Utilice la API

StorageGRID software

NetApp
December 03, 2025

Tabla de contenidos

Utilice la API

Utilice la API de gestión de red

Puede realizar tareas de administración del sistema utilizando la API REST de administración de cuadrícula en lugar de la interfaz de usuario de Grid Manager. Por ejemplo, es posible que desee utilizar la API para automatizar operaciones o crear múltiples entidades, como usuarios, más rápidamente.

Recursos de alto nivel

La API de administración de red proporciona los siguientes recursos de nivel superior:

- `/grid`:El acceso está restringido a los usuarios de Grid Manager y se basa en los permisos de grupo configurados.
- `/org`:El acceso está restringido a los usuarios que pertenecen a un grupo LDAP local o federado para una cuenta de inquilino. Para obtener más información, consulte "Utilice una cuenta de inquilino" .
- `/private`:El acceso está restringido a los usuarios de Grid Manager y se basa en los permisos de grupo configurados. Las API privadas están sujetas a cambios sin previo aviso. Los puntos finales privados de StorageGRID también ignoran la versión API de la solicitud.

Emitir solicitudes de API

La API de administración de red utiliza la plataforma API de código abierto Swagger. Swagger proporciona una interfaz de usuario intuitiva que permite a los desarrolladores y no desarrolladores realizar operaciones en tiempo real en StorageGRID con la API.

La interfaz de usuario de Swagger proporciona detalles completos y documentación para cada operación de API.

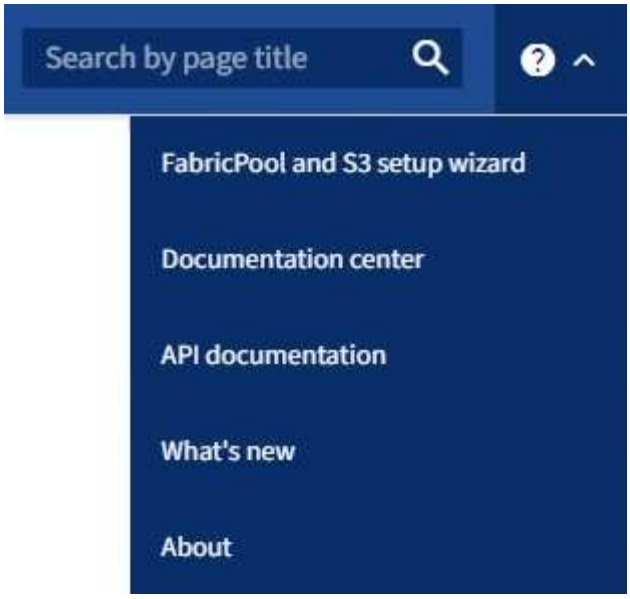
Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un"navegador web compatible" .
- Tienes"permisos de acceso específicos" .

> Cualquier operación de API que realice utilizando la página web de Documentación de API son operaciones en vivo. Tenga cuidado de no crear, actualizar o eliminar datos de configuración u otros datos por error.

