Gestion des groupes et des utilisateurs

StorageGRID

NetApp
November 04, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/storagegrid-117/tenant/using-identity-federation.html on November 04, 2025. Always check docs.netapp.com for the latest.

Sommaire

Gestion des groupes et des utilisateurs . . . 1
- Utiliser la fédération des identités . . . 1
  - Configurez la fédération des identités pour le gestionnaire des locataires . . . 1
  - Forcer la synchronisation avec le référentiel d'identité . . . 5
  - Désactiver la fédération des identités . . . 5
  - Instructions de configuration du serveur OpenLDAP . . . 5
- Gestion des groupes de locataires . . . 6
  - Créez des groupes pour un locataire S3 . . . 6
  - Créez des groupes pour un locataire Swift . . . 9
  - Autorisations de gestion des locataires . . . 11
  - Gérer les groupes . . . 13
- Gérez les utilisateurs locaux . . . 15
  - Créez un utilisateur local . . . 16
  - Afficher ou modifier un utilisateur local . . . 18
  - Dupliquer l'utilisateur local . . . 19
  - Supprimez un ou plusieurs utilisateurs locaux . . . 19

Gestion des groupes et des utilisateurs

Utiliser la fédération des identités

L'utilisation de la fédération des identités accélère la configuration des groupes de locataires et des utilisateurs, et permet aux utilisateurs de se connecter au compte du locataire à l'aide des identifiants familiers.

Configurez la fédération des identités pour le gestionnaire des locataires

Vous pouvez configurer la fédération des identités pour le Gestionnaire de locataires si vous souhaitez que les groupes et les utilisateurs de locataires soient gérés dans un autre système, tel qu'Active Directory, Azure Active Directory (Azure AD), OpenLDAP ou Oracle Directory Server.

Avant de commencer

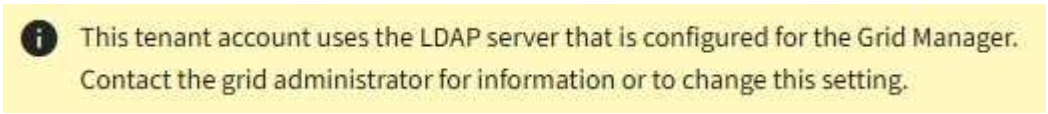
- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Autorisation d'accès racine".
- Vous utilisez Active Directory, Azure AD, OpenLDAP ou Oracle Directory Server comme fournisseur d'identité.

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

- Si vous avez l'intention d'utiliser OpenLDAP, vous devez configurer le serveur OpenLDAP. Voir Instructions de configuration du serveur OpenLDAP.
- Si vous prévoyez d'utiliser TLS (transport Layer Security) pour les communications avec le serveur LDAP, le fournisseur d'identité doit utiliser TLS 1.2 ou 1.3. Voir "Chiffrement pris en charge pour les connexions TLS sortantes".

Description de la tâche

La configuration d'un service de fédération des identités pour votre locataire dépend de la configuration de votre compte locataire. Votre locataire peut partager le service de fédération des identités configuré pour Grid Manager. Si ce message s'affiche lorsque vous accédez à la page Fédération des identités, vous ne pouvez pas configurer un référentiel d'identité fédéré distinct pour ce locataire.

