使用StorageGRID

StorageGRID

NetApp
October 03, 2025

目錄

使用StorageGRID

使用租戶帳戶

使用租戶帳戶：總覽

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

什麼是租戶帳戶？

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

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

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

  > 如果您使用S3用戶端傳輸協定、也可以使用S3儲存區和儲存區原則來分隔企業部門之間的物件。您不需要建立個別的租戶帳戶。請參閱 實作S3用戶端應用程式的指示。

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

如何建立租戶帳戶

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

- 租戶的顯示名稱（租戶的帳戶ID會自動指派、無法變更）。
- 租戶帳戶是否會使用S3或Swift。
- 對於S3租戶帳戶：是否允許租戶帳戶使用平台服務。如果允許使用平台服務、則必須設定網格以支援其使用。
- 或者、租戶帳戶的儲存配額、也就是租戶物件可用的GB、TB或PB上限。租戶的儲存配額代表邏輯容量（物件大小）、而非實體容量（磁碟大小）。
- 如果啟用StorageGRID 身分識別聯盟以供支援整個系統、則哪個聯盟群組具有root存取權限可設定租戶帳戶。
- 如果StorageGRID 不使用單一登入（SSO）進行支援、則租戶帳戶是使用自己的身分識別來源、還是共用網格的身分識別來源、以及租戶本機root使用者的初始密碼。

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

設定**S3**租戶

之後是 S3租戶帳戶已建立、您可以存取租戶管理程式來執行下列工作：

- 設定身分識別聯盟（除非身分識別來源與網格共用）、或建立本機群組和使用者
- 管理S3存取金鑰
- 建立及管理S3儲存區、包括符合法規的儲存區
- 使用平台服務（若已啟用）
- 監控儲存使用量

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

設定**Swift**租戶

之後 Swift租戶帳戶已建立、您可以存取租戶管理程式來執行下列工作：

- 設定身分識別聯盟（除非身分識別來源與網格共用）、以及建立本機群組和使用者
- 監控儲存使用量

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

使用租戶管理程式

租戶管理程式可讓您管理StorageGRID 一個無租戶帳戶的所有層面。

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

如何登入及登出

登入租戶管理程式

若要存取租戶管理程式、請在的網址列中輸入租戶的URL 支援的網頁瀏覽器。

您需要的產品

- 您必須擁有登入認證資料。
- 您必須擁有網格管理員所提供的URL、才能存取租戶管理程式。此URL的範例如下所示：

```
https://FQDN_or_Admin_Node_IP/
```

```
https://FQDN_or_Admin_Node_IP:port/
```

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

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

URL一律包含完整網域名稱（FQDN）或用於存取管理節點的IP位址、也可以選擇性地包含連接埠號碼、20位數租戶帳戶ID或兩者。

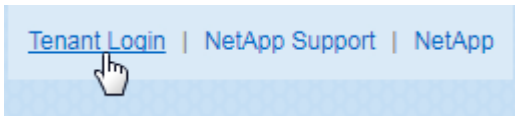
- 如果URL不包含租戶的20位數帳戶ID、您必須擁有此帳戶ID。
- 您必須使用 支援的網頁瀏覽器。
- Cookie必須在您的網路瀏覽器中啟用。
- 您必須擁有特定的存取權限。

步驟

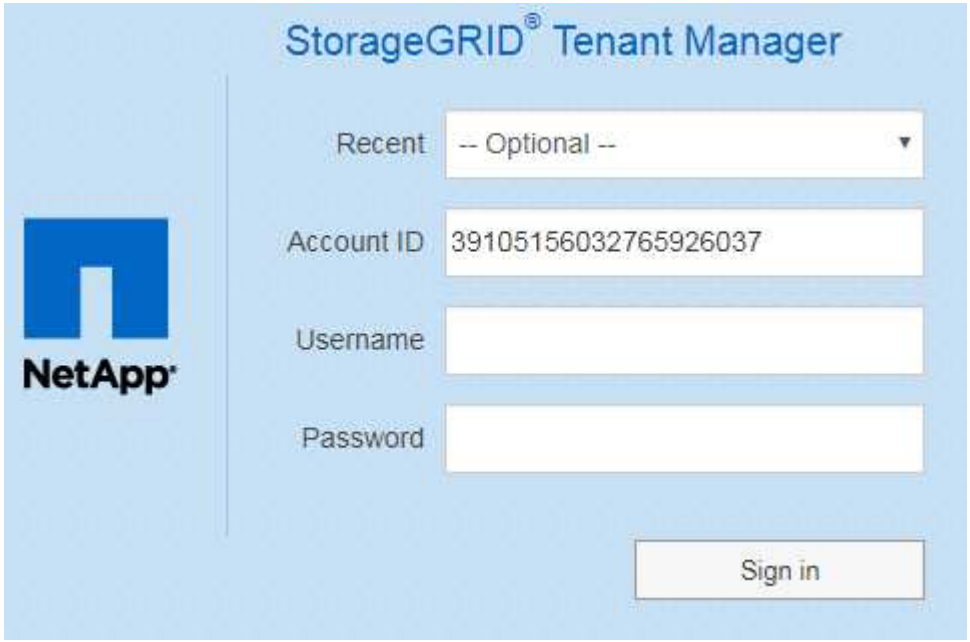
1. 啟動A 支援的網頁瀏覽器。
2. 在瀏覽器的網址列中、輸入存取租戶管理程式的URL。
3. 如果系統提示您輸入安全性警示、請使用瀏覽器的安裝精靈來安裝憑證。
4. 登入租戶管理程式。

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

   - Grid Manager登入頁面。按一下右上角的*租戶登入*連結。

   - 租戶管理程式登入頁面。「帳戶**ID**」欄位可能已經完成、如下所示。

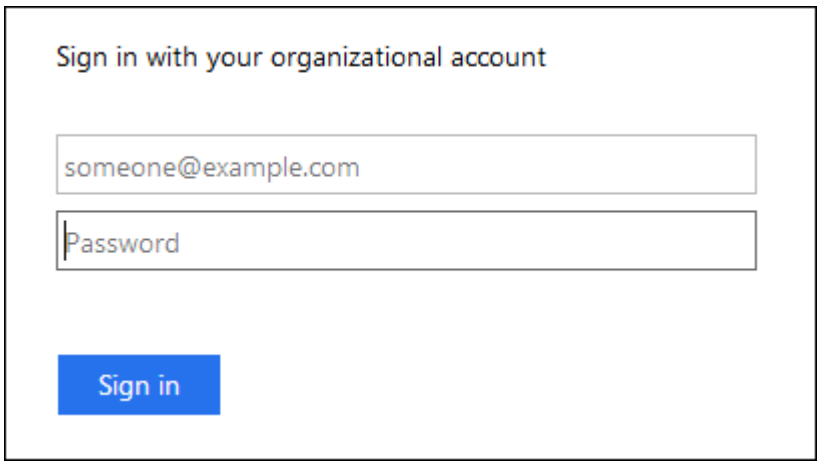
     i. 如果租戶的20位數帳戶ID未顯示、請選取租戶帳戶名稱（如果出現在最近帳戶清單中）、或輸入帳戶ID。

ii. 輸入您的使用者名稱和密碼。

iii. 按一下*登入*。

此時會顯示租戶管理程式儀表板。

- 如果網格上已啟用SSO、則會顯示貴組織的SSO頁面。例如：



輸入您的標準SSO認證、然後按一下*登入*。

- 租戶管理程式SSO登入頁面。

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

ii. 按一下*登入*。

iii. 在組織的SSO登入頁面上、以標準SSO認證登入。

此時會顯示租戶管理程式儀表板。

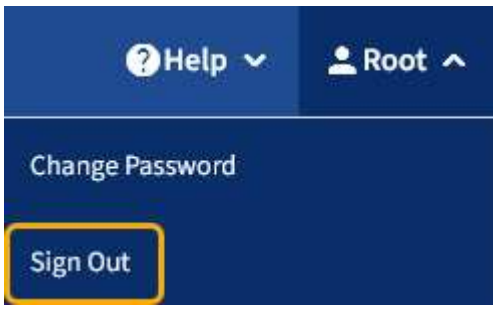
5. 如果您收到其他人的初始密碼、請變更密碼以保護您的帳戶安全。選擇「使用者名稱_>*變更密碼*」。

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

使用Tenant Manager之後、您必須登出、以確保未獲授權的使用者無法存取StorageGRID該系統。根據瀏覽器Cookie設定、關閉瀏覽器可能不會將您登出系統。

步驟

1. 在使用者介面的右上角找到使用者名稱下拉式清單。



2. 選取使用者名稱、然後選取*登出*。

   - 如果未使用SSO：

     您已登出管理節點。隨即顯示「租戶管理程式」登入頁面。

     如果您登入多個管理節點、則必須登出每個節點。

   - 如果啟用SSO：

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

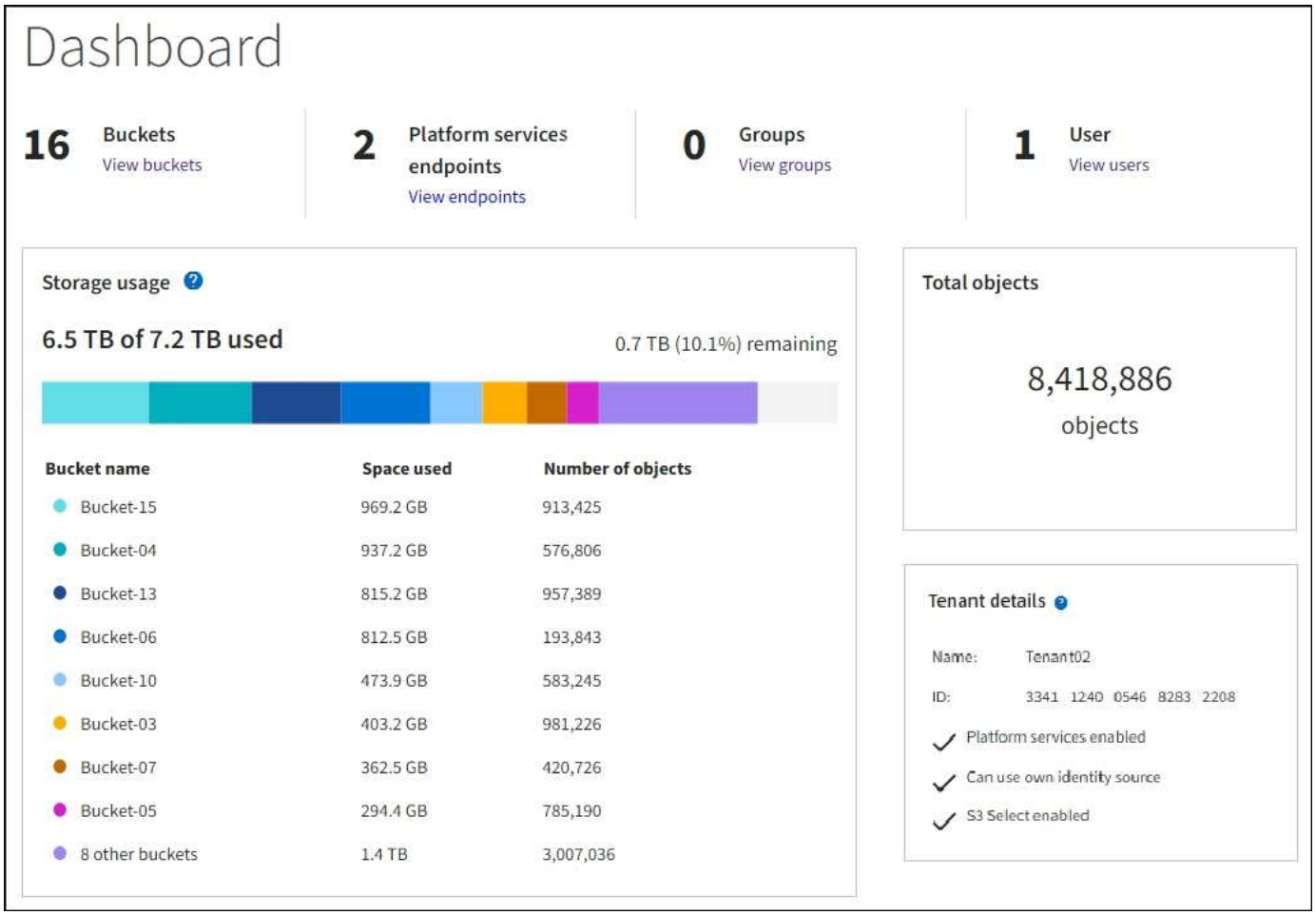
如果已啟用SSO、而且您也已登入Grid Manager、您也必須登出Grid Manager以登出SSO。

瞭解租戶管理程式儀表板

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

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

物件上傳後、儀表板的範例如下所示：



租戶帳戶摘要

儀表板頂端包含下列資訊：

- 已設定的儲存區或容器、群組和使用者數量
- 平台服務端點的數量（若有）

您可以選取連結來檢視詳細資料。

儀表板右側包含下列資訊：

- 租戶的物件總數。

  對於S3帳戶、如果沒有任何物件被擷取、而且您具有「根存取」權限、則會顯示「入門指南」、而非物件總數。

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

儲存設備與配額使用量

「儲存設備」使用面板包含下列資訊：

- 租戶的物件資料量。

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

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

配額使用率是根據內部預估、在某些情況下可能會超過。例如StorageGRID 、當租戶開始上傳物件時、會檢查配額、如果租戶超過配額、則會拒絕新的擷取。不過StorageGRID 、判斷是否超過配額時、不考慮目前上傳的大小。如果刪除物件、則在重新計算配額使用率之前、租戶可能會暫時無法上傳新物件。配額使用率計算可能需要10分鐘或更長時間。

- 代表最大桶或容器之相對大小的長條圖。

  您可以將游標放在任何圖表區段上、以檢視該區段或容器所耗用的總空間。

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

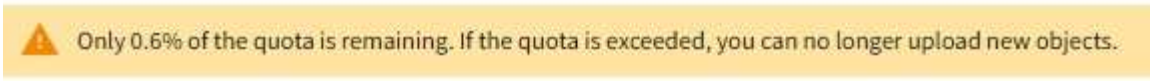
Bucket name	Space used	Number of objects
Bucket-02	944.7 GB	7,575
Bucket-09	899.6 GB	589,677
Bucket-15	889.6 GB	623,542
Bucket-06	846.4 GB	648,619
Bucket-07	730.8 GB	808,655
Bucket-04	700.8 GB	420,493
Bucket-11	663.5 GB	993,729
Bucket-03	656.9 GB	379,329
9 other buckets	2.3 TB	5,171,588

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

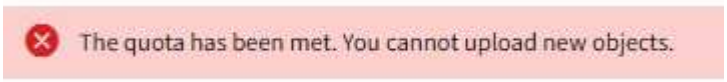
配額使用量警示

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

如果已使用90%以上的租戶配額、則會觸發*租戶配額使用量高*警示。如需詳細資訊、請參閱監控StorageGRID和疑難排解功能的說明中的警示參考資料。



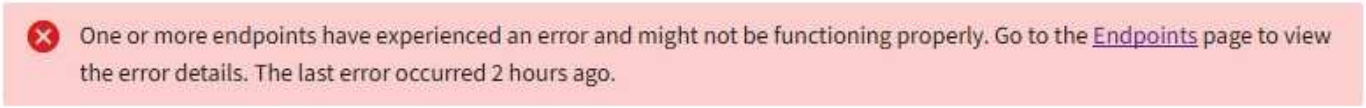
如果超出配額、就無法上傳新物件。



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

端點錯誤

如果您已使用Grid Manager設定一或多個端點以搭配平台服務使用、則租戶管理程式儀表板會在過去七天內發生任何端點錯誤時顯示警示。



若要查看端點錯誤的詳細資料、請選取「端點」以顯示「端點」頁面。

相關資訊

疑難排解平台服務端點錯誤

監控及疑難排解

租戶管理API

瞭解租戶管理API

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

租戶管理API：

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

若要存取租戶管理API的Swagger文件：

步驟

1. 登入租戶管理程式。
2. 從租戶管理程式頂端、選取說明圖示、然後選取* API Documentation *。

API作業

租戶管理API會將可用的API作業組織成下列區段：

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

  租戶管理API支援承載權杖驗證方案。對於租戶登入、您可以在驗證要求的Json實體（即「POST /API/v3/授權」）中提供使用者名稱、密碼和帳戶ID。如果使用者已成功驗證、則會傳回安全性權杖。此權杖必須在後續API要求（「授權：承載權杖」）的標頭中提供。

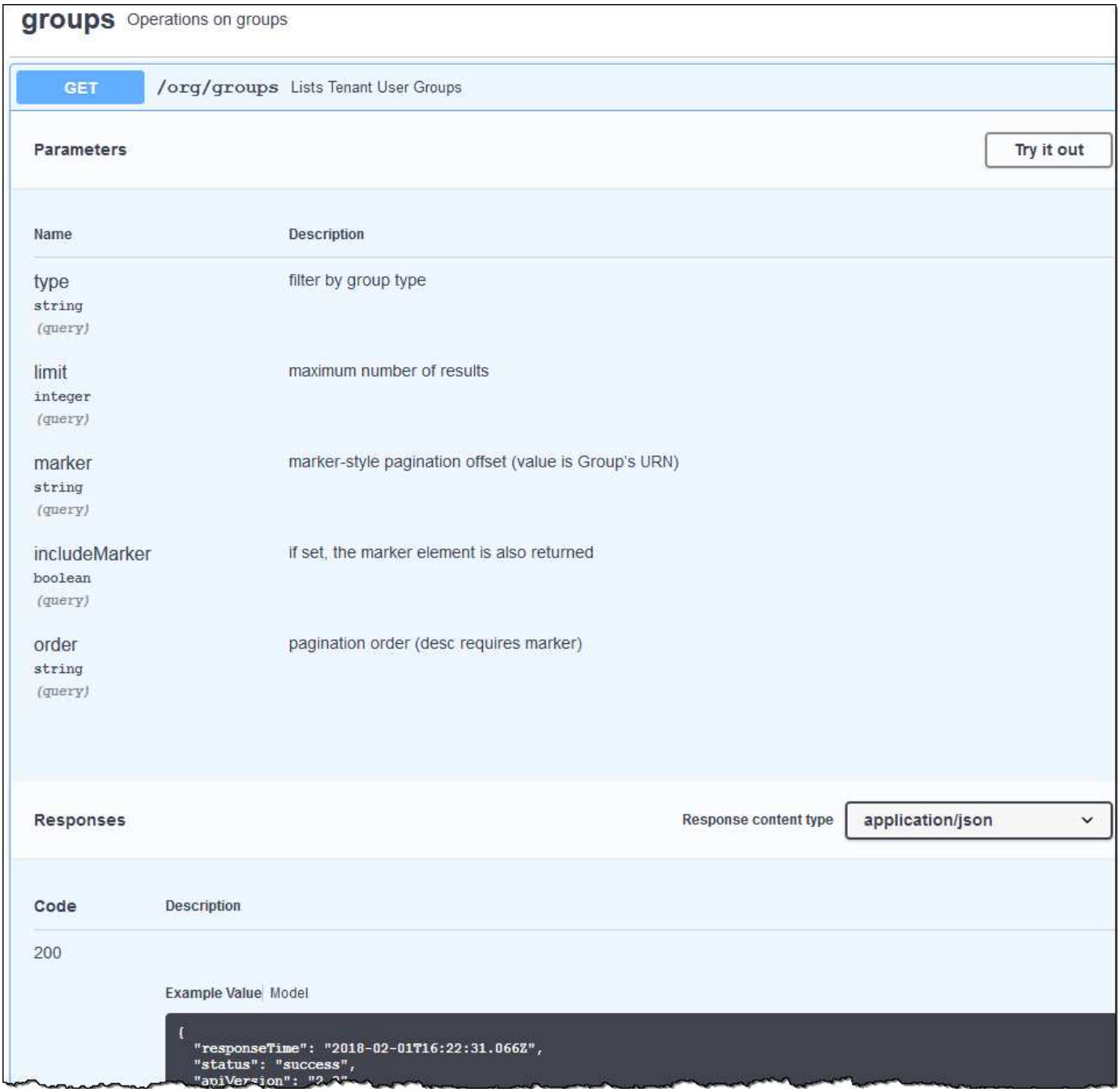
  如需改善驗證安全性的資訊、請參閱 防止跨網站要求偽造。

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

- 組態-與租戶管理API產品版本相關的作業。您可以列出該版本所支援的產品版本和主要API版本。
- * Container *：在S3貯體或Swift Container上的作業、如下所示：
- S三*
  - 建立儲存區（啟用或不啟用S3物件鎖定）
  - 修改庫位預設保留（適用於啟用S3物件鎖定的庫位）
  - 設定對物件執行之作業的一致性控制
  - 建立、更新及刪除儲存庫的CORS組態
  - 啟用和停用物件的上次存取時間更新
  - 管理平台服務的組態設定、包括CloudMirror複寫、通知及搜尋整合（中繼資料通知）
  - 刪除空的儲存區
- Swift *：設定用於容器的一致性層級
- 停用功能-檢視可能已停用之功能的作業。
- 端點：管理端點的作業。端點可讓S3儲存區使用外部服務StorageGRID 來進行CloudMirror複寫、通知或搜尋整合。
- 群組：管理本機租戶群組及從外部身分識別來源擷取同盟租戶群組的作業。
- 身分識別來源-作業：設定外部身分識別來源、以及手動同步處理聯盟群組與使用者資訊。
- 地區-作業、以判斷StorageGRID 哪些地區已設定用於該系統。
- * S3 *：管理租戶使用者S3存取金鑰的作業。
- * S3-object-lock *-在全域S3物件鎖定設定上執行作業、用於支援法規遵循。
- 使用者-檢視及管理租戶使用者的作業。

營運詳細資料

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



發出**API**要求

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

步驟

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

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

租戶管理**API**版本管理

租戶管理API使用版本管理來支援不中斷營運的升級。

例如、此Request URL會指定API版本3。

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

當進行*不相容*的變更時、會使租戶管理API的主要版本與舊版相容。當做出*與舊版相容*的變更時、租戶管理API的次要版本會被提升。相容的變更包括新增端點或新屬性。下列範例說明如何根據所做的變更類型來提高API版本。

