Commencez à utiliser Grid Manager

StorageGRID software

NetApp
July 23, 2026

Sommaire

Commencez à utiliser Grid Manager

Configuration requise du navigateur Web pour StorageGRID

Vous devez utiliser un navigateur Web compatible.

Navigateur Web	Version minimale prise en charge
Google Chrome	138
Microsoft Edge	138
Mozilla Firefox	140

Définissez la fenêtre du navigateur sur une largeur recommandée.

Largeur du navigateur	Pixels
Minimum	1024
Optimum	1280

Connectez-vous au gestionnaire de grille StorageGRID

Vous accédez à la page de connexion de Grid Manager en saisissant le domaine complet (FQDN) ou l'adresse IP d'un nœud d'administration dans la barre d'adresse d'un navigateur web compatible.

Chaque système StorageGRID comprend un nœud d'administration principal et un nombre quelconque de nœuds d'administration non principaux. Vous pouvez vous connecter à Grid Manager sur n'importe quel nœud d'administration pour gérer le système StorageGRID. Cependant, certaines procédures de maintenance ne peuvent être effectuées que depuis le nœud d'administration principal.

Se connecter au groupe HA

Si des nœuds d'administration sont inclus dans un groupe à haute disponibilité (HA), vous vous connectez à l'aide de l'adresse IP virtuelle du groupe HA ou d'un domaine complet qui pointe vers cette adresse IP virtuelle. Le nœud d'administration principal doit être sélectionné comme interface principale du groupe, de sorte que lorsque vous accédez à Grid Manager, vous y accédez via le nœud d'administration principal, sauf si celui-ci n'est pas disponible. Voir "Gérer les groupes à haute disponibilité".

Utilisez l'authentification unique (SSO)

Les étapes de connexion sont légèrement différentes si "L'authentification unique (SSO) a été configurée".

Connectez-vous à Grid Manager sur le premier nœud d'administration

Avant de commencer

- Vous disposez de vos identifiants de connexion.
- Vous utilisez un "navigateur Web pris en charge".
- Les cookies sont activés dans votre navigateur web.
- Vous appartenez à un groupe d'utilisateurs qui possède au moins une autorisation.
- Vous disposez de l'URL du Grid Manager :

  `https://FQDN_or_Admin_Node_IP/`

  Vous pouvez utiliser le domaine complet, l'adresse IP d'un nœud d'administration ou l'adresse IP virtuelle d'un groupe HA de nœuds d'administration.

  Pour accéder au Grid Manager sur un port autre que le port par défaut pour HTTPS (443), incluez le numéro de port dans l'URL :

  `https://FQDN_or_Admin_Node_IP:port/`

  > L'authentification unique (SSO) n'est pas disponible sur le port restreint de Grid Manager. Vous devez utiliser le port 443.

Étapes

1. Lancez un navigateur web compatible.
2. Dans la barre d'adresse du navigateur, saisissez l'URL du Grid Manager.
3. Si vous recevez une alerte de sécurité, installez le certificat à l'aide de l'assistant d'installation de votre navigateur. Voir "Gérer les certificats de sécurité".
4. Connectez-vous au Grid Manager.

   L'écran de connexion qui apparaît dépend de la configuration de l'authentification unique (SSO) pour StorageGRID.

Ne pas utiliser l'authentification unique (SSO)

a. Saisissez votre nom d'utilisateur et votre mot de passe pour le Grid Manager.

b. Sélectionnez **Se connecter**.

Utilisation de l'authentification unique (SSO)

- Si StorageGRID utilise l'authentification unique (SSO) et que c'est la première fois que vous accédez à l'URL sur ce navigateur :

  i. Sélectionnez **Se connecter**. Vous pouvez laisser le 0 dans le champ Compte.

  ii. Saisissez vos identifiants SSO standard sur la page de connexion SSO de votre organisation.

  Par exemple, si StorageGRID utilise l'authentification unique (SSO) et que vous avez déjà accédé à Grid Manager ou à un compte locataire :

  A. Saisissez **0** (l'identifiant du compte pour le Grid Manager) ou sélectionnez **Grid Manager** s'il apparaît dans la liste des comptes récents.

  B. Sélectionnez **Se connecter**.

  C. Connectez-vous avec vos identifiants SSO habituels sur la page de connexion SSO de votre organisation.

Une fois connecté, la page d'accueil du Grid Manager s'affiche et contient le tableau de bord. Pour savoir quelles informations sont fournies, consultez "Afficher et gérer le tableau de bord".

Connectez-vous à un autre nœud d'administration

Suivez ces étapes pour vous connecter à un autre nœud d'administration.

Ne pas utiliser l'authentification unique (SSO)

Étapes

1. Dans la barre d'adresse du navigateur, saisissez le nom de domaine complet ou l'adresse IP de l'autre nœud d'administration. Indiquez le numéro de port si nécessaire.
2. Saisissez votre nom d'utilisateur et votre mot de passe pour le Grid Manager.
3. Sélectionnez **Se connecter**.

