Create ILM policy

StorageGRID 11.7

NetApp
January 09, 2024

Table of Contents

Create ILM policy

Create an ILM policy: Overview

An information lifecycle management (ILM) policy is an ordered set of ILM rules that determines how the StorageGRID system manages object data over time.

When you create an ILM policy, you start by selecting and arranging the ILM rules. Then, you verify the behavior of your proposed policy by simulating it against previously ingested objects. When you are satisfied that the proposed policy is functioning as intended, you can activate it to create the active policy.

> An ILM policy that has been incorrectly configured can result in unrecoverable data loss. Before activating an ILM policy, carefully review the ILM policy and its ILM rules, and then simulate the ILM policy. Always confirm that the ILM policy will work as intended.

Default ILM policy

When you install StorageGRID and add sites, a default ILM policy is automatically created. If your grid contains one site, the default policy contains a default rule that replicates two copies of each object at that site. If your grid contains more than one site, the default rule replicates one copy of each object at each site.

If the default policy does not meet your storage requirements, you can create your own rules and policy. See What an ILM rule is and Creating a proposed ILM policy.

How does an ILM policy evaluate objects?

The active ILM policy for your StorageGRID system controls the placement, duration, and data protection of all objects.

When clients save objects to StorageGRID, the objects are evaluated against the ordered set of ILM rules in the active policy, as follows:

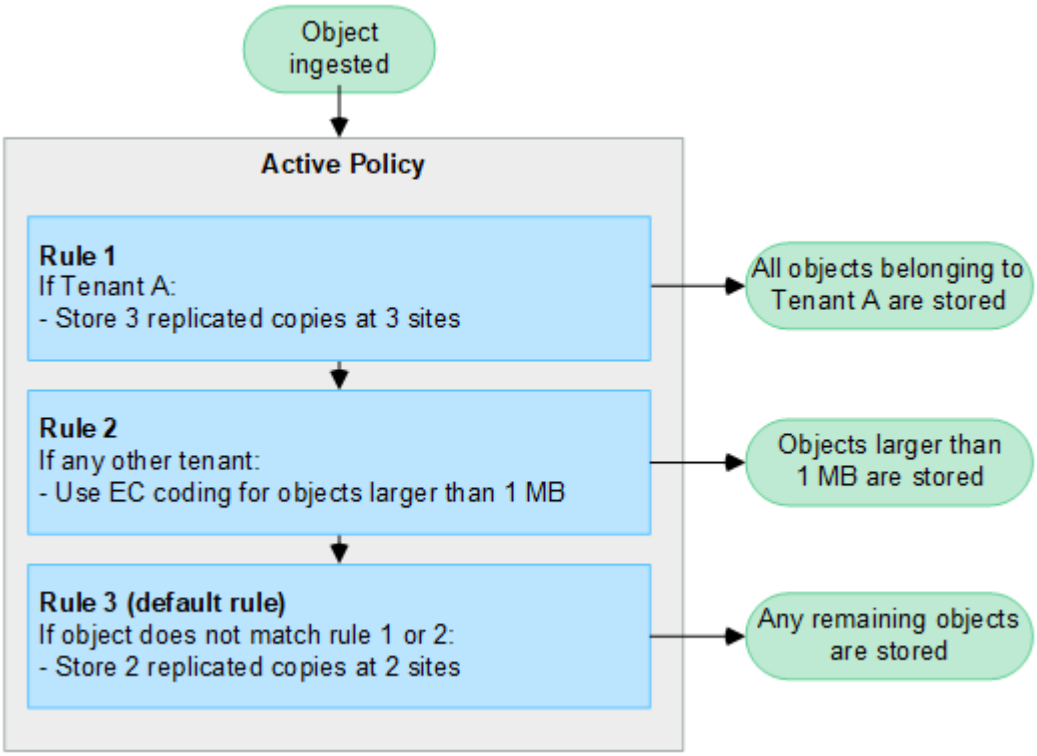
1. If the filters for the first rule in the policy match an object, the object is ingested according to that rule's ingest behavior and stored according to that rule's placement instructions.
2. If the filters for the first rule don't match the object, the object is evaluated against each subsequent rule in the policy until a match is made.
3. If no rules match an object, the ingest behavior and placement instructions for the default rule in the policy are applied. The default rule is the last rule in a policy. The default rule must apply to all tenants, all buckets, and all object versions and can't use any advanced filters.

Example ILM policy

As an example, an ILM policy could contain three ILM rules that specify the following:

- **Rule 1: Replicated copies for Tenant A**
  - Match all objects belonging to Tenant A.
  - Store these objects as three replicated copies at three sites.
  - Objects belonging to other tenants aren't matched by Rule 1, so they are evaluated against Rule 2.
- **Rule 2: Erasure coding for objects greater than 1 MB**

    - Match all objects from other tenants, but only if they are greater than 1 MB. These larger objects are stored using 6+3 erasure coding at three sites.
    - Does not match objects 1 MB or smaller, so these objects are evaluated against Rule 3.
- **Rule 3: 2 copies 2 data centers** (default)
    - Is the last and default rule in the policy. Does not use filters.
    - Make two replicated copies of all objects not matched by Rule 1 or Rule 2 (objects not belonging to Tenant A that are 1 MB or smaller).



