



Utiliser l'API si l'authentification unique est activée

StorageGRID software

NetApp
December 03, 2025

Sommaire

- Utiliser l'API si l'authentification unique est activée 1
 - Utiliser l'API si l'authentification unique est activée (Active Directory)..... 1
 - Sign in à l'API si l'authentification unique est activée 1
 - Déconnectez-vous de l'API si l'authentification unique est activée 6
 - Utiliser l'API si l'authentification unique est activée (Azure)..... 8
 - Sign in à l'API si l'authentification unique Azure est activée 8
 - Utiliser l'API si l'authentification unique est activée (PingFederate) 9
 - Sign in à l'API si l'authentification unique est activée 9
 - Déconnectez-vous de l'API si l'authentification unique est activée 13

Utiliser l'API si l'authentification unique est activée

Utiliser l'API si l'authentification unique est activée (Active Directory)

Si vous avez "configuré et activé l'authentification unique (SSO)" et que vous utilisez Active Directory comme fournisseur SSO, vous devez émettre une série de requêtes API pour obtenir un jeton d'authentification valide pour l'API Grid Management ou l'API Tenant Management.

Sign in à l'API si l'authentification unique est activée

Ces instructions s'appliquent si vous utilisez Active Directory comme fournisseur d'identité SSO.

Avant de commencer

- Vous connaissez le nom d'utilisateur et le mot de passe SSO d'un utilisateur fédéré qui appartient à un groupe d'utilisateurs StorageGRID .
- Si vous souhaitez accéder à l'API de gestion des locataires, vous connaissez l'ID du compte locataire.

À propos de cette tâche

Pour obtenir un jeton d'authentification, vous pouvez utiliser l'un des exemples suivants :

- Le `storagegrid-ssoauth.py` Script Python, situé dans le répertoire des fichiers d'installation de StorageGRID(`./rpms` pour Red Hat Enterprise Linux, `./debs` pour Ubuntu ou Debian, et `./vsphere` pour VMware).
- Un exemple de flux de travail de requêtes curl.

Le flux de travail curl peut expirer si vous l'exécutez trop lentement. Vous pourriez voir l'erreur : `A valid SubjectConfirmation was not found on this Response.`



L'exemple de workflow curl ne protège pas le mot de passe contre toute visualisation par d'autres utilisateurs.

Si vous avez un problème d'encodage d'URL, vous pourriez voir l'erreur : `Unsupported SAML version.`

Étapes

1. Sélectionnez l'une des méthodes suivantes pour obtenir un jeton d'authentification :
 - Utilisez le `storagegrid-ssoauth.py` Script Python. Passez à l'étape 2.
 - Utilisez les requêtes curl. Passez à l'étape 3.
2. Si vous souhaitez utiliser le `storagegrid-ssoauth.py` script, transmettez le script à l'interpréteur Python et exécutez le script.

Lorsque vous y êtes invité, saisissez des valeurs pour les arguments suivants :

- La méthode SSO. Entrez ADFS ou adfs.

- Le nom d'utilisateur SSO
- Le domaine où StorageGRID est installé
- L'adresse de StorageGRID
- L'ID du compte locataire, si vous souhaitez accéder à l'API de gestion des locataires.

```
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
```

Le jeton d'autorisation StorageGRID est fourni dans la sortie. Vous pouvez désormais utiliser le jeton pour d'autres requêtes, de la même manière que vous utiliseriez l'API si SSO n'était pas utilisé.

3. Si vous souhaitez utiliser des requêtes curl, utilisez la procédure suivante.

a. Déclarez les variables nécessaires à la connexion.

```
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'
```



Pour accéder à l'API de gestion de grille, utilisez 0 comme TENANTACCOUNTID.

b. Pour recevoir une URL d'authentification signée, émettez une requête POST à `/api/v3/authorize-saml` et supprimez l'encodage JSON supplémentaire de la réponse.

Cet exemple montre une requête POST pour une URL d'authentification signée pour TENANTACCOUNTID. Les résultats seront transmis à `python -m json.tool` pour supprimer l'encodage JSON.

```
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
```

La réponse pour cet exemple inclut une URL signée qui est codée en URL, mais elle n'inclut pas la

couche de codage JSON supplémentaire.

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

c. Sauver le SAMLRequest à partir de la réponse à utiliser dans les commandes suivantes.

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

d. Obtenez une URL complète qui inclut l'ID de demande client d'AD FS.

Une option consiste à demander le formulaire de connexion en utilisant l'URL de la réponse précédente.

