Contrôler l'accès à StorageGRID

StorageGRID software

NetApp
December 03, 2025

Sommaire

Contrôler l’accès à StorageGRID

Contrôler l’accès à StorageGRID

Vous contrôlez qui peut accéder à StorageGRID et quelles tâches les utilisateurs peuvent effectuer en créant ou en important des groupes et des utilisateurs et en attribuant des autorisations à chaque groupe. En option, vous pouvez activer l’authentification unique (SSO), créer des certificats clients et modifier les mots de passe de la grille.

Contrôler l’accès au Grid Manager

Vous déterminez qui peut accéder au Grid Manager et à l’API Grid Management en important des groupes et des utilisateurs à partir d’un service de fédération d’identité ou en configurant des groupes et des utilisateurs locaux.

En utilisant"fédération d’identité" facilite la mise en place"groupes" et"utilisateurs" plus rapide et permet aux utilisateurs de se connecter à StorageGRID à l’aide d’informations d’identification familières. Vous pouvez configurer la fédération d’identité si vous utilisez Active Directory, OpenLDAP ou Oracle Directory Server.

> Contactez le support technique si vous souhaitez utiliser un autre service LDAP v3.

Vous déterminez les tâches que chaque utilisateur peut effectuer en attribuant des rôles différents."autorisations" à chaque groupe. Par exemple, vous souhaiterez peut-être que les utilisateurs d’un groupe puissent gérer les règles ILM et que les utilisateurs d’un autre groupe puissent effectuer des tâches de maintenance. Un utilisateur doit appartenir à au moins un groupe pour accéder au système.

En option, vous pouvez configurer un groupe pour qu’il soit en lecture seule. Les utilisateurs d’un groupe en lecture seule peuvent uniquement afficher les paramètres et les fonctionnalités. Ils ne peuvent apporter aucune modification ni effectuer aucune opération dans Grid Manager ou l’API Grid Management.

Activer l’authentification unique

Le système StorageGRID prend en charge l’authentification unique (SSO) à l’aide de la norme Security Assertion Markup Language 2.0 (SAML 2.0). Après vous"configurer et activer SSO" , tous les utilisateurs doivent être authentifiés par un fournisseur d’identité externe avant de pouvoir accéder au Grid Manager, au Tenant Manager, à l’API Grid Management ou à l’API Tenant Management. Les utilisateurs locaux ne peuvent pas se connecter à StorageGRID.

Modifier la phrase secrète d’approvisionnement

La phrase secrète de provisionnement est requise pour de nombreuses procédures d’installation et de maintenance, ainsi que pour le téléchargement du package de récupération StorageGRID . La phrase secrète est également requise pour télécharger les sauvegardes des informations de topologie de grille et des clés de chiffrement pour le système StorageGRID . Tu peux"changer la phrase secrète" selon les besoins.

Modifier les mots de passe de la console du nœud

Chaque nœud de votre grille possède un mot de passe de console de nœud unique, dont vous avez besoin pour vous connecter au nœud en tant qu'« admin » via SSH, ou en tant qu’utilisateur root sur une connexion VM/console physique. Au besoin, vous pouvez"modifier le mot de passe de la console du nœud" pour chaque nœud.

Modifier la phrase secrète de provisionnement

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

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous disposez des autorisations d'accès Maintenance ou Root.
- Vous disposez de la phrase secrète de provisionnement actuelle.

À propos de cette tâche

La phrase secrète de provisionnement est requise pour de nombreuses procédures d'installation et de maintenance, ainsi que pour"téléchargement du package de récupération" . La phrase secrète de provisionnement n'est pas répertoriée dans le `Passwords.txt` déposer. Assurez-vous de documenter la phrase secrète de provisionnement et de la conserver dans un endroit sûr et sécurisé.

Étapes

1. Sélectionnez **CONFIGURATION** > **Contrôle d'accès**> **Mots de passe de la grille**.
2. Sous **Modifier la phrase secrète d'approvisionnement**, sélectionnez **Effectuer une modification**
3. Saisissez votre mot de passe de provisionnement actuel.
4. Entrez la nouvelle phrase secrète. La phrase secrète doit contenir au moins 8 et pas plus de 32 caractères. Les phrases secrètes sont sensibles à la casse.
5. Stockez la nouvelle phrase secrète de provisionnement dans un endroit sûr. Il est nécessaire pour les procédures d'installation, d'extension et de maintenance.
6. Saisissez à nouveau la nouvelle phrase secrète et sélectionnez **Enregistrer**.

   Le système affiche une bannière de réussite verte lorsque la modification de la phrase secrète de provisionnement est terminée.

7. Sélectionnez **Pack de récupération**.
8. Saisissez la nouvelle phrase secrète de provisionnement pour télécharger le nouveau package de récupération.

   Après avoir modifié la phrase secrète de provisionnement, vous devez immédiatement télécharger un nouveau package de récupération. Le fichier Recovery Package vous permet de restaurer le système en cas de panne.

Modifier les mots de passe de la console du nœud

Chaque nœud de votre grille possède un mot de passe de console de nœud unique, dont vous avez besoin pour vous connecter au nœud. Suivez ces étapes pour modifier chaque mot de passe de console de nœud unique pour chaque nœud de votre grille.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Autorisation d'accès de maintenance ou root" .
- Vous disposez de la phrase secrète de provisionnement actuelle.

À propos de cette tâche

Utilisez le mot de passe de la console du nœud pour vous connecter à un nœud en tant qu'« administrateur » à l'aide de SSH ou en tant qu'utilisateur root sur une connexion VM/console physique. Le processus de changement de mot de passe de la console du nœud crée de nouveaux mots de passe pour chaque nœud de votre grille et stocke les mots de passe dans un fichier mis à jour. `Passwords.txt` fichier dans le package de récupération. Les mots de passe sont répertoriés dans la colonne Mot de passe du fichier Passwords.txt.

> Il existe des mots de passe d'accès SSH distincts pour les clés SSH utilisées pour la communication entre les nœuds. Les mots de passe d'accès SSH ne sont pas modifiés par cette procédure.

Accéder à l'assistant

Étapes

1. Sélectionnez **CONFIGURATION** > **Contrôle d'accès** > **Mots de passe de la grille**.
2. Sous **Modifier les mots de passe de la console du nœud**, sélectionnez **Effectuer une modification**.

Saisissez la phrase secrète de provisionnement

Étapes

1. Saisissez la phrase secrète de provisionnement de votre grille.
2. Sélectionnez **Continuer**.

Télécharger le package de récupération actuel

Avant de modifier les mots de passe de la console du nœud, téléchargez le package de récupération actuel. Vous pouvez utiliser les mots de passe de ce fichier si le processus de changement de mot de passe échoue pour un nœud.

Étapes

1. Sélectionnez **Télécharger le package de récupération**.
2. Copier le fichier du package de récupération(`.zip`) vers deux endroits sûrs, sécurisés et séparés.

> Le fichier du package de récupération doit être sécurisé car il contient des clés de chiffrement et des mots de passe qui peuvent être utilisés pour obtenir des données à partir du système StorageGRID .

3. Sélectionnez **Continuer**.
4. Lorsque la boîte de dialogue de confirmation s'affiche, sélectionnez **Oui** si vous êtes prêt à commencer à modifier les mots de passe de la console du nœud.

   Vous ne pouvez pas annuler ce processus une fois qu'il a commencé.

Modifier les mots de passe de la console du nœud

Lorsque le processus de mot de passe de la console du nœud démarre, un nouveau package de récupération est généré qui inclut les nouveaux mots de passe. Ensuite, les mots de passe sont mis à jour sur chaque nœud.

Étapes

1. Attendez que le nouveau package de récupération soit généré, ce qui peut prendre quelques minutes.
2. Sélectionnez **Télécharger un nouveau package de récupération**.
3. Une fois le téléchargement terminé :

   a. Ouvrez le `.zip` déposer.

   b. Confirmez que vous pouvez accéder au contenu, y compris le `Passwords.txt` fichier, qui contient les nouveaux mots de passe de la console du nœud.

   c. Copiez le nouveau fichier du package de récupération(`.zip`) vers deux endroits sûrs, sécurisés et séparés.

   > ⚠ N'écrasez pas l'ancien package de récupération.

   Le fichier du package de récupération doit être sécurisé car il contient des clés de chiffrement et des mots de passe qui peuvent être utilisés pour obtenir des données à partir du système StorageGRID .

4. Cochez la case pour indiquer que vous avez téléchargé le nouveau package de récupération et vérifié le contenu.
5. Sélectionnez **Modifier les mots de passe de la console du nœud** et attendez que tous les nœuds soient mis à jour avec les nouveaux mots de passe. Cela peut prendre quelques minutes.

   Si les mots de passe sont modifiés pour tous les nœuds, une bannière de réussite verte apparaît. Passez à l'étape suivante.

   S'il y a une erreur pendant le processus de mise à jour, un message de bannière répertorie le nombre de nœuds dont le mot de passe n'a pas pu être modifié. Le système réessaiera automatiquement le processus sur tout nœud dont le mot de passe n'a pas été modifié. Si le processus se termine et que certains nœuds n'ont toujours pas de mot de passe modifié, le bouton **Réessayer** apparaît.

   Si la mise à jour du mot de passe a échoué pour un ou plusieurs nœuds :

   a. Consultez les messages d'erreur répertoriés dans le tableau.

   b. Résoudre les problèmes.

   c. Sélectionnez **Réessayer**.

La nouvelle tentative modifie uniquement les mots de passe de la console du nœud sur les nœuds qui ont échoué lors des tentatives de modification de mot de passe précédentes.

6. Une fois les mots de passe de la console de nœud modifiés pour tous les nœuds, supprimez lepremier package de récupération que vous avez téléchargé .
7. Vous pouvez également utiliser le lien **Pack de récupération** pour télécharger une copie supplémentaire du nouveau package de récupération.

Modifier les mots de passe d'accès SSH pour les nœuds d'administration

La modification des mots de passe d'accès SSH pour les nœuds d'administration met également à jour les ensembles uniques de clés SSH internes pour chaque nœud de la grille. Le nœud d'administration principal utilise ces clés SSH pour accéder aux nœuds à l'aide d'une authentification sécurisée et sans mot de passe.

Utilisez une clé SSH pour vous connecter à un nœud en tant que `admin` ou à l'utilisateur root sur une connexion VM ou console physique.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Autorisation d'accès de maintenance ou root" .
- Vous disposez de la phrase secrète de provisionnement actuelle.

À propos de cette tâche

Les nouveaux mots de passe d'accès pour les nœuds d'administration et les nouvelles clés internes pour chaque nœud sont stockés dans le `Passwords.txt` fichier dans le package de récupération. Les clés sont répertoriées dans la colonne Mot de passe de ce fichier.

Il existe des mots de passe d'accès SSH distincts pour les clés SSH utilisées pour la communication entre les nœuds. Ceux-ci ne sont pas modifiés par cette procédure.

Accéder à l'assistant

Étapes

1. Sélectionnez **CONFIGURATION** > **Contrôle d'accès** > **Mots de passe de la grille**.
2. Sous **Modifier les clés SSH**, sélectionnez **Effectuer une modification**.

Télécharger le package de récupération actuel

Avant de modifier les clés d'accès SSH, téléchargez le package de récupération actuel. Vous pouvez utiliser les clés de ce fichier si le processus de changement de clé échoue pour un nœud.

Étapes

1. Saisissez la phrase secrète de provisionnement de votre grille.
2. Sélectionnez **Télécharger le package de récupération**.

3. Copier le fichier du package de récupération(`.zip`) vers deux endroits sûrs, sécurisés et séparés.

> Le fichier du package de récupération doit être sécurisé car il contient des clés de chiffrement et des mots de passe qui peuvent être utilisés pour obtenir des données à partir du système StorageGRID .

4. Sélectionnez **Continuer**.
5. Lorsque la boîte de dialogue de confirmation apparaît, sélectionnez **Oui** si vous êtes prêt à commencer à modifier les clés d'accès SSH.

> Vous ne pouvez pas annuler ce processus une fois qu'il a commencé.

Modifier les clés d'accès SSH

Lorsque le processus de modification des clés d'accès SSH démarre, un nouveau package de récupération est généré qui inclut les nouvelles clés. Ensuite, les clés sont mises à jour sur chaque nœud.

Étapes

1. Attendez que le nouveau package de récupération soit généré, ce qui peut prendre quelques minutes.
2. Lorsque le bouton Télécharger un nouveau package de récupération est activé, sélectionnez **Télécharger un nouveau package de récupération** et enregistrez le nouveau fichier de package de récupération(`.zip`) vers deux endroits sûrs, sécurisés et séparés.
3. Une fois le téléchargement terminé :

   a. Ouvrez le `.zip` déposer.

   b. Confirmez que vous pouvez accéder au contenu, y compris le `Passwords.txt` fichier, qui contient les nouvelles clés d'accès SSH.

   c. Copiez le nouveau fichier du package de récupération(`.zip`) vers deux endroits sûrs, sécurisés et séparés.

   > N'écrasez pas l'ancien package de récupération.

   Le fichier du package de récupération doit être sécurisé car il contient des clés de chiffrement et des mots de passe qui peuvent être utilisés pour obtenir des données à partir du système StorageGRID .

4. Attendez que les clés soient mises à jour sur chaque nœud, ce qui peut prendre quelques minutes.

   Si les clés sont modifiées pour tous les nœuds, une bannière de réussite verte apparaît.

   En cas d'erreur lors du processus de mise à jour, un message de bannière répertorie le nombre de nœuds dont les clés n'ont pas pu être modifiées. Le système réessaiera automatiquement le processus sur tout nœud dont la clé n'a pas été modifiée. Si le processus se termine avec certains nœuds n'ayant toujours pas de clé modifiée, le bouton **Réessayer** apparaît.

   Si la mise à jour de la clé a échoué pour un ou plusieurs nœuds :

   a. Consultez les messages d'erreur répertoriés dans le tableau.

   b. Résoudre les problèmes.

c. Sélectionnez **Réessayer**.

La nouvelle tentative modifie uniquement les clés d'accès SSH sur les nœuds qui ont échoué lors des tentatives de modification de clé précédentes.

5. Une fois les clés d'accès SSH modifiées pour tous les nœuds, supprimez lepremier package de récupération que vous avez téléchargé .
6. Vous pouvez également sélectionner **MAINTENANCE** > **Système** > **Pack de récupération** pour télécharger une copie supplémentaire du nouveau package de récupération.

