■ NetApp

Manage groups

StorageGRID

NetApp May 17, 2022

This PDF was generated from https://docs.netapp.com/us-en/storagegrid-116/tenant/creating-groups-for-s3-tenant.html on May 17, 2022. Always check docs.netapp.com for the latest.

Table of Contents

age groups
reate groups for an S3 tenant
reate groups for a Swift tenant
enant management permissions
iew and edit group details
dd users to a local group
dit group name
uplicate group
elete group

Manage groups

Create groups for an S3 tenant

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

What you'll need

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

For information about S3, see Use S3.

Steps

1. Select ACCESS MANAGEMENT > Groups.



- 2. Select Create group.
- 3. 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.

- 4. 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 samacountName attribute. For OpenLDAP, the unique name is the name
 associated with the unique attribute.
- 5. Select Continue.
- 6. Select an Access mode. 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.
 - Read-write (default): Users can log into Tenant Manager and manage the tenant configuration.
 - Read-only: Users can only view settings and features. They cannot make any changes or perform any
 operations in the Tenant Manager or Tenant Management API. Local read-only users can change their
 own passwords.
- 7. Select the Group permissions for this group.

See the information about tenant management permissions.

- 8. Select Continue.
- 9. Select a group policy to determine which S3 access permissions the members of this group will have.
 - No S3 Access: Default. Users in this group do not 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 cannot 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 cannot edit this
 string.
 - Custom: Users in the group are granted the permissions you specify in the text box. See the
 instructions for implementing an S3 client application for detailed information about group policies,
 including language syntax and examples.
- 10. 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.

In this example, members of the group are only permitted to list and access a folder matching their username (key prefix) in the specified bucket. Note that access permissions from other group policies and the bucket policy should be considered when determining the privacy of these folders.

```
No S3 Access
                                              "Statement": [
Read Only Access
                                                "Sid": "AllowListBucketOfASpecificUserPrefix",
Full Access
                                                "Effect": "Allow",
                                                "Action": "s3:ListBucket",
Custom
                                                "Resource": "arn:aws.s3:::department-bucket",
(Must be a valid JSON formatted string.)
                                                "Condition": {
                                                 "StringLike": {
                                                  "s3:prefix": "${aws:username}/*"
                                                "Sid": "AllowUserSpecificActionsOnlyInTheSpecificFolder",
                                                "Effect": "Allow",
                                                "Action": "s3:*Object",
                                                "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
```

- 11. Select the button that appears, depending on whether you are creating a federated group or a local group:
 - Federated group: Create group
 - · Local group: Continue

If you are creating a local group, step 4 (Add users) appears after you select **Continue**. This step does not appear for federated groups.

12. Select the check box for each user you want to add to the group, then select **Create group**.

Optionally, you can save the group without adding users. You can add users to the group later, or select the group when you add new users.

13. Select Finish.

The group you created appears in the list of groups. Changes might take up to 15 minutes to take effect because of caching.

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.

What you'll need

You must be signed in to the Tenant Manager using a supported web browser.

- You must 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.

Steps

Select ACCESS MANAGEMENT > Groups.



- 2. Select Create group.
- 3. 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.

- 4. 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.
- Select Continue.
- 6. Select an Access mode. 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.
 - · Read-write (default): Users can log into Tenant Manager and manage the tenant configuration.
 - Read-only: Users can only view settings and features. They cannot make any changes or perform any
 operations in the Tenant Manager or Tenant Management API. Local read-only users can change their
 own passwords.
- 7. Set the Group permission.
 - Select the Root Access check box if users need to sign in to the Tenant Manager or Tenant

Management API. (Default)

- Unselect the Root Access check box if users do not need access to the Tenant Manager or Tenant Management API. For example, unselect the check box for applications that do not need to access the tenant. Then, assign the Swift Administrator permission to allow these users to manage containers and objects.
- 8. Select Continue.
- Select the Swift administrator check box if the user needs to be able to use the Swift REST API.

Swift users must have the Root Access permission to access the Tenant Manager. However, the Root Access permission does not allow users to authenticate into the Swift REST API to create containers and ingest objects. Users must have the Swift Administrator permission to authenticate into the Swift REST API.

- 10. Select the button that appears, depending on whether you are creating a federated group or a local group:
 - · Federated group: Create group
 - · Local group: Continue

If you are creating a local group, step 4 (Add users) appears after you select **Continue**. This step does not appear for federated groups.

11. Select the check box for each user you want to add to the group, then select **Create group**.

Optionally, you can save the group without adding users. You can add users to the group later, or select the group when you create new users.

12. Select Finish.

The group you created appears in the list of groups. Changes might take up to 15 minutes to take effect because of caching.

Related information

Tenant management permissions

Use Swift

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. Changes might take up to 15 minutes to take effect because of caching.

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	S3 tenants only. Allows users to create and remove their own S3 access keys. Users who do not have this permission do not 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 do not have this permission do not 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 cannot assign this permission to Swift groups using the Tenant Manager.
Manage Endpoints	S3 tenants only. Allows users to use the Tenant Manager or the Tenant Management API to create or edit endpoints, which are used as the destination for StorageGRID platform services. Users who do not have this permission do not see the Platform services endpoints menu option.