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

La réponse inclut l'ID de la demande du client :

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

e. Enregistrez l'ID de demande du client à partir de la réponse.

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

f. Envoyez vos informations d'identification à l'action du formulaire de la réponse précédente.

```
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 renvoie une redirection 302, avec des informations supplémentaires dans les en-têtes.



Si l'authentification multifacteur (MFA) est activée pour votre système SSO, le formulaire de publication contiendra également le deuxième mot de passe ou d'autres informations d'identification.

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRToMwFIZfhh...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. Sauver le MSISAuth cookie de la réponse.

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

h. Envoyez une requête GET à l'emplacement spécifié avec les cookies du POST d'authentification.

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

Les en-têtes de réponse contiendront des informations de session AD FS pour une utilisation ultérieure lors de la déconnexion, et le corps de la réponse contient la réponse SAML dans un champ de formulaire masqué.

```

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=a3dpbnRlcnMtUHJpbWYyeS1BZG1pbi0xNzgmRmFsc2Umcng4NnJDZmFKV
XfXVWx3bk1lMnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LTNmMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjoxMjoxOVpcMQ==;
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="PHNhbWxwOlJlc3Bvb3N...1scDpSZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />

```

- i. Sauver le SAMLResponse du champ caché :

```
export SAMLResponse='PHNhbWxwOlJlc3Bvb3N...1scDpSZXNwb25zZT4='
```

- j. Utilisation de la sauvegarde SAMLResponse , créer un StorageGRID/api/saml-response demande de génération d'un jeton d'authentification StorageGRID .

Pour RelayState , utilisez l'ID de compte locataire ou utilisez 0 si vous souhaitez vous connecter à l'API Grid Management.

```

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

```

La réponse inclut le jeton d'authentification.

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

- a. Enregistrez le jeton d'authentification dans la réponse sous MYTOKEN .

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

Vous pouvez désormais utiliser MYTOKEN pour d'autres demandes, de la même manière que vous utiliseriez l'API si SSO n'était pas utilisé.

Déconnectez-vous de l'API si l'authentification unique est activée

Si l'authentification unique (SSO) a été activée, vous devez émettre une série de requêtes API pour vous déconnecter de l'API Grid Management ou de l'API Tenant Management. Ces instructions s'appliquent si vous utilisez Active Directory comme fournisseur d'identité SSO

À propos de cette tâche

Si nécessaire, vous pouvez vous déconnecter de l'API StorageGRID en vous déconnectant de la page de déconnexion unique de votre organisation. Vous pouvez également déclencher une déconnexion unique (SLO) à partir de StorageGRID, ce qui nécessite un jeton porteur StorageGRID valide.

Étapes

1. Pour générer une demande de déconnexion signée, transmettez `cookie "sso=true"` à l'API SLO :

```
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
```

Une URL de déconnexion est renvoyée :


```
{
  "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. Enregistrez l'URL de déconnexion.