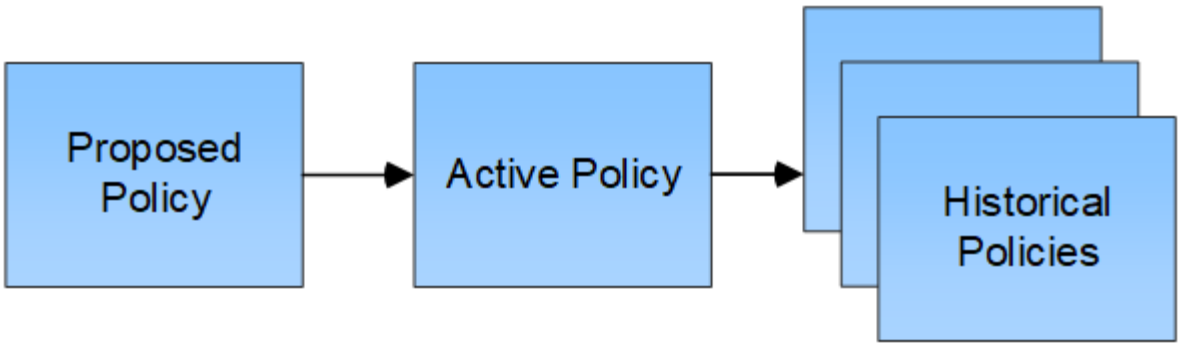
What are proposed, active, and historical policies?

Every StorageGRID system must have one active ILM policy. A StorageGRID system might also have one proposed ILM policy and any number of historical policies.

When you first create an ILM policy, you create a proposed policy by selecting one or more ILM rules and arranging them in a specific order. After you have simulated the proposed policy to confirm its behavior, you activate it to create the active policy.

When you activate a new ILM policy, StorageGRID uses that policy to manage all objects, including existing objects and newly ingested objects. Existing objects might be moved to new locations when the ILM rules in the new policy are implemented.

Activating the proposed policy causes the previously active policy to become a historical policy. Historical ILM policies can’t be deleted.



Considerations for creating an ILM policy

- Only use the system-provided policy, Baseline 2 copies policy, in test systems. For StorageGRID 11.6 and earlier, the Make 2 Copies rule in this policy uses the All Storage Nodes storage pool, which contains all sites. If your StorageGRID system has more than one site, two copies of an object might be placed on the same site.

> The All Storage Nodes storage pool is automatically created during the installation of StorageGRID 11.6 and earlier. If you upgrade to a later version of StorageGRID, the All Storage Nodes pool will still exist. If you install StorageGRID 11.7 or later as a new installation, the All Storage Nodes pool is not created.

- When designing a new policy, consider all of the different types of objects that might be ingested into your grid. Make sure the policy includes rules to match and place these objects as required.
- Keep the ILM policy as simple as possible. This avoids potentially dangerous situations where object data is not protected as intended when changes are made to the StorageGRID system over time.
- Make sure that the rules in the policy are in the correct order. When the policy is activated, new and existing objects are evaluated by the rules in the order listed, starting at the top. For example, if the first rule in a policy matches an object, that object will not be evaluated by any other rule.
- The last rule in every ILM policy is the default ILM rule, which can't use any filters. If an object has not been matched by another rule, the default rule controls where that object is placed and for how long it is retained.
- Before activating a new policy, review any changes that the policy is making to the placement of existing objects. Changing an existing object's location might result in temporary resource issues when the new placements are evaluated and implemented.

Create a proposed ILM policy

You can create a proposed ILM policy from scratch, or you can clone the current active policy if you want to start with the same set of rules.

Before creating your own policy, verify that the default ILM policy does not meet your storage requirements.

> If the global S3 Object Lock setting has been enabled, you must ensure that the ILM policy is compliant with the requirements of buckets that have S3 Object Lock enabled. In this section, follow the instructions that mention having S3 Object Lock enabled.

Before you begin

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

- You have the required access permissions.
- You have created ILM rules based on whether S3 Object Lock is enabled.

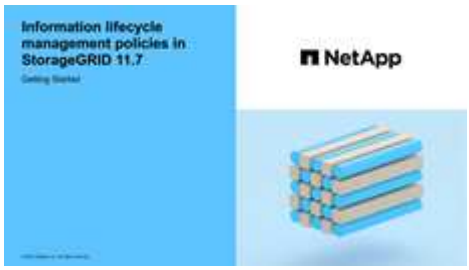
S3 Object Lock not enabled

- You have created the ILM rules you want to add to the proposed policy. As required, you can save a proposed policy, create additional rules, and then edit the proposed policy to add the new rules.
- You have created a default ILM rule that does not contain any filters.