Utilisation de l'authentification unique (SSO)

Si StorageGRID utilise l'authentification unique (SSO) et que vous vous êtes connecté à un nœud d'administration, vous pouvez accéder aux autres nœuds d'administration sans avoir à vous reconnecter.

Étapes

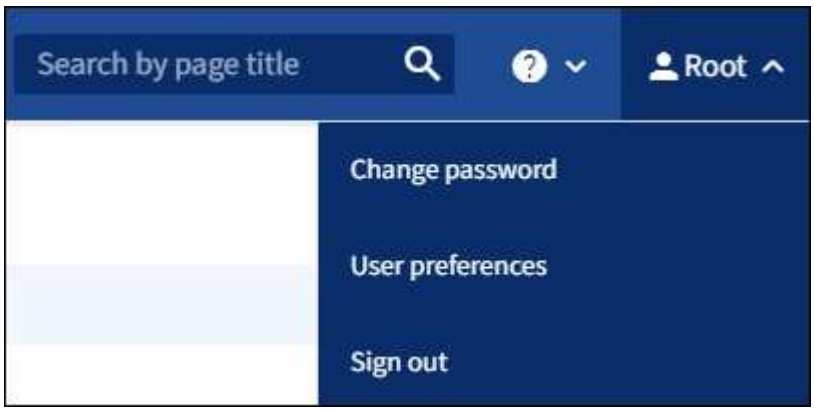
1. Saisissez le nom de domaine complet ou l'adresse IP de l'autre nœud d'administration dans la barre d'adresse du navigateur.
2. Si votre session SSO a expiré, veuillez saisir à nouveau vos identifiants.

Déconnectez-vous du StorageGRID Grid Manager

Une fois votre session d'utilisation de Grid Manager terminée, vous devez vous déconnecter afin d'empêcher tout accès non autorisé au système StorageGRID. La fermeture de votre navigateur ne vous déconnectera pas nécessairement du système, selon les paramètres des cookies de votre navigateur.

Étapes

1. Sélectionnez votre nom d'utilisateur dans le coin supérieur droit.



2. Sélectionnez **Se déconnecter**.

Option	Description
SSO non utilisé	Vous êtes déconnecté du nœud d'administration. La page de connexion de Grid Manager s'affiche. **Remarque :** Si vous vous êtes connecté à plusieurs nœuds d'administration, vous devez vous déconnecter de chaque nœud.
SSO activé	Vous êtes déconnecté de tous les nœuds d'administration auxquels vous accédiez. La page de connexion StorageGRID s'affiche. **Grid Manager** est indiqué par défaut dans le menu déroulant **Recent Accounts**, et le champ **Account ID** affiche 0. **Remarque :** Si l'authentification unique (SSO) est activée et que vous êtes également connecté au Tenant Manager, vous devez également "déconnectez-vous du compte locataire" à "Déconnexion de SSO".

Modifiez votre mot de passe StorageGRID Grid Manager

Si vous êtes un utilisateur local de Grid Manager, vous pouvez modifier votre propre mot de passe.

Avant de commencer

Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur Web pris en charge".

À propos de cette tâche

Si vous vous connectez à StorageGRID en tant qu'utilisateur fédéré ou si l'authentification unique (SSO) est activée, vous ne pouvez pas modifier votre mot de passe dans Grid Manager. Vous devez alors modifier votre mot de passe dans la source d'identité externe, par exemple Active Directory ou OpenLDAP.

Étapes

1. Dans l'en-tête du Grid Manager, sélectionnez ***your name*** > **Change password**.
2. Saisissez votre mot de passe actuel.
3. Saisissez un nouveau mot de passe.

   Votre mot de passe doit contenir au moins 8 et au plus 32 caractères. Les mots de passe sont sensibles à la casse.

4. Saisissez à nouveau le nouveau mot de passe.
5. Sélectionnez **Enregistrer**.

Consultez les informations de licence StorageGRID

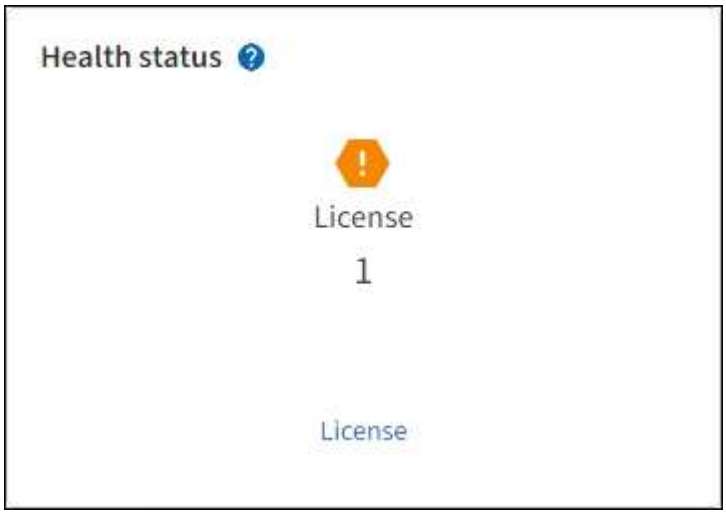
Vous pouvez consulter les informations de licence de votre système StorageGRID, telles que la capacité de stockage maximale de votre grille, à tout moment.