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

3. Envoyez une demande à l'URL de déconnexion pour déclencher SLO et rediriger vers StorageGRID.

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

La réponse 302 est renvoyée. L'emplacement de redirection ne s'applique pas à la déconnexion de l'API uniquement.

```
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. Supprimez le jeton porteur StorageGRID .

La suppression du jeton porteur StorageGRID fonctionne de la même manière que sans SSO. Si `cookie "sso=true" n'est pas fourni, l'utilisateur est déconnecté de StorageGRID sans affecter l'état SSO.

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

UN 204 No Content la réponse indique que l'utilisateur est maintenant déconnecté.

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

Utiliser l'API si l'authentification unique est activée (Azure)

Si vous avez "[configuré et activé l'authentification unique \(SSO\)](#)" et vous utilisez Azure comme fournisseur SSO, vous pouvez utiliser deux exemples de scripts pour obtenir un jeton d'authentification valide pour l'API Grid Management ou l'API Tenant Management.

Sign in à l'API si l'authentification unique Azure est activée

Ces instructions s'appliquent si vous utilisez Azure comme fournisseur d'identité SSO

Avant de commencer

- Vous connaissez l'adresse e-mail et le mot de passe SSO d'un utilisateur fédéré qui appartient à un groupe d'utilisateurs StorageGRID .
- Si vous souhaitez accéder à l'API de gestion des locataires, vous connaissez l'ID du compte locataire.

À propos de cette tâche

Pour obtenir un jeton d'authentification, vous pouvez utiliser les exemples de scripts suivants :

- Le `storagegrid-ssoauth-azure.py` Script Python
- Le `storagegrid-ssoauth-azure.js` Script Node.js

Les deux scripts se trouvent dans le répertoire des fichiers d'installation de StorageGRID(`./rpms` pour Red Hat Enterprise Linux, `./debs` pour Ubuntu ou Debian, et `./vsphere` pour VMware).

Pour écrire votre propre intégration d'API avec Azure, consultez le `storagegrid-ssoauth-azure.py` scénario. Le script Python envoie deux requêtes directement à StorageGRID (d'abord pour obtenir le SAMLRequest, puis pour obtenir le jeton d'autorisation) et appelle également le script Node.js pour interagir avec Azure afin d'effectuer les opérations SSO.

Les opérations SSO peuvent être exécutées à l'aide d'une série de requêtes API, mais cela n'est pas simple. Le module Puppeteer Node.js est utilisé pour récupérer l'interface Azure SSO.

Si vous avez un problème d'encodage d'URL, vous pourriez voir l'erreur : `Unsupported SAML version` .

Étapes

1. Installez les dépendances requises, comme suit :
 - a. Installez Node.js (voir "<https://nodejs.org/en/download/>").
 - b. Installez les modules Node.js requis (puppeteer et jsdom) :

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

2. Transmettez le script Python à l'interpréteur Python pour exécuter le script.

Le script Python appellera ensuite le script Node.js correspondant pour effectuer les interactions Azure SSO.

3. Lorsque vous y êtes invité, saisissez des valeurs pour les arguments suivants (ou transmettez-les à l'aide de paramètres) :
 - L'adresse e-mail SSO utilisée pour se connecter à Azure

- L'adresse de StorageGRID
 - L'ID du compte locataire, si vous souhaitez accéder à l'API de gestion des locataires
4. Lorsque vous y êtes invité, saisissez le mot de passe et soyez prêt à fournir une autorisation MFA à Azure si nécessaire.

```
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'}
```



Le script suppose que l'authentification multifacteur est effectuée à l'aide de Microsoft Authenticator. Vous devrez peut-être modifier le script pour prendre en charge d'autres formes d'authentification multifacteur (comme la saisie d'un code reçu dans un message texte).

Le jeton d'autorisation StorageGRID est fourni dans la sortie. Vous pouvez désormais utiliser le jeton pour d'autres requêtes, de la même manière que vous utiliseriez l'API si SSO n'était pas utilisé.

Utiliser l'API si l'authentification unique est activée (PingFederate)

Si vous avez [configuré et activé l'authentification unique \(SSO\)](#) et que vous utilisez PingFederate comme fournisseur SSO, vous devez émettre une série de requêtes API pour obtenir un jeton d'authentification valide pour l'API de gestion de grille ou l'API de gestion des locataires.

Sign in à l'API si l'authentification unique est activée

Ces instructions s'appliquent si vous utilisez PingFederate comme fournisseur d'identité SSO

Avant de commencer

- Vous connaissez le nom d'utilisateur et le mot de passe SSO d'un utilisateur fédéré qui appartient à un groupe d'utilisateurs StorageGRID .
- Si vous souhaitez accéder à l'API de gestion des locataires, vous connaissez l'ID du compte locataire.

À propos de cette tâche

Pour obtenir un jeton d'authentification, vous pouvez utiliser l'un des exemples suivants :

- Le `storagegrid-ssoauth.py` Script Python, situé dans le répertoire des fichiers d'installation de StorageGRID (`./rpms` pour Red Hat Enterprise Linux, `./debs` pour Ubuntu ou Debian, et `./vsphere` pour VMware).
- Un exemple de flux de travail de requêtes curl.

Le flux de travail curl peut expirer si vous l'exécutez trop lentement. Vous pourriez voir l'erreur : `A valid SubjectConfirmation was not found on this Response`.



L'exemple de workflow curl ne protège pas le mot de passe contre toute visualisation par d'autres utilisateurs.

Si vous avez un problème d'encodage d'URL, vous pourriez voir l'erreur : `Unsupported SAML version`

Étapes

1. Sélectionnez l'une des méthodes suivantes pour obtenir un jeton d'authentification :
 - Utilisez le `storagegrid-ssoauth.py` Script Python. Passez à l'étape 2.
 - Utilisez les requêtes curl. Passez à l'étape 3.
2. Si vous souhaitez utiliser le `storagegrid-ssoauth.py` script, transmettez le script à l'interpréteur Python et exécutez le script.

Lorsque vous y êtes invité, saisissez des valeurs pour les arguments suivants :

- La méthode SSO. Vous pouvez saisir n'importe quelle variante de « pingfederate » (PINGFEDERATE, pingfederate, etc.).
- Le nom d'utilisateur SSO
- Le domaine où StorageGRID est installé. Ce champ n'est pas utilisé pour PingFederate. Vous pouvez le laisser vide ou saisir n'importe quelle valeur.
- L'adresse de StorageGRID
- L'ID du compte locataire, si vous souhaitez accéder à l'API de gestion des locataires.

