



使用租戶帳戶 StorageGRID

NetApp
October 03, 2025

目錄

使用租戶帳戶	1
使用租戶管理程式	1
使用StorageGRID 綁定帳戶	1
網頁瀏覽器需求	2
登入租戶管理程式	3
登出租戶管理程式	6
瞭解租戶管理程式儀表板	6
瞭解租戶管理API	9
管理租戶使用者的系統存取	14
使用身分識別聯盟	14
管理群組	19
管理本機使用者	32
管理S3租戶帳戶	35
管理S3存取金鑰	35
管理S3儲存區	46
管理S3平台服務	63
什麼是平台服務	63
使用平台服務的考量	68
設定平台服務端點	69
設定CloudMirror複寫	85
設定事件通知	88
使用搜尋整合服務	92

使用租戶帳戶

瞭解如何使用StorageGRID 綁定帳戶。

- ["使用租戶管理程式"](#)
- ["管理租戶使用者的系統存取"](#)
- ["管理S3租戶帳戶"](#)
- ["管理S3平台服務"](#)

使用租戶管理程式

租戶管理程式可讓您管理StorageGRID 一個無租戶帳戶的所有層面。

您可以使用租戶管理程式來監控租戶帳戶的儲存使用量、並透過身分識別聯盟或建立本機群組和使用者來管理使用者。對於S3租戶帳戶、您也可以管理S3金鑰、管理S3儲存區、以及設定平台服務。

使用StorageGRID 綁定帳戶

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。

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。

或者、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S3用戶端應用程式的指示。

- 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。

建立租戶帳戶

租戶帳戶是StorageGRID 由使用Grid Manager的資料網格管理員所建立。建立租戶帳戶時、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) 。
- 租戶帳戶是否會使用S3或Swift 。
- 對於S3租戶帳戶：是否允許租戶帳戶使用平台服務。如果允許使用平台服務、則必須設定網格以支援其使用。
- 或者、租戶帳戶的儲存配額、也就是租戶物件可用的GB、TB或PB上限。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) 。
- 如果啟用StorageGRID 身分識別聯盟以供支援整個系統、則哪個聯盟群組具有root存取權限可設定租戶帳

戶。

- 如果StorageGRID 不使用單一登入 (SSO) 進行支援、則租戶帳戶是使用自己的身分識別來源、還是共用網絡的身分識別來源、以及租戶本機root使用者的初始密碼。

此外、如果StorageGRID S3租戶帳戶需要符合法規要求、網絡管理員也可以針對該系統啟用S3物件鎖定設定。啟用S3物件鎖定时、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

建立S3租戶帳戶之後、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絡共用) 、或建立本機群組和使用者
- 管理S3存取金鑰
- 建立及管理S3儲存區、包括符合法規的儲存區
- 使用平台服務 (若已啟用)
- 監控儲存使用量



雖然您可以使用租戶管理程式來建立和管理S3儲存區、但您必須擁有S3存取金鑰、並使用S3 REST API來擷取和管理物件。

設定Swift租戶

建立Swift租戶帳戶之後、具有「根存取」權限的使用者就能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絡共用) 、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。

相關資訊

["管理StorageGRID"](#)

["使用S3"](#)

["使用Swift"](#)

網頁瀏覽器需求

您必須使用支援的網頁瀏覽器。

網頁瀏覽器	支援的最低版本
Google Chrome	87

網頁瀏覽器	支援的最低版本
Microsoft Edge	87
Mozilla Firefox	84.

您應該將瀏覽器視窗設定為建議的寬度。

瀏覽器寬度	像素
最低	1024.
最佳化	1280

登入租戶管理程式

若要存取租戶管理程式、請在支援的網頁瀏覽器網址列中輸入租戶的URL。

您需要的產品

- 您必須擁有登入認證資料。
- 您必須擁有網格管理員所提供的URL、才能存取租戶管理程式。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）或用於存取管理節點的IP位址、也可以選擇性地包含連接埠號碼、20位數租戶帳戶ID或兩者。

- 如果URL不包含租戶的20位數帳戶ID、您必須擁有此帳戶ID。
- 您必須使用支援的網頁瀏覽器。
- Cookie必須在您的網路瀏覽器中啟用。
- 您必須擁有特定的存取權限。

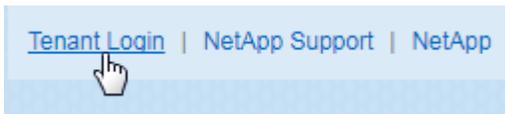
步驟

1. 啟動支援的網頁瀏覽器。

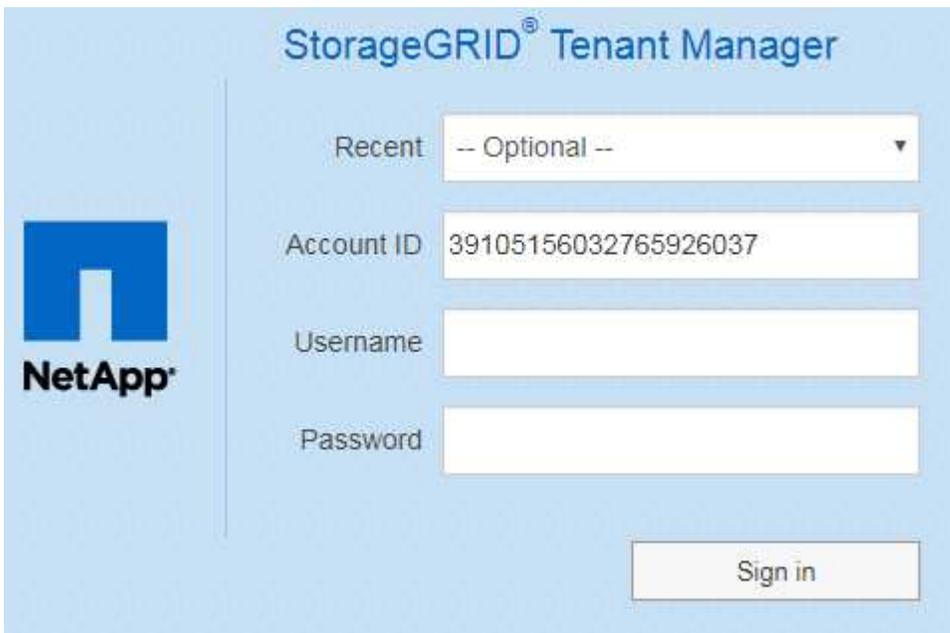
2. 在瀏覽器的網址列中、輸入存取租戶管理程式的URL。
3. 如果系統提示您輸入安全性警示、請使用瀏覽器的安裝精靈來安裝憑證。
4. 登入租戶管理程式。

您看到的登入畫面取決於您輸入的URL、以及組織是否使用單一登入（SSO）。您會看到下列其中一個畫面：

- Grid Manager登入頁面。按一下右上角的*租戶登入*連結。



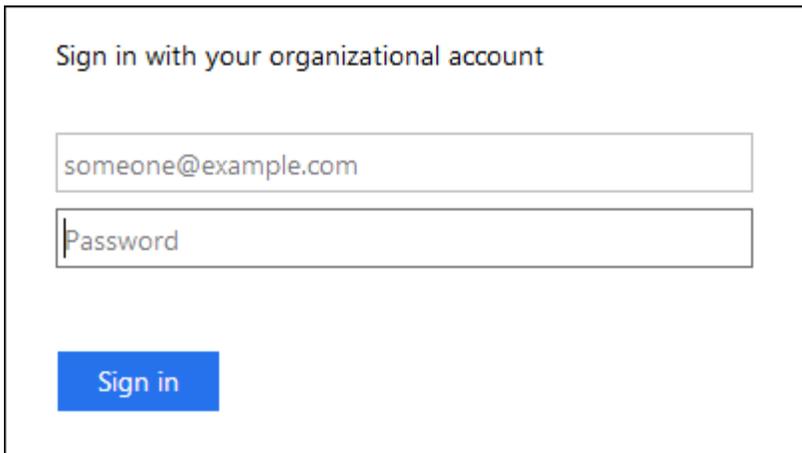
- 租戶管理程式登入頁面。「帳戶ID」欄位可能已經完成、如下所示。

A screenshot of the StorageGRID Tenant Manager login page. The page has a light blue background. On the left is the NetApp logo. The main content area contains a 'Recent' dropdown menu with '-- Optional --' selected. Below it are three input fields: 'Account ID' with the value '39105156032765926037', 'Username', and 'Password'. At the bottom right is a 'Sign in' button.

- 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. 按一下*登入*。

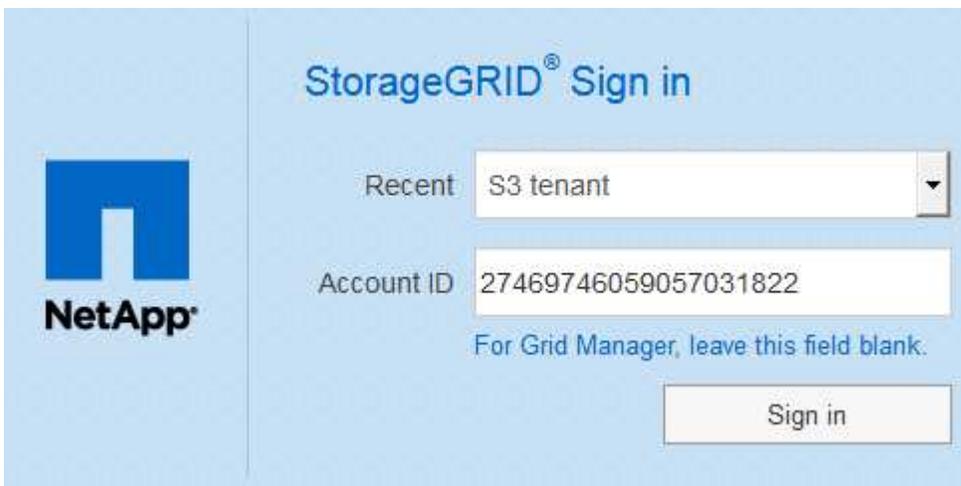
此時會顯示租戶管理程式儀表板。

- 如果網絡上已啟用SSO、則會顯示貴組織的SSO頁面。例如：



輸入您的標準SSO認證、然後按一下*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. 按一下*登入*。
- iii. 在組織的SSO登入頁面上、以標準SSO認證登入。

此時會顯示租戶管理程式儀表板。

5. 如果您收到其他人的初始密碼、請變更密碼以保護您的帳戶安全。選擇「使用者名稱_>*變更密碼*」。



如果StorageGRID 啟用SSO以供支援整個系統、您就無法從Tenant Manager變更密碼。

相關資訊

["管理StorageGRID"](#)

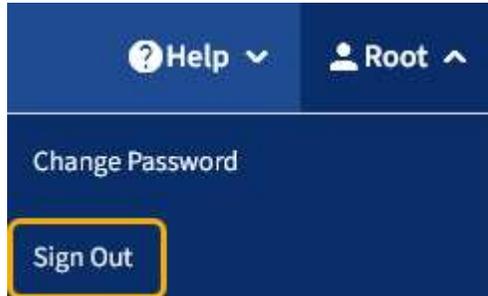
["網頁瀏覽器需求"](#)

登出租戶管理程式

使用Tenant Manager之後、您必須登出、以確保未獲授權的使用者無法存取StorageGRID該系統。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*。

選項	說明
SSO未在使用中	您已登出管理節點。隨即顯示「租戶管理程式」登入頁面。 *附註：*如果您登入一個以上的管理節點、則必須登出每個節點。
SSO已啟用	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*。 *附註：*如果啟用SSO、而且您也已登入Grid Manager、您也必須登出Grid Manager以登出SSO。

瞭解租戶管理程式儀表板

租戶管理程式儀表板提供租戶帳戶組態的總覽、以及租戶貯體 (S3) 或容器 (Swift) 中物件所使用的空間量。如果租戶有配額、儀表板會顯示配額使用量及剩餘量。如果有任何與租戶帳戶相關的錯誤、則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、儀表板的範例如下所示：

Dashboard

16 Buckets
View buckets

2 Platform services endpoints
View endpoints

0 Groups
View groups

1 User
View users

Storage usage

6.5 TB of 7.2 TB used

0.7 TB (10.1%) remaining



Bucket name	Space used	Number of objects
 Bucket-15	969.2 GB	913,425
 Bucket-04	937.2 GB	576,806
 Bucket-13	815.2 GB	957,389
 Bucket-06	812.5 GB	193,843
 Bucket-10	473.9 GB	583,245
 Bucket-03	403.2 GB	981,226
 Bucket-07	362.5 GB	420,726
 Bucket-05	294.4 GB	785,190
 8 other buckets	1.4 TB	3,007,036

Total objects

8,418,886
objects

Tenant details

Name Human Resources
ID 4955 9096 9804 4285 4354

 View the instructions for Tenant Manager.

[Go to documentation](#) 

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、如果沒有任何物件被擷取、而且您具有「根存取」權限、則會顯示「入門指南」、而非物件總數。

- 租戶帳戶名稱和ID。
- 連結至《The》資料StorageGRID。

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。



配額使用率是根據內部預估、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、則在重新計算配額使用率之前、租戶可能會暫時無法上傳新物件。配額使用率計算可能需要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。

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。如需詳細資訊、請參閱監控StorageGRID和疑難排解功能的說明中的警示參考資料。

 Only 0.6% of the quota is remaining. If the quota is exceeded, you can no longer upload new objects.

如果超出配額、就無法上傳新物件。

 The quota has been met. You cannot upload new objects.