S3 Object Lock enabled

- The global S3 Object Lock setting is already enabled for the StorageGRID system.
- You have created the compliant and non-compliant ILM rules you want to add to the proposed policy. As required, you can save a proposed policy, create additional rules, and then edit the proposed policy to add the new rules.
- You have created a default ILM rule for the policy that is compliant.

- Optionally, you have watched the video: Video: Information lifecycle management policies in StorageGRID 11.7



See also Create an ILM policy: Overview.

About this task

Typical reasons for creating a proposed ILM policy include:

- You added a new site and need to use new ILM rules to place objects at that site.
- You are decommissioning a site and you need to remove all ILM rules that refer to the site.
- You added a new tenant that has special data protection requirements.
- You started to use a Cloud Storage Pool.

> Only use the system-provided policy, Baseline 2 copies policy, in test systems. For StorageGRID 11.6 and earlier, the default rule in this policy uses the All Storage Nodes storage pool, which contains all sites. If your StorageGRID system has more than one site, two copies of an object might be placed on the same site.

Steps

1. Select **ILM** > **Policies**.

   If the global S3 Object Lock setting is enabled, the ILM policies page indicates which ILM rules are compliant.

2. Determine how you want to create the proposed ILM policy.

Start from scratch

a. If a proposed ILM policy currently exists, select **Proposed policy** > **Actions** > **Remove**.

   You can't create a new proposed policy if a proposed policy already exists.

b. Select **Create proposed policy** > **Create new policy**.

Start with rules from active policy

a. If a proposed ILM policy currently exists, select **Proposed policy** > **Actions** > **Remove**.

   You can't clone the active policy if a proposed policy already exists.

b. Select **Create proposed policy** > **Clone active policy**.

Edit existing proposed policy

a. Select **Proposed policy** > **Actions** > **Edit**.

3. In the **Proposed policy name** field, enter a unique name for the proposed policy.
4. In the **Reason for change** field, enter the reason you are creating a new proposed policy.
5. To add rules to the policy, select **Select rules**. Select a rule name to view the settings for that rule.

   Periodically, the list of rules is automatically updated to reflect additions or removals. If a rule is removed after you select it, an error message appears.

   If you are cloning a policy:

   - The rules used by the policy you are cloning are selected.
   - If the policy you are cloning used any rules with no filters that were not the default rule, you are prompted to remove all but one of those rules.
   - If the default rule used a filter, you are prompted to select a new default rule.
   - If the default rule was not the last rule, you can move the rule to the end of the new policy.

S3 Object Lock not enabled

a. Select one default rule for the proposed policy. To create a new default rule, select **ILM rules page**.

   The default rule applies to any objects that don't match another rule in the policy. The default rule can't use any filters and is always evaluated last.

   > Don't use the Make 2 Copies rule as the default rule for a policy. The Make 2 Copies rule uses a single storage pool, All Storage Nodes, which contains all sites. If your StorageGRID system has more than one site, two copies of an object might be placed on the same site.

S3 Object Lock enabled

a. Select one default rule for the proposed policy. To create a new default rule, select **ILM rules page**.

   The list of rules contains only the rules that are compliant and don't use any filters.

   > Don't use the Make 2 Copies rule as the default rule for a policy. The Make 2 Copies rule uses a single storage pool, All Storage Nodes, which contains all sites. If you use this rule, multiple copies of an object might be placed on the same site.

b. If you need a different "default" rule for objects in non-compliant S3 buckets, select **Include a rule without filters for non-compliant S3 buckets**, and select one non-compliant rule that does not use a filter.

   For example, you might want to use a Cloud Storage Pool to store objects in buckets that don't have S3 Object Lock enabled.

   > You can only select one non-compliant rule that does not use a filter.

See also Example 7: Compliant ILM policy for S3 Object Lock.

6. When you are done selecting the default rule, select **Continue**.
7. For the Other rules step, select any other rules you want to add to the policy. These rules use at least one filter (tenant account, bucket name, advanced filter, or the Noncurrent reference time). Then select **Select**.

   The Create a proposed policy window now lists the rules you selected. The default rule is at the end, with the other rules above it.

   If S3 Object Lock is enabled and you also selected a non-compliant "default" rule, that rule is added as the second-to-last rule in the policy.

   > A warning appears if any rule does not retain objects forever. When you activate this policy, you must confirm that you want StorageGRID to delete objects when the placement instructions for the default rule elapse (unless a bucket lifecycle keeps the objects for a longer time period).

8. Drag the rows for the non-default rules to determine the order in which these rules will be evaluated.

   You can't move the default rule. If S3 Object Lock is enabled, you also can't move the non-compliant

"default" rule if one was selected.

> You must confirm that the ILM rules are in the correct order. When the policy is activated, new and existing objects are evaluated by the rules in the order listed, starting at the top.

