



Administration d'un système StorageGRID

StorageGRID 11.5

NetApp
April 11, 2024

This PDF was generated from <https://docs.netapp.com/fr-fr/storagegrid-115/admin/web-browser-requirements.html> on April 11, 2024. Always check docs.netapp.com for the latest.

Sommaire

- Administration d'un système StorageGRID 1
 - Navigateurs Web pris en charge 1
 - Connexion au Grid Manager 1
 - Déconnexion du gestionnaire de grille 5
 - Modification de votre mot de passe 6
 - Modification de la phrase secrète de provisionnement 7
 - Modification du délai d'expiration de la session du navigateur 8
 - Affichage des informations de licence StorageGRID 10
 - Mise à jour des informations de licence StorageGRID 11
 - Via l'API de gestion du grid 11
 - Utilisation des certificats de sécurité StorageGRID 25

Administration d'un système StorageGRID

Suivez ces instructions pour configurer et administrer un système StorageGRID.

Ces instructions expliquent comment utiliser Grid Manager pour configurer des groupes et des utilisateurs, créer des comptes de locataires pour permettre aux applications client S3 et Swift de stocker et récupérer des objets, configurer et gérer des réseaux StorageGRID, configurer AutoSupport, gérer des paramètres de nœud, etc.



Il a été déplacé les instructions de gestion des objets avec des règles et des règles de gestion du cycle de vie des informations (ILM) vers "[Gestion des objets avec ILM](#)".

Ces instructions s'adresse au personnel technique qui devra configurer, administrer et prendre en charge un système StorageGRID après son installation.

Ce dont vous avez besoin

- Vous disposez d'une compréhension générale du système StorageGRID.
- Vous disposez d'une connaissance assez détaillée des shells de commande Linux, de la mise en réseau et de la configuration matérielle du serveur.

Navigateurs Web pris en charge

Vous devez utiliser un navigateur Web pris en charge.

Navigateur Web	Version minimale prise en charge
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

Vous devez régler la fenêtre du navigateur sur une largeur recommandée.

Largeur du navigateur	Pixels
Minimum	1024
Optimale	1280

Connexion au Grid Manager

Vous accédez à la page de connexion de Grid Manager en entrant le nom de domaine complet (FQDN) ou l'adresse IP d'un nœud d'administration dans la barre d'adresse d'un navigateur Web pris en charge.

Ce dont vous avez besoin

- Vous devez disposer de vos identifiants de connexion.
- Vous devez disposer de l'URL pour Grid Manager.
- Vous devez utiliser un navigateur Web pris en charge.
- Les cookies doivent être activés dans votre navigateur Web.
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

Chaque système StorageGRID comprend un nœud d'administration principal et un nombre quelconque de nœuds d'administration non primaires. Vous pouvez vous connecter au Gestionnaire de grille sur n'importe quel nœud d'administration pour gérer le système StorageGRID. Cependant, les nœuds d'administration ne sont pas exactement les mêmes :

- Les accusés de réception d'alarme (système hérité) effectués sur un nœud d'administration ne sont pas copiés sur d'autres nœuds d'administration. Pour cette raison, les informations affichées pour les alarmes peuvent ne pas être identiques sur chaque nœud d'administration.
- Certaines procédures de maintenance peuvent uniquement être effectuées depuis le nœud d'administration principal.

Si des nœuds admin sont inclus dans un groupe haute disponibilité (HA), vous vous connectez à l'aide de l'adresse IP virtuelle du groupe haute disponibilité ou d'un nom de domaine complet mappé sur l'adresse IP virtuelle. Le nœud d'administration principal doit être sélectionné comme maître préféré du groupe, de sorte que lorsque vous accédez au Grid Manager, vous y accédez sur le nœud d'administration principal, sauf si le nœud d'administration principal n'est pas disponible.

Étapes

1. Lancez un navigateur Web pris en charge.
2. Dans la barre d'adresse du navigateur, entrez l'URL du Grid Manager :

`https://FQDN_or_Admin_Node_IP/`

où *FQDN_or_Admin_Node_IP* Est un nom de domaine complet ou l'adresse IP d'un nœud d'administration ou l'adresse IP virtuelle d'un groupe de nœuds d'administration haute disponibilité.

Si vous devez accéder à Grid Manager sur un port autre que le port standard pour HTTPS (443), entrez les informations suivantes, où *FQDN_or_Admin_Node_IP* Est un nom de domaine complet ou une adresse IP et le port est le numéro de port :

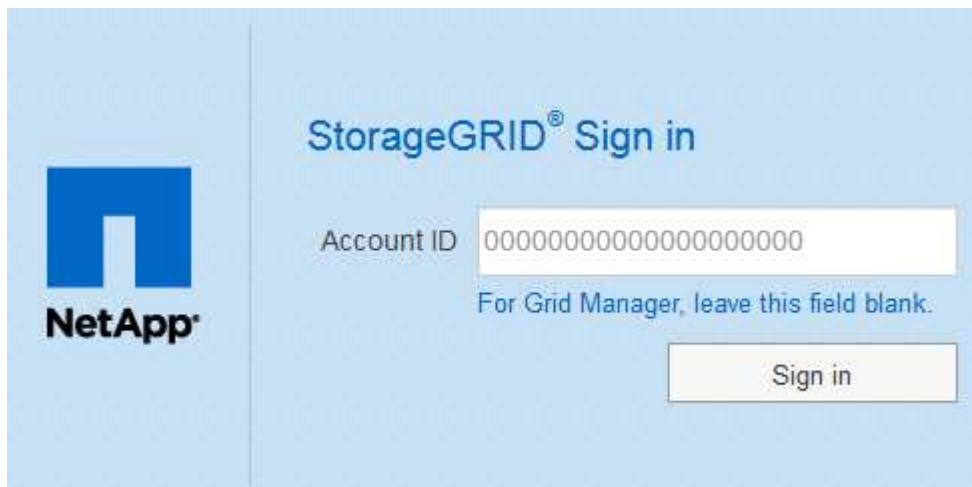
`https://FQDN_or_Admin_Node_IP:port/`

3. Si vous êtes invité à recevoir une alerte de sécurité, installez le certificat à l'aide de l'assistant d'installation du navigateur.
4. Connectez-vous au Grid Manager :
 - Si l'authentification unique (SSO) n'est pas utilisée pour votre système StorageGRID :
 - i. Saisissez votre nom d'utilisateur et votre mot de passe pour le Grid Manager.
 - ii. Cliquez sur **connexion**.



