NetApp

Use grid federation connections

StorageGRID 11.7

NetApp
April 12, 2024

Table of Contents

# Use grid federation connections

Clone tenant groups and users

If a new tenant has permission to use a grid federation connection, that tenant is replicated from one StorageGRID system to another StorageGRID system when it is created. After the tenant has been replicated, any groups and users added to the source tenant are cloned to the destination tenant.

The StorageGRID system where the tenant is originally created is the tenant's *source grid*. The StorageGRID system where the tenant is replicated is the tenant's *destination grid*. Both tenant accounts have the same account ID, name, description, storage quota, and assigned permissions, but the destination tenant does not initially have a root user password. For details, see What is account clone and Manage permitted tenants.

The cloning of tenant account information is required for cross-grid replication of bucket objects. Having the same tenant groups and users on both grids ensures you can access the corresponding buckets and objects on either grid.

Tenant workflow for account clone

If your tenant account has the **Use grid federation connection** permission, review the workflow diagram to see the steps you will perform to clone groups, users, and S3 access keys.
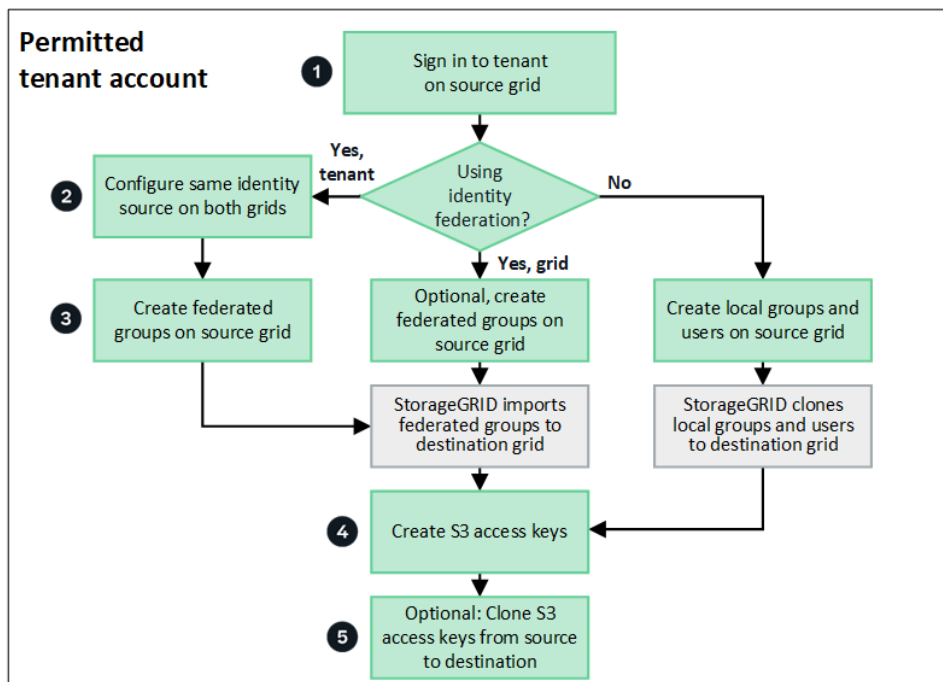
These are the primary steps in the workflow:

1 **Sign in to tenant**

Sign in to the tenant account on the source grid (the grid where the tenant was initially created.)

2   **Optionally, configure identity federation**

If your tenant account has the **Use own identity source** permission to use federated groups and users, configure the same identity source (with the same settings) for both the source and destination tenant accounts. Federated groups and users can't be cloned unless both grids are using the same identity source. For instructions, see Use identity federation.

3   **Create groups and users**

When creating groups and users, always start from the tenant's source grid. When you add a new group, StorageGRID automatically clones it to the destination grid.

- If identity federation is configured for the entire StorageGRID system or for your tenant account, create new tenant groups by importing federated groups from the identity source.

- If you aren't using identity federation, create new local groups and then create local users.

4   **Create S3 access keys**

You can create your own access keys or to create another user's access keys on either the source grid or the destination grid to access buckets on that grid.

