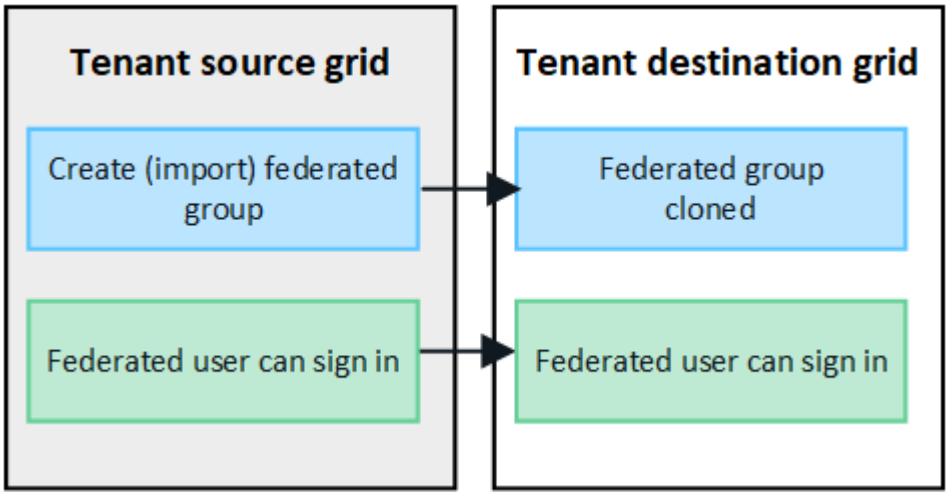


複製在來源網格上建立的同盟群組

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。

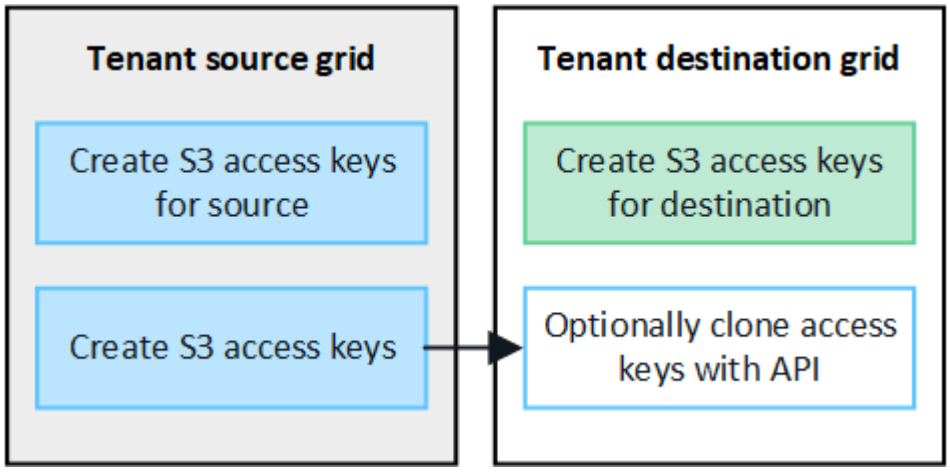


S3 存取金鑰可以手動複製

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：

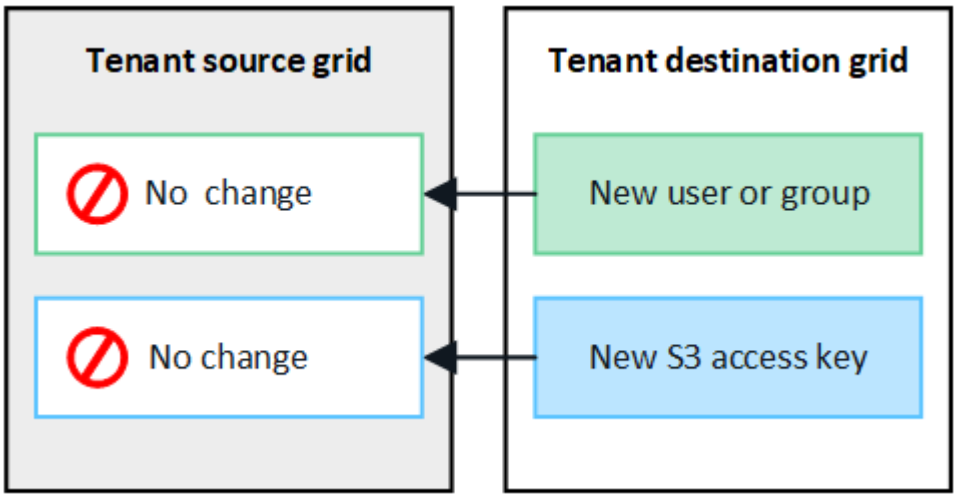
- 如果您不需要對每個網格使用相同的按鍵、您可以 "建立您自己的存取金鑰" 或 "建立其他使用者的存取金鑰" 在每個網格上。
- 如果您需要在兩個網格上使用相同的金鑰、您可以在來源網格上建立金鑰、然後使用 Tenant Manager API 手動建立金鑰 "複製金鑰" 至目的地網格。



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

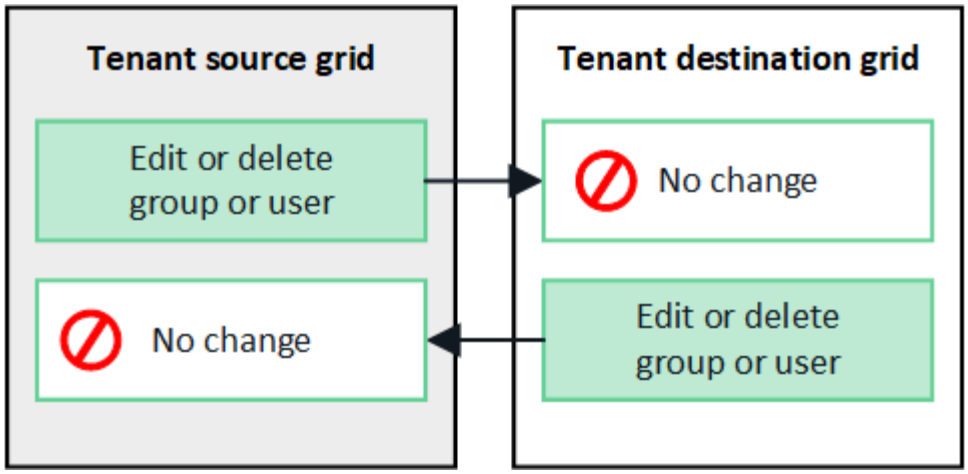
只會從租戶的來源網格到租戶的目的地網格進行複製。如果您在租戶的目的地網格上建立或匯入群組和使用者、StorageGRID 將不會將這些項目複製回租戶的來源網格。



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。

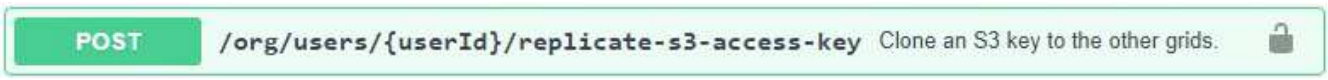
步驟

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。

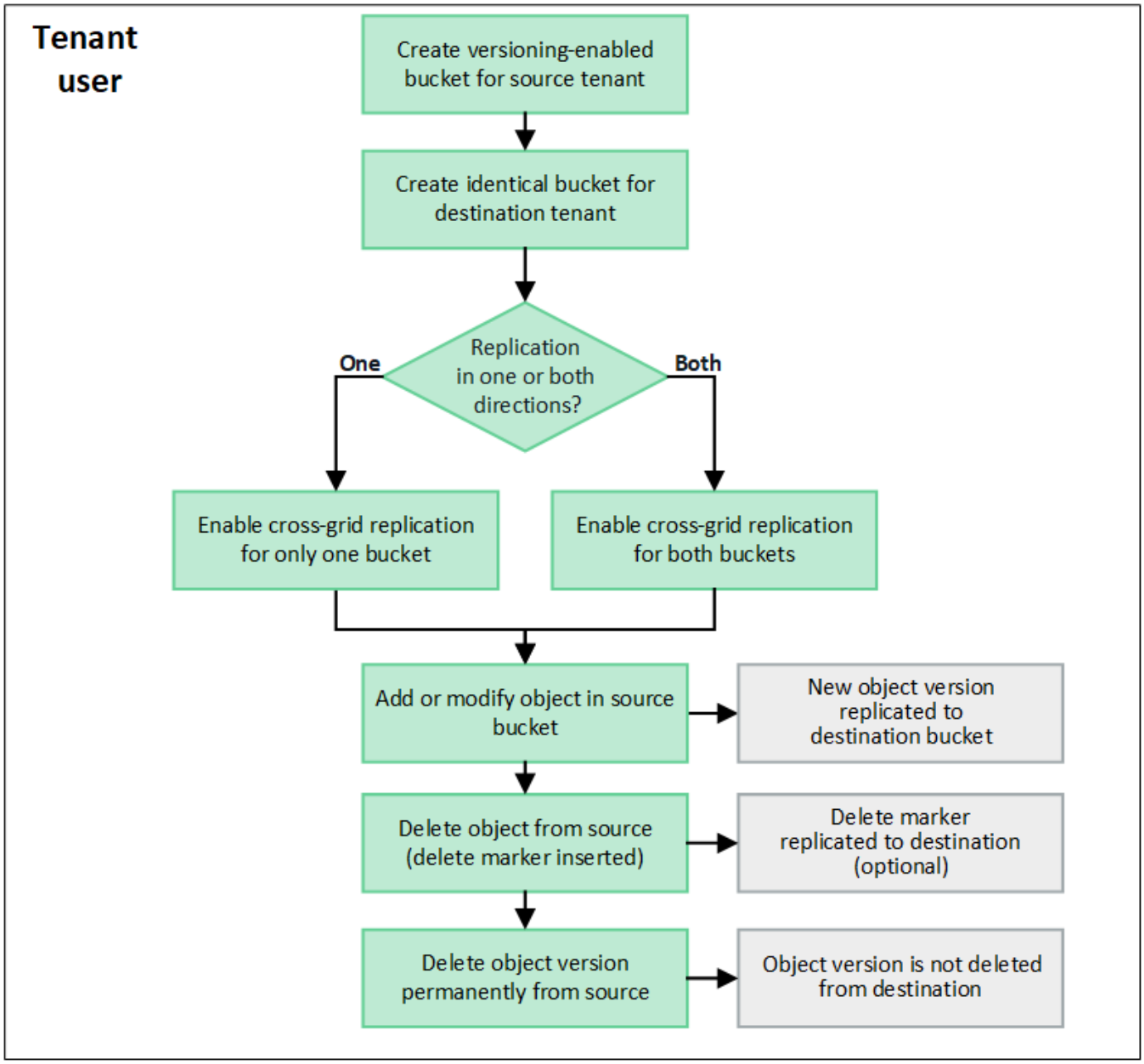
8. 如果金鑰即將過期、請以 ISO 8601 資料時間格式的字串形式、將 * Expires* 的範例項目取代為過期日期和時間（例如、 `2023-02-28T22:46:33-08:00`）。如果金鑰不會過期、請輸入 * null * 作為 * Expires* 項目的值（或移除 * Expires* 行及前面的逗號）。
9. 選擇*執行*。
10. 確認伺服器回應碼為 **204** 、表示金鑰已成功複製到目的地網格。

