



使用租用戶帳戶 StorageGRID software

NetApp
May 29, 2026

目錄

使用租用戶帳戶	1
使用租用戶帳戶	1
什麼是租戶帳戶？	1
如何建立租用戶帳戶	1
如何登入和登出	2
Sign in租戶管理器	2
退出租戶管理器	5
了解租戶管理器儀表板	6
租戶帳號資訊	7
儲存和配額使用情況	7
配額使用警報	8
容量限制使用情況	8
端點錯誤	9
租戶管理 API	9
了解租戶管理 API	9
租用戶管理 API 版本控制	12
防止跨站請求偽造 (CSRF)	13
使用電網聯合連接	14
克隆租戶群組和用戶	14
使用 API 克隆 S3 存取金鑰	18
管理跨網格複製	20
查看電網聯合連接	25
管理群組和用戶	26
使用身分聯合	26
管理租戶群組	31
管理本地用戶	39
管理 S3 存取密鑰	43
管理 S3 存取密鑰	43
建立您自己的 S3 存取金鑰	44
查看您的 S3 存取金鑰	45
刪除您自己的 S3 存取金鑰	45
建立另一個使用者的 S3 存取金鑰	46
查看其他使用者的 S3 存取金鑰	47
刪除其他使用者的 S3 存取金鑰	48
管理 S3 儲存桶	48
建立 S3 儲存桶	48
查看儲存桶詳細信息	51
將 ILM 策略標籤應用於儲存桶	53
管理儲存桶策略	54

管理儲存桶一致性	54
啟用或停用上次訪問時間更新	56
更改儲存桶的物件版本控制	57
使用 S3 對象鎖保留對象	58
更新 S3 物件鎖定預設保留	61
配置跨域資源共享 (CORS)	62
刪除儲存桶中的對象	64
刪除 S3 儲存桶	66
使用 S3 控制台	67
管理 S3 平台服務	68
S3平台服務	68
管理平台服務端點	74
配置 CloudMirror 複製	86
配置事件通知	88
配置搜尋整合服務	91

使用租用戶帳戶

使用租用戶帳戶

租用戶帳戶可讓您使用簡單儲存服務 (S3) REST API 或 Swift REST API 在StorageGRID系統中儲存和擷取物件。

什麼是租戶帳戶？

每個租用戶帳戶都有自己的聯合或本機群組、使用者、S3 儲存桶或 Swift 容器和物件。

租用戶帳戶可用於依不同實體隔離儲存的物件。例如，多個租用戶帳戶可用於下列任一用例：

- *企業用例：*如果在企業內部使用StorageGRID系統，則網格的物件儲存可能會由組織內的不同部門隔離。例如，可能有行銷部門、客戶支援部門、人力資源部門等的租戶帳戶。



如果您使用 S3 用戶端協議，您也可以使用 S3 儲存桶和儲存桶策略在企業各部門之間隔離物件。您不需要建立單獨的租用戶帳戶。請參閱實施說明["S3 儲存桶和儲存桶策略"](#)了解更多。

- *服務提供者用例：*如果服務提供者正在使用StorageGRID系統，則網格的物件儲存可能會由租用儲存的不同實體隔離。例如，可能有公司 A、公司 B、公司 C 等的租戶帳戶。

如何建立租用戶帳戶

租戶帳戶由["使用網格管理器的StorageGRID網格管理員"](#)。建立租用戶帳戶時，網格管理員指定以下內容：

- 基本資訊包括租用戶名稱、用戶端類型 (S3) 和可選儲存配額。
- 租用戶帳戶的權限，例如租用戶帳戶是否可以使用 S3 平台服務、設定自己的身分來源、使用 S3 Select 或使用網格聯合連線。
- 租用戶的初始根存取權限，取決於StorageGRID系統是否使用本機群組和使用者、身分聯合或單一登入 (SSO)。

此外，如果 S3 租用戶帳戶需要遵守法規要求，網格管理員可以為StorageGRID系統啟用 S3 物件鎖定設定。啟用 S3 物件鎖定後，所有 S3 租用戶帳戶都可以建立和管理相容的儲存桶。

配置 S3 租戶

經過["S3 租用戶帳戶已建立"](#)，您可以存取租用戶管理員來執行下列任務：

- 設定身份聯合（除非身份來源與網格共享）
- 管理群組和用戶
- 使用網格聯合進行帳戶克隆和跨網格複製
- 管理 S3 存取密鑰
- 建立和管理 S3 儲存桶
- 使用 S3 平台服務

- 使用 S3 Select
- 監控儲存使用情況



雖然您可以使用租用戶管理器建立和管理 S3 儲存桶，但您必須使用"[S3 用戶端](#)"或者"[S3 控制台](#)"擷取和管理物件。

如何登入和登出

Sign in租戶管理器

您可以透過在網址列中輸入租用戶的 URL 來存取租用戶管理員"[支援的網頁瀏覽器](#)"。

開始之前

- 您有登入憑證。
- 您有一個用於存取租用戶管理員的 URL，由您的網格管理員提供。URL 將類似於以下範例之一：

```
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 始終包含完全限定網域名稱 (FQDN)、管理節點的 IP 位址或管理節點 HA 群組的虛擬 IP 位址。它可能還包括連接埠號碼、20 位租戶帳戶 ID 或兩者。

- 如果 URL 不包含租用戶的 20 位帳戶 ID，則您擁有此帳戶 ID。
- 您正在使用"[支援的網頁瀏覽器](#)"。
- 您的網頁瀏覽器已啟用 Cookie。
- 您屬於一個使用者群組"[特定存取權限](#)"。

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訪問租用戶管理員的URL。
3. 如果出現安全性警報，請使用瀏覽器的安裝精靈安裝憑證。
4. Sign in租戶管理器。

出現的登入畫面取決於您輸入的 URL 以及是否已為StorageGRID設定單一登入 (SSO)。

不使用 SSO

如果StorageGRID未使用 SSO，則會出現下列其中一個畫面：

- 網格管理器登入頁面。選擇*租戶登入*連結。



NetApp StorageGRID®
Grid Manager

Username

Password

[Sign in](#)

[Tenant sign in](#) | [NetApp support](#) | [NetApp.com](#)

- 租戶管理器登入頁面。*帳戶*欄位可能已填寫完畢，如下所示。

NetApp StorageGRID®

Tenant Manager

Recent

-- Optional --

Account

64600207336181242061

Username

|

Password

Sign in

[NetApp support](#) | [NetApp.com](#)

- i. 如果未顯示租用戶的 20 位元帳戶 ID，請選擇租用戶帳戶的名稱（如果它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*Sign in*。

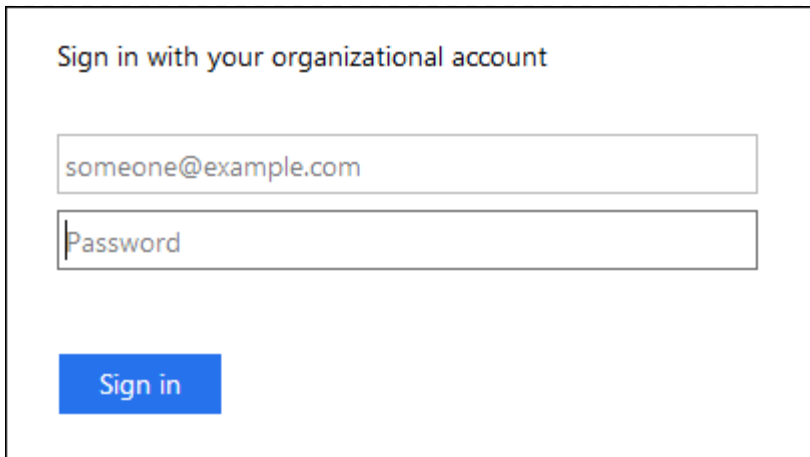
出現租戶管理器儀表板。

- iv. 如果您從其他人收到了初始密碼，請選擇 **username** > 變更密碼 來保護您的帳戶。

使用 SSO


如果StorageGRID使用 SSO，則會出現下列其中一個畫面：

- 您組織的 SSO 頁面。例如：



輸入您的標準 SSO 憑證，然後選擇 **Sign in**。

- 租戶管理器 SSO 登入頁面。



- 如果未顯示租用戶的 20 位元帳戶 ID，請選擇租用戶帳戶的名稱（如果它出現在最近帳戶清單中），或輸入帳戶 ID。
- 選擇*Sign in*。
- 使用您的標準 SSO 憑證在您組織的 SSO 登入頁面上Sign in。

出現租戶管理器儀表板。

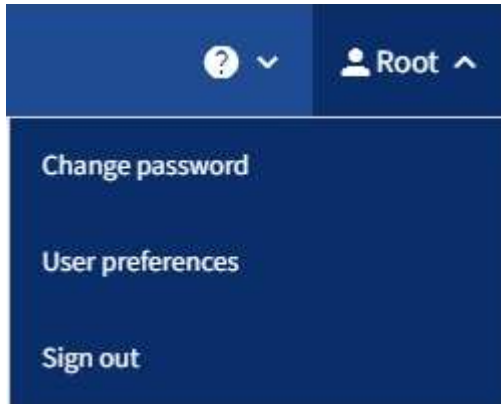
退出租戶管理器

當您完成租用戶管理器的工作後，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使您退出系統。

步驟

1. 找到使用者介面右上角的使用者名稱下拉式選單。



2. 選擇使用者名，然後選擇*退出*。

- 如果未使用 SSO：

您已退出管理節點。顯示租用戶管理員登入頁面。



如果您登入了多個管理節點，則必須從每個節點登出。

- 如果啟用了 SSO：

您已退出正在存取的所有管理節點。顯示StorageGRIDSIGN in頁面。您剛剛造訪的租用戶帳戶的名稱在「最近的帳戶」下拉式功能表中列為預設名稱，並顯示租用戶的「帳戶 ID」。



如果啟用了 SSO 並且您也登入了網格管理器，則您也必須登出網格管理器才能登出 SSO。

了解租戶管理器儀表板

租戶管理器儀表板概述了租戶帳戶的配置以及租戶儲存桶 (S3) 或容器 (Swift) 中的物件使用的空間量。如果租戶有配額，儀表板會顯示已使用的配額量以及剩餘的配額量。如果存在與租用戶帳戶相關的任何錯誤，則錯誤將顯示在儀表板上。



已用空間值是估計值。這些估計值受到攝取時間、網路連接和節點狀態的影響。

物件上傳後，儀表板如下例所示：

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

Top buckets by capacity limit usage [?](#)

Bucket name	Usage
Bucket-10	82%
Bucket-03	57%
Bucket-15	20%

Tenant details [?](#)

Name: Tenant02
ID: 3341 1240 0546 8283 2208

- Platform services enabled
- Can use own identity source
- S3 Select enabled

租戶帳號資訊

儀表板頂部顯示已配置的儲存桶或容器、群組和使用者的數量。如果已配置，它也會顯示平台服務端點的數量。選擇連結來查看詳細資訊。

取決於"租用戶管理權限"您擁有的和您配置的選項，儀表板的其餘部分顯示指南、儲存使用情況、物件資訊和租戶詳細資訊的各種組合。

儲存和配額使用情況

儲存使用情況面板包含以下資訊：

- 租戶的對象資料量。

該值表示上傳的物件資料總量，並不代表用於儲存這些物件及其元資料的副本的空間。

- 如果設定了配額，則表示物件資料可用的空間總量以及剩餘空間量和百分比。配額限制了可以攝取的物件資料量。



配額使用基於內部估計，在某些情況下可能會超出。例如，當租用戶開始上傳物件時，StorageGRID會檢查配額，如果租用戶超出配額，則會拒絕新的攝取。但是，StorageGRID在決定是否超出配額時不會考慮目前上傳的大小。如果對象被刪除，租用戶可能會暫時無法上傳新對象，直到重新計算配額使用量。配額使用情況計算可能需要 10 分鐘或更長。

- 表示最大桶子或容器的相對大小的長條圖。

您可以將遊標放在任何圖表段上，以查看該儲存桶或容器消耗的總空間。



- 與長條圖相對應，最大的儲存桶或容器的列表，包括物件資料的總量和每個儲存桶或容器的物件數量。

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

如果租戶有超過九個儲存桶或容器，則所有其他儲存桶或容器將合併為清單底部的單一條目。



若要變更租用戶管理員中顯示的儲存值的單位，請選擇租用戶管理員右上角的使用者下拉式選單，然後選擇*使用者首選項*。

配額使用警報

如果在網格管理員中啟用了配額使用警報，則當配額較低或超出時，這些警報將顯示在租用戶管理員中，如下所示：

- 如果已使用租戶配額的 90% 或更多，則會觸發「租戶配額使用率高」警報。

考慮要求您的電網管理員增加配額。

- 如果超出配額，則會收到通知，告知您無法上傳新物件。


容量限制使用情況

如果您為儲存桶設定了容量限制，租用戶管理器儀表板將顯示按容量限制使用情況排列的頂級儲存桶清單。

如果未設定 bucket 的限制，則其容量是無限的。但是，如果您的租用戶帳戶具有總儲存配額並且已達到該配額，則無論儲存桶的剩餘容量限制如何，您都將無法提取更多物件。

端點錯誤

如果您已使用網格管理器設定一個或多個端點以用於平台服務，則如果過去七天內發生任何端點錯誤，租用戶管理器儀表板將顯示警報。

 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.

查看有關["平台服務端點錯誤"](#)，選擇 **Endpoints** 以顯示 Endpoints 頁面。

租戶管理 API

了解租戶管理 API

您可以使用租用戶管理 REST API 而不是租用戶管理器使用者介面執行系統管理任務。例如，您可能希望使用 API 來自動化操作或更快地建立多個實體（例如使用者）。

租戶管理 API：

- 使用Swagger開源API平台。Swagger 提供了直覺的使用者介面，允許開發人員和非開發人員與 API 進行互動。Swagger 使用者介面為每個 API 操作提供了完整的詳細資訊和文件。
- 用途["版本控制以支援無中斷升級"](#)。

若要存取租戶管理 API 的 Swagger 文件：

1. Sign in租戶管理器。
2. 從租戶管理員的頂部，選擇說明圖示並選擇*API 文件*。

API 操作

租用戶管理 API 將可用的 API 作業組織到以下部分：

- **account**：目前租用戶帳戶的操作，包括取得儲存使用資訊。
- **auth**：執行使用者會話認證的操作。

租用戶管理 API 支援 Bearer Token 身分驗證方案。對於租用戶登入，您需要在身份驗證請求的 JSON 主體中提供使用者名稱、密碼和 accountId（即 POST /api/v3/authorize）。如果使用者驗證成功，則會傳回安全令牌。必須在後續 API 請求的標頭中提供此令牌（「授權：承載令牌」）。

有關提高身份驗證安全性的信息，請參閱["防止跨站請求偽造"](#)。



如果為StorageGRID系統啟用了單一登入 (SSO)，則必須執行不同的步驟進行驗證。查看["網格管理 API 使用說明"](#)。

- **config**：與產品發布和租戶管理API版本相關的操作。您可以列出產品發布版本以及該版本支援的 API 的主要版本。
- **容器**：對 S3 儲存桶或 Swift 容器的操作。
- **deactivated-features**：查看可能已停用的功能的操作。
- **端點**：管理端點的操作。端點允許 S3 儲存桶使用外部服務進行StorageGRID CloudMirror 複製、通知或搜尋整合。
- **grid-federation-connections**：網格聯合連接和跨網格複製的操作。
- **groups**：管理本機租用戶群組和從外部身分識別來源擷取共同租用戶群組的操作。
- **identity-source**：設定外部身分來源並手動同步聯合群組和使用者資訊的操作。
- **ilm**：資訊生命週期管理 (ILM) 設定的操作。
- **regions**：確定已為StorageGRID系統配置哪些區域的操作。
- **s3**：管理租用戶用戶的 S3 存取金鑰的操作。
- **s3-object-lock**：對全域 S3 物件鎖定設定的操作，用於支援法規遵循。
- **使用者**：檢視和管理租戶使用者的操作。

操作細節

展開每個 API 操作時，您可以看到其 HTTP 操作、端點 URL、任何必需或可選參數的清單、請求正文的範例（需要時）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	<div style="display: flex; justify-content: space-between;"> Example Value Model </div> <pre> { "responseTime": "2018-02-01T16:22:31.066Z", "status": "success", "apiVersion": "2.1" } </pre>

發出 API 請求



您使用 API 文件網頁執行的任何 API 操作都是即時操作。請注意不要錯誤地建立、更新或刪除配置資料或其他資料。

步驟

1. 選擇 HTTP 操作以查看請求詳細資訊。
2. 確定請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 請求來取得所需的資訊。
3. 確定是否需要修改範例請求正文。如果是，您可以選擇*模型*來了解每個領域的要求。
4. 選擇*試用*。

5. 提供任何所需的參數，或根據需要修改請求正文。
6. 選擇*執行*。
7. 查看回應代碼以確定請求是否成功。

租用戶管理 API 版本控制

租用戶管理 API 使用版本控制來支援無中斷升級。

例如，此請求 URL 指定 API 的版本 4。

```
https://hostname_or_ip_address/api/v4/authorize
```

當做出與舊版不相容的變更時，API 的主要版本就會被提升。當進行與舊版相容的變更時，API 的次要版本就會增加。相容的變化包括添加新的端點或新的屬性。

以下範例說明如何根據所做變更的類型來升級 API 版本。

API 變更類型	舊版	新版本
與舊版本相容	2.1	2.2
與舊版本不相容	2.1	3.0

首次安裝StorageGRID軟體時，僅啟用最新版本的 API。但是，當您升級到StorageGRID的新功能版本時，您仍然可以存取至少一個StorageGRID功能版本的舊 API 版本。



您可以配置支援的版本。請參閱 Swagger API 文件的 **config** 部分以了解"電網管理API"了解更多。更新所有 API 用戶端以使用新版本後，您應該停用對舊版本的支援。

過時的請求透過以下方式標記為已棄用：

- 回應頭為"Deprecated: true"
- JSON 回應主體包含「deprecated」：true
- 已棄用的警告已新增至 nms.log。例如：

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

確定目前版本支援哪些 API 版本

使用 `GET /versions` API 請求傳回支援的 API 主要版本清單。此請求位於 Swagger API 文件的 **config** 部分。

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

為請求指定 API 版本

您可以使用路徑參數指定 API 版本(/api/v4) 或標題(Api-Version: 4) 。如果您提供這兩個值，則標頭值將覆寫路徑值。

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

防止跨站請求偽造 (CSRF)

您可以使用 CSRF 令牌來增強使用 cookie 的身份驗證，從而幫助防止針對StorageGRID 的跨站點請求偽造 (CSRF) 攻擊。網格管理器和租用戶管理器會自動啟用此安全功能；其他 API 用戶端可以在登入時選擇是否啟用它。

可以觸發對不同網站的請求（例如使用 HTTP 表單 POST）的攻擊者可以使用登入使用者的 cookie 發出某些請求。

StorageGRID透過使用 CSRF 令牌來幫助防禦 CSRF 攻擊。啟用後，特定 cookie 的內容必須與特定標頭或特定 POST 正文參數的內容相符。

若要啟用該功能，請設定 csrfToken 參數 true 在身份驗證期間。預設值是 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"
```

當為真時，GridCsrfToken cookie 設定為用於登入網格管理器的隨機值，並且 AccountCsrfToken 為登入租

戶管理器，cookie 設定了一個隨機值。

如果存在 cookie，則所有可以修改系統狀態的請求（POST、PUT、PATCH、DELETE）都必須包含下列內容之一：

- 這 `X-Csrf-Token` 標頭，標頭的值設定為 CSRF 令牌 cookie 的值。
- 對於接受表單編碼主體的端點：`csrfToken` 表單編碼的請求主體參數。

若要設定 CSRF 保護，請使用"[電網管理API](#)"或者"[租戶管理 API](#)"。



設定了 CSRF 令牌 cookie 的請求也將對任何需要 JSON 請求主體的請求強制執行「Content-Type: application/json」標頭，作為 CSRF 攻擊的額外保護。

使用電網聯合連接

克隆租戶群組和用戶

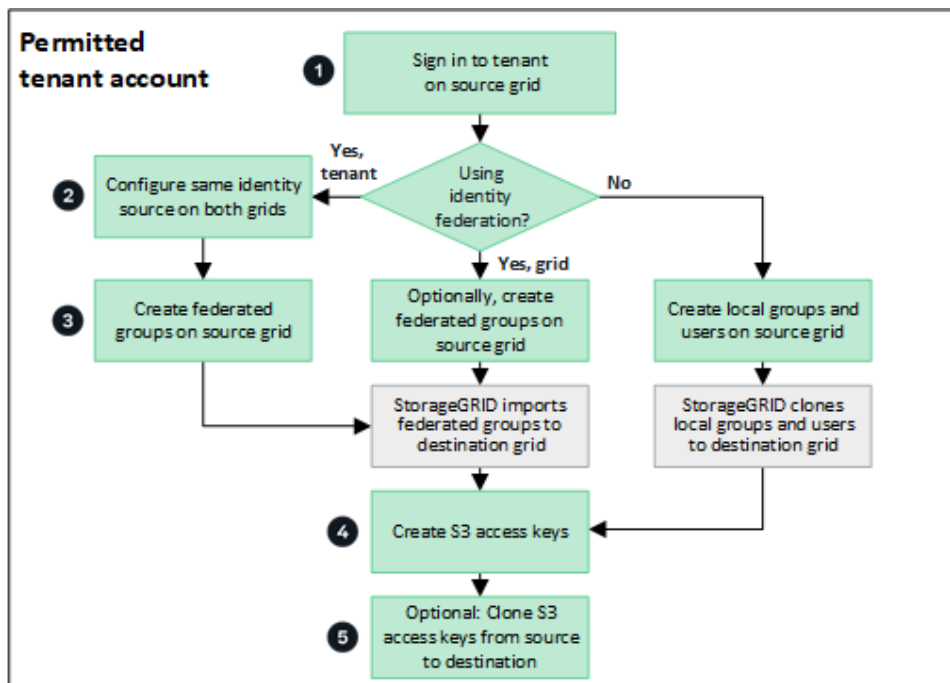
如果建立或編輯租用戶以使用網格聯合連接，則該租用戶將從一個StorageGRID系統（來源租用戶）複製到另一個StorageGRID系統（副本租用戶）。複製租用戶後，新增至來源租用戶的任何群組和使用者都會複製到副本租用戶。

最初建立租戶的StorageGRID系統是租戶的_來源網格_。複製租戶的StorageGRID系統是租戶的_目標網格_。兩個租用戶帳戶具有相同的帳戶 ID、名稱、描述、儲存配額和分配的權限，但目標租用戶最初沒有 root 使用者密碼。有關詳細信息，請參閱"[什麼是帳戶克隆](#)"和"[管理獲準租戶](#)"。

需要克隆租戶帳戶資訊"[跨網格複製](#)"存儲桶對象。兩個網格上具有相同的租戶群組和使用者可確保您可以存取任一網格上的相應儲存桶和物件。

帳戶克隆的租用戶工作流程

如果您的租用戶帳戶具有*使用網格聯合連線*權限，請查看工作流程圖以了解複製群組、使用者和 S3 存取金鑰將執行的步驟。



這些是工作流程中的主要步驟：

1 Sign in租戶

Sign in來源網格（最初建立租戶的網格）上的租戶帳戶。

2 （可選）配置身份聯合

如果您的租用戶帳戶具有使用聯合群組和使用者的「使用自己的身分來源」權限，請為來源租用戶帳戶和目標租用戶帳戶配置相同的身分來源（具有相同的設定）。除非兩個網格使用相同的身分來源，否則無法複製聯合群組和使用者。有關說明，請參閱["使用身分聯合"](#)。

3 建立群組和用戶

建立群組和使用者時，請始終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標網格。

- 如果為整個StorageGRID系統或您的租用戶帳戶配置了身分聯合，["建立新的租戶群組"](#)透過從身分來源匯入聯合群組。
- 如果您不使用身份聯合，["建立新的本機群組"](#)進而["建立本地用戶"](#)。

4 建立 S3 存取密鑰

您可以["建立您自己的存取金鑰"](#)或["建立另一個使用者的存取金鑰"](#)在來源網格或目標網格上存取該網格上的儲存桶。

5 （可選）克隆 S3 存取密鑰

如果您需要在兩個網格上使用相同的存取金鑰存取儲存桶，請在來源網格上建立存取金鑰，然後使用租用戶管理員 API 手動將它們複製到目標網格。有關說明，請參閱["使用 API 克隆 S3 存取金鑰"](#)。