Pasos

1. Desde el encabezado de Grid Manager, seleccione el ícono de ayuda y seleccione **Documentación de API**.



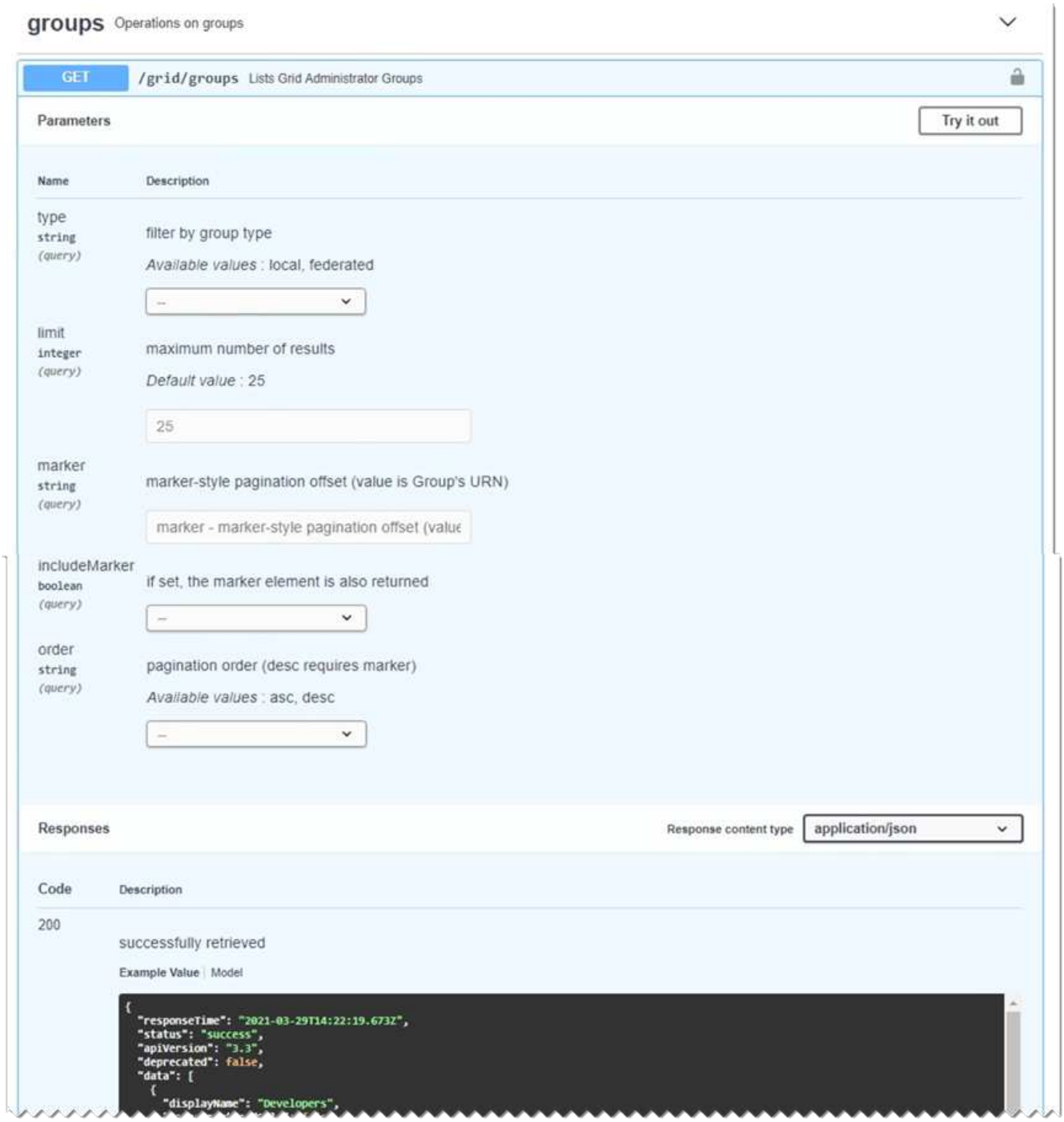
2. Para realizar una operación con la API privada, seleccione **Ir a la documentación de la API privada** en la página API de administración de StorageGRID .

   Las API privadas están sujetas a cambios sin previo aviso. Los puntos finales privados de StorageGRID también ignoran la versión API de la solicitud.

3. Seleccione la operación deseada.

   Cuando expande una operación de API, puede ver las acciones HTTP disponibles, como GET, PUT, UPDATE y DELETE.

4. Seleccione una acción HTTP para ver los detalles de la solicitud, incluida la URL del punto final, una lista de parámetros obligatorios u opcionales, un ejemplo del cuerpo de la solicitud (cuando sea necesario) y las posibles respuestas.



5. Determinar si la solicitud requiere parámetros adicionales, como un ID de grupo o usuario. Luego, obtenga estos valores. Es posible que primero debas emitir una solicitud API diferente para obtener la información que necesitas.
6. Determina si necesitas modificar el cuerpo de la solicitud de ejemplo. Si es así, puede seleccionar **Modelo** para conocer los requisitos de cada campo.
7. Seleccione **Probarlo**.
8. Proporcione los parámetros necesarios o modifique el cuerpo de la solicitud según sea necesario.
9. Seleccione **Ejecutar**.
10. Revise el código de respuesta para determinar si la solicitud fue exitosa.

