

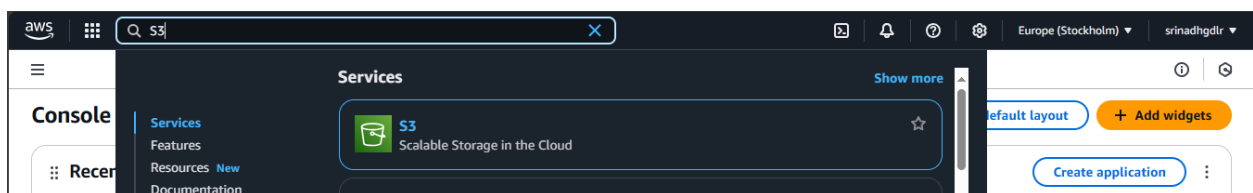
Project-Retrieving S3 Archives Using AWS Console

Tasks:

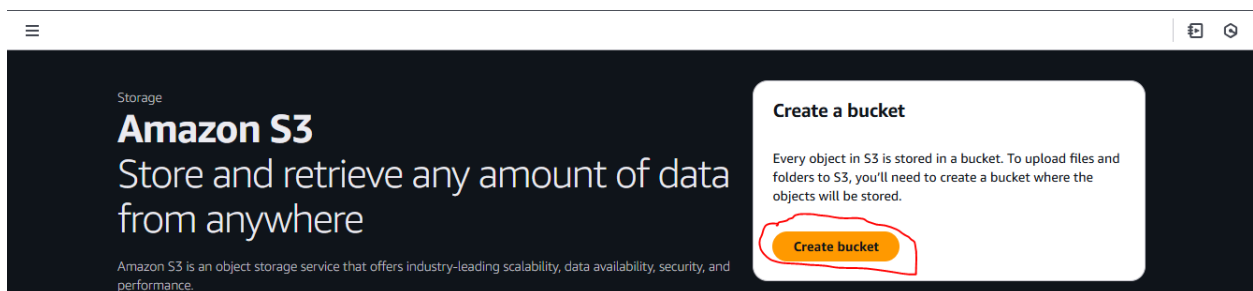
- * Create S3 bucket
- * Upload the object
- * Retrieve the data
- * Cleanup

Task1: Create S3 bucket

In the AWS Console search bar, search for S3



Choose S3 and click on Create bucket button



In the Create bucket window, Configure below settings.

-Enter a descriptive globally unique name for your bucket name: retrieve-s3-archives1

-The default Block Public Access setting is appropriate for this workload, so leave this section as is.

(Next, enable bucket versioning to protect your data from accidental or malicious user deletes or overwrites.)

-Bucket Versioning: Enable

(Now you have the option to enable S3 Object Lock in the Advanced settings section. With S3 Object Lock, you can store objects using a write-once-read-many (WORM) model. S3 Object Lock can help prevent objects from being deleted or overwritten for a fixed amount of time, or indefinitely. S3 Object Lock can be used to help meet regulatory requirements that require WORM storage, or to simply add another layer of protection against object changes and deletion. For this workload, it is appropriate to enable S3 Object Lock to ensure important archived data is not deleted prematurely by unauthorized users.)

-In the Advanced settings section Choose the Enable option and check the check box to acknowledge enabling the S3 Object Lock settings.

Then, select the Create bucket button.

Search

[Alt+S]

Europe (Stockholm)

srinadhgdlr

Amazon S3

Buckets

Create bucket

Create bucket [Info](#)

Buckets are containers for data stored in S3.

General configuration

AWS Region
Europe (Stockholm) eu-north-1

Bucket type [Info](#)

☒ **General purpose**
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

☐ **Directory**
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name [Info](#)

retrive-s3-archives

Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). [Learn More](#)

Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

Format: s3://bucket/prefix

Object Ownership [Info](#)

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

☒ **ACLs disabled (recommended)**
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

☐ **ACLs enabled**
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Object Ownership
Bucket owner enforced

Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

☒ **Block all public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- ☒ **Block public access to buckets and objects granted through new access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- ☒ **Block public access to buckets and objects granted through any access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.
- ☒ **Block public access to buckets and objects granted through new public bucket or access point policies**
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- ☒ **Block public and cross-account access to buckets and objects through any public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning

☐ Disable

☒ Enable

Tags - optional (2)

You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

Key	Value - optional	
dept	accounting	Remove
archive	true	Remove
Add tag		

Default encryption [Info](#)

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type [Info](#)

- ☒ Server-side encryption with Amazon S3 managed keys (SSE-S3)
- ☐ Server-side encryption with AWS Key Management Service keys (SSE-KMS)
- ☐ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see [DSSE-KMS pricing](#) on the [Storage](#) tab of the [Amazon S3 pricing page](#).