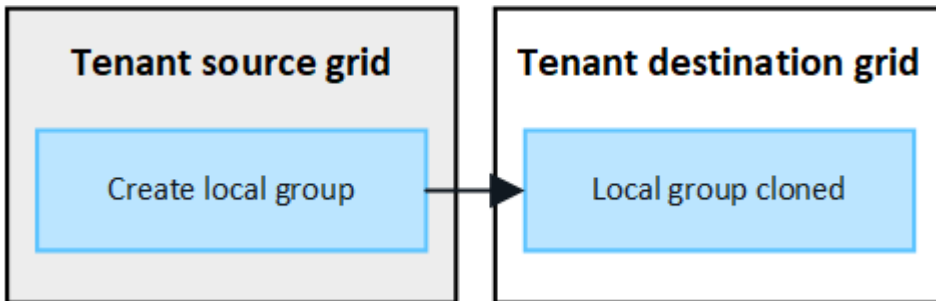
如何複製群組、使用者和 S3 存取金鑰？

請參閱本節以了解如何在租戶來源網格和租戶目標網格之間複製群組、使用者和 S3 存取金鑰。

克隆在來源網格上建立的本機群組

建立租用戶帳戶並將其複製到目標網格後，StorageGRID會自動將您新增至租用戶來源網格的任何本機群組複製到租用戶的目標網格。

原始群組及其複製都具有相同的存取模式、群組權限和 S3 群組原則。有關說明，請參閱["為 S3 租用戶建立群組"](#)。

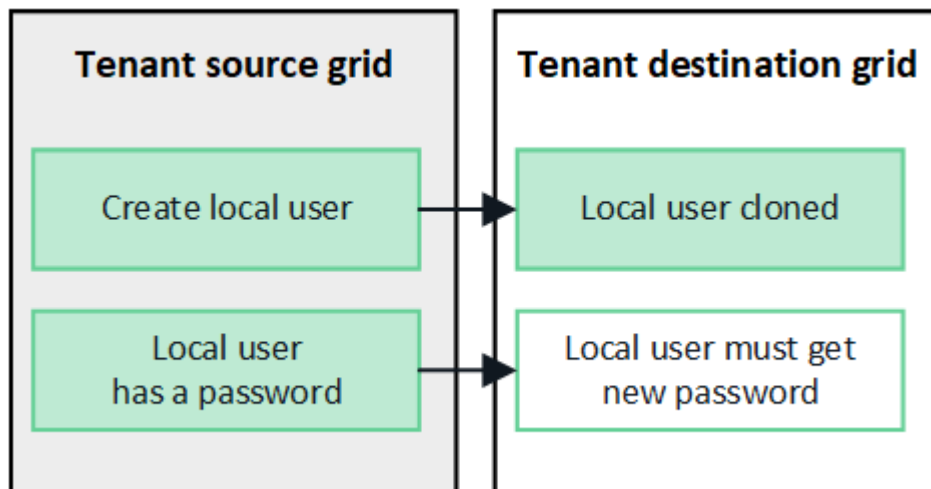


將群組複製到目標網格時，不會包括在來源網格上建立本機群組時選擇的任何使用者。因此，在創建群組時不要選擇使用者。相反，在建立使用者時選擇群組。

克隆在來源網格上建立的本機用戶

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標網格。原始使用者及其複製使用者俱有相同的全名、使用者名稱和*拒絕存取*設定。兩個用戶也屬於同一組。有關說明，請參閱["管理本地用戶"](#)。

出於安全原因，本機使用者密碼不會被複製到目標網格。如果本機使用者需要存取目標網格上的租用戶管理器，則租用戶帳戶的根用戶必須在目標網格上為該用戶新增密碼。有關說明，請參閱["管理本地用戶"](#)。

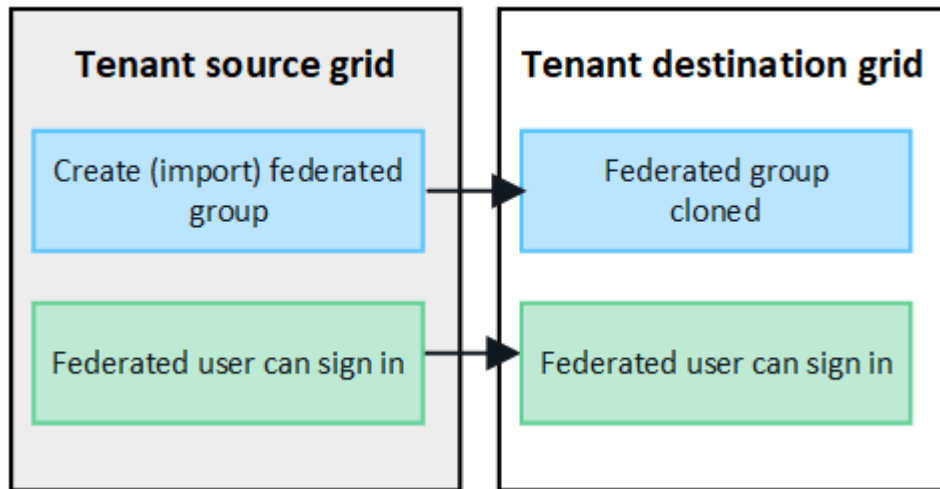


克隆在來源網格上建立的聯合組

假設使用帳戶克隆的要求"單一登入"和"身分聯合"已滿足，您為來源網格上的租戶建立（匯入）的聯合群組將自動複製到目標網格上的租戶。

兩個群組具有相同的存取模式、群組權限和 S3 群組原則。

為來源租戶建立聯合群組並將其複製到目標租戶後，聯合使用者可以在任一網格上登入該租戶。

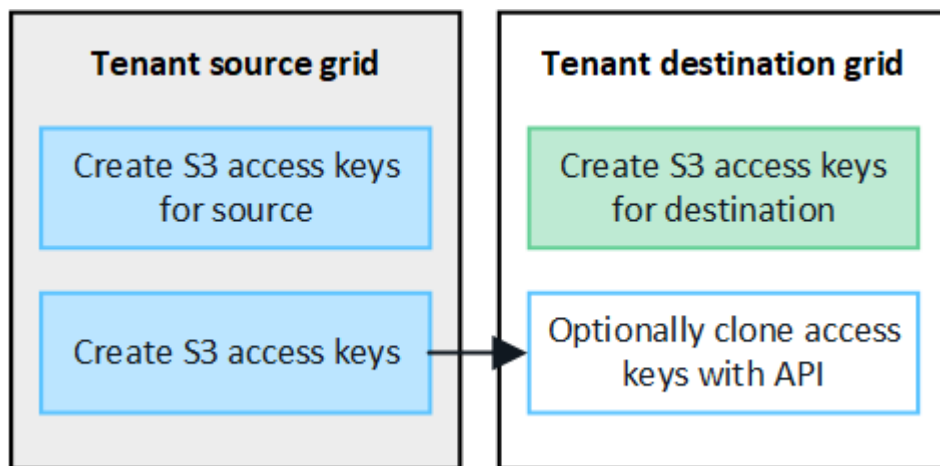


S3 存取密鑰可以手動克隆

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可以提高安全性。

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操作：

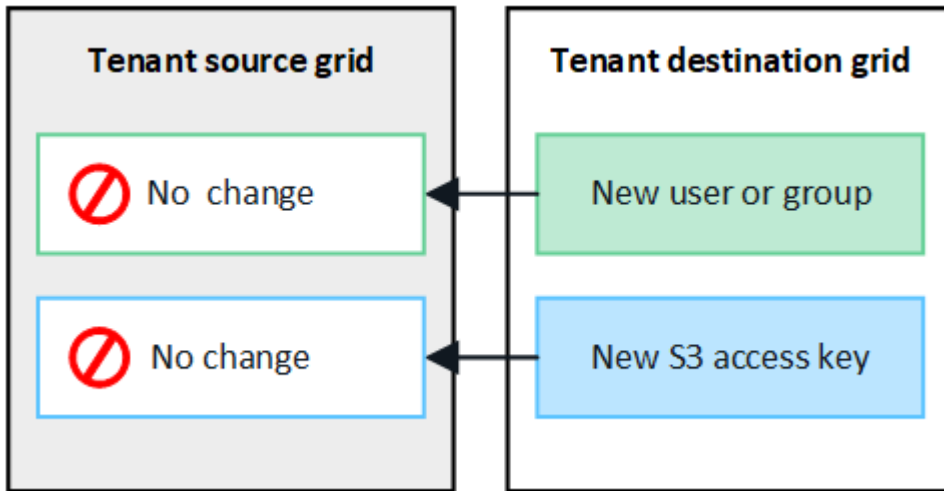
- 如果你不需要對每個網格使用相同的鍵，你可以"建立您自己的存取金鑰"或者"建立另一個使用者的存取金鑰"在每個網格上。
- 如果需要在兩個網格上使用相同的金鑰，則可以在來源網格上建立金鑰，然後使用租用戶管理員 API 手動"克隆密鑰"到目的地格。



當您為聯合用戶複製 S3 存取金鑰時，使用者和 S3 存取金鑰都會複製到目標租用戶。

新增到目標網格的群組和使用者未被克隆

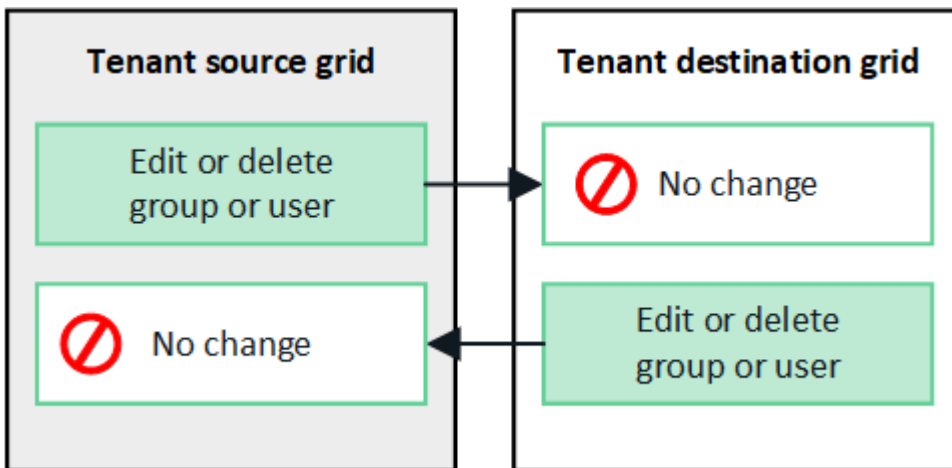
克隆僅從租戶的來源網格發生到租戶的目標網格。如果您在租用戶的目標網格上建立或匯入群組和用戶，StorageGRID將不會將這些項目複製回租戶的來源網格。



已編輯或刪除的群組、使用者和存取金鑰不會被克隆

僅當您建立新的群組和使用者時才會發生複製。

如果您在任一網格上編輯或刪除群組、使用者或存取金鑰，您的變更將不會被複製到另一個網格。



使用 API 克隆 S3 存取金鑰

如果您的租用戶帳戶具有 使用網格聯合連線 權限，則可以使用租用戶管理 API 將 S3 存取金鑰從來源網格上的租用戶手動複製到目標網格上的租用戶。

開始之前

- 租用戶帳戶具有*使用網格聯合連線*權限。
- 電網聯合連線的*連線狀態*為*已連線*。
- 您已使用"支援的網頁瀏覽器"。
- 您屬於具有"管理您自己的 S3 憑證或 Root 存取權限"。

- 如果您正在為本機使用者複製存取金鑰，則該使用者已存在於兩個網格中。



當您為聯合用戶複製 S3 存取金鑰時，該使用者和 S3 存取金鑰都會新增至目標租用戶。

克隆您自己的存取密鑰

如果您需要存取兩個網格上的相同儲存桶，您可以複製自己的存取金鑰。

步驟

1. 使用來源網格上的租用戶管理器，"[建立您自己的存取金鑰](#)"並下載`.csv`文件。
2. 從租戶管理員的頂部，選擇說明圖示並選擇*API 文件*。
3. 在 **s3** 部分中，選擇以下端點：

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



4. 選擇*試用*。
5. 在 **body** 文字方塊中，將 **accessKey** 和 **secretAccessKey** 的範例條目替換為您下載的`.csv`檔案中的值。

確保保留每個字串周圍的雙引號。



6. 如果金鑰即將過期，請將 **expires** 的範例條目替換為 ISO 8601 資料時間格式的過期日期和時間字串（例如，2024-02-28T22:46:33-08:00）。如果金鑰不會過期，請輸入 **null** 作為 **expires** 條目的值（或刪除 **Expires** 行和前面的逗號）。
7. 選擇*執行*。
8. 確認伺服器回應代碼為*204*，表示金鑰已成功複製到目標網格。

克隆其他使用者的存取密鑰

如果另一個使用者需要存取兩個網格上的相同儲存桶，您可以複製該使用者的存取金鑰。

步驟

1. 使用來源網格上的租用戶管理器，"[建立其他使用者的 S3 存取金鑰](#)"並下載`.csv`文件。
2. 從租戶管理員的頂部，選擇說明圖示並選擇*API 文件*。
3. 取得用戶ID。您將需要此值來克隆其他使用者的存取金鑰。

- a. 從 **users** 部分，選擇以下端點：

```
GET /org/users
```

- b. 選擇*試用*。
 - c. 指定查找使用者時要使用的任何參數。
 - d. 選擇*執行*。
 - e. 找到您想要複製其金鑰的用戶，並複製 **id** 欄位中的數字。
4. 在 **s3** 部分中，選擇以下端點：

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



5. 選擇*試用*。
6. 在 **userId** 文字方塊中，貼上您複製的使用者 ID。
7. 在 **body** 文字方塊中，將 **example access key** 和 **secret access key** 的範例條目替換為該使用者的 **.csv** 檔案中的值。

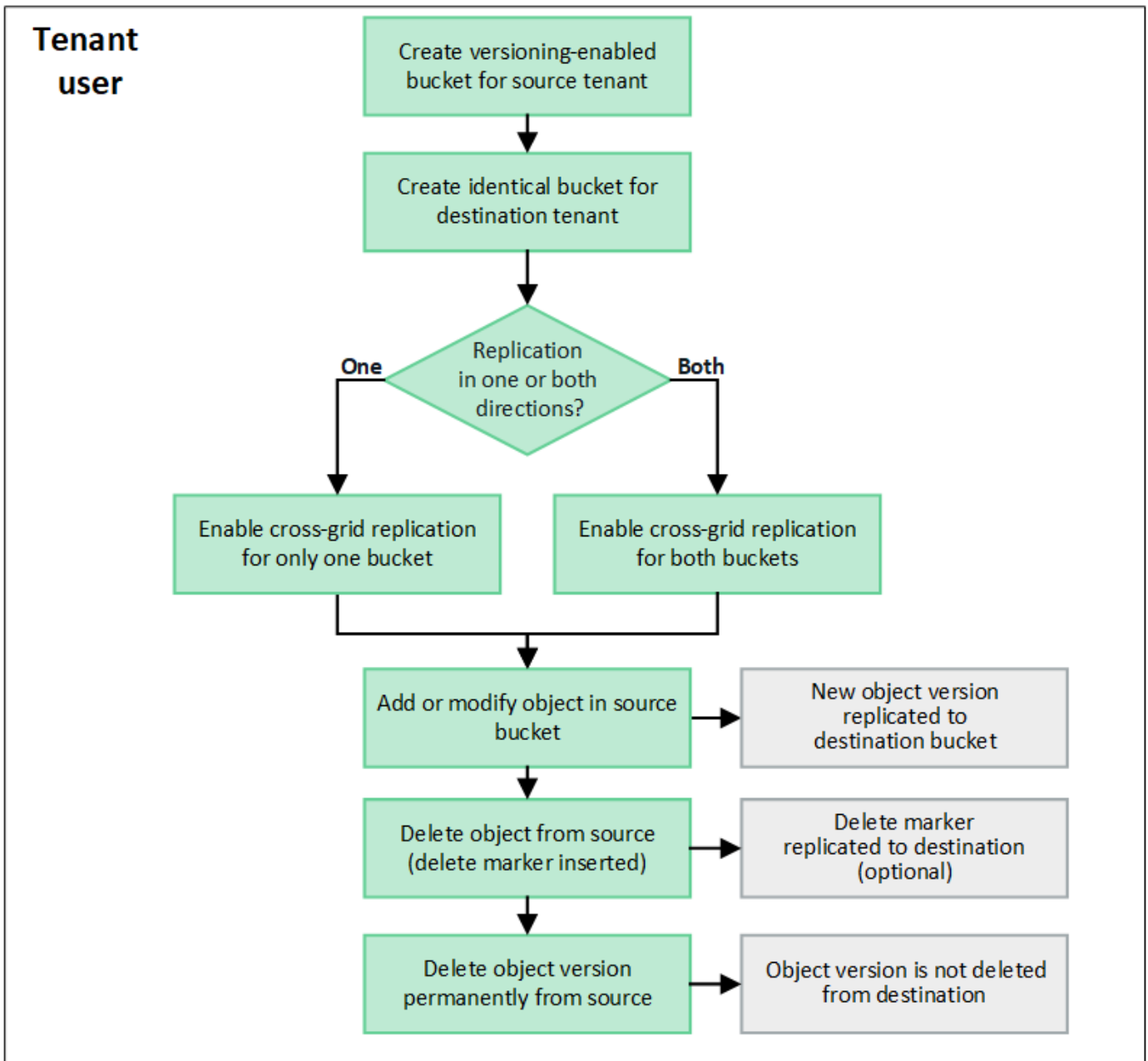
確保保留字串周圍的雙引號。
8. 如果金鑰即將過期，請將 **expires** 的範例條目替換為 ISO 8601 資料時間格式的過期日期和時間字串（例如，2023-02-28T22:46:33-08:00）。如果金鑰不會過期，請輸入 **null** 作為 **expires** 條目的值（或刪除 **Expires** 行和前面的逗號）。
9. 選擇*執行*。
10. 確認伺服器回應代碼為*204*，表示金鑰已成功複製到目標網格。

管理跨網格複製

如果您的租用戶帳戶在建立時被指派了 **使用網格聯合連線** 權限，則您可以使用跨網格複製在租用戶來源網格上的儲存桶和租用戶目標網格上的儲存桶之間自動複製物件。跨網格複製可以單向或雙向進行。

跨網格複製的工作流程

工作流程圖總結了配置兩個網格上的儲存桶之間的跨網格複製所要執行的步驟。以下將更詳細地描述這些步驟。



配置跨網格複製

在使用跨網格複製之前，您必須登入每個網格上對應的租用戶帳戶並建立相同的儲存桶。然後，您可以在一個或兩個儲存桶上啟用跨網格複製。

開始之前

- 您已查看了跨網格複製的要求。看"[什麼是跨網格複製](#)"。
- 您正在使用"[支援的網頁瀏覽器](#)"。
- 租用戶帳戶具有*使用網格聯合連線*權限，且兩個網格上都存在相同的租用戶帳戶。看"[管理允許的電網聯合連接租戶](#)"。
- 您將以該身分登入的租戶使用者已存在於兩個網格中，並且屬於具有"[Root存取權限](#)"。
- 如果您將以本機使用者身分登入租用戶的目標網格，則租用戶帳戶的根使用者已為您該網格上的使用者帳戶設定了密碼。

建立兩個相同的儲存桶

第一步，登入每個網格上對應的租戶帳戶並建立相同的儲存桶。

步驟

1. 從網格聯合連接中的任一網格開始，建立一個新的儲存桶：
 - a. 使用兩個網格上都存在的租戶使用者的憑證Sign in租戶帳戶。



如果您無法以本機使用者身分登入租用戶的目標網格，請確認租用戶帳戶的根用戶已為您的使用者帳戶設定密碼。

- b. 按照說明"[建立一個 S3 儲存桶](#)"。
 - c. 在*管理物件設定*標籤上，選擇*啟用物件版本控制*。
 - d. 如果您的StorageGRID系統啟用了 S3 物件鎖，請不要為儲存桶啟用 S3 物件鎖。
 - e. 選擇*建立儲存桶*。
 - f. 選擇*完成*。
2. 重複這些步驟，為網格聯合連接中的另一個網格上的相同租用戶帳戶建立相同的儲存桶。



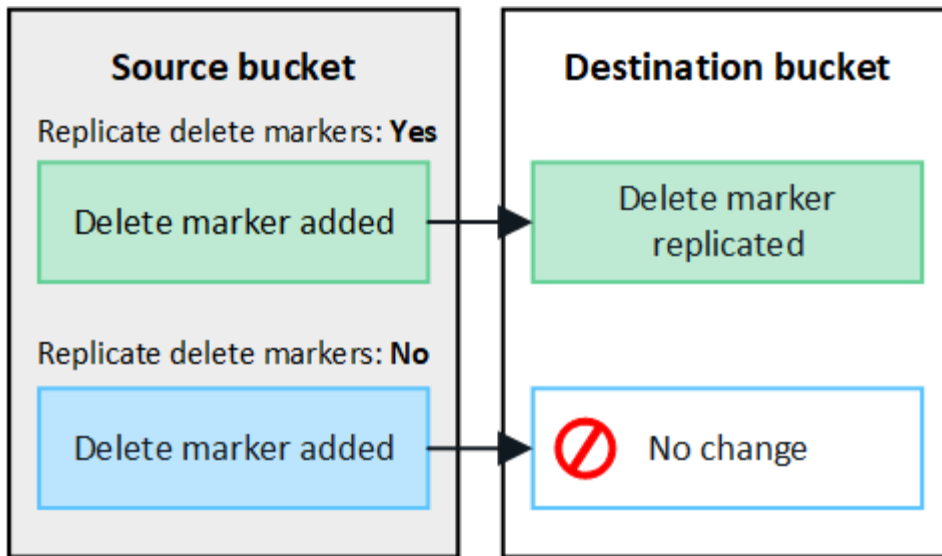
根據需要，每個儲存桶可以使用不同的區域。

啟用跨網格複製

在將任何物件新增至任一儲存桶之前，您必須執行這些步驟。

步驟

1. 從要複製物件的網格開始，啟用"[單向跨網格複製](#)"：
 - a. Sign in儲存桶的租用戶帳戶。
 - b. 從儀表板中選擇 [查看儲存桶](#)，或選擇 [儲存 \(S3\)](#) > [儲存桶](#)。
 - c. 從表格中選擇儲存桶名稱以存取儲存桶詳細資訊頁面。
 - d. 選擇*跨網格複製*標籤。
 - e. 選擇*啟用*，並查看要求清單。
 - f. 如果所有要求都已滿足，請選擇要使用的電網聯合連接。
 - g. 或者，變更 [複製刪除標記](#) 的設置，以確定當 S3 用戶端向來源網格發出不包含版本 ID 的刪除請求時目標網格上會發生什麼：
 - 是（預設）：將刪除標記新增至來源儲存桶並複製到目標儲存桶。
 - 否：刪除標記已新增至來源儲存桶，但未複製到目標儲存桶。



如果刪除請求包含版本 ID，則該物件版本將從來源儲存桶中永久刪除。StorageGRID 不會複製包含版本 ID 的刪除要求，因此不會從目標中刪除相同的物件版本。

看"[什麼是跨網格複製](#)"了解詳情。

- a. 或者，變更「跨網格複製」審計類別的設定來管理審計訊息的數量：
 - 錯誤（預設）：審計輸出中僅包含失敗的跨網格複製請求。
 - 正常：包括所有跨網格複製請求，這顯著增加了審計輸出量。
- b. 檢查您的選擇。除非兩個儲存桶都為空，否則您無法變更這些設定。
- c. 選擇*啟用並測試*。

片刻之後，會出現成功訊息。新增至此儲存桶的物件現在將自動複製到另一個網格。*跨網格複製*在儲存桶詳細資料頁面上顯示為已啟用的功能。

2. 或者，轉到另一個網格上的相應儲存桶，然後"[啟用雙向跨網格複製](#)"。

測試網格之間的複製

如果為儲存桶啟用了跨網格複製，您可能需要驗證連線和跨網格複製是否正常運作，以及來源儲存桶和目標儲存桶是否仍符合所有要求（例如，版本控制仍然啟用）。

開始之前

- 您正在使用"[支援的網頁瀏覽器](#)"。
- 您屬於具有"[Root存取權限](#)"。

步驟

1. Sign in 儲存桶的租用戶帳戶。
2. 從儀表板中選擇 [查看儲存桶](#)，或選擇 [儲存 \(S3\)](#) > [儲存桶](#)。
3. 從表格中選擇儲存桶名稱以存取儲存桶詳細資訊頁面。
4. 選擇*跨網格複製*標籤。

5. 選擇*測試連線*。

如果連接正常，則會出現成功橫幅。否則，會出現一條錯誤訊息，您和網絡管理員可以使用它來解決問題。有關詳細信息，請參閱["解決網絡聯合錯誤"](#)。

6. 如果跨網絡複製配置為雙向進行，請轉到另一個網絡上的相應儲存桶並選擇*測試連接*以驗證跨網絡複製是否在另一個方向上有效。

禁用跨網絡複製

如果您不再想將物件複製到另一個網絡，您可以永久停止跨網絡複製。

在停用跨網絡複製之前，請注意以下事項：

- 停用跨網絡複製不會刪除任何已在網絡之間複製的物件。例如，`my-bucket` 網絡 1 上已複製到 `my-bucket` 如果您停用該儲存桶的跨網絡複製，則網絡 2 上的資料不會被刪除。如果要刪除這些對象，則必須手動將其刪除。
- 如果每個儲存桶都啟用了跨網絡複製（即，如果複製在兩個方向上發生），則可以停用一個或兩個儲存桶的跨網絡複製。例如，您可能想要停用從 `my-bucket` 在網絡 1 上 `my-bucket` 在網絡 2 上，同時繼續從 `my-bucket` 在網絡 2 上 `my-bucket` 在網絡 1 上。
- 您必須先停用跨網絡複製，然後才能刪除租用戶使用網絡聯合連線的權限。看["管理獲準租戶"](#)。
- 如果您停用包含對象的儲存桶的跨網絡複製，除非您從來源儲存桶和目標儲存桶中刪除所有對象，否則將無法重新啟用跨網絡複製。