Operaciones de la API de gestión de red

La API de administración de red organiza las operaciones disponibles en las siguientes secciones.

Esta lista solo incluye operaciones disponibles en la API pública.

- **cuentas**: Operaciones para administrar cuentas de inquilinos de almacenamiento, incluida la creación de nuevas cuentas y la recuperación del uso de almacenamiento para una cuenta determinada.
- **alert-history**: Operaciones sobre alertas resueltas.
- **alert-receivers**: Operaciones sobre receptores de notificaciones de alerta (correo electrónico).
- **alert-rules**: Operaciones sobre reglas de alerta.
- **alert-silences**: Operaciones sobre silencios de alerta.
- **alertas**: Operaciones sobre alertas.
- **audit**: Operaciones para listar y actualizar la configuración de auditoría.
- **auth**: Operaciones para realizar la autenticación de la sesión del usuario.

  La API de administración de red admite el esquema de autenticación de token de portador. Para iniciar sesión, debe proporcionar un nombre de usuario y una contraseña en el cuerpo JSON de la solicitud de autenticación (es decir, `POST /api/v3/authorize`). Si el usuario se autentica correctamente, se devuelve un token de seguridad. Este token debe proporcionarse en el encabezado de las solicitudes de API posteriores ("Autorización: Bearer *token*"). El token caduca después de 16 horas.

  Si el inicio de sesión único está habilitado para el sistema StorageGRID , debe realizar diferentes pasos para autenticarse. Consulte "Autenticación en la API si el inicio de sesión único está habilitado".

  Consulte "Protección contra la falsificación de solicitudes entre sitios" para obtener información sobre cómo mejorar la seguridad de la autenticación.

- **client-certificates**: Operaciones para configurar certificados de cliente para que se pueda acceder a StorageGRID de forma segura mediante herramientas de monitoreo externas.
- **config**: Operaciones relacionadas con el lanzamiento del producto y las versiones de la API de administración de cuadrícula. Puede enumerar la versión de lanzamiento del producto y las versiones principales de la API de administración de cuadrícula compatibles con esa versión, y puede deshabilitar las versiones obsoletas de la API.
- **funciones-desactivadas**: Operaciones para ver funciones que podrían haber sido desactivadas.
- **dns-servers**: Operaciones para listar y cambiar servidores DNS externos configurados.
- **drive-details**: Operaciones en unidades para modelos de dispositivos de almacenamiento específicos.
- **endpoint-domain-names**: Operaciones para enumerar y cambiar los nombres de dominio de los puntos finales de S3.
- **erasure-coding**: Operaciones sobre perfiles de codificación de borrado.
- **expansión**: Operaciones de expansión (nivel de procedimiento).
- **expansion-nodes**: Operaciones de expansión (nivel de nodo).
- **sitios-de-expansión**: Operaciones de expansión (a nivel de sitio).

- **grid-networks**: Operaciones para listar y cambiar la lista de redes de cuadrícula.
- **grid-passwords**: Operaciones para la gestión de contraseñas de la red.
- **grupos**: Operaciones para administrar grupos de administradores de grid locales y para recuperar grupos de administradores de grid federados desde un servidor LDAP externo.
- **identity-source**: Operaciones para configurar una fuente de identidad externa y sincronizar manualmente la información de usuarios y grupos federados.
- **ilm**: Operaciones sobre la gestión del ciclo de vida de la información (ILM).
- **in-progress-procedures**: recupera los procedimientos de mantenimiento que están actualmente en curso.
- **licencia**: Operaciones para recuperar y actualizar la licencia de StorageGRID .
- **logs**: Operaciones para recopilar y descargar archivos de registro.v
- **métricas**: Operaciones sobre métricas de StorageGRID , incluidas consultas de métricas instantáneas en un único punto en el tiempo y consultas de métricas de rango durante un período de tiempo. La API de administración de red utiliza la herramienta de monitoreo de sistemas Prometheus como fuente de datos de back-end. Para obtener información sobre cómo construir consultas de Prometheus, consulte el sitio web de Prometheus.

