Use la API si está activado el inicio de sesión único

StorageGRID 11.7

NetApp
April 12, 2024

Tabla de contenidos

Use la API si está activado el inicio de sesión único

Utilizar la API si está activado el inicio de sesión único (Active Directory)

Si lo tiene "Inicio de sesión único configurado y habilitado (SSO)" Además, se utiliza Active Directory como proveedor SSO, debe emitir una serie de solicitudes API para obtener un token de autenticación válido para la API de administración de grid o la API de administración de inquilinos.

Inicie sesión en la API si está habilitado el inicio de sesión único

Estas instrucciones se aplican si utiliza Active Directory como proveedor de identidades SSO.

Antes de empezar

- Conoce el nombre de usuario y la contraseña de SSO para un usuario federado que pertenece a un grupo de usuarios de StorageGRID.
- Si desea acceder a la API de gestión de inquilinos, conoce el ID de cuenta de inquilino.

Acerca de esta tarea

Para obtener un token de autenticación, puede utilizar uno de los siguientes ejemplos:

- La `storagegrid-ssoauth.py` Script Python, que se encuentra en el directorio de archivos de instalación de StorageGRID (`./rpms` Para Red Hat Enterprise Linux o CentOS, `./debs` Para Ubuntu o Debian, y. `./vsphere` Para VMware).
- Ejemplo de flujo de trabajo de solicitudes curl.

  El flujo de trabajo curl podría llegar a ocurrir si lo hace demasiado lentamente. Es posible que aparezca el error: `A valid SubjectConfirmation was not found on this Response`.

  > ⓘ El flujo de trabajo curl de ejemplo no protege la contraseña de ser vista por otros usuarios.

Si tiene un problema de codificación URL, puede que aparezca el error: `Unsupported SAML version`.

Pasos

1. Seleccione uno de los siguientes métodos para obtener un token de autenticación:
   - Utilice la `storagegrid-ssoauth.py` Guión Python. Vaya al paso 2.
   - Usar solicitudes curl. Vaya al paso 3.
2. Si desea utilizar el `storagegrid-ssoauth.py` Guión, pase el script al intérprete Python y ejecute el script.

   Cuando se le solicite, escriba valores para los siguientes argumentos:

   - El método SSO. Introduzca ADFS o adfs.

- El nombre de usuario de SSO
- El dominio en el que está instalado StorageGRID
- La dirección de StorageGRID
- El ID de cuenta de inquilino, si desea acceder a la API de gestión de inquilinos.

```
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
```

El token de autorización de StorageGRID se proporciona en la salida. Ahora puede utilizar el token para otras solicitudes, de forma similar a cómo utilizaría la API si no se estuviera utilizando SSO.

3. Si desea usar solicitudes curl, use el siguiente procedimiento.

   a. Declare las variables necesarias para iniciar sesión.

```
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'
```

   > Para acceder a la API de gestión de grid, utilice 0 AS `TENANTACCOUNTID`.

   b. Para recibir una URL de autenticación firmada, emita una solicitud DE ENVÍO `/api/v3/authorize-saml`, Y quite la codificación JSON adicional de la respuesta.

   En este ejemplo se muestra una solicitud POST para una dirección URL de autenticación firmada `TENANTACCOUNTID`. Los resultados se pasan a. `python -m json.tool` Para quitar la codificación 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 respuesta de este ejemplo incluye una dirección URL firmada codificada por URL, pero no incluye

la capa de codificación JSON adicional.

```
{
    "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. Guarde la `SAMLRequest` de la respuesta para su uso en comandos posteriores.

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

d. Obtenga una URL completa que incluya el ID de solicitud de cliente de AD FS.

Una opción es solicitar el formulario de inicio de sesión mediante la URL de la respuesta anterior.

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

La respuesta incluye el ID de solicitud del cliente:

```
<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. Guarde el ID de solicitud de cliente de la respuesta.

