



# **Example ILM rules and policies**

## **StorageGRID**

NetApp  
April 10, 2024

# Table of Contents

- Example ILM rules and policies ..... 1
  - Example 1: ILM rules and policy for object storage ..... 1
  - Example 2: ILM rules and policy for EC object size filtering ..... 4
  - Example 3: ILM rules and policy for better protection for image files ..... 6
  - Example 4: ILM rules and policy for S3 versioned objects..... 8
  - Example 5: ILM rules and policy for Strict ingest behavior..... 11
  - Example 6: Changing an ILM policy..... 15
  - Example 7: Compliant ILM policy for S3 Object Lock ..... 20

# Example ILM rules and policies

## Example 1: ILM rules and policy for object storage

You can use the following example rules and policy as a starting point when defining an ILM policy to meet your object protection and retention requirements.



The following ILM rules and policy are only examples. There are many ways to configure ILM rules. Before activating a new policy, simulate the proposed policy to confirm it will work as intended to protect content from loss.

### ILM rule 1 for example 1: Copy object data to two data centers

This example ILM rule copies object data to storage pools in two data centers.

Rule definition	Example value
Storage Pools	Two storage pools, each at different data centers, named Storage Pool DC1 and Storage Pool DC2.
Rule Name	Two Copies Two Data Centers
Reference Time	Ingest Time
Content Placement	On Day 0, keep two replicated copies forever—one in Storage Pool DC1 and one in Storage Pool DC2.

Configure placement instructions to specify how you want objects matched by this rule to be stored.

Two Copies Two Data Centers

Reference Time

Ingest Time

Placements

Sort by start day

From day

0

store

forever

Add Remove

Type

replicated

Location

Storage Pool DC1

Storage Pool DC2

Add Pool

Copies

2

+ -

Specifying multiple storage pools might cause data to be stored at the same site if the pools overlap. See [Managing objects with information lifecycle management](#) for more information.

Retention Diagram

Refresh

Trigger

Day 0

Storage Pool DC1

Storage Pool DC2

Duration

Forever

Cancel Back Next

## ILM rule 2 for example 1: Erasure Coding profile with bucket matching

This example ILM rule uses an Erasure Coding profile and an S3 bucket to determine where and how long the object is stored.

Rule definition	Example value
Erasure Coding Profile	<ul style="list-style-type: none"> <li>One storage pool across three data centers (All 3 sites)</li> <li>Use 6+3 erasure-coding scheme</li> </ul>
Rule Name	EC for S3 bucket finance-records
Reference Time	Ingest Time
Content Placement	For objects in the S3 bucket named finance-records, create one erasure-coded copy in the pool specified by the Erasure Coding profile. Keep this copy forever.

Configure placement instructions to specify how you want objects matched by this rule to be stored.

**EC for S3 bucket finance-records**

Reference Time
Ingest Time

**Placements**
Sort by start day

From day 0 store forever
Add Remove

Type erasure coded Location All 3 sites (6 plus 3) Copies 1
+ x

**Retention Diagram**
Refresh

Trigger
Day 0
Duration
Forever

Cancel Back Next

## ILM policy for example 1

The StorageGRID system allows you to design sophisticated and complex ILM policies; however, in practice, most ILM policies are simple.

A typical ILM policy for a multi-site topology might include ILM rules such as the following:

- At ingest, use 6+3 erasure coding to store all objects belonging to the S3 bucket named `finance-records` across three data centers.
- If an object does not match the first ILM rule, use the policy's default ILM rule, Two Copies Two Data Centers, to store a copy of that object in two data centers, DC1 and DC2.

## Configure ILM Policy

Create a proposed policy by selecting and arranging rules. Then, save the policy and edit it later as required. Click Simulate to verify a saved policy using test objects. When you are ready, click Activate to make this policy the active ILM policy for the grid.

Name	Object Storage Policy
Reason for change	new proposed policy

### Rules

1. Select the rules you want to add to the policy.
2. Determine the order in which the rules will be evaluated by dragging and dropping the rows. The default rule will be automatically placed at the end of the policy and cannot be moved.

+ Select Rules			
Default	Rule Name	Tenant Account	Actions
	EC for S3 bucket finance-records	Ignore	✕
✓	Two Copies Two Data Centers	Ignore	✕

Cancel

Save

## Example 2: ILM rules and policy for EC object size filtering

You can use the following example rules and policy as starting points to define an ILM policy that filters by object size to meet recommended EC requirements.



The following ILM rules and policy are only examples. There are many ways to configure ILM rules. Before activating a new policy, simulate the proposed policy to confirm it will work as intended to protect content from loss.

### ILM rule 1 for example 2: Use EC for objects greater than 1 MB

This example ILM rule erasure codes objects that are greater than 1 MB.



Erasure coding is best suited for objects greater than 1 MB. Do not use erasure coding for objects smaller than 200 KB to avoid the overhead of managing very small erasure-coded fragments.