> Métricas que incluyen`private` en sus nombres están destinados únicamente para uso interno. Estas métricas están sujetas a cambios entre versiones de StorageGRID sin previo aviso.

- **node-details**: Operaciones sobre los detalles del nodo.
- **node-health**: Operaciones sobre el estado de salud del nodo.
- **node-storage-state**: Operaciones sobre el estado de almacenamiento del nodo.
- **ntp-servers**: Operaciones para listar o actualizar servidores externos de Protocolo de tiempo de red (NTP).
- **objetos**: Operaciones sobre objetos y metadatos de objetos.
- **recuperación**: Operaciones para el procedimiento de recuperación.
- **recovery-package**: Operaciones para descargar el paquete de recuperación.
- **regiones**: Operaciones para ver y crear regiones.
- **s3-object-lock**: Operaciones en la configuración global de bloqueo de objetos S3.
- **server-certificate**: Operaciones para ver y actualizar los certificados del servidor de Grid Manager.
- **snmp**: Operaciones en la configuración SNMP actual.
- **storage-watermarks**: Marcas de agua del nodo de almacenamiento.
- **traffic-classes**: Operaciones para políticas de clasificación de tráfico.
- **untrusted-client-network**: Operaciones en la configuración de red de cliente no confiable.
- **usuarios**: Operaciones para ver y administrar usuarios de Grid Manager.

Control de versiones de la API de gestión de red

La API de administración de red utiliza versiones para admitir actualizaciones sin interrupciones.

Por ejemplo, esta URL de solicitud especifica la versión 4 de la API.

`https://hostname_or_ip_address/api/v4/authorize`

La versión principal de la API se actualiza cuando se realizan cambios que *no son compatibles* con versiones anteriores. La versión menor de la API se actualiza cuando se realizan cambios que *son compatibles* con versiones anteriores. Los cambios compatibles incluyen la adición de nuevos puntos finales o nuevas propiedades.

El siguiente ejemplo ilustra cómo se actualiza la versión de la API según el tipo de cambios realizados.

Tipo de cambio en la API	Versión antigua	Nueva versión
Compatible con versiones anteriores	2,1	2,2
No compatible con versiones anteriores	2,1	3,0

Cuando instala el software StorageGRID por primera vez, solo se habilita la versión más reciente de la API. Sin embargo, cuando actualiza a una nueva versión de funciones de StorageGRID, continúa teniendo acceso a la versión anterior de API durante al menos una versión de funciones de StorageGRID .

> Puede configurar las versiones compatibles. Consulte la sección **config** de la documentación de la API de Swagger para obtener más información."API de gestión de red" Para más información. Debe desactivar el soporte para la versión anterior después de actualizar todos los clientes API para usar la versión más nueva.

Las solicitudes obsoletas se marcan como obsoletas de las siguientes maneras:

- El encabezado de respuesta es "Obsoleto: verdadero".
- El cuerpo de la respuesta JSON incluye "deprecated": true
- Se agrega una advertencia obsoleta a nms.log. Por ejemplo:

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

Determinar qué versiones de API son compatibles con la versión actual

Utilice el `GET /versions` Solicitud de API para devolver una lista de las principales versiones de API compatibles. Esta solicitud se encuentra en la sección **config** de la documentación de la API de Swagger.

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

Especificar una versión de API para una solicitud

Puede especificar la versión de la API utilizando un parámetro de ruta(`/api/v4`) o un encabezado(`Api-Version: 4`). Si proporciona ambos valores, el valor del encabezado anula el valor de la ruta.

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

Protección contra la falsificación de solicitudes entre sitios (CSRF)

Puede ayudar a protegerse contra ataques de falsificación de solicitud entre sitios (CSRF) contra StorageGRID mediante el uso de tokens CSRF para mejorar la autenticación que utiliza cookies. El administrador de red y el administrador de inquilinos habilitan automáticamente esta función de seguridad; otros clientes de API pueden elegir si habilitarla cuando inician sesión.

