Gérer les groupes et les utilisateurs

StorageGRID software

NetApp
July 23, 2026

Sommaire

Gérer les groupes et les utilisateurs

Utilisez la fédération d'identité dans StorageGRID

${post_edited_translations.segment}

Configurer la fédération d'identité pour Tenant Manager

Vous pouvez configurer la fédération d'identité pour le Tenant Manager si vous souhaitez que les groupes et utilisateurs de locataires soient gérés dans un autre système tel que Active Directory, Microsoft Entra ID, 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 root".
- Vous utilisez Active Directory, Microsoft Entra ID, 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 Instructions pour la configuration du serveur OpenLDAP.
- Si vous prévoyez d'utiliser le protocole Transport Layer Security (TLS) pour les communications avec le serveur LDAP, le fournisseur d'identité doit utiliser TLS 1.2 ou 1.3. Voir "Chiffrements pris en charge pour les connexions TLS sortantes".

À propos de cette tâche

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

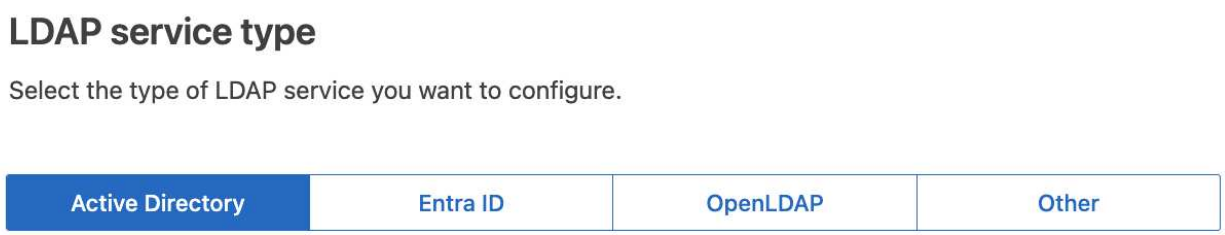
> This tenant account uses the LDAP server that is configured for the Grid Manager. Contact the grid administrator for information or to change this setting.

${post_edited_translations.segment}

${post_edited_translations.segment}

Étapes

1. Sélectionnez **Gestion des accès** > **Fédération d'identités**.
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**, complétez les champs de la section Attributs LDAP. Sinon, 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, saisissez `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, saisissez `nsuniqueid`. La valeur de chaque utilisateur pour l'attribut spécifié doit être un nombre hexadécimal de 32 chiffres, au format 16 octets ou chaîne, les traits d'union étant 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, saisissez `cn`.
   - **UUID de groupe** : le nom de l'attribut qui contient l'identifiant unique permanent d'un groupe LDAP. Cet attribut est équalent à `objectGUID` pour Active Directory et `entryUUID` pour OpenLDAP. Si vous configurez Oracle Directory Server, saisissez `nsuniqueid`. La valeur de chaque groupe pour l'attribut spécifié doit être un nombre hexadécimal de 32 chiffres, au format 16 octets ou chaîne de caractères, où les tirets sont ignorés.
5. Pour tous les types de services LDAP, saisissez les informations requises concernant le serveur LDAP et la connexion réseau 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 unique (DN) de l'utilisateur qui se connectera au serveur LDAP.

     Pour Active Directory, vous pouvez également spécifier le nom d'ouverture de session de niveau inférieur ou le User Principal Name.

     L'utilisateur spécifié doit avoir l'autorisation de lister 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`
- **Entra ID** : `accountEnabled` et `userPrincipalName`

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

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

◦ **DN de base du groupe** : le chemin complet du nom unique (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 du **nom unique du groupe** doivent être uniques au sein du **DN de base du groupe** auquel elles appartiennent.

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

> Les valeurs du **nom unique de l'utilisateur** doivent être uniques au sein du **DN de base utilisateur** auquel elles appartiennent.