Rule definition	Example value
Rule Name	EC only objects > 1 MB
Reference Time	Ingest Time
Advanced Filtering for Object Size	Object Size (MB) greater than 1
Content Placement	Create a 2+1 erasure-coded copy using three sites

**EC only objects > 1 MB**

Matches all of the following metadata:

Object Size (MB) ▼	greater than ▼	1	+ ×
<div style="float: left; border: 1px solid #ccc; padding: 2px 5px; margin-right: 5px;">+ ×</div>			

### ILM rule 2 for example 2: Two replicated copies

This example ILM rule creates two replicated copies and does not filter by object size. This rule is the default rule for the policy. Because the first rule filters out all objects greater than 1 MB, this rule only applies to objects that are 1 MB or smaller.

Rule definition	Example value
Rule Name	Two Replicated Copies
Reference Time	Ingest Time
Advanced Filtering for Object Size	None
Content Placement	Create two replicated copies and save them at two data centers, DC1 and DC2

### ILM policy for example 2: Use EC for objects greater than 1 MB

This example ILM policy includes two ILM rules:

- The first rule erasure codes all objects that are greater than 1 MB.
- The second (default) ILM rule creates two replicated copies. Because objects greater than 1 MB have been filtered out by rule 1, rule 2 only applies to objects that are 1 MB or smaller.

Create a proposed policy by selecting and arranging rules. Then, save the policy and edit it later as required. Click Simulate to verify a saved policy using test objects. When you are ready, click Activate to make this policy the active ILM policy for the grid.

Name

Use EC for objects greater than 1 MB

Reason for change






new policy

Rules

1. Select the rules you want to add to the policy.

2. Determine the order in which the rules will be evaluated by dragging and dropping the rows. The default rule will be automatically placed at the end of the policy and cannot be moved.

+ Select Rules

Default	Rule Name	Tenant Account	Actions
	EC only objects > 1 MB 	—	
	Two replicated copies 	—	

Cancel

Save

## Example 3: ILM rules and policy for better protection for image files

You can use the following example rules and policy to ensure that images greater than 1 MB are erasure coded and that two copies are made of smaller images.



The following ILM rules and policy are only examples. There are many ways to configure ILM rules. Before activating a new policy, simulate the proposed policy to confirm it will work as intended to protect content from loss.

### ILM rule 1 for example 3: Use EC for image files greater than 1 MB

This example ILM rule uses advanced filtering to erasure code all image files greater than 1 MB.



Erasur coding is best suited for objects greater than 1 MB. Do not use erasure coding for objects smaller than 200 KB to avoid the overhead of managing very small erasure-coded fragments.

Rule definition	Example value
Rule Name	EC image files > 1 MB



Rule definition	Example value
Reference Time	Ingest Time
Advanced Filtering for Object Size	Object Size (MB) greater than 1.0
Advanced Filtering for User Metadata	User Metadata type equals image
Content Placement	Create a 2+1 erasure-coded copy using three sites

**EC image files > 1 MB**

Matches all of the following metadata:

Object Size (MB)
greater than
1
+
x

User Metadata
type
equals
image
+
x

+
x

Because this rule is configured as the first rule in the policy, the erasure-coding placement instruction only applies to images that are greater than 1 MB.

## ILM rule 2 for example 3: Create 2 replicated copies for all remaining image files

This example ILM rule uses advanced filtering to specify that smaller image files be replicated. Because the first rule in the policy has already matched image files greater than 1 MB, this rule applies to image files that are 1 MB or smaller.

Rule definition	Example value
Rule Name	2 copies for image files
Reference Time	Ingest Time
Advanced Filtering for User Metadata	User Metadata type equals image files
Content Placement	Create 2 replicated copies in two Storage Pools

## ILM policy for example 3: Better protection for image files

This example ILM policy includes three rules:

- The first rule erasure codes all image files greater than 1 MB.

- The second rule creates two copies of any remaining image files (that is, images that are 1 MB or smaller).
- The default rule applies to all remaining objects (that is, any non-image files).

Reason for change: new policy		
Rules are evaluated in order, starting from the top.		
Rule Name	Default	Tenant Account
EC image files > 1 MB 		—
2 copies for small images 		—
Default rule 	✓	—

## Example 4: ILM rules and policy for S3 versioned objects

If you have an S3 bucket with versioning enabled, you can manage the noncurrent object versions by including rules in your ILM policy that use **Noncurrent time** as the Reference Time.

As this example shows, you can control the amount of storage used by versioned objects by using different placement instructions for noncurrent object versions.



The following ILM rules and policy are only examples. There are many ways to configure ILM rules. Before activating a new policy, simulate the proposed policy to confirm it will work as intended to protect content from loss.



