開始使用網格管理器

StorageGRID software

NetApp
May 29, 2026

目錄

開始使用網格管理器 . . . 1
- Web 瀏覽器需求 . . . 1
- Sign in入網格管理器 . . . 1
  - 在第一個管理節點Sign in入網格管理器 . . . 1
  - 登入另一個管理節點 . . . 6
- 退出網格管理器 . . . 7
- 更改密碼 . . . 7
- 查看StorageGRID許可證信息 . . . 8
- 更新StorageGRID許可證信息 . . . 9
- 使用 API . . . 9
  - 使用網格管理 API . . . 9
  - 網格管理 API 操作 . . . 12
  - 網格管理 API 版本控制 . . . 13
  - 防止跨站請求偽造（CSRF） . . . 15
  - 如果啟用了單一登錄，請使用 API . . . 15
  - 使用 API 停用功能 . . . 29

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**

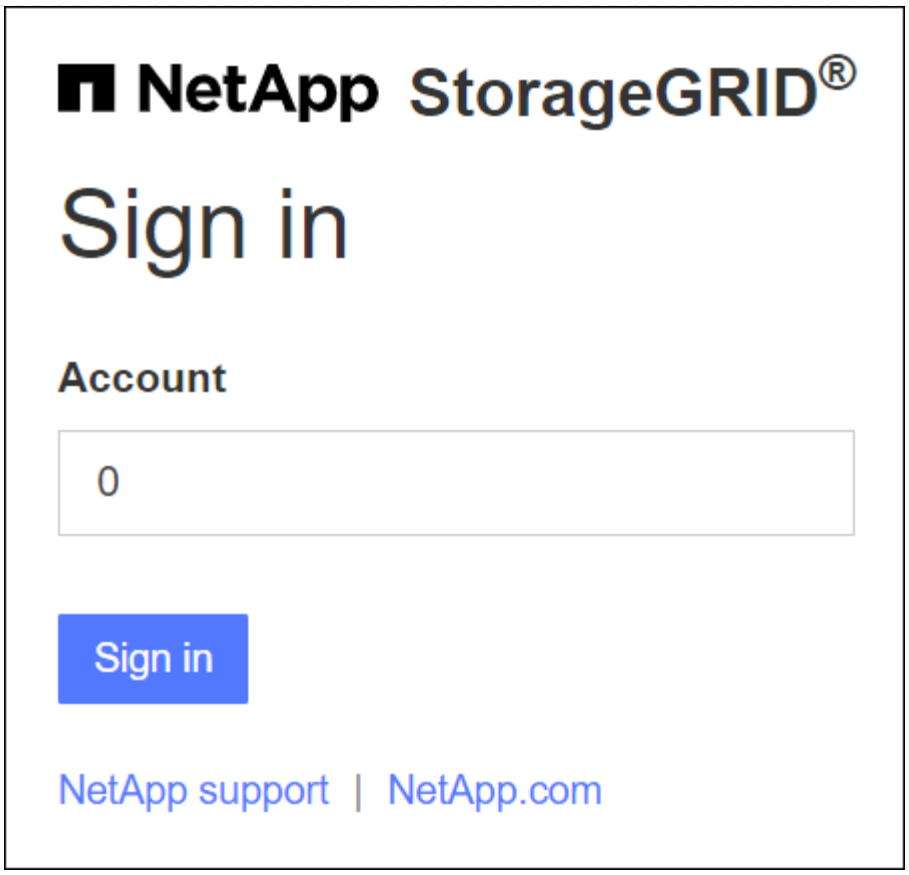
a. 輸入網格管理器的使用者名稱和密碼。

b. 選擇*登入*。

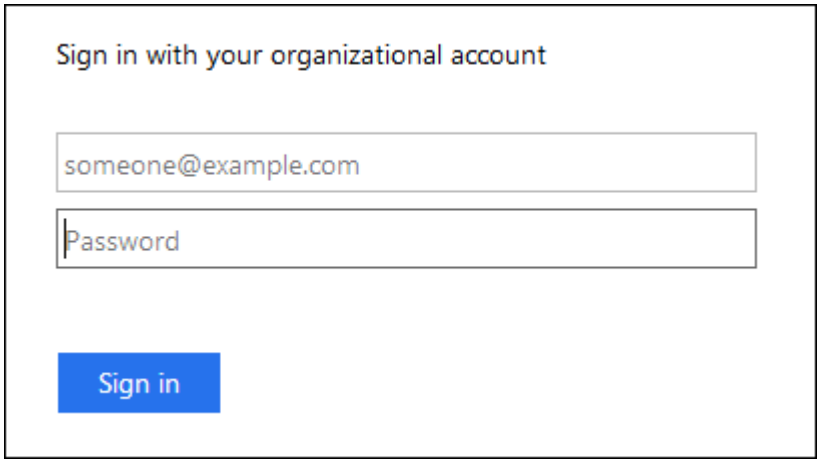
使用 **SSO**

- 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：



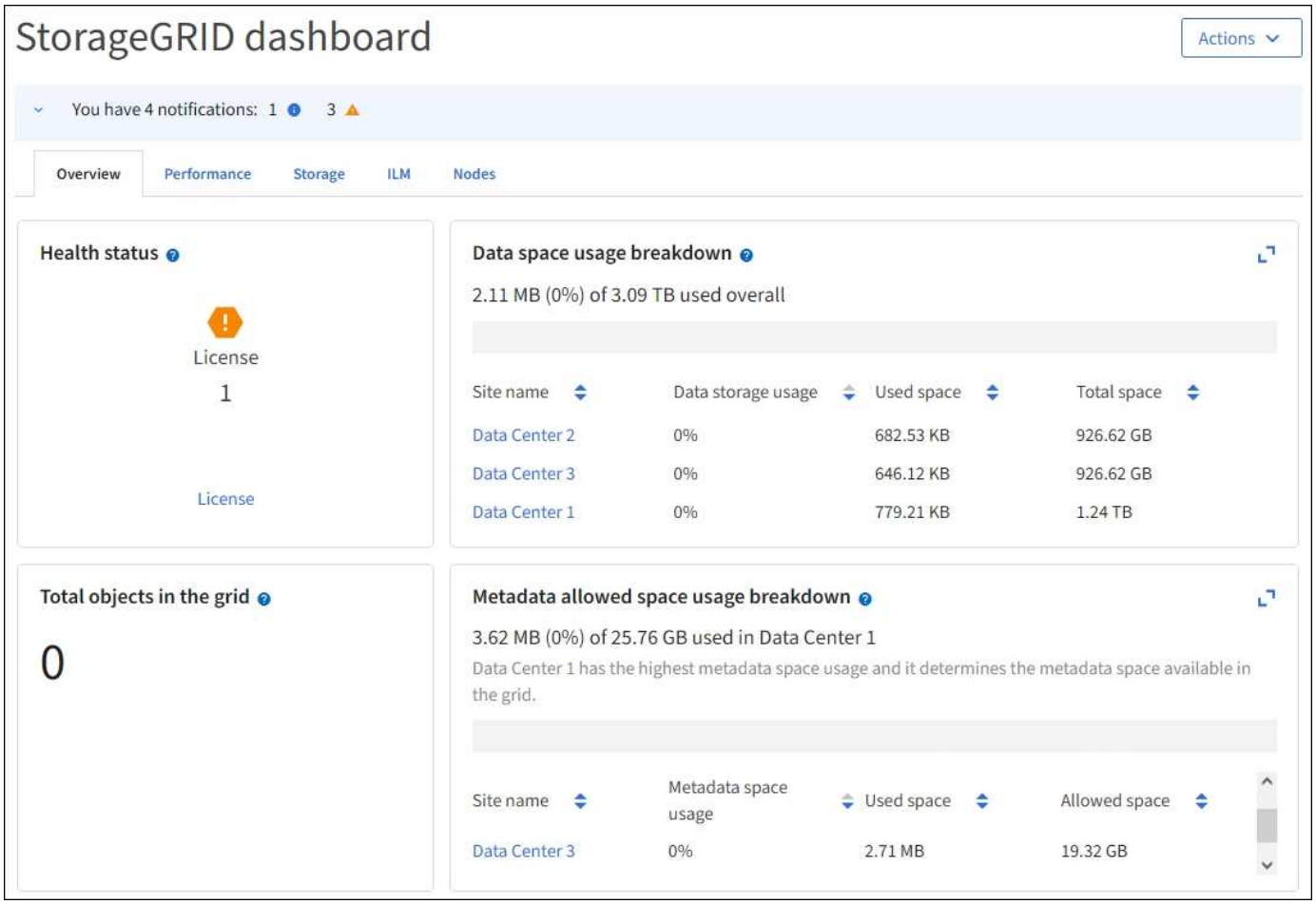
- 如果StorageGRID正在使用 SSO 且您之前曾造訪網格管理器或租用戶帳戶：