5   **Optionally, clone S3 access keys**

If you need to access buckets with the same access keys on both grids, create the access keys on the source grid and then use the Tenant Manager API to manually clone them to the destination grid. For instructions, see Clone S3 access keys using the API.

How are groups, users, and S3 access keys cloned?

Review this section to understand how groups, users, and S3 access keys are cloned between the tenant source grid and the tenant destination grid.

Local groups created on source grid are cloned

After a tenant account is created and replicated to the destination grid, StorageGRID automatically clones any local groups you add to the tenant's source grid to the tenant's destination grid.

Both the original group and its clone have the same access mode, group permissions, and S3 group policy. For instructions, see Create groups for S3 tenant.
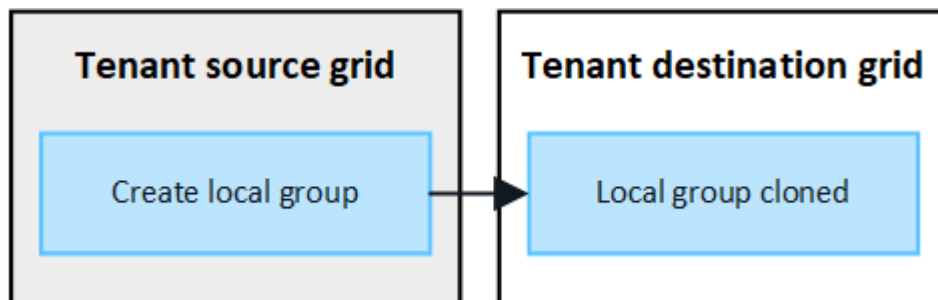
> ⓘ Any users you select when you create a local group on the source grid aren't included when the group is cloned to the destination grid. For this reason, don't select users when you create the group. Instead, select the group when you create the users.

Local users created on source grid are cloned

When you create a new local user on the source grid, StorageGRID automatically clones that user to the destination grid. Both the original user and its clone have the same full name, username, and **Deny access** setting. Both users also belong to the same groups. For instructions, see Manage local users.

For security reasons, local user passwords aren't cloned to the destination grid. If a local user needs to access Tenant Manager on the destination grid, the root user for the tenant account must add a password for that user on the destination grid. For instructions, see Manage local users.
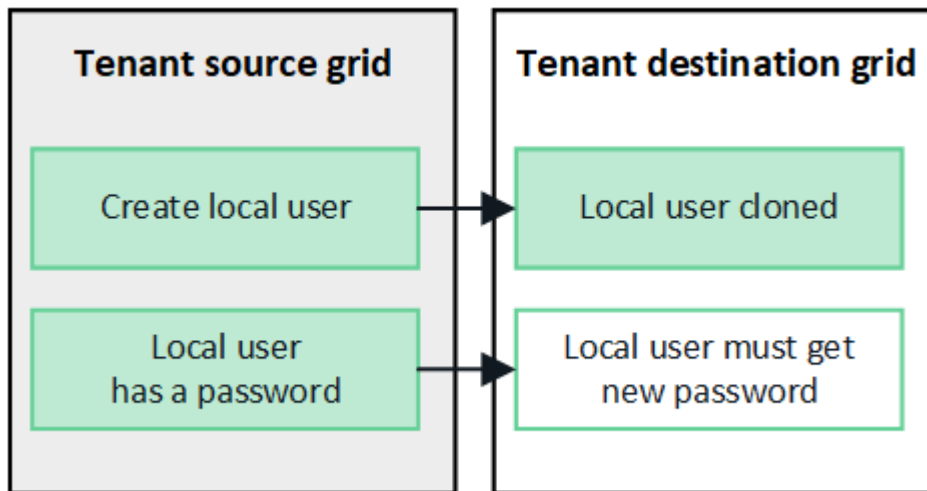

Federated groups created on source grid are cloned

Assuming the requirements for using account clone with single sign-on and identity federation have been met, federated groups that you create (import) for the tenant on the source grid are automatically cloned to the tenant on the destination grid.

