Use o API

StorageGRID software

NetApp
July 23, 2026

Índice

Use o API

Use a API de gerenciamento de grid do StorageGRID

Você pode executar tarefas de gerenciamento do sistema usando a API REST de gerenciamento do Grid em vez da interface de usuário do Grid Manager. Por exemplo, você pode querer usar a API para automatizar operações ou criar várias entidades, como usuários, mais rapidamente.

Recursos de alto nível

A API de gerenciamento de grid fornece os seguintes recursos de nível superior:

- `/grid`: O acesso é restrito aos usuários do Grid Manager e baseia-se nas permissões de grupo configuradas.
- `/org`: O acesso é restrito a usuários que pertencem a um grupo LDAP local ou federado para uma conta de locatário. Para obter detalhes, consulte "Use uma conta de tenant".
- `/private`: O acesso é restrito a usuários do Grid Manager e é baseado nas permissões de grupo configuradas. As APIs privadas estão sujeitas a alterações sem aviso prévio. Os endpoints privados do StorageGRID também ignoram a versão da API da solicitação.

Emitir solicitações de API

A API de Gerenciamento de Grid utiliza a plataforma de API de código aberto Swagger. O Swagger fornece uma interface de usuário intuitiva que permite que desenvolvedores e não desenvolvedores realizem operações em tempo real no StorageGRID com a API.

A interface de usuário Swagger fornece detalhes completos e documentação para cada operação da API.

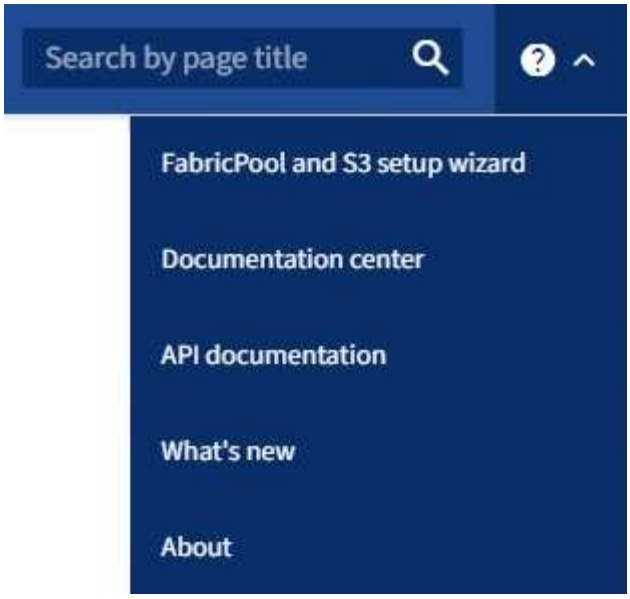
Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem "permissões de acesso específicas".

> Qualquer operação de API realizada por meio da página de documentação da API é uma operação em tempo real. Tenha cuidado para não criar, atualizar ou excluir dados de configuração ou outros dados por engano.

