



使用**StorageGRID**

StorageGRID software

NetApp
May 29, 2026

目錄

使用StorageGRID租戶和客戶端	1
使用租用戶帳戶	1
使用租用戶帳戶	1
如何登入和登出	2
了解租戶管理器儀表板	6
租戶管理 API	9
使用電網聯合連接	14
管理群組和用戶	26
管理 S3 存取密鑰	43
管理 S3 儲存桶	48
管理 S3 平台服務	68
使用 S3 REST API	96
S3 REST API 支援的版本與更新	96
快速參考：支援的 S3 API 請求	99
測試 S3 REST API 配置	118
StorageGRID如何實作 S3 REST API	119
支援 Amazon S3 REST API	132
StorageGRID自訂操作	177
儲存桶和群組存取策略	196
審計日誌中追蹤的 S3 操作	220
使用 Swift REST API (生命週期結束)	221
使用 Swift REST API	221

使用StorageGRID租戶和客戶端

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](#)"攝取和管理物件。

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：

Sign in with your organizational account

someone@example.com

Password

Sign in

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。

NetApp StorageGRID®

Tenant Manager

Recent

S3 tenant ▼

Account

62984032838045582045

Sign in

NetApp support | NetApp.com

- 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。

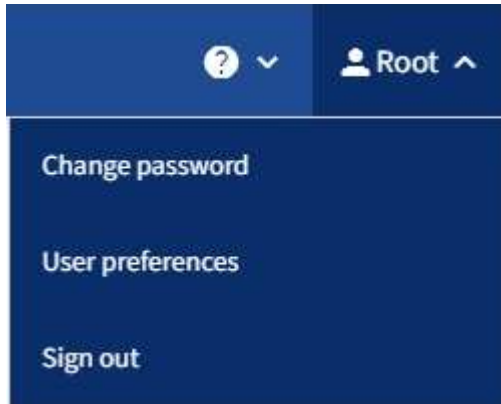
退出租戶管理器

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

如果在網絡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

Example Value Model

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

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-Csrftoken` 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

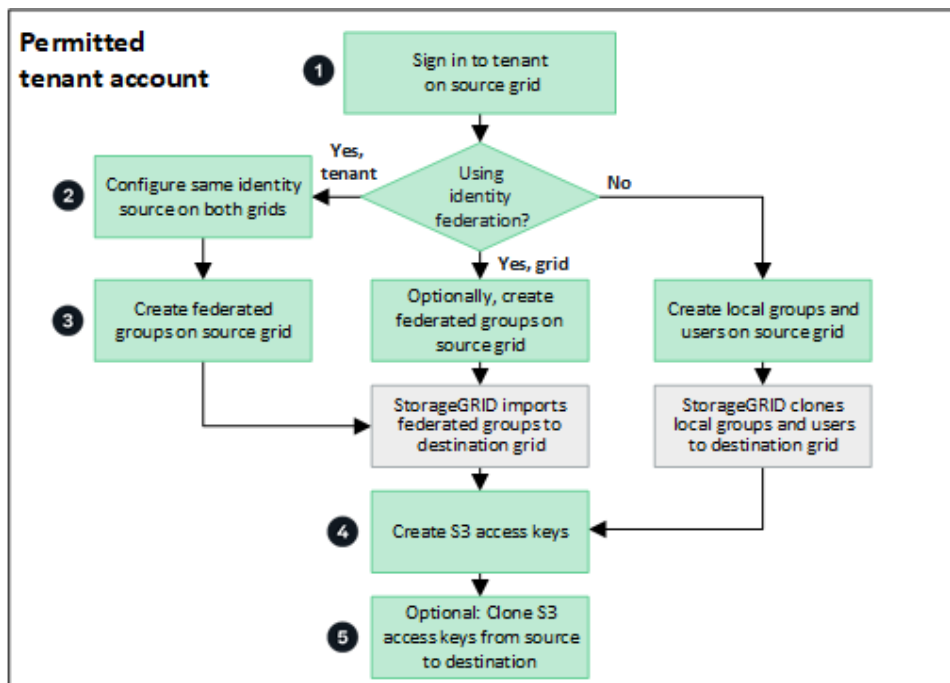
如果建立或編輯租用戶以使用網格聯合連接，則該租用戶將從一個StorageGRID系統（來源租用戶）複製到另一個StorageGRID系統（副本租用戶）。複製租用戶後，新增至來源租用戶的任何群組和使用者都會複製到副本租用戶。

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"](#)。

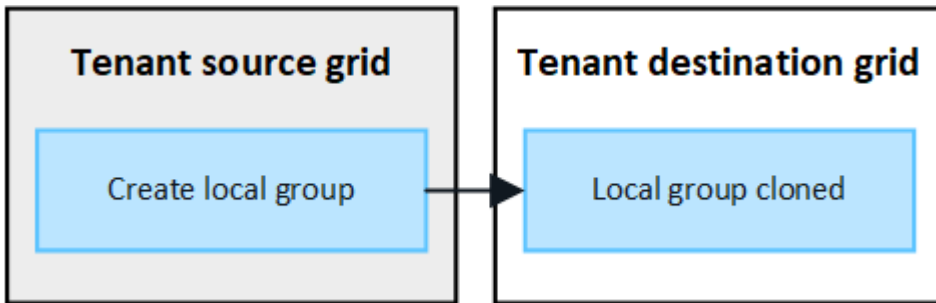
如何複製群組、使用者和 S3 存取金鑰？

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"](#)。

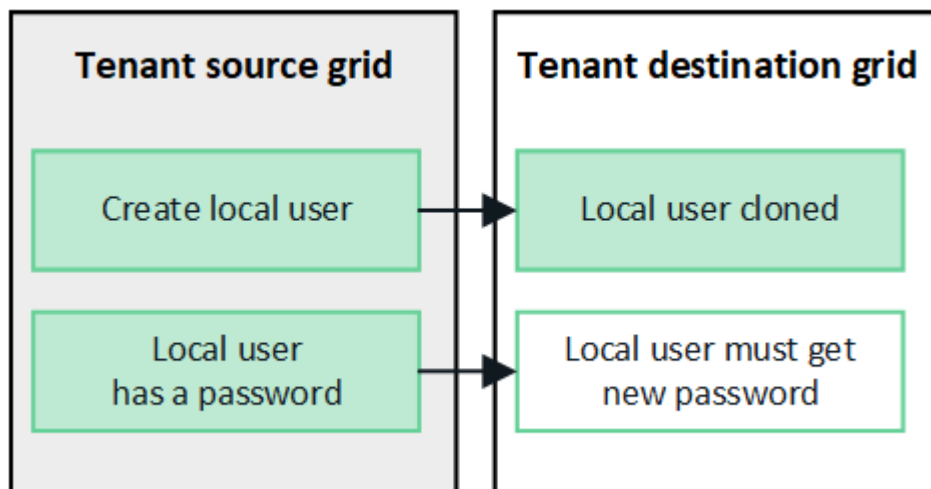


將群組複製到目標網格時，不會包括在來源網格上建立本機群組時選擇的任何使用者。因此，在創建群組時不要選擇使用者。相反，在建立使用者時選擇群組。

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"](#)。

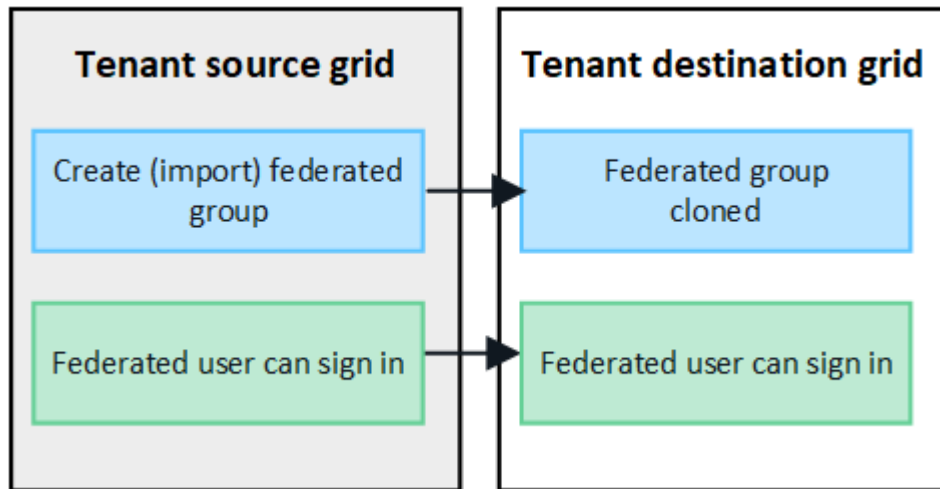


克隆在來源網格上建立的聯合組

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。

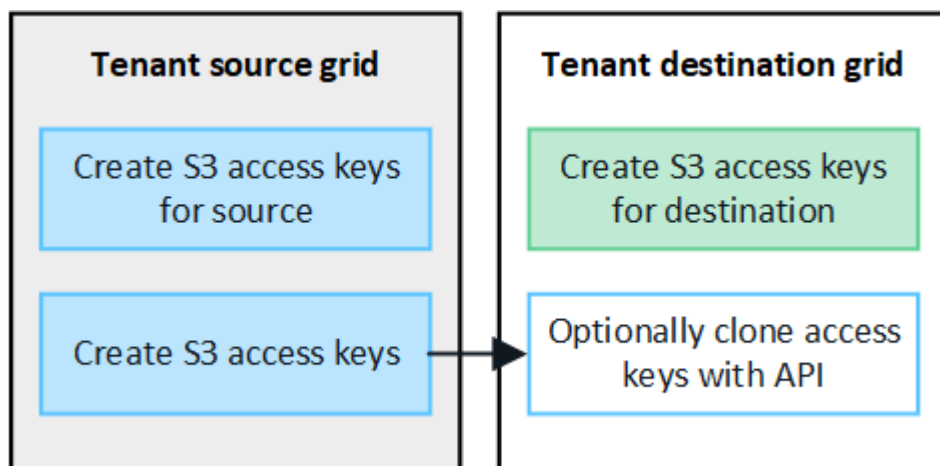


S3 存取密鑰可以手動克隆

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：

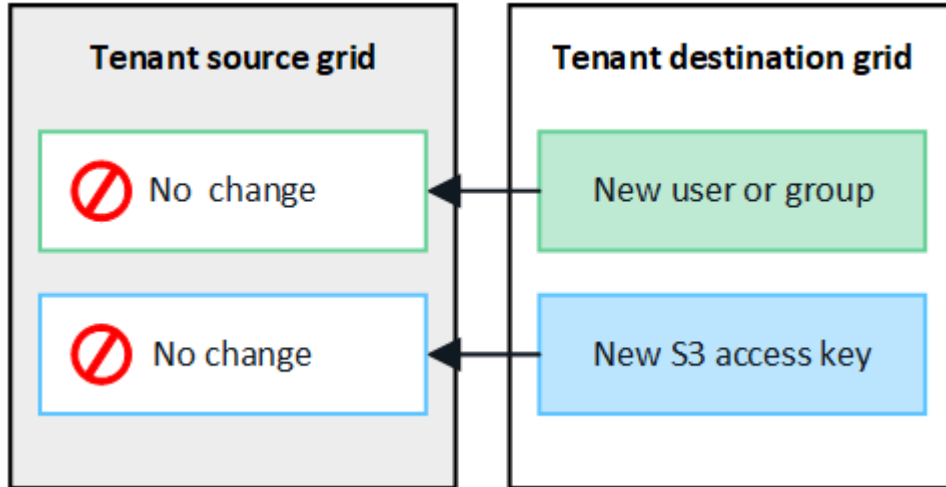
- 如果你不需要對每個網格使用相同的鍵，你可以"建立您自己的存取金鑰"或者"建立另一個使用者的存取金鑰"在每個網格上。
- 如果需要在兩個網格上使用相同的金鑰，則可以在來源網格上建立金鑰，然後使用租用戶管理員 API 手動"克隆密鑰"到目的地格。



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

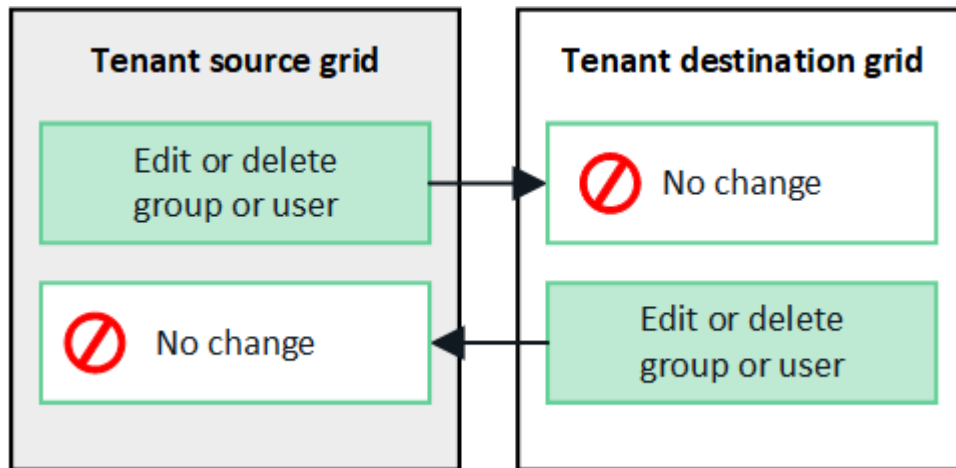
克隆僅從租戶的來源網格發生到租戶的目標網格。如果您在租用戶的目標網格上建立或匯入群組和用戶，StorageGRID將不會將這些項目複製回租戶的來源網格。



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。

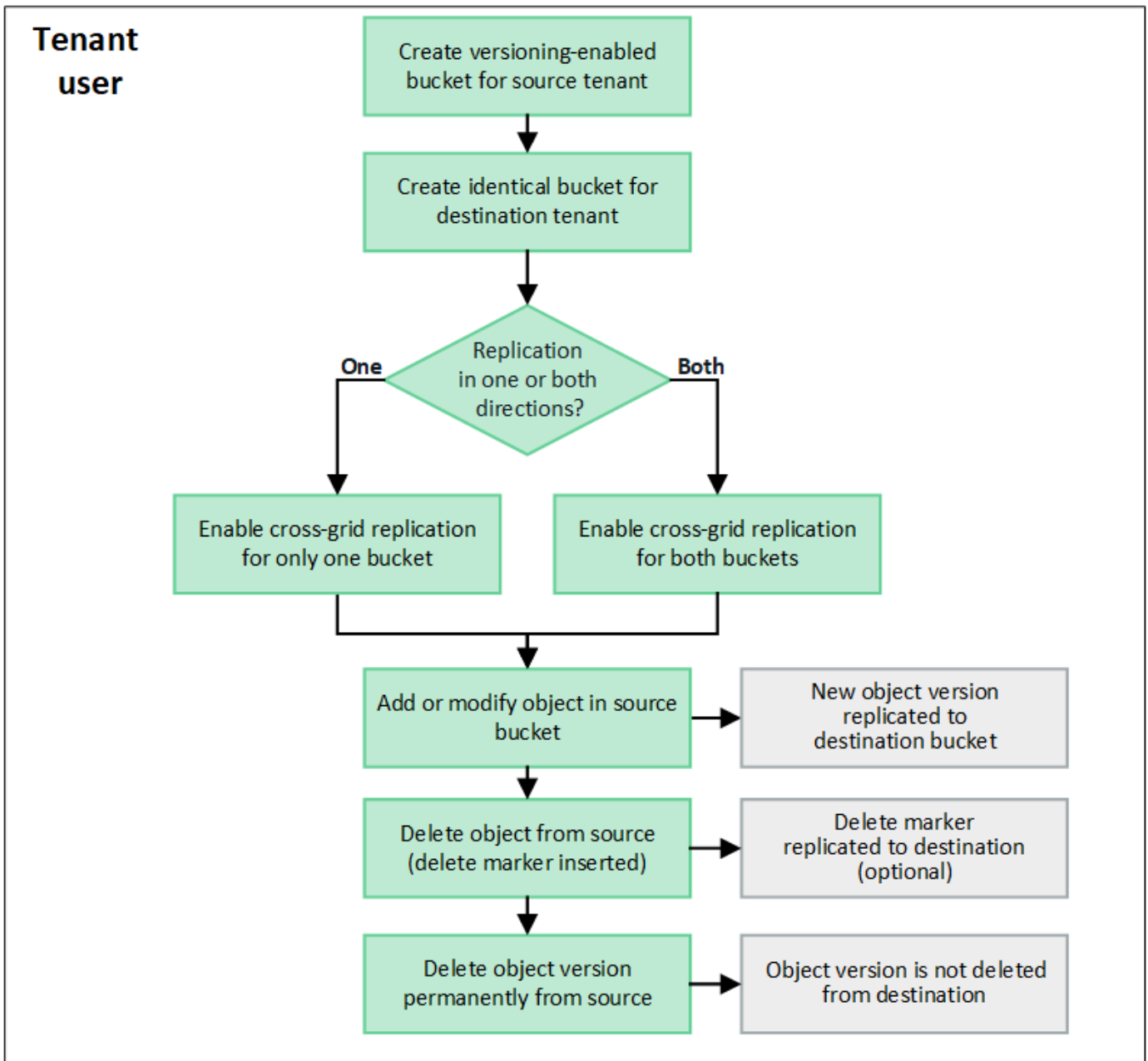
確保保留字串周圍的雙引號。
8. 如果金鑰即將過期，請將 **expires** 的範例條目替換為 ISO 8601 資料時間格式的過期日期和時間字串（例如，2023-02-28T22:46:33-08:00）。如果金鑰不會過期，請輸入 **null** 作為 **expires** 條目的值（或刪除 **Expires** 行和前面的逗號）。
9. 選擇*執行*。
10. 確認伺服器回應代碼為*204*，表示金鑰已成功複製到目標網格。

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在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。

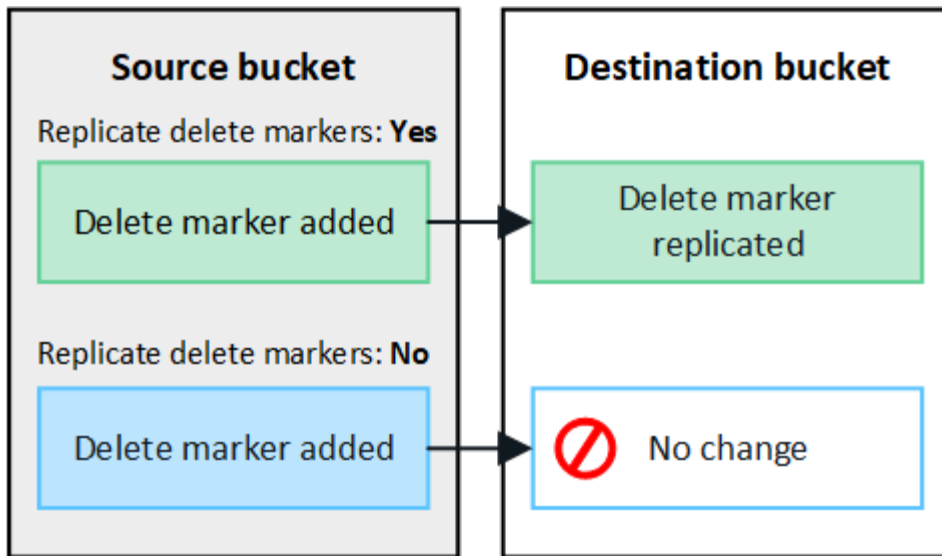
d. 選擇*跨網格複製*標籤。

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` 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的身份聯合。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

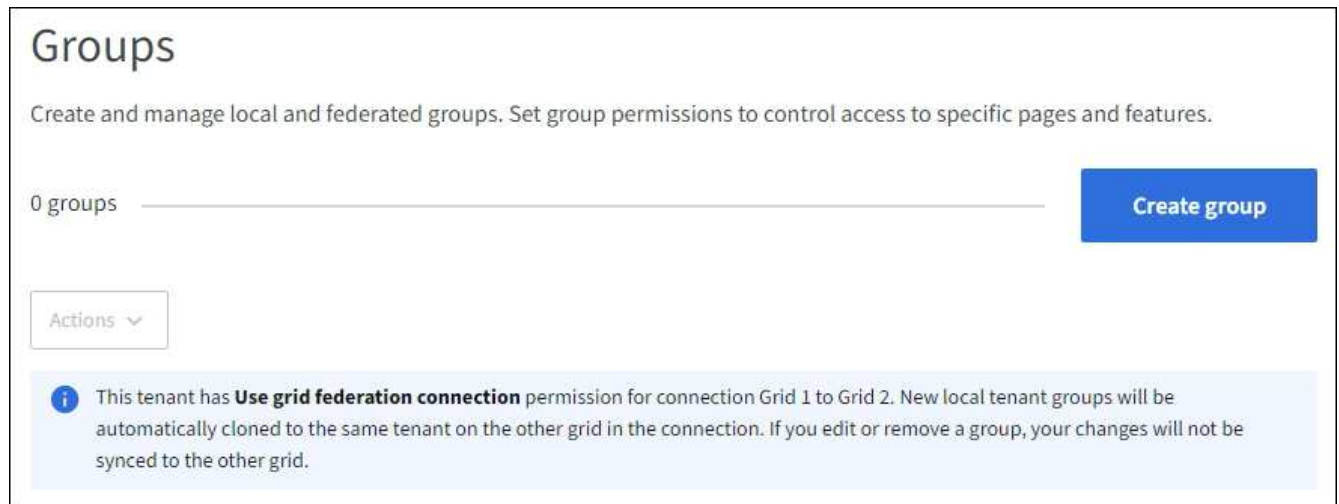
- 您已使用"[支援的網頁瀏覽器](#)"。
- 您屬於具有"[Root存取權限](#)"。
- 如果您計劃匯入聯合群組，則必須"[配置身份聯合](#)"，且聯合群組已存在於配置的身份來源中。
- 如果您的租用戶帳戶具有「使用網格聯合連線」權限，則您已查看了下列工作流程和注意事項：["克隆租戶群組和用戶"](#)，您已登入租戶的來源網格。

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。

- 為此群組選擇一個或多個權限。

看"[租用用戶管理權限](#)"。

- 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

- 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。

- 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](#)"。

- 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。
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。

允許	描述	細節
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

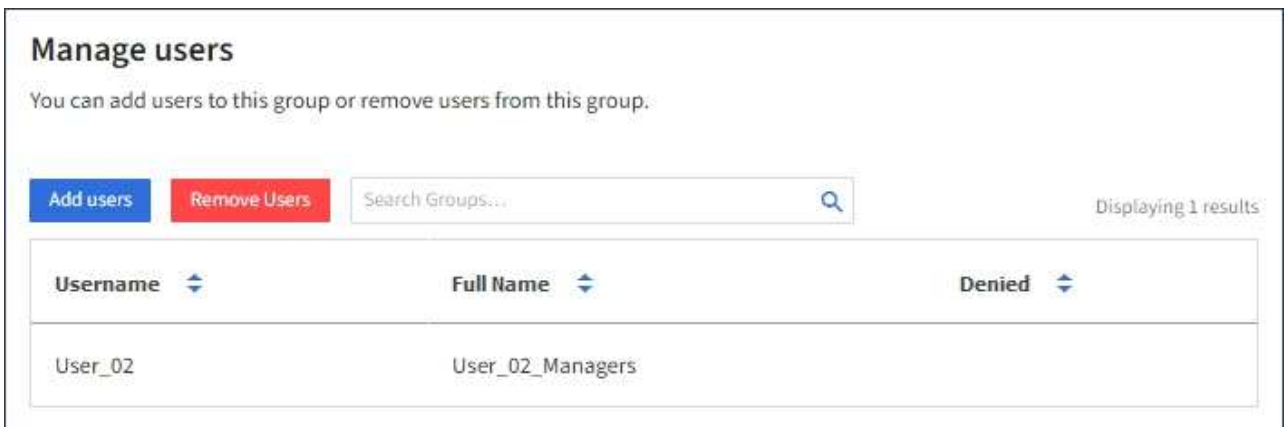
1. 選擇*存取管理* > 群組。
2. 查看「群組」頁面上提供的信息，其中列出了此租用戶帳戶的所有本機群組和聯合群組的基本資訊。

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
 - 如果租用用戶帳戶具有 使用網格聯合連線 權限且您正在查看租用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 租用用戶建立群組](#)"和"[為 Swift 租用用戶建立群組](#)"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。

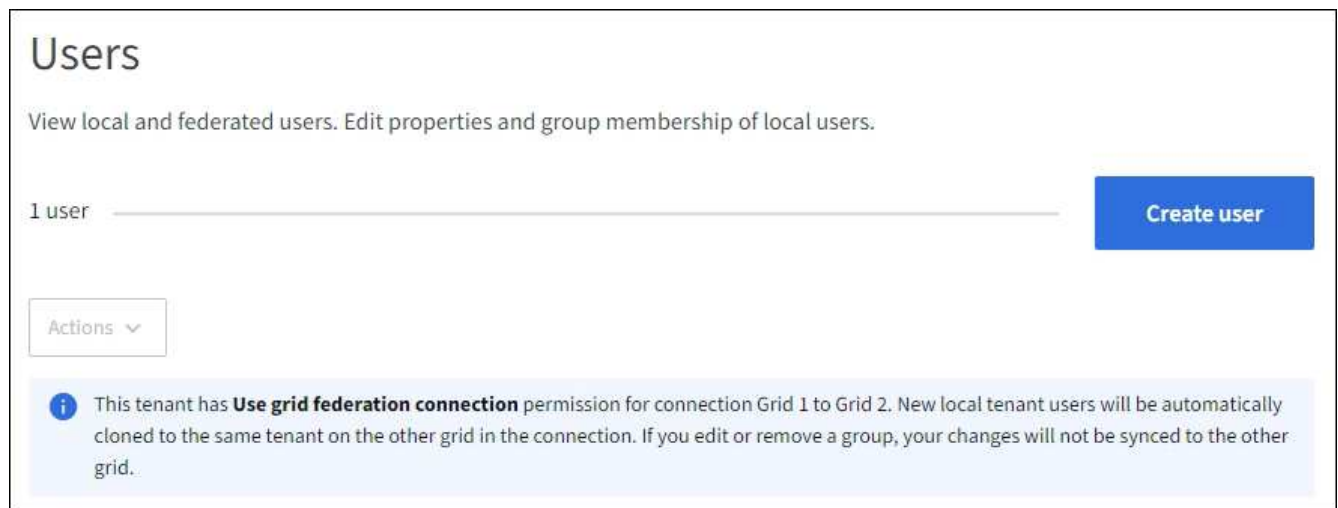
不屬於任何群組的 Swift 使用者沒有管理權限或 Swift 容器存取權限。

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。

場地	描述
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*使用網絡聯合連線*權限，則當目標網絡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*使用網絡聯合連線*權限且您位於租用戶的來源網絡上，則新的本機使用者將被複製到租用戶的目標網絡。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 使用網絡聯合連線 權限，且您正在查看租用戶來源網絡上的使用者：

