Manage S3 buckets

StorageGRID 11.7

NetApp
January 09, 2024

Table of Contents

Manage S3 buckets

Create an S3 bucket

You can use the Tenant Manager to create S3 buckets for object data.

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 or Manage all buckets permission. These permissions override the permissions settings in group or bucket policies.

> Permissions to set or modify S3 Object Lock properties of buckets or objects can be granted by bucket policy or group policy.

- If you plan to enable S3 Object Lock for a bucket, a grid admin has enabled the global S3 Object Lock setting for the StorageGRID system, and you have reviewed the requirements for S3 Object Lock buckets and objects. See Use S3 Object Lock to retain objects.

Access the wizard

Steps

1. Select **View buckets** from the dashboard, or select **STORAGE (S3)** > **Buckets**.
2. Select **Create bucket**.

Enter details

Steps

1. Enter details for the bucket.

Field	Description
Bucket name	A name for the bucket that complies with these rules: • Must be unique across each StorageGRID system (not just unique within the tenant account). • Must be DNS compliant. • Must contain at least 3 and no more than 63 characters. • Each label must start and end with a lowercase letter or a number and can only use lowercase letters, numbers, and hyphens. • Should not use periods in virtual hosted style requests. Periods will cause problems with server wildcard certificate verification. For more information, see the Amazon Web Services (AWS) documentation on bucket naming rules. **Note**: You can't change the bucket name after creating the bucket.

Field	Description
Region	The bucket's region. Your StorageGRID administrator manages the available regions. A bucket's region can affect the data-protection policy applied to objects. By default, all buckets are created in the `us-east-1` region. **Note**: You can't change the region after creating the bucket.

2. Select **Continue**.

Manage object settings

Steps

1. Optionally, enable object versioning for the bucket.

   Enable object versioning if you want to store every version of each object in this bucket. You can then retrieve previous versions of an object as needed. You must enable object versioning if the bucket will be used for cross-grid replication.

2. If the global S3 Object Lock setting is enabled, optionally enable S3 Object Lock for the bucket to store objects using a write-once-read-many (WORM) model.

   Enable S3 Object Lock for a bucket only if you need to keep objects for fixed amount of time, for example, to meet certain regulatory requirements. S3 Object Lock is a permanent setting that helps you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely.

   > After the S3 Object Lock setting is enabled for a bucket, it can't be disabled. Anyone with the correct permissions can add objects to this bucket that can't be changed. You might not be able to delete these objects or the bucket itself.

   If you enable S3 Object Lock for a bucket, bucket versioning is enabled automatically.

3. If you selected **Enable S3 Object Lock**, optionally enable **Default retention** for this bucket.

   When **Default retention** is enabled, new objects added to the bucket will be automatically protected from being deleted or overwritten. The **Default retention** setting does not apply to objects that have their own retention periods.

   a. If **Default retention** is enabled, specify a **Default retention mode** for the bucket.

Default retention mode	Description
Compliance	• The object can't be deleted until its retain-until-date is reached. • The object's retain-until-date can be increased, but it can't be decreased. • The object's retain-until-date can't be removed until that date is reached.

Default retention mode	Description
Governance	• Users with the `s3:BypassGovernanceRetention` permission can use the `x-amz-bypass-governance-retention: true` request header to bypass retention settings. • These users can delete an object version before its retain-until-date is reached. • These users can increase, decrease, or remove an object's retain-until-date.

b. If **Default retention** is enabled, specify the **Default retention period** for the bucket.

   The **Default retention period** indicates how long new objects added to this bucket should be retained, starting from the time they are ingested. Specify a value between 1 and 36,500 days or between 1 and 100 years, inclusive.

4. Select **Create bucket**.

   The bucket is created and added to the table on the Buckets page.

5. Optionally, select **Go to bucket details page** to view bucket details and perform additional configuration.

View bucket details

You can view the buckets in your tenant account.

Before you begin

- You are signed in to the Tenant Manager using a supported web browser.

Steps

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

   The Buckets page appears.

2. Review the summary information for each bucket.

   As required, you can sort the information by any column, or you can page forward and back through the list.

   > The Object Count and Space Used values displayed are estimates. These estimates are affected by the timing of ingests, network connectivity, and node status. If buckets have versioning enabled, deleted object versions are included in the object count.

Column	Description
Name	The bucket's unique name, which can't be changed.
Enabled features	The list of features that are enabled for the bucket.

Column	Description
S3 Object Lock	Whether S3 Object Lock is enabled for the bucket. This column appears only if S3 Object Lock is enabled for the grid. This column also shows information for any legacy Compliant buckets.
Region	The bucket's region, which can't be changed.
Object count	The number of objects in this bucket. When objects are added or deleted, this value might not update immediately. If buckets have versioning enabled, non-current object versions are included in this value.
Space used	The logical size of all objects in the bucket. The logical size does not include the actual space required for replicated or erasure-coded copies or for object metadata.
Date created	The date and time the bucket was created.

3. To view details for a specific bucket, select the bucket name from the table.

   The bucket details page appears. From this page, you can perform the following tasks:

   - Configure and manage bucket options, such as consistency level, last access time updates, object versioning, S3 Object Lock and default bucket retention
   - Configure bucket access, such as cross-origin resource sharing (CORS)
   - Manage platform services (if allowed for the tenant), including replication, event notifications, and search integration
   - Enable and manage cross-grid replication (if allowed for the tenant) to replicate objects ingested into this bucket to another StorageGRID system
   - Access the Experimental S3 Console to manage the objects in the bucket
   - Delete all objects in a bucket
   - Delete a bucket that is already empty

Change a bucket's consistency level

If you are using an S3 tenant, you can change the consistency level for operations performed on the objects in S3 buckets.