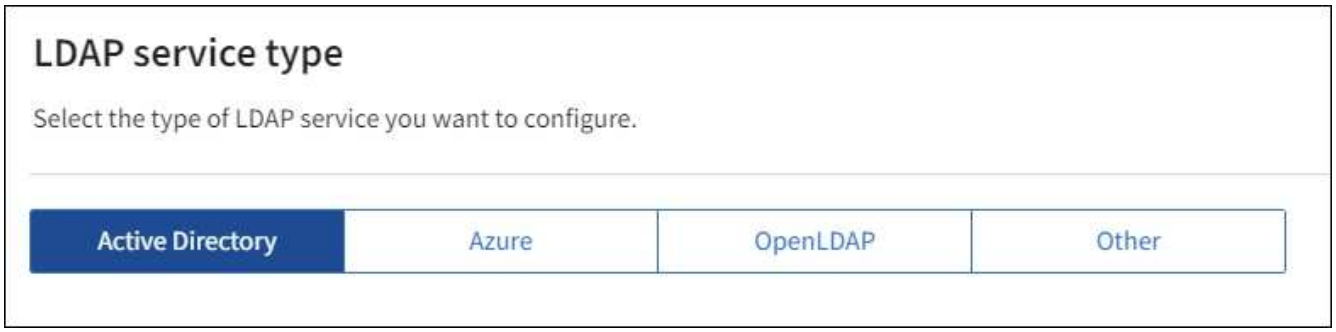


Entrez la configuration

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

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **identity federation**.
2. Sélectionnez **Activer la fédération d'identités**.
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**, renseignez les champs de la section attributs LDAP. Dans le cas contraire, passez à l'étape suivante.
   - **Nom unique utilisateur** : nom de l'attribut qui contient l'identifiant unique d'un utilisateur LDAP. Cet attribut est équivalent à `sAMAccountName` Pour Active Directory et `uid` Pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `uid`.
   - **UUID d'utilisateur** : nom de l'attribut qui contient l'identifiant unique permanent d'un utilisateur LDAP. Cet attribut est équivalent à `objectGUID` Pour Active Directory et `entryUUID` Pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `nsuniqueid`. La valeur de chaque utilisateur pour l'attribut spécifié doit être un nombre hexadécimal à 32 chiffres au format 16 octets ou chaîne, où les tirets sont ignorés.
   - **Nom unique de groupe** : nom de l'attribut qui contient l'identifiant unique d'un groupe LDAP. Cet attribut est équivalent à `sAMAccountName` Pour Active Directory et `cn` Pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `cn`.
   - **UUID de groupe** : nom de l'attribut qui contient l'identificateur unique permanent d'un groupe LDAP. Cet attribut est équivalent à `objectGUID` Pour Active Directory et `entryUUID` Pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `nsuniqueid`. La valeur de chaque groupe pour l'attribut spécifié doit être un nombre hexadécimal à 32 chiffres au format 16 octets ou chaîne, où les tirets sont ignorés.
5. Pour tous les types de services LDAP, entrez les informations de connexion réseau et de serveur LDAP 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** : port utilisé pour se connecter au serveur LDAP.

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

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

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

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

     - `sAMAccountName` ou `uid`

- `objectGUID`, `entryUUID`, ou `nsuniqueid`
- `cn`
- `memberOf` ou `isMemberOf`
- **Active Directory** : `objectSid`, `primaryGroupID`, `userAccountControl`, et `userPrincipalName`
- **Azure**: `accountEnabled` et `userPrincipalName`

◦ **Mot de passe** : mot de passe associé au nom d'utilisateur.

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

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

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

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

◦ **Bind username format** (facultatif) : le nom d'utilisateur par défaut StorageGRID devrait utiliser si le modèle ne peut pas être déterminé automatiquement.

Il est recommandé de fournir le format **Bind username** car il peut permettre aux utilisateurs de se connecter si StorageGRID ne parvient pas à se lier avec le compte de service.

Entrez l'un des motifs suivants :

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

  Inclure **[NOM D'UTILISATEUR]** exactement comme écrit.

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

◦ **Utilisez 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.

