Use a API

StorageGRID software

NetApp
December 03, 2025

Índice

Use a API

Use a API de gerenciamento de grade

Você pode executar tarefas de gerenciamento do sistema usando a API REST do Grid Management 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 nível superior

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

- `/grid`: O acesso é restrito aos usuários do Grid Manager e é baseado 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 inquilino" .
- `/private`: O acesso é restrito aos 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 grade usa 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 do Swagger fornece detalhes completos e documentação para cada operação de API.

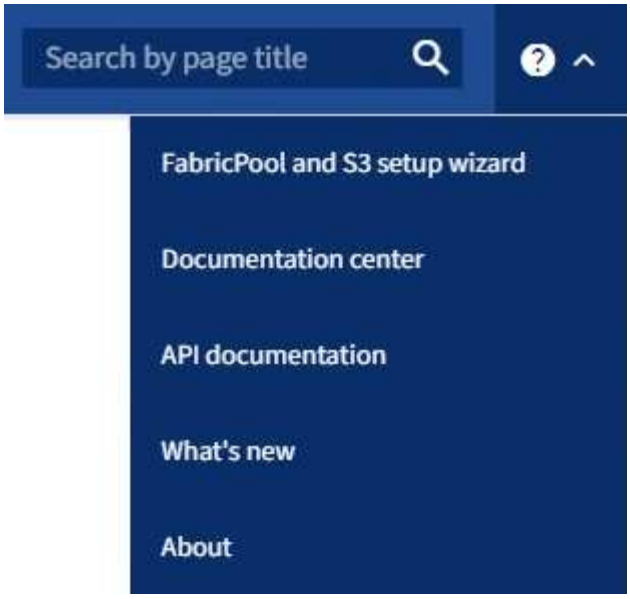
Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem"permissões de acesso específicas" .

> Todas as operações de API que você realiza usando a página de documentação da API são operações ativas. Tenha cuidado para não criar, atualizar ou excluir dados de configuração ou outros dados por engano.

