Gestion de l'accès au système pour les utilisateurs locataires

StorageGRID 11.5

NetApp
April 11, 2024

This PDF was generated from https://docs.netapp.com/fr-fr/storagegrid-115/tenant/guidelines-for-configuring-openldap-server.html on April 11, 2024. Always check docs.netapp.com for the latest.

Sommaire

Gestion de l’accès au système pour les utilisateurs locataires

Vous accordez aux utilisateurs l’accès à un compte de tenant en important des groupes à partir d’un référentiel d’identité fédéré et en attribuant des autorisations de gestion. Vous pouvez également créer des groupes et des utilisateurs de locataires locaux, sauf si l’authentification unique (SSO) est en vigueur pour l’ensemble du système StorageGRID.

- "Utilisation de la fédération des identités"
- "Gestion des groupes"
- "Gestion des utilisateurs locaux"

Utilisation de 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.

- "Configuration d’un référentiel d’identité fédéré"
- "Forcer la synchronisation avec le référentiel d’identité"
- "Désactivation de la fédération des identités"

Configuration d’un référentiel d’identité fédéré

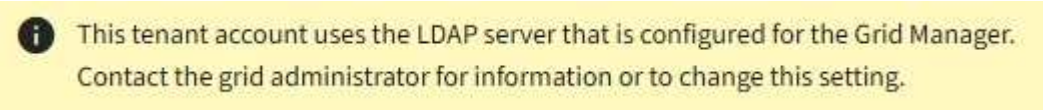
Vous pouvez configurer la fédération des identités si vous souhaitez que les groupes de locataires et les utilisateurs soient gérés dans un autre système, tel qu’Active Directory, OpenLDAP ou Oracle Directory Server.

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l’aide d’un navigateur pris en charge.
- Vous devez disposer d’autorisations d’accès spécifiques.
- Vous devez utiliser Active Directory, OpenLDAP ou Oracle Directory Server comme fournisseur d’identité. Si vous souhaitez utiliser un service LDAP v3 non répertorié, contactez le support technique.
- Si vous prévoyez d’utiliser TLS (transport Layer Security) pour les communications avec le serveur LDAP, le fournisseur d’identité doit utiliser TLS 1.2 ou 1.3.

Description de la tâche

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.



Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **identity federation**.
2. Sélectionnez **Activer la fédération d'identités**.
3. Dans la section Type de service LDAP, sélectionnez **Active Directory**, **OpenLDAP** ou **Other**.

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

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

4. Si vous avez sélectionné **autre**, renseignez les champs de la section attributs LDAP.
   - **Nom unique utilisateur** : nom de l'attribut qui contient l'identifiant unique d'un utilisateur LDAP. Cet attribut est équivalent à `sAMAccountName` Pour Active Directory et `uid` Pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `uid`.
   - **UUID d'utilisateur** : nom de l'attribut qui contient l'identifiant unique permanent d'un utilisateur LDAP. Cet attribut est équivalent à `objectGUID` Pour Active Directory et `entryUUID` Pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `nsuniqueid`. La valeur de chaque utilisateur pour l'attribut spécifié doit être un nombre hexadécimal à 32 chiffres au format 16 octets ou chaîne, où les tirets sont ignorés.
   - **Nom unique de groupe** : nom de l'attribut qui contient l'identifiant unique d'un groupe LDAP. Cet attribut est équivalent à `sAMAccountName` Pour Active Directory et `cn` Pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `cn`.
   - **UUID de groupe** : nom de l'attribut qui contient l'identificateur unique permanent d'un groupe LDAP. Cet attribut est équivalent à `objectGUID` Pour Active Directory et `entryUUID` Pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `nsuniqueid`. La valeur de chaque groupe pour l'attribut spécifié doit être un nombre hexadécimal à 32 chiffres au format 16 octets ou chaîne, où les tirets sont ignorés.
5. Dans la section configurer le serveur LDAP, entrez les informations de serveur LDAP et de connexion réseau requises.
   - **Nom d'hôte** : le nom d'hôte du serveur ou l'adresse IP du serveur LDAP.
   - **Port** : port utilisé pour se connecter au serveur LDAP. Le port par défaut de STARTTLS est 389 et le port par défaut de LDAPS est 636. Cependant, vous pouvez utiliser n'importe quel port tant que votre pare-feu est configuré correctement.
   - **Nom d'utilisateur** : chemin complet du nom distinctif (DN) de l'utilisateur qui se connectera au serveur LDAP. Pour Active Directory, vous pouvez également spécifier le nom de connexion bas niveau ou le nom principal d'utilisateur.

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

     - `sAMAccountName` ou `uid`
     - `objectGUID`, `entryUUID`, ou `nsuniqueid`
     - `cn`
     - `memberOf` ou `isMemberOf`
   - **Mot de passe** : mot de passe associé au nom d'utilisateur.
   - **DN de base de groupe** : chemin complet du nom distinctif (DN) pour une sous-arborescence LDAP que vous voulez rechercher des groupes. Dans l'exemple Active Directory (ci-dessous), tous les

groupes dont le nom unique est relatif au DN de base (DC=storagegrid,DC=exemple,DC=com) peuvent être utilisés comme groupes fédérés.