9. As required, select **Select rules** to add or remove rules.
10. When you are done, select **Save**.
11. Go to Simulate an ILM policy. You should always simulate a proposed policy before activating it to ensure it works as expected.

Simulate an ILM policy

Simulate a proposed policy on test objects before activating the policy and applying it to your production data. The simulation window provides a standalone environment that is safe for testing policies before they are activated and applied to data in the production environment.

Before you begin

- You are signed in to the Grid Manager using a supported web browser.
- You have the required access permissions.
- You know the S3 bucket/object-key or the Swift container/object-name for each object you want to test.

About this task

Carefully select the objects you want the proposed policy to test. To simulate a policy thoroughly, you should test at least one object for each filter in each rule.

For example, if a policy includes one rule to match objects in bucket A and another rule to match objects in bucket B, you must select at least one object from bucket A and one object from bucket B to test the policy thoroughly. You must also select at least one object from another bucket to test the default rule.

When simulating a policy, the following considerations apply:

- After you make changes to a policy, save the proposed policy. Then, simulate the behavior of the saved proposed policy.
- When you simulate a policy, the ILM rules in the policy filter the test objects, so you can see which rule was applied to each object. However, no object copies are made and no objects are placed. Running a simulation does not modify your data, rules, or the policy in any way.
- The Simulate proposed policy window retains the objects you tested until you select either **Clear all** or the remove icon ✕ for each object in the Simulation results list.
- Simulation returns the name of the matched rule. To determine which storage pool or erasure coding profile is in effect, select the name of the rule to go to the rule details page, where you can view the retention diagram and other details about the rule.
- If S3 versioning is enabled, you can enter the version ID for the version of the object you want to use for the simulation.

Steps

1. Create a proposed policy.
2. Using an S3 or Swift client or the experimental S3 Console, which is available in Tenant Manager for each

tenant, ingest the objects required to test each rule.

3. On the ILM policy page, Proposed policy tab, select **Simulate**.
4. In the **Object** field, enter the S3 `bucket/object-key` or the Swift `container/object-name` for a test object. For example, `bucket-01/filename.png`.
5. Optionally, enter a version ID for the object in the **Version ID** field.
6. Select **Simulate**.
7. In the Simulation results section, confirm that each object was matched by the correct rule.

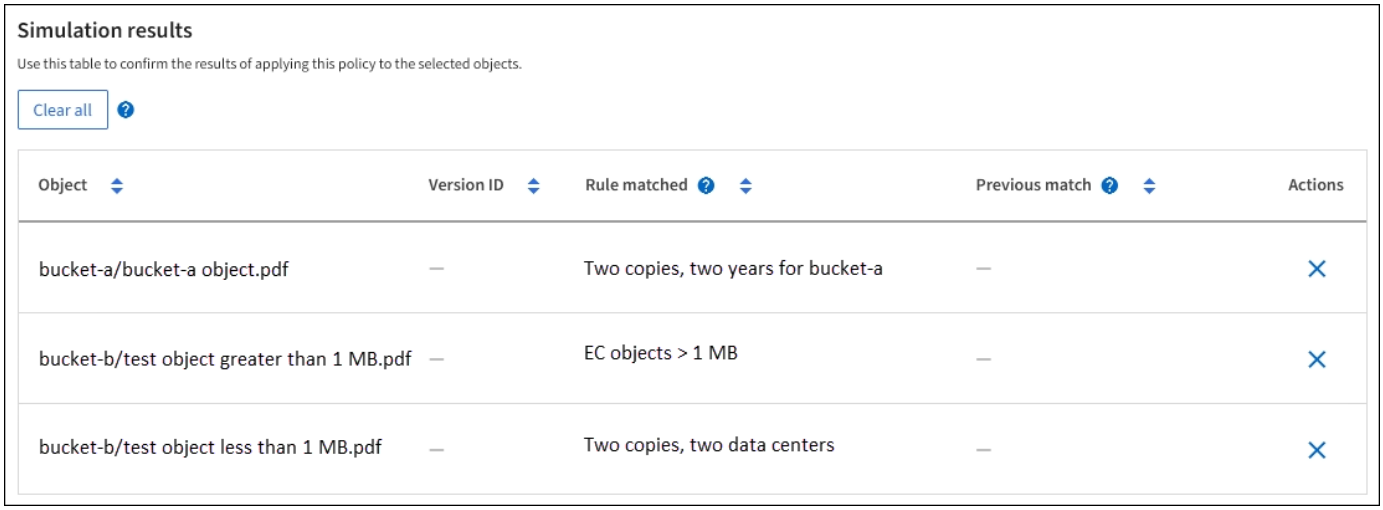
Example 1: Verify rules when simulating a proposed ILM policy

This example describes how to verify rules when simulating a proposed policy.

