Create ILM policy

StorageGRID

NetApp
June 13, 2025

Table of Contents

Create ILM policy

Create ILM policy: Overview

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.

Considerations for creating an ILM policy

- Use the system's built-in policy, Baseline 2 Copies Policy, in test systems only. 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.
- 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 rule will not be evaluated by any other rule.
- The last rule in every ILM policy is the default ILM rule, which cannot 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.

> If the global S3 Object Lock setting has been enabled, use this procedure instead: Create an ILM policy after S3 Object Lock is enabled.

What you'll need

- You are signed in to the Grid Manager using a supported web browser.
- You have specific access permissions.
- 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 for the policy that does not contain any filters.
- Optionally, you have watched the video: Video: StorageGRID ILM Policies

About this task

Typical reasons for creating a proposed ILM policy include:

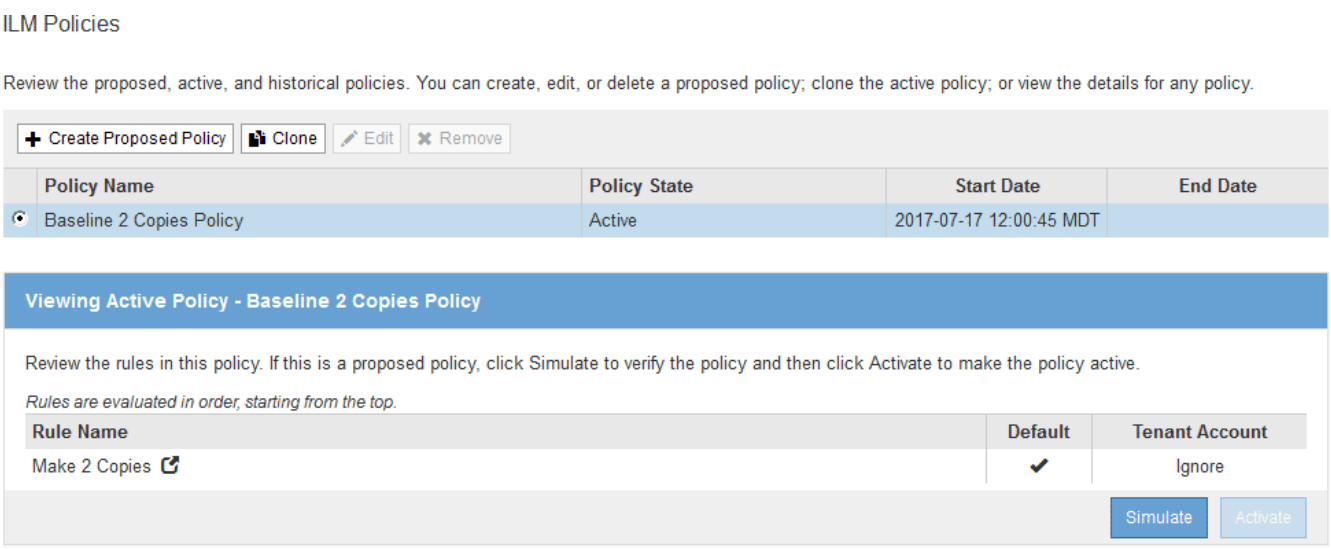
- You added a new site and need to use new ILM rules to place objects at that site.
- You are decommissioning a site and you need to remove all rules that refer to the site.
- You added a new tenant that has special data protection requirements.
- You started to use a Cloud Storage Pool.

> Use the system's built-in policy, Baseline 2 Copies Policy, in test systems only. 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.

Steps

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

   The ILM Policies page appears. From this page, you can review the list of proposed, active, and historical policies; create, edit, or remove a proposed policy; clone the active policy; or view the details for any policy.

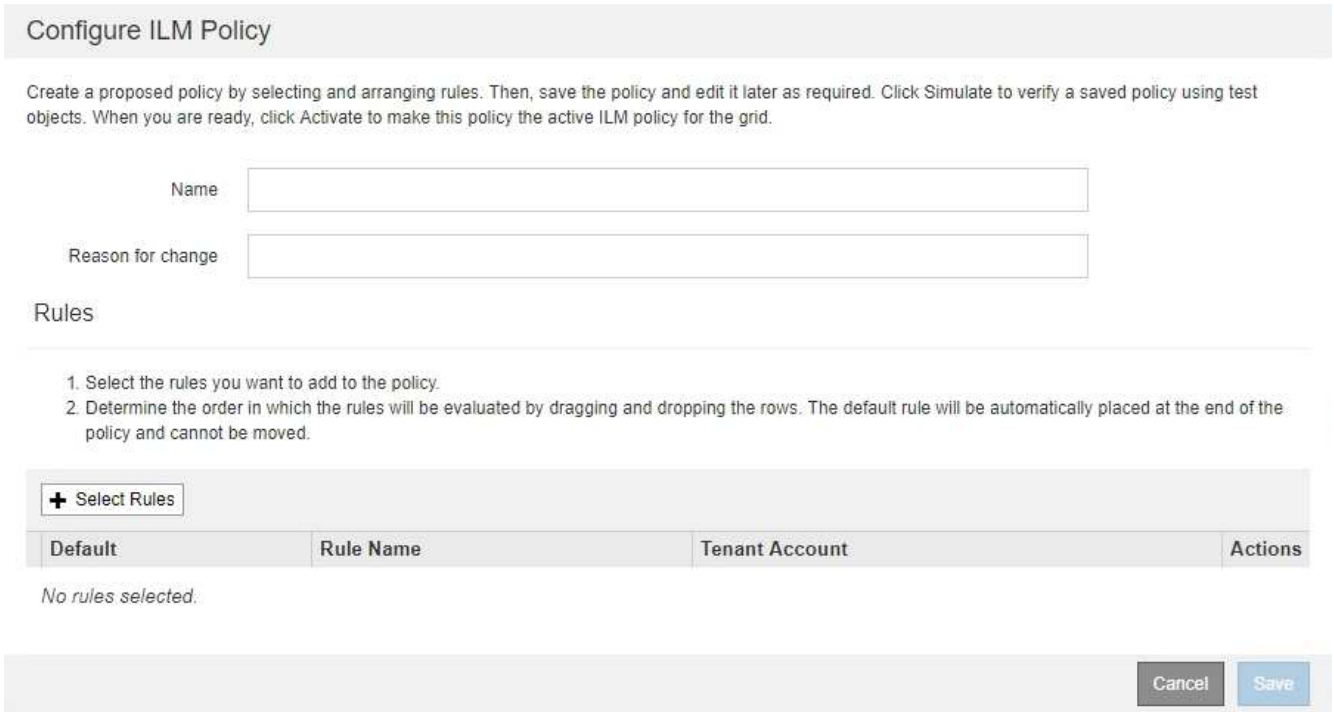


2. Determine how you want to create the proposed ILM policy.

Option	Steps
Create a new proposed policy that has no rules already selected	a. If a proposed ILM policy currently exists, select that policy, and select **Remove**. You cannot create a new proposed policy if a proposed policy already exists. b. Select **Create Proposed Policy**.
Create a proposed policy based on the active policy	a. If a proposed ILM policy currently exists, select that policy, and select **Remove**. You cannot clone the active policy if a proposed policy already exists. b. Select the active policy from the table. c. Select **Clone**.
Edit the existing proposed policy	a. Select the proposed policy from the table. b. Select **Edit**.

The Configure ILM Policy dialog box appears.

If you are creating a new proposed policy, all fields are blank and no rules are selected.



If you are cloning the active policy, the **Name** field shows the name of the active policy, appended by a version number ("v2" in the example). The rules used in the active policy are selected and shown in their current order.

3. Enter a unique name for the proposed policy in the **Name** field.

   You must enter at least 1 and no more than 64 characters. If you are cloning the active policy, you can use the current name with the appended version number or you can enter a new name.

4. Enter the reason you are creating a new proposed policy in the **Reason for change** field.

   You must enter at least 1 and no more than 128 characters.

