



使用 **API**

StorageGRID software

NetApp
May 29, 2026

目錄

使用 API	1
使用網格管理 API	1
頂級資源	1
發出 API 請求	1
網格管理 API 操作	4
網格管理 API 版本控制	5
確定目前版本支援哪些 API 版本	6
為請求指定 API 版本	6
防止跨站請求偽造 (CSRF)	7
如果啟用了單一登錄，請使用 API	7
如果啟用了單一登入 (Active Directory) ，則使用 API	8
如果啟用了單一登錄，則使用 API (Azure)	14
如果啟用了單一登錄，則使用 API (PingFederate)	16
使用 API 停用功能	21
重新啟用已停用的功能	21

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

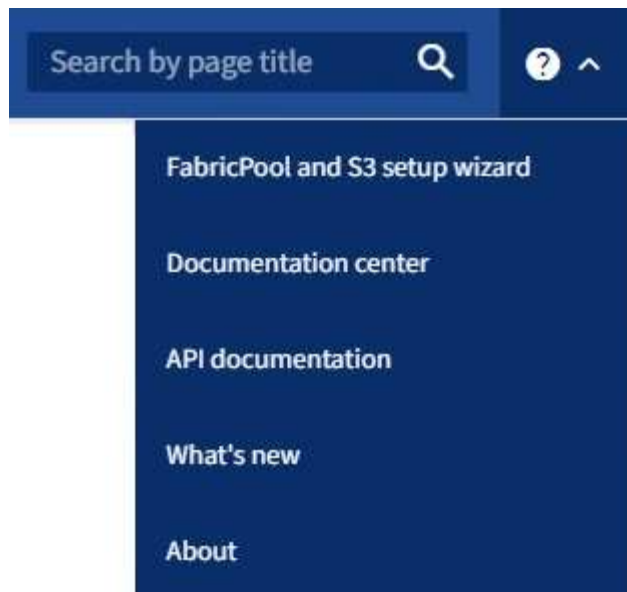
- 您已使用["支援的網頁瀏覽器"](#)。
- 你有["特定存取權限"](#)。



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。

GET /grid/groups Lists Grid Administrator Groups

Parameters Try it out

Name	Description
type string (query)	filter by group type Available values : local, federated <input type="text" value="--"/>
limit integer (query)	maximum number of results Default value : 25 <input type="text" value="25"/>
marker string (query)	marker-style pagination offset (value is Group's URN) <input type="text" value="marker - marker-style pagination offset (value"/>
includeMarker boolean (query)	if set, the marker element is also returned <input type="text" value="--"/>
order string (query)	pagination order (desc requires marker) Available values : asc, desc <input type="text" value="--"/>

Responses Response content type application/json

Code	Description
200	successfully retrieved Example Value Model <pre>{ "responseTime": "2021-03-29T14:22:19.673Z", "status": "success", "apiVersion": "3.3", "deprecated": false, "data": [{ "displayName": "Developers", </pre>

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。
- **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` 參數為 `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` 為登入租用戶管理器，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=fZHRTOMwFIZfhh...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=
$SAMPLPASSWORD&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=fZHRTomwFIZfhh...UJikvo
77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-
ee02-0080000000de
Set-Cookie: MSISAuth=AEEAADAvsHpXk6ApV...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='AEEAADAvsHpXk6ApV...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。


```
{
  "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://ads.example.com/ads/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",
  "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: MSISignoutProtocol=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 in API**

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 in API**

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=  
$SAMPLPASSWORD&pf.ok=clicked&pf.cancel=&pf.adapterId=$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

您可以使用網絡管理 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

停用功能系統可讓您阻止存取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用戶帳戶。

公司 A 可以透過使用網絡管理 API 中的停用功能系統來實現這一目標。透過在網絡管理員 (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. 存取網絡管理 API 的 Swagger 文件。看["使用網絡管理 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，您可以使用網絡管理 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. 存取網絡管理 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 } }
```

版權資訊

Copyright © 2026 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。