Manage tenant groups

StorageGRID 11.7

NetApp
August 30, 2024

Table of Contents

Manage tenant groups

Create groups for an S3 tenant

You can manage permissions for S3 user groups by importing federated groups or creating local groups.

Before you begin

- You are signed in to the Tenant Manager using a supported web browser.
- You belong to a user group that has the Root access permission.
- If you plan to import a federated group, you have configured identity federation, and the federated group already exists in the configured identity source.
- If your tenant account has the **Use grid federation connection** permission, you have reviewed the workflow and considerations for cloning tenant groups and users, and you are signed in to the tenant's source grid.

Access the Create group wizard

As your first step, access the Create group wizard.

Steps

1. Select **ACCESS MANAGEMENT** > **Groups**.
2. If your tenant account has the **Use grid federation connection** permission, confirm that a blue banner appears, indicating that new groups created on this grid will be cloned to the same tenant on the other grid in the connection. If this banner does not appear, you might be signed in to the tenant's destination grid.

3. Select **Create group**.

Choose a group type

You can create a local group or import a federated group.

Steps

1. Select the **Local group** tab to create a local group, or select the **Federated group** tab to import a group

from the previously configured identity source.

If single sign-on (SSO) is enabled for your StorageGRID system, users belonging to local groups will not be able to sign in to the Tenant Manager, although they can use client applications to manage the tenant's resources, based on group permissions.

2. Enter the group's name.
   - **Local group**: Enter both a display name and a unique name. You can edit the display name later.

     > If your tenant account has the **Use grid federation connection** permission, a cloning error will occur if the same **Unique name** already exists for the tenant on the destination grid.

   - **Federated group**: Enter the unique name. For Active Directory, the unique name is the name associated with the `sAMAccountName` attribute. For OpenLDAP, the unique name is the name associated with the `uid` attribute.
3. Select **Continue**.

Manage group permissions

Group permissions control which tasks users can perform in the Tenant Manager and Tenant Management API.

Steps

1. For **Access mode**, select one of the following:
   - **Read-write** (default): Users can sign in to Tenant Manager and manage the tenant configuration.
   - **Read-only**: Users can only view settings and features. They can't make any changes or perform any operations in the Tenant Manager or Tenant Management API. Local read-only users can change their own passwords.

     > If a user belongs to multiple groups and any group is set to Read-only, the user will have read-only access to all selected settings and features.

2. Select one or more permissions for this group.

   See Tenant management permissions.

3. Select **Continue**.

Set S3 group policy

The group policy determines which S3 access permissions users will have.

Steps

1. Select the policy you want to use for this group.

Group policy	Description
No S3 Access	Default. Users in this group don't have access to S3 resources, unless access is granted with a bucket policy. If you select this option, only the root user will have access to S3 resources by default.
Read Only Access	Users in this group have read-only access to S3 resources. For example, users in this group can list objects and read object data, metadata, and tags. When you select this option, the JSON string for a read-only group policy appears in the text box. You can't edit this string.
Full Access	Users in this group have full access to S3 resources, including buckets. When you select this option, the JSON string for a full-access group policy appears in the text box. You can't edit this string.
Ransomware Mitigation	This sample policy applies to all buckets for this tenant. Users in this group can perform common actions, but can't permanently delete objects from buckets that have object versioning enabled. Tenant Manager users who have the **Manage all buckets** permission can override this group policy. Limit the Manage all buckets permission to trusted users, and use Multi-Factor Authentication (MFA) where available.
Custom	Users in the group are granted the permissions you specify in the text box.

2. If you selected **Custom**, enter the group policy. Each group policy has a size limit of 5,120 bytes. You must enter a valid JSON formatted string.

   For detailed information about group policies, including language syntax and examples, see Example group policies.

3. If you are creating a local group, select **Continue**. If you are creating a federated group, select **Create group** and **Finish**.

Add users (local groups only)

You can save the group without adding users, or you can optionally add any local users that already exist.

> If your tenant account has the **Use grid federation connection** permission, any users you select when you create a local group on the source grid aren't included when the group is cloned to the destination grid. For this reason, don't select users when you create the group. Instead, select the group when you create the users.

Steps

1. Optionally, select one or more local users for this group.
2. Select **Create group** and **Finish**.

   The group you created appears in the list of groups.

If your tenant account has the **Use grid federation connection** permission and you are on the tenant's source grid, the new group is cloned to the tenant's destination grid. **Success** appears as the **Cloning status** in the Overview section of the group's detail page.

Create groups for a Swift tenant

You can manage access permissions for a Swift tenant account by importing federated groups or creating local groups. At least one group must have the Swift Administrator permission, which is required to manage the containers and objects for a Swift tenant account.

> Support for Swift client applications has been deprecated and will be removed in a future release.

Before you begin

- You are signed in to the Tenant Manager using a supported web browser.
- You belong to a user group that has the Root access permission.
- If you plan to import a federated group, you have configured identity federation, and the federated group already exists in the configured identity source.

