



Verwenden Sie die API, wenn Single Sign-On aktiviert ist

StorageGRID 11.7

NetApp
April 12, 2024

Inhalt

- Verwenden Sie die API, wenn Single Sign-On aktiviert ist. 1
- Verwenden Sie die API, wenn Single Sign-On aktiviert ist (Active Directory). 1
- Verwenden der API bei Aktivierung der Single Sign-On (Azure) 8
- Verwenden Sie die API, wenn Single Sign-On aktiviert ist (PingFederate) 9

Verwenden Sie die API, wenn Single Sign-On aktiviert ist

Verwenden Sie die API, wenn Single Sign-On aktiviert ist (Active Directory).

Wenn Sie haben "[Konfiguration und Aktivierung von Single Sign On \(SSO\)](#)" Wenn Sie Active Directory als SSO-Provider verwenden, müssen Sie eine Reihe von API-Anforderungen ausstellen, um ein Authentifizierungs-Token zu erhalten, das für die Grid-Management-API oder die Mandantenmanagement-API gültig ist.

Melden Sie sich bei der API an, wenn Single Sign-On aktiviert ist

Diese Anweisungen gelten, wenn Sie Active Directory als SSO-Identitäts-Provider verwenden.

Bevor Sie beginnen

- Sie kennen den SSO-Benutzernamen und das Passwort für einen föderierten Benutzer, der einer StorageGRID-Benutzergruppe angehört.
- Wenn Sie auf die Mandanten-Management-API zugreifen möchten, kennen Sie die Mandanten-Account-ID.

Über diese Aufgabe

Um ein Authentifizierungs-Token zu erhalten, können Sie eines der folgenden Beispiele verwenden:

- Der `storagegrid-ssoauth.py` Python-Skript, das sich im Verzeichnis der Installationsdateien von StorageGRID befindet (`./rpms` Für Red hat Enterprise Linux oder CentOS, `./debs` Für Ubuntu oder Debian, und `./vsphere` Für VMware).
- Ein Beispielworkflow von Curl-Anforderungen.

Der Curl-Workflow kann sich aushalten, wenn Sie ihn zu langsam ausführen. Möglicherweise wird der Fehler angezeigt: `A valid SubjectConfirmation was not found on this Response.`



Der Beispiel-Curl-Workflow schützt das Passwort nicht vor der Sicht anderer Benutzer.

Falls Sie ein Problem mit der URL-Codierung haben, wird möglicherweise der Fehler angezeigt: `Unsupported SAML version.`

Schritte

1. Wählen Sie eine der folgenden Methoden aus, um ein Authentifizierungs-Token zu erhalten:
 - Verwenden Sie die `storagegrid-ssoauth.py` Python-Skript Fahren Sie mit Schritt 2 fort.
 - Verwenden Sie Curl-Anforderungen. Fahren Sie mit Schritt 3 fort.
2. Wenn Sie den verwenden möchten `storagegrid-ssoauth.py` Skript, übergeben Sie das Skript an den Python-Interpreter und führen Sie das Skript aus.

Geben Sie bei der entsprechenden Aufforderung Werte für die folgenden Argumente ein:

- Die SSO-Methode. Geben Sie ADFS oder adfs ein.
- Der SSO-Benutzername
- Die Domäne, in der StorageGRID installiert ist
- Die Adresse für StorageGRID
- Die Mandantenkonto-ID, wenn Sie auf die Mandantenmanagement-API zugreifen möchten.

```
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
```

Das StorageGRID-Autorisierungs-Token wird in der Ausgabe bereitgestellt. Sie können das Token jetzt auch für andere Anforderungen verwenden. Dies entspricht der Verwendung der API, wenn SSO nicht verwendet wurde.

3. Wenn Sie Curl-Anforderungen verwenden möchten, gehen Sie wie folgt vor.
 - a. Deklarieren der Variablen, die für die Anmeldung erforderlich sind.

```
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'
```



Um auf die Grid Management API zuzugreifen, verwenden Sie 0 als TENANTACCOUNTID.

- b. Um eine signierte Authentifizierungs-URL zu erhalten, senden Sie eine POST-Anfrage an /api/v3/authorize-saml, und entfernen Sie die zusätzliche JSON-Kodierung aus der Antwort.