◦ **Format du nom d'utilisateur de liaison** (facultatif) : 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 du nom d'utilisateur de liaison** car cela 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 :

- **UserPrincipalName modèle (AD et Entra ID)**: `[USERNAME]@*example*.com`
- **Modèle de nom d'ouverture de session de niveau inférieur (AD et Entra ID)** : `*example*\[USERNAME]`
- **Modèle de nom unique** : `CN=[USERNAME],CN=Users,DC=*example*,DC=com`

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

6. Dans la section Transport Layer Security (TLS), sélectionnez un paramètre de sécurité.
   ◦ **Utiliser STARTTLS** : Utilisez STARTTLS pour sécuriser les communications avec le serveur LDAP. Cette option est recommandée pour Active Directory, OpenLDAP ou Autre, mais cette option n'est pas prise en charge pour Microsoft Entra ID.
   ◦ **Utiliser LDAPS** : L'option LDAPS (LDAP sur SSL) utilise TLS pour établir une connexion au serveur LDAP. Vous devez sélectionner cette option pour Microsoft Entra ID.
   ◦ **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 Microsoft Entra ID.

> L'option « Ne pas utiliser TLS » n'est pas prise en charge si votre serveur Active Directory impose 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.
   - **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 du certificat d'autorité de certification.

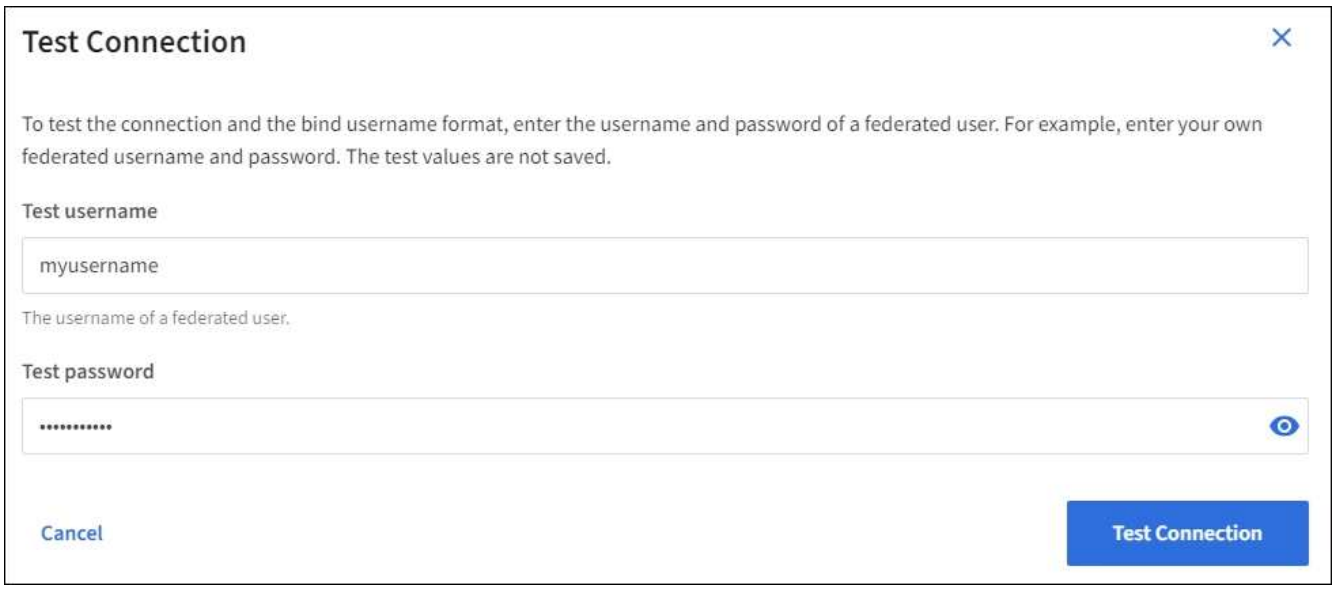
Testez la connexion et enregistrez la configuration

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

Étapes

1. Sélectionnez **Test connection**.
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 « Impossible d'établir la connexion de test » s'affiche si les paramètres de connexion sont incorrects. Sélectionnez **Fermer**. Ensuite, résolvez les problèmes éventuels 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, saisissez 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 sont invalides. Résolvez les problèmes éventuels 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 de fédération d'identités.
2. Sélectionnez **Sync server** 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'identités** est déclenchée en cas de problème lors de la synchronisation des groupes et utilisateurs fédérés à partir de la source d'identité.