Access the Create group wizard

Steps

As your first step, access the Create group wizard.

1. Select **ACCESS MANAGEMENT** > **Groups**.
2. Select **Create group**.

Choose a group type

You can create a local group or import a federated group.

Steps

1. Select the **Local group** tab to create a local group, or select the **Federated group** tab to import a group from the previously configured identity source.

   If single sign-on (SSO) is enabled for your StorageGRID system, users belonging to local groups will not be able to sign in to the Tenant Manager, although they can use client applications to manage the tenant's resources, based on group permissions.

2. Enter the group's name.
   - **Local group**: Enter both a display name and a unique name. You can edit the display name later.
   - **Federated group**: Enter the unique name. For Active Directory, the unique name is the name associated with the `sAMAccountName` attribute. For OpenLDAP, the unique name is the name associated with the `uid` attribute.
3. Select **Continue**.

Manage group permissions

Group permissions control which tasks users can perform in the Tenant Manager and Tenant Management API.

Steps

1. For **Access mode**, select one of the following:
   - **Read-write** (default): Users can sign in to Tenant Manager and manage the tenant configuration.
   - **Read-only**: Users can only view settings and features. They can't make any changes or perform any operations in the Tenant Manager or Tenant Management API. Local read-only users can change their own passwords.

     > If a user belongs to multiple groups and any group is set to Read-only, the user will have read-only access to all selected settings and features.

2. Select the **Root access** checkbox if group users need to sign in to the Tenant Manager or Tenant Management API.
3. Select **Continue**.

Set Swift group policy

Swift users need administrator permission to authenticate into the Swift REST API to create containers and ingest objects.

1. Select the **Swift administrator** checkbox if group users need to use the Swift REST API to manage containers and objects.
2. If you are creating a local group, select **Continue**. If you are creating a federated group, select **Create group** and **Finish**.

Add users (local groups only)

You can save the group without adding users, or you can optionally add any local users that already exist.

Steps

1. Optionally, select one or more local users for this group.

   If you have not yet created local users, you can add this group to the user on the Users page. See Manage local users.

2. Select **Create group** and **Finish**.

   The group you created appears in the list of groups.

Tenant management permissions

Before you create a tenant group, consider which permissions you want to assign to that group. Tenant management permissions determine which tasks users can perform using the Tenant Manager or the Tenant Management API. A user can belong to one or more groups. Permissions are cumulative if a user belongs to multiple groups.

To sign in to the Tenant Manager or to use the Tenant Management API, users must belong to a group that has at least one permission. All users who can sign in can perform the following tasks:

- View the dashboard
- Change their own password (for local users)

For all permissions, the group's Access mode setting determines whether users can change settings and perform operations or whether they can only view the related settings and features.

> If a user belongs to multiple groups and any group is set to Read-only, the user will have read-only access to all selected settings and features.

You can assign the following permissions to a group. Note that S3 tenants and Swift tenants have different group permissions.

Permission	Description
Root access	Provides full access to the Tenant Manager and the Tenant Management API. **Note:** Swift users must have Root access permission to sign in to the tenant account.
Administrator	Swift tenants only. Provides full access to the Swift containers and objects for this tenant account **Note:** Swift users must have the Swift Administrator permission to perform any operations with the Swift REST API.
Manage your own S3 credentials	Allows users to create and remove their own S3 access keys. Users who don't have this permission don't see the **STORAGE (S3)** > **My S3 access keys** menu option.
Manage all buckets	• S3 tenants: Allows users to use the Tenant Manager and the Tenant Management API to create and delete S3 buckets and to manage the settings for all S3 buckets in the tenant account, regardless of S3 bucket or group policies. Users who don't have this permission don't see the **Buckets** menu option. • Swift tenants: Allows Swift users to control the consistency level for Swift containers using the Tenant Management API. **Note:** You can only assign the Manage all buckets permission to Swift groups from the Tenant Management API. You can't assign this permission to Swift groups using the Tenant Manager.

Permission	Description
Manage endpoints	Allows users to use the Tenant Manager or the Tenant Management API to create or edit platform service endpoints, which are used as the destination for StorageGRID platform services. Users who don't have this permission don't see the **Platform services endpoints** menu option.
Manage objects with S3 Console	When combined with the Manage all buckets permission, allows users to access the Experimental S3 Console from the Buckets page. Users who have this permission but who don't have the Manage all buckets permission can still navigate directly to the Experimental S3 Console.

Manage groups

You can view a group; edit a group's name, permissions, policies, and users; duplicate a group; or delete a group.

Before you begin

- You are signed in to the Tenant Manager using a supported web browser.
- You belong to a user group that has the Root access permission.

View or edit group

You can view and edit the basic information and details for each group.