Utiliser la fédération d'identité

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

Configurer la fédération d'identité pour Grid Manager

Vous pouvez configurer la fédération d'identité dans Grid Manager si vous souhaitez que les groupes d'administrateurs et les utilisateurs soient gérés dans un autre système tel qu'Active Directory, Azure Active Directory (Azure AD), OpenLDAP ou Oracle Directory Server.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Tu as"autorisations d'accès spécifiques" .
- Vous utilisez Active Directory, Azure AD, OpenLDAP ou Oracle Directory Server comme fournisseur d'identité.

> Si vous souhaitez utiliser un service LDAP v3 qui n'est pas répertorié, contactez le support technique.

- Si vous prévoyez d'utiliser OpenLDAP, vous devez configurer le serveur OpenLDAP. Voir Directives pour la configuration d'un serveur OpenLDAP .
- Si vous envisagez d'activer l'authentification unique (SSO), vous avez examiné les"exigences et considérations relatives à l'authentification unique" .
- Si vous prévoyez d'utiliser Transport Layer Security (TLS) pour les communications avec le serveur LDAP, le fournisseur d'identité utilise TLS 1.2 ou 1.3. Voir "Chiffres pris en charge pour les connexions TLS sortantes" .

À propos de cette tâche

Vous pouvez configurer une source d'identité pour Grid Manager si vous souhaitez importer des groupes à partir d'un autre système tel qu'Active Directory, Azure AD, OpenLDAP ou Oracle Directory Server. Vous pouvez importer les types de groupes suivants :

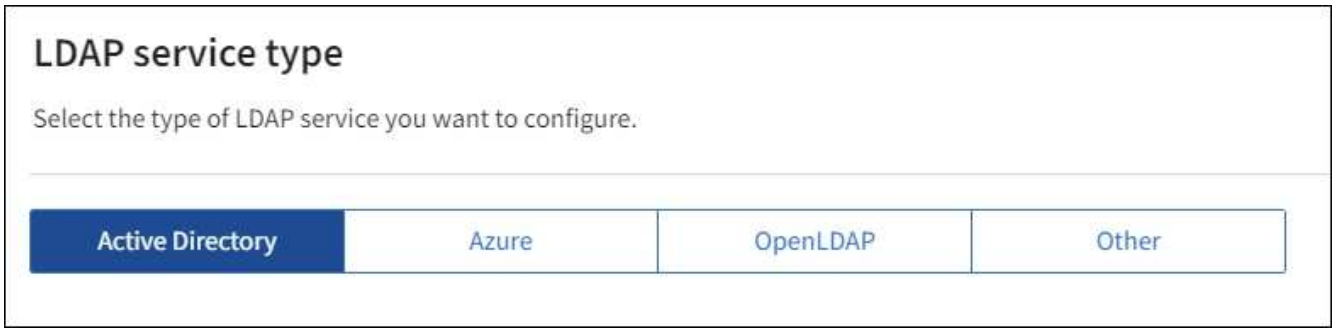
- Groupes d'administrateurs. Les utilisateurs des groupes d'administrateurs peuvent se connecter au gestionnaire de grille et effectuer des tâches, en fonction des autorisations de gestion attribuées au groupe.
- Groupes d'utilisateurs locataires pour les locataires qui n'utilisent pas leur propre source 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. Voir"Créer un compte locataire" et"Utiliser un compte locataire" pour plus de détails.

Entrer la configuration

Étapes

1. Sélectionnez **CONFIGURATION** > **Contrôle d'accès** > **Fédération d'identité**.
2. Sélectionnez **Activer la fédération d'identité**.
3. Dans la section Type de service LDAP, sélectionnez le type de service LDAP que vous souhaitez configurer.



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

4. Si vous avez sélectionné **Autre**, remplissez les champs de la section Attributs LDAP. , passez à l'étape suivante.
   - **Nom unique de l'utilisateur** : le 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 utilisateur** : le 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 du groupe** : le 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** : le nom de l'attribut qui contient l'identifiant 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. Pour tous les types de services LDAP, saisissez les informations de serveur LDAP et de connexion réseau requises dans la section Configurer le serveur LDAP.
   - **Nom d'hôte** : le nom de domaine complet (FQDN) ou l'adresse IP du serveur LDAP.
   - **Port** : Le port utilisé pour se connecter au serveur LDAP.

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

- **Nom d'utilisateur** : le 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 de niveau inférieur ou le nom d'utilisateur principal.

  L'utilisateur spécifié doit avoir l'autorisation de répertorier les groupes et les utilisateurs et d'accéder aux attributs suivants :

  - `sAMAccountName`ou `uid`
  - `objectGUID`, `entryUUID` , ou `nsuniqueid`
  - `cn`
  - `memberOf`ou `isMemberOf`
  - **Active Directory**: `objectSid` , `primaryGroupID` , `userAccountControl` , et `userPrincipalName`
  - **Azuré**: `accountEnabled` et `userPrincipalName`
- **Mot de passe** : Le mot de passe associé au nom d'utilisateur.

  > Si vous modifiez le mot de passe à l'avenir, vous devez le mettre à jour sur cette page.

- **DN de base du groupe** : le chemin complet du nom distinctif (DN) d'une sous-arborescence LDAP dans laquelle vous souhaitez 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=example,DC=com) peuvent être utilisés comme groupes fédérés.

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

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

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

- * Format de nom d'utilisateur de liaison * (facultatif) : le modèle de nom d'utilisateur par défaut que StorageGRID doit utiliser si le modèle ne peut pas être déterminé automatiquement.

  Il est recommandé de fournir le **format de nom d'utilisateur de liaison** car il peut permettre aux utilisateurs de se connecter si StorageGRID ne parvient pas à se lier au compte de service.

  Saisissez l'un de ces modèles :

  - **Modèle UserPrincipalName (Active Directory et Azure)**: `[USERNAME]@*example*.com`
  - **Modèle de nom de connexion de niveau inférieur (Active Directory et Azure)**: `*example*\[USERNAME]`
  - **Modèle de nom distinctif**: `CN=[USERNAME],CN=Users,DC=*example*,DC=com`

    Incluez **[USERNAME]** exactement comme écrit.

6. Dans la section Sécurité de la couche de transport (TLS), sélectionnez un paramètre de sécurité.
   - **Utiliser STARTTLS** : Utilisez STARTTLS pour sécuriser les communications avec le serveur LDAP. Il s'agit de l'option recommandée pour Active Directory, OpenLDAP ou Autre, mais cette option n'est pas prise en charge pour Azure.
   - **Utiliser LDAPS** : L'option LDAPS (LDAP sur SSL) utilise TLS pour établir une connexion au serveur LDAP. Vous devez sélectionner cette option pour Azure.
   - **N'utilisez pas TLS** : le trafic réseau entre le système StorageGRID et le serveur LDAP ne sera pas sécurisé. Cette option n'est pas prise en charge pour Azure.

   > 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.
   - **Utiliser le certificat CA du système d'exploitation** : utilisez le certificat CA Grid par défaut installé sur le système d'exploitation pour sécuriser les connexions.
   - **Utiliser un certificat CA 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 CA.

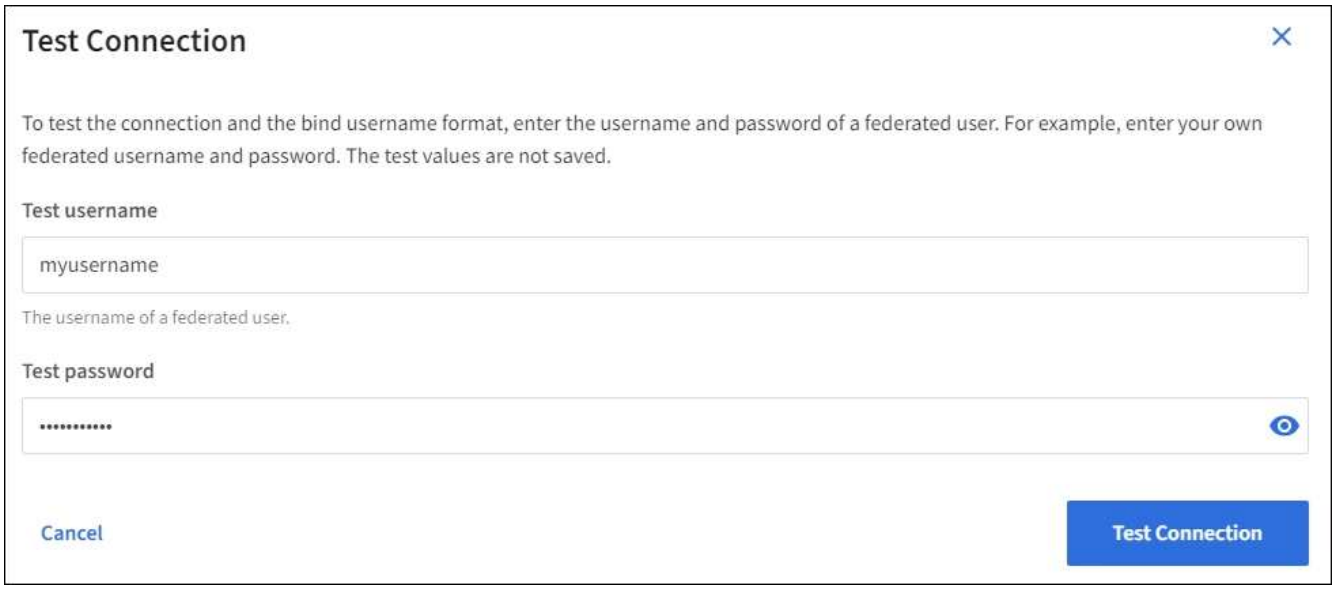
Tester la connexion et enregistrer la configuration

Après avoir saisi toutes les valeurs, vous devez tester la connexion avant de pouvoir enregistrer la configuration. StorageGRID vérifie les paramètres de connexion pour le serveur LDAP et le format du nom d'utilisateur de liaison, si vous en avez fourni un.

Étapes

1. Sélectionnez **Tester la connexion**.
2. Si vous n'avez pas fourni de format de nom d'utilisateur de liaison :
   - Un message « Test de connexion réussi » s'affiche si les paramètres de connexion sont valides. Sélectionnez **Enregistrer** pour enregistrer la configuration.
   - Un message « La connexion de test n'a pas pu être établie » s'affiche si les paramètres de connexion ne sont pas valides. Sélectionnez **Fermer**. Ensuite, résolvez tous les problèmes et testez à nouveau la connexion.
3. Si vous avez fourni un format de nom d'utilisateur de liaison, saisissez le nom d'utilisateur et le mot de passe d'un utilisateur fédéré valide.

   Par exemple, entrez votre propre nom d'utilisateur et votre mot de passe. N'incluez aucun caractère spécial dans le nom d'utilisateur, tel que @ ou /.



- Un message « Test de connexion réussi » s'affiche si les paramètres de connexion sont valides. Sélectionnez **Enregistrer** pour enregistrer la configuration.
- Un message d'erreur s'affiche si les paramètres de connexion, le format du nom d'utilisateur de liaison ou le nom d'utilisateur et le mot de passe de test ne sont pas valides. Résolvez tous les problèmes et testez à nouveau la connexion.

Forcer la synchronisation avec la source d'identité

Le système StorageGRID synchronise périodiquement les groupes fédérés et les utilisateurs à partir de la source d'identité. Vous pouvez forcer le démarrage de la synchronisation si vous souhaitez activer ou restreindre les autorisations des utilisateurs le plus rapidement possible.

Étapes

1. Accédez à la page Fédération d'identité.
2. Sélectionnez **Serveur de synchronisation** en haut de la page.

   Le processus de synchronisation peut prendre un certain temps en fonction de votre environnement.

   L'alerte **Échec de la synchronisation de la fédération d'identité** est déclenchée s'il y a un problème de synchronisation des groupes fédérés et des utilisateurs à partir de la source d'identité.

Désactiver la fédération d'identité

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

À propos de cette tâche

Avant de désactiver la fédération d'identité, vous devez tenir compte des points suivants :

- Les utilisateurs fédérés ne pourront pas se connecter.

- Les utilisateurs fédérés actuellement connectés conserveront 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 la source d'identité n'aura pas lieu et les alertes ne seront pas générées pour les comptes qui n'ont pas été synchronisés.
- La case à cocher **Activer la fédération d'identité** est désactivée si l'authentification unique (SSO) est définie sur **Activé** ou **Mode Sandbox**. Le statut SSO sur la page d'authentification unique doit être **Désactivé** avant de pouvoir désactiver la fédération d'identité. Voir "Désactiver l'authentification unique" .

Étapes

1. Accédez à la page Fédération d'identité.
2. Décochez la case **Activer la fédération d'identité**.

Directives pour la configuration d'un serveur OpenLDAP

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

> Pour les sources d'identité qui ne sont pas ActiveDirectory ou Azure, StorageGRID ne bloquera pas automatiquement l'accès S3 aux utilisateurs désactivés en externe. Pour bloquer l'accès S3, supprimez toutes les clés S3 de l'utilisateur ou supprimez l'utilisateur de tous les groupes.

Superpositions Memberof et refint

Les superpositions memberof et refint doivent être activées. Pour plus d'informations, consultez les instructions relatives à la maintenance de l'appartenance à un groupe inversé dans lehttp://www.openldap.org/doc/admin24/index.html["Documentation OpenLDAP : Guide de l'administrateur version 2.4"^] .

Indexage

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.

Consultez les informations sur la maintenance de l'appartenance à un groupe inversé dans lehttp://www.openldap.org/doc/admin24/index.html["Documentation OpenLDAP : Guide de l'administrateur version 2.4"^] .

Gérer les groupes d'administrateurs

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

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Tu as"autorisations d'accès spécifiques" .
- Si vous prévoyez d'importer un groupe fédéré, vous avez configuré la fédération d'identité et le groupe fédéré existe déjà dans la source d'identité configurée.

Créer un groupe d'administrateurs

Les groupes d'administrateurs vous permettent de déterminer quels utilisateurs peuvent accéder à quelles fonctionnalités et opérations dans Grid Manager et l'API Grid Management.

Accéder à l'assistant

Étapes

1. Sélectionnez **CONFIGURATION** > **Contrôle d'accès** > **Groupes d'administrateurs**.
2. Sélectionnez **Créer un groupe**.

Choisissez un type de groupe

Vous pouvez créer un groupe local ou importer un groupe fédéré.

- Créez un groupe local si vous souhaitez attribuer des autorisations aux utilisateurs locaux.
- Créez un groupe fédéré pour importer des utilisateurs à partir de la source d'identité.