除非兩個儲存桶都為空，否則您無法重新啟用複製。

開始之前

- 您正在使用["支援的網頁瀏覽器"](#)。
- 您屬於具有["Root存取權限"](#)。

步驟

1. 從不再需要複製其物件的網絡開始，停止儲存桶的跨網絡複製：

- a. Sign in 儲存桶的租用戶帳戶。
- b. 從儀表中選擇 查看儲存桶，或選擇 儲存 (S3) > 儲存桶。
- c. 從表格中選擇儲存桶名稱以存取儲存桶詳細資訊頁面。
- d. 選擇*跨網絡複製*標籤。
- e. 選擇*禁用複製*。
- f. 如果您確定要停用此儲存桶的跨網絡複製，請在文字方塊中輸入*是*，然後選擇*停用*。

片刻之後，會出現成功訊息。新增至此儲存桶的新物件無法再自動複製到其他網絡。*跨網絡複製*不再 在 Buckets 頁面上顯示為已啟用的功能。

2. 如果跨網絡複製配置為雙向進行，請轉到另一個網絡上的相應儲存桶並停止另一個方向的跨網絡複製。

查看電網聯合連接

如果您的租用戶帳戶具有*使用網格聯合連線*權限，您可以查看允許的連線。

開始之前

- 租用戶帳戶具有*使用網格聯合連線*權限。
- 您已使用"[支援的網頁瀏覽器](#)"。
- 您屬於具有"[Root存取權限](#)"。

步驟

1. 選擇*儲存 (S3)* > 電網聯合連接。

出現電網聯合連線頁面，其中包含一個匯總以下資訊的表格：

柱子	描述
連接名稱	此租戶有權使用的電網聯合連線。
具有跨網格複製的儲存桶	對於每個網格聯合連接，啟用了跨網格複製的租戶儲存桶。新增到這些儲存桶的物件將複製到連接中的另一個網格。
上次錯誤	對於每個網格聯合連接，當資料複製到另一個網格時，最近發生的錯誤（如果有）。看 清除最後一個錯誤 。

2. （可選）選擇一個儲存桶名稱"[查看儲存桶詳細信息](#)"。

清除最後一個錯誤

由於以下原因之一，錯誤可能會出現在「上次錯誤」欄位中：

- 未找到來源物件版本。
- 未找到來源儲存桶。
- 目標儲存桶已被刪除。
- 目標儲存桶已由其他帳戶重新建立。
- 目標儲存桶已暫停版本控制。
- 目標儲存桶由相同帳戶重新創建，但現在尚未版本控制。



此列僅顯示最後發生的跨網格複製錯誤；之前可能發生的錯誤將不會顯示。

步驟

1. 如果「最後錯誤」欄位中出現訊息，請查看訊息文字。

例如，此錯誤表示跨網格複製的目標儲存桶處於無效狀態，可能是因為版本控制已暫停或啟用了 S3 物件鎖定。

Grid federation connections

Clear error Search... Displaying one result

Connection name	Buckets with cross-grid replication	Last error
<input type="radio"/> Grid 1-Grid 2	my-cgr-bucket	<p>2022-12-07 16:02:20 MST</p> <p>Cross-grid replication has encountered an error. Failed to send cross-grid replication request from source bucket 'my-cgr-bucket' to destination bucket 'my-cgr-bucket'. Error code: DestinationRequestError. Detail: InvalidBucketState. Confirm that the source and destination buckets have object versioning enabled and S3 Object Lock disabled. (logID 4791585492825418592)</p>

- 執行任何建議的操作。例如，如果在目標儲存桶上暫停跨網格複製的版本控制，則重新啟用該儲存桶的版本控制。
- 從表格中選擇連接。
- 選擇*清除錯誤*。
- 選擇“是”清除該訊息並更新系統狀態。
- 等待 5-6 分鐘，然後將新物件放入儲存桶中。確認錯誤訊息不再出現。



為確保清除錯誤訊息，請在訊息中的時間戳記之後至少等待 5 分鐘，然後再提取新物件。

- 若要確定是否有任何物件因儲存桶錯誤而複製失敗，請參閱["識別並重試失敗的複製操作"](#)。

管理群組和用戶

使用身分聯合

使用身分聯合可以更快地設定租用戶群組和用戶，並允許租用戶用戶使用熟悉的憑證登入租用戶帳戶。

為租用戶管理器配置身份聯合

如果您希望在另一個系統（例如 Active Directory、Azure Active Directory (Azure AD)、OpenLDAP 或 Oracle Directory Server）中管理租用戶群組和用戶，則可以為租用戶管理器設定身分聯合。

開始之前

- 您已使用["支援的網頁瀏覽器"](#)。
- 您屬於具有["Root存取權限"](#)。
- 您正在使用 Active Directory、Azure AD、OpenLDAP 或 Oracle Directory Server 作為身分提供者。



如果您想使用未列出的 LDAP v3 服務，請聯絡技術支援。

- 如果您打算使用 OpenLDAP，則必須設定 OpenLDAP 伺服器。看[OpenLDAP 伺服器設定指南](#)。
- 如果您打算使用傳輸層安全性 (TLS) 與 LDAP 伺服器進行通信，則身分提供者必須使用 TLS 1.2 或 1.3。看

傳出 TLS 連線支援的密碼"。

關於此任務

您是否可以為租用戶配置身分聯合服務取決於租用戶帳戶的設定方式。您的租戶可能會共用為網格管理器配置的身分聯合服務。如果您在造訪身分聯合頁面時看到此訊息，則表示您無法為此租用戶配置單獨的聯合身分識別來源。

i 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.

輸入配置

設定身分聯合時，您需要提供StorageGRID連接到 LDAP 服務所需的值。

步驟

1. 選擇*存取管理* > 身分聯合。
2. 選擇*啟用身份聯合*。
3. 在 LDAP 服務類型部分中，選擇要設定的 LDAP 服務類型。

LDAP service type

Select the type of LDAP service you want to configure.

Active Directory	Azure	OpenLDAP	Other
------------------	-------	----------	-------

選擇「其他」來設定使用 Oracle Directory Server 的 LDAP 伺服器的值。

4. 如果您選擇了“其他”，請填寫 LDAP 屬性部分中的欄位。否則，轉到下一步。
 - 使用者唯一名稱：包含 LDAP 使用者唯一識別碼的屬性名稱。此屬性相當於 sAMAccountName`對於 Active Directory 和 `uid`對於 OpenLDAP。如果您正在設定 Oracle Directory Server，請輸入 `uid`。
 - 使用者 **UUID**：包含 LDAP 使用者的永久唯一識別碼的屬性名稱。此屬性相當於 objectGUID`對於 Active Directory 和 `entryUUID`對於 OpenLDAP。如果您正在設定 Oracle Directory Server，請輸入 `nsuniqueid`。每個使用者的指定屬性值必須是 16 位元組或字串格式的 32 位元十六進位數，其中連字元將被忽略。
 - 群組唯一名稱：包含 LDAP 群組唯一識別碼的屬性的名稱。此屬性相當於 sAMAccountName`對於 Active Directory 和 `cn`對於 OpenLDAP。如果您正在設定 Oracle Directory Server，請輸入 `cn`。
 - 群組 **UUID**：包含 LDAP 群組的永久唯一識別碼的屬性的名稱。此屬性相當於 objectGUID`對於 Active Directory 和 `entryUUID`對於 OpenLDAP。如果您正在設定 Oracle Directory Server，請輸入 `nsuniqueid`。每個群組的指定屬性的值必須是 16 位元組或字串格式的 32 位元十六進位數，其中連字元將被忽略。
5. 對於所有 LDAP 服務類型，請在設定 LDAP 伺服器部分輸入所需的 LDAP 伺服器和網路連線資訊。

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



STARTTLS 的預設連接埠是 389，LDAPS 的預設連接埠是 636。但是，只要您的防火牆配置正確，您就可以使用任何連接埠。

- 使用者名稱：將連接到 LDAP 伺服器的使用者的專有名稱 (DN) 的完整路徑。

對於 Active Directory，您也可以指定下級登入名稱或使用者主體名稱。

指定的使用者必須具有列出群組和使用者以及存取以下屬性的權限：

- `sAMAccountName` 或者 `\uid`
- `objectGUID`，`entryUUID`，或者 `nsuniqueid`
- `cn`
- `memberOf` 或者 `\isMemberOf`
- 活動目錄：`objectSid`，`primaryGroupID`，`userAccountControl`，和 `userPrincipalName`
- 蔚藍：`accountEnabled` 和 `\userPrincipalName`

- 密碼：與使用者名稱關聯的密碼。



如果您將來更改密碼，則必須在此頁面上更新。

- 群組基礎 DN：您要搜尋群組的 LDAP 子樹的可分辨名稱 (DN) 的完整路徑。在 Active Directory 範例（如下）中，所有可分辨名稱相對於基本 DN（`DC=storagegrid`、`DC=example`、`DC=com`）的群組都可以用作聯合群組。



*群組唯一名稱*值在其所屬的*群組基本 DN*內必須是唯一的。

- 使用者基礎 DN：您要搜尋使用者的 LDAP 子樹的可分辨名稱 (DN) 的完整路徑。



*使用者唯一名稱*值在其所屬的*使用者基本 DN*內必須是唯一的。

- 綁定使用者名稱格式（選用）：如果無法自動確定模式，StorageGRID 應使用預設使用者名稱模式。

建議提供*綁定使用者名稱格式*，因為如果 StorageGRID 無法與服務帳戶綁定，它可以允許使用者登入。

輸入以下模式之一：

- **UserPrincipalName 模式（Active Directory 和 Azure）**：`[USERNAME]@example.com`
- **下級登入名稱模式（Active Directory 和 Azure）**：`example\[USERNAME]`
- **可分辨名稱模式**：`CN=[USERNAME],CN=Users,DC=example,DC=com`

完全按照書寫方式包含 [USERNAME]。

6. 在傳輸層安全性 (TLS) 部分中，選擇一個安全性設定。
- 使用 **STARTTLS**：使用 STARTTLS 確保與 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（透過 SSL 的 LDAP）選項使用 TLS 建立與 LDAP 伺服器的連線。您必須為 Azure 選擇此選項。
 - 請勿使用 **TLS**：StorageGRID系統和 LDAP 伺服器之間的網路流量將不安全。Azure 不支援此選項。



如果您的 Active Directory 伺服器強制執行 LDAP 簽名，則不支援使用 不使用 **TLS** 選項。您必須使用 STARTTLS 或 LDAPS。

7. 如果您選擇了 STARTTLS 或 LDAPS，請選擇用於保護連線的憑證。
- 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。
 - 使用自訂 **CA** 憑證：使用自訂安全性憑證。

如果選擇此設置，請將自訂安全性憑證複製並貼上到 CA 憑證文字方塊中。

測試連接並儲存配置

輸入所有值後，必須先測試連接，然後才能儲存配置。如果您提供了 LDAP 伺服器的連線設定和綁定使用者名稱格式，StorageGRID會驗證該設定。

步驟

1. 選擇*測試連線*。
2. 如果您沒有提供綁定使用者名稱格式：
 - 如果連線設定有效，則會出現「測試連線成功」訊息。選擇*儲存*以儲存配置。
 - 如果連線設定無效，則會出現「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. 如果您提供了綁定使用者名稱格式，請輸入有效聯合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。用戶名中不要包含任何特殊字符，例如 @ 或 /。

Test Connection ✕

To test the connection and the bind username format, enter the username and password of a federated user. For example, enter your own federated username and password. The test values are not saved.

Test username

The username of a federated user.

Test password

Cancel Test Connection

- 如果連線設定有效，則會出現「測試連線成功」訊息。選擇*儲存*以儲存配置。
- 如果連線設定、綁定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。解決任何問題並再次測試連接。

強制與身分來源同步

StorageGRID系統會定期從身分識別來源同步聯合群組和使用者。如果您想盡快啟用或限制使用者權限，您可以強制啟動同步。

步驟

1. 前往身份聯合頁面。
2. 選擇頁面頂部的*同步伺服器*。

同步過程可能需要一些時間，具體取決於您的環境。



如果從身分來源同步聯合群組和使用者時出現問題，則會觸發*身分聯合同步失敗*警報。

禁用身份聯合

您可以暫時或永久停用群組和使用者身份聯合。當身分聯合被停用時，StorageGRID和身分來源之間就沒有通訊。但是，您配置的任何設定都會保留，以便您將來可以輕鬆地重新啟用身份聯合。

關於此任務

在停用身分聯合之前，您應該注意以下事項：

- 聯合用戶將無法登入。
- 目前已登入的聯合用戶將保留對StorageGRID系統的存取權限，直到其會話過期，但會話過期後他們將無法登入。
- StorageGRID系統和身分來源之間不會發生同步，並且不會針對未同步的帳戶發出警報。
- 如果單一登入 (SSO) 設定為 已啟用 或 沙盒模式，則 啟用身分聯合 核取方塊將會停用。在停用身分聯合之前，單一登入頁面上的 SSO 狀態必須為 已停用。看"[停用單一登入](#)"。

步驟

1. 前往身份聯合頁面。
2. 取消選取「啟用身份聯合」複選框。

OpenLDAP 伺服器設定指南

如果您想要使用 OpenLDAP 伺服器進行身份聯合，則必須在 OpenLDAP 伺服器上設定特定設定。



對於非 ActiveDirectory 或 Azure 的識別來源，StorageGRID 不會自動阻止外部停用的使用者存取 S3。若要封鎖 S3 訪問，請刪除使用者的所有 S3 金鑰或從所有群組中刪除該使用者。

Memberof 和 refint 覆蓋

應該啟用 memberof 和 refint 覆蓋。有關詳細信息，請參閱 <http://www.openldap.org/doc/admin24/index.html>["OpenLDAP 文件：版本 2.4 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，請確保幫助中提到的使用者名字段已索引，以獲得最佳效能。

請參閱有關反向群組成員資格維護的信息 <http://www.openldap.org/doc/admin24/index.html>["OpenLDAP 文件：版本 2.4 管理員指南"]。

管理租戶群組

為 S3 租用戶建立群組

您可以透過匯入聯合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

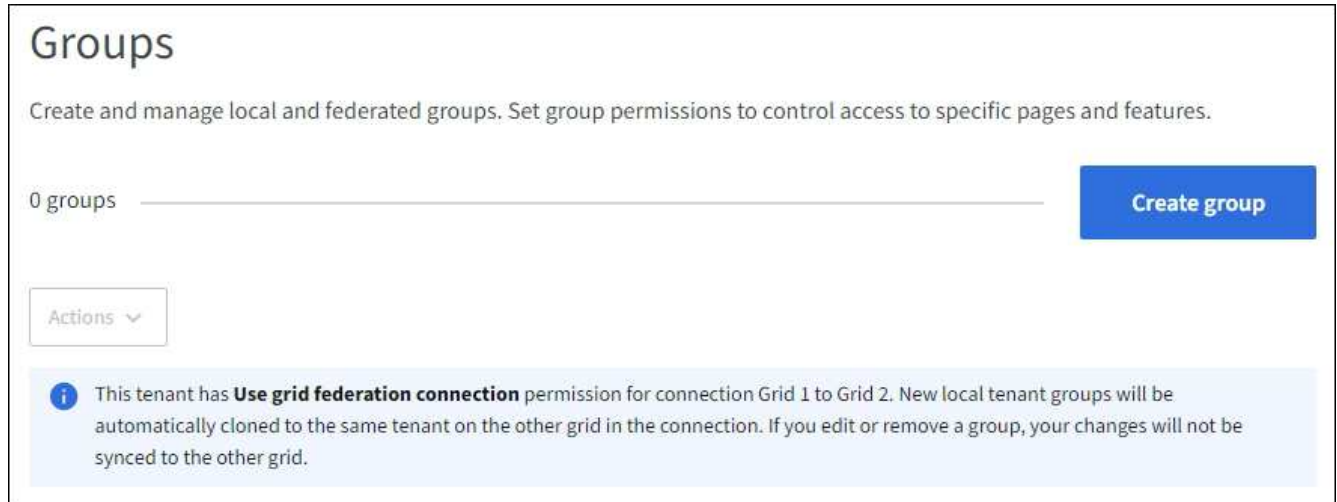
- 您已使用["支援的網頁瀏覽器"](#)。
- 您屬於具有["Root存取權限"](#)。
- 如果您計劃匯入聯合群組，則必須["配置身份聯合"](#)，且聯合群組已存在於配置的身份來源中。
- 如果您的租用戶帳戶具有「使用網格聯合連線」權限，則您已查看了下列工作流程和注意事項：["克隆租戶群組和用戶"](#)，您已登入租戶的來源網格。

存取建立群組精靈

第一步，存取建立群組精靈。

步驟

1. 選擇*存取管理* > 群組。
2. 如果您的租用戶帳戶具有*使用網格聯合連線*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被複製到連線中另一個網格上的相同租用戶。如果沒有出現此橫幅，您可能已登入租戶的目標網格。



3. 選擇*建立群組*。

選擇群組類型

您可以建立本機群組或匯入聯合群組。

步驟

1. 選擇「本機群組」標籤來建立本機群組，或選擇「聯合群組」標籤來從先前配置的身分來源匯入群組。

如果您的StorageGRID系統啟用了單一登入 (SSO)，則屬於本機群組的使用者將無法登入租用戶管理器，但他們可以根據群組權限使用用戶端應用程式來管理租用戶的資源。

2. 輸入群組的名稱。

- 本機群組：輸入顯示名稱和唯一名稱。您可以稍後編輯顯示名稱。



如果您的租用戶帳戶具有*使用網格聯合連線*權限，則當目標網格上已存在相同的租用戶*唯一名稱*時，將發生複製錯誤。

- 聯合組：輸入唯一名稱。對於 Active Directory，唯一名稱是與 `sAMAccountName` 屬性。對於 OpenLDAP，唯一名稱是與 `uid` 屬性。

3. 選擇*繼續*。

管理群組權限

群組權限控制使用者可以在租用戶管理員和租用戶管理 API 中執行哪些任務。

步驟

1. 對於*存取模式*，請選擇以下之一：

- 讀寫（預設）：使用者可以登入租用戶管理員並管理租用戶設定。

- 只讀：使用者只能查看設定和功能。他們無法在租用戶管理員或租用戶管理 API 中進行任何變更或執行任何操作。本機只讀使用者可以更改自己的密碼。



如果使用者屬於多個群組，並且任何群組設定為唯讀，則該使用者將對所有選定的設定和功能具有唯讀存取權限。

2. 為此群組選擇一個或多個權限。

看"[租用戶管理權限](#)"。

3. 選擇*繼續*。

設定 S3 組策略

群組原則決定使用者將擁有哪些 S3 存取權限。

步驟

1. 選擇您想要用於該群組的策略。

群組原則	描述
無 S3 存取權限	預設.除非透過儲存桶策略授予存取權限，否則該群組中的使用者無權存取 S3 資源。如果選擇此選項，則預設只有 root 使用者才有權存取 S3 資源。
只讀訪問	此群組中的使用者對 S3 資源具有唯讀存取權限。例如，該群組中的使用者可以列出物件並讀取物件資料、元資料和標籤。選擇此選項時，唯讀群組原則的 JSON 字串將出現在文字方塊中。您無法編輯此字串。
完全存取權限	此群組中的使用者對 S3 資源（包括儲存桶）具有完全存取權限。當您選擇此選項時，完全存取群組原則的 JSON 字串將出現在文字方塊中。您無法編輯此字串。
勒索軟體緩解	此範例策略適用於此租用戶的所有儲存桶。該群組中的使用者可以執行常見操作，但無法從啟用了物件版本控制的儲存桶中永久刪除物件。 擁有「管理所有儲存桶」權限的租用戶管理員使用者可以覆寫此群組原則。將管理所有儲存桶的權限限制為受信任的用戶，並在可用的情況下使用多重身份驗證 (MFA)。
風俗	群組中的使用者被授予您在文字方塊中指定的權限。

2. 如果您選擇了*自訂*，請輸入群組原則。每個群組策略的大小限制為 5,120 位元組。您必須輸入有效的 JSON 格式的字串。

有關群組策略的詳細資訊（包括語言語法和範例），請參閱"[群組原則範例](#)"。

3. 如果您正在建立本機群組，請選擇*繼續*。如果您正在建立聯合群組，請選擇*建立群組*和*完成*。

新增使用者（僅限本地群組）

您可以儲存群組而不新增用戶，也可以選擇新增任何已存在的本機用戶。



如果您的租用戶帳戶具有 **使用網格聯合連接** 權限，則在將群組複製到目標網格時，您在來源網格上建立本機群組時選擇的任何使用者都不會包括在內。因此，在創建群組時不要選擇使用者。相反，在建立使用者時選擇群組。

步驟

1. 或者，為此群組選擇一個或多個本機使用者。
2. 選擇***建立群組***和***完成***。

您建立的群組將出現在群組清單中。

如果您的租用戶帳戶具有***使用網格聯合連線***權限且您位於租用戶的來源網格上，則新群組將複製到租用戶的目標網格。成功***在群組詳細資料頁面的概述部分中顯示為***克隆狀態。

為 **Swift** 租用戶建立群組

您可以透過匯入聯合群組或建立本機群組來管理 Swift 租用戶帳戶的存取權。至少一個群組必須具有 Swift 管理員權限，這是管理 Swift 租用戶帳戶的容器和物件所必需的。



對 Swift 用戶端應用程式的支援已被棄用，並將在未來的版本中刪除。

開始之前

- 您已使用**"支援的網頁瀏覽器"**。
- 您屬於具有**"Root存取權限"**。
- 如果您計劃匯入聯合群組，則必須**"配置身份聯合"**，且聯合群組已存在於配置的身份來源中。

存取建立群組精靈

步驟

第一步，存取建立群組精靈。

1. 選擇***存取管理*** > 群組。
2. 選擇***建立群組***。

選擇群組類型

您可以建立本機群組或匯入聯合群組。

步驟

1. 選擇「本機群組」標籤來建立本機群組，或選擇「聯合群組」標籤來從先前配置的身分來源匯入群組。

如果您的StorageGRID系統啟用了單一登入 (SSO)，則屬於本機群組的使用者將無法登入租用戶管理器，但他們可以根據群組權限使用用戶端應用程式來管理租用戶的資源。

2. 輸入群組的名稱。

- 本機群組：輸入顯示名稱和唯一名稱。您可以稍後編輯顯示名稱。
- 聯合組：輸入唯一名稱。對於 Active Directory，唯一名稱是與 `sAMAccountName` 屬性。對於 OpenLDAP，唯一名稱是與 `uid` 屬性。

3. 選擇*繼續*。

管理群組權限

群組權限控制使用者可以在租用戶管理員和租用戶管理 API 中執行哪些任務。

步驟

1. 對於*存取模式*，請選擇以下之一：

- 讀寫（預設）：使用者可以登入租用戶管理員並管理租用戶設定。
- 只讀：使用者只能查看設定和功能。他們無法在租用戶管理員或租用戶管理 API 中進行任何變更或執行任何操作。本機只讀使用者可以更改自己的密碼。



如果使用者屬於多個群組，並且任何群組設定為唯讀，則該使用者將對所有選定的設定和功能具有唯讀存取權限。

2. 如果群組使用者需要登入租用戶管理員或租用戶管理 API，請選取 **Root** 存取 複選框。

3. 選擇*繼續*。

設定 **Swift** 組策略

Swift 使用者需要管理員權限才能驗證 Swift REST API 來建立容器和提取物件。

1. 如果群組使用者需要使用 Swift REST API 來管理容器和對象，請選取 **Swift** 管理員 複選框。
2. 如果您正在建立本機群組，請選擇*繼續*。如果您正在建立聯合群組，請選擇*建立群組*和*完成*。