Bucket Key
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

- ☐ Disable
- ☒ Enable

▼ Advanced settings

Object Lock
Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. Object Lock works only in versioned buckets. [Learn more](#)

☐ Disable

☒ Enable
Permanently allows objects in this bucket to be locked. Additional Object Lock configuration is required in bucket details after bucket creation to protect objects in this bucket from being deleted or overwritten.

[Object Lock works only in versioned buckets. Enabling Object Lock automatically enables Versioning.](#)

Enabling Object Lock will permanently allow objects in this bucket to be locked
After you enable Object Lock for a bucket, you can't disable Object Lock or suspend Versioning for that bucket. [Learn more about Using Object Lock](#)

☒ I acknowledge that enabling Object Lock will permanently allow objects in this bucket to be locked.

[After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.](#)

[Cancel](#) [Create bucket](#)

[Amazon S3](#) > Buckets

Successfully created bucket "retrieve-s3-archives1"
To upload files and folders, or to configure additional bucket settings, choose [View details](#).

Additional configuration is required to protect objects in bucket "retrieve-s3-archives1" from being deleted or overwritten using Object Lock. To view Object Lock bucket settings, go to [bucket details](#).

Account snapshot - updated every 24 hours [All AWS Regions](#) [View Storage Lens dashboard](#)
Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. [Learn more](#)

[General purpose buckets](#) | [Directory buckets](#)

* Next, the S3 console will present a banner indicating the bucket creation was successful. The S3 console will also present a prompt informing you that additional configuration is needed to enable the S3 Object Lock feature. Select the bucket details link presented in the prompt. Making this selection will open the Properties tab for your newly created bucket.

* <Note: For this exercise, use Governance mode for the S3 Object Lock configuration. This will allow you to permanently delete your test object using an admin user after this tutorial has completed.>

Click on the S3 bucket

-On the bucket Properties tab, navigate to the Object Lock section and select the Edit button. Here you can set your default values for objects uploaded to your bucket. For this example, you want to enable

retention for all objects uploaded to this bucket for 2 years. Select Enable for the Default retention option, choose governance mode by selecting the Governance option under Default retention mode and enter '2' as the default retention period. Lastly, select Years for the unit of measure and then select the Save changes button.

Amazon S3 > Buckets

Account snapshot - updated every 24 hours

All AWS Regions

View Storage Lens dashboard

General purpose buckets

Directory buckets

General purpose buckets (1)

Info

All AWS Regions

Buckets are containers for data stored in S3.

Find buckets by name

< 1 >

☐

Name

▲

☐

retrive-s3-archives1

▲

AWS Region

▼

Europe (Stockholm) eu-north-1

☐

IAM Access Analyzer

▼

View analyzer for eu-north-1

☐

Creation date

▼

March 23, 2025, 14:47:31 (UTC+00:00)

Amazon S3 > Buckets > retrive-s3-archives1

retrive-s3-archives1

Info

Objects

Properties

Permissions

Metrics

Management

Access Points

Bucket overview

AWS Region

Europe (Stockholm) eu-north-1

Amazon Resource Name (ARN)

arn:aws:s3:::retrive-s3-archives1

Creation date

March 23, 2025, 14:47:31 (UTC+00:00)

Bucket Versioning

Edit

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning can't be suspended because Object Lock is enabled for this bucket.

Bucket Versioning

Enabled

Multi-factor authentication (MFA) delete

An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](#)

Disabled

Object Lock

Edit

Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. Object Lock works only in versioned buckets. [Learn more](#)

Object Lock

Enabled

Default retention

Automatically protect new objects put into this bucket from being deleted or overwritten.

Disabled

Edit Object Lock [Info](#)

Object Lock
Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. Object Lock works only in versioned buckets. [Learn more](#)

Once Amazon S3 Object Lock is enabled, you can't disable Object Lock or suspend Versioning for the bucket.

Object Lock
Enabled

Default retention
Automatically protect new objects put into this bucket from being deleted or overwritten.
☐ Disable
☒ Enable

Default retention mode
☒ Governance
Users with specific IAM permissions can overwrite or delete protected object versions during the retention period.
☐ Compliance
No users can overwrite or delete protected object versions during the retention period.

Default retention period
2
Must be a positive whole number.
Years

[Cancel](#) [Save changes](#)

Task2: Upload the object

- Now that your bucket has been created and configured, you are ready to upload archive data to the Amazon S3 IA storage classes.

— Object upload

- Navigate to the S3 console, From the list of available buckets, select the bucket name of the bucket retrieve-s3-archives1 you just created and click on it.