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

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

過時的要求會以下列方式標示為已過時：

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

判斷目前版本支援哪些**API**版本

使用下列API要求傳回支援的API主要版本清單：

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

指定要申請的**API**版本

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

```
curl https://[IP-Address]/api/v3/grid/accounts

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

防範跨網站要求偽造（**CSRF**）

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

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

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

若要啟用此功能、請在驗證期間將「csrfToken」參數設為「true」。預設值為「假」。

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

如果為真、「GridCsrfToken」Cookie會以隨機值設定、以供登入Grid Manager、而「AccountCsrfToken」Cookie則會以隨機值設定、以供登入租戶管理程式。

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

- 「X-CSRF-Token」標頭、其標頭值設為CSRF權杖Cookie的值。
- 對於接受格式編碼實體的端點：「csrfToken」格式編碼的要求實體參數。

若要設定CSRF保護、請使用 網格管理API 或 租戶管理API。

> 若要求具有CSRF權杖Cookie集、也會針對任何要求執行「Content-Type：application/json」標頭、以進一步保護Json要求實體免受CSRF攻擊。

管理系統存取

使用身分識別聯盟

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

設定租戶管理程式的身分識別聯盟

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

您需要的產品

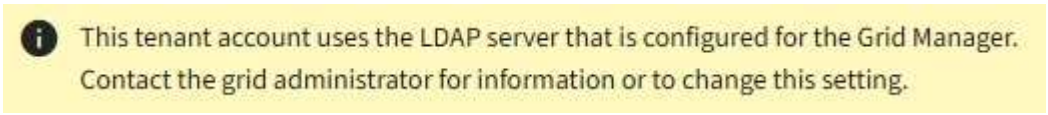
- 您將使用登入租戶管理程式 支援的網頁瀏覽器。
- 您擁有特定的存取權限。
- 您使用Active Directory、Azure AD、OpenLDAP或Oracle Directory Server做為身分識別供應商。

  如果您想使用未列出的LDAP v3服務、請聯絡技術支援部門。

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

關於這項工作

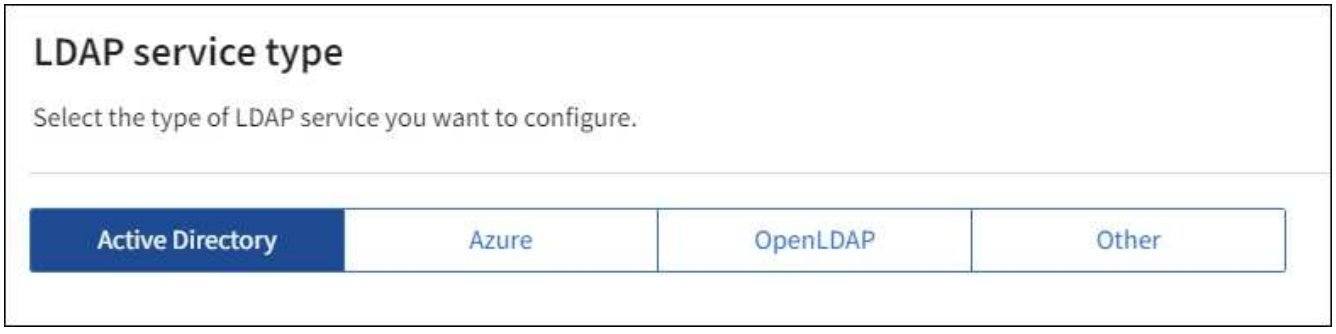
您是否可以為租戶設定身分識別聯盟服務、取決於租戶帳戶的設定方式。您的租戶可能會共用為Grid Manager設定的身分識別聯盟服務。如果您在存取「身分識別聯盟」頁面時看到此訊息、則無法為此租戶設定個別的聯盟身分識別來源。



輸入組態

步驟

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



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

4. 如果選擇*其他*、請填寫「LDAP屬性」區段中的欄位。否則、請前往下一步。
   - 使用者唯一名稱：含有LDAP使用者唯一識別碼的屬性名稱。此屬性相當於Active Directory的「shamAccountName」和OpenLDAP的「uid」。如果您要設定Oracle Directory Server、請輸入「uid」。
   - *使用者UUID *：含有LDAP使用者永久唯一識別碼的屬性名稱。此屬性相當於Active Directory的「objectGuid」和OpenLDAP的「entryUUID」。如果要配置Oracle Directory Server、請輸入「nssiuniuniid」。指定屬性的每個使用者值必須是16位元組或字串格式的32位數十六進位數字、連字號會被忽略。
   - 群組唯一名稱：包含LDAP群組唯一識別碼的屬性名稱。此屬性相當於Active Directory的「shamAccountName」和OpenLDAP的「CN」。如果您要設定Oracle Directory Server、請輸入「CN」。
   - *群組UUID *：包含LDAP群組永久唯一識別碼的屬性名稱。此屬性相當於Active Directory的「objectGuid」和OpenLDAP的「entryUUID」。如果要配置Oracle Directory Server、請輸入「nssiuniuniid」。指定屬性的每個群組值必須是16位元組或字串格式的32位數十六進位數字、連字號會被忽略。
5. 對於所有LDAP服務類型、請在「設定LDAP伺服器」區段中輸入所需的LDAP伺服器和網路連線資訊。
   - 主機名稱：LDAP伺服器的完整網域名稱（FQDN）或IP位址。
   - 連接埠：用於連接LDAP伺服器的連接埠。

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

   - 使用者名稱：將連線至LDAP伺服器之使用者的辨別名稱（DN）完整路徑。

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

     指定的使用者必須擁有列出群組和使用者的權限、並可存取下列屬性：

     - 「AMAccountName」或「uid」
     - "objectGUID"、"entryUUUID"或"nssiuniuniid"
     - 《中國》
     - 「memberof」或「isMemberOf」
     - * Active Directory *：「objectSid」、「primaryGroupID」、「userAccountControl」及「userPrincipalName」
     - * Azure *：「帳戶已啟用」和「userPrincipalName」
   - 密碼：與使用者名稱相關的密碼。
   - 群組基礎**DN**：您要搜尋群組之LDAP子樹狀結構的辨別名稱（DN）完整路徑。在Active Directory範例（如下）中、識別名稱相對於基礎DN（DC=storagegRID、DC=example、DC=com）的所有群組均可做為聯盟群組使用。

     「群組唯一名稱*」值必須在所屬的*群組基礎DN*中是唯一的。

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

  *使用者唯一名稱*值必須在其所屬的*使用者基礎DN*內是唯一的。

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

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

  輸入下列其中一種模式：

  - 使用者主體名稱模式（**Active Directory**和**Azure**）：「[username]@*example*.com」
  - 低層級登入名稱模式（**Active Directory**和**Azure**）：「*example*\[username]」
  - 辨別名稱模式：「CN=[username]、CN=Users、DC=*examends*、DC=com」

    請準確附上所寫的*（使用者名稱）*。

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

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

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

     如果選取此設定、請將自訂安全性憑證複製並貼到CA憑證文字方塊中。

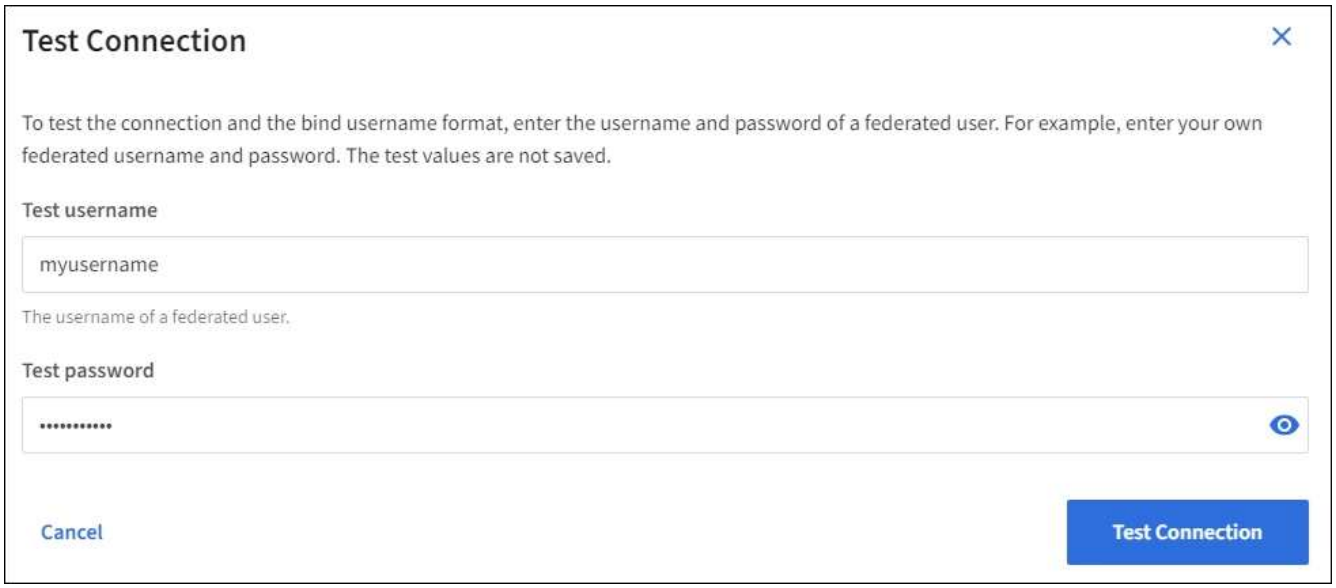
測試連線並儲存組態

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

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

3. 如果您提供連結使用者名稱格式、請輸入有效同盟使用者的使用者名稱和密碼。

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



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

強制與身分識別來源同步

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

步驟

1. 前往「身分識別聯盟」頁面。
2. 選取頁面頂端的*同步伺服器*。

   視您的環境而定、同步處理程序可能需要一些時間。

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

停用身分識別聯盟

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

關於這項工作

在停用身分識別聯盟之前、您應注意下列事項：

- 聯盟使用者將無法登入。

- 目前已登入的聯盟使用者將在StorageGRID 其工作階段過期之前保留對此系統的存取權、但在工作階段過期後仍無法登入。
- 不會在不同步系統與身分識別來源之間進行同步、StorageGRID 也不會針對尚未同步的帳戶發出警示或警示。
- 如果單一登入（SSO）設定為*已啟用*或*沙箱模式*、則「啟用身分聯盟」核取方塊會停用。「單一登入」頁面的SSO狀態必須為*停用*、才能停用身分識別聯盟。請參閱 停用單一登入。

步驟

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

設定**OpenLDAP**伺服器的準則

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

> 對於非ActiveDirectory或Azure的身分識別來源、StorageGRID 無法自動封鎖S3存取外部停用的使用者。若要封鎖S3存取、請刪除使用者的任何S3金鑰、並將使用者從所有群組中移除。

memberOf和**refert**覆疊

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

索引

您必須使用指定的索引關鍵字來設定下列OpenLDAP屬性：

- 「olcDbIndex：objectClass eq」
- 「olcDbIndex：UID eq、pres、sub」
- 「olcDbIndex：cN eq、pres、sub」
- 「olcDbIndex：entryUUID eq」

此外、請確定使用者名稱說明中所述的欄位已建立索引、以獲得最佳效能。

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

管理群組

為**S3**租戶建立群組

您可以匯入同盟群組或建立本機群組、來管理S3使用者群組的權限。

您需要的產品

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

如需S3的相關資訊、請參閱 使用S3。

步驟

1. 選擇*存取管理*>*群組*。

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

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

4. 輸入群組名稱。
   - 本機群組：輸入顯示名稱和唯一名稱。您可以稍後再編輯顯示名稱。
   - 聯盟群組：輸入唯一名稱。對於Active Directory、唯一名稱是與「shamAccountName」屬性相關聯的名稱。對於OpenLDAP、唯一名稱是與「uid」屬性相關聯的名稱。
5. 選擇*繼續*。
6. 選取存取模式。如果使用者屬於多個群組、且任何群組設定為唯讀、則使用者將擁有所有選取設定和功能的唯讀存取權。
   - 讀寫（預設）：使用者可以登入租戶管理程式、並管理租戶組態。
   - 唯讀：使用者只能檢視設定和功能。他們無法在租戶管理程式或租戶管理API中進行任何變更或執行任何作業。本機唯讀使用者可以變更自己的密碼。
7. 選取此群組的群組權限。

   請參閱租戶管理權限的相關資訊。

8. 選擇*繼續*。
9. 選取群組原則、以判斷此群組成員將擁有哪些S3存取權限。

- 無**S3**存取：預設。此群組中的使用者沒有S3資源的存取權、除非使用資源桶原則授予存取權。如果選取此選項、預設只有root使用者可以存取S3資源。
- 唯讀存取：此群組中的使用者擁有S3資源的唯讀存取權。例如、此群組中的使用者可以列出物件並讀取物件資料、中繼資料和標記。選取此選項時、唯讀群組原則的Json字串會出現在文字方塊中。您無法編輯此字串。
- 完整存取：此群組中的使用者可完整存取S3資源、包括儲存區。選取此選項時、會在文字方塊中顯示完整存取群組原則的Json字串。您無法編輯此字串。
- 自訂：群組中的使用者會被授予您在文字方塊中指定的權限。如需群組原則的詳細資訊、包括語言語法和範例、請參閱實作S3用戶端應用程式的指示。

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

    在此範例中、群組成員只能列出及存取符合其使用者名稱（金鑰前置碼）的資料夾、並在指定的儲存區中使用。請注意、在決定這些資料夾的隱私權時、應考慮其他群組原則和儲存區原則的存取權限。

11. 根據您要建立同盟群組或本機群組、選取出現的按鈕：
    - 聯盟群組：建立群組
    - 本機群組：繼續

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

12. 選取您要新增至群組的每個使用者核取方塊、然後選取*建立群組*。

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

13. 選擇*完成*。

    您建立的群組會出現在群組清單中。由於快取、變更可能需要15分鐘才能生效。

為**Swift**租戶建立群組

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

您需要的產品

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

步驟

1. 選擇*存取管理*>*群組*。

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

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

4. 輸入群組名稱。
   - 本機群組：輸入顯示名稱和唯一名稱。您可以稍後再編輯顯示名稱。
   - 聯盟群組：輸入唯一名稱。對於Active Directory、唯一名稱是與「shamAccountName」屬性相關聯的名稱。對於OpenLDAP、唯一名稱是與「uid」屬性相關聯的名稱。

5. 選擇*繼續*。
6. 選取存取模式。如果使用者屬於多個群組、且任何群組設定為唯讀、則使用者將擁有所有選取設定和功能的唯讀存取權。
   - 讀寫（預設）：使用者可以登入租戶管理程式、並管理租戶組態。
   - 唯讀：使用者只能檢視設定和功能。他們無法在租戶管理程式或租戶管理API中進行任何變更或執行任何作業。本機唯讀使用者可以變更自己的密碼。
7. 設定群組權限。
   - 如果使用者需要登入租戶管理程式或租戶管理API、請選取*根存取*核取方塊。（預設）
   - 如果使用者不需要存取租戶管理程式或租戶管理API、請取消選取「根存取」核取方塊。例如、取消選取不需要存取租戶的應用程式核取方塊。然後、指派* Swift管理員*權限、讓這些使用者能夠管理容器和物件。
8. 選擇*繼續*。
9. 如果使用者需要使用Swift REST API、請選取「* Swift管理員*」核取方塊。

   Swift使用者必須擁有root存取權限、才能存取租戶管理程式。不過、「根存取」權限不允許使用者驗證Swift REST API、以建立容器和擷取物件。使用者必須具有Swift Administrator權限、才能驗證到Swift REST API。
10. 根據您要建立同盟群組或本機群組、選取出現的按鈕：
    - 聯盟群組：建立群組
    - 本機群組：繼續

      如果您要建立本機群組、在您選取*繼續*之後、會出現步驟4（新增使用者）。聯盟群組不會顯示此步驟。
11. 選取您要新增至群組的每個使用者核取方塊、然後選取*建立群組*。

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

    您建立的群組會出現在群組清單中。由於快取、變更可能需要15分鐘才能生效。

相關資訊

租戶管理權限

使用Swift

租戶管理權限

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

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

- 檢視儀表板
- 變更自己的密碼（適用於本機使用者）

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

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

您可以將下列權限指派給群組。請注意、S3租戶和Swift租戶擁有不同的群組權限。由於快取、變更可能需要15分鐘才能生效。

權限	說明
root存取權	提供租戶管理程式和租戶管理API的完整存取權限。 附註： Swift使用者必須擁有root存取權限、才能登入租戶帳戶。
系統管理員	僅限Swift租戶。提供此租戶帳戶的Swift容器和物件的完整存取權 附註： Swift使用者必須擁有Swift管理員權限、才能使用Swift REST API執行任何作業。
管理您自己的S3認證	僅限S3租戶。可讓使用者建立及移除自己的S3存取金鑰。沒有此權限的使用者不會看到*儲存設備（S3）*>*我的S3存取金鑰*功能表選項。
管理所有的儲存區	• S3租戶：可讓使用者使用租戶管理程式和租戶管理API來建立及刪除S3桶、並管理租戶帳戶中所有S3桶的設定、無論S3桶或群組原則為何。 沒有此權限的使用者將不會看到「桶」功能表選項。 • Swift租戶：可讓Swift使用者使用租戶管理API來控制Swift Container的一致性層級。 *附註：*您只能從租戶管理API將「管理所有桶」權限指派給Swift群組。您無法使用租戶管理程式將此權限指派給Swift群組。
管理端點	僅限S3租戶。可讓使用者使用租戶管理程式或租戶管理API來建立或編輯端點、這些端點是StorageGRID 用作支援不整平台服務的目的地。 沒有此權限的使用者不會看到*平台服務端點*功能表選項。

相關資訊

使用S3

使用Swift

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

您需要的產品

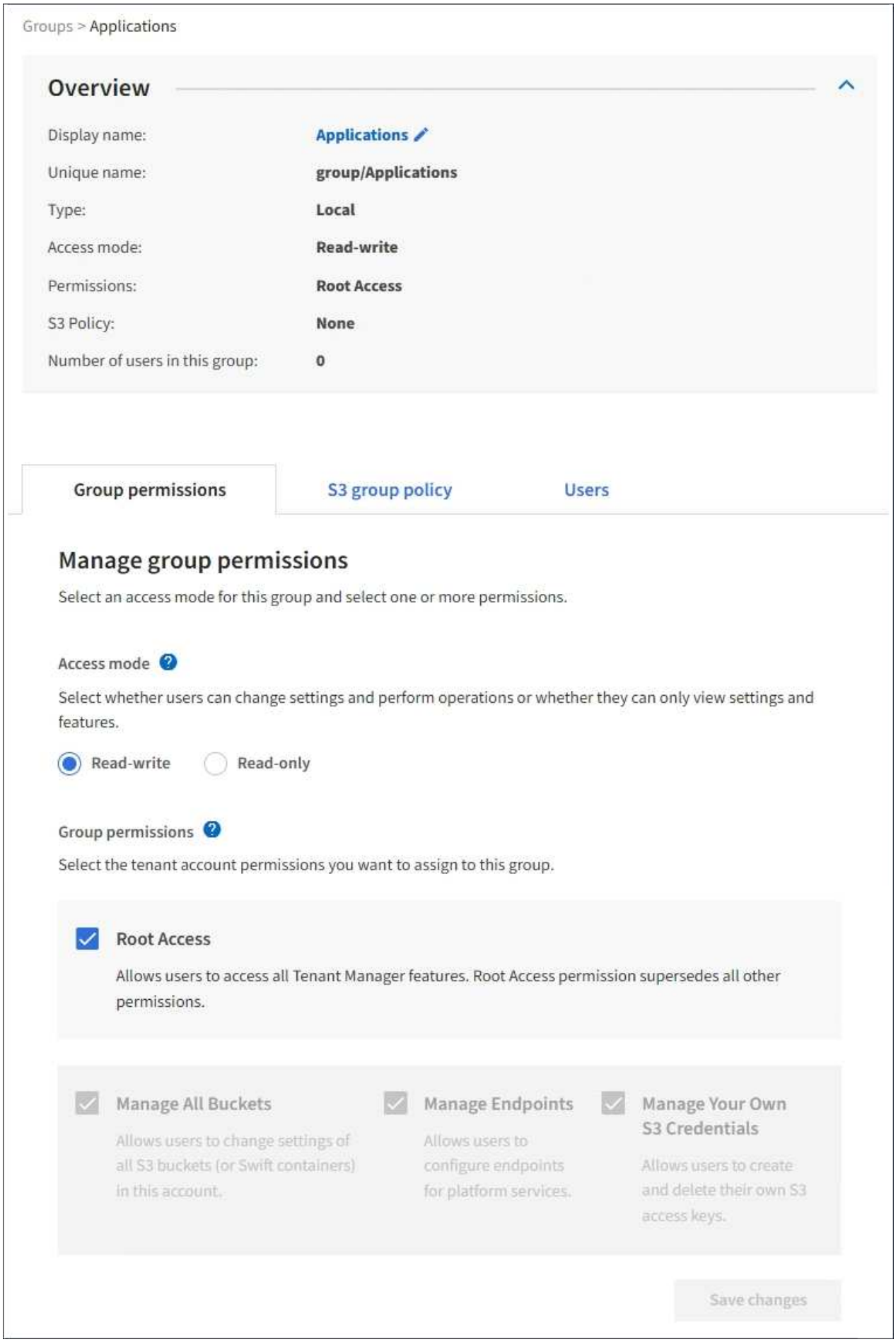
- 您必須使用登入租戶管理程式 支援的網頁瀏覽器。
- 您必須屬於具有「根存取」權限的使用者群組。

步驟

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

   或者、您也可以選取*「動作」>「檢視群組詳細資料」*。

   隨即顯示群組詳細資料頁面。以下範例顯示S3群組詳細資料頁面。


Groups > Applications
Overview
Display name:
Applications
Unique name:
group/Applications
Type:
Local
Access mode:
Read-write
Permissions:
Root Access
S3 Policy:
None
Number of users in this group:
0
Group permissions
S3 group policy
Users
Manage group permissions
Select an access mode for this group and select one or more permissions.
Access mode
Select whether users can change settings and perform operations or whether they can only view settings and features.
Read-write
Read-only
Group permissions
Select the tenant account permissions you want to assign to this group.
Root Access
Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.
Manage All Buckets
Allows users to change settings of all S3 buckets (or Swift containers) in this account.
Manage Endpoints
Allows users to configure endpoints for platform services.
Manage Your Own S3 Credentials
Allows users to create and delete their own S3 access keys.
Save changes

3. 視需要變更群組設定。

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

   a. 或者、選取顯示名稱或編輯圖示 以更新顯示名稱。

      您無法變更群組的唯一名稱。您無法編輯同盟群組的顯示名稱。

   b. 或者、請更新權限。

   c. 針對群組原則、請針對S3或Swift租戶進行適當的變更。

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

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

   d. 或者、新增或移除使用者。

4. 確認您已針對每個變更的區段選擇*儲存變更*。

   由於快取、變更可能需要15分鐘才能生效。

相關資訊

為S3租戶建立群組

為Swift租戶建立群組

新增使用者至本機群組

您可以視需要將使用者新增至本機群組。

您需要的產品

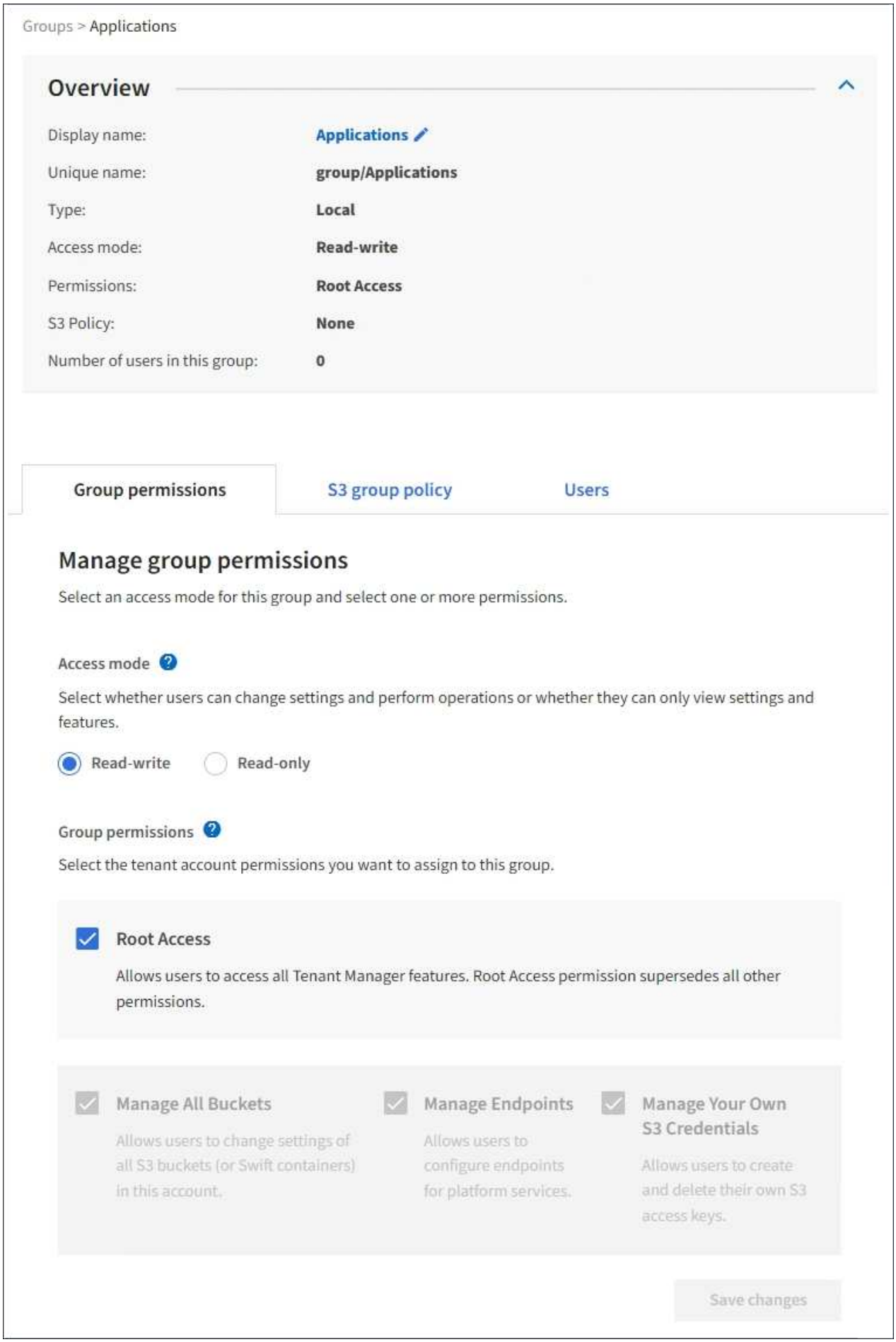
- 您必須使用登入租戶管理程式 支援的網頁瀏覽器。
- 您必須屬於具有「根存取」權限的使用者群組。

步驟

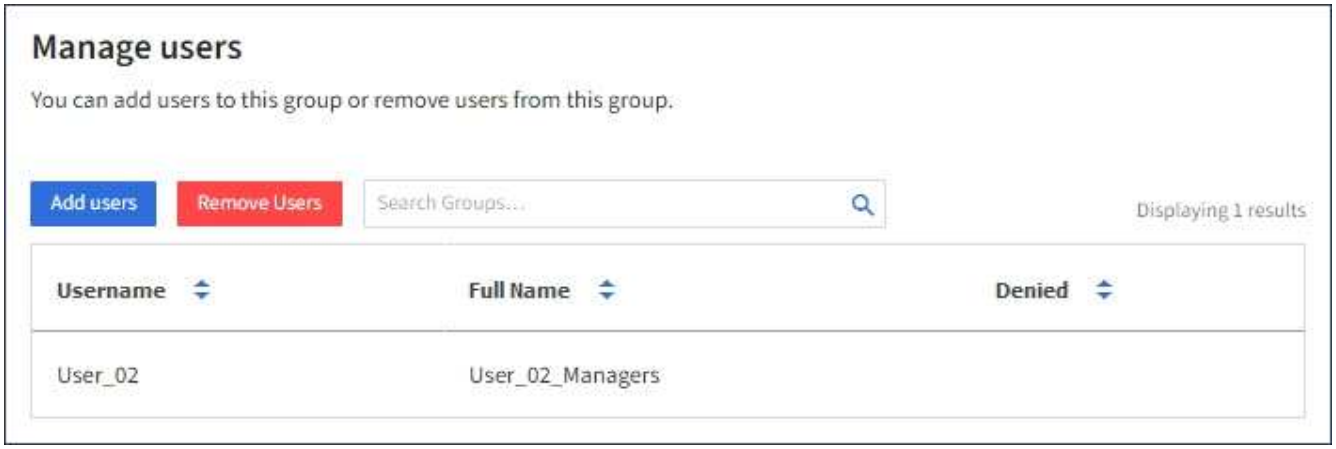
1. 選擇*存取管理*>*群組*。
2. 選取您要新增使用者的本機群組名稱。

   或者、您也可以選取*「動作」>「檢視群組詳細資料」*。

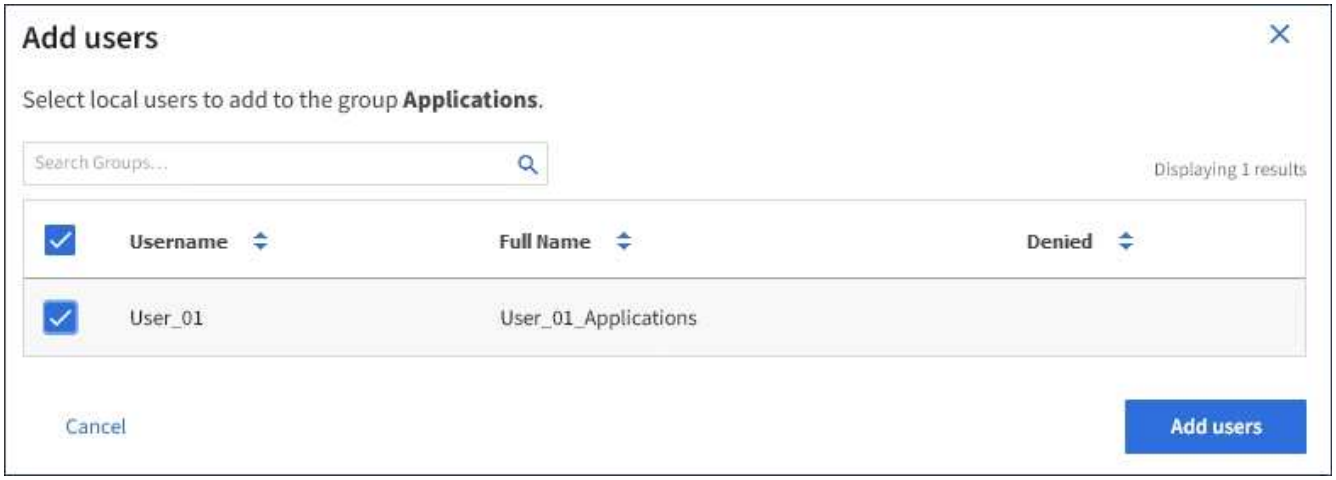
   隨即顯示群組詳細資料頁面。


Groups > Applications
Overview
Display name:
Applications
Unique name:
group/Applications
Type:
Local
Access mode:
Read-write
Permissions:
Root Access
S3 Policy:
None
Number of users in this group:
0
Group permissions
S3 group policy
Users
Manage group permissions
Select an access mode for this group and select one or more permissions.
Access mode
Select whether users can change settings and perform operations or whether they can only view settings and features.
Read-write
Read-only
Group permissions
Select the tenant account permissions you want to assign to this group.
Root Access
Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.
Manage All Buckets
Allows users to change settings of all S3 buckets (or Swift containers) in this account.
Manage Endpoints
Allows users to configure endpoints for platform services.
Manage Your Own S3 Credentials
Allows users to create and delete their own S3 access keys.
Save changes

3. 選取*使用者*、然後選取*新增使用者*。



4. 選取您要新增至群組的使用者、然後選取*新增使用者*。



頁面右上角會出現確認訊息。由於快取、變更可能需要15分鐘才能生效。

編輯群組名稱

您可以編輯群組的顯示名稱。您無法編輯群組的唯一名稱。

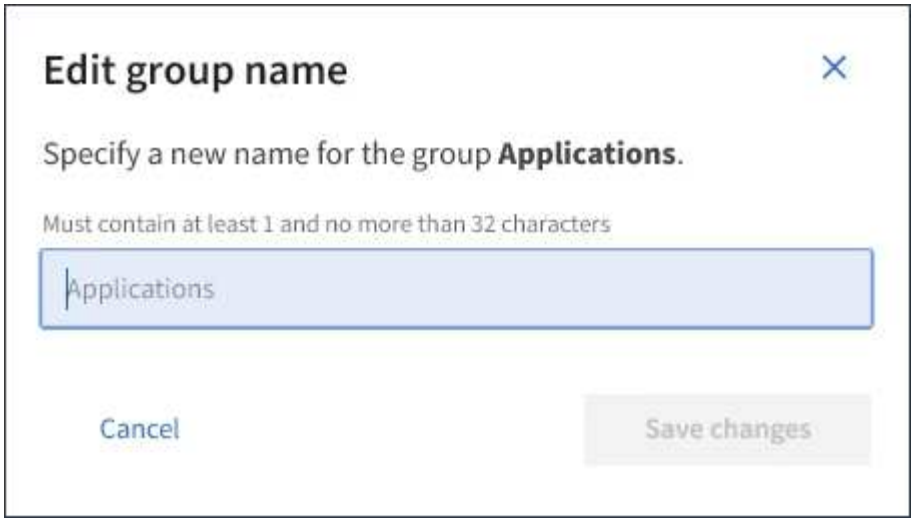
您需要的產品

- 您必須使用登入租戶管理程式 支援的網頁瀏覽器。
- 您必須屬於具有「根存取」權限的使用者群組。請參閱 租戶管理權限。

步驟

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

「編輯群組名稱」對話方塊隨即出現。



4. 如果您正在編輯本機群組、請視需要更新顯示名稱。

   您無法變更群組的唯一名稱。您無法編輯同盟群組的顯示名稱。

5. 選取*儲存變更*。

   頁面右上角會出現確認訊息。由於快取、變更可能需要15分鐘才能生效。

複製群組

您可以複製現有群組、以更快建立新群組。

您需要的產品

- 您必須使用登入租戶管理程式 支援的網頁瀏覽器。
- 您必須屬於具有「根存取」權限的使用者群組。請參閱 租戶管理權限。

步驟

1. 選擇*存取管理*>*群組*。
2. 選取您要複製之群組的核取方塊。
3. 選擇*複製群組*。如需建立群組的其他詳細資料、請參閱建立群組的指示 S3租戶 或是 Swift租戶。
4. 選取*本機群組*索引標籤以建立本機群組、或選取*聯盟群組*索引標籤、從先前設定的身分識別來源匯入群組。

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

5. 輸入群組名稱。
   - 本機群組：輸入顯示名稱和唯一名稱。您可以稍後再編輯顯示名稱。
   - 聯盟群組：輸入唯一名稱。對於Active Directory、唯一名稱是與「shamAccountName」屬性相關聯的名稱。對於OpenLDAP、唯一名稱是與「uid」屬性相關聯的名稱。
6. 選擇*繼續*。
7. 視需要修改此群組的權限。

8. 選擇*繼續*。
9. 如有需要、如果您要複製S3租戶的群組、請從*新增S3原則*選項按鈕中選擇不同的原則。如果您選取自訂原則、請視需要更新Json字串。
10. 選取*建立群組*。

刪除群組

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

您需要的產品

- 您必須使用登入租戶管理程式 支援的網頁瀏覽器。
- 您必須屬於具有「根存取」權限的使用者群組。請參閱 租戶管理權限。

步驟

1. 選擇*存取管理*>*群組*。

2. 選取您要刪除之群組的核取方塊。
3. 選擇*操作*>*刪除群組*。

   隨即顯示確認訊息。

4. 選擇*刪除群組*以確認您要刪除確認訊息中所示的群組。

   頁面右上角會出現確認訊息。由於快取、變更可能需要15分鐘才能生效。

管理本機使用者

您可以建立本機使用者並將其指派給本機群組、以決定這些使用者可以存取哪些功能。租

戶管理程式包含一個預先定義的本機使用者、名為「root」。 雖然您可以新增及移除本機使用者、但無法移除root使用者。

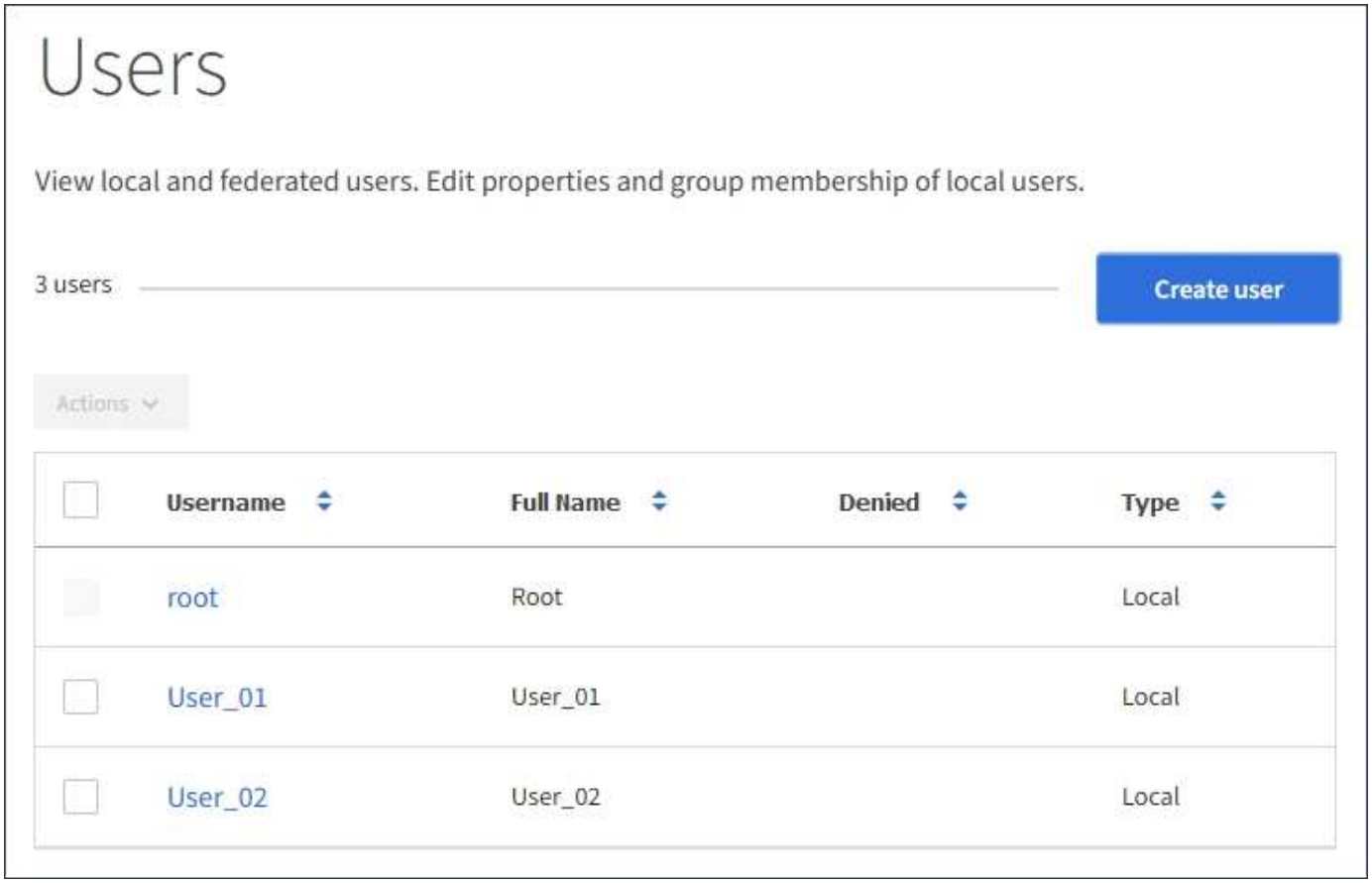
您需要的產品

- 您必須使用登入租戶管理程式 支援的網頁瀏覽器。
- 您必須屬於具有「根存取」權限的讀寫使用者群組。請參閱 租戶管理權限。

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

存取「使用者」頁面

選擇*存取管理*>*使用者*。



建立本機使用者

您可以建立本機使用者、並將其指派給一或多個本機群組、以控制其存取權限。

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

不屬於任何群組的Swift使用者不具備管理權限或Swift Container存取權。

步驟

1. 選取*建立使用者*。

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

     例如、您可以使用此功能暫時暫停使用者登入的能力。
3. 選擇*繼續*。
4. 將使用者指派給一或多個本機群組。

   不屬於任何群組的使用者將沒有管理權限。權限是累積性的。使用者將擁有所屬所有群組的所有權限。
5. 選取*建立使用者*。

   由於快取、變更可能需要15分鐘才能生效。

編輯使用者詳細資料

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

步驟

1. 在使用者清單中、選取您要檢視或編輯其詳細資料的使用者名稱。

   或者、您也可以選取使用者的核取方塊、然後選取*「Actions」（動作）>「View user details」（檢視使用者詳細資料）*。
2. 視需要變更使用者設定。
   a. 選取全名或編輯圖示、視需要變更使用者的全名 在「總覽」區段中。

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

      由於快取、變更可能需要15分鐘才能生效。

複製本機使用者

您可以複製本機使用者、以更快建立新使用者。

步驟

1. 在使用者清單中、選取您要複製的使用者。
2. 選擇*複製使用者*。
3. 修改新使用者的下列欄位。
   - 全名：此使用者的全名、例如、人員的名字和姓氏或應用程式的名稱。
   - 使用者名稱：此使用者用來登入的名稱。使用者名稱必須是唯一的、而且無法變更。
   - 密碼：使用者登入時使用的密碼。
   - 確認密碼：在「密碼」欄位中輸入相同的密碼。
   - 拒絕存取：如果您選取*是*、此使用者就無法登入租戶帳戶、即使該使用者仍屬於一或多個群組。

     例如、您可以使用此功能暫時暫停使用者登入的能力。
4. 選擇*繼續*。
5. 選取一或多個本機群組。

   不屬於任何群組的使用者將沒有管理權限。權限是累積性的。使用者將擁有所屬所有群組的所有權限。
6. 選取*建立使用者*。

   由於快取、變更可能需要15分鐘才能生效。

刪除本機使用者

您可以永久刪除不再需要存取StorageGRID 該經銷帳戶的本機使用者。

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

步驟

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

   由於快取、變更可能需要15分鐘才能生效。

管理**S3**租戶帳戶

管理**S3**存取金鑰

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

關於這項工作

S3存取金鑰的管理方式如下：

- 擁有*管理您自己的S3認證*權限的使用者、可以建立或移除自己的S3存取金鑰。

- 擁有「根存取」權限的使用者可以管理S3根帳戶和所有其他使用者的存取金鑰。根存取金鑰可讓租戶完整存取所有的貯體和物件、除非已明確停用貯體原則。

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

建立自己的**S3**存取金鑰

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

您需要的產品

- 您必須使用登入租戶管理程式 支援的網頁瀏覽器。
- 您必須擁有「管理自己的S3認證」權限。請參閱 租戶管理權限。

關於這項工作

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

每個金鑰都可以有特定的到期時間、或是沒有到期時間。請遵循下列到期時間準則：

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

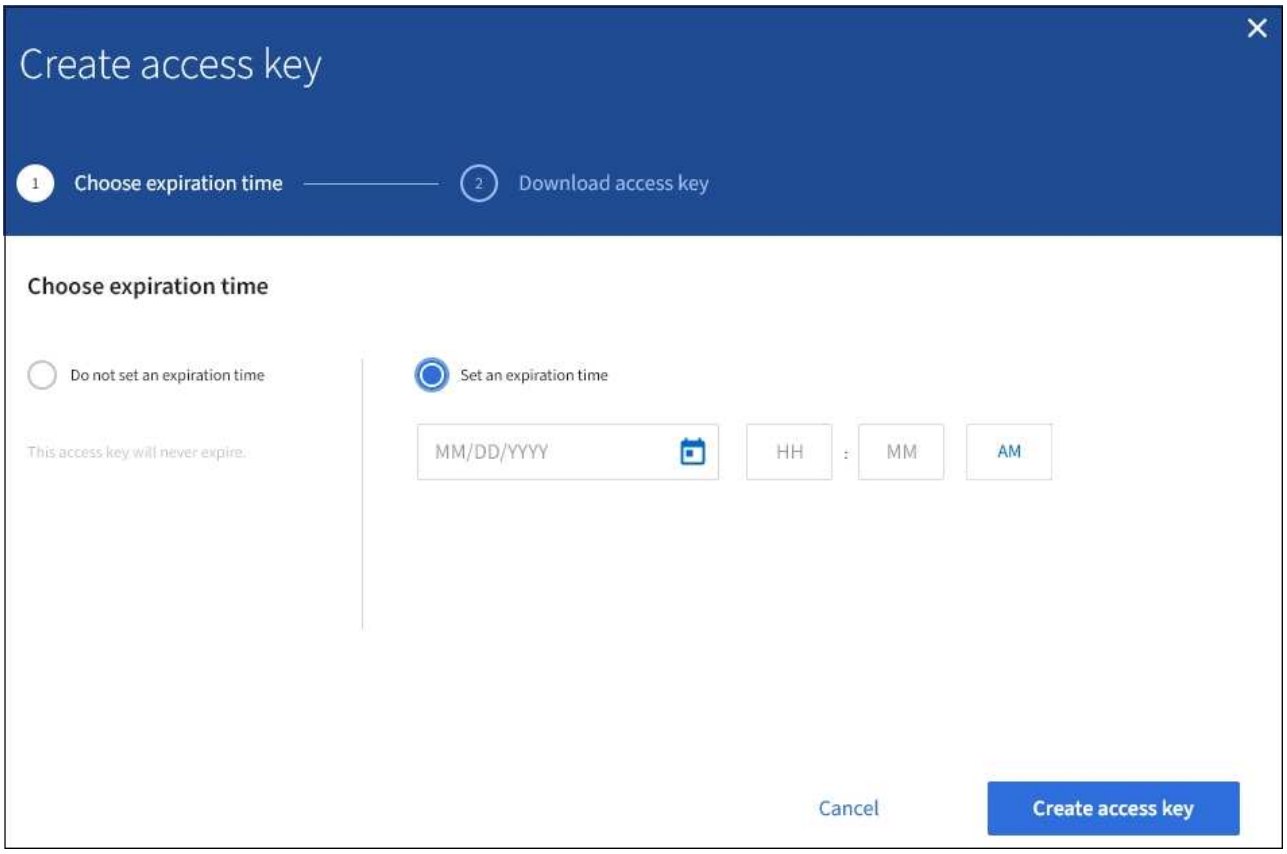
> 您可以使用租戶管理程式中顯示的帳戶存取金鑰ID和秘密存取金鑰、來存取屬於您帳戶的S3儲存區和物件。因此、請像保護密碼一樣保護存取金鑰。定期旋轉存取金鑰、從帳戶中移除任何未使用的金鑰、而且切勿與其他使用者共用。

步驟

1. 選擇*儲存設備（S3）>*我的存取金鑰。

   「我的存取金鑰」頁面隨即出現、並列出任何現有的存取金鑰。

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

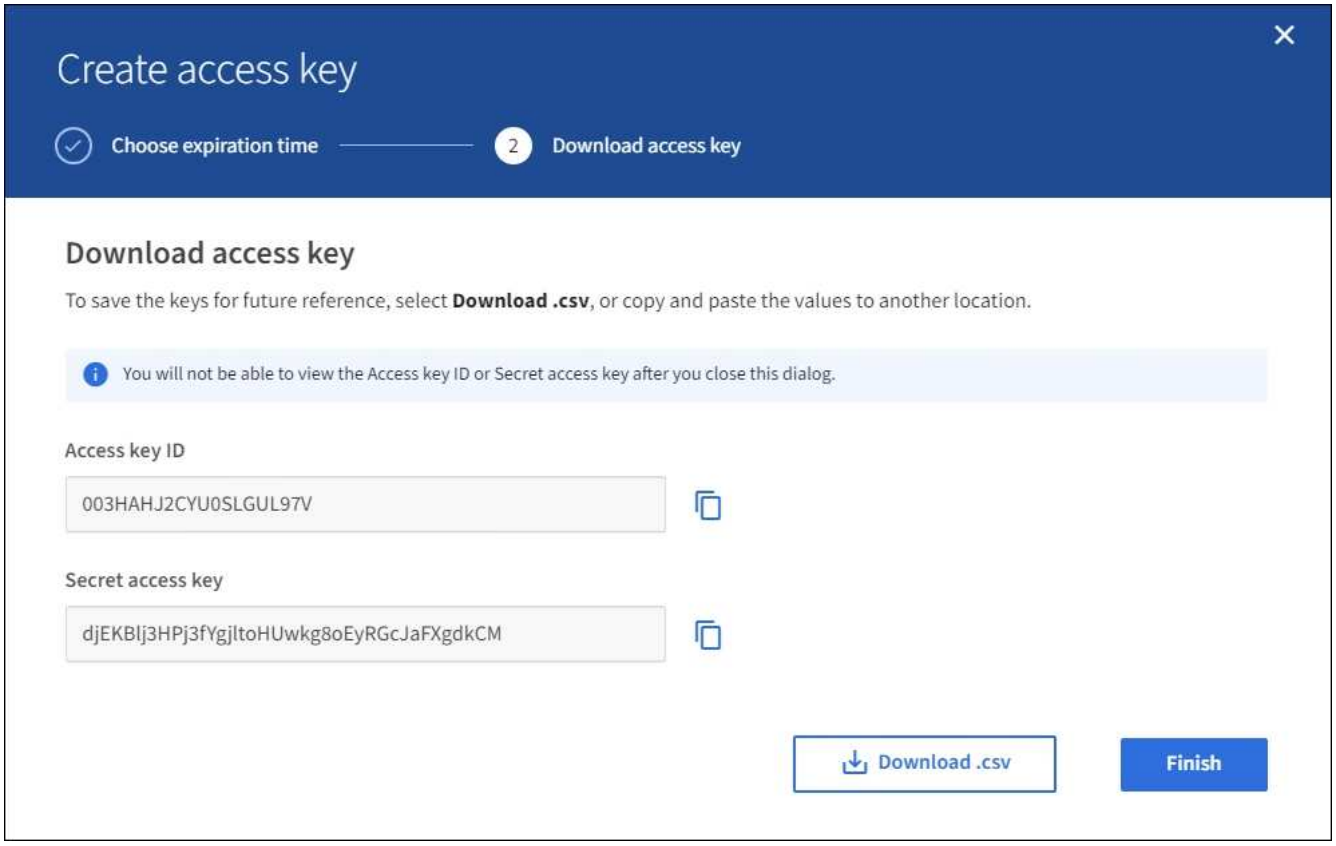


4. 選取*建立存取金鑰*。

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

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

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



6. 選擇*完成*。

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

檢視您的**S3**存取金鑰

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

您需要的產品

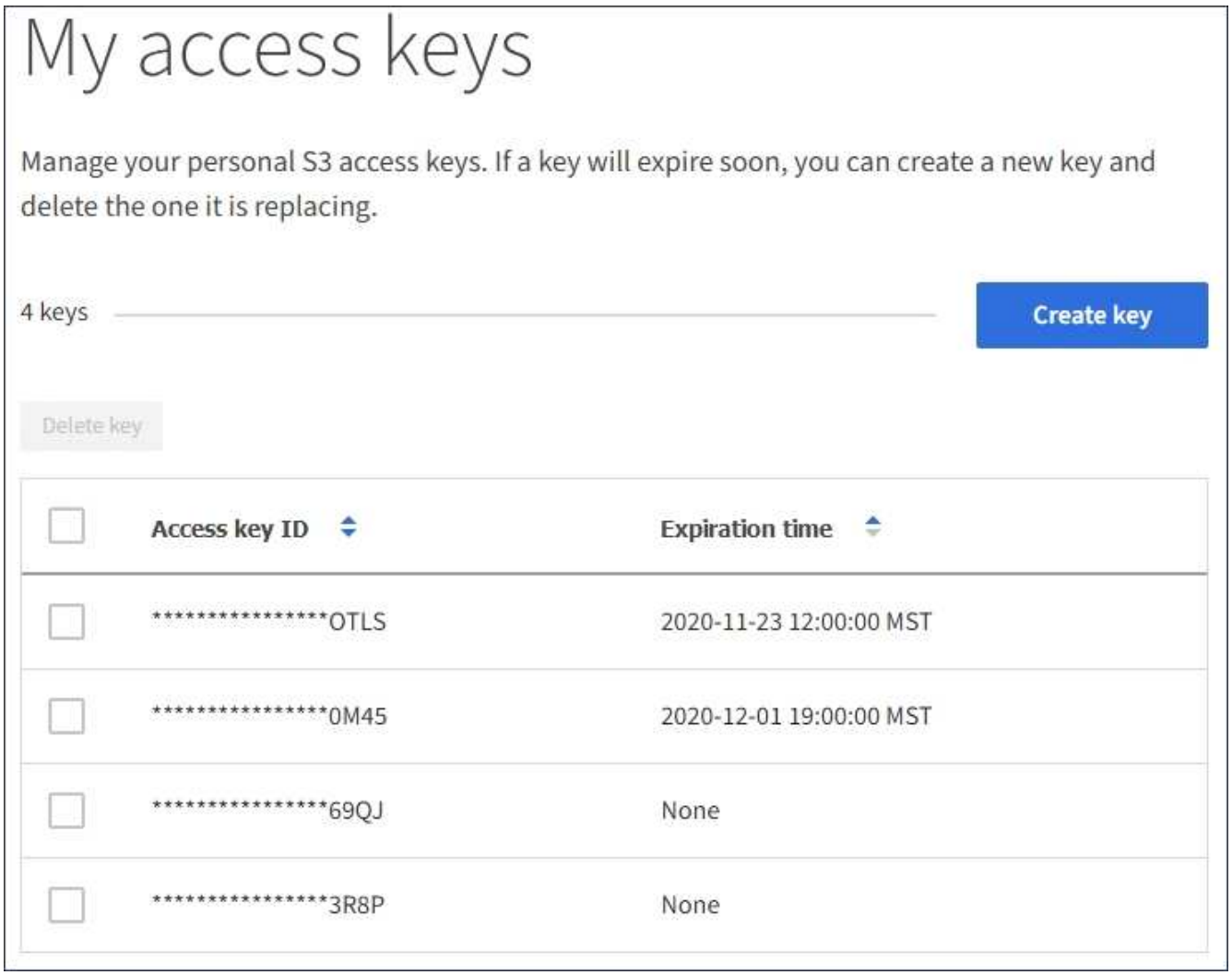
- 您必須使用登入租戶管理程式 支援的網頁瀏覽器。
- 您必須擁有「管理自己的S3認證」權限。

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

步驟

1. 選擇*儲存設備（S3）>*我的存取金鑰。

   「我的存取金鑰」頁面隨即出現、並列出任何現有的存取金鑰。



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

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

   過期的金鑰會自動移除。

相關資訊

建立自己的S3存取金鑰

刪除您自己的S3存取金鑰

刪除您自己的**S3**存取金鑰

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

您需要的產品

- 您必須使用登入租戶管理程式 支援的網頁瀏覽器。

- 您必須擁有「管理自己的S3認證」權限。請參閱 租戶管理權限。

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

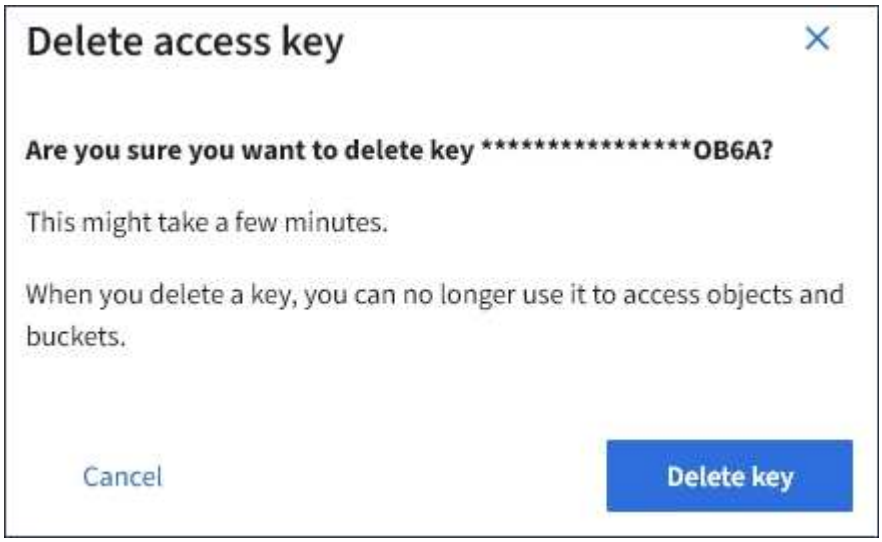
步驟

1. 選擇*儲存設備（S3）>*我的存取金鑰。

   「我的存取金鑰」頁面隨即出現、並列出任何現有的存取金鑰。

2. 選取您要移除之每個存取金鑰的核取方塊。
3. 選取*刪除機碼*。

   隨即顯示確認對話方塊。



4. 選取*刪除機碼*。

   頁面右上角會出現確認訊息。由於快取、變更可能需要15分鐘才能生效。

建立其他使用者的**S3**存取金鑰

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

您需要的產品

- 您必須使用登入租戶管理程式 支援的網頁瀏覽器。
- 您必須具有「根存取」權限。

關於這項工作

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

每個金鑰都可以有特定的到期時間、或是沒有到期時間。請遵循下列到期時間準則：

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

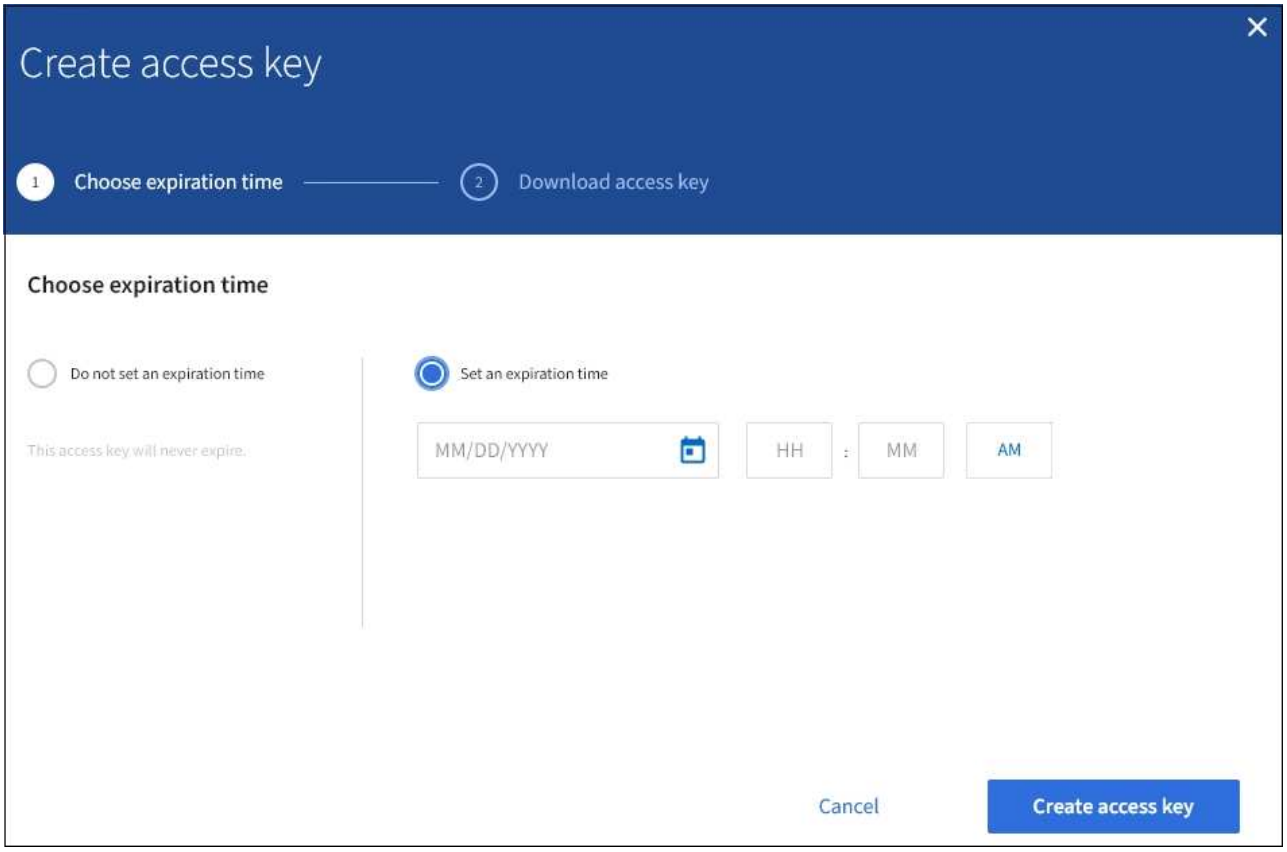
> 您可以使用租戶管理程式中顯示的該使用者存取金鑰ID和秘密存取金鑰、來存取屬於該使用者的S3儲存區和物件。因此、請像保護密碼一樣保護存取金鑰。定期旋轉存取金鑰、從帳戶中移除任何未使用的金鑰、而且切勿與其他使用者共用。

步驟

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

   使用者詳細資料頁面隨即出現。

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

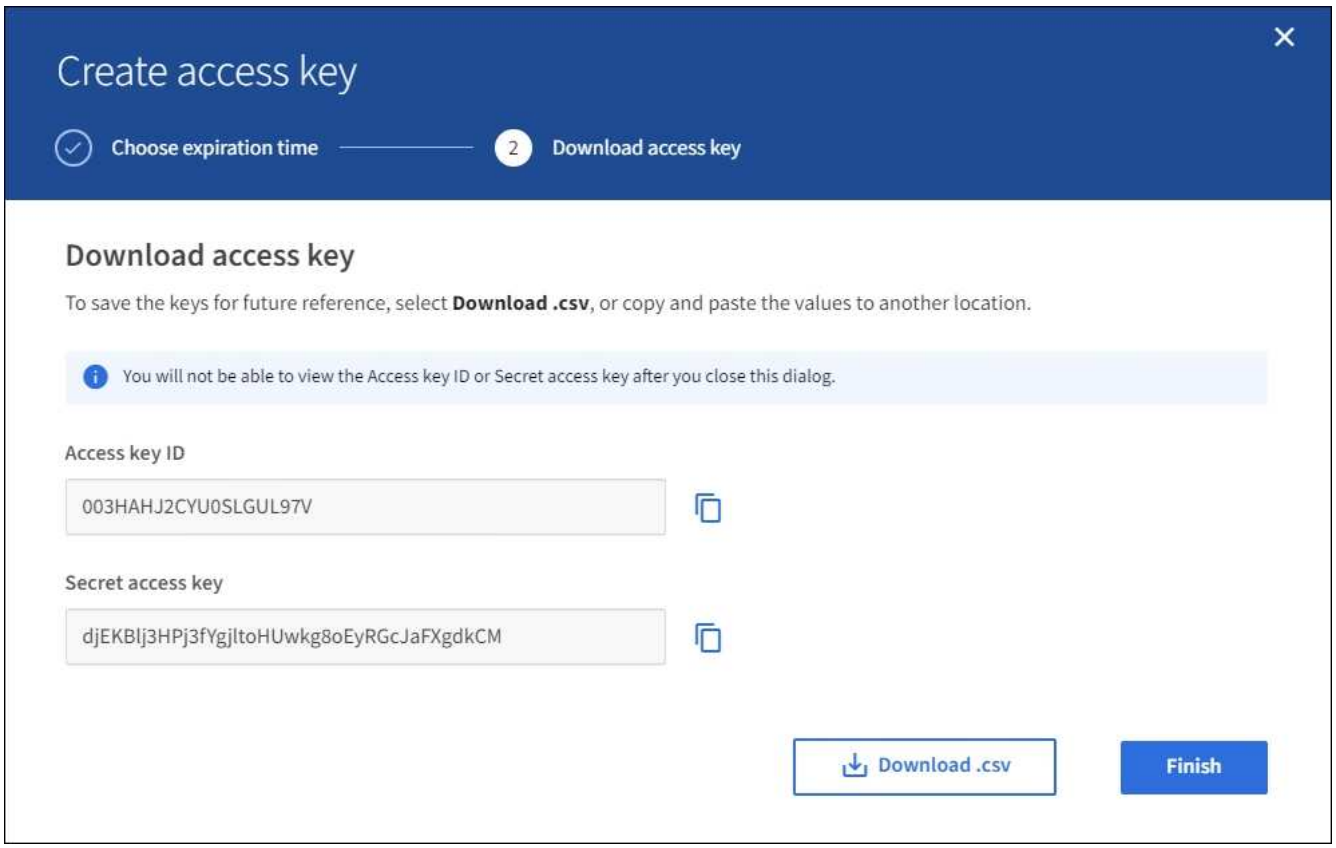


5. 選取*建立存取金鑰*。

   此時會出現「下載存取金鑰」對話方塊、列出存取金鑰ID和秘密存取金鑰。

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

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



7. 選擇*完成*。

   新金鑰會列在使用者詳細資料頁面的「存取金鑰」索引標籤上。由於快取、變更可能需要15分鐘才能生效。

相關資訊

租戶管理權限

檢視其他使用者的**S3**存取金鑰

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

您需要的產品

- 您必須使用登入租戶管理程式 支援的網頁瀏覽器。
- 您必須具有「根存取」權限。

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

步驟

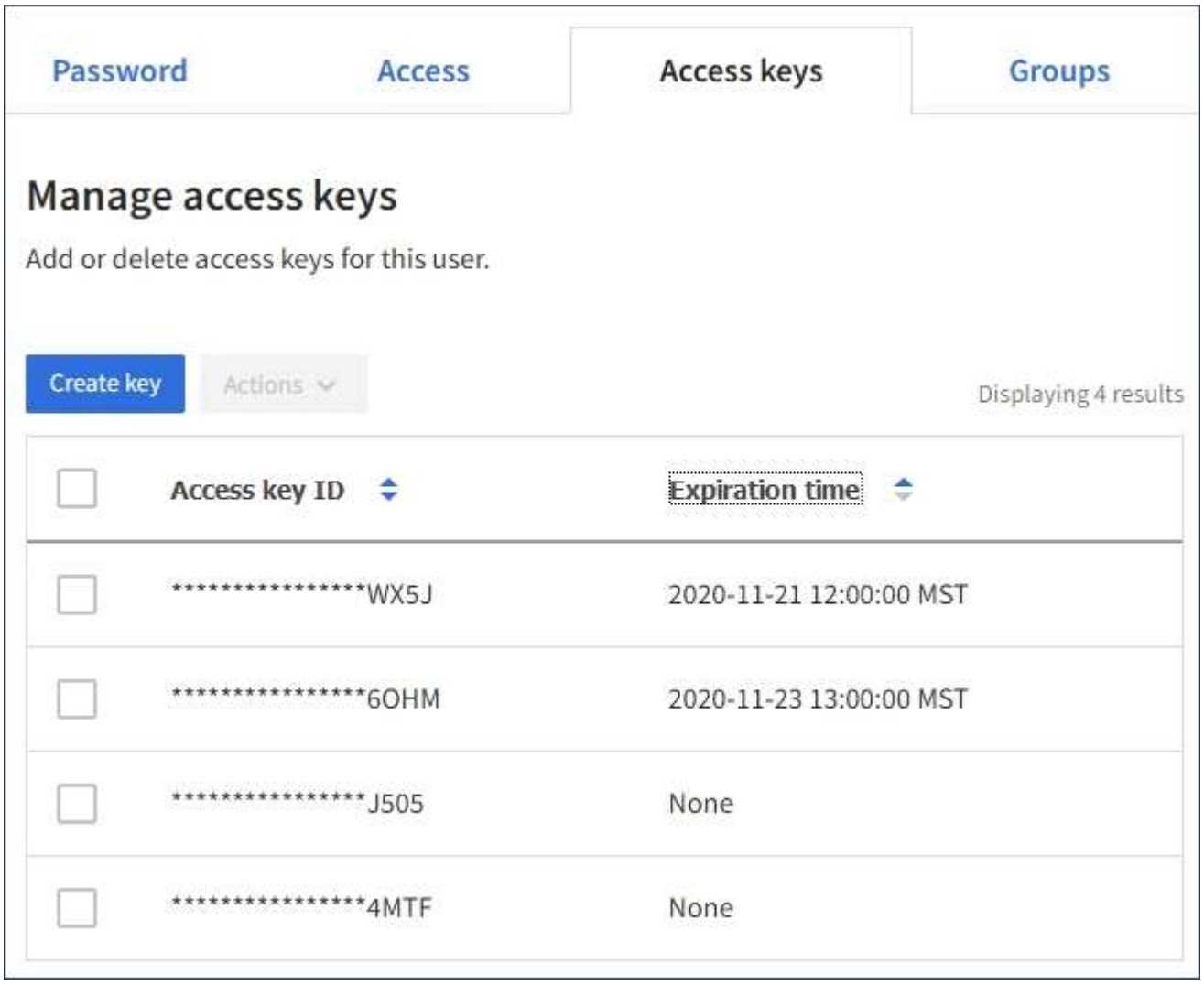
1. 選擇*存取管理*>*使用者*。

   此時會出現「使用者」頁面、並列出現有的使用者。

2. 選取您要檢視其S3存取金鑰的使用者。

   隨即顯示「使用者詳細資料」頁面。

3. 選擇*存取金鑰*。



4. 按*過期時間*或*存取金鑰ID*來排序金鑰。
5. 視需要建立新金鑰、並手動刪除不再使用的金鑰。

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

過期的金鑰會自動移除。

相關資訊

建立另一個使用者的S3存取金鑰

刪除其他使用者的S3存取金鑰

刪除其他使用者的**S3**存取金鑰

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

您需要的產品

- 您必須使用登入租戶管理程式 支援的網頁瀏覽器。
- 您必須具有「根存取」權限。請參閱 租戶管理權限。

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

步驟

1. 選擇*存取管理*>*使用者*。

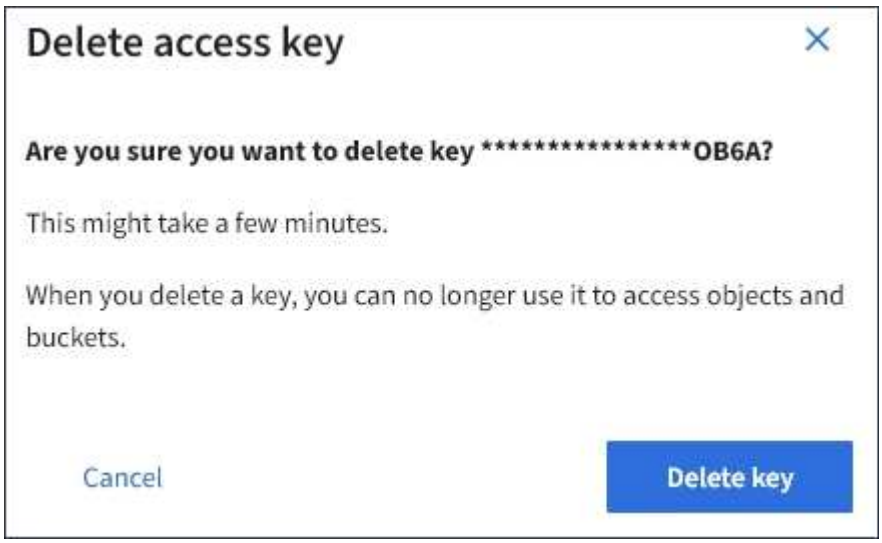
   此時會出現「使用者」頁面、並列出現有的使用者。

2. 選取您要管理其S3存取金鑰的使用者。

   隨即顯示「使用者詳細資料」頁面。

3. 選取*存取金鑰*、然後選取您要刪除的每個存取金鑰核取方塊。
4. 選取*「動作*」>*「刪除選取的金鑰*」。

   隨即顯示確認對話方塊。



5. 選取*刪除機碼*。

   頁面右上角會出現確認訊息。由於快取、變更可能需要15分鐘才能生效。

管理S3儲存區

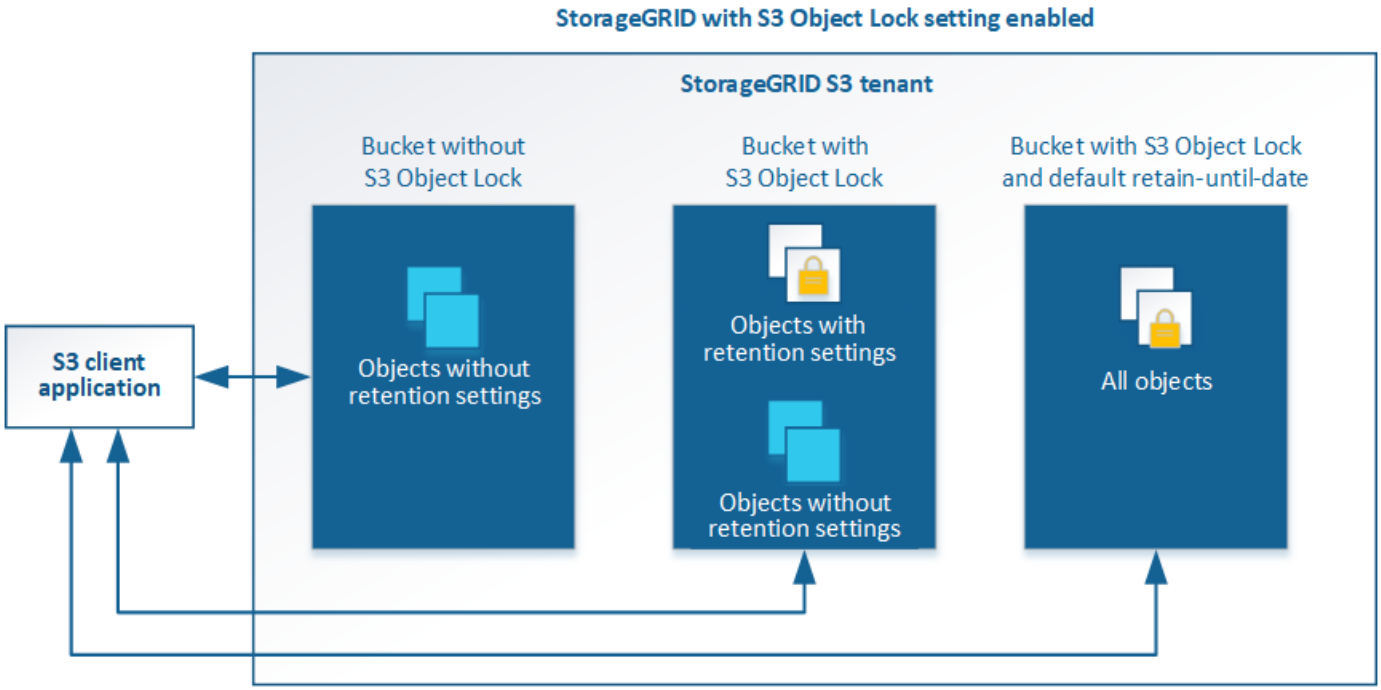
使用S3物件鎖定搭配租戶使用

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

什麼是S3物件鎖定？

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

如圖所示、當啟用StorageGRID 全域S3物件鎖定設定以供支援某個功能時、S3租戶帳戶可以建立啟用或不啟用S3物件鎖定的儲存區。如果某個儲存區已啟用S3物件鎖定、則S3用戶端應用程式可選擇性地指定該儲存區中任何物件版本的保留設定。物件版本必須具有指定的保留設定、才能受到S3物件鎖定的保護。



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

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

- 保留截止日期：如果物件版本的保留截止日期在未來、則可擷取物件、但無法修改或刪除。視需要可增加物件的保留截止日期、但此日期不可減少。
- 合法持有：將合法持有套用至物件版本、會立即鎖定該物件。例如、您可能需要對與調查或法律爭議相關的物件保留法律。合法持有沒有到期日、但在明確移除之前、仍會保留到位。合法持有不受保留至日期的限制。

您也可以 指定儲存貯體的預設保留模式和預設保留期間。這些物件會套用至新增至儲存區的每個物件、而這些物件並未指定其本身的保留設定。

如需這些設定的詳細資訊、請參閱 使用S3物件鎖定。

管理符合舊規範的儲存庫

S3物件鎖定功能取代先前StorageGRID 版本的Compliance功能。如果您使用StorageGRID 舊版的《不規則》建立了相容的儲存桶、您可以繼續管理這些儲存桶的設定、但是您無法再建立新的相容儲存桶。如需相關指示、請參閱NetApp知識庫文章。

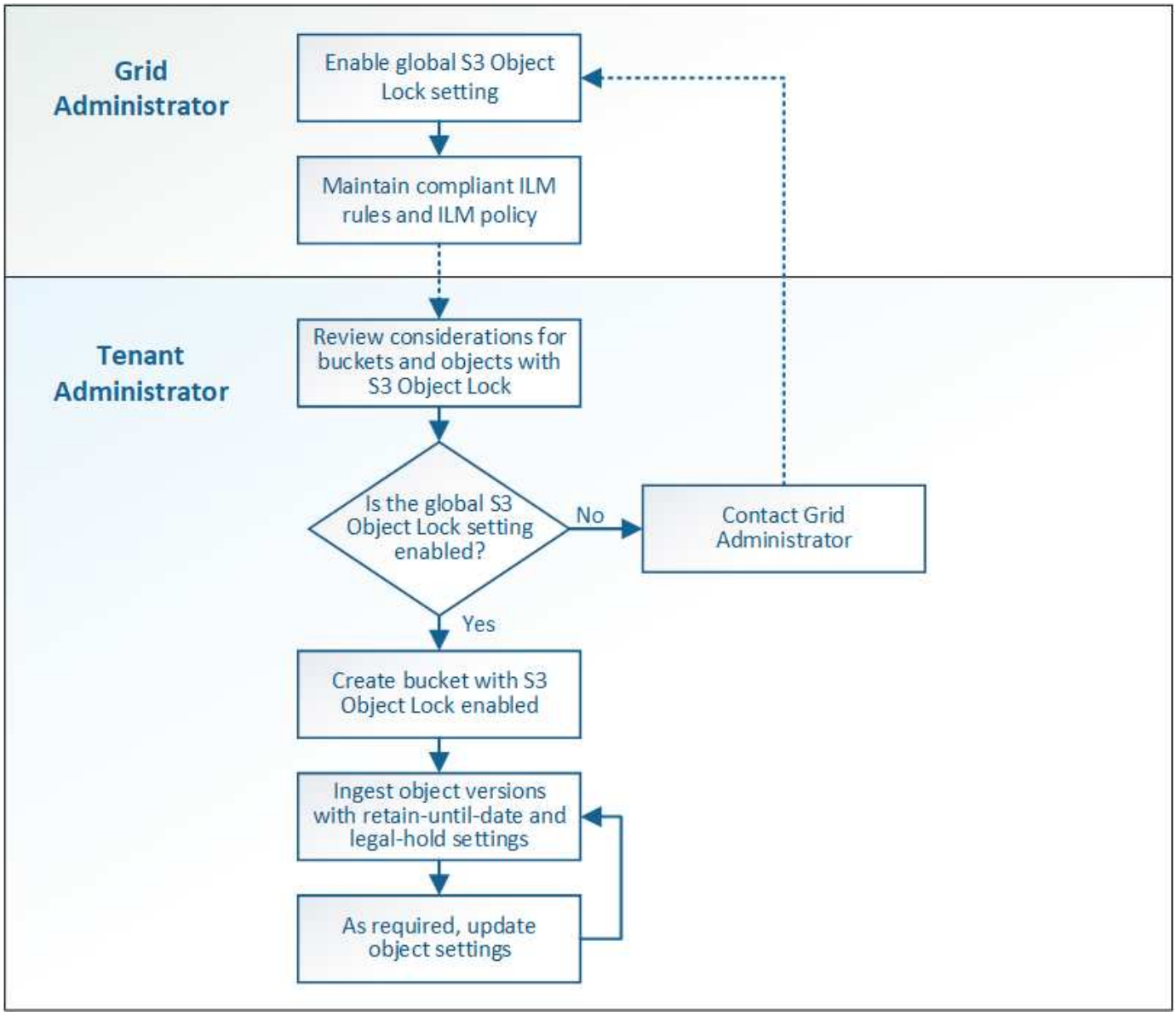
"NetApp知識庫：如何管理StorageGRID 支援老舊的知識庫、請參閱《知識庫文章"

S3物件鎖定工作流程

工作流程圖顯示StorageGRID 使用S3物件鎖定功能的高階步驟。

在啟用S3物件鎖定功能的情況下建立儲存區之前、網格管理員必須先為整個StorageGRID 支援整個系統啟用全域S3物件鎖定設定。網格管理員也必須確保 資訊生命週期管理（ILM）原則 符合「合規」；必須符合啟用S3物件鎖定的貯體需求。如需詳細資料、請聯絡網格管理員、或參閱資訊生命週期管理的物件管理說明。

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



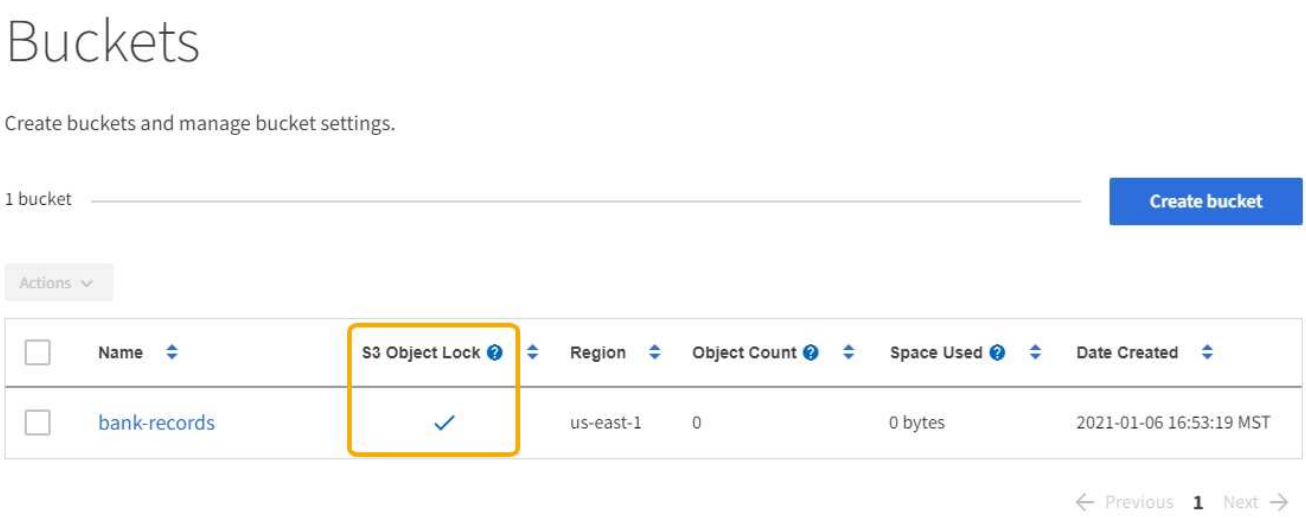
S3物件鎖定需求

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

啟用**S3**物件鎖定的儲存區需求

- 如果StorageGRID 已針對整個S3物件鎖定設定啟用for the S廳 系統、您可以使用租戶管理程式、租戶管理API或S3 REST API來建立啟用S3物件鎖定的儲存區。

  此租戶管理程式範例顯示已啟用S3物件鎖定的儲存區。



- 如果您打算使用S3物件鎖定、則必須在建立儲存區時啟用S3物件鎖定。您無法為現有的儲存區啟用S3物件鎖定。
- S3物件鎖定需要庫位版本管理。當「S3物件鎖定」已啟用時、StorageGRID 即可自動啟用該儲存區的版本管理功能。
- 在建立啟用S3物件鎖定的儲存區之後、您無法停用該儲存區的S3物件鎖定或暫停版本管理。
- 您也可以設定儲存區的預設保留。上傳物件版本時、預設保留會套用至物件版本。您可以指定保留模式來覆寫儲存區預設值、並在上傳物件版本的要求中保留截止日期。
- S3物件生命週期儲存區支援儲存區生命週期組態。
- 啟用S3物件鎖定的儲存區不支援CloudMirror複寫。

啟用**S3**物件鎖定之儲存區中的物件需求

- 為了保護物件版本、S3用戶端應用程式必須設定儲存區預設保留、或在每個上傳要求中指定保留設定。
- 您可以增加物件版本的保留截止日期、但絕不能減少此值。
- 如果您收到尚待處理的法律行動或法規調查通知、您可以在物件版本上保留合法資訊、以保留相關資訊。當物件版本處於合法持有狀態時、即使StorageGRID 物件已達到保留日期、也無法從該物件刪除。一旦取消合法持有、如果已達到保留截止日期、就可以刪除物件版本。
- S3物件鎖定需要使用版本控制的儲存區。保留設定適用於個別物件版本。物件版本可以同時具有「保留直到日期」和「合法保留」設定、但不能有另一個設定、或兩者都沒有。指定物件的保留截止日期或合法保留設定、只會保護要求中指定的版本。您可以建立物件的新版本、而舊版物件仍會保持鎖定狀態。

啟用**S3**物件鎖定的儲存區物件生命週期

儲存在已啟用S3物件鎖定的儲存區中的每個物件都會經過三個階段：

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

料複本。

2. 物件保留
   - 物件的多個複本是StorageGRID 由NetApp儲存的。複本的確切數量和類型、以及儲存位置、取決於使用中ILM原則中的相容規則。
3. 物件刪除
   - 物件到達保留截止日期時、即可刪除。
   - 無法刪除合法持有的物件。

建立**S3**儲存區

您可以使用租戶管理程式來建立S3儲存區以供物件資料使用。當您建立桶時、必須指定桶的名稱和區域。如果StorageGRID 已針對整個S3物件鎖定設定啟用for the Sing系統、您可以選擇性地為儲存區啟用S3物件鎖定。

您需要的產品

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

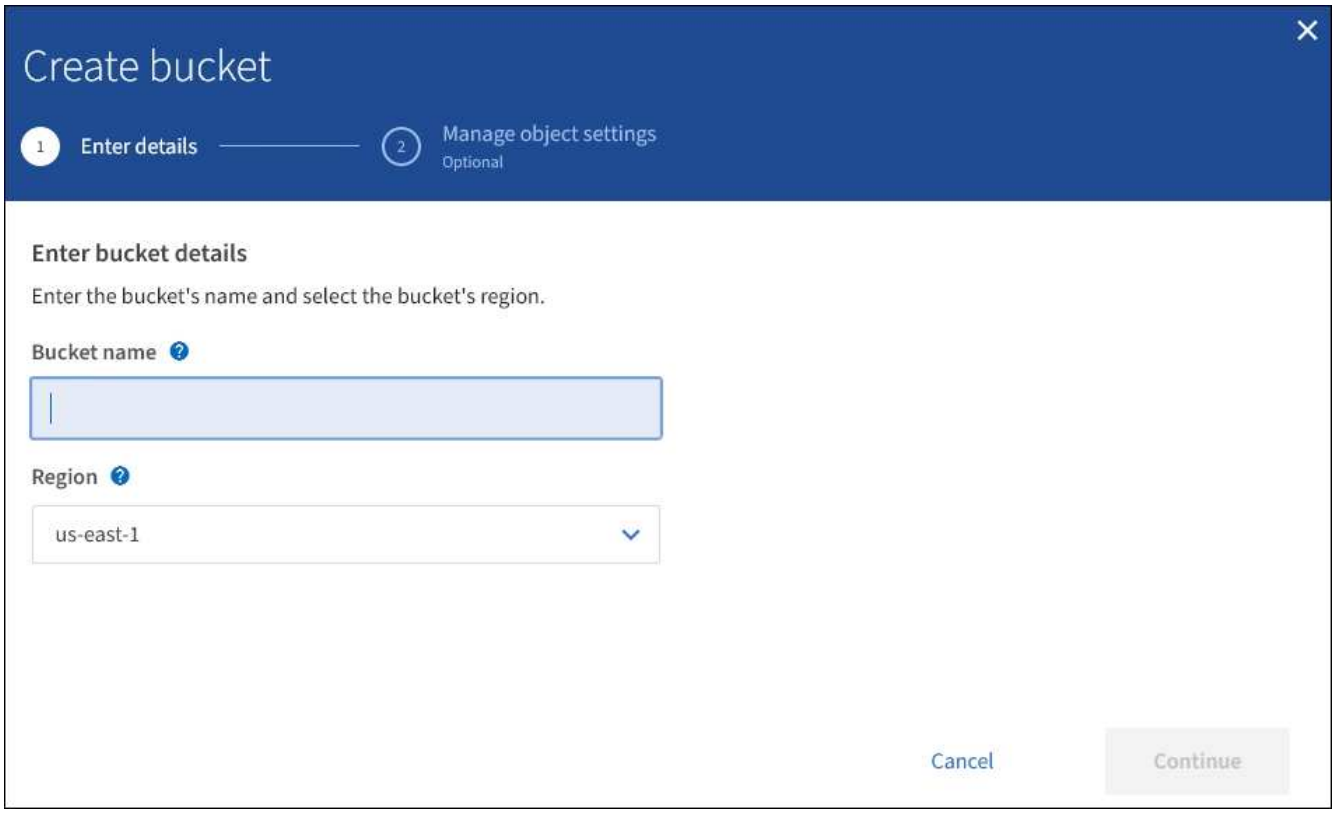
  可以授予設定或修改區段或物件之S3物件鎖定內容的權限 庫位原則或群組原則。

- 如果您計畫建立S3物件鎖定的儲存區、則表示您已啟用StorageGRID 適用於此系統的全域S3物件鎖定設定、並已檢閱S3物件鎖定儲存區和物件的需求。

  使用S3物件鎖定

步驟

1. 選擇*儲存設備（S3）>*桶。
2. 選取*建立桶*。



3. 輸入庫位的唯一名稱。

   建立貯體後、您無法變更貯體名稱。

   庫位名稱必須符合下列規則：

   - 必須在各個StorageGRID 方面都是獨一無二的（不只是租戶帳戶內的獨特功能）。
   - 必須符合DNS規範。
   - 必須包含至少3個字元、且不得超過63個字元。
   - 每個標籤都必須以英文字母或數字開頭和結尾、而且只能使用英文字母、數字和連字號。
   - 不應在虛擬託管樣式要求中使用期間。期間會導致伺服器萬用字元憑證驗證發生問題。

   如需詳細資訊、請參閱 "Amazon Web Services（AWS）儲存區命名規則文件"。

4. 選取此儲存區的區域。

   您的系統管理員負責管理可用的區域。StorageGRID儲存區的區域可能會影響套用至物件的資料保護原則。根據預設、所有的貯體都會建立在「us-east-1」區域。

   建立儲存貯體後、您無法變更區域。

5. 選擇*繼續*。
6. 或者、為儲存區啟用物件版本管理。

   如果您要儲存此儲存區中每個物件的每個版本、請啟用物件版本管理。然後您可以視需要擷取物件的舊版。

7. 如果出現「S3物件鎖定」區段、請選擇性啟用儲存區的S3物件鎖定。

   建立儲存區之後、您無法啟用或停用S3物件鎖定。

   「S3物件鎖定」區段只有在全域S3物件鎖定設定已啟用時才會出現。

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

   如果您為儲存區啟用S3物件鎖定、則會自動啟用儲存區版本設定。您也可以 指定儲存貯體的預設保留模式和預設保留期間 套用至未指定其保留設定之貯體所擷取的每個物件。

8. 選取*建立桶*。

   此庫位會建立並新增至「庫位」頁面上的表格。

相關資訊

使用ILM管理物件

瞭解租戶管理API

使用S3

檢視**S3**儲存貯體詳細資料

您可以在租戶帳戶中檢視庫存箱和庫位設定清單。

您需要的產品

- 您必須使用登入租戶管理程式 支援的網頁瀏覽器。

步驟

1. 選擇*儲存設備（S3）>*桶。

   此時會顯示「資源庫」頁面、並列出租戶帳戶的所有資源庫。

2. 檢閱每個儲存區的資訊。

   視需要、您可以依任何欄排序資訊、也可以在清單中前後翻頁。

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

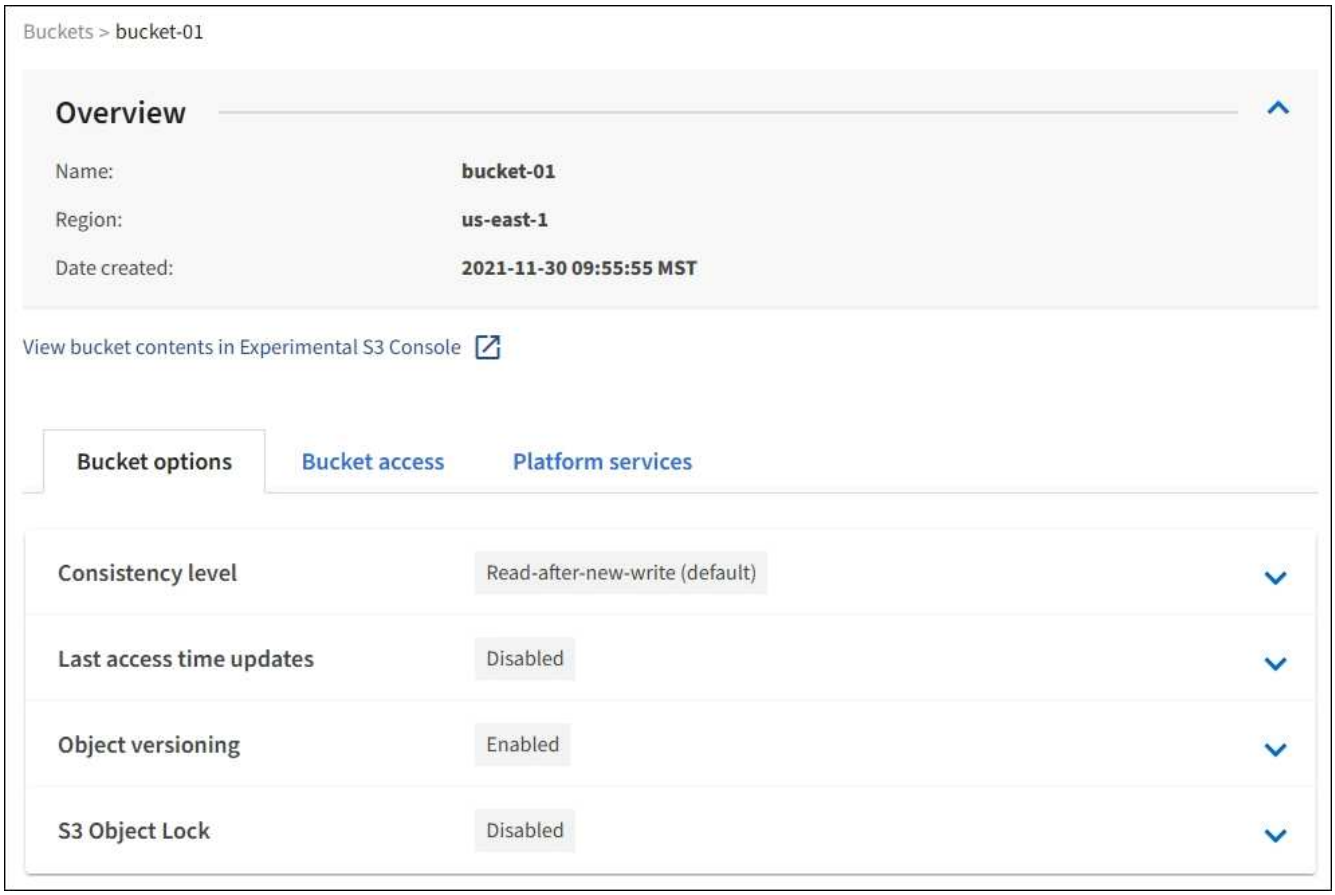
     如果停用全域S3物件鎖定設定、則不會顯示此欄。此欄也會顯示任何舊版相容桶的資訊。

   - 區域：無法變更的庫位區域。
   - 物件數：此儲存區中的物件數。
   - 已用空間：此儲存區中所有物件的邏輯大小。邏輯大小不包含複寫或銷毀編碼複本或物件中繼資料所需的實際空間。
   - 建立日期：建立桶的日期和時間。

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

3. 若要檢視及管理儲存區的設定、請選取儲存區名稱。

   「庫位詳細資料」頁面可讓您檢視及編輯庫位選項、庫位存取和的設定 平台服務。



變更一致性層級

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

您需要的產品

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

關於這項工作

一致性層級可在物件的可用度與這些物件在不同儲存節點和站台之間的一致性之間取得平衡。一般而言、您應該使用庫存箱的*新寫入後讀取*一致性層級。

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

當您變更桶的一致性層級時、只有變更後擷取的物件才保證符合修訂的層級。

步驟

1. 選擇*儲存設備（S3）>*桶。
2. 從清單中選取儲存貯體名稱。

此時會顯示「庫位詳細資料」頁面。

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

啟用或停用上次存取時間更新

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

這些指示僅適用於StorageGRID 包含至少一個ILM規則的Sesrast Access Times*選項、其放置指示中才會使用。如果您的支援系統不包含此類規則、您可以忽略這些指示StorageGRID 。

您需要的產品

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

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

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

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

請參閱使用資訊生命週期管理來管理物件的指示。

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

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

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

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

下表摘要說明上次存取時間停用或啟用時、套用至儲存區中所有物件的行為。

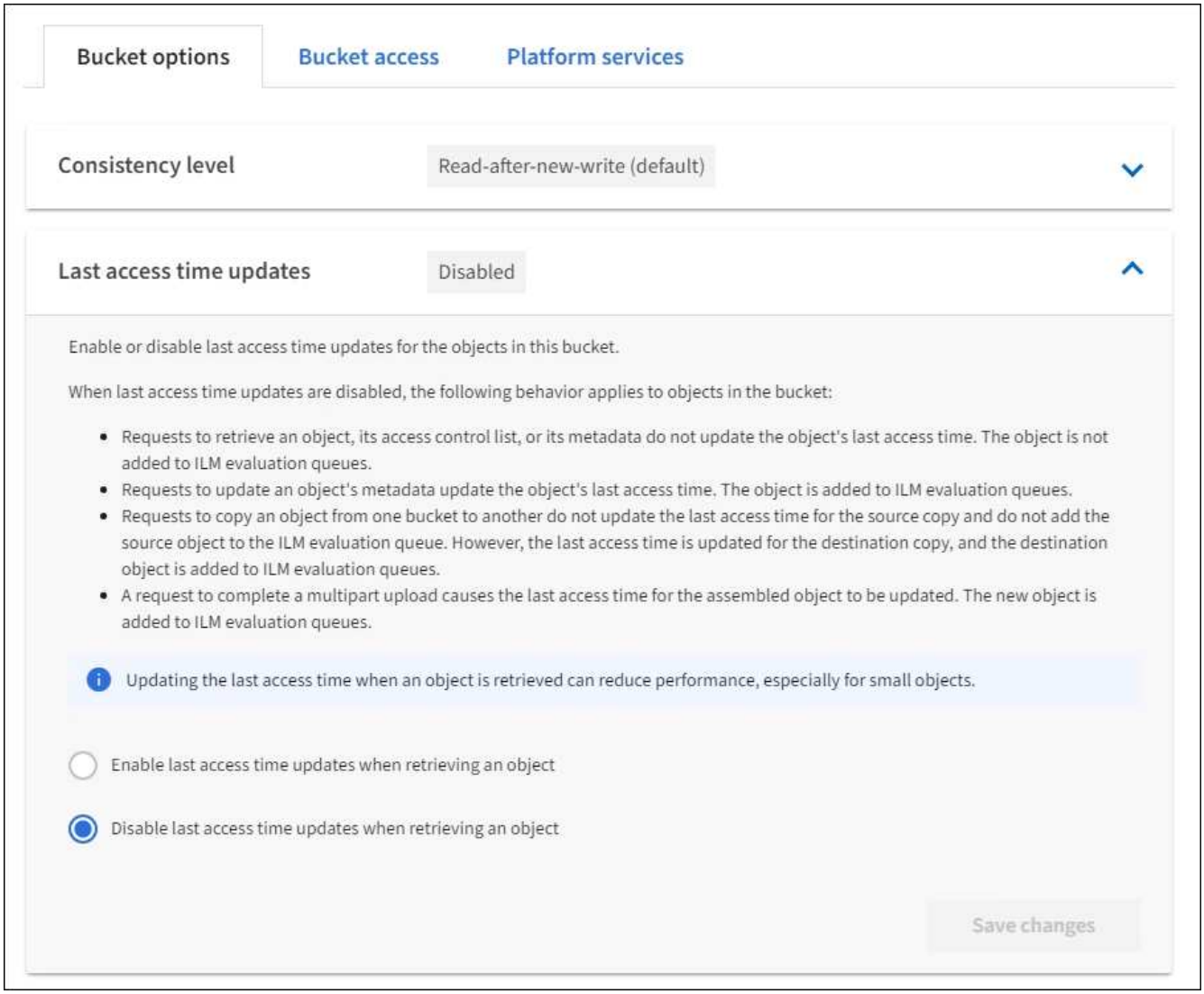
申請類型	停用上次存取時間時的行為（預設）		啟用上次存取時間時的行為	
	上次存取時間已更新？	新增至ILM評估佇列的物件？	上次存取時間已更新？	新增至ILM評估佇列的物件？
要求擷取物件、其存取控制清單或其中繼資料	否	否	是的	是的
要求更新物件的中繼資料	是的	是的	是的	是的
要求將物件從一個儲存區複製到另一個儲存區	• 否、來源複本 • 是、適用於目的地複本	• 否、來源複本 • 是、適用於目的地複本	• 是、來源複本 • 是、適用於目的地複本	• 是、來源複本 • 是、適用於目的地複本
要求完成多部分上傳	是的、適用於組裝好的物件	是的、適用於組裝好的物件	是的、適用於組裝好的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

步驟

1. 選擇*儲存設備（S3）>*桶。
2. 從清單中選取儲存貯體名稱。

   此時會顯示「庫位詳細資料」頁面。

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



5. 選取*儲存變更*。

相關資訊

租戶管理權限

使用ILM管理物件

變更儲存區的物件版本設定

如果您使用的是S3租戶、可以使用租戶管理程式或租戶管理API來變更S3桶的版本設定狀態。

您需要的產品

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

  租戶管理權限

關於這項工作

您可以啟用或暫停儲存區的物件版本管理。在啟用某個儲存區的版本管理之後、它將無法回到未版本化的狀態。不過、您可以暫停儲存區的版本管理。

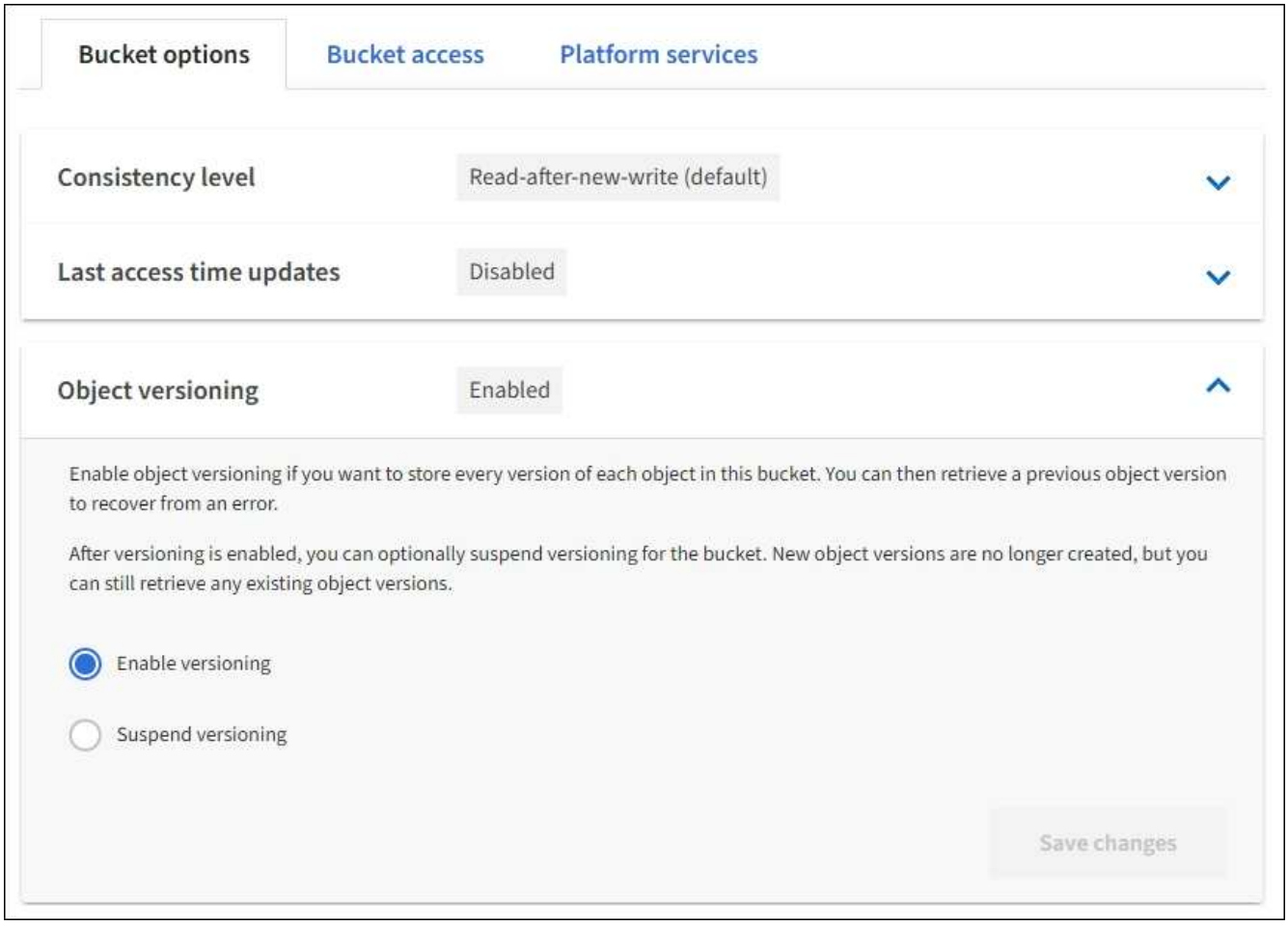
- 停用：從未啟用版本管理
- 已啟用：已啟用版本管理
- 已暫停：先前已啟用版本管理、並已暫停

S3物件版本管理

S3版本化物件的ILM規則和原則（範例4）

步驟

1. 選擇*儲存設備（S3）>*桶。
2. 從清單中選取儲存貯體名稱。
3. 選擇*儲存庫選項*>*物件版本管理*。



4. 選取此儲存區中物件的版本管理狀態。

如果啟用S3物件鎖定或舊版規範、則會停用*物件版本管理*選項。

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

5. 選取*儲存變更*。

設定跨來源資源共享（**CORS**）

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

您需要的產品

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

關於這項工作

跨來源資源共享（CORS）是一種安全機制、可讓一個網域中的用戶端Web應用程式存取不同網域中的資源。例如、假設您使用名為「imag像」的S3儲存區來儲存圖形。如果將CORS設定為「映像」儲存區、您就能在網站「http://www.example.com`」上顯示該儲存區中的影像。

步驟

1. 使用文字編輯器建立啟用CORS所需的XML。

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

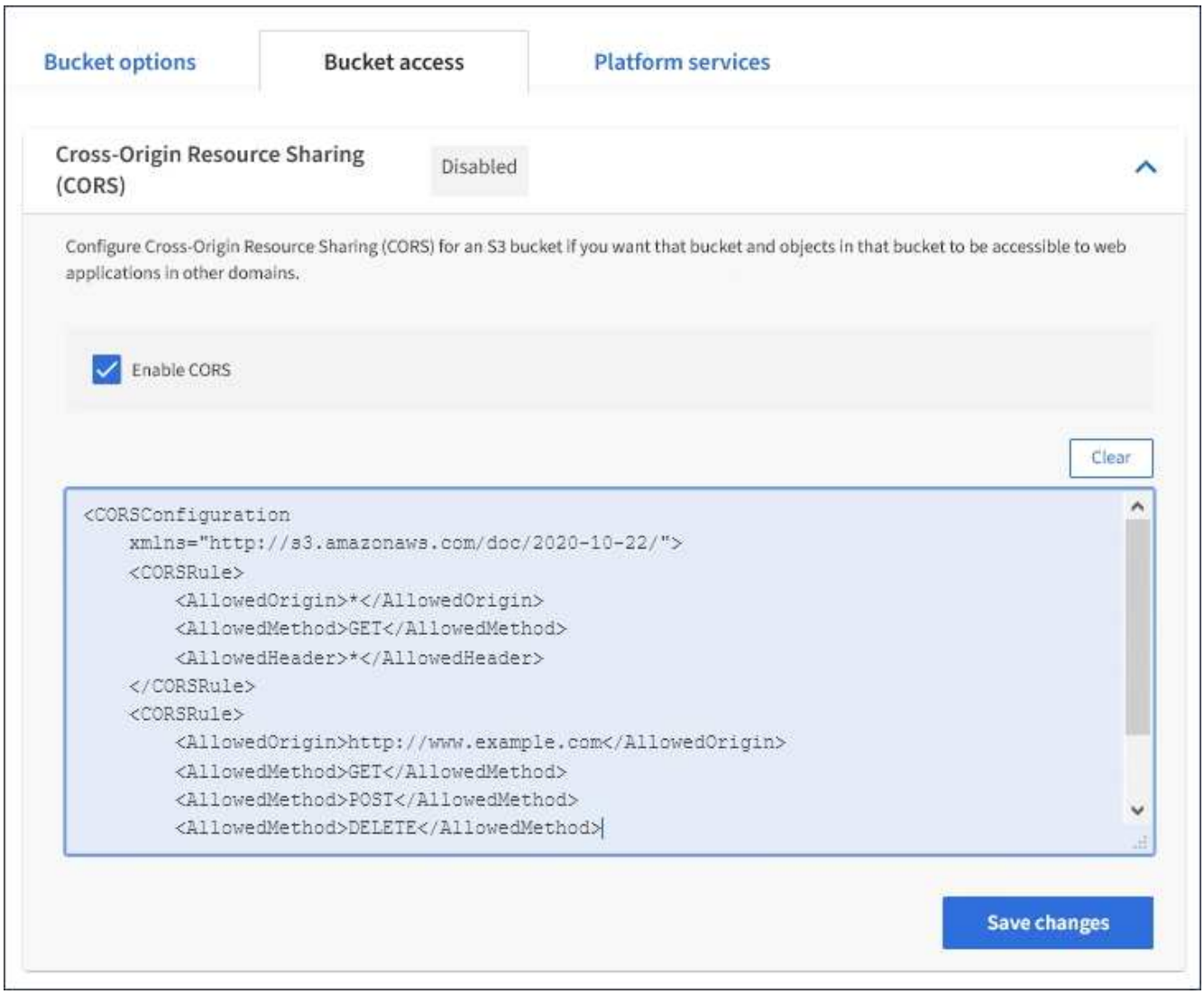
```
<CORSConfiguration
    xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
    <CORSRule>
        <AllowedOrigin>*</AllowedOrigin>
        <AllowedMethod>GET</AllowedMethod>
        <AllowedHeader>*</AllowedHeader>
    </CORSRule>
    <CORSRule>
        <AllowedOrigin>http://www.example.com</AllowedOrigin>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

