シングルサインオンが有効になっている場合は**API**を使用する

StorageGRID software

NetApp
December 03, 2025

目次

シングルサインオンが有効になっている場合はAPIを使用する

シングル サインオンが有効になっている場合は API を使用する (Active Directory)

もしあなたが"シングル サインオン (SSO) を設定して有効にする"Active Directory を SSO プロバイダーとして使用する場合は、一連の API 要求を発行して、グリッド管理 API またはテナント管理 API に有効な認証トークンを取得する必要があります。

シングル サインオンが有効になっている場合は、API にSign in。

これらの手順は、Active Directory を SSO ID プロバイダーとして使用している場合に適用されます。

開始する前に

- StorageGRIDユーザー グループに属するフェデレーション ユーザーの SSO ユーザー名とパスワードがわかっています。
- テナント管理 API にアクセスする場合は、テナント アカウント ID がわかっている必要があります。

タスク概要

認証トークンを取得するには、次のいずれかの例を使用できます。

- その `storagegrid-ssoauth.py`StorageGRIDインストール ファイル ディレクトリにある Python スクリプト (./rpms`Red Hat Enterprise Linuxの場合、 `./debs` UbuntuまたはDebianの場合、 `./vsphere` VMware の場合)。
- curl リクエストのワークフローの例。

  curl ワークフローは、実行速度が遅すぎるとタイムアウトする可能性があります。次のエラーが表示される場合があります: `A valid SubjectConfirmation was not found on this Response`。

  > サンプルの curl ワークフローでは、パスワードが他のユーザーから見られないように保護されません。

URL エンコードの問題がある場合は、次のエラーが表示されることがあります。 `Unsupported SAML version`。

手順

1. 認証トークンを取得するには、次のいずれかの方法を選択します。
   - 使用 `storagegrid-ssoauth.py`Python スクリプト。ステップ 2 に進みます。
   - curl リクエストを使用します。ステップ 3 に進みます。
2. 使用したい場合は `storagegrid-ssoauth.py`スクリプトの場合は、スクリプトを Python インタープリターに渡してスクリプトを実行します。

   プロンプトが表示されたら、次の引数の値を入力します。

- SSO 方式。 ADFS または adfs を入力します。
- SSOユーザ名
- StorageGRIDがインストールされているドメイン
- StorageGRIDのアドレス
- テナント管理 API にアクセスする場合のテナント アカウント 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認証トークンが出力に提供されます。 SSO が使用されていない場合に API を使用するのと同様に、他のリクエストにもトークンを使用できるようになりました。

3. curl リクエストを使用する場合は、次の手順に従います。

   a. サインインに必要な変数を宣言します。

```
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'
```

   > グリッド管理APIにアクセスするには、0を次のように使用します。 `TENANTACCOUNTID` 。

   b. 署名された認証URLを受け取るには、POSTリクエストを発行します。 `/api/v3/authorize-saml` 、レスポンスから追加の JSON エンコーディングを削除します。

   この例では、署名付き認証URLのPOSTリクエストを示しています。 `TENANTACCOUNTID` 。結果は `python -m json.tool`JSON エンコーディングを削除します。

```
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
```

この例の応答には、URL エンコードされた署名付き URL が含まれますが、追加の JSON エンコードレイヤーは含まれません。

```
{
    "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. 保存する `SAMLRequest`後続のコマンドで使用するために応答から取得します。

```
export SAMLREQUEST='fZHLbsIwEEV%2FJTuv7...sSl%2BfQ33cvfwA%3D'
```

d. AD FS からクライアント要求 ID を含む完全な URL を取得します。

1 つのオプションは、前の応答からの URL を使用してログイン フォームを要求することです。

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

応答にはクライアント要求 ID が含まれます。

```
<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. 応答からクライアント要求 ID を保存します。

