Usa la API

StorageGRID software

NetApp
July 23, 2026

Tabla de contenidos

Usa la API

Usa la API de gestión de StorageGRID Grid

Puedes realizar tareas de administración de sistemas mediante la API de REST de Grid Management en lugar de la interfaz de usuario de Grid Manager. Por ejemplo, es posible que quieras utilizar la API para automatizar operaciones o para crear varias entidades, como usuarios, de forma más rápida.

Recursos de primer nivel

La API de gestión de la red ofrece los siguientes recursos de primer nivel:

- `/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 pertenezcan a un grupo LDAP local o federado de una cuenta de inquilino. Para obtener más información, consulta "Utiliza 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 endpoints privados de StorageGRID también ignoran la versión de la API de la solicitud.

Realizar solicitudes a la API

La API de gestión de la red utiliza la plataforma de API de código abierto Swagger. Swagger ofrece una interfaz de usuario intuitiva que permite tanto a desarrolladores como a usuarios sin conocimientos de programación realizar operaciones en tiempo real en StorageGRID mediante la API.

La interfaz de usuario de Swagger ofrece información completa y documentación detallada para cada operación de la API.

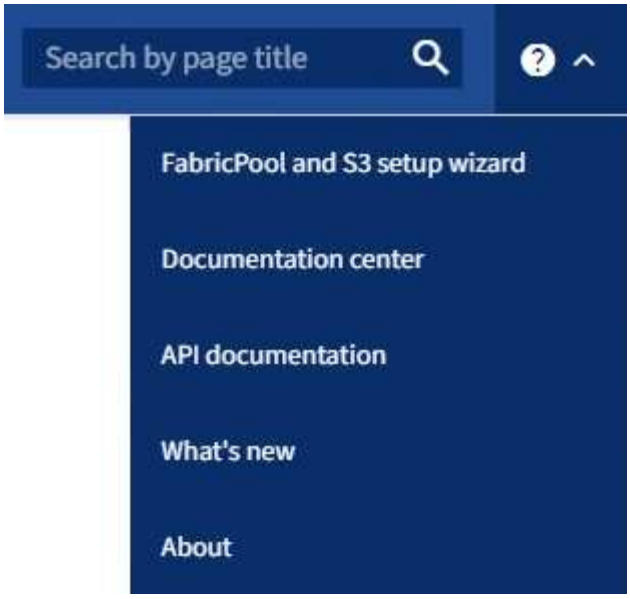
Antes de empezar

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

> Cualquier operación de la API que realices a través de la página web de la documentación de la API es una operación en tiempo real. Ten cuidado de no crear, actualizar ni eliminar por error datos de configuración u otros datos.