Passos

1. No cabeçalho do Gerenciador de Grade, selecione o ícone de ajuda e selecione **API documentation**.



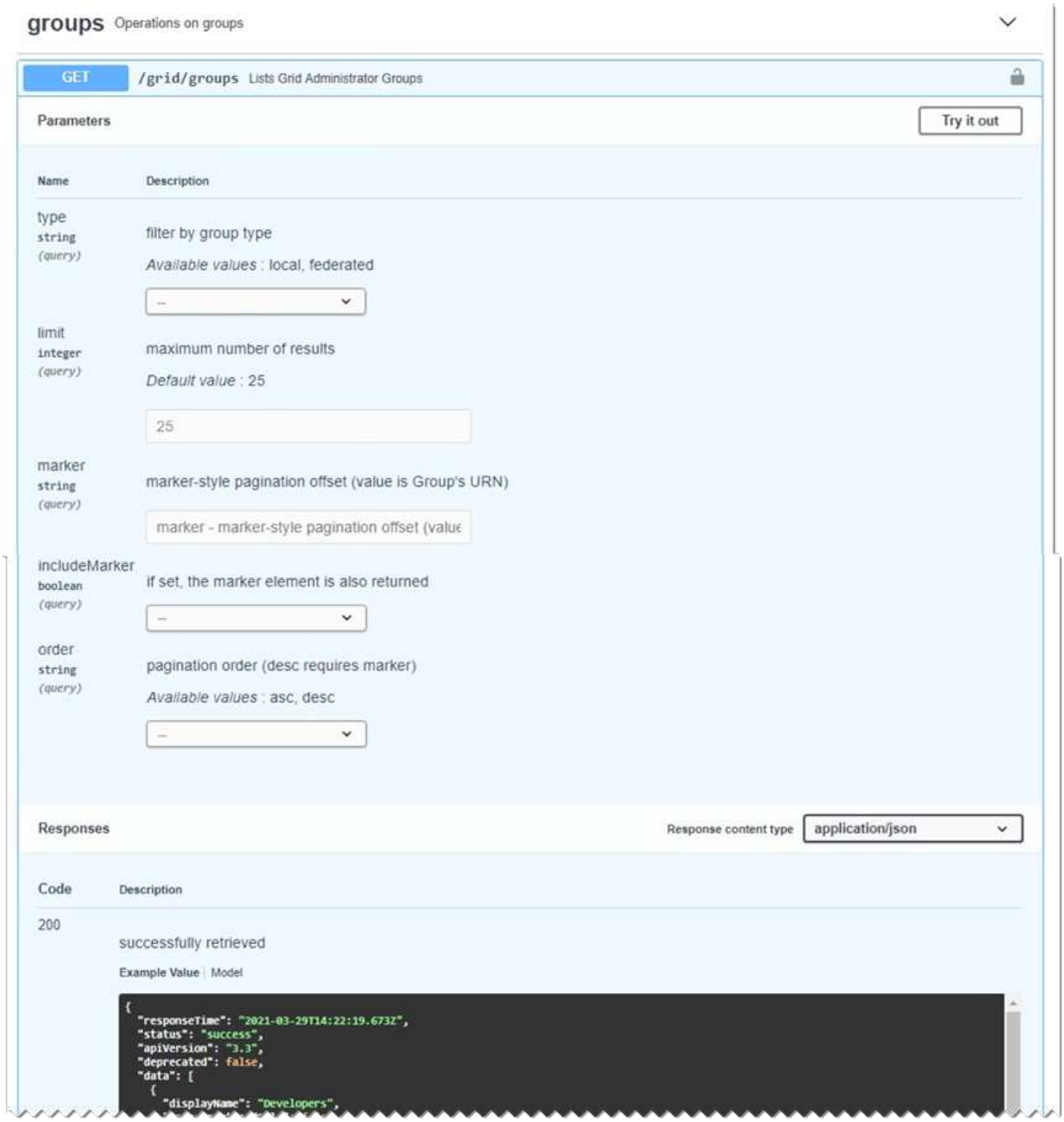
2. Para executar uma operação com a API privada, selecione **Acessar a documentação da API privada** na página da API de gerenciamento do StorageGRID.

   As APIs privadas estão sujeitas a alterações sem aviso prévio. Os endpoints privados do StorageGRID também ignoram a versão da API da solicitação.

3. Selecione a operação desejada.

   Ao expandir uma operação da API, você pode visualizar as ações HTTP disponíveis, como GET, PUT, UPDATE e DELETE.

4. Selecione uma ação HTTP para ver os detalhes da solicitação, incluindo o URL do endpoint, uma lista de parâmetros obrigatórios ou opcionais, um exemplo do corpo da solicitação (quando necessário) e as possíveis respostas.



5. Determine se a solicitação requer parâmetros adicionais, como um ID de grupo ou de usuário. Em seguida, obtenha esses valores. Pode ser necessário fazer uma solicitação de API diferente primeiro para obter as informações de que você precisa.
6. Determine se você precisa modificar o corpo da solicitação de exemplo. Caso precise, selecione **Model** para conhecer os requisitos de cada campo.
7. Selecione **Experimentar**.
8. Forneça todos os parâmetros necessários ou modifique o corpo da solicitação conforme necessário.
9. Selecione **Executar**.
10. Analise o código de resposta para determinar se a solicitação foi bem-sucedida.

Operações da API de gerenciamento de grid no StorageGRID

A API de Gerenciamento de Grid organiza as operações disponíveis nas seguintes seções.

Esta lista inclui apenas as operações disponíveis na API pública.

- **contas**: Operações para gerenciar contas de locatários de armazenamento, incluindo criar novas contas e recuperar o uso de armazenamento para uma determinada conta.
- **histórico de alertas**: operações em alertas resolvidos.
- **receptores de alertas**: Operações em receptores de notificações de alerta (email).
- **alert-rules**: Operações em regras de alerta.
- **alert-silences**: Operações em silêncios de alerta.
- **alertas**: Operações em alertas.
- **auditoria**: Operações para listar e atualizar a configuração de auditoria.
- **auth**: Operações para realizar autenticação de sessão do usuário.