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

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

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

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

     Cette option n'est pas prise en charge si votre serveur Active Directory applique la signature LDAP. Vous devez utiliser STARTTLS ou LDAPS.

7. Si vous avez sélectionné STARTTLS ou LDAPS, choisissez le certificat utilisé pour sécuriser la connexion.
   - **Utilisez le certificat CA du système d'exploitation** : utilisez le certificat CA par défaut installé sur le système d'exploitation pour sécuriser les connexions.
   - **Utilisez un certificat d'autorité de certification personnalisé** : utilisez un certificat de sécurité personnalisé.

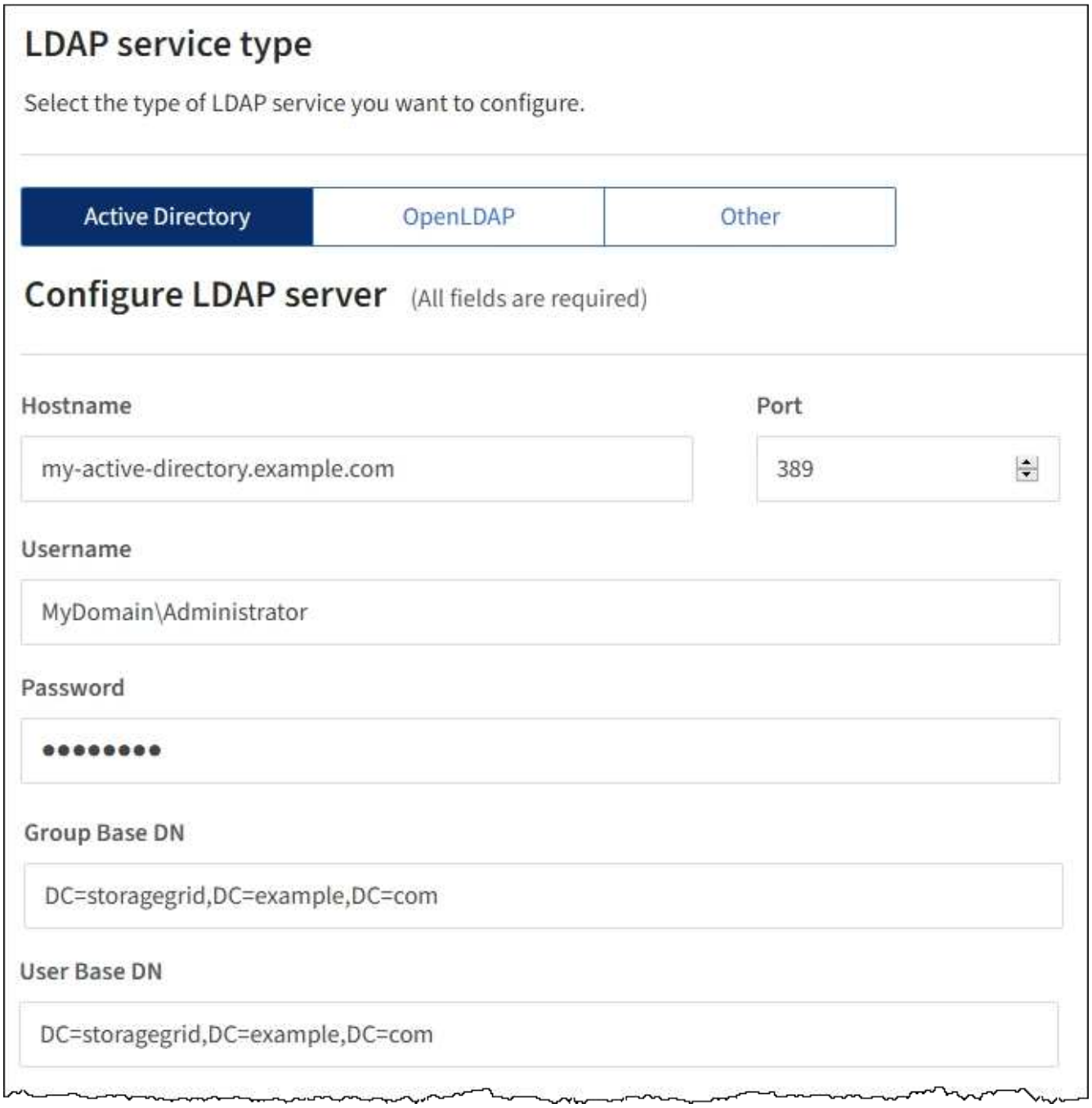
     Si vous sélectionnez ce paramètre, copiez et collez le certificat de sécurité personnalisé dans la zone de texte certificat de l'autorité de certification.

8. Sélectionnez **Tester la connexion** pour valider vos paramètres de connexion pour le serveur LDAP.

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

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

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



Informations associées

"Autorisations de gestion des locataires"

"Instructions de configuration d'un serveur OpenLDAP"

Instructions de configuration d'un serveur OpenLDAP

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

Recouvrements de memberOf et de raffint

Les recouvrements de membre et de raffinage doivent être activés. Pour plus d'informations, reportez-vous

aux instructions relatives à la maintenance de l'adhésion inverse au groupe dans le Guide de l'administrateur pour OpenLDAP.