Pasos

1. En la barra de encabezado de Grid Manager, selecciona el icono de ayuda y selecciona **Documentación de la API**.



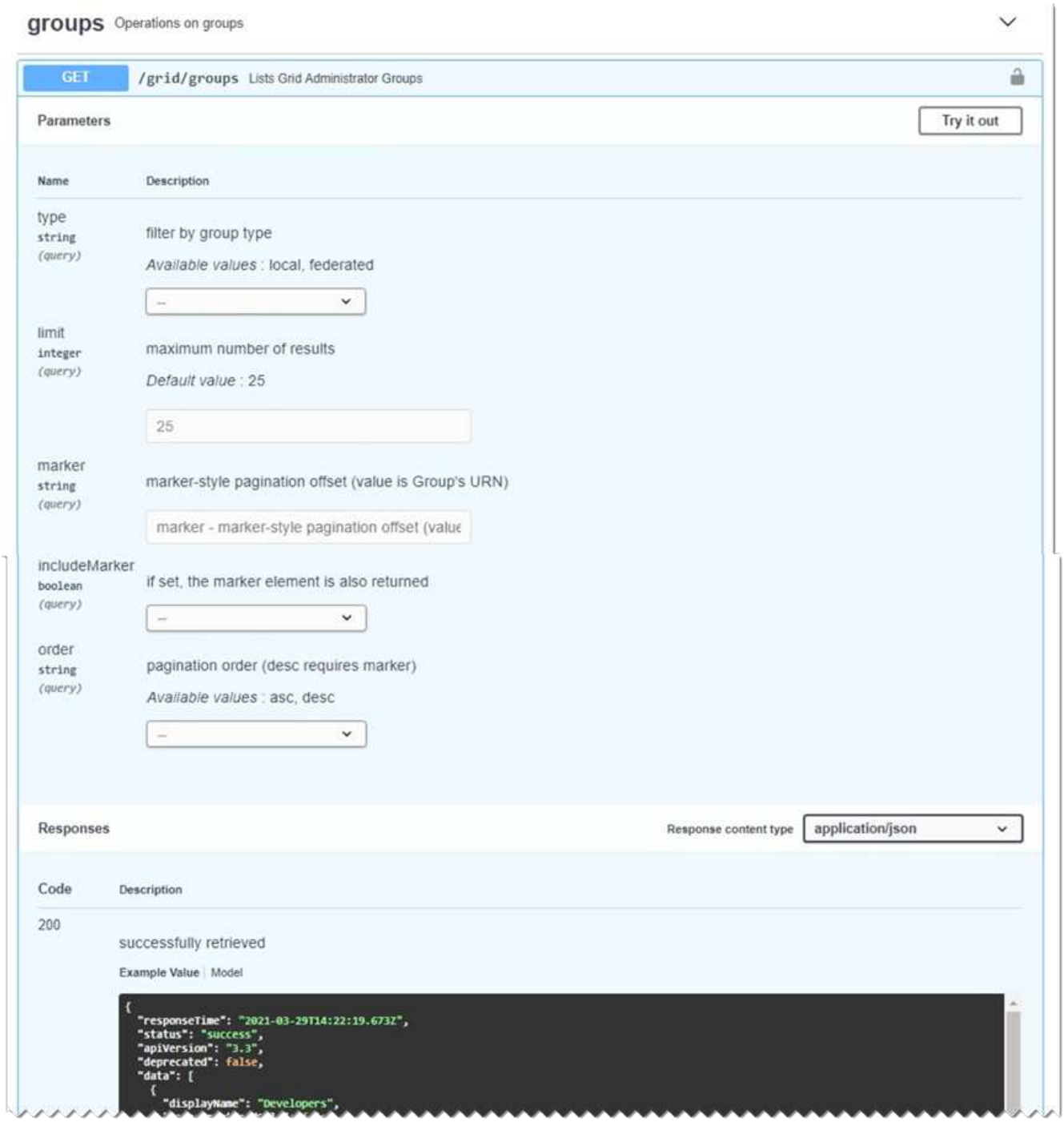
2. Para realizar una operación con la API privada, selecciona **Ir a la documentación de la API privada** en la página StorageGRID Management API.

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

3. Selecciona la operación que desees.

   Al desplegar una operación de la API, podrás ver las acciones HTTP disponibles, como GET, PUT, UPDATE y DELETE.

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



5. Comprueba si la solicitud requiere parámetros adicionales, como un ID de grupo o de usuario. Luego, obtén estos valores. Puede que primero tengas que enviar otra solicitud a la API para obtener la información que necesitas.
6. Comprueba si es necesario modificar el cuerpo de la solicitud de ejemplo. Si es así, puedes seleccionar **Modelo** para conocer los requisitos de cada campo.
7. ${post_edited_translations.segment}
8. Introduce los parámetros necesarios o modifica el cuerpo de la solicitud según sea necesario.
9. Selecciona **Ejecutar**.
10. Revisa el código de respuesta para determinar si la solicitud fue exitosa.

Operaciones de Grid Management API en StorageGRID

${post_edited_translations.segment}

Esta lista solo incluye las operaciones disponibles en la API pública.