若要檢視其他詳細資料、並管理警示的規則和通知、請參閱監控和疑難排解StorageGRID 的指示。

端點錯誤

如果您已使用Grid Manager設定一或多個端點以搭配平台服務使用、則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。

 One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

若要查看端點錯誤的詳細資料、請選取「端點」以顯示「端點」頁面。

相關資訊

["疑難排解平台服務端點錯誤"](#)

["監控安培；疑難排解"](#)

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。

若要存取租戶管理API的Swagger文件：

步驟

1. 登入租戶管理程式。
2. 從「租戶管理程式」標頭中選取「說明>* API說明文件*」。

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。

請參閱「防範跨網站要求偽造」、以取得改善驗證安全性的資訊。



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《管理StorageGRID》中的「若啟用單一登入、則驗證API」。

- 組態-與租戶管理API產品版本相關的作業。您可以列出該版本所支援的產品版本和主要API版本。
- * Container *：在S3貯體或Swift Container上的作業、如下所示：

傳輸協定	權限允許
S3	<ul style="list-style-type: none"> • 建立符合法規且不符合法規的儲存庫 • 修改舊版法規遵循設定 • 設定物件上執行作業的一致性控制 • 建立、更新及刪除儲存庫的CORS組態 • 啟用和停用物件的上次存取時間更新 • 管理平台服務的組態設定、包括CloudMirror複寫、通知及搜尋整合（中繼資料通知） • 刪除空的儲存區
Swift	設定用於容器的一致性層級

- 停用功能-檢視可能已停用之功能的作業。
- 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。
- 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-作業：設定外部身分識別來源、以及手動同步處理聯盟群組與使用者資訊。
- 地區-作業、以判斷StorageGRID 哪些地區已設定用於該系統。
- * S3 *：管理租戶使用者S3存取金鑰的作業。
- * S3-object-lock *-決定如何為StorageGRID 該系統設定全域S3物件鎖定（法規遵循）的作業。
- 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。

groups Operations on groups

GET

/org/groups Lists Tenant User Groups

Parameters

Try it out

Name	Description
type string (query)	filter by group type
limit integer (query)	maximum number of results
marker string (query)	marker-style pagination offset (value is Group's URN)
includeMarker boolean (query)	if set, the marker element is also returned
order string (query)	pagination order (desc requires marker)

Responses

Response content type

application/json

Code Description

200

Example Value Model

```
{  
  "responseTime": "2018-02-01T16:22:31.066Z",  
  "status": "success",  
  "apiVersion": "2.1"  
}
```

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. 按一下HTTP動作以查看申請詳細資料。
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、您可以按一下*模型*來瞭解每個欄位的需求。
4. 按一下*試用*。

5. 提供任何必要的參數、或視需要修改申請本文。
6. 按一下*執行*。
7. 檢閱回應代碼以判斷要求是否成功。

相關資訊

["防範跨網站要求偽造 \(CSRF\) "](#)

["管理StorageGRID"](#)

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*不相容*的變更時、會使租戶管理API的主要版本與舊版相容。當做出*與舊版相容*的變更時、租戶管理API的次要版本會被提升。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
  ]
}
```

指定要求的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。

如需其他範例與詳細資料、請參閱線上API文件。



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、

管理租戶使用者的系統存取

您可以從聯盟身分識別來源匯入群組並指派管理權限、藉此授予使用者存取租戶帳戶的權限。您也可以建立本機租戶群組和使用者、除非整個StorageGRID 整個版的整套系統都有單一登入（SSO）功能。

- "使用身分識別聯盟"
- "管理群組"
- "管理本機使用者"

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。

- "設定聯盟身分識別來源"
- "強制與身分識別來源同步"
- "停用身分識別聯盟"

設定聯盟身分識別來源

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

您需要的產品

- 您必須使用支援的瀏覽器登入租戶管理程式。
- 您必須擁有特定的存取權限。
- 您必須使用Active Directory、OpenLDAP或Oracle Directory Server做為身分識別供應商。如果您要使用未列出的LDAP v3服務、則必須聯絡技術支援部門。
- 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。

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、則無法為此租戶設定個別聯盟身分識別來源。



This tenant account uses the LDAP server that is configured for the Grid Manager.
Contact the grid administrator for information or to change this setting.

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* Active Directory 、 OpenLDAP*或*其他*。

如果選擇* OpenLDAP*、請設定OpenLDAP伺服器。請參閱OpenLDAP伺服器設定指南。

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。
 - 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. 在「Configure LDAP server（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伺服器的伺服器主機名稱或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`
- 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。

6. 在*傳輸層安全性 (TLS) *區段中、選取安全性設定。

- 使用**ARTTLS** (建議使用)：使用ARTTLS來保護與LDAP伺服器的通訊安全。這是建議的選項。
- 使用**LDAPS**：LDAPS (LDAP over SSL) 選項使用TLS建立與LDAP伺服器的連線。基於相容性考量、支援此選項。
- 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。

如果Active Directory伺服器強制執行LDAP簽署、則不支援此選項。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。

8. 選取*測試連線*以驗證LDAP伺服器的連線設定。

如果連線有效、頁面右上角會出現確認訊息。

9. 如果連線有效、請選取*儲存*。

下列螢幕擷取畫面顯示使用Active Directory之LDAP伺服器的組態值範例。

LDAP service type

Select the type of LDAP service you want to configure.

Active Directory

OpenLDAP

Other

Configure LDAP server (All fields are required)

Hostname

my-active-directory.example.com

Port

389

Username

MyDomain\Administrator

Password

●●●●●●●●

Group Base DN

DC=storagegrid,DC=example,DC=com

User Base DN

DC=storagegrid,DC=example,DC=com

相關資訊

["租戶管理權限"](#)

["設定OpenLDAP伺服器的準則"](#)

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。

memberOf和refert覆疊

應啟用memberOf和refert覆疊。如需詳細資訊、請參閱OpenLDAP管理員指南中的反轉群組成員資格維護說明。

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OpenLDAP系統管理員指南中有關反轉群組成員資格維護的資訊。

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。

您需要的產品

- 您必須使用支援的瀏覽器登入租戶管理程式。
- 您必須擁有特定的存取權限。
- 必須啟用已儲存的身分識別來源。

步驟

1. 選擇*存取管理*>*身分識別聯盟*。

此時會出現「身分識別聯盟」頁面。「同步伺服器」按鈕位於頁面右上角。



如果未啟用儲存的身分識別來源、則*同步伺服器*按鈕將不會作用。

2. 選擇*同步伺服器*。

隨即顯示確認訊息、指出同步已成功啟動。

相關資訊

["租戶管理權限"](#)

停用身分識別聯盟

如果您為此租戶設定身分識別聯盟服務、則可以暫時或永久停用租戶群組和使用者的身分識別聯盟。停用身分識別聯盟時StorageGRID、不會在該系統與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、讓您日後可以輕鬆地重新啟用身分識別聯

盟。

您需要的產品

- 您必須使用支援的瀏覽器登入租戶管理程式。
- 您必須擁有特定的存取權限。

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保留對租戶帳戶的存取權、直到工作階段過期為止、但他們將無法在工作階段到期後登入。
- 不會在StorageGRID 整個系統與身分識別來源之間進行同步。

步驟

1. 選擇*存取管理*>*身分識別聯盟*。
2. 取消選取「啟用身分識別聯盟」核取方塊。
3. 選擇*保存*。

相關資訊

["租戶管理權限"](#)

管理群組

您可以指派權限給使用者群組、以控制租戶使用者可以執行的工作。您可以從身分識別來源（例如Active Directory或OpenLDAP）匯入聯盟群組、也可以建立本機群組。



如果StorageGRID 您的系統啟用單一登入（SSO）、則本機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來存取S3和Swift資源。

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。由於快取、變更可能需要15分鐘才能生效。

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	僅限S3租戶。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) *>*我的S3存取金鑰*功能表選項。
管理所有的儲存區	<ul style="list-style-type: none">• 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將不會看到「桶」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。 <p>*附註：*您只能從租戶管理API將「管理所有桶」權限指派給Swift群組。您無法使用租戶管理程式將此權限指派給Swift群組。</p>
管理端點	僅限S3租戶。可讓使用者使用租戶管理程式或租戶管理API來建立或編輯端點、這些端點是StorageGRID 用作支援不整平台服務的目的地。 沒有此權限的使用者不會看到*平台服務端點*功能表選項。

相關資訊

["使用S3"](#)

["使用Swift"](#)

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。

您需要的產品

- 您必須使用支援的瀏覽器登入租戶管理程式。
- 您必須屬於具有「根存取」權限的使用者群組。
- 如果您打算匯入聯盟群組、表示您已設定身分識別聯盟、而且聯盟群組已存在於設定的身分識別來源中。

步驟

1. 選擇*存取管理*>*群組*。



2. 選取*建立群組*。
3. 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。

4. 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。
5. 選擇*繼續*。
6. 選取存取模式。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。
 - 讀寫（預設）：使用者可以登入租戶管理程式、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程式或租戶管理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。
7. 選取此群組的群組權限。

請參閱租戶管理權限的相關資訊。
8. 選擇*繼續*。
9. 選取群組原則、以判斷此群組成員將擁有哪些S3存取權限。
 - 無**S3**存取：預設。此群組中的使用者沒有S3資源的存取權、除非使用資源桶原則授予存取權。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。
- 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。如需群組原則的詳細資訊、包括語言語法和範例、請參閱實作S3用戶端應用程式的指示。

10. 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。

在此範例中、群組成員只能列出及存取符合其使用者名稱（金鑰前置碼）的資料夾、並在指定的儲存區中使用。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。

No S3 Access
 Read Only Access
 Full Access
 Custom
 (Must be a valid JSON formatted string.)