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 Manage all buckets or Root access permission. These permissions override the permissions settings in group or bucket policies.

About this task

Consistency controls provide a balance between the availability of the objects and the consistency of those objects across different Storage Nodes and sites. In general, you should use the **Read-after-new-write**

consistency level for your buckets.

If the **Read-after-new-write** consistency level does not meet the client application's requirements, you can change the consistency level by setting the bucket consistency level or by using the `Consistency-Control` header. The `Consistency-Control` header overrides the bucket consistency level.

> When you change a bucket's consistency level, only those objects that are ingested after the change are guaranteed to meet the revised level.

Steps

1. Select **View buckets** from the dashboard, or select **STORAGE (S3)** > **Buckets**.
2. Select the bucket name from the table.

   The bucket details page appears.

3. From the **Bucket options** tab, select the **Consistency level** accordion.
4. Select a consistency level for operations performed on the objects in this bucket.
   - **All**: Provides the highest level of consistency. All nodes receive the data immediately, or the request will fail.
   - **Strong-global**: Guarantees read-after-write consistency for all client requests across all sites.
   - **Strong-site**: Guarantees read-after-write consistency for all client requests within a site.
   - **Read-after-new-write** (default): Provides read-after-write consistency for new objects and eventual consistency for object updates. Offers high availability and data protection guarantees. Recommended for most cases.
   - **Available**: Provides eventual consistency for both new objects and object updates. For S3 buckets, use only as required (for example, for a bucket that contains log values that are rarely read, or for HEAD or GET operations on keys that don't exist). Not supported for S3 FabricPool buckets.
5. Select **Save changes**.

Enable or disable last access time updates

When grid administrators create the information lifecycle management (ILM) rules for a StorageGRID system, they can optionally specify that an object's last access time be used to determine whether to move that object to a different storage location. If you are using an S3 tenant, you can take advantage of such rules by enabling last access time updates for the objects in an S3 bucket.

These instructions only apply to StorageGRID systems that include at least one ILM rule that uses the **Last access time** option as an advanced filter or as a reference time. You can ignore these instructions if your StorageGRID system does not include such a rule. See Use Last access time in ILM rules for details.

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 Manage all buckets or Root access permission. These permissions override the permissions settings in group or bucket policies.

About this task

Last access time is one of the options available for the **Reference time** placement instruction for an ILM rule.

Setting the Reference time for a rule to Last access time lets grid administrators specify that objects be placed in certain storage locations based on when those objects were last retrieved (read or viewed).

For example, to ensure that recently viewed objects remain on faster storage, a grid administrator can create an ILM rule specifying the following:

- Objects that have been retrieved in the past month should remain on local Storage Nodes.
- Objects that have not been retrieved in the past month should be moved to an off-site location.

By default, updates to last access time are disabled. If your StorageGRID system includes an ILM rule that uses the **Last access time** option and you want this option to apply to objects in this bucket, you must enable updates to last access time for the S3 buckets specified in that rule.

> Updating the last access time when an object is retrieved can reduce StorageGRID performance, especially for small objects.

A performance impact occurs with last access time updates because StorageGRID must perform these additional steps every time objects are retrieved:

- Update the objects with new timestamps
- Add the objects to the ILM queue, so they can be reevaluated against current ILM rules and policy

The table summarizes the behavior applied to all objects in the bucket when last access time is disabled or enabled.

Type of request	Behavior if last access time is disabled (default)		Behavior if last access time is enabled	
	Last access time updated?	Object added to ILM evaluation queue?	Last access time updated?	Object added to ILM evaluation queue?
Request to retrieve an object, its access control list, or its metadata	No	No	Yes	Yes
Request to update an object's metadata	Yes	Yes	Yes	Yes
Request to copy an object from one bucket to another	• No, for the source copy • Yes, for the destination copy	• No, for the source copy • Yes, for the destination copy	• Yes, for the source copy • Yes, for the destination copy	• Yes, for the source copy • Yes, for the destination copy
Request to complete a multipart upload	Yes, for the assembled object	Yes, for the assembled object	Yes, for the assembled object	Yes, for the assembled object

Steps

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

2. Select the bucket name from the table.

   The bucket details page appears.

3. From the **Bucket options** tab, select the **Last access time updates** accordion.
4. Enable or disable last access time updates.
5. Select **Save changes**.

Change object versioning for a bucket

If you are using an S3 tenant, you can change the versioning state for S3 buckets.

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 Manage all buckets or Root access permission. These permissions override the permissions settings in group or bucket policies.

About this task

You can enable or suspend object versioning for a bucket. After you enable versioning for a bucket, it can't return to an unversioned state. However, you can suspend versioning for the bucket.

- Disabled: Versioning has never been enabled
- Enabled: Versioning is enabled
- Suspended: Versioning was previously enabled and is suspended

For more information, see the following:

- Object versioning
- ILM rules and policies for S3 versioned objects (Example 4)
- How objects are deleted

Steps

1. Select **View buckets** from the dashboard, or select **STORAGE (S3)** > **Buckets**.
2. Select the bucket name from the table.

   The bucket details page appears.

3. From the **Bucket options** tab, select the **Object versioning** accordion.
4. Select a versioning state for the objects in this bucket.

   Object versioning must remain enabled for a bucket used for cross-grid replication. If S3 Object Lock or legacy compliance is enabled, the **Object versioning** options are disabled.

Option	Description
Enable versioning	Enable object versioning if you want to store every version of each object in this bucket. You can then retrieve previous versions of an object as needed. Objects that were already in the bucket will be versioned when they are modified by a user.
Suspend versioning	Suspend object versioning if you no longer want new object versions to be created. You can still retrieve any existing object versions.

