管理StorageGRID

StorageGRID software

NetApp
May 29, 2026

目錄

管理StorageGRID

管理StorageGRID

使用這些說明來設定和管理StorageGRID系統。

關於這些說明

配置和管理StorageGRID的主要任務可讓您：

- 使用網格管理器設定群組和用戶
- 建立租用戶帳戶以允許 S3 用戶端應用程式儲存和擷取對象
- 設定與管理StorageGRID網路
- 配置AutoSupport
- 管理節點設定

開始之前

- 您對StorageGRID系統有大致的了解。
- 您對 Linux 命令 shell、網路以及伺服器硬體設定和配置有相當詳細的了解。

開始使用網格管理器

Web 瀏覽器需求

您必須使用受支援的 Web 瀏覽器。

Web 瀏覽器	最低支援版本
谷歌瀏覽器	119
微軟 Edge	119
火狐瀏覽器	119

您應該將瀏覽器視窗設定為建議的寬度。

瀏覽器寬度	像素
最低限度	1024
最佳	1280

Sign in入網格管理器

您可以透過在支援的 Web 瀏覽器的位址列中輸入管理節點的完全限定網域名稱 (FQDN) 或 IP 位址來存取網格管理員登入頁面。

每個StorageGRID系統包含一個主管理節點和任意數量的非主管理節點。您可以登入任何管理節點上的網格管理器來管理StorageGRID系統。但是，某些維護程序只能從主管理節點執行。

連接到 **HA** 組

如果管理節點包含在高可用性 (HA) 群組中，則可以使用 HA 群組的虛擬 IP 位址或對應到虛擬 IP 位址的完全限定網域名稱進行連線。應選擇主管理節點作為群組的主接口，以便當您存取網格管理器時，您可以在主管理節點上存取它，除非主管理節點不可用。看"管理高可用性組" 。

使用 **SSO**

如果"已設定單一登入 (SSO)"。

在第一個管理節點**Sign in**入網格管理器

開始之前

- 您有登入憑證。
- 您正在使用"支援的網頁瀏覽器"。
- 您的網頁瀏覽器已啟用 Cookie。
- 您屬於至少具有一項權限的使用者群組。
- 您有網格管理器的 URL：

  `https://FQDN_or_Admin_Node_IP/`

  您可以使用完全限定網域名稱、管理節點的 IP 位址或管理節點 HA 群組的虛擬 IP 位址。

  若要透過 HTTPS 預設連接埠 (443) 以外的連接埠存取網格管理器，請在 URL 中包含連接埠號碼：

  `https://FQDN_or_Admin_Node_IP:port/`

  > 受限網格管理器連接埠上不提供 SSO。您必須使用連接埠 443。

步驟

1. 啟動支援的 Web 瀏覽器。
2. 在瀏覽器的網址列中，輸入網格管理員的 URL。
3. 如果出現安全性警報，請使用瀏覽器的安裝精靈安裝憑證。看"管理安全證書" 。
4. Sign in入網格管理器。

   出現的登入畫面取決於是否為StorageGRID配置了單一登入 (SSO)。

不使用 **SSO**

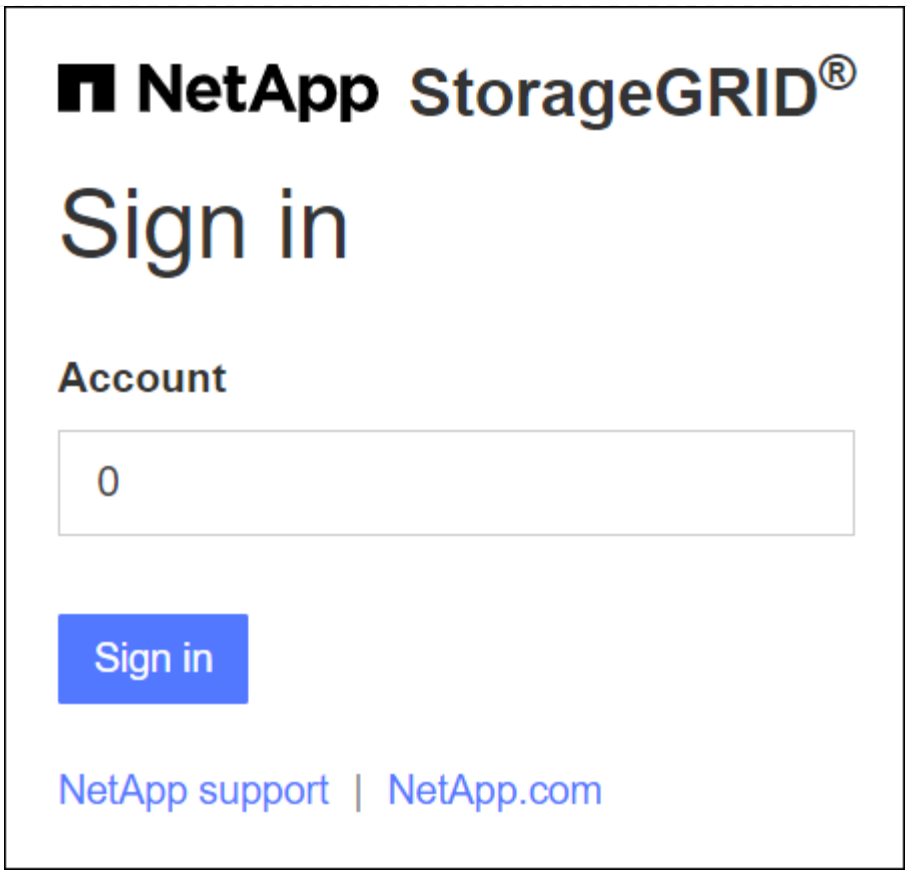
a. 輸入網格管理器的使用者名稱和密碼。

b. 選擇*登入*。

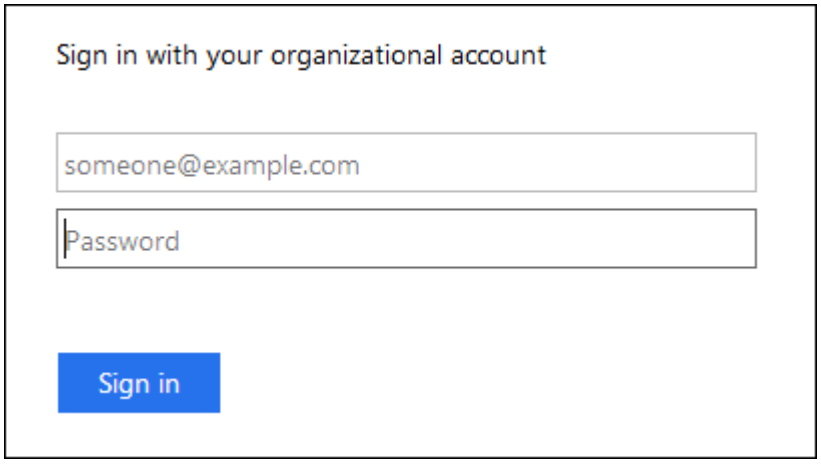
使用 **SSO**

- 如果StorageGRID正在使用 SSO，並且這是您第一次在此瀏覽器上存取 URL：

  i. 選擇*Sign in*。您可以在帳戶欄位中保留 0。



ii. 在您組織的 SSO 登入頁面上輸入您的標準 SSO 憑證。例如：



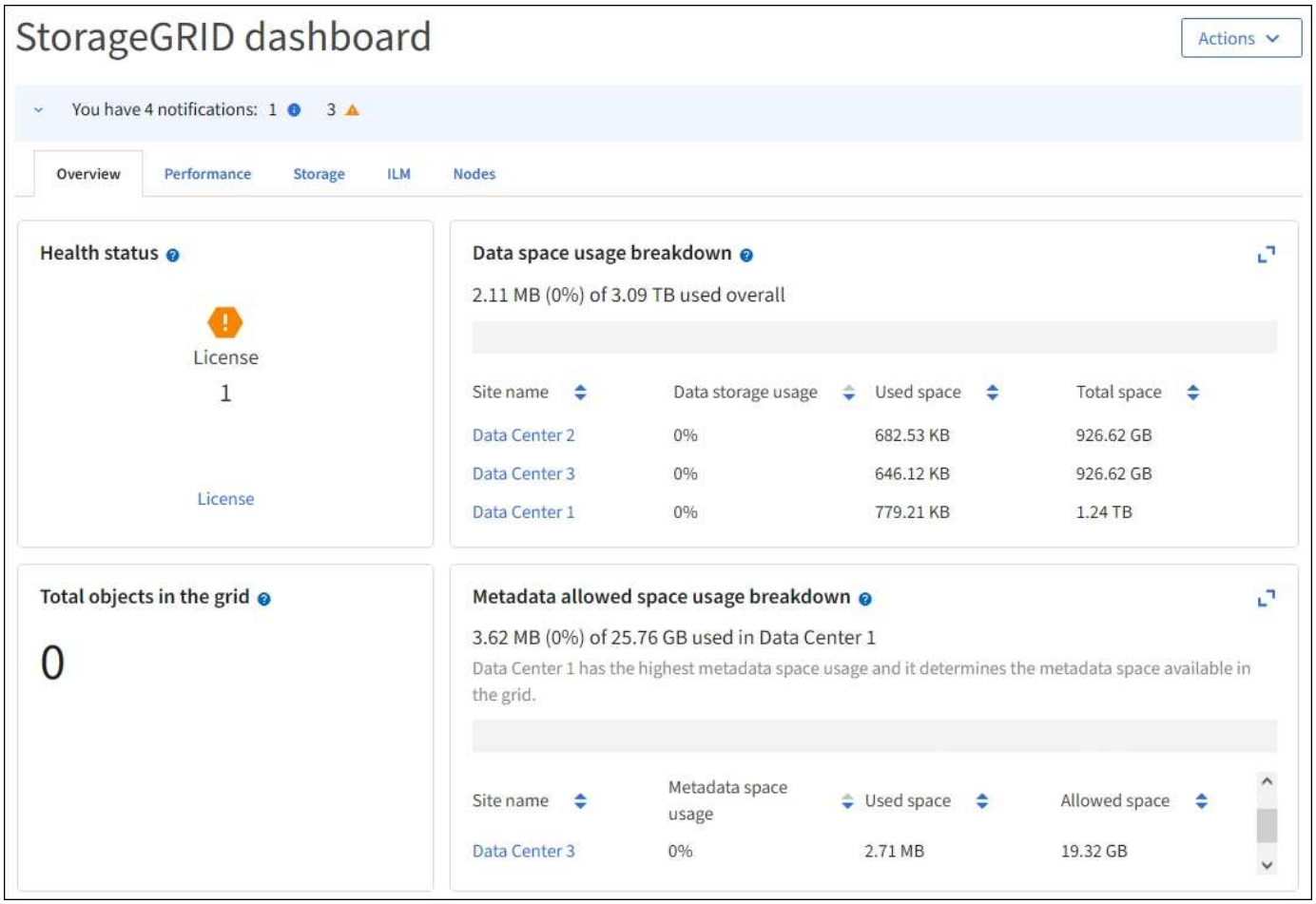
- 如果StorageGRID正在使用 SSO 且您之前曾造訪網格管理器或租用戶帳戶：

  i. 輸入 **0**（網格管理員的帳戶 ID）或選擇 網格管理員（如果它出現在最近的帳戶清單中）。

ii. 選擇*Sign in*。

iii. 使用您的標準 SSO 憑證在您組織的 SSO 登入頁面上Sign in。

登入後，將出現網格管理器的主頁，其中包括儀表板。要了解提供的信息，請參閱"查看和管理儀表板"。



登入另一個管理節點

請依照下列步驟登入另一個管理節點。

不使用 **SSO**

步驟

1. 在瀏覽器的網址列中，輸入另一個管理節點的完全限定網域名稱或 IP 位址。根據需要包含連接埠號碼。
2. 輸入網格管理器的使用者名稱和密碼。
3. 選擇*登入*。

使用 **SSO**

如果StorageGRID使用 SSO 並且您已登入一個管理節點，則您可以存取其他管理節點，而無需再次登入。

步驟

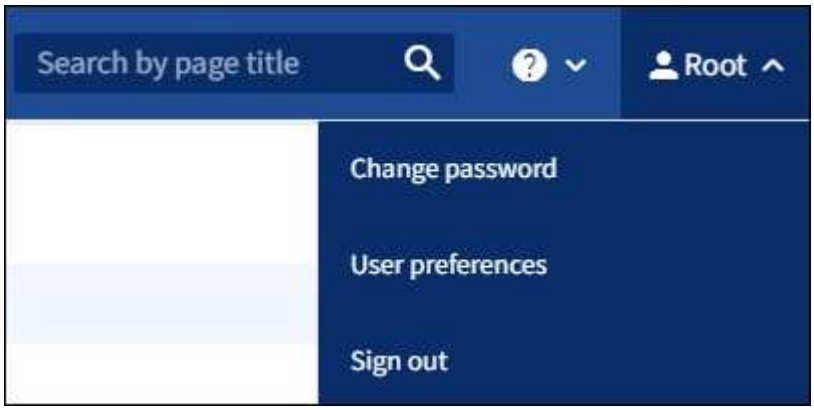
1. 在瀏覽器的網址列中輸入另一個管理節點的完全限定網域名稱或 IP 位址。
2. 如果您的 SSO 會話已過期，請再次輸入您的憑證。

退出網格管理器

當您完成網格管理員的工作後，您必須登出以確保未經授權的使用者無法存取StorageGRID系統。根據瀏覽器 cookie 設定，關閉瀏覽器可能不會使您退出系統。

步驟

1. 在右上角選擇您的使用者名稱。



2. 選擇“退出”。

選項	描述
SSO 未使用	您已退出管理節點。 顯示網格管理器登入頁面。 *注意：*如果您登入了多個管理節點，則必須登出每個節點。
已啟用 SSO	您已退出正在存取的所有管理節點。顯示StorageGRID登入頁面。 *網格管理器*在*最近的帳戶*下拉選單中列為預設值，並且*帳戶 ID*欄位顯示 0。 *注意：*如果啟用了 SSO 並且您也登入了租戶管理器，您也必須"登出租用戶帳戶"到"退出 SSO"。

更改密碼

如果您是網格管理器的本機用戶，您可以變更自己的密碼。

開始之前

您已使用"支援的網頁瀏覽器"。

關於此任務

如果您以聯合使用者登入StorageGRID或啟用了單一登入 (SSO)，則無法在 Grid Manager 中變更密碼。相反，您必須在外部身分識別來源（例如 Active Directory 或 OpenLDAP）中變更密碼。

步驟

1. 從網格管理器標題中，選擇 ***your name*** > **Change password**。
2. 輸入您目前的密碼。
3. 輸入新密碼。

   您的密碼必須至少包含 8 個字符，且不超過 32 個字符。密碼區分大小寫。

4. 重新輸入新密碼。
5. 選擇*儲存*。

查看StorageGRID許可證信息

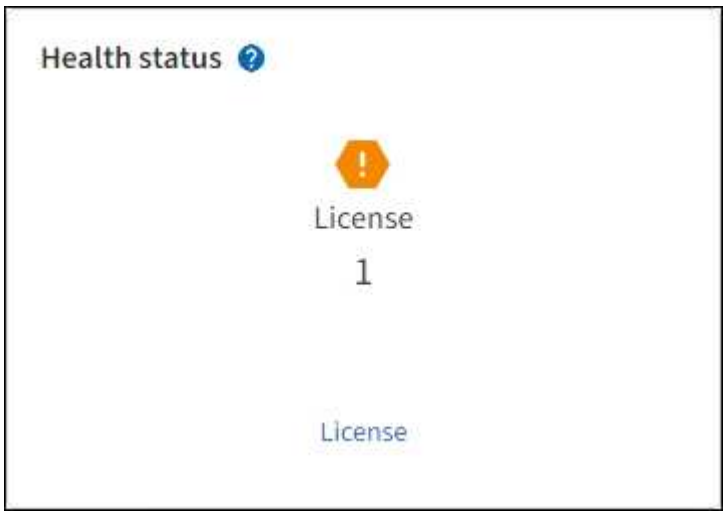
您可以隨時查看StorageGRID系統的許可證信息，例如網格的最大儲存容量。

開始之前

您已使用"支援的網頁瀏覽器"。

關於此任務

如果此StorageGRID系統的軟體許可證有問題，則儀表板上的健康狀態卡將包含許可證狀態圖示和 許可證 連結。該數字表示與許可證相關的問題的數量。



步驟

1. 透過執行下列操作之一存取許可證頁面：
   - 選擇*維護* > 系統 > 許可證。
   - 從儀表板上的健康狀態卡中，選擇許可證狀態圖示或*許可證*連結。

     僅當許可證出現問題時才會出現此連結。

2. 查看目前許可證的唯讀詳細資訊：
   - StorageGRID系統 ID，這是此StorageGRID安裝的唯一識別號
   - 許可證序號
   - 授權類型，永久*或*訂閱

- 電網許可儲存容量
- 支援的儲存容量
- 許可證結束日期。永久許可證顯示為 **N/A**。
- 支援結束日期

  此日期是從當前許可證文件中讀取的，如果您在獲取許可證文件後延長或續訂了支援服務合同，則該日期可能會過期。若要更新此值，請參閱"更新StorageGRID許可證信息"。您也可以使用Active IQ查看實際合約結束日期。

- 許可證文字檔案的內容

更新**StorageGRID**許可證信息

當您的授權條款發生變更時，您必須更新StorageGRID系統的授權資訊。例如，如果您為電網購買了額外的儲存容量，則必須更新許可證資訊。

開始之前

- 您有一個新的許可證文件可以套用到您的StorageGRID系統。
- 你有"特定存取權限"。
- 您有配置密碼。

步驟

1. 選擇*維護* > 系統 > 許可證。
2. 在更新許可證部分，選擇*瀏覽*。
3. 找到並選擇新的許可證文件(`.txt`）。

   新的許可證文件已驗證並顯示。

4. 輸入配置密碼。
5. 選擇*儲存*。

使用 **API**

使用網格管理 **API**

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

頂級資源

網格管理 API 提供以下頂級資源：

- `/grid`：存取僅限於 Grid Manager 用戶，並且基於配置的群組權限。
- `/org`：存取權限僅限於屬於租用戶帳戶的本機或聯合 LDAP 群組的使用者。有關詳細信息，請參閱"使用租用戶帳戶" 。

- `/private`：存取僅限於 Grid Manager 用戶，並且基於配置的群組權限。私有 API 如有更改，恕不另行通知。 StorageGRID私有端點也會忽略請求的 API 版本。

發出 **API** 請求

網格管理API使用Swagger開源API平台。 Swagger 提供了直覺的使用者介面，允許開發人員和非開發人員使用 API 在StorageGRID中執行即時操作。

Swagger 使用者介面為每個 API 操作提供了完整的詳細資訊和文件。

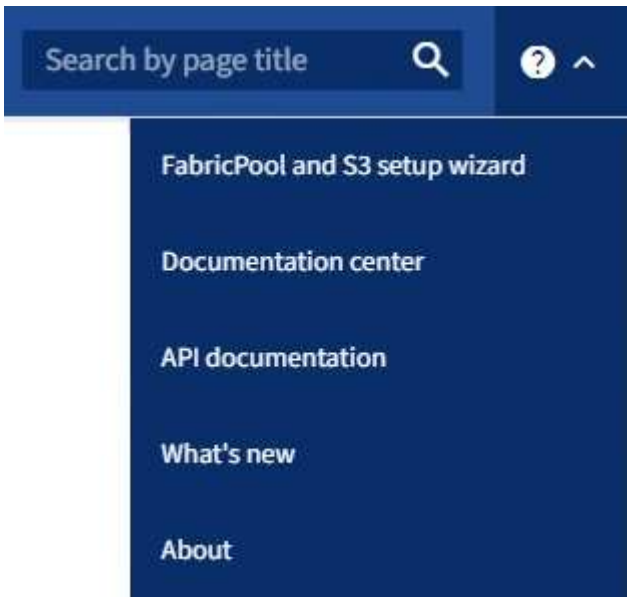
開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"特定存取權限"。

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

步驟

1. 從網格管理器標題中，選擇幫助圖示並選擇*API 文件*。



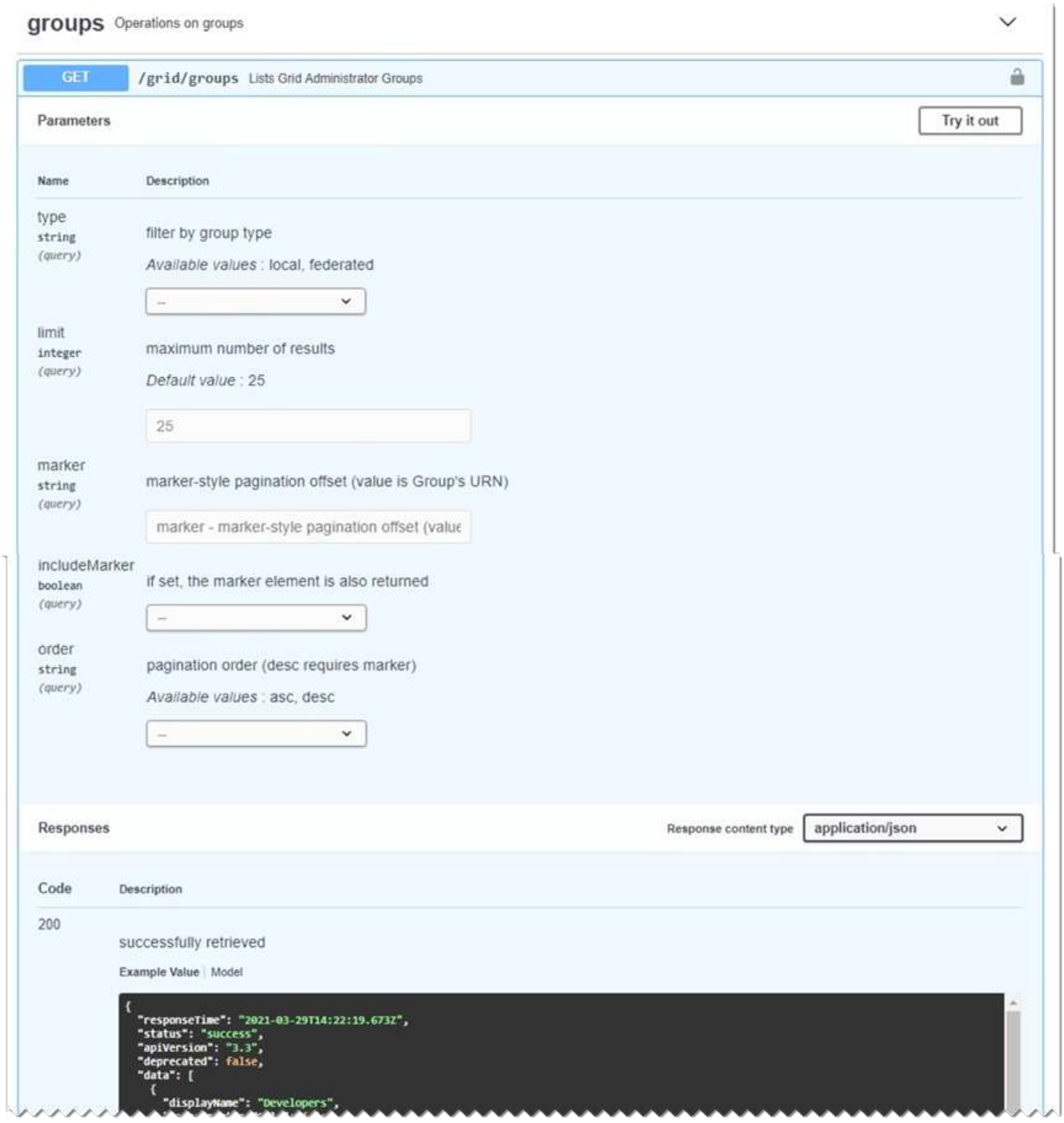
2. 若要使用私有 API 執行操作，請在StorageGRID管理 API 頁面上選擇 前往私有 **API** 文件。

   私有 API 如有更改，恕不另行通知。 StorageGRID私有端點也會忽略請求的 API 版本。

3. 選擇所需的操作。

   展開 API 操作時，您可以看到可用的 HTTP 操作，例如 GET、PUT、UPDATE 和 DELETE。

4. 選擇一個 HTTP 操作來查看請求詳細信息，包括端點 URL、任何必需或可選參數的列表、請求正文的範例（需要時）以及可能的回應。



5. 確定請求是否需要其他參數，例如群組或使用者 ID。然後，取得這些值。您可能需要先發出不同的 API 請求來取得所需的資訊。
6. 確定是否需要修改範例請求正文。如果是，您可以選擇*模型*來了解每個領域的要求。
7. 選擇*試用*。
8. 提供任何所需的參數，或根據需要修改請求正文。
9. 選擇*執行*。
10. 查看回應代碼以確定請求是否成功。

網格管理 API 將可用的操作組織到以下部分。

此清單僅包含公共 API 中可用的操作。

- **accounts**：管理儲存租用戶帳戶的操作，包括建立新帳戶和檢索給定帳戶的儲存使用情況。
- **alert-history**：已解決警報的操作。
- **alert-receivers**：對警報通知接收器（電子郵件）的操作。
- **alert-rules**：對警報規則的操作。
- **alert-silences**：警報靜默操作。
- 警報：警報操作。
- 審計：列出並更新審計配置的操作。
- **auth**：執行使用者會話認證的操作。

  網格管理 API 支援 Bearer Token 身份驗證方案。要登入，您需要在身份驗證請求的 JSON 主體中提供使用者名稱和密碼（即 `POST /api/v3/authorize`）。如果使用者驗證成功，則會傳回安全令牌。必須在後續 API 請求的標頭中提供此令牌（“Authorization: Bearer *token*”）。令牌將在 16 小時後過期。

  如果為StorageGRID系統啟用了單一登錄，則必須執行不同的步驟進行身份驗證。請參閱「如果啟用了單一登錄，則對 API 進行身份驗證」。

  有關提高身份驗證安全性的信息，請參閱「防止跨站點請求偽造」。

- **client-certificates**：設定客戶端憑證的操作，以便可以使用外部監控工具安全地存取StorageGRID 。
- **config**：與網格管理 API 的產品發佈和版本相關的操作。您可以列出產品發布版本和該版本支援的網格管理 API 的主要版本，並且可以停用 API 的棄用版本。
- **deactivated-features**：查看可能已停用的功能的操作。
- **dns-servers**：列出並變更已設定的外部 DNS 伺服器的操作。
- **drive-details**：針對特定儲存裝置型號的磁碟機的操作。
- **endpoint-domain-names**：列出並更改 S3 端點網域的操作。
- 擦除編碼：對擦除編碼設定檔的操作。
- 擴充：擴充操作（流程層級）。
- **expansion-nodes**：擴充操作（節點層級）。
- **expansion-sites**：擴充操作（站點層級）。
- **grid-networks**：列出並變更網格網路清單的操作。
- **grid-passwords**：網格密碼管理操作。
- **groups**：管理本機網格管理員群組和從外部 LDAP 伺服器檢索聯合網格管理員群組的操作。
- **identity-source**：設定外部身分來源並手動同步聯合群組和使用者資訊的操作。
- **ilm**：資訊生命週期管理（ILM）的操作。

- **in-progress-procedures**：檢索目前正在進行的維護程序。
- **license**：擷取並更新StorageGRID許可證的操作。
- **logs**：收集和下載日誌檔案的操作。 v
- 指標：對StorageGRID指標的操作，包括單一時間點的即時指標查詢和一段時間內的範圍指標查詢。網格管理 API 使用 Prometheus 系統監控工具作為後端資料來源。有關建立 Prometheus 查詢的信息，請參閱 Prometheus 網站。

> 指標包括*private*其名稱僅供內部使用。這些指標在StorageGRID版本之間可能會發生變化，恕不另行通知。

- **node-details**：對節點詳細資訊的操作。
- **node-health**：節點健康狀態的操作。
- **node-storage-state**：對節點儲存狀態的操作。
- **ntp-servers**：列出或更新外部網路時間協定 (NTP) 伺服器的操作。
- 物件：對物件和物件元資料的操作。
- 恢復：恢復過程的操作。
- **recovery-package**：下載復原套件的操作。
- **regions**：檢視和建立區域的操作。
- **s3-object-lock**：對全域 S3 物件鎖定設定的操作。
- **server-certificate**：檢視並更新 Grid Manager 伺服器憑證的操作。
- **snmp**：對目前 SNMP 配置進行操作。
- **storage-watermarks**：儲存節點浮水印。
- **traffic-classes**：流量分類策略的操作。
- **untrusted-client-network**：對不受信任的客戶端網路設定進行操作。
- 使用者：檢視和管理網格管理器使用者的操作。

網格管理 **API** 版本控制

網格管理 API 使用版本控制來支援無中斷升級。

例如，此請求 URL 指定 API 的版本 4。

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

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

以下範例說明如何根據所做變更的類型來升級 API 版本。

API 變更類型	舊版	新版本
與舊版本相容	2.1	2.2

API 變更類型	舊版	新版本
與舊版本不相容	2.1	3.0

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

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

過時的請求透過以下方式標記為已棄用：

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

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

確定目前版本支援哪些 API 版本

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

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

為請求指定 API 版本

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

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

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

防止跨站請求偽造（**CSRF**）

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

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

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

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

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

當為真時， `GridCsrfToken` cookie 設定為用於登入網格管理器的隨機值，並且 `AccountCsrfToken`為登入租戶管理器，cookie 設定了一個隨機值。

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

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

請參閱線上 API 文件以取得更多範例和詳細資訊。

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

如果啟用了單一登錄，請使用 **API**

如果啟用了單一登入（**Active Directory**），則使用 **API**

如果你有"設定並啟用單一登入（SSO）"並且您使用 Active Directory 作為 SSO 提供程序，則必須發出一系列 API 請求以取得對網格管理 API 或租用戶管理 API 有效的身份驗證令牌。

如果啟用了單一登錄，**Sign inAPI**

如果您使用 Active Directory 作為 SSO 身分提供者，則這些說明適用。

開始之前

- 您知道屬於StorageGRID使用者群組的聯合使用者的 SSO 使用者名稱和密碼。
- 如果您想存取租用戶管理 API，您需要知道租用戶帳戶 ID。

關於此任務

若要取得身份驗證令牌，您可以使用下列範例之一：

- 這 `storagegrid-ssoauth.py`Python 腳本，位於StorageGRID安裝檔目錄中 (./rpms`對於 Red Hat Enterprise Linux， `./debs`適用於 Ubuntu 或 Debian，以及 `./vsphere`對於 VMware)。
- curl 請求的工作流程範例。

  如果執行速度太慢，curl 工作流程可能會逾時。您可能會看到以下錯誤： `A valid SubjectConfirmation was not found on this Response`。

  範例 curl 工作流程不能保護密碼不被其他使用者看到。

如果您遇到 URL 編碼問題，您可能會看到以下錯誤： `Unsupported SAML version`。

步驟

1. 選擇以下方法之一來取得身份驗證令牌：
   - 使用 `storagegrid-ssoauth.py`Python 腳本。轉到步驟 2。
   - 使用 curl 請求。轉到步驟 3。
2. 如果你想使用 `storagegrid-ssoauth.py`腳本，將腳本傳遞給Python解釋器並運行腳本。

   出現提示時，輸入以下參數的值：

   - SSO 方法。輸入 ADFS 或 adfs。
   - SSO 使用者名稱
   - 安裝StorageGRID的網域
   - StorageGRID的位址
   - 如果您想存取租用戶管理 API，請輸入租用戶帳戶 ID。

```
python3 storagegrid-ssoauth.py
sso_method: adfs
saml_user: my-sso-username
saml_domain: my-domain
sg_address: storagegrid.example.com
tenant_account_id: 12345
Enter the user's SAML password:
********************************************************************************

********************************************************************************
StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
```

   輸出中提供了StorageGRID授權令牌。現在，您可以將令牌用於其他請求，類似於未使用 SSO 時使用 API 的方式。

3. 如果您想使用 curl 請求，請使用下列步驟。

   a. 聲明登入所需的變數。

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export SAMLDOMAIN='my-domain'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
export AD_FS_ADDRESS='adfs.example.com'
```

   若要存取網格管理 API，請使用 0 作為 `TENANTACCOUNTID`。

   b. 若要接收已簽署的身份驗證 URL，請發出 POST 請求 `/api/v3/authorize-saml`，並從回應中刪除額外的 JSON 編碼。

   此範例顯示了對簽名身份驗證 URL 的 POST 請求 `TENANTACCOUNTID`。結果將傳遞給 `python -m json.tool`刪除 JSON 編碼。

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

   此範例的回應包含經過 URL 編碼的簽章 URL，但不包括額外的 JSON 編碼層。

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...
sSl%2BfQ33cvfwA%3D&RelayState=12345",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

   c. 儲存 `SAMLRequest`從回應中取得用於後續命令的資訊。

```
export SAMLREQUEST='fZHLbsIwEEV%2FJTuv7...sSl%2BfQ33cvfwA%3D'
```

   d. 從 AD FS 取得包含用戶端請求 ID 的完整 URL。

   一種選擇是使用上一個回應中的 URL 請求登入表單。

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
$SAMLREQUEST&RelayState=$TENANTACCOUNTID" | grep 'form method="post"
id="loginForm"'
```

回應包含客戶端請求ID：

```
<form method="post" id="loginForm" autocomplete="off"
novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13)
Login.submitLoginRequest();" action="/adfs/ls/?
SAMLRequest=fZHRToMwFIZfhb...UJikvo77sXPw%3D%3D&RelayState=12345&clie
nt-request-id=00000000-0000-0000-ee02-0080000000de" >
```

e. 保存回應中的客戶端請求 ID。

```
export SAMLREQUESTID='00000000-0000-0000-ee02-0080000000de'
```

f. 將您的憑證從上一個回應傳送到表單操作。

```
curl -X POST "https://$AD_FS_ADDRESS
/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client
-request-id=$SAMLREQUESTID" \
--data "UserName=$SAMLUSER@$SAMLDOMAIN&Password=
$SAMLPASSWORD&AuthMethod=FormsAuthentication" --include
```

AD FS 返回 302 重定向，並在標頭中包含其他資訊。

> ⓘ 如果您的 SSO 系統啟用了多因素身份驗證 (MFA)，表單貼文還將包含第二個密碼或其他憑證。

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRToMwFIZfhb...UJikvo
77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-
ee02-0080000000de
Set-Cookie: MSISAuth=AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY=; path=/adfs;
HttpOnly; Secure
Date: Tue, 06 Nov 2018 16:55:05 GMT
```

g. 儲存 `MSISAuth`來自回應的 cookie。

```
export MSISAuth='AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY='
```

h. 使用來自驗證 POST 的 cookie 向指定位置發送 GET 請求。

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client-request-
id=$SAMLREQUESTID" \
--cookie "MSISAuth=$MSISAuth" --include
```

回應頭將包含 AD FS 會話資訊以供稍後登出使用，回應主體在隱藏的表單欄位中包含 SAMLResponse。

```
HTTP/1.1 200 OK
Cache-Control: no-cache,no-store
Pragma: no-cache
Content-Length: 5665
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-HTTPAPI/2.0
P3P: ADFS doesn't have P3P policy, please contact your site's admin
for more details
Set-Cookie:
SamlSession=a3dpbnRlcnMtUHJpbWFyeS1BZG1pbi0xNzgmRmFsc2Umcng4NnJDZmFKV
XFxVWx3bkl1MnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LThmMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMjo1OVpcMQ==;
path=/adfs; HttpOnly; Secure
Date: Wed, 07 Nov 2018 16:32:59 GMT

<form method="POST" name="hiddenform"
action="https://storagegrid.example.com:443/api/saml-response">
  <input type="hidden" name="SAMLResponse"
value="PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />
```

i. 儲存 `SAMLResponse`來自隱藏欄位：

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. 使用已儲存的 `SAMLResponse`，建立一個StorageGRID`/api/saml-response`請求產生StorageGRID

身份驗證令牌。

為了 `RelayState`，使用租用戶帳戶 ID，或如果要登入網格管理 API，則使用 0。

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

回應包含身份驗證令牌。

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. 將回應中的身份驗證令牌儲存為 `MYTOKEN`。

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

您現在可以使用 `MYTOKEN`對於其他請求，類似於未使用 SSO 時使用 API 的方式。

如果啟用了單一登錄，請退出 API

如果已啟用單一登入 (SSO)，則必須發出一系列 API 請求才能登出網格管理 API 或租用戶管理 API。如果您使用 Active Directory 作為 SSO 身分提供者，則適用這些說明

關於此任務

如果需要，您可以從組織的單一登出頁面登出StorageGRID API。或者，您可以從StorageGRID觸發單一登出(SLO)，這需要有效的StorageGRID承載令牌。

步驟

1. 若要產生簽署的登出請求，請將 cookie「sso=true」傳遞給 SLO API：

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

返回註銷 URL：

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3
D",
    "responseTime": "2018-11-20T22:20:30.839Z",
    "status": "success"
}
```

2. 儲存註銷 URL。

```
export LOGOUT_REQUEST
='https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%
3D'
```

3. 向登出 URL 發送請求以觸發 SLO 並重新導向回StorageGRID。

```
curl --include "$LOGOUT_REQUEST"
```

返回 302 響應。重定向位置不適用於僅 API 登出。

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: MSISSignoutProtocol=U2FtbA==; expires=Tue, 20 Nov 2018
22:35:03 GMT; path=/adfs; HttpOnly; Secure
```

4. 刪除StorageGRID承載令牌。

刪除StorageGRID承載令牌的方式與沒有 SSO 的方式相同。如果未提供“cookie“sso=true”，則使用者將從StorageGRID中登出，而不會影響 SSO 狀態。

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

一個 `204 No Content`回應表示用戶現在已退出。

```
HTTP/1.1 204 No Content
```

如果啟用了單一登錄，則使用 **API (Azure)**

如果你有"設定並啟用單一登入（SSO）"並且您使用 Azure 作為 SSO 提供程序，您可以使用兩個範例腳本來取得對網格管理 API 或租用戶管理 API 有效的身份驗證令牌。

如果啟用了 **Azure** 單一登入，**Sign inAPI**

如果您使用 Azure 作為 SSO 身分提供者，則這些說明適用

開始之前

- 您知道屬於StorageGRID使用者群組的聯合使用者的 SSO 電子郵件地址和密碼。
- 如果您想存取租用戶管理 API，您需要知道租用戶帳戶 ID。

關於此任務

若要取得身分驗證令牌，您可以使用下列範例腳本：

- 這 `storagegrid-ssoauth-azure.py`Python 腳本
- 這 `storagegrid-ssoauth-azure.js`Node.js 腳本

這兩個腳本都位於StorageGRID安裝檔目錄中(`./rpms`對於 Red Hat Enterprise Linux， `./debs`適用於 Ubuntu 或 Debian，以及 `./vsphere`對於 VMware)。

要編寫您自己的 Azure API 集成，請參閱 `storagegrid-ssoauth-azure.py`腳本。 Python 腳本直接向StorageGRID發出兩個請求（先取得 SAMLRequest，然後取得授權令牌），也呼叫 Node.js 腳本與 Azure 互動以執行 SSO 操作。

SSO 操作可以透過一系列 API 請求來執行，但這樣做並不簡單。Puppeteer Node.js 模組用於抓取 Azure SSO 介面。

如果您遇到 URL 編碼問題，您可能會看到以下錯誤： `Unsupported SAML version` 。

步驟

1. 安裝所需的依賴項，如下所示：
   a. 安裝 Node.js（參見 "https://nodejs.org/en/download/"）。
   b. 安裝所需的 Node.js 模組（puppeteer 和 jsdom）：

      ```
      npm install -g <module>
      ```

2. 將 Python 腳本傳遞給 Python 解釋器來執行該腳本。

   然後，Python 腳本將呼叫對應的 Node.js 腳本來執行 Azure SSO 互動。

3. 出現提示時，輸入以下參數的值（或使用參數傳遞它們）：
   ◦ 用於登入 Azure 的 SSO 電子郵件地址

- StorageGRID的位址
- 如果您想存取租用戶管理 API，請輸入租用戶帳戶 ID

4. 出現提示時，輸入密碼並準備在 Azure 要求時提供 MFA 授權。

```
c:\Users\user\Documents\azure_sso>py storagegrid-azure-ssoauth.py --sso-email-address user@my-domain.com
--sg-address storagegrid.examp.e.com --tenant-account-id 0
Enter the user's SSO password:
********************************************************************************

Watch for and approve a 2FA authorization request
********************************************************************************
StorageGRID Auth Token: {'responseTime': '2021-10-04T21:30:48.807Z', 'status': 'success', 'apiVersion':
'3.4', 'data': '4807d93e-a3df-48f2-9680-906cd255979e'}
```

> 該腳本假定使用 Microsoft Authenticator 完成 MFA。您可能需要修改腳本以支援其他形式的 MFA（例如輸入簡訊中收到的代碼）。

輸出中提供了StorageGRID授權令牌。現在，您可以將令牌用於其他請求，類似於未使用 SSO 時使用 API 的方式。

如果啟用了單一登錄，則使用 **API**（**PingFederate**）

如果你有"設定並啟用單一登入（SSO）"並且您使用 PingFederate 作為 SSO 提供程序，則必須發出一系列 API 請求以取得對網格管理 API 或租用戶管理 API 有效的身份驗證令牌。

如果啟用了單一登錄，**Sign inAPI**

如果您使用 PingFederate 作為 SSO 身分提供者，則適用這些說明

開始之前

- 您知道屬於StorageGRID使用者群組的聯合使用者的 SSO 使用者名稱和密碼。
- 如果您想存取租用戶管理 API，您需要知道租用戶帳戶 ID。

關於此任務

若要取得身份驗證令牌，您可以使用下列範例之一：

- 這 `storagegrid-ssoauth.py`Python 腳本，位於StorageGRID安裝檔目錄中 (./rpms`對於 Red Hat Enterprise Linux， `./debs`適用於 Ubuntu 或 Debian，以及 `./vsphere`對於 VMware)。
- curl 請求的工作流程範例。

  如果執行速度太慢，curl 工作流程可能會逾時。您可能會看到以下錯誤： `A valid SubjectConfirmation was not found on this Response`。

  > 範例 curl 工作流程不能保護密碼不被其他使用者看到。

  如果您遇到 URL 編碼問題，您可能會看到以下錯誤： `Unsupported SAML version`。

步驟

1. 選擇以下方法之一來取得身份驗證令牌：
   - 使用 `storagegrid-ssoauth.py`Python 腳本。轉到步驟 2。
   - 使用 curl 請求。轉到步驟 3。
2. 如果你想使用 `storagegrid-ssoauth.py`腳本，將腳本傳遞給Python解釋器並運行腳本。

   出現提示時，輸入以下參數的值：

   - SSO 方法。您可以輸入「pingfederate」的任何變體（PINGFEDERATE、pingfederate 等等）。
   - SSO 使用者名稱
   - 安裝StorageGRID的網域。此欄位不用於 PingFederate。您可以將其留空或輸入任何值。
   - StorageGRID的位址
   - 如果您想存取租用戶管理 API，請輸入租用戶帳戶 ID。

   ```
   python3 storagegrid-ssoauth.py
   sso_method: pingfederate
   saml_user: my-sso-username
   saml_domain:
   sg_address: storagegrid.example.com
   tenant_account_id: 12345
   Enter the user's SAML password:
   ********************************************************************************

   ********************************************************************************
   StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
   ```

   輸出中提供了StorageGRID授權令牌。現在，您可以將令牌用於其他請求，類似於未使用 SSO 時使用 API 的方式。

3. 如果您想使用 curl 請求，請使用下列步驟。

   a. 聲明登入所需的變數。

   ```
   export SAMLUSER='my-sso-username'
   export SAMLPASSWORD='my-password'
   export TENANTACCOUNTID='12345'
   export STORAGEGRID_ADDRESS='storagegrid.example.com'
   ```

   若要存取網格管理 API，請使用 0 作為 `TENANTACCOUNTID`。

   b. 若要接收已簽署的身份驗證 URL，請發出 POST 請求 `/api/v3/authorize-saml`，並從回應中刪除額外的 JSON 編碼。

   此範例顯示了針對 TENANTACCOUNTID 的簽章驗證 URL 的 POST 要求。結果將傳遞給 python -m json.tool 以刪除 JSON 編碼。

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

此範例的回應包含經過 URL 編碼的簽章 URL，但不包括額外的 JSON 編碼層。

```
{
    "apiVersion": "3.0",
    "data": "https://my-pf-baseurl/idp/SSO.saml2?...",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. 儲存 `SAMLRequest`從回應中取得用於後續命令的資訊。

```
export SAMLREQUEST="https://my-pf-baseurl/idp/SSO.saml2?..."
```

d. 匯出回應和 cookie，並回顯回應：

```
RESPONSE=$(curl -c - "$SAMLREQUEST")
```

```
echo "$RESPONSE" | grep 'input type="hidden" name="pf.adapterId"
id="pf.adapterId"'
```

e. 匯出“pf.adapterId”值，並回顯回應：

```
export ADAPTER='myAdapter'
```

```
echo "$RESPONSE" | grep 'base'
```

f. 匯出“href”值（刪除尾部的斜線/），並回顯響應：

```
export BASEURL='https://my-pf-baseurl'
```

```
echo "$RESPONSE" | grep 'form method="POST"'
```

g. 匯出"動作"值：

```
export SSOPING='/idp/.../resumeSAML20/idp/SSO.ping'
```

h. 發送 cookie 和憑證：

```
curl -b <(echo "$RESPONSE") -X POST "$BASEURL$SSOPING" \
--data "pf.username=$SAMLUSER&pf.pass=
$SAMLPASSWORD&pf.ok=clicked&pf.cancel=&pf.adapterId=$ADAPTER"
--include
```

i. 儲存 `SAMLResponse`來自隱藏欄位：

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. 使用已儲存的 `SAMLResponse`，建立一個StorageGRID`/api/saml-response`請求產生StorageGRID身份驗證令牌。

為了 `RelayState`，使用租用戶帳戶 ID，或如果要登入網格管理 API，則使用 0。

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

回應包含身份驗證令牌。

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. 將回應中的身份驗證令牌儲存為 `MYTOKEN`。

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

您現在可以使用 `MYTOKEN`對於其他請求，類似於未使用 SSO 時使用 API 的方式。

如果啟用了單一登錄，請退出 API

如果已啟用單一登入 (SSO)，則必須發出一系列 API 請求才能登出網格管理 API 或租用戶管理 API。如果您使用 PingFederate 作為 SSO 身分提供者，則適用這些說明

關於此任務

如果需要，您可以從組織的單一登出頁面登出StorageGRID API。或者，您可以從StorageGRID觸發單一登出 (SLO)，這需要有效的StorageGRID承載令牌。

步驟

1. 若要產生簽署的登出請求，請將 cookie「sso=true」傳遞給 SLO API：

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

返回註銷 URL：

```
{
    "apiVersion": "3.0",
    "data": "https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",
    "responseTime": "2021-10-12T22:20:30.839Z",
    "status": "success"
}
```

2. 儲存註銷 URL。

```
export LOGOUT_REQUEST='https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D'
```

3. 向登出 URL 發送請求以觸發 SLO 並重新導向回StorageGRID。

```
curl --include "$LOGOUT_REQUEST"
```

返回 302 響應。重定向位置不適用於僅 API 登出。

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: PF=QoKs...SgCC; Path=/; Secure; HttpOnly; SameSite=None
```

4. 刪除StorageGRID承載令牌。

   刪除StorageGRID承載令牌的方式與沒有 SSO 的方式相同。如果未提供“cookie“sso=true”，則使用者將從StorageGRID中登出，而不會影響 SSO 狀態。

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

   一個 `204 No Content`回應表示用戶現在已退出。

```
HTTP/1.1 204 No Content
```

使用 **API** 停用功能

您可以使用網格管理 API 完全停用StorageGRID系統中的某些功能。當某項功能停用時，任何人都無法被指派執行與該功能相關的任務的權限。

關於此任務

停用功能係統可讓您阻止存取StorageGRID系統中的某些功能。停用某項功能是阻止根使用者或具有 **Root** 存取權限的管理群組使用者使用此功能的唯一方法。

要了解此功能如何有用，請考慮以下場景：

_公司 A 是一家服務供應商，透過建立租用戶帳戶來租賃其StorageGRID系統的儲存容量。為了保護其租賃對象的安全，A 公司希望確保其員工在部署帳戶後永遠無法存取任何租戶帳戶。

_公司 A 可以透過使用網格管理 API 中的停用功能係統來實現這一目標。透過在網格管理員（UI 和 API）中完全停用「變更租用戶根密碼」功能，公司 A 確保管理員使用者（包括根使用者和屬於具有「根存取」權限的群組的使用者）無法變更任何租用戶帳戶的根用戶的密碼。

步驟

1. 存取網格管理 API 的 Swagger 文件。看"使用網格管理 API" 。
2. 找到停用功能端點。
3. 若要停用某項功能（例如變更租用戶根密碼），請向 API 傳送如下正文：

```
{ "grid": {"changeTenantRootPassword": true} }
```

請求完成後，更改租用戶 root 密碼功能將被停用。 *更改租用戶根密碼*管理權限不再出現在使用者介面中，並且任何嘗試更改租用戶根密碼的 API 請求都將失敗並顯示「403 禁止」。

重新啟用已停用的功能

預設情況下，您可以使用網格管理 API 重新啟用已停用的功能。但是，如果您想要防止已停用的功能被重新激活，您可以停用 **activateFeatures** 功能本身。

activateFeatures 功能無法重新啟動。如果您決定停用此功能，請注意，您將永久失去重新啟用任何其他已停用功能的能力。您必須聯絡技術支援以恢復任何遺失的功能。

步驟

1. 存取網格管理 API 的 Swagger 文件。
2. 找到停用功能端點。
3. 若要重新啟動所有功能，請向 API 發送如下正文：

```
{ "grid": null }
```

當此請求完成後，所有功能（包括變更租用戶根密碼功能）都會重新啟用。 *更改租用戶根密碼*管理權限現在出現在使用者介面中，並且任何嘗試更改租用戶根密碼的 API 請求都將成功，假設使用者俱有*根存取權*或*更改租用戶根密碼*管理權限。

前面的範例導致所有已停用的功能被重新啟用。如果其他功能已停用且應保持停用狀態，則必須在 PUT 請求中明確指定它們。例如，若要重新啟用變更租用戶 root 密碼功能並繼續停用 storageAdmin 管理權限，請傳送此 PUT 要求：+ `{ "grid": {"storageAdmin": true} }`

控制對StorageGRID 的存取

控制StorageGRID訪問

您可以透過建立或匯入群組和使用者並為每個群組分配權限來控制誰可以存取StorageGRID以及使用者可以執行哪些任務。您也可以選擇啟用單一登入 (SSO)、建立用戶端憑證以及變更網格密碼。

控制對網格管理器的訪問

您可以透過從身分聯合服務匯入群組和使用者或設定本機群組和本機使用者來確定誰可以存取網格管理器和網格管理 API。

使用"身分聯合"使設定"群組"和"使用者"速度更快，並且允許使用者使用熟悉的憑證登入StorageGRID 。如果您使用 Active Directory、OpenLDAP 或 Oracle Directory Server，則可以設定身分聯合。

如果您想使用其他 LDAP v3 服務，請聯絡技術支援。

您可以透過指派不同的任務來確定每個使用者可以執行哪些任務"權限"到每個組。例如，您可能希望一個群組中

的使用者能夠管理 ILM 規則，而另一個群組中的使用者能夠執行維護任務。使用者必須至少屬於一個群組才能存取系統。

或者，您可以將群組配置為唯讀。只讀群組中的使用者只能查看設定和功能。他們無法在網格管理器或網格管理 API 中進行任何更改或執行任何操作。

啟用單一登入

StorageGRID系統支援使用安全性斷言標記語言 2.0 (SAML 2.0) 標準的單一登入 (SSO)。您先請"設定並啟用 SSO"，所有使用者必須經過外部身分提供者的驗證，然後才能存取網格管理器、租用戶管理器、網格管理 API 或租用戶管理 API。本機使用者無法登入StorageGRID。

更改配置密碼

許多安裝和維護過程以及下載StorageGRID恢復包都需要設定密碼。下載StorageGRID系統的網格拓樸資訊和加密金鑰的備份也需要密碼。你可以"更改密碼"按要求。

更改節點控制台密碼

網格中的每個節點都有一個唯一的節點控制台密碼，您需要使用 SSH 以「管理員」身分登入節點，或以 VM/實體控制台連線上的 root 使用者身分登入。根據需要，您可以"更改節點控制台密碼"對於每個節點。

更改配置密碼

使用此程序更改StorageGRID配置密碼。恢復、擴充和維護過程都需要密碼。下載恢復包備份也需要密碼，其中包括網格拓撲資訊、網格節點控制台密碼和StorageGRID系統的加密金鑰。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 您具有維護或 Root 存取權限。
- 您擁有目前的設定密碼。

關於此任務

許多安裝和維護過程都需要配置密碼，並且"下載恢復包"。配置密碼未在 `Passwords.txt`文件。確保記錄配置密碼並將其保存在安全的地方。

步驟

1. 選擇*設定* > 存取控制 > 電網密碼。
2. 在“更改配置密碼”下，選擇“進行更改”
3. 輸入您目前的設定密碼。
4. 輸入新密碼。密碼必須至少包含 8 個字符，但不能超過 32 個字符。密碼區分大小寫。
5. 將新的設定密碼儲存在安全的位置。它是安裝、擴充和維護過程所必需的。
6. 重新輸入新密碼，然後選擇*儲存*。

   當配置密碼變更完成後，系統將顯示綠色成功橫幅。

7. 選擇*恢復包*。
8. 輸入新的設定密碼來下載新的復原包。

更改配置密碼後，您必須立即下載新的恢復包。如果發生故障，恢復包檔案可讓您恢復系統。

更改節點控制台密碼

網格中的每個節點都有一個唯一的節點控制台密碼，您需要該密碼才能登入該節點。使用這些步驟來變更網格中每個節點的每個唯一節點控制台密碼。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"維護或 Root 存取權限"。
- 您擁有目前的設定密碼。

關於此任務

使用節點控制台密碼透過 SSH 以「管理員」身分登入節點，或透過 VM/實體控制台連線以 root 使用者身分登入。更改節點控制台密碼程序會為網格中的每個節點建立新密碼，並將密碼儲存在更新的 `Passwords.txt`恢復包中的檔案。密碼列在 Passwords.txt 檔案的密碼欄位中。

節點間通訊使用的 SSH 金鑰有單獨的 SSH 存取密碼。此程序不會變更 SSH 存取密碼。

訪問嚮導

步驟

1. 選擇*設定* > 存取控制 > 電網密碼。
2. 在*更改節點控制台密碼*下，選擇*進行更改*。

輸入設定密碼

步驟

1. 輸入您的網格的配置密碼。
2. 選擇*繼續*。

下載當前復原包

在變更節點控制台密碼之前，請下載目前的復原包。如果任何節點的密碼變更過程失敗，您可以使用此檔案中的密碼。

步驟

1. 選擇*下載恢復包*。

2. 複製復原包文件(`.zip`）到兩個安全、可靠且獨立的地點。

   復原包檔案必須是安全的，因為它包含可用於從StorageGRID系統取得資料的加密金鑰和密碼。

3. 選擇*繼續*。
4. 當確認對話方塊出現時，如果您準備好開始更改節點控制台密碼，請選擇*是*。

   一旦該過程開始，您就無法取消。

更改節點控制台密碼

當節點控制台密碼程序啟動時，將產生一個包含新密碼的新復原包。然後，在每個節點上更新密碼。

步驟

1. 等待新的恢復包生成，這可能需要幾分鐘。
2. 選擇*下載新的恢復包*。
3. 下載完成後：

   a. 打開 `.zip`文件。

   b. 確認您可以存取內容，包括 `Passwords.txt`文件，其中包含新的節點控制台密碼。

   c. 複製新的復原包文件(`.zip`）到兩個安全、可靠且獨立的地點。

      不要覆蓋舊的恢復包。

   復原包檔案必須是安全的，因為它包含可用於從StorageGRID系統取得資料的加密金鑰和密碼。

4. 選取核取方塊表示您已下載新的復原套件並驗證了內容。
5. 選擇*更改節點控制台密碼*並等待所有節點更新新密碼。這可能需要幾分鐘。

   如果所有節點的密碼都已更改，則會出現綠色的成功橫幅。轉至下一步。

   如果更新過程中出現錯誤，橫幅訊息會列出密碼變更失敗的節點數。系統將自動在密碼變更失敗的任何節點上重試該過程。如果該過程結束時某些節點仍未更改密碼，則會出現「重試」按鈕。

   如果一個或多個節點的密碼更新失敗：

   a. 查看表中列出的錯誤訊息。

   b. 解決問題。

   c. 選擇*重試*。

      重試僅更改在前一次密碼變更嘗試中失敗的節點上的節點控制台密碼。

6. 更改所有節點的節點控制台密碼後，刪除您下載的第一個復原包。
7. 或者，使用*恢復包*鏈接下載新恢復包的附加副本。

更改管理節點的 SSH 存取密碼

變更管理節點的 SSH 存取密碼也會更新網格中每個節點的唯一內部 SSH 金鑰集。主管理節點使用這些 SSH 金鑰透過安全、無密碼的身份驗證存取節點。

使用 SSH 金鑰以以下身分登入節點 `admin`或虛擬機器或實體控制台連接上的 root 使用者。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"維護或 Root 存取權限"。
- 您擁有目前的設定密碼。

關於此任務

管理節點的新存取密碼和每個節點的新內部金鑰儲存在 `Passwords.txt`恢復包中的檔案。密鑰列在該文件中的密碼列中。

節點間通訊使用的 SSH 金鑰有單獨的 SSH 存取密碼。這些不會因該過程而改變。

訪問嚮導

步驟

1. 選擇*設定* > 存取控制 > 電網密碼。
2. 在*更改 SSH 金鑰*下，選擇*進行更改*。

下載當前復原包

在變更 SSH 存取金鑰之前，請下載目前的復原包。如果任何節點的金鑰變更過程失敗，您可以使用此文件中的金鑰。

步驟

1. 輸入您的網格的配置密碼。
2. 選擇*下載恢復包*。
3. 複製復原包文件(`.zip`）到兩個安全、可靠且獨立的地點。

> 復原包檔案必須是安全的，因為它包含可用於從StorageGRID系統取得資料的加密金鑰和密碼。

4. 選擇*繼續*。
5. 當確認對話方塊出現時，如果您準備好開始變更 SSH 存取金鑰，請選擇「是」。

> 一旦該過程開始，您就無法取消。

變更 **SSH** 存取金鑰

當變更 SSH 存取金鑰程序開始時，將產生一個包含新金鑰的新復原包。然後，在每個節點上更新金鑰。

步驟

1. 等待新的恢復包生成，這可能需要幾分鐘。
2. 當「下載新的復原包」按鈕啟用時，選擇「下載新的復原包」並儲存新的復原包文件(`.zip`）到兩個安全、可靠且獨立的位置。
3. 下載完成後：

   a. 打開 `.zip`文件。

   b. 確認您可以存取內容，包括 `Passwords.txt`文件，其中包含新的 SSH 存取金鑰。

   c. 複製新的復原包文件(`.zip`）到兩個安全、可靠且獨立的地點。

   ! 不要覆蓋舊的恢復包。

   復原包檔案必須是安全的，因為它包含可用於從StorageGRID系統取得資料的加密金鑰和密碼。

4. 等待金鑰在每個節點上更新，這可能需要幾分鐘。

   如果所有節點的金鑰都發生了更改，則會出現綠色的成功橫幅。

   如果更新過程中出現錯誤，橫幅訊息會列出未能更改金鑰的節點數。系統將自動在密鑰更改失敗的任何節點上重試該過程。如果該過程結束時某些節點仍未更改金鑰，則會出現「重試」按鈕。

   如果一個或多個節點的金鑰更新失敗：

   a. 查看表中列出的錯誤訊息。

   b. 解決問題。

   c. 選擇*重試*。

      重試只會變更先前金鑰變更嘗試期間失敗的節點上的 SSH 存取金鑰。

5. 在所有節點的 SSH 存取金鑰變更後，刪除您下載的第一個復原包。
6. 或者，選擇 維護 > 系統 > 恢復包 來下載新恢復包的額外副本。

使用身分聯合

使用身份聯合可以更快地設定群組和用戶，並允許用戶使用熟悉的憑證登入StorageGRID。

為網格管理器配置身份聯合

如果您希望在另一個系統（例如 Active Directory、Azure Active Directory（Azure AD）、OpenLDAP 或 Oracle Directory Server）中管理管理員群組和用戶，則可以在網格管理器中設定身分合併。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"特定存取權限"。
- 您正在使用 Active Directory、Azure AD、OpenLDAP 或 Oracle Directory Server 作為身分提供者。

如果您想使用未列出的 LDAP v3 服務，請聯絡技術支援。

- 如果您打算使用 OpenLDAP，則必須設定 OpenLDAP 伺服器。看配置 OpenLDAP 伺服器的指南 。
- 如果您打算啟用單一登入 (SSO)，您已查看"單一登入的要求和注意事項"。
- 如果您打算使用傳輸層安全性 (TLS) 與 LDAP 伺服器進行通信，則身分提供者將使用 TLS 1.2 或 1.3。看"傳出 TLS 連線支援的密碼" 。

關於此任務

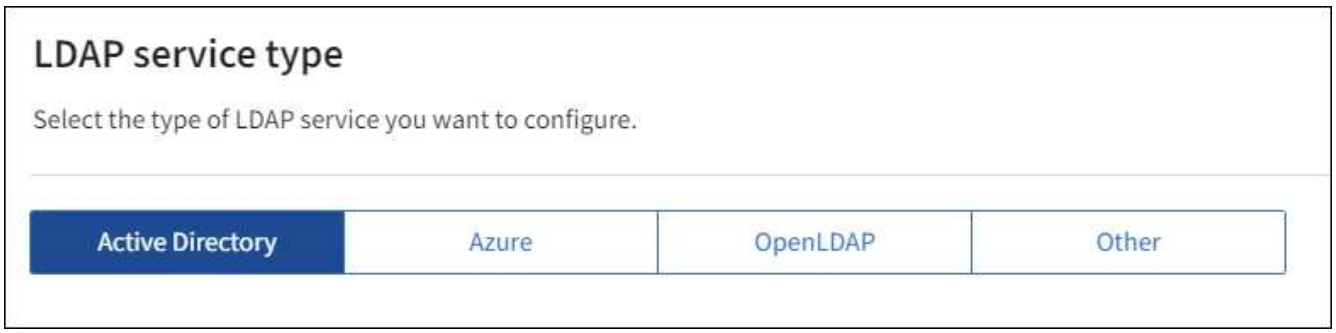
如果您想要從其他系統（例如 Active Directory、Azure AD、OpenLDAP 或 Oracle Directory Server）匯入群組，則可以為網格管理員設定身分來源。您可以匯入以下類型的群組：

- 管理組。管理群組中的使用者可以登入網格管理器並根據指派給該群組的管理權限執行任務。
- 不使用自己的身分來源的租用戶的租用戶使用者群組。租用戶群組中的使用者可以登入租用戶管理員並根據租用戶管理員中指派給該群組的權限執行任務。看"建立租用戶帳戶"和"使用租用戶帳戶"了解詳情。

輸入配置

步驟

1. 選擇*配置* > 存取控制 > 身份聯合。
2. 選擇*啟用身份聯合*。
3. 在 LDAP 服務類型部分中，選擇要設定的 LDAP 服務類型。



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

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

Active Directory 和 `entryUUID`對於 OpenLDAP。如果您正在設定 Oracle Directory Server，請輸入 `nsuniqueid。每個群組的指定屬性的值必須是 16 位元組或字串格式的 32 位元十六進位數，其中連字元將被忽略。

5. 對於所有 LDAP 服務類型，請在設定 LDAP 伺服器部分輸入所需的 LDAP 伺服器和網路連線資訊。
   - 主機名稱：LDAP 伺服器的完全限定網域名稱 (FQDN) 或 IP 位址。
   - 連接埠：用於連接 LDAP 伺服器的連接埠。

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

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

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

     指定的使用者必須具有列出群組和使用者以及存取以下屬性的權限：

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

   - 密碼：與使用者名稱關聯的密碼。

     如果您將來更改密碼，則必須在此頁面上更新。

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

     *群組唯一名稱*值在其所屬的*群組基本 DN*內必須是唯一的。

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

     *使用者唯一名稱*值在其所屬的*使用者基本 DN*內必須是唯一的。

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

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

     輸入以下模式之一：

     - **UserPrincipalName** 模式（**Active Directory** 和 **Azure**）：[USERNAME]@*example*.com

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

  完全按照書寫方式包含 **[USERNAME]**。

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

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

7. 如果您選擇了 STARTTLS 或 LDAPS，請選擇用於保護連線的憑證。
   - 使用作業系統 **CA** 憑證：使用作業系統上安裝的預設 Grid CA 憑證來保護連線。
   - 使用自訂 **CA** 憑證：使用自訂安全性憑證。

     如果選擇此設置，請將自訂安全性憑證複製並貼上到 CA 憑證文字方塊中。

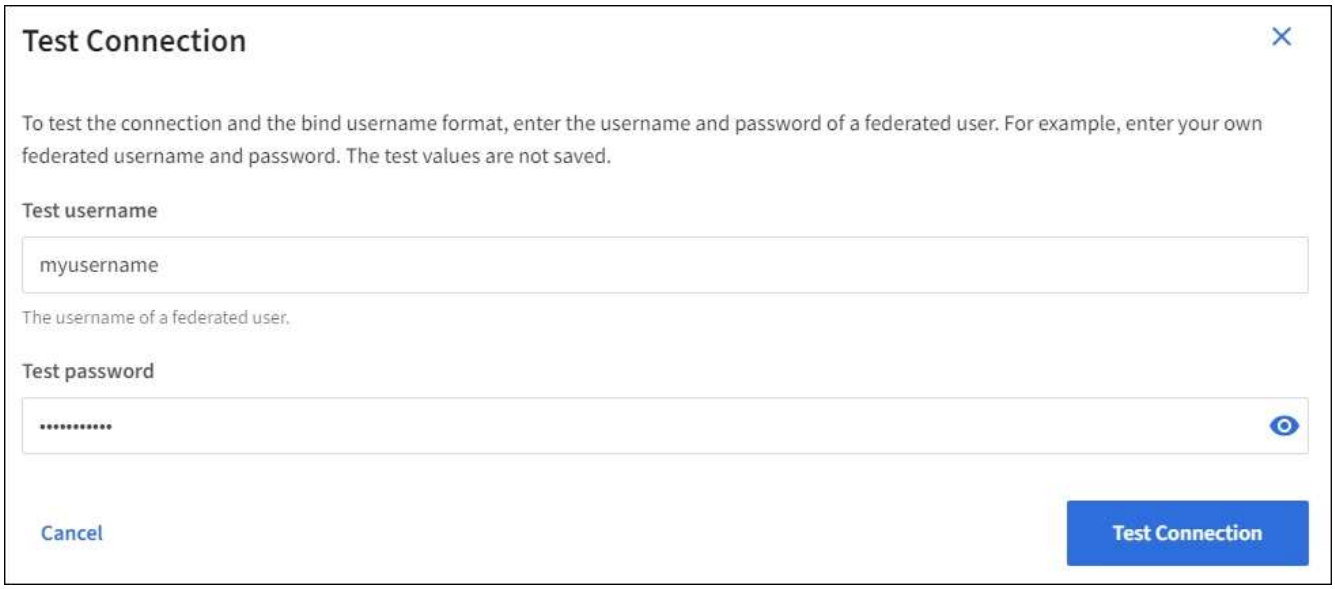
測試連接並儲存配置

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

步驟

1. 選擇*測試連線*。
2. 如果您沒有提供綁定使用者名稱格式：
   - 如果連線設定有效，則會出現「測試連線成功」訊息。選擇*儲存*以儲存配置。
   - 如果連線設定無效，則會出現「無法建立測試連線」訊息。選擇*關閉*。然後，解決所有問題並再次測試連線。
3. 如果您提供了綁定使用者名稱格式，請輸入有效聯合使用者的使用者名稱和密碼。

   例如，輸入您自己的使用者名稱和密碼。用戶名中不要包含任何特殊字符，例如 @ 或 /。



- 如果連線設定有效，則會出現「測試連線成功」訊息。選擇*儲存*以儲存配置。
- 如果連線設定、綁定使用者名稱格式或測試使用者名稱和密碼無效，則會出現錯誤訊息。解決任何問題並再次測試連接。

強制與身分來源同步

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

步驟

1. 前往身份聯合頁面。
2. 選擇頁面頂部的*同步伺服器*。

   同步過程可能需要一些時間，具體取決於您的環境。

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

禁用身份聯合

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

關於此任務

在停用身分聯合之前，您應該注意以下事項：

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

步驟

1. 前往身份聯合頁面。
2. 取消選取「啟用身份聯合」複選框。

配置 **OpenLDAP** 伺服器的指南

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

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

Memberof 和 **refint** 覆蓋

應該啟用 memberof 和 refint 覆蓋。有關詳細信息，請參閱http://www.openldap.org/doc/admin24/index.html["OpenLDAP 文件：版本 2.4 管理員指南"^]。

索引

您必須使用指定的索引關鍵字來設定下列 OpenLDAP 屬性：

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

此外，請確保幫助中提到的使用者名字段已索引，以獲得最佳效能。

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

管理管理員群組

您可以建立管理員群組來管理一個或多個管理員使用者的安全權限。使用者必須屬於某個群組才能被授予對StorageGRID系統的存取權限。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"特定存取權限"。
- 如果您計劃匯入聯合群組，則您已配置身分聯合，且聯合群組已存在於配置的身分來源中。

建立管理員群組

管理群組可讓您確定哪些使用者可以存取網格管理器和網格管理 API 中的哪些功能和操作。

訪問嚮導

步驟

1. 選擇 配置 > 存取控制 > 管理群組。
2. 選擇*建立群組*。

選擇群組類型

您可以建立本機群組或匯入聯合群組。

- 如果要為本機使用者指派權限，請建立本機群組。
- 建立聯合群組以從身分來源匯入使用者。

本地群組

步驟

1. 選擇*本機群組*。
2. 輸入群組的顯示名稱，您可以根據需要稍後更新。例如，「維護使用者」或「ILM 管理員」。
3. 為該群組輸入一個唯一的名稱，該名稱以後無法更新。
4. 選擇*繼續*。

聯合組

步驟

1. 選擇*聯合組*。
2. 輸入要匯入的群組的名稱，與設定的身份來源中顯示的名稱完全一致。
   - 對於 Active Directory 和 Azure，使用 sAMAccountName。
   - 對於 OpenLDAP，使用 CN（通用名稱）。
   - 對於另一個 LDAP，請使用 LDAP 伺服器的適當唯一名稱。
3. 選擇*繼續*。

管理群組權限

步驟

1. 對於*存取模式*，選擇群組中的使用者是否可以更改設定並在網格管理器和網格管理 API 中執行操作，或者他們是否只能查看設定和功能。
   - 讀寫（預設）：使用者可以更改設定並執行其管理權限允許的操作。
   - 只讀：使用者只能查看設定和功能。他們無法在網格管理器或網格管理 API 中進行任何更改或執行任何操作。本機只讀使用者可以更改自己的密碼。

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

2. 選擇一個或多個"管理員群組權限"。

   您必須為每個群組指派至少一個權限；否則，屬於該群組的使用者將無法登入StorageGRID。

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

新增使用者（僅限本地群組）

步驟

1. 或者，為此群組選擇一個或多個本機使用者。

   如果您尚未建立本機用戶，則可以儲存群組而不新增使用者。您可以在「使用者」頁面上將此群組新增至使用者。看"管理用戶"了解詳情。

2. 選擇*建立群組*和*完成*。

檢視和編輯管理員群組

您可以查看現有群組的詳細資訊、修改群組或複製群組。

- 要查看所有群組的基本信息，請查看群組頁面上的表格。
- 若要查看特定群組的所有詳細資訊或編輯群組，請使用*操作*功能表或詳細資料頁面。

任務	操作選單	詳細資訊頁面
查看群組詳情	a. 選取該組的複選框。 b. 選擇*動作* > 查看群組詳情。	在表中選擇組名。
編輯顯示名稱（僅限本機群組）	a. 選取該組的複選框。 b. 選擇*操作* > 編輯群組名稱。 c. 輸入新名稱。 d. 選擇“儲存變更”。	a. 選擇群組名稱以顯示詳細資訊。 b. 選擇編輯圖標 。 c. 輸入新名稱。 d. 選擇“儲存變更”。
編輯存取模式或權限	a. 選取該組的複選框。 b. 選擇*動作* > 查看群組詳情。 c. 或者，更改群組的存取模式。 d. （可選）選擇或清除"管理員群組權限"。 e. 選擇“儲存變更”。	a. 選擇群組名稱以顯示詳細資訊。 b. 或者，更改群組的存取模式。 c. （可選）選擇或清除"管理員群組權限"。 d. 選擇“儲存變更”。

複製群組

步驟

1. 選取該組的複選框。
2. 選擇*動作* > 複製群組。
3. 完成複製組精靈。

刪除群組

當您想要從系統中刪除該群組時，您可以刪除該管理員群組，並刪除與該群組相關的所有權限。刪除管理員群組會從群組中刪除所有用戶，但不會刪除用戶。

步驟

1. 在「群組」頁面中，選取要刪除的每個群組的核取方塊。
2. 選擇*動作* > 刪除群組。
3. 選擇*刪除群組*。

管理員群組權限

建立管理員使用者群組時，您可以選擇一個或多個權限來控制對網格管理器特定功能的存取。然後，您可以將每個使用者指派到一個或多個管理群組，以確定該使用者可以執行哪些任務。

您必須為每個群組指派至少一個權限；否則，屬於該群組的使用者將無法登入網格管理器或網格管理 API。

預設情況下，屬於具有至少一個權限的群組的任何使用者都可以執行以下任務：

- Sign in入網格管理器
- 查看儀表板
- 查看節點頁面
- 查看當前和已解決的警報
- 更改自己的密碼（僅限本地用戶）
- 查看配置和維護頁面上提供的某些信息

權限與存取模式的交互

對於所有權限，群組的*存取模式*設定決定使用者是否可以變更設定和執行操作，或者是否只能查看相關設定和功能。如果使用者屬於多個群組，並且任何群組設定為*只讀*，則該使用者將對所有選定的設定和功能具有唯讀存取權限。

以下部分描述了建立或編輯管理員群組時可以指派的權限。任何未明確提及的功能都需要*Root 存取*權限。

Root 存取權限

此權限提供對所有網格管理功能的存取。

更改租用戶 **root** 密碼

此權限提供對租用戶頁面上的*更改 root 密碼*選項的存取權限，讓您可以控制誰可以更改租用戶本地 root 使用者的密碼。啟用 S3 金鑰導入功能時，此權限也用於遷移 S3 金鑰。沒有此權限的使用者無法看到*更改 root 密碼*選項。

若要授予包含「變更根密碼」選項的「租用戶」頁面的存取權限，也需指派「租用戶帳號」權限。

電網拓撲頁面配置

此權限提供對 **SUPPORT** > **Tools** > **Grid topology** 頁面上的配置標籤的存取權限。

網格拓撲頁面已被棄用，並將在未來版本中刪除。

工業光魔

此權限提供對以下 **ILM** 選單選項的存取：

- 規則
- 政策
- 策略標籤
- 儲存池
- 儲存等級
- 區域
- 對像元資料查找

使用者必須具備*其他電網配置*和*電網拓撲頁面配置*權限才能管理儲存等級。

維護

使用者必須具有維護權限才能使用這些選項：

- 配置 > 存取控制：
  - 電網密碼
- 配置 > 網路：
  - S3 端點域名
- 維護 > 任務：
  - 退休
  - 擴張
  - 對象存在性檢查
  - 恢復
- 維護 > 系統：
  - 恢復包
  - 軟體更新
- 支援 > 工具：
  - 紀錄

沒有維護權限的使用者可以查看但不能編輯以下頁面：

- 維護 > 網路：
  - DNS 伺服器
  - 網格網絡
  - NTP 伺服器
- 維護 > 系統：
  - 執照
- 配置 > 網路：
  - S3 端點域名
- 配置 > 安全：
  - 證書
- 配置 > 監控：
  - 審計和系統日誌伺服器

管理警報

此權限提供對管理警報選項的存取。使用者必須擁有此權限才能管理靜默、警報通知和警報規則。

指標查詢

此權限提供以下存取權限：

- 支援 > 工具 > *指標*頁面
- 使用網格管理 API 的 **Metrics** 部分自訂 Prometheus 指標查詢
- 包含指標的網格管理器儀表闆卡

對像元資料查找

此權限提供對 **ILM** > 物件元資料查找 頁面的存取權限。

其他電網配置

此權限提供對其他網格配置選項的存取。

要查看這些附加選項，使用者還必須具有*網格拓撲頁面配置*權限。

- 工業光魔（ILM）：
  - 儲存等級
- 配置 > 系統：
- 支援 > 其他：
  - 鏈路成本

儲存設備管理員

此權限提供：

- 透過網格管理器存取儲存設備上的 E 系列SANtricity系統管理器。
- 能夠在支援這些操作的裝置的「管理磁碟機」標籤上執行故障排除和維護任務。

租戶帳戶

此權限提供以下功能：

- 造訪租戶頁面，您可以在其中建立、編輯和刪除租戶帳戶
- 查看現有的流量分類策略
- 查看包含租戶詳細資訊的網格管理器儀表闆卡

管理用戶

您可以查看本地用戶和聯合用戶。您還可以建立本機使用者並將其指派到本機管理員群組，以確定這些使用者可以存取哪些網格管理器功能。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"特定存取權限"。