Désactivez la fédération d'identités

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

À propos de cette tâche

Avant de désactiver la fédération d'identités, vous devez prendre en compte les 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 plus se connecter après l'expiration de celle-ci.
- La synchronisation entre le système StorageGRID et la source d'identité n'aura pas lieu et aucune alerte ne sera émise pour les comptes qui n'ont pas été synchronisés.
- La case à cocher **Activer la fédération d'identités** est désactivée si le statut de l'authentification unique (SSO) est **Activé** ou **Mode bac à sable**. Le statut SSO sur la page d'authentification unique doit être **Désactivé** avant que vous puissiez désactiver la fédération d'identités. Voir "Désactivez l'authentification unique".

Étapes

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

Instructions pour la configuration du serveur OpenLDAP

Si vous souhaitez utiliser un serveur OpenLDAP pour la fédération d'identités, vous devez configurer des

paramètres spécifiques sur le serveur OpenLDAP.

> Pour les sources d'identité autres qu'Active Directory ou Microsoft Entra ID, StorageGRID ne bloque pas automatiquement l'accès S3 aux utilisateurs désactivés en externe. Pour bloquer l'accès S3, supprimez les clés S3 de l'utilisateur ou retirez l'utilisateur de tous les groupes.

Overlays Memberof et refint

Les superpositions memberof et refint doivent être activées. Pour plus d'informations, consultez les instructions relatives à la gestion des appartenances aux groupes inversées dans le "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 relatives à la gestion des appartenances aux groupes inversés dans le "Documentation OpenLDAP : Guide de l'administrateur version 2.4".

${post_edited_translations.segment}

Créez des groupes pour un locataire S3 dans StorageGRID

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 prévoyez d'importer un groupe fédéré, vous avez "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 de fédération de grille**, vous avez examiné le flux de travail et les considérations pour "clonage des groupes de locataires et des utilisateurs", et vous êtes connecté à la grille source du locataire.

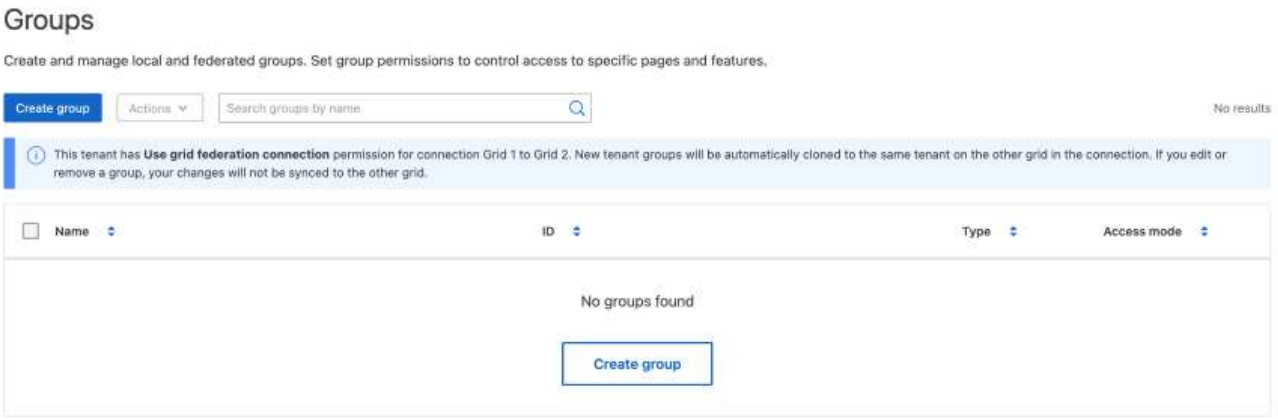
${post_edited_translations.segment}

Pour commencer, 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 de fédération de grilles**, vérifiez qu'une bannière bleue s'affiche, indiquant que les nouveaux groupes créés sur cette grille seront clonés sur le même locataire dans 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 Tenant Manager, bien qu'ils puissent utiliser des applications clientes pour gérer les ressources du locataire, en fonction des autorisations du groupe.

2. Saisissez 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 locataire dispose de l'autorisation **Utiliser la connexion de 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 à l'attribut `sAMAccountName`. Pour OpenLDAP, le nom unique est le nom associé à l'attribut `uid`.
3. Sélectionnez **Continue**.

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 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 consulter les paramètres et les fonctionnalités. Ils ne peuvent apporter aucune modification ni effectuer d'opérations dans le Tenant Manager ou l'API Tenant Management. Les utilisateurs locaux en lecture seule peuvent changer leur propre mot de passe.