Related information

Use S3

Use Swift

View and edit group details

When you view the details for a group, you can change the group's display name, permissions, policies, and the users that belong to the group.

What you'll need

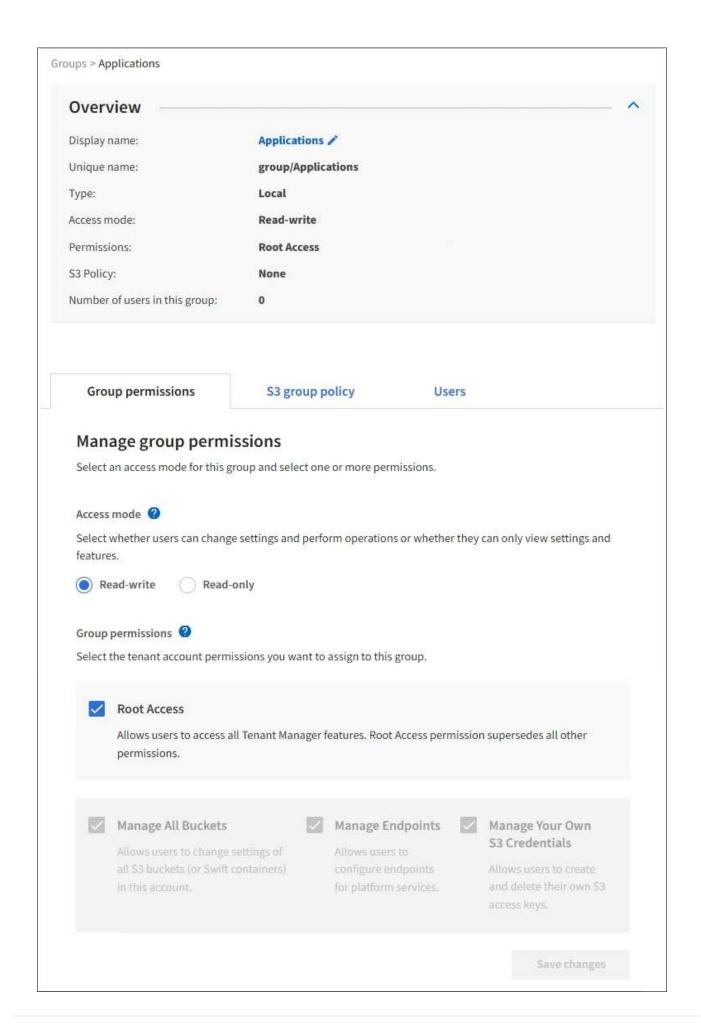
- You must be signed in to the Tenant Manager using a supported web browser.
- You must belong to a user group that has the Root Access permission.

Steps

- 1. Select ACCESS MANAGEMENT > Groups.
- 2. Select the name of the group whose details you want to view or edit.

Alternatively, you can select **Actions** > **View group details**.

The group details page appears. The following example shows the S3 group details page.



3. Make changes to the group settings as needed.



To ensure your changes are saved, select **Save changes** after you make changes in each section. When your changes are saved, a confirmation message appears in the upper right corner of the page.

a. Optionally, select the display name or edit icon to update the display name.

You cannot change a group's unique name. You cannot edit the display name for a federated group.

- b. Optionally, update the permissions.
- c. For group policy, make the appropriate changes for your S3 or Swift tenant.
 - If you are editing a group for an S3 tenant, optionally select a different S3 group policy. If you select a custom S3 policy, update the JSON string as required.
 - If you are editing a group for a Swift tenant, optionally select or unselect the Swift Administrator check box.

For more information about the Swift Administrator permission, see the instructions for creating groups for a Swift tenant.

- d. Optionally, add or remove users.
- 4. Confirm that you have selected **Save changes** for each section you changed.

Changes might take up to 15 minutes to take effect because of caching.

Related information

Create groups for S3 tenant

Create groups for Swift tenant

Add users to a local group

You can add users to a local group as needed.

