



使用 **API** StorageGRID software

NetApp
July 23, 2026

目錄

使用 API	1
使用 StorageGRID Grid Management API	1
\${post_edited_translations.segment}	1
發出 API 請求	1
StorageGRID 中的 Grid Management API 操作	4
StorageGRID 中的 Grid Management 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 StorageGRID 中的跨站請求偽造（CSRF）攻擊	7
如果啟用了單一登入，請使用 API。	7
如果啟用了單一登入（Active Directory），請使用 StorageGRID API	7
如果啟用了單一登入（Entra ID），請使用 StorageGRID API	14
如果啟用單一登入，請使用 StorageGRID API（PingFederate）	16
使用 API 停用 StorageGRID 功能	21
\${post_edited_translations.segment}	21

使用 API

使用 StorageGRID Grid Management API

您可以使用 Grid Management REST API 而非 Grid Manager 使用者介面來執行系統管理工作。例如，您可能想要使用 API 來自動化作業，或更快速地建立多個實體（例如使用者）。

`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

- `/grid`: 存取僅限於 Grid Manager 使用者，並根據設定的群組權限而定。
- `/org`: 存取權限僅限於屬於租戶帳戶的本機或聯合 LDAP 群組的使用者。如需詳細資訊，請參閱 ["使用租戶帳戶"](#)。
- `/private`: 存取權限僅限於 Grid Manager 使用者，並以設定的群組權限為基礎。私有 API 可能隨時變更，恕不另行通知。StorageGRID 私有端點也會忽略請求中的 API 版本。

發出 API 請求

Grid Management API 使用 Swagger 開放原始碼 API 平台。Swagger 提供直覺式使用者介面，讓開發人員和非開發人員都能使用該 API 在 StorageGRID 中執行即時操作。

`${post_edited_translations.segment}`

開始之前

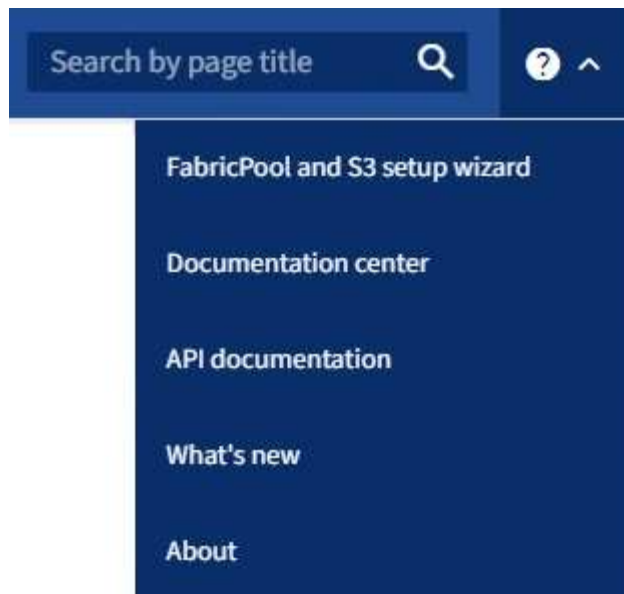
- 您已使用 ["支援的網頁瀏覽器"](#) 登入 Grid Manager。
- 您有 ["特定存取權限"](#)。



您透過 API 文件網頁執行的任何 API 操作都是即時操作。請務必小心，避免誤建立、更新或刪除組態資料或其他資料。

步驟

1. `${post_edited_translations.segment}`



neoplasms_and_cancer_types_1000_1000.jpg

(1000×1000)

Neoplasms and cancer types are broad categories of abnormal cell growth. Neoplasms, commonly known as tumors, can be benign (non-cancerous) or malignant (cancerous). Cancer, on the other hand, refers specifically to malignant neoplasms that have the potential to invade or spread to other parts of the body.

There are over 100 different types of cancer, which are typically classified by the type of cell or organ in which they originate. Some of the most common types of cancer include:

1. **Carcinoma:** This is the most common type of cancer, originating in the epithelial cells that line the inside and outside of organs. Examples include breast, lung, prostate, and colon cancers.
2. **Sarcoma:** This type of cancer originates in supportive and connective tissues, such as bones, tendons, cartilage, muscle, and fat.
3. **Leukemia:** This is a cancer of the blood-forming tissues, including the bone marrow and lymphatic system. It leads to the overproduction of abnormal white blood cells.
4. **Lymphoma:** This cancer originates in the lymphatic system, which is part of the body's immune system. It affects lymphocytes, a type of white blood cell.
5. **Myeloma:** This cancer starts in the plasma cells of the bone marrow, which are responsible for producing antibodies.
6. **Central Nervous System Cancers:** These cancers originate in the brain and spinal cord.

