NetApp

Create ILM rule

StorageGRID 11.7

NetApp
April 12, 2024

Table of Contents

Create ILM rule

Create an ILM rule: Overview

To manage objects, you create a set of information lifecycle management (ILM) rules and organize them into an ILM policy.

Every object ingested into the system is evaluated against the active policy. When a rule in the policy matches an object's metadata, the instructions in the rule determine what actions StorageGRID takes to copy and store that object.

> ℹ️ Object metadata is not managed by ILM rules. Instead, object metadata is stored in a Cassandra database in what is known as a metadata store. Three copies of object metadata are automatically maintained at each site to protect the data from loss.

Elements of an ILM rule

An ILM rule has three elements:

- **Filtering criteria**: A rule's basic and advanced filters define which objects the rule applies to. If an object matches all filters, StorageGRID applies the rule and creates the object copies specified in the rule's placement instructions.
- **Placement instructions**: A rule's placement instructions define the number, type, and location of object copies. Each rule can include a sequence of placement instructions to change the number, type, and location of object copies over time. When the time period for one placement expires, the instructions in the next placement are automatically applied by the next ILM evaluation.
- **Ingest behavior**: A rule's ingest behavior allows you to choose how the objects filtered by the rule are protected as they are ingested (when an S3 or Swift client saves an object to the grid).

ILM rule filtering

When you create an ILM rule, you specify filters to identify which objects the rule applies to.

In the simplest case, a rule might not use any filters. Any rule that does not use filters applies to all objects, so it must be the last (default) rule in an ILM policy. The default rule provides storage instructions for objects that don't match the filters in another rule.

- Basic filters allow you to apply different rules to large, distinct groups of objects. These filters allow you to apply a rule to specific tenant accounts, specific S3 buckets or Swift containers, or both.

  Basic filters give you a simple way to apply different rules to large numbers of objects. For example, your company's financial records might need to be stored to meet regulatory requirements, while data from the marketing department might need to be stored to facilitate daily operations. After creating separate tenant accounts for each department or after segregating data from the different departments into separate S3 buckets, you can easily create one rule that applies to all financial records and a second rule that applies to all marketing data.

- Advanced filters give you granular control. You can create filters to select objects based on the following object properties:
  - Ingest time

- ◦ Last access time

- ◦ All or part of the object name (Key)

- ◦ Location constraint (S3 only)

- ◦ Object size

- ◦ User metadata

- ◦ Object tag (S3 only)

You can filter objects on very specific criteria. For example, objects stored by a hospital's imaging department might be used frequently when they are less than 30 days old and infrequently afterwards, while objects that contain patient visit information might need to be copied to the billing department at the health network's headquarters. You can create filters that identify each type of object based on object name, size, S3 object tags, or any other relevant criteria, and then create separate rules to store each set of objects appropriately.

You can combine filters as needed in a single rule. For example, the marketing department might want to store large image files differently than their vendor records, while the Human Resources department might need to store personnel records in a specific geography and policy information centrally. In this case you can create rules that filter by tenant account to segregate the records from each department, while using filters in each rule to identify the specific type of objects that the rule applies to.

ILM rule placement instructions

Placement instructions determine where, when, and how object data is stored. An ILM rule can include one or more placement instructions. Each placement instruction applies to a single period of time.

When you create placement instructions:

- You start by specifying the reference time, which determines when the placement instructions start. The reference time might be when an object is ingested, when an object is accessed, when a versioned object becomes noncurrent, or a user-defined time.

- Next, you specify when the placement will apply, relative to the reference time. For example, a placement might start on day 0 and continue for 365 days, relative to when the object was ingested.

- Finally, you specify the type of copies (replication or erasure coding) and the location where the copies are stored. For example, you might want to store two replicated copies at two different sites.

Each rule can define multiple placements for a single time period and different placements for different time periods.

- To place objects in multiple locations during a single time period, select **Add other type or location** to add more than one line for that time period.