新增使用者（僅限本地群組）

您可以儲存群組而不新增用戶，也可以選擇新增任何已存在的本機用戶。

步驟

1. 或者，為此群組選擇一個或多個本機使用者。

如果您尚未建立本機用戶，您可以在用戶頁面上將此群組新增至用戶。看"[管理本地用戶](#)"。

2. 選擇*建立群組*和*完成*。

您建立的群組將出現在群組清單中。

租用戶管理權限

在建立租用戶群組之前，請考慮要指派給該群組哪些權限。租用戶管理權限決定使用者可以使用租用戶管理員或租用戶管理 API 執行哪些任務。一個使用者可以屬於一個或多個群

組。如果使用者屬於多個群組，則權限是累積的。

若要登入租用戶管理員或使用租用戶管理 API，使用者必須屬於具有至少一個權限的群組。所有可以登入的使用者都可以執行以下任務：

- 查看儀表板
- 更改自己的密碼（針對本機用戶）

對於所有權限，群組的存取模式設定決定使用者是否可以變更設定和執行操作，或者是否只能查看相關設定和功能。



如果使用者屬於多個群組，並且任何群組設定為唯讀，則該使用者將對所有選定的設定和功能具有唯讀存取權限。

您可以為群組指派以下權限。請注意，S3 租用戶和 Swift 租用戶具有不同的群組權限。

允許	描述	細節
Root 存取權限	提供對租用戶管理器和租用戶管理 API 的完全存取權。	Swift 使用者必須具有 Root 存取權限才能登入租用戶帳戶。
行政人員	僅限 Swift 租戶。提供此租用戶帳戶的 Swift 容器和物件的完全存取權限	Swift 使用者必須具有 Swift 管理員權限才能使用 Swift REST API 執行任何操作。
管理您自己的 S3 憑證	允許使用者建立和刪除自己的 S3 存取密鑰。	沒有此權限的使用者看不到 儲存 (S3) > 我的 S3 存取金鑰 選單選項。
查看所有儲存桶	S3 租用戶 ：允許使用者查看所有儲存桶和儲存桶配置。 Swift 租用戶 ：允許 Swift 使用者使用租用戶管理 API 查看所有容器和容器配置。	沒有查看所有儲存桶或管理所有儲存桶權限的使用者看不到*儲存桶*選單選項。 此權限已被「管理所有儲存桶」權限取代。它不會影響 S3 用戶端或 S3 控制台使用的 S3 儲存桶或群組原則。 您只能從租用戶管理 API 將此權限指派給 Swift 群組。您不能使用租用戶管理員將此權限指派給 Swift 群組。
管理所有儲存桶	S3 租用戶 ：允許使用者使用租用戶管理器和租用戶管理 API 建立和刪除 S3 儲存桶，並管理租用戶帳戶中所有 S3 儲存桶的設置，而無需考慮 S3 儲存桶或群組原則。 Swift 租用戶 ：允許 Swift 使用者使用租用戶管理 API 控制 Swift 容器的一致性。	沒有查看所有儲存桶或管理所有儲存桶權限的使用者看不到*儲存桶*選單選項。 此權限取代了查看所有儲存桶的權限。它不會影響 S3 用戶端或 S3 控制台使用的 S3 儲存桶或群組原則。 您只能從租用戶管理 API 將此權限指派給 Swift 群組。您不能使用租用戶管理員將此權限指派給 Swift 群組。

允許	描述	細節
管理端點	允許使用者使用租用戶管理器或租用戶管理 API 建立或編輯平台服務端點，這些端點用作StorageGRID平台服務的目標。	沒有此權限的使用者看不到*平台服務端點*選單選項。
使用 S3 控制台選項卡	與查看所有儲存桶或管理所有儲存桶權限結合使用時，可讓使用者從儲存桶詳細資料頁面上的 S3 控制台標籤檢視和管理物件。	

管理群組

根據需要管理您的租用戶群組，以查看、編輯或複製群組等。

開始之前

- 您已使用["支援的網頁瀏覽器"](#)。
- 您屬於具有["Root存取權限"](#)。

檢視或編輯群組

您可以查看和編輯每個群組的基本資訊和詳細資訊。


步驟

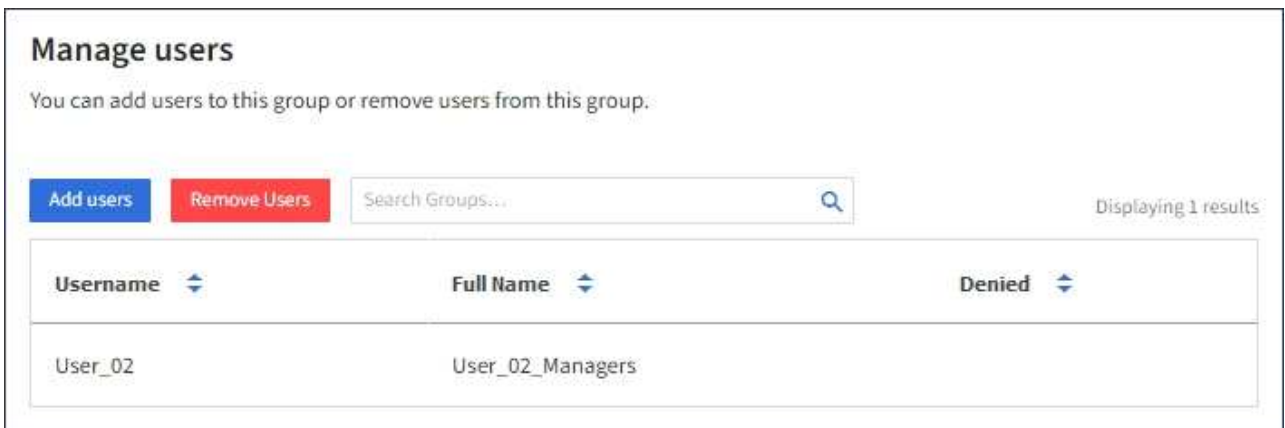
1. 選擇*存取管理* > 群組。
2. 查看「群組」頁面上提供的信息，其中列出了此租用戶帳戶的所有本機群組和聯合群組的基本資訊。

如果租用戶帳戶具有 使用網格聯合連線 權限，並且您正在查看租用戶來源網格上的群組：

- 橫幅訊息表明，如果您編輯或刪除一個群組，您的變更將不會同步到另一個網格。
- 根據需要，橫幅訊息會指示群組是否未複製到目標網格上的租戶。你可以[重試組克隆](#)失敗了。

3. 如果您想要變更群組名稱：
 - a. 選取該組的複選框。
 - b. 選擇*操作* > 編輯群組名稱。
 - c. 輸入新名稱。
 - d. 選擇“儲存變更”。
4. 如果您想要查看更多詳細資訊或進行其他編輯，請執行以下操作之一：
 - 選擇組名。
 - 選取該群組的複選框，然後選擇*操作* > 查看群組詳細資訊。
5. 查看“概述”部分，其中顯示每個組的以下資訊：
 - 顯示名稱
 - 唯一名稱
 - 類型

- 訪問模式
 - 權限
 - S3 策略
 - 本群組用戶數
 - 如果租用戶帳戶具有 使用網格聯合連線 權限且您正在查看租用戶來源網格上的群組，則附加欄位：
 - 克隆狀態，成功*或*失敗
 - 藍色橫幅表示如果您編輯或刪除該群組，您的變更將不會同步到其他網格。
6. 根據需要編輯群組設定。看"[為 S3 租用戶建立群組](#)"和"[為 Swift 租用戶建立群組](#)"了解輸入內容的詳細資訊。
- a. 在「概述」部分中，透過選擇名稱或編輯圖標。
 - b. 在*群組權限*標籤上，更新權限，然後選擇*儲存變更*。
 - c. 在「群組原則」標籤上進行任何更改，然後選擇「儲存變更」。
 - 如果您正在編輯 S3 群組，則可以根據需要選擇不同的 S3 群組原則或輸入自訂策略的 JSON 字串。
 - 如果您正在編輯 Swift 群組，可以選擇或清除 **Swift** 管理員 複選框。
7. 若要將一個或多個現有本機使用者新增至群組：
- a. 選擇“用戶”選項卡。



- b. 選擇*新增使用者*。
 - c. 選擇您想要新增的現有用戶，然後選擇*新增用戶*。
- 右上角會出現成功訊息。
8. 若要從群組中刪除本機使用者：
- a. 選擇“用戶”選項卡。
 - b. 選擇*刪除使用者*。
 - c. 選擇要刪除的用戶，然後選擇*刪除用戶*。
- 右上角會出現成功訊息。
9. 確認您為變更的每個部分選擇了「儲存變更」。

重複組

您可以複製現有群組以更快地建立新群組。



如果您的租用戶帳戶具有*使用網格聯合連線*權限，並且您從租用戶的來源網格複製一個群組，則複製的群組將被複製到租戶的目標網格。

步驟

1. 選擇*存取管理* > 群組。
2. 選取要複製的群組的複選框。
3. 選擇*動作* > 複製群組。
4. 看"[為 S3 租用戶建立群組](#)"或者"[為 Swift 租用戶建立群組](#)"了解輸入內容的詳細資訊。
5. 選擇*建立群組*。

重試組克隆

要重試失敗的克隆：

1. 選擇群組名稱下方指示「(克隆失敗)」的每個群組。
2. 選擇*操作* > 克隆組。
3. 從您正在複製的每個群組的詳細資訊頁面查看克隆操作的狀態。

有關更多信息，請參閱"[克隆租戶群組和用戶](#)"。

刪除一個或多個群組

您可以刪除一個或多個群組。任何僅屬於已刪除群組的使用者將不再能夠登入租用戶管理員或使用租用戶帳戶。



如果您的租用戶帳戶具有*使用網格聯合連線*權限並且您刪除了一個群組，StorageGRID將不會刪除另一個網格上的相應群組。如果您需要保持此資訊同步，則必須從兩個網格中刪除相同的群組。

步驟

1. 選擇*存取管理* > 群組。
2. 選取要刪除的每個群組的複選框。
3. 選擇*動作* > 刪除群組*或*操作 > 刪除群組。

出現確認對話框。

4. 選擇*刪除群組*或*刪除群組*。

管理本地用戶

您可以建立本機使用者並將他們指派到本機群組，以確定這些使用者可以存取哪些功能。租用戶管理器包括一個名為「root」的預先定義本機使用者。雖然您可以新增和刪除本機用戶，但您無法刪除根用戶。



如果您的StorageGRID系統啟用了單一登入 (SSO)，本機使用者將無法登入租用戶管理器或租用戶管理 API，但他們可以根據群組權限使用用戶端應用程式存取租用戶的資源。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 您屬於具有"Root存取權限"。
- 如果您的租用戶帳戶具有「使用網格聯合連線」權限，則您已查看了下列工作流程和注意事項："克隆租用戶群組和用戶"，您已登入租戶的來源網格。

建立本機用戶

您可以建立本機使用者並將其指派給一個或多個本機群組以控制他們的存取權限。

不屬於任何群組的 S3 使用者沒有管理權限或不套用 S3 群組原則。這些使用者可能透過儲存桶策略取得 S3 儲存桶存取權限。

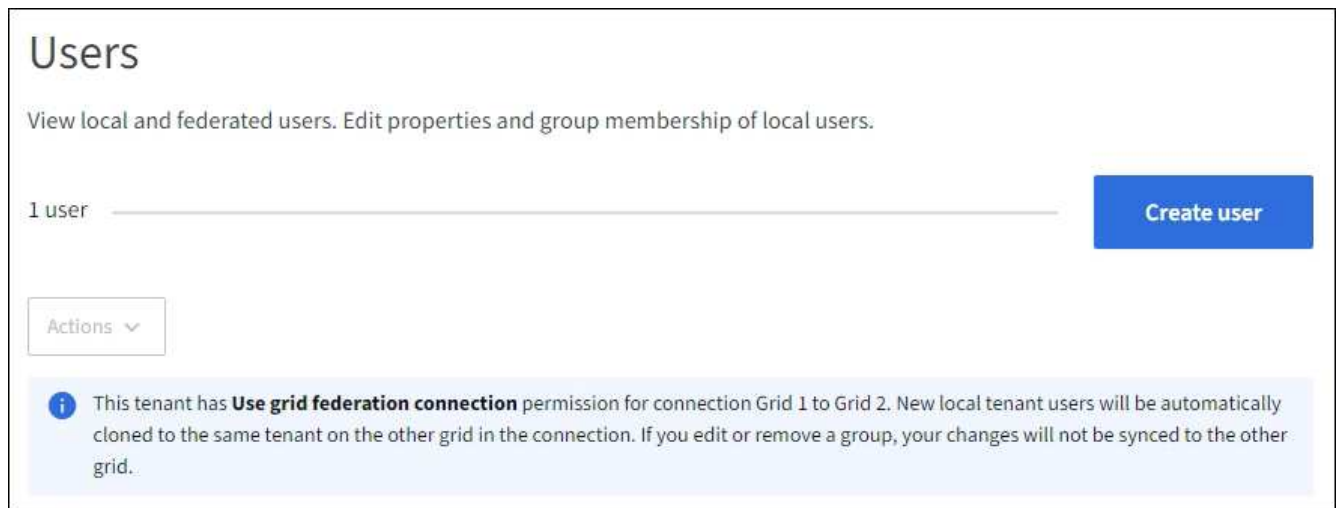
不屬於任何群組的 Swift 使用者沒有管理權限或 Swift 容器存取權限。

存取建立使用者精靈

步驟

1. 選擇*存取管理* > 使用者。

如果您的租用戶帳戶具有*使用網格聯合連線*權限，則藍色橫幅表示這是租用戶的來源網格。您在此網格上建立的任何本機使用者都會被複製到連接中的另一個網格。



2. 選擇*建立使用者*。

輸入憑證

步驟

1. 對於*輸入使用者憑證*步驟，請填寫以下欄位。

場地	描述
姓名	此使用者的全名，例如，一個人的名字和姓氏或應用程式的名稱。
使用者名稱	此用戶將用於登入的名稱。使用者名稱必須是唯一的，並且不能更改。 注意：如果您的租用戶帳戶具有*使用網格聯合連線*權限，則當目標網格上已存在與該租用戶相同的*使用者名稱*時，將發生複製錯誤。
密碼和確認密碼	使用者最初登入時所使用的密碼。
拒絕訪問	選擇「是」可阻止該使用者登入租用戶帳戶，即使他們可能仍屬於一個或多個群組。 例如，選擇「是」可暫時中止使用者的登入權限。

2. 選擇*繼續*。

分配給群組

步驟

1. 將使用者指派到一個或多個本地群組以確定他們可以執行哪些任務。

將使用者指派到群組是可選的。如果您願意，您可以在建立或編輯群組時選擇使用者。

不屬於任何群組的使用者將沒有管理權限。權限是累積的。使用者將擁有其所屬的所有群組的所有權限。看"[租用戶管理權限](#)"。

2. 選擇*建立使用者*。

如果您的租用戶帳戶具有*使用網格聯合連線*權限且您位於租用戶的來源網格上，則新的本機使用者將被複製到租用戶的目標網格。成功*在使用者詳細資料頁面的概覽部分中顯示為*克隆狀態*。

3. 選擇“完成”返回“使用者”頁面。

查看或編輯本機用戶


步驟

1. 選擇*存取管理* > 使用者。
2. 查看「使用者」頁面上提供的信息，其中列出了此租戶帳戶的所有本地用戶和聯合用戶的基本資訊。

如果租用戶帳戶具有 使用網格聯合連線 權限，且您正在查看租用戶來源網格上的使用者：

- 橫幅訊息表明，如果您編輯或刪除用戶，您的變更將不會同步到另一個網格。
- 根據需要，橫幅訊息會指示使用者是否未複製到目標網格上的租戶。您可以[重試失敗的用戶克隆](#)。

3. 如果要更改使用者的全名：
 - a. 選取使用者的複選框。

- b. 選擇*動作* > 編輯全名。
 - c. 輸入新名稱。
 - d. 選擇“儲存變更”。
4. 如果您想要查看更多詳細資訊或進行其他編輯，請執行以下操作之一：
- 選擇用戶名。
 - 選取使用者的複選框，然後選擇*操作* > 查看使用者詳細資料。
5. 查看“概述”部分，其中顯示每個用戶的以下資訊：
- 姓名
 - 使用者名稱
 - 使用者類型
 - 拒絕訪問
 - 訪問模式
 - 團體成員資格
 - 如果租用用戶帳戶具有 使用網格聯合連線 權限且您正在租用用戶的來源網格上檢視用戶，則附加欄位：
 - 克隆狀態，成功*或*失敗
 - 藍色橫幅表示如果您編輯此用戶，您的變更將不會同步到其他網格。
6. 根據需要編輯用戶設定。看[建立本地用戶](#)了解輸入內容的詳細資訊。
- a. 在「概述」部分中，透過選擇名稱或編輯圖示來變更全名 。
您不能更改使用者名稱。
 - b. 在*密碼*標籤上，變更使用者密碼，然後選擇*儲存變更*。
 - c. 在「存取」標籤上，選擇「否」以允許使用者登錄，或選擇「是」以阻止使用者登入。然後，選擇“儲存變更”。
 - d. 在「存取金鑰」標籤上，選擇「建立金鑰」並按照指示進行操作"[建立另一個使用者的 S3 存取金鑰](#)"。
 - e. 在「群組」標籤上，選擇「編輯群組」將使用者新增至群組或從群組中刪除使用者。然後，選擇*儲存變更*。
7. 確認您為變更的每個部分選擇了「儲存變更」。

重複的本地用戶

您可以複製本機使用者以更快地建立新使用者。



如果您的租用用戶帳戶具有*使用網格聯合連線*權限，並且您從租用用戶的來源網格複製用戶，則重複的用戶將被複製到租用用戶的目標網格。

步驟

1. 選擇*存取管理* > 使用者。
2. 選取您想要複製的使用者的複選框。

3. 選擇*動作* > 重複使用者。
4. 看[建立本地用戶](#)了解輸入內容的詳細資訊。
5. 選擇*建立使用者*。

重試用戶克隆

要重試失敗的克隆：

1. 選擇用戶名下方標有“（克隆失敗）”的每個用戶。
2. 選擇*操作* > 複製使用者。
3. 從您正在複製的每個使用者的詳細資訊頁面查看克隆操作的狀態。

有關更多信息，請參閱["克隆租戶群組和用戶"](#)。

刪除一個或多個本機用戶

您可以永久刪除一個或多個不再需要存取StorageGRID租用戶帳戶的本機使用者。



如果您的租用戶帳戶具有*使用網格聯合連線*權限並且您刪除本機用戶，則StorageGRID將不會刪除另一個網格上的對應用戶。如果您需要保持此資訊同步，則必須從兩個網格中刪除同一個使用者。



您必須使用聯合身份來源來刪除聯合使用者。

步驟

1. 選擇*存取管理* > 使用者。
2. 選取要刪除的每個使用者的複選框。
3. 選擇*操作* > 刪除使用者*或*操作 > 刪除使用者。

出現確認對話框。

4. 選擇*刪除使用者*或*刪除使用者*。

管理 S3 存取密鑰

管理 S3 存取密鑰

S3 租用戶帳戶的每個使用者都必須擁有一個存取金鑰才能在StorageGRID系統中儲存和擷取物件。存取密鑰由存取密鑰ID和秘密存取密鑰組成。

S3 存取密鑰可以如下管理：

- 擁有*管理您自己的 S3 憑證*權限的使用者可以建立或刪除自己的 S3 存取金鑰。
- 擁有*Root access*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。除非儲存桶策略明確停用，否則根存取金鑰為租用戶提供對所有儲存桶和物件的完全存取權。

StorageGRID支援簽章版本 2 和簽章版本 4 驗證。除非儲存桶策略明確啟用，否則不允許跨帳戶存取。

建立您自己的 S3 存取金鑰

如果您使用 S3 租用戶並且擁有適當的權限，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儲存桶和物件。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 您屬於具有"管理您自己的 S3 憑證或 Root 存取權限"。

關於此任務

您可以建立一個或多個 S3 存取金鑰，以便為您的租用戶帳戶建立和管理儲存桶。建立新的存取金鑰後，使用新的存取金鑰 ID 和秘密存取金鑰更新應用程式。為了安全起見，請不要建立超過所需數量的金鑰，並刪除不使用的金鑰。如果您只有一個密鑰並且它即將過期，請在舊密鑰過期之前建立新密鑰，然後刪除舊密鑰。

每個密鑰可以有特定的到期時間或沒有到期時間。請遵循以下有關到期時間的準則：

- 為您的金鑰設定到期時間，以限制您在特定時間段內的存取。如果您的存取金鑰 ID 和秘密存取金鑰意外洩露，設定較短的到期時間可以幫助降低您的風險。過期的密鑰將自動刪除。
- 如果您的環境中的安全風險較低，且您不需要定期建立新金鑰，則不必為金鑰設定到期時間。如果您稍後決定建立新密鑰，請手動刪除舊密鑰。



您可以使用租用戶管理員中顯示的您帳戶的存取金鑰 ID 和秘密存取金鑰存取屬於您帳戶的 S3 儲存桶和物件。因此，請像保護密碼一樣保護存取金鑰。定期輪換存取金鑰，從您的帳戶中刪除任何未使用的金鑰，並且切勿與其他使用者共用。

步驟

1. 選擇*儲存 (S3)* > 我的存取金鑰。

出現「我的造訪金鑰」頁面並列出所有現有的存取金鑰。

2. 選擇*建立金鑰*。

3. 執行下列操作之一：

- 選擇「不設定過期時間」來建立不會過期的金鑰。(預設)
- 選擇*設定到期時間*，並設定到期日期和時間。



到期日最長為當期起五年。到期時間可以從當前時間開始至少一分鐘。

4. 選擇*建立存取金鑰*。

出現「下載存取金鑰」對話框，其中列出您的存取金鑰 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，或選擇 下載 .csv 以儲存包含存取金鑰 ID 和秘密存取金鑰的電子表格檔案。



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*。

新密鑰列在「我的存取密鑰」頁面上。

7. 如果您的租用戶帳戶具有 使用網格聯合連線 權限，則可以選擇使用租用戶管理 API 將 S3 存取金鑰從來源網格上的租用戶手動複製到目標網格上的租用戶。看["使用 API 克隆 S3 存取金鑰"](#)。

查看您的 S3 存取金鑰

如果您正在使用 S3 租戶，並且您有["適當的許可"](#)，您可以查看您的 S3 存取金鑰清單。您可以按到期時間對清單進行排序，這樣您就可以確定哪些金鑰即將到期。根據需要，您可以["建立新密鑰"](#)或者["刪除鍵"](#)您不再使用。



您可以使用租用戶管理員中顯示的您帳戶的存取金鑰 ID 和秘密存取金鑰存取屬於您帳戶的 S3 儲存桶和物件。因此，請像保護密碼一樣保護存取金鑰。定期輪換存取金鑰，從您的帳戶中刪除任何未使用的金鑰，並且切勿與其他使用者共用。

開始之前

- 您已使用["支援的網頁瀏覽器"](#)。
- 您屬於擁有「管理您自己的 S3 憑證」權限的使用者群組["允許"](#)。

步驟

1. 選擇*儲存 (S3)* > 我的存取金鑰。
2. 在「我的存取金鑰」頁面中，按「到期時間」或「存取金鑰 ID」對任何現有存取金鑰進行排序。
3. 根據需要，建立新密鑰或刪除不再使用的任何密鑰。

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

過期的密鑰將自動刪除。

刪除您自己的 S3 存取金鑰

如果您正在使用 S3 租用戶並且擁有適當的權限，則可以刪除您自己的 S3 存取金鑰。存取密鑰刪除後，將無法再用於存取租戶帳戶中的物件和儲存桶。

開始之前

- 您已使用["支援的網頁瀏覽器"](#)。
- 你有["管理您自己的 S3 憑證權限"](#)。



您可以使用租用戶管理員中顯示的您帳戶的存取金鑰 ID 和秘密存取金鑰存取屬於您帳戶的 S3 儲存桶和物件。因此，請像保護密碼一樣保護存取金鑰。定期輪換存取金鑰，從您的帳戶中刪除任何未使用的金鑰，並且切勿與其他使用者共用。

步驟

1. 選擇*儲存 (S3)* > 我的存取金鑰。

2. 在「我的存取金鑰」頁面中，選取要刪除的每個存取金鑰的核取方塊。
3. 選擇*刪除鍵*。
4. 從確認對話方塊中，選擇*刪除鍵*。

頁面右上角會出現確認訊息。

建立另一個使用者的 S3 存取金鑰

如果您正在使用 S3 租用戶並且擁有適當的權限，則可以為其他使用者建立 S3 存取金鑰，例如需要存取儲存體桶和物件的應用程式。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 您屬於具有"Root存取權限"。