Passos

1. No cabeçalho do Grid Manager, selecione o ícone de ajuda e selecione **Documentação da API**.



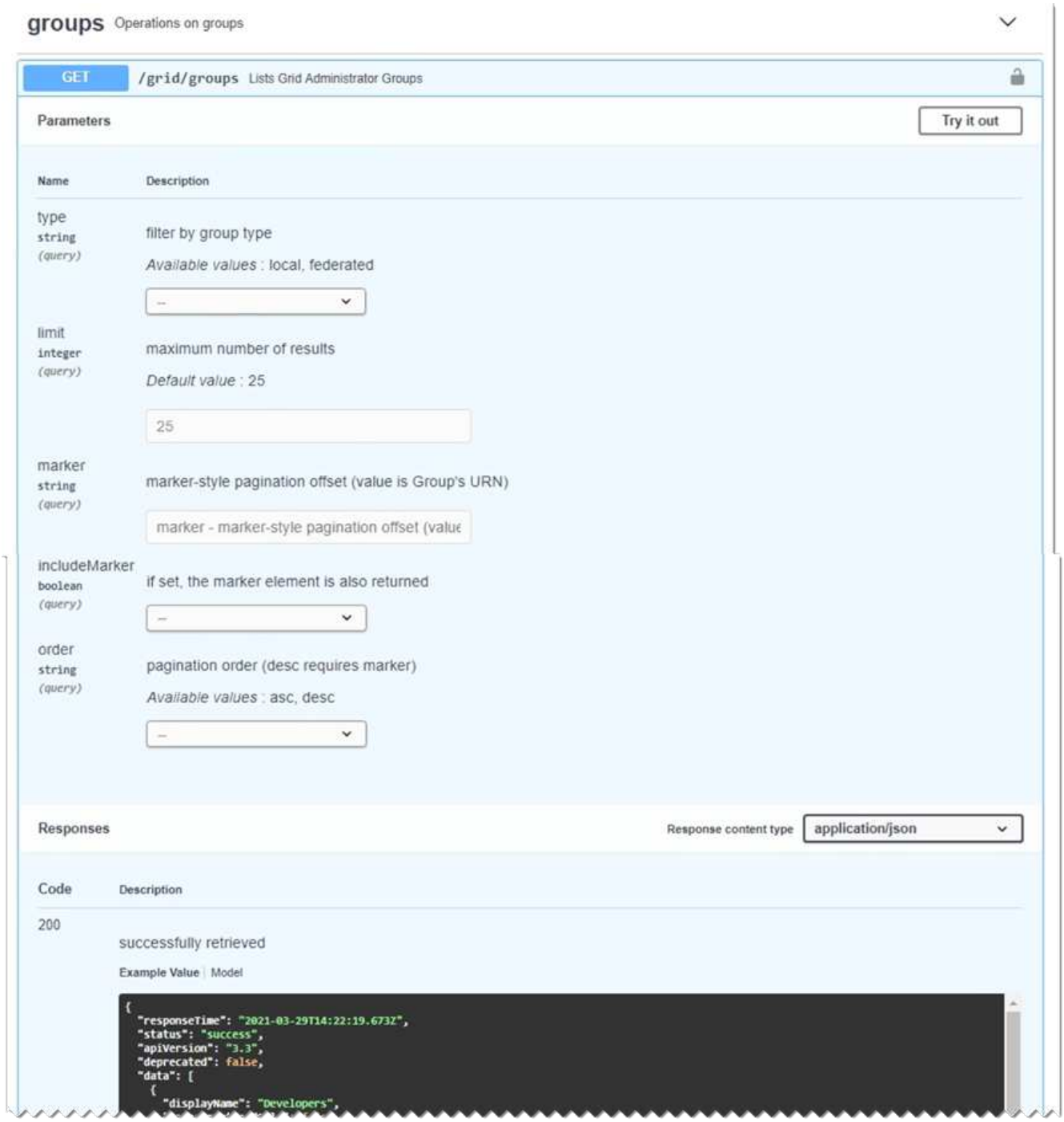
2. Para executar uma operação com a API privada, selecione **Ir para a documentação da API privada** na página da API de gerenciamento do StorageGRID .

   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 de API, você pode ver as ações HTTP disponíveis, como GET, PUT, UPDATE e DELETE.

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



5. Determine se a solicitação requer parâmetros adicionais, como um ID de grupo ou usuário. Então, obtenha esses valores. Talvez seja necessário emitir uma solicitação de API diferente primeiro para obter as informações necessárias.
6. Determine se você precisa modificar o corpo da solicitação de exemplo. Se sim, você pode selecionar **Modelo** para saber os requisitos de cada campo.
7. Selecione **Experimentar**.
8. Forneça quaisquer parâmetros necessários ou modifique o corpo da solicitação conforme necessário.
9. Selecione **Executar**.
10. Revise o código de resposta para determinar se a solicitação foi bem-sucedida.

Operações da API de gerenciamento de grade

A API de gerenciamento de grade organiza as operações disponíveis nas seguintes seções.

Esta lista inclui apenas operações disponíveis na API pública.

- **contas**: Operações para gerenciar contas de locatários de armazenamento, incluindo a criação de novas contas e a recuperação do uso de armazenamento para uma determinada conta.
- **alert-history**: Operações em alertas resolvidos.
- **alert-receivers**: Operações em receptores de notificação de alerta (e-mail).
- **alert-rules**: Operações em regras de alerta.
- **alert-silences**: Operações em silêncios de alerta.
- **alertas**: Operações em alertas.
- **audit**: Operações para listar e atualizar a configuração de auditoria.
- **auth**: Operações para realizar autenticação de sessão do usuário.

  A API de gerenciamento de grade oferece suporte ao esquema de autenticação de token de portador. 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. Este token deve ser fornecido no cabeçalho de solicitações de API subsequentes ("Autorização: Token do portador"). O token expira após 16 horas.

  Se o logon único estiver habilitado para o sistema StorageGRID , você deverá executar etapas diferentes para autenticar. Consulte "Autenticação na API se o logon único estiver habilitado".