```
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
```

Le jeton d'autorisation StorageGRID est fourni dans la sortie. Vous pouvez désormais utiliser le jeton pour d'autres requêtes, de la même manière que vous utiliseriez l'API si SSO n'était pas utilisé.

3. Si vous souhaitez utiliser des requêtes curl, utilisez la procédure suivante.

- a. Déclarez les variables nécessaires à la connexion.

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



Pour accéder à l'API de gestion de grille, utilisez 0 comme TENANTACCOUNTID.

- b. Pour recevoir une URL d'authentification signée, émettez une requête POST à `/api/v3/authorize-saml` et supprimez l'encodage JSON supplémentaire de la réponse.

Cet exemple montre une requête POST pour une URL d'authentification signée pour TENANTACCOUNTID. Les résultats seront transmis à `python -m json.tool` pour supprimer l'encodage JSON.

```
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
```

La réponse pour cet exemple inclut une URL signée qui est codée en URL, mais elle n'inclut pas la couche de codage JSON supplémentaire.

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

- c. Sauver le SAMLRequest à partir de la réponse à utiliser dans les commandes suivantes.

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

- d. Exportez la réponse et le cookie, et faites écho à la réponse :

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

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

- e. Exportez la valeur « pf.adapterId » et renvoyez la réponse :

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

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

- f. Exportez la valeur « href » (supprimez la barre oblique /) et affichez la réponse :

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

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

- g. Exporter la valeur « action » :

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

- h. Envoyer des cookies avec les informations d'identification :

```
curl -b <(echo "$RESPONSE") -X POST "$BASEURL$SSOPING" \  
--data "pf.username=$SAMLUSER&pf.pass=  
$SAMPLPASSWORD&pf.ok=clicked&pf.cancel=&pf.adapterId=$ADAPTER"  
--include
```

- i. Sauver le SAMLResponse du champ caché :

```
export SAMLResponse='PHNhbwXwOlJlc3BvbN...1scDpSZXNwb25zZT4='
```

- j. Utilisation de la sauvegarde SAMLResponse , créer un StorageGRID/api/saml-response demande de génération d'un jeton d'authentification StorageGRID .

Pour RelayState , utilisez l'ID de compte locataire ou utilisez 0 si vous souhaitez vous connecter à l'API Grid Management.

```
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
```

La réponse inclut le jeton d'authentification.

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

- a. Enregistrez le jeton d'authentification dans la réponse sous MYTOKEN .

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

Vous pouvez désormais utiliser MYTOKEN pour d'autres demandes, de la même manière que vous utiliseriez l'API si SSO n'était pas utilisé.

Déconnectez-vous de l'API si l'authentification unique est activée

Si l'authentification unique (SSO) a été activée, vous devez émettre une série de requêtes API pour vous déconnecter de l'API Grid Management ou de l'API Tenant Management. Ces instructions s'appliquent si vous utilisez PingFederate comme fournisseur d'identité SSO

À propos de cette tâche

Si nécessaire, vous pouvez vous déconnecter de l'API StorageGRID en vous déconnectant de la page de déconnexion unique de votre organisation. Vous pouvez également déclencher une déconnexion unique (SLO) à partir de StorageGRID, ce qui nécessite un jeton porteur StorageGRID valide.

Étapes

1. Pour générer une demande de déconnexion signée, transmettez `cookie "sso=true" à l'API SLO :

```
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
```

Une URL de déconnexion est renvoyée :

```
{
  "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. Enregistrez l'URL de déconnexion.

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

3. Envoyez une demande à l'URL de déconnexion pour déclencher SLO et rediriger vers StorageGRID.

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

La réponse 302 est renvoyée. L'emplacement de redirection ne s'applique pas à la déconnexion de l'API uniquement.

```
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. Supprimez le jeton porteur StorageGRID .

La suppression du jeton porteur StorageGRID fonctionne de la même manière que sans SSO. Si `cookie "sso=true" n'est pas fourni, l'utilisateur est déconnecté de StorageGRID sans affecter l'état SSO.

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

UN 204 No Content la réponse indique que l'utilisateur est maintenant déconnecté.

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


Informations sur le copyright

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.