- 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絡。
- 根據需要，橫幅訊息會指示使用者是否未複製到目標網絡上的租戶。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
 - 如果租用戶帳戶具有 使用網格聯合連線 權限且您正在租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用戶，則重複的用戶將被複製到租用戶的目標網格。

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：

- 為您的金鑰設定期間，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，則不必為金鑰設定期間。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。

- 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。

- 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。

- 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

- 選擇*存取管理* > 使用者。
- 在「使用者」頁面中，選擇您想要查看其 S3 存取金鑰的使用者。
- 從使用者詳細資料頁面中，選擇*存取金鑰*。
- 依*到期時間*或*存取金鑰ID*對金鑰進行排序。
- 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用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. 從儀表板中選擇 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。
 - ["管理存儲桶一致性"](#)
 - ["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定時間段後刪除資料。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。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。只有當您的網絡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](#)"。

管理儲存桶一致性

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*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

以下針對網絡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。

網絡管理員

- 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**」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。

預設保留模式	描述
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

- 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)

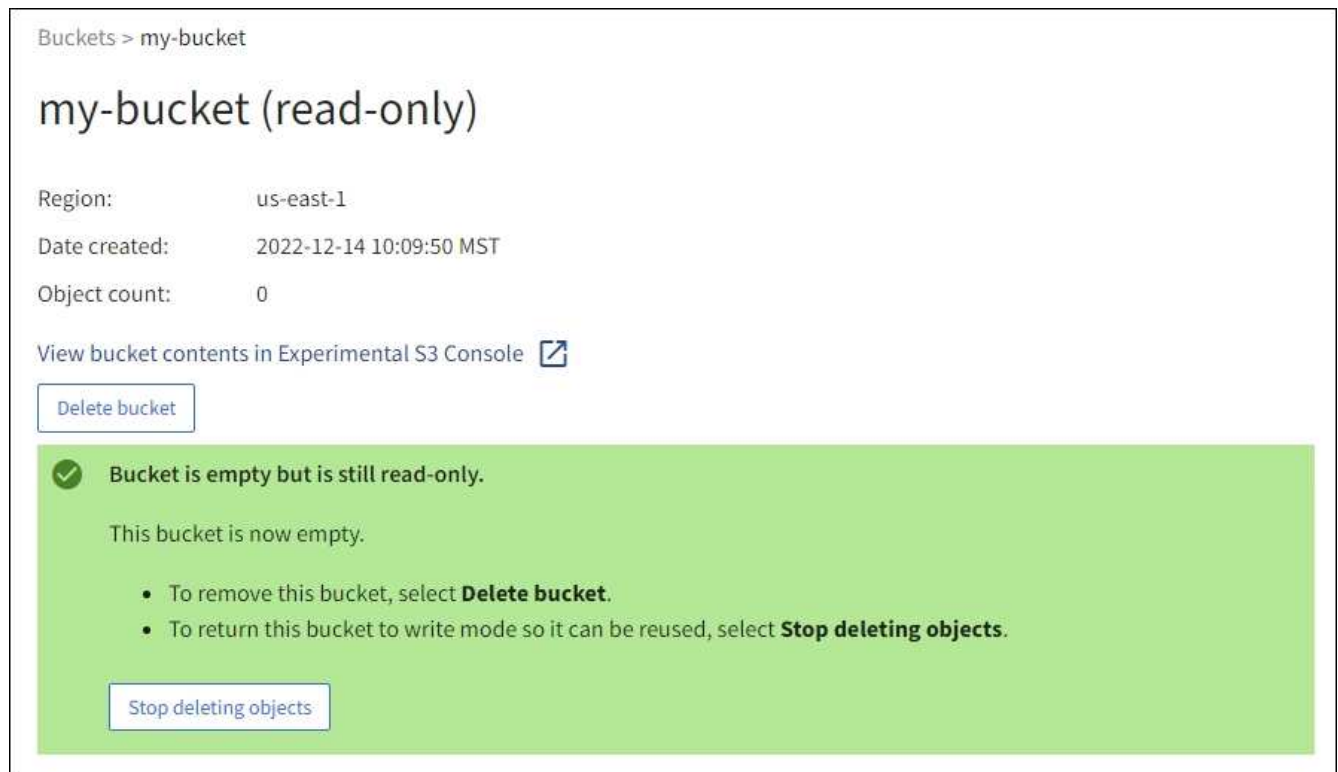
Stop deleting objects

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"](#)。

平台服務概覽

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。

考慮	細節
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。您也可以在未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:mystore: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:mystore:sns:optional:optional:sns-topic-name
```

指定 Kafka 端點：

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

- 搜尋整合：

```
urn:mystore: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。

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，請聯絡網格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。

使用 **S3 REST API**

S3 REST API 支援的版本與更新

StorageGRID支援簡單儲存服務 (S3) API，該 API 作為一組表述性狀態轉移 (REST) Web 服務實作。

對 S3 REST API 的支援可讓您將為 S3 Web 服務開發的服務導向的應用程式與使用StorageGRID系統的內部部署物件儲存連接起來。只需對客戶端應用程式目前使用的 S3 REST API 呼叫進行最少的更改。

支援的版本

StorageGRID支援以下特定版本的 S3 和 HTTP。

物品	版本
S3 API 規範	"Amazon Web Services (AWS) 文件：Amazon Simple Storage Service API 參考"
HTTP	1.1 有關 HTTP 的更多信息，請參閱 HTTP/1.1 (RFC 7230-35)。 "IETF RFC 2616：超文本傳輸協定 (HTTP/1.1) " 注意：StorageGRID不支援 HTTP/1.1 管線。

對 **S3 REST API** 支援的更新

發布	評論
11.9	<ul style="list-style-type: none"> • 增加了對以下請求和支援的標頭的預先計算的 SHA-256 校驗和值的支援。您可以使用此功能來驗證已上傳物件的完整性： <ul style="list-style-type: none"> ◦ 完成分段上傳： <code>x-amz-checksum-sha256</code> ◦ 建立多部分上傳： <code>x-amz-checksum-algorithm</code> ◦ 取得對象： <code>x-amz-checksum-mode</code> ◦ 頭部對象： <code>x-amz-checksum-mode</code> ◦ 列出零件 ◦ 放置對象： <code>x-amz-checksum-sha256</code> ◦ 上傳部分： <code>x-amz-checksum-sha256</code> • 增加了網格管理員控制租戶級保留和合規性設定的能力。這些設定會影響 S3 物件鎖定設定。 <ul style="list-style-type: none"> ◦ 儲存桶預設保留模式和物件保留模式：治理或合規（如果網格管理員允許）。 ◦ 儲存桶預設保留期和物件保留截止日期：必須小於或等於網格管理員設定的最大保留期所允許的值。 • 改進了對 <code>`aws-chunked`</code> 內容編碼和串流媒體 <code>`x-amz-content-sha256`</code> 值。限制： <ul style="list-style-type: none"> ◦ 如果存在，<code>`chunk-signature`</code> 是可選的，並且未經驗證 ◦ 如果存在，<code>`x-amz-trailer`</code> 內容被忽略
11.8	<p>更新了 S3 操作的名稱，以匹配 "Amazon Web Services (AWS) 文件：Amazon Simple Storage Service API 參考"。</p>
11.7	<ul style="list-style-type: none"> • 額外"快速參考：支援的 S3 API 請求"。 • 增加了對使用 GOVERNANCE 模式和 S3 物件鎖的支援。 • 增加了對StorageGRID特定的支持 <code>`x-ntap-sg-cgr-replication-status`</code> GET Object 和 HEAD Object 請求的回應頭。此標頭提供跨網格複製的物件複製狀態。 • SelectObjectContent 請求現在支援 Parquet 物件。
11.6	<ul style="list-style-type: none"> • 增加了對使用 <code>`partNumber`</code> GET Object 和 HEAD Object 請求中的請求參數。 • 增加了對 S3 物件鎖的儲存桶層級的預設保留模式和預設保留期的支援。 • 增加了對 <code>`s3:object-lock-remaining-retention-days`</code> 策略條件鍵來設定物件允許的保留期範圍。 • 將單一 PUT 物件操作的最大 <code>建議</code> 大小變更為 5 GiB (5,368,709,120 位元組)。 如果您的物件大於 5 GiB，請改用分段上傳。

發布	評論
11.5	<ul style="list-style-type: none"> • 增加了對管理儲存桶加密的支援。 • 增加了對 S3 物件鎖定的支援並棄用了舊版合規性請求。 • 增加了在版本化儲存桶上使用 DELETE 多個物件的支援。 • 這 `Content-MD5` 請求標頭現在已正確支援。
11.4	<ul style="list-style-type: none"> • 增加了對 DELETE Bucket 標記、GET Bucket 標記和 PUT Bucket 標記的支援。不支援成本分配標籤。 • 對於在StorageGRID 11.4 中建立的儲存桶，不再需要限制物件鍵名稱以滿足效能最佳實務。 • 增加了對 bucket 通知的支持 `s3:ObjectRestore:Post` 事件類型。 • AWS 現已強制執行多部分物件的大小限制。分段上傳中的每個部分必須介於 5 MiB 和 5 GiB 之間。最後一部分可以小於 5 MiB。 • 增加了對 TLS 1.3 的支持
11.3	<ul style="list-style-type: none"> • 增加了使用客戶提供的金鑰 (SSE-C) 對物件資料進行伺服器端加密的支援。 • 增加了對 DELETE、GET 和 PUT Bucket 生命週期操作 (僅限到期操作) 的支持，以及 `x-amz-expiration` 響應頭。 • 更新了 PUT 物件、PUT 物件 - 複製和分段上傳，以描述在攝取時使用同步放置的 ILM 規則的影響。 • TLS 1.1 密碼不再支援。
11.2	<p>增加了對用於雲端儲存池的 POST 物件還原的支援。增加了在群組和儲存桶策略中使用 ARN、策略條件鍵和策略變數的 AWS 語法的支援。使用StorageGRID語法的現有群組和儲存桶策略將繼續受到支援。</p> <p>*注意：*其他配置 JSON/XML 中 ARN/URN 的使用 (包括自訂StorageGRID功能中使用的 ARN/URN 的使用) 沒有改變。</p>
11.1	<p>增加了對跨網域資源共享 (CORS)、S3 用戶端連接到網格節點的 HTTP 以及儲存桶上的合規性設定的支援。</p>
11.0	<p>增加了對儲存桶配置平台服務 (CloudMirror 複製、通知和 Elasticsearch 搜尋整合) 的支援。還增加了對儲存桶的物件標記位置約束以及可用一致性的支援。</p>
10.4	<p>增加了對 ILM 掃描版本控制變更、端點網域名稱頁面更新、策略中的條件和變數、策略範例以及 PutOverwriteObject 權限的支援。</p>
10.3	<p>增加了對版本控制的支援。</p>
10.2	<p>增加了對群組和儲存桶存取策略以及分段複製 (上傳部分 - 複製) 的支援。</p>

發布	評論
10.1	增加了對分段上傳、虛擬託管式請求和 v4 身份驗證的支援。
10.0	StorageGRID系統初步支援 S3 REST API。目前支援的《簡單儲存服務 API 參考》版本是 2006-03-01。

快速參考：支援的 **S3 API** 請求

本頁總結了StorageGRID如何支援 Amazon Simple Storage Service (S3) API。

此頁僅包含StorageGRID支援的 S3 操作。



若要查看每個操作的 AWS 文檔，請選擇標題中的連結。

通用 **URI** 查詢參數和請求標頭

除非另有說明，否則支援以下常見 URI 查詢參數：

- `versionId`（根據物件操作的需要）

除非另有說明，否則支援以下常見請求標頭：

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

相關資訊

- ["S3 REST API 實作細節"](#)
- ["Amazon Simple Storage Service API 參考：常見請求標頭"](#)

"中止分段上傳"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求，加上以下附加 URI 查詢參數：

- `uploadId`

請求正文
沒有任何

StorageGRID文檔

["分段上傳的操作"](#)

["完成多部分上傳"](#)

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求，加上以下附加 URI 查詢參數：

- uploadId
- x-amz-checksum-sha256

請求主體 XML 標籤

StorageGRID支援以下請求正文 XML 標籤：

- ChecksumSHA256
- CompleteMultipartUpload
- ETag
- Part
- PartNumber

StorageGRID文檔

["完成多部分上傳"](#)

["複製對象"](#)

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求，加上以下附加標頭：

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

- x-amz-object-lock-retain-until-date
- x-amz-server-side-encryption
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-storage-class
- x-amz-tagging
- x-amz-tagging-directive
- x-amz-meta-`<metadata-name>`

請求正文

沒有任何

StorageGRID文檔

["複製對象"](#)

["創建桶"](#)

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求，加上以下附加標頭：

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

請求正文

StorageGRID支援實作時由 Amazon S3 REST API 定義的所有請求正文參數。

StorageGRID文檔

["對 bucket 的操作"](#)

["建立多部分上傳"](#)

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求，加上以下附加標頭：

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- x-amz-checksum-algorithm
- x-amz-server-side-encryption
- x-amz-storage-class

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

請求正文

沒有任何

StorageGRID文檔

["建立多部分上傳"](#)

["刪除桶"](#)

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求。

StorageGRID文檔

["對 bucket 的操作"](#)

["刪除BucketCors"](#)

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求。

請求正文

沒有任何

StorageGRID文檔

["對 bucket 的操作"](#)

["刪除桶加密"](#)

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求。

請求正文

沒有任何

StorageGRID文檔

["對 bucket 的操作"](#)

"DeleteBucket生命週期"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求。

請求正文

沒有任何

StorageGRID文檔

- ["對 bucket 的操作"](#)
- ["建立 S3 生命週期配置"](#)

"刪除桶策略"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求。

請求正文

沒有任何

StorageGRID文檔

["對 bucket 的操作"](#)

"刪除桶複製"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求。

請求正文

沒有任何

StorageGRID文檔

["對 bucket 的操作"](#)

"刪除桶標記"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求。

請求正文

沒有任何

StorageGRID文檔

["對 bucket 的操作"](#)

"刪除對象"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求，加上以下附加請求標頭：

- x-amz-bypass-governance-retention

請求正文

沒有任何

StorageGRID文檔

["對物件的操作"](#)

"刪除對象"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求，加上以下附加請求標頭：

- x-amz-bypass-governance-retention

請求正文

StorageGRID支援實作時由 Amazon S3 REST API 定義的所有請求正文參數。

StorageGRID文檔

["對物件的操作"](#)

"刪除物件標記"

StorageGRID支援所有[通用參數和標頭](#)對於此請求。

請求正文

沒有任何

StorageGRID文檔

["對物件的操作"](#)

"獲取BucketAcl"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求。

請求正文

沒有任何

StorageGRID文檔

["對 bucket 的操作"](#)

"獲取BucketCors"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求。

請求正文

沒有任何

StorageGRID文檔

["對 bucket 的操作"](#)

"取得桶加密"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求。

請求正文

沒有任何

StorageGRID文檔

["對 bucket 的操作"](#)

"取得BucketLifecycleConfiguration"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求。

請求正文

沒有任何

StorageGRID文檔

- ["對 bucket 的操作"](#)
- ["建立 S3 生命週期配置"](#)

"取得儲存桶位置"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求。

請求正文

沒有任何

StorageGRID文檔

["對 bucket 的操作"](#)

"取得儲存桶通知配置"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求。

請求正文

沒有任何

StorageGRID文檔

["對 bucket 的操作"](#)

"取得BucketPolicy"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求。

請求正文

沒有任何

StorageGRID文檔

["對 bucket 的操作"](#)

"獲取Bucket複製"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求。

請求正文

沒有任何

StorageGRID文檔

["對 bucket 的操作"](#)

"取得桶標記"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求。

請求正文

沒有任何

StorageGRID文檔

["對 bucket 的操作"](#)

"取得Bucket版本"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求。

請求正文

沒有任何

StorageGRID文檔

["對 bucket 的操作"](#)

["取得對象"](#)

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求，加上以下附加 URI 查詢參數：

- x-amz-checksum-mode
- partNumber
- response-cache-control
- response-content-disposition
- response-content-encoding
- response-content-language
- response-content-type
- response-expires

以及這些額外的請求標頭：

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

請求正文

沒有任何

StorageGRID文檔

["取得對象"](#)

["取得對象Acl"](#)

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求。

請求正文
沒有任何

StorageGRID文檔

["對物件的操作"](#)

["獲取對象合法持有"](#)

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求。

請求正文
沒有任何

StorageGRID文檔

["使用 S3 REST API 設定 S3 物件鎖"](#)

["取得物件鎖配置"](#)

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求。

請求正文
沒有任何

StorageGRID文檔

["使用 S3 REST API 設定 S3 物件鎖"](#)

["取得對象保留"](#)

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求。

請求正文
沒有任何

StorageGRID文檔

["使用 S3 REST API 設定 S3 物件鎖"](#)

["取得物件標記"](#)

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求。

請求正文
沒有任何

StorageGRID文檔

"對物件的操作"

"頭桶"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求。

請求正文

沒有任何

StorageGRID文檔

["對 bucket 的操作"](#)

"頭部對象"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求，加上以下附加標頭：

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

請求正文

沒有任何

StorageGRID文檔

["頭部對象"](#)

"列表桶"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求。

請求正文

沒有任何

StorageGRID文檔

[服務上的操作](#) › [ListBuckets](#)

"列出多部分上傳"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求，加上以下附加參數：

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

請求正文

沒有任何

StorageGRID文檔

"列出多部分上傳"

"清單對象"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求，加上以下附加參數：

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

請求正文

沒有任何

StorageGRID文檔

"對 bucket 的操作"

"ListObjectsV2"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求，加上以下附加參數：

- continuation-token
- delimiter
- encoding-type
- fetch-owner

- max-keys
- prefix
- start-after

請求正文

沒有任何

StorageGRID文檔

["對 bucket 的操作"](#)

["列出物件版本"](#)

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求，加上以下附加參數：

- delimiter
- encoding-type
- key-marker
- max-keys
- prefix
- version-id-marker

請求正文

沒有任何

StorageGRID文檔

["對 bucket 的操作"](#)

["列出零件"](#)

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求，加上以下附加參數：

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

請求正文

沒有任何

StorageGRID文檔

["列出多部分上傳"](#)

"PutBucketCors"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求。

請求正文

StorageGRID支援實作時由 Amazon S3 REST API 定義的所有請求正文參數。

StorageGRID文檔

["對 bucket 的操作"](#)

"PutBucket加密"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求。

請求主體 XML 標籤

StorageGRID支援以下請求正文 XML 標籤：

- ApplyServerSideEncryptionByDefault
- Rule
- ServerSideEncryptionConfiguration
- SSEAlgorithm

StorageGRID文檔

["對 bucket 的操作"](#)

"PutBucket生命週期配置"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求。

請求主體 XML 標籤

StorageGRID支援以下請求正文 XML 標籤：

- And
- Days
- Expiration
- ExpiredObjectDeleteMarker
- Filter
- ID
- Key
- LifecycleConfiguration
- NewerNoncurrentVersions

- NoncurrentDays
- NoncurrentVersionExpiration
- Prefix
- Rule
- Status
- Tag
- Value

StorageGRID文檔

- ["對 bucket 的操作"](#)
- ["建立 S3 生命週期配置"](#)

"PutBucketNotification配置"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求。

請求主體 XML 標籤

StorageGRID支援以下請求正文 XML 標籤：

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

StorageGRID文檔

["對 bucket 的操作"](#)

"PutBucketPolicy"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求。

請求正文

有關支援的 JSON 主體欄位的詳細信息，請參閱["使用儲存桶和群組存取策略"](#)。

"PutBucket複製"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求。

請求主體 **XML** 標籤

- Bucket
- Destination
- Prefix
- ReplicationConfiguration
- Rule
- Status
- StorageClass

StorageGRID文檔

["對 bucket 的操作"](#)

"PutBucketTagging"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求。

請求正文

StorageGRID支援實作時由 Amazon S3 REST API 定義的所有請求正文參數。

StorageGRID文檔

["對 bucket 的操作"](#)

"PutBucket版本控制"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求。

請求主體參數

StorageGRID支援以下請求正文參數：

- VersioningConfiguration
- Status

StorageGRID文檔

["對 bucket 的操作"](#)

"放置對象"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求，加上以下附加標頭：

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- x-amz-checksum-sha256
- x-amz-server-side-encryption
- x-amz-storage-class
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-tagging
- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-object-lock-legal-hold
- x-amz-meta-`<metadata-name>`

請求正文

- 物件的二進位數據

StorageGRID文檔

"放置對象"

"放置對象合法保留"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求。

請求正文

StorageGRID支援實作時由 Amazon S3 REST API 定義的所有請求正文參數。

StorageGRID文檔

"使用 S3 REST API 設定 S3 物件鎖"

"PutObjectLock配置"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求。

請求正文

StorageGRID支援實作時由 Amazon S3 REST API 定義的所有請求正文參數。

StorageGRID文檔

["使用 S3 REST API 設定 S3 物件鎖"](#)

"PutObjectRetention"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求，加上以下附加標頭：

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

請求正文

StorageGRID支援實作時由 Amazon S3 REST API 定義的所有請求正文參數。

StorageGRID文檔

["使用 S3 REST API 設定 S3 物件鎖"](#)

"PutObjectTagging"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求。

請求正文

StorageGRID支援實作時由 Amazon S3 REST API 定義的所有請求正文參數。

StorageGRID文檔

["對物件的操作"](#)

"復原對象"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求。

請求正文

有關支援的主體欄位的詳細信息，請參閱["復原對象"](#)。

"選擇對象內容"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求。

請求正文

有關支援的主體欄位的詳細信息，請參閱以下內容：

- ["使用 S3 Select"](#)
- ["選擇對象內容"](#)

"上傳部分"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求，加上以下附加 URI 查詢參數：

- partNumber
- uploadId

以及這些額外的請求標頭：

- x-amz-checksum-sha256
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5

請求正文

- 該部分的二進位數據

StorageGRID文檔

"上傳部分"

"上傳部分複製"

URI 查詢參數和請求標頭

StorageGRID支援所有[通用參數和標頭](#)對於此請求，加上以下附加 URI 查詢參數：

- partNumber
- uploadId

以及這些額外的請求標頭：

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

- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-copy-source-server-side-encryption-customer-algorithm
- x-amz-copy-source-server-side-encryption-customer-key
- x-amz-copy-source-server-side-encryption-customer-key-MD5

請求正文

沒有任何

StorageGRID文檔

["上傳部分複製"](#)

測試 S3 REST API 配置

您可以使用 Amazon Web Services 命令列介面 (AWS CLI) 測試與系統的連線並驗證您是否可以讀取和寫入物件。

開始之前

- 您已從 ["aws.amazon.com/cli"](https://aws.amazon.com/cli)。
- 或者，你有["建立負載平衡器端點"](#)。否則，您知道要連接的儲存節點的 IP 位址和要使用的連接埠號碼。看["用戶端連接的 IP 位址和連接埠"](#)。
- 你有["建立了 S3 租用戶帳戶"](#)。
- 您已登入租戶，並且["建立了存取密鑰"](#)。

有關這些步驟的詳細信息，請參閱["設定客戶端連接"](#)。

步驟

1. 設定 AWS CLI 設定以使用您在StorageGRID系統中建立的帳戶：
 - a. 進入配置模式：`aws configure`
 - b. 輸入您建立的帳戶的存取金鑰 ID。
 - c. 輸入您建立的帳戶的秘密存取金鑰。
 - d. 輸入要使用的預設區域。例如，`us-east-1`。
 - e. 輸入要使用的預設輸出格式，或按 **Enter** 選擇 JSON。
2. 建立一個儲存桶。

此範例假設您配置了負載平衡器端點以使用 IP 位址 10.96.101.17 和連接埠 10443。

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

如果 bucket 建立成功，則傳回 bucket 的位置，如下例所示：

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

3. 上傳對象。

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

如果物件上傳成功，則會傳回一個 Etag，它是物件資料的雜湊值。

4. 列出儲存桶的內容以驗證物件是否已上傳。

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

5. 刪除對象。

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

6. 刪除儲存桶。

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

StorageGRID如何實作 S3 REST API

客戶端請求衝突

衝突的客戶端請求（例如兩個客戶端寫入同一個金鑰）將根據「最新勝利」的原則解決。

「最新勝利」評估的時間取決於StorageGRID系統完成給定請求的時間，而不是 S3 用戶端開始操作的時間。

一致性值

一致性在物件的可用性和不同儲存節點和站點之間的物件的一致性之間提供了平衡。您可以根據應用程式的需要更改一致性。

預設情況下，StorageGRID保證新建立物件的讀寫一致性。成功完成 PUT 之後的任何 GET 都將能夠讀取新寫入的資料。現有物件的覆蓋、元資料更新和刪除最終是一致的。覆蓋通常需要幾秒鐘或幾分鐘才能傳播，但可能需要長達 15 天。

如果要以不同的一致性執行物件操作，您可以：

- 指定一致性**每個桶**。
- 指定一致性**每個 API 操作**。
- 透過執行下列任務之一來變更預設的網格範圍一致性：
 - 在網格管理員中，前往*配置* > 系統 > 儲存設定 > 預設一致性。
 - 。



對網格範圍一致性的變更僅適用於變更設定後建立的儲存桶。要確定更改的詳細信息，請參閱位於 `/var/local/log`（搜尋*consistencyLevel*）。

一致性值

一致性會影響StorageGRID用於追蹤物件的元資料在節點之間的分佈方式，進而影響物件對於客戶端請求的可用性。

您可以將儲存桶或 API 操作的一致性設定為下列值之一：

- **全部**：所有節點立即接收數據，否則請求失敗。
- **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。