In this example, the **Example ILM policy** is being simulated against the ingested objects in two buckets. The policy includes three rules, as follows:

- The first rule, **Two copies, two years for bucket-a**, applies only to objects in bucket-a.
- The second rule, **EC objects > 1 MB**, applies to all buckets but filters on objects greater than 1 MB.
- The third rule, **Two copies, two data centers**, is the default rule. It does not include any filters and does not use the Noncurrent reference time.

After simulating the policy, confirm that each object was matched by the correct rule.



In this example:

- `bucket-a/bucket-a object.pdf` correctly matched the first rule, which filters on objects in `bucket-a`.
- `bucket-b/test object greater than 1 MB.pdf` is in `bucket-b`, so it did not match the first rule. Instead, it was correctly matched by the second rule, which filters on objects greater than 1 MB.
- `bucket-b/test object less than 1 MB.pdf` did not match the filters in the first two rules, so it will be placed by the default rule, which includes no filters.

Example 2: Reorder rules when simulating a proposed ILM policy

This example shows how you can reorder rules to change the results when simulating a policy.

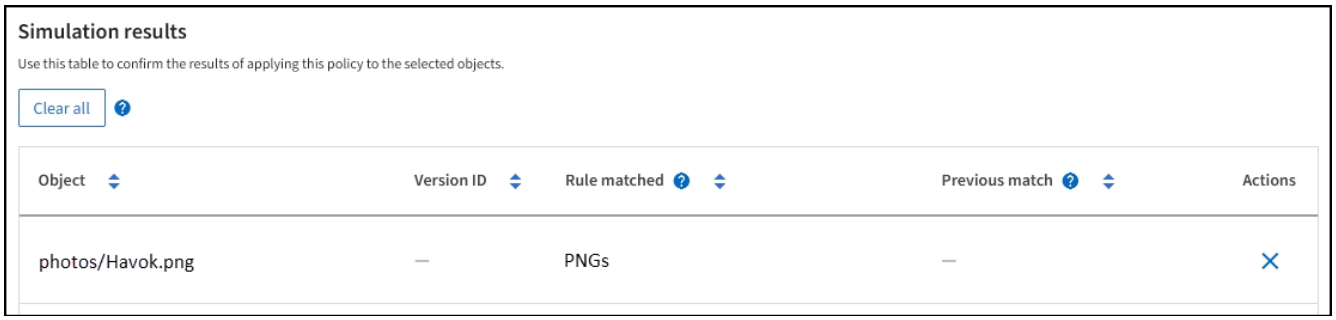
In this example, the **Demo** policy is being simulated. This policy, which is intended to find objects that have series=x-men user metadata, includes three rules, as follows:

- The first rule, **PNGs**, filters for key names that end in `.png`.
- The second rule, **X-men**, applies only to objects for Tenant A and filters for `series=x-men` user metadata.
- The last rule, **Two copies two data centers**, is the default rule, which matches any objects that don't match the first two rules.

Steps

1. After adding the rules and saving the policy, select **Simulate**.
2. In the **Object** field, enter the S3 bucket/object-key or the Swift container/object-name for a test object, and select **Simulate**.

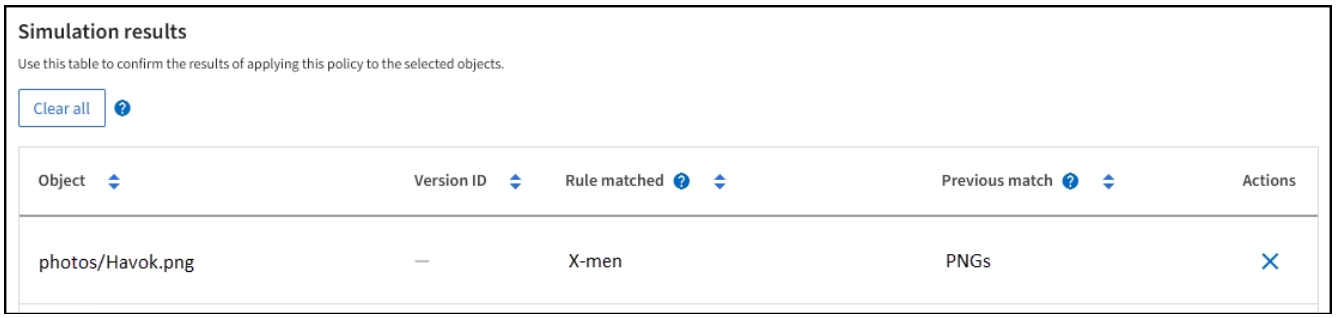
   The Simulation results appear, showing that the `Havok.png` object was matched by the **PNGs** rule.



   However, `Havok.png` was meant to test the **X-men** rule.

3. To resolve the issue, reorder the rules.
   a. Select **Finish** to close the Simulate ILM Policy window.
   b. Select **Actions** > **Edit** to edit the policy.
   c. Drag the **X-men** rule to the top of the list.
   d. Select **Save**.
4. Select **Simulate**.