Avant de commencer

Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur Web pris en charge".

À propos de cette tâche

En cas de problème de licence logicielle pour ce système StorageGRID, la carte « État de santé » du tableau de bord affiche une icône d'état de licence et un lien **Licence**. Le nombre indique le nombre de problèmes liés à la licence.



Étapes

1. Accédez à la page de licence en procédant de l'une des manières suivantes :
   - Sélectionnez **Maintenance** > **Système** > **Licence**.
   - Depuis la carte d'état de santé du tableau de bord, sélectionnez l'icône d'état de la licence ou le lien **License**.

Ce lien n'apparaît que s'il y a un problème avec la licence.

2. Consultez les détails en lecture seule de la licence actuelle :
   - ID du système StorageGRID, qui est le numéro d'identification unique de cette installation StorageGRID
   - numéro de série de la licence
   - Type de licence, soit **Perpetual** ou **Subscription**
   - Capacité de stockage autorisée du grid
   - Capacité de stockage prise en charge
   - Date de fin de licence. **N/A** apparaît pour une licence perpétuelle.
   - Date de fin de support

     Cette date est extraite du fichier de licence actuel et peut être obsolète si vous avez prolongé ou renouvelé le contrat de service d'assistance après l'obtention du fichier de licence. Pour mettre à jour cette valeur, consultez "Mettre à jour les informations de licence StorageGRID". Vous pouvez également consulter la date de fin de contrat réelle à l'aide de Active IQ.

   - Contenu du fichier texte de la licence

Mettre à jour les informations de licence StorageGRID

Vous devez mettre à jour les informations de licence de votre système StorageGRID chaque fois que les conditions de votre licence changent. Par exemple, vous devez mettre à jour les informations de licence si vous achetez une capacité de stockage supplémentaire pour votre grid.

Avant de commencer

- Vous disposez d'un nouveau fichier de licence à appliquer à votre système StorageGRID.
- Vous avez "autorisations d'accès spécifiques".
- Vous disposez de la phrase secrète de provisionnement.

Étapes

1. Sélectionnez **Maintenance** > **Système** > **Licence**.
2. Dans la section Mise à jour de la licence, sélectionnez **Parcourir**.
3. Localisez et sélectionnez le nouveau fichier de licence (`.txt`).

   Le nouveau fichier de licence est validé et affiché.

4. Saisissez la phrase secrète de provisionnement.
5. Sélectionnez **Enregistrer**.

Utilisez la ligne de commandes (API)

Utilisez l'API de gestion de grille StorageGRID

Vous pouvez effectuer des tâches de gestion système à l'aide de l'API REST de Grid

Management plutôt qu'en utilisant l'interface utilisateur de Grid Manager. Par exemple, vous pourriez vouloir utiliser l'API pour automatiser des opérations ou pour créer plusieurs entités, telles que des utilisateurs, plus rapidement.

Ressources de haut niveau

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

- `/grid` : L'accès est réservé aux utilisateurs de Grid Manager et dépend des autorisations de groupe configurées.
- `/org` : L'accès est limité aux utilisateurs appartenant à un groupe LDAP local ou fédéré pour un compte locataire. Pour plus de détails, consultez "Utilisez un compte locataire".
- `/private` : L'accès est réservé aux utilisateurs de Grid Manager et dépend des autorisations de groupe configurées. Les API privées sont susceptibles d'être modifiées sans préavis. Les points de terminaison privés de StorageGRID ignorent également la version de l'API de la requête.

Émettre des requêtes API

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

L'interface utilisateur Swagger fournit des informations et une documentation complètes pour chaque opération API.

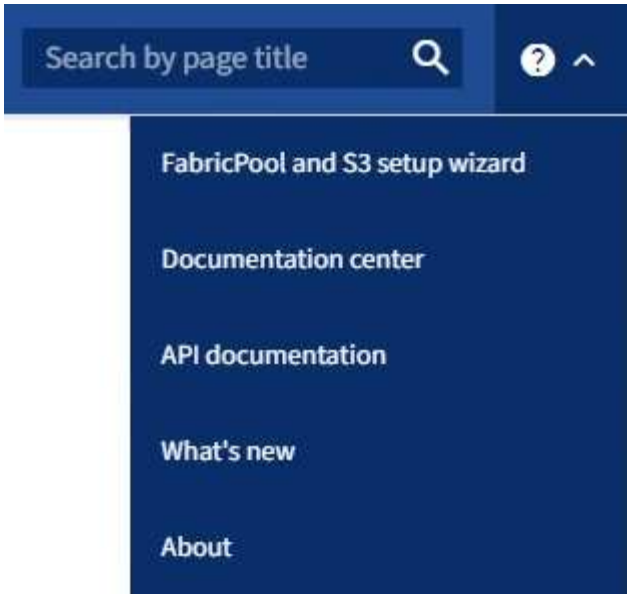
Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur Web pris en charge".
- Vous avez "autorisations d'accès spécifiques".

> Toute opération API effectuée via la page de documentation API est une opération en direct. Veillez à ne pas créer, modifier ou supprimer par erreur des données de configuration ou autres.

