Gérer les groupes et les utilisateurs

StorageGRID software

NetApp
December 03, 2025

Sommaire

Gérer les groupes et les utilisateurs . . . 1
- Utiliser la fédération d'identité . . . 1
  - Configurer la fédération d'identité pour Tenant Manager . . . 1
  - Forcer la synchronisation avec la source d'identité . . . 5
  - Désactiver la fédération d'identité . . . 5
  - Directives pour la configuration du serveur OpenLDAP . . . 5
- Gérer les groupes de locataires . . . 6
  - Créer des groupes pour un locataire S3 . . . 6
  - Créer des groupes pour un locataire Swift . . . 9
  - Autorisations de gestion des locataires . . . 11
  - Gérer les groupes . . . 13
- Gérer les utilisateurs locaux . . . 16
  - Créer un utilisateur local . . . 17
  - Afficher ou modifier l'utilisateur local . . . 18
  - Utilisateur local en double . . . 20
    - Réessayer le clonage de l'utilisateur . . . 20
  - Supprimer un ou plusieurs utilisateurs locaux . . . 20

Gérer les groupes et les utilisateurs

Utiliser la fédération d’identité

L’utilisation de la fédération d’identité accélère la configuration des groupes de locataires et des utilisateurs et permet aux utilisateurs locataires de se connecter au compte locataire à l’aide d’informations d’identification familières.

Configurer la fédération d’identité pour Tenant Manager

Vous pouvez configurer la fédération d’identité pour Tenant Manager si vous souhaitez que les groupes de locataires 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

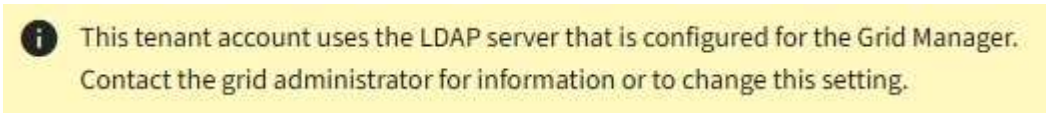
- Vous êtes connecté au Tenant Manager à l’aide d’un"navigateur Web pris en charge" .
- Vous appartenez à un groupe d’utilisateurs qui possède le"Autorisation d’accès root" .
- Vous utilisez Active Directory, Azure AD, OpenLDAP ou Oracle Directory Server comme fournisseur d’identité.

  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 du serveur OpenLDAP .
- Si vous prévoyez d’utiliser Transport Layer Security (TLS) pour les communications avec le serveur LDAP, le fournisseur d’identité doit utiliser TLS 1.2 ou 1.3. Voir "Chiffres pris en charge pour les connexions TLS sortantes" .

À propos de cette tâche

La possibilité de configurer un service de fédération d’identité pour votre locataire dépend de la façon dont votre compte de locataire a été configuré. Votre locataire peut partager le service de fédération d’identité qui a été configuré pour Grid Manager. Si vous voyez ce message lorsque vous accédez à la page Fédération d’identité, vous ne pouvez pas configurer une source d’identité fédérée distincte pour ce locataire.

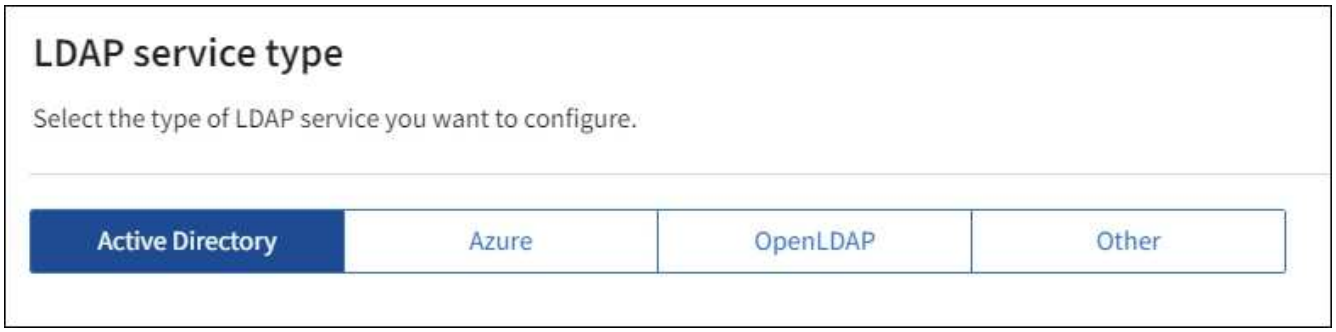


Entrer la configuration

Lorsque vous configurez l’identification de la fédération, vous fournissez les valeurs dont StorageGRID a besoin pour se connecter à un service LDAP.