關於此任務

您可以為其他使用者建立一個或多個 S3 存取金鑰，以便他們可以為其租用戶帳戶建立和管理儲存桶。建立新的存取金鑰後，使用新的存取金鑰 ID 和秘密存取金鑰更新應用程式。為了安全起見，不要建立超過使用者所需的金鑰，並刪除未使用的金鑰。如果您只有一個密鑰並且它即將過期，請在舊密鑰過期之前建立新密鑰，然後刪除舊密鑰。

每個密鑰可以有特定的到期時間或沒有到期時間。請遵循以下有關到期時間的準則：

- 設定密鑰的過期時間，以限制使用者在一定時間內的存取。如果存取密鑰 ID 和秘密存取密鑰意外洩露，設定較短的到期時間可以幫助降低風險。過期的密鑰將自動刪除。
- 如果您的環境中的安全風險較低，且您不需要定期建立新金鑰，則不必為金鑰設定到期時間。如果您稍後決定建立新密鑰，請手動刪除舊密鑰。



可以使用租用戶管理員中顯示的該使用者的存取金鑰 ID 和秘密存取金鑰來存取屬於該使用者的 S3 儲存桶和物件。因此，請像保護密碼一樣保護存取金鑰。定期輪換存取金鑰，從帳戶中刪除任何未使用的金鑰，並且切勿與其他使用者共用。

步驟

1. 選擇*存取管理* > 使用者。
2. 選擇您想要管理其 S3 存取金鑰的使用者。

出現使用者詳細資料頁面。

3. 選擇*存取金鑰*，然後選擇*建立金鑰*。
4. 執行下列操作之一：
 - 選擇「不設定過期時間」來建立不會過期的密鑰。(預設)
 - 選擇*設定到期時間*，並設定到期日期和時間。



到期日最長為當期起五年。到期時間可以從當前時間開始至少一分鐘。

5. 選擇*建立存取金鑰*

出現「下載存取金鑰」對話框，其中列出存取金鑰 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，或選擇 下載 .csv 以儲存包含存取金鑰 ID 和秘密存取金鑰的電子表格檔案。



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*

新密鑰列在使用者詳細資料頁面的存取密鑰標籤上。

8. 如果您的租用戶帳戶具有 使用網格聯合連線 權限，則可以選擇使用租用戶管理 API 將 S3 存取金鑰從來源網格上的租用戶手動複製到目標網格上的租用戶。看["使用 API 克隆 S3 存取金鑰"](#)。

查看其他使用者的 S3 存取金鑰

如果您正在使用 S3 租用戶並且擁有適當的權限，則可以查看其他使用者的 S3 存取金鑰。您可以按到期時間對清單進行排序，以便確定哪些金鑰即將到期。根據需要，您可以建立新的金鑰並刪除不再使用的金鑰。

開始之前

- 您已使用["支援的網頁瀏覽器"](#)。
- 你有["Root存取權限"](#)。



可以使用租用戶管理員中顯示的該使用者的存取金鑰 ID 和秘密存取金鑰來存取屬於該使用者的 S3 儲存桶和物件。因此，請像保護密碼一樣保護存取金鑰。定期輪換存取金鑰，從帳戶中刪除任何未使用的金鑰，並且切勿與其他使用者共用。

步驟

1. 選擇*存取管理* > 使用者。
2. 在「使用者」頁面中，選擇您想要查看其 S3 存取金鑰的使用者。
3. 從使用者詳細資料頁面中，選擇*存取金鑰*。
4. 依*到期時間*或*存取金鑰ID*對金鑰進行排序。
5. 根據需要，建立新密鑰並手動刪除不再使用的密鑰。

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

過期的密鑰將自動刪除。

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

如果您正在使用 S3 租用戶並且擁有適當的權限，則可以刪除其他使用者的 S3 存取金鑰。存取密鑰刪除後，將無法再用於存取租戶帳戶中的物件和儲存桶。

開始之前

- 您已使用["支援的網頁瀏覽器"](#)。
- 你有["Root存取權限"](#)。



可以使用租用戶管理員中顯示的該使用者的存取金鑰 ID 和秘密存取金鑰來存取屬於該使用者的 S3 儲存桶和物件。因此，請像保護密碼一樣保護存取金鑰。定期輪換存取金鑰，從帳戶中刪除任何未使用的金鑰，並且切勿與其他使用者共用。

步驟

1. 選擇*存取管理* > 使用者。
2. 在「使用者」頁面中，選擇您想要管理其 S3 存取金鑰的使用者。
3. 在使用者詳細資料頁面中，選擇*存取金鑰*，然後選取要刪除的每個存取金鑰的核取方塊。
4. 選擇*動作* > 刪除選取的鍵。
5. 從確認對話方塊中，選擇*刪除鍵*。

頁面右上角會出現確認訊息。

管理 S3 儲存桶

建立 S3 儲存桶

您可以使用租用戶管理器為物件資料建立 S3 儲存桶。

開始之前

- 您已使用["支援的網頁瀏覽器"](#)。
- 您屬於具有 Root 存取權或管理所有儲存桶的使用者群組["允許"](#)。這些權限將覆蓋群組或儲存桶策略中的權限設定。



設定或修改儲存桶或物件的 S3 物件鎖定屬性的權限可以透過以下方式授予["儲存桶策略或群組策略"](#)。

- 如果您打算為儲存桶啟用 S3 物件鎖定，則網格管理員已為StorageGRID系統啟用全域 S3 物件鎖定設置，並且您已查看了 S3 物件鎖定儲存桶和物件的要求。
- 如果每個租戶有 5,000 個儲存桶，則網格中的每個儲存節點至少有 64 GB 的 RAM。



每個網格最多可以有 100,000 個桶。

訪問嚮導

步驟

1. 從儀表中選擇 查看儲存桶，或選擇 儲存 (S3) > 儲存桶。
2. 選擇*建立儲存桶*。

輸入詳細信息

步驟

1. 輸入儲存桶的詳細資訊。

場地	描述
儲存桶名稱	<p>符合以下規則的儲存桶的名稱：</p> <ul style="list-style-type: none">• 每個StorageGRID系統中必須是唯一的（而不僅僅是在租用戶帳戶內是唯一的）。• 必須符合 DNS 標準。• 必須包含至少 3 個字元且不超過 63 個字元。• 每個標籤必須以小寫字母或數字開頭和結尾，並且只能使用小寫字母、數字和連字符。• 虛擬託管樣式請求中不得包含句點。句點將導致伺服器通配符憑證驗證出現問題。 <p>有關詳細信息，請參閱 "Amazon Web Services (AWS) 有關儲存桶命名規則的文檔"。</p> <p>注意：建立儲存桶後，您無法變更儲存桶名稱。</p>
地區	<p>儲存桶的區域。</p> <p>您的StorageGRID管理員管理可用區域。儲存桶的區域會影響應用於物件的資料保護策略。預設情況下，所有儲存桶均在 `us-east-1` 地區。</p> <p>注意：建立儲存桶後，您無法變更區域。</p>

2. 選擇*繼續*。

管理設定

步驟

1. （可選）為儲存桶啟用物件版本控制。

如果您想要將每個物件的每個版本儲存在此儲存桶中，請啟用物件版本控制。然後，您可以根據需要檢索物件的先前版本。如果儲存桶將用於跨網格複製，則必須啟用物件版本控制。

2. 如果啟用了全域 S3 物件鎖定設置，則可以選擇為儲存桶啟用 S3 物件鎖定，以使用一次寫入多次讀取 (WORM) 模型儲存物件。

只有當您需要將物件保留固定時間（例如，為了滿足某些監管要求）時，才會為儲存桶啟用 S3 物件鎖定。S3 物件鎖定是一種永久性設置，可協助您防止物件在固定時間內或無限期限內被刪除或覆蓋。



一旦為儲存桶啟用 S3 物件鎖定設置，就無法停用它。任何擁有正確權限的人都可以將物件新增到此儲存桶中，並且不能更改。您可能無法刪除這些物件或儲存桶本身。

如果您為儲存桶啟用 S3 物件鎖定，則儲存桶版本控制將自動啟用。

3. 如果您選擇了“啟用 S3 物件鎖定”，則可以選擇為此儲存桶啟用“預設保留”。



您的網格管理員必須授予您以下權限“[使用 S3 Object Lock 的特定功能](#)”。

當啟用*預設保留*時，新增至儲存桶的新物件將自動受到保護，免遭刪除或覆蓋。*預設保留*設定不適用於具有自己的保留期的物件。

- a. 如果啟用了*預設保留*，請為儲存桶指定*預設保留模式*。

預設保留模式	描述
治理	<ul style="list-style-type: none">• 使用者 `s3:BypassGovernanceRetention` 許可可以使用 `x-amz-bypass-governance-retention: true` 請求標頭以繞過保留設定。• 這些用戶可以在達到保留截止日期之前刪除物件版本。• 這些使用者可以增加、減少或刪除物件的保留期限。
遵守	<ul style="list-style-type: none">• 在達到保留截止日期之前，無法刪除該物件。• 物件的保留截止日期可以增加，但不能減少。• 在達到該日期之前，不能刪除物件的保留截止日期。 <p>注意：您的電網管理員必須允許您使用合規模式。</p>

- b. 如果啟用了*預設保留*，請指定儲存桶的*預設保留期*。

*預設保留期*表示從提取新物件開始，新增至此儲存桶的新物件應保留多長時間。指定一個小於或等於網格管理員設定的租用戶最大保留期的值。

網格管理員建立租用戶時會設定最大保留期，其值可以是 1 天到 100 年。當您設定_預設_保留期時，它不能超過為最大保留期設定的值。如果需要，請您的網格管理員增加或減少最長保留期。

4. 可選，選擇*啟用容量限制*。

容量限制是此儲存桶中物件可用的最大容量。該值代表邏輯量（物件大小），而不是物理量（磁碟上的大小）。

如果沒有設定限制，則該儲存桶的容量是無限的。請參閱“[容量限制使用情況](#)”了解更多。

5. 選擇*建立儲存桶*。

儲存桶已建立並新增至「儲存桶」頁面上的表格中。

6. 或者，選擇“前往儲存桶詳細資料頁面”“[查看儲存桶詳細信息](#)”並執行額外的配置。

查看儲存桶詳細信息

您可以在您的租用戶帳戶中查看儲存桶。

開始之前

- 您已使用“[支援的網頁瀏覽器](#)”。
- 您屬於具有“[Root 存取權限](#)、[管理所有儲存桶](#)或[查看所有儲存桶權限](#)”。這些權限會覆寫群組或儲存桶策略中的權限設定。

步驟

1. 從儀表板中選擇 [查看儲存桶](#)，或選擇 [儲存 \(S3\)](#) > [儲存桶](#)。

出現「儲存桶」頁面。

2. 查看每個儲存桶的摘要表。

根據需要，您可以按任意列對資訊進行排序，也可以在清單中向前或向後翻頁。



顯示的物件計數、已使用空間和使用值都是估計值。這些估計值受到攝取時間、網路連接和節點狀態的影響。如果儲存桶啟用了版本控制，則已刪除的物件版本將包含在物件計數中。

Name

儲存桶的唯一名稱，無法變更。

已啟用的功能

為儲存桶啟用的功能清單。

S3 對象鎖

是否為儲存桶啟用了 S3 物件鎖定。

僅當為網格啟用了 S3 物件鎖定時才會出現此列。此列還顯示任何舊版相容儲存桶的資訊。

地區

bucket 的區域，不可更改。預設情況下，此列是隱藏的。

對象計數

此儲存桶中的物件數量。如果儲存桶啟用了版本控制，則非目前物件版本將包含在此值中。

當新增或刪除物件時，該值可能不會立即更新。

已用空間

儲存桶中所有物件的邏輯大小。邏輯大小不包括複製或擦除編碼副本或物件元資料所需的實際空間。

此值可能需要長達 10 分鐘才能更新。

用法

如果已設置，則為儲存桶容量限制的使用百分比。

使用價值基於內部估計，在某些情況下可能會超出。例如，當租用戶開始上傳物件時，StorageGRID會檢查容量限制（如果設定），如果租用戶已超出容量限制，則拒絕將此儲存桶進行新的攝取。但是，StorageGRID在決定是否超出容量限制時不會考慮目前上傳的大小。如果物件被刪除，租用戶可能會暫時無法將新物件上傳到此儲存桶，直到重新運算容量限制使用情況。計算可能需要 10 分鐘或更長。

該值表示邏輯大小，而不是儲存物件及其元資料所需的物理大小。

容量

如果設置，則為儲存桶的容量限制。

建立日期

儲存桶的建立日期和時間。預設情況下，此列是隱藏的。

3. 要查看特定儲存桶的詳細信息，請從表中選擇儲存桶名稱。

- a. 查看網頁頂部的摘要資訊以確認儲存桶的詳細信息，例如區域和物件數量。
- b. 查看容量限制使用欄。如果使用率達到或接近 100%，請考慮增加限制或刪除一些物件。
- c. 根據需要選擇*刪除儲存桶中的物件*和*刪除儲存桶*。



選擇每個選項時，請密切注意出現的警告。有關詳細信息，請參閱：

- "刪除儲存桶中的所有對象"
- "刪除儲存桶"（儲存桶必須為空）

d. 根據需要查看或變更每個標籤中儲存桶的設定。

- **S3 控制台**：檢視儲存桶的物件。有關詳細信息，請參閱["使用 S3 控制台"](#)。
- **儲存桶選項**：檢視或變更選項設定。某些設定（例如 S3 物件鎖定）在儲存桶建立後無法變更。
 - "管理儲存桶一致性"
 - "最後訪問時間更新"
 - "容量限制"
 - "物件版本控制"
 - "S3 對象鎖"
 - "預設儲存桶保留"
 - "管理跨網格複製"（如果租戶允許）
- **平台服務**："管理平台服務"（如果租戶允許）
- **儲存桶存取**：檢視或變更選項設定。您必須具有特定的存取權限。
 - 配置"跨域資源共享 (CORS)"因此其他網域中的 Web 應用程式可以存取該儲存桶和儲存桶中的物件。
 - "控制用戶訪問"針對 S3 儲存桶及其中的物件。

將 ILM 策略標籤應用於儲存桶

根據您的物件儲存要求，選擇要套用於儲存桶的 ILM 策略標籤。

ILM 策略控制物件資料的儲存位置以及是否在一段時間後刪除資料。當使用多個活動策略時，您的網格管理員會建立 ILM 策略並將其指派給 ILM 策略標籤。



避免頻繁重新分配儲存桶的策略標籤。否則，可能會出現效能問題。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 您屬於具有"Root 存取權限、管理所有儲存桶或查看所有儲存桶權限"。這些權限會覆寫群組或儲存桶策略中的權限設定。

步驟

1. 從儀表中選擇 查看儲存桶，或選擇 儲存 (S3) > 儲存桶。

出現「儲存桶」頁面。根據需要，您可以按任意列對資訊進行排序，也可以在清單中向前或向後翻頁。

2. 選擇要指派 ILM 策略標籤的儲存桶的名稱。

您也可以變更已指派標籤的儲存桶的 ILM 策略標籤指派。



顯示的物件數量和已使用空間值是估計值。這些估計值受到攝取時間、網路連接和節點狀態的影響。如果儲存桶啟用了版本控制，則已刪除的物件版本將包含在物件計數中。

3. 在 Bucket 選項標籤中，展開 ILM 策略標籤折疊面板。只有當您的網格管理員啟用自訂策略標籤的使用時，才會出現此手風琴。
4. 閱讀每個策略標籤的描述以確定應將哪個標籤應用於儲存桶。



更改儲存桶的 ILM 策略標籤將觸發儲存桶中所有物件的 ILM 重新評估。如果新策略在有限的時間內保留對象，則較舊的對象將被刪除。

5. 選擇要指派給儲存桶的標籤的單選按鈕。
6. 選擇“儲存變更”。新的 S3 bucket 標籤將使用 key 設定到 bucket 上 `NTAP-SG-ILM-BUCKET-TAG` 以及 ILM 策略標籤名稱的值。



確保您的 S3 應用程式不會意外覆蓋或刪除新的儲存桶標籤。如果在將新的 TagSet 套用至儲存桶時省略此標籤，則儲存桶中的物件將還原為根據預設 ILM 策略進行評估。



僅使用已驗證 ILM 策略標籤的租用戶管理器或租用戶管理器 API 來設定和修改 ILM 策略標籤。請勿修改 `NTAP-SG-ILM-BUCKET-TAG` 使用 S3 PutBucketTagging API 或 S3 DeleteBucketTagging API 的 ILM 策略標籤。



在使用新的 ILM 策略重新評估物件時，變更指派給儲存桶的策略標籤會對效能產生暫時影響。

管理儲存桶策略

您可以控制使用者對 S3 儲存桶及其中的物件的存取。

開始之前

- 您已使用["支援的網頁瀏覽器"](#)。
- 您屬於具有["Root存取權限"](#)。查看所有儲存桶和管理所有儲存桶權限僅允許查看。
- 您已驗證所需數量的儲存節點和網站可用。如果任何站點內沒有兩個或多個儲存節點可用，或者某個站點不可用，則這些設定的變更可能無法進行。

步驟

1. 選擇*[Buckets](#)*，然後選擇您想要管理的儲存桶。
2. 在儲存桶詳情頁面，選擇「[儲存桶存取](#)」>「[儲存桶策略](#)」。
3. 執行下列操作之一：
 - 透過選擇「[啟用策略](#)」複選框輸入儲存桶策略。然後輸入有效的 JSON 格式的字串。

每個儲存桶策略的大小限制為 20,480 位元組。
 - 透過編輯字串來修改現有策略。
 - 透過取消選擇*[啟用策略](#)*來停用策略。

有關儲存桶策略的詳細資訊（包括語言語法和範例），請參閱["儲存桶策略範例"](#)。

管理存儲桶一致性

一致性值可用於指定儲存桶設定變更的可用性，以及在儲存桶內的物件的可用性與不同儲存節點和網站之間的物件的一致性之間提供平衡。您可以將一致性值變更為不同於預設值，以使用戶端應用程式能夠滿足其操作需求。

開始之前

- 您已使用["支援的網頁瀏覽器"](#)。
- 您屬於具有["管理所有 bucket 或 Root 存取權限"](#)。這些權限將覆蓋群組或儲存桶策略中的權限設定。

桶一致性指南

儲存桶一致性用於確定影響該 S3 儲存桶內物件的用戶端應用程式的一致性。一般來說，您應該對儲存桶使用“Read-after-new-write”一致性。

更改儲存桶一致性

如果「Read-after-new-write」一致性不符合用戶端應用程式的要求，您可以透過設定儲存桶一致性或使用`Consistency-Control`標頭。這`Consistency-Control`標頭覆蓋了儲存桶一致性。



當您變更儲存桶的一致性時，只有在變更後擷取的物件才保證滿足修改後的設定。

步驟

1. 從儀表中選擇 查看儲存桶，或選擇 儲存 (S3) > 儲存桶。

2. 從表格中選擇儲存桶名稱。

出現儲存桶詳細資訊頁面。

3. 從“Bucket options”標籤中，選擇“手風琴”。

4. 選擇對此儲存桶中的物件執行的操作的一致性。

- 全部：提供最高等級的一致性。所有節點立即接收數據，否則請求將失敗。
- 強全域：保證所有網站上所有客戶端請求的讀寫一致性。
- 強站點：保證站點內所有客戶端請求的讀寫一致性。
- **Read-after-new-write**（預設）：為新物件提供讀取後寫入一致性，並為物件更新提供最終一致性。提供高可用性和資料保護保證。在大多數情況下建議使用。
- 可用：為新物件和物件更新提供最終一致性。對於 S3 儲存桶，僅在需要時使用（例如，對於包含很少讀取的日誌值的儲存桶，或對於不存在的鍵的 HEAD 或 GET 操作）。不支援 S3 FabricPool 儲存桶。

5. 選擇“儲存變更”。

更改儲存桶設定時會發生什麼情況

儲存桶具有多個設置，這些設置會影響儲存桶及其內的物件的行為。

以下儲存桶設定預設使用*強*一致性。如果任何站點內沒有兩個或多個儲存節點可用，或者某個站點不可用，則對這些設定的任何變更都可能無法使用。

- ["後台空桶刪除"](#)
- ["上次訪問時間"](#)
- ["儲存桶生命週期"](#)
- ["儲存桶策略"](#)
- ["桶標記"](#)
- ["儲存桶版本控制"](#)
- ["S3 對象鎖"](#)
- ["儲存桶加密"](#)



儲存桶版本控制、S3 物件鎖定和儲存桶加密的一致性值不能設定為不強一致的值。

以下儲存桶設定不使用強一致性，並且對變更具有更高的可用性。這些設定的變更可能需要一些時間才能生效。

- ["平台服務配置：通知、複製或搜尋集成"](#)
- ["CORS 配置"](#)
- [更改存儲桶一致性](#)



如果更改儲存桶設定時使用的預設一致性不符合用戶端應用程式的要求，則可以使用 `Consistency-Control` 標題為 "S3 REST API" 或使用 `reducedConsistency` 或者 `force` 選項 "租戶管理 API"。

啟用或停用上次訪問時間更新

當網格管理員為StorageGRID系統建立資訊生命週期管理 (ILM) 規則時，他們可以選擇指定使用物件的最後存取時間來確定是否將該物件移至不同的儲存位置。如果您正在使用 S3 租用戶，則可以透過為 S3 儲存桶中的物件啟用上次存取時間更新來利用此類規則。

這些說明僅適用於包含至少一條 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StorageGRID系統不包含這樣的規則，您可以忽略這些說明。看"[在 ILM 規則中使用上次存取時間](#)"了解詳情。

開始之前

- 您已使用"[支援的網頁瀏覽器](#)"。
- 您屬於具有"[管理所有 bucket 或 Root 存取權限](#)"。這些權限將覆蓋群組或儲存桶策略中的權限設定。

關於此任務

*上次造訪時間*是 ILM 規則的*參考時間*放置指令可用的選項之一。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）物件的時間來指定將物件放置在特定的儲存位置。

例如，為了確保最近查看的物件保留在更快的儲存中，網格管理員可以建立 ILM 規則，指定以下內容：

- 過去一個月檢索到的物件應保留在本機儲存節點上。
- 過去一個月內未被取回的物品應移至異地。

預設情況下，上次訪問時間的更新是禁用的。如果您的StorageGRID系統包含使用 上次存取時間 選項的 ILM 規則，並且您希望此選項應用於此儲存桶中的對象，則必須啟用對該規則中指定的 S3 儲存桶的上次存取時間更新。



檢索物件時更新最後存取時間可能會降低StorageGRID效能，尤其是對於小物件。

上次存取時間更新會對效能產生影響，因為StorageGRID每次擷取物件時都必須執行以下額外步驟：

- 使用新的時間戳更新對象
- 將物件新增至 ILM 佇列，以便可以根據目前 ILM 規則和策略重新評估它們

此表總結了當上次存取時間已停用或啟用時應用於儲存桶中所有物件的行為。

請求類型	上次訪問時間禁用時的行為（預設）		啟用上次造訪時間時的行為	
	上次造訪時間已更新？	物件已新增至 ILM 評估佇列？	上次造訪時間已更新？	物件已新增至 ILM 評估佇列？

請求檢索物件、其存取控制清單或其元數據	不	不	是的	是的
請求更新物件的元數據	是的	是的	是的	是的
請求列出物件或物件版本	不	不	不	不
請求將物件從一個儲存桶複製到另一個儲存桶	<ul style="list-style-type: none"> 不，對於來源副本 是的，對於目標副本 	<ul style="list-style-type: none"> 不，對於來源副本 是的，對於目標副本 	<ul style="list-style-type: none"> 是的，對於來源副本 是的，對於目標副本 	<ul style="list-style-type: none"> 是的，對於來源副本 是的，對於目標副本
請求完成分段上傳	是的，對於組裝好的物體	是的，對於組裝好的物體	是的，對於組裝好的物體	是的，對於組裝好的物體

步驟

1. 從儀表板中選擇 查看儲存桶，或選擇 儲存 (S3) > 儲存桶。
2. 從表格中選擇儲存桶名稱。
出現儲存桶詳細資訊頁面。
3. 從*Bucket options*選項卡中，選擇*Last access time updates*折疊面板。
4. 啟用或停用上次造訪時間更新。
5. 選擇“儲存變更”。

更改儲存桶的物件版本控制

如果您正在使用 S3 租用戶，則可以變更 S3 儲存桶的版本狀態。

開始之前

- 您已使用“支援的網頁瀏覽器”。
- 您屬於具有“管理所有 bucket 或 Root 存取權限”。這些權限將覆蓋群組或儲存桶策略中的權限設定。
- 您已驗證所需數量的儲存節點和網站可用。如果任何站點內沒有兩個或多個儲存節點可用，或者某個站點不可用，則這些設定的變更可能無法進行。