- To place objects in different locations in different time periods, select **Add another time period** to add the next time period. Then, specify one or more lines within the time period.

The example shows two placement instructions on the Define placements page of the Create ILM rule wizard.

The first placement instruction ① has two lines for the first year:

- The first line creates two replicated object copies at two data center sites.
- The second line creates a 6+3 erasure-coded copy using three data center sites.

The second placement instruction ② creates two archived copies after one year and keeps those copies forever.

When you define the set of placement instructions for a rule, you must ensure that at least one placement instruction begins at day 0, that there are no gaps between the time periods you have defined, and that the final placement instruction continues either forever or until you no longer require any object copies.

As each time period in the rule expires, the content placement instructions for the next time period are applied. New object copies are created and any unneeded copies are deleted.

ILM rule ingest behavior

Ingest behavior controls whether object copies are immediately placed according to the instructions in the rule, or if interim copies are made and the placement instructions are applied later. The following ingest behaviors are available for ILM rules:

- **Balanced**: StorageGRID attempts to make all copies specified in the ILM rule at ingest; if this is not possible, interim copies are made and success is returned to the client. The copies specified in the ILM rule are made when possible.
- **Strict**: All copies specified in the ILM rule must be made before success is returned to the client.
- **Dual commit**: StorageGRID immediately makes interim copies of the object and returns success to the client. Copies specified in the ILM rule are made when possible.

Related information

- Ingest options
- Advantages, disadvantages, and limitations of the ingest options
- How consistency controls and ILM rules interact to affect data protection

Example ILM rule

As an example, an ILM rule could specify the following:

- Apply only to the objects belonging to Tenant A.

- Make two replicated copies of those objects and store each copy at a different site.

- Retain the two copies "forever," which means that StorageGRID will not automatically delete them. Instead, StorageGRID will retain these objects until they are deleted by a client delete request or by the expiration of a bucket lifecycle.

- Use the Balanced option for ingest behavior: the two-site placement instruction is applied as soon as Tenant A saves an object to StorageGRID, unless it is not possible to immediately make both required copies.

  For example, if Site 2 is unreachable when Tenant A saves an object, StorageGRID will make two interim copies on Storage Nodes at Site 1. As soon as Site 2 becomes available, StorageGRID will make the required copy at that site.

Related information
- What is a storage pool?
- What is a Cloud Storage Pool?

Access the Create an ILM rule wizard

ILM rules allow you to manage the placement of object data over time. To create an ILM rule, you use the Create an ILM rule wizard.

> (i) If you want to create the default ILM rule for a policy, follow the instructions for creating a default ILM rule instead.

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

- You have specific access permissions.

- If you want to specify which tenant accounts this rule applies to, you have the Tenant accounts permission or you know the account ID for each account.

- If you want the rule to filter objects on last access time metadata, Last access time updates must be enabled by bucket for S3 or by container for Swift.

- You have configured any Cloud Storage Pools you plan to use. See Create Cloud Storage Pool.

- You are familiar with the ingest options.

- If you need to create a compliant rule for use with S3 Object Lock, you are familiar with the requirements for S3 Object Lock.

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

Information lifecycle
management rules in
StorageGRID 11.7
Getting Started

■ NetApp
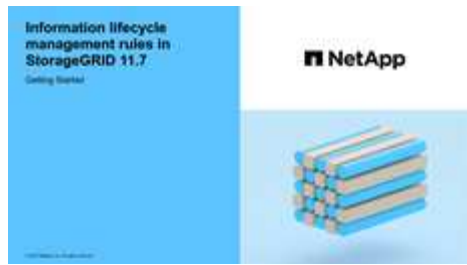
About this task

When creating ILM rules:

- Consider the StorageGRID system's topology and storage configurations.
- Consider what types of object copies you want to make (replicated or erasure coded) and the number of copies of each object that are required.
- Determine what types of object metadata are used in the applications that connect to the StorageGRID system. ILM rules filter objects based on their metadata.
- Consider where you want object copies to be placed over time.
- Decide which ingest option to use (Balanced, Strict, or Dual commit).