Groupe local

Étapes

1. Sélectionnez **Groupe local**.
2. Saisissez un nom d'affichage pour le groupe, que vous pourrez mettre à jour ultérieurement si nécessaire. Par exemple, « Utilisateurs de maintenance » ou « Administrateurs ILM ».
3. Saisissez un nom unique pour le groupe, que vous ne pourrez pas mettre à jour ultérieurement.
4. Sélectionnez **Continuer**.

Groupe fédéré

Étapes

1. Sélectionnez **Groupe fédéré**.
2. Saisissez le nom du groupe que vous souhaitez importer, exactement tel qu'il apparaît dans la source d'identité configurée.
   - Pour Active Directory et Azure, utilisez sAMAccountName.
   - Pour OpenLDAP, utilisez le CN (Common Name).
   - Pour un autre LDAP, utilisez le nom unique approprié pour le serveur LDAP.
3. Sélectionnez **Continuer**.

Gérer les autorisations de groupe

Étapes

1. Pour le **Mode d'accès**, 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 peuvent uniquement afficher 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 apporter aucune modification ni effectuer aucune opération dans Grid Manager ou l'API Grid Management. 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 aura un accès en lecture seule à tous les paramètres et fonctionnalités sélectionnés.

2. Sélectionnez un ou plusieurs"autorisations du groupe administrateur" .

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

3. Si vous créez un groupe local, sélectionnez **Continuer**. Si vous créez un groupe fédéré, sélectionnez **Créer un groupe** et **Terminer**.

Ajouter des utilisateurs (groupes locaux uniquement)

Étapes

1. Vous pouvez également sélectionner un ou plusieurs utilisateurs locaux pour ce groupe.

   Si vous n'avez pas encore créé d'utilisateurs locaux, vous pouvez enregistrer le groupe sans ajouter d'utilisateurs. Vous pouvez ajouter ce groupe à l'utilisateur sur la page Utilisateurs. Voir"Gérer les utilisateurs" pour plus de détails.

2. Sélectionnez **Créer un groupe** et **Terminer**.

Afficher et modifier les groupes d'administrateurs

Vous pouvez afficher les détails des groupes existants, modifier un groupe ou dupliquer un groupe.

- Pour afficher les informations de base de tous les groupes, consultez le tableau sur la page Groupes.
- Pour afficher tous les détails d'un groupe spécifique ou pour modifier un groupe, utilisez le menu **Actions** ou la page de détails.

Tâche	Menu Actions	Page de détails
Afficher les détails du groupe	a. Cochez la case correspondant au groupe. b. Sélectionnez **Actions** > **Afficher les détails du groupe**.	Sélectionnez le nom du groupe dans le tableau.

Tâche	Menu Actions	Page de détails
Modifier le nom d'affichage (groupes locaux uniquement)	a. Cochez la case correspondant au groupe. b. Sélectionnez **Actions** > **Modifier le nom du groupe**. c. Entrez le nouveau nom. d. Sélectionnez **Enregistrer les modifications**.	a. Sélectionnez le nom du groupe pour afficher les détails. b. Sélectionnez l'icône d'édition . c. Entrez le nouveau nom. d. Sélectionnez **Enregistrer les modifications**.
Modifier le mode d'accès ou les autorisations	a. Cochez la case correspondant au groupe. b. Sélectionnez **Actions** > **Afficher les détails du groupe**. c. Vous pouvez également modifier le mode d'accès du groupe. d. En option, sélectionnez ou désélectionnez"autorisations du groupe administrateur" . e. Sélectionnez **Enregistrer les modifications**.	a. Sélectionnez le nom du groupe pour afficher les détails. b. Vous pouvez également modifier le mode d'accès du groupe. c. En option, sélectionnez ou désélectionnez"autorisations du groupe administrateur" . d. Sélectionnez **Enregistrer les modifications**.

Dupliquer un groupe

Étapes

1. Cochez la case correspondant au groupe.
2. Sélectionnez **Actions** > **Dupliquer le groupe**.
3. Complétez l'assistant de duplication de groupe.

Supprimer un groupe

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

Étapes

1. Depuis la page Groupes, cochez la case correspondant à chaque groupe que vous souhaitez supprimer.
2. Sélectionnez **Actions** > **Supprimer le groupe**.
3. Sélectionnez **Supprimer les groupes**.

Autorisations du groupe d'administrateurs

Lors de la création de groupes d'utilisateurs administrateurs, vous sélectionnez une ou plusieurs autorisations pour contrôler l'accès à des fonctionnalités spécifiques du gestionnaire de grille. Vous pouvez ensuite affecter chaque utilisateur à un ou plusieurs

de ces groupes d'administrateurs pour déterminer les tâches que cet utilisateur peut effectuer.

Vous devez attribuer au moins une autorisation à chaque groupe ; sinon, les utilisateurs appartenant à ce groupe ne pourront pas se connecter au gestionnaire de grille ou à l'API de gestion de grille.

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

- Sign in au gestionnaire de grille
- Afficher le tableau de bord
- Afficher les pages Nœuds
- Afficher les alertes actuelles et résolues
- Modifier leur propre mot de passe (utilisateurs locaux uniquement)
- Consultez certaines informations fournies sur les pages Configuration et Maintenance

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 peuvent uniquement afficher les paramètres et fonctionnalités associés. Si un utilisateur appartient à plusieurs groupes et qu'un groupe est défini sur **Lecture seule**, l'utilisateur aura un accès en lecture seule à tous les paramètres et fonctionnalités sélectionnés.

Les sections suivantes décrivent les autorisations que vous pouvez attribuer lors de la création ou de la modification d'un groupe d'administrateurs. Toute fonctionnalité non explicitement mentionnée nécessite l'autorisation **Accès root**.

Accès root

Cette autorisation donne accès à toutes les fonctionnalités d'administration du réseau.

Modifier le mot de passe root du locataire

Cette autorisation donne accès à l'option **Modifier le mot de passe root** sur la page Locataires, vous permettant de contrôler qui peut modifier le mot de passe de l'utilisateur root local du locataire. Cette autorisation est également utilisée pour migrer les clés S3 lorsque la fonctionnalité d'importation de clés S3 est activée. Les utilisateurs qui ne disposent pas de cette autorisation ne peuvent pas voir l'option **Modifier le mot de passe root**.

> Pour accorder l'accès à la page Locataires, qui contient l'option **Modifier le mot de passe root**, attribuez également l'autorisation **Comptes locataires**.

Configuration de la page de topologie de grille

Cette autorisation donne accès aux onglets de configuration sur la page **SUPPORT** > **Outils** > **Topologie de grille**.

> La page Topologie de grille est obsolète et sera supprimée dans une prochaine version.

ILM

Cette autorisation donne accès aux options de menu **ILM** suivantes :

- Règles
- Politiques
- Balises de politique
- Piscines de stockage
- Niveaux de stockage
- Régions
- Recherche de métadonnées d'objet

> Les utilisateurs doivent disposer des autorisations **Autre configuration de grille** et **Configuration de la page de topologie de grille** pour gérer les niveaux de stockage.

Entretien

Les utilisateurs doivent disposer de l'autorisation Maintenance pour utiliser ces options :

- **CONFIGURATION** > **Contrôle d'accès**:
  - Mots de passe de la grille
- **CONFIGURATION** > **Réseau**:
  - Noms de domaine de point de terminaison S3
- **ENTRETIEN** > **Tâches**:
  - Déclassement
  - Expansion
  - Vérification de l'existence de l'objet
  - Récupération
- **ENTRETIEN** > **Système** :
  - Paquet de relance
  - Mise à jour du logiciel
- **SUPPORT** > **Outils**:
  - Journaux

Les utilisateurs qui ne disposent pas de l'autorisation Maintenance peuvent afficher, mais pas modifier, ces pages :

- **ENTRETIEN** > **Réseau** :
  - serveurs DNS
  - Réseau de grille
  - Serveurs NTP
- **ENTRETIEN** > **Système** :
  - Licence

- **CONFIGURATION** > **Réseau**:
  - Noms de domaine de point de terminaison S3
- **CONFIGURATION** > **Sécurité**:
  - Certificats
- **CONFIGURATION** > **Surveillance**:
  - Serveur d'audit et syslog

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.

Requête de métriques

Cette autorisation donne accès à :

- **SUPPORT** > **Outils** > Page **Métriques**
- Requêtes de métriques Prometheus personnalisées à l'aide de la section **Metrics** de l'API Grid Management
- Cartes de tableau de bord Grid Manager contenant des métriques

Recherche de métadonnées d'objet

Cette autorisation donne accès à la page **ILM** > **Recherche de métadonnées d'objet**.

Autre configuration de grille

Cette autorisation donne accès à des options de configuration de grille supplémentaires.

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

- **ILM**:
  - Niveaux de stockage
- **CONFIGURATION** > **Système**:
- **SOUTIEN** > **Autre** :
  - Coût du lien

Administrateur d'appareils de stockage

Cette autorisation prévoit :

- Accès au gestionnaire de système SANtricity E-Series sur les appliances de stockage via Grid Manager.
- La possibilité d'effectuer des tâches de dépannage et de maintenance sur l'onglet Gérer les lecteurs pour les appareils qui prennent en charge ces opérations.

Comptes locataires

Cette autorisation donne la possibilité de :

- Accédez à la page Locataires, où vous pouvez créer, modifier et supprimer des comptes locataires
- Afficher les politiques de classification du trafic existantes
- Afficher les cartes du tableau de bord Grid Manager qui contiennent les détails du locataire

Gérer les utilisateurs

Vous pouvez afficher les utilisateurs locaux et fédérés. Vous pouvez également créer des utilisateurs locaux et les affecter à des groupes d'administrateurs locaux pour déterminer les fonctionnalités de Grid Manager auxquelles ces utilisateurs peuvent accéder.

Avant de commencer

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

Créer un utilisateur local

Vous pouvez créer un ou plusieurs utilisateurs locaux et affecter chaque utilisateur à un ou plusieurs groupes locaux. Les autorisations du groupe contrôlent les fonctionnalités de Grid Manager et de l'API Grid Management auxquelles l'utilisateur peut accéder.

Vous ne pouvez créer que des utilisateurs locaux. Utilisez la source d'identité externe pour gérer les utilisateurs et les groupes fédérés.

Le gestionnaire de grille comprend un utilisateur local prédéfini, nommé « root ». Vous ne pouvez pas supprimer l'utilisateur root.

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

Accéder à l'assistant

Étapes

1. Sélectionnez **CONFIGURATION** > **Contrôle d'accès** > **Utilisateurs administrateurs**.
2. Sélectionnez **Créer un utilisateur**.

Entrez les informations d'identification de l'utilisateur

Étapes

1. Saisissez le nom complet de l'utilisateur, un nom d'utilisateur unique et un mot de passe.
2. Si vous le souhaitez, sélectionnez **Oui** si cet utilisateur ne doit pas avoir accès au Grid Manager ou à l'API Grid Management.
3. Sélectionnez **Continuer**.

Affecter à des groupes

Étapes

1. Vous pouvez également affecter l'utilisateur à un ou plusieurs groupes pour déterminer les autorisations de l'utilisateur.

   Si vous n'avez pas encore créé de groupes, vous pouvez enregistrer l'utilisateur sans sélectionner de groupes. Vous pouvez ajouter cet utilisateur à un groupe sur la page Groupes.

   Si un utilisateur appartient à plusieurs groupes, les autorisations sont cumulatives. Voir"Gérer les groupes d'administrateurs" pour plus de détails.

2. Sélectionnez **Créer un utilisateur** et sélectionnez **Terminer**.

Afficher et modifier les utilisateurs locaux

Vous pouvez afficher les détails des utilisateurs locaux et fédérés existants. Vous pouvez modifier un utilisateur local pour modifier son nom complet, son mot de passe ou son appartenance à un groupe. Vous pouvez également empêcher temporairement un utilisateur d'accéder au Grid Manager et à l'API Grid Management.

Vous ne pouvez modifier que les utilisateurs locaux. Utilisez la source d'identité externe pour gérer les utilisateurs fédérés.

- Pour afficher les informations de base de tous les utilisateurs locaux et fédérés, consultez le tableau sur la page Utilisateurs.
- Pour afficher tous les détails d'un utilisateur spécifique, modifier un utilisateur local ou changer le mot de passe d'un utilisateur local, utilisez le menu **Actions** ou la page de détails.

  Toutes les modifications sont appliquées la prochaine fois que l'utilisateur se déconnecte, puis se reconnecte au gestionnaire de grille.

> Les utilisateurs locaux peuvent modifier leurs propres mots de passe à l'aide de l'option **Modifier le mot de passe** dans la bannière du gestionnaire de grille.

Tâche	Menu Actions	Page de détails
Afficher les détails de l'utilisateur	a. Cochez la case correspondant à l'utilisateur. b. Sélectionnez **Actions** > **Afficher les détails de l'utilisateur**.	Sélectionnez le nom de l'utilisateur dans le tableau.
Modifier le nom complet (utilisateurs locaux uniquement)	a. Cochez la case correspondant à l'utilisateur. b. Sélectionnez **Actions** > **Modifier le nom complet**. c. Entrez le nouveau nom. d. Sélectionnez **Enregistrer les modifications**.	a. Sélectionnez le nom de l'utilisateur pour afficher les détails. b. Sélectionnez l'icône d'édition . c. Entrez le nouveau nom. d. Sélectionnez **Enregistrer les modifications**.