```

{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificFolder",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}
  
```

11. 根據您要建立同盟群組或本機群組、選取出現的按鈕：

- 聯盟群組：建立群組
- 本機群組：繼續

如果您要建立本機群組、在您選取*繼續*之後、會出現步驟4（新增使用者）。聯盟群組不會顯示此步驟。

12. 選取您要新增至群組的每個使用者核取方塊、然後選取*建立群組*。

您也可以選擇儲存群組、而不新增使用者。您可以稍後新增使用者至群組、或在新增使用者時選取群組。

13. 選擇*完成*。

您建立的群組會出現在群組清單中。由於快取、變更可能需要15分鐘才能生效。

相關資訊

["租戶管理權限"](#)

["使用S3"](#)

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。

您需要的產品

- 您必須使用支援的瀏覽器登入租戶管理程式。
- 您必須屬於具有「根存取」權限的使用者群組。
- 如果您打算匯入聯盟群組、表示您已設定身分識別聯盟、而且聯盟群組已存在於設定的身分識別來源中。

步驟

1. 選擇*存取管理*>*群組*。

<input type="checkbox"/>	Name	ID	Type	Access mode
<input type="checkbox"/>	Applications	22cc2e27-88ee-4461-a8c6-30b550beec0	Local	Read-write
<input type="checkbox"/>	Managers	8b15b131-1d21-4539-93ad-f2298347c4d8	Local	Read-write

2. 選取*建立群組*。
3. 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。

4. 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。

5. 選擇*繼續*。

6. 選取存取模式。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。

- 讀寫（預設）：使用者可以登入租戶管理程式、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程式或租戶管理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。

7. 設定群組權限。

- 如果使用者需要登入租戶管理程式或租戶管理API、請選取*根存取*核取方塊。（預設）
- 如果使用者不需要存取租戶管理程式或租戶管理API、請取消選取「根存取」核取方塊。例如、取消選取不需要存取租戶的應用程式核取方塊。然後、指派* Swift管理員*權限、讓這些使用者能夠管理容器和物件。

8. 選擇*繼續*。

9. 如果使用者需要使用Swift REST API、請選取「* Swift管理員*」核取方塊。

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。

10. 根據您要建立同盟群組或本機群組、選取出現的按鈕：

- 聯盟群組：建立群組
- 本機群組：繼續

如果您要建立本機群組、在您選取*繼續*之後、會出現步驟4（新增使用者）。聯盟群組不會顯示此步驟。

11. 選取您要新增至群組的每個使用者核取方塊、然後選取*建立群組*。

您也可以選擇儲存群組、而不新增使用者。您可以稍後新增使用者至群組、或在建立新使用者時選取群組。

12. 選擇*完成*。

您建立的群組會出現在群組清單中。由於快取、變更可能需要15分鐘才能生效。

相關資訊

["租戶管理權限"](#)

["使用Swift"](#)

檢視及編輯群組詳細資料

當您檢視群組的詳細資料時、可以變更群組的顯示名稱、權限、原則及屬於群組的使用者。

您需要的產品

- 您必須使用支援的瀏覽器登入租戶管理程式。
- 您必須屬於具有「根存取」權限的使用者群組。

步驟

1. 選擇*存取管理*>*群組*。
2. 選取您要檢視或編輯其詳細資料的群組名稱。

或者、您也可以選取*「動作」>「檢視群組詳細資料」*。

隨即顯示群組詳細資料頁面。以下範例顯示S3群組詳細資料頁面。

Overview

Display name:	Applications 
Unique name:	group/Applications
Type:	Local
Access mode:	Read-write
Permissions:	Root Access
S3 Policy:	None
Number of users in this group:	0

Group permissions

S3 group policy

Users

Manage group permissions

Select an access mode for this group and select one or more permissions.

Access mode

Select whether users can change settings and perform operations or whether they can only view settings and features.

Read-write Read-only

Group permissions

Select the tenant account permissions you want to assign to this group.

Root Access

Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.

Manage All Buckets

Allows users to change settings of all S3 buckets (or Swift containers) in this account.

Manage Endpoints

Allows users to configure endpoints for platform services.

Manage Your Own S3 Credentials

Allows users to create and delete their own S3 access keys.

Save changes

3. 視需要變更群組設定。



若要確保儲存變更、請在每個區段進行變更後、選取*儲存變更*。儲存變更時、頁面右上角會出現確認訊息。

- a. 或者、選取顯示名稱或編輯圖示  以更新顯示名稱。

您無法變更群組的唯一名稱。您無法編輯同盟群組的顯示名稱。

- b. 或者、請更新權限。

- c. 針對群組原則、請針對S3或Swift租戶進行適當的變更。

- 如果您正在編輯S3租戶的群組、請選擇不同的S3群組原則。如果您選取自訂S3原則、請視需要更新Json字串。
- 如果您正在編輯Swift租戶的群組、請選擇或取消選取「* Swift管理員*」核取方塊。

如需Swift Administrator權限的詳細資訊、請參閱建立Swift租戶群組的指示。

- d. 或者、新增或移除使用者。

4. 確認您已針對每個變更的區段選擇*儲存變更*。

由於快取、變更可能需要15分鐘才能生效。

相關資訊

["為S3租戶建立群組"](#)

["為Swift租戶建立群組"](#)

新增使用者至本機群組

您可以視需要將使用者新增至本機群組。

您需要的產品

- 您必須使用支援的瀏覽器登入租戶管理程式。
- 您必須屬於具有「根存取」權限的使用者群組。

步驟

1. 選擇*存取管理*>*群組*。

2. 選取您要新增使用者的本機群組名稱。

或者、您也可以選取*「動作」>「檢視群組詳細資料」*。

隨即顯示群組詳細資料頁面。

Overview

Display name:	Applications 
Unique name:	group/Applications
Type:	Local
Access mode:	Read-write
Permissions:	Root Access
S3 Policy:	None
Number of users in this group:	0

Group permissions

S3 group policy

Users

Manage group permissions

Select an access mode for this group and select one or more permissions.

Access mode

Select whether users can change settings and perform operations or whether they can only view settings and features.

Read-write Read-only

Group permissions

Select the tenant account permissions you want to assign to this group.

Root Access

Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.

Manage All Buckets

Allows users to change settings of all S3 buckets (or Swift containers) in this account.

Manage Endpoints

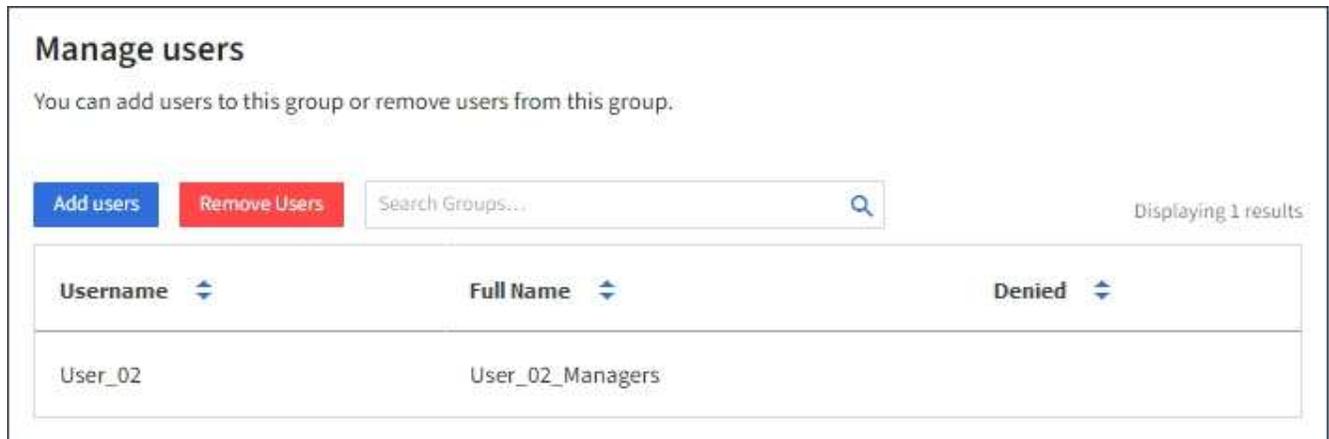
Allows users to configure endpoints for platform services.

Manage Your Own S3 Credentials

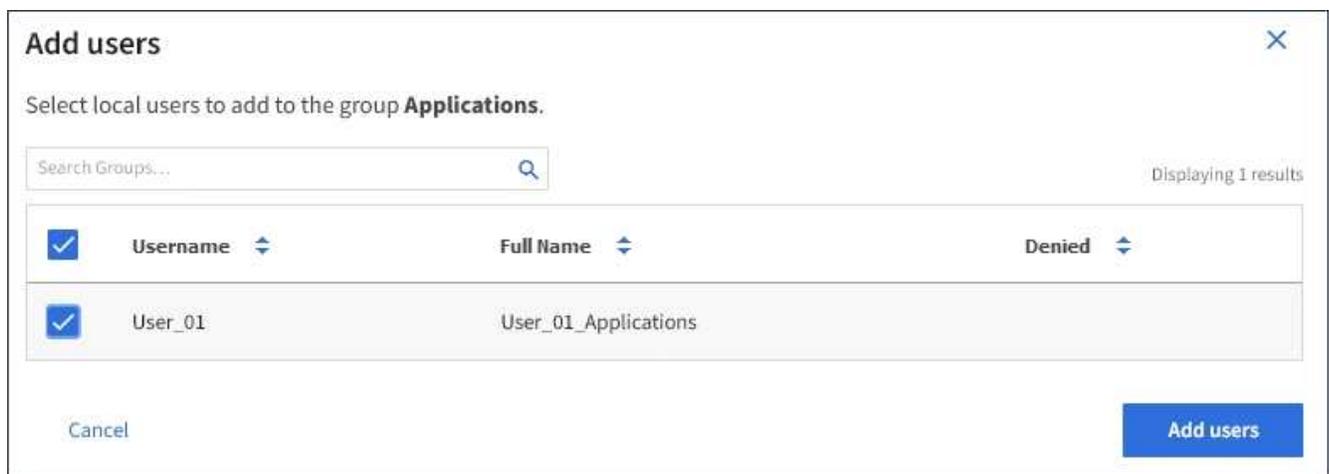
Allows users to create and delete their own S3 access keys.

Save changes

3. 選取*管理使用者*、然後選取*新增使用者*。



4. 選取您要新增至群組的使用者、然後選取*新增使用者*。



頁面右上角會出現確認訊息。由於快取、變更可能需要15分鐘才能生效。

編輯群組名稱

您可以編輯群組的顯示名稱。您無法編輯群組的唯一名稱。

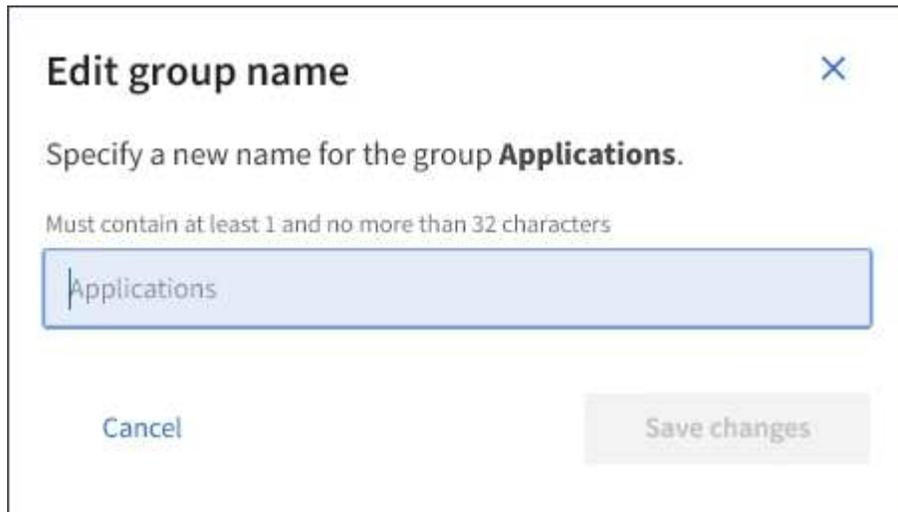
您需要的產品

- 您必須使用支援的瀏覽器登入租戶管理程式。
- 您必須屬於具有「根存取」權限的使用者群組。

步驟

1. 選擇*存取管理*>*群組*。
2. 選取您要編輯其顯示名稱之群組的核取方塊。
3. 選擇*操作*>*編輯群組名稱*。

「編輯群組名稱」對話方塊隨即出現。



4. 如果您正在編輯本機群組、請視需要更新顯示名稱。

您無法變更群組的唯一名稱。您無法編輯同盟群組的顯示名稱。

5. 選取*儲存變更*。

頁面右上角會出現確認訊息。由於快取、變更可能需要15分鐘才能生效。

相關資訊

["租戶管理權限"](#)

複製群組

您可以複製現有群組、以更快建立新群組。

您需要的產品

- 您必須使用支援的瀏覽器登入租戶管理程式。
- 您必須屬於具有「根存取」權限的使用者群組。

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. 選擇*複製群組*。如需建立群組的其他詳細資料、請參閱建立S3租戶或Swift租戶群組的指示。
4. 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。

5. 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。

- 選擇*繼續*。
- 視需要修改此群組的權限。
- 選擇*繼續*。
- 如有需要、如果您要複製S3租戶的群組、請從*新增S3原則*選項按鈕中選擇不同的原則。如果您選取自訂原則、請視需要更新Json字串。
- 選取*建立群組*。

相關資訊

["為S3租戶建立群組"](#)

["為Swift租戶建立群組"](#)

["租戶管理權限"](#)

刪除群組

您可以從系統中刪除群組。只屬於該群組的任何使用者將無法再登入租戶管理程式或使用租戶帳戶。

您需要的產品

- 您必須使用支援的瀏覽器登入租戶管理程式。
- 您必須屬於具有「根存取」權限的使用者群組。

步驟

- 選擇*存取管理*>*群組*。



The screenshot shows a web interface titled "Groups". Below the title is a subtitle: "Create and manage local and federated groups. Set group permissions to control access to specific pages and features." There is a "2 groups" indicator and a "Create group" button. Below this is an "Actions" dropdown menu. The main content is a table with the following data:

<input type="checkbox"/>	Name	ID	Type	Access mode
<input type="checkbox"/>	Applications	22cc2e27-88ee-4461-a8c6-30b550beec0	Local	Read-write