- **cuentas**: Operaciones para gestionar cuentas de inquilinos de almacenamiento, incluyendo la creación de nuevas cuentas y la obtención del uso de almacenamiento para una cuenta determinada.
- **historial-alertas**: Operaciones en alertas resueltas.
- **alert-receivers**: Operaciones sobre los receptores de notificaciones de alertas (correo electrónico).
- ${post_edited_translations.segment}
- **alert-silences**: Operaciones sobre el silenciamiento de alertas.
- **alertas**: Operaciones sobre alertas.
- ${post_edited_translations.segment}
- **auth**: Operaciones para realizar la autenticación de la sesión del usuario.

  La API de gestión de la red es compatible con el esquema de autenticación mediante token de portador. Para iniciar sesión, debes introducir 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 incluirse en el encabezado de las solicitudes posteriores a la API ("Authorization: Bearer *token*"). El token caduca después de 16 horas.

  Si el inicio de sesión único está habilitado para el sistema StorageGRID, debes realizar pasos diferentes para autenticarte. Consulta "Autenticación en la API si el inicio de sesión único está habilitado".

  Consulta «Protección contra la falsificación de solicitudes entre sitios» para obtener información sobre cómo mejorar la seguridad de autenticación.

- ${post_edited_translations.segment}
- **config**: operaciones relacionadas con la versión del producto y las versiones de la Grid Management API. Puedes enumerar la versión del producto y las versiones principales de la Grid Management API compatibles con esa versión, y puedes desactivar las versiones obsoletas de la API.
- ${post_edited_translations.segment}
- **dns-servers**: Operaciones para ver y modificar los servidores DNS externos configurados.
- **drive-details**: Operaciones en unidades para modelos específicos de dispositivos de almacenamiento.
- **endpoint-domain-names**: Operaciones para mostrar y cambiar los nombres de dominio de los endpoints de S3.
- **código de borrado**: Operaciones sobre perfiles de código de borrado.
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- **emplazamientos-de-expansión**: Operaciones de expansión (a nivel de emplazamiento).
- **grid-networks**: Operaciones para mostrar y cambiar la lista de la Grid Network.
- **grid-passwords**: Operaciones para la gestión de contraseñas de grid.

- **grupos**: Operaciones para gestionar los grupos de administradores de Grid locales y para recuperar los grupos de administradores de Grid federados desde un servidor LDAP externo.
- **fuente-de-identidad**: Operaciones para configurar una fuente de identidad externa y para sincronizar manualmente la información de grupos y usuarios federados.
- **ilm**: Operaciones sobre la gestión del ciclo de vida de la información (ILM).
- **procedimientos-en-curso**: Recupera los procedimientos de mantenimiento que están en curso.
- **licencia**: Operaciones para recuperar y actualizar la licencia de StorageGRID.
- **registros**: Operaciones para recopilar y descargar archivos de registro.v
- **métricas**: Operaciones con métricas de StorageGRID, incluidas consultas de métricas instantáneas en un único punto en el tiempo y consultas de métricas en un intervalo de tiempo. La Grid Management API utiliza la herramienta de monitoreo de sistemas Prometheus como fuente de datos backend. Para obtener información sobre cómo crear consultas de Prometheus, consulta el sitio web de Prometheus.

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

- **node-details**: Operaciones sobre los detalles de los nodos.
- **node-health**: Operaciones sobre el estado de salud del nodo.
- **node-storage-state**: Operaciones sobre el estado de almacenamiento del nodo.
- ${post_edited_translations.segment}
- **objetos**: Operaciones sobre objetos y metadatos de objetos.
- ${post_edited_translations.segment}
- **paquete-de-recuperación**: Operaciones para descargar el paquete de recuperación.
- **regiones**: Operaciones para ver y crear regiones.
- **s3-object-lock**: Operaciones sobre la configuración global de S3 Object Lock.
- ${post_edited_translations.segment}
- **snmp**: Operaciones sobre la configuración actual de SNMP.
- **marcas de agua de almacenamiento**: Marcas de agua de los nodos de almacenamiento.
- **clases-de-tráfico**: Operaciones para las políticas de clasificación de tráfico.
- ${post_edited_translations.segment}
- **Usuarios**: Operaciones para ver y gestionar usuarios de Grid Manager.

