

Hands-on tutorials

# Getting started using the Amazon S3 Glacier storage classes



# Getting started using the Amazon S3 Glacier storage classes: Hands-on tutorials

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

# Table of Contents

**Getting started using the Amazon S3 Glacier storage classes .....****i**

Overview ..... 1

What you'll accomplish ..... 2

Implementation ..... 2

Congratulations! ..... 18

# Getting started using the Amazon S3 Glacier storage classes

<b>AWS experience</b>	Beginner
<b>Time to complete</b>	20 minutes
<b>Cost to complete</b>	Less than \$1 ( <a href="#">Amazon S3 pricing page</a> )
<b>Services used</b>	<a href="#">Amazon S3</a>

## Overview

The [Amazon S3 Glacier storage classes](#) are purpose-built for data archiving, providing you with the highest performance, most retrieval flexibility, and the lowest cost archive storage in the cloud. To keep costs low yet suitable for varying retrieval needs, these storage classes support flexible retrieval options from milliseconds to several hours. The purpose of this tutorial is to show you how easy it is to begin storing your archive datasets in the Amazon S3 Glacier storage classes.

You can choose from three archive storage classes optimized for different access patterns and storage duration. For archive data that needs immediate access, choose the [Amazon S3 Glacier Instant Retrieval](#) storage class, an archive storage class that delivers the lowest cost storage with milliseconds retrieval. For archive data that does not require immediate access but needs the flexibility to retrieve large sets of data at no cost, choose Amazon S3 Glacier Flexible Retrieval (formerly S3 Glacier), with retrieval in minutes or free bulk retrievals in 5-12 hours. To save even more on long-lived archive storage, choose Amazon S3 Glacier Deep Archive, the lowest cost storage in the cloud with data retrieval within twelve hours.

By archiving on AWS you'll have access to very low cost cloud storage, you'll be able to digitally preserve and retain your data for the long term, and you'll be able to leverage comprehensive security and compliance capabilities. The Amazon S3 Glacier storage classes are used by customers for their long-term enterprise archive data, media archives, backup data, and data lake archives.

Use the [S3 console](#) and S3 API to easily archive your data in [Amazon S3](#). The S3 console and S3 API allow you to access all the features and functionality that the Amazon S3 service

provides. Follow this tutorial to begin using the S3 console to store your archive datasets in the Amazon S3 Glacier storage classes.