Tâche	Menu Actions	Page de détails
Refuser ou autoriser l'accès à StorageGRID	a. Cochez la case correspondant à l'utilisateur. b. Sélectionnez **Actions** > **Afficher les détails de l'utilisateur**. c. Sélectionnez l'onglet Accès. d. Sélectionnez **Oui** pour empêcher l'utilisateur de se connecter au gestionnaire de grille ou à l'API de gestion de grille, ou sélectionnez **Non** pour autoriser l'utilisateur à se connecter. e. Sélectionnez **Enregistrer les modifications**.	a. Sélectionnez le nom de l'utilisateur pour afficher les détails. b. Sélectionnez l'onglet Accès. c. Sélectionnez **Oui** pour empêcher l'utilisateur de se connecter au gestionnaire de grille ou à l'API de gestion de grille, ou sélectionnez **Non** pour autoriser l'utilisateur à se connecter. d. Sélectionnez **Enregistrer les modifications**.
Changer le mot de passe (utilisateurs locaux uniquement)	a. Cochez la case correspondant à l'utilisateur. b. Sélectionnez **Actions** > **Afficher les détails de l'utilisateur**. c. Sélectionnez l'onglet Mot de passe. d. Entrez un nouveau mot de passe. e. Sélectionnez **Modifier le mot de passe**.	a. Sélectionnez le nom de l'utilisateur pour afficher les détails. b. Sélectionnez l'onglet Mot de passe. c. Entrez un nouveau mot de passe. d. Sélectionnez **Modifier le mot de passe**.
Changer de groupe (utilisateurs locaux uniquement)	a. Cochez la case correspondant à l'utilisateur. b. Sélectionnez **Actions** > **Afficher les détails de l'utilisateur**. c. Sélectionnez l'onglet Groupes. d. Vous pouvez également sélectionner le lien après le nom d'un groupe pour afficher les détails du groupe dans un nouvel onglet du navigateur. e. Sélectionnez **Modifier les groupes** pour sélectionner différents groupes. f. Sélectionnez **Enregistrer les modifications**.	a. Sélectionnez le nom de l'utilisateur pour afficher les détails. b. Sélectionnez l'onglet Groupes. c. Vous pouvez également sélectionner le lien après le nom d'un groupe pour afficher les détails du groupe dans un nouvel onglet du navigateur. d. Sélectionnez **Modifier les groupes** pour sélectionner différents groupes. e. Sélectionnez **Enregistrer les modifications**.

Dupliquer un utilisateur

Vous pouvez dupliquer un utilisateur existant pour créer un nouvel utilisateur avec les mêmes autorisations.

Étapes

1. Cochez la case correspondant à l'utilisateur.

2. Sélectionnez **Actions** > **Dupliquer l'utilisateur**.
3. Complétez l'assistant de duplication d'utilisateur.

Supprimer un utilisateur

Vous pouvez supprimer un utilisateur local pour supprimer définitivement cet utilisateur du système.

Vous ne pouvez pas supprimer l'utilisateur root.

Étapes

1. Depuis la page Utilisateurs, cochez la case correspondant à chaque utilisateur que vous souhaitez supprimer.
2. Sélectionnez **Actions** > **Supprimer l'utilisateur**.
3. Sélectionnez **Supprimer l'utilisateur**.

Utiliser l'authentification unique (SSO)

Configurer l'authentification unique

Lorsque l'authentification unique (SSO) est activée, les utilisateurs ne peuvent accéder au gestionnaire de grille, au gestionnaire de locataires, à l'API de gestion de grille ou à l'API de gestion de locataires que si leurs informations d'identification sont autorisées à l'aide du processus de connexion SSO mis en œuvre par votre organisation. Les utilisateurs locaux ne peuvent pas se connecter à StorageGRID.

Comment fonctionne l'authentification unique

Le système StorageGRID prend en charge l'authentification unique (SSO) à l'aide de la norme Security Assertion Markup Language 2.0 (SAML 2.0).

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

Sign in lorsque SSO est activé

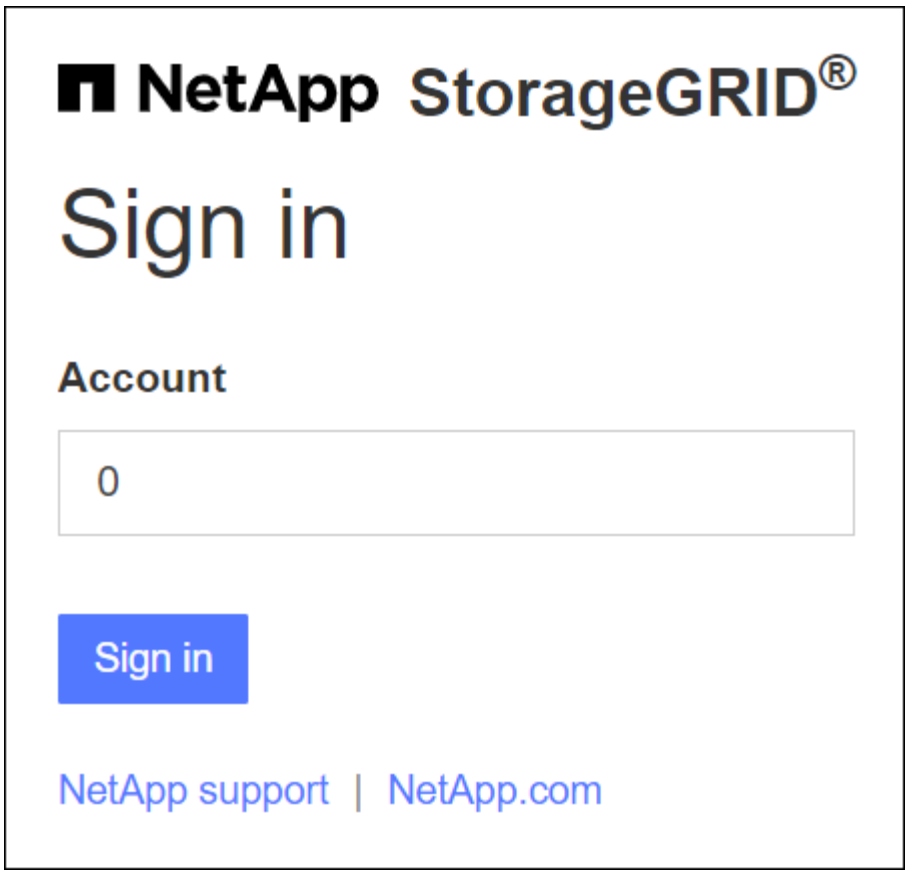
Lorsque SSO est activé et que vous vous connectez à StorageGRID, vous êtes redirigé vers la page SSO de votre organisation pour valider vos informations d'identification.

Étapes

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

   La page de Sign in StorageGRID s'affiche.

   - Si c'est la première fois que vous accédez à l'URL sur ce navigateur, vous êtes invité à saisir un identifiant de compte :

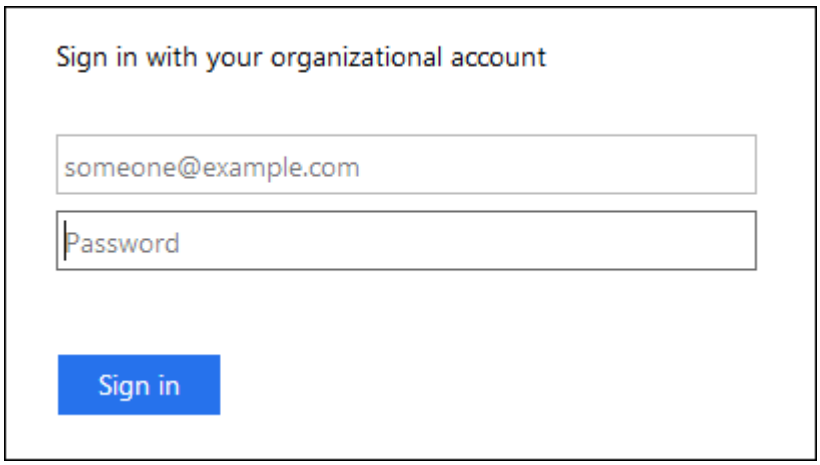


- Si vous avez déjà accédé au Grid Manager ou au Tenant Manager, vous êtes invité à sélectionner un compte récent ou à saisir un ID de compte :

La page de Sign in StorageGRID ne s'affiche pas lorsque vous saisissez l'URL complète d'un compte 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 organisation, où vous pouvezconnectez-vous avec vos identifiants SSO .

2. Indiquez si vous souhaitez accéder au Grid Manager ou au Tenant Manager :
   - Pour accéder au Gestionnaire de grille, laissez le champ **ID de compte** vide, saisissez **0** comme ID de compte ou sélectionnez **Gestionnaire de grille** s'il apparaît dans la liste des comptes récents.
   - Pour accéder au gestionnaire de locataires, saisissez l'ID de compte locataire à 20 chiffres ou sélectionnez un locataire par son nom s'il apparaît dans la liste des comptes récents.
3. Sélectionner * Sign in*

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



4. Sign in avec vos identifiants SSO.

   Si vos informations d'identification SSO sont correctes :

   a. Le fournisseur d'identité (IdP) 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 avec des autorisations d'accès StorageGRID , vous êtes connecté au Grid Manager ou au Tenant Manager, selon le compte que vous avez sélectionné.

   Si le compte de service est inaccessible, vous pouvez toujours vous connecter, à condition que vous soyez un utilisateur existant appartenant à un groupe fédéré avec des autorisations d'accès StorageGRID .

5. Vous pouvez également accéder à d'autres nœuds d'administration ou accéder au gestionnaire de grille ou au gestionnaire de locataires, si vous disposez des autorisations adéquates.

   Vous n'avez pas besoin de ressaisir vos identifiants SSO.

Déconnectez-vous lorsque SSO est activé

Lorsque SSO est activé pour StorageGRID, ce qui se passe lorsque vous vous déconnectez dépend de ce à quoi vous êtes connecté et de l'endroit d'où vous vous déconnectez.

Étapes

1. Localisez le lien **Déconnexion** dans le coin supérieur droit de l'interface utilisateur.
2. Sélectionnez **Déconnexion**.

   La page de Sign in 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 à ces interfaces utilisateur plus rapidement à l'avenir.

Si vous êtes connecté à…	Et vous vous déconnectez de…	Vous êtes déconnecté de…
Gestionnaire de grille sur un ou plusieurs nœuds d'administration	Gestionnaire de grille sur n'importe quel nœud d'administration	Gestionnaire de grille sur tous les nœuds d'administration **Remarque :** si vous utilisez Azure pour l'authentification unique, la déconnexion de tous les nœuds d'administration peut prendre quelques minutes.
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
Gestionnaire de réseau et gestionnaire de locataires	Gestionnaire de grille	Le gestionnaire de grille uniquement. Vous devez également vous déconnecter du gestionnaire de locataires 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 sur plusieurs sessions de navigateur, vous devez vous déconnecter de toutes les sessions de navigateur séparément.

Exigences et considérations relatives à l'authentification unique

Avant d'activer l'authentification unique (SSO) pour un système StorageGRID , examinez les exigences et les considérations.

Exigences relatives aux fournisseurs d'identité

StorageGRID prend en charge les fournisseurs d'identité SSO (IdP) suivants :

- Service de fédération Active Directory (AD FS)
- Azure Active Directory (Azure AD)
- PingFédéré

Vous devez configurer la fédération d'identité pour votre système StorageGRID avant de pouvoir configurer un fournisseur d'identité SSO. Le type de service LDAP que vous utilisez pour la fédération d'identité contrôle le type de SSO que vous pouvez implémenter.

Type de service LDAP configuré	Options pour le fournisseur d'identité SSO
Active Directory	• Active Directory • Azuré • PingFédéré
Azuré	Azuré

Exigences AD FS

Vous pouvez utiliser l'une des versions suivantes d'AD FS :

- Windows Server 2022 AD FS
- Windows Server 2019 AD FS
- Windows Server 2016 AD FS

> Windows Server 2016 devrait utiliser le "Mise à jour KB3201845" , ou supérieur.

Exigences supplémentaires

- Sécurité de la couche transport (TLS) 1.2 ou 1.3
- Microsoft .NET Framework, version 3.5.1 ou supérieure

Considérations pour Azure

Si vous utilisez Azure comme type SSO et que les utilisateurs ont des noms d'utilisateur principaux qui n'utilisent pas sAMAccountName comme préfixe, des problèmes de connexion peuvent survenir si StorageGRID perd sa connexion avec le serveur LDAP. Pour permettre aux utilisateurs de se connecter, vous devez restaurer la connexion au serveur LDAP.

Exigences relatives aux certificats de serveur

Par défaut, StorageGRID utilise un certificat d'interface de gestion sur chaque nœud d'administration pour sécuriser l'accès au gestionnaire de grille, au gestionnaire de locataires, à l'API de gestion de grille et à l'API de gestion de locataires. Lorsque vous configurez des approbations de parties de confiance (AD FS), des applications d'entreprise (Azure) ou des connexions de fournisseurs de services (PingFederate) pour StorageGRID, vous utilisez le certificat du serveur comme certificat de signature pour les demandes StorageGRID .

Si vous ne l'avez pas déjà fait"configuré un certificat personnalisé pour l'interface de gestion" , tu devrais 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 parties de confiance StorageGRID , les applications d'entreprise ou les connexions SP .

L'utilisation du certificat de serveur par défaut d'un nœud d'administration dans une connexion de confiance, une application d'entreprise ou un SP n'est pas recommandée. 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 récupéré, vous devez mettre à jour l'approbation de la partie de confiance, l'application d'entreprise ou la connexion SP avec le nouveau certificat.

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

Exigences portuaires

L'authentification unique (SSO) n'est pas disponible sur les ports restreints Grid Manager ou Tenant Manager. Vous devez utiliser le port HTTPS par défaut (443) si vous souhaitez que les utilisateurs s'authentifient avec l'authentification unique. Voir "Contrôler l'accès au pare-feu externe" .

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 gestionnaire de grille et au gestionnaire de locataires pour tous les comptes de locataires existants.

Avant de commencer

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

Étapes

1. S'il existe des comptes locataires existants, confirmez qu'aucun des locataires n'utilise sa propre source d'identité.

   Lorsque vous activez SSO, une source d'identité configurée dans le gestionnaire de locataires est remplacée par la source d'identité configurée dans le gestionnaire de grille. Les utilisateurs appartenant à la source d'identité du locataire ne pourront plus se connecter à moins qu'ils ne disposent d'un compte auprès de la source d'identité Grid Manager.

   a. Sign in au gestionnaire de locataires pour chaque compte locataire.
   b. Sélectionnez **GESTION DES ACCÈS** > **Fédération d'identité**.
   c. Vérifiez que la case à cocher **Activer la fédération d'identité** n'est pas sélectionnée.
   d. Si tel est le cas, confirmez que tous les groupes fédérés susceptibles d'être utilisés pour ce compte locataire ne sont plus nécessaires, décochez la case et sélectionnez **Enregistrer**.

2. Confirmer qu'un utilisateur fédéré peut accéder au gestionnaire de grille :
   a. Depuis le Gestionnaire de grille, sélectionnez **CONFIGURATION** > **Contrôle d'accès** > **Groupes d'administrateurs**.
   b. Assurez-vous qu'au moins un groupe fédéré a été importé à partir de la source d'identité Active Directory et que l'autorisation d'accès racine lui a été attribuée.

c. Se déconnecter.

d. Confirmez que vous pouvez vous reconnecter au gestionnaire de grille en tant qu'utilisateur du groupe fédéré.