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。



設定跨網格複寫

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。

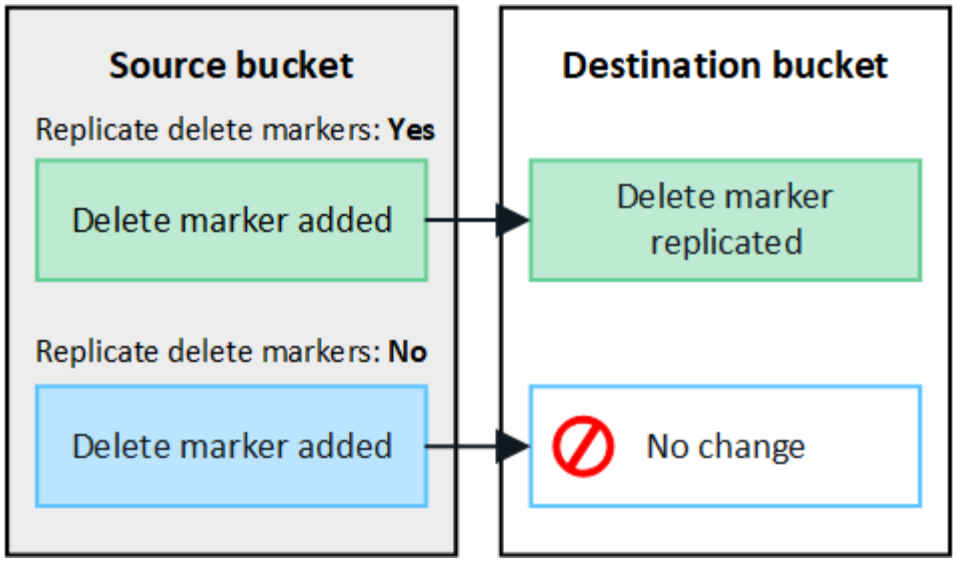
   b. 請依照的指示進行 "建立 S3 儲存貯體"。
   c. 在 * 管理物件設定 * 索引標籤上、選取 * 啟用物件版本設定 * 。
   d. 如果您的 StorageGRID 系統已啟用 S3 物件鎖定、請勿啟用儲存貯體的 S3 物件鎖定。
   e. 選取*建立桶*。
   f. 選擇*完成*。
2. 重複這些步驟、在 Grid Federation 連線的其他網格上、為相同的租戶帳戶建立相同的貯體。

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：

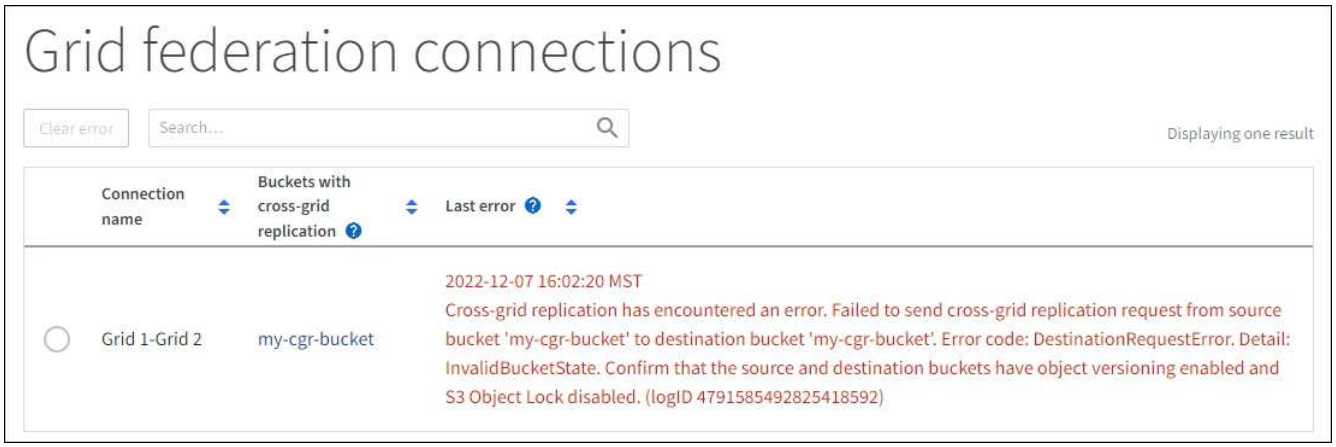
- 找不到來源物件版本。
- 找不到來源貯體。
- 目的地貯體已刪除。
- 目的地貯體是由不同的帳戶重新建立。
- 目的地貯體已暫停版本設定。
- 目的地貯體是由相同的帳戶重新建立、但現在已取消版本管理。

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。

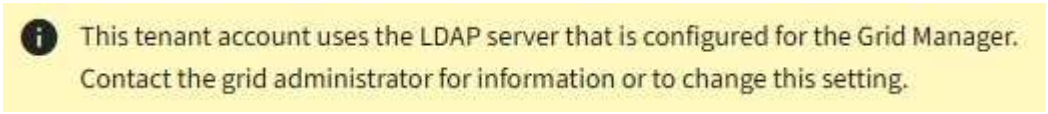
  如果您想使用未列出的LDAP v3服務、請聯絡技術支援部門。

- 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。

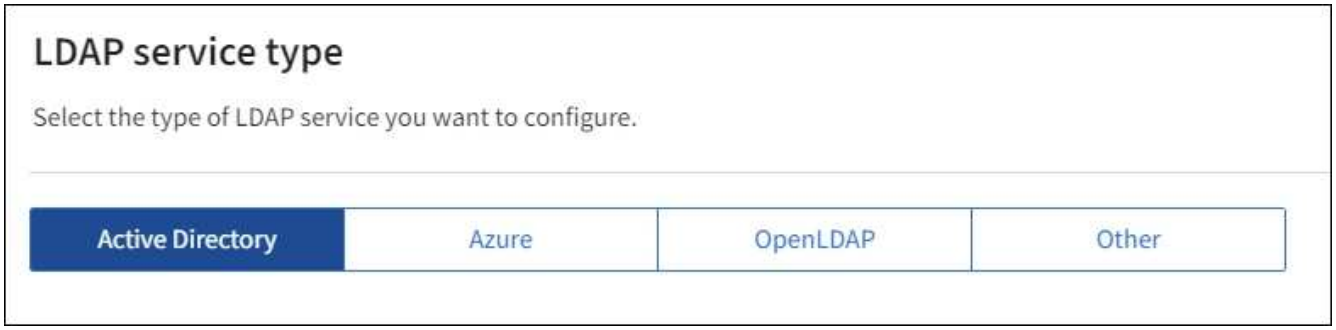


輸入組態

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。

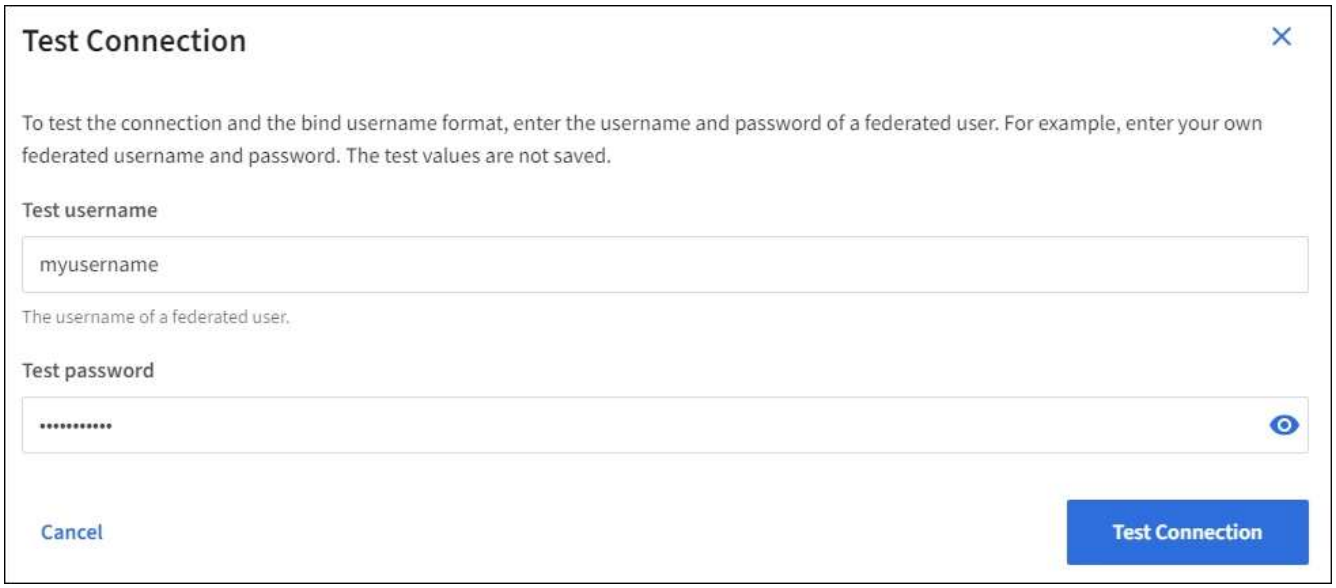
測試連線並儲存組態

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。
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 。

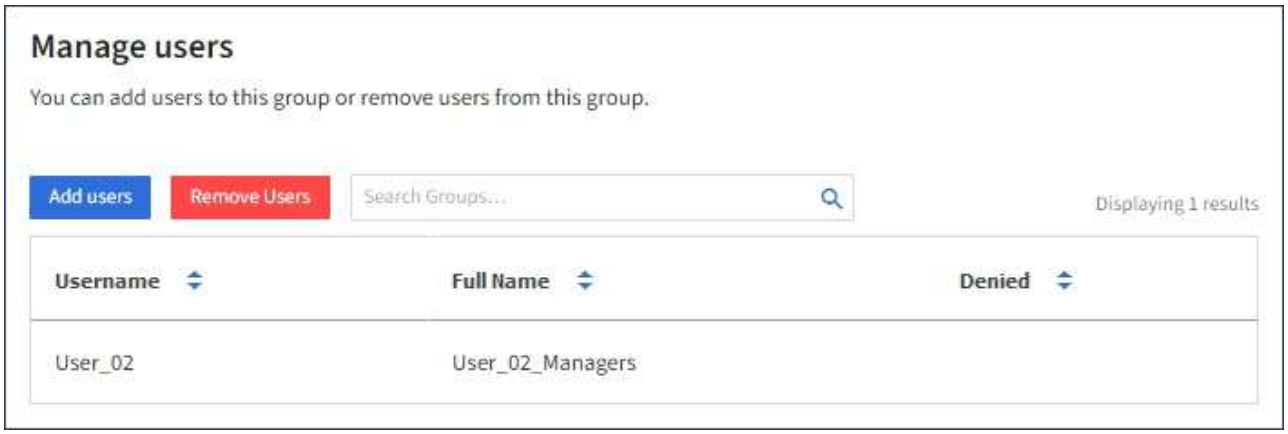
b. 在 * 群組權限 * 索引標籤上、更新權限、然後選取 * 儲存變更 * 。

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。

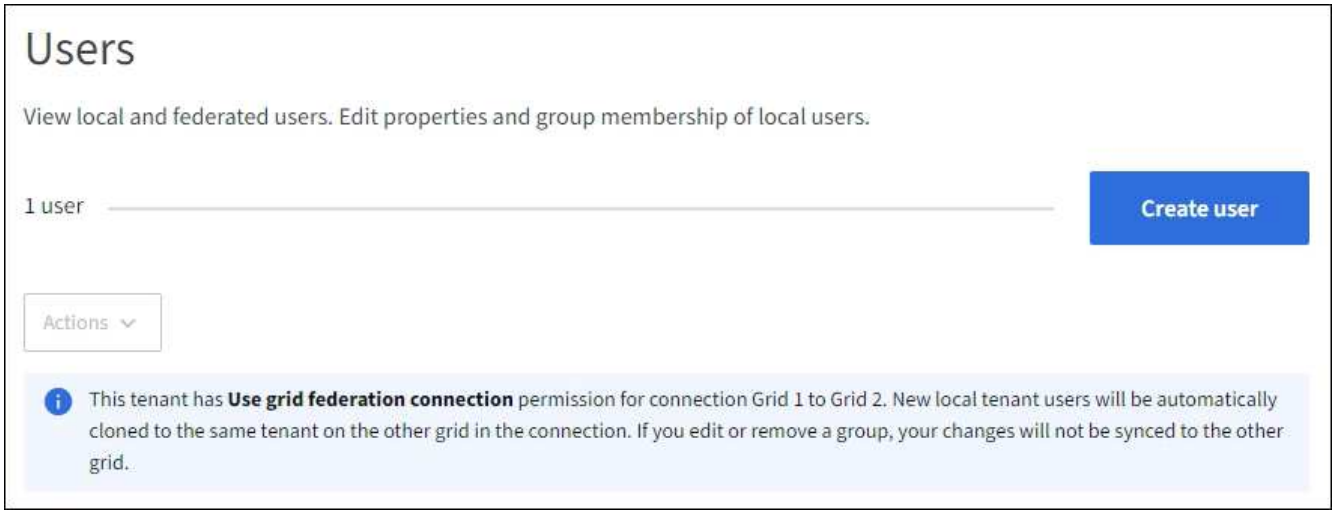
不屬於任何群組的 Swift 使用者沒有管理權限或 Swift Container 存取權。