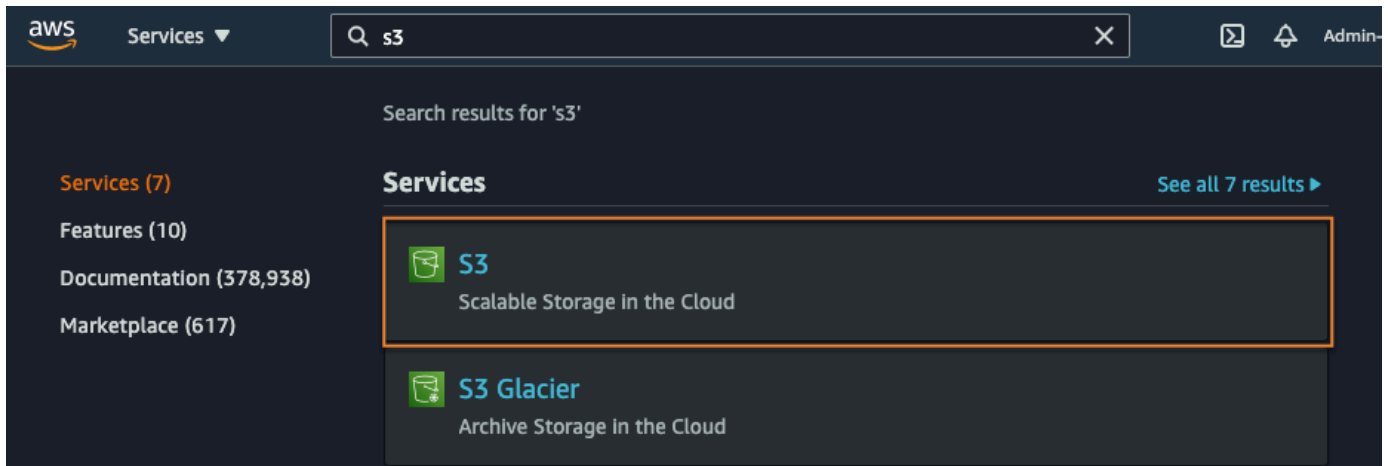
## What you'll accomplish

- Create an Amazon S3 bucket
- Upload objects to the Amazon S3 Glacier storage classes
- Restore your objects stored in the Amazon S3 Glacier Flexible Retrieval or S3 Glacier Deep Archive storage classes

## Implementation

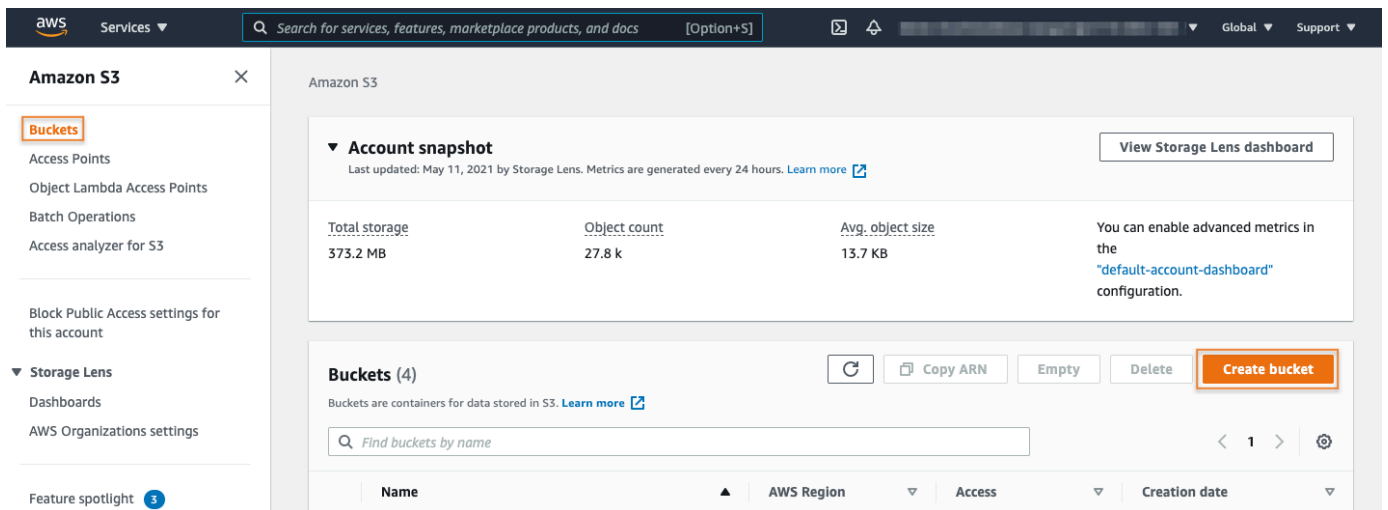
### Step 1: Getting started using the Amazon S3 Glacier storage classes

1. Sign into the Amazon S3 console
  - If you have not already done so, create an AWS account. [Access this support page for more information on how to create and activate a new AWS account.](#)
  - Log into the [AWS Management Console](#) using your account information.
  - From the AWS console services search bar, enter '**S3**'. Under the services search results section, select **S3**. You may notice an option for S3 Glacier. This option is for the Glacier service prior to integration with Amazon S3. We recommend all new S3 Glacier users use the S3 console.