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

- **client-certificates**: Operações para configurar certificados de cliente para que o StorageGRID possa ser acessado com segurança usando ferramentas de monitoramento externas.
- **config**: Operações relacionadas ao lançamento do produto e versões da API de gerenciamento de grade. Você pode listar a versão de lançamento do produto e as principais versões da API de gerenciamento de grade suportadas por essa versão, além de desabilitar versões obsoletas da API.
- **deactivated-features**: Operações para visualizar recursos que podem ter sido desativados.
- **dns-servers**: Operações para listar e alterar servidores DNS externos configurados.
- **drive-details**: Operações em unidades para modelos específicos de dispositivos de armazenamento.
- **endpoint-domain-names**: Operações para listar e alterar nomes de domínio de endpoint S3.
- **erasure-coding**: Operações em perfis de codificação de apagamento.
- **expansão**: Operações de expansão (nível de procedimento).
- **expansion-nodes**: Operações de expansão (nível de nó).
- **expansion-sites**: Operações de expansão (nível de site).
- **grid-networks**: Operações para listar e alterar a Lista de Redes de Grade.

- **grid-passwords**: Operações para gerenciamento de senhas de grade.
- **grupos**: Operações para gerenciar grupos de administradores de grade locais e recuperar grupos de administradores de grade federados de um servidor LDAP externo.
- **identity-source**: Operações para configurar uma fonte de identidade externa e sincronizar manualmente informações de grupos federados e usuários.
- **ilm**: Operações em gerenciamento do ciclo de vida da informação (ILM).
- **in-progress-procedures**: Recupera os procedimentos de manutenção que estão em andamento.
- **licença**: Operações para recuperar e atualizar a licença do StorageGRID .
- **logs**: Operações para coleta e download de arquivos de log.v
- **métricas**: Operações em métricas do StorageGRID , incluindo consultas de métricas instantâneas em um único ponto no tempo e consultas de métricas de intervalo ao longo de um intervalo de tempo. A API de gerenciamento de grade usa a ferramenta de monitoramento de sistemas Prometheus como fonte de dados de backend. Para obter informações sobre como construir consultas do Prometheus, consulte o site do Prometheus.

> ⓘ Métricas que incluem `private` em seus nomes são destinados apenas para uso interno. Essas métricas estão sujeitas a alterações entre as versões do StorageGRID sem aviso prévio.

- **node-details**: Operações em 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 de Protocolo de Tempo de Rede (NTP).
- **objetos**: Operações em objetos e metadados de objetos.
- **recuperação**: Operações para o procedimento de recuperação.
- **recovery-package**: Operações para baixar o pacote de recuperação.
- **regiões**: Operações para visualizar e criar regiões.
- **s3-object-lock**: Operações nas configurações globais de bloqueio de objetos do S3.
- **server-certificate**: Operações para visualizar e atualizar certificados do servidor do Grid Manager.
- **snmp**: Operações na configuração SNMP atual.
- **storage-watermarks**: Marcas d'água do nó de armazenamento.
- **traffic-classes**: Operações para políticas de classificação de tráfego.
- **untrusted-client-network**: Operações na configuração de rede de cliente não confiável.
- **usuários**: Operações para visualizar e gerenciar usuários do Grid Manager.

Controle de versão da API de gerenciamento de grade

A API de gerenciamento de grade usa controle de versão para oferecer suporte a atualizações sem interrupções.

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 alterada quando são feitas alterações que *não são compatíveis* com versões mais antigas. A versão secundária da API é alterada quando são feitas alterações que *são compatíveis* com versões mais antigas. Alterações compatíveis incluem a adição de novos pontos de extremidade ou novas propriedades.

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

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

Quando você instala o software StorageGRID pela primeira vez, somente a versão mais recente da API é habilitada. No entanto, ao atualizar para uma nova versão de recurso do StorageGRID, você continua tendo acesso à versão mais antiga da API para pelo menos uma versão de recurso do StorageGRID .