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

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

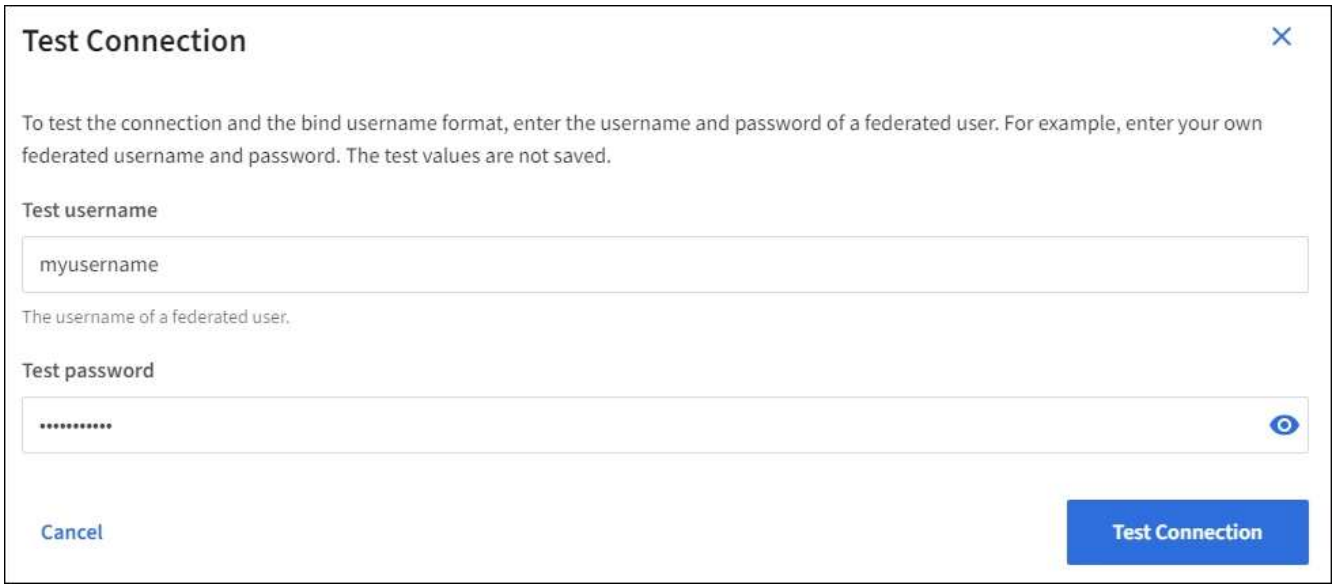
Testez la connexion et enregistrez la configuration

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 de nom d'utilisateur BIND, 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 connexion réussie » s'affiche si les paramètres de connexion sont valides. Sélectionnez **Enregistrer** pour enregistrer la configuration.
   - Un message « Impossible d'établir la connexion test » s'affiche si les paramètres de connexion ne sont pas valides. Sélectionnez **Fermer**. Ensuite, résolvez tout problème et testez à nouveau la connexion.
3. Si vous avez fourni un format de nom d'utilisateur BIND, entrez le nom d'utilisateur et le mot de passe d'un utilisateur fédéré valide.

   Par exemple, entrez votre nom d'utilisateur et votre mot de passe. N'incluez pas de caractères spéciaux dans le nom d'utilisateur, tels que @ ou /.



   - Un message « Test connexion réussie » 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 du test sont incorrects. Résolvez tout problème et testez à nouveau la connexion.

Forcer la synchronisation avec le référentiel d'identité

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

Étapes

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

Désactiver la fédération des identités

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

Description de la tâche

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

- Les utilisateurs fédérés ne pourront pas se connecter.
- Les utilisateurs fédérés qui sont actuellement connectés conservent l'accès au système StorageGRID jusqu'à l'expiration de leur session, mais ils ne pourront pas se connecter après l'expiration de leur session.
- La synchronisation entre le système StorageGRID et le référentiel d'identité ne se produira pas et des alertes ou des alarmes ne seront pas émises pour les comptes qui n'ont pas été synchronisés.
- La case **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 connexion unique doit être **désactivé** avant de pouvoir désactiver la fédération d'identités. Voir "Désactiver l'authentification unique".

Étapes

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

Instructions de configuration du serveur OpenLDAP

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

> Pour les référentiels 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 les clés S3 de l'utilisateur ou supprimez l'utilisateur de tous les groupes.

Recouvrements de memberOf et de raffint

Les recouvrements de membre et de raffinage doivent être activés. Pour plus d'informations, reportez-vous aux instructions relatives à la maintenance de l'adhésion au groupe inverse dans lehttp://www.openldap.org/doc/admin24/index.html["Documentation OpenLDAP : version 2.4 - Guide de l'administrateur"^].

Indexation

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

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

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

Reportez-vous aux informations relatives à la maintenance de l'adhésion au groupe inverse dans lehttp://www.openldap.org/doc/admin24/index.html["Documentation OpenLDAP : version 2.4 - Guide de l'administrateur"^].

Gestion des groupes de locataires

Créez 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 Gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Autorisation d'accès racine".
- Si vous prévoyez d'importer un groupe fédéré, vous avez "fédération des identités configurée", et le groupe fédéré existe déjà dans le référentiel d'identité configuré.
- Si votre compte locataire dispose de l'autorisation **utiliser la connexion de 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.