Un atacante que puede activar una solicitud a un sitio diferente (por ejemplo, con un formulario HTTP POST) puede provocar que ciertas solicitudes se realicen utilizando las cookies del usuario que inició sesión.

StorageGRID ayuda a proteger contra ataques CSRF mediante el uso de tokens CSRF. Cuando está habilitada, el contenido de una cookie específica debe coincidir con el contenido de un encabezado específico o de un parámetro de cuerpo POST específico.

Para habilitar la función, configure el `csrfToken` parámetro a `true` durante la autenticación. El valor predeterminado es `false` .

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

Cuando es cierto, una `GridCsrfToken` La cookie se establece con un valor aleatorio para los inicios de sesión en Grid Manager y `AccountCsrfToken` La cookie se establece con un valor aleatorio para los inicios de sesión en el Administrador de inquilinos.

Si la cookie está presente, todas las solicitudes que puedan modificar el estado del sistema (POST, PUT, PATCH, DELETE) deben incluir uno de los siguientes:

- El `X-Csrf-Token` encabezado, con el valor del encabezado establecido en el valor de la cookie del token CSRF.
- Para los puntos finales que aceptan un cuerpo codificado por formulario: A `csrfToken` parámetro del cuerpo de la solicitud codificado en formulario.

Consulte la documentación de la API en línea para obtener ejemplos y detalles adicionales.

> Las solicitudes que tienen una cookie de token CSRF configurada también aplicarán el encabezado "Content-Type: application/json" para cualquier solicitud que espere un cuerpo de solicitud JSON como protección adicional contra ataques CSRF.

Utilice la API si el inicio de sesión único está habilitado

Utilice la API si el inicio de sesión único está habilitado (Active Directory)

Si tienes"Inicio de sesión único (SSO) configurado y habilitado" y utiliza Active Directory como proveedor de SSO, debe emitir una serie de solicitudes de API para obtener un token de autenticación que sea válido para la API de administración de Grid o la API de administración de inquilinos.

Sign in en la API si el inicio de sesión único está habilitado

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

Antes de empezar

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

Acerca de esta tarea

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

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

  El flujo de trabajo curl puede expirar si lo realiza demasiado lento. Es posible que veas el error: `A valid SubjectConfirmation was not found on this Response`.

  > El flujo de trabajo curl de ejemplo no protege la contraseña para que otros usuarios no la vean.

Si tiene un problema de codificación de URL, es posible que vea el error: `Unsupported SAML version`.

Pasos

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

   Cuando se le solicite, ingrese valores para los siguientes argumentos:
   - El método SSO. Introduzca ADFS o adfs.
   - El nombre de usuario de SSO
   - El dominio donde está instalado StorageGRID
   - La dirección de StorageGRID
   - El ID de la cuenta del inquilino, si desea acceder a la API de administración 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 puedes usar el token para otras solicitudes, de manera similar a como usarías la API si no se estuviera utilizando SSO.
3. Si desea utilizar solicitudes curl, utilice 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 administración de red, utilice 0 como `TENANTACCOUNTID` .

b. Para recibir una URL de autenticación firmada, emita una solicitud POST a `/api/v3/authorize-saml` y elimine la codificación JSON adicional de la respuesta.

Este ejemplo muestra una solicitud POST para una URL de autenticación firmada para `TENANTACCOUNTID` . Los resultados se transmitirán a `python -m json.tool` para eliminar 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 para este ejemplo incluye una URL firmada que está codificada como 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. Guardar el `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 del cliente de AD FS.

Una opción es solicitar el formulario de inicio de sesión utilizando 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 la 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 la solicitud del cliente de la respuesta.

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

f. Envía tus credenciales a la acción del 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 una redirección 302, con información adicional en los encabezados.

> Si la autenticación multifactor (MFA) está habilitada para su sistema SSO, la publicación 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. Guardar el `MSISAuth` cookie de la respuesta.