  A API de gerenciamento de grid suporta o esquema de autenticação Bearer Token. Para fazer login, você fornece um nome de usuário e uma senha no corpo JSON da solicitação de autenticação (ou seja, `POST /api/v3/authorize`). Se o usuário for autenticado com sucesso, um token de segurança será retornado. Esse token deve ser fornecido no cabeçalho das solicitações de API subsequentes ("Authorization: Bearer *token*"). O token expira após 16 horas.

  Se o single sign-on estiver habilitado para o StorageGRID, você deve executar etapas diferentes para autenticar. Consulte "Autenticando na API se o single sign-on estiver habilitado".

  Consulte "Proteção contra falsificação de solicitações entre sites" para obter informações sobre como melhorar a segurança de autenticação.

- **client-certificates**: Operações para configurar certificados de cliente para que StorageGRID possa ser acessado com segurança usando ferramentas de monitoramento externas.
- **config**: Operações relacionadas ao lançamento do produto e às versões da API de Gerenciamento de Grid. Você pode listar a versão de lançamento do produto e as principais versões da API de Gerenciamento de Grid suportadas por esse lançamento, além de desativar versões obsoletas da API.
- **recursos-desativados**: operações para visualizar recursos que podem ter sido desativados.
- **servidores-dns**: Operações para listar e alterar servidores DNS externos configurados.
- **drive-details**: Operações em unidades para modelos específicos de dispositivos de storage.
- **endpoint-domain-names**: Operações para listar e alterar nomes de domínio de endpoint do S3.
- **erasure-coding**: Operações em perfis de codificação de apagamento.
- **expansão**: operações de expansão (nível de procedimento).
- **expansion-nodes**: Operações em expansão (nível de nó).
- **locais de expansão**: Operações em expansão (nível do local).

- **grid-networks**: Operações para listar e alterar a Lista de Redes da Grid.
- **grid-passwords**: operações para gerenciamento de senhas em grid.
- **grupos**: Operações para gerenciar grupos de administradores de Grid locais e para recuperar grupos de administradores de Grid federados de um servidor LDAP externo.
- **identity-source**: Operações para configurar uma fonte de identidade externa e sincronizar manualmente informações de grupo e usuário federados.
- **ilm**: Operações de gerenciamento do ciclo de vida das informações (ILM).
- **procedimentos-em-andamento**: Recupera os procedimentos de manutenção que estão atualmente em andamento.
- **licença**: Operações para recuperar e atualizar a licença do StorageGRID.
- **logs**: Operações para coletar e baixar arquivos de log.v
- **metrics**: Operações em métricas do StorageGRID, incluindo consultas instantâneas de métricas em um ponto único no tempo e consultas de métricas de intervalo ao longo de um período de tempo. A Grid Management API utiliza a ferramenta de monitoramento de sistemas Prometheus como fonte de dados de backend. Para obter informações sobre como construir consultas Prometheus, consulte o site do Prometheus.

> As métricas que incluem `private` em seus nomes destinam-se apenas ao uso interno. Essas métricas estão sujeitas a alterações entre versões do StorageGRID sem aviso prévio.

- **node-details**: Operações nos detalhes do nó.
- **node-health**: Operações sobre o status de integridade do nó.
- **node-storage-state**: Operações no status de armazenamento do nó.
- **ntp-servers**: Operações para listar ou atualizar servidores externos do Protocolo de Tempo de Rede (NTP).
- **objetos**: Operações em objetos e metadados de objetos.
- **recuperação**: Operações para o procedimento de recuperação.
- **pacote de recuperação**: operações para baixar o pacote de recuperação.
- **regiões**: Operações para visualizar e criar regiões.
- **s3-object-lock**: Operações nas configurações globais de S3 Object Lock.
- **server-certificate**: Operações para visualizar e atualizar os certificados do servidor Grid Manager.
- **snmp**: Operações na configuração SNMP atual.
- **storage-watermarks**: Marcas d'água de nós de storage.
- **classes-de-tráfego**: Operações para políticas de classificação de tráfego.
- **rede-cliente-não-confiável**: Operações na configuração da rede de cliente não confiável.
- **usuários**: Operações para visualizar e gerenciar usuários do Grid Manager.

Controle de versão da Grid Management API no StorageGRID

A API de gerenciamento de grid utiliza versionamento para suportar atualizações não

disruptivas.

Por exemplo, esta URL de solicitação especifica a versão 4 da API.

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

A versão principal da API é atualizada quando são feitas alterações que *não são compatíveis* com versões anteriores. A versão secundária da API é atualizada quando são feitas alterações que *são compatíveis* com versões anteriores. Alterações compatíveis incluem a adição de novos endpoints ou novas propriedades.