Étapes

1. Sélectionnez **GESTION DES 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.

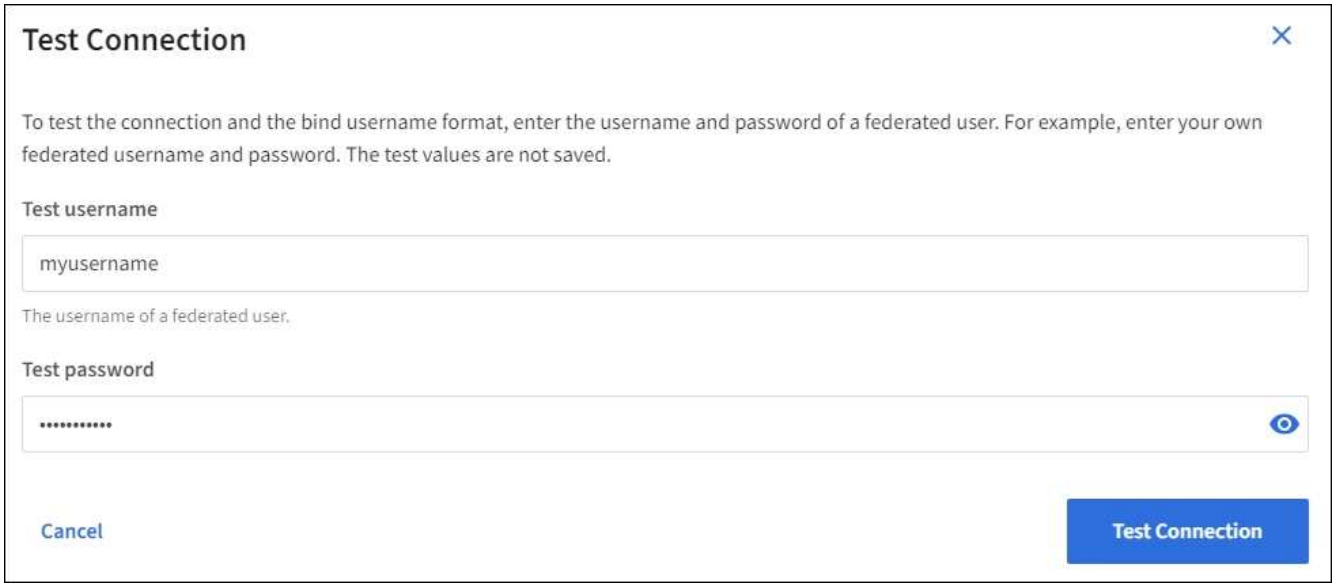
Tester la connexion et enregistrer la configuration

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 du 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 de locataires

Créer des groupes pour un locataire S3

Vous pouvez gérer les autorisations des groupes d'utilisateurs S3 en important des groupes fédérés ou en créant des groupes locaux.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous appartenez à un groupe d'utilisateurs qui possède le"Autorisation d'accès root" .
- Si vous envisagez d'importer un groupe fédéré, vous devez"fédération d'identité configurée" , et le groupe fédéré existe déjà dans la source d'identité configurée.
- Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille**, vous avez examiné le flux de travail et les considérations pour"clonage de groupes de locataires et d'utilisateurs" , et vous êtes connecté à la grille source du locataire.

Accéder à l'assistant de création de groupe

Dans un premier temps, accédez à l'assistant de création de groupe.

Étapes

1. Sélectionnez **GESTION DES ACCÈS** > **Groupes**.
2. Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille**, confirmez qu'une bannière bleue apparaît, indiquant que les nouveaux groupes créés sur cette grille seront clonés sur le même locataire sur l'autre grille de la connexion. Si cette bannière n'apparaît pas, vous êtes peut-être connecté à la grille de destination du locataire.

3. Sélectionnez **Créer un groupe**.

Choisissez un type de groupe

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

Étapes

1. Sélectionnez l'onglet **Groupe local** pour créer un groupe local ou sélectionnez l'onglet **Groupe fédéré** pour importer un groupe à partir de la source d'identité précédemment configurée.

   Si l'authentification unique (SSO) est activée pour votre système StorageGRID , les utilisateurs appartenant à des groupes locaux ne pourront pas se connecter au gestionnaire de locataires, bien qu'ils puissent utiliser des applications clientes pour gérer les ressources du locataire, en fonction des autorisations de groupe.

2. Entrez le nom du groupe.
   - **Groupe local** : saisissez un nom d'affichage et un nom unique. Vous pouvez modifier le nom d'affichage ultérieurement.

     Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille**, une erreur de clonage se produira si le même **Nom unique** existe déjà pour le locataire sur la grille de destination.

   - **Groupe fédéré** : Saisissez le nom unique. Pour Active Directory, le nom unique est le nom associé au `sAMAccountName` attribut. Pour OpenLDAP, le nom unique est le nom associé au `uid` attribut.
3. Sélectionnez **Continuer**.

Gérer les autorisations de groupe

Les autorisations de groupe contrôlent les tâches que les utilisateurs peuvent effectuer dans Tenant Manager et l'API Tenant Management.

Étapes

1. Pour le **Mode d'accès**, sélectionnez l'une des options suivantes :
   - **Lecture-écriture** (par défaut) : les utilisateurs peuvent se connecter à Tenant Manager et gérer la configuration du locataire.
   - **Lecture seule** : les utilisateurs peuvent uniquement afficher les paramètres et les fonctionnalités. Ils ne peuvent apporter aucune modification ni effectuer aucune opération dans l'API Tenant Manager ou Tenant 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 une ou plusieurs autorisations pour ce groupe.