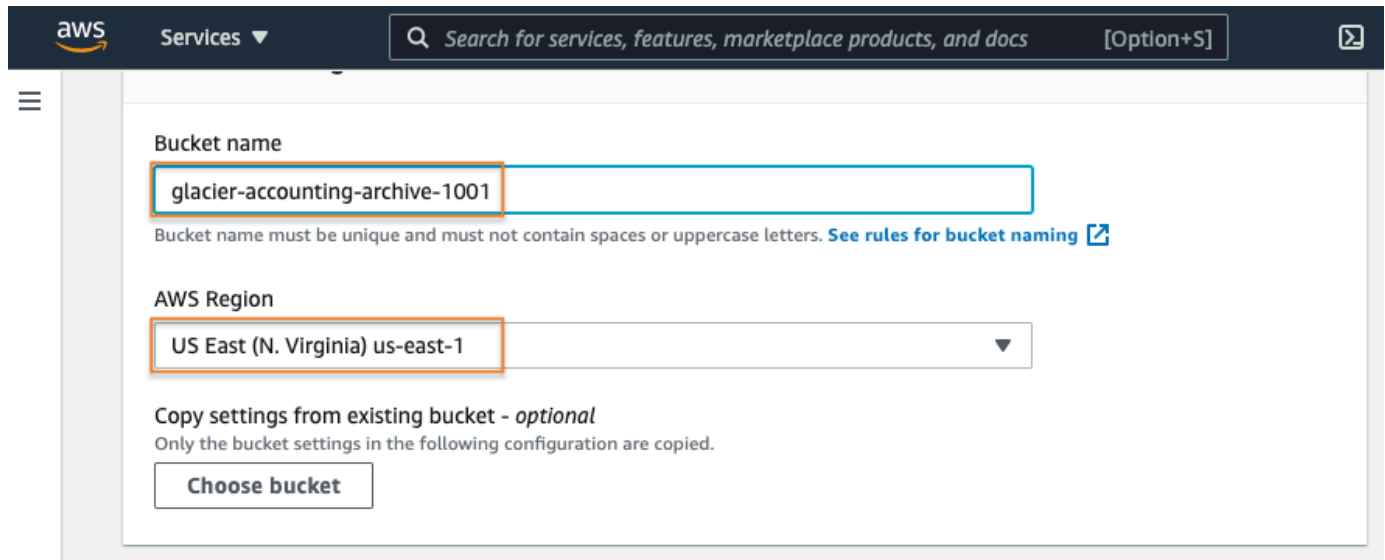
## 2. Create an S3 bucket

Choose **Buckets** from the S3 menu on the left rail and then select the **Create bucket** button.



## 3. Configure the bucket

- Enter a descriptive globally unique name for your bucket.
- Select which AWS Region you would like your bucket created in.
- The default Block Public Access setting is appropriate for this workload, so leave this section as is.



The screenshot shows the AWS S3 console interface for creating a new bucket. The top navigation bar includes the AWS logo, a 'Services' dropdown, a search bar with the placeholder text 'Search for services, features, marketplace products, and docs', and a keyboard shortcut '[Option+S]'. On the left, there is a hamburger menu icon. The main content area is titled 'Bucket name' and contains a text input field with the value 'glacier-accounting-archive-1001'. Below the input field, a note states: 'Bucket name must be unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)'. Below this, the 'AWS Region' is shown as a dropdown menu with 'US East (N. Virginia) us-east-1' selected. Further down, there is a section titled 'Copy settings from existing bucket - optional' with the subtext 'Only the bucket settings in the following configuration are copied.' and a button labeled 'Choose bucket'.

#### 4. Enable versioning

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

[Read more about bucket versioning here.](#) Then, add some tags to help track costs associated with our archive data over time.