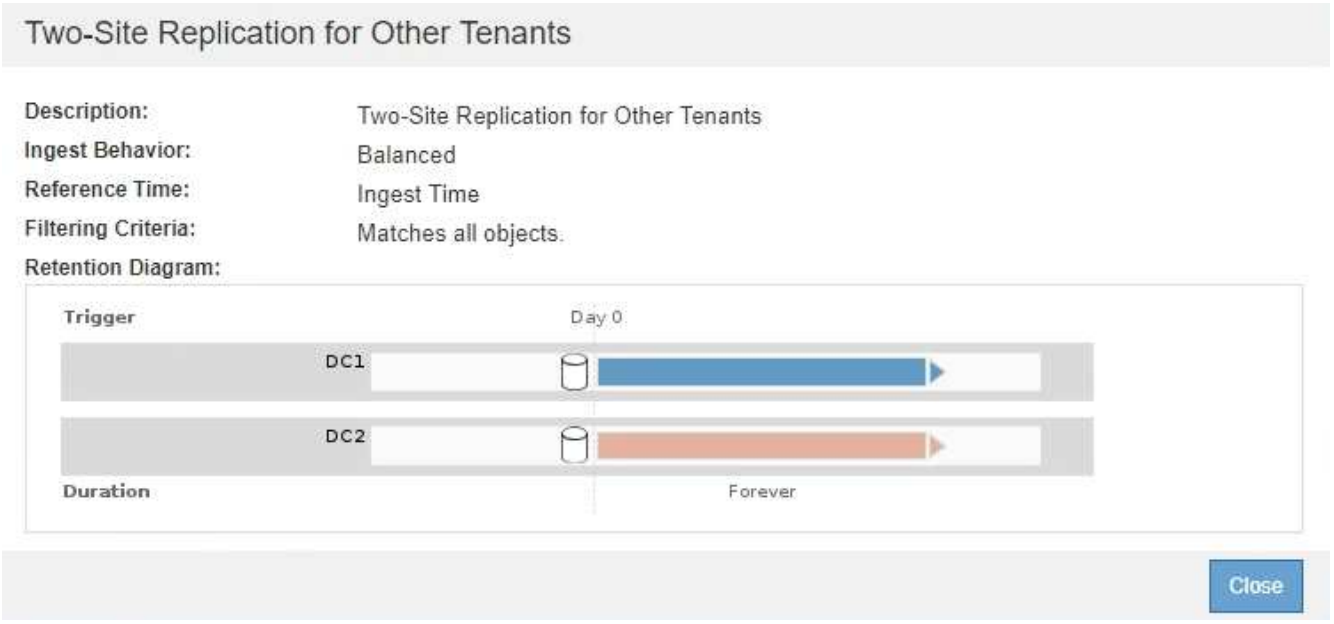
5. To add rules to the policy, select **Select Rules**.

   The Select Rules for Policy dialog box appears, with all defined rules listed. 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 or the Noncurrent reference time, you are prompted to select a new default rule.
   - If the default rule was not the last rule, a button allows you to move the rule to the end of the new policy.

6. Select a rule name or the more details icon to view the settings for that rule.

   This example shows the details of an ILM rule that makes two replicated copies at two sites.



7. In the **Select Default Rule** section, select one default rule for the proposed policy.

   The default rule applies to any objects that do not match another rule in the policy. The default rule cannot use any filters and is always evaluated last.

   > If no rule is listed in the Select Default Rule section, you must exit the ILM policy page and create a default ILM rule.

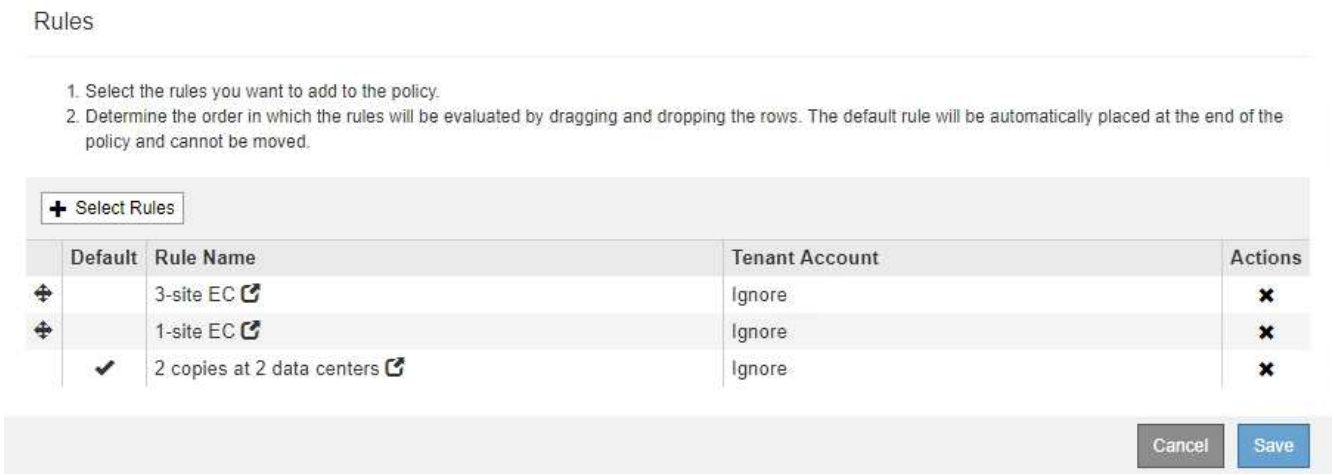
Do not use the Make 2 Copies stock rule as the default rule for a policy. The Make 2 Copies rule uses a single storage pool, All Storage Nodes, which contains all sites. If your StorageGRID system has more than one site, two copies of an object might be placed on the same site.

8. In the **Select Other Rules** section, select any other rules you want to include in the policy.

   The other rules are evaluated before the default rule and must use at least one filter (tenant account, bucket name, advanced filter, or the Noncurrent reference time).

9. When you are done selecting rules, select **Apply**.

   The rules you selected are listed. The default rule is at the end, with the other rules above it.



A warning appears if the default 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 longer).

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

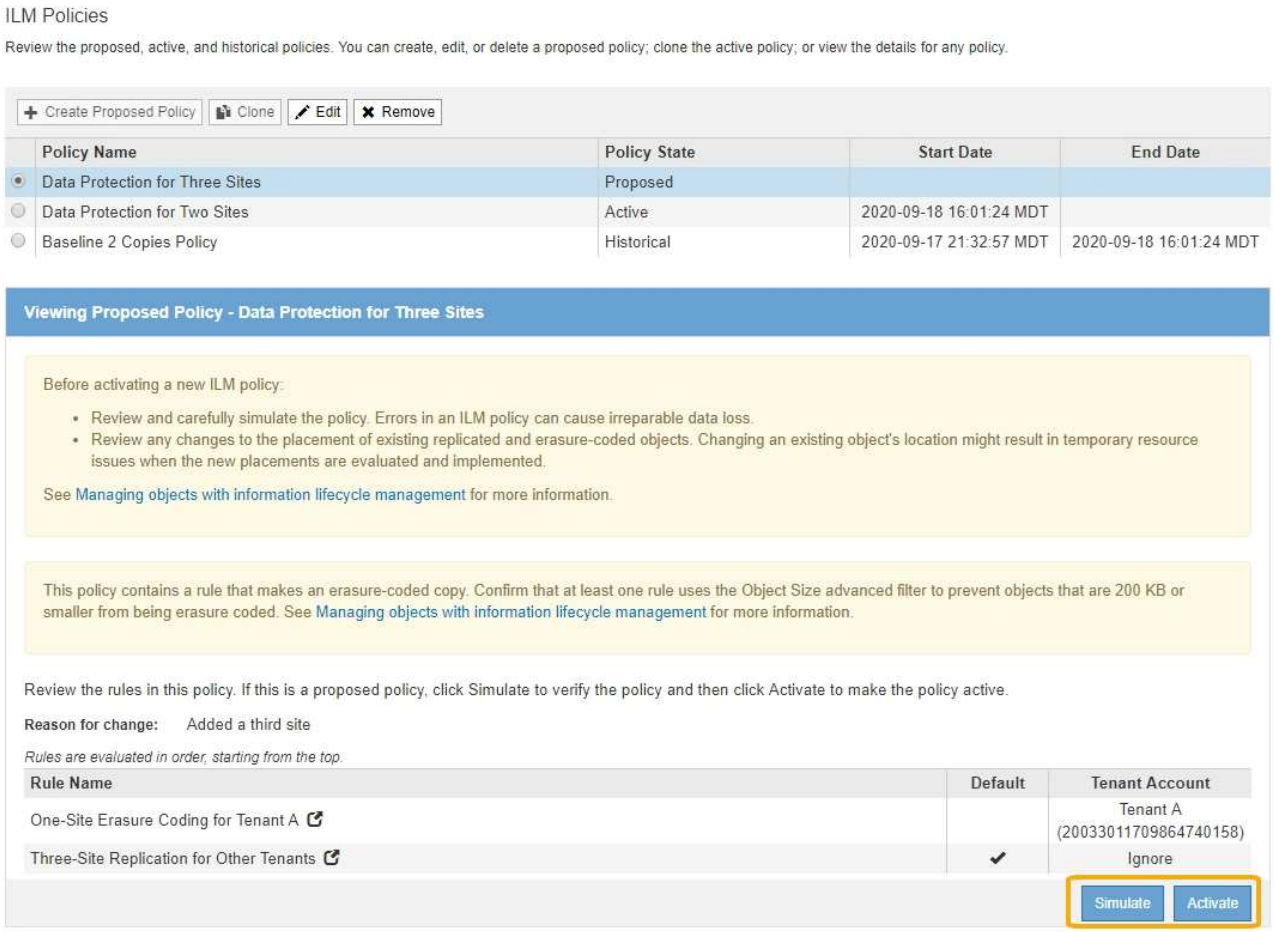
    You cannot move the default rule.

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.

11. As required, select the delete icon ✖ to delete any rules that you do not want in the policy, or select **Select Rules** to add more rules.
12. When you are done, select **Save**.

The ILM Policies page is updated:

- The policy you saved is shown as Proposed. Proposed policies do not have start and end dates.
- The **Simulate** and **Activate** buttons are enabled.