Both groups have the same access mode, group permissions and S3 group policy.

After federated groups are created for the source tenant and cloned to the destination tenant, federated users can sign in to the tenant on either grid.
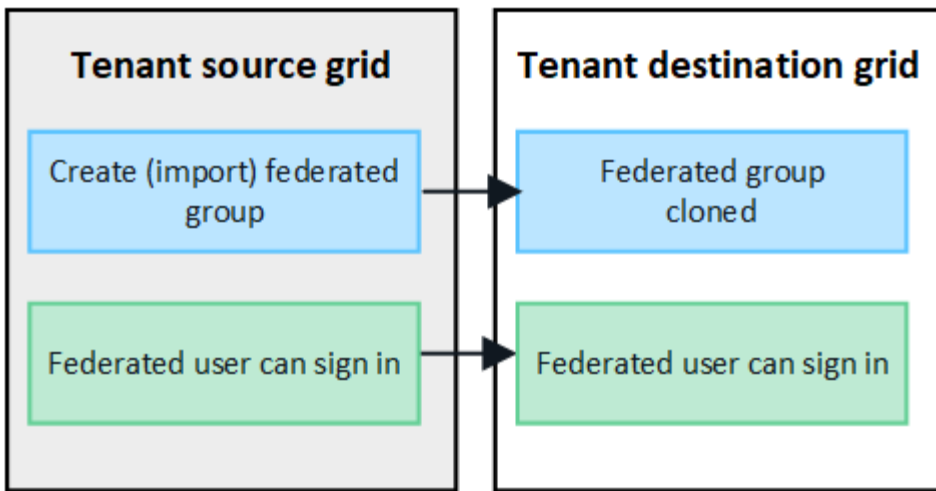
S3 access keys can be manually cloned

StorageGRID does not automatically clone S3 access keys because security is improved by having different keys on each grid.

To manage access keys on the two grids, you can do either of the following:

- If you don't need to use the same keys for each grid, you can create your own access keys or create another user's access keys on each grid.

- If you need to use the same keys on both grids, you can create keys on the source grid and then use the Tenant Manager API to manually clone the keys to the destination grid.
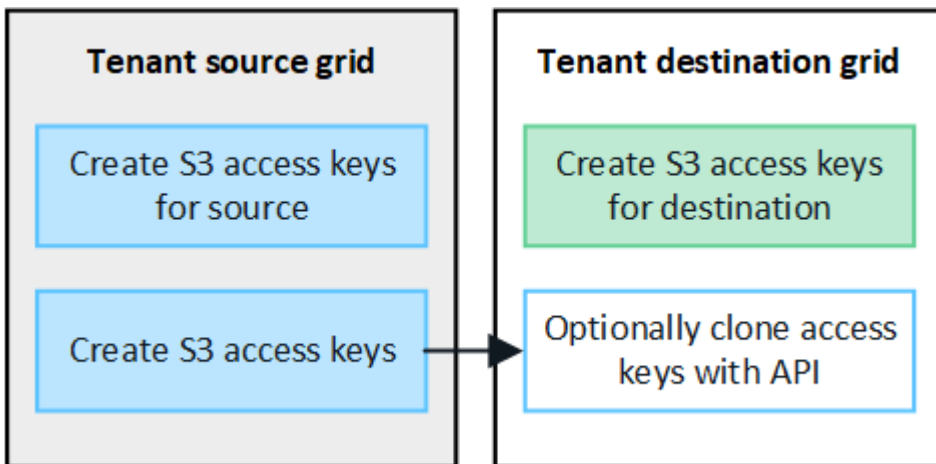
 When you clone S3 access keys for a federated user, both the user and the S3 access keys are cloned to the destination tenant.