   The objects you previously tested are re-evaluated against the updated policy, and the new simulation results are shown. In the example, the Rule matched column shows that the `Havok.png` object now matches the X-men metadata rule, as expected. The Previous match column shows that the PNGs rule matched the object in the previous simulation.

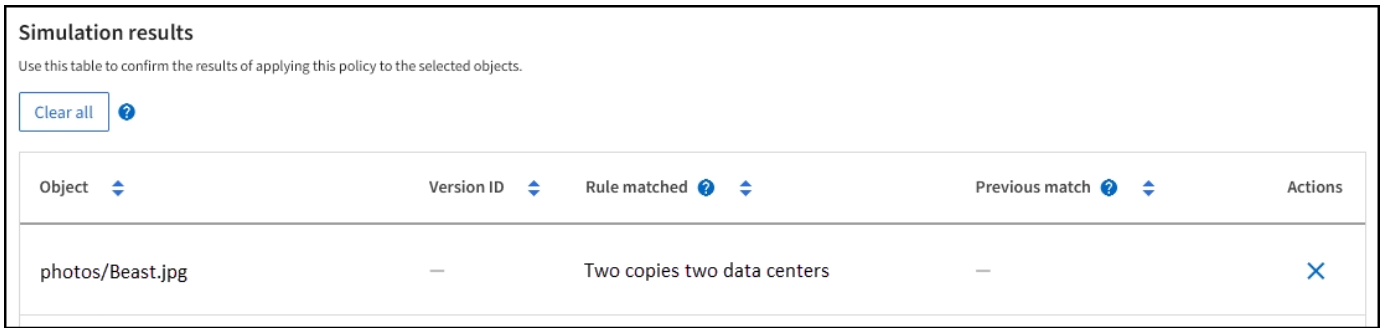


If you stay on the Proposed policy tab, you can re-simulate a policy after making changes without needing to re-enter the names of the test objects.

Example 3: Correct a rule when simulating a proposed ILM policy

This example shows how to simulate a policy, correct a rule in the policy, and continue the simulation.

In this example, the **Demo** policy is being simulated. This policy is intended to find objects that have `series=x-men` user metadata. However, unexpected results occurred when simulating this policy against the `Beast.jpg` object. Instead of matching the X-men metadata rule, the object matched the default rule, Two copies two data centers.



When a test object is not matched by the expected rule in the policy, you must examine each rule in the policy and correct any errors.

Steps

1. Select **Finish** to close the Simulate policy dialog. On the Proposed policy tab, select **Retention diagram**. Then select **Expand all** or **View details** for each rule as needed.
2. Review the rule's tenant account, reference time, and filtering criteria.

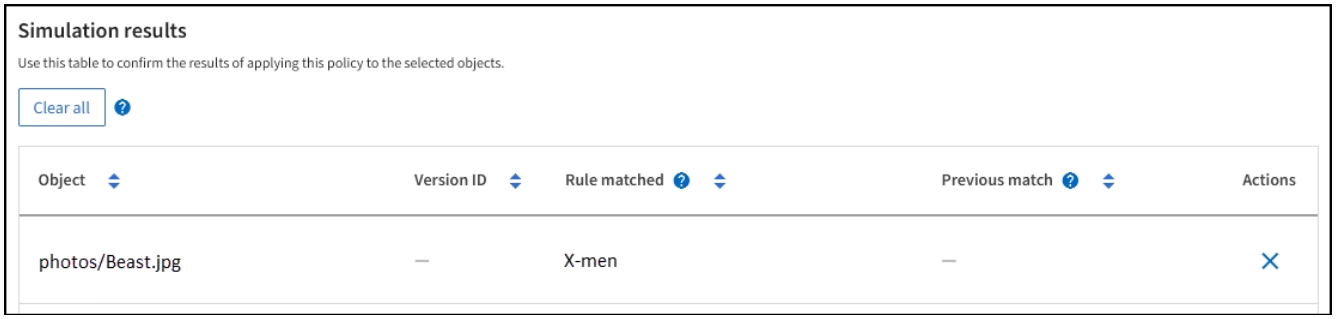
   As an example, suppose the metadata for the X-men rule was entered as "x-men01" instead of "x-men."

3. To resolve the error, correct the rule as follows:
   - If the rule is part of the proposed policy, you can either clone the rule or remove the rule from the policy and then edit it.
   - If the rule is part of the active policy, you must clone the rule. You can't edit or remove a rule from the active policy.

