싱글 사인온(SSO)이 활성화된 경우 API를 사용합니다.

StorageGRID software

NetApp
July 23, 2026

목차

싱글 사인온(SSO)이 활성화된 경우 API를 사용합니다. . . . 1
SSO(Single Sign-On)가 활성화된 경우(Active Directory) StorageGRID API를 사용하십시오 . . . 1
싱글 사인온이 활성화된 경우 API에 로그인합니다. . . . 1
싱글 사인온(SSO)이 활성화된 경우 API에서 로그아웃 . . . 6
싱글 사인온이 활성화된 경우(Entra ID) StorageGRID API를 사용하십시오 . . . 7
Entra ID 싱글 사인온이 활성화된 경우 API에 로그인 . . . 8
SSO(Single Sign-On)가 활성화된 경우(PingFederate) StorageGRID API를 사용합니다 . . . 9
싱글 사인온이 활성화된 경우 API에 로그인합니다. . . . 9
싱글 사인온(SSO)이 활성화된 경우 API에서 로그아웃 . . . 13

싱글 사인온(SSO)이 활성화된 경우 API를 사용합니다.

SSO(Single Sign-On)가 활성화된 경우(Active Directory) StorageGRID API를 사용하십시오

"싱글 사인온(SSO)을 구성하고 활성화했습니다."가 있고 Active Directory를 SSO 공급자로 사용하는 경우, 그리드 관리 API 또는 테넌트 관리 API에 유효한 인증 토큰을 얻기 위해 일련의 API 요청을 실행해야 합니다.

싱글 사인온이 활성화된 경우 API에 로그인합니다.

이 지침은 Active Directory를 SSO ID 공급자로 사용하는 경우에 적용됩니다.

시작하기 전에

- StorageGRID 사용자 그룹에 속한 페더레이션 사용자의 SSO 사용자 이름과 암호를 알고 있습니다.
- 테넌트 관리 API에 액세스하려면 테넌트 계정 ID를 알고 있어야 합니다.

이 작업 정보

인증 토큰을 얻으려면 다음 예시 중 하나를 사용할 수 있습니다.

- 해당 `storagegrid-ssoauth.py` Python 스크립트는 StorageGRID 설치 파일 디렉터리((`./rpms` RHEL, `./debs` Ubuntu 또는 Debian, `./vsphere` VMware)에 있습니다.
- curl 요청의 예시 워크플로입니다.

  curl 워크플로를 너무 느리게 실행하면 시간 초과 오류가 발생할 수 있습니다. 다음과 같은 오류 메시지가 표시될 수 있습니다. `A valid SubjectConfirmation was not found on this Response`.

  > 예시로 제시된 curl 워크플로는 다른 사용자가 비밀번호를 볼 수 없도록 보호하지 않습니다.

URL 인코딩 문제가 있는 경우 다음과 같은 오류 메시지가 표시될 수 있습니다. `Unsupported SAML version`.

단계

1. 인증 토큰을 얻으려면 다음 방법 중 하나를 선택하십시오.
   - Use the `storagegrid-ssoauth.py` Python 스크립트를 사용합니다. 2단계로 이동합니다.
   - curl 요청을 사용합니다. 3단계로 이동합니다.
2. `storagegrid-ssoauth.py` 스크립트를 사용하려면 Python 인터프리터에 스크립트를 전달하고 실행하십시오.

   메시지가 나타나면 다음 인수에 대한 값을 입력하십시오.
   - SSO 방식입니다. ADFS 또는 adfs를 입력하세요.
   - SSO 사용자 이름
   - StorageGRID가 설치된 도메인
   - StorageGRID의 주소

◦ 테넌트 관리 API에 액세스하려면 테넌트 계정 ID가 필요합니다.

```
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 인증 토큰이 출력 결과에 제공됩니다. 이제 SSO를 사용하지 않을 때 API를 사용하는 방법과 유사하게 이 토큰을 다른 요청에 사용할 수 있습니다.

3. curl 요청을 사용하려면 다음 절차를 따르십시오.

   a. 로그인에 필요한 변수를 선언합니다.