<input type="checkbox"/>	Managers	8b15b131-1d21-4539-93ad-f2298347c4d8	Local	Read-write

At the bottom right of the table area, there are navigation arrows: "← Previous 1 Next →".

- 選取您要刪除之群組的核取方塊。

3. 選擇*操作*>*刪除群組*。

隨即顯示確認訊息。

4. 選擇*刪除群組*以確認您要刪除確認訊息中所示的群組。

頁面右上角會出現確認訊息。由於快取、變更可能需要15分鐘才能生效。

相關資訊

["租戶管理權限"](#)

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root使用者。

您需要的產品

- 您必須使用支援的瀏覽器登入租戶管理程式。
- 您必須屬於具有「根存取」權限的讀寫使用者群組。



如果StorageGRID 您的系統啟用單一登入 (SSO) 、則本機使用者將無法登入租戶管理程式或租戶管理API、不過他們可以根據群組權限、使用S3或Swift用戶端應用程式來存取租戶的資源。

存取「使用者」頁面

選擇*存取管理*>*使用者*。

Users

View local and federated users. Edit properties and group membership of local users.

3 users

Create user

Actions

<input type="checkbox"/>	Username	Full Name	Denied	Type
<input type="checkbox"/>	root	Root		Local
<input type="checkbox"/>	User_01	User_01		Local
<input type="checkbox"/>	User_02	User_02		Local

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使用者沒有套用管理權限或S3群組原則。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使用者不具備管理權限或Swift Container存取權。

步驟

1. 選取*建立使用者*。
2. 填寫下列欄位。
 - 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：此使用者用來登入的名稱。使用者名稱必須是唯一的、而且無法變更。
 - 密碼：使用者登入時使用的密碼。
 - 確認密碼：在「密碼」欄位中輸入相同的密碼。
 - 拒絕存取：如果您選取*是*、此使用者就無法登入租戶帳戶、即使該使用者仍屬於一或多個群組。

例如、您可以使用此功能暫時暫停使用者登入的能力。

3. 選擇*繼續*。
4. 將使用者指派給一或多個本機群組。

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。

5. 選取*建立使用者*。

由於快取、變更可能需要15分鐘才能生效。

編輯使用者詳細資料

當您編輯使用者的詳細資料時、可以變更使用者的全名和密碼、將使用者新增至不同的群組、以及防止使用者存取租戶。

步驟

1. 在使用者清單中、選取您要檢視或編輯其詳細資料的使用者名稱。

或者、您也可以選取使用者的核取方塊、然後選取*「Actions」 (動作) > 「View user details」 (檢視使用者詳細資料) *。

2. 視需要變更使用者設定。

- a. 選取全名或編輯圖示、視需要變更使用者的全名  在「總覽」區段中。

您無法變更使用者名稱。

- b. 在*密碼*索引標籤上、視需要變更使用者的密碼。
- c. 在*存取*索引標籤上、允許使用者登入 (選取*否*)、或視需要禁止使用者登入 (選取*是*)。
- d. 在*群組*索引標籤上、視需要將使用者新增至群組或從群組中移除使用者。
- e. 視需要為每個區段選取*儲存變更*。

由於快取、變更可能需要15分鐘才能生效。

複製本機使用者

您可以複製本機使用者、以更快建立新使用者。

步驟

1. 在使用者清單中、選取您要複製的使用者。

2. 選擇*複製使用者*。

3. 修改新使用者的下列欄位。

- 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：此使用者用來登入的名稱。使用者名稱必須是唯一的、而且無法變更。
- 密碼：使用者登入時使用的密碼。
- 確認密碼：在「密碼」欄位中輸入相同的密碼。
- 拒絕存取：如果您選取*是*、此使用者就無法登入租戶帳戶、即使該使用者仍屬於一或多個群組。

例如、您可以使用此功能暫時暫停使用者登入的能力。

4. 選擇*繼續*。

5. 選取一或多個本機群組。

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。

6. 選取*建立使用者*。

由於快取、變更可能需要15分鐘才能生效。

刪除本機使用者

您可以永久刪除不再需要存取StorageGRID 該經銷帳戶的本機使用者。

使用租戶管理程式、您可以刪除本機使用者、但不能刪除同盟使用者。您必須使用同盟識別來源來刪除同盟使用者。

步驟

1. 在使用者清單中、選取您要刪除之本機使用者的核取方塊。
2. 選取*「動作*」>*「刪除使用者*」。
3. 在確認對話方塊中、選取*刪除使用者*以確認您要從系統中刪除使用者。

由於快取、變更可能需要15分鐘才能生效。

相關資訊

["租戶管理權限"](#)

管理S3租戶帳戶

您可以使用租戶管理程式來管理S3存取金鑰、以及建立和管理S3儲存區。

- ["管理S3存取金鑰"](#)
- ["管理S3儲存區"](#)

管理S3存取金鑰

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。

關於這項工作

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S3租戶帳戶中的貯體和物件。

您需要的產品

- 您必須使用支援的瀏覽器登入租戶管理程式。
- 您必須擁有「管理自己的S3認證」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、請勿建立超過您所需的金鑰、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很低、而且您不需要定期建立新金鑰、則不必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。

Create access key

1 Choose expiration time ————— 2 Download access key

Choose expiration time

Do not set an expiration time
This access key will never expire.

Set an expiration time

MM/DD/YYYY  HH : MM AM

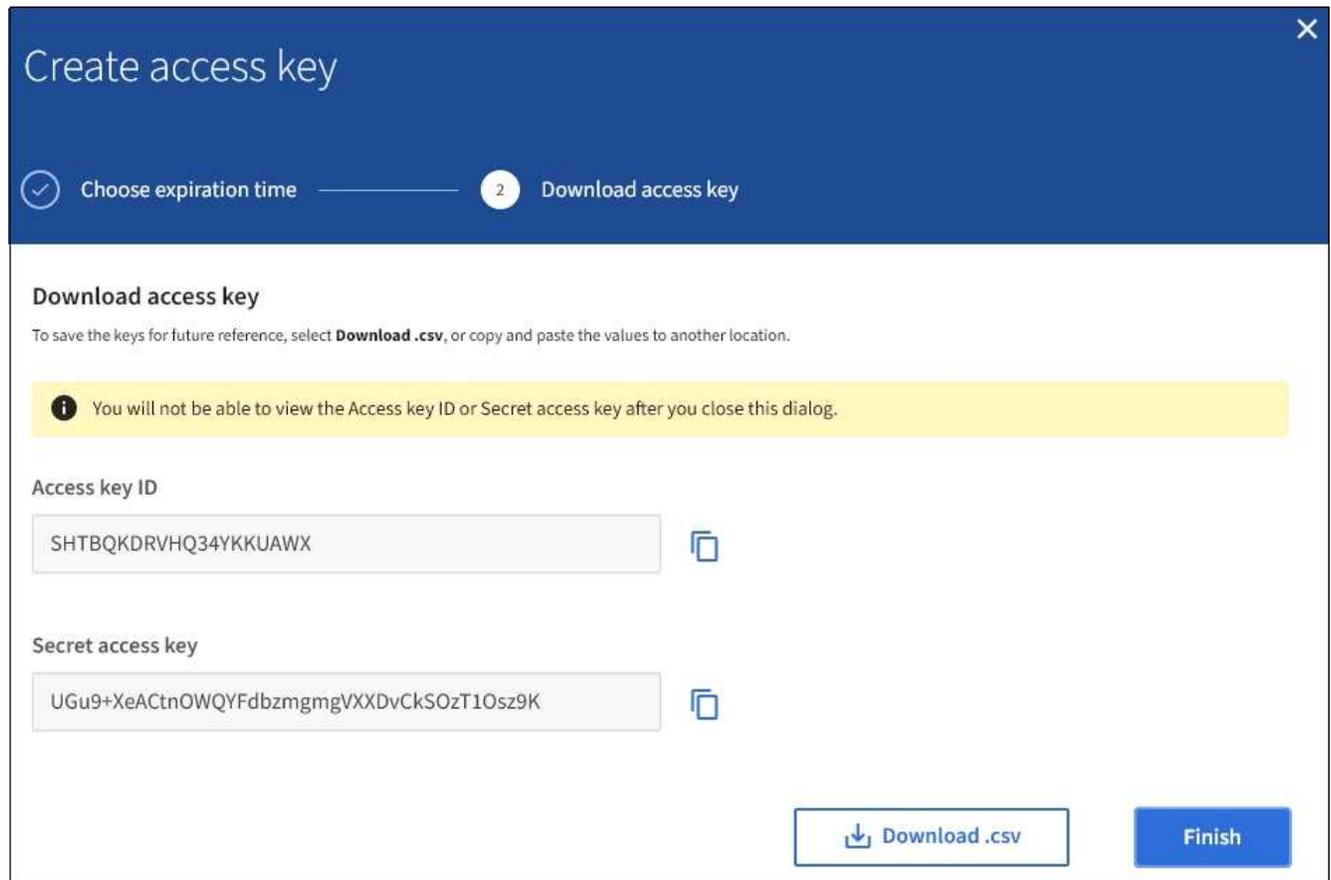
Cancel **Create access key**

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。



6. 選擇*完成*。

新金鑰會列在「我的存取金鑰」頁面上。由於快取、變更可能需要15分鐘才能生效。

相關資訊

["租戶管理權限"](#)

檢視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。您可以視需要建立新的金鑰或刪除不再使用的金鑰。

您需要的產品

- 您必須使用支援的瀏覽器登入租戶管理程式。
- 您必須擁有「管理自己的S3認證」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。

「我的存取金鑰」頁面隨即出現、並列出任何現有的存取金鑰。

My access keys

Manage your personal S3 access keys. If a key will expire soon, you can create a new key and delete the one it is replacing.

4 keys Create key

Delete key

<input type="checkbox"/>	Access key ID	Expiration time
<input type="checkbox"/>	*****OTLS	2020-11-23 12:00:00 MST
<input type="checkbox"/>	*****0M45	2020-12-01 19:00:00 MST
<input type="checkbox"/>	*****69QJ	None
<input type="checkbox"/>	*****3R8P	None

2. 按*過期時間*或*存取金鑰ID*來排序金鑰。
3. 視需要建立新的金鑰、並手動刪除您不再使用的金鑰。

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。

相關資訊

["建立自己的S3存取金鑰"](#)

["刪除自己的S3存取金鑰"](#)

刪除自己的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。

您需要的產品

- 您必須使用支援的瀏覽器登入租戶管理程式。
- 您必須擁有「管理自己的S3認證」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。

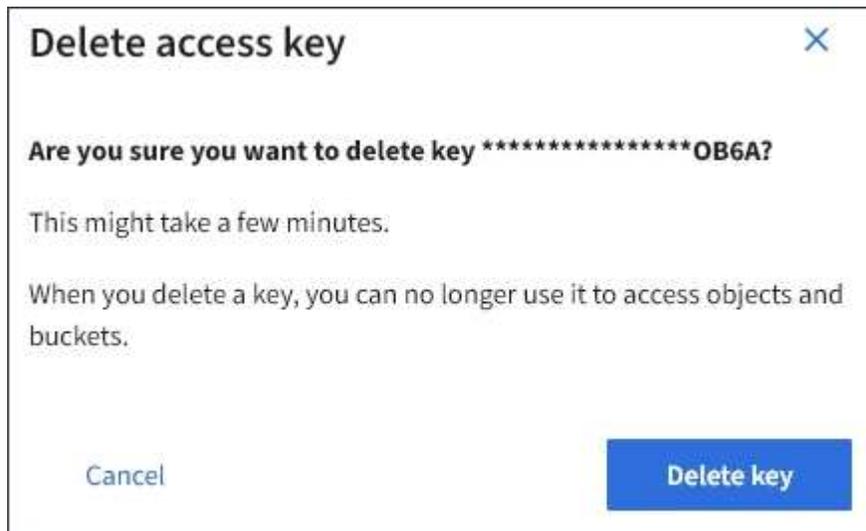
步驟

1. 選擇*儲存設備 (S3) >*我的存取金鑰。

「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. 選取您要移除之每個存取金鑰的核取方塊。
3. 選取*刪除機碼*。

隨即顯示確認對話方塊。



4. 選取*刪除機碼*。

頁面右上角會出現確認訊息。由於快取、變更可能需要15分鐘才能生效。

相關資訊

["租戶管理權限"](#)

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。

您需要的產品

- 您必須使用支援的瀏覽器登入租戶管理程式。
- 您必須具有「根存取」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、請勿建立超過使用者需求的金鑰、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很低、而且您不需要定期建立新金鑰、則不必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*」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。

Create access key

1 Choose expiration time ————— 2 Download access key

Choose expiration time

Do not set an expiration time
This access key will never expire.

Set an expiration time

MM/DD/YYYY  HH : MM AM

Cancel Create access key

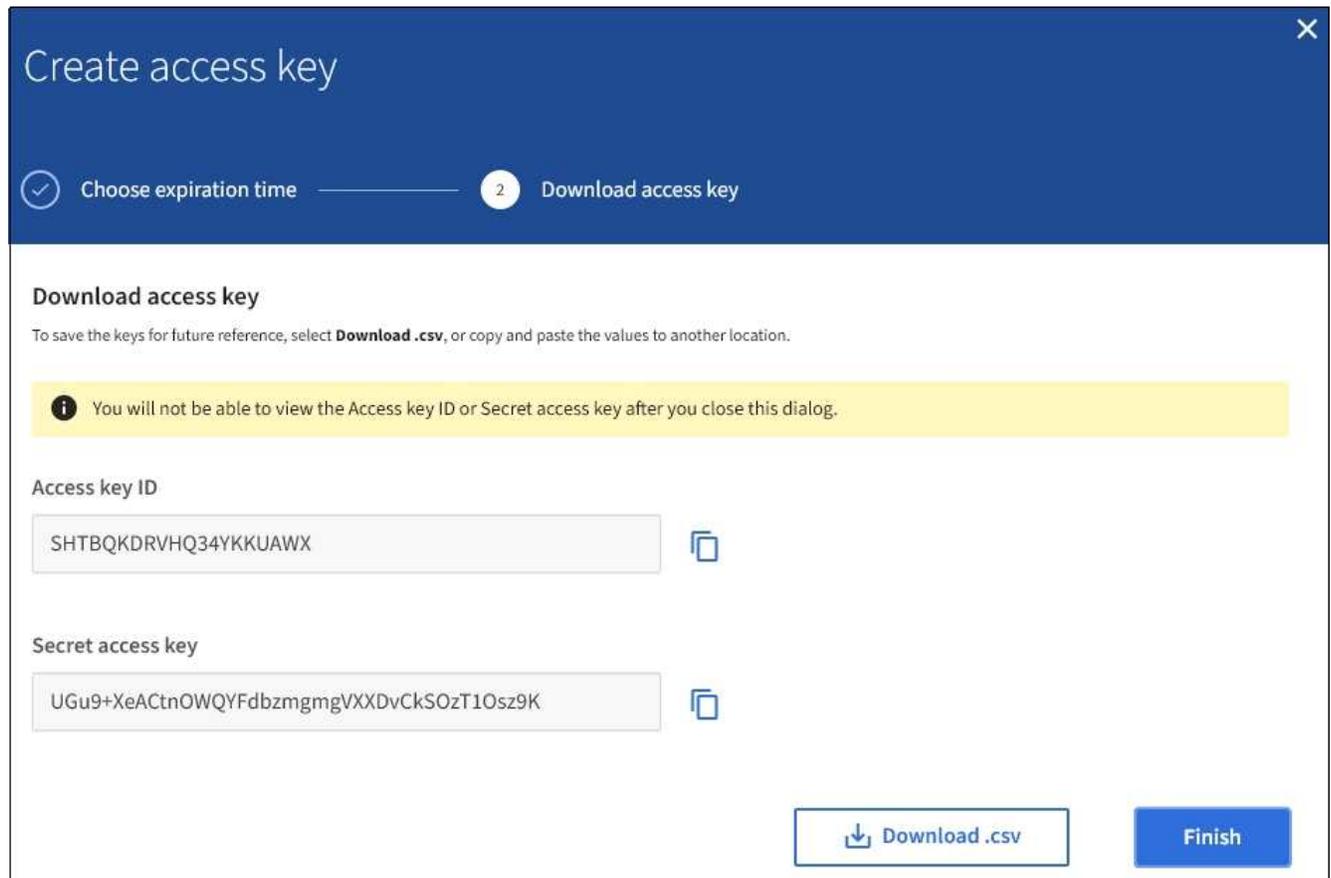
5. 選取*建立存取金鑰*。

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。



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。由於快取、變更可能需要15分鐘才能生效。

相關資訊

"租戶管理權限"

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。

您需要的產品

- 您必須使用支援的瀏覽器登入租戶管理程式。
- 您必須具有「根存取」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

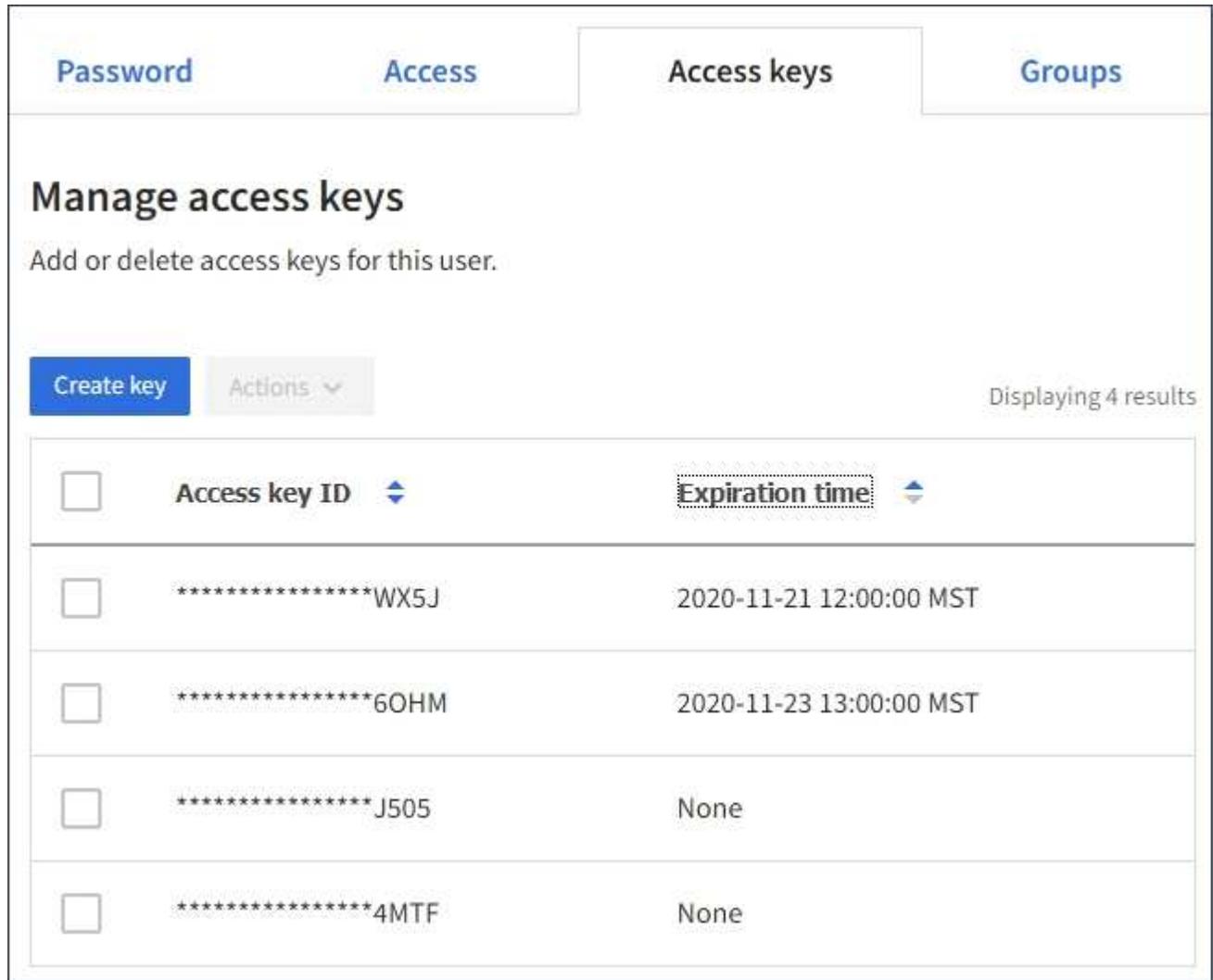
1. 選擇*存取管理*>*使用者*。

此時會出現「使用者」頁面、並列出現有的使用者。

2. 選取您要檢視其S3存取金鑰的使用者。

隨即顯示「使用者詳細資料」頁面。

3. 選擇*存取金鑰*。



The screenshot shows the 'Manage access keys' page in the AWS IAM console. The page has tabs for 'Password', 'Access', 'Access keys', and 'Groups'. The 'Access keys' tab is selected. Below the tabs, there is a heading 'Manage access keys' and a sub-heading 'Add or delete access keys for this user.' There are two buttons: 'Create key' and 'Actions'. The text 'Displaying 4 results' is visible. The main content is a table with the following data:

<input type="checkbox"/>	Access key ID	Expiration time
<input type="checkbox"/>	*****WX5J	2020-11-21 12:00:00 MST
<input type="checkbox"/>	*****6OHM	2020-11-23 13:00:00 MST
<input type="checkbox"/>	*****J505	None
<input type="checkbox"/>	*****4MTF	None

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

["建立其他使用者的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。

您需要的產品

- 您必須使用支援的瀏覽器登入租戶管理程式。
- 您必須具有「根存取」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*。

此時會出現「使用者」頁面、並列出現有的使用者。

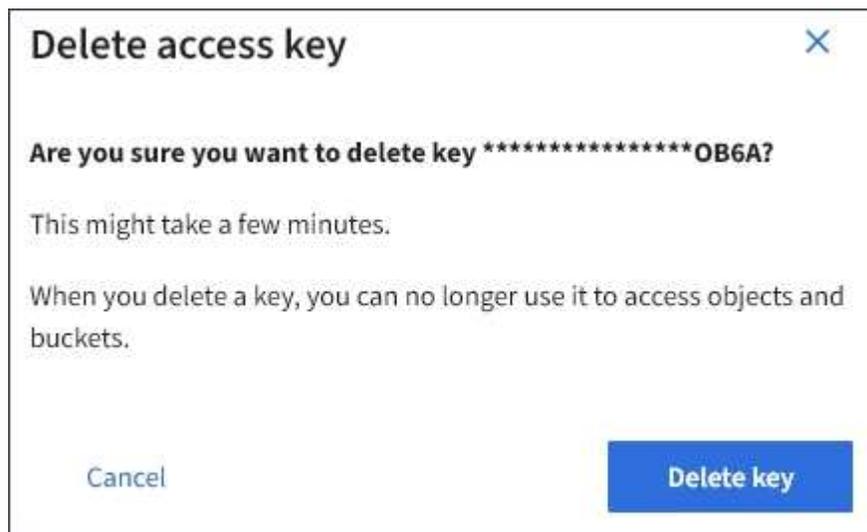
2. 選取您要管理其S3存取金鑰的使用者。

隨即顯示「使用者詳細資料」頁面。

3. 選取*存取金鑰*、然後選取您要刪除的每個存取金鑰核取方塊。

4. 選取*「動作*」>*「刪除選取的金鑰*」。

隨即顯示確認對話方塊。



5. 選取*刪除機碼*。

頁面右上角會出現確認訊息。由於快取、變更可能需要15分鐘才能生效。

相關資訊

["租戶管理權限"](#)

管理S3儲存區

如果您使用具有適當權限的S3租戶、可以建立、檢視及刪除S3儲存區、更新一致性層級設定、設定跨來源資源共用（CORS）、啟用及停用上次存取時間更新設定、以及管理S3平台服務。

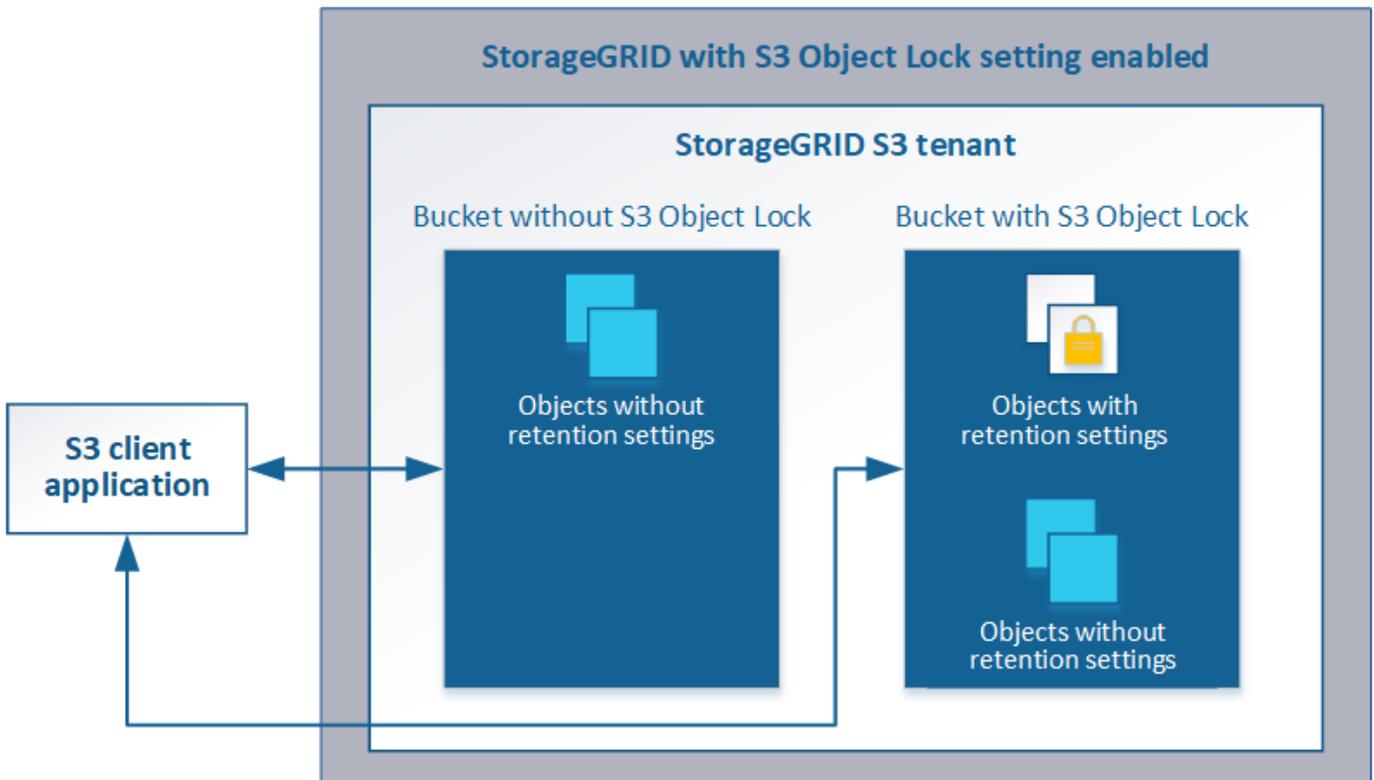
使用S3物件鎖定

如果物件必須符合保留法規要求、您可以使用StorageGRID 支援功能的S3物件鎖定功能。

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。如果某個儲存區已啟用S3物件鎖定、則S3用戶端應用程式可選擇性地指定該儲存區中任何物件版本的保留設定。物件版本必須具有指定的保留設定、才能受到S3物件鎖定的保護。



「S3物件鎖定」StorageGRID 功能提供單一保留模式、相當於Amazon S3法規遵循模式。依預設、受保護的物件版本無法由任何使用者覆寫或刪除。「S3物件鎖定」StorageGRID 功能不支援管理模式、也不允許具有特殊權限的使用者略過保留設定或刪除受保護的物件。

如果某個儲存區已啟用S3物件鎖定、則S3用戶端應用程式可在建立或更新物件時、選擇性地指定下列任一或兩個物件層級保留設定：

- 保留截止日期：如果物件版本的保留截止日期在未來、則可擷取物件、但無法修改或刪除。視需要可增加物件的保留截止日期、但此日期不可減少。

- 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。

如需這些設定的詳細資訊、請前往「使用S3物件鎖定」 ["S3 REST API支援的作業和限制"](#)。

管理符合舊規範的儲存庫

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NetApp知識庫文章。

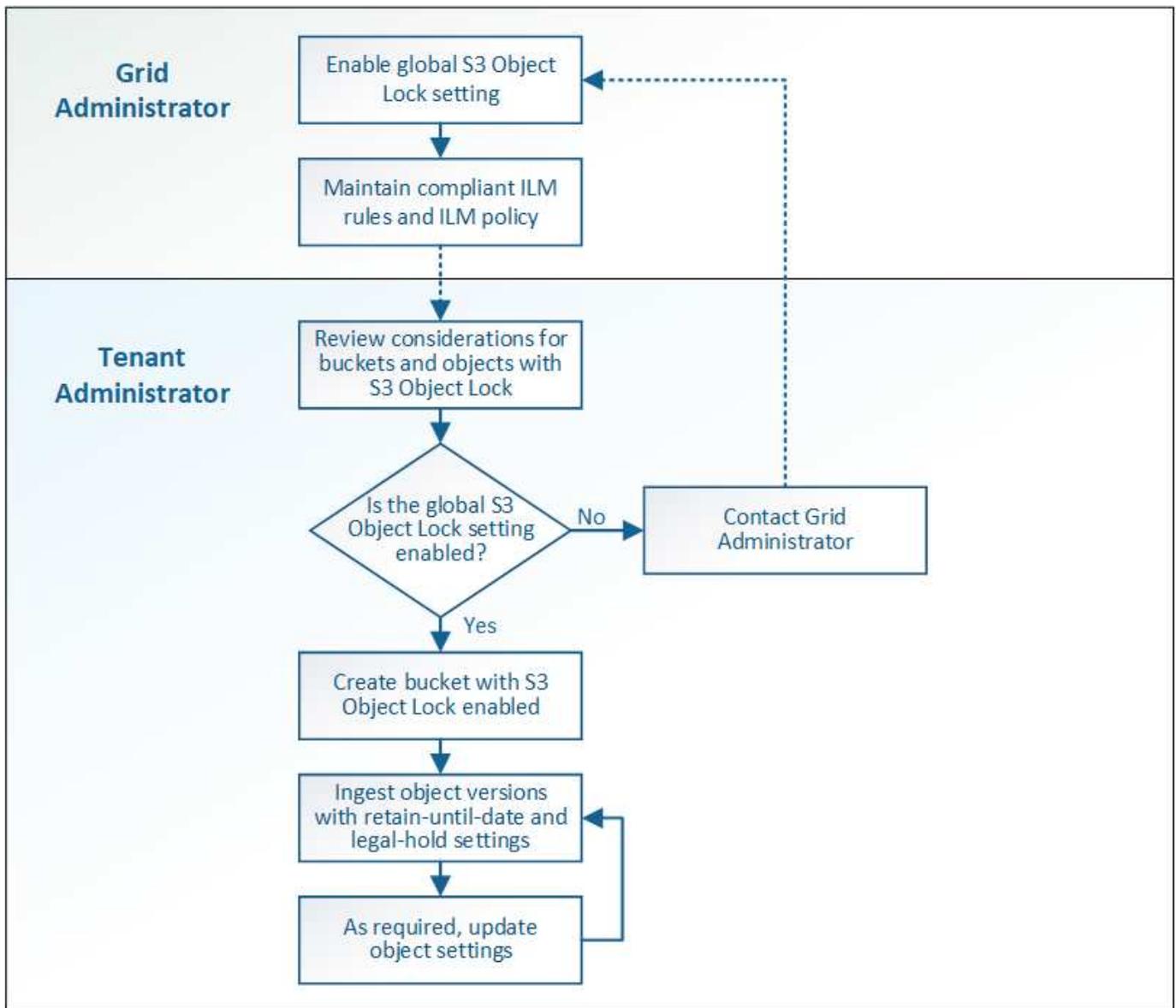
["NetApp知識庫：如何管理StorageGRID 支援老舊的知識庫、請參閱《知識庫文章"](#)

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。如需詳細資料、請聯絡網格管理員、或參閱資訊生命週期管理的物件管理說明。

啟用全域S3物件鎖定設定之後、您可以建立啟用S3物件鎖定的儲存區。然後、您可以使用S3用戶端應用程式、選擇性地為每個物件版本指定保留設定。



相關資訊

"使用ILM管理物件"

S3物件鎖定需求

在啟用儲存區的S3物件鎖定之前、請先檢閱S3物件鎖定儲存區和物件的需求、以及啟用S3物件鎖定之儲存區中物件的生命週期。

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。

此租戶管理程式範例顯示已啟用S3物件鎖定的儲存區。

Buckets

Create buckets and manage bucket settings.

1 bucket Create bucket

Actions ▾

<input type="checkbox"/>	Name ▾	S3 Object Lock [?] ▾	Region ▾	Object Count [?] ▾	Space Used [?] ▾	Date Created ▾
<input type="checkbox"/>	bank-records	✓	us-east-1	0	0 bytes	2021-01-06 16:53:19 MST

← Previous **1** Next →

- 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。您無法為現有的儲存區啟用S3物件鎖定。
- S3物件鎖定需要庫位版本管理。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。
- 在建立啟用S3物件鎖定的儲存區之後、您無法停用該儲存區的S3物件鎖定或暫停版本管理。
- 啟用S3物件鎖定的支援區段沒有預設保留期間StorageGRID。而是S3用戶端應用程式可以選擇性地為新增至該儲存區的每個物件版本指定保留日期和合法保留設定。
- S3物件生命週期儲存區支援儲存區生命週期組態。
- 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

- S3用戶端應用程式必須針對需要受到S3物件鎖定保護的每個物件、指定保留設定。
- 您可以增加物件版本的保留截止日期、但絕不能減少此值。
- 如果您收到尚待處理的法律行動或法規調查通知、您可以在物件版本上保留合法資訊、以保留相關資訊。當物件版本處於合法持有狀態時、即使StorageGRID 物件已達到保留日期、也無法從該物件刪除。一旦取消合法持有、如果已達到保留截止日期、就可以刪除物件版本。
- S3物件鎖定需要使用版本控制的儲存區。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物件鎖定的儲存區中的每個物件都會經過三個階段：

1. 物件擷取

- 在啟用S3物件鎖定的儲存區中新增物件版本時、S3用戶端應用程式可選擇性地指定物件的保留設定（保留至日期、合法保留或兩者皆保留）。接著、將產生該物件的中繼資料、其中包括唯一的物件識別碼（UUID）和擷取日期與時間。StorageGRID
- 擷取具有保留設定的物件版本之後、就無法修改其資料和S3使用者定義的中繼資料。
- 不受物件資料限制、可獨立儲存物件中繼資料。StorageGRID它會在每個站台維護三份所有物件中繼資

料複本。

2. 物件保留

- 物件的多個複本是StorageGRID 由NetApp儲存的。複本的確切數量和類型、以及儲存位置、取決於使用中ILM原則中的相容規則。

3. 物件刪除

- 物件到達保留截止日期時、即可刪除。
- 無法刪除合法持有的物件。

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。當您建立桶時、必須指定桶的名稱和區域。如果StorageGRID 已針對整個S3物件鎖定設定啟用for the Sing系統、您可以選擇性地為儲存區啟用S3物件鎖定。

您需要的產品

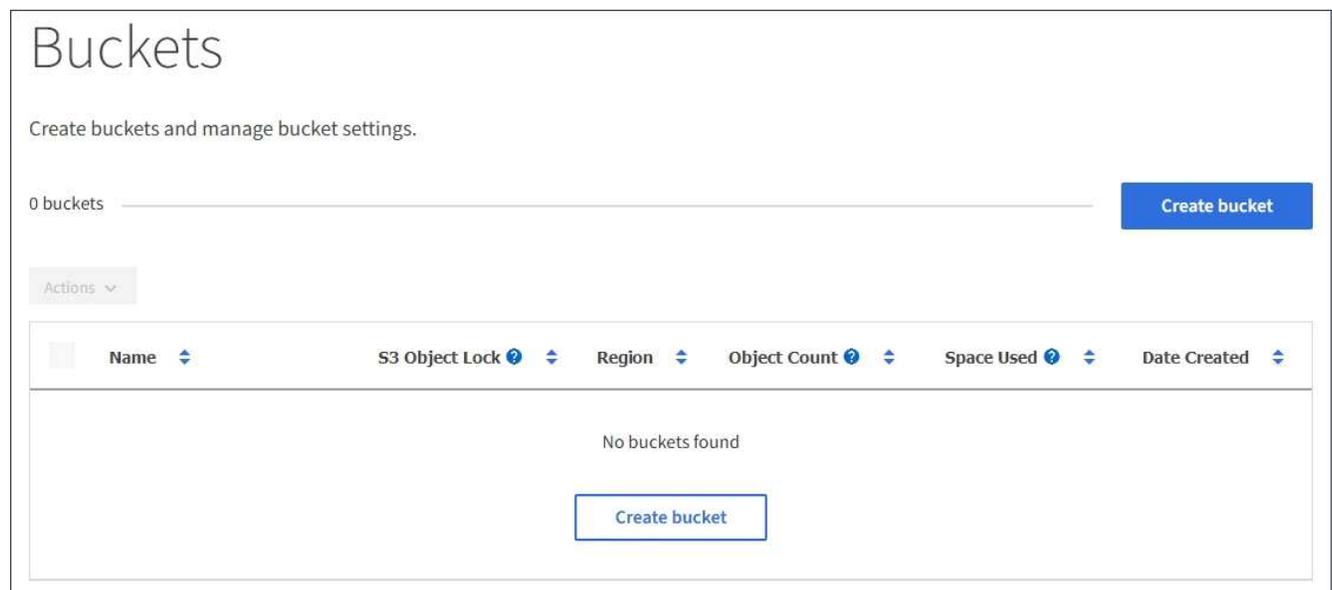
- 您必須使用支援的瀏覽器登入租戶管理程式。
- 您必須屬於具有「管理所有庫位」或「根存取」權限的使用者群組。這些權限會覆寫群組或儲存區原則中的權限設定。
- 如果您計畫建立S3物件鎖定的儲存區、StorageGRID 則必須已針對該系統啟用全域S3物件鎖定設定、而且您必須檢閱S3物件鎖定儲存區和物件的需求。

"使用S3物件鎖定"

步驟

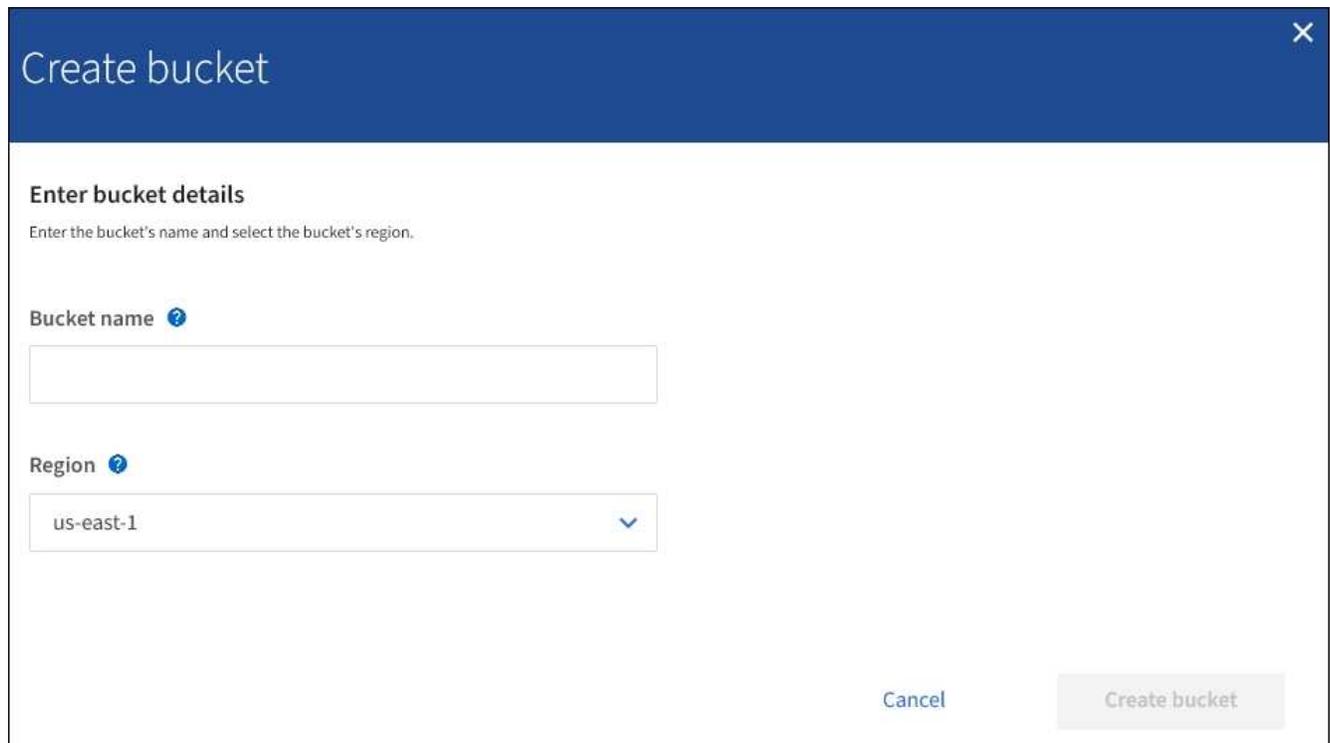
1. 選擇*儲存設備 (S3) >*桶。

此時會顯示「庫位」頁面、並列出所有已建立的庫位。



2. 選取*建立桶*。

此時會出現「建立儲存區」精靈。



如果已啟用全域S3物件鎖定設定、「建立儲存區」會包含第二個步驟、以管理儲存區的S3物件鎖定。

3. 輸入庫位的唯一名稱。



建立貯體後、您無法變更貯體名稱。

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。



如需詳細資訊、請參閱Amazon Web Services (AWS) 說明文件。

4. 選取此儲存區的區域。

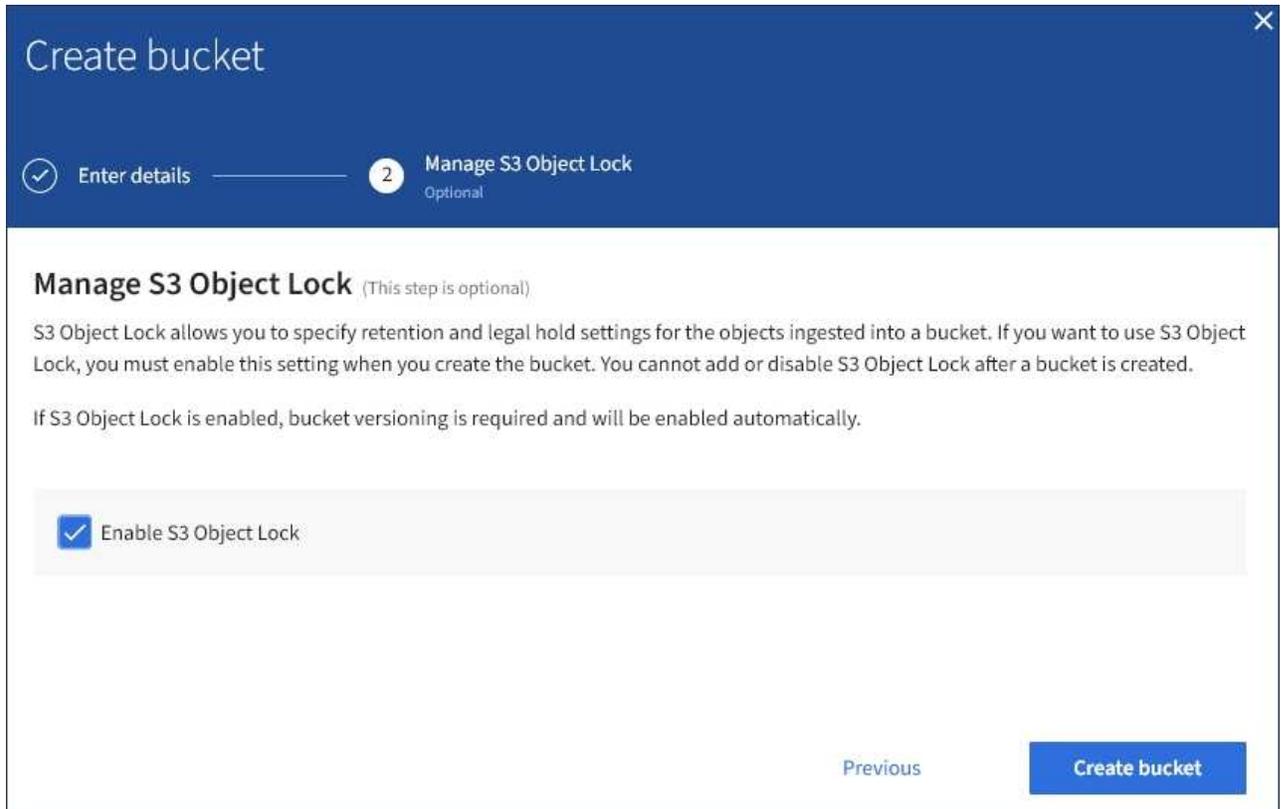
您的系統管理員負責管理可用的區域。StorageGRID儲存區的區域可能會影響套用至物件的資料保護原則。依預設、所有的儲存區都會在中建立 us-east-1 區域。



建立儲存貯體後、您無法變更區域。

5. 選擇* Create Bucket 或 Continue *。

- 如果未啟用全域S3物件鎖定設定、請選取*建立儲存區*。此庫位會建立並新增至「庫位」頁面上的表格。
- 如果已啟用全域S3物件鎖定設定、請選取*繼續*。出現步驟2「管理S3物件鎖定」。



6. 您也可以選取核取方塊來啟用此儲存區的S3物件鎖定。

S3用戶端應用程式必須先為儲存區啟用S3物件鎖定、才能為新增至儲存區的物件指定保留直到日期和合法保留設定。



建立儲存區之後、您無法啟用或停用S3物件鎖定。



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。

7. 選取*建立桶*。

此庫位會建立並新增至「庫位」頁面上的表格。

相關資訊

["使用ILM管理物件"](#)

["瞭解租戶管理API"](#)

"使用S3"

檢視S3儲存貯體詳細資料

您可以在租戶帳戶中檢視庫存箱和庫位設定清單。

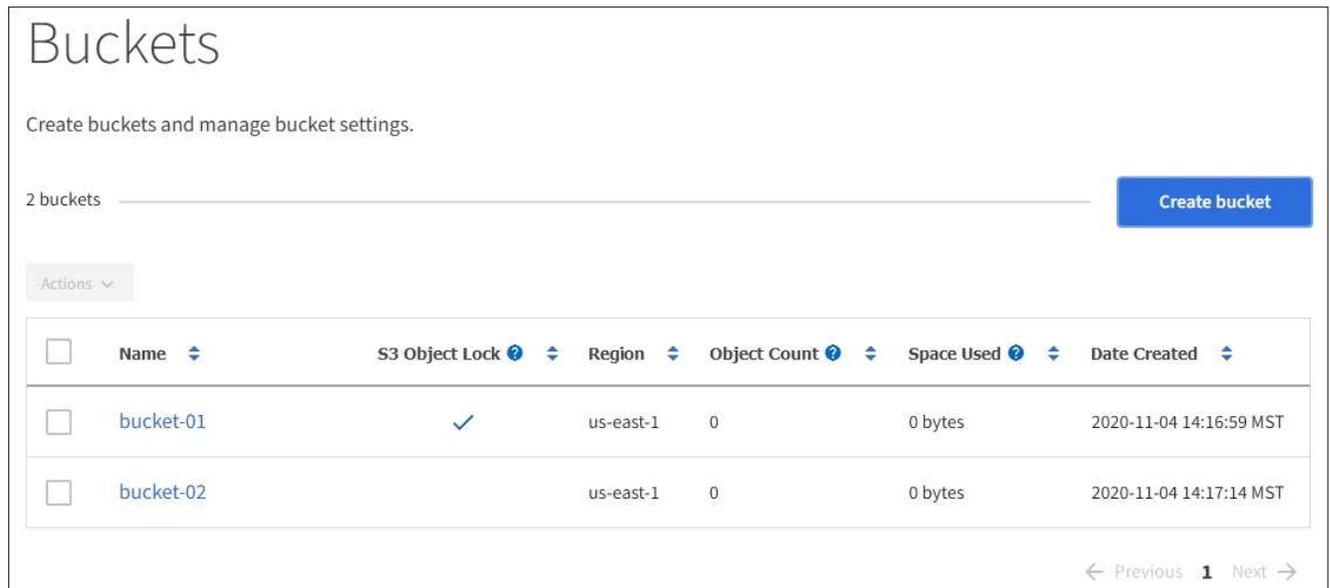
您需要的產品

- 您必須使用支援的瀏覽器登入租戶管理程式。

步驟

1. 選擇*儲存設備 (S3) >*桶。

此時會顯示「資源庫」頁面、並列出租戶帳戶的所有資源庫。



The screenshot shows a web interface titled "Buckets" with the subtitle "Create buckets and manage bucket settings." Below the title, it indicates "2 buckets" and a "Create bucket" button. An "Actions" dropdown menu is visible. The main content is a table with the following data:

<input type="checkbox"/>	Name	S3 Object Lock	Region	Object Count	Space Used	Date Created
<input type="checkbox"/>	bucket-01	✓	us-east-1	0	0 bytes	2020-11-04 14:16:59 MST
<input type="checkbox"/>	bucket-02		us-east-1	0	0 bytes	2020-11-04 14:17:14 MST

At the bottom right of the table, there are navigation controls: "← Previous 1 Next →".

2. 檢閱每個儲存區的資訊。

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。

- 名稱：庫位的唯一名稱、無法變更。
- S3物件鎖定：是否為此儲存區啟用S3物件鎖定。

如果停用全域S3物件鎖定設定、則不會顯示此欄。此欄也會顯示任何舊版相容桶的資訊。

- 區域：無法變更的庫位區域。
- 物件數：此儲存區中的物件數。
- 已用空間：此儲存區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：建立桶的日期和時間。



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。

3. 若要檢視及管理儲存區的設定、請選取儲存區名稱。

此時會顯示「庫位詳細資料」頁面。

此頁面可讓您檢視及編輯庫位選項、庫位存取及平台服務的設定。

請參閱設定每項設定或平台服務的指示。

The screenshot shows the AWS console interface for a bucket named 'bucket-02'. The breadcrumb is 'Buckets > bucket-02'. The main section is titled 'Overview' and contains the following details:

Name:	bucket-02
Region:	us-east-1
S3 Object Lock:	Disabled
Date created:	2020-11-04 14:51:59 MST