Accédez à l'assistant de création de groupe

Pour la première étape, accédez à l'assistant de création de groupe.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **Groups**.
2. Si votre compte locataire dispose de l'autorisation **utiliser la connexion de fédération de grille**, vérifiez qu'une bannière bleue s'affiche, 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 pouvez être connecté à la grille de destination du locataire.

3. Sélectionnez **Créer 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 du référentiel d'identité configuré précédemment.

   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 les applications client pour gérer les ressources du locataire, en fonction des autorisations de groupe.

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

     Si votre compte de locataire dispose de l'autorisation **utiliser la connexion de fédération de grille**, une erreur de clonage se produit 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 à l' `sAMAccountName` attribut. Pour OpenLDAP, le nom unique est le nom associé à `uid` attribut.
3. Sélectionnez **Continuer**.

Gérer les autorisations de groupe

Les autorisations de groupe contrôlent les tâches que les utilisateurs peuvent effectuer dans le Gestionnaire de locataires et l'API de gestion des locataires.

Étapes

1. Pour **Access mode**, sélectionnez l'une des options suivantes :
   - **Lecture-écriture** (par défaut) : les utilisateurs peuvent se connecter au gestionnaire de locataires et gérer la configuration du locataire.

- **Lecture seule** : les utilisateurs peuvent uniquement afficher les paramètres et les fonctionnalités. Ils ne peuvent pas apporter de modifications ni exécuter d'opérations dans le gestionnaire de locataires ou l'API de gestion des locataires. Les utilisateurs locaux en lecture seule peuvent modifier leurs propres mots de passe.

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

2. Sélectionnez une ou plusieurs autorisations pour ce groupe.

   Voir "Autorisations de gestion des locataires".

3. Sélectionnez **Continuer**.

Définissez la règle de groupe S3

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

Étapes

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

Stratégie de groupe	Description
Aucun accès à S3	Par défaut. Les utilisateurs de ce groupe n'ont pas accès aux ressources S3, sauf si l'accès est accordé avec une règle de compartiment. Si vous sélectionnez cette option, seul l'utilisateur root peut accéder aux ressources S3 par défaut.
Accès en lecture seule	Les utilisateurs de ce groupe disposent d'un accès en lecture seule aux ressources S3. Par exemple, les utilisateurs de ce groupe peuvent afficher la liste des objets et lire les données d'objet, les métadonnées et les balises. Lorsque vous sélectionnez cette option, la chaîne JSON pour une stratégie de groupe en lecture seule s'affiche dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
Accès complet	Les utilisateurs de ce groupe bénéficient d'un accès complet aux ressources S3, y compris les compartiments. Lorsque vous sélectionnez cette option, la chaîne JSON pour une stratégie de groupe à accès complet s'affiche dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.

Stratégie de groupe	Description
Réduction des ransomwares	Cet exemple de règle s'applique à toutes les compartiments pour ce locataire. Les utilisateurs de ce groupe peuvent effectuer des actions courantes, mais ne peuvent pas supprimer définitivement des objets des compartiments pour lesquels la gestion des versions d'objet est activée. Les utilisateurs de tenant Manager disposant 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), le cas échéant.
Personnalisées	Les utilisateurs du groupe se voient accorder les autorisations que vous spécifiez dans la zone de texte.

2. Si vous avez sélectionné **personnalisé**, entrez la stratégie de groupe. Chaque stratégie de groupe a une taille limite de 5,120 octets. Vous devez entrer une chaîne au format JSON valide.

   Pour plus d'informations sur les stratégies de groupe, notamment la syntaxe de la langue et des exemples, reportez-vous à la section "Exemples de stratégies de groupe".

3. Si vous créez un groupe local, sélectionnez **Continuer**. Si vous créez un groupe fédéré, sélectionnez **Créer 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 qui existent déjà.

> Si votre compte de locataire dispose de l'autorisation **utiliser la connexion de 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 dans 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 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 de fédération de grille** et que vous êtes sur la grille source du locataire, le nouveau groupe est cloné dans la grille de destination du locataire. **Succès** apparaît comme l'état **clonage** dans la section vue d'ensemble de la page de détails du groupe.

Créez des groupes pour un locataire Swift

Vous pouvez gérer les autorisations d'accès pour un compte de 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 de locataire Swift.