```
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'
```

   그리드 관리 API에 액세스하려면 0을 `TENANTACCOUNTID`로 사용하십시오.

   b. 서명된 인증 URL을 받으려면 `/api/v3/authorize-saml`에 POST 요청을 보내고 응답에서 추가 JSON 인코딩을 제거하십시오.

   이 예시는 `TENANTACCOUNTID`에 대한 서명된 인증 URL의 POST 요청을 보여줍니다. 결과는 JSON 인코딩을 제거하기 위해 `python -m json.tool`에 전달됩니다.

```
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
```

   이 예시의 응답에는 URL 인코딩된 서명된 URL이 포함되지만, 추가적인 JSON 인코딩 계층은 포함되지 않습니다.

```
{
    "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. 응답에서 `SAMLRequest`을(를) 저장하여 이후 명령에서 사용하십시오.

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

d. AD FS에서 클라이언트 요청 ID가 포함된 전체 URL을 가져옵니다.

한 가지 방법은 이전 응답에서 받은 URL을 사용하여 로그인 양식을 요청하는 것입니다.

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

응답에는 클라이언트 요청 ID가 포함되어 있습니다.

```
<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. 응답에서 클라이언트 요청 ID를 저장합니다.

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

f. 이전 응답의 양식 작업으로 자격 증명을 전송합니다.

```
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 FS는 헤더에 추가 정보를 포함하여 302 리디렉션을 반환합니다.

> SSO 시스템에 다단계 인증(MFA)이 활성화된 경우, 폼 제출 시 두 번째 암호 또는 기타 자격 증명도 포함됩니다.

```
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. 응답에서 `MSISAuth` 쿠키를 저장합니다.

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

h. 인증 POST 요청에서 받은 쿠키를 사용하여 지정된 위치로 GET 요청을 보냅니다.

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

응답 헤더에는 나중에 로그아웃할 때 사용할 AD FS 세션 정보가 포함되고, 응답 본문에는 숨겨진 폼 필드에 SAMLResponse가 포함됩니다.

```
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. 숨겨진 필드에서 `SAMLResponse`을(를) 저장합니다.

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

j. 저장된 `SAMLResponse`을 사용하여 StorageGRID `/api/saml-response` 요청을 통해 StorageGRID 인증 토큰을 생성합니다.

`RelayState`의 경우, 테넌트 계정 ID를 사용하거나, 그리드 관리 API에 로그인하려면 0을 사용하십시오.

```
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
```

응답에는 인증 토큰이 포함되어 있습니다.

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

a. 응답에 포함된 인증 토큰을 `MYTOKEN`으로 저장합니다.

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

이제 `MYTOKEN`를 SSO를 사용하지 않을 때 API를 사용하는 방식과 유사하게 다른 요청에도 사용할 수 있습니다.

싱글 사인온(SSO)이 활성화된 경우 API에서 로그아웃

싱글 사인온(SSO)이 활성화된 경우, 그리드 관리 API 또는 테넌트 관리 API에서 로그아웃하려면 일련의 API 요청을 실행해야 합니다. 이 지침은 Active Directory를 SSO ID 공급자로 사용하는 경우에 적용됩니다.

이 작업 정보

필요한 경우 조직의 단일 로그아웃 페이지에서 로그아웃하여 StorageGRID API에서 로그아웃할 수 있습니다. 또는 유효한 StorageGRID 베어러 토큰이 필요한 StorageGRID에서 단일 로그아웃(SLO)을 트리거할 수도 있습니다.

단계

1. 서명된 로그아웃 요청을 생성하려면 SLO API에 `cookie "sso=true"`를 전달하세요.

```
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
```

로그아웃 URL이 반환됩니다.

```
{
    "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. 로그아웃 URL을 저장합니다.

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

3. SLO를 트리거하고 StorageGRID로 다시 리디렉션하려면 로그아웃 URL에 요청을 보내십시오.

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

302 응답이 반환됩니다. 리디렉션 위치는 API 전용 로그아웃에는 적용되지 않습니다.