13. Go to Simulate an ILM policy.

Related information

- What an ILM policy is
- Manage objects with S3 Object Lock

Create an ILM policy after S3 Object Lock is enabled

If the global S3 Object Lock setting is enabled, the steps for creating a policy are slightly different. You must ensure that the ILM policy is compliant with the requirements of buckets that have S3 Object Lock enabled.

What you'll need

- You are signed in to the Grid Manager using a supported web browser.
- You have specific access permissions.
- The global S3 Object Lock setting is already enabled for the StorageGRID system.

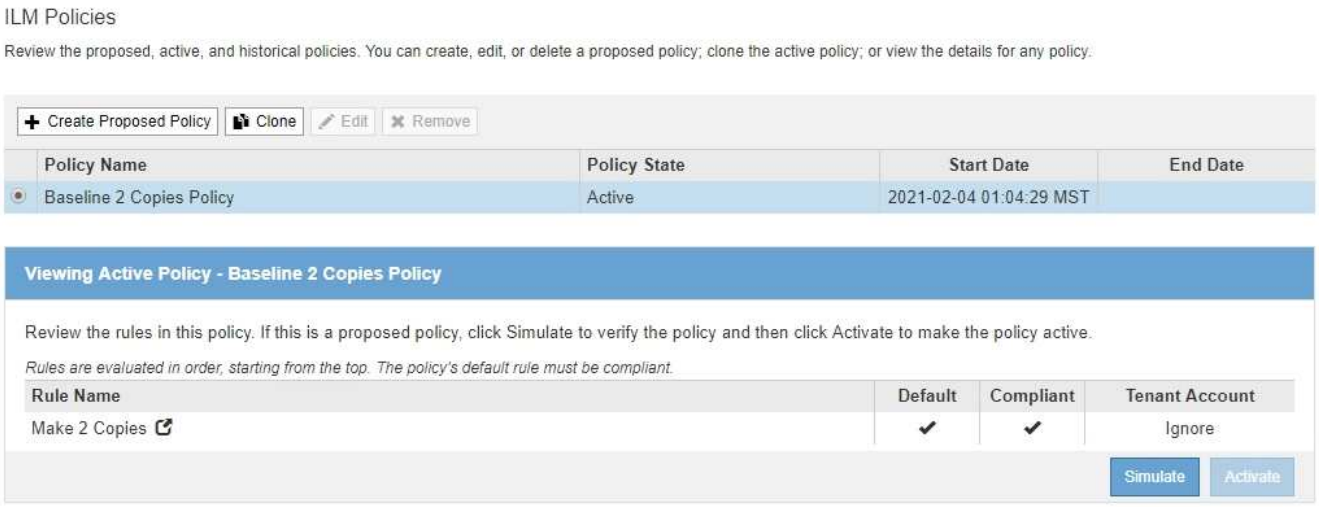
If the global S3 Object Lock setting has not been enabled, use the general instructions for creating a proposed ILM policy.

- 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. See Example 7: Compliant ILM policy for S3 Object Lock.
- You have created a default ILM rule for the policy that is compliant.
- Optionally, you have watched the video: Video: StorageGRID ILM Policies

Steps

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

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



2. Enter a unique name for the proposed policy in the **Name** field.

   You must enter at least 1 and no more than 64 characters.

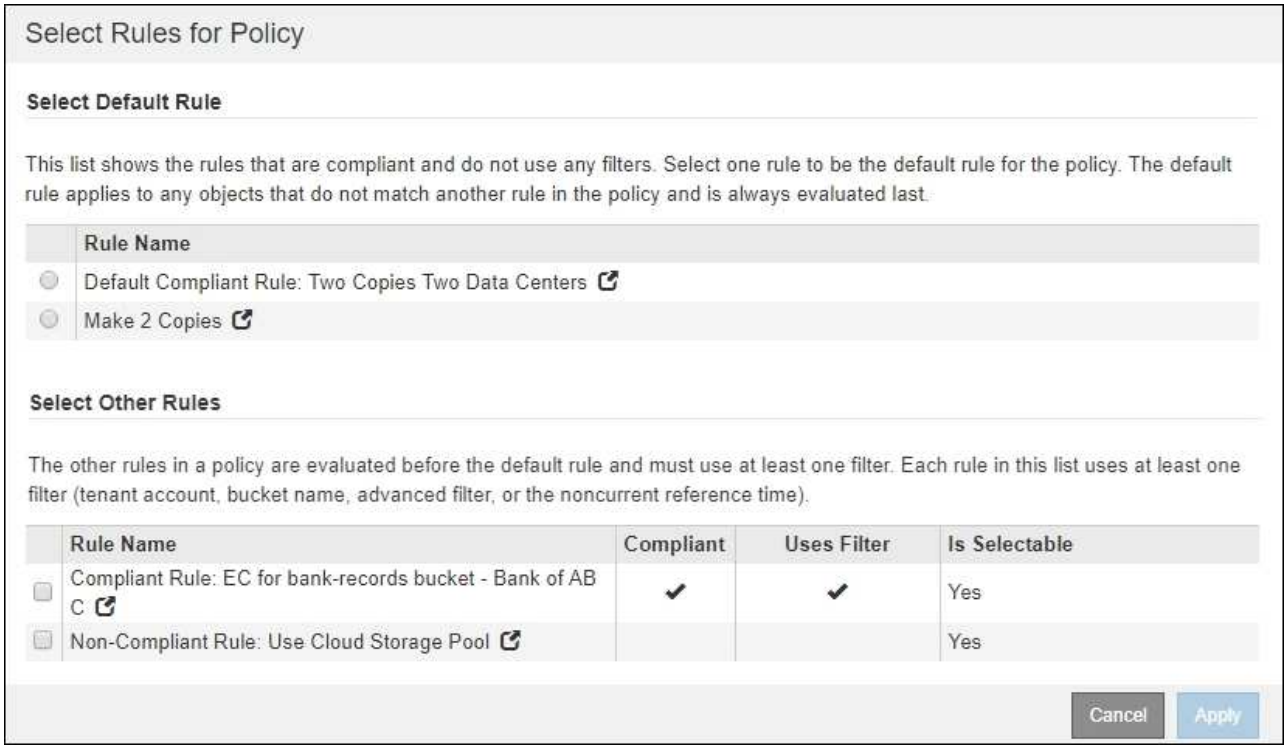
3. Enter the reason you are creating a new proposed policy in the **Reason for change** field.

You must enter at least 1 and no more than 128 characters.

4. To add rules to the policy, select **Select Rules**.

   The Select Rules for Policy dialog box appears, with all defined rules listed.

   - The Select Default Rule section lists the rules that can be the default for a compliant policy. It includes compliant rules that do not use filters or the Noncurrent reference time.
   - The Select Other Rules section lists the other compliant and non-compliant rules that can be selected for this policy.



5. Select a rule name or the more details icon to view the settings for that rule.
6. In the **Select Default Rule** section, select one default rule for the proposed policy.

   The table in this section only lists the rules that are compliant and do not use any filters.

   If no rule is listed in the Select Default Rule section, you must exit the ILM policy page and create a default ILM rule that is compliant.

   Do not use the Make 2 Copies stock 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.

7. In the **Select Other Rules** section, select any other rules you want to include in the policy.
   a. If you need a different “default” rule for objects in non-compliant S3 buckets, optionally select one non-compliant rule that does not use a filter.

      For example, you might want to use a Cloud Storage Pool or an Archive Node to store objects in buckets that do not have S3 Object Lock enabled.

> You can only select one non-compliant rule that does not use a filter. As soon as you select one rule, the **Is Selectable** column shows **No** for any other non-compliant rules without filters.

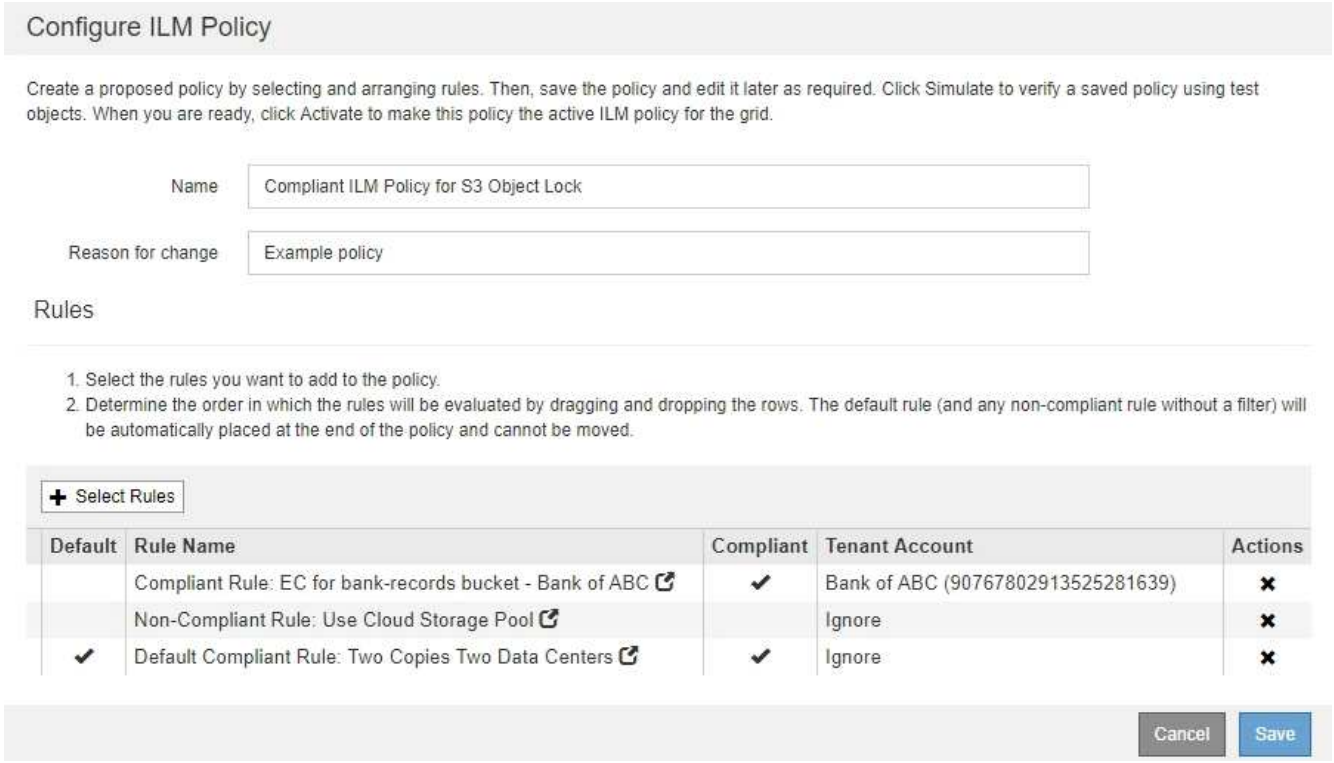
b. Select any other compliant or non-compliant rules you want to use in the policy.