建立本地用戶

您可以建立一個或多個本機用戶，並將每個用戶指派到一個或多個本機群組。此群組的權限控制使用者可以存取哪些網格管理器和網格管理 API 功能。

您只能建立本機使用者。使用外部身分來源來管理聯合使用者和群組。

網格管理器包含一個預先定義的本機用戶，名為「root」。您不能刪除 root 使用者。

如果啟用單一登入 (SSO)，本機使用者將無法登入StorageGRID。

訪問嚮導

步驟

1. 選擇 配置 > 存取控制 > 管理員使用者。
2. 選擇*建立使用者*。

輸入使用者憑證

步驟

1. 輸入使用者的全名、唯一的使用者名稱和密碼。
2. 或者，如果此使用者不應存取網格管理器或網格管理 API，請選擇「是」。

3. 選擇*繼續*。

分配給群組

步驟

1. 或者，將使用者指派到一個或多個群組以確定使用者的權限。

   如果您尚未建立群組，則可以在不選擇群組的情況下儲存使用者。您可以在「群組」頁面上將此使用者新增至群組。

   如果使用者屬於多個群組，則權限是累積的。看"管理管理員群組"了解詳情。

2. 選擇*建立使用者*並選擇*完成*。

查看和編輯本地用戶

您可以查看現有本地用戶和聯合用戶的詳細資訊。您可以修改本機使用者以變更使用者的全名、密碼或群組成員身分。您也可以暫時阻止使用者存取網格管理器和網格管理 API。

您只能編輯本機使用者。使用外部身分來源來管理聯合使用者。

- 要查看所有本地和聯合用戶的基本信息，請查看“用戶”頁面上的表格。
- 若要查看特定使用者的所有詳細資訊、編輯本機使用者或變更本機使用者的密碼，請使用*操作*功能表或詳細資料頁面。

  任何編輯都會在使用者下次登出並重新登入網格管理器時套用。

  本機使用者可以使用網格管理器橫幅中的「變更密碼」選項來變更自己的密碼。

任務	操作選單	詳細資訊頁面
查看用戶詳細信息	a. 選取使用者的複選框。 b. 選擇*操作* > 查看使用者詳細資料。	在表中選擇用戶的姓名。
編輯全名（僅限本地用戶）	a. 選取使用者的複選框。 b. 選擇*動作* > 編輯全名。 c. 輸入新名稱。 d. 選擇“儲存變更”。	a. 選擇使用者的名稱以顯示詳細資訊。 b. 選擇編輯圖標。 c. 輸入新名稱。 d. 選擇“儲存變更”。

任務	操作選單	詳細資訊頁面
拒絕或允許StorageGRID訪問	a. 選取使用者的複選框。 b. 選擇*操作* > 查看使用者詳細資料。 c. 選擇“訪問”選項卡。 d. 選擇「是」以阻止使用者登入網格管理員或網格管理 API，或選擇「否」以允許使用者登入。 e. 選擇“儲存變更”。	a. 選擇使用者的名稱以顯示詳細資訊。 b. 選擇“訪問”選項卡。 c. 選擇「是」以阻止使用者登入網格管理員或網格管理 API，或選擇「否」以允許使用者登入。 d. 選擇“儲存變更”。
更改密碼（僅限本機用戶）	a. 選取使用者的複選框。 b. 選擇*操作* > 查看使用者詳細資料。 c. 選擇密碼選項卡。 d. 輸入新密碼。 e. 選擇*更改密碼*。	a. 選擇使用者的名稱以顯示詳細資訊。 b. 選擇密碼選項卡。 c. 輸入新密碼。 d. 選擇*更改密碼*。
更改群組（僅限本機用戶）	a. 選取使用者的複選框。 b. 選擇*操作* > 查看使用者詳細資料。 c. 選擇“群組”標籤。 d. 或者，選擇群組名稱後的連結以在新瀏覽器標籤中查看群組的詳細資訊。 e. 選擇*編輯群組*來選擇不同的群組。 f. 選擇“儲存變更”。	a. 選擇使用者的名稱以顯示詳細資訊。 b. 選擇“群組”標籤。 c. 或者，選擇群組名稱後的連結以在新瀏覽器標籤中查看群組的詳細資訊。 d. 選擇*編輯群組*來選擇不同的群組。 e. 選擇“儲存變更”。

複製用戶

您可以複製現有使用者來建立具有相同權限的新使用者。

步驟

1. 選取使用者的複選框。
2. 選擇*動作* > 重複使用者。
3. 完成重複使用者嚮導。

刪除用戶

您可以刪除本機使用者以從系統中永久刪除該使用者。

您不能刪除 root 使用者。

步驟

1. 在「使用者」頁面中，選取要刪除的每個使用者的核取方塊。

2. 選擇*操作* > 刪除使用者。
3. 選擇*刪除使用者*。

使用單一登入 (SSO)

配置單一登入

啟用單一登入 (SSO) 後，只有使用貴組織實作的 SSO 登入流程授權使用者的憑證，使用者才能存取網格管理員、租用戶管理器、網格管理 API 或租用戶管理 API。本機使用者無法登入StorageGRID。

單一登入的工作原理

StorageGRID系統支援使用安全性斷言標記語言 2.0 (SAML 2.0) 標準的單一登入 (SSO)。

在啟用單一登入 (SSO) 之前，請先查看啟用 SSO 時StorageGRID登入和登出程序會受到怎樣的影響。

啟用 **SSO** 後**Sign in**

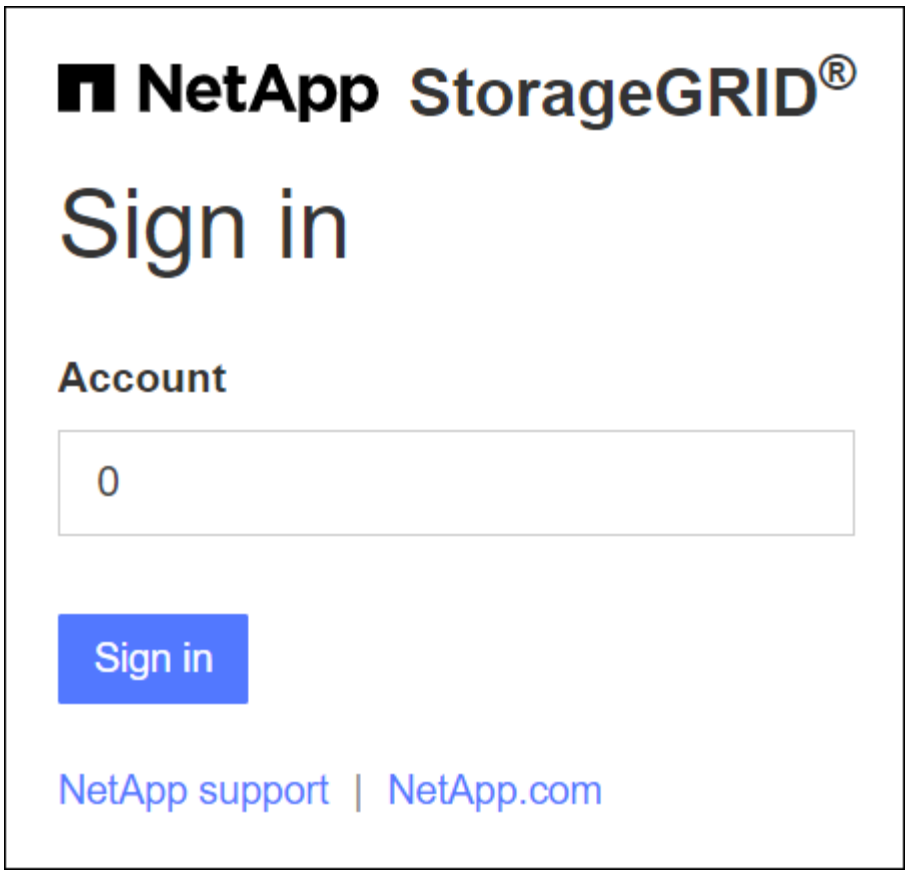
當啟用 SSO 並且您登入StorageGRID時，您將被重新導向到您組織的 SSO 頁面以驗證您的憑證。

步驟

1. 在 Web 瀏覽器中輸入任何StorageGRID管理節點的完全限定網域名稱或 IP 位址。

   出現StorageGRIDSign in頁面。

   - 如果這是您第一次在此瀏覽器上造訪該 URL，系統會提示您輸入帳戶 ID：

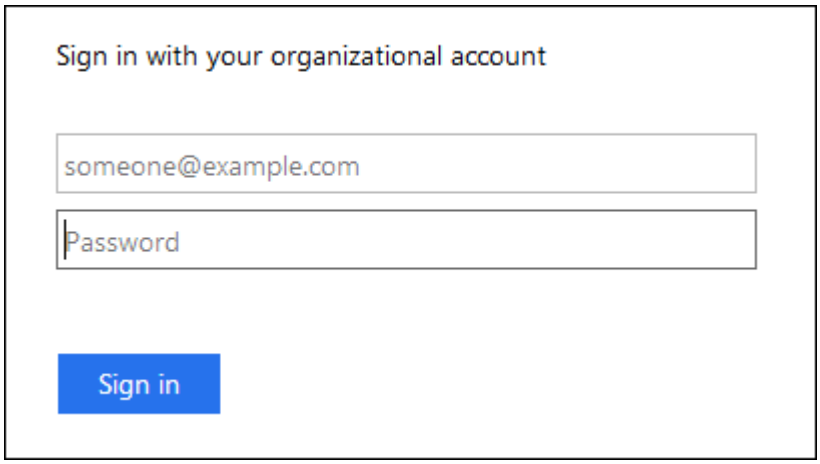


- 如果您之前曾造訪過網格管理器或租用戶管理器，系統會提示您選擇最近的帳戶或輸入帳戶 ID：

當您Sign in租用戶帳戶的完整 URL（即完全限定網域名稱或 IP 位址，後面接著 `/?accountId=20-digit-account-id`）。相反，您會立即重定向到您組織的 SSO 登入頁面，您可以在其中使用您的 SSO 憑證登入。

2. 指示您是否要存取網格管理器或租戶管理器：
   - 若要存取網格管理器，請將「帳戶 **ID**」欄位留空，輸入「**0**」作為帳戶 ID，或選擇「網格管理員」（如果它出現在最近帳戶清單中）。
   - 若要存取租用戶管理器，請輸入 20 位租用戶帳號 ID，或按名稱選擇最近帳戶清單中出現的租用戶。
3. 選擇 **Sign in**

   StorageGRID將您重新導向至您組織的 SSO 登入頁面。例如：



4. 使用您的 SSO 憑證Sign in。

   如果您的 SSO 憑證正確：

   a. 身分提供者 (IdP) 向StorageGRID提供驗證回應。
   b. StorageGRID驗證身份驗證回應。
   c. 如果回應有效且您屬於具有StorageGRID存取權限的聯合群組，您將登入網格管理器或租用戶管理器，具體取決於您選擇的帳戶。

   > 如果服務帳戶無法訪問，您仍然可以登錄，只要您是屬於具有StorageGRID存取權限的聯合群組的現有使用者。

5. 或者，如果您有足夠的權限，可以存取其他管理節點，或存取網格管理器或租用戶管理器。

   您不需要重新輸入您的 SSO 憑證。

啟用 **SSO** 後退出

當為StorageGRID啟用 SSO 時，您登出時發生的情況取決於您登入的內容以及您從哪裡登出。

步驟

1. 找到使用者介面右上角的「退出」連結。
2. 選擇“退出”。

   出現StorageGRIDSign in頁面。 *最近的帳戶*下拉式選單已更新，包括*網格管理員*或租用戶的名稱，因此您將來可以更快地存取這些使用者介面。

如果您已登入...	然後您退出...	您已退出...
一個或多個管理節點上的網格管理器	任何管理節點上的網格管理器	所有管理節點上的網格管理器 *注意：*如果您使用 Azure 進行 SSO，可能需要幾分鐘才能退出所有管理節點。
一個或多個管理節點上的租戶管理器	任何管理節點上的租戶管理器	所有管理節點上的租戶管理器
網格管理器和租戶管理器	網格管理器	僅限網格管理器。您也必須退出租戶管理器才能退出 SSO。

表格總結了當您使用單一瀏覽器工作階段時登出時發生的情況。如果您透過多個瀏覽器會話登入StorageGRID ，則必須分別登出所有瀏覽器工作階段。

單一登入的要求和注意事項

在為StorageGRID系統啟用單一登入 (SSO) 之前，請查看要求和注意事項。

身份提供者要求

StorageGRID支援以下 SSO 身分提供者 (IdP)：

- Active Directory 聯合驗證服務 (AD FS)
- Azure Active Directory (Azure AD)
- Ping聯邦

您必須先為StorageGRID系統設定身分聯合，然後才能設定 SSO 身分提供者。用於身分聯合的 LDAP 服務類型控制您可以實現哪種類型的 SSO。

配置的 **LDAP** 服務類型	**SSO** 身分提供者的選項
活動目錄	• 活動目錄 • Azure • Ping聯邦
Azure	Azure

AD FS 要求

您可以使用下列任一版本的 AD FS：

- Windows Server 2022 AD FS
- Windows Server 2019 AD FS

- Windows Server 2016 AD FS

> Windows Server 2016 應該使用 "KB3201845 更新"或更高。

其他要求

- 傳輸層安全性 (TLS) 1.2 或 1.3
- Microsoft .NET Framework，版本 3.5.1 或更高版本

Azure 的注意事項

如果您使用 Azure 作為 SSO 類型，且使用者的使用者主體名稱不使用 sAMAccountName 作為前綴，則當StorageGRID與 LDAP 伺服器失去連線時，可能會發生登入問題。若要允許使用者登入，您必須恢復與 LDAP 伺服器的連線。

伺服器證書要求

預設情況下， StorageGRID在每個管理節點上使用管理介面憑證來保護對網格管理器、租用戶管理員、網格管理 API 和租用戶管理 API 的存取。為StorageGRID設定信賴方信任 (AD FS)、企業應用程式 (Azure) 或服務供應商連線 (PingFederate) 時，您可以使用伺服器憑證作為StorageGRID請求的簽章憑證。

如果你還沒有"為管理介面配置自訂證書"，你現在就應該這麼做。當您安裝自訂伺服器憑證時，它將用於所有管理節點，並且您可以在所有StorageGRID依賴方信任、企業應用程式或SP連線中使用它。

> 不建議在依賴方信任、企業應用程式或SP連線中使用管理節點的預設伺服器憑證。如果節點發生故障並且您恢復了它，則會產生新的預設伺服器憑證。在登入復原的節點之前，您必須使用新憑證更新信賴方信任、企業應用程式或SP連線。

您可以透過登入節點的命令 shell 並轉到 `/var/local/mgmt-api`目錄。自訂伺服器憑證名為 `custom-server.crt`。該節點的預設伺服器憑證名為 `server.crt`。

端口要求

受限的網格管理器或租戶管理器連接埠上不提供單一登入 (SSO)。如果您希望使用者透過單一登入進行驗證，則必須使用預設 HTTPS 連接埠 (443)。看"控制外部防火牆的訪問" 。

確認聯合用戶可以登入

在啟用單一登入 (SSO) 之前，您必須確認至少有一個共同使用者可以登入網格管理員和任何現有租用戶帳戶的租用戶管理員。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"特定存取權限"。
- 您已經配置了身份聯合。

步驟

1. 如果存在現有租用戶帳戶，請確認沒有任何租戶使用其自己的身分來源。

啟用 SSO 時，租用戶管理員中設定的身份來源將會被網格管理器中設定的身份來源覆寫。屬於租用戶身分來源的使用者將無法再登入，除非他們擁有 Grid Manager 身分來源的帳戶。

a. Sign in每個租用戶帳戶的租用戶管理員。

b. 選擇*存取管理* > 身分聯合。

c. 確認未選取「啟用身份聯合」複選框。

d. 如果是，請確認該租用戶帳戶可能使用的任何聯合群組不再需要，清除複選框，然後選擇*儲存*。

2. 確認聯合用戶可以存取網格管理器：

a. 從網格管理員中，選擇 配置 > 存取控制 > 管理群組。

b. 確保已從 Active Directory 身分來源匯入至少一個聯合群組，並且已為其指派 Root 存取權限。

c. 登出。

d. 確認您可以作為聯合群組中的使用者重新登入網格管理器。

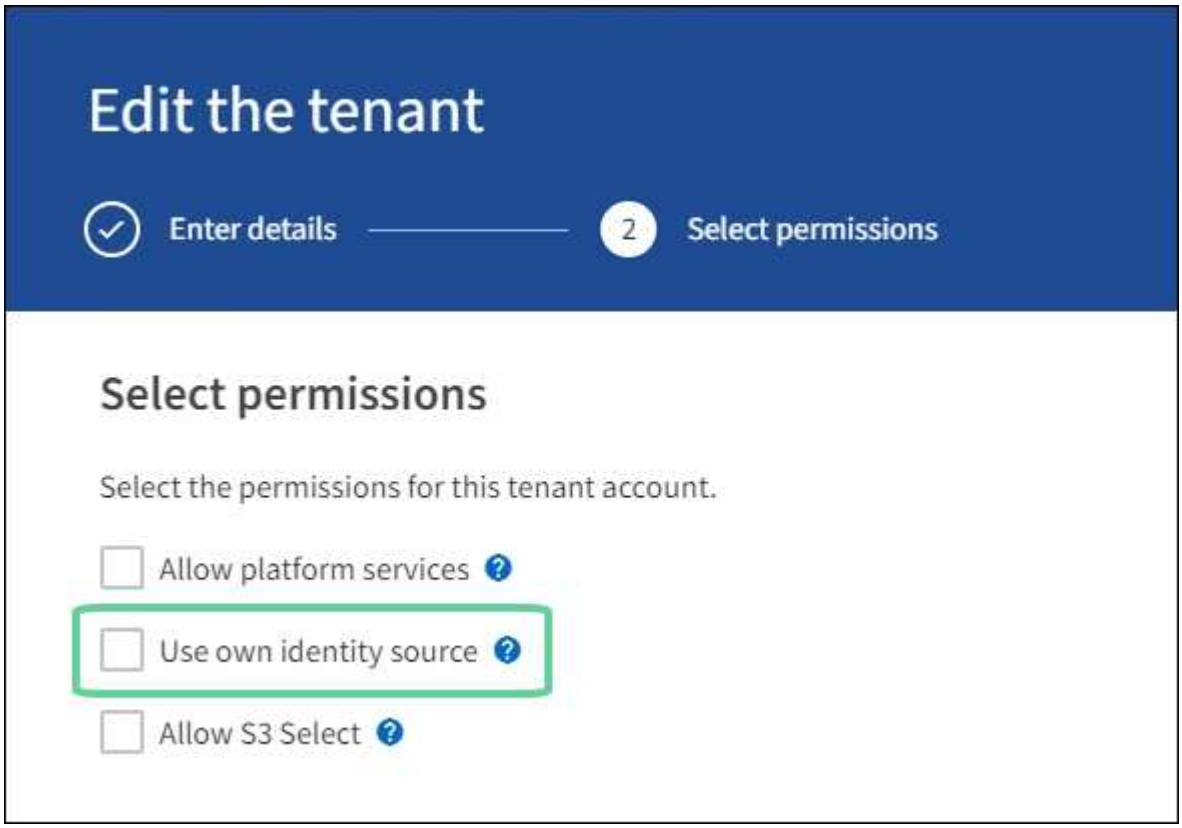
3. 如果存在現有的租用戶帳戶，請確認具有 Root 存取權限的共同使用者可以登入：

a. 從網格管理器中選擇*TENANTS*。

b. 選擇租用戶帳戶，然後選擇*操作* > 編輯。

c. 在「輸入詳細資料」標籤上，選擇「繼續」。

d. 如果選取了*使用自己的身分來源*複選框，請取消選取該框並選擇*儲存*。



出現「租戶」頁面。

a. 選擇租戶帳號，選擇*Sign in*，以本地root用戶登入租戶帳號。

b. 從租用戶管理員中，選擇*存取管理* > 群組。

c. 確保網格管理員中的至少一個聯合群組已指派此租用戶的 Root 存取權限。

d. 登出。

e. 確認您可以以聯合群組中的使用者重新登入租用戶。

相關資訊

- "單一登入的要求和注意事項"
- "管理管理員群組"
- "使用租用戶帳戶"

使用沙盒模式

您可以使用沙盒模式來設定和測試單一登入 (SSO)，然後為所有StorageGRID使用者啟用它。啟用 SSO 後，您可以在需要變更或重新測試設定時返回沙盒模式。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"Root存取權限"。
- 您已為StorageGRID系統配置身份聯合。
- 對於身分識別聯合 **LDAP** 服務類型，您可以根據計畫使用的 SSO 身分提供者選擇 Active Directory 或 Azure。

配置的 **LDAP** 服務類型	**SSO** 身分提供者的選項
活動目錄	• 活動目錄 • Azure • Ping聯邦
Azure	Azure

關於此任務

當啟用 SSO 且使用者嘗試登入管理節點時， StorageGRID會向 SSO 身分提供者傳送驗證請求。反過來，SSO 身份提供者將身份驗證回應傳送回StorageGRID，指示身份驗證請求是否成功。對於成功的請求：

- Active Directory 或 PingFederate 的回應包括使用者的通用唯一識別碼 (UUID)。
- Azure 的回應包括使用者主體名稱 (UPN)。

為了允許StorageGRID （服務提供者）和 SSO 身分提供者就使用者驗證請求進行安全通信，您必須在StorageGRID中設定某些設定。接下來，您必須使用 SSO 身分提供者的軟體為每個管理節點建立信賴方信任 (AD FS)、企業應用程式 (Azure) 或服務提供者 (PingFederate)。最後，您必須返回StorageGRID以啟用 SSO。

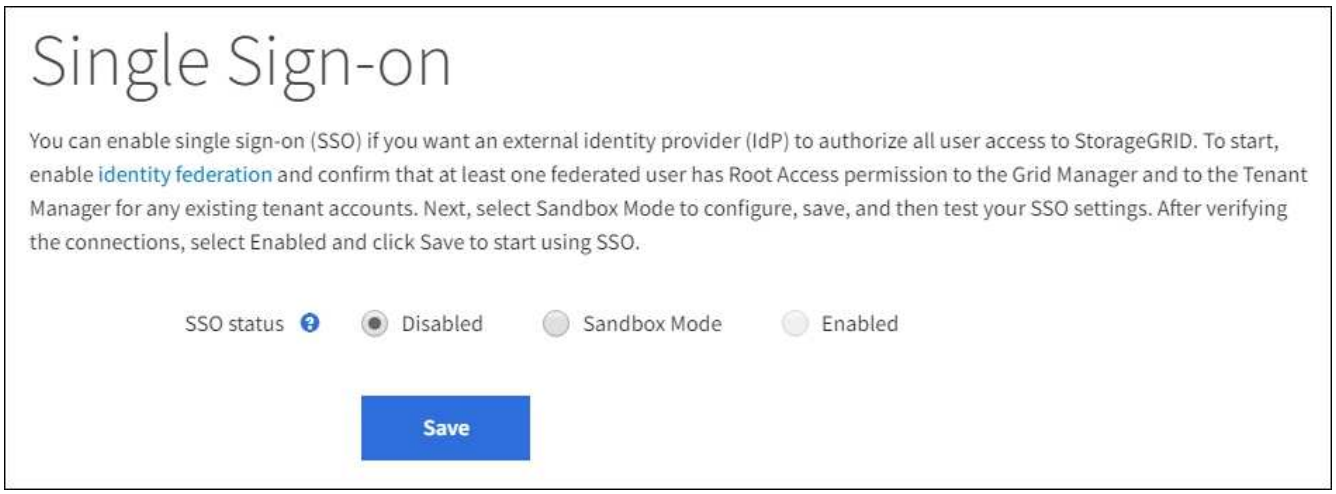
沙盒模式可以輕鬆執行此來回配置，並在啟用 SSO 之前測試所有設定。當您使用沙盒模式時，使用者無法使用 SSO 登入。

訪問沙盒模式

步驟

1. 選擇*設定* > 存取控制 > 單一登入。

   出現「單一登入」頁面，其中選擇了「已停用」選項。



   如果未出現 SSO 狀態選項，請確認您已將身分提供者設定為聯合身分識別來源。看"單一登入的要求和注意事項" 。

2. 選擇*沙盒模式*。

   出現身分提供者部分。

輸入身份提供者詳細信息

步驟

1. 從下拉清單中選擇 **SSO** 類型。
2. 根據您選擇的 SSO 類型填入身分提供者部分中的欄位。

活動目錄

a. 輸入身分識別提供者的*聯合身分驗證服務名稱*，與其在 Active Directory 聯合驗證服務 (AD FS) 中顯示的名稱完全一致。

> 若要找到聯合服務名稱，請前往 Windows 伺服器管理員。選擇“工具”>“AD FS 管理”。從操作選單中，選擇*編輯聯合服務屬性*。聯合服務名稱顯示在第二個欄位中。

b. 指定當身分識別提供者回應StorageGRID請求傳送 SSO 設定資訊時將使用哪個 TLS 憑證來保護連線。

- 使用作業系統 **CA** 憑證：使用作業系統上安裝的預設 CA 憑證來保護連線。
- 使用自訂 **CA** 憑證：使用自訂 CA 憑證來保護連線。

  如果選擇此設置，請複製自訂憑證的文字並將其貼上到 **CA** 憑證 文字方塊中。
- 不要使用 **TLS**：不要使用 TLS 憑證來保護連線。

> 如果您更改了 CA 證書，請立即"在管理節點上重新啟動 mgmt-api 服務"並測試是否成功 SSO 進入網格管理器。

c. 在「依賴方」部分中，指定StorageGRID的「依賴方識別碼」。此值控制您在 AD FS 中為每個信賴方信任所使用的名稱。

- 例如，如果您的網格只有一個管理節點，且您不打算在將來新增更多管理節點，請輸入 `SG` 或者 `StorageGRID`。
- 如果您的網格包含多個管理節點，請包含字串 `[HOSTNAME]` 在標識符中。例如，`SG-[HOSTNAME]`。這將產生一個表，根據節點的主機名稱顯示系統中每個管理節點的依賴方識別碼。

> 您必須為StorageGRID系統中的每個管理節點建立一個依賴方信任。每個管理節點都擁有依賴方信任，確保使用者可以安全地登入和登出任何管理節點。

d. 選擇*儲存*。

*儲存*按鈕上會出現綠色複選標記，持續幾秒鐘。

Azure

a. 指定當身分識別提供者回應StorageGRID請求傳送 SSO 設定資訊時將使用哪個 TLS 憑證來保護連線。

- 使用作業系統 **CA** 憑證：使用作業系統上安裝的預設 CA 憑證來保護連線。
- 使用自訂 **CA** 憑證：使用自訂 CA 憑證來保護連線。

  如果選擇此設置，請複製自訂憑證的文字並將其貼上到 **CA** 憑證 文字方塊中。

- 不要使用 **TLS**：不要使用 TLS 憑證來保護連線。

> 如果您更改了 CA 證書，請立即"在管理節點上重新啟動 mgmt-api 服務"並測試是否成功 SSO 進入網格管理器。

b. 在企業應用程式部分，指定StorageGRID的 企業應用程式名稱。此值控制您在 Azure AD 中為每個企業應用程式使用的名稱。

- 例如，如果您的網格只有一個管理節點，且您不打算在將來新增更多管理節點，請輸入 `SG`或者 `StorageGRID`。
- 如果您的網格包含多個管理節點，請包含字串 `[HOSTNAME]`在標識符中。例如， `SG-[HOSTNAME]` 。這將產生一個表，根據節點的主機名稱顯示系統中每個管理節點的企業應用程式名稱。

> 您必須為StorageGRID系統中的每個管理節點建立一個企業應用程式。每個管理節點都有一個企業應用程序，可確保使用者可以安全地登入和登出任何管理節點。

c. 請依照以下步驟操作"在 Azure AD 中建立企業應用程式"為表中列出的每個管理節點建立一個企業應用程式。

d. 從 Azure AD 複製每個企業應用程式的聯合元資料 URL。然後，將此 URL 貼到StorageGRID中對應的 **Federation metadata URL** 欄位中。

e. 複製並貼上所有管理節點的聯合元資料 URL 後，選擇 儲存。

*儲存*按鈕上會出現綠色複選標記，持續幾秒鐘。

Ping聯邦

a. 指定當身分識別提供者回應StorageGRID請求傳送 SSO 設定資訊時將使用哪個 TLS 憑證來保護連線。

- 使用作業系統 **CA** 憑證：使用作業系統上安裝的預設 CA 憑證來保護連線。
- 使用自訂 **CA** 憑證：使用自訂 CA 憑證來保護連線。

  如果選擇此設置，請複製自訂憑證的文字並將其貼上到 **CA** 憑證 文字方塊中。

- 不要使用 **TLS**：不要使用 TLS 憑證來保護連線。

> 如果您更改了 CA 證書，請立即"在管理節點上重新啟動 mgmt-api 服務"並測試是否成功 SSO 進入網格管理器。

b. 在服務提供者 (SP) 部分中，指定StorageGRID的 * SP連線 ID *。此值控制您在 PingFederate 中為每個SP連線使用的名稱。

- 例如，如果您的網格只有一個管理節點，且您不打算在將來新增更多管理節點，請輸入 `SG`或者 `StorageGRID`。

- 如果您的網格包含多個管理節點，請包含字串 `[HOSTNAME]`在標識符中。例如， `SG-[HOSTNAME]` 。這將產生一個表，根據節點的主機名稱顯示系統中每個管理節點的SP連線ID。

> 您必須為StorageGRID系統中的每個管理節點建立一個SP連線。每個管理節點都有一個SP連接，可確保使用者可以安全地登入和登出任何管理節點。

c. 在 **Federation metadata URL** 欄位中指定每個管理節點的聯合元資料 URL。

使用以下格式：

```
https://<Federation Service
Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP
Connection ID>
```

d. 選擇*儲存*。

*儲存*按鈕上會出現綠色複選標記，持續幾秒鐘。

配置信賴方信任、企業應用程式或**SP**連接

儲存配置後，會出現沙盒模式確認通知。此通知確認沙盒模式現已啟用並提供概述說明。

StorageGRID可依需求維持沙盒模式。但是，當在單一登入頁面上選擇「沙盒模式」時，所有StorageGRID使用者的 SSO 都會被停用。只有本地用戶可以登入。

請依照下列步驟設定信賴方信任（Active Directory）、完成企業應用程式（Azure）或設定SP連線（PingFederate）。

活動目錄

步驟

1. 前往 Active Directory 聯合驗證服務 (AD FS)。
2. 使用StorageGRID單一登入頁面上的表格中顯示的每個依賴方標識符，為StorageGRID建立一個或多個依賴方信任。

   您必須為表中顯示的每個管理節點建立一個信任。

   有關說明，請訪問"在 AD FS 中創造信賴方信任"。

Azure

步驟

1. 從您目前登入的管理節點的單一登入頁面，選擇按鈕下載並儲存 SAML 元資料。
2. 然後，對於網格中的任何其他管理節點，重複以下步驟：
   a. Sign in節點。
   b. 選擇*設定* > 存取控制 > 單一登入。
   c. 下載並儲存該節點的 SAML 元資料。
3. 前往 Azure 入口網站。
4. 請依照以下步驟操作"在 Azure AD 中建立企業應用程式"將每個管理節點的 SAML 元資料檔案上傳到其對應的 Azure 企業應用程式中。

Ping聯邦

步驟

1. 從您目前登入的管理節點的單一登入頁面，選擇按鈕下載並儲存 SAML 元資料。
2. 然後，對於網格中的任何其他管理節點，重複以下步驟：
   a. Sign in節點。
   b. 選擇*設定* > 存取控制 > 單一登入。
   c. 下載並儲存該節點的 SAML 元資料。
3. 前往 PingFederate。
4. "為StorageGRID建立一個或多個服務提供者（SP）連接" 。使用每個管理節點的SP連線 ID（顯示在StorageGRID單一登入頁面上的表格中）以及為該管理節點下載的 SAML 元資料。

   您必須為表格中顯示的每個管理節點建立一個SP連線。

測試 **SSO** 連接

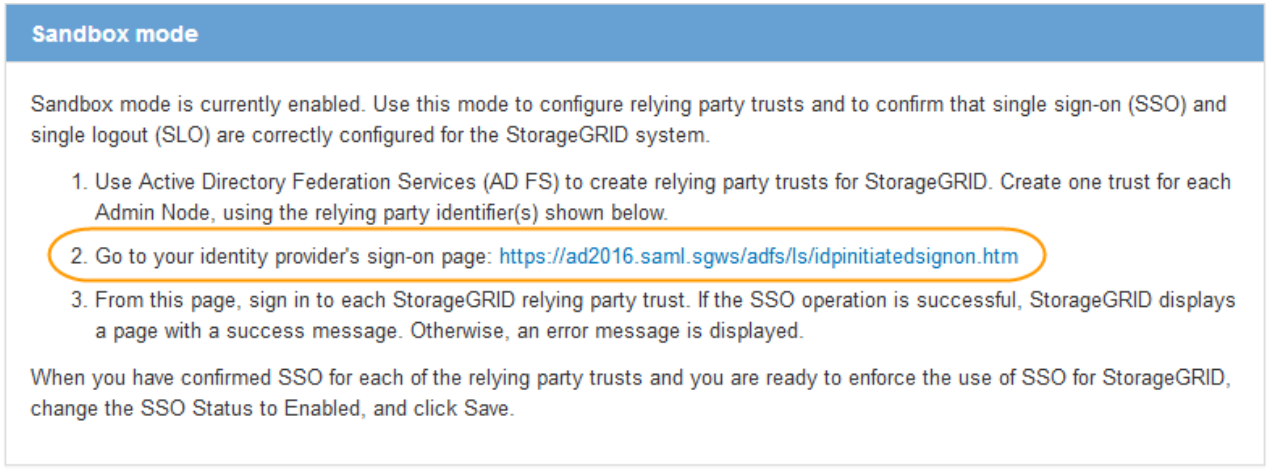
在強制整個StorageGRID系統使用單一登入之前，您應該確認每個管理節點的單一登入和單一登出都已正確配置。

活動目錄

步驟

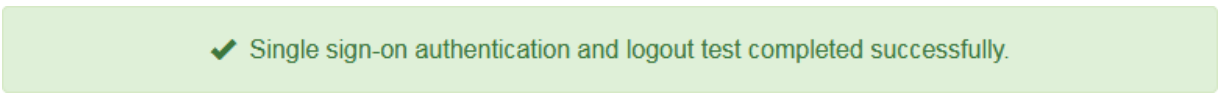
1. 在StorageGRID單一登入頁面中，找到沙盒模式訊息中的連結。

   該 URL 源自於您在 聯合服務名稱 欄位中輸入的值。



2. 選擇連結或將 URL 複製並貼上到瀏覽器中，以存取您的身分提供者的登入頁面。
3. 若要確認您可以使用 SSO 登入StorageGRID，請選擇 **Sign in**下列網站之一，選擇主管理節點的信賴方標識符，然後選擇 **Sign in**。

4. 輸入您的聯合用戶名和密碼。
   - 如果 SSO 登入和登出操作成功，則會顯示成功訊息。



   - 如果 SSO 操作不成功，則會顯示錯誤訊息。解決問題，清除瀏覽器的 cookie，然後重試。
5. 重複這些步驟來驗證網格中每個管理節點的 SSO 連線。

Azure

步驟

1. 前往 Azure 入口網站中的單一登入頁面。
2. 選擇*測試此應用程式*。
3. 輸入聯合用戶的憑證。
   - 如果 SSO 登入和登出操作成功，則會顯示成功訊息。

     ✔ Single sign-on authentication and logout test completed successfully.

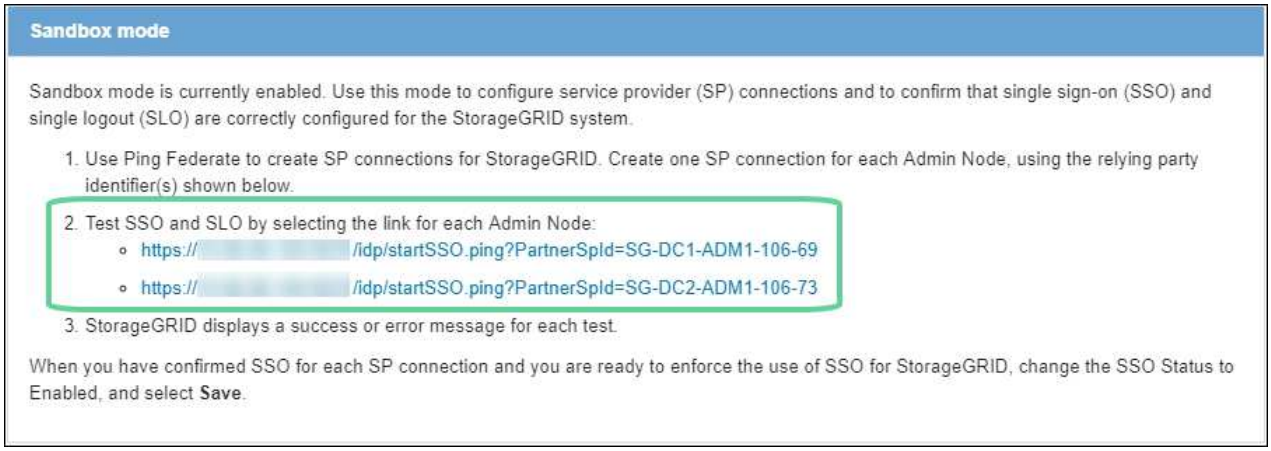
   - 如果 SSO 操作不成功，則會顯示錯誤訊息。解決問題，清除瀏覽器的 cookie，然後重試。
4. 重複這些步驟來驗證網格中每個管理節點的 SSO 連線。

Ping聯邦

步驟

1. 從StorageGRID單一登入頁面，選擇沙盒模式訊息中的第一個連結。

   一次選擇並測試一個連結。



2. 輸入聯合用戶的憑證。
   - 如果 SSO 登入和登出操作成功，則會顯示成功訊息。

     ✔ Single sign-on authentication and logout test completed successfully.

   - 如果 SSO 操作不成功，則會顯示錯誤訊息。解決問題，清除瀏覽器的 cookie，然後重試。
3. 選擇下一個連結來驗證網格中每個管理節點的 SSO 連線。

   如果您看到「頁面已過期」訊息，請選擇瀏覽器中的「返回」按鈕並重新提交您的憑證。

啟用單一登入

當您確認可以使用 SSO 登入每個管理節點後，您可以為整個StorageGRID系統啟用 SSO。

啟用 SSO 後，所有使用者都必須使用 SSO 來存取網格管理器、租用戶管理器、網格管理 API 和租用戶管理 API。本機用戶無法再存取StorageGRID。

步驟

1. 選擇*設定* > 存取控制 > 單一登入。
2. 將 SSO 狀態變更為 已啟用。
3. 選擇*儲存*。
4. 查看警告訊息，然後選擇“確定”。

   單一登入現已啟用。

如果您使用 Azure 入口網站並從用於存取 Azure 的相同電腦存取StorageGRID ，請確保 Azure 入口網站使用者也是授權的StorageGRID使用者（已匯入StorageGRID 的聯合群組中的使用者）或在嘗試登入StorageGRID之前登出 Azure 入口網站。

在 **AD FS** 中創造信賴方信任

您必須使用 Active Directory 聯合驗證服務 (AD FS) 為系統中的每個管理節點建立信賴方信任。您可以使用 PowerShell 指令、透過從StorageGRID匯入 SAML 元資料或手動輸入資料來建立信賴方信任。

開始之前

- 您已為StorageGRID設定單一登入，並選擇 **AD FS** 作為 SSO 類型。
- 在網格管理員的單一登入頁面上選擇了*沙盒模式*。看"使用沙盒模式" 。
- 您知道系統中每個管理節點的完全限定網域名稱（或 IP 位址）和信賴方識別碼。您可以在StorageGRID單一登入頁面上的管理節點詳細資料表中找到這些值。

  您必須為StorageGRID系統中的每個管理節點建立一個依賴方信任。每個管理節點都擁有依賴方信任，確保使用者可以安全地登入和登出任何管理節點。

- 您具有在 AD FS 中建立信任方信任的經驗，或者您可以存取 Microsoft AD FS 文件。
- 您正在使用 AD FS 管理管理單元，並且您屬於管理員群組。
- 如果您手動建立依賴方信任，則您擁有為StorageGRID管理介面上傳的自訂證書，或者您知道如何從命令 shell 登入管理節點。

關於此任務

這些說明適用於 Windows Server 2016 AD FS。如果您使用的是不同版本的 AD FS，您會注意到過程中略有不同。如果您有任何疑問，請參閱 Microsoft AD FS 文件。

使用 **Windows PowerShell** 建立信賴方信任

您可以使用 Windows PowerShell 快速建立一個或多個信賴方信任。

步驟

1. 從 Windows 開始功能表中，右鍵單擊選擇 PowerShell 圖標，然後選擇*以管理員身份執行*。

2. 在 PowerShell 命令提示字元下，輸入以下命令：

   ```
   Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL
   "https://Admin_Node_FQDN/api/saml-metadata"
   ```

   - 為了 *Admin_Node_Identifier*，輸入管理節點的依賴方標識符，與單一登入頁面上顯示的完全一致。例如， `SG-DC1-ADM1` 。
   - 為了 *Admin_Node_FQDN*，輸入同一管理節點的完全限定網域名稱。 （如有必要，您可以使用節點的 IP 位址。但是，如果您在此處輸入 IP 位址，請注意，如果該 IP 位址發生變化，則必須更新或重新建立此信賴方信任。）

3. 從 Windows 伺服器管理員中，選擇「工具」>「AD FS 管理」。

   出現 AD FS 管理工具。

4. 選擇 **AD FS** > 依賴方信任。

   出現依賴方信任的清單。

5. 在新建立的依賴方信任中新增存取控制策略：
   a. 找到您剛剛創建的信任方信任。
   b. 右鍵單擊信任，然後選擇“編輯存取控制策略”。
   c. 選擇存取控制策略。
   d. 選擇“應用”，然後選擇“確定”
6. 在新建立的依賴方信任中新增聲明發布策略：
   a. 找到您剛剛創建的信任方信任。
   b. 右鍵點選信託，然後選擇「編輯索賠頒發政策」。
   c. 選擇*新增規則*。
   d. 在選擇規則範本頁面上，從清單中選擇*將 LDAP 屬性傳送為聲明*，然後選擇*下一步*。
   e. 在設定規則頁面上，輸入此規則的顯示名稱。

      例如，**ObjectGUID** 到名稱 **ID** 或 **UPN** 到名稱 **ID**。

   f. 對於屬性存儲，選擇*Active Directory*。
   g. 在映射表的 LDAP 屬性列中，鍵入 **objectGUID** 或選擇 **User-Principal-Name**。
   h. 在映射表的傳出聲明類型列中，從下拉清單中選擇*名稱 ID*。
   i. 選擇“完成”，然後選擇“確定”。
7. 確認元資料已成功導入。
   a. 右鍵單擊信賴方信任以開啟其屬性。
   b. 確認「**Endpoints**」、「**Identifiers**」和「**Signature**」標籤上的欄位已填入。

      如果缺少元數據，請確認聯邦元數據地址是否正確，或手動輸入值。

8. 重複這些步驟，為StorageGRID系統中的所有管理節點配置依賴方信任。

9. 完成後，返回StorageGRID並測試所有依賴方信任以確認它們配置正確。看"使用沙盒模式"以取得說明。

透過匯入聯合元資料創建信賴方信任

您可以透過存取每個管理節點的 SAML 元資料來匯入每個依賴方信任的值。

步驟

1. 在 Windows 伺服器管理員中，選擇“工具”，然後選擇“AD FS 管理”。
2. 在操作下，選擇*新增依賴方信任*。
3. 在歡迎頁面上，選擇*索賠意識*，然後選擇*開始*。
4. 選擇*匯入線上或本機網路上發佈的有關依賴方的資料*。
5. 在 聯合元資料位址（主機名稱或 **URL**） 中，鍵入此管理節點的 SAML 元資料的位置：

   `https://Admin_Node_FQDN/api/saml-metadata`

   為了 *Admin_Node_FQDN*，輸入同一管理節點的完全限定網域名稱。 （如有必要，您可以使用節點的 IP 位址。但是，如果您在此處輸入 IP 位址，請注意，如果該 IP 位址發生變化，則必須更新或重新建立此信賴方信任。）

6. 完成依賴方信任嚮導，儲存依賴方信任，然後關閉嚮導。

   輸入顯示名稱時，請使用管理節點的依賴方標識符，與網格管理器中的單點登入頁面上顯示的完全一樣。例如， `SG-DC1-ADM1` 。

7. 新增聲明規則：
   a. 右鍵點選信託，然後選擇「編輯索賠頒發政策」。
   b. 選擇*新增規則*：
   c. 在選擇規則範本頁面上，從清單中選擇*將 LDAP 屬性傳送為聲明*，然後選擇*下一步*。
   d. 在設定規則頁面上，輸入此規則的顯示名稱。

      例如，**ObjectGUID** 到名稱 **ID** 或 **UPN** 到名稱 **ID**。

   e. 對於屬性存儲，選擇*Active Directory*。
   f. 在映射表的 LDAP 屬性列中，鍵入 **objectGUID** 或選擇 **User-Principal-Name**。
   g. 在映射表的傳出聲明類型列中，從下拉清單中選擇*名稱 ID*。
   h. 選擇“完成”，然後選擇“確定”。
8. 確認元資料已成功導入。
   a. 右鍵單擊信賴方信任以開啟其屬性。
   b. 確認「**Endpoints**」、「**Identifiers**」和「**Signature**」標籤上的欄位已填入。

      如果缺少元數據，請確認聯邦元數據地址是否正確，或手動輸入值。

9. 重複這些步驟，為StorageGRID系統中的所有管理節點配置依賴方信任。

10. 完成後，返回StorageGRID並測試所有依賴方信任以確認它們配置正確。看"使用沙盒模式"以取得說明。

手動創建信賴方信任

如果您選擇不匯入依賴部分信託的數據，您可以手動輸入值。

步驟

1. 在 Windows 伺服器管理員中，選擇“工具”，然後選擇“AD FS 管理”。
2. 在操作下，選擇*新增依賴方信任*。
3. 在歡迎頁面上，選擇*索賠意識*，然後選擇*開始*。
4. 選擇*手動輸入依賴方的資料*，然後選擇*下一步*。
5. 完成依賴方信任嚮導：

   a. 輸入此管理節點的顯示名稱。

      為了保持一致性，請使用管理節點的依賴方標識符，與網格管理器中的單點登入頁面上顯示的完全一樣。例如， `SG-DC1-ADM1` 。

   b. 跳過配置可選令牌加密憑證的步驟。

   c. 在設定 URL 頁面上，選取 啟用對 **SAML 2.0 WebSSO** 協定的支援 複選框。

   d. 輸入管理節點的 SAML 服務端點 URL：

      `https://Admin_Node_FQDN/api/saml-response`

      為了 `*Admin_Node_FQDN*`中，輸入管理節點的完全限定網域名稱。 （如有必要，您可以使用節點的 IP 位址。但是，如果您在此處輸入 IP 位址，請注意，如果該 IP 位址發生變化，則必須更新或重新建立此信賴方信任。 ）

   e. 在設定標識符頁面上，為同一個管理節點指定依賴方識別碼：

      `*Admin_Node_Identifier*`

      為了 `*Admin_Node_Identifier*`，輸入管理節點的依賴方標識符，與單一登入頁面上顯示的完全一致。例如， `SG-DC1-ADM1` 。

   f. 檢查設置，儲存信賴方信任，然後關閉精靈。

      出現「編輯索賠簽發政策」對話框。

      如果未出現對話框，請右鍵點選信任，然後選擇「編輯聲明頒發政策」。

6. 若要啟動聲明規則精靈，請選擇*新增規則*：

   a. 在選擇規則範本頁面上，從清單中選擇*將 LDAP 屬性傳送為聲明*，然後選擇*下一步*。

   b. 在設定規則頁面上，輸入此規則的顯示名稱。

      例如，**ObjectGUID** 到名稱 **ID** 或 **UPN** 到名稱 **ID**。

c. 對於屬性存儲，選擇*Active Directory*。

d. 在映射表的 LDAP 屬性列中，鍵入 **objectGUID** 或選擇 **User-Principal-Name**。

e. 在映射表的傳出聲明類型列中，從下拉清單中選擇*名稱 ID*。

f. 選擇“完成”，然後選擇“確定”。

7. 右鍵單擊信賴方信任以開啟其屬性。

8. 在「端點」標籤上，設定單點登出 (SLO) 的端點：

a. 選擇“新增 SAML”。

b. 選擇*端點類型* > **SAML** 登出。

c. 選擇*綁定* > 重定向。

d. 在「可信任 **URL**」欄位中，輸入用於從此管理節點單點登出 (SLO) 的 URL：

```
https://Admin_Node_FQDN/api/saml-logout
```

為了 `*Admin_Node_FQDN*`中，輸入管理節點的完全限定網域名稱。 （如有必要，您可以使用節點的 IP 位址。但是，如果您在此處輸入 IP 位址，請注意，如果該 IP 位址發生變化，則必須更新或重新建立此信賴方信任。）

a. 選擇“確定”。

9. 在「簽署」標籤上，指定此信賴方信任的簽章憑證：

a. 新增自訂憑證：

- 如果您有上傳到StorageGRID 的自訂管理證書，請選擇該證書。
- 如果您沒有自訂證書，請登入管理節點，前往 `/var/local/mgmt-api`管理節點的目錄，並且加入 `custom-server.crt`證書文件。

> 使用管理節點的預設證書(`server.crt`) 是不推薦的。如果管理節點發生故障，則恢復節點時將重新產生預設證書，並且您需要更新信賴方信任。

b. 選擇“應用”，然後選擇“確定”。

依賴方屬性已儲存並關閉。

10. 重複這些步驟，為StorageGRID系統中的所有管理節點配置依賴方信任。

11. 完成後，返回StorageGRID並測試所有依賴方信任以確認它們配置正確。看"使用沙盒模式"以取得說明。

在 **Azure AD** 中建立企業應用程式

您使用 Azure AD 為系統中的每個管理節點建立一個企業應用程式。

開始之前

- 您已開始為StorageGRID設定單一登錄，並選擇 **Azure** 作為 SSO 類型。
- 在網格管理員的單一登入頁面上選擇了*沙盒模式*。看"使用沙盒模式" 。
- 您的系統中的每個管理節點都有*企業應用程式名稱*。您可以從StorageGRID單一登入頁面上的管理節點詳

細資料表中複製這些值。

> 您必須為StorageGRID系統中的每個管理節點建立一個企業應用程式。每個管理節點都有一個企業應用程序，可確保使用者可以安全地登入和登出任何管理節點。

- 您有在 Azure Active Directory 中建立企業應用程式的經驗。
- 您有一個具有有效訂閱的 Azure 帳戶。
- 您在 Azure 帳戶中擁有下列角色之一：全域管理員、雲端應用程式管理員、應用程式管理員或服務主體的擁有者。

存取 **Azure AD**

步驟

1. 登入 "Azure 入口網站"。
2. 導航至 "Azure Active Directory"。
3. 選擇 "企業應用程式"。

建立企業應用程式並儲存**StorageGRID SSO** 配置

若要在StorageGRID中儲存 Azure 的 SSO 配置，您必須使用 Azure 為每個管理節點建立一個企業應用程式。您將從 Azure 複製聯合元資料 URL，並將其貼上到StorageGRID單一登入頁面上對應的 聯合元資料 **URL** 欄位中。

步驟

1. 對每個管理節點重複以下步驟。
   a. 在 Azure Enterprise 應用程式窗格中，選擇「新應用程式」。
   b. 選擇*創建您自己的應用程式*。
   c. 對於名稱，請輸入從StorageGRID單一登入頁面上的管理節點詳細資料表複製的 企業應用程式名稱。
   d. 保持選取*整合您在圖庫中找不到的任何其他應用程式（非圖庫）*單選按鈕。
   e. 選擇“創建”。
   f. 選擇*2 中的*開始*連結。設定單一登入*框，或選擇左邊距中的*單一登入*連結。
   g. 選擇 **SAML** 框。
   h. 複製 **App Federation Metadata Url**，您可以在 **Step 3 SAML Signing Certificate** 下找到它。
   i. 前往StorageGRID單一登入頁面，並將 URL 貼到與您使用的 企業應用程式名稱 相對應的 聯合元資料 **URL** 欄位中。
2. 為每個管理節點貼上聯合元資料 URL 並對 SSO 配置進行所有其他必要的變更後，在StorageGRID單一登入頁面上選擇 儲存。

下載每個管理節點的 **SAML** 元數據

儲存 SSO 設定後，您可以為StorageGRID系統中的每個管理節點下載一個 SAML 元資料檔。

步驟

1. 對每個管理節點重複這些步驟。

a. 從管理節點Sign inStorageGRID 。
b. 選擇*設定* > 存取控制 > 單一登入。
c. 選擇按鈕下載該管理節點的 SAML 元資料。
d. 儲存文件，然後將其上傳到 Azure AD。

將 **SAML** 元資料上傳到每個企業應用程式

為每個StorageGRID管理節點下載 SAML 元資料檔案後，在 Azure AD 中執行下列步驟：

步驟

1. 返回 Azure 入口網站。
2. 對每個企業應用程式重複以下步驟：

> 您可能需要刷新企業應用程式頁面才能看到先前在清單中新增的應用程式。

a. 轉到企業應用程式的屬性頁面。
b. 將 需要分配 設定為 否（除非您想單獨配置分配）。
c. 前往單一登入頁面。
d. 完成 SAML 設定。
e. 選擇*上傳元資料檔案*按鈕，然後選擇您為對應管理節點下載的 SAML 元資料檔案。
f. 檔案載入後，選擇*儲存*，然後選擇*X*關閉窗格。您將返回使用 SAML 設定單一登入頁面。

3. 請依照以下步驟操作"使用沙盒模式"測試每個應用程式。

在 **PingFederate** 中建立服務提供者 **(SP)** 連接

您使用 PingFederate 為系統中的每個管理節點建立服務提供者 (SP) 連線。為了加快這個過程，您將從StorageGRID匯入 SAML 元資料。

開始之前

- 您已為StorageGRID設定單一登錄，並選擇 **Ping Federate** 作為 SSO 類型。
- 在網格管理員的單一登入頁面上選擇了*沙盒模式*。看"使用沙盒模式" 。
- 您系統中每個管理節點都有* SP連線 ID *。您可以在StorageGRID單一登入頁面上的管理節點詳細資料表中找到這些值。
- 您已下載系統中每個管理節點的 **SAML** 元資料。
- 您有在 PingFederate 伺服器中建立SP連線的經驗。
- 你有https://docs.pingidentity.com/pingfederate/latest/administrators_reference_guide/pf_administrators_reference_guide.html["管理員參考指南"^]用於 PingFederate 伺服器。PingFederate 文件提供了詳細的逐步說明和解釋。
- 你有"管理員權限"用於 PingFederate 伺服器。

關於此任務

這些說明總結如何將 PingFederate Server 版本 10.3 設定為StorageGRID的 SSO 提供者。如果您使用的是其他版本的 PingFederate，則可能需要調整這些說明。有關您的版本的詳細說明，請參閱 PingFederate 伺服器文件。

完成 **PingFederate** 中的先決條件

在建立將用於StorageGRID 的SP連線之前，您必須完成 PingFederate 中的先決條件任務。配置SP連線時，您將使用這些先決條件中的資訊。

建立資料儲存

如果您還沒有，請建立資料儲存以將 PingFederate 連接到 AD FS LDAP 伺服器。使用您使用過的值"配置身份聯合"在StorageGRID中。

- 類型：目錄（LDAP）
- **LDAP** 類型：Active Directory
- 二進位屬性名稱：在 LDAP 二進位屬性標籤上輸入 **objectGUID**，與所示完全一致。

建立密碼憑證驗證器

如果您還沒有，請建立密碼憑證驗證器。

- 類型：LDAP 使用者名稱密碼憑證驗證器
- 資料儲存：選擇您建立的資料儲存。
- 搜尋基礎：輸入來自 LDAP 的資訊（例如，DC=saml,DC=sgws）。
- 搜尋篩選器：sAMAccountName=${username}
- 範圍：子樹

建立 **IdP** 適配器實例

如果您還沒有，請建立 IdP 適配器實例。

步驟

1. 前往*身份驗證* > 整合 > **IdP** 適配器。
2. 選擇“建立新實例”。
3. 在類型標籤上，選擇*HTML 表單 IdP 適配器*。
4. 在 IdP 適配器標籤上，選擇*為「憑證驗證器」新增一行*。
5. 選擇密碼憑證驗證器你創造的。
6. 在適配器屬性標籤上，選擇 **Pseudonym** 的 **username** 屬性。
7. 選擇*儲存*。

建立或匯入簽章憑證

如果您還沒有，請建立或匯入簽名證書。

步驟

1. 前往*安全* > 簽署和解密金鑰和憑證。
2. 建立或匯入簽名證書。

在 **PingFederate** 中建立**SP**連接

在 PingFederate 中建立SP連線時，您會匯入從StorageGRID為管理節點下載的 SAML 元資料。元資料檔案包含您需要的許多特定值。

> 您必須為StorageGRID系統中的每個管理節點建立一個SP連接，以便使用者可以安全地登入和登出任何節點。使用這些說明來建立第一個SP連線。然後，轉到建立其他SP連接建立您需要的任何其他連線。

選擇**SP**連線類型

步驟

1. 前往*應用程式* > 整合 > * SP連接*。
2. 選擇*建立連線*。
3. 選擇*不要對此連線使用範本*。
4. 選擇 瀏覽器 **SSO** 設定檔 和 **SAML 2.0** 作為協定。

導入**SP**元數據

步驟

1. 在導入元資料標籤上，選擇*檔案*。
2. 選擇從管理節點的StorageGRID單一登入頁面下載的 SAML 元資料檔。
3. 查看元資料摘要和常規資訊標籤上提供的資訊。

   合作夥伴的實體 ID 和連線名稱設定為StorageGRID SP連線 ID。 （例如，10.96.105.200-DC1-ADM1-105-200）。基本 URL 是StorageGRID管理節點的 IP。

4. 選擇“下一步”。

設定 **IdP** 瀏覽器 **SSO**

步驟

1. 從瀏覽器 SSO 標籤中，選擇 設定瀏覽器 **SSO**。
2. 在 SAML 設定檔標籤上，選擇 * SP-initiated SSO*、* SP-initial SLO*、* IdP-initiated SSO* 和 * IdP-initiated SLO* 選項。
3. 選擇“下一步”。
4. 在「斷言生命週期」標籤上，不做任何更改。
5. 在「斷言建立」標籤上，選擇「配置斷言建立」。
   a. 在「身分映射」標籤上，選擇「標準」。
   b. 在屬性合約標籤上，使用 **SAML_SUBJECT** 作為屬性合約和匯入的未指定的名稱格式。
6. 對於延長合同，選擇“刪除”以刪除 `urn:oid`，未使用。

地圖適配器實例

步驟

1. 在驗證來源對應標籤上，選擇*對應新適配器實例*。
2. 在適配器實例標籤上，選擇適配器實例你創造的。
3. 在「映射方法」標籤上，選擇「從資料儲存體中檢索附加屬性」。
4. 在「屬性來源和使用者尋找」標籤上，選擇「新增屬性來源」。
5. 在資料儲存標籤上，提供描述並選擇資料儲存你補充道。
6. 在 LDAP 目錄搜尋標籤上：
   - 輸入*Base DN*，它應該與您在StorageGRID中為 LDAP 伺服器輸入的值完全相符。
   - 對於搜尋範圍，選擇*子樹*。
   - 對於根物件類，搜尋並新增以下任一屬性：**objectGUID** 或 **userPrincipalName**。
7. 在 LDAP 二進位屬性編碼類型標籤上，為 **objectGUID** 屬性選擇 **Base64**。
8. 在 LDAP 過濾器標籤上，輸入 **sAMAccountName=${username}**。
9. 在“屬性合約履行”標籤上，從“來源”下拉選單中選擇“**LDAP**（屬性）”，然後從“值”下拉選單中選擇“**objectGUID**”或“**userPrincipalName**”。
10. 審查並保存屬性來源。
11. 在「Failsave Attribute Source」標籤上，選擇「**Abort the SSO Transaction**」。
12. 查看摘要並選擇*完成*。
13. 選擇*完成*。

配置協議設定

步驟

1. 在 * SP連線 * > * 瀏覽器 SSO * > * 協定設定 * 標籤上，選擇 * 設定協定設定 *。
2. 在斷言消費者服務 URL 標籤上，接受從StorageGRID SAML 元資料匯入的預設值（用於綁定和 `/api/saml-response`（用於端點 URL）。
3. 在 SLO 服務 URL 標籤上，接受從StorageGRID SAML 元資料匯入的預設值（用於綁定和 `/api/saml-logout` 用於端點 URL。
4. 在允許的 SAML 綁定標籤上，清除 **ARTIFACT** 和 **SOAP**。只需要 **POST** 和 **REDIRECT**。
5. 在「簽章原則」標籤上，勾選「要求對身分驗證要求進行簽署」和「始終簽署斷言」複選框。
6. 在加密策略標籤上，選擇*無*。
7. 查看摘要並選擇*完成*以儲存協定設定。
8. 查看摘要並選擇*完成*以儲存瀏覽器 SSO 設定。

配置憑證

步驟

1. 從SP連線標籤中，選擇 憑證。

2. 從「憑證」標籤中，選擇「配置憑證」。
3. 選擇簽署證書您建立或匯入的。
4. 選擇*下一步*進入*管理簽名驗證設定*。
   a. 在「信任模型」標籤上，選擇「**Unanchored**」。
   b. 在「簽署驗證憑證」標籤上，檢視從StorageGRID SAML 元資料匯入的簽名憑證資訊。
5. 查看摘要畫面並選擇*儲存*以儲存SP連線。

建立其他**SP**連接

您可以複製第一個SP連線來為網格中的每個管理節點建立所需的SP連線。您為每個副本上傳新的元資料。

> 不同管理節點的SP連線使用相同的設置，但合作夥伴的實體 ID、基本 URL、連線 ID、連線名稱、簽章驗證和 SLO 回應 URL 除外。

步驟

1. 選擇「操作」>「複製」為每個附加管理節點建立初始SP連線的副本。
2. 輸入副本的連線 ID 和連線名稱，然後選擇*儲存*。
3. 選擇與管理節點對應的元資料檔：
   a. 選擇*操作* > 使用元資料更新。
   b. 選擇*選擇檔案*並上傳元資料。
   c. 選擇“下一步”。
   d. 選擇*儲存*。
4. 解決由於未使用屬性而導致的錯誤：
   a. 選擇新的連接。
   b. 選擇*設定瀏覽器 SSO > 設定斷言建立 > 屬性契約*。
   c. 刪除 **urn:oid** 的條目。
   d. 選擇*儲存*。

停用單一登入

如果您不再想使用此功能，可以停用單一登入 (SSO)。您必須先停用單一登錄，然後才能停用身份聯合。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"特定存取權限"。

步驟

1. 選擇*設定* > 存取控制 > 單一登入。

   出現「單一登入」頁面。

2. 選擇“已停用”選項。
3. 選擇*儲存*。

   出現警告訊息，表示本地用戶現在可以登入。

4. 選擇“確定”。

   下次登入StorageGRID時，將出現StorageGRIDSign in頁面，您必須輸入本機或聯合StorageGRID使用者的使用者名稱和密碼。

暫時停用並重新啟用一個管理節點的單一登入

如果單一登入 (SSO) 系統發生故障，您可能無法登入網格管理員。在這種情況下，您可以暫時停用並重新啟用一個管理節點的 SSO。若要停用然後重新啟用 SSO，您必須存取節點的命令 shell。

開始之前

- 你有"特定存取權限"。
- 你有 `Passwords.txt`文件。
- 您知道本機 root 使用者的密碼。

關於此任務

停用一個管理節點的 SSO 後，您可以以本機 root 使用者身分登入網格管理員。為了保護您的StorageGRID系統，您必須在登出後立即使用節點的命令 shell 在管理節點上重新啟用 SSO。

> 停用一個管理節點的 SSO 不會影響網格中任何其他管理節點的 SSO 設定。網格管理器中單一登入頁面上的「啟用 SSO」複選框保持選取狀態，並且所有現有的 SSO 設定都將保留，除非您更新它們。

步驟

1. 登入管理節點：
   a. 輸入以下命令： `ssh admin@Admin_Node_IP`
   b. 輸入 `Passwords.txt`文件。
   c. 輸入以下命令切換到root： `su -`
   d. 輸入 `Passwords.txt`文件。

      當您以 root 身分登入時，提示字元將從 `$`到 `#`。

2. 運行以下命令：`disable-saml`

   一條訊息表明該命令僅適用於此管理節點。

3. 確認您要停用 SSO。

   一則訊息表示該節點上的單一登入已停用。

4. 從 Web 瀏覽器存取相同管理節點上的網格管理器。

   由於 SSO 已停用，因此現在顯示 Grid Manager 登入頁面。

5. 使用使用者名稱 root 和本機 root 使用者的密碼Sign in。
6. 如果您因為需要更正 SSO 設定而暫時停用了 SSO：
   a. 選擇*設定* > 存取控制 > 單一登入。
   b. 更改不正確或過時的 SSO 設定。
   c. 選擇*儲存*。

      從單一登入頁面選擇「儲存」會自動為整個網格重新啟用 SSO。

7. 如果您因其他原因需要存取網格管理員而暫時停用了 SSO：
   a. 執行您需要執行的任何任務。
   b. 選擇*退出*，然後關閉網格管理員。
   c. 在管理節點上重新啟用 SSO。您可以執行下列任何步驟：

      - 運行以下命令： `enable-saml`

        一條訊息表明該命令僅適用於此管理節點。

      確認您要啟用 SSO。

   一則訊息表示該節點上已啟用單一登入。

   - 重新啟動網格節點： `reboot`
8. 透過 Web 瀏覽器，從同一個管理節點存取網格管理器。
9. 確認出現StorageGRIDSign in頁面，並且您必須輸入 SSO 憑證才能存取網格管理員。

使用網格聯合

什麼是電網聯合？

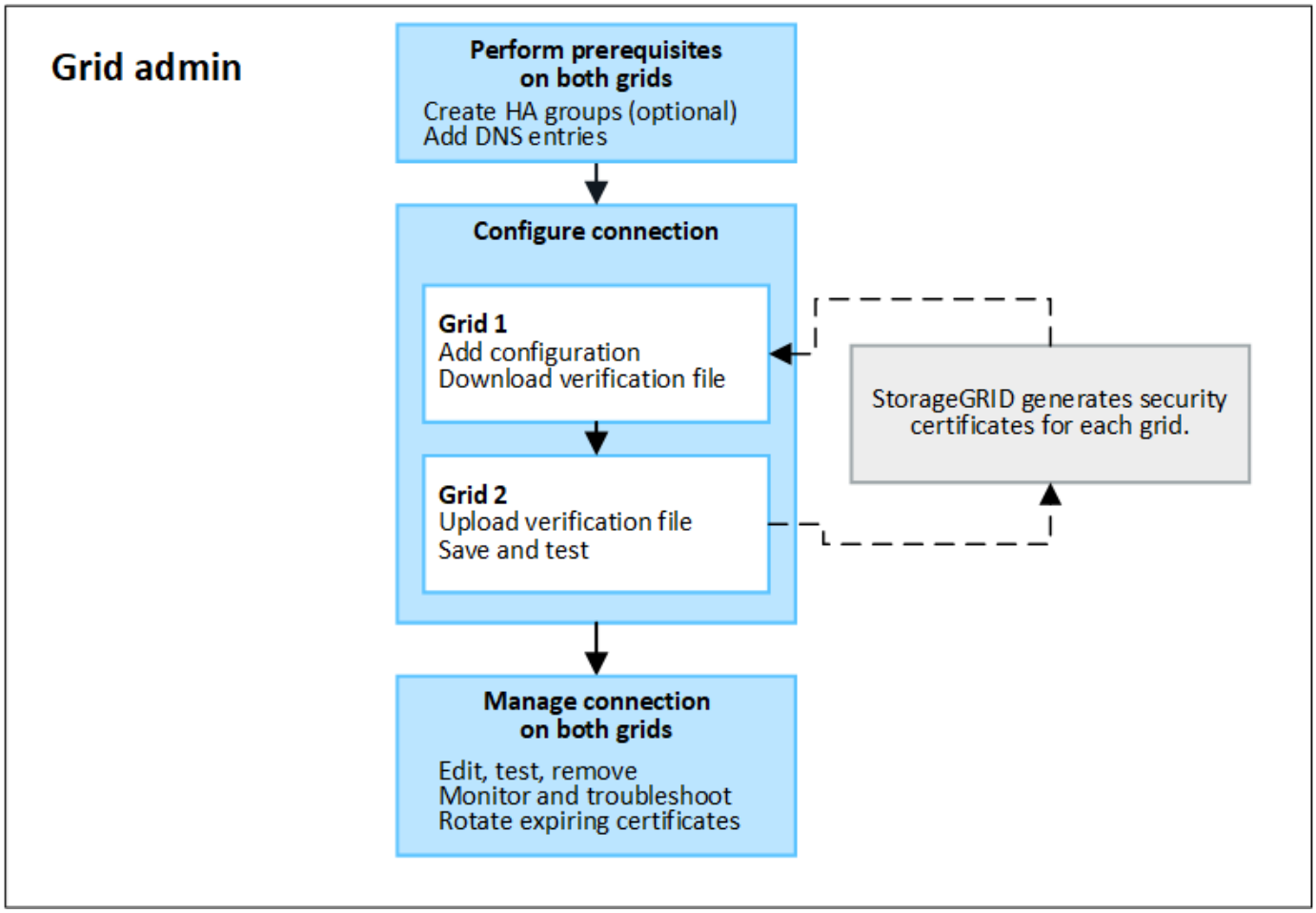
您可以使用網格聯合來複製租用戶並在兩個StorageGRID系統之間複製其物件以實現災難復原。

什麼是電網聯合連接？

網格聯合連接是兩個StorageGRID系統中的管理節點和網關節點之間的雙向、可信任和安全的連接。

網格聯合的工作流程

工作流程圖總結了在兩個網格之間配置網格聯合連接的步驟。



電網聯合連接的注意事項與要求

- 用於網格聯合的網格必須運行相同的StorageGRID版本，或者它們之間主要版本差異不超過一個。

  有關版本要求的詳細信息，請參閱"發行說明"。

- 一個網格可以與其他網格有一個或多個網格聯合連接。每個電網聯合連接都獨立於任何其他連接。例如，如果網格 1 與網格 2 有一個連接，與網格 3 有第二個連接，則網格 2 和網格 3 之間沒有隱含的連接。
- 電網聯合連接是雙向的。建立連線後，您可以從任一網格監控和管理連線。
- 必須至少存在一個網格聯合連接才能使用"帳戶克隆"或者"跨網格複製"。

網路和 **IP** 位址要求

- 網格聯合連接可以發生在網格網路、管理網路或客戶端網路上。
- 電網聯合連接將一個電網連接到另一個電網。每個網格的配置指定另一個網格上的網格聯合端點，該端點由管理節點、網關節點或兩者組成。
- 最佳做法是連接"高可用性 (HA) 組"每個網格上的網關和管理節點。使用 HA 群組有助於確保節點不可用時網格聯合連接仍保持在線。如果任一 HA 組中的活動介面發生故障，則連接可以使用備用介面。
- 不建議建立使用單一管理節點或網關節點的 IP 位址的網格聯合連接。如果節點不可用，則電網聯合連接也將不可用。
- "跨網格複製"物件要求每個網格上的儲存節點能夠存取另一個網格上配置的管理節點和網關節點。對於每個網格，確認所有儲存節點都具有高頻寬路由作為用於連接的管理節點或網關節點。

使用 FQDN 對連線進行負載平衡

對於生產環境，使用完全限定網域名稱 (FQDN) 來標識連線中的每個網格。然後，建立適當的 DNS 項目，如下所示：

- 網格 1 的 FQDN 會對應到網格 1 中 HA 群組的一個或多個虛擬 IP (VIP) 位址，或對應到網格 1 中一個或多個管理節點或網關節點的 IP 位址。
- 網格 2 的 FQDN 會對應到網格 2 的一個或多個 VIP 位址，或對應到網格 2 中一個或多個管理節點或網關節點的 IP 位址。

當您使用多個 DNS 項目時，使用連線的請求將進行負載平衡，如下所示：

- 對應到多個 HA 群組的 VIP 位址的 DNS 條目在 HA 群組中的活動節點之間進行負載平衡。
- 對應到多個管理節點或網關節點的 IP 位址的 DNS 項目在映射節點之間進行負載平衡。

端口要求

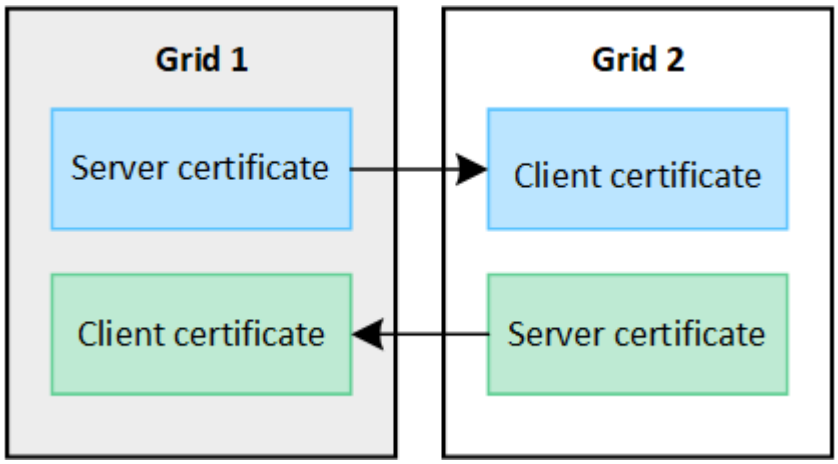
建立電網聯合連接時，您可以指定 23000 到 23999 之間的任何未使用的連接埠號碼。此連接中的兩個電網將使用相同的連接埠。

您必須確保任一網格中均沒有節點使用此連接埠進行其他連接。

證書要求

設定網格聯合連線時， StorageGRID會自動產生四個 SSL 憑證：

- 伺服器和客戶端憑證用於驗證和加密從網格 1 傳送到網格 2 的訊息
- 伺服器和客戶端憑證用於驗證和加密從網格 2 傳送到網格 1 的訊息



預設情況下，證書有效期為 730 天（2 年）。當這些證書接近到期日時，*網格聯合證書到期*警報會提醒您輪換證書，您可以使用網格管理器來執行此操作。

如果連接兩端的憑證過期，連線將停止運作。資料複製將處於待處理狀態，直到憑證更新為止。

了解更多

- "建立電網聯合連接"

- "管理電網聯合連接"
- "解決網格聯合錯誤"

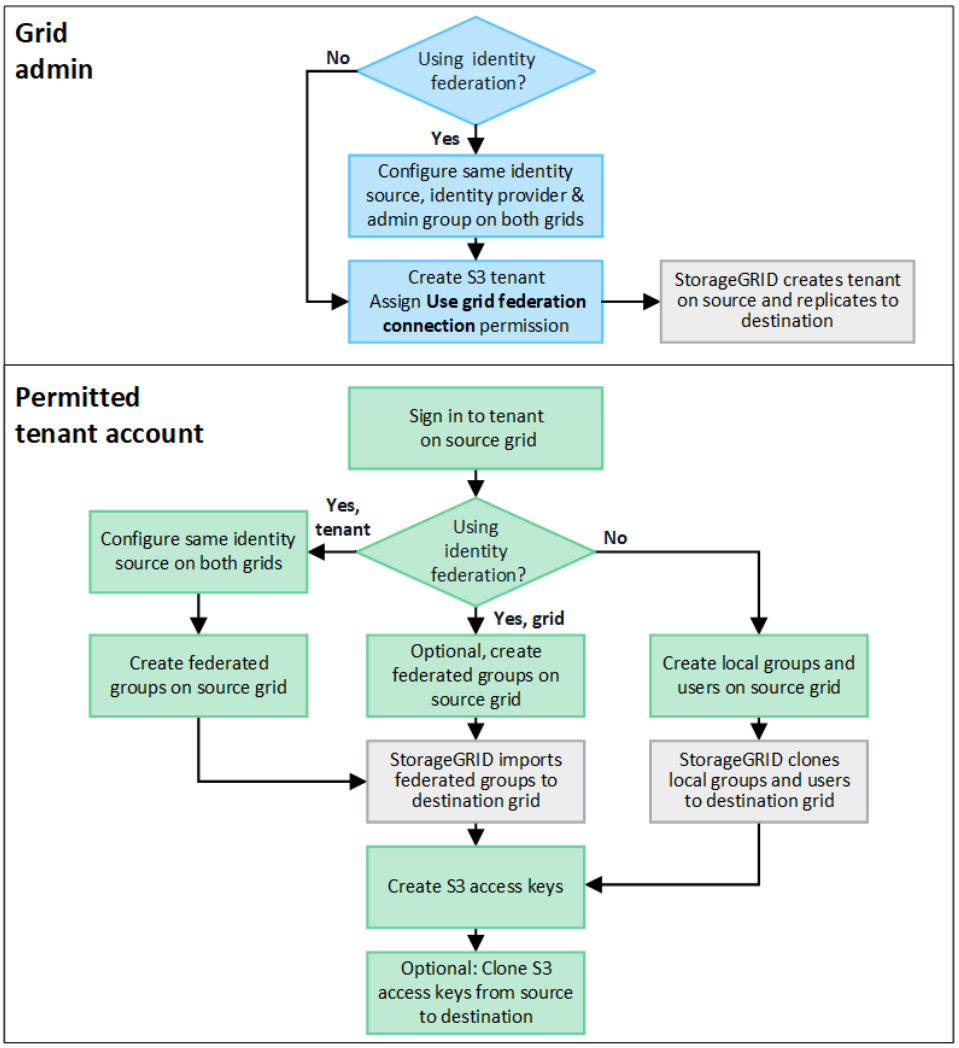
什麼是帳戶克隆？

帳戶複製是租用戶帳戶、租用戶群組、租用戶用戶以及可選的 S3 存取金鑰在StorageGRID系統之間的自動複製。"電網聯合連接" 。

需要克隆帳戶"跨網格複製"。將帳戶資訊從來源StorageGRID系統複製到目標StorageGRID系統可確保租用戶使用者和群組可以存取任一網格上的對應儲存桶和物件。