O exemplo a seguir ilustra como a versão da API é atualizada com base no tipo de alterações realizadas.

Tipo de alteração na API	Versão antiga	Nova versão
Compatível com versões anteriores	2,1	2,2
Não é compatível com versões antigas	2,1	3,0

Ao instalar o software StorageGRID pela primeira vez, apenas a versão mais recente da API é habilitada. No entanto, ao atualizar para uma nova versão de recursos do StorageGRID, você continua tendo acesso à versão anterior da API por pelo menos uma versão de recursos do StorageGRID.

> Você pode configurar as versões suportadas. Consulte a seção **config** da documentação da API Swagger para o "API de gerenciamento de grid" para mais informações. Você deve desativar o suporte para a versão antiga após atualizar todos os clientes da API para usar a versão mais recente.

As solicitações desatualizadas são marcadas como obsoletas das seguintes maneiras:

- O cabeçalho da resposta é "Deprecated: true"
- O corpo da resposta JSON inclui "deprecated": true
- Um aviso de descontinuação é adicionado ao nms.log. Por exemplo:

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

Determine quais versões da API são compatíveis na versão atual

Use a solicitação `GET /versions` à API para retornar uma lista das versões principais da API suportadas. Essa solicitação está localizada na seção **config** da documentação da API Swagger.

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

Especifique uma versão da API para uma solicitação

Você pode especificar a versão da API usando um parâmetro de caminho (`/api/v4`) ou um cabeçalho (`Api-Version: 4`). Se você fornecer ambos os valores, o valor do cabeçalho substitui o valor do caminho.

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

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

Proteja contra ataques de falsificação de solicitação entre sites (CSRF) no StorageGRID

Você pode ajudar a proteger contra ataques de Cross-Site Request Forgery (CSRF) ao StorageGRID usando tokens CSRF para aprimorar a autenticação que utiliza cookies. O Grid Manager e o Tenant Manager habilitam automaticamente esse recurso de segurança; outros clientes da API podem escolher se desejam habilitá-lo ao fazer login.

Um atacante capaz de enviar uma solicitação para um site diferente (como por meio de um formulário HTTP POST) pode fazer com que determinadas solicitações sejam realizadas usando os cookies do usuário autenticado.

StorageGRID ajuda a proteger contra ataques CSRF usando tokens CSRF. Quando ativado, o conteúdo de um cookie específico deve corresponder ao conteúdo de um cabeçalho específico ou de um parâmetro específico no corpo de uma POST.

Para ativar o recurso, defina o `csrfToken`parâmetro como `true` durante a autenticação. O padrão é `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"
```

Quando verdadeiro, um cookie `GridCsrfToken` é definido com um valor aleatório para autenticações no Grid Manager, e o cookie `AccountCsrfToken` é definido com um valor aleatório para autenticações no Tenant Manager.

Se o cookie estiver presente, todas as solicitações que podem modificar o estado do sistema (POST, PUT, PATCH, DELETE) devem incluir um dos seguintes:

- O `X-Csrf-Token`cabeçalho, com o valor do cabeçalho definido como o valor do cookie do token CSRF.
- Para endpoints que aceitam um corpo codificado em formulário: um `csrfToken`parâmetro de corpo de requisição codificado em formulário.

Consulte a documentação da API online para obter exemplos e detalhes adicionais.

> As solicitações que possuem um cookie de token CSRF definido também imporão o cabeçalho "Content-Type: application/json" para qualquer solicitação que espere um corpo de solicitação JSON como proteção adicional contra ataques CSRF.

Use a API se o single sign-on estiver ativado

Use a API do StorageGRID se o logon único estiver habilitado (Active Directory)

Se você tem "configurou e ativou o single sign-on (SSO)" e utiliza o Active Directory como provedor de SSO, é necessário emitir uma série de solicitações de API para obter um token de autenticação válido para a Grid Management API ou a Tenant Management API.

Faça login na API se o single sign-on estiver ativado

Estas instruções se aplicam se você estiver usando o Active Directory como provedor de identidade SSO.

Antes de começar

- Você conhece o nome de usuário e a senha do SSO de um usuário federado que pertence a um grupo de usuários do StorageGRID.
- Se você deseja acessar a API de Gerenciamento de Tenant, você sabe o ID da conta do tenant.

Sobre esta tarefa

Para obter um token de autenticação, você pode usar um dos seguintes exemplos:

- O `storagegrid-ssoauth.py`script Python, que está localizado no diretório de arquivos de instalação do StorageGRID (./rpms`para RHEL, `./debs`para Ubuntu ou Debian, e

`./vsphere`para VMware).

- Um exemplo de fluxo de trabalho com requisições curl.

  O fluxo de trabalho curl pode expirar se você o executar muito lentamente. Você poderá ver o erro: `A valid SubjectConfirmation was not found on this Response`.

  > O fluxo de trabalho curl de exemplo não protege a senha de ser vista por outros usuários.

Se você tiver um problema de codificação de URL, poderá ver o seguinte erro: `Unsupported SAML version`.

Passos

1. Selecione um dos seguintes métodos para obter um token de autenticação:
   - Use o `storagegrid-ssoauth.py`script Python. Vá para o passo 2.
   - Use requisições curl. Vá para o passo 3.
2. Se você quiser usar o `storagegrid-ssoauth.py`script, passe o script para o interpretador Python e execute o script.

   Quando solicitado, insira valores para os seguintes argumentos:

   - O método SSO. Digite ADFS ou adfs.
   - O nome de usuário SSO
   - O domínio onde StorageGRID está instalado
   - O endereço do StorageGRID
   - O ID da conta do locatário, caso você queira acessar a Tenant Management API.

   ```
   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
   ```

   O token de autorização do StorageGRID é fornecido na saída. Agora você pode usar o token para outras solicitações, de forma semelhante a como usaria a API se o SSO não estivesse sendo utilizado.

3. Se você deseja usar solicitações curl, use o procedimento a seguir.

   a. Declare as variáveis necessárias para efetuar o login.