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*。

使用 **S3** 物件鎖定來保留物件

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。

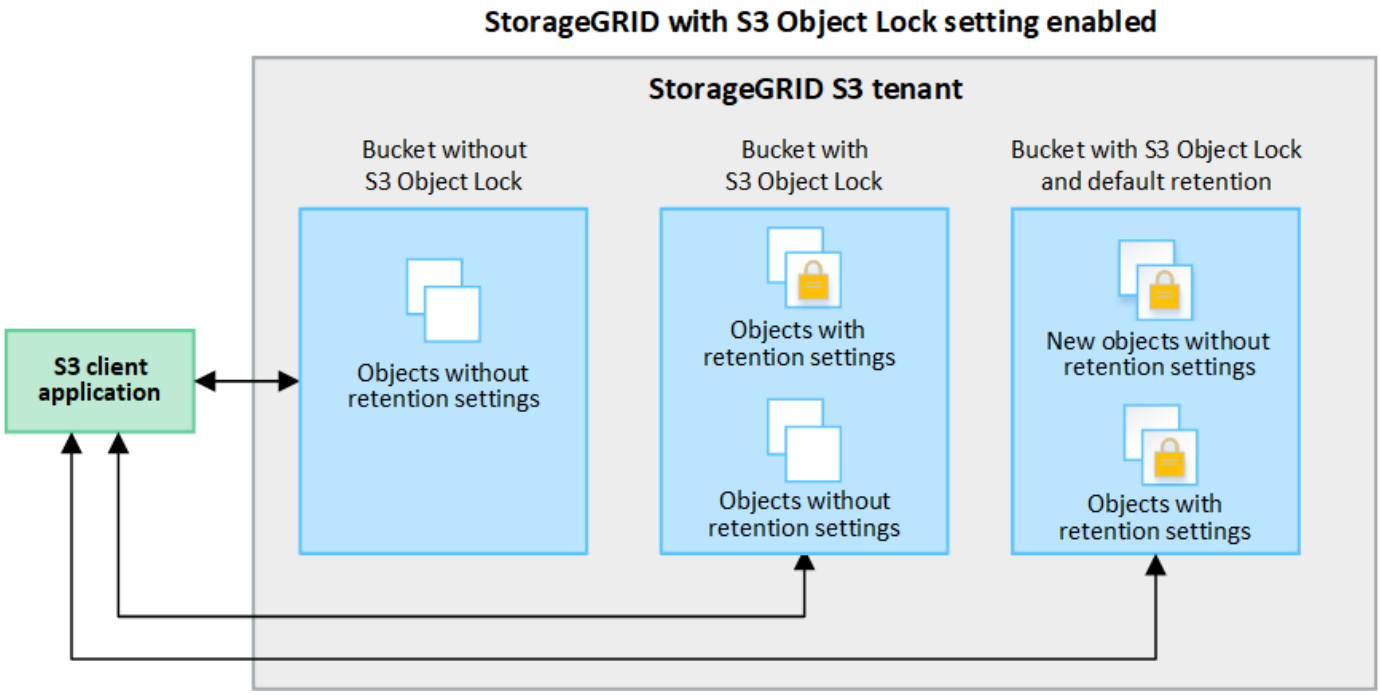
什麼是**S3**物件鎖定？

「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。

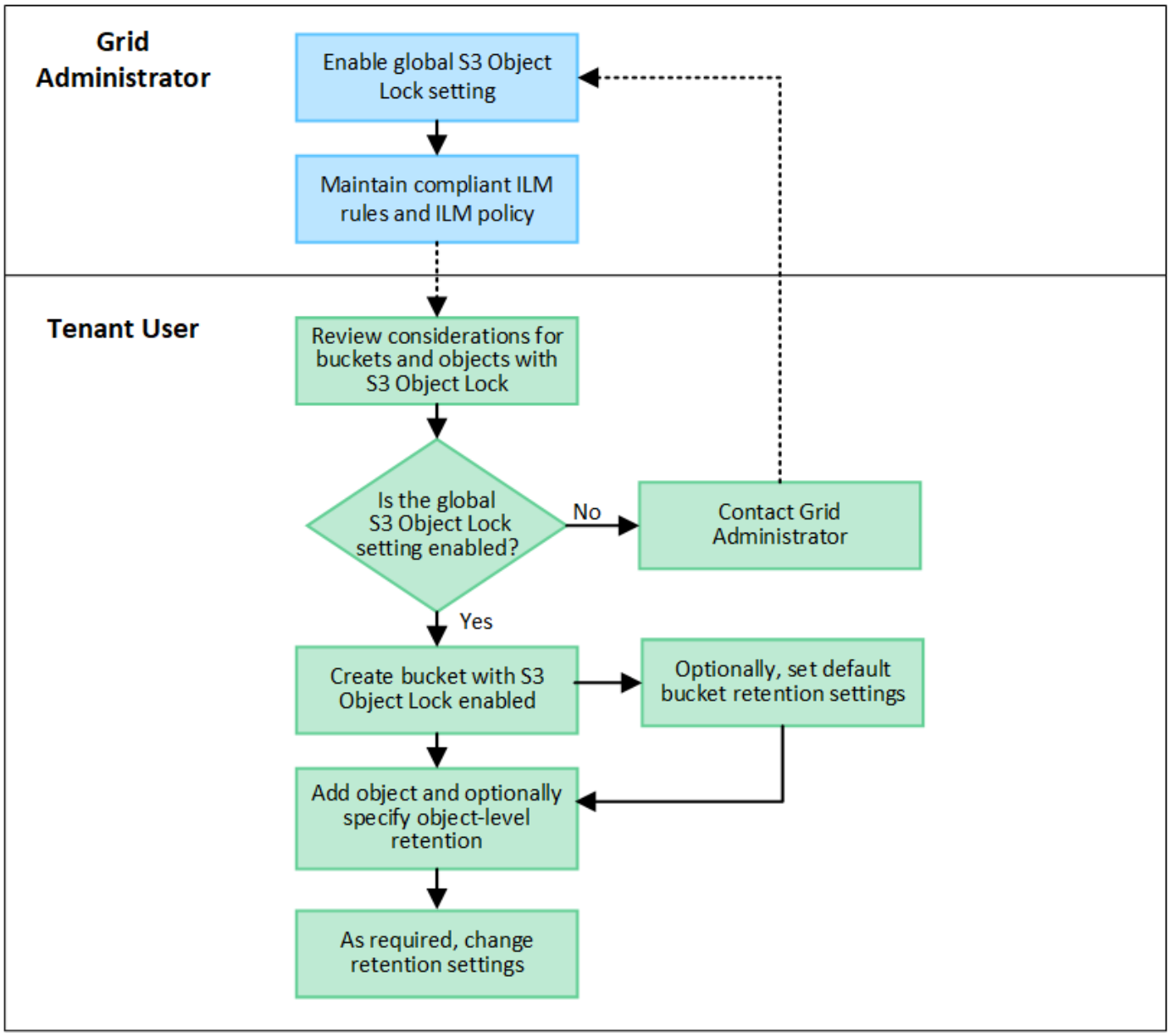
請參閱 "建立S3儲存區" 和 "更新 S3 物件鎖定預設保留"。

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

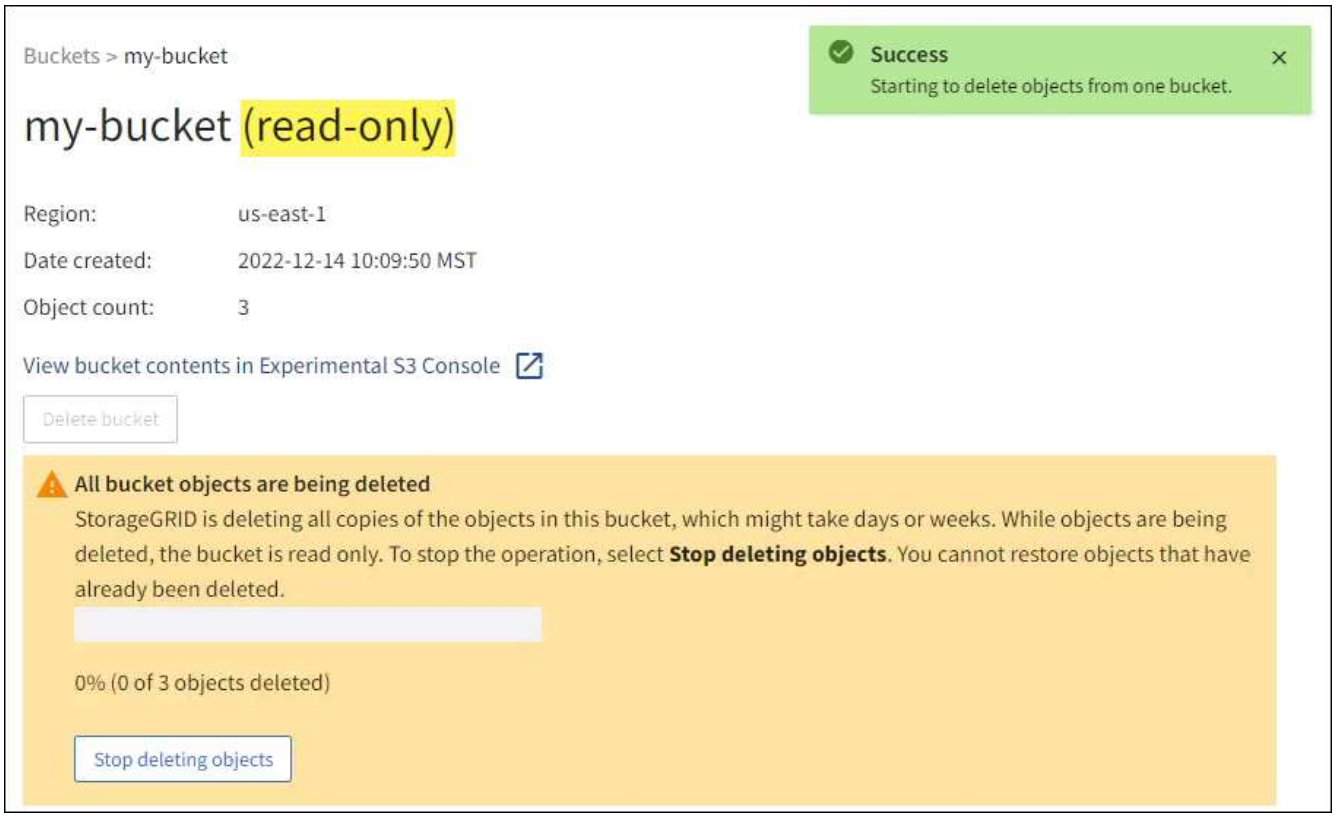
a. 選取貯體名稱以顯示其詳細資料。

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。

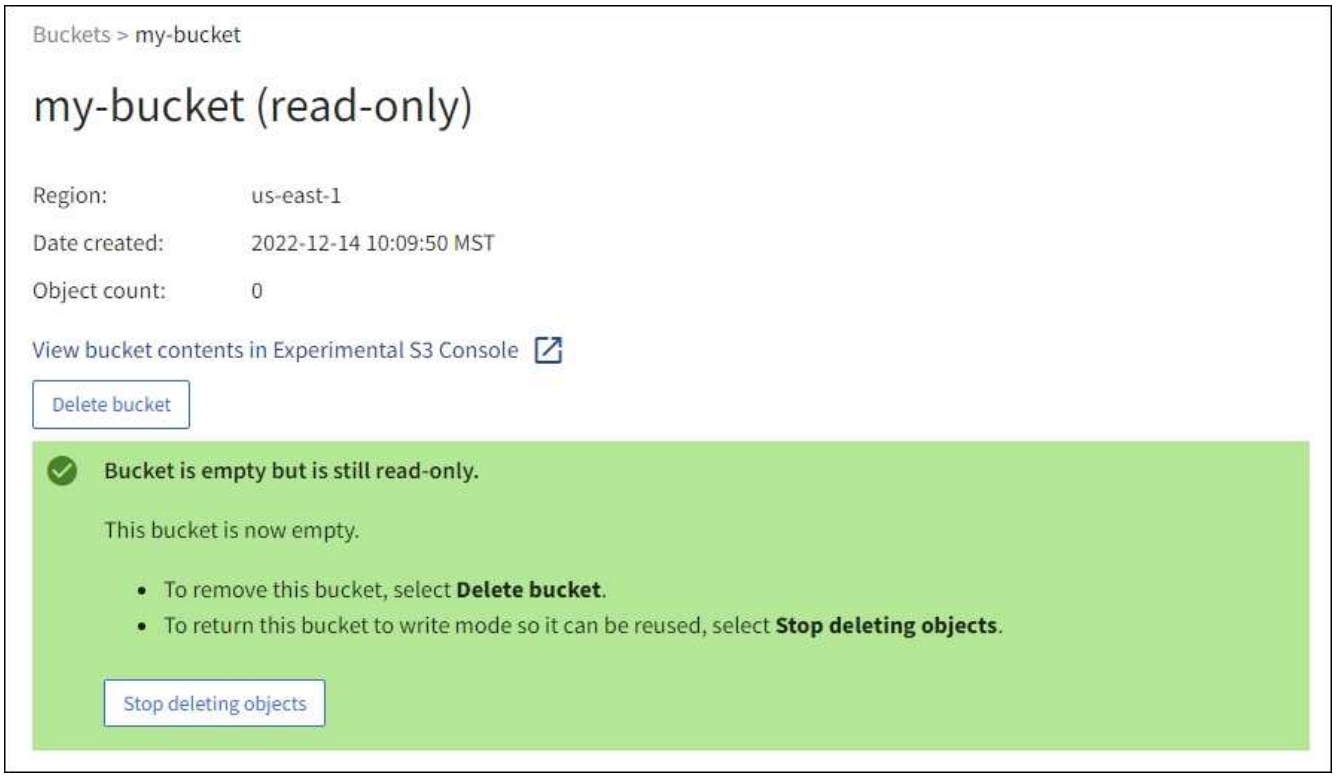


5. 在作業執行時視需要選取 * 停止刪除物件 * 以停止處理程序。然後、您也可以選擇 * 刪除貯體中的物件 * 來恢復處理程序。

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

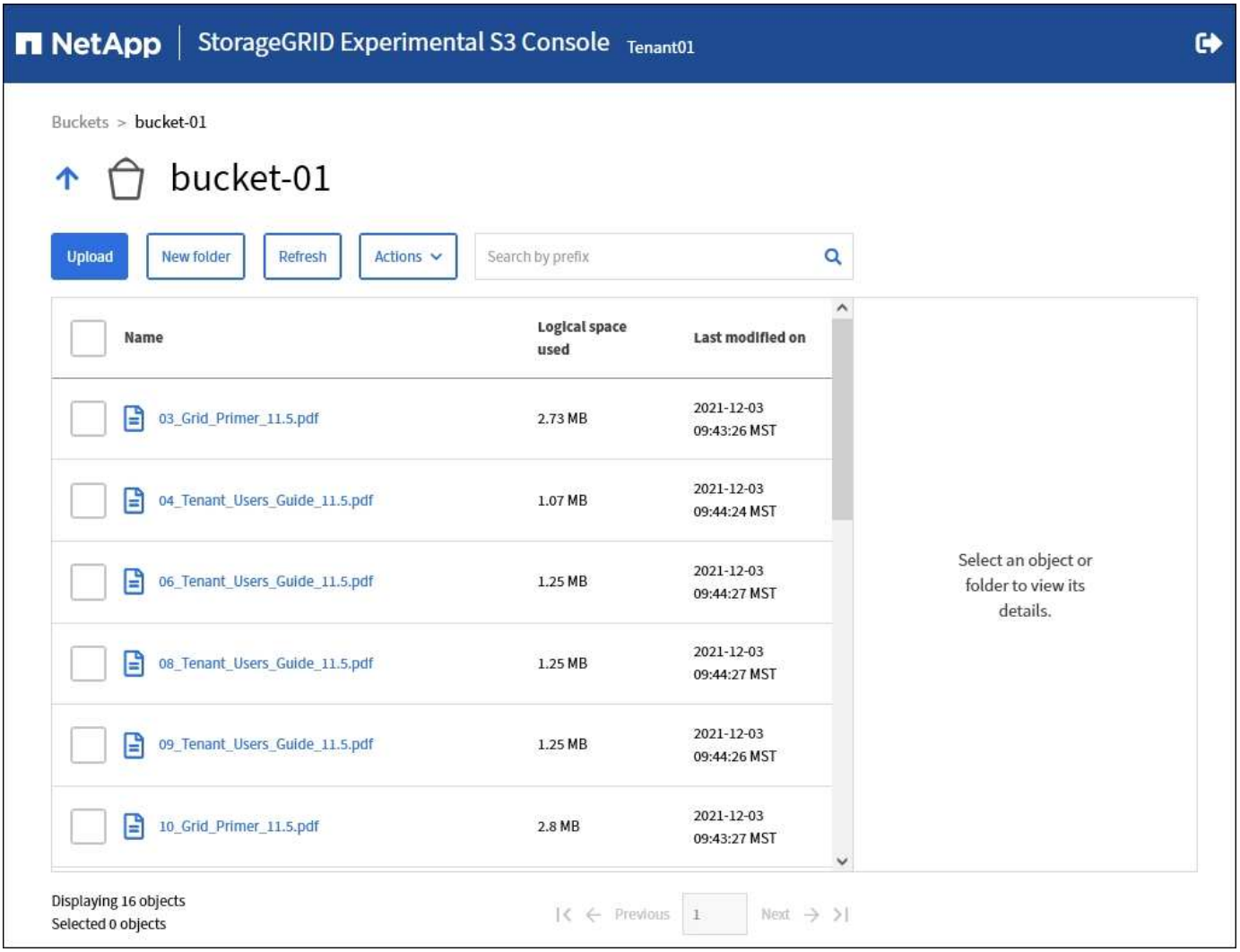