```
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 베어러 토큰을 삭제합니다.

StorageGRID 베어러 토큰 삭제는 SSO를 사용하지 않을 때와 동일한 방식으로 작동합니다. 쿠키 `"sso=true"`가 제공되지 않으면 SSO 상태에 영향을 주지 않고 사용자가 StorageGRID에서 로그아웃됩니다.

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

A `204 No Content` 응답은 사용자가 로그아웃되었음을 나타냅니다.

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

싱글 사인온이 활성화된 경우(Entra ID) StorageGRID API를 사용하십시오

"싱글 사인온(SSO)을 구성하고 활성화했습니다."가 있고 Entra ID를 SSO 공급자로 사용하는 경우, 두 가지 예제 스크립트를 사용하여 Grid Management API 또는 테넌트 관리 API에 유효한 인증 토큰을 얻을 수 있습니다.

Entra ID 싱글 사인온이 활성화된 경우 API에 로그인

이 지침은 Entra ID를 SSO ID 공급자로 사용하는 경우에 적용됩니다.

시작하기 전에

- StorageGRID 사용자 그룹에 속한 페더레이션 사용자의 SSO 이메일 주소와 비밀번호를 알고 있습니다.
- 테넌트 관리 API에 액세스하려면 테넌트 계정 ID를 알고 있어야 합니다.

이 작업 정보

인증 토큰을 얻으려면 다음 예제 스크립트를 사용할 수 있습니다.

- `storagegrid-ssoauth-azure.py` Python 스크립트
- The `storagegrid-ssoauth-azure.js` Node.js 스크립트

두 스크립트 모두 StorageGRID 설치 파일 디렉터리((`./rpms`RHEL, `./debs`Ubuntu 또는 Debian, `./vsphere`VMware)에 있습니다.

Entra ID와의 API 통합을 직접 작성하려면 `storagegrid-ssoauth-azure.py` 스크립트를 참조하세요. 이 Python 스크립트는 StorageGRID에 직접 두 번의 요청(첫 번째는 SAMLRequest를 가져오기 위한 요청, 두 번째는 인증 토큰을 가져오기 위한 요청)을 보내고, Node.js 스크립트를 호출하여 Entra ID와 상호 작용하며 SSO 작업을 수행합니다.

SSO 작업은 일련의 API 요청을 통해 실행할 수 있지만, 그 과정이 간단하지는 않습니다. Puppeteer Node.js 모듈을 사용하여 Entra ID SSO 인터페이스를 스크래핑합니다.

URL 인코딩 문제가 있는 경우 다음과 같은 오류 메시지가 표시될 수 있습니다. `Unsupported SAML version.`

단계

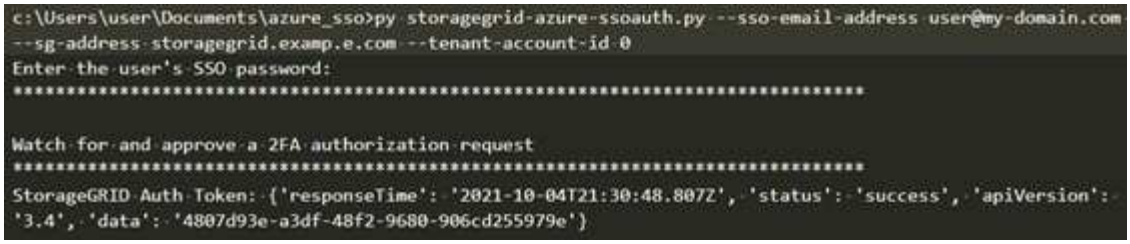
1. 다음과 같이 필요한 종속성을 설치하십시오.
   a. Node.js를 설치합니다(참조 "https://nodejs.org/en/download/").
   b. 필요한 Node.js 모듈(puppeteer 및 jsdom)을 설치합니다.

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

2. 파이썬 스크립트를 파이썬 인터프리터에 전달하여 스크립트를 실행합니다.

