シングルサインオンが有効な場合は、 API を使用します

StorageGRID

NetApp
October 03, 2025

目次

シングルサインオンが有効な場合は、 API を使用します

シングルサインオンが有効な場合（ Active Directory ）は API を使用

ある場合 シングルサインオン（ SSO ）の設定と有効化 また、 Active Directory を SSO プロバイダとして使用する場合は、一連の API 要求を問題 で実行して、グリッド管理 API またはテナント管理 API で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な場合は、 API にサインインします

ここで説明する手順は、 Active Directory を SSO アイデンティティプロバイダとして使用する場合に該当します。

必要なもの

- StorageGRID ユーザグループに属するフェデレーテッドユーザの SSO ユーザ名とパスワードが必要です。
- 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 を確認しておきます。

このタスクについて

認証トークンを取得するには、次のいずれかの例を使用します。

- StorageGRID インストールファイルディレクトリ (Red Hat Enterprise Linux または CentOS の場合は「 ./rpms 」、 Ubuntu または Debian の場合は「 ./debs 」、 VMware の場合は「 ./vsphere-vsphere 」) にある「 storagegrid-ssoauth.py 」 p`python スクリプト。
- cURL 要求のワークフローの例。

  cURL ワークフローは、実行に時間がかかりすぎるとタイムアウトする場合があります。「 A valid SubjectConfirmation was not found on this Response 」というエラーが表示される可能性があります。

  cURL ワークフローの例では、パスワードが他のユーザに表示されないように保護されていません。

URL エンコーディング問題 を使用している場合は、「 Unsupported SAML version 」というエラーが表示される可能性があります。

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。
   - 「 storagegrid -ssoauth.py 」 Python スクリプトを使用します。手順 2 に進みます。
   - curl 要求を使用します。手順 3 に進みます。
2. 「 storagegrid -ssoauth.py 」スクリプトを使用する場合は、 Python インタープリタにスクリプトを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 と入力します。
- 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は、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表示されます。SSO を使用していない場合の API の使用方法と同様に、トークンを他の要求に使用できるようになりました。

3. cURL 要求を使用する場合は、次の手順 を使用します。

   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'
```

   Grid Management API にアクセスするには、 0 を「 TENANTACCOUNTID 」として使用します。

   b. 署名付き認証 URL を受信するには、問題 A POST 要求を「 /api/v3/authorize-saml 」に送信し、応答から JSON エンコードを削除します。

   次の例は 'TENANTACCOUNTID' の署名済み認証 URL に対する POST 要求を示しています結果は 'python-m JSOT' 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済み URL が含まれていますが、 JSON エンコードされたレイヤは含まれていません。

```
{
    "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. 後続のコマンドで使用するために ' 応答から SAMLRequest を保存します

```
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 つは、前の応答の URL を使用してログインフォームを要求する方法です。

```
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 が含まれています。

```
<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. 前の応答のフォームアクションにクレデンシャルを送信します。

```
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 からヘッダーに追加情報 が含まれた 302 リダイレクトが返されます。

SSO システムで多要素認証（ MFA ）が有効になっている場合、フォームポストには 2 つ目のパスワードまたはその他のクレデンシャルも含まれます。

```
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. 応答から MSISAuth クッキーを保存します。

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

h. 認証 POST からクッキーを使用して、指定した場所に GET 要求を送信します。