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

f. Envíe sus credenciales a la acción de formulario de la respuesta anterior.

```
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 devuelve un redireccionamiento 302, con información adicional en los encabezados.

> Si la autenticación multifactor (MFA) está habilitada para el sistema SSO, la entrada del formulario también contendrá la segunda contraseña u otras credenciales.

```
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. Guarde la `MSISAuth` cookie de la respuesta.

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

h. Envíe una solicitud GET a la ubicación especificada con las cookies de LA PUBLICACIÓN de autenticación.

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

Los encabezados de respuesta contendrán información de sesión de AD FS para el uso posterior del cierre de sesión y el cuerpo de respuesta contiene el SAMLResponse en un campo de formulario oculto.

```
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. Guarde la `SAMLResponse` en el campo oculto:

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

j. Utilizando el guardado `SAMLResponse`, Haga un StorageGRID`/api/saml-response` Solicitud para generar un token de autenticación de StorageGRID.

Para `RelayState`, Utilice el ID de cuenta de arrendatario o utilice 0 si desea iniciar sesión en la API de administración de grid.

```
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 respuesta incluye el token de autenticación.

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

a. Guarde el token de autenticación en la respuesta como `MYTOKEN`.

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

Ahora puede utilizar `MYTOKEN` Para otras solicitudes, del mismo modo que utilizaría la API si no se utiliza SSO.

Cierre sesión en la API si el inicio de sesión único está habilitado

Si se ha activado el inicio de sesión único (SSO), debe emitir una serie de solicitudes API para cerrar sesión en la API de gestión de grid o en la API de gestión de inquilinos. Estas instrucciones se aplican si utiliza Active Directory como proveedor de identidades SSO

Acerca de esta tarea

Si es necesario, puede cerrar sesión en la API de StorageGRID cerrando sesión en la página de cierre de sesión único de su organización. O bien, puede activar el cierre de sesión único (SLO) desde StorageGRID, que requiere un token de portador de StorageGRID válido.

Pasos

1. Para generar una solicitud de cierre de sesión firmada, pase `cookie "sso=true"` En la API de 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
```

Se devuelve una URL de cierre de sesión:

```
{
    "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. Guarde la URL de cierre de sesión.

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

3. Envíe una solicitud a la URL de cierre de sesión para activar SLO y redirigir de nuevo a StorageGRID.

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

Se devuelve la respuesta de 302. La ubicación de redirección no se aplica a la salida de sólo API.

```
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. Elimine el token del portador de StorageGRID.

La eliminación del token del portador de StorageGRID funciona de la misma forma que sin SSO. Si `cookie "sso=true"` No proporciona, el usuario cierra la sesión de StorageGRID sin afectar al estado de SSO.

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

1. `204 No Content` la respuesta indica que el usuario ha cerrado la sesión.

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

Use la API si el inicio de sesión único está habilitado (Azure)

Si lo tiene "Inicio de sesión único configurado y habilitado (SSO)" Además, utilice Azure como proveedor SSO, puede utilizar dos scripts de ejemplo para obtener un token de autenticación válido para la API de gestión de grid o la API de gestión de inquilinos.

Inicie sesión en la API si el inicio de sesión único de Azure está habilitado

Estas instrucciones se aplican si utiliza Azure como proveedor de identidades de SSO

Antes de empezar

- Conoce la dirección de correo electrónico y la contraseña de SSO para un usuario federado que pertenece a un grupo de usuarios de StorageGRID.
- Si desea acceder a la API de gestión de inquilinos, conoce el ID de cuenta de inquilino.

Acerca de esta tarea

Para obtener un token de autenticación, puede utilizar las siguientes secuencias de comandos de ejemplo:

- La `storagegrid-ssoauth-azure.py` Guión Python
- La `storagegrid-ssoauth-azure.js` Secuencia de comandos Node.js

Ambos scripts se encuentran en el directorio de archivos de instalación de StorageGRID (`./rpms` Para Red Hat Enterprise Linux o CentOS, `./debs` Para Ubuntu o Debian, y. `./vsphere` Para VMware).

Para escribir su propia integración de API con Azure, consulte `storagegrid-ssoauth-azure.py` guión. El script de Python hace dos solicitudes a StorageGRID directamente (primero para obtener el SAMLRequest, y más tarde para obtener el token de autorización), y también llama al script Node.js para interactuar con Azure para realizar las operaciones de SSO.

Las operaciones SSO se pueden ejecutar mediante una serie de solicitudes API, pero hacerlo no es sencillo. El módulo Puppeteer Node.js se utiliza para raspar la interfaz SSO de Azure.

Si tiene un problema de codificación URL, puede que aparezca el error: `Unsupported SAML version`.

Pasos

1. Instale las dependencias necesarias de la siguiente manera:
   a. Instale Node.js (consulte "https://nodejs.org/en/download/").
   b. Instale los módulos Node.js necesarios (tippeteer y jsdom):

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

2. Pase la secuencia de comandos de Python al intérprete de Python para ejecutar la secuencia de comandos.

   La secuencia de comandos Python llamará al script Node.js correspondiente para realizar las interacciones de SSO de Azure.

3. Cuando se le solicite, introduzca valores para los siguientes argumentos (o bien, pasarlos mediante parámetros):

- La dirección de correo electrónico de SSO que se utiliza para iniciar sesión en Azure
- La dirección de StorageGRID
- El ID de cuenta de inquilino, si desea acceder a la API de gestión de inquilinos

4. Cuando se le solicite, introduzca la contraseña y esté preparado para proporcionar una autorización de MFA para Azure si así se lo solicita.