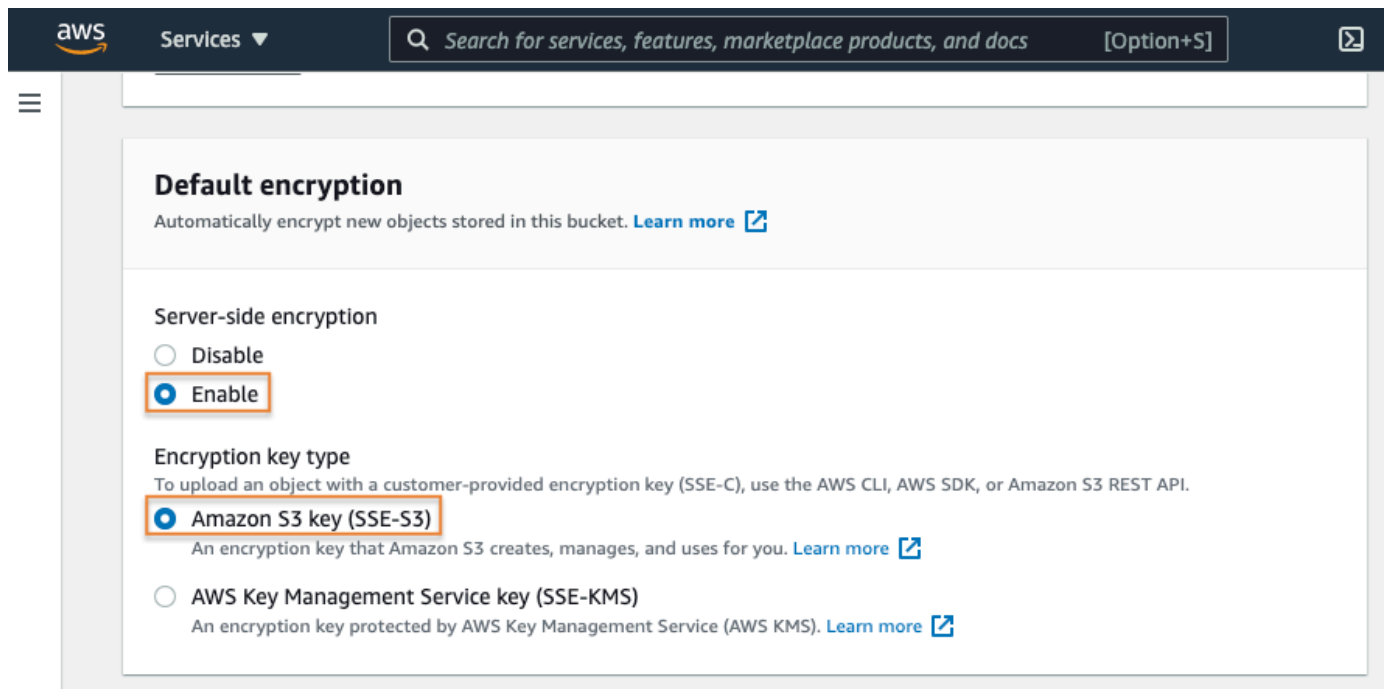
[You can find more information about S3 bucket cost allocation tagging here.](#)

The screenshot shows the Amazon S3 console interface. At the top, there's a navigation bar with the AWS logo, a 'Services' dropdown, a search bar with the placeholder 'Search for services, features, marketplace products, and docs', and a keyboard shortcut '[Option+S]'. Below the navigation bar, on the left, is a hamburger menu icon. The main content area is divided into two sections. The first section is titled 'Bucket Versioning' and includes a descriptive paragraph: '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](#)'. Below this, there are two radio buttons: 'Disable' and 'Enable'. The 'Enable' radio button is selected and highlighted with an orange box. The second section is titled 'Tags (2) - optional' and includes a descriptive paragraph: 'Track storage cost or other criteria by tagging your bucket. [Learn more](#)'. Below this, there is a table-like structure for tags. It has two columns: 'Key' and 'Value - optional'. The first row has 'dept' in the 'Key' column and 'accounting' in the 'Value' column, with a 'Remove' button to the right. The second row has 'archive' in the 'Key' column and 'true' in the 'Value' column, also with a 'Remove' button to the right. Both 'dept' and 'archive' in the 'Key' column are highlighted with orange boxes. At the bottom left of the tag section is an 'Add tag' button.