5. Select **Save changes**.

Use S3 Object Lock to retain objects

You can use S3 Object Lock if buckets and objects must comply with regulatory requirements for retention.

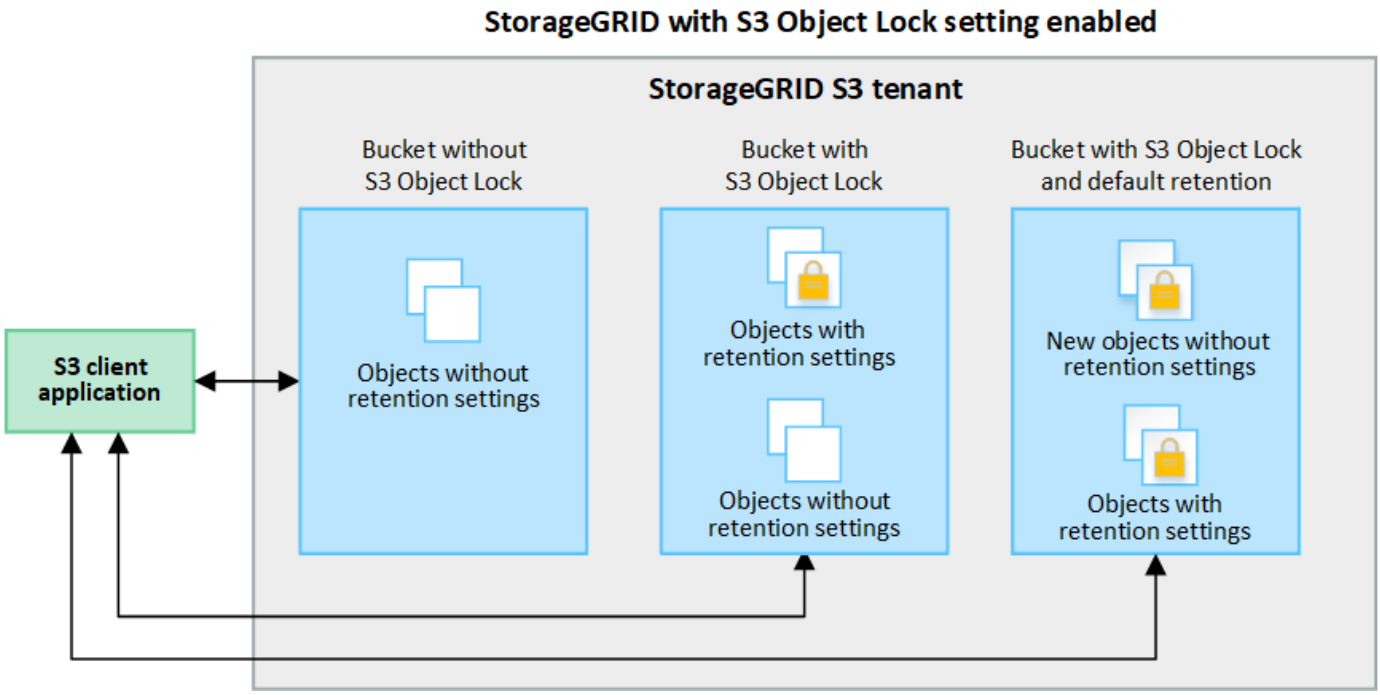
What is S3 Object Lock?

The StorageGRID S3 Object Lock feature is an object-protection solution that is equivalent to S3 Object Lock in Amazon Simple Storage Service (Amazon S3).

As shown in the figure, when the global S3 Object Lock setting is enabled for a StorageGRID system, an S3 tenant account can create buckets with or without S3 Object Lock enabled. If a bucket has S3 Object Lock enabled, bucket versioning is required and is enabled automatically.

If a bucket has S3 Object Lock enabled, S3 client applications can optionally specify retention settings for any object version saved to that bucket.

In addition, a bucket that has S3 Object Lock enabled can optionally have a default retention mode and retention period. The default settings apply only to objects that are added to the bucket without their own retention settings.



Retention modes

The StorageGRID S3 Object Lock feature supports two retention modes to apply different levels of protection to objects. These modes are equivalent to the Amazon S3 retention modes.

- In compliance mode:
  - The object can't be deleted until its retain-until-date is reached.
  - The object's retain-until-date can be increased, but it can't be decreased.
  - The object's retain-until-date can't be removed until that date is reached.
- In governance mode:
  - Users with special permission can use a bypass header in requests to modify certain retention settings.
  - These users can delete an object version before its retain-until-date is reached.
  - These users can increase, decrease, or remove an object's retain-until-date.

Retention settings for object versions

If a bucket is created with S3 Object Lock enabled, users can use the S3 client application to optionally specify the following retention settings for each object that is added to the bucket:

- **Retention mode**: Either compliance or governance.
- **Retain-until-date**: If an object version's retain-until-date is in the future, the object can be retrieved, but it can't be deleted.
- **Legal hold**: Applying a legal hold to an object version immediately locks that object. For example, you might need to put a legal hold on an object that is related to an investigation or legal dispute. A legal hold has no expiration date, but remains in place until it is explicitly removed. Legal holds are independent of the retain-until-date.

If an object is under a legal hold, no one can delete the object, regardless of its retention mode.

For details on the object settings, see Use S3 REST API to configure S3 Object Lock.

Default retention setting for buckets

If a bucket is created with S3 Object Lock enabled, users can optionally specify the following default settings for the bucket:

- **Default retention mode**: Either compliance or governance.
- **Default retention period**: How long new object versions added to this bucket should be retained, starting from the day they are added.