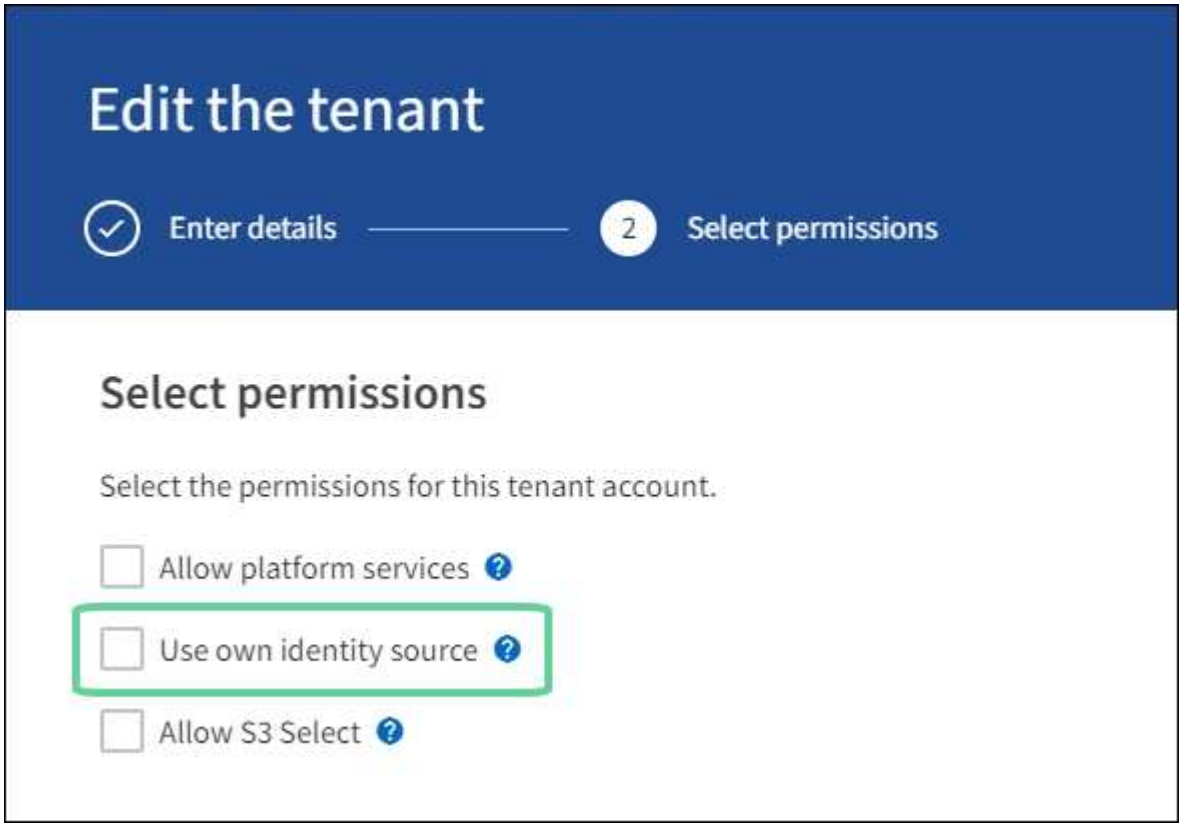
3. S'il existe des comptes locataires existants, confirmez qu'un utilisateur fédéré disposant d'une autorisation d'accès root peut se connecter :

a. Depuis le gestionnaire de grille, sélectionnez **LOCATAIRES**.

b. Sélectionnez le compte locataire, puis sélectionnez **Actions** > **Modifier**.

c. Dans l'onglet Entrer les détails, sélectionnez **Continuer**.

d. Si la case à cocher **Utiliser sa propre source d'identité** est sélectionnée, décochez la case et sélectionnez **Enregistrer**.



La page Locataire apparaît.

a. Sélectionnez le compte locataire, sélectionnez * Sign in* et connectez-vous au compte locataire en tant qu'utilisateur root local.

b. Depuis le gestionnaire de locataires, sélectionnez **GESTION DES ACCÈS** > **Groupes**.

c. Assurez-vous qu'au moins un groupe fédéré du gestionnaire de grille s'est vu attribuer l'autorisation d'accès racine pour ce locataire.

d. Se déconnecter.

e. Confirmez que vous pouvez vous reconnecter au locataire en tant qu'utilisateur du groupe fédéré.

Informations connexes

- "Exigences et considérations relatives à l'authentification unique"
- "Gérer les groupes d'administrateurs"

- "Utiliser un compte locataire"

Utiliser le mode sandbox

Vous pouvez utiliser le mode sandbox pour configurer et tester l'authentification unique (SSO) avant de l'activer pour tous les utilisateurs StorageGRID . Une fois l'authentification unique activée, vous pouvez revenir au mode sandbox chaque fois que vous devez modifier ou retester la configuration.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Autorisation d'accès root" .
- Vous avez configuré la fédération d'identité pour votre système StorageGRID .
- Pour le type de service LDAP de fédération d'identité, vous avez sélectionné Active Directory ou Azure, en fonction du fournisseur d'identité SSO que vous prévoyez d'utiliser.

Type de service LDAP configuré	Options pour le fournisseur d'identité SSO
Active Directory	• Active Directory • Azuré • PingFédéré
Azuré	Azuré

À propos de cette tâche

Lorsque SSO est activé et qu'un utilisateur tente de se connecter à un nœud d'administration, StorageGRID envoie une demande d'authentification au fournisseur d'identité SSO. À son tour, le fournisseur d'identité SSO renvoie une réponse d'authentification à StorageGRID, indiquant si la demande d'authentification a réussi. Pour des demandes réussies :

- La réponse d'Active Directory ou de PingFederate inclut un identifiant unique universel (UUID) pour l'utilisateur.
- La réponse d'Azure inclut un nom d'utilisateur principal (UPN).

Pour permettre à StorageGRID (le fournisseur de services) et au fournisseur d'identité SSO de communiquer en toute sécurité sur les demandes d'authentification des utilisateurs, vous devez configurer certains paramètres dans StorageGRID. Ensuite, vous devez utiliser le logiciel du fournisseur d'identité SSO pour créer une approbation de partie de confiance (AD FS), une application d'entreprise (Azure) ou un fournisseur de services (PingFederate) pour chaque nœud d'administration. Enfin, vous devez revenir à StorageGRID pour activer SSO.

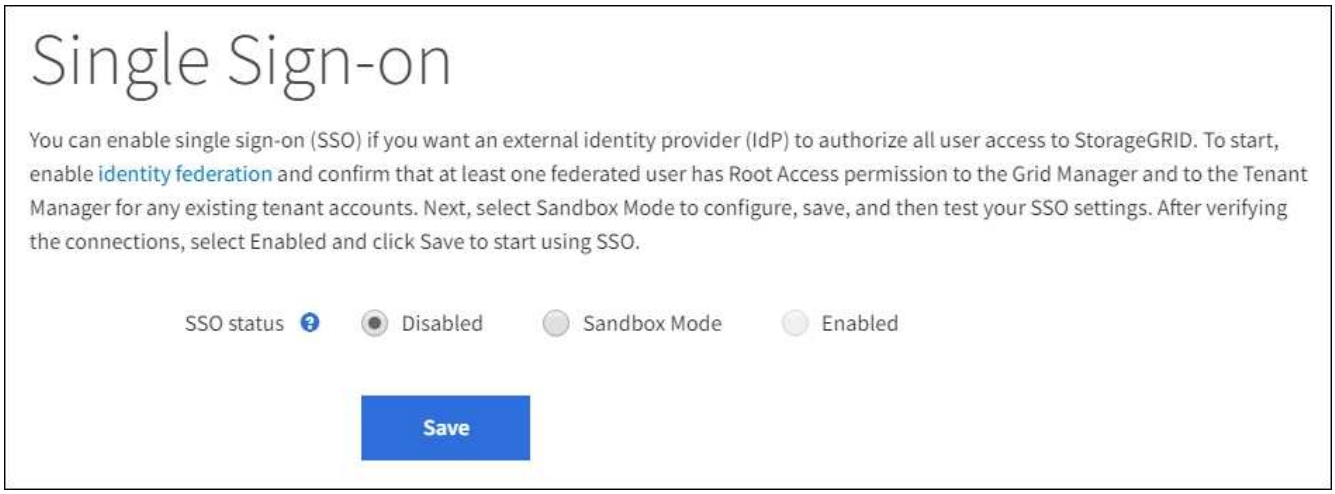
Le mode Sandbox facilite l'exécution de cette configuration aller-retour et permet de tester tous vos paramètres avant d'activer SSO. Lorsque vous utilisez le mode sandbox, les utilisateurs ne peuvent pas se connecter à l'aide de SSO.

Accéder au mode sandbox

Étapes

1. Sélectionnez **CONFIGURATION** > **Contrôle d'accès** > **Authentification unique**.

   La page d'authentification unique s'affiche, avec l'option **Désactivé** sélectionnée.



> Si les options d'état SSO n'apparaissent pas, confirmez que vous avez configuré le fournisseur d'identité comme source d'identité fédérée. Voir "Exigences et considérations relatives à l'authentification unique" .

2. Sélectionnez **Mode Sandbox**.

   La section Fournisseur d'identité apparaît.

Entrez les détails du fournisseur d'identité

Étapes

1. Sélectionnez le **type SSO** dans la liste déroulante.
2. Remplissez les champs de la section Fournisseur d'identité en fonction du type SSO que vous avez sélectionné.

Active Directory

a. Saisissez le **Nom du service de fédération** pour le fournisseur d'identité, exactement tel qu'il apparaît dans Active Directory Federation Service (AD FS).

> Pour localiser le nom du service de fédération, accédez au Gestionnaire de serveur Windows. Sélectionnez **Outils** > **Gestion AD FS**. Dans le menu Action, sélectionnez **Modifier les propriétés du service de fédération**. Le nom du service de fédération est affiché dans le deuxième champ.

b. Spécifiez quel certificat TLS sera utilisé pour sécuriser la connexion lorsque le fournisseur d'identité envoie des informations de configuration SSO en réponse aux demandes StorageGRID .

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

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

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

> Si vous modifiez le certificat CA, immédiatement"redémarrer le service mgmt-api sur les nœuds d'administration" et tester une connexion SSO réussie dans le Grid Manager.

c. Dans la section Partie de confiance, spécifiez l'**identifiant de la partie de confiance** pour StorageGRID. Cette valeur contrôle le nom que vous utilisez pour chaque approbation de partie de confiance dans AD FS.

- Par exemple, si votre grille ne comporte qu'un seul nœud d'administration et que vous ne prévoyez pas d'ajouter d'autres nœuds d'administration à l'avenir, entrez `SG` ou `StorageGRID`.
- Si votre grille comprend plusieurs nœuds d'administration, incluez la chaîne `[HOSTNAME]` dans l'identifiant. Par exemple : `SG-[HOSTNAME]` . Cela génère un tableau qui affiche l'identifiant de la partie de confiance pour chaque nœud d'administration de votre système, en fonction du nom d'hôte du nœud.

> Vous devez créer une approbation de partie de confiance pour chaque nœud d'administration de votre système StorageGRID . Le fait de disposer d'une partie de confiance pour chaque nœud d'administration garantit que les utilisateurs peuvent se connecter et se déconnecter en toute sécurité de n'importe quel nœud d'administration.

d. Sélectionnez **Enregistrer**.

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

Azuré

a. Spécifiez quel certificat TLS sera utilisé pour sécuriser la connexion lorsque le fournisseur d'identité envoie des informations de configuration SSO en réponse aux demandes StorageGRID .

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

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

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

   > Si vous modifiez le certificat CA, immédiatement"redémarrer le service mgmt-api sur les nœuds d'administration" et tester une connexion SSO réussie dans le Grid Manager.

b. Dans la section Application d'entreprise, spécifiez le **Nom de l'application d'entreprise** pour StorageGRID. Cette valeur contrôle le nom que vous utilisez pour chaque application d'entreprise dans Azure AD.

   - Par exemple, si votre grille ne comporte qu'un seul nœud d'administration et que vous ne prévoyez pas d'ajouter d'autres nœuds d'administration à l'avenir, entrez `SG` ou `StorageGRID` .
   - Si votre grille comprend plusieurs nœuds d'administration, incluez la chaîne `[HOSTNAME]` dans l'identifiant. Par exemple : `SG-[HOSTNAME]` . Cela génère un tableau qui affiche un nom d'application d'entreprise pour chaque nœud d'administration de votre système, en fonction du nom d'hôte du nœud.

   > Vous devez créer une application d'entreprise pour chaque nœud d'administration de votre système StorageGRID . Disposer d'une application d'entreprise pour chaque nœud d'administration garantit que les utilisateurs peuvent se connecter et se déconnecter en toute sécurité de n'importe quel nœud d'administration.

c. Suivez les étapes dans"Créer des applications d'entreprise dans Azure AD" pour créer une application d'entreprise pour chaque nœud d'administration répertorié dans le tableau.

d. Depuis Azure AD, copiez l'URL des métadonnées de fédération pour chaque application d'entreprise. Ensuite, collez cette URL dans le champ **URL des métadonnées de la fédération** correspondant dans StorageGRID.

e. Après avoir copié et collé une URL de métadonnées de fédération pour tous les nœuds d'administration, sélectionnez **Enregistrer**.

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

PingFédéré

a. Spécifiez quel certificat TLS sera utilisé pour sécuriser la connexion lorsque le fournisseur d'identité envoie des informations de configuration SSO en réponse aux demandes StorageGRID .

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

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

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

   > Si vous modifiez le certificat CA, immédiatement"redémarrer le service mgmt-api sur les nœuds d'administration" et tester une connexion SSO réussie dans le Grid Manager.

b. Dans la section Fournisseur de services (SP), spécifiez l'*ID de connexion SP * pour StorageGRID. Cette valeur contrôle le nom que vous utilisez pour chaque connexion SP dans PingFederate.

   - Par exemple, si votre grille ne comporte qu'un seul nœud d'administration et que vous ne prévoyez pas d'ajouter d'autres nœuds d'administration à l'avenir, entrez `SG` ou `StorageGRID` .
   - Si votre grille comprend plusieurs nœuds d'administration, incluez la chaîne `[HOSTNAME]` dans l'identifiant. Par exemple : `SG-[HOSTNAME]` . Cela génère un tableau qui affiche l'ID de connexion SP pour chaque nœud d'administration de votre système, en fonction du nom d'hôte du nœud.