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

h. Envía una solicitud GET a la ubicación especificada con las cookies del POST 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 la sesión de AD FS para su uso posterior al cerrar sesión, y el cuerpo de la respuesta contiene 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. Guardar el `SAMLResponse` del campo oculto:

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

j. Usando lo guardado `SAMLResponse` , crear un StorageGRID`/api/saml-response` solicitud para

generar un token de autenticación de StorageGRID .

Para `RelayState` , use el ID de la cuenta del inquilino o use 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"
```

Ya puedes utilizar `MYTOKEN` para otras solicitudes, de forma similar a como usarías la API si no se estuviera utilizando SSO.

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

Si se ha habilitado el inicio de sesión único (SSO), debe emitir una serie de solicitudes de API para cerrar sesión en la API de administración de red o en la API de administración de inquilinos. Estas instrucciones se aplican si está utilizando Active Directory como proveedor de identidad SSO

Acerca de esta tarea

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

Pasos

1. Para generar una solicitud de cierre de sesión firmada, pase `cookie "sso=true" a 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. Guardar 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 nuevamente a StorageGRID.

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

Se devuelve la respuesta 302. La ubicación de redireccionamiento no es aplicable al cierre de sesión exclusivo de 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. Eliminar el token portador de StorageGRID .

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

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

A `204 No Content` La respuesta indica que el usuario ahora ha cerrado la sesión.

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

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

Si tienes"Inicio de sesión único (SSO) configurado y habilitado" y usa Azure como proveedor de SSO, puede usar dos scripts de ejemplo para obtener un token de autenticación que sea válido para la API de administración de red o la API de administración de inquilinos.

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

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

Antes de empezar

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

Acerca de esta tarea

Para obtener un token de autenticación, puede utilizar los siguientes scripts de ejemplo:

- El `storagegrid-ssoauth-azure.py` secuencia de comandos de Python
- El `storagegrid-ssoauth-azure.js` Script de Node.js

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

Para escribir su propia integración de API con Azure, consulte la `storagegrid-ssoauth-azure.py` guion. El script de Python realiza dos solicitudes a StorageGRID directamente (primero para obtener SAMLRequest y luego 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 de SSO se pueden ejecutar mediante una serie de solicitudes de API, pero hacerlo no es sencillo. El módulo Node.js Puppeteer se utiliza para rastrear la interfaz SSO de Azure.

Si tiene un problema de codificación de URL, es posible que vea el error: `Unsupported SAML version` .

Pasos

1. Instale las dependencias necesarias, de la siguiente manera:

a. Instalar Node.js (ver "https://nodejs.org/en/download/").

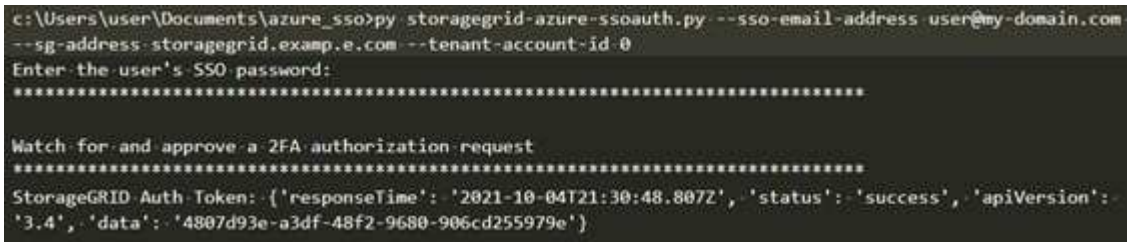
b. Instale los módulos Node.js necesarios (puppeteer y jsdom):

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

2. Pase el script de Python al intérprete de Python para ejecutarlo.

   Luego, el script de Python llamará al script Node.js correspondiente para realizar las interacciones de SSO de Azure.

3. Cuando se le solicite, ingrese valores para los siguientes argumentos (o páselos mediante parámetros):
   - La dirección de correo electrónico SSO utilizada para iniciar sesión en Azure
   - La dirección de StorageGRID
   - El ID de la cuenta del inquilino, si desea acceder a la API de administración de inquilinos