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

2. 在租戶管理程式中、選取*儲存設備（S3）>*桶。
3. 從清單中選取儲存貯體名稱。

   此時會顯示「庫位詳細資料」頁面。

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



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

刪除**S3**儲存區

您可以使用租戶管理程式刪除一或多個空的S3儲存區。

您需要的產品

- 您必須使用登入租戶管理程式 支援的網頁瀏覽器。
- 您必須屬於具有「管理所有庫位」或「根存取」權限的使用者群組。這些權限會覆寫群組或儲存區原則中的權限設定。請參閱 租戶管理權限。
- 您要刪除的儲存區是空的。

關於這項工作

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

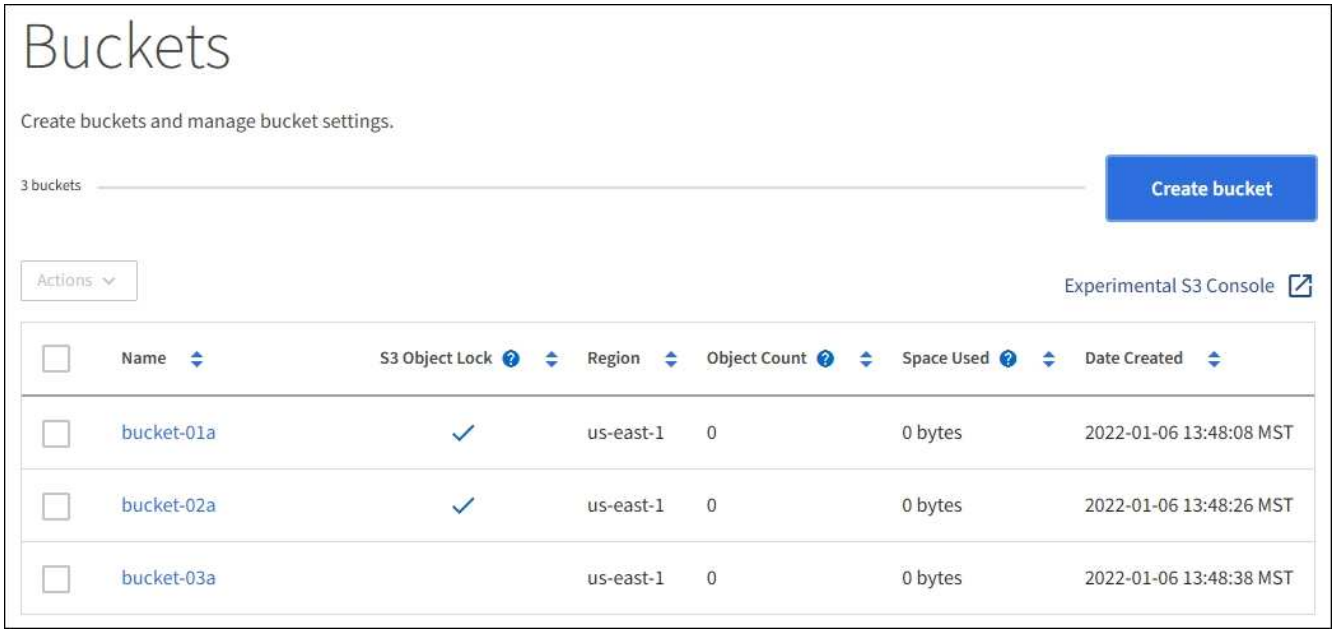
如果S3儲存區包含物件或非目前物件版本、則無法刪除。如需如何刪除S3版本控制物件的相關資訊、請參閱 使

用資訊生命週期管理來管理物件的指示。

步驟

1. 選擇*儲存設備（S3）>*桶。

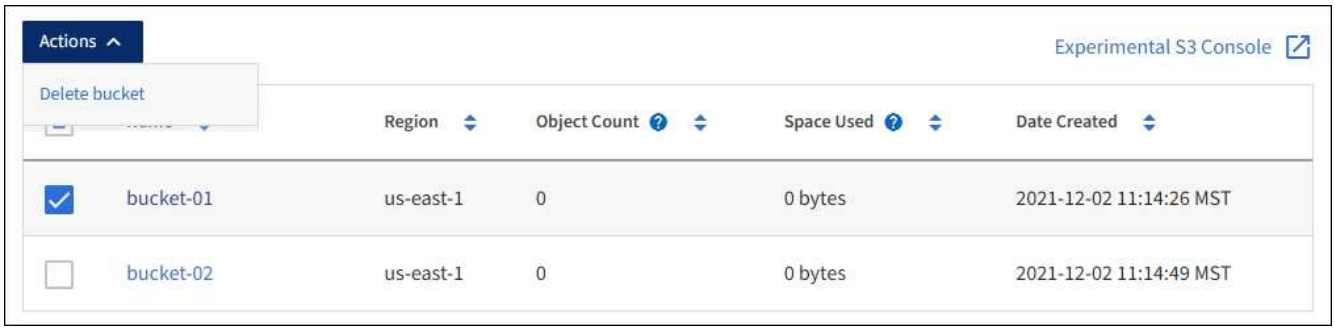
   此時會顯示「庫位」頁面、並顯示所有現有的S3庫位。



2. 選取您要刪除之空白儲存格的核取方塊。您一次可以選取多個儲存桶。

   「動作」功能表已啟用。

3. 從「Actions（動作）」功能表中、選取*「Delete Bucket*（刪除桶）」（如果您選擇多個桶、請選取*「Delete Bucket*（刪除桶）」）。



4. 當確認對話方塊出現時、請選取* Yes*刪除您選擇的所有儲存區。

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

   如果儲存區不是空的、就會出現錯誤訊息。您必須先刪除所有物件、才能刪除儲存區。

使用實驗性**S3**主控台

您可以使用S3主控台檢視S3儲存區中的物件。

您也可以使用S3主控台執行下列動作：

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

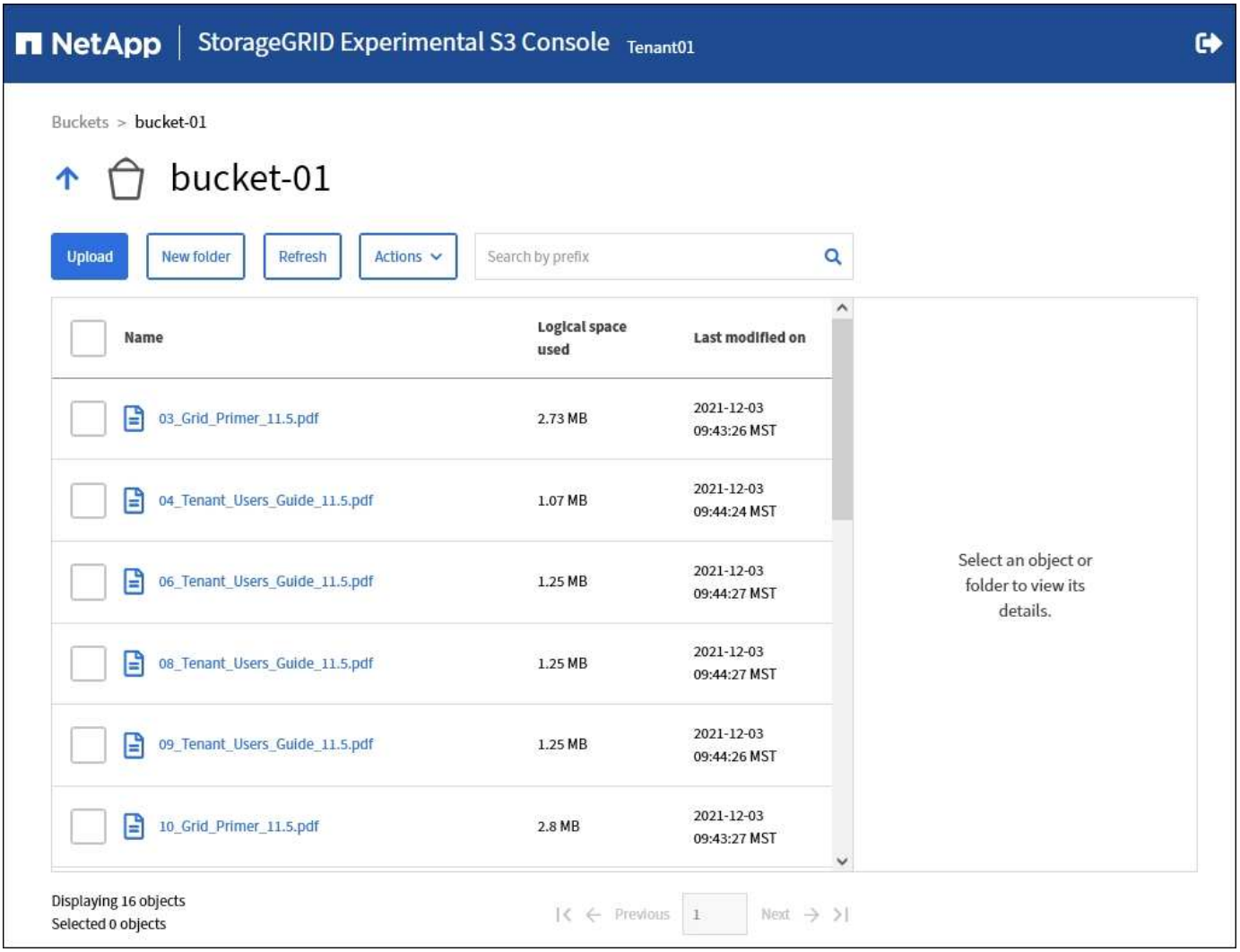
> S3主控台尚未經過完整測試、並標示為「實驗性」。 它不適用於物件的大量管理、也不適用於正式作業環境。租戶只能在執行少量物件的功能時使用S3主控台、例如上傳物件以模擬新的ILM原則、疑難排解擷取問題、或使用概念驗證或非正式作業網格時。

您需要的產品

- 您將使用登入租戶管理程式 支援的網頁瀏覽器。
- 您擁有「管理自己的S3認證」權限。
- 您已經建立了一個儲存庫。
- 您知道使用者的存取金鑰ID和秘密存取金鑰。您也可以選擇包含此資訊的「.csv"檔案。請參閱 建立存取金鑰的說明。

步驟

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



管理S3平台服務

什麼是平台服務？

支援各種平台服務、協助您實作混合雲策略。StorageGRID

如果您的租戶帳戶允許使用平台服務、您可以針對任何S3儲存區設定下列服務：

- * CloudMirror複寫* CloudMirror複寫服務StorageGRID 用於將特定物件從StorageGRID 靜止庫鏡射到指定的外部目的地。

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

  如果來源儲存區已啟用S3物件鎖定、則不支援CloudMirror複寫。

- 通知： 每桶活動通知 用於將物件執行特定動作的通知傳送至指定的外部Amazon Simple Notification Service™（SNS）。

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

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

- 搜尋整合服務 搜尋整合服務 用於將S3物件中繼資料傳送至指定的Elasticsearch索引、以便使用外部服務搜尋或分析中繼資料。

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

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

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

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

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

平台服務的設定方式

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

建立端點之後、您可以將XML組態新增至儲存區、為儲存區啟用平台服務。XML組態可識別儲存區應執行的物件、儲存區應採取的動作、以及儲存區應用於服務的端點。

您必須為每個要設定的平台服務新增個別的XML組態。例如：

1. 如果您想要將金鑰以「/images/映 像」開頭的所有物件複寫到Amazon S3儲存區、則必須將複寫組態新增至來源儲存區。
2. 如果您也想要在這些物件儲存至儲存區時傳送通知、則必須新增通知組態。
3. 最後、如果您要為這些物件的中繼資料建立索引、則必須新增用於實作搜尋整合的中繼資料通知組態。

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

平台服務	**S3 REST API**
CloudMirror複寫	• 取得庫位複寫 • 放入資源桶複寫
通知	• 取得庫存箱通知 • 放置時段通知

平台服務	**S3 REST API**
搜尋整合	• 取得Bucket中繼資料通知組態 • 放置時段中繼資料通知組態 這些作業是根據StorageGRID 需求量身打造的。

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

相關資訊

使用平台服務的考量

使用S3

CloudMirror複寫服務

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

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

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

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

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

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

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

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

用於標記複本的自訂標頭為「X-nTap sg-replica」。此標記可防止串聯鏡射。支援兩個網格之間的雙向CloudMirror。StorageGRID

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

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

瞭解庫存箱通知

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

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

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

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

支援的通知和訊息

下列限制會遵循Amazon S3 API的事件通知：StorageGRID

- 您無法設定下列事件類型的通知。這些事件類型*不支援*。
  - 'S 3：ReducedRedundancyLostObject'
  - 「s 3：ObjectRestore：completed」
- 從Suse傳送的事件通知StorageGRID 會使用標準Json格式、但不包含某些金鑰、並使用其他金鑰的特定值、如表所示：

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

瞭解搜尋整合服務

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

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

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

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

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

在下列情況下、系統會產生通知並排入傳送佇列：

- 隨即建立物件。
- 刪除物件、包括因網格ILM原則運作而刪除物件的時間。
- 物件中繼資料或標記會新增、更新或刪除。一律會在更新時傳送完整的中繼資料和標記集、而不只是變更的值。

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

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

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

相關資訊

搜尋整合的組態XML

中繼資料通知中包含的物件中繼資料

由搜尋整合服務產生的JSON

設定搜尋整合服務

使用平台服務的考量

在實作平台服務之前、請先檢閱使用這些服務的建議與考量事項。

如需S3的相關資訊、請參閱 使用S3。

使用平台服務的考量

考量	詳細資料
目的地端點監控	您必須監控每個目的地端點的可用度。如果連線到目的地端點的時間過長、而且有大量的要求待處理、那麼額外的用戶端要求StorageGRID （例如提出要求）將會失敗。當端點可連線時、您必須重試這些失敗的要求。

考量	詳細資料
目的地端點節流	如果傳送要求的速度超過目的地端點接收要求的速度、則支援使用此軟體來限制傳入S3的貯體要求。StorageGRID節流只會在有待傳送至目的地端點的要求待處理項目時發生。 唯一的可見效果是傳入S3要求執行時間較長。如果您開始偵測到效能大幅降低、應該降低擷取速度、或是使用容量較大的端點。如果要求的待處理項目持續增加、用戶端S3作業（例如PUT要求）最終將會失敗。 CloudMirror要求較容易受到目的地端點效能的影響、因為這些要求通常比搜尋整合或事件通知要求涉及更多資料傳輸。
訂購保證	可保證站台內物件的作業順序。StorageGRID只要物件的所有作業都在同一個站台內、最終的物件狀態（用於複寫）就會永遠等於StorageGRID 該站台的狀態。 在整個景點進行作業時、盡力訂購申請。StorageGRID StorageGRID例如、如果您一開始將物件寫入站台A、然後在站台B覆寫相同的物件、則CloudMirror複寫到目的地儲存區的最終物件將無法保證為較新的物件。
ILM導向物件刪除	為了符合AWS CRR和SNS服務的刪除行為、當來源儲存區中的物件因StorageGRID 採用《ILM規則》而遭刪除時、不會傳送CloudMirror和事件通知要求。例如、如果ILM規則在14天後刪除物件、則不會傳送CloudMirror或事件通知要求。 相反地、因為ILM而刪除物件時、會傳送搜尋整合要求。

使用**CloudMirror**複寫服務的考量

考量	詳細資料
複寫狀態	不支援「x-amz-replying狀態」標頭。StorageGRID
物件大小	CloudMirror複寫服務可複寫至目的地儲存區的物件大小上限為5 TiB、與最大_supported物件大小相同。 附註：單一放置物件作業的最大_Recommended大小為5 GiB（5、368、709、120位元組）。如果您的物件大於5 GiB、請改用多部份上傳。
儲存區版本管理和版本ID	如果StorageGRID 支援版本管理功能的來源S3儲存區、您也應該啟用目的地儲存區的版本管理功能。 使用版本管理時、請注意、由於S3傳輸協定的限制、CloudMirror服務無法保證目的地儲存庫中物件版本的順序順序。 附註：StorageGRID 來源程式庫的版本ID與目的地程式庫的版本ID無關。

考量	詳細資料
標記物件版本	由於S3傳輸協定的限制、CloudMirror服務不會複寫提供版本ID的任何「放置物件」標記或刪除物件標記要求。由於來源和目的地的版本ID無關、因此無法確保將標記更新複寫至特定版本ID。 相較之下、CloudMirror服務會複寫「放置物件標記」要求、或刪除未指定版本ID的物件標記要求。這些要求會更新最新金鑰的標記（如果儲存庫版本已有版本、則會更新最新版本）。也會複寫含有標記的一般擷取（非標記更新）。
多部份上傳和"ETag"值	鏡射使用多重上傳的物件時、CloudMirror服務不會保留這些部分。因此、鏡射物件的「ETag」值將與原始物件的「ETag」值不同。
使用SSE-C加密的物件（使用客戶提供的金鑰進行伺服器端加密）	CloudMirror服務不支援以SSE-C加密的物件如果您嘗試將物件擷取至來源儲存區以進行CloudMirror複寫、且要求中包含SSE-C要求標頭、則作業會失敗。
啟用S3物件鎖定的儲存區	如果用於CloudMirror複寫的目的地S3儲存區已啟用S3物件鎖定、則設定儲存區複寫（放置儲存區複寫）的嘗試將會失敗、並顯示AccessDenied錯誤。

設定平台服務端點

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

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

什麼是平台服務端點？

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

例如、如果您想要將物件從StorageGRID 某個物件庫複寫到AWS S3庫位、您可以建立一個平台服務端點、其中包含StorageGRID 資訊和認證。這個端點是用來存取AWS上的目的地庫位所需的資訊和認證資料。

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

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

用於**CloudMirror**複寫的端點

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

通知的端點

支援Simple Notification Service（SNS）端點。StorageGRID不支援簡單佇列服務（SQS）或AWS Lambda端點。

搜尋整合服務的端點

支援代表Elasticsearch叢集的搜尋整合端點。StorageGRID這些彈性搜尋叢集可位於本機資料中心、或託管於AWS雲端或其他地方。

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

相關資訊

管理StorageGRID

指定平台服務端點的**URN**

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

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

urnElements

平台服務端點的URN必須以「arn:AWS」或「urn:mysite」開頭、如下所示：

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

例如、如果您指定的是位於StorageGRID VMware上的CloudMirror端點的URN、則URN可能會以「urn:sgws」開頭。

URN的下一個元素會指定平台服務的類型、如下所示：

服務	類型
CloudMirror複寫	S3
通知	SnS
搜尋整合	ES

例如、若要繼續為StorageGRID 設於支援的CloudMirror端點指定URN、您可以新增「3」以取得「urn:sgws:S3」。

URN的最後一個元素會在目的地URI上識別特定的目標資源。

服務	特定資源
CloudMirror複寫	儲存庫名稱

服務	特定資源
通知	SnS-topic-name
搜尋整合	「網域名稱/索引名稱/類型名稱」 *注意：*如果Elasticsearch叢集*未*設定為自動建立索引、則必須在建立端點之前手動建立索引。

提供**AWS**和**GCP**上的服務

對於AWS和GCP實體而言、完整的URN是有效的AWS ARN。例如：

- CloudMirror複寫：

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

- 通知：

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

- 搜尋整合：

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

> 對於AWS搜尋整合端點、「domain-name」必須包含文字字串「domain/」、如下所示。

適用於本機代管服務

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

- CloudMirror複寫：

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

若為StorageGRID 以位址為基礎的CloudMirror端點、您可以指定以「urn:sgws」開頭的有效URN：

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

- 通知：

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

- 搜尋整合：

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

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

建立平台服務端點

您必須至少建立一個正確類型的端點、才能啟用平台服務。

您需要的產品

- 您必須使用登入租戶管理程式 支援的網頁瀏覽器。
- 平台服務必須由StorageGRID 管理員為您的租戶帳戶啟用。
- 您必須屬於具有「管理端點」權限的使用者群組。
- 平台服務端點所參照的資源必須已建立：
  - CloudMirror複寫：S3儲存區
  - 事件通知：SnS主題
  - 搜尋通知：彈性搜尋索引、如果目的地叢集未設定為自動建立索引。
- 您必須擁有目的地資源的相關資訊：
  - 統一資源識別元（URI）的主機和連接埠

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

  - 獨特資源名稱（URN）

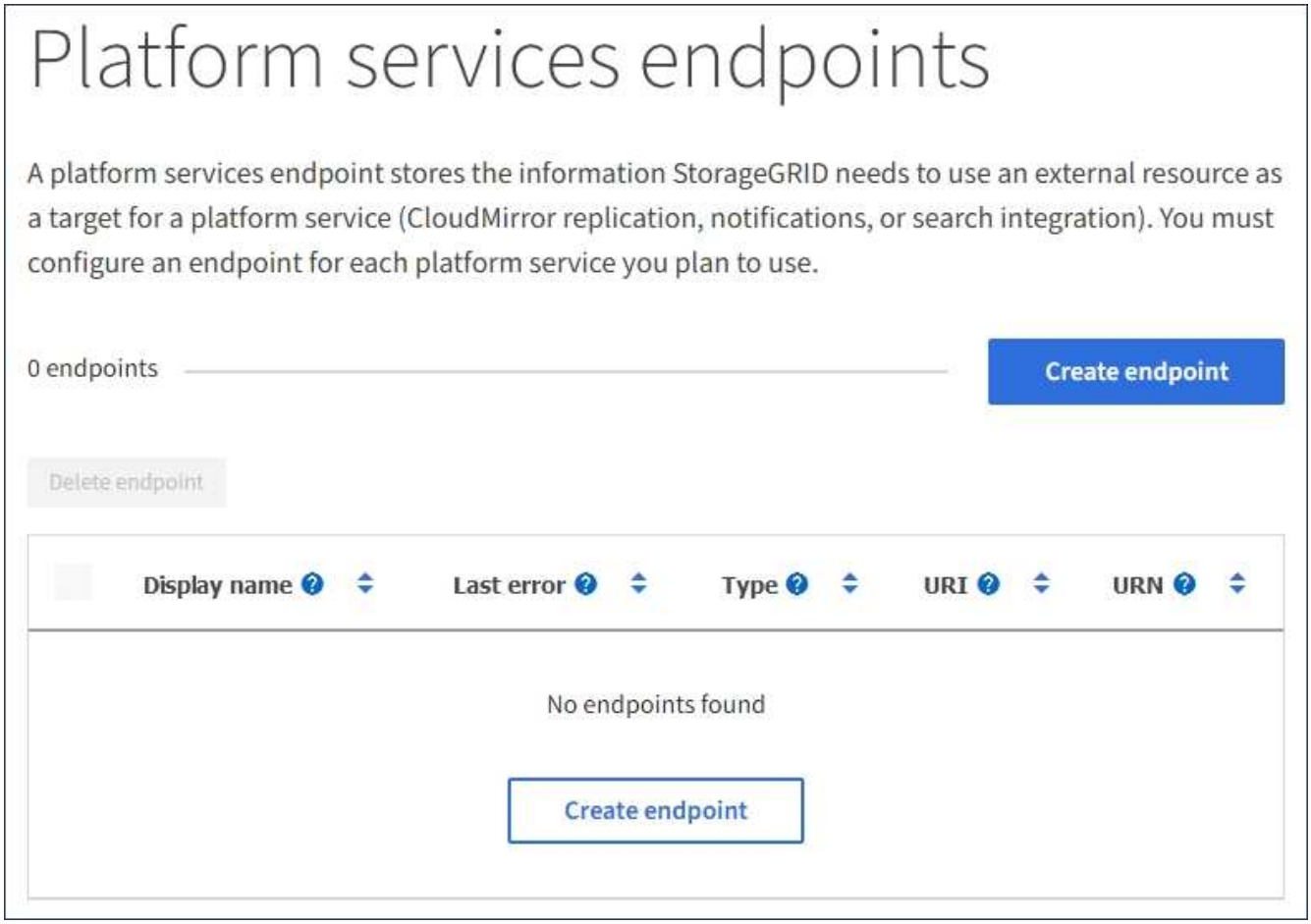
    指定平台服務端點的URN

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

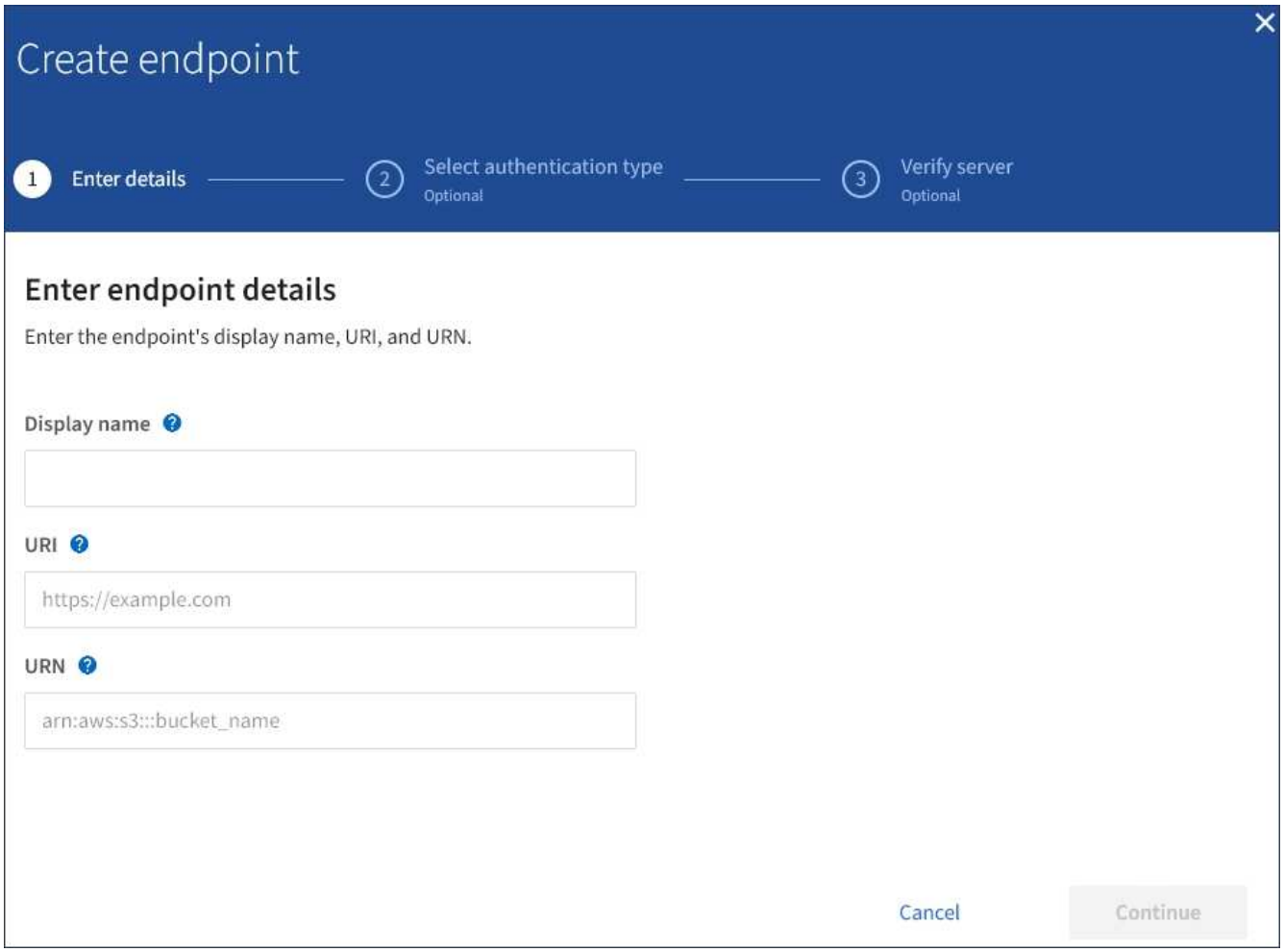
步驟

1. 選擇*儲存設備（S3）>*平台服務端點。

「平台服務端點」頁面隨即出現。



2. 選取*建立端點*。



3. 輸入顯示名稱、簡短說明端點及其用途。

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

4. 在「* URI *」欄位中、指定端點的唯一資源識別元（URI）。

   請使用下列其中一種格式：

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

   如果您未指定連接埠、則連接埠443用於HTTPS URI、連接埠80用於HTTP URI。

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

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

   在此範例中、「3.example.com」代表StorageGRID 適用於「支援高可用度（HA）」群組之虛擬IP（VIP）的DNS項目、而「10443」代表負載平衡器端點中定義的連接埠。