- 您將使用登入租戶管理程式 "支援的網頁瀏覽器"。
- 您屬於具有「根目錄」存取權限的使用者群組、或是擁有「使用 S3 主控台管理所有儲存區」和「管理物件」的使用者群組 "權限"。

> 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

平台服務	S3 REST API
"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。
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。
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"

指定平台服務端點的**URN**

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。

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。

建立平台服務端點

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"

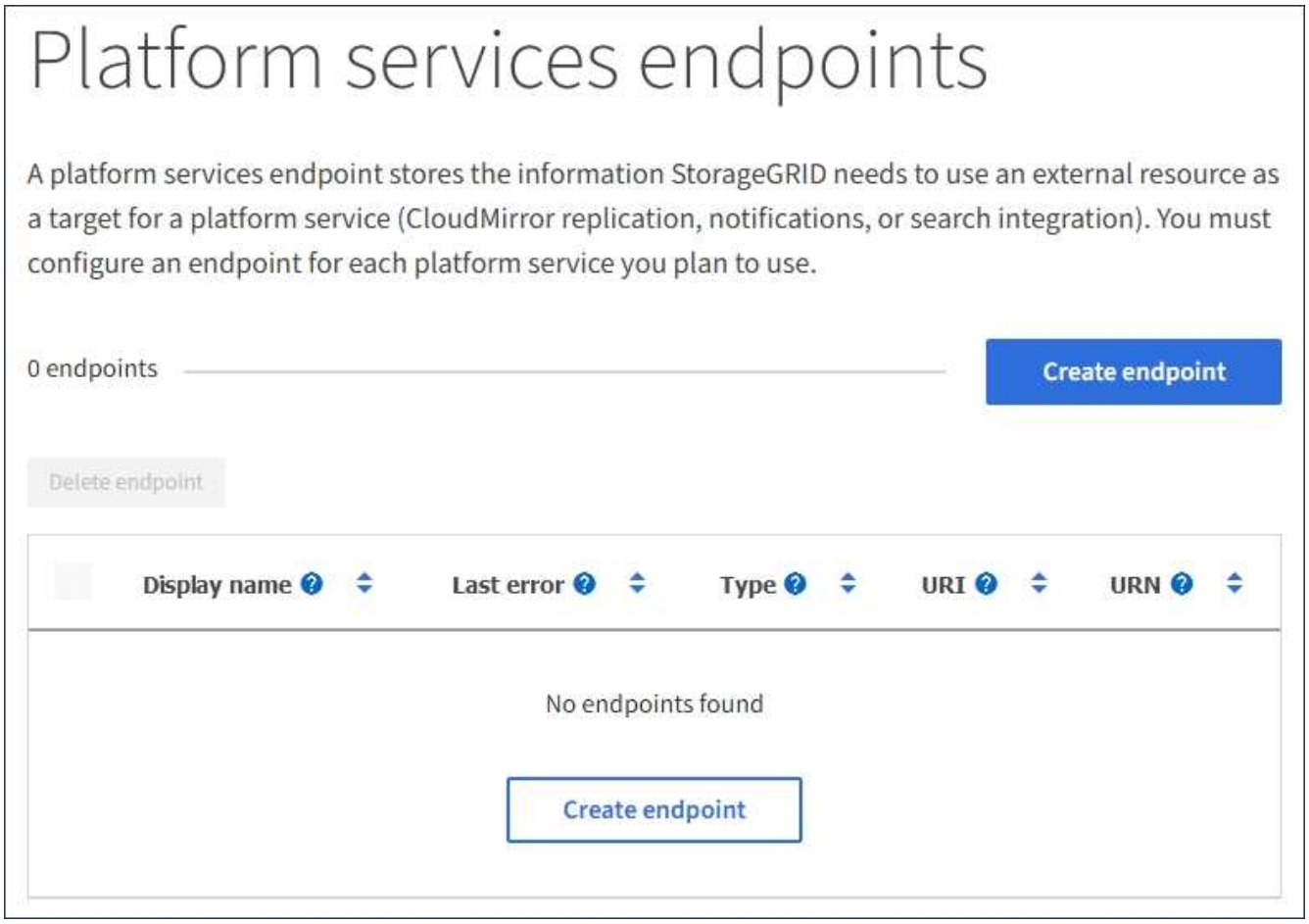
- 驗證認證資料（若有需要）：
  - 存取金鑰：存取金鑰ID和秘密存取金鑰
  - 基本HTTP：使用者名稱和密碼
  - CAP（C2S存取入口網站）：暫用認證URL、伺服器與用戶端認證、用戶端金鑰、以及選用的用戶端私密金鑰複雜密碼。
- 安全性憑證（如果使用自訂CA憑證）