Versionado de la Grid Management API en StorageGRID

La API de gestión de la red utiliza versionado para permitir 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 incrementa cuando se realizan cambios que *no son compatibles* con las

versiones anteriores. La versión secundaria de la API se incrementa cuando se realizan cambios que *sí son compatibles* con las versiones anteriores. Los cambios compatibles incluyen la adición de nuevos endpoints o nuevas propiedades.

El siguiente ejemplo ilustra cómo se incrementa la versión de la API en función del tipo de cambios realizados.

Tipo de cambio en la API	${post_edited_translations.segment}	Nueva versión
Compatible con versiones anteriores	2,1	2,2
No es compatible con versiones anteriores	2,1	3,0

Al instalar el software StorageGRID por primera vez, solo se habilita la versión más reciente de la API. Sin embargo, al actualizar a una nueva versión funcional de StorageGRID, sigues teniendo acceso a la versión anterior de la API durante al menos una versión funcional de StorageGRID.

> Puedes configurar las versiones compatibles. Consulta la sección **config** de la documentación de la API de Swagger para el "API de gestión de grid" para más información. Debes desactivar la compatibilidad con la versión anterior después de actualizar todos los clientes de la API para que usen la versión más reciente.

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

- ${post_edited_translations.segment}
- El cuerpo de la respuesta JSON incluye "deprecated": true
- Se añade una advertencia de obsolescencia a nms.log. Por ejemplo:

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

Averigua qué versiones de la API son compatibles en la versión actual

Utiliza la solicitud de API `GET /versions` para devolver una lista de las versiones principales de la 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
  ]
}
```

Especifica una versión de la API para una solicitud

Puedes especificar la versión de la API utilizando un parámetro de ruta (`/api/v4`) o un encabezado (`Api-Version: 4`). Si proporcionas ambos valores, el valor del encabezado tiene prioridad sobre el de la ruta.

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

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

Protege contra la falsificación de petición en sitios cruzados (CSRF) en StorageGRID

Puedes ayudar a proteger StorageGRID contra los ataques de falsificación de solicitudes entre sitios (CSRF) utilizando tokens CSRF para reforzar la autenticación que usa cookies. Grid Manager y Tenant Manager activan automáticamente esta función de seguridad; otros clientes de la API pueden elegir si desean activarla al iniciar sesión.

${post_edited_translations.segment}

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

Para habilitar la función, establece el parámetro `csrfToken` en `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 verdadero, se establece una cookie `GridCsrfToken` con un valor aleatorio para los inicios de sesión en el Grid Manager, y la cookie `AccountCsrfToken` se establece con un valor aleatorio para los inicios de sesión en el Tenant Manager.

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:

- La cabecera `X-Csrf-Token`, con el valor de la cabecera establecido en el valor de la cookie de token CSRF.
- Para los puntos finales que aceptan un cuerpo codificado en formato form-encoded: un parámetro del cuerpo de la solicitud codificado en formato form-encoded. `csrfToken`

Consulta la documentación en línea de la API para ver más ejemplos y detalles.

> Las solicitudes que tengan configurada una cookie con un token CSRF también aplicarán el encabezado "Content-Type: application/json" a cualquier solicitud que requiera un cuerpo de solicitud en formato JSON como protección adicional contra los ataques CSRF.

${post_edited_translations.segment}

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

Si tienes "configurado y activado el inicio de sesión único (SSO)" y usas Active Directory como proveedor de inicio de sesión único, debes hacer una serie de solicitudes de API para obtener un token de autenticación válido para la Grid Management API o la Tenant Management API.

Inicia sesión en la API si está activado el inicio de sesión único

Estas instrucciones aplican si usas Active Directory como proveedor de identidad de inicio de sesión único (SSO).

Antes de empezar

- Conoces el nombre de usuario y la contraseña de inicio de sesión único de un usuario federado que pertenece a un grupo de usuarios de StorageGRID.
- Si quieres acceder a la API de gestión de inquilinos, sabes el ID de la cuenta del inquilino.

Acerca de esta tarea

Para obtener un token de autenticación, puedes usar uno de los siguientes ejemplos:

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

  El flujo de trabajo de curl podría agotar el tiempo de espera si lo ejecutas demasiado despacio. Es posible que aparezca el siguiente error: `A valid SubjectConfirmation was not found on this Response`.

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

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

Pasos

1. Selecciona uno de los siguientes métodos para obtener un token de autenticación:
   - Utiliza el `storagegrid-ssoauth.py` script de Python. Ve al paso 2.
   - Utiliza solicitudes con curl. Ve al paso 3.
2. Si quieres utilizar el script `storagegrid-ssoauth.py`, pásalo al intérprete de Python y ejecútalo.

   Cuando se te solicite, introduce los valores para los siguientes argumentos:

   - El método SSO. Introduce ADFS o adfs.
   - El nombre de usuario de SSO
   - El dominio en el que está instalado StorageGRID
   - La dirección de StorageGRID
   - El ID de la cuenta del tenant, si deseas acceder a la API de Tenant Management.

   ```
   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 aparece en la salida. Ahora puedes utilizar el token para otras solicitudes, de forma similar a como lo harías si no se utilizara el inicio de sesión único.
3. Si quieres utilizar solicitudes curl, usa el siguiente procedimiento.
   a. Declara 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 la red, utiliza 0 como `TENANTACCOUNTID`.