Steps

1. Select **ILM** > **Rules**.

   Based on the number of sites in the grid, the Make 2 Copies rule or the 1 Copy Per Site rule is shown in the list of rules.

   > ⓘ   If the global S3 Object Lock setting has been enabled for the StorageGRID system, the summary table includes a **Compliant** column, and the details for the selected rule include a **Compliant** field.

2. Select **Create**. Step 1 (Enter details) of the Create an ILM rule wizard appears.

Step 1 of 3: Enter details

The **Enter details** step of the Create an ILM rule wizard allows you to enter a name and description for the rule and to define filters for the rule.

Entering a description and defining filters for the rule are optional.

About this task

When evaluating an object against an ILM rule, StorageGRID compares the object metadata to the rule's filters. If the object metadata matches all filters, StorageGRID uses the rule to place the object. You can design a rule to apply to all objects, or you can specify basic filters, such as one or more tenant accounts or bucket names, or advanced filters, such as the object's size or user metadata.

Steps

1. Enter a unique name for the rule in the **Name** field.

2. Optionally, enter a short description for the rule in the **Description** field.

   You should describe the rule's purpose or function so you can recognize the rule later.

3. Optionally, select one or more S3 or Swift tenant accounts to which this rule applies. If this rule applies to all tenants, leave this field blank.

   If you don't have either the Root access permission or the Tenant accounts permission, you can't select tenants from the list. Instead, enter the tenant ID or enter multiple IDs as a comma-delimited string.

4. Optionally, specify the S3 buckets or Swift containers to which this rule applies.

   If **matches all** is selected (default), the rule applies to all S3 buckets or Swift containers.

5. For S3 tenants, optionally select **Yes** to apply the rule only to older object versions in S3 buckets that have versioning enabled.

   If you select **Yes**, "Noncurrent time" will be automatically selected for Reference time in Step 2 of the Create an ILM rule wizard.

   > ⓘ   Noncurrent time applies only to S3 objects in versioning-enabled buckets. See Operations on buckets, PUT Bucket versioning and Manage objects with S3 Object Lock.

   You can use this option to reduce the storage impact of versioned objects by filtering for noncurrent object versions. See Example 4: ILM rules and policy for S3 versioned objects.

6. Optionally, select **Add an advanced filter** to specify additional filters.

   If you don't configure advanced filtering, the rule applies to all objects that match the basic filters. For more information about advanced filtering, see Use advanced filters in ILM rules and Specify multiple metadata types and values.

7. Select **Continue**. Step 2 (Define placements) of the Create an ILM rule wizard appears.

Use advanced filters in ILM rules

Advanced filtering allows you to create ILM rules that apply only to specific objects based on their metadata. When you set up advanced filtering for a rule, you select the type of metadata you want to match, select an operator, and specify a metadata value. When objects are evaluated, the ILM rule is applied only to those objects that have metadata matching the advanced filter.

The table shows the types of metadata you can specify in advanced filters, the operators you can use for each type of metadata, and the metadata values expected.

Metadata type	Supported operators	Metadata value
Ingest time	• is • is not • is before • is on or before • is after • is on or after	Time and date the object was ingested. **Note:** To avoid resource issues when activating an new ILM policy, you can use the Ingest time advanced filter in any rule that might change the location of large numbers of existing objects. Set Ingest time to be greater than or equal to the approximate time when the new policy will go into effect to ensure that existing objects aren't moved unnecessarily.