## 5. Enable default encryption

Next, you have the option of enabling default 'at-rest' encryption for the bucket. The settings here will apply to any objects uploaded to the bucket where you have not defined at-rest encryption details during the upload process.

For this example, enable server-side encryption leveraging S3 service managed keys (SSE-S3). If your workload requirements are not satisfied by SSE-S3, you can also leverage AWS Key Management Service (KMS). [More information about Amazon S3 and AWS KMS can be found here.](#)



## 6. Enable S3 Object Lock

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.

- Choose **Enable**.
- Select the check box to acknowledge enabling the S3 Object Lock settings
- Select the **Create bucket** button.

aws Services ▾ Search for services, features, marketplace products, and docs [Option+S]

An encryption key protected by AWS Key Management Service (AWS KMS). [Learn more](#)

### ▼ 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. [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 Bucket Versioning.**

**⚠ Enabling Object Lock will permanently allow objects in this bucket to be locked**

Enable Object Lock only if you need to prevent objects from being deleted to have data integrity and regulatory compliance. After you enable this feature, anyone with the appropriate permissions can put immutable objects in the bucket. You might be blocked from deleting the objects and the bucket. Additional Object Lock configuration is required in bucket details after bucket creation to protect objects in this bucket from being deleted or overwritten. [Learn more](#)

☒ 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**

## 7. Configure S3 Object Lock

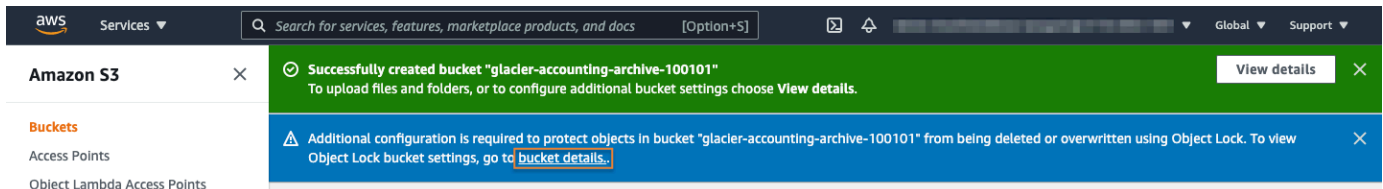
Next, the S3 console will present a banner indicating the bucket creation was successful. The S3 console will also present a prompt informing you that additional configuration is needed to enable the S3 Object Lock feature.

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.

For more information about S3 Object Lock, read the blog featuring "[Protecting data with Amazon S3 Object Lock](#)."



## 8. Edit the S3 Object Lock

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 5 years. Select **Enable** for the **Default retention** option, choose governance mode by selecting the **Governance** option under **Default retention mode** and enter **5** as the default retention period.

Lastly, select **Years** for the unit of measure and then select the **Save changes** button.

**Amazon S3** ×

**Buckets**

- Access Points
- Object Lambda Access Points
- Batch Operations
- Access analyzer for S3

Block Public Access settings for this account

▼ **Storage Lens**

- Dashboards
- AWS Organizations settings

Feature spotlight 5

► AWS Marketplace for S3

## Edit Object Lock

**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. [Learn more](#)

ⓘ Once Amazon S3 Object Lock is enabled, you can't disable Object Lock or suspend Bucket 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**  
   
Must be a positive whole number.

Cancel **Save changes**

## Step 2: Uploading data to an Amazon S3 bucket

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

### 1. Select the bucket

If you have logged out of your AWS Management Console session, log back in.

Navigate to the [S3 console](#) and select the **Buckets** menu option.

From the list of available buckets, select the bucket name of the bucket you just created.

The screenshot shows the Amazon S3 console interface. On the left, the 'Buckets' tab is selected in the navigation pane. The main content area displays the 'Account snapshot' and a list of buckets. The bucket 'glacier-accounting-archive-100101' is highlighted with an orange box.