- 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。

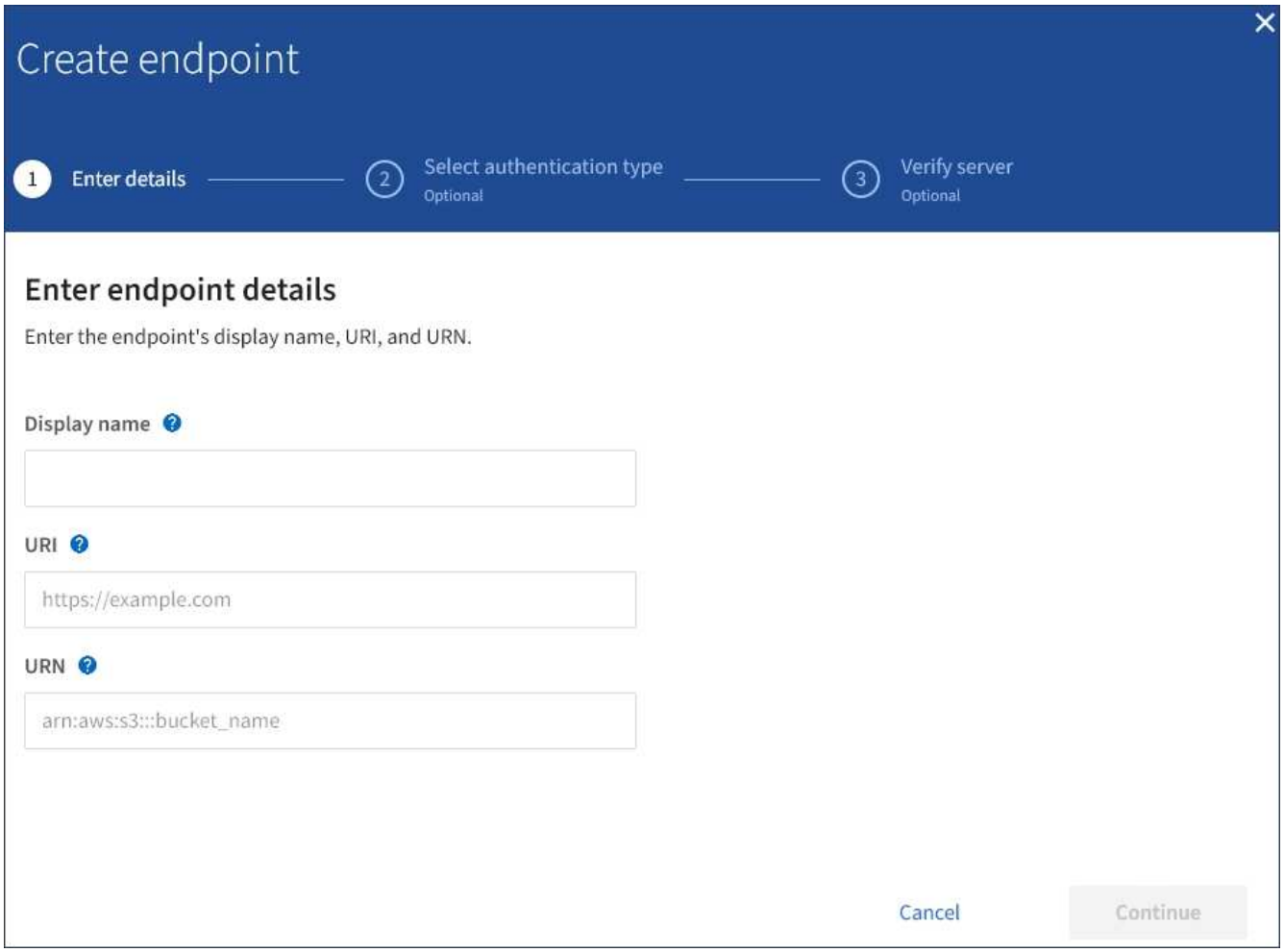
步驟

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。



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：

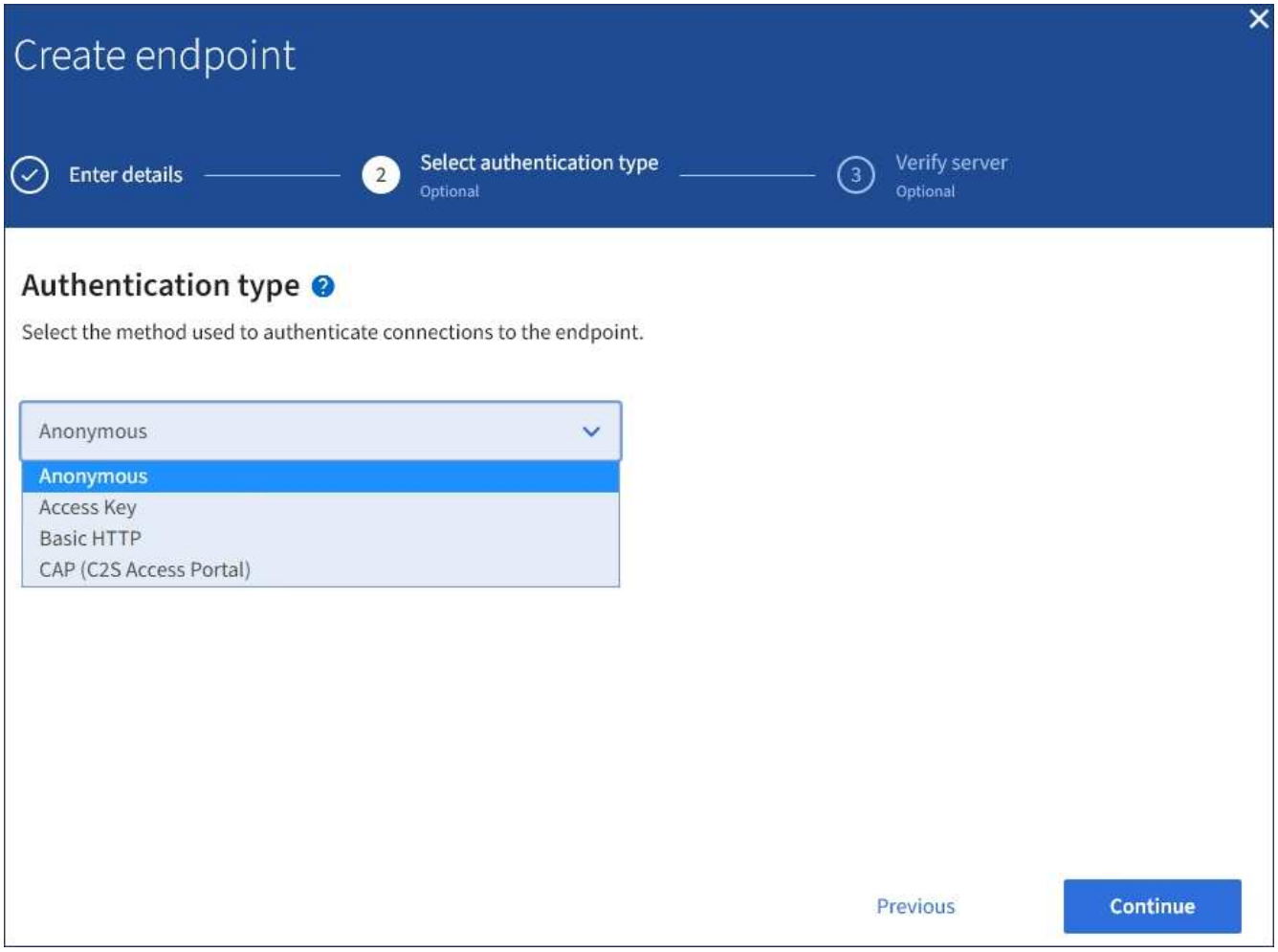
```
https://s3-aws-region.amazonaws.com
```

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 。

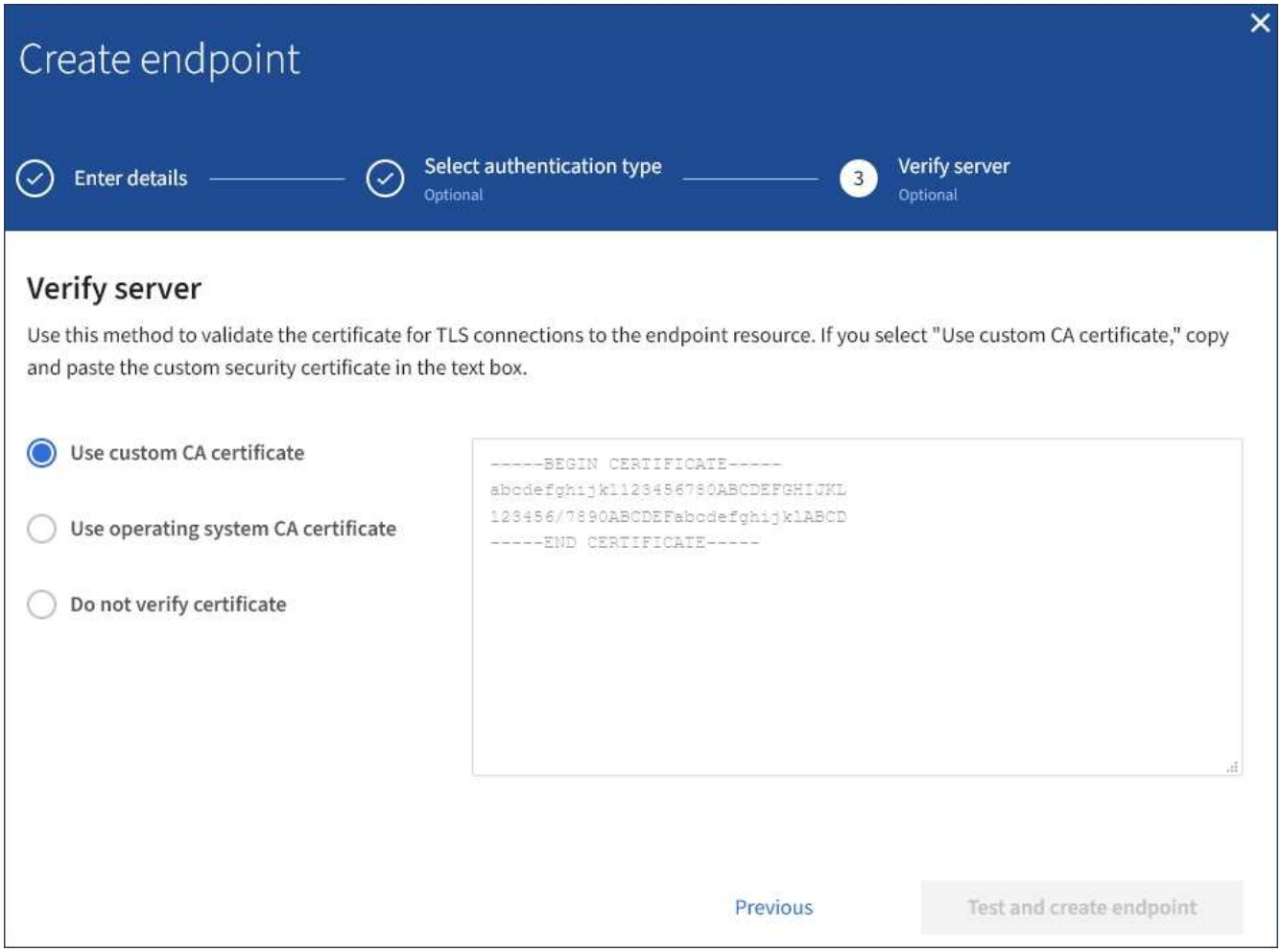
6. 選擇*繼續*。
7. 選取*驗證類型*的值、然後輸入或上傳所需的認證資料。