Indexation

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

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

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

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

Forcer la synchronisation avec le référentiel d'identité

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

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.
- Le référentiel d'identité enregistré doit être activé.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **identity federation**.

   La page fédération des identités s'affiche. Le bouton **Sync Server** se trouve en haut à droite de la page.

   > Si le référentiel d'identité enregistré n'est pas activé, le bouton **Sync Server** n'est pas actif.

2. Sélectionnez **serveur de synchronisation**.

   Un message de confirmation s'affiche pour indiquer que la synchronisation a démarré correctement.

Informations associées

"Autorisations de gestion des locataires"

Désactivation de la fédération des identités

Si vous avez configuré un service de fédération des identités pour ce locataire, vous pouvez désactiver temporairement ou définitivement la fédération des identités pour les

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

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

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

- Les utilisateurs fédérés ne pourront pas se connecter.
- Les utilisateurs fédérés qui sont actuellement connectés conserveront l'accès au compte du locataire 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 fera pas.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **identity federation**.
2. Décochez la case **Activer la fédération d'identités**.
3. Sélectionnez **Enregistrer**.

Informations associées

"Autorisations de gestion des locataires"

Gestion des groupes

Vous attribuez des autorisations aux groupes d'utilisateurs pour contrôler les tâches que les utilisateurs peuvent effectuer. Vous pouvez importer des groupes fédérés à partir d'un référentiel d'identité, tel qu'Active Directory ou OpenLDAP, ou créer des groupes locaux.

> Si l'authentification unique est activée pour votre système StorageGRID, les utilisateurs locaux ne pourront pas se connecter au gestionnaire de locataires, même s'ils peuvent accéder aux ressources S3 et Swift, en fonction des autorisations de groupe.

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. L'application des modifications peut prendre jusqu'à 15 minutes à cause de la mise en cache.

Autorisations	Description
Accès racine	Donne un accès complet au gestionnaire des locataires et à l'API de gestion des locataires. **Remarque :** les utilisateurs de Swift doivent disposer de l'autorisation d'accès racine pour se connecter au compte du 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 propres identifiants S3	Locataires S3 uniquement. 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**.
Gérer toutes les rubriques	• 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 **seaux**. • 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 pouvez uniquement attribuer l'autorisation gérer toutes les rubriques 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.

Autorisations	Description
Gérer les terminaux	Locataires S3 uniquement. Permet aux utilisateurs d'utiliser le Gestionnaire de locataires ou l'API de gestion des locataires pour créer ou modifier des terminaux, 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**.

Informations associées

"Utilisation de S3"

"Utiliser Swift"

Création de 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.

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur pris en charge.
- Vous devez appartenir à un groupe d'utilisateurs qui dispose de l'autorisation accès racine.
- Si vous envisagez d'importer un groupe fédéré, vous avez configuré la fédération des identités et le groupe fédéré existe déjà dans le référentiel d'identité configuré.

Étapes

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

2. Sélectionnez **Créer groupe**.
3. 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.

4. 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.
5. Sélectionnez **Continuer**.
6. Sélectionnez un mode d'accès. 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.
   - **Read-write** (valeur 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 effectuer d'opérations dans le Gestionnaire des locataires ou l'API de gestion des locataires. Les utilisateurs locaux en lecture seule peuvent modifier leurs propres mots de passe.
7. Sélectionnez les autorisations de groupe pour ce groupe.

   Reportez-vous aux informations sur les autorisations de gestion des locataires.

8. Sélectionnez **Continuer**.
9. Sélectionnez une stratégie de groupe pour déterminer quelles autorisations d'accès S3 seront attribuées aux membres de ce groupe.
   - **Pas d'accès 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 ont 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 ont accès aux ressources S3, y compris aux 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.
   - **Custom** : les utilisateurs du groupe disposent des autorisations que vous spécifiez dans la zone de texte. Pour plus d'informations sur les règles de groupe, notamment la syntaxe du langage et des exemples, reportez-vous aux instructions de mise en œuvre d'une application client S3.
10. 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.

    Dans cet exemple, les membres du groupe sont uniquement autorisés à répertorier et accéder à un dossier correspondant à leur nom d'utilisateur (préfixe de clé) dans le champ spécifié. Notez que les autorisations d'accès à partir d'autres stratégies de groupes et de la règle de compartiment doivent être

prises en compte lors de la détermination de la confidentialité de ces dossiers.

11. Sélectionnez le bouton qui s'affiche, selon que vous créez un groupe fédéré ou local :

    - Groupe fédéré : **Créer groupe**
    - Groupe local : **Continuer**

    Si vous créez un groupe local, STEP 4 (Ajouter des utilisateurs) apparaît après avoir sélectionné **Continuer**. Cette étape n'apparaît pas pour les groupes fédérés.

12. Cochez la case de chaque utilisateur que vous souhaitez ajouter au groupe, puis sélectionnez **Créer groupe**.

    Vous pouvez également enregistrer le groupe sans ajouter d'utilisateurs. Vous pouvez ajouter des utilisateurs au groupe ultérieurement ou sélectionner le groupe lorsque vous ajoutez de nouveaux utilisateurs.

13. Sélectionnez **Terminer**.

    Le groupe que vous avez créé apparaît dans la liste des groupes. L'application des modifications peut prendre jusqu'à 15 minutes à cause de la mise en cache.