> La prise en charge des applications du client Swift a été obsolète et sera supprimée dans une prochaine version.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Autorisation d'accès racine".
- Si vous prévoyez d'importer un groupe fédéré, vous avez "fédération des identités configurée", et le groupe fédéré existe déjà dans le référentiel d'identité configuré.

Accédez à l'assistant de création de groupe

Étapes

Pour la première étape, accédez à l'assistant de création de groupe.

1. Sélectionnez **ACCESS MANAGEMENT** > **Groups**.
2. Sélectionnez **Créer 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 du référentiel d'identité configuré précédemment.

   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 les applications client pour gérer les ressources du locataire, en fonction des autorisations de groupe.

2. Entrez le nom du groupe.
   - **Groupe local** : saisissez à la fois 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 à l' `sAMAccountName` attribut. Pour OpenLDAP, le nom unique est le nom associé à `uid` attribut.
3. Sélectionnez **Continuer**.

Gérer les autorisations de groupe

Les autorisations de groupe contrôlent les tâches que les utilisateurs peuvent effectuer dans le Gestionnaire de locataires et l'API de gestion des locataires.

Étapes

1. Pour **Access mode**, sélectionnez l'une des options suivantes :
   - **Lecture-écriture** (par défaut) : les utilisateurs peuvent se connecter au gestionnaire de locataires et

gérer la configuration du locataire.

- **Lecture seule** : les utilisateurs peuvent uniquement afficher les paramètres et les fonctionnalités. Ils ne peuvent pas apporter de modifications ni exécuter d'opérations dans le gestionnaire de locataires ou l'API de gestion des locataires. Les utilisateurs locaux en lecture seule peuvent modifier leurs propres mots de passe.

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

2. Cochez la case **accès racine** si les utilisateurs du groupe doivent se connecter à l'API tenant Manager ou tenant Management.
3. Sélectionnez **Continuer**.

Définissez la stratégie de groupe Swift

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

1. Cochez la case **Swift Administrator** 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 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 qui existent déjà.

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 "Gérez les utilisateurs locaux".

2. Sélectionnez **Créer 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, tenez compte des 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 vous 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 autorisés à se connecter peuvent effectuer les tâches suivantes :

- Afficher le tableau de bord
- Modifier son 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 ne peuvent afficher que les paramètres et les fonctions associés.

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

Vous pouvez attribuer les autorisations suivantes à un groupe. Notez que les locataires S3 et Swift disposent d'autorisations de groupe différentes.

Autorisations	Description
Accès racine	Donne un accès complet au gestionnaire des locataires et à l'API de gestion des locataires. **Remarque :** les utilisateurs Swift doivent disposer d'une autorisation d'accès racine pour se connecter au compte locataire.
Administrateur	Les locataires Swift uniquement. Fournit un accès complet aux conteneurs et objets Swift pour ce compte de locataire **Remarque :** les utilisateurs de Swift doivent disposer de l'autorisation Administrateur Swift pour effectuer toutes les opérations avec l'API REST Swift.
Gérez vos 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 **STORAGE (S3)** > **My S3 Access keys**.
Gestion de 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 gérer les paramètres de tous les compartiments S3 du compte, indépendamment des règles du compartiment S3 ou du groupe. Les utilisateurs qui ne disposent pas de cette autorisation ne voient pas l'option de menu **rubriques**. • Locataires Swift : permet aux utilisateurs Swift de contrôler le niveau de cohérence des conteneurs Swift à l'aide de l'API de gestion des locataires. **Remarque :** vous ne pouvez attribuer l'autorisation gérer tous les compartiments aux groupes Swift qu'à partir de l'API de gestion des locataires. Vous ne pouvez pas attribuer cette autorisation à des groupes Swift à l'aide du Gestionnaire de locataires.

Autorisations	Description
Gestion des terminaux	Permet aux utilisateurs d'utiliser le gestionnaire de locataires ou l'API de gestion des locataires pour créer ou modifier des terminaux 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 **Platform Services Endpoints**.
Gestion des objets avec la console S3	Associé à l'autorisation gérer tous les compartiments, permet aux utilisateurs d'accéder à la console S3 expérimentale à partir de la page compartiments. Les utilisateurs qui disposent de cette autorisation mais qui ne disposent pas de l'autorisation gérer tous les compartiments peuvent toujours naviguer directement vers la console S3 expérimentale.