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

Este ejemplo muestra una solicitud POST para obtener una URL de autenticación firmada para `TENANTACCOUNTID`. Los resultados se enviarán 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 de este ejemplo incluye una URL firmada que está codificada como URL, pero no incluye la capa adicional de codificación JSON.

```
{
    "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. Guarda el `SAMLRequest` de la respuesta para usarlo en comandos posteriores.

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

d. Obtén una URL completa que incluya el ID de la 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"'
```

${post_edited_translations.segment}

```
<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. Guarda 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 tu sistema de SSO, el envío 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. Guarda la `MSISAuth` cookie de la respuesta.

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

h. Envía una solicitud GET a la ubicación especificada con las cookies de la autenticación POST.

```
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 uso posterior en el cierre de sesión, y el cuerpo de la respuesta contiene el SAMLResponse en un campo oculto del formulario.

```
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. Guarda el `SAMLResponse` del campo oculto:

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

j. Utilizando el archivo guardado `SAMLResponse`, haz una solicitud StorageGRID`/api/saml-response` para generar un token de autenticación de StorageGRID.

Para `RelayState`, usa el ID de la cuenta de inquilino o usa 0 si quieres iniciar sesión en la API de gestión 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. Guarda el token de autenticación de la respuesta como `MYTOKEN`.

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

Ahora puedes utilizar `MYTOKEN` para otras solicitudes, de forma similar a como lo harías si no se utilizara el inicio de sesión único.

Cierra sesión en la API si el inicio de sesión único está activado

Si se ha habilitado el inicio de sesión único (SSO), debes realizar una serie de solicitudes de API para cerrar la sesión en la Grid Management API o en la Tenant Management API. Estas instrucciones aplican si usas Active Directory como proveedor de identidad de SSO.

Acerca de esta tarea

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

Pasos

1. Para generar una solicitud de cierre de sesión con firma, pasa `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. Guarda la URL de cierre de sesión.

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

3. ${post_edited_translations.segment}

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

Se devuelve la respuesta 302. La ubicación de redireccionamiento no es aplicable al cierre de sesión exclusivo de la 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. ${post_edited_translations.segment}

Eliminar el token de portador de StorageGRID funciona igual que sin SSO. Si no se proporciona la `cookie "sso=true"`, el usuario se desconecta 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
```