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"。

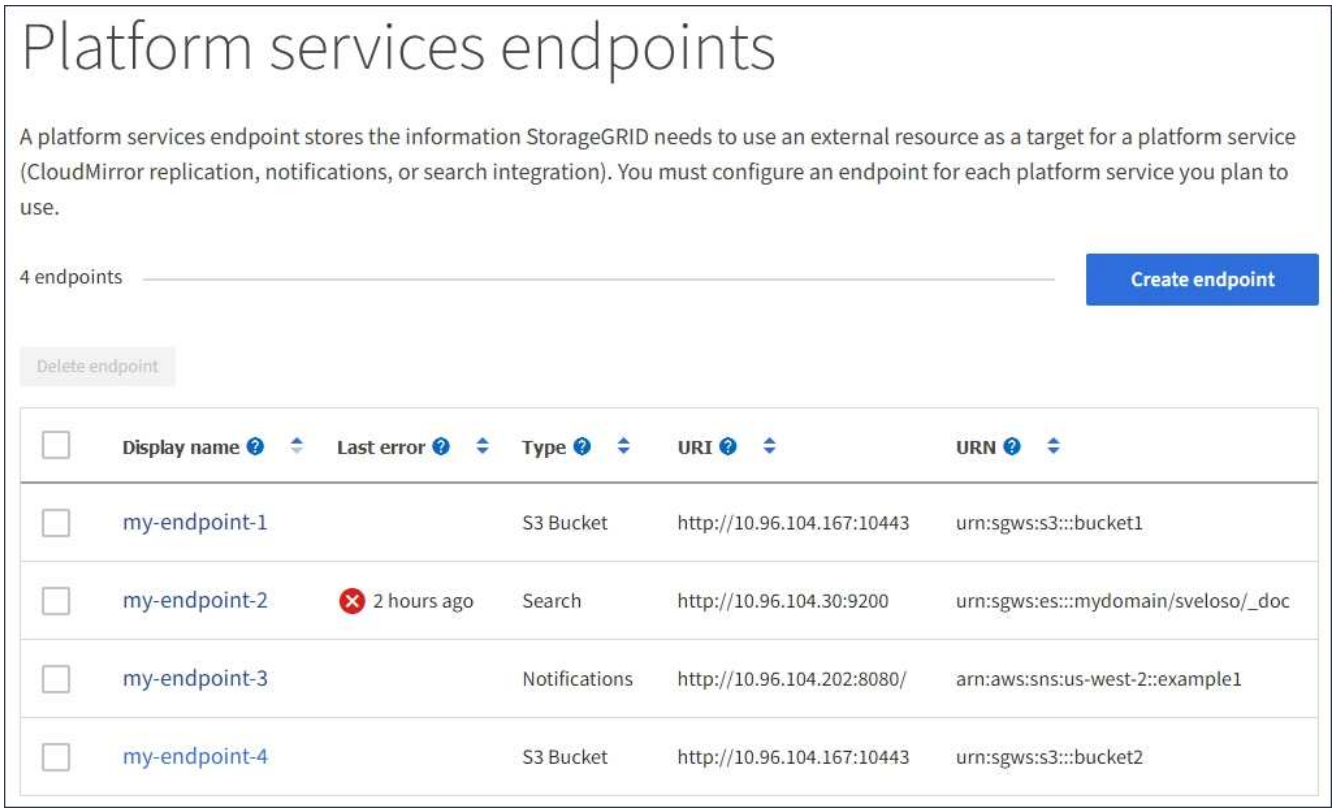
關於這項工作

無法驗證認證資料是否擁有正確的權限。StorageGRID

步驟

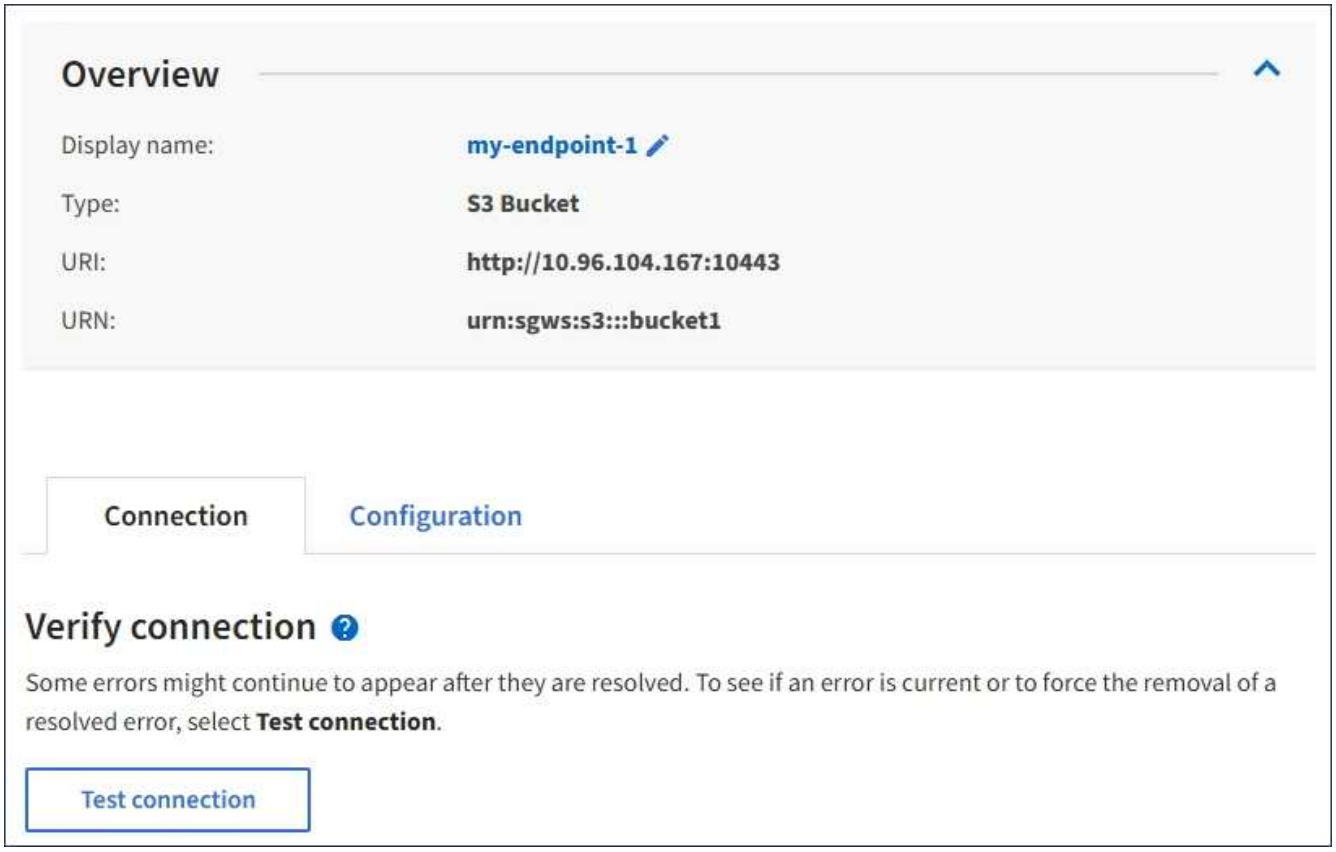
1. 選擇*儲存設備（S3）>*平台服務端點。

   「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 。

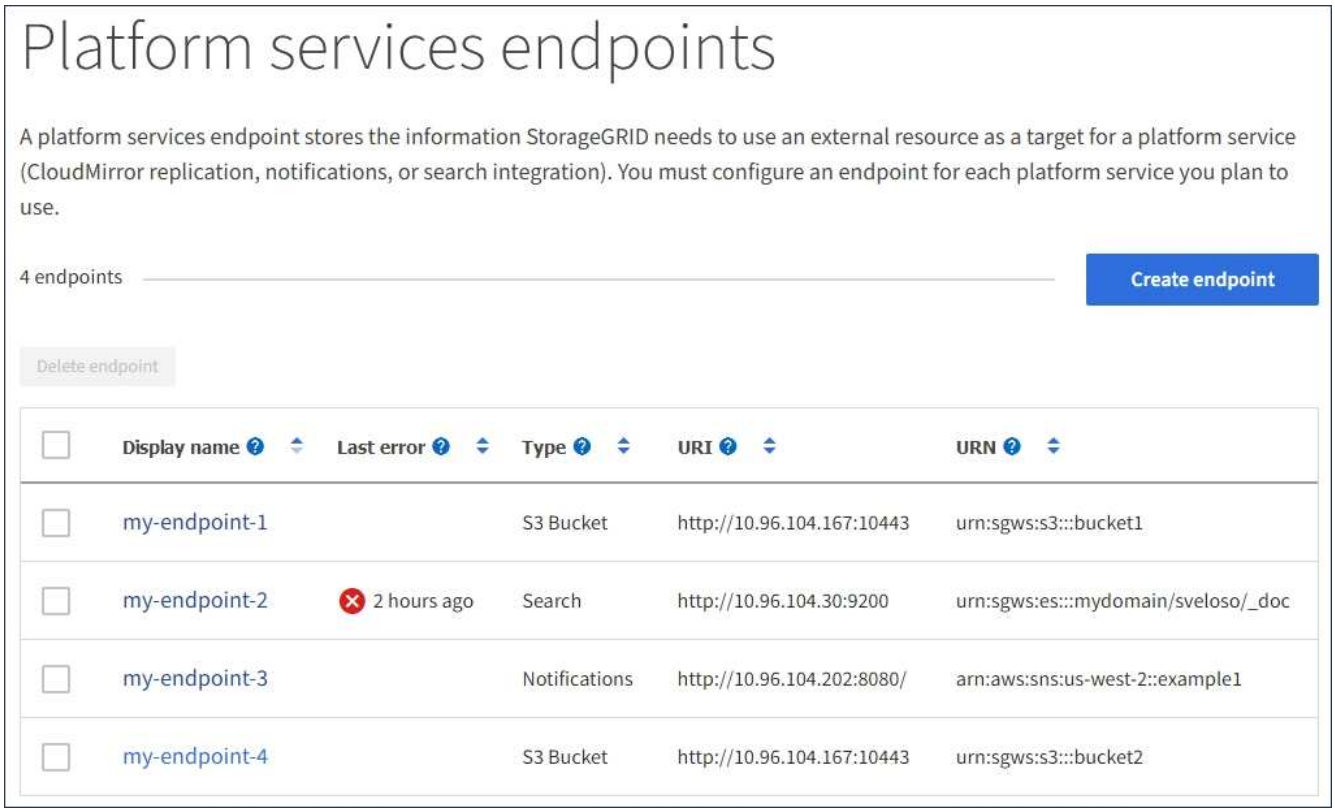
開始之前

- 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。

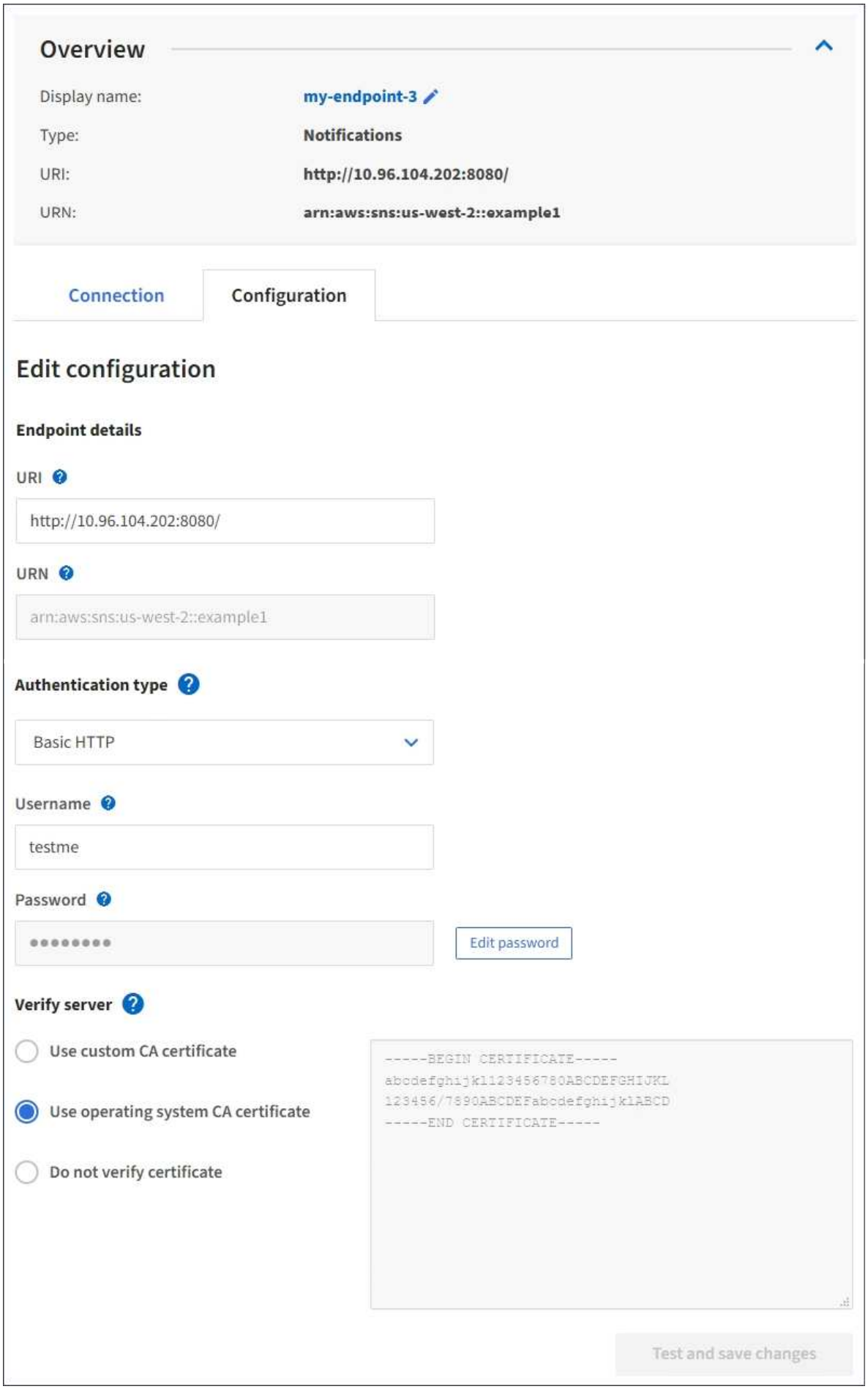
   「平台服務端點」頁面隨即出現、並顯示已設定的平台服務端點清單。