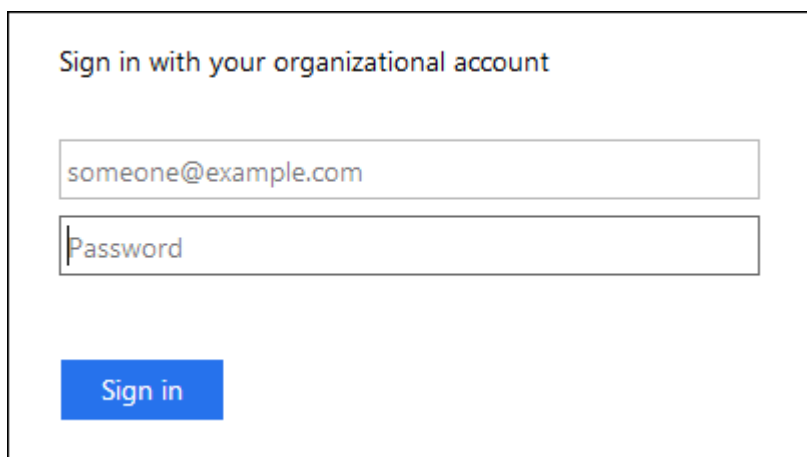
The image shows the 'StorageGRID® Grid Manager' login page. On the left is the NetApp logo. The main area has a light blue background with the title 'StorageGRID® Grid Manager' in blue. Below the title are two white input fields: 'Username' and 'Password'. To the right of the 'Password' field is a grey 'Sign in' button.

- Si l'authentification SSO est activée pour votre système StorageGRID et qu'il s'agit de la première fois que vous avez accédé à l'URL sur ce navigateur :
 - i. Cliquez sur **connexion**. Vous pouvez laisser le champ ID compte vide.



The image shows the 'StorageGRID® Sign in' page. On the left is the NetApp logo. The main area has a light blue background with the title 'StorageGRID® Sign in' in blue. Below the title is a white input field labeled 'Account ID' containing a long string of zeros. Below this field is the text 'For Grid Manager, leave this field blank.' in blue. To the right of the input field is a grey 'Sign in' button.

- ii. Saisissez vos identifiants SSO standard sur la page de connexion SSO de votre entreprise. Par exemple :



The image shows a login form titled 'Sign in with your organizational account'. It has two white input fields: the first contains the email 'someone@example.com' and the second is labeled 'Password'. Below the fields is a blue 'Sign in' button.

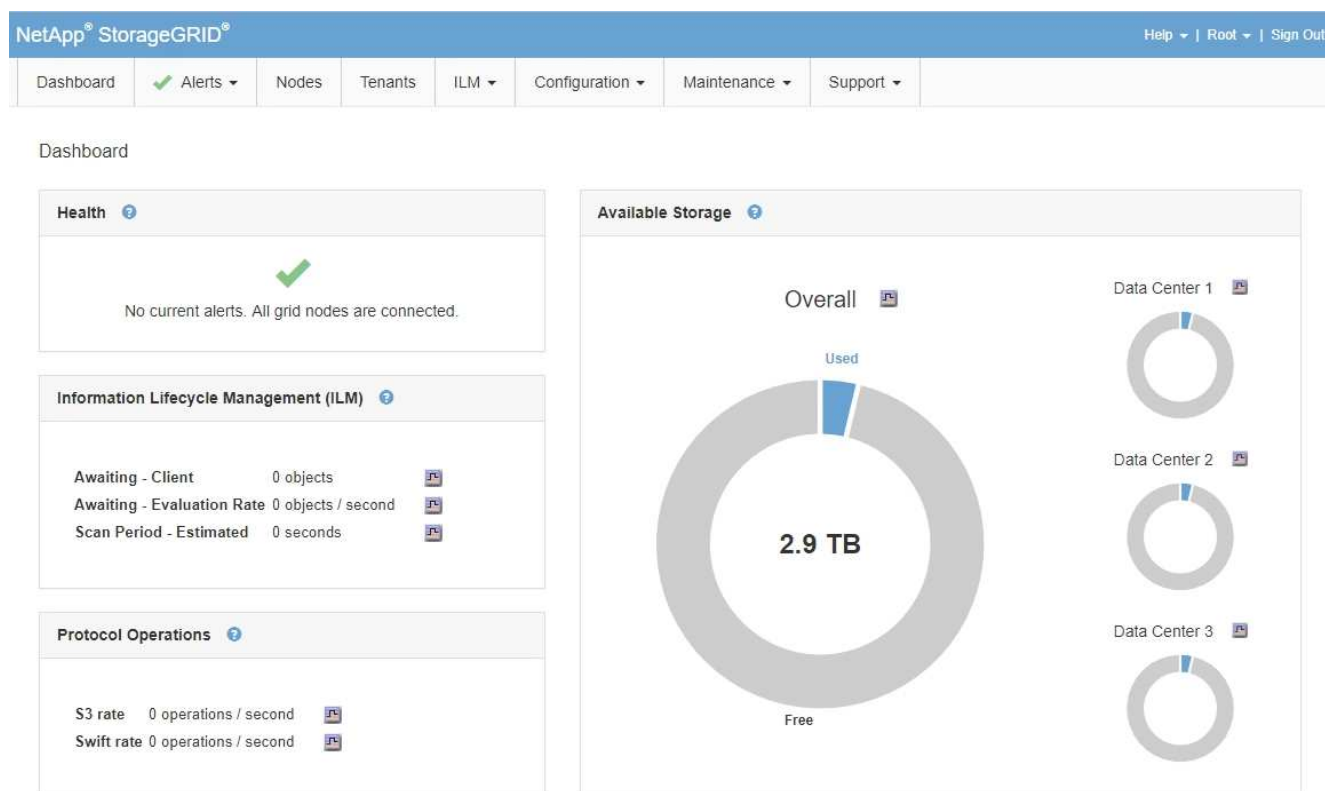
- Si l'authentification SSO est activée pour votre système StorageGRID et que vous avez déjà accédé au Grid Manager ou à un compte de locataire :

i. Effectuez l'une des opérations suivantes :

- Saisissez **0** (l'ID de compte du gestionnaire de grille), puis cliquez sur **connexion**.
- Sélectionnez **Grid Manager** s'il apparaît dans la liste des comptes récents, puis cliquez sur **connexion**.



ii. Connectez-vous à l'aide de vos identifiants SSO standard sur la page de connexion SSO de votre entreprise. Lorsque vous êtes connecté, la page d'accueil de Grid Manager s'affiche, qui inclut le tableau de bord. Pour connaître les informations fournies, consultez la section « Affichage du tableau de bord » dans les instructions de surveillance et de dépannage de StorageGRID.