Informations associées

"Autorisations de gestion des locataires"

"Utilisation de S3"

Création de 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.

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur pris en charge.
- Vous devez appartenir à un groupe d'utilisateurs qui dispose de l'autorisation accès racine.
- Si vous envisagez d'importer un groupe fédéré, vous avez configuré la fédération des identités et le groupe fédéré existe déjà dans le référentiel d'identité configuré.

Étapes

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

2. Sélectionnez **Créer groupe**.
3. 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.

4. 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.

5. Sélectionnez **Continuer**.
6. Sélectionnez un mode d'accès. 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.
   - **Read-write** (valeur 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 effectuer d'opérations dans le Gestionnaire des locataires ou l'API de gestion des locataires. Les utilisateurs locaux en lecture seule peuvent modifier leurs propres mots de passe.
7. Définissez l'autorisation Groupe.
   - Cochez la case **accès racine** si les utilisateurs doivent se connecter au Gestionnaire de locataires ou à l'API de gestion des locataires. (Valeur par défaut)
   - Désélectionnez la case **accès racine** si les utilisateurs n'ont pas besoin d'accéder au Gestionnaire de locataires ou à l'API de gestion des locataires. Par exemple, désélectionnez la case à cocher pour les applications qui n'ont pas besoin d'accéder au locataire. Attribuez ensuite l'autorisation **Swift Administrator** pour permettre à ces utilisateurs de gérer des conteneurs et des objets.
8. Sélectionnez **Continuer**.
9. Cochez la case **Administrateur Swift** si l'utilisateur doit pouvoir utiliser l'API REST Swift.

   Les utilisateurs Swift doivent disposer de l'autorisation d'accès racine pour accéder au gestionnaire de locataires. Toutefois, l'autorisation accès racine ne permet pas aux utilisateurs de s'authentifier auprès de l'API REST Swift pour créer des conteneurs et ingérer des objets. Les utilisateurs doivent disposer de l'autorisation Administrateur Swift pour s'authentifier dans l'API REST de Swift.

10. Sélectionnez le bouton qui s'affiche, selon que vous créez un groupe fédéré ou local :
    - Groupe fédéré : **Créer groupe**
    - Groupe local : **Continuer**

      Si vous créez un groupe local, STEP 4 (Ajouter des utilisateurs) apparaît après avoir sélectionné **Continuer**. Cette étape n'apparaît pas pour les groupes fédérés.

11. Cochez la case de chaque utilisateur que vous souhaitez ajouter au groupe, puis sélectionnez **Créer groupe**.

    Vous pouvez également enregistrer le groupe sans ajouter d'utilisateurs. Vous pouvez ajouter des utilisateurs au groupe ultérieurement ou sélectionner le groupe lorsque vous créez de nouveaux utilisateurs.

12. Sélectionnez **Terminer**.

    Le groupe que vous avez créé apparaît dans la liste des groupes. L'application des modifications peut prendre jusqu'à 15 minutes à cause de la mise en cache.

Informations associées

"Autorisations de gestion des locataires"

"Utiliser Swift"

Affichage et modification des détails du groupe

Lorsque vous affichez les détails d'un groupe, vous pouvez modifier le nom d'affichage, les autorisations, les règles et les utilisateurs appartenant au groupe.

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur pris en charge.
- Vous devez appartenir à un groupe d'utilisateurs qui dispose de l'autorisation accès racine.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **Groups**.
2. Sélectionnez le nom du groupe dont vous souhaitez afficher ou modifier les détails.

   Vous pouvez également sélectionner **actions** > **Afficher les détails du groupe**.

   La page des détails du groupe s'affiche. L'exemple suivant montre la page des détails du groupe S3.

Groups > Applications

Overview

Display name:	**Applications**
Unique name:	**group/Applications**
Type:	**Local**
Access mode:	**Read-write**
Permissions:	**Root Access**
S3 Policy:	**None**
Number of users in this group:	**0**

Group permissions | S3 group policy | Users

Manage group permissions

Select an access mode for this group and select one or more permissions.

Access mode

Select whether users can change settings and perform operations or whether they can only view settings and features.

(●) Read-write ( ) Read-only

Group permissions

Select the tenant account permissions you want to assign to this group.

[x] **Root Access**

Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.

[x] **Manage All Buckets**

Allows users to change settings of all S3 buckets (or Swift containers) in this account.

[x] **Manage Endpoints**

Allows users to configure endpoints for platform services.

[x] **Manage Your Own S3 Credentials**

Allows users to create and delete their own S3 access keys.

Save changes

3. Modifiez les paramètres du groupe selon vos besoins.

> Pour vous assurer que vos modifications sont enregistrées, sélectionnez **Enregistrer les modifications** après avoir effectué des modifications dans chaque section. Lorsque vos modifications sont enregistrées, un message de confirmation s'affiche dans le coin supérieur droit de la page.

   a. Vous pouvez également sélectionner le nom d'affichage ou l'icône de modification pour mettre à jour le nom d'affichage.

      Vous ne pouvez pas modifier le nom unique d'un groupe. Vous ne pouvez pas modifier le nom d'affichage d'un groupe fédéré.

   b. Si vous le souhaitez, mettez à jour les autorisations.

   c. Pour les règles de groupe, apportez les modifications appropriées à votre locataire S3 ou Swift.