帳戶克隆工作流程

工作流程圖顯示了網格管理員和允許的租戶將執行的設定帳戶複製的步驟。這些步驟在"電網聯合連接已配置"。



網格管理工作流程

網格管理員執行的步驟取決於StorageGRID系統是否"電網聯合連接"使用單一登入（SSO）或身分聯合。

配置帳戶克隆的 **SSO**（可選）

如果網格聯合連接中的任一StorageGRID系統使用 SSO，則兩個網格都必須使用 SSO。在建立網格聯合的租用戶帳戶之前，租用戶的來源網格和目標網格的網格管理員必須執行下列步驟。

步驟

1. 為兩個網格配置相同的身份來源。看"使用身分聯合" 。
2. 為兩個網格配置相同的 SSO 身分提供者 (IdP)。看"配置單一登入" 。
3. "建立相同的管理員群組"透過匯入相同的聯合群組在兩個網格上。

   當您建立租用戶時，您將選擇此群組以擁有來源和目標租用戶帳戶的初始 Root 存取權。

   > ⓘ 如果在建立租用戶之前兩個網格上都不存在此管理群組，則該租用戶不會被複製到目標。

為帳戶複製配置網格層級身分聯合（可選）

若任一StorageGRID系統使用不含 SSO 的身份聯合，則兩個網格都必須使用身分聯合。在建立網格聯合的租用戶帳戶之前，租用戶的來源網格和目標網格的網格管理員必須執行下列步驟。

步驟

1. 為兩個網格配置相同的身份來源。看"使用身分聯合" 。
2. 或者，如果聯合群組對來源租用戶帳戶和目標租用戶帳戶都具有初始 Root 存取權限，"建立相同的管理群組"透過匯入相同的聯合群組在兩個網格上。

   > ⓘ 如果您將 Root 存取權限指派給兩個網格上均不存在的聯合群組，則租用戶不會被複製到目標網格。

3. 如果您不希望聯合群組對兩個帳戶都具有初始 Root 存取權限，請為本機 root 使用者指定密碼。

建立允許的 **S3** 租用戶帳戶

在選擇性地設定 SSO 或身分聯合後，網格管理員執行下列步驟來確定哪些租用戶可以將儲存桶物件複製到其他StorageGRID系統。

步驟

1. 確定您希望哪個網格作為租用戶帳戶複製操作的來源網格。

   最初建立租戶的網格稱為租戶的_來源網格_。複製租戶的網格稱為租戶的_目標網格_。

2. 在該網格上，建立一個新的 S3 租用戶帳戶或編輯現有帳戶。
3. 分配*使用電網聯合連線*權限。
4. 如果租用戶帳戶將管理其自己的聯合用戶，請指派*使用自己的身分來源*權限。

   如果指派了此權限，則在建立聯合群組之前，來源租用戶帳戶和目標租用戶帳戶都必須配置相同的身分來源。除非兩個網格使用相同的身分來源，否則新增至來源租用戶的聯合群組無法複製到目標租用戶。

5. 選擇特定的電網聯合連接。

6. 保存新的或修改後的租戶。

   當儲存具有「使用網格聯合連線」權限的新租用戶時， StorageGRID會自動在另一個網格上建立該租用戶的副本，如下所示：

   - 兩個租用戶帳戶具有相同的帳戶 ID、名稱、儲存配額和分配的權限。
   - 如果您選擇聯合群組來為租用戶提供 Root 存取權限，則該群組將被複製到目標租用戶。
   - 如果您選擇本機使用者擁有租用戶的 Root 存取權限，則該使用者將被複製到目標租用戶。但是，該用戶的密碼未被複製。

有關詳細信息，請參閱"管理電網聯合的允許租戶" 。

允許的租用戶帳戶工作流程

將具有 使用網格聯合連線 權限的租用戶複製到目標網格後，允許的租用戶帳戶可以執行下列步驟來複製租用戶群組、使用者和 S3 存取金鑰。

步驟

1. Sign in租戶來源網格上的租戶帳戶。
2. 如果允許，請在來源租用戶帳戶和目標租用戶帳戶上配置身分聯合。
3. 在來源租用戶上建立群組和使用者。

   當在來源租用戶上建立新的群組或使用者時， StorageGRID會自動將其複製到目標租用戶，但不會從目標複製回來源。

4. 建立 S3 存取密鑰。
5. 或者，將 S3 存取金鑰從來源租用戶複製到目標租用戶。

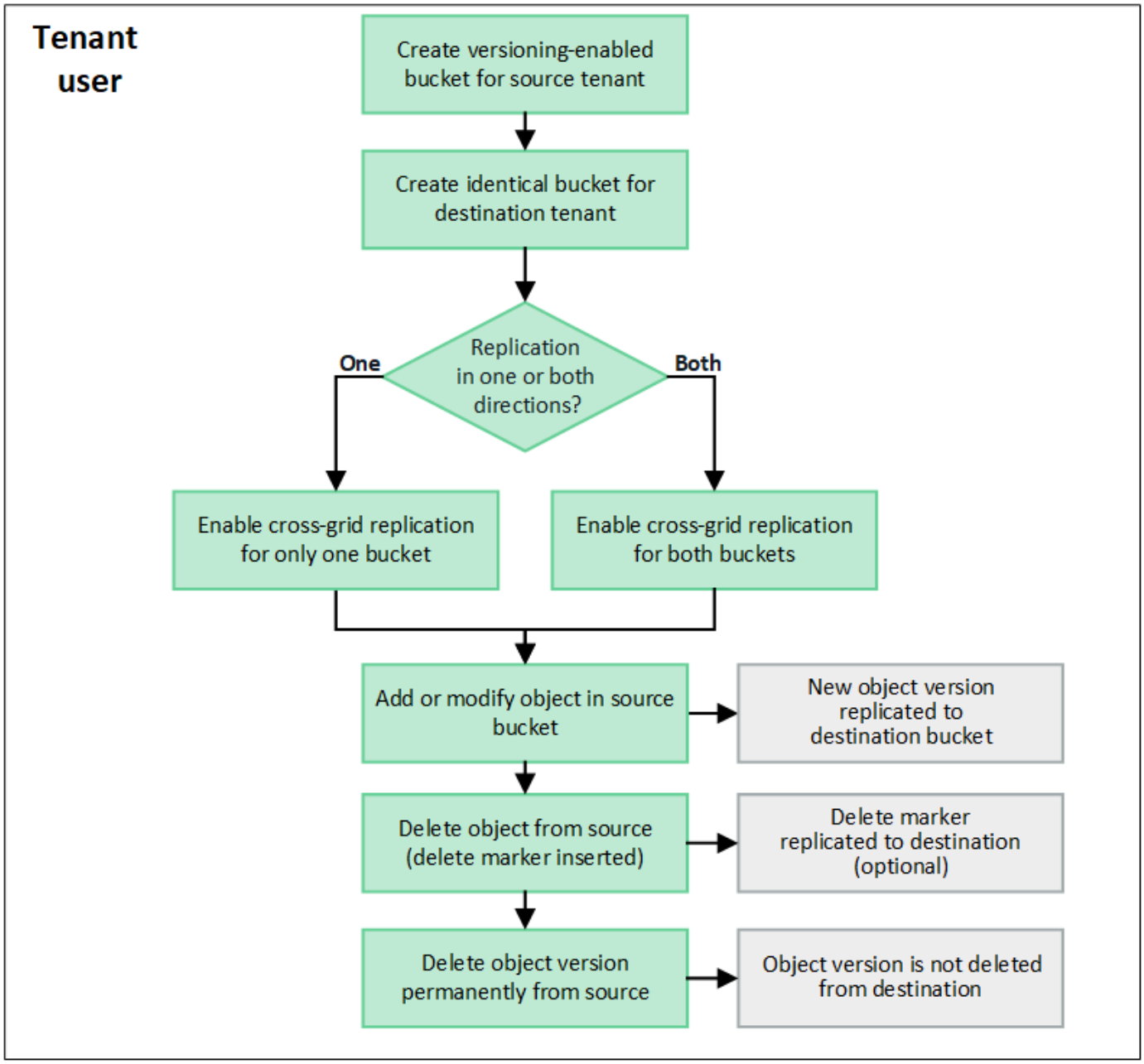
有關允許租用戶帳戶工作流程的詳細資訊以及如何複製群組、使用者和 S3 存取金鑰，請參閱"克隆租戶群組和用戶"和"使用 API 克隆 S3 存取金鑰"。

什麼是跨網格複製？

跨網格複製是指在兩個StorageGRID系統中選定的 S3 儲存桶之間自動複製對象，這兩個系統以"電網聯合連接"。"帳戶克隆"是跨網格複製所必需的。

跨網格複製的工作流程

工作流程圖總結了在兩個網格上的儲存桶之間配置跨網格複製的步驟。



跨網格複製的要求

如果租用戶帳戶具有使用網格聯合連線權限，則可以使用一個或多個"電網聯合連接"，具有 Root 存取權限的租用戶用戶可以在每個網格上對應的租用戶帳戶中建立相同的 bucket。這些存儲桶：

- 必須具有相同的名稱，但可以有不同的區域
- 必須啟用版本控制
- 必須停用 S3 物件鎖
- 必須為空

建立兩個儲存桶後，可以為其中一個或兩個儲存桶配置跨網格複製。

了解更多

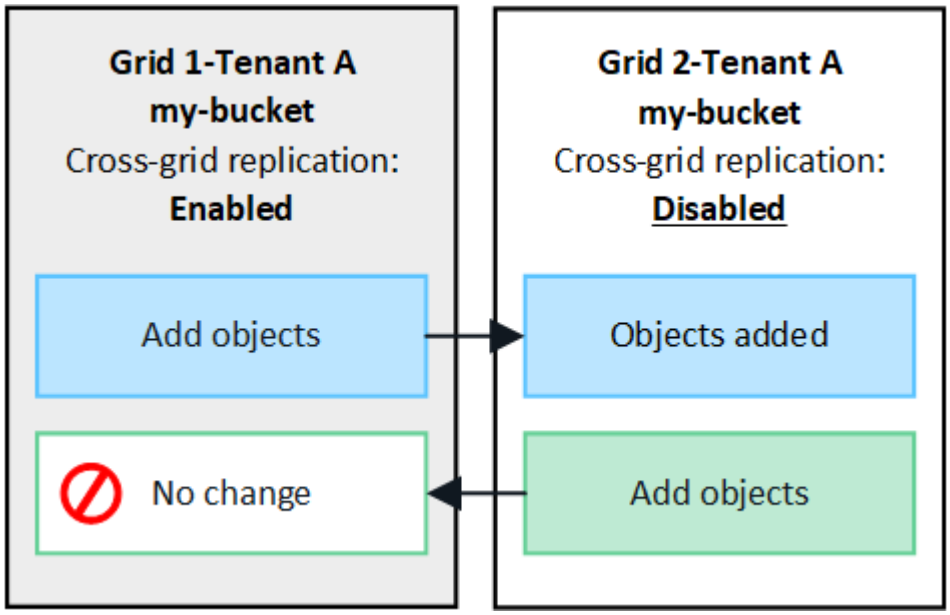
"管理跨網格複製"

跨網格複製的工作原理

跨網格複製可以配置為單向或雙向進行。

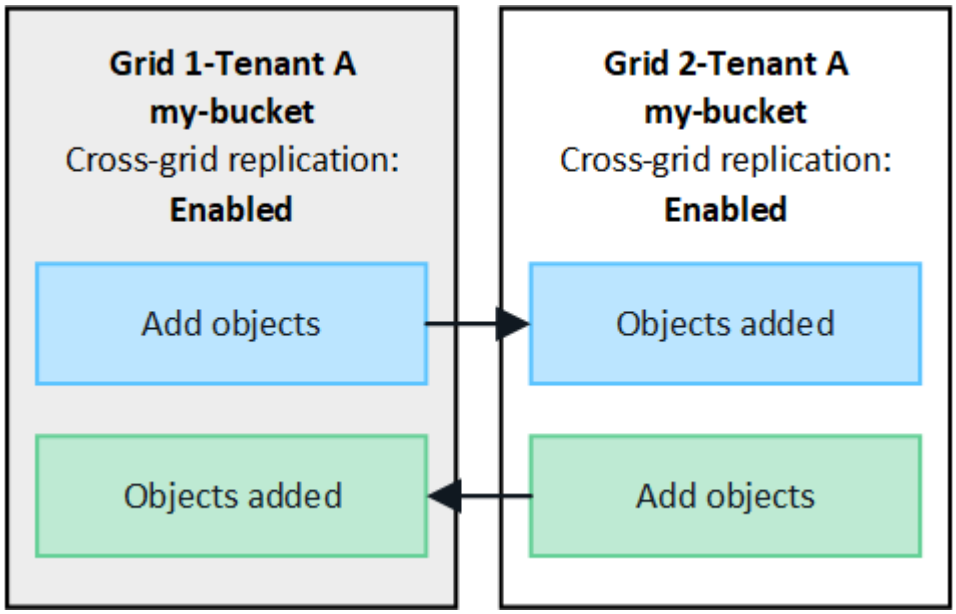
單向複製

如果僅為一個網格上的儲存桶啟用跨網格複製，則新增至該儲存桶（來源儲存桶）的物件將複製到另一個網格上的對應儲存桶（目標儲存桶）。但是，新增到目標儲存桶的物件不會被複製回來源。圖中，啟用了跨網格複製 `my-bucket`從網格 1 到網格 2，但在另一個方向未啟用。



雙向複製

如果在兩個網格上為同一個儲存桶啟用跨網格複製，則新增至任一儲存桶的物件都會複製到另一個網格。圖中，啟用了跨網格複製 `my-bucket`在兩個方向上。



當物體被吞食時會發生什麼事？

當 S3 用戶端將物件新增至啟用了跨網格複製的儲存桶時，會發生以下情況：

1. StorageGRID會自動將物件從來源儲存桶複製到目標儲存桶。執行此後台複製作業的時間取決於幾個因素，包括待處理的其他複製作業的數量。

   S3 用戶端可以透過發出 GetObject 或 HeadObject 請求來驗證物件的複製狀態。響應包括StorageGRID特定的 `x-ntap-sg-cgr-replication-status`回應標頭，它將具有以下值之一：S3 用戶端可以透過發出 GetObject 或 HeadObject 請求來驗證物件的複製狀態。響應包括StorageGRID特定的 `x-ntap-sg-cgr-replication-status`響應標頭，它將具有以下值之一：

網格	複製狀態
來源	• 已完成：所有電網連線的複製均已成功。 • 待定：物件尚未複製到至少一個電網連線。 • 失敗：任何電網連線均未掛起複製，且至少有一個電網連線發生永久性故障。使用者必須解決該錯誤。
目的地	**REPLICA**：物件已從來源網格複製。

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

2. StorageGRID使用每個網格的活動 ILM 策略來管理對象，就像管理任何其他對像一樣。例如，網格 1 上的物件 A 可能儲存為兩個副本並永久保留，而複製到網格 2 的物件 A 的副本可能使用 2+1 擦除編碼儲存並在三年後刪除。

當物件被刪除時會發生什麼？

正如所述"刪除資料流"， StorageGRID可能會因以下任何原因刪除物件：

- S3客戶端發出刪除請求。
- 租戶管理器用戶選擇"刪除儲存桶中的對象"從儲存桶中刪除所有物件的選項。
- bucket有一個生命週期配置，它會過期。
- 物件的 ILM 規則中的最後一個時間段結束，並且沒有指定進一步的放置位置。

當StorageGRID因刪除儲存桶操作中的物件、儲存桶生命週期到期或 ILM 放置到期而刪除物件時，複製的物件永遠不會從網格聯合連接中的另一個網格中刪除。但是，S3 用戶端刪除新增至來源儲存桶的刪除標記可以選擇複製到目標儲存桶。

要了解當 S3 用戶端從啟用了跨網格複製的儲存桶中刪除對象時會發生什麼，請查看 S3 用戶端如何從啟用了版本控制的儲存桶中刪除對象，如下所示：

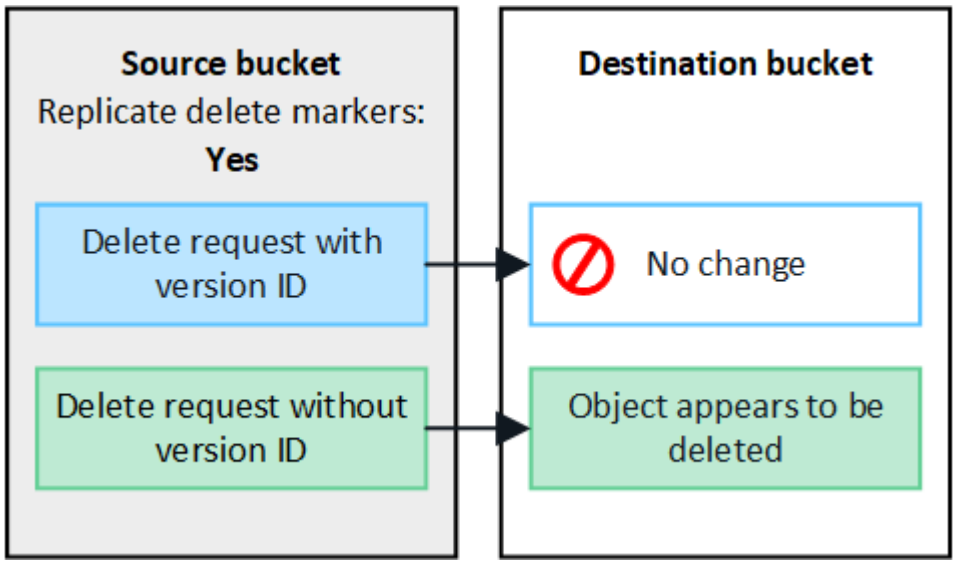
- 如果 S3 用戶端發出包含版本 ID 的刪除要求，則該版本的物件將永久刪除。未向儲存桶新增刪除標記。
- 如果 S3 用戶端發出不包含版本 ID 的刪除請求， StorageGRID不會刪除任何物件版本。相反，它會向儲存桶添加一個刪除標記。刪除標記使StorageGRID表現得好像物件已被刪除：
  - 沒有版本 ID 的 GetObject 請求將會失敗，並顯示 `404 No Object Found`

- 具有有效版本 ID 的 GetObject 請求將會成功並傳回請求的物件版本。

當 S3 用戶端從啟用了跨網格複製的儲存桶中刪除物件時， StorageGRID會決定是否將刪除請求複製到目標，如下所示：

- 如果刪除請求包含版本 ID，則該物件版本將從來源網格中永久刪除。但是， StorageGRID不會複製包含版本 ID 的刪除請求，因此相同的物件版本不會從目標中刪除。
- 如果刪除請求不包含版本 ID， StorageGRID可以根據儲存桶的跨網格複製配置方式選擇性地複製刪除標記：
  - 如果您選擇複製刪除標記（預設），則刪除標記將新增至來源儲存桶並複製到目標儲存體桶。實際上，該物件似乎在兩個網格上都被刪除了。
  - 如果您選擇不複製刪除標記，則刪除標記將新增至來源儲存桶，但不會複製到目標儲存桶。實際上，在來源網格上刪除的物件不會在目標網格上刪除。

在圖中，當"跨網格複製已啟用"。包含版本 ID 的來源儲存桶的刪除請求不會從目標儲存桶中刪除物件。不包含版本 ID 的來源儲存桶的刪除請求將顯示為刪除目標儲存桶中的物件。



如果要保持網格之間的物件刪除同步，請建立對應的"S3 生命週期配置"對於兩個網格上的桶。

如何複製加密對象

當您使用跨網格複製在網格之間複製物件時，您可以加密單一物件、使用預設儲存桶加密或配置網格範圍加密。您可以在為儲存桶啟用跨網格複製之前或之後新增、修改或刪除預設儲存體桶或網格範圍的加密設定。

若要加密單一對象，您可以在將物件新增至來源儲存桶時使用 SSE（使用StorageGRID管理金鑰的伺服器端加密）。使用 `x-amz-server-side-encryption`請求標頭並指定 `AES256`。看"使用伺服器端加密"。

跨網格複製不支援使用 SSE-C（使用客戶提供的金鑰的伺服器端加密）。攝取操作將會失敗。

若要對儲存桶使用預設加密，請使用 PutBucketEncryption 請求並設定 `SSEAlgorithm`參數 `AES256`。儲存桶級加密適用於未經 `x-amz-server-side-encryption`請求標頭。看"對 bucket 的操作"。

若要使用網格級加密，請將*儲存物件加密*選項設為*AES-256*。網格級加密適用於未在儲存桶層級加密的任何對象，或未經 `x-amz-server-side-encryption`請求標頭。看"配置網路和物件選項"。

SSE 不支援 AES-128。如果使用 **AES-128** 選項為來源網格啟用了 儲存物件加密 選項，則 AES-128 演算法的使用將不會傳播到複製的物件。相反，複製的物件將使用目標的預設儲存桶或網格級加密設定（如果可用）。

在決定如何加密來源物件時， StorageGRID會套用下列規則：

1. 使用 `x-amz-server-side-encryption`攝取標頭（如果存在）。
2. 如果不存在攝取標頭，則使用儲存桶預設加密設定（如果已配置）。
3. 如果未配置儲存桶設置，則使用網格範圍的加密設定（如果已配置）。
4. 如果不存在網格範圍的設置，則不要加密來源物件。

在決定如何加密複製物件時， StorageGRID會依照下列順序套用這些規則：

1. 使用與來源物件相同的加密，除非該物件使用 AES-128 加密。
2. 如果來源物件未加密或使用 AES-128，則使用目標儲存桶的預設加密設定（如果已配置）。
3. 如果目標儲存桶沒有加密設置，則使用目標的網格範圍加密設定（如果已配置）。
4. 如果不存在網格範圍的設置，則不要加密目標物件。

不支援 **PutObjectTagging** 和 **DeleteObjectTagging**

對於已啟用跨網格複製的儲存桶中的對象，不支援 PutObjectTagging 和 DeleteObjectTagging 請求。

如果 S3 用戶端發出 PutObjectTagging 或 DeleteObjectTagging 請求， `501 Not Implemented`被退回。訊息是 `Put(Delete) ObjectTagging is not available for buckets that have cross-grid replication configured`。

如何複製分段對象

來源網格的最大段大小適用於複製到目標網格的物件。當物件被複製到另一個網格時，來源網格的*最大段大小*設定（配置>*系統*>*儲存選項*）將在兩個網格上使用。例如，假設來源網格的最大段大小為 1 GB，而目標網格的最大段大小為 50 MB。如果您在來源網格上提取一個 2 GB 的對象，則該對象將保存為兩個 1 GB 的段。它還將作為兩個 1 GB 的段複製到目標網格，即使該網格的最大段大小為 50 MB。

比較跨網格複製和 **CloudMirror** 複製

當你開始使用網格聯合時，回顧一下"跨網格複製"以及"StorageGRID CloudMirror 複製服務"。

	跨網格複製	**CloudMirror**複製服務
主要目的是什麼？	一個StorageGRID系統充當災難復原系統。儲存桶中的物件可以在網格之間單向或雙向複製。	使租用戶能夠自動將物件從StorageGRID （來源）中的儲存桶複製到外部 S3 儲存桶（目標）。 CloudMirror 複製在獨立的 S3 基礎架構中建立物件的獨立副本。此獨立副本不用作備份，但通常在雲端中進一步處理。

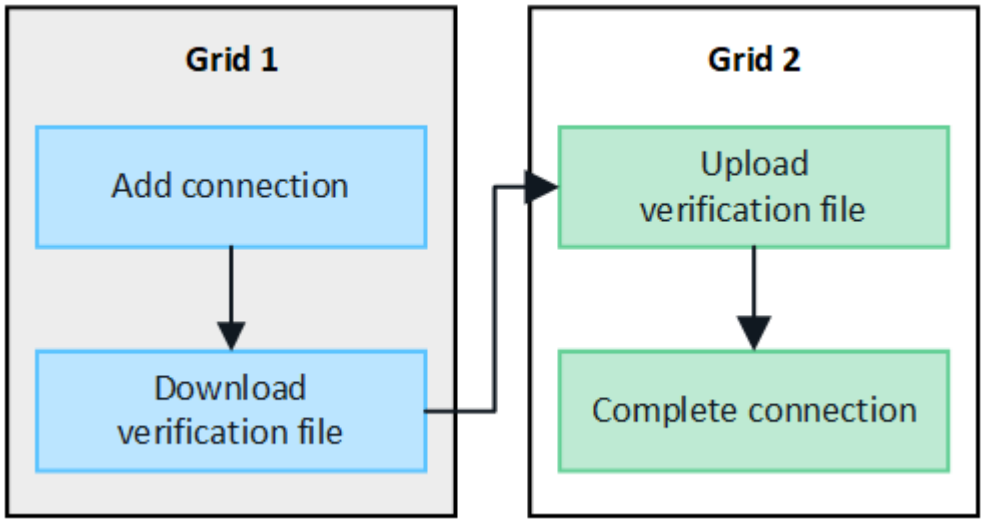
	跨網格複製	**CloudMirror**複製服務
如何設置？	1. 配置兩個網格之間的網格聯合連接。 2. 新增的租用戶帳戶，這些帳戶會自動複製到另一個網格。 3. 新增新的租戶群組和用戶，也進行克隆。 4. 在每個網格上建立相應的儲存桶，並啟用跨網格複製以在一個方向或兩個方向上進行。	1. 租用戶用戶透過使用租用戶管理器或 S3 API 定義 CloudMirror 端點（IP 位址、憑證等）來設定 CloudMirror 複製。 2. 此租用戶帳戶擁有的任何儲存桶都可以設定為指向 CloudMirror 端點。
誰負責設置它？	• 網格管理員配置連線和租用戶。 • 租戶用戶配置群組、用戶、密鑰和儲存桶。	通常是租戶用戶。
目的地是哪裡？	網格聯合連接中另一個StorageGRID系統上對應且相同的 S3 儲存桶。	• 任何相容的 S3 基礎設施（包括 Amazon S3）。 • 谷歌雲端平台（GCP）
是否需要物件版本控制？	是的，來源儲存桶和目標儲存桶都必須啟用物件版本控制。	不，CloudMirror 複製支援來源和目標上任意組合的非版本化和版本化儲存桶。
什麼原因導致物體移動到目的地？	當物件被加入到啟用了跨網格複製的儲存桶時，它們會自動複製。	當物件被加入到已配置 CloudMirror 端點的儲存桶時，物件會自動複製。在使用 CloudMirror 端點配置儲存桶之前，來源儲存桶中存在的物件不會被複製，除非它們被修改。
物件是如何複製的？	跨網格複製建立版本化對象，並將版本 ID 從來源儲存桶複製到目標儲存桶。這允許在兩個網格中維護版本順序。	CloudMirror 複製不需要啟用版本控制的儲存桶，因此 CloudMirror 只能維護網站內金鑰的排序。無法保證對不同站點的物件請求的順序能夠保持不變。
如果一個物件無法被複製怎麼辦？	該物件正在排隊等待複製，但受到元資料儲存限制。	該物件正在排隊等待複製，但受平台服務限制（請參閱"使用平台服務的建議"）。
物件的系統元資料是否被複製？	是的，當一個物件被複製到另一個網格時，它的系統元資料也會被複製。兩個網格上的元資料將是相同的。	不會，當物件被複製到外部儲存桶時，其係統元資料會被更新。元資料在不同位置會有所不同，取決於攝取時間和獨立 S3 基礎設施的行為。
如何檢索物件？	應用程式可以透過向任一網格上的儲存桶發出請求來檢索或讀取物件。	應用程式可以透過向StorageGRID或 S3 目標發出請求來檢索或讀取物件。例如，假設您使用 CloudMirror 複製將物件映像到合作夥伴組織。合作夥伴可以使用自己的應用程式直接從 S3 目標讀取或更新物件。不需要使用StorageGRID 。

	跨網格複製	CloudMirror複製服務
如果刪除物件會發生什麼？	• 包含版本 ID 的刪除請求永遠不會複製到目標網格。 • 不包含版本 ID 的刪除請求會向來源儲存桶新增刪除標記，可以選擇將其複製到目標網格。 • 如果跨網格複製僅配置為一個方向，則可以刪除目標儲存體桶中的物件而不會影響來源。	結果將根據來源儲存桶和目標儲存桶的版本狀態而有所不同（它們不需要相同）： • 如果兩個儲存桶都已版本化，則刪除請求將在兩個位置新增刪除標記。 • 如果僅對來源儲存桶進行版本控制，則刪除請求將向來源新增刪除標記，但不會向目標新增刪除標記。 • 如果兩個儲存桶都沒有版本控制，則刪除請求將從來源中刪除對象，但不會從目標中刪除。 同樣，可以刪除目標儲存桶中的對象，而不會影響來源。

建立電網聯合連接

如果您想要複製租用戶詳細資料並複製物件數據，您可以在兩個StorageGRID系統之間建立網格聯合連接。

如圖所示，建立電網聯合連接包括兩個電網上的步驟。您在一個網格上新增連接，然後在另一個網格上完成它。您可以從任一網格開始。



開始之前

- 您已審閱"注意事項和要求"用於配置電網聯合連接。
- 如果您打算為每個網格使用完全限定網域名稱 (FQDN) 而不是 IP 或 VIP 位址，那麼您知道要使用哪些名稱，並且您已確認每個網格的 DNS 伺服器都有適當的項目。
- 您正在使用"支援的網頁瀏覽器"。
- 您擁有兩個網格的 Root 存取權限和設定密碼。

新增連接

在兩個StorageGRID系統之一上執行這些步驟。

步驟

1. 從任一網格上的主管理節點Sign in入網格管理器。
2. 選擇 配置 > 系統 > 網格聯合。
3. 選擇*新增連線*。
4. 輸入連接的詳細資訊。

場地	描述
連接名稱	幫助您識別此連接的唯一名稱，例如「網格 1-網格 2」。
此網格的 FQDN 或 IP	以下之一： • 您目前登入的網格的 FQDN • 此網格上 HA 組的 VIP 位址 • 此網格上的管理節點或網關節點的 IP 位址。 IP 可以位於目標網格可以到達的任何網路上。
港口	您想要用於此連線的連接埠。您可以輸入 23000 至 23999 之間的任何未使用的連接埠號碼。 此連接中的兩個電網將使用相同的連接埠。您必須確保任一網格中均沒有節點使用此連接埠進行其他連接。
此網格的證書有效天數	您希望連接中此網格的安全性憑證有效的天數。預設值為 730 天（2 年），但您可以輸入 1 到 762 天之間的任意值。 儲存連線時， StorageGRID會自動為每個網格產生用戶端和伺服器憑證。
為此網格配置密碼	您所登入的網格的設定密碼。
另一個網格的 FQDN 或 IP	以下之一： • 您要連接的網格的 FQDN • 另一個網格上的 HA 群組的 VIP 位址 • 另一個網格上的管理節點或網關節點的 IP 位址。 IP 可以位於來源網格可以到達的任何網路上。

5. 選擇*儲存並繼續*。
6. 對於下載驗證檔案步驟，選擇*下載驗證檔案*。

   在另一個網格上完成連線後，您將無法再從任一網格下載驗證檔。

7. 找到下載的文件(*connection-name*.grid-federation)，並將其儲存到安全位置。

   該文件包含機密資訊（偽裝成 *) 和其他敏感訊息，必須安全儲存和傳輸。

8. 選擇*關閉*返回網格聯合頁面。
9. 確認顯示了新連線並且其*連線狀態*為*等待連線*。
10. 提供 `*connection-name*.grid-federation`檔案發送給另一個網格的網格管理員。

完成連接

在您要連接的StorageGRID系統（另一個網格）上執行這些步驟。

步驟

1. 從主管理節點Sign in入網格管理器。
2. 選擇 配置 > 系統 > 網格聯合。
3. 選擇*上傳驗證檔案*進入上傳頁面。
4. 選擇*上傳驗證檔*。然後，瀏覽並選擇從第一個網格下載的文件(*connection-name*.grid-federation) 。

   顯示連接的詳細資訊。

5. 或者，為此網格的安全性憑證輸入不同的有效天數。 *證書有效天數*條目預設為您在第一個網格中輸入的值，但每個網格可以使用不同的到期日期。

   一般來說，連接兩端的憑證使用相同的天數。

   如果連線兩端的憑證過期，連線將停止運作，並且複製將處於待處理狀態，直到憑證更新為止。

6. 輸入您目前登入的網格的設定密碼。
7. 選擇*儲存並測試*。

   產生證書並測試連線。如果連線有效，則會出現成功訊息，並且新連線會列在網格聯合頁面上。 連線狀態*將為*已連線。

   如果出現錯誤訊息，請解決任何問題。看"解決網格聯合錯誤" 。

8. 前往第一個網格上的網格聯合頁面並刷新瀏覽器。確認*連線狀態*現在為*已連線*。
9. 建立連線後，安全刪除驗證文件的所有副本。

   如果您編輯此連接，將會建立一個新的驗證文件。原始檔案無法重複使用。

完成後

- 回顧以下考慮事項"管理獲準租戶"。
- "建立一個或多個新的租用戶帳戶"，指派*使用網格聯合連接*權限，並選擇新的連線。
- "管理連線"按要求。您可以編輯連接值、測試連接、輪換連接憑證或刪除連接。

- "監控連線"作為正常StorageGRID監控活動的一部分。
- "排除連線故障"，包括解決與帳戶克隆和跨網格複製相關的任何警報和錯誤。

管理電網聯合連接

管理StorageGRID系統之間的網格聯合連線包括編輯連線詳細資料、輪替憑證、刪除租用戶權限以及刪除未使用的連線。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"Root存取權限"針對您登入的網格。

編輯電網聯合連接

您可以透過登入連線中任一網格上的主管理節點來編輯網格聯合連線。對第一個網格進行變更後，您必須下載一個新的驗證檔案並將其上傳到另一個網格。

> ⓘ 在編輯連線時，帳戶複製或跨網格複製請求將繼續使用現有的連線設定。您對第一個網格所做的任何編輯都會保存在本機，但只有在將其上傳到第二個網格、儲存並測試後才會使用。

開始編輯連接

步驟

1. 從任一網格上的主管理節點Sign in入網格管理器。
2. 選擇 **NODES** 並確認系統中的所有其他管理節點都在線上。

> ⓘ 當您編輯網格聯合連線時， StorageGRID會嘗試在第一個網格上的所有管理節點上儲存「候選設定」檔案。如果該檔案無法儲存到所有管理節點，則當您選擇*儲存並測試*時會出現警告訊息。

3. 選擇 配置 > 系統 > 網格聯合。
4. 使用網格聯合頁面或特定連接的詳細資訊頁面上的*操作*功能表編輯連線詳細資訊。看"建立電網聯合連接"輸入什麼內容。

操作選單

a. 選擇連接的單選按鈕。
b. 選擇*操作* > 編輯。
c. 輸入新資訊。

詳細資訊頁面

a. 選擇連接名稱以顯示其詳細資訊。
b. 選擇*編輯*。
c. 輸入新資訊。

5. 輸入您登入的網格的設定密碼。
6. 選擇*儲存並繼續*。

   新值已儲存，但直到您將新的驗證檔案上傳到另一個網格後，它們才會套用於連線。

7. 選擇*下載驗證檔*。

   要稍後下載此文件，請轉到連接的詳細資訊頁面。

8. 找到下載的文件(*connection-name*.grid-federation)，並將其儲存到安全位置。

   驗證文件包含秘密，必須安全地儲存和傳輸。

9. 選擇*關閉*返回網格聯合頁面。
10. 確認*連線狀態*為*待編輯*。

    如果您開始編輯連線時連線狀態不是*已連線*，則它將不會變更為*待編輯*。

11. 提供 `*connection-name*.grid-federation`檔案發送給另一個網格的網格管理員。

完成編輯連接

透過在另一個網格上傳驗證檔案來完成連接編輯。

步驟

1. 從主管理節點Sign in入網格管理器。
2. 選擇 配置 > 系統 > 網格聯合。
3. 選擇*上傳驗證檔案*進入上傳頁面。
4. 選擇*上傳驗證檔*。然後，瀏覽並選擇從第一個網格下載的檔案。
5. 輸入您目前登入的網格的設定密碼。
6. 選擇*儲存並測試*。

   如果可以使用編輯的值建立連接，則會顯示成功訊息。否則，會出現錯誤訊息。查看訊息並解決任何問題。

7. 關閉精靈以返回網格聯合頁面。
8. 確認*連線狀態*為*已連線*。
9. 前往第一個網格上的網格聯合頁面並刷新瀏覽器。確認*連線狀態*現在為*已連線*。
10. 建立連線後，安全刪除驗證文件的所有副本。

測試電網聯合連接

步驟

1. 從主管理節點Sign in入網格管理器。
2. 選擇 配置 > 系統 > 網格聯合。

3. 使用網格聯合頁面或特定連接的詳細資訊頁面上的*操作*功能表測試連線。

操作選單

a. 選擇連接的單選按鈕。

b. 選擇*操作* > 測試。

詳細資訊頁面

a. 選擇連接名稱以顯示其詳細資訊。

b. 選擇*測試連線*。

4. 查看連線狀態：

連線狀態	描述
已連接	兩個電網均已連接並正常通訊。
錯誤	連線處於錯誤狀態。例如，憑證已過期或設定值不再有效。
待處理編輯	您已編輯此網格上的連接，但該連接仍在使用現有配置。若要完成編輯，請將新的驗證檔上傳到另一個網格。
等待連接	您已在此網格上配置了連接，但另一個網格上的連接尚未完成。從此網格下載驗證檔案並將其上傳到另一個網格。
未知	連線處於未知狀態，可能是由於網路問題或離線節點。

5. 如果連線狀態為*錯誤*，請解決任何問題。然後，再次選擇*測試連線*以確認問題已修復。

輪替連線憑證

每個網格聯合連線使用四個自動產生的 SSL 憑證來保護連線。當每個網格的兩個證書接近到期日期時，*網格聯合證書到期*警報會提醒您輪換證書。

如果連線兩端的憑證過期，連線將停止運作，並且複製將處於待處理狀態，直到憑證更新為止。

步驟

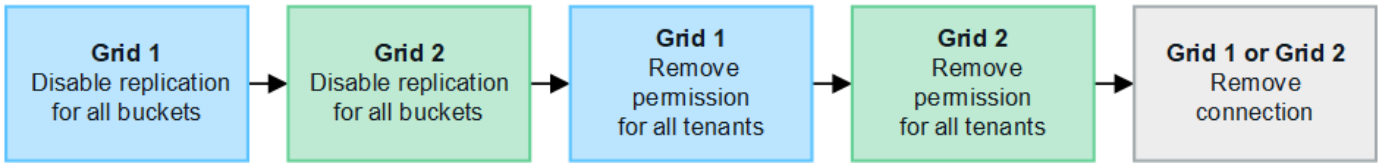
1. 從任一網格上的主管理節點Sign in入網格管理器。
2. 選擇 配置 > 系統 > 網格聯合。
3. 從網格聯合頁面上的任一標籤中，選擇連接名稱以顯示其詳細資訊。
4. 選擇“證書”選項卡。
5. 選擇*輪換證書*。
6. 指定新證書的有效期限。

7. 輸入您登入的網格的設定密碼。
8. 選擇*輪換證書*。
9. 根據需要，在連接中的另一個網格上重複這些步驟。

   一般來說，連接兩端的憑證使用相同的天數。

刪除電網聯合連接

您可以從連接中的任一網格中刪除網格聯合連接。如圖所示，您必須在兩個網格上執行先決條件步驟，以確認任一網格上都沒有任何租戶使用該連接。



刪除連線前，請注意以下事項：

- 刪除連接不會刪除網格之間已複製的任何項目。例如，當租用戶的權限被刪除時，兩個網格上都存在的租用戶用戶、群組和物件不會從任何一個網格中刪除。如果要刪除這些項目，則必須從兩個網格中手動刪除它們。
- 當您刪除連線時，任何待複製的物件（已擷取但尚未複製到其他網格）的複製都會永久失敗。

停用所有租用戶儲存桶的複製

步驟

1. 從任一網格開始，從主管理節點登入網格管理器。
2. 選擇 配置 > 系統 > 網格聯合。
3. 選擇連接名稱以顯示其詳細資訊。
4. 在「允許的租戶」標籤上，確定是否有任何租戶正在使用該連線。
5. 如果列出了任何租戶，指示所有租戶"禁用跨網格複製"連接中兩個網格上的所有儲存桶。

> 如果任何租用戶儲存桶啟用了跨網格複製，則您無法刪除*使用網格聯合連線*權限。每個租用戶帳戶必須停用兩個網格上其儲存桶的跨網格複製。

刪除每個租用戶的權限

在所有租用戶儲存桶的跨網格複製都停用後，從兩個網格上的所有租用戶中刪除「使用網格聯合權限」。

步驟

1. 選擇 配置 > 系統 > 網格聯合。
2. 選擇連接名稱以顯示其詳細資訊。
3. 對於「允許的租用戶」標籤上的每個租用戶，從每個租用戶中刪除「使用網格聯合連線*」權限。看"管理獲準租戶"。
4. 對另一個網格上允許的租戶重複這些步驟。

刪除連接

步驟

1. 當任一網格上都沒有租戶使用該連接時，選擇*刪除*。
2. 查看確認訊息，然後選擇*刪除*。
   - 如果可以刪除連接，則會顯示成功訊息。電網聯合連接現已從兩個電網中刪除。
   - 如果無法刪除連線（例如，它仍在使用中或存在連線錯誤），則會顯示錯誤訊息。您可以執行下列任一操作：
     - 解決錯誤（推薦）。看"解決網格聯合錯誤" 。
     - 強制斷開連線。請參閱下一部分。

強制刪除電網聯合連接

如果有必要，您可以強制刪除沒有*已連線*狀態的連線。

強制刪除只會從本地電網中刪除連線。若要完全刪除連接，請對兩個網格執行相同的步驟。

步驟

1. 從確認對話方塊中，選擇*強制刪除*。

   出現成功訊息。此電網聯合連接無法再使用。但是，租戶儲存桶可能仍然啟用跨網格複製，並且某些物件副本可能已經在連接中的網格之間複製。

2. 從連接中的另一個網格，從主管理節點登入網格管理器。
3. 選擇 配置 > 系統 > 網格聯合。
4. 選擇連接名稱以顯示其詳細資訊。
5. 選擇*刪除*和*是*。
6. 選擇“強制刪除”以從該網格中刪除連接。

管理電網聯合的允許租戶

您可以允許 S3 租用戶帳戶在兩個StorageGRID系統之間使用網格聯合連線。當允許租用戶使用連線時，需要採取特殊步驟來編輯租用戶詳細資料或永久刪除租用戶使用該連線的權限。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"Root存取權限"針對您登入的網格。
- 你有"創建了電網聯合連接"兩個網格之間。
- 您已查看了"帳戶克隆"和"跨網格複製"。
- 根據要求，您已經為連線中的兩個網格配置了單一登入 (SSO) 或識別聯合。看"什麼是帳戶克隆" 。

建立允許的租戶

如果您希望允許新的或現有的租用戶帳戶使用網格聯合連線進行帳戶複製和跨網格複製，請按照常規說明進行操作"建立新的 S3 租戶"或者"編輯租戶帳戶"並注意以下幾點：

- 您可以從連線中的任一網格建立租戶。建立租戶的網格是_租戶的來源網格_。
- 連線狀態必須為*已連線*。
- 當建立或編輯租戶以啟用*使用網格聯合連接*權限，然後保存在第一個網格上時，相同的租戶會自動複製到另一個網格。租戶被複製的網格是_租戶的目標網格_。
- 兩個網格上的租戶將具有相同的 20 位元帳戶 ID、名稱、描述、配額和權限。或者，您可以使用*描述*欄位來協助識別哪個是來源租戶，哪個是目標租戶。例如，在網格 1 上建立的租戶的描述也會出現在複製到網格 2 的租戶中：“此租戶是在網格 1 上建立的。”
- 出於安全原因，本機 root 使用者的密碼不會被複製到目標網格。

  在本機 root 使用者登入目標網格上的複製租用戶之前，該網格的網格管理員必須"更改本機 root 使用者的密碼"。

- 當新的或編輯的租戶在兩個網格上都可用時，租戶使用者可以執行以下操作：
  - 從租戶的來源網格建立群組和本機用戶，這些群組和本機用戶會自動複製到租戶的目標網格。看"克隆租戶群組和用戶" 。
  - 建立新的 S3 存取金鑰，可以選擇將其複製到租戶的目標網格。看"使用 API 克隆 S3 存取金鑰" 。
  - 在連接中的兩個網格上建立相同的儲存桶，並啟用單向或雙向跨網格複製。看"管理跨網格複製" 。

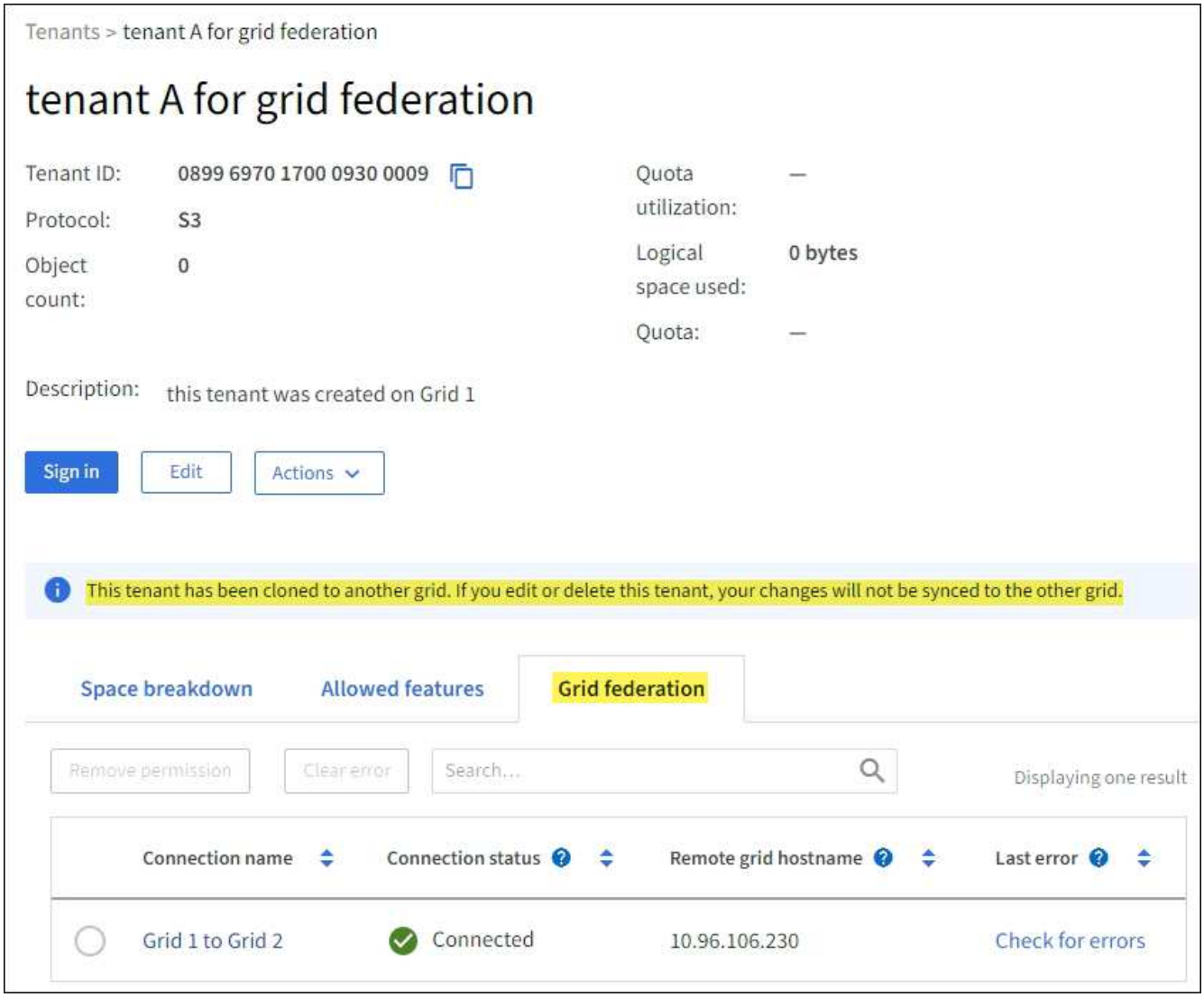
查看允許的租戶

您可以查看允許使用電網聯合連接的租戶的詳細資訊。

步驟

1. 選擇*租戶*。
2. 在租戶頁面中，選擇租戶名稱以查看租戶詳細資料頁面。

   如果這是租戶的來源網格（即，如果租戶是在此網格上建立的），則會出現一個橫幅提醒您租戶已複製到另一個網格。如果您編輯或刪除此租戶，您的變更將不會同步到其他網格。



3. （可選）選擇“網格聯合”選項卡"監控電網聯合連接"。

編輯允許的租戶

如果您需要編輯具有「使用網格聯合連線」權限的租用戶，請按照以下常規說明進行操作"編輯租戶帳戶"並注意以下幾點：

- 如果租用戶具有*使用網格聯合連線*權限，您可以從連線中的任一網格編輯租用戶詳細資料。但是，您所做的任何變更都不會複製到另一個網格。如果您想要保持網格之間的租戶詳細資訊同步，則必須在兩個網格上進行相同的編輯。
- 編輯租用戶時，您無法清除*使用網格聯合連線*權限。
- 編輯租戶時，您無法選擇不同的網格聯合連接。

刪除允許的租戶

如果您需要刪除具有「使用網格聯合連線」權限的租用戶，請按照以下常規說明進行操作"刪除租用戶帳戶"並注意以下幾點：

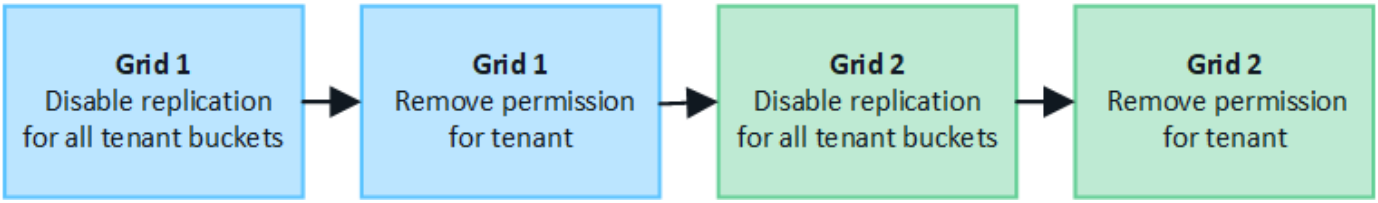
- 在刪除來源網格上的原始租用戶之前，您必須刪除來源網格上該帳戶的所有儲存體桶。

- 在刪除目標網格上的複製租戶之前，您必須刪除目標網格上該帳戶的所有儲存桶。
- 如果您刪除原始租戶或複製的租戶，則帳戶將不再用於跨網格複製。
- 如果您要刪除來源網格上的原始租用戶，則複製到目標網格的任何租用戶群組、使用者或金鑰都不會受到影響。您可以刪除複製的租用戶，也可以允許其管理自己的群組、使用者、存取金鑰和儲存桶。
- 如果您正在刪除目標網格上的複製租戶，則當向原始租戶新增群組或使用者時，將發生複製錯誤。

  為了避免這些錯誤，請在從此網格中刪除租用戶之前刪除該租用戶使用網格聯合連線的權限。

刪除使用電網聯合連線權限

若要阻止租用戶使用電網聯合連接，您必須刪除*使用電網聯合連接*權限。



在刪除租用戶使用電網聯合連線的權限之前，請注意以下事項：

- 如果任何租用戶的儲存桶啟用了跨網格複製，則您無法刪除*使用網格聯合連線*權限。租用戶帳戶必須先停用其所有儲存桶的跨網格複製。
- 刪除「使用網格聯合連線」權限不會刪除任何已在網格之間複製的項目。例如，當租戶的權限被刪除時，兩個網格上存在的任何租戶使用者、群組和物件都不會從任何一個網格中刪除。如果要刪除這些項目，則必須從兩個網格中手動刪除它們。
- 如果要使用相同的網格聯合連線重新啟用此權限，請先在目標網格上刪除此租用戶；否則，重新啟用此權限將導致錯誤。

> ⓘ 重新啟用*使用網格聯合連接*權限會使本機網格成為來源網格，並觸發複製到所選網格聯合連接指定的遠端網格。如果租用戶帳戶已存在於遠端網格上，則複製將導致衝突錯誤。

開始之前

- 您正在使用"支援的網頁瀏覽器"。
- 你有"Root存取權限"對於兩個網格。

停用租戶儲存桶的複製

第一步，停用所有租用戶儲存桶的跨網格複製。

步驟

1. 從任一網格開始，從主管理節點登入網格管理器。
2. 選擇 配置 > 系統 > 網格聯合。
3. 選擇連接名稱以顯示其詳細資訊。
4. 在「允許的租戶」標籤上，確定租戶是否正在使用該連線。
5. 如果租戶已列入名單，指示他們"禁用跨網格複製"連接中兩個網格上的所有儲存桶。

如果任何租用戶儲存桶啟用了跨網格複製，則您無法刪除*使用網格聯合連線*權限。租戶必須停用兩個網格上的儲存桶的跨網格複製。

刪除租用戶的權限

停用租用戶儲存桶的跨網格複製後，您可以刪除租用戶使用網格聯合連線的權限。

步驟

1. 從主管理節點Sign in入網格管理器。
2. 從網格聯合頁面或租用戶頁面中刪除權限。

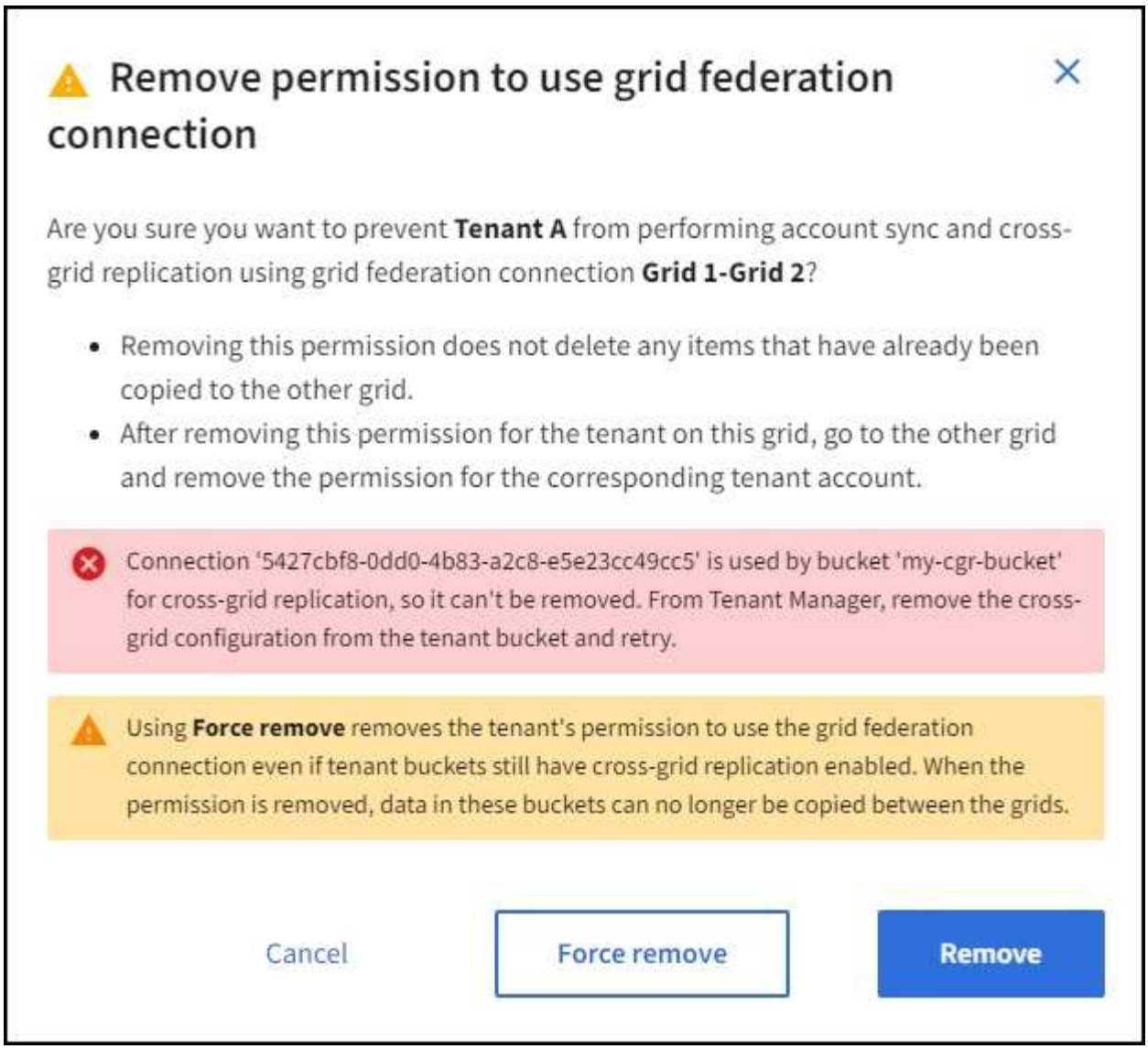
電網聯合頁面

a. 選擇 配置 > 系統 > 網格聯合。
b. 選擇連接名稱以顯示其詳細資訊頁面。
c. 在「允許的租戶」標籤上，選擇租戶的單選按鈕。
d. 選擇*刪除權限*。

租戶頁面

a. 選擇*租戶*。
b. 選擇租戶名稱以顯示詳細資訊頁面。
c. 在*網格聯合*標籤上，選擇連接的單選按鈕。
d. 選擇*刪除權限*。

3. 查看確認對話方塊中的警告，然後選擇*刪除*。
   - 如果可以刪除權限，您將返回詳細資料頁面並顯示成功訊息。該租戶無法再使用電網聯合連線。
   - 如果一個或多個租戶儲存桶仍啟用了跨網格複製，則會顯示錯誤。



您可以執行下列任一操作：

- （受到推崇的。）Sign in租用戶管理器並停用每個租用戶儲存桶的複製。看"管理跨網格複製" 。然後，重複這些步驟以刪除*使用電網連接*權限。
- 強制刪除權限。請參閱下一部分。

4. 轉到另一個網格並重複這些步驟以刪除另一個網格上相同租用戶的權限。

強制移除權限

如有必要，即使租用戶儲存桶已啟用跨網格複製，您也可以強制刪除租用戶使用網格聯合連線的權限。

在強制取消租戶許可之前，請注意以下一般注意事項刪除權限以及以下額外考慮：

- 如果您強制刪除*使用網格聯合連接*權限，則任何等待複製到另一個網格（已攝取但尚未複製）的物件將繼續被複製。為了防止這些正在處理的物件到達目標儲存桶，您還必須刪除租用戶在另一個網格上的權限。
- 刪除「使用網格聯合連線」權限後，任何被提取到來源儲存桶中的物件都不會被複製到目標儲存桶。

步驟

1. 從主管理節點Sign in入網格管理器。
2. 選擇 配置 > 系統 > 網格聯合。
3. 選擇連接名稱以顯示其詳細資訊頁面。
4. 在「允許的租戶」標籤上，選擇租戶的單選按鈕。
5. 選擇*刪除權限*。
6. 查看確認對話方塊中的警告，然後選擇*強制刪除*。

   出現成功訊息。該租戶無法再使用電網聯合連線。

7. 根據需要，請轉到另一個網格並重複這些步驟，強制刪除另一個網格上相同租用戶帳戶的權限。例如，您應該在另一個網格上重複這些步驟，以防止正在處理的物件到達目標儲存桶。

解決網格聯合錯誤

您可能需要排除與網格聯合連接、帳戶複製和跨網格複製相關的警報和錯誤。

網格聯合連接警報和錯誤

您可能會收到警報或遇到電網聯合連接錯誤。

進行任何變更以解決連線問題後，請測試連線以確保連線狀態已返回*已連線*。有關說明，請參閱"管理電網聯合連接"。

電網聯合連接失敗警報

問題

觸發了「電網聯合連線失敗」警報。

細節

此警報表示網格之間的網格聯合連接無法運作。

建議的操作

1. 檢查兩個網格的網格聯合頁面上的設定。確認所有數值均正確。看"管理電網聯合連接" 。
2. 檢查用於連接的憑證。確保沒有關於網格聯合證書過期的警報，並且每個證書的詳細資訊都是有效的。請參閱輪換連接證書的說明"管理電網聯合連接"。
3. 確認兩個網格中的所有管理節點和網關節點均在線且可用。解決可能影響這些節點的任何警報並重試。
4. 如果您為本地或遠端網格提供了完全限定網域名稱 (FQDN)，請確認 DNS 伺服器在線上且可用。看"什麼是電網聯合？"滿足網路、IP 位址和 DNS 需求。

電網聯合證書到期警報

問題

觸發了「電網聯合證書過期」警報。

細節

此警示表示一個或多個網格聯合憑證即將過期。

建議的操作

請參閱輪換連接證書的說明"管理電網聯合連接"。

編輯電網聯合連接時出錯

問題

編輯網格聯合連接時，選擇“儲存並測試”時會看到以下警告訊息：“無法在一個或多個節點上建立候選設定檔。”

細節

當您編輯網格聯合連線時， StorageGRID會嘗試在第一個網格上的所有管理節點上儲存「候選設定」檔案。如果無法將此檔案儲存到所有管理節點（例如，由於管理節點處於離線狀態），則會出現警告訊息。

建議的操作

1. 從用於編輯連接的網格中，選擇*NODES*。
2. 確認該網格的所有管理節點均在線。
3. 如果任何節點處於離線狀態，請將其重新連線並嘗試再次編輯連線。

帳戶克隆錯誤

無法登入克隆的租用戶帳戶

問題

您無法登入克隆的租用戶帳戶。租戶管理員登入頁面上的錯誤訊息是「此帳戶的憑證無效。請重試。

細節

出於安全原因，當租用戶帳戶從租用戶的來源網格複製到租用戶的目標網格時，您為租用戶的本機 root 使用者設定的密碼不會被複製。同樣，當租戶在其來源網格上建立本地用戶時，本地用戶密碼不會被複製到目標網格。

建議的操作

在 root 使用者登入租用戶的目標網格之前，網格管理員必須先"更改本機 root 使用者的密碼"在目標網格上。

在複製的本機使用者可以登入租用戶的目標網格之前，複製租用戶的根用戶必須在目標網格上為該用戶新增密碼。有關說明，請參閱"管理本地用戶"在使用租戶管理器的說明中。

未使用克隆創建的租戶

問題

使用 使用網格聯合連線 權限建立新租用戶後，您會看到訊息「建立租用戶時沒有複製」。

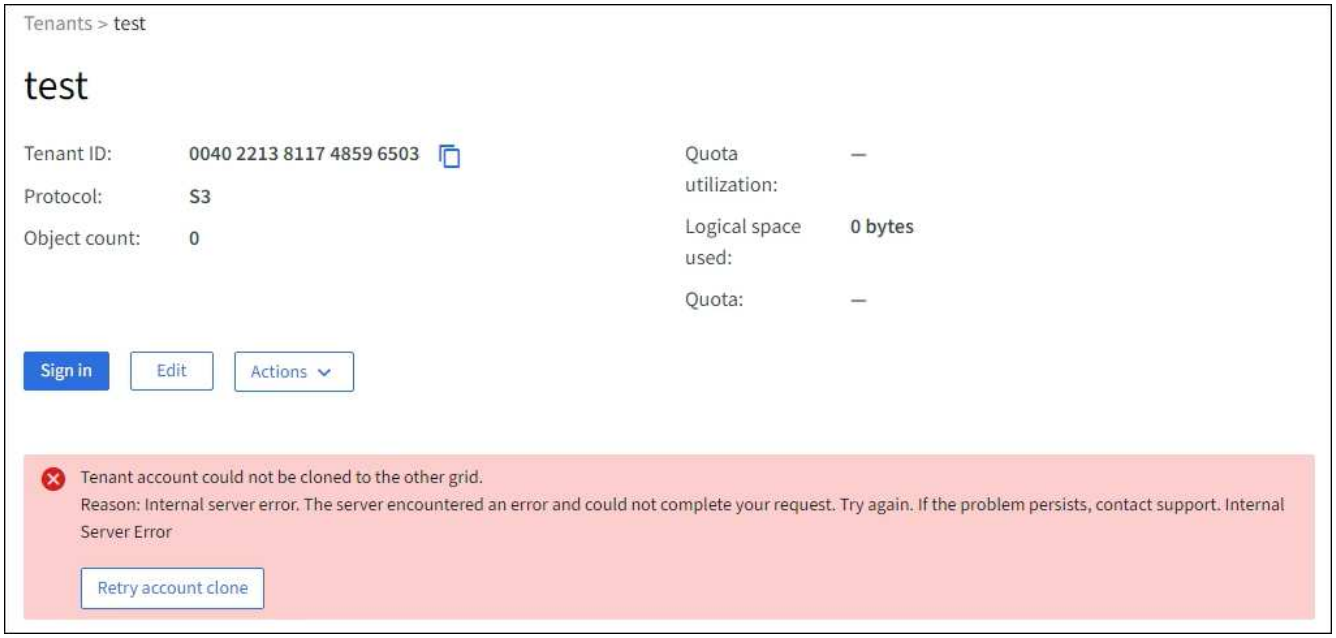
細節

如果連線狀態更新延遲，則可能會出現此問題，這可能會導致不健康的連線被列為*已連線*。

建議的操作

1. 查看錯誤訊息中列出的原因並解決任何可能阻止連接工作的網路或其他問題。看電網聯合連接警報和錯誤 。
2. 依照說明測試電網聯合連接"管理電網聯合連接"確認問題已解決。
3. 從租戶的來源網格中，選擇 **TENANTS**。

4. 找到克隆失敗的租用戶帳戶。
5. 選擇租戶名稱以顯示詳細資訊頁面。
6. 選擇*重試帳戶克隆*。



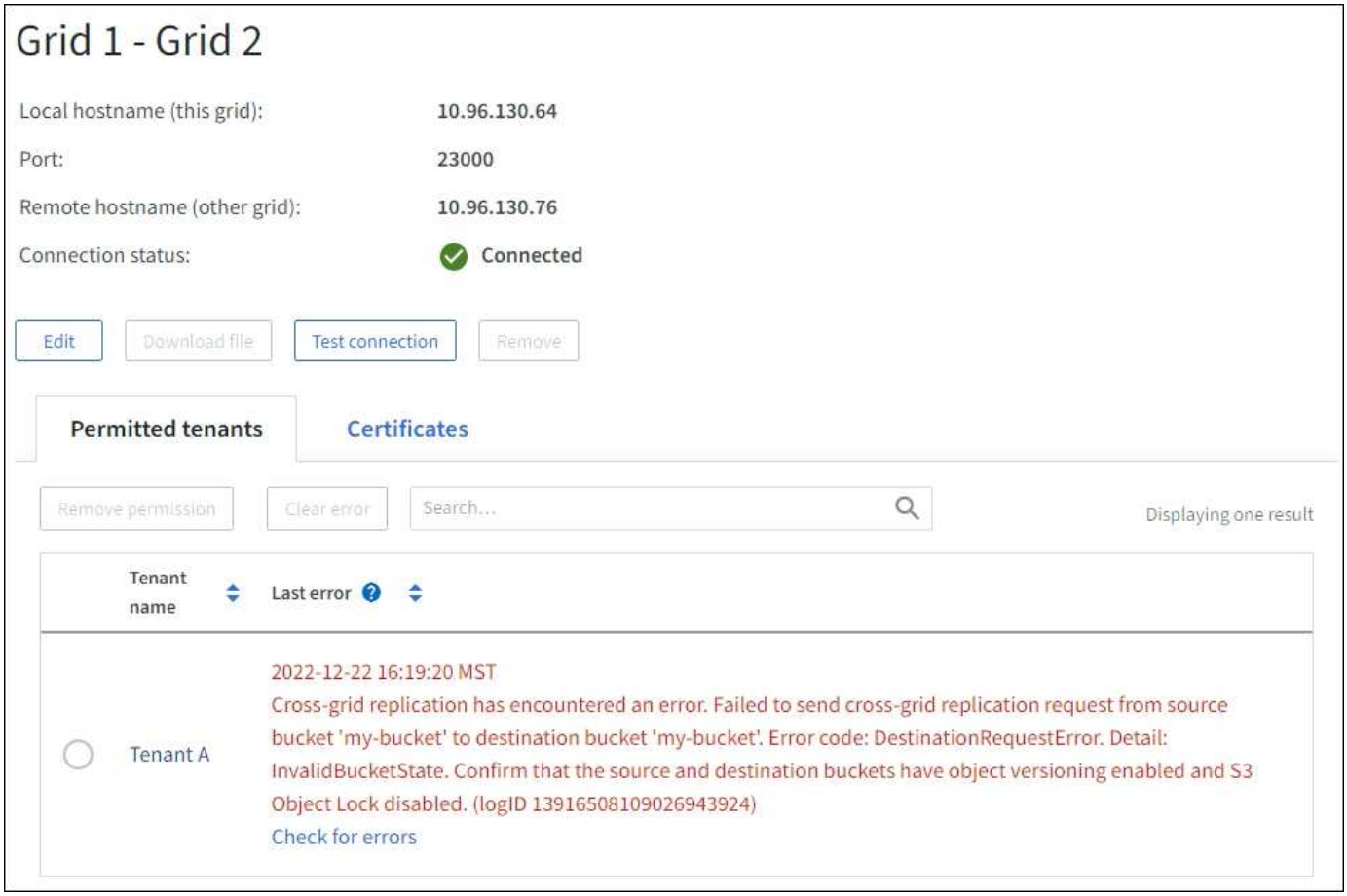
如果錯誤已解決，租用戶帳戶現在將被複製到另一個網格。

跨網格複製警報和錯誤

顯示連線或租戶的最後一個錯誤

問題

什麼時候"查看電網聯合連接"（或當"管理獲準租戶"對於連接），您會注意到連接詳細資訊頁面上的「最後錯誤」列中有一個錯誤。例如：



細節

對於每個網格聯合連接，*最後一個錯誤*列顯示租戶資料複製到另一個網格時發生的最近錯誤（如果有）。此列僅顯示最後發生的跨網格複製錯誤；之前可能發生的錯誤將不會顯示。此列中的錯誤可能由於以下原因之一而發生：

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

建議的操作

如果「上次錯誤」欄位中出現錯誤訊息，請依照下列步驟操作：

1. 查看訊息文字。
2. 執行任何建議的操作。例如，如果在目標儲存桶上暫停跨網格複製的版本控制，則重新啟用該儲存桶的版本控制。
3. 從表格中選擇連線或租用戶帳戶。
4. 選擇*清除錯誤*。

5. 選擇“是”清除該訊息並更新系統狀態。
6. 等待 5-6 分鐘，然後將新物件放入儲存桶中。確認錯誤訊息不再出現。

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

> 清除錯誤後，如果將物件提取到同樣存在錯誤的不同儲存桶中，則可能會出現新的*最後錯誤*。

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

跨網格複製永久故障警報

問題

觸發了「跨網格複製永久失敗」警報。

細節

此警報表示由於需要使用者乾預才能解決的原因，租戶物件無法在兩個網格上的儲存桶之間複製。此警報通常是由來源儲存桶或目標儲存桶的變更引起的。

建議的操作

1. Sign in觸發警報的網格。
2. 前往 配置 > 系統 > 網格聯合，然後找到警報中列出的連接名稱。
3. 在「允許的租用戶」標籤上，檢視「最後一個錯誤」欄位以確定哪些租用戶帳戶有錯誤。
4. 要了解有關失敗的更多信息，請參閱"監控電網聯合連接"查看跨網格複製指標。
5. 對於每個受影響的租戶帳戶：
   a. 請參閱"監控租戶活動"確認租戶在目標網格上沒有超出其跨網格複製的配額。
   b. 根據需要，增加目標網格上的租戶配額以允許保存新物件。
6. 對於每個受影響的租戶，登入兩個網格上的租戶管理器，以便您可以比較儲存桶清單。
7. 對於每個啟用了跨網格複製的儲存桶，請確認以下內容：
   - 另一個網格上有一個針對同一租戶的對應儲存桶（必須使用完全相同的名稱）。
   - 兩個儲存桶都啟用了物件版本控制（任一網格上都不能暫停版本控制）。
   - 兩個儲存桶均已停用 S3 物件鎖。
   - 兩個儲存桶均未處於*刪除物件：唯讀*狀態。
8. 若要確認問題是否已解決，請參閱"監控電網聯合連接"查看跨網格複製指標，或執行下列步驟：
   a. 返回網格聯合頁面。
   b. 選擇受影響的租戶，然後在*最後一個錯誤*列中選擇*清除錯誤*。
   c. 選擇“是”清除該訊息並更新系統狀態。
   d. 等待 5-6 分鐘，然後將新物件放入儲存桶中。確認錯誤訊息不再出現。

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

警報解決後可能需要一天的時間才能清除。

a. 前往"識別並重試失敗的複製操作"識別任何物件或刪除無法複製到另一個網格的標記，並根據需要重試複製。

跨網格複製資源不可用警報

問題

觸發了「跨網格複製資源不可用」警報。

細節

此警報表示由於資源不可用，跨網格複製請求處於待處理狀態。例如，可能存在網路錯誤。

建議的操作

1. 監視警報以查看問題是否自行解決。
2. 如果問題仍然存在，請確定任一網格是否對同一連接有*網格聯合連接失敗*警報或對某個節點有*無法與節點通訊*警報。當您解決這些警報時，此警報可能會解決。
3. 要了解有關失敗的更多信息，請參閱"監控電網聯合連接"查看跨網格複製指標。
4. 如果您無法解決警報，請聯絡技術支援。

問題解決後，跨網格複製將正常進行。

識別並重試失敗的複製操作

解決*跨網格複製永久失敗*警報後，您應該確定是否有任何物件或刪除標記無法複製到另一個網格。然後，您可以重新擷取這些物件或使用網格管理 API 重試複製。

*跨網格複製永久失敗*警報表示由於需要使用者乾預才能解決的原因，租戶物件無法在兩個網格上的儲存桶之間複製。此警報通常是由來源儲存桶或目標儲存桶的變更引起的。有關詳細信息，請參閱"解決網格聯合錯誤" 。

確定是否有任何物件複製失敗

若要確定是否有任何物件或刪除標記尚未複製到另一個網格，您可以搜尋稽核日誌"CGRR（跨網格複製請求）"消息。當StorageGRID無法將物件、多部分物件或刪除標記複製到目標儲存桶時，此訊息將會新增至日誌中。

您可以使用"審計解釋工具"將結果轉換成更易於閱讀的格式。

開始之前

- 您擁有 Root 存取權限。
- 你有 `Passwords.txt`文件。
- 您知道主管理節點的 IP 位址。

步驟

1. 登入主管理節點：
   a. 輸入以下命令： `ssh admin@primary_Admin_Node_IP`
   b. 輸入 `Passwords.txt`文件。

c. 輸入以下命令切換到root： `su -`

d. 輸入 `Passwords.txt`文件。

當您以 root 身分登入時，提示字元將從 `$`到 `#`。

2. 在 audit.log 中搜尋 CGRR 訊息，並使用 audit-explain 工具格式化結果。

例如，此命令會尋找過去 30 分鐘內的所有 CGRR 訊息並使用 audit-explain 工具。

```
# awk -vdate=$(date -d "30 minutes ago" '+%Y-%m-%dT%H:%M:%S') '$1$2 >= date {
print }' audit.log | grep CGRR | audit-explain
```

該命令的結果將類似於此範例，其中包含六個 CGRR 訊息的條目。在範例中，所有跨網格複製請求都傳回了一般錯誤，因為無法複製物件。前三個錯誤是針對「複製物件」操作的，後三個錯誤是針對「複製刪除標記」操作的。

```
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-0"
version:QjRBNDIzODAtNjQ3My0xMUVELTg2QjEtODJBMjAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-3"
version:QjRDOTRCOUMtNjQ3My0xMUVELTkzM0YtOTg1MTAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-1"
version:NUQ0OEYxMDAtNjQ3NC0xMUVELTg2NjMtOTY5NzAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-5"
version:NUQ1ODUwQkUtNjQ3NC0xMUVELTg1NTItRDkwNzAwQkI3NEM4 error:general
error
```

每個條目包含以下資訊：

場地	描述
CGRR 跨網格複製請求	請求的名稱
租戶	租戶的帳戶ID
聯繫	電網聯合連接的ID

場地	描述
手術	正在嘗試的複製操作類型： • 複製對象 • 複製刪除標記 • 複製多部分對象
桶	儲存桶名稱
目的	物件名稱
版本	物件的版本 ID
錯誤	錯誤類型。如果跨網格複製失敗，則錯誤為「常規錯誤」。

重試失敗的複製

產生未複製到目標儲存桶的物件和刪除標記清單並解決底層問題後，您可以透過以下兩種方式之一重試複製：

- 將每個物件重新放入來源儲存桶。
- 按照說明使用網格管理私有 API。

步驟

1. 從網格管理器的頂部，選擇幫助圖示並選擇*API 文件*。
2. 選擇*轉到私有 API 文件*。

   標記為「私有」的StorageGRID API 端點如有更改，恕不另行通知。 StorageGRID私有端點也會忽略請求的 API 版本。

3. 在 **cross-grid-replication-advanced** 部分中，選擇以下端點：

   ```
   POST /private/cross-grid-replication-retry-failed
   ```

4. 選擇*試用*。
5. 在 **body** 文字方塊中，將 **versionID** 的範例條目替換為 audit.log 中與失敗的跨網格複製請求相對應的版本 ID。