   Voir "Autorisations de gestion des locataires" .

3. Sélectionnez **Continuer**.

Définir la stratégie de groupe S3

La stratégie de groupe détermine les autorisations d'accès S3 dont disposeront les utilisateurs.

Étapes

1. Sélectionnez la politique que vous souhaitez utiliser pour ce groupe.

Politique de groupe	Description
Pas d'accès S3	Défaut. Les utilisateurs de ce groupe n'ont pas accès aux ressources S3, sauf si l'accès est accordé avec une stratégie de compartiment. Si vous sélectionnez cette option, seul l'utilisateur root aura accès aux ressources S3 par défaut.
Accès en lecture seule	Les utilisateurs de ce groupe ont un accès en lecture seule aux ressources S3. Par exemple, les utilisateurs de ce groupe peuvent répertorier les objets et lire les données d'objet, les métadonnées et les balises. Lorsque vous sélectionnez cette option, la chaîne JSON d'une stratégie de groupe en lecture seule apparaît dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
Accès complet	Les utilisateurs de ce groupe ont un accès complet aux ressources S3, y compris les buckets. Lorsque vous sélectionnez cette option, la chaîne JSON d'une stratégie de groupe à accès complet apparaît dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.

Politique de groupe	Description
Atténuation des ransomwares	Cet exemple de politique s'applique à tous les compartiments de ce locataire. Les utilisateurs de ce groupe peuvent effectuer des actions courantes, mais ne peuvent pas supprimer définitivement les objets des buckets pour lesquels le contrôle de version des objets est activé. Les utilisateurs de Tenant Manager qui disposent de l'autorisation **Gérer tous les compartiments** peuvent remplacer cette stratégie de groupe. Limitez l'autorisation Gérer tous les compartiments aux utilisateurs de confiance et utilisez l'authentification multifacteur (MFA) lorsqu'elle est disponible.
Coutume	Les utilisateurs du groupe bénéficient des autorisations que vous spécifiez dans la zone de texte.

2. Si vous avez sélectionné **Personnalisé**, saisissez la stratégie de groupe. Chaque stratégie de groupe a une limite de taille de 5 120 octets. Vous devez saisir une chaîne formatée JSON valide.

   Pour des informations détaillées sur les stratégies de groupe, y compris la syntaxe du langage et des exemples, voir"Exemples de stratégies de groupe" .

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)

Vous pouvez enregistrer le groupe sans ajouter d'utilisateurs, ou vous pouvez éventuellement ajouter des utilisateurs locaux déjà existants.

> Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille**, tous les utilisateurs que vous sélectionnez lorsque vous créez un groupe local sur la grille source ne sont pas inclus lorsque le groupe est cloné sur la grille de destination. Pour cette raison, ne sélectionnez pas d'utilisateurs lorsque vous créez le groupe. Sélectionnez plutôt le groupe lorsque vous créez les utilisateurs.

Étapes

1. Vous pouvez également sélectionner un ou plusieurs utilisateurs locaux pour ce groupe.
2. Sélectionnez **Créer un groupe** et **Terminer**.

   Le groupe que vous avez créé apparaît dans la liste des groupes.

   Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille** et que vous êtes sur la grille source du locataire, le nouveau groupe est cloné sur la grille de destination du locataire. **Succès** apparaît comme **Statut de clonage** dans la section Présentation de la page de détails du groupe.

Créer des groupes pour un locataire Swift

Vous pouvez gérer les autorisations d'accès pour un compte locataire Swift en important des groupes fédérés ou en créant des groupes locaux. Au moins un groupe doit disposer

de l'autorisation Administrateur Swift, qui est requise pour gérer les conteneurs et les objets d'un compte locataire Swift.

> La prise en charge des applications clientes Swift est obsolète et sera supprimée dans une prochaine version.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous appartenez à un groupe d'utilisateurs qui possède le"Autorisation d'accès root" .
- Si vous envisagez d'importer un groupe fédéré, vous devez"fédération d'identité configurée" , et le groupe fédéré existe déjà dans la source d'identité configurée.

Accéder à l'assistant de création de groupe

Étapes

Dans un premier temps, accédez à l'assistant de création de groupe.

1. Sélectionnez **GESTION DES ACCÈS** > **Groupes**.
2. Sélectionnez **Créer un groupe**.

Choisissez un type de groupe

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

Étapes

1. Sélectionnez l'onglet **Groupe local** pour créer un groupe local ou sélectionnez l'onglet **Groupe fédéré** pour importer un groupe à partir de la source d'identité précédemment configurée.

   Si l'authentification unique (SSO) est activée pour votre système StorageGRID , les utilisateurs appartenant à des groupes locaux ne pourront pas se connecter au gestionnaire de locataires, bien qu'ils puissent utiliser des applications clientes pour gérer les ressources du locataire, en fonction des autorisations de groupe.