關於此任務

您可以啟用或暫停儲存桶的物件版本控制。為儲存桶啟用版本控制後，它就無法回到未版本控制狀態。但是，您可以暫停儲存桶的版本控制。

- 已停用：版本控制從未啟用
- 已啟用：版本控制已啟用

- 已暫停：版本控制之前已啟用，現已暫停

有關詳細信息，請參閱以下內容：

- ["物件版本控制"](#)
- ["S3 版本化物件的 ILM 規則和策略（範例 4）"](#)
- ["如何刪除對象"](#)

步驟

1. 從儀表中選擇 查看儲存桶，或選擇 儲存 (S3) > 儲存桶。
2. 從表格中選擇儲存桶名稱。

出現儲存桶詳細資訊頁面。

3. 從*Bucket options*標籤中，選擇*Object versioning*手風琴。
4. 為此儲存桶中的物件選擇版本控制狀態。

對於用於跨網格複製的儲存桶，物件版本控制必須保持啟用狀態。如果啟用了 S3 物件鎖定或舊版合規性，則 物件版本控制 選項將被停用。

選項	描述
啟用版本控制	如果您想要將每個物件的每個版本儲存在此儲存桶中，請啟用物件版本控制。然後，您可以根據需要檢索物件的先前版本。 當使用者修改儲存桶中已有的物件時，它們將會被版本化。
暫停版本控制	如果您不再希望建立新的物件版本，請暫停物件版本控制。您仍然可以檢索任何現有的物件版本。

5. 選擇“儲存變更”。

使用 S3 對象鎖保留對象

如果儲存桶和物件必須符合保留的監管要求，則可以使用 S3 物件鎖。



您的網格管理員必須授予您使用 S3 物件鎖定的特定功能的權限。

什麼是 S3 物件鎖？

StorageGRID S3 物件鎖定功能是一種物件保護解決方案，相當於 Amazon Simple Storage Service (Amazon S3) 中的 S3 物件鎖定。

當為StorageGRID系統啟用全域 S3 物件鎖定設定時，S3 租用戶帳戶可以建立啟用或未啟用 S3 物件鎖定的儲存桶。如果儲存桶啟用了 S3 物件鎖，則需要儲存桶版本控制，並且會自動啟用。

*沒有 S3 物件鎖的儲存桶*只能包含未指定保留設定的物件。任何攝取的物件都不會有保留設定。

*具有 S3 物件鎖定的儲存桶*可以包含由 S3 用戶端應用程式指定的具有或不具有保留設定的物件。一些攝取的物件將具有保留設定。

*配置了 S3 物件鎖定和預設保留的儲存桶*可以擁有指定了保留設定的上傳物件和不帶保留設定的新物件。新物件使用預設設置，因為尚未在物件層級配置保留設定。

實際上，當配置預設保留時，所有新攝取的物件都有保留設定。沒有物件保留設定的現有物件不受影響。

保留模式

StorageGRID S3 物件鎖定功能支援兩種保留模式，以對物件套用不同層級的保護。這些模式相當於 Amazon S3 保留模式。

- 在合規模式下：
 - 在達到保留截止日期之前，無法刪除該物件。
 - 物件的保留截止日期可以增加，但不能減少。
 - 在達到該日期之前，不能刪除物件的保留截止日期。
- 在治理模式下：
 - 具有特殊權限的使用者可以在請求中使用繞過標頭來修改某些保留設定。
 - 這些用戶可以在達到保留截止日期之前刪除物件版本。
 - 這些使用者可以增加、減少或刪除物件的保留期限。

物件版本的保留設定

如果在建立儲存桶時啟用了 S3 物件鎖定，則使用者可以使用 S3 用戶端應用程式選擇性地為新增至儲存桶的每個物件指定以下保留設定：

- 保留模式：合規或治理。
- 保留至日期：如果對象版本的保留至日期在未來，則可以檢索該對象，但不能刪除它。
- 合法保留：對物件版本套用合法保留會立即鎖定該物件。例如，您可能需要對與調查或法律糾紛相關的對象實施法律保留。合法保留沒有到期日，但會一直有效，直到明確取消。合法保留與保留截止日期無關。



如果某個物件處於合法保留之下，則無論其保留模式為何，任何人都無法刪除該物件。

有關對象設定的詳細信息，請參閱["使用 S3 REST API 設定 S3 物件鎖"](#)。

儲存桶的預設保留設定

如果在建立儲存桶時啟用了 S3 物件鎖定，使用者可以選擇為儲存桶指定以下預設設定：

- 預設保留模式：合規或治理。
- 預設保留期：新增至此儲存桶的新物件版本應保留多長時間（從新增之日起）。

預設儲存桶設定僅適用於沒有自己的保留設定的新物件。新增或變更這些預設設定時，現有的儲存桶物件不會受到影響。

看["建立 S3 儲存桶"](#)和["更新 S3 物件鎖定預設保留"](#)。

S3 物件鎖定任務

以下針對網格管理員和租用戶用戶的清單包含使用 S3 物件鎖定功能的進階任務。

網格管理員

- 為整個StorageGRID系統啟用全域 S3 物件鎖定設定。
- 確保資訊生命週期管理 (ILM) 政策符合規定；也就是說，它們滿足"啟用 S3 物件鎖的儲存桶的要求"。
- 根據需要，允許租戶使用合規性作為保留模式。否則，只允許治理模式。
- 根據需要，為租戶設定最長保留期。

租戶用戶

- 查看具有 S3 物件鎖的儲存桶和物件的注意事項。
- 根據需要聯絡網格管理員啟用全域S3物件鎖定設定並設定權限。
- 建立啟用 S3 物件鎖的儲存桶。
- 或者，配置儲存桶的預設保留設定：
 - 預設保留模式：治理或合規（如果電網管理員允許）。
 - 預設保留期：必須小於或等於網格管理員設定的最大保留期。
- 使用 S3 用戶端應用程式新增物件並選擇性地設定特定於物件的保留：
 - 保留模式。如果電網管理員允許，則進行治理或合規。
 - 保留截止日期：必須小於或等於網格管理員設定的最長保留期限。

啟用 S3 物件鎖定的儲存桶的要求

- 如果為StorageGRID系統啟用了全域 S3 物件鎖定設置，則您可以使用租用戶管理器、租用戶管理 API 或 S3 REST API 建立啟用了 S3 物件鎖定的儲存桶。
- 如果您打算使用 S3 物件鎖，則必須在建立儲存桶時啟用 S3 物件鎖。您無法為現有儲存桶啟用 S3 物件鎖定。
- 當為儲存桶啟用 S3 物件鎖時，StorageGRID會自動為該儲存桶啟用版本控制。您無法停用 S3 物件鎖定或暫停儲存桶的版本控制。
- 或者，您可以使用租用戶管理器、租用戶管理 API 或 S3 REST API 為每個儲存桶指定預設保留模式和保留期限。儲存桶的預設保留設定僅適用於新增至儲存桶且沒有自己的保留設定的新物件。您可以透過在上傳每個物件版本時為其指定保留模式和保留截止日期來覆寫這些預設值。
- 啟用 S3 物件鎖的儲存桶支援儲存桶生命週期配置。
- 啟用了 S3 物件鎖的儲存桶不支援 CloudMirror 複製。

啟用 S3 物件鎖的儲存桶中的物件要求

- 為了保護物件版本，您可以為儲存桶指定預設保留設置，也可以為每個物件版本指定保留設定。可以使用 S3 用戶端應用程式或 S3 REST API 指定物件級保留設定。
- 保留設定適用於單一物件版本。物件版本可以同時具有保留截止日期和合法保留設置，或者只具有其中之一，或者兩者都不具有。為物件指定保留期限或合法保留設定僅保護請求中指定的版本。您可以建立該物件的新版本，同時該物件的先前版本仍保持鎖定狀態。

啟用 S3 物件鎖的儲存桶中物件的生命週期

啟用 S3 物件鎖定後，儲存在儲存桶中的每個物件都會經歷以下階段：

1. 物件攝取

當物件版本新增至啟用了 S3 物件鎖定的儲存桶時，將套用下列保留設定：

- 如果為物件指定了保留設置，則套用物件層級的設定。任何預設儲存桶設定都將被忽略。
- 如果沒有為物件指定保留設置，則套用預設儲存桶設定（如果存在）。
- 如果沒有為物件或儲存桶指定保留設置，則該物件不受 S3 物件鎖定保護。

如果套用了保留設置，則物件和任何 S3 使用者定義的元資料都受到保護。

2. 物件保留和刪除

StorageGRID會儲存每個受保護物件的多個副本，並保留指定的期限。物件副本的確切數量和類型以及儲存位置由活動 ILM 策略中的相容規則決定。受保護物件是否可以在達到保留期限之前被刪除取決於其保留模式。

- 如果某個物件處於合法保留之下，則無論其保留模式為何，任何人都無法刪除該物件。

我還能管理舊版合規儲存桶嗎？

S3 物件鎖定功能取代了先前StorageGRID版本中提供的合規性功能。如果您使用先前版本的StorageGRID建立了相容儲存桶，則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。有關說明，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：如何在StorageGRID 11.5 中管理舊版相容儲存桶]。

更新 S3 物件鎖定預設保留

如果您在建立儲存桶時啟用了 S3 物件鎖定，則可以編輯儲存桶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限。

開始之前

- 您已使用["支援的網頁瀏覽器"](#)。
- 您屬於具有["管理所有 bucket 或 Root 存取權限"](#)。這些權限將覆蓋群組或儲存桶策略中的權限設定。
- S3 物件鎖定已為您的StorageGRID系統全域啟用，並且您在建立儲存桶時啟用了 S3 物件鎖定。看["使用 S3 對象鎖保留對象"](#)。

步驟

1. 從儀表中選擇 [查看儲存桶](#)，或選擇 **儲存 (S3)** > [儲存桶](#)。
2. 從表格中選擇儲存桶名稱。

出現儲存桶詳細資訊頁面。

3. 從「**Bucket options**」標籤中，選擇「**S3 Object Lock**」折疊面板。
4. 可選地，啟用或停用此儲存桶的*預設保留*。

對此設定的變更不適用於儲存桶中已有的物件或可能有其自己的保留期的任何物件。

5. 如果啟用了*預設保留*，請為儲存桶指定*預設保留模式*。

預設保留模式	描述
治理	<ul style="list-style-type: none">• 使用者 `s3:BypassGovernanceRetention` 許可可以使用 `x-amz-bypass-governance-retention: true` 請求標頭以繞過保留設定。• 這些用戶可以在達到保留截止日期之前刪除物件版本。• 這些使用者可以增加、減少或刪除物件的保留期限。
遵守	<ul style="list-style-type: none">• 在達到保留截止日期之前，無法刪除該物件。• 物件的保留截止日期可以增加，但不能減少。• 在達到該日期之前，不能刪除物件的保留截止日期。 <p>注意：您的電網管理員必須允許您使用合規模式。</p>

6. 如果啟用了*預設保留*，請指定儲存桶的*預設保留期*。

*預設保留期*表示從提取新物件開始，新增至此儲存桶的新物件應保留多長時間。指定一個小於或等於網格管理員設定的租用戶最大保留期的值。

網格管理員建立租用戶時會設定最大保留期，其值可以是 1 天到 100 年。當您設定_預設_保留期時，它不能超過為最大保留期設定的值。如果需要，請您的網格管理員增加或減少最長保留期。

7. 選擇“儲存變更”。

配置跨域資源共享 (CORS)

如果您希望其他網域中的 Web 應用程式可以存取 S3 儲存桶及其中的對象，則可以為該儲存桶配置跨網域資源共用 (CORS)。

開始之前

- 您已使用[支援的網頁瀏覽器](#)。
- 對於 GET CORS 配置請求，您屬於具有["管理所有儲存桶或查看所有儲存桶權限"](#)。這些權限將覆蓋群組或儲存桶策略中的權限設定。
- 對於 PUT CORS 設定請求，您屬於具有["管理所有 bucket 權限"](#)。此權限將覆蓋群組或儲存桶策略中的權限設定。
- 這["Root存取權限"](#)提供對所有 CORS 配置請求的存取。

關於此任務

跨域資源共用 (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 `Images`儲存圖形`。透過為 ``Images`bucket`，您可以允許該 `bucket` 中的圖像顯示在網站上 ``http://www.example.com`。

為儲存桶啟用 CORS

步驟

1. 使用文字編輯器建立所需的 XML。此範例顯示用於為 S3 儲存桶啟用 CORS 的 XML。具體來說：
 - 允許任何網域向儲存桶發送 GET 請求
 - 僅允許 `http://www.example.com` 發送 GET、POST 和 DELETE 請求的網域
 - 允許所有請求標頭

```
<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>
```

有關 CORS 配置 XML 的詳細信息，請參閱 ["Amazon Web Services \(AWS\) 文件：Amazon Simple Storage Service 使用者指南"](#)。

2. 從儀表板中選擇 查看儲存桶，或選擇 儲存 (S3) > 儲存桶。
3. 從表格中選擇儲存桶名稱。

出現儲存桶詳細資訊頁面。

4. 從「Bucket access」標籤中，選擇「Cross-Origin Resource Sharing (CORS)」手風琴。
5. 選取“啟用 CORS”複選框。
6. 將 CORS 配置 XML 貼到文字方塊中。
7. 選擇“儲存變更”。

修改 CORS 設定

步驟

1. 在文字方塊中更新 CORS 設定 XML，或選擇 清除 重新開始。
2. 選擇“儲存變更”。

禁用 CORS 設定

步驟

1. 清除“啟用 CORS”複選框。
2. 選擇“儲存變更”。

刪除儲存桶中的對象

您可以使用租用戶管理員刪除一個或多個儲存桶中的物件。

注意事項和要求

在執行這些步驟之前，請注意以下事項：

- 當您刪除儲存桶中的物件時，StorageGRID會從StorageGRID系統中的所有節點和網站永久刪除每個選取儲存桶中的所有物件和所有物件版本。StorageGRID也會刪除任何相關的物件元資料。您將無法恢復此資訊。
- 根據物件的數量、物件副本和並發操作，刪除儲存桶中的所有物件可能需要幾分鐘、幾天甚至幾週的時間。
- 如果桶中有“已啟用 S3 物件鎖定”，它可能會保持「刪除物件：只讀」狀態長達_年_。



使用 S3 物件鎖定的儲存桶將保持 刪除物件：只讀 狀態，直到所有物件的保留日期都達到並且任何合法保留都被刪除。

- 當物件被刪除時，儲存桶的狀態為*刪除物件：唯讀*。在此狀態下，您無法為儲存桶新增物件。
- 當所有物件都被刪除後，儲存桶仍保持唯讀狀態。您可以執行下列操作之一：
 - 將儲存桶恢復為寫入模式，並將其重新用於新對象
 - 刪除儲存桶
 - 將儲存桶保持在唯讀模式，以保留其名稱以供將來使用
- 如果儲存桶啟用了物件版本控制，則可以使用儲存桶操作中的刪除物件刪除在StorageGRID 11.8 或更高版本中建立的刪除標記。
- 如果儲存桶啟用了物件版本控制，則刪除物件操作將不會刪除在StorageGRID 11.7 或更早版本中建立的刪除標記。請參閱有關刪除儲存桶中物件的信息“[如何刪除 S3 版本控制對象](#)”。
- 如果你使用“[跨網格複製](#)”，請注意以下事項：
 - 使用此選項不會從另一個網格上的儲存桶中刪除任何物件。
 - 如果您為來源儲存桶選擇此選項，則在將物件新增至另一個網格上的目標儲存桶時將觸發*跨網格複製失敗*警報。如果你不能保證沒有人會將物件添加到另一個網格的儲存桶中，“[禁用跨網格複製](#)”在刪除所有儲存桶物件之前，請先刪除該儲存桶的所有物件。

開始之前

- 您已使用“[支援的網頁瀏覽器](#)”。
- 您屬於具有“[Root存取權限](#)”。此權限將覆蓋群組或儲存桶策略中的權限設定。

步驟

1. 從儀表板中選擇 [查看儲存桶](#)，或選擇 [儲存 \(S3\)](#) > [儲存桶](#)。

出現「儲存桶」頁面並顯示所有現有的 S3 儲存桶。

2. 使用*操作*選單或特定儲存桶的詳細資訊頁面。

操作選單

- a. 選取要從中刪除物件的每個儲存桶的核取方塊。
- b. 選擇*操作* > 刪除儲存桶中的物件。

詳細資訊頁面

- a. 選擇一個儲存桶名稱以顯示其詳細資訊。
- b. 選擇*刪除儲存桶中的物件*。

3. 當確認對話方塊出現時，檢查詳細信息，輸入*是*，然後選擇*確定*。

4. 等待刪除操作開始。

幾分鐘後：

- 儲存桶詳細資料頁面上會出現黃色狀態橫幅。進度條表示已刪除物件的百分比。
- (唯讀) 出現在儲存桶詳細資料頁面上的儲存桶名稱後面。
- (刪除物件：唯讀) 出現在儲存桶頁面上儲存桶名稱的旁邊。

Buckets > my-bucket

my-bucket (read-only)

Region: us-east-1

Date created: 2022-12-14 10:09:50 MST

Object count: 3

View bucket contents in Experimental S3 Console

Delete bucket

All bucket objects are being deleted

StorageGRID is deleting all copies of the objects in this bucket, which might take days or weeks. While objects are being deleted, the bucket is read only. To stop the operation, select **Stop deleting objects**. You cannot restore objects that have already been deleted.

0% (0 of 3 objects deleted)

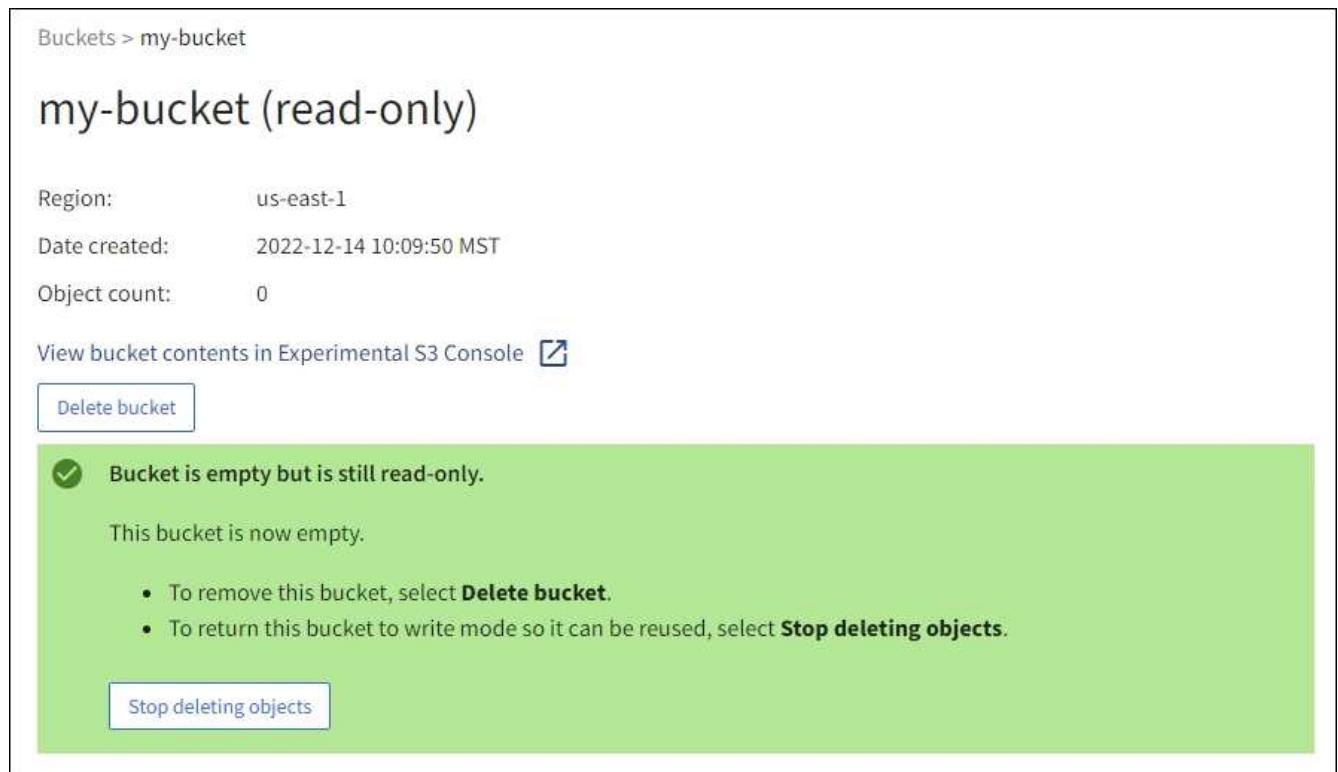
Stop deleting objects

5. 操作運行時，根據需要選擇*停止刪除物件*以停止該過程。然後，可選擇選擇「刪除儲存桶中的物件」以恢復該程序。

當您選擇*停止刪除物件*時，儲存桶將返回寫入模式；但是，您無法存取或還原任何已刪除的物件。

6. 等待操作完成。

當儲存桶為空時，狀態橫幅會更新，但儲存桶仍保持唯讀狀態。



7. 執行下列操作之一：

- 退出頁面以使儲存桶保持唯讀模式。例如，您可以將空白儲存桶保持在唯讀模式，以保留儲存桶名稱以供將來使用。
- 刪除儲存桶。您可以選擇「刪除儲存桶」來刪除單一儲存桶，或返回「儲存桶」頁面並選擇「操作」>「*刪除*儲存桶」來刪除多個儲存桶。



如果在刪除所有物件後無法刪除受版本控制的儲存桶，則刪除標記可能會保留。若要刪除儲存桶，您必須刪除所有剩餘的刪除標記。

- 將儲存桶返回寫入模式並可選擇將其重新用於新物件。您可以為單一儲存桶選擇*停止刪除物件*，或返回儲存桶頁面並為多個儲存桶選擇*操作* > 停止刪除物件。

刪除 S3 儲存桶

您可以使用租用戶管理員刪除一個或多個空的 S3 儲存桶。

開始之前

- 您已使用["支援的網頁瀏覽器"](#)。
- 您屬於具有["管理所有 bucket 或 Root 存取權限"](#)。這些權限將覆蓋群組或儲存桶策略中的權限設定。
- 您要刪除的儲存桶是空的。如果要刪除的儲存桶不為空，["從儲存桶中刪除對象"](#)。

關於此任務

這些說明描述如何使用租用戶管理員刪除 S3 儲存桶。您也可以使用["租戶管理 API"](#)或["S3 REST API"](#)。

如果 S3 儲存桶包含物件、非目前物件版本或刪除標記，則您無法刪除它。有關如何刪除 S3 版本控制對象的信息，請參閱["如何刪除對象"](#)。

步驟

1. 從儀表板中選擇 查看儲存桶，或選擇 儲存 (S3) > 儲存桶。

出現「儲存桶」頁面並顯示所有現有的 S3 儲存桶。

2. 使用*操作*選單或特定儲存桶的詳細資訊頁面。

操作選單

- a. 選取要刪除的每個儲存桶的複選框。
- b. 選擇*操作* > 刪除儲存桶。

詳細資訊頁面

- a. 選擇一個儲存桶名稱以顯示其詳細資訊。
- b. 選擇*刪除儲存桶*。

3. 當出現確認對話框時，選擇*是*。

StorageGRID確認每個儲存桶為空，然後刪除每個儲存桶。此操作可能需要幾分鐘。

如果儲存桶不為空，則會出現錯誤訊息。你必須["刪除儲存桶中的所有物件和所有刪除標記"](#)然後您才可以刪除該儲存桶。

使用 S3 控制台

您可以使用 S3 控制台檢視和管理 S3 儲存桶中的物件。

S3 控制台可讓您：

- 上傳、下載、重新命名、複製、移動和刪除對象
- 檢視、還原、下載和刪除物件版本
- 以前綴搜尋對象
- 管理對象標籤
- 查看對象元數據
- 檢視、建立、重新命名、複製、移動和刪除資料夾

S3 控制台為最常見的情況提供了改進的使用者體驗。它並非設計用於在所有情況下取代 CLI 或 API 操作。



如果使用 S3 控制台導致操作耗時過長（例如幾分鐘或幾小時），請考慮：

- 減少選定物件的數量
- 使用非圖形（API 或 CLI）方法存取您的數據

開始之前

- 您已使用["支援的網頁瀏覽器"](#)。
- 如果您想要管理對象，您屬於具有 Root 存取權限的使用者群組。或者，您屬於具有使用 S3 控制台標籤權限以及查看所有儲存桶權限或管理所有儲存桶權限的使用者群組。看["租用戶管理權限"](#)。
- 已為使用者配置 S3 群組或儲存桶策略。看["使用儲存桶和群組存取策略"](#)。
- 您知道使用者的存取金鑰 ID 和秘密存取金鑰。或者，你有一個 `.csv` 包含此資訊的文件。查看["建立存取密鑰的說明"](#)。

