如果啟用了單一登錄，請使用 API

StorageGRID software

NetApp
May 29, 2026

目錄

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。

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
```

版權資訊

商標資訊