Steps

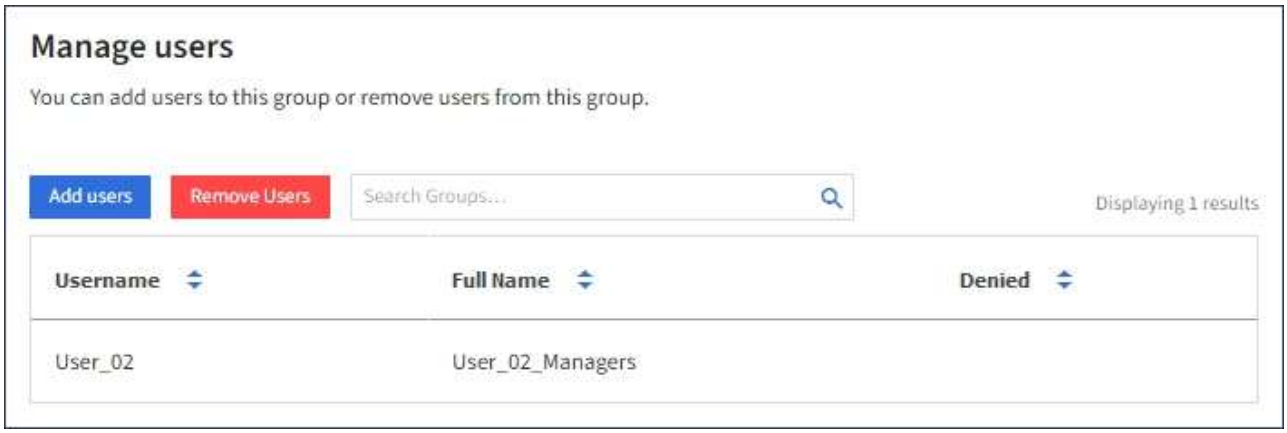
1. Select **ACCESS MANAGEMENT** > **Groups**.
2. Review the information provided on the Groups page, which lists basic information for all local and federated groups for this tenant account.

   If the tenant account has the **Use grid federation connection** permission and you are viewing groups on the tenant's source grid, a blue banner indicates that if you edit or remove a group, your changes will not be synced to the other grid. See Clone tenant groups and users.

3. If you want to change the group's name:
   a. Select the checkbox for the group.
   b. Select **Actions** > **Edit group name**.
   c. Enter the new name.
   d. Select **Save changes.**
4. If you want to view more details or make additional edits, do either of the following:
   - Select the group name.
   - Select the checkbox for the group, and select **Actions** > **View group details**.
5. Review the Overview section, which shows the following information for each group:
   - Display name

- Unique name
- Type
- Access mode
- Permissions
- S3 Policy
- Number of users in this group
- Additional fields if the tenant account has the **Use grid federation connection** permission and you are viewing the group on the tenant's source grid:
  - Cloning status, either **Success** or **Failure**
  - A blue banner indicating that if you edit or delete this group, your changes will not be synced to the other grid.

6. Edit group settings as needed. See Create groups for an S3 tenant and Create groups for a Swift tenant for details about what to enter.
   a. In the Overview section, change the display name by selecting the name or the edit icon .
   b. On the **Group permissions** tab, update the permissions, and select **Save changes**.
   c. On the **Group policy** tab, make any changes, and select **Save changes**.
      - If you are editing an S3 group, optionally select a different S3 group policy or enter the JSON string for a custom policy, as required.
      - If you are editing a Swift group, optionally select or clear the **Swift Administrator** checkbox.
7. To add one or more existing local users to the group:
   a. Select the Users tab.



   b. Select **Add users**.
   c. Select the existing users you want to add, and select **Add users**.

      A success message appears in the upper right.

8. To remove local users from the group:
   a. Select the Users tab.
   b. Select **Remove users**.
   c. Select the users you want to remove, and select **Remove users**.

A success message appears in the upper right.

9. Confirm that you selected **Save changes** for each section you changed.

Duplicate group

You can duplicate an existing group to create new groups more quickly.

> If your tenant account has the **Use grid federation connection** permission and you duplicate a group from the tenant's source grid, the duplicated group will be cloned to the tenant's destination grid.

Steps

1. Select **ACCESS MANAGEMENT** > **Groups**.
2. Select the checkbox for the group you want to duplicate.
3. Select **Actions** > **Duplicate group**.
4. See Create groups for an S3 tenant or Create groups for a Swift tenant for details about what to enter.
5. Select **Create group**.

Delete one or more groups

You can delete one or more groups. Any users who belong only to a group that is deleted will no longer be able to sign in to the Tenant Manager or use the tenant account.

> If your tenant account has the **Use grid federation connection** permission and you delete a group, StorageGRID will not delete the corresponding group on the other grid. If you need to keep this information in sync, you must delete the same group from both grids.

Steps

1. Select **ACCESS MANAGEMENT** > **Groups**.
2. Select the checkbox for each group you want to delete.
3. Select **Actions** > **Delete group** or **Actions** > **Delete groups**.

   A confirmation dialog box appears.

4. Select **Delete group** or **Delete groups**.