2. Entrez le nom du groupe.
   - **Groupe local** : saisissez un nom d'affichage et un nom unique. Vous pouvez modifier le nom d'affichage ultérieurement.
   - **Groupe fédéré** : Saisissez le nom unique. Pour Active Directory, le nom unique est le nom associé au `sAMAccountName` attribut. Pour OpenLDAP, le nom unique est le nom associé au `uid` attribut.
3. Sélectionnez **Continuer**.

Gérer les autorisations de groupe

Les autorisations de groupe contrôlent les tâches que les utilisateurs peuvent effectuer dans Tenant Manager et l'API Tenant Management.

Étapes

1. Pour le **Mode d'accès**, sélectionnez l'une des options suivantes :
   - **Lecture-écriture** (par défaut) : les utilisateurs peuvent se connecter à Tenant Manager et gérer la configuration du locataire.

- **Lecture seule** : les utilisateurs peuvent uniquement afficher les paramètres et les fonctionnalités. Ils ne peuvent apporter aucune modification ni effectuer aucune opération dans l'API Tenant Manager ou Tenant 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. Cochez la case **Accès root** si les utilisateurs du groupe doivent se connecter au gestionnaire de locataires ou à l'API de gestion des locataires.
3. Sélectionnez **Continuer**.

Définir la politique de groupe Swift

Les utilisateurs de Swift ont besoin d'une autorisation d'administrateur pour s'authentifier dans l'API REST Swift afin de créer des conteneurs et d'ingérer des objets.

1. Cochez la case **Administrateur Swift** si les utilisateurs du groupe doivent utiliser l'API REST Swift pour gérer les conteneurs et les objets.
2. 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)

Vous pouvez enregistrer le groupe sans ajouter d'utilisateurs, ou vous pouvez éventuellement ajouter des utilisateurs locaux déjà existants.

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 ajouter ce groupe à l'utilisateur sur la page Utilisateurs. Voir "Gérer les utilisateurs locaux" .

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

   Le groupe que vous avez créé apparaît dans la liste des groupes.

Autorisations de gestion des locataires

Avant de créer un groupe de locataires, réfléchissez aux autorisations que vous souhaitez attribuer à ce groupe. Les autorisations de gestion des locataires déterminent les tâches que les utilisateurs peuvent effectuer à l'aide du gestionnaire de locataires ou de l'API de gestion des locataires. Un utilisateur peut appartenir à un ou plusieurs groupes. Les autorisations sont cumulatives si un utilisateur appartient à plusieurs groupes.

Pour se connecter au gestionnaire de locataires ou utiliser l'API de gestion des locataires, les utilisateurs doivent appartenir à un groupe disposant d'au moins une autorisation. Tous les utilisateurs qui peuvent se connecter peuvent effectuer les tâches suivantes :

- Afficher le tableau de bord
- Changer leur propre mot de passe (pour les utilisateurs locaux)

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.

Vous pouvez attribuer les autorisations suivantes à un groupe. Notez que les locataires S3 et les locataires Swift ont des autorisations de groupe différentes.

Autorisation	Description	Détails
Accès root	Fournit un accès complet au gestionnaire de locataires et à l'API de gestion des locataires.	Les utilisateurs Swift doivent disposer de l'autorisation d'accès root pour se connecter au compte locataire.
Administrateur	Locataires rapides seulement. Fournit un accès complet aux conteneurs et objets Swift pour ce compte locataire	Les utilisateurs Swift doivent disposer de l'autorisation d'administrateur Swift pour effectuer des opérations avec l'API REST Swift.
Gérez vos propres identifiants S3	Permet aux utilisateurs de créer et de supprimer leurs propres clés d'accès S3.	Les utilisateurs qui ne disposent pas de cette autorisation ne voient pas l'option de menu **STOCKAGE (S3)** > **Mes clés d'accès S3**.
Voir tous les seaux	• Locataires S3 * : permet aux utilisateurs d'afficher tous les buckets et configurations de buckets. • Locataires Swift * : permet aux utilisateurs Swift d'afficher tous les conteneurs et configurations de conteneurs à l'aide de l'API de gestion des locataires.	Les utilisateurs qui ne disposent pas de l'autorisation Afficher tous les buckets ou Gérer tous les buckets ne voient pas l'option de menu **Buckets**. Cette autorisation est remplacée par l'autorisation Gérer tous les buckets. Cela n'affecte pas les stratégies de groupe ou de compartiment S3 utilisées par les clients S3 ou la console S3. Vous ne pouvez attribuer cette autorisation qu'aux groupes Swift à partir de l'API de gestion des locataires. Vous ne pouvez pas attribuer cette autorisation aux groupes Swift à l'aide du gestionnaire de locataires.