If you create ILM policies to manage noncurrent object versions, be aware that you must know the object version's UUID or CBID to simulate the policy. To find an object's UUID and CBID, use Object Metadata Lookup while the object is still current. See [Verify an ILM policy with object metadata lookup](#).

### Related information

- [How objects are deleted](#)

### ILM rule 1 for example 4: Save three copies for 10 years

This example ILM rule stores a copy of each object at three data centers for 10 years.

This rule applies to all objects, whether or not they are versioned.

Rule definition	Example value
Storage Pools	Three storage pools, each at different data centers, named DC1, DC2, and DC3.
Rule Name	Three Copies Ten Years
Reference Time	Ingest Time

Rule definition	Example value
Content Placement	On Day 0, keep three replicated copies for 10 years (3,652 days), one in DC1, one in DC2, and one in DC3. At the end of 10 years, delete all copies of the object.

#### Create ILM Rule Step 2 of 3: Define Placements

Configure placement instructions to specify how you want objects matched by this rule to be stored.

**Three Copies Ten Years**  
 Save three copies for ten years

Reference Time

**Placements** ? Sort by start day

From day  store for  days Add Remove

Type  Location  Copies  + x

Specifying multiple storage pools might cause data to be stored at the same site if the pools overlap. See [Managing objects with information lifecycle management](#) for more information.

**Retention Diagram** ? Refresh

Trigger	Day 0	Day 3652
DC1		
DC2		
DC3		
Duration	3652 days	Forever

Cancel Back Next

## ILM rule 2 for example 4: Save two copies of noncurrent versions for 2 years

This example ILM rule stores two copies of the noncurrent versions of an S3 versioned object for 2 years.

Because ILM rule 1 applies to all versions of the object, you must create another rule to filter out any noncurrent versions. This rule uses the **Noncurrent Time** option for Reference Time.

In this example, only two copies of the noncurrent versions are stored, and those copies will be stored for two years.

Rule definition	Example value
Storage Pools	Two storage pools, each at different data centers, named DC1 and DC2.
Rule Name	Noncurrent Versions: Two Copies Two Years
Reference Time	Noncurrent Time

Rule definition	Example value
Content Placement	On Day 0 relative to Noncurrent Time (that is, starting from the day the object version becomes the noncurrent version), keep two replicated copies of the noncurrent object versions for 2 years (730 days), one in DC1 and one in DC2. At the end of 2 years, delete the noncurrent versions.

### Noncurrent Versions: Two Copies Two Years

Save two copies of noncurrent versions for two years

Reference Time
Noncurrent Time

#### Placements ?

Sort by start day

From day
0
store
for
730
days
Add Remove

Type
replicated
Location
DC1 x DC2 x Add Pool
Copies
2
+ x

Specifying multiple storage pools might cause data to be stored at the same site if the pools overlap. See [Managing objects with information lifecycle management](#) for more information.

#### Retention Diagram ?

Refresh

Trigger

Day 0 Year 2

DC1

DC2

Duration

2 years Forever

## ILM policy for example 4: S3 versioned objects

If you want to manage older versions of an object differently than the current version, rules that use **Noncurrent Time** as the Reference Time must appear in the ILM policy before rules that apply to the current object version.

An ILM policy for S3 versioned objects might include ILM rules such as the following:

- Keep any older (noncurrent) versions of each object for 2 years, starting from the day the version became noncurrent.



The Noncurrent Time rules must appear in the policy before the rules that apply to the current object version. Otherwise, the noncurrent object versions will never be matched by the Noncurrent Time rule.

- At ingest, create three replicated copies and store one copy at each of three data centers. Keep copies of the current object version for 10 years.

## Configure ILM Policy

Create a proposed policy by selecting and arranging rules. Then, save the policy and edit it later as required. Click Simulate to verify a saved policy using test objects. When you are ready, click Activate to make this policy the active ILM policy for the grid.





Name ILM Policy for S3 Versioned Objects

Reason for change store 3 copies of current version for 10 years and 2 copies of noncurrent versions for 2 years

### Rules

1. Select the rules you want to add to the policy.
2. Determine the order in which the rules will be evaluated by dragging and dropping the rows. The default rule will be automatically placed at the end of the policy and cannot be moved.

+ Select Rules

Default	Rule Name	Tenant Account	Actions
	Noncurrent Versions: Two Copies Two Years 	Ignore	
✓	Three Copies Ten Years 	Ignore	

The default ILM rule in this policy does not retain objects forever. Confirm this is the behavior you expect. Otherwise, any objects that are not matched by another rule will be deleted after 3652 days.

Cancel

Save

When you simulate the example policy, you would expect test objects to be evaluated as follows:

- Any noncurrent object versions would be matched by the first rule. If a noncurrent object version is older than 2 years, it is permanently deleted by ILM (all copies of the noncurrent version removed from the grid).



To simulate noncurrent object versions, you must use that version's UUID or CBID. While the object is still current, you can use Object Metadata Lookup to find its UUID and CBID.

