



Contrôle de l'accès administrateur à StorageGRID

StorageGRID 11.5

NetApp
April 11, 2024

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

Sommaire

- Contrôle de l'accès administrateur à StorageGRID 1
 - Contrôle de l'accès par pare-feu 1
 - Utilisation de la fédération des identités 2
 - Gestion des groupes d'administration 8
 - Gestion des utilisateurs locaux 17
 - Utilisation de l'authentification unique (SSO) pour StorageGRID 19
 - Configuration des certificats client administrateur 38

Contrôle de l'accès administrateur à StorageGRID

Vous pouvez contrôler l'accès des administrateurs au système StorageGRID en ouvrant ou en fermant des ports de pare-feu, en gérant les groupes et les utilisateurs d'administration, en configurant l'authentification unique (SSO) et en fournissant des certificats client pour autoriser un accès externe sécurisé aux mesures StorageGRID.

- ["Contrôle de l'accès par pare-feu"](#)
- ["Utilisation de la fédération des identités"](#)
- ["Gestion des groupes d'administration"](#)
- ["Gestion des utilisateurs locaux"](#)
- ["Utilisation de l'authentification unique \(SSO\) pour StorageGRID"](#)
- ["Configuration des certificats client administrateur"](#)

Contrôle de l'accès par pare-feu

Lorsque vous souhaitez contrôler l'accès par le biais de pare-feu, vous ouvrez ou fermez des ports spécifiques au niveau du pare-feu externe.

Contrôle de l'accès au pare-feu externe

Vous pouvez contrôler l'accès aux interfaces utilisateur et aux API des nœuds d'administration StorageGRID en ouvrant ou en fermant des ports spécifiques au pare-feu externe. Par exemple, vous pouvez empêcher les locataires de se connecter à Grid Manager au niveau du pare-feu, en plus d'utiliser d'autres méthodes pour contrôler l'accès au système.

Port	Description	Si le port est ouvert...
443	Port HTTPS par défaut pour les nœuds d'administration	<p>Les navigateurs Web et les clients d'API de gestion peuvent accéder à Grid Manager, à l'API de gestion du grid, au gestionnaire des locataires et à l'API de gestion des locataires.</p> <p>Remarque : le port 443 est également utilisé pour un trafic interne.</p>
8443	Port restreint de Grid Manager sur les nœuds d'administration	<ul style="list-style-type: none">• Les navigateurs Web et les clients d'API de gestion peuvent accéder à Grid Manager et à l'API de gestion Grid via HTTPS.• Les navigateurs Web et les clients de l'API de gestion ne peuvent pas accéder au Gestionnaire de locataires ou à l'API de gestion des locataires.• Les demandes de contenu interne seront rejetées.

Port	Description	Si le port est ouvert...
9443	Port de gestionnaire de locataires restreint sur les nœuds d'administration	<ul style="list-style-type: none"> • Les navigateurs Web et les clients d'API de gestion peuvent accéder au Gestionnaire de locataires et à l'API de gestion des locataires via HTTPS. • Les navigateurs Web et les clients de l'API de gestion ne peuvent pas accéder à Grid Manager ou à l'API de gestion Grid. • Les demandes de contenu interne seront rejetées.



L'authentification unique (SSO) n'est pas disponible sur les ports du gestionnaire de grille restreinte ou du gestionnaire de locataires. Vous devez utiliser le port HTTPS par défaut (443) si vous souhaitez que les utilisateurs s'authentifient avec une connexion unique.

Informations associées

["Connexion au Grid Manager"](#)

["Création d'un compte de locataire si StorageGRID n'utilise pas SSO"](#)

["Résumé : adresses IP et ports pour les connexions client"](#)

["Gestion des réseaux clients non fiables"](#)

["Installez Ubuntu ou Debian"](#)

["Installez VMware"](#)

["Installez Red Hat Enterprise Linux ou CentOS"](#)

Utilisation de la fédération des identités

L'utilisation de la fédération des identités accélère la configuration des groupes et des utilisateurs et permet aux utilisateurs de se connecter à StorageGRID à l'aide des informations d'identification familières.

Configuration de la fédération des identités

Vous pouvez configurer la fédération des identités si vous souhaitez que les groupes et utilisateurs d'administration soient gérés dans un autre système, tel qu'Active Directory, OpenLDAP ou Oracle Directory Server.

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.
- Si vous prévoyez d'activer l'authentification unique (SSO), vous devez utiliser Active Directory comme source d'identité fédérée et AD FS comme fournisseur d'identité. Voir « exigences relatives à l'utilisation d'un seul signe ».

- Vous devez utiliser Active Directory, OpenLDAP ou Oracle Directory Server comme fournisseur d'identité.



Si vous souhaitez utiliser un service LDAP v3 non répertorié, contactez le support technique.

- Si vous prévoyez d'utiliser TLS (transport Layer Security) pour les communications avec le serveur LDAP, le fournisseur d'identité doit utiliser TLS 1.2 ou 1.3.

Description de la tâche

Vous devez configurer un référentiel d'identité pour le Grid Manager si vous souhaitez importer les types de groupes fédérés suivants :

- Groupes d'administration. Les utilisateurs des groupes admin peuvent se connecter au gestionnaire de grille et effectuer des tâches en fonction des autorisations de gestion attribuées au groupe.
- Groupes d'utilisateurs locataires pour les locataires qui n'utilisent pas leur propre référentiel d'identité. Les utilisateurs des groupes de locataires peuvent se connecter au Gestionnaire de locataires et effectuer des tâches en fonction des autorisations attribuées au groupe dans le Gestionnaire de locataires.

Étapes

1. Sélectionnez **Configuration > contrôle d'accès > fédération d'identités**.
2. Sélectionnez **Activer la fédération d'identités**.

Les champs de configuration du serveur LDAP s'affichent.

3. Dans la section Type de service LDAP, sélectionnez le type de service LDAP que vous souhaitez configurer.

Vous pouvez sélectionner **Active Directory**, **OpenLDAP** ou **autre**.



Si vous sélectionnez **OpenLDAP**, vous devez configurer le serveur OpenLDAP. Reportez-vous aux instructions de configuration d'un serveur OpenLDAP.



Sélectionnez **autre** pour configurer les valeurs d'un serveur LDAP qui utilise Oracle Directory Server.

4. Si vous avez sélectionné **autre**, renseignez les champs de la section attributs LDAP.
 - **Nom unique utilisateur** : nom de l'attribut qui contient l'identifiant unique d'un utilisateur LDAP. Cet attribut est équivalent à `sAMAccountName` Pour Active Directory et `uid` Pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `uid`.
 - **UUID d'utilisateur** : nom de l'attribut qui contient l'identifiant unique permanent d'un utilisateur LDAP. Cet attribut est équivalent à `objectGUID` Pour Active Directory et `entryUUID` Pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `nsuniqueid`. La valeur de chaque utilisateur pour l'attribut spécifié doit être un nombre hexadécimal à 32 chiffres au format 16 octets ou chaîne, où les tirets sont ignorés.
 - **Nom unique de groupe** : nom de l'attribut qui contient l'identifiant unique d'un groupe LDAP. Cet attribut est équivalent à `sAMAccountName` Pour Active Directory et `cn` Pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `cn`.
 - **UUID de groupe** : nom de l'attribut qui contient l'identificateur unique permanent d'un groupe LDAP. Cet attribut est équivalent à `objectGUID` Pour Active Directory et `entryUUID` Pour OpenLDAP. Si

vous configurez Oracle Directory Server, entrez `nsuniqueid`. La valeur de chaque groupe pour l'attribut spécifié doit être un nombre hexadécimal à 32 chiffres au format 16 octets ou chaîne, où les tirets sont ignorés.

5. Dans la section configurer le serveur LDAP, entrez les informations de serveur LDAP et de connexion réseau requises.

- **Nom d'hôte** : le nom d'hôte du serveur ou l'adresse IP du serveur LDAP.
- **Port** : port utilisé pour se connecter au serveur LDAP.



Le port par défaut de STARTTLS est 389 et le port par défaut de LDAPS est 636. Cependant, vous pouvez utiliser n'importe quel port tant que votre pare-feu est configuré correctement.

- **Nom d'utilisateur** : chemin complet du nom distinctif (DN) de l'utilisateur qui se connectera au serveur LDAP.



Pour Active Directory, vous pouvez également spécifier le nom de connexion bas niveau ou le nom principal d'utilisateur.

L'utilisateur spécifié doit être autorisé à répertorier les groupes et les utilisateurs et à accéder aux attributs suivants :

- `sAMAccountName` ou `uid`
- `objectGUID`, `entryUUID`, ou `nsuniqueid`
- `cn`
- `memberOf` ou `isMemberOf`

- **Mot de passe** : mot de passe associé au nom d'utilisateur.
- **DN de base de groupe** : chemin complet du nom distinctif (DN) pour une sous-arborescence LDAP que vous voulez rechercher des groupes. Dans l'exemple Active Directory (ci-dessous), tous les groupes dont le nom unique est relatif au DN de base (`DC=storagegrid,DC=exemple,DC=com`) peuvent être utilisés comme groupes fédérés.



Les valeurs **Nom unique de groupe** doivent être uniques dans le **DN de base de groupe** auquel elles appartiennent.

- **DN de base d'utilisateur** : le chemin complet du nom distinctif (DN) d'une sous-arborescence LDAP que vous voulez rechercher des utilisateurs.



Les valeurs **Nom unique utilisateur** doivent être uniques dans le **DN de base utilisateur** auquel elles appartiennent.

6. Dans la section **transport Layer Security (TLS)**, sélectionnez un paramètre de sécurité.

- **Utilisez STARTTLS (recommandé)** : utilisez STARTTLS pour sécuriser les communications avec le serveur LDAP. Il s'agit de l'option recommandée.
- **Utilisez LDAPS** : l'option LDAPS (LDAP sur SSL) utilise TLS pour établir une connexion au serveur LDAP. Cette option est prise en charge pour des raisons de compatibilité.
- **N'utilisez pas TLS** : le trafic réseau entre le système StorageGRID et le serveur LDAP ne sera pas sécurisé.



L'utilisation de l'option **ne pas utiliser TLS** n'est pas prise en charge si votre serveur Active Directory applique la signature LDAP. Vous devez utiliser STARTTLS ou LDAPS.

7. Si vous avez sélectionné STARTTLS ou LDAPS, choisissez le certificat utilisé pour sécuriser la connexion.

- **Utilisez le certificat CA du système d'exploitation** : utilisez le certificat CA par défaut installé sur le système d'exploitation pour sécuriser les connexions.
- **Utilisez un certificat d'autorité de certification personnalisé** : utilisez un certificat de sécurité personnalisé.

Si vous sélectionnez ce paramètre, copiez et collez le certificat de sécurité personnalisé dans la zone de texte certificat de l'autorité de certification.

8. Vous pouvez également sélectionner **Tester la connexion** pour valider vos paramètres de connexion pour le serveur LDAP.

Un message de confirmation s'affiche dans le coin supérieur droit de la page si la connexion est valide.

9. Si la connexion est valide, sélectionnez **Enregistrer**.

La capture d'écran suivante montre des exemples de valeurs de configuration pour un serveur LDAP qui utilise Active Directory.

LDAP service type

Select the type of LDAP service you want to configure.

Active Directory

OpenLDAP

Other

Configure LDAP server (All fields are required)

Hostname

my-active-directory.example.com

Port

389

Username

MyDomain\Administrator

Password

••••••••

Group Base DN

DC=storagegrid,DC=example,DC=com

User Base DN

DC=storagegrid,DC=example,DC=com

Informations associées

["Chiffrement pris en charge pour les connexions TLS sortantes"](#)

["Conditions requises pour l'utilisation de l'authentification unique"](#)

["Création d'un compte de locataire"](#)

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

Instructions de configuration d'un serveur OpenLDAP

Si vous souhaitez utiliser un serveur OpenLDAP pour la fédération des identités, vous devez configurer des paramètres spécifiques sur le serveur OpenLDAP.

Recouvrements de memberOf et de raffint

Les recouvrements de membre et de raffinage doivent être activés. Pour plus d'informations, reportez-vous aux instructions relatives à la maintenance de l'adhésion inverse au groupe dans le Guide de l'administrateur pour OpenLDAP.

Indexation

Vous devez configurer les attributs OpenLDAP suivants avec les mots-clés d'index spécifiés :

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

De plus, assurez-vous que les champs mentionnés dans l'aide pour le nom d'utilisateur sont indexés pour des performances optimales.

Reportez-vous aux informations sur la maintenance de l'adhésion au groupe inverse dans le Guide de l'administrateur pour OpenLDAP.

Informations associées

["Documentation OpenLDAP : version 2.4 - Guide de l'administrateur"](#)

Forcer la synchronisation avec le référentiel d'identité

Le système StorageGRID synchronise régulièrement les groupes fédérés et les utilisateurs à partir du référentiel d'identité. Vous pouvez forcer la synchronisation à démarrer si vous souhaitez activer ou restreindre les autorisations utilisateur le plus rapidement possible.