Understanding the different types of neoplasms and cancers is crucial for accurate diagnosis, treatment planning, and prognosis. Treatment options vary widely depending on the type and stage of the cancer, and may include surgery, chemotherapy, radiation therapy, immunotherapy, and targeted therapy.

1. `${post_edited_translations.segment}`

私有 API 如有變更，恕不另行通知。StorageGRID 私有端點也會忽略要求的 API 版本。

2. `${post_edited_translations.segment}`

`${post_edited_translations.segment}`

3. `${post_edited_translations.segment}`

GET
/grid/groups
Lists Grid Administrator Groups

Parameters
Try it out

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

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>

- 確定請求是否需要其他參數，例如群組 ID 或使用者 ID。然後，取得這些值。您可能需要先發出另一個 API 請求，才能獲得所需資訊。
- 確定是否需要修改範例要求本文。如果需要，您可以選取 **Model** 來瞭解每個欄位的需求。
- `${post_edited_translations.segment}`
- `${post_edited_translations.segment}`
- 選擇 **Execute**。
- `${post_edited_translations.segment}`

StorageGRID 中的 Grid Management API 操作

網格管理 API 將可用作業組織成以下幾個部分。



此清單僅包含公用 API 中可用的操作。

- 帳戶：管理儲存設備租戶帳戶的作業，包括建立新帳戶及擷取指定帳戶的儲存設備使用情況。
- **alert-history**：對已解決警報的操作。
- **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**：對警報靜默的操作。
- `${post_edited_translations.segment}`
- `${post_edited_translations.segment}`
- **auth**：執行使用者工作階段驗證的操作。

Grid Management API 支援 Bearer Token 驗證機制。若要登入，您必須在驗證要求的 JSON 本文中提供使用者名稱與密碼（也就是 `POST /api/v3/authorize`）。如果使用者成功通過驗證，系統將會傳回安全性權杖。必須在後續 API 要求的標頭中提供此權杖（"Authorization: Bearer *token*"）。此權杖將在 16 小時後逾期。



如果 StorageGRID 系統啟用了單一登入，則必須執行不同的驗證步驟。請參閱「如果啟用了單一登入，如何對 API 進行驗證」。

`${post_edited_translations.segment}`

- **client-certificates**：設定用戶端憑證的操作，以便使用外部監控工具安全地存取 StorageGRID。
- **config**：與產品版本及網格管理 API 版本相關的作業。您可以列出產品版本以及該版本支援的網格管理 API 主要版本，也可以停用已過時的 API 版本。
- **deactivated-features**：檢視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**：針對特定儲存應用裝置型號的磁碟機操作。
- **endpoint-domain-names**：列出並變更 S3 端點網域名稱的操作。
- **erasure-coding**：對糾刪碼設定檔進行操作。
- `${post_edited_translations.segment}`
- **expansion-nodes**：擴展操作（節點層級）。
- **expansion-sites**：擴充作業（站台層級）。
- **grid-networks**：列出並變更網格網路清單的操作。
- **grid-passwords**：網格密碼管理操作。
- `${post_edited_translations.segment}`
- **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。

- `${post_edited_translations.segment}`
- `${post_edited_translations.segment}`
- `${post_edited_translations.segment}`
- `${post_edited_translations.segment}`
- **metrics**：針對 StorageGRID 計量執行的作業，包括單一時間點的即時計量查詢，以及一段時間範圍內的範圍計量查詢。Grid Management API 使用 Prometheus 系統監控工具作為後端資料來源。如需建構 Prometheus 查詢的相關資訊，請參閱 Prometheus 網站。



名稱中包含 *private* 的計量僅供內部使用。這些計量可能會在不同的 StorageGRID 版本之間變更，恕不另行通知。

- `${post_edited_translations.segment}`
- `${post_edited_translations.segment}`
- `${post_edited_translations.segment}`
- **ntp-servers**：列出或更新外部網路時間協定 (NTP) 伺服器的作業。
- `${post_edited_translations.segment}`
- `${post_edited_translations.segment}`
- **recovery-package**：下載恢復套件的操作。
- `${post_edited_translations.segment}`
- `${post_edited_translations.segment}`
- `${post_edited_translations.segment}`
- `${post_edited_translations.segment}`
- `${post_edited_translations.segment}`
- `${post_edited_translations.segment}`
- **untrusted-client-network**：對不受信任的用戶端網路組態執行操作。
- `${post_edited_translations.segment}`