> Si un utilisateur appartient à plusieurs groupes et que l'un de ces groupes est configuré en 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 "${post_edited_translations.segment}".

3. Sélectionnez **Continue**.

Définir la stratégie de groupe S3

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

Étapes

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

stratégie de groupe	Description
Aucun accès S3	Par défaut. Les utilisateurs de ce groupe n'ont pas accès aux ressources S3, à moins que l'accès ne soit accordé par une politique 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 disposent d'un accès en lecture seule aux ressources S3. Par exemple, les utilisateurs de ce groupe peuvent lister les 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 apparaît dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
Accès complet	Les utilisateurs de ce groupe disposent d'un accès complet aux ressources S3, y compris les compartiments. Lorsque vous sélectionnez cette option, la chaîne JSON d'une stratégie de groupe d'accès complet s'affiche dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.

stratégie 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 des objets des compartiments pour lesquels le versionnement d'objets est activé. Les utilisateurs Tenant Manager disposant de l'autorisation **Manage all buckets** peuvent ignorer cette stratégie de groupe. Limitez l'autorisation **Manage all buckets** aux utilisateurs de confiance et utilisez l'authentification multifacteur (MFA) lorsque disponible.
Personnalisé	${post_edited_translations.segment}

2. Si vous avez sélectionné **Custom**, saisissez la stratégie de groupe. Chaque stratégie de groupe est limitée à une taille de 5 120 octets. Vous devez saisir une chaîne au format JSON valide.

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

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

Ajouter des utilisateurs (groupes locaux uniquement)

${post_edited_translations.segment}

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

Étapes

1. Facultativement, sélectionnez 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 de fédération de grilles** et que vous êtes sur la grille source du locataire, le nouveau groupe est cloné vers la grille de destination du locataire. **Réussi** apparaît comme l'**état du clonage** dans la section Vue d'ensemble de la page de détails du groupe.

Autorisations de gestion des locataires StorageGRID

Avant de créer un groupe de locataires, réfléchissez aux autorisations que vous souhaitez lui attribuer. Les autorisations de gestion des locataires déterminent les tâches que les utilisateurs peuvent effectuer à l'aide du Tenant Manager 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 Tenant Manager ou utiliser l'API Tenant Management, 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
- ${post_edited_translations.segment}

Pour toutes les autorisations, le paramètre de mode d'accès du groupe détermine si les utilisateurs peuvent modifier les paramètres et effectuer des opérations ou s'ils peuvent uniquement consulter les paramètres et fonctionnalités associés.

> Si un utilisateur appartient à plusieurs groupes et que l'un de ces groupes est configuré en lecture seule, l'utilisateur aura un accès en lecture seule à tous les paramètres et fonctionnalités sélectionnés.

${post_edited_translations.segment}

Autorisation	Description	Détails
Accès root	Offre un accès complet au Tenant Manager et à l'API Tenant Management.	
Gérez vos propres identifiants S3	${post_edited_translations.segment}	Les utilisateurs qui ne disposent pas de cette autorisation ne voient pas l'option de menu **STOCKAGE (S3)** > **Mes clés d'accès S3**.
${post_edited_translations.segment}	${post_edited_translations.segment}	${post_edited_translations.segment} Cette autorisation est remplacée par l'autorisation Gérer tous les compartiments. Elle n'affecte pas les politiques de groupe ou de compartiment S3 utilisées par les clients S3 ou la console S3.
${post_edited_translations.segment}	Permet aux utilisateurs d'utiliser le Tenant Manager et l'API Tenant Management pour créer et supprimer des compartiments S3 et gérer les paramètres de tous les compartiments S3 du compte locataire, indépendamment des stratégies de compartiment S3 ou de groupe.	${post_edited_translations.segment} Cette autorisation remplace l'autorisation Afficher tous les compartiments. Elle n'affecte pas les politiques de compartiment ou de groupe S3 utilisées par les clients S3 ou la S3 Console.
Gérer les points de terminaison	Permet aux utilisateurs d'utiliser le Tenant Manager ou l'API de gestion des locataires pour créer ou modifier des points de terminaison de services 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 la plateforme**.