      - Si vous modifiez un groupe pour un locataire S3, vous pouvez choisir une autre règle de groupe S3. Si vous sélectionnez une règle S3 personnalisée, mettez à jour la chaîne JSON si nécessaire.
      - Si vous modifiez un groupe pour un locataire Swift, vous pouvez sélectionner ou désélectionner la case à cocher **Administrateur Swift**.

        Pour plus d'informations sur l'autorisation de l'administrateur Swift, reportez-vous aux instructions de création de groupes pour un locataire Swift.

   d. Si vous le souhaitez, vous pouvez ajouter ou supprimer des utilisateurs.

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

   L'application des modifications peut prendre jusqu'à 15 minutes à cause de la mise en cache.

Informations associées

"Création de groupes pour un locataire S3"

"Création de groupes pour un locataire Swift"

Ajout d'utilisateurs à un groupe local

Vous pouvez ajouter des utilisateurs à un groupe local si nécessaire.

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur pris en charge.
- Vous devez appartenir à un groupe d'utilisateurs qui dispose de l'autorisation accès racine.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **Groups**.
2. Sélectionnez le nom du groupe local auquel vous souhaitez ajouter des utilisateurs.

   Vous pouvez également sélectionner **actions** > **Afficher les détails du groupe**.

   La page des détails du groupe s'affiche.

Groups > Applications

Overview

Display name:	**Applications**
Unique name:	**group/Applications**
Type:	**Local**
Access mode:	**Read-write**
Permissions:	**Root Access**
S3 Policy:	**None**
Number of users in this group:	**0**

Group permissions | S3 group policy | Users

Manage group permissions

Select an access mode for this group and select one or more permissions.

Access mode

Select whether users can change settings and perform operations or whether they can only view settings and features.

(●) Read-write ( ) Read-only

Group permissions

Select the tenant account permissions you want to assign to this group.

[x] **Root Access**

Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.

[x] **Manage All Buckets**

Allows users to change settings of all S3 buckets (or Swift containers) in this account.

[x] **Manage Endpoints**

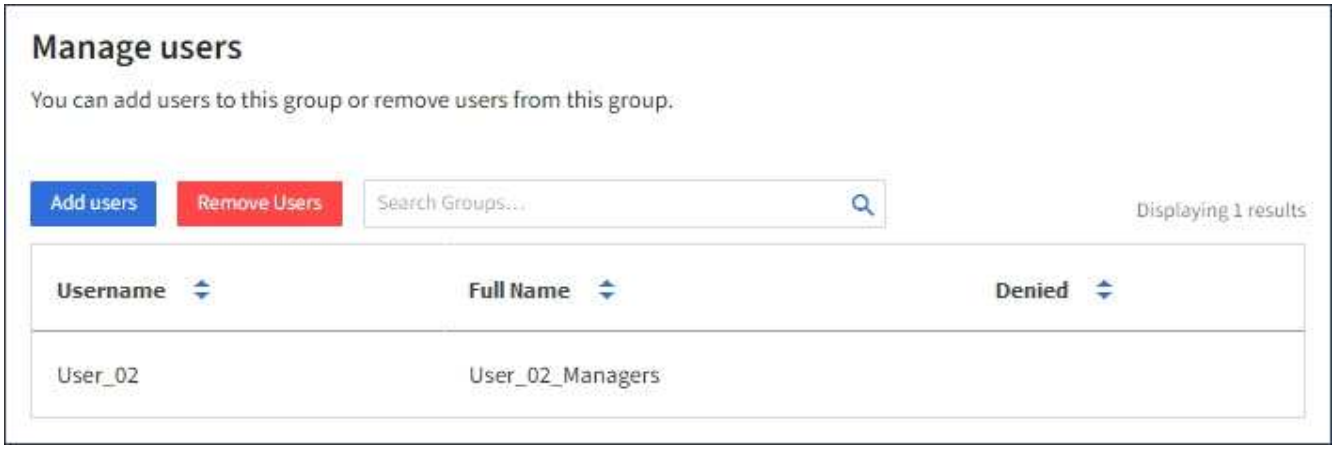
Allows users to configure endpoints for platform services.