```
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 acessar a API de Gerenciamento de Grid, use 0 como `TENANTACCOUNTID`.

b. Para receber uma URL de autenticação assinada, envie uma solicitação POST para `/api/v3/authorize-saml` e remova a codificação JSON adicional da resposta.

Este exemplo mostra uma solicitação POST para uma URL de autenticação assinada para `TENANTACCOUNTID`. Os resultados serão passados para `python -m json.tool` para remover a codificação 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
```

A resposta para este exemplo inclui uma URL assinada que está codificada em URL, mas não inclui a camada adicional de codificação 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. Salve o `SAMLRequest` da resposta para uso em comandos subsequentes.

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

d. Obtenha uma URL completa que inclua o ID da solicitação do cliente do AD FS.

Uma opção é solicitar o formulário de login usando a URL da resposta anterior.

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

A resposta inclui o ID da solicitação do 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. Salve o ID da solicitação do cliente a partir da resposta.

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

f. Envie suas credenciais para a ação do formulário da resposta 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
```

O AD FS retorna um redirecionamento 302, com informações adicionais nos cabeçalhos.

> Se a autenticação multifator (MFA) estiver habilitada para o seu sistema SSO, o formulário enviado também conterá a segunda senha ou outras credenciais.

```
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. Salve o `MSISAuth`cookie da resposta.

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

h. Envie uma solicitação GET para o local especificado com os cookies da autenticação POST.

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

Os cabeçalhos da resposta conterão informações da sessão do AD FS para uso posterior no logout, e o corpo da resposta conterá o SAMLResponse em um campo de formulário 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. Salve o `SAMLResponse` do campo oculto:

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

j. Utilizando o valor salvo `SAMLResponse`, faça uma solicitação StorageGRID `/api/saml-response`

para gerar um token de autenticação do StorageGRID.

Para `RelayState`, use o ID da conta do tenant ou use 0 se você quiser fazer login na Grid Management API.

```
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
```

A resposta inclui o token de autenticação.

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

a. Salve o token de autenticação na resposta como `MYTOKEN`.

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

Agora você pode usar `MYTOKEN` para outras solicitações, de forma semelhante a como usaria a API se o SSO não estivesse sendo utilizado.

Saia da API se o single sign-on estiver ativado

Se o login único (SSO) estiver habilitado, você deve emitir uma série de solicitações de API para sair da Grid Management API ou da Tenant Management API. Essas instruções se aplicam se você estiver usando Active Directory como provedor de identidade SSO

Sobre esta tarefa

Caso necessário, você pode sair da StorageGRID API fazendo logout na página de logout único da sua organização. Ou, você pode acionar o logout único (SLO) a partir do StorageGRID, o que requer um token de portador StorageGRID válido.

Passos

1. Para gerar uma solicitação de logout assinada, passe o cookie `sso=true` para a API SLO:

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

Uma URL de logout é retornada:

```
{
    "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. Salve a URL de logout.