Gérer les groupes

Vous pouvez afficher un groupe, modifier le nom, les autorisations, les stratégies et les utilisateurs d'un groupe, dupliquer un groupe ; ou supprimer un groupe.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Autorisation d'accès racine".

Afficher ou modifier un groupe

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

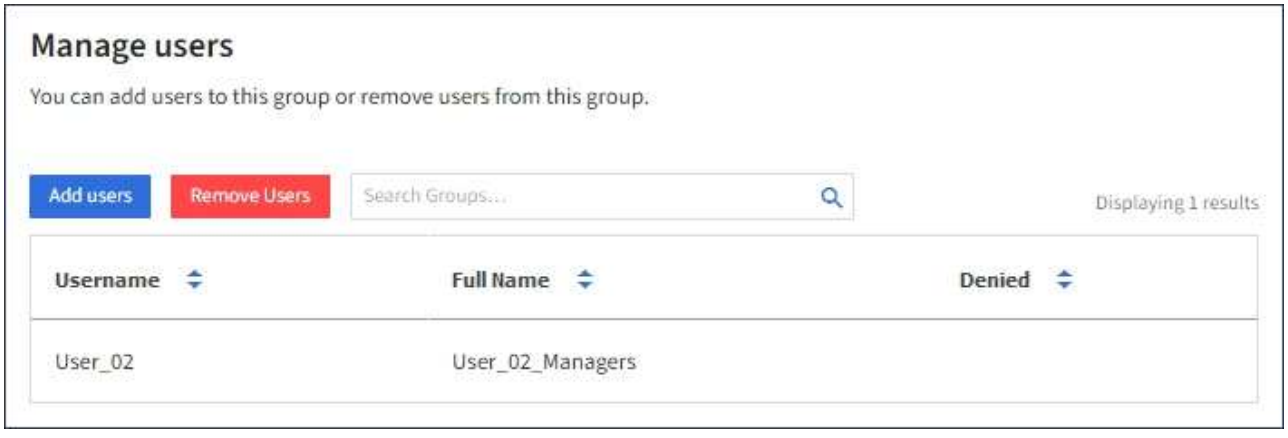
Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **Groups**.
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 de tenant.

   Si le compte de tenant dispose de l'autorisation **utiliser la connexion de fédération de grille** et que vous affichez des groupes sur la grille source du locataire, une bannière bleue indique que si vous modifiez ou supprimez un groupe, vos modifications ne seront pas synchronisées avec l'autre grille. Voir "Cloner des groupes de locataires et des utilisateurs".

3. Si vous souhaitez modifier le nom du groupe :
   a. Cochez la case du groupe.
   b. Sélectionnez **actions** > **Modifier le nom du groupe**.
   c. Saisissez 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 du groupe et sélectionnez **actions** > **Afficher les détails du groupe**.

5. Consultez la section Présentation, qui présente les informations suivantes pour chaque groupe :
   - Nom d'affichage
   - Nom unique
   - Type
   - Mode d'accès
   - Autorisations
   - Règle S3
   - Nombre d'utilisateurs dans ce groupe
   - Champs supplémentaires si le compte de tenant dispose de l'autorisation **utiliser la connexion de fédération de grille** et que vous affichez le groupe sur la grille source du locataire :
     - État de 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 de groupe selon vos besoins. Voir "Créez des groupes pour un locataire S3" et "Créez des groupes pour un locataire Swift" pour plus d'informations sur ce que vous devez saisir.
   a. Dans la section vue d'ensemble, 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 une règle de groupe S3 différente ou entrez la chaîne JSON pour une règle personnalisée, si nécessaire.
      - Si vous modifiez un groupe Swift, cochez ou décochez 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 s'affiche en haut à droite.

8. Pour supprimer des utilisateurs locaux du groupe :
   a. Sélectionnez l'onglet utilisateurs.
   b. Sélectionnez **Supprimer utilisateurs**.
   c. Sélectionnez les utilisateurs que vous souhaitez supprimer, puis sélectionnez **Supprimer utilisateurs**.

      Un message de réussite s'affiche en haut à droite.
9. Confirmez que vous avez sélectionné **Enregistrer les modifications** pour chaque section que vous avez modifiée.