   > Vous devez créer une connexion SP pour chaque nœud d'administration de votre système StorageGRID . Disposer d'une connexion SP pour chaque nœud d'administration garantit que les utilisateurs peuvent se connecter et se déconnecter en toute sécurité de n'importe quel nœud d'administration.

c. Spécifiez l'URL des métadonnées de la fédération pour chaque nœud d'administration dans le champ **URL des métadonnées de la fédération**.

   Utilisez le format suivant :

   ```
   https://<Federation Service
   Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP
   Connection ID>
   ```

d. Sélectionnez **Enregistrer**.

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

Configurer les approbations des parties de confiance, les applications d'entreprise ou les connexions SP

Lorsque la configuration est enregistrée, l'avis de confirmation du mode Sandbox apparaît. Cet avis confirme que le mode sandbox est désormais activé et fournit des instructions générales.

StorageGRID peut rester en mode sandbox aussi longtemps que nécessaire. Cependant, lorsque le **Mode Sandbox** est sélectionné sur la page d'authentification unique, l'authentification unique est désactivée pour tous les utilisateurs de StorageGRID . Seuls les utilisateurs locaux peuvent se connecter.

Suivez ces étapes pour configurer les approbations des parties de confiance (Active Directory), compléter les applications d'entreprise (Azure) ou configurer les connexions SP (PingFederate).

Active Directory

Étapes

1. Accédez aux services de fédération Active Directory (AD FS).
2. Créez une ou plusieurs approbations de partie de confiance pour StorageGRID, en utilisant chaque identifiant de partie de confiance indiqué dans le tableau de la page d'authentification unique StorageGRID .

   Vous devez créer une approbation pour chaque nœud d'administration affiché dans le tableau.

   Pour obtenir des instructions, rendez-vous sur"Créer des approbations de parties de confiance dans AD FS" .

Azuré

Étapes

1. Depuis la page d'authentification unique du nœud d'administration auquel vous êtes actuellement connecté, sélectionnez le bouton pour télécharger et enregistrer les métadonnées SAML.
2. Ensuite, pour tous les autres nœuds d'administration de votre grille, répétez ces étapes :
   a. Sign in au nœud.
   b. Sélectionnez **CONFIGURATION** > **Contrôle d'accès** > **Authentification unique**.
   c. Téléchargez et enregistrez les métadonnées SAML pour ce nœud.
3. Accédez au portail Azure.
4. Suivez les étapes dans"Créer des applications d'entreprise dans Azure AD" pour télécharger le fichier de métadonnées SAML pour chaque nœud d'administration dans son application d'entreprise Azure correspondante.

PingFédéré

Étapes

1. Depuis la page d'authentification unique du nœud d'administration auquel vous êtes actuellement connecté, sélectionnez le bouton pour télécharger et enregistrer les métadonnées SAML.
2. Ensuite, pour tous les autres nœuds d'administration de votre grille, répétez ces étapes :
   a. Sign in au nœud.
   b. Sélectionnez **CONFIGURATION** > **Contrôle d'accès** > **Authentification unique**.
   c. Téléchargez et enregistrez les métadonnées SAML pour ce nœud.
3. Accédez à PingFederate.
4. "Créer une ou plusieurs connexions de fournisseur de services (SP) pour StorageGRID" . Utilisez l'ID de connexion SP pour chaque nœud d'administration (affiché dans le tableau de la page d'authentification unique StorageGRID) et les métadonnées SAML que vous avez téléchargées pour ce nœud d'administration.

   Vous devez créer une connexion SP pour chaque nœud d'administration indiqué dans le tableau.

Tester les connexions SSO

Avant d'appliquer l'utilisation de l'authentification unique pour l'ensemble de votre système StorageGRID ,

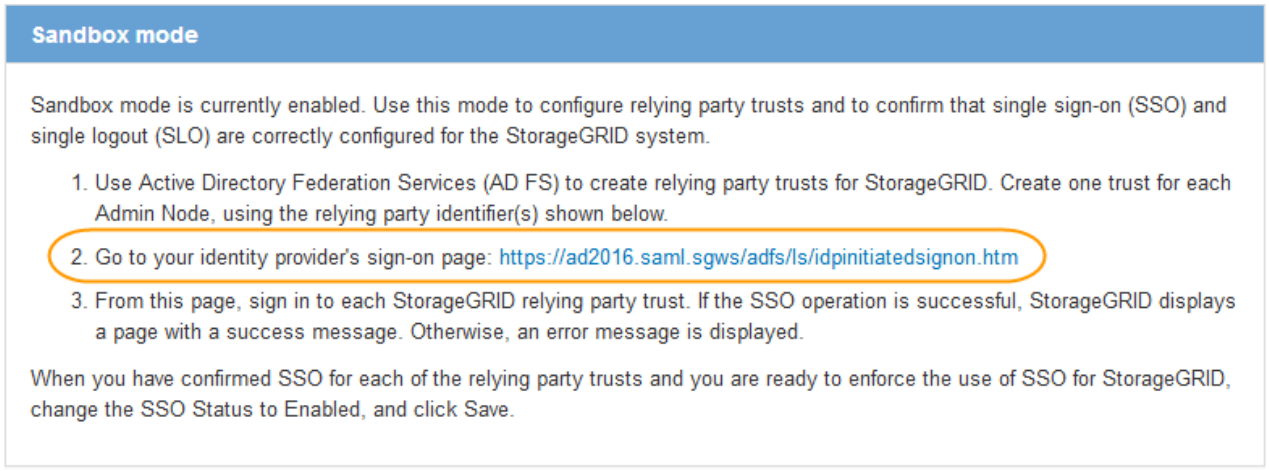
vous devez confirmer que l’authentification unique et la déconnexion unique sont correctement configurées pour chaque nœud d’administration.

Active Directory

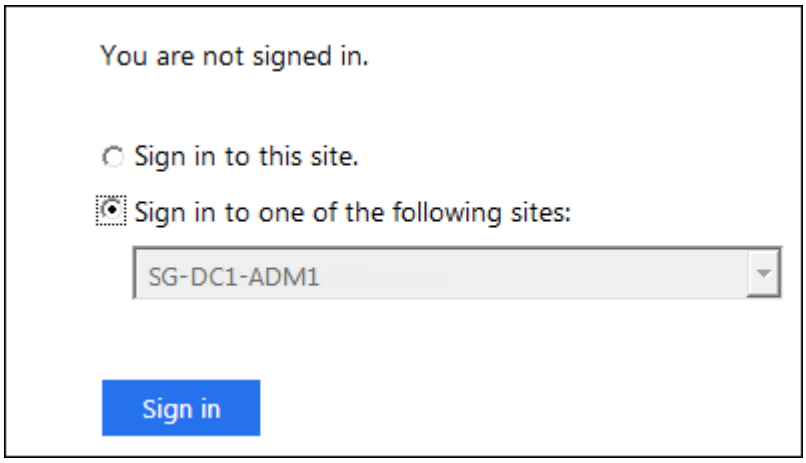
Étapes

1. À partir de la page d'authentification unique StorageGRID , recherchez le lien dans le message du mode Sandbox.

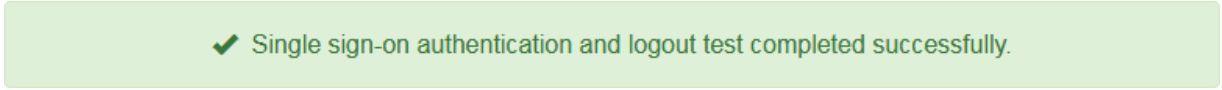
   L'URL est dérivée de la valeur que vous avez saisie dans le champ **Nom du service de fédération**.



2. Sélectionnez le lien ou copiez et collez l'URL dans un navigateur pour accéder à la page de connexion de votre fournisseur d'identité.
3. Pour confirmer que vous pouvez utiliser SSO pour vous connecter à StorageGRID, sélectionnez * Sign in à l'un des sites suivants*, sélectionnez l'identifiant de la partie de confiance pour votre nœud d'administration principal et sélectionnez * Sign in*.



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



   - Si l'opération SSO échoue, un message d'erreur s'affiche. Résolvez le problème, effacez les cookies du navigateur et réessayez.
5. Répétez ces étapes pour vérifier la connexion SSO pour chaque nœud d'administration de votre

grille.

Azuré

Étapes

1. Accédez à la page d'authentification unique dans le portail Azure.
2. Sélectionnez **Tester cette application**.
3. Saisissez les informations d'identification d'un utilisateur fédéré.
   - Si les opérations de connexion et de déconnexion SSO réussissent, un message de réussite s'affiche.

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

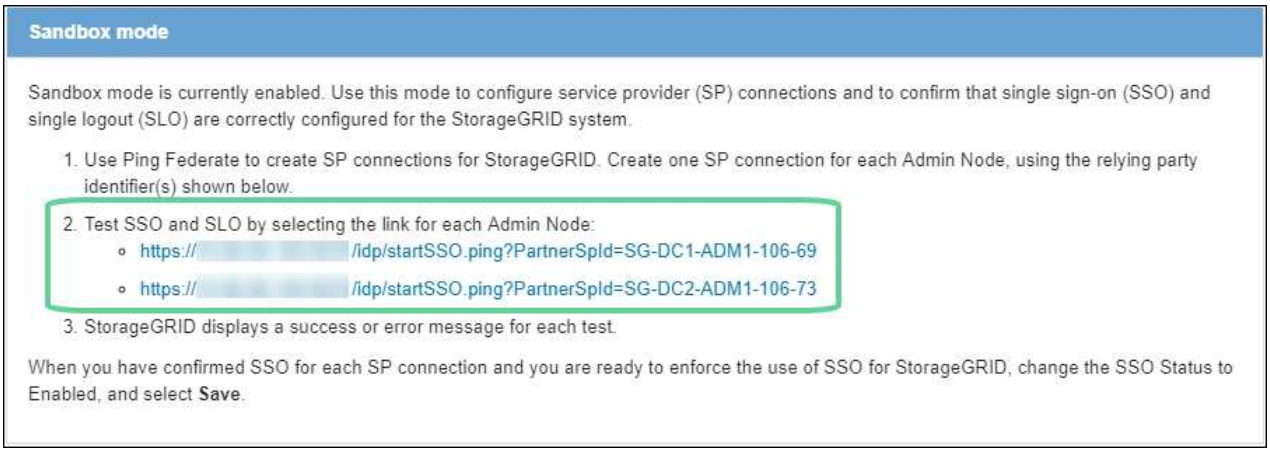
   - Si l'opération SSO échoue, un message d'erreur s'affiche. Résolvez le problème, effacez les cookies du navigateur et réessayez.
4. Répétez ces étapes pour vérifier la connexion SSO pour chaque nœud d'administration de votre grille.

PingFédéré

Étapes

1. À partir de la page d'authentification unique StorageGRID , sélectionnez le premier lien dans le message du mode Sandbox.

   Sélectionnez et testez un lien à la fois.



2. Saisissez les informations d'identification d'un utilisateur fédéré.
   - Si les opérations de connexion et de déconnexion SSO réussissent, 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. Résolvez le problème, effacez les cookies du navigateur et réessayez.
3. Sélectionnez le lien suivant pour vérifier la connexion SSO pour chaque nœud d'administration de votre grille.

Si vous voyez un message indiquant que la page a expiré, sélectionnez le bouton **Retour** dans votre navigateur et soumettez à nouveau vos informations d'identification.

Activer l'authentification unique

Une fois que vous avez confirmé que vous pouvez utiliser SSO pour vous connecter à chaque nœud d'administration, vous pouvez activer SSO pour l'ensemble de votre système StorageGRID .

Lorsque SSO est activé, tous les utilisateurs doivent utiliser SSO pour accéder au gestionnaire de grille, au gestionnaire de locataires, à l'API de gestion de grille et à l'API de gestion de locataires. Les utilisateurs locaux ne peuvent plus accéder à StorageGRID.

Étapes

1. Sélectionnez **CONFIGURATION** > **Contrôle d'accès** > **Authentification unique**.
2. Modifiez le statut SSO sur **Activé**.
3. Sélectionnez **Enregistrer**.
4. Lisez le message d'avertissement et sélectionnez **OK**.

   L'authentification unique est désormais activée.

Si vous utilisez le portail Azure et que vous accédez à StorageGRID à partir du même ordinateur que celui que vous utilisez pour accéder à Azure, assurez-vous que l'utilisateur du portail Azure est également un utilisateur StorageGRID autorisé (un utilisateur d'un groupe fédéré qui a été importé dans StorageGRID) ou déconnectez-vous du portail Azure avant de tenter de vous connecter à StorageGRID.

Créer des approbations de parties de confiance dans AD FS

Vous devez utiliser les services de fédération Active Directory (AD FS) pour créer une approbation de partie de confiance pour chaque nœud d'administration de votre système. Vous pouvez créer des approbations de parties de confiance à l'aide de commandes PowerShell, en important des métadonnées SAML à partir de StorageGRID ou en saisissant les données manuellement.

Avant de commencer

- Vous avez configuré l'authentification unique pour StorageGRID et vous avez sélectionné **AD FS** comme type d'authentification unique.
- Le **mode Sandbox** est sélectionné sur la page d'authentification unique dans Grid Manager. Voir "Utiliser le mode sandbox" .
- Vous connaissez le nom de domaine complet (ou l'adresse IP) et l'identifiant de la partie de confiance pour chaque nœud d'administration de votre système. Vous pouvez trouver ces valeurs dans le tableau détaillé des nœuds d'administration sur la page d'authentification unique StorageGRID .

Vous devez créer une approbation de partie de confiance pour chaque nœud d'administration de votre système StorageGRID . Le fait de disposer d'une partie de confiance pour chaque nœud d'administration garantit que les utilisateurs peuvent se connecter et se déconnecter en toute sécurité de n'importe quel nœud d'administration.

- Vous avez de l'expérience dans la création d'approbations de parties de confiance dans AD FS ou vous avez accès à la documentation Microsoft AD FS.
- Vous utilisez le composant logiciel enfichable Gestion AD FS et vous appartenez au groupe Administrateurs.
- Si vous créez manuellement l'approbation de partie de confiance, vous disposez du certificat personnalisé qui a été téléchargé pour l'interface de gestion StorageGRID ou vous savez comment vous connecter à un nœud d'administration à partir de l'interpréteur de commandes.

À propos de cette tâche

Ces instructions s'appliquent à Windows Server 2016 AD FS. Si vous utilisez une version différente d'AD FS, vous remarquerez de légères différences dans la procédure. Consultez la documentation Microsoft AD FS si vous avez des questions.

