Utiliser la API

StorageGRID software

NetApp
December 03, 2025

Sommaire

Utiliser la API . . . 1
- Utiliser l’API de gestion de grille . . . 1
  - Ressources de haut niveau . . . 1
  - Émettre des requêtes API . . . 1
- Opérations de l’API de gestion de grille . . . 4
- Gestion des versions de l’API de gestion de grille . . . 5
  - Déterminer quelles versions d’API sont prises en charge dans la version actuelle . . . 6
  - Spécifier une version d’API pour une requête . . . 7
- Protection contre la falsification de requêtes intersites (CSRF) . . . 7
- Utiliser l’API si l’authentification unique est activée . . . 8
  - Utiliser l’API si l’authentification unique est activée (Active Directory) . . . 8
  - Utiliser l’API si l’authentification unique est activée (Azure) . . . 15
  - Utiliser l’API si l’authentification unique est activée (PingFederate) . . . 16
- Désactiver les fonctionnalités avec l’API . . . 22
  - Réactiver les fonctionnalités désactivées . . . 22

Utiliser la API

Utiliser l'API de gestion de grille

Vous pouvez effectuer des tâches de gestion du système à l'aide de l'API REST Grid Management au lieu de l'interface utilisateur Grid Manager. Par exemple, vous souhaiterez peut-être utiliser l'API pour automatiser des opérations ou créer plusieurs entités, telles que des utilisateurs, plus rapidement.

Ressources de haut niveau

L'API de gestion de grille fournit les ressources de niveau supérieur suivantes :

- `/grid`:L'accès est limité aux utilisateurs de Grid Manager et est basé sur les autorisations de groupe configurées.
- `/org`:L'accès est limité aux utilisateurs qui appartiennent à un groupe LDAP local ou fédéré pour un compte locataire. Pour plus de détails, consultez la section "Utiliser un compte locataire" .
- `/private`:L'accès est limité aux utilisateurs de Grid Manager et est basé sur les autorisations de groupe configurées. Les API privées sont susceptibles d'être modifiées sans préavis. Les points de terminaison privés StorageGRID ignorent également la version API de la demande.

Émettre des requêtes API

L'API de gestion de grille utilise la plate-forme API open source Swagger. Swagger fournit une interface utilisateur intuitive qui permet aux développeurs et aux non-développeurs d'effectuer des opérations en temps réel dans StorageGRID avec l'API.

L'interface utilisateur de Swagger fournit des détails complets et une documentation pour chaque opération API.

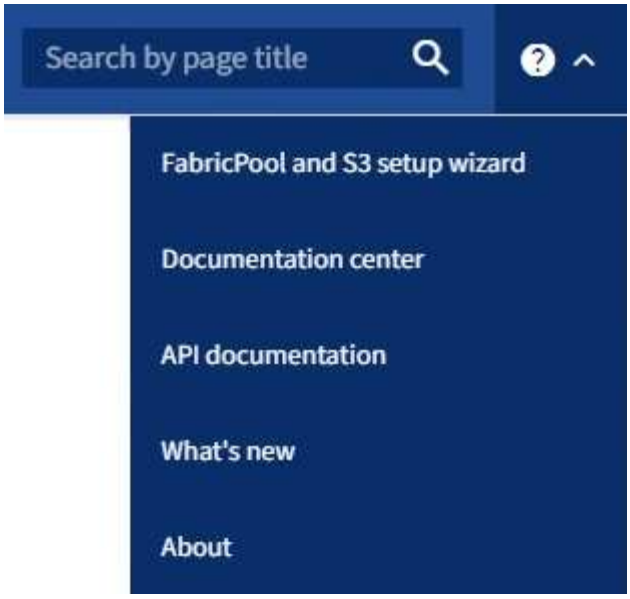
Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Tu as"autorisations d'accès spécifiques" .

> Toutes les opérations API que vous effectuez à l'aide de la page Web de documentation API sont des opérations en direct. Veillez à ne pas créer, mettre à jour ou supprimer des données de configuration ou d'autres données par erreur.