- The current object version would be matched by the second rule. When the current object version has been stored for 10 years, the ILM process adds a delete marker as the current version of the object, and it makes the previous object version "noncurrent." The next time ILM evaluation occurs, this noncurrent version is matched by the first rule. As a result, the copy at DC3 is purged and the two copies at DC1 and DC2 are stored for 2 more years.

## Example 5: ILM rules and policy for Strict ingest behavior

You can use a location filter and the Strict ingest behavior in a rule to prevent objects from being saved at a particular data center location.

In this example, a Paris-based tenant does not want to store some objects outside of the EU because of regulatory concerns. Other objects, including all objects from other tenant accounts, can be stored at either the Paris data center or the US data center.



The following ILM rules and policy are only examples. There are many ways to configure ILM rules. Before activating a new policy, simulate the proposed policy to confirm it will work as intended to protect content from loss.

#### Related information

- [Data-protection options for ingest](#)
- [Step 3 of 3: Define ingest behavior](#)

### ILM rule 1 for example 5: Strict ingest to guarantee Paris data center

This example ILM rule uses the Strict ingest behavior to guarantee that objects saved by a Paris-based tenant to S3 buckets with the region set to eu-west-3 region (Paris) are never stored at the US data center.

This rule applies to objects that belong to the Paris tenant and that have the S3 bucket region set to eu-west-3 (Paris).

Rule definition	Example value
Tenant Account	Paris tenant
Advanced Filtering	Location Constraint equals eu-west-3
Storage Pools	DC1 (Paris)
Rule Name	Strict ingest to guarantee Paris data center
Reference Time	Ingest Time
Content Placement	On Day 0, keep two replicated copies forever in DC1 (Paris)
Ingest Behavior	Strict. Always use this rule's placements on ingest. Ingest fails if it is not possible to store two copies of the object at the Paris data center.

## Strict ingest to guarantee Paris data center

Description: Strict ingest to guarantee Paris data center  
 Ingest Behavior: Strict  
 Tenant Account: Paris tenant (25580610012441844135)  
 Reference Time: Ingest Time  
 Filtering Criteria:

Matches all of the following metadata:

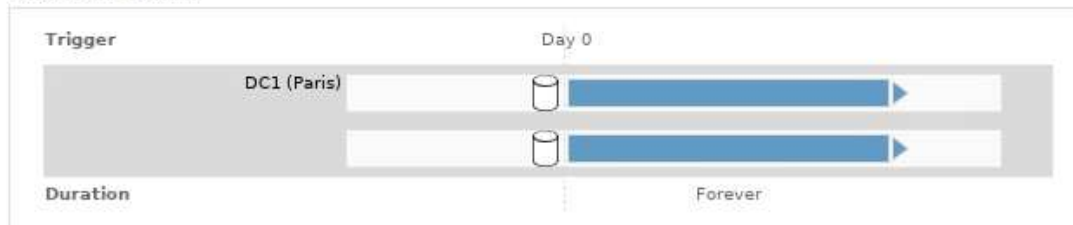
System Metadata

Location Constraint (S3 only)

equals

eu-west-3

Retention Diagram:



## ILM rule 2 for example 5: Balanced ingest for other objects

This example ILM rule uses the Balanced ingest behavior to provide optimum ILM efficiency for any objects not matched by the first rule. Two copies of all objects matched by this rule will be stored—one at the US data center and one at the Paris data center. If the rule cannot be satisfied immediately, interim copies are stored at any available location.

This rule applies to objects that belong to any tenant and any region.

Rule definition	Example value
Tenant Account	Ignore
Advanced Filtering	<i>Not specified</i>
Storage Pools	DC1 (Paris) and DC2 (US)
Rule Name	2 Copies 2 Data Centers
Reference Time	Ingest Time
Content Placement	On Day 0, keep two replicated copies forever at two data centers
Ingest Behavior	Balanced. Objects that match this rule are placed according to the rule's placement instructions if possible. Otherwise, interim copies are made at any available location.

## 2 Copies 2 Data Centers

Description: 2 Copies 2 Data Centers

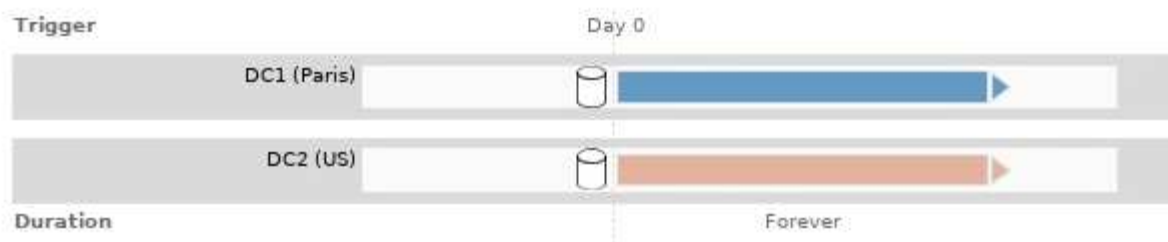
Ingest Behavior: Balanced

Reference Time: Ingest Time

Filtering Criteria:

Matches all objects.