Étapes

1. Dans l'en-tête de Grid Manager, sélectionnez l'icône d'aide et sélectionnez **API documentation**.



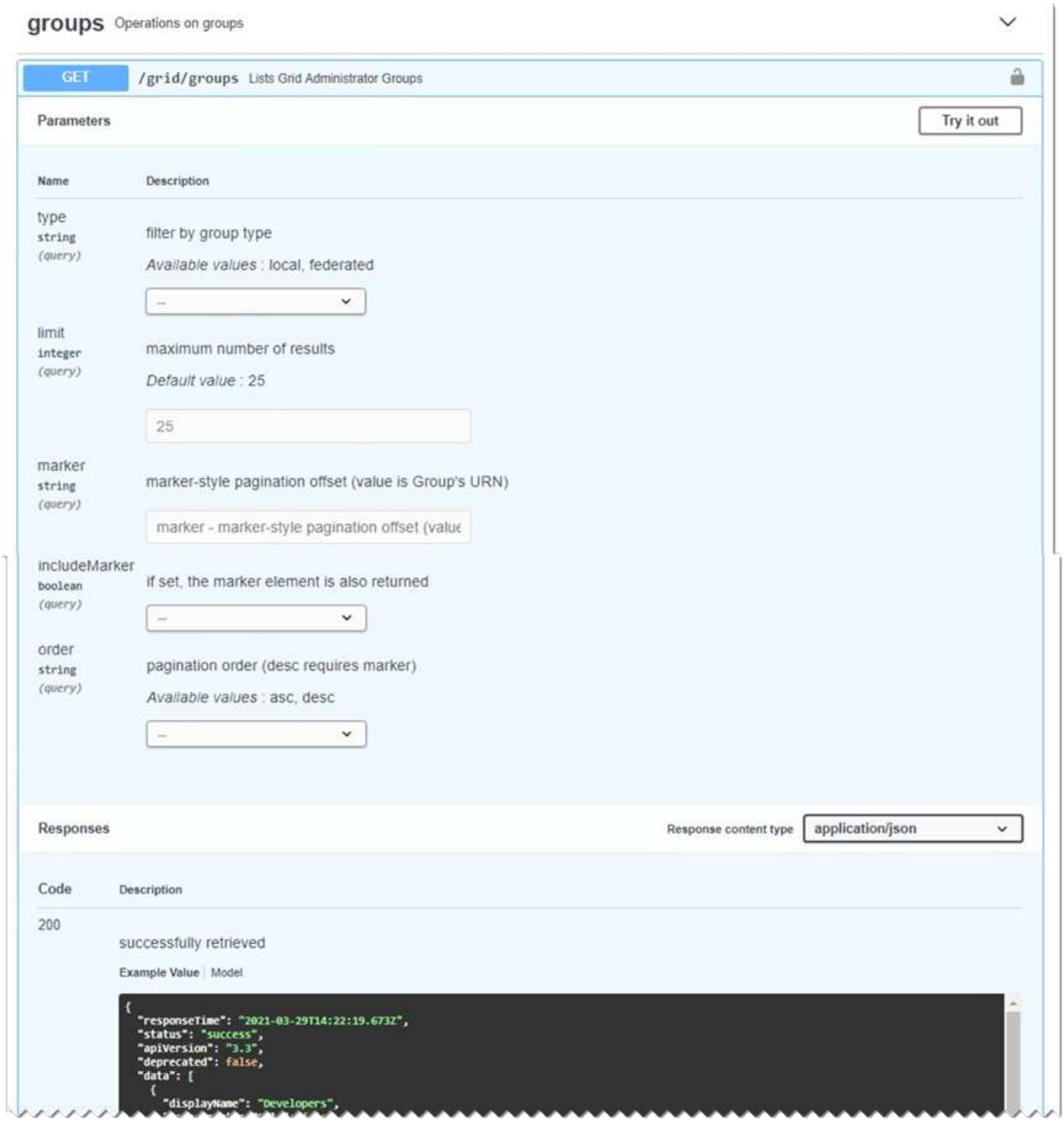
2. Pour effectuer une opération avec l'API privée, sélectionnez **Accéder à la documentation de l'API privée** sur la page de l'API de gestion StorageGRID.

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

3. Sélectionnez l'opération souhaitée.

   Lorsque vous développez une opération d'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 requête, notamment l'URL du point de terminaison, la liste des paramètres obligatoires ou facultatifs, un exemple du corps de la requête (le cas échéant) et les réponses possibles.



5. Déterminez si la requête nécessite des paramètres supplémentaires, tels qu'un identifiant de groupe ou d'utilisateur. Ensuite, obtenez ces valeurs. Vous devrez peut-être d'abord effectuer une autre requête API pour obtenir les informations dont vous avez besoin.
6. Déterminez si vous devez modifier le corps de la requête d'exemple. Le cas échéant, vous pouvez sélectionner **Modèle** pour connaître les exigences relatives à chaque champ.
7. Sélectionnez **Try it out**.
8. Fournissez les paramètres requis ou modifiez le corps de la requête selon les besoins.
9. Sélectionnez **Exécuter**.
10. Examinez le code de réponse pour déterminer si la requête a réussi.