Étapes

1. Depuis l'en-tête du gestionnaire de grille, sélectionnez l'icône d'aide et sélectionnez **Documentation API**.



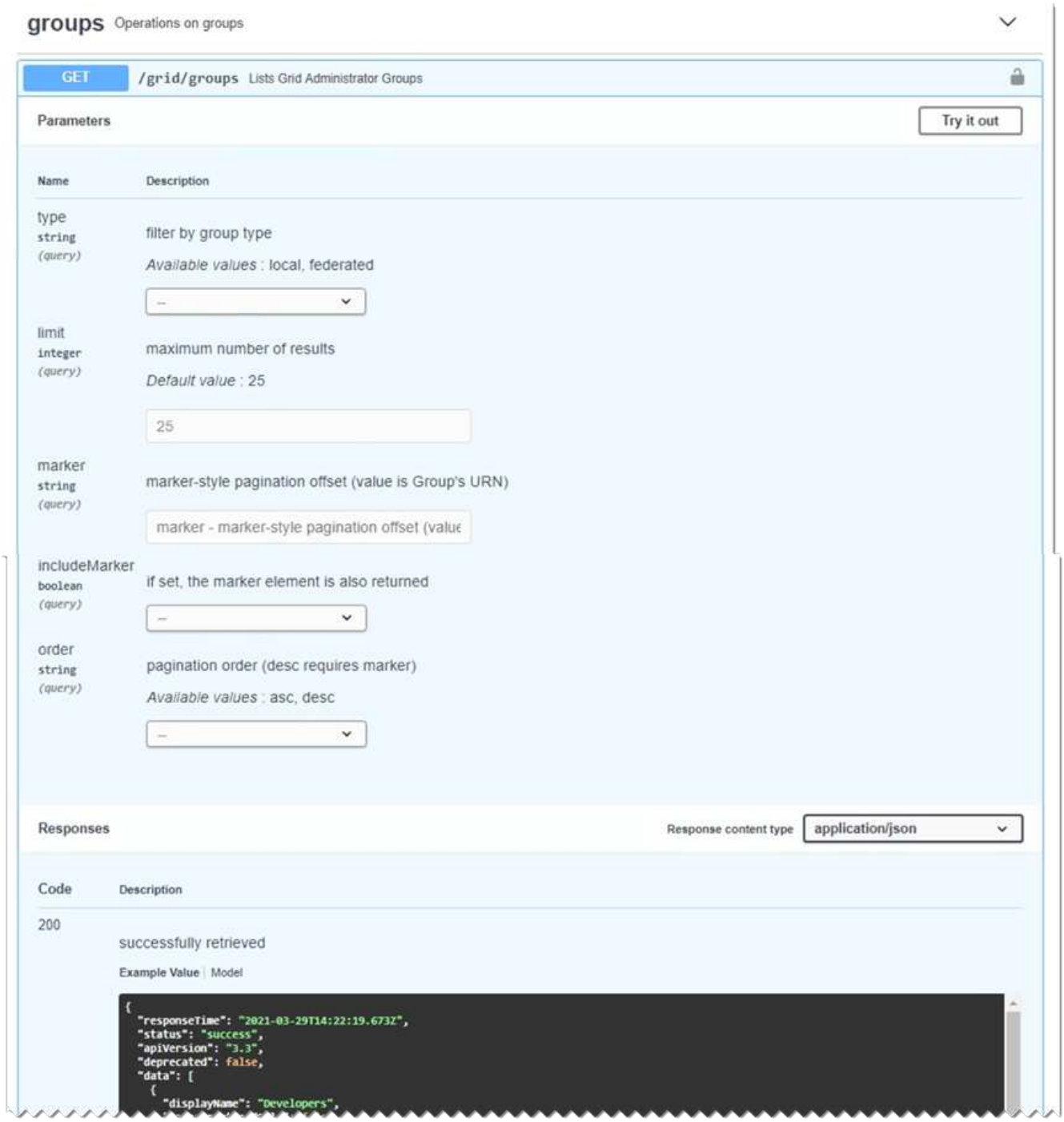
2. Pour effectuer une opération avec l'API privée, sélectionnez **Accéder à la documentation de l'API privée** sur la page API de gestion StorageGRID .

   Les API privées sont susceptibles d'être modifiées sans préavis. Les points de terminaison privés StorageGRID ignorent également la version API de la demande.

3. Sélectionnez l'opération souhaitée.

   Lorsque vous développez une opération API, vous pouvez voir les actions HTTP disponibles, telles que GET, PUT, UPDATE et DELETE.

4. Sélectionnez une action HTTP pour afficher les détails de la demande, y compris l'URL du point de terminaison, une liste de tous les paramètres obligatoires ou facultatifs, un exemple du corps de la demande (si nécessaire) et les réponses possibles.



5. Déterminez si la demande nécessite des paramètres supplémentaires, tels qu'un ID de groupe ou d'utilisateur. Ensuite, obtenez ces valeurs. Vous devrez peut-être d'abord émettre une demande d'API différente pour obtenir les informations dont vous avez besoin.
6. Déterminez si vous devez modifier le corps de la demande d'exemple. Si tel est le cas, vous pouvez sélectionner **Modèle** pour connaître les exigences de chaque champ.
7. Sélectionnez **Essayer**.
8. Fournissez tous les paramètres requis ou modifiez le corps de la demande selon vos besoins.
9. Sélectionnez **Exécuter**.
10. Consultez le code de réponse pour déterminer si la demande a réussi.

Opérations de l'API de gestion de grille

L'API de gestion de grille organise les opérations disponibles dans les sections suivantes.

Cette liste inclut uniquement les opérations disponibles dans l'API publique.

- **comptes** : opérations de gestion des comptes de locataires de stockage, y compris la création de nouveaux comptes et la récupération de l'utilisation du stockage pour un compte donné.
- **alert-history** : Opérations sur les alertes résolues.
- **alert-receivers** : Opérations sur les récepteurs de notifications d'alerte (e-mail).
- **alert-rules** : Opérations sur les règles d'alerte.
- **alert-silences** : Opérations sur les silences d'alerte.
- **alertes** : Opérations sur les alertes.
- **audit** : opérations permettant de répertorier et de mettre à jour la configuration de l'audit.
- **auth** : opérations permettant d'effectuer l'authentification de la session utilisateur.