使用“新寫後讀”和“可用”一致性

當 HEAD 或 GET 操作使用「新寫後讀取」一致性時，StorageGRID會分多個步驟執行查找，如下所示：

- 它首先使用低一致性來查找物件。
- 如果查找失敗，它會在下一個一致性值處重複查找，直到達到與強全域行為相當的一致性。

如果 HEAD 或 GET 操作使用「Read-after-new-write」一致性但物件不存在，則物件尋找將始終達到與強全域行為等效的一致性。由於這種一致性要求每個網站都有物件元資料的多個副本，因此如果同一網站上有兩個或多個儲存節點不可用，您可能會收到大量 500 內部伺服器錯誤。

除非您需要類似於 Amazon S3 的一致性保證，否則您可以透過將一致性設為「可用」來防止 HEAD 和 GET 操作出現這些錯誤。當 HEAD 或 GET 操作使用「可用」一致性時，StorageGRID僅提供最終一致性。它不會在增加一致性時重試失敗的操作，因此它不需要提供物件元資料的多個副本。

指定 API 操作的一致性

若要為單一 API 操作設定一致性，該操作必須支援一致性值，並且必須在請求標頭中指定一致性。此範例將 GetObject 操作的一致性設定為「Strong-site」。

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



您必須對 PutObject 和 GetObject 操作使用相同的一致性。

指定 bucket 的一致性

若要設定儲存桶的一致性，您可以使用StorageGRID"PUT桶一致性"要求。或者您可以"改變桶的一致性"來自租戶經理。

設定儲存桶的一致性時，請注意以下事項：

- 設定儲存桶的一致性決定了對儲存桶中的物件或儲存桶配置執行的 S3 操作使用哪種一致性。它不會影響儲存桶本身的操作。
- 單一 API 操作的一致性會覆蓋儲存桶的一致性。
- 一般來說，儲存桶應該使用預設一致性"新寫後讀取"。如果請求無法正常運作，請盡可能變更應用程式用戶端行為。或者，配置客戶端以指定每個 API 請求的一致性。僅在萬不得已的情況下才在儲存桶層級設定一致性。

一致性和 ILM 規則如何相互作用以影響資料保護

您的一致性選擇和 ILM 規則都會影響物件的保護方式。這些設定可以相互作用。

例如，儲存物件時使用的一致性會影響物件元資料的初始位置，而為 ILM 規則選擇的攝取行為會影響物件副本的初始位置。由於StorageGRID需要存取物件的元資料及其資料來滿足客戶端請求，因此為一致性和攝取行為選擇相符的保護等級可以提供更好的初始資料保護和更可預測的系統回應。

下列"攝取選項"適用於 ILM 規則：

雙重提交

StorageGRID立即製作物件的臨時副本並將成功傳回給客戶端。在可能的情況下，將製作 ILM 規則中指定的副本。

嚴格的

在向客戶端返回成功之前，必須完成 ILM 規則中指定的所有複製。

均衡

StorageGRID嘗試在攝取時製作 ILM 規則中指定的所有副本；如果無法做到這一點，則會製作臨時副本並將成功傳回給用戶端。在可能的情況下，將進行 ILM 規則中指定的複製。

一致性和 ILM 規則如何交互的範例

假設您有一個雙站點網格，具有以下 ILM 規則和以下一致性：

- ILM 規則：建立兩個物件副本，一個在本機站點，一個在遠端站點。使用嚴格的攝取行為。

- 一致性：強全域（物件元資料立即分發到所有站點）。

當客戶端將物件儲存到網格時，StorageGRID會複製兩個物件並將元資料分發到兩個站點，然後再將成功返回給客戶端。

在接收成功訊息時，物件將受到完全保護，不會遺失。例如，如果本機站點在攝取後不久遺失，則物件資料和物件元資料的副本仍然存在於遠端站點。該物件完全可檢索。

如果您使用相同的 ILM 規則和強站點一致性，則用戶端可能會在物件資料複製到遠端站點之後但在物件元資料分發到那裡之前收到成功訊息。在這種情況下，物件元資料的保護等級與物件資料的保護等級不符。如果本地站點在攝取後不久遺失，則物件元資料就會遺失。無法檢索該物件。

一致性和 ILM 規則之間的相互關係可能很複雜。如果您需要協助，請聯絡NetApp。

物件版本控制

如果您想要保留每個物件的多個版本，您可以設定儲存桶的版本控制狀態。啟用儲存桶的版本控制有助於防止意外刪除對象，並使您能夠檢索和還原對象的早期版本。

StorageGRID系統實現了版本控制，支援大多數功能，但也有一些限制。StorageGRID支援每個物件最多10,000個版本。

物件版本控制可以與StorageGRID資訊生命週期管理 (ILM) 或 S3 儲存桶生命週期配置結合。您必須明確啟用每個儲存桶的版本控制。當為儲存桶啟用版本控制時，新增至儲存桶的每個物件都會被指派一個版本 ID，該 ID 由StorageGRID系統產生。

不支援使用 MFA（多因素身份驗證）刪除。



僅可在使用StorageGRID版本 10.3 或更高版本建立的儲存桶上啟用版本控制。

ILM 和版本控制

ILM 策略適用於物件的每個版本。ILM 掃描過程會持續掃描所有物件並根據目前 ILM 策略重新評估它們。您對 ILM 策略所做的任何變更都將套用於所有先前攝取的物件。如果啟用了版本控制，這包括先前攝取的版本。ILM 掃描將新的 ILM 變更套用至先前擷取的物件。

對於啟用版本控制的儲存桶中的 S3 對象，版本控制支援可讓您建立使用“非目前時間”作為參考時間的 ILM 規則（對於“僅將此規則應用於較舊的對象版本？”問題，選擇“是”["建立 ILM 規則精靈的第 1 步"](#)）。當物件更新時，其先前版本將變為非目前版本。使用「非當前時間」篩選器可讓您建立減少物件先前版本儲存影響的策略。



當您使用分段上傳作業上傳物件的新版本時，物件原始版本的非當前時間反映的是新版本的分段上傳的建立時間，而不是分段上傳的完成時間。在有限的情況下，原始版本的非當前時間可能比目前版本的時間早幾小時或幾天。

相關資訊

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

使用 S3 REST API 設定 S3 物件鎖

如果您的StorageGRID系統啟用了全域 S3 物件鎖定設置，則可以建立啟用了 S3 物件鎖定的儲存桶。您可以為每個儲存桶指定預設保留或為每個物件版本指定保留設定。

如何為儲存桶啟用 S3 物件鎖定

如果您的StorageGRID系統啟用了全域 S3 物件鎖定設置，則可以在建立每個儲存桶時選擇啟用 S3 物件鎖定。

S3 物件鎖定是一個永久設置，只有在建立儲存桶時才能啟用。建立儲存桶後，您無法新增或停用 S3 物件鎖定。

若要為儲存桶啟用 S3 物件鎖定，請使用下列任一方法：

- 使用租用戶管理器建立儲存桶。看["建立 S3 儲存桶"](#)。
- 使用 CreateBucket 請求建立儲存桶 `x-amz-bucket-object-lock-enabled` 請求標頭。看["對 bucket 的操作"](#)。

S3 物件鎖定需要儲存桶版本控制，該功能在建立儲存桶時自動啟用。您無法暫停儲存桶的版本控制。看["物件版本控制"](#)。

儲存桶的預設保留設定

當為儲存桶啟用 S3 物件鎖定时，您可以選擇為儲存桶啟用預設保留，並指定預設保留模式和預設保留期。

預設保留模式

- 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：
 - 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。

預設保留期

每個儲存桶可以具有以年或天為單位指定的預設保留期。

如何設定儲存桶的預設保留

若要設定儲存桶的預設保留，請使用下列任一方法：

- 從租戶管理器管理儲存桶設定。看["建立 S3 儲存桶"](#)和["更新 S3 物件鎖定預設保留"](#)。
- 針對儲存桶發出 PutObjectLockConfiguration 請求，指定預設模式和預設天數或年數。

PutObjectLock配置

PutObjectLockConfiguration 請求可讓您設定和修改已啟用 S3 物件鎖定的儲存桶的預設保留模式和預設保留期。您也可以刪除先前配置的預設保留設定。

當新的物件版本被提取到儲存桶時，如果 `x-amz-object-lock-mode` 和 `x-amz-object-lock-retain-until-date` 未指定。如果 `x-amz-object-lock-retain-until-date` 未指定。

如果在擷取物件版本後修改了預設保留期，則物件版本的保留截止日期保持不變，並且不會使用新的預設保留期重新計算。

你必須擁有 `s3:PutBucketObjectLockConfiguration` 權限，或成為帳戶 root，即可完成此操作。

這 `Content-MD5` 必須在 PUT 請求中指定請求標頭。

請求範例

此範例為儲存桶啟用 S3 物件鎖定，並將預設保留模式設為 COMPLIANCE，將預設保留期設為 6 年。

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

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

如何決定儲存桶的預設保留時間

若要確定儲存桶是否啟用了 S3 物件鎖定並查看預設保留模式和保留期，請使用下列任一方法：

- 在租用戶管理員中查看儲存桶。看["查看 S3 儲存桶"](#)。
- 發出 GetObjectLockConfiguration 請求。

取得物件鎖配置

`GetObjectLockConfiguration` 要求可讓您確定是否為儲存桶啟用了 S3 物件鎖定，如果啟用，則檢視是否為儲存桶配置了預設保留模式和保留期。

當新的物件版本被提取到儲存桶時，如果 ``x-amz-object-lock-mode`` 未指定。如果 ``x-amz-object-lock-retain-until-date`` 未指定。

你必須擁有 ``s3:GetBucketObjectLockConfiguration`` 權限，或成為帳戶 `root`，即可完成此操作。

請求範例

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

回應範例

```
HTTP/1.1 200 OK
x-amz-id-2:
iVmcB7OXXJRkRH1FiVq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpX1knabA0LTvBYJpSIX
k=
x-amz-request-id: B34E94CACB2CEF6D
Date: Fri, 04 Sep 2020 22:47:09 GMT
Transfer-Encoding: chunked
Server: AmazonS3

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

如何指定物件的保留設定

啟用了 S3 物件鎖的儲存桶可以包含具有和不具有 S3 物件鎖保留設定的物件的組合。

使用 S3 REST API 指定物件級保留設定。物件的保留設定會覆蓋儲存桶的任何預設保留設定。

您可以為每個物件指定以下設定：

- 保留模式：合規或治理。
- **Retain-until-date**：指定StorageGRID必須保留物件版本多久的日期。
 - 在 COMPLIANCE 模式下，如果保留截止日期是將來，則可以檢索對象，但不能修改或刪除它。保留截止日期可以增加，但不能減少或刪除。
 - 在治理模式下，具有特殊權限的使用者可以繞過保留截止日期設定。他們可以在保留期結束之前刪除物件版本。他們還可以增加、減少甚至刪除保留截止日期。
- 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。

物件的合法保留設定與保留模式和保留截止日期無關。如果物件版本處於合法保留狀態，則任何人都無法刪除該版本。

若要在將物件版本新增至儲存桶時指定 S3 物件鎖定設置，請發出"[放置對象](#)"，"[複製對象](#)"，或者"[建立多部分上傳](#)"要求。

您可以使用以下內容：

- `x-amz-object-lock-mode`，可以是 COMPLIANCE 或 GOVERNANCE（區分大小寫）。



如果您指定 `x-amz-object-lock-mode`，您還必須指定 `x-amz-object-lock-retain-until-date`。

- `x-amz-object-lock-retain-until-date`
 - 保留截止日期值必須採用以下格式 `2020-08-10T21:46:00Z`。允許使用小數秒，但只保留 3 位小數（毫秒精度）。不允許使用其他 ISO 8601 格式。
 - 保留截止日期必須是將來的日期。
- `x-amz-object-lock-legal-hold`

如果合法保留處於開啟狀態（區分大小寫），則該物件將被置於合法保留之下。如果合法保留處於關閉狀態，則不會設定合法保留。任何其他值都會導致 400 Bad Request (InvalidArgument) 錯誤。

如果您使用以下任何請求標頭，請注意以下限制：

- 這 ``Content-MD5`` 請求標頭（如果有）``x-amz-object-lock-*`` 請求標頭存在於 PutObject 請求中。``Content-MD5`` 對於 CopyObject 或 CreateMultipartUpload 來說不是必需的。
- 如果儲存桶未啟用 S3 物件鎖定，且 ``x-amz-object-lock-*`` 請求標頭存在，則傳回 400 錯誤請求 (InvalidRequest) 錯誤。
- PutObject 請求支援使用 ``x-amz-storage-class: REDUCED_REDUNDANCY`` 以匹配 AWS 行為。但是，當將物件提取到啟用了 S3 物件鎖定的儲存桶中時，StorageGRID將始終執行雙重提交提取。

- 後續的 GET 或 HeadObject 版本回應將包含標頭 `x-amz-object-lock-mode`、`x-amz-object-lock-retain-until-date`、和 `x-amz-object-lock-legal-hold`，如果配置並且請求發送者有正確的 `s3:Get*` 權限。

您可以使用 `s3:object-lock-remaining-retention-days` 策略條件鍵用於限制物件的最小和最大允許保留期。

如何更新物件的保留設定

如果需要更新現有物件版本的合法保留或保留設置，您可以執行下列物件子資源操作：

- `PutObjectLegalHold`

如果新的合法保留值為 ON，則該物件將被置於合法保留之下。如果合法保留值為 OFF，則解除合法保留。

- `PutObjectRetention`

- 模式值可以是 COMPLIANCE 或 GOVERNANCE（區分大小寫）。
- 保留截止日期值必須採用以下格式 2020-08-10T21:46:00Z。允許使用小數秒，但只保留 3 位小數（毫秒精度）。不允許使用其他 ISO 8601 格式。
- 如果物件版本具有現有的保留截止日期，則只能增加它。新值必須是未來的值。

如何使用治理模式

擁有 `s3:BypassGovernanceRetention` 權限可以繞過使用治理模式的物件的活動保留設定。任何 DELETE 或 `PutObjectRetention` 操作都必須包含 `x-amz-bypass-governance-retention:true` 請求標頭。這些使用者可以執行以下附加操作：

- 執行 `DeleteObject` 或 `DeleteObjects` 操作，在物件版本的保留期結束之前刪除該物件版本。

處於合法保留狀態的物件無法被刪除。必須關閉合法保留。

- 在物件的保留期結束之前，執行 `PutObjectRetention` 操作，將物件版本的模式從 GOVERNANCE 變更為 COMPLIANCE。

絕不允許將模式從合規性改為治理性。

- 執行 `PutObjectRetention` 操作以增加、減少或刪除物件版本的保留期。

相關資訊

- ["使用 S3 對象鎖管理對象"](#)
- ["使用 S3 對象鎖保留對象"](#)
- ["Amazon Simple Storage Service 使用者指南：鎖定對象"](#)

建立 S3 生命週期配置

您可以建立 S3 生命週期配置來控制何時從 StorageGRID 系統中刪除特定物件。

本節中的簡單範例說明了 S3 生命週期配置如何控制何時從特定 S3 儲存桶中刪除（過期）某些物件。本節中的範例僅用於說明目的。有關建立 S3 生命週期配置的完整詳細信息，請參閱 ["Amazon Simple Storage Service 使用者指南：物件生命週期管理"](#)。請注意，StorageGRID 僅支援 Expiration 操作；它不支援 Transition 操作。

什麼是生命週期配置

生命週期配置是一組應用於特定 S3 儲存桶中的物件的規則。每條規則指定哪些物件會受到影響以及這些物件何時過期（在特定日期或幾天後）。

StorageGRID在生命週期配置中支援最多 1,000 條生命週期規則。每個規則可以包含以下 XML 元素：

- 過期：從物件被攝取時開始，當達到指定日期或指定天數時刪除物件。
- NoncurrentVersionExpiration：從物件變成非目前版本開始，當達到指定的天數時刪除該物件。
- 過濾器（前綴、標籤）
- 地位
- ID

每個物件都遵循 S3 儲存桶生命週期或 ILM 策略的保留設定。配置 S3 儲存桶生命週期後，生命週期到期作業將覆蓋與儲存桶生命週期過濾器相符的物件的 ILM 策略。與儲存桶生命週期過濾器不符的物件使用 ILM 策略的保留設定。如果物件與儲存桶生命週期過濾器匹配，且未明確指定到期操作，則不使用 ILM 策略的保留設置，這表示物件版本將永遠保留。看"[S3 儲存桶生命週期和 ILM 策略的範例優先級](#)"。

因此，即使 ILM 規則中的放置說明仍然適用於該對象，該對象也可能會從網格中移除。或者，即使物件的任何 ILM 放置指令已經失效，該物件仍可能保留在網格上。有關詳細信息，請參閱"[ILM 如何在物件的整個生命週期中運作](#)"。



儲存桶生命週期配置可與啟用了 S3 物件鎖的儲存桶一起使用，但舊版相容儲存桶不支援儲存桶生命週期配置。

StorageGRID支援使用下列儲存桶操作來管理生命週期配置：

- DeleteBucket生命週期
- 取得BucketLifecycleConfiguration
- PutBucket生命週期配置

建立生命週期配置

作為建立生命週期配置的第一步，您需要建立一個包含一個或多個規則的 JSON 檔案。例如，此 JSON 檔案包含三條規則，如下所示：

1. 規則 1 僅適用於與前綴相符的對象 `category1/` 並且有一個 `key2` 的價值 `tag2`。這 `Expiration` 參數指定與過濾器匹配的物件將於 2020 年 8 月 22 日午夜到期。
2. 規則 2 僅適用於與前綴相符的對象 `category2/`。這 `Expiration` 參數指定與篩選器相符的物件將在被攝取後 100 天過期。



指定天數的規則與物件被攝取的時間有關。如果目前日期超過攝取日期加上天數，則套用生命週期配置後，某些物件可能會從儲存桶中刪除。

3. 規則 3 僅適用於與前綴相符的對象 `category3/`。這 `Expiration` 參數指定匹配對象的任何非當前版本將在成為非當前版本後 50 天過期。

```

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

```

將生命週期配置應用於儲存桶

建立生命週期設定檔後，您可以透過發出 `PutBucketLifecycleConfiguration` 請求將其套用到儲存桶。

此請求將範例檔案中的生命週期配置套用至名為 `testbucket`。

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

若要驗證生命週期配置是否已成功套用於儲存桶，請發出 `GetBucketLifecycleConfiguration` 要求。例如：

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

成功的回應列出了您剛剛應用的生命週期配置。

驗證儲存桶生命週期到期是否適用於對象

您可以在發出 `PutObject`、`HeadObject` 或 `GetObject` 請求時確定生命週期配置中的過期規則是否適用於特定物件。如果適用規則，則回應包括 `Expiration` 指示物件何時過期以及符合哪個過期規則的參數。



由於 bucket 生命週期覆蓋 ILM，`expiry-date` 顯示的是物件被刪除的實際日期。有關詳細信息，請參閱["如何確定對象保留"](#)。

例如，此 `PutObject` 請求於 2020 年 6 月 22 日發出，並將一個物件放入 `testbucket` 桶。

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

成功回應表示該物件將在 100 天後（2020 年 10 月 1 日）過期，並且符合生命週期配置的規則 2。

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

例如，此 `HeadObject` 請求用於取得 `testbucket` 儲存桶中相同物件的元資料。

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

成功回應包括物件的元數據，並表明該物件將在 100 天後過期，並且符合規則 2。

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



對於啟用版本控制的儲存桶，`x-amz-expiration` 回應頭僅適用於物件的目前版本。

實作 S3 REST API 的建議

在實作用於 StorageGRID 的 S3 REST API 時，您應該遵循這些建議。

對不存在對象的 HEAD 建議

如果您的應用程式定期檢查某個物件是否存在於您認為該物件實際上不存在的路徑中，則應使用“可用”**一致性**。例如，如果您的應用程式在 PUT 之前 HEAD 某個位置，則您應該使用「可用」一致性。

否則，如果 HEAD 操作未找到該對象，且同一站點上有兩個或多個儲存節點不可用或遠端站點無法訪問，您可能收到大量 500 內部伺服器錯誤。

您可以使用**PUT桶一致性**請求，或者您可以在單一 API 操作的請求標頭中指定一致性。

對象鍵的建議

根據儲存桶首次建立的時間，遵循以下物件鍵名稱建議。

在 StorageGRID 11.4 或更早版本中建立的儲存桶

- 不要使用隨機值作為物件鍵的前四個字元。這與 AWS 先前對鍵前綴的建議形成了對比。相反，使用非隨機、非唯一的前綴，例如 image。
- 如果您確實遵循先前的 AWS 建議在鍵前綴中使用隨機和唯一字符，請在物件鍵前加上目錄名稱。也就是說，使用這種格式：