Amazon S3

[Account snapshot - updated every 24 hours](#) [View Storage Lens dashboard](#)

[General purpose buckets](#) | [Directory buckets](#)

General purpose buckets (1/1) [Info](#) [All AWS Regions](#)

Buckets are containers for data stored in S3.

[Copy ARN](#) [Empty](#) [Delete](#) [Create bucket](#)

Name	AWS Region	IAM Access Analyzer	Creation date
retrive-s3-archives1	Europe (Stockholm) eu-north-1	View analyzer for eu-north-1	March 23, 2025, 14:47:31 (UTC+00:00)

- Next, choose the Objects tab. Then from within the Objects section, select the Upload button.

Amazon S3 > Buckets > retrieve-s3-archives1

retrieve-s3-archives1 Info

Objects | Properties | Permissions | Metrics | Management | Access Points

Objects (0) [Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#) [Actions](#) [Create folder](#) [Upload](#)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

☐ Show versions < 1 > [Settings](#)

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
No objects You don't have any objects in this bucket.					

[Upload](#)

- Then, select the Add files button. Navigate your local file system to locate the archive file you would like to upload. Select the appropriate file and then select Open. Your file will be listed in the Files and folders section.

Amazon S3 > Buckets > retrieve-s3-archives1 > Upload

Upload Info

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDKs or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose [Add files](#) or [Add folder](#).

Files and folders (1 total, 2.5 KB) [Remove](#) [Add files](#) [Add folder](#)

All files and folders in this table will be uploaded.

< 1 >

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	AWS_key_Projets.txt	-	text/plain	2.5 KB

Destination Info

Destination
[s3://retrieve-s3-archives1](#)

► Destination details
Bucket settings that impact new objects stored in the specified destination.

► Permissions
Grant public access and access to other AWS accounts.

► Properties
Specify storage class, encryption settings, tags, and more.

- Expand the Properties section, select the S3 storage class you would like to upload your archive to. Select Standard IA and click on Upload button.

▼ Properties

Specify storage class, encryption settings, tags, and more.

Storage class [Info](#)

Amazon S3 offers a range of storage classes designed for different use cases. [Learn more](#) or see [Amazon S3 pricing](#).

	Storage class	Designed for	Bucket type	Availability Zones	Min storage duration	Min billable object size	Monitoring and auto-tiering fees	Retrieval fees
<input type="radio"/>	Standard	Frequently accessed data (more than once a month) with milliseconds access	General purpose	≥ 3	-	-	-	-
<input type="radio"/>	Intelligent-Tiering	Data with changing or unknown access patterns	General purpose	≥ 3	-	-	Per-object fees apply for objects ≥ 128 KB	-
<input type="radio"/>	Standard-IA	Infrequently accessed data (once a month) with milliseconds access	General purpose	≥ 3	30 days	128 KB	-	Per-GB fees apply
<input type="radio"/>	One Zone-IA	Recreateable, infrequently accessed data (once a month) with milliseconds access	General purpose or directory	1	30 days	128 KB	-	Per-GB fees apply
<input type="radio"/>	Glacier Instant Retrieval	Long-lived archive data accessed once a quarter with instant retrieval in milliseconds	General purpose	≥ 3	90 days	128 KB	-	Per-GB fees apply
<input checked="" type="radio"/>	Glacier Flexible Retrieval (formerly Glacier)	Long-lived archive data accessed once a year with retrieval of minutes to hours	General purpose	≥ 3	90 days	-	-	Per-GB fees apply
<input type="radio"/>	Glacier Deep Archive	Long-lived archive data accessed less than once a year with retrieval of hours	General purpose	≥ 3	180 days	-	-	Per-GB fees apply

- After your file upload operations have completed, you will be presented with a summary of the operations indicating if it has completed successfully or if it has failed. In this case, the file has uploaded successfully. Select the Close button.

Upload succeeded
For more information, see the [Files and folders](#) table.

Upload: status Close

After you navigate away from this page, the following information is no longer available.