步驟

1. 選擇 儲存 > 儲存桶 > 儲存桶名稱。
2. 選擇 S3 控制台標籤。
3. 將存取金鑰 ID 和秘密存取金鑰貼到欄位中。否則，選擇“上傳訪問密鑰”並選擇您的 `.csv` 文件。
4. 選擇*Sign in*。
5. 出現儲存桶物件表。您可以根據需要管理對象。

附加資訊

- 按前綴搜尋：前綴搜尋功能僅搜尋相對於目前資料夾以特定單字開頭的物件。搜尋不包括在其他地方包含該詞的物件。此規則也適用於資料夾內的物件。例如，搜尋 `folder1/folder2/somefile-` 將返回 `folder1/folder2/`資料夾並以單字開頭 `somefile-`。
- 拖放：您可以將檔案從電腦的檔案管理器拖曳到 S3 控制台。但是，您不能上傳資料夾。
- 資料夾操作：當您移動、複製或重新命名資料夾時，資料夾中的所有物件都會逐一更新，這可能需要一些時間。
- 儲存桶版本控制停用時永久刪除：當您覆寫或刪除已停用版本控制的儲存桶中的物件時，此動作是永久性的。看["更改儲存桶的物件版本控制"](#)。

管理 S3 平台服務

S3 平台服務

平台服務概述與注意事項

在實施平台服務之前，請先查看使用這些服務的概述和注意事項。

有關 S3 的信息，請參閱["使用 S3 REST API"](#)。

StorageGRID平台服務可讓您將事件通知以及 S3 物件和物件元資料的副本傳送至外部目的地，從而協助您實施混合雲策略。

由於平台服務的目標位置通常位於StorageGRID部署的外部，因此平台服務為您提供了使用外部儲存資源、通知服務以及資料搜尋或分析服務所帶來的強大功能和靈活性。

可為單一 S3 儲存桶配置任意平台服務組合。例如，您可以配置"[CloudMirror 服務](#)"和"[通知](#)"在StorageGRID S3 儲存桶上，以便您可以將特定物件鏡像到 Amazon 簡單儲存服務 (S3)，同時將有關每個此類物件的通知傳送給第三方監控應用程序，以協助您追蹤 AWS 費用。



StorageGRID管理員必須使用網絡管理器或網絡管理 API 為每個租用戶帳戶啟用平台服務的使用。

如何配置平台服務

平台服務與您使用設定的外部端點進行通信"[租戶經理](#)"或"[租戶管理 API](#)"。每個端點代表一個外部目的地，例如StorageGRID S3 儲存桶、Amazon Web Services 儲存桶、Amazon SNS 主題或在本機、AWS 或其他地方託管的 Elasticsearch 叢集。

建立外部端點後，您可以透過向儲存桶新增 XML 配置來為儲存桶啟用平台服務。XML 配置標識了儲存桶應該作用的物件、儲存桶應該採取的操作以及儲存桶應該用於服務的端點。

您必須為要設定的每個平台服務新增單獨的 XML 配置。例如：

- 如果您想要所有鍵以以下項目開頭的對象 `/images` 若要複製到 Amazon S3 儲存桶，您必須在來源儲存桶中新增複製配置。
- 如果您還想在這些物件儲存到儲存桶時發送通知，則必須新增通知配置。
- 如果要索引這些物件的元數據，則必須新增用於實現搜尋整合的元資料通知配置。

配置 XML 的格式由用於實作StorageGRID平台服務的 S3 REST API 控制：

平台服務	S3 REST API	參考
CloudMirror 複製	<ul style="list-style-type: none">• 獲取Bucket複製• PutBucket複製	<ul style="list-style-type: none">• "CloudMirror 複製"• "對 bucket 的操作"
通知	<ul style="list-style-type: none">• 取得儲存桶通知配置• PutBucketNotification配置	<ul style="list-style-type: none">• "通知"• "對 bucket 的操作"
搜尋集成	<ul style="list-style-type: none">• 取得 Bucket 元資料通知配置• PUT Bucket 元資料通知配置	<ul style="list-style-type: none">• "搜尋集成"• "StorageGRID自訂操作"

使用平台服務的注意事項

考慮	細節
目標端點監控	您必須監視每個目標端點的可用性。如果與目標端點的連線長時間遺失，且存在大量積壓請求，則對StorageGRID 的其他用戶端請求（例如 PUT 請求）將會失敗。當端點可存取時，您必須重試這些失敗的請求。
目標端點限制	<p>如果傳送請求的速率超過目標端點接收請求的速率，StorageGRID軟體可能會限制儲存桶的傳入 S3 請求。只有當有大量請求等待傳送到目標端點時才會發生限制。</p> <p>唯一可見的效果是傳入的 S3 請求將需要更長時間才能執行。如果您開始偵測到效能明顯下降，則應降低攝取率或使用容量更高的端點。如果積壓的請求持續增加，客戶端 S3 操作（例如 PUT 請求）最終將會失敗。</p> <p>CloudMirror 請求更有可能受到目標端點效能的影響，因為這些請求通常涉及比搜尋整合或事件通知請求更多的資料傳輸。</p>
訂購保證	<p>StorageGRID保證站內物件的操作順序。只要針對某個物件的所有操作都在同一站點內，最終物件狀態（用於複製）將始終等於StorageGRID中的狀態。</p> <p>當跨StorageGRID站點進行操作時，StorageGRID會盡力嘗試對請求進行排序。例如，如果您最初將物件寫入網站 A，然後在網站 B 覆寫同一個對象，則 CloudMirror 複製到目標儲存桶的最終物件不能保證是較新的物件。</p>
ILM 驅動程式的物件刪除	<p>為了符合 AWS CRR 和 Amazon Simple Notification Service 的刪除行為，由於StorageGRID ILM 規則，當來源儲存桶中的物件被刪除時，不會傳送 CloudMirror 和事件通知請求。例如，如果 ILM 規則在 14 天後刪除某個對象，則不會發送任何 CloudMirror 或事件通知請求。</p> <p>相反，當由於 ILM 而刪除物件時，就會發送搜尋整合請求。</p>
使用 Kafka 端點	<p>對於 Kafka 端點，不支援 Mutual TLS。因此，如果你有 `ssl.client.auth` 設定為 `required` 在您的 Kafka 代理配置中，它可能會導致 Kafka 端點配置問題。</p> <p>Kafka 端點的身份驗證使用下列身份驗證類型。這些類型與用於其他端點（例如 Amazon SNS）的身份驗證的類型不同，並且需要使用者名稱和密碼憑證。</p> <ul style="list-style-type: none"> • SASL/普通 • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 <p>*注意：*配置的儲存代理設定不適用於 Kafka 平台服務端點。</p>

使用 CloudMirror 複製服務的注意事項

考慮	細節
複製狀態	StorageGRID不支援 `x-amz-replication-status` 標頭。

考慮	細節
物件大小	<p>CloudMirror 複製服務可以複製到目標儲存桶的物件的最大大小為 5 TiB，與最大支援的物件大小相同。</p> <p>注意：單一 PutObject 操作的最大_建議_大小為 5 GiB (5,368,709,120 位元組)。如果您的物件大於 5 GiB，請改用分段上傳。</p>
儲存桶版本控制和版本 ID	<p>如果StorageGRID中的來源 S3 儲存桶已啟用版本控制，則您也應該為目標儲存桶啟用版本控制。</p> <p>使用版本控制時，請注意，由於 S3 協定的限制，目標儲存桶中物件版本的排序是盡力而為的，並且 CloudMirror 服務不保證。</p> <p>注意：StorageGRID中來源儲存桶的版本 ID 與目標儲存桶的版本 ID 無關。</p>
物件版本標記	<p>由於 S3 協定的限制，CloudMirror 服務不會複製任何提供版本 ID 的 PutObjectTagging 或 DeleteObjectTagging 請求。由於來源和目標的版本 ID 不相關，因此無法確保特定版本 ID 的標籤更新會被複製。</p> <p>相較之下，CloudMirror 服務會複製未指定版本 ID 的 PutObjectTagging 請求或 DeleteObjectTagging 請求。這些請求更新最新金鑰的標籤（如果儲存桶有版本控制，則更新最新版本的標籤）。帶有標籤的正常攝取（不含標籤的更新）也會被複製。</p>
分段上傳和 `ETag` 價值觀	<p>當映像使用分段上傳方式上傳的物件時，CloudMirror 服務不會保留這些部分。因此，`ETag` 鏡像物件的值將不同於 `ETag` 原始物件的值。</p>
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）	<p>CloudMirror 服務不支援使用 SSE-C 加密的物件。如果您嘗試將物件提取到來源儲存桶以進行 CloudMirror 複製，並且請求包含 SSE-C 請求標頭，則操作將失敗。</p>
啟用了 S3 物件鎖的儲存桶	<p>啟用 S3 物件鎖定的來源儲存桶或目標儲存桶不支援複製。</p>

了解 CloudMirror 複製服務

如果您希望StorageGRID將新增至儲存桶的指定物件複製到一個或多個外部目標儲存桶，則可以為 S3 儲存桶啟用 CloudMirror 複製。

例如，您可以使用 CloudMirror 複製將特定客戶記錄鏡像到 Amazon S3，然後利用 AWS 服務對您的資料執行分析。



如果來源儲存桶啟用了 S3 物件鎖，則不支援 CloudMirror 複製。

CloudMirror 和 ILM

CloudMirror 複製獨立於網格的活動 ILM 策略運作。CloudMirror 服務會在物件儲存到來源儲存桶時進行複製，並儘快將其傳送到目標儲存桶。當物件攝取成功時，就會觸發複製物件的傳遞。

CloudMirror 和跨網格複製

CloudMirror 複製與跨網格複製功能有重要的相似之處和差異。請參閱["比較跨網格複製和 CloudMirror 複製"](#)。

CloudMirror 和 S3 儲存桶

CloudMirror 複製通常配置為使用外部 S3 儲存桶作為目標。但是，您也可以設定複製以使用另一個StorageGRID部署或任何與 S3 相容的服務。

現有儲存桶

當您為現有儲存桶啟用 CloudMirror 複製時，僅複製新增至該儲存桶的新物件。儲存桶中任何現有的物件都不會被複製。若要強制複製現有對象，您可以透過執行物件複製來更新現有物件的元資料。



如果您使用 CloudMirror 複製將物件複製到 Amazon S3 目標，請注意 Amazon S3 將每個 PUT 請求標頭內的使用者定義元資料的大小限制為 2 KB。如果某個物件的使用者定義元資料大於 2 KB，則不會複製該物件。

多個目標儲存桶

若要將單一儲存桶中的物件複製到多個目標儲存桶，請在複製配置 XML 中為每個規則指定目標。您不能同時將一個物件複製到多個儲存桶。

版本控制或非版本控制的儲存桶

您可以在版本化或非版本化儲存桶上設定 CloudMirror 複製。目標儲存桶可以是版本化的，也可以是非版本化的。您可以使用版本化儲存桶和非版本化儲存桶的任意組合。例如，您可以指定一個受版本控制的儲存桶作為不受版本控制的來源儲存桶的目標，反之亦然。您也可以在不受版本控制的儲存桶之間進行複製。

刪除、複製循環和事件

刪除行為

與Amazon S3服務的刪除行為相同，跨區域複製（CRR）。刪除來源儲存桶中的物件並不會刪除目標儲存桶中的複製物件。如果來源儲存桶和目標儲存桶都已版本化，則會複製刪除標記。如果目標儲存桶未進行版本控制，則刪除來源儲存桶中的物件不會將刪除標記複製到目標儲存桶或刪除目標物件。

防止複製循環

當物件被複製到目標儲存桶時，StorageGRID會將它們標記為「副本」。目標StorageGRID桶不會再次複製標記為副本的對象，從而保護您免受意外複製循環的影響。此副本標記是StorageGRID內部的，並且不會阻止您在使用 Amazon S3 儲存桶作為目標時利用 AWS CRR。



用於標記副本的自訂標頭是 `x-ntap-sg-replica`。此標記可防止鏡像層疊。StorageGRID 確實支援兩個網格之間的雙向 CloudMirror。

目標儲存桶中的事件

無法保證目標儲存桶中事件的唯一性和順序。為了確保傳送成功，可能會將來源物件的多個相同副本傳送到目標。在極少數情況下，當從兩個或多個不同的StorageGRID站點同時更新同一個物件時，目標儲存桶上的操作順序可能與來源儲存桶上的事件順序不符。

了解儲存桶的通知

如果您希望StorageGRID將有關指定事件的通知傳送至目標 Kafka 叢集或 Amazon Simple Notification Service，則可以為 S3 儲存桶啟用事件通知。

例如，您可以設定警報，以便向管理員發送有關新增至儲存桶的每個物件的警報，其中物件代表與關鍵系統事件相關的日誌檔案。

事件通知會依照通知配置中的指定在來源儲存桶中建立並傳遞到目標。如果與物件關聯的事件成功，則會建立有關該事件的通知並排隊等待傳遞。

無法保證通知的唯一性和順序。為了確保傳遞成功，可能會將一個事件的多個通知傳遞到目的地。而且由於傳遞是異步的，因此不能保證目標位置的通知時間順序與來源儲存桶上的事件順序相匹配，特別是對於源自不同StorageGRID網站的操作。您可以使用 `sequencer` 事件訊息中的鍵來決定特定物件的事件順序，如 Amazon S3 文件所述。

StorageGRID事件通知遵循 Amazon S3 API，但有一些限制。

- 支援以下事件類型：
 - s3：物件創建：
 - s3：物件創建：放置
 - s3：物件創建：發布
 - s3：物件創建：複製
 - s3：物件創建：完成分段上傳
 - s3：物件已移除：
 - s3：物件已移除：刪除
 - s3：物件已移除：刪除標記已建立
 - s3：對象恢復：發布
- 從StorageGRID發送的事件通知使用標準 JSON 格式，但不包含某些鍵，而對其他鍵使用特定值，如下表所示：

鍵名稱	StorageGRID值
事件來源	sgws:s3
aws區域	不包括
x-amz-id-2	不包括
阿恩	urn:sgws:s3:::bucket_name

了解搜尋整合服務

如果您想要對物件元資料使用外部搜尋和資料分析服務，則可以為 S3 儲存桶啟用搜尋整合。

搜尋整合服務是一種自訂StorageGRID服務，每當建立或刪除對象，或更新其元資料或標籤時，它都會自動且非同步地將 S3 對象元資料傳送到目標端點。然後，您可以使用目標服務提供的複雜搜尋、資料分析、視覺化或機器學習工具來搜尋、分析和洞察您的物件資料。

例如，您可以設定儲存桶以將 S3 物件元資料傳送到遠端 Elasticsearch 服務。然後，您可以使用 Elasticsearch 跨儲存桶執行搜索，並對物件元資料中存在的模式執行複雜的分析。

儘管可以在啟用了 S3 物件鎖定的儲存桶上配置 Elasticsearch 集成，但物件的 S3 物件鎖定元資料（包括保留截止日期和合法保留狀態）將不會包含在傳送至 Elasticsearch 的元資料中。



由於搜尋整合服務會導致物件元資料被傳送到目的地，因此其配置 XML 被稱為「_metadata_通知配置 XML」。此配置 XML 與用於啟用_事件_通知的「通知配置 XML」不同。

搜尋整合和 S3 儲存桶

您可以為任何版本化或未版本化的儲存桶啟用搜尋整合服務。透過將元資料通知配置 XML 與指定要操作的物件以及物件元資料的目的地的儲存桶關聯起來，可以配置搜尋整合。

元資料通知以 JSON 文件的形式生成，該文件以儲存桶名稱、物件名稱和版本 ID（如果有）命名。每個元資料通知除了包含物件的所有標籤和使用者元資料之外，還包含該物件的一組標準系統元資料。



對於標籤和使用者元數據，StorageGRID將日期和數字作為字串或 S3 事件通知傳遞給 Elasticsearch。若要設定 Elasticsearch 將這些字串解釋為日期或數字，請按照 Elasticsearch 的動態欄位對應和對應日期格式的說明進行操作。在配置搜尋整合服務之前，您必須在索引上啟用動態欄位對應。文檔被索引後，您無法在索引中編輯文檔的欄位類型。

搜尋通知

每當出現以下情況時，就會產生元資料通知並排隊等待傳送：

- 已建立一個物件。
- 物件被刪除，包括由於網格的 ILM 策略操作而刪除物件的情況。
- 新增、更新或刪除物件元資料或標籤。更新時總是會發送完整的元資料和標籤集——而不僅僅是更改的值。

將元資料通知配置 XML 新增至儲存桶後，系統會為您建立的任何新物件以及透過更新其資料、使用者元資料或標籤而修改的任何物件傳送通知。但是，不會針對儲存桶中已經存在的任何物件發送通知。為了確保儲存桶中所有物件的物件元資料都傳送到目標，您應該執行下列其中一項操作：

- 在建立儲存桶之後和新增任何物件之前立即配置搜尋整合服務。
- 對儲存桶中已有的所有物件執行操作，該操作將觸發元資料通知訊息傳送至目標。

搜尋集成服務和 Elasticsearch

StorageGRID搜尋整合服務支援 Elasticsearch 叢集作為目標。與其他平台服務一樣，目的地在端點中指定，該端點的 URN 用於服務的配置 XML。使用 "[NetApp互通性表工具](#)"確定支援的 Elasticsearch 版本。

管理平台服務端點

配置平台服務端點

在為儲存桶配置平台服務之前，您必須設定至少一個端點作為平台服務的目標。

StorageGRID管理員可以按租用戶啟用對平台服務的存取。若要建立或使用平台服務端點，您必須是具有管理端點或 Root 存取權限的租用戶用戶，且網格中的網路已設定為允許儲存節點存取外部端點資源。單一租用戶最多

可以配置500個平台服務端點。請聯絡您的StorageGRID管理員以取得更多資訊。

什麼是平台服務端點？

平台服務端點指定StorageGRID存取外部目標所需的資訊。

例如，如果您想要將物件從StorageGRID儲存桶複製到 Amazon S3 儲存桶，則可以建立一個平台服務端點，其中包含StorageGRID存取 Amazon 上的目標儲存桶所需的資訊和憑證。

每種類型的平台服務都需要自己的端點，因此您必須為計劃使用的每個平台服務配置至少一個端點。定義平台服務端點後，您可以使用端點的 URN 作為啟用服務的設定 XML 中的目標。

您可以將相同終端節點用作多個來源儲存桶的目標。例如，您可以設定多個來源儲存桶以將物件元資料傳送到同一個搜尋整合端點，以便您可以跨多個儲存桶執行搜尋。您還可以將來源儲存桶配置為使用多個終端節點作為目標，這使您能夠執行諸如將有關物件建立的通知傳送至一個 Amazon Simple Notification Service (Amazon SNS) 主題以及將有關物件刪除的通知傳送至第二個 Amazon SNS 主題等操作。

CloudMirror 複製的端點

StorageGRID支援代表 S3 儲存桶的複製端點。這些儲存桶可能託管在 Amazon Web Services、相同或遠端StorageGRID部署或其他服務上。

通知端點

StorageGRID支援 Amazon SNS 和 Kafka 端點。不支援簡單佇列服務 (SQS) 或 AWS Lambda 端點。

對於 Kafka 端點，不支援 Mutual TLS。因此，如果你有 `ssl.client.auth` 設定為 `required` 在您的 Kafka 代理配置中，它可能會導致 Kafka 端點配置問題。

搜尋整合服務的端點

StorageGRID支援代表 Elasticsearch 叢集的搜尋整合端點。這些 Elasticsearch 叢集可以位於本機資料中心，也可以託管在 AWS 雲端或其他地方。

搜尋整合端點是指特定的 Elasticsearch 索引和類型。您必須先在 Elasticsearch 中建立索引，然後才能在StorageGRID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，StorageGRID在將物件元資料傳送到端點時將建立該類型。

相關資訊

["管理StorageGRID"](#)

指定平台服務端點的 URN

建立平台服務端點時，必須指定唯一資源名稱 (URN)。當您為平台服務建立配置 XML 時，您將使用 URN 來引用端點。每個端點的 URN 必須是唯一的。

StorageGRID會在您建立平台服務端點時進行驗證。在建立平台服務端點之前，請確認端點中指定的資源存在並且可以存取。

URN 元素

平台服務端點的 URN 必須以 `arn:aws` 或者 `urn:mysite`，如下圖所示：

- 如果服務託管在 Amazon Web Services (AWS) 上，請使用 `arn:aws`
- 如果服務託管在 Google Cloud Platform (GCP) 上，請使用 `arn:aws`
- 如果服務在本機上託管，請使用 `urn:mysite`

例如，如果您要為StorageGRID上託管的 CloudMirror 端點指定 URN，則 URN 可能以 `urn:sgws`。

URN 的下一個元素指定平台服務的類型，如下所示：

服務	類型
CloudMirror 複製	s3
通知	sns`或者`kafka
搜尋集成	es

例如，要繼續指定StorageGRID上託管的 CloudMirror 端點的 URN，您可以新增 `s3`要得到`urn:sgws:s3`。

URN 的最後一個元素標識目標 URI 處的特定目標資源。

服務	特定資源
CloudMirror 複製	bucket-name
通知	sns-topic-name`或者`kafka-topic-name
搜尋集成	domain-name/index-name/type-name *注意：*如果 Elasticsearch 叢集未配置為自動建立索引，則必須在建立端點之前手動建立索引。

AWS 和 GCP 上託管的服務的 URN

對於 AWS 和 GCP 實體，完整的 URN 是有效的 AWS ARN。例如：

- CloudMirror 複製：

```
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
```



對於 AWS 搜尋整合終端節點，`domain-name` 必須包含文字字串 `domain/`，如下圖所示。

本地代管服務的 URN

當使用本機託管服務而不是雲端服務時，您可以以任何方式指定 URN，以建立有效且唯一的 URN，只要 URN 在第三個和最後一個位置包含所需的元素。您可以將可選指示的元素留空，也可以以任何有助於識別資源並使 URN 唯一的方式來指定它們。例如：

- CloudMirror 複製：

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

對於託管在 StorageGRID 上的 CloudMirror 端點，您可以指定以開頭有效的 URN `urn:sgws`：

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

- 通知：

指定 Amazon Simple Notification Service 終端節點：

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

指定 Kafka 端點：

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

- 搜尋整合：

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



對於本地託管的搜尋整合端點，`domain-name` 只要端點的 URN 是唯一的，元素可以是任何字串。

創建平台服務端點

您必須先建立至少一個正確類型的端點，然後才能啟用平台服務。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- StorageGRID管理員已為您的租用戶帳戶啟用平台服務。
- 您屬於具有"管理端點或 Root 存取權限"。
- 平台服務端點所引用的資源已建立：
 - CloudMirror 複製：S3 儲存桶
 - 事件通知：Amazon Simple Notification Service (Amazon SNS) 或 Kafka 主題
 - 搜尋通知：Elasticsearch 索引，如果目標群集未配置為自動建立索引。
- 您擁有有關目標資源的資訊：
 - 統一資源識別碼 (URI) 的主機和連接埠



如果您打算使用StorageGRID系統上託管的儲存桶作為 CloudMirror 複製的端點，請聯絡網絡管理員以確定您需要輸入的值。

- 唯一資源名稱 (URN)

"指定平台服務端點的 URN"

- 身份驗證憑證 (如果需要)：

搜尋整合端點

對於搜尋整合端點，您可以使用下列憑證：

- 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

CloudMirror 複製端點

對於 CloudMirror 複製端點，您可以使用下列憑證：

- 存取金鑰：存取金鑰 ID 和秘密存取金鑰
- CAP (C2S 存取入口網站)：臨時憑證 URL、伺服器 and 用戶端憑證、用戶端金鑰以及可選的用戶端私鑰密碼。

Amazon SNS 終端節點

對於 Amazon SNS 終端節點，您可以使用下列憑證：

- 存取金鑰：存取金鑰 ID 和秘密存取金鑰

Kafka 端點

對於 Kafka 端點，您可以使用下列憑證：

- SASL/PLAIN：使用者名稱和密碼
- SASL/SCRAM-SHA-256：使用者名稱和密碼
- SASL/SCRAM-SHA-512：使用者名稱和密碼

◦ 安全性憑證 (如果使用自訂 CA 憑證)

- 如果啟用了 Elasticsearch 安全功能，您將擁有用於連線測試的監視叢集權限，以及用於文件更新的寫入索引權限或索引和刪除索引權限。

步驟

1. 選擇*儲存 (S3) * > 平台服務端點。出現平台服務端點頁面。
2. 選擇*建立端點*。
3. 輸入顯示名稱以簡要描述端點及其用途。

當端點在「端點」頁面上列出時，端點支援的平台服務類型會顯示在端點名稱旁邊，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碼 (URI)。