Autorisation	Description	Détails
${post_edited_translations.segment}	${post_edited_translations.segment}	

Gérer les groupes de locataires StorageGRID

${post_edited_translations.segment}

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".

${post_edited_translations.segment}

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

Étapes

1. Sélectionnez **Gestion des accès** > **Groupes**.
2. ${post_edited_translations.segment}

   Si le compte du locataire dispose de l'autorisation **Utiliser la connexion de fédération de grille** et que vous consultez des groupes sur la grille source du locataire :

   - ${post_edited_translations.segment}
   - Au besoin, un message de bannière indique si des groupes n'ont pas été clonés sur le locataire de la grille de destination. Vous pouvez ${post_edited_translations.segment} qui ont échoué.
3. ${post_edited_translations.segment}
   a. Cochez la case correspondant au groupe.
   b. Sélectionnez **Actions** > **Modifier le nom du groupe**.
   c. Saisissez le nouveau nom.
   d. ${post_edited_translations.segment}
4. ${post_edited_translations.segment}
   - ${post_edited_translations.segment}
   - Sélectionnez la case à cocher du groupe, puis sélectionnez **Actions** > **Afficher les détails du groupe**.
5. ${post_edited_translations.segment}
   - Nom d'affichage
   - Nom unique
   - Type
   - Mode d'accès
   - Autorisations
   - ${post_edited_translations.segment}

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
  - ${post_edited_translations.segment}
  - ${post_edited_translations.segment}

6. Modifiez les paramètres de groupe selon vos besoins. Reportez-vous à "Créer des groupes pour un locataire S3" pour obtenir des détails sur les informations à 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 du groupe**, mettez à jour les autorisations et sélectionnez **Enregistrer les modifications**.
   c. ${post_edited_translations.segment}

      ${post_edited_translations.segment}

7. Pour ajouter un ou plusieurs utilisateurs locaux existants au groupe :
   a. ${post_edited_translations.segment}

   b. ${post_edited_translations.segment}
   c. ${post_edited_translations.segment}

      Un message de confirmation apparaît en haut à droite.

8. ${post_edited_translations.segment}
   a. ${post_edited_translations.segment}
   b. ${post_edited_translations.segment}
   c. ${post_edited_translations.segment}

      Un message de confirmation apparaît en haut à droite.

9. ${post_edited_translations.segment}

${post_edited_translations.segment}

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

> Si votre compte 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 **Gestion des accès** > **Groupes**.
2. ${post_edited_translations.segment}
3. Sélectionnez **Actions** > **Dupliquer le groupe**.
4. Reportez-vous à "Créer des groupes pour un locataire S3" pour plus de détails sur les informations à saisir.
5. Sélectionnez **Créer un groupe**.

Réessayer le clonage du groupe

${post_edited_translations.segment}

1. Sélectionnez chaque groupe qui indique *(Échec du clonage)* sous le nom du groupe.
2. Sélectionnez **Actions** > **Clone groups**.
3. Consultez l'état de l'opération de clonage sur la page de détails de chaque groupe que vous clonez.

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

Supprimer un ou plusieurs groupes

Vous pouvez supprimer un ou plusieurs groupes. Tous les utilisateurs qui appartiennent 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 de fédération de grilles** 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 pour 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**.

Configurez AssumeRole

Avant de commencer

Vous devez être administrateur pour configurer AssumeRole.

À propos de cette tâche

Pour configurer AssumeRole, créez le groupe cible à assumer, si le groupe n'existe pas déjà. Modifiez la politique S3 du groupe pour spécifier les actions autorisées pour assumer ce groupe. Modifiez la politique de confiance S3 du groupe pour spécifier les utilisateurs de confiance autorisés à assumer le groupe avec l'API AssumeRole.

Les informations d'identification de sécurité temporaires créées lors de l'adoption de ce groupe sont valides pour une durée limitée. La session dure entre 15 minutes et 12 heures, et la durée par défaut est d'une heure. Lorsque vous retirez l'utilisateur de la stratégie d'approbation S3 du groupe, l'utilisateur ne peut plus adopter

ce groupe.