**Groups and users added to destination grid aren't cloned**

Cloning occurs only from the tenant's source grid to the tenant's destination grid. If you create or import groups and users on the tenant's destination grid, StorageGRID will not clone these items back the tenant's source grid.
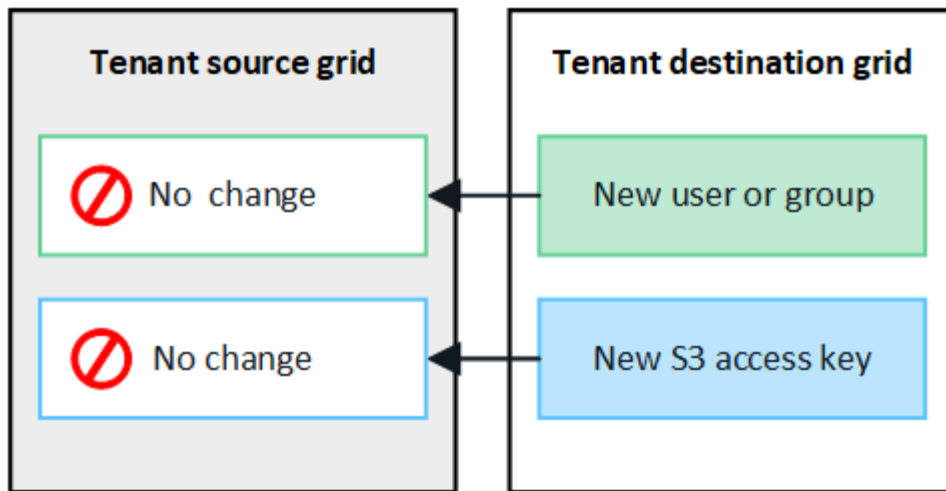
Edited or deleted groups, users, and access keys aren't cloned

Cloning occurs only when you create new groups and users.

If you edit or delete groups, users, or access keys on either grid, your changes will not be cloned to the other grid.
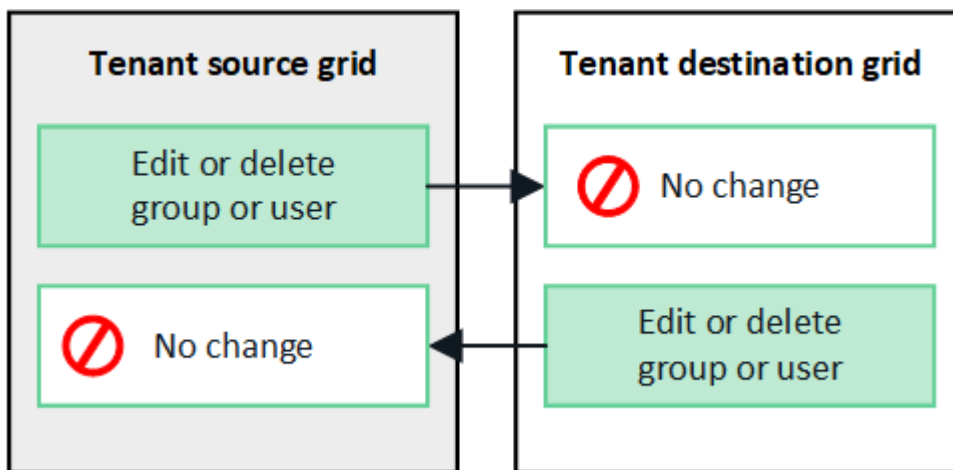
Clone S3 access keys using the API

If your tenant account has the **Use grid federation connection** permission, you can use the Tenant Management API to manually clone S3 access keys from the tenant on the source grid to the tenant on the destination grid.

Before you begin

- The tenant account has the **Use grid federation connection** permission.
- The grid federation connection has a **Connection status** of **Connected**.
- You are signed in to the Tenant Manager on the tenant's source grid using a supported web browser.
- You belong to a user group that has the Manage your own S3 credentials or Root access permission.
- If you are cloning access keys for a local user, the user already exists on both grids.

> **ⓘ** When you clone S3 access keys for a federated user, both the user and the S3 access keys are added to the destination tenant.

Clone your own access keys

You can clone your own access keys if you need to access the same buckets on both grids.