```
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、あとでログアウトに使用する AD FS セッション情報が含まれます。応答の本文には、非表示のフォームフィールドに SAMLResponse が含まれています。

```
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. 非表示フィールドから SAMLResponse を保存します

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

j. 保存した SAMLResponse を使用して、 StorageGRID 認証トークンを生成する StorageGRID の「 /api/saml-response` 要求」を作成します。

「 RelayState 」の場合はテナントアカウント ID を使用し、 Grid 管理 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ています。

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

a. 認証トークンを応答に「 MYTOKEN 」として保存します。

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

これで、 SSO を使用していない場合の API の使用方法と同じように、他の要求に「 MYTOKEN 」を使用できます。

シングルサインオンが有効な場合は、 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 要求を問題 で処理する必要があります。ここで説明する手順は、 Active Directory を SSO アイデンティティプロバイダとして使用する場合に該当します

このタスクについて

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だけで、 StorageGRID API からサインアウトできます。または、 StorageGRID からシングルログアウト（ SLO ）を実行することもできます。この場合、有効な StorageGRID ベアラトークンが必要です。

手順

1. 署名されたログアウト要求を生成するには、「 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. 要求をログアウト URL に送信し、 SLO を実行して StorageGRID にリダイレクトします。

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

302 応答が返されます。リダイレクト先は 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 Bearer トークンを削除します。

StorageGRID Bearer トークンを削除すると、 SSO を使用しない場合と同じように動作します。「 cookie 」 sso=true' が指定されていない場合、ユーザーは SSO 状態に影響を与えることなく 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
```

「 204 No Content 」応答は、ユーザがサインアウトしたことを示します。

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

シングルサインオンが有効な場合（ Azure ）は API を使用

ある場合 シングルサインオン（ SSO ）の設定と有効化 また、 Azure を SSO プロバイダとして使用している場合は、 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 で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な場合は、 API にサインインします

以下の手順は、 Azure を SSO アイデンティティプロバイダとして使用する場合に該当します

必要なもの

- StorageGRID ユーザグループに属するフェデレーテッドユーザの SSO E メールアドレスとパスワードが必要です。
- 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 を確認しておきます。

このタスクについて

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します。

- 「 storagegrid-ssoauth-caz.py 」 Python スクリプト
- 「 storagegrid-ssoauth-azure.js 」スクリプト

どちらのスクリプトも、 StorageGRID インストールファイルディレクトリ (Red Hat Enterprise Linux または CentOS 用の場合は「 ./rpms 」、 Ubuntu または Debian 用の場合は「 ./debs 」、 VMware 用の「 ./vsphere 」) にあります。

独自の API 統合を Azure に記述するには、「 storagegrid-ssoauth-azure.py 」スクリプトを参照してください。Python スクリプトは、 StorageGRID に対して 2 つの要求を直接実行し（まず SAMLRequest を取得し、あとで認証トークンを取得するため）、さらに Node.js スクリプトを呼び出して、 SSO 処理を実行します。

SSO 処理は一連の API 要求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破棄するために使用します。

URL エンコーディング問題 を使用している場合は、「 Unsupported SAML version 」というエラーが表示される可能性があります。

手順

1. 必要な依存関係を次のようにインストールします。
   a. Node.js をインストールします（を参照） "https://nodejs.org/en/download/"）。
   b. 必要な Node.js モジュール（ puppeteer および jsdom ）を取り付けます。

      'NPM install-g <module>`
2. Python スクリプトを Python インタープリタに渡して、スクリプトを実行します。

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 のインタラクションを実行します。

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 E 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は、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 に対する 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ていることを前提として他の形式の MFA （テキストメッセージで受信したコードの入力など）をサポートするために、スクリプトの変更が必要になる場合があります。

StorageGRID 認証トークンが出力に表示されます。SSO を使用していない場合の API の使用方法と同様に、トークンを他の要求に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な場合は **API** を使用（ **PingFederate** ）

ある場合 シングルサインオン（ SSO ）の設定と有効化 また、 SSO プロバイダとして PingFederate を使用するには、グリッド管理 API またはテナント管理 API で有効な認証トークンを取得するための一連の API 要求を問題 で処理する必要があります。

シングルサインオンが有効な場合は、 **API** にサインインします

これらの手順は、 SSO アイデンティティプロバイダとして PingFederate を使用している場合に適用されます

必要なもの

- StorageGRID ユーザグループに属するフェデレーテッドユーザの SSO ユーザ名とパスワードが必要です。
- 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 を確認しておきます。