```
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'}
```

> La secuencia de comandos asume que la MFA se realiza utilizando Microsoft Authenticator. Es posible que necesite modificar el script para admitir otras formas de MFA (como introducir un código recibido en un mensaje de texto).

El token de autorización de StorageGRID se proporciona en la salida. Ahora puede utilizar el token para otras solicitudes, de forma similar a cómo utilizaría la API si no se estuviera utilizando SSO.

Utilizar la API si está activado el inicio de sesión único (PingFederate)

Si lo tiene "Inicio de sesión único configurado y habilitado (SSO)" Además, debe utilizar PingFederate como proveedor SSO, para obtener un token de autenticación válido para la API de gestión de grid o la API de gestión de inquilinos, debe emitir una serie de solicitudes API.

Inicie sesión en la API si está habilitado el inicio de sesión único

Estas instrucciones se aplican si está utilizando PingFederate como proveedor de identidades SSO

Antes de empezar

- Conoce el nombre de usuario y la contraseña de SSO para un usuario federado que pertenece a un grupo de usuarios de StorageGRID.
- Si desea acceder a la API de gestión de inquilinos, conoce el ID de cuenta de inquilino.

Acerca de esta tarea

Para obtener un token de autenticación, puede utilizar uno de los siguientes ejemplos:

- La `storagegrid-ssoauth.py` Script Python, que se encuentra en el directorio de archivos de instalación de StorageGRID (`./rpms` Para Red Hat Enterprise Linux o CentOS, `./debs` Para Ubuntu o Debian, y. `./vsphere` Para VMware).
- Ejemplo de flujo de trabajo de solicitudes curl.

  El flujo de trabajo curl podría llegar a ocurrir si lo hace demasiado lentamente. Es posible que aparezca el error: `A valid SubjectConfirmation was not found on this Response`.

El flujo de trabajo curl de ejemplo no protege la contraseña de ser vista por otros usuarios.

Si tiene un problema de codificación URL, puede que aparezca el error: `Unsupported SAML version`.

Pasos

1. Seleccione uno de los siguientes métodos para obtener un token de autenticación:
   - Utilice la `storagegrid-ssoauth.py` Guión Python. Vaya al paso 2.
   - Usar solicitudes curl. Vaya al paso 3.
2. Si desea utilizar el `storagegrid-ssoauth.py` Guión, pase el script al intérprete Python y ejecute el script.

   Cuando se le solicite, escriba valores para los siguientes argumentos:

   - El método SSO. Puede introducir cualquier variación de "'pingfederate'" (PINGFEDERATE, pingfederate, etc.).
   - El nombre de usuario de SSO
   - El dominio en el que está instalado StorageGRID. Este campo no se utiliza para PingFederate. Puede dejarlo en blanco o introducir cualquier valor.
   - La dirección de StorageGRID
   - El ID de cuenta de inquilino, si desea acceder a la API de gestión de inquilinos.

   ```
   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
   ```

   El token de autorización de StorageGRID se proporciona en la salida. Ahora puede utilizar el token para otras solicitudes, de forma similar a cómo utilizaría la API si no se estuviera utilizando SSO.

3. Si desea usar solicitudes curl, use el siguiente procedimiento.
   a. Declare las variables necesarias para iniciar sesión.

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

   Para acceder a la API de gestión de grid, utilice 0 AS `TENANTACCOUNTID`.

b. Para recibir una URL de autenticación firmada, emita una solicitud DE ENVÍO `/api/v3/authorize-saml`, Y quite la codificación JSON adicional de la respuesta.

   En este ejemplo se muestra una solicitud POST para una dirección URL de autenticación firmada para TENANTACCOUNTID. Los resultados se pasan a python -m json.tool para quitar la codificación 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 respuesta de este ejemplo incluye una dirección URL firmada codificada por URL, pero no incluye la capa de codificación JSON adicional.

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

c. Guarde la `SAMLRequest` de la respuesta para su uso en comandos posteriores.

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

d. Exporte la respuesta y el cookie y añada la respuesta:

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

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

e. Exporte el valor 'pf.adapterId' y añada la respuesta:

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

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

f. Exporte el valor 'href' (retire la barra diagonal inversa /) y añada la respuesta:

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

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

g. Exporte el valor de 'acción':

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

h. Enviar cookies junto con credenciales:

```
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. Guarde la `SAMLResponse` en el campo oculto:

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

j. Utilizando el guardado `SAMLResponse`, Haga un StorageGRID`/api/saml-response` Solicitud para generar un token de autenticación de StorageGRID.

Para `RelayState`, Utilice el ID de cuenta de arrendatario o utilice 0 si desea iniciar sesión en la API de administración de grid.

```
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 respuesta incluye el token de autenticación.

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

a. Guarde el token de autenticación en la respuesta como `MYTOKEN`.

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

Ahora puede utilizar `MYTOKEN` Para otras solicitudes, del mismo modo que utilizaría la API si no se utiliza SSO.

Cierre sesión en la API si el inicio de sesión único está habilitado

Si se ha activado el inicio de sesión único (SSO), debe emitir una serie de solicitudes API para cerrar sesión en la API de gestión de grid o en la API de gestión de inquilinos. Estas instrucciones se aplican si está utilizando PingFederate como proveedor de identidades SSO

Acerca de esta tarea

Si es necesario, puede cerrar sesión en la API de StorageGRID cerrando sesión en la página de cierre de sesión único de su organización. O bien, puede activar el cierre de sesión único (SLO) desde StorageGRID, que requiere un token de portador de StorageGRID válido.

Pasos

1. Para generar una solicitud de cierre de sesión firmada, pase `cookie "sso=true"` En la API de 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
```

Se devuelve una URL de cierre de sesión:

```
{
    "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. Guarde la URL de cierre de sesión.

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

3. Envíe una solicitud a la URL de cierre de sesión para activar SLO y redirigir de nuevo a StorageGRID.

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

Se devuelve la respuesta de 302. La ubicación de redirección no se aplica a la salida de sólo API.

```
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. Elimine el token del portador de StorageGRID.

   La eliminación del token del portador de StorageGRID funciona de la misma forma que sin SSO. Si `cookie "sso=true"` No proporciona, el usuario cierra la sesión de StorageGRID sin afectar al estado de SSO.

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

   1. `204 No Content` la respuesta indica que el usuario ha cerrado la sesión.

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