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

3. Envie uma solicitação para o URL de logout para acionar o SLO e redirecionar de volta para StorageGRID.

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

A resposta 302 é retornada. O local de redirecionamento não se aplica ao logout somente via 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. Exclua o token de portador do StorageGRID.

Excluir o token de portador do StorageGRID funciona da mesma forma que sem SSO. Se o cookie `sso=true` não for fornecido, o usuário será desconectado do StorageGRID sem afetar o estado do SSO.

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

Uma `204 No Content`resposta indica que o usuário agora está desconectado.

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

Use a API do StorageGRID se o single sign-on estiver ativado (Entra ID)

Se você possui "configurou e ativou o single sign-on (SSO)" e utiliza o Entra ID como provedor de SSO, pode usar dois scripts de exemplo para obter um token de autenticação válido para a Grid Management API ou para a Tenant Management API.

Faça login na API se o single sign-on do Entra ID estiver ativado

Estas instruções se aplicam se você estiver usando o Entra ID como provedor de identidade SSO

Antes de começar

- Você conhece o endereço de e-mail e a senha de SSO de um usuário federado que pertence a um grupo de usuários do StorageGRID.
- Se você deseja acessar a API de Gerenciamento de Tenant, você sabe o ID da conta do tenant.

Sobre esta tarefa

Para obter um token de autenticação, você pode usar os seguintes scripts de exemplo:

- O `storagegrid-ssoauth-azure.py`script Python
- O `storagegrid-ssoauth-azure.js` script Node.js

Ambos os scripts estão localizados no diretório de arquivos de instalação do StorageGRID (`./rpms` para RHEL, `./debs` para Ubuntu ou Debian, e `./vsphere` para VMware.

Para criar sua própria integração de API com o Entra ID, consulte o `storagegrid-ssoauth-azure.py`script. O script em Python faz duas requisições diretamente ao StorageGRID (primeiro para obter o SAMLRequest e, posteriormente, para obter o token de autorização) e também chama o script em Node.js para interagir com o Entra ID e realizar as operações de SSO.

As operações de SSO podem ser executadas usando uma série de solicitações de API, mas isso não é trivial. O módulo Puppeteer para Node.js é usado para extrair dados da interface Entra ID SSO.

Se você tiver um problema de codificação de URL, poderá ver o seguinte erro: `Unsupported SAML version`.

Passos

1. Instale as dependências necessárias, conforme a seguir:

a. Instale o Node.js (consulte "https://nodejs.org/en/download/").

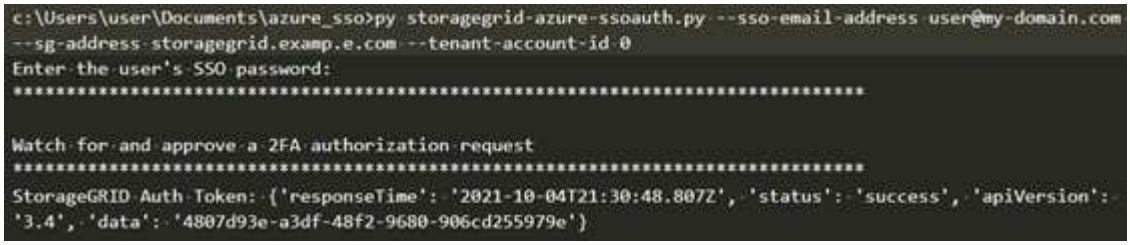
b. Instale os módulos Node.js necessários (puppeteer e jsdom):

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

2. Passe o script Python para o interpretador Python para executar o script.

   O script Python então chamará o script Node.js correspondente para executar as interações de SSO do Entra ID.

3. Quando solicitado, insira os valores para os seguintes argumentos (ou passe-os usando parâmetros):
   - O endereço de e-mail SSO usado para fazer login no Entra ID
   - O endereço do StorageGRID
   - O ID da conta do locatário, caso você queira acessar a API de gerenciamento de locatários
4. Quando solicitado, insira a senha e esteja preparado para fornecer uma autorização MFA ao Entra ID, caso seja solicitado.



> O script pressupõe que a autenticação multifator (MFA) seja feita usando o Microsoft Authenticator. Pode ser necessário modificar o script para suportar outras formas de MFA (como inserir um código recebido por mensagem de texto).

O token de autorização do StorageGRID é fornecido na saída. Agora você pode usar o token para outras solicitações, de forma semelhante a como usaria a API se o SSO não estivesse sendo utilizado.