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。

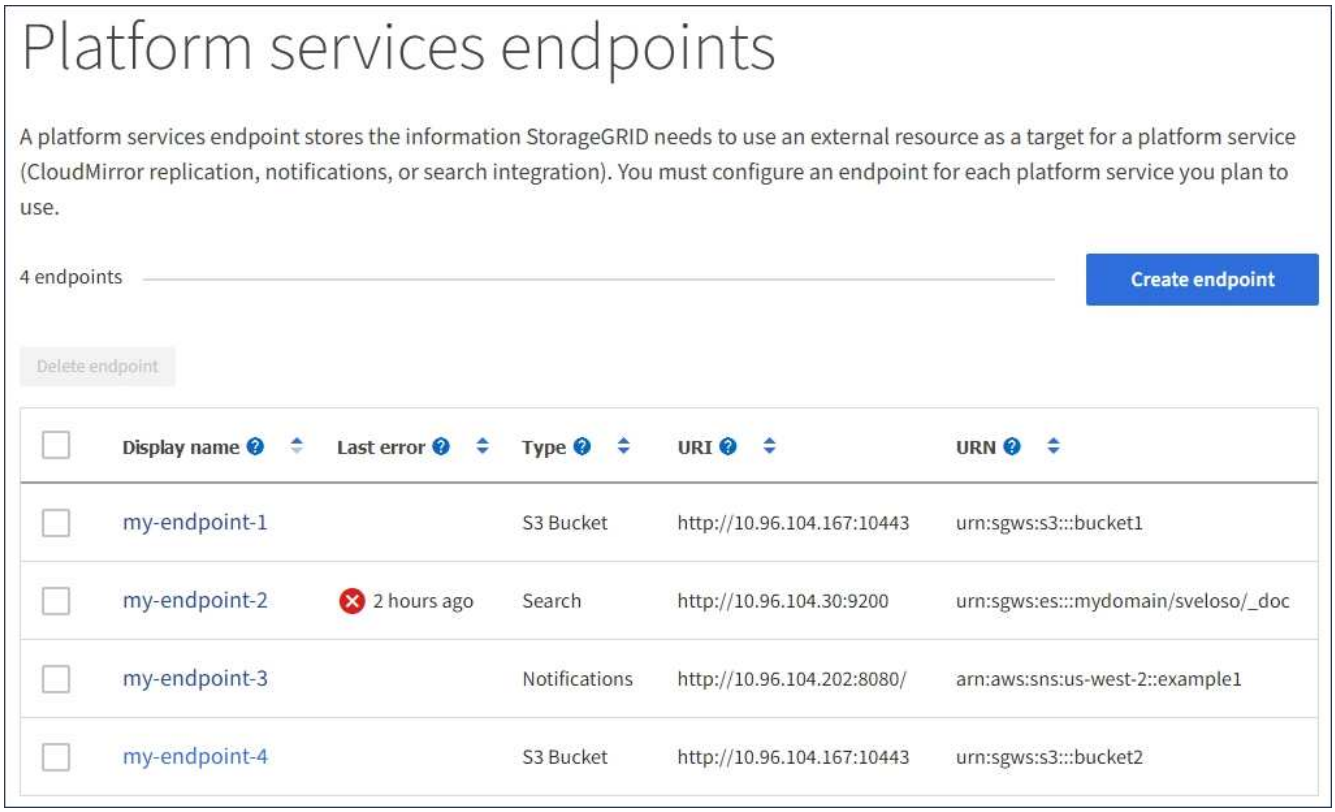
開始之前

- 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。

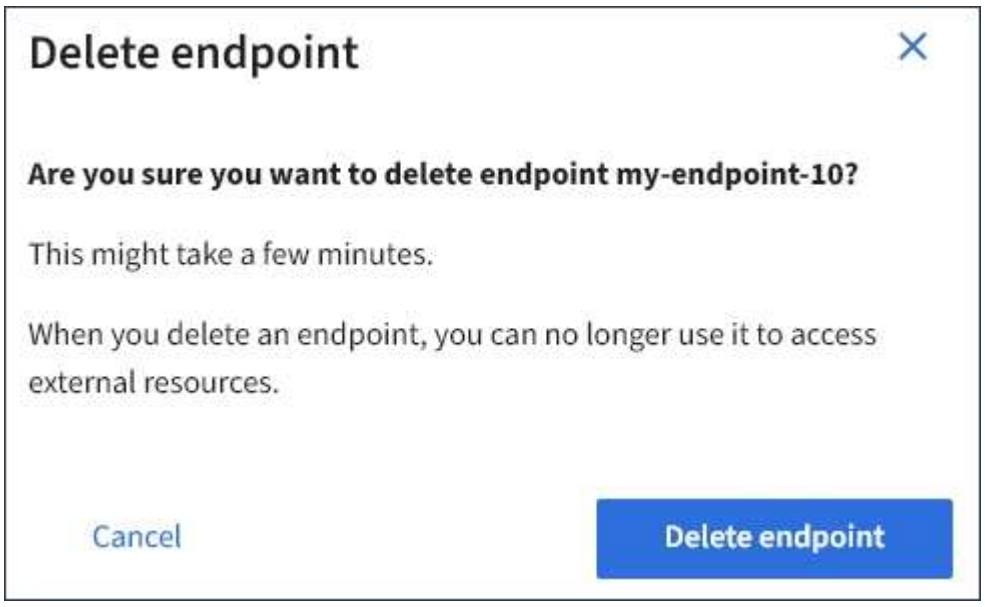


2. 選取您要刪除的每個端點的核取方塊。

> 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。

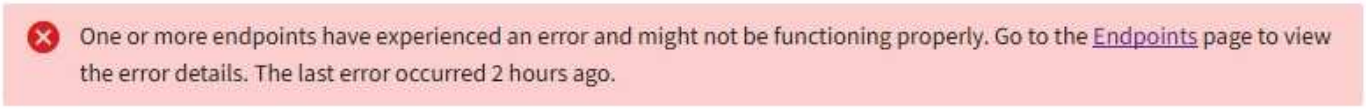


4. 選擇*刪除端點*。

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

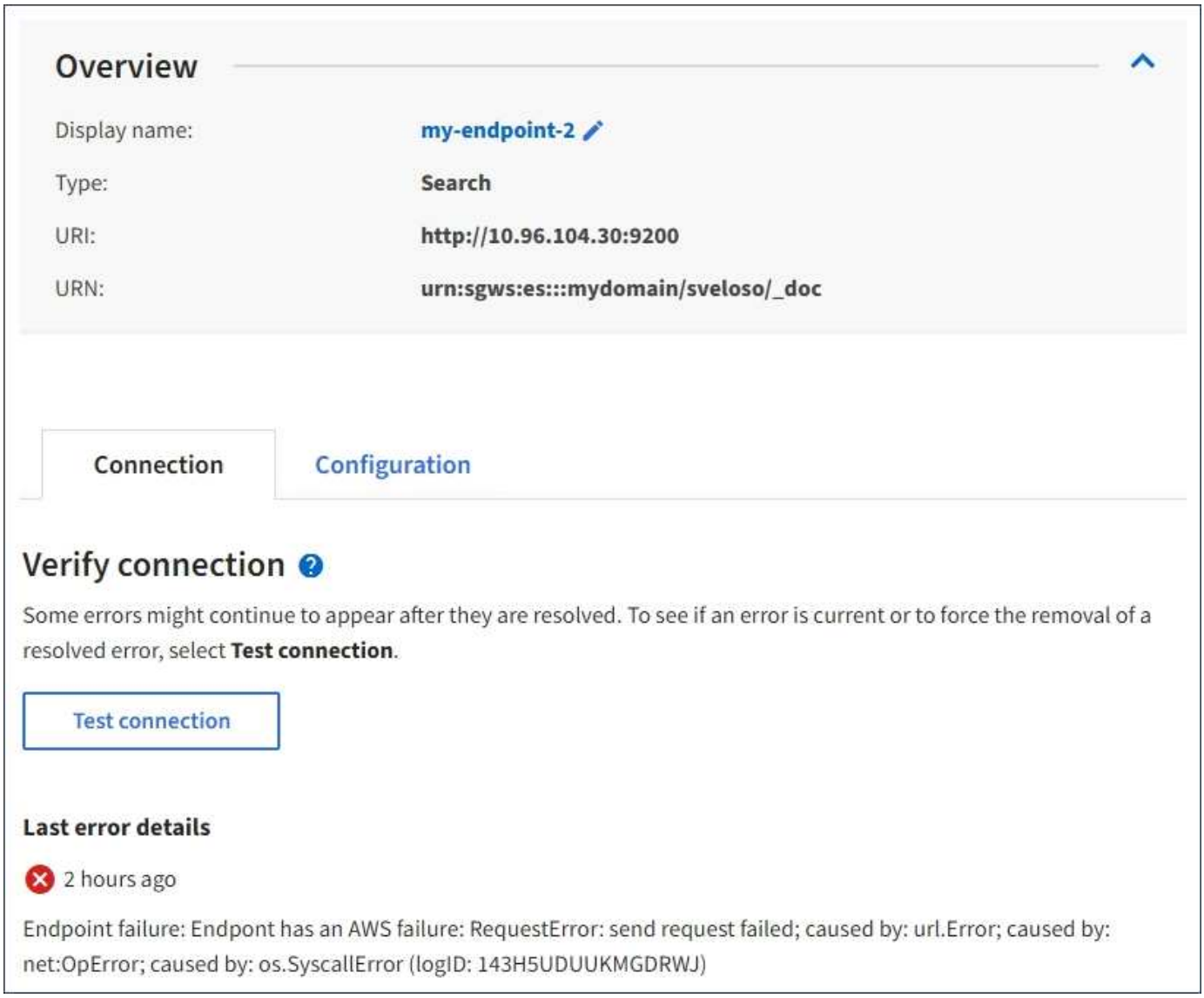
如果過去 7 天內發生任何平台服務端點錯誤、租戶管理器儀表板會顯示警示訊息。您可以移至「平台服務端點」頁面、查看錯誤的詳細資料。