Opérations de l'API de gestion de la grille dans StorageGRID

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

Cette liste ne comprend que les opérations disponibles dans l'API publique.

- **comptes** : Opérations permettant de gérer les comptes locataires de stockage, y compris la création de nouveaux comptes et la récupération de l'utilisation du stockage pour un compte donné.
- **historique des alertes** : opérations sur les alertes résolues.
- **récepteurs d'alertes** : Opérations sur les récepteurs de notifications d'alerte (courriel).
- **règles d'alerte** : Opérations sur les règles d'alerte.
- **silences d'alerte** : opérations sur les silences d'alerte.
- **Alertes** : Opérations sur les alertes.
- **audit** : Opérations permettant de lister et de mettre à jour la configuration d'audit.
- **auth** : Opérations permettant d'authentifier la session utilisateur.

  L'API Grid Management prend en charge le schéma d'authentification par jeton porteur. Pour vous connecter, vous fournissez un nom d'utilisateur et un mot de passe dans le corps JSON de la requête 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 suivantes (« Authorization: Bearer *token* »). Le jeton expire après 16 heures.

  Si l'authentification unique est activée pour le système StorageGRID, vous devez suivre une procédure différente. Consultez la section « Authentification à l'API si l'authentification unique est activée ».

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

- **client-certificates** : Opérations permettant de configurer les certificats clients afin que StorageGRID puisse être accessible en toute sécurité à l'aide d'outils de surveillance externes.
- **config** : Opérations relatives à la version du produit et aux versions de l'API de gestion de grille. Vous pouvez afficher la version de la publication du produit et les versions majeures de l'API de gestion de grille prises en charge par cette publication, et vous pouvez désactiver les versions obsolètes de l'API.
- **Fonctionnalités désactivées** : Opérations permettant d'afficher les fonctionnalités qui pourraient avoir été désactivées.
- **serveurs DNS** : Opérations permettant de lister et de modifier les serveurs DNS externes configurés.
- **drive-details** : Opérations sur les disques pour des modèles spécifiques d'appliances de stockage.
- **endpoint-domain-names** : Opérations permettant de lister et de modifier les noms de domaine des endpoints S3.
- **codage d'effacement** : opérations sur les profils de codage d'effacement.
- **expansion** : opérations sur l'expansion (niveau procédure).
- **expansion-nodes** : Opérations sur l'expansion (niveau du nœud).
- **sites d'expansion** : Opérations sur l'expansion (au niveau du site).
- **grid-networks** : Opérations permettant de lister et de modifier la liste du Grid Network.

- **grid-passwords** : Opérations pour la gestion des mots de passe de la grille.
- **Groupes** : Opérations permettant de gérer les groupes d'administrateurs de grille locaux et de récupérer les 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 de groupe et d'utilisateur fédérés.
- **ilm** : Opérations sur la gestion du cycle de vie de l'information (ILM).
- **in-progress-procedures** : Récupère les procédures de maintenance en cours.
- **licence** : Opérations permettant de récupérer et de mettre à jour la licence StorageGRID.
- **journaux** : Opérations de collecte et de téléchargement des fichiers journaux.v
- **Métriques** : Opérations sur les métriques StorageGRID, notamment les requêtes de métriques instantanées à un instant précis et les requêtes de métriques sur une plage de temps. L'API de gestion du réseau utilise l'outil de surveillance système Prometheus comme source de données principale. Pour plus d'informations sur la construction de requêtes Prometheus, consultez le site web de Prometheus.

> Les indicateurs dont le nom contient `private` sont destinés à un usage interne uniquement. Ces indicateurs sont susceptibles d'être modifiés 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 du stockage des nœuds.
- **ntp-servers** : Opérations permettant de lister ou de mettre à jour les serveurs externes Network Time Protocol (NTP).
- **objets** : Opérations sur les objets et les métadonnées des objets.
- **récupération** : Opérations pour la procédure de récupération.
- **recovery-package** : Opérations de téléchargement du recovery package.
- **régions** : Opérations permettant de visualiser et de créer des régions.
- **s3-object-lock** : Opérations sur les paramètres globaux de verrouillage d'objet S3.
- **server-certificate** : Opérations permettant de consulter 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.
- **classes-de-trafic** : Opérations relatives aux politiques de classification du trafic.
- **untrusted-client-network** : Opérations sur la configuration du réseau client non fiable.
- **utilisateurs** : Opérations permettant de consulter et de gérer les utilisateurs de Grid Manager.

Gestion des versions de l'API Grid Management dans StorageGRID

L'API de gestion de grille utilise le versionnage pour permettre des mises à niveau sans interruption de service.

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

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

La version majeure de l'API est mise à jour lorsque des modifications qui ne sont pas compatibles avec les versions précédentes sont apportées. La version mineure de l'API est mise à jour lorsque des modifications qui sont compatibles avec les versions précédentes sont apportées. 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 incrémentée en fonction du type de modifications apportées.