Summary

Destination
s3://retrive-s3-archives1

Succeeded

1 file, 2.5 KB (100.00%)

Failed

0 files, 0 B (0%)

Files and folders

Configuration

Files and folders (1 total, 2.5 KB)

Find by name

< 1 >

Name	Folder	Type	Size	Status	Error
AWS_key_Projctcs.txt	-	text/plain	2.5 KB	Succeeded	-

Amazon S3

Buckets

retrive-s3-archives1

retrive-s3-archives1 [Info](#)

Objects

Properties

Permissions

Metrics

Management

Access Points

Objects (1)

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Find objects by prefix

Show versions

< 1 >

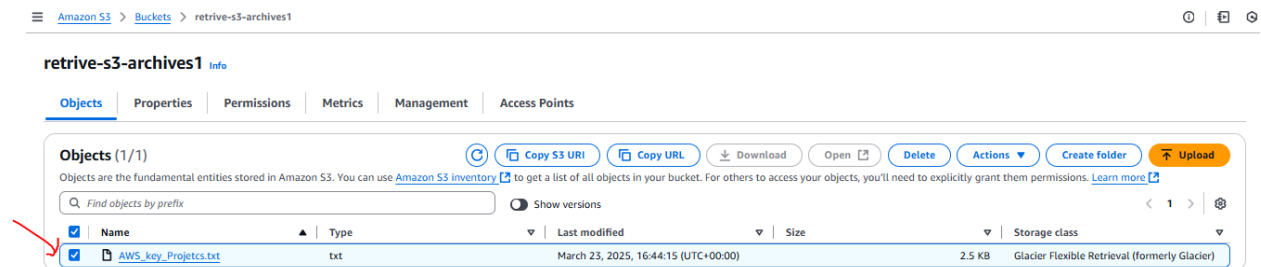
Name	Type	Last modified	Size	Storage class
AWS_key_Projctcs.txt	txt	March 23, 2025, 16:44:15 (UTC+00:00)	2.5 KB	Glacier Flexible Retrieval (formerly Glacier)

Task3: Retrieve the data

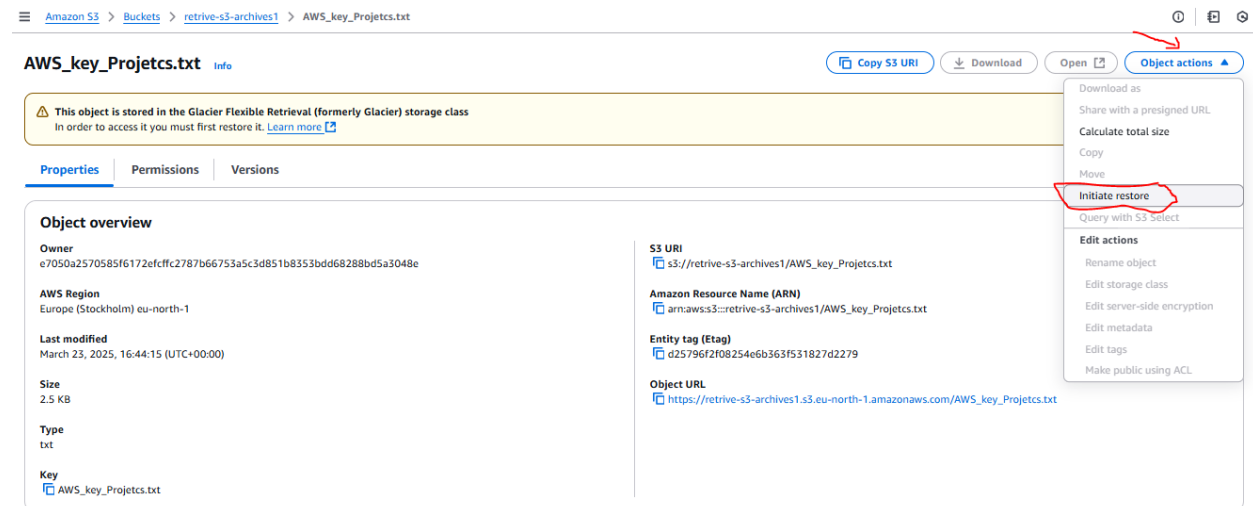
Now that you have successfully uploaded your data to Glacier Flexible Retrieval, let's go over the process of restoring your data.

--Initiate object restore

- Navigate to the S3 console, From the list of available buckets, select the bucket name of the bucket you have created. From the Objects menu, select the name of the test file you just uploaded.



- After selecting your test file's name, you will be presented with a banner indicating that your object is stored in the Glacier Flexible Retrieval storage class and that you need to restore it if you would like to access your data. You can initiate the restore process by simply selecting the Initiate restore button attached to the information banner, or you can choose Initiate restore from the Object actions menu.



o From the Initiate restore page, you will define the number of days you desire to make your restored copy available. Next, you will have a choice between standard or bulk retrieval. For this exercise, choose the Standard retrieval option. Then, select the Initiate restore button to continue.