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.
- Le référentiel d'identité doit être activé.

Étapes

1. Sélectionnez **Configuration > contrôle d'accès > fédération d'identités**.

La page Fédération des identités s'affiche. Le bouton **Synchroniser** se trouve en bas de la page.

Synchronize

StorageGRID periodically synchronizes federated groups and users from the configured LDAP server. Clicking the button below will immediately start the synchronization process against the saved LDAP server.

Synchronize

2. Cliquez sur **Synchroniser**.

Un message de confirmation indique que la synchronisation a démarré correctement. Le processus de synchronisation peut prendre un certain temps en fonction de votre environnement.



L'alerte **échec de synchronisation de la fédération d'identités** est déclenchée en cas de problème de synchronisation des groupes fédérés et des utilisateurs à partir du référentiel d'identité.

Désactivation de la fédération des identités

Vous pouvez désactiver temporairement ou définitivement la fédération des identités pour les groupes et les utilisateurs. Lorsque la fédération des identités est désactivée, il n'y a aucune communication entre StorageGRID et le référentiel d'identité. Cependant, tous les paramètres que vous avez configurés sont conservés, ce qui vous permet de réactiver facilement la fédération d'identités à l'avenir.

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

Avant de désactiver la fédération des identités, vous devez prendre connaissance des points suivants :

- Les utilisateurs fédérés ne pourront pas se connecter.
- Les utilisateurs fédérés qui sont actuellement connectés conservent l'accès au système StorageGRID jusqu'à l'expiration de leur session, mais ils ne pourront pas se connecter après l'expiration de leur session.
- La synchronisation entre le système StorageGRID et le référentiel d'identité ne se produira pas et des alertes ou des alarmes ne seront pas émises pour les comptes qui n'ont pas été synchronisés.
- La case à cocher **Activer la fédération d'identités** est désactivée si l'authentification unique (SSO) est définie sur **Enabled** ou **Sandbox mode**. Le statut SSO sur la page connexion unique doit être **désactivé** avant de pouvoir désactiver la fédération d'identités.

Étapes

1. Sélectionnez **Configuration > contrôle d'accès > fédération d'identités**.
2. Décochez la case **Activer la fédération d'identités**.
3. Cliquez sur **Enregistrer**.

Informations associées

["Désactivation de la connexion unique"](#)

Gestion des groupes d'administration

Vous pouvez créer des groupes d'administration pour gérer les autorisations de sécurité d'un ou plusieurs utilisateurs administrateurs. Les utilisateurs doivent appartenir à un groupe pour pouvoir accéder au système StorageGRID.

Création de groupes d'administration

Les groupes Admin vous permettent de déterminer quels utilisateurs peuvent accéder aux fonctions et opérations du gestionnaire de grille et de l'API Grid Management.

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.
- Si vous envisagez d'importer un groupe fédéré, vous devez avoir configuré la fédération des identités et le groupe fédéré doit déjà exister dans le référentiel d'identité configuré.

Étapes

1. Sélectionnez **Configuration > contrôle d'accès > groupes d'administration**.

La page groupes d'administration s'affiche et répertorie tous les groupes d'administration existants.

Admin Groups

Add and manage local and federated user groups, allowing member users to sign in to the Grid Manager. Set group permissions to control access to specific pages and features.


<div> + Add Clone Edit Remove </div>				
	Name	ID	Group Type ?	Access Mode ?
<input checked="" type="radio"/>	Flintstone	264083d0-23b5-3046-9bd4-88b7097731ab	Federated	Read-write
<input type="radio"/>	Simpson	cc8ad11f-68d0-f84a-af29-e7a6fcdc63a2	Federated	Read-only
<input type="radio"/>	ILM (read-only group)	88446141-9599-4543-b183-9c227ce7767a	Local	Read-only
<input type="radio"/>	API Developers	974b2faa-f9a1-4cfc-b364-914cdba2905f	Local	Read-write
<input type="radio"/>	ILM Admins (read-write)	a528c0c2-2417-4559-86ed-f0d2e31da820	Local	Read-write
<input type="radio"/>	Maintenance Users	7e3400ec-de8c-45a7-8bb8-e1496b362a8d	Local	Read-write
<div> Group Type All Show 20 rows per page <div>◀ ▶</div> </div>				

2. Sélectionnez **Ajouter**.

La boîte de dialogue Ajouter un groupe s'affiche.


Add Group

Create a new local group or import a group from the external identity source.

Group Type  ☒ Local ☐ Federated

Display Name


Unique Name 

Access Mode  ☒ Read-write ☐ Read-only

Management Permissions


☐ Root Access 


☐ Acknowledge Alarms 

☐ Other Grid Configuration 

☐ Change Tenant Root Password 

☐ Metrics Query 

☐ Object Metadata Lookup 

☐ Manage Alerts 

☐ Grid Topology Page Configuration 

☐ Tenant Accounts 

☐ Maintenance 

☐ ILM 

☐ Storage Appliance Administrator 

Cancel

Save

3. Pour Type de groupe, sélectionnez **local** si vous souhaitez créer un groupe qui sera utilisé uniquement dans StorageGRID, ou sélectionnez **fédéré** si vous souhaitez importer un groupe à partir du référentiel d'identité.
4. Si vous avez sélectionné **local**, entrez un nom d'affichage pour le groupe. Le nom affiché est le nom qui apparaît dans le gestionnaire de grille. Par exemple, « Maintenance Users » ou « ILM Administrators ».
5. Entrez un nom unique pour le groupe.
 - **Local** : saisissez le nom unique de votre choix. Par exemple, « administrateurs ILM ».
 - **Fédéré** : saisissez le nom du groupe exactement tel qu'il apparaît dans le référentiel d'identité configuré.
6. Dans **Access mode**, sélectionnez si les utilisateurs du groupe peuvent modifier les paramètres et effectuer des opérations dans le gestionnaire de grille et l'API de gestion de grille ou s'ils ne peuvent afficher que les paramètres et les fonctionnalités.
 - **Lecture-écriture** (par défaut) : les utilisateurs peuvent modifier les paramètres et effectuer les opérations autorisées par leurs autorisations de gestion.
 - **Lecture seule** : les utilisateurs peuvent uniquement afficher les paramètres et les fonctionnalités. Ils ne peuvent pas apporter de modifications ni effectuer d'opérations dans Grid Manager ou Grid Management API. Les utilisateurs locaux en lecture seule peuvent modifier leurs propres mots de passe.



Si un utilisateur appartient à plusieurs groupes et qu'un groupe est défini sur **lecture seule**, l'utilisateur dispose d'un accès en lecture seule à tous les paramètres et fonctions sélectionnés.

7. Sélectionnez une ou plusieurs autorisations de gestion.

Vous devez attribuer au moins une autorisation à chaque groupe ; sinon, les utilisateurs appartenant au groupe ne pourront pas se connecter à StorageGRID.

8. Sélectionnez **Enregistrer**.

Le nouveau groupe est créé. S'il s'agit d'un groupe local, vous pouvez à présent ajouter un ou plusieurs utilisateurs. S'il s'agit d'un groupe fédéré, le référentiel d'identité gère quels utilisateurs appartiennent au groupe.

Informations associées

["Gestion des utilisateurs locaux"](#)

Autorisations de groupe d'administration

Lors de la création de groupes d'utilisateurs admin, vous sélectionnez une ou plusieurs autorisations pour contrôler l'accès à des fonctions spécifiques de Grid Manager. Vous pouvez ensuite affecter chaque utilisateur à un ou plusieurs de ces groupes d'administration pour déterminer les tâches que l'utilisateur peut effectuer.

Vous devez affecter au moins une autorisation à chaque groupe ; sinon, les utilisateurs appartenant à ce groupe ne pourront pas se connecter au gestionnaire de grille.

Par défaut, tout utilisateur appartenant à un groupe disposant d'au moins une autorisation peut effectuer les tâches suivantes :

- Connectez-vous au Grid Manager
- Afficher le tableau de bord
- Affichez les pages nœuds
- Surveiller la topologie de la grille
- Afficher les alertes actuelles et résolues
- Afficher les alarmes actuelles et historiques (système hérité)
- Modifier son propre mot de passe (utilisateurs locaux uniquement)
- Afficher certaines informations sur les pages Configuration et maintenance

Les sections suivantes décrivent les autorisations que vous pouvez attribuer lors de la création ou de la modification d'un groupe d'administration. Toute fonctionnalité qui n'est pas explicitement mentionnée requiert l'autorisation accès racine.

Accès racine

Cette autorisation donne accès à toutes les fonctions d'administration de la grille.

Gérer les alertes

Cette autorisation donne accès aux options de gestion des alertes. Les utilisateurs doivent disposer de cette

autorisation pour gérer les silences, les notifications d'alerte et les règles d'alerte.

Accuser réception d'alarmes (système hérité)

Cette autorisation permet d'accuser réception et de répondre aux alarmes (système hérité). Tous les utilisateurs connectés peuvent afficher les alarmes actuelles et historiques.

Si vous souhaitez qu'un utilisateur surveille la topologie de la grille et accuse réception des alarmes uniquement, vous devez attribuer cette autorisation.

Configuration de la page topologie de la grille

Cette autorisation permet d'accéder aux options de menu suivantes :

- Onglets de configuration disponibles dans les pages **support > Outils > topologie de grille**.
- **Réinitialiser le nombre d'événements** sur l'onglet **noeuds > Événements**.

Autre configuration de grille

Cette autorisation donne accès à d'autres options de configuration de grille.



Pour voir ces options supplémentaires, les utilisateurs doivent également disposer de l'autorisation Configuration de la page de topologie de la grille.

- **Alarmes** (système hérité) :
 - Alarmes globales
 - Configuration de l'ancien e-mail
- **ILM** :
 - Pools de stockage
 - Notes de stockage
- **Configuration > Paramètres réseau**
 - Coût des liens
- **Configuration > Paramètres système** :
 - Options d'affichage
 - Options de grid
 - Options de stockage
- **Configuration > surveillance** :
 - Événements
- **Support**:
 - AutoSupport

Comptes de locataires

Cette autorisation permet d'accéder à la page **locataires > tenant Accounts**.



La version 1 de l'API de gestion du grid (obsolète) utilise cette autorisation pour gérer les règles de groupe de locataires, réinitialiser les mots de passe d'administration Swift et gérer les clés d'accès S3 des utilisateurs root.

Modifier le mot de passe racine du locataire

Cette autorisation donne accès à l'option **changer mot de passe racine** de la page comptes de tenant, ce qui vous permet de contrôler qui peut modifier le mot de passe de l'utilisateur racine local du locataire. Les utilisateurs qui ne disposent pas de cette autorisation ne peuvent pas voir l'option **Modifier le mot de passe racine**.



Vous devez attribuer l'autorisation comptes de tenant au groupe avant de pouvoir attribuer cette autorisation.

Maintenance

Cette autorisation permet d'accéder aux options de menu suivantes :

- **Configuration > Paramètres système :**
 - Noms de domaine*
 - Certificats de serveur*
- **Configuration > surveillance :**
 - Vérification*
- **Configuration > contrôle d'accès :**
 - Mots de passe de grille
- **Maintenance > tâches de maintenance**
 - Désaffectation
 - De développement
 - Reprise après incident
- **Maintenance > réseau :**
 - Serveurs DNS*
 - Réseau de grille*
 - Serveurs NTP*
- **Maintenance > système :**
 - Licence*
 - Package de restauration
 - Mise à jour logicielle
- **Support > Outils :**
 - Journaux
- Les utilisateurs qui ne disposent pas de l'autorisation Maintenance peuvent afficher, mais pas modifier, les pages marquées d'un astérisque.

Requête de metrics

Cette autorisation permet d'accéder à la page **support > Outils > métriques**. Cette autorisation permet également d'accéder à des requêtes de metrics Prometheus personnalisées à l'aide de la section **Metrics** de l'API Grid Management.

ILM

Cette autorisation permet d'accéder aux options de menu **ILM** suivantes :

- **Codage d'effacement**
- **Règles**
- **Politiques**
- * Régions*



L'accès aux options de menu **ILM > Storage pools** et **ILM > Storage Grapes** est contrôlé par les autres autorisations de configuration de la page de configuration de la grille et de la topologie de la grille.

Recherche des métadonnées d'objet

Cette autorisation permet d'accéder à l'option de menu **ILM > Object Metadata Lookup**.

Administrateur de l'appliance de stockage

Cette autorisation permet d'accéder à la gamme E-Series SANtricity System Manager sur les appliances de stockage via Grid Manager.

Interaction entre les autorisations et le mode d'accès

Pour toutes les autorisations, le paramètre mode d'accès du groupe détermine si les utilisateurs peuvent modifier les paramètres et effectuer des opérations ou s'ils ne peuvent afficher que les paramètres et les fonctions associés. Si un utilisateur appartient à plusieurs groupes et qu'un groupe est défini sur **lecture seule**, l'utilisateur dispose d'un accès en lecture seule à tous les paramètres et fonctions sélectionnés.