```
mybucket/mydir/f8e3-image3132.jpg
```

而不是這種格式：

mybucket/f8e3-image3132.jpg

在**StorageGRID 11.4** 或更高版本中建立的儲存桶

不需要限制物件鍵名稱以滿足效能最佳實務。大多數情況下，您可以對物件鍵名稱的前四個字元使用隨機值。



一個例外是 S3 工作負載，它會在短時間後連續刪除所有物件。為了盡量減少此用例對效能的影響，每隔幾千個物件就會用日期之類的內容改變鍵名的前導部分。例如，假設 S3 用戶端通常每秒寫入 2,000 個對象，而 ILM 或儲存桶生命週期策略會在三天後刪除所有物件。為了最大限度地減少對效能的影響，您可以使用以下模式命名鍵：`/mybucket/mydir/yyyymmddhhmmss-random_UUID.jpg`

“範圍讀取”的建議

如果“[壓縮儲存物件的全域選項](#)”啟用後，S3 用戶端應用程式應避免執行指定傳回位元組範圍的 `GetObject` 操作。這些「範圍讀取」操作效率低下，因為 StorageGRID 必須有效地解壓縮物件才能存取請求的位元組。從非常大的物件中請求一小段位元組的 `GetObject` 操作效率特別低；例如，從 50 GB 的壓縮物件中讀取 10 MB 範圍的位元組效率很低。

如果從壓縮物件讀取範圍，客戶端請求可能會逾時。



如果您需要壓縮物件並且客戶端應用程式必須使用範圍讀取，請增加應用程式的讀取逾時。

支援 Amazon S3 REST API

S3 REST API 實作細節

StorageGRID 系統實作了簡單儲存服務 API (API 版本 2006-03-01)，支援大多數操作，但也有一些限制。在整合 S3 REST API 用戶端應用程式時，您需要了解實作細節。

StorageGRID 系統支援虛擬託管式請求和路徑式請求。

日期處理

S3 REST API 的 StorageGRID 實作僅支援有效的 HTTP 日期格式。

StorageGRID 系統僅支援接受日期值的任何標頭的有效 HTTP 日期格式。日期的時間部分可以採用格林威治標準時間 (GMT) 格式指定，也可以採用沒有時區偏移的協調世界時 (UTC) 格式指定 (必須指定 +0000)。如果你包括 `x-amz-date` 請求中的標頭，它會覆寫 `Date` 請求標頭中指定的任何值。使用 AWS 簽章版本 4 時，`x-amz-date` 標頭必須存在於簽署的請求中，因為不支援日期標頭。

常見請求標頭

StorageGRID 系統支援由下列定義的通用請求標頭 ["Amazon Simple Storage Service API 參考：常見請求標頭"](#)，但有一個例外。

請求頭	執行
授權	<p>完全支援 AWS 簽章版本 2</p> <p>支援 AWS 簽章版本 4，但有以下例外：</p> <ul style="list-style-type: none"> 當您提供實際有效載荷校驗和值時 <code>x-amz-content-sha256</code>，該值無需驗證即可被接受，就像該值 <code>UNSIGNED-PAYLOAD</code> 已提供標題。當你提供 <code>x-amz-content-sha256</code> 標頭值暗示 <code>aws-chunked</code> 串流（例如，<code>STREAMING-AWS4-HMAC-SHA256-PAYLOAD</code>），區塊簽章不會根據區塊資料進行驗證。
x-amz-安全令牌	未實施。返回 <code>XNotImplemented</code> 。

常見響應頭

StorageGRID系統支援《簡單儲存服務 API 參考》定義的所有常見回應標頭，但有一個例外。

回應頭	執行
x-amz-id-2	未使用

驗證請求

StorageGRID系統支援使用 S3 API 對物件進行經過驗證和匿名存取。

S3 API 支援簽章版本 2 和簽章版本 4 用於驗證 S3 API 請求。

必須使用您的存取金鑰 ID 和秘密存取金鑰對經過驗證的請求進行簽署。

StorageGRID系統支援兩種身份驗證方法：HTTP `Authorization` 標題並使用查詢參數。

使用 HTTP 授權標頭

HTTP `Authorization` 除儲存桶策略允許的匿名請求外，所有 S3 API 操作都使用標頭。這 `Authorization` 標頭包含驗證請求所需的所有簽名資訊。

使用查詢參數

您可以使用查詢參數向 URL 新增身份驗證資訊。這稱為預簽名 URL，可用於授予對特定資源的臨時存取權限。具有預簽名 URL 的使用者不需要知道秘密存取金鑰即可存取資源，這使您能夠提供對資源的第三方受限存取。

對服務的操作

StorageGRID系統支援對服務進行下列操作。

手術	執行
列表桶 (以前稱為 GET 服務)	使用所有 Amazon S3 REST API 行為實作。如有變更，恕不另行通知。
取得儲存使用情況	StorageGRID "取得儲存使用情況" 請求會告訴您帳戶使用的儲存總量以及與該帳戶關聯的每個儲存桶的儲存總量。這是對具有 / 路徑和自訂查詢參數的服務的操作(?x-ntap-sg-usage) 補充道。
選項 /	客戶端應用程式可以發出 `OPTIONS /` 向儲存節點上的 S3 連接埠發出請求，無需提供 S3 驗證憑證，以確定儲存節點是否可用。您可以使用此請求進行監控，或允許外部負載平衡器識別儲存節點何時關閉。

對 bucket 的操作

StorageGRID 系統支援每個 S3 租用戶帳戶最多 5,000 個儲存桶。

每個網格最多可以有 100,000 個桶。

為了支援 5,000 個儲存桶，網格中的每個儲存節點必須至少具有 64 GB 的 RAM。

儲存桶名稱限制遵循 AWS 美國標準區域限制，但您應該進一步將它們限制為 DNS 命名約定，以支援 S3 虛擬託管樣式請求。

有關詳細信息，請參閱以下內容：

- ["Amazon Simple Storage Service 使用者指南：儲存桶配額、限制和局限性"](#)
- ["配置 S3 端點域名"](#)

ListObjects (取得 Bucket) 和 ListObjectVersions (取得 Bucket 物件版本) 操作支援 StorageGRID "一致性值"。

您可以檢查是否針對各個儲存桶啟用或停用了上次存取時間的更新。看 ["取得 Bucket 上次造訪時間"](#)。

下表描述了 StorageGRID 如何實作 S3 REST API 儲存桶操作。要執行任何這些操作，必須為帳戶提供必要的存取憑證。

手術	執行
創建桶	<p>建立一個新的儲存桶。透過建立儲存桶，您就成為儲存桶的擁有者。</p> <ul style="list-style-type: none"> • Bucket 名稱必須遵循以下規則： <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。 ◦ 可以是一系列一個或多個標籤，相鄰的標籤以句點分隔。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。 ◦ 不能看起來像文字格式的 IP 位址。 ◦ 不應在虛擬託管樣式請求中使用句點。句點將導致伺服器通配符憑證驗證出現問題。 • 預設情況下，儲存桶在 `us-east-1` 區域；但是，您可以使用 `LocationConstraint` 請求主體中的請求元素來指定不同的區域。使用時 `LocationConstraint` 元素，您必須指定使用網格管理器或網格管理 API 定義的區域的確切名稱。如果您不知道應該使用的區域名稱，請聯絡您的系統管理員。 <p>注意：如果您的 CreateBucket 要求使用StorageGRID中未定義的區域，則會發生錯誤。</p> <ul style="list-style-type: none"> • 您可以包括 `x-amz-bucket-object-lock-enabled` 請求標頭來建立啟用了 S3 物件鎖的儲存桶。看"使用 S3 REST API 設定 S3 物件鎖"。 <p>建立儲存桶時必須啟用 S3 物件鎖定。建立儲存桶後，您無法新增或停用 S3 物件鎖定。S3 物件鎖定需要儲存桶版本控制，該功能在您建立儲存桶時自動啟用。</p>
刪除桶	刪除儲存桶。
刪除BucketCors	刪除儲存桶的 CORS 配置。
刪除桶加密	從儲存桶中刪除預設加密。現有的加密物件仍保持加密狀態，但新增至儲存桶的任何新物件都不會加密。
DeleteBucket生命週期	從儲存桶中刪除生命週期配置。看 "建立 S3 生命週期配置" 。
刪除桶策略	刪除附加到儲存桶的策略。
刪除桶複製	刪除附加到儲存桶的複製配置。

手術	執行
刪除桶標記	<p>使用 `tagging` 子資源從儲存桶中刪除所有標籤。</p> <p>警告：如果為此儲存桶設定了非預設的 ILM 策略標籤，則會出現 `NTAP-SG-ILM-BUCKET-TAG` 已指派值的 bucket 標籤。如果存在 `NTAP-SG-ILM-BUCKET-TAG` 桶標籤。相反，發出僅包含 `NTAP-SG-ILM-BUCKET-TAG` 標籤及其指派的值，以從儲存桶中刪除所有其他標籤。請勿修改或刪除 `NTAP-SG-ILM-BUCKET-TAG` 桶標籤。</p>
獲取BucketAcl	傳回肯定回應以及儲存桶擁有者的 ID、DisplayName 和 Permission，表示擁有者對該儲存桶具有完全存取權。
獲取BucketCors	返回 `cors` 儲存桶的配置。
取得桶加密	傳回儲存桶的預設加密配置。
取得BucketLifecycleConfiguration (以前稱為 GET Bucket 生命週期)	傳回儲存桶的生命週期配置。看 "建立 S3 生命週期配置" 。
取得儲存桶位置	返回使用 LocationConstraint `CreateBucket` 請求中的元素。如果 bucket 的區域是 `us-east-1`，則該區域傳回一個空字串。
取得儲存桶通知配置 (以前稱為 GET Bucket 通知)	傳回附加到儲存桶的通知配置。
取得BucketPolicy	傳回附加到儲存桶的策略。
獲取Bucket複製	傳回附加到儲存桶的複製配置。
取得桶標記	<p>使用 `tagging` 子資源傳回儲存桶的所有標籤。</p> <p>警告：如果為此儲存桶設定了非預設的 ILM 策略標籤，則會出現 `NTAP-SG-ILM-BUCKET-TAG` 已指派值的 bucket 標籤。請勿修改或刪除此標籤。</p>
取得Bucket版本	<p>此實作使用 `versioning` 子資源傳回儲存桶的版本控制狀態。</p> <ul style="list-style-type: none"> • <i>blank</i>：從未啟用版本控制（儲存桶為「未版本控制」） • 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

手術	執行
取得物件鎖配置	<p>如果已配置，則傳回儲存桶預設保留模式和預設保留期。</p> <p>看"使用 S3 REST API 設定 S3 物件鎖"。</p>
頭桶	<p>確定儲存桶是否存在以及您是否有權存取它。</p> <p>此操作返回：</p> <ul style="list-style-type: none"> • <code>x-ntap-sg-bucket-id</code>：Bucket 的 UUID，格式為 UUID。 • <code>x-ntap-sg-trace-id</code>：關聯請求的唯一追蹤 ID。
ListObjects 和 ListObjectsV2 (以前稱為 GET Bucket)	<p>傳回儲存桶中的部分或全部（最多 1,000 個）物件。物件的儲存類別可以有兩個值，即使物件是透過 <code>REDUCED_REDUNDANCY</code> 儲存類別選項：</p> <ul style="list-style-type: none"> • <code>STANDARD</code>，表示該物件儲存在由 Storage Node 組成的儲存池中。 • <code>GLACIER</code>，表示該物件已移至雲端儲存池指定的外部儲存桶中。 <p>如果儲存桶包含大量具有相同前綴的已刪除鍵，則回應可能包含一些 <code>CommonPrefixes</code> 不包含密鑰。</p>
列出物件版本 (以前稱為 GET Bucket Object 版本)	<p>擁有儲存桶的讀取權限，使用此操作 <code>versions</code> 子資源列出了儲存桶中所有版本的物件的元資料。</p>
PutBucketCors	<p>設定儲存桶的 CORS 配置，以便儲存桶可以處理跨域請求。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 <code>images</code> 儲存圖形。透過設定 CORS 配置 <code>images</code> bucket，您可以允許該 bucket 中的圖像顯示在網站上 <code>http://www.example.com</code>。</p>
PutBucket加密	<p>設定現有儲存桶的預設加密狀態。啟用儲存桶級加密後，新增至儲存桶的任何新物件都將被加密。StorageGRID 支援使用 StorageGRID 管理的金鑰進行伺服器端加密。指定伺服器端加密配置規則時，設定 <code>SSEAlgorithm</code> 參數 <code>AES256</code>，並且不要使用 <code>KMSMasterKeyID</code> 範圍。</p> <p>如果物件上傳請求已經指定了加密（即，如果請求包含 <code>x-amz-server-side-encryption-*</code> 請求標頭）。</p>

手術	執行
PutBucket生命週期配置 (以前稱為 PUT Bucket 生命週期)	<p>為儲存桶建立新的生命週期配置或取代現有的生命週期配置。StorageGRID在生命週期配置中支援最多 1,000 條生命週期規則。每個規則可以包含以下 XML 元素：</p> <ul style="list-style-type: none"> • 到期日 (天數、日期、ExpiredObjectDeleteMarker) • NoncurrentVersionExpiration (NewerNoncurrentVersions、NoncurrentDays) • 過濾器 (前綴、標籤) • 地位 • ID <p>StorageGRID不支援以下操作：</p> <ul style="list-style-type: none"> • 中止未完成的分段上傳 • 過渡 <p>看"建立 S3 生命週期配置"。若要了解儲存桶生命週期中的到期操作如何與 ILM 放置指令交互，請參閱"ILM 如何在物件的整個生命週期中運作"。</p> <p>注意：儲存桶生命週期配置可與啟用了 S3 物件鎖的儲存桶一起使用，但儲存桶生命週期配置不支援舊版相容儲存桶。</p>

手術	執行
PutBucketNotification配置 (以前稱為 PUT Bucket 通知)	<p>使用請求正文中包含的通知配置 XML 為儲存桶配置通知。您應該了解以下實施細節：</p> <ul style="list-style-type: none"> • StorageGRID支援 Amazon Simple Notification Service (Amazon SNS) 或 Kafka 主題作為目的地。不支援簡單佇列服務 (SQS) 或 Amazon Lambda 終端節點。 • 通知的目的地必須指定為StorageGRID端點的 URN。可以使用租用戶管理器或租用戶管理 API 建立端點。 <p>端點必須存在才能成功配置通知。如果端點不存在，400 Bad Request 錯誤與代碼一起返回 InvalidArgument。</p> <ul style="list-style-type: none"> • 您無法為以下事件類型設定通知。這些事件類型不受支援。 <ul style="list-style-type: none"> ◦ s3:ReducedRedundancyLostObject ◦ s3:ObjectRestore:Completed • 從StorageGRID傳送的事件通知使用標準 JSON 格式，但它們不包含某些鍵，而對其他鍵使用特定值，如下列清單所示： <ul style="list-style-type: none"> ◦ 事件源 <ul style="list-style-type: none"> sgws:s3 ◦ aws區域 <ul style="list-style-type: none"> 不包括 ◦ x-amz-id-2 <ul style="list-style-type: none"> 不包括 ◦ 阿恩 <ul style="list-style-type: none"> urn:sgws:s3:::bucket_name
PutBucketPolicy	設定附加到儲存桶的策略。看 "使用儲存桶和群組存取策略" 。

手術	執行
PutBucket複製	<p>配置"StorageGRID CloudMirror 複製"對於儲存桶，使用請求正文中提供的複製配置 XML。對於 CloudMirror 複製，您應該注意以下實作細節：</p> <ul style="list-style-type: none"> 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 "Amazon Simple Storage Service 使用者指南：複製配置"。 可以在版本化或非版本化的儲存桶上配置儲存桶複製。 您可以在複製配置 XML 的每個規則中指定不同的目標儲存桶。一個來源儲存桶可以複製到多個目標儲存桶。 目標儲存桶必須指定為租用戶管理器或租用戶管理 API 中指定的StorageGRID 端點的 URN。看"配置 CloudMirror 複製"。 <p>端點必須存在才能成功進行複製配置。如果端點不存在，請求將會失敗，因為 400 Bad Request。錯誤訊息指出：Unable to save the replication policy. The specified endpoint URN does not exist: URN.</p> <ul style="list-style-type: none"> 您不需要指定 `Role` 在配置 XML 中。StorageGRID不使用此值，如果提交將被忽略。 如果您從配置 XML 中省略儲存類，StorageGRID將使用 `STANDARD` 預設儲存類別。 如果您從來源儲存桶中刪除物件或刪除來源儲存桶本身，則跨區域複製行為如下： <ul style="list-style-type: none"> 如果您在複製之前刪除物件或儲存桶，則該物件/儲存桶不會被複製，並且您不會收到通知。 如果在複製後刪除物件或儲存桶，StorageGRID將遵循跨區域複製 V1 的標準 Amazon S3 刪除行為。
PutBucketTagging	<p>使用 `tagging` 子資源來新增或更新儲存桶的一組標籤。在新增儲存桶標籤時，請注意以下限制：</p> <ul style="list-style-type: none"> StorageGRID和 Amazon S3 都支援每個儲存桶最多 50 個標籤。 與儲存桶關聯的標籤必須具有唯一的標籤鍵。標籤鍵的長度最多可達 128 個 Unicode 字元。 標籤值的長度最多可達 256 個 Unicode 字元。 鍵和值區分大小寫。 <p>警告：如果為此儲存桶設定了非預設的 ILM 策略標籤，則會出現 `NTAP-SG-ILM-BUCKET-TAG` 已指派值的 bucket 標籤。確保 `NTAP-SG-ILM-BUCKET-TAG` 所有 PutBucketTagging 請求中都包含儲存桶標籤和已指派的值。請勿修改或刪除此標籤。</p> <p>注意：此操作將覆蓋儲存桶已有的任何目前標籤。如果集合中省略了任何現有標籤，則將從儲存桶中刪除這些標籤。</p>

手術	執行
PutBucket版本控制	<p>使用 `versioning` 子資源來設定現有儲存桶的版本控制狀態。您可以使用下列值之一設定版本控制狀態：</p> <ul style="list-style-type: none"> • 已啟用：為儲存桶中的物件啟用版本控制。新增到儲存桶的所有物件都會收到唯一的版本 ID。 • 暫停：停用儲存桶中物件的版本控制。新增到儲存桶的所有物件都會收到版本 ID null。
PutObjectLock配置	<p>配置或刪除儲存桶預設保留模式和預設保留期。</p> <p>如果修改了預設保留期，則現有物件版本的保留截止日期保持不變，並且不會使用新的預設保留期重新計算。</p> <p>看"使用 S3 REST API 設定 S3 物件鎖"了解詳細資訊。</p>

對物件的操作

對物件的操作

本節介紹StorageGRID系統如何為物件實作 S3 REST API 操作。

以下條件適用於所有物件操作：

- StorageGRID"[一致性值](#)"所有物件操作均支持，但以下操作除外：
 - 取得對象Acl
 - OPTIONS /
 - 放置對象合法保留
 - PutObjectRetention
 - 選擇對象內容
- 衝突的客戶端請求（例如兩個客戶端寫入同一個金鑰）將根據「最新勝利」的原則解決。「最新勝利」評估的時間取決於StorageGRID系統完成給定請求的時間，而不是 S3 用戶端開始操作的時間。
- StorageGRID儲存桶中的所有物件均歸儲存體桶擁有者所有，包括由匿名使用者或其他帳號建立的物件。
- 透過 Swift 提取到StorageGRID系統的資料物件無法透過 S3 存取。

下表描述了StorageGRID如何實作 S3 REST API 物件操作。

手術	執行
刪除對象	<p>在處理 DeleteObject 請求時，StorageGRID 會嘗試立即從所有儲存位置刪除該物件的所有副本。如果成功，StorageGRID 會立即向用戶端回傳回應。如果無法在 30 秒內刪除所有副本（例如，由於某個位置暫時無法使用），StorageGRID 會將副本排隊等待刪除，然後向用戶端指示成功。</p> <p>限制</p> <ul style="list-style-type: none"> • 多重身份驗證 (MFA) 和回應標頭 `x-amz-mfa` 不受支援。 • The If-None 和 If-None-Match 標頭已被接受，但無法正常工作。 <p>版本控制</p> <p>要刪除特定版本，請求者必須是儲存桶擁有者並使用 versionId 子資源。使用此子資源將永久刪除該版本。如果 `versionId` 對應刪除標記，響應頭 `x-amz-delete-marker` 返回設定為 `true`。</p> <ul style="list-style-type: none"> • 如果刪除物件時沒有 versionId 啟用版本控制的儲存桶上的子資源，會導致產生刪除標記。這 `versionId` 刪除標記的回傳方式是使用 `x-amz-version-id` 響應頭，以及 `x-amz-delete-marker` 響應頭返回設定為 `true`。 • 如果刪除物件時沒有 versionId 在暫停版本控制的儲存桶上刪除子資源，將導致永久刪除已經存在的「空白」版本或「空」刪除標記，並產生新的「空」刪除標記。這 `x-amz-delete-marker` 響應頭返回設定為 `true`。 <p>注意：在某些情況下，一個物件可能存在多個刪除標記。</p> <p>看"使用 S3 REST API 設定 S3 物件鎖"了解如何在治理模式下刪除物件版本。</p>
刪除對象 (以前稱為 DELETE 多個物件)	<p>多重身份驗證 (MFA) 和回應標頭 `x-amz-mfa` 不受支援。</p> <p>可以在同一個請求訊息中刪除多個物件。</p> <p>看"使用 S3 REST API 設定 S3 物件鎖"了解如何在治理模式下刪除物件版本。</p>
刪除物件標記	<p>使用 `tagging` 子資源會從物件中刪除所有標籤。</p> <p>版本控制</p> <p>如果 versionId 如果請求中未指定查詢參數，則該操作將從版本化儲存桶中物件的最新版本中刪除所有標籤。如果物件的目前版本是刪除標記，則傳回「MethodNotAllowed」狀態，並 `x-amz-delete-marker` 響應頭設定為 `true`。</p>
取得對象	"取得對象"

手術	執行
取得對象Acl	如果為帳戶提供了必要的存取憑證，則操作將傳回肯定回應以及物件擁有者的 ID、DisplayName 和 Permission，表示擁有人對該物件具有完全存取權。
獲取對象合法持有	"使用 S3 REST API 設定 S3 物件鎖"
取得對象保留	"使用 S3 REST API 設定 S3 物件鎖"
取得物件標記	使用 `tagging` 子資源傳回物件的所有標籤。 版本控制 如果 `versionId` 如果請求中未指定查詢參數，則操作將傳回版本化儲存桶中物件最新版本的所有標籤。如果物件的目前版本是刪除標記，則傳回「MethodNotAllowed」狀態，並 `x-amz-delete-marker` 響應頭設定為 `true`。
頭部對象	"頭部對象"
復原對象	"復原對象"
放置對象	"放置對象"
複製對象 (之前名為 PUT 物件 - 複製)	"複製對象"
放置對象合法保留	"使用 S3 REST API 設定 S3 物件鎖"
PutObjectRetention	"使用 S3 REST API 設定 S3 物件鎖"

手術	執行
PutObjectTagging	<p>使用 `tagging` 子資源會為現有物件新增一組標籤。</p> <p>對象標籤限制</p> <p>您可以在上傳新物件時為其新增標籤，也可以將其新增至現有物件中。StorageGRID和 Amazon S3 都支援每個物件最多 10 個標籤。與物件關聯的標籤必須具有唯一的標籤鍵。標籤鍵的長度最多為 128 個 Unicode 字符，標籤值的長度最多為 256 個 Unicode 字元。鍵和值區分大小寫。</p> <p>標籤更新和攝取行為</p> <p>當您使用 PutObjectTagging 更新物件的標籤時，StorageGRID不會重新擷取該物件。這表示符合的 ILM 規則中指定的 Ingest Behavior 選項未被使用。當 ILM 由正常後台 ILM 程序重新評估時，將對更新觸發的物件位置進行任何變更。</p> <p>這意味著，如果 ILM 規則對攝取行為使用嚴格選項，則當無法進行所需的物件放置時（例如，因為新需要的位置不可用），不會採取任何措施。更新後的物件將保留其目前位置，直到可以實現所需的位置。</p> <p>解決衝突</p> <p>衝突的客戶端請求（例如兩個客戶端寫入同一個金鑰）將根據「最新勝利」的原則解決。「最新勝利」評估的時間取決於StorageGRID系統完成給定請求的時間，而不是 S3 用戶端開始操作的時間。</p> <p>版本控制</p> <p>如果 <code>versionId</code> 如果請求中未指定查詢參數，則操作會將標籤新增至版本化儲存桶中物件的最新版本。如果物件的目前版本是刪除標記，則傳回「MethodNotAllowed」狀態，並 <code>x-amz-delete-marker</code> 響應頭設定為 <code>true</code>。</p>
選擇對象內容	"選擇對象內容"

使用 S3 Select

StorageGRID支援以下 Amazon S3 Select 子句、資料類型和運算符"[SelectObjectContent 指令](#)"。



任何未列出的項目均不受支援。

有關語法，請參閱"[選擇對象內容](#)"。有關 S3 Select 的更多信息，請參閱 "[S3 Select 的 AWS 文檔](#)"。

只有啟用了 S3 Select 的租用戶帳戶才能發出 SelectObjectContent 查詢。查看"[使用 S3 Select 的注意事項和要求](#)"。

條款

- [選擇清單](#)

- FROM 子句
- WHERE 子句
- LIMIT 子句

資料類型

- 布林值
- 整數
- 細繩
- 漂浮
- 十進制，數字
- 時間戳

運算符

邏輯運算符

- 和
- 不是
- 或者

比較運算符

- <
- >
- <=
- >=
- =
- =
- <>
- !=
- 之間
- 在

模式匹配運算符

- 喜歡
- _
- %

廬正算子

- 為空
- 不為空

數學運算符

- +
- -
- *
- /
- %

StorageGRID遵循 Amazon S3 Select 運算子優先權。

聚合函數

- 平均值()
- 數數 (*)
- 最大限度 ()
- MIN()
- 和 ()

條件函數

- 案件
- 合併
- NULLIF

轉換函數

- CAST (針對支援的資料類型)

日期函數

- DATE_ADD
- 日期差異
- 提煉
- 至字串
- 到時間戳
- UTCNOW

字串函數

- 字元長度，字元長度
- 降低
- 子字串
- 修剪
- 上

使用伺服器端加密

伺服器端加密可讓您保護靜態的物件資料。StorageGRID在寫入物件時會對資料進行加密，並在您存取物件時解密資料。

如果您想使用伺服器端加密，您可以根據加密金鑰的管理方式選擇兩個互斥選項之一：

- **SSE**（使用StorageGRID管理金鑰的伺服器端加密）：當您發出 S3 請求來儲存物件時，StorageGRID會使用唯一金鑰加密該物件。當您發出 S3 請求來擷取物件時，StorageGRID會使用儲存的金鑰來解密該物件。
- **SSE-C**（使用客戶提供的金鑰進行伺服器端加密）：當您發出 S3 請求來儲存物件時，您需要提供自己的加密金鑰。當您檢索物件時，您會提供相同的加密金鑰作為請求的一部分。如果兩個加密金鑰匹配，則解密物件並傳回物件資料。

雖然StorageGRID管理所有物件加密和解密操作，但您必須管理您提供的加密金鑰。



您提供的加密金鑰永遠不會被儲存。如果遺失了加密金鑰，您就會遺失對應的物件。



如果使用 SSE 或 SSE-C 加密對象，則會忽略任何儲存桶層級或網格層級的加密設定。

使用 SSE

若要使用StorageGRID管理的唯一金鑰加密對象，請使用下列請求標頭：