Use a API do StorageGRID se o login único estiver ativado (PingFederate)

Se você tem "configurou e ativou o single sign-on (SSO)" e utiliza PingFederate como provedor de SSO, é necessário emitir uma série de solicitações de API para obter um token de autenticação válido para a Grid Management API ou a Tenant Management API.

Faça login na API se o single sign-on estiver ativado

Estas instruções se aplicam se você estiver usando PingFederate como o provedor de identidade SSO

Antes de começar

- Você conhece o nome de usuário e a senha do SSO de um usuário federado que pertence a um grupo de usuários do StorageGRID.
- Se você deseja acessar a API de Gerenciamento de Tenant, você sabe o ID da conta do tenant.

Sobre esta tarefa

Para obter um token de autenticação, você pode usar um dos seguintes exemplos:

- O `storagegrid-ssoauth.py`script Python, que está localizado no diretório de arquivos de instalação do StorageGRID (./rpms`para RHEL, `./debs`para Ubuntu ou Debian, e `./vsphere`para VMware).
- Um exemplo de fluxo de trabalho com requisições curl.

  O fluxo de trabalho curl pode expirar se você o executar muito lentamente. Você poderá ver o erro: `A valid SubjectConfirmation was not found on this Response`.

  > O fluxo de trabalho curl de exemplo não protege a senha de ser vista por outros usuários.

  Se você tiver um problema de codificação de URL, poderá ver o seguinte erro: `Unsupported SAML version`.

Passos

1. Selecione um dos seguintes métodos para obter um token de autenticação:
   - Use o `storagegrid-ssoauth.py`script Python. Vá para o passo 2.
   - Use requisições curl. Vá para o passo 3.
2. Se você quiser usar o `storagegrid-ssoauth.py`script, passe o script para o interpretador Python e execute o script.

   Quando solicitado, insira valores para os seguintes argumentos:

   - O método SSO. Você pode inserir qualquer variação de "pingfederate" (PINGFEDERATE, pingfederate e assim por diante).
   - O nome de usuário SSO
   - O domínio onde StorageGRID está instalado. Este campo não é utilizado para PingFederate. Você pode deixá-lo em branco ou inserir qualquer valor.
   - O endereço do StorageGRID
   - O ID da conta do locatário, caso você queira acessar a Tenant Management API.

   ```
   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
   ```

   O token de autorização do StorageGRID é fornecido na saída. Agora você pode usar o token para outras solicitações, de forma semelhante a como usaria a API se o SSO não estivesse sendo utilizado.
3. Se você deseja usar solicitações curl, use o procedimento a seguir.

a. Declare as variáveis necessárias para efetuar o login.

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

> Para acessar a API de Gerenciamento de Grid, use 0 como `TENANTACCOUNTID`.

b. Para receber uma URL de autenticação assinada, envie uma solicitação POST para `/api/v3/authorize-saml` e remova a codificação JSON adicional da resposta.

Este exemplo mostra uma solicitação POST para uma URL de autenticação assinada para TENANTACCOUNTID. Os resultados serão passados para python -m json.tool para remover a codificação 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
```

A resposta para este exemplo inclui uma URL assinada que está codificada em URL, mas não inclui a camada adicional de codificação JSON.

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

c. Salve o `SAMLRequest` da resposta para uso em comandos subsequentes.

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

d. Exporte a resposta e o cookie e exiba a resposta:

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

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

e. Exporte o valor "pf.adapterId" e exiba a resposta:

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

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

f. Exporte o valor 'href' (remova a barra final /) e exiba a resposta:

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

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

g. Exporte o valor de "ação":

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

h. Enviar cookies juntamente com credenciais:

```
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. Salve o `SAMLResponse` do campo oculto:

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

j. Utilizando o valor salvo `SAMLResponse`, faça uma solicitação StorageGRID `/api/saml-response` para gerar um token de autenticação do StorageGRID.

   Para `RelayState`, use o ID da conta do tenant ou use 0 se você quiser fazer login na Grid Management API.

```
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
```

A resposta inclui o token de autenticação.

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

a. Salve o token de autenticação na resposta como `MYTOKEN`.

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

Agora você pode usar `MYTOKEN` para outras solicitações, de forma semelhante a como usaria a API se o SSO não estivesse sendo utilizado.

Saia da API se o single sign-on estiver ativado

Se o login único (SSO) estiver habilitado, você deve emitir uma série de solicitações de API para sair da API de Gerenciamento de Grid ou da API de Gerenciamento de Locatários. Essas instruções se aplicam se você estiver usando PingFederate como provedor de identidade SSO

Sobre esta tarefa

Caso necessário, você pode sair da StorageGRID API fazendo logout na página de logout único da sua organização. Ou, você pode acionar o logout único (SLO) a partir do StorageGRID, o que requer um token de portador StorageGRID válido.