  L'API de gestion de grille prend en charge le schéma d'authentification du jeton porteur. Pour vous connecter, vous fournissez un nom d'utilisateur et un mot de passe dans le corps JSON de la demande d'authentification (c'est-à-dire, `POST /api/v3/authorize`). Si l'utilisateur est authentifié avec succès, un jeton de sécurité est renvoyé. Ce jeton doit être fourni dans l'en-tête des requêtes API ultérieures (« Authorization : Bearer *token* »). Le jeton expire après 16 heures.

  Si l'authentification unique est activée pour le système StorageGRID , vous devez effectuer différentes étapes pour vous authentifier. Voir « Authentification auprès de l'API si l'authentification unique est activée ».

  Consultez « Protection contre la falsification de requêtes intersites » pour obtenir des informations sur l'amélioration de la sécurité de l'authentification.

- **client-certificates** : opérations de configuration des certificats clients afin que StorageGRID soit accessible en toute sécurité à l'aide d'outils de surveillance externes.
- **config** : opérations liées à la version du produit et aux versions de l'API Grid Management. Vous pouvez répertorier la version du produit et les versions principales de l'API Grid Management prises en charge par cette version, et vous pouvez désactiver les versions obsolètes de l'API.
- **fonctionnalités désactivées** : opérations permettant d'afficher les fonctionnalités qui pourraient avoir été désactivées.
- **dns-servers** : opérations permettant de lister et de modifier les serveurs DNS externes configurés.
- **drive-details** : opérations sur les lecteurs pour des modèles d'appareils de stockage spécifiques.
- **endpoint-domain-names** : opérations permettant de répertorier et de modifier les noms de domaine de point de terminaison S3.
- **erasure-coding** : Opérations sur les profils d'effacement-codage.
- **expansion** : Opérations sur l'expansion (niveau procédure).
- **expansion-nodes** : opérations sur l'expansion (au niveau du nœud).
- **expansion-sites** : Opérations sur l'extension (au niveau du site).
- **grid-networks** : Opérations permettant de lister et de modifier la liste des réseaux de grille.

- **grid-passwords** : Opérations pour la gestion des mots de passe de la grille.
- **groupes** : opérations de gestion des groupes d'administrateurs de grille locaux et de récupération des groupes d'administrateurs de grille fédérés à partir d'un serveur LDAP externe.
- **identity-source** : opérations permettant de configurer une source d'identité externe et de synchroniser manuellement les informations des groupes fédérés et des utilisateurs.
- **ilm** : Opérations sur la gestion du cycle de vie de l'information (ILM).
- **in-progress-procedures**: Récupère les procédures de maintenance actuellement en cours.
- **licence** : opérations permettant de récupérer et de mettre à jour la licence StorageGRID .
- **logs** : opérations de collecte et de téléchargement des fichiers journaux.v
- **métriques** : opérations sur les métriques StorageGRID , y compris les requêtes de métriques instantanées à un moment donné et les requêtes de métriques de plage sur une plage de temps. L'API Grid Management utilise l'outil de surveillance des systèmes Prometheus comme source de données back-end. Pour plus d'informations sur la construction de requêtes Prometheus, consultez le site Web Prometheus.

> Les mesures qui incluent`private` dans leurs noms sont destinés à un usage interne uniquement. Ces mesures sont susceptibles d'être modifiées entre les versions de StorageGRID sans préavis.

- **node-details** : Opérations sur les détails du nœud.
- **node-health** : opérations sur l'état de santé du nœud.
- **node-storage-state** : opérations sur l'état de stockage des nœuds.
- **ntp-servers** : opérations permettant de répertorier ou de mettre à jour les serveurs NTP (Network Time Protocol) externes.
- **objets** : opérations sur les objets et les métadonnées des objets.
- **récupération** : opérations pour la procédure de récupération.
- **recovery-package** : opérations de téléchargement du package de récupération.
- **régions** : opérations permettant d'afficher et de créer des régions.
- **s3-object-lock** : opérations sur les paramètres globaux de verrouillage d'objet S3.
- **server-certificate** : opérations permettant d'afficher et de mettre à jour les certificats du serveur Grid Manager.
- **snmp** : opérations sur la configuration SNMP actuelle.
- **storage-watermarks** : Filigranes des nœuds de stockage.
- **traffic-classes** : opérations pour les politiques de classification du trafic.
- **untrusted-client-network** : opérations sur la configuration du réseau client non approuvé.
- **utilisateurs** : opérations permettant d'afficher et de gérer les utilisateurs de Grid Manager.

Gestion des versions de l'API de gestion de grille

L'API de gestion de grille utilise le contrôle de version pour prendre en charge les mises à niveau sans interruption.

Par exemple, cette URL de demande spécifie la version 4 de l'API.

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

La version principale de l'API est mise à jour lorsque des modifications sont apportées qui ne sont pas compatibles avec les versions plus anciennes. La version mineure de l'API est mise à jour lorsque des modifications sont apportées qui sont *compatibles* avec les versions plus anciennes. Les modifications compatibles incluent l'ajout de nouveaux points de terminaison ou de nouvelles propriétés.