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

f. 前の応答からのフォーム アクションに資格情報を送信します。

```
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 は、ヘッダーに追加情報を含む 302 リダイレクトを返します。

SSO システムで多要素認証 (MFA) が有効になっている場合は、フォーム投稿に 2 番目のパスワードまたはその他の資格情報も含まれます。

```
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. 保存する `MSISAuth`応答から Cookie を取得します。

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

h. 認証 POST からの Cookie を含む GET リクエストを指定された場所に送信します。

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client-request-
id=$SAMLREQUESTID" \
--cookie "MSISAuth=$MSISAuth" --include
```

応答ヘッダーには、後でログアウトする際に使用する AD FS セッション情報が含まれ、応答本体には非表示のフォーム フィールドに SAMLResponse が含まれます。

```
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. 保存する `SAMLResponse`隠しフィールドから:

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

j. 保存した `SAMLResponse`、 StorageGRIDを作成する`/api/saml-response`StorageGRID認証トークンを生成するためのリクエスト。

のために `RelayState`、テナント アカウント ID を使用するか、Grid Management API にサインインする場合は 0 を使用します。

```
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
```

応答には認証トークンが含まれます。

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. レスポンス内の認証トークンを次のように保存します。 `MYTOKEN` 。

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

使用できるようになりました `MYTOKEN`その他のリクエストについては、SSO が使用されていない場合に API を使用する方法と同様です。

シングル サインオンが有効になっている場合は、**API** からサインアウトします。

シングル サインオン (SSO) が有効になっている場合は、グリッド管理 API またはテナント管理 API からサインアウトするための一連の API 要求を発行する必要があります。これらの手順は、Active Directory を SSO ID プロバイダーとして使用している場合に適用されます。

タスク概要

必要に応じて、組織のシングル ログアウト ページからログアウトすることで、 StorageGRID API からサインアウトできます。または、有効なStorageGRIDベアラー トークンを必要とするStorageGRIDからシングル ログアウト (SLO) をトリガーすることもできます。

手順

1. 署名付きログアウト リクエストを生成するには、`cookie "sso=true" を SLO API に渡します。

```
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
```

ログアウト URL が返されます:

```
{
    "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. ログアウト URL を保存します。

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

3. ログアウト URL にリクエストを送信して、SLO をトリガーし、 StorageGRIDにリダイレクトします。

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

302 応答が返されます。リダイレクト場所は、API のみのログアウトには適用されません。

```
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. StorageGRIDベアラー トークンを削除します。

StorageGRIDベアラー トークンの削除は、SSO がない場合と同じように機能します。 `cookie "sso=true" が提供されない場合、ユーザーは SSO 状態に影響を与えずにStorageGRIDからログアウトされます。

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

あ `204 No Content`この応答は、ユーザーが現在サインアウトしていることを示します。

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

シングル サインオンが有効になっている場合は API を使用する (Azure)

もしあなたが"シングル サインオン (SSO) を設定して有効にする"Azure を SSO プロバイダーとして使用する場合、2 つのサンプル スクリプトを使用して、グリッド管理 API またはテナント管理 API に有効な認証トークンを取得できます。

Azure シングル サインオンが有効になっている場合は、API にSign in。

これらの手順は、Azure を SSO ID プロバイダーとして使用している場合に適用されます。

開始する前に

- StorageGRIDユーザー グループに属するフェデレーション ユーザーの SSO 電子メール アドレスとパスワードがわかっています。
- テナント管理 API にアクセスする場合は、テナント アカウント ID がわかっている必要があります。

タスク概要

認証トークンを取得するには、次のサンプル スクリプトを使用できます。

- その `storagegrid-ssoauth-azure.py`Pythonスクリプト
- その `storagegrid-ssoauth-azure.js`Node.jsスクリプト

両方のスクリプトはStorageGRIDインストールファイルディレクトリにあります。(`./rpms` Red Hat Enterprise Linuxの場合、 `./debs` UbuntuまたはDebianの場合、 `./vsphere` VMware の場合)。