Désactivation des fonctions à partir de l'API Grid Management

Vous pouvez utiliser l'API de gestion de grille pour désactiver complètement certaines fonctions du système StorageGRID. Lorsqu'une fonction est désactivée, aucune autorisation ne peut être attribuée pour effectuer les tâches associées à cette fonctionnalité.

Description de la tâche

Le système de fonctions désactivées vous permet d'empêcher l'accès à certaines fonctions du système StorageGRID. La désactivation d'une fonctionnalité est le seul moyen d'empêcher l'utilisateur racine ou les utilisateurs appartenant à des groupes admin disposant de l'autorisation accès racine d'utiliser cette fonctionnalité.

Pour comprendre l'utilité de cette fonctionnalité, prenez en compte 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 de tenant. Pour protéger la sécurité des objets de leurs détenteurs de bail, la Société A veut s'assurer que ses employés ne peuvent jamais accéder à un compte de locataire après le déploiement du compte.

*Société A peut atteindre cet objectif en utilisant le système Désactiver les fonctions dans l'API de gestion de grille. En désactivant complètement la fonction **Modifier le mot de passe racine du locataire** dans le gestionnaire de grille (à la fois l'interface utilisateur et l'API), la société A peut s'assurer qu'aucun utilisateur Admin, y compris l'utilisateur racine et les utilisateurs appartenant à des groupes avec l'autorisation accès racine, ne peut modifier le mot de passe de l'utilisateur racine d'un compte locataire.*

Réactivation des fonctions désactivées

Par défaut, vous pouvez utiliser l'API Grid Management pour réactiver une fonction qui a été désactivée. Toutefois, si vous souhaitez empêcher la réactivation des fonctions désactivées, vous pouvez désactiver la fonction **activeFeatures** elle-même.



La fonction **activateFeatures** ne peut pas être réactivée. Si vous décidez de désactiver cette fonction, sachez que vous perdrez définitivement la capacité de réactiver les autres fonctions désactivées. Vous devez contacter le support technique pour restaurer toute fonctionnalité perdue.

Pour plus de détails, consultez les instructions d'implémentation des applications client S3 ou Swift.

Étapes

1. Accédez à la documentation de swagger pour l'API Grid Management.
2. Localisez le point d'extrémité Désactiver les fonctions.
3. Pour désactiver une fonction, telle que **changer le mot de passe racine du locataire**, envoyez un corps à l'API comme suit :

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

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

4. Pour réactiver toutes les fonctions, envoyez un corps à l'API comme suit :

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

Lorsque cette demande est terminée, toutes les fonctions, y compris la fonction Modifier le mot de passe racine du locataire, sont réactivées. L'autorisation de gestion du mot de passe racine de locataire s'affiche maintenant dans l'interface utilisateur et toute demande d'API qui tente de modifier le mot de passe racine d'un locataire va réussir, à condition que l'utilisateur dispose de l'autorisation de gestion accès racine ou de modification du mot de passe racine de locataire.



L'exemple précédent provoque la réactivation des fonctions **API DESACTIVE**. Si d'autres fonctions doivent rester désactivées, vous devez les spécifier explicitement dans la demande PUT. Par exemple, pour réactiver la fonction Modifier le mot de passe racine du locataire et continuer à désactiver la fonction accusé de réception d'alarme, envoyez cette demande PUT :

```
{ "grid": { "alarmAcknowledgment": true } }
```

Informations associées

["Via l'API de gestion du grid"](#)

Modification d'un groupe d'administration

Vous pouvez modifier un groupe d'administration pour modifier les autorisations associées au groupe. Pour les groupes d'administration locaux, vous pouvez également mettre à jour le nom d'affichage.

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.

Étapes

1. Sélectionnez **Configuration > contrôle d'accès > groupes d'administration**.
2. Sélectionnez le groupe.

Si votre système comprend plus de 20 éléments, vous pouvez spécifier le nombre de lignes affichées simultanément sur chaque page. Vous pouvez ensuite utiliser la fonction Recherche de votre navigateur pour rechercher un élément spécifique dans les lignes affichées.

3. Cliquez sur **Modifier**.
4. Éventuellement, pour les groupes locaux, entrez le nom du groupe qui apparaîtra aux utilisateurs, par exemple "utilisateurs de maintenance".

Vous ne pouvez pas modifier le nom unique, qui est le nom du groupe interne.

5. Vous pouvez également modifier le mode d'accès du groupe.
 - **Lecture-écriture** (par défaut) : les utilisateurs peuvent modifier les paramètres et effectuer les opérations autorisées par leurs autorisations de gestion.
 - **Lecture seule** : les utilisateurs peuvent uniquement afficher les paramètres et les fonctionnalités. Ils ne peuvent pas apporter de modifications ni effectuer d'opérations dans Grid Manager ou Grid Management API. Les utilisateurs locaux en lecture seule peuvent modifier leurs propres mots de passe.



Si un utilisateur appartient à plusieurs groupes et qu'un groupe est défini sur **lecture seule**, l'utilisateur dispose d'un accès en lecture seule à tous les paramètres et fonctions sélectionnés.

6. Vous pouvez éventuellement ajouter ou supprimer des autorisations de groupe.

Reportez-vous à la section informations sur les autorisations de groupe d'administration.

7. Sélectionnez **Enregistrer**.

Informations associées

[Autorisations de groupe d'administration](#)

Suppression d'un groupe d'administration

Vous pouvez supprimer un groupe d'administration lorsque vous souhaitez supprimer le groupe du système et supprimer toutes les autorisations associées au groupe. La suppression d'un groupe admin supprime tous les utilisateurs admin du groupe, mais ne supprime pas les utilisateurs admin.

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

Lorsque vous supprimez un groupe, les utilisateurs affectés à ce groupe perdront tous les privilèges d'accès au gestionnaire de grille, à moins qu'ils ne soient accordés par un autre groupe.

Étapes

1. Sélectionnez **Configuration > contrôle d'accès > groupes d'administration**.
2. Sélectionnez le nom du groupe.

Si votre système comprend plus de 20 éléments, vous pouvez spécifier le nombre de lignes affichées simultanément sur chaque page. Vous pouvez ensuite utiliser la fonction Recherche de votre navigateur pour rechercher un élément spécifique dans les lignes affichées.

3. Sélectionnez **Supprimer**.
4. Sélectionnez **OK**.

Gestion des utilisateurs locaux

Vous pouvez créer des utilisateurs locaux et les affecter à des groupes d'administration locaux pour déterminer les fonctions de Grid Manager auxquelles ces utilisateurs peuvent accéder.

Le gestionnaire de grille inclut un utilisateur local prédéfini, nommé « root ». Bien que vous puissiez ajouter et supprimer des utilisateurs locaux, vous ne pouvez pas supprimer l'utilisateur racine.



Si l'authentification unique (SSO) a été activée, les utilisateurs locaux ne peuvent pas se connecter à StorageGRID.

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

Création d'un utilisateur local

Si vous avez créé des groupes d'administration locaux, vous pouvez créer un ou plusieurs utilisateurs locaux et attribuer chaque utilisateur à un ou plusieurs groupes. Les autorisations du groupe contrôlent les fonctions de Grid Manager auxquelles l'utilisateur peut accéder.

Description de la tâche

Vous ne pouvez créer que des utilisateurs locaux, et vous pouvez uniquement attribuer ces utilisateurs à des groupes d'administration locaux. Les utilisateurs fédérés et les groupes fédérés sont gérés à l'aide du référentiel d'identité externe.

Étapes

1. Sélectionnez **Configuration > contrôle d'accès > utilisateurs Admin**.
2. Cliquez sur **Créer**.
3. Entrez le nom d'affichage, le nom unique et le mot de passe de l'utilisateur.
4. Attribuez l'utilisateur à un ou plusieurs groupes qui régissent les autorisations d'accès.

La liste des noms de groupes est générée à partir de la table Groups.

5. Cliquez sur **Enregistrer**.

Informations associées

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

Modification du compte d'un utilisateur local

Vous pouvez modifier le compte d'un administrateur local pour mettre à jour le nom d'affichage de l'utilisateur ou l'appartenance à un groupe. Vous pouvez également empêcher temporairement un utilisateur d'accéder au système.

Description de la tâche

Vous ne pouvez modifier que les utilisateurs locaux. Les détails de l'utilisateur fédéré sont automatiquement synchronisés avec le référentiel d'identité externe.

Étapes

1. Sélectionnez **Configuration > contrôle d'accès > utilisateurs Admin**.
2. Sélectionnez l'utilisateur que vous souhaitez modifier.

Si votre système comprend plus de 20 éléments, vous pouvez spécifier le nombre de lignes affichées simultanément sur chaque page. Vous pouvez ensuite utiliser la fonction Rechercher de votre navigateur pour rechercher un élément spécifique dans les lignes affichées.

3. Cliquez sur **Modifier**.
4. Vous pouvez éventuellement modifier le nom ou l'appartenance à un groupe.
5. Si vous le souhaitez, pour empêcher l'utilisateur d'accéder temporairement au système, cochez la case **refuser l'accès**.
6. Cliquez sur **Enregistrer**.

Les nouveaux paramètres sont appliqués à la prochaine ouverture de session de l'utilisateur, puis se reconnecte au Gestionnaire de grille.

Suppression du compte d'un utilisateur local

Vous pouvez supprimer des comptes pour les utilisateurs locaux qui n'ont plus besoin d'accéder à Grid Manager.

Étapes

1. Sélectionnez **Configuration > contrôle d'accès > utilisateurs Admin**.
2. Sélectionnez l'utilisateur local que vous souhaitez supprimer.



Vous ne pouvez pas supprimer l'utilisateur local racine prédéfini.

Si votre système comprend plus de 20 éléments, vous pouvez spécifier le nombre de lignes affichées simultanément sur chaque page. Vous pouvez ensuite utiliser la fonction Recherche de votre navigateur pour rechercher un élément spécifique dans les lignes affichées.

3. Cliquez sur **Supprimer**.

4. Cliquez sur **OK**.

Modification du mot de passe d'un utilisateur local

Les utilisateurs locaux peuvent modifier leurs propres mots de passe à l'aide de l'option **changer mot de passe** de la bannière du gestionnaire de grille. En outre, les utilisateurs qui ont accès à la page Admin Users peuvent modifier les mots de passe d'autres utilisateurs locaux.

Description de la tâche

Vous ne pouvez modifier les mots de passe que pour les utilisateurs locaux. Les utilisateurs fédérés doivent modifier leurs propres mots de passe dans le référentiel d'identité externe.

Étapes

1. Sélectionnez **Configuration > contrôle d'accès > utilisateurs Admin**.

2. Sur la page utilisateurs, sélectionnez l'utilisateur.

Si votre système comprend plus de 20 éléments, vous pouvez spécifier le nombre de lignes affichées simultanément sur chaque page. Vous pouvez ensuite utiliser la fonction Recherche de votre navigateur pour rechercher un élément spécifique dans les lignes affichées.

3. Cliquez sur **Modifier le mot de passe**.

4. Saisissez et confirmez le mot de passe, puis cliquez sur **Enregistrer**.

Utilisation de l'authentification unique (SSO) pour StorageGRID

Le système StorageGRID prend en charge la fonctionnalité SSO (Single Sign-on) en utilisant la 2.0 norme SAML 2.0 (Security assertion Markup Language). Lorsque l'authentification SSO est activée, tous les utilisateurs doivent être authentifiés par un fournisseur d'identités externe avant d'accéder au Grid Manager, au tenant Manager, à l'API Grid Management ou à l'API de gestion des locataires. Les utilisateurs locaux ne peuvent pas se connecter à StorageGRID.

- ["Fonctionnement de l'authentification unique"](#)
- ["Conditions requises pour l'utilisation de l'authentification unique"](#)
- ["Configuration de l'authentification unique"](#)

Fonctionnement de l'authentification unique

Avant d'activer l'authentification unique (SSO), vérifiez comment les processus de connexion et de déconnexion StorageGRID sont affectés lorsque l'authentification SSO

est activée.

Connexion lorsque SSO est activé

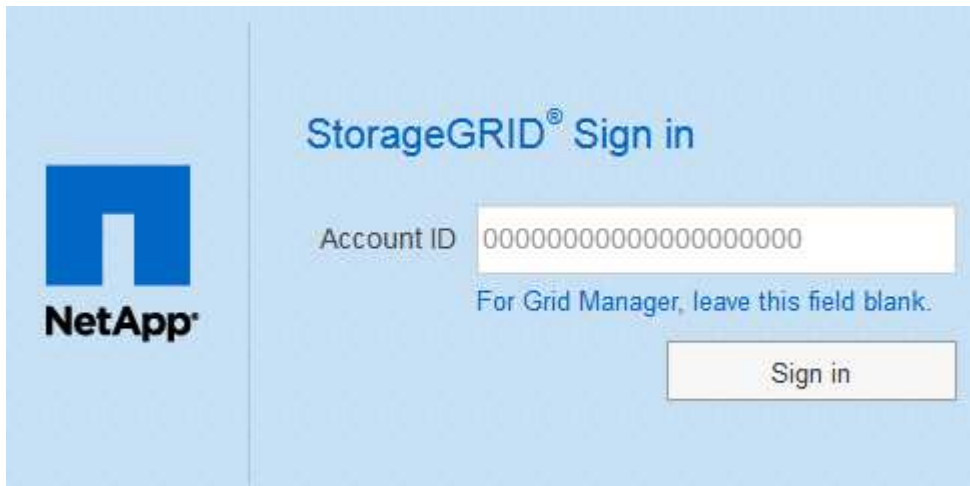
Lorsque l'authentification SSO est activée et que vous vous connectez à StorageGRID, vous êtes redirigé vers la page SSO de votre entreprise afin de valider vos identifiants.