Steps

1. Using the Tenant Manager on the source grid, create your own access keys and download the `.csv` file.

2. From the top of the Tenant Manager, select the help icon and select **API documentation**.

3. In the **s3** section, select the following endpoint:

   `POST /org/users/current-user/replicate-s3-access-key`

POST	/org/users/current-user/replicate-s3-access-key	Clone the current user's S3 key to the other grids.	🔓

4. Select **Try it out**.

5. In the **body** text box, replace the example entries for **accessKey** and **secretAccessKey** with the values from the **.csv** file you downloaded.

   Be sure to retain the double quotes around each string.

   body * required

   Edit Value | Model

   (body)

   ```
   {
       "accessKey": "AKIAIOSFODNN7EXAMPLE",
       "secretAccessKey": "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY",
       "expires": "2028-09-04T00:00:00.000Z"
   }
   ```

6. If the key will expire, replace the example entry for **expires** with the expiration date and time as a string in ISO 8601 data-time format (for example, `2024-02-28T22:46:33-08:00`). If the key will not expire, enter **null** as the value for the **expires** entry (or remove the **Expires** line and the preceding comma).

7. Select **Execute**.

8. Confirm that the server response code is **204**, indicating that the key was successfully cloned to the destination grid.

Clone another user's access keys

You can clone another user's access keys if they need to access the same buckets on both grids.

Steps

1. Using the Tenant Manager on the source grid, create the other user's S3 access keys and download the `.csv` file.

2. From the top of the Tenant Manager, select the help icon and select **API documentation**.

3. Obtain the user ID. You will need this value to clone the other user's access keys.

a. From the **users** section, select the following endpoint:

```
GET /org/users
```

b. Select **Try it out**.

c. Specify any parameters you want to use when looking up users.

d. Select **Execute**.

e. Find the user whose keys you want to clone, and copy the number in the **id** field.

4. In the **s3** section, select the following endpoint:

```
POST /org/users/{userId}/replicate-s3-access-key
```


5. Select **Try it out**.

6. In the **userId** text box, paste the user ID you copied.

7. In the **body** text box, replace the example entries for **example access key** and **secret access key** with the values from the **.csv** file for that user.

   Be sure to retain the double quotes around the string.

8. If the key will expire, replace the example entry for **expires** with the expiration date and time as a string in ISO 8601 data-time format (for example, `2023-02-28T22:46:33-08:00`). If the key will not expire, enter **null** as the value for the **expires** entry (or remove the **Expires** line and the preceding comma).

9. Select **Execute**.

10. Confirm that the server response code is **204**, indicating that the key was successfully cloned to the destination grid.

Manage cross-grid replication

If your tenant account was assigned the **Use grid federation connection** permission when it was created, you can use cross-grid replication to automatically replicate objects between buckets on the tenant's source grid and buckets on the tenant's destination grid. Cross-grid replication can occur in one or both directions.