Below the overview, there are three tabs: 'Bucket options' (selected), 'Bucket access', and 'Platform services'. Under the 'Bucket options' tab, there are two settings:

Consistency level	Read-after-new-write	▼
Last access time updates	Disabled	▼

相關資訊

["變更一致性層級"](#)

["啟用或停用上次存取時間更新"](#)

["設定跨來源資源共享 \(CORS\) "](#)

["設定CloudMirror複寫"](#)

["設定事件通知"](#)

["設定搜尋整合服務"](#)

變更一致性層級

如果您使用的是S3租戶、則可以使用租戶管理程式或租戶管理API來變更在S3貯體中物件上執行的作業一致性控制。

您需要的產品

- 您必須使用支援的瀏覽器登入租戶管理程式。
- 您必須屬於具有「管理所有庫位」或「根存取」權限的使用者群組。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

一致性層級可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進行權衡。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. 選擇*儲存設備 (S3) >*桶。
2. 從清單中選取儲存貯體名稱。

此時會顯示「庫位詳細資料」頁面。

3. 選擇*庫位選項*>*一致性層級*。

Bucket options
Bucket access
Platform services

Consistency level
Read-after-new-write (default)
^

Change the consistency control for operations performed on the objects in the bucket. Consistency level makes a trade-off between the availability of the objects and the consistency of those objects across different Storage Nodes and sites.

In general, use the **Read-after-new-write** consistency level for your buckets. Then, if objects do not meet availability or consistency requirements, change the client application's behavior, or set the Consistency-Control header for an individual API request, which overrides the bucket setting.

- All
Provides the highest guarantee of consistency. All nodes receive the data immediately, or the request will fail.
- Strong-global
Guarantees read-after-write consistency for all client requests across all sites.
- Strong-site
Guarantees read-after-write consistency for all client requests within a site.
- Read-after-new-write (default)**
Provides read-after-write consistency for new objects and eventual consistency for object updates. Offers high availability, and data protection guarantees.

Note: If your application attempts HEAD operations on keys that do not exist, set the Consistency Level to **Available**, unless you require AWS S3 consistency guarantees. Otherwise, a high number of 500 Internal Server errors can result if one or more Storage Nodes are unavailable.

- Available
Behaves the same as the **Read-after-new-write** consistency level, but only provides eventual consistency for HEAD operations. Offers higher availability for HEAD operations than **Read-after-new-write** if Storage Nodes are unavailable. Differs from AWS S3 consistency guarantees for HEAD operations only.

4. 針對此儲存區中的物件執行的作業、選取一致性層級。

一致性層級	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。

一致性層級	說明
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。
讀取後新寫入（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。符合Amazon S3一致性保證。 附註：*如果您的應用程式嘗試對不存在的金鑰執行一般作業、請將一致性層級設為*可用、除非您需要Amazon S3一致性保證。否則、如果一個或多個儲存節點無法使用、可能會導致500個內部伺服器錯誤。
可用的（最終的頭端作業一致性）	其行為與*新寫入後讀取*一致性層級相同、但最終只能為頭端作業提供一致性。如果儲存節點無法使用、則頭端作業的可用度比*新寫入後讀取*高。不同於Amazon S3一致性保證、僅適用於頭端作業。

5. 選取*儲存變更*。

相關資訊

"租戶管理權限"

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StorageGRID 包含至少一個ILM規則的Sesrast Access Times*選項、其放置指示中才會使用。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 。

您需要的產品

- 您必須使用支援的瀏覽器登入租戶管理程式。
- 您必須屬於具有「管理所有庫位」或「根存取」權限的使用者群組。這些權限會覆寫群組或儲存區原則中的權限設定。

*上次存取時間*是ILM規則*參考時間*放置指示的其中一個可用選項。將規則的參考時間設定為「上次存取時間」、可讓網格管理員根據上次擷取（讀取或檢視）的時間、指定將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。



請參閱使用資訊生命週期管理來管理物件的指示。

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



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	<ul style="list-style-type: none"> • 否、來源複本 • 是、適用於目的地複本 	<ul style="list-style-type: none"> • 否、來源複本 • 是、適用於目的地複本 	<ul style="list-style-type: none"> • 是、來源複本 • 是、適用於目的地複本 	<ul style="list-style-type: none"> • 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. 選擇*儲存設備 (S3) >*桶。
2. 從清單中選取儲存貯體名稱。

此時會顯示「庫位詳細資料」頁面。

3. 選擇*庫位選項*>*上次存取時間更新*。
4. 選取適當的選項按鈕以啟用或停用上次存取時間更新。

Bucket options
Bucket access
Platform services

Consistency level Read-after-new-write ▼

Last access time updates Disabled ▲

Enable or disable last access time updates for the objects in this bucket.

When last access time updates are disabled, the following behavior applies to objects in the bucket:

- Requests to retrieve an object, its access control list, or its metadata do not update the object's last access time. The object is not added to ILM evaluation queues.
- Requests to update an object's metadata update the object's last access time. The object is added to ILM evaluation queues.
- Requests to copy an object from one bucket to another do not update the last access time for the source copy and do not add the source object to the ILM evaluation queue. However, the last access time is updated for the destination copy, and the destination object is added to ILM evaluation queues.
- A request to complete a multipart upload causes the last access time for the assembled object to be updated. The new object is added to ILM evaluation queues.

ⓘ Updating the last access time when an object is retrieved can reduce performance, especially for small objects.

Enable last access time updates when retrieving an object

Disable last access time updates when retrieving an object

Save changes

5. 選取*儲存變更*。

相關資訊

["租戶管理權限"](#)

["使用ILM管理物件"](#)

設定跨來源資源共享 (CORS)

如果您想要讓其他網域中的Web應用程式能夠存取S3儲存區中的儲存區和物件、可以設定S3儲存區的跨來源資源共享 (CORS)。

您需要的產品

- 您必須使用支援的瀏覽器登入租戶管理程式。
- 您必須屬於具有「管理所有庫位」或「根存取」權限的使用者群組。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

跨來源資源共享 (CORS) 是一種安全機制、可讓一個網域中的用戶端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>。

步驟

1. 使用文字編輯器建立啟用CORS所需的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。

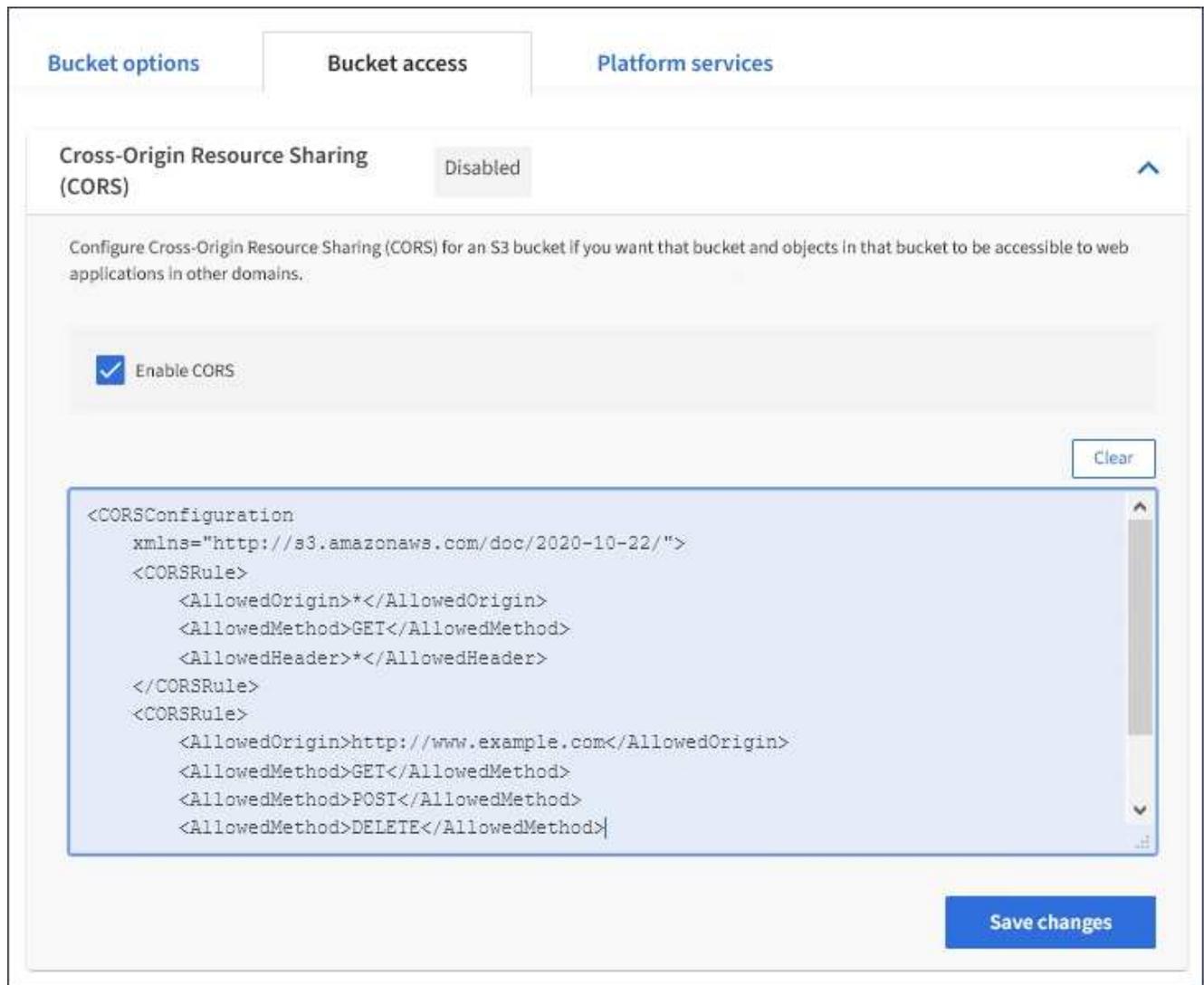
```
<CORSConfiguration
  xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
  <CORSRule>
    <AllowedOrigin>*</AllowedOrigin>
    <AllowedMethod>GET</AllowedMethod>
    <AllowedHeader>*</AllowedHeader>
  </CORSRule>
  <CORSRule>
    <AllowedOrigin>http://www.example.com</AllowedOrigin>
    <AllowedMethod>GET</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. 在租戶管理程式中、選取*儲存設備 (S3) >*桶。
3. 從清單中選取儲存貯體名稱。