Étapes

1. Sélectionnez **Gestion des accès** > **Groupes**.
2. Cliquez sur le nom du groupe.
3. Sélectionnez l'onglet **Stratégie de confiance S3**.
4. Ajoutez votre politique de confiance S3, y compris une liste d'utilisateurs pouvant effectuer AssumeRole.
5. Sélectionnez **Save changes**.
6. Sélectionnez l'onglet **Stratégie de groupe S3**.
7. ${post_edited_translations.segment}
8. Sélectionnez **Save changes**.

Exemple d'une AssumeRole politique de fiducie S3

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Principal": {
                "AWS": [
                    "urn:sgws:identity::1234567890:user/user1",
                    "arn:aws:iam::1234567890:user/user2"
                ]
            }
        }
    ]
}
```

Une fois la configuration terminée, les utilisateurs listés dans la stratégie d'approbation S3 peuvent effectuer AssumeRole et recevoir des informations d'identification. Les autorisations finales sont déterminées par la stratégie de groupe, la stratégie de compartiment et la stratégie de session. Pour plus d'informations, consultez "Utilisez les politiques d'accès".

Gérer les utilisateurs locataires de StorageGRID

Vous pouvez créer des utilisateurs locaux et les affecter à des groupes locaux afin de définir les fonctionnalités auxquelles ces utilisateurs peuvent accéder. Vous pouvez également importer des utilisateurs fédérés. Le Tenant Manager inclut 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 Tenant Manager ni 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 de fédération de grille**, vous avez examiné le flux de travail et les considérations pour "clonage des groupes de locataires et des utilisateurs", et vous êtes connecté à la grille source du locataire.

${post_edited_translations.segment}

${post_edited_translations.segment}

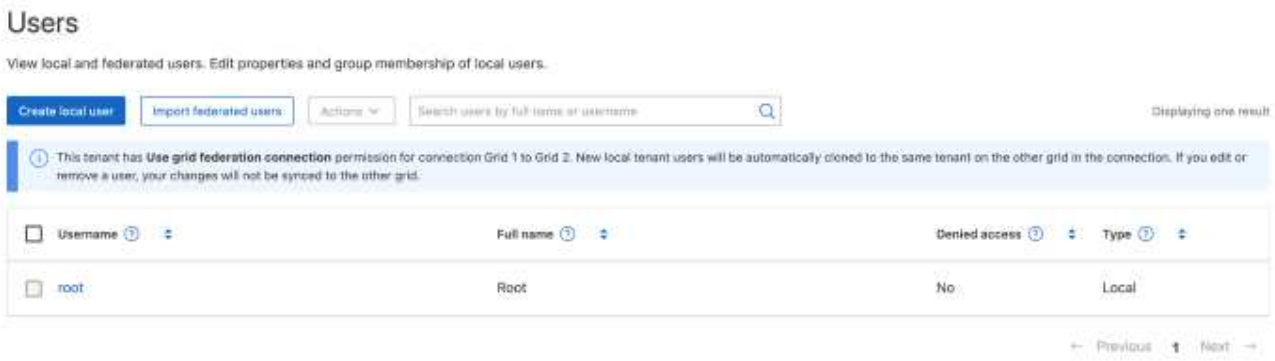
Les utilisateurs S3 qui n'appartiennent à aucun groupe ne disposent pas d'autorisations de gestion et aucune politique de groupe S3 ne leur est appliquée. Ces utilisateurs peuvent disposer d'un accès aux compartiments S3 accordé via une politique de compartiment.

Accédez à l'assistant de création d'utilisateur

Étapes

1. ${post_edited_translations.segment}

   Si votre compte locataire dispose de l'autorisation **Utiliser la connexion de fédération de grilles**, 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**.

Saisissez vos identifiants

Étapes

1. ${post_edited_translations.segment}

Champ	Description
${post_edited_translations.segment}	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	${post_edited_translations.segment} ${post_edited_translations.segment}
Mot de passe et confirmation du mot de passe	${post_edited_translations.segment}
${post_edited_translations.segment}	Sélectionnez **Oui** pour empêcher cet utilisateur de se connecter au compte locataire, même s'il peut encore appartenir à un ou plusieurs groupes. ${post_edited_translations.segment}

2. Sélectionnez **Continue**.

Attribuer aux groupes

Étapes

1. Attribuez 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 ne disposeront d'aucune autorisation de gestion. Les autorisations sont cumulatives. Les utilisateurs disposeront de toutes les autorisations pour tous les groupes auxquels ils appartiennent. Voir "${post_edited_translations.segment}".

2. Sélectionnez **Créer un utilisateur**.

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

3. ${post_edited_translations.segment}

${post_edited_translations.segment}

Étapes

1. ${post_edited_translations.segment}
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.

   ${post_edited_translations.segment}

   - ${post_edited_translations.segment}

- Au besoin, un message de bannière indique si des utilisateurs n'ont pas été clonés vers le locataire sur la grille de destination. Vous pouvez ${post_edited_translations.segment}.

3. ${post_edited_translations.segment}