  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

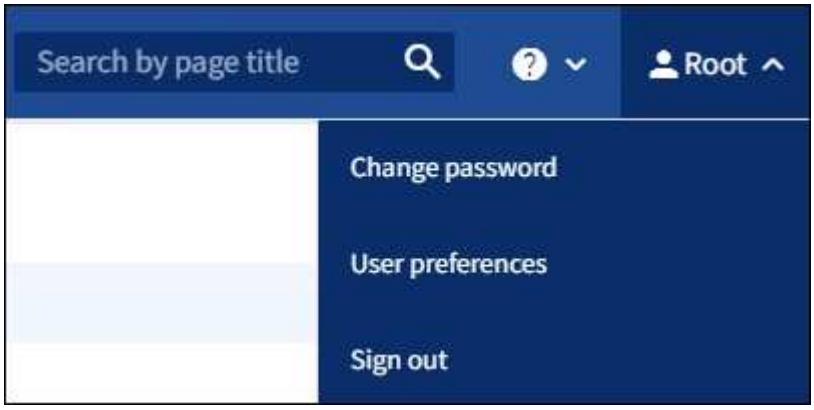
1. 在瀏覽器的網址列中輸入另一個管理節點的完全限定網域名稱或 IP 位址。
2. 如果您的 SSO 會話已過期，請再次輸入您的憑證。