[x] **Manage Your Own S3 Credentials**

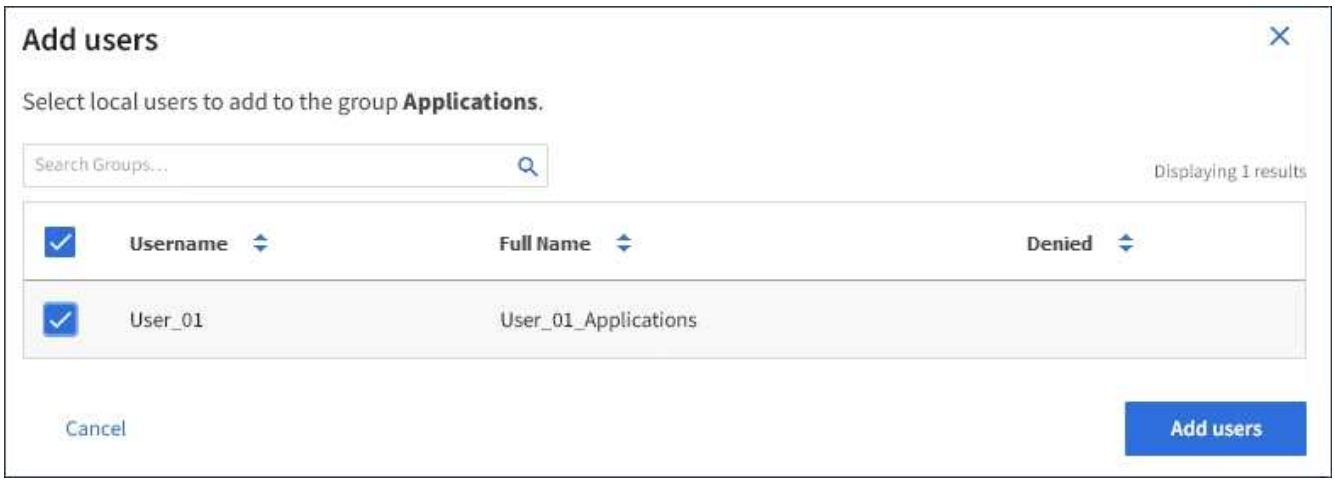
Allows users to create and delete their own S3 access keys.

Save changes

3. Sélectionnez **gérer les utilisateurs**, puis **Ajouter des utilisateurs**.



4. Sélectionnez les utilisateurs que vous souhaitez ajouter au groupe, puis sélectionnez **Ajouter utilisateurs**.



Un message de confirmation s'affiche dans le coin supérieur droit de la page. L'application des modifications peut prendre jusqu'à 15 minutes à cause de la mise en cache.

Modification d'un nom de groupe

Vous pouvez modifier le nom d'affichage d'un groupe. Vous ne pouvez pas modifier le nom unique d'un groupe.

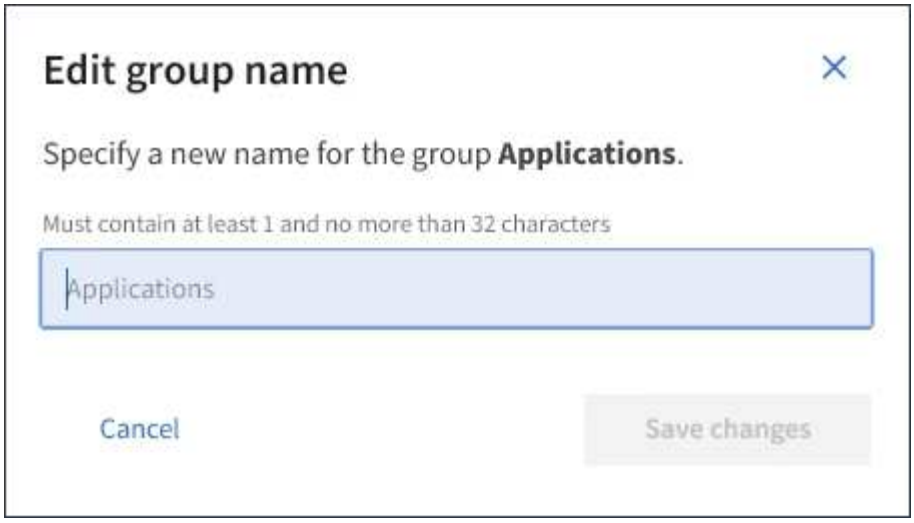
Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur pris en charge.
- Vous devez appartenir à un groupe d'utilisateurs qui dispose de l'autorisation accès racine.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **Groups**.
2. Cochez la case du groupe dont vous souhaitez modifier le nom d'affichage.
3. Sélectionnez **actions** > **Modifier le nom du groupe**.

   La boîte de dialogue Modifier le nom du groupe s'affiche.



4. Si vous modifiez un groupe local, mettez à jour le nom d'affichage selon vos besoins.

   Vous ne pouvez pas modifier le nom unique d'un groupe. Vous ne pouvez pas modifier le nom d'affichage d'un groupe fédéré.

5. Sélectionnez **Enregistrer les modifications**.

   Un message de confirmation s'affiche dans le coin supérieur droit de la page. L'application des modifications peut prendre jusqu'à 15 minutes à cause de la mise en cache.

Informations associées

"Autorisations de gestion des locataires"

Duplication d'un groupe

Vous pouvez créer de nouveaux groupes plus rapidement en dupliquant un groupe existant.

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur pris en charge.
- Vous devez appartenir à un groupe d'utilisateurs qui dispose de l'autorisation accès racine.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **Groups**.
2. Cochez la case correspondant au groupe que vous souhaitez dupliquer.
3. Sélectionnez **Dupliquer le groupe**. Pour plus d'informations sur la création d'un groupe, consultez les instructions de création de groupes pour un locataire S3 ou pour un locataire Swift.
4. 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.

5. 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.
6. Sélectionnez **Continuer**.
7. Si nécessaire, modifiez les autorisations pour ce groupe.
8. Sélectionnez **Continuer**.
9. Si nécessaire, si vous copiez un groupe pour un locataire S3, vous pouvez sélectionner une autre stratégie à partir des boutons d'option **Ajouter une stratégie S3**. Si vous avez sélectionné une règle personnalisée, mettez à jour la chaîne JSON si nécessaire.
10. Sélectionnez **Créer groupe**.