   그러면 파이썬 스크립트는 해당 Node.js 스크립트를 호출하여 Entra ID SSO 상호 작용을 수행합니다.

3. 메시지가 표시되면 다음 인수에 대한 값을 입력하거나 매개변수를 사용하여 전달하십시오.
   - Entra ID에 로그인하는 데 사용되는 SSO 이메일 주소
   - StorageGRID의 주소
   - 테넌트 관리 API에 액세스하려는 경우 테넌트 계정 ID
4. 메시지가 나타나면 비밀번호를 입력하고, 요청 시 Entra ID에 대한 다단계 인증(MFA)을 제공할 준비를 하십시오.



> 이 스크립트는 Microsoft Authenticator를 사용한 MFA를 가정합니다. 다른 형태의 MFA(예: 문자 메시지로 받은 코드 입력)를 지원하도록 스크립트를 수정해야 할 수도 있습니다.

StorageGRID 인증 토큰이 출력 결과에 제공됩니다. 이제 SSO를 사용하지 않을 때 API를 사용하는 방법과 유사하게 이 토큰을 다른 요청에 사용할 수 있습니다.

SSO(Single Sign-On)가 활성화된 경우(PingFederate) StorageGRID API를 사용합니다

"싱글 사인온(SSO)을 구성하고 활성화했습니다."가 있고 PingFederate를 SSO 제공업체로 사용하는 경우, 그리드 관리 API 또는 테넌트 관리 API에 유효한 인증 토큰을 얻기 위해 일련의 API 요청을 실행해야 합니다.

싱글 사인온이 활성화된 경우 **API**에 로그인합니다**.**

이 지침은 SSO ID 공급자로 PingFederate를 사용하는 경우에 적용됩니다.

시작하기 전에

- StorageGRID 사용자 그룹에 속한 페더레이션 사용자의 SSO 사용자 이름과 암호를 알고 있습니다.
- 테넌트 관리 API에 액세스하려면 테넌트 계정 ID를 알고 있어야 합니다.

이 작업 정보

인증 토큰을 얻으려면 다음 예시 중 하나를 사용할 수 있습니다.

- 해당 `storagegrid-ssoauth.py` Python 스크립트는 StorageGRID 설치 파일 디렉터리((`./rpms` RHEL, `./debs` Ubuntu 또는 Debian, `./vsphere` VMware)에 있습니다.
- curl 요청의 예시 워크플로입니다.

  curl 워크플로를 너무 느리게 실행하면 시간 초과 오류가 발생할 수 있습니다. 다음과 같은 오류 메시지가 표시될 수 있습니다. `A valid SubjectConfirmation was not found on this Response`.

  > 예시로 제시된 curl 워크플로는 다른 사용자가 비밀번호를 볼 수 없도록 보호하지 않습니다.

  URL 인코딩 문제가 있는 경우 다음과 같은 오류 메시지가 표시될 수 있습니다. `Unsupported SAML version`.

단계

1. 인증 토큰을 얻으려면 다음 방법 중 하나를 선택하십시오.
   - Use the `storagegrid-ssoauth.py` Python 스크립트를 사용합니다. 2단계로 이동합니다.

- curl 요청을 사용합니다. 3단계로 이동합니다.

2. `storagegrid-ssoauth.py` 스크립트를 사용하려면 Python 인터프리터에 스크립트를 전달하고 실행하십시오.

   메시지가 나타나면 다음 인수에 대한 값을 입력하십시오.

   - SSO 방식입니다. "pingfederate"의 어떤 변형이든 입력할 수 있습니다(PINGFEDERATE, pingfederate 등).
   - SSO 사용자 이름
   - StorageGRID가 설치된 도메인입니다. 이 필드는 PingFederate에 사용되지 않습니다. 비워두거나 임의의 값을 입력할 수 있습니다.
   - StorageGRID의 주소
   - 테넌트 관리 API에 액세스하려면 테넌트 계정 ID가 필요합니다.