```
x-amz-server-side-encryption
```

以下物件操作支援 SSE 請求頭：

- "放置對象"
- "複製對象"
- "建立多部分上傳"

使用 SSE-C

若要使用您管理的唯一密鑰加密對象，請使用三個請求標頭：

請求頭	描述
x-amz-server-side-encryption-customer-algorithm	指定加密算法。標頭值必須是 AES256。
x-amz-server-side-encryption-customer-key	指定用於加密或解密物件的加密金鑰。密鑰的值必須是 256 位元、base64 編碼的。
x-amz-server-side-encryption-customer-key-MD5	根據RFC 1321指定加密金鑰的MD5摘要，用於確保加密金鑰傳輸無誤。MD5 摘要的值必須是 base64 編碼的 128 位元。

以下物件操作支援 SSE-C 請求標頭：

- "取得對象"
- "頭部對象"
- "放置對象"
- "複製對象"
- "建立多部分上傳"
- "上傳部分"
- "上傳部分複製"

使用客戶提供的金鑰進行伺服器端加密 (SSE-C) 的注意事項

在使用 SSE-C 之前，請注意以下事項：

- 您必須使用 https。



使用 SSE-C 時，StorageGRID會拒絕任何透過 http 發出的請求。出於安全考慮，您應將任何意外使用 http 發送的密鑰視為已洩露。丟棄鑰匙，並進行適當的旋轉。

- 響應中的ETag不是物件資料的MD5。
- 您必須管理加密金鑰到物件的對應。StorageGRID不會儲存加密金鑰。您有責任追蹤為每個物件提供的加密金鑰。
- 如果您的儲存桶啟用了版本控制，則每個物件版本都應該有自己的加密金鑰。您有責任追蹤每個物件版本所使用的加密金鑰。
- 因為您在客戶端管理加密金鑰，所以您還必須在客戶端管理任何其他保護措施，例如金鑰輪換。



您提供的加密金鑰永遠不會被儲存。如果遺失了加密金鑰，您就會遺失對應的物件。

- 如果為儲存桶配置了跨網格複製或 CloudMirror 複製，則無法擷取 SSE-C 物件。攝取操作將會失敗。

相關資訊

"Amazon S3 使用者指南：使用客戶提供的金鑰進行伺服器端加密 (SSE-C)"

複製對象

您可以使用 S3 CopyObject 請求來建立已儲存在 S3 中的物件的副本。CopyObject 操作與執行 GetObject 後再執行 PutObject 操作相同。

解決衝突

衝突的客戶端請求（例如兩個客戶端寫入同一個金鑰）將根據「最新勝利」的原則解決。「最新勝利」評估的時間取決於StorageGRID系統完成給定請求的時間，而不是 S3 用戶端開始操作的時間。

物件大小

單一 PutObject 操作的最大_建議_大小為 5 GiB（5,368,709,120 位元組）。如果您有大於 5 GiB 的對象，請使用["分段上傳"](#)反而。

單一 PutObject 操作支援的最大大小為 5 TiB（5,497,558,138,880 位元組）。



如果您從StorageGRID 11.6 或更早版本升級，則當您嘗試上傳超過 5 GiB 的物件時，將觸發 S3 PUT 物件大小過大警報。如果您新安裝了StorageGRID 11.7 或 11.8，則在這種情況下不會觸發警報。但是，為了與 AWS S3 標準保持一致，StorageGRID的未來版本將不支援上傳大於 5 GiB 的物件。

用戶元資料中的 UTF-8 字符

如果請求在使用者定義元資料的鍵名或值中包含（未轉義的）UTF-8 值，則StorageGRID行為未定義。

StorageGRID不會解析或解釋使用者定義元資料的鍵名或值中包含的轉義 UTF-8 字元。轉義的 UTF-8 字元將被視為 ASCII 字元：

- 如果使用者定義的元資料包含轉義的 UTF-8 字符，則請求成功。
- StorageGRID不回傳 `x-amz-missing-meta` 如果鍵名或值的解釋值包含不可列印的字符，則為標頭。

支援的請求標頭

支援以下請求標頭：

- Content-Type
- x-amz-copy-source
- x-amz-copy-source-if-match
- x-amz-copy-source-if-none-match
- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-if-modified-since
- x-amz-meta-，後面跟著包含使用者定義元資料的名稱-值對
- x-amz-metadata-directive：預設值為 COPY，它使您能夠複製物件和相關元資料。

您可以指定 `REPLACE` 在複製物件時覆寫現有的元數據，或更新物件元數據。

- `x-amz-storage-class`
- `x-amz-tagging-directive`：預設值為 `COPY`，它使您能夠複製物件和所有標籤。

您可以指定 `REPLACE` 在複製物件時覆寫現有標籤，或更新標籤。

- S3 物件鎖定請求標頭：
 - `x-amz-object-lock-mode`
 - `x-amz-object-lock-retain-until-date`
 - `x-amz-object-lock-legal-hold`

如果發出的請求沒有這些標頭，則使用儲存桶預設保留設定來計算物件版本模式和保留截止日期。看"[使用 S3 REST API 設定 S3 物件鎖](#)"。

- SSE 請求標頭：
 - `x-amz-copy-source-server-side-encryption-customer-algorithm`
 - `x-amz-copy-source-server-side-encryption-customer-key`
 - `x-amz-copy-source-server-side-encryption-customer-key-MD5`
 - `x-amz-server-side-encryption`
 - `x-amz-server-side-encryption-customer-key-MD5`
 - `x-amz-server-side-encryption-customer-key`
 - `x-amz-server-side-encryption-customer-algorithm`

看[\[伺服器端加密的請求標頭\]](#)

不支援的請求標頭

不支援以下請求標頭：

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `If-Match`

⚠️ ``If-Match header` 已被接受，但無法正常使用。`

- `If-None-Match`

`If-None-Match` header`已被接受，但無法正常使用。

- `x-amz-checksum-algorithm`

當您複製物件時，如果來源物件具有校驗和，StorageGRID不會將該校驗和值複製到新物件。無論您是否嘗試使用`x-amz-checksum-algorithm`在物件請求中。

- `x-amz-website-redirect-location`

儲存類別選項

這`x-amz-storage-class`支援請求標頭，並且會影響StorageGRID在符合的 ILM 規則使用雙重提交或平衡時建立的物件副本數量"[攝取選項](#)"。

- STANDARD

(預設) 當 ILM 規則使用雙重提交選項時，或當平衡選項回退到建立臨時副本時，指定雙重提交接收操作。

- REDUCED_REDUNDANCY

當 ILM 規則使用雙重提交選項時，或當平衡選項回退到建立臨時副本時，指定單一提交攝取操作。



如果您將物件提取到啟用了 S3 物件鎖定的儲存桶中，則`REDUCED_REDUNDANCY`選項被忽略。如果您將物件提取到舊版相容儲存桶中，`REDUCED_REDUNDANCY`選項傳回錯誤。StorageGRID將始終執行雙重提交攝取以確保滿足合規性要求。

在 CopyObject 中使用 x-amz-copy-source

如果來源儲存桶和金鑰在`x-amz-copy-source`標頭與目標儲存桶和鍵不同，來源物件資料的副本將寫入目標。

如果來源和目標匹配，並且`x-amz-metadata-directive`標題指定為`REPLACE`，物件的元資料將使用請求中提供的元資料值進行更新。在這種情況下，StorageGRID不會重新擷取該物件。這有兩個重要後果：

- 您不能使用 CopyObject 來加密現有對象，或變更現有物件的加密。如果你提供`x-amz-server-side-encryption`標題或`x-amz-server-side-encryption-customer-algorithm`標題，StorageGRID拒絕請求並返回`XNotImplemented`。
- 不使用符合的 ILM 規則中指定的 Ingest Behavior 選項。當 ILM 由正常後台 ILM 程序重新評估時，將對更新觸發的物件位置進行任何變更。

這意味著，如果 ILM 規則對攝取行為使用嚴格選項，則當無法進行所需的物件放置時（例如，因為新需要的位置不可用），不會採取任何措施。更新後的物件將保留其目前位置，直到可以實現所需的位置。

伺服器端加密的請求標頭

如果你"[使用伺服器端加密](#)"，您提供的請求標頭取決於來源物件是否加密以及您是否計劃加密目標物件。

- 如果來源物件使用客戶提供的金鑰（SSE-C）加密，則必須在 CopyObject 請求中包含以下三個標頭，以便可以解密然後複製物件：

- `x-amz-copy-source-server-side-encryption-customer-algorithm`：指定 AES256。
- `x-amz-copy-source-server-side-encryption-customer-key`：指定您在建立來源物件時提供的加密金鑰。
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`：指定您在建立來源物件時提供的 MD5 摘要。
- 如果要使用您提供和管理的唯一密鑰加密目標物件（副本），請包含以下三個標頭：
 - `x-amz-server-side-encryption-customer-algorithm`：指定 AES256。
 - `x-amz-server-side-encryption-customer-key`：為目標對象指定新的加密金鑰。
 - `x-amz-server-side-encryption-customer-key-MD5`：指定新加密金鑰的 MD5 摘要。



您提供的加密金鑰永遠不會被儲存。如果遺失了加密金鑰，您就會遺失對應的物件。在使用客戶提供的金鑰保護物件資料之前，請先查看以下注意事項"使用伺服器端加密"。

- 如果要使用StorageGRID (SSE) 管理的唯一金鑰加密目標物件（副本），請在 `CopyObject` 請求中包含此標頭：
 - `x-amz-server-side-encryption`



這 `server-side-encryption`` 物件的值無法更新。相反，用新的 ``server-side-encryption`` 價值使用 ``x-amz-metadata-directive: REPLACE``。

版本控制

如果來源儲存桶已版本化，則可以使用 ``x-amz-copy-source`` 標頭來複製物件的最新版本。要複製物件的特定版本，必須使用 ``versionId`` 子資源。如果目標儲存桶有版本控制，則產生的版本將傳回 ``x-amz-version-id`` 響應標頭。如果目標儲存桶的版本控制已暫停，則 ``x-amz-version-id`` 傳回"null"值。

取得對象

您可以使用 S3 `GetObject` 請求從 S3 儲存桶中擷取物件。

`GetObject` 和多部分對象

您可以使用 ``partNumber`` 請求參數來檢索多部分或分段物件的特定部分。這 ``x-amz-mp-parts-count`` 響應元素指示物件有多少個部分。

您可以設定 ``partNumber`` 對於分段/多部分對象和非分段/非多部分對象，皆為 1；但是，``x-amz-mp-parts-count`` 響應元素僅針對分段或多部分物件傳回。

用戶元資料中的 UTF-8 字符

StorageGRID不會解析或解釋使用者定義元資料中的轉義 UTF-8 字元。對使用者定義元資料中含有轉義 UTF-8 字元的物件進行 GET 請求不會傳回 ``x-amz-missing-meta`` 如果鍵名或值包含不可列印的字符，則為標頭。

支援的請求標頭

支援以下請求標頭：

- `x-amz-checksum-mode`：指定 `ENABLED`

這 `Range` 標頭不支援 `x-amz-checksum-mode` 用於取得物件。當你包括 `Range` 在請求中 `x-amz-checksum-mode` 啟用後，StorageGRID 不會在回應中傳回校驗和值。

不支援的請求標頭

不支援以下請求標頭並返回 `XNotImplemented`：

- `x-amz-website-redirect-location`

版本控制

如果 `versionId` 如果未指定子資源，則操作將取得版本化儲存桶中物件的最新版本。如果物件的目前版本是刪除標記，則傳回「未找到」狀態，並 `x-amz-delete-marker` 響應頭設定為 `true`。

使用客戶提供的加密金鑰進行伺服器端加密的請求標頭 (SSE-C)

如果物件使用您提供的唯一密鑰加密，請使用所有三個標頭。

- `x-amz-server-side-encryption-customer-algorithm`：指定 `AES256`。
- `x-amz-server-side-encryption-customer-key`：指定物件的加密金鑰。
- `x-amz-server-side-encryption-customer-key-MD5`：指定物件加密金鑰的 MD5 摘要。



您提供的加密金鑰永遠不會被儲存。如果遺失了加密金鑰，您就會遺失對應的物件。在使用客戶提供的金鑰保護物件資料之前，請先查看["使用伺服器端加密"](#)。

雲端儲存池物件的 `GetObject` 行為

如果一個物件被儲存在"[雲端儲存池](#)"，`GetObject` 請求的行為取決於物件的狀態。看"[頭部對象](#)"了解更多詳情。



如果物件儲存在雲端儲存池中，並且該物件的一個或多個副本也存在於網格中，則 `GetObject` 請求將嘗試從網格中檢索數據，然後再從雲端儲存池中檢索資料。

物體狀態	<code>GetObject</code> 的行為
物件已匯入StorageGRID但尚未經過 ILM 評估，或儲存在傳統儲存池中使用擦除編碼的對象	200 OK 檢索物件的副本。
物件位於雲端儲存池中，但尚未轉換為不可檢索狀態	200 OK 檢索物件的副本。
物件已轉換為不可檢索狀態	403 Forbidden , InvalidObjectState 使用" 復原對象 "請求將物件恢復到可檢索狀態。

物體狀態	GetObject 的行為
物件正在從不可恢復狀態恢復	403 Forbidden , InvalidObjectState 等待 RestoreObject 請求完成。
物件已完全恢復到雲端儲存池	200 OK 檢索物件的副本。

雲端儲存池中的多部分或分段對象

如果您上傳了多部分對象，或者StorageGRID將大型對象拆分為多個段，StorageGRID會透過對該對象的部分或段的子集進行採樣來確定該對象是否在雲端儲存池中可用。在某些情況下，GetObject 請求可能會錯誤地傳回 `200 OK` 當物件的某些部分已轉換為不可檢索狀態或物件的某些部分尚未復原時。

在這些情況下：

- GetObject 請求可能會傳回一些數據，但在傳輸過程中停止。
- 後續的 GetObject 請求可能會傳回 403 Forbidden。

GetObject 和跨網格複製

如果您正在使用"網格聯盟"和"跨網格複製"為儲存桶啟用後，S3 用戶端可以透過發出 GetObject 請求來驗證物件的複製狀態。響應包括StorageGRID特定的 `x-ntap-sg-cgr-replication-status` 響應標頭，它將具有以下值之一：

網格	複製狀態
來源	<ul style="list-style-type: none"> • 已完成：複製成功。 • 待定：物件尚未被複製。 • 失敗：複製失敗，並發生永久性故障。使用者必須解決該錯誤。
目的地	REPLICA ：物件已從來源網格複製。



StorageGRID不支援 `x-amz-replication-status` 標頭。

頭部對象

您可以使用 S3 HeadObject 請求從物件中檢索元數據，而不回傳物件本身。如果物件儲存在雲端儲存池中，則可以使用 HeadObject 來確定物件的過渡狀態。

HeadObject 和多部分對象

您可以使用 `partNumber` 請求參數來檢索多部分或分段物件的特定部分的元資料。這 `x-amz-mp-parts-count` 響應元素指示物件有多少個部分。

您可以設定 `partNumber` 對於分段/多部分對象和非分段/非多部分對象，皆為 1；但是，`x-amz-mp-parts-

count` 響應元素僅針對分段或多部分物件傳回。

用戶元資料中的 **UTF-8** 字符

StorageGRID 不會解析或解釋使用者定義元資料中的轉義 UTF-8 字元。對使用者定義元資料中含有轉義 UTF-8 字元的物件進行 HEAD 請求不會傳回 `x-amz-missing-meta` 如果鍵名或值包含不可列印的字符，則為標頭。

支援的請求標頭

支援以下請求標頭：

- `x-amz-checksum-mode`

這 `partNumber` 參數和 `Range` 標頭不支援 `x-amz-checksum-mode` 對於 HeadObject。當您將它們包含在請求中時 `x-amz-checksum-mode` 啟用後，StorageGRID 不會在回應中傳回校驗和值。

不支援的請求標頭

以下請求標頭不受支援並返回 XNotImplemented：

- `x-amz-website-redirect-location`

版本控制

如果 `versionId` 如果未指定子資源，則操作將取得版本化儲存桶中物件的最新版本。如果物件的目前版本是刪除標記，則傳回「未找到」狀態，並 `x-amz-delete-marker` 響應頭設定為 `true`。

使用客戶提供的加密金鑰進行伺服器端加密的請求標頭 (**SSE-C**)

如果物件使用您提供的唯一密鑰加密，請使用所有這三個標頭。

- `x-amz-server-side-encryption-customer-algorithm`：指定 AES256。
- `x-amz-server-side-encryption-customer-key`：指定物件的加密金鑰。
- `x-amz-server-side-encryption-customer-key-MD5`：指定物件加密金鑰的 MD5 摘要。



您提供的加密金鑰永遠不會被儲存。如果遺失了加密金鑰，您就會遺失對應的物件。在使用客戶提供的金鑰保護物件資料之前，請先查看["使用伺服器端加密"](#)。

Cloud Storage Pool 物件的 HeadObject 回應

如果物件儲存在["雲端儲存池"](#)，將返回以下響應標頭：

- `x-amz-storage-class`: GLACIER
- `x-amz-restore`

回應標頭提供有關物件狀態的信息，因為它被移動到雲端儲存池，可選地轉換為不可檢索狀態，並恢復。

物體狀態	對 HeadObject 的回應
物件已匯入StorageGRID但尚未經過 ILM 評估，或儲存在傳統儲存池中或使用擦除編碼的對象	200 OK (沒有回傳特殊的回應頭。)
物件位於雲端儲存池中，但尚未轉換為不可檢索狀態	200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT" 在物件轉換為不可檢索狀態之前，`expiry-date`設定為未來某個遙遠的時間。轉換的確切時間不受StorageGRID系統控制。
物件已轉換為不可檢索狀態，但網格上還存在至少一個副本	200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT" 價值 `expiry-date` 設定為未來某個遙遠的時間。 注意：如果網格上的副本不可用（例如，儲存節點關閉），則必須發出"復原對象"請求從雲端儲存池恢復副本，然後才能成功檢索物件。
物件已轉換為不可檢索狀態，且網格上不存在副本	200 OK x-amz-storage-class: GLACIER
物件正在從不可恢復狀態恢復	200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="true"

物體狀態	對 HeadObject 的回應
物件已完全恢復到雲端儲存池	<pre>200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT" 這 `expiry-date` 指示雲端儲存池中的物件何時將返回不可檢索狀態。</pre>

雲端儲存池中的多部分或分段對象

如果您上傳了多部分對象，或者StorageGRID將大型對象拆分為多個段，StorageGRID會透過對該對象的部分或段的子集進行採樣來確定該對象是否在雲端儲存池中可用。在某些情況下，HeadObject 請求可能會錯誤地傳回 `x-amz-restore: ongoing-request="false"` 當物件的某些部分已轉換為不可檢索狀態或物件的某些部分尚未復原時。

HeadObject 和跨網格複製

如果您正在使用"網格聯盟"和"跨網格複製"為儲存桶啟用後，S3 用戶端可以透過發出 HeadObject 請求來驗證物件的複製狀態。響應包括StorageGRID特定的 `x-ntap-sg-cgr-replication-status` 響應標頭，它將具有以下值之一：

網格	複製狀態
來源	<ul style="list-style-type: none"> • 已完成：複製成功。 • 待定：物件尚未被複製。 • 失敗：複製失敗，並發生永久性故障。使用者必須解決該錯誤。
目的地	REPLICA ：物件已從來源網格複製。



StorageGRID不支援 `x-amz-replication-status` 標頭。

放置對象

您可以使用 S3 PutObject 請求將物件新增至儲存桶。

解決衝突

衝突的客戶端請求（例如兩個客戶端寫入同一個金鑰）將根據「最新勝利」的原則解決。「最新勝利」評估的時間取決於StorageGRID系統完成給定請求的時間，而不是 S3 用戶端開始操作的時間。

物件大小

單一 PutObject 操作的最大_建議_大小為 5 GiB（5,368,709,120 位元組）。如果您有大於 5 GiB 的對象，請使

用"分段上傳"反而。

單一 PutObject 操作支援的最大大小為 5 TiB (5,497,558,138,880 位元組)。



如果您從StorageGRID 11.6 或更早版本升級，則當您嘗試上傳超過 5 GiB 的物件時，將觸發 S3 PUT 物件大小過大警報。如果您新安裝了StorageGRID 11.7 或 11.8，則在這種情況下不會觸發警報。但是，為了與 AWS S3 標準保持一致，StorageGRID的未來版本將不支援上傳大於 5 GiB 的物件。

用戶元資料大小

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。StorageGRID將用戶元資料限制為 24 KiB。使用者定義元資料的大小是透過計算每個鍵和值的 UTF-8 編碼的位元組數總和來衡量的。

用戶元資料中的 UTF-8 字符

如果請求在使用者定義元資料的鍵名或值中包含（未轉義的）UTF-8 值，則StorageGRID行為未定義。

StorageGRID不會解析或解釋使用者定義元資料的鍵名或值中包含的轉義 UTF-8 字元。轉義的 UTF-8 字元將被視為 ASCII 字元：

- 如果使用者定義的元資料包含轉義的 UTF-8 字符，則 PutObject、CopyObject、GetObject 和 HeadObject 請求會成功。
- StorageGRID不回傳 `x-amz-missing-meta` 如果鍵名或值的解釋值包含不可列印的字符，則為標頭。

對象標籤限制

您可以在上傳新物件時為其新增標籤，也可以將其新增至現有物件中。StorageGRID和 Amazon S3 都支援每個物件最多 10 個標籤。與物件關聯的標籤必須具有唯一的標籤鍵。標籤鍵的長度最多為 128 個 Unicode 字符，標籤值的長度最多為 256 個 Unicode 字元。鍵和值區分大小寫。

物件所有權

在StorageGRID中，所有物件都歸儲存桶擁有者帳戶所有，包括由非擁有者帳戶或匿名使用者建立的物件。

支援的請求標頭

支援以下請求標頭：

- Cache-Control
- Content-Disposition
- Content-Encoding

當您指定 `aws-chunked` 為了Content-EncodingStorageGRID不驗證下列項目：

- StorageGRID不驗證 `chunk-signature` 針對區塊資料。
- StorageGRID不會驗證您提供的值 `x-amz-decoded-content-length` 針對該對象。
- Content-Language

- Content-Length
- Content-MD5
- Content-Type
- Expires
- Transfer-Encoding

如果支援分塊傳輸編碼 `aws-chunked` 也使用了有效載荷簽名。

- x-amz-checksum-sha256
- x-amz-meta-，後面跟著包含使用者定義元資料的名稱-值對。

為使用者定義的元資料指定名稱-值對時，請使用下列通用格式：

```
x-amz-meta-name: value
```

如果要使用 使用者定義建立時間 選項作為 ILM 規則的參考時間，則必須使用 `creation-time` 作為記錄物件建立時間的元資料的名稱。例如：

```
x-amz-meta-creation-time: 1443399726
```

價值 `creation-time` 以 1970 年 1 月 1 日以來的秒數計算。



ILM 規則不能同時使用 使用者定義的創建時間 作為參考時間以及平衡或嚴格的攝取選項。建立 ILM 規則時傳回錯誤。

- x-amz-tagging
- S3 物件鎖定請求標頭
 - x-amz-object-lock-mode
 - x-amz-object-lock-retain-until-date
 - x-amz-object-lock-legal-hold

如果發出的請求沒有這些標頭，則使用儲存桶預設保留設定來計算物件版本模式和保留截止日期。看["使用 S3 REST API 設定 S3 物件鎖"](#)。

- SSE 請求標頭：
 - x-amz-server-side-encryption
 - x-amz-server-side-encryption-customer-key-MD5
 - x-amz-server-side-encryption-customer-key
 - x-amz-server-side-encryption-customer-algorithm

看[\[伺服器端加密的請求標頭\]](#)

不支援的請求標頭

不支援以下請求標頭：

- If-Match

``If-Match header`` 已被接受，但無法正常使用。

- If-None-Match

``If-None-Match header`` 已被接受，但無法正常使用。

- x-amz-acl
- x-amz-sdk-checksum-algorithm
- x-amz-trailer
- x-amz-website-redirect-location

這 `x-amz-website-redirect-location`` 標題返回 ``XNotImplemented``。

儲存類別選項

這 ``x-amz-storage-class`` 支援請求標頭。提交的價值 ``x-amz-storage-class`` 影響 StorageGRID 在攝取期間如何保護物件數據，而不是影響 StorageGRID 系統中儲存了多少個物件的持久副本（由 ILM 決定）。

如果與已攝取物件相符的 ILM 規則使用嚴格攝取選項，``x-amz-storage-class`` 標頭無效。

以下值可用於 `x-amz-storage-class``：

- STANDARD(預設)
 - 雙重提交：如果 ILM 規則為攝取行為指定了雙重提交選項，則一旦攝取對象，就會建立該對象的第二個副本並分發到不同的儲存節點（雙重提交）。在評估 ILM 時，StorageGRID 會決定這些初始臨時副本是否符合規則中的放置說明。如果沒有，則可能需要在不同位置製作新的物件副本，並且可能需要刪除初始臨時副本。
 - 平衡：如果 ILM 規則指定了平衡選項，且 StorageGRID 無法立即製作規則中指定的所有副本，StorageGRID 會在不同的儲存節點上製作兩個暫存副本。

如果 StorageGRID 可以立即建立 ILM 規則中指定的所有物件副本（同步放置），則 ``x-amz-storage-class`` 標頭無效。

- REDUCED_REDUNDANCY
 - 雙重提交：如果 ILM 規則為攝取行為指定了雙重提交選項，則 StorageGRID 會在攝取物件時建立單一暫存副本（單次提交）。
 - 平衡：如果 ILM 規則指定了平衡選項，則僅當系統無法立即製作規則中指定的所有副本時，StorageGRID 才會製作單一暫存副本。如果 StorageGRID 可以執行同步放置，則此標頭無效。這

`REDUCED_REDUNDANCY` 當與物件相符的 ILM 規則建立單一複製副本時，最好使用此選項。在這種情況下使用 `REDUCED_REDUNDANCY` 消除了每次攝取操作時不必要的額外物件副本的建立和刪除。

使用 `REDUCED_REDUNDANCY` 在其他情況下不建議選擇此選項。`REDUCED_REDUNDANCY` 增加了攝取過程中物件資料遺失的風險。例如，如果單一副本最初儲存在儲存節點上，而該儲存節點在 ILM 評估發生之前發生故障，則您可能會遺失資料。



任何時間段內只有一個複製副本會使資料面臨永久遺失的風險。如果某個物件的副本只有一個，則當儲存節點發生故障或發生重大錯誤時，該物件將會遺失。在升級等維護過程中，您也會暫時失去對該物件的存取權限。

指定 `REDUCED_REDUNDANCY` 僅影響首次攝取物件時所建立的副本數量。它不會影響活動 ILM 策略評估物件時產生的物件副本數量，也不會導致資料在 StorageGRID 系統中以較低的冗餘層級進行儲存。



如果您將物件提取到啟用了 S3 物件鎖定的儲存桶中，則 `REDUCED_REDUNDANCY` 選項被忽略。如果您將物件提取到舊版相容儲存桶中，`REDUCED_REDUNDANCY` 選項傳回錯誤。StorageGRID 將始終執行雙重提交攝取以確保滿足合規性要求。

伺服器端加密的請求標頭

您可以使用下列請求標頭來使用伺服器端加密來加密物件。SSE 和 SSE-C 選項是互斥的。

- **SSE**：如果您想要使用由 StorageGRID 管理的唯一金鑰加密對象，請使用下列標頭。

- `x-amz-server-side-encryption`

當 `x-amz-server-side-encryption` 標頭未包含在 PutObject 請求中，網格範圍的"儲存物件加密設定"從 PutObject 回應中省略。

- **SSE-C**：如果您想使用您提供和管理的唯一金鑰加密對象，請使用所有這三個標頭。

- `x-amz-server-side-encryption-customer-algorithm`：指定 AES256。

- `x-amz-server-side-encryption-customer-key`：為新物件指定加密金鑰。

- `x-amz-server-side-encryption-customer-key-MD5`：指定新物件的加密金鑰的 MD5 摘要。



您提供的加密金鑰永遠不會被儲存。如果遺失了加密金鑰，您就會遺失對應的物件。在使用客戶提供的金鑰保護物件資料之前，請先查看以下注意事項"使用伺服器端加密"。



如果使用 SSE 或 SSE-C 加密對象，則會忽略任何儲存桶層級或網格層級的加密設定。

版本控制

如果為儲存桶啟用了版本控制，則唯一的 `versionId` 針對所儲存物件的版本會自動產生。這 `versionId` 也會在回應中返回 `x-amz-version-id` 響應頭。

如果版本控制暫停，則物件版本將以空值儲存 `versionId` 如果空版本已經存在，它將被覆蓋。

授權標頭的簽章計算

使用時 `Authorization` 標頭來驗證請求，StorageGRID 與 AWS 有以下不同：

- StorageGRID 不需要 `host` 標頭包含在 ``CanonicalHeaders``。
- StorageGRID 不需要 `Content-Type` 被納入 ``CanonicalHeaders``。
- StorageGRID 不需要 `x-amz-*` 標頭包含在 ``CanonicalHeaders``。



作為一般的最佳做法，請始終將這些標頭包含在 ``CanonicalHeaders`` 以確保它們已被驗證；但是，如果排除這些標頭，StorageGRID 不會傳回錯誤。

有關詳細信息，請參閱 ["授權標頭的簽章計算：在單一區塊中傳輸有效負載 \(AWS 簽章版本 4\)"](#)。

相關資訊

- ["使用 ILM 管理對象"](#)
- ["Amazon Simple Storage Service API 參考：PutObject"](#)

復原對象

您可以使用 S3 `RestoreObject` 請求來還原儲存在雲端儲存池中的物件。

支援的請求類型

StorageGRID 僅支援 `RestoreObject` 請求來還原物件。它不支援 `SELECT` 修復類型。選擇請求返回 ``XNotImplemented``。

版本控制

(可選) 指定 `versionId` 還原受版本控制的儲存桶中物件的特定版本。如果你沒有指定 ``versionId``，該物件的最新版本已恢復。

RestoreObject 在雲端儲存池物件上的行為

如果一個物件被儲存在 ["雲端儲存池"](#)，根據物件的狀態，`RestoreObject` 請求具有以下行為。看 ["頭部對象"](#) 了解更多詳情。



如果物件儲存在雲端儲存池中，且該物件的一個或多個副本也存在於網格上，則無需透過發出 `RestoreObject` 請求來還原該物件。相反，可以使用 `GetObject` 請求直接檢索本機副本。

物體狀態	RestoreObject 的行為
物件已匯入 StorageGRID 但尚未由 ILM 評估，或物件不在雲端儲存池中	403 Forbidden, InvalidObjectState
物件位於雲端儲存池中，但尚未轉換為不可檢索狀態	<code>`200 OK`</code> 沒有做出任何改變。 注意：在物件轉換為不可檢索狀態之前，您無法變更其 <code>expiry-date</code> 。

物體狀態	RestoreObject 的行為
物件已轉換為不可檢索狀態	<p>`202 Accepted` 將物件的可檢索副本還原到雲端儲存池，保留天數為請求正文中指定的天數。在此期限結束時，物件將返回到不可檢索的狀態。</p> <p>或者，使用 Tier 請求元素來決定還原作業需要多長時間才能完成（`Expedited`，`Standard`，或者 `Bulk`）。如果你沒有指定 Tier，這 `Standard` 層被使用。</p> <p>重要：如果物件已轉換到 S3 Glacier Deep Archive 或雲端儲存池使用 Azure Blob 存儲，則無法使用 Expedited 層。傳回以下錯誤 `403 Forbidden, InvalidTier: Retrieval option is not supported by this storage class`。</p>
物件正在從不可恢復狀態恢復	409 Conflict, RestoreAlreadyInProgress
物件已完全恢復到雲端儲存池	<p>200 OK</p> <p>*注意：*如果物件已恢復到可檢索狀態，您可以變更其 expiry-date 透過重新發出 RestoreObject 請求並使用新值 `Days`。恢復日期根據請求的時間進行更新。</p>

選擇對象內容

您可以使用 S3 SelectObjectContent 請求根據簡單的 SQL 語句過濾 S3 物件的內容。

有關詳細信息，請參閱 "[Amazon Simple Storage Service API 參考：SelectObjectContent](#)"。

開始之前

- 租用戶帳戶具有 S3 Select 權限。
- 你有 `s3:GetObject` 您要查詢的物件的權限。
- 您要查詢的物件必須採用以下格式之一：
 - **CSV**。可原樣使用或壓縮為 GZIP 或 BZIP2 檔案。
 - 鑲木地板。Parquet 物件的附加要求：
 - S3 Select 僅支援使用 GZIP 或 Snappy 進行列壓縮。S3 Select 不支援 Parquet 物件的整個物件壓縮。
 - S3 Select 不支援 Parquet 輸出。您必須將輸出格式指定為 CSV 或 JSON。
 - 未壓縮的行組最大大小為 512 MB。
 - 您必須使用物件模式中指定的資料類型。
 - 您不能使用 INTERVAL、JSON、LIST、TIME 或 UUID 邏輯類型。
- 您的 SQL 表達式的最大長度為 256 KB。
- 輸入或結果中的任何記錄的最大長度為 1 MiB。

CSV 請求語法範例

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Expression>string</Expression>
  <ExpressionType>string</ExpressionType>
  <RequestProgress>
    <Enabled>boolean</Enabled>
  </RequestProgress>
  <InputSerialization>
    <CompressionType>GZIP</CompressionType>
    <CSV>
      <AllowQuotedRecordDelimiter>boolean</AllowQuotedRecordDelimiter>
      <Comments>#</Comments>
      <FieldDelimiter>\t</FieldDelimiter>
      <FileHeaderInfo>USE</FileHeaderInfo>
      <QuoteCharacter>'</QuoteCharacter>
      <QuoteEscapeCharacter>\\</QuoteEscapeCharacter>
      <RecordDelimiter>\n</RecordDelimiter>
    </CSV>
  </InputSerialization>
  <OutputSerialization>
    <CSV>
      <FieldDelimiter>string</FieldDelimiter>
      <QuoteCharacter>string</QuoteCharacter>
      <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
      <QuoteFields>string</QuoteFields>
      <RecordDelimiter>string</RecordDelimiter>
    </CSV>
  </OutputSerialization>
  <ScanRange>
    <End>long</End>
    <Start>long</Start>
  </ScanRange>
</SelectObjectContentRequest>
```