Créer une approbation de partie de confiance à l'aide de Windows PowerShell

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

Étapes

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

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

   - Pour *Admin_Node_Identifier* , saisissez l'identifiant de la partie de confiance pour le nœud d'administration, exactement tel qu'il apparaît sur la page d'authentification unique. Par exemple : `SG-DC1-ADM1` .
   - Pour *Admin_Node_FQDN* , entrez le nom de domaine complet pour le même nœud d'administration. (Si nécessaire, vous pouvez utiliser l'adresse IP du nœud à la place. Cependant, si vous saisissez une adresse IP ici, sachez que vous devez mettre à jour ou recréer cette approbation de partie de confiance si cette adresse IP change un jour.)
3. Dans le Gestionnaire de serveur Windows, sélectionnez **Outils** > **Gestion AD FS**.

   L'outil de gestion AD FS apparaît.
4. Sélectionnez **AD FS** > **Approbations de parties de confiance**.

   La liste des fiducies de parties utilisatrices s'affiche.
5. Ajoutez une politique de contrôle d'accès à la nouvelle approbation de partie de confiance créée :
   a. Localisez la fiducie de partie de confiance que vous venez de créer.
   b. Cliquez avec le bouton droit sur l'approbation et sélectionnez **Modifier la politique de contrôle d'accès**.
   c. Sélectionnez une politique de contrôle d'accès.
   d. Sélectionnez **Appliquer**, puis **OK**
6. Ajoutez une politique d'émission de réclamation à la fiducie de partie utilisatrice nouvellement créée :

a. Localisez la fiducie de partie de confiance que vous venez de créer.

b. Cliquez avec le bouton droit sur la fiducie et sélectionnez **Modifier la politique d'émission de réclamation**.

c. Sélectionnez **Ajouter une règle**.

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

e. Sur la page Configurer la règle, entrez un nom d'affichage pour cette règle.

   Par exemple, **ObjectGUID vers Name ID** ou **UPN vers Name ID**.

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

g. Dans la colonne Attribut LDAP de la table de mappage, saisissez **objectGUID** ou sélectionnez **User-Principal-Name**.

h. Dans la colonne Type de réclamation sortante de la table de mappage, sélectionnez **ID de nom** dans la liste déroulante.

i. Sélectionnez **Terminer**, puis **OK**.

7. Confirmez que les métadonnées ont été importées avec succès.

   a. Cliquez avec le bouton droit sur l'approbation de la partie de confiance pour ouvrir ses propriétés.

   b. Confirmez que les champs des onglets **Points de terminaison**, **Identifiants** et **Signature** sont renseignés.

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

8. Répétez ces étapes pour configurer une approbation de partie de confiance pour tous les nœuds d'administration de votre système StorageGRID .

9. Une fois que vous avez terminé, revenez à StorageGRID et testez toutes les approbations des parties de confiance pour confirmer qu'elles sont correctement configurées. Voir"Utiliser le mode Sandbox" pour les instructions.

Créer une approbation de partie de confiance en important des métadonnées de fédération

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

Étapes

1. Dans le Gestionnaire de serveur Windows, sélectionnez **Outils**, puis **Gestion AD FS**.
2. Sous Actions, sélectionnez **Ajouter une approbation de partie de confiance**.
3. Sur la page d'accueil, choisissez **Réclamations prises en compte**, puis sélectionnez **Démarrer**.
4. Sélectionnez **Importer des données sur la partie utilisatrice publiées en ligne ou sur un réseau local**.
5. Dans **Adresse des métadonnées de la fédération (nom d'hôte ou URL)**, saisissez l'emplacement des métadonnées SAML pour ce nœud d'administration :

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

   Pour *`Admin_Node_FQDN`* , entrez le nom de domaine complet pour le même nœud d'administration. (Si nécessaire, vous pouvez utiliser l'adresse IP du nœud à la place. Cependant, si vous saisissez une

adresse IP ici, sachez que vous devez mettre à jour ou recréer cette approbation de partie de confiance si cette adresse IP change un jour.)

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

> Lors de la saisie du nom d'affichage, utilisez l'identifiant de la partie de confiance pour le nœud d'administration, exactement tel qu'il apparaît sur la page d'authentification unique dans le gestionnaire de grille. Par exemple : `SG-DC1-ADM1` .

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

      Par exemple, **ObjectGUID vers Name ID** ou **UPN vers Name ID**.

   e. Pour le magasin d'attributs, sélectionnez **Active Directory**.
   f. Dans la colonne Attribut LDAP de la table de mappage, saisissez **objectGUID** ou sélectionnez **User-Principal-Name**.
   g. Dans la colonne Type de réclamation sortante de la table de mappage, sélectionnez **ID de nom** dans la liste déroulante.
   h. Sélectionnez **Terminer**, puis **OK**.
8. Confirmez que les métadonnées ont été importées avec succès.
   a. Cliquez avec le bouton droit sur l'approbation de la partie de confiance pour ouvrir ses propriétés.
   b. Confirmez que les champs des onglets **Points de terminaison**, **Identifiants** et **Signature** sont renseignés.

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

9. Répétez ces étapes pour configurer une approbation de partie de confiance pour tous les nœuds d'administration de votre système StorageGRID .
10. Une fois que vous avez terminé, revenez à StorageGRID et testez toutes les approbations des parties de confiance pour confirmer qu'elles sont correctement configurées. Voir"Utiliser le mode Sandbox" pour les instructions.

Créer manuellement une fiducie de partie utilisatrice

Si vous choisissez de ne pas importer les données des approbations de partie de confiance, vous pouvez saisir les valeurs manuellement.

Étapes

1. Dans le Gestionnaire de serveur Windows, sélectionnez **Outils**, puis **Gestion AD FS**.
2. Sous Actions, sélectionnez **Ajouter une approbation de partie de confiance**.

3. Sur la page d'accueil, choisissez **Réclamations prises en compte**, puis sélectionnez **Démarrer**.
4. Sélectionnez **Saisir manuellement les données sur la partie de confiance**, puis sélectionnez **Suivant**.
5. Complétez l'assistant d'approbation de partie de confiance :

   a. Saisissez un nom d'affichage pour ce nœud d'administration.

      Par souci de cohérence, utilisez l'identifiant de partie de confiance pour le nœud d'administration, exactement tel qu'il apparaît sur la page d'authentification unique dans le gestionnaire de grille. 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 point de terminaison du service SAML pour le nœud 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. Cependant, si vous saisissez une adresse IP ici, sachez que vous devez mettre à jour ou recréer cette approbation de partie de confiance si cette adresse IP change un jour.)

   e. Sur la page Configurer les identifiants, spécifiez l'identifiant de la partie de confiance pour le même nœud d'administration :

      `Admin_Node_Identifier`

      Pour *`Admin_Node_Identifier`* , saisissez l'identifiant de la partie de confiance pour le nœud d'administration, exactement tel qu'il apparaît sur la page d'authentification unique. Par exemple : `SG-DC1-ADM1` .

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

      La boîte de dialogue Modifier la politique d'émission de réclamation s'affiche.

      > Si la boîte de dialogue n'apparaît pas, cliquez avec le bouton droit sur la fiducie et sélectionnez **Modifier la politique d'émission de réclamation**.

6. Pour démarrer l'assistant de règle de revendication, sélectionnez **Ajouter une règle** :

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

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

      Par exemple, **ObjectGUID vers Name ID** ou **UPN vers Name ID**.

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

   d. Dans la colonne Attribut LDAP de la table de mappage, saisissez **objectGUID** ou sélectionnez **User-Principal-Name**.

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

f. Sélectionnez **Terminer**, puis **OK**.

7. Cliquez avec le bouton droit sur l'approbation de la partie de confiance pour ouvrir ses propriétés.
8. Dans l'onglet **Points de terminaison**, configurez le point de terminaison pour la déconnexion unique (SLO) :

   a. Sélectionnez **Ajouter SAML**.

   b. Sélectionnez **Type de point de terminaison** > **Déconnexion SAML**.

   c. Sélectionnez **Liaison** > **Redirection**.

   d. Dans le champ **URL de confiance**, saisissez l'URL utilisée pour la déconnexion unique (SLO) de ce nœud 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. Cependant, si vous saisissez une adresse IP ici, sachez que vous devez mettre à jour ou recréer cette approbation de partie de confiance si cette adresse IP change un jour.)

   a. Sélectionnez **OK**.

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

   a. Ajoutez le certificat personnalisé :

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

      > 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 récupérerez le nœud et vous devrez mettre à jour l'approbation de la partie de confiance.

   b. Sélectionnez **Appliquer**, puis **OK**.

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

10. Répétez ces étapes pour configurer une approbation de partie de confiance pour tous les nœuds d'administration de votre système StorageGRID .
11. Une fois que vous avez terminé, revenez à StorageGRID et testez toutes les approbations des parties de confiance pour confirmer qu'elles sont correctement configurées. Voir"Utiliser le mode sandbox" pour les instructions.

Créer des applications d'entreprise dans Azure AD

Vous utilisez Azure AD pour créer une application d'entreprise pour chaque nœud d'administration de votre système.

Avant de commencer

- Vous avez commencé à configurer l'authentification unique pour StorageGRID et vous avez sélectionné **Azure** comme type d'authentification unique.
- Le **mode Sandbox** est sélectionné sur la page d'authentification unique dans Grid Manager. Voir "Utiliser le mode sandbox" .
- Vous disposez du **nom de l'application d'entreprise** pour chaque nœud d'administration de votre système. Vous pouvez copier ces valeurs à partir du tableau des détails du nœud d'administration sur la page d'authentification unique StorageGRID .

> Vous devez créer une application d'entreprise pour chaque nœud d'administration de votre système StorageGRID . Disposer d'une application d'entreprise pour chaque nœud d'administration garantit que les utilisateurs peuvent se connecter et se déconnecter en toute sécurité de n'importe quel nœud d'administration.

- Vous avez de l'expérience dans la création d'applications d'entreprise dans Azure Active Directory.
- Vous disposez d'un compte Azure avec un abonnement actif.
- Vous disposez de l'un des rôles suivants dans le compte Azure : administrateur général, administrateur d'applications cloud, administrateur d'applications ou propriétaire du principal du service.

Accéder à Azure AD

Étapes

1. Connectez-vous à la "Portail Azure" .
2. Accéder à "Azure Active Directory" .
3. Sélectionner "Applications d'entreprise" .

Créez des applications d'entreprise et enregistrez la configuration SSO de StorageGRID

Pour enregistrer la configuration SSO pour Azure dans StorageGRID, vous devez utiliser Azure pour créer une application d'entreprise pour chaque nœud d'administration. Vous copierez les URL de métadonnées de fédération depuis Azure et les collerez dans les champs **URL de métadonnées de fédération** correspondants sur la page d'authentification unique StorageGRID .

Étapes

1. Répétez les étapes suivantes pour chaque nœud d'administration.
   a. Dans le volet Applications Azure Enterprise, sélectionnez **Nouvelle application**.
   b. Sélectionnez **Créer votre propre application**.
   c. Pour le nom, saisissez le **Nom de l'application d'entreprise** que vous avez copié à partir du tableau des détails du nœud d'administration sur la page d'authentification unique StorageGRID .
   d. Laissez le bouton radio **Intégrer toute autre application que vous ne trouvez pas dans la galerie (Hors galerie)** sélectionné.
   e. Sélectionnez **Créer**.
   f. Sélectionnez le lien **Commencer** dans le **2. Configurer l'authentification unique** ou sélectionner le lien **Authentification unique** dans la marge de gauche.
   g. Sélectionnez la case **SAML**.
   h. Copiez l'**URL des métadonnées de la fédération d'applications**, que vous pouvez trouver sous **Étape 3 Certificat de signature SAML**.

i. Accédez à la page d'authentification unique StorageGRID et collez l'URL dans le champ **URL des métadonnées de la fédération** qui correspond au **nom de l'application d'entreprise** que vous avez utilisé.

2. Après avoir collé une URL de métadonnées de fédération pour chaque nœud d'administration et apporté toutes les autres modifications nécessaires à la configuration SSO, sélectionnez **Enregistrer** sur la page d'authentification unique StorageGRID .

Téléchargez les métadonnées SAML pour chaque nœud d'administration

Une fois la configuration SSO enregistrée, vous pouvez télécharger un fichier de métadonnées SAML pour chaque nœud d'administration de votre système StorageGRID .

Étapes

1. Répétez ces étapes pour chaque nœud d'administration.
   a. Sign in à StorageGRID à partir du nœud d'administration.
   b. Sélectionnez **CONFIGURATION** > **Contrôle d'accès** > **Authentification unique**.
   c. Sélectionnez le bouton pour télécharger les métadonnées SAML pour ce nœud d'administration.
   d. Enregistrez le fichier que vous téléchargerez dans Azure AD.

Télécharger les métadonnées SAML vers chaque application d'entreprise

Après avoir téléchargé un fichier de métadonnées SAML pour chaque nœud d'administration StorageGRID , effectuez les étapes suivantes dans Azure AD :

Étapes

1. Revenez au portail Azure.
2. Répétez ces étapes pour chaque application d'entreprise :

   > Vous devrez peut-être actualiser la page Applications d'entreprise pour voir les applications que vous avez précédemment ajoutées dans la liste.

   a. Accédez à la page Propriétés de l'application d'entreprise.
   b. Définissez **Affectation requise** sur **Non** (sauf si vous souhaitez configurer les affectations séparément).
   c. Accédez à la page d'authentification unique.
   d. Terminez la configuration SAML.
   e. Sélectionnez le bouton **Télécharger le fichier de métadonnées** et sélectionnez le fichier de métadonnées SAML que vous avez téléchargé pour le nœud d'administration correspondant.
   f. Une fois le fichier chargé, sélectionnez **Enregistrer** puis sélectionnez **X** pour fermer le volet. Vous êtes redirigé vers la page Configurer l'authentification unique avec SAML.
3. Suivez les étapes dans"Utiliser le mode sandbox" pour tester chaque application.

Créer des connexions de fournisseur de services (SP) dans PingFederate

Vous utilisez PingFederate pour créer une connexion de fournisseur de services (SP) pour chaque nœud d'administration de votre système. Pour accélérer le processus, vous importerez les métadonnées SAML depuis StorageGRID.