Retention Diagram:



### ILM policy for example 5: Combining ingest behaviors

The example ILM policy includes two rules that have different ingest behaviors.

An ILM policy that uses two different ingest behaviors might include ILM rules such as the following:

- Store objects that belong to the Paris tenant and that have the S3 bucket region set to eu-west-3 (Paris) only in the Paris data center. Fail ingest if the Paris data center is not available.
- Store all other objects (including those that belong to the Paris tenant but that have a different bucket region) in both the US data center and the Paris data center. Make interim copies in any available location if the placement instruction cannot be satisfied.



## Configure ILM Policy

Create a proposed policy by selecting and arranging rules. Then, save the policy and edit it later as required. Click Simulate to verify a saved policy using test objects. When you are ready, click Activate to make this policy the active ILM policy for the grid.

Name	Example policy for Strict ingest
Reason for change	Do not store certain objects for Paris tenant in US

### Rules

1. Select the rules you want to add to the policy.
2. Determine the order in which the rules will be evaluated by dragging and dropping the rows. The default rule will be automatically placed at the end of the policy and cannot be moved.

+ Select Rules

Default	Rule Name	Tenant Account	Actions
	Strict ingest to guarantee Paris data center	Paris tenant (25580610012441844135)	✕
✓	2 Copies 2 Data Centers	Ignore	✕

Cancel

Save

When you simulate the example policy, you expect test objects to be evaluated as follows:

- Any objects that belong to the Paris tenant and that have the S3 bucket region set to eu-west-3 are matched by the first rule and are stored at the Paris data center. Because the first rule uses Strict ingest, these objects are never stored at the US data center. If the Storage Nodes at the Paris data center are not available, ingest fails.
- All other objects are matched by the second rule, including objects that belong to the Paris tenant and that do not have the S3 bucket region set to eu-west-3. One copy of each object is saved at each data center. However, because the second rule uses Balanced ingest, if one data center is unavailable, two interim copies are saved at any available location.

## Example 6: Changing an ILM policy

You might need to create and activate a new ILM policy if your data protection needs change or you add new sites.

Before changing a policy, you must understand how changes in ILM placements can temporarily affect the overall performance of a StorageGRID system.

In this example, a new StorageGRID site has been added in an expansion and the active ILM policy needs to be revised to store data at the new site.



The following ILM rules and policy are only examples. There are many ways to configure ILM rules. Before activating a new policy, simulate the proposed policy to confirm it will work as intended to protect content from loss.

## How does changing an ILM policy affect performance

When you activate a new ILM policy, the performance of your StorageGRID system might be temporarily affected, especially if the placement instructions in the new policy require many existing objects to be moved to new locations.



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.

The types of ILM policy changes that can temporarily affect StorageGRID performance include the following:

- Applying a different Erasure Coding profile to existing erasure-coded objects.



StorageGRID considers each Erasure Coding profile to be unique and does not reuse erasure-coding fragments when a new profile is used.

- Changing the type of copies required for existing objects; for example, converting a large percentage of replicated objects to erasure-coded objects.
- Moving copies of existing objects to a completely different location; for example, moving a large number of objects to or from a Cloud Storage Pool or to or from a remote site.

### Related information

[Create an ILM policy](#)

## Active ILM policy for example 6: Data protection at two sites

In this example, the active ILM policy was initially designed for a two-site StorageGRID system and uses two ILM rules.

### ILM Policies

Review the proposed, active, and historical policies. You can create, edit, or delete a proposed policy; clone the active policy; or view the details for any policy.

<a href="#">+ Create Proposed Policy</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Remove</a>			
Policy Name	Policy State	Start Date	End Date
<input checked="" type="radio"/> Data Protection for Two Sites	Active	2020-06-10 16:42:09 MDT	
<input type="radio"/> Baseline 2 Copies Policy	Historical	2020-06-09 21:48:34 MDT	2020-06-10 16:42:09 MDT

### Viewing Active Policy - Data Protection for Two Sites

Review the rules in this policy. If this is a proposed policy, click Simulate to verify the policy and then click Activate to make the policy active.

Reason for change: Data Protection for Two Sites

Rules are evaluated in order, starting from the top.

Rule Name	Default	Tenant Account
One-Site Erasure Coding for Tenant A		Tenant A (49752734300032812036)
Two-Site Replication for Other Tenants	✓	Ignore

[Simulate](#)

[Activate](#)

In this ILM policy, objects belonging to Tenant A are protected by 2+1 erasure coding at a single site, while

objects belonging to all other tenants are protected across two sites using 2-copy replication.