Azureとの独自のAPI統合を作成するには、 `storagegrid-ssoauth-azure.py`スクリプト。 Python スクリプトは、 StorageGRIDに 2 つのリクエストを直接送信します (最初に SAMLRequest を取得し、後で認証トークンを取得します)。また、Node.js スクリプトを呼び出して Azure と対話し、SSO 操作を実行します。

SSO 操作は一連の API リクエストを使用して実行できますが、実行するのは簡単ではありません。Puppeteer Node.js モジュールは、Azure SSO インターフェイスをスクレイピングするために使用されます。

URL エンコードの問題がある場合は、次のエラーが表示されることがあります。 `Unsupported SAML version` 。

手順

1. 次のように、必要な依存関係をインストールします。
   a. Node.jsをインストールする（ "https://nodejs.org/en/download/" ）。
   b. 必要な Node.js モジュール (puppeteer と jsdom) をインストールします。

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

2. Python スクリプトを Python インタープリターに渡してスクリプトを実行します。

   次に、Python スクリプトは対応する Node.js スクリプトを呼び出して、Azure SSO のやり取りを実行します。

3. プロンプトが表示されたら、次の引数の値を入力します (またはパラメータを使用して渡します)。
   - Azure へのサインインに使用する SSO 電子メール アドレス
   - StorageGRIDのアドレス
   - テナント管理 API にアクセスする場合のテナント アカウント ID
4. プロンプトが表示されたら、パスワードを入力し、要求された場合に Azure に MFA 認証を提供できるように準備します。

```
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'}
```

> このスクリプトでは、MFA が Microsoft Authenticator を使用して実行されることを前提としています。他の形式の MFA (テキスト メッセージで受信したコードの入力など) をサポートするには、スクリプトを変更する必要がある場合があります。

StorageGRID認証トークンが出力に提供されます。 SSO が使用されていない場合に API を使用するのと同様に、他のリクエストにもトークンを使用できるようになりました。

シングル サインオンが有効になっている場合は API を使用する (PingFederate)

もしあなたが"シングル サインオン (SSO) を設定して有効にする"PingFederate を SSO プロバイダーとして使用する場合は、一連の API 要求を発行して、Grid Management API または Tenant Management API に有効な認証トークンを取得する必要があります。

シングル サインオンが有効になっている場合は、API にSign in。

これらの手順は、PingFederateをSSO IDプロバイダーとして使用している場合に適用されます。

開始する前に

- StorageGRIDユーザー グループに属するフェデレーション ユーザーの SSO ユーザー名とパスワードがわかっています。
- テナント管理 API にアクセスする場合は、テナント アカウント ID がわかっている必要があります。

タスク概要

認証トークンを取得するには、次のいずれかの例を使用できます。

- その `storagegrid-ssoauth.py`StorageGRIDインストール ファイル ディレクトリにある Python スクリプト (./rpms`Red Hat Enterprise Linuxの場合、 `./debs` UbuntuまたはDebianの場合、 `./vsphere` VMware の場合)。
- curl リクエストのワークフローの例。

curl ワークフローは、実行速度が遅すぎるとタイムアウトする可能性があります。次のエラーが表示される場合があります: `A valid SubjectConfirmation was not found on this Response` 。

> サンプルの curl ワークフローでは、パスワードが他のユーザーから見られないように保護されません。

URL エンコードの問題がある場合は、次のエラーが表示されることがあります。 `Unsupported SAML version` 。

手順

1. 認証トークンを取得するには、次のいずれかの方法を選択します。
   - 使用 `storagegrid-ssoauth.py`Python スクリプト。ステップ 2 に進みます。
   - curl リクエストを使用します。ステップ 3 に進みます。
2. 使用したい場合は `storagegrid-ssoauth.py`スクリプトの場合は、スクリプトを Python インタープリターに渡してスクリプトを実行します。