Autorisation	Description	Détails
Gérer tous les compartiments	• Locataires S3 * : permet aux utilisateurs d'utiliser le gestionnaire de locataires et l'API de gestion des locataires pour créer et supprimer des compartiments S3 et pour gérer les paramètres de tous les compartiments S3 du compte de locataire, quels que soient les compartiments S3 ou les stratégies de groupe. • Locataires Swift * : permet aux utilisateurs Swift de contrôler la cohérence des conteneurs Swift à l'aide de l'API de gestion des locataires.	Les utilisateurs qui ne disposent pas de l'autorisation Afficher tous les buckets ou Gérer tous les buckets ne voient pas l'option de menu **Buckets**. Cette autorisation remplace l'autorisation Afficher tous les buckets. Cela n'affecte pas les stratégies de groupe ou de compartiment S3 utilisées par les clients S3 ou la console S3. Vous ne pouvez attribuer cette autorisation qu'aux groupes Swift à partir de l'API de gestion des locataires. Vous ne pouvez pas attribuer cette autorisation aux groupes Swift à l'aide du gestionnaire de locataires.
Gérer les points de terminaison	Permet aux utilisateurs d'utiliser Tenant Manager ou l'API Tenant Management pour créer ou modifier des points de terminaison de service de plateforme, qui sont utilisés comme destination pour les services de plateforme StorageGRID .	Les utilisateurs qui ne disposent pas de cette autorisation ne voient pas l'option de menu **Points de terminaison des services de plateforme**.
Utiliser l'onglet Console S3	Associée à l'autorisation Afficher tous les buckets ou Gérer tous les buckets, cette option permet aux utilisateurs d'afficher et de gérer les objets à partir de l'onglet Console S3 sur la page de détails d'un bucket.	

Gérer les groupes

Gérez vos groupes de locataires selon vos besoins pour afficher, modifier ou dupliquer un groupe, et bien plus encore.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous appartenez à un groupe d'utilisateurs qui possède le"Autorisation d'accès root" .

Afficher ou modifier le groupe

Vous pouvez afficher et modifier les informations de base et les détails de chaque groupe.

Étapes

1. Sélectionnez **GESTION DES ACCÈS** > **Groupes**.
2. Consultez les informations fournies sur la page Groupes, qui répertorie les informations de base pour tous les groupes locaux et fédérés pour ce compte locataire.

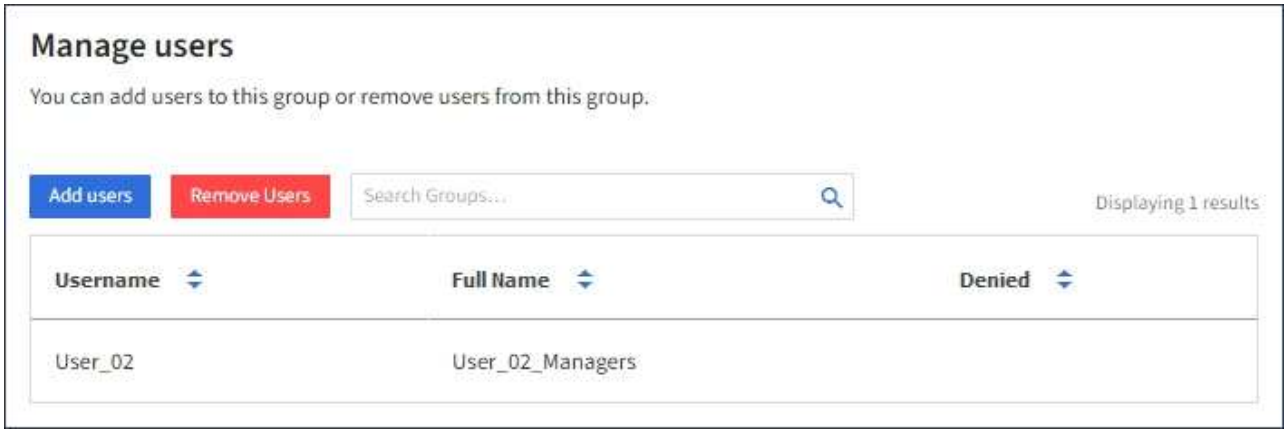
   Si le compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille** et que vous

visualisez les groupes sur la grille source du locataire :

- Un message de bannière indique que si vous modifiez ou supprimez un groupe, vos modifications ne seront pas synchronisées avec l'autre grille.
- Si nécessaire, un message de bannière indique si les groupes n'ont pas été clonés sur le locataire sur la grille de destination. Tu peuxréessayer un clonage de groupe ça a échoué.

3. Si vous souhaitez modifier le nom du groupe :
   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**.
4. Si vous souhaitez afficher plus de détails ou apporter des modifications supplémentaires, effectuez l'une des opérations suivantes :
   - Sélectionnez le nom du groupe.
   - Cochez la case correspondant au groupe, puis sélectionnez **Actions** > **Afficher les détails du groupe**.
5. Consultez la section Présentation, qui affiche les informations suivantes pour chaque groupe :
   - Nom d'affichage
   - Nom unique
   - Type
   - Mode d'accès
   - Autorisations
   - Politique S3
   - Nombre d'utilisateurs dans ce groupe
   - Champs supplémentaires si le compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille** et que vous visualisez le groupe sur la grille source du locataire :
     - Statut du clonage, soit **Succès** soit **Échec**
     - Une bannière bleue indiquant que si vous modifiez ou supprimez ce groupe, vos modifications ne seront pas synchronisées avec l'autre grille.
6. Modifiez les paramètres du groupe selon vos besoins. Voir"Créer des groupes pour un locataire S3" et"Créer des groupes pour un locataire Swift" pour plus de détails sur ce qu'il faut saisir.
   a. Dans la section Aperçu, modifiez le nom d'affichage en sélectionnant le nom ou l'icône de modification .
   b. Dans l'onglet **Autorisations de groupe**, mettez à jour les autorisations et sélectionnez **Enregistrer les modifications**.
   c. Dans l'onglet **Stratégie de groupe**, apportez les modifications nécessaires et sélectionnez **Enregistrer les modifications**.
      - Si vous modifiez un groupe S3, sélectionnez éventuellement une autre stratégie de groupe S3 ou saisissez la chaîne JSON d'une stratégie personnalisée, selon vos besoins.
      - Si vous modifiez un groupe Swift, cochez ou décochez éventuellement la case **Administrateur Swift**.
7. Pour ajouter un ou plusieurs utilisateurs locaux existants au groupe :