このタスクについて

認証トークンを取得するには、次のいずれかの例を使用します。

- StorageGRID インストールファイルディレクトリ (Red Hat Enterprise Linux または CentOS の場合は「 ./rpms 」、 Ubuntu または Debian の場合は「 ./debs 」、 VMware の場合は「 ./vsphere-vsphere 」) に

ある「 storagegrid-ssoauth.py 」 p`python スクリプト。

- cURL 要求のワークフローの例。

  cURL ワークフローは、実行に時間がかかりすぎるとタイムアウトする場合があります。「 A valid SubjectConfirmation was not found on this Response 」というエラーが表示される可能性があります。

  > cURL ワークフローの例では、パスワードが他のユーザに表示されないように保護されていません。

  URL エンコーディング問題 を使用している場合は、「 Unsupported SAML version 」というエラーが表示される可能性があります。

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。
   - 「 storagegrid -ssoauth.py 」 Python スクリプトを使用します。手順 2 に進みます。
   - curl 要求を使用します。手順 3 に進みます。
2. 「 storagegrid -ssoauth.py 」スクリプトを使用する場合は、 Python インタープリタにスクリプトを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 」（ PingFederate 、 PingFederate など）の任意のバリエーションを入力できます。
   - 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 には使用されません。空白のままにするか、任意の値を入力できます。
   - StorageGRID のアドレス
   - テナント管理 API にアクセスする場合は、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表示されます。SSO を使用していない場合の API の使用方法と同様に、トークンを他の要求に使用できるようになりました。

3. cURL 要求を使用する場合は、次の手順 を使用します。

   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'
```

Grid Management API にアクセスするには、 0 を「 TENANTACCOUNTID 」として使用します。

b. 署名付き認証 URL を受信するには、問題 A POST 要求を「 /api/v3/authorize-saml 」に送信し、応答から JSON エンコードを削除します。

次の例は、 TENANTACCOUNTID の署名済み認証 URL を取得するための POST 要求です。結果は python-m json ツールに渡され、 JSON エンコードが削除されます。

```
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済み URL が含まれていますが、 JSON エンコードされたレイヤは含まれていません。

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

c. 後続のコマンドで使用するために ' 応答から SAMLRequest を保存します

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

d. 応答とクッキーをエクスポートし、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' 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. 「 action 」の値をエクスポートします。

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

h. クレデンシャルとともに Cookie を送信する：

```
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. 非表示フィールドから SAMLResponse を保存します

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

j. 保存した SAMLResponse を使用して、 StorageGRID 認証トークンを生成する StorageGRID の「 /api/saml-response` 要求」を作成します。

「 RelayState 」の場合はテナントアカウント ID を使用し、 Grid 管理 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ています。

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

a. 認証トークンを応答に「 MYTOKEN 」として保存します。

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

これで、 SSO を使用していない場合の API の使用方法と同じように、他の要求に「 MYTOKEN 」を使用できます。

シングルサインオンが有効な場合は、 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 要求を問題 で処理する必要があります。これらの手順は、 SSO アイデンティティプロバイダとして PingFederate を使用している場合に適用されます

このタスクについて

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だけで、 StorageGRID API からサインアウトできます。または、 StorageGRID からシングルログアウト（ SLO ）を実行することもできます。この場合、有効な StorageGRID ベアラトークンが必要です。

手順

1. 署名されたログアウト要求を生成するには、「 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. 要求をログアウト URL に送信し、 SLO を実行して StorageGRID にリダイレクトします。

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

302 応答が返されます。リダイレクト先は 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 Bearer トークンを削除します。

StorageGRID Bearer トークンを削除すると、 SSO を使用しない場合と同じように動作します。「 cookie 」 sso=true' が指定されていない場合、ユーザーは SSO 状態に影響を与えることなく 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
```

「 204 No Content 」応答は、ユーザがサインアウトしたことを示します。

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

著作権に関する情報

商標に関する情報