5. Pour vous connecter à un autre nœud d'administration :

Option	Étapes
SSO non activé	<p>a. Dans la barre d'adresse du navigateur, entrez le nom de domaine complet ou l'adresse IP de l'autre nœud d'administration. Indiquez le numéro de port requis.</p> <p>b. Saisissez votre nom d'utilisateur et votre mot de passe pour le Grid Manager.</p> <p>c. Cliquez sur connexion.</p>
SSO activé	<p>Dans la barre d'adresse du navigateur, entrez le nom de domaine complet ou l'adresse IP de l'autre nœud d'administration.</p> <p>Si vous vous êtes connecté à un nœud d'administration, vous pouvez accéder aux autres nœuds d'administration sans avoir à vous reconnecter. Toutefois, si votre session SSO expire, vous êtes invité à saisir à nouveau vos informations d'identification.</p> <p>Remarque : SSO n'est pas disponible sur le port restreint Grid Manager. Vous devez utiliser le port HTTPS par défaut (443) si vous souhaitez que les utilisateurs s'authentifient avec une connexion unique.</p>

Informations associées

["Navigateurs Web pris en charge"](#)

["Contrôle de l'accès par pare-feu"](#)

["Configuration des certificats de serveur"](#)

["Configuration de l'authentification unique"](#)

["Gestion des groupes d'administration"](#)

["Gestion des groupes haute disponibilité"](#)

["Utilisez un compte de locataire"](#)

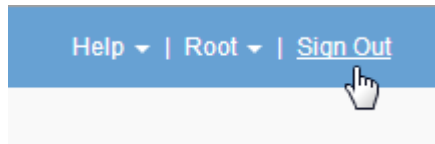
["Moniteur et amp ; dépannage"](#)

Déconnexion du gestionnaire de grille

Lorsque vous avez terminé de travailler avec le Gestionnaire de grille, vous devez vous déconnecter pour vous assurer que les utilisateurs non autorisés ne peuvent pas accéder au système StorageGRID. La fermeture de votre navigateur risque de ne pas vous déconnecter du système, en fonction des paramètres des cookies du navigateur.

Étapes

1. Repérez le lien **Déconnexion** dans le coin supérieur droit de l'interface utilisateur.



2. Cliquez sur **Déconnexion**.

Option	Description
SSO non utilisé	<p>Vous êtes déconnecté du nœud d'administration.</p> <p>La page de connexion de Grid Manager s'affiche.</p> <p>Remarque : si vous vous êtes connecté à plusieurs nœuds d'administration, vous devez vous déconnecter de chaque nœud.</p>
SSO activé	<p>Vous êtes déconnecté de tous les nœuds d'administration auxquels vous accédez. La page de connexion StorageGRID s'affiche. Grid Manager est répertorié comme valeur par défaut dans la liste déroulante comptes récents et le champ ID compte affiche 0.</p> <p>Remarque : si SSO est activé et que vous êtes également connecté au Gestionnaire de tenant, vous devez également vous déconnecter du compte de tenant pour vous déconnecter de SSO.</p>

Informations associées

["Configuration de l'authentification unique"](#)

["Utilisez un compte de locataire"](#)

Modification de votre mot de passe

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

Ce dont vous avez besoin

Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.

Description de la 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 plutôt modifier votre mot de passe dans le référentiel d'identité externe, par exemple Active Directory ou OpenLDAP.

Étapes

1. Dans l'en-tête de Grid Manager, sélectionnez **votre nom** > **Modifier le mot de passe**.
2. Saisissez votre mot de passe actuel.
3. Saisissez un nouveau mot de passe.

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

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

Modification de la phrase secrète de provisionnement

Utilisez cette procédure pour modifier la phrase secrète du provisionnement StorageGRID. La phrase de passe est requise pour les procédures de restauration, d'extension et de maintenance. La phrase de passe est également requise pour télécharger les sauvegardes du pack de récupération qui incluent les informations de topologie de la grille et les clés de chiffrement pour le système StorageGRID.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations Maintenance ou accès racine.
- Vous devez disposer de la phrase secrète de provisionnement actuelle.

Description de la tâche

Le mot de passe de provisionnement est requis pour de nombreuses procédures d'installation et de maintenance, ainsi que pour le téléchargement du progiciel de restauration. La phrase de passe de provisionnement n'est pas répertoriée dans le `Passwords.txt` fichier. Veuillez à documenter la phrase de passe de provisionnement et à la conserver dans un emplacement sûr et sécurisé.

Étapes

1. Sélectionnez **Configuration** > **contrôle d'accès** > **mots de passe de grille**.

The screenshot shows the NetApp StorageGRID web interface. At the top is a blue header bar with the text 'NetApp® StorageGRID®' on the left and 'Help ▼ | Root ▼ | Sign Out' on the right. Below the header is a navigation menu with tabs: 'Dashboard', 'Alerts ▼' (with a green checkmark), 'Nodes', 'Tenants', 'ILM ▼', 'Configuration ▼', 'Maintenance ▼', and 'Support ▼'. The 'Configuration' tab is selected. Below the navigation menu, the page title is 'Grid Passwords' with a subtitle 'Change the provisioning passphrase and other passwords for your StorageGRID system.' The main section is titled 'Change Provisioning Passphrase'. It contains a paragraph explaining that the provisioning passphrase is required for installation, expansion, or maintenance procedures that change the grid topology, and that it is also required for downloading backups and encryption keys. Below this text are three input fields: 'Current Provisioning Passphrase', 'New Provisioning Passphrase', and 'Confirm New Provisioning Passphrase'. Each field contains a series of asterisks. A blue 'Save' button is located at the bottom right of the form.

2. Saisissez votre phrase secrète pour le provisionnement.
3. Saisissez la nouvelle phrase de passe. La phrase de passe doit contenir au moins 8 caractères et 32 caractères. Les phrases passe sont sensibles à la casse.



Stocker la nouvelle phrase secrète pour le provisionnement dans un emplacement sécurisé. Elle est requise pour les procédures d'installation, d'extension et de maintenance.