a. Sélectionnez l'onglet Utilisateurs.



b. Sélectionnez **Ajouter des utilisateurs**.

c. Sélectionnez les utilisateurs existants que vous souhaitez ajouter, puis sélectionnez **Ajouter des utilisateurs**.

Un message de réussite apparaît dans le coin supérieur droit.

8. Pour supprimer les utilisateurs locaux du groupe :

a. Sélectionnez l'onglet Utilisateurs.

b. Sélectionnez **Supprimer les utilisateurs**.

c. Sélectionnez les utilisateurs que vous souhaitez supprimer, puis sélectionnez **Supprimer les utilisateurs**.

Un message de réussite apparaît dans le coin supérieur droit.

9. Confirmez que vous avez sélectionné **Enregistrer les modifications** pour chaque section que vous avez modifiée.

Groupe en double

Vous pouvez dupliquer un groupe existant pour créer de nouveaux groupes plus rapidement.

> Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille** et que vous dupliquez un groupe à partir de la grille source du locataire, le groupe dupliqué sera cloné sur la grille de destination du locataire.

Étapes

1. Sélectionnez **GESTION DES ACCÈS** > **Groupes**.
2. Cochez la case correspondant au groupe que vous souhaitez dupliquer.
3. Sélectionnez **Actions** > **Dupliquer le groupe**.
4. Voir"Créer des groupes pour un locataire S3" ou"Créer des groupes pour un locataire Swift" pour plus de détails sur ce qu'il faut saisir.
5. Sélectionnez **Créer un groupe**.

Réessayer le clonage du groupe

Pour réessayer un clonage qui a échoué :

1. Sélectionnez chaque groupe qui indique *(Échec du clonage)* sous le nom du groupe.
2. Sélectionnez **Actions** > **Cloner les groupes**.
3. Affichez l'état de l'opération de clonage à partir de la page de détails de chaque groupe que vous clonez.

Pour plus d'informations, voir"Cloner des groupes de locataires et des utilisateurs" .

Supprimer un ou plusieurs groupes

Vous pouvez supprimer un ou plusieurs groupes. Tous les utilisateurs appartenant uniquement à un groupe supprimé ne pourront plus se connecter au gestionnaire de locataires ni utiliser le compte de locataire.

> Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille** et que vous supprimez un groupe, StorageGRID ne supprimera pas le groupe correspondant sur l'autre grille. Si vous devez conserver ces informations synchronisées, vous devez supprimer le même groupe des deux grilles.

Étapes

1. Sélectionnez **GESTION DES ACCÈS** > **Groupes**.
2. Cochez la case correspondant à chaque groupe que vous souhaitez supprimer.
3. Sélectionnez **Actions** > **Supprimer le groupe** ou **Actions** > **Supprimer les groupes**.

   Une boîte de dialogue de confirmation apparaît.
4. Sélectionnez **Supprimer le groupe** ou **Supprimer les groupes**.

Gérer les utilisateurs locaux

Vous pouvez créer des utilisateurs locaux et les affecter à des groupes locaux pour déterminer les fonctionnalités auxquelles ces utilisateurs peuvent accéder. Le gestionnaire de locataires comprend un utilisateur local prédéfini, nommé « root ». Bien que vous puissiez ajouter et supprimer des utilisateurs locaux, vous ne pouvez pas supprimer l'utilisateur root.

> Si l'authentification unique (SSO) est activée pour votre système StorageGRID , les utilisateurs locaux ne pourront pas se connecter au gestionnaire de locataires ou à l'API de gestion des locataires, bien qu'ils puissent utiliser des applications clientes pour accéder aux ressources du locataire, en fonction des autorisations de groupe.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous appartenez à un groupe d'utilisateurs qui possède le"Autorisation d'accès root" .
- Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille**, vous avez examiné le flux de travail et les considérations pour"clonage de groupes de locataires et d'utilisateurs" , et vous êtes connecté à la grille source du locataire.

Créer un utilisateur local

Vous pouvez créer un utilisateur local et l'affecter à un ou plusieurs groupes locaux pour contrôler ses autorisations d'accès.

Les utilisateurs S3 qui n'appartiennent à aucun groupe ne disposent pas d'autorisations de gestion ni de stratégies de groupe S3 qui leur sont appliquées. Ces utilisateurs peuvent bénéficier d'un accès au compartiment S3 accordé via une politique de compartiment.