The default bucket settings apply only to new objects that don't have their own retention settings. Existing bucket objects aren't affected when you add or change these default settings.

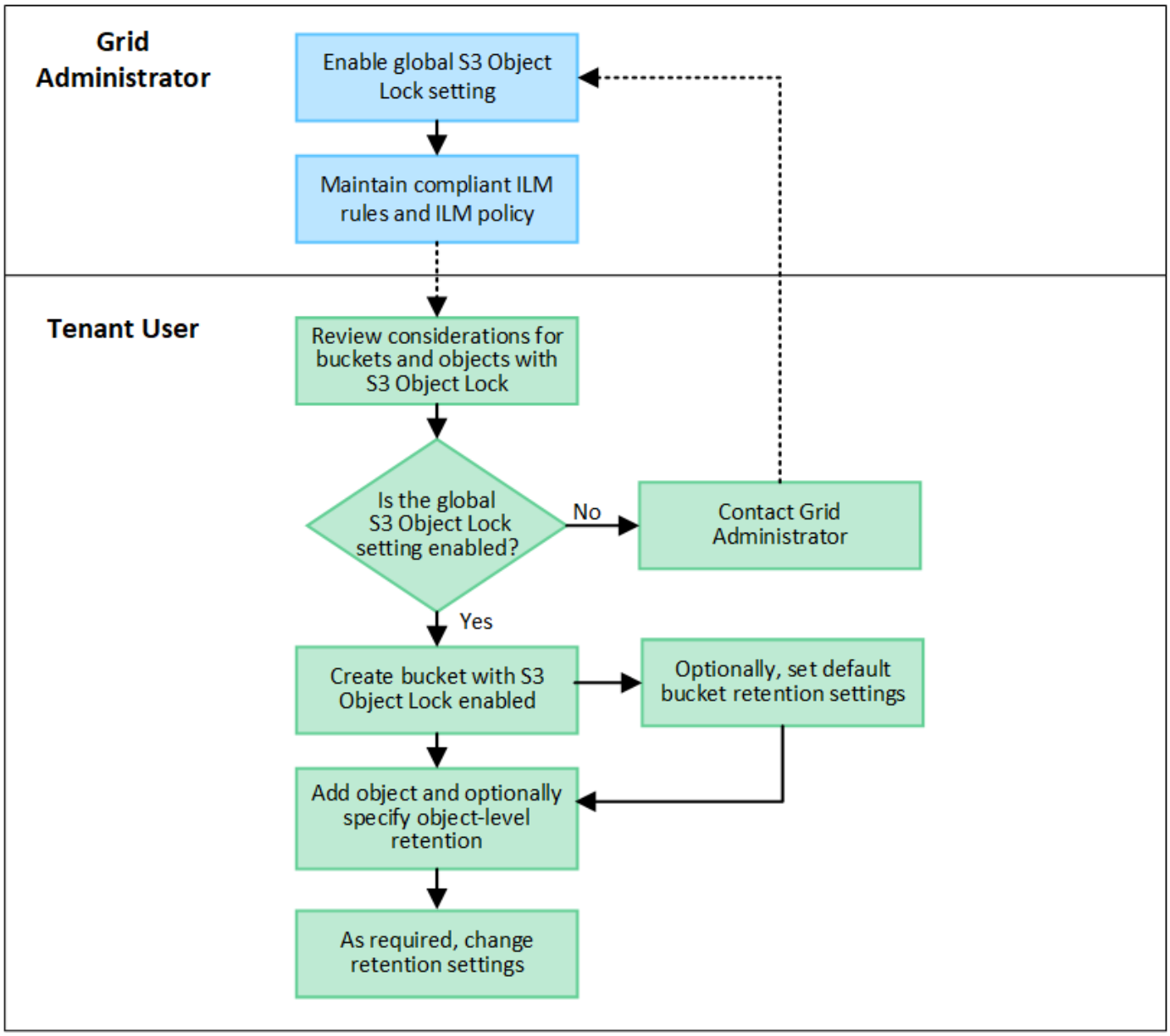
See Create an S3 bucket and Update S3 Object Lock default retention.

S3 Object Lock workflow

The workflow diagram shows the high-level steps for using the S3 Object Lock feature in StorageGRID.

Before you can create buckets with S3 Object Lock enabled, the grid administrator must enable the global S3 Object Lock setting for the entire StorageGRID system. The grid administrator must also ensure that the information lifecycle management (ILM) policy is "compliant"; it must meet the requirements of buckets with S3 Object Lock enabled. For details, contact your grid administrator or see the instructions for manage objects with S3 Object Lock.

After the global S3 Object Lock setting has been enabled, you can create buckets with S3 Object Lock enabled and optionally specify default retention settings for each bucket. In addition, you can use the S3 client application to optionally specify retention settings for each object version.



Requirements for buckets with S3 Object Lock enabled

- If the global S3 Object Lock setting is enabled for the StorageGRID system, you can use the Tenant Manager, the Tenant Management API, or the S3 REST API to create buckets with S3 Object Lock enabled.
- If you plan to use S3 Object Lock, you must enable S3 Object Lock when you create the bucket. You can't enable S3 Object Lock for an existing bucket.
- When S3 Object Lock is enabled for a bucket, StorageGRID automatically enables versioning for that bucket. You can't disable S3 Object Lock or suspend versioning for the bucket.
- Optionally, you can specify a default retention mode and retention period for each bucket using the Tenant Manager, the Tenant Management API, or the S3 REST API. The bucket's default retention settings apply only to new objects added to the bucket that don't have their own retention settings. You can override these default settings by specifying a retention mode and retain-until-date for each object version when it is uploaded.
- Bucket lifecycle configuration is supported for buckets with S3 Object Lock enabled.