4. Saisissez à nouveau la nouvelle phrase de passe, puis cliquez sur **Enregistrer**.

Le système affiche une bannière verte de réussite lorsque la modification de la phrase de passe de provisionnement est terminée. Le changement devrait prendre moins d'une minute.

NetApp® StorageGRID® Help ▾ | Root ▾ | Sign Out

Dashboard Alerts ▾ Nodes Tenants ILM ▾ Configuration ▾ Maintenance ▾ Support ▾

Grid Passwords
Change the provisioning passphrase and other passwords for your StorageGRID system.

Provisioning passphrase successfully changed. Go to the [Recovery Package page](#) to download a new Recovery Package.

Change Provisioning Passphrase

The provisioning passphrase is required for any installation, expansion, or maintenance procedure that makes changes to the grid topology. This passphrase is also required to download backups of the grid topology information and encryption keys for the StorageGRID system. After changing the provisioning passphrase, you must download a new Recovery Package.

Current Provisioning Passphrase

New Provisioning Passphrase

Confirm New Provisioning Passphrase

5. Sélectionnez le lien **Recovery Package page** dans la bannière de réussite.
6. Téléchargez le nouveau package de récupération depuis Grid Manager. Sélectionnez **Maintenance > Recovery Package** et saisissez la nouvelle phrase de passe d'approvisionnement.



Après avoir modifié la phrase de passe de provisionnement, vous devez télécharger immédiatement un nouveau progiciel de restauration. Le fichier du progiciel de récupération vous permet de restaurer le système en cas de défaillance.

Modification du délai d'expiration de la session du navigateur

Vous pouvez contrôler si les utilisateurs de Grid Manager et de tenant Manager sont déconnectés s'ils sont inactifs pendant plus d'un certain temps.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

Le délai d'inactivité de l'interface graphique est défini par défaut sur 900 secondes (15 minutes). Si la session de navigateur d'un utilisateur n'est pas active pendant cette période, la session est expirée.

Si nécessaire, vous pouvez augmenter ou diminuer le délai d'inactivité en définissant l'option d'affichage délai d'inactivité de l'interface graphique.

Si l'authentification unique (SSO) est activée et que la session du navigateur d'un utilisateur est expirée, le système se comporte comme si l'utilisateur a cliqué sur **Déconnexion** manuellement. L'utilisateur doit saisir à nouveau ses identifiants SSO pour accéder à StorageGRID.



Le délai d'expiration de session utilisateur peut également être contrôlé par les éléments suivants :

- Un minuteur StorageGRID séparé non configurable, inclus pour la sécurité du système. Par défaut, le jeton d'authentification de chaque utilisateur expire 16 heures après la connexion de l'utilisateur. Lorsqu'une authentification de l'utilisateur expire, cet utilisateur est automatiquement déconnecté, même si la valeur du délai d'inactivité de l'interface graphique n'a pas été atteinte. Pour renouveler le jeton, l'utilisateur doit se reconnecter.
- Paramètres de délai pour le fournisseur d'identité, en supposant que SSO est activé pour StorageGRID.

Étapes

1. Sélectionnez **Configuration > Paramètres système > Options d'affichage**.
2. Pour **délai d'inactivité de l'interface graphique utilisateur**, entrez un délai d'expiration de 60 secondes ou plus.

Définissez ce champ sur 0 si vous ne souhaitez pas utiliser cette fonctionnalité. Les utilisateurs sont déconnectés 16 heures après leur connexion, quand leurs jetons d'authentification expirent.



Display Options

Updated: 2017-03-09 20:36:53 MST

Current Sender	ADMIN-DC1-ADM1
Preferred Sender	ADMIN-DC1-ADM1
GUI Inactivity Timeout	900
Notification Suppress All	<input type="checkbox"/>

Apply Changes

3. Cliquez sur **appliquer les modifications**.

Le nouveau paramètre n'affecte pas les utilisateurs actuellement connectés. Les utilisateurs doivent se reconnecter ou actualiser leur navigateur pour que le nouveau paramètre de délai d'expiration prenne effet.

Informations associées

["Fonctionnement de l'authentification unique"](#)

Affichage des informations de licence StorageGRID

Vous pouvez afficher les informations relatives aux licences de votre système StorageGRID, comme la capacité de stockage maximale de votre réseau, si nécessaire.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.

Description de la tâche

En cas de problème avec la licence logicielle de ce système StorageGRID, le panneau intégrité du tableau de bord inclut une icône d'état de la licence et un lien **Licence**. Le numéro indique le nombre de problèmes liés à la licence.

Dashboard



Étape

Pour afficher la licence, effectuez l'une des opérations suivantes :

- Dans le panneau Santé du tableau de bord, cliquez sur l'icône d'état de la licence ou sur le lien **Licence**. Ce lien apparaît uniquement en cas de problème avec la licence.
- Sélectionnez **Maintenance > système > Licence**.

La page Licence s'affiche et fournit les informations suivantes en lecture seule sur la licence actuelle :

- ID du système StorageGRID, qui est le numéro d'identification unique de cette installation StorageGRID
- Numéro de série de la licence
- Capacité de stockage sous licence de la grille
- Date de fin de la licence logicielle
- Date de fin du contrat de service de support
- Contenu du fichier texte de licence



Pour les licences émises avant StorageGRID 10.3, la capacité de stockage sous licence n'est pas incluse dans le fichier de licence et un message « Voir contrat de licence » s'affiche au lieu d'une valeur.

Mise à jour des informations de licence StorageGRID

Vous devez mettre à jour les informations de licence de votre système StorageGRID à tout moment que les conditions de votre modification de licence changent. Par exemple, vous devez mettre à jour les informations de licence si vous achetez de la capacité de stockage supplémentaire pour votre grid.

Ce dont vous avez besoin

- Vous devez disposer d'un nouveau fichier de licence pour appliquer votre système StorageGRID.
- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous devez disposer de la phrase secrète pour le provisionnement.

Étapes

1. Sélectionnez **Maintenance > système > Licence**.
2. Saisissez le mot de passe de provisionnement de votre système StorageGRID dans la zone de texte **phrase de passe de provisionnement**.
3. Cliquez sur **Parcourir**.
4. Dans la boîte de dialogue Ouvrir, localisez et sélectionnez le nouveau fichier de licence (.txt), puis cliquez sur **Ouvrir**.

Le nouveau fichier de licence est validé et affiché.