L'exemple suivant illustre comment la version de l'API est augmentée en fonction du type de modifications apportées.

Type de modification de l'API	Ancienne version	Nouvelle version
Compatible avec les anciennes versions	2,1	2,2
Non compatible avec les anciennes versions	2,1	3,0

Lorsque vous installez le logiciel StorageGRID pour la première fois, seule la version la plus récente de l'API est activée. Cependant, lorsque vous effectuez une mise à niveau vers une nouvelle version de fonctionnalité de StorageGRID, vous continuez à avoir accès à l'ancienne version de l'API pour au moins une version de fonctionnalité de StorageGRID .

> Vous pouvez configurer les versions prises en charge. Consultez la section **config** de la documentation de l'API Swagger pour le"API de gestion de grille" pour plus d'informations. Vous devez désactiver la prise en charge de l'ancienne version après avoir mis à jour tous les clients API pour utiliser la version la plus récente.

Les demandes obsolètes sont marquées comme obsolètes des manières suivantes :

- L'en-tête de réponse est « Obsolète : vrai »
- Le corps de la réponse JSON inclut « obsolète » : vrai
- Un avertissement obsolète est ajouté à nms.log. Par exemple:

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

Déterminer quelles versions d'API sont prises en charge dans la version actuelle

Utilisez le `GET /versions` Requête d'API pour renvoyer une liste des versions majeures d'API prises en charge. Cette demande se trouve dans la section **config** de la documentation de l'API Swagger.

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

Spécifier une version d'API pour une requête

Vous pouvez spécifier la version de l'API à l'aide d'un paramètre de chemin(`/api/v4`) ou un en-tête(`Api-Version: 4`). Si vous fournissez les deux valeurs, la valeur de l'en-tête remplace la valeur du chemin.

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

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

Protection contre la falsification de requêtes intersites (CSRF)

Vous pouvez contribuer à vous protéger contre les attaques de falsification de requête intersite (CSRF) contre StorageGRID en utilisant des jetons CSRF pour améliorer l'authentification qui utilise des cookies. Le gestionnaire de grille et le gestionnaire de locataires activent automatiquement cette fonctionnalité de sécurité ; les autres clients API peuvent choisir de l'activer ou non lorsqu'ils se connectent.

Un attaquant capable de déclencher une requête vers un autre site (par exemple avec un formulaire HTTP POST) peut provoquer l'exécution de certaines requêtes à l'aide des cookies de l'utilisateur connecté.

StorageGRID aide à se protéger contre les attaques CSRF en utilisant des jetons CSRF. Lorsqu'elle est activée, le contenu d'un cookie spécifique doit correspondre au contenu d'un en-tête spécifique ou d'un paramètre de corps POST spécifique.

Pour activer la fonctionnalité, définissez le `csrfToken` paramètre à `true` lors de l'authentification. La valeur par défaut est `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"
```

Lorsque c'est vrai, un `GridCsrfToken` Le cookie est défini avec une valeur aléatoire pour les connexions au Grid Manager, et le `AccountCsrfToken` le cookie est défini avec une valeur aléatoire pour les connexions au Tenant Manager.

Si le cookie est présent, toutes les requêtes pouvant modifier l'état du système (POST, PUT, PATCH, DELETE) doivent inclure l'un des éléments suivants :

- Le `X-Csrf-Token` en-tête, avec la valeur de l'en-tête définie sur la valeur du cookie de jeton CSRF.
- Pour les points de terminaison qui acceptent un corps codé par formulaire : A `csrfToken` paramètre de corps de requête codé par formulaire.

Consultez la documentation de l'API en ligne pour des exemples et des détails supplémentaires.

> Les requêtes qui ont un cookie de jeton CSRF défini appliqueront également l'en-tête « Content-Type : application/json » pour toute requête qui attend un corps de requête JSON comme protection supplémentaire contre les attaques CSRF.

Utiliser l'API si l'authentification unique est activée

Utiliser l'API si l'authentification unique est activée (Active Directory)

Si vous avez"configuré et activé l'authentification unique (SSO)" et que vous utilisez Active Directory comme fournisseur SSO, vous devez émettre une série de requêtes API pour obtenir un jeton d'authentification valide pour l'API Grid Management ou l'API Tenant Management.

Sign in à l'API si l'authentification unique est activée

Ces instructions s'appliquent si vous utilisez Active Directory comme fournisseur d'identité SSO.

Avant de commencer

- Vous connaissez le nom d'utilisateur et le mot de passe SSO d'un utilisateur fédéré qui appartient à un groupe d'utilisateurs StorageGRID .
- Si vous souhaitez accéder à l'API de gestion des locataires, vous connaissez l'ID du compte locataire.

À propos de cette tâche

Pour obtenir un jeton d'authentification, vous pouvez utiliser l'un des exemples suivants :

- Le `storagegrid-ssoauth.py` Script Python, situé dans le répertoire des fichiers d'installation de

StorageGRID(`./rpms` pour Red Hat Enterprise Linux, `./debs` pour Ubuntu ou Debian, et `./vsphere` pour VMware).

- Un exemple de flux de travail de requêtes curl.

  Le flux de travail curl peut expirer si vous l'exécutez trop lentement. Vous pourriez voir l'erreur : `A valid SubjectConfirmation was not found on this Response`.

  > L'exemple de workflow curl ne protège pas le mot de passe contre toute visualisation par d'autres utilisateurs.

Si vous avez un problème d'encodage d'URL, vous pourriez voir l'erreur : `Unsupported SAML version`.

Étapes

1. Sélectionnez l'une des méthodes suivantes pour obtenir un jeton d'authentification :
   - Utilisez le `storagegrid-ssoauth.py` Script Python. Passez à l'étape 2.
   - Utilisez les requêtes curl. Passez à l'étape 3.
2. Si vous souhaitez utiliser le `storagegrid-ssoauth.py` script, transmettez le script à l'interpréteur Python et exécutez le script.

   Lorsque vous y êtes invité, saisissez des valeurs pour les arguments suivants :
   - La méthode SSO. Entrez ADFS ou adfs.
   - Le nom d'utilisateur SSO
   - Le domaine où StorageGRID est installé
   - L'adresse de StorageGRID
   - L'ID du compte locataire, si vous souhaitez accéder à l'API de gestion des locataires.

   ```
   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
   ```

   Le jeton d'autorisation StorageGRID est fourni dans la sortie. Vous pouvez désormais utiliser le jeton pour d'autres requêtes, de la même manière que vous utiliseriez l'API si SSO n'était pas utilisé.
3. Si vous souhaitez utiliser des requêtes curl, utilisez la procédure suivante.
   a. Déclarez les variables nécessaires à la connexion.