Metadata type	Supported operators	Metadata value
Key	• equals • does not equal • contains • does not contain • starts with • does not start with • ends with • does not end with	All or part of a unique S3 or Swift object key. For example, you might want to match objects that end with `.txt` or start with `test-object/`.
Last access time	• is • is not • is before • is on or before • is after • is on or after	Time and date the object was last retrieved (read or viewed). **Note:** If you plan to use last access time as an advanced filter, Last access time updates must be enabled for the S3 bucket or Swift container.
Location constraint (S3 only)	• equals • does not equal	The region where an S3 bucket was created. Use **ILM > Regions** to define the regions that are shown. **Note:** A value of us-east-1 will match objects in buckets created in the us-east-1 region as well as objects in buckets that have no region specified. See Configure regions (optional and S3 only).
Object size	• equals • does not equal • less than • less than or equal to • greater than • greater than or equal to	The object's size. Erasure coding is best suited for objects greater than 1 MB. Don't use erasure coding for objects smaller than 200 KB to avoid the overhead of managing very small erasure-coded fragments. **Note:** To filter on object sizes smaller than 1 MB, enter a decimal value. Your browser type and locale settings control whether you need to use a period or a comma as the decimal separator.

Metadata type	Supported operators	Metadata value
User metadata	• contains • ends with • equals • exists • does not contain • does not end with • does not equal • does not exist • does not start with • starts with	Key-value pair, where **User metadata name** is the key and **Metadata value** is the value. For example, to filter on objects that have user metadata of `color=blue`, specify `color` for **User metadata name**, `equals` for the operator, and `blue` for **Metadata value**. **Note:** User-metadata names aren't case sensitive; user-metadata values are case sensitive.
Object tag (S3 only)	• contains • ends with • equals • exists • does not contain • does not end with • does not equal • does not exist • does not start with • starts with	Key-value pair, where **Object tag name** is the key and **Object tag value** is the value. For example, to filter on objects that have an object tag of `Image=True`, specify `Image` for **Object tag name**, `equals` for the operator, and `True` for **Object tag value**. **Note:** Object tag names and object tag values are case sensitive. You must enter these items exactly as they were defined for the object.

Specify multiple metadata types and values

When you define advanced filtering, you can specify multiple types of metadata and multiple metadata values. For example, if you want a rule to match objects between 10 MB and 100 MB in size, you would select the **Object size** metadata type and specify two metadata values.

- The first metadata value specifies objects greater than or equal to 10 MB.
- The second metadata value specifies objects less than or equal to 100 MB.

Using multiple entries allows you to have precise control over which objects are matched. In the following example, the rule applies to objects that have a Brand A or Brand B as the value of the camera_type user metadata. However, the rule only applies to those Brand B objects that are smaller than 10 MB.

Step 2 of 3: Define placements

The **Define placements** step of the Create ILM Rule wizard allows you to define the placement instructions that determine how long objects are stored, the type of copies (replicated or erasure coded), the storage location, and the number of copies.

About this task

An ILM rule can include one or more placement instructions. Each placement instruction applies to a single period of time. When you use more than one instruction, the time periods must be contiguous, and at least one instruction must start on day 0. The instructions can continue either forever, or until you no longer require any object copies.

Each placement instruction can have multiple lines if you want to create different types of copies or use different locations during that time period.

In this example, the ILM rule stores one replicated copy in Site 1 and one replicated copy in Site 2 for the first year. After one year, a 2+1 erasure-coded copy is made and saved at only one site.

Steps

1. For **Reference time**, select the type of time to use when calculating the start time for a placement instruction.

Option	Description
Ingest time	The time when the object was ingested.
Last access time	The time when the object was last retrieved (read or viewed). **Note:** To use this option, updates to Last access time must be enabled for the S3 bucket or Swift container. See Use Last access time in ILM rules.
User defined creation time	A time specified in user-defined metadata.
Noncurrent time	"Noncurrent time" is automatically selected if you selected **Yes** for the question, "Apply this rule to older object versions only (in S3 buckets with versioning enabled)?" in Step 1 of the Create an ILM rule wizard.

> (i) If you want to create a compliant rule, you must select **Ingest time**. See Manage objects with S3 Object Lock.

2. In the **Time period and placements** section, enter a starting time and a duration for the first time period.

   For example, you might want to specify where to store objects for the first year (*From day 0 store for 365 days*). At least one instruction must start at day 0.