5. Cliquez sur **Enregistrer**.

Via l'API de gestion du grid

Vous pouvez effectuer des tâches de gestion du système à l'aide de l'API REST Grid Management plutôt que de l'interface utilisateur Grid Manager. Par exemple, vous pouvez utiliser l'API pour automatiser les opérations ou créer plusieurs entités plus rapidement (par exemple, les utilisateurs).

L'API Grid Management utilise la plateforme d'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.

Ressources générales

L'API de gestion du grid fournit les ressources de premier niveau 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, reportez-vous aux informations sur l'utilisation des comptes de tenant.
- `/private`: L'accès est limité aux utilisateurs de Grid Manager et est basé sur les autorisations de groupe configurées. Ces API sont destinées à un usage interne uniquement et ne sont pas documentées publiquement. Ces API sont également susceptibles d'être modifiées sans préavis.

Informations associées

["Utilisez un compte de locataire"](#)

["Prometheus : notions de base sur les requêtes"](#)

Opérations de l'API de gestion du grid

L'API Grid Management organise les opérations d'API disponibles dans les sections suivantes.

- **Comptes** — opérations pour gérer les comptes de tenant du stockage, y compris la création de nouveaux comptes et la récupération de l'utilisation du stockage pour un compte donné.
- **Alarmes** — opérations pour répertorier les alarmes en cours (système hérité) et renvoyer des informations sur l'intégrité de la grille, y compris les alertes en cours et un résumé des États de connexion du nœud.
- **Alerte-historique** — opérations sur les alertes résolues.
- **Alertes-récepteurs** — opérations sur les récepteurs de notification d'alerte (e-mail).
- **Règles d'alerte** — opérations sur les règles d'alerte.
- **Seuils d'alerte** — opérations sur les silences d'alerte.
- **Alertes** — opérations sur les alertes.
- **Audit** — opérations pour répertorier et mettre à jour la configuration d'audit.
- **Auth** — opérations pour effectuer l'authentification de session utilisateur.

L'API Grid Management prend en charge le schéma d'authentification par jeton Bearer. 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, un jeton de sécurité est renvoyé. Ce token doit être fourni dans l'en-tête des requêtes API suivantes (« autorisation : porteur *token* »).



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

Voir « protection contre la contrefaçon de demandes intersites » pour des informations sur l'amélioration de la sécurité de l'authentification.

- **Certificats-client** — opérations pour configurer les certificats client 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 de gestion de grille. Vous pouvez répertorier la version du produit et les principales versions de l'API Grid Management prises en charge par cette version, et désactiver les versions obsolètes de l'API.
- **DESACTIVE-fonctions** — opérations pour afficher les fonctions qui pourraient avoir été désactivées.
- **dns-serveurs** — opérations pour répertorier et modifier les serveurs DNS externes configurés.
- **Endpoint-domain-names** — opérations pour lister et modifier les noms de domaine de nœud final.
- **Code d'effacement** — opérations sur les profils de code d'effacement.
- **Expansion** — opérations sur l'expansion (niveau procédure).
- **Nœuds d'extension** — opérations sur l'extension (au niveau du nœud).

- **Sites d'expansion** — opérations sur l'expansion (au niveau du site).
- **Grid-réseaux** — opérations pour lister et modifier la liste des réseaux de grille.
- **GRID-mots de passe** — opérations pour la gestion des mots de passe de grille.
- **Groupes** — opérations pour gérer les groupes d'administrateurs Grid locaux et pour extraire des groupes d'administrateurs Grid fédérés à partir d'un serveur LDAP externe.
- **Identity-source** — opérations pour configurer un référentiel d'identité externe et synchroniser manuellement les informations de groupe et d'utilisateur fédérés.
- **ilm** — opérations sur la gestion du cycle de vie de l'information (ILM).
- **Licence** — opérations pour récupérer et mettre à jour la licence StorageGRID.
- **Logs** — opérations de collecte et de téléchargement de fichiers journaux.
- **Métriques** — opérations sur les métriques StorageGRID incluant des requêtes métriques instantanées à un point unique dans les requêtes métriques de temps et de plage sur une plage de temps. L'API de gestion du grid utilise l'outil de contrôle des systèmes Prometheus comme source de données back-end. Pour plus d'informations sur la création de requêtes Prometheus, consultez le site Web Prometheus.



Indicateurs qui incluent *private* dans leur nom sont destinés à un usage interne uniquement. Ces metrics sont susceptibles d'être modifiés sans préavis entre les versions d'StorageGRID.

- **Node-Health** — opérations sur l'état de santé du noeud.
- **ntp-Server** — opérations pour répertorier ou mettre à jour les serveurs NTP (Network Time Protocol) externes.
- **Objets** — opérations sur les objets et les métadonnées d'objet.
- **Récupération** — opérations pour la procédure de récupération.
- **Progiciel de récupération** — opérations pour télécharger le progiciel de récupération.
- **Régions** — opérations pour afficher et créer des régions.
- **s3-Object-lock** — opérations sur les paramètres globaux de verrouillage d'objet S3.
- **Server-Certificate** — opérations pour afficher et mettre à jour les certificats de serveur Grid Manager.
- **snmp** — opérations sur la configuration SNMP actuelle.
- **Classes de trafic** — opérations pour les politiques de classification du trafic.
- **Réseau-client-non fiable** — opérations sur la configuration réseau client non fiable.
- **Utilisateurs** — opérations pour afficher et gérer les utilisateurs de Grid Manager.

Émission de requêtes API

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

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.



Toutes les opérations d'API que vous effectuez à l'aide de la page Web API Docs 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. Sélectionnez **aide > Documentation API** dans l'en-tête de Grid Manager.
2. Sélectionnez l'opération souhaitée.

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

3. Sélectionnez une action HTTP pour afficher les détails de la demande, notamment l'URL du noeud final, la liste de tous les paramètres obligatoires ou facultatifs, un exemple de l'organisme de demande (si nécessaire) et les réponses possibles.