Total storage	Object count	Avg. object size
373.9 MB	28.6 k	13.4 KB

Name	AWS Region
cloudtrail-awslogs-411020521031-jvuc6dah-isengard-do-not-delete	US East (N. Virginia) us-east-1
do-not-delete-gatedgarden-audit-411020521031	US West (Oregon) us-west-2
eab-testdata-prod1a	US East (N. Virginia) us-east-1
<b>glacier-accounting-archive-100101</b>	US East (N. Virginia) us-east-1
prod-datalake-8123	US East (N. Virginia) us-east-1

## 2. Start the upload

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

The screenshot shows the Amazon S3 console interface for the bucket 'glacier-accounting-archive-100101'. The 'Objects' tab is selected. The 'Upload' button is highlighted with an orange box.

**Objects (0)**

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](#)

Copy URL Open Download Delete Actions Create folder **Upload**

Find objects by prefix Show versions

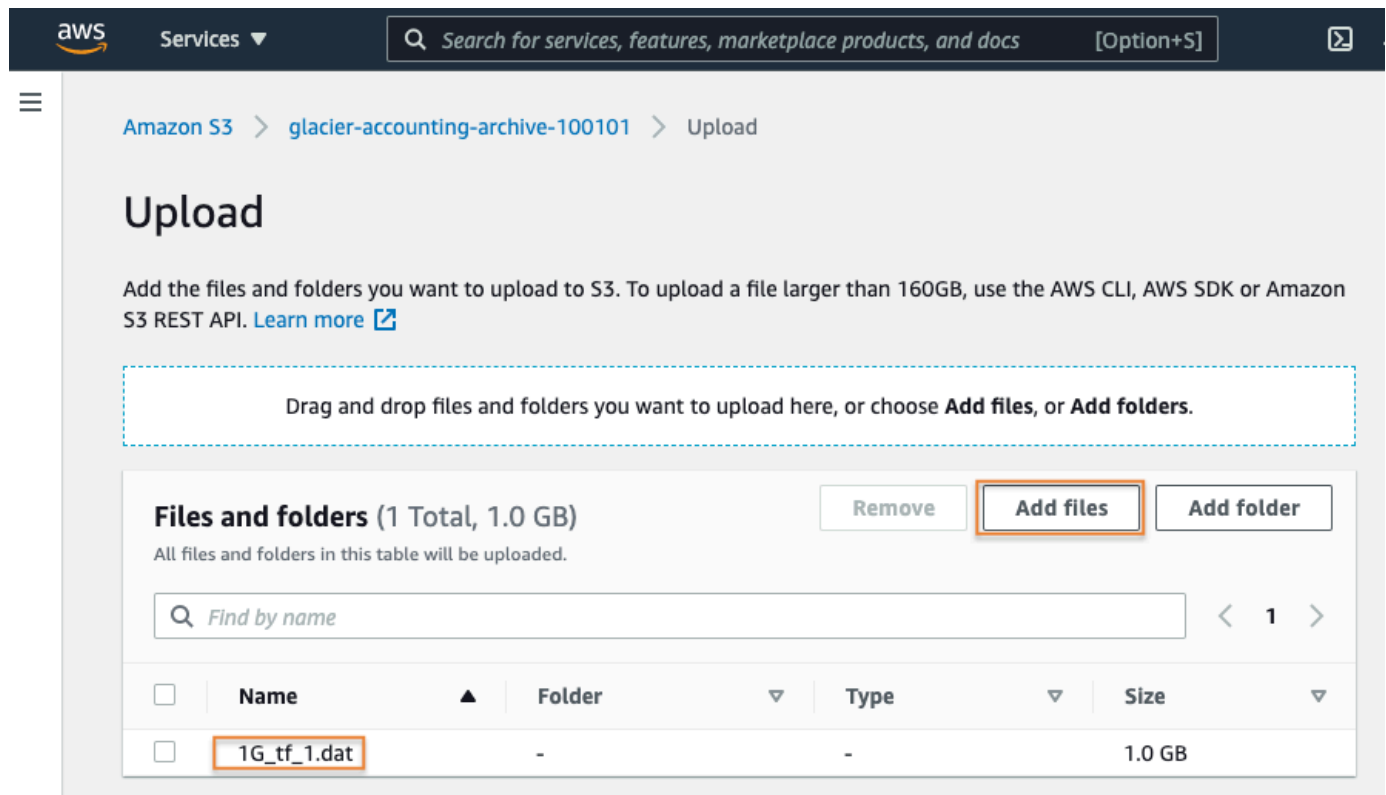
## 3. Select the file to upload

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.



#### 4. Select the storage class

In the **Properties** section, select the S3 storage class you would like to upload your archive to.

Select **Glacier Deep Archive**, as the example dataset needs to be retained for 5 years and there is a low probability the data will be accessed often.

#### **Note**

If your workload requires milliseconds access and single API call access to your archived data, the S3 Glacier Instant Retrieval storage class should be selected here instead. More information about the Amazon S3 Glacier storage class options can be viewed [here](#).

Leave the rest of the options on the default settings and select the **Upload** button.