Dupliquer le groupe

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

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

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **Groups**.
2. Cochez la case du groupe que vous souhaitez dupliquer.
3. Sélectionnez **actions** > **Dupliquer le groupe**.
4. Voir "Créez des groupes pour un locataire S3" ou "Créez des groupes pour un locataire Swift" pour plus d'informations sur ce que vous devez saisir.
5. Sélectionnez **Créer groupe**.

Supprimer un ou plusieurs groupes

Vous pouvez supprimer un ou plusieurs groupes. Les utilisateurs qui appartiennent uniquement à un groupe supprimé ne pourront plus se connecter au gestionnaire de tenant ni utiliser le compte de tenant.

> Si votre compte de locataire dispose de l'autorisation **utiliser la connexion de 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 **ACCESS MANAGEMENT** > **Groups**.
2. Cochez la case correspondant à chaque groupe à supprimer.
3. Sélectionnez **actions** > **Supprimer groupe** ou **actions** > **Supprimer groupes**.

   Une boîte de dialogue de confirmation s'affiche.
4. Sélectionnez **Supprimer le groupe** ou **Supprimer les groupes**.

Gérez les utilisateurs locaux

Vous pouvez créer des utilisateurs locaux et les affecter à des groupes locaux pour

déterminer les fonctions 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 racine.

> 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 Gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Autorisation d'accès racine".
- Si votre compte locataire dispose de l'autorisation **utiliser la connexion de 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.

Créez un utilisateur local

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

Les utilisateurs S3 qui n'appartiennent à aucun groupe ne disposent pas d'autorisations de gestion ni de règles de groupe S3 qui leur sont appliquées. Il est possible que les utilisateurs bénéficient d'un accès par compartiment S3 accordé via une règle de compartiment.

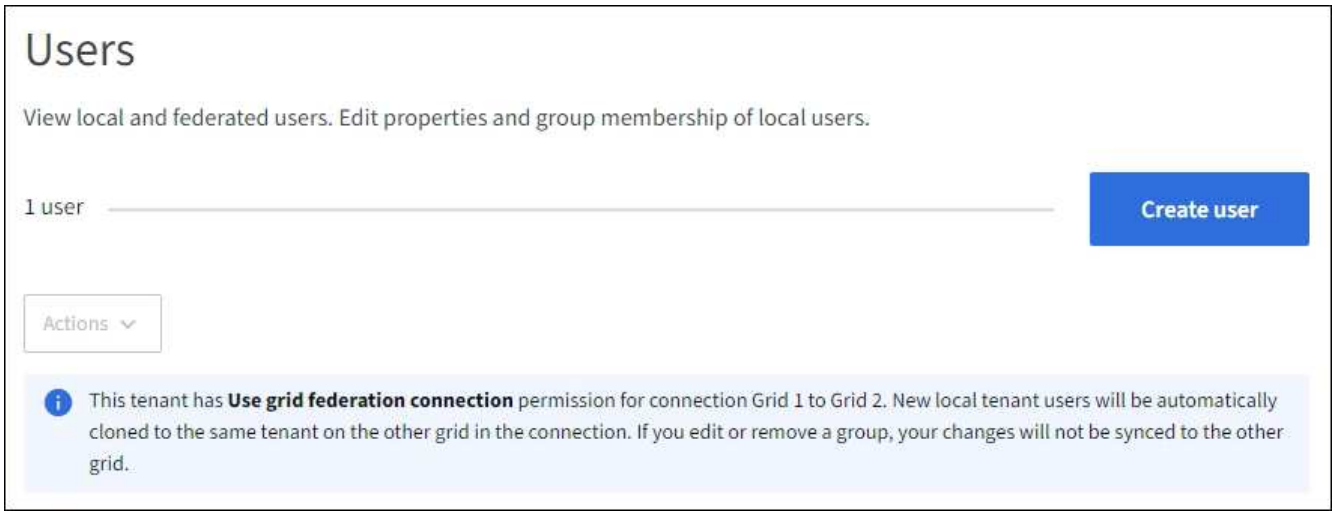
Les utilisateurs Swift qui n'appartiennent à aucun groupe ne disposent d'aucune autorisation de gestion ou d'un accès au conteneur Swift.

Accédez à l'assistant de création d'utilisateur

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **Users**.

   Si votre compte de locataire dispose de l'autorisation **utiliser la connexion de 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 dans l'autre grille de la connexion.