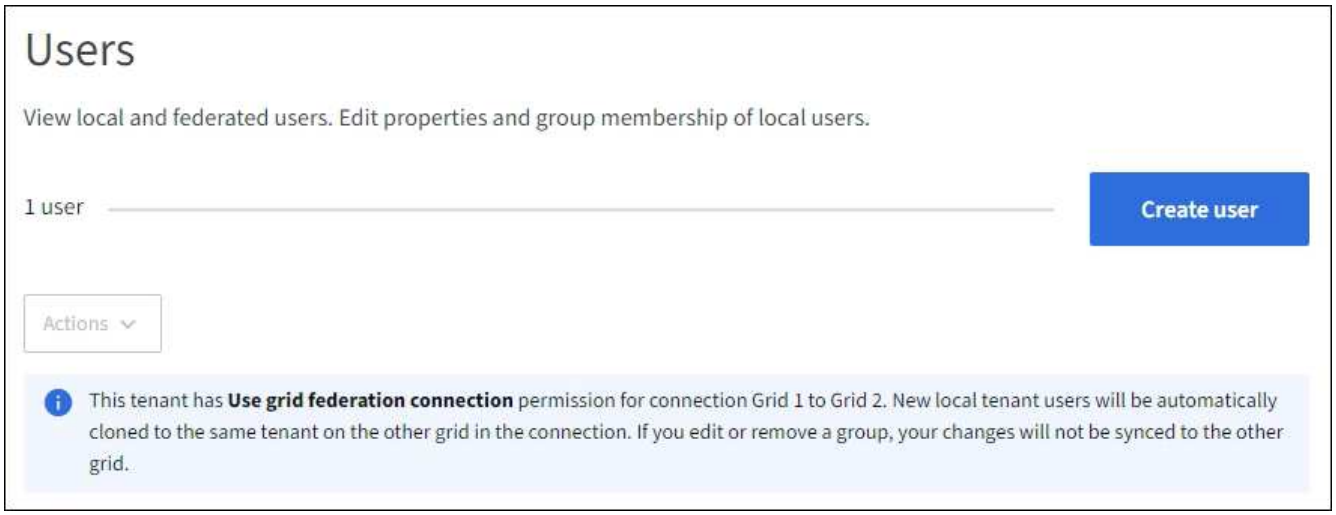
Les utilisateurs Swift qui n'appartiennent à aucun groupe ne disposent pas d'autorisations de gestion ni d'accès au conteneur Swift.

Accéder à l'assistant de création d'utilisateur

Étapes

1. Sélectionnez **GESTION DES ACCÈS** > **Utilisateurs**.

   Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille**, une bannière bleue indique qu'il s'agit de la grille source du locataire. Tous les utilisateurs locaux que vous créez sur cette grille seront clonés sur l'autre grille de la connexion.



2. Sélectionnez **Créer un utilisateur**.

Entrez les informations d'identification

Étapes

1. Pour l'étape **Saisir les informations d'identification de l'utilisateur**, remplissez les champs suivants.

Champ	Description
Nom et prénom	Le nom complet de cet utilisateur, par exemple, le prénom et le nom d'une personne ou le nom d'une application.

Champ	Description
Nom d'utilisateur	Le nom que cet utilisateur utilisera pour se connecter. Les noms d'utilisateur doivent être uniques et ne peuvent pas être modifiés. **Remarque** : si votre compte de locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille**, une erreur de clonage se produira si le même **Nom d'utilisateur** existe déjà pour le locataire sur la grille de destination.
Mot de passe et confirmation du mot de passe	Le mot de passe que l'utilisateur utilisera initialement lors de la connexion.
Refuser l'accès	Sélectionnez **Oui** pour empêcher cet utilisateur de se connecter au compte locataire, même s'il appartient toujours à un ou plusieurs groupes. Par exemple, sélectionnez **Oui** pour suspendre temporairement la possibilité pour un utilisateur de se connecter.

2. Sélectionnez **Continuer**.

Affecter à des groupes

Étapes

1. Affectez l'utilisateur à un ou plusieurs groupes locaux pour déterminer les tâches qu'il peut effectuer.

   L'affectation d'un utilisateur à des groupes est facultative. Si vous préférez, vous pouvez sélectionner des utilisateurs lorsque vous créez ou modifiez des groupes.

   Les utilisateurs qui n'appartiennent à aucun groupe n'auront aucune autorisation de gestion. Les autorisations sont cumulatives. Les utilisateurs disposeront de toutes les autorisations pour tous les groupes auxquels ils appartiennent. Voir "Autorisations de gestion des locataires" .

2. Sélectionnez **Créer un utilisateur**.

   Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille** et que vous êtes sur la grille source du locataire, le nouvel utilisateur local est cloné sur la grille de destination du locataire. **Succès** apparaît comme **Statut de clonage** dans la section Présentation de la page de détails de l'utilisateur.