   a. Cochez la case pour l'utilisateur.
   b. Sélectionnez **Actions** > **Modifier le nom complet**.
   c. Saisissez le nouveau nom.
   d. ${post_edited_translations.segment}
4. ${post_edited_translations.segment}
   - Sélectionnez le nom d'utilisateur.
   - ${post_edited_translations.segment}
5. ${post_edited_translations.segment}
   - ${post_edited_translations.segment}
   - Nom d'utilisateur
   - ${post_edited_translations.segment}
   - ${post_edited_translations.segment}
   - Mode d'accès
   - Adhésion au groupe
   - ${post_edited_translations.segment}
     - ${post_edited_translations.segment}
     - Une bannière bleue indique que si vous modifiez cet utilisateur, vos modifications ne seront pas synchronisées avec l'autre grille.
6. Modifiez les paramètres utilisateur selon vos besoins. Consultez ${post_edited_translations.segment} pour obtenir des détails sur les informations à 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 changer le nom d'utilisateur.

   b. ${post_edited_translations.segment}
   c. Dans l'onglet **Accès**, sélectionnez **Non** pour autoriser l'utilisateur à se connecter ou **Oui** pour l'empêcher de se connecter. Ensuite, sélectionnez **Enregistrer les modifications**.
   d. Dans l'onglet **Touches d'accès**, sélectionnez **Créer une clé** et suivez les instructions pour "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 le retirer de groupes. Ensuite, sélectionnez **Enregistrer les modifications**.
7. ${post_edited_translations.segment}

Importer les utilisateurs fédérés

Vous pouvez importer un ou plusieurs utilisateurs fédérés, jusqu'à un maximum de 100 utilisateurs, directement dans la page Utilisateurs.

Étapes

1. ${post_edited_translations.segment}
2. Sélectionnez **Importer les utilisateurs fédérés**.
3. Saisissez l'UUID ou le nom d'utilisateur d'un ou de plusieurs utilisateurs fédérés.

   Pour plusieurs entrées, ajoutez chaque UUID ou nom d'utilisateur sur une nouvelle ligne.

4. Sélectionnez **Importer**.

   Si l'importation dans le champ Utilisateurs échoue pour un ou plusieurs utilisateurs, procédez comme suit :

   a. Développez **Utilisateurs non importés** et sélectionnez **Copier les utilisateurs**.
   b. Réessayez l'importation en sélectionnant **Précédent** et en collant les utilisateurs copiés dans la boîte de dialogue **Import federated users**.

   Après la fermeture de la boîte de dialogue **Importer les utilisateurs fédérés**, les informations des utilisateurs fédérés s'affichent sur la page Utilisateurs pour les utilisateurs importés avec succès.

${post_edited_translations.segment}

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

${post_edited_translations.segment}

Étapes

1. ${post_edited_translations.segment}
2. Cochez la case correspondant à l'utilisateur que vous souhaitez dupliquer.
3. ${post_edited_translations.segment}
4. Consultez ${post_edited_translations.segment} pour obtenir des détails sur les informations à saisir.
5. Sélectionnez **Créer un utilisateur**.

${post_edited_translations.segment}

${post_edited_translations.segment}

1. ${post_edited_translations.segment}
2. Sélectionnez **Actions** > **Cloner les utilisateurs**.
3. Consultez l'état de l'opération de clonage depuis la page de détails de chaque utilisateur que vous clonez.

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

${post_edited_translations.segment}

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 de fédération de grilles** et que vous supprimez un utilisateur local, StorageGRID ne supprimera pas l'utilisateur correspondant sur l'autre grille. Si vous devez maintenir ces informations synchronisées, vous devez supprimer le même utilisateur des deux grilles.

${post_edited_translations.segment}

Étapes

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
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**.