What you'll need

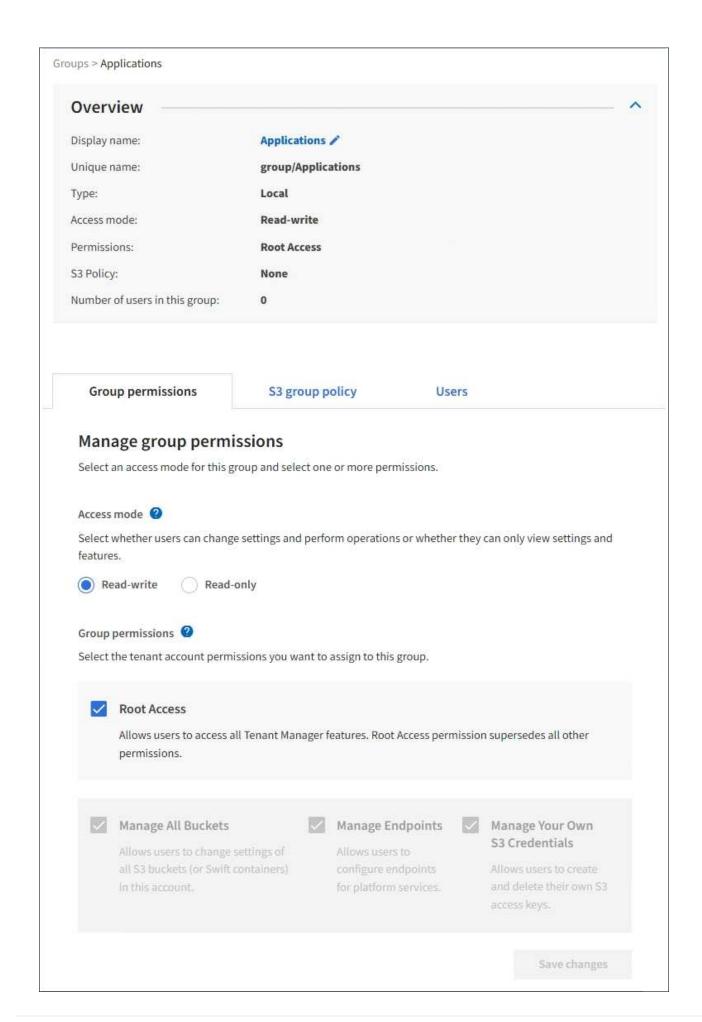
- You must be signed in to the Tenant Manager using a supported web browser.
- You must belong to a user group that has the Root Access permission.

Steps

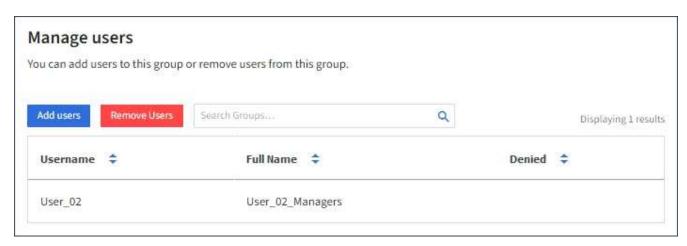
- 1. Select ACCESS MANAGEMENT > Groups.
- 2. Select the name of the local group you want to add users to.

Alternatively, you can select **Actions > View group details**.

The group details page appears.



3. Select **Users**, and then select **Add users**.



4. Select the users you want to add to the group, and then select **Add users**.



A confirmation message appears in the upper right corner of the page. Changes might take up to 15 minutes to take effect because of caching.

Edit group name

You can edit the display name for a group. You cannot edit the unique name for a group.

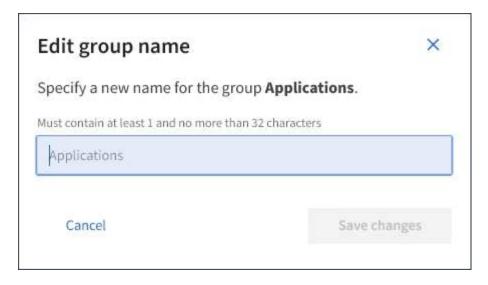
What you'll need

- You must be signed in to the Tenant Manager using a supported web browser.
- You must belong to a user group that has the Root Access permission. See Tenant management permissions.

Steps

- 1. Select ACCESS MANAGEMENT > Groups.
- 2. Select the check box for the group whose display name you want to edit.
- 3. Select Actions > Edit group name.

The Edit group name dialog box appears.



4. If you are editing a local group, update the display name as needed.

You cannot change a group's unique name. You cannot edit the display name for a federated group.

5. Select Save changes.

A confirmation message appears in the upper right corner of the page. Changes might take up to 15 minutes to take effect because of caching.

Duplicate group

You can create new groups more quickly by duplicating an existing group.

What you'll need

- You must be signed in to the Tenant Manager using a supported web browser.
- You must belong to a user group that has the Root Access permission. See Tenant management permissions.

Steps

- 1. Select ACCESS MANAGEMENT > Groups.
- 2. Select the check box for the group you want to duplicate.
- 3. Select **Duplicate group**. For additional details on creating a group, see the instructions for creating groups for an S3 tenant or for a Swift tenant.
- 4. 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.

- 5. 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.

- 6. Select Continue.
- 7. As needed, modify the permissions for this group.
- 8. Select Continue.
- 9. As needed, if you are duplicating a group for an S3 tenant, optionally select a different policy from the **Add S3 policy** radio buttons. If you selected a custom policy, update the JSON string as required.
- 10. Select Create group.

Delete group

You can delete a group from the system. Any users who belong only to that group will no longer be able to sign in to the Tenant Manager or use the tenant account.

What you'll need

- You must be signed in to the Tenant Manager using a supported web browser.
- You must belong to a user group that has the Root Access permission. See Tenant management permissions.

Steps

1. Select ACCESS MANAGEMENT > Groups.



- 2. Select the check boxes for the groups you want to delete.
- 3. Select **Actions > Delete group**.

A confirmation message appears.

4. Select **Delete group** to confirm you want to delete the groups indicated in the confirmation message.

A confirmation message appears in the upper right corner of the page. Changes might take up to 15

minutes to take effect because of caching.

Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system- without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.