如果啟用了單一登入，請使用 API。

StorageGRID software

NetApp
July 23, 2026

目錄

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=fZHRToMwFIZfhb...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=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. 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=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://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3
D",
    "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: MSISSignoutProtocol=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
```

版權資訊

商標資訊