您應該盡可能連線到 HA 群組的負載平衡節點、以避免單點故障。

同樣地、AWS上裝載的儲存區URI可能是：

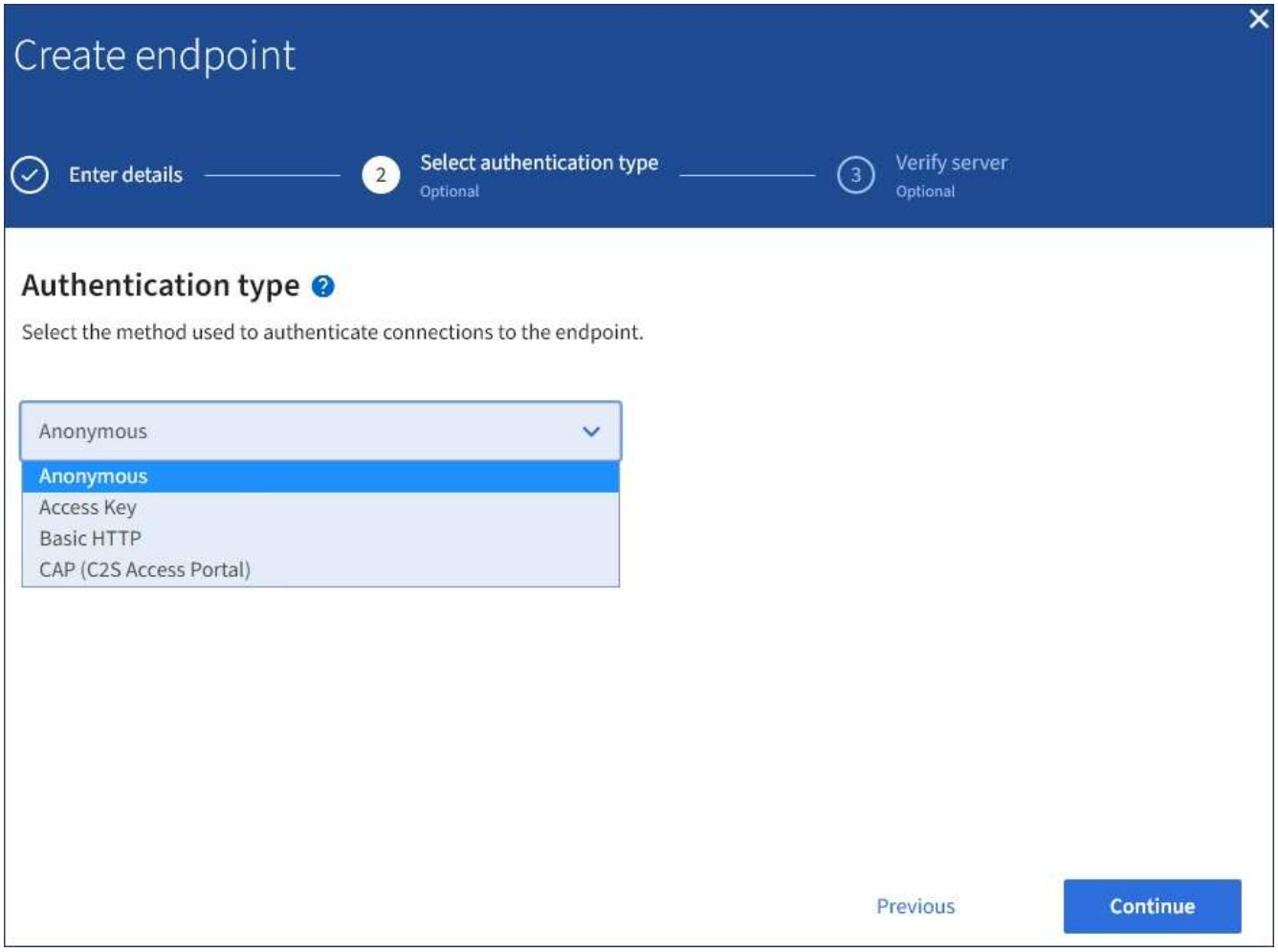
```
https://s3-aws-region.amazonaws.com
```

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

5. 輸入端點的唯一資源名稱（URN）。

建立端點之後、您無法變更端點的URN。

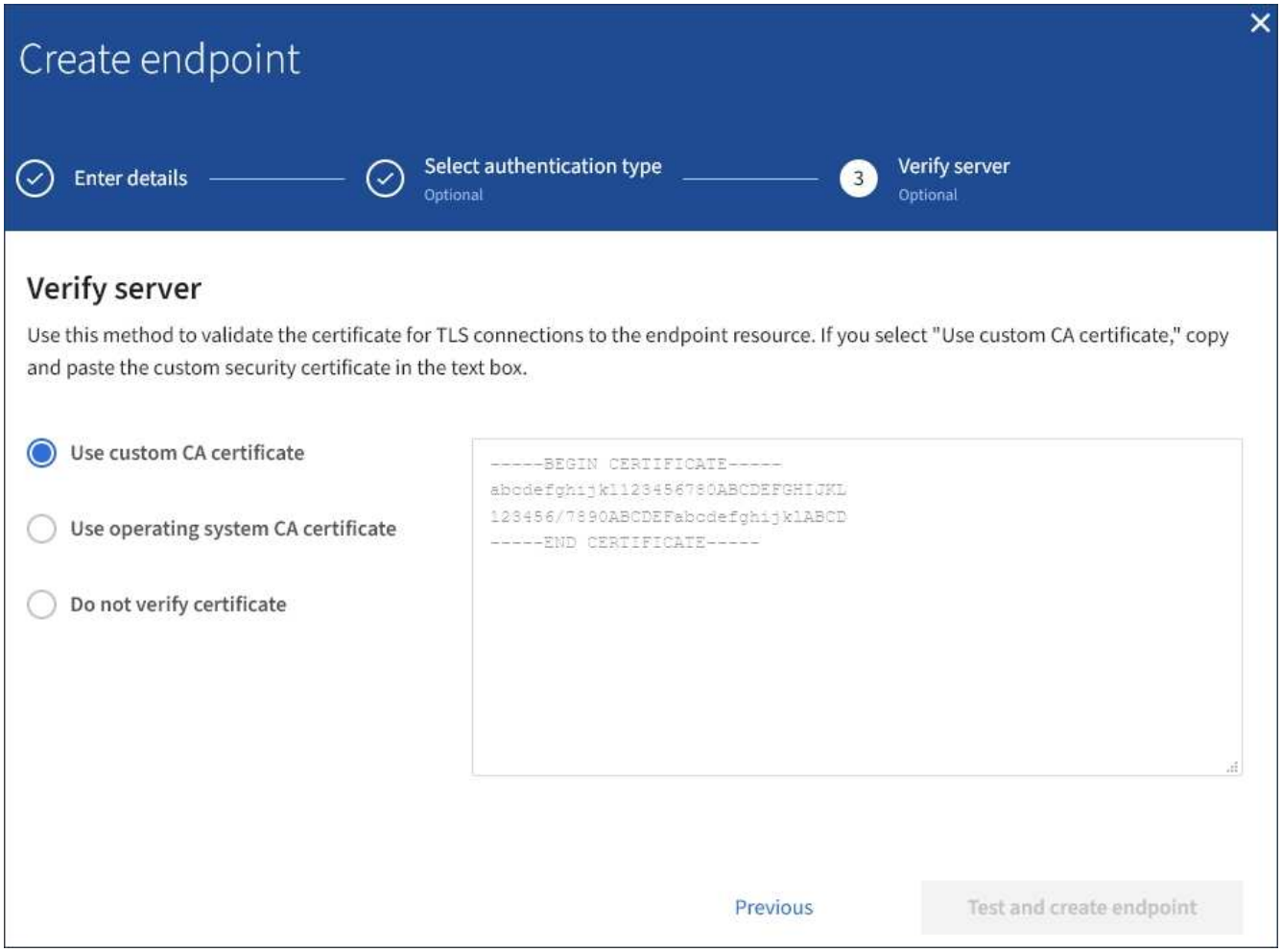
6. 選擇*繼續*。
7. 選取*驗證類型*的值、然後輸入或上傳所需的認證資料。



您提供的認證必須具有目的地資源的寫入權限。

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

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



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

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

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

設定端點之後、您可以使用其URN來設定平台服務。

相關資訊

指定平台服務端點的URN

設定CloudMirror複寫

設定事件通知

設定搜尋整合服務

測試平台服務端點的連線

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

您需要的產品

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

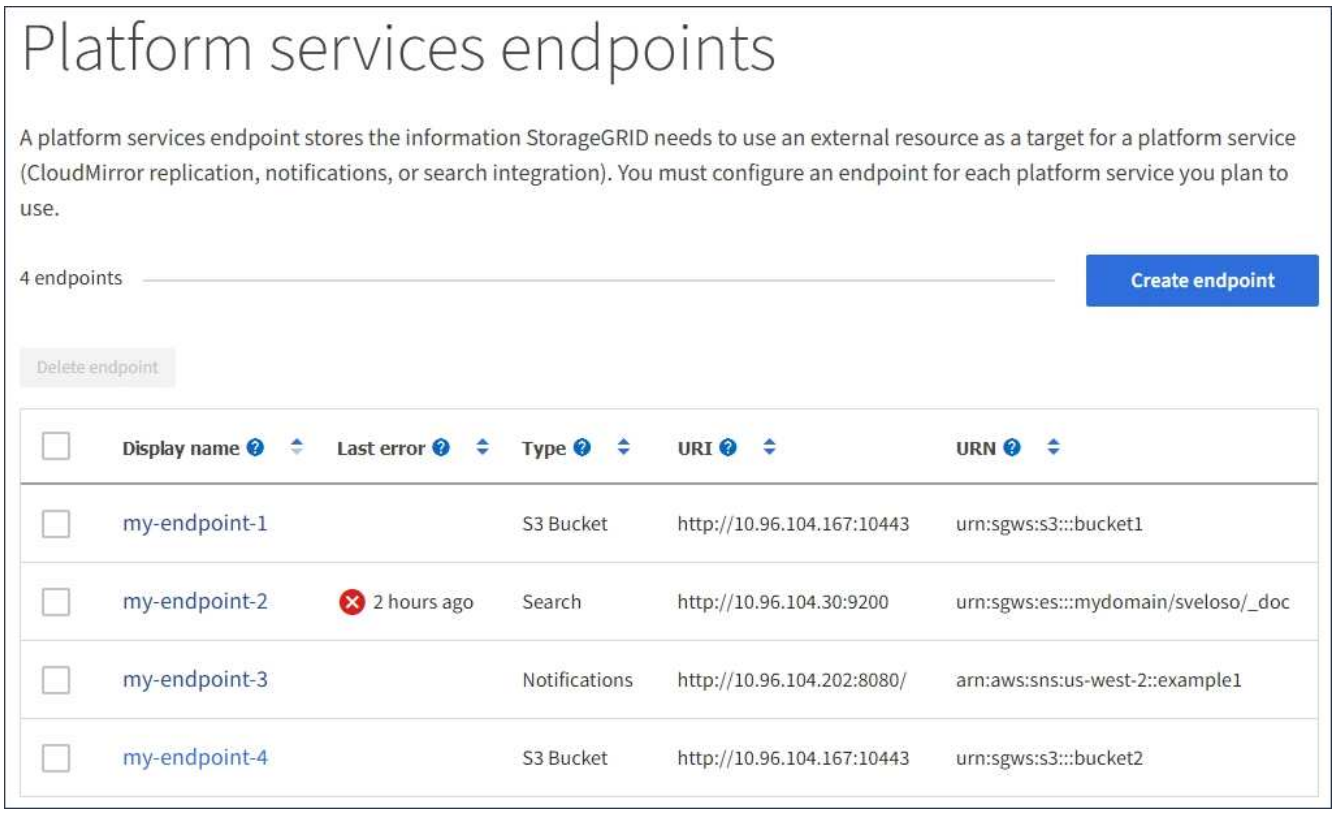
關於這項工作

無法驗證認證資料是否擁有正確的權限。StorageGRID

步驟

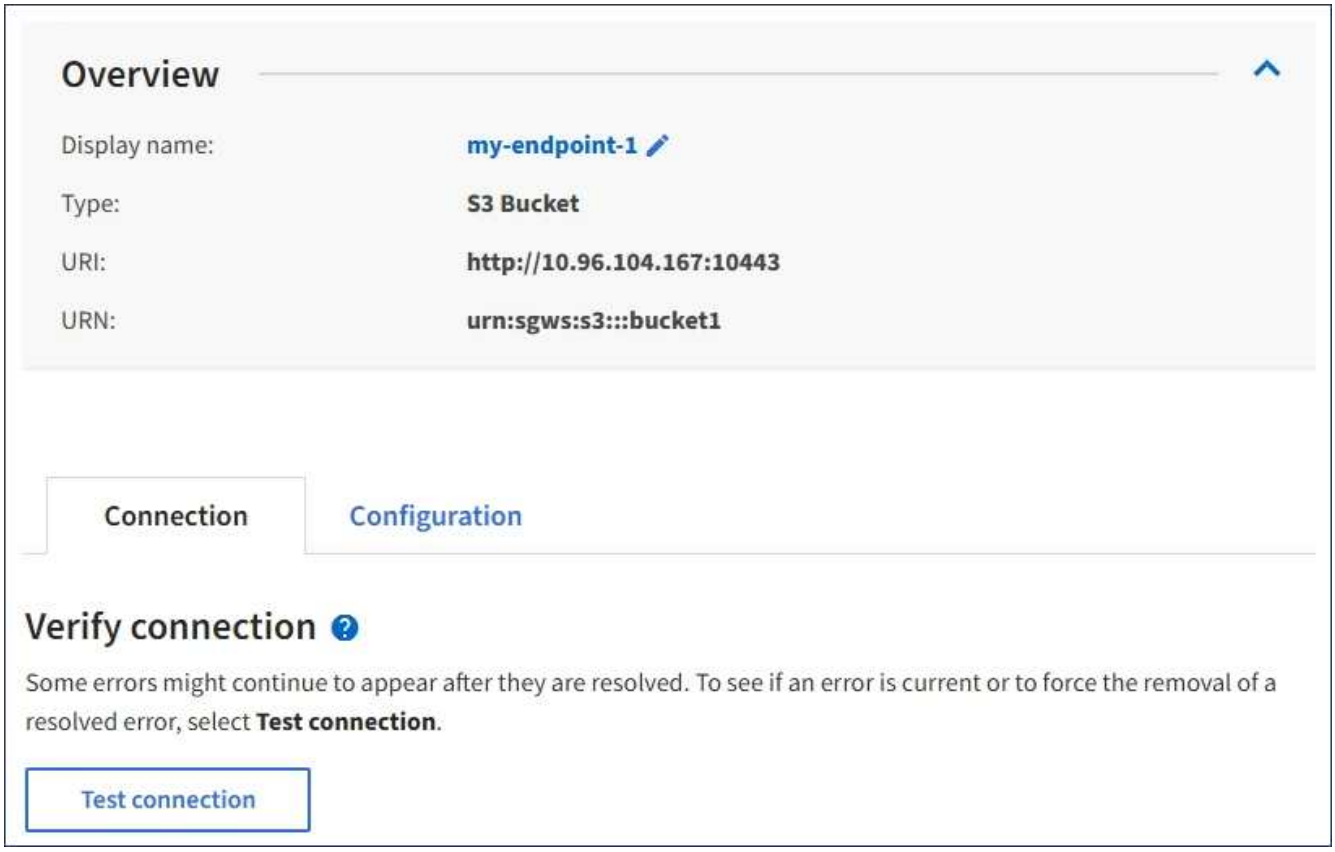
1. 選擇*儲存設備（S3）>*平台服務端點。

   「平台服務端點」頁面隨即出現、並顯示已設定的平台服務端點清單。



2. 選取您要測試其連線的端點。

端點詳細資料頁面隨即出現。



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

編輯平台服務端點

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

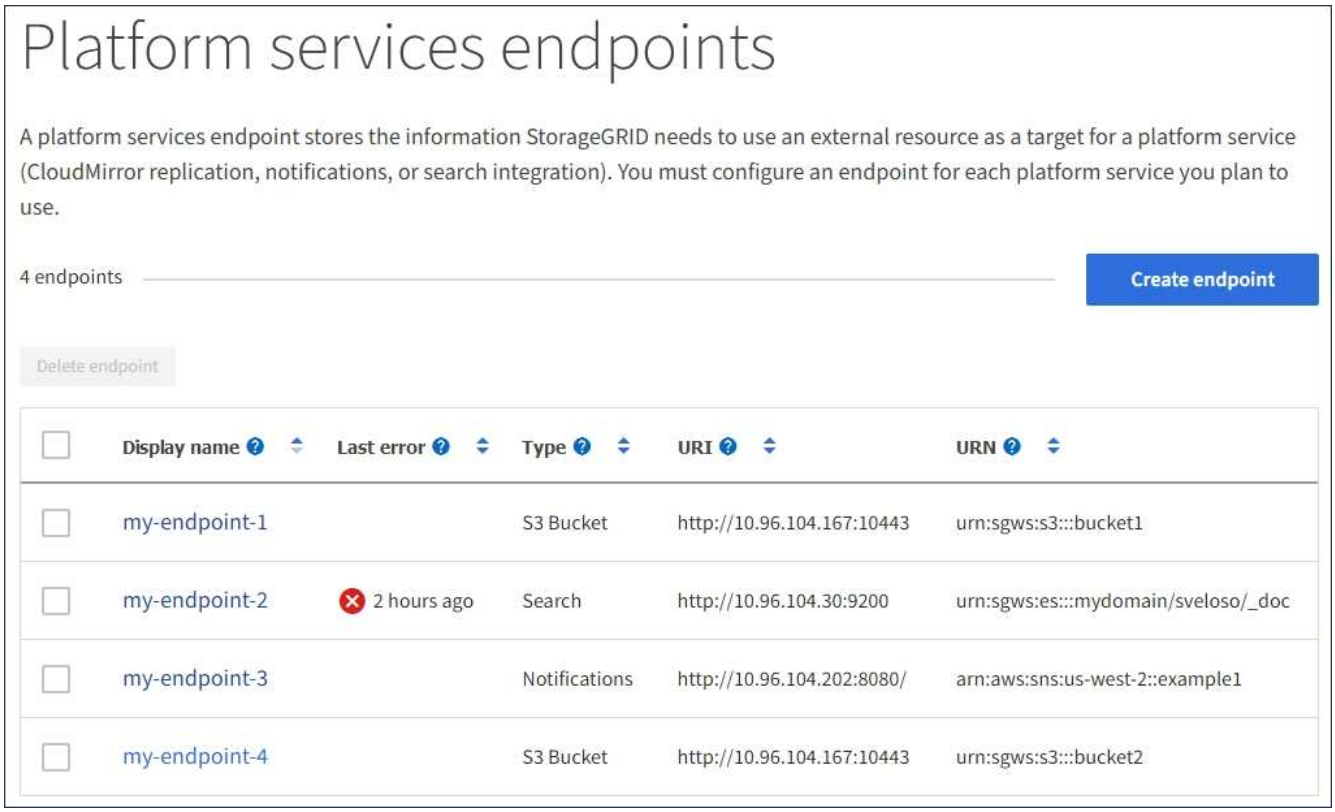
您需要的產品

- 您必須使用登入租戶管理程式 支援的網頁瀏覽器。
- 您必須屬於具有「管理端點」權限的使用者群組。請參閱 租戶管理權限。

步驟

1. 選擇*儲存設備（S3）>*平台服務端點。

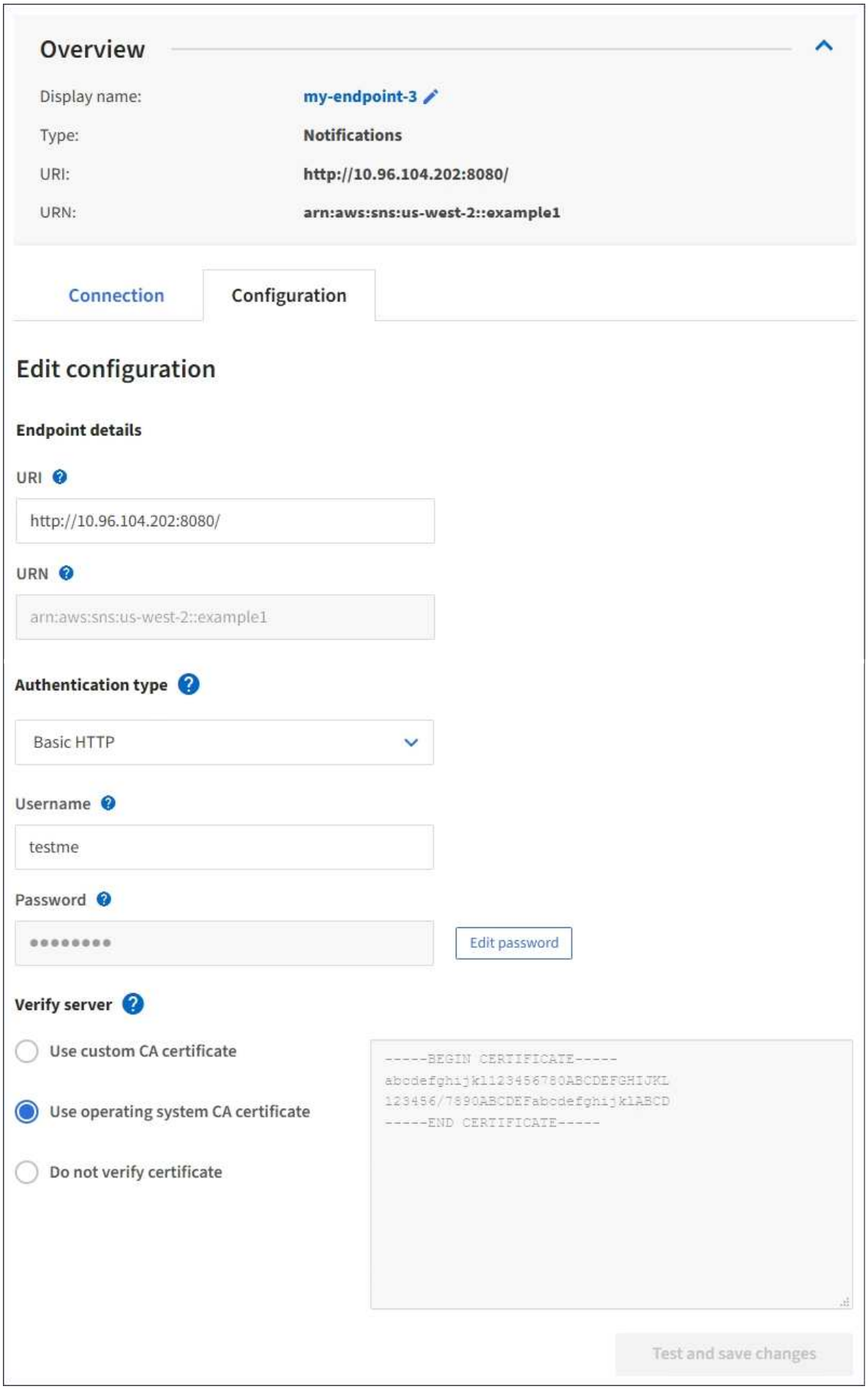
   「平台服務端點」頁面隨即出現、並顯示已設定的平台服務端點清單。



2. 選取您要編輯的端點。

   端點詳細資料頁面隨即出現。

3. 選擇*組態*。


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

4. 視需要變更端點的組態。

   建立端點之後、您無法變更端點的URN。

   a. 若要變更端點的顯示名稱、請選取編輯圖示 。

   b. 視需要變更URI。

   c. 視需要變更驗證類型。

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

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

   d. 視需要變更驗證伺服器的方法。

5. 選擇*測試並儲存變更*。

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

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

刪除平台服務端點

如果您不想再使用相關的平台服務、可以刪除端點。

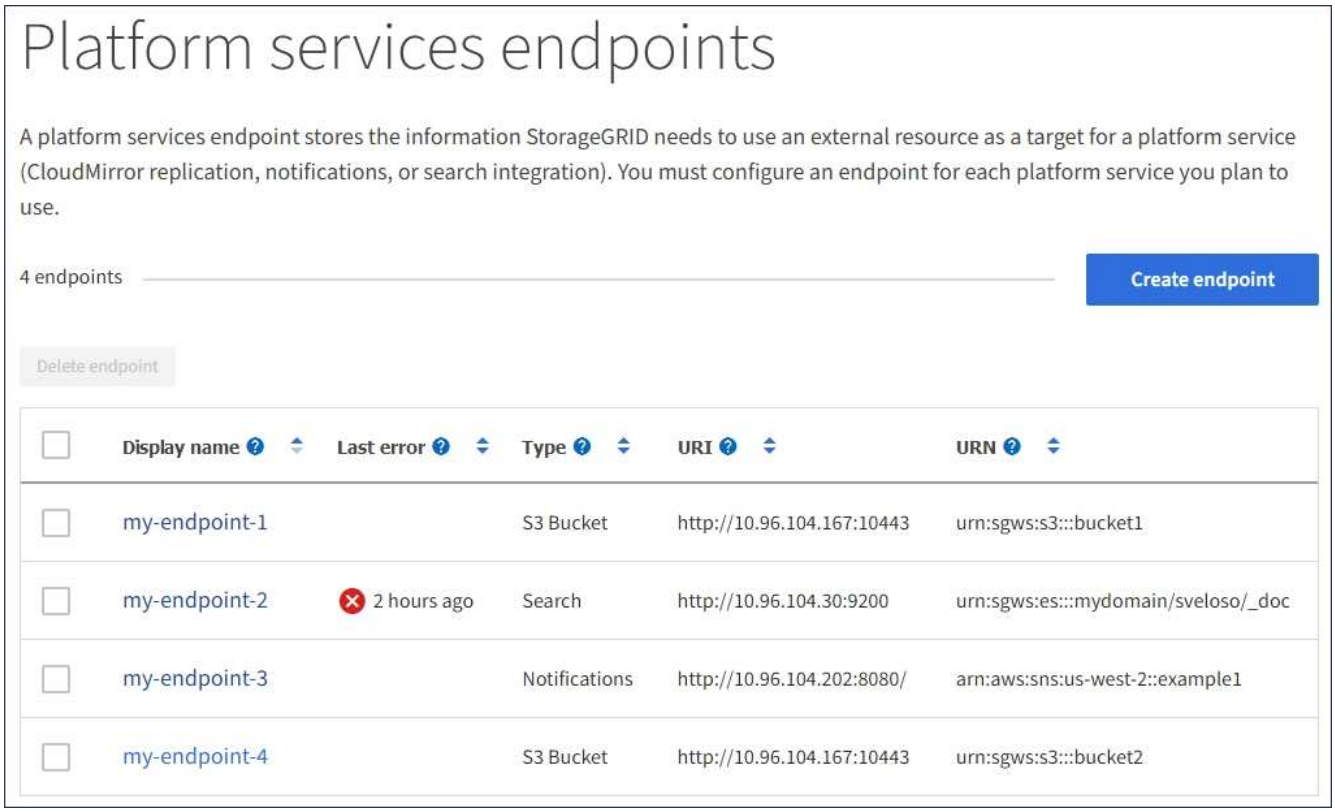
您需要的產品

- 您必須使用登入租戶管理程式 支援的網頁瀏覽器。
- 您必須屬於具有*管理端點*權限的使用者群組。請參閱 租戶管理權限。

步驟

1. 選擇*儲存設備（S3）>*平台服務端點。

   「平台服務端點」頁面隨即出現、並顯示已設定的平台服務端點清單。

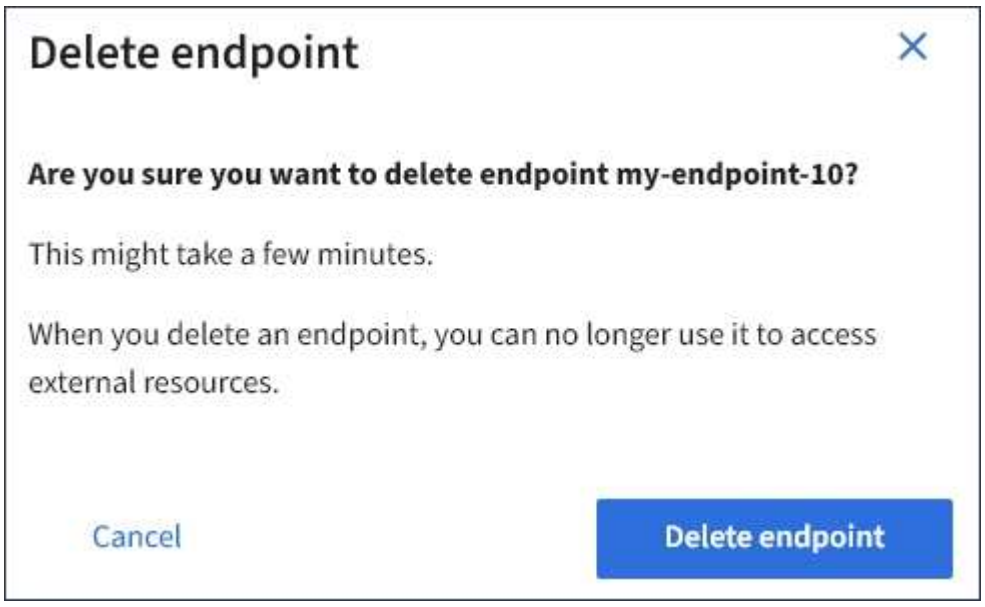


2. 選取您要刪除之每個端點的核取方塊。

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

3. 選取*「動作*」>*「刪除端點*」。

隨即顯示確認訊息。

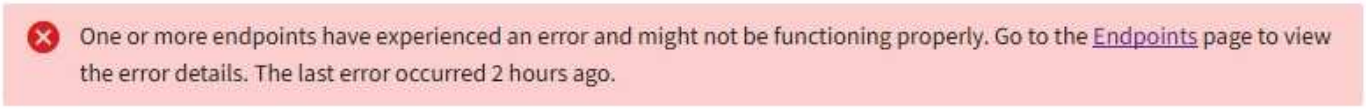


4. 選擇*刪除端點*。

如果在嘗試與平台服務端點通訊時發生錯誤StorageGRID 、儀表板上會顯示一則訊息。在「Platform Services Endives」（平台服務端點）頁面上、最後一個錯誤欄位會指出錯誤發生的時間已過多久。如果端點認證的相關權限不正確、則不會顯示錯誤。

判斷是否發生錯誤

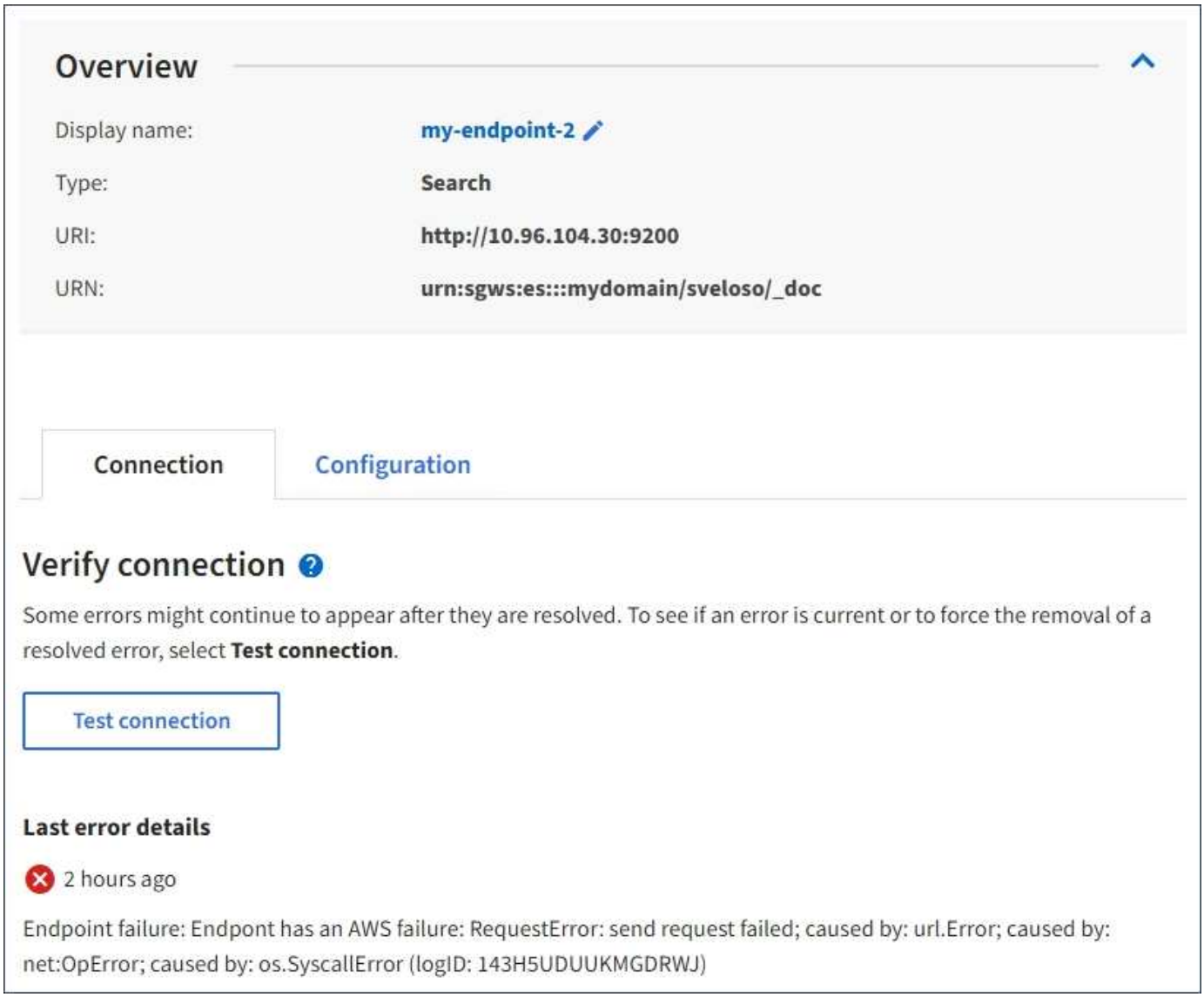
如果過去7天內發生任何平台服務端點錯誤、則租戶管理程式儀表板會顯示警示訊息。您可以移至「平台服務端點」頁面、查看錯誤的詳細資料。



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

步驟

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



檢查錯誤是否仍為最新狀態

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

步驟

1. 選取端點。

   端點詳細資料頁面隨即出現。

2. 選擇*連線*>*測試連線*。

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

解決端點錯誤

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

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

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

步驟

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

權限不足的端點認證

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

其他平台服務疑難排解

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

管理StorageGRID

相關資訊

建立平台服務端點

測試平台服務端點的連線

編輯平台服務端點

設定**CloudMirror**複寫

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

您需要的產品

- 平台服務必須由StorageGRID 管理員為您的租戶帳戶啟用。
- 您必須已經建立一個儲存區、做為複寫來源。
- 您打算做為CloudMirror複寫目的地的端點必須已經存在、而且您必須擁有它的URN。
- 您必須屬於具有「管理所有庫位」或「根存取」權限的使用者群組、才能管理租戶帳戶中所有S3庫位的設定。這些權限會在使用租戶管理程式設定儲存區時、覆寫群組或儲存區原則中的權限設定。

關於這項工作

CloudMirror複寫會將物件從來源儲存區複製到端點中指定的目的地儲存區。若要為儲存區啟用CloudMirror複寫、您必須建立並套用有效的儲存區複寫組態XML。複寫組態XML必須針對每個目的地使用S3儲存區端點的URN。

啟用S3物件鎖定的來源或目的地桶不支援複寫。

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

如果您在包含物件的儲存區上啟用CloudMirror複寫、則會複寫新增至儲存區的新物件、但儲存區中的現有物件則不會複寫。您必須更新現有物件、才能觸發複寫。

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

步驟

1. 啟用來源儲存區的複寫：

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

   - 請注意StorageGRID 、僅支援V1複寫組態。這表示StorageGRID 、由於不支援使用「Filter」元素來執行規則、因此遵循V1慣例來刪除物件版本。如需詳細資訊、請參閱Amazon複寫組態文件。
   - 使用S3貯體端點的URN作為目的地。
   - （可選）添加"<StorageClass>'元素，然後指定以下選項之一：
     - 「標準」：預設儲存類別。如果您在上傳物件時未指定儲存類別、則會使用「標準」儲存類別。
     - 「tandard_ia'：（標準-不常存取）。 此儲存類別適用於存取頻率較低、但仍需在需要時快速存取的資料。
     - 「資源冗餘」：此儲存類別適用於非關鍵且可重複產生的資料、其備援能力可低於「標準」儲存類別。
   - 如果您在組態XML中指定「角色」、則會忽略該角色。此值不供StorageGRID 下列項目使用：