使用以下格式之一：

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

如果您未指定端口，則使用以下預設端口：

- HTTPS URI 的连接埠為 443，HTTP URI 的连接埠為 80（大多數端點）
- HTTPS 和 HTTP URI 的连接埠 9092（僅限 Kafka 端點）

例如，StorageGRID上託管的儲存桶的 URI 可能是：

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

在這個例子中，`s3.example.com` 表示 StorageGRID 高可用性 (HA) 群組的虛擬 IP (VIP) 的 DNS 條目，並且 `10443` 表示負載平衡器端點中定義的连接埠。



只要有可能，您就應該连接到負載平衡節點的 HA 群組，以避免單點故障。

類似地，AWS 上託管的儲存桶的 URI 可能是：

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



如果端點用於 CloudMirror 複製服務，請不要在 URI 中包含儲存桶名稱。您將儲存桶名稱包含在 **URN** 欄位中。

5. 輸入端點的唯一資源名稱 (URN)。



端點建立後，您無法變更端點的 URN。

6. 選擇*繼續*。

7. 為*身份驗證類型*選擇一個值。

搜尋整合端點

輸入或上傳搜尋整合端點的憑證。

您提供的憑證必須具有目標資源的寫入權限。

身份驗證類型	描述	證書
匿名的	提供對目的地的匿名訪問。僅適用於已停用安全性的端點。	沒有驗證。
存取密鑰	使用 AWS 樣式的憑證來驗證與目標的連線。	<ul style="list-style-type: none">存取密鑰 ID秘密存取密鑰
基本 HTTP	使用使用者名稱和密碼來驗證與目的地的連線。	<ul style="list-style-type: none">使用者名稱密碼

CloudMirror 複製端點

輸入或上傳 CloudMirror 複製端點的憑證。

您提供的憑證必須具有目標資源的寫入權限。

身份驗證類型	描述	證書
匿名的	提供對目的地的匿名訪問。僅適用於已停用安全性的端點。	沒有驗證。
存取密鑰	使用 AWS 樣式的憑證來驗證與目標的連線。	<ul style="list-style-type: none">存取密鑰 ID秘密存取密鑰
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。	<ul style="list-style-type: none">臨時憑證 URL伺服器CA憑證 (PEM檔案上傳)客戶端憑證 (PEM文件上傳)客戶端私鑰 (PEM檔案上傳，OpenSSL加密格式或未加密私鑰格式)客戶端私鑰密碼 (可選)

Amazon SNS 終端節點

輸入或上傳 Amazon SNS 終端節點的憑證。

您提供的憑證必須具有目標資源的寫入權限。

身份驗證類型	描述	證書
匿名的	提供對目的地的匿名訪問。僅適用於已停用安全性的端點。	沒有驗證。
存取密鑰	使用 AWS 樣式的憑證來驗證與目標的連線。	<ul style="list-style-type: none"> 存取密鑰 ID 秘密存取密鑰

Kafka 端點

輸入或上傳 Kafka 端點的憑證。

您提供的憑證必須具有目標資源的寫入權限。

身份驗證類型	描述	證書
匿名的	提供對目的地的匿名訪問。僅適用於已停用安全性的端點。	沒有驗證。
SASL/普通	使用純文字的使用者名稱和密碼來驗證與目的地的連線。	<ul style="list-style-type: none"> 使用者名稱 密碼
SASL/SCRAM-SHA-256	使用使用者名稱和密碼透過質詢-回應協定和 SHA-256 雜湊來驗證與目的地的連線。	<ul style="list-style-type: none"> 使用者名稱 密碼
SASL/SCRAM-SHA-512	使用使用者名稱和密碼透過質詢回應協定和 SHA-512 雜湊來驗證與目的地的連線。	<ul style="list-style-type: none"> 使用者名稱 密碼

如果使用者名稱和密碼來自從 Kafka 叢集取得的委託令牌，請選擇「使用委託採取的身份驗證」。

- 選擇*繼續*。
- 選擇*驗證伺服器*單選按鈕來選擇如何驗證與端點的 TLS 連線。

證書驗證類型	描述
使用自訂 CA 證書	使用自訂安全性證書。如果選擇此設置，請將自訂安全性憑證複製並貼上到 CA 憑證 文字方塊中。
使用作業系統CA證書	使用作業系統上安裝的預設 Grid CA 憑證來保護連線。
不驗證證書	未驗證用於 TLS 連線的憑證。此選項不安全。

- 選擇*測試並建立端點*。

- 如果可以使用指定的憑證到達端點，則會顯示成功訊息。每個站點的一個節點都會驗證與端點的連線。
- 如果端點驗證失敗，則會出現錯誤訊息。如果需要修改端點以修正錯誤，請選擇*返回端點詳細資訊*並更新資訊。然後，選擇*測試並建立端點*。



如果您的租用戶帳戶未啟用平台服務，則端點建立會失敗。聯絡您的StorageGRID管理員。

配置端點後，您可以使用其 URN 來配置平台服務。

相關資訊

- ["指定平台服務端點的 URN"](#)
- ["配置 CloudMirror 複製"](#)
- ["配置事件通知"](#)
- ["配置搜尋整合服務"](#)

測試平台服務端點的連接

如果與平台服務的連線發生變化，您可以測試端點的連線以驗證目標資源是否存在以及是否可以使用您指定的憑證存取該資源。

開始之前

- 您已使用["支援的網頁瀏覽器"](#)。
- 您屬於具有["管理端點或 Root 存取權限"](#)。

關於此任務

StorageGRID不會驗證憑證是否具有正確的權限。

步驟

1. 選擇*儲存 (S3) * > 平台服務端點。

出現「平台服務端點」頁面並顯示已設定的平台服務端點清單。

2. 選擇要測試其連線的端點。

出現端點詳細資料頁面。

3. 選擇*測試連線*。

- 如果可以使用指定的憑證到達端點，則會顯示成功訊息。每個站點的一個節點都會驗證與端點的連線。
- 如果端點驗證失敗，則會出現錯誤訊息。如果需要修改端點以修正錯誤，請選擇*設定*並更新資訊。然後，選擇*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配置以變更其名稱、URI 或其他詳細資訊。例如，您可能需要更新過期的憑證或變更 URI 以指向備份 Elasticsearch 索引以進行故障轉移。您無法變更

平台服務端點的 URN。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 您屬於具有"管理端點或 Root 存取權限"。

步驟

1. 選擇*儲存 (S3) * > 平台服務端點。

出現「平台服務端點」頁面並顯示已設定的平台服務端點清單。

2. 選擇要編輯的端點。


出現端點詳細資料頁面。

3. 選擇*配置*。

4. 根據需要，更改端點的配置。



端點建立後，您無法變更端點的 URN。

- a. 若要變更端點的顯示名稱，請選擇編輯圖標.
- b. 根據需要更改 URI。
- c. 根據需要變更身份驗證類型。
 - 對於存取金鑰身份驗證，請根據需要透過選擇*編輯 S3 金鑰*並貼上新的存取金鑰 ID 和秘密存取金鑰來變更金鑰。如果您需要取消更改，請選擇*恢復 S3 鍵編輯*。
 - 對於 CAP (C2S 存取入口網站) 驗證，變更臨時憑證 URL 或可選用戶端私鑰密碼，並根據需要上傳新的憑證和金鑰檔案。



客戶端私鑰必須是OpenSSL加密格式或未加密私鑰格式。

- d. 根據需要，更改驗證伺服器的方法。

5. 選擇*測試並儲存變更*。

- 如果可以使用指定的憑證到達端點，則會顯示成功訊息。從每個站點的一個節點驗證與端點的連線。
- 如果端點驗證失敗，則會出現錯誤訊息。修改端點以修正錯誤，然後選擇*測試並儲存變更*。

刪除平台服務端點

如果您不再想使用相關的平台服務，您可以刪除端點。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 您屬於具有"管理端點或 Root 存取權限"。

步驟

1. 選擇*儲存 (S3) * > 平台服務端點。

出現「平台服務端點」頁面並顯示已設定的平台服務端點清單。

2. 選取要刪除的每個端點的核取方塊。



如果刪除正在使用的平台服務端點，則對於使用該端點的任何儲存桶，關聯的平台服務都會被停用。任何尚未完成的請求將被丟棄。任何新請求都會繼續生成，直到您將儲存桶配置變更為不再引用已刪除的 URN。StorageGRID 會將這些請求報告為不可恢復的錯誤。

3. 選擇*動作* > 刪除端點。

出現確認訊息。

4. 選擇*刪除端點*。

排查平台服務端點錯誤

如果StorageGRID嘗試與平台服務端點通訊時發生錯誤，則儀表板上會顯示一則訊息。在平台服務端點頁面上，「上次錯誤」欄位指示錯誤發生的時間。如果與端點憑證相關的權限不正確，則不會顯示錯誤。

確定是否發生錯誤


如果過去 7 天內發生任何平台服務端點錯誤，租用戶管理器儀表板將顯示一則警報訊息。您可以前往平台服務端點頁面以查看有關該錯誤的更多詳細資訊。



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部。要查看更詳細的錯誤訊息：

步驟

1. 從端點清單中，選擇出現錯誤的端點。
2. 在端點詳細資料頁面上，選擇*連線*。此標籤僅顯示端點的最新錯誤並指示錯誤發生的時間。包含紅色 X 圖示的錯誤  發生在過去 7 天內。

檢查錯誤是否仍然存在

某些錯誤即使已解決，仍可能繼續顯示在「最後錯誤」欄位中。若要查看錯誤是否為目前錯誤或強制從表中刪除已解決的錯誤：

步驟

1. 選擇端點。
出現端點詳細資料頁面。
2. 選擇*連線* > 測試連線。

選擇*測試連線*會導致StorageGRID驗證平台服務端點是否存在以及是否可以使用目前憑證存取它。每個站點的一個節點都會驗證與端點的連線。

解決端點錯誤

您可以使用端點詳細資料頁面上的「最後錯誤」訊息來協助確定導致錯誤的原因。某些錯誤可能需要您編輯端點來解決問題。例如，如果StorageGRID由於沒有正確的存取權限或存取金鑰已過期而無法存取目標 S3 儲存桶，則可能會發生 CloudMirroring 錯誤。訊息為“需要更新端點憑證或目標存取”，詳細資訊為“AccessDenied”或“InvalidAccessKeyId”。

如果您需要編輯端點來解決錯誤，選擇*測試並儲存變更*將導致StorageGRID驗證更新後的端點並確認可以使用目前憑證存取它。每個站點的一個節點都會驗證與端點的連線。

步驟

1. 選擇端點。
2. 在端點詳細資料頁面上，選擇*配置*。
3. 根據需要編輯端點配置。
4. 選擇*連線* > 測試連線。

權限不足的端點憑證

當StorageGRID驗證平台服務端點時，它會確認端點的憑證可用於聯絡目標資源，並進行基本權限檢查。但是，StorageGRID不會驗證某些平台服務操作所需的所有權限。因此，如果您在嘗試使用平台服務時收到錯誤（例如「403 禁止」），請檢查與端點憑證相關的權限。

相關資訊

- [管理StorageGRID](#) > [排除平台服務故障](#)
- ["創建平台服務端點"](#)
- ["測試平台服務端點的連接"](#)
- ["編輯平台服務端點"](#)

配置 CloudMirror 複製

若要為儲存桶啟用 CloudMirror 複製，您需要建立並套用有效的儲存桶複製配置 XML。

開始之前

- StorageGRID管理員已為您的租用戶帳戶啟用平台服務。
- 您已經建立了一個儲存桶作為複製來源。
- 您打算用作 CloudMirror 複製目標的端點已經存在，並且您有其 URN。
- 您屬於具有“[管理所有 bucket 或 Root 存取權限](#)”。使用租用戶管理器配置儲存桶時，這些權限會覆寫群組或儲存桶原則中的權限設定。

關於此任務

CloudMirror 複製將物件從來源儲存桶複製到端點中指定的目標儲存桶。

有關儲存桶複製及其配置方法的一般信息，請參閱 ["Amazon Simple Storage Service \(S3\) 文件：複製對象"](#)。有

關StorageGRID如何實現 GetBucketReplication、DeleteBucketReplication 和 PutBucketReplication 的信息，請參閱["對 bucket 的操作"](#)。



CloudMirror 複製與跨網格複製功能有重要的相似之處和差異。要了解更多信息，請參閱["比較跨網格複製和 CloudMirror 複製"](#)。

配置CloudMirror複製時請注意以下要求和特點：

- 當您建立並套用有效的儲存桶複製配置 XML 時，它必須使用每個目標的 S3 儲存桶端點的 URN。
- 啟用 S3 物件鎖定的來源儲存桶或目標儲存桶不支援複製。
- 如果在包含對象的儲存桶上啟用 CloudMirror 複製，則會複製新增至儲存桶的新對象，但不會複製儲存桶中的現有物件。您必須更新現有物件才能觸發複製。
- 如果您在複製配置 XML 中指定儲存類， StorageGRID會在針對目標 S3 端點執行操作時使用該類別。目標端點也必須支援指定的儲存類別。請務必遵循目標系統供應商提供的所有建議。

步驟

1. 為來源儲存桶啟用複製：

- 使用文字編輯器建立啟用複製所需的複製配置 XML，如 S3 複製 API 中所指定。
- 配置 XML 時：
 - 請注意， StorageGRID僅支援複製配置的 V1。這意味著StorageGRID不支援使用 `Filter` 元素作為規則，並遵循 V1 約定來刪除物件版本。有關詳細信息，請參閱有關複製配置的 Amazon 文件。
 - 使用 S3 儲存桶端點的 URN 作為目標。
 - 可選地添加 `` 元素，並指定下列之一：
 - STANDARD：預設儲存類別。如果您在上傳物件時未指定儲存類別，則 `STANDARD` 使用儲存類別。
 - STANDARD_IA：（標準 - 不頻繁訪問。）將此儲存類別用於存取頻率較低但仍需要快速存取的資料。
 - REDUCED_REDUNDANCY：此儲存類別用於儲存非關鍵、可重現的數據，其儲存冗餘度比 `STANDARD` 儲存類別。
 - 如果您指定 `Role` 在配置 XML 中它將被忽略。 StorageGRID不使用此值。

```
<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. 從儀表中選擇 查看儲存桶，或選擇 儲存 (S3) > 儲存桶。

3. 選擇來源儲存桶的名稱。

出現儲存桶詳細資訊頁面。

4. 選擇“平台服務”>“複製”。

5. 選取“啟用複製”複選框。

6. 將複製配置 XML 貼上到文字方塊中，然後選擇*儲存變更*。



StorageGRID管理員必須使用 Grid Manager 或 Grid Management API 為每個租用戶帳戶啟用平台服務。如果儲存配置 XML 時發生錯誤，請聯絡您的StorageGRID管理員。

7. 驗證複製配置是否正確：

a. 將符合複製配置中指定的複製要求的物件新增至來源儲存桶。

在前面顯示的範例中，與前綴「2020」相符的物件被複製。

b. 確認物件已複製到目標儲存桶。

對於小物體，複製會很快發生。

相關資訊

["創建平台服務端點"](#)

配置事件通知

您可以透過建立通知配置 XML 並使用租用戶管理器將 XML 套用到儲存桶來啟用儲存桶的通知。

開始之前

- StorageGRID管理員已為您的租用戶帳戶啟用平台服務。
- 您已經建立了一個儲存桶作為通知來源。
- 您打算用作事件通知目標的端點已經存在，並且您有其 URN。
- 您屬於具有“[管理所有 bucket 或 Root 存取權限](#)”。使用租用戶管理器配置儲存桶時，這些權限會覆寫群組或儲存桶原則中的權限設定。

關於此任務

您可以將通知配置 XML 與來源儲存桶關聯來設定事件通知。通知配置 XML 遵循 S3 約定來配置儲存桶通知，並將目標 Kafka 或 Amazon SNS 主題指定為端點的 URN。

有關事件通知及其配置方法的一般信息，請參閱 ["亞馬遜文檔"](#)。有關StorageGRID如何實現 S3 儲存桶通知配置 API 的信息，請參閱["實施 S3 客戶端應用程式的說明"](#)。

為儲存桶配置事件通知時，請注意以下要求和特徵：

- 當您建立並套用有效的通知配置 XML 時，它必須使用每個目標的事件通知端點的 URN。

- 雖然可以在啟用 S3 物件鎖定的儲存桶上配置事件通知，但物件的 S3 物件鎖定元資料（包括保留截止日期和合法保留狀態）不會包含在通知訊息中。
- 配置事件通知後，每當來源儲存桶中的物件發生指定事件時，都會產生通知並傳送至用作目標終端節點的 Amazon SNS 或 Kafka 主題。
- 如果您為包含物件的儲存桶啟用事件通知，則僅針對儲存通知配置後執行的操作傳送通知。

步驟

1. 為您的來源儲存桶啟用通知：

- 使用文字編輯器建立啟用事件通知所需的配置 XML，如 S3 通知 API 中所指定。
- 配置 XML 時，使用事件通知端點的 URN 作為目標主題。

```
<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. 在租用戶管理員中，選擇 **STORAGE (S3) > Buckets**。

3. 選擇來源儲存桶的名稱。

出現儲存桶詳細資訊頁面。

4. 選擇*平台服務* > 事件通知。

5. 選取「啟用事件通知」複選框。

6. 將通知配置 XML 貼上到文字方塊中，然後選擇*儲存變更*。



StorageGRID 管理員必須使用 Grid Manager 或 Grid Management API 為每個租用戶帳戶啟用平台服務。如果儲存配置 XML 時發生錯誤，請聯絡您的 StorageGRID 管理員。

7. 驗證事件通知是否配置正確：

- a. 對來源儲存桶中符合配置 XML 中配置的觸發通知要求的物件執行操作。

在範例中，每當使用以下方式建立物件時，都會發送事件通知：`images/` 前綴。

b. 確認通知已傳送至目標 Amazon SNS 或 Kafka 主題。

例如，如果您的目標主題託管在 Amazon SNS 上，您可以設定服務以在通知送達時向您發送電子郵件。

```
{
  "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"
        }
      }
    }
  ]
}
```

+ 如果在目標主題收到通知，則表示您已成功為StorageGRID通知配置來源儲存桶。

相關資訊

["了解儲存桶的通知"](#)

"使用 S3 REST API"

"創建平台服務端點"

配置搜尋整合服務

您可以透過建立搜尋整合 XML 並使用租用戶管理器將 XML 套用於儲存桶來啟用儲存桶的搜尋整合。

開始之前

- StorageGRID 管理員已為您的租用戶帳戶啟用平台服務。
- 您已經建立了一個想要索引其內容的 S3 儲存桶。
- 您打算用作搜尋整合服務目標的端點已經存在，並且您有其 URN。
- 您屬於具有"管理所有 bucket 或 Root 存取權限"。使用租用戶管理器配置儲存桶時，這些權限會覆寫群組或儲存桶原則中的權限設定。

關於此任務

為來源儲存桶配置搜尋整合服務後，建立物件或更新物件的元資料或標籤會觸發將物件元資料傳送至目標端點。

如果為已包含物件的儲存桶啟用搜尋整合服務，則不會自動為現有物件傳送元資料通知。更新這些現有物件以確保其元資料已新增至目標搜尋索引。

步驟

1. 為儲存桶啟用搜尋整合：
 - 使用文字編輯器建立啟用搜尋整合所需的元資料通知 XML。
 - 配置 XML 時，使用搜尋整合端點的 URN 作為目標。

可以根據物件名稱的前綴來過濾物件。例如，您可以發送帶有前綴的物件元數據 `images` 到一個目標，以及帶有前綴的物件的元數據 `videos` 到另一個。具有重疊前綴的配置無效，並且在提交時會被拒絕。例如，包含一個針對具有前綴的物件規則的配置 `test` 第二個規則針對的是帶有前綴的對象 `test2` 是不允許的。

根據需要，參考[元資料配置 XML 的範例](#)。

```
<MetadataNotificationConfiguration>
  <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>/Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

元資料通知配置 XML 中的元素：

Name	描述	必需的
元數據通知配置	<p>用於指定元資料通知的物件和目的地的規則的容器標籤。</p> <p>包含一個或多個 Rule 元素。</p>	是的
規則	<p>規則的容器標籤，用於標識應將其元資料新增至指定索引的物件。</p> <p>前綴重疊的規則將被拒絕。</p> <p>包含在 MetadataNotificationConfiguration 元素中。</p>	是的
ID	<p>規則的唯一識別碼。</p> <p>包含在 Rule 元素中。</p>	不
地位	<p>狀態可以是「啟用」或「停用」。對於已停用的規則，不會採取任何措施。</p> <p>包含在 Rule 元素中。</p>	是的
前綴	<p>與前綴相符的物件會受到規則的影響，並且其元資料會被傳送到指定的目標。</p> <p>若要符合所有對象，請指定一個空前綴。</p> <p>包含在 Rule 元素中。</p>	是的
目的地	<p>規則目標的容器標籤。</p> <p>包含在 Rule 元素中。</p>	是的

Name	描述	必需的
甕	<p>發送物件元資料的目標的 URN。必須是具有以下屬性的 StorageGRID 端點的 URN：</p> <ul style="list-style-type: none"> • `es` 必須是第三個元素。 • URN 必須以儲存元資料的索引和類型結尾，格式如下 domain-name/myindex/mytype。 <p>端點是使用租用戶管理器或租用戶管理 API 進行設定的。它們的形式如下：</p> <ul style="list-style-type: none"> • arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype • urn:mysite:es:::mydomain/myindex/mytype <p>必須在提交配置 XML 之前配置端點，否則配置將失敗並出現 404 錯誤。</p> <p>URN 包含在目標元素中。</p>	是的

2. 在租用戶管理員中選擇*儲存 (S3) * > 儲存桶。
3. 選擇來源儲存桶的名稱。

出現儲存桶詳細資訊頁面。
4. 選擇“平台服務”>“搜尋整合”
5. 選取“啟用搜尋整合”複選框。
6. 將元資料通知配置貼上到文字方塊中，然後選擇*儲存變更*。



StorageGRID 管理員必須使用 Grid Manager 或 Management API 為每個租用戶帳戶啟用平台服務。如果儲存配置 XML 時發生錯誤，請聯絡您的 StorageGRID 管理員。

7. 驗證搜尋整合服務是否配置正確：
 - a. 將符合配置 XML 中指定的觸發元資料通知要求的物件新增至來源儲存桶。

在前面顯示的範例中，新增到儲存桶的所有物件都會觸發元資料通知。
 - b. 確認包含物件元資料和標籤的 JSON 文件已新增至端點中指定的搜尋索引。

完成後

根據需要，您可以使用以下任一方法停用儲存桶的搜尋整合：

- 選擇 儲存 (S3) > 儲存桶 並清除 啟用搜尋整合 複選框。
- 如果您直接使用 S3 API，請使用 DELETE Bucket 元資料通知請求。請參閱實作 S3 用戶端應用程式的說明。

範例：適用於所有物件的元資料通知配置

在此範例中，所有物件的物件元資料都被傳送到同一個目的地。

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

範例：具有兩個規則的元資料通知配置

在此範例中，與前綴相符的物件的物件元數據 `/images` 發送到一個目的地，而與前綴匹配的對象的對象元數據 `/videos` 被送到第二個目的地。

```
<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>
```

元資料通知格式

當您為儲存桶啟用搜尋整合服務時，每次新增、更新或刪除物件元資料或標籤時都會產生 JSON 文件並將其傳送至目標端點。

此範例展示了當物件具有以下按鍵時可以產生的 JSON 範例 SGWS/Tagging.txt 在名為 test。這 test bucket 沒有版本控制，因此 versionId 標籤為空。

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

JSON 文檔中包含的字段

文件名稱包括儲存桶名稱、物件名稱和版本 ID（如果存在）。

儲存桶和物件資訊

bucket：儲存桶的名稱

key：物件鍵名

versionID：物件版本，用於版本化儲存桶中的對象

region：例如桶區域 us-east-1

系統元數據

size：HTTP 用戶端可見的物件大小（以位元組為單位）

md5：物件哈希

用戶元數據

metadata：物件的所有用戶元數據，以鍵值對的形式

key:value

標籤

tags：為物件定義的所有物件標籤，以鍵值對的形式

key:value

如何在 **Elasticsearch** 中查看結果

對於標籤和使用者元數據，StorageGRID將日期和數字作為字串或 S3 事件通知傳遞給 Elasticsearch。若要設定 Elasticsearch 將這些字串解釋為日期或數字，請按照 Elasticsearch 的動態欄位對應和對應日期格式的說明進行操作。在配置搜尋整合服務之前，請在索引上啟用動態欄位對應。文檔被索引後，您無法在索引中編輯文檔的欄位類型。

版權資訊

Copyright © 2026 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。