```
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'
```

Pour accéder à l'API de gestion de grille, utilisez 0 comme `TENANTACCOUNTID` .

b. Pour recevoir une URL d'authentification signée, émettez une requête POST à `/api/v3/authorize-saml` et supprimez l'encodage JSON supplémentaire de la réponse.

Cet exemple montre une requête POST pour une URL d'authentification signée pour `TENANTACCOUNTID` . Les résultats seront transmis à `python -m json.tool` pour supprimer l'encodage 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 réponse pour cet exemple inclut une URL signée qui est codée en URL, mais elle n'inclut pas la couche de codage JSON supplémentaire.

```
{
    "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. Sauver le `SAMLRequest` à partir de la réponse à utiliser dans les commandes suivantes.

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

d. Obtenez une URL complète qui inclut l'ID de demande client d'AD FS.

Une option consiste à demander le formulaire de connexion en utilisant l'URL de la réponse précédente.

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

La réponse inclut l'ID de la demande du client :

```
<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. Enregistrez l'ID de demande du client à partir de la réponse.

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

f. Envoyez vos informations d'identification à l'action du formulaire de la réponse précédente.

```
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 renvoie une redirection 302, avec des informations supplémentaires dans les en-têtes.

> Si l'authentification multifacteur (MFA) est activée pour votre système SSO, le formulaire de publication contiendra également le deuxième mot de passe ou d'autres informations d'identification.

```
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. Sauver le `MSISAuth` cookie de la réponse.

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

h. Envoyez une requête GET à l'emplacement spécifié avec les cookies du POST d'authentification.

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

Les en-têtes de réponse contiendront des informations de session AD FS pour une utilisation ultérieure lors de la déconnexion, et le corps de la réponse contient la réponse SAML dans un champ de formulaire masqué.

```
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. Sauver le `SAMLResponse` du champ caché :

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

j. Utilisation de la sauvegarde `SAMLResponse` , créer un StorageGRID`/api/saml-response` demande de génération d'un jeton d'authentification StorageGRID .

Pour `RelayState` , utilisez l'ID de compte locataire ou utilisez 0 si vous souhaitez vous connecter à l'API Grid Management.

```
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 réponse inclut le jeton d'authentification.

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

a. Enregistrez le jeton d'authentification dans la réponse sous `MYTOKEN` .

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

Vous pouvez désormais utiliser `MYTOKEN` pour d'autres demandes, de la même manière que vous utiliseriez l'API si SSO n'était pas utilisé.

Déconnectez-vous de l'API si l'authentification unique est activée

Si l'authentification unique (SSO) a été activée, vous devez émettre une série de requêtes API pour vous déconnecter de l'API Grid Management ou de l'API Tenant Management. Ces instructions s'appliquent si vous utilisez Active Directory comme fournisseur d'identité SSO

À propos de cette tâche

Si nécessaire, vous pouvez vous déconnecter de l'API StorageGRID en vous déconnectant de la page de déconnexion unique de votre organisation. Vous pouvez également déclencher une déconnexion unique (SLO) à partir de StorageGRID, ce qui nécessite un jeton porteur StorageGRID valide.

Étapes

1. Pour générer une demande de déconnexion signée, transmettez `cookie "sso=true" à l'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
```

Une URL de déconnexion est renvoyée :

```
{
    "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. Enregistrez l'URL de déconnexion.

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

3. Envoyez une demande à l'URL de déconnexion pour déclencher SLO et rediriger vers StorageGRID.

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

La réponse 302 est renvoyée. L'emplacement de redirection ne s'applique pas à la déconnexion de l'API uniquement.