Étapes

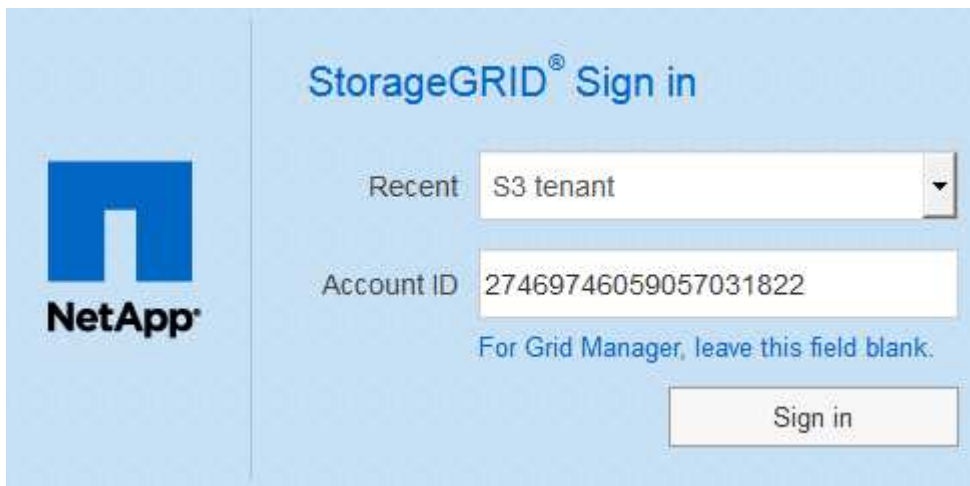
1. Entrez le nom de domaine complet ou l'adresse IP d'un nœud d'administration StorageGRID dans un navigateur Web.

La page de connexion StorageGRID s'affiche.

- S'il s'agit de la première fois que vous accédez à l'URL sur ce navigateur, vous êtes invité à entrer un ID de compte :

The image shows the StorageGRID Sign in page. On the left is the NetApp logo. The main heading is "StorageGRID® Sign in". Below this is a label "Account ID" followed by a text input field containing a long string of zeros. Below the input field is the text "For Grid Manager, leave this field blank." At the bottom right is a "Sign in" button.

- Si vous avez déjà accédé au Grid Manager ou au tenant Manager, vous êtes invité à sélectionner un compte récent ou à saisir un ID de compte :

The image shows the StorageGRID Sign in page for a returning user. On the left is the NetApp logo. The main heading is "StorageGRID® Sign in". Below this is a "Recent" label followed by a dropdown menu showing "S3 tenant". Below the dropdown is a label "Account ID" followed by a text input field containing the number "27469746059057031822". Below the input field is the text "For Grid Manager, leave this field blank." At the bottom right is a "Sign in" button.

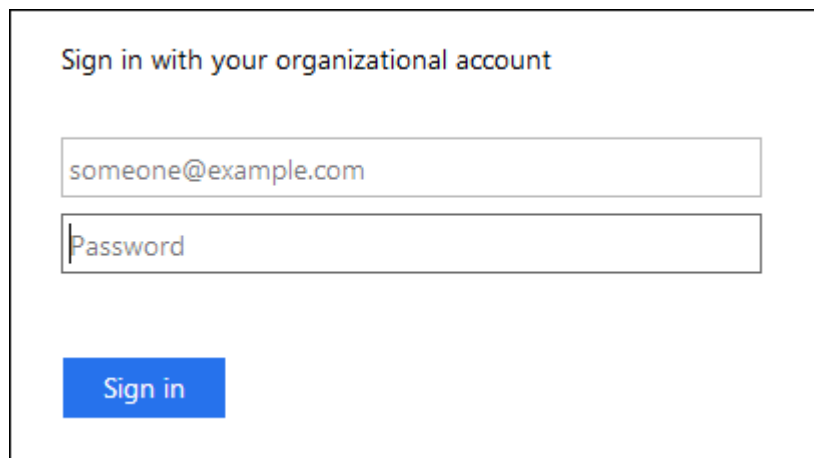
La page de connexion StorageGRID n'apparaît pas lorsque vous saisissez l'URL complète d'un compte de locataire (c'est-à-dire un nom de domaine complet ou une adresse IP suivi de `/?accountId=20-digit-account-id`). Au lieu de cela, vous êtes immédiatement redirigé vers la page de connexion SSO de votre entreprise, où vous pouvez [Connectez-vous à l'aide de vos identifiants SSO](#).

2. Indiquez si vous souhaitez accéder au Grid Manager ou au tenant Manager :

- Pour accéder au Grid Manager, laissez le champ Identifiant de compte** vide, saisissez **0** comme ID de compte ou sélectionnez **Grid Manager** si celui-ci apparaît dans la liste des comptes récents.
- Pour accéder au Gestionnaire de locataires, entrez l'ID de compte de tenant à 20 chiffres ou sélectionnez un locataire par nom s'il apparaît dans la liste des comptes récents.

3. Cliquez sur **connexion**

StorageGRID vous redirige vers la page de connexion SSO de votre entreprise. Par exemple :



Sign in with your organizational account

someone@example.com

Password

Sign in

4. Connectez-vous à l'aide de vos identifiants SSO.

Si vos informations d'identification SSO sont correctes :

- a. Le fournisseur d'identités fournit une réponse d'authentification à StorageGRID.
 - b. StorageGRID valide la réponse d'authentification.
 - c. Si la réponse est valide et que vous appartenez à un groupe fédéré disposant d'une autorisation d'accès adéquate, vous êtes connecté au Grid Manager ou au tenant Manager, selon le compte que vous avez sélectionné.
5. Accédez éventuellement à d'autres nœuds d'administration ou à Grid Manager ou au tenant Manager, si vous disposez des autorisations adéquates.

Il n'est pas nécessaire de saisir à nouveau vos identifiants SSO.

Déconnexion lorsque SSO est activé

Lorsque l'authentification SSO est activée pour StorageGRID, le processus de déconnexion dépend de ce que vous êtes connecté et de l'endroit où vous vous déconnectez.

Étapes

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

La page de connexion StorageGRID s'affiche. La liste déroulante **comptes récents** est mise à jour pour inclure **Grid Manager** ou le nom du locataire, afin que vous puissiez accéder plus rapidement à ces interfaces utilisateur à l'avenir.

Si vous êtes connecté à...	Et vous vous déconnectez de...	Vous êtes déconnecté de...
Grid Manager sur un ou plusieurs nœuds d'administration	Grid Manager sur n'importe quel nœud d'administration	Grid Manager sur tous les nœuds d'administration
Gestionnaire de locataires sur un ou plusieurs nœuds d'administration	Gestionnaire de locataires sur n'importe quel nœud d'administration	Gestionnaire de locataires sur tous les nœuds d'administration
Grid Manager et tenant Manager	Gestionnaire de grille	Le Grid Manager uniquement. Vous devez également vous déconnecter du tenant Manager pour vous déconnecter de SSO.



Le tableau résume ce qui se passe lorsque vous vous déconnectez si vous utilisez une seule session de navigateur. Si vous êtes connecté à StorageGRID à travers plusieurs sessions de navigateur, vous devez vous déconnecter de toutes les sessions de navigateur séparément.

Conditions requises pour l'utilisation de l'authentification unique

Avant d'activer la signature unique (SSO) pour un système StorageGRID, consultez les conditions requises dans cette section.



L'authentification unique (SSO) n'est pas disponible sur les ports du gestionnaire de grille restreinte ou du gestionnaire de locataires. Vous devez utiliser le port HTTPS par défaut (443) si vous souhaitez que les utilisateurs s'authentifient avec une connexion unique.

Exigences du fournisseur d'identités

Le fournisseur d'identités (IDP) pour SSO doit satisfaire aux exigences suivantes :

- L'une des versions suivantes d'Active Directory Federation Service (AD FS) :
 - AD FS 4.0, inclus dans Windows Server 2016



Windows Server 2016 doit utiliser le "[Mise à jour KB3201845](#)", ou supérieur.

- AD FS 3.0, inclus avec la mise à jour Windows Server 2012 R2, ou une version ultérieure.
- TLS (transport Layer Security) 1.2 ou 1.3
- Microsoft .NET Framework, version 3.5.1 ou supérieure

Configuration requise pour le certificat de serveur

StorageGRID utilise un certificat de serveur d'interface de gestion sur chaque nœud d'administration pour sécuriser l'accès à Grid Manager, au gestionnaire de locataires, à l'API de gestion du grid et à l'API de gestion des locataires. Lorsque vous configurez les approbations de tiers basés SSO pour StorageGRID dans AD FS, vous utilisez le certificat de serveur comme certificat de signature pour les requêtes StorageGRID à AD FS.

Si vous n'avez pas encore installé de certificat de serveur personnalisé pour l'interface de gestion, vous devriez le faire maintenant. Lorsque vous installez un certificat de serveur personnalisé, il est utilisé pour tous

les nœuds d'administration et vous pouvez l'utiliser dans toutes les approbations de tiers StorageGRID.



Il n'est pas recommandé d'utiliser le certificat de serveur par défaut d'un nœud d'administration dans la confiance de l'intervenant de confiance AD FS. Si le nœud échoue et que vous le récupérez, un nouveau certificat de serveur par défaut est généré. Avant de pouvoir vous connecter au nœud restauré, vous devez mettre à jour la confiance de la partie utilisatrice dans AD FS avec le nouveau certificat.

Vous pouvez accéder au certificat de serveur d'un nœud d'administration en vous connectant au shell de commande du nœud et en allant à `/var/local/mgmt-api` répertoire. Un certificat de serveur personnalisé est nommé `custom-server.crt`. Le certificat de serveur par défaut du nœud est nommé `server.crt`.

Informations associées

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

["Configuration d'un certificat de serveur personnalisé pour le Grid Manager et le tenant Manager"](#)

Configuration de l'authentification unique

Lorsque l'authentification unique (SSO) est activée, les utilisateurs n'ont accès qu'au Grid Manager, au tenant Manager, à l'API Grid Management ou à l'API de gestion des locataires si leurs identifiants sont autorisés à l'aide du processus de connexion SSO mis en œuvre par votre entreprise.

- ["Confirmer que les utilisateurs fédérés peuvent se connecter"](#)
- ["Utilisation du mode sandbox"](#)
- ["Création de fiducies de tiers de confiance dans AD FS"](#)
- ["Confiance de la partie qui fait confiance aux essais"](#)
- ["Activation de l'authentification unique"](#)
- ["Désactivation de la connexion unique"](#)
- ["Désactivation et réactivation temporaire de l'authentification unique pour un nœud d'administration"](#)

Confirmer que les utilisateurs fédérés peuvent se connecter

Avant d'activer l'authentification unique (SSO), vous devez confirmer qu'au moins un utilisateur fédéré peut se connecter au Grid Manager et au tenant Manager pour tout compte de tenant existant.

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.
- Vous utilisez Active Directory en tant que source d'identité fédérée et AD FS en tant que fournisseur d'identité.

["Conditions requises pour l'utilisation de l'authentification unique"](#)

Étapes

1. S'il existe des comptes de tenant existants, vérifiez qu'aucun des locataires n'utilise son propre référentiel d'identité.



Lorsque vous activez SSO, un référentiel d'identité configuré dans le Gestionnaire de locataires est remplacé par le référentiel d'identité configuré dans le Gestionnaire de grille. Les utilisateurs appartenant au référentiel d'identité du locataire ne pourront plus se connecter à moins qu'ils aient un compte avec le référentiel d'identité Grid Manager.

- a. Connectez-vous au Gestionnaire de locataires pour chaque compte de locataire.
 - b. Sélectionnez **contrôle d'accès > fédération d'identités**.
 - c. Vérifiez que la case à cocher **Activer la fédération d'identités** n'est pas cochée.
 - d. Si c'est le cas, vérifiez que les groupes fédérés qui pourraient être utilisés pour ce compte de locataire ne sont plus nécessaires, désélectionnez la case à cocher et cliquez sur **Enregistrer**.
2. Vérifiez qu'un utilisateur fédéré peut accéder au Grid Manager :
 - a. Dans Grid Manager, sélectionnez **Configuration > contrôle d'accès > groupes d'administration**.
 - b. Assurez-vous qu'au moins un groupe fédéré a été importé du référentiel d'identité Active Directory et qu'il a reçu l'autorisation accès racine.
 - c. Se déconnecter.
 - d. Confirmez que vous pouvez vous reconnecter au Grid Manager en tant qu'utilisateur dans le groupe fédéré.
 3. S'il existe déjà des comptes de tenant, confirmez qu'un utilisateur fédéré disposant d'une autorisation accès racine peut se connecter :
 - a. Dans Grid Manager, sélectionnez **tenants**.
 - b. Sélectionnez le compte de tenant, puis cliquez sur **Modifier le compte**.
 - c. Si la case **utilise son propre référentiel d'identité** est cochée, décochez la case et cliquez sur **Enregistrer**.