   The other rules must use at least one filter (tenant account, bucket name, or an advanced filter, such as object size).

8. When you are done selecting the rules, select **Apply**.

   The rules you selected are listed. The default rule is at the end, with the other rules above it. If you also selected a non-compliant “default” rule, that rule is added as the second-to-last rule in the policy.

   In this example, the last rule, 2 Copies 2 Data Centers, is the default rule: it is compliant and has no filters. The second-to-last rule, Cloud Storage Pool, also has no filters but it is not compliant.



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

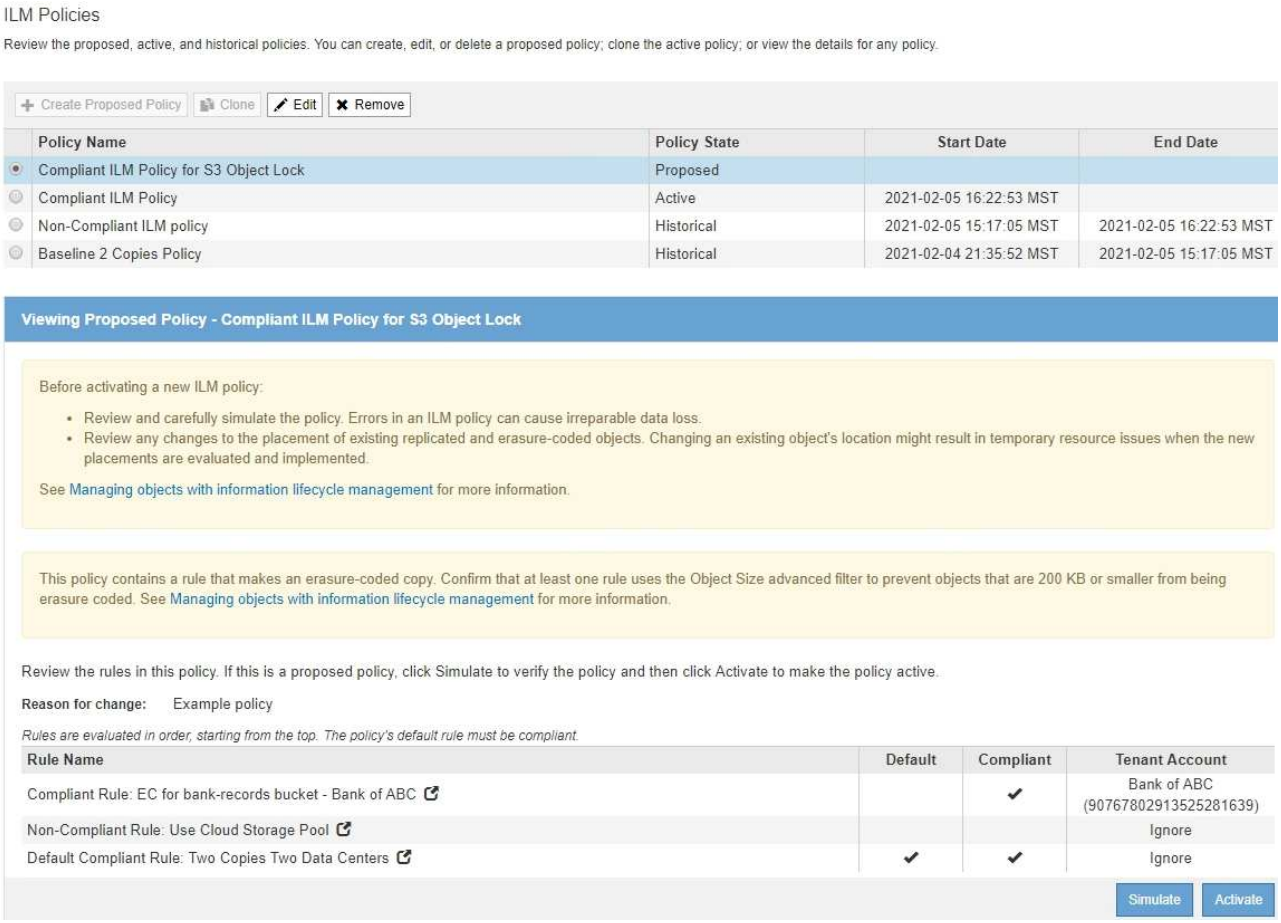
   You cannot move the default rule or the non-compliant “default” rule.

> 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.

10. As required, select the delete icon ✖ to delete any rules that you do not want in the policy, or **Select Rules** to add more rules.
11. When you are done, select **Save**.

    The ILM Policies page is updated:

- The policy you saved is shown as Proposed. Proposed policies do not have start and end dates.
- The **Simulate** and **Activate** buttons are enabled.



12. Go to Simulate an ILM policy.

Simulate an ILM policy

You should 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.

What you'll need

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

About this task

You must 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:

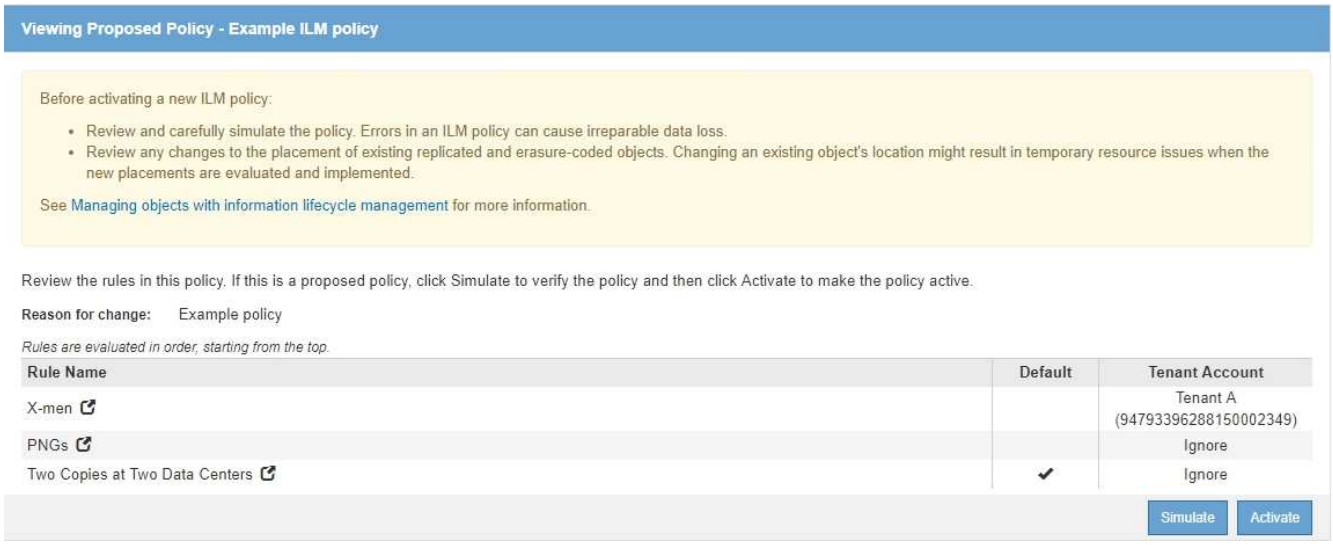
- After you make changes to a policy, save the proposed policy. Then, simulate the behavior of the saved proposed policy.
- When you simulate a policy, the ILM rules in the policy filter the test objects, so you can see which rule was applied to each object. However, no object copies are made and no objects are placed. Running a simulation does not modify your data, rules, or the policy in any way.
- The Simulation page retains the objects you tested until you close, navigate away from, or refresh the ILM Policies page.
- Simulation returns the name of the matched rule. To determine which storage pool or Erasure Coding profile is in effect, you can view the Retention Diagram by selecting the rule name or the more details icon .
- If S3 Versioning is enabled, the policy is only simulated against the current version of the object.