4. Cuando se le solicite, ingrese la contraseña y prepárese para proporcionar una autorización MFA a Azure si se le solicita.



> El script asume que la MFA se realiza mediante Microsoft Authenticator. Es posible que necesites modificar el script para admitir otras formas de MFA (como ingresar un código recibido en un mensaje de texto).

El token de autorización de StorageGRID se proporciona en la salida. Ahora puedes usar el token para otras solicitudes, de manera similar a como usarías la API si no se estuviera utilizando SSO.

Utilice la API si el inicio de sesión único está habilitado (PingFederate)

Si tienes"Inicio de sesión único (SSO) configurado y habilitado" y utiliza PingFederate como proveedor de SSO, debe emitir una serie de solicitudes de API para obtener un token de autenticación que sea válido para la API de administración de red o la API de administración de inquilinos.

Sign in en la API si el inicio de sesión único está habilitado

Estas instrucciones se aplican si utiliza PingFederate como proveedor de identidad SSO

Antes de empezar

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

Acerca de esta tarea

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

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

  El flujo de trabajo curl puede expirar si lo realiza demasiado lento. Es posible que veas el error: `A valid SubjectConfirmation was not found on this Response`.

  > El flujo de trabajo curl de ejemplo no protege la contraseña para que otros usuarios no la vean.

  Si tiene un problema de codificación de URL, es posible que vea el error: `Unsupported SAML version`.

Pasos

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

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

   - El método SSO. Puede ingresar cualquier variación de "pingfederate" (PINGFEDERATE, pingfederate, etc.).
   - El nombre de usuario de SSO
   - El dominio donde está instalado StorageGRID . Este campo no se utiliza para PingFederate. Puede dejarlo en blanco o ingresar cualquier valor.
   - La dirección de StorageGRID
   - El ID de la cuenta del inquilino, si desea acceder a la API de administración 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 puedes usar el token para otras solicitudes, de manera similar a como usarías la API si no se estuviera utilizando SSO.
3. Si desea utilizar solicitudes curl, utilice 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 administración de red, utilice 0 como `TENANTACCOUNTID` .

b. Para recibir una URL de autenticación firmada, emita una solicitud POST a `/api/v3/authorize-saml` y elimine la codificación JSON adicional de la respuesta.

Este ejemplo muestra una solicitud POST para una URL de autenticación firmada para TENANTACCOUNTID. Los resultados se pasarán a python -m json.tool para eliminar 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 para este ejemplo incluye una URL firmada que está codificada como 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. Guardar el `SAMLRequest` de la respuesta para su uso en comandos posteriores.

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

d. Exportar la respuesta y la cookie, y hacer eco de la respuesta:

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

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

e. Exporta el valor 'pf.adapterId' y repite la respuesta:

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

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

f. Exporta el valor 'href' (elimina la barra diagonal final /) y repite la respuesta:

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

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

g. Exportar el valor de 'acción':

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

h. Enviar cookies junto con las 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. Guardar el `SAMLResponse` del campo oculto:

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

j. Usando lo guardado `SAMLResponse` , crear un StorageGRID`/api/saml-response` solicitud para generar un token de autenticación de StorageGRID .

Para `RelayState` , use el ID de la cuenta del inquilino o use 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"
```