Edit Tenant Account

Tenant Details

Display Name

S3 tenant account

Uses Own Identity Source

☐

Allow Platform Services

☒

Storage Quota (optional)

GB

▼

Cancel

Save

La page comptes de tenant s'affiche.

- a. Sélectionnez le compte de tenant, cliquez sur **connexion** et connectez-vous au compte de tenant en tant qu'utilisateur racine local.

- b. Dans le Gestionnaire de locataires, cliquez sur **contrôle d'accès > groupes**.
- c. Assurez-vous qu'au moins un groupe fédéré du Grid Manager a reçu l'autorisation accès racine pour ce locataire.
- d. Se déconnecter.
- e. Confirmez que vous pouvez vous reconnecter au locataire en tant qu'utilisateur dans le groupe fédéré.

Informations associées

["Conditions requises pour l'utilisation de l'authentification unique"](#)

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

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

Utilisation du mode sandbox

Vous pouvez utiliser le mode sandbox pour configurer et tester les approbations de parties utilisatrices Active Directory Federation Services (AD FS) avant d'appliquer l'authentification unique (SSO) pour les utilisateurs StorageGRID. Une fois l'authentification SSO activée, vous pouvez réactiver le mode sandbox pour configurer ou tester les approbations nouvelles et existantes. La réactivation du mode sandbox désactive temporairement l'authentification SSO pour les utilisateurs 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 d'accès spécifiques.

Description de la tâche

Lorsque SSO est activé et qu'un utilisateur tente de se connecter à un nœud d'administration, StorageGRID envoie une demande d'authentification à AD FS. À son tour, AD FS renvoie une réponse d'authentification à StorageGRID, indiquant si la demande d'autorisation a réussi. Pour les requêtes réussies, la réponse inclut un identificateur unique universel (UUID) pour l'utilisateur.

Pour permettre à StorageGRID (le fournisseur de services) et à AD FS (le fournisseur d'identité) de communiquer en toute sécurité au sujet des demandes d'authentification des utilisateurs, vous devez configurer certains paramètres dans StorageGRID. Ensuite, vous devez utiliser AD FS pour créer une confiance de partie de confiance pour chaque nœud d'administration. Enfin, vous devez revenir à StorageGRID pour activer le SSO.

Le mode sandbox facilite l'exécution de cette configuration et le test de tous vos paramètres avant l'activation de SSO.



L'utilisation du mode sandbox est fortement recommandée, mais pas strictement nécessaire. Si vous êtes prêt à créer des approbations de tiers AD FS immédiatement après avoir configuré SSO dans StorageGRID, Vous n'avez pas besoin de tester les processus SSO et SLO (Single logout) pour chaque nœud d'administration, cliquez sur **Enabled**, saisissez les paramètres StorageGRID, créez une confiance de partie de confiance pour chaque nœud d'administration dans AD FS, puis cliquez sur **Save** pour activer SSO.

Étapes

1. Sélectionnez **Configuration > contrôle d'accès > connexion unique**.

La page connexion unique s'affiche, avec l'option **Disabled** sélectionnée.

Single Sign-on

You can enable single sign-on (SSO) if you want an external identity provider (IdP) to authorize all user access to StorageGRID. To start, enable [identity federation](#) and confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts. Next, select Sandbox Mode to configure, save, and then test your SSO settings. After verifying the connections, select Enabled and click Save to start using SSO.

SSO Status ☒ Disabled ☐ Sandbox Mode ☐ Enabled

Save



Si les options d'état SSO ne s'affichent pas, confirmez que vous avez configuré Active Directory en tant que référentiel d'identité fédéré. Voir « exigences relatives à l'utilisation d'un seul signe ».

2. Sélectionnez l'option **Sandbox mode**.

Les paramètres fournisseur d'identité et partie de confiance s'affichent. Dans la section Identity Provider, le champ **Service Type** est en lecture seule. Elle indique le type de service de fédération d'identités que vous utilisez (par exemple, Active Directory).

3. Dans la section Identity Provider :

- a. Entrez le nom du service de fédération, exactement tel qu'il apparaît dans AD FS.



Pour localiser le nom du service de fédération, accédez à Windows Server Manager. Sélectionnez **Outils > AD FS Management**. Dans le menu action, sélectionnez **Modifier les propriétés du service de fédération**. Le nom du service de fédération est indiqué dans le second champ.

- b. Indiquez si vous souhaitez utiliser TLS (transport Layer Security) pour sécuriser la connexion lorsque le fournisseur d'identité envoie des informations de configuration SSO en réponse aux requêtes StorageGRID.

- **Utilisez le certificat CA du système d'exploitation** : utilisez le certificat CA par défaut installé sur le système d'exploitation pour sécuriser la connexion.
- **Utilisez un certificat d'autorité de certification personnalisé** : utilisez un certificat d'autorité de certification personnalisé pour sécuriser la connexion.

Si vous sélectionnez ce paramètre, copiez et collez le certificat dans la zone de texte **certificat CA**.

- **N'utilisez pas TLS**: N'utilisez pas de certificat TLS pour sécuriser la connexion.

4. Dans la section partie utilisatrice, spécifiez l'identifiant de partie utilisatrice que vous utiliserez pour les nœuds Admin StorageGRID lorsque vous configurez des approbations de partie utilisatrice.

- Par exemple, si votre grid ne comporte qu'un seul nœud d'administration et que vous n'prévoyez pas d'ajouter de nœuds d'administration à l'avenir, entrez SG ou StorageGRID.
- Si votre grid inclut plusieurs nœuds d'administration, incluez la chaîne [HOSTNAME] dans l'identificateur. Par exemple : SG-[HOSTNAME]. Cela génère une table qui inclut un identifiant de partie de confiance pour chaque nœud d'administration, en fonction du nom d'hôte du nœud. + REMARQUE : vous devez créer une confiance en tiers pour chaque nœud d'administration de votre système StorageGRID. Le fait d'avoir une confiance de partie de confiance pour chaque nœud d'administration

permet aux utilisateurs de se connecter et de se déconnecter en toute sécurité à n'importe quel nœud d'administration.

5. Cliquez sur **Enregistrer**.

- Une coche verte apparaît sur le bouton **Save** pendant quelques secondes.



- L'avis de confirmation du mode Sandbox s'affiche, confirmant que le mode sandbox est à présent activé. Vous pouvez utiliser ce mode pendant que vous utilisez AD FS pour configurer une confiance de tiers de confiance pour chaque nœud d'administration et tester les processus d'ouverture de session unique (SSO) et de déconnexion unique (SLO).

Single Sign-on

You can enable single sign-on (SSO) if you want an external identity provider (IdP) to authorize all user access to StorageGRID. To start, enable [identity federation](#) and confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts. Next, select Sandbox Mode to configure, save, and then test your SSO settings. After verifying the connections, select Enabled and click Save to start using SSO.

SSO Status ☐ Disabled ☒ Sandbox Mode ☐ Enabled

Sandbox mode

Sandbox mode is currently enabled. Use this mode to configure relying party trusts and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

1. Use Active Directory Federation Services (AD FS) to create relying party trusts for StorageGRID. Create one trust for each Admin Node, using the relying party identifier(s) shown below.
2. Go to your identity provider's sign-on page: <https://ad2016.saml.sgws/adfs/ls/idpinitiatedsignon.htm>
3. From this page, sign in to each StorageGRID relying party trust. If the SSO operation is successful, StorageGRID displays a page with a success message. Otherwise, an error message is displayed.

When you have confirmed SSO for each of the relying party trusts and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and click Save.

Informations associées

["Conditions requises pour l'utilisation de l'authentification unique"](#)

Création de fiducies de tiers de confiance dans AD FS

Vous devez utiliser Active Directory Federation Services (AD FS) pour créer une confiance de partie de confiance pour chaque nœud d'administration de votre système. Vous pouvez créer des approbations tierces via les commandes PowerShell, en important les métadonnées SAML depuis StorageGRID ou en saisissant manuellement les données.

Création d'une confiance de confiance avec Windows PowerShell

Vous pouvez utiliser Windows PowerShell pour créer rapidement une ou plusieurs approbations de parties qui font confiance.

Ce dont vous avez besoin

- Vous avez configuré l'authentification unique dans StorageGRID et vous connaissez le nom de domaine complet (ou l'adresse IP) et l'identifiant de partie utilisatrice pour chaque nœud d'administration de votre système.



Vous devez créer une confiance en tiers pour chaque nœud d'administration de votre système StorageGRID. Le fait d'avoir une confiance de partie de confiance pour chaque nœud d'administration permet aux utilisateurs de se connecter et de se déconnecter en toute sécurité à n'importe quel nœud d'administration.

- Vous avez l'expérience de créer des approbations de tiers de confiance dans AD FS, ou vous avez accès à la documentation Microsoft AD FS.
- Vous utilisez le composant logiciel enfichable AD FS Management et vous appartenez au groupe administrateurs.

Description de la tâche

Ces instructions s'appliquent à AD FS 4.0, qui est inclus dans Windows Server 2016. Si vous utilisez AD FS 3.0, qui est inclus dans Windows 2012 R2, vous remarquerez de légères différences dans la procédure. Pour toute question, consultez la documentation Microsoft AD FS.

Étapes

1. Dans le menu Démarrer de Windows, cliquez avec le bouton droit de la souris sur l'icône PowerShell et sélectionnez **Exécuter en tant qu'administrateur**.
2. À l'invite de commande PowerShell, saisissez la commande suivante :

```
Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL  
"https://Admin_Node_FQDN/api/saml-metadata"
```

- Pour *Admin_Node_Identifier*, Entrez l'identifiant de partie de confiance du nœud d'administration, exactement comme il apparaît sur la page Single Sign-On. Par exemple : SG-DC1-ADM1.
- Pour *Admin_Node_FQDN*, Entrez le nom de domaine complet du même nœud d'administration. (Si nécessaire, vous pouvez utiliser l'adresse IP du nœud à la place. Toutefois, si vous saisissez une adresse IP ici, sachez que vous devez mettre à jour ou recréer cette confiance de partie de confiance si cette adresse IP change.)

3. Dans le Gestionnaire de serveur Windows, sélectionnez **Outils > AD FS Management**.

L'outil de gestion AD FS s'affiche.

4. Sélectionnez **AD FS > confiance de la partie de confiance**.

La liste des fiduciaires de tiers de confiance s'affiche.

5. Ajouter une stratégie de contrôle d'accès à la confiance de la partie qui vient d'être créée :
 - a. Recherchez la confiance de la partie de confiance que vous venez de créer.
 - b. Cliquez avec le bouton droit de la souris sur la confiance et sélectionnez **Modifier la stratégie de contrôle d'accès**.
 - c. Sélectionnez une stratégie de contrôle d'accès.
 - d. Cliquez sur **appliquer**, puis sur **OK**
6. Ajouter une politique d'émission de demandes de remboursement à la nouvelle fiducie de compte

comptant :

- a. Recherchez la confiance de la partie de confiance que vous venez de créer.
- b. Cliquez avec le bouton droit de la souris sur la fiducie et sélectionnez **Modifier la politique d'émission des sinistres**.
- c. Cliquez sur **Ajouter règle**.
- d. Sur la page Sélectionner un modèle de règle, sélectionnez **Envoyer attributs LDAP en tant que revendications** dans la liste, puis cliquez sur **Suivant**.
- e. Sur la page configurer la règle, entrez un nom d'affichage pour cette règle.

Par exemple, **objectGUID to Name ID**.

- f. Pour le magasin d'attributs, sélectionnez **Active Directory**.
 - g. Dans la colonne attribut LDAP de la table mappage, saisissez **objectGUID**.
 - h. Dans la colonne Type de demande sortante de la table mappage, sélectionnez **Nom ID** dans la liste déroulante.
 - i. Cliquez sur **Terminer**, puis sur **OK**.
7. Confirmez que les métadonnées ont été importées avec succès.
- a. Cliquez avec le bouton droit de la souris sur la confiance de la partie utilisatrices pour ouvrir ses propriétés.
 - b. Vérifiez que les champs des onglets **Endpoints**, **identificateurs** et **Signature** sont renseignés.
- Si les métadonnées sont manquantes, confirmez que l'adresse des métadonnées de la fédération est correcte ou entrez simplement les valeurs manuellement.
8. Répétez ces étapes pour configurer une confiance de tiers pour tous les nœuds d'administration de votre système StorageGRID.
9. Lorsque vous avez terminé, revenez à StorageGRID et "[tester toutes les fiducies de la partie qui repose](#)" pour confirmer qu'ils sont correctement configurés.