   ```
   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 인증 토큰이 출력 결과에 제공됩니다. 이제 SSO를 사용하지 않을 때 API를 사용하는 방법과 유사하게 이 토큰을 다른 요청에 사용할 수 있습니다.

3. curl 요청을 사용하려면 다음 절차를 따르십시오.

   a. 로그인에 필요한 변수를 선언합니다.

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

   그리드 관리 API에 액세스하려면 0을 `TENANTACCOUNTID`로 사용하십시오.

   b. 서명된 인증 URL을 받으려면 `/api/v3/authorize-saml`에 POST 요청을 보내고 응답에서 추가 JSON 인코딩을 제거하십시오.

   이 예시는 TENANTACCOUNTID에 대한 서명된 인증 URL을 요청하는 POST 요청을 보여줍니다. 결과는 python -m json.tool에 전달되어 JSON 인코딩이 제거됩니다.

```
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
```

이 예시의 응답에는 URL 인코딩된 서명된 URL이 포함되지만, 추가적인 JSON 인코딩 계층은 포함되지 않습니다.

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

c. 응답에서 `SAMLRequest`을(를) 저장하여 이후 명령에서 사용하십시오.

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

d. 응답과 쿠키를 내보내고 응답을 출력합니다.

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

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

e. 'pf.adapterId' 값을 내보내고 응답을 출력합니다.

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

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

f. 'href' 값을 내보내고(끝에 있는 슬래시(/)를 제거), 응답을 출력합니다.

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

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

g. 'action' 값을 내보냅니다.

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

h. 쿠키를 자격 증명과 함께 전송:

```
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. 숨겨진 필드에서 `SAMLResponse`을(를) 저장합니다.

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

j. 저장된 `SAMLResponse`을 사용하여 StorageGRID `/api/saml-response` 요청을 통해 StorageGRID 인증 토큰을 생성합니다.

`RelayState`의 경우, 테넌트 계정 ID를 사용하거나, 그리드 관리 API에 로그인하려면 0을 사용하십시오.

```
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
```

응답에는 인증 토큰이 포함되어 있습니다.

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

a. 응답에 포함된 인증 토큰을 `MYTOKEN`으로 저장합니다.

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

이제 `MYTOKEN`를 SSO를 사용하지 않을 때 API를 사용하는 방식과 유사하게 다른 요청에도 사용할 수 있습니다.

싱글 사인온(SSO)이 활성화된 경우 API에서 로그아웃

싱글 사인온(SSO)이 활성화된 경우, 그리드 관리 API 또는 테넌트 관리 API에서 로그아웃하려면 일련의 API 요청을 실행해야 합니다. 이 지침은 PingFederate를 SSO ID 공급자로 사용하는 경우에 적용됩니다.

이 작업 정보

필요한 경우 조직의 단일 로그아웃 페이지에서 로그아웃하여 StorageGRID API에서 로그아웃할 수 있습니다. 또는 유효한 StorageGRID 베어러 토큰이 필요한 StorageGRID에서 단일 로그아웃(SLO)을 트리거할 수도 있습니다.

단계

1. 서명된 로그아웃 요청을 생성하려면 SLO API에 `cookie "sso=true"`를 전달하세요.

```
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
```

로그아웃 URL이 반환됩니다.

```
{
    "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. 로그아웃 URL을 저장합니다.

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

3. SLO를 트리거하고 StorageGRID로 다시 리디렉션하려면 로그아웃 URL에 요청을 보내십시오.

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

302 응답이 반환됩니다. 리디렉션 위치는 API 전용 로그아웃에는 적용되지 않습니다.

```
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 베어러 토큰을 삭제합니다.

StorageGRID 베어러 토큰 삭제는 SSO를 사용하지 않을 때와 동일한 방식으로 작동합니다. 쿠키 `"sso=true"`가 제공되지 않으면 SSO 상태에 영향을 주지 않고 사용자가 StorageGRID에서 로그아웃됩니다.

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

A `204 No Content` 응답은 사용자가 로그아웃되었음을 나타냅니다.

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