StorageGRID 中的 Grid Management 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 指定了 API 的版本 4。

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

當 API 進行了與舊版本不相容的變更時，主版本號碼會提升。當 API 進行了與舊版本相容的變更時，次版本號碼會提升。相容的變更包括新增新的端點或屬性。

以下範例說明如何根據所做的變更類型來提升 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，升級到 StorageGRID 的新功能版本後，您至少可以在一個 StorageGRID 功能版本內繼續存取舊版的 API。



您可以設定支援的版本。如需詳細資訊，請參閱 ["網格管理 API"](#) 的 Swagger API 文件的 **config** 部分。將所有 API 用戶端更新至新版本後，您應停用對舊版本的支援。

過時的請求會透過以下方式標記為已棄用：

- 回應標頭為「Deprecated: true」
- JSON 回應正文包含「deprecated」：true
- nms.log 中新增了一條已棄用的警告訊息。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 請求傳回受支援的 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 (/api/v4) 或標頭 (Api-Version: 4) 指定 API 版本。如果您同時提供這兩個值，則標頭值會覆寫路徑值。


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

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

防止 StorageGRID 中的跨站請求偽造（CSRF）攻擊

您可以使用 CSRF 令牌來增強基於 Cookie 的驗證，從而協助 StorageGRID 防範跨站請求偽造（CSRF）攻擊。Grid Manager 和 Tenant Manager 會自動啟用此安全性功能；其他 API 用戶端可以在登入時選擇是否啟用此功能。

`${post_edited_translations.segment}`

StorageGRID 透過使用 CSRF 令牌來協助防範 CSRF 攻擊。啟用此功能後，特定 Cookie 的內容必須與特定標頭或特定 POST 請求體參數的內容相符。

若要啟用此功能，請在驗證期間將 `csrfToken` 參數設定為 `true`。預設值為 `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"
```

設為 `true` 時，系統會為登入 Grid Manager 的作業設定具有隨機值的 `GridCsrfToken` Cookie，並為登入 Tenant Manager 的作業設定具有隨機值的 `AccountCsrfToken` Cookie。

`${post_edited_translations.segment}`

- 此 `X-Csrf-Token` 標頭，且標頭的值設定為 CSRF token Cookie 的值。
- 對於接受表單編碼主體的端點：A `csrfToken` 表單編碼的要求主體參數。

`${post_edited_translations.segment}`



`${post_edited_translations.segment}`

如果啟用了單一登入，請使用 **API**。

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

如果您擁有"`${post_edited_translations.segment}`"並使用 Active Directory 作為 SSO 供應商，則必須發出一系列 API 請求，以取得對 Grid Management API 或 Tenant Management API 有效的驗證權杖。

如果啟用了單一登入，請登入 **API**。

如果您使用 Active Directory 作為 SSO 身分識別供應商，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。
- 如果您想存取租戶管理 API，您需要知道租戶帳戶 ID。

關於此任務

若要取得驗證令牌，您可以使用下列範例之一：

- The `storagegrid-ssoauth.py` Python 指令碼位於 StorageGRID 安裝檔案目錄中，（`./rpms` 適用於 RHEL，`./debs` 適用於 Ubuntu 或 Debian，以及 `./vsphere` 適用於 VMware）。
- curl 請求的工作流程範例。

如果您執行 curl 工作流程的速度太慢，該工作流程可能會逾時。您可能會看到錯誤：A valid SubjectConfirmation was not found on this Response。



`${post_edited_translations.segment}`

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

步驟

1. 請選擇以下其中一種方法來取得驗證權杖：
 - 使用 `storagegrid-ssoauth.py` Python 指令碼。前往步驟 2。
 - 使用 curl 請求。前往步驟 3。
2. 如果您想使用該 `storagegrid-ssoauth.py` 指令碼，請將指令碼傳遞給 Python 解譯器並執行該指令碼。

`${post_edited_translations.segment}`

- 單一登入 (SSO) 方法。輸入 ADFS 或 adfs。
- SSO 使用者名稱
- StorageGRID 安裝所在的網域
- `${post_edited_translations.segment}`
- 如果您想存取租戶管理 API，則需要租戶帳戶 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
```