Création d'une confiance de tiers de confiance en important des métadonnées de fédération

Vous pouvez importer les valeurs de chaque confiance de fournisseur en accédant aux métadonnées SAML de chaque nœud d'administration.

Ce dont vous avez besoin

- Vous avez configuré l'authentification unique dans StorageGRID et vous connaissez le nom de domaine complet (ou l'adresse IP) et l'identifiant de partie utilisatrice pour chaque nœud d'administration de votre système.



Vous devez créer une confiance en tiers pour chaque nœud d'administration de votre système StorageGRID. Le fait d'avoir une confiance de partie de confiance pour chaque nœud d'administration permet aux utilisateurs de se connecter et de se déconnecter en toute sécurité à n'importe quel nœud d'administration.

- Vous avez l'expérience de créer des approbations de tiers de confiance dans AD FS, ou vous avez accès à la documentation Microsoft AD FS.
- Vous utilisez le composant logiciel enfichable AD FS Management et vous appartenez au groupe administrateurs.

Description de la tâche

Ces instructions s'appliquent à AD FS 4.0, qui est inclus dans Windows Server 2016. Si vous utilisez AD FS 3.0, qui est inclus dans Windows 2012 R2, vous remarquerez de légères différences dans la procédure. Pour toute question, consultez la documentation Microsoft AD FS.

Étapes

1. Dans le Gestionnaire de serveur Windows, cliquez sur **Outils**, puis sélectionnez **AD FS Management**.
2. Sous actions, cliquez sur **Ajouter la confiance de la partie de confiance**.
3. Sur la page de bienvenue, choisissez **revendications Aware**, puis cliquez sur **Démarrer**.
4. Sélectionnez **Importer les données concernant la partie de confiance publiée en ligne ou sur un réseau local**.
5. Dans **adresse de métadonnées de fédération (nom d'hôte ou URL)**, saisissez l'emplacement des métadonnées SAML pour ce noeud d'administration :

`https://Admin_Node_FQDN/api/saml-metadata`

Pour *Admin_Node_FQDN*, Entrez le nom de domaine complet du même nœud d'administration. (Si nécessaire, vous pouvez utiliser l'adresse IP du nœud à la place. Toutefois, si vous saisissez une adresse IP ici, sachez que vous devez mettre à jour ou recréer cette confiance de partie de confiance si cette adresse IP change.)

6. Terminez l'assistant confiance de la partie de confiance, enregistrez la confiance de la partie de confiance et fermez l'assistant.



Lors de la saisie du nom d'affichage, utilisez l'identificateur de partie comptant pour le noeud d'administration, exactement comme il apparaît sur la page d'ouverture de session unique dans le Gestionnaire de grille. Par exemple : SG-DC1-ADM1.

7. Ajouter une règle de sinistre :
 - a. Cliquez avec le bouton droit de la souris sur la fiducie et sélectionnez **Modifier la politique d'émission des sinistres**.
 - b. Cliquez sur **Ajouter règle** :
 - c. Sur la page Sélectionner un modèle de règle, sélectionnez **Envoyer attributs LDAP en tant que revendications** dans la liste, puis cliquez sur **Suivant**.
 - d. Sur la page configurer la règle, entrez un nom d'affichage pour cette règle.

Par exemple, **objectGUID to Name ID**.
 - e. Pour le magasin d'attributs, sélectionnez **Active Directory**.
 - f. Dans la colonne attribut LDAP de la table mappage, saisissez **objectGUID**.
 - g. Dans la colonne Type de demande sortante de la table mappage, sélectionnez **Nom ID** dans la liste déroulante.
 - h. Cliquez sur **Terminer**, puis sur **OK**.
8. Confirmez que les métadonnées ont été importées avec succès.
 - a. Cliquez avec le bouton droit de la souris sur la confiance de la partie utilisatrices pour ouvrir ses propriétés.
 - b. Vérifiez que les champs des onglets **Endpoints**, **identificateurs** et **Signature** sont renseignés.

Si les métadonnées sont manquantes, confirmez que l'adresse des métadonnées de la fédération est correcte ou entrez simplement les valeurs manuellement.

9. Répétez ces étapes pour configurer une confiance de tiers pour tous les nœuds d'administration de votre système StorageGRID.
10. Lorsque vous avez terminé, revenez à StorageGRID et "[tester toutes les fiducies de la partie qui repose](#)" pour confirmer qu'ils sont correctement configurés.

Création manuelle d'une confiance de partie de confiance

Si vous choisissez de ne pas importer les données pour les approbations de pièces de confiance, vous pouvez entrer les valeurs manuellement.

Ce dont vous avez besoin

- Vous avez configuré l'authentification unique dans StorageGRID et vous connaissez le nom de domaine complet (ou l'adresse IP) et l'identifiant de partie utilisatrice pour chaque nœud d'administration de votre système.



Vous devez créer une confiance en tiers pour chaque nœud d'administration de votre système StorageGRID. Le fait d'avoir une confiance de partie de confiance pour chaque nœud d'administration permet aux utilisateurs de se connecter et de se déconnecter en toute sécurité à n'importe quel nœud d'administration.

- Vous disposez du certificat personnalisé chargé pour l'interface de gestion StorageGRID, ou vous savez comment vous connecter à un nœud d'administration à partir du shell de commande.
- Vous avez l'expérience de créer des approbations de tiers de confiance dans AD FS, ou vous avez accès à la documentation Microsoft AD FS.
- Vous utilisez le composant logiciel enfichable AD FS Management et vous appartenez au groupe administrateurs.

Description de la tâche

Ces instructions s'appliquent à AD FS 4.0, qui est inclus dans Windows Server 2016. Si vous utilisez AD FS 3.0, qui est inclus dans Windows 2012 R2, vous remarquerez de légères différences dans la procédure. Pour toute question, consultez la documentation Microsoft AD FS.

Étapes

1. Dans le Gestionnaire de serveur Windows, cliquez sur **Outils**, puis sélectionnez **AD FS Management**.
2. Sous actions, cliquez sur **Ajouter la confiance de la partie de confiance**.
3. Sur la page de bienvenue, choisissez **revendications Aware**, puis cliquez sur **Démarrer**.
4. Sélectionnez **Entrez les données relatives à la partie de confiance manuellement**, puis cliquez sur **Suivant**.
5. Suivez l'assistant confiance de la partie de confiance :
 - a. Entrez un nom d'affichage pour ce nœud d'administration.

Pour plus de cohérence, utilisez l'identifiant de partie utilisatrices du nœud d'administration, exactement comme il apparaît sur la page Single Sign-On du Grid Manager. Par exemple : SG-DC1-ADM1.

- b. Ignorez l'étape pour configurer un certificat de chiffrement de jeton facultatif.

c. Sur la page configurer l'URL, cochez la case **Activer la prise en charge du protocole SAML 2.0 WebSSO**.

d. Saisissez l'URL du noeud final du service SAML pour le noeud d'administration :

`https://Admin_Node_FQDN/api/saml-response`

Pour *Admin_Node_FQDN*, Entrez le nom de domaine complet du nœud d'administration. (Si nécessaire, vous pouvez utiliser l'adresse IP du nœud à la place. Toutefois, si vous saisissez une adresse IP ici, sachez que vous devez mettre à jour ou recréer cette confiance de partie de confiance si cette adresse IP change.)

e. Sur la page configurer les identificateurs, spécifiez l'identificateur de partie de confiance pour le même noeud d'administration :

Admin_Node_Identifier

Pour *Admin_Node_Identifier*, Entrez l'identifiant de partie de confiance du noeud d'administration, exactement comme il apparaît sur la page Single Sign-On. Par exemple : SG-DC1-ADM1.

f. Vérifiez les paramètres, enregistrez la confiance de la partie utilisatrices et fermez l'assistant.

La boîte de dialogue Modifier la politique d'émission des demandes de remboursement s'affiche.



Si la boîte de dialogue ne s'affiche pas, cliquez avec le bouton droit de la souris sur la fiducie et sélectionnez **Modifier la politique d'émission des sinistres**.

6. Pour démarrer l'assistant règle de sinistre, cliquez sur **Ajouter règle** :

a. Sur la page Sélectionner un modèle de règle, sélectionnez **Envoyer attributs LDAP en tant que revendications** dans la liste, puis cliquez sur **Suivant**.

b. Sur la page configurer la règle, entrez un nom d'affichage pour cette règle.

Par exemple, **objectGUID to Name ID**.

c. Pour le magasin d'attributs, sélectionnez **Active Directory**.

d. Dans la colonne attribut LDAP de la table mappage, saisissez **objectGUID**.

e. Dans la colonne Type de demande sortante de la table mappage, sélectionnez **Nom ID** dans la liste déroulante.

f. Cliquez sur **Terminer**, puis sur **OK**.

7. Cliquez avec le bouton droit de la souris sur la confiance de la partie utilisatrices pour ouvrir ses propriétés.

8. Dans l'onglet **Endpoints**, configurez le noeud final pour une déconnexion unique (SLO) :

a. Cliquez sur **Ajouter SAML**.

b. Sélectionnez **Endpoint Type > SAML Logout**.

c. Sélectionnez **Redirect > Redirect**.

d. Dans le champ **URL de confiance**, entrez l'URL utilisée pour la déconnexion unique (SLO) à partir de ce noeud d'administration :

`https://Admin_Node_FQDN/api/saml-logout`

Pour *Admin_Node_FQDN*, Entrez le nom de domaine complet du nœud d'administration. (Si nécessaire, vous pouvez utiliser l'adresse IP du nœud à la place. Toutefois, si vous saisissez une adresse IP ici, sachez que vous devez mettre à jour ou recréer cette confiance de partie de confiance si cette adresse IP change.)

a. Cliquez sur **OK**.

9. Dans l'onglet **Signature**, spécifiez le certificat de signature pour la fiducie de cette partie de confiance :

a. Ajouter le certificat personnalisé :

- Si vous disposez du certificat de gestion personnalisé que vous avez téléchargé vers StorageGRID, sélectionnez ce certificat.
- Si vous ne disposez pas du certificat personnalisé, connectez-vous au nœud d'administration, accédez au `/var/local/mgmt-api` Répertoire du nœud d'administration et ajoutez le `custom-server.crt` fichier de certificat.

Remarque : utilisation du certificat par défaut du nœud d'administration (`server.crt`) n'est pas recommandé. Si le nœud d'administration échoue, le certificat par défaut sera régénéré lorsque vous restaurez le nœud et vous devrez mettre à jour la confiance de l'organisme de confiance.

b. Cliquez sur **appliquer**, puis sur **OK**.

Les propriétés de la partie de confiance sont enregistrées et fermées.

10. Répétez ces étapes pour configurer une confiance de tiers pour tous les nœuds d'administration de votre système StorageGRID.

11. Lorsque vous avez terminé, revenez à StorageGRID et "[tester toutes les fiducies de la partie qui repose](#)" pour confirmer qu'ils sont correctement configurés.

Confiance de la partie qui fait confiance aux essais

Avant d'appliquer l'utilisation de l'authentification unique (SSO) pour StorageGRID, vérifiez que l'authentification unique et la déconnexion unique (SLO) sont correctement configurées. Si vous avez créé une confiance en tiers pour chaque nœud d'administration, confirmez que vous pouvez utiliser SSO et SLO pour chaque nœud d'administration.

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.
- Vous avez configuré une ou plusieurs fiducies de tiers de confiance dans AD FS.

Étapes

1. Sélectionnez **Configuration > contrôle d'accès > connexion unique**.

La page connexion unique s'affiche, avec l'option **Sandbox mode** sélectionnée.

2. Dans les instructions pour le mode sandbox, recherchez le lien vers la page de connexion de votre fournisseur d'identités.

L'URL est dérivée de la valeur que vous avez saisie dans le champ **Nom du service fédéré**.

Sandbox mode

Sandbox mode is currently enabled. Use this mode to configure relying party trusts and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

1. Use Active Directory Federation Services (AD FS) to create relying party trusts for StorageGRID. Create one trust for each Admin Node, using the relying party identifier(s) shown below.
2. Go to your identity provider's sign-on page: <https://ad2016.saml.sgws/adfs/ls/idpinitiatedsignon.htm>
3. From this page, sign in to each StorageGRID relying party trust. If the SSO operation is successful, StorageGRID displays a page with a success message. Otherwise, an error message is displayed.

When you have confirmed SSO for each of the relying party trusts and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and click Save.

3. Cliquez sur le lien ou copiez et collez l'URL dans un navigateur pour accéder à la page de connexion de votre fournisseur d'identités.
4. Pour confirmer que vous pouvez utiliser l'authentification SSO pour vous connecter à StorageGRID, sélectionnez **connexion à l'un des sites suivants**, sélectionnez l'identifiant de partie de confiance pour votre nœud d'administration principal, puis cliquez sur **connexion**.



You are not signed in.

☐ Sign in to this site.

☒ Sign in to one of the following sites:

SG-DC1-ADM1

Sign in

Vous devez entrer votre nom d'utilisateur et votre mot de passe.