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

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

Usa la API de StorageGRID si el inicio de sesión único está activado (Entra ID)

Si tienes "configurado y activado el inicio de sesión único (SSO)" y usas Entra ID como proveedor de inicio de sesión único, puedes usar dos scripts de ejemplo para obtener un token de autenticación válido para la API de gestión de Grid o la API de gestión de Tenant.

Inicia sesión en la API si está activado el inicio de sesión único de Entra ID

Estas instrucciones aplican si usas Entra ID como proveedor de identidad de inicio de sesión único

Antes de empezar

- Conoces la dirección de correo electrónico y la contraseña de inicio de sesión único de un usuario federado que pertenece a un grupo de usuarios de StorageGRID.
- Si quieres acceder a la API de gestión de inquilinos, sabes el ID de la cuenta del inquilino.

Acerca de esta tarea

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

- El `storagegrid-ssoauth-azure.py` script de Python
- El `storagegrid-ssoauth-azure.js` script Node.js

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

Para escribir tu propia integración de API con Entra ID, consulta el script `storagegrid-ssoauth-azure.py`. El script de Python realiza dos solicitudes directamente a StorageGRID (primero para obtener el SAMLRequest y luego para obtener el token de autorización), y también llama al script de Node.js para interactuar con Entra ID y realizar las operaciones de inicio de sesión único.

Las operaciones de SSO pueden ejecutarse mediante una serie de solicitudes de API, pero hacerlo no es sencillo. Se utiliza el módulo Puppeteer de Node.js para extraer datos de la interfaz de SSO de Entra ID.

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

Pasos

1. Instala las dependencias necesarias de la siguiente manera:

a. Instala Node.js (consulta "https://nodejs.org/en/download/").

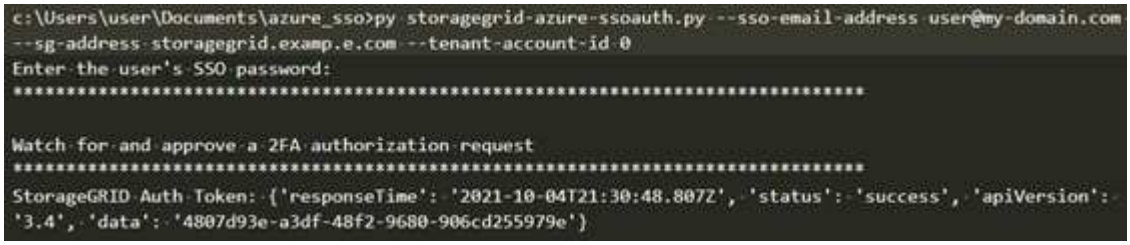
b. Instala los módulos necesarios de Node.js (puppeteer y jsdom):

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

2. Pasa el script de Python al intérprete de Python para ejecutar el script.

   Luego, el script de Python llamará al script correspondiente de Node.js para realizar las interacciones de inicio de sesión único de Entra ID.

3. Cuando se te solicite, introduce los valores de los siguientes argumentos (o pásalos mediante parámetros):
   - La dirección de correo electrónico de SSO utilizada para iniciar sesión en Entra ID
   - La dirección de StorageGRID
   - El ID de la cuenta del inquilino, si quieres acceder a la API de gestión de inquilinos
4. Cuando se te solicite, introduce la contraseña y prepárate para proporcionar una autorización MFA a Entra ID si se te pide.



> El script parte de la base de que la autenticación multifactor (MFA) se realiza usando Microsoft Authenticator. Es posible que tengas que 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 aparece en la salida. Ahora puedes utilizar el token para otras solicitudes, de forma similar a como lo harías si no se utilizara el inicio de sesión único.