Type de modification de l'API	Ancienne version	Nouvelle version
Compatible avec les versions antérieures	2,1	2,2
Non compatible avec les versions antérieures	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 StorageGRID, vous continuez à avoir accès à l'ancienne version de l'API pendant au moins une version de StorageGRID.

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

Les requêtes obsolètes sont marquées comme dépréciées de la manière suivante :

- L'en-tête de réponse est « Deprecated: true »
- Le corps de la réponse JSON inclut "deprecated": true
- Un avertissement de dépréciation est ajouté au fichier nms.log. Par exemple :

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

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

Utilisez la `GET /versions` requête API pour obtenir une liste des versions majeures de l'API prises en charge. Cette requête 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
  ]
}
```

Spécifiez 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 d'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
```

Protégez-vous contre les attaques Cross-Site Request Forgery (CSRF) dans StorageGRID

Vous pouvez contribuer à protéger StorageGRID contre les attaques de type Cross-Site Request Forgery (CSRF) en utilisant des jetons CSRF pour renforcer l'authentification qui utilise des cookies. Le Grid Manager et le Tenant Manager activent automatiquement cette fonctionnalité de sécurité ; les autres clients API peuvent choisir de l'activer ou non lors de leur connexion.

Un attaquant capable de déclencher une requête vers un autre site (par exemple avec un formulaire HTTP POST) peut faire en sorte que certaines requêtes soient effectuées en utilisant les cookies de l'utilisateur connecté.

StorageGRID contribue à la protection contre les attaques CSRF grâce à l'utilisation de jetons CSRF. Lorsqu'elle est activée, le contenu d'un cookie spécifique doit correspondre à celui d'un en-tête spécifique ou d'un paramètre spécifique du corps de la requête POST.

Pour activer cette fonctionnalité, définissez le paramètre `csrfToken` sur `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 cette option est activée, un `GridCsrfToken` cookie est défini avec une valeur aléatoire pour les connexions au Grid Manager, et le `AccountCsrfToken` cookie est défini avec une valeur aléatoire pour les connexions au Tenant Manager.

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

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

Consultez la documentation API en ligne pour obtenir des exemples et des détails supplémentaires.

> Les requêtes comportant un cookie de jeton CSRF défini appliqueront également l'en-tête "Content-Type: application/json" à toute requête attendant un corps de requête JSON, comme protection supplémentaire contre les attaques CSRF.

Utilisez l'API si l'authentification unique est activée

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

Si vous avez "authentification unique (SSO) configurée et activée" 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 de gestion de la grille ou l'API de gestion des locataires.

Connectez-vous 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.
- Pour accéder à l'API de gestion des locataires, vous devez connaître l'identifiant 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, qui se trouve dans le répertoire des fichiers d'installation de StorageGRID (`./rpms` pour RHEL, `./debs` pour Ubuntu ou Debian, et `./vsphere` pour VMware).

- Un exemple de workflow 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`.

  > Le flux de travail curl présenté en exemple ne protège pas le mot de passe contre la consultation par d'autres utilisateurs.

Si vous rencontrez 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 les valeurs des arguments suivants :
   - La méthode SSO. Saisissez ADFS ou adfs.
   - Nom d'utilisateur SSO
   - Le domaine sur lequel StorageGRID est installé
   - L'adresse de StorageGRID
   - L'identifiant 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 le résultat. Vous pouvez désormais utiliser le jeton pour d'autres requêtes, comme vous le feriez avec l'API si l'authentification unique n'était pas utilisée.
3. Si vous souhaitez utiliser des requêtes curl, suivez 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 la grille, utilisez 0 comme `TENANTACCOUNTID`.

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

Cet exemple illustre 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 et encodée en URL, mais elle n'inclut pas la couche d'encodage 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. Enregistrez le `SAMLRequest` de la réponse pour l'utiliser dans les commandes suivantes.

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

d. Obtenez une URL complète qui inclut l'ID de requête client depuis 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'identifiant de la requête 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'identifiant de la requête client à partir de la réponse.

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

f. Envoyez vos identifiants 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 multifactorielle (MFA) est activée pour votre système SSO, le formulaire envoyé 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. Enregistrez le `MSISAuth` cookie issu de la réponse.

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

h. Envoyez une requête GET à l'emplacement spécifié avec les cookies issus de la requête 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 les informations de session AD FS pour une utilisation ultérieure lors de la déconnexion, et le corps de la réponse contient la SAMLResponse dans un champ de formulaire caché.

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

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

j. À l'aide des données enregistrées `SAMLResponse`, effectuez une demande StorageGRID`/api/saml-response` pour générer un jeton d'authentification StorageGRID.