5. Entrez votre nom d'utilisateur et votre mot de passe fédérés.
 - Si les opérations de connexion SSO et de déconnexion ont réussi, un message de réussite s'affiche.

✓ Single sign-on authentication and logout test completed successfully.

- Si l'opération SSO échoue, un message d'erreur s'affiche. Corrigez le problème, effacez les cookies du navigateur et réessayez.
6. Répétez les étapes précédentes pour confirmer que vous pouvez vous connecter à n'importe quel autre nœud d'administration.

Si toutes les opérations de connexion SSO et de déconnexion ont réussi, vous êtes prêt à activer SSO.

Activation de l'authentification unique

Après avoir utilisé le mode sandbox pour tester toutes vos approbations StorageGRID, vous êtes prêt à activer l'authentification unique (SSO).

Ce dont vous avez besoin

- Vous devez avoir importé au moins un groupe fédéré du référentiel d'identité et affecté des autorisations de gestion de l'accès racine au groupe. Vous devez confirmer qu'au moins un utilisateur fédéré dispose d'une autorisation d'accès racine au gestionnaire de grille et au gestionnaire de locataires pour tout compte de locataire existant.
- Vous devez avoir testé toutes les approbations de parties utilisatrices à l'aide du mode sandbox.

Étapes

1. Sélectionnez **Configuration > contrôle d'accès > connexion unique**.

La page Single Sign-On s'affiche avec **Sandbox mode** sélectionné.

2. Définissez l'état SSO sur **activé**.
3. Cliquez sur **Enregistrer**.

Un message d'avertissement s'affiche.

Warning

Enable single sign-on

After you enable SSO, no local users—including the root user—will be able to sign in to the Grid Manager, the Tenant Manager, the Grid Management API, or the Tenant Management API.

Before proceeding, confirm the following:

- You have imported at least one federated group from the identity source and assigned Root Access management permissions to the group. You must confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts.
- You have tested all relying party trusts using sandbox mode.

Are you sure you want to enable single sign-on?

Cancel

OK

4. Vérifiez l'avertissement et cliquez sur **OK**.

L'authentification unique est désormais activée.



Tous les utilisateurs doivent utiliser l'authentification SSO pour accéder au Grid Manager, au Gestionnaire de locataires, à l'API de gestion Grid et à l'API de gestion des locataires. Les utilisateurs locaux ne peuvent plus accéder à StorageGRID.

Désactivation de la connexion unique

Vous pouvez désactiver l'authentification unique (SSO) si vous ne souhaitez plus utiliser cette fonctionnalité. Vous devez désactiver l'authentification unique avant de pouvoir désactiver la fédération des identités.

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.

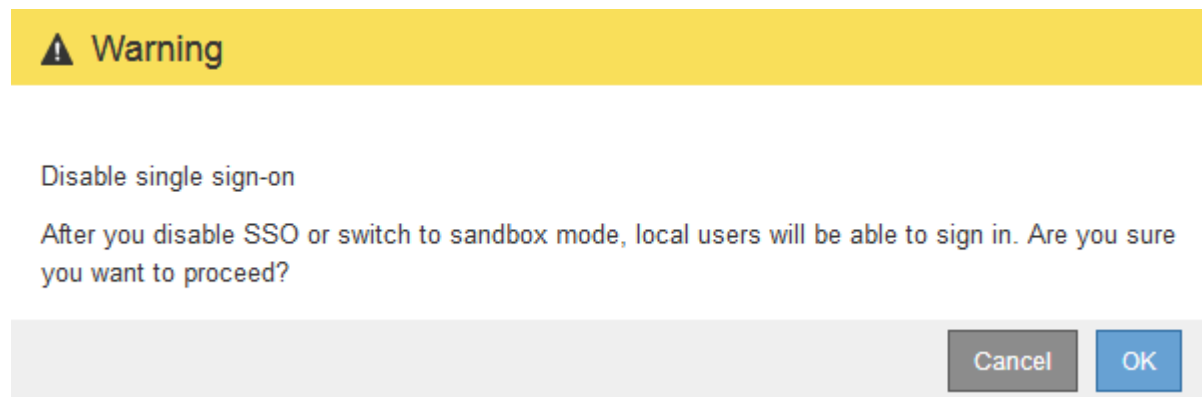
Étapes

1. Sélectionnez **Configuration > contrôle d'accès > connexion unique**.

La page authentification unique s'affiche.

2. Sélectionnez l'option **Disabled**.
3. Cliquez sur **Enregistrer**.

Un message d'avertissement s'affiche pour indiquer que les utilisateurs locaux pourront maintenant se connecter.



4. Cliquez sur **OK**.

La prochaine fois que vous vous connectez à StorageGRID, la page de connexion StorageGRID s'affiche et vous devez entrer le nom d'utilisateur et le mot de passe d'un utilisateur StorageGRID local ou fédéré.

Désactivation et réactivation temporaire de l'authentification unique pour un nœud d'administration

Il se peut que vous ne puissiez pas vous connecter à Grid Manager si le système d'authentification unique (SSO) est en panne. Dans ce cas, vous pouvez temporairement désactiver et réactiver SSO pour un nœud d'administration. Pour désactiver puis réactiver SSO, vous devez accéder au shell de commande du nœud.

Ce dont vous avez besoin

- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous devez avoir le `Passwords.txt` fichier.
- Vous devez connaître le mot de passe de l'utilisateur root local.

Description de la tâche

Après avoir désactivé SSO pour un nœud d'administration, vous pouvez vous connecter à Grid Manager en tant qu'utilisateur racine local. Pour sécuriser votre système StorageGRID, vous devez utiliser le shell de commande du nœud pour réactiver SSO sur le nœud d'administration dès que vous vous déconnectez.



La désactivation de SSO pour un nœud d'administration n'affecte pas les paramètres SSO pour les autres nœuds d'administration de la grille. La case à cocher **Activer SSO** sur la page d'ouverture de session unique dans Grid Manager reste sélectionnée et tous les paramètres SSO existants sont conservés à moins que vous ne les mettez à jour.

Étapes

1. Connectez-vous à un nœud d'administration :

- a. Saisissez la commande suivante : `ssh admin@Admin_Node_IP`
- b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
- c. Entrez la commande suivante pour passer à la racine : `su -`
- d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

2. Exécutez la commande suivante : `disable-saml`

Un message indique que la commande s'applique uniquement à ce nœud d'administration.

3. Confirmez que vous souhaitez désactiver l'authentification SSO.

Un message indique que l'authentification unique est désactivée sur le nœud.

4. À partir d'un navigateur Web, accédez à Grid Manager sur le même nœud d'administration.

La page de connexion à Grid Manager s'affiche car SSO a été désactivé.

5. Connectez-vous avec le nom d'utilisateur root et le mot de passe de l'utilisateur root local.

6. Si vous avez désactivé l'authentification SSO temporairement car vous avez besoin de corriger la configuration SSO :

- a. Sélectionnez **Configuration > contrôle d'accès > connexion unique**.
- b. Modifiez les paramètres SSO incorrects ou obsolètes.
- c. Cliquez sur **Enregistrer**.

Si vous cliquez sur **Enregistrer** à partir de la page connexion unique, l'option SSO est automatiquement réactivée pour l'ensemble de la grille.

7. Si vous avez désactivé l'authentification SSO temporairement car vous devez accéder au Grid Manager pour une autre raison :

- a. Effectuez les tâches que vous souhaitez effectuer.
- b. Cliquez sur **Déconnexion** et fermez le gestionnaire de grille.
- c. Réactivez SSO sur le nœud d'administration. Vous pouvez effectuer l'une des opérations suivantes :

- Exécutez la commande suivante : `enable-saml`

Un message indique que la commande s'applique uniquement à ce nœud d'administration.

Confirmez que vous souhaitez activer le SSO.

Un message indique que l'authentification unique est activée sur le nœud.

◦ Redémarrez le nœud grid : `reboot`

8. À partir d'un navigateur Web, accédez à Grid Manager à partir du même nœud d'administration.

9. Vérifiez que la page de connexion StorageGRID s'affiche et que vous devez saisir vos informations d'identification SSO pour accéder au Gestionnaire de grille.

Informations associées

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

Configuration des certificats client administrateur

Vous pouvez utiliser les certificats client pour permettre aux clients externes autorisés d'accéder à la base de données StorageGRID Prometheus. Les certificats client constituent un moyen sécurisé d'utiliser des outils externes pour surveiller StorageGRID.

Si vous devez accéder à StorageGRID à l'aide d'un outil de surveillance externe, vous devez télécharger ou générer un certificat client à l'aide de Grid Manager et copier les informations de certificat dans l'outil externe.

Ajout de certificats client administrateur

Pour ajouter un certificat client, vous pouvez fournir votre propre certificat ou en générer un à l'aide de Grid Manager.

Ce dont vous avez besoin

- Vous devez disposer de l'autorisation accès racine.
- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez connaître l'adresse IP ou le nom de domaine du nœud d'administration.
- Vous devez avoir configuré le certificat de serveur de l'interface de gestion StorageGRID et avoir le bundle CA correspondant
- Si vous souhaitez télécharger votre propre certificat, la clé publique et la clé privée du certificat doivent être disponibles sur votre ordinateur local.

Étapes

1. Dans Grid Manager, sélectionnez **Configuration > contrôle d'accès > certificats client**.

La page certificats client s'affiche.

Client Certificates


You can upload or generate one or more client certificates to allow StorageGRID to authenticate external client access.


<div>+ Add Edit ✕ Remove</div>		
Name	Allow Prometheus	Expiration Date
No client certificates configured.		

2. Sélectionnez **Ajouter**.

La page Télécharger le certificat s'affiche.

Upload Certificate

Name 

Allow Prometheus  ☐

Certificate Details

Upload the public key for the client certificate.

3. Saisissez un nom entre 1 et 32 caractères pour le certificat.

4. Pour accéder aux metrics Prometheus à l'aide de votre outil de surveillance externe, cochez la case **Autoriser Prometheus**.

5. Télécharger ou générer un certificat :


- a. Pour télécharger un certificat, accédez à [ici](#).
- b. Pour générer un certificat, accédez à [ici](#).

6. pour télécharger un certificat :

- a. Sélectionnez **Télécharger le certificat client**.
- b. Recherchez la clé publique du certificat.

Une fois la clé publique chargée pour le certificat, les champs **métadonnées de certificat** et **PEM de certificat** sont renseignés.

Upload Certificate

Name  test-certificate-upload

Allow Prometheus  ☒

Certificate Details

Upload the public key for the client certificate.

Upload Client Certificate

Generate Client Certificate

Uploaded file name: client (1).crt

Certificate metadata 

```
Subject DN: /C=US/ST=California/L=Sunnyvale/O=Example Co./OU=IT/CN=*.s3.example.com
Serial Number: 0D:0E:FC:16:75:B8:BE:3E:7D:47:4D:05:49:08:F3:7B:E8:4A:71:90
Issuer DN: /C=US/ST=California/L=Sunnyvale/O=Example Co./OU=IT/CN=*.s3.example.com
Issued On: 2020-06-19T22:11:56.000Z
Expires On: 2021-06-19T22:11:56.000Z
SHA-1 Fingerprint: 13:AA:D6:06:2B:90:FE:B7:7B:EB:1A:83:BE:C3:62:39:B7:A6:E7:F0
SHA-256 Fingerprint: 5C:29:06:6B:CF:81:50:B8:4F:A9:56:F7:A7:AB:3C:36:FA:3D:B7:32:A4:C9:74:85:2C:8D:E6:67:37:C3:AC:60
```

Certificate PEM 

```
-----BEGIN CERTIFICATE-----
MIIDmzCCAoOgAwIBAgIUUDQ78FnW4vj59R00FSQjze+hKcZAwDQYJKoZIhvcNAQEL
BQAwDELMAkGA1UEBhMCVVMxExARBgNVBAgMCkNhbg1mb3JuaWVxExJALzBhMB4G
A1UEAwwtZW50bm55dmFzZTEUMBIGA1UECgwLRXhhbXBsZSBDb3Y4eCZAJBgNVBAeM
AklUMRkwFwYDQDDBAQgLnMzLmV4YW1wbGUuY29tMB4XDTEwMDYxOTIyMTE1N1oXDTI
xMDYxOTIyMTE1N1owDELMAkGA1UEBhMCVVMxExARBgNVBAgMCkNhbg1mb3JuaWVxEx
JALzBhMB4GMA1UEAwwtZW50bm55dmFzZTEUMBIGA1UECgwLRXhhbXBsZSBDb3Y4eC
ZAJBgNVBAeMAklUMRkwFwYDQDDBAQgLnMzLmV4YW1wbGUuY29tMIIIBIjANBgkqhki
G9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzVqq2MnjvVotLeGtq1Co4coJmsQ2yRhuwS2a
0bgMnjfcwUgHNVFXGuGlzY/Tl37r3Dk5buZfyGYAeJ6mqbQA6cE3yp0p5Hx7Cm/ANJ
knPw6
```

Copy certificate to clipboard

Cancel

Save

- Sélectionnez **Copier le certificat dans le presse-papiers** et collez le certificat dans votre outil de surveillance externe.
 - Utilisez un outil d'édition pour copier et coller la clé privée dans votre outil de surveillance externe.
 - Sélectionnez **Enregistrer** pour enregistrer le certificat dans Grid Manager.
7. pour générer un certificat :
- Sélectionnez **générer certificat client**.
 - Entrez le nom de domaine ou l'adresse IP du nœud d'administration.
 - Vous pouvez également saisir un sujet X.509, également appelé Nom unique (DN), pour identifier l'administrateur qui possède le certificat.
 - Vous pouvez également sélectionner le nombre de jours pendant lesquels le certificat est valide. La valeur par défaut est 730 jours.
 - Sélectionnez **generate**.