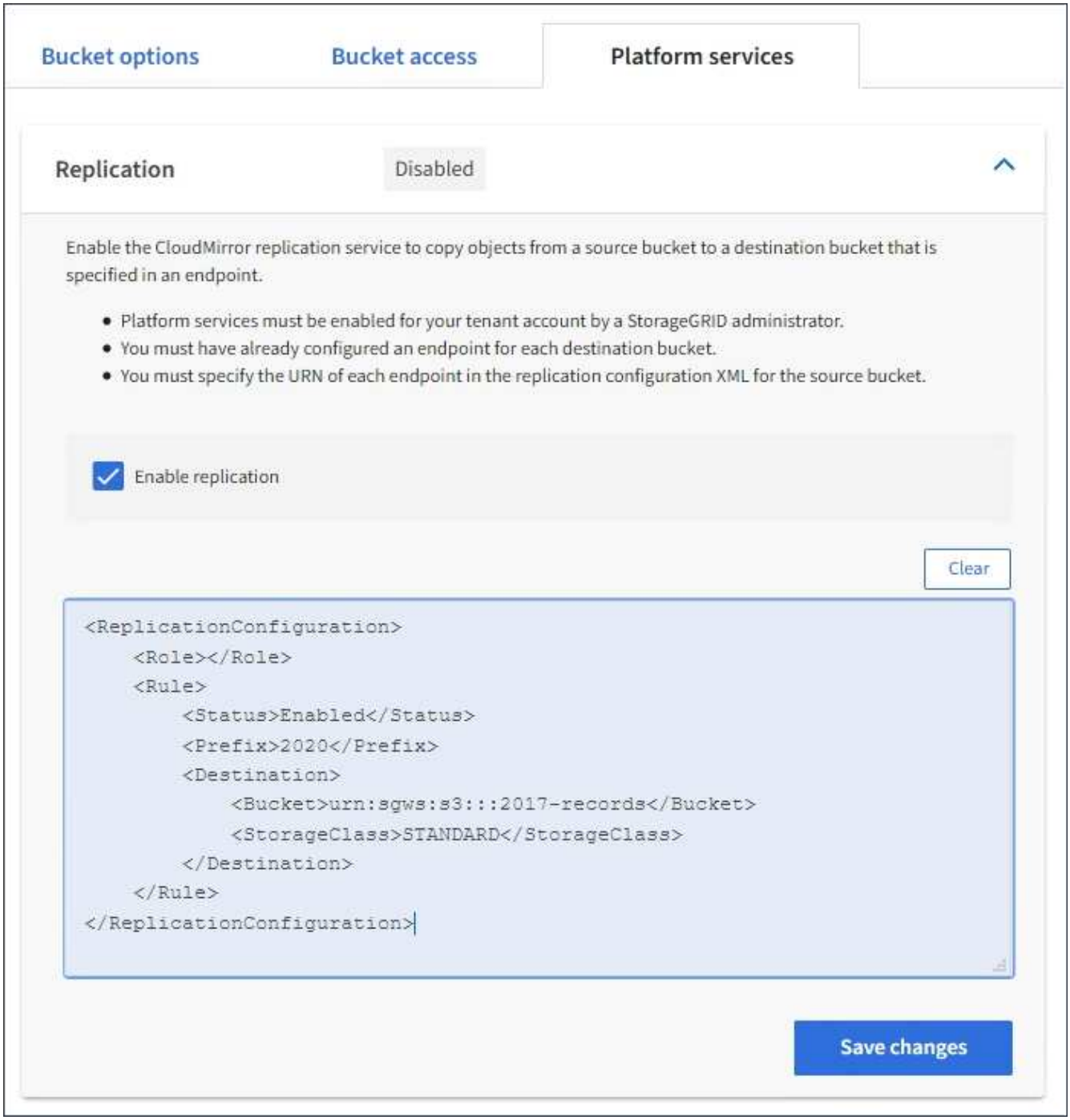
```
<ReplicationConfiguration>
    <Role></Role>
    <Rule>
        <Status>Enabled</Status>
        <Prefix>2020</Prefix>
        <Destination>
           <Bucket>urn:sgws:s3:::2017-records</Bucket>
           <StorageClass>STANDARD</StorageClass>
         </Destination>
     </Rule>
</ReplicationConfiguration>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

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

   此時會顯示「庫位詳細資料」頁面。

4. 選擇*平台服務*>*複寫*。

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



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

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

      在前面所示的範例中、會複寫與前置詞「'2020」相符的物件。

b. 確認物件已複寫至目的地儲存區。

對於小型物件、複寫作業很快就會完成。

相關資訊

使用S3

建立平台服務端點

設定事件通知

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

您需要的產品

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

關於這項工作

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

如需事件通知及其設定方式的一般資訊、請參閱Amazon文件。如需StorageGRID 瞭解有關如何實作S3儲存區通知組態API的資訊、請參閱實作S3用戶端應用程式的指示。

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

步驟

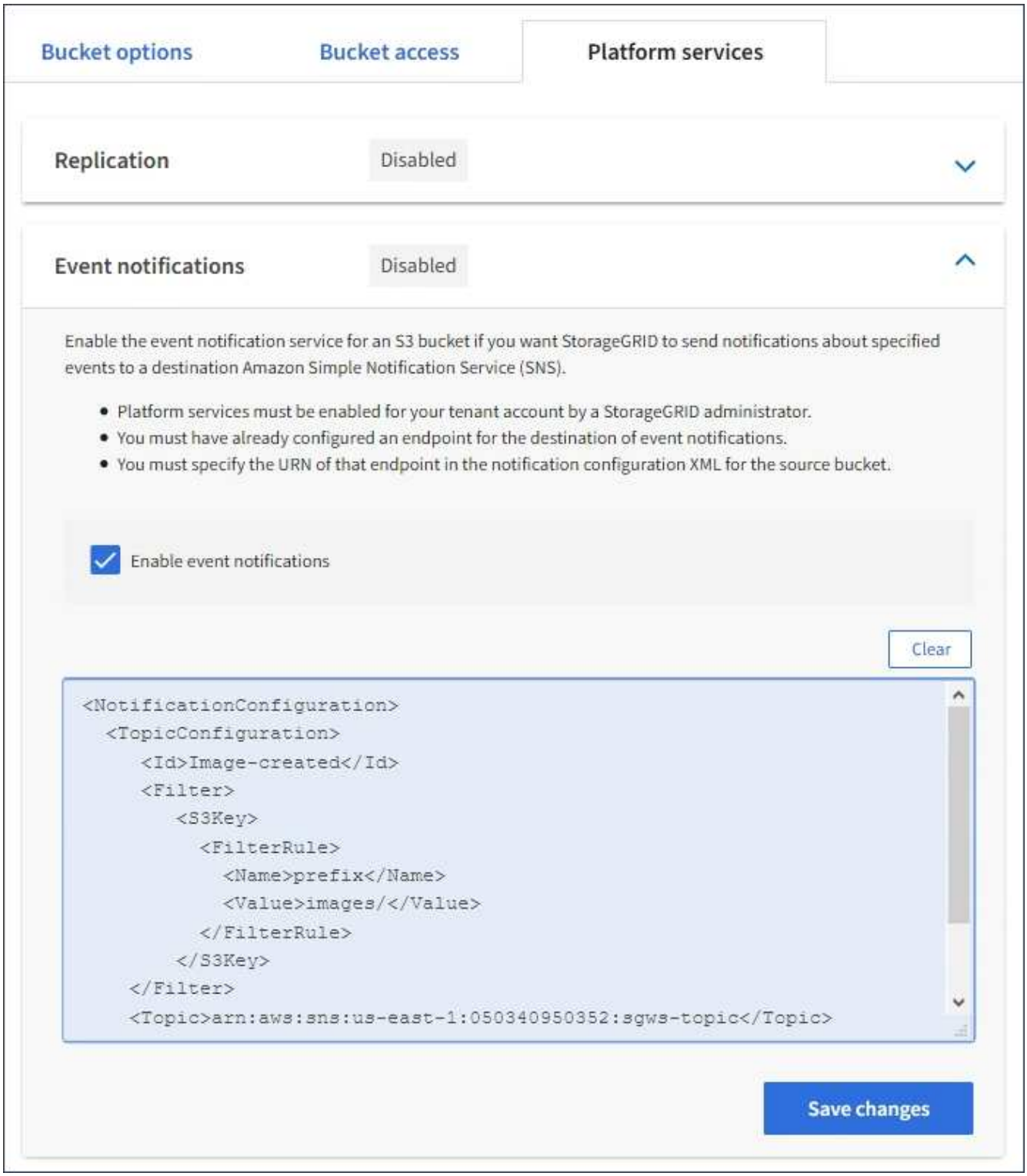
1. 啟用來源儲存區的通知：
   - 使用文字編輯器建立啟用事件通知所需的通知組態XML、如S3通知API所指定。
   - 設定XML時、請使用事件通知端點的URN作為目的地主題。

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

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

   此時會顯示「庫位詳細資料」頁面。

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



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

7. 確認事件通知設定正確：

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

      在此範例中、每當建立含有「images/」字首的物件時、就會傳送事件通知。

b. 確認已將通知傳送至目的地SNS主題。

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

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

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

相關資訊

瞭解庫存箱通知

使用S3

建立平台服務端點

使用搜尋整合服務

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

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

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

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

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

相關資訊

搜尋整合的組態XML

中繼資料通知中包含的物件中繼資料

由搜尋整合服務產生的JSON

設定搜尋整合服務

使用S3

搜尋整合的組態**XML**

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

物件可依物件名稱的前置詞進行篩選。例如、您可以將前置詞為「Images（影像）」的物件中繼資料傳送到一個目的地、並將前置詞為「videos（視訊）」的物件中繼資料傳送到另一個目的地。具有重疊前置碼的組態無效、在提交時會遭到拒絕。例如、不允許使用含有前置詞「test」的物件規則、以及含有前置詞「test2」之物件的第二個規則的組態。

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

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

下表說明中繼資料通知組態XML中的元素。

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

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

使用範例中繼資料通知組態XML來瞭解如何建構您自己的XML。

適用於所有物件的中繼資料通知組態

在此範例中、所有物件的物件中繼資料都會傳送到相同的目的地。

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

中繼資料通知組態有兩條規則

在此範例中、與首碼「/影像」相符的物件之物件中繼資料會傳送至一個目的地、而與首碼「/視訊」相符的物件之物件中繼資料則會傳送至第二個目的地。

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

相關資訊

使用S3

中繼資料通知中包含的物件中繼資料

由搜尋整合服務產生的JSON

設定搜尋整合服務

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

您需要的產品

- 平台服務必須由StorageGRID 管理員為您的租戶帳戶啟用。
- 您必須已建立S3儲存區、其內容必須為您要建立索引。
- 您要做為搜尋整合服務目的地的端點必須已經存在、而且您必須擁有它的URN。
- 您必須屬於具有「管理所有庫位」或「根存取」權限的使用者群組、才能管理租戶帳戶中所有S3庫位的設定。這些權限會在使用租戶管理程式設定儲存區時、覆寫群組或儲存區原則中的權限設定。

關於這項工作

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

步驟

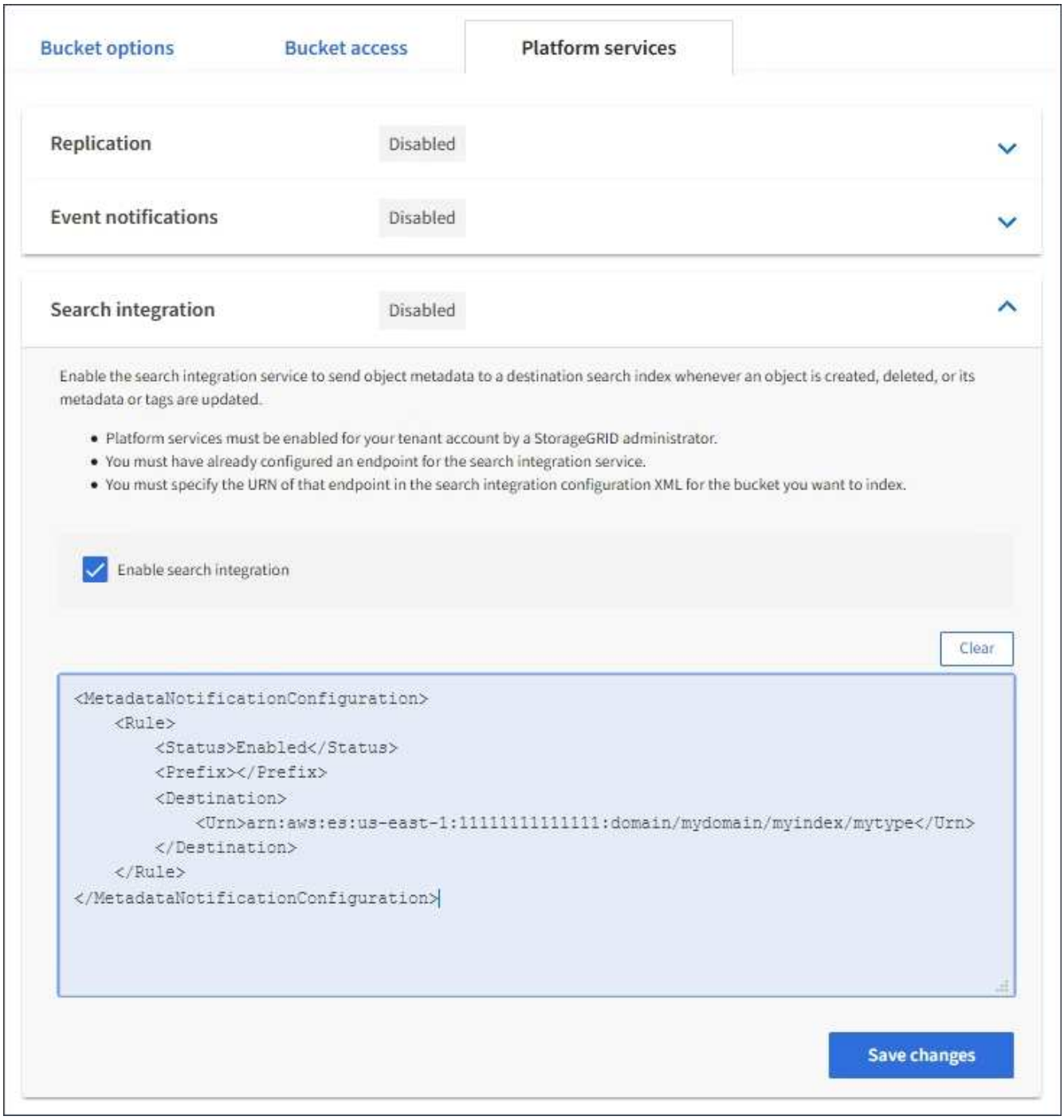
1. 使用文字編輯器建立啟用搜尋整合所需的中繼資料通知XML。
   - 請參閱組態XML的相關資訊以進行搜尋整合。
   - 設定XML時、請使用搜尋整合端點的URN作為目的地。

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

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

   此時會顯示「庫位詳細資料」頁面。

4. 選擇*平台服務*>*搜尋整合*
5. 選取*啟用搜尋整合*核取方塊。
6. 將中繼資料通知組態貼到文字方塊中、然後選取*儲存變更*。



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

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

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

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

完成後

如有必要、您可以使用下列任一方法來停用儲存區的搜尋整合：

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

相關資訊

瞭解搜尋整合服務

搜尋整合的組態XML

使用S3

建立平台服務端點

由搜尋整合服務產生的**JSON**

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

此範例顯示在名為「test」的儲存格中建立具有「GWS/Tagging.txt」鍵的物件時、可能產生的Json範例。「test」儲存區並非版本化、因此「vrionId」標記為空白。

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

中繼資料通知中包含的物件中繼資料

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

文件名稱包含儲存區名稱、物件名稱及版本ID（若有）。

類型	項目名稱與說明
儲存區和物件資訊	「桶」：桶的名稱

類型	項目名稱與說明
「金鑰」：物件金鑰名稱	「版本ID」：物件版本、適用於版本控制的儲存區中的物件
《只園》：桶區、例如「美東一號」	系統中繼資料
「尺寸」：HTTP用戶端可見的物件大小（以位元組為單位）	「md5」：物件雜湊
使用者中繼資料	「metadata」：物件的所有使用者中繼資料、做為金鑰值配對 金鑰：價值
標記	「標記」：為物件定義的所有物件標記、做為金鑰值配對 金鑰：價值

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

使用S3

使用S3：總覽

支援簡單儲存服務（S3）API、此API是以代表狀態傳輸（REST）網路服務的形式實作。StorageGRID支援S3 REST API、可讓您將專為S3網路服務開發的服務導向應用程式、連接到使用StorageGRID 該系統的內部部署物件儲存設備。這需要將用戶端應用程式目前使用S3 REST API呼叫的變更降至最低。

S3 REST API支援變更

您應該注意StorageGRID 到支援S3 REST API的功能有所變更。

版本	註解
11.6%	• 新增了使用「零件編號」要求參數的支援、可在「Get Object」（取得物件）和「head Object Request」（標頭物件要求）中使用。 • 新增S3物件鎖定的預設保留模式支援、以及儲存區層級的預設保留期間。 • 新增對「3：物件鎖定剩餘保留天數」原則條件金鑰的支援、以設定物件的允許保留期間範圍。 • 單一放置物件作業的最大_Recommended大小現在為5 GiB（5、368、709、120位元組）。如果您的物件大於5 GiB、請改用多部份上傳。 在S2011.6中StorageGRID 、單一放置物件作業的最大_supported大小仍為5 TiB（5、497、558、13880位元組）。但是、如果您嘗試上傳超過5 GiB的物件、則會觸發* S3「Pure Object size too large （將物件大小設為太大）」警示。
11.5	• 新增對管理儲存區加密的支援。 • 新增了對S3物件鎖定和過時舊版規範要求的支援。 • 新增使用刪除版本型儲存區上的多個物件的支援。 • 現在已正確支援「Content-MD5」要求標頭。
11.4	• 新增刪除庫位標記、取得庫位標記及置入庫位標記的支援。不支援成本分攤標記。 • 對於StorageGRID 在VMware 11.4中建立的儲存區、不再需要限制物件金鑰名稱以符合效能最佳實務做法。 • 增加了對「3：ObjectRestore：Post」事件類型的儲存區通知支援。 • 現在已強制多部分零件的AWS大小限制。多部分上傳中的每個部分必須介於5個mib和5 GiB之間。最後一個部分可能小於5個mib。 • 新增對TLS 1.3的支援、以及支援的TLS加密套件更新清單。 • CLB服務已過時。
11.3	• 新增支援使用客戶提供的金鑰（SSE-C）進行物件資料的伺服器端加密。 • 新增刪除、取得及置放資源庫生命週期作業（僅限到期行動）和「x-amz-expiration」回應標頭的支援。 • 更新的「放置物件」、「放置物件」-「複製」和「多重成分上傳」、說明ILM規則在擷取時使用同步放置的影響。 • 更新支援的TLS加密套件清單。不再支援TLS 1.1密碼。
11.2	新增後物件還原支援、可搭配雲端儲存資源池使用。新增了使用AWS語法的支援、可用於ARN、原則條件金鑰、以及群組和儲存區原則中的原則變數。我們StorageGRID 將繼續支援使用此功能的現有群組和儲存區原則。 *附註：*在其他組態JSON/XML中使用ARN/URN StorageGRID （包括用於自訂的版本功能）並未變更。

版本	註解
11.1.	新增跨來源資源共享（CORS）支援、S3用戶端連線至網格節點的HTTP、以及儲存區的法規遵循設定。
11.0	新增支援、可設定適用於儲存區的平台服務（CloudMirror複寫、通知及Elasticsearch整合）。此外、也新增了對儲存區物件標記位置限制的支援、以及可用的一致性控制設定。
10.4	新增對ILM掃描版本設定、端點網域名稱頁面更新、原則、原則範例及PuttoverwriteObject權限中的條件和變數的支援。
10.3.1	新增版本管理支援。
10.2	新增對群組和庫位存取原則的支援、以及多部份複本（上傳零件-複本）的支援。
10.1	新增多部分上傳、虛擬託管樣式要求及v4驗證的支援。
10.0%	由整個系統初始支援S3 REST API StorageGRID 。目前支援的_Simple Storage Service API Reference版本為2009-03-01。

支援的版本

支援下列S3和HTTP的特定版本。StorageGRID

項目	版本
S3規格	*Simple Storage Service API*參考資料 2006年3月1日
HTTP	1.1 如需HTTP的詳細資訊、請參閱HTTP / 1.1（RFC 7230-35）。 附註 StorageGRID ：不支援HTTP / 1.1鋪管。

相關資訊

"IETF RFC 2616：超文字傳輸傳輸協定（HTTP / 1.1）"

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

支援**StorageGRID** 支援功能

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

下表摘要說明可用的平台服務和用來設定的S3 API。

平台服務	目的	用來設定服務的**S3 API**
CloudMirror複寫	將物件從來源StorageGRID 的靜止庫複寫到設定的遠端S3庫位。	放入資源桶複寫
通知	將來源StorageGRID 資訊庫中的事件通知傳送至設定的簡易通知服務（SNS）端點。	放置時段通知
搜尋整合	將StorageGRID 儲存在物件庫的物件中繼資料傳送至已設定的彈性搜尋索引。	放置時段中繼資料通知 *附註：*這是StorageGRID 一套由人自訂的S3 API。

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

使用平台服務的建議

在使用平台服務之前、您必須瞭解下列建議：

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

相關資訊

使用租戶帳戶

管理StorageGRID

在貯體上作業

放置時段中繼資料通知組態要求

設定租戶帳戶和連線

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

建立及設定**S3**租戶帳戶

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

S3租戶帳戶是StorageGRID 由使用Grid Manager或Grid Management API的資訊網管理員所建立。建立S3租戶

帳戶時、網格管理員會指定下列資訊：

- 租戶的顯示名稱（租戶的帳戶ID會自動指派、無法變更）。
- 租戶帳戶是否允許使用平台服務。如果允許使用平台服務、則必須設定網格以支援其使用。
- 或者、租戶帳戶的儲存配額、也就是租戶物件可用的GB、TB或PB上限。租戶的儲存配額代表邏輯容量（物件大小）、而非實體容量（磁碟大小）。
- 如果啟用StorageGRID 身分識別聯盟以供支援整個系統、則哪個聯盟群組具有root存取權限可設定租戶帳戶。
- 如果StorageGRID 不使用單一登入（SSO）進行支援、則租戶帳戶是使用自己的身分識別來源、還是共用網格的身分識別來源、以及租戶本機root使用者的初始密碼。

建立S3租戶帳戶之後、租戶使用者就能存取租戶管理程式來執行下列工作：

- 設定身分識別聯盟（除非身分識別來源與網格共用）、並建立本機群組和使用者
- 管理S3存取金鑰
- 建立及管理S3儲存區、包括已啟用S3物件鎖定的儲存區
- 使用平台服務（若已啟用）
- 監控儲存使用量

> S3租戶使用者可以使用租戶管理程式來建立和管理S3儲存區、但必須擁有S3存取金鑰、並使用S3 REST API來擷取和管理物件。

相關資訊

管理StorageGRID

使用租戶帳戶

如何設定用戶端連線

網格管理員會做出組態選擇、影響S3用戶端連線StorageGRID 至以儲存及擷取資料的方式。建立連線所需的特定資訊取決於所選的組態。

用戶端應用程式可連線至下列任一項目、以儲存或擷取物件：

- 管理節點或閘道節點上的負載平衡器服務、或是管理節點或閘道節點之高可用度（HA）群組的虛擬IP位址（可選）
- 閘道節點上的CLB服務、或是閘道節點高可用度群組的虛擬IP位址（可選）

> CLB服務已過時。在發佈版推出之前設定的用戶端StorageGRID 、可以繼續在閘道節點上使用CLB服務。所有其他仰賴StorageGRID 以提供負載平衡的用戶端應用程式、都應該使用負載平衡器服務進行連線。

- 儲存節點、無論是否有外部負載平衡器

設定StorageGRID 功能時、網格管理員可以使用Grid Manager或Grid Management API來執行下列步驟、這些步驟都是選用的：

1. 設定負載平衡器服務的端點。

   您必須設定端點以使用負載平衡器服務。管理節點或閘道節點上的負載平衡器服務會將傳入的網路連線從用戶端應用程式分散到儲存節點。建立負載平衡器端點時StorageGRID 、系統管理員會指定連接埠號碼、端點是否接受HTTP或HTTPS連線、使用端點的用戶端類型（S3或Swift）、以及用於HTTPS連線的憑證（若適用）。

2. 設定不受信任的用戶端網路。

   如果StorageGRID 某個節點的用戶端網路設定為不受信任、則該節點僅接受用戶端網路上明確設定為負載平衡器端點之連接埠的傳入連線。

3. 設定高可用度群組。

   如果系統管理員建立HA群組、則多個管理節點或閘道節點的網路介面會置於主動備份組態中。用戶端連線是使用HA群組的虛擬IP位址進行。

如需每個選項的詳細資訊、請參閱《關於管理StorageGRID 功能的說明》。

相關資訊

管理StorageGRID

摘要：用於用戶端連線的**IP**位址和連接埠

用戶端應用程式StorageGRID 會使用網格節點的IP位址和該節點上服務的連接埠號碼來連線至功能區。如果已設定高可用度（HA）群組、用戶端應用程式就可以使用HA群組的虛擬IP位址進行連線。

建立用戶端連線所需的資訊

下表摘要說明用戶端連線StorageGRID 至靜態的不同方式、以及每種連線類型所使用的IP位址和連接埠。如StorageGRID 需更多資訊、請聯絡您的管理員、或參閱《管理StorageGRID 》的說明、以瞭解如何在Grid Manager中找到這些資訊。

連線位置	用戶端連線的服務	**IP** 位址	連接埠
HA群組	負載平衡器	HA群組的虛擬IP位址	• 負載平衡器端點連接埠
HA群組	CLB *附註： CLB服務已過時。	HA群組的虛擬IP位址	預設S3連接埠： • HTTPS：8082 • HTTP：8084
管理節點	負載平衡器	管理節點的IP位址	• 負載平衡器端點連接埠
閘道節點	負載平衡器	閘道節點的IP位址	• 負載平衡器端點連接埠

連線位置	用戶端連線的服務	IP 位址	連接埠
閘道節點	CLB *附註： CLB服務已過時。	閘道節點的IP位址 **附註：*根據預設、不會啟用CLB和LDR的HTTP連接埠。	預設S3連接埠： • HTTPS：8082 • HTTP：8084
儲存節點	LdR	儲存節點的IP位址	預設S3連接埠： • HTTPS：18082 • HTTP：18084

範例

若要將S3用戶端連線至閘道節點HA群組的負載平衡器端點、請使用結構如下所示的URL：

- https://*VIP-of-HA-group*:_LB-endpoint-port_`

例如、如果HA群組的虛擬IP位址為192.0.2.5、而S3負載平衡器端點的連接埠號碼為10443、則S3用戶端可以使用下列URL連線StorageGRID 到SESH:

- https://192.0.2.5:10443`

您可以為用戶端用來連線StorageGRID 到靜態的IP位址設定DNS名稱。請聯絡您的本機網路管理員。

相關資訊

管理StorageGRID

決定使用**HTTPS**或**HTTP**連線

使用負載平衡器端點進行用戶端連線時、必須使用為該端點指定的傳輸協定（HTTP或HTTPS）來建立連線。若要在用戶端連線至儲存節點或閘道節點上的CLB服務時使用HTTP、您必須啟用它的使用。

根據預設、當用戶端應用程式連線至閘道節點上的儲存節點或CLB服務時、它們必須使用加密的HTTPS進行所有連線。或者、您也可以選取「Grid Manager（網格管理器）」中的*「Enable HTTP Connection* Grid（啟用HTTP連線*網格）」選項、來啟用較不安全的HTTP連線。例如、用戶端應用程式在非正式作業環境中測試與儲存節點的連線時、可能會使用HTTP。

啟用正式作業網格的HTTP時請務必小心、因為要求會以不加密的方式傳送。

CLB服務已過時。

如果選取*「啟用HTTP連線*」選項、則用戶端的HTTP連接埠必須與HTTPS使用的連接埠不同。請參閱「管理StorageGRID 功能」的說明。

相關資訊

管理StorageGRID

作用中、閒置及並行HTTP連線的優點

S3要求的端點網域名稱

在用戶端要求使用S3網域名稱之前、StorageGRID 管理員必須先將系統設定為接受在S3路徑樣式和S3虛擬託管樣式要求中使用S3網域名稱的連線。

關於這項工作

若要使用S3虛擬託管樣式要求、網格管理員必須執行下列工作：

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

  例如、如果端點是「3.company.com`」、則網格管理員必須確保用於HTTPS連線的憑證包含「s3.company.com`端點和端點的萬用字元主體替代名稱（SAN）：「*.s3.company.com`」。

- 設定用戶端使用的DNS伺服器、以納入符合端點網域名稱的DNS記錄、包括任何必要的萬用字元記錄。

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

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

如果用戶端連線至閘道節點上的儲存節點或CLB服務、則網格管理員設定的憑證是用於網格的單一自訂伺服器憑證。

CLB服務已過時。

如StorageGRID 需詳細資訊、請參閱《關於管理功能的說明》。

完成這些步驟之後、您就可以使用虛擬託管樣式的要求（例如「bucket.s3.company.com`」）。

相關資訊

管理StorageGRID

設定REST API的安全性

測試S3 REST API組態

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

您需要的產品

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

步驟

1. 設定Amazon Web Services設定、以使用StorageGRID 您在該系統中建立的帳戶：
   a. 進入組態模式：「AWS configure」

b. 輸入您所建立帳戶的AWS存取金鑰ID。

c. 輸入您所建立帳戶的AWS秘密存取金鑰。

d. 輸入要使用的預設區域、例如us-east-1。

e. 輸入要使用的預設輸出格式、或按* Enter *選取Json。

2. 建立儲存庫。

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

如果成功建立了儲存區、則會傳回儲存區的位置、如下列範例所示：

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

1. 上傳物件。

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

如果物件上傳成功、則會傳回Etag、這是物件資料的雜湊。

2. 列出儲存區的內容、以驗證物件是否已上傳。

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

3. 刪除物件。

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

4. 刪除儲存庫。

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

如何實作S3 REST API StorageGRID

用戶端應用程式可以使用S3 REST API呼叫來連線StorageGRID 至以建立、刪除和修改儲存區、以及儲存和擷取物件。

衝突的用戶端要求

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

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

一致性控管

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

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

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

一致性控管

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

您可以將桶或API作業的一致性控制設定為下列其中一個值：

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

使用「全新寫入後的準備」和「可用」一致性控制

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

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

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

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

指定**API**作業的一致性控制

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

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

您必須對「放置物件」和「取得物件」作業使用相同的一致性控制。

指定桶的一致性控制

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

設定桶的一致性控制時、請注意下列事項：

- 設定區段的一致性控制可決定哪些一致性控制用於在區段或區段組態中的物件上執行S3作業。它不會影響儲存庫本身的作業。
- 個別API作業的一致性控制會覆寫貯體的一致性控制。
- 一般而言、儲存貯體應該使用預設的一致性控制：「全新寫入後的讀取」。 如果要求無法正常運作、請盡可能變更應用程式用戶端行為。或者、將用戶端設定為針對每個API要求指定一致性控制。只能將貯體層級的一致性控制設定為最後的方法。

一致性控制與**ILM**規則如何互動、以影響資料保護

您選擇的一致性控制和ILM規則都會影響物件的保護方式。這些設定可以互動。

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

下列擷取行為適用於ILM規則：

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

選取 ILM 規則的擷取行為之前、請先閱讀中這些設定的完整說明 使用ILM管理物件。

一致性控制和**ILM**規則如何互動的範例

假設您有一個雙站台網格、其中包含下列ILM規則和下列一致性層級設定：

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

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

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

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

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

相關資訊

取得時段一致性要求

置入時段一致性要求

如何利用**ILM**規則來管理物件**StorageGRID**

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

ILM設定決定物件的下列層面：

- 地理

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

- 儲存等級

  用於儲存物件資料的儲存類型：例如Flash或旋轉式磁碟。

- 損失保護

  製作了多少份複本、以及建立的複本類型：複寫、銷毀編碼或兩者。

- 保留

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

- 擷取期間的保護

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

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

- 租戶帳戶
- 儲存區名稱
- 擷取時間
- 金鑰
- 上次存取時間

> 根據預設、所有S3儲存區的上次存取時間更新都會停用。如果StorageGRID 您的支援系統包含使用「上次存取時間」選項的ILM規則、則必須針對該規則中指定的S3儲存區、啟用更新以達到上次存取時間。您可以使用租戶管理程式中的「放置時段上次存取時間」要求、「* S3 > Bucket >*設定上次存取時間」核取方塊、或使用租戶管理API來啟用上次存取時間更新。啟用上次存取時間更新時、請注意StorageGRID 、可能會降低不佳效能、尤其是在使用小型物件的系統中。

- 位置限制
- 物件大小
- 使用者中繼資料
- 物件標記

如需ILM的詳細資訊、請參閱資訊生命週期管理的物件管理說明。

相關資訊

使用租戶帳戶

使用ILM管理物件

將時段放入上次存取時間要求

物件版本管理

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

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

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

不支援使用MFA（多因素驗證）刪除。

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

ILM與版本管理

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

對於啟用版本管理的儲存區中的S3物件、版本管理支援可讓您建立使用非目前時間做為參考時間的ILM規則。更新物件時、其舊版本會變成非最新版本。使用非目前時間篩選器可讓您建立原則、以降低舊版物件的儲存影響。

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

如需S3版本物件的ILM原則範例、請參閱使用資訊生命週期管理來管理物件的指示。

相關資訊

使用ILM管理物件

實作S3 REST API的建議

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

針對不存在物件的使用者提出建議

如果您的應用程式經常檢查某個物件是否存在於您預期該物件實際上不存在的路徑中、您應該使用「可用」一致性控制。例如、如果您的應用程式在放入之前就先前往某個位置、則應該使用「可用」一致性控制。

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

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

物件金鑰建議

對於StorageGRID 在VMware 11.4或更新版本中建立的儲存區、不再需要限制物件金鑰名稱以符合效能最佳實務做法。例如、您現在可以將隨機值用於物件金鑰名稱的前四個字元。

對於StorageGRID 在更新版本早於《物件金鑰名稱》的版本中所建立的儲存區、請繼續遵循下列建議：

- 您不應使用隨機值做為物件金鑰的前四個字元。這與前AWS關於金鑰前置碼的建議不同。您應該改用非隨機、非獨特的前置詞、例如「image」。
- 如果您遵循前一項AWS建議、在金鑰前置字元中使用隨機和獨特的字元、則應該在物件金鑰前置一個目錄名稱。也就是使用此格式：

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

而非此格式：

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

「range Reads」建議

如果選擇*壓縮儲存物件*選項（組態>*系統*>*網格選項*）、S3用戶端應用程式應避免執行指定位元組範圍的「Get物件」作業。這些「範圍讀取」作業效率不彰、因為StorageGRID 必須有效解壓縮物件才能存取所要求的位元組。從非常大的物件要求少量位元組的「Get Object」（取得物件）作業效率特別低；例如、從50 GB壓縮物件讀取10 MB範圍的效率非常低。

如果從壓縮物件讀取範圍、用戶端要求可能會逾時。

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

相關資訊

- 一致性控管
- 置入時段一致性要求
- 管理StorageGRID

S3 REST API支援的作業和限制

此系統實作簡單儲存服務API（API版本2002-03）、支援大部分作業、並有一些限制。StorageGRID整合S3 REST API用戶端應用程式時、您必須瞭解實作詳細資料。

支援虛擬託管型要求和路徑型要求的支援。StorageGRID

日期處理

S3 REST API的支援僅支援有效的HTTP日期格式。StorageGRID

支援此功能的僅支援接受日期值的任何標頭的有效HTTP日期格式。StorageGRID日期的時間部分可以格林尼治標準時間（GMT）格式指定、或以通用協調時間（UTC）格式指定、且無時區偏移（必須指定+0000）。如果您在申請中加入「x-amz-date」標頭、它會覆寫在「日期」申請標頭中指定的任何值。使用AWS簽名版本4時、由於不支援日期標頭、因此簽署的要求中必須有「x-amz-date」標頭。

一般要求標頭

支援由定義的一般要求標頭StorageGRID "Amazon Web Services（AWS）文件：Amazon Simple Storage Service API Reference"、但有一項例外。

要求標頭	實作
授權	完整支援AWS簽名版本2 支援AWS簽名版本4、但有下列例外： • SHA256值不會針對申請本文進行計算。使用者提交的值會在未經驗證的情況下接受、如同「X-amz-content-sha256」標頭所提供的值「unsign-payload」一樣。
X-amz-security-token	未實作。返回"XNotImplemated（XNotImplemed）"。

通用回應標頭

支援所有由_Simple Storage Service API Reference（簡易儲存服務API參考）定義的通用回應標頭、但有一項例外。StorageGRID

回應標頭	實作
X-amz-id-2	未使用

驗證要求

支援使用S3 API驗證和匿名存取物件的功能。StorageGRID

S3 API支援驗證S3 API要求的簽名版本2和簽名版本4。

驗證的要求必須使用您的存取金鑰ID和秘密存取金鑰來簽署。

支援兩種驗證方法：HTTP「授權」標頭和使用查詢參數。StorageGRID

使用**HTTP**授權標頭

除了資源庫原則允許的匿名要求之外、所有S3 API作業都會使用HTTP「授權」標頭。「授權」標頭包含驗證要求所需的所有簽署資訊。

使用查詢參數

您可以使用查詢參數將驗證資訊新增至URL。這稱為URL預先簽署、可用來授予特定資源的暫時存取權。具有預先簽署URL的使用者不需要知道秘密存取金鑰、就能存取資源、讓您提供第三方受限的資源存取權。

服務營運

支援下列服務作業的支援。StorageGRID

營運	實作
取得服務	以所有Amazon S3 REST API行為來實作。

營運	實作
取得儲存使用量	「Get Storage使用量」要求會告訴您某個帳戶所使用的總儲存容量、以及與該帳戶相關聯的每個儲存區容量。這是一項服務作業、其路徑為/、並新增自訂查詢參數（「x - ntap - sg - usage」）。
選項/	用戶端應用程式可在不提供S3驗證認證的情況下、對儲存節點上的S3連接埠發出「選項/」要求、以判斷儲存節點是否可用。您可以使用此要求進行監控、或允許外部負載平衡器識別儲存節點何時當機。

相關資訊

取得儲存使用量要求

在貯體上作業

這個系統最多可為每個S3租戶帳戶支援1、000個貯體。StorageGRID

儲存區名稱限制遵循AWS US Standard地區限制、但您應該進一步限制它們使用DNS命名慣例、以支援S3虛擬託管型要求。

"Amazon Web Services（AWS）文件：儲存區限制與限制"

設定S3 API端點網域名稱

Get Bucket（列出物件）和Get Bucket版本作業支援StorageGRID 一致性控管。

您可以檢查是否為個別的儲存區啟用或停用上次存取時間的更新。

下表說明StorageGRID 了為什麼由Ss哪些 人執行S3 REST API貯體作業。若要執行上述任何作業、必須為帳戶提供必要的存取認證資料。

營運	實作
刪除時段	以所有Amazon S3 REST API行為來實作。
刪除庫位檢查	此作業會刪除儲存區的CORS組態。
刪除時段加密	此作業會從儲存區刪除預設加密。現有的加密物件仍會保持加密狀態、但新增至儲存區的任何新物件都不會加密。
刪除時段生命週期	此作業會從儲存庫中刪除生命週期組態。
刪除庫位原則	此作業會刪除附加至儲存貯體的原則。
刪除時段複寫	此作業會刪除附加至儲存區的複寫組態。

營運	實作
刪除庫位標記	此作業使用「標記」子資源來移除貯體中的所有標記。
Get Bucket（列出物件）、版本1和版本2	此作業會傳回某個儲存區中的部分或全部（最多1、000個）物件。物件的儲存類別可以有兩個值之一、即使物件是使用「已儲存的備援」儲存類別選項擷取的： • 「標準」、表示物件儲存在儲存節點所組成的儲存資源池中。 • 「Glacier」、表示物件已移至Cloud Storage Pool指定的外部儲存桶。 如果儲存區包含大量具有相同前置碼的刪除金鑰、回應可能會包含一些不含金鑰的「CommonPrechs」。
取得Bucket ACL	此作業會傳回正面回應、並傳回貯體擁有者的ID、顯示名稱和權限、表示擁有者對該貯體具有完整存取權。
獲取庫位檢查器	此操作會傳回該鏟斗的「cors」組態。
取得Bucket加密	此作業會傳回儲存區的預設加密組態。
取得生命週期	此作業會傳回該儲存庫的生命週期組態。
取得理想位置	此作業會傳回使用PUT Bucket要求中的「LocationConstraint」元素所設定的區域。如果桶區為「us-east-1」、則會傳回該區域的空白字串。
取得庫存箱通知	此作業會傳回附加至儲存貯體的通知組態。
取得Bucket物件版本	此作業可透過儲存區的讀取存取權限、以「版本」子資源列出儲存區中所有物件版本的中繼資料。
取得庫存管理政策	此作業會傳回附加至庫位的原則。
取得庫位複寫	此作業會傳回附加至儲存區的複寫組態。
取得庫位標記	此作業使用「標記」子資源來傳回某個儲存區的所有標記。
取得版本管理	此實作會使用「資料夾」子資源來傳回儲存庫的版本管理狀態。 • *blank*：從未啟用版本管理（儲存庫為「未版本管理」） • 已啟用：已啟用版本管理 • 已暫停：先前已啟用版本管理、並已暫停
取得物件鎖定組態	此作業會傳回儲存區預設保留模式和預設保留期間（若已設定）。 請參閱 取得物件鎖定組態 以取得詳細資訊。

營運	實作
鏟斗	此作業會判斷儲存區是否存在、且您是否有權存取它。 此作業會傳回： • 「X-nTap sg-bucke-id」：UUID格式的儲存區UUID。 • 「X-ntap-sg-scale-id」：相關要求的唯一追蹤ID。
放入鏟斗	此作業會建立新的儲存桶。建立貯體後、您就成為了貯體的擁有者。 • 庫位名稱必須符合下列規則： ◦ 必須在各個StorageGRID 方面都是獨一無二的（不只是租戶帳戶內的獨特功能）。 ◦ 必須符合DNS規範。 ◦ 必須包含至少3個字元、且不得超過63個字元。 ◦ 可以是一或多個標籤的系列、相鄰的標籤以句點分隔。每個標籤都必須以英文字母或數字開頭和結尾、而且只能使用英文字母、數字和連字號。 ◦ 不得看起來像是文字格式的IP位址。 ◦ 不應在虛擬託管樣式要求中使用期間。期間會導致伺服器萬用字元憑證驗證發生問題。 • 根據預設、會在「us-east-1」區域建立貯體、不過您可以在要求主體中使用「LocationConstraint」要求元素來指定不同的區域。使用「LocationConstraint」元素時、您必須指定已使用Grid Manager或Grid Management API定義的確切區域名稱。如果您不知道應該使用的地區名稱、請聯絡系統管理員。 附註：如果您的Pet Bucket要求使用StorageGRID 未在功能區中定義的區域、就會發生錯誤。 • 您可以加入「X-amz-Bucket物件鎖定」要求標頭、以建立啟用S3物件鎖定的儲存區。請參閱 使用S3物件鎖定。 建立儲存區時、您必須啟用S3物件鎖定。建立儲存區之後、您無法新增或停用S3物件鎖定。S3物件鎖定需要儲存區版本管理、這會在您建立儲存區時自動啟用。
放入庫位	此作業會設定儲存區的CORS組態、以便儲存區能夠處理跨來源要求。跨來源資源共用（CORS）是一種安全機制、可讓單一網域中的用戶端Web應用程式存取不同網域中的資源。例如、假設您使用名為「imag像」的S3儲存區來儲存圖形。設定「映像」儲存區的CORS組態、即可讓該儲存區中的映像顯示在網站上。http://www.example.com`

營運	實作
使用資源桶加密	此作業會設定現有儲存區的預設加密狀態。啟用桶層級加密時、任何新增至桶的新物件都會加密。StorageGRID支援使用StorageGRID管理的金鑰進行伺服器端加密。指定伺服器端加密組態規則時、請將「SEAlgorithm」參數設為「AES256」、而不要使用「KMSmsterKeyID」參數。 如果物件上傳要求已指定加密（亦即、如果要求包含「x-amz-server端加密-*」要求標頭）、則會忽略儲存區預設加密組態。
放入鏟斗生命週期	此作業會為儲存庫建立新的生命週期組態、或取代現有的生命週期組態。在生命週期組態中、支援多達1、000個生命週期規則。StorageGRID每個規則可包含下列XML元素： • 到期日（天數、日期） • 非目前版本過期（非目前日期） • 篩選器（前置、標記） • 狀態 • ID 不支援下列動作：StorageGRID • AbortIncompleteMultiPart上 傳 • ExpiredObjectDelete標記 • 移轉 若要瞭解儲存庫生命週期中的到期行動如何與ILM放置指示互動、請參閱資訊生命週期管理物件說明中的「ILM在物件生命週期內的運作方式」。 附註：鏟斗生命週期組態可搭配已啟用S3物件鎖定的鏟斗使用、但舊型符合標準的鏟斗不支援鏟斗生命週期組態。

營運	實作
放置時段通知	此作業會使用要求內文所含的通知組態XML來設定儲存區的通知。您應該瞭解下列實作詳細資料： • 支援簡單通知服務（SNS）主題作為目的地。StorageGRID不支援簡單佇列服務（SQS）或Amazon Lambda端點。 • 通知的目的地必須指定為StorageGRID 一個端點的URN。端點可以使用租戶管理程式或租戶管理API來建立。 端點必須存在、通知組態才能成功。如果端點不存在、則會傳回「400 Bad Request」錯誤、並顯示「InvalidArgument」代碼。 • 您無法設定下列事件類型的通知。這些事件類型*不支援*。 ◦ 'S 3：ReducedRedundancyLostObject' ◦ 「s 3：ObjectRestore：completed」 • 從Suse傳送的事件通知StorageGRID 會使用標準Json格式、但不包含某些金鑰、而且會針對其他金鑰使用特定值、如下列清單所示： • 事件來源 "gws:s3" • * awsRegion * 不含 • * X-amz-id-2* 不含 • * arn* 「urn:sgws:s3：：bucket_name」
資源桶政策	此作業會設定附加至庫位的原則。

營運	實作
放入資源桶複寫	此作業會使用StorageGRID 要求本文中提供的複寫組態XML、為儲存區設定「CloudMirror複寫」。對於CloudMirror複寫、您應該瞭解下列實作詳細資料： • 僅支援複寫組態的V1。StorageGRID這表示StorageGRID 、由於不支援使用「Filter」元素來執行規則、因此遵循V1慣例來刪除物件版本。如需詳細資訊、請參閱 "有關複寫組態的Amazon S3文件"。 • 儲存區複寫可在版本控制或未版本控制的儲存區上進行設定。 • 您可以在複寫組態XML的每個規則中指定不同的目的地儲存區。來源儲存區可複寫至多個目的地儲存區。 • 目的地貯體必須指定為StorageGRID 租戶管理程式或租戶管理API中指定的非功能性端點的URN。 複寫組態必須存在端點才能成功。如果端點不存在、則要求會以「400個不良要求」的形式失敗。錯誤訊息顯示：「無法儲存複寫原則。指定的端點URN不存在：*URN*.' • 您不需要在組態XML中指定「角色」。此值不供StorageGRID Some使用、如果提交、將會忽略此值。 • 如果您從組態XML中省略儲存類別、StorageGRID 則根據預設、功能不一定會使用「標準」儲存類別。 • 如果您從來源儲存區刪除物件、或是刪除來源儲存區本身、跨區域複寫行為如下： ◦ 如果您在複寫物件或儲存區之前先將其刪除、則不會複寫物件/儲存區、也不會通知您。 ◦ 如果您在複寫物件或儲存區之後將其刪除、StorageGRID 則針對跨區域複寫的V1、執行標準Amazon S3刪除行為。
置入庫位標記	此作業使用「標記」子資源來新增或更新一組桶的標記。新增庫位標記時、請注意下列限制： • 支援每個儲存區最多50個標籤的支援功能包括：StorageGRID • 與庫位關聯的標記必須具有唯一的標記金鑰。標籤金鑰長度最多可達128個UNICODE字元。 • 標記值長度最多可達256個UNICODE字元。 • 金鑰和值區分大小寫。
放入資源桶版本管理	此實作會使用「資料夾」子資源來設定現有儲存區的版本管理狀態。您可以使用下列其中一個值來設定版本設定狀態： • 已啟用：啟用儲存區中物件的版本管理。新增至儲存庫的所有物件都會收到唯一的版本ID。 • 暫停：停用儲存區中物件的版本設定。所有新增至儲存庫的物件都會收到版本ID「null」。

營運	實作
放置物件鎖定組態	此作業會設定或移除庫位預設保留模式和預設保留期間。 如果修改了預設保留期間、現有物件版本的保留截止日期將維持不變、且不會使用新的預設保留期間重新計算。 請參閱 放置物件鎖定組態 以取得詳細資訊。

相關資訊

一致性控管

取得時段上次存取時間要求

儲存庫和群組存取原則

在稽核記錄中追蹤S3作業

使用ILM管理物件

使用租戶帳戶

建立**S3**生命週期組態

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

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

什麼是生命週期組態

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

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

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

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

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

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

支援使用下列庫位作業來管理生命週期組態：StorageGRID

- 刪除時段生命週期
- 取得生命週期
- 放入鏟斗生命週期

建立生命週期組態

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

1. 規則1僅適用於前置詞「chategory1」/且「key2」值為「tag2」的物件。「Expiration」參數指定符合篩選條件的物件將於2020年8月22日午夜到期。
2. 規則2僅適用於符合前置詞「Category2」/的物件。「Expiration」（過期）參數指定符合篩選條件的物件在擷取後100天過期。

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

3. 規則3僅適用於符合前置詞「ategory3」/的物件。「Expiration」（過期）參數指定任何非目前版本的相符物件、將會在非目前版本50天後過期。

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

將生命週期組態套用至貯體

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

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

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

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

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

成功的回應會列出您剛套用的生命週期組態。

驗證目標是否適用庫位生命週期到期

您可以在發出「放置物件」、「標頭物件」或「取得物件」要求時、判斷生命週期組態中的到期規則是否適用於特定物件。如果套用規則、回應會包含一個「Expiration」（到期）參數、指出物件何時到期、以及符合哪些到期規則。

由於儲存區生命週期會覆寫ILM、因此顯示的「過期日」是物件刪除的實際日期。如需詳細資訊、請參閱 如何判斷物件保留。

例如、此「放置物件」要求是在2020年6月22日發出、並將物件放置在「testBucket」儲存區中。

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

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

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

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

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

成功回應包括物件的中繼資料、指出物件將在100天內過期、且符合規則2。

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

使用**S3**物件鎖定預設儲存區保留

如果某個儲存區已啟用S3物件鎖定、您可以指定套用至新增至儲存區之每個物件的預設保留模式和預設保留期間。

- 在建立儲存區期間、可針對儲存區啟用或停用S3物件鎖定。
- 如果已針對某個儲存區啟用S3物件鎖定、您可以設定該儲存區的預設保留。
- 預設保留組態指定：
  - 預設保留模式：StorageGRID 僅支援「法規遵循」模式。
  - 預設保留期間（以天或年為單位）。

取得物件鎖定組態

「Get Object Lock Configuration」（取得物件鎖定組態）要求可讓您判斷是否已針對某個儲存區啟用「物件鎖定」、如果已啟用、請查看是否有針對該儲存區設定的預設保留模式和保留期間。

將新的物件版本擷取至儲存區時、如果未指定「x-amz-object-lock mode」、則會套用預設保留模式。如果未指定「x-amz-object-lock-ret-截至 日期」、則預設保留期間會用於計算「截至日期」。

您必須具有S3：GetBucketObjectLockConfiguration權限、或是帳戶root、才能完成此作業。

申請範例

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

回應範例

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

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

放置物件鎖定組態

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

將新的物件版本擷取至儲存區時、如果未指定「x-amz-object-lock mode」、則會套用預設保留模式。如果未指定「x-amz-object-lock-ret-截至 日期」、則預設保留期間會用於計算「截至日期」。

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

您必須具有S3：PuttBucketObjectLockConfiguration權限或帳戶根權限、才能完成此作業。

必須在PUT要求中指定「Content-MD5」要求標頭。

申請範例