Steps

1. Select and arrange the rules, and save the proposed policy.

   The policy in this example has three rules:

Rule Name	Filter	Type of Copies	Retention
X-men	• Tenant A • User metadata (series=x-men)	2 copies at two data centers	2 years
PNGs	Key ends with .png	2 copies at two data centers	5 years
Two Copies Two Data Centers	*None*	2 copies at two data centers	Forever



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

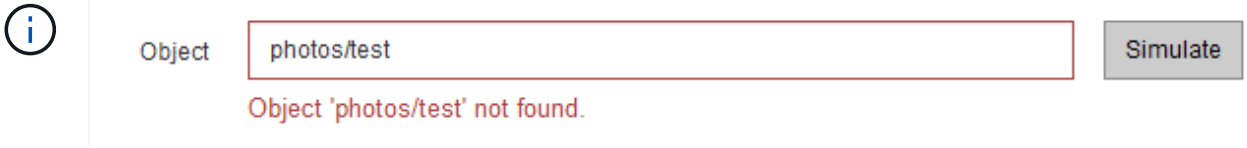
tenant, ingest the objects required to test each rule.

3. Select **Simulate**.

   The Simulation ILM Policy dialog box appears.

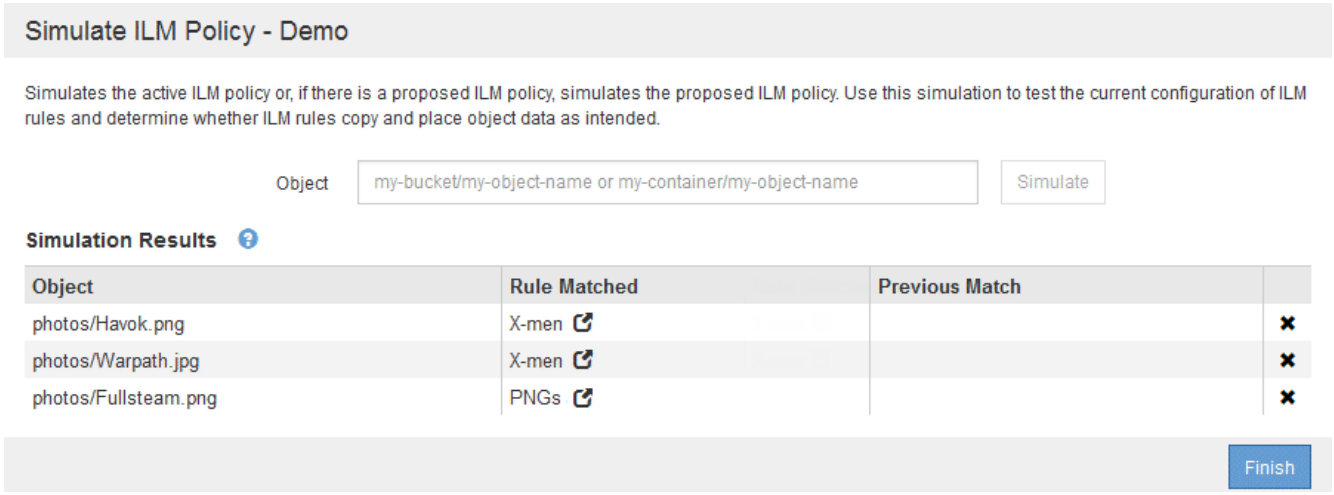
4. In the **Object** field, enter the S3 bucket/object-key or the Swift container/object-name for a test object, and select **Simulate**.

   A message appears if you specify an object that has not been ingested.



5. Under **Simulation Results**, confirm that each object was matched by the correct rule.

   In the example, the `Havok.png` and `Warpath.jpg` objects were correctly matched by the X-men rule. The `Fullsteam.png` object, which does not include `series=x-men` user metadata, was not matched by the X-men rule but was correctly matched by the PNGs rule. The default rule was not used because all three objects were matched by other rules.

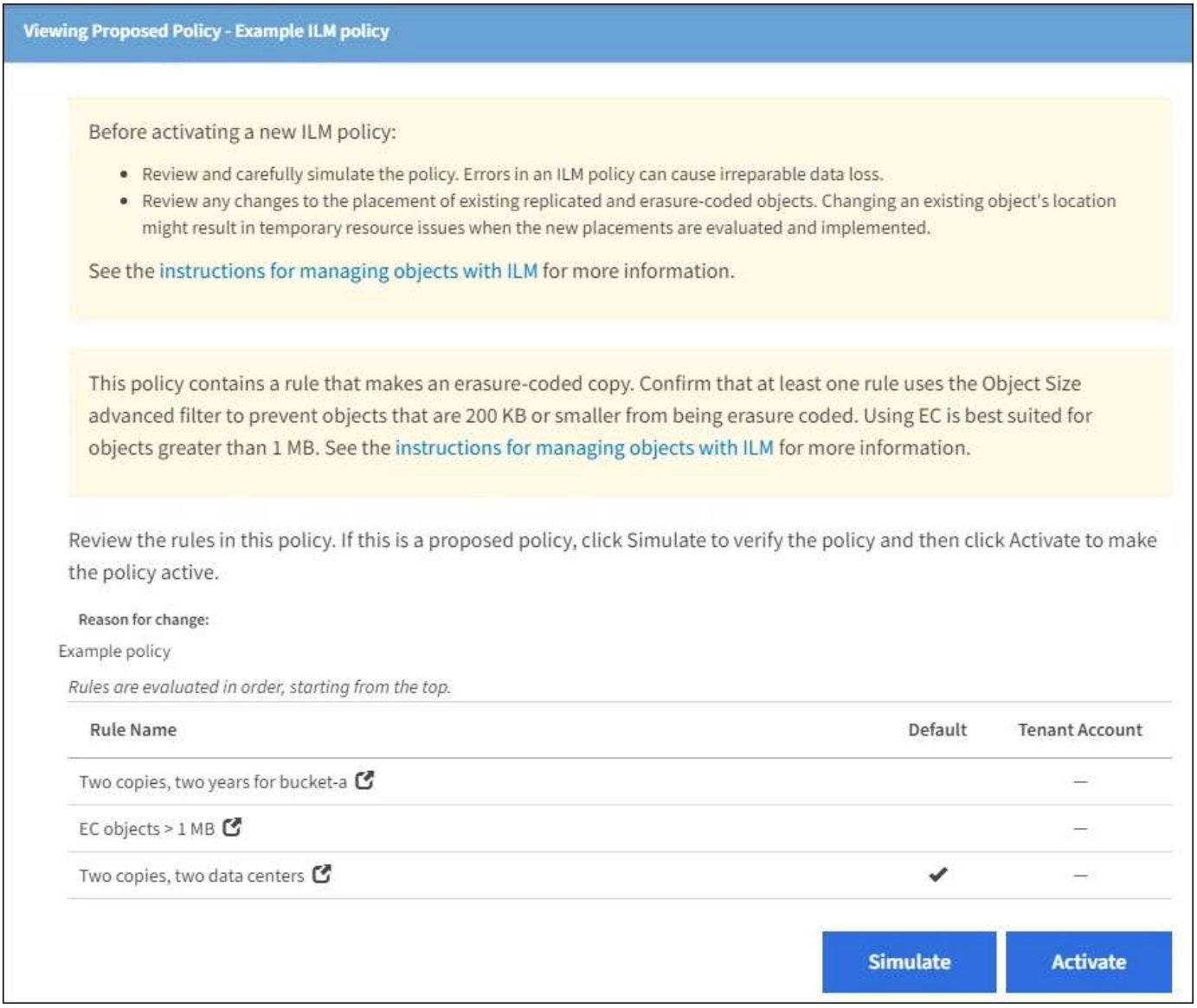


Example 1: Verify rules when simulating a proposed ILM policy

This example shows 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.