3. Sélectionnez **Terminer** pour revenir à la page Utilisateurs.

Afficher ou modifier l'utilisateur local

Étapes

1. Sélectionnez **GESTION DES ACCÈS** > **Utilisateurs**.
2. Consultez les informations fournies sur la page Utilisateurs, qui répertorie les informations de base pour tous les utilisateurs locaux et fédérés de ce compte locataire.

   Si le compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille** et que vous visualisez l'utilisateur sur la grille source du locataire :

- Un message de bannière indique que si vous modifiez ou supprimez un utilisateur, vos modifications ne seront pas synchronisées avec l'autre grille.
- Si nécessaire, un message de bannière indique si les utilisateurs n'ont pas été clonés sur le locataire sur la grille de destination. Vous pouvez réessayer un clone d'utilisateur qui a échoué .

3. Si vous souhaitez modifier le nom complet de l'utilisateur :
   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**.
4. Si vous souhaitez afficher plus de détails ou apporter des modifications supplémentaires, effectuez l'une des opérations suivantes :
   - Sélectionnez le nom d'utilisateur.
   - Cochez la case correspondant à l'utilisateur, puis sélectionnez **Actions** > **Afficher les détails de l'utilisateur**.
5. Consultez la section Présentation, qui affiche les informations suivantes pour chaque utilisateur :
   - Nom et prénom
   - Nom d'utilisateur
   - Type d'utilisateur
   - Accès refusé
   - Mode d'accès
   - Adhésion au groupe
   - Champs supplémentaires si le compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille** et que vous visualisez l'utilisateur sur la grille source du locataire :
     - Statut du clonage, soit **Succès** soit **Échec**
     - Une bannière bleue indiquant que si vous modifiez cet utilisateur, vos modifications ne seront pas synchronisées avec l'autre grille.
6. Modifiez les paramètres utilisateur selon vos besoins. VoirCréer un utilisateur local pour plus de détails sur ce qu'il faut saisir.
   a. Dans la section Aperçu, modifiez le nom complet en sélectionnant le nom ou l'icône de modification .

      Vous ne pouvez pas changer le nom d'utilisateur.

   b. Dans l'onglet **Mot de passe**, modifiez le mot de passe de l'utilisateur et sélectionnez **Enregistrer les modifications**.
   c. Dans l'onglet **Accès**, sélectionnez **Non** pour autoriser l'utilisateur à se connecter ou sélectionnez **Oui** pour empêcher l'utilisateur de se connecter. Ensuite, sélectionnez **Enregistrer les modifications**.
   d. Dans l'onglet **Clés d'accès**, sélectionnez **Créer une clé** et suivez les instructions pour"créer les clés d'accès S3 d'un autre utilisateur" .
   e. Dans l'onglet **Groupes**, sélectionnez **Modifier les groupes** pour ajouter l'utilisateur à des groupes ou supprimer l'utilisateur des groupes. Ensuite, sélectionnez **Enregistrer les modifications**.
7. Confirmez que vous avez sélectionné **Enregistrer les modifications** pour chaque section que vous avez modifiée.

Utilisateur local en double

Vous pouvez dupliquer un utilisateur local pour créer un nouvel utilisateur plus rapidement.

> Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille** et que vous dupliquez un utilisateur à partir de la grille source du locataire, l'utilisateur dupliqué sera cloné sur la grille de destination du locataire.

Étapes

1. Sélectionnez **GESTION DES ACCÈS** > **Utilisateurs**.
2. Cochez la case correspondant à l'utilisateur que vous souhaitez dupliquer.
3. Sélectionnez **Actions** > **Dupliquer l'utilisateur**.
4. VoirCréer un utilisateur local pour plus de détails sur ce qu'il faut saisir.
5. Sélectionnez **Créer un utilisateur**.

Réessayer le clonage de l'utilisateur

Pour réessayer un clonage qui a échoué :

1. Sélectionnez chaque utilisateur qui indique *(Échec du clonage)* sous le nom d'utilisateur.
2. Sélectionnez **Actions** > **Cloner les utilisateurs**.
3. Affichez l'état de l'opération de clonage à partir de la page de détails de chaque utilisateur que vous clonez.

Pour plus d'informations, voir"Cloner des groupes de locataires et des utilisateurs" .

Supprimer un ou plusieurs utilisateurs locaux

Vous pouvez supprimer définitivement un ou plusieurs utilisateurs locaux qui n'ont plus besoin d'accéder au compte locataire StorageGRID .

> Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille** et que vous supprimez un utilisateur local, StorageGRID ne supprimera pas l'utilisateur correspondant sur l'autre grille. Si vous devez conserver ces informations synchronisées, vous devez supprimer le même utilisateur des deux grilles.

> Vous devez utiliser la source d'identité fédérée pour supprimer les utilisateurs fédérés.

Étapes

1. Sélectionnez **GESTION DES ACCÈS** > **Utilisateurs**.
2. Cochez la case correspondant à chaque utilisateur que vous souhaitez supprimer.
3. Sélectionnez **Actions** > **Supprimer l'utilisateur** ou **Actions** > **Supprimer les utilisateurs**.

   Une boîte de dialogue de confirmation apparaît.

4. Sélectionnez **Supprimer l'utilisateur** ou **Supprimer les utilisateurs**.