Pour `RelayState`, utilisez l'ID du compte locataire ou 0 si vous souhaitez vous connecter à l'API de gestion de la grille.

```
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 en tant que `MYTOKEN`.

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

Vous pouvez désormais utiliser `MYTOKEN` pour d'autres requêtes, de la même manière que vous utiliseriez l'API si l'authentification unique n'était pas utilisée.

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

Si l'authentification unique (SSO) est activée, vous devez effectuer une série de requêtes API pour vous déconnecter de l'API de gestion de la grille ou de l'API de gestion des locataires. 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 depuis la page de déconnexion unique de votre organisation. Ou, vous pouvez déclencher une déconnexion unique (SLO) depuis StorageGRID, ce qui requiert un jeton d'authentification StorageGRID valide.

Étapes

1. Pour générer une requête de déconnexion signée, transmettez le `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 requête à l'URL de déconnexion pour déclencher le SLO et pour être redirigé vers StorageGRID.

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

La réponse 302 est renvoyée. L'emplacement de redirection n'est pas applicable à la déconnexion via 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 d'accès StorageGRID fonctionne de la même manière qu'en l'absence d'authentification unique (SSO). Si le cookie « sso=true » n'est pas fourni, l'utilisateur est déconnecté de StorageGRID sans affecter l'état de l'authentification unique.

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

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

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

Utilisez l'API StorageGRID si l'authentification unique est activée (Entra ID)

Si vous avez "authentification unique (SSO) configurée et activée" et que vous utilisez Entra ID comme fournisseur SSO, vous pouvez utiliser deux exemples de scripts pour obtenir un jeton d'authentification valide pour l'API de gestion de grille ou l'API de gestion des locataires.

Connectez-vous à l'API si l'authentification unique Entra ID est activée

Ces instructions s'appliquent si vous utilisez Entra ID 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.
- Pour accéder à l'API de gestion des locataires, vous devez connaître l'identifiant 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 RHEL, `./debs` pour Ubuntu ou Debian, et `./vsphere` pour VMware).

Pour créer votre propre intégration API avec Entra ID, consultez le script `storagegrid-ssoauth-azure.py`. Le script Python effectue deux requêtes directement à StorageGRID (la première pour obtenir la SAMLRequest, et la seconde pour obtenir le jeton d'autorisation), et appelle également le script Node.js pour interagir avec Entra ID afin d'effectuer les opérations SSO.

Les opérations d'authentification unique (SSO) peuvent être exécutées via une série de requêtes API, mais leur mise en œuvre n'est pas simple. Le module Puppeteer Node.js est utilisé pour extraire les données de l'interface SSO Entra ID.

Si vous rencontrez 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 SSO Entra ID.

3. Lorsque vous y êtes invité, saisissez les valeurs des arguments suivants (ou transmettez-les en tant que paramètres) :
   - L'adresse e-mail SSO utilisée pour vous connecter à Entra ID
   - L'adresse de StorageGRID
   - L'identifiant du compte locataire, si vous souhaitez accéder à l'API de gestion des locataires
4. Lorsque vous y serez invité, saisissez votre mot de passe et soyez prêt à fournir une autorisation MFA à Entra ID si cela vous est demandé.

```
c:\Users\user\Documents\azure_sso>py storagegrid-azure-ssoauth.py --sso-email-address user@my-domain.com
--sg-address storagegrid.examp.e.com --tenant-account-id 0
Enter the user's SSO password:
********************************************************************************

Watch for and approve a 2FA authorization request
********************************************************************************
StorageGRID Auth Token: {'responseTime': '2021-10-04T21:30:48.807Z', 'status': 'success', 'apiVersion':
'3.4', 'data': '4807d93e-a3df-48f2-9680-906cd255979e'}
```

> Ce script suppose que l'authentification multifacteur (MFA) est effectuée via Microsoft Authenticator. Il se peut que vous deviez modifier le script pour prendre en charge d'autres formes de MFA (comme la saisie d'un code reçu par message texte).

Le jeton d'autorisation StorageGRID est fourni dans le résultat. Vous pouvez désormais utiliser le jeton pour d'autres requêtes, comme vous le feriez avec l'API si l'authentification unique n'était pas utilisée.

Utilisez l'API StorageGRID si l'authentification unique est activée (PingFederate)

Si vous avez "authentification unique (SSO) configurée et activée" 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 la grille ou l'API de gestion des locataires.

Connectez-vous 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.
- Pour accéder à l'API de gestion des locataires, vous devez connaître l'identifiant 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, qui se trouve dans le répertoire des fichiers d'installation de StorageGRID (`./rpms` pour RHEL, `./debs` pour Ubuntu ou Debian, et `./vsphere` pour VMware).
- Un exemple de workflow 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`.

  > Le flux de travail curl présenté en exemple ne protège pas le mot de passe contre la consultation par d'autres utilisateurs.

  Si vous rencontrez 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 les valeurs des arguments suivants :

   - La méthode SSO. Vous pouvez saisir n'importe quelle variante de « pingfederate » (PINGFEDERATE, pingfederate, etc.).
   - 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 une valeur quelconque.
   - L'adresse de StorageGRID
   - L'identifiant 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 le résultat. Vous pouvez désormais utiliser le jeton pour d'autres requêtes, comme vous le feriez avec l'API si l'authentification unique n'était pas utilisée.

3. Si vous souhaitez utiliser des requêtes curl, suivez 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 la grille, utilisez 0 comme `TENANTACCOUNTID`.

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

   Cet exemple illustre une requête POST pour obtenir une URL d'authentification signée pour TENANTACCOUNTID. Les résultats seront transmis à python -m json.tool afin de 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 et encodée en URL, mais elle n'inclut pas la couche d'encodage JSON supplémentaire.

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

   c. Enregistrez le `SAMLRequest` de la réponse pour l'utiliser dans les commandes suivantes.

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

   d. Exportez la réponse et le cookie, puis affichez 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 affichez la réponse :

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

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

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

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

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

g. Exportez la valeur « action » :

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

h. Envoyez les cookies avec les identifiants :

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

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

j. À l'aide des données enregistrées `SAMLResponse`, effectuez une demande StorageGRID`/api/saml-response` pour générer un jeton d'authentification StorageGRID.

   Pour `RelayState`, utilisez l'ID du compte locataire ou 0 si vous souhaitez vous connecter à l'API de gestion de la grille.