```
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. Supprimez le jeton porteur StorageGRID .

La suppression du jeton porteur StorageGRID fonctionne de la même manière que sans SSO. Si `cookie "sso=true" n'est pas fourni, l'utilisateur est déconnecté de StorageGRID sans affecter l'état SSO.

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

UN `204 No Content` la réponse indique que l'utilisateur est maintenant déconnecté.

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

Utiliser l'API si l'authentification unique est activée (Azure)

Si vous avez"configuré et activé l'authentification unique (SSO)" et vous utilisez Azure comme fournisseur SSO, vous pouvez utiliser deux exemples de scripts pour obtenir un jeton d'authentification valide pour l'API Grid Management ou l'API Tenant Management.

Sign in à l'API si l'authentification unique Azure est activée

Ces instructions s'appliquent si vous utilisez Azure comme fournisseur d'identité SSO

Avant de commencer

- Vous connaissez l'adresse e-mail et le mot de passe SSO d'un utilisateur fédéré qui appartient à un groupe d'utilisateurs StorageGRID .
- Si vous souhaitez accéder à l'API de gestion des locataires, vous connaissez l'ID du compte locataire.

À propos de cette tâche

Pour obtenir un jeton d'authentification, vous pouvez utiliser les exemples de scripts suivants :

- Le `storagegrid-ssoauth-azure.py` Script Python
- Le `storagegrid-ssoauth-azure.js` Script Node.js

Les deux scripts se trouvent dans le répertoire des fichiers d'installation de StorageGRID(`./rpms` pour Red Hat Enterprise Linux, `./debs` pour Ubuntu ou Debian, et `./vsphere` pour VMware).

Pour écrire votre propre intégration d'API avec Azure, consultez le `storagegrid-ssoauth-azure.py` scénario. Le script Python envoie deux requêtes directement à StorageGRID (d'abord pour obtenir le SAMLRequest, puis pour obtenir le jeton d'autorisation) et appelle également le script Node.js pour interagir avec Azure afin d'effectuer les opérations SSO.

Les opérations SSO peuvent être exécutées à l'aide d'une série de requêtes API, mais cela n'est pas simple. Le module Puppeteer Node.js est utilisé pour récupérer l'interface Azure SSO.

Si vous avez un problème d'encodage d'URL, vous pourriez voir l'erreur : `Unsupported SAML version`.

Étapes

1. Installez les dépendances requises, comme suit :
   a. Installez Node.js (voir "https://nodejs.org/en/download/").

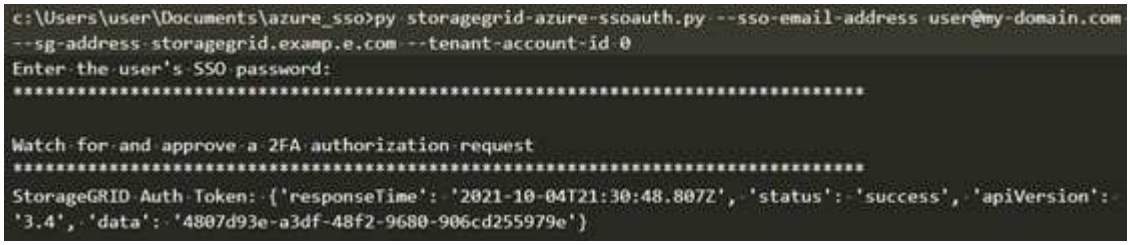
b. Installez les modules Node.js requis (puppeteer et jsdom) :

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

2. Transmettez le script Python à l'interpréteur Python pour exécuter le script.

   Le script Python appellera ensuite le script Node.js correspondant pour effectuer les interactions Azure SSO.

3. Lorsque vous y êtes invité, saisissez des valeurs pour les arguments suivants (ou transmettez-les à l'aide de paramètres) :
   - L'adresse e-mail SSO utilisée pour se connecter à Azure
   - L'adresse de StorageGRID
   - L'ID du compte locataire, si vous souhaitez accéder à l'API de gestion des locataires
4. Lorsque vous y êtes invité, saisissez le mot de passe et soyez prêt à fournir une autorisation MFA à Azure si nécessaire.



> Le script suppose que l'authentification multifacteur est effectuée à l'aide de Microsoft Authenticator. Vous devrez peut-être modifier le script pour prendre en charge d'autres formes d'authentification multifacteur (comme la saisie d'un code reçu dans un message texte).

Le jeton d'autorisation StorageGRID est fourni dans la sortie. Vous pouvez désormais utiliser le jeton pour d'autres requêtes, de la même manière que vous utiliseriez l'API si SSO n'était pas utilisé.

Utiliser l'API si l'authentification unique est activée (PingFederate)

Si vous avez"configuré et activé l'authentification unique (SSO)" et que vous utilisez PingFederate comme fournisseur SSO, vous devez émettre une série de requêtes API pour obtenir un jeton d'authentification valide pour l'API de gestion de grille ou l'API de gestion des locataires.