Workflow for cross-grid replication

The workflow diagram summarize the steps you will perform to configure cross-grid replication between buckets on two grids. These steps are described in more detail below.
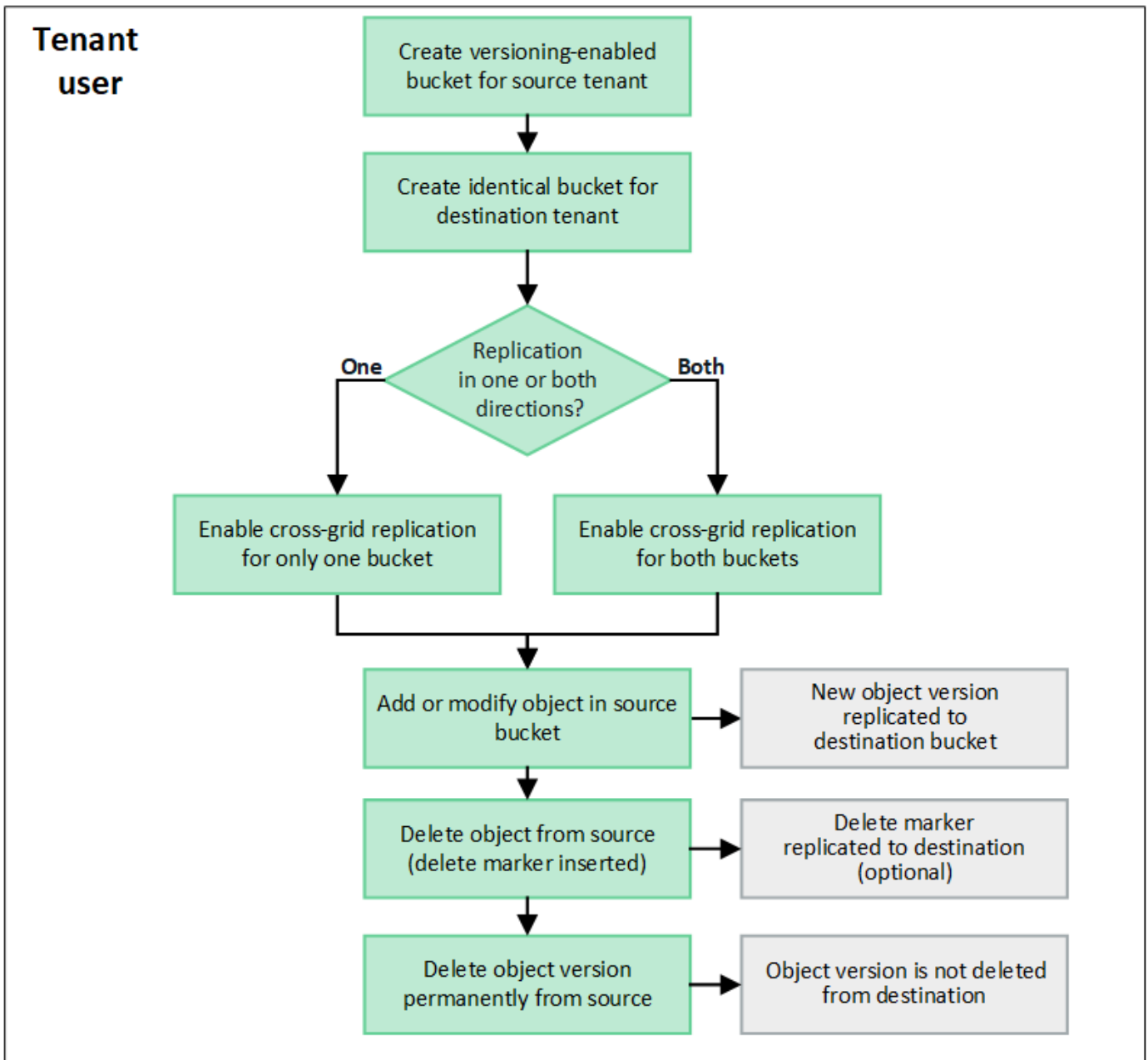
Configure cross-grid replication

Before you can use cross-grid replication, you must sign in to the corresponding tenant accounts on each grid and create identical buckets. Then, you can enable cross-grid replication on either or both buckets.

Before you begin

- You have reviewed the requirements for cross-grid replication. See What is cross-grid replication.
- You are using a supported web browser.
- The tenant account has the **Use grid federation connection** permission, and identical tenant accounts exist on both grids. See Manage the permitted tenants for grid federation connection.
- The tenant user you will be signing in as already exists on both grids and belongs to a user group that has the Root access permission.
- If you will be signing in to the tenant's destination grid as a local user, the root user for the tenant account has set a password for your user account on that grid .

8

Create two identical buckets

As a first step, sign in to the corresponding tenant accounts on each grid and create identical buckets.

Steps

1. Starting from either grid in the grid federation connection, create a new bucket:

   a. Sign in to the tenant account using the credentials of a tenant user who exists on both grids.

   > (i) If you are unable to sign in to the tenant's destination grid as a local user, confirm that the root user for the tenant account has set a password for your user account.

   b. Follow the instructions to create an S3 bucket.

   c. On the **Manage object settings** tab, select **Enable object versioning**.

   d. If S3 Object Lock is enabled for your StorageGRID system, don't enable S3 Object Lock for the bucket.

   e. Select **Create bucket**.

   f. Select **Finish**.