- CloudMirror replication is not supported for buckets with S3 Object Lock enabled.

Requirements for objects in buckets with S3 Object Lock enabled

- To protect an object version, you can specify default retention settings for the bucket, or you can specify retention settings for each object version. Object-level retention settings can be specified using the S3 client application or the S3 REST API.
- Retention settings apply to individual object versions. An object version can have both a retain-until-date and a legal hold setting, one but not the other, or neither. Specifying a retain-until-date or a legal hold setting for an object protects only the version specified in the request. You can create new versions of the object, while the previous version of the object remains locked.

Lifecycle of objects in buckets with S3 Object Lock enabled

Each object that is saved in a bucket with S3 Object Lock enabled goes through these stages:

1. **Object ingest**

   When an object version is added to bucket that has S3 Object Lock enabled, retention settings are applied as follows:

   - If retention settings are specified for the object, the object-level settings are applied. Any default bucket settings are ignored.
   - If no retention settings are specified for the object, the default bucket settings are applied, if they exist.
   - If no retention settings are specified for the object or the bucket, the object is not protected by S3 Object Lock.

   If retention settings are applied, both the object and any S3 user-defined metadata are protected.

2. **Object retention and deletion**

   Multiple copies of each protected object are stored by StorageGRID for the specified retention period. The exact number and type of object copies and the storage locations are determined by the compliant rules in the active ILM policy. Whether a protected object can be deleted before its retain-until-date is reached depends on its retention mode.

   - If an object is under a legal hold, no one can delete the object, regardless of its retention mode.

Can I still manage legacy Compliant buckets?

The S3 Object Lock feature replaces the Compliance feature that was available in previous StorageGRID versions. If you created compliant buckets using a previous version of StorageGRID, you can continue to manage the settings of these buckets; however, you can no longer create new compliant buckets. For instructions, see NetApp Knowledge Base: How to manage legacy Compliant buckets in StorageGRID 11.5.

Update S3 Object Lock default retention

If you enabled S3 Object Lock when you created the bucket, you can edit the bucket to change the default retention settings. You can enable (or disable) default retention and set a default retention mode and retention period.

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 Manage all buckets or Root access permission. These permissions override the permissions settings in group or bucket policies.
- S3 Object Lock is enabled globally for your StorageGRID system, and you enabled S3 Object Lock when you created the bucket. See Use S3 Object Lock to retain objects.

Steps

1. Select **View buckets** from the dashboard, or select **STORAGE (S3)** > **Buckets**.
2. Select the bucket name from the table.

   The bucket details page appears.

3. From the **Bucket options** tab, select the **S3 Object Lock** accordion.
4. Optionally, enable or disable **Default retention** for this bucket.

   Changes to this setting don't apply to objects already in the bucket or to any objects that might have their own retention periods.

5. If **Default retention** is enabled, specify a **Default retention mode** for the bucket.

Default retention mode	Description
Compliance	• The object can't be deleted until its retain-until-date is reached. • The object's retain-until-date can be increased, but it can't be decreased. • The object's retain-until-date can't be removed until that date is reached.
Governance	• Users with the `s3:BypassGovernanceRetention` permission can use the `x-amz-bypass-governance-retention: true` request header to bypass retention settings. • These users can delete an object version before its retain-until-date is reached. • These users can increase, decrease, or remove an object's retain-until-date.

6. If **Default retention** is enabled, specify the **Default retention period** for the bucket.

   The **Default retention period** indicates how long new objects added to this bucket should be retained, starting from the time they are ingested. Specify a value between 1 and 36,500 days or between 1 and 100 years, inclusive.

7. Select **Save changes**.

Configure cross-origin resource sharing (CORS)

You can configure cross-origin resource sharing (CORS) for an S3 bucket if you want that bucket and objects in that bucket to be accessible to web applications in other domains.

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 Manage all buckets or Root access permission. These permissions override the permissions settings in group or bucket policies.

About this task

Cross-origin resource sharing (CORS) is a security mechanism that allows client web applications in one domain to access resources in a different domain. For example, suppose you use an S3 bucket named `Images` to store graphics. By configuring CORS for the `Images` bucket, you can allow the images in that bucket to be displayed on the website `http://www.example.com`.

Enable CORS for a bucket

Steps

1. Use a text editor to create the required XML.

   This example shows the XML used to enable CORS for an S3 bucket. This XML allows any domain to send GET requests to the bucket, but it only allows the `http://www.example.com` domain to send POST and DELETE requests. All request headers are allowed.

   ```
   <CORSConfiguration
       xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
       <CORSRule>
           <AllowedOrigin>*</AllowedOrigin>
           <AllowedMethod>GET</AllowedMethod>
           <AllowedHeader>*</AllowedHeader>
       </CORSRule>
       <CORSRule>
           <AllowedOrigin>http://www.example.com</AllowedOrigin>
           <AllowedMethod>GET</AllowedMethod>
           <AllowedMethod>POST</AllowedMethod>
           <AllowedMethod>DELETE</AllowedMethod>
           <AllowedHeader>*</AllowedHeader>
       </CORSRule>
   </CORSConfiguration>
   ```

   For more information about the CORS configuration XML, see Amazon Web Services (AWS) Documentation: Amazon Simple Storage Service Developer Guide.

2. Select **View buckets** from the dashboard, or select **STORAGE (S3)** > **Buckets**.
3. Select the bucket name from the table.

   The bucket details page appears.

4. From the **Bucket access** tab, select the **Cross-Origin Resource Sharing (CORS)** accordion.
5. Select the **Enable CORS** checkbox.
6. Paste the CORS configuration XML into the text box.