3. If you want to create replicated copies:

   a. From the **Store objects by** drop-down list, select **replicating**.

   b. Select the number of copies you want to make.

   A warning appears if you change the number of copies to 1. An ILM rule that creates only one replicated copy for any time period puts data at risk of permanent loss. See Why you should not use single-copy replication.

   To avoid the risk, do one or more of the following:

   - Increase the number of copies for the time period.
   - Add copies to other storage pools or to a Cloud Storage Pool.
   - Select **erasure coding** instead of **replicating**.

     You can safely ignore this warning if this rule already creates multiple copies for all time periods.

   c. In the **copies at** field, select the storage pools you want to add.

   If you specify only one storage pool, be aware that StorageGRID can store only one replicated copy of an object on any given Storage Node. If your grid includes three Storage Nodes and you select 4 as the number of copies, only three copies will be made—one copy for each Storage Node.

> **(i)** The **ILM placement unachievable** alert is triggered to indicate that the ILM rule could not be completely applied.

If you specify more than one storage pool, keep these rules in mind:

- The number of copies can't be greater than the number of storage pools.

- If the number of copies equals the number of storage pools, one copy of the object is stored in each storage pool.

- If the number of copies is less than the number of storage pools, one copy is stored at the ingest site, and then the system distributes the remaining copies to keep disk usage among the pools balanced, while ensuring that no site gets more than one copy of an object.

- If the storage pools overlap (contain the same Storage Nodes), all copies of the object might be saved at only one site. For this reason, don't specify the All Storage Nodes storage pool (StorageGRID 11.6 and earlier) and another storage pool.

4. If you want to create an erasure-coded copy:

   a. From the **Store objects by** drop-down list, select **erasure coding**.

   > **(i)** Erasure coding is best suited for objects greater than 1 MB. Don't use erasure coding for objects smaller than 200 KB to avoid the overhead of managing very small erasure-coded fragments.

   b. If you didn't add an Object size filter for a value greater than 0.2 MB, select **Previous** to return to Step 1. Then, select **Add an advanced filter** and set an **Object size** filter to any value greater than 0.2 MB.

   c. Select the storage pool you want to add and the erasure-coding scheme you want to use.

   The storage location for an erasure-coded copy includes the name of the erasure coding scheme, followed by the name of the storage pool.

5. Optionally:

   a. Select **Add other type or location** to create additional copies at different locations.

   b. Select **Add another time period** to add different time periods.

   > **(i)** Objects are automatically deleted at the end of the final time period unless the final time period ends with **forever**.

6. If you want to store objects in a Cloud Storage Pool:

   a. In the **Store objects by** drop-down list, select **replicating**.

   b. Select the **copies at** field, then select a Cloud Storage Pool.

   When using Cloud Storage Pools, keep these rules in mind:

   - You can't select more than one Cloud Storage Pool in a single placement instruction. Similarly, you can't select a Cloud Storage Pool and a storage pool in the same placement instruction.

   - You can store only one copy of an object in any given Cloud Storage Pool. An error message appears if you set **Copies** to 2 or more.

   - You can't store more than one object copy in any Cloud Storage Pool at the same time. An error message appears if multiple placements that use a Cloud Storage Pool have overlapping dates or if multiple lines in the same placement use a Cloud Storage Pool.

- You can store an object in a Cloud Storage Pool at the same time that object is being stored as replicated or erasure coded copies in StorageGRID. However, you must include more than one line in the placement instruction for the time period, so you can specify the number and types of copies for each location.

7. In the Retention diagram, confirm your placement instructions.

   Each line in the diagram shows where and when object copies will be placed. The color of a line represents the type of copy:

▭	Replicated copy
▭	Erasure-coded copy
▭	Cloud Storage Pool copy

   In this example, the ILM rule stores one replicated copy in Site 1 and one replicated copy in Site 2 for the first year. After one year and for an additional 10 years, a 6+3 erasure-coded copy will be saved at three sites. After 11 years total, the objects will be deleted from StorageGRID.