   確保保留字串周圍的雙引號。

6. 選擇*執行*。
7. 確認伺服器回應代碼為*204*，表示物件或刪除標記已被標記為待跨網格複製到另一個網格。

   待處理意味著跨網格複製請求已新增至內部佇列等待處理。

監視複製重試

您應該監視複製重試操作以確保它們完成。

將物件或刪除標記複製到另一個網格可能需要幾個小時或更長時間。

您可以透過以下兩種方式之一監視重試操作：

- 使用 S3"頭部對象"或者"取得對象"要求。響應包括StorageGRID特定的 `x-ntap-sg-cgr-replication-status`響應標頭，它將具有以下值之一：

網格	複製狀態
來源	• 已完成：複製成功。 • 待定：物件尚未被複製。 • 失敗：複製失敗，並發生永久性故障。使用者必須解決該錯誤。
目的地	**REPLICA**：物件已從來源網格複製。

- 按照說明使用網格管理私有 API。

步驟

1. 在私有 API 文件的 **cross-grid-replication-advanced** 部分中，選擇以下端點：

   ```
   GET /private/cross-grid-replication-object-status/{id}
   ```

2. 選擇*試用*。
3. 在參數部分中，輸入您在 `cross-grid-replication-retry-failed`要求。
4. 選擇*執行*。
5. 確認伺服器回應代碼為*200*。
6. 查看複製狀態，其狀態將是以下之一：
   - 待定：物件尚未被複製。
   - 已完成：複製成功。
   - 失敗：複製失敗，並發生永久性故障。使用者必須解決該錯誤。

管理安全

管理安全

您可以從網格管理器配置各種安全性設定來協助保護您的StorageGRID系統。

管理加密

StorageGRID提供了多種資料加密選項。你應該"查看可用的加密方法"以確定哪些符合您的資料保護要求。

管理證書

你可以"設定和管理伺服器證書"用於 HTTP 連線或用於向伺服器驗證用戶端或使用者身分的用戶端憑證。

配置金鑰管理伺服器

使用"金鑰管理伺服器"即使設備從資料中心移除，也能保護StorageGRID資料。裝置磁碟區加密後，除非節點可以與 KMS 通信，否則您無法存取裝置上的任何資料。

> 若要使用加密金鑰管理，您必須在安裝期間、將裝置新增至電網之前為每個裝置啟用「節點加密」設定。

管理代理設定

如果您使用 S3 平台服務或雲端儲存池，您可以設定"儲存代理伺服器"儲存節點和外部 S3 端點之間。如果您使用 HTTPS 或 HTTP 傳送AutoSupport軟體包，則可以設定"管理代理伺服器"管理節點和技術支援之間。

控制防火牆

為了增強系統的安全性，您可以透過開啟或關閉特定連接埠來控制對StorageGRID管理節點的存取"外部防火牆"。您還可以透過配置每個節點來控制其網路存取"內部防火牆"。您可以阻止部署所需連接埠之外的所有連接埠的存取。

查看**StorageGRID**加密方法

StorageGRID提供了多種資料加密選項。您應該檢查可用的方法以確定哪些方法符合您的資料保護要求。

此表提供了StorageGRID中可用的加密方法的進階摘要。

加密選項	工作原理	適用於
Grid Manager 中的金鑰管理伺服器 (KMS)	你"配置金鑰管理伺服器"對於StorageGRID站點和 "為裝置啟用節點加密"。然後，裝置節點連接到 KMS 以請求金鑰加密金鑰 (KEK)。此金鑰對每個磁碟區上的資料加密金鑰 (DEK) 進行加密和解密。	安裝期間啟用了*節點加密*的裝置節點。設備上的所有資料都受到保護，不會發生實體遺失或從資料中心移除。 注意：僅儲存節點和服務設備支援使用 KMS 管理加密金鑰。
StorageGRID裝置安裝程式中的磁碟機加密頁面	如果裝置包含支援硬體加密的驅動器，您可以在安裝期間設定驅動器密碼。當您設定磁碟機密碼時，任何人都不可能從已從系統中刪除的磁碟機中恢復有效數據，除非他們知道密碼。在開始安裝之前，請前往*設定硬體*>*磁碟機加密*來設定適用於節點中所有StorageGRID管理的自加密磁碟機的磁碟機密碼。	包含自加密磁碟機的裝置。安全驅動器上的所有資料都受到保護，不會發生實體遺失或從資料中心移除。 磁碟機加密不適用於SANtricity管理的磁碟機。如果您擁有具有自加密磁碟機和SANtricity控制器的儲存設備，則可以在SANtricity中啟用磁碟機安全性。

加密選項	工作原理	適用於
推動SANtricity System Manager 的安全性	如果您的StorageGRID裝置啟用了磁碟機安全功能，則可以使用"SANtricity系統管理員"建立和管理安全密鑰。需要密鑰才能存取安全驅動器上的資料。	具有全碟加密 (FDE) 磁碟機或自加密磁碟機的儲存裝置。安全驅動器上的所有資料都受到保護，不會發生實體遺失或從資料中心移除。不能與某些儲存設備或任何服務設備一起使用。
儲存物件加密	您啟用"儲存物件加密"網格管理器中的選項。啟用後，任何未在儲存桶層級或物件層級加密的新物件都會在攝取期間加密。	新攝取的 S3 物件資料。 現有儲存的物件未加密。對像元資料和其他敏感資料未加密。
S3 儲存桶加密	您發出 PutBucketEncryption 請求來為儲存桶啟用加密。任何未在物件層級加密的新物件都會在攝取期間加密。	僅限新攝取的 S3 物件資料。 必須為儲存桶指定加密。現有的儲存桶物件未加密。對像元資料和其他敏感資料未加密。 "對 bucket 的操作"
S3 物件伺服器端加密 (SSE)	您發出一個 S3 請求來儲存一個物件並包括 `x-amz-server-side-encryption`請求標頭。	僅限新攝取的 S3 物件資料。 必須為物件指定加密。對像元資料和其他敏感資料未加密。 StorageGRID管理金鑰。 "使用伺服器端加密"
使用客戶提供的金鑰對 S3 物件進行伺服器端加密 (SSE-C)	您發出 S3 請求來儲存物件並包含三個請求標頭。 • `x-amz-server-side-encryption-customer-algorithm` • `x-amz-server-side-encryption-customer-key` • `x-amz-server-side-encryption-customer-key-MD5`	僅限新攝取的 S3 物件資料。 必須為物件指定加密。對像元資料和其他敏感資料未加密。 密鑰在StorageGRID之外進行管理。 "使用伺服器端加密"

加密選項	工作原理	適用於
外部磁碟區或資料儲存加密	如果您的部署平台支持，您可以使用StorageGRID以外的加密方法來加密整個磁碟區或資料儲存。	所有物件資料、元資料和系統配置資料（假設每個磁碟區或資料儲存都經過加密）。 外部加密方法可以對加密演算法和金鑰進行更嚴格的控制。可以與列出的其他方法結合使用。
StorageGRID以外的物件加密	您可以使用StorageGRID外部的加密方法在物件資料和元資料被匯入StorageGRID之前對其進行加密。	僅物件資料和元資料（系統配置資料未加密）。 外部加密方法可以對加密演算法和金鑰進行更嚴格的控制。可以與列出的其他方法結合使用。 "Amazon Simple Storage Service - 使用者指南：使用客戶端加密保護資料"

使用多種加密方法

根據您的要求，您可以一次使用多種加密方法。例如：

- 您可以使用 KMS 來保護裝置節點，也可以使用SANtricity System Manager 中的磁碟機安全功能對同一裝置中自加密磁碟機上的資料進行「雙重加密」。
- 您可以使用 KMS 來保護裝置節點上的數據，也可以使用儲存物件加密選項在提取所有物件時進行加密。

如果只有一小部分物件需要加密，請考慮在儲存桶或單一物件層級控制加密。啟用多層加密會產生額外的效能成本。

管理證書

管理安全證書

安全性憑證是用於在StorageGRID組件之間以及StorageGRID組件與外部系統之間建立安全、可信任連接的小型資料檔案。

StorageGRID使用兩種類型的安全性憑證：

- 使用 HTTPS 連線時需要*伺服器憑證*。伺服器憑證用於在客戶端和伺服器之間建立安全連接，向客戶端驗證伺服器的身份並為資料提供安全通訊路徑。伺服器和客戶端各自擁有一份憑證副本。
- *用戶端憑證*向伺服器驗證用戶端或使用者身份，提供比單獨使用密碼更安全的身份驗證。客戶端證書不加密資料。

當客戶端使用 HTTPS 連接到伺服器時，伺服器會使用包含公鑰的伺服器憑證進行回應。用戶端透過將伺服器簽章與其憑證副本上的簽章進行比較來驗證此憑證。如果簽章匹配，客戶端將使用相同的公鑰與伺服器開始會話。

StorageGRID可作為某些連線（例如負載平衡器端點）的伺服器，或充當其他連線（例如 CloudMirror 複製服務

）的用戶端。

預設網格 **CA** 憑證

StorageGRID包括一個內建憑證授權單位 (CA)，它在系統安裝期間產生內部 Grid CA 憑證。預設情況下，使用 Grid CA 憑證來保護內部StorageGRID流量。外部憑證授權單位 (CA) 可以頒發完全符合您組織的資訊安全策略的自訂憑證。雖然您可以在非生產環境中使用 Grid CA 證書，但生產環境的最佳做法是使用外部憑證授權單位簽署的自訂憑證。也支援沒有證書的不安全連接，但不建議。

- 自訂 CA 憑證不會刪除內部憑證；但是，自訂憑證應該是用於驗證伺服器連線的憑證。
- 所有客製化證書必須滿足"伺服器證書的系統強化指南"。
- StorageGRID支援將來自 CA 的憑證捆綁到單一檔案中（稱為 CA 憑證包）。

> StorageGRID還包括所有網格上相同的作業系統 CA 憑證。在生產環境中，請確保指定由外部憑證授權單位簽署的自訂憑證來取代作業系統 CA 憑證。

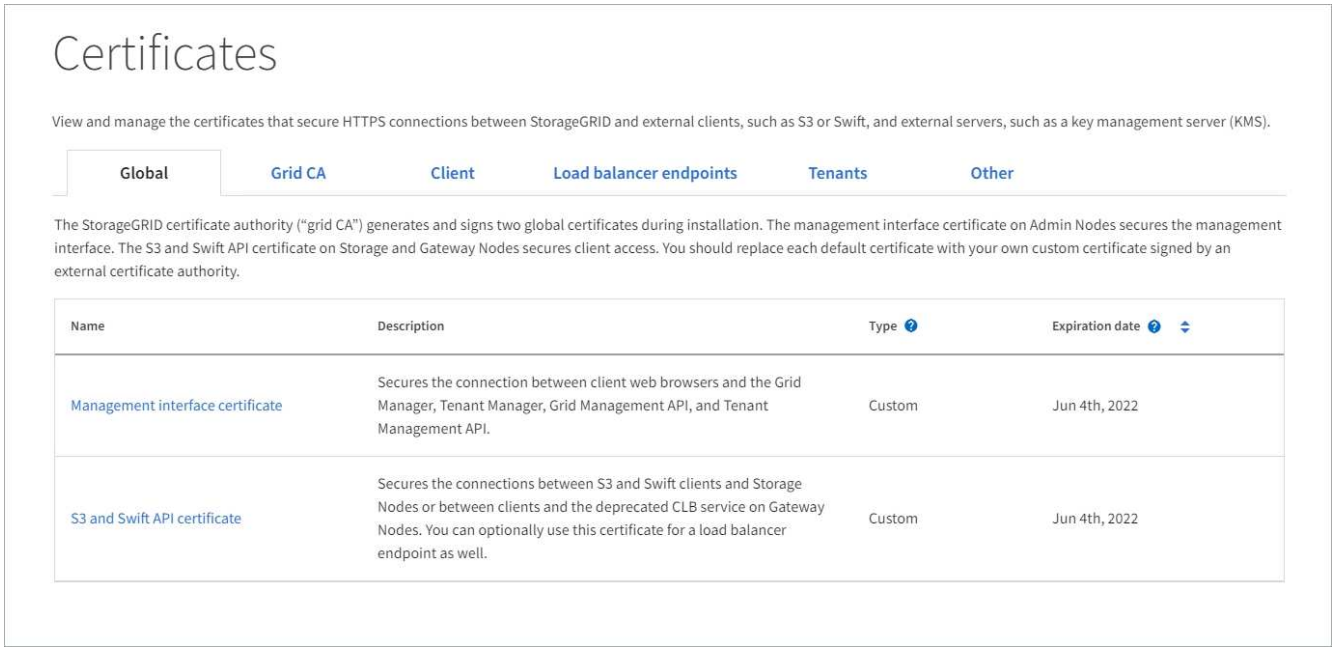
伺服器和客戶端憑證類型的變體以多種方式實現。在配置系統之前，您應該準備好特定StorageGRID配置所需的所有憑證。

存取安全憑證

您可以在單一位置存取有關所有StorageGRID憑證的信息，以及每個憑證的設定工作流程的連結。

步驟

1. 從網格管理器中，選擇 配置 > 安全性 > 證書。



2. 選擇「證書」頁面上的標籤以取得有關每個證書類別的資訊並存取證書設定。如果您有"適當的許可"。
   - 全域：保護從 Web 瀏覽器和外部 API 用戶端存取StorageGRID 的安全性。
   - **Grid CA**：保護內部StorageGRID流量。
   - 客戶端：保護外部客戶端和StorageGRID Prometheus 資料庫之間的連線。

- 負載平衡器端點：保護 S3 用戶端與StorageGRID負載平衡器之間的連線。
- 租用戶：保護與身分識別聯合伺服器或從平台服務端點到 S3 儲存資源的連線。
- 其他：保護需要特定憑證的StorageGRID連線。

  下面描述了每個選項卡，並提供了指向其他證書詳細資訊的連結。

全球的

全域憑證可確保從 Web 瀏覽器和外部 S3 API 用戶端存取StorageGRID 的安全性。在安裝過程中，StorageGRID憑證授權單位最初會產生兩個全域憑證。生產環境的最佳實踐是使用由外部憑證授權單位簽署的自訂憑證。

- [管理介面證書]：保護客戶端 Web 瀏覽器與StorageGRID管理介面的連線。
- S3 API 證書：保護客戶端 API 與儲存節點、管理節點和網關節點的連接，S3 用戶端應用程式使用這些連接上傳和下載物件資料。

有關已安裝的全域憑證的資訊包括：

- 名稱：證書名稱以及證書管理連結。
- 描述
- 類型：自訂或預設。 + 您應該始終使用自訂憑證來提高電網安全性。
- 到期日：如果使用預設證書，則不顯示到期日。

你可以：

- 將預設證書取代為由外部證書頒發機構簽署的自訂證書，以提高網格安全性：
  - "取代預設的StorageGRID產生的管理介面證書"用於網格管理器和租戶管理器連線。
  - "替換 S3 API 證書"用於儲存節點和負載平衡器端點（可選）連線。
- "恢復預設管理介面證書" 。
- "恢復預設的 S3 API 證書" 。
- "使用腳本產生新的自簽名管理介面證書" 。
- 複製或下載"管理介面證書"或者"S3 API 證書"。

網格**CA**

這網格CA證書由StorageGRID憑證授權單位在StorageGRID安裝期間生成，可保護所有內部StorageGRID流量。

證書資訊包括證書有效期限、證書內容等。

你可以"複製或下載 Grid CA 憑證"，但您無法更改它。

用戶端

客戶端憑證由外部憑證授權單位生成，確保外部監控工具與StorageGRID Prometheus 資料庫之間的連線安全。

證書表為每個配置的用戶端證書都有一行，並指示該證書是否可用於 Prometheus 資料庫訪問，以及證書到期日。

你可以：

- "上傳或產生新的客戶端憑證。"
- 選擇證書名稱以顯示證書詳細信息，您可以在其中：

- "更改客戶端證書名稱。"
- "設定Prometheus存取權限。"
- "上傳並替換客戶端憑證。"
- "複製或下載客戶端憑證。"
- "刪除客戶端證書。"

◦ 選擇*操作*快速"編輯"，"附" ， 或者"消除"客戶端證書。您最多可以選擇 10 個客戶端證書，並使用操作 > 刪除 一次將其刪除。

負載平衡器端點

負載平衡器端點憑證保護 S3 用戶端與網關節點和管理節點上的StorageGRID負載平衡器服務之間的連線。

負載平衡器端點表為每個配置的負載平衡器端點都有一行，並指示該端點是否使用全域 S3 API 憑證或自訂負載平衡器端點憑證。也會顯示每個憑證的到期日期。

端點憑證的變更可能需要長達 15 分鐘才能套用到所有節點。

你可以：

◦ "查看負載平衡器端點"，包括其證書詳細資訊。

◦ "為FabricPool指定負載平衡器端點憑證。"

◦ "使用全域 S3 API 證書"而不是產生新的負載平衡器端點憑證。

租戶

租戶可以使用身份聯合伺服器憑證或者平台服務端點憑證以確保與StorageGRID 的連線安全。

租戶表為每個租戶分配一行，並指示每個租戶是否有權使用自己的身份來源或平台服務。

你可以：

◦ "選擇租戶名稱以登入租戶管理器"

◦ "選擇租戶名稱以查看租戶身份聯合詳細信息"

◦ "選擇租戶名稱查看租戶平台服務詳情"

◦ "在端點建立期間指定平台服務端點憑證"

其他

StorageGRID使用其他安全性憑證來達到特定目的。這些證書按其功能名稱列出。其他安全性憑證包括：

◦ 雲端儲存池憑證

◦ 電子郵件警報通知證書

◦ 外部系統日誌伺服器證書

◦ 電網聯合連接證書

◦ 身分聯合憑證

- 金鑰管理伺服器 (KMS) 證書
- 單一登入憑證

資訊指示功能使用的憑證類型及其伺服器和用戶端憑證到期日期（如適用）。選擇函數名稱將開啟一個瀏覽器選項卡，您可以在其中查看和編輯憑證詳細資訊。

僅當您擁有"適當的許可"。

你可以：

- "為 S3、C2S S3 或 Azure 指定雲端儲存池憑證"
- "指定警報電子郵件通知的證書"
- "使用外部系統日誌伺服器的證書"
- "輪換電網聯合連接證書"
- "查看並編輯身份聯合證書"
- "上傳金鑰管理伺服器 (KMS) 伺服器和用戶端證書"
- "為信賴方信任手動指定 SSO 證書"

安全證書詳細信息

以下描述了每種類型的安全證書，並附有實施說明的連結。

管理介面證書

證書類型	描述	導航位置	細節
伺服器	驗證用戶端 Web 瀏覽器與StorageGRID管理介面之間的連接，允許使用者存取網格管理器和租用戶管理器而不會出現安全警告。 此憑證還驗證網格管理 API 和租用戶管理 API 連線。 您可以使用安裝期間建立的預設憑證或上傳自訂憑證。	設定 > 安全 > 憑證，選擇 全域 選項卡，然後選擇 管理介面憑證	"設定管理介面證書"

S3 API 證書

證書類型	描述	導航位置	細節
伺服器	驗證與儲存節點和負載平衡器端點的安全 S3 用戶端連線（可選）。	設定 > 安全 > 憑證，選擇 全域 選項卡，然後選擇 **S3 API** 憑證	"配置 S3 API 證書"

網格**CA**證書

查看預設網格 CA 憑證描述。

管理員客戶端憑證

證書類型	描述	導航位置	細節
用戶端	安裝在每個客戶端上，允許StorageGRID驗證外部客戶端存取。 • 允許授權的外部用戶端存取StorageGRID Prometheus 資料庫。 • 允許使用外部工具對StorageGRID進行安全監控。	配置 > 安全性 > 憑證，然後選擇 用戶端 選項卡	"設定客戶端證書"

負載平衡器端點憑證

證書類型	描述	導航位置	細節
伺服器	驗證 S3 用戶端與網關節點和管理節點上的StorageGRID負載平衡器服務之間的連線。您可以在設定負載平衡器端點時上傳或產生負載平衡器憑證。用戶端應用程式在連接到StorageGRID以儲存和檢索物件資料時使用負載平衡器憑證。 您也可以使用全域的自訂版本S3 API 證書憑證來驗證與負載平衡器服務的連線。如果使用全域憑證來驗證負載平衡器連接，則無需為每個負載平衡器端點上傳或產生單獨的憑證。 *注意：*用於負載平衡器驗證的憑證是正常StorageGRID作業期間使用最多的憑證。	配置 > 網路 > 負載平衡器端點	• "配置負載平衡器端點" • "為FabricPool建立負載平衡器端點"

雲端儲存池端點憑證

證書類型	描述	導航位置	細節
伺服器	驗證從StorageGRID雲端儲存池到外部儲存位置（例如 S3 Glacier 或 Microsoft Azure Blob 儲存體）的連線。每種雲端提供者類型都需要不同的憑證。	**ILM** > 儲存池	"建立雲端儲存池"

電子郵件警報通知證書

證書類型	描述	導航位置	細節
伺服器和客戶端	驗證用於警報通知的SMTP 電子郵件伺服器和StorageGRID之間的連線。 • 如果與 SMTP 伺服器的通訊需要傳輸層安全性 (TLS)，則必須指定電子郵件伺服器 CA 憑證。 • 僅當 SMTP 電子郵件伺服器需要用戶端憑證進行驗證時才指定用戶端憑證。	警報 > 電子郵件設定	"設定警報的電子郵件通知"

外部系統日誌伺服器證書

證書類型	描述	導航位置	細節
伺服器	對在StorageGRID中記錄事件的外部系統日誌伺服器之間的 TLS 或 RELP/TLS 連線進行驗證。 *注意：*與外部系統日誌伺服器的 TCP 、RELP/TCP 和 UDP 連線不需要外部系統日誌伺服器憑證。	配置 > 監控 > 審計和系統日誌伺服器	"使用外部系統日誌伺服器"

電網聯合連接憑證

證書類型	描述	導航位置	細節
伺服器和客戶端	對目前StorageGRID系統和網格聯合連接中的另一個網格之間所傳送的資訊進行驗證和加密。	配置 > 系統 > 網格聯合	• "建立電網聯合連接" • "輪換連接證書"

身分聯合憑證

證書類型	描述	導航位置	細節
伺服器	驗證StorageGRID與外部身分提供者（例如 Active Directory、OpenLDAP 或 Oracle Directory Server）之間的連線。用於身分聯合，允許管理群組和使用者由外部系統管理。	配置 > 存取控制 > 身份聯合	"使用身分聯合"

金鑰管理伺服器 **(KMS)** 證書

證書類型	描述	導航位置	細節
伺服器和客戶端	驗證StorageGRID與外部金鑰管理伺服器 (KMS) 之間的連接，該伺服器為StorageGRID設備節點提供加密金鑰。	配置 > 安全 > 金鑰管理伺服器	"新增金鑰管理伺服器（KMS）"

平台服務端點憑證

證書類型	描述	導航位置	細節
伺服器	驗證從StorageGRID平台服務到 S3 儲存資源的連線。	租用戶管理員 > 儲存 **(S3)** > 平台服務端點	"創建平台服務端點" "編輯平台服務端點"

單一登入 **(SSO)** 證書

證書類型	描述	導航位置	細節
伺服器	驗證用於單一登入 (SSO) 請求的身份聯合服務（例如 Active Directory 聯合驗證服務 (AD FS)）和StorageGRID之間的連線。	配置 > 存取控制 > 單一登入	"配置單一登入"

證書範例

範例 **1**：負載平衡器服務

在此範例中， StorageGRID充當伺服器。

1. 您設定負載平衡器端點並在StorageGRID中上傳或產生伺服器憑證。
2. 您配置與負載平衡器端點的 S3 用戶端連接，並將相同的憑證上傳到用戶端。
3. 當客戶端想要儲存或檢索資料時，它使用 HTTPS 連接到負載平衡器端點。

4. StorageGRID使用包含公鑰的伺服器憑證和基於私密金鑰的簽章進行回應。
5. 用戶端透過將伺服器簽章與其憑證副本上的簽章進行比較來驗證此憑證。如果簽章匹配，客戶端將使用相同的公鑰開始會話。
6. 客戶端將物件資料傳送到StorageGRID。

範例 **2**：外部金鑰管理伺服器 **(KMS)**

在此範例中， StorageGRID充當用戶端。

1. 使用外部金鑰管理伺服器軟體，您可以將StorageGRID設定為 KMS 用戶端並取得 CA 簽署的伺服器憑證、公用用戶端憑證以及用戶端憑證的私密金鑰。
2. 使用網格管理器，您可以設定 KMS 伺服器並上傳伺服器和用戶端憑證以及用戶端私鑰。
3. 當StorageGRID節點需要加密金鑰時，它會向 KMS 伺服器發出請求，其中包含來自憑證的資料和基於私密金鑰的簽章。
4. KMS 伺服器驗證憑證簽章並決定它可以信任StorageGRID。
5. KMS 伺服器使用已驗證的連線進行回應。

支援的伺服器憑證類型

StorageGRID系統支援使用 RSA 或 ECDSA（橢圓曲線數位簽章演算法）加密的自訂憑證。

安全性原則的密碼類型必須與伺服器憑證類型相符。例如，RSA 密碼需要 RSA 證書，ECDSA 密碼需要 ECDSA 證書。看"管理安全證書" 。如果您配置了與伺服器憑證不相容的自訂安全性原則，您可以"暫時恢復預設安全策略"。

有關StorageGRID如何保護客戶端連接的更多信息，請參閱"S3 用戶端的安全性"。

設定管理介面證書

您可以用單一自訂證書取代預設管理介面證書，該證書允許使用者存取網格管理器和租戶管理器而不會遇到安全警告。您也可以還原預設管理介面憑證或產生新的憑證。

關於此任務

預設情況下，每個管理節點都會頒發由網格 CA 簽署的憑證。這些 CA 簽署的憑證可以被單一通用自訂管理介面憑證和對應的私鑰所取代。

由於所有管理節點都使用單一自訂管理介面證書，因此如果用戶端在連接到網格管理器和租用戶管理器時需要驗證主機名，則必須將證書指定為通配符或多網域證書。定義自訂證書，使其與網格中的所有管理節點相符。

您需要在伺服器上完成配置，並且根據您使用的根憑證授權單位 (CA)，使用者可能還需要在用於存取網格管理員和租用戶管理員的 Web 瀏覽器中安裝網格 CA 憑證。

為了確保操作不會因伺服器憑證失敗而中斷，當此伺服器憑證即將過期時，會觸發*管理介面伺服器憑證過期*警報。根據需要，您可以透過選擇 **CONFIGURATION** > **Security** > **Certificates** 並查看 Global 標籤上的管理介面憑證的到期日期來查看目前憑證的到期時間。

如果您使用網域名稱而不是 IP 位址存取網格管理員或租用戶管理器，則在發生下列任一情況時，瀏覽器將顯示憑證錯誤，且沒有繞過選項：

- 您的自訂管理介面憑證已過期。
- 你從自訂管理介面證書恢復為預設伺服器憑證。

新增自訂管理介面證書

若要新增自訂管理介面證書，您可以提供自己的證書或使用網格管理器產生證書。

步驟

1. 選擇 設定 > 安全 > 憑證。
2. 在*全域*標籤上，選擇*管理介面憑證*。
3. 選擇*使用自訂憑證*。
4. 上傳或產生證書。

上傳證書

上傳所需的伺服器憑證檔案。

a. 選擇*上傳證書*。

b. 上傳所需的伺服器憑證檔案：

   - 伺服器憑證：自訂伺服器憑證檔案（PEM編碼）。
   - 證書私鑰：自訂伺服器憑證私鑰文件(`.key`）。

     EC 私鑰必須為 224 位元或更大。 RSA 私鑰必須為 2048 位元或更大。

   - **CA** 包：一個可選文件，包含來自每個中間發行憑證機構 (CA) 的憑證。該文件應包含每個 PEM 編碼的 CA 憑證文件，並按憑證鏈順序連接。

c. 展開*證書詳細資訊*以查看您上傳的每個證書的元資料。如果您上傳了可選的 CA 包，則每個憑證都會顯示在其自己的標籤上。

   - 選擇*下載憑證*儲存憑證檔案或選擇*下載 CA 套件*儲存憑證套件。

     指定證書檔案名稱和下載位置。使用副檔名儲存檔案 `.pem`。

   例如： `storagegrid_certificate.pem`

   - 選擇*複製憑證 PEM*或*複製 CA 套件 PEM*以複製憑證內容以便貼上到其他地方。

d. 選擇*儲存*。+ 自訂管理介面憑證用於與網格管理器、租用戶管理員、網格管理器 API 或租用戶管理器 API 的所有後續新連接。

產生證書

產生伺服器憑證檔案。

生產環境的最佳實務是使用由外部憑證授權單位簽署的自訂管理介面憑證。

a. 選擇*產生證書*。

b. 指定證書資訊：

場地	描述
網域	證書中包含的一個或多個完全限定域名。使用 * 作為通配符來表示多個網域。
智慧財產	證書中包含的一個或多個 IP 位址。
主題（可選）	證書擁有者的 X.509 主題或專有名稱 (DN)。 如果此欄位未輸入任何值，則產生的憑證將使用第一個網域名稱或 IP 位址作為主題通用名稱 (CN)。

場地	描述
有效天數	證書建立後過期的天數。
新增密鑰使用擴展	如果選擇（預設和推薦），密鑰使用和擴展密鑰使用擴充將新增至產生的憑證。 這些擴充定義了憑證中包含的金鑰的用途。 注意：請選取此複選框，除非當憑證包含這些擴充功能時您遇到與舊用戶端的連線問題。

c. 選擇*生成*。

d. 選擇*證書詳細資訊*以查看產生的證書的元資料。

- 選擇*下載證書*儲存證書檔案。

  指定證書檔案名稱和下載位置。使用副檔名儲存檔案 `.pem`。

  例如： `storagegrid_certificate.pem`

- 選擇*複製證書 PEM* 以複製證書內容並貼上到其他地方。

e. 選擇*儲存*。+ 自訂管理介面憑證用於與網格管理器、租用戶管理員、網格管理器 API 或租用戶管理器 API 的所有後續新連接。

5. 重新整理頁面以確保 Web 瀏覽器已更新。

> 上傳或產生新證書後，請等待最多一天的時間以清除所有相關的證書到期警報。

6. 新增自訂管理介面憑證後，管理介面憑證頁面將顯示正在使用的憑證的詳細憑證資訊。 +您可以根據需要下載或複製憑證PEM。

恢復預設管理介面證書

您可以還原使用網格管理器和租用戶管理器連線的預設管理介面憑證。

步驟

1. 選擇 設定 > 安全 > 憑證。
2. 在*全域*標籤上，選擇*管理介面憑證*。
3. 選擇*使用預設證書*。

   當您還原預設管理介面憑證時，您設定的自訂伺服器憑證檔案將會被刪除，並且無法從系統中復原。所有後續的新用戶端連線均使用預設管理介面憑證。

4. 重新整理頁面以確保 Web 瀏覽器已更新。

使用腳本產生新的自簽名管理介面證書

如果需要嚴格的主機名稱驗證，您可以使用腳本產生管理介面憑證。

開始之前

- 你有"特定存取權限"。
- 你有 `Passwords.txt`文件。

關於此任務

生產環境的最佳實務是使用由外部憑證授權單位簽署的憑證。

步驟

1. 取得每個管理節點的完全限定網域名稱 (FQDN)。
2. 登入主管理節點：
   a. 輸入以下命令： `ssh admin@primary_Admin_Node_IP`
   b. 輸入 `Passwords.txt`文件。
   c. 輸入以下命令切換到root： `su -`
   d. 輸入 `Passwords.txt`文件。

   當您以 root 身分登入時，提示字元將從 `$`到 `#`。
3. 使用新的自簽章憑證設定StorageGRID 。

   ```
   $ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
   ```

   - 為了 `--domains`，使用通配符來表示所有管理節點的完全限定網域名稱。例如， `*.ui.storagegrid.example.com`使用 `*` 通配符來表示 `admin1.ui.storagegrid.example.com`和 `admin2.ui.storagegrid.example.com`。
   - 放 `--type`到 `management`配置管理介面證書，供Grid Manager和Tenant Manager使用。
   - 預設情況下，產生的憑證有效期為一年（365 天），必須在到期前重新建立。您可以使用 `--days`參數來覆蓋預設有效期。

     > 證書有效期限從 `make-certificate`正在運行。您必須確保管理用戶端與StorageGRID同步到相同時間來源；否則，用戶端可能會拒絕該憑證。

     ```
     $ sudo make-certificate --domains *.ui.storagegrid.example.com --type management --days 720
     ```

     結果輸出包含管理 API 用戶端所需的公共憑證。
4. 選擇並複製證書。

   在您的選擇中包含 BEGIN 和 END 標籤。
5. 退出命令 shell。 `$ exit`

6. 確認證書已設定：
   a. 存取網格管理器。
   b. 選擇 設定 > 安全 > 憑證
   c. 在*全域*標籤上，選擇*管理介面憑證*。
7. 配置您的管理用戶端以使用您複製的公共憑證。包括 BEGIN 和 END 標籤。

下載或複製管理介面證書

您可以儲存或複製管理介面證書內容以供其他地方使用。

步驟

1. 選擇 設定 > 安全 > 憑證。
2. 在*全域*標籤上，選擇*管理介面憑證*。
3. 選擇“伺服器”或“**CA** 套件”選項卡，然後下載或複製憑證。

下載憑證檔案或 **CA** 套件

下載憑證或 CA 套件 `.pem`文件。如果您使用可選的 CA 捆綁包，捆綁包中的每個憑證都會顯示在其自己的子選項卡上。

a. 選擇*下載憑證*或*下載 CA 套件*。

   如果您正在下載 CA 捆綁包，則 CA 捆綁包二級標籤中的所有憑證都會作為單一檔案下載。

b. 指定證書檔案名稱和下載位置。使用副檔名儲存檔案 `.pem`。

   例如： `storagegrid_certificate.pem`

複製憑證或 **CA** 捆綁包 **PEM**

複製證書文字並貼上到其他地方。如果您使用可選的 CA 捆綁包，捆綁包中的每個憑證都會顯示在其自己的子選項卡上。

a. 選擇*複製憑證 PEM*或*複製 CA 套件 PEM*。

   如果您正在複製 CA 捆綁包，則 CA 捆綁包輔助標籤中的所有憑證都會一起複製。

b. 將複製的憑證貼到文字編輯器中。
c. 儲存帶有擴展名的文字文件 `.pem`。

   例如： `storagegrid_certificate.pem`

配置 **S3 API** 證書

您可以替換或還原用於 S3 用戶端連接到儲存節點或負載平衡器端點的伺服器憑證。替換的自訂伺服器憑證特定於您的組織。

此版本的文件網站已刪除 Swift 詳細資訊。看 "StorageGRID 11.8：設定 S3 和 Swift API 證書"。

關於此任務

預設情況下，每個儲存節點都會頒發由網格 CA 簽署的 X.509 伺服器憑證。這些 CA 簽署的憑證可以被單一通用自訂伺服器憑證和相應的私鑰所取代。

所有儲存節點都使用單一自訂伺服器證書，因此如果用戶端在連接到儲存端點時需要驗證主機名，則必須將證書指定為通配符或多網域證書。定義自訂證書，使其與網格中的所有儲存節點相符。

在伺服器上完成設定後，您可能還需要在用於存取系統的 S3 API 用戶端中安裝 Grid CA 證書，具體取決於您使用的根憑證授權單位 (CA)。

為了確保操作不會因伺服器憑證失敗而中斷，當根伺服器憑證即將過期時，會觸發*S3 API 的全域伺服器憑證過期*警報。根據需要，您可以透過選擇 **CONFIGURATION** > **Security** > **Certificates** 並查看 Global 標籤上 S3 API 憑證的到期日期來查看目前憑證的到期時間。

您可以上傳或產生自訂 S3 API 憑證。

新增自訂 **S3 API** 證書

步驟

1. 選擇 設定 > 安全 > 憑證。
2. 在*全域*標籤上，選擇*S3 API 憑證*。
3. 選擇*使用自訂憑證*。
4. 上傳或產生證書。

上傳證書

上傳所需的伺服器憑證檔案。

a. 選擇*上傳證書*。

b. 上傳所需的伺服器憑證檔案：

- 伺服器憑證：自訂伺服器憑證檔案（PEM編碼）。
- 證書私鑰：自訂伺服器憑證私鑰文件(`.key`）。

> EC 私鑰必須為 224 位元或更大。 RSA 私鑰必須為 2048 位元或更大。

- **CA** 包：一個可選文件，包含來自每個中間頒發憑證機構的憑證。該文件應包含每個 PEM 編碼的 CA 憑證文件，並按憑證鏈順序連接。

c. 選擇憑證詳細資訊以顯示已上傳的每個自訂 S3 API 憑證的元資料和 PEM。如果您上傳了可選的 CA 包，則每個憑證都會顯示在其自己的標籤上。

- 選擇*下載憑證*儲存憑證檔案或選擇*下載 CA 套件*儲存憑證套件。

  指定證書檔案名稱和下載位置。使用副檔名儲存檔案 `.pem`。

  例如： `storagegrid_certificate.pem`

- 選擇*複製憑證 PEM*或*複製 CA 套件 PEM*以複製憑證內容以便貼上到其他地方。

d. 選擇*儲存*。

自訂伺服器憑證用於後續新的 S3 用戶端連線。

產生證書

產生伺服器憑證檔案。

a. 選擇*產生證書*。

b. 指定證書資訊：

場地	描述
網域	證書中包含的一個或多個完全限定域名。使用 * 作為通配符來表示多個網域。
智慧財產	證書中包含的一個或多個 IP 位址。
主題（可選）	證書擁有者的 X.509 主題或專有名稱 (DN)。 如果此欄位未輸入任何值，則產生的憑證將使用第一個網域名稱或 IP 位址作為主題通用名稱 (CN)。
有效天數	證書建立後過期的天數。

場地	描述
新增密鑰使用擴展	如果選擇（預設和推薦），密鑰使用和擴展密鑰使用擴充將新增至產生的憑證。 這些擴充定義了憑證中包含的金鑰的用途。 注意：請選取此複選框，除非當憑證包含這些擴充功能時您遇到與舊用戶端的連線問題。

c. 選擇*生成*。

d. 選擇*證書詳細資訊*以顯示產生的自訂 S3 API 證書的元資料和 PEM。

- 選擇*下載證書*儲存證書檔案。

  指定證書檔案名稱和下載位置。使用副檔名儲存檔案 `.pem`。

  例如： `storagegrid_certificate.pem`

- 選擇*複製證書 PEM* 以複製證書內容並貼上到其他地方。

e. 選擇*儲存*。

自訂伺服器憑證用於後續新的 S3 用戶端連線。

5. 選擇一個標籤以顯示預設StorageGRID伺服器憑證、已上傳的 CA 簽章憑證或產生的自訂憑證的元資料。

   上傳或產生新證書後，請等待最多一天的時間以清除所有相關的證書到期警報。

6. 重新整理頁面以確保 Web 瀏覽器已更新。

7. 新增自訂 S3 API 憑證後，S3 API 憑證頁面將顯示正在使用的自訂 S3 API 憑證的詳細憑證資訊。 +您可以根據需要下載或複製憑證PEM。

恢復預設的 **S3 API** 證書

您可以恢復使用預設 S3 API 憑證來將 S3 用戶端連接到儲存節點。但是，您不能將預設的 S3 API 憑證用於負載平衡器端點。

步驟

1. 選擇 設定 > 安全 > 憑證。
2. 在*全域*標籤上，選擇*S3 API 憑證*。
3. 選擇*使用預設證書*。

   當您還原全域 S3 API 憑證的預設版本時，您設定的自訂伺服器憑證檔案將會被刪除，並且無法從系統中復原。預設 S3 API 憑證將用於後續新的 S3 用戶端與儲存節點的連接。

4. 選擇「確定」確認警告並恢復預設的 S3 API 憑證。

如果您具有 Root 存取權限，並且自訂 S3 API 憑證用於負載平衡器端點連接，則會顯示負載平衡器端點列表，這些端點將無法再使用預設 S3 API 憑證進行存取。前往"配置負載平衡器端點"編輯或刪除受影響的端點。

5. 重新整理頁面以確保 Web 瀏覽器已更新。

下載或複製 **S3 API** 證書

您可以儲存或複製 S3 API 憑證內容以供在其他地方使用。

步驟

1. 選擇 設定 > 安全 > 憑證。
2. 在*全域*標籤上，選擇*S3 API 憑證*。
3. 選擇"伺服器"或"**CA** 套件"選項卡，然後下載或複製憑證。

下載憑證檔案或 **CA** 套件

下載憑證或 CA 套件 `.pem`文件。如果您使用可選的 CA 捆綁包，捆綁包中的每個憑證都會顯示在其自己的子選項卡上。

a. 選擇*下載憑證*或*下載 CA 套件*。

   如果您正在下載 CA 捆綁包，則 CA 捆綁包二級標籤中的所有憑證都會作為單一檔案下載。

b. 指定證書檔案名稱和下載位置。使用副檔名儲存檔案 `.pem`。

   例如： `storagegrid_certificate.pem`

複製憑證或 **CA** 捆綁包 **PEM**

複製證書文字並貼上到其他地方。如果您使用可選的 CA 捆綁包，捆綁包中的每個憑證都會顯示在其自己的子選項卡上。

a. 選擇*複製憑證 PEM*或*複製 CA 套件 PEM*。

   如果您正在複製 CA 捆綁包，則 CA 捆綁包輔助標籤中的所有憑證都會一起複製。

b. 將複製的憑證貼到文字編輯器中。

c. 儲存帶有擴展名的文字文件 `.pem`。

   例如： `storagegrid_certificate.pem`

相關資訊

- "使用 S3 REST API"
- "配置 S3 端點域名"

複製網格 **CA** 證書

StorageGRID使用內部憑證授權單位 (CA) 來保護內部流量。如果您上傳自己的證書，此證書不會改變。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"特定存取權限"。

關於此任務

如果已配置自訂伺服器證書，則用戶端應用程式應使用自訂伺服器證書來驗證伺服器。他們不應該從StorageGRID系統複製 CA 憑證。

步驟

1. 選擇 **CONFIGURATION** > **Security** > **Certificates**，然後選擇 **Grid CA** 選項卡。
2. 在 證書 **PEM** 部分，下載或複製證書。

   下載證書文件

   下載證書 `.pem`文件。

   a. 選擇*下載證書*。

   b. 指定證書檔案名稱和下載位置。使用副檔名儲存檔案 `.pem`。

      例如： `storagegrid_certificate.pem`

   複製證書 **PEM**

   複製證書文字並貼上到其他地方。

   a. 選擇*複製憑證 PEM*。

   b. 將複製的憑證貼到文字編輯器中。

   c. 儲存帶有擴展名的文字文件 `.pem`。

      例如： `storagegrid_certificate.pem`

為**FabricPool**配置**StorageGRID**證書

對於執行嚴格主機名稱驗證且不支援停用嚴格主機名稱驗證的 S3 用戶端（例如使用FabricPool的ONTAP用戶端），您可以在設定負載平衡器端點時產生或上傳伺服器憑證。

開始之前

- 你有"特定存取權限"。
- 您已使用"支援的網頁瀏覽器"。

關於此任務

建立負載平衡器端點時，您可以產生自簽章伺服器憑證或上傳已知憑證授權單位 (CA) 簽署的憑證。在生產環境中，您應該使用已知 CA 簽署的憑證。由 CA 簽署的憑證可以不間斷地輪替。它們也更安全，因為它們可以更好地防禦中間人攻擊。

以下步驟為使用FabricPool的 S3 用戶端提供了一般準則。如需更多詳細資訊和步驟，請參閱"為FabricPool配置StorageGRID"。

步驟

1. 或者，配置一個高可用性 (HA) 群組供FabricPool使用。
2. 建立一個 S3 負載平衡器端點供FabricPool使用。

   當您建立 HTTPS 負載平衡器端點時，系統會提示您上傳伺服器憑證、憑證私鑰和選用 CA 套件。

3. 將StorageGRID作為雲層附加到ONTAP。

   指定您上傳的 CA 憑證中所使用的負載平衡器端點連接埠和完全限定網域名稱。然後，提供 CA 憑證。

   如果中間 CA 頒發了StorageGRID證書，則必須提供中間 CA 證書。如果StorageGRID憑證是由根 CA 直接頒發的，則必須提供根 CA 憑證。

設定客戶端證書

用戶端憑證允許授權的外部用戶端存取StorageGRID Prometheus 資料庫，為外部工具監控StorageGRID提供一種安全的方式。

如果需要使用外部監控工具存取StorageGRID ，則必須使用 Grid Manager 上傳或產生用戶端證書，並將證書資訊複製到外部工具。

看"管理安全證書"和"配置自訂伺服器證書"。

為了確保操作不會因伺服器憑證失敗而中斷，當此伺服器憑證即將過期時，將觸發*憑證頁面上配置的用戶端憑證過期*警報。根據需要，您可以透過選擇 設定 > 安全 > 憑證 並查看用戶端標籤上的用戶端憑證的到期日期來查看目前憑證的到期時間。

如果您使用金鑰管理伺服器 (KMS) 來保護特殊配置的設備節點上的數據，請參閱有關"上傳 KMS 用戶端證書"。

開始之前

- 您擁有 Root 存取權限。
- 您已使用"支援的網頁瀏覽器"。
- 要設定客戶端憑證：
  - 您擁有管理節點的 IP 位址或網域名稱。
  - 如果您已設定StorageGRID管理介面證書，則您擁有用於設定管理介面憑證的 CA、用戶端憑證和私密金鑰。
  - 要上傳您自己的證書，該證書的私鑰可以在您的本機電腦上找到。

- 私鑰在創建時必須被保存或記錄。如果您沒有原始私鑰，則必須建立一個新的私鑰。

- 若要編輯客戶端憑證：
  - 您擁有管理節點的 IP 位址或網域名稱。
  - 要上傳您自己的證書或新證書，您的本機電腦上需要有私鑰、用戶端證書和 CA（如果使用）。

新增客戶端證書

若要新增客戶端證書，請使用下列步驟之一：

- [管理介面憑證已配置]
- CA核發的客戶端證書
- [從網格管理器產生的證書]

管理介面憑證已配置

如果已使用客戶提供的 CA、用戶端證書和私鑰配置了管理介面證書，請使用此程序新增用戶端證書。

步驟

1. 在網格管理員中，選擇 配置 > 安全性 > 憑證，然後選擇 用戶端 標籤。
2. 選擇“新增”。
3. 輸入證書名稱。
4. 若要使用外部監控工具存取 Prometheus 指標，請選擇 允許 **prometheus**。
5. 選擇*繼續*。
6. 對於*附加憑證*步驟，上傳管理介面憑證。
   a. 選擇*上傳證書*。
   b. 選擇*瀏覽*並選擇管理介面憑證文件(`.pem`）。
      - 選擇*用戶端憑證詳細資料*以顯示憑證元資料和憑證 PEM。
      - 選擇*複製證書 PEM* 以複製證書內容並貼上到其他地方。
   c. 選擇*建立*將憑證保存在網格管理員中。

      新證書出現在客戶端選項卡上。
7. 設定外部監控工具，例如 Grafana。

CA核發的客戶端證書

如果未設定管理介面證書，且您計劃為 Prometheus 新增使用 CA 頒發的用戶端憑證和私鑰的用戶端證書，請使用此流程新增管理員用戶端憑證。

步驟

1. 執行以下步驟"設定管理介面證書"。
2. 在網格管理員中，選擇 配置 > 安全性 > 憑證，然後選擇 用戶端 標籤。

3. 選擇“新增”。
4. 輸入證書名稱。
5. 若要使用外部監控工具存取 Prometheus 指標，請選擇 允許 **prometheus**。
6. 選擇*繼續*。
7. 對於*附加憑證*步驟，上傳客戶端憑證、私密金鑰和 CA 捆綁檔案：
   a. 選擇*上傳證書*。
   b. 選擇「瀏覽」並選擇用戶端憑證、私鑰和 CA 捆綁文件(`.pem`）。
      - 選擇*用戶端憑證詳細資料*以顯示憑證元資料和憑證 PEM。
      - 選擇*複製證書 PEM* 以複製證書內容並貼上到其他地方。
   c. 選擇*建立*將憑證保存在網格管理員中。

      新證書出現在客戶端選項卡上。
8. 設定外部監控工具，例如 Grafana。

從網格管理器產生的證書

如果未設定管理介面證書，且您計劃為使用 Grid Manager 中的產生憑證功能的 Prometheus 新增用戶端證書，請使用此流程新增管理員用戶端憑證。

步驟

1. 在網格管理員中，選擇 配置 > 安全性 > 憑證，然後選擇 用戶端 標籤。
2. 選擇“新增”。
3. 輸入證書名稱。
4. 若要使用外部監控工具存取 Prometheus 指標，請選擇 允許 **prometheus**。
5. 選擇*繼續*。
6. 對於*附加憑證*步驟，選擇*產生憑證*。
7. 指定證書資訊：
   - 主題（可選）：證書擁有者的 X.509 主題或專有名稱 (DN)。
   - 有效天數：產生的憑證從產生時開始的有效天數。
   - 新增金鑰使用擴充功能：如果選擇（預設和建議），則金鑰使用和擴充金鑰使用擴充將新增至產生的憑證中。

     這些擴充定義了憑證中包含的金鑰的用途。

     除非憑證包含這些擴充功能時遇到與舊客戶端的連線問題，否則請選取此核取方塊。
8. 選擇*生成*。
9. 選擇*用戶端憑證詳細資料*以顯示憑證元資料和憑證 PEM。

關閉對話方塊後，您將無法查看憑證私鑰。將金鑰複製或下載到安全位置。

- 選擇*複製證書 PEM* 以複製證書內容並貼上到其他地方。
- 選擇*下載證書*儲存證書檔案。

  指定證書檔案名稱和下載位置。使用副檔名儲存檔案 `.pem`。

  例如： `storagegrid_certificate.pem`

- 選擇*複製私密金鑰*複製憑證私鑰以便貼到其他地方。
- 選擇*下載私鑰*將私鑰儲存為檔案。

  指定私鑰檔案名稱和下載位置。

10. 選擇*建立*將憑證保存在網格管理員中。

    新證書出現在客戶端選項卡上。

11. 在網格管理員中，選擇 配置 > 安全性 > 憑證，然後選擇 全域 標籤。
12. 選擇*管理介面證書*。
13. 選擇*使用自訂憑證*。
14. 從上傳 certificate.pem 和 private_key.pem 文件客戶端證書詳細信息步。無需上傳 CA 包。
    a. 選擇*上傳憑證*，然後選擇*繼續*。
    b. 上傳每個證書文件(`.pem`）。
    c. 選擇*儲存*將憑證儲存在網格管理員中。

       新證書出現在管理介面證書頁面上。

15. 設定外部監控工具，例如 Grafana。

設定外部監控工具

步驟

1. 在您的外部監控工具（例如 Grafana）上設定以下設定。
   a. 名稱：輸入連線的名稱。

      StorageGRID不需要此信息，但您必須提供名稱來測試連接。

   b. **URL**：輸入管理節點的網域名稱或 IP 位址。指定 HTTPS 和連接埠 9091。

      例如： `https://admin-node.example.com:9091`

   c. 啟用 **TLS** 用戶端身份驗證 和 使用 **CA** 憑證。
   d. 在 TLS/SSL 身份驗證詳細資訊下，複製並貼上：+
      - 管理介面CA憑證到**CA Cert**

- 客戶端證書到客戶端證書
- 客戶端金鑰的私鑰

e. **ServerName**：輸入管理節點的網域名稱。

ServerName 必須與管理介面憑證中顯示的網域名稱相符。

2. 儲存並測試從StorageGRID或本機檔案複製的憑證和私密金鑰。

現在您可以使用外部監控工具從StorageGRID存取 Prometheus 指標。

有關指標的信息，請參閱"StorageGRID監控說明"。

編輯客戶端證書

您可以編輯管理員用戶端憑證以變更其名稱、啟用或停用 Prometheus 訪問，或在目前憑證過期時上傳新憑證。

步驟

1. 選擇 設定 > 安全 > 憑證，然後選擇 用戶端 標籤。

表中列出了證書到期日期和 Prometheus 存取權限。如果憑證即將過期或已經過期，表中會出現一則訊息並觸發警報。

2. 選擇您要編輯的憑證。
3. 選擇*編輯*，然後選擇*編輯名稱和權限*
4. 輸入證書名稱。
5. 若要使用外部監控工具存取 Prometheus 指標，請選擇 允許 **prometheus**。
6. 選擇“繼續”將憑證儲存在網格管理員中。

更新後的憑證顯示在客戶端標籤上。

附加新的客戶端憑證

當前證書過期後，您可以上傳新證書。

步驟

1. 選擇 設定 > 安全 > 憑證，然後選擇 用戶端 標籤。

表中列出了證書到期日期和 Prometheus 存取權限。如果憑證即將過期或已經過期，表中會出現一則訊息並觸發警報。

2. 選擇您要編輯的憑證。
3. 選擇*編輯*，然後選擇編輯選項。

上傳證書

複製證書文字並貼上到其他地方。

a. 選擇*上傳憑證*，然後選擇*繼續*。

b. 上傳客戶端憑證名稱(`.pem`）。

   選擇*用戶端憑證詳細資料*以顯示憑證元資料和憑證 PEM。

   - 選擇*下載證書*儲存證書檔案。

     指定證書檔案名稱和下載位置。使用副檔名儲存檔案 `.pem`。

     例如： `storagegrid_certificate.pem`

   - 選擇*複製證書 PEM* 以複製證書內容並貼上到其他地方。

c. 選擇*建立*將憑證保存在網格管理員中。

   更新後的憑證顯示在客戶端標籤上。

產生證書

產生證書文字以貼上到其他地方。

a. 選擇*產生證書*。

b. 指定證書資訊：

   - 主題（可選）：證書擁有者的 X.509 主題或專有名稱 (DN)。
   - 有效天數：產生的憑證從產生時開始的有效天數。
   - 新增金鑰使用擴充功能：如果選擇（預設和建議），則金鑰使用和擴充金鑰使用擴充將新增至產生的憑證中。

     這些擴充定義了憑證中包含的金鑰的用途。

     除非憑證包含這些擴充功能時遇到與舊客戶端的連線問題，否則請選取此核取方塊。

c. 選擇*生成*。

d. 選擇*用戶端憑證詳細資料*以顯示憑證元資料和憑證 PEM。

   關閉對話方塊後，您將無法查看憑證私鑰。將金鑰複製或下載到安全位置。

   - 選擇*複製證書 PEM* 以複製證書內容並貼上到其他地方。
   - 選擇*下載證書*儲存證書檔案。

     指定證書檔案名稱和下載位置。使用副檔名儲存檔案 `.pem`。

   例如： `storagegrid_certificate.pem`

- 選擇*複製私密金鑰*複製憑證私鑰以便貼到其他地方。
- 選擇*下載私鑰*將私鑰儲存為檔案。

  指定私鑰檔案名稱和下載位置。

e. 選擇*建立*將憑證保存在網格管理員中。

新證書出現在客戶端選項卡上。

下載或複製客戶端證書

您可以下載或複製客戶端憑證以供其他地方使用。

步驟

1. 選擇 設定 > 安全 > 憑證，然後選擇 用戶端 標籤。
2. 選擇您要複製或下載的憑證。
3. 下載或複製證書。

下載證書文件

下載證書 `.pem`文件。

a. 選擇*下載證書*。
b. 指定證書檔案名稱和下載位置。使用副檔名儲存檔案 `.pem`。

   例如： `storagegrid_certificate.pem`

影印證書

複製證書文字並貼上到其他地方。

a. 選擇*複製憑證 PEM*。
b. 將複製的憑證貼到文字編輯器中。
c. 儲存帶有擴展名的文字文件 `.pem`。

   例如： `storagegrid_certificate.pem`

刪除客戶端證書

如果您不再需要管理員用戶端證書，您可以將其刪除。

步驟

1. 選擇 設定 > 安全 > 憑證，然後選擇 用戶端 標籤。
2. 選擇您要刪除的憑證。

3. 選擇*刪除*然後確認。

> 若要刪除最多 10 個證書，請在「用戶端」標籤上選擇要刪除的每個證書，然後選擇「操作」>「刪除」。

刪除憑證後，使用該憑證的用戶端必須指定新的用戶端憑證才能存取StorageGRID Prometheus 資料庫。

配置安全設定

管理 **TLS** 和 **SSH** 策略

TLS 和 SSH 原則決定使用哪些協定和密碼與用戶端應用程式建立安全的 TLS 連線以及與內部StorageGRID服務建立安全的 SSH 連線。

安全性策略控制 TLS 和 SSH 如何加密傳輸中的資料。一般來說，使用現代相容性（預設）策略，除非您的系統需要符合通用標準或您需要使用其他密碼。

> 某些StorageGRID服務尚未更新以使用這些原則中的密碼。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"Root存取權限"。

選擇安全策略

步驟

1. 選擇*配置* > 安全 > 安全設定。

   *TLS 和 SSH 策略*標籤顯示可用的策略。目前有效的策略在策略圖塊上以綠色複選標記表示。

2. 查看圖塊以了解可用的策略。

政策	描述
現代相容性（預設）	如果您需要強加密並且除非您有特殊要求，請使用預設策略。此策略與大多數 TLS 和 SSH 用戶端相容。

政策	描述
舊版相容性	如果您需要為舊客戶端提供額外的相容性選項，請使用此原則。此策略中的附加選項可能會使其安全性低於現代相容性策略。
通用標準	如果您需要通用標準認證，請使用此政策。
FIPS 嚴格	如果您需要通用標準認證並且需要使用NetApp加密安全模組 3.0.8 將外部用戶端連接到負載平衡器端點、租用戶管理器和網格管理器，請使用此原則。使用此策略可能會降低效能。 注意：選擇此策略後，所有節點都必須"以滾動方式重啟"啟動NetApp加密安全模組。使用*維護* > *滾動重新啟動*來啟動和監控重新啟動。
風俗	如果您需要套用自己的密碼，請建立自訂原則。

3. 要查看有關每個策略的密碼、協定和演算法的詳細信息，請選擇*查看詳細資訊*。
4. 若要變更目前策略，請選擇*使用策略*。

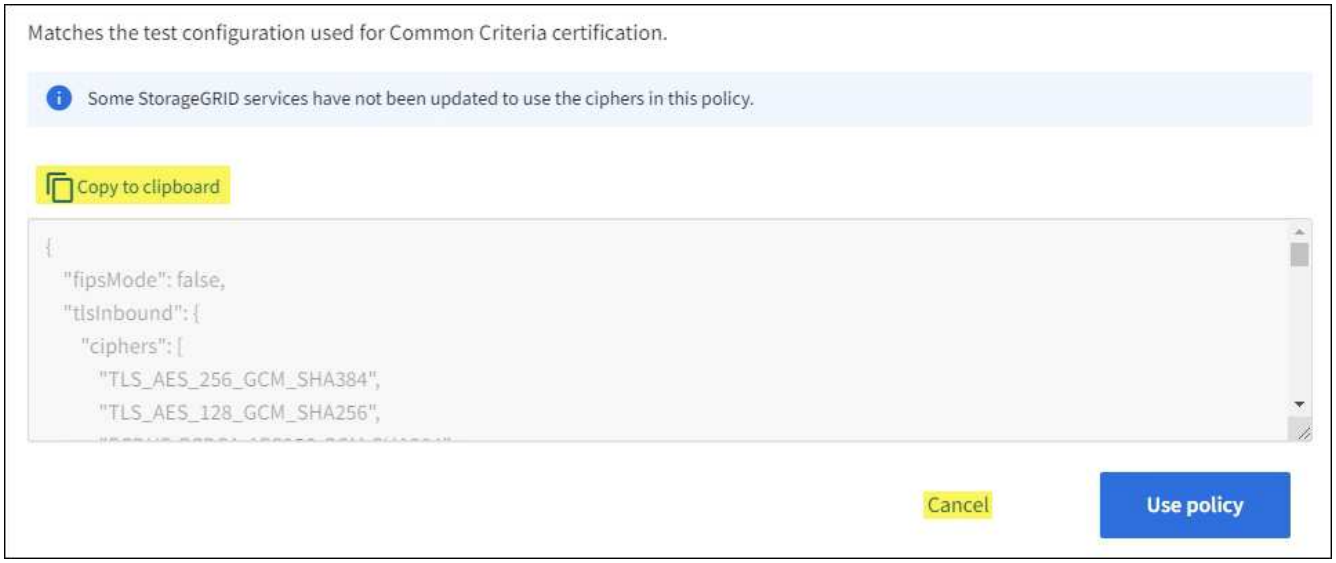
   政策圖塊上的「目前政策」旁邊會出現一個綠色複選標記。

建立自訂安全性策略

如果您需要套用自己的密碼，您可以建立自訂原則。

步驟

1. 從與您要建立的自訂策略最相似的策略的圖塊中，選擇「查看詳細資訊」。
2. 選擇*複製到剪貼簿*，然後選擇*取消*。



3. 從*自訂策略*圖塊中，選擇*配置和使用*。
4. 貼上您複製的 JSON 並進行所需的更改。

5. 選擇*使用策略*。

   自訂策略圖塊上的「目前策略」旁邊會出現一個綠色複選標記。

6. 或者，選擇「編輯配置」對新的自訂策略進行更多變更。

暫時恢復預設安全策略

如果您設定了自訂安全性策略，且設定的 TLS 策略與"設定伺服器憑證"。

您可以暫時恢復預設安全性策略。

步驟

1. 登入管理節點：
   a. 輸入以下命令： `ssh admin@Admin_Node_IP`
   b. 輸入 `Passwords.txt`文件。
   c. 輸入以下命令切換到root： `su -`
   d. 輸入 `Passwords.txt`文件。

      當您以 root 身分登入時，提示字元將從 `$`到 `#`。

2. 運行以下命令：

   ```
   restore-default-cipher-configurations
   ```

3. 從 Web 瀏覽器存取相同管理節點上的網格管理器。
4. 請依照以下步驟操作選擇安全策略重新配置策略。

設定網路和物件安全

您可以設定網路和物件安全性來加密儲存的對象，阻止某些 S3 請求，或允許用戶端連接到儲存節點使用 HTTP 而不是 HTTPS。

儲存物件加密

儲存物件加密可以對透過 S3 提取的所有物件資料進行加密。預設情況下，儲存的物件未加密，但您可以選擇使用 AES-128 或 AES-256 加密演算法來加密物件。啟用該設定後，所有新攝取的物件都會被加密，但現有儲存的物件不會發生任何變更。如果停用加密，目前加密的物件仍保持加密，但新攝取的物件不會被加密。

儲存物件加密設定僅適用於尚未透過儲存桶級或物件層級加密進行加密的 S3 物件。

有關StorageGRID加密方法的更多詳細信息，請參閱"查看StorageGRID加密方法"。

防止客戶端修改

防止客戶端修改是一個系統範圍的設定。當選擇“防止客戶端修改”選項時，以下請求將被拒絕。

S3 REST API

- DeleteBucket 請求
- 任何修改現有物件的資料、使用者定義的元資料或 S3 物件標記的請求

為儲存節點連線啟用 HTTP

預設情況下，客戶端應用程式使用 HTTPS 網路協定與儲存節點建立任何直接連線。您可以選擇為這些連線啟用 HTTP，例如，在測試非生產網格時。

只有當 S3 用戶端需要直接與儲存節點建立 HTTP 連線時，才使用 HTTP 進行儲存節點連線。對於僅使用 HTTPS 連線的用戶端或連線到負載平衡器服務的用戶端，您不需要使用此選項（因為您可以"配置每個負載平衡器端點"使用 HTTP 或 HTTPS)。

看"摘要：客戶端連接的 IP 位址和連接埠"了解 S3 用戶端使用 HTTP 或 HTTPS 連接到儲存節點時使用哪些連接埠。

選擇選項

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 您擁有 Root 存取權限。

步驟

1. 選擇*配置* > 安全 > 安全設定。
2. 選擇“網路和物件”標籤。
3. 對於儲存對象加密，如果您不想加密儲存對象，請使用 **None**（預設）設置，或選擇 **AES-128** 或 **AES-256** 來加密儲存對象。
4. 如果您想阻止 S3 用戶端發出特定請求，可以選擇「阻止客戶端修改」。

   如果您更改此設置，則大約需要一分鐘才能應用新設置。配置的值被緩存，以提高效能和擴展性。

5. 如果用戶端直接連接到儲存節點並且您想要使用 HTTP 連接，則可以選擇*為儲存節點連接啟用 HTTP*。

   為生產網格啟用 HTTP 時要小心，因為請求將以未加密的形式傳送。

6. 選擇*儲存*。

更改介面安全設定

透過介面安全性設置，您可以控制當使用者處於非活動狀態的時間超過指定時間時是否將其註銷，以及是否在 API 錯誤回應中包含堆疊追蹤。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"Root存取權限"。

關於此任務

*安全設定*頁麵包括*瀏覽器不活動逾時*和*管理 API 堆疊追蹤*設定。

瀏覽器不活動逾時

指示使用者登出之前瀏覽器可以處於非活動狀態的時間。預設值為 15 分鐘。

瀏覽器不活動逾時也受以下因素控制：

- 一個單獨的、不可設定的StorageGRID計時器，用於系統安全。每個使用者的身份驗證令牌在使用者登入 16 小時後過期。當使用者的身份驗證過期時，該使用者將自動登出，即使瀏覽器不活動逾時已停用或尚未達到瀏覽器逾時值。若要更新令牌，使用者必須重新登入。
- 身分提供者的逾時設置，假設為StorageGRID啟用了單一登入 (SSO)。

  如果啟用了 SSO 並且使用者的瀏覽器逾時，則使用者必須重新輸入其 SSO 憑證才能再次存取StorageGRID 。看"配置單一登入" 。

管理 **API** 堆疊追蹤

控制是否在網格管理器和租用戶管理器 API 錯誤回應中傳回堆疊追蹤。

預設此選項是停用的，但您可能希望為測試環境啟用此功能。一般來說，您應該在生產環境中停用堆疊追蹤，以避免在發生 API 錯誤時洩露內部軟體詳細資訊。

步驟

1. 選擇*配置* > 安全 > 安全設定。
2. 選擇“介面”選項卡。
3. 若要更改瀏覽器不活動逾時設定：
   a. 展開手風琴。
   b. 若要變更逾時期限，請指定 60 秒到 7 天之間的值。預設超時時間為 15 分鐘。
   c. 若要停用此功能，請取消選取該複選框。
   d. 選擇*儲存*。

      新設定不會影響目前已登入的使用者。使用者必須重新登入或刷新瀏覽器才能使新的逾時設定生效。
4. 若要變更管理 API 堆疊追蹤的設定：
   a. 展開手風琴。
   b. 選取該複選框以在網格管理器和租用戶管理器 API 錯誤回應中傳回堆疊追蹤。

      在生產環境中停用堆疊追蹤，以避免在發生 API 錯誤時洩露內部軟體詳細資訊。

   c. 選擇*儲存*。

配置金鑰管理伺服器

金鑰管理伺服器 (KMS) 是一個外部第三方系統，它使用金鑰管理互通性協定 (KMIP) 向相關StorageGRID站點上的StorageGRID設備節點提供加密金鑰。

StorageGRID僅支援某些金鑰管理伺服器。要取得受支援的產品和版本的列表，請使用 "NetApp互通性矩陣工具 (IMT)"。

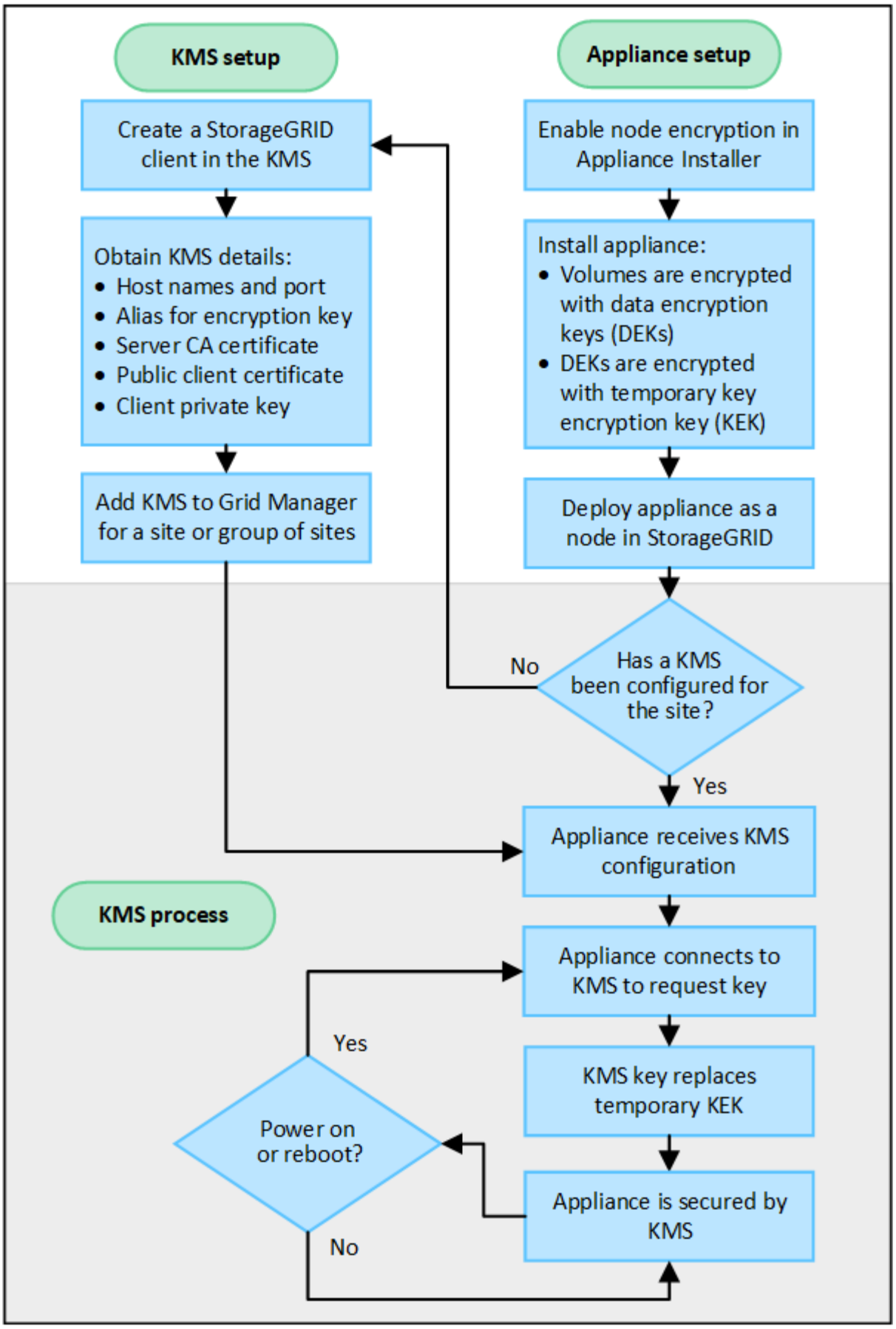
您可以使用一個或多個金鑰管理伺服器來管理在安裝期間啟用了「節點加密」設定的任何StorageGRID裝置節點的節點加密金鑰。透過將這些設備節點與金鑰管理伺服器結合使用，即使設備從資料中心移除，您也可以保護資料。裝置磁碟區加密後，除非節點可以與 KMS 通信，否則您無法存取裝置上的任何資料。

> StorageGRID不會建立或管理用於加密和解密裝置節點的外部金鑰。如果您打算使用外部金鑰管理伺服器來保護StorageGRID數據，則必須了解如何設定該伺服器，並且必須了解如何管理加密金鑰。執行金鑰管理任務超出了這些說明的範圍。如果您需要協助，請參閱金鑰管理伺服器的文件或聯絡技術支援。

KMS 和設備配置

在使用金鑰管理伺服器 (KMS) 保護裝置節點上的StorageGRID資料之前，您必須完成兩個設定任務：設定一個或多個 KMS 伺服器並為裝置節點啟用節點加密。當這兩個設定任務完成後，金鑰管理過程將會自動發生。

此流程圖顯示了使用 KMS 保護設備節點上的StorageGRID資料的進階步驟。



流程圖顯示 KMS 設定和裝置設定並行進行；但是，您可以根據需要在為新裝置節點啟用節點加密之前或之後設

定金鑰管理伺服器。

設定金鑰管理伺服器（KMS）

設定密鑰管理伺服器包括以下進階步驟。

步	參考
存取 KMS 軟體並為每個 KMS 或 KMS 叢集新增StorageGRID的用戶端。	"在 KMS 中將StorageGRID配置為客戶端"
取得 KMS 上StorageGRID客戶端所需的資訊。	"在 KMS 中將StorageGRID配置為客戶端"
將 KMS 新增至網格管理器，將其指派給單一網站或預設網站群組，上傳所需的證書，然後儲存 KMS 配置。	"新增金鑰管理伺服器 (KMS)"

設定設備

設定用於 KMS 的設備節點包括以下進階步驟。

1. 在設備安裝的硬體配置階段，使用StorageGRID設備安裝程式為設備啟用 節點加密 設定。

   > 將裝置新增至電網後，您無法啟用*節點加密*設置，且無法對未啟用節點加密的裝置使用外部金鑰管理。

2. 運行StorageGRID設備安裝程式。在安裝過程中，會為每個裝置磁碟區指派一個隨機資料加密金鑰 (DEK)，如下所示：
   - DEK 用於加密每個磁碟區上的資料。這些金鑰是使用裝置作業系統中的 Linux 統一金鑰設定 (LUKS) 磁碟加密產生的，無法變更。
   - 每個單獨的 DEK 都由主金鑰加密金鑰 (KEK) 加密。初始 KEK 是一個臨時金鑰，用於加密 DEK，直到裝置可以連接到 KMS。
3. 將設備節點新增至StorageGRID。

看 "啟用節點加密"了解詳情。

密鑰管理加密過程（自動發生）

金鑰管理加密包括以下自動執行的進階步驟。

1. 當您將啟用了節點加密的裝置安裝到網格中時， StorageGRID會決定包含新節點的網站是否存在 KMS 設定。
   - 如果已經為網站配置了 KMS，設備將接收 KMS 配置。
   - 如果尚未為網站配置 KMS，裝置上的資料將繼續由臨時 KEK 加密，直到您為網站配置 KMS 並且裝置收到 KMS 設定為止。
2. 該裝置使用 KMS 設定連接到 KMS 並請求加密金鑰。
3. KMS 向裝置發送加密金鑰。 KMS 的新金鑰取代了臨時 KEK，現在用於加密和解密裝置磁碟區的 DEK。

加密裝置節點連接到配置的 KMS 之前存在的任何資料都使用臨時金鑰加密。但是，在臨時金鑰被 KMS 加密金鑰取代之前，裝置磁碟區不應被視為受到保護，不能從資料中心移除。

4. 如果裝置開啟或重新啟動，它會重新連線到 KMS 來請求金鑰。此密鑰保存在揮發性記憶體中，斷電或重新啟動後將無法恢復。

使用金鑰管理伺服器的注意事項和要求

在設定外部金鑰管理伺服器 (KMS) 之前，您必須了解注意事項和要求。

支援哪個版本的 **KMIP**？

StorageGRID支援 KMIP 版本 1.4。

"密鑰管理互通性協定規範版本 1.4"

網路考量有哪些？

網路防火牆設定必須允許每個設備節點透過用於金鑰管理互通協定 (KMIP) 通訊的連接埠進行通訊。預設 KMIP 連接埠為 5696。

您必須確保使用節點加密的每個裝置節點都具有對您為網站配置的 KMS 或 KMS 叢集的網路存取權限。

支援哪些版本的 **TLS**？

設備節點和配置的 KMS 之間的通訊使用安全的 TLS 連線。 StorageGRID在與 KMS 或 KMS 叢集建立 KMIP 連線時，可以支援 TLS 1.2 或 TLS 1.3 協議，具體取決於 KMS 支援的內容以及"TLS 和 SSH 策略"您正在使用。

StorageGRID在建立連線時與 KMS 協商協定和密碼（TLS 1.2）或密碼套件（TLS 1.3）。要查看可用的協定版本和密碼/密碼套件，請查看 `tlsOutbound`網格的活動 TLS 和 SSH 策略部分（配置 > 安全 安全設定）。

支援哪些設備？

您可以使用金鑰管理伺服器 (KMS) 來管理網格中啟用了 節點加密 設定的任何StorageGRID裝置的加密金鑰。此設定只能在使用StorageGRID Appliance Installer 的裝置安裝硬體設定階段啟用。