GET
/grid/groups
Lists Grid Administrator Groups

Parameters
Try it out

Name	Description
type string (query)	filter by group type Available values : local, federated <div> -- </div>
limit integer (query)	maximum number of results Default value : 25 <div> 25 </div>
marker string (query)	marker-style pagination offset (value is Group's URN) <div> marker - marker-style pagination offset (value </div>
includeMarker boolean (query)	if set, the marker element is also returned <div> -- </div>
order string (query)	pagination order (desc requires marker) Available values : asc, desc <div> -- </div>

Responses
Response content type application/json

Code	Description
200	successfully retrieved Example Value Model <pre> { "responseTime": "2021-03-29T14:22:19.673Z", "status": "success", "apiVersion": "3.3", "deprecated": false, "data": [{ "displayName": "Developers", </pre>

- Déterminez si la demande nécessite des paramètres supplémentaires, tels qu'un ID de groupe ou d'utilisateur. Ensuite, obtenir ces valeurs. Vous devrez peut-être d'abord lancer une autre demande d'API pour obtenir les informations dont vous avez besoin.
- Déterminez si vous devez modifier l'exemple de corps de la demande. Si c'est le cas, vous pouvez cliquer sur **modèle** pour connaître les exigences de chaque champ.
- Cliquez sur **essayez-le**.
- Fournir tous les paramètres requis ou modifier le corps de la demande selon les besoins.
- Cliquez sur **Exécuter**.
- Vérifiez le code de réponse pour déterminer si la demande a réussi.

Gestion des versions de l'API de gestion du grid

L'API de gestion du grid utilise la gestion des versions pour prendre en charge les mises à niveau sans interruption.

Par exemple, cette URL de demande spécifie la version 3 de l'API.

`https://hostname_or_ip_address/api/v3/authorize`

La version majeure de l'API de gestion des locataires est incrémentée lorsque des modifications sont effectuées, qui sont **non compatibles** avec des versions antérieures. La version mineure de l'API de gestion des locataires est incrémentée lorsque des modifications sont effectuées que **sont compatibles** avec des versions antérieures. Les modifications compatibles incluent l'ajout de nouveaux noeuds finaux 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 plus anciennes	2.1	2.2
Non compatible avec les versions plus anciennes	2.1	3.0

Lors de la première installation du logiciel StorageGRID, seule la version la plus récente de l'API de gestion de grille est activée. Cependant, lorsque vous effectuez une mise à niveau vers une nouvelle version de StorageGRID, vous continuez à accéder à l'ancienne version de l'API pour au moins une version de StorageGRID.



Vous pouvez utiliser l'API Grid Management pour configurer les versions prises en charge. Pour plus d'informations, reportez-vous à la section « config » de la documentation de l'API swagger. Vous devez désactiver la prise en charge de l'ancienne version après avoir mis à jour tous les clients de l'API Grid Management pour utiliser la version la plus récente.

Les requêtes obsolètes sont marquées comme obsolètes de l'une 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 v1 API at POST "/api/v1/authorize"
```

Détermination des versions d'API prises en charge dans la version actuelle

Utilisez la requête d'API suivante pour renvoyer une liste des versions principales de l'API prises en charge :

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

Spécification d'une version d'API pour une requête

Vous pouvez spécifier la version de l'API à l'aide d'un paramètre de chemin d'accès (/api/v3) ou un en-tête (Api-Version: 3). Si vous indiquez les deux valeurs, la valeur de l'en-tête remplace la valeur du chemin d'accès.

```
curl https://[IP-Address]/api/v3/grid/accounts

curl -H "Api-Version: 3" https://[IP-Address]/api/grid/accounts
```

Protection contre la contrefaçon de demandes intersites (CSRF)

Vous pouvez vous protéger contre les attaques de contrefaçon de requêtes intersites (CSRF) contre StorageGRID en utilisant des jetons CSRF pour améliorer l'authentification qui utilise des cookies. Grid Manager et tenant Manager activent automatiquement cette fonction de sécurité ; les autres clients API peuvent choisir de l'activer lorsqu'ils se connectent.

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

StorageGRID contribue à la protection contre les attaques CSRF en utilisant des jetons CSRF. Lorsque cette option 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 fonction, définissez l' `csrfToken` paramètre à `true` pendant 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"
```

Si vrai, un `GridCsrfToken` Le cookie est défini avec une valeur aléatoire pour les connexions dans Grid Manager et dans `AccountCsrfToken` Le cookie est défini avec une valeur aléatoire pour les connexions au Gestionnaire de locataires.

Si le cookie est présent, toutes les demandes pouvant modifier l'état du système (POST, PUT, PATCH, DELETE) doivent inclure l'une des options suivantes :

- Le `X-Csrf-Token` En-tête, avec la valeur de l'en-tête définie sur la valeur du cookie de jeton CSRF.
- Pour les noeuds finaux qui acceptent un corps codé par formulaire : a `csrfToken` paramètre corps de demande codé par formulaire.

Reportez-vous à la documentation en ligne de l'API pour obtenir des exemples et des détails supplémentaires.



Les demandes disposant d'un jeu de cookies de jeton CSRF appliquent également le `"Content-Type: application/json"` En-tête pour toute demande qui attend un corps de requête JSON comme une protection supplémentaire contre les attaques CSRF.

Utilisation de l'API si l'authentification unique est activée

Si l'authentification unique (SSO) a été activée pour votre système StorageGRID, vous ne pouvez pas utiliser les requêtes standard de l'API d'authentification pour vous connecter à l'API de gestion du grid ou l'API de gestion des locataires et vous déconnecter.

Connexion à 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 obtenir un jeton d'authentification auprès d'AD FS valide pour l'API de gestion de grille ou l'API de gestion des locataires.

Ce dont vous avez besoin

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

Description de la 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 ou CentOS, `./debs` Pour Ubuntu ou Debian, et `./vsphere` Pour VMware).

- Un exemple de flux de travail des requêtes Curl.

Le flux de travail de boucle risque de s'échapper si vous l'effectuez trop lentement. L'erreur peut s'afficher : aucune confirmation de soumission valide n'a été trouvée dans cette réponse.



L'exemple de flux de travail Curl ne protège pas le mot de passe d'être vu par d'autres utilisateurs.

Si vous avez un problème de codage d'URL, l'erreur peut s'afficher : version SAML non prise en charge.

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.
 - Utiliser les demandes de gondoles. Passez à l'étape 3.
2. Si vous souhaitez utiliser le `storagegrid-ssoauth.py` Passez le script à l'interpréteur Python et exécutez le script.

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

- Le nom d'utilisateur SSO
- Domaine dans lequel StorageGRID est installé
- L'adresse de StorageGRID
- Pour accéder à l'API de gestion des locataires, entrez l'ID de compte de locataire.

```
python3 /tmp/storagegrid-ssoauth.py
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 maintenant utiliser le token pour d'autres requêtes, de la même manière que vous utilisiez l'API si SSO n'était pas utilisé.

3. Si vous souhaitez utiliser des requêtes Curl, suivez la procédure ci-dessous.
 - a. Déclarez les variables nécessaires pour 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='ads.example.com'
```



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

- b. Pour recevoir une URL d'authentification signée, lancez une demande POST à `/api/v3/authorize-saml`, Et supprimez le codage JSON supplémentaire de la réponse.