Parquet 請求語法範例

```

POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns=http://s3.amazonaws.com/doc/2006-03-01/>
  <Expression>string</Expression>
  <ExpressionType>string</ExpressionType>
  <RequestProgress>
    <Enabled>boolean</Enabled>
  </RequestProgress>
  <InputSerialization>
    <CompressionType>GZIP</CompressionType>
    <PARQUET>
    </PARQUET>
  </InputSerialization>
  <OutputSerialization>
    <CSV>
      <FieldDelimiter>string</FieldDelimiter>
      <QuoteCharacter>string</QuoteCharacter>
      <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
      <QuoteFields>string</QuoteFields>
      <RecordDelimiter>string</RecordDelimiter>
    </CSV>
  </OutputSerialization>
  <ScanRange>
    <End>long</End>
    <Start>long</Start>
  </ScanRange>
</SelectObjectContentRequest>

```

SQL 查詢範例

此查詢取得州名稱、2010 年人口、估計 2015 年人口以及美國人口普查資料的變化百分比。文件中非狀態的記錄將被忽略。

```

SELECT STNAME, CENSUS2010POP, POPESTIMATE2015, CAST((POPESTIMATE2015 -
CENSUS2010POP) AS DECIMAL) / CENSUS2010POP * 100.0 FROM S3Object WHERE
NAME = STNAME

```

要查詢的文件的前幾行，SUB-EST2020_ALL.csv，看起來像這樣：

```
SUMLEV, STATE, COUNTY, PLACE, COUSUB, CONCIT, PRIMGEO_FLAG, FUNCSTAT, NAME, STNAME,
CENSUS2010POP,
ESTIMATESBASE2010, POPESTIMATE2010, POPESTIMATE2011, POPESTIMATE2012, POPESTIM
ATE2013, POPESTIMATE2014,
POPESTIMATE2015, POPESTIMATE2016, POPESTIMATE2017, POPESTIMATE2018, POPESTIMAT
E2019, POPESTIMATE042020,
POPESTIMATE2020
040, 01, 000, 00000, 00000, 00000, 0, A, Alabama, Alabama, 4779736, 4780118, 4785514, 4
799642, 4816632, 4831586,
4843737, 4854803, 4866824, 4877989, 4891628, 4907965, 4920706, 4921532
162, 01, 000, 00124, 00000, 00000, 0, A, Abbeville
city, Alabama, 2688, 2705, 2699, 2694, 2645, 2629, 2610, 2602,
2587, 2578, 2565, 2555, 2555, 2553
162, 01, 000, 00460, 00000, 00000, 0, A, Adamsville
city, Alabama, 4522, 4487, 4481, 4474, 4453, 4430, 4399, 4371,
4335, 4304, 4285, 4254, 4224, 4211
162, 01, 000, 00484, 00000, 00000, 0, A, Addison
town, Alabama, 758, 754, 751, 750, 745, 744, 742, 734, 734, 728,
725, 723, 719, 717
```

AWS-CLI 使用範例 (CSV)

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--no-verify-ssl --bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.csv --expression-type SQL --input-serialization '{"CSV":
{"FileHeaderInfo": "USE", "Comments": "#", "QuoteEscapeCharacter": "\"",
"RecordDelimiter": "\n", "FieldDelimiter": ",", "QuoteCharacter": "\"",
"AllowQuotedRecordDelimiter": false}, "CompressionType": "NONE"}' --output
-serialization '{"CSV": {"QuoteFields": "ASNEEDED",
"QuoteEscapeCharacter": "#", "RecordDelimiter": "\n", "FieldDelimiter":
",", "QuoteCharacter": "\"}}}' --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" changes.csv
```

輸出文件的前幾行，changes.csv，看起來像這樣：

```
Alabama, 4779736, 4854803, 1.5705260708959658022953568983726297854
Alaska, 710231, 738430, 3.9703983633493891424057806544631253775
Arizona, 6392017, 6832810, 6.8959922978928247531256565807005832431
Arkansas, 2915918, 2979732, 2.1884703204959810255295244928012378949
California, 37253956, 38904296, 4.4299724839960620557988526104449148971
Colorado, 5029196, 5454328, 8.4532796097030221132761578590295546246
```

AWS-CLI 使用範例 (Parquet)

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.parquet --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" --expression-type
'SQL' --input-serialization '{"Parquet":{}}' --output-serialization
'{"CSV":{}}' changes.csv
```

輸出檔 changes.csv 的前幾行如下：

```
Alabama,4779736,4854803,1.5705260708959658022953568983726297854
Alaska,710231,738430,3.9703983633493891424057806544631253775
Arizona,6392017,6832810,6.8959922978928247531256565807005832431
Arkansas,2915918,2979732,2.1884703204959810255295244928012378949
California,37253956,38904296,4.4299724839960620557988526104449148971
Colorado,5029196,5454328,8.4532796097030221132761578590295546246
```

分段上傳的操作

分段上傳的操作

本節介紹StorageGRID如何支援分段上傳操作。

以下條件和注意事項適用於所有分段上傳操作：

- 單一儲存桶的並發分段上傳不應超過 1,000 個，因為該儲存桶的 ListMultipartUploads 查詢結果可能會傳回不完整的結果。
- StorageGRID對多部分元件強制實施 AWS 大小限制。S3 用戶端必須遵循以下準則：
 - 分段上傳中的每個部分必須介於 5 MiB (5,242,880 位元組) 和 5 GiB (5,368,709,120 位元組) 之間。
 - 最後一部分可以小於 5 MiB (5,242,880 位元組)。
 - 一般來說，零件尺寸應盡可能大。例如，對於 100 GiB 的對象，使用 5 GiB 的部分大小。由於每個部分都被視為唯一對象，因此使用較大部分大小可以減少StorageGRID元資料開銷。
 - 對於小於 5 GiB 的對象，請考慮使用非分段上傳。
- 如果 ILM 規則使用「平衡」或「嚴格」模式，則在分段上傳完成時，將對分段物件的每個部分進行 ILM 評估；如果 ILM 規則使用「平衡」或「嚴格」模式，則將對整個物件進行 ILM 評估。["攝取選項"](#)。您應該了解這會影響物件和部件的放置：
 - 如果在 S3 分段上傳過程中 ILM 發生變化，則分段上傳完成時物件的某些部分可能不符合目前的 ILM 要求。任何未正確放置的部件都會排隊等待 ILM 重新評估，然後移動到正確的位置。
 - 在評估某個零件的 ILM 時，StorageGRID會根據該零件的大小進行過濾，而不是物件的大小。這意味著物件的各個部分可以儲存在不滿足物件整體的 ILM 要求的位置。例如，如果規則指定所有 10 GB 或更大的物件都儲存在 DC1，而所有較小的物件都儲存在 DC2，則 10 部分分段上傳的每個 1 GB 部分在攝取

時都儲存在 DC2。但是，當對整個物件進行 ILM 評估時，物件的所有部分都會移至 DC1。

- 所有分段上傳操作都支援StorageGRID"一致性值"。
- 當使用分段上傳提取物件時，"物件分割閾值（1 GiB）"不適用。
- 根據需要，您可以使用"伺服器端加密"使用分段上傳。若要使用 SSE（使用StorageGRID管理金鑰的伺服器端加密），您需要包含 `x-amz-server-side-encryption` 僅在 CreateMultipartUpload 請求中的請求標頭。若要使用 SSE-C（使用客戶提供的金鑰的伺服器端加密），您需要在 CreateMultipartUpload 請求和每個後續 UploadPart 請求中指定相同的三個加密金鑰請求標頭。

手術	執行
中止分段上傳	使用所有 Amazon S3 REST API 行為實作。如有變更，恕不另行通知。
完成多部分上傳	看" 完成多部分上傳 "
建立多部分上傳 (之前名為「啟動分段上傳」)	看" 建立多部分上傳 "
列出多部分上傳	看" 列出多部分上傳 "
列出零件	使用所有 Amazon S3 REST API 行為實作。如有變更，恕不另行通知。
上傳部分	看" 上傳部分 "
上傳部分複製	看" 上傳部分複製 "

完成多部分上傳

CompleteMultipartUpload 作業透過組裝先前上傳的部分來完成物件的分段上傳。



StorageGRID支援按升序排列非連續值 `partNumber` 請求參數與CompleteMultipartUpload一致。此參數可以以任意值開頭。

解決衝突

衝突的客戶端請求（例如兩個客戶端寫入同一個金鑰）將根據「最新勝利」的原則解決。「最新勝利」評估的時間取決於StorageGRID系統完成給定請求的時間，而不是 S3 用戶端開始操作的時間。

支援的請求標頭

支援以下請求標頭：

- `x-amz-checksum-sha256`
- `x-amz-storage-class`

這 `x-amz-storage-class` StorageGRID 符合的 ILM 規則指定了"雙重提交或平衡攝取選項"。

- STANDARD

(預設) 當 ILM 規則使用雙重提交選項時，或當平衡選項回退到建立臨時副本時，指定雙重提交接收操作。

- REDUCED_REDUNDANCY

當 ILM 規則使用雙重提交選項時，或當平衡選項回退到建立臨時副本時，指定單一提交攝取操作。



如果您將物件提取到啟用了 S3 物件鎖定的儲存桶中，則 `REDUCED_REDUNDANCY` 選項被忽略。如果您將物件提取到舊版相容儲存桶中，`REDUCED_REDUNDANCY` 選項傳回錯誤。StorageGRID 將始終執行雙重提交攝取以確保滿足合規性要求。



如果分段上傳未在 15 天內完成，則該操作將標記為非活動狀態，並且所有相關資料將從系統中刪除。



這 `ETag` 傳回的值不是資料的 MD5 和，而是遵循 Amazon S3 API 實現的 `ETag` 多部分物件的值。

不支援的請求標頭

不支援以下請求標頭：

- If-Match

`If-Match` header 已被接受，但無法正常使用。

- If-None-Match

`If-None-Match` header 已被接受，但無法正常使用。

- x-amz-sdk-checksum-algorithm
- x-amz-trailer

版本控制

此操作完成分段上傳。如果儲存桶啟用了版本控制，則在分段上傳完成後會建立物件版本。

如果為儲存桶啟用了版本控制，則唯一的 `versionId` 針對所儲存物件的版本會自動產生。這 `versionId` 也會在回應中返回 `x-amz-version-id` 響應頭。

如果版本控制暫停，則物件版本將以空值儲存 `versionId` 如果空版本已經存在，它將被覆蓋。



當為儲存桶啟用版本控制時，完成分段上傳總是會建立一個新版本，即使在同一個物件鍵上完成了並發分段上傳。當儲存桶未啟用版本控制時，可以啟動分段上傳，然後讓另一個分段上傳先在同一個物件鍵上啟動並完成。在非版本化儲存桶上，最後完成的分段上傳具有優先權。

複製、通知或元資料通知失敗

如果發生分段上傳的儲存桶配置了平台服務，即使相關的複製或通知操作失敗，分段上傳也會成功。

租用戶可以透過更新物件的元資料或標籤來觸發失敗的複製或通知。租戶可以重新提交現有值以避免做出不必要的更改。

請參閱["平台服務故障排除"](#)。

建立多部分上傳

CreateMultipartUpload（以前稱為 Initiate Multipart Upload）操作為物件啟動分段上傳，並傳回上傳 ID。

這 `x-amz-storage-class` 支援請求標頭。提交的價值 `x-amz-storage-class` 影響 StorageGRID 在攝取期間如何保護物件數據，而不是影響 StorageGRID 系統中儲存了多少個物件的持久副本（由 ILM 決定）。

如果與已攝取物件相符的 ILM 規則使用嚴格 ["攝取選項"](#)，這 `x-amz-storage-class` 標頭無效。

以下值可用於 `x-amz-storage-class`：

- STANDARD(預設)
 - 雙重提交：如果 ILM 規則指定了雙重提交攝取選項，則一旦攝取對象，就會建立該對象的第二個副本並將其分發到不同的儲存節點（雙重提交）。在評估 ILM 時，StorageGRID 會決定這些初始臨時副本是否符合規則中的放置說明。如果沒有，則可能需要在不同位置製作新的物件副本，並且可能需要刪除初始臨時副本。
 - 平衡：如果 ILM 規則指定了平衡選項，且 StorageGRID 無法立即製作規則中指定的所有副本，StorageGRID 會在不同的儲存節點上製作兩個暫存副本。

如果 StorageGRID 可以立即建立 ILM 規則中指定的所有物件副本（同步放置），則 `x-amz-storage-class` 標頭無效。

- REDUCED_REDUNDANCY
 - 雙重提交：如果 ILM 規則指定了雙重提交選項，StorageGRID 會在物件被攝取時建立一個臨時副本（單次提交）。
 - 平衡：如果 ILM 規則指定了平衡選項，則僅當系統無法立即製作規則中指定的所有副本時，StorageGRID 才會製作單一暫存副本。如果 StorageGRID 可以執行同步放置，則此標頭無效。這 `REDUCED_REDUNDANCY` 當與物件相符的 ILM 規則建立單一複製副本時，最好使用此選項。在這種情況下使用 `REDUCED_REDUNDANCY` 消除了每次攝取操作時不必要的額外物件副本的建立和刪除。

使用 `REDUCED_REDUNDANCY` 在其他情況下不建議選擇此選項。`REDUCED_REDUNDANCY` 增加了攝取過程中物件資料遺失的風險。例如，如果單一副本最初儲存在儲存節點上，而該儲存節點在 ILM 評估發生之前發生故障，則您可能會遺失資料。



任何時間段內只有一個複製副本會使資料面臨永久遺失的風險。如果某個物件的副本只有一個，則當儲存節點發生故障或發生重大錯誤時，該物件將會遺失。在升級等維護過程中，您也會暫時失去對該物件的存取權限。

指定 `REDUCED_REDUNDANCY` 僅影響首次攝取物件時所建立的副本數量。它不會影響活動 ILM 策略評估物件時產生的物件副本數量，也不會導致資料在 StorageGRID 系統中以較低的冗餘層級進行儲存。



如果您將物件提取到啟用了 S3 物件鎖定的儲存桶中，則 `REDUCED_REDUNDANCY` 選項被忽略。如果您將物件提取到舊版相容儲存桶中，`REDUCED_REDUNDANCY` 選項傳回錯誤。StorageGRID 將始終執行雙重提交攝取以確保滿足合規性要求。

支援的請求標頭

支援以下請求標頭：

- Content-Type
- x-amz-checksum-algorithm

目前，只有 `x-amz-checksum-algorithm` 受支持。

- x-amz-meta-，後面跟著包含使用者定義元資料的名稱-值對

為使用者定義的元資料指定名稱-值對時，請使用下列通用格式：

```
x-amz-meta-__name__: `value`
```

如果要使用 使用者定義建立時間 選項作為 ILM 規則的參考時間，則必須使用 `creation-time` 作為記錄物件建立時間的元資料的名稱。例如：

```
x-amz-meta-creation-time: 1443399726
```

價值 `creation-time` 以 1970 年 1 月 1 日以後的秒數計算。



添加 `creation-time` 因為如果您將物件新增至已啟用舊版合規性的儲存桶，則不允許使用者定義的元資料。將返回錯誤。

- S3 物件鎖定請求標頭：
 - x-amz-object-lock-mode
 - x-amz-object-lock-retain-until-date
 - x-amz-object-lock-legal-hold

如果發出的請求沒有這些標頭，則使用儲存桶預設保留設定來計算物件版本的保留截止日期。

["使用 S3 REST API 設定 S3 物件鎖"](#)

- SSE 請求標頭：

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

[伺服器端加密的請求標頭]



有關StorageGRID如何處理 UTF-8 字元的信息，請參閱["放置對象"](#)。

伺服器端加密的請求標頭

您可以使用下列請求標頭透過伺服器端加密來加密多部分物件。SSE 和 SSE-C 選項是互斥的。

- **SSE**：如果您想使用由StorageGRID管理的唯一金鑰加密對象，請在 CreateMultipartUpload 請求中使用下列標頭。不要在任何 UploadPart 請求中指定此標頭。
 - x-amz-server-side-encryption
- **SSE-C**：如果您想使用您提供和管理的唯一密鑰加密對象，請在 CreateMultipartUpload 請求（以及每個後續 UploadPart 請求）中使用所有這三個標頭。
 - x-amz-server-side-encryption-customer-algorithm：指定 AES256。
 - x-amz-server-side-encryption-customer-key：為新物件指定加密金鑰。
 - x-amz-server-side-encryption-customer-key-MD5：指定新物件的加密金鑰的 MD5 摘要。



您提供的加密金鑰永遠不會被儲存。如果遺失了加密金鑰，您就會遺失對應的物件。在使用客戶提供的金鑰保護物件資料之前，請先查看以下注意事項["使用伺服器端加密"](#)。

不支援的請求標頭

不支援以下請求標頭：

- x-amz-website-redirect-location

這 x-amz-website-redirect-location 標題返回 `XNotImplemented`。

版本控制

分段上傳包括啟動上傳、列出上傳、上傳部分、組裝上傳部分和完成上傳的單獨操作。執行 CompleteMultipartUpload 作業時會建立物件（如果適用，也會進行版本控制）。

列出多部分上傳

ListMultipartUploads 操作列出儲存桶正在進行的分段上傳。

支援以下請求參數：

- encoding-type
- key-marker
- max-uploads
- prefix
- upload-id-marker
- Host
- Date
- Authorization

版本控制

分段上傳包括啟動上傳、列出上傳、上傳部分、組裝上傳部分和完成上傳的單獨操作。執行 CompleteMultipartUpload 作業時會建立物件（如果適用，也會進行版本控制）。

上傳部分

UploadPart 作業用於在物件的分段上傳中上傳某個部分。

支援的請求標頭

支援以下請求標頭：

- x-amz-checksum-sha256
- Content-Length
- Content-MD5

伺服器端加密的請求標頭

如果您為 CreateMultipartUpload 要求指定了 SSE-C 加密，則也必須在每個 UploadPart 請求中包含下列請求標頭：

- x-amz-server-side-encryption-customer-algorithm：指定 AES256。
- x-amz-server-side-encryption-customer-key：指定您在 CreateMultipartUpload 請求中提供的相同加密金鑰。
- x-amz-server-side-encryption-customer-key-MD5：指定您在 CreateMultipartUpload 請求中提供的相同 MD5 摘要。



您提供的加密金鑰永遠不會被儲存。如果遺失了加密金鑰，您就會遺失對應的物件。在使用客戶提供的金鑰保護物件資料之前，請先查看["使用伺服器端加密"](#)。

如果您在 CreateMultipartUpload 請求期間指定了 SHA-256 校驗和，則還必須在每個 UploadPart 請求中包含下列請求標頭：

- x-amz-checksum-sha256：指定此部分的 SHA-256 校驗和。

不支援的請求標頭

不支援以下請求標頭：

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`

版本控制

分段上傳包括啟動上傳、列出上傳、上傳部分、組裝上傳部分和完成上傳的單獨操作。執行 `CompleteMultipartUpload` 作業時會建立物件（如果適用，也會進行版本控制）。

上傳部分複製

`UploadPartCopy` 操作透過從現有物件作為資料來源複製資料來上傳物件的一部分。

`UploadPartCopy` 操作是透過所有 Amazon S3 REST API 行為實現的。如有變更，恕不另行通知。

此請求讀取並寫入指定的物件數據 ``x-amz-copy-source-range`` 在 StorageGRID 系統內。

支援以下請求標頭：

- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`

伺服器端加密的請求標頭

如果您為 `CreateMultipartUpload` 要求指定了 SSE-C 加密，則也必須在每個 `UploadPartCopy` 請求中包含以下請求標頭：

- `x-amz-server-side-encryption-customer-algorithm`：指定 AES256。
- `x-amz-server-side-encryption-customer-key`：指定您在 `CreateMultipartUpload` 請求中提供的相同加密金鑰。
- `x-amz-server-side-encryption-customer-key-MD5`：指定您在 `CreateMultipartUpload` 請求中提供的相同 MD5 摘要。

如果來源物件使用客戶提供的金鑰（SSE-C）加密，則必須在 `UploadPartCopy` 請求中包含以下三個標頭，以便可以解密然後複製物件：

- `x-amz-copy-source-server-side-encryption-customer-algorithm`：指定 AES256。
- `x-amz-copy-source-server-side-encryption-customer-key`：指定您在建立來源物件時提供的加密金鑰。
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`：指定您在建立來源物件時提供的 MD5 摘要。



您提供的加密金鑰永遠不會被儲存。如果遺失了加密金鑰，您就會遺失對應的物件。在使用客戶提供的金鑰保護物件資料之前，請先查看["使用伺服器端加密"](#)。

版本控制

分段上傳包括啟動上傳、列出上傳、上傳部分、組裝上傳部分和完成上傳的單獨操作。執行 CompleteMultipartUpload 作業時會建立物件（如果適用，也會進行版本控制）。

錯誤回應

StorageGRID系統支援所有適用的標準 S3 REST API 錯誤回應。此外，StorageGRID實作還新增了幾個自訂回應。

支援的 S3 API 錯誤代碼

Name	HTTP 狀態
拒絕訪問	403 禁止
壞文摘	400 錯誤請求
BucketAlreadyExists	409衝突
BucketNotEmpty	409衝突
不完整的身體	400 錯誤請求
內部錯誤	500 內部伺服器錯誤
無效存取金鑰	403 禁止
無效參數	400 錯誤請求
無效的儲存桶名稱	400 錯誤請求
無效的BucketState	409衝突
無效摘要	400 錯誤請求
無效加密演算法錯誤	400 錯誤請求
無效部分	400 錯誤請求
無效零件訂單	400 錯誤請求

Name	HTTP 狀態
無效範圍	416 請求範圍不滿足
無效請求	400 錯誤請求
無效的儲存類	400 錯誤請求
無效標籤	400 錯誤請求
無效URI	400 錯誤請求
鍵太長	400 錯誤請求
格式錯誤的XML	400 錯誤請求
元數據太大	400 錯誤請求
方法不允許	405 方法不允許
缺失內容長度	411 長度要求
MissingRequestBody錯誤	400 錯誤請求
缺少安全標頭	400 錯誤請求
沒有這樣的桶	404 未找到
NoSuchKey	404 未找到
NoSuchUpload	404 未找到
未實施	501 未實現
NoSuchBucketPolicy	404 未找到
ObjectLockConfigurationNotFoundError	404 未找到
前提條件不成立	412 先決條件失敗
請求時間偏差過大	403 禁止
暫停服務	503 服務不可用