將裝置新增至電網後，您無法啟用節點加密，且無法對未啟用節點加密的裝置使用外部金鑰管理。

您可以將配置的 KMS 用於StorageGRID設備和設備節點。

您無法將配置的 KMS 用於基於軟體（非設備）的節點，包括以下內容：

- 部署為虛擬機器 (VM) 的節點
- 部署在 Linux 主機上的容器引擎內的節點

部署在這些其他平台上的節點可以在資料儲存或磁碟層級使用StorageGRID以外的加密。

我應該何時配置密鑰管理伺服器？

對於新安裝，您通常應該在建立租用戶之前在網格管理員中設定一個或多個金鑰管理伺服器。此順序確保在節點

上儲存任何物件資料之前，節點受到保護。

您可以在安裝設備節點之前或之後在網格管理器中設定金鑰管理伺服器。

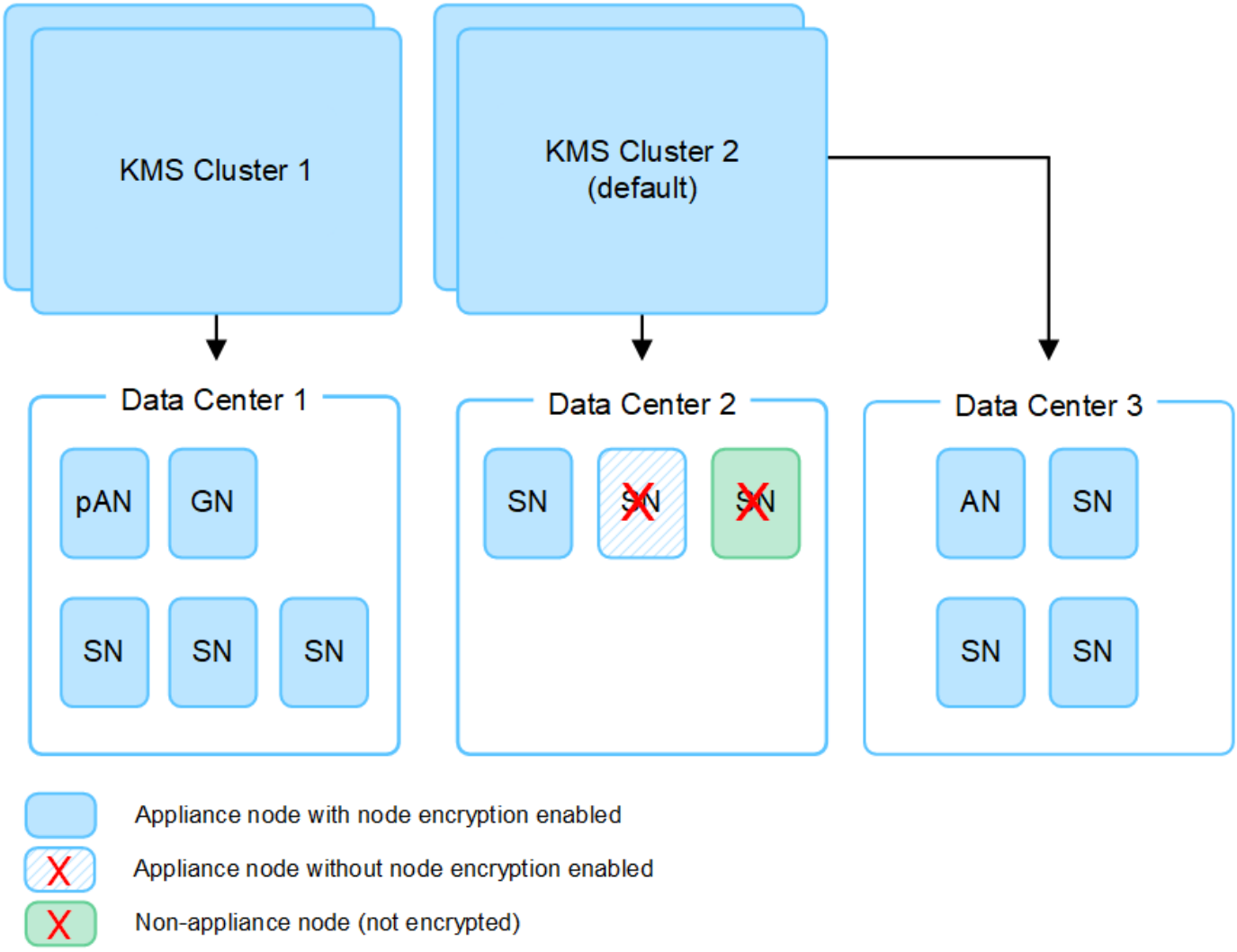
我需要多少個金鑰管理伺服器？

您可以設定一個或多個外部金鑰管理伺服器來為StorageGRID系統中的設備節點提供加密金鑰。每個 KMS 為單一站點或一組站點的StorageGRID設備節點提供單一加密金鑰。

StorageGRID支援使用 KMS 叢集。每個 KMS 叢集包含多個共用設定設定和加密金鑰的複製金鑰管理伺服器。建議使用 KMS 叢集進行金鑰管理，因為它可以提高高可用性配置的故障轉移能力。

例如，假設您的StorageGRID系統有三個資料中心站點。您可以設定 KMS 叢集來為資料中心 1 的所有裝置節點提供金鑰，並配置第二個 KMS 叢集來為所有其他網站的所有裝置節點提供金鑰。當您新增第二個 KMS 叢集時，您可以為資料中心 2 和資料中心 3 設定一個預設 KMS。

請注意，您不能將 KMS 用於非裝置節點或安裝期間未啟用 節點加密 設定的任何裝置節點。



當密鑰被旋轉時會發生什麼？

作為最佳安全做法，您應該定期"旋轉加密密鑰"由每個配置的 KMS 使用。

當新的密鑰版本可用時：

- 它會自動分發到與 KMS 關聯的網站上的加密設備節點。分發應在密鑰輪換後一小時內進行。
- 如果在分發新金鑰版本時加密裝置節點處於離線狀態，則該節點將在重新啟動後立即收到新金鑰。
- 如果因任何原因無法使用新金鑰版本加密裝置磁碟區，則會針對裝置節點觸發 **KMS** 加密金鑰輪替失敗 警報。您可能需要聯絡技術支援以取得協助來解決此警報。

設備節點加密後可以重複使用嗎？

如果需要將加密設備安裝到另一個StorageGRID系統中，則必須先停用網格節點才能將物件資料移至另一個節點。然後，您可以使用StorageGRID Appliance Installer "清除 KMS 配置" 。清除 KMS 設定將停用 節點加密 設定並刪除裝置節點與StorageGRID站點的 KMS 設定之間的關聯。

如果無法存取 KMS 加密金鑰，裝置上保留的任何資料將無法再訪問，並且會永久鎖定。

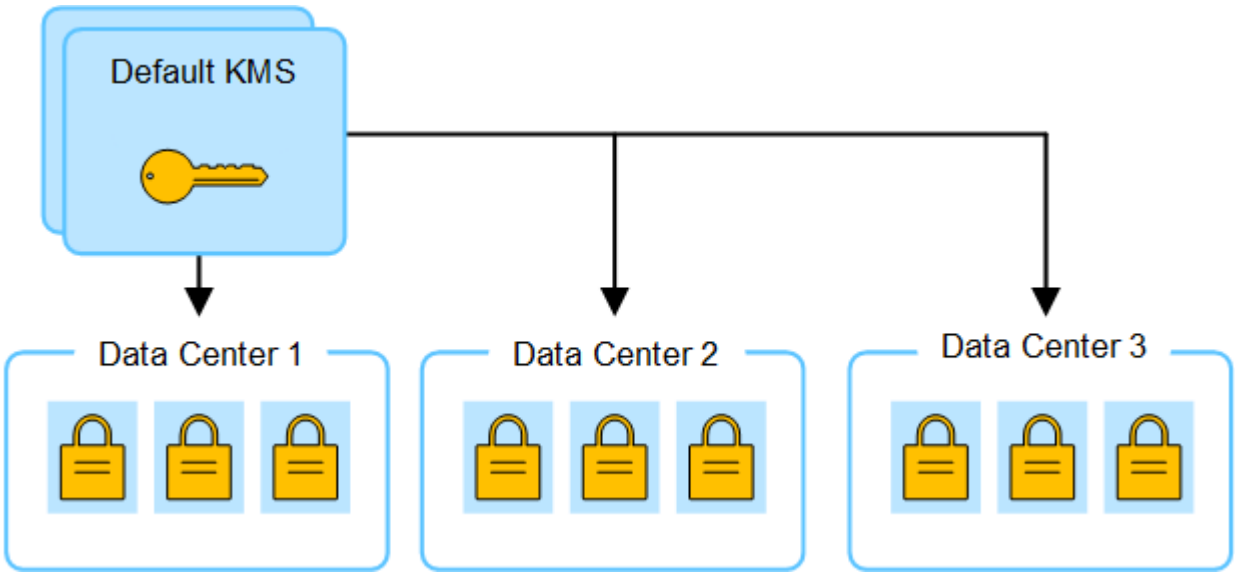
更改站點 **KMS** 的注意事項

每個金鑰管理伺服器 (KMS) 或 KMS 叢集會向單一網站或一組網站的所有裝置節點提供加密金鑰。如果您需要變更網站使用的 KMS，則可能需要將加密金鑰從一個 KMS 複製到另一個 KMS。

如果您變更網站所使用的 KMS，則必須確保該網站上先前加密的裝置節點可以使用儲存在新 KMS 上的金鑰解密。在某些情況下，您可能需要將目前版本的加密金鑰從原始 KMS 複製到新的 KMS。您必須確保 KMS 具有正確的金鑰來解密網站上的加密裝置節點。

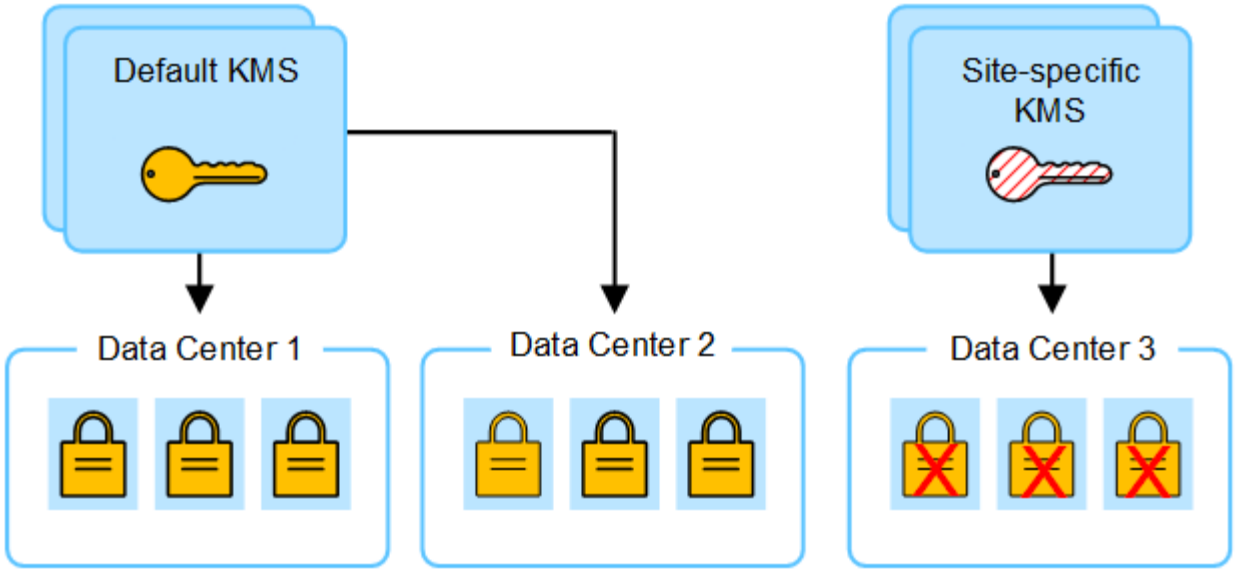
例如：

1. 您最初配置一個適用於所有沒有專用 KMS 的網站的預設 KMS。
2. 儲存 KMS 後，所有啟用了 節點加密 設定的裝置節點都會連接到 KMS 並要求加密金鑰。此金鑰用於加密所有網站的設備節點。也必須使用相同的金鑰來解密這些裝置。

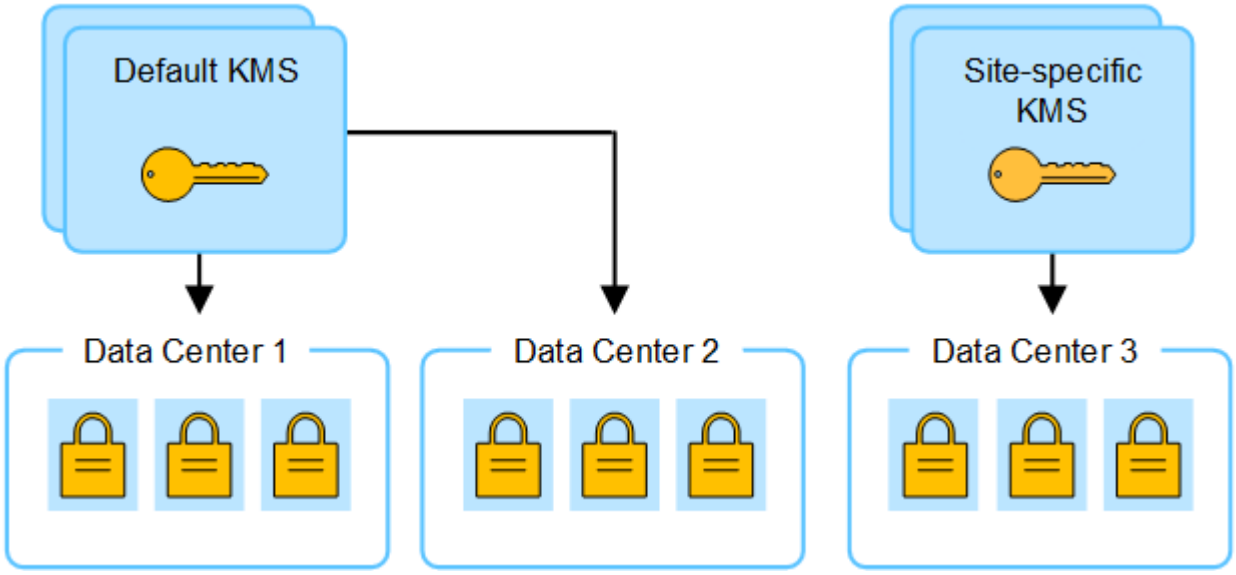


3. 您決定為一個站點（圖中的資料中心 3）新增特定於站點的 KMS。但是，由於裝置節點已加密，因此當您嘗試儲存網站特定 KMS 的設定時會發生驗證錯誤。發生該錯誤的原因是網站特定的 KMS 沒有正確的金鑰來

解密該網站的節點。



4. 為了解決這個問題，您可以將目前版本的加密金鑰從預設 KMS 複製到新的 KMS。 （從技術上講，您將原始金鑰複製到具有相同別名的新金鑰。原始密鑰將成為新密鑰的先前版本。）網站特定的 KMS 現在具有解密資料中心 3 的裝置節點的正確金鑰，因此可以將其保存在StorageGRID中。



更改網站所用 **KMS** 的用例

該表總結了更改站點 KMS 的最常見情況所需的步驟。

更改網站 **KMS** 的用例	必要步驟
您有一個或多個特定於網站的 KMS 條目，並且想要使用其中一個作為預設 KMS。	編輯特定於站點的 KMS。在「管理金鑰」欄位中，選擇「未由其他 KMS 管理的網站（預設為 KMS）」。站點特定的 KMS 現在將用作預設 KMS。它將適用於任何沒有專用 KMS 的網站。 "編輯金鑰管理伺服器 (KMS)"

更改網站 **KMS** 的用例	必要步驟
您有一個預設的 KMS，並且在擴充功能中新增了一個新網站。您不想對新網站使用預設的 KMS。	1. 如果新網站的裝置節點已由預設 KMS 加密，請使用 KMS 軟體將目前版本的加密金鑰從預設 KMS 複製到新的 KMS。 2. 使用網格管理器新增新的 KMS 並選擇網站。 "新增金鑰管理伺服器 (KMS)"
您希望網站的 KMS 使用不同的伺服器。	1. 如果網站上的裝置節點已被現有 KMS 加密，請使用 KMS 軟體將目前版本的加密金鑰從現有 KMS 複製到新的 KMS。 2. 使用網格管理器，編輯現有的 KMS 設定並輸入新的主機名稱或 IP 位址。 "新增金鑰管理伺服器 (KMS)"

在 **KMS** 中將**StorageGRID**配置為客戶端

您必須先將StorageGRID配置為每個外部金鑰管理伺服器或 KMS 叢集的用戶端，然後才能將 KMS 新增至StorageGRID。

這些說明適用於 Thales CipherTrust Manager 和 Hashicorp Vault。要取得受支援的產品和版本的列表，請使用 "NetApp互通性矩陣工具 (IMT)"。

步驟

1. 從 KMS 軟體中，為您計劃使用的每個 KMS 或 KMS 叢集建立一個StorageGRID用戶端。

   每個 KMS 管理單一站點或一組站點的StorageGRID設備節點的單一加密金鑰。

2. 使用以下兩種方法之一建立金鑰：

   - 使用您的 KMS 產品的金鑰管理頁面。為每個 KMS 或 KMS 叢集建立一個 AES 加密金鑰。

     加密金鑰必須為 2,048 位元或更多，且必須可匯出。

   - 讓StorageGRID建立金鑰。測試並儲存後會提示你"上傳客戶端證書"。

3. 記錄每個 KMS 或 KMS 群集的以下資訊。

   將 KMS 新增至StorageGRID時需要此資訊：

   - 每個伺服器的主機名稱或 IP 位址。
   - KMS 使用的 KMIP 連接埠。
   - KMS 中加密金鑰的金鑰別名。

4. 對於每個 KMS 或 KMS 集群，取得由憑證授權單位 (CA) 簽署的伺服器憑證或包含每個 PEM 編碼的 CA 憑證檔案的憑證包，按憑證連結順序連接。

   伺服器憑證允許外部 KMS 向StorageGRID進行身份驗證。

- 憑證必須使用隱私增強郵件 (PEM) Base-64 編碼的 X.509 格式。
- 每個伺服器憑證中的主題備用名稱 (SAN) 欄位必須包含StorageGRID將連接到的完全限定網域名稱 (FQDN) 或 IP 位址。

> 在StorageGRID中設定 KMS 時，必須在 **Hostname** 欄位中輸入相同的 FQDN 或 IP 位址。

- 伺服器憑證必須與 KMS 的 KMIP 介面使用的憑證匹配，後者通常使用連接埠 5696。

5. 取得外部 KMS 頒發給StorageGRID 的公共用戶端憑證以及用戶端憑證的私密金鑰。

   用戶端憑證允許StorageGRID向 KMS 驗證自身身分。

新增金鑰管理伺服器 **(KMS)**

您可以使用StorageGRID金鑰管理伺服器精靈新增每個 KMS 或 KMS 叢集。

開始之前

- 您已審閱"使用金鑰管理伺服器的注意事項和要求"。
- 你有"在 KMS 中將StorageGRID配置為客戶端"，並且您擁有每個 KMS 或 KMS 叢集所需的資訊。
- 您已使用"支援的網頁瀏覽器"。
- 你有"Root存取權限"。

關於此任務

如果可能，請在配置適用於所有未由其他 KMS 管理的網站的預設 KMS 之前配置任何特定於網站的金鑰管理伺服器。如果您先建立預設 KMS，則網格中的所有節點加密裝置都將由預設 KMS 加密。如果您以後想要建立特定於網站的 KMS，則必須先將目前版本的加密金鑰從預設 KMS 複製到新的 KMS。看"更改站點 KMS 的注意事項"了解詳情。

步驟 **1**：**KMS** 詳細信息

在新增金鑰管理伺服器精靈的步驟 1（KMS 詳細資料）中，您需要提供有關 KMS 或 KMS 叢集的詳細資訊。

步驟

1. 選擇 設定 > 安全 > 金鑰管理伺服器。

   出現密鑰管理伺服器頁面，其中已選取配置詳細資訊標籤。

2. 選擇“創建”。

   出現新增金鑰管理伺服器精靈的第 1 步（KMS 詳細資訊）。

3. 為 KMS 和在該 KMS 中配置的StorageGRID用戶端輸入以下資訊。

場地	描述
KMS 名稱	協助您識別此 KMS 的描述性名稱。必須介於 1 到 64 個字元之間。

場地	描述
鍵名稱	KMS 中StorageGRID客戶端的精確金鑰別名。必須介於 1 到 255 個字元之間。 注意：如果您尚未使用 KMS 產品建立金鑰，系統將提示您讓StorageGRID建立金鑰。
管理密鑰	將與此 KMS 關聯的StorageGRID站點。如果可能，您應該在配置適用於所有未由其他 KMS 管理的網站的預設 KMS 之前配置任何特定於網站的金鑰管理伺服器。 • 如果此 KMS 將管理特定站點的裝置節點的加密金鑰，請選擇一個站點。 • 選擇*未由其他 KMS 管理的網站（預設 KMS）*來配置一個預設 KMS，該預設 KMS 將套用於任何沒有專用 KMS 的網站以及您在後續擴充中新增的任何網站。 *注意：*如果您選擇先前由預設 KMS 加密的網站但未向新 KMS 提供目前版本的原始加密金鑰，則在儲存 KMS 設定時將發生驗證錯誤。
港口	KMS 伺服器用於金鑰管理互通協定 (KMIP) 通訊的連接埠。預設為 5696，這是 KMIP 標準連接埠。
主機名稱	KMS 的完全限定網域名稱或 IP 位址。 *注意：*伺服器憑證的主題備用名稱 (SAN) 欄位必須包含您在此輸入的 FQDN 或 IP 位址。否則， StorageGRID將無法連接到 KMS 或 KMS 叢集中的所有伺服器。

4. 如果您正在配置 KMS 集群，請選擇「新增另一個主機名稱」為集群中的每個伺服器新增一個主機名稱。
5. 選擇*繼續*。

步驟**2**：上傳伺服器憑證

在新增金鑰管理伺服器精靈的第 2 步（上傳伺服器憑證）中，您可以上傳 KMS 的伺服器憑證（或憑證包）。伺服器憑證允許外部 KMS 向StorageGRID進行身份驗證。

步驟

1. 從*步驟 2（上傳伺服器憑證）*開始，瀏覽到已儲存的伺服器憑證或憑證包的位置。
2. 上傳證書檔案。

   出現伺服器憑證元資料。

   如果您上傳了憑證包，則每個憑證的元資料都會顯示在自己的標籤上。

3. 選擇*繼續*。

步驟 **3**：上傳客戶端憑證

在新增金鑰管理伺服器精靈的步驟 3（上傳用戶端憑證）中，上傳用戶端憑證和用戶端憑證私鑰。用戶端憑證允許StorageGRID向 KMS 驗證自身身分。

步驟

1. 從*步驟 3（上傳客戶端憑證）*開始，瀏覽到客戶端憑證的位置。
2. 上傳客戶端證書檔案。

   出現客戶端證書元資料。
3. 瀏覽到客戶端憑證的私鑰的位置。
4. 上傳私鑰檔案。
5. 選擇*測試並儲存*。

   如果金鑰不存在，系統會提示您讓StorageGRID建立一個。

   測試金鑰管理伺服器和設備節點之間的連線。如果所有連線均有效，並且在 KMS 上找到了正確的金鑰，則新的金鑰管理伺服器將會新增至金鑰管理伺服器頁面的表中。

   新增 KMS 後，金鑰管理伺服器頁面上的憑證狀態立即顯示為未知。 StorageGRID可能需要長達 30 分鐘才能取得每個憑證的實際狀態。您必須刷新 Web 瀏覽器才能查看目前狀態。
6. 如果在選擇“測試並儲存”時出現錯誤訊息，請查看訊息詳細信息，然後選擇“確定”。

   例如，如果連線測試失敗，您可能會收到 422：無法處理的實體錯誤。
7. 如果需要儲存目前配置而不測試外部連接，請選擇*強制儲存*。

   選擇「強制儲存」將儲存 KMS 配置，但不會測試從每個裝置到該 KMS 的外部連線。如果設定有問題，您可能無法重新啟動在受影響網站上啟用了節點加密的裝置節點。在問題解決之前，您可能會無法存取您的資料。
8. 查看確認警告，如果確定要強制儲存配置，請選擇「確定」。

   KMS 配置已儲存，但未測試與 KMS 的連線。

管理 **KMS**

管理金鑰管理伺服器 (KMS) 包括查看或編輯詳細資訊、管理憑證、查看加密節點以及在不再需要時刪除 KMS。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"所需的存取權限"。

查看 **KMS** 詳細信息

您可以查看有關StorageGRID系統中每個金鑰管理伺服器 (KMS) 的信息，包括金鑰詳細資訊以及伺服器和用戶端憑證的目前狀態。

步驟

1. 選擇 設定 > 安全 > 金鑰管理伺服器。

   出現密鑰管理伺服器頁面並顯示以下資訊：

   - 配置詳細資訊標籤列出了已設定的所有金鑰管理伺服器。
   - 加密節點標籤列出了所有啟用了節點加密的節點。

2. 若要查看特定 KMS 的詳細資訊並對該 KMS 執行操作，請選擇該 KMS 的名稱。 KMS 的詳細資訊頁面列出了以下資訊：

場地	描述
管理密鑰	與 KMS 關聯的StorageGRID站點。 此欄位顯示特定StorageGRID站點或*未由其他 KMS 管理的站點（預設 KMS）*的名稱。
主機名稱	KMS 的完全限定網域名稱或 IP 位址。 如果有兩個金鑰管理伺服器的集群，則會列出兩個伺服器的完全限定網域名稱或 IP 位址。如果叢集中有兩個以上的金鑰管理伺服器，則會列出第一個 KMS 的完全限定網域名稱或 IP 位址以及叢集中其他金鑰管理伺服器的數量。 例如： `10.10.10.10 and 10.10.10.11`或者 `10.10.10.10 and 2 others`。 若要查看叢集中的所有主機名，請選擇 KMS 並選擇 編輯 或 操作 > 編輯。

3. 選擇 KMS 詳細資料頁面上的標籤以查看以下資訊：

Tab	場地	描述
關鍵細節	鍵名稱	KMS 中StorageGRID客戶端的金鑰別名。
密鑰 UID	密鑰最新版本的唯一識別碼。	上次修改時間
密鑰最新版本的日期和時間。	伺服器憑證	元數據

Tab	場地	描述
證書的元數據，例如序號、到期日和時間以及證書 PEM。	證書 PEM	證書的 PEM（隱私增強郵件）文件的內容。
客戶端憑證	元數據	證書的元數據，例如序號、到期日和時間以及證書 PEM。

4. 根據組織的安全實務要求，選擇*輪替金鑰*，或使用 KMS 軟體來建立金鑰的新版本。

   當密鑰輪換成功時，密鑰 UID 和上次修改欄位將被更新。

   如果您使用 KMS 軟體輪替加密金鑰，請將其從金鑰的最後使用的版本輪替為相同金鑰的新版本。不要旋轉到完全不同的鍵。

   切勿嘗試透過更改 KMS 的金鑰名稱（別名）來輪換密鑰。 StorageGRID要求所有先前使用的金鑰版本（以及任何未來的版本）都可以使用相同的金鑰別名從 KMS 存取。如果您變更已設定的 KMS 的金鑰別名， StorageGRID可能無法解密您的資料。

管理證書

及時解決任何伺服器或客戶端證書問題。如果可能，請在證書過期之前更換證書。

您必須盡快解決任何憑證問題以維持資料存取。

步驟

1. 選擇 設定 > 安全 > 金鑰管理伺服器。
2. 在表格中，查看每個 KMS 的憑證到期值。
3. 如果任何 KMS 的憑證到期日期未知，請等待最多 30 分鐘，然後重新整理您的 Web 瀏覽器。
4. 如果憑證過期列指示憑證已過期或即將過期，請選擇 KMS 前往 KMS 詳細資料頁面。
   a. 選擇*伺服器憑證*並驗證「到期日」欄位的值。
   b. 若要取代證書，請選擇*編輯證書*上傳新證書。
   c. 重複這些子步驟並選擇*客戶端憑證*而不是伺服器憑證。
5. 當觸發*KMS CA 憑證過期*、*KMS 用戶端憑證過期*和*KMS 伺服器憑證過期*警報時，請注意每個警報的描述並執行建議的操作。

   StorageGRID可能需要長達 30 分鐘才能取得憑證過期更新。刷新您的網頁瀏覽器以查看當前值。

如果您獲得的狀態為*伺服器憑證狀態未知*，請確保您的 KMS 允許取得伺服器憑證而無需用戶端憑證。

查看加密節點

您可以查看有關StorageGRID系統中啟用了 節點加密 設定的裝置節點的資訊。

步驟

1. 選擇 設定 > 安全 > 金鑰管理伺服器。

   出現密鑰管理伺服器頁面。配置詳細資訊標籤顯示已設定的任何金鑰管理伺服器。

2. 從頁面頂部，選擇“加密節點”標籤。

   「加密節點」標籤列出了StorageGRID系統中啟用了「節點加密」設定的裝置節點。

3. 查看表中每個設備節點的資訊。

柱子	描述
節點名稱	設備節點的名稱。
節點類型	節點類型：儲存、管理或網關。
地點	安裝節點的StorageGRID站點的名稱。
KMS 名稱	用於節點的 KMS 的描述性名稱。 如果沒有列出 KMS，請選擇設定詳細資料標籤以新增 KMS。 "新增金鑰管理伺服器 (KMS)"
密鑰 UID	用於加密和解密裝置節點上資料的加密金鑰的唯一 ID。若要查看整個密鑰 UID，請選擇文字。 破折號 (--) 表示金鑰 UID 未知，可能是由於裝置節點和 KMS 之間的連線問題。
地位	KMS 與裝置節點之間的連線狀態。如果節點已連接，則時間戳記每 30 分鐘更新一次。 KMS 配置變更後，連線狀態可能需要幾分鐘才能更新。 *注意：*刷新您的網頁瀏覽器以查看新值。

4. 如果狀態列指示 KMS 問題，請立即解決該問題。

   在正常的 KMS 操作期間，狀態將為 已連接到 **KMS**。如果節點與電網斷開連接，則會顯示節點連接狀態（管理關閉或未知）。

   其他狀態訊息對應於具有相同名稱的StorageGRID警報：

   - KMS 配置載入失敗
   - KMS 連線錯誤
   - 未找到 KMS 加密金鑰名稱
   - KMS 加密金鑰輪換失敗
   - KMS 金鑰解密裝置磁碟區失敗

◦ 未配置 KMS

針對這些警報執行建議的操作。

您必須立即解決任何問題，以確保您的資料受到充分保護。

編輯 KMS

例如，如果憑證即將過期，您可能需要編輯金鑰管理伺服器的設定。

開始之前

- 如果您計劃更新為 KMS 選擇的站點，則您已查看"更改站點 KMS 的注意事項"。
- 您已使用"支援的網頁瀏覽器"。
- 你有"Root存取權限"。

步驟

1. 選擇 設定 > 安全 > 金鑰管理伺服器。

   出現金鑰管理伺服器頁面，其中顯示所有已設定的金鑰管理伺服器。

2. 選擇要編輯的 KMS，然後選擇*操作* > 編輯。

   您也可以透過選擇表格中的 KMS 名稱並在 KMS 詳細資料頁面上選擇 編輯 來編輯 KMS。

3. 或者，更新編輯金鑰管理伺服器精靈的*步驟 1（KMS 詳細資料）*中的詳細資訊。

場地	描述
KMS 名稱	協助您識別此 KMS 的描述性名稱。必須介於 1 到 64 個字元之間。
鍵名稱	KMS 中StorageGRID客戶端的精確金鑰別名。必須介於 1 到 255 個字元之間。 您只需在極少數情況下編輯密鑰名稱。例如，如果別名在 KMS 中被重新命名，或者先前密鑰的所有版本都已複製到新別名的版本歷史記錄中，則必須編輯密鑰名稱。
管理密鑰	如果您正在編輯特定於網站的 KMS，並且還沒有預設 KMS，則可以選擇 未由其他 **KMS** 管理的網站（預設 **KMS**）。此選擇將網站特定的 KMS 轉換為預設 KMS，這將適用於所有沒有專用 KMS 的網站以及擴充功能中新增的任何網站。 *注意：*如果您正在編輯特定於網站的 KMS，則不能選擇其他網站。如果您正在編輯預設 KMS，則無法選擇特定網站。
港口	KMS 伺服器用於金鑰管理互通協定 (KMIP) 通訊的連接埠。預設為 5696，這是 KMIP 標準連接埠。

場地	描述
主機名稱	KMS 的完全限定網域名稱或 IP 位址。 *注意：*伺服器憑證的主題備用名稱 (SAN) 欄位必須包含您在此輸入的 FQDN 或 IP 位址。否則， StorageGRID將無法連接到 KMS 或 KMS 叢集中的所有伺服器。

4. 如果您正在配置 KMS 集群，請選擇「新增另一個主機名稱」為集群中的每個伺服器新增一個主機名稱。
5. 選擇*繼續*。

   出現編輯金鑰管理伺服器精靈的第 2 步（上傳伺服器憑證）。
6. 如果需要更換伺服器證書，請選擇*瀏覽*並上傳新檔案。
7. 選擇*繼續*。

   出現編輯金鑰管理伺服器精靈的步驟 3（上傳用戶端憑證）。
8. 如果需要更換用戶端憑證和用戶端憑證私鑰，請選擇*瀏覽*並上傳新檔案。
9. 選擇*測試並儲存*。

   測試金鑰管理伺服器和受影響網站的所有節點加密設備節點之間的連線。如果所有節點連接均有效，並且在 KMS 上找到了正確的金鑰，則金鑰管理伺服器將新增至金鑰管理伺服器頁面的表中。
10. 如果出現錯誤訊息，請查看訊息詳細訊息，然後選擇「確定」。

    例如，如果您為此 KMS 選擇的網站已由另一個 KMS 管理，或連線測試失敗，您可能會收到 422：無法處理的實體錯誤。
11. 如果您需要在解決連線錯誤之前儲存目前配置，請選擇*強制儲存*。

    > 選擇「強制儲存」將儲存 KMS 配置，但不會測試從每個裝置到該 KMS 的外部連線。如果設定有問題，您可能無法重新啟動在受影響網站上啟用了節點加密的裝置節點。在問題解決之前，您可能會無法存取您的資料。

    KMS 配置已儲存。
12. 查看確認警告，如果確定要強制儲存配置，請選擇「確定」。

    KMS 配置已儲存，但未測試與 KMS 的連線。

刪除金鑰管理伺服器 (KMS)

在某些情況下，您可能想要刪除金鑰管理伺服器。例如，如果您已退役該站點，則可能想要刪除特定於站點的 KMS。

開始之前

- 您已審閱"使用金鑰管理伺服器的注意事項和要求"。

- 您已使用"支援的網頁瀏覽器"。
- 你有"Root存取權限"。

關於此任務

您可以在以下情況下刪除 KMS：

- 如果網站已退役或網站不包含啟用了節點加密的裝置節點，則可以刪除網站特定的 KMS。
- 如果每個啟用了節點加密的裝置節點的網站都已存在網站特定的 KMS，則可以刪除預設 KMS。

步驟

1. 選擇 設定 > 安全 > 金鑰管理伺服器。

   出現金鑰管理伺服器頁面，其中顯示所有已設定的金鑰管理伺服器。

2. 選擇要刪除的 KMS，然後選擇*操作* > 刪除。

   您也可以透過選擇表格中的 KMS 名稱並從 KMS 詳細資料頁面中選擇 刪除 來刪除 KMS。

3. 確認以下內容屬實：
   - 您正在刪除沒有啟用節點加密的裝置節點的網站特定 KMS。
   - 您正在刪除預設的 KMS，但每個具有節點加密的網站已經存在網站特定的 KMS。
4. 選擇“是”。

   KMS 配置已被刪除。

管理代理設定

配置儲存代理

如果您正在使用平台服務或雲端儲存池，則可以在儲存節點和外部 S3 端點之間設定非透明代理。例如，您可能需要一個非透明代理來允許將平台服務訊息傳送到外部端點，例如網路上的端點。

配置的儲存代理設定不適用於 Kafka 平台服務端點。

開始之前

- 你有"特定存取權限"。
- 您已使用"支援的網頁瀏覽器"。

關於此任務

您可以配置單一儲存代理程式的設定。

步驟

1. 選擇*配置* > 安全 > 代理設定。
2. 在「儲存」標籤上，選取「啟用儲存代理程式」複選框。

3. 選擇儲存代理的協定。
4. 輸入代理伺服器的主機名稱或 IP 位址。
5. 或者，輸入用於連接代理伺服器的連接埠。

   將此欄位留空以使用協定的預設連接埠：HTTP 為 80，SOCKS5 為 1080。

6. 選擇*儲存*。

   儲存儲存代理程式後，可以設定和測試平台服務或雲端儲存池的新端點。

   代理更改最多可能需要 10 分鐘才能生效。

7. 檢查代理伺服器的設置，以確保來自StorageGRID 的平台服務相關訊息不會被封鎖。
8. 如果您需要停用儲存代理，請清除複選框，然後選擇*儲存*。

配置管理代理設定

如果您使用 HTTP 或 HTTPS 傳送AutoSupport套件，則可以在管理節點和技術支援（AutoSupport）之間設定非透明代理伺服器。

有關AutoSupport的更多信息，請參閱"配置AutoSupport"。

開始之前

- 你有"特定存取權限"。
- 您已使用"支援的網頁瀏覽器"。

關於此任務

您可以配置單一管理代理程式的設定。

步驟

1. 選擇*配置* > 安全 > 代理設定。

   出現“代理設定”頁面。預設情況下，在選項卡選單中選擇“儲存”。

2. 選擇“管理”標籤。
3. 選取“啟用管理代理”複選框。
4. 輸入代理伺服器的主機名稱或 IP 位址。
5. 輸入用於連接代理伺服器的連接埠。
6. （可選）輸入代理伺服器的使用者名稱和密碼。

   如果您的代理伺服器不需要使用者名稱或密碼，請將這些欄位留空。

7. 選擇下列選項之一：

   - 如果您想確保與管理代理程式的連線安全，請選擇*驗證代理證書*。上傳 CA 套件以驗證管理代理伺服器提供的 SSL 憑證的真實性。

如果驗證了代理證書，則按需AutoSupport、透過StorageGRID 的E 系列AutoSupport以及StorageGRID升級頁面上的更新路徑確定將無法運作。

上傳 CA 包後，其元資料就會出現。

。如果您不想在與管理代理伺服器通訊時驗證證書，請選擇*不驗證代理證書*。

8. 選擇*儲存*。

儲存管理代理程式後，管理節點和技術支援之間的代理伺服器就配置好了。

代理更改最多可能需要 10 分鐘才能生效。

9. 如果您需要停用管理代理，請清除*啟用管理代理*複選框，然後選擇*儲存*。

控制防火牆

控制外部防火牆的訪問

您可以在外部防火牆處開啟或關閉特定連接埠。

您可以透過開啟或關閉外部防火牆上的特定連接埠來控制對StorageGRID管理節點上的使用者介面和 API 的存取。例如，除了使用其他方法來控制系統存取之外，您可能還希望阻止租戶連接到防火牆處的網格管理器。

如果要設定StorageGRID內部防火牆，請參閱"配置內部防火牆"。

港口	描述	如果連接埠開放...
443	管理節點的預設 HTTPS 連接埠	Web 瀏覽器和管理 API 用戶端可以存取網格管理器、網格管理 API、租用戶管理器和租用戶管理 API。 *注意：*連接埠 443 也用於一些內部流量。
8443	管理節點上的網格管理器連接埠受限	• Web 瀏覽器和管理 API 用戶端可以使用 HTTPS 存取網格管理器和網格管理 API。 • Web 瀏覽器和管理 API 用戶端無法存取租用戶管理器或租用戶管理 API。 • 內部內容請求將被拒絕。
9443	管理節點上的限制租用戶管理器端口	• Web 瀏覽器和管理 API 用戶端可以使用 HTTPS 存取租用戶管理器和租用戶管理 API。 • Web 瀏覽器和管理 API 用戶端無法存取網格管理器或網格管理 API。 • 內部內容請求將被拒絕。

受限的網格管理器或租戶管理器連接埠上不提供單一登入 (SSO)。如果您希望使用者透過單一登入進行驗證，則必須使用預設 HTTPS 連接埠 (443)。

相關資訊

- "Sign in入網格管理器"
- "建立租用戶帳戶"
- "外部溝通"

管理內部防火牆控制

StorageGRID在每個節點上都包含一個內部防火牆，透過讓您能夠控制對節點的網路存取來增強網格的安全性。使用防火牆阻止除特定網格部署所需連接埠之外的所有連接埠的網路存取。您在防火牆控制頁面上所做的設定變更將部署到每個節點。

使用防火牆控制頁面上的三個標籤來自訂網格所需的存取權限。

- 特權位址清單：使用此標籤允許選擇存取已關閉的連接埠。您可以使用「管理外部存取」標籤以 CIDR 表示法新增可存取已關閉連接埠的 IP 位址或子網路。
- 管理外部存取：使用此選項卡關閉預設開啟的端口，或重新開啟先前關閉的端口。
- 不受信任的客戶端網路：使用此選項卡指定節點是否信任來自客戶端網路的入站流量。

  此標籤上的設定將覆蓋「管理外部存取」標籤中的設定。

  - 具有不受信任的客戶端網路的節點將僅接受該節點上配置的負載平衡器端點連接埠（全域、節點介面和節點類型綁定端點）上的連線。
  - 無論「管理外部網路」標籤上的設定為何，負載平衡器端點連接埠都是不受信任的用戶端網路上唯一開放的連接埠。
  - 當受信任時，管理外部存取標籤下開啟的所有連接埠以及用戶端網路上開啟的任何負載平衡器端點都是可存取的。

> 您在一個選項卡上所做的設定可能會影響您在另一個選項卡上所做的存取變更。請務必檢查所有選項卡上的設置，以確保您的網路按照您預期的方式運作。

若要設定內部防火牆控制，請參閱"配置防火牆控制"。

有關外部防火牆和網路安全的更多信息，請參閱"控制外部防火牆的訪問"。

特權地址清單和管理外部存取選項卡

特權位址清單標籤可讓您註冊一個或多個被授予存取已關閉的網格連接埠的 IP 位址。管理外部存取標籤可讓您關閉對選定外部連接埠或所有開啟的外部連接埠（外部連接埠是預設非網格節點可存取的連接埠）的外部存取。這兩個選項卡通常可以一起使用，以自訂您需要允許電網的精確網路存取。

> 預設情況下，特權 IP 位址沒有內部網格連接埠存取權限。

範例 **1**：使用跳轉主機執行維護任務

假設您想使用跳轉主機（安全強化的主機）進行網路管理。您可以使用以下一般步驟：

1. 使用特權位址清單標籤新增跳轉主機的IP位址。

2. 使用“管理外部存取”標籤來阻止所有連接埠。

> 在封鎖連接埠 443 和 8443 之前新增特權 IP 位址。任何目前連接到被封鎖連接埠的使用者（包括您）都將失去對網格管理器的存取權限，除非他們的 IP 位址已新增至特權位址清單中。

儲存配置後，網格中管理節點上的所有外部連接埠都將被阻止，跳轉主機除外。然後，您可以使用跳轉主機更安全地在電網上執行維護任務。

範例 **2**：鎖定敏感端口

假設您想要鎖定敏感連接埠和該連接埠上的服務（例如，連接埠 22 上的 SSH）。您可以使用以下一般步驟：

1. 使用特權位址清單標籤僅向需要存取該服務的主機授予存取權限。
2. 使用“管理外部存取”標籤來阻止所有連接埠。

> 在阻止存取指派給網格管理器和租用戶管理員的任何連接埠（預設連接埠為 443 和 8443）之前，請新增特權 IP 位址。任何目前連接到被封鎖連接埠的使用者（包括您）都將失去對網格管理器的存取權限，除非他們的 IP 位址已新增至特權位址清單中。

儲存配置後，連接埠 22 和 SSH 服務將可供特權位址清單上的主機使用。無論請求來自哪個接口，所有其他主機都將被拒絕存取該服務。

範例 **3**：停用對未使用的服務的訪問

在網路級別，您可以停用一些您不想使用的服務。例如，要阻止 HTTP S3 用戶端流量，您可以使用「管理外部存取」標籤上的切換按鈕來封鎖連接埠 18084。

不受信任的客戶端網路選項卡

如果您使用用戶端網絡，則可以透過僅在明確配置的端點上接受入站用戶端流量來協助保護StorageGRID免受惡意攻擊。

預設情況下，每個網格節點上的客戶端網路都是_受信任的_。也就是說，預設情況下， StorageGRID信任所有"可用的外部連接埠"。

您可以透過指定每個節點上的用戶端網路為_不受信任的_來減少對StorageGRID系統的惡意攻擊的威脅。如果節點的用戶端網路不受信任，則該節點僅接受明確配置為負載平衡器端點的連接埠上的入站連線。看"配置負載平衡器端點"和"配置防火牆控制"。

範例 **1**：網關節點僅接受 **HTTPS S3** 請求

假設您希望網關節點拒絕用戶端網路上除 HTTPS S3 請求之外的所有入站流量。您將執行以下常規步驟：

1. 從"負載平衡器端點"頁面上，在連接埠 443 上透過 HTTPS 為 S3 配置負載平衡器端點。
2. 從防火牆控制頁面中，選擇不受信任以指定網關節點上的用戶端網路不受信任。

儲存設定後，網關客戶端網路上的所有入站流量都將被丟棄，但連接埠 443 上的 HTTPS S3 請求和 ICMP 回顯（ping）請求除外。

範例 **2**：儲存節點發送 **S3** 平台服務請求

假設您想要啟用來自儲存節點的出站 S3 平台服務流量，但您想要阻止用戶端網路上到該儲存節點的任何入站連線。您將執行以下常規步驟：

- 從防火牆控制頁面的不受信任的用戶端網路標籤中，指示儲存節點上的用戶端網路不受信任。

儲存配置後，儲存節點不再接受客戶端網路上的任何傳入流量，但它繼續允許向配置的平台服務目標發出出站請求。

範例 **3**：將對網格管理器的存取限制在子網路內

假設您只想允許 Grid Manager 存取特定子網路。您將執行以下步驟：

1. 將管理節點的客戶端網路附加到子網路。
2. 使用不受信任的客戶端網路標籤將客戶端網路配置為不受信任。
3. 建立管理介面負載平衡器端點時，輸入連接埠並選擇該連接埠將存取的管理介面。
4. 對於不受信任的客戶端網絡，選擇「是」。
5. 使用「管理外部存取」標籤來封鎖所有外部連接埠（無論是否為該子網路外的主機設定了特權 IP 位址）。

儲存配置後，只有您指定的子網路上的主機才能存取網格管理器。所有其他主機均被封鎖。

配置內部防火牆

您可以設定StorageGRID防火牆來控制對StorageGRID節點上特定連接埠的網路存取。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"特定存取權限"。
- 您已查看了"管理防火牆控制"和"網路指南"。
- 如果您希望管理節點或網關節點僅在明確配置的端點上接受入站流量，則您已定義負載平衡器端點。

> 變更客戶端網路的配置時，如果尚未配置負載平衡器端點，則現有客戶端連線可能會失敗。

關於此任務

StorageGRID在每個節點上都包含一個內部防火牆，可讓您開啟或關閉網格節點上的某些連接埠。您可以使用防火牆控制標籤來開啟或關閉網格網路、管理網路和用戶端網路上預設開啟的連接埠。您也可以建立可以存取已關閉的網格連接埠的特權 IP 位址清單。如果您使用用戶端網絡，您可以指定節點是否信任來自客戶端網路的入站流量，並且可以設定客戶端網路上特定連接埠的存取。

將對網格外部 IP 位址開放的連接埠數量限制為僅絕對必要的端口，可增強網格的安全性。您使用三個防火牆控制標籤上的設定來確保僅開啟所需的連接埠。

有關使用防火牆控制的詳細資訊（包括範例），請參閱"管理防火牆控制"。

有關外部防火牆和網路安全的更多信息，請參閱"控制外部防火牆的訪問"。

存取防火牆控制

步驟

1. 選擇*設定* > 安全 > 防火牆控制。

   此頁面上的三個選項卡的描述如下"管理防火牆控制"。

2. 選擇任意選項卡來配置防火牆控制。

   您可以按任意順序使用這些選項卡。您在一個選項卡上設定的配置不會限制您在其他選項卡上可以執行的操作；但是，您在一個選項卡上所做的配置更改可能會更改在其他選項卡上配置的連接埠的行為。

特權地址列表

您可以使用「特權位址清單」標籤授予主機對預設關閉或透過「管理外部存取」標籤上的設定關閉的連接埠的存取權。

預設情況下，特權 IP 位址和子網路沒有內部網格存取權限。此外，即使在「管理外部存取」標籤中被阻止，也可以存取在「特權位址清單」標籤中開啟的負載平衡器端點和其他連接埠。

「特權位址清單」標籤上的設定不能覆蓋「不受信任的用戶端網路」標籤上的設定。

步驟

1. 在特權位址清單標籤上，輸入要授予對封閉連接埠的存取權限的位址或 IP 子網路。
2. 或者，選擇*以 CIDR 表示法新增另一個 IP 位址或子網路*來新增其他特權用戶端。

   將盡可能少的地址添加到特權清單中。

3. 或者，選擇*允許特權 IP 位址存取StorageGRID內部連接埠*。看"StorageGRID內部連接埠" 。

   此選項刪除了一些內部服務的保護。如果可能的話，將其保持禁用狀態。

4. 選擇*儲存*。

管理外部訪問

當在「管理外部存取」標籤中關閉某個端口時，任何非網格 IP 位址都無法存取該端口，除非您將該 IP 位址新增至特權位址清單。您只能關閉預設開啟的端口，並且只能打開您已關閉的端口。

「管理外部存取」標籤上的設定不能覆蓋「不受信任的用戶端網路」標籤上的設定。例如，如果某個節點不受信任，則即使在「管理外部存取」標籤上開啟了連接埠 SSH/22，該連接埠也會在用戶端網路上被封鎖。不受信任的客戶端網路標籤上的設定將覆蓋客戶端網路上的已關閉連接埠（例如 443、8443、9443）。

步驟

1. 選擇*管理外部存取*。此標籤顯示一個表，其中包含網格中節點的所有外部連接埠（預設非網格節點可存取的連接埠）。
2. 使用以下選項配置要開啟和關閉的連接埠：

- 使用每個連接埠旁邊的開關來開啟或關閉選定的連接埠。
- 選擇*開啟所有顯示的連接埠*以開啟表中列出的所有連接埠。
- 選擇*關閉所有顯示的連接埠*以關閉表中列出的所有連接埠。

> 如果您關閉 Grid Manager 連接埠 443 或 8443，則目前連接到封鎖連接埠的任何使用者（包括您）都會失去對 Grid Manager 的存取權限，除非他們的 IP 位址已新增至特權位址清單中。

> 使用表格右側的捲軸確保您已查看所有可用連接埠。使用搜尋欄位輸入連接埠號碼來尋找任何外部連接埠的設定。您可以輸入部分連接埠號碼。例如，如果輸入 **2**，則會顯示名稱中包含字串「2」的所有連接埠。

3. 選擇“儲存”

不受信任的客戶端網絡

如果節點的用戶端網路不受信任，則該節點僅接受配置為負載平衡器端點的連接埠上的入站流量，以及（可選）您在此標籤上選擇的其他連接埠。您也可以使用此標籤指定擴充功能中新增的新節點的預設值。

> 如果尚未配置負載平衡器端點，現有客戶端連線可能會失敗。

您在「不受信任的用戶端網路」標籤上所做的設定變更將覆蓋「管理外部存取」標籤上的設定。

步驟

1. 選擇*不受信任的客戶端網路*。
2. 在「設定新節點預設值」部分中，指定在擴充過程中將新節點新增至網格時的預設設定。
   - 受信任（預設）：當在擴充功能中新增節點時，其客戶端網路是受信任的。
   - 不受信任：當在擴展中添加節點時，其客戶端網路不受信任。

   根據需要，您可以返回此選項卡來更改特定新節點的設定。

   > 此設定不會影響StorageGRID系統中的現有節點。

3. 使用下列選項來選擇應僅允許在明確配置的負載平衡器端點或其他選定連接埠上進行用戶端連線的節點：
   - 選擇*不信任顯示的節點*將表中顯示的所有節點新增至不受信任的客戶端網路清單。
   - 選擇「信任顯示的節點」以從不受信任的客戶端網路清單中刪除表中顯示的所有節點。
   - 使用每個節點旁邊的切換按鈕將所選節點的客戶端網路設定為受信任或不受信任。

   例如，您可以選擇*不信任顯示的節點*將所有節點新增至不受信任的用戶端網路清單中，然後使用單一節點旁的切換按鈕將該單一節點新增至受信任的用戶端網路清單。

   > 使用表格右側的捲軸確保您已查看所有可用節點。使用搜尋欄位輸入節點名稱來尋找任何節點的設定。您可以輸入部分名稱。例如，如果輸入 **GW**，則會顯示名稱中包含字串「GW」的所有節點。

4. 選擇*儲存*。

新的防火牆設定將立即套用並強制執行。如果尚未配置負載平衡器端點，現有客戶端連線可能會失敗。

管理租戶

什麼是租戶帳戶？

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

此版本的文件網站已刪除 Swift 詳細資訊。看 "StorageGRID 11.8：管理租戶"。

身為網格管理員，您可以建立和管理 S3 用戶端用於儲存和擷取物件的租用戶帳戶。

每個租用戶帳戶都有聯合或本機群組、使用者、S3 儲存桶和物件。

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

- *企業用例：*如果您在企業應用程式中管理StorageGRID系統，您可能想要按組織中的不同部門隔離網格的物件儲存。在這種情況下，您可以為行銷部門、客戶支援部門、人力資源部門等建立租戶帳戶。

  如果您使用 S3 用戶端協議，則可以使用 S3 儲存桶和儲存桶策略在企業各部門之間隔離物件。您不需要使用租用戶帳戶。請參閱實施說明"S3 儲存桶和儲存桶策略"了解更多。

- *服務提供者使用案例：*如果您作為服務提供者管理StorageGRID系統，則可以透過租用網格儲存的不同實體來隔離網格的物件儲存。在這種情況下，您將為公司 A、公司 B、公司 C 等建立租戶帳戶。

有關更多信息，請參閱"使用租用戶帳戶" 。

如何建立租用戶帳戶？

使用網格管理器建立租戶帳戶。建立租用戶帳戶時，請指定以下資訊：

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

此外，如果 S3 租用戶帳戶需要遵守監管要求，您可以為StorageGRID系統啟用 S3 物件鎖定設定。啟用 S3 物件鎖定後，所有 S3 租用戶帳戶都可以建立和管理相容的儲存桶。

租戶管理器有什麼用途？

建立租用戶帳戶後，租用戶用戶可以登入租用戶管理員執行下列任務：

- 設定身份聯合（除非身份來源與網格共享）

- 管理群組和用戶
- 使用網格聯合進行帳戶克隆和跨網格複製
- 管理 S3 存取密鑰
- 建立和管理 S3 儲存桶
- 使用 S3 平台服務
- 使用 S3 Select
- 監控儲存使用情況

雖然 S3 租用戶用戶可以使用租用戶管理器建立和管理 S3 存取金鑰和儲存桶，但他們必須使用 S3 用戶端應用程式來提取和管理物件。看"使用 S3 REST API"了解詳情。

建立租用戶帳戶

您必須建立至少一個租用戶帳戶來控制對StorageGRID系統中儲存的存取。

建立租用戶帳戶的步驟取決於"身分聯合"和"單一登入"是否配置，以及用於建立租用戶帳戶的網格管理器帳戶是否屬於具有 Root 存取權限的管理員群組。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"根存取權限或租用戶帳戶權限"。
- 如果租用戶帳戶將使用為網格管理員配置的身分來源，並且您想要將租用戶帳戶的 Root 存取權限授予聯合群組，則您已將該組合群組匯入網格管理器。您不需要為該管理群組指派任何網格管理器權限。看"管理管理員群組" 。
- 如果您希望允許 S3 租用戶複製帳戶資料並使用網格聯合連線將儲存桶物件複製到另一個網格：
  - 你有"配置電網聯合連接"。
  - 連線狀態為*已連線*。
  - 您擁有 Root 存取權限。
  - 您已查看了以下注意事項"管理電網聯合的允許租戶"。
  - 如果租用戶帳戶將使用為網格管理器配置的身分來源，則您已將相同的聯合群組匯入兩個網格上的網格管理器。

    當您建立租用戶時，您將選擇此群組以擁有來源和目標租用戶帳戶的初始 Root 存取權。

如果在建立租用戶之前兩個網格上都不存在此管理群組，則該租用戶不會被複製到目標。

訪問嚮導

步驟

1. 選擇*租戶*。
2. 選擇“創建”。

輸入詳細信息

步驟

1. 輸入租戶的詳細資料。

場地	描述
Name	租戶帳戶的名稱。租戶名稱不需要是唯一的。建立租用戶帳戶時，它會收到一個唯一的 20 位元帳戶 ID。
描述（可選）	幫助識別租戶的描述。 如果您正在建立將使用網格聯合連線的租用戶，則可以選擇使用此欄位來協助識別哪個是來源租用戶，哪一個是目標租用戶。例如，在網格 1 上建立的租戶的描述也會出現在複製到網格 2 的租戶中：“此租戶是在網格 1 上建立的。”
客戶端類型	此租戶將使用的用戶端協定類型，**S3** 或 **Swift**。 注意：對 Swift 用戶端應用程式的支援已被棄用，並將在未來的版本中刪除。
儲存配額（可選）	如果您希望該租用戶擁有儲存配額，請為配額和單位指定一個數值。

2. 選擇*繼續*。

選擇權限

步驟

1. 或者，選擇您希望此租用戶擁有的基本權限。

其中一些權限有額外的要求。有關詳細信息，請選擇每個權限的幫助圖示。

允許	如果選擇...
允許平台服務	租戶可以使用CloudMirror等S3平台服務。看"管理 S3 租戶帳戶的平台服務" 。
使用自己的身分來源	租用戶可以為聯合群組和使用者配置和管理自己的身分來源。如果您有以下情況，則此選項被停用"設定 SSO"適用於您的StorageGRID系統。
允許 S3 選擇	租用戶可以發出 S3 SelectObjectContent API 請求來過濾和擷取物件資料。看"管理租用戶帳戶的 S3 Select" 。 重要：SelectObjectContent 請求可能會降低所有 S3 用戶端和所有租用戶的負載平衡器效能。僅在需要時且僅對受信任的租戶啟用此功能。

2. 或者，選擇您希望此租用戶擁有的高級權限。

允許	如果選擇...
電網聯合連接	租戶可以使用電網聯合連接，它可以： • 導致此租戶以及新增至帳戶的所有租用戶群組和使用者從此網格（來源網格）複製到所選連接中的另一個網格（目標網格）。 • 允許此租戶在每個網格上的相應儲存桶之間配置跨網格複製。 看"管理電網聯合的允許租戶"。
S3 對象鎖	允許租用戶使用 S3 Object Lock 的特定功能： • 設定最長保留期 定義從提取新物件開始，新增至此儲存桶的新物件應保留多長時間。 • *允許合規模式*可防止使用者在保留期間內覆寫或刪除受保護的物件版本。

3. 選擇*繼續*。

定義根存取權限並建立租用戶

步驟

1. 根據您的StorageGRID系統是否使用身分聯合、單一登入 (SSO) 或兩者，定義租用戶帳戶的根存取權限。

選項	執行此操作
如果未啟用身份聯合	指定以本機 root 使用者身分登入租用戶時所使用的密碼。
如果啟用了身份聯合	a. 選擇一個現有的聯合群組，為租用戶提供 Root 存取權限。 b. 或者，指定以本機 root 使用者身分登入租用戶時所使用的密碼。
如果同時啟用身份聯合和單一登入 (SSO)	選擇一個現有的聯合群組，為租用戶提供 Root 存取權限。沒有本地用戶可以登入。

2. 選擇*建立租戶*。

出現成功訊息，並且新租戶會列在「租戶」頁面上。若要了解如何查看租戶詳細資訊和監控租戶活動，請參閱"監控租戶活動"。

> 根據網路連線、節點狀態和 Cassandra 操作，在整個網格中套用租用戶設定可能需要 15 分鐘或更長時間。

3. 如果您為租用戶選擇了「使用網格聯合連線」權限：
   a. 確認相同的租戶已複製到連接中的另一個網格。兩個網格上的租戶將具有相同的 20 位元帳戶 ID、名稱、描述、配額和權限。

> 如果您看到錯誤訊息“建立租用戶時沒有複製”，請參閱"解決網格聯合錯誤"。

b. 如果您在定義 root 存取權時提供了本機 root 使用者密碼，"更改本機 root 使用者的密碼"對於複製的租戶。

本機 root 使用者在密碼變更之前無法登入目標網格上的租用戶管理員。

Sign in租戶（可選）

根據需要，您可以立即登入新租戶以完成配置，也可以稍後登入租戶。登入步驟取決於您是否使用預設連接埠（443）或受限連接埠登入網格管理器。看"控制外部防火牆的訪問" 。

立即Sign in

如果您正在使用...	這樣做...
連接埠 443 並為本機 root 使用者設定密碼	1. 選擇*以 rootSign in*。 當您登入時，會出現用於設定儲存桶、身分聯合、群組和使用者的連結。 2. 選擇連結來配置租用戶帳戶。 每個連結都會開啟租戶管理器中的對應頁面。若要完成該頁面，請參閱"租戶帳戶使用說明"。
連接埠 443 且您沒有為本機 root 使用者設定密碼	選擇*Sign in*，然後輸入根存取聯合群組中使用者的憑證。
受限連接埠	1. 選擇“完成” 2. 在租用戶表中選擇「受限」以了解有關存取此租用戶帳戶的詳細資訊。 租用戶管理員的 URL 格式如下： `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/` ◦ `FQDN_or_Admin_Node_IP`是管理節點的完全限定網域名稱或 IP 位址 ◦ `port`是僅限租用戶的連接埠 ◦ `20-digit-account-id`是租戶的唯一帳戶ID

稍後Sign in

如果您正在使用...	做其中之一...
埠 443	• 從網格管理員中，選擇 **TENANTS**，然後選擇租用戶名稱右側的 **Sign in**。 • 在 Web 瀏覽器中輸入租用戶的 URL： `https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/` ◦ `FQDN_or_Admin_Node_IP`是管理節點的完全限定網域名稱或 IP 位址 ◦ `20-digit-account-id`是租戶的唯一帳戶ID
受限連接埠	• 從網格管理員中，選擇*TENANTS*，然後選擇*Restricted*。 • 在 Web 瀏覽器中輸入租用戶的 URL： `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id` ◦ `FQDN_or_Admin_Node_IP`是管理節點的完全限定網域名稱或 IP 位址 ◦ `port`是僅限租用戶的限制端口 ◦ `20-digit-account-id`是租戶的唯一帳戶ID

配置租戶

按照"使用租用戶帳戶"管理租戶群組和使用者、S3 存取密鑰、儲存桶、平台服務以及帳戶克隆和跨網格複製。

編輯租戶帳戶

您可以編輯租用戶帳戶以變更顯示名稱、儲存配額或租用戶權限。

如果租用戶具有*使用網格聯合連線*權限，您可以從連線中的任一網格編輯租用戶詳細資料。但是，您在連接中的一個網格上所做的任何變更都不會複製到另一個網格。如果您希望租戶詳細資料在網格之間保持完全同步，請在兩個網格上進行相同的編輯。看"管理允許的電網聯合連接租戶" 。

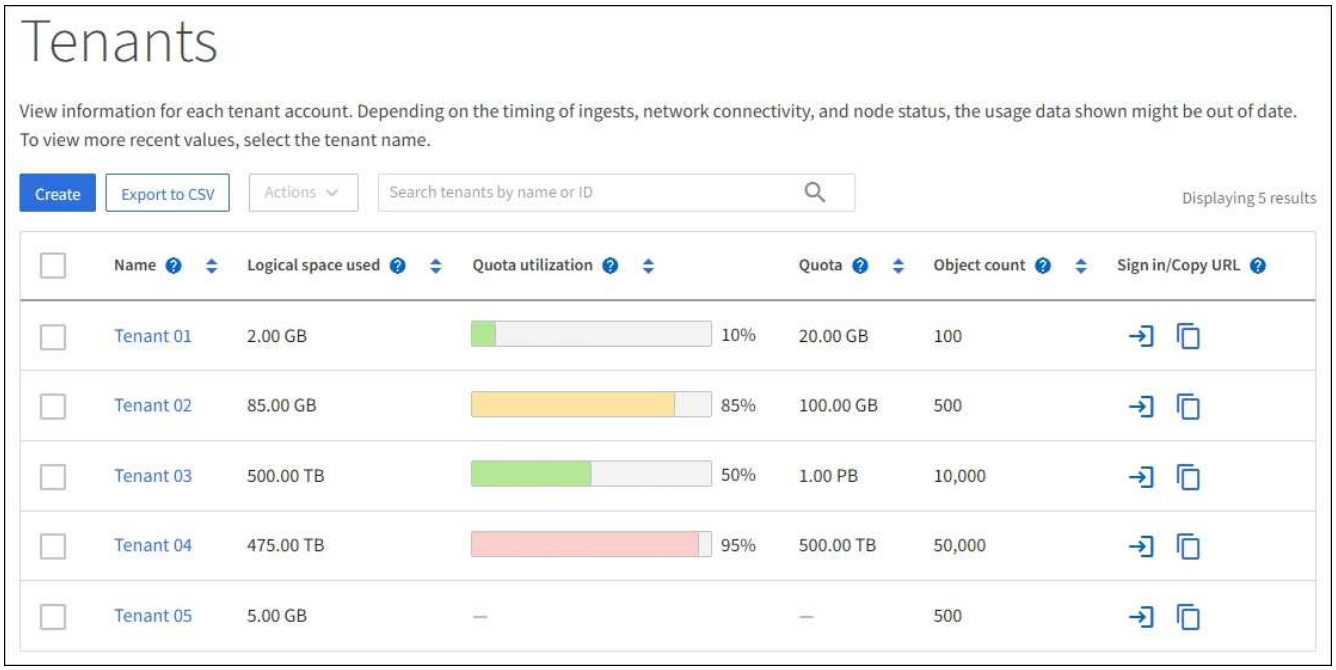
開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"根存取權限或租用戶帳戶權限"。

根據網路連線、節點狀態和 Cassandra 操作，在整個網格中套用租用戶設定可能需要 15 分鐘或更長時間。

步驟

1. 選擇*租戶*。



2. 找到您要編輯的租用戶帳戶。

   使用搜尋框按名稱或租戶 ID 搜尋租戶。

3. 選擇租戶。您可以執行下列任一操作：
   - 選取租戶的複選框，然後選擇*操作* > 編輯。
   - 選擇租戶名稱以顯示詳細資訊頁面，然後選擇*編輯*。
4. （可選）更改以下欄位的值：
   - 姓名
   - 描述
   - 儲存配額
5. 選擇*繼續*。
6. 選擇或清除租用戶帳戶的權限。
   - 如果您為已經在使用平台服務的租戶停用該服務，則他們為其 S3 儲存桶配置的服務將停止運作。沒有向租戶發送任何錯誤訊息。例如，如果租戶已為 S3 儲存桶配置了 CloudMirror 複製，他們仍然可以將物件儲存在儲存桶中，但這些物件的副本將不再在他們已配置為端點的外部 S3 儲存桶中製作。看"管理 S3 租戶帳戶的平台服務" 。
   - 變更*使用自己的身分來源*的設置，以決定租用戶帳戶是否使用其自己的身分來源或為網格管理員配置的身分來源。

     如果*使用自己的身份來源*是：

     - 停用並選中，租戶已經啟用了自己的身份來源。租用戶必須先停用其身分來源，然後才能使用為網格管理員配置的身份來源。
     - 停用且未選擇， StorageGRID系統啟用 SSO。租戶必須使用為網格管理器配置的身份來源。
   - 根據需要選擇或清除*允許 S3 選擇*權限。看"管理租用戶帳戶的 S3 Select" 。

- 若要刪除 使用網格聯合連線 權限：
  i. 選擇*網格聯合*選項卡。
  ii. 選擇*刪除權限*。
- 若要新增*使用網格聯合連線*權限：
  i. 選擇*網格聯合*選項卡。
  ii. 勾選“使用電網聯合連接”複選框。
  iii. 或者，選擇“克隆現有的本機使用者和群組”以將它們複製到遠端網格。如果需要，您可以停止正在進行的克隆，或者如果在上次克隆操作完成後某些本地用戶或群組克隆失敗，則可以重試克隆。
- 要設定最長保留期或允許合規模式：

  您必須先在網格上啟用 S3 物件鎖定，然後才能使用這些設定。

  i. 選擇“**S3** 物件鎖定”標籤。
  ii. 對於*設定最長保留期*，輸入值並從下拉式選單中選擇時間段。
  iii. 對於*允許合規模式*，選取複選框。

更改租戶本地 **root** 使用者的密碼

如果根使用者被鎖定在帳戶之外，您可能需要變更租用戶本機根使用者的密碼。

開始之前

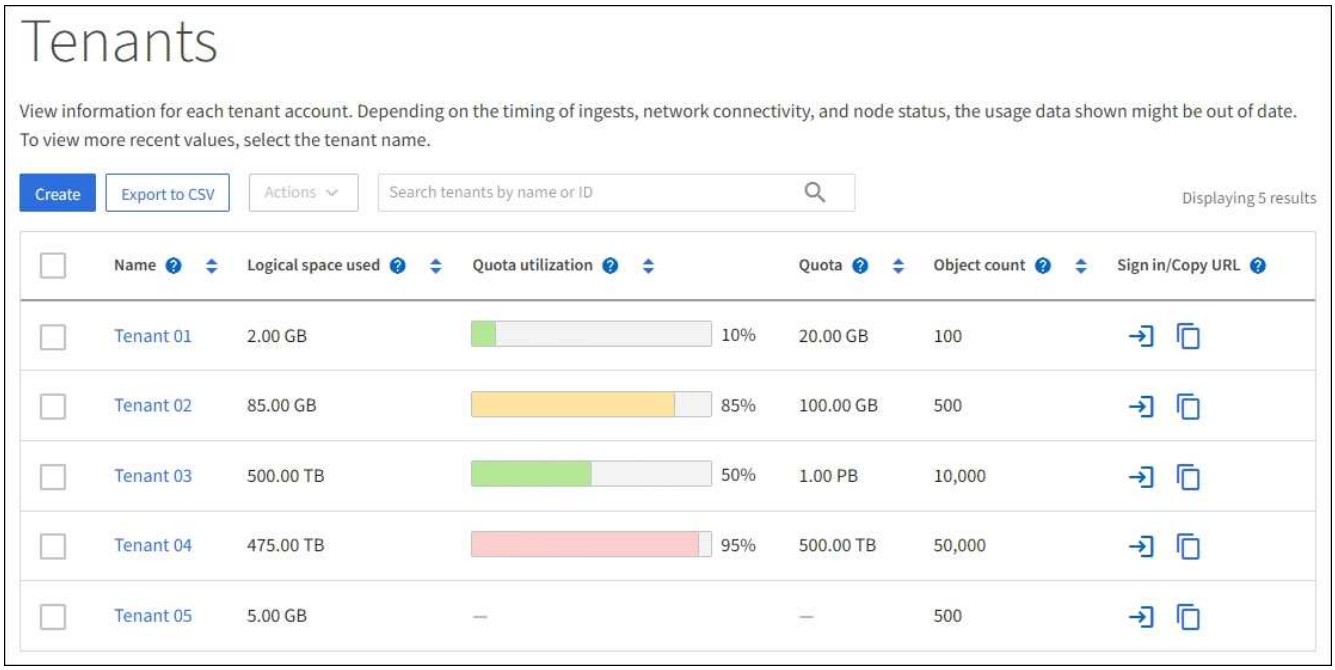
- 您已使用"支援的網頁瀏覽器"。
- 你有"特定存取權限"。

關於此任務

如果您的StorageGRID系統啟用了單一登入 (SSO)，則本機根使用者無法登入租用戶帳號。若要執行 root 使用者任務，使用者必須屬於具有租用戶的 Root 存取權限的聯合群組。

步驟

1. 選擇*租戶*。



2. 選擇租戶帳戶。您可以執行下列任一操作：
   - 選取租用戶的複選框，然後選擇*操作*>*更改 root 密碼*。
   - 選擇租用戶的名稱以顯示詳細資料頁面，然後選擇*操作*>*變更 root 密碼*。
3. 輸入租用戶帳戶的新密碼。
4. 選擇*儲存*。

刪除租用戶帳戶

如果您想永久刪除租用戶對系統的存取權限，您可以刪除租用戶帳戶。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"特定存取權限"。
- 您已刪除與租用戶帳戶相關聯的所有 S3 儲存桶和物件。
- 如果允許租戶使用電網聯合連接，您已查看了以下注意事項"刪除具有使用網格聯合連線權限的租用戶"。

步驟

1. 選擇*租戶*。
2. 找到您要刪除的一個或多個租用戶帳戶。

   使用搜尋框按名稱或租戶 ID 搜尋租戶。

3. 若要刪除多個租用戶，請選取核取方塊並選擇*操作* > 刪除。
4. 若要刪除單一租用戶，請執行下列操作之一：
   - 選取複選框，然後選擇*操作* > 刪除。
   - 選擇租戶名稱以顯示詳細資訊頁面，然後選擇*操作*>*刪除*。

5. 選擇“是”。

管理平台服務

什麼是平台服務？

平台服務包括CloudMirror複製、事件通知和搜尋整合服務。

如果您為 S3 租用戶帳戶啟用平台服務，則必須設定網格，以便租用戶可以存取使用這些服務所需的外部資源。

CloudMirror 複製

StorageGRID CloudMirror 複製服務用於將特定物件從StorageGRID桶鏡像到指定的外部目標。

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

> CloudMirror 複製與跨網格複製功能有一些重要的相似之處和差異。要了解更多信息，請參閱"比較跨網格複製和 CloudMirror 複製"。

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

通知

每個儲存桶事件通知用於將有關對物件執行的特定操作的通知傳送到指定的外部 Kafka 叢集或 Amazon Simple Notification Service。

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

> 雖然可以在啟用了 S3 物件鎖定的儲存桶上配置事件通知，但物件的 S3 物件鎖定元資料（包括保留截止日期和合法保留狀態）將不會包含在通知訊息中。

搜尋整合服務

搜尋整合服務用於將 S3 物件元資料傳送到指定的 Elasticsearch 索引，在那裡可以使用外部服務搜尋或分析元資料。

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

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

平台服務使租戶能夠使用外部儲存資源、通知服務以及對其資料的搜尋或分析服務。由於平台服務的目標位置通常位於StorageGRID部署的外部，因此您必須決定是否允許租用戶使用這些服務。如果您這樣做，則必須在建立或編輯租用戶帳戶時啟用平台服務的使用。您還必須配置您的網絡，以便租戶產生的平台服務訊息能夠到達目的地。

在使用平台服務之前，請注意以下建議：

- 如果StorageGRID系統中的 S3 儲存桶同時啟用了版本控制和 CloudMirror 複製，則也應該為目標端點啟用 S3 儲存桶版本控制。這允許 CloudMirror 複製在端點上產生類似的物件版本。
- 您不應使用超過 100 個需要 CloudMirror 複製、通知和搜尋整合的 S3 請求的活動租戶。擁有超過 100 個活躍租戶可能會導致 S3 用戶端效能下降。
- 對無法完成的端點的請求將排隊，最多 500,000 個請求。此限制由活躍租戶平均分擔。允許新租戶暫時超過這個 500,000 的限制，以便新創建的租戶不會受到不公平的懲罰。

相關資訊

- "管理平台服務"
- "配置儲存代理設定"
- "監控StorageGRID"

平台服務的網路和端口

如果您允許 S3 租用戶使用平台服務，則必須為網格配置網路以確保平台服務訊息能夠傳遞到其目的地。

您可以在建立或更新租用戶帳戶時為 S3 租用戶帳戶啟用平台服務。如果啟用了平台服務，租用戶可以建立端點作為 CloudMirror 複製、事件通知或從其 S3 儲存桶搜尋整合訊息的目標。這些平台服務訊息從執行 ADC 服務的儲存節點傳送到目標端點。

例如，租用戶可能會配置以下類型的目標端點：

- 本地託管的 Elasticsearch 集群
- 支援接收 Amazon Simple Notification Service 訊息的本機應用程式
- 本機託管的 Kafka 集群
- 位於同一或另一個StorageGRID實例上的本機託管的 S3 儲存桶
- 外部端點，例如 Amazon Web Services 上的端點。

為了確保平台服務訊息能夠傳遞，您必須配置包含 ADC 儲存節點的網路。您必須確保以下連接埠可用於將平台服務訊息傳送至目標端點。

預設情況下，平台服務訊息在以下連接埠發送：

- **80**：適用於以 http 開頭的端點 URI（大多數端點）
- **443**：適用於以 https 開頭的端點 URI（大多數端點）
- **9092**：對於以 http 或 https 開頭的端點 URI（僅限 Kafka 端點）

租戶在建立或編輯端點時可以指定不同的連接埠。

> 如果使用StorageGRID部署作為 CloudMirror 複製的目標，則可能會在 80 或 443 以外的連接埠上收到複製訊息。確保在端點中指定目標StorageGRID部署用於 S3 的連接埠。