7. Select **Save changes**.

Modify CORS setting

Steps

1. Update the CORS configuration XML in the text box, or select **Clear** to start over.
2. Select **Save changes**.

Disable CORS setting

Steps

1. Clear the **Enable CORS** checkbox.
2. Select **Save changes**.

Delete objects in bucket

You can use the Tenant Manager to delete the objects in one or more buckets.

Considerations and requirements

Before performing these steps, note the following:

- When you delete the objects in a bucket, StorageGRID permanently removes all objects and all object versions in each selected bucket from all nodes and sites in your StorageGRID system. StorageGRID also removes any related object metadata. You will not be able to recover this information.
- Deleting all of the objects in a bucket might take minutes, days, or even weeks, based on the number of objects, object copies, and concurrent operations.
- If a bucket has S3 Object Lock enabled, it might remain in the **Deleting objects: read-only** state for *years*.

A bucket that uses S3 Object Lock will remain in the **Deleting objects: read-only** state until the retention date is reached for all objects and any legal holds are removed.

- While objects are being deleted, the bucket's state is **Deleting objects: read-only**. In this state, you can't add new objects to the bucket.
- When all objects have been deleted, the bucket remains in the read-only state. You can do one of the following:
  - Return the bucket to write mode and reuse it for new objects
  - Delete the bucket
  - Keep the bucket in read-only mode to reserve its name for future use
- If a bucket has object versioning enabled, any delete markers that are in the bucket when you start these steps will not be removed by the delete objects operation. If you want to delete a versioned bucket after all objects have been deleted, you must remove any pre-existing delete markers.
- If you use cross-grid replication, note the following:
  - Using this option does not delete any objects from the bucket on the other grid.
  - If you select this option for the source bucket, the **Cross-grid replication failure** alert will be triggered if you add objects to the destination bucket on the other grid. If you can't guarantee no one will add objects to the bucket on the other grid, disable cross-grid replication for that bucket before deleting all

bucket objects.

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. This permission overrides the permissions settings in group or bucket policies.

Steps

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

   The Buckets page appears and shows all existing S3 buckets.

2. Use the **Actions** menu or the details page for a specific bucket.

   Actions menu

   a. Select the checkbox for each bucket you want to delete objects from.

   b. Select **Actions** > **Delete objects in bucket**.

   Details page

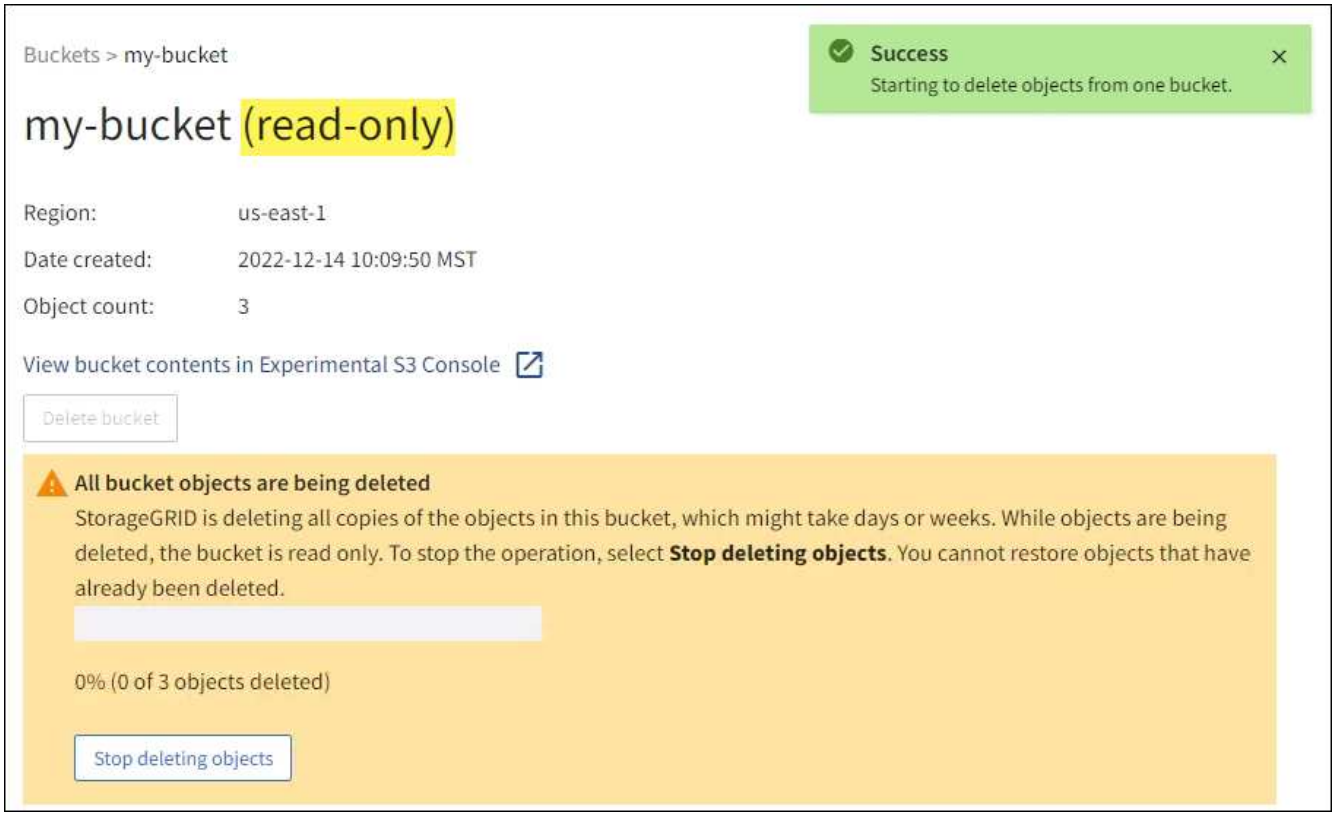
   a. Select a bucket name to display its details.

   b. Select **Delete objects in bucket**.