```
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>
```

在貯體上進行自訂作業

支援將自訂儲存區作業新增至S3 REST API、並專供系統使用。StorageGRID

下表列出StorageGRID 支援的自訂儲存區作業。

營運	說明	以取得更多資訊
取得庫位一致性	傳回套用至特定儲存庫的一致性層級。	取得時段一致性要求
實現庫位一致性	設定套用至特定儲存庫的一致性層級。	置入時段一致性要求
取得時段上次存取時間	傳回是否為特定儲存區啟用或停用上次存取時間更新。	取得時段上次存取時間要求
將資源桶放在最後存取時間	可讓您啟用或停用特定儲存區的上次存取時間更新。	將時段放入上次存取時間要求
刪除時段中繼資料通知組態	刪除與特定儲存區相關聯的中繼資料通知組態XML。	刪除時段中繼資料通知組態要求

營運	說明	以取得更多資訊
取得Bucket中繼資料通知組態	傳回與特定儲存區相關聯的中繼資料通知組態XML。	取得Bucket中繼資料通知組態要求
放置時段中繼資料通知組態	設定區段的中繼資料通知服務。	放置時段中繼資料通知組態要求
運用法規遵循設定來滿足需求	已過時且不受支援：您無法再建立啟用「符合性」的新儲存區。	已過時：將資源桶放在符合法規的設定中
取得符合需求的產品	已過時但受支援：傳回現有舊版相容儲存區目前有效的法規遵循設定。	已過時：Get Bucket Compliance要求
符合資源需求	已過時但受支援：可讓您修改現有舊版相容儲存區的法規遵循設定。	已過時：提出資源桶法規遵循要求

相關資訊

稽核記錄中追蹤的S3作業

物件上的作業

本節說明StorageGRID 此「物件」的「物件」功能如何執行S3 REST API作業。

下列條件適用於所有物件作業：

- StorageGRID 一致性控管 受物件上的所有作業支援、但下列項目除外：
  - 取得物件ACL
  - 「選項/」
  - 將物件保留為合法
  - 保留物件
  - 選取「物件內容」
- 衝突的用戶端要求（例如兩個寫入同一個金鑰的用戶端）會以「最新致勝」的方式解決。「最新致勝」評估的時間取決於StorageGRID VMware系統何時完成指定的要求、而非S3用戶端何時開始作業。
- 所有物件均由庫位擁有者擁有、包括匿名使用者或其他帳戶所建立的物件。StorageGRID
- 透過StorageGRID Swift擷取至整個系統的資料物件無法透過S3存取。

下表說明StorageGRID 了Ss哪些 物件是由S3 REST API物件執行。

營運	實作
刪除物件	不支援多因素驗證（MFA）和回應標頭「x-amz-MFA」。 處理刪除物件要求時StorageGRID 、功能區會嘗試立即從所有儲存位置移除物件的所有複本。如果成功、StorageGRID 則會立即將回應傳回給用戶端。如果無法在30秒內移除所有複本（例如、因為某個位置暫時無法使用）、StorageGRID 則將複本排入佇列以供移除、然後向用戶端指出成功。 版本管理 若要移除特定版本、申請者必須是貯體擁有者、並使用「版本ID」子資源。使用此子資源會永久刪除版本。如果「版本ID」對應於刪除標記、回應標頭「x-amz-delete-marker」會傳回設定為「true」。 • 如果在啟用版本的儲存區上刪除沒有「版本ID」子資源的物件、則會產生刪除標記。刪除標記的「版本ID」會使用「x-amz-version-id」回應標頭傳回、而「x-amz-delete-marker」回應標頭會傳回設定為「true」。 • 如果刪除的物件在版本暫停的儲存區上沒有'VrionId' SubResource、則會永久刪除已存在的'null '版本或'null '刪除標記、並產生新的'null ' 刪除標記。將"x-amz-delete-marker"回應標頭設為"true"。 附註：在某些情況下、物件可能會有多個刪除標記。
刪除多個物件	不支援多因素驗證（MFA）和回應標頭「x-amz-MFA」。 您可以在同一個要求訊息中刪除多個物件。
刪除物件標記	使用「標記」子資源從物件移除所有標記。以所有Amazon S3 REST API行為來實作。 版本管理 如果要求中未指定「vrionId」查詢參數、則該作業會刪除版本控制儲存區中物件最新版本的所有標記。如果物件的目前版本是刪除標記、則會傳回「MethodNotSupported」狀態、並將「x-amz-delete-marker」回應標頭設為「true」。
取得物件	取得物件
取得物件ACL	如果提供帳戶所需的存取認證資料、則作業會傳回正面回應、並傳回物件擁有者的ID、顯示名稱和權限、表示擁有者擁有物件的完整存取權。
取得物件合法持有	使用S3物件鎖定
取得物件保留	使用S3物件鎖定

營運	實作
取得物件標記	使用「標記」子資源來傳回物件的所有標記。以所有Amazon S3 REST API行為來實作 版本管理 如果要求中未指定「vrionId」查詢參數、則該作業會傳回版本控制儲存區中物件最新版本的所有標記。如果物件的目前版本是刪除標記、則會傳回「MethodNotSupported」狀態、並將「x-amz-delete-marker」回應標頭設為「true」。
標頭物件	標頭物件
POST物件還原	POST物件還原
放置物件	放置物件
放置物件-複製	放置物件-複製
將物件保留為合法	使用S3物件鎖定
保留物件	使用S3物件鎖定

營運	實作
放置物件標記	使用「標記」子資源將一組標記新增至現有物件。以所有Amazon S3 REST API行為來實作 物件標籤限制 您可以在上傳新物件時新增標記、也可以將標記新增至現有物件。每個物件最多可支援10個標記的支援功能。StorageGRID與物件相關聯的標記必須具有唯一的標記金鑰。標籤金鑰長度最多可達128個UNICODE字元、標籤值長度最多可達256個UNICODE字元。金鑰和值區分大小寫。 標記更新和擷取行為 當您使用「放置物件」標記來更新物件的標記時、StorageGRID 無法重新擷取物件。這表示不會使用相符ILM規則中指定的擷取行為選項。當ILM由正常背景ILM程序重新評估時、會對更新所觸發的物件放置位置進行任何變更。 這表示、如果ILM規則使用嚴格選項來擷取行為、則無法進行所需的物件放置（例如、因為新需要的位置無法使用）、則不會採取任何行動。更新後的物件會保留其目前的放置位置、直到能夠放置所需的位置為止。 解決衝突 衝突的用戶端要求（例如兩個寫入同一個金鑰的用戶端）會以「最新致勝」的方式解決。「最新致勝」評估的時間取決於StorageGRID VMware系統何時完成指定的要求、而非S3用戶端何時開始作業。 版本管理 如果要求中未指定「vrionId」查詢參數、則該作業會在版本控制的儲存區中、將標記新增至物件的最新版本。如果物件的目前版本是刪除標記、則會傳回「MethodNotSupported」狀態、並將「x-amz-delete-marker」回應標頭設為「true」。

相關資訊

在稽核記錄中追蹤S3作業

使用**S3**物件鎖定

如果StorageGRID 您的還原系統已啟用全域S3物件鎖定設定、您可以在啟用S3物件鎖定的情況下建立儲存區、然後針對每個儲存區指定預設保留期間、或針對您新增至該儲存區的每個物件版本、指定特定的保留截止日期和合法保留設定。

S3物件鎖定可讓您指定物件層級的設定、以防止物件在固定時間內或無限期刪除或覆寫。

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

啟用儲存區的**S3**物件鎖定

如果StorageGRID 您的整個S3物件鎖定設定已啟用、則您可以在建立每個儲存區時、選擇性地啟用S3物件鎖定。您可以使用下列任一種方法：

- 使用租戶管理程式建立桶。

  使用租戶帳戶

- 使用「X-amz-Bucket物件鎖定啟用」要求標頭的「置放貯體」要求來建立貯體。

  在貯體上作業

建立儲存區之後、您無法新增或停用S3物件鎖定。S3物件鎖定需要儲存區版本管理、這會在您建立儲存區時自動啟用。

啟用S3物件鎖定的儲存區可包含具有和不具有S3物件鎖定設定的物件組合。支援S3物件鎖定儲存區中物件的預設保留期間、並支援「放置物件鎖定組態」儲存區作業。StorageGRID「3：物件鎖定剩餘保留天數」原則條件金鑰可設定物件的最短和最長允許保留期間。

判斷是否已針對儲存區啟用**S3**物件鎖定

若要判斷是否已啟用S3物件鎖定、請使用 取得物件鎖定組態 申請。

使用**S3**物件鎖定設定建立物件

若要在將物件版本新增至已啟用S3物件鎖定的儲存區時、指定S3物件鎖定設定、請發出「放置物件」、「放置物件-複製」或啟動「多重組件上傳」要求。請使用下列要求標頭。

> 建立儲存區時、您必須啟用S3物件鎖定。建立儲存區之後、您無法新增或停用S3物件鎖定。

- 「X-amz-object-lock-mode」、必須符合法規（區分大小寫）。

  > 如果指定"x-amz-object-lock-mod"，則還必須指定"x-amz-object-lock-capse-截至 日期"。

- 《X-amz-object-lock-Retain直到日期》
  - 保留截止日期值必須採用「2020-08-10T21：46:00Z」格式。允許分數秒、但只保留3個小數位數（毫秒精度）。不允許使用其他ISO 8601格式。
  - 保留截止日期必須為未來日期。
- 「X-amz-object-lock-legal hold」

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

如果您使用上述任一要求標頭、請注意下列限制：

- 如果放置物件要求中有任何「x-amz-object-lock」*要求標頭、則需要「Content-md5」要求標頭。「內容-md5」不適用於「放置物件-複製」或「啟動多重成分上傳」。

- 如果儲存區未啟用S3物件鎖定、且出現「x-amz-object-lock-*」要求標頭、則會傳回400個不良要求（InvalidRequest）錯誤。
- 「放置物件」要求支援使用「x-amz-storage類別：dime_dure」來符合AWS行為。然而、當物件被擷取至啟用S3物件鎖定的儲存區時StorageGRID 、則會一律執行雙重認可擷取。
- 後續的Get或head物件版本回應將包括標頭「x-amz-object-lock mode」、「x-amz-object-lock -h比 得上日期」、以及「x-amz-object-lock合法保留」（若已設定）、以及要求傳送者是否擁有正確的「3：Get*」權限。
- 如果在保留截止日期之前或在合法持有之前、後續的刪除物件版本或刪除物件版本要求將會失敗。

更新**S3**物件鎖定設定

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

- 「將物件置於合法持有狀態」

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

- 「放置物件保留」
  - 模式值必須符合法規（區分大小寫）。
  - 保留截止日期值必須採用「2020-08-10T21：46:00Z」格式。允許分數秒、但只保留3個小數位數（毫秒精度）。不允許使用其他ISO 8601格式。
  - 如果物件版本有現有的截至日期保留、您只能增加。新的價值必須是未來的價值。

相關資訊

使用ILM管理物件

使用租戶帳戶

放置物件

放置物件-複製

啟動多部份上傳

物件版本管理

"Amazon簡易儲存服務使用者指南：使用S3物件鎖定"

使用**S3 Select**

支援的下列AWS S3 Select子句、資料類型和運算子StorageGRID SelectObjectContent命令。

> 不支援任何未列出的項目。

如需語法、請參閱 選取物件內容。如需S3 Select的詳細資訊、請參閱 "S3 Select的AWS文件"。

只有啟用S3 Select的租戶帳戶才能發出SelectObjectContent查詢。請參閱 使用S3 Select的考量與要求。

條款

- 選取清單
- from子句
- where子句
- 限制條款

資料類型

- 布爾
- 整數
- 字串
- 浮動
- 十進位、數字
- 時間戳記

運算子

邏輯運算子

- 和
- 不是
- 或

比較運算子

- <
- >
- &l;=
- >=
- =
- =
- <>
- ！=
- 兩者之間
- 在中

模式比對運算子

- 喜歡
- _
- %

單一運算子

- 為空值
- 不是空值

數學運算子

- +
- -
- *
- /
- %

支援AWS S3 Select運算子優先順序。StorageGRID

Aggregate函數

- 平均（）
- 計數（*）
- 最大（）
- 最小（）
- 總計（）

條件式函數

- 案例
- 合併
- NULLIF

轉換功能

- CAST（適用於支援的資料類型）

日期函數

- 日期新增
- 日期_差異
- 擷取
- 至字串
- 目標時間戳記
- UTCNOW

字串函數

- char_length、字元長度
- 降低
- 子字串
- 修剪
- 上

使用伺服器端加密

伺服器端加密可讓您保護閒置的物件資料。當資料寫入物件時、系統會加密資料、並在您存取物件時解密資料。StorageGRID

如果您想要使用伺服器端加密、您可以根據加密金鑰的管理方式、選擇兩個互不相容的選項之一：

- * SSE（使用StorageGRID管理金鑰的伺服器端加密）*：當您發出S3要求以儲存物件時StorageGRID 、用唯一的金鑰來加密物件。當您發出S3要求以擷取物件時StorageGRID 、則會使用儲存的金鑰來解密物件。
- * SSE-C（使用客戶提供的金鑰進行伺服器端加密）*：當您發出S3要求以儲存物件時、您會提供自己的加密金鑰。擷取物件時、您提供的加密金鑰與要求的一部分相同。如果兩個加密金鑰相符、則會解密物件並傳回物件資料。

  雖然此功能可管理所有物件加密與解密作業、但您必須管理所提供的加密金鑰。StorageGRID

  您提供的加密金鑰永遠不會儲存。如果您遺失加密金鑰、就會遺失對應的物件。

  如果物件是以SSE或SSE-C加密、則會忽略任何儲存區層級或網格層級的加密設定。

使用**SS**

若要使用StorageGRID 由支援此功能的唯一金鑰來加密物件、請使用下列要求標頭：

「X-amz-server端點加密」

下列物件作業可支援SSe要求標頭：

- 放置物件
- 放置物件-複製
- 啟動多部份上傳

使用**SSE-C**

若要使用您管理的唯一金鑰來加密物件、請使用三個要求標頭：

要求標頭	說明
「X-amz-server -side-ridencionse-customer-r演算法」	指定加密演算法。標頭值必須為「AES256」。
《x-amz-server-side-ridestion,《x-amz-server-side-ridencion,客戶密鑰》	指定將用於加密或解密物件的加密金鑰。金鑰的值必須是256位元、已編碼的base64。
《x-amz-server-side-ridestion,《x-amz-server-sidrencion,客戶密鑰-md5》	根據RFC 1321指定加密金鑰的md5摘要、以確保傳輸加密金鑰時不會發生錯誤。md5摘要的值必須是以64編碼的128位元。

下列物件作業可支援SSE-C要求標頭：

- 取得物件
- 標頭物件
- 放置物件
- 放置物件-複製
- 啟動多部份上傳
- 上傳零件
- 上傳零件-複製

使用伺服器端加密搭配客戶提供的金鑰（**SSE-C**）時的考量

使用SSE-C之前、請注意下列考量事項：

- 您必須使用https。

> 使用SSE-C時、不接受透過http提出的任何要求StorageGRID基於安全考量、您應該考慮使用http意外傳送的任何金鑰是否會遭到入侵。捨棄按鍵、然後視需要旋轉。

- 回應中的ETag不是物件資料的MD5。
- 您必須管理加密金鑰與物件之間的對應關係。不儲存加密金鑰。StorageGRID您必須負責追蹤為每個物件提供的加密金鑰。
- 如果您的儲存區已啟用版本管理功能、則每個物件版本都應該擁有自己的加密金鑰。您負責追蹤每個物件版本所使用的加密金鑰。
- 由於您管理用戶端的加密金鑰、因此也必須管理用戶端上的任何其他安全防護措施、例如金鑰輪替。

> 您提供的加密金鑰永遠不會儲存。如果您遺失加密金鑰、就會遺失對應的物件。

- 如果已針對儲存區設定CloudMirror複寫、您就無法擷取SSE-C物件。擷取作業將會失敗。

相關資訊

取得物件

標頭物件

放置物件

放置物件-複製

啟動多部份上傳

上傳零件

上傳零件-複製

"Amazon S3開發人員指南：使用客戶提供的加密金鑰（SSE-C）、使用伺服器端加密來保護資料"

取得物件

您可以使用S3取得物件要求、從S3儲存區擷取物件。

取得物件和多個部分物件

您可以使用「partNumber」要求參數來擷取多個部分或分段物件的特定部分。「x-amz-mp-零 件數」回應元素會指出物件有多少個部分。

您可以將分段/多部份物件和非分段/非多部份物件的「partNumber」設為1、但是「x-amz-mp-part-count」回應元素只會針對分段或多部份物件傳回。

使用客戶提供的加密金鑰（**SSE-C**）要求伺服器端加密標頭

如果物件是以您提供的唯一金鑰加密、請使用所有三個標頭。

- 「X-amz-server端加密客戶演算法」：指定「AES256」。
- 「X-amz-server端加密客戶金鑰」：指定物件的加密金鑰。
- 「X-amz-server端加密- 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儲存。如果您遺失加密金鑰、就會遺失對應的物件。在使用客戶提供的金鑰來保護物件資料之前、請先檢閱「使用伺服器端加密」中的考量事項。

使用者中繼資料中的**UTF-8**字元

在使用者定義的中繼資料中、無法剖析或解譯轉義的utf-8字元。StorageGRID如果金鑰名稱或值包含不可列印的字元、則在使用者定義的中繼資料中、取得內含轉義式utf-8字元的物件要求時、不會傳回「x-amz-missing中繼資料」標頭。

不支援的要求標頭

不支援下列要求標頭、並傳回「XNotImplemed」：

- 「X-amz-website - redirect-location」

版本管理

如果未指定「版本ID」子資源、則作業會擷取版本控制儲存區中的物件最新版本。如果物件的目前版本是刪除標記、則會傳回「找不到」狀態、並將「x-amz-delete-marker'回應標頭設為「true」。

取得雲端儲存池物件的行為

如果物件已儲存在Cloud Storage Pool中（請參閱管理物件的指示、並進行資訊生命週期管理）、則Get物件要求的行為取決於物件的狀態。如需詳細資訊、請參閱「標頭物件」。

如果物件儲存在雲端儲存資源池中、而且網格上也有一個或多個物件複本、則「Get Object（取得物件）」要求會先嘗試從網格擷取資料、然後再從雲端儲存資源池擷取資料。

物件狀態	**Get**物件的行為
物件擷取到StorageGRID 不經ILM評估、或儲存在傳統儲存資源池中的物件、或使用銷毀編碼	「200 OK」 系統會擷取物件複本。
Cloud Storage Pool中的物件、但尚未轉換為無法擷取的狀態	「200 OK」 系統會擷取物件複本。
物件移轉至無法擷取的狀態	"403 Forbidbid"、"InvalidObjectState" 使用POST物件還原要求、將物件還原至可擷取的狀態。
正在從無法擷取的狀態還原的物件	"403 Forbidbid"、"InvalidObjectState" 等待POST物件還原要求完成。
物件已完全還原至雲端儲存資源池	「200 OK」 系統會擷取物件複本。

雲端儲存資源池中的多部份或分段物件

如果您上傳了多個部分的物件、或StorageGRID 是將一個大型物件分割成多個區段、StorageGRID 則透過取樣物件的一部分或區段、決定該物件是否可在Cloud Storage Pool中使用。在某些情況下、當物件的某些部分已轉換為無法擷取的狀態、或物件的某些部分尚未還原時、「Get物件」要求可能會錯誤傳回「200 OK」。

在這些情況下：

- Get Object要求可能會傳回部分資料、但會在傳輸中途停止。
- 隨後的Get Object要求可能會傳回「403 Forbidbid禁 用」。

相關資訊

使用伺服器端加密

使用ILM管理物件

POST物件還原

在稽核記錄中追蹤S3作業

標頭物件

您可以使用S3頭物件要求從物件擷取中繼資料、而不傳回物件本身。如果物件儲存在Cloud Storage Pool中、您可以使用「標頭物件」來判斷物件的轉換狀態。

標頭物件和多個部分物件

您可以使用「partNumber」要求參數來擷取多個部分或分段物件特定部分的中繼資料。「x-amz-mp-零 件數」回應元素會指出物件有多少個部分。

您可以將分段/多部份物件和非分段/非多部份物件的「partNumber」設為1、但是「x-amz-mp-part-count」回應元素只會針對分段或多部份物件傳回。

使用客戶提供的加密金鑰（**SSE-C**）要求伺服器端加密標頭

如果物件使用您提供的唯一金鑰加密、請使用這三個標頭。

- 「X-amz-server端加密客戶演算法」：指定「AES256」。
- 「X-amz-server端加密客戶金鑰」：指定物件的加密金鑰。
- 「X-amz-server端加密- 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儲存。如果您遺失加密金鑰、就會遺失對應的物件。在使用客戶提供的金鑰來保護物件資料之前、請先檢閱「使用伺服器端加密」中的考量事項。

使用者中繼資料中的**UTF-8**字元

在使用者定義的中繼資料中、無法剖析或解譯轉義的utf-8字元。StorageGRID如果金鑰名稱或值包含不可列印的字元、則使用者定義中繼資料中轉義的UTF-8字元物件的標頭要求不會傳回「x-amz-missing中繼資料」標頭。

不支援的要求標頭

不支援下列要求標頭、並傳回「XNotImplemed」：

- 「X-amz-website - redirect-location」

Cloud Storage Pool物件的回應標頭

如果物件儲存在Cloud Storage Pool中（請參閱使用資訊生命週期管理來管理物件的指示）、則會傳回下列回應標頭：

- 《X-amz-storage等級：Glacier》（《X-amz-storage等級：Glacier》）
- 「X-amz-restore」

回應標頭會提供物件移至雲端儲存集區時的狀態資訊、並選擇性地移轉至無法擷取的狀態、然後還原。

物件狀態	回應標頭物件
物件擷取到StorageGRID 不經ILM評估、或儲存在傳統儲存資源池中的物件、或使用銷毀編碼	「200 OK」（未傳回特殊回應標頭）。
Cloud Storage Pool中的物件、但尚未轉換為無法擷取的狀態	「200 OK」 《X-amz-storage等級：Glacier》（《X-amz-storage等級：Glacier》） 「X-amz-restore：展中要求=「假」、過期日期=「週六、7月23日2030：00：00 GMT" 在物件轉換為無法擷取的狀態之前、「過期日期」的值會設定為未來的某個時間。確切的轉換時間不受StorageGRID 此功能的控制。
物件已轉換為無法擷取的狀態、但網格上至少也有一個複本	「200 OK」 《X-amz-storage等級：Glacier》（《X-amz-storage等級：Glacier》） 「X-amz-restore：展中要求=「假」、過期日期=「週六、7月23日2030：00：00 GMT" 「過期日」的值會設定為未來的某段時間。 附註：如果網格上的複本無法使用（例如、儲存節點當機）、您必須發出物件後還原要求、以便從雲端儲存池還原複本、才能成功擷取物件。
物件移轉至無法擷取的狀態、而且網格上不存在複本	「200 OK」 《X-amz-storage等級：Glacier》（《X-amz-storage等級：Glacier》）
正在從無法擷取的狀態還原的物件	「200 OK」 《X-amz-storage等級：Glacier》（《X-amz-storage等級：Glacier》） 「x-amz-restore：持續要求=「true」

物件狀態	回應標頭物件
物件已完全還原至雲端儲存資源池	「200 OK」 《X-amz-storage等級：Glacier》（《X-amz-storage等級：Glacier》） 「X-amz-restore：展中要求=「假」、過期日期=「2018年7月23日星期六00：00：00 GMT」 「過期日」表示Cloud Storage Pool中的物件何時會恢復為無法擷取的狀態。

Cloud Storage Pool中的多部份或分段物件

如果您上傳了多個部分的物件、或StorageGRID 是將一個大型物件分割成多個區段、StorageGRID 則透過取樣物件的一部分或區段、決定該物件是否可在Cloud Storage Pool中使用。在某些情況下、當物件的某些部分已轉換為無法擷取的狀態、或物件的某些部分尚未還原時、物件要求可能會錯誤地傳回「x-amz-restore: onale-request ="false"（x-amz-restore:持續要求=「假」）。

版本管理

如果未指定「版本ID」子資源、則作業會擷取版本控制儲存區中的物件最新版本。如果物件的目前版本是刪除標記、則會傳回「找不到」狀態、並將「x-amz-delete-marker'回應標頭設為「true」。

相關資訊

使用伺服器端加密

使用ILM管理物件

POST物件還原

在稽核記錄中追蹤S3作業

POST物件還原

您可以使用S3 POST物件還原要求來還原儲存在雲端儲存池中的物件。

支援的要求類型

僅支援POST物件還原要求以還原物件。StorageGRID它不支援「選擇」還原類型。選取「要求傳回XNotImplemed」。

版本管理

或者、指定「版本ID」來還原版本控制儲存區中物件的特定版本。如果您未指定「版本ID」、則會還原物件的最新版本

在**Cloud Storage Pool**物件上進行物件後還原的行為

如果物件儲存在Cloud Storage Pool中（請參閱使用資訊生命週期管理來管理物件的指示）、則根據物件的狀

態、POST物件還原要求會出現下列行為。如需詳細資訊、請參閱「標頭物件」。

如果物件儲存在雲端儲存資源池中、而且網格上也存在物件的一或多個複本、就不需要發出物件後還原要求來還原物件。相反地、您可以使用「取得物件」要求、直接擷取本機複本。

物件狀態	**POST**物件還原的行為
物件擷取至StorageGRID 不受ILM評估、或物件不在雲端儲存資源池中	"403 Forbidbid"、"InvalidObjectState"
Cloud Storage Pool中的物件、但尚未轉換為無法擷取的狀態	200 OK（正常）沒有任何變更。 附註：在物件移轉至無法擷取的狀態之前、您無法變更其「過期日」。
物件移轉至無法擷取的狀態	「可接受的時間為202-20…」會將物件的可擷取複本還原至Cloud Storage Pool、直到要求本文指定的天數。在此期間結束時、物件會返回無法擷取的狀態。 您也可以選擇使用「Tier」（層級）要求元素來判斷還原工作完成所需的時間（「Expedited」（加速）、「tandard」（標準）或「Bulk」（大量））。如果您未指定「Tier」（層級）、則會使用「標準」層級。 注意：如果某個物件已轉換為S3 Glacier Deep歸檔、或是雲端儲存資源池使用Azure Blob儲存設備、則無法使用「Expedited」層級還原。傳回下列錯誤訊息：「403 Forbidbidbided」、「InvalidTier」：「此儲存類別不支援擷取選項」。
正在從無法擷取的狀態還原的物件	《409衝突》、《恢復性進展》
物件已完全還原至雲端儲存資源池	「200 OK」 *附註：*如果某個物件已還原至可擷取的狀態、您可以使用「日期」的新值重新發出POST物件還原要求、以變更其「過期日期」。還原日期會根據申請時間而更新。

相關資訊

使用ILM管理物件

標頭物件

在稽核記錄中追蹤S3作業

放置物件

您可以使用S3放置物件要求、將物件新增至儲存區。

解決衝突

衝突的用戶端要求（例如兩個寫入同一個金鑰的用戶端）會以「最新致勝」的方式解決。「最新致勝」評估的時間取決於StorageGRID 何時由VMware系統完成指定的要求、而非S3用戶端開始作業的時間。

物件大小

單一放置物件作業的最大_Recommended大小為5 GiB（5、368、709、120位元組）。如果您的物件大於5 GiB、請改用多部份上傳。

> 在S2011.6中StorageGRID 、單一放置物件作業的最大_supported大小為5 TiB（5、497、558、13880位元組）。但是、如果您嘗試上傳超過5 GiB的物件、則會觸發* S3「Pure Object size too large （將物件大小設為太大）」警示。

使用者中繼資料大小

Amazon S3會將每個PUT要求標頭內使用者定義的中繼資料大小限制為2 KB。支援範圍將使用者中繼資料限制為24 KiB。StorageGRID使用者定義的中繼資料大小是以每個金鑰和值的utf-8編碼方式、計算出位元組數的總和。

使用者中繼資料中的**UTF-8**字元

如果要求在使用者定義的中繼資料金鑰名稱或值中包含（未轉義）utf-8值、StorageGRID 則無法定義任何不正常的行為。

不剖析或解譯使用者定義之中繼資料的金鑰名稱或值中包含的轉義式utf-8字元。StorageGRID轉義的UTF-8字元會視為Ascii字元：

- 如果使用者定義的中繼資料包含轉義的UTF-8字元、則放置、放置物件複製、取得和標頭要求都會成功。
- 如果關鍵字名稱或值的解譯值包含不可列印的字元、則不傳回「x-amz-misse-meta」標頭。StorageGRID

物件標籤限制

您可以在上傳新物件時新增標記、也可以將標記新增至現有物件。每個物件最多可支援10個標記的支援功能。StorageGRID與物件相關聯的標記必須具有唯一的標記金鑰。標籤金鑰長度最多可達128個UNICODE字元、標籤值長度最多可達256個UNICODE字元。金鑰和值區分大小寫。

物件擁有權

在功能區中StorageGRID 、所有物件均歸庫位擁有者帳戶所有、包括非擁有者帳戶或匿名使用者所建立的物件。

支援的要求標頭

支援下列要求標頭：

- 「快取控制」
- 「內容處理」
- 「內容編碼」

當您為「Content-Encoding」指定「AWS/chunked」時、「儲存設備GRID」不會驗證下列項目：

- 不驗證區塊資料的「區塊簽章」StorageGRID 。
- 不驗證您針對物件提供的「X-amz-解碼內容長度」值。StorageGRID

- 《內容-語言》
- 《內容長度》
- 《Content-MD5》
- 「內容類型」
- 《過期》
- 「傳輸編碼」

如果也使用「AWS/chunked」有效負載簽署、則支援chunked傳輸編碼。

- 「x-amz-meta-」、接著是包含使用者定義中繼資料的名稱值配對。

為使用者定義的中繼資料指定名稱值配對時、請使用以下一般格式：

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

如果您要使用*使用者定義的建立時間*選項做為ILM規則的參考時間、則必須使用「建立時間」做為建立物件時記錄的中繼資料名稱。例如：

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

自70年1月1日起、「創造時間」的值會以秒計算。

> ILM規則無法同時使用*使用者定義的建立時間*作為參考時間、以及用於擷取行為的平衡或嚴格選項。建立ILM規則時會傳回錯誤。

- 「X-amz-標記」
- S3物件鎖定要求標頭
  - 「X-amz-object-lock-mode」
  - 《X-amz-object-lock-Retain直到日期》
  - 「X-amz-object-lock-legal hold」

  如果提出的要求沒有這些標頭、則會使用儲存庫預設保留設定來計算物件版本的保留日期。

使用S3物件鎖定

- SSe要求標頭：
  - 「X-amz-server端點加密」

- 「X-amz-server端加密- customer-key-md5」
- 「X-amz-server端加密客戶金鑰」
- 「X-amz-server端加密- customer-演算 法」

  請參閱 [要求伺服器端加密的標頭]

不支援的要求標頭

不支援下列要求標頭：

- 不支援「x-amz-acl」要求標頭。
- 不支援「x-amz-website - redirect-location」要求標頭、並傳回「XNotImplemed」。

儲存類別選項

支援「x-amz-storage -Class」要求標頭。提交給「x-amz-Storage-Class」的值、會影響StorageGRID 到在擷取期間、如何保護物件資料、以及StorageGRID 不需要將物件的持續複本儲存在包含在ILM系統中的數量。

如果符合擷取物件的ILM規則使用擷取行為的嚴格選項、則「x-amz-Storage-Class」標頭不會有任何影響。

下列值可用於「x-amz-storage類別」：

- 「標準」（預設）
  - 雙重提交：如果ILM規則指定「內嵌行為」的「雙重提交」選項、則只要物件擷取到另一個物件複本、就會建立該物件的第二個複本、並將其分散到不同的儲存節點（雙重提交）。評估ILM時、StorageGRID會判斷這些初始過渡複本是否符合規則中的放置指示。如果沒有、可能需要在不同位置建立新的物件複本、而且可能需要刪除初始的過渡複本。
  - 平衡：如果ILM規則指定平衡選項、StorageGRID 且無法立即製作規則中指定的所有複本、StorageGRID 則在不同的儲存節點上製作兩份臨時複本。

    如果能夠立即建立ILM規則（同步放置）中指定的所有物件複本、「x-amz-Storage-Class」標頭就不會有任何影響。StorageGRID
- "educed_deete"
  - 雙重提交：如果ILM規則指定擷取行為的雙重提交選項、StorageGRID 則會在擷取物件時建立單一的過渡複本（單一提交）。
  - 平衡：如果ILM規則指定平衡選項、StorageGRID 則僅當系統無法立即製作規則中指定的所有複本時、才能製作單一的過渡複本。如果能夠執行同步放置、則此標頭不會有任何影響。StorageGRID當符合物件的ILM規則建立單一複寫複本時、最適合使用「已儲存的備援」選項。在這種情況下、使用「reduced_dere通用」可免除每次擷取作業不必要地建立和刪除額外的物件複本。

  在其他情況下、不建議使用「已儲存的備援」選項。「已導入的備援」會增加擷取期間物件資料遺失的風險。例如、如果單一複本一開始儲存在無法進行ILM評估的儲存節點上、則可能會遺失資料。

注意：在任何時間段內只有一個複寫複本、會使資料面臨永久遺失的風險。如果只有一個物件複寫複本存在、則當儲存節點故障或發生重大錯誤時、該物件就會遺失。在升級等維護程序期間、您也會暫時失去物件的存取權。

指定「已儲存的備援」僅會影響第一次擷取物件時所建立的複本數量。它不會影響使用中ILM原則評估物件時所

製作的物件複本數量、也不會導致資料儲存在StorageGRID 較低層級的資料冗餘環境中。

附註：如果您在啟用S3物件鎖定的情況下、將物件放入儲存區、則會忽略「已傳入的備援」選項。如果您將物件放入符合舊規範的儲存區、則「educed_de隊」選項會傳回錯誤。執行「雙重承諾」的程序時、務必確保符合法規遵循要求。StorageGRID

要求伺服器端加密的標頭

您可以使用下列要求標頭、以伺服器端加密來加密物件。「SSE」和「SSE-C」選項互不相關。

- * SSE-*：如果您想使用StorageGRID 由支援的唯一金鑰來加密物件、請使用下列標頭。
  - 「X-amz-server端點加密」
- * SSE-C*：如果您想使用您提供及管理的唯一金鑰來加密物件、請使用這三個標頭。
  - 「X-amz-server端加密客戶演算法」：指定「AES256」。
  - 「X-amz-server端加密客戶金鑰」：指定新物件的加密金鑰。
  - 「X-amz-server端加密- customer-key-md5」：指定新物件加密金鑰的md5摘要。

*注意：*您提供的加密金鑰永遠不會儲存。如果您遺失加密金鑰、就會遺失對應的物件。在使用客戶提供的金鑰來保護物件資料之前、請先檢閱「使用伺服器端加密」中的考量事項。

*附註：*如果物件是以SSE或SSE-C加密、則會忽略任何儲存區層級或網格層級的加密設定。

版本管理

如果已針對儲存區啟用版本管理、系統會針對儲存的物件版本自動產生唯一的「版本ID」。此「版本ID」也會在回應中使用「x-amz-version -id」回應標頭傳回。

如果版本控制暫停、則物件版本會以null「VrionId」儲存、如果null版本已經存在、則會覆寫該版本。

相關資訊

使用ILM管理物件

在貯體上作業

在稽核記錄中追蹤S3作業

使用伺服器端加密

如何設定用戶端連線

放置物件-複製

您可以使用「S3放置物件-複製」要求來建立S3中已儲存物件的複本。「放置物件」-「複製」作業與執行「取得」和「放置」相同。

解決衝突

衝突的用戶端要求（例如兩個寫入同一個金鑰的用戶端）會以「最新致勝」的方式解決。「最新致勝」評估的時間取決於StorageGRID 何時由VMware系統完成指定的要求、而非S3用戶端開始作業的時間。

物件大小

單一放置物件作業的最大_Recommended大小為5 GiB（5、368、709、120位元組）。如果您的物件大於5 GiB、請改用多部份上傳。

> 在S2011.6中StorageGRID 、單一放置物件作業的最大_supported大小為5 TiB（5、497、558、13880位元組）。但是、如果您嘗試上傳超過5 GiB的物件、則會觸發* S3「Pure Object size too large （將物件大小設為太大）」警示。

使用者中繼資料中的**UTF-8**字元

如果要求在使用者定義的中繼資料金鑰名稱或值中包含（未轉義）utf-8值、StorageGRID 則無法定義任何不正常的行為。

不剖析或解譯使用者定義之中繼資料的金鑰名稱或值中包含的轉義式utf-8字元。StorageGRID轉義的UTF-8字元會視為Ascii字元：

- 如果使用者定義的中繼資料包含轉義的utf-8字元、則要求會成功。
- 如果關鍵字名稱或值的解譯值包含不可列印的字元、則不傳回「x-amz-misse-meta」標頭。StorageGRID

支援的要求標頭

支援下列要求標頭：

- 「內容類型」
- 《X-amz-copy-source-》
- 「x-amz-copy-source-if-match」
- 「x-amz-copy-source-if-none-MATCH」
- 「x-amz-copy-source-if-modif-since」
- 《X-amz-copy-source-if-modif-s自》
- 「x-amz-meta-」、接著是包含使用者定義中繼資料的名稱值配對
- 「x-amz-meta中繼資料指令」：預設值為「copy」、可讓您複製物件及相關的中繼資料。

  您可以指定「放置」、以在複製物件時覆寫現有的中繼資料、或更新物件中繼資料。

- 「X-amz-storage等級」
- 「x-amz-tagging指令」：預設值為「copy」、可讓您複製物件和所有標記。

  您可以指定「放置」、以在複製物件時覆寫現有的標記、或是更新標記。

- S3物件鎖定要求標頭：
  - 「X-amz-object-lock-mode」
  - 《X-amz-object-lock-Retain直到日期》
  - 「X-amz-object-lock-legal hold」

如果提出的要求沒有這些標頭、則會使用儲存庫預設保留設定來計算物件版本的保留日期。

使用S3物件鎖定

- SSe要求標頭：
  - 「X-amz-copy-sourceSection-server-s側 邊邊邊邊邊邊邊邊邊邊邊邊邊邊邊邊邊邊邊邊邊邊邊邊邊邊邊邊邊邊邊邊邊邊邊邊邊邊邊
  - 「X-amz-copy-sourcez-server端加密客戶金鑰」
  - 「X-amz-copy-sourceSe-ser-side -ence-customer-key-md5」
  - 「X-amz-server端點加密」
  - 「X-amz-server端加密- customer-key-md5」
  - 「X-amz-server端加密客戶金鑰」
  - 「X-amz-server端加密- customer-演算 法」

  請參閱 [要求伺服器端加密的標頭]

不支援的要求標頭

不支援下列要求標頭：

- 「快取控制」
- 「內容處理」
- 「內容編碼」
- 《內容-語言》
- 《過期》
- 「X-amz-website - redirect-location」

儲存類別選項

支援「x-amz-Storage-Class」要求標頭、如果StorageGRID 相符的ILM規則指定「雙重認可」或「平衡」的擷取行為、則會影響到所建立的物件複本數量。

- 《標準》

  （預設）當ILM規則使用雙重提交選項、或平衡選項回到建立臨時複本時、指定雙重提交擷取作業。

- "educed_deete"

  當ILM規則使用雙重提交選項、或平衡選項回到建立過渡複本時、指定單一提交擷取作業。

> 如果在啟用S3物件鎖定的情況下、將物件放入儲存區、則會忽略「已儲存的備援」選項。如果您將物件放入符合舊規範的儲存區、則「educed_de隊」選項會傳回錯誤。執行「雙重承諾」的程序時、務必確保符合法規遵循要求。StorageGRID

在「放置物件-複製」中使用**x-amz-copy-**來源

如果在「x-amz-copy-SOUR來源」標頭中指定的來源儲存區和金鑰與目的地儲存區和金鑰不同、則會將來源物件資料的複本寫入目的地。

如果來源和目的地相符、且「x-amz-madmad瞭-指令」標頭指定為「放置」、則會使用要求中提供的中繼資料值來更新物件的中繼資料。在這種情況StorageGRID 下、無法重新擷取物件。這有兩個重要後果：

- 您無法使用「放置物件」-「複製」來加密現有物件、或是變更現有物件的加密。如果您提供「x-amz-server端加密」標頭或「x-amz-server端加密- customer-amer-演算法」標頭、StorageGRID 則無法接受要求、並傳回「XNotImplemed」。
- 不會使用相符ILM規則中指定的擷取行為選項。當ILM由正常背景ILM程序重新評估時、會對更新所觸發的物件放置位置進行任何變更。

  這表示、如果ILM規則使用嚴格選項來擷取行為、則無法進行所需的物件放置（例如、因為新需要的位置無法使用）、則不會採取任何行動。更新後的物件會保留其目前的放置位置、直到能夠放置所需的位置為止。

要求伺服器端加密的標頭

如果您使用伺服器端加密、所提供的要求標頭取決於來源物件是否加密、以及您是否打算加密目標物件。

- 如果來源物件是使用客戶提供的金鑰（SSE-C）加密、您必須在「放置物件-複製」要求中包含下列三個標頭、以便解密物件、然後複製：
  - 《x-amz-copy-sourceese-sider-se-ridionese-customer-alr演算 法》指定「AES256」。
  - 「x-amz-copy-sourcez-server端加密客戶金鑰」指定您在建立來源物件時所提供的加密金鑰。
  - 「x-amz-copy-sourceze-server端加密-客戶金鑰-md5」：指定您在建立來源物件時所提供的md5摘要。
- 如果您要使用您提供及管理的唯一金鑰來加密目標物件（複本）、請包含下列三個標頭：
  - 「X-amz-server端加密客戶演算法」：指定「AES256」。
  - 「X-amz-server端加密客戶金鑰」：為目標物件指定新的加密金鑰。
  - 「X-amz-server端加密- customer-key-md5」：指定新加密金鑰的md5摘要。

*注意：*您提供的加密金鑰永遠不會儲存。如果您遺失加密金鑰、就會遺失對應的物件。在使用客戶提供的金鑰來保護物件資料之前、請先檢閱「使用伺服器端加密」中的考量事項。

- 如果您想要使用StorageGRID 由支援對象（複本）的獨特金鑰來加密目標物件（複本）、請在「放置物件-複製」要求中加入此標頭：
  - 「X-amz-server端點加密」

*注意：*無法更新物件的「伺服器端加密」值。相反地、請使用「x-amz-madmite-指令」（「放置」）、使用新的「伺服器端加密」值來製作複本。

版本管理

如果來源儲存區已有版本、您可以使用「x-amz-copy-source-」標頭來複製物件的最新版本。若要複製物件的特定版本、您必須使用「版本ID」子資源明確指定要複製的版本。如果目標儲存區版本已有版本、則產生的版本會傳回「x-amz-verse-id」回應標頭中。如果暫停目標儲存區的版本設定、則「x-amz-version-id」會傳回「null」值。

相關資訊

使用ILM管理物件

使用伺服器端加密

在稽核記錄中追蹤S3作業

放置物件

選取物件內容

您可以使用S3 SelectObjectContent要求、根據簡單的SQL陳述來篩選S3物件的內容。

如需詳細資訊、請參閱 "SelectObjectContent的AWS文件"。

您需要的產品

- 租戶帳戶具有S3 Select權限。
- 您對要查詢的物件具有「3：GetObject」權限。
- 您要查詢的物件為CSV格式、或是含有CSV格式檔案的GZIP或bzip2壓縮檔。
- SQL運算式的最大長度為256 KB。
- 輸入或結果中的任何記錄最大長度為1個mib。

要求語法範例

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

SQL查詢範例

此查詢會取得州名、2010年人口、2015年估計人口、以及美國統計資料的變更百分比。檔案中非狀態的記錄會被忽略。

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

要查詢的檔案前幾行「之前」、例如「之前」、「之後」、「之後」、「現在」、

```
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

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

輸出檔案的前幾行「變更」。csv"如下所示：

```
Alabama,4779736,4854803,1.570526070895965802295356898372629785 4
Alaska,710231,738430,3.970398363349389142405780654463125377 5
Arizona,6392017,6832810,6.895992297892824753125656580700583243 1
Arkansas,2915918,2979732,2.188470320495981025529524492801237894 9
California,37253956,38904296,4.429972483996062055798852610444914897 1
Colorado,5029196,5454328,8.453279609703022113276157859029554624 6
```

多部份上傳作業

本節說明StorageGRID 此功能如何支援多部份上傳作業。

下列條件與附註適用於所有多重部分上傳作業：

- 您不應超過1、000次同時將多個部分上傳至單一儲存庫、因為針對該儲存庫列出多個部分上傳查詢的結果可能會傳回不完整的結果。
- 針對多個零件執行AWS大小限制。StorageGRIDS3用戶端必須遵循下列準則：
  - 多部份上傳的每個部分必須介於5個mib（5、242,880位元組）和5 GiB（5、368,709,120位元組）之間。
  - 最後一部分可小於5個mib（5、242,880位元組）。
  - 一般而言、零件尺寸應盡量大。例如、對於100 GiB物件使用5 GiB的零件大小。由於每個零件都被視為獨特的物件、因此使用大尺寸的零件可減少StorageGRID 元資料負荷。
  - 對於小於5 GiB的物件、請考慮改用非多部份上傳。
- 如果ILM規則使用嚴格或平衡的擷取行為、則會針對多部分物件的每個部分進行ILM評估、並在多部分上傳完成時、針對整個物件進行ILM評估。您應該瞭解這會如何影響物件和零件放置：
  - 如果在S3多部份上傳進行期間ILM發生變更、則當多部份上傳完成物件的部分時、可能無法符合目前的ILM需求。未正確放置的任何零件都會排入ILM重新評估佇列、稍後會移至正確位置。
  - 評估零件的ILM時StorageGRID 、會根據零件大小而非物件大小來篩選。這表示物件的部分可儲存在不符合整個物件ILM需求的位置。例如、如果規則指定所有10 GB或更大的物件都儲存在DC1、而所有較小的物件則儲存在DC2、則在10部分多部分上傳的每1 GB擷取部分、都會儲存在DC2。當針對整個物件評估ILM時、物件的所有部分都會移至DC1。
- 所有的多部份上傳作業都支援StorageGRID 不一致的控管功能。
- 視需要、您可以使用伺服器端加密來上傳多個部分。若要使用SSe（使用StorageGRID管理金鑰的伺服器端加密）、您只能在「初始化多重部分上傳」要求中加入「x-amz-server端加密」要求標頭。若要使用SSE-C（使用客戶提供的金鑰進行伺服器端加密）、您可以在「初始化多部份上傳」要求和後續每個「上傳零件」要求中、指定相同的三個加密金鑰要求標頭。

營運	實作
列出多個部分上傳	請參閱 列出多個部分上傳
啟動多部份上傳	請參閱 啟動多部份上傳
上傳零件	請參閱 上傳零件

營運	實作
上傳零件-複製	請參閱 上傳零件-複製
完成多部份上傳	請參閱 完成多部份上傳
中止多部份上傳	以所有Amazon S3 REST API行為來實作
列出零件	以所有Amazon S3 REST API行為來實作

相關資訊

- 一致性控管
- 使用伺服器端加密

列出多個部分上傳

「列出多部份上傳」作業會列出某個儲存庫正在進行的多部份上傳。

支援下列要求參數：

- 「encoding-type」
- 「上傳影片」
- 「關鍵標記」
- 前置詞
- 「上傳ID標記」

不支援「delimiter」要求參數。

版本管理

多部分上傳包含不同的作業、可用於初始化上傳、列出上傳內容、上傳零件、組裝上傳的零件、以及完成上傳。當執行完整的「多部份上傳」作業時、即為建立物件的時間點（若適用、則為版本控制）。

啟動多部份上傳

「初始化多部份上傳」作業會針對物件啟動多部份上傳、並傳回上傳ID。

支援「x-amz-storage -Class」要求標頭。提交給「x-amz-Storage-Class」的值、會影響StorageGRID 到在擷取期間、如何保護物件資料、以及StorageGRID 不需要將物件的持續複本儲存在包含在ILM系統中的數量。

如果符合擷取物件的ILM規則使用擷取行為的嚴格選項、則「x-amz-Storage-Class」標頭不會有任何影響。

下列值可用於「x-amz-storage類別」：

- 「標準」（預設）
  - 雙重提交：如果ILM規則指定「內嵌行為」的「雙重提交」選項、則只要物件擷取到另一個物件複本、就

會建立該物件的第二個複本、並將其分散到不同的儲存節點（雙重提交）。評估ILM時、StorageGRID會判斷這些初始過渡複本是否符合規則中的放置指示。如果沒有、可能需要在不同位置建立新的物件複本、而且可能需要刪除初始的過渡複本。

- 平衡：如果ILM規則指定平衡選項、StorageGRID 且無法立即製作規則中指定的所有複本、StorageGRID 則在不同的儲存節點上製作兩份臨時複本。

  如果能夠立即建立ILM規則（同步放置）中指定的所有物件複本、「x-amz-Storage-Class」標頭就不會有任何影響。StorageGRID

- "educed_deete"

  - 雙重提交：如果ILM規則指定擷取行為的雙重提交選項、StorageGRID 則會在擷取物件時建立單一的過渡複本（單一提交）。
  - 平衡：如果ILM規則指定平衡選項、StorageGRID 則僅當系統無法立即製作規則中指定的所有複本時、才能製作單一的過渡複本。如果能夠執行同步放置、則此標頭不會有任何影響。StorageGRID當符合物件的ILM規則建立單一複寫複本時、最適合使用「已儲存的備援」選項。在這種情況下、使用「reduced_dere通用」可免除每次擷取作業不必要地建立和刪除額外的物件複本。

  在其他情況下、不建議使用「已儲存的備援」選項。「已導入的備援」會增加擷取期間物件資料遺失的風險。例如、如果單一複本一開始儲存在無法進行ILM評估的儲存節點上、則可能會遺失資料。

注意：在任何時間段內只有一個複寫複本、會使資料面臨永久遺失的風險。如果只有一個物件複寫複本存在、則當儲存節點故障或發生重大錯誤時、該物件就會遺失。在升級等維護程序期間、您也會暫時失去物件的存取權。

指定「已儲存的備援」僅會影響第一次擷取物件時所建立的複本數量。它不會影響使用中ILM原則評估物件時所製作的物件複本數量、也不會導致資料儲存在StorageGRID 較低層級的資料冗餘環境中。

附註：如果您在啟用S3物件鎖定的情況下、將物件放入儲存區、則會忽略「已傳入的備援」選項。如果您將物件放入符合舊規範的儲存區、則「educed_de隊」選項會傳回錯誤。執行「雙重承諾」的程序時、務必確保符合法規遵循要求。StorageGRID

支援下列要求標頭：

- 「內容類型」
- 「x-amz-meta-」、接著是包含使用者定義中繼資料的名稱值配對

  為使用者定義的中繼資料指定名稱值配對時、請使用以下一般格式：

  ```
  x-amz-meta-_name_: `value`
  ```

  如果您要使用*使用者定義的建立時間*選項做為ILM規則的參考時間、則必須使用「建立時間」做為建立物件時記錄的中繼資料名稱。例如：

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

  自70年1月1日起、「創造時間」的值會以秒計算。

如果您要將物件新增至已啟用舊版法規遵循的儲存區、則不允許將「creation - Time」新增為使用者定義的中繼資料。將傳回錯誤。

- S3物件鎖定要求標頭：
  - 「X-amz-object-lock-mode」
  - 《X-amz-object-lock-Retain直到日期》
  - 「X-amz-object-lock-legal hold」

  如果提出的要求沒有這些標頭、則會使用儲存庫預設保留設定來計算物件版本的保留日期。

使用S3物件鎖定

- SSe要求標頭：
  - 「X-amz-server端點加密」
  - 「X-amz-server端加密- customer-key-md5」
  - 「X-amz-server端加密客戶金鑰」
  - 「X-amz-server端加密- customer-演算 法」

[要求伺服器端加密的標頭]

如需StorageGRID 瞭解如何處理UTF-8字元的資訊、請參閱「放置物件」的文件。

要求伺服器端加密的標頭

您可以使用下列要求標頭、以伺服器端加密來加密多部份物件。「SSE」和「SSE-C」選項互不相關。

- * SSE-*：如果您想要使用StorageGRID 由支援的唯一金鑰來加密物件、請在「初始化多部份上傳」要求中使用下列標頭。請勿在任何上傳零件要求中指定此標頭。
  - 「X-amz-server端點加密」
- * SSE-C*：如果您想要使用您提供及管理的唯一金鑰來加密物件、請在「初始化多部份上傳」要求（以及後續的每個「上傳零件」要求）中使用這三個標頭。
  - 「X-amz-server端加密客戶演算法」：指定「AES256」。
  - 「X-amz-server端加密客戶金鑰」：指定新物件的加密金鑰。
  - 「X-amz-server端加密- customer-key-md5」：指定新物件加密金鑰的md5摘要。

*注意：*您提供的加密金鑰永遠不會儲存。如果您遺失加密金鑰、就會遺失對應的物件。在使用客戶提供的金鑰來保護物件資料之前、請先檢閱「使用伺服器端加密」中的考量事項。

不支援的要求標頭

不支援下列要求標頭、並傳回「XNotImplemed」

- 「X-amz-website - redirect-location」

版本管理

多部分上傳包含不同的作業、可用於初始化上傳、列出上傳內容、上傳零件、組裝上傳的零件、以及完成上傳。執行完整的「多重組件上傳」作業時、會建立物件（並在適用情況下建立版本）。

相關資訊

使用ILM管理物件

使用伺服器端加密

放置物件

上傳零件

「上傳零件」作業會上傳物件的多部份上傳中的零件。

支援的要求標頭

支援下列要求標頭：

- 《內容長度》
- 《Content-MD5》

要求伺服器端加密的標頭

如果您為「初始化多重組件上傳」要求指定SSE-C加密、則您也必須在每個「上傳零件」要求中包含下列要求標頭：

- 「X-amz-server端加密客戶演算法」：指定「AES256」。
- 「X-amz-server端加密客戶金鑰」：指定您在「初始化多重成分上傳」要求中提供的相同加密金鑰。
- 「X-amz-server端加密- customer-key-md5」：指定您在「初始化多重成分上傳」要求中提供的相同md5摘要。

> 您提供的加密金鑰永遠不會儲存。如果您遺失加密金鑰、就會遺失對應的物件。在使用客戶提供的金鑰來保護物件資料之前、請先檢閱「使用伺服器端加密」中的考量事項。

版本管理

多部分上傳包含不同的作業、可用於初始化上傳、列出上傳內容、上傳零件、組裝上傳的零件、以及完成上傳。執行完整的「多重組件上傳」作業時、會建立物件（並在適用情況下建立版本）。

相關資訊

使用伺服器端加密

上傳零件-複製

「上傳零件-複製」作業會將現有物件的資料複製為資料來源、藉此上傳物件的一部分。

「上傳零件-複製」作業會在所有Amazon S3 REST API行為下執行。

此要求會讀取StorageGRID 並寫入在「x-amz-copy-source-range」中指定的物件資料。

支援下列要求標頭：

- 「x-amz-copy-source-if-match」
- 「x-amz-copy-source-if-none-MATCH」
- 「x-amz-copy-source-if-modif-since」
- 《X-amz-copy-source-if-modif-s自》

要求伺服器端加密的標頭

如果您為「初始化多重成分上傳」要求指定SSE-C加密、則您也必須在每個「上傳成分-複製」要求中包含下列要求標頭：

- 「X-amz-server端加密客戶演算法」：指定「AES256」。
- 「X-amz-server端加密客戶金鑰」：指定您在「初始化多重成分上傳」要求中提供的相同加密金鑰。
- 「X-amz-server端加密- customer-key-md5」：指定您在「初始化多重成分上傳」要求中提供的相同md5摘要。

如果來源物件是使用客戶提供的金鑰（SSE-C）加密、您必須在「上傳零件-複製」要求中包含下列三個標頭、以便解密物件、然後複製：

- 《x-amz-copy-sourceese-sider-side-ridionese-customer-alralc演算 法》：指定「AES256」。
- 「x-amz-copy-sourcez-server端加密客戶金鑰」：指定您在建立來源物件時所提供的加密金鑰。
- 「x-amz-copy-sourceze-server端加密-客戶金鑰-md5」：指定您在建立來源物件時所提供的md5摘要。

> 您提供的加密金鑰永遠不會儲存。如果您遺失加密金鑰、就會遺失對應的物件。在使用客戶提供的金鑰來保護物件資料之前、請先檢閱「使用伺服器端加密」中的考量事項。

版本管理

多部分上傳包含不同的作業、可用於初始化上傳、列出上傳內容、上傳零件、組裝上傳的零件、以及完成上傳。執行完整的「多重組件上傳」作業時、會建立物件（並在適用情況下建立版本）。

完成多部份上傳

完整的「多重零件上傳」作業會透過組裝先前上傳的零件、完成物件的多重部分上傳。

解決衝突

衝突的用戶端要求（例如兩個寫入同一個金鑰的用戶端）會以「最新致勝」的方式解決。「最新致勝」評估的時間取決於StorageGRID 何時由VMware系統完成指定的要求、而非S3用戶端開始作業的時間。

要求標頭

支援「x-amz-Storage-Class」要求標頭、如果StorageGRID 相符的ILM規則指定「雙重認可」或「平衡」的擷取行為、則會影響到所建立的物件複本數量。

- 《標準》

  （預設）當ILM規則使用雙重提交選項、或平衡選項回到建立臨時複本時、指定雙重提交擷取作業。

- "educed_deete"

  當ILM規則使用雙重提交選項、或平衡選項回到建立過渡複本時、指定單一提交擷取作業。

> 如果在啟用S3物件鎖定的情況下、將物件放入儲存區、則會忽略「已儲存的備援」選項。如果您將物件放入符合舊規範的儲存區、則「educed_de隊」選項會傳回錯誤。執行「雙重承諾」的程序時、務必確保符合法規遵循要求。StorageGRID

> 如果多部分上傳未在15天內完成、則該作業會標示為非作用中、且所有相關資料都會從系統中刪除。

> 傳回的「ETag」值不是資料的一組MD5總和、而是在Amazon S3 API實作多部份物件的「ETag」值之後。

版本管理

此作業會完成多部份上傳。如果已針對某個儲存區啟用版本管理、則會在完成多重部分上傳時建立物件版本。

如果已針對儲存區啟用版本管理、系統會針對儲存的物件版本自動產生唯一的「版本ID」。此「版本ID」也會在回應中使用「x-amz-version -id」回應標頭傳回。

如果版本控制暫停、則物件版本會以null「VrionId」儲存、如果null版本已經存在、則會覆寫該版本。

> 當某個儲存區啟用版本管理時、完成多部份上傳會一律建立新版本、即使在同一個物件金鑰上同時完成多部份上傳也一樣。如果未針對某個儲存區啟用版本管理、則可以啟動多重部分上傳、然後在同一個物件金鑰上啟動並完成另一個多重部分上傳。在非版本的儲存區上、完成最後一次的多部分上傳優先。

複寫失敗、通知或中繼資料通知

如果平台服務已設定多重零件上傳的儲存區、即使相關的複寫或通知動作失敗、多重零件上傳仍會成功。

如果發生這種情況、則會在Grid Manager中針對Total事件（SMT）發出警示。最後一個事件訊息會針對通知失敗的最後一個物件、顯示「無法發佈Bucket名稱物件金鑰的通知」。（要查看此訊息、請選取*節點*>*儲存節點_*>*事件*。檢視表格頂端的最後一個事件。） 事件訊息也會列在「/var/local/log/bycast-err.log」中。

租戶可透過更新物件的中繼資料或標記來觸發失敗的複寫或通知。租戶可以重新提交現有的值、以避免進行不必要的變更。

相關資訊

使用ILM管理物件

錯誤回應

支援所有適用的標準S3 REST API錯誤回應。StorageGRID此外、此功能還會加入數個自

訂回應。StorageGRID

支援的**S3 API**錯誤代碼

名稱	**HTTP**狀態
ACCESSDENIED	403禁止
《標誌摘要》	400個錯誤要求
BuckketAlreadyEx分子	衝突
BucketNotEmpty	衝突
不完整正文	400個錯誤要求
內部錯誤	500內部伺服器錯誤
InvalidAccessKeyId	403禁止
InvalidArgument	400個錯誤要求
InvalidBucketName	400個錯誤要求
InvalidBucketState	衝突
InvalidDigest	400個錯誤要求
InvalidEncryptionAlgorithm錯誤	400個錯誤要求
InvalidPart	400個錯誤要求
InvalidPartOrder	400個錯誤要求
InvalidRang	無法滿足416個要求的範圍
InvalidRequest	400個錯誤要求
InvalidStorageClass	400個錯誤要求
InvalidTag	400個錯誤要求
InvalidURI	400個錯誤要求

名稱	**HTTP**狀態
KeyTooLong	400個錯誤要求
MalformedXML	400個錯誤要求
Metadata TooLarg	400個錯誤要求
方法未允許	不允許使用405方法
內容長度	需要411長度
MissingRequestBodyError	400個錯誤要求
MISingSecurityHeader	400個錯誤要求
NoSuchBucket	找不到404
NoSuchKey	找不到404
NoSuchUpload	找不到404
未實作	501未實作
NoSuchBucketPolicy	找不到404
ObjectLockConfiguration未找到錯誤	找不到404
預先條件失敗	412先決條件失敗
要求時間TooSkewed	403禁止
服務無法使用	503服務無法使用
簽名DoesNotMatch	403禁止
TooManyboo	400個錯誤要求
使用者KeyMustBeSpecified	400個錯誤要求

零點自訂錯誤代碼StorageGRID

名稱	說明	HTTP狀態
XBucketLifecycleNotSupported	不允許在符合舊版規範的儲存庫中進行貯體生命週期組態	400個錯誤要求
XBucketPolicyParseException	無法剖析收到的儲存區原則Json。	400個錯誤要求
XComplianceConflict	因為舊版規範設定而拒絕作業。	403禁止
XComplianceReducedRedundancyForbided	舊型符合標準的儲存區不允許減少備援	400個錯誤要求
XMaxBucketPolicyLengthExceed	您的原則超過允許的儲存區原則長度上限。	400個錯誤要求
XMissingInternalRequestHeader	缺少內部要求的標頭。	400個錯誤要求
XNoSuchBucketCompliance	指定的儲存庫未啟用舊版法規遵循。	找不到404
XNotAcceptable	要求包含一或多個無法滿足的Accept標頭。	無法接受的406
XNotImplemed	您提供的要求暗示功能尚未實作。	501未實作

支援SS3 REST API作業StorageGRID

S3 REST API上新增了特定StorageGRID 於該系統的作業。

- 取得時段一致性要求

  「Get Bucket一致性」要求可讓您決定套用至特定Bucket的一致性層級。

- 置入時段一致性要求

  「放入庫位一致性」要求可讓您指定要套用至庫位執行作業的一致性層級。

- 取得時段上次存取時間要求

  「取得時段上次存取時間」要求可讓您決定是否為個別的時區啟用或停用上次存取時間更新。

- 將時段放入上次存取時間要求

  「放置時段上次存取時間」要求可讓您針對個別的時段啟用或停用上次存取時間更新。停用上次存取時間更新可改善效能、是所有以10.3.0版或更新版本建立之儲存區的預設設定。

- 刪除時段中繼資料通知組態要求

刪除庫位中繼資料通知組態要求可讓您刪除組態XML、以停用個別庫位的搜尋整合服務。

- 取得Bucket中繼資料通知組態要求

  「Get Bucket中繼資料」通知組態要求可讓您擷取組態XML、以設定個別儲存區的搜尋整合。

- 放置時段中繼資料通知組態要求

  「置入庫位元資料」通知組態要求可讓您針對個別的庫位啟用搜尋整合服務。您在要求本文中提供的中繼資料通知組態XML、會指定將中繼資料傳送至目的地搜尋索引的物件。

- 取得儲存使用量要求

  「Get Storage使用量」要求會告訴您某個帳戶所使用的總儲存容量、以及與該帳戶相關聯的每個儲存區容量。

- 舊版法規遵循的已過時資源桶要求

  您可能需要使用StorageGRID Sfs3 REST API來管理使用舊版Compliance功能所建立的儲存區。

取得時段一致性要求

「Get Bucket一致性」要求可讓您決定套用至特定Bucket的一致性層級。

預設的一致性控制項設定為保證新建立物件的寫入後讀取。

您有S3：GetBucketConsistency權限、或是帳戶root權限、才能完成此作業。

申請範例

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

回應

在回應XML中、「<一致性>」會傳回下列其中一個值：

一致性控制	說明
全部	所有節點都會立即接收資料、否則要求將會失敗。
強大的全球化技術	保證所有站台所有用戶端要求的寫入後讀取一致性。
強式網站	保證站台內所有用戶端要求的寫入後讀取一致性。

一致性控制	說明
全新寫入後讀取	（預設）為新物件提供寫入後讀取一致性、並最終確保物件更新一致。提供高可用度與資料保護保證。最符合Amazon S3一致性保證。 *附註：*如果您的應用程式在不存在的物件上使用標頭要求、如果一個或多個儲存節點無法使用、您可能會收到大量500個內部伺服器錯誤。若要避免這些錯誤、請將一致性控制設為「可用」、除非您需要類似Amazon S3的一致性保證。
可用的（最終的頭端作業一致性）	其行為與「全新寫入後的讀取」一致性層級相同、但最終只能提供一致的執行方式。如果儲存節點無法使用、則頭端作業的可用度比「全新寫入後的準備」高。不同於Amazon S3一致性保證、僅適用於頭端作業。

回應範例

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

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

相關資訊

一致性控管

置入時段一致性要求

「放入庫位一致性」要求可讓您指定要套用至庫位執行作業的一致性層級。

預設的一致性控制項設定為保證新建立物件的寫入後讀取。

您有S3：PuttBucketConsistency權限、或是帳戶root、才能完成此作業。

申請

「x-ntap-sg-consistency」參數必須包含下列其中一個值：

一致性控制	說明
全部	所有節點都會立即接收資料、否則要求將會失敗。
強大的全球化技術	保證所有站台所有用戶端要求的寫入後讀取一致性。
強式網站	保證站台內所有用戶端要求的寫入後讀取一致性。
全新寫入後讀取	（預設）為新物件提供寫入後讀取一致性、並最終確保物件更新一致。提供高可用度與資料保護保證。最符合Amazon S3一致性保證。 *附註：*如果您的應用程式在不存在的物件上使用標頭要求、如果一個或多個儲存節點無法使用、您可能會收到大量500個內部伺服器錯誤。若要避免這些錯誤、請將一致性控制設為「可用」、除非您需要類似Amazon S3的一致性保證。
可用的（最終的頭端作業一致性）	其行為與「全新寫入後的讀取」一致性層級相同、但最終只能提供一致的執行方式。如果儲存節點無法使用、則頭端作業的可用度比「全新寫入後的準備」高。不同於Amazon S3一致性保證、僅適用於頭端作業。

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

申請範例

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

相關資訊

一致性控管

取得時段上次存取時間要求

「取得時段上次存取時間」要求可讓您決定是否為個別的時區啟用或停用上次存取時間更新。

您有S3：GetBucketLastAccessTime權限、或是帳戶root權限、才能完成此作業。

申請範例

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

回應範例

此範例顯示已針對儲存庫啟用上次存取時間更新。

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

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

將時段放入上次存取時間要求

「放置時段上次存取時間」要求可讓您針對個別的時段啟用或停用上次存取時間更新。停用上次存取時間更新可改善效能、是所有以10.3.0版或更新版本建立之儲存區的預設設定。

您擁有儲存區的S3：PuttBucketLastAccessTime權限、或是帳戶root權限、即可完成此作業。

> 從版本10.3開始StorageGRID 、所有新的儲存庫預設都會停用上次存取時間的更新。如果您有使用StorageGRID 舊版的更新程式建立的儲存區、而且想要符合新的預設行為、則必須明確停用這些舊版儲存區的上次存取時間更新。您可以使用租戶管理程式中的「放置時段上次存取時間」要求、「* S3 > Bucket >*變更上次存取設定」核取方塊、或「租戶管理API」、來啟用或停用上次存取時間的更新。

如果某個儲存區的上次存取時間更新已停用、則會將下列行為套用至儲存區上的作業：

- 「取得物件」、「取得物件ACL」、「取得物件標記」和「標頭物件要求」不會更新上次存取時間。不會將物件新增至佇列、以進行資訊生命週期管理（ILM）評估。
- 放置物件：只更新中繼資料的複製和放置物件標記要求、也會更新上次存取時間。物件會新增至佇列以進行ILM評估。
- 如果來源儲存區的上次存取時間更新已停用、則「放置物件」-「複製要求」不會更新來源儲存區的上次存取時間。複製的物件不會新增至來源儲存區的ILM評估佇列。但是、對於目的地、「放置物件」-「複製要求」一律會更新上次存取時間。物件複本會新增至佇列以進行ILM評估。

- 完成多重成分上傳要求更新上次存取時間。完成的物件會新增至佇列以進行ILM評估。

申請範例

此範例可讓儲存區的上次存取時間達到。

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

此範例會停用儲存區的上次存取時間。

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

相關資訊

使用租戶帳戶

刪除時段中繼資料通知組態要求

刪除庫位中繼資料通知組態要求可讓您刪除組態XML、以停用個別庫位的搜尋整合服務。

您擁有儲存區的S3：刪除BucketMetadata通知權限、或是帳戶根權限、即可完成此作業。

申請範例

此範例顯示停用區段的搜尋整合服務。

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

取得**Bucket**中繼資料通知組態要求

「Get Bucket中繼資料」通知組態要求可讓您擷取組態XML、以設定個別儲存區的搜尋整合。

您有S3：GetBucketMetadata通知權限、或是帳戶root、才能完成此作業。

申請範例

此要求會擷取名為「Bucket」之儲存區的中繼資料通知組態。

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

回應

回應本文包含儲存區的中繼資料通知組態。中繼資料通知組態可讓您決定儲存區的搜尋整合設定方式。也就是、它可讓您決定要建立索引的物件、以及要將物件中繼資料傳送至哪個端點。

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

每個中繼資料通知組態都包含一或多個規則。每個規則都會指定套用的物件、StorageGRID 以及應將物件中繼資料傳送到哪個目的地。目的地必須使用StorageGRID 不實端點的URN來指定。

名稱	說明	必要
Metadata NotifyationConfiguration	用於指定中繼資料通知物件和目的地之規則的容器標籤。 包含一或多個規則元素。	是的

名稱	說明	必要
規則	規則的容器標記、用於識別應將中繼資料新增至指定索引的物件。 會拒絕具有重疊前置碼的規則。 包括在Metadata NotifyationConfiguration元素中。	是的
ID	規則的唯一識別碼。 包含在Rule元素中。	否
狀態	狀態可以是「已啟用」或「已停用」。不針對停用的規則採取任何行動。 包含在Rule元素中。	是的
前置碼	符合前置碼的物件會受到規則影響、其中繼資料會傳送到指定的目的地。 若要符合所有物件、請指定一個空白首碼。 包含在Rule元素中。	是的
目的地	規則目的地的容器標記。 包含在Rule元素中。	是的

名稱	說明	必要
urn	傳送物件中繼資料的目的地之一。必須是StorageGRID 具有下列屬性的不景端點的URN： • 第三個要素是「es」。 • URN必須以索引結尾、並以「domain-name/myindex/mytype」格式輸入中繼資料的儲存位置。 端點是使用租戶管理程式或租戶管理API來設定。它們採用下列形式： • 「arn：AWS：es：_region：帳戶ID：網域/mydomain/myindex/mytype」 • 「urn:mysite：es：：mydomain/myindex/mytype」 端點必須在提交組態XML之前進行設定、否則組態將會失敗並顯示404錯誤。 目標元素中包含urn.	是的

回應範例

包含在「<Metadata NotifyationConfiguration></Metadata NotifyationConfiguration >」標籤之間的XML、顯示如何為儲存區設定與搜尋整合端點的整合。在此範例中、物件中繼資料會傳送至名為「目前」的ElasticSearch索引、並在名為「資源」的AWS網域中、輸入名為「2017」的類型。

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

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

相關資訊

使用租戶帳戶

放置時段中繼資料通知組態要求

「置入庫位元資料」通知組態要求可讓您針對個別的庫位啟用搜尋整合服務。您在要求本文中提供的中繼資料通知組態XML、會指定將中繼資料傳送至目的地搜尋索引的物件。

您擁有儲存區的S3：PuttBucketMetadata通知權限、或是帳戶根權限、即可完成此作業。

申請

要求必須在要求本文中包含中繼資料通知組態。每個中繼資料通知組態都包含一或多個規則。每個規則都會指定要套用的物件、StorageGRID 以及應將物件中繼資料傳送到哪個目的地。

物件可依物件名稱的前置詞進行篩選。例如、您可以將前置詞為「/影像」的物件中繼資料傳送至一個目的地、並將前置詞為「/視訊」的物件傳送至另一個目的地。

具有重疊前置碼的組態無效、在提交時會遭到拒絕。例如、如果組態中包含一個物件規則、其前置詞為「test」、第二個規則則為「test2」、就不允許。

目的地必須使用StorageGRID 不實端點的URN來指定。提交中繼資料通知組態時、端點必須存在、否則要求會以「400個不良要求」的形式失敗。錯誤訊息指出：「無法儲存中繼資料通知（搜尋）原則。指定的端點URN不存在：*URN*.'