Informations associées

"Création de groupes pour un locataire S3"

"Création de groupes pour un locataire Swift"

"Autorisations de gestion des locataires"

Suppression d'un groupe

Vous pouvez supprimer un groupe du système. Les utilisateurs appartenant uniquement à ce groupe ne pourront plus se connecter au Gestionnaire de locataires ni utiliser le compte de tenant.

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur pris en charge.
- Vous devez appartenir à un groupe d'utilisateurs qui dispose de l'autorisation accès racine.

Étapes

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

2. Cochez les cases des groupes que vous souhaitez supprimer.
3. Sélectionnez **actions** > **Supprimer le groupe**.

   Un message de confirmation s'affiche.

4. Sélectionnez **Supprimer le groupe** pour confirmer la suppression des groupes indiqués dans le message de confirmation.

   Un message de confirmation s'affiche dans le coin supérieur droit de la page. L'application des modifications peut prendre jusqu'à 15 minutes à cause de la mise en cache.

Informations associées

"Autorisations de gestion des locataires"

Gestion des 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.

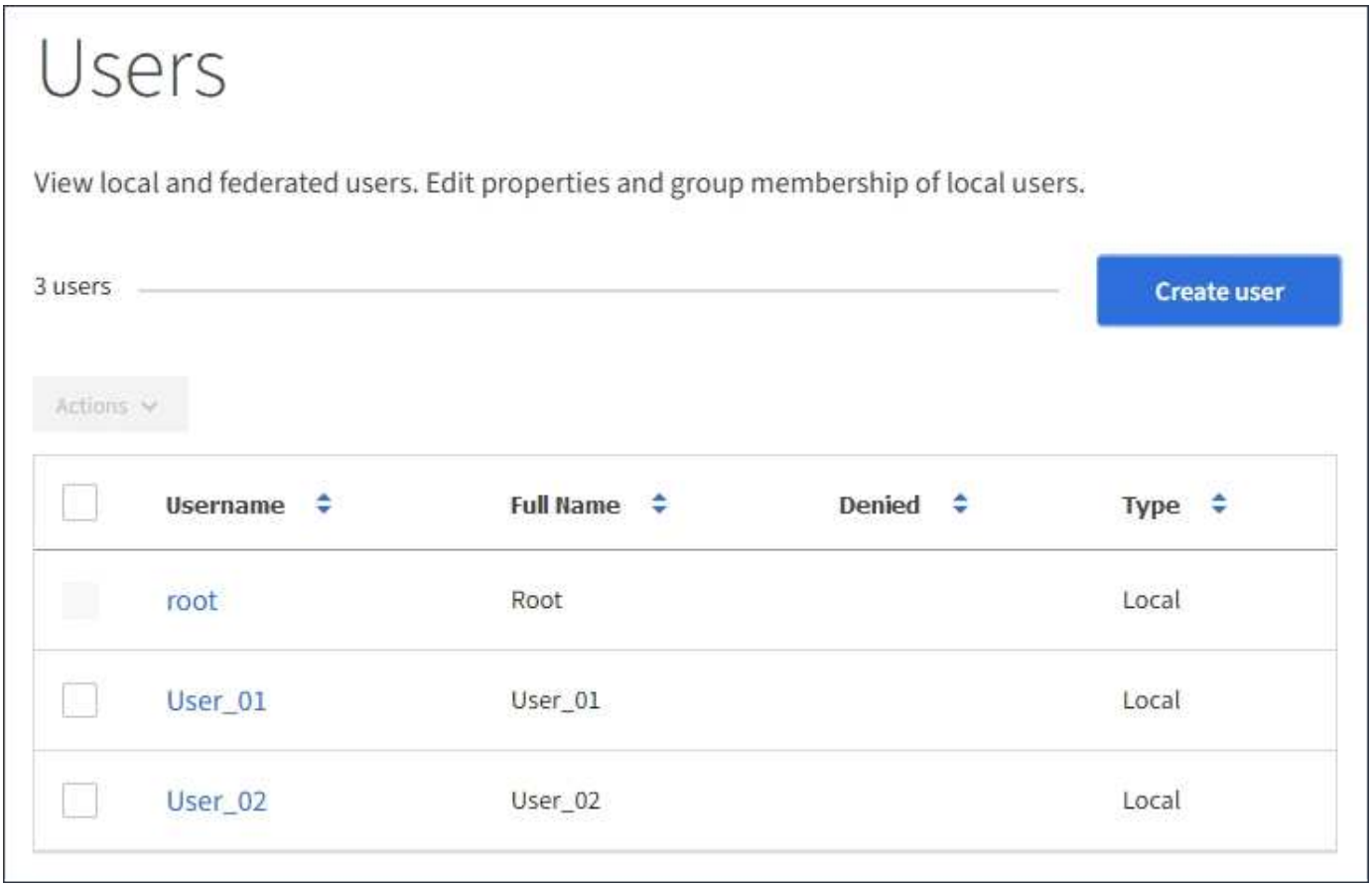
Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur pris en charge.
- Vous devez appartenir à un groupe d'utilisateurs en lecture/écriture doté de l'autorisation accès racine.