Passos

1. Para gerar uma solicitação de logout assinada, passe o cookie `sso=true` para a API SLO:

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

Uma URL de logout é retornada:

```
{
    "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. Salve a URL de logout.

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

3. Envie uma solicitação para o URL de logout para acionar o SLO e redirecionar de volta para StorageGRID.

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

A resposta 302 é retornada. O local de redirecionamento não se aplica ao logout somente via 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. Exclua o token de portador do StorageGRID.

Excluir o token de portador do StorageGRID funciona da mesma forma que sem SSO. Se o cookie `sso=true` não for fornecido, o usuário será desconectado do StorageGRID sem afetar o estado do SSO.

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

Uma `204 No Content`resposta indica que o usuário agora está desconectado.

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

Desative os recursos do StorageGRID com a API

Você pode usar a API de Gerenciamento de Grid para desativar completamente certos recursos no sistema StorageGRID. Quando um recurso é desativado, ninguém pode receber permissões para executar as tarefas relacionadas a esse recurso.

Sobre esta tarefa

O sistema de Recursos Desativados permite impedir o acesso a determinados recursos no sistema StorageGRID. Desativar um recurso é a única maneira de impedir que o usuário raiz ou usuários pertencentes a grupos de administradores com permissão de **acesso à raiz** possam usar esse recurso.

Para entender como essa funcionalidade pode ser útil, considere o seguinte cenário:

A Company A é uma prestadora de serviços que aluga a capacidade de storage do seu sistema StorageGRID criando contas de locatário. Para proteger a segurança dos objetos dos seus locatários, a Company A deseja garantir que seus próprios funcionários nunca possam acessar nenhuma conta de locatário após a implantação da conta.

A Company A pode atingir esse objetivo usando o sistema Deactivate Features na Grid Management API. Ao desativar completamente o recurso **Change tenant root password** no Grid Manager (tanto na interface de usuário quanto na API), a Company A garante que usuários Admin — incluindo o usuário raiz e usuários pertencentes a grupos com a permissão **Root access** — não possam alterar a senha do usuário raiz de nenhuma conta de tenant.

Passos

1. Acesse a documentação Swagger para a API de Gerenciamento de Grid. Veja "Use a API de gerenciamento de grid".
2. Localize o endpoint Desativar recursos.
3. Para desativar um recurso, como Alterar a senha raiz do locatário, envie um corpo para a API assim:

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

   Quando a solicitação for concluída, o recurso Alterar senha raiz do locatário será desativado. A permissão de gerenciamento **Alterar senha raiz do locatário** não aparece mais na interface de usuário, e qualquer solicitação de API que tente alterar a senha raiz de um locatário falha com "403 Forbidden".

Reativar funcionalidades desativadas

Por padrão, você pode usar a API de Gerenciamento de Grid para reativar um recurso que foi desativado. No entanto, se você quiser impedir que recursos desativados sejam reativados, você pode desativar o recurso **activateFeatures**.

> O recurso **activateFeatures** não pode ser reativado. Se você decidir desativar este recurso, esteja ciente de que perderá permanentemente a capacidade de reativar quaisquer outros recursos desativados. Você deve entrar em contato com o suporte técnico para restaurar qualquer funcionalidade perdida.

Passos

1. Acesse a documentação Swagger para a API de gerenciamento de Grid.
2. Localize o endpoint Desativar recursos.

3. Para reativar todas as funcionalidades, envie um corpo para a API da seguinte forma:

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

Quando esta solicitação for concluída, todos os recursos, incluindo o recurso Alterar senha raiz do locatário, serão reativados. A permissão de gerenciamento **Alterar senha raiz do locatário** agora aparece na interface de usuário, e qualquer solicitação de API que tente alterar a senha raiz de um locatário será bem-sucedida, assumindo que o usuário tenha a permissão de gerenciamento **Acesso à raiz** ou **Alterar senha raiz do locatário**.

O exemplo anterior faz com que *todos* os recursos desativados sejam reativados. Se outros recursos foram desativados e devem permanecer desativados, você deve especificá-los explicitamente na solicitação PUT. Por exemplo, para reativar o recurso Alterar senha raiz do locatário e continuar a desativar a permissão de gerenciamento storageAdmin, envie esta solicitação PUT: `{ "grid": {"storageAdmin": true} }`

Informações sobre direitos autorais

Informações sobre marcas comerciais