2. Repeat these steps to create an identical bucket for the same tenant account on the other grid in the grid federation connection.

Enable cross-grid replication

You must perform these steps before adding any objects to either bucket.

Steps

1. Starting from a grid whose objects you want to replicate, enable cross-grid replication in one direction:

   a. Sign in to the tenant account for the bucket.

   b. Select **View buckets** from the dashboard, or select **STORAGE (S3)** > **Buckets**.

   c. Select the bucket name from the table to access the bucket details page.

   d. Select the **Cross-grid replication** tab.

   e. Select **Enable**, and review the list of requirements.

   f. If all requirements have been met, select the grid federation connection you want to use.

   g. Optionally, change the setting of **Replicate delete markers** to determine what happens on the destination grid if an S3 client issues a delete request to the source grid that doesn't include a version ID:

      ▪ If **Yes** (default), a delete marker is added to the source bucket and replicated to the destination bucket.

      ▪ If **No**, a delete marker is added to the source bucket but is not replicated to the destination bucket.
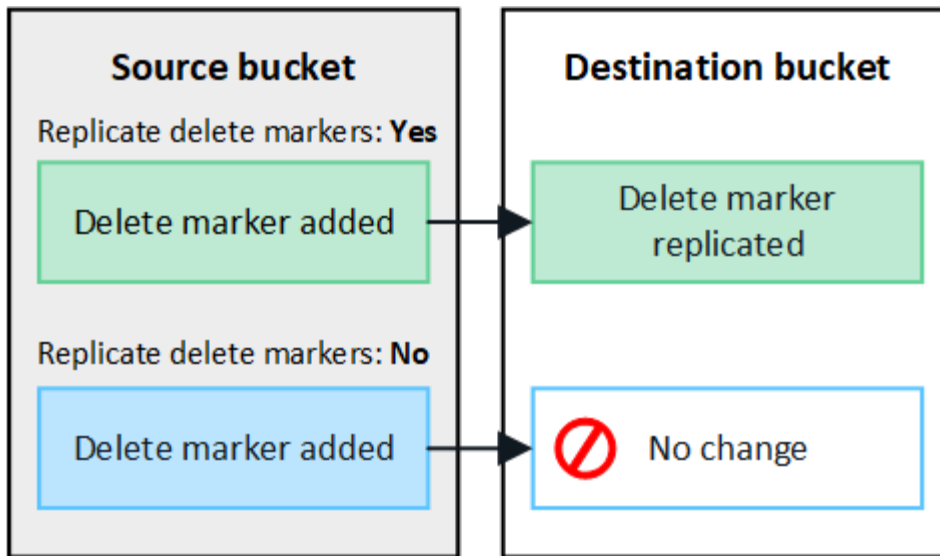
> ⓘ If the delete request includes a version ID, that object version is permanently removed from the source bucket. StorageGRID does not replicate delete requests that include a version ID, so the same object version is not deleted from the destination.

See What is cross-grid replication for details.

   h. Review your selections. You aren't able to change these settings unless both buckets are empty.

   i. Select **Enable and test**.

     After a few moments, a success message appears. Objects added to this bucket will now be automatically replicated to the other grid. **Cross-grid replication** is shown as an enabled feature on the bucket details page.

2. Optionally, go to the corresponding bucket on the other grid and enable cross-grid replication in both directions.

Test replication between grids

If cross-grid replication is enabled for a bucket, you might need to verify that the connection and cross-grid replication are working correctly and that the source and destination buckets still meet all requirements (for example, versioning is still enabled).

Before you begin

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

Steps

1. Sign in to the tenant account for the bucket.
2. Select **View buckets** from the dashboard, or select **STORAGE (S3)** > **Buckets**.
3. Select the bucket name from the table to access the bucket details page.
4. Select the **Cross-grid replication** tab.
5. Select **Test connection**.

If the connection is healthy, a success banner appears. Otherwise, an error message appears, which you and the grid admin can use to resolve the issue. For details, see Troubleshoot grid federation errors.