The first rule in this example uses an advanced filter to ensure that erasure coding is not used for small objects. Any of Tenant A's objects that are smaller than 1 MB will be protected by the second rule, which uses replication.

#### Rule 1: One-site erasure coding for Tenant A

Rule definition	Example value
Rule Name	One-Site Erasure Coding for Tenant A
Tenant Account	Tenant A
Storage Pool	Data Center 1
Content Placement	2+1 erasure coding in Data Center 1 from day 0 to forever

#### Rule 2: Two-site replication for other tenants

Rule definition	Example value
Rule Name	Two-Site Replication for Other Tenants
Tenant Account	Ignore
Storage Pools	Data Center 1 and Data Center 2
Content Placement	Two replicated copies from day 0 to forever: one copy at Data Center 1 and one copy at Data Center 2.

### Proposed ILM policy for example 6: Data protection at three sites

In this example, the ILM policy is being updated for a three-site StorageGRID system.

After performing an expansion to add the new site, the grid administrator created two new storage pools: a storage pool for Data Center 3 and a storage pool containing all three sites (not the same as the All Storage Nodes default storage pool). Then, the administrator created two new ILM rules and a new proposed ILM policy, which is designed to protect data at all three sites.

## Viewing Proposed Policy - Data Protection for Three Sites

Before activating a new ILM policy:

- Review and carefully simulate the policy. Errors in an ILM policy can cause irreparable data loss.
- 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.

See [Managing objects with information lifecycle management](#) for more information.

This policy contains a rule that makes an erasure-coded copy. Confirm that at least one rule uses the Object Size advanced filter to prevent objects that are 200 KB or smaller from being erasure coded. See [Managing objects with information lifecycle management](#) for more information.

Review the rules in this policy. If this is a proposed policy, click Simulate to verify the policy and then click Activate to make the policy active.

**Reason for change:** Data Protection for Three Sites

*Rules are evaluated in order, starting from the top.*

Rule Name	Default	Tenant Account
Three-Site Erasure Coding for Tenant A 		Tenant A (49752734300032812036)
Three-Site Replication for Other Tenants 	✓	Ignore

When this new ILM policy is activated, objects belonging to Tenant A will be protected by 2+1 erasure coding at three sites, while objects belonging to other tenants (and smaller objects belonging to Tenant A) will be protected across three sites using 3-copy replication.

### Rule 1: Three-site erasure coding for Tenant A

Rule definition	Example value
Rule Name	Three-Site Erasure Coding for Tenant A
Tenant Account	Tenant A
Storage Pool	All 3 Data Centers (includes Data Center 1, Data Center 2, and Data Center 3)
Content Placement	2+1 erasure coding in All 3 Data Centers from day 0 to forever

### Rule 2: Three-site replication for other tenants

Rule definition	Example value
Rule Name	Three-Site Replication for Other Tenants
Tenant Account	Ignore
Storage Pools	Data Center 1, Data Center 2, and Data Center 3
Content Placement	Three replicated copies from day 0 to forever: one copy at Data Center 1, one copy at Data Center 2, and one copy at Data Center 3.

## Activating the proposed ILM policy for example 6

When you activate a new proposed ILM policy, existing objects might be moved to new locations or new object copies might be created for existing objects, based on the placement instructions in any new or updated rules.



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.

### What happens when erasure-coding instructions change

In the currently active ILM policy for this example, objects belonging to Tenant A are protected using 2+1 erasure coding at Data Center 1. In the new proposed ILM policy, objects belonging to Tenant A will be protected using 2+1 erasure coding at Data Centers 1, 2, and 3.

When the new ILM policy is activated, the following ILM operations occur:

- New objects ingested by Tenant A are split into two data fragments and one parity fragment is added. Then, each of the three fragments is stored at a different data center.
- The existing objects belonging to Tenant A are re-evaluated during the ongoing ILM scanning process. Because the ILM placement instructions use a new Erasure Coding profile, entirely new erasure-coded fragments are created and distributed to the three data centers.



The existing 2+1 fragments at Data Center 1 are not reused. StorageGRID considers each Erasure Coding profile to be unique and does not reuse erasure-coding fragments when a new profile is used.

### What happens when replication instructions change

In the currently active ILM policy for this example, objects belonging to other tenants are protected using two replicated copies in storage pools at Data Centers 1 and 2. In the new proposed ILM policy, objects belonging to other tenants will be protected using three replicated copies in storage pools at Data Centers 1, 2, and 3.

When the new ILM policy is activated, the following ILM operations occur:

- When any tenant other than Tenant A ingests a new object, StorageGRID creates three copies and saves one copy at each data center.
- Existing objects belonging to these other tenants are re-evaluated during the ongoing ILM scanning process. Because the existing object copies at Data Center 1 and Data Center 2 continue to satisfy the replication requirements of the new ILM rule, StorageGRID only needs to create one new copy of the object for Data Center 3.