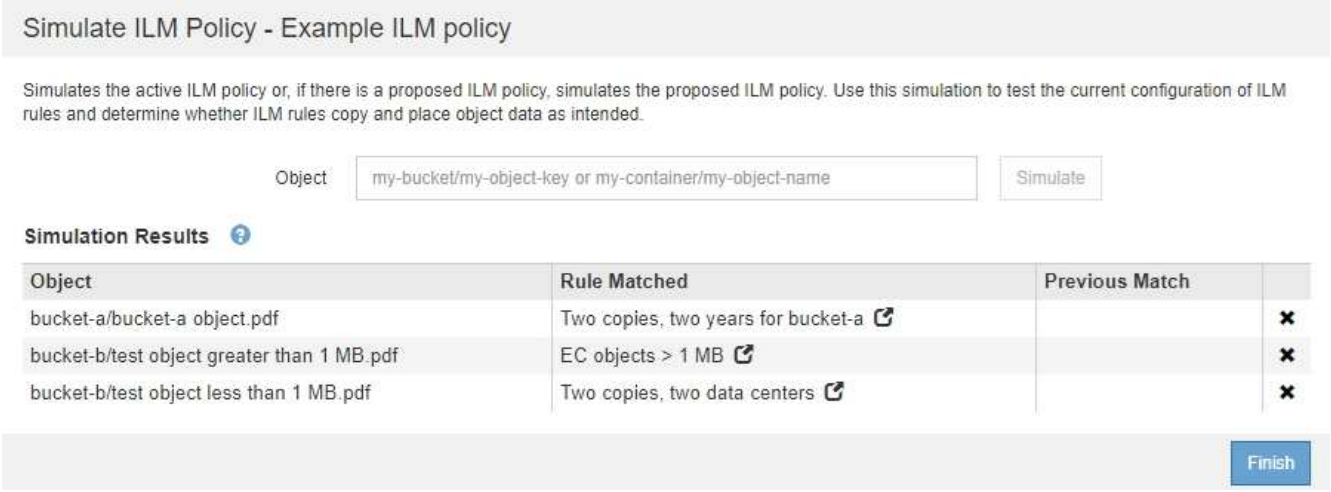
Steps

1. After adding the rules and saving the policy, select **Simulate**.

   The Simulate ILM Policy dialog box appears.

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 which rule in the policy matched each object you tested.



3. Confirm that each object was matched by the correct rule.

   In this example:

   a. `bucket-a/bucket-a object.pdf` correctly matched the first rule, which filters on objects in `bucket-a`.

   b. `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.

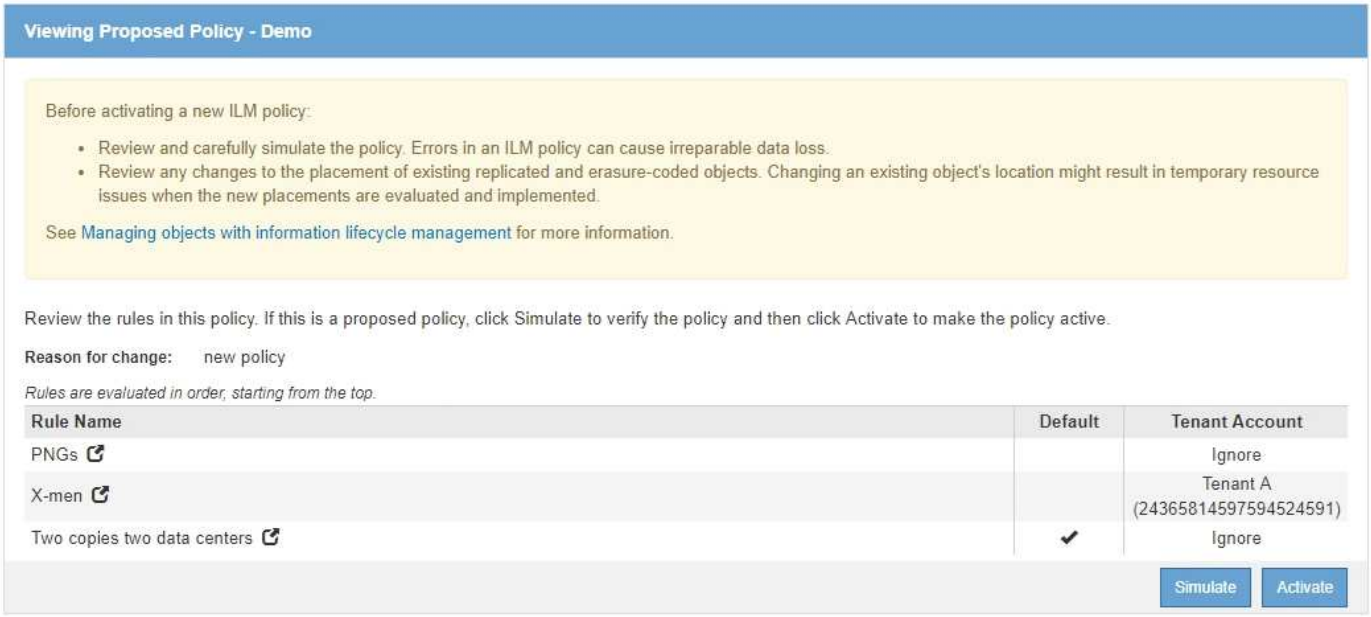
   c. `bucket-b/test object less than 1 MB.pdf` did not match the filters in the first two rules, so it will be placed by the default rule, which includes no filters.

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:

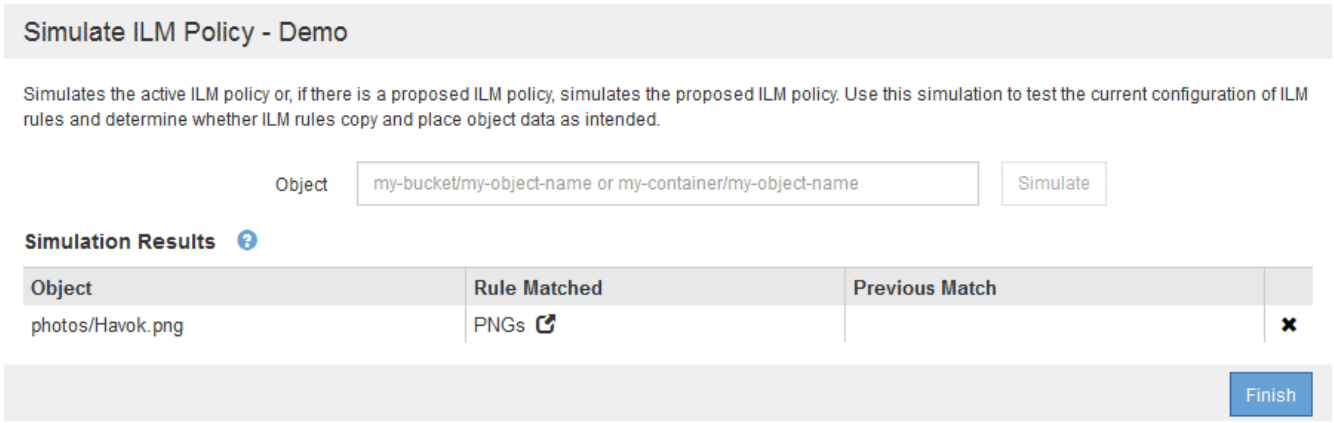
- The first rule, **PNGs**, filters for key names that end in `.png`.
- The second rule, **X-men**, applies only to objects for Tenant A and filters for `series=x-men` user metadata.
- The last rule, **Two copies two data centers**, is the default rule, which matches any objects that do not match the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



Steps

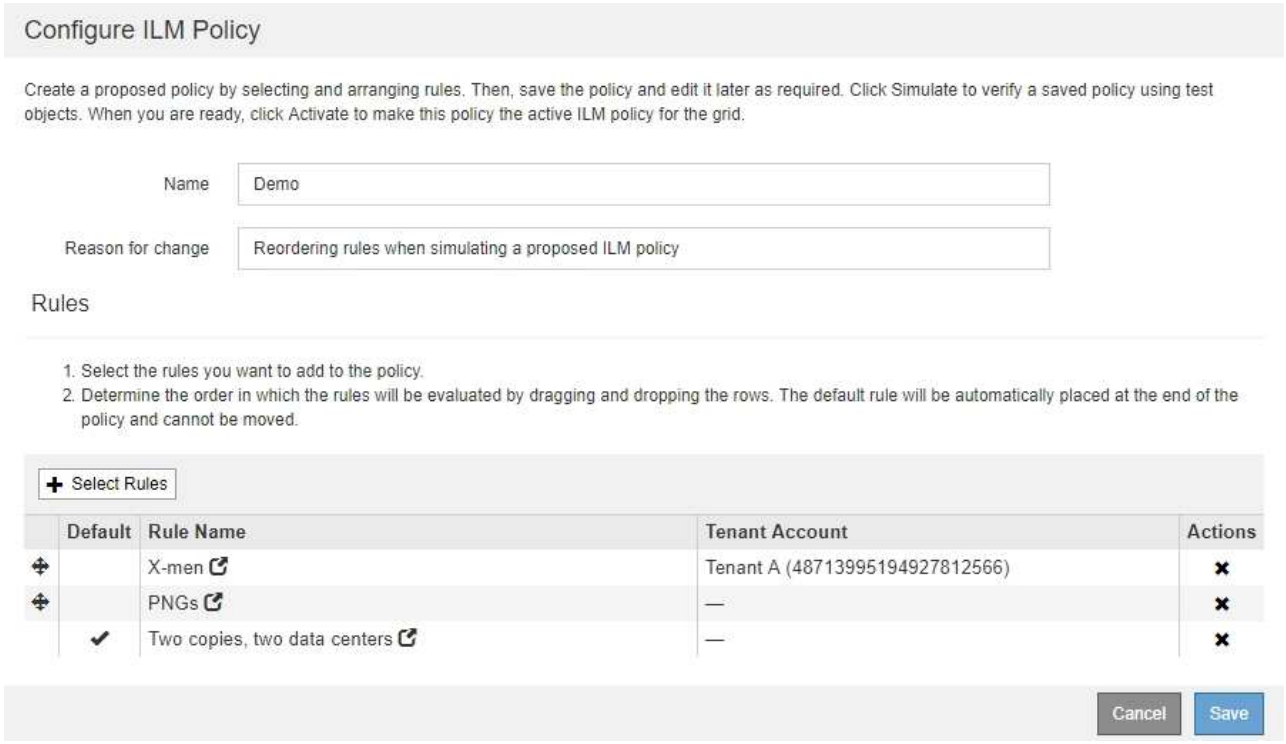
1. After adding the rules and saving the policy, select **Simulate**.
2. In the **Object** field, enter the S3 bucket/object-key or the Swift container/object-name for a test object, and select **Simulate**.