Initiate restore

Info

To restore objects you must first initiate a restore request, and then wait until the objects are available. Retrieval fees apply. [Learn more](#) or [see pricing](#)

Restore objects from Glacier Flexible Retrieval (formerly Glacier)

When the restore request is initiated, temporary copies of the objects will be available for the number of days you specify in the requests. Retrieval fees apply. [Learn more](#) or [see pricing](#)

Number of days that the restored copy is available

The restored copy is automatically deleted after a specified number of days.

3

Number of days must be a positive integer.

The restored copy will be available until approximately 03-26-2025.

Retrieval tier

☐ Bulk retrieval

Typically within 5-12 hours.

☒ Standard retrieval

Typically within 3-5 hours.

☐ Expedited retrieval

Typically within 1-5 minutes when retrieving less than 250 MB.

Specified objects

Find objects by name

Name	Type	Last modified	Size	Storage class	Intelligent-Tiering Access
AWS_key_Projctcs.txt	txt	March 23, 2025, 16:44:15 (UTC+00:00)	2.5 KB	Glacier Flexible Retrieval (formerly Glacier)	-

Cancel

Initiate restore

o A summary page will be displayed indicating if the restore request was successful or if any errors occurred. In this case, the restore request was successful. Select the Close button to continue.

Successfully initiated restore

View details below.

×

Initiate restore: status

Info

Close

After you navigate away from this page, the following information is no longer available.

Summary

Source

s3://retrive-s3-archives1

Successful restore requests

1 object, 2.5 KB

Failed restore requests

0 objects

Failed restore requests

Configuration

Failed restore requests (0)

Find objects by name

Name	Folder	Type	Last modified	Size	Error
No failed restore requests					

AWS_key_Projctcs.txt

Info

Copy S3 URI

Download

Open

Object actions

This object is stored in the Glacier Flexible Retrieval (formerly Glacier) storage class

In order to access it you must first restore it. [Learn more](#)

Restoration in progress

To upgrade the speed of your restoration while it is in progress choose "Upgrade retrieval tier". Learn more about [restoring archived objects](#)

Upgrade retrieval tier

Restoration status

In-progress

Restoration started date

March 23, 2025, 16:54:25 (UTC+00:00)

Retrieval tier

Typically within 3-5 hours.

Standard retrieval

Properties

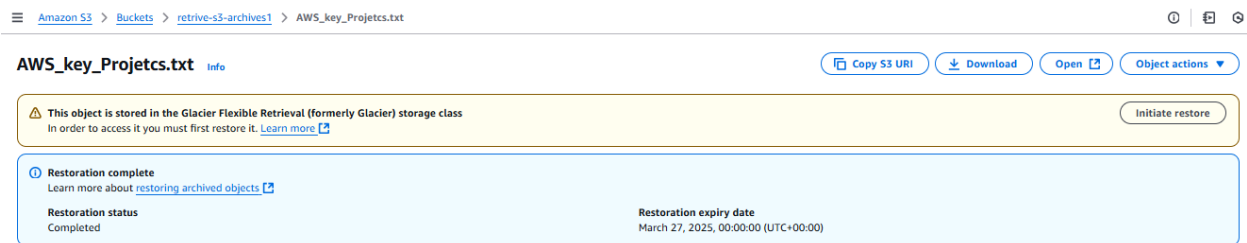
Permissions

Versions

- Verify restore has completed

* Now you can verify that your object has been restored. After waiting about 3-5 hours for the restore operation to complete, go ahead and log back into your S3 console. Select the file name of the object you have attempted to restore to see its current status.

* Here you can see that the object's Restore status is listed as Completed. The Restoration expiry date, which is based on the number of days we defined in the restore process, is listed as well. You have successfully restored your archived object. This object will be available until the time specified in the Restoration expiry date section. You can now perform actions like run S3 select queries against this file, copy the object to another bucket in your account or to another account, or download the data to your local machine.



Task4: Cleanup

- In the following steps, you clean up the resources you created in this project. It is a best practice to delete resources that you are no longer using so that you do not incur unintended charges.

Delete test object

- Navigate to the S3 console and select the Buckets menu option. First you will need to delete the test object from your bucket. Select the name of the bucket you have been working with for this project. Put a check mark in the checkbox to the left of your test object name, then select the Delete button. On the Delete objects page, verify that you have selected the proper object to delete and type "permanently delete" into the Permanently delete objects confirmation box. Then, select the Delete object button to continue. Next, you will be presented with a banner indicating if the deletion has been successful.

Delete test bucket

- Finally, you need to delete the test bucket you have created. Return to the list of buckets in your account. Select the radio button to the left of the bucket you created for this project, and then select the Delete button. Review the warning message. If you desire to continue deletion of this bucket, type the bucket name into the Delete bucket confirmation box and select Delete bucket.