Avant de commencer

- Vous avez configuré l'authentification unique pour StorageGRID et vous avez sélectionné **Ping Federate** comme type d'authentification unique.
- Le **mode Sandbox** est sélectionné sur la page d'authentification unique dans Grid Manager. Voir "Utiliser le mode sandbox" .
- Vous disposez de l'*ID de connexion SP * pour chaque nœud d'administration de votre système. Vous pouvez trouver ces valeurs dans le tableau détaillé des nœuds d'administration sur la page d'authentification unique StorageGRID .
- Vous avez téléchargé les **métadonnées SAML** pour chaque nœud d'administration de votre système.
- Vous avez de l'expérience dans la création de connexions SP dans PingFederate Server.
- Vous avez lehttps://docs.pingidentity.com/pingfederate/latest/administrators_reference_guide/pf_administrators_reference_guide.html["Guide de référence de l'administrateur"^] pour le serveur PingFederate. La documentation de PingFederate fournit des instructions et des explications détaillées étape par étape.
- Vous avez le"Autorisation d'administrateur" pour le serveur PingFederate.

À propos de cette tâche

Ces instructions résument comment configurer PingFederate Server version 10.3 en tant que fournisseur SSO pour StorageGRID. Si vous utilisez une autre version de PingFederate, vous devrez peut-être adapter ces instructions. Reportez-vous à la documentation du serveur PingFederate pour obtenir des instructions détaillées pour votre version.

Prérequis complets dans PingFederate

Avant de pouvoir créer les connexions SP que vous utiliserez pour StorageGRID, vous devez effectuer les tâches préalables dans PingFederate. Vous utiliserez les informations de ces prérequis lorsque vous configurerez les connexions SP .

Créer un magasin de données

Si vous ne l'avez pas déjà fait, créez un magasin de données pour connecter PingFederate au serveur LDAP AD FS. Utilisez les valeurs que vous avez utilisées lorsque"configuration de la fédération d'identité" dans StorageGRID.

- **Type** : Répertoire (LDAP)
- **Type LDAP** : Active Directory
- **Nom de l'attribut binaire** : saisissez **objectGUID** dans l'onglet Attributs binaires LDAP exactement comme indiqué.

Créer un validateur d'informations d'identification de mot de passe

Si vous ne l'avez pas déjà fait, créez un validateur d'informations d'identification de mot de passe.

- **Type** : Validateur d'informations d'identification de mot de passe de nom d'utilisateur LDAP
- **Magasin de données** : sélectionnez le magasin de données que vous avez créé.
- **Base de recherche** : saisissez les informations de LDAP (par exemple, DC=saml,DC=sgws).
- **Filtre de recherche** : sAMAccountName=${username}
- **Portée** : Sous-arbre

Créer une instance d'adaptateur IdP

Si vous ne l'avez pas déjà fait, créez une instance d'adaptateur IdP.

Étapes

1. Accédez à **Authentification** > **Intégration** > **Adaptateurs IdP**.
2. Sélectionnez **Créer une nouvelle instance**.
3. Dans l'onglet Type, sélectionnez **Adaptateur IdP de formulaire HTML**.
4. Dans l'onglet Adaptateur IdP, sélectionnez **Ajouter une nouvelle ligne à « Validateurs d'informations d'identification »**.
5. Sélectionnez levalidateur d'informations d'identification de mot de passe tu as créé.
6. Dans l'onglet Attributs de l'adaptateur, sélectionnez l'attribut **username** pour **Pseudonyme**.
7. Sélectionnez **Enregistrer**.

Créer ou importer un certificat de signature

Si vous ne l'avez pas déjà fait, créez ou importez le certificat de signature.

Étapes

1. Accédez à **Sécurité** > **Clés et certificats de signature et de déchiffrement**.
2. Créez ou importez le certificat de signature.

Créer une connexion SP dans PingFederate

Lorsque vous créez une connexion SP dans PingFederate, vous importez les métadonnées SAML que vous avez téléchargées à partir de StorageGRID pour le nœud d'administration. Le fichier de métadonnées contient de nombreuses valeurs spécifiques dont vous avez besoin.

> Vous devez créer une connexion SP pour chaque nœud d'administration de votre système StorageGRID , afin que les utilisateurs puissent se connecter et se déconnecter en toute sécurité de n'importe quel nœud. Utilisez ces instructions pour créer la première connexion SP . Ensuite, allez àCréer des connexions SP supplémentaires pour créer toutes les connexions supplémentaires dont vous avez besoin.

Choisissez le type de connexion SP

Étapes

1. Accédez à **Applications** > **Intégration** > *Connexions SP *.
2. Sélectionnez **Créer une connexion**.
3. Sélectionnez **Ne pas utiliser de modèle pour cette connexion**.
4. Sélectionnez **Profils SSO du navigateur** et **SAML 2.0** comme protocole.

Importer les métadonnées SP

Étapes

1. Dans l'onglet Importer des métadonnées, sélectionnez **Fichier**.
2. Choisissez le fichier de métadonnées SAML que vous avez téléchargé à partir de la page d'authentification unique StorageGRID pour le nœud d'administration.

3. Consultez le résumé des métadonnées et les informations fournies dans l'onglet Informations générales.

   L'ID d'entité du partenaire et le nom de connexion sont définis sur l'ID de connexion StorageGRID SP . (par exemple, 10.96.105.200-DC1-ADM1-105-200). L'URL de base est l'IP du nœud d'administration StorageGRID .

4. Sélectionnez **Suivant**.

Configurer l'authentification unique du navigateur IdP

Étapes

1. Dans l'onglet SSO du navigateur, sélectionnez **Configurer SSO du navigateur**.
2. Dans l'onglet Profils SAML, sélectionnez les options * SP-initiated SSO*, * SP-initial SLO*, **IdP-initiated SSO** et **IdP-initiated SLO**.
3. Sélectionnez **Suivant**.
4. Dans l'onglet Durée de vie de l'assertion, n'apportez aucune modification.
5. Dans l'onglet Création d'assertion, sélectionnez **Configurer la création d'assertion**.
   a. Dans l'onglet Mappage d'identité, sélectionnez **Standard**.
   b. Dans l'onglet Contrat d'attribut, utilisez **SAML_SUBJECT** comme contrat d'attribut et le format de nom non spécifié qui a été importé.
6. Pour prolonger le contrat, sélectionnez **Supprimer** pour supprimer le `urn:oid` , qui n'est pas utilisé.

Instance d'adaptateur de carte

Étapes

1. Dans l'onglet Mappage de la source d'authentification, sélectionnez **Mapper une nouvelle instance d'adaptateur**.
2. Dans l'onglet Instance de l'adaptateur, sélectionnez l'instance d'adaptateur tu as créé.
3. Dans l'onglet Méthode de mappage, sélectionnez **Récupérer des attributs supplémentaires à partir d'un magasin de données**.
4. Dans l'onglet Source d'attribut et recherche d'utilisateur, sélectionnez **Ajouter une source d'attribut**.
5. Dans l'onglet Magasin de données, fournissez une description et sélectionnez l'optionmagasin de données tu as ajouté.
6. Dans l'onglet Recherche d'annuaire LDAP :
   - Saisissez le **DN de base**, qui doit correspondre exactement à la valeur que vous avez saisie dans StorageGRID pour le serveur LDAP.
   - Pour la portée de la recherche, sélectionnez **Sous-arbre**.
   - Pour la classe d'objet racine, recherchez et ajoutez l'un de ces attributs : **objectGUID** ou **userPrincipalName**.
7. Dans l'onglet Types de codage d'attribut binaire LDAP, sélectionnez **Base64** pour l'attribut **objectGUID**.
8. Dans l'onglet Filtre LDAP, saisissez **sAMAccountName=${username}**.
9. Dans l'onglet Exécution du contrat d'attribut, sélectionnez **LDAP (attribut)** dans la liste déroulante Source et sélectionnez **objectGUID** ou **userPrincipalName** dans la liste déroulante Valeur.
10. Vérifiez puis enregistrez la source de l'attribut.

11. Dans l'onglet Source d'attribut Failsave, sélectionnez **Annuler la transaction SSO**.
12. Consultez le résumé et sélectionnez **Terminé**.
13. Sélectionnez **Terminé**.

Configurer les paramètres du protocole

Étapes

1. Dans l'onglet * Connexion SP * > * SSO du navigateur* > * Paramètres du protocole*, sélectionnez * Configurer les paramètres du protocole*.
2. Dans l'onglet URL du service consommateur d'assertions, acceptez les valeurs par défaut, qui ont été importées à partir des métadonnées SAML StorageGRID (**POST** pour la liaison et `/api/saml-response` pour l'URL du point de terminaison).
3. Dans l'onglet URL du service SLO, acceptez les valeurs par défaut, qui ont été importées à partir des métadonnées SAML StorageGRID (**REDIRECT** pour la liaison et `/api/saml-logout` pour l'URL du point de terminaison.
4. Dans l'onglet Liaisons SAML autorisées, décochez **ARTIFACT** et **SOAP**. Seuls **POST** et **REDIRECT** sont obligatoires.
5. Dans l'onglet Politique de signature, laissez les cases à cocher **Exiger que les demandes d'authentification soient signées** et **Toujours signer l'assertion** sélectionnées.
6. Dans l'onglet Politique de chiffrement, sélectionnez **Aucun**.
7. Consultez le résumé et sélectionnez **Terminé** pour enregistrer les paramètres du protocole.
8. Consultez le résumé et sélectionnez **Terminé** pour enregistrer les paramètres SSO du navigateur.

Configurer les informations d'identification

Étapes

1. Dans l'onglet Connexion SP , sélectionnez **Informations d'identification**.
2. Dans l'onglet Informations d'identification, sélectionnez **Configurer les informations d'identification**.
3. Sélectionnez lecertificat de signature vous avez créé ou importé.
4. Sélectionnez **Suivant** pour accéder à **Gérer les paramètres de vérification de signature**.
   a. Dans l'onglet Modèle de confiance, sélectionnez **Non ancré**.
   b. Dans l'onglet Certificat de vérification de signature, vérifiez les informations du certificat de signature, qui ont été importées à partir des métadonnées SAML StorageGRID .
5. Consultez les écrans récapitulatifs et sélectionnez **Enregistrer** pour enregistrer la connexion SP .

Créer des connexions SP supplémentaires

Vous pouvez copier la première connexion SP pour créer les connexions SP dont vous avez besoin pour chaque nœud d'administration de votre grille. Vous téléchargez de nouvelles métadonnées pour chaque copie.

> Les connexions SP pour différents nœuds d'administration utilisent des paramètres identiques, à l'exception de l'ID d'entité du partenaire, de l'URL de base, de l'ID de connexion, du nom de connexion, de la vérification de la signature et de l'URL de réponse SLO.

Étapes

1. Sélectionnez **Action** > **Copier** pour créer une copie de la connexion SP initiale pour chaque nœud

d'administration supplémentaire.

2. Saisissez l'ID de connexion et le nom de connexion pour la copie, puis sélectionnez **Enregistrer**.
3. Choisissez le fichier de métadonnées correspondant au nœud d'administration :
   a. Sélectionnez **Action** > **Mettre à jour avec les métadonnées**.
   b. Sélectionnez **Choisir un fichier** et téléchargez les métadonnées.
   c. Sélectionnez **Suivant**.
   d. Sélectionnez **Enregistrer**.
4. Résoudre l'erreur due à l'attribut inutilisé :
   a. Sélectionnez la nouvelle connexion.
   b. Sélectionnez **Configurer l'authentification unique du navigateur > Configurer la création d'assertions > Contrat d'attribut**.
   c. Supprimez l'entrée pour **urn:oid**.
   d. Sélectionnez **Enregistrer**.

Désactiver l'authentification 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 d'identité.

Avant de commencer

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

Étapes

1. Sélectionnez **CONFIGURATION** > **Contrôle d'accès** > **Authentification unique**.

   La page d'authentification unique s'affiche.

2. Sélectionnez l'option **Désactivé**.
3. Sélectionnez **Enregistrer**.

   Un message d'avertissement apparaît indiquant que les utilisateurs locaux pourront désormais se connecter.

4. Sélectionnez **OK**.

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

Désactiver et réactiver temporairement l'authentification unique pour un nœud d'administration

Vous ne pourrez peut-être pas vous connecter au Grid Manager si le système d'authentification unique (SSO) tombe en panne. Dans ce cas, vous pouvez désactiver et réactiver temporairement SSO pour un nœud d'administration. Pour désactiver puis

réactiver SSO, vous devez accéder à l'interpréteur de commandes du nœud.

Avant de commencer

- Tu as"autorisations d'accès spécifiques" .
- Vous avez le `Passwords.txt` déposer.
- Vous connaissez le mot de passe de l'utilisateur root local.

À propos de cette tâche

Après avoir désactivé SSO pour un nœud d'administration, vous pouvez vous connecter au gestionnaire de grille en tant qu'utilisateur root local. Pour sécuriser votre système StorageGRID , vous devez utiliser l'interpréteur de commandes 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 des autres nœuds d'administration de la grille. La case à cocher **Activer SSO** sur la page Authentification unique dans le Gestionnaire de grille reste sélectionnée et tous les paramètres SSO existants sont conservés, sauf si vous les mettez à jour.

Étapes

1. Connectez-vous à un nœud d'administration :
   a. Entrez la commande suivante : `ssh admin@Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
   c. Entrez la commande suivante pour passer en root : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

   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 SSO.

   Un message indique que l'authentification unique est désactivée sur le nœud.
4. À partir d'un navigateur Web, accédez au gestionnaire de grille sur le même nœud d'administration.

   La page de connexion de Grid Manager s'affiche désormais car SSO a été désactivé.
5. Sign in avec le nom d'utilisateur root et le mot de passe de l'utilisateur root local.
6. Si vous avez désactivé temporairement SSO parce que vous deviez corriger la configuration SSO :
   a. Sélectionnez **CONFIGURATION** > **Contrôle d'accès** > **Authentification unique**.
   b. Modifiez les paramètres SSO incorrects ou obsolètes.
   c. Sélectionnez **Enregistrer**.

   La sélection de **Enregistrer** sur la page d'authentification unique réactive automatiquement l'authentification unique pour l'ensemble de la grille.

7. Si vous avez désactivé temporairement SSO parce que vous aviez besoin d'accéder au Grid Manager pour une autre raison :

   a. Effectuez la ou les tâches que vous devez effectuer.

   b. Sélectionnez **Déconnexion** et fermez le gestionnaire de grille.

   c. Réactiver SSO sur le nœud d'administration. Vous pouvez effectuer l'une des étapes 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 SSO.

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

   ◦ Redémarrer le nœud de grille : `reboot`

8. À partir d'un navigateur Web, accédez au gestionnaire de grille à partir du même nœud d'administration.
9. Confirmez que la page de Sign in StorageGRID s'affiche et que vous devez saisir vos informations d'identification SSO pour accéder au Grid Manager.

Informations sur le copyright

Informations sur les marques commerciales