Dieses Beispiel zeigt eine POST-Anforderung für eine signierte Authentifizierungs-URL für TENANTACCOUNTID. Die Ergebnisse werden an weitergeleitet `python -m json.tool` Um die JSON-Kodierung zu entfernen.

```
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
```

Die Antwort für dieses Beispiel enthält eine signierte URL, die URL-codiert ist, aber nicht die zusätzliche JSON-Kodierungsschicht enthält.

```
{
  "apiVersion": "3.0",
  "data":
  "https://ads.example.com/ads/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...
  sS1%2BfQ33cvfwA%3D&RelayState=12345",
  "responseTime": "2018-11-06T16:30:23.355Z",
  "status": "success"
}
```

c. Speichern Sie die `SAMLRequest` Aus der Antwort zur Verwendung in nachfolgenden Befehlen.

```
export SAMLREQUEST='fZHLbsIwEEV%2FJTuv7...sS1%2BfQ33cvfwA%3D'
```

d. Rufen Sie eine vollständige URL ab, die die Client-Anforderungs-ID aus AD FS enthält.

Eine Möglichkeit besteht darin, das Anmeldeformular über die URL der vorherigen Antwort anzufordern.

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

Die Antwort umfasst die Client-Anforderungs-ID:

```
<form method="post" id="loginForm" autocomplete="off"
novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13)
Login.submitLoginRequest();" action="/ads/ls/?
SAMLRequest=fZHRToMwFIZfhh...UJikvo77sXPw%3D%3D&RelayState=12345&clie
nt-request-id=00000000-0000-0000-ee02-0080000000de" >
```

e. Speichern Sie die Client-Anforderungs-ID aus der Antwort.

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

f. Senden Sie Ihre Zugangsdaten an die Formularaktion aus der vorherigen Antwort.

```
curl -X POST "https://$AD_FS_ADDRESS  
/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client  
-request-id=$SAMLREQUESTID" \  
--data "UserName=$SAMLUSER@$SAMLDOMAIN&Password=  
$SAMPLPASSWORD&AuthMethod=FormsAuthentication" --include
```

AD FS gibt eine Umleitung 302 mit zusätzlichen Informationen in den Kopfzeilen zurück.



Wenn Multi-Faktor-Authentifizierung (MFA) für Ihr SSO-System aktiviert ist, enthält der Formularpost auch das zweite Passwort oder andere Anmeldedaten.

```
HTTP/1.1 302 Found  
Content-Length: 0  
Content-Type: text/html; charset=utf-8  
Location:  
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRT0MwFIZfhh...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. Speichern Sie die MSISAuth Cookie aus der Antwort.

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

h. Senden Sie eine GET-Anfrage an den angegebenen Ort mit den Cookies aus dem AUTHENTIFIZIERUNGPOST.

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

Die Antwortheader enthalten AD FS-Sitzungsdaten für die spätere Abmeldung, und der Antwortkörper enthält die SAMLResponse in einem verborgenen Formularfeld.


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

- a. Speichern Sie das Authentifizierungs-Token in der Antwort als `MYTOKEN`.

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

Jetzt können Sie verwenden `MYTOKEN` Für andere Anfragen, ähnlich wie Sie die API verwenden würden, wenn SSO nicht verwendet wurde.

Melden Sie sich von der API ab, wenn Single Sign-On aktiviert ist

Wenn Single Sign-On (SSO) aktiviert ist, müssen Sie eine Reihe von API-Anforderungen zum Abzeichnen der Grid Management API oder der Mandantenmanagement-API ausstellen. Diese Anweisungen gelten, wenn Sie Active Directory als SSO-Identitäts-Provider verwenden

Über diese Aufgabe

Falls erforderlich, können Sie sich von der StorageGRID-API abmelden, indem Sie sich von der einzelnen Abmeldeseite Ihres Unternehmens abmelden. Alternativ können Sie einzelne Abmeldungen (SLO) von StorageGRID auslösen, was ein gültiges StorageGRID-Überträger-Token erfordert.

Schritte

1. Um eine signierte Abmeldeanforderung zu erstellen, übergeben `cookie "sso=true"` Zur 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
```