Name	HTTP 狀態
簽名不匹配	403 禁止
桶太多	400 錯誤請求
必須指定使用者金鑰	400 錯誤請求

StorageGRID 自訂錯誤代碼

Name	描述	HTTP 狀態
XBucketLifecycleNotAllowed	舊版相容儲存桶中不允許配置儲存桶生命週期	400 錯誤請求
XBucketPolicyParseException	無法解析收到的儲存桶策略 JSON。	400 錯誤請求
XComplianceConflict	由於舊版合規性設置，操作被拒絕。	403 禁止
XComplianceReducedRedundancyForbidden	舊版相容存儲桶中不允許減少冗餘	400 錯誤請求
XMaxBucketPolicyLengthExceeded	您的策略超出了允許的最大儲存桶策略長度。	400 錯誤請求
XMissingInternalRequestHeader	缺少內部請求的標頭。	400 錯誤請求
XNoSuchBucketCompliance	指定的儲存桶未啟用舊版合規性。	404 未找到
X不可接受	此請求包含一個或多個無法滿足的接受標頭。	406 不可接受
XNotImplemented	您提供的請求暗示了尚未實現的功能。	501 未實現

StorageGRID 自訂操作

StorageGRID 自訂操作

StorageGRID 系統支援新增至 S3 REST API 的自訂操作。

下表列出了 StorageGRID 支援的自訂操作。

手術	描述
"取得桶一致性"	傳回應用於特定儲存桶的一致性。

手術	描述
"PUT 桶一致性"	設定應用於特定儲存桶的一致性。
"取得 Bucket 上次造訪時間"	傳回是否為特定儲存桶啟用或停用上次存取時間更新。
"PUT Bucket 上次訪問時間"	允許您啟用或停用特定儲存桶的上次存取時間更新。
"刪除儲存桶元資料通知配置"	刪除與特定儲存桶關聯的元資料通知配置 XML。
"取得 Bucket 元資料通知配置"	傳回與特定儲存桶關聯的元資料通知配置 XML。
"PUT Bucket 元資料通知配置"	為儲存桶配置元資料通知服務。
"取得儲存使用情況"	告訴您帳戶使用的儲存總量以及與該帳戶關聯的每個儲存桶的儲存總量。
"已棄用：具有合規性設定的 CreateBucket"	已棄用且不受支援：您無法再建立啟用合規性的新儲存桶。
"已棄用：GET Bucket 合規性"	已棄用但受支援：傳回目前對現有舊版合規儲存桶有效的合規性設定。
"棄用：PUT Bucket 合規性"	已棄用但受支援：允許您修改現有舊版合規儲存桶的合規性設定。

取得桶一致性

GET Bucket 一致性請求可讓您確定應用於特定儲存桶的一致性。

預設一致性設定為保證新建立物件的先讀後寫。

您必須擁有 `s3:GetBucketConsistency` 權限，或成為帳戶根，才能完成此操作。

請求範例

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

回覆

在響應 XML 中，`<Consistency>` 將傳回下列值之一：

一致性	描述
全部	所有節點立即接收數據，否則請求將失敗。
強大的全球	保證所有網站上所有客戶端請求的讀寫一致性。
強位點	保證站點內所有客戶端請求的讀寫一致性。
新寫後讀	(預設) 為新物件提供寫入後讀一致性，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。
可用的	為新物件和物件更新提供最終的一致性。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。

回應範例

```
HTTP/1.1 200 OK
Date: Fri, 18 Sep 2020 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/11.5.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<Consistency xmlns="http://s3.storagegrid.com/doc/2015-02-01/">read-after-
new-write</Consistency>
```

相關資訊

["一致性值"](#)

PUT 桶一致性

PUT Bucket 一致性要求可讓您指定套用於對儲存桶執行的操作的一致性。

預設一致性設定為保證新建立物件的先讀後寫。

開始之前

您必須擁有 s3:PutBucketConsistency 權限，或成為帳戶根，才能完成此操作。

要求

這 `x-ntap-sg-consistency` 參數必須包含以下值之一：

一致性	描述
全部	所有節點立即接收數據，否則請求將失敗。
強大的全球	保證所有網站上所有客戶端請求的讀寫一致性。
強位點	保證站點內所有客戶端請求的讀寫一致性。
新寫後讀	(預設) 為新物件提供寫入後讀一致性，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。
可用的	為新物件和物件更新提供最終的一致性。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。

*注意：*一般來說，您應該使用“Read-after-new-write”一致性。如果請求無法正常運作，請盡可能變更應用程式用戶端行為。或者，配置客戶端以指定每個 API 請求的一致性。僅在萬不得已的情況下才在儲存桶層級設定一致性。

請求範例

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

相關資訊

["一致性值"](#)

取得 **Bucket** 上次造訪時間

GET Bucket 最後存取時間請求可讓您確定是否為各個儲存桶啟用或停用最後存取時間更新。

您必須擁有 s3:GetBucketLastAccessTime 權限，或成為帳戶 root，才能完成此操作。

請求範例

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

回應範例

此範例顯示已為儲存桶啟用上次存取時間更新。

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/10.3.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<LastAccessTime xmlns="http://s3.storagegrid.com/doc/2015-02-01/">enabled
</LastAccessTime>
```

PUT Bucket 上次訪問時間

PUT Bucket 最後存取時間請求可讓您啟用或停用單一儲存桶的最後存取時間更新。停用上次存取時間更新可提高效能，並且是使用 10.3.0 或更高版本建立的所有儲存桶的預設值。

您必須擁有儲存桶的 s3:PutBucketLastAccessTime 權限，或成為帳戶 root，才能完成此操作。



從StorageGRID版本 10.3 開始，所有新儲存桶的上次存取時間更新預設為停用狀態。如果您有使用早期版本的StorageGRID建立的儲存桶，並且您想要符合新的預設行為，則必須明確停用每個早期儲存桶的上次存取時間更新。您可以使用 PUT Bucket 上次存取時間請求或從租用戶管理員中儲存桶的詳細資訊頁面啟用或停用上次存取時間的更新。看["啟用或停用上次訪問時間更新"](#)。

如果停用了儲存桶的上次存取時間更新，則下列行為將套用於儲存桶上的操作：

- GetObject、GetObjectAcl、GetObjectTagging 和 HeadObject 要求不會更新上次存取時間。該物件未新增至資訊生命週期管理 (ILM) 評估佇列。
- 僅更新元資料的 CopyObject 和 PutObjectTagging 請求也會更新上次存取時間。該物件被加入到隊列以供 ILM 評估。
- 如果停用來源儲存桶的上次存取時間更新，則 CopyObject 請求不會更新來源儲存體的上次存取時間。被複製的物件不會加入到來源儲存桶的 ILM 評估佇列中。但是，對於目標，CopyObject 請求總是更新上次存取時間。物件的副本被加入到隊列中以便 ILM 評估。
- CompleteMultipartUpload 請求更新上次訪問時間。完成的物件被加入到隊列中以便 ILM 評估。

請求範例

此範例啟用儲存桶的最後存取時間。

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

此範例禁用儲存桶的上次存取時間。

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

刪除儲存桶元資料通知配置

DELETE Bucket 元資料通知設定請求可讓您透過刪除配置 XML 來停用單一儲存桶的搜尋整合服務。

您必須擁有儲存桶的 `s3:DeleteBucketMetadataNotification` 權限，或成為帳戶根，才能完成此操作。

請求範例

此範例顯示停用儲存桶的搜尋整合服務。

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

取得 **Bucket** 元資料通知配置

GET Bucket 元資料通知設定請求可讓您檢索用於配置各個儲存桶的搜尋整合的配置 XML。

您必須擁有 `s3:GetBucketMetadataNotification` 權限，或成為帳戶根，才能完成此操作。

請求範例

此請求檢索名為 `bucket`。

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

回覆

回應主體包含儲存桶的元資料通知配置。元資料通知配置讓您決定如何配置儲存桶以進行搜尋整合。也就是說，它允許您確定哪些物件被索引，以及它們的物件元資料被傳送到哪些端點。

```
<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>rule-status</Status>
    <Prefix>key-prefix</Prefix>
    <Destination>
      <Urn>arn:aws:es:_region:account-
ID_:domain/_mydomain/myindex/mytype_</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Rule-2</ID>
    ...
  </Rule>
  ...
</MetadataNotificationConfiguration>
```

每個元資料通知配置都包含一個或多個規則。每條規則指定其適用的物件以及StorageGRID應發送物件元資料的目的地。必須使用StorageGRID端點的 URN 指定目標。

Name	描述	必需的
元數據通知配置	用於指定元資料通知的物件和目的地的規則的容器標籤。 包含一個或多個 Rule 元素。	是的
規則	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。 前綴重疊的規則將被拒絕。 包含在 MetadataNotificationConfiguration 元素中。	是的
ID	規則的唯一識別碼。 包含在 Rule 元素中。	不
地位	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。 包含在 Rule 元素中。	是的

Name	描述	必需的
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
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 Destination 元素中。</p>	是的

回應範例

XML 包含在 `<MetadataNotificationConfiguration></MetadataNotificationConfiguration>` 標籤顯示如何為儲存桶配置與搜尋整合端點的整合。在此範例中，物件元資料被傳送到名為 `current` 並輸入命名 `2017` 託管在名為 `records`。

```
HTTP/1.1 200 OK
Date: Thu, 20 Jul 2017 18:24:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/11.0.0
x-amz-request-id: 3832973499
Content-Length: 264
Content-Type: application/xml
```

```
<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>Enabled</Status>
    <Prefix>2017</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-
1:3333333:domain/records/current/2017</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

相關資訊

["使用租用戶帳戶"](#)

PUT Bucket 元資料通知配置

PUT Bucket 元資料通知設定請求可讓您為單一儲存桶啟用搜尋整合服務。您在請求正文中提供的元資料通知配置 XML 指定將其元資料傳送至目標搜尋索引的物件。

您必須擁有儲存桶的 `s3:PutBucketMetadataNotification` 權限，或成為帳戶根，才能完成此操作。

要求

請求必須在請求正文中包含元資料通知配置。每個元資料通知配置都包含一個或多個規則。每條規則指定其適用的物件以及 StorageGRID 應發送物件元資料的目的地。

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` 到一個目的地，以及帶有前綴的對象 `/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。

必須使用 StorageGRID 端點的 URN 指定目標。提交元資料通知配置時，端點必須存在，否則請求失敗，因為 400 Bad Request。錯誤訊息指出：`Unable to save the metadata notification (search) policy. The specified endpoint URN does not exist: URN.`

```

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

```

此表描述了元資料通知配置 XML 中的元素。

Name	描述	必需的
元數據通知配置	用於指定元資料通知的物件和目的地的規則的容器標籤。 包含一個或多個 Rule 元素。	是的
規則	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。 前綴重疊的規則將被拒絕。 包含在 MetadataNotificationConfiguration 元素中。	是的
ID	規則的唯一識別碼。 包含在 Rule 元素中。	不
地位	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。 包含在 Rule 元素中。	是的

Name	描述	必需的
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
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 Destination 元素中。</p>	是的

請求範例

此範例顯示啟用儲存桶的搜尋整合。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。

```

PUT /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

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

```

在此範例中，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像元數據 `/videos` 被送到第二個目的地。

```

PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

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

```

搜尋整合服務產生的 JSON

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"
  }
}
```

元數據通知中包含的對象元數據

表格列出了啟用搜尋整合時傳送到目標端點的 JSON 文件中包含的所有欄位。

文件名稱包括儲存桶名稱、物件名稱和版本 ID（如果存在）。

類型	項目名稱	描述
儲存桶和物件資訊	桶	儲存桶的名稱
儲存桶和物件資訊	鑰匙	物件鍵名
儲存桶和物件資訊	版本ID	物件版本，適用於版本化儲存桶中的對象
儲存桶和物件資訊	地區	例如，儲存桶區域 us-east-1
系統元數據	尺寸	HTTP 用戶端可見的物件大小（以位元組為單位）
系統元數據	md5	物件哈希

類型	項目名稱	描述
用戶元數據	元數據 <i>key:value</i>	物件的所有用戶元數據，以鍵值對的形式
標籤	標籤 <i>key:value</i>	為物件定義的所有物件標籤，以鍵值對的形式



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。

相關資訊

["使用租用戶帳戶"](#)

取得儲存使用情況請求

GET 儲存使用情況要求會告訴您帳戶使用的儲存總量以及與該帳戶關聯的每個儲存桶的儲存總量。

可以透過修改後的 ListBuckets 請求來取得帳戶及其儲存桶使用的儲存量，其中包含 `x-ntap-sg-usage` 查詢參數。儲存桶儲存使用情況與系統處理的 PUT 和 DELETE 請求分開追蹤。根據請求的處理，使用值與預期值相符之前可能會有一些延遲，特別是當系統負載很重時。

預設情況下，StorageGRID嘗試使用強全域一致性來擷取使用情況資訊。如果無法實現強全域一致性，StorageGRID將嘗試在強站點一致性下擷取使用資訊。

您必須擁有 s3:ListAllMyBuckets 權限，或成為帳戶 root，才能完成此操作。

請求範例

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

回應範例

此範例顯示一個帳戶，該帳戶在兩個儲存桶中擁有四個物件和 12 個位元組的資料。每個儲存桶包含兩個物件和六個位元組的資料。

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 00:49:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/10.2.0
x-amz-request-id: 727237123
Content-Length: 427
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<UsageResult xmlns="http://s3.storagegrid.com/doc/2015-02-01">
<CalculationTime>2014-11-19T05:30:11.000000Z</CalculationTime>
<ObjectCount>4</ObjectCount>
<DataBytes>12</DataBytes>
<Buckets>
<Bucket>
<Name>bucket1</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
<Bucket>
<Name>bucket2</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
</Buckets>
</UsageResult>
```

版本控制

儲存的每個物件版本都將有助於 `ObjectCount` 和 `DataBytes` 響應中的值。刪除標記不會新增到 `ObjectCount` 全部的。

相關資訊

["一致性值"](#)

已棄用舊版合規性儲存桶請求

已棄用舊版合規性儲存桶請求

您可能需要使用StorageGRID S3 REST API 來管理使用舊版合規功能建立的儲存桶。

合規性功能已棄用

先前版本的StorageGRID中提供的StorageGRID合規功能已被棄用，並已被 S3 物件鎖定取代。

如果您之前啟用了全域合規性設置，則全域 S3 物件鎖定設定在StorageGRID 11.6 中啟用。您無法再建立啟用了合規性的新儲存桶；但是，根據需要，您可以使用StorageGRID S3 REST API 來管理任何現有的舊版合規儲

存桶。

- ["使用 S3 REST API 設定 S3 物件鎖"](#)
- ["使用 ILM 管理對象"](#)
- ["NetApp知識庫：如何在StorageGRID 11.5 中管理舊版相容儲存桶"](#)

已棄用的合規性請求：

- ["已棄用 - PUT Bucket 請求修改以實現合規性"](#)

SGCompliance XML 元素已被棄用。以前，您可以在 PUT Bucket 請求的可選 XML 請求正文中包含此StorageGRID自訂元素來建立相容儲存桶。

- ["已棄用 - GET Bucket 合規性"](#)

GET Bucket 合規性請求已被棄用。但是，您可以繼續使用此要求來確定現有舊版合規儲存桶目前有效的合規性設定。

- ["已棄用 - PUT Bucket 合規性"](#)

PUT Bucket 合規性請求已被棄用。但是，您可以繼續使用此請求來修改現有舊版合規儲存桶的合規性設定。例如，您可以將現有儲存桶置於合法保留狀態或延長其保留期。

已棄用：**CreateBucket** 請求修改以實現合規性

SGCompliance XML 元素已被棄用。以前，您可以在 CreateBucket 請求的可選 XML 請求正文中包含此StorageGRID自訂元素來建立相容儲存桶。



先前版本的StorageGRID中提供的StorageGRID合規功能已被棄用，並已被 S3 物件鎖定取代。請參閱以下內容以了解更多詳細資訊：

- ["使用 S3 REST API 設定 S3 物件鎖"](#)
- ["NetApp知識庫：如何在StorageGRID 11.5 中管理舊版相容儲存桶"](#)

您無法再建立啟用合規性的新儲存桶。如果您嘗試使用 CreateBucket 要求修改來建立新的合規儲存桶，則會傳回下列錯誤訊息：

```
The Compliance feature is deprecated.  
Contact your StorageGRID administrator if you need to create new Compliant  
buckets.
```

已棄用：**GET Bucket** 合規性請求

GET Bucket 合規性請求已被棄用。但是，您可以繼續使用此要求來確定現有舊版合規儲存桶目前有效的合規性設定。



先前版本的StorageGRID中提供的StorageGRID合規功能已被棄用，並已被 S3 物件鎖定取代。請參閱以下內容以了解更多詳細資訊：

- ["使用 S3 REST API 設定 S3 物件鎖"](#)
- ["NetApp知識庫：如何在StorageGRID 11.5 中管理舊版相容儲存桶"](#)

您必須擁有 `s3:GetBucketCompliance` 權限，或成為帳戶根，才能完成此操作。

請求範例

此範例請求允許您確定名為 `mybucket`。

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

回應範例

在響應 XML 中，`<SGCompliance>` 列出儲存桶有效的合規性設定。此範例回應顯示了儲存桶的合規性設置，其中每個物件將從物件引入電網時開始保留一年（525,600 分鐘）。目前，此儲存桶不存在任何合法保留。每個物件將在一年後自動刪除。

```
HTTP/1.1 200 OK
Date: date
Connection: connection
Server: StorageGRID/11.1.0
x-amz-request-id: request ID
Content-Length: length
Content-Type: application/xml

<SGCompliance>
  <RetentionPeriodMinutes>525600</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Name	描述
保留期分鐘	新增至此儲存桶的物件的保留期限長度（以分鐘為單位）。保留期從物件納入電網時開始。

Name	描述
法律保留	<ul style="list-style-type: none"> • 真：此儲存桶目前處於合法保留狀態。在解除合法保留之前，此儲存桶中的物件無法被刪除，即使其保留期已過期。 • 錯誤：此儲存桶目前未處於合法保留之下。當保留期到期時，可以刪除此儲存桶中的物件。
自動刪除	<ul style="list-style-type: none"> • True：除非儲存桶處於合法保留狀態，否則當保留期到期時，此儲存桶中的物件將自動刪除。 • False：保留期到期後，此儲存桶中的物件不會自動刪除。如果需要刪除這些對象，則必須手動刪除它們。

錯誤回應

如果儲存桶的建立不符合要求，則回應的 HTTP 狀態代碼為 404 Not Found，S3 錯誤代碼為 XNoSuchBucketCompliance。

已棄用：**PUT Bucket** 合規性請求

PUT Bucket 合規性請求已被棄用。但是，您可以繼續使用此請求來修改現有舊版合規儲存桶的合規性設定。例如，您可以將現有儲存桶置於合法保留狀態或延長其保留期。



先前版本的StorageGRID中提供的StorageGRID合規功能已被棄用，並已被 S3 物件鎖定取代。請參閱以下內容以了解更多詳細資訊：

- ["使用 S3 REST API 設定 S3 物件鎖"](#)
- ["NetApp知識庫：如何在StorageGRID 11.5 中管理舊版相容儲存桶"](#)

您必須擁有 s3:PutBucketCompliance 權限，或成為帳戶根，才能完成此操作。

發出 PUT Bucket 合規性請求時，必須為合規性設定的每個欄位指定一個值。

請求範例

此範例請求修改名為 mybucket。在這個例子中，對象 `mybucket` 從對象納入電網時起，將保留兩年（1,051,200 分鐘），而不是一年。此儲存桶不存在合法保留。每個物件將在兩年後自動刪除。

```

PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Content-Length: 152

<SGCompliance>
  <RetentionPeriodMinutes>1051200</RetentionPeriodMinutes>
  <LegalHold>>false</LegalHold>
  <AutoDelete>>true</AutoDelete>
</SGCompliance>

```

Name	描述
保留期分鐘	<p>新增至此儲存桶的物件的保留期限長度（以分鐘為單位）。保留期從物件納入電網時開始。</p> <p>重要 為 <code>RetentionPeriodMinutes</code> 指定新值時，必須指定等於或大於儲存桶目前保留期的值。設定儲存桶的保留期後，您無法減少該值；您只能增加它。</p>
法律保留	<ul style="list-style-type: none"> • 真：此儲存桶目前處於合法保留狀態。在解除合法保留之前，此儲存桶中的物件無法被刪除，即使其保留期已過期。 • 錯誤：此儲存桶目前未處於合法保留之下。當保留期到期時，可以刪除此儲存桶中的物件。
自動刪除	<ul style="list-style-type: none"> • True：除非儲存桶處於合法保留狀態，否則當保留期到期時，此儲存桶中的物件將自動刪除。 • False：保留期到期後，此儲存桶中的物件不會自動刪除。如果需要刪除這些對象，則必須手動刪除它們。

合規性設定的一致性

當您使用 PUT Bucket 合規性要求更新 S3 儲存桶的合規性設定時，StorageGRID會嘗試在整個網格中更新儲存桶的元資料。預設情況下，StorageGRID使用 強全域 一致性來確保所有資料中心站點和所有包含儲存桶元資料的儲存節點對於變更的合規性設定具有讀寫一致性。

如果StorageGRID因資料中心網站或網站上的多個儲存節點不可用而無法實現 強全域 一致性，則回應的 HTTP 狀態碼為 503 Service Unavailable。

如果收到此回復，則必須聯絡網格管理員，以確保盡快提供所需的儲存服務。如果網格管理員無法在每個站點提供足夠的儲存節點，技術支援可能會指導您透過強制*強站點*一致性來重試失敗的請求。



切勿強制使用 **Strong-site** 一致性來遵守 PUT bucket 規定，除非技術支援指示您這樣做，並且您了解使用此級別的潛在後果。

當一致性降低到*強站點*時， StorageGRID保證更新後的合規性設定僅對站點內的用戶端請求具有讀寫一致性。這意味著StorageGRID系統可能會暫時對該儲存桶具有多個不一致的設置，直到所有站點和儲存節點都可用。不一致的設定可能會導致意外和不良的行為。例如，如果您將儲存桶置於合法保留之下並強制降低一致性，則儲存桶先前的合規性設定（即合法保留）可能會在某些資料中心網站繼續有效。因此，您認為處於合法保留狀態的物件可能會在保留期到期時被使用者或自動刪除功能（如果已啟用）刪除。

若要強制使用 **Strong-site** 一致性，請重新發出 PUT Bucket 合規性要求，並包含 `Consistency-Control` HTTP 請求頭，如下：

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

錯誤回應

- 如果儲存桶的建立不符合要求，則回應的 HTTP 狀態代碼為 404 Not Found。
- 如果 RetentionPeriodMinutes`如果請求小於儲存桶的目前保留期，則 HTTP 狀態碼為 `400 Bad Request。

相關資訊

["已棄用：PUT Bucket 請求修改以實現合規性"](#)

儲存桶和群組存取策略

使用儲存桶和群組存取策略

StorageGRID使用 Amazon Web Services (AWS) 原則語言可讓 S3 租用戶控制對儲存桶及其儲存體桶內物件的存取。StorageGRID系統實作了 S3 REST API 原則語言的子集。S3 API 的存取策略以 JSON 編寫。

訪問策略概述

StorageGRID支援兩種存取策略。

- **Bucket** 政策，使用 GetBucketPolicy、PutBucketPolicy 和 DeleteBucketPolicy S3 API 操作或 Tenant Manager 或 Tenant Management API 進行管理。儲存桶策略附加到儲存桶，因此它們配置為控制儲存桶擁有者帳戶或其他帳戶中的使用者對儲存桶及其中的物件的存取。一個儲存桶策略僅適用於一個儲存桶，也可能適用於多個群組。
- 群組原則，使用租用戶管理器或租用戶管理 API 進行設定。群組原則會附加到帳戶中的群組，因此它們配置為允許該群組存取該帳戶擁有的特定資源。群組原則僅適用於一個群組，也可能適用於多個儲存桶。



組策略和儲存桶策略之間的優先順序沒有區別。

StorageGRID桶和群組原則遵循 Amazon 定義的特定語法。每個策略內部都有一個策略語句數組，每個語句包含以下元素：

- 語句 ID (Sid) (可選)
- 影響

- 校長/非校長
- 資源/非資源
- 行動/不行動
- 條件 (可選)

策略語句使用此結構建構以指定權限：授予<Effect>以允許/拒絕<Principal>在適用<Condition>時對<Resource>執行<Action>。

每個策略元素都有其特定的功能：

元素	描述
席德	Sid 元素是可選的。Sid 僅供使用者描述。它被儲存但不被StorageGRID系統解釋。
影響	使用 Effect 元素來決定是否允許或拒絕指定的操作。您必須使用支援的 Action 元素關鍵字來識別對儲存桶或物件允許 (或拒絕) 的操作。
校長/非校長	您可以允許使用者、群組和帳戶存取特定資源並執行特定操作。如果請求中不包含 S3 簽名，則透過指定通配符 (*) 作為主體來允許匿名存取。預設情況下，只有帳戶根可以存取該帳戶擁有的資源。 您只需要在儲存桶策略中指定 Principal 元素。對於群組策略，策略所附加到的群組是隱式的 Principal 元素。
資源/非資源	Resource 元素標識儲存桶和物件。您可以使用 Amazon 資源名稱 (ARN) 來識別資源，從而允許或拒絕對儲存桶和物件的權限。
行動/不行動	Action 和 Effect 元素是權限的兩個組成部分。當一個群組請求資源時，他們要麼被授予存取該資源的權限，要麼被拒絕存取該資源。除非您明確指派權限，否則存取將被拒絕，但您可以使用明確拒絕來覆寫另一個策略授予的權限。
狀態	Condition 元素是可選的。條件允許您建立表達式來確定何時應用策略。

在 Action 元素中，可以使用通配符 (*) 來指定所有動作或部分動作。例如，此 Action 符合 s3:GetObject、s3:PutObject 和 s3:DeleteObject 等權限。

```
s3:*Object
```

在 Resource 元素中，可以使用通配符 (*) 和 (?)。星號 (*) 符合 0 個或多個字符，而問號 (?) 則匹配任意單一字符。

在 Principal 元素中，不支援通配符，除非設定匿名存取 (向所有人授予權限)。例如，您將通配符 (*) 設定為主體值。