2. Sélectionnez **Créer utilisateur**.

Entrez les informations d'identification

Étapes

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

Champ	Description
Nom complet	Le nom complet de cet utilisateur, par exemple le prénom et le nom d'une personne ou le nom d'une application.
Nom d'utilisateur	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 locataire dispose de l'autorisation **utiliser la connexion de fédération de grille**, une erreur de clonage se produit si le même **Nom d'utilisateur** existe déjà pour le locataire sur la grille de destination.
Mot de passe et confirmer le mot de passe	Le mot de passe que l'utilisateur utilisera lors de sa connexion.
Refuser l'accès	Sélectionnez **Oui** pour empêcher cet utilisateur de se connecter au compte de tenant, même s'il appartient toujours à un ou plusieurs groupes. Par exemple, sélectionnez **Oui** pour suspendre temporairement la capacité d'un utilisateur à se connecter.

2. Sélectionnez **Continuer**.

Affecter à des groupes

Étapes

1. Attribuez l'utilisateur à un ou plusieurs groupes locaux pour déterminer les tâches qu'ils peuvent effectuer.

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

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

2. Sélectionnez **Créer utilisateur**.

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

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

Afficher ou modifier un utilisateur local

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **Users**.
2. Consultez les informations fournies sur la page utilisateurs, qui répertorie les informations de base pour tous les utilisateurs locaux et fédérés pour ce compte de tenant.

   Si le compte de tenant dispose de l'autorisation **utiliser la connexion de fédération de grille** et que vous affichez l'utilisateur sur la grille source du locataire, une bannière bleue indique que si vous modifiez ou supprimez l'utilisateur, vos modifications ne seront pas synchronisées avec l'autre grille.

3. Si vous souhaitez modifier le nom complet de l'utilisateur :
   a. Cochez la case de l'utilisateur.
   b. Sélectionnez **actions** > **Modifier le nom complet**.
   c. Saisissez 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 de l'utilisateur et sélectionnez **actions** > **Afficher les détails de l'utilisateur**.
5. Consultez la section Présentation, qui présente les informations suivantes pour chaque utilisateur :
   - Nom complet
   - Nom d'utilisateur
   - Type d'utilisateur
   - Accès refusé
   - Mode d'accès
   - Appartenance à un groupe
   - Champs supplémentaires si le compte de tenant dispose de l'autorisation **utiliser la connexion de fédération de grille** et que vous affichez l'utilisateur sur la grille source du locataire :
     - État de 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. Voir Créer un utilisateur local pour plus d'informations sur ce que vous devez saisir.
   a. Dans la section vue d'ensemble, modifiez le nom complet en sélectionnant le nom ou l'icône de modification .

      Vous ne pouvez pas modifier 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 permettre à l'utilisateur de se connecter ou sélectionnez **Oui** pour empêcher l'utilisateur de se connecter. Sélectionnez ensuite **Enregistrer les modifications**.
   d. Dans l'onglet **clés d'accès**, sélectionnez **Créer une clé** et suivez les instructions de "Création des 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. Sélectionnez ensuite **Enregistrer les modifications**.
7. Confirmez que vous avez sélectionné **Enregistrer les modifications** pour chaque section que vous avez modifiée.

Dupliquer l'utilisateur local

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

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

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **Users**.
2. Cochez la case correspondant à l'utilisateur que vous souhaitez dupliquer.
3. Sélectionnez **actions** > **Dupliquer utilisateur**.
4. Voir Créer un utilisateur local pour plus d'informations sur ce que vous devez saisir.
5. Sélectionnez **Créer utilisateur**.

Supprimez un ou plusieurs utilisateurs locaux

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

> Si votre compte de tenant dispose de l'autorisation **utiliser la connexion de 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 le référentiel d'identité fédéré pour supprimer des utilisateurs fédérés.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **Users**.
2. Cochez la case correspondant à chaque utilisateur à supprimer.
3. Sélectionnez **actions** > **Supprimer utilisateur** ou **actions** > **Supprimer utilisateurs**.

   Une boîte de dialogue de confirmation s'affiche.

4. Sélectionnez **Supprimer utilisateur** ou **Supprimer utilisateurs**.

Informations sur le copyright

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

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

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

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

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

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

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

Informations sur les marques commerciales

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