### Performance impact of activating this policy

When the proposed ILM policy in this example is activated, the overall performance of this StorageGRID system will be temporarily affected. Higher than normal levels of grid resources will be required to create new erasure-coded fragments for Tenant A's existing objects and new replicated copies at Data Center 3 for other

tenants' existing objects.

As a result of the ILM policy change, client read and write requests might temporarily experience higher than normal latencies. Latencies will return to normal levels after the placement instructions are fully implemented across the grid.

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 are not moved unnecessarily.



Contact technical support if you need to slow or increase the rate at which objects are processed after an ILM policy change.

## Example 7: Compliant ILM policy for S3 Object Lock

You can use the S3 bucket, ILM rules, and ILM policy in this example as a starting point when defining an ILM policy to meet the object protection and retention requirements for objects in buckets with S3 Object Lock enabled.



If you used the legacy Compliance feature in previous StorageGRID releases, you can also use this example to help manage any existing buckets that have the legacy Compliance feature enabled.



The following ILM rules and policy are only examples. There are many ways to configure ILM rules. Before activating a new policy, simulate the proposed policy to confirm it will work as intended to protect content from loss.

### Related information

- [Manage objects with S3 Object Lock](#)
- [Create an ILM policy](#)

### Bucket and objects for S3 Object Lock example

In this example, an S3 tenant account named Bank of ABC has used the Tenant Manager to create a bucket with S3 Object Lock enabled to store critical bank records.

Bucket definition	Example value
Tenant Account Name	Bank of ABC
Bucket Name	bank-records
Bucket Region	us-east-1 (default)

# Buckets

Create buckets and manage bucket settings.

1 bucket

Create bucket

Actions

<input type="checkbox"/>	Name	S3 Object Lock	Region	Object Count	Space Used	Date Created
<input type="checkbox"/>	bank-records	✓	us-east-1	0	0 bytes	2021-01-06 16:53:19 MST

← Previous 1 Next →

Each object and object version that is added to the bank-records bucket will use the following values for retain-until-date and legal hold settings.

Setting for each object	Example value
retain-until-date	"2030-12-30T23:59:59Z" (December 30, 2030)  Each object version has its own retain-until-date setting. This setting can be increased, but not decreased.
legal hold	"OFF" (Not in effect)  A legal hold can be placed or lifted on any object version at any time during the retention period. If an object is under a legal hold, the object cannot be deleted even if the retain-until-date has been reached.

## ILM rule 1 for S3 Object Lock example: Erasure Coding profile with bucket matching

This example ILM rule applies only to the S3 tenant account named Bank of ABC. It matches any object in the bank-records bucket and then uses erasure coding to store the object on Storage Nodes at three data center sites using a 6+3 Erasure Coding profile. This rule satisfies the requirements of buckets with S3 Object Lock enabled: an erasure-coded copy is kept on Storage Nodes from day 0 to forever, using Ingest Time as the reference time.

Rule definition	Example value
Rule Name	Compliant Rule: EC objects in bank-records bucket - Bank of ABC
Tenant Account	Bank of ABC
Bucket Name	bank-records

Rule definition	Example value
Advanced filtering	Object Size (MB) greater than 1  <b>Note:</b> This filter ensures that erasure coding is not used for objects 1 MB or smaller.

#### Create ILM Rule Step 1 of 3: Define Basics

Name

Description

Tenant Accounts (optional)

Bucket Name

[Advanced filtering...](#) (0 defined)

Cancel

Next

Rule definition	Example value
Reference Time	Ingest Time
Placements	From day 0 store forever
Erasure Coding Profile	<ul style="list-style-type: none"> <li>• Create an erasure-coded copy on Storage Nodes at three data center sites</li> <li>• Uses 6+3 erasure-coding scheme</li> </ul>



## Edit ILM Rule Step 2 of 3: Define Placements

Configure placement instructions to specify how you want objects matched by this rule to be stored.

**Compliant Rule: EC objects in bank-record bucket - Bank of ABC**

Reference Time
Ingest Time

**Placements**
Sort by start day

From day 0 store forever
Add Remove

Type erasure coded Location Three Data Centers (6 plus 3) Copies 1
+ x

**Retention Diagram**
Refresh

Trigger
Day 0
Three Data Centers (6 plus 3)
Duration
Forever

Cancel Back Save

## ILM rule 2 for S3 Object Lock example: Non-compliant rule

This example ILM rule initially stores two replicated object copies on Storage Nodes. After one year, it stores one copy on a Cloud Storage Pool forever. Because this rule uses a Cloud Storage Pool, it is not compliant and will not apply to the objects in buckets with S3 Object Lock enabled.