Es wird eine Abmeldung-URL zurückgegeben:


```
{
  "apiVersion": "3.0",
  "data":
  "https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",
  "responseTime": "2018-11-20T22:20:30.839Z",
  "status": "success"
}
```

2. Speichern Sie die Abmeldung-URL.

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

3. Senden Sie eine Anfrage an die Logout-URL, um SLO auszulösen und zu StorageGRID zurückzukehren.

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

Die Antwort 302 wird zurückgegeben. Der Umleitungsort gilt nicht für die nur-API-Abmeldung.

```
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. Löschen Sie das StorageGRID-Überträger-Token.

Das Löschen des StorageGRID-Inhabertoken funktioniert auf die gleiche Weise wie ohne SSO. Wenn cookie "sso=true" Wird nicht angegeben, wird der Benutzer von StorageGRID abgemeldet, ohne dass der SSO-Status beeinträchtigt wird.

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

A 204 No Content Die Antwort zeigt an, dass der Benutzer jetzt abgemeldet ist.

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

Verwenden der API bei Aktivierung der Single Sign-On (Azure)

Wenn Sie haben "[Konfiguration und Aktivierung von Single Sign On \(SSO\)](#)" Und Sie verwenden Azure als SSO-Provider. Mit zwei Beispielskripten können Sie ein für die Grid-Management-API oder die Mandanten-Management-API gültiges Authentifizierungs-Token anfordern.

Melden Sie sich bei der API an, wenn die Single-Sign-On-Funktion von Azure aktiviert ist

Diese Anweisungen gelten, wenn Sie Azure als SSO-Identitäts-Provider verwenden

Bevor Sie beginnen

- Sie kennen die SSO E-Mail-Adresse und das Passwort für einen föderierten Benutzer, der zu einer StorageGRID Benutzergruppe gehört.
- Wenn Sie auf die Mandanten-Management-API zugreifen möchten, kennen Sie die Mandanten-Account-ID.

Über diese Aufgabe

Um ein Authentifizierungs-Token zu erhalten, können Sie die folgenden Beispielskripte verwenden:

- Der `storagegrid-ssoauth-azure.py` Python-Skript
- Der `storagegrid-ssoauth-azure.js` Node.js-Skript

Beide Skripte befinden sich im Verzeichnis der StorageGRID Installationsdateien (`./rpms` Für Red hat Enterprise Linux oder CentOS, `./debs` Für Ubuntu oder Debian, und `./vsphere` Für VMware).

Informationen zum Schreiben Ihrer eigenen API-Integration in Azure finden Sie im `storagegrid-ssoauth-azure.py` Skript: Das Python-Skript stellt zwei Anfragen direkt an StorageGRID (zuerst um die SAMLRequest zu erhalten, und später um das Autorisierungs-Token zu erhalten) und ruft auch das Node.js-Skript auf, um mit Azure zu interagieren, um die SSO-Operationen durchzuführen.

SSO-Vorgänge können mit einer Reihe von API-Anfragen ausgeführt werden, allerdings ist dies relativ unkompliziert. Das Puppeteer Node.js-Modul wird verwendet, um die Azure SSO-Schnittstelle zu kratzen.

Falls Sie ein Problem mit der URL-Codierung haben, wird möglicherweise der Fehler angezeigt:
`Unsupported SAML version.`

Schritte

1. Installieren Sie die erforderlichen Abhängigkeiten:
 - a. Installieren Sie Node.js (siehe "<https://nodejs.org/en/download/>").
 - b. Installieren Sie die erforderlichen Node.js-Module (Puppenspieler und jsdom):

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

2. Übergeben Sie das Python-Skript an den Python-Interpreter, um das Skript auszuführen.

Das Python-Skript wird dann das entsprechende Node.js-Skript aufrufen, um die Azure SSO-Interaktionen

durchzuführen.

3. Geben Sie bei Aufforderung Werte für die folgenden Argumente ein (oder geben Sie diese mit Hilfe von Parametern weiter):
 - Die SSO-E-Mail-Adresse, mit der Sie sich bei Azure anmelden können
 - Die Adresse für StorageGRID
 - Die Mandantenkonto-ID, wenn Sie auf die Mandantenmanagement-API zugreifen möchten
4. Geben Sie bei der entsprechenden Aufforderung das Passwort ein und bereiten Sie sich darauf vor, auf Wunsch Azure eine MFA-Autorisierung zur Verfügung zu stellen.