Cet exemple montre une demande 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 dans cet exemple inclut une URL signée codée par URL, mais n'inclut pas la couche supplémentaire de codage JSON.

```
{
  "apiVersion": "3.0",
  "data":
  "https://ads.example.com/ads/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...
sSl%2BfQ33cvfwA%3D&RelayState=12345",
  "responseTime": "2018-11-06T16:30:23.355Z",
  "status": "success"
}
```

- c. Enregistrez le SAMLRequest à partir de la réponse pour une utilisation dans les commandes suivantes.

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

- d. Obtenir une URL complète incluant l'ID de demande client d'AD FS.

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

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

La réponse inclut l'ID de demande client :

```
<form method="post" id="loginForm" autocomplete="off"
novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13)
Login.submitLoginRequest();" action="/adfs/ls/?
SAMLRequest=fZHRT0MwFIZfhh...UJikvo77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-ee02-0080000000de" >
```

- e. Enregistrez l'ID de la demande client à partir de la réponse.

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

- f. Envoyez vos informations d'identification à l'action de 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 multifactor (MFA) est activée pour votre système SSO, le post du formulaire 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=fZHRT0MwFIZfhh...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 de la réponse.

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

- h. Envoyez une demande 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 contiennent des informations sur la session AD FS pour une utilisation de déconnexion ultérieure et le corps de réponse contient SAMLResponse 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
XFxVWx3bk1lMnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LTNmMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjZjYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMj01OVpcMQ==;
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 dans le champ masqué :

```
export SAMLResponse='PHNhbWxwOlJlc3Bvb3N...1scDpSZXNwb25zZT4='
```

- j. À l'aide de la sauvegarde `SAMLResponse`, Faire un `StorageGRID/api/saml-response` Demande de génération d'un jeton d'authentification `StorageGRID`.

Pour RelayState, Utilisez l'ID du compte locataire ou 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 maintenant utiliser MYTOKEN Pour les autres demandes, comme le ferait l'utilisation de l'API si SSO n'était pas utilisé.

Déconnexion 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 de gestion Grid ou de l'API de gestion des locataires.

Description de la tâche

Si nécessaire, vous pouvez vous déconnecter de l'API StorageGRID simplement en vous connectant à partir 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 de porteur StorageGRID valide.

Étapes

1. Pour générer une demande de déconnexion signée, passez cookie "sso=true" Pour 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%3D",
  "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 redirection vers StorageGRID.

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

La réponse 302 est renvoyée. L'emplacement de redirection ne s'applique pas à la déconnexion 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 de support StorageGRID.