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



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

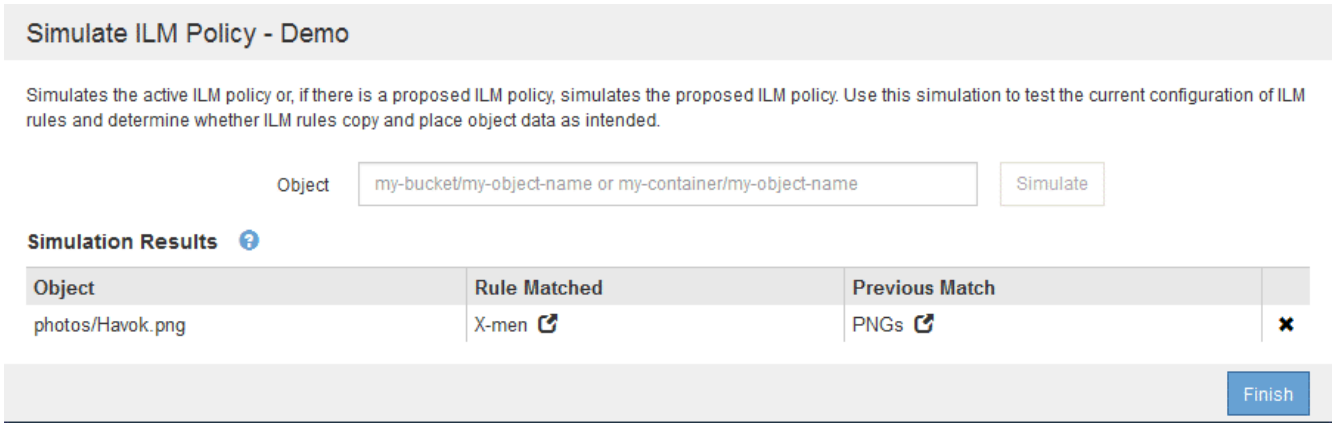
3. To resolve the issue, reorder the rules.
   a. Select **Finish** to close the Simulate ILM Policy page.
   b. Select **Edit** to edit the policy.
   c. Drag the **X-men** rule to the top of the list.



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.



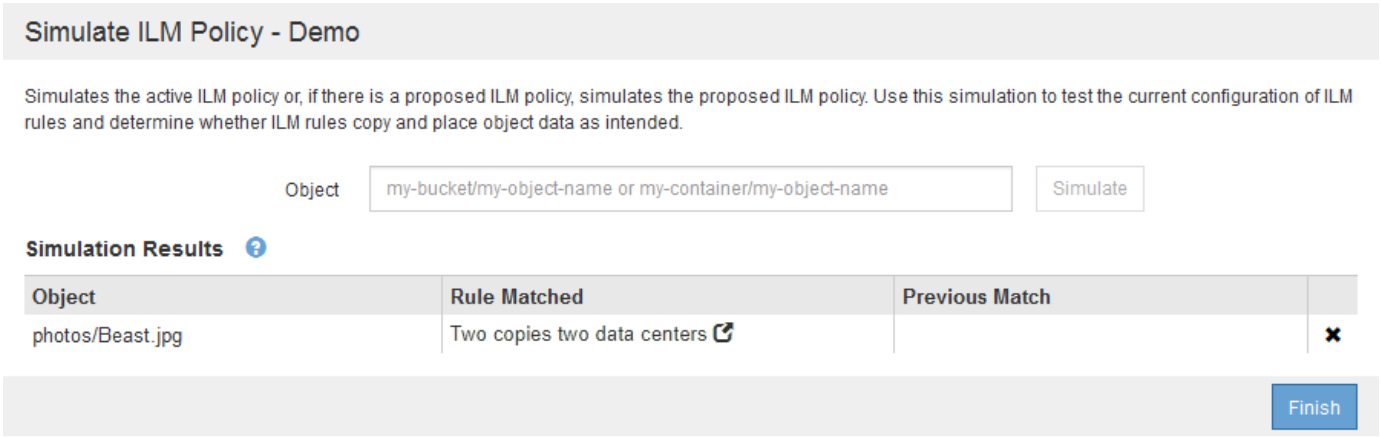
If you stay on the Configure Policies page, you can re-simulate a policy after making changes without needing to re-enter the names of the test objects.

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.

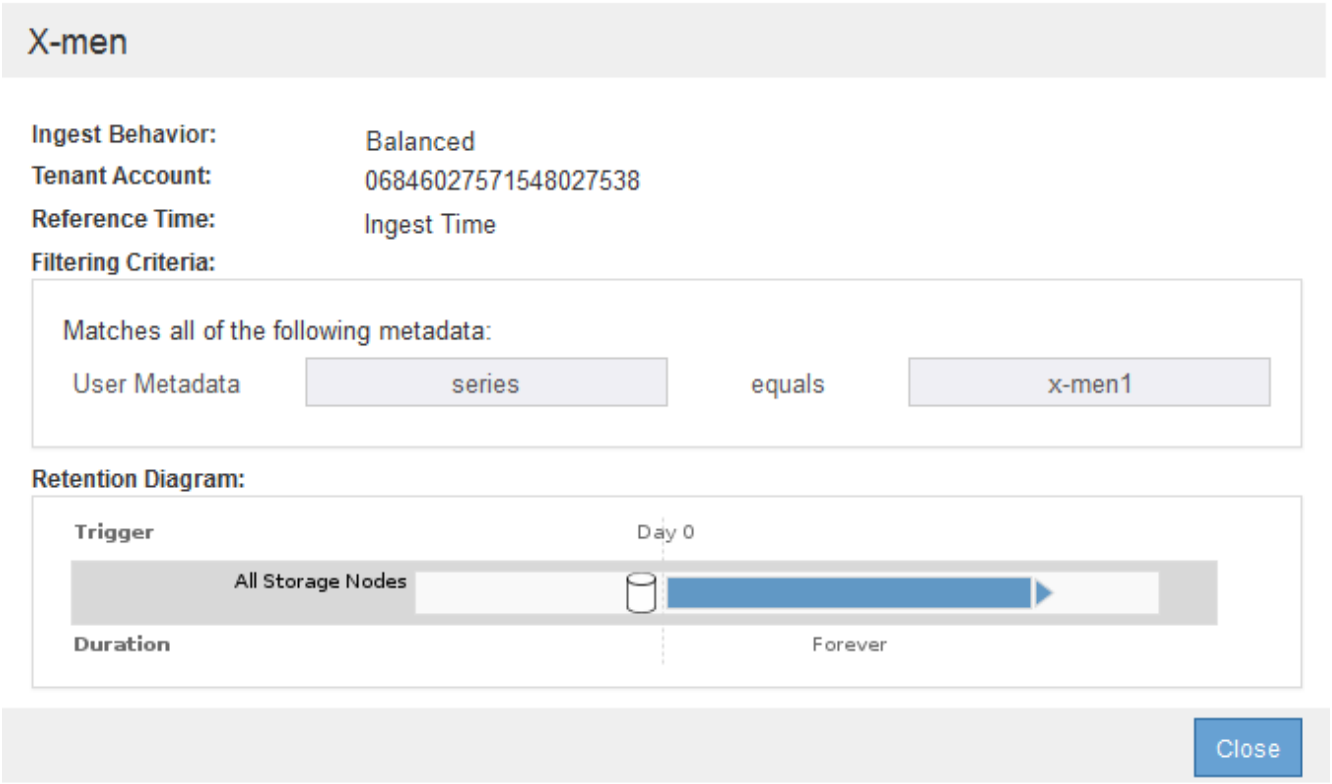


When a test object is not matched by the expected rule in the policy, you must examine each rule in the policy and correct any errors.

Steps

1. For each rule in the policy, view the rule settings by selecting the rule name or the more details icon on any dialog box where the rule is displayed.
2. Review the rule's tenant account, reference time, and filtering criteria.

   In this example, the metadata for the X-men rule includes an error. The metadata value was entered as "x-men1" instead of "x-men."