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。

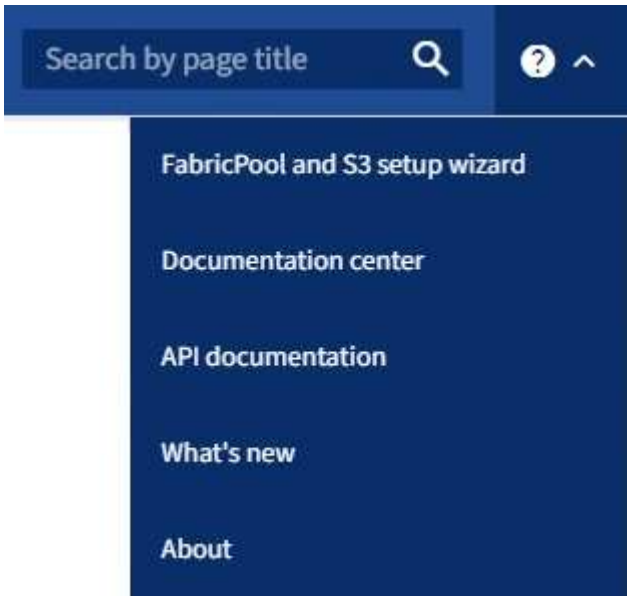
開始之前

- 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*。



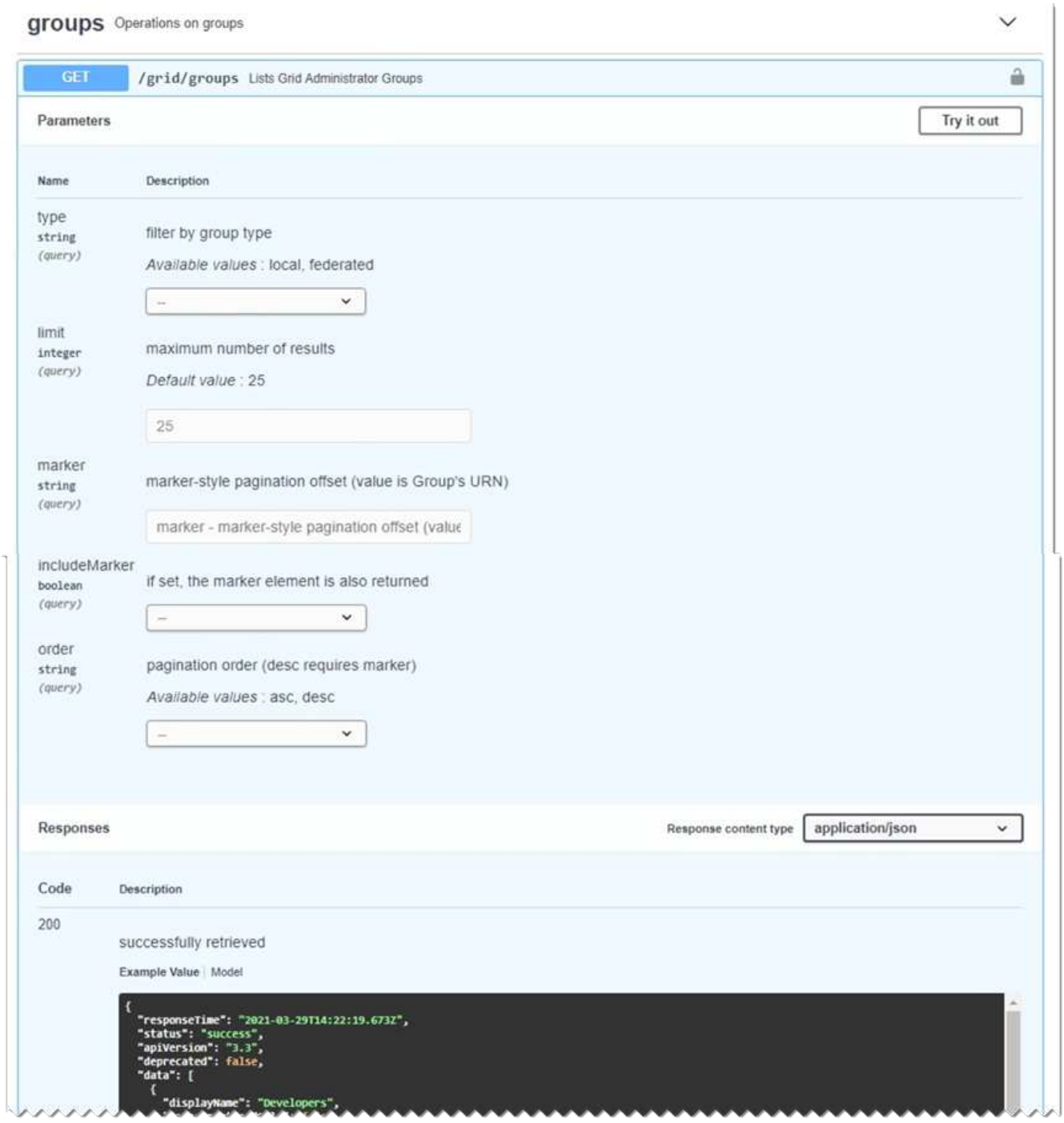
2. 若要使用私有 API 執行操作，請在StorageGRID管理 API 頁面上選擇 前往私有 **API** 文件。

   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** 操作

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
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} }`