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

Solicitações desatualizadas são marcadas como obsoletas das seguintes maneiras:

- O cabeçalho de resposta é "Obsoleto: verdadeiro"
- O corpo da resposta JSON inclui "deprecated": true
- Um aviso obsoleto foi adicionado ao nms.log. Por exemplo:

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

Determinar quais versões de API são suportadas na versão atual

Use o `GET /versions` Solicitação de API para retornar uma lista das principais versões de API suportadas. Esta solicitação está localizada na seção **config** da documentação da API do 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 de 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 substituirá o valor do caminho.

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

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

Proteja-se contra falsificação de solicitação entre sites (CSRF)

Você pode ajudar a proteger contra ataques de falsificação de solicitação entre sites (CSRF) contra o StorageGRID usando tokens CSRF para aprimorar a autenticação que usa 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 efetuar login.

Um invasor que pode disparar uma solicitação para um site diferente (como com um formulário HTTP POST) pode fazer com que certas solicitações sejam feitas usando os cookies do usuário conectado.

O 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 de corpo POST específico.

Para habilitar o recurso, defina o `csrfToken` parâmetro para `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 `GridCsrfToken` O cookie é definido com um valor aleatório para logins no Grid Manager e o `AccountCsrfToken` O cookie é definido com um valor aleatório para logins 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 terminais que aceitam um corpo codificado em formulário: A `csrfToken` parâmetro do corpo da solicitação codificado em formulário.

Consulte a documentação da API on-line para obter exemplos e detalhes adicionais.

> Solicitações que tenham um cookie de token CSRF definido também aplicarão 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 logon único estiver habilitado

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

Se você tem"configurou e habilitou o logon único (SSO)" e você usa o Active Directory como o provedor de SSO, você deve emitir uma série de solicitações de API para obter um token de autenticação válido para a API de gerenciamento de grade ou a API de gerenciamento de locatários.

Sign in na API se o logon único estiver habilitado

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

Antes de começar

- Você sabe o nome de usuário e a senha do SSO para um usuário federado que pertence a um grupo de usuários do StorageGRID .
- Se você quiser acessar a API de gerenciamento de locatários, saiba o ID da conta do locatário.

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 Red Hat Enterprise Linux, `./debs` para Ubuntu ou Debian, e `./vsphere`

para VMware).

- Um exemplo de fluxo de trabalho de solicitações curl.

  O fluxo de trabalho do curl pode expirar se você o executar muito lentamente. Você pode 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 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 solicitações curl. Vá para a etapa 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 do SSO
   - O domínio onde o StorageGRID está instalado
   - O endereço para StorageGRID
   - O ID da conta do locatário, se você quiser acessar a API de gerenciamento de locatários.

   ```
   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 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 usado.

3. Se você quiser usar solicitações curl, use o seguinte procedimento.

   a. Declare as variáveis necessárias para fazer 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 grade, use 0 como `TENANTACCOUNTID` .

b. Para receber uma URL de autenticação assinada, emita 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 repassados 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 é codificada por 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 de solicitação do cliente do AD FS.

Uma opção é solicitar o formulário de login usando o 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 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 seu sistema SSO, a postagem do formulário 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 do POST de autenticação.

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

Os cabeçalhos de resposta conterão informações de sessão do AD FS para uso posterior em caso de 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. Usando o salvo `SAMLResponse` , faça um StorageGRID`/api/saml-response` solicitação para gerar

um token de autenticação StorageGRID .

Para `RelayState` , use o ID da conta do locatário ou use 0 se quiser fazer login na API de gerenciamento de grade.

```
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, semelhante a como você usaria a API se o SSO não estivesse sendo usado.

Sair da API se o logon único estiver habilitado

Se o logon único (SSO) estiver habilitado, você deverá emitir uma série de solicitações de API para sair da API de gerenciamento de grade ou da API de gerenciamento de locatários. Estas instruções se aplicam se você estiver usando o Active Directory como provedor de identidade SSO

Sobre esta tarefa

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

Passos

1. Para gerar uma solicitação de logout assinada, passe `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
```

Um URL de logout é retornado:

```
{
    "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 o 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 o StorageGRID.