```
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 en tant que `MYTOKEN`.

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

Vous pouvez désormais utiliser `MYTOKEN` pour d'autres requêtes, de la même manière que vous utiliseriez l'API si l'authentification unique n'était pas utilisée.

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

Si l'authentification unique (SSO) est activée, vous devez effectuer une série de requêtes API pour vous déconnecter de l'API de gestion de la grille ou de l'API de gestion des locataires. 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 depuis la page de déconnexion unique de votre organisation. Ou, vous pouvez déclencher une déconnexion unique (SLO) depuis StorageGRID, ce qui requiert un jeton d'authentification StorageGRID valide.

Étapes

1. Pour générer une requête de déconnexion signée, transmettez le `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 requête à l'URL de déconnexion pour déclencher le SLO et pour être redirigé vers StorageGRID.

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

La réponse 302 est renvoyée. L'emplacement de redirection n'est pas applicable à la déconnexion via 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 d'accès StorageGRID fonctionne de la même manière qu'en l'absence d'authentification unique (SSO). Si le cookie « sso=true » n'est pas fourni, l'utilisateur est déconnecté de StorageGRID sans affecter l'état de l'authentification unique.

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

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

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

Désactivez les fonctionnalités de StorageGRID avec l'API

Vous pouvez utiliser l'API de gestion de la grille pour désactiver complètement certaines fonctionnalités dans le 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 dans le 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 disposant de l'autorisation **Root access** d'utiliser cette fonctionnalité.

Pour comprendre en quoi cette fonctionnalité peut 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 clients. Afin de protéger la sécurité des objets de ses locataires, la société A souhaite s'assurer que ses propres employés ne puissent jamais accéder à un compte client après son déploiement._

Company A peut atteindre cet objectif en utilisant le système Deactivate Features dans l'API Grid Management. En désactivant complètement la fonctionnalité **Change tenant root password** dans le Grid Manager (à la fois dans l'interface utilisateur et dans l'API), Company A s'assure que les utilisateurs Admin — y compris l'utilisateur root et les utilisateurs appartenant à des groupes disposant de l'autorisation **Root access** — ne peuvent pas modifier le mot de passe de l'utilisateur root de n'importe quel compte locataire._

Étapes

1. Accédez à la documentation Swagger de l'API de gestion de grille. Voir "Utilisez l'API de gestion de grille".
2. Localisez le point de terminaison Deactivate Features.
3. Pour désactiver une fonctionnalité, telle que Change tenant root password, envoyez un corps à l'API comme ceci :

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

   Lorsque la demande est terminée, la fonctionnalité Modifier le mot de passe root du locataire est désactivée. L'autorisation de gestion **Modifier le mot de passe root du locataire** n'apparaît plus dans l'interface utilisateur, et toute requête API qui tente de modifier le mot de passe root d'un locataire échouera avec "403 Forbidden."

Réactiver les fonctionnalités désactivées

Par défaut, vous pouvez utiliser l'API de gestion de la grille pour réactiver une fonctionnalité désactivée. Toutefois, si vous souhaitez empêcher que des fonctionnalités désactivées ne soient jamais 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 rétablir toute fonctionnalité perdue.

Étapes

1. Accédez à la documentation Swagger de l'API Grid Management.

2. Localisez le point de terminaison Deactivate Features.
3. Pour réactiver toutes les fonctionnalités, envoyez un corps de requête à l'API comme ceci :

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

Une fois cette requête terminée, toutes les fonctionnalités, y compris la fonctionnalité Changer le mot de passe racine du locataire, sont réactivées. L'autorisation de gestion **Changer le mot de passe racine du locataire** apparaît désormais dans l'interface utilisateur, et toute requête API visant à modifier le mot de passe racine d'un locataire aboutira, à condition que l'utilisateur dispose de l'autorisation de gestion **Accès racine** ou **Changer le mot de passe racine du locataire**.

L'exemple précédent réactive *toutes* les fonctionnalités désactivées. Si d'autres fonctionnalités ont été désactivées et doivent le rester, vous devez les spécifier explicitement dans la requête PUT. Par exemple, pour réactiver la fonctionnalité « Modifier le mot de passe racine du locataire » tout en continuant de désactiver l'autorisation de gestion storageAdmin, envoyez la requête PUT suivante :

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