> Si l'authentification unique 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, même s'ils peuvent utiliser les applications client S3 ou Swift pour accéder aux ressources du locataire en fonction des autorisations de groupe.

Accès à la page utilisateurs

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



Création d'utilisateurs locaux

Vous pouvez créer des utilisateurs locaux et les attribuer à un ou plusieurs groupes locaux pour contrôler leurs autorisations d'accès.

Les utilisateurs S3 qui n'appartiennent à aucun groupe ne disposent 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 n'appartenant à aucun groupe ne disposent d'autorisations de gestion ni d'un accès au conteneur Swift.

Étapes

1. Sélectionnez **Créer utilisateur**.
2. Renseignez les champs suivants.
    - **Nom complet** : le nom complet de cet utilisateur, par exemple le prénom et le nom de famille d'une personne ou le nom d'une application.
    - **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.
    - **Mot de passe** : mot de passe utilisé lorsque l'utilisateur ouvre une session.
    - **Confirmer le mot de passe** : saisissez le même mot de passe que celui que vous avez saisi dans le

champ Mot de passe.

- **Refuser l'accès**: Si vous sélectionnez **Oui**, cet utilisateur ne peut pas se connecter au compte de tenant, même si l'utilisateur peut toujours appartenir à un ou plusieurs groupes.

  Par exemple, vous pouvez utiliser cette fonction pour suspendre temporairement la connexion d'un utilisateur.

3. Sélectionnez **Continuer**.
4. Attribuez l'utilisateur à un ou plusieurs groupes locaux.

   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.

5. Sélectionnez **Créer utilisateur**.

   L'application des modifications peut prendre jusqu'à 15 minutes à cause de la mise en cache.

Modification des détails de l'utilisateur

Lorsque vous modifiez les détails d'un utilisateur, vous pouvez modifier le nom complet et le mot de passe de l'utilisateur, ajouter l'utilisateur à différents groupes et empêcher l'utilisateur d'accéder au locataire.

Étapes

1. Dans la liste utilisateurs, sélectionnez le nom de l'utilisateur dont vous souhaitez afficher ou modifier les détails.

   Vous pouvez également cocher la case de l'utilisateur, puis sélectionner **actions** > **Afficher les détails de l'utilisateur**.

2. Apportez les modifications nécessaires aux paramètres utilisateur.
   a. Modifiez le nom complet de l'utilisateur selon vos besoins en sélectionnant le nom complet ou l'icône de modification Dans la section vue d'ensemble.

      Vous ne pouvez pas modifier le nom d'utilisateur.

   b. Dans l'onglet **Mot de passe**, modifiez le mot de passe de l'utilisateur si nécessaire.
   c. Dans l'onglet **Access**, permettez à l'utilisateur de se connecter (sélectionnez **non**) ou d'empêcher l'utilisateur de se connecter (sélectionnez **Oui**) selon les besoins.
   d. Dans l'onglet **groupes**, ajoutez l'utilisateur aux groupes ou supprimez l'utilisateur des groupes si nécessaire.
   e. Si nécessaire pour chaque section, sélectionnez **Enregistrer les modifications**.

      L'application des modifications peut prendre jusqu'à 15 minutes à cause de la mise en cache.

Duplication des utilisateurs locaux

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

Étapes

1. Dans la liste utilisateurs, sélectionnez l'utilisateur que vous souhaitez dupliquer.
2. Sélectionnez **Dupliquer l'utilisateur**.
3. Modifiez les champs suivants pour le nouvel utilisateur.
   - **Nom complet** : le nom complet de cet utilisateur, par exemple le prénom et le nom de famille d'une personne ou le nom d'une application.
   - **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.
   - **Mot de passe** : mot de passe utilisé lorsque l'utilisateur ouvre une session.
   - **Confirmer le mot de passe** : saisissez le même mot de passe que celui que vous avez saisi dans le champ Mot de passe.
   - **Refuser l'accès**: Si vous sélectionnez **Oui**, cet utilisateur ne peut pas se connecter au compte de tenant, même si l'utilisateur peut toujours appartenir à un ou plusieurs groupes.

     Par exemple, vous pouvez utiliser cette fonction pour suspendre temporairement la connexion d'un utilisateur.
4. Sélectionnez **Continuer**.
5. Sélectionnez un ou plusieurs groupes locaux.

   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.
6. Sélectionnez **Créer utilisateur**.

   L'application des modifications peut prendre jusqu'à 15 minutes à cause de la mise en cache.

Suppression d'utilisateurs locaux

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

À l'aide du Gestionnaire de locataires, vous pouvez supprimer des utilisateurs locaux, mais pas des utilisateurs fédérés. Vous devez utiliser le référentiel d'identité fédéré pour supprimer des utilisateurs fédérés.

Étapes

1. Dans la liste utilisateurs, cochez la case de l'utilisateur local que vous souhaitez supprimer.
2. Sélectionnez **actions** > **Supprimer l'utilisateur**.
3. Dans la boîte de dialogue de confirmation, sélectionnez **Supprimer l'utilisateur** pour confirmer que vous souhaitez supprimer l'utilisateur du système.

   L'application des modifications peut prendre jusqu'à 15 minutes à cause de la mise en cache.

Informations associées

"Autorisations de gestion des locataires"

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

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

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