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

Si tienes "configurado y activado el inicio de sesión único (SSO)" y usas PingFederate como proveedor de inicio de sesión único, debes realizar una serie de solicitudes de API para obtener un token de autenticación válido para la Grid Management API o la Tenant Management API.

Inicia sesión en la API si está activado el inicio de sesión único

Estas instrucciones aplican si usas PingFederate como proveedor de identidad de SSO

Antes de empezar

- Conoces el nombre de usuario y la contraseña de inicio de sesión único de un usuario federado que pertenece a un grupo de usuarios de StorageGRID.
- Si quieres acceder a la API de gestión de inquilinos, sabes el ID de la cuenta del inquilino.

Acerca de esta tarea

Para obtener un token de autenticación, puedes usar uno de los siguientes ejemplos:

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

  El flujo de trabajo de curl podría agotar el tiempo de espera si lo ejecutas demasiado despacio. Es posible que aparezca el siguiente error: `A valid SubjectConfirmation was not found on this Response`.

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

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

Pasos

1. Selecciona uno de los siguientes métodos para obtener un token de autenticación:
   - Utiliza el `storagegrid-ssoauth.py` script de Python. Ve al paso 2.
   - Utiliza solicitudes con curl. Ve al paso 3.
2. Si quieres utilizar el script `storagegrid-ssoauth.py`, pásalo al intérprete de Python y ejecútalo.

   Cuando se te solicite, introduce los valores para los siguientes argumentos:

   - El método SSO. Puedes introducir cualquier variante de «pingfederate» (PINGFEDERATE, pingfederate, y así sucesivamente).
   - El nombre de usuario de SSO
   - El dominio en el que está instalado StorageGRID. Este campo no se utiliza para PingFederate. Puedes dejarlo en blanco o ingresar cualquier valor.
   - La dirección de StorageGRID
   - El ID de la cuenta del tenant, si deseas acceder a la API de Tenant Management.

   ```
   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 aparece en la salida. Ahora puedes utilizar el token para otras solicitudes, de forma similar a como lo harías si no se utilizara el inicio de sesión único.

3. Si quieres utilizar solicitudes curl, usa el siguiente procedimiento.

   a. Declara 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 la red, utiliza 0 como `TENANTACCOUNTID`.

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

   Este ejemplo muestra una solicitud POST para una URL de autenticación firmada para TENANTACCOUNTID. Los resultados se pasan 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 de este ejemplo incluye una URL firmada que está codificada como URL, pero no incluye la capa adicional de codificación JSON.

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

   c. Guarda el `SAMLRequest` de la respuesta para usarlo en comandos posteriores.

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

   d. Exporta la respuesta y la cookie, y muestra 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 muestra la respuesta:

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

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

f. Exporta el valor de «href» (elimina la barra al final /) y muestra la respuesta:

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

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

g. Exporta el valor 'action':

```
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. Guarda el `SAMLResponse` del campo oculto:

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

j. Utilizando el archivo guardado `SAMLResponse`, haz una solicitud StorageGRID`/api/saml-response` para generar un token de autenticación de StorageGRID.

   Para `RelayState`, usa el ID de la cuenta de inquilino o usa 0 si quieres iniciar sesión en la API de gestión 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. Guarda el token de autenticación de la respuesta como `MYTOKEN`.

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

Ahora puedes utilizar `MYTOKEN` para otras solicitudes, de forma similar a como lo harías si no se utilizara el inicio de sesión único.

Cierra sesión en la API si el inicio de sesión único está activado

Si se ha habilitado el inicio de sesión único (SSO), debes realizar una serie de solicitudes de API para cerrar la sesión en la API de gestión de Grid o en la API de gestión de Tenant. Estas instrucciones aplican si usas PingFederate como proveedor de identidad de SSO.

Acerca de esta tarea

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

Pasos

1. Para generar una solicitud de cierre de sesión con firma, pasa `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. Guarda la URL de cierre de sesión.