如果您使用非透明代理伺服器，您還必須"配置儲存代理設定"允許將訊息傳送到外部端點，例如網路上的端點。

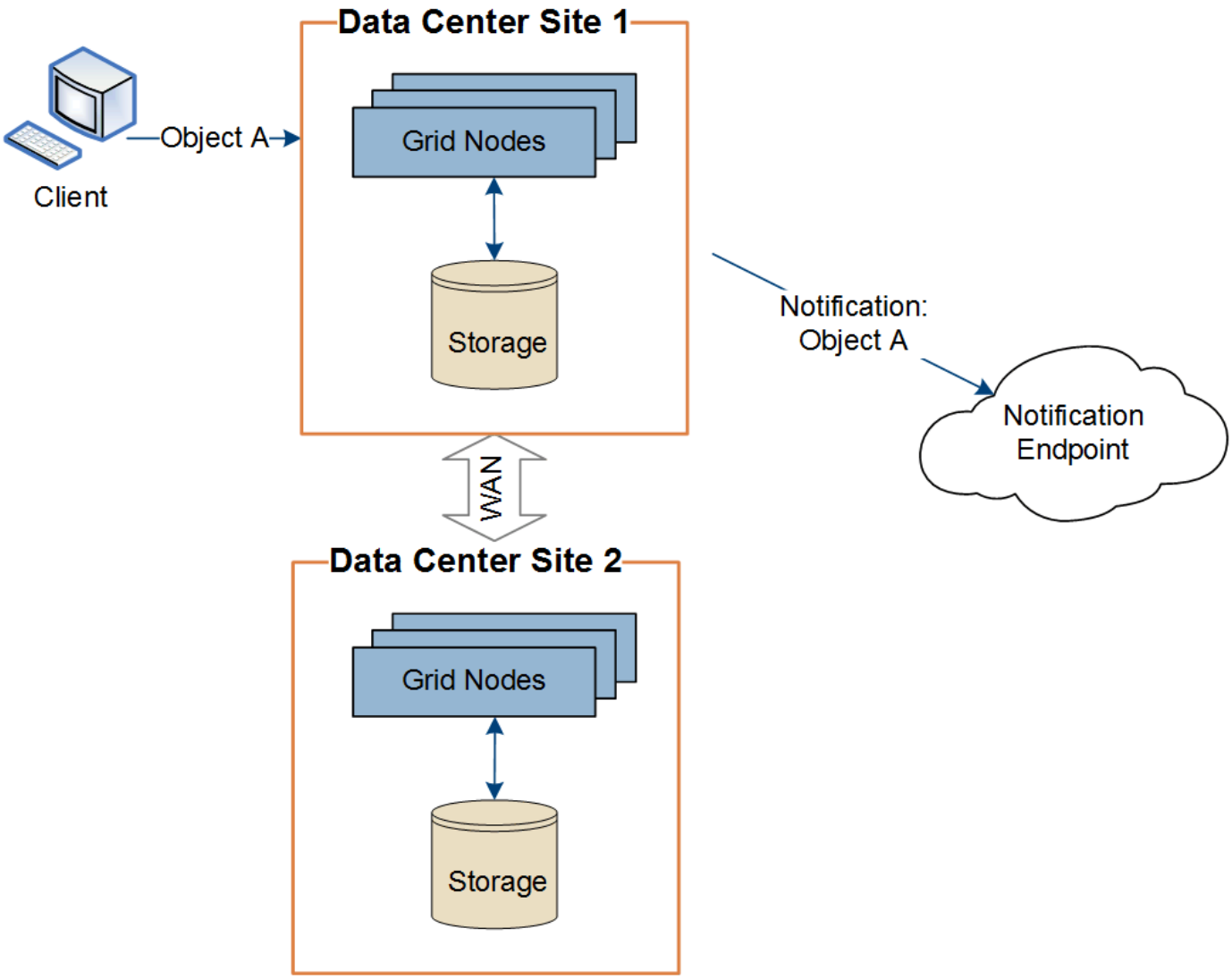
相關資訊

"使用租用戶帳戶"

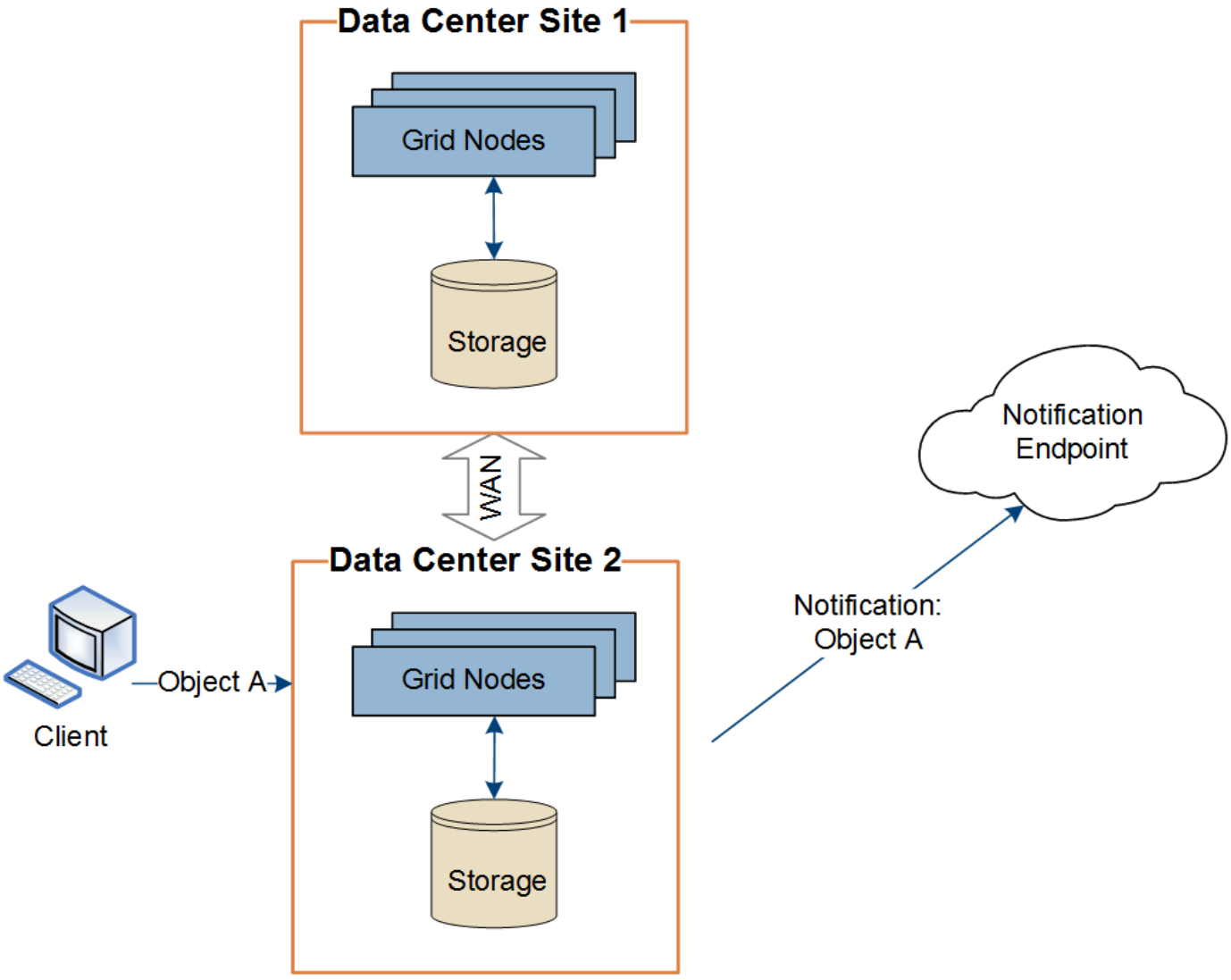
按站點傳遞平台服務訊息

所有平台服務操作均依站點執行。

也就是說，如果租用戶使用用戶端透過連接到資料中心站點 1 的網關節點對物件執行 S3 API 建立操作，則會從資料中心站點 1 觸發並發送有關該操作的通知。



如果用戶端隨後從資料中心站點 2 對相同物件執行 S3 API 刪除操作，則會觸發有關刪除操作的通知並從資料中心站點 2 傳送。



確保每個站點的網路配置都能夠使平台服務訊息傳送到目的地。

平台服務故障排除

平台服務中使用的端點由租用戶用戶在租用戶管理器中建立和維護；但是，如果租用戶在配置或使用平台服務時遇到問題，您可能能夠使用網格管理器來協助解決問題。

新端點的問題

在租用戶可以使用平台服務之前，他們必須使用租用戶管理器建立一個或多個端點。每個端點代表一個平台服務的外部目標，例如StorageGRID S3 儲存桶、Amazon Web Services 儲存桶、Amazon Simple Notification Service 主題、Kafka 主題或在本機或 AWS 上託管的 Elasticsearch 叢集。每個端點都包含外部資源的位置和存取該資源所需的憑證。

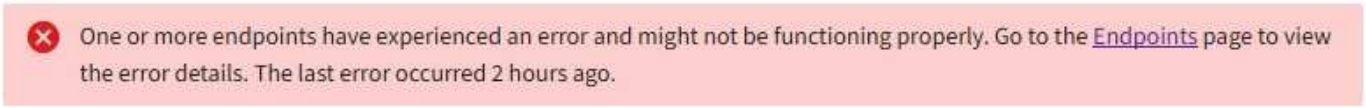
當租用戶建立端點時， StorageGRID系統會驗證該端點是否存在以及是否可以使用指定的憑證存取該端點。每個站點的一個節點都會驗證與端點的連線。

如果端點驗證失敗，錯誤訊息會解釋端點驗證失敗的原因。租用戶用戶應解決該問題，然後嘗試再次建立端點。

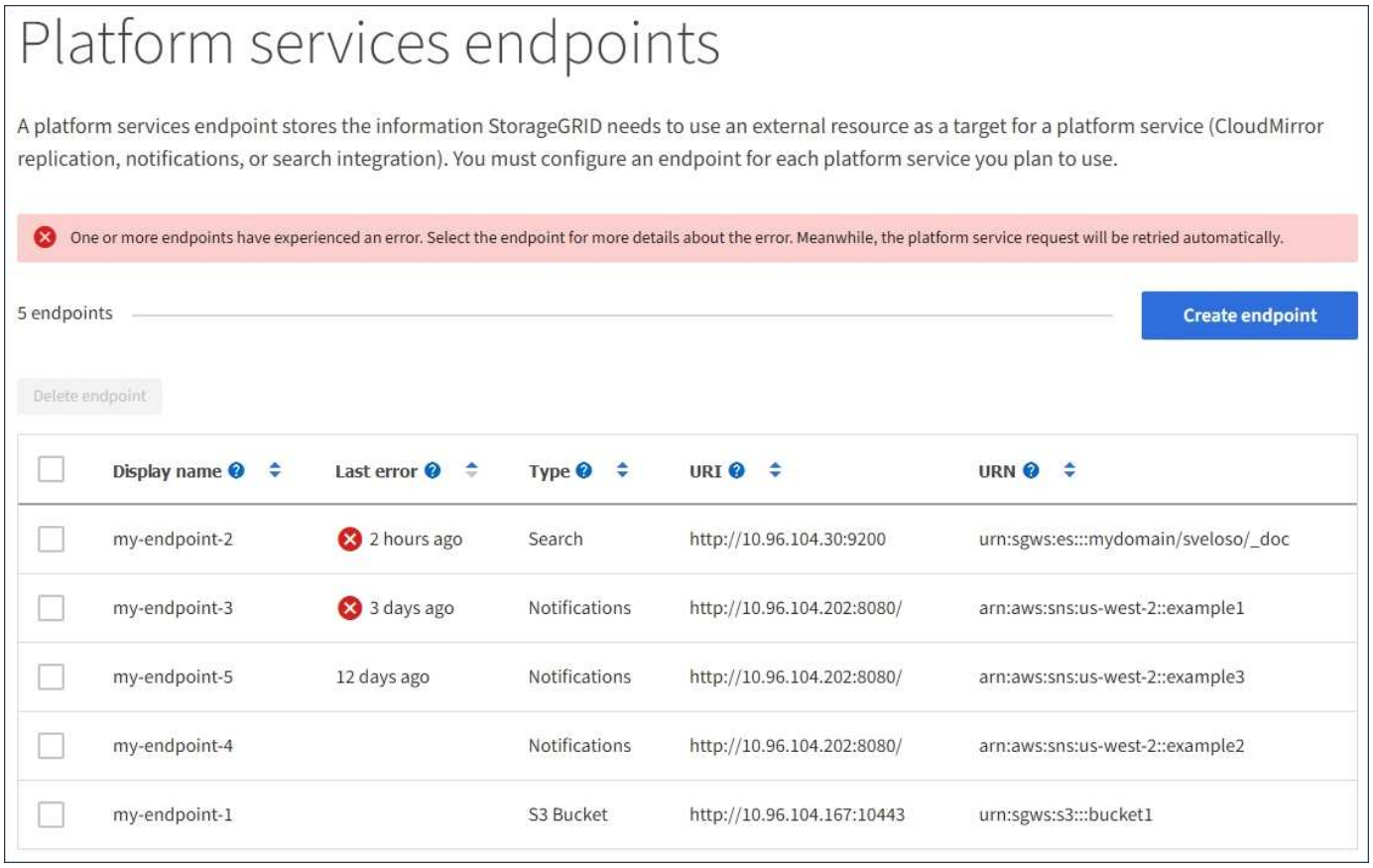
如果未為租用戶帳戶啟用平台服務，則端點建立將會失敗。

現有端點的問題

如果StorageGRID嘗試存取現有端點時發生錯誤，則會在租用戶管理員的儀表板上顯示一則訊息。



租用戶用戶可以前往「端點」頁面查看每個端點的最新錯誤訊息，並確定錯誤發生的時間。 *上次錯誤*列顯示每個端點的最新錯誤訊息，並指示錯誤發生的時間。錯誤包括圖示出現在過去 7 天內。



Last error 欄位中的某些錯誤訊息可能包含括號中的 logID。網格管理員或技術支援可以使用此 ID 在 bycast.log 中查找有關錯誤的更多詳細資訊。

與代理伺服器相關的問題

如果您已配置"儲存代理"在儲存節點和平台服務端點之間，如果您的代理服務不允許來自StorageGRID的訊息，則可能會發生錯誤。若要解決這些問題，請檢查代理伺服器的設置，以確保與平台服務相關的訊息不會被封鎖。

確定是否發生錯誤

如果過去 7 天內發生任何端點錯誤，租用戶管理員中的儀表板將顯示一則警報訊息。您可以前往「端點」頁面查看有關該錯誤的更多詳細資訊。

客戶端操作失敗

某些平台服務問題可能會導致 S3 儲存桶上的用戶端操作失敗。例如，如果內部複製狀態機 (RSM) 服務停止，或排隊等待傳送的平台服務訊息太多，S3 用戶端操作將會失敗。

檢查服務狀態：

1. 選擇*支援* > 工具 > 網格拓撲。
2. 選擇 ***site*** > ***Storage Node*** > **SSM** > **Services**。

可恢復和不可恢復的端點錯誤

端點建立後，平台服務請求可能會因各種原因而發生錯誤。某些錯誤可以透過使用者介入來恢復。例如，可恢復的錯誤可能由於以下原因而發生：

- 用戶的憑證已被刪除或已過期。
- 目標儲存桶不存在。
- 通知無法送達。

如果StorageGRID遇到可恢復的錯誤，則會重試平台服務請求，直到成功為止。

其他錯誤是無法恢復的。例如，如果刪除端點，則會發生不可恢復的錯誤。

如果StorageGRID遇到無法復原的端點錯誤：

- 在網格管理員中，前往 支援 > 工具 > 指標 > **Grafana** > 平台服務概述 查看錯誤詳情。
- 在租用戶管理員中，前往 儲存 **(S3)** > 平台服務端點 查看錯誤詳情。
- 檢查 `/var/local/log/bycast-err.log`相關錯誤。具有 ADC 服務的儲存節點包含此日誌檔案。

平台服務訊息無法傳遞

如果目標遇到無法接受平台服務訊息的問題，則儲存桶上的用戶端操作會成功，但平台服務訊息不會被傳遞。例如，如果在目標上更新憑證，使得StorageGRID無法再對目標服務進行身份驗證，則可能會發生此錯誤。

檢查相關警報。

平台服務請求效能較慢

如果傳送請求的速率超過目標端點接收請求的速率， StorageGRID軟體可能會限制儲存桶的傳入 S3 請求。只有當有大量請求等待傳送到目標端點時才會發生限制。

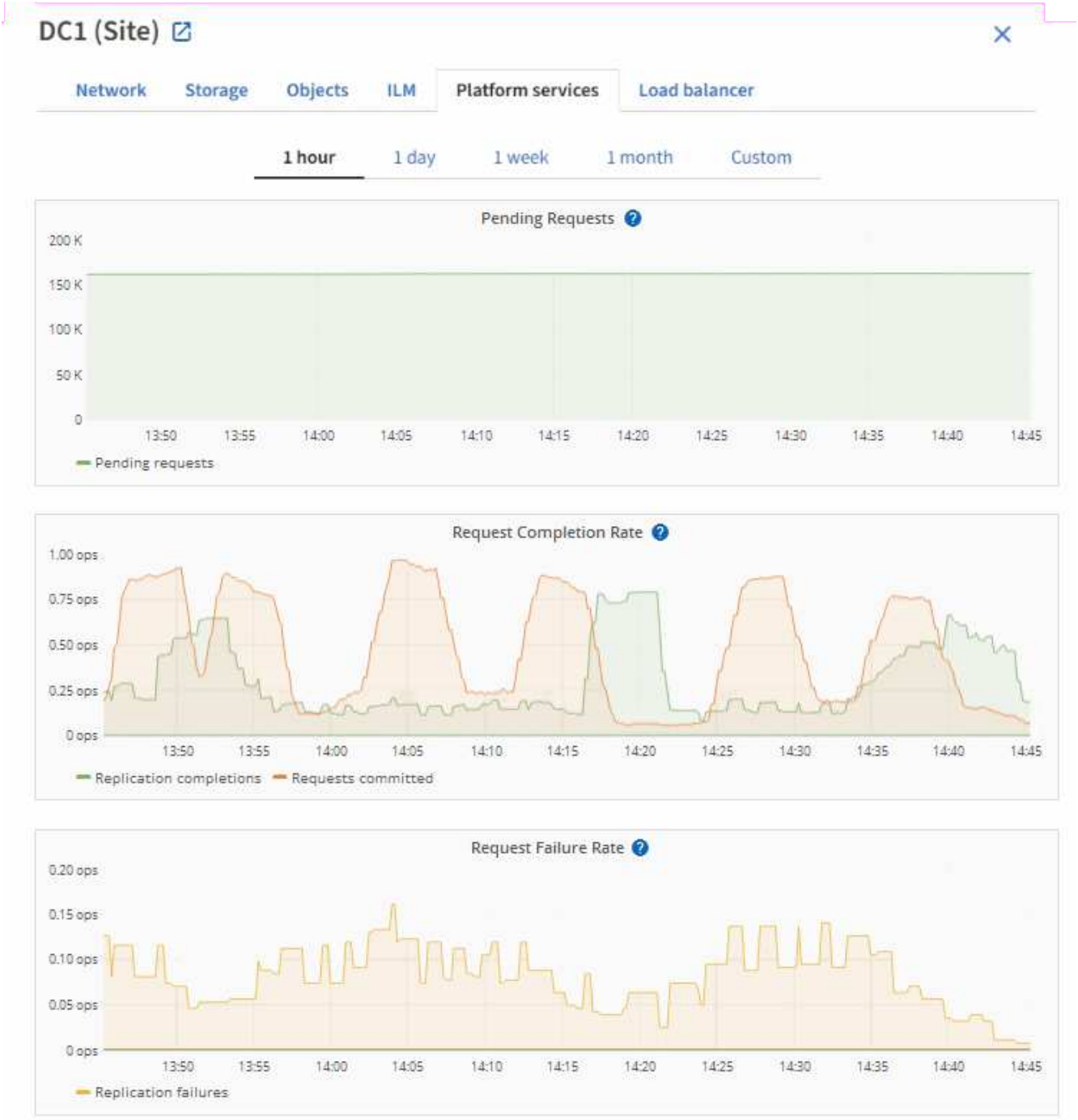
唯一可見的效果是傳入的 S3 請求將需要更長時間才能執行。如果您開始偵測到效能明顯下降，則應降低攝取率或使用容量更高的端點。如果積壓的請求持續增加，客戶端 S3 操作（例如 PUT 請求）最終將會失敗。

CloudMirror 請求更有可能受到目標端點效能的影響，因為這些請求通常涉及比搜尋整合或事件通知請求更多的資料傳輸。

平台服務請求失敗

查看平台服務的請求失敗率：

1. 選擇*NODES*。
2. 選擇 ***site*** > 平台服務。
3. 查看請求錯誤率圖表。



平台服務不可用警報

*平台服務不可用*警報表示站點上無法執行任何平台服務操作，因為正在運行或可用的具有 RSM 服務的儲存節點太少。

RSM 服務確保平台服務請求傳送到各自的端點。

若要解決此警報，請確定網站中的哪些儲存節點包含 RSM 服務。（RSM 服務存在於也包含 ADC 服務的儲存節點上。）然後，確保這些儲存節點中的大多數都在運行並且可用。

> 如果某個站點上包含 RSM 服務的多個儲存節點發生故障，您將遺失該站點的所有待處理的平台服務請求。

平台服務端點的其他故障排除指南

有關更多信息，請參閱使用租用戶帳戶 › 平台服務端點故障排除。

相關資訊

"排除StorageGRID系統故障"

管理租用戶帳戶的 S3 Select

您可以允許某些 S3 租用戶使用 S3 Select 對單一物件發出 SelectObjectContent 請求。

S3 Select 提供了一種有效的方法來搜尋大量數據，而無需部署資料庫和相關資源來實現搜尋。它還降低了檢索資料的成本和延遲。

什麼是 S3 Select？

S3 Select 允許 S3 用戶端使用 SelectObjectContent 請求來過濾和檢索物件所需的資料。 S3 Select 的StorageGRID實作包括 S3 Select 指令和功能的子集。

使用 S3 Select 的注意事項和要求

電網管理要求

網格管理員必須授予租用戶 S3 Select 能力。當選擇“允許 S3 選擇”時"建立租戶"或者"編輯租戶"。

物件格式要求

您要查詢的物件必須採用以下格式之一：

- **CSV**。可原樣使用或壓縮為 GZIP 或 BZIP2 檔案。
- 鑲木地板。 Parquet 物件的附加要求：
  - S3 Select 僅支援使用 GZIP 或 Snappy 進行列壓縮。 S3 Select 不支援 Parquet 物件的整個物件壓縮。
  - S3 Select 不支援 Parquet 輸出。您必須將輸出格式指定為 CSV 或 JSON。
  - 未壓縮的行組最大大小為 512 MB。
  - 您必須使用物件模式中指定的資料類型。
  - 您不能使用 INTERVAL、JSON、LIST、TIME 或 UUID 邏輯類型。

端點要求

SelectObjectContent 請求必須傳送到"StorageGRID負載平衡器端點"。

端點使用的管理節點和網關節點必須是以下之一：

- 服務設備節點
- 基於 VMware 的軟體節點
- 運行啟用了 cgroup v2 的核心的裸機節點

一般考慮

查詢不能直接傳送到儲存節點。

SelectObjectContent 請求可能會降低所有 S3 用戶端和所有租用戶的負載平衡器效能。僅在需要時且僅對受信任的租戶啟用此功能。

查看"S3 Select 使用說明"。

查看"Grafana 圖表"對於 S3 選擇隨時間推移的操作，在網格管理器中選擇 **SUPPORT** > **Tools** > **Metrics**。

設定客戶端連接

配置 **S3** 用戶端連接

身為網格管理員，您可以管理設定選項，控制 S3 用戶端應用程式如何連接到您的StorageGRID系統以儲存和擷取資料。

此版本的文件網站已刪除 Swift 詳細資訊。看 "StorageGRID 11.8：設定 S3 和 Swift 用戶端連接"。

配置任務

1. 根據客戶端應用程式連接到StorageGRID的方式，在StorageGRID中執行先決條件任務。

必需任務

您必須獲得：

- IP 位址
- 網域
- SSL 憑證

選用任務

可選地，配置：

- 身分聯合
- 單一登入

1. 使用StorageGRID取得應用程式連接到網格所需的值。您可以使用 S3 設定精靈或手動設定每個StorageGRID實體。+

使用 **S3** 設定精靈

請依照 S3 設定精靈中的步驟進行操作。

手動配置

1. 建立高可用性群組
2. 建立負載平衡器端點
3. 建立租用戶帳戶
4. 建立儲存桶和存取金鑰
5. 配置 ILM 規則和策略

1. 使用 S3 應用程式完成與StorageGRID 的連線。建立 DNS 項目以將 IP 位址與您計劃使用的任何網域名稱關聯。

   根據需要，執行額外的應用程式設定。

2. 在應用程式和StorageGRID中執行持續任務，以管理和監控物件儲存。

將**StorageGRID**附加到客戶端應用程式所需的信息

在將StorageGRID連接到 S3 用戶端應用程式之前，您必須在StorageGRID中執行設定步驟並取得某些值。

我需要什麼價值觀？

下表顯示了您必須在StorageGRID中配置的值以及 S3 應用程式和 DNS 伺服器使用這些值的位置。

價值	配置值的位置	價值的使用地點
虛擬 IP (VIP) 位址	StorageGRID > HA 群組	DNS 項目
港口	StorageGRID > 負載平衡器端點	客戶端應用程式
SSL 憑證	StorageGRID > 負載平衡器端點	客戶端應用程式
伺服器名稱 (FQDN)	StorageGRID > 負載平衡器端點	• 客戶端應用程式 • DNS 項目
S3 存取金鑰 ID 和秘密存取金鑰	StorageGRID > 租用戶與儲存桶	客戶端應用程式
儲存桶/容器名稱	StorageGRID > 租用戶與儲存桶	客戶端應用程式

我如何獲得這些值？

根據您的要求，您可以執行以下操作之一來獲取所需的資訊：

- 使用**"S3 設定嚮導"**. S3 設定精靈可協助您快速設定StorageGRID中所需的值，並輸出一個或兩個在設定 S3 應用程式時可使用的檔案。此精靈將引導您完成所需的步驟，並協助確保您的設定符合StorageGRID最佳實務。

  如果您正在配置 S3 應用程序，建議使用 S3 設定嚮導，除非您知道您有特殊要求或您的實施需要大量自訂。

- 使用**"FabricPool設定精靈"**.與 S3 設定精靈類似， FabricPool設定精靈可協助您快速配置所需的值並輸出一個文件，您可以在ONTAP中設定FabricPool雲層時使用該文件。

  如果您打算使用StorageGRID作為FabricPool雲層的物件儲存系統，建議使用FabricPool設定精靈，除非您知道您有特殊要求或您的實作需要大量自訂。

- 手動配置項目。如果您要連線至 S3 應用程式且不想使用 S3 設定精靈，則可以透過手動執行設定來取得所需的值。請依照以下步驟操作：

  a. 配置您想要用於 S3 應用程式的高可用性 (HA) 群組。看"配置高可用性組" 。

  b. 建立 S3 應用程式將使用的負載平衡器端點。看"配置負載平衡器端點" 。

  c. 建立 S3 應用程式將使用的租用戶帳戶。看"建立租用戶帳戶" 。

  d. 對於 S3 租用戶，登入租用戶帳戶，並為將存取應用程式的每個使用者產生存取金鑰 ID 和秘密存取金鑰。看"建立您自己的存取金鑰" 。

  e. 在租用戶帳戶內建立一個或多個 S3 儲存桶。關於 S3，請參閱"建立 S3 儲存桶"。

  f. 若要為屬於新租用戶或儲存桶/容器的物件新增特定的放置說明，請建立新的 ILM 規則並啟動新的 ILM 策略以使用該規則。看"建立 ILM 規則"和"建立 ILM 策略"。

S3 用戶端的安全性

StorageGRID租用戶帳戶使用 S3 用戶端應用程式將物件資料儲存到StorageGRID。您應該檢查針對客戶端應用程式實施的安全措施。

總結

以下列表總結如何實現 S3 REST API 的安全性：

連線安全
: TLS

伺服器身份驗證
: 由系統 CA 簽署的 X.509 伺服器憑證或由管理員提供的自訂伺服器憑證

客戶端身份驗證
: S3 帳戶存取金鑰 ID 和秘密存取金鑰

客戶端授權
: 儲存桶所有權和所有適用的存取控制策略

StorageGRID如何為客戶端應用程式提供安全性

S3 用戶端應用程式可以連接到網關節點或管理節點上的負載平衡器服務，或直接連接到儲存節點。

- 連接到負載平衡器服務的用戶端可以使用 HTTPS 或 HTTP，具體取決於您"配置負載平衡器端點"。

  HTTPS 提供安全的 TLS 加密通信，值得推薦。您必須將安全性憑證附加到端點。

  HTTP 提供的通訊安全性較低，且未加密，因此僅套用於非生產或測試網格。

- 連接到儲存節點的用戶端也可以使用 HTTPS 或 HTTP。

  HTTPS 是預設設置，也是建議的。

  HTTP 提供較不安全、未加密的通信，但可以選擇"已啟用"適用於非生產或測試網格。

- StorageGRID和客戶端之間的通訊使用 TLS 加密。
- 無論負載平衡器端點配置為接受 HTTP 還是 HTTPS 連接，負載平衡器服務和網格內的儲存節點之間的通訊都是加密的。
- 客戶必須提供"HTTP 驗證標頭"到StorageGRID執行 REST API 操作。

安全性憑證和客戶端應用程式

在所有情況下，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系統產生的憑證建立 TLS 連線：

- 當客戶端應用程式連接到負載平衡器服務時，它們使用為負載平衡器端點配置的憑證。每個負載平衡器端點都有自己的證書——要么是網格管理員上傳的自訂伺服器證書，要么是網格管理員在配置端點時在StorageGRID中產生的證書。

  看"負載平衡的注意事項" 。

- 當客戶端應用程式直接連接到儲存節點時，它們要麼使用安裝StorageGRID系統時為儲存節點產生的系統產生的伺服器憑證（由系統憑證授權單位簽署），要麼使用網格管理員為網格提供的單一自訂伺服器憑證。看"新增自訂 S3 API 證書" 。

用戶端應設定為信任簽署其用於建立 TLS 連線的任何憑證的憑證授權單位。

TLS 庫支援的雜湊和加密演算法

StorageGRID系統支援一組用戶端應用程式在建立 TLS 會話時可以使用的密碼套件。若要設定密碼，請前往 設定 > 安全 > 安全設定 並選擇 **TLS** 和 **SSH** 原則。

支援的 TLS 版本

StorageGRID支援 TLS 1.2 和 TLS 1.3。

SSLv3 和 TLS 1.1（或更早版本）不再支援。

使用 S3 設定精靈

使用 S3 設定精靈：注意事項與要求

您可以使用 S3 設定精靈將StorageGRID配置為 S3 應用程式的物件儲存系統。

何時使用 S3 設定嚮導

S3 設定精靈將引導您完成設定StorageGRID以與 S3 應用程式一起使用的每個步驟。作為完成精靈的一部分，您可以下載可用於將值輸入到 S3 應用程式中的檔案。使用精靈可以更快地配置您的系統並確保您的設定符合StorageGRID最佳實務。

如果你有"Root存取權限"，您可以在開始使用StorageGRID Grid Manager 時完成 S3 設定精靈，也可以在以後的任何時間存取並完成該精靈。根據您的要求，您也可以手動配置部分或全部所需項目，然後使用精靈來組裝 S3 應用程式所需的值。

使用精靈之前

在使用該精靈之前，請確認您已完成這些先決條件。

取得 **IP** 位址並設定 **VLAN** 介面

如果您要設定高可用性 (HA) 群組，您就會知道 S3 應用程式將連接到哪些節點以及將使用哪個StorageGRID網路。您也知道要為子網路 CIDR、閘道 IP 位址和虛擬 IP (VIP) 位址輸入哪些值。

如果您打算使用虛擬 LAN 來隔離來自 S3 應用程式的流量，則您已經設定了 VLAN 介面。看"配置VLAN介面" 。

設定身份聯合和 **SSO**

如果您打算對StorageGRID系統使用身分聯合或單一登入 (SSO)，則您已啟用這些功能。您也知道哪個聯合群組應該對 S3 應用程式將使用的租用戶帳戶具有根存取權限。看"使用身分聯合"和"配置單一登入"。

取得並配置域名

您知道要為StorageGRID使用哪一個完全限定網域名稱 (FQDN)。網域名稱伺服器 (DNS) 項目會將此 FQDN 對應到您使用精靈建立的 HA 群組的虛擬 IP (VIP) 位址。

如果您打算使用 S3 虛擬託管式請求，您應該"配置的 S3 端點域名"。建議使用虛擬託管式請求。

審查負載平衡器和安全性證書要求

如果您打算使用StorageGRID負載平衡器，則您已經查看了負載平衡的一般注意事項。您擁有要上傳的憑證或產生憑證所需的值。

如果您打算使用外部（第三方）負載平衡器端點，則您擁有該負載平衡器的完全限定網域名稱（FQDN）、連接埠和憑證。

配置任何電網聯合連接

如果您希望允許 S3 租用戶複製帳戶資料並使用網格聯合連線將儲存桶物件複製到另一個網格，請在啟動精靈之前確認以下內容：

- 你有"配置電網聯合連接"。
- 連線狀態為*已連線*。

- 您擁有 Root 存取權限。

存取並完成 **S3** 設定精靈

您可以使用 S3 設定精靈配置StorageGRID以用於 S3 應用程式。安裝精靈提供了應用程式存取StorageGRID儲存桶和保存物件所需的值。

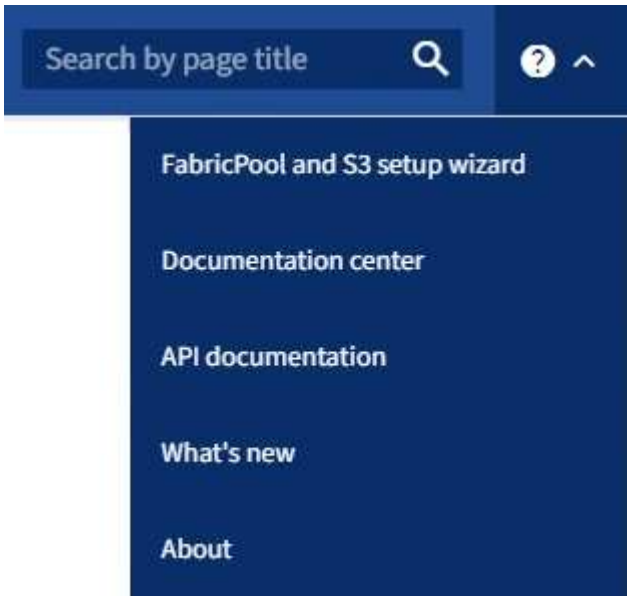
開始之前

- 你有"Root存取權限"。
- 您已審閱"注意事項和要求"使用嚮導。

訪問嚮導

步驟

1. Sign in"支援的網頁瀏覽器"。
2. 如果儀表板上出現 * FabricPool和 S3 設定精靈* 橫幅，請選擇橫幅中的連結。如果橫幅不再出現，請從網格管理器的標題列中選擇幫助圖標，然後選擇* FabricPool和 S3 設定精靈*。



3. 在FabricPool和 S3 設定精靈頁面的 S3 應用程式部分中，選擇 立即配置。

步驟 **1**（共 **6** 步）：配置 **HA** 組

HA 群組是每個包含StorageGRID負載平衡器服務的節點集合。 HA 群組可以包含網關節點、管理節點或兩者。

您可以使用 HA 組來幫助保持 S3 資料連線可用。如果 HA 組中的活動介面發生故障，則備份介面可以管理工作負載，而對 S3 作業的影響很小。

有關此任務的詳細信息，請參閱"管理高可用性組"。

步驟

1. 如果您打算使用外部負載平衡器，則無需建立 HA 群組。選擇“跳過此步驟”並前往第 2 步（共 6 步）：配置負載平衡器端點。

2. 若要使用StorageGRID負載平衡器，您可以建立一個新的 HA 群組或使用現有的 HA 群組。

建立 **HA** 組

a. 若要建立新的 HA 群組，請選擇*建立 HA 組*。

b. 對於*輸入詳細資料*步驟，請填寫以下欄位。

場地	描述
HA組名稱	此 HA 組的唯一顯示名稱。
描述（可選）	該 HA 組的描述。

c. 對於*新增介面*步驟，選擇您想要在此 HA 群組中使用的節點介面。

使用列標題對行進行排序，或輸入搜尋字詞以更快找到介面。

您可以選擇一個或多個節點，但每個節點只能選擇一個介面。

d. 對於*優先考慮介面*步驟，請確定此 HA 群組的主介面和任何備份介面。

拖曳行來變更「優先順序」列中的值。

清單中的第一個介面是主介面。除非發生故障，否則主介面是活動介面。

如果 HA 群組包含多個介面且活動介面發生故障，則虛擬 IP (VIP) 位址將依優先順序移至第一個備份介面。如果該接口發生故障，VIP 位址將移動到下一個備份接口，依此類推。當故障解決後，VIP 位址將移回可用的最高優先權介面。

e. 對於*輸入 IP 位址*步驟，請填寫以下欄位。

場地	描述
子網路 CIDR	CIDR 表示法中的 VIP 子網路位址－IPv4 位址後面接著斜槓和子網路長度（0-32）。 網路位址不得設定任何主機位元。例如， `192.16.0.0/22` 。
網關 IP 位址（可選）	如果用於存取StorageGRID 的S3 IP 位址與StorageGRID VIP 位址不在同一子網路中，請輸入StorageGRID VIP 本機閘道 IP 位址。本機網關IP位址必須在VIP子網路內。
虛擬 IP 位址	為 HA 組中的活動介面輸入至少一個、最多十個 VIP 位址。所有 VIP 位址都必須位於 VIP 子網路內。 至少一個位址必須是 IPv4。您也可以選擇指定其他 IPv4 和 IPv6 位址。

f. 選擇*建立 HA 組*，然後選擇*完成*返回 S3 設定精靈。

g. 選擇“繼續”進入負載平衡器步驟。

使用現有的 **HA** 組

a. 若要使用現有的 HA 組，請從 選擇 **HA** 組 中選擇 HA 組名稱。

b. 選擇“繼續”進入負載平衡器步驟。

第 **2** 步（共 **6** 步）：配置負載平衡器端點

StorageGRID使用負載平衡器來管理來自用戶端應用程式的工作負載。負載平衡可最大限度地提高多個儲存節點的速度和連接容量。

您可以使用所有閘道器和管理節點上存在的StorageGRID負載平衡器服務，也可以連接到外部（第三方）負載平衡器。建議使用StorageGRID負載平衡器。

有關此任務的詳細信息，請參閱"負載平衡的注意事項"。

若要使用StorageGRID負載平衡器服務，請選擇 * StorageGRID負載平衡器* 選項卡，然後建立或選擇要使用的負載平衡器端點。若要使用外部負載平衡器，請選擇“外部負載平衡器”標籤並提供有關已配置的系統的詳細資訊。

建立端點

步驟

1. 若要建立負載平衡器端點，請選擇*建立端點*。
2. 對於*輸入端點詳細資料*步驟，請填寫以下欄位。

場地	描述
Name	端點的描述性名稱。
港口	您想要用於負載平衡的StorageGRID連接埠。對於您建立的第一個端點，此欄位預設為 10433，但您可以輸入任何未使用的外部連接埠。如果輸入 80 或 443，則端點僅在網關節點上配置，因為這些連接埠在管理節點上保留。 *注意：*不允許使用其他網格服務使用的連接埠。查看"網路連接埠參考"。
客戶端類型	必須是*S3*。
網路協定	選擇 **HTTPS**。 注意：支援但不建議使用沒有 TLS 加密的StorageGRID進行通訊。

3. 對於*選擇綁定模式*步驟，指定綁定模式。綁定模式控制如何使用任意 IP 位址或使用特定 IP 位址和網路介面存取端點。

模式	描述
全域（預設）	用戶端可以使用任何網關節點或管理節點的 IP 位址、任何網路上任何 HA 群組的虛擬 IP (VIP) 位址或對應的 FQDN 存取端點。 除非您需要限制此端點的可存取性，否則請使用*全域*設定（預設）。
HA 群組的虛擬 IP	用戶端必須使用 HA 群組的虛擬 IP 位址（或對應的 FQDN）來存取此端點。 具有此綁定模式的端點都可以使用相同的連接埠號，只要您為端點選擇的 HA 群組不重疊。
節點介面	用戶端必須使用選定節點介面的 IP 位址（或對應的 FQDN）來存取此端點。
節點類型	根據您選擇的節點類型，用戶端必須使用任何管理節點的 IP 位址（或對應的 FQDN）或任何網關節點的 IP 位址（或對應的 FQDN）來存取此端點。

4. 對於租戶存取步驟，選擇以下選項之一：

場地	描述
允許所有租戶（預設）	所有租用戶帳戶都可以使用此端點存取他們的儲存桶。
允許選定的租戶	只有選定的租用戶帳戶可以使用此端點存取他們的儲存桶。
阻止選定的租戶	選定的租用戶帳戶不能使用此端點存取其儲存桶。所有其他租戶都可以使用此端點。

5. 對於*附加憑證*步驟，選擇以下之一：

場地	描述
上傳證書（推薦）	使用此選項上傳 CA 簽署的伺服器憑證、憑證私鑰和可選的 CA 套件。
產生證書	使用此選項產生自簽名憑證。看"配置負載平衡器端點"了解輸入內容的詳細資訊。
使用StorageGRID S3 證書	僅當您已上傳或產生StorageGRID全域憑證的自訂版本時才使用此選項。看"配置 S3 API 證書"了解詳情。

6. 選擇“完成”返回 S3 安裝精靈。
7. 選擇“繼續”進入租戶和儲存桶步驟。

端點憑證的變更可能需要長達 15 分鐘才能套用到所有節點。

使用現有的負載平衡器端點

步驟

1. 若要使用現有端點，請從*選擇負載平衡器端點*中選擇其名稱。
2. 選擇“繼續”進入租戶和儲存桶步驟。

使用外部負載平衡器

步驟

1. 若要使用外部負載平衡器，請填寫以下欄位。

場地	描述
完全限定域名 (FQDN)	外部負載平衡器的完全限定網域名稱 (FQDN)。
港口	S3 應用程式將用於連接外部負載平衡器的連接埠號碼。
證書	複製外部負載平衡器的伺服器憑證並將其貼上到此欄位中。

2. 選擇“繼續”進入租戶和儲存桶步驟。

步驟 **3**（共 **6** 步）：建立租用戶和儲存桶

租用戶是可以使用 S3 應用程式在StorageGRID中儲存和擷取物件的實體。每個租戶都有自己的使用者、存取金鑰、儲存桶、物件和一組特定的功能。

bucket 是用於儲存租用戶的物件和物件元資料的容器。儘管租戶可能擁有多個儲存桶，但精靈可以協助您以最快捷、最簡單的方式建立租用戶和儲存桶。如果您稍後需要新增儲存桶或設定選項，則可以使用租用戶管理器。

有關此任務的詳細信息，請參閱"建立租用戶帳戶"和"建立 S3 儲存桶"。

步驟

1. 輸入租用戶帳戶的名稱。

   租戶名稱不需要是唯一的。建立租用戶帳戶時，它會收到一個唯一的數位帳戶 ID。

2. 根據您的StorageGRID系統是否使用，定義租用戶帳戶的根存取權限"身分聯合"，"單一登入（SSO）"，或兩者兼而有之。

選項	執行此操作
如果未啟用身份聯合	指定以本機 root 使用者身分登入租用戶時所使用的密碼。
如果啟用了身份聯合	a. 選擇一個現有的聯合組"Root存取權限"對於租戶來說。 b. 或者，指定以本機 root 使用者身分登入租用戶時所使用的密碼。
如果同時啟用身份聯合和單一登入 (SSO)	選擇一個現有的聯合組"Root存取權限"對於租戶來說。沒有本地用戶可以登入。

3. 如果您希望精靈為根使用者建立存取金鑰 ID 和秘密存取金鑰，請選擇*自動建立根使用者 S3 存取金鑰*。

   如果租戶的唯一用戶是根用戶，請選擇此選項。如果其他使用者要使用此租戶，"使用租戶管理器"配置金鑰和權限。

4. 如果您現在要為該租用戶建立儲存桶，請選擇「為該租用戶建立儲存桶」。

   如果為網格啟用了 S3 物件鎖，則在此步驟中建立的儲存桶未啟用 S3 物件鎖。如果您需要為此 S3 應用程式使用 S3 物件鎖定儲存桶，請不要選擇現在建立儲存桶。相反，使用租戶管理器"建立儲存桶"之後。

   a. 輸入 S3 應用程式將使用的儲存桶的名稱。例如， `s3-bucket` 。

      建立儲存桶後，您無法變更儲存桶名稱。

   b. 選擇此儲存桶的*區域*。

      使用預設區域(`us-east-1`) 除非您期望將來使用 ILM 根據儲存桶的區域過濾物件。

5. 選擇*建立並繼續*。

第 **4** 步（共 **6** 步）：下載數據

在下載資料步驟中，您可以下載一個或兩個檔案來保存剛剛配置的詳細資訊。

步驟

1. 如果您選擇了“自動建立根用戶 S3 存取金鑰”，請執行下列操作之一或全部執行：
   - 選擇*下載存取金鑰*下載 `.csv`包含租用戶帳戶名稱、存取金鑰 ID 和秘密存取金鑰的檔案。
   - 選擇複製圖示 ( ) 將存取金鑰 ID 和秘密存取金鑰複製到剪貼簿。
2. 選擇*下載設定值*來下載 `.txt`包含負載平衡器端點、租用戶、儲存桶和根用戶的設定的檔案。
3. 將此資訊儲存到安全的位置。

> 在複製兩個存取金鑰之前，請勿關閉此頁面。關閉此頁面後，密鑰將不可用。確保將此資訊保存在安全的位置，因為它可用於從StorageGRID系統取得資料。

4. 如果出現提示，請選取核取方塊以確認您已下載或複製金鑰。
5. 選擇“繼續”前往 ILM 規則和策略步驟。

步驟 **5**（共 **6** 步）：查看 **S3** 的 **ILM** 規則和 **ILM** 策略

資訊生命週期管理 (ILM) 規則控制StorageGRID系統中所有物件的放置、持續時間和攝取行為。 StorageGRID 附帶的 ILM 策略為所有物件製作了兩個副本。此策略將一直有效，直到您啟動至少一項新策略為止。

步驟

1. 查看頁面上提供的資訊。
2. 如果您要為屬於新租用戶或儲存桶的物件新增具體說明，請建立新規則和新策略。看"建立 ILM 規則"和"使用 ILM 策略"。
3. 選擇*我已查看這些步驟並了解我需要做什麼*。
4. 選取核取方塊表示您了解下一步該做什麼。
5. 選擇“繼續”前往“摘要”。

第 **6** 步（共 **6** 步）：審核摘要

步驟

1. 查看摘要。
2. 記下後續步驟中的詳細信息，這些詳細資訊描述了連接到 S3 用戶端之前可能需要的附加配置。例如，選擇「以 root 身分Sign in」將帶您進入租用戶管理器，您可以在其中新增租用戶用戶、建立其他儲存桶以及更新儲存桶設定。
3. 選擇*完成*。
4. 使用從StorageGRID下載的檔案或手動取得的值來設定應用程式。

管理 **HA** 組

高可用性 (HA) 群組為 S3 用戶端提供高可用性資料連接，並為網格管理器和租用戶管理器提供高可用性連接。

您可以將多個管理和網關節點的網路介面分組為高可用性 (HA) 群組。如果 HA 群組中的活動介面發生故障，則備用介面可以管理工作負載。

每個 HA 群組提供對選定節點上的共用服務的存取。

- 包含網關節點、管理節點或兩者的 HA 群組為 S3 用戶端提供高可用性資料連線。
- 僅包含管理節點的 HA 群組為網格管理器和租戶管理器提供高可用性連線。
- 僅包含服務設備和基於 VMware 的軟體節點的 HA 群組可以為"使用 S3 Select 的 S3 租用戶"。使用 S3 Select 時建議使用 HA 組，但這不是必需的。

如何建立 **HA** 組？

1. 您為一個或多個管理節點或網關節點選擇一個網路介面。您可以使用網格網路（eth0）介面、客戶端網路（eth2）介面、VLAN 介面或已新增至節點的存取介面。

   如果介面具有 DHCP 指派的 IP 位址，則無法將其新增至 HA 群組。

2. 您指定一個介面作為主介面。除非發生故障，否則主介面是活動介面。
3. 您可以確定任何備份介面的優先順序。
4. 您為該群組指派 1 到 10 個虛擬 IP (VIP) 位址。客戶端應用程式可以使用這些 VIP 位址中的任何一個連接到StorageGRID。

有關說明，請參閱"配置高可用性組"。

活動介面是什麼？

在正常運作期間，HA 組的所有 VIP 位址都會新增至主接口，即優先順序中的第一個介面。只要主介面保持可用，當客戶端連接到該群組的任何 VIP 位址時就會使用它。也就是說，在正常運作期間，主介面是該群組的「活動」介面。

同樣，在正常運作期間，HA 組的任何較低優先權介面都充當「備份」介面。除非主（目前活動）介面不可用，否則不會使用這些備份介面。

查看節點當前**HA**組狀態

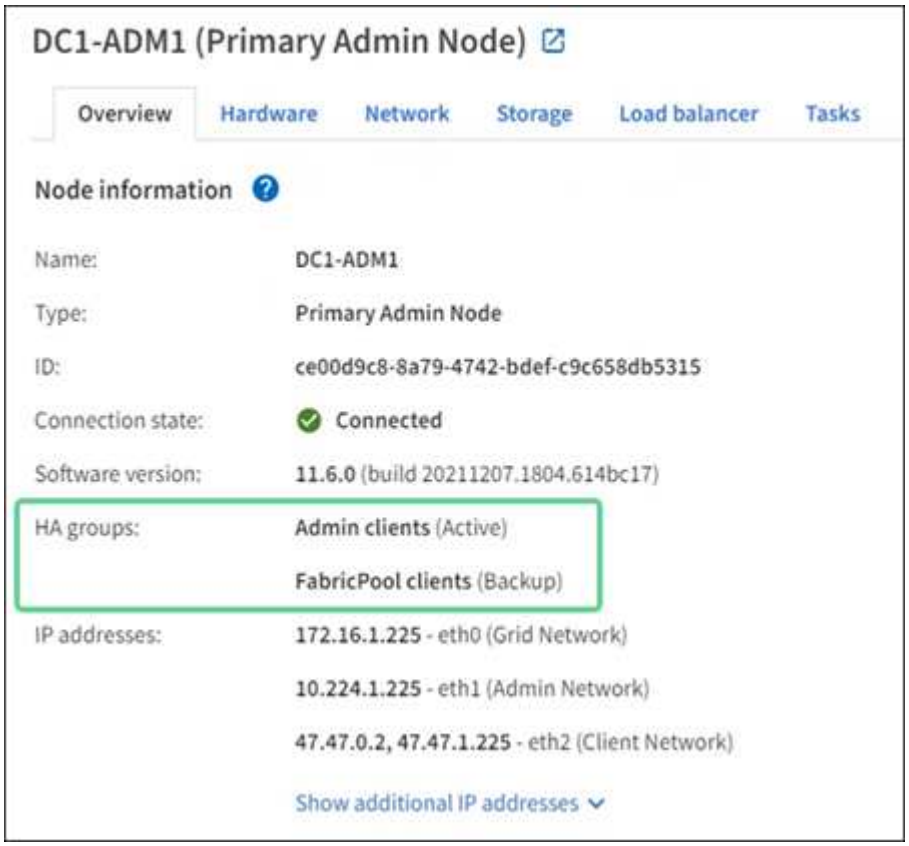
若要查看某個節點是否已指派給 HA 群組並確定其目前狀態，請選擇 **NODES** > ***node***。

如果「概覽」標籤包含「**HA** 群組」條目，則節點將指派給列出的 HA 群組。組名後面的值是該節點在HA組中的目前狀態：

- 活動：HA 群組目前託管在此節點上。
- 備份：HA 群組目前未使用此節點；這是一個備份介面。
- 已停止：由於高可用性（keepalived）服務已被手動停止，因此 HA 群組無法託管在此節點上。

- 故障：由於以下一個或多個原因，HA 群組無法託管在此節點上：
  - 負載平衡器（nginx-gw）服務未在節點上執行。
  - 節點的 eth0 或 VIP 介面已關閉。
  - 節點已關閉。

在此範例中，主管理節點已新增至兩個 HA 群組。該節點目前是管理員客戶端群組的活動介面和FabricPool客戶端群組的備份介面。



當活動介面發生故障時會發生什麼？

目前託管 VIP 位址的介面是活動介面。如果 HA 群組包含多個介面且活動介面發生故障，則 VIP 位址將依優先順序移至第一個可用的備用介面。如果該接口發生故障，VIP 位址將移動到下一個可用的備份接口，依此類推。

下列任一原因都可能觸發故障轉移：

- 配置該介面的節點發生故障。
- 配置此介面的節點與所有其他節點失去連線至少 2 分鐘。
- 活動介面處於 Down 狀態。
- 負載平衡器服務停止。
- 高可用性服務停止。

> 託管活動介面的節點外部的網路故障可能不會觸發故障轉移。同樣，故障轉移不是由網格管理器或租戶管理器的服務觸發的。

故障轉移過程通常只需要幾秒鐘，而且速度足夠快，客戶端應用程式幾乎不會受到任何影響，並且可以依靠正常的重試行為繼續運行。

當故障解決並且更高優先權的介面再次可用時，VIP 位址將自動移至可用的最高優先權介面。

HA 組如何使用？

您可以使用高可用性 (HA) 群組為物件資料和管理用途提供與StorageGRID的高可用性連線。

- HA 群組可以為網格管理器或租用戶管理器提供高可用性管理連線。
- HA 組可以為 S3 用戶端提供高可用性資料連線。
- 僅包含一個介面的 HA 群組可讓您提供多個 VIP 位址並明確設定 IPv6 位址。

只有當群組中包含的所有節點都提供相同的服務時，HA 組才能提供高可用性。建立 HA 群組時，從提供所需服務的節點類型中新增介面。

- 管理節點：包含負載平衡器服務並啟用對網格管理器或租戶管理器的存取。
- 網關節點：包含負載平衡器服務。

HA 組的目的	將此類型的節點新增至 **HA** 群組
存取網格管理器	• 主管理節點（主） • 非主管理節點 *注意：*主管理節點必須是主介面。某些維護程序只能從主管理節點執行。
僅限租戶經理訪問	• 主要或非主要管理節點
S3 用戶端存取權－負載平衡器服務	• 管理節點 • 閘道
S3 用戶端訪問"S3 選擇"	• 服務設備 • 基於 VMware 的軟體節點 注意：使用 S3 Select 時建議使用 HA 組，但這不是必需的。

使用 **HA** 群組與 **Grid Manager** 或 **Tenant Manager** 的限制

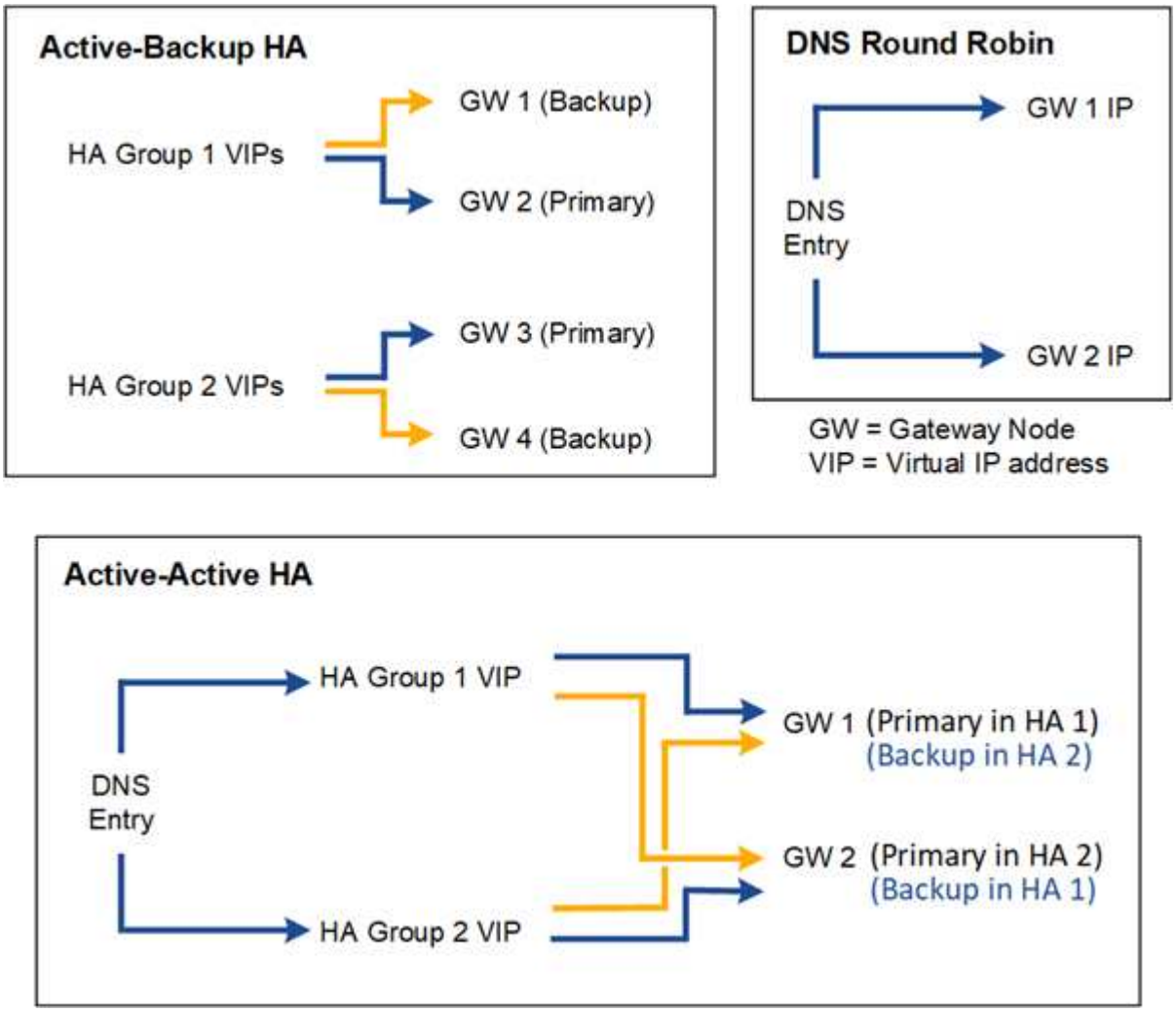
如果網格管理器或租用戶管理器服務發生故障，則不會觸發 HA 群組故障轉移。

如果在發生故障轉移時您已登入網格管理器或租用戶管理器，則您將被登出，並且必須再次登入才能恢復您的任務。

當主管理節點不可用時，某些維護程序無法執行。在故障轉移期間，您可以使用網格管理器來監控您的StorageGRID系統。

下圖提供了配置 HA 組的不同方法的範例。每個選項都有優點和缺點。

圖中藍色表示HA組的主接口，黃色表示HA組內的備援接口。



此表總結了圖中所示的每種 HA 配置的優點。

配置	優勢	缺點
主動備份高可用性	• 由StorageGRID管理，無需任何外部依賴。 • 快速故障轉移。	• HA 組中只有一個節點處於活動狀態。每個 HA 組至少有一個節點處於空閒狀態。
DNS 循環	• 增加總吞吐量。 • 沒有閒置的主機。	• 故障轉移緩慢，這可能取決於客戶端行為。 • 需要在StorageGRID之外配置硬體。 • 需要客戶實施的健康檢查。

配置	優勢	缺點
雙活高可用性	• 流量分佈在多個 HA 組之間。 • 高聚合吞吐量，可隨 HA 組的數量擴展。 • 快速故障轉移。	• 配置更複雜。 • 需要在StorageGRID之外配置硬體。 • 需要客戶實施的健康檢查。

配置高可用性組

您可以設定高可用性 (HA) 群組以提供對管理節點或閘道上的服務的高可用性存取。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"Root存取權限"。
- 如果您打算在 HA 群組中使用 VLAN 接口，則您已經建立了 VLAN 介面。看"配置VLAN介面" 。
- 如果您打算為 HA 群組中的節點使用存取接口，則您已建立該接口：
  - **Red Hat Enterprise Linux**（安裝節點前）："建立節點設定檔"
  - **Ubuntu** 或 **Debian**（安裝節點之前）："建立節點設定檔"
  - **Linux**（安裝節點後）："Linux：為節點新增主幹或存取介面"
  - **VMware**（安裝節點後）："VMware：向節點新增中繼或存取介面"

建立高可用性群組

建立高可用性群組時，您可以選擇一個或多個介面並按優先順序組織它們。然後，為該組分配一個或多個 VIP 位址。

介面必須用於網關節點或管理節點才能包含在 HA 群組中。一個 HA 群組只能為任何給定節點使用一個介面；但是，同一節點的其他介面可以在其他 HA 群組中使用。

訪問嚮導

步驟

1. 選擇 配置 > 網路 > 高可用性群組。
2. 選擇“創建”。

輸入 **HA** 組的詳細信息

步驟

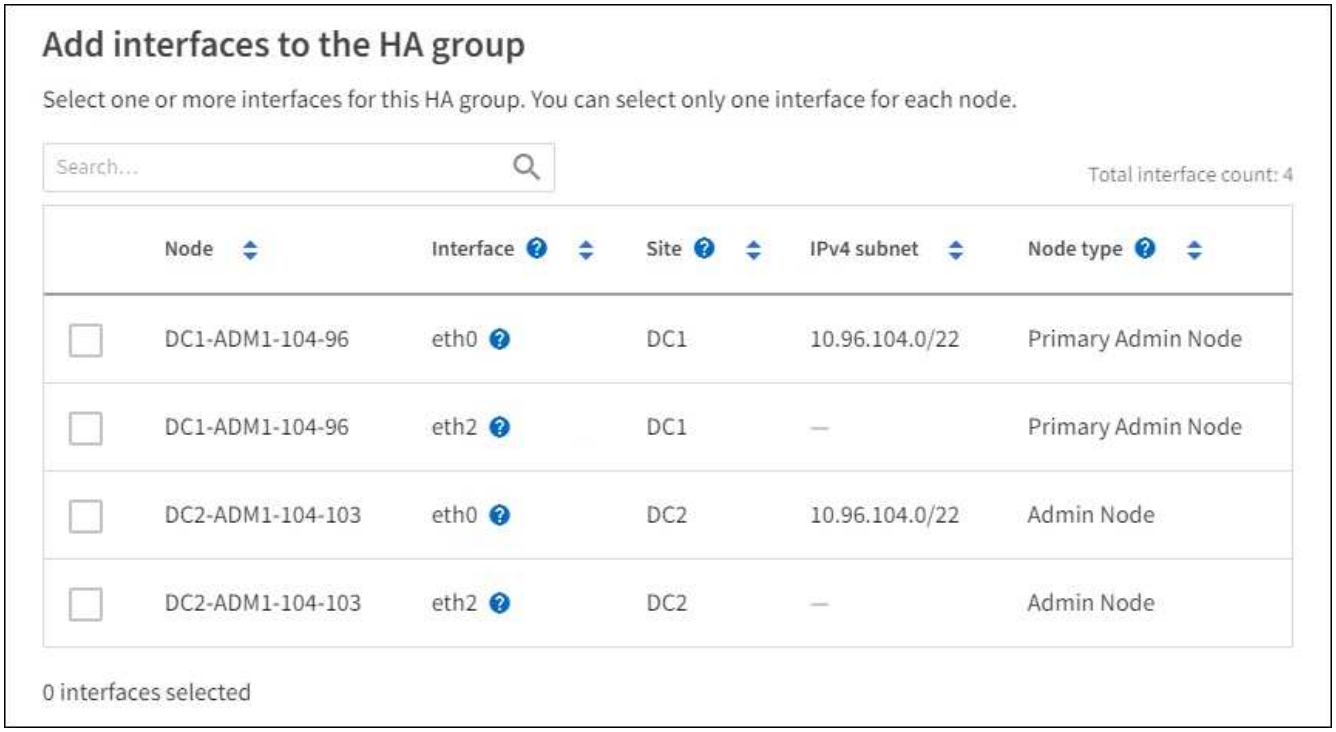
1. 為 HA 組提供唯一的名稱。
2. 或者，輸入 HA 組的描述。
3. 選擇*繼續*。

將介面加入 **HA** 組

步驟

1. 選擇一個或多個要新增至此 HA 群組的介面。

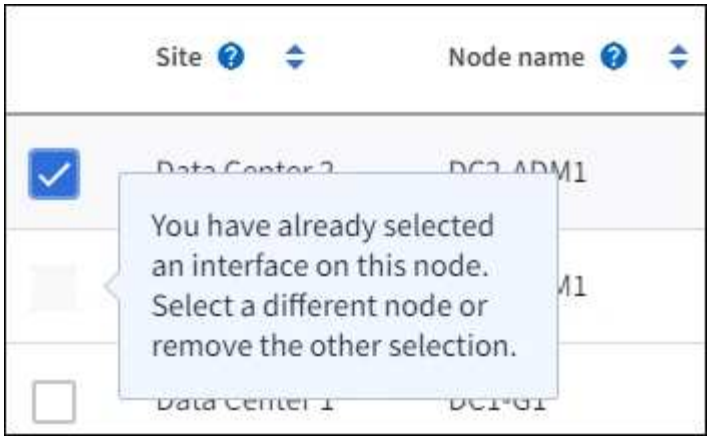
   使用列標題對行進行排序，或輸入搜尋字詞以更快找到介面。



   建立 VLAN 介面後，最多等待 5 分鐘，新介面就會出現在表中。

   選擇介面的指南

   - 您必須至少選擇一個介面。
   - 一個節點只能選擇一個介面。
   - 如果 HA 群組用於管理節點服務（包括網格管理器和租戶管理器）的 HA 保護，則僅選擇管理節點上的介面。
   - 如果 HA 群組用於 S3 用戶端流量的 HA 保護，請選擇管理節點、網關節點或兩者上的介面。
   - 如果您選擇不同類型節點上的接口，則會出現一條訊息說明。需要提醒您的是，如果發生故障轉移，先前活動節點提供的服務可能無法在新活動節點上使用。例如，備份網關節點無法為管理節點服務提供 HA 保護。同樣，備份管理節點無法執行主管理節點可以提供的所有維護程序。
   - 如果您無法選擇接口，則其複選框將被停用。工具提示提供了更多資訊。



- 如果某個介面的子網路值或閘道與另一個選取的介面衝突，則您無法選擇該介面。
- 如果配置的介面沒有靜態 IP 位址，則無法選擇該介面。

2. 選擇*繼續*。

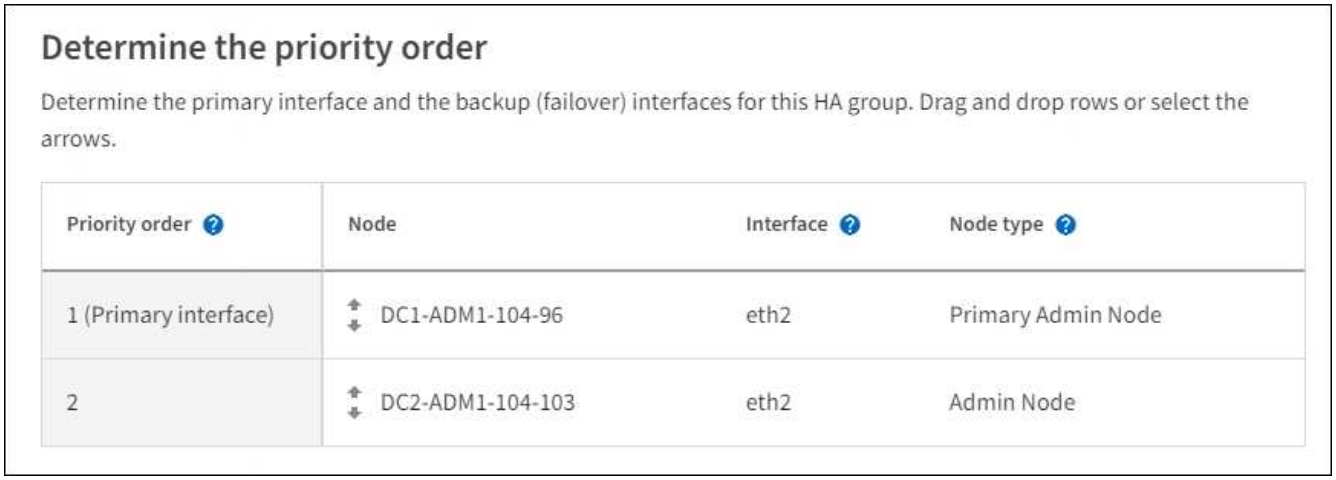
確定優先順序

如果 HA 群組包含多個接口，您可以確定哪個是主接口，哪些是備份（故障轉移）接口。如果主介面發生故障，VIP 位址將移至可用的最高優先權介面。如果該接口發生故障，VIP 位址將移至下一個可用的最高優先權接口，依此類推。

步驟

1. 拖曳「優先順序」列中的行來決定主介面和任何備份介面。

   清單中的第一個介面是主介面。除非發生故障，否則主介面是活動介面。



如果 HA 群組提供對網格管理器的存取權限，則必須選擇主管理節點上的一個介面作為主介面。某些維護程序只能從主管理節點執行。

2. 選擇*繼續*。

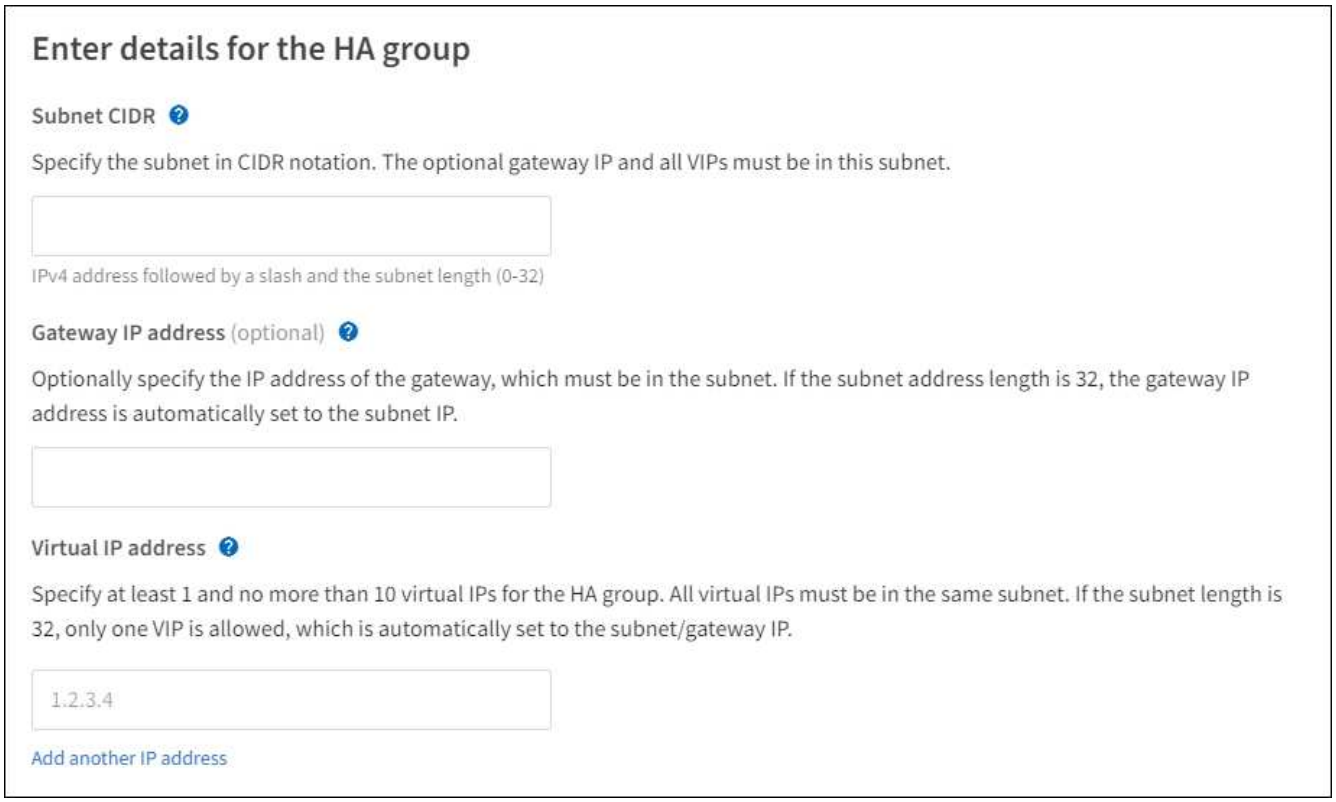
輸入 **IP** 位址

步驟

1. 在 **Subnet CIDR** 欄位中，以 CIDR 表示法指定 VIP 子網路－IPv4 位址後面接著斜槓和子網路長度（0-32）。

   網路位址不得設定任何主機位元。例如， `192.16.0.0/22` 。

   如果使用32位元前綴，VIP網路位址也充當網關位址和VIP位址。



2. 或者，如果任何 S3 管理或租用戶用戶端將從不同的子網路存取這些 VIP 位址，請輸入 網關 **IP** 位址。網關位址必須在 VIP 子網路內。

   用戶端和管理員用戶將使用此網關存取虛擬 IP 位址。

3. 為 HA 組中的活動介面輸入至少一個、最多十個 VIP 位址。所有 VIP 位址都必須位於 VIP 子網路內，並且所有 VIP 位址都將在活動介面上同時處於活動狀態。

   您必須提供至少一個 IPv4 位址。您也可以選擇指定其他 IPv4 和 IPv6 位址。

4. 選擇*建立 HA 群組*並選擇*完成*。

   HA 群組已創建，您現在可以使用配置的虛擬 IP 位址。

後續步驟**Next steps**

如果您將使用此 HA 群組進行負載平衡，請建立負載平衡器端點以決定連接埠和網路協定並附加任何所需的憑證。看"配置負載平衡器端點" 。

編輯高可用性群組

您可以編輯高可用性 (HA) 群組以變更其名稱和描述、新增或刪除介面、變更優先順序或新增或更新虛擬 IP 位址。

例如，如果您想要在網站或節點退役過程中刪除與選定介面關聯的節點，則可能需要編輯 HA 群組。

步驟

1. 選擇 配置 > 網路 > 高可用性群組。

   高可用性組頁面顯示所有現有的 HA 組。

2. 選取要編輯的 HA 群組的複選框。
3. 根據您要更新的內容執行以下操作之一：
   - 選擇*動作* > *編輯虛擬 IP 位址*來新增或刪除 VIP 位址。
   - 選擇*操作* > *編輯 HA 群組*來更新群組的名稱或描述、新增或刪除介面、變更優先順序或新增或刪除 VIP 位址。
4. 如果您選擇了「編輯虛擬 IP 位址」：
   a. 更新 HA 群組的虛擬 IP 位址。
   b. 選擇*儲存*。
   c. 選擇*完成*。
5. 如果您選擇了「編輯 HA 群組」：
   a. 或者，更新群組的名稱或描述。
   b. 或者，選擇或清除複選框來新增或刪除介面。

      如果 HA 群組提供對網格管理器的存取權限，則必須選擇主管理節點上的一個介面作為主介面。某些維護程序只能從主管理節點執行

   c. 或者，拖曳行來變更此 HA 群組的主介面和任何備份介面的優先權順序。
   d. 或者，更新虛擬 IP 位址。
   e. 選擇*儲存*，然後選擇*完成*。

刪除高可用性群組

您可以一次刪除一個或多個高可用性 (HA) 群組。

如果 HA 群組綁定到負載平衡器端點，則無法刪除它。若要刪除 HA 群組，您必須將其從使用它的任何負載平衡器端點中刪除。

為防止用戶端中斷，請在刪除 HA 群組之前更新任何受影響的 S3 用戶端應用程式。更新每個用戶端以使用另一個 IP 位址進行連接，例如，不同 HA 群組的虛擬 IP 位址或在安裝期間為介面配置的 IP 位址。

步驟

1. 選擇 配置 > 網路 > 高可用性群組。

2. 檢查要刪除的每個 HA 群組的 負載平衡器端點 列。如果列出了任何負載平衡器端點：
   a. 前往 配置 > 網路 > 負載平衡器端點。
   b. 選取端點的複選框。
   c. 選擇*操作* > 編輯端點綁定模式。
   d. 更新綁定模式以刪除 HA 群組。
   e. 選擇“儲存變更”。
3. 如果沒有列出負載平衡器端點，請選取要刪除的每個 HA 群組的核取方塊。
4. 選擇*操作* > 刪除 **HA** 群組。
5. 查看訊息並選擇*刪除 HA 群組*以確認您的選擇。

   您選擇的所有 HA 組都將刪除。高可用性群組頁面上會出現綠色的成功橫幅。

管理負載平衡

負載平衡的注意事項

您可以使用負載平衡來處理來自 S3 用戶端的提取和檢索工作負載。

什麼是負載平衡？

當用戶端應用程式從StorageGRID系統儲存或擷取資料時， StorageGRID使用負載平衡器來管理擷取和擷取工作負載。負載平衡透過在多個儲存節點之間分配工作負載來最大限度地提高速度和連接容量。

StorageGRID負載平衡器服務安裝在所有管理節點和所有網關節點上，並提供第 7 層負載平衡。它執行客戶端請求的傳輸層安全性 (TLS) 終止，檢查請求，並與儲存節點建立新的安全連線。

將客戶端流量轉送到儲存節點時，每個節點上的負載平衡器服務會獨立運作。透過加權流程，負載平衡器服務將更多請求路由到具有更高 CPU 可用性的儲存節點。

> ⓘ 儘管 StorageGRID 負載平衡器服務是建議的負載平衡機制，但您也可以選擇整合第三方負載平衡器。有關資訊，請聯繫您的 NetApp 客戶代表或參閱 "將第三方負載平衡器與 StorageGRID 結合使用"。

我需要多少個負載平衡節點？

作為一般的最佳實踐， StorageGRID系統中的每個站點都應包含兩個或更多具有負載平衡器服務的節點。例如，一個站點可能包括兩個網關節點或一個管理節點和一個網關節點。確保每個負載平衡節點都有足夠的網路、硬體或虛擬化基礎設施，無論您使用的是服務設備、裸機節點還是基於虛擬機器 (VM) 的節點。

什麼是負載平衡器端點？

負載平衡器端點定義傳入和傳出的客戶端應用程式請求將用於存取包含負載平衡器服務的節點的連接埠和網路協定（HTTPS 或 HTTP）。端點也會定義用戶端類型（S3）、綁定模式以及可選的允許或封鎖租用戶清單。

若要建立負載平衡器端點，請選擇 **CONFIGURATION** > **Network** > **Load balancer endpoints** 或完成FabricPool和 S3 設定精靈。說明：

- "配置負載平衡器端點"
- "使用 S3 設定精靈"
- "使用FabricPool設定精靈"

港口的考慮因素

對於您建立的第一個端點，負載平衡器端點的連接埠預設為 10433，但您可以指定 1 到 65535 之間的任何未使用的外部連接埠。如果您使用連接埠 80 或 443，端點將僅使用網關節點上的負載平衡器服務。這些連接埠在管理節點上保留。如果對多個端點使用相同的端口，則必須為每個端點指定不同的綁定模式。