此時會顯示「庫位詳細資料」頁面。

4. 選擇* Bucket access*>* Cross-Origin Resource Sharing (CORS) *。
5. 選取「啟用**CORS**」核取方塊。
6. 將CORS組態XML貼到文字方塊中、然後選取*儲存變更*。



7. 若要修改儲存區的CORS設定、請更新文字方塊中的CORS組態XML、或選取* Clear*重新開始。然後選取* 儲存變更*。
8. 若要停用儲存區的CORS、請取消選取「啟用**CORS**」核取方塊、然後選取「儲存變更」。

刪除S3儲存區

您可以使用租戶管理程式刪除空的S3儲存區。

您需要的產品

- 您必須使用支援的瀏覽器登入租戶管理程式。
- 您必須屬於具有「管理所有庫位」或「根存取」權限的使用者群組。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

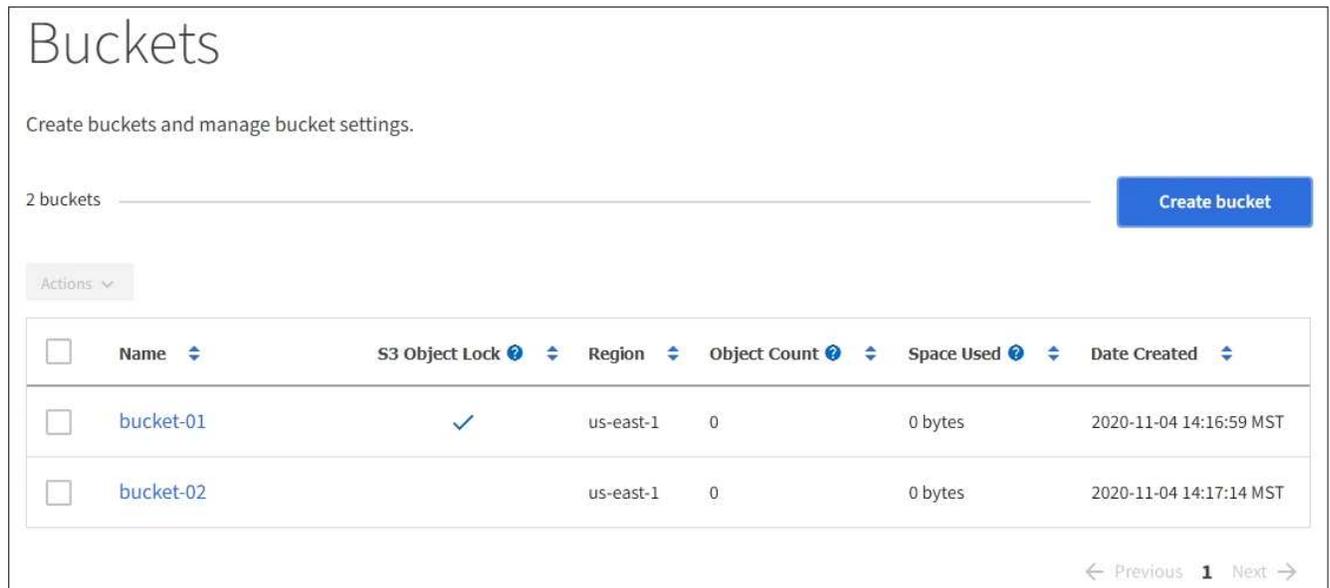
這些指示說明如何使用租戶管理程式刪除S3儲存區。您也可以使用租戶管理API或S3 REST API來刪除S3桶。

如果S3儲存區包含物件或非目前物件版本、則無法刪除。如需如何刪除S3版本控制物件的相關資訊、請參閱資訊生命週期管理物件的管理指示。

步驟

1. 選擇*儲存設備 (S3) >*桶。

此時會顯示「庫位」頁面、並顯示所有現有的S3庫位。



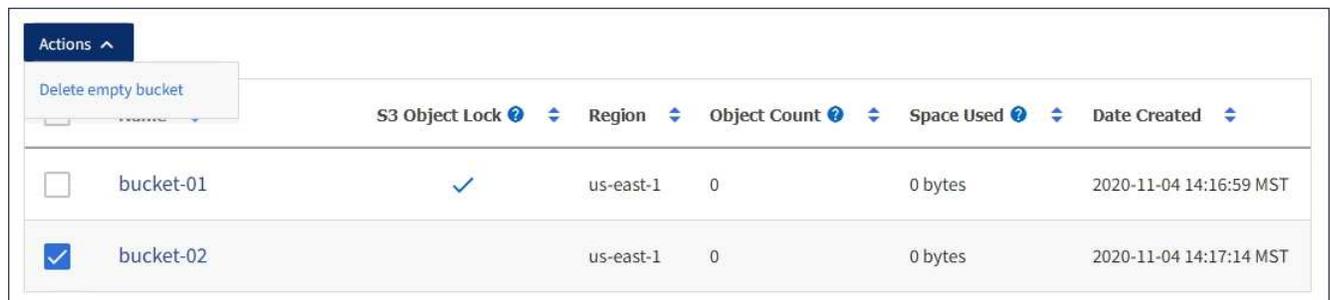
The screenshot shows the AWS S3 Buckets console. At the top, it says "Buckets" and "Create buckets and manage bucket settings." Below this, it indicates "2 buckets" and has a "Create bucket" button. There is an "Actions" dropdown menu. The main content is a table with the following columns: Name, S3 Object Lock, Region, Object Count, Space Used, and Date Created. The table contains two rows: "bucket-01" and "bucket-02".

<input type="checkbox"/>	Name	S3 Object Lock	Region	Object Count	Space Used	Date Created
<input type="checkbox"/>	bucket-01	✓	us-east-1	0	0 bytes	2020-11-04 14:16:59 MST
<input type="checkbox"/>	bucket-02		us-east-1	0	0 bytes	2020-11-04 14:17:14 MST

2. 選取您要刪除之空白儲存格的核取方塊。

「動作」功能表已啟用。

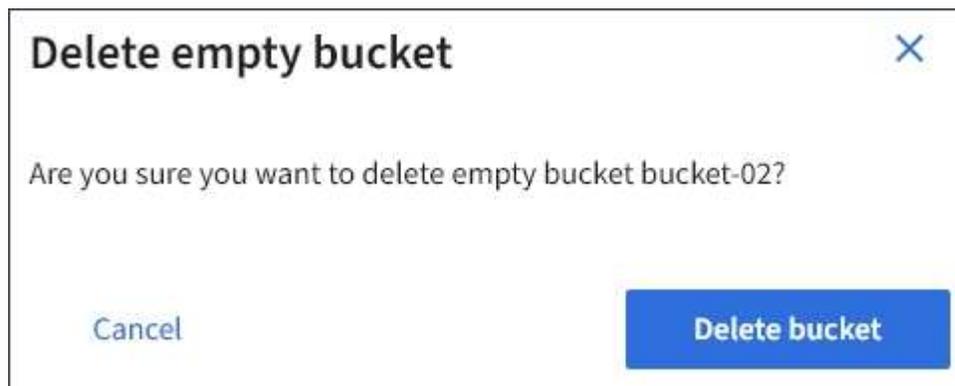
3. 從「動作」功能表中、選取*「刪除空桶」*。



The screenshot shows the AWS S3 Buckets console with the "Actions" dropdown menu open. The "Delete empty bucket" option is selected. The table below shows that the checkbox for "bucket-02" is checked.

<input type="checkbox"/>	Name	S3 Object Lock	Region	Object Count	Space Used	Date Created
<input type="checkbox"/>	bucket-01	✓	us-east-1	0	0 bytes	2020-11-04 14:16:59 MST
<input checked="" type="checkbox"/>	bucket-02		us-east-1	0	0 bytes	2020-11-04 14:17:14 MST

隨即顯示確認訊息。



The screenshot shows a confirmation dialog box titled "Delete empty bucket". The text inside asks "Are you sure you want to delete empty bucket bucket-02?". There are two buttons: "Cancel" and "Delete bucket".

4. 如果確定要刪除此儲存區、請選取*刪除儲存區*。

確認儲存區已空、然後刪除儲存區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。您必須先刪除所有物件、才能刪除儲存區。

 Unable to delete the bucket because it is not empty. You must delete all objects before you can delete this bucket.