   プロンプトが表示されたら、次の引数の値を入力します。
   - SSO 方式。 「pingfederate」の任意のバリエーション（PINGFEDERATE、pingfederate など）を入力できます。
   - SSOユーザ名
   - StorageGRIDがインストールされているドメイン。このフィールドは PingFederate では使用されません。空白のままにすることも、任意の値を入力することもできます。
   - StorageGRIDのアドレス
   - テナント管理 API にアクセスする場合のテナント アカウント 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認証トークンが出力に提供されます。 SSO が使用されていない場合に API を使用するのと同様に、他のリクエストにもトークンを使用できるようになりました。
3. curl リクエストを使用する場合は、次の手順に従います。
   a. サインインに必要な変数を宣言します。

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
```

グリッド管理APIにアクセスするには、0を次のように使用します。 `TENANTACCOUNTID` 。

b. 署名された認証URLを受け取るには、POSTリクエストを発行します。 `/api/v3/authorize-saml` 、レスポンスから追加の JSON エンコーディングを削除します。

この例は、TENANTACCOUNTID の署名付き認証 URL に対する POST リクエストを示しています。結果は python -m json.tool に渡され、JSON エンコーディングが削除されます。

```
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
```

この例の応答には、URL エンコードされた署名付き URL が含まれますが、追加の JSON エンコードレイヤーは含まれません。

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

c. 保存する `SAMLRequest`後続のコマンドで使用するために応答から取得します。

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

d. 応答と Cookie をエクスポートし、応答をエコーします。

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

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

e. 'pf.adapterId' の値をエクスポートし、応答をエコーします。

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

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

f. 'href' 値をエクスポートし (末尾のスラッシュ / を削除)、応答をエコーします。

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

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

g. 「アクション」値をエクスポートします。

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

h. 資格情報とともに Cookie を送信します。

```
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. 保存する `SAMLResponse`隠しフィールドから:

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

j. 保存した `SAMLResponse`、 StorageGRIDを作成する`/api/saml-response`StorageGRID認証トークンを生成するためのリクエスト。

のために `RelayState`、テナント アカウント ID を使用するか、Grid Management API にサインインする場合は 0 を使用します。

```
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
```

応答には認証トークンが含まれます。

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. レスポンス内の認証トークンを次のように保存します。 `MYTOKEN` 。

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

使用できるようになりました `MYTOKEN`その他のリクエストについては、SSO が使用されていない場合に API を使用する方法と同様です。

シングル サインオンが有効になっている場合は、**API** からサインアウトします。

シングル サインオン (SSO) が有効になっている場合は、グリッド管理 API またはテナント管理 API からサインアウトするための一連の API 要求を発行する必要があります。これらの手順は、PingFederateをSSO IDプロバイダーとして使用している場合に適用されます。

タスク概要

必要に応じて、組織のシングル ログアウト ページからログアウトすることで、 StorageGRID API からサインアウトできます。または、有効なStorageGRIDベアラー トークンを必要とするStorageGRIDからシングル ログアウト (SLO) をトリガーすることもできます。

手順

1. 署名付きログアウト リクエストを生成するには、`cookie "sso=true" を SLO API に渡します。

```
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
```

ログアウト URL が返されます:

```
{
    "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. ログアウト URL を保存します。

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

3. ログアウト URL にリクエストを送信して、SLO をトリガーし、 StorageGRIDにリダイレクトします。

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

302 応答が返されます。リダイレクト場所は、API のみのログアウトには適用されません。

```
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. StorageGRIDベアラー トークンを削除します。

StorageGRIDベアラー トークンの削除は、SSO がない場合と同じように機能します。 `cookie "sso=true" が提供されない場合、ユーザーは SSO 状態に影響を与えずにStorageGRIDからログアウトされます。

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

あ `204 No Content`この応答は、ユーザーが現在サインアウトしていることを示します。

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

著作権に関する情報

商標に関する情報