```
"Principal": "*" }
```

```
"Principal": {"AWS": "*" }
```

在以下範例中，該語句使用了 Effect、Principal、Action 和 Resource 元素。此範例展示了一個完整的儲存桶策略語句，該語句使用效果「允許」來授予 Principals、管理群組 `federated-group/admin` 以及財務集團 `federated-group/finance`，執行操作的權限 `s3:ListBucket` 在名為 `mybucket` 和行動 `s3:GetObject` 在該儲存桶內的所有物件上。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::mybucket",
        "arn:aws:s3:::mybucket/*"
      ]
    }
  ]
}
```

儲存桶策略的大小限制為 20,480 字節，群組原則的大小限制為 5,120 位元組。

政策一致性

預設情況下，您對群組原則所做的任何更新最終都是一致的。當群組原則變得一致時，由於策略緩存，變更可能需要額外 15 分鐘才能生效。預設情況下，您對儲存桶策略所做的任何更新都是高度一致的。

根據需要，您可以變更儲存桶策略更新的一致性保證。例如，您可能希望在網站中斷期間變更儲存桶策略。

在這種情況下，您可以設定 `Consistency-Control` PutBucketPolicy 請求中的標頭，或者您可以使用 PUT Bucket 一致性請求。當儲存桶策略變得一致時，由於策略快取，變更可能需要額外 8 秒才能生效。



如果您將一致性設為不同的值以解決臨時情況，請確保在完成後將儲存桶層級設定還原為其原始值。否則，所有未來的儲存桶請求都將使用修改後的設定。

在策略聲明中使用 ARN

在策略聲明中，ARN 用於 Principal 和 Resource 元素。

- 使用此語法指定 S3 資源 ARN：

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

- 使用此語法指定身分資源 ARN（使用者和群組）：

```
arn:aws:iam::account_id:root
arn:aws:iam::account_id:user/user_name
arn:aws:iam::account_id:group/group_name
arn:aws:iam::account_id:federated-user/user_name
arn:aws:iam::account_id:federated-group/group_name
```

其他考慮因素：

- 您可以使用星號 (*) 作為通配符來匹配物件鍵內的零個或多個字元。
- 可以在物件鍵中指定的國際字元應使用 JSON UTF-8 或 JSON \u 轉義序列進行編碼。不支援百分比編碼。

"RFC 2141 URN語法"

PutBucketPolicy 操作的 HTTP 請求主體必須使用 charset=UTF-8 進行編碼。

在策略中指定資源

在策略語句中，您可以使用 Resource 元素來指定允許或拒絕權限的儲存桶或物件。

- 每個策略聲明都需要一個資源元素。在策略中，資源由元素表示 `Resource` 或者，`NotResource` 以進行排除。
- 您可以使用 S3 資源 ARN 指定資源。例如：

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- 您也可以物件鍵內使用策略變數。例如：

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- 資源值可以指定在建立群組原則時尚不存在的儲存桶。

在策略中指定主體

使用 Principal 元素來識別政策聲明允許/拒絕存取資源的使用者、群組或租戶帳戶。

- 儲存桶策略中的每個策略語句都必須包含一個 Principal 元素。群組原則中的策略語句不需要 Principal 元素，因為群組被視為主體。
- 在策略中，主體由元素「Principal」表示，或由「NotPrincipal」表示排除。
- 必須使用 ID 或 ARN 指定基於帳戶的身份：

```
"Principal": { "AWS": "account_id"}  
"Principal": { "AWS": "identity_arn" }
```

- 本範例使用租用戶帳號 ID 27233906934684427525，其中包括帳號 root 和帳號內的所有使用者：

```
"Principal": { "AWS": "27233906934684427525" }
```

- 您可以僅指定帳戶根：

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- 您可以指定特定的聯合使用者（「Alex」）：

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-  
user/Alex" }
```

- 您可以指定特定的聯合群組（「管理員」）：

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-  
group/Managers" }
```

- 您可以指定一個匿名主體：

```
"Principal": "*" 
```

- 為了避免歧義，您可以使用使用者 UUID 而不是使用者名稱：

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-eb6b9e546013
```

例如，假設 Alex 離開了組織，而用戶名 `Alex` 被刪除。如果一個新的 Alex 加入組織並且被分配相同的 `Alex` 使用者名，新使用者可能會無意中繼承授予原始使用者的權限。

- 主體值可以指定在建立儲存桶策略時尚不存在的群組/使用者名稱。

在策略中指定權限

在策略中，Action 元素用於允許/拒絕對資源的權限。您可以在策略中指定一組權限，這些權限由元素「Action」表示，或由「NotAction」表示排除。每個元素都對應到特定的 S3 REST API 操作。

表格列出了適用於儲存桶的權限和適用於物件的權限。



Amazon S3 現在對 PutBucketReplication 和 DeleteBucketReplication 作業使用 s3:PutReplicationConfiguration 權限。StorageGRID 對每個操作使用單獨的權限，這與原始 Amazon S3 規格相符。



當使用 put 覆寫現有值時，將執行刪除。

適用於儲存桶的權限

權限	S3 REST API 操作	為StorageGRID定制
s3: 創建桶	創建桶	是的。 注意：僅在群組原則中使用。
s3: 刪除桶	刪除桶	
s3: 刪除儲存桶元資料通知	刪除儲存桶元資料通知配置	是的
s3: 刪除儲存桶策略	刪除桶策略	
s3: 刪除複製配置	刪除桶複製	是的，PUT 和 DELETE 的權限是分開的
s3: 取得儲存桶Acl	獲取BucketAcl	
s3: 取得儲存桶合規性	GET Bucket 合規性 (已棄用)	是的
s3: 取得儲存桶一致性	取得桶一致性	是的

權限	S3 REST API 操作	為StorageGRID定制
s3：取得儲存桶CORS	獲取BucketCors	
s3:取得加密配置	取得桶加密	
s3：取得儲存桶上次存取時間	取得 Bucket 上次造訪時間	是的
s3：取得儲存桶位置	取得儲存桶位置	
s3：取得儲存桶元資料通知	取得 Bucket 元資料通知配置	是的
s3：取得儲存桶通知	取得儲存桶通知配置	
s3：取得儲存桶物件鎖配置	取得物件鎖配置	
s3：取得儲存桶策略	取得BucketPolicy	
s3：取得儲存桶標記	取得桶標記	
s3：取得儲存桶版本	取得Bucket版本	
s3:獲取生命週期配置	取得BucketLifecycleConfiguration	
s3：取得複製配置	獲取Bucket複製	
s3：列出所有我的儲存桶	<ul style="list-style-type: none"> • 列表桶 • 取得儲存使用情況 	<p>是的，用於獲取儲存使用情況。</p> <p>注意：僅在群組原則中使用。</p>
s3：列表桶	<ul style="list-style-type: none"> • 清單對象 • 頭桶 • 復原對象 	
s3：列出桶多部分上傳	<ul style="list-style-type: none"> • 列出多部分上傳 • 復原對象 	
s3：列出儲存桶版本	取得儲存桶版本	
s3：PutBucket合規性	PUT Bucket 合規性（已棄用）	是的

權限	S3 REST API 操作	為StorageGRID定制
s3:PutBucket一致性	PUT桶一致性	是的
s3:PutBucketCORS	<ul style="list-style-type: none"> DeleteBucketCors† PutBucketCors 	
s3 : PutEncryption配置	<ul style="list-style-type: none"> 刪除桶加密 PutBucket加密 	
s3:PutBucket上次訪問時間	PUT Bucket 上次訪問時間	是的
s3 : PutBucketMetadata通知	PUT Bucket 元資料通知配置	是的
s3 : PutBucket通知	PutBucketNotification配置	
s3:PutBucketObjectLock配置	<ul style="list-style-type: none"> 使用 CreateBucket `x-amz-bucket-object-lock-enabled: true` 請求標頭 (也需要 s3:CreateBucket 權限) PutObjectLock配置 	
s3 : PutBucket策略	PutBucketPolicy	
s3 : PutBucket標記	<ul style="list-style-type: none"> 刪除儲存桶標記† PutBucketTagging 	
s3 : PutBucket版本控制	PutBucket版本控制	
s3 : PutLifecycle配置	<ul style="list-style-type: none"> DeleteBucketLifecycle† PutBucket生命週期配置 	
s3 : Put複製配置	PutBucket複製	是的，PUT 和 DELETE 的權限是分開的

適用於物件的權限

權限	S3 REST API 操作	為StorageGRID定制
s3 : 中止分段上傳	<ul style="list-style-type: none"> 中止分段上傳 復原對象 	

權限	S3 REST API 操作	為StorageGRID定制
s3：繞過治理保留	<ul style="list-style-type: none"> • 刪除對象 • 刪除對象 • PutObjectRetention 	
s3：刪除對象	<ul style="list-style-type: none"> • 刪除對象 • 刪除對象 • 復原對象 	
s3：刪除物件標記	刪除物件標記	
s3：刪除物件版本標記	DeleteObjectTagging（物件的特定版本）	
s3：刪除物件版本	DeleteObject（物件的特定版本）	
s3：獲取對象	<ul style="list-style-type: none"> • 取得對象 • 頭部對象 • 復原對象 • 選擇對象內容 	
s3:獲取對象Acl	取得對象Acl	
s3：獲取對象合法持有狀態	獲取對象合法持有	
s3：取得對象保留	取得對象保留	
s3:取得物件標記	取得物件標記	
s3:取得物件版本標記	GetObjectTagging（物件的特定版本）	
s3：取得物件版本	GetObject（物件的特定版本）	
s3:列出多部分上傳部分	列出零件，恢復對象	

權限	S3 REST API 操作	為StorageGRID定制
s3:Put對象	<ul style="list-style-type: none"> • 放置對象 • 複製對象 • 復原對象 • 建立多部分上傳 • 完成多部分上傳 • 上傳部分 • 上傳部分複製 	
s3:PutObjectLegalHold	放置對象合法保留	
s3:PutObjectRetention	PutObjectRetention	
s3:PutObjectTagging	PutObjectTagging	
s3:PutObjectVersionTagging	PutObjectTagging (物件的特定版本)	
s3:PutOverwrite對象	<ul style="list-style-type: none"> • 放置對象 • 複製對象 • PutObjectTagging • 刪除物件標記 • 完成多部分上傳 	是的
s3:恢復對象	復原對象	

使用 PutOverwriteObject 權限

s3:PutOverwriteObject 權限是自訂StorageGRID權限，適用於建立或更新物件的操作。此權限的設定決定用戶端是否可以覆寫物件的資料、使用者定義的元資料或 S3 物件標記。

此權限的可能設定包括：

- 允許：客戶端可以覆蓋物件。這是預設值。
- 拒絕：客戶端無法覆蓋物件。當設定為 Deny 時，PutOverwriteObject 權限的工作方式如下：
 - 如果在同一路徑上找到現有物件：
 - 物件的資料、使用者定義的元資料或 S3 物件標記無法被覆寫。
 - 任何正在進行的攝取操作都將被取消，並傳回錯誤。
 - 如果啟用了 S3 版本控制，則 Deny 設定會阻止 PutObjectTagging 或 DeleteObjectTagging 操作修改物件及其非目前版本的 TagSet。

- 如果未找到現有對象，則此權限無效。
- 當不存在此權限時，效果與設定「允許」相同。



如果目前 S3 策略允許覆蓋，且 PutOverwriteObject 權限設定為 Deny，則用戶端無法覆寫物件的資料、使用者定義的元資料或物件標記。此外，如果選取了「防止用戶端修改」核取方塊（配置 > 安全設定 > 網路和物件），則該設定將覆寫 PutOverwriteObject 權限的設定。

在策略中指定條件

條件定義了政策何時生效。條件由運算子和鍵值對組成。

條件使用鍵值對進行評估。一個 Condition 元素可以包含多個條件，每個條件可以包含多個鍵值對。條件區塊使用以下格式：

```
Condition: {
  condition_type: {
    condition_key: condition_values
```

在下列範例中，IpAddress 條件使用 SourceIp 條件鍵。

```
"Condition": {
  "IpAddress": {
    "aws:SourceIp": "54.240.143.0/24"
    ...
  },
  ...
```

支援的條件運算符

條件運算子分類如下：

- 細繩
- 數位
- 布林值
- IP 位址
- 空值檢查

條件運算符	描述
字串等於	根據精確匹配（區分大小寫）將鍵與字串值進行比較。
字串不等於	根據否定匹配（區分大小寫）將鍵與字串值進行比較。

條件運算符	描述
字串等於忽略大小寫	根據精確匹配（忽略大小寫）將鍵與字串值進行比較。
字串不等於忽略大小寫	根據否定匹配（忽略大小寫）將鍵與字串值進行比較。
StringLike	根據精確匹配（區分大小寫）將鍵與字串值進行比較。可以包含 * 和 ? 通配符。
StringNotLike	根據否定匹配（區分大小寫）將鍵與字串值進行比較。可以包含 * 和 ? 通配符。
數字等於	根據精確匹配將鍵與數值進行比較。
數字不等於	根據否定匹配將鍵與數值進行比較。
數字大於	根據“大於”匹配將鍵與數值進行比較。
數字大於等於	根據“大於或等於”匹配將鍵與數值進行比較。
數字小於	根據“小於”匹配將鍵與數值進行比較。
數字小於等於	根據“小於或等於”匹配將鍵與數值進行比較。
布林值	根據“真或假”匹配將鍵與布林值進行比較。
IP位址	將金鑰與 IP 位址或 IP 位址範圍進行比較。
不存在IP位址	根據否定匹配將鍵與 IP 位址或 IP 位址範圍進行比較。
無效的	檢查目前請求上下文中是否存在條件鍵。

支援的條件鍵

條件鍵	行動	描述
aws:來源IP	IP營運商	<p>將與發送請求的 IP 位址進行比較。可用於儲存桶或物件操作。</p> <p>*注意：*如果 S3 請求是透過管理節點和網關節點上的負載平衡器服務發送的，這將與負載平衡器服務上游的 IP 位址進行比較。</p> <p>注意：如果使用第三方非透明負載平衡器，這將與該負載平衡器的 IP 位址進行比較。任何 `X-Forwarded-For` 標頭將被忽略，因為無法確定其有效性。</p>
aws:用戶名	資源/身份	將與發送請求的寄件者的使用者名稱進行比較。可用於儲存桶或物件操作。
s3:分隔符	s3:ListBucket 和 s3:ListBucketVersions 權 限	將與 ListObjects 或 ListObjectVersions 請求中指定的分隔符號參數進行比較。
s3:ExistingObjectTag/<標 籤鍵>	s3：刪除物件標記 s3：刪除物件版本標記 s3：獲取對象 s3:獲取對象Acl 3：取得物件標記 s3：取得物件版本 s3:取得物件版本Acl s3:取得物件版本標記 s3：PutObjectAcl s3：PutObjectTagging s3:PutObjectVersionAcl s3 ：PutObjectVersionTaggi ng	將要求現有物件具有特定的標籤鍵和值。
s3:最大鍵數	s3:ListBucket 和 s3:ListBucketVersions 權 限	將與 ListObjects 或 ListObjectVersions 請求中指定的 max-keys 參數進行比較。

條件鍵	行動	描述
s3:對象鎖剩餘保留天數	s3:Put對象	與保留至日期中指定的日期進行比較 `x-amz-object-lock-retain-until-date` 請求標頭或根據儲存桶預設保留期間計算得出，以確保這些值在以下請求的允許範圍內： <ul style="list-style-type: none"> • 放置對象 • 複製對象 • 建立多部分上傳
s3:對象鎖剩餘保留天數	s3:PutObjectRetention	與 PutObjectRetention 請求中指定的 retain-until-date 進行比較，以確保其在允許範圍內。
s3:前綴	s3:ListBucket 和 s3:ListBucketVersions 權 限	將與 ListObjects 或 ListObjectVersions 請求中指定的前綴參數進行比較。
s3:RequestObjectTag/<標 籤鍵>	s3:Put對象 s3:PutObjectTagging s3 :PutObjectVersionTaggi ng	當物件請求包含標記時，將需要特定的標籤鍵和值。

在策略中指定變數

您可以使用策略中的變數來填入可用的策略資訊。您可以在 `Resource` 元素和字串比較中的 `Condition` 元素。

在這個例子中，變數 `\${aws:username}` 是 Resource 元素的一部分：

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

在這個例子中，變數 `\${aws:username}` 是條件區塊中條件值的一部分：

```
"Condition": {
  "StringLike": {
    "s3:prefix": "${aws:username}/*"
    ...
  },
  ...
}
```

多變的	描述
<code>\${aws:SourceIp}</code>	使用 SourceIp 鍵作為提供的變數。
<code>\${aws:username}</code>	使用使用者名稱鍵作為提供的變數。
<code>\${s3:prefix}</code>	使用特定於服務的前綴鍵作為提供的變數。
<code>\${s3:max-keys}</code>	使用特定於服務的 max-keys 鍵作為提供的變數。
<code>\${*}</code>	特殊字元。將該字元用作文字 * 字元。
<code>\${?}</code>	特殊字元。將該字元用作文字 ? 字元。
<code>\${\$}</code>	特殊字元。將該字元用作文字 \$ 字元。

創建需要特殊處理的政策

有時，政策授予的權限可能會對安全性造成危險，或對持續操作造成危險，例如鎖定帳戶的根使用者。StorageGRID S3 REST API 實作在政策驗證期間的限制比 Amazon 少，但在策略評估期間同樣嚴格。

政策說明	策略類型	亞馬遜行為	StorageGRID行為
拒絕自己對 root 帳號的任何權限	桶	有效且強制執行，但根用戶帳戶保留所有 S3 儲存桶策略操作的權限	相同的
拒絕任何使用者/群組權限	團體	有效且強制執行	相同的
允許外部帳戶群組任何權限	桶	無效的委託人	有效，但所有 S3 儲存桶策略操作的權限在策略允許的情況下都會傳回 405 方法不允許錯誤
允許外部帳戶root或使用者任何權限	桶	有效，但所有 S3 儲存桶策略操作的權限在策略允許的情況下都會傳回 405 方法不允許錯誤	相同的
允許每個人執行所有操作的權限	桶	有效，但所有 S3 儲存桶策略操作的權限都會為外部帳戶根和使用者傳回 405 方法不允許錯誤	相同的

政策說明	策略類型	亞馬遜行為	StorageGRID行為
拒絕所有人執行所有操作的權限	桶	有效且強制執行，但根用戶帳戶保留所有 S3 儲存桶策略操作的權限	相同的
主體是不存在的使用者或群組	桶	無效的委託人	有效的
資源是不存在的 S3 儲存桶	團體	有效的	相同的
校長是當地團體	桶	無效的委託人	有效的
策略授予非所有者帳戶（包括匿名帳戶）放置物件的權限。	桶	有效的。物件歸創建者帳戶所有，且儲存桶策略不適用。創建者帳戶必須使用物件 ACL 授予該物件的存取權限。	有效的。物件歸儲存桶擁有者帳戶所有。儲存桶策略適用。

一次寫入多次讀取 (WORM) 保護

您可以建立一次寫入多次讀取 (WORM) 儲存桶來保護資料、使用者定義的物件元資料和 S3 物件標記。您可以配置 WORM 儲存桶以允許建立新物件並防止覆蓋或刪除現有內容。使用此處描述的方法之一。

為了確保始終拒絕覆蓋，您可以：

- 從網格管理員中，前往 配置 > 安全 > 安全設定 > 網路和物件，然後選擇 *防止客戶端修改* 複選框。
- 應用以下規則和 S3 策略：
 - 將 PutOverwriteObject DENY 操作新增至 S3 策略。
 - 在 S3 策略中新增 DeleteObject DENY 操作。
 - 在 S3 策略中新增 PutObject ALLOW 操作。



當存在「30 天後零副本」等規則時，在 S3 策略中將 DeleteObject 設為 DENY 並不能阻止 ILM 刪除物件。



即使應用了所有這些規則和策略，它們也無法防止並發寫入（請參閱情況 A）。它們確實可以防止連續完成的覆蓋（參見情況 B）。

情況 A：併發寫入（未防範）

```
/mybucket/important.doc
PUT#1 ---> OK
PUT#2 -----> OK
```

情況 B：順序完成覆蓋（防範）

```
/mybucket/important.doc
PUT#1 -----> PUT#2 ---X (denied)
```

相關資訊

- ["StorageGRID ILM 規則如何管理對象"](#)
- ["儲存桶策略範例"](#)
- ["群組原則範例"](#)
- ["使用 ILM 管理對象"](#)
- ["使用租用戶帳戶"](#)

儲存桶策略範例

使用本節中的範例為儲存桶建立StorageGRID存取策略。

儲存桶策略指定該策略所附加到的儲存桶的存取權限。您可以透過以下工具之一使用 S3 PutBucketPolicy API 設定儲存桶策略：

- ["租戶經理"](#)。
- AWS CLI 使用此命令（請參閱["對 bucket 的操作"](#)):

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
file://policy.json
```

範例：允許每個人對儲存桶進行唯讀訪問

在這個例子中，允許所有人（包括匿名使用者）列出儲存桶中的對象，並對儲存桶中的所有物件執行 GetObject 操作。所有其他操作都將被拒絕。請注意，此策略可能不是特別有用，因為除了帳戶根之外沒有人有權限寫入儲存桶。

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket", "arn:aws:s3:::examplebucket/*"]
    }
  ]
}
```

範例：允許一個帳戶中的每個人對儲存桶進行完全訪問，並允許另一個帳戶中的每個人對儲存桶進行唯讀訪問

在此範例中，一個指定帳戶中的每個人都被允許完全存取儲存桶，而另一個指定帳戶中的每個人只被允許列出儲存桶並對儲存桶中以開頭的物件執行 `GetObject` 操作 `shared/` 物件鍵前綴。



在StorageGRID中，非擁有者帳戶（包括匿名帳戶）建立的物件歸儲存桶擁有者帳戶所有。儲存桶策略適用於這些物件。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "95390887230002558202"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/shared/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::examplebucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "shared/*"
        }
      }
    }
  ]
}
```

範例：允許每個人對儲存桶進行唯讀訪問，並允許指定群組進行完全訪問

在這個例子中，包括匿名用戶在內的每個人都可以列出儲存桶並對儲存桶中的所有物件執行 `GetObject` 操作，而只有屬於該群組的用戶 `Marketing` 指定帳戶中的使用者可以獲得完全存取權限。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/Marketing"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3:ListBucket", "s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

範例：如果客戶端在 IP 範圍內，則允許每個人對儲存桶進行讀寫訪問

在此範例中，允許所有人（包括匿名使用者）列出儲存桶並對儲存桶中的所有物件執行任何物件操作，前提是請求來自指定的 IP 範圍（54.240.143.0 到 54.240.143.255，54.240.143.188 除外）。所有其他操作都將被拒絕，並且所有超出 IP 範圍的請求都將被拒絕。

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadWriteAccessIfInSourceIpRange",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:*Object", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket", "arn:aws:s3:::examplebucket/*"],
      "Condition": {
        "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
        "NotIpAddress": {"aws:SourceIp": "54.240.143.188"}
      }
    }
  ]
}
```

範例：允許指定聯合用戶獨佔存取儲存桶的完全權限

在此範例中，聯合用戶 Alex 被允許完全訪問 `examplebucket` bucket 及其物件。所有其他使用者（包括“root”）均被明確拒絕所有操作。但請注意，「root」永遠不會被拒絕 Put/Get/DeleteBucketPolicy 的權限。

```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}

```

範例：PutOverwriteObject 權限

在這個例子中，Deny PutOverwriteObject 和 DeleteObject 的效果可確保沒有人可以覆寫或刪除物件的資料、使用者定義的元資料和 S3 物件標記。

```

{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutOverwriteObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::wormbucket/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"
      },
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}

```

群組原則範例

使用本節中的範例為群組建置StorageGRID存取策略。

群組原則指定該策略所屬群組的存取權限。沒有 `Principal` 元素，因為它是隱含的。群組原則是使用租用戶管理器或 API 進行設定的。

範例：使用租用戶管理器設定群組原則

當您在租用戶管理員中新增或編輯群組時，您可以選擇一個群組原則來確定該群組的成員將擁有哪些 S3 存取權。看 [為 S3 租用戶建立群組](#)。

- 無 **S3** 存取：預設選項。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。
- 唯讀存取：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：此群組中的使用者對 S3 資源（包括儲存桶）擁有完全存取權。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)。

- 自訂：群組中的使用者被授予您在文字方塊中指定的權限。

範例：允許群組完全存取所有儲存桶

在此範例中，除非儲存桶策略明確拒絕，否則群組中的所有成員都被允許完全存取租用戶帳戶擁有的所有儲存桶。

```
{
  "Statement": [
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

範例：允許群組對所有儲存桶進行唯讀訪問

在此範例中，群組中的所有成員都具有對 S3 資源的唯讀存取權限，除非儲存桶策略明確拒絕。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。

```
{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

範例：允許群組成員僅完全存取儲存桶中的“資料夾”

在此範例中，群組成員只被允許列出和存取指定儲存桶中的特定資料夾（鍵前綴）。請注意，在確定這些資料夾的隱私時，應考慮來自其他群組原則和儲存桶策略的存取權限。

```

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

```

審計日誌中追蹤的 S3 操作

審計訊息由StorageGRID服務產生並儲存在文字日誌檔案中。您可以查看審計日誌中特定於 S3 的審計訊息，以取得有關儲存桶和物件操作的詳細資訊。

審計日誌中追蹤的儲存桶操作

- 創建桶
- 刪除桶
- 刪除桶標記
- 刪除對象
- 取得桶標記
- 頭桶
- 清單對象
- 列出物件版本
- PUT Bucket 合規性
- PutBucketTagging
- PutBucket版本控制

審計日誌中追蹤的物件操作

- 完成多部分上傳
- 複製對象
- 刪除對象
- 取得對象
- 頭部對象
- 放置對象
- 復原對象
- 選擇對象
- UploadPart (當 ILM 規則使用 Balanced 或 Strict 攝取)
- UploadPartCopy (當 ILM 規則使用平衡或嚴格提取時)

相關資訊

- ["訪問審計日誌文件"](#)
- ["客戶端寫入審計訊息"](#)
- ["客戶端讀取審計訊息"](#)

使用 **Swift REST API** (生命週期結束)

使用 **Swift REST API**

對 Swift API 的支援已終止，並將在未來版本中刪除。



此版本的文件網站已刪除 Swift 詳細資訊。看 ["StorageGRID 11.8：使用 Swift REST API"](#)。

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。