相關資訊

["使用ILM管理物件"](#)

管理S3平台服務

如果您的S3租戶帳戶允許使用平台服務、您可以使用平台服務來運用外部服務、並設定CloudMirror複寫、通知、以及搜尋S3時段的整合功能。

- ["什麼是平台服務"](#)
- ["使用平台服務的考量"](#)
- ["設定平台服務端點"](#)
- ["設定CloudMirror複寫"](#)
- ["設定事件通知"](#)
- ["使用搜尋整合服務"](#)

什麼是平台服務

支援各種平台服務、協助您實作混合雲策略。StorageGRID

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*：StorageGRID 《Sirror CloudMirror複寫服務》可用來將特定物件從StorageGRID 一個物件庫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：每個儲存區事件通知用於將針對物件執行的特定動作通知傳送至指定的外部Amazon Simple Notification Service™ (SNS)。

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：搜尋整合服務用於將S3物件中繼資料傳送至指定的Elasticsearch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租戶管理程式或租戶管理API設定的外部端點通訊。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。

建立端點之後、您可以將XML組態新增至儲存區、為儲存區啟用平台服務。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：

1. 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。
2. 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。
3. 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	<ul style="list-style-type: none"> • 取得庫位複寫 • 放入資源桶複寫
通知	<ul style="list-style-type: none"> • 取得庫存箱通知 • 放置時段通知

平台服務	S3 REST API
搜尋整合	<ul style="list-style-type: none"> • 取得Bucket中繼資料通知組態 • 放置時段中繼資料通知組態 <p>這些作業是根據StorageGRID 需求量身打造的。</p>

請參閱實作S3用戶端應用程式的指示、以取得StorageGRID 有關如何實作這些API的詳細資訊。

相關資訊

["使用S3"](#)

["瞭解CloudMirror複寫服務"](#)

["瞭解庫存箱通知"](#)

["瞭解搜尋整合服務"](#)

["使用平台服務的考量"](#)

瞭解**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。

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。儲存區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複寫將物件複製到AWS 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為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區。

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。支援兩個網格之間的雙向CloudMirror。StorageGRID

無法保證目的地庫位中的活動獨特性和順序。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。

相關資訊

["設定CloudMirror複寫"](#)

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。

您可以將通知組態XML與來源儲存區建立關聯、以設定事件通知。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。

不保證通知的獨特性和順序。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

下列限制會遵循Amazon S3 API的事件通知：StorageGRID

- 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Suse傳送的事件通知StorageGRID 會使用標準Json格式、但不包含某些金鑰、並使用其他金鑰的特定值、如表所示：

金鑰名稱	價值StorageGRID
事件來源	<code>sgws:s3</code>
<code>awsRegion</code>	不含
<code>X-amz-id-2</code>	不含

金鑰名稱	價值StorageGRID
不需要	urn:sgws:s3:::bucket_name

相關資訊

["設定事件通知"](#)

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。建立文件索引之後、就無法在索引中編輯文件的欄位類型。

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。但是、系統不會針對儲存庫中已有的任何物件傳送通知。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_互通性對照表工具_來判斷支援的Elasticsearch版本。

相關資訊

["NetApp 互通性對照表工具"](#)

["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。

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	<p>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。</p> <p>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。</p> <p>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。</p>
訂購保證	<p>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。</p> <p>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。</p>
ILM導向物件刪除	<p>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 採用《ILM規則》而遭刪除時、不會傳送CloudMirror和事件通知要求。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。</p> <p>相反地、因為ILM而刪除物件時、會傳送搜尋整合要求。</p>

使用CloudMirror複寫服務的考量

考量	詳細資料
複寫狀態	不支援StorageGRID <code>x-amz-replication-status</code> 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 TB、與StorageGRID 支援的最大物件大小相同。
儲存區版本管理和版本ID	<p>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。</p> <p>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。</p> <p>附註：StorageGRID 來源程式庫的版本ID與目的地程式庫的版本ID無關。</p>
標記物件版本	<p>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ID無關、因此無法確保將標記更新複寫至特定版本ID。</p> <p>相較之下、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）。</p>
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、複寫作業將會失敗、並顯示AccessDenied錯誤。

相關資訊

["使用S3"](#)

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、位於已設定網路以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 某個物件庫複寫到S3庫位、您可以建立一個平台服務端點、其中包含StorageGRID 資訊和認證、供您存取AWS上的目的地庫位所需的資訊和認證資料。

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不支援簡單佇列服務 (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位於本機資料中心、或託管於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。您不需要在建立端點之前建立類型。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：

- 如果服務裝載於AWS上、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**託管的服務

對於AWS實體、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。

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。

您需要的產品

- 您必須使用支援的瀏覽器登入租戶管理程式。
- 平台服務必須由StorageGRID 管理員為您的租戶帳戶啟用。
- 您必須屬於具有「管理端點」權限的使用者群組。
- 平台服務端點所參照的資源必須已建立：
 - 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。

- 您必須擁有目的地資源的相關資訊：
 - 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
- 安全性憑證 (如果使用自訂CA憑證)

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*。

Create endpoint

1 Enter details — 2 Select authentication type Optional — 3 Verify server Optional

Enter endpoint details

Enter the endpoint's display name, URI, and URN.

Display name ?

URI ?

URN ?

Cancel Continue

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、當端點名稱列在端點頁面上時、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、則連接埠443用於HTTPS URI、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。



只要可能、您應該連線到HA負載平衡節點群組、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
```



如果將端點用於CloudMirror複寫服務、請勿在URI中加入貯體名稱。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) 。



建立端點之後、您無法變更端點的URN。

6. 選擇*繼續*。

7. 選取*驗證類型*的值、然後輸入所需的認證資料。

Create endpoint

1 Enter details — 2 Select authentication type (Optional) — 3 Verify server (Optional)

Authentication type ?

Select the method used to authenticate connections to the endpoint.

Anonymous

- Anonymous
- Access Key
- Basic HTTP

Previous Continue

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。	<ul style="list-style-type: none"> 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。	<ul style="list-style-type: none"> 使用者名稱 密碼

- 選擇*繼續*。
- 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。

Create endpoint

Enter details — Select authentication type (Optional) — **3 Verify server (Optional)**

Verify server

Use this method to validate the certificate for TLS connections to the endpoint resource. If you select "Use custom CA certificate," copy and paste the custom security certificate in the text box.

Use custom CA certificate
 Use operating system CA certificate
 Do not verify certificate

```

-----BEGIN CERTIFICATE-----
abodefghijkl123456780ABCDEFGHIJL
123456/7890ABCDEFabodefghijklABCD
-----END CERTIFICATE-----
  
```

Previous Test and create endpoint

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。

憑證驗證類型	說明
使用作業系統CA憑證	使用作業系統上安裝的預設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。

您需要的產品

- 您必須使用支援的瀏覽器登入租戶管理程式。
- 您必須屬於具有「管理端點」權限的使用者群組。

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。

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.

4 endpoints

Create endpoint

Delete endpoint

<input type="checkbox"/>	Display name ? ⬇	Last error ? ⬇	Type ? ⬇	URI ? ⬇	URN ? ⬇
<input type="checkbox"/>	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1
<input type="checkbox"/>	my-endpoint-2	✖ 2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es:::mydomain/sveloso/_doc
<input type="checkbox"/>	my-endpoint-3		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
<input type="checkbox"/>	my-endpoint-4		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket2

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。

Overview ⬆

Display name: **my-endpoint-1** [✎](#)

Type: **S3 Bucket**

URI: **http://10.96.104.167:10443**

URN: **urn:sgws:s3:::bucket1**

Connection **Configuration**

Verify connection [?](#)

Some errors might continue to appear after they are resolved. To see if an error is current or to force the removal of a resolved error, select **Test connection**.

Test connection

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。

您需要的產品

- 您必須使用支援的瀏覽器登入租戶管理程式。
- 您必須屬於具有「管理端點」權限的使用者群組。

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。

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.

4 endpoints Create endpoint

Delete endpoint

<input type="checkbox"/>	Display name [?] [⌵]	Last error [?] [⌵]	Type [?] [⌵]	URI [?] [⌵]	URN [?] [⌵]
<input type="checkbox"/>	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1
<input type="checkbox"/>	my-endpoint-2	✖ 2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es:::mydomain/sveloso/_doc
<input type="checkbox"/>	my-endpoint-3		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
<input type="checkbox"/>	my-endpoint-4		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket2

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-----  
abcdefghijklmnop123456780ABCDEFGHIJKL  
123456/7890ABCDEFabcdefghijklmnop1ABCD  
-----END CERTIFICATE-----
```

Test and save changes

4. 視需要變更端點的組態。



建立端點之後、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。
 - 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*。
- 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*。

相關資訊

["建立平台服務端點"](#)

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。

您需要的產品

- 您必須使用支援的瀏覽器登入租戶管理程式。
- 您必須屬於具有*管理端點*權限的使用者群組。

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。

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.

4 endpoints

Create endpoint

Delete endpoint

<input type="checkbox"/>	Display name	Last error	Type	URI	URN
<input type="checkbox"/>	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1
<input type="checkbox"/>	my-endpoint-2	2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es:::mydomain/sveloso/_doc
<input type="checkbox"/>	my-endpoint-3		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
<input type="checkbox"/>	my-endpoint-4		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket2

2. 選取您要刪除之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。

Delete endpoint

Are you sure you want to delete endpoint my-endpoint-10?

This might take a few minutes.

When you delete an endpoint, you can no longer use it to access external resources.

4. 選擇*刪除端點*。

疑難排解平台服務端點錯誤

如果在嘗試與平台服務端點通訊時發生錯誤StorageGRID、儀表板上會顯示一則訊息。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、則租戶管理程式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。

 One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

儀表板上出現的相同錯誤也會出現在「平台服務端點」頁面的頂端。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。

Overview ^

Display name:	my-endpoint-2
Type:	Search
URI:	http://10.96.104.30:9200
URN:	urn:sgws:es:::mydomain/sveloso/_doc

Connection

Configuration

Verify connection

Some errors might continue to appear after they are resolved. To see if an error is current or to force the removal of a resolved error, select **Test connection**.

Test connection

Last error details

2 hours ago

Endpoint failure: Endpont has an AWS failure: RequestError: send request failed; caused by: url.Error; caused by: net:OpError; caused by: os.SyscallError (logID: 143H5UDUUKMGDRWJ)

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

84

為「AccessDenied」或「InvalidAccessKeyId」。

如果您需要編輯端點來解決錯誤：選取*測試並儲存變更*會使StorageGRID 更新的端點驗證、並確認可以使用目前的認證來達到。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 Forbidbidbidbidbide」）、請檢查與端點認證相關的權限。

其他平台服務疑難排解

如需疑難排解平台服務的其他資訊、請參閱《關於管理StorageGRID 功能的說明》。

["管理StorageGRID"](#)

相關資訊

["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 三項功能完善的平台服務之一。您可以使用CloudMirror複寫、將物件自動複寫到外部S3儲存區。

您需要的產品

- 平台服務必須由StorageGRID 管理員為您的租戶帳戶啟用。
- 您必須已經建立一個儲存區、做為複寫來源。
- 您打算做為CloudMirror複寫目的地的端點必須已經存在、而且您必須擁有它的URN。
- 您必須屬於具有「管理所有庫位」或「根存取」權限的使用者群組、才能管理租戶帳戶中所有S3庫位的設定。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。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。

如需儲存區複寫及其設定方式的一般資訊、請參閱Amazon跨區域複寫 (CRR) 文件。如需StorageGRID 有關如何實作S3儲存區複寫組態API的資訊、請參閱實作S3用戶端應用程式的指示。

如果您在包含物件的儲存區上啟用CloudMirror複寫、則會複寫新增至儲存區的新物件、但儲存區中的現有物件則不會複寫。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 `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. 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*>*複寫*。

5. 選取「啟用複寫」核取方塊。
6. 將複寫組態XML貼到文字方塊中、然後選取*儲存變更*。

Bucket options Bucket access Platform services

Replication Disabled ^

Enable the CloudMirror replication service to copy objects from a source bucket to a destination bucket that is specified in an endpoint.

- Platform services must be enabled for your tenant account by a StorageGRID administrator.
- You must have already configured an endpoint for each destination bucket.
- You must specify the URN of each endpoint in the replication configuration XML for the source bucket.

Enable replication

Clear

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

Save changes



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

["瞭解CloudMirror複寫服務"](#)

["使用S3"](#)

["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。

您需要的產品

- 平台服務必須由StorageGRID 管理員為您的租戶帳戶啟用。
- 您必須已經建立一個儲存區、才能做為通知來源。
- 您要用作事件通知目的地的端點必須已經存在、而且您必須擁有它的URN。
- 您必須屬於具有「管理所有庫位」或「根存取」權限的使用者群組、才能管理租戶帳戶中所有S3庫位的設定。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。

如需事件通知及其設定方式的一般資訊、請參閱Amazon文件。如需StorageGRID 瞭解有關如何實作S3儲存區通知組態API的資訊、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. 選取*啟用事件通知*核取方塊。

6. 將通知組態XML貼到文字方塊中、然後選取*儲存變更*。

Bucket options
Bucket access
Platform services

Replication
Disabled
▼

Event notifications
Disabled
▲

Enable the event notification service for an S3 bucket if you want StorageGRID to send notifications about specified events to a destination Amazon Simple Notification Service (SNS).

- Platform services must be enabled for your tenant account by a StorageGRID administrator.
- You must have already configured an endpoint for the destination of event notifications.
- You must specify the URN of that endpoint in the notification configuration XML for the source bucket.

Enable event notifications

```

<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>
      
```



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": "11111111111111111111"
      },
      "requestParameters": {
        "sourceIPAddress": "193.51.100.20"
      },
      "responseElements": {
        "x-amz-request-id": "122047343"
      },
      "s3": {
        "s3SchemaVersion": "1.0",
        "configurationId": "Image-created",
        "bucket": {
          "name": "test1",
          "ownerIdentity": {
            "principalId": "11111111111111111111"
          },
          "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。

["瞭解庫存箱通知"](#)

["使用S3"](#)

["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、以取得下列自訂StorageGRID 的S3 REST API作業的詳細資料：

- [刪除時段中繼資料通知組態要求](#)
- [取得Bucket中繼資料通知組態要求](#)
- [放置時段中繼資料通知組態要求](#)

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"](#)

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。具有重疊前置碼的組態無效、在提交時會遭到拒絕。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 NotificationConfiguration	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 NotificationConfiguration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	<p>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。</p> <p>若要符合所有物件、請指定一個空白首碼。</p> <p>包含在Rule元素中。</p>	是的
目的地	<p>規則目的地的容器標記。</p> <p>包含在Rule元素中。</p>	是的
urn	<p>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：</p> <ul style="list-style-type: none"> • 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。 <p>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：</p> <ul style="list-style-type: none"> • arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype • urn:mysite:es:::mydomain/myindex/mytype <p>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。</p> <p>目標元素中包含urn.</p>	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-1:2222222:domain/es-
domain/graphics/videotype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

相關資訊

["使用S3"](#)

["由搜尋整合服務產生的JSON"](#)

["設定搜尋整合服務"](#)

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。

您需要的產品

- 平台服務必須由StorageGRID 管理員為您的租戶帳戶啟用。
- 您必須已建立S3儲存區、其內容必須為您要建立索引。
- 您要做為搜尋整合服務目的地的端點必須已經存在、而且您必須擁有它的URN。
- 您必須屬於具有「管理所有庫位」或「根存取」權限的使用者群組、才能管理租戶帳戶中所有S3庫位的設定。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儲存區啟用搜尋整合服務、則不會針對現有物件自動傳送中繼資料通知。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-
1:1111111111111111: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. 選取*啟用搜尋整合*核取方塊。
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*。

Bucket options
Bucket access
Platform services

Replication
Disabled
▼

Event notifications
Disabled
▼

Search integration
Disabled
▲

Enable the search integration service to send object metadata to a destination search index whenever an object is created, deleted, or its metadata or tags are updated.

- Platform services must be enabled for your tenant account by a StorageGRID administrator.
- You must have already configured an endpoint for the search integration service.
- You must specify the URN of that endpoint in the search integration configuration XML for the bucket you want to index.

Enable search integration

Clear

```

<MetadataNotificationConfiguration>
  <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:111111111111:domain/mydomain/myindex/mytype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
          
```

Save changes



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*儲存設備 (S3) >*儲存設備、然後取消選取*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"](#)

["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（作為鍵值對） 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。建立文件索引之後、就無法在索引中編輯文件的欄位類型。

版權資訊

Copyright © 2025 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。