3. When the confirmation dialog box appears, review the details, enter **Yes**, and select **OK**.
4. Wait for the delete operation to begin.

   After a few minutes:

   - A yellow status banner appears on the bucket details page. The progress bar represents what percentage of objects have been deleted.
   - **(read-only)** appears after the bucket's name on the bucket details page.
   - **(Deleting objects: read-only)** appears next to the bucket's name on the Buckets page.

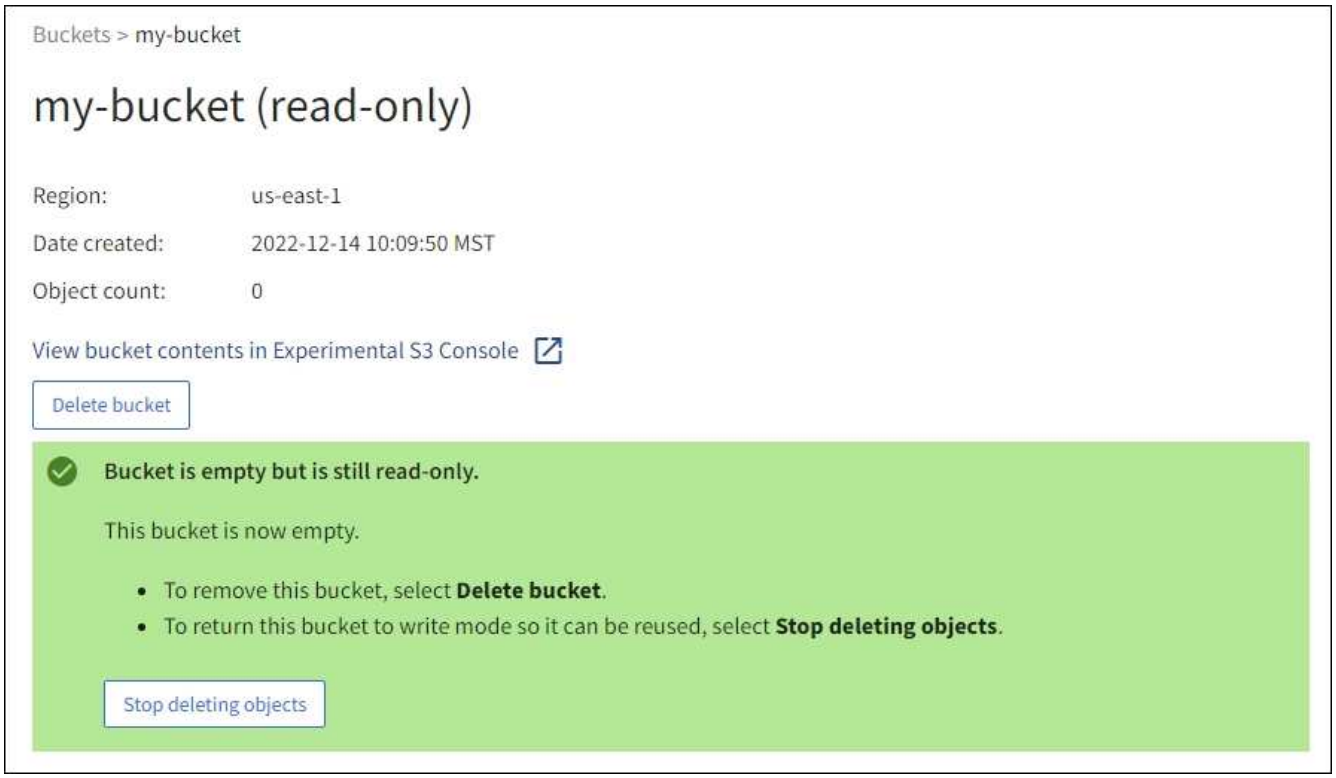


5. As required while the operation is running, select **Stop deleting objects** to halt the process. Then, optionally, select **Delete objects in bucket** to resume the process.

   When you select **Stop deleting objects**, the bucket is returned to write mode; however, you can't access or restore any objects that have been deleted.

6. Wait for the operation to complete.

   When the bucket is empty, the status banner is updated, but the bucket remains read only.



7. Do one of the following:
   - Exit the page to keep the bucket in read-only mode. For example, you might keep an empty bucket in read-only mode to reserve the bucket name for future use.
   - Delete the bucket. You can select **Delete bucket** to delete a single bucket or return the Buckets page and select **Actions** > **Delete** buckets to remove more than one bucket.

     If you are unable to delete a versioned bucket after all objects were deleted, delete markers might remain. To delete the bucket, you must remove all remaining delete markers.

   - Return the bucket to write mode and optionally reuse it for new objects. You can select **Stop deleting objects** for a single bucket or return to the Buckets page and select **Action** > **Stop deleting objects** for more than one bucket.

Delete S3 bucket

You can use the Tenant Manager to delete one or more S3 buckets that are empty.

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 Manage all buckets or Root access permission. These permissions override the permissions settings in group or bucket policies.
- The buckets you want to delete are empty.

About this task

These instructions describe how to delete an S3 bucket using the Tenant Manager. You can also delete S3 buckets using the Tenant Management API or the S3 REST API.

You can't delete an S3 bucket if it contains objects, noncurrent object versions, or delete markers. For information about how S3 versioned objects are deleted, see How objects are deleted.

Steps

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

   The Buckets page appears and shows all existing S3 buckets.