```
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'}
```



Das Skript geht davon aus, dass MFA mithilfe von Microsoft Authenticator ausgeführt wird. Möglicherweise müssen Sie das Skript ändern, um andere Formen von MFA zu unterstützen (z. B. die Eingabe eines Codes, der in einer Textnachricht empfangen wird).

Das StorageGRID-Autorisierungs-Token wird in der Ausgabe bereitgestellt. Sie können das Token jetzt auch für andere Anforderungen verwenden. Dies entspricht der Verwendung der API, wenn SSO nicht verwendet wurde.

Verwenden Sie die API, wenn Single Sign-On aktiviert ist (PingFederate)

Wenn Sie haben "[Konfiguration und Aktivierung von Single Sign On \(SSO\)](#)" Und Sie verwenden PingFederate als SSO-Provider. Um ein Authentifizierungs-Token zu erhalten, das für die Grid Management API oder die Mandantenmanagement-API gültig ist, müssen Sie eine Reihe von API-Anforderungen ausgeben.

Melden Sie sich bei der API an, wenn Single Sign-On aktiviert ist

Diese Anweisungen gelten, wenn Sie PingFederate als SSO-Identitäts-Provider verwenden

Bevor Sie beginnen

- Sie kennen den SSO-Benutzernamen und das Passwort für einen föderierten Benutzer, der einer StorageGRID-Benutzergruppe angehört.
- Wenn Sie auf die Mandanten-Management-API zugreifen möchten, kennen Sie die Mandanten-Account-ID.

Über diese Aufgabe

Um ein Authentifizierungs-Token zu erhalten, können Sie eines der folgenden Beispiele verwenden:

- Der `storagegrid-ssoauth.py` Python-Skript, das sich im Verzeichnis der Installationsdateien von StorageGRID befindet (`./rpms` Für Red hat Enterprise Linux oder CentOS, `./debs` Für Ubuntu oder

Debian, und ./vsphere Für VMware).

- Ein Beispielworkflow von Curl-Anforderungen.

Der Curl-Workflow kann sich aushalten, wenn Sie ihn zu langsam ausführen. Möglicherweise wird der Fehler angezeigt: A valid SubjectConfirmation was not found on this Response.



Der Beispiel-Curl-Workflow schützt das Passwort nicht vor der Sicht anderer Benutzer.

Falls Sie ein Problem mit der URL-Codierung haben, wird möglicherweise der Fehler angezeigt: Unsupported SAML version.

Schritte

1. Wählen Sie eine der folgenden Methoden aus, um ein Authentifizierungs-Token zu erhalten:
 - Verwenden Sie die `storagegrid-ssoauth.py` Python-Skript Fahren Sie mit Schritt 2 fort.
 - Verwenden Sie Curl-Anforderungen. Fahren Sie mit Schritt 3 fort.
2. Wenn Sie den verwenden möchten `storagegrid-ssoauth.py` Skript, übergeben Sie das Skript an den Python-Interpreter und führen Sie das Skript aus.

Geben Sie bei der entsprechenden Aufforderung Werte für die folgenden Argumente ein:

- Die SSO-Methode. Sie können eine beliebige Variante von „pingfederate“ (PINGFEDERATE, pingfederate usw.) eingeben.
- Der SSO-Benutzername
- Die Domäne, in der StorageGRID installiert ist. Dieses Feld wird nicht für PingFederate verwendet. Sie können es leer lassen oder einen beliebigen Wert eingeben.
- Die Adresse für StorageGRID
- Die Mandantenkonto-ID, wenn Sie auf die Mandantenmanagement-API zugreifen möchten.