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：

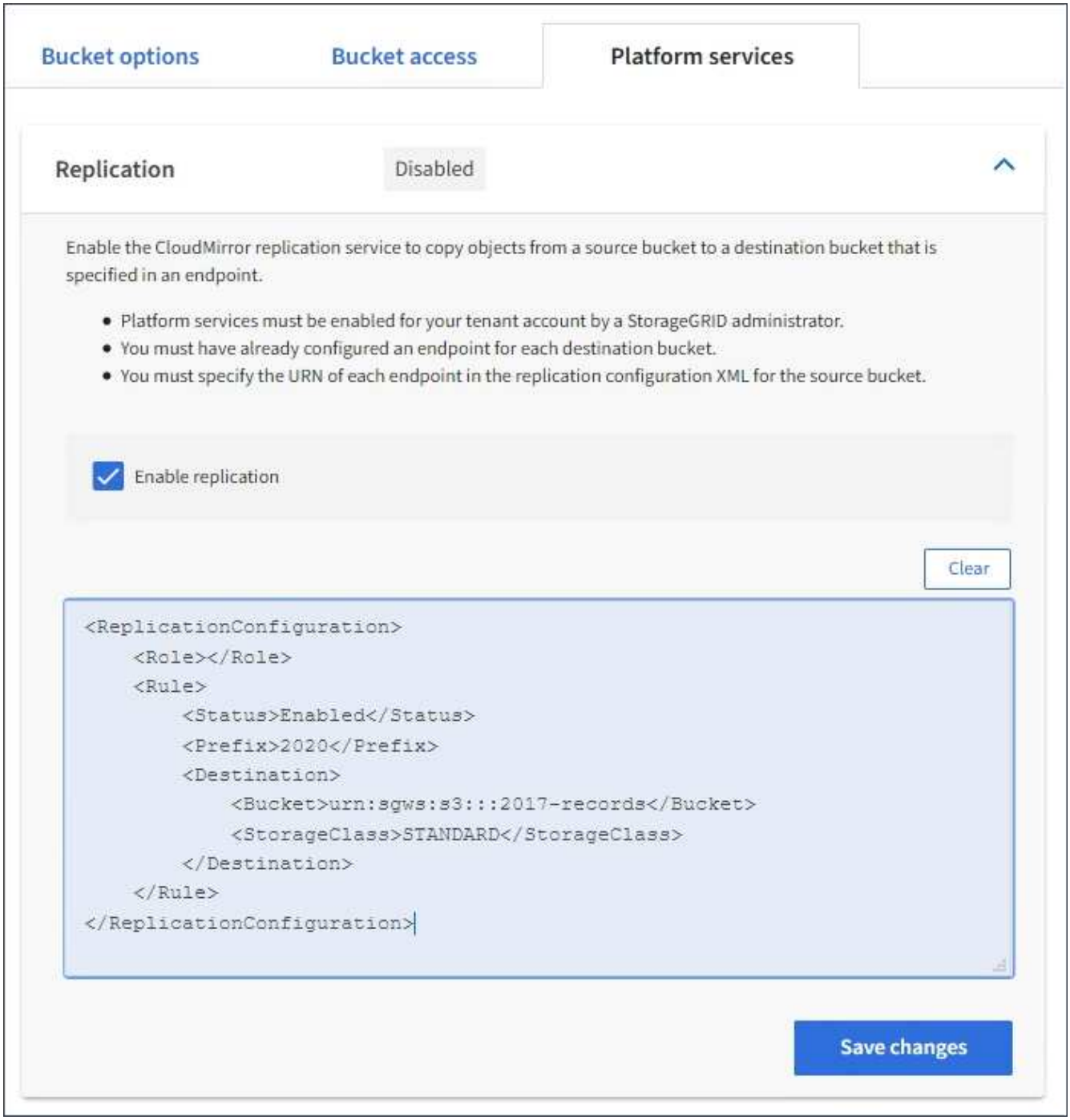
   ```
   <ReplicationConfiguration>
       <Role></Role>
       <Rule>
           <Status>Enabled</Status>
           <Prefix>2020</Prefix>
           <Destination>
              <Bucket>urn:sgws:s3:::2017-records</Bucket>
              <StorageClass>STANDARD</StorageClass>
            </Destination>
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

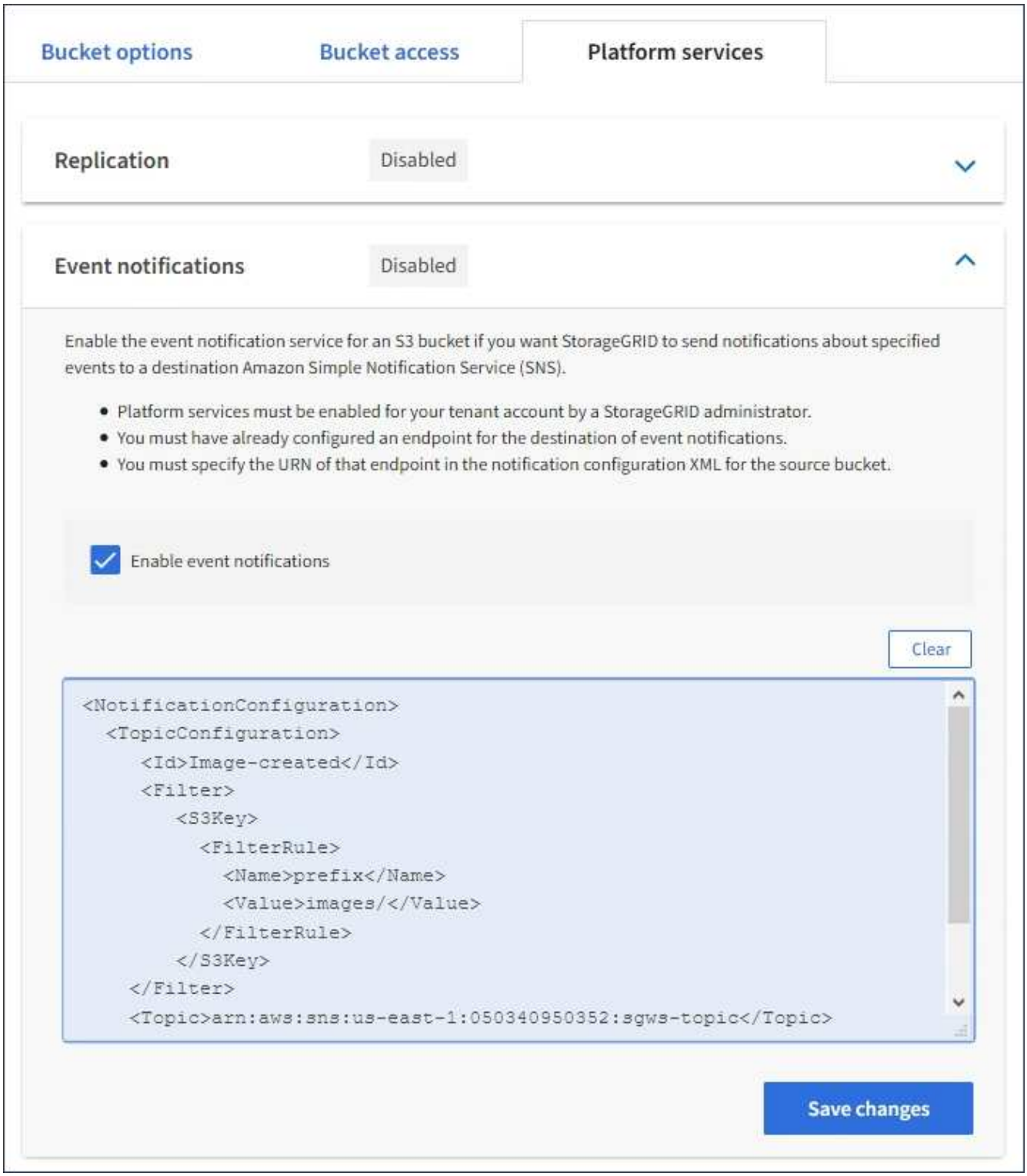
1. 啟用來源儲存區的通知：
   - 使用文字編輯器建立啟用事件通知所需的通知組態XML、如S3通知API所指定。
   - 設定XML時、請使用事件通知端點的URN作為目的地主題。

```
<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

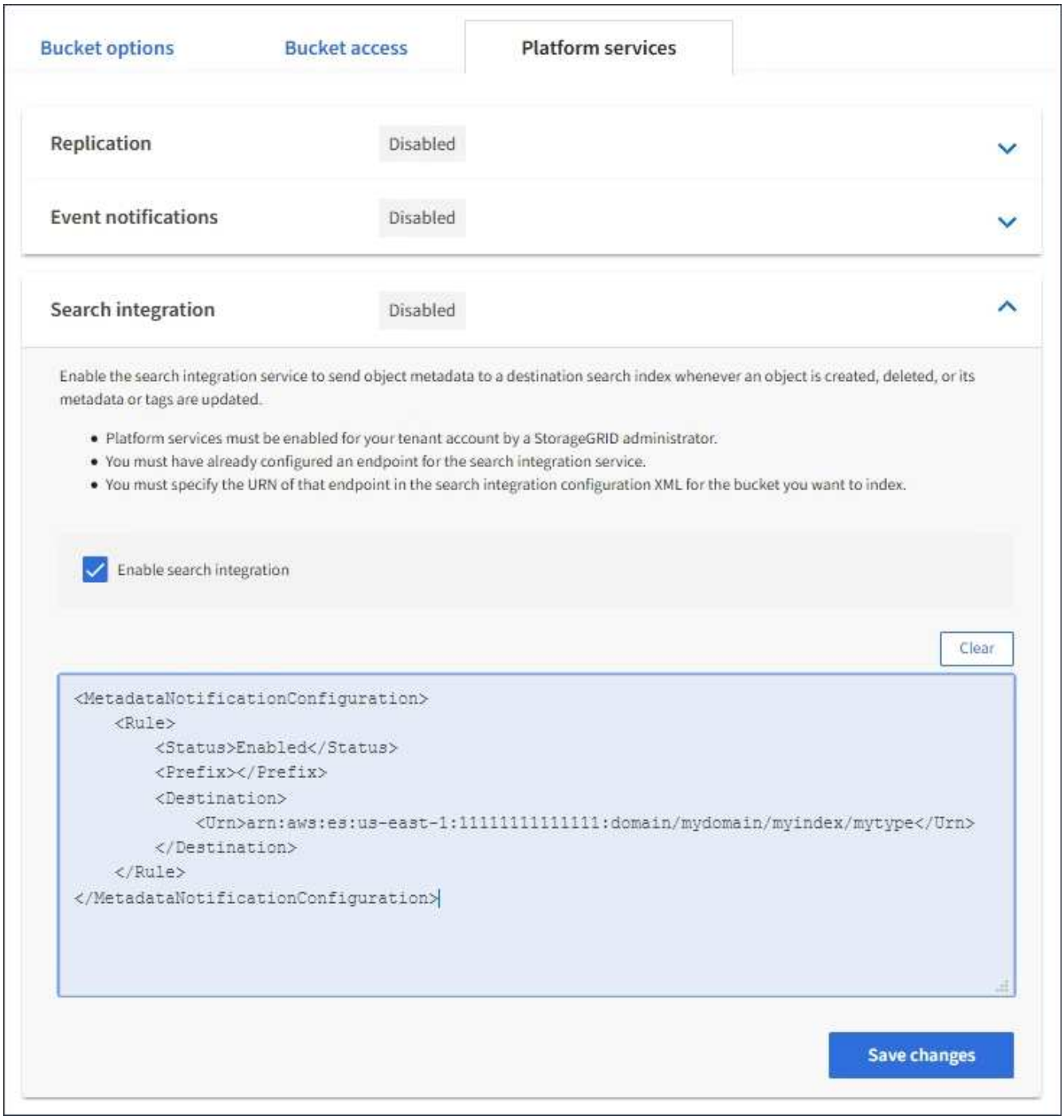
1. 使用文字編輯器建立啟用搜尋整合所需的中繼資料通知XML。
   - 請參閱組態XML的相關資訊以進行搜尋整合。
   - 設定XML時、請使用搜尋整合端點的URN作為目的地。

```
<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
`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。