不允許使用其他網格服務使用的連接埠。查看"網路連接埠參考"。

網路協定的注意事項

大多數情況下，客戶端應用程式和StorageGRID之間的連線應該使用傳輸層安全性 (TLS) 加密。支援但不建議在沒有 TLS 加密的情況下連接到StorageGRID ，尤其是在生產環境中。當您為StorageGRID負載平衡器端點選擇網路協定時，您應該選擇 **HTTPS**。

負載平衡器端點憑證的注意事項

如果選擇 **HTTPS** 作為負載平衡器端點的網路協議，則必須提供安全性憑證。建立負載平衡器端點時，您可以使用以下三個選項中的任何一個：

- 上傳已簽署的憑證（建議）。該證書可以由公眾信任的或私人的證書頒發機構 (CA) 簽署。使用公眾信任的 CA 伺服器憑證來保護連線是最佳做法。與產生的憑證相比，CA 簽署的憑證可以不間斷地輪換，這有助於避免過期問題。

  在建立負載平衡器端點之前，您必須取得下列檔案：

  - 自訂伺服器證書檔案。
  - 自訂伺服器憑證私鑰檔案。
  - 可選地，來自每個中間頒發證書機構的證書的 CA 包。
- 產生自簽名憑證。
- 使用全球**StorageGRID S3** 憑證。您必須上傳或產生此憑證的自訂版本，然後才能為負載平衡器端點選擇它。看"配置 S3 API 證書"。

我需要什麼價值觀？

要建立證書，您必須知道 S3 用戶端應用程式將用於存取端點的所有網域名稱和 IP 位址。

憑證的 **Subject DN**（可分辨名稱）條目必須包含客戶端應用程式將用於StorageGRID 的完全限定網域名稱。例如：

```
Subject DN:
/C=Country/ST=State/O=Company,Inc./CN=s3.storagegrid.example.com
```

根據需要，憑證可以使用通配符來表示執行負載平衡器服務的所有管理節點和網關節點的完全限定網域名稱。例

如， `*.storagegrid.example.com`使用 * 通配符來表示 `adm1.storagegrid.example.com`和 `gn1.storagegrid.example.com`。

如果您打算使用 S3 虛擬託管式要求，憑證也必須包含每個"S3 端點域名"您已配置，包括任何通配符名稱。例如：

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```

如果您使用通配符作為域名，請查看"伺服器證書強化指南"。

您也必須為安全性憑證中的每個名稱定義一個 DNS 項目。

如何管理即將過期的憑證？

如果用於保護 S3 應用程式和StorageGRID之間的連線的憑證過期，則該應用程式可能會暫時失去對StorageGRID 的存取權。

為避免憑證過期問題，請遵循以下最佳做法：

- 仔細監控任何警告憑證即將到期的警報，例如*負載平衡器端點憑證到期*和*S3 API 的全域伺服器憑證到期*警報。
- 始終保持StorageGRID和 S3 應用程式的憑證版本同步。如果您取代或更新用於負載平衡器端點的證書，則必須取代或更新 S3 應用程式使用的等效證書。
- 使用公開簽署的 CA 憑證。如果您使用由 CA 簽署的證書，則可以無中斷地替換即將過期的證書。
- 如果您已產生自簽署StorageGRID憑證且該憑證即將過期，則必須在現有憑證過期之前手動取代StorageGRID和 S3 應用程式中的該憑證。

綁定模式的注意事項

綁定模式可讓您控制哪些 IP 位址可用於存取負載平衡器端點。如果端點使用綁定模式，則用戶端應用程式只有使用允許的 IP 位址或其對應的完全限定網域名稱 (FQDN) 才能存取該端點。使用任何其他 IP 位址或 FQDN 的用戶端應用程式無法存取該端點。

您可以指定以下任一種綁定模式：

- 全域（預設）：用戶端應用程式可以使用任何網關節點或管理節點的 IP 位址、任何網路上任何 HA 群組的虛擬 IP（VIP）位址或對應的 FQDN 存取端點。除非您需要限制端點的可訪問性，否則請使用此設定。
- **HA** 群組的虛擬 **IP**。客戶端應用程式必須使用 HA 群組的虛擬 IP 位址（或對應的 FQDN）。
- 節點介面。客戶端必須使用所選節點介面的 IP 位址（或對應的 FQDN）。
- 節點類型。根據您選擇的節點類型，用戶端必須使用任何管理節點的 IP 位址（或對應的 FQDN）或任何網關節點的 IP 位址（或對應的 FQDN）。

租戶訪問注意事項

租用戶存取是可選的安全功能，可讓您控制哪些StorageGRID租用戶帳戶可以使用負載平衡器端點存取其儲存桶。您可以允許所有租用戶存取一個端點（預設），也可以為每個端點指定允許或封鎖的租用戶清單。

您可以使用此功能在租戶和他們的端點之間提供更好的安全隔離。例如，您可以使用此功能來確保一個租戶擁有的絕密或高度機密的資料對其他租戶完全無法存取。

> 為了實現存取控制，租用戶是根據客戶端請求中使用的存取金鑰來確定的，如果請求中沒有提供存取金鑰（例如匿名存取），則儲存桶擁有者將用於確定租用戶。

租戶訪問範例

若要了解此安全功能的工作原理，請考慮以下範例：

1. 您已建立兩個負載平衡器端點，如下所示：
   - *公共*端點：使用連接埠 10443 並允許所有租戶存取。
   - *最高機密*端點：使用連接埠 10444 並僅允許存取 *最高機密*租用戶。所有其他租戶均無法存取此端點。
2. 這 `top-secret.pdf`位於*最高機密*租戶擁有的儲存桶中。

要訪問 `top-secret.pdf`，**Top secret** 租戶中的使用者可以向 `https://w.x.y.z:10444/top-secret.pdf`。由於該租用戶被允許使用 10444 端點，因此使用者可以存取該物件。但是，如果屬於任何其他租用戶的使用者向同一 URL 發出相同請求，他們會立即收到「訪問被拒絕」訊息。即使憑證和簽名有效，存取也會被拒絕。

CPU 可用性

每個管理節點和網關節點上的負載平衡器服務在將 S3 流量轉送到儲存節點時獨立運作。透過加權流程，負載平衡器服務將更多請求路由到具有更高 CPU 可用性的儲存節點。節點 CPU 負載資訊每隔幾分鐘更新一次，但權重可能會更頻繁地更新。所有儲存節點都被分配一個最小基本權重值，即使節點報告 100% 使用率或未能報告其利用率。

在某些情況下，有關 CPU 可用性的資訊僅限於負載平衡器服務所在的站點。

配置負載平衡器端點

負載平衡器端點決定 S3 用戶端在連接到網關和管理節點上的StorageGRID負載平衡器時可以使用的連接埠和網路協定。您也可以使用端點存取網格管理員、租用戶管理器或兩者。

> 此版本的文件網站已刪除 Swift 詳細資訊。看 "配置 S3 和 Swift 用戶端連接"。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"Root存取權限"。
- 您已審閱"負載平衡的注意事項"。
- 如果您之前重新映射了要用於負載平衡器端點的端口，則您必須"刪除了連接埠重新映射"。
- 您已建立計劃使用的任何高可用性 (HA) 群組。建議使用 HA 組，但這不是必需的。看"管理高可用性組" 。
- 如果負載平衡器端點將由"S3 Select 的 S3 租戶"，它不能使用任何裸機節點的 IP 位址或 FQDN。僅允許服務設備和基於 VMware 的軟體節點作為用於 S3 Select 的負載平衡器端點。

- 您已設定計劃使用的所有 VLAN 介面。看"配置VLAN介面" 。
- 如果您正在建立 HTTPS 端點（建議），則您擁有伺服器憑證的資訊。

  端點憑證的變更可能需要長達 15 分鐘才能套用到所有節點。

  - 要上傳證書，您需要伺服器證書、證書私鑰以及可選的 CA 套件。
  - 要產生證書，您需要 S3 用戶端將用於存取端點的所有網域名稱和 IP 位址。您還必須知道主題（專有名稱）。
  - 如果您想使用StorageGRID S3 API 憑證（也可用於直接連接到儲存節點），您已經用外部憑證授權單位簽署的自訂憑證取代了預設憑證。看"配置 S3 API 證書" 。

建立負載平衡器端點

每個 S3 用戶端負載平衡器端點指定一個連接埠、一個客戶端類型（S3）和一個網路協定（HTTP 或 HTTPS ）。管理介面負載平衡器端點指定連接埠、介面類型和不受信任的客戶端網路。

訪問嚮導

步驟

1. 選擇 配置 > 網路 > 負載平衡器端點。
2. 若要為 S3 或 Swift 用戶端建立端點，請選擇 **S3** 或 **Swift** 用戶端 標籤。
3. 若要建立用於存取網格管理器、租用戶管理員或兩者的端點，請選擇「管理介面」標籤。
4. 選擇“創建”。

輸入端點詳細信息

步驟

1. 選擇適當的說明來輸入您想要建立的端點類型的詳細資訊。

S3 或 **Swift** 用戶端

場地	描述
Name	端點的描述性名稱，將顯示在負載平衡器端點頁面的表格中。
港口	您想要用於負載平衡的StorageGRID連接埠。對於您建立的第一個端點，此欄位預設為 10433，但您可以輸入 1 到 65535 之間的任何未使用的外部連接埠。 如果您輸入 **80** 或 **8443**，則端點僅在網關節點上配置，除非您釋放了連接埠 8443。然後，您可以使用連接埠 8443 作為 S3 端點，並且該連接埠將在網關和管理節點上進行設定。
客戶端類型	將使用此端點的客戶端應用程式的類型，**S3** 或 **Swift**。
網路協定	用戶端連接到此端點時將使用的網路協定。 • 選擇 **HTTPS** 進行安全的 TLS 加密通訊（建議）。您必須先附加安全性證書，然後才能儲存端點。 • 選擇 **HTTP** 進行安全性較低、未加密的通訊。僅對非生產網格使用 HTTP。

管理介面

場地	描述
Name	端點的描述性名稱，將顯示在負載平衡器端點頁面的表格中。
港口	您要用於存取網格管理器、租用戶管理器或兩者的StorageGRID連接埠。 • 電網經理：**8443** • 租戶經理：**9443** • 網格經理和租戶經理：**443** 注意：您可以使用這些預設連接埠或其他可用連接埠。
介面類型	選擇您將使用此端點存取的StorageGRID介面的單選按鈕。
不受信任的客戶端網絡	如果此端點可供不受信任的客戶端網路訪問，請選擇「是」。否則，選擇“否”。 當您選擇「是」時，該連接埠在所有不受信任的用戶端網路上均處於開啟狀態。 注意：建立負載平衡器端點時，您只能將連接埠配置為對不受信任的用戶端網路開放或關閉。

1. 選擇*繼續*。

選擇綁定模式

步驟

1. 選擇端點的綁定模式來控制如何使用任意 IP 位址或使用特定 IP 位址和網路介面存取端點。

   某些綁定模式適用於客戶端端點或管理介面端點。兩種端點類型的所有模式均列於此。

模式	描述
全域（客戶端端點的預設設定）	用戶端可以使用任何網關節點或管理節點的 IP 位址、任何網路上任何 HA 群組的虛擬 IP (VIP) 位址或對應的 FQDN 存取端點。 除非您需要限制此端點的可存取性，否則請使用*全域*設定。
HA 群組的虛擬 IP	用戶端必須使用 HA 群組的虛擬 IP 位址（或對應的 FQDN）來存取此端點。 具有此綁定模式的端點都可以使用相同的連接埠號，只要您為端點選擇的 HA 群組不重疊。
節點介面	用戶端必須使用選定節點介面的 IP 位址（或對應的 FQDN）來存取此端點。
節點類型（僅限客戶端端點）	根據您選擇的節點類型，用戶端必須使用任何管理節點的 IP 位址（或對應的 FQDN）或任何網關節點的 IP 位址（或對應的 FQDN）來存取此端點。
所有管理節點（管理介面端點的預設設定）	用戶端必須使用任何管理節點的 IP 位址（或對應的 FQDN）來存取此端點。

   如果多個端點使用相同的端口， StorageGRID將使用此優先權順序來決定使用哪個端點：**HA** 群組的虛擬 **IP** > 節點介面 > 節點類型 > 全域。

   如果您正在建立管理介面端點，則只允許管理節點。

2. 如果您選擇了*HA 群組的虛擬 IP*，請選擇一個或多個 HA 群組。

   如果您正在建立管理介面端點，請選擇僅與管理節點關聯的 VIP。

3. 如果您選擇了*節點介面*，請為要與此端點關聯的每個管理節點或網關節點選擇一個或多個節點介面。
4. 如果您選擇了*節點類型*，請選擇管理節點（包括主管理節點和任何非主管理節點）或網關節點。

控制租戶訪問

管理介面端點僅當端點具有租用戶管理器的介面類型。

步驟

1. 對於「租戶存取」步驟，選擇以下選項之一：

場地	描述
允許所有租戶（預設）	所有租用戶帳戶都可以使用此端點存取他們的儲存桶。 如果您尚未建立任何租用戶帳戶，則必須選擇此選項。新增租用戶帳戶後，您可以編輯負載平衡器端點以允許或封鎖特定帳戶。
允許選定的租戶	只有選定的租用戶帳戶可以使用此端點存取他們的儲存桶。
阻止選定的租戶	選定的租用戶帳戶不能使用此端點存取其儲存桶。所有其他租戶都可以使用此端點。

2. 如果您正在建立 **HTTP** 端點，則無需附加憑證。選擇“創建”以新增新的負載平衡器端點。然後，轉到完成後。否則，請選擇“繼續”以附加憑證。

附上證書

步驟

1. 如果您正在建立 **HTTPS** 端點，請選擇要附加至該端點的安全性憑證類型。

   此憑證可保護 S3 用戶端與管理節點或閘道點上的負載平衡器服務之間的連線。

   - 上傳證書。如果您有自訂憑證需要上傳，請選擇此選項。
   - 產生證書。如果您擁有產生自訂憑證所需的值，請選擇此選項。
   - 使用**StorageGRID S3** 憑證。如果您想使用全域 S3 API 證書，請選擇此選項，該證書也可用於直接連接到儲存節點。

     除非您已將由網格 CA 簽署的預設 S3 API 證書替換為由外部證書頒發機構簽署的自訂證書，否則您無法選擇此選項。看"配置 S3 API 證書" 。

   - 使用管理介面證書。如果您想使用全域管理介面證書，請選擇此選項，該證書也可用於直接連接到管理節點。
2. 如果您不使用StorageGRID S3 證書，請上傳或產生該證書。

上傳證書

a. 選擇*上傳證書*。

b. 上傳所需的伺服器憑證檔案：

   - 伺服器憑證：PEM編碼的自訂伺服器憑證檔案。
   - 證書私鑰：自訂伺服器憑證私鑰文件(`.key`）。

     EC 私鑰必須為 224 位元或更大。 RSA 私鑰必須為 2048 位元或更大。

   - **CA** 包：一個可選文件，包含來自每個中間發行憑證機構 (CA) 的憑證。該文件應包含每個 PEM 編碼的 CA 憑證文件，並按憑證鏈順序連接。

c. 展開*證書詳細資訊*以查看您上傳的每個證書的元資料。如果您上傳了可選的 CA 包，則每個憑證都會顯示在其自己的標籤上。

   - 選擇*下載憑證*儲存憑證檔案或選擇*下載 CA 套件*儲存憑證套件。

     指定證書檔案名稱和下載位置。使用副檔名儲存檔案 `.pem`。

     例如： `storagegrid_certificate.pem`

   - 選擇*複製憑證 PEM*或*複製 CA 套件 PEM*以複製憑證內容以便貼上到其他地方。

d. 選擇“創建”。+ 負載平衡器端點已建立。自訂憑證用於 S3 用戶端或管理介面與端點之間的所有後續新連線。

產生證書

a. 選擇*產生證書*。

b. 指定證書資訊：

場地	描述
網域	證書中包含的一個或多個完全限定域名。使用 * 作為通配符來表示多個網域。
智慧財產	證書中包含的一個或多個 IP 位址。
主題（可選）	證書擁有者的 X.509 主題或專有名稱 (DN)。 如果此欄位未輸入任何值，則產生的憑證將使用第一個網域名稱或 IP 位址作為主題通用名稱 (CN)。
有效天數	證書建立後過期的天數。

場地	描述
新增密鑰使用擴展	如果選擇（預設和推薦），密鑰使用和擴展密鑰使用擴充將新增至產生的憑證。 這些擴充定義了憑證中包含的金鑰的用途。 注意：請選取此複選框，除非當憑證包含這些擴充功能時您遇到與舊用戶端的連線問題。

c. 選擇*生成*。

d. 選擇*證書詳細資訊*以查看產生的證書的元資料。

- 選擇*下載證書*儲存證書檔案。

  指定證書檔案名稱和下載位置。使用副檔名儲存檔案 `.pem`。

  例如： `storagegrid_certificate.pem`

- 選擇*複製證書 PEM* 以複製證書內容並貼上到其他地方。

e. 選擇“創建”。

負載平衡器端點已建立。自訂憑證用於 S3 用戶端或管理介面與此端點之間的所有後續新連線。

完成後

步驟

1. 如果您使用 DNS，請確保 DNS 包含一筆記錄，以將StorageGRID完全限定網域名稱 (FQDN) 與用戶端將用於建立連線的每個 IP 位址關聯。

   您在 DNS 記錄中輸入的 IP 位址取決於您是否使用負載平衡節點的 HA 群組：

   - 如果您已設定 HA 群組，用戶端將連線至該 HA 群組的虛擬 IP 位址。
   - 如果您不使用 HA 群組，用戶端將使用網關節點或管理節點的 IP 位址連線至StorageGRID負載平衡器服務。

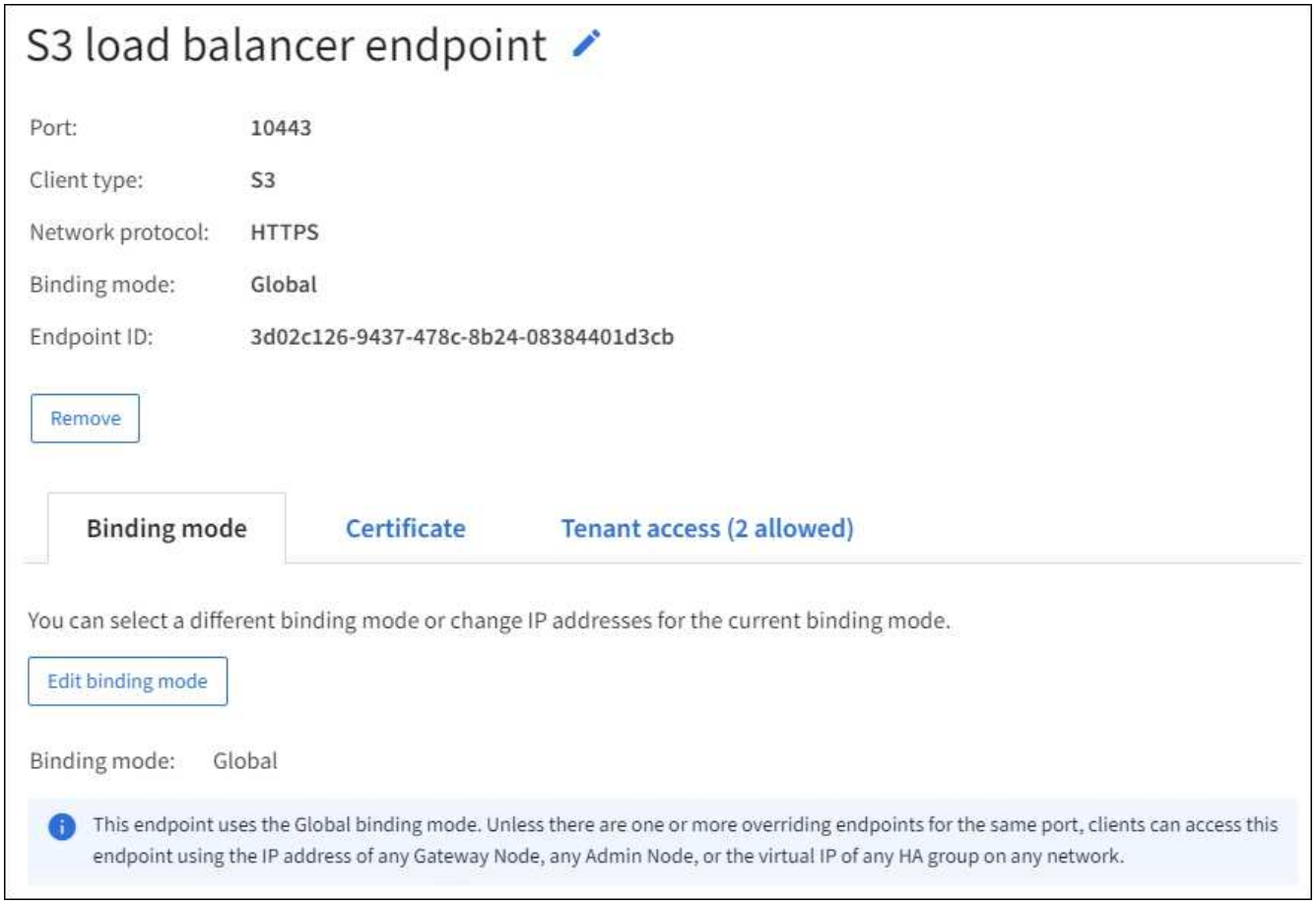
     您還必須確保 DNS 記錄引用所有必要的端點域名，包括任何通配符名稱。

2. 向 S3 用戶端提供連接到端點所需的資訊：
   - 連接埠號
   - 完全限定網域名稱或 IP 位址
   - 任何所需的證書詳細信息

檢視並編輯負載平衡器端點

您可以查看現有負載平衡器端點的詳細信息，包括安全端點的憑證元資料。您可以變更端點的某些設定。

- 要查看所有負載平衡器端點的基本信息，請查看負載平衡器端點頁面上的表格。
- 若要查看有關特定端點的所有詳細資訊（包括憑證元資料），請在表中選擇該端點的名稱。顯示的資訊會根據端點類型及其配置方式而有所不同。



- 若要編輯端點，請使用負載平衡器端點頁面上的「操作」功能表。

如果在編輯管理介面端點的連接埠時失去對網格管理器的存取權限，請更新 URL 和連接埠以重新取得存取權限。

編輯端點後，您可能需要等待最多 15 分鐘才能將變更套用到所有節點。

任務	操作選單	詳細資訊頁面
編輯端點名稱	a. 選取端點的複選框。 b. 選擇*動作* > 編輯端點名稱。 c. 輸入新名稱。 d. 選擇*儲存*。	a. 選擇端點名稱以顯示詳細資訊。 b. 選擇編輯圖標。 c. 輸入新名稱。 d. 選擇*儲存*。

任務	操作選單	詳細資訊頁面
編輯端點埠	a. 選取端點的複選框。 b. 選擇“操作”>“編輯端點連接埠” c. 輸入有效的連接埠號碼。 d. 選擇*儲存*。	無
編輯端點綁定模式	a. 選取端點的複選框。 b. 選擇*操作* > 編輯端點綁定模式。 c. 根據需要更新綁定模式。 d. 選擇“儲存變更”。	a. 選擇端點名稱以顯示詳細資訊。 b. 選擇*編輯綁定模式*。 c. 根據需要更新綁定模式。 d. 選擇“儲存變更”。
編輯端點憑證	a. 選取端點的複選框。 b. 選擇*動作* > 編輯端點憑證。 c. 根據需要上傳或產生新的自訂憑證或開始使用全域 S3 憑證。 d. 選擇“儲存變更”。	a. 選擇端點名稱以顯示詳細資訊。 b. 選擇“證書”選項卡。 c. 選擇*編輯證書*。 d. 根據需要上傳或產生新的自訂憑證或開始使用全域 S3 憑證。 e. 選擇“儲存變更”。
編輯租戶存取權限	a. 選取端點的複選框。 b. 選擇*操作* > 編輯租戶存取。 c. 選擇不同的存取選項，從清單中選擇或刪除租戶，或同時執行這兩項操作。 d. 選擇“儲存變更”。	a. 選擇端點名稱以顯示詳細資訊。 b. 選擇“租戶訪問”標籤。 c. 選擇*編輯租戶訪問*。 d. 選擇不同的存取選項，從清單中選擇或刪除租戶，或同時執行這兩項操作。 e. 選擇“儲存變更”。

刪除負載平衡器端點

您可以使用「動作」功能表刪除一個或多個端點，也可以從詳細資料頁面中刪除單一端點。

為防止用戶端中斷，請在刪除負載平衡器端點之前更新任何受影響的 S3 用戶端應用程式。更新每個用戶端以使用分配給另一個負載平衡器端點的連接埠進行連線。請務必更新所有必要的證書資訊。

如果在刪除管理介面端點時失去對網格管理器的存取權限，請更新 URL。

- 若要刪除一個或多個端點：
  a. 在負載平衡器頁面中，選取要刪除的每個端點的核取方塊。
  b. 選擇*操作* > 刪除。

c. 選擇“確定”。

- 若要從詳細資料頁面中刪除一個端點：
  a. 從負載平衡器頁面選擇端點名稱。
  b. 在詳細資料頁面上選擇“刪除”。
  c. 選擇“確定”。

配置 S3 端點域名

若要支援 S3 虛擬託管式請求，您必須使用網格管理員來設定 S3 用戶端連線到的 S3 端點網域清單。

不支援使用 IP 位址作為端點網域名稱。未來版本將阻止這種配置。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"特定存取權限"。
- 您已確認電網升級未正在進行中。

在電網升級過程中，請勿對網域配置進行任何變更。

關於此任務

若要讓客戶端能夠使用 S3 端點域名，您必須執行以下所有操作：

- 使用網格管理器將 S3 端點網域新增至StorageGRID系統。
- 確保"用戶端用於與StorageGRID進行 HTTPS 連線的憑證"已為客戶端所需的所有網域簽署。

  例如，如果端點是 `s3.company.com`，您必須確保用於 HTTPS 連線的憑證包含 `s3.company.com`端點和端點的通配符主題備用名稱 （SAN）： `*.s3.company.com` 。

- 設定客戶端使用的DNS伺服器。包含用戶端用於建立連線的 IP 位址的 DNS 記錄，並確保記錄引用所有必要的 S3 端點域名，包括任何通配符名稱。

用戶端可以使用網關節點、管理節點或儲存節點的 IP 位址連接到StorageGRID ，或透過連接到高可用性群組的虛擬 IP 位址連接到 StorageGRID。您應該了解用戶端應用程式如何連接到電網，以便在 DNS 記錄中包含正確的 IP 位址。

使用 HTTPS 連線（建議）到電網的用戶端可以使用下列任一憑證：

- 連接到負載平衡器端點的用戶端可以使用該端點的自訂憑證。每個負載平衡器端點可以設定為識別不同的 S3 端點網域名稱。
- 連接到負載平衡器端點或直接連接到儲存節點的用戶端可以自訂全域 S3 API 憑證以包含所有必要的 S3 端點網域。

如果您不新增 S3 端點網域名稱且清單為空，則對 S3 虛擬託管式要求的支援將被停用。

新增 **S3** 端點域名

步驟

1. 選擇 設定 > 網路 > **S3** 端點網域。
2. 在*網域 1* 欄位中輸入網域名稱。選擇*新增其他網域*以新增更多網域。
3. 選擇*儲存*。
4. 確保用戶端使用的伺服器憑證與所需的 S3 端點網域名稱相符。
   - 如果用戶端連接到使用其自己的憑證的負載平衡器端點，"更新與端點關聯的憑證" 。
   - 如果用戶端連接到使用全域 S3 API 憑證的負載平衡器端點或直接連接到儲存節點，"更新全域 S3 API 證書" 。
5. 新增所需的DNS記錄，確保終端域名請求能夠被解析。

結果

現在，當客戶端使用端點時 *bucket.s3.company.com*，DNS 伺服器解析到正確的端點，並且憑證按預期對端點進行身份驗證。

重新命名 **S3** 端點域名

如果您變更 S3 應用程式使用的名稱，虛擬託管樣式的請求將會失敗。

步驟

1. 選擇 設定 > 網路 > **S3** 端點網域。
2. 選擇您要編輯的網域名稱欄位並進行必要的變更。
3. 選擇*儲存*。
4. 選擇“是”確認您的更改。

刪除 **S3** 終端節點域名

如果刪除 S3 應用程式使用的名稱，虛擬託管樣式請求將會失敗。

步驟

1. 選擇 設定 > 網路 > **S3** 端點網域。
2. 選擇刪除圖標❌域名旁邊。
3. 選擇“是”確認刪除。

相關資訊

- "使用 S3 REST API"
- "查看 IP 位址"
- "配置高可用性組"

摘要：客戶端連接的 **IP** 位址和連接埠

為了儲存或檢索對象，S3 用戶端應用程式連接到所有管理節點和網關節點上包含的負載平

衡器服務，或連接到所有儲存節點上包含的本機分發路由器 (LDR) 服務。

用戶端應用程式可以使用網格節點的 IP 位址和該節點上的服務的連接埠號碼連接到StorageGRID 。或者，您可以建立負載平衡節點的高可用性 (HA) 群組，以提供使用虛擬 IP (VIP) 位址的高可用性連線。如果您想要使用完全限定網域名稱 (FQDN) 而不是 IP 或 VIP 位址連線到StorageGRID ，您可以設定 DNS 項目。

此表總結了用戶端連接到StorageGRID 的不同方式以及用於每種連接類型的 IP 位址和連接埠。如果您已建立負載平衡器端點和高可用性 (HA) 群組，請參閱在哪裡查找 IP 位址在網格管理器中定位這些值。

連接地點	用戶端連線的服務	**IP** 位址	港口
HA組	負載平衡器	HA組的虛擬IP位址	分配給負載平衡器端點的端口
管理節點	負載平衡器	管理節點的 IP 位址	分配給負載平衡器端點的端口
閘道	負載平衡器	網關節點的IP位址	分配給負載平衡器端點的端口
儲存節點	遠距離駕駛	儲存節點IP位址	預設 S3 連接埠： • HTTPS：18082 • HTTP：18084

範例 **URL**

若要將用戶端應用程式連接到網關節點 HA 群組的負載平衡器端點，請使用如下所示結構的 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，負載平衡器端點的連接埠號碼為 10443，則應用程式可以使用下列 URL 連接至StorageGRID：

`https://192.0.2.5:10443`

在哪裡查找 **IP** 位址

1. Sign in"支援的網頁瀏覽器"。
2. 若要尋找網格節點的 IP 位址：
   a. 選擇*NODES*。
   b. 選擇要連接的管理節點、網關節點或儲存節點。
   c. 選擇“概覽”標籤。
   d. 在節點資訊部分中，記下節點的 IP 位址。
   e. 選擇*顯示更多*以查看 IPv6 位址和介面映射。

      您可以從客戶端應用程式與清單中的任何 IP 位址建立連線：

- **eth0:** 網格網絡
- *eth1：*管理網路（可選）
- *eth2：*客戶端網路（選購）

> 如果您正在查看管理節點或網關節點，並且它是高可用性群組中的活動節點，則 HA 群組的虛擬 IP 位址將顯示在 eth2 上。

3. 若要尋找高可用性群組的虛擬 IP 位址：
   a. 選擇 配置 > 網路 > 高可用性群組。
   b. 在表中，記下 HA 群組的虛擬 IP 位址。
4. 若要尋找負載平衡器端點的連接埠號碼：
   a. 選擇 配置 > 網路 > 負載平衡器端點。
   b. 記下您要使用的端點的連接埠號碼。

> 如果連接埠號碼是 80 或 443，則端點僅在網關節點上配置，因為這些連接埠在管理節點上保留。所有其他連接埠均在網關節點和管理節點上配置。

   c. 從表格中選擇端點的名稱。
   d. 確認*客戶端類型*（S3）與將使用端點的客戶端應用程式相符。

管理網路和連接

設定網路設定

您可以從網格管理器配置各種網路設定來微調StorageGRID系統的運作。

配置**VLAN**介面

你可以"建立虛擬 LAN (VLAN) 介面"隔離和劃分流量以確保安全性、靈活性和效能。每個 VLAN 介面都與管理節點和網關節點上的一個或多個父介面相關聯。您可以在 HA 群組和負載平衡器端點中使用 VLAN 介面依應用程式或租用戶隔離用戶端或管理流量。

流量分類策略

您可以使用"流量分類策略"識別和處理不同類型的網路流量，包括與特定儲存桶、租戶、客戶端子網或負載平衡器端點相關的流量。這些策略可以幫助限制和監控流量。

StorageGRID網路指南

您可以使用網格管理器來設定和管理StorageGRID網路和連接。

看"配置 S3 用戶端連接"了解如何連接 S3 用戶端。

預設StorageGRID網絡

預設情況下， StorageGRID支援每個網格節點三個網路接口，可讓您為每個單獨的網格節點配置網路以滿足您的安全性和存取要求。

有關網路拓撲的詳細信息，請參閱"網路指南"。

網格網絡

必需的。網格網路用於所有內部StorageGRID流量。它提供網格中所有節點、所有站點和子網路之間的連接。

管理網路

選修的。管理網路通常用於系統管理和維護。它還可以用於客戶端協定存取。管理網路通常是私人網絡，不需要在站點之間路由。

客戶網路

選修的。客戶端網路是一個開放網絡，通常用於提供對 S3 客戶端應用程式的訪問，因此網格網路可以被隔離和保護。用戶端網路可以與透過本地網關可達的任何子網路進行通訊。

指南

- 每個StorageGRID節點都需要為其分配到的每個網路配備專用的網路介面、IP 位址、子網路遮罩和網關。
- 網格節點在網路上不能擁有多個介面。
- 每個網路、每個網格節點支援一個網關，而且它必須與節點位於同一子網路。如果需要，您可以在網關中實現更複雜的路由。
- 在每個節點上，每個網路都會對應到特定的網路介面。

網路	介面名稱
網格	eth0
管理員（可選）	eth1
客戶端（可選）	eth2

- 如果節點連接到StorageGRID設備，則每個網路都會使用特定的連接埠。有關詳細信息，請參閱設備的安裝說明。
- 每個節點都會自動產生預設路由。如果啟用了 eth2，則 0.0.0.0/0 使用 eth2 上的用戶端網路。如果未啟用 eth2，則 0.0.0.0/0 使用 eth0 上的網格網路。
- 客戶端網路在網格節點加入網格之前無法運行
- 可以在網格節點部署期間配置管理網絡，以允許在網格完全安裝之前存取安裝使用者介面。

可選接口

您可以選擇向節點新增額外的介面。例如，您可能想要在管理節點或網關節點新增中繼接口，以便可以使用"VLAN 介面"隔離屬於不同應用程式或租戶的流量。或者，您可能想要新增一個存取介面以在"高可用性 (HA)

組"。

若要新增中繼或存取接口，請參閱以下內容：

- **VMware**（安裝節點後）："VMware：向節點新增中繼或存取介面"
  - **Red Hat Enterprise Linux**（安裝節點前）："建立節點設定檔"
  - **Ubuntu** 或 **Debian**（安裝節點之前）："建立節點設定檔"
  - **RHEL**、**Ubuntu** 或 **Debian**（安裝節點後）："Linux：為節點新增主幹或存取介面"

查看 **IP** 位址

您可以查看StorageGRID系統中每個網格節點的 IP 位址。然後，您可以使用此 IP 位址在命令列登入網格節點並執行各種維護程序。

開始之前

您已使用"支援的網頁瀏覽器"。

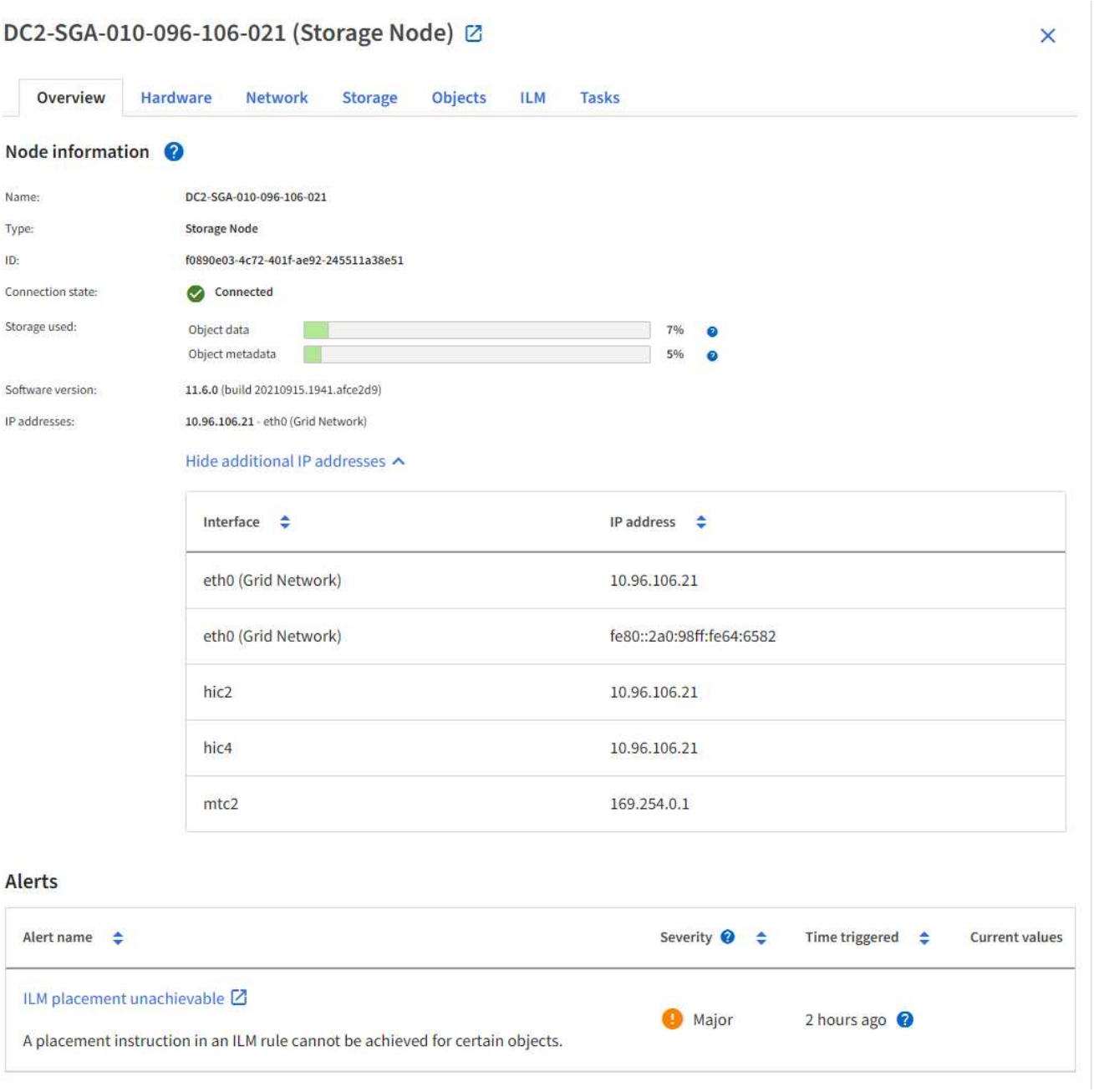
關於此任務

有關更改 IP 位址的信息，請參閱"配置 IP 位址"。

步驟

1. 選擇 **NODES** > ***grid node*** > **Overview**。
2. 選擇 IP 位址標題右側的 顯示更多。

   此網格節點的 IP 位址列在表中。



配置VLAN介面

您可以在管理節點和網關節點上建立虛擬 LAN (VLAN) 接口，並在 HA 群組和負載平衡器端點中使用它們來隔離和分區流量，從而實現安全性、靈活性和效能。HA 群組中選定的節點可以使用 VLAN 介面共用最多 10 個虛擬 IP 位址，這樣，如果一個節點發生故障，另一個節點將接管往返虛擬 IP 位址的流量。

VLAN 介面的注意事項

- 您可以透過輸入 VLAN ID 並在一個或多個節點上選擇父介面來建立 VLAN 介面。
- 必須在交換器上將父介面配置為中繼介面。
- 父介面可以是網格網路（eth0）、客戶端網路（eth2）或虛擬機器或裸機主機的附加中繼介面（例如

，ens256）。

- 對於每個 VLAN 接口，您只能為給定節點選擇一個父接口。例如，您不能將同一網關節點上的網格網路介面和用戶端網路介面同時用作相同 VLAN 的父介面。
- 如果 VLAN 介面用於管理節點流量（包括與網格管理器和租戶管理器相關的流量），則僅選擇管理節點上的介面。
- 如果 VLAN 介面用於 S3 用戶端流量，請選擇管理節點或網關節點上的介面。
- 如果需要新增Trunk接口，請參閱以下內容：
  - **VMware**（安裝節點後）："VMware：向節點新增中繼或存取介面"
  - **RHEL**（安裝節點之前）："建立節點設定檔"
  - **Ubuntu** 或 **Debian**（安裝節點之前）："建立節點設定檔"
  - **RHEL**、**Ubuntu** 或 **Debian**（安裝節點後）："Linux：為節點新增主幹或存取介面"

建立 **VLAN** 介面

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"Root存取權限"。
- 網路中已配置中繼介面並將其連接到 VM 或 Linux 節點。您知道中繼介面的名稱。
- 您知道正在設定的 VLAN 的 ID。

關於此任務

您的網路管理員可能已設定一個或多個中繼介面和一個或多個 VLAN 來隔離屬於不同應用程式或租用戶的用戶端或管理流量。每個 VLAN 由數位 ID 或標籤標識。例如，您的網路可能使用 VLAN 100 來傳輸FabricPool流量，使用 VLAN 200 來傳輸存檔應用程式。

您可以使用網格管理器建立 VLAN 接口，允許客戶端存取特定 VLAN 上的StorageGRID 。建立 VLAN 介面時，您可以指定 VLAN ID 並在一個或多個節點上選擇父（中繼）介面。

訪問嚮導

步驟

1. 選擇 配置 > 網路 > **VLAN** 介面。
2. 選擇“創建”。

輸入 **VLAN** 介面的詳細信息

步驟

1. 指定網路中 VLAN 的 ID。您可以輸入 1 到 4094 之間的任意值。

   VLAN ID 不需要是唯一的。例如，您可能在一個站點上使用 VLAN ID 200 來傳輸管理流量，而在另一個站點上使用相同的 VLAN ID 來傳輸客戶端流量。您可以在每個站點建立具有不同父介面集的單獨 VLAN 介面。但是，兩個具有相同 ID 的 VLAN 介面不能共用同一節點上的同一個介面。如果您指定的 ID 已被使用，則會出現一則訊息。

2. 或者，輸入 VLAN 介面的簡短描述。

3. 選擇*繼續*。

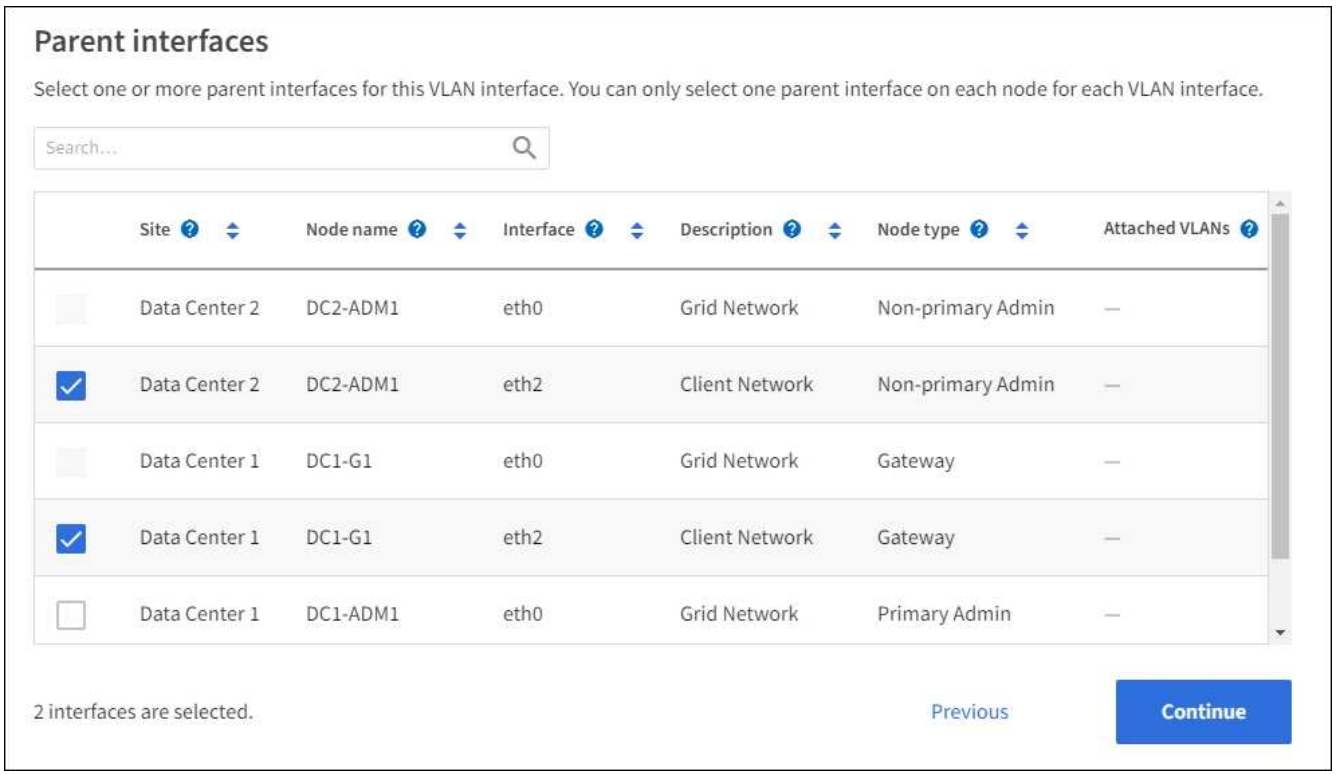
選擇父接口

此表列出了網格中每個站點的所有管理節點和網關節點的可用介面。管理網路（eth1）介面不能用作父接口，因此不會顯示。

步驟

1. 選擇一個或多個要將此 VLAN 附加到的父介面。

   例如，您可能想要將 VLAN 附加到網關節點和管理節點的用戶端網路 (eth2) 介面。



2. 選擇*繼續*。

確認設定

步驟

1. 檢查配置並進行任何更改。
   - 如果需要變更 VLAN ID 或描述，請選擇頁面頂部的 輸入 **VLAN** 詳細資料。
   - 如果需要變更父接口，請選擇頁面頂部的*選擇父接口*或選擇*上一個*。
   - 如果需要刪除父接口，請選擇垃圾桶。
2. 選擇*儲存*。
3. 等待最多 5 分鐘，新的介面才會作為選擇出現在「高可用性群組」頁面上，並列在節點的 網路介面 表中（**NODES** > ***parent interface node*** > **Network**）。

編輯 **VLAN** 介面

編輯 VLAN 介面時，您可以進行以下類型的變更：

- 更改 VLAN ID 或描述。
- 新增或刪除父介面。

例如，如果您計劃停用關聯節點，則可能需要從 VLAN 介面中刪除父介面。

請注意以下事項：

- 如果 VLAN 介面在 HA 群組中使用，則無法變更 VLAN ID。
- 如果父介面在 HA 群組中使用，則您無法刪除該父介面。

  例如，假設 VLAN 200 連接到節點 A 和 B 上的父介面。如果 HA 群組對節點 A 使用 VLAN 200 接口，對節點 B 使用 eth2 接口，則可以刪除節點 B 未使用的父接口，但不能刪除節點 A 已使用的父接口。

步驟

1. 選擇 配置 > 網路 > **VLAN** 介面。
2. 選取要編輯的 VLAN 介面的複選框。然後，選擇*動作* > 編輯。
3. 或者，更新 LAN ID 或描述。然後，選擇*繼續*。

   如果 VLAN 在 HA 群組中使用，則無法更新 VLAN ID。

4. 或者，選擇或清除複選框以新增父介面或刪除未使用的介面。然後，選擇*繼續*。
5. 檢查配置並進行任何更改。
6. 選擇*儲存*。

刪除 **VLAN** 介面

您可以刪除一個或多個 VLAN 介面。

如果 VLAN 介面目前在 HA 群組中使用，則無法刪除它。您必須先從 HA 群組中刪除 VLAN 介面，然後才能將其刪除。

為了避免客戶端流量中斷，請考慮執行以下操作之一：

- 刪除此 VLAN 介面之前，請先將新的 VLAN 介面新增至 HA 群組。
- 建立不使用此 VLAN 介面的新 HA 群組。
- 如果要刪除的 VLAN 介面目前是活動接口，請編輯 HA 群組。將要刪除的 VLAN 介面移至優先權清單的底部。等待新的主介面上建立通信，然後從 HA 群組中刪除舊介面。最後，刪除該節點上的 VLAN 介面。

步驟

1. 選擇 配置 > 網路 > **VLAN** 介面。
2. 選取要刪除的每個 VLAN 介面的複選框。然後，選擇*動作* > 刪除。
3. 選擇“是”確認您的選擇。

您選擇的所有 VLAN 介面都將被刪除。 VLAN 介面頁面上會出現綠色的成功橫幅。

管理流量分類策略

什麼是流量分類策略？

流量分類策略可讓您識別和監控不同類型的網路流量。這些策略可以幫助限制和監控流量，以增強您的服務品質 (QoS)。

流量分類策略應用於網關節點和管理節點的StorageGRID負載平衡器服務上的端點。若要建立流量分類策略，您必須已經建立負載平衡器端點。

匹配規則

每個流量分類策略包含一個或多個符合規則，用於識別與以下一個或多個實體相關的網路流量：

- 鏟鬥
- 子網
- 租戶
- 負載平衡器端點

StorageGRID根據規則的目標監控與策略內任何規則相符的流量。任何與策略規則相符的流量都由該策略處理。相反，您可以設定規則來符合除指定實體之外的所有流量。

限流

您可以選擇將以下限制類型新增至策略：

- 總頻寬
- 每個請求的頻寬
- 並發請求
- 請求率

限制值是根據每個負載平衡器強制執行的。如果流量同時分佈在多個負載平衡器之間，則總最大速率是您指定的速率限制的倍數。

> 您可以建立策略來限制總頻寬或限制每個要求的頻寬。但是， StorageGRID不能同時限制兩種類型的頻寬。總頻寬限制可能會對不受限制的流量造成額外的輕微效能影響。

對於聚合或每個請求的頻寬限制，請求以您設定的速率流入或流出。 StorageGRID只能強制執行一種速度，因此根據匹配器類型，最具體的政策匹配就是強制執行的策略。此請求消耗的頻寬不會計入包含聚合頻寬限制策略的其他不太具體的配對策略。對於所有其他限制類型，用戶端請求將延遲 250 毫秒，並且對於超出任何匹配策略限制的請求，將收到 503 Slow Down 回應。

在網格管理器中，您可以查看流量圖表並驗證策略是否正在執行您期望的流量限制。

您可以將流量分類策略與容量限制和資料保護結合使用，以強制執行提供容量、資料保護和效能細節的服務等級協定 (SLA)。

以下範例顯示了 SLA 的三個層級。您可以建立流量分類策略來實現每個 SLA 層的效能目標。

服務等級層	容量	資料保護	允許的最大性能	成本
金子	允許 1 PB 儲存空間	3 份 ILM 規則	25K 個請求/秒 5 GB/秒（40 Gbps）頻寬	$$$ 每月
銀	允許 250 TB 儲存空間	2 份 ILM 規則	每秒 10 K 個請求 1.25 GB/秒（10 Gbps）頻寬	每月$$
青銅	允許 100 TB 儲存空間	2 份 ILM 規則	5K 個請求/秒 1 GB/秒（8 Gbps）頻寬	$ 每月

建立流量分類策略

如果您想要監控，則可以建立流量分類策略，並選擇性地透過儲存桶、儲存桶正規表示式、CIDR、負載平衡器端點或租用戶限製網路流量。或者，您可以根據頻寬、並發請求數或請求率設定策略限制。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"Root存取權限"。
- 您已建立想要匹配的任何負載平衡器端點。
- 您已建立任何想要匹配的租戶。

步驟

1. 選擇*配置* > 網路 > 流量分類。
2. 選擇“創建”。
3. 輸入策略的名稱和描述（可選），然後選擇*繼續*。

   例如，描述此流量分類策略適用於什麼以及它將限制什麼。

4. 選擇*新增規則*並指定以下詳細資訊以為策略建立一個或多個符合規則。您建立的任何策略都應至少有一條符合規則。選擇*繼續*。

場地	描述
類型	選擇符合規則適用的流量類型。流量類型包括儲存桶、儲存桶正規表示式、CIDR、負載平衡器端點和租用戶。
匹配值	輸入與所選類型相符的值。 • 儲存桶：輸入一個或多個儲存桶名稱。 • Bucket regex：輸入一個或多個用來符合一組 bucket 名稱的正規表示式。 正規表示式未錨定。使用 ^ 錨點在 bucket 名稱的開頭進行匹配，並使用 $ 錨點在名稱的結尾進行匹配。正規表示式匹配支援 PCRE（Perl 相容正規表示式）語法的子集。 • CIDR：以 CIDR 表示法輸入與所需子網路相符的一個或多個 IPv4 子網路。 • 負載平衡器端點：選擇端點名稱。這些是您在"配置負載平衡器端點"。 • 租戶：租戶匹配使用存取密鑰ID。如果請求中不包含存取金鑰ID（例如匿名存取），則使用所存取的儲存桶的所有權來確定租用戶。
反向匹配	如果您想要符合剛剛定義的類型和符合值一致的流量之外的所有網路流量，請勾選「反向符合」複選框。否則，請清除該複選框。 例如，如果您希望此策略套用於除一個負載平衡器端點之外的所有端點，請指定要排除的負載平衡器端點，然後選擇*反向符合*。 對於包含多個匹配器（其中至少有一個是逆匹配器）的策略，請注意不要建立匹配所有請求的策略。

5. 或者，選擇*新增限制*並選擇以下詳細資訊以新增一個或多個限制來控制規則匹配的網路流量。

   即使您不新增任何限制， StorageGRID也會收集指標，因此您可以了解流量趨勢。

場地	描述
類型	您想要對規則相符的網路流量套用的限制類型。例如，您可以限制頻寬或請求速率。 注意：您可以建立策略來限制總頻寬或限制每個要求的頻寬。但是，StorageGRID不能同時限制兩種類型的頻寬。當聚合頻寬正在使用時，每個請求的頻寬不可用。相反，當每個請求的頻寬都在使用中時，聚合頻寬不可用。總頻寬限制可能會對不受限制的流量造成額外的輕微效能影響。 對於頻寬限制， StorageGRID會套用與限制集類型最相符的策略。例如，如果您有一個僅限制一個方向流量的策略，那麼相反方向的流量將不受限制，即使存在符合具有頻寬限制的其他策略的流量。 StorageGRID會依照下列順序實現頻寬限制的「最佳」配對： • 精確的 IP 位址（/32 遮罩） • 確切的儲存桶名稱 • 桶正規表示式 • 租戶 • 端點 • 非精確 CIDR 匹配（非 /32） • 反向匹配
適用於	此限制是否適用於客戶端讀取請求（GET 或 HEAD）或寫入請求（PUT 、POST 或 DELETE）。
價值	根據您選擇的單位，網路流量將被限制的值。例如輸入10並選擇MiB/s，則該規則所符合的網路流量不能超過10MiB/s。 注意：根據單位設置，可用的單位將是二進制（例如，GiB）或十進制（例如，GB）。若要變更單位設置，請選擇網格管理員右上角的使用者下拉式選單，然後選擇*使用者首選項*。
單元	描述您輸入的值的單位。

例如，如果您想要為 SLA 層建立 40 GB/s 的頻寬限制，請建立兩個聚合頻寬限制：GET/HEAD 為 40 GB/s ，PUT/POST/DELETE 為 40 GB/s。

6. 選擇*繼續*。
7. 閱讀並檢討流量分類政策。使用“上一步”按鈕返回並根據需要進行更改。當您對政策滿意時，選擇*保存並繼續*。

   S3 用戶端流量現在會根據流量分類策略進行處理。

完成後

"查看網路流量指標"驗證政策是否正在執行您期望的流量限制。

編輯流量分類策略

您可以編輯流量分類策略以變更其名稱或描述，或建立、編輯或刪除該策略的任何規則或限制。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"Root存取權限"。

步驟

1. 選擇*配置* > 網路 > 流量分類。

   出現「流量分類策略」頁面，現有策略列在表格中。

2. 使用「操作」功能表或詳細資料頁面編輯策略。看"建立流量分類策略"輸入什麼內容。

   操作選單

   a. 選取該策略的複選框。

   b. 選擇*操作* > 編輯。

   詳細資訊頁面

   a. 選擇策略名稱。

   b. 選擇策略名稱旁的“編輯”按鈕。

3. 對於輸入策略名稱步驟，可選擇編輯策略名稱或描述，然後選擇*繼續*。
4. 對於新增符合規則步驟，可選擇新增規則或編輯現有規則的*類型*和*符合值*，然後選擇*繼續*。
5. 對於設定限制步驟，可選擇新增、編輯或刪除限制，然後選擇*繼續*。
6. 查看更新後的政策，然後選擇*儲存並繼續*。

   您對策略所做的變更已儲存，現在將根據流量分類策略處理網路流量。您可以查看流量圖表並驗證策略是否正在執行您期望的流量限制。

刪除流分類策略

如果您不再需要某個流量分類策略，可以將其刪除。確保刪除正確的策略，因為刪除後將無法檢索策略。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"Root存取權限"。

步驟

1. 選擇*配置* > 網路 > 流量分類。

出現「流量分類策略」頁面，其中的現有策略列在表中。

2. 使用“操作”功能表或詳細資料頁面刪除策略。

操作選單

a. 選取該策略的複選框。

b. 選擇*操作* > 刪除。

政策詳情頁面

a. 選擇策略名稱。

b. 選擇策略名稱旁的“刪除”按鈕。

3. 選擇“是”確認您要刪除該策略。

該策略已刪除。

查看網路流量指標

您可以透過查看「流量分類策略」頁面提供的圖表來監控網路流量。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"根存取權限或租用戶帳戶權限"。

關於此任務

對於任何現有的流量分類策略，您可以查看負載平衡器服務的指標，以確定該策略是否成功限制了整個網路的流量。圖表中的數據可以幫助您確定是否需要調整策略。

即使沒有為流量分類策略設定限制，也會收集指標，圖表可以提供有用的資訊來了解流量趨勢。

步驟

1. 選擇*配置* > 網路 > 流量分類。

出現「流量分類策略」頁面，並在表格中列出現有策略。

2. 選擇要查看其指標的流量分類策略名稱。
3. 選擇“**Metrics**”選項卡。

出現流量分類策略圖表。圖表僅顯示與所選策略相符的流量的指標。

此頁麵包含以下圖表。

- 請求率：此圖表提供所有負載平衡器處理的符合此策略的頻寬量。接收到的資料包括所有請求的請求標頭以及包含正文資料的回應的正文資料大小。已發送包括所有請求的回應標頭以及回應中包含正文資料的請求的回應正文資料大小。

當請求完成時，此圖表僅顯示頻寬使用量。對於緩慢或較大的物件請求，實際瞬時頻寬可能與此圖中報告的值不同。

- 錯誤回應率：此圖表提供與此策略相符的請求向客戶端傳回錯誤（HTTP 狀態碼 >= 400）的大致速率。
- 平均請求持續時間（非錯誤）：此圖表提供符合此策略的成功請求的平均持續時間。
- 策略頻寬使用量：此圖表提供所有負載平衡器處理的與此策略相符的頻寬量。接收到的資料包括所有請求的請求標頭以及包含正文資料的回應的正文資料大小。已發送包括所有請求的回應標頭以及回應中包含正文資料的請求的回應正文資料大小。

4. 將遊標放在折線圖上即可查看圖表特定部分的彈出值。
5. 選擇「Metrics」標題正下方的「Grafana dashboard」來查看策略的所有圖表。除了「**Metrics**」標籤中的四個圖表之外，您還可以查看另外兩個圖表：
   - 依物件大小的寫入請求率：符合此策略的 PUT/POST/DELETE 請求的速率。單一單元格上的定位顯示每秒的速率。懸停視圖中顯示的速率將被截斷為整數計數，並且當儲存桶中有非零請求時可能會報告 0。
   - 依物件大小讀取請求率：符合此策略的 GET/HEAD 請求的速率。單一單元格上的定位顯示每秒的速率。懸停視圖中顯示的速率將被截斷為整數計數，並且當儲存桶中有非零請求時可能會報告 0。
6. 或者，從*SUPPORT*選單存取圖表。
   a. 選擇*支援* > 工具 > 指標。
   b. 從 **Grafana** 部分選擇 流量分類策略。
   c. 從頁面左上角的選單中選擇策略。
   d. 將遊標放在圖表上即可看到彈出窗口，其中顯示樣本的日期和時間、聚合到計數中的物件大小以及該時間段內每秒的請求數。

      流量分類策略透過其 ID 來識別。策略 ID 列在流量分類策略頁面上。
7. 分析圖表以確定策略限制流量的頻率以及是否需要調整策略。

傳出 **TLS** 連線支援的密碼

StorageGRID系統支援一組有限的密碼套件，用於與用於身分聯合和雲端儲存池的外部系統建立傳輸層安全性 (TLS) 連線。

支援的 **TLS** 版本

StorageGRID支援 TLS 1.2 和 TLS 1.3，用於連接用於身分識別聯合和雲端儲存池的外部系統。

已選擇支援與外部系統一起使用的 TLS 密碼，以確保與一系列外部系統相容。此清單大於支援與 S3 用戶端應用程式一起使用的密碼清單。若要設定密碼，請前往 設定 > 安全 > 安全設定 並選擇 **TLS** 和 **SSH** 原則。

TLS 設定選項（例如協定版本、密碼、金鑰交換演算法和 MAC 演算法）在StorageGRID中無法設定。如果您對這些設定有具體要求，請聯絡您的NetApp客戶代表。

活動、空閒和並發 **HTTP** 連線的優勢

如何設定 HTTP 連線會影響StorageGRID系統的效能。配置會根據 HTTP 連線是處於活動狀態還是空閒狀態或您是否有並發的多個連線而有所不同。

您可以確定以下類型的 HTTP 連線的效能優勢：

- 空閒 HTTP 連接
- 活動的 HTTP 連接
- 並發 HTTP 連接

保持空閒 **HTTP** 連線開放的好處

即使客戶端應用程式處於空閒狀態，您也應該保持 HTTP 連線打開，以允許客戶端應用程式透過開啟的連線執行後續交易。根據系統測量和整合經驗，您應該保持空閒 HTTP 連線最多開放 10 分鐘。 StorageGRID可能會自動關閉保持開啟狀態並空閒超過 10 分鐘的 HTTP 連線。

開啟和空閒的 HTTP 連線具有以下優點：

- 減少從StorageGRID系統決定必須執行 HTTP 交易到StorageGRID系統可以執行交易的延遲

  減少延遲是主要優勢，尤其是建立 TCP/IP 和 TLS 連線所需的時間。

- 透過使用先前執行的傳輸來啟動 TCP/IP 慢啟動演算法來提高資料傳輸速率
- 即時通知中斷客戶端應用程式和StorageGRID系統之間連接的幾類故障情況

確定保持空閒連線開啟的時間長度是與現有連線相關的慢啟動的好處與將連線理想地分配給內部系統資源之間的權衡。

主動 **HTTP** 連線的好處

對於直接連接到儲存節點，您應該將活動 HTTP 連線的持續時間限制為最多 10 分鐘，即使 HTTP 連線持續執行交易。

確定連接保持開啟的最長持續時間是連接持久性的好處和將連接理想地分配到內部系統資源之間的權衡。

對於客戶端與儲存節點的連接，限制活動的 HTTP 連接具有以下好處：

- 實現StorageGRID系統內的最佳負載平衡。

  隨著時間的推移，由於負載平衡要求的變化，HTTP 連接可能不再是最佳的。當用戶端應用程式為每個交易建立單獨的 HTTP 連線時，系統會執行最佳的負載平衡，但這會抵消與持久連線相關的更有價值的效益。

- 允許客戶端應用程式將 HTTP 事務定向到具有可用空間的 LDR 服務。
- 允許啟動維護程序。

  某些維護程序僅在所有正在進行的 HTTP 連線完成後才啟動。

對於與負載平衡器服務的用戶端連接，限制開啟連線的持續時間對於允許某些維護程序及時啟動很有用。如果用戶端連線的持續時間不受限制，則活動連線可能需要幾分鐘才能自動終止。

並發 **HTTP** 連線的好處

您應該保持與StorageGRID系統的多個 TCP/IP 連線處於開啟狀態以允許並行，從而提高效能。最佳並行連線數取決於多種因素。

並發 HTTP 連線具有以下優勢：

- 減少延遲

  交易可以立即開始，而不必等待其他交易完成。

- 提高吞吐量

  StorageGRID系統可以執行並行事務並增加總事務吞吐量。

客戶端應用程式應該建立多個 HTTP 連線。當客戶端應用程式必須執行事務時，它可以選擇並立即使用任何目前未處理交易的已建立連線。

在效能開始下降之前，每個StorageGRID系統的拓撲對於並發事務和連接都有不同的峰值吞吐量。峰值吞吐量取決於運算資源、網路資源、儲存資源和 WAN 鏈路等因素。 StorageGRID系統支援的伺服器和服務的數量以及應用程式的數量也是影響因素。

StorageGRID系統通常支援多個客戶端應用程式。在確定客戶端應用程式使用的最大並發連線數時，應牢記這一點。如果用戶端應用程式由多個軟體實體組成，每個實體都與StorageGRID系統建立連接，則應將跨實體的所有連接加起來。在以下情況下，您可能需要調整最大並發連線數：

- StorageGRID系統的拓樸影響系統可以支援的最大並發事務和連線數。
- 透過頻寬有限的網路與StorageGRID系統互動的客戶端應用程式可能必須降低並發度，以確保各個事務在合理的時間內完成。
- 當許多客戶端應用程式共用StorageGRID系統時，您可能必須降低並發度以避免超出系統的限制。

分離用於讀取和寫入操作的 **HTTP** 連線池

您可以使用單獨的 HTTP 連線池進行讀取和寫入操作，並控制每個操作使用的池量。單獨的 HTTP 連線池可讓您更好地控制事務和平衡負載。

客戶端應用程式可以建立以檢索為主（讀取）或以儲存為主（寫入）的負載。透過為讀取和寫入事務提供單獨的 HTTP 連線池，您可以調整每個池中用於讀取或寫入交易的連線數量。

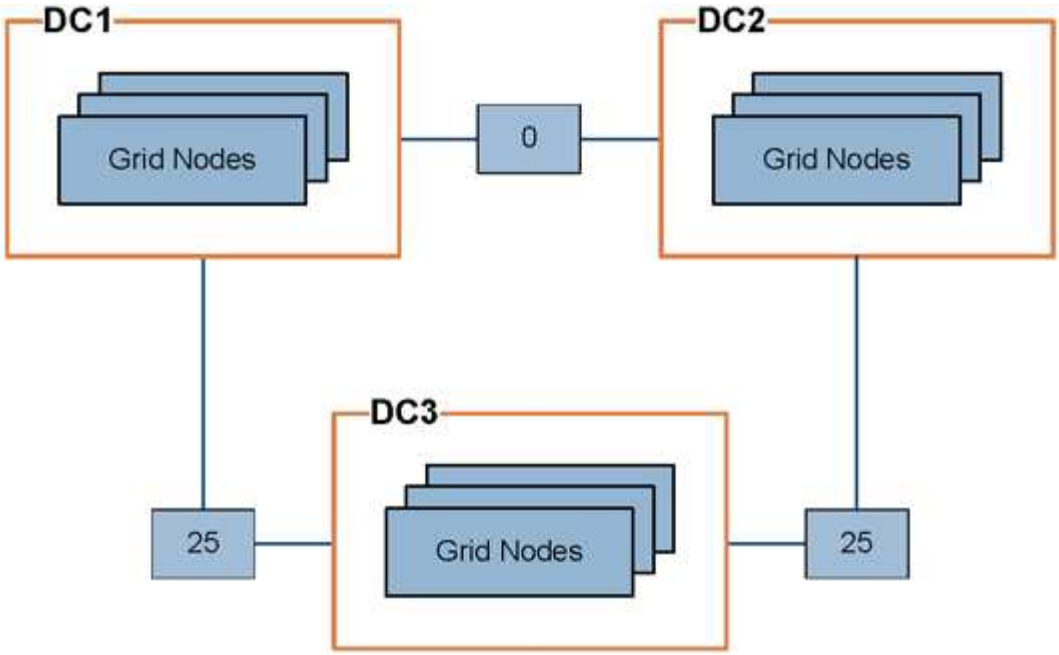
管理連結成本

當存在兩個或多個資料中心站點時，連結成本可讓您確定哪個資料中心站點優先提供所要求的服務。您可以調整連結成本以反映網站之間的延遲。

什麼是連結成本？

- 連結成本用於決定使用哪個物件副本來完成物件檢索的優先順序。
- 網格管理 API 和租用戶管理 API 使用連結成本來決定使用哪些內部StorageGRID服務。
- 管理節點和網關節點上的負載平衡器服務使用連結成本來引導客戶端連線。看"負載平衡的注意事項" 。

該圖顯示了一個三站點網格，其中站點之間配置了連結成本：



- 管理節點和網關節點上的負載平衡器服務將客戶端連接平均分配給同一資料中心站點的所有儲存節點以及連結成本為 0 的任何資料中心站點。

  在範例中，資料中心站點 1 (DC1) 的網關節點將用戶端連線平均指派給 DC1 的儲存節點和 DC2 的儲存節點。 DC3 處的網關節點僅將客戶端連線傳送至 DC3 處的儲存節點。

- 當擷取作為多個複製副本存在的物件時， StorageGRID會擷取具有最低連結成本的資料中心的副本。

  在範例中，如果 DC2 上的用戶端應用程式檢索同時儲存在 DC1 和 DC3 上的對象，則會從 DC1 檢索該對象，因為從 DC1 到 DC2 的連結成本為 0，低於從 DC3 到 DC2 的連結成本 (25)。

連結成本是任意相對數字，沒有特定的計量單位。例如，連結成本 50 的使用優先順序低於連結成本 25。此表顯示了常用的鏈路成本。

關聯	鏈路成本	筆記
實體資料中心站點之間	25（預設值）	透過 WAN 連結連接的資料中心。
同一實體位置的邏輯資料中心站點之間	0	同一實體建築物或校園內的邏輯資料中心透過 LAN 連線。

更新連結成本

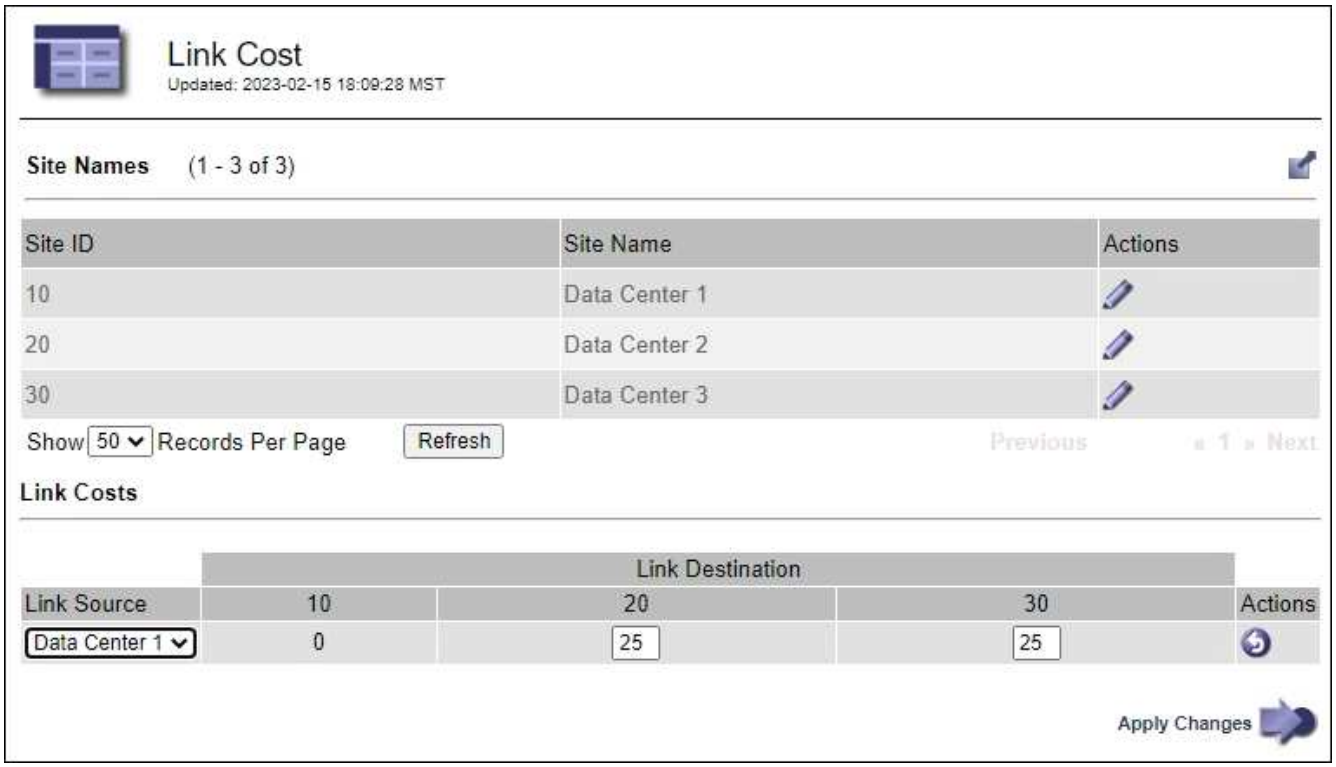
您可以更新資料中心網站之間的連結成本以反映網站之間的延遲。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"電網拓撲頁面配置權限"。

步驟

1. 選擇 支援 > 其他 > 連結成本。



2. 在*連結來源*下選擇一個站點，並在*連結目標*下輸入 0 到 100 之間的成本值。

   如果來源與目的地相同，則無法更改連結成本。

   若要取消更改，請選擇 恢復。

3. 選擇*應用變更*。

使用AutoSupport

什麼是AutoSupport？

AutoSupport功能使StorageGRID能夠將健康和狀態包傳送給NetApp技術支援。

使用AutoSupport可以顯著加快問題的確定和解決速度。技術支援還可以監控系統的儲存需求，並幫助您確定是否需要新增節點或網站。或者，您可以設定AutoSupport套件以傳送到另一個目的地。

StorageGRID有兩種類型的AutoSupport：

- * StorageGRID AutoSupport* 回報StorageGRID軟體問題。首次安裝StorageGRID時預設啟用。你可以"更改預設AutoSupport配置"如果需要的話。

> 如果未啟用StorageGRID AutoSupport ，網格管理器儀表板上會出現一則訊息。該訊息包含指向AutoSupport設定頁面的連結。如果您關閉該訊息，即使AutoSupport保持停用狀態，它也不會再次出現，直到您的瀏覽器快取已清除。

- 設備硬體**AutoSupport** 回報StorageGRID設備問題。你必須"在每個設備上配置硬體AutoSupport"。

什麼是**Active IQ**？

Active IQ是一個基於雲端的數位顧問，它利用 NetApp 安裝基礎的預測分析和社群智慧。其持續的風險評估、預測警報、規範指導和自動化操作可幫助您預防問題的發生，從而改善系統健康並提高系統可用性。

如果您想使用NetApp支援網站上的Active IQ儀表板和功能，則必須啟用AutoSupport。

"Active IQDigital Advisor文檔"

AutoSupport包中包含的訊息

AutoSupport包包含以下文件和詳細資訊。

檔案名稱	欄位	描述
自動支援歷史記錄.XML	AutoSupport序號 + 此AutoSupport的目標 + 傳送狀態 + 傳送嘗試次數 + AutoSupport主題 + 傳送 URI + 上一個錯誤 + AutoSupport PUT 檔案名稱 + 產生時間 + AutoSupport 壓縮大小 + AutoSupport 解壓縮大小 + 總收集時間（毫秒）	AutoSupport歷史檔案。
自動支援.XML	節點 + 聯絡支援的協定 + HTTP/HTTPS 的支援 URL + 支援位址 + AutoSupport OnDemand 狀態 + AutoSupport OnDemand 伺服器 URL + AutoSupport OnDemand 輪詢間隔	AutoSupport狀態檔案。提供所用協定、技術支援 URL 和位址、輪詢間隔以及 OnDemand AutoSupport （如果啟用或停用）的詳細資訊。
桶.XML	儲存桶 ID + 帳戶 ID + 建置版本 + 位置約束配置 + 合規性已啟用 + 合規性配置 + S3 物件鎖定已啟用 + S3 物件鎖定配置 + 一致性配置 + CORS 已啟用 + CORS 配置 + 上次存取時間已啟用 + 原則已啟用 + 策略配置 + 通知已啟用 + 配置設定 + 鏡像配置已啟用 + 原則已啟用 + 策略配置 + 通知已啟用 + 配置設定 + 工具已啟用配置已啟用設定 空間已啟用標記儲存桶標記配置 + 版本控製配置	提供儲存桶層級的配置詳細資訊和統計資訊。儲存桶配置的範例包括平台服務、合規性和儲存桶一致性。