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

A resposta 302 é retornada. O local de redirecionamento não se aplica ao logout somente da 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 portador do StorageGRID .

A exclusão do token portador do StorageGRID funciona da mesma forma que sem o SSO. Se `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
```

UM `204 No Content` a resposta indica que o usuário está desconectado.

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

Use a API se o logon único estiver habilitado (Azure)

Se você tem"configurou e habilitou o logon único (SSO)" e você usa o Azure como o provedor de SSO, você pode usar dois scripts de exemplo para obter um token de autenticação válido para a API de Gerenciamento de Grade ou a API de Gerenciamento de Locatários.

Sign in na API se o logon único do Azure estiver habilitado

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

Antes de começar

- Você sabe o endereço de e-mail e a senha do SSO de um usuário federado que pertence a um grupo de usuários do StorageGRID .
- Se você quiser acessar a API de gerenciamento de locatários, saiba o ID da conta do locatário.

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 Red Hat Enterprise Linux, `./debs` para Ubuntu ou Debian, e `./vsphere` para VMware).

Para escrever sua própria integração de API com o Azure, consulte o `storagegrid-ssoauth-azure.py` roteiro. O script Python faz duas solicitações diretamente ao StorageGRID (primeiro para obter o SAMLRequest e depois para obter o token de autorização) e também chama o script Node.js para interagir com o Azure para executar as operações de SSO.

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

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

Passos

1. Instale as dependências necessárias, da seguinte forma:

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

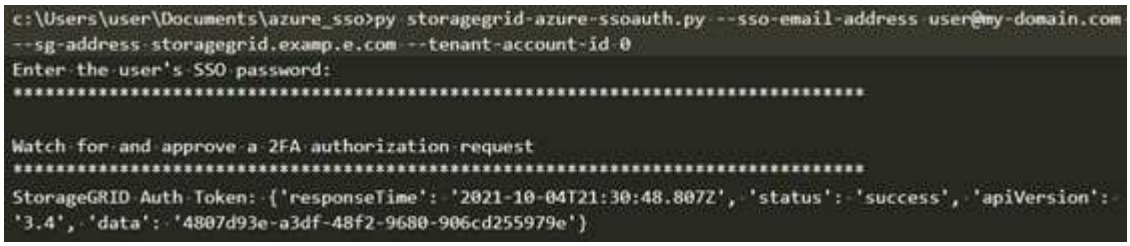
b. Instale os módulos Node.js necessários (puppeteer e jsdom):

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

2. Passe o script Python para o interpretador Python para executá-lo.

   O script Python chamará o script Node.js correspondente para executar as interações do Azure SSO.

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



> O script pressupõe que o MFA seja feito usando o Microsoft Authenticator. Talvez seja necessário modificar o script para oferecer suporte a outras formas de MFA (como inserir um código recebido em uma mensagem de texto).

O token de autorização 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 usado.

Use a API se o logon único estiver habilitado (PingFederate)

Se você tem"configurou e habilitou o logon único (SSO)" e você usa o PingFederate como provedor de SSO, você deve emitir uma série de solicitações de API para obter um token de autenticação válido para a API de gerenciamento de grade ou a API de gerenciamento de locatários.

Sign in na API se o logon único estiver habilitado

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

Antes de começar

- Você sabe o nome de usuário e a senha do SSO para um usuário federado que pertence a um grupo de usuários do StorageGRID .
- Se você quiser acessar a API de gerenciamento de locatários, saiba o ID da conta do locatário.

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 Red Hat Enterprise Linux, `./debs` para Ubuntu ou Debian, e `./vsphere` para VMware).
- Um exemplo de fluxo de trabalho de solicitações curl.

  O fluxo de trabalho do curl pode expirar se você o executar muito lentamente. Você pode 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 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 solicitações curl. Vá para a etapa 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 do SSO
   - O domínio onde o StorageGRID está instalado. Este campo não é usado para PingFederate. Você pode deixar em branco ou inserir qualquer valor.
   - O endereço para StorageGRID
   - O ID da conta do locatário, se você quiser acessar a API de gerenciamento de locatários.

   ```
   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 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 usado.
3. Se você quiser usar solicitações curl, use o seguinte procedimento.
   a. Declare as variáveis necessárias para fazer 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 grade, use 0 como `TENANTACCOUNTID` .