Option	Steps
Clone the rule	a. Select **ILM** > **Rules**. b. Select the incorrect rule, and select **Clone**. c. Enter a name for the new rule, then change the incorrect information and select **Create**. d. Select **ILM** > **Policies** > **Proposed policy**. e. Select **Actions** > **Edit**. f. Select **Select rules**, then select **Continue** to accept the same default rule. g. In the Select other rules step, select the checkbox for the new rule, clear the checkbox for the original rule, and select **Select**. h. If necessary, reorder the rules by dragging the new rule to the correct location. i. Select **Save**.
Edit the rule	a. Select **ILM** > **Policies** > **Proposed policy** and remove the rule you want to edit. b. Select **ILM** > **Rules**. c. Select the rule you want to edit and select **Edit**. Or select the checkbox for the rule and select **Actions** > **Edit**. d. Change the incorrect information for each part of the wizard, then select **Update**. e. Select **ILM** > **Policies** > **Proposed policy**. f. Select **Actions** > **Edit**. g. Select **Select rules**, then select **Continue** to accept the same default rule. h. In the Select other rules dialog box, select the checkbox for the corrected rule, select **Select**, then select **Save**. i. Drag the rows for the non-default rules to determine the order in which these rules will be evaluated.

4. Perform the simulation again.

   In this example, the corrected X-men rule now matches the `Beast.jpg` object based on the `series=x-men` user metadata, as expected.



Activate the ILM policy

After you add ILM rules to a proposed ILM policy, simulate the policy, and confirm it behaves as you expect, you are ready to activate the proposed policy.

Before you begin

- You are signed in to the Grid Manager using a supported web browser.
- You have specific access permissions.
- You have saved and simulated the proposed ILM policy.

> Errors in an ILM policy can cause unrecoverable data loss. Carefully review and simulate the policy before activating it to confirm that it will work as intended.
> When you activate a new ILM policy, StorageGRID uses it to manage all objects, including existing objects and newly ingested objects. Before activating a new ILM policy, review any changes to the placement of existing replicated and erasure-coded objects. Changing an existing object's location might result in temporary resource issues when the new placements are evaluated and implemented.

About this task

When you activate an ILM policy, the system distributes the new policy to all nodes. However, the new active policy might not actually take effect until all grid nodes are available to receive the new policy. In some cases, the system waits to implement a new active policy to ensure that grid objects aren't accidentally removed.

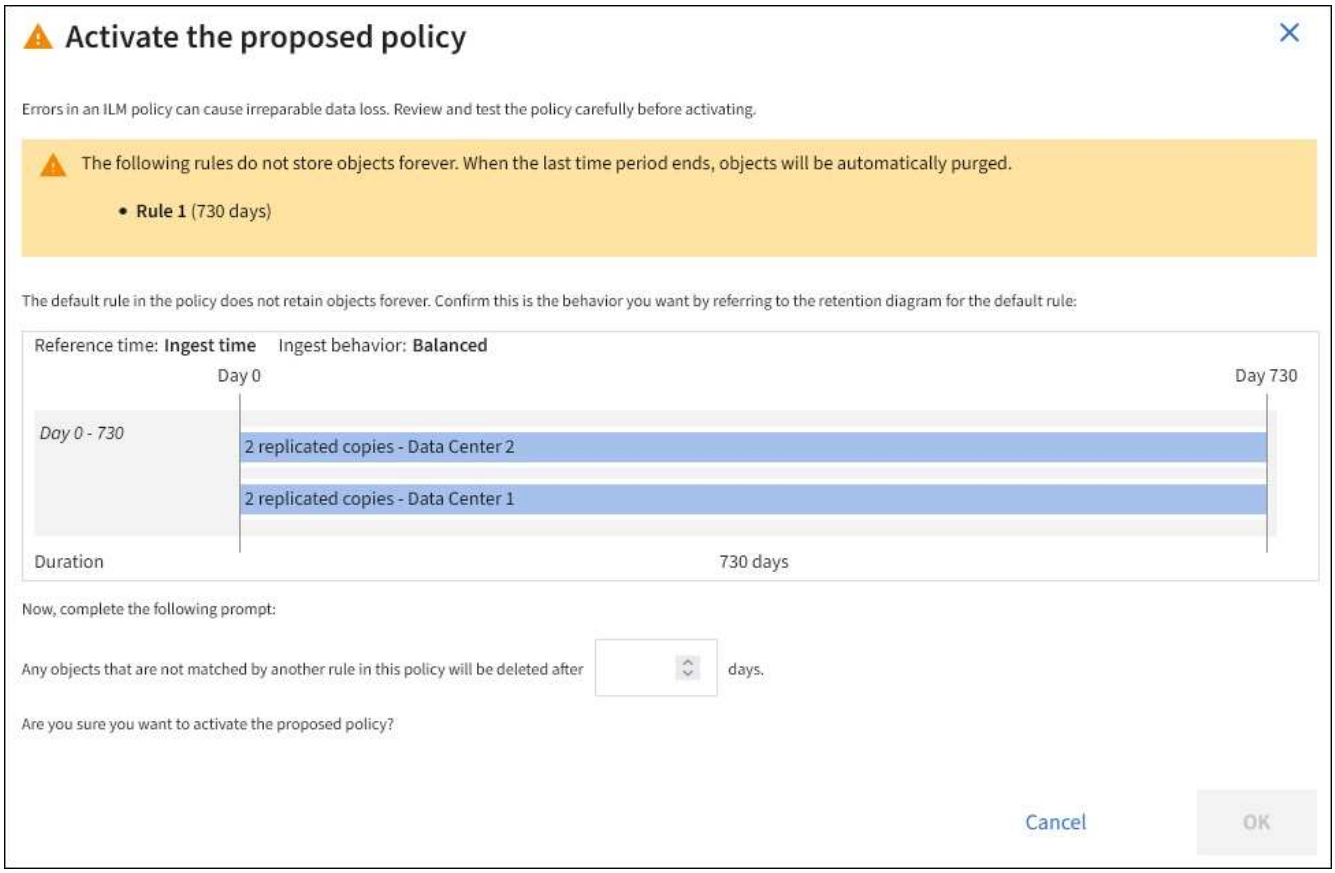
- If you make policy changes that increase data redundancy or durability, those changes are implemented immediately. For example, if you activate a new policy that includes a three-copies rule instead of a two-copies rule, that policy will be implemented right away because it increases data redundancy.
- If you make policy changes that could decrease data redundancy or durability, those changes will not be implemented until all grid nodes are available. For example, if you activate a new policy that uses a two-copies rule instead of a three-copies rule, the new policy will appear in the Active policy tab but it will not take effect until all nodes are online and available.