StorageGRID 授權權杖已在輸出中提供。現在，您可以像未使用 SSO 時使用 API 一樣，使用此權杖發出其他請求。

3. 如果要使用 curl 請求，請依照下列步驟操作。

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 Grid Management API，請使用 0 作為 TENANTACCOUNTID。

b. 若要接收已簽署的驗證 URL，請向 /api/v3/authorize-saml 發出 POST 要求，並從回應中移除額外的 JSON 編碼。

此範例展示了針對已簽名驗證 URL 的 POST 請求 TENANTACCOUNTID。結果將傳遞給 `python -m json.tool` 以移除 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
```

此範例的回應包含一個經過 URL 編碼的簽章 URL，但不包含額外的 JSON 編碼階層。

```
{
  "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. 儲存回應中的 SAMLRequest，以便在後續命令中使用。

```
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。

一種方法是使用先前回應中的 URL 請求登入表單。

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

回應包含用戶端請求 ID：

```
<form method="post" id="loginForm" autocomplete="off"
novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13)
Login.submitLoginRequest();" action="/adfs/ls/?
SAMLRequest=fZHRT0MwFIZfhh...UJikvo77sXPw%3D%3D&RelayState=12345&clie
nt-request-id=00000000-0000-0000-ee02-0080000000de" >
```

- e. 從回應中儲存用戶端請求 ID。

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

- f. \${post_edited_translations.segment}

```
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 傳回 302 重新導向，並在標頭中包含額外資訊。



如果您的 SSO 系統啟用了多因素驗證（MFA），則表單提交中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=AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY=; path=/adfs;
HttpOnly; Secure
Date: Tue, 06 Nov 2018 16:55:05 GMT
```

g. 從回應中儲存 MSISAuth Cookie。

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

h. 使用驗證 POST 請求中的 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
```

回應標頭將包含 AD FS 工作階段資訊，以供稍後登出使用，回應本文包含隱藏表單欄位中的 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=a3dpbnRlcnMtUHJpbWYyeS1BZG1pbi0xNzgmRmFsc2Umcng4NnJDZmFKV
XFxVWx3bk1lMnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LTNmMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjoxMjoxOVpcMQ==;
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. 儲存隱藏欄位中的 SAMLResponse 值：

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

- j. 使用已儲存的 SAMLResponse，向 StorageGRID 發出 /api/saml-response 請求以產生 StorageGRID 驗證權杖。

對於 RelayState，請使用租戶帳戶 ID，或者如果您想要登入 Grid Management API，請使用 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. 將回應中的驗證權杖儲存為 MYTOKEN。

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

現在您可以使用 MYTOKEN 來處理其他請求，就像未使用 SSO 時使用 API 一樣。

如果啟用了單一登入，請登出 **API**。

如果已啟用單一登入（SSO），則必須發出一系列 API 請求才能從 Grid Management API 或 Tenant Management API 登出。如果您使用 Active Directory 作為 SSO 身分識別供應商，則這些說明適用。

關於此任務

如有需要，您可以透過組織的單一登出頁面登出，從而退出 StorageGRID API。或者，您也可以從 StorageGRID 觸發單一登出（SLO），這需要有效的 StorageGRID 持有者權杖。

步驟

1. 若要產生已簽署的登出請求，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
```

傳回一個登出 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. 儲存登出 URL。

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

3. \${post_edited_translations.segment}

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

返回 302 回應。重新導向位置不適用於僅透過 API 進行的登出。

```
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. \${post_edited_translations.segment}

刪除 StorageGRID bearer token 的運作方式與沒有 SSO 時相同。如果未提供 `Cookie "sso=true"，使用者將從 StorageGRID 登出，而不影響 SSO 狀態。

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

A 204 No Content 回應表示使用者現在已登出。

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

如果啟用了單一登入（**Entra ID**），請使用 **StorageGRID API**

如果您有 "[\\${post_edited_translations.segment}](#)" 且使用 Entra ID 作為 SSO 供應商，您可以使用兩個範例指令碼來取得適用於 Grid Management API 或 Tenant Management API 的有效驗證權杖。

如果已啟用 **Entra ID** 單一登入，請登入 **API**。

如果您使用 Entra ID 作為 SSO 身分供應商，則適用以下說明。

開始之前

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

關於此任務

若要取得驗證權杖，可以使用下列範例指令碼：

- The `storagegrid-ssoauth-azure.py` Python 指令碼
- The `storagegrid-ssoauth-azure.js` Node.js 指令碼

這兩個指令碼都位於 StorageGRID 安裝檔案目錄中（RHEL 為 `./rpms`，Ubuntu 或 Debian 為 `./debs`，VMware 則為 `./vsphere`）。