Sign in à l'API si l'authentification unique est activée

Ces instructions s'appliquent si vous utilisez PingFederate comme fournisseur d'identité SSO

Avant de commencer

- Vous connaissez le nom d'utilisateur et le mot de passe SSO d'un utilisateur fédéré qui appartient à un groupe d'utilisateurs StorageGRID .
- Si vous souhaitez accéder à l'API de gestion des locataires, vous connaissez l'ID du compte locataire.

À propos de cette tâche

Pour obtenir un jeton d'authentification, vous pouvez utiliser l'un des exemples suivants :

- Le `storagegrid-ssoauth.py` Script Python, situé dans le répertoire des fichiers d'installation de StorageGRID(`./rpms` pour Red Hat Enterprise Linux, `./debs` pour Ubuntu ou Debian, et `./vsphere` pour VMware).
- Un exemple de flux de travail de requêtes curl.

  Le flux de travail curl peut expirer si vous l'exécutez trop lentement. Vous pourriez voir l'erreur : `A valid SubjectConfirmation was not found on this Response`.

  > L'exemple de workflow curl ne protège pas le mot de passe contre toute visualisation par d'autres utilisateurs.

  Si vous avez un problème d'encodage d'URL, vous pourriez voir l'erreur : `Unsupported SAML version`.

Étapes

1. Sélectionnez l'une des méthodes suivantes pour obtenir un jeton d'authentification :
   - Utilisez le `storagegrid-ssoauth.py` Script Python. Passez à l'étape 2.
   - Utilisez les requêtes curl. Passez à l'étape 3.
2. Si vous souhaitez utiliser le `storagegrid-ssoauth.py` script, transmettez le script à l'interpréteur Python et exécutez le script.

   Lorsque vous y êtes invité, saisissez des valeurs pour les arguments suivants :

   - La méthode SSO. Vous pouvez saisir n'importe quelle variante de « pingfederate » (PINGFEDERATE, pingfederate, etc.).
   - Le nom d'utilisateur SSO
   - Le domaine où StorageGRID est installé. Ce champ n'est pas utilisé pour PingFederate. Vous pouvez le laisser vide ou saisir n'importe quelle valeur.
   - L'adresse de StorageGRID
   - L'ID du compte locataire, si vous souhaitez accéder à l'API de gestion des locataires.

   ```
   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
   ```

   Le jeton d'autorisation StorageGRID est fourni dans la sortie. Vous pouvez désormais utiliser le jeton pour d'autres requêtes, de la même manière que vous utiliseriez l'API si SSO n'était pas utilisé.
3. Si vous souhaitez utiliser des requêtes curl, utilisez la procédure suivante.

a. Déclarez les variables nécessaires à la connexion.

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

> Pour accéder à l'API de gestion de grille, utilisez 0 comme `TENANTACCOUNTID` .

b. Pour recevoir une URL d'authentification signée, émettez une requête POST à `/api/v3/authorize-saml` et supprimez l'encodage JSON supplémentaire de la réponse.

Cet exemple montre une requête POST pour une URL d'authentification signée pour TENANTACCOUNTID. Les résultats seront transmis à python -m json.tool pour supprimer l'encodage 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 réponse pour cet exemple inclut une URL signée qui est codée en URL, mais elle n'inclut pas la couche de codage JSON supplémentaire.

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

c. Sauver le `SAMLRequest` à partir de la réponse à utiliser dans les commandes suivantes.

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

d. Exportez la réponse et le cookie, et faites écho à la réponse :

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

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

e. Exportez la valeur « pf.adapterId » et renvoyez la réponse :

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

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

f. Exportez la valeur « href » (supprimez la barre oblique /) et affichez la réponse :

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

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

g. Exporter la valeur « action » :

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

h. Envoyer des cookies avec les informations d'identification :

```
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. Sauver le `SAMLResponse` du champ caché :

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

j. Utilisation de la sauvegarde `SAMLResponse` , créer un StorageGRID`/api/saml-response` demande de génération d'un jeton d'authentification StorageGRID .

   Pour `RelayState` , utilisez l'ID de compte locataire ou utilisez 0 si vous souhaitez vous connecter à l'API Grid Management.

```
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 réponse inclut le jeton d'authentification.

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

a. Enregistrez le jeton d'authentification dans la réponse sous `MYTOKEN` .

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

Vous pouvez désormais utiliser `MYTOKEN` pour d'autres demandes, de la même manière que vous utiliseriez l'API si SSO n'était pas utilisé.

Déconnectez-vous de l'API si l'authentification unique est activée

Si l'authentification unique (SSO) a été activée, vous devez émettre une série de requêtes API pour vous déconnecter de l'API Grid Management ou de l'API Tenant Management. Ces instructions s'appliquent si vous utilisez PingFederate comme fournisseur d'identité SSO

À propos de cette tâche

Si nécessaire, vous pouvez vous déconnecter de l'API StorageGRID en vous déconnectant de la page de déconnexion unique de votre organisation. Vous pouvez également déclencher une déconnexion unique (SLO) à partir de StorageGRID, ce qui nécessite un jeton porteur StorageGRID valide.