Steps

1. When you are ready to activate a proposed policy, select **ILM policies** > **Proposed policy**, then select **Activate**.

   A warning message is displayed, prompting you to confirm that you want to activate the proposed policy.

   A prompt appears in the warning message if the default rule does not retain objects forever. In this example, the retention diagram shows that the default rule will delete objects after 730 days (2 years). You must type **730** in the text box to acknowledge that any objects not matched by another rule in the policy will be removed from StorageGRID after 730 days.



2. Select **OK**.

Result

When a new ILM policy has been activated:

- The policy is shown on the Active policy tab. The Start date entry indicates the date and time the policy was activated.
- The previously active policy appears in the Policy history tab. The Start date and End date entries indicate when the policy became active and when it was no longer in effect.

Related information

Example 6: Changing an ILM policy

Verify an ILM policy with object metadata lookup

After you have activated an ILM policy, you should ingest representative test objects into the StorageGRID system. You should then perform an object metadata lookup to confirm that copies are being made as intended and placed in the correct locations.

Before you begin

- You have an object identifier, which can be one of:
  - **UUID**: The object's Universally Unique Identifier. Enter the UUID in all uppercase.
  - **CBID**: The object's unique identifier within StorageGRID. You can obtain an object's CBID from the audit log. Enter the CBID in all uppercase.

- **S3 bucket and object key**: When an object is ingested through the S3 interface, the client application uses a bucket and object key combination to store and identify the object. If the S3 bucket is versioned and you want to look up a specific version of an S3 object using the bucket and object key, you have the **version ID**.
- **Swift container and object name**: When an object is ingested through the Swift interface, the client application uses a container and object name combination to store and identify the object.

Steps

1. Ingest the object.
2. Select **ILM** > **Object metadata lookup**.
3. Type the object's identifier in the **Identifier** field. You can enter a UUID, CBID, S3 bucket/object-key, or Swift container/object-name.
4. Optionally, enter a version ID for the object (S3 only).

5. Select **Look Up**.

   The object metadata lookup results appear. This page lists the following types of information:

   - System metadata, including the object ID (UUID), the object name, the name of the container, the tenant account name or ID, the logical size of the object, the date and time the object was first created, and the date and time the object was last modified.
   - Any custom user metadata key-value pairs associated with the object.
   - For S3 objects, any object tag key-value pairs associated with the object.
   - For replicated object copies, the current storage location of each copy.
   - For erasure-coded object copies, the current storage location of each fragment.
   - For object copies in a Cloud Storage Pool, the location of the object, including the name of the external bucket and the object's unique identifier.
   - For segmented objects and multipart objects, a list of object segments including segment identifiers and data sizes. For objects with more than 100 segments, only the first 100 segments are shown.
   - All object metadata in the unprocessed, internal storage format. This raw metadata includes internal system metadata that is not guaranteed to persist from release to release.

   The following example shows the object metadata lookup results for an S3 test object that is stored as two replicated copies.

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H$|TFbnQQ}|CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H$|TFboW28|CXG%

Raw Metadata


```
{
    "TYPE": "CTNT",
    "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
    "NAME": "testobject",
    "CBID": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```


6. Confirm that the object is stored in the correct location or locations and that it is the correct type of copy.

> If the Audit option is enabled, you can also monitor the audit log for the ORLM Object Rules Met message. The ORLM audit message can provide you with more information about the status of the ILM evaluation process, but it can't give you information about the correctness of the object data's placement or the completeness of the ILM policy. You must evaluate this yourself. For details, see Review audit logs.

Related information

- Use S3 REST API
- Use Swift REST API

Copyright information

Trademark information