```
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
```

Das StorageGRID-Autorisierungs-Token wird in der Ausgabe bereitgestellt. Sie können das Token jetzt auch für andere Anforderungen verwenden. Dies entspricht der Verwendung der API, wenn SSO nicht verwendet wurde.

3. Wenn Sie Curl-Anforderungen verwenden möchten, gehen Sie wie folgt vor.
 - a. Deklarieren der Variablen, die für die Anmeldung erforderlich sind.

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



Um auf die Grid Management API zuzugreifen, verwenden Sie 0 als TENANTACCOUNTID.

- b. Um eine signierte Authentifizierungs-URL zu erhalten, senden Sie eine POST-Anfrage an `/api/v3/authorize-saml`, und entfernen Sie die zusätzliche JSON-Kodierung aus der Antwort.

Dieses Beispiel zeigt eine POST-Anforderung für eine signierte Authentifizierungs-URL für TENANTACCOUNTID. Die Ergebnisse werden an Python `-m json.tool` übergeben, um die JSON-Codierung zu entfernen.

```
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
```

Die Antwort für dieses Beispiel enthält eine signierte URL, die URL-codiert ist, aber nicht die zusätzliche JSON-Kodierungsschicht enthält.

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

- c. Speichern Sie die `SAMLRequest` aus der Antwort zur Verwendung in nachfolgenden Befehlen.

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

- d. Exportieren Sie die Antwort und das Cookie, und wiederholen Sie die Antwort:

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

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

e. Exportieren Sie den Wert „pf.adaptterId“, und geben Sie die Antwort ein:

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

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

f. Exportieren Sie den 'href'-Wert (entfernen Sie den hinteren Schrägstrich /), und wiederholen Sie die Antwort:

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

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

g. Den Wert „Aktion“ exportieren:

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

h. Senden von Cookies zusammen mit den Zugangsdaten:

```
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. Speichern Sie die SAMLResponse Aus dem ausgeblendeten Feld:

```
export SAMLResponse='PHNhbWxwOlJlc3Bvb2N...1scDpSZXNwb25zZT4='
```

j. Verwenden des gespeicherten SAMLResponse, Erstellen Sie eine StorageGRID/api/saml-response Anforderung zum Generieren eines StorageGRID-Authentifizierungs-Tokens

Für RelayState, Verwenden Sie die Mandanten-Konto-ID oder verwenden Sie 0, wenn Sie sich bei der Grid Management-API anmelden möchten.

```
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
```

Die Antwort umfasst das Authentifizierungs-Token.

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

a. Speichern Sie das Authentifizierungs-Token in der Antwort als MYTOKEN.

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

Jetzt können Sie verwenden MYTOKEN Für andere Anfragen, ähnlich wie Sie die API verwenden würden, wenn SSO nicht verwendet wurde.

Melden Sie sich von der API ab, wenn Single Sign-On aktiviert ist

Wenn Single Sign-On (SSO) aktiviert ist, müssen Sie eine Reihe von API-Anforderungen zum Abzeichnen der Grid Management API oder der Mandantenmanagement-API ausstellen. Diese Anweisungen gelten, wenn Sie PingFederate als SSO-Identitäts-Provider verwenden

Über diese Aufgabe

Falls erforderlich, können Sie sich von der StorageGRID-API abmelden, indem Sie sich von der einzelnen Abmeldeseite Ihres Unternehmens abmelden. Alternativ können Sie einzelne Abmeldungen (SLO) von StorageGRID auslösen, was ein gültiges StorageGRID-Überträger-Token erfordert.

Schritte

1. Um eine signierte Abmeldeanforderung zu erstellen, übergeben `cookie "sso=true"` Zur 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
```

Es wird eine Abmeldung-URL zurückgegeben:

```
{
  "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. Speichern Sie die Abmeldung-URL.

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

3. Senden Sie eine Anfrage an die Logout-URL, um SLO auszulösen und zu StorageGRID zurückzukehren.

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

Die Antwort 302 wird zurückgegeben. Der Umleitungsort gilt nicht für die nur-API-Abmeldung.

```
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. Löschen Sie das StorageGRID-Überträger-Token.

Das Löschen des StorageGRID-Inhabertoken funktioniert auf die gleiche Weise wie ohne SSO. Wenn cookie "sso=true" Wird nicht angegeben, wird der Benutzer von StorageGRID abgemeldet, ohne dass der SSO-Status beeinträchtigt wird.

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

A 204 No Content Die Antwort zeigt an, dass der Benutzer jetzt abgemeldet ist.

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


Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.