若要撰寫您自己與 Entra ID 的 API 整合，請參閱 `storagegrid-ssoauth-azure.py` 指令碼。這個 Python 指令碼直接向 StorageGRID 發出兩個請求（第一個請求用於取得 SAMLRequest，第二個請求用於取得授權權杖），同時也呼叫 Node.js 指令碼與 Entra ID 互動以執行 SSO 操作。

SSO 作業可以使用一系列 API 要求來執行，但這樣做並不簡單。Puppeteer Node.js 模組可用於抓取 Entra ID SSO 介面。

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

步驟

1. 依下列步驟安裝所需的相依性：
 - a. 安裝 Node.js（請參閱 "<https://nodejs.org/en/download/>"）。
 - b. 安裝所需的 Node.js 模組（puppeteer 和 jsdom）：

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

2. `${post_edited_translations.segment}`

然後，Python 指令碼將呼叫對應的 Node.js 指令碼來執行 Entra ID SSO 互動。

3. 出現提示時，請輸入以下參數的值（或使用參數傳遞它們）：
 - 用於登入 Entra ID 的 SSO 電子郵件地址
 - `${post_edited_translations.segment}`
 - `${post_edited_translations.segment}`
4. 出現提示時，輸入密碼，並準備好在 Entra ID 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'}
```



該指令碼假定使用 Microsoft Authenticator 進行多因素驗證 (MFA)。您可能需要修改指令碼以支援其他形式的 MFA (例如輸入透過簡訊收到的驗證碼)。

StorageGRID 授權權杖已在輸出中提供。現在，您可以像未使用 SSO 時使用 API 一樣，使用此權杖發出其他請求。

如果啟用單一登入，請使用 **StorageGRID API (PingFederate)**

如果您擁有"`${post_edited_translations.segment}`"並使用 PingFederate 作為 SSO 供應商，則必須發出一系列 API 請求，以取得對 Grid Management API 或 Tenant Management API 有效的驗證權杖。

如果啟用了單一登入，請登入 **API**。

如果您使用 PingFederate 作為 SSO 身分供應商，則適用以下說明。

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。
- 如果您想存取租戶管理 API，您需要知道租戶帳戶 ID。

關於此任務

若要取得驗證令牌，您可以使用下列範例之一：

- The `storagegrid-ssoauth.py` Python 指令碼位於 StorageGRID 安裝檔案目錄中，(`./rpms``適用於 RHEL，`./debs``適用於 Ubuntu 或 Debian，以及 `./vsphere``適用於 VMware)。
- curl 請求的工作流程範例。

如果您執行 curl 工作流程的速度太慢，該工作流程可能會逾時。您可能會看到錯誤：A valid SubjectConfirmation was not found on this Response。



`${post_edited_translations.segment}`

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

步驟

1. 請選擇以下其中一種方法來取得驗證權杖：

- 使用 `storagegrid-ssoauth.py` Python 指令碼。前往步驟 2。
- 使用 curl 請求。前往步驟 3。

2. 如果您想使用該 `storagegrid-ssoauth.py` 指令碼，請將指令碼傳遞給 Python 解譯器並執行該指令碼。

`${post_edited_translations.segment}`

- SSO 方法。您可以輸入 "pingfederate" 的任何變體 (PINGFEDERATE、pingfederate 等)。
- SSO 使用者名稱
- 安裝 StorageGRID 的網域。此欄位不用於 PingFederate。您可以將其保留空白，或輸入任何值。

- `${post_edited_translations.segment}`
- 如果您想存取租戶管理 API，則需要租戶帳戶 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
```

StorageGRID 授權權杖已在輸出中提供。現在，您可以像未使用 SSO 時使用 API 一樣，使用此權杖發出其他請求。

3. 如果要使用 curl 請求，請依照下列步驟操作。

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 Grid Management API，請使用 0 作為 TENANTACCOUNTID。

b. 若要接收已簽署的驗證 URL，請向 `/api/v3/authorize-saml` 發出 POST 要求，並從回應中移除額外的 JSON 編碼。

此範例顯示針對 TENANTACCOUNTID 的已簽署驗證 URL 的 POST 要求。結果將傳遞至 `python -m json.tool` 以移除 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
```

此範例的回應包含一個經過 URL 編碼的簽章 URL，但不包含額外的 JSON 編碼階層。

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

- c. 儲存回應中的 SAMLRequest，以便在後續命令中使用。

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

- d. 匯出回應和 Cookie，並輸出回應：

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

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

- e. 匯出「pf.adapterId」值，並輸出回應：

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

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

- f. \${post_edited_translations.segment}

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

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

- g. 匯出「行動」值：

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

- h. 傳送 Cookie 及憑證：