La suppression du jeton de support StorageGRID fonctionne de la même manière que sans SSO. Si cookie "sso=true" Non 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
```

A 204 No Content réponse indique que l'utilisateur est déconnecté.

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

Utilisation des certificats de sécurité StorageGRID

Les certificats de sécurité sont de petits fichiers de données utilisés pour créer des connexions sécurisées et fiables entre les composants StorageGRID et entre les composants StorageGRID et les systèmes externes.

StorageGRID utilise deux types de certificats de sécurité :

- **Les certificats de serveur** sont requis lorsque vous utilisez des connexions HTTPS. Les certificats de serveur permettent d'établir des connexions sécurisées entre les clients et les serveurs, d'authentifier l'identité d'un serveur pour ses clients et de fournir un chemin de communication sécurisé pour les données. Le serveur et le client ont chacun une copie du certificat.
- **Certificats client** authentifient une identité client ou utilisateur au serveur, fournissant une authentification plus sécurisée que les mots de passe seuls. Les certificats client ne cryptent pas les données.

Lorsqu'un client se connecte au serveur via HTTPS, le serveur répond avec le certificat du serveur, qui contient une clé publique. Le client vérifie ce certificat en comparant la signature du serveur à la signature figurant sur sa copie du certificat. Si les signatures correspondent, le client démarre une session avec le serveur en utilisant la même clé publique.

StorageGRID fonctionne comme serveur pour certaines connexions (par exemple, le point de terminaison de l'équilibreur de charge) ou comme client pour d'autres connexions (par exemple, le service de réplication CloudMirror).

Une autorité de certification externe peut émettre des certificats personnalisés qui sont entièrement conformes aux politiques de sécurité des informations de votre entreprise. StorageGRID inclut également une autorité de certification intégrée qui génère des certificats CA internes lors de l'installation du système. Ces certificats d'autorité de certification internes sont utilisés par défaut pour sécuriser le trafic StorageGRID interne. Bien que vous puissiez utiliser les certificats d'autorité de certification internes pour un environnement non productif, la meilleure pratique pour un environnement de production consiste à utiliser des certificats personnalisés signés par une autorité de certification externe. Les connexions non sécurisées sans certificat sont également prises en charge mais ne sont pas recommandées.

- Les certificats d'autorité de certification personnalisés ne suppriment pas les certificats internes ; cependant, les certificats personnalisés doivent être ceux spécifiés pour vérifier les connexions du serveur.
- Tous les certificats personnalisés doivent respecter les directives de renforcement du système pour les certificats de serveur.

"Durcissement du système"

- StorageGRID prend en charge le regroupement de certificats d'une autorité de certification dans un seul fichier (appelé bundle de certificats d'autorité de certification).



StorageGRID inclut également des certificats CA du système d'exploitation identiques sur toutes les grilles. Dans les environnements de production, assurez-vous de spécifier un certificat personnalisé signé par une autorité de certification externe à la place du certificat d'autorité de certification du système d'exploitation.

Les variantes du serveur et des types de certificats client sont mises en œuvre de plusieurs façons. Avant de configurer le système, tous les certificats nécessaires à votre configuration StorageGRID spécifique doivent être prêts.

Certificat	Type de certificat	Description	Emplacement de navigation	Détails
Certificat du client administrateur	Client	<p>Installé sur chaque client, permettant à StorageGRID d'authentifier l'accès client externe.</p> <ul style="list-style-type: none"> • Permet aux clients externes autorisés d'accéder à la base de données StorageGRID Prometheus. • Contrôle sécurisé de StorageGRID à l'aide d'outils externes. 	Configuration > contrôle d'accès > certificats client	"Configuration des certificats client administrateur"
Certificat de fédération des identités	Serveur	Authentifie la connexion entre StorageGRID et un Active Directory externe, OpenLDAP ou Oracle Directory Server.utilisé pour la fédération des identités, ce qui permet aux groupes d'administration et aux utilisateurs d'être gérés par un système externe.	Configuration > contrôle d'accès > Fédération d'identité	"Utilisation de la fédération des identités"
Certificat SSO (Single Sign-on)	Serveur	Authentifie la connexion entre Active Directory Federation Services (AD FS) et StorageGRID utilisée pour les demandes SSO (Single Sign-on).	Configuration > contrôle d'accès > connexion unique	"Configuration de l'authentification unique"

Certificat	Type de certificat	Description	Emplacement de navigation	Détails
Certificat de serveur de gestion des clés (KMS)	Serveur et client	Authentifie la connexion entre StorageGRID et un serveur de gestion des clés (KMS) externe qui fournit les clés de chiffrement aux nœuds d'appliance StorageGRID.	Configuration > Paramètres système > serveur de gestion des clés	"Ajout d'un serveur de gestion des clés (KMS)"
Certificat de notification d'alerte par e-mail	Serveur et client	<p>Authentifie la connexion entre un serveur de messagerie SMTP et StorageGRID utilisé pour les notifications d'alerte.</p> <ul style="list-style-type: none"> • Si les communications avec le serveur SMTP nécessitent TLS (transport Layer Security), vous devez spécifier le certificat AC du serveur de messagerie. • Spécifiez un certificat client uniquement si le serveur de messagerie SMTP nécessite des certificats client pour l'authentification. 	Alertes > Configuration email	"Moniteur et amp ; dépannage"

Certificat	Type de certificat	Description	Emplacement de navigation	Détails
Certificat de terminal de l'équilibreur de charge	Serveur	<p>Authentifie la connexion entre les clients S3 ou Swift et le service StorageGRID Load Balancer sur les nœuds de passerelle ou les nœuds d'administration. Vous téléchargez ou générez un certificat d'équilibreur de charge lorsque vous configurez un nœud final d'équilibreur de charge.les applications client utilisent le certificat d'équilibreur de charge lors de la connexion à StorageGRID pour enregistrer et récupérer les données d'objet.</p> <p>Remarque : le certificat d'équilibreur de charge est le certificat le plus utilisé pendant le fonctionnement normal de StorageGRID.</p>	Configuration > Paramètres réseau > points d'extrémité Load Balancer	<ul style="list-style-type: none"> • "Configuration des terminaux d'équilibrage de charge" • Création d'un nœud final d'équilibrage de charge pour FabricPool <p>"Configuration de StorageGRID pour FabricPool"</p>

Certificat	Type de certificat	Description	Emplacement de navigation	Détails
Certificat de serveur de l'interface de gestion	Serveur	<p>Authentifie la connexion entre les navigateurs Web client et l'interface de gestion StorageGRID, permettant aux utilisateurs d'accéder à Grid Manager et au gestionnaire de locataires sans avertissement de sécurité.</p> <p>Ce certificat authentifie également les connexions de l'API de gestion du grid et de l'API de gestion des locataires.</p> <p>Vous pouvez utiliser le certificat de l'autorité de certification interne ou télécharger un certificat personnalisé.</p>	Configuration > Paramètres réseau > certificats serveur	<ul style="list-style-type: none"> • "Configuration des certificats de serveur" • "Configuration d'un certificat de serveur personnalisé pour le Grid Manager et le tenant Manager"
Certificat de terminal Cloud Storage Pool	Serveur	Authentifie la connexion entre le pool de stockage cloud StorageGRID et un emplacement de stockage externe (tel que le stockage Glacier S3 ou Microsoft Azure Blob). Un certificat différent est requis pour chaque type de fournisseur cloud.	ILM > pools de stockage	"Gestion des objets avec ILM"

Certificat	Type de certificat	Description	Emplacement de navigation	Détails
Certificat de terminal des services de plate-forme	Serveur	Authentification de la connexion depuis le service de la plateforme StorageGRID vers une ressource de stockage S3	Tenant Manager > STORAGE (S3) > Platform services Endpoints	"Utilisez un compte de locataire"
Certificat de serveur de point final de service d'API de stockage d'objet	Serveur	Authentifie les connexions client S3 ou Swift sécurisées vers le service LDR (local distribution Router) sur un nœud de stockage ou vers le service CLB (Connection Load Balancer) obsolète sur un nœud de passerelle.	Configuration > Paramètres réseau > points d'extrémité Load Balancer	"Configuration d'un certificat de serveur personnalisé pour les connexions au nœud de stockage ou au service CLB"

Exemple 1 : service Load Balancer

Dans cet exemple, StorageGRID sert de serveur.

1. Vous configurez un nœud final de l'équilibreur de charge et téléchargez ou générez un certificat de serveur dans StorageGRID.
2. Vous configurez une connexion client S3 ou Swift au point de terminaison de l'équilibreur de charge et téléchargez le même certificat au client.
3. Lorsque le client souhaite enregistrer ou récupérer des données, il se connecte au point de terminaison de l'équilibreur de charge à l'aide de HTTPS.
4. StorageGRID répond avec le certificat du serveur, qui contient une clé publique, et une signature basée sur la clé privée.
5. Le client vérifie ce certificat en comparant la signature du serveur à la signature figurant sur sa copie du certificat. Si les signatures correspondent, le client lance une session à l'aide de la même clé publique.
6. Le client envoie des données d'objet à StorageGRID.

Exemple 2 : serveur de gestion externe des clés (KMS)

Dans cet exemple, StorageGRID agit comme client.

1. À l'aide du logiciel serveur de gestion de clés externe, vous configurez StorageGRID en tant que client KMS et obtenez un certificat de serveur signé par l'autorité de certification, un certificat de client public et la clé privée pour le certificat client.
2. À l'aide de Grid Manager, vous configurez un serveur KMS et téléchargez les certificats du serveur et du client ainsi que la clé privée du client.

3. Lorsqu'un nœud StorageGRID a besoin d'une clé de chiffrement, il envoie une requête au serveur KMS qui inclut les données du certificat et une signature basée sur la clé privée.
4. Le serveur KMS valide la signature du certificat et décide qu'il peut faire confiance à StorageGRID.
5. Le serveur KMS répond à l'aide de la connexion validée.

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.