Rule definition	Example value
Rule Name	Non-Compliant Rule: Use Cloud Storage Pool
Tenant Accounts	Not specified
Bucket Name	Not specified, but will only apply to buckets that do not have S3 Object Lock (or the legacy Compliance feature) enabled.
Advanced filtering	Not specified

## Create ILM Rule Step 1 of 3: Define Basics

Name
Non-Compliant Rule: Use Cloud Storage Pool

Description
DC1 and 2 for 1 year then move to CSP

Tenant Accounts (optional)
Select tenant accounts or enter tenant IDs

Bucket Name
matches all
Value

Advanced filtering... (0 defined)

Cancel Next

Rule definition	Example value
Reference Time	Ingest Time
Placements	<ul style="list-style-type: none"> <li>• On Day 0, keep two replicated copies on Storage Nodes in Data Center 1 and Data Center 2 for 365 days</li> <li>• After 1 year, keep one replicated copy in a Cloud Storage Pool forever</li> </ul>

## ILM rule 3 for S3 Object Lock example: Default rule

This example ILM rule copies object data to storage pools in two data centers. This compliant rule is designed to be the default rule in the ILM policy. It does not include any filters, does not use the Noncurrent reference time, and satisfies the requirements of buckets with S3 Object Lock enabled: two object copies are kept on Storage Nodes from day 0 to forever, using Ingest as the reference time.

Rule definition	Example value
Rule Name	Default Compliant Rule: Two Copies Two Data Centers
Tenant Account	Not specified
Bucket Name	Not specified
Advanced filtering	Not specified

### Create ILM Rule Step 1 of 3: Define Basics

Name

Description

Tenant Accounts (optional)

Bucket Name

[Advanced filtering...](#) (0 defined)

Cancel

Next

Rule definition	Example value
Reference Time	Ingest Time
Placements	From Day 0 to forever, keep two replicated copies—one on Storage Nodes in Data Center 1 and one on Storage Nodes in Data Center 2.

Compliant Rule: Two Copies Two Data Centers

Reference Time
Ingest Time

Placements
Sort by start day

From day 0 store forever
Add Remove

Type replicated Location Data Center 1 Data Center 2 Add Pool Copies 2
+

Specifying multiple storage pools might cause data to be stored at the same site if the pools overlap. See [Managing objects with information lifecycle management](#) for more information.

Retention Diagram
Refresh

Trigger
Day 0
Data Center 1
Data Center 2
Duration
Forever

## Compliant ILM policy for S3 Object Lock example

To create an ILM policy that will effectively protect all objects in your system, including those in buckets with S3 Object Lock enabled, you must select ILM rules that satisfy the storage requirements for all objects. Then, you must simulate and activate the proposed policy.

### Add rules to the policy

In this example, the ILM policy includes three ILM rules, in the following order:

1. A compliant rule that uses erasure coding to protect objects greater than 1 MB in a specific bucket with S3 Object Lock enabled. The objects are stored on Storage Nodes from day 0 to forever.
2. A non-compliant rule that creates two replicated object copies on Storage Nodes for a year and then moves one object copy to a Cloud Storage Pool forever. This rule does not apply to buckets with S3 Object Lock enabled because it uses a Cloud Storage Pool.
3. The default compliant rule that creates two replicated object copies on Storage Nodes from day 0 to forever.

## Configure ILM Policy

Create a proposed policy by selecting and arranging rules. Then, save the policy and edit it later as required. Click Simulate to verify a saved policy using test objects. When you are ready, click Activate to make this policy the active ILM policy for the grid.

Name

Reason for change

### Rules

1. Select the rules you want to add to the policy.
2. Determine the order in which the rules will be evaluated by dragging and dropping the rows. The default rule (and any non-compliant rule without a filter) will be automatically placed at the end of the policy and cannot be moved.

[+ Select Rules](#)

Default	Rule Name	Compliant	Tenant Account	Actions
	Compliant Rule: EC for bank-records bucket - Bank of ABC 	✓	Bank of ABC (90767802913525281639)	✕
	Non-Compliant Rule: Use Cloud Storage Pool 		Ignore	✕
✓	Default Compliant Rule: Two Copies Two Data Centers 	✓	Ignore	✕

Cancel

Save

## Simulate the proposed policy

After you have added rules in your proposed policy, chosen a default compliant rule, and arranged the other rules, you should simulate the policy by testing objects from the bucket with S3 Object Lock enabled and from other buckets. For example, when you simulate the example policy, you would expect test objects to be evaluated as follows:

- The first rule will only match test objects that are greater than 1 MB in the bucket bank-records for the Bank of ABC tenant.
- The second rule will match all objects in all non-compliant buckets for all other tenant accounts.
- The default rule will match these objects:
  - Objects 1 MB or smaller in the bucket bank-records for the Bank of ABC tenant.
  - Objects in any other bucket that has S3 Object Lock enabled for all other tenant accounts.

## Activate the policy

When you are completely satisfied that the new policy protects object data as expected, you can activate it.

## Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.