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

下表說明中繼資料通知組態XML中的元素。

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

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

申請範例

此範例顯示啟用儲存庫的搜尋整合功能。在此範例中、所有物件的物件中繼資料都會傳送到相同的目的地。

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

<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、與首碼「/影像」相符的物件之物件中繼資料會傳送至一個目的地、而與首碼「/視訊」相符的物件之物件中繼資料則會傳送至第二個目的地。

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

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

由搜尋整合服務產生的**JSON**

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

此範例顯示在名為「test」的儲存格中建立具有「GWS/Tagging.txt」鍵的物件時、可能產生的Json範例。「test」儲存區並非版本化、因此「vrionId」標記為空白。

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

中繼資料通知中包含的物件中繼資料

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

文件名稱包含儲存區名稱、物件名稱及版本ID（若有）。

類型	項目名稱	說明
儲存區和物件資訊	鏟斗	庫位名稱
儲存區和物件資訊	金鑰	物件金鑰名稱
儲存區和物件資訊	版本ID	物件版本、適用於版本控制的儲存區中的物件
儲存區和物件資訊	區域	例如「us-east-1」
系統中繼資料	尺寸	HTTP用戶端可見的物件大小（以位元組為單位）
系統中繼資料	md5	物件雜湊

類型	項目名稱	說明
使用者中繼資料	中繼資料：*key:value*'	物件的所有使用者中繼資料、做為金鑰值配對
標記	標記`*key:value*'	為物件定義的所有物件標記、做為金鑰值配對

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

相關資訊

使用租戶帳戶

取得儲存使用量要求

「Get Storage使用量」要求會告訴您某個帳戶所使用的總儲存容量、以及與該帳戶相關聯的每個儲存區容量。

帳戶及其儲存區所使用的儲存容量、可透過修改後的Get Service（取得服務）要求、使用「x-ntap-sg-usage（x-ntap-sg-usage）」查詢參數來取得。儲存區的使用量會與系統處理的PUT和DELETE要求分開追蹤。使用值可能會在處理要求時延遲、使其符合預期值、尤其是系統負載過重時。

根據預設StorageGRID 、功能區會嘗試使用強大的全域一致性來擷取使用資訊。如果無法達到強大的全球一致性、StorageGRID 則嘗試以強大的站台一致性擷取使用資訊。

您有S3：listAllMybops權限、或是帳戶root、可以完成此作業。

申請範例

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

回應範例

此範例顯示一個帳戶、其中兩個儲存區中有四個物件和12個位元組的資料。每個儲存區包含兩個物件和六個位元組的資料。

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

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

版本管理

每個儲存的物件版本都會在回應中產生「ObjectCount」和「Data Bytes」值。刪除標記不會新增至「ObjectCount」總計。

相關資訊

一致性控管

已過時的資源桶要求、適用於舊版法規遵循

您可能需要使用StorageGRID Sfs3 REST API來管理使用舊版Compliance功能所建立的儲存區。

法規遵循功能已過時

先前版本的不支援《支援不符合要求》功能、現已由S3物件鎖定取代。StorageGRID StorageGRID

如果您先前已啟用「全域符合性」設定、StorageGRID 則會在「支援物件鎖定」中啟用「全域S3物件鎖定」設定。您不再能夠在啟用「法規遵循」的情況下建立新的儲存庫、不過、您可以視需要使用StorageGRID 「S3 REST API」來管理任何現有的符合舊規範的儲存庫。

- 使用S3物件鎖定
- 使用ILM管理物件
- "NetApp知識庫：如何管理StorageGRID 支援老舊的知識庫、請參閱《知識庫文章"

過時的法規遵循要求：

- 已過時-將資源桶要求修改以符合法規要求

  SGCompliance XML元素已過時。先前、您可以將StorageGRID 此等不必要的自訂元素納入可選的XML要求內容中、以建立符合法規的儲存庫要求。

- 已過時-取得資源桶法規遵循要求

  Get Bucket法規遵循要求已過時。不過、您可以繼續使用此要求來判斷現有舊版相容儲存區目前有效的法規遵循設定。

- 已過時-提出資源桶法規遵循要求

  「放入時段」法規遵循要求已過時。不過、您可以繼續使用此要求來修改現有舊版相容桶的法規遵循設定。例如、您可以將現有的貯體置於合法持有狀態、或是延長保留期間。

已過時：將資源桶要求修改以符合法規要求

SGCompliance XML元素已過時。先前、您可以將StorageGRID 此等不必要的自訂元素納入可選的XML要求內容中、以建立符合法規的儲存庫要求。

> 先前版本的不支援《支援不符合要求》功能、現已由S3物件鎖定取代。StorageGRID StorageGRID

使用S3物件鎖定

使用ILM管理物件

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

您無法再建立啟用「法規遵循」的新庫位。如果您嘗試使用「置放桶」要求修改以符合法規要求、以建立新的「符合法規」桶、則會傳回下列錯誤訊息：

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

相關資訊

使用ILM管理物件

使用租戶帳戶

Get Bucket法規遵循要求已過時。不過、您可以繼續使用此要求來判斷現有舊版相容儲存區目前有效的法規遵循設定。

> 先前版本的不支援《支援不符合要求》功能、現已由S3物件鎖定取代。StorageGRID StorageGRID

使用S3物件鎖定

使用ILM管理物件

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

您有S3：GetBucketCompliance權限、或是帳戶root、可以完成此作業。

申請範例

此範例要求可讓您決定名為「mybucket」的儲存貯體的法規遵循設定。

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

回應範例

在回應XML中、「<SGCompliance >」會列出此儲存區的有效法規遵循設定。此回應範例顯示儲存區的法規遵循設定、其中每個物件將保留一年（525600分鐘）、從物件擷取到網格開始算起。此庫位目前沒有合法持有。每個物件將在一年後自動刪除。

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

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

名稱	說明
RetentionPeriodMinutes	新增至此儲存區之物件的保留期間長度（以分鐘為單位）。保留期間是從物件擷取至網格時開始。
LegalHold	• 是：此儲存庫目前處於合法持有狀態。在取消合法持有之前、即使保留期間已過期、也無法刪除此儲存區中的物件。 • 假：此庫位目前未合法持有。此儲存區中的物件可在保留期間到期時刪除。
自動刪除	• 是：此儲存區中的物件會在保留期間到期時自動刪除、除非儲存區處於合法持有狀態。 • 否：保留期間到期時、此儲存區中的物件不會自動刪除。如果需要刪除這些物件、您必須手動刪除這些物件。

錯誤回應

如果儲存區的建立不符合法規要求、回應的HTTP狀態代碼為「找不到404」、S3錯誤代碼為「XNoSuchBucketCompliance」（XNoSuchBucketCompliance）。

相關資訊

使用ILM管理物件

使用租戶帳戶

已過時：提出資源桶法規遵循要求

「放入時段」法規遵循要求已過時。不過、您可以繼續使用此要求來修改現有舊版相容桶的法規遵循設定。例如、您可以將現有的貯體置於合法持有狀態、或是延長保留期間。

先前版本的不支援《支援不符合要求》功能、現已由S3物件鎖定取代。StorageGRID StorageGRID

使用S3物件鎖定

使用ILM管理物件

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

您有S3：PuttBucketCompliance權限、或是帳戶root、才能完成此作業。

在發出「放入庫位」法規遵循要求時、您必須為法規遵循設定的每個欄位指定一個值。

申請範例

此範例要求會修改名為「mybucket」之儲存區的法規遵循設定。在此範例中、「mybucket」中的物件現在將保留兩年（1、051、200分鐘）、而非一年、從物件進入網格開始。此庫位沒有合法持有。每個物件將在兩年後自

動刪除。

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

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

名稱	說明
RetentionPeriodMinutes	新增至此儲存區之物件的保留期間長度（以分鐘為單位）。保留期間是從物件擷取至網格時開始。 *注意：*當為RetentionPeriodMinute指定新值時、您必須指定等於或大於該儲存格目前保留期間的值。在桶的保留期間設定完成之後、您就無法減少該值、只能增加該值。
LegalHold	• 是：此儲存庫目前處於合法持有狀態。在取消合法持有之前、即使保留期間已過期、也無法刪除此儲存區中的物件。 • 假：此庫位目前未合法持有。此儲存區中的物件可在保留期間到期時刪除。
自動刪除	• 是：此儲存區中的物件會在保留期間到期時自動刪除、除非儲存區處於合法持有狀態。 • 否：保留期間到期時、此儲存區中的物件不會自動刪除。如果需要刪除這些物件、您必須手動刪除這些物件。

法規遵循設定的一致性層級

當您更新S3儲存區的法規遵循設定、並提出「置放儲存區法規遵循」要求時StorageGRID 、即可嘗試更新整個網格的儲存區中繼資料。根據預設、StorageGRID 支援使用*強式全域*一致性層級、以保證所有資料中心站台及包含儲存庫中繼資料的所有儲存節點、在變更的法規遵循設定中、具有寫入後讀取一致性。

如果StorageGRID 由於某個站台的資料中心站台或多個儲存節點無法使用、導致無法達到*強式全域*一致性等級、則回應的HTTP狀態代碼為「503服務無法使用」

如果您收到此回應、則必須聯絡網格管理員、以確保所需的儲存服務能夠儘快提供。如果網格管理員無法在每個站台上提供足夠的儲存節點、技術支援可能會強制*強站台*一致性層級、引導您重試失敗的要求。

除非您是技術支援人員的指示、而且您不瞭解使用此層級可能造成的後果、否則請勿強迫*強站台*一致性層級以符合放置桶規範。

當一致性層級降至*強站台*時StorageGRID 、更新的法規遵循設定只有在站台內的用戶端要求才具有寫入後讀取一致性。這表示StorageGRID 在所有站台和儲存節點都可用之前、此儲存區的設定可能會暫時有多個不一致的設定。不一致的設定可能會導致非預期和非預期的行為。例如、如果您將儲存庫置於合法持有之下、而強制降低一致性層級、則儲存庫先前的法規遵循設定（即合法暫停）可能會繼續在某些資料中心站台上生效。因此、您認為合法保留的物件、可能會在保留期間到期時遭到刪除、使用者或自動刪除（如果已啟用）。

若要強制使用*強站台*一致性層級、請重新發出PPUT Bucket法規遵循要求、並加入「一致性控制」HTTP要求標頭、如下所示：

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

錯誤回應

- 如果儲存區的建立不符合法規要求、回應的HTTP狀態代碼為「找不到404」。
- 如果申請中的「RetentionPeriodMinutes」低於庫位目前的保留期間、則HTTP狀態代碼為「400 Bad Request」（400錯誤要求）。

相關資訊

已過時：將資源桶要求修改以符合法規要求

使用租戶帳戶

使用ILM管理物件

儲存庫和群組存取原則

支援使用Amazon Web Services（AWS）原則語言、讓S3租戶能夠控制對這些儲存區內的儲存區和物件的存取。StorageGRID此系統實作S3 REST API原則語言的子集。StorageGRIDS3 API的存取原則是以Json撰寫。

存取原則總覽

支援的存取原則有兩種。StorageGRID

- 資源庫原則、使用「取得資源庫」原則設定、「放入資源庫」原則、以及刪除資源庫原則S3 API作業。庫位原則會附加至庫位、因此這些原則可設定為控制庫位擁有者帳戶或其他帳戶中的使用者對庫位及其中物件的存取。庫位原則僅適用於一個庫位、可能也適用於多個群組。
- 群組原則、使用租戶管理程式或租戶管理API進行設定。群組原則會附加至帳戶中的群組、因此這些原則會設定為允許該群組存取該帳戶所擁有的特定資源。群組原則僅適用於一個群組、可能也適用於多個儲存區。

根據Amazon定義的特定語法、執行庫位和群組原則。StorageGRID每個原則內部都有一組原則聲明、每個陳述都包含下列元素：

- 對帳單ID（Sid）（選用）

- 效果
- 委託人/未委託人
- 資源/未資源
- 行動/未行動
- 條件（選用）

原則陳述是使用此結構來指定權限：在套用<condition>時，授與<effect>允許/拒絕<Principe>執行<Action"。

每個原則元素都用於特定功能：

元素	說明
SID	Sid元素為選用項目。Sid僅供使用者說明使用。它會儲存、但StorageGRID 不會被作業系統解讀。
效果	使用effect元素來確定是否允許或拒絕指定的作業。您必須使用支援的Action元素關鍵字、識別您允許（或拒絕）的貯體或物件作業。
委託人/未委託人	您可以允許使用者、群組和帳戶存取特定資源並執行特定動作。如果要求中未包含S3簽名、則可指定萬用字元（*）做為主體、以匿名存取。根據預設、只有root帳戶可以存取該帳戶擁有的資源。 您只需要在庫位原則中指定主要元素。對於群組原則而言、附加原則的群組是內含的主體元素。
資源/未資源	資源元素可識別儲存區和物件。您可以使用Amazon資源名稱（ARN）來允許或拒絕貯體和物件的權限、以識別資源。
行動/未行動	「行動」和「效果」元素是權限的兩個元件。當群組要求資源時、系統會將資源的存取權限授予或拒絕。除非您特別指派權限、否則存取會遭拒、但您可以使用明確拒絕來覆寫其他原則所授予的權限。
條件	條件元素為選用項目。條件可讓您建置運算式、以判斷何時應套用原則。

在Action元素中、您可以使用萬用字元（*）來指定所有作業或作業子集。例如、此動作會比對S3：GetObject、S3：PuttObject和S3：Delete物件等權限。

```
s3:*Object
```

在資源元素中、您可以使用萬用字元（*）和（？）。星號（*）與0個以上的字元相符、但問號（？） 符合任何單一字元。

在主體元素中、除了設定匿名存取（將權限授予每個人）之外、不支援萬用字元。例如、您將萬用字元（*）設為主要值。

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

在下列範例中、陳述式使用的是「效果」、「主要」、「行動」和「資源」元素。此範例顯示完整的儲存區原則聲明、其使用「允許」的效果來賦予主體、管理群組「聯盟群組/管理員」和財務群組「聯盟群組/財務」、在該儲存區內所有物件上執行「行動」「3：清單儲存區」的權限、以及「行動」「3：GetObject」的權限。

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

儲存區原則的大小上限為20、480個位元組、而且群組原則的大小上限為5、120個位元組。

相關資訊

使用租戶帳戶

原則的一致性控制設定

根據預設、您對群組原則所做的任何更新最終都是一致的。一旦群組原則一致、因為原則快取、變更可能需要額外15分鐘才能生效。根據預設、您對庫位原則所做的任何更新、最終也會保持一致。

您可以視需要變更庫位原則更新的一致性保證。例如、基於安全考量、您可能希望變更庫位原則、使其儘快生效。

在這種情況下、您可以在「放入庫位」原則要求中設定「一致性控制」標頭、也可以使用「放入庫位一致性」要求。變更此要求的一致性控制時、您必須使用* all *值、以提供寫入後讀取一致性的最高保證。如果您在「放置時段一致性要求」的標頭中指定任何其他一致性控制值、則該要求將被拒絕。如果您為「放入庫位」原則要求指定任何其他值、則會忽略該值。當儲存區原則一致之後、由於原則快取、變更可能需要額外8秒的時間才能生效。

如果您將一致性層級設為*全部*、以強制新的儲存庫原則更快生效、請務必在完成時將儲存庫層級控制權設回其原始值。否則、所有未來的貯體要求都會使用* all*設定。

在原則聲明中使用**ARN**

在原則聲明中、ARN用於主要和資源元素。

- 使用此語法來指定S3資源ARN：

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

- 使用此語法來指定身分識別資源ARN（使用者和群組）：

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

其他考量事項：

- 您可以使用星號（*）做為萬用字元、以比對物件金鑰內的零個或多個字元。
- 可以在物件金鑰中指定的國際字元、應使用Json utf-8或Json \u轉義序列進行編碼。不支援百分比編碼。

  "RFC 2141 URN語法"

  PPUT Bucket原則作業的HTTP要求本文必須以charset=utf-8進行編碼。

在原則中指定資源

在原則聲明中、您可以使用資源元素來指定允許或拒絕權限的儲存區或物件。

- 每個原則聲明都需要資源元素。在原則中、資源會以「Resource」（資源）元素表示、或是以「NotResource」（不資源）來表示排除。
- 您可以使用S3資源ARN來指定資源。例如：

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

- 您也可以在物件機碼內使用原則變數。例如：

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

- 資源值可以指定在建立群組原則時尚未存在的儲存區。

相關資訊

[在原則中指定變數]

在原則中指定主體

使用主體元素來識別原則聲明允許/拒絕存取資源的使用者、群組或租戶帳戶。

- 庫位原則中的每個原則聲明都必須包含主要元素。群組原則中的原則聲明不需要主體元素、因為群組被理解為主體。
- 在原則中、原則會以「主體」或「NotPrincipal」等元素表示、以排除原則。
- 帳戶型身分識別必須使用ID或ARN來指定：

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

- 此範例使用租戶帳戶ID 27233906934684427525、其中包含帳戶root和帳戶中的所有使用者：

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

- 您只能指定帳戶根目錄：

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

- 您可以指定特定的聯盟使用者（「Alex」）：

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

- 您可以指定特定的聯盟群組（「經理」）：

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

- 您可以指定匿名主體：

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

- 為了避免混淆、您可以使用使用者UUID、而非使用者名稱：

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

例如、假設Alex離開組織、而使用者名稱「Alex」也被刪除。如果新的Alex加入組織並被指派相同的「Alex」使用者名稱、新使用者可能會不小心繼承授予原始使用者的權限。

- 主要值可以指定建立儲存區原則時尚未存在的群組/使用者名稱。

在原則中指定權限

在原則中、會使用Action元素來允許/拒絕資源的權限。您可以在原則中指定一組權限、以元素「Action」表示、或是以「NotAction」表示排除權限。每個元素都對應到特定的S3 REST API作業。

這些表格列出套用至儲存區的權限、以及套用至物件的權限。

Amazon S3現在使用S3：PuttReplicationConfiguration權限來執行PPUT和DELETE Bucket複寫動作。針對每個行動使用不同的權限、這與原始的Amazon S3規格相符。StorageGRID

使用PUT覆寫現有值時、會執行刪除。

套用至貯體的權限

權限	**S3 REST API**作業	客製**StorageGRID** 化以供選擇
S3：建立桶	放入鏟斗	
S3：刪除資源桶	刪除時段	
S3：刪除BucketMetadata通知	刪除時段中繼資料通知組態	是的
S3：刪除BucketPolicy	刪除庫位原則	
S3：刪除複製組態	刪除時段複寫	是的、請針對「放置」和「刪除」*分別設定權限
S3：GetBucketAcl	取得Bucket ACL	
S3：GetBucketCompliance	取得資源桶法規遵循（已過時）	是的
S3：GetBucketConsistency	取得庫位一致性	是的
S3：GetBucketCORS	獲取庫位檢查器	
S3：GetEncryptionConfiguration	取得Bucket加密	

權限	**S3 REST API**作業	客製**StorageGRID** 化以供選擇
S3：GetBucketLastAccessTime	取得時段上次存取時間	是的
S3：GetBucketLocation	取得理想位置	
S3：GetBucketMetadata通知	取得Bucket中繼資料通知組態	是的
S3：GetBucketNotification	取得庫存箱通知	
S3 ：GetBucketObjectLockConfiguration	取得物件鎖定組態	
S3：GetBucketPolicy	取得庫存管理政策	
S3：GetBucketting	取得庫位標記	
S3：GetBucketVersion	取得版本管理	
S3：Get生命 週期組態	取得生命週期	
S3：GetReplicationConfiguration	取得庫位複寫	
S3：ListAllMyb桶	• 取得服務 • 取得儲存使用量	是的、適用於取得儲存設備使用量
S3：清單庫	• Get Bucket（列出物件） • 鏟斗 • POST物件還原	
S3：listBucketMultiPartUploads	• 列出多個部分上傳 • POST物件還原	
S3：listBucketVerions	取得Bucket版本	
S3：PuttBucketCompliance	符合資源桶規範（已過時）	是的
S3：PuttBucketConsistency	實現庫位一致性	是的
S3：PuttBucketCORS	• 刪除庫位檢查 • 放入庫位	

權限	**S3 REST API**作業	客製**StorageGRID** 化以供選擇
S3：PuttEncryptionConfiguration	• 刪除時段加密 • 使用資源桶加密	
S3：PuttBucketLastAccessTime	將資源桶放在最後存取時間	是的
S3：PuttBucketMetadata通知	放置時段中繼資料通知組態	是的
S3：PuttBucketNotification	放置時段通知	
S3 ：PuttBucketObjectLockConfiguration	• 使用「X-amz-Bucket物件鎖定：true」要求標頭（也需要S3：建立Bucket權限）放置Bucket • 放置物件鎖定組態	
S3：PuttBucketPolicy	資源桶政策	
S3：PuttBucketting	• 刪除庫位標記 • 置入庫位標記	
S3：PuttBucketVersion	放入資源桶版本管理	
S3：Putt升降 器組態	• 刪除時段生命週期 • 放入鏟斗生命週期	
S3：PuttReplicationConfiguration	放入資源桶複寫	是的、請針對「放置」和「刪除」*分別設定權限

套用至物件的權限

權限	**S3 REST API**作業	客製**StorageGRID** 化以供選擇
S3：中止多重角色上傳	• 中止多部份上傳 • POST物件還原	
S3：刪除物件	• 刪除物件 • 刪除多個物件 • POST物件還原	
S3：刪除ObjectTagging	刪除物件標記	

權限	**S3 REST API**作業	客製**StorageGRID** 化以供選擇
S3：刪除ObjectVersion標記	刪除物件標記（物件的特定版本）	
S3：刪除ObjectVersion	刪除物件（物件的特定版本）	
S3：GetObject	• 取得物件 • 標頭物件 • POST物件還原 • 選取「物件內容」	
S3：GetObjectAcl	取得物件ACL	
S3：GetObjectLegalHold	取得物件合法持有	
S3：GetObjectRetention	取得物件保留	
S3：GetObjectTagging	取得物件標記	
S3：GetObjectVersion標記	取得物件標記（物件的特定版本）	
S3：GetObjectVersion	Get物件（物件的特定版本）	
S3：列出多個零件上傳零件	列出零件、POST物件還原	
S3：PuttObject	• 放置物件 • 放置物件-複製 • POST物件還原 • 啟動多部份上傳 • 完成多部份上傳 • 上傳零件 • 上傳零件-複製	
S3：PuttObjectLegalHold	將物件保留為合法	
S3：PuttObjectRetention	保留物件	
S3：PuttObjectTagging	放置物件標記	
S3：PuttObjectVersion標記	放置物件標記（物件的特定版本）	

權限	S3 REST API作業	客製StorageGRID 化以供選擇
S3：PuttOverwriteObject	• 放置物件 • 放置物件-複製 • 放置物件標記 • 刪除物件標記 • 完成多部份上傳	是的
S3：恢復物件	POST物件還原	

使用**PuttOverwriteObject**權限

S3：PuttOverwriteObject權限是套StorageGRID 用至建立或更新物件之作業的自訂功能。此權限的設定決定用戶端是否可以覆寫物件的資料、使用者定義的中繼資料或S3物件標記。

此權限的可能設定包括：

- 允許：用戶端可以覆寫物件。這是預設設定。
- 拒絕：用戶端無法覆寫物件。設為「拒絕」時、PuttOverwriteObject權限的運作方式如下：
  - 如果在同一路徑找到現有物件：
    - 無法覆寫物件的資料、使用者定義的中繼資料或S3物件標記。
    - 任何進行中的擷取作業都會取消、並傳回錯誤。
    - 如果啟用S3版本管理、則「拒絕」設定可防止「放置物件標記」或「刪除物件標記」作業修改物件及其非目前版本的TagSet。
  - 如果找不到現有的物件、此權限將不會生效。
- 當此權限不存在時、效果與「允許」設定相同。

> 如果目前的S3原則允許覆寫、而且PuttOverwriteObject權限設定為「拒絕」、則用戶端無法覆寫物件的資料、使用者定義的中繼資料或物件標記。此外、如果選中*防止用戶端修改*核取方塊（組態>*系統*>*網格選項*）、該設定會覆寫「PuttoverriteObject」權限的設定。

相關資訊

S3群組原則範例

在原則中指定條件

條件會定義原則的生效時間。條件包括運算子和金鑰值配對。

條件使用金鑰值配對進行評估。條件元素可以包含多個條件、而且每個條件可以包含多個金鑰值配對。條件區塊使用下列格式：

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

在下列範例中、ipAddress條件使用SourceIp條件金鑰。

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

支援的條件運算子

條件運算子的分類如下：

- 字串
- 數字
- 布林值
- IP 位址
- null檢查

條件運算子	說明
擷取等量資料	根據完全相符（區分大小寫）、將金鑰與字串值進行比較。
擷取NotEquals	根據否定比對（區分大小寫）、將金鑰與字串值進行比較。
StringEqualsIgnoreCase	根據完全相符的結果（忽略大小寫）、將金鑰與字串值進行比較。
StringNotEqualsIgnoreCase	根據否定比對（忽略大小寫）、將金鑰與字串值進行比較。
StringLike	根據完全相符（區分大小寫）、將金鑰與字串值進行比較。可以包括*和？萬用字元。
StringNotLike	根據否定比對（區分大小寫）、將金鑰與字串值進行比較。可以包括*和？萬用字元。

條件運算子	說明
分子等量	根據完全相符的結果、將金鑰與數值進行比較。
NumericNotEquals	根據已否定的比對、將金鑰與數值進行比較。
數值資料	根據「大於」比對、將金鑰與數值進行比較。
NumericGreaterThang Equals	根據「大於或等於」比對、將金鑰與數值進行比較。
數字LessThan	根據「小於」比對、將金鑰與數值進行比較。
NumericLessThang Equals	根據「小於或等於」比對、將金鑰與數值進行比較。
布爾	根據「'true or假'」比對、將金鑰與布林值進行比較。
IP地址	比較金鑰與IP位址或IP位址範圍。
NotIppAddress	根據已否定的比對、將金鑰與IP位址或IP位址範圍進行比較。
null	檢查條件金鑰是否存在於目前的要求內容中。

支援的條件金鑰

類別	適用的條件金鑰	說明
IP營運者	AWS：來源Ip	將會與傳送要求的IP位址進行比較。可用於庫位或物件作業。 *附註：*如果S3要求是透過管理節點和閘道節點上的負載平衡器服務傳送、則這會與負載平衡器服務上游的IP位址進行比較。 附註：如果使用第三方、不透明的負載平衡器、則會比較該負載平衡器的IP位址。任何「X-Forwarded-for」標頭都會被忽略、因為無法確定其有效性。
資源/身分識別	AWS：使用者名稱	將會比較傳送者的使用者名稱、以從中傳送要求。可用於庫位或物件作業。

類別	適用的條件金鑰	說明
S3：清單儲存庫和 S3：listBucketVerions權限	S3：分隔符號	會比較「Get Bucket」或「Get Bucket Object versions」要求中指定的分隔符號參數。
S3：清單儲存庫和 S3：listBucketVerions權限	S3：金鑰上限	會比較「Get Bucket」或「Get Bucket Object版本」要求中指定的最大金鑰參數。
S3：清單儲存庫和 S3：listBucketVerions權限	S3：前置碼	會比較「Get Bucket」或「Get Bucket Object versions」要求中指定的前置字元參數。
S3：PuttObject	S3：物件鎖定剩餘保留天數	比較「x-amz-object-lock-retest-the-date」要求標頭中指定的保留截止日期、或是從庫位預設保留期間計算、以確保這些值符合下列要求的允許範圍： • 放置物件 • 放置物件-複製 • 啟動多部份上傳
S3：PuttObjectRetention	S3：物件鎖定剩餘保留天數	與「放置物件保留」要求中指定的保留截止日期進行比較、以確保其在允許的範圍內。

在原則中指定變數

您可以在原則中使用變數、在原則可用時填入原則資訊。您可以在「資源」元素中使用原則變數、也可以在「條件」元素中使用字串比較。

在此範例中、變數'${AWS:username}是資源元素的一部分：

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

在此範例中、變數'${AWS:username}是條件區塊中條件值的一部分：

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

變動	說明
「$｛AWS：來源Ip｝」	使用來源Ip金鑰作為提供的變數。
「$｛AWS：使用者名稱｝」	使用UserName金鑰做為提供的變數。
「$｛S3：prefix｝」	使用服務專屬的前置碼作為提供的變數。
「$｛S3：max金鑰｝」	使用服務專屬的最大金鑰作為提供的變數。
「${*}」	特殊字元。使用字元做為文字*字元。
「${?}」	特殊字元。使用字元做為字型？字元。
${$}	特殊字元。使用字元做為文字$字元。

建立需要特殊處理的原則

有時候原則可能會授與安全性危險或危險的權限、以便繼續執行作業、例如封鎖帳戶的root使用者。在原則驗證期間、不像Amazon、StorageGRID 執行「支援S3 REST API」的限制較少、但在原則評估期間同樣嚴格。

原則說明	原則類型	**Amazon**行為	運作方式**StorageGRID**
拒絕root帳戶的任何權限	鏟斗	有效且強制、但root使用者帳戶保留所有S3儲存區原則作業的權限	相同
拒絕對使用者/群組擁有任何權限	群組	有效且強制	相同
允許外部帳戶群組擁有任何權限	鏟斗	無效的主體	有效、但原則允許時、所有S3儲存區原則作業的權限都會傳回「不允許使用405方法」錯誤
允許外部帳戶root或使用者擁有任何權限	鏟斗	有效、但原則允許時、所有S3儲存區原則作業的權限都會傳回「不允許使用405方法」錯誤	相同
允許每個人都有權執行所有動作	鏟斗	有效、但所有S3儲存區原則作業的權限都會傳回異帳戶根目錄和使用者不允許的「405方法」錯誤	相同

原則說明	原則類型	**Amazon**行為	運作方式**StorageGRID**
拒絕所有人對所有動作的權限	鏟斗	有效且強制、但root使用者帳戶保留所有S3儲存區原則作業的權限	相同
主體是不存在的使用者或群組	鏟斗	無效的主體	有效
資源是不存在的S3儲存區	群組	有效	相同
主體是本機群組	鏟斗	無效的主體	有效
原則授予非擁有者帳戶（包括匿名帳戶）放置物件的權限	鏟斗	有效。物件由建立者帳戶擁有、且庫位原則不適用。建立者帳戶必須使用物件ACL來授與物件的存取權限。	有效。物件由庫位擁有者帳戶擁有。適用庫位政策。

一次寫入多讀（**WORM**）保護

您可以建立一次寫入多次讀取（WORM）儲存區、以保護資料、使用者定義的物件中繼資料、以及S3物件標記。您可以設定WORM儲存區、以允許建立新物件、並防止覆寫或刪除現有內容。請使用本文所述的其中一種方法。

為了確保覆寫永遠被拒絕、您可以：

- 在Grid Manager中，轉至* configuration **>** System*>* Grid options ，然後選中 Prevent Client Modification * 複選框。
- 套用下列規則和S3原則：
  - 將PuttOverwriteObject拒絕作業新增至S3原則。
  - 將刪除物件拒絕作業新增至S3原則。
  - 新增「允許放置物件」作業至S3原則。

若在S3原則中將刪除物件設為拒絕、則不會在存在「30天後歸零複本」等規則時、防止ILM刪除物件。

即使套用所有這些規則和原則、也無法防止並行寫入（請參閱情況A）。它們確實能防止連續完成的覆寫（請參閱情況B）。

情況**A**：並行寫入（不受保護）

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

情況**B**：連續完成覆寫（防範）

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

相關資訊

使用ILM管理物件

[建立需要特殊處理的原則]

如何利用ILM規則來管理物件StorageGRID

S3群組原則範例

S3原則範例

請利用本節的範例、針對StorageGRID 庫位和群組建構不需執行的存取原則。

S3儲存區政策範例

儲存區原則會指定原則附加的儲存區存取權限。儲存區原則是使用S3 PuttBucketPolicy API進行設定。

根據下列命令、可使用AWS CLI設定儲存區原則：

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

範例：允許每個人只讀存取儲存區

在此範例中、每個人（包括匿名）都可以列出儲存區中的物件、並對儲存區中的所有物件執行「Get Object」（取得物件）作業。所有其他作業都將遭拒。請注意、此原則可能並不特別實用、因為除了帳戶根以外、沒有其他人擁有寫入儲存區的權限。

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

範例：允許同一個帳戶中的每個人都擁有完整存取權、以及其他帳戶中的每個人只讀存取庫位

在此範例中、某個指定帳戶中的每個人都可以完整存取某個儲存區、而另一個指定帳戶中的每個人只能列出該儲存區、並對儲存區中以「共享/」物件金鑰字首開頭的物件執行GetObject作業。

在功能區中StorageGRID 、非擁有者帳戶所建立的物件（包括匿名帳戶）、均由庫位擁有者帳戶擁有。庫位原則適用於這些物件。

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

範例：允許每個人只讀存取儲存區、並由指定群組進行完整存取

在此範例中、每個人（包括匿名）都可以列出目標區段、並對目標區中的所有物件執行「Get Object」（取得物件）作業、而只有屬於指定帳戶中「市場行銷」群組的使用者才允許完整存取。

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

範例：如果用戶端位於**IP**範圍、則允許每個人讀取及寫入儲存區的存取權

在此範例中、每個人（包括匿名）都可以列出儲存區、並在儲存區中的所有物件上執行任何物件作業、前提是要求來自指定的IP範圍（54.240.143.0至54.240.143.255、但54.240.143.188除外）。所有其他作業都會遭到拒絕、而且IP範圍以外的所有要求都會遭到拒絕。

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

範例：允許特定同盟使用者專屬完整存取儲存區

在此範例中、聯盟使用者Alex可以完整存取「範例桶」儲存區及其物件。所有其他使用者、包括「root」、都會明確拒絕所有作業。不過請注意、「root」永遠不會被拒絕存取權限來放置/取得/刪除BucketPolicy。