b. Para receber uma URL de autenticação assinada, emita 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 é codificada por 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 faça eco da resposta:

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

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

e. Exporte o valor 'pf.adapterId' e repita a resposta:

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

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

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

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

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

g. Exporte o valor 'action':

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

h. Enviar cookies junto com as 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. Usando o salvo `SAMLResponse` , faça um StorageGRID `/api/saml-response` solicitação para gerar um token de autenticação StorageGRID .

Para `RelayState` , use o ID da conta do locatário ou use 0 se quiser fazer login na API de gerenciamento de grade.

```
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, semelhante a como você usaria a API se o SSO não estivesse sendo usado.

Sair da API se o logon único estiver habilitado

Se o logon único (SSO) estiver habilitado, você deverá emitir uma série de solicitações de API para sair da API de gerenciamento de grade ou da API de gerenciamento de locatários. Estas instruções se aplicam se você estiver usando o PingFederate como provedor de identidade SSO

Sobre esta tarefa

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

Passos

1. Para gerar uma solicitação de logout assinada, passe `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
```

Um URL de logout é retornado:

```
{
    "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 o 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 o StorageGRID.

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

A resposta 302 é retornada. O local de redirecionamento não se aplica ao logout somente da 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 portador do StorageGRID .

A exclusão do token portador do StorageGRID funciona da mesma forma que sem o SSO. Se `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
```

UM `204 No Content` a resposta indica que o usuário está desconectado.

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

Desativar recursos com a API

Você pode usar a API de gerenciamento de grade para desativar completamente determinados 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 Recursos Desativados permite que você impeça o acesso a determinados recursos no sistema StorageGRID . Desativar um recurso é a única maneira de impedir que o usuário root ou usuários que pertencem a grupos de administradores com permissão de **acesso root** possam usar esse recurso.

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

_A Empresa A é uma provedora de serviços que aluga a capacidade de armazenamento do seu sistema StorageGRID criando contas de locatário. Para proteger a segurança dos objetos de seus locatários, a Empresa A quer garantir que seus próprios funcionários nunca possam acessar nenhuma conta de locatário após a conta ter sido implantada.

_A empresa A pode atingir esse objetivo usando o sistema Desativar recursos na API de gerenciamento de grade. Ao desativar completamente o recurso **Alterar senha raiz do locatário** no Grid Manager (tanto na IU quanto na API), a Empresa A garante que os usuários administradores — incluindo o usuário raiz e os usuários pertencentes a grupos com a permissão **Acesso raiz** — não possam alterar a senha de nenhum usuário raiz da conta do locatário.

Passos

1. Acesse a documentação do Swagger para a API de gerenciamento de grade. Ver "Use a API de gerenciamento de grade" .
2. Localize o ponto de extremidade Desativar recursos.
3. Para desativar um recurso, como Alterar senha raiz do locatário, envie um corpo para a API como este:

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

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

Reativar recursos desativados

Por padrão, você pode usar a API de gerenciamento de grade para reativar um recurso que foi desativado. Entretanto, se você quiser impedir que recursos desativados sejam reativados, você pode desativar o próprio 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 do Swagger para a API de gerenciamento de grade.
2. Localize o ponto de extremidade Desativar recursos.

3. Para reativar todos os recursos, envie um corpo para a API como este:

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

Quando essa 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 do usuário, e qualquer solicitação de API que tente alterar a senha raiz de um locatário será bem-sucedida, supondo que o usuário tenha a permissão de gerenciamento **Acesso raiz** ou **Alterar senha raiz do locatário**.

O exemplo anterior faz com que *todos* os recursos desativados sejam reativados. Se outros recursos que devem permanecer desativados tiverem sido desativados, você deverá 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