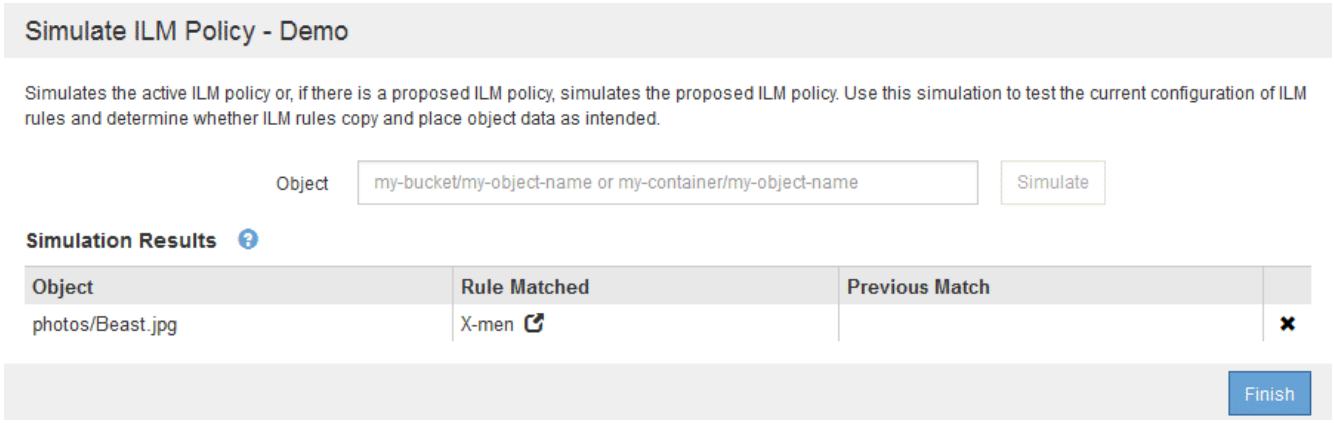
3. To resolve the error, correct the rule, as follows:
   - If the rule is part of the proposed policy, you can either clone the rule or remove the rule from the policy and then edit it.
   - If the rule is part of the active policy, you must clone the rule. You cannot edit or remove a rule from the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

Option	Description
Clone the rule	a. Select **ILM** > **Rules**. b. Select the incorrect rule, and select **Clone**. c. Change the incorrect information, and select **Save**. d. Select **ILM** > **Policies**. e. Select the proposed policy, and select **Edit**. f. Select **Select Rules**. g. Select the check box for the new rule, uncheck the check box for the original rule, and select **Apply**. h. Select **Save**.
Edit the rule	a. Select the proposed policy, and select **Edit**. b. Select the delete icon ✖ to remove the incorrect rule, and select **Save**. c. Select **ILM** > **Rules**. d. Select the incorrect rule, and select **Edit**. e. Change the incorrect information, and select **Save**. f. Select **ILM** > **Policies**. g. Select the proposed policy, and select **Edit**. h. Select the corrected rule, select **Apply**, and select **Save**.

4. Perform the simulation again.

> ⓘ Because you navigated away from the ILM Policies page to edit the rule, the objects you previously entered for simulation are no longer displayed. You must re-enter the names of the objects.

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.

What you'll need

- 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

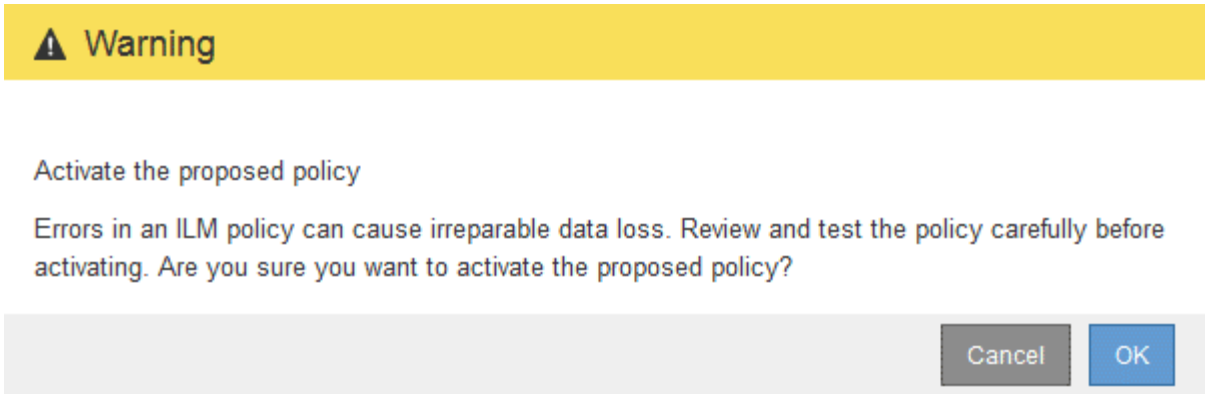
When you activate an ILM policy, the system distributes the new policy to all nodes. However, the new active policy might not actually take effect until all grid nodes are available to receive the new policy. In some cases, the system waits to implement a new active policy to ensure that grid objects are not 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 be marked as "Active," but it will not take effect until all nodes are online and available.

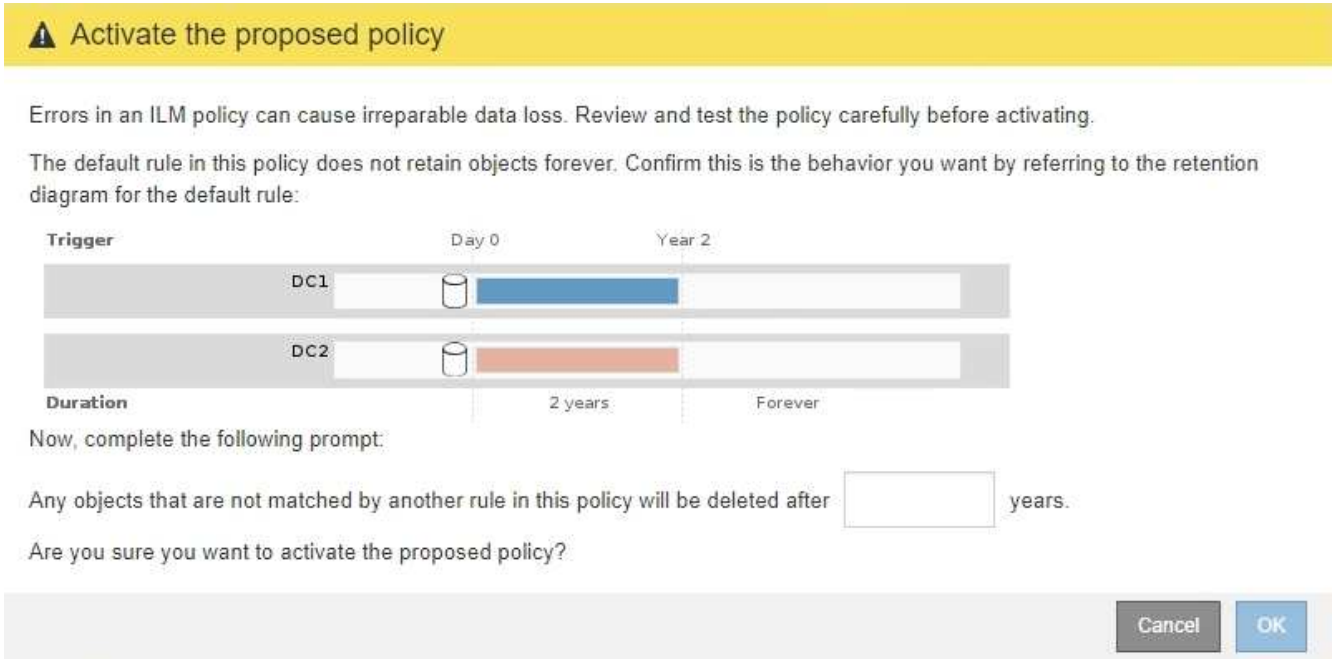
Steps

1. When you are ready to activate a proposed policy, select the policy on the ILM Policies page and 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 for the policy does not retain objects forever. In this example, the retention diagram shows that the default rule will delete objects after 2 years. You must type **2** in the text box to acknowledge that any objects not matched by another rule in the policy will be removed from StorageGRID after 2 years.

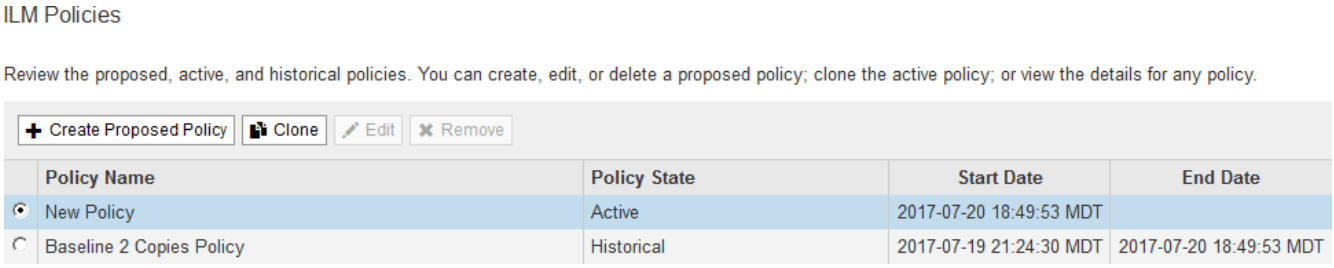


2. Select **OK**.

Result

When a new ILM policy has been activated:

- The policy is shown with a Policy State of Active in the table on the ILM Policies page. The Start Date entry indicates the date and time the policy was activated.



- The previously active policy is shown with a Policy State of Historical. 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.

What you'll need

- 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 cannot 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
- Use Swift

Copyright information

Trademark information