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

範例：**PuttOverwriteObject**權限

在此範例中、「推桿套用物件」和「刪除物件」的「延遲」效果可確保無人能夠覆寫或刪除物件的資料、使用者定義的中繼資料和S3物件標記。

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

},
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}
```

相關資訊

在貯體上作業

S3群組原則範例

群組原則會指定原則所附加之群組的存取權限。政策中沒有「主要」元素、因為它是內含的。群組原則是使用租戶管理程式或API來設定。

範例：使用租戶管理程式設定群組原則

使用租戶管理程式新增或編輯群組時、您可以選取建立群組原則的方式、以定義此群組中哪些S3存取權限成員

將擁有的群組原則、如下所示：

- 無**S3**存取：預設選項。此群組中的使用者沒有S3資源的存取權、除非使用資源桶原則授予存取權。如果選取此選項、預設只有root使用者可以存取S3資源。
- 唯讀存取：此群組中的使用者擁有S3資源的唯讀存取權。例如、此群組中的使用者可以列出物件並讀取物件資料、中繼資料和標記。選取此選項時、唯讀群組原則的Json字串會出現在文字方塊中。您無法編輯此字串。
- 完整存取：此群組中的使用者可完整存取S3資源、包括儲存區。選取此選項時、會在文字方塊中顯示完整存取群組原則的Json字串。您無法編輯此字串。
- 自訂：群組中的使用者會被授予您在文字方塊中指定的權限。

  在此範例中、群組成員只能在指定的儲存區中列出及存取其特定資料夾（金鑰首碼）。

範例：允許群組完整存取所有儲存區

在此範例中、除非庫位原則明確拒絕、否則群組的所有成員都可以完整存取租戶帳戶擁有的所有庫位。

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

範例：允許群組唯讀存取所有儲存區

在此範例中、除非資源庫原則明確拒絕、否則群組的所有成員都擁有S3資源的唯讀存取權。例如、此群組中的使用者可以列出物件並讀取物件資料、中繼資料和標記。

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

範例：允許群組成員只能完整存取儲存庫中的「**'folder"**」

在此範例中、群組成員只能在指定的儲存區中列出及存取其特定資料夾（金鑰首碼）。請注意、在決定這些資料夾的隱私權時、應考慮其他群組原則和儲存區原則的存取權限。

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

相關資訊

使用租戶帳戶

設定REST API的安全性

您應該檢閱針對REST API實作的安全措施、並瞭解如何保護系統安全。

如何為REST API提供安全性StorageGRID

您應該瞭解StorageGRID 什麼是讓此系統為REST API實作安全性、驗證和授權。

使用下列安全措施。StorageGRID

- 如果已針對負載平衡器端點設定HTTPS、則用戶端與負載平衡器服務的通訊會使用HTTPS。

  當您設定負載平衡器端點時、可以選擇啟用HTTP。例如、您可能想要使用HTTP進行測試或其他非正式作業用途。如StorageGRID 需詳細資訊、請參閱《關於管理功能的說明》。

- 根據預設StorageGRID 、使用HTTPS與儲存節點進行用戶端通訊、並在閘道節點上使用CLB服務。

  您可以選擇性地為這些連線啟用HTTP。例如、您可能想要使用HTTP進行測試或其他非正式作業用途。如StorageGRID 需詳細資訊、請參閱《關於管理功能的說明》。

  CLB服務已過時。

- 支援使用TLS加密支援不支援的客戶端與StorageGRID 之通訊。
- 無論負載平衡器端點是設定為接受HTTP或HTTPS連線、網格內負載平衡器服務與儲存節點之間的通訊都會加密。
- 用戶端必須提供HTTP驗證標頭StorageGRID 給才能執行REST API作業。

安全性憑證與用戶端應用程式

用戶端可連線至閘道節點或管理節點上的負載平衡器服務、直接連線至儲存節點、或連線至閘道節點上的CLB服務。

在任何情況下、用戶端應用程式都可以使用網格管理員上傳的自訂伺服器憑證或StorageGRID 由該系統產生的憑證來建立TLS連線：

- 當用戶端應用程式連線至負載平衡器服務時、應用程式會使用針對用於建立連線的特定負載平衡器端點所設定的憑證來執行此作業。每個端點都有自己的憑證、可以是由網格管理員上傳的自訂伺服器憑證、也可以是網格管理員StorageGRID 在設定端點時產生的憑證。
- 當用戶端應用程式直接連線至儲存節點或閘道節點上的CLB服務時、它們會使用StorageGRID 安裝時（由系統憑證授權單位簽署）為儲存節點產生的系統產生伺服器憑證、 或是由網格管理員提供的單一自訂伺服器憑證。

用戶端應設定為信任已簽署其用於建立TLS連線之任何憑證的憑證授權單位。

如StorageGRID 需設定負載平衡器端點的相關資訊、以及新增單一自訂伺服器憑證以供TLS連線直接連線至儲存節點或閘道節點上的CLB服務的相關指示、請參閱《for Administering》（管理功能）。

摘要

下表顯示S3和Swift REST API如何實作安全性問題：

安全問題	**REST API**的實作
連線安全性	TLS
伺服器驗證	由系統CA或系統管理員提供的自訂伺服器憑證簽署的X・509伺服器憑證
用戶端驗證	• S3：S3帳戶（存取金鑰ID和秘密存取金鑰） • Swift：Swift帳戶（使用者名稱和密碼）
用戶端授權	• S3：貯體所有權及所有適用的存取控制原則 • Swift：系統管理員角色存取

相關資訊

管理StorageGRID

TLS程式庫支援的雜湊和加密演算法

支援一套有限的加密套件、用戶端應用程式可在建立傳輸層安全性（TLS）工作階段時使用。StorageGRID

支援的**TLS**版本

支援TLS 1.2和TLS 1.3。StorageGRID

不再支援SSLv3和TLS 1.1（或更早版本）。

支援的加密套件

TLS版本	加密套件的**IANA**名稱
1.2	TLS_ECDHE_RSA_with _AES-256_GCM_SHA384
1.2	TLS_ECDHE_RSA_with _CHACHA20_POLY1305_SHA256
1.2	TLS_ECDHE_RSA_with _AES-122_GCM_SHA256
1.3	TLS_AES-256_GCM_SHA384
1.3	TLS_CHACHA20_POLY1305_SHA256
1.3	TLS_AES-128_GCM_SHA256

已過時的加密套件

下列加密套件已過時。未來版本將會移除對這些密碼的支援。

IANA名稱
TLS_RSA_AT_AES-122_GCM_SHA256
TLS_RSA_AT_AES-256_GCM_SHA384

相關資訊

如何設定用戶端連線

監控與稽核作業

您可以檢視整個網格或特定節點的交易趨勢、來監控用戶端作業的工作負載和效率。您可以使用稽核訊息來監控用戶端作業和交易。

監控物件擷取和擷取速率

您可以監控物件擷取和擷取速率、以及物件計數、查詢和驗證的度量。您可以檢視用戶端應用程式在StorageGRID 讀取、寫入及修改物件時、成功和失敗的嘗試次數。

步驟

1. 使用登入Grid Manager 支援的網頁瀏覽器。
2. 在儀表板上、找到「傳輸協定作業」區段。

   本節概述StorageGRID 您的一套系統執行的用戶端作業數量。在過去兩分鐘內平均傳輸協定速率。

3. 選擇*節點*。
4. 在節點首頁（部署層級）中、按一下*負載平衡器*索引標籤。

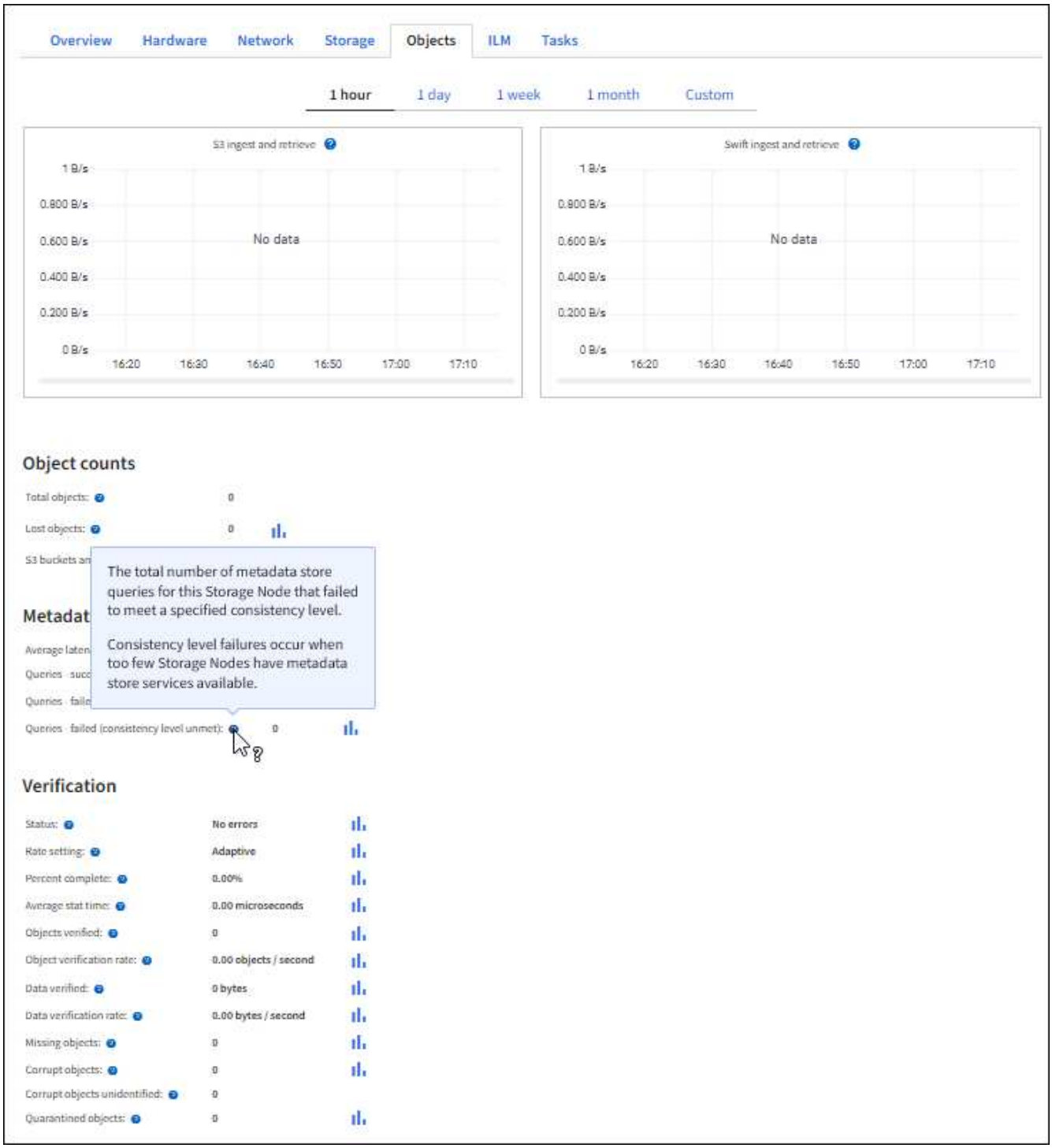
   這些圖表顯示了導向至網格內負載平衡器端點的所有用戶端流量趨勢。您可以選擇以小時、天、週、月或年為單位的時間間隔、 您也可以套用自訂時間間隔。

5. 在節點首頁（部署層級）中、按一下*物件*索引標籤。

   此圖表以StorageGRID 每秒位元組數和總位元組數顯示整個系統的擷取和擷取速率。您可以選擇以小時、天、週、月或年為單位的時間間隔、 您也可以套用自訂時間間隔。

6. 若要查看特定儲存節點的資訊、請從左側清單中選取節點、然後按一下「物件」索引標籤。

   此圖表顯示此儲存節點的物件擷取和擷取速率。此索引標籤也包含物件計數、查詢和驗證的度量。您可以按一下標籤來查看這些度量的定義。



7. 如果您想要更詳細的資料：
   a. 選取*支援*>*工具*>*網格拓撲*。
   b. 選擇*站台_*>*總覽*>*主選項*。

      「API作業」區段會顯示整個網格的摘要資訊。

   c. 選擇「儲存節點_」>「最大」>「用戶端應用程式_」>「總覽」>「主要」

      「作業」區段會顯示所選儲存節點的摘要資訊。

存取及檢閱稽核記錄

稽核訊息是StorageGRID 由支援服務產生、並儲存在文字記錄檔中。稽核日誌中的API專屬稽核訊息可提供關鍵的安全性、作業和效能監控資料、協助您評估系統的健全狀況。

您需要的產品

- 您擁有特定的存取權限。
- 您有「pes密碼」檔案。
- 您知道管理節點的IP位址。

關於這項工作

作用中的稽核記錄檔名為「稽核記錄」、儲存在管理節點上。

一天只要儲存一次作用中的audit.log檔案、就會啟動新的「稽核記錄」檔案。儲存檔案的名稱會以「*edy-mm-dd.txt*」格式指出儲存時間。

一天後、儲存的檔案會壓縮並重新命名、格式為「*youty-mm-dd.txt.gz*」、保留原始日期。

此範例顯示使用中的「稽核記錄」檔案、前一天的檔案（「2018年4月15日」）、以及前一天的壓縮檔案（「2018年4月14日.tx.gz」）。

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

步驟

1. 登入管理節點：
   a. 輸入下列命令：「sh admin@_primary管理節點IP」
   b. 輸入「passwords.txt」檔案中所列的密碼。
2. 移至包含稽核記錄檔的目錄：

   ```
   cd /var/local/audit/export
   ```

3. 視需要檢視目前或已儲存的稽核記錄檔。

稽核記錄中追蹤的**S3**作業

在不完整的稽核記錄中、會追蹤多項庫位作業和物件作業StorageGRID 。

稽核記錄中追蹤的庫位作業

- 刪除時段
- 刪除庫位標記

- 刪除多個物件
- Get Bucket（列出物件）
- 取得Bucket物件版本
- 取得庫位標記
- 鏟斗
- 放入鏟斗
- 符合資源需求
- 置入庫位標記
- 放入資源桶版本管理

稽核記錄中追蹤的物件作業

- 完成多部份上傳
- 上傳零件（ILM規則使用嚴格或平衡的擷取行為時）
- 上傳零件-複本（ILM規則使用嚴格或平衡的擷取行為時）
- 刪除物件
- 取得物件
- 標頭物件
- POST物件還原
- 放置物件
- 放置物件-複製

相關資訊

在貯體上作業

物件上的作業

作用中、閒置及並行**HTTP**連線的優點

如何設定HTTP連線、可能會影響StorageGRID 到整個系統的效能。組態會因HTTP連線為作用中或閒置狀態、或是您同時有多個連線而有所不同。

您可以找出下列類型HTTP連線的效能優勢：

- 閒置HTTP連線
- 作用中HTTP連線
- 並行HTTP連線

保持閒置**HTTP**連線開啟的優點

即使用戶端應用程式閒置、您仍應保持HTTP連線開啟、以允許用戶端應用程式透過開放式

連線執行後續交易。根據系統測量與整合體驗、您應將閒置的HTTP連線保持開啟狀態最長10分鐘。可能會自動關閉持續開啟和閒置超過10分鐘的HTTP連線。StorageGRID

開放式和閒置的HTTP連線提供下列優點：

- 縮短延遲時間、從StorageGRID 由整個過程中、由整個過程中的資訊系統判斷它必須執行HTTP交易到StorageGRID 整個系統能夠執行交易的時間

  縮短延遲是主要優勢、尤其是在建立TCP/IP和TLS連線所需的時間內。

- 使用先前執行的傳輸來初始化TCP/IP慢速啟動演算法、藉此提高資料傳輸率
- 即時通知多種故障情況、可中斷用戶端應用程式與StorageGRID 該系統之間的連線

判斷閒置連線開啟的時間長度、是在與現有連線相關的慢速啟動優點與內部系統資源連線的理想分配之間取得平衡。

作用中**HTTP**連線的優點

對於直接連線至儲存節點或閘道節點上的CLB服務（已過時）、您應該將作用中HTTP連線的持續時間限制在最長10分鐘內、即使HTTP連線持續執行交易。

判斷連線應保持開啟的最長時間、是在連線持續性的優點與連線至內部系統資源的理想分配之間取得平衡。

對於用戶端連線至儲存節點或CLB服務、限制作用中HTTP連線可提供下列優點：

- 在StorageGRID 整個支援過程中實現最佳負載平衡。

  使用CLB服務時、您應避免長時間使用的TCP/IP連線、以最佳化StorageGRID 整個VMware系統的負載平衡。您應該設定用戶端應用程式來追蹤每個HTTP連線的持續時間、並在設定時間後關閉HTTP連線、以便重新建立及重新平衡HTTP連線。

  CLB服務會在StorageGRID 用戶端應用程式建立HTTP連線時、平衡整個整個作業系統的負載。隨著時間推移、隨著負載平衡需求的變更、HTTP連線可能不再是最佳狀態。當用戶端應用程式為每筆交易建立獨立的HTTP連線時、系統會執行最佳負載平衡、但這會使持續連線所帶來的更多寶貴成果喪失價值。

  CLB服務已過時。

- 允許用戶端應用程式將HTTP交易導向具有可用空間的LDR服務。
- 可啟動維護程序。

  部分維護程序只會在所有進行中的HTTP連線完成後才會開始。

對於連接到負載平衡器服務的用戶端連線、限制開放連線的持續時間、有助於讓部分維護程序立即啟動。如果用戶端連線的持續時間不受限制、可能需要幾分鐘的時間才能自動終止作用中的連線。

並行**HTTP**連線的優點

您應該StorageGRID 將多個TCP/IP連線保持開放狀態、以允許平行處理、進而提升效能。最佳的平行連線數量取決於各種因素。

並行HTTP連線提供下列優點：

- 縮短延遲時間

  交易可以立即開始、而非等待其他交易完成。

- 提高處理量

  此系統可執行平行交易、並提高集合交易處理量。StorageGRID

用戶端應用程式應建立多個HTTP連線。當用戶端應用程式必須執行交易時、它可以選取並立即使用任何目前未處理交易的已建立連線。

在StorageGRID 效能開始降級之前、每個支援系統的拓撲在並行交易和連線方面都有不同的尖峰處理量。尖峰處理量取決於運算資源、網路資源、儲存資源和WAN連結等因素。此外、伺服器和服務的數量、StorageGRID 以及支援哪些應用程式、也是因素。

支援多種用戶端應用程式的系統。StorageGRID當您決定用戶端應用程式所使用的並行連線數目上限時、請謹記這一點。如果用戶端應用程式包含多個軟體實體、每個實體都會建立StorageGRID 與該系統的連線、您應該新增整個實體之間的所有連線。在下列情況下、您可能必須調整並行連線的最大數量：

- 此系統的拓撲會影響系統可支援的並行交易和連線數量上限。StorageGRID
- 在StorageGRID 頻寬有限的網路上與該系統互動的用戶端應用程式、可能必須降低並行度、以確保在合理的時間內完成個別交易。
- 當許多用戶端應用程式共用StorageGRID 該系統時、您可能必須減少並行處理的程度、以避免超出系統限制。

分隔**HTTP**連線集區以進行讀取和寫入作業

您可以使用不同的HTTP連線集區進行讀取和寫入作業、並控制每個集區的使用量。獨立的HTTP連線集區可讓您更有效地控制交易並平衡負載。

用戶端應用程式可建立擷取主導（讀取）或儲存主導（寫入）的負載。有了個別的HTTP連線集區、即可針對讀寫交易調整每個集區的專屬容量、以處理讀寫交易。

使用**Swift**

使用**Swift**：總覽

用戶端應用程式可以使用OpenStack Swift API與StorageGRID 該系統進行介面。

支援下列Swift和HTTP的特定版本。StorageGRID

項目	版本
Swift規格	OpenStack Swift Object Storage API v1（截至2015年11月）

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

相關資訊

"OpenStack：物件儲存API"

Swift API支援的歷史**StorageGRID** 記錄

您應該注意StorageGRID 到支援Swift REST API的功能有所變更。

版本	註解
11.6%	略有編輯變更。
11.5	移除弱一致性控制。將改用可用的一致性層級。
11.4	新增對TLS 1.3的支援、並更新支援的TLS加密套件清單。CLB已過時。新增ILM與一致性設定之間相互關係的說明。
11.3	更新的「放置物件」作業、說明ILM規則在擷取時使用同步放置的影響（擷取行為的平衡和嚴格選項）。新增使用負載平衡器端點或高可用度群組的用戶端連線說明。更新支援的TLS加密套件清單。不再支援TLS 1.1密碼。
11.2	文件的編輯略有變更。
11.1.	新增使用HTTP的支援、可將Swift用戶端連線至網格節點。更新一致性控制的定義。
11.0	新增每個租戶帳戶的1、000個容器支援。
10.3.1	文件的管理更新與修正。移除設定自訂伺服器憑證的區段。
10.2	Swift API的初始支援StorageGRID 、由整個系統提供。目前支援的版本為OpenStack Swift Object Storage API v1。

如何實作**Swift REST API StorageGRID**

用戶端應用程式可以使用Swift REST API呼叫來連線至儲存節點和閘道節點、以建立容

器、以及儲存和擷取物件。如此一來、專為OpenStack Swift開發的服務導向應用程式就能與StorageGRID 由該系統提供的內部部署物件儲存設備連線。

Swift物件管理

在StorageGRID Swift物件被擷取到整個物件系統之後、這些物件會由系統作用中ILM原則中的資訊生命週期管理（ILM）規則來管理。ILM規則和原則決定StorageGRID 了如何建立及散佈物件資料複本、以及如何長期管理這些複本。例如、ILM規則可能會套用至特定Swift容器中的物件、並可能指定將多個物件複本儲存至數個資料中心、保留一段時間。

如果StorageGRID 您需要瞭解網格的ILM規則和原則如何影響Swift租戶帳戶中的物件、請聯絡您的管理員。

衝突的用戶端要求

衝突的用戶端要求（例如兩個寫入同一個金鑰的用戶端）會以「最新致勝」的方式解決。「最新致勝」評估的時間取決於StorageGRID VMware系統何時完成指定的要求、而非Swift用戶端何時開始作業。

一致性保證與控管

根據預設、StorageGRID 針對新建立的物件、提供寫入後讀取一致性、並在物件更新和執行前置作業時提供最終一致性。任何「Get」追蹤成功完成的「PUT」、都能讀取新寫入的資料。覆寫現有物件、更新中繼資料及刪除的動作最終一致。覆寫通常需要幾秒鐘或幾分鐘才能傳播、但可能需要15天的時間。

利用此功能、您也可以控制每個容器的一致性。StorageGRID您可以變更一致性控制、以根據應用程式的需求、在物件的可用度與不同儲存節點和站台之間的物件一致性之間取得平衡。

相關資訊

使用ILM管理物件

取得Container一致性要求

放置容器一致性要求

實作**Swift REST API**的建議

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

針對不存在物件的使用者提出建議

如果您的應用程式經常檢查某個物件是否存在於您預期該物件實際上不存在的路徑中、您應該使用「可用」一致性控制。例如、如果您的應用程式在執行放置作業之前、先對某個位置執行頭作業、則應使用「可用」一致性控制。

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

您可以使用放置容器一致性要求、為每個容器設定「可用」一致性控制。

物件名稱建議

對於StorageGRID 以VMware 11.4或更新版本建立的容器、不再需要限制物件名稱以符合效能最佳實務做法。例如、您現在可以將隨機值用於物件名稱的前四個字元。

若容器是在StorageGRID 版本早於物件名稱的版本中建立、請繼續遵循以下建議：

- 您不應使用隨機值做為物件名稱的前四個字元。這與前AWS關於名稱前置詞的建議不同。您應該改用非隨機、非獨特的前置詞、例如「image」。
- 如果您遵循前一項AWS建議、在名稱前置字元中使用隨機和獨特的字元、則應該在物件名稱前置一個目錄名稱。也就是使用此格式：

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

而非此格式：

```
mycontainer/f8e3-image3132.jpg
```

「range Reads」建議

如果選擇*壓縮儲存物件*選項（組態>*系統*>*網格選項*）、Swift用戶端應用程式應避免執行指定要傳回位元組範圍的Get物件作業。這些「範圍讀取」作業效率不彰、因為StorageGRID 必須有效解壓縮物件才能存取所要求的位元組。從非常大的物件要求少量位元組的「Get Object」（取得物件）作業效率特別低；例如、從50 GB壓縮物件讀取10 MB範圍的效率非常低。

如果從壓縮物件讀取範圍、用戶端要求可能會逾時。

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

相關資訊

取得Container一致性要求

放置容器一致性要求

管理StorageGRID

設定租戶帳戶和連線

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

建立及設定Swift租戶帳戶

Swift API用戶端必須先有Swift租戶帳戶、才能將物件儲存及擷取StorageGRID 到靜止不動的地方。每個租戶帳戶都有自己的帳戶ID、群組和使用者、以及容器和物件。

Swift租戶帳戶是StorageGRID 由使用Grid Manager或Grid Management API的資訊網管理員所建立。

建立Swift租戶帳戶時、網格管理員會指定下列資訊：

- 租戶的顯示名稱（租戶的帳戶ID會自動指派、無法變更）

- 或者、租戶帳戶的儲存配額、也就是租戶物件可用的GB、TB或PB上限。租戶的儲存配額代表邏輯容量（物件大小）、而非實體容量（磁碟大小）。
- 如果StorageGRID 不使用單一登入（SSO）進行支援、則租戶帳戶是使用自己的身分識別來源、還是共用網格的身分識別來源、以及租戶本機root使用者的初始密碼。
- 如果啟用SSO、則哪個聯盟群組具有root存取權限可設定租戶帳戶。

建立Swift租戶帳戶之後、具有「根存取」權限的使用者就能存取租戶管理程式來執行下列工作：

- 設定身分識別聯盟（除非身分識別來源與網格共用）、以及建立本機群組和使用者
- 監控儲存使用量

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

相關資訊

管理StorageGRID

使用租戶帳戶

支援的Swift API端點

如何設定用戶端連線

網格管理員會做出組態選擇、影響Swift用戶端連線StorageGRID 至以儲存及擷取資料的方式。建立連線所需的特定資訊取決於所選的組態。

用戶端應用程式可連線至下列任一項目、以儲存或擷取物件：

- 管理節點或閘道節點上的負載平衡器服務、或是管理節點或閘道節點之高可用度（HA）群組的虛擬IP位址（可選）
- 閘道節點上的CLB服務、或是閘道節點高可用度群組的虛擬IP位址（可選）

> CLB服務已過時。在發佈版推出之前設定的用戶端StorageGRID 、可以繼續在閘道節點上使用CLB服務。所有其他仰賴StorageGRID 以提供負載平衡的用戶端應用程式、都應該使用負載平衡器服務進行連線。

- 儲存節點、無論是否有外部負載平衡器

設定StorageGRID 功能時、網格管理員可以使用Grid Manager或Grid Management API來執行下列步驟、這些步驟都是選用的：

1. 設定負載平衡器服務的端點。

   您必須設定端點以使用負載平衡器服務。管理節點或閘道節點上的負載平衡器服務會將傳入的網路連線從用戶端應用程式分散到儲存節點。建立負載平衡器端點時StorageGRID 、系統管理員會指定連接埠號碼、端點是否接受HTTP或HTTPS連線、使用端點的用戶端類型（S3或Swift）、以及用於HTTPS連線的憑證（若適用）。

2. 設定不受信任的用戶端網路。

   如果StorageGRID 某個節點的用戶端網路設定為不受信任、則該節點僅接受用戶端網路上明確設定為負載平衡器端點之連接埠的傳入連線。

3. 設定高可用度群組。

   如果系統管理員建立HA群組、則多個管理節點或閘道節點的網路介面會置於主動備份組態中。用戶端連線是使用HA群組的虛擬IP位址進行。

如需每個選項的詳細資訊、請參閱《關於管理StorageGRID 功能的說明》。

摘要：用於用戶端連線的**IP**位址和連接埠

用戶端應用程式StorageGRID 會使用網格節點的IP位址和該節點上服務的連接埠號碼來連線至功能區。如果已設定高可用度（HA）群組、用戶端應用程式就可以使用HA群組的虛擬IP位址進行連線。

建立用戶端連線所需的資訊

下表摘要說明用戶端連線StorageGRID 至靜態的不同方式、以及每種連線類型所使用的IP位址和連接埠。如StorageGRID 需更多資訊、請聯絡您的管理員、或參閱《管理StorageGRID 》的說明、以瞭解如何在Grid Manager中找到這些資訊。

連線位置	用戶端連線的服務	**IP** 位址	連接埠
HA群組	負載平衡器	HA群組的虛擬IP位址	• 負載平衡器端點連接埠
HA群組	CLB 附註： CLB服務已過時。	HA群組的虛擬IP位址	預設Swift連接埠： • HTTPS：8083 • HTTP：8085
管理節點	負載平衡器	管理節點的IP位址	• 負載平衡器端點連接埠
閘道節點	負載平衡器	閘道節點的IP位址	• 負載平衡器端點連接埠
閘道節點	CLB 附註： CLB服務已過時。	閘道節點的IP位址 *附註：*根據預設、不會啟用CLB和LDR的HTTP連接埠。	預設Swift連接埠： • HTTPS：8083 • HTTP：8085
儲存節點	LdR	儲存節點的IP位址	預設Swift連接埠： • HTTPS：18083 • HTTP：18085

範例

若要將Swift用戶端連線至閘道節點HA群組的負載平衡器端點、請使用結構如下所示的URL：

- https://*VIP-of-HA-group:LB-endpoint-port*`

例如、如果HA群組的虛擬IP位址為192.0.2.6、而Swift負載平衡器端點的連接埠號碼為104444、則Swift用戶端可使用下列URL連線StorageGRID 到Sender:

- https://192.0.2.6:10444`

您可以為用戶端用來連線StorageGRID 到靜態的IP位址設定DNS名稱。請聯絡您的本機網路管理員。

決定使用**HTTPS**或**HTTP**連線

使用負載平衡器端點進行用戶端連線時、必須使用為該端點指定的傳輸協定（HTTP或HTTPS）來建立連線。若要在用戶端連線至儲存節點或閘道節點上的CLB服務時使用HTTP、您必須啟用它的使用。

根據預設、當用戶端應用程式連線至閘道節點上的儲存節點或CLB服務時、它們必須使用加密的HTTPS進行所有連線。或者、您也可以選取「Grid Manager（網格管理器）」中的*「Enable HTTP Connection* Grid（啟用HTTP連線*網格）」選項、來啟用較不安全的HTTP連線。例如、用戶端應用程式在非正式作業環境中測試與儲存節點的連線時、可能會使用HTTP。

> 啟用正式作業網格的HTTP時請務必小心、因為要求會以不加密的方式傳送。

> CLB服務已過時。

如果選取*「啟用HTTP連線*」選項、則用戶端的HTTP連接埠必須與HTTPS使用的連接埠不同。請參閱「管理StorageGRID 功能」的說明。

相關資訊

管理StorageGRID

在**Swift API**組態中測試連線

您可以使用Swift CLI來測試與StorageGRID 該系統的連線、並驗證您是否可以讀取物件並將物件寫入系統。

您需要的產品

- 您必須下載並安裝python swiftClient、Swift命令列用戶端。

  "SwiftStack：Python-swiftClient"

- 您必須在StorageGRID 整個作業系統中擁有Swift租戶帳戶。

關於這項工作

如果您尚未設定安全性、則必須將「不安全」旗標新增至這些命令。

步驟

1. 查詢StorageGRID 資訊URL以進行您的NetApp Swift部署：

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/info
capabilities
```

這足以測試您的Swift部署是否正常運作。若要儲存物件以進一步測試帳戶組態、請繼續執行其他步驟。

2. 將物件放入容器：

```
touch test_object
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
upload test_container test_object
--object-name test_object
```

3. 取得容器以驗證物件：

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
list test_container
```

4. 刪除物件：

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
delete test_container test_object
```

5. 刪除容器：

```
swift
-U `<_Tenant_Account_ID:Account_User_Name_>`
-K `<_User_Password_>`
-A `\https://<_FQDN_ | _IP_>:<_Port_>/auth/v1.0'
delete test_container
```

相關資訊

建立及設定Swift租戶帳戶

設定REST API的安全性

Swift REST API支援的作業

此系統支援OpenStack Swift API的大部分作業。StorageGRID在將Swift REST API用戶端與StorageGRID NetApp整合之前、請先檢閱帳戶、容器和物件作業的實作詳細資料。

支援的作業StorageGRID

支援下列Swift API作業：

- 帳戶營運
- 容器作業
- 物件作業

所有作業的通用回應標頭

根據OpenStack Swift Object Storage API v1的定義、此系統可實作所有支援作業的通用標頭。StorageGRID

相關資訊

"OpenStack：物件儲存API"

支援的Swift API端點

支援下列Swift API端點：資訊URL、驗證URL及儲存URL。StorageGRID

資訊URL

您可以StorageGRID 使用/info路徑、向Swift基礎URL發出Get要求、藉此判斷執行過程的功能和限制。

「https://*FQDN*|*Node IP*：*Swift Port*/info/」

在要求中：

- 「_FQDN」是完整網域名稱。
- 「節點IP」是StorageGRID 指儲存節點或位於該網路上之閘道節點的IP位址。
- 「Swift Port_」是儲存節點或閘道節點上用於Swift API連線的連接埠號碼。

例如、下列資訊URL會向IP位址為10.99.106.103且使用連接埠18083的儲存節點要求資訊。

https://10.99.106.103:18083/info/`

回應內容包括Swift實作的功能、即Json字典。用戶端工具可剖析Json回應、判斷實作的功能、並將其作為後續儲存作業的限制。

Swift的支援功能可未經驗證存取資訊URL。StorageGRID

驗證URL

用戶端可以使用Swift驗證URL來驗證租戶帳戶使用者身分。

「https://*FQDN*|*Node IP*：*Swift Port*/auth/v1.0 /」

您必須提供租戶帳戶ID、使用者名稱和密碼做為「X-AUTH使用者」和「X-AUTH金鑰」要求標頭中的參數、如下所示：

「X-AUuth使用者：*Tenant_Account_ID*：使用者名稱」

「X-AUTH金鑰：*Password*」

在要求標頭中：

- 「*Tenant_Account_ID*」是StorageGRID 指在建立Swift租戶時、由支援部指派的帳戶ID。這是租戶管理員登入頁面上使用的相同租戶帳戶ID。
- 「*usernam_*」是租戶使用者在租戶管理程式中建立的名稱。此使用者必須屬於具有Swift Administrator權限的群組。租戶的root使用者無法設定為使用Swift REST API。

  如果租戶帳戶已啟用Identity Federation、請提供LDAP伺服器的聯盟使用者名稱和密碼。或者、提供LDAP使用者的網域名稱。例如：

  「X-AUTH使用者：*Tenant_Account_ID*：使用者名稱@網域名稱」

- 「密碼」是租戶使用者的密碼。使用者密碼是在租戶管理程式中建立及管理的。

成功驗證要求的回應會傳回儲存URL和驗證權杖、如下所示：

「X-Storage-URL： https://FQDN|Node_ip:Swift連接埠/v1/Tenant_Account_ID`

「X-AUTH-Token：*token*」

「X-Storage-Token：*token*」

根據預設、權杖自產生時間起24小時內有效。

會針對特定租戶帳戶產生權杖。一個帳戶的有效權杖並未授權使用者存取另一個帳戶。

儲存URL

用戶端應用程式可以發出Swift REST API呼叫、以便針對閘道節點或儲存節點執行支援的帳戶、容器和物件作業。儲存要求會被定址至驗證回應中傳回的儲存URL。要求也必須包含從驗證要求傳回的X-auth-Token標頭和值。

https://FQDN |*IP*：*Swift*連接埠/v1/*Tenant_Account_ID*

「X-AUTH-Token：*token*」

有些儲存回應標頭包含使用量統計資料、可能無法反映最近修改物件的準確數字。這些標頭可能需要幾分鐘的時間才能顯示準確的數字。

下列帳戶和容器作業的回應標頭是包含使用統計資料的範例：

- 「X-Account-bytes -已用」
- 「X-Account-Object-Count」
- 「X-Container-bytes -已用」
- 「X-Container-Object-Count」

相關資訊

設定租戶帳戶和連線

帳戶營運

容器作業

物件作業

帳戶營運

下列Swift API作業會在帳戶上執行。

取得帳戶

此作業會擷取與帳戶和帳戶使用量統計資料相關的容器清單。

需要下列要求參數：

- 「帳戶」

需要下列要求標頭：

- 「X-AUTH-Token」

下列支援的要求查詢參數為選用項目：

- "限制者"
- "end_market"
- 格式化
- 「限制」
- 《馬拉克人》
- 前置詞

如果找到帳戶且沒有容器或容器清單為空白、成功執行會傳回下列標頭「HTTP / 1.1 204無內容」回應；如果找到帳戶且容器清單為非空白、則會傳回「HTTP / 1.1 200 OK」回應：

- 「Accept-Range-」
- 《內容長度》
- 「內容類型」

- '日期'
- 「X-Account-bytes -已用」
- 「X-Account-Container-Count」
- 「X-Account-Object-Count」
- 「X-Timestamp'」
- 「X-trans-ID」

總公司帳戶

此作業會從Swift帳戶擷取帳戶資訊和統計資料。

需要下列要求參數：

- 「帳戶」

需要下列要求標頭：

- 「X-AUTH-Token」

成功執行會傳回下列標頭、並顯示「HTTP / 1.1 204無內容」回應：

- 「Accept-Range-」
- 《內容長度》
- '日期'
- 「X-Account-bytes -已用」
- 「X-Account-Container-Count」
- 「X-Account-Object-Count」
- 「X-Timestamp'」
- 「X-trans-ID」

相關資訊

監控與稽核作業

容器作業

每個Swift帳戶最多可支援1、000個容器。StorageGRID下列Swift API作業會在Container上執行。

刪除容器

此作業會從StorageGRID Swift帳戶的一個空容器中移除一個位在整個系統中的容器。

需要下列要求參數：

- 「帳戶」

- 《Container》

需要下列要求標頭：

- 「X-AUTH-Token」

成功執行會傳回下列標頭、並顯示「HTTP / 1.1 204無內容」回應：

- 《內容長度》
- 「內容類型」
- '日期'
- 「X-trans-ID」

取得**Container**

此作業會擷取與容器相關聯的物件清單、以及StorageGRID 物件統計資料和元資料在一個作業系統中。

需要下列要求參數：

- 「帳戶」
- 《Container》

需要下列要求標頭：

- 「X-AUTH-Token」

下列支援的要求查詢參數為選用項目：

- "限制者"
- "end_market"
- 格式化
- 「限制」
- 《馬拉克人》
- 路徑
- 前置詞

成功執行會傳回下列標頭、並顯示「HTTP / 1.1 200成功」或「HTTP / 1.1 204無內容」回應：

- 「Accept-Range-」
- 《內容長度》
- 「內容類型」
- '日期'
- 「X-Container-bytes -已用」
- 「X-Container-Object-Count」

- 「X-Timestamp'」
- 「X-trans-ID」

頭端容器

此作業會從StorageGRID 作業系統擷取Container統計資料和中繼資料。

需要下列要求參數：

- 「帳戶」
- 《Container》

需要下列要求標頭：

- 「X-AUTH-Token」

成功執行會傳回下列標頭、並顯示「HTTP / 1.1 204無內容」回應：

- 「Accept-Range-」
- 《內容長度》
- '日期'
- 「X-Container-bytes -已用」
- 「X-Container-Object-Count」
- 「X-Timestamp'」
- 「X-trans-ID」

放入容器

此作業會在StorageGRID 一個不穩定系統中建立帳戶的容器。

需要下列要求參數：

- 「帳戶」
- 《Container》

需要下列要求標頭：

- 「X-AUTH-Token」

成功執行會傳回下列標頭、並顯示「HTTP / 1.1 201已建立」或「HTTP / 1.1 2已接受」（如果此帳戶下已存在該容器）回應：

- 《內容長度》
- '日期'
- 「X-Timestamp'」
- 「X-trans-ID」

Container名稱必須在StorageGRID lsname命名空間中是唯一的。如果該容器存在於其他帳戶下、則會傳回下列標頭：「HTTP / 1.1 409衝突」。

相關資訊

監控與稽核作業

物件作業

下列Swift API作業會在物件上執行。

刪除物件

此作業會從StorageGRID 作業系統刪除物件的內容和中繼資料。

需要下列要求參數：

- 「帳戶」
- 《Container》
- 「物件」

需要下列要求標頭：

- 「X-AUTH-Token」

成功執行會傳回下列回應標頭、並顯示「HTTP / 1.1 204無內容」回應：

- 《內容長度》
- 「內容類型」
- '日期'
- 「X-trans-ID」

處理刪除物件要求時StorageGRID 、功能區會嘗試立即從所有儲存位置移除物件的所有複本。如果成功、StorageGRID 則會立即將回應傳回給用戶端。如果無法在30秒內移除所有複本（例如、因為某個位置暫時無法使用）、StorageGRID 則將複本排入佇列以供移除、然後向用戶端指出成功。

如需如何刪除物件的詳細資訊、請參閱使用資訊生命週期管理來管理物件的指示。

Get物件

此作業會擷取物件內容、並從StorageGRID 一套系統取得物件中繼資料。

需要下列要求參數：

- 「帳戶」
- 《Container》
- 「物件」

需要下列要求標頭：

- 「X-AUTH-Token」

以下是選用的要求標頭：

- 「Accept-編碼」
- 「如果符合」
- 「If-Modified、自…」
- 「如果-無-比對」
- 《如果沒有修改過的自此》
- 《範圍》

成功執行會傳回下列標頭、並顯示「HTTP / 1.1 200 OK」回應：

- 「Accept-Range-」
- 只有在設定「內容處理」中繼資料後、才會傳回「內容處理」
- 只有在設定了「內容編碼」中繼資料之後、才會傳回「內容編碼」
- 《內容長度》
- 「內容類型」
- '日期'
- 《ETag》
- 「上次修改日期」
- 「X-Timestamp'」
- 「X-trans-ID」

標頭物件

此作業會從StorageGRID 作業系統擷取擷取物件的中繼資料和屬性。

需要下列要求參數：

- 「帳戶」
- 《Container》
- 「物件」

需要下列要求標頭：

- 「X-AUTH-Token」

成功執行會傳回下列標頭、並顯示「HTTP / 1.1 200 OK」回應：

- 「Accept-Range-」
- 只有在設定「內容處理」中繼資料後、才會傳回「內容處理」
- 只有在設定了「內容編碼」中繼資料之後、才會傳回「內容編碼」

- 《內容長度》
- 「內容類型」
- '日期'
- 《ETag》
- 「上次修改日期」
- 「X-Timestamp'」
- 「X-trans-ID」

放置物件

此作業會以資料和中繼資料建立新物件、或以StorageGRID 資料和中繼資料取代現有物件。

支援最多5 TiB（5、497、558、13880位元組）的物件。StorageGRID

> 衝突的用戶端要求（例如兩個寫入同一個金鑰的用戶端）會以「最新致勝」的方式解決。「最新致勝」評估的時間取決於StorageGRID VMware系統何時完成指定的要求、而非Swift用戶端何時開始作業。

需要下列要求參數：

- 「帳戶」
- 《Container》
- 「物件」

需要下列要求標頭：

- 「X-AUTH-Token」

以下是選用的要求標頭：

- 「內容處理」
- 「內容編碼」

  如果適用於物件的ILM規則會根據大小來篩選物件、並在擷取時使用同步放置（擷取行為的平衡或嚴格選項）、請勿使用chunked「Content-Encoding」（內容編碼）。

- 「傳輸編碼」

  如果適用於物件的ILM規則會根據大小來篩選物件、並在擷取時使用同步放置（擷取行為的平衡或嚴格選項）、則請勿使用壓縮或解開的「Transfer-Encoding」（傳輸編碼）。

- 《內容長度》

  如果ILM規則會根據大小篩選物件、並在擷取時使用同步位置、則必須指定「Content-Length」（內容長度）。

如果您不遵守這些「內容編碼」、「傳輸編碼」和「內容長度」準則、StorageGRID 那麼在物件判斷物件大小並套用ILM規則之前、必須先儲存物件。換句話說StorageGRID 、在擷取時、必須預設使用功能來建立物件的過渡複本。也就是StorageGRID 、對於內嵌行為、必須使用雙重認可選項。

如需同步放置和ILM規則的詳細資訊、請參閱使用資訊生命週期管理來管理物件的指示。

- 「內容類型」
- 《ETag》
- 「X-Object-Meta-<name\>'（物件相關中繼資料）

如果您要使用*使用者定義的建立時間*選項做為ILM規則的參考時間、您必須將該值儲存在名為「X-Object-Meta-creation-Time」的使用者定義標頭中。例如：

```
X-Object-Meta-Creation-Time: 1443399726
```

此欄位自1970年1月1日起計算為秒數。

- 「X-Storage-Class：縮減冗餘」

如果符合擷取物件的ILM規則指定「雙重認可」或「平衡」的擷取行為、則此標頭會影響StorageGRID 到所建立的物件複本數量。

  - 雙重提交：如果ILM規則指定擷取行為的雙重提交選項、StorageGRID 則會在擷取物件時建立單一的過渡複本（單一提交）。
  - 平衡：如果ILM規則指定平衡選項、StorageGRID 則僅當系統無法立即製作規則中指定的所有複本時、才能製作單一的過渡複本。如果能夠執行同步放置、則此標頭不會有任何影響。StorageGRID

    當符合物件的ILM規則建立單一複寫複本時、最適合使用「已儲存的備援」標頭。在這種情況下、使用「reduced_dere通用」可免除每次擷取作業不必要地建立和刪除額外的物件複本。

    在其他情況下、不建議使用「已儲存的備援」標頭、因為它會增加擷取期間物件資料遺失的風險。例如、如果單一複本一開始儲存在無法進行ILM評估的儲存節點上、則可能會遺失資料。

    在任何時間段只複寫一個複本、會使資料面臨永久遺失的風險。如果只有一個物件複寫複本存在、則當儲存節點故障或發生重大錯誤時、該物件就會遺失。在升級等維護程序期間、您也會暫時失去物件的存取權。

請注意、指定「已儲存的備援」僅會影響第一次擷取物件時所建立的複本數量。當物件由作用中的ILM原則評估時、不會影響物件的複本份數、也不會導致資料儲存在StorageGRID 較低層級的資料冗餘環境中。

成功執行會傳回下列標頭、並顯示「已建立的HTTP/1.1 201」回應：

- 《內容長度》
- 「內容類型」
- '日期'

- 《ETag》
- 「上次修改日期」
- 「X-trans-ID」

相關資訊

使用ILM管理物件

監控與稽核作業

選項要求

選項要求會檢查個別Swift服務的可用度。選項要求由URL中指定的儲存節點或閘道節點處理。

選項方法

例如、用戶端應用程式可以在儲存節點上向Swift連接埠發出選項要求、而無需提供Swift驗證認證、以判斷儲存節點是否可用。您可以使用此要求來監控或允許外部負載平衡器識別儲存節點何時當機。

搭配資訊URL或儲存URL使用時、options方法會傳回指定URL所支援的動詞清單（例如、標頭、Get、選項及PUT）。選項方法無法與驗證URL搭配使用。

需要下列要求參數：

- 「帳戶」

下列要求參數為選用項目：

- 《Container》
- 「物件」

成功執行會傳回下列標頭、並顯示「HTTP / 1.1 204無內容」回應。儲存URL的選項要求不需要目標存在。

- 「允許」（特定URL的支援動詞清單、例如：標頭、取得、選項、 並投入）
- 《內容長度》
- 「內容類型」
- '日期'
- 「X-trans-ID」

相關資訊

支援的Swift API端點

Swift API作業的錯誤回應

瞭解可能的錯誤回應有助於疑難排解作業。

當作業期間發生錯誤時、可能會傳回下列HTTP狀態代碼：

Swift錯誤名稱	HTTP狀態
AccountNameTooLong、ContainerNameTooLong、HeaderTooBig、InvalidContainerName、InvalidRequest、 InvalidURI、Metadata NameTooLong、Metadata ValueTooBig、MISingSecurityHeader、ObjectNameTooLong、 TooManyContainers,TooManyMetadata項目,TotalMetadata TooLarg	400個錯誤要求
ACCESSDENIED	403禁止
ContainerNotEmpty、ContainerAlreadyExiss	衝突
內部錯誤	500內部伺服器錯誤
InvalidRang	無法滿足416個要求的範圍
方法未允許	不允許使用405方法
內容長度	需要411長度
NotFound	找不到404
未實作	501未實作
預先條件失敗	412先決條件失敗
資源NotFound	找不到404
未獲授權	401未獲授權
UnprocessableEntity	無法處理的實體

Swift REST API作業StorageGRID

Swift REST API上新增了特定StorageGRID 於該系統的作業。

取得Container一致性要求

一致性層級可在物件的可用度與這些物件在不同儲存節點和站台之間的一致性之間取得平衡。「Get Container一致性」要求可讓您判斷要套用至特定容器的一致性層級。

申請

要求**HTTP**標頭	說明
「X-AUTH-Token」	指定要用於要求的帳戶Swift驗證權杖。
《X-ntot-sg-consistency》	指定要求類型、其中「true」=取得容器一致性、「false」= Get Container。
「主機」	要求導向的主機名稱。

申請範例

```
GET /v1/28544923908243208806/Swift container
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29
x-ntap-sg-consistency: true
Host: test.com
```

回應

回應**HTTP**標頭	說明
'日期'	回應的日期和時間。
「連線」	是否開啟或關閉與伺服器的連線。
「X-trans-ID」	要求的唯一交易識別碼。
《內容長度》	回應本文的長度。

回應HTTP標頭	說明
《X-ntot-sg-consistency》	套用至容器的一致性控制層級。支援下列值： • 全部：所有節點都會立即接收資料、否則要求將會失敗。 • 強式全域：保證所有站台所有用戶端要求的寫入後讀取一致性。 • * Strong站台*：保證站台內所有用戶端要求的寫入後讀取一致性。 • 新寫入後讀取：提供新物件的寫入後讀取一致性、以及物件更新的最終一致性。提供高可用度與資料保護保證。 附註：如果您的應用程式在不存在的物件上使用標頭要求、如果一個或多個儲存節點無法使用、您可能會收到大量500個內部伺服器錯誤。若要避免這些錯誤、請使用「可用」層級。 • 可用（最終的頭端作業一致性）：行為與「全新寫入後的讀取」一致性層級相同、但最終只能提供頭端作業的一致性。如果儲存節點無法使用、則頭端作業的可用度比「全新寫入後的準備」高。

回應範例

```
HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
x-ntap-sg-consistency: strong-site
```

相關資訊

使用租戶帳戶

放置容器一致性要求

放置容器一致性要求可讓您指定要套用至容器上執行之作業的一致性層級。根據預設、新的容器是使用「全新寫入後的讀取」一致性層級來建立。

申請

要求HTTP標頭	說明
「X-AUTH-Token」	用於要求的帳戶Swift驗證權杖。

要求**HTTP**標頭	說明
《X-ntot-sg-consistency》	套用至容器作業的一致性控制層級。支援下列值： • 全部：所有節點都會立即接收資料、否則要求將會失敗。 • 強式全域：保證所有站台所有用戶端要求的寫入後讀取一致性。 • * Strong站台*：保證站台內所有用戶端要求的寫入後讀取一致性。 • 新寫入後讀取：提供新物件的寫入後讀取一致性、以及物件更新的最終一致性。提供高可用度與資料保護保證。 附註：如果您的應用程式在不存在的物件上使用標頭要求、如果一個或多個儲存節點無法使用、您可能會收到大量500個內部伺服器錯誤。若要避免這些錯誤、請使用「可用」層級。 • 可用（最終的頭端作業一致性）：行為與「全新寫入後的讀取」一致性層級相同、但最終只能提供頭端作業的一致性。如果儲存節點無法使用、則頭端作業的可用度比「全新寫入後的準備」高。
「主機」	要求導向的主機名稱。

一致性控制與**ILM**規則如何互動、以影響資料保護

您選擇的一致性控制和ILM規則都會影響物件的保護方式。這些設定可以互動。

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

下列擷取行為適用於ILM規則：

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

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

一致性控制和**ILM**規則如何互動的範例

假設您有一個雙站台網格、其中包含下列ILM規則和下列一致性層級設定：

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

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

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

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

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

申請範例

```
PUT /v1/28544923908243208806/_Swift container_
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29
x-ntap-sg-consistency: strong-site
Host: test.com
```

回應

回應**HTTP**標頭	說明
'日期'	回應的日期和時間。
「連線」	是否開啟或關閉與伺服器的連線。
「X-trans-ID」	要求的唯一交易識別碼。
《內容長度》	回應本文的長度。

回應範例

```
HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
```

相關資訊

使用租戶帳戶

設定REST API的安全性

您應該檢閱針對REST API實作的安全措施、並瞭解如何保護系統安全。

如何為REST API提供安全性StorageGRID

您應該瞭解StorageGRID 什麼是讓此系統為REST API實作安全性、驗證和授權。

使用下列安全措施。StorageGRID

- 如果已針對負載平衡器端點設定HTTPS、則用戶端與負載平衡器服務的通訊會使用HTTPS。

  當您設定負載平衡器端點時、可以選擇啟用HTTP。例如、您可能想要使用HTTP進行測試或其他非正式作業用途。如StorageGRID 需詳細資訊、請參閱《關於管理功能的說明》。

- 根據預設StorageGRID 、使用HTTPS與儲存節點進行用戶端通訊、並在閘道節點上使用CLB服務。

  您可以選擇性地為這些連線啟用HTTP。例如、您可能想要使用HTTP進行測試或其他非正式作業用途。如StorageGRID 需詳細資訊、請參閱《關於管理功能的說明》。

  CLB服務已過時。

- 支援使用TLS加密支援不支援的客戶端與StorageGRID 之通訊。
- 無論負載平衡器端點是設定為接受HTTP或HTTPS連線、網格內負載平衡器服務與儲存節點之間的通訊都會加密。
- 用戶端必須提供HTTP驗證標頭StorageGRID 給才能執行REST API作業。

安全性憑證與用戶端應用程式

用戶端可連線至閘道節點或管理節點上的負載平衡器服務、直接連線至儲存節點、或連線至閘道節點上已過時的CLB服務。

在任何情況下、用戶端應用程式都可以使用網格管理員上傳的自訂伺服器憑證或StorageGRID 由該系統產生的憑證來建立TLS連線：

- 當用戶端應用程式連線至負載平衡器服務時、應用程式會使用針對用於建立連線的特定負載平衡器端點所設定的憑證來執行此作業。每個端點都有自己的憑證、可以是由網格管理員上傳的自訂伺服器憑證、也可以是網格管理員StorageGRID 在設定端點時產生的憑證。
- 當用戶端應用程式直接連線至儲存節點或閘道節點上的CLB服務時、它們會使用StorageGRID 安裝時（由系統憑證授權單位簽署）為儲存節點產生的系統產生伺服器憑證、 或是由網格管理員提供的單一自訂伺服器憑證。

用戶端應設定為信任已簽署其用於建立TLS連線之任何憑證的憑證授權單位。

如StorageGRID 需設定負載平衡器端點的相關資訊、以及新增單一自訂伺服器憑證以供TLS連線直接連線至儲存節點或閘道節點上的CLB服務的相關指示、請參閱《for Administering》（管理功能）。

摘要

下表顯示S3和Swift REST API如何實作安全性問題：

安全問題	**REST API**的實作
連線安全性	TLS
伺服器驗證	由系統CA或系統管理員提供的自訂伺服器憑證簽署的X・509伺服器憑證
用戶端驗證	• S3：S3帳戶（存取金鑰ID和秘密存取金鑰） • Swift：Swift帳戶（使用者名稱和密碼）
用戶端授權	• S3：貯體所有權及所有適用的存取控制原則 • Swift：系統管理員角色存取

相關資訊

管理StorageGRID

TLS程式庫支援的雜湊和加密演算法

支援一套有限的加密套件、用戶端應用程式可在建立傳輸層安全性（TLS）工作階段時使用。StorageGRID

支援的**TLS**版本

支援TLS 1.2和TLS 1.3。StorageGRID

不再支援SSLv3和TLS 1.1（或更早版本）。

支援的加密套件

TLS版本	加密套件的**IANA**名稱
1.2	TLS_ECDHE_RSA_with _AES-256_GCM_SHA384
TLS_ECDHE_RSA_with _CHACHA20_POLY1305_SHA256	TLS_ECDHE_RSA_with _AES-122_GCM_SHA256
1.3	TLS_AES-256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256	TLS_AES-128_GCM_SHA256

已過時的加密套件

下列加密套件已過時。未來版本將會移除對這些密碼的支援。

IANA名稱
TLS_RSA_AT_AES-122_GCM_SHA256
TLS_RSA_AT_AES-256_GCM_SHA384

相關資訊

設定租戶帳戶和連線

監控與稽核作業

您可以檢視整個網格或特定節點的交易趨勢、來監控用戶端作業的工作負載和效率。您可以使用稽核訊息來監控用戶端作業和交易。

監控物件擷取和擷取速率

您可以監控物件擷取和擷取速率、以及物件計數、查詢和驗證的度量。您可以檢視用戶端應用程式在StorageGRID 讀取、寫入及修改物件時、成功和失敗的嘗試次數。

步驟

1. 使用登入Grid Manager 支援的網頁瀏覽器。
2. 在儀表板上、找到「傳輸協定作業」區段。

   本節概述StorageGRID 您的一套系統執行的用戶端作業數量。在過去兩分鐘內平均傳輸協定速率。

3. 選擇*節點*。
4. 在節點首頁（部署層級）中、按一下*負載平衡器*索引標籤。

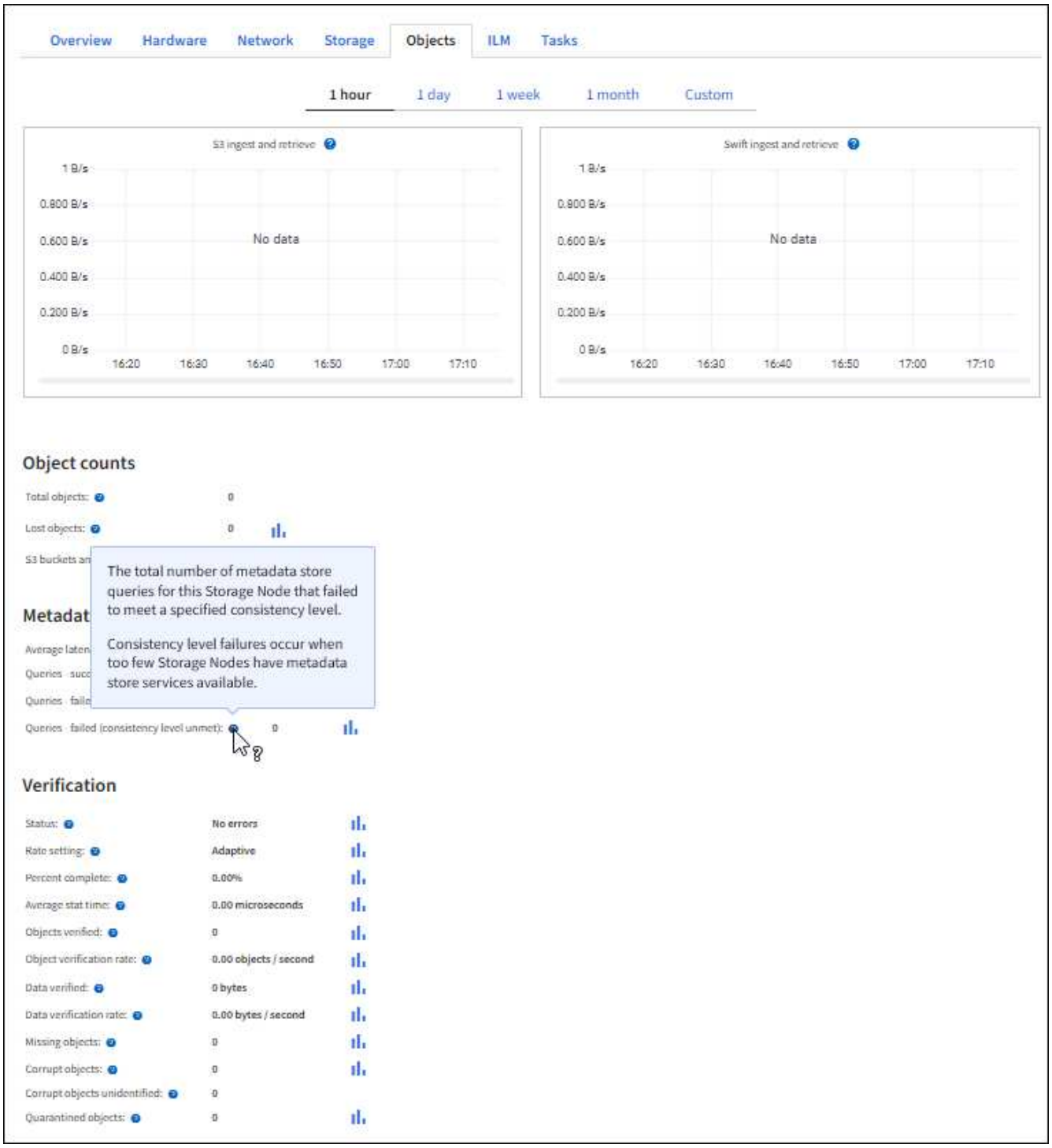
   這些圖表顯示了導向至網格內負載平衡器端點的所有用戶端流量趨勢。您可以選擇以小時、天、週、月或年為單位的時間間隔、 您也可以套用自訂時間間隔。

5. 在節點首頁（部署層級）中、按一下*物件*索引標籤。

   此圖表以StorageGRID 每秒位元組數和總位元組數顯示整個系統的擷取和擷取速率。您可以選擇以小時、天、週、月或年為單位的時間間隔、 您也可以套用自訂時間間隔。

6. 若要查看特定儲存節點的資訊、請從左側清單中選取節點、然後按一下「物件」索引標籤。

   此圖表顯示此儲存節點的物件擷取和擷取速率。此索引標籤也包含物件計數、查詢和驗證的度量。您可以按一下標籤來查看這些度量的定義。



7. 如果您想要更詳細的資料：
   a. 選取*支援*>*工具*>*網格拓撲*。
   b. 選擇*站台_*>*總覽*>*主選項*。

      「API作業」區段會顯示整個網格的摘要資訊。

   c. 選擇「儲存節點_」>「最大」>「用戶端應用程式_」>「總覽」>「主要」

      「作業」區段會顯示所選儲存節點的摘要資訊。

存取及檢閱稽核記錄

稽核訊息是StorageGRID 由支援服務產生、並儲存在文字記錄檔中。稽核日誌中的API專屬稽核訊息可提供關鍵的安全性、作業和效能監控資料、協助您評估系統的健全狀況。

您需要的產品

- 您必須擁有特定的存取權限。
- 您必須擁有「passwors.txt」檔案。
- 您必須知道管理節點的IP位址。

關於這項工作

作用中的稽核記錄檔名為「稽核記錄」、儲存在管理節點上。

一天只要儲存一次作用中的audit.log檔案、就會啟動新的audit.log檔案。儲存檔案的名稱會以「youty-mm-dd.txt"格式、指出儲存檔案的時間。

一天後、儲存的檔案會壓縮並重新命名、格式為「yyyy-mm-dd.gt」、保留原始日期。

此範例顯示使用中的audit.log檔案、前一天的檔案（2018-04-15.TXT）、以及前一天的壓縮檔案（「2018-04-14.txt.gz」）。

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

步驟

1. 登入管理節點：
   a. 輸入下列命令：「sh_admin@primary管理節點IP」
   b. 輸入「passwords.txt」檔案中所列的密碼。
2. 移至包含稽核記錄檔的目錄：`CD /var/local/exit/export/export/export/export/eap`
3. 視需要檢視目前或已儲存的稽核記錄檔。

相關資訊

檢閱稽核記錄

在稽核記錄中追蹤的**Swift**作業

所有成功的儲存刪除、取得、顯示、張貼及放置作業、都會記錄在StorageGRID 「停止稽核」記錄中。不會記錄故障、也不會要求資訊、驗證或選項。

請參閱_瞭解稽核訊息_、以取得下列Swift作業所追蹤資訊的詳細資料。

帳戶營運

- 取得帳戶
- 總公司帳戶

容器作業

- 刪除容器
- 取得Container
- 頭端容器
- 放入容器

物件作業

- 刪除物件
- Get物件
- 標頭物件
- 放置物件

相關資訊

檢閱稽核記錄

帳戶營運

容器作業

物件作業