   The Rule analysis section of the Retention diagram states:

   - StorageGRID site-loss protection will apply for the duration of this rule.
   - Objects processed by this rule will be deleted after Day 4015.

     ⓘ | See Enable site-loss protection.
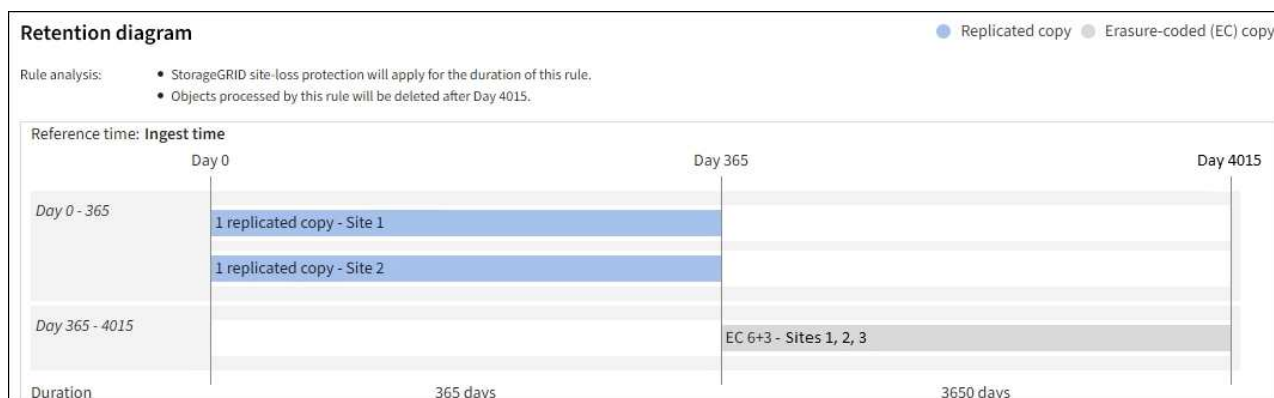
8. Select **Continue**. Step 3 (Select ingest behavior) of the Create an ILM rule wizard appears.

Use Last access time in ILM rules

You can use Last access time as the reference time in an ILM rule. For example, you might want to leave objects that have been viewed in the last three months on local Storage Nodes, while moving objects that have not been viewed as recently to an off-site location. You can also use Last access time as an advanced filter if you want an ILM rule to apply only to objects that were last accessed on a specific date.

About this task

Before using Last access time in an ILM rule, review the following considerations:

- When using Last access time as a reference time, be aware that changing the Last access time for an object does not trigger an immediate ILM evaluation. Instead, the object's placements are assessed and the object is moved as required when background ILM evaluates the object. This could take two weeks or more after the object is accessed.

  Take this latency into account when creating ILM rules based on Last access time and avoid placements that use short time periods (less than one month).

- When using Last access time as an advanced filter or as a reference time, you must enable last access time updates for S3 buckets. You can use the Tenant Manager or the Tenant Management API.

  > ⓘ Last access time updates are always enabled for Swift containers, but are disabled by default for S3 buckets.

  > ⓘ Be aware that enabling last access time updates can reduce performance, especially in systems with small objects. The performance impact occurs because StorageGRID must update the objects with new timestamps every time the objects are retrieved.

The following table summarizes whether the Last access time is updated for all objects in the bucket for different types of requests.

Type of request	Whether Last access time is updated when last access time updates are disabled	Whether Last access time is updated when last access time updates are enabled
Request to retrieve an object, its access control list, or its metadata	No	Yes
Request to update an object's metadata	Yes	Yes
Request to copy an object from one bucket to another	- No, 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

Step 3 of 3: Select ingest behavior

The **Select ingest behavior** step of the Create ILM Rule wizard allows you to choose how the objects filtered by this rule are protected as they are ingested.

About this task

StorageGRID can make interim copies and queue the objects for ILM evaluation later, or it can make copies to meet the rule's placement instructions immediately.