Ya puedes utilizar `MYTOKEN` para otras solicitudes, de forma similar a como usarías la API si no se estuviera utilizando SSO.

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

Si se ha habilitado el inicio de sesión único (SSO), debe emitir una serie de solicitudes de API para cerrar sesión en la API de administración de red o en la API de administración de inquilinos. Estas instrucciones se aplican si utiliza PingFederate como proveedor de identidad SSO

Acerca de esta tarea

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

Pasos

1. Para generar una solicitud de cierre de sesión firmada, pase `cookie "sso=true" a 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. Guardar 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 nuevamente a StorageGRID.

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

Se devuelve la respuesta 302. La ubicación de redireccionamiento no es aplicable al cierre de sesión exclusivo de 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. Eliminar el token portador de StorageGRID .

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

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

A `204 No Content` La respuesta indica que el usuario ahora ha cerrado la sesión.

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

Desactivar funciones con la API

Puede utilizar la API de administración de red para desactivar por completo ciertas funciones en el sistema StorageGRID . Cuando una función está desactivada, no se pueden asignar permisos a nadie para realizar las tareas relacionadas con esa función.

Acerca de esta tarea

El sistema de funciones desactivadas le permite evitar el acceso a ciertas funciones en el sistema StorageGRID . Desactivar una función es la única forma de evitar que el usuario root o los usuarios que pertenecen a grupos de administradores con permiso de **acceso root** puedan usar esa función.

Para comprender cómo esta funcionalidad podría ser útil, considere el siguiente escenario:

_La empresa A es un proveedor de servicios que alquila la capacidad de almacenamiento de su sistema StorageGRID mediante la creación de cuentas de inquilino. Para proteger la seguridad de los objetos de sus arrendatarios, la Compañía A quiere asegurarse de que sus propios empleados nunca puedan acceder a ninguna cuenta de inquilino después de que la cuenta se haya implementado.

La empresa A puede lograr este objetivo mediante el sistema de desactivación de funciones en la API de administración de la red. Al desactivar por completo la función **Cambiar contraseña de root del inquilino** en el Administrador de Grid (tanto la UI como la API), la Compañía A garantiza que los usuarios administradores, incluido el usuario root y los usuarios que pertenecen a grupos con permiso de **Acceso root**, no puedan cambiar la contraseña de ningún usuario root de la cuenta de inquilino.

Pasos

1. Acceda a la documentación de Swagger para la API de administración de cuadrícula. Ver "Utilice la API de gestión de red" .
2. Localice el punto final Desactivar funciones.
3. Para desactivar una función, como Cambiar la contraseña raíz del inquilino, envíe un cuerpo a la API como este:

   ```
   { "grid": {"changeTenantRootPassword": true} }
   ```

   Cuando se completa la solicitud, la función Cambiar la contraseña raíz del inquilino se deshabilita. El permiso de administración **Cambiar contraseña de root del inquilino** ya no aparece en la interfaz de usuario, y cualquier solicitud de API que intente cambiar la contraseña de root de un inquilino fallará con "403 Prohibido".

Reactivar funciones desactivadas

De forma predeterminada, puede utilizar la API de administración de cuadrícula para reactivar una función que se ha desactivado. Sin embargo, si desea evitar que las funciones desactivadas se vuelvan a activar, puede desactivar la función **activateFeatures**.

> La función **activateFeatures** no se puede reactivar. Si decide desactivar esta función, tenga en cuenta que perderá permanentemente la capacidad de reactivar cualquier otra función desactivada. Debe ponerse en contacto con el soporte técnico para restaurar cualquier funcionalidad perdida.

Pasos

1. Acceda a la documentación de Swagger para la API de administración de cuadrícula.
2. Localice el punto final Desactivar funciones.
3. Para reactivar todas las funciones, envíe un cuerpo a la API como este:

```
{ "grid": null }
```

Cuando se completa esta solicitud, se reactivan todas las funciones, incluida la función Cambiar la contraseña raíz del inquilino. El permiso de administración **Cambiar contraseña de root del inquilino** ahora aparece en la interfaz de usuario, y cualquier solicitud de API que intente cambiar la contraseña de root de un inquilino tendrá éxito, asumiendo que el usuario tiene el permiso de administración **Acceso de root** o **Cambiar contraseña de root del inquilino**.

El ejemplo anterior hace que *todas* las funciones desactivadas se reactiven. Si se han desactivado otras funciones que deben permanecer desactivadas, deberá especificarlas explícitamente en la solicitud PUT. Por ejemplo, para reactivar la función Cambiar contraseña de root del inquilino y continuar desactivando el permiso de administración de storageAdmin, envíe esta solicitud PUT:

```
{ "grid": {"storageAdmin": true} }
```