```
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. 儲存隱藏欄位中的 SAMLResponse 值：

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

- j. 使用已儲存的 SAMLResponse，向 StorageGRID 發出 /api/saml-response 請求以產生 StorageGRID 驗證權杖。

對於 RelayState，請使用租戶帳戶 ID，或者如果您想要登入 Grid Management API，請使用 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. 將回應中的驗證權杖儲存為 MYTOKEN。

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

現在您可以使用 MYTOKEN 來處理其他請求，就像未使用 SSO 時使用 API 一樣。

如果啟用了單一登入，請登出 **API**。

如果已啟用單一登入（SSO），您必須發出一系列 API 要求，以登出 Grid Management API 或 Tenant Management API。如果您使用 PingFederate 作為 SSO 身分識別供應商，則適用這些說明

關於此任務

如有需要，您可以透過組織的單一登出頁面登出，從而退出 StorageGRID API。或者，您也可以從 StorageGRID 觸發單一登出（SLO），這需要有效的 StorageGRID 持有者權杖。

步驟

1. 若要產生已簽署的登出請求，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
```

傳回一個登出 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. 儲存登出 URL。

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

3. \${post_edited_translations.segment}

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

返回 302 回應。重新導向位置不適用於僅透過 API 進行的登出。

```
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. \${post_edited_translations.segment}

刪除 StorageGRID bearer token 的運作方式與沒有 SSO 時相同。如果未提供 `Cookie "sso=true"，使用者將從 StorageGRID 登出，而不影響 SSO 狀態。

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

A 204 No Content 回應表示使用者現在已登出。

HTTP/1.1 204 No Content

使用 API 停用 StorageGRID 功能

您可以使用 Grid Management API 完全停用 StorageGRID 系統中的特定功能。停用功能後，即無法指派任何人執行與該功能相關工作的權限。

關於此任務

「已停用功能」系統可讓您封鎖對 StorageGRID 系統中某些功能的存取。停用功能是阻止 root 使用者或屬於具有 **Root access** 權限之管理員群組的使用者使用該功能的唯一方法。

為了理解此功能的用途，請考慮以下場景：

A 公司是一家服務供應商，透過建立租戶帳戶的方式出租其 StorageGRID 系統的儲存容量。為了保護租戶物件的安全性，A 公司希望確保其員工在帳戶部署後永遠無法存取任何租戶帳戶。

公司 A 可以透過使用 Grid Management API 中的「停用功能」系統來達成此目標。透過在 Grid Manager（包括使用者介面和 API）中完全停用「變更租戶 root 密碼」功能，公司 A 可確保管理員使用者（包括 root 使用者和屬於具有「Root 存取權」權限之群組的使用者）無法變更任何租戶帳戶的 root 使用者密碼。

步驟

1. 存取網格管理 API 的 Swagger 文件。參見"[\\${post_edited_translations.segment}](#)"。
2. 找到「停用功能」端點。
3. 若要停用某項功能（例如「變更租戶 root 使用者密碼」），請向 API 傳送如下的請求本文：

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

當要求完成時，「變更租戶 root 密碼」功能即會停用。變更租戶 **root** 密碼 管理權限將不再出現在使用者介面中，且任何嘗試變更租戶 root 密碼的 API 要求都將失敗，並出現 "403 Forbidden"。

[\\${post_edited_translations.segment}](#)

預設情況下，您可以使用 Grid Management API 重新啟用已停用的功能。但是，如果您希望防止已停用的功能被重新啟用，則可以停用 **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還原任何遺失的功能。

步驟

1. `${post_edited_translations.segment}`
2. 找到「停用功能」端點。
3. `${post_edited_translations.segment}`

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

當此要求完成時，所有功能（包括變更租戶根目錄密碼功能）都會重新啟用。「變更租戶根目錄密碼」管理權限現在會顯示在使用者介面中，且任何嘗試變更租戶根目錄密碼的 API 要求都將成功，前提是使用者具有「**root** 存取權」或「變更租戶根目錄密碼」管理權限。



前面的範例會重新啟用所有已停用的功能。如果還有其他已停用但應保持停用狀態的功能，則必須在 PUT 請求中明確指定它們。例如，若要重新啟用「變更租戶根目錄密碼」功能並繼續停用 storageAdmin 管理權限，請傳送下列 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。