Steps

1. Select the ingest behavior to use.

   For more information, see Advantages, disadvantages, and limitations of the ingest options.

   > ⓘ   You can't use the Balanced or Strict option if the rule uses one of these placements:
   >
   > - A Cloud Storage Pool at day 0
   > - An Archive Node at day 0
   > - A Cloud Storage Pool or an Archive Node when the rule uses a User defined creation time as a Reference time
   >
   > See Example 5: ILM rules and policy for Strict ingest behavior.

2. Select **Create**.

   The ILM rule is created. The rule does not become active until it is added to an ILM policy and that policy is activated.

   To view the details of the rule, select the rule's name on the ILM rules page.

Create a default ILM rule

Before creating an ILM policy, you must create a default rule to place any objects not matched by another rule in the policy. The default rule can't use any filters. It must apply to all tenants, all buckets, and all object versions.

Before you begin

- You are signed in to the Grid Manager using a supported web browser.
- You have specific access permissions.

About this task

The default rule is the last rule to be evaluated in an ILM policy, so it can't use any filters. The placement instructions for the default rule are applied to any objects that aren't matched by another rule in the policy.

In this example policy, the first rule applies only to objects belonging to test-tenant-1. The default rule, which is last, applies to objects belonging to all other tenant accounts.

When you create the default rule, keep these requirements in mind:

- The default rule is automatically placed as the last rule in the policy.
- The default rule can't use any basic or advanced filters.
- The default rule must apply to all object versions.
- The default rule should create replicated copies.

> (i) Don't use a rule that creates erasure-coded copies as the default rule for a policy. Erasure-coding rules should use an advanced filter to prevent smaller objects from being erasure coded.

- In general, the default rule should retain objects forever.
- If you are using (or you plan to enable) the global S3 Object Lock setting, the default rule for the active or proposed policy must be compliant.

Steps

1. Select **ILM** > **Rules**.
2. Select **Create**.

   Step 1 (Enter details) of the Create ILM rule wizard appears.

3. Enter a unique name for the rule in the **Rule name** field.
4. Optionally, enter a short description for the rule in the **Description** field.
5. Leave the **Tenant accounts** field blank.

   The default rule must apply to all tenant accounts.

6. Leave the Bucket name drop-down selection as **matches all**.

   The default rule must apply to all S3 buckets and Swift containers.

7. Keep the default answer, **No**, for the question, "Apply this rule to older object versions only (in S3 buckets with versioning enabled)?"

8. Don't add advanced filters.

   The default rule can't specify any filters.

9. Select **Next**.

   Step 2 (Define placements) appears.

10. For Reference time, select any option.

    If you kept the default answer, **No**, for the question, "Apply this rule to older object versions only?" Noncurrent time will not be included in the pull-down list. The default rule must apply all object versions.

11. Specify the placement instructions for the default rule.

    ○ The default rule should retain objects forever. A warning appears when you activate a new policy if the default rule does not retain objects forever. You must confirm this is the behavior you expect.

    ○ The default rule should create replicated copies.

    > ⓘ Don't use a rule that creates erasure-coded copies as the default rule for a policy. Erasure-coding rules should include the **Object size (MB) greater than 0.2** advanced filter to prevent smaller objects from being erasure coded.

    ○ If you are using (or you plan to enable) the global S3 Object Lock setting, the default rule must be compliant:

      ▪ It must create at least two replicated object copies or one erasure-coded copy.

      ▪ These copies must exist on Storage Nodes for the entire duration of each line in the placement instructions.

      ▪ Object copies can't be saved in a Cloud Storage Pool.

      ▪ Object copies can't be saved on Archive Nodes.

      ▪ At least one line of the placement instructions must start at day 0, using Ingest time as the reference time.

      ▪ At least one line of the placement instructions must be "forever."

12. Look at the Retention diagram to confirm your placement instructions.

13. Select **Continue**.

    Step 3 (Select ingest behavior) appears.

14. Select the ingest option to use, and select **Create**.