Étapes

1. Pour générer une demande de déconnexion signée, transmettez `cookie "sso=true" à l'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
```

Une URL de déconnexion est renvoyée :

```
{
    "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. Enregistrez l'URL de déconnexion.

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

3. Envoyez une demande à l'URL de déconnexion pour déclencher SLO et rediriger vers StorageGRID.

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

La réponse 302 est renvoyée. L'emplacement de redirection ne s'applique pas à la déconnexion de l'API uniquement.

```
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. Supprimez le jeton porteur StorageGRID .

La suppression du jeton porteur StorageGRID fonctionne de la même manière que sans SSO. Si `cookie "sso=true" n'est pas fourni, l'utilisateur est déconnecté de StorageGRID sans affecter l'état SSO.

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

UN `204 No Content` la réponse indique que l'utilisateur est maintenant déconnecté.

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

Désactiver les fonctionnalités avec l'API

Vous pouvez utiliser l'API Grid Management pour désactiver complètement certaines fonctionnalités du système StorageGRID . Lorsqu'une fonctionnalité est désactivée, personne ne peut se voir attribuer d'autorisations pour effectuer les tâches liées à cette fonctionnalité.

À propos de cette tâche

Le système de fonctionnalités désactivées vous permet d'empêcher l'accès à certaines fonctionnalités du système StorageGRID . La désactivation d'une fonctionnalité est le seul moyen d'empêcher l'utilisateur root ou les utilisateurs appartenant à des groupes d'administrateurs avec l'autorisation **Accès root** de pouvoir utiliser cette fonctionnalité.

Pour comprendre comment cette fonctionnalité pourrait être utile, considérez le scénario suivant :

_La société A est un fournisseur de services qui loue la capacité de stockage de son système StorageGRID en créant des comptes locataires. Pour protéger la sécurité des objets de ses locataires, la société A souhaite s'assurer que ses propres employés ne pourront jamais accéder à un compte locataire après le déploiement du compte.

_L'entreprise A peut atteindre cet objectif en utilisant le système de désactivation des fonctionnalités dans l'API de gestion de la grille. En désactivant complètement la fonctionnalité **Modifier le mot de passe root du locataire** dans le gestionnaire de grille (à la fois l'interface utilisateur et l'API), la société A garantit que les utilisateurs administrateurs, y compris l'utilisateur root et les utilisateurs appartenant à des groupes disposant de l'autorisation **Accès root**, ne peuvent pas modifier le mot de passe de l'utilisateur root d'un compte locataire.

Étapes

1. Accédez à la documentation Swagger pour l'API de gestion de grille. Voir "Utiliser l'API de gestion de grille" .
2. Localisez le point de terminaison Désactiver les fonctionnalités.
3. Pour désactiver une fonctionnalité, telle que Modifier le mot de passe racine du locataire, envoyez un corps à l'API comme ceci :

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

   Une fois la demande terminée, la fonctionnalité Modifier le mot de passe racine du locataire est désactivée. L'autorisation de gestion **Modifier le mot de passe racine du locataire** n'apparaît plus dans l'interface utilisateur et toute demande d'API qui tente de modifier le mot de passe racine d'un locataire échouera avec le message « 403 Forbidden ».

Réactiver les fonctionnalités désactivées

Par défaut, vous pouvez utiliser l'API de gestion de grille pour réactiver une fonctionnalité qui a été désactivée. Cependant, si vous souhaitez empêcher que les fonctionnalités désactivées ne soient réactivées, vous pouvez désactiver la fonctionnalité **activateFeatures** elle-même.

> La fonctionnalité **activateFeatures** ne peut pas être réactivée. Si vous décidez de désactiver cette fonctionnalité, sachez que vous perdrez définitivement la possibilité de réactiver toute autre fonctionnalité désactivée. Vous devez contacter le support technique pour restaurer toute fonctionnalité perdue.

Étapes

1. Accédez à la documentation Swagger pour l'API de gestion de grille.
2. Localisez le point de terminaison Désactiver les fonctionnalités.
3. Pour réactiver toutes les fonctionnalités, envoyez un corps à l'API comme ceci :

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

Une fois cette demande terminée, toutes les fonctionnalités, y compris la fonctionnalité Modifier le mot de passe racine du locataire, sont réactivées. L'autorisation de gestion **Modifier le mot de passe racine du locataire** apparaît désormais dans l'interface utilisateur, et toute demande d'API qui tente de modifier le mot de passe racine d'un locataire réussira, en supposant que l'utilisateur dispose de l'autorisation de gestion **Accès racine** ou **Modifier le mot de passe racine du locataire**.

L'exemple précédent provoque la réactivation de *toutes* les fonctionnalités désactivées. Si d'autres fonctionnalités ont été désactivées et doivent rester désactivées, vous devez les spécifier explicitement dans la requête PUT. Par exemple, pour réactiver la fonctionnalité Modifier le mot de passe root du locataire et continuer à désactiver l'autorisation de gestion storageAdmin, envoyez cette requête PUT :

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

Informations sur le copyright

Informations sur les marques commerciales