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

3. ${post_edited_translations.segment}

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

Se devuelve la respuesta 302. La ubicación de redireccionamiento no es aplicable al cierre de sesión exclusivo de la 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. ${post_edited_translations.segment}

Eliminar el token de portador de StorageGRID funciona igual que sin SSO. Si no se proporciona la `cookie "sso=true"`, el usuario se desconecta 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
```

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

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

Desactiva las funciones de StorageGRID con la API

Puedes usar la API de gestión de grid para desactivar por completo ciertas funciones en el sistema StorageGRID. Cuando se desactiva una función, no se pueden asignar permisos a nadie para realizar las tareas relacionadas con esa función.

Acerca de esta tarea

El sistema de funciones desactivadas te permite impedir el acceso a determinadas funciones del sistema StorageGRID. Desactivar una función es la única forma de impedir que el usuario raíz o los usuarios que pertenezcan a grupos de administración con permiso de acceso a raíz puedan utilizar esa función.

Para comprender cómo puede resultar útil esta funcionalidad, imagina la siguiente situación:

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 inquilinos, la empresa A quiere asegurarse de que sus propios empleados nunca puedan acceder a ninguna cuenta de inquilino una vez que esta se haya implementado.

La empresa A puede alcanzar este objetivo utilizando el sistema Deactivate Features en la Grid Management API. Al desactivar por completo la función **Change tenant root password** en el Grid Manager (tanto en la interfaz de usuario como en la API), la empresa A se asegura de que los usuarios Admin —incluidos el usuario raíz y los usuarios que pertenecen a grupos con el permiso **Root access**— no puedan cambiar la contraseña del usuario raíz de ninguna cuenta de tenant._

Pasos

1. Accede a la documentación de Swagger sobre la API de gestión de la red. Consulta "Usa la API de gestión de Grid".
2. Ubica el endpoint Deactivate Features.
3. Para desactivar una función, como Cambiar la contraseña raíz del inquilino, envía un cuerpo a la API como este:

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

   Cuando se completa la solicitud, la función Cambiar la contraseña de root del inquilino queda desactivada. El permiso de administración **Cambiar la 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 Forbidden".

Reactivar las funciones desactivadas

De forma predeterminada, puedes utilizar la API de gestión de la red para reactivar una función que se haya desactivado. Sin embargo, si deseas evitar que las funciones desactivadas se vuelvan a activar en ningún momento, puedes desactivar la propia función **activateFeatures**.

> La función **activateFeatures** no se puede volver a activar. Si decides desactivar esta función, ten en cuenta que perderás de forma permanente la posibilidad de volver a activar cualquier otra función desactivada. Debes ponerte en contacto con el soporte técnico para recuperar cualquier funcionalidad perdida.

Pasos

1. Accede a la documentación de Swagger para la API de gestión de la red.
2. Ubica el endpoint Deactivate Features.
3. Para reactivar todas las funciones, envía un cuerpo a la API como este:

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

Una vez completada esta solicitud, se reactivan todas las funciones, incluida la función **Cambiar la contraseña de root del inquilino**. El permiso de administración **Cambiar la contraseña de root del inquilino** aparece ahora en la interfaz de usuario, y cualquier solicitud de API que intente cambiar la contraseña de root de un inquilino se ejecutará con éxito, siempre que el usuario disponga del permiso de administración **Acceso a raíz** o **Cambiar la contraseña de root del inquilino**.

El ejemplo anterior hace que se reactiven *todas* las funciones desactivadas. Si se han desactivado otras funciones que deberían permanecer desactivadas, debes especificarlas explícitamente en la solicitud PUT. Por ejemplo, para reactivar la función Cambiar la contraseña raíz del inquilino y mantener desactivado el permiso de gestión storageAdmin, envía esta solicitud PUT: `{ "grid": {"storageAdmin": true} }`

Información de copyright

Información de la marca comercial