



# **Gestion des groupes**

## **StorageGRID**

NetApp

October 03, 2025

# Sommaire

- Gestion des groupes ..... 1
  - Autorisations de gestion des locataires ..... 1
  - Création de groupes pour un locataire S3 ..... 2
  - Création de groupes pour un locataire Swift ..... 5
  - Affichage et modification des détails du groupe ..... 7
  - Ajout d'utilisateurs à un groupe local ..... 9
  - Modification d'un nom de groupe ..... 11
  - Duplication d'un groupe ..... 12
  - Suppression d'un groupe ..... 13

# 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.  <b>Remarque :</b> 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  <b>Remarque :</b> les utilisateurs de Swift doivent disposer de l'autorisation Administrateur Swift pour effectuer toutes les opérations avec l'API REST Swift.

Autorisations	Description
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 <b>STORAGE (S3) &gt; My S3 Access Keys</b> .
Gérer toutes les rubriques	<ul style="list-style-type: none"> <li>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.</li> </ul> <p>Les utilisateurs qui ne disposent pas de cette autorisation ne voient pas l'option de menu <b>seaux</b>.</p> <ul style="list-style-type: none"> <li>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.</li> </ul> <p><b>Remarque :</b> 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.</p>
Gérer les terminaux	<p>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.</p> <p>Les utilisateurs qui ne disposent pas de cette autorisation ne voient pas l'option de menu <b>Platform services Endpoints</b>.</p>

#### 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**.

# Groups

Create and manage local and federated groups. Set group permissions to control access to specific pages and features.

2 groups Create group

Actions

<input type="checkbox"/>	Name	ID	Type	Access mode
<input type="checkbox"/>	Applications	22cc2e27-88ee-4461-a8c6-30b550beec0	Local	Read-write
<input type="checkbox"/>	Managers	8b15b131-1d21-4539-93ad-f2298347c4d8	Local	Read-write

Previous **1** Next

- Sélectionnez **Créer groupe**.
- 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.

- 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.
- Sélectionnez **Continuer**.
- 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.
- Sélectionnez les autorisations de groupe pour ce groupe.

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

- 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.

The screenshot shows the AWS IAM console interface for creating a group policy. On the left, four radio buttons are visible: 'No S3 Access', 'Read Only Access', 'Full Access', and 'Custom'. The 'Custom' option is selected, and a note below it states '(Must be a valid JSON formatted string.)'. On the right, a text area displays a JSON policy document. The policy consists of two statements: one for listing buckets with a condition on the s3:prefix, and another for allowing object actions on a specific folder within a bucket, also with a condition on the s3:prefix.

```
{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificFolder",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}
```

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**.

# Groups

Create and manage local and federated groups. Set group permissions to control access to specific pages and features.

2 groups Create group

Actions

<input type="checkbox"/>	Name	ID	Type	Access mode
<input type="checkbox"/>	Applications	22cc2e27-88ee-4461-a8c6-30b550beec0	Local	Read-write
<input type="checkbox"/>	Managers	8b15b131-1d21-4539-93ad-f2298347c4d8	Local	Read-write

Previous **1** Next

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.

## Overview

Display name:	<a href="#">Applications</a> 
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.

☒ **Root Access**

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

☒ **Manage All Buckets**

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

☒ **Manage Endpoints**

Allows users to configure endpoints for platform services.

☒ **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.

## Overview

Display name:	<a href="#">Applications</a> 
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.

☒ **Root Access**

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

☒ **Manage All Buckets**

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

☒ **Manage Endpoints**

Allows users to configure endpoints for platform services.

☒ **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**.

**Manage users**

You can add users to this group or remove users from this group.

**Add users** **Remove Users** Search Groups... Displaying 1 results

Username	Full Name	Denied
User_02	User_02_Managers	

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

**Add users** ×

Select local users to add to the group **Applications**.

Search Groups... Displaying 1 results

<input checked="" type="checkbox"/>	Username	Full Name	Denied
<input checked="" type="checkbox"/>	User_01	User_01_Applications	

**Cancel** **Add users**

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.

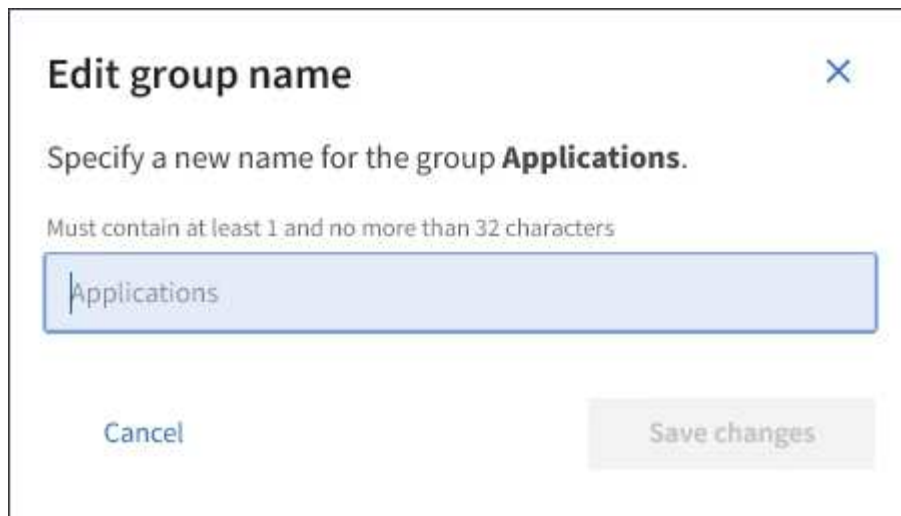
### Ce dont vous avez besoin

- 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.



**Edit group name** ✕

Specify a new name for the group **Applications**.

Must contain at least 1 and no more than 32 characters

Applications

Cancel Save changes

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**.

# Groups

Create and manage local and federated groups. Set group permissions to control access to specific pages and features.

2 groups

Create group

Actions

<input type="checkbox"/>	Name	ID	Type	Access mode
<input type="checkbox"/>	Applications	22cc2e27-88ee-4461-a8c6-30b550beee0	Local	Read-write
<input type="checkbox"/>	Managers	8b15b131-1d21-4539-93ad-f2298347c4d8	Local	Read-write

← Previous 1 Next →

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"](#)



## 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 DÉLICTELLE (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.