Les champs **Certificate Metadata**, **Certificate PEM** et **Certificate Private Key** sont renseignés.

Upload Certificate

Name

test-certificate-generate

Allow Prometheus

☒

Certificate Details

Upload the public key for the client certificate.

Upload Client Certificate

Generate Client Certificate

Certificate metadata

Subject DN: /CN=test.com

Serial Number: 08:F8:FB:76:B2:13:E4:DF:54:83:3D:35:56:6F:2A:03:53:B0:E2:0A

Issuer DN: /CN=test.com

Issued On: 2020-11-20T22:44:46.000Z

Expires On: 2022-11-20T22:44:46.000Z

SHA-1 Fingerprint: 6E:DB:8C:F8:3E:20:68:E4:C6:42:52:5F:32:7E:E7:93:66:69:F3:3D

SHA-256 Fingerprint: 73:D3:51:83:ED:D3:89:AD:7B:89:4C:AF:AE:34:76:B6:42:FE:0D:EF:78:C0:A4:86:C2:EB:65:64:C3:D4:7A:B0

Certificate PEM

-----BEGIN CERTIFICATE-----

MIICyzCCABQgAwIBAgIUCPj7drITSN9Uga01Vm8qA1Ow4gwoDQYJKoZIhvcNAQELBQAwEsERMA8GA1UEAwwIdGVudC5jb20wHhcNMjA0MTIwMjI0NDQ2WHcNMjIwMjI0NDQ2WjATMREwDwYDVQQDDAh0ZXN0LmNvb3RCCAsIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBBAK02dS9mx2jFrGuBb2ZMjcidf/cTcKxLcBgm4vIwtailgrvRXgH231B9Y1Qn/Vo729R2mNKKYBwkyQTkGCO2Ixxv0STBLcIWfbb8sTgcIcMyt1V1FOss5WYs4O2xxjnK3/X+AX+6s2WZ1sVe+8CDjGu4ic0V/uVQx4yA1T9S0KnjBmo0LCVjL6iVnkUGB8GbkYUFeOaoMjL6TN1QsoFv9VEB0x8KCP4D7FDba1y2f9Ng5z3FEOQoLNtNcKCaL04D7j2qFqOYUpFJ3M0oh1x0n5pQ78Z5KfYwVvDRg6v52P8UEM1o8GeucofaWfdbpLZM09N1VfHqghXs9AxxNs+7kCAwEAAsMxMSEUwEwIDVR0RBAww

Copy certificate to clipboard

Certificate private key

-----BEGIN RSA PRIVATE KEY-----

MIIEpQIBAAKCAQEAxT20H2bHaM+sa4Fv2kyNyJ1/+1NwxEu0Eab7i8jC2KWC/BFeAdneUH1ghCf9WjvblHaY0oxIHCTJBOQYI5kjG+/RJME+4h29sKx0BwigsK2VWU07CwF2jP97bP6O0rF9f4Bf7xN1ZAxV75IICMa7iJzRX+5VDFHjIDVf1KggcMGY5s0JWMrvqJWwRQYFI2uTJQ948ggyOwvpM2VDOgW/1UQHTEEsKngPvUNtojLZ/02DmtJ8QSCgs202xc0xMz7gPuNmoWo5hSxUnaw6iHXHSfm1Dvxnkp9jBw0MqDm/nY/xQEaWjw266h9pb5lukt2k703VW0WGCf470DPE3yyQQIDAQABAoIBAQCfEUFY4pE0Hqgv2uEL6De4yXMTwg/S6n+WSmvtgdQB4xWEGQrk1kiEUG+HTHyrfJcn6XX0+ACDYAC/Hh1Q67xVDPwRjdpuK0xr1W8srrvsEmpBx99MqH9Y2UGx6Yub3USJaQfDvjA4NvaonMxaYJREBtVAK7f22x2xXVY8b0sRPAjrrn0YCqslLqt5Y0K73s0GSnaTmwIdm2YM6EE

Copy private key to clipboard

You will not be able to view the certificate private key after you close this dialog. To save the keys for future reference, copy and paste the values to another location.

Cancel

Save

- Sélectionnez **Copier le certificat dans le presse-papiers** et collez le certificat dans votre outil de surveillance externe.
- Sélectionnez **Copier la clé privée dans le presse-papiers** et collez la clé dans votre outil de surveillance externe.



- c. Sélectionnez **Enregistrer** pour enregistrer le certificat dans Grid Manager.

8. Configurez les paramètres suivants sur votre outil de surveillance externe, tels que Grafana.

L'exemple de Grafana est présenté dans la capture d'écran suivante :

Name ⓘ sg-prometheus Default ☒

HTTP

URL ⓘ https://admin-node.example.com:9091

Access Server (default) ▼ [Help >](#)

Whitelisted Cookies ⓘ New tag (enter key to [Add](#))

Auth

Basic auth ☐ With Credentials ⓘ ☐

TLS Client Auth ☒ With CA Cert ⓘ ☒

Skip TLS Verify ☐

Forward OAuth Identity ⓘ ☐

TLS/SSL Auth Details ⓘ

CA Cert Begins with ---BEGIN CERTIFICATE---

ServerName admin-node.example.com

Client Cert Begins with ---BEGIN CERTIFICATE---

a. **Nom** : saisissez un nom pour la connexion.

StorageGRID ne requiert pas ces informations, mais vous devez fournir un nom pour tester la connexion.

- b. **URL** : saisissez le nom de domaine ou l'adresse IP du noeud d'administration. Spécifiez HTTPS et le port 9091.

Par exemple : `https://admin-node.example.com:9091`

- c. Activez **TLS client Authorization** et **avec CA Cert**.
- d. Copiez et collez le certificat de serveur d'interface de gestion ou le paquet CA dans le fichier **CA Cert** sous TLS/SSL Auth Details.
- e. **NomServeur** : saisissez le nom de domaine du noeud d'administration.

Le nom de serveur doit correspondre au nom de domaine tel qu'il apparaît dans le certificat de serveur de l'interface de gestion.

- f. Enregistrez et testez le certificat et la clé privée que vous avez copiés à partir de StorageGRID ou d'un fichier local.

Vous avez désormais accès aux metrics Prometheus à partir de StorageGRID grâce à votre outil de surveillance externe.

Pour plus d'informations sur les mesures, reportez-vous aux instructions de contrôle et de dépannage de StorageGRID.

Informations associées

["Utilisation des certificats de sécurité StorageGRID"](#)

["Configuration d'un certificat de serveur personnalisé pour le Grid Manager et le tenant Manager"](#)

["Moniteur et amp ; dépannage"](#)

Modification des certificats du client administrateur

Vous pouvez modifier un certificat pour en changer le nom, activer ou désactiver l'accès Prometheus, ou télécharger un nouveau certificat lorsque celui actuel a expiré.

Ce dont vous avez besoin

- Vous devez disposer de l'autorisation accès racine.
- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez connaître l'adresse IP ou le nom de domaine du nœud d'administration.
- Si vous souhaitez télécharger un nouveau certificat et une nouvelle clé privée, ils doivent être disponibles sur votre ordinateur local.

Étapes

1. Sélectionnez **Configuration > contrôle d'accès > certificats client**.

La page certificats client s'affiche. Les certificats existants sont répertoriés.

Les dates d'expiration du certificat sont répertoriées dans le tableau. Si un certificat expire bientôt ou est déjà expiré, un message apparaît dans le tableau et une alerte est déclenchée.

<div> <div>+ Add</div> <div>✎ Edit</div> <div>✕ Remove</div> </div>			
	Name	Allow Prometheus	Expiration Date
<input type="radio"/>	test-certificate-upload	✓	2021-06-19 16:11:56 MDT
<input checked="" type="radio"/>	test-certificate-generate	✓	2022-08-20 09:42:00 MDT

- Sélectionnez le bouton radio à gauche du certificat que vous souhaitez modifier.
- Sélectionnez **Modifier**.

La boîte de dialogue Modifier le certificat s'affiche.

Edit Certificate test-certificate-generate

Name

test-certificate-generate

Allow Prometheus

☒

Certificate Details

Upload the public key for the client certificate.

Upload Client Certificate

Generate Client Certificate

Certificate metadata

Subject DN: /CN=test.com

Serial Number: 0C:11:87:6C:1E:FD:13:16:F3:F2:06:D9:DA:6D:BC:CE:2A:A9:C3:53

Issuer DN: /CN=test.com

Issued On: 2020-11-23T15:53:33.000Z

Expires On: 2022-11-23T15:53:33.000Z

SHA-1 Fingerprint: AE:E6:70:A7:D3:C3:39:7A:09:F9:62:9B:81:8A:87:CD:43:16:89:A7

SHA-256 Fingerprint: 63:07:BF:FF:08:1E:84:F1:D4:67:C6:16:B0:35:26:00:C6:A3:13:11:7E:5E:90:EC:7A:7B:EF:23:14:55:3D:56

Certificate PEM

-----BEGIN CERTIFICATE-----

MIICyzCCAbOgAwIBAgIUDBGHbB79Exbz8gbZ2m28ziqpW1MwDQYJKoZIhvcNAQELBQAwEzERMASGA1UEAwwIdGVzdC5jb20wHicNMjAwMTIzMTU1MzZWhcNMjIwMTIzMTU1MzZWajATMRcwDwYDVQQDDAh0ZXN0LmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBBAKdgEcneCDFDsljvlnX9ow6oPrdU7m2EN6SS6xdVI156sCH+hkwOs2Mym7EhbnRfwOt2nMjQkcaKIrksOAmutRgG6N1N12FIW0qY0uzFQ0QddLqn7ymEx6wSa9zYSu7bLp84Yn0/LSDPk+h3Jio7Mxt2X70It52DRwFmbLNvEvVEtISh+FbN885AIRO2eLxwC0IRij1bySe76wK+Wmc97HdxRSGyxIWk6BD47XC+d0rv55wrtjc/4lqc5xsE6XmJs2yJg4VARr10y8Icwa9fz00+xpWIdC0NwxkpWJXeBnCoXxYqQxbWz1r+iVLJqLTMxU8zTTI30zUqN00M82GJUCAwEAAAMXMBUwEwYDVR0RBAMw

Copy certificate to clipboard

4. Apportez les modifications souhaitées au certificat.
5. Sélectionnez **Enregistrer** pour enregistrer le certificat dans Grid Manager.
6. Si vous avez téléchargé un nouveau certificat :
 - a. Sélectionnez **Copier le certificat dans le presse-papiers** pour coller le certificat dans votre outil de surveillance externe.
 - b. Utilisez un outil de modification pour copier et coller la nouvelle clé privée dans votre outil de surveillance externe.

- c. Enregistrez et testez le certificat et la clé privée dans votre outil de surveillance externe.
7. Si vous avez généré un nouveau certificat :
- Sélectionnez **Copier le certificat dans le presse-papiers** pour coller le certificat dans votre outil de surveillance externe.
 - Sélectionnez **Copier la clé privée dans le presse-papiers** pour coller le certificat dans votre outil de surveillance externe.



Vous ne pourrez pas afficher ou copier la clé privée après avoir fermé la boîte de dialogue. Copiez la clé dans un endroit sûr.

- c. Enregistrez et testez le certificat et la clé privée dans votre outil de surveillance externe.

Suppression des certificats client administrateur

Si vous n'avez plus besoin d'un certificat, vous pouvez le supprimer.

Ce dont vous avez besoin

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

Étapes

1. Sélectionnez **Configuration > contrôle d'accès > certificats client**.

La page certificats client s'affiche. Les certificats existants sont répertoriés.

+ Add

Edit

Remove

	Name	Allow Prometheus	Expiration Date
<input type="radio"/>	test-certificate-upload		2021-06-19 16:11:56 MDT
<input checked="" type="radio"/>	test-certificate-generate		2022-08-20 09:42:00 MDT

Displaying 2 certificates.

2. Sélectionnez le bouton radio à gauche du certificat que vous souhaitez supprimer.
3. Sélectionnez **Supprimer**.

Une boîte de dialogue de confirmation s'affiche.

Warning

Delete certificate

Are you sure you want to delete the certificate "test-certificate-generate"?

Cancel **OK**

4. Sélectionnez **OK**.

Le certificat a été supprimé.

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.