2. Use the **Actions** menu or the details page for a specific bucket.

   Actions menu

   a. Select the checkbox for each bucket you want to delete.

   b. Select **Actions** > **Delete buckets**.

   Details page

   a. Select a bucket name to display its details.

   b. Select **Delete bucket**.

3. When the confirmation dialog box appears, select **Yes**.

   StorageGRID confirms that each bucket is empty and then deletes each bucket. This operation might take a few minutes.

   If a bucket is not empty, an error message appears. You must delete all objects and any delete markers in the bucket before you can delete the bucket.

Use Experimental S3 Console

You can use S3 Console to view the objects in an S3 bucket.

You can also use S3 Console to do the following:

- Add and delete objects, object versions, and folders
- Rename objects
- Move and copy objects between buckets and folders
- Manage object tags
- View object metadata
- Download objects

> The S3 Console is marked as "experimental" because it is not yet complete or approved for use in a production environment. Tenants should only use S3 Console when performing functions for a small number of objects, such as when uploading objects to simulate a new ILM policy, troubleshooting ingest issues, or using proof-of-concept or non-production grids.

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 or that has both the Manage all buckets

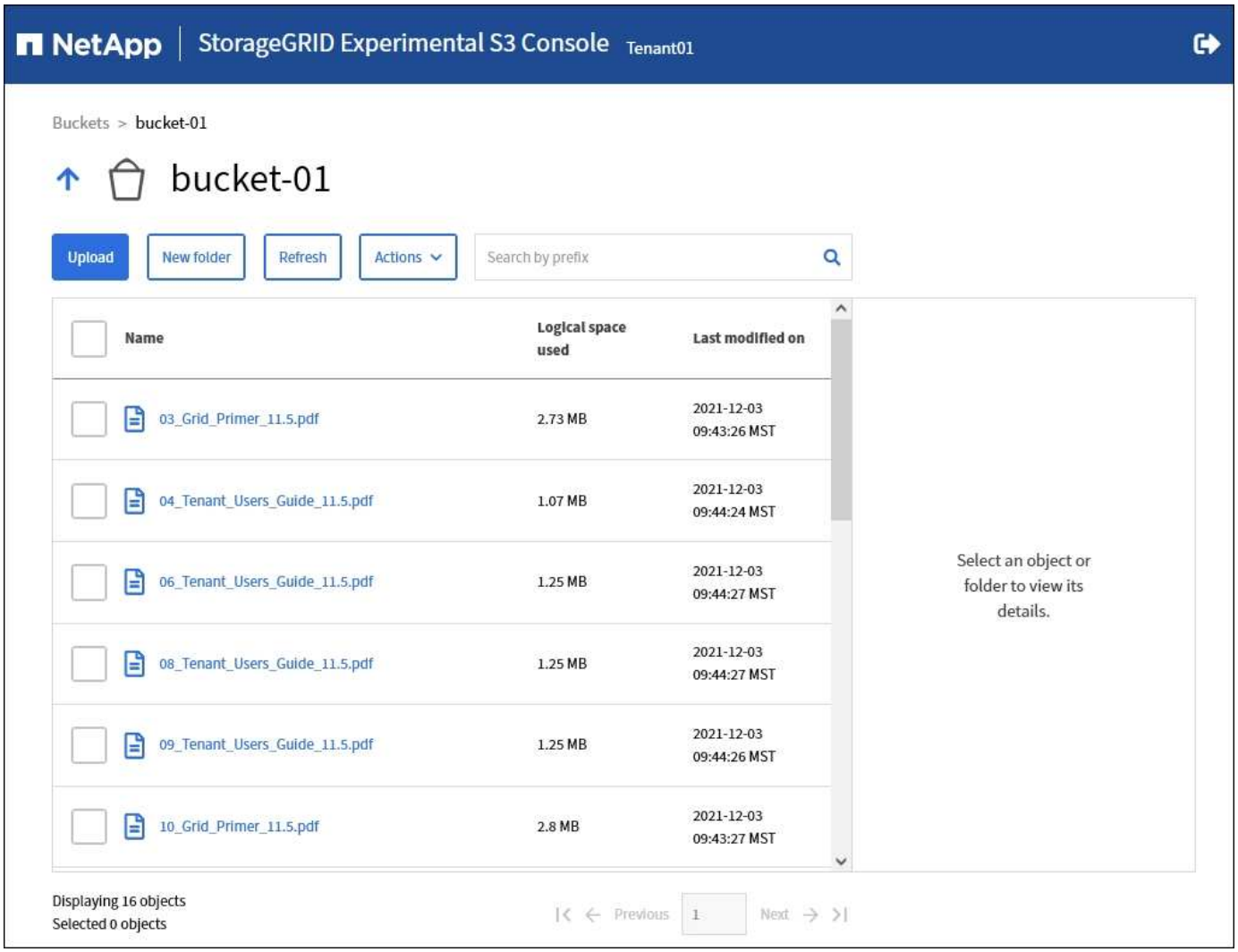
and Manage objects with S3 Console permissions.

> Users who have the Manage objects with S3 Console permission but who don't have the Manage all buckets permission can still navigate directly to the Experimental S3 Console.

- You have created a bucket.
- An S3 Group or Bucket policy has been configured for the user.
- You know the user's access key ID and secret access key. Optionally, you have a `.csv` file containing this information. See the instructions for creating access keys.

Steps

1. Select **Buckets**.
2. Select Experimental S3 Console . You can also access this link from the bucket details page.
3. On the Experimental S3 Console sign-in page, paste the access key ID and secret access key into the fields. Otherwise, select **Upload access keys** and select your `.csv` file.
4. Select **Sign in**.
5. Manage objects as needed.



Copyright information

Trademark information