檔案名稱	欄位	描述
網格配置.XML	屬性ID+屬性名稱+值+索引+表ID+表名稱	網格範圍的設定資訊檔。包含有關網格證書、元資料保留空間、網格範圍配置設定（合規性、S3 物件鎖定、物件壓縮、警報、系統日誌和 ILM 配置）、擦除編碼設定檔詳細資訊、DNS 名稱和"NMS 名稱"。
網格規範.XML	網格規範，原始 XML	用於設定和部署StorageGRID。包含網格規格、NTP 伺服器 IP、DNS 伺服器 IP、網路拓撲和節點的硬體設定檔。
網格任務.XML	節點+服務路徑+屬性ID+屬性名稱+值+索引+表ID+表名稱	網格任務（維護程序）狀態檔。提供網格的活動、終止、完成、失敗和待處理任務的詳細資訊。
網格.JSON	網格 + 修訂 + 軟體版本 + 說明 + 許可證 + 密碼 + DNS + NTP + 網站 + 節點	電網資訊。
ILM配置.XML	屬性ID+屬性名稱+值+索引+表ID+表名稱	ILM 配置的屬性清單。
ILM-狀態.XML	節點+服務路徑+屬性ID+屬性名稱+值+索引+表ID+表名稱	ILM 指標資訊文件。包含每個節點的 ILM 評估率和網格範圍指標。
工業生命週期管理XML	ILM 原始 XML	ILM 活動策略文件。包含有關活動 ILM 策略的詳細信息，例如儲存池 ID、提取行為、過濾器、規則和描述。
LOG.TGZ	無	可下載的日誌檔。包含 `bycast-err.log`和 `servermanager.log`來自每個節點。
清單.XML	收集順序 + 此資料的AutoSupport內容檔案名稱 + 此資料項目的描述 + 收集的位元組數 + 收集所用時間 + 此資料項目的狀態 + 錯誤描述 + 此資料的AutoSupport內容類型	包含AutoSupport元資料和所有AutoSupport檔案的簡要說明。
NMS-實體.XML	屬性索引+實體OID+節點ID+設備型號ID+設備型號版本+實體名稱	集團和服務實體"NMS樹"。提供電網拓撲詳細資訊。可以根據節點上運行的服務來確定節點。
物件狀態.XML	節點+服務路徑+屬性ID+屬性名稱+值+索引+表ID+表名稱	物件狀態，包括後台掃描狀態、活動傳輸、傳輸速率、總傳輸、刪除速率、損壞的片段、遺失的物件、缺少的物件、嘗試修復、掃描速率、估計掃描時間和修復完成狀態。

檔案名稱	欄位	描述
伺服器狀態.XML	節點+服務路徑+屬性ID+屬性名稱+值+索引+表ID+表名稱	伺服器配置。包含每個節點的以下詳細資訊：平台類型、作業系統、已安裝記憶體、可用記憶體、儲存連接、儲存裝置底盤序號、儲存控制器故障磁碟機數量、運算控制器底盤溫度、運算硬體、運算控制器序號、電源、磁碟機大小和磁碟機類型。
服務狀態.XML	節點+服務路徑+屬性ID+屬性名稱+值+索引+表ID+表名稱	服務節點資訊檔。包含已指派表空間、可用表空間、資料庫的 Reaper 指標、段修復持續時間、修復作業持續時間、自動作業重新啟動和自動作業終止等詳細資訊。
儲存等級.XML	儲存等級ID+儲存等級名稱+儲存節點ID+儲存節點路徑	每個儲存節點的儲存等級定義檔。
摘要屬性.XML	群組 OID + 群組路徑 + 摘要屬性 ID + 摘要屬性名稱 + 值 + 索引 + 表 ID + 表名稱	總結StorageGRID使用量資訊的高階系統狀態資料。提供網格名稱、站點名稱、每個網格和每個站點的儲存節點數、許可證類型、許可證容量和使用情況、軟體支援條款以及 S3 操作的詳細資訊。
系統警報.XML	名稱 + 嚴重程度 + 節點名稱 + 警報狀態 + 站點名稱 + 警報觸發時間 + 警報解決時間 + 規則 ID + 節點 ID + 站點 ID + 已靜音 + 其他註釋 + 其他標籤	目前系統警示表示StorageGRID系統中存在潛在問題。
用戶代理.XML	使用者代理 + 天數 + HTTP 請求總數 + 提取的總位元組數 + 檢索的總位元組數 + PUT 請求 + GET 請求 + DELETE 請求 + HEAD 請求 + POST 請求 + OPTIONS 請求 + 平均請求時間（毫秒）+ 平均 PUT 請求時間（毫秒）+ 20 毫秒）請求時間（毫秒）+ 平均 POST 請求時間（毫秒）+ 平均 OPTIONS 請求時間（毫秒）	基於應用程式用戶代理的統計。例如，每個使用者代理程式的 PUT/GET/DELETE/HEAD 操作數以及每個操作的總位元組大小。
X-頭數據	X-Netapp-asup-產生的+ X-Netapp-asup-主機名稱 + X-Netapp-asup-os-版本 + X-Netapp-asup-序號 + X-Netapp-asup-主題 + X-Netapp-asup-系統-id + X-Netapp-asup-模型名稱	AutoSupport標頭資料。

配置AutoSupport

預設情況下，首次安裝StorageGRID時會啟用StorageGRID AutoSupport功能。但是，您必須在每個裝置上設定硬體AutoSupport 。根據需要，您可以變更AutoSupport配置。

如果要變更StorageGRID AutoSupport的配置，請僅在主管理節點上進行變更。你必須配置硬體AutoSupport在每台設備上。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"Root存取權限"。
- 如果您將使用 HTTPS 傳送AutoSupport軟體包，則您已提供對主管理節點的出站網路存取（直接或"使用代理伺服器"（不需要入站連線）。
- 如果在StorageGRID AutoSupport頁面上選擇了 HTTP，則您必須"配置了代理伺服器"將AutoSupport包轉送為 HTTPS。 NetApp 的AutoSupport伺服器將拒絕使用 HTTP 傳送的套件。
- 如果您將使用 SMTP 作為AutoSupport軟體套件的協議，則您已設定 SMTP 郵件伺服器。

關於此任務

您可以使用下列選項的任何組合將AutoSupport套件傳送給技術支援：

- 每週：每週自動發送一次AutoSupport包。預設設定：已啟用。
- 事件觸發：每小時或發生重大系統事件時自動發送AutoSupport包。預設設定：已啟用。
- 按需：允許技術支援請求您的StorageGRID系統自動發送AutoSupport包，這在他們積極解決問題時很有用（需要 HTTPS AutoSupport傳輸協定）。預設設定：禁用。
- 使用者觸發：隨時手動發送AutoSupport套件。

[[specify-protocol-for- AutoSupport -packages]]指定AutoSupport軟體包的協議

您可以使用下列任何協定傳送AutoSupport套件：

- **HTTPS**：這是新安裝的預設和建議設定。該協定使用連接埠 443。如果你想啟用AutoSupport on Demand功能，則必須使用 HTTPS。
- **HTTP**：如果選擇 HTTP，則必須設定代理伺服器以將AutoSupport套件轉送為 HTTPS。 NetApp的AutoSupport伺服器拒絕使用 HTTP 傳送的套件。該協定使用連接埠 80。
- **SMTP**：如果您希望透過電子郵件傳送AutoSupport包，請使用此選項。

您設定的協定用於傳送所有類型的AutoSupport套件。

步驟

1. 選擇 支援 > 工具 > **AutoSupport** > 設定。
2. 選擇要用於發送AutoSupport套件的協定。
3. 如果您選擇了 **HTTPS**，請選擇是否使用NetApp支援憑證（TLS 憑證）來保護與技術支援伺服器的連線。
   - 驗證憑證（預設）：確保AutoSupport套件的傳輸是安全的。 NetApp支援憑證已隨StorageGRID軟體一起安裝。

。不驗證憑證：只有當您有充分的理由不使用憑證驗證時才選擇此選項，例如當憑證出現臨時問題時。

4. 選擇*儲存*。所有每週、使用者觸發和事件觸發的套件均使用所選協定發送。

停用每週**AutoSupport**

預設情況下， StorageGRID系統配置為每週一次向技術支援發送AutoSupport套件。

若要確定何時發送每週AutoSupport包，請前往 * AutoSupport* > 結果 標籤。在「每週AutoSupport」部分中，查看「下一個計畫時間」的值。

您可以隨時停用每週AutoSupport套件的自動傳送。

步驟

1. 選擇 支援 > 工具 > **AutoSupport** > 設定。
2. 清除「啟用每周AutoSupport」複選框。
3. 選擇*儲存*。

停用事件觸發的**AutoSupport**

預設情況下， StorageGRID系統配置為每小時向技術支援發送AutoSupport套件。

您可以隨時停用事件觸發的AutoSupport 。

步驟

1. 選擇 支援 > 工具 > **AutoSupport** > 設定。
2. 清除「啟用事件觸發的AutoSupport」複選框。
3. 選擇*儲存*。

按需啟用**AutoSupport**

AutoSupport on Demand 可以協助解決技術支援正在積極處理的問題。

預設情況下， AutoSupport on Demand 處於停用狀態。啟用此功能可允許技術支援請求您的StorageGRID系統自動傳送AutoSupport套件。技術支援還可以設定AutoSupport on Demand 查詢的輪詢時間間隔。

技術支援無法按需啟用或停用AutoSupport 。

步驟

1. 選擇 支援 > 工具 > **AutoSupport** > 設定。
2. 選擇 **HTTPS** 作為協定。
3. 選取「啟用每周AutoSupport」複選框。
4. 選取「按需啟用AutoSupport」複選框。
5. 選擇*儲存*。

   AutoSupport on Demand 已啟用，技術支援可以向StorageGRID發送AutoSupport on Demand 請求。

停用軟體更新檢查

預設情況下， StorageGRID會聯絡NetApp以確定您的系統是否有可用的軟體更新。如果有StorageGRID修補程式或新版本可用，則新版本將顯示在StorageGRID升級頁面上。

根據需要，您可以選擇停用軟體更新檢查。例如，如果您的系統沒有 WAN 存取權限，您應該停用檢查以避免下載錯誤。

步驟

1. 選擇 支援 > 工具 > **AutoSupport** > 設定。
2. 清除*檢查軟體更新*複選框。
3. 選擇*儲存*。

新增其他**AutoSupport**目標

當您啟用AutoSupport時，健康和狀態套件將發送給技術支援。您可以為所有AutoSupport套件指定一個額外的目標。

若要驗證或變更用於傳送AutoSupport套件的協議，請參閱指定AutoSupport軟體包的協議。

> ⓘ 您不能使用 SMTP 協定將AutoSupport套件傳送到其他目的地。

步驟

1. 選擇 支援 > 工具 > **AutoSupport** > 設定。
2. 選擇“啟用附加AutoSupport目標”*。
3. 指定以下內容：

   主機名稱
   附加AutoSupport目標伺服器的伺服器主機名稱或 IP 位址。

   > ⓘ 您只能輸入一個附加目的地。

   港口
   用於連接到其他AutoSupport目標伺服器的連接埠。預設為 HTTP 連接埠 80 或 HTTPS 連接埠 443。

   證書驗證
   是否使用 TLS 憑證來保護與其他目的地的連線。

   - 選擇*驗證證書*以使用證書驗證。
   - 選擇「不驗證憑證」以傳送不經過憑證驗證的AutoSupport套件。

     只有當您有充分理由不使用憑證驗證時才選擇此選項，例如當憑證出現臨時問題時。

4. 如果您選擇了*驗證證書*，請執行以下操作：
   a. 瀏覽到 CA 憑證的位置。
   b. 上傳CA憑證檔案。

出現 CA 憑證元資料。

5. 選擇*儲存*。

所有未來的每週、事件觸發和用戶觸發的AutoSupport包都將發送到其他目的地。

為設備配置**AutoSupport**

設備的AutoSupport報告StorageGRID硬體問題， StorageGRID AutoSupport報告StorageGRID軟體問題，但有一個例外：對於 SGF6112， StorageGRID AutoSupport同時報告硬體和軟體問題。您必須在 SGF6112 以外的每台裝置上設定AutoSupport ，因為 SGF6112 不需要額外的設定。 AutoSupport對於服務設備和儲存設備的實作方式不同。

您可以使用SANtricity為每個儲存設備啟用AutoSupport 。您可以在初始設備設定期間或設備安裝後配置SANtricity AutoSupport ：

- 對於 SG6000 和 SG5700 設備， "在SANtricity System Manager 中配置AutoSupport"

如果您在 StorageGRID AutoSupport中設定了代理AutoSupport交付，則 E 系列裝置的AutoSupport軟體套件可以包含在StorageGRID AutoSupport 中"SANtricity系統管理員"。

StorageGRID AutoSupport不會回報硬體問題，例如 DIMM 或主機介面卡 (HIC) 故障。然而，某些組件故障可能會引發"硬體警報"。對於具有基板管理控制器（BMC）的StorageGRID設備，您可以設定電子郵件和 SNMP 陷阱來報告硬體故障：

- "設定BMC警報的電子郵件通知"
- "為BMC配置 SNMP 設定"

相關資訊

"NetApp支援"

手動觸發**AutoSupport**包

為了協助技術支援解決您的StorageGRID系統的問題，您可以手動觸發發送AutoSupport套件。

開始之前

- 您必須使用"支援的網頁瀏覽器"。
- 您必須具有 Root 存取權限或其他網格配置權限。

步驟

1. 選擇 **SUPPORT** > **Tools** > * AutoSupport*。
2. 在「操作」標籤上，選擇「傳送使用者觸發的AutoSupport*」。

StorageGRID嘗試將AutoSupport套件傳送到NetApp支援站點。如果嘗試成功，則*結果*標籤上的*最近結果*和*上次成功時間*值將會更新。如果出現問題，*最新結果*值將更新為“失敗”，且StorageGRID不會再次嘗試傳送AutoSupport套件。

發送使用者觸發的AutoSupport套件後，請在 1 分鐘後刷新瀏覽器中的AutoSupport頁面以存取最新結果。

排除**AutoSupport**軟體套件故障

如果嘗試傳送AutoSupport套件失敗， StorageGRID系統將根據AutoSupport套件的類型採取不同的操作。您可以選擇 **SUPPORT** > **Tools** > * AutoSupport * > **Results** 來檢查AutoSupport套件的狀態。

當AutoSupport套件發送失敗時， AutoSupport頁面的「結果」標籤上將顯示「失敗」。

如果您設定了代理伺服器以將AutoSupport軟體套件轉送至NetApp，則應"驗證代理伺服器設定是否正確"。

每週**AutoSupport**包失敗

如果每週AutoSupport套件發送失敗， StorageGRID系統將採取以下措施：

1. 將最新結果屬性更新為重試。
2. 嘗試每四分鐘重新發送AutoSupport包 15 次，持續一小時。
3. 發送失敗一小時後，將「最新結果」屬性更新為「失敗」。
4. 嘗試在下一個計劃時間再次發送AutoSupport套件。
5. 如果由於 NMS 服務無法使用而導致軟體包失敗，且軟體包在七天之內發送，則維持常規AutoSupport計劃。
6. 當 NMS 服務再次可用時，如果七天或更長時間未發送包，則立即發送AutoSupport包。

使用者觸發或事件觸發的**AutoSupport**套件故障

如果使用者觸發或事件觸發的AutoSupport包發送失敗， StorageGRID系統將採取以下措施：

1. 如果已知錯誤，則顯示錯誤訊息。例如，如果使用者選擇 SMTP 協定而沒有提供正確的電子郵件配置設置，則會顯示以下錯誤： `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. 不再嘗試發送包裹。
3. 將錯誤記錄在 `nms.log`。

如果發生故障且 SMTP 是選定的協議，請驗證StorageGRID系統的電子郵件伺服器是否正確配置以及您的電子郵件伺服器是否正在執行（支援 > 警報（舊版） > 舊版電子郵件設定）。AutoSupport頁面上可能會出現以下錯誤訊息： `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

了解如何"設定電子郵件伺服器設定"。

糾正**AutoSupport**故障

如果發生故障且 SMTP 是選定的協議，請驗證StorageGRID系統的電子郵件伺服器是否已正確配置以及您的電子郵件伺服器是否正在執行。AutoSupport頁面上可能會出現以下錯誤訊息： `AutoSupport packages`

cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.

透過StorageGRID發送 E 系列AutoSupport包

您可以透過StorageGRID管理節點（而非儲存設備管理連接埠）將 E 系列SANtricity System Manager AutoSupport套件傳送給技術支援。

看 "E系列硬體AutoSupport"有關將AutoSupport與 E 系列設備結合使用的詳細資訊。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"儲存設備管理員或 Root 存取權限"。
- 您已設定SANtricity AutoSupport：
  - 對於 SG6000 和 SG5700 設備， "在SANtricity System Manager 中配置AutoSupport"

> 您必須擁有SANtricity韌體 8.70 或更高版本才能使用網格管理器存取SANtricity System Manager。

關於此任務

E 系列AutoSupport套件包含儲存硬體的詳細信息，並且比StorageGRID系統發送的其他AutoSupport套件更具體。

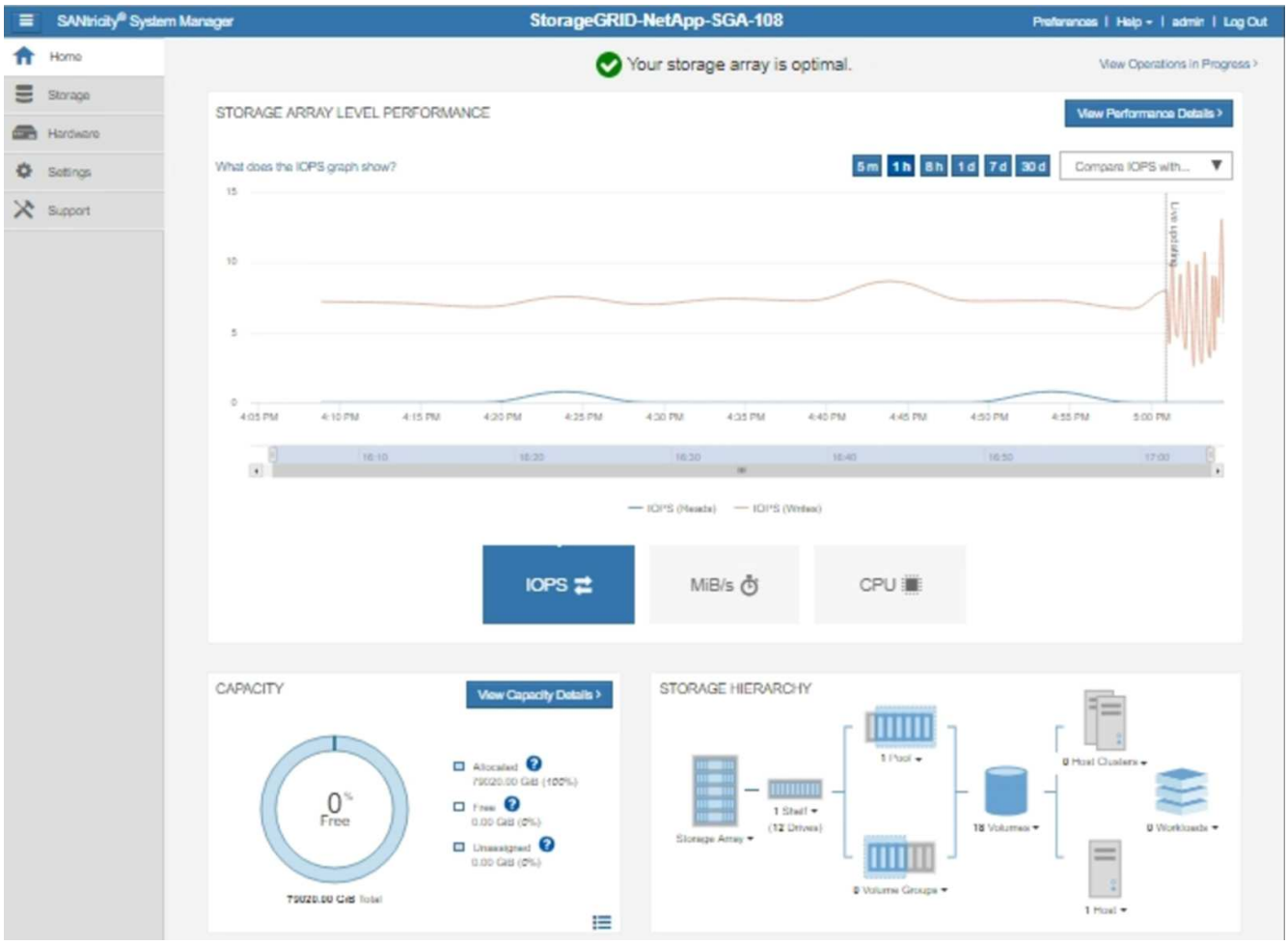
您可以在SANtricity System Manager 中設定一個特殊的代理伺服器位址，以便透過StorageGRID管理節點傳輸AutoSupport包，而無需使用設備的管理連接埠。以這種方式傳輸的AutoSupport包由"首選發送者管理節點"，他們使用任何"管理員代理設定"已在網格管理器中配置。

> 此程序僅適用於為 E 系列AutoSupport套件配置StorageGRID代理伺服器。有關 E 系列AutoSupport配置的更多詳細信息，請參閱 "NetApp E 系列和SANtricity文檔"。

步驟

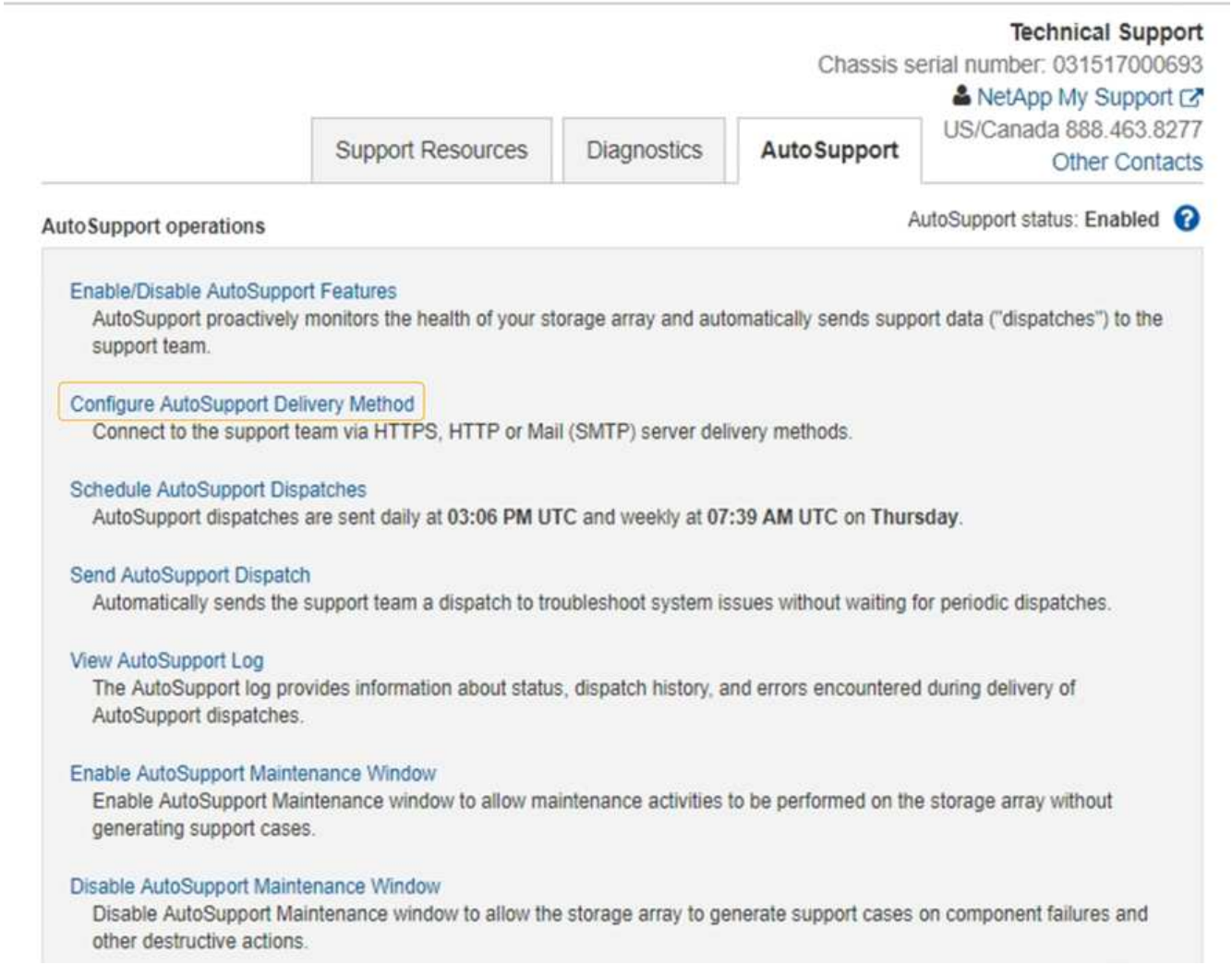
1. 在網格管理器中，選擇*NODES*。
2. 從左側的節點清單中，選擇要設定的儲存設備節點。
3. 選擇* SANtricity System Manager*。

   出現SANtricity System Manager 主頁。



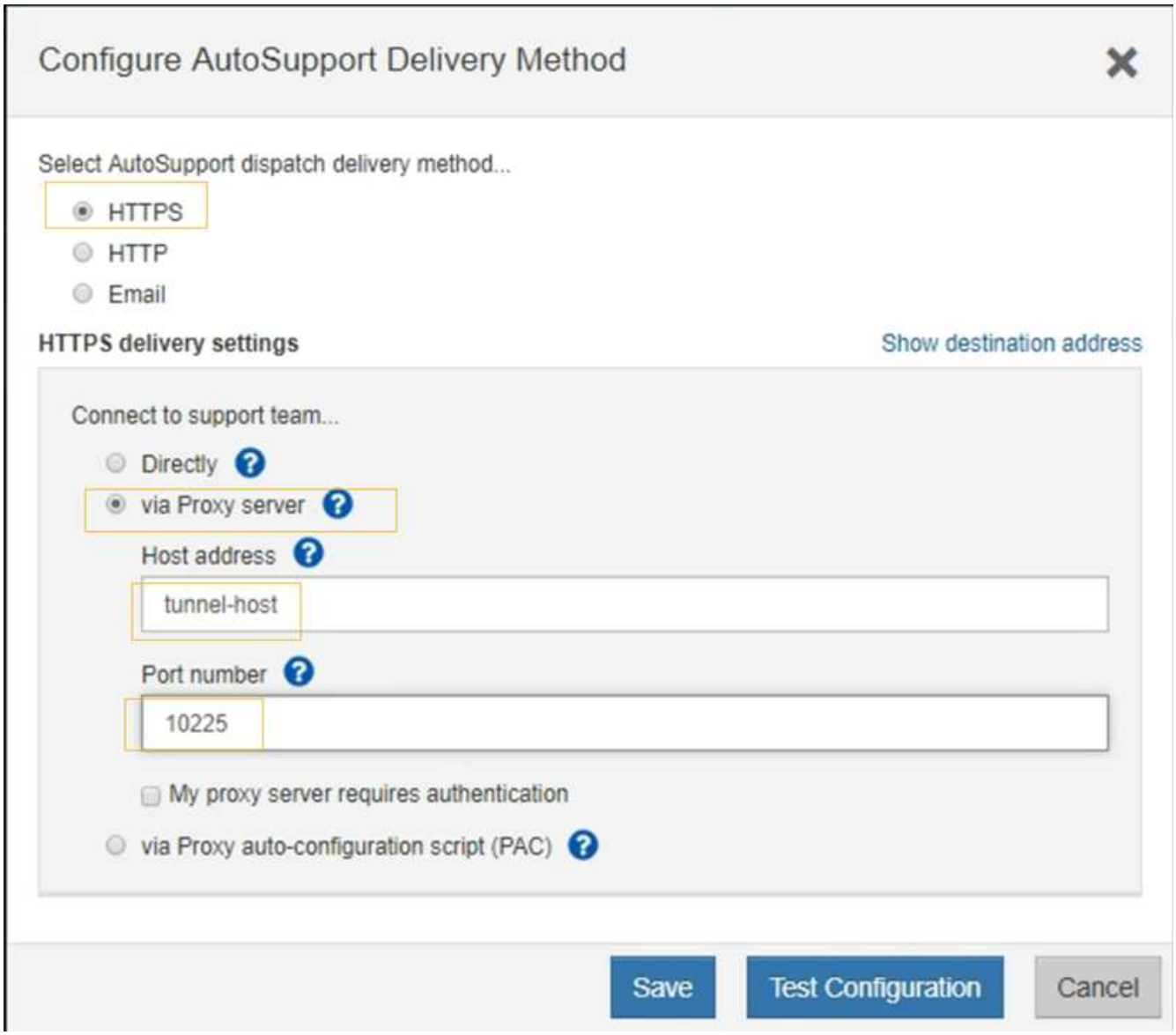
4. 選擇 支援 > 支援中心 > **AutoSupport**。

   出現AutoSupport操作頁面。



5. 選擇*配置AutoSupport交付方法*。

   出現「設定AutoSupport交付方法」頁面。



6. 選擇 **HTTPS** 作為傳送方式。

   已預先安裝啟用 HTTPS 的憑證。

7. 選擇*透過代理伺服器*。
8. 進入 `tunnel-host`用於*主機位址*。

   `tunnel-host`是使用管理節點發送 E 系列AutoSupport套件的特殊位址。

9. 進入 `10225`用於*連接埠號碼*。

   `10225`是從裝置中的 E 系列控制器接收AutoSupport套件的StorageGRID代理伺服器上的連接埠號碼。

10. 選擇「測試配置」來測試AutoSupport代理伺服器的路由和配置。

    如果正確，則會出現一條綠色橫幅訊息：“您的AutoSupport配置已經驗證。”

    如果測試失敗，則會在紅色橫幅中顯示錯誤訊息。檢查您的StorageGRID DNS 設定和網絡，確保"首選發送

者管理節點"可以連接到NetApp支援站點，然後再次嘗試測試。

11. 選擇*儲存*。

    配置已儲存，並出現確認訊息：“AutoSupport交付方法已配置。”

管理儲存節點

管理儲存節點

儲存節點提供磁碟儲存容量和服務。管理儲存節點需要執行以下操作：

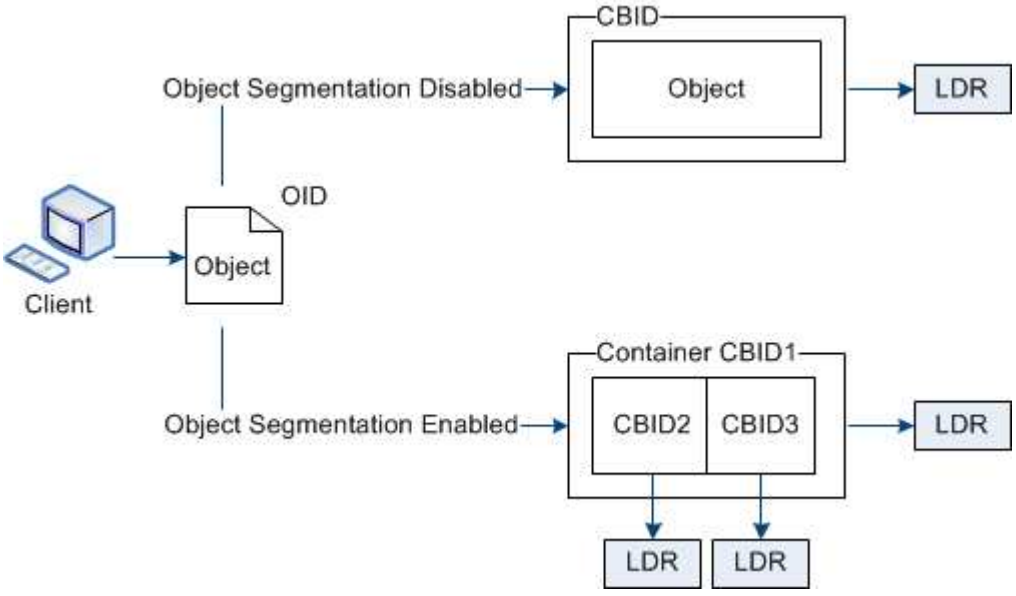
- 管理儲存選項
- 了解儲存卷水印是什麼以及如何使用浮水印覆蓋來控制儲存節點何時變為唯讀
- 監控和管理用於物件元資料的空間
- 配置儲存物件的全域設定
- 應用程式儲存節點配置設定
- 管理完整儲存節點

使用儲存選項

什麼是對象分割？

物件分割是將一個物件分割成一組較小的固定大小物件的過程，以最佳化大物件的儲存和資源使用。 S3 多部分上傳也會建立分段對象，每個部分都有一個對象代表。

當物件被攝取到StorageGRID系統時，LDR 服務會將物件拆分為多個段，並建立一個段容器，將所有段的標頭資訊列為內容。



在檢索到段容器時，LDR 服務會從其段組裝原始物件並將該物件傳回給客戶端。

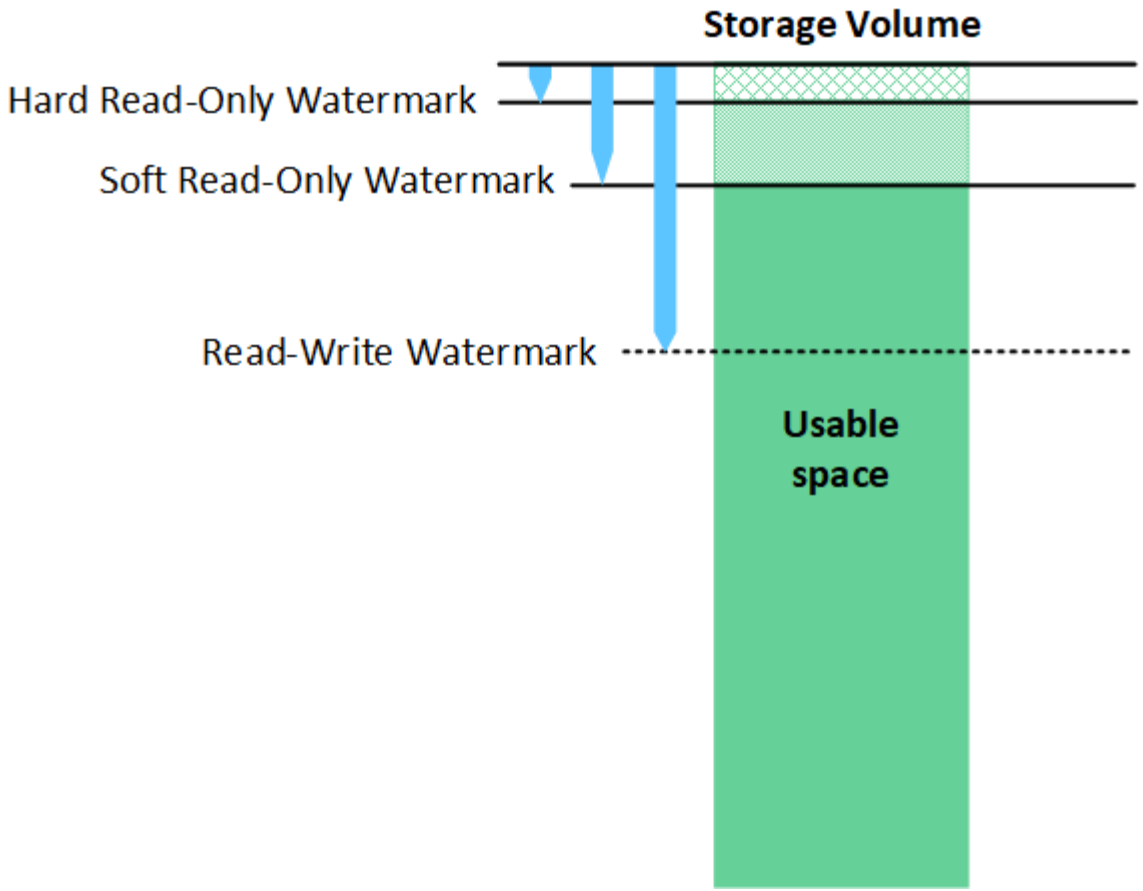
容器和段不一定儲存在同一個儲存節點上。容器和段可以儲存在 ILM 規則中指定的儲存池內的任何儲存節點上。

每個段都由StorageGRID系統獨立處理，並有助於統計管理物件和儲存物件等屬性的數量。例如，如果儲存到StorageGRID系統的物件被分成兩個區段，則在攝取完成後，「託管物件」的值將增加 3，如下所示：

```
segment container + segment 1 + segment 2 = three stored objects
```

什麼是儲存卷水印？

StorageGRID使用三個儲存卷浮水印來確保儲存節點在空間嚴重不足之前安全地轉換為唯讀狀態，並允許已轉換為唯讀狀態的儲存節點再次變為讀寫狀態。



儲存卷浮水印僅適用於用於複製和擦除編碼物件資料的空間。若要了解磁碟區 0 上為物件元資料保留的空間，請前往"管理對像元資料存儲"。

什麼是軟唯讀浮水印？

*儲存卷軟唯讀浮水印*是第一個指示儲存節點的物件資料可用空間已滿的浮水印。

如果儲存節點中每個磁碟區的可用空間小於該磁碟區的軟唯讀浮水印，則儲存節點將轉換為_唯讀模式_。唯讀模式意味著儲存節點向StorageGRID系統的其餘部分公佈唯讀服務，但滿足所有待處理的寫入請求。

例如，假設儲存節點中的每個磁碟區都有 10 GB 的軟唯讀浮水印。一旦每個磁碟區的可用空間少於 10 GB，儲存節點就會轉換為軟唯讀模式。

什麼是硬唯讀浮水印？

*儲存卷硬唯讀浮水印*是下一個浮水印，表示節點可用於儲存物件資料的空間已滿。

如果磁碟區上的可用空間小於該磁碟區的硬唯讀浮水印，則對該磁碟區的寫入將會失敗。但是，對其他磁碟區的寫入可以繼續，直到這些磁碟區上的可用空間小於其硬唯讀浮水印。

例如，假設儲存節點中的每個磁碟區都有 5 GB 的硬唯讀浮水印。一旦每個磁碟區的可用空間少於 5 GB，儲存節點就不再接受任何寫入請求。

硬唯讀浮水印總是小於軟唯讀浮水印。

什麼是讀寫浮水印？

*儲存卷讀寫浮水印*僅適用於已轉換為唯讀模式的儲存節點。它決定節點何時可以再次變成讀寫。當儲存節點中任何一個儲存卷的可用空間大於該磁碟區的讀寫浮水印時，該節點會自動轉換回讀寫狀態。

例如，假設儲存節點已轉換為唯讀模式。也假設每個磁碟區都有 30 GB 的讀寫浮水印。一旦任何磁碟區的可用空間增加到 30 GB，該節點就會再次變為讀寫狀態。

讀寫浮水印總是大於軟唯讀浮水印和硬唯讀浮水印。

查看儲存卷浮水印

您可以查看目前浮水印設定和系統最佳化值。如果沒有使用最佳化浮水印，您可以確定是否可以或應該調整設定。

開始之前

- 您已完成升級至StorageGRID 11.6 或更高版本。
- 您已使用"支援的網頁瀏覽器"。
- 你有"Root存取權限"。

查看目前浮水印設定

您可以在網格管理器中查看目前儲存浮水印設定。

步驟

1. 選擇 支援 > 其他 > 儲存浮水印。
2. 在儲存浮水印頁面上，查看使用最佳化值複選框。
   - 如果選取該複選框，則根據儲存節點的大小和磁碟區的相對容量，針對每個儲存節點上的每個儲存磁碟區最佳化所有三個浮水印。

     這是預設和推薦的設定。不要更新這些值。或者，您可以查看優化的儲存浮水印。
   - 如果未選取「使用最佳化值」複選框，則將使用自訂（非最佳化）浮水印。不建議使用自訂水印設定。使用說明"故障排除低唯讀浮水印覆蓋警報"確定您是否可以或應該調整設定。

     指定自訂浮水印設定時，必須輸入大於 0 的值。

查看優化的儲存浮水印

StorageGRID使用兩個 Prometheus 指標來顯示它為儲存磁碟區軟唯讀浮水印計算的最佳化值。您可以查看網格中每個儲存節點的最小和最大最佳化值。

1. 選擇*支援* > 工具 > 指標。
2. 在 Prometheus 部分，選擇連結以存取 Prometheus 使用者介面。
3. 若要查看建議的最小軟唯讀浮水印，請輸入以下 Prometheus 指標，然後選擇 執行：

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

   最後一列顯示每個儲存節點上所有儲存磁碟區的軟唯讀浮水印的最小最佳化值。如果該值大於儲存磁碟區軟體只讀浮水印的自訂設置，則會觸發儲存節點的*低唯讀浮水印覆蓋*警報。

4. 若要查看建議的最大軟唯讀浮水印，請輸入以下 Prometheus 指標，然後選擇 執行：

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   最後一列顯示每個儲存節點上所有儲存磁碟區的軟唯讀浮水印的最大最佳化值。

管理對像元資料存儲

StorageGRID系統的物件元資料容量控制該系統上可儲存的最大物件數量。為了確保您的StorageGRID系統有足夠的空間來儲存新對象，您必須了解StorageGRID儲存對像元資料的位置和方式。

什麼是對像元資料？

對像元資料是描述對象的任何資訊。 StorageGRID使用物件元資料來追蹤網格中所有物件的位置並管理每個物件的生命週期。

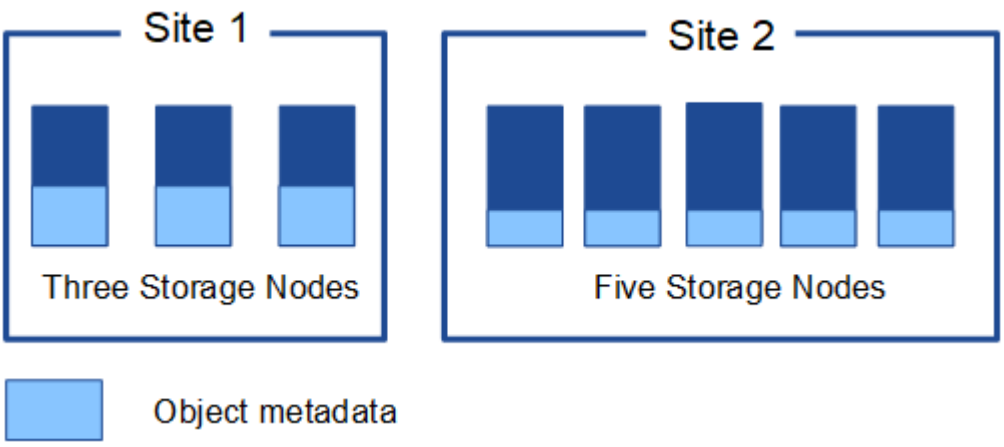
對於StorageGRID中的對象，對像元資料包括以下類型的信息：

- 系統元數據，包括每個物件的唯一 ID（UUID）、物件名稱、S3 儲存桶的名稱、租用戶帳戶名稱或 ID、物件的邏輯大小、物件首次建立的日期和時間以及物件最後修改的日期和時間。
- 與物件關聯的任何自訂用戶元資料鍵值對。
- 對於 S3 對象，與該對象關聯的任何對象標籤鍵值對。
- 對於複製的物件副本，每個副本的目前儲存位置。
- 對於擦除編碼物件副本，每個片段的目前儲存位置。
- 對於雲端儲存池中的物件副本，物件的位置，包括外部儲存桶的名稱和物件的唯一識別碼。
- 對於分段對象和多部分對象，分段標識符和資料大小。

對像元資料如何儲存？

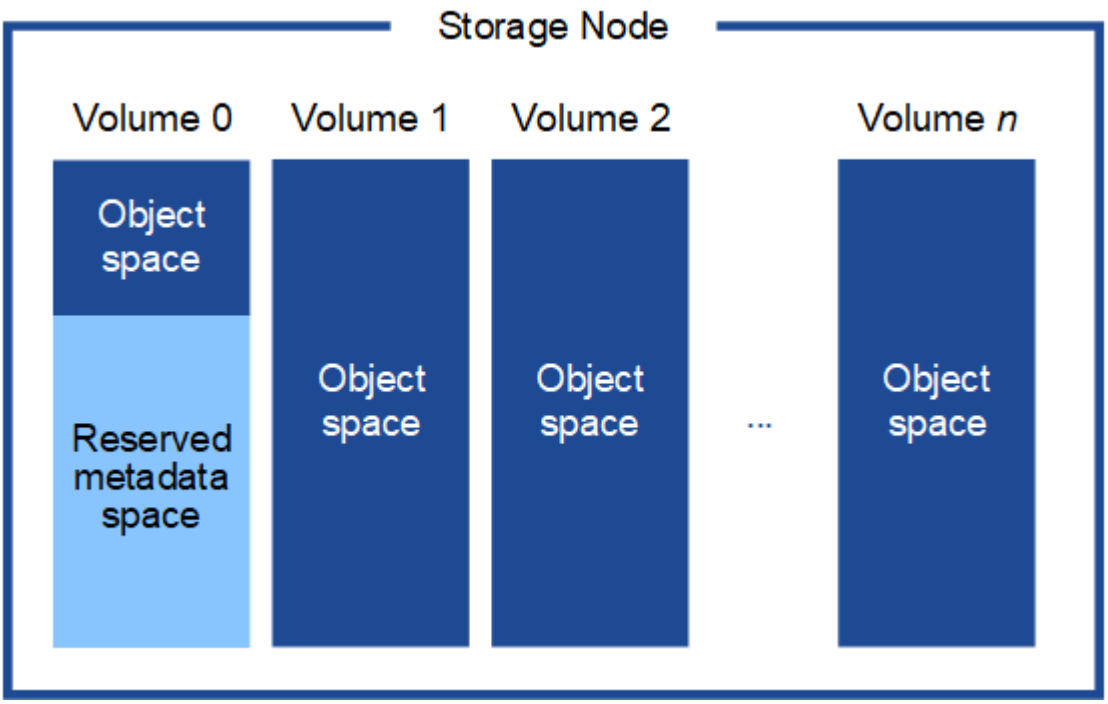
StorageGRID在 Cassandra 資料庫中維護物件元數據，該資料庫獨立於物件資料進行儲存。為了提供冗餘並保護物件元資料免於遺失， StorageGRID在每個站點儲存系統中所有物件的元資料的三個副本。

此圖代表兩個站點的儲存節點。每個站點都有相同數量的物件元數據，並且每個站點的元數據在該站點的所有儲存節點之間細分。



物件元資料儲存在哪裡？

此圖表示單一儲存節點的儲存量。



如圖所示， StorageGRID在每個儲存節點的儲存磁碟區 0 上為物件元資料保留空間。它使用保留空間來儲存物件元資料並執行必要的資料庫操作。儲存磁碟區 0 和儲存節點中所有其他儲存磁碟區上的任何剩餘空間專門用於物件資料（複製的副本和擦除編碼片段）。

特定儲存節點上為物件元資料保留的空間量取決於幾個因素，如下所述。

元資料保留空間設置

_元資料保留空間_是系統範圍的設置，表示每個儲存節點的磁碟區 0 上為元資料保留的空間量。如表所示，此設定的預設值是基於：

- 您最初安裝StorageGRID時所使用的軟體版本。
- 每個儲存節點上的 RAM 數量。

用於初始**StorageGRID**安裝的版本	儲存節點上的 **RAM** 數量	預設元資料保留空間設置
11.5 至 11.9	網格中每個儲存節點上 128 GB 或更多	8 TB（8,000 GB）
	網格中任何儲存節點上的容量小於 128 GB	3 TB（3,000 GB）
11.1 至 11.4	任何一個站點的每個儲存節點上都有 128 GB 或更多	4 TB（4,000 GB）
	每個站點的任何儲存節點上少於 128 GB	3 TB（3,000 GB）
11.0 或更早版本	任何金額	2 TB（2,000 GB）

查看元資料保留空間設置

請依照下列步驟查看StorageGRID系統的元資料保留空間設定。

步驟

1. 選擇*配置* > 系統 > 儲存設定。
2. 在儲存設定頁面上，展開「元資料保留空間」部分。

對於StorageGRID 11.8 或更高版本，元資料保留空間值必須至少為 100 GB 且不超過 1 PB。

對於新的StorageGRID 11.6 或更高版本安裝，其中每個儲存節點具有 128 GB 或更多 RAM，其預設為 8,000 GB（8 TB）。

元資料實際保留空間

與系統範圍的元資料保留空間設定相反，物件元資料的_實際保留空間_是針對每個儲存節點確定的。對於任何給定的儲存節點，元資料的實際保留空間取決於節點的磁碟區 0 的大小和系統範圍的元資料保留空間設定。

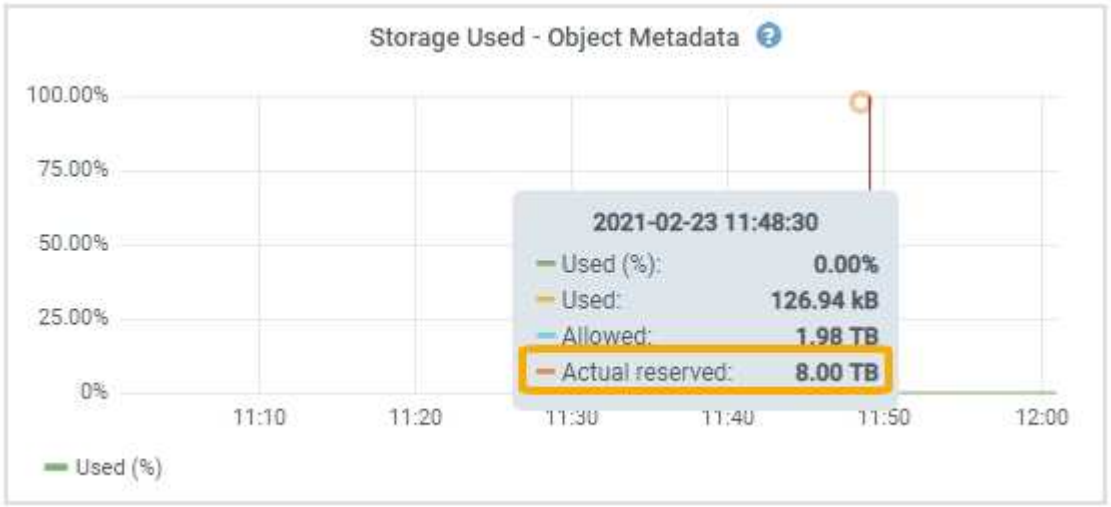
節點的磁碟區 **0** 的大小	元資料實際保留空間
少於 500 GB（非生產用途）	10% 音量 0
500 GB 或更多 + 或 + 僅元資料儲存節點	以下值中較小的一個： • 第 0 卷 • 元資料保留空間設置 注意：僅元資料儲存節點只需要一個 rangedb。

查看元資料實際預留空間

請依照下列步驟查看特定儲存節點上元資料的實際保留空間。

步驟

1. 從網格管理器中，選擇 **NODES** > ***Storage Node***。
2. 選擇“儲存”標籤。
3. 將遊標放在「已使用儲存 - 物件元資料」圖表上並找到「實際保留」值。



在螢幕截圖中，「實際保留」值為 8 TB。此螢幕截圖適用於新StorageGRID 11.6 安裝中的大型儲存節點。由於系統範圍的元資料預留空間設定小於此儲存節點的磁碟區 0，因此此節點的實際預留空間等於元資料預留空間設定。

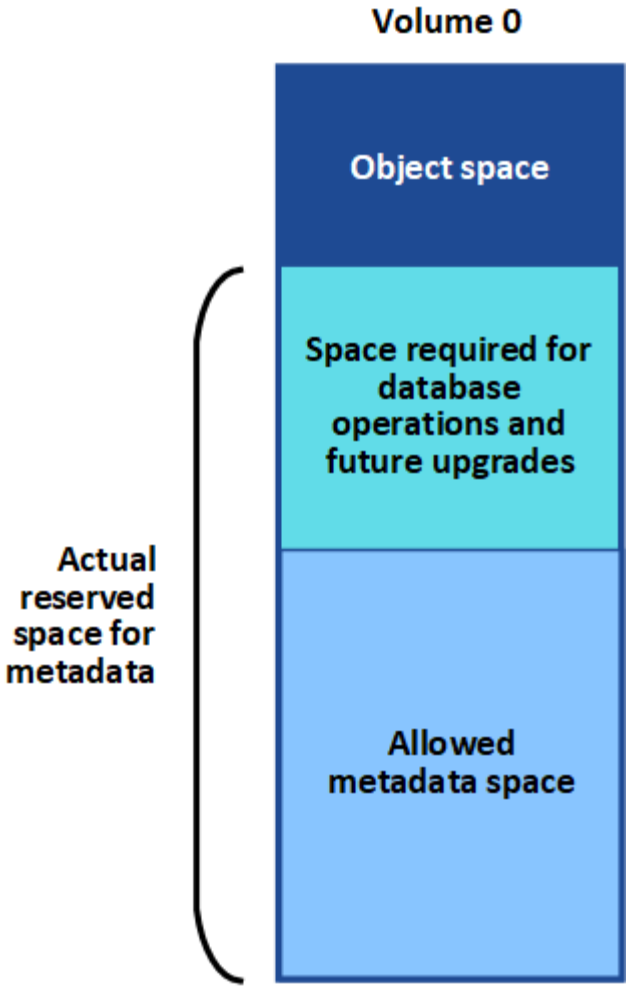
實際保留元資料空間的範例

假設您使用 11.7 或更高版本安裝新的StorageGRID系統。對於此範例，假設每個儲存節點都有超過 128 GB 的 RAM，且儲存節點 1 (SN1) 的磁碟區 0 為 6 TB。基於這些價值觀：

- 系統範圍的*元資料保留空間*設定為 8 TB。 （如果每個儲存節點都有超過 128 GB 的 RAM，則這是新StorageGRID 11.6 或更高版本安裝的預設值。）
- SN1 實際預留的元資料空間為 6 TB。 （由於磁碟區 0 小於 元資料保留空間 設置，因此整個磁碟區都被保留。）

允許的元資料空間

每個儲存節點為元資料實際保留的空間細分為可用於物件元資料的空間（允許的元資料空間）和基本資料庫操作（例如壓縮和修復）以及未來硬體和軟體升級所需的空間。允許的元資料空間決定了整體物件容量。



下表顯示了StorageGRID如何根據節點的記憶體量和元資料的實際保留空間來計算不同儲存節點的*允許的元資料空間*。

		儲存節點上的記憶體量	
	小於 128 GB	≥ 128 GB	實際為元資料保留的空間
≤ 4 TB	元資料實際預留空間的 60%，最大可達 1.32 TB	元資料實際預留空間的 60%，最大可達 1.98 TB	大於 4 TB

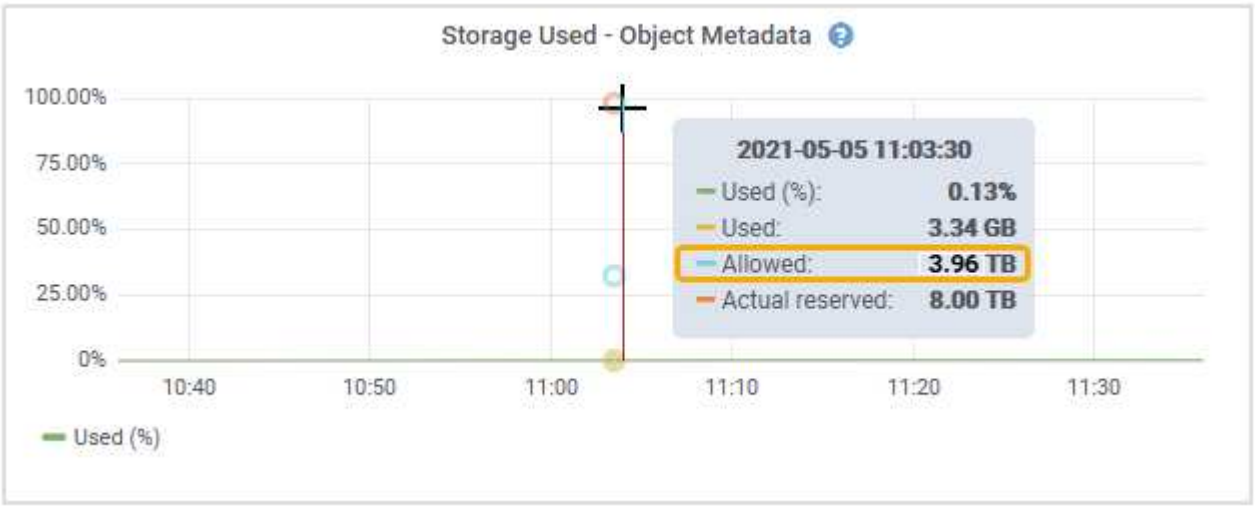
查看允許的元資料空間

請依照下列步驟查看儲存節點允許的元資料空間。

步驟

1. 從網格管理器中選擇*NODES*。
2. 選擇儲存節點。
3. 選擇“儲存”標籤。

4. 將遊標放在使用的儲存空間 - 物件元資料圖表上並找到*允許*值。



在螢幕截圖中，*允許*值為 3.96 TB，這是實際為元資料保留的空間超過 4 TB 的儲存節點的最大值。

Allowed 值對應於此 Prometheus 指標：

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

允許的元資料空間範例

假設您使用版本 11.6 安裝StorageGRID系統。對於此範例，假設每個儲存節點都有超過 128 GB 的 RAM，且儲存節點 1 (SN1) 的磁碟區 0 為 6 TB。基於這些價值觀：

- 系統範圍的*元資料保留空間*設定為 8 TB。 （當每個儲存節點具有超過 128 GB 的 RAM 時，這是StorageGRID 11.6 或更高版本的預設值。）
- SN1 實際預留的元資料空間為 6 TB。 （由於磁碟區 0 小於 元資料保留空間 設置，因此整個磁碟區都被保留。）
- 根據允許元資料空間的表：（實際預留元資料空間-1TB）×60%，最大為3.96TB。

不同大小的儲存節點如何影響物件容量

如上所述， StorageGRID在每個站點的儲存節點上均勻分佈物件元資料。因此，如果網站包含不同大小的儲存節點，則站點上最小的節點決定了站點的元資料容量。

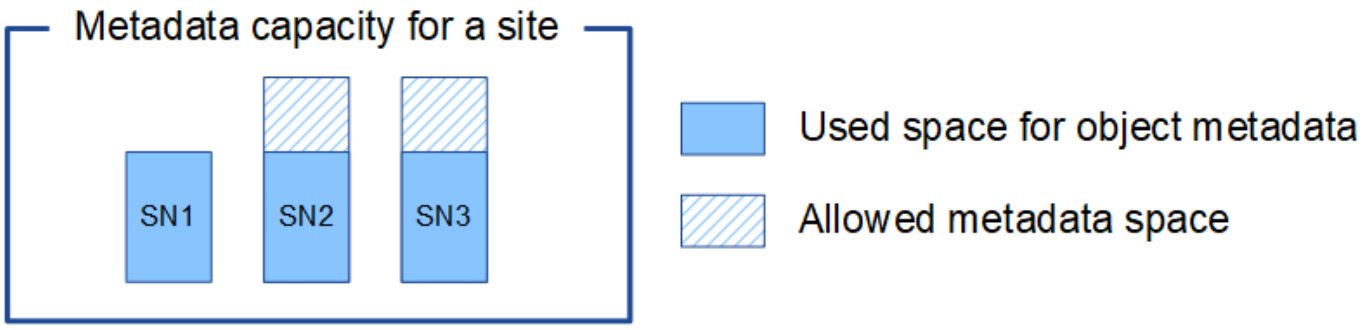
請考慮以下範例：

- 您有一個包含三個不同大小的儲存節點的單站點網格。
- *元資料保留空間*設定為 4 TB。
- 儲存節點實際保留的元資料空間和允許的元資料空間有以下值。

儲存節點	卷 **0** 的大小	實際預留元資料空間	允許的元資料空間
SN1	2.2TB	2.2TB	1.32TB

儲存節點	卷 **0** 的大小	實際預留元資料空間	允許的元資料空間
SN2	5TB	4TB	1.98TB
SN3	6TB	4TB	1.98TB

由於物件元資料均勻分佈在站點的各個儲存節點上，因此本例中的每個節點只能容納 1.32 TB 的元資料。 SN2 和 SN3 允許的額外 0.66 TB 元資料空間無法使用。



同樣，由於StorageGRID在每個站點維護StorageGRID系統的所有物件元數據，因此StorageGRID系統的整體元資料容量由最小站點的物件元資料容量決定。

由於物件元資料容量控制最大物件數，因此當一個節點的元資料容量耗盡時，網格實際上已滿。

相關資訊

- 若要了解如何監控每個儲存節點的物件元資料容量，請參閱"監控StorageGRID"。
- 為了增加系統的物件元資料容量，"展開網格"透過新增新的儲存節點。

增加元資料保留空間設置

如果您的儲存節點符合 RAM 和可用空間的特定要求，您可能能夠增加元資料保留空間系統設定。

你需要什麼

- 您已使用"支援的網頁瀏覽器"。
- 你有"Root 存取權限或網格拓撲頁面配置和其他網格配置權限"。

網格拓撲頁面已被棄用，並將在未來版本中刪除。

關於此任務

您可能能夠手動將系統範圍的元資料保留空間設定增加到 8 TB。

只有當以下兩個語句都成立時，您才可以增加系統範圍的元資料保留空間設定的值：

- 系統中任何站點的儲存節點均具有 128 GB 或更多 RAM。
- 系統中任何站點的儲存節點在儲存磁碟區 0 上都有足夠的可用空間。

請注意，如果增加此設置，則會同時減少所有儲存節點的儲存磁碟區 0 上可用於物件儲存的空間。因此，您可能想要根據預期的物件元資料要求將元資料保留空間設定為小於 8 TB 的值。

> 一般來說，最好使用較高的值而不是較低的值。如果元資料保留空間設定太大，您可以稍後減少它。相反，如果您稍後增加該值，系統可能需要移動物件資料以釋放空間。

有關元資料保留空間設定如何影響特定儲存節點上物件元資料儲存的允許空間的詳細說明，請參閱"管理對像元資料存儲"。

步驟

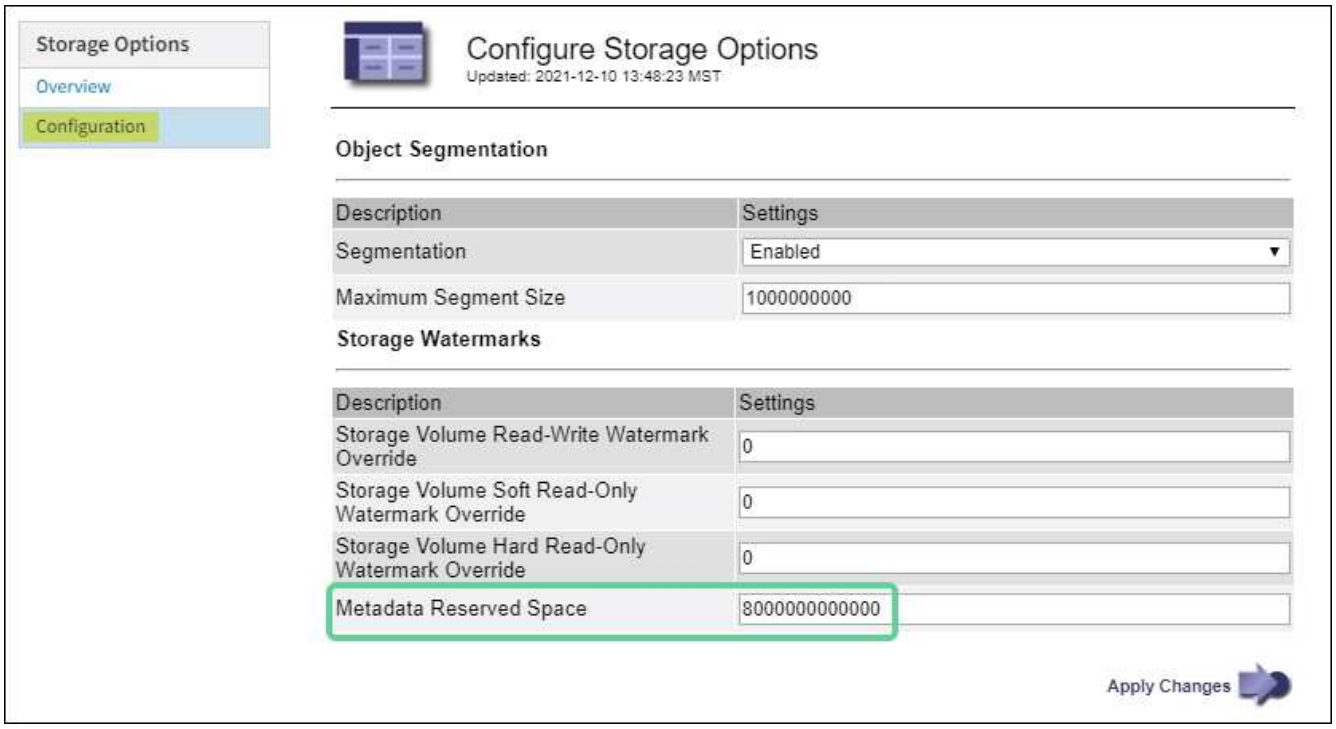
1. 確定目前元資料保留空間設定。
   a. 選擇*配置* > 系統 > 儲存選項。
   b. 在儲存浮水印部分，記下「元資料保留空間」的值。
2. 確保每個儲存節點的儲存磁碟區 0 上有足夠的可用空間來增加此值。
   a. 選擇*NODES*。
   b. 選擇網格中的第一個儲存節點。
   c. 選擇“儲存”標籤。
   d. 在 Volumes 部分中，找到 **/var/local/rangedb/0** 條目。
   e. 確認可用值等於或大於您要使用的新值與目前元資料保留空間值之間的差異。

      例如，如果元資料保留空間設定目前為 4 TB，而您想要將其增加到 6 TB，則可用值必須為 2 TB 或更大。

   f. 對所有儲存節點重複這些步驟。
      - 如果一個或多個儲存節點沒有足夠的可用空間，則無法增加元資料預留空間值。不要繼續此過程。
      - 如果每個儲存節點在磁碟區 0 上都有足夠的可用空間，請前往下一個步驟。
3. 確保每個儲存節點上至少有 128 GB 的 RAM。
   a. 選擇*NODES*。
   b. 選擇網格中的第一個儲存節點。
   c. 選擇“硬體”標籤。
   d. 將遊標懸停在記憶體使用圖上。確保*總記憶體*至少為 128 GB。
   e. 對所有儲存節點重複這些步驟。
      - 如果一個或多個儲存節點沒有足夠的可用總內存，則無法增加元資料保留空間值。不要繼續此過程。
      - 如果每個儲存節點至少有 128 GB 的總內存，請轉到下一步。
4. 更新元資料保留空間設定。
   a. 選擇*配置* > 系統 > 儲存選項。
   b. 選擇“配置”標籤。
   c. 在儲存浮水印部分，選擇*元資料保留空間*。

d. 輸入新值。

例如，要輸入 8 TB（即支援的最大值），請輸入 **8000000000000**（8，後面跟著 12 個零）



a. 選擇*應用變更*。

壓縮儲存的對象

您可以啟用物件壓縮來減少儲存在StorageGRID中的物件的大小，從而減少物件消耗的儲存空間。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"特定存取權限"。

關於此任務

預設情況下，物件壓縮是禁用的。如果啟用壓縮， StorageGRID會在儲存每個物件時嘗試使用無損壓縮來壓縮每個物件。

如果您更改此設置，則大約需要一分鐘才能應用新設置。配置的值被緩存，以提高效能和擴展性。

在啟用物件壓縮之前，請注意以下事項：

- 除非您知道儲存的資料是可壓縮的，否則不應選擇*壓縮儲存的物件*。
- 將物件儲存到StorageGRID 的應用程式可能會在儲存物件之前對其進行壓縮。如果用戶端應用程式在將物件儲存到StorageGRID之前已經壓縮了該對象，則選擇此選項將不會進一步減少對象的大小。
- 如果您將NetApp FabricPool與StorageGRID一起使用，請不要選擇「壓縮儲存物件」。

- 如果選擇了*壓縮儲存的物件*，S3 用戶端應用程式應避免執行指定傳回位元組範圍的 GetObject 操作。這些「範圍讀取」操作效率低下，因為StorageGRID必須有效地解壓縮物件才能存取請求的位元組。從非常大的物件中請求一小段位元組的 GetObject 操作效率特別低；例如，從 50 GB 的壓縮物件中讀取 10 MB 範圍的位元組效率很低。

  如果從壓縮物件讀取範圍，客戶端請求可能會逾時。

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

步驟

1. 選擇 配置 > 系統 > 儲存設定 > 物件壓縮。
2. 選取“壓縮儲存的物件”複選框。
3. 選擇*儲存*。

管理完整的儲存節點

當儲存節點達到容量時，您必須透過新增儲存空間來擴充StorageGRID系統。有三個可用選項：新增儲存磁碟區、新增儲存擴充架和新增儲存節點。

新增儲存卷

每個儲存節點支援最大數量的儲存卷。定義的最大值因平台而異。如果儲存節點包含的儲存磁碟區數量少於最大數量，則可以新增磁碟區來增加其容量。請參閱說明"擴充StorageGRID系統"。

新增儲存擴充架

一些StorageGRID設備儲存節點（例如 SG6060 或 SG6160）可以支援額外的儲存架。如果您擁有具有擴充功能的StorageGRID設備，但尚未擴展到最大容量，則可以新增儲存架來增加容量。請參閱說明"擴充StorageGRID系統"。

新增儲存節點

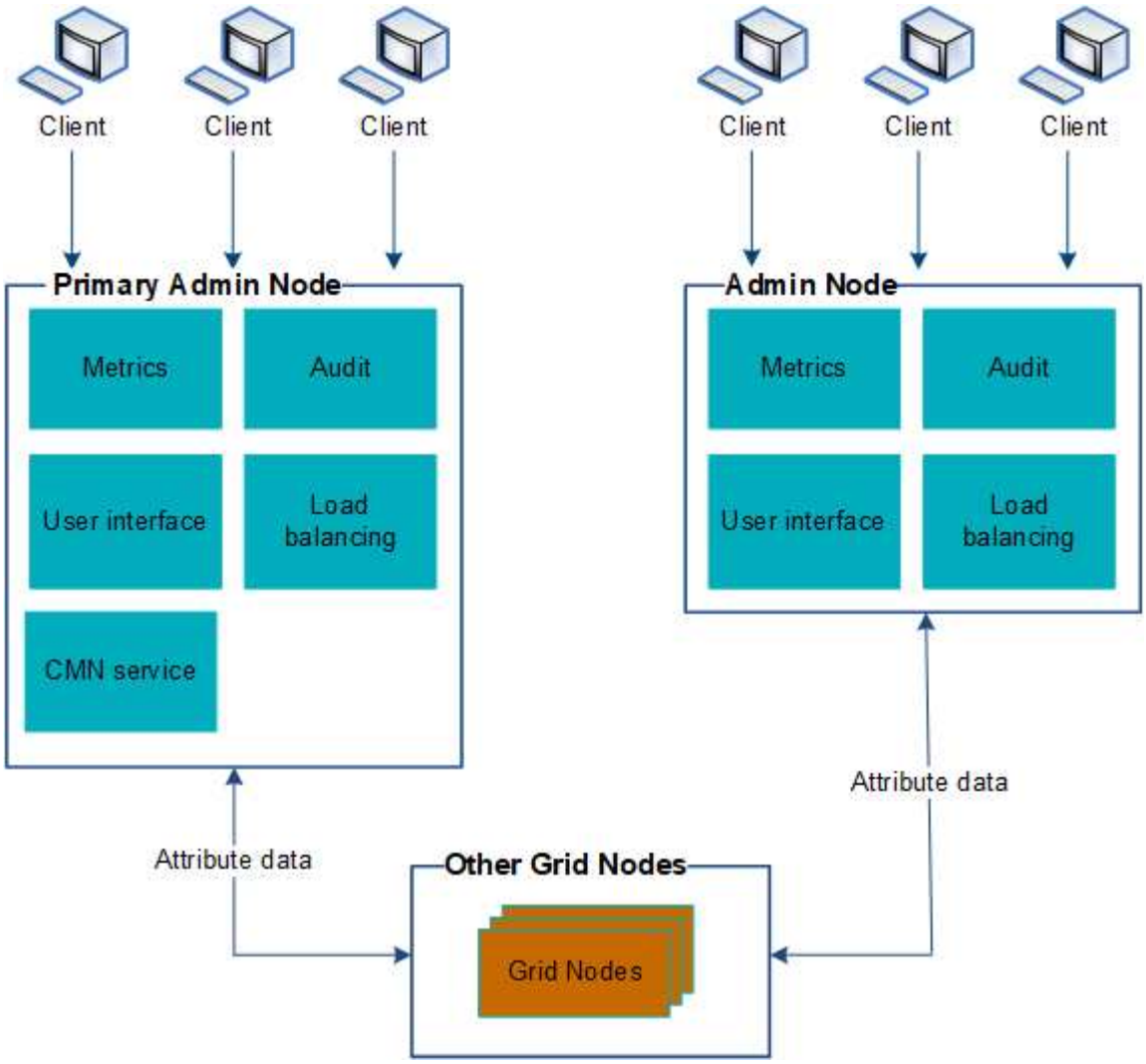
您可以透過新增儲存節點來增加儲存容量。新增儲存時必須仔細考慮目前有效的 ILM 規則和容量要求。請參閱說明"擴充StorageGRID系統"。

管理管理節點

使用多個管理節點

StorageGRID系統可以包含多個管理節點，以便即使一個管理節點發生故障，您也能夠持續監控和設定StorageGRID系統。

如果管理節點不可用，屬性處理仍會持續，警報仍會觸發，且電子郵件通知和AutoSupport套件仍會傳送。但是，除了通知和AutoSupport套件之外，擁有多個管理節點並不提供故障轉移保護。



如果管理節點發生故障，則有兩個選項可以繼續檢視和設定StorageGRID系統：

- Web 用戶端可以重新連線到任何其他可用的管理節點。
- 如果系統管理員配置了管理節點的高可用性群組，則 Web 用戶端可以繼續使用 HA 群組的虛擬 IP 位址存取網格管理員或租用戶管理員。看"管理高可用性組" 。

> 使用 HA 群組時，如果活動管理節點發生故障，存取就會中斷。當 HA 群組的虛擬 IP 位址故障轉移到群組中的另一個管理節點後，使用者必須重新登入。

某些維護任務只能使用主管理節點執行。如果主管理節點發生故障，則必須先恢復它， StorageGRID系統才能再次完全正常運作。

識別主管理節點

主管理節點比非主管理節點提供更多功能。例如，必須使用主管理節點執行某些維護程序。

有關管理節點的更多信息，請參閱"什麼是管理節點"。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"特定存取權限"。

步驟

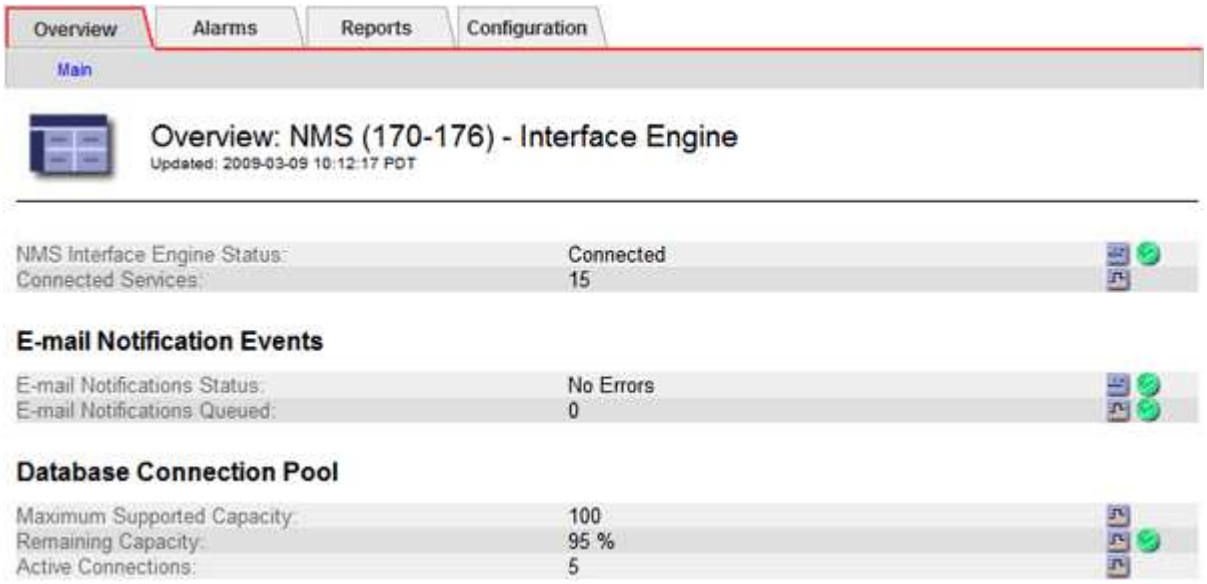
1. 選擇*NODES*。
2. 在搜尋框中輸入*primary*。

   在搜尋結果中，找到類型列中顯示「主管理節點」的節點。應列出一個主要管理節點。

查看通知狀態和佇列

管理節點上的網路管理系統 (NMS) 服務會向郵件伺服器發送通知。您可以在介面引擎頁面查看NMS服務的目前狀態及其通知佇列的大小。

若要存取介面引擎頁面，請選擇*支援* > 工具 > 網格拓撲。然後選擇 ***site*** > ***Admin Node*** > **NMS** > **Interface Engine**。



通知透過電子郵件通知佇列進行處理，並按照觸發的順序逐一發送到郵件伺服器。如果在嘗試傳送通知時出現問題（例如，網路連線錯誤）且郵件伺服器無法使用，則會盡力嘗試在 60 秒內重新傳送通知至郵件伺服器。如果 60 秒後通知仍未傳送到郵件伺服器，則該通知將從通知佇列中刪除，並嘗試傳送佇列中的下一個通知。