6. If cross-grid replication is configured to occur in both directions, go to the corresponding bucket on the other grid and select **Test connection** to verify that cross-grid replication is working in the other direction.

Disable cross-grid replication

You can permanently stop cross-grid replication if you no longer want to copy objects to the other grid.

Before disabling cross-grid replication, note the following:

- Disabling cross-grid replication does not remove any objects that have already been copied between grids. For example, objects in `my-bucket` on Grid 1 that have been copied to `my-bucket` on Grid 2 aren't removed if you disable cross-grid replication for that bucket. If you want to delete these objects, you must remove them manually.

- If cross-grid replication was enabled for each of the buckets (that is, if replication occurs in both directions), you can disable cross-grid replication for either or both buckets. For example, you might want to disable replicating objects from `my-bucket` on Grid 1 to `my-bucket` on Grid 2, while continuing to replicate objects from `my-bucket` on Grid 2 to `my-bucket` on Grid 1.

- You must disable cross-grid replication before you can remove a tenant's permission to use the grid federation connection. See Manage permitted tenants.

- If you disable cross-grid replication for a bucket that contains objects, you will not be able to reenable cross-grid replication unless you delete all objects from both the source and destination buckets.

> ⚠️ You can't reenable replication unless both buckets are empty.

Before you begin
- You are using a supported web browser.
- You belong to a user group that has the Root access permission.

Steps
1. Starting from the grid whose objects you no longer want to replicate, stop cross-grid replication for the bucket:

   a. Sign in to the tenant account for the bucket.

   b. Select **View buckets** from the dashboard, or select **STORAGE (S3)** > **Buckets**.

   c. Select the bucket name from the table to access the bucket details page.

   d. Select the **Cross-grid replication** tab.

   e. Select **Disable replication**.

   f. If you are sure you want to disable cross-grid replication for this bucket, type **Yes** in the text box, and select **Disable**.

   After a few moments, a success message appears. New objects added to this bucket can no longer be automatically replicated to the other grid. **Cross-grid replication** is no longer shown as a Enabled feature on the Buckets page.

2. If cross-grid replication was configured to occur in both directions, go to the corresponding bucket on the other grid and stop cross-grid replication in the other direction.

View grid federation connections

If your tenant account has the **Use grid federation connection** permission, you can view the allowed connections.

Before you begin

- The tenant account has the **Use grid federation connection** permission.
- 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.

Steps

1. Select **STORAGE (S3)** > **Grid federation connections**.

   The Grid federation connection page appears and includes a table that summarizes the following information:

Column	Description
Connection name	The grid federation connections this tenant has permission to use.
Buckets with cross-grid replication	For each grid federation connection, the tenant buckets that have cross-grid replication enabled. Objects added to these buckets will be replicated to the other grid in the connection.
Last error	For each grid federation connection, the most recent error to occur, if any, when data was being replicated to the other grid. See Clear the last error.

2. Optionally, select a bucket name to view bucket details.

Clear the last error

An error might appear in the **Last error** column for one of these reasons:

- The source object version was not found.
- The source bucket was not found.
- The destination bucket was deleted.
- The destination bucket was re-created by a different account.
- The destination bucket has versioning suspended.
- The destination bucket was re-created by the same account but is now unversioned.

ⓘ   This column only shows the last cross-grid replication error to occur; previous errors that might have occurred will not be shown.

Steps

1. If a message appears in the **Last error** column, view the message text.

   For example, this error indicates that the destination bucket for cross-grid replication was in an invalid

state, possibly because versioning was suspended or S3 Object Lock was enabled.

2. Perform any recommended actions. For example, if versioning was suspended on the destination bucket for cross-grid replication, reenable versioning for that bucket.

3. Select the connection from the table.

4. Select **Clear error**.

5. Select **Yes** to clear the message and update the system's status.

6. Wait 5-6 minutes and then ingest a new object into the bucket. Confirm that the error message does not reappear.

   > (i) To ensure the error message is cleared, wait at least 5 minutes after the timestamp in the message before ingesting a new object.

7. To determine if any objects failed to be replicated because of the bucket error, see Identify and retry failed replication operations.