**Note**

Objects stored in many S3 storage classes have minimum object durations associated with them. In this case, uploading the test file to Glacier Deep Archive will result in 180 days of billing even if it is deleted early. Storing 1 GB in S3 Glacier Deep Archive for 180 days with the retrieval is ~\$0.03. [You can read more about S3 pricing here.](#)

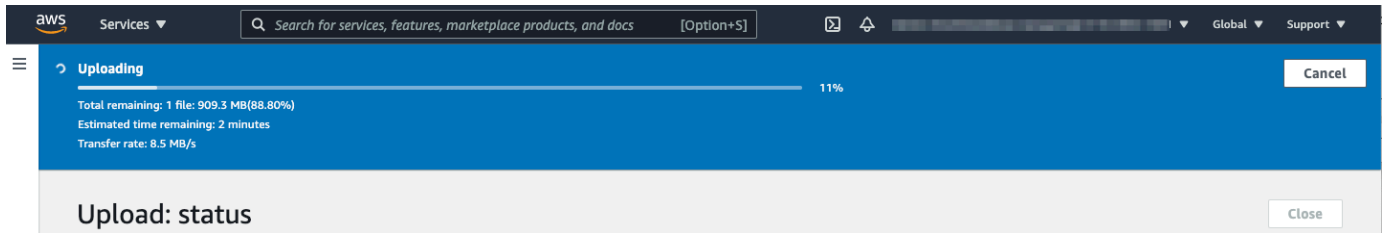
**Storage class**

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

	Storage class	Designed for	Availability Zones	Min storage duration	Minimum object size
<input type="radio"/>	Standard	Frequently accessed data (more than once a month) with milliseconds access	≥ 3	-	-
<input type="radio"/>	Intelligent-Tiering	Data with changing or unknown access patterns	≥ 3	-	-
<input type="radio"/>	Standard-IA	Infrequently accessed data (once a month) with milliseconds access	≥ 3	30 days	1
<input type="radio"/>	One Zone-IA	Recreatable, infrequently accessed data (once a month) stored in a single Availability Zone with milliseconds access	1	30 days	1
<input type="radio"/>	Glacier Instant Retrieval	Long-lived archive data accessed once a quarter with instant retrieval in milliseconds	≥ 3	90 days	1
<input type="radio"/>	Glacier Flexible Retrieval (formerly Glacier)	Long-lived archive data accessed once a year with retrieval of minutes to hours	≥ 3	90 days	-
<input checked="" type="radio"/>	Glacier Deep Archive	Long-lived archive data accessed less than once a year with retrieval of hours	≥ 3	180 days	-
<input type="radio"/>	Reduced redundancy	Noncritical, frequently accessed data with milliseconds access (not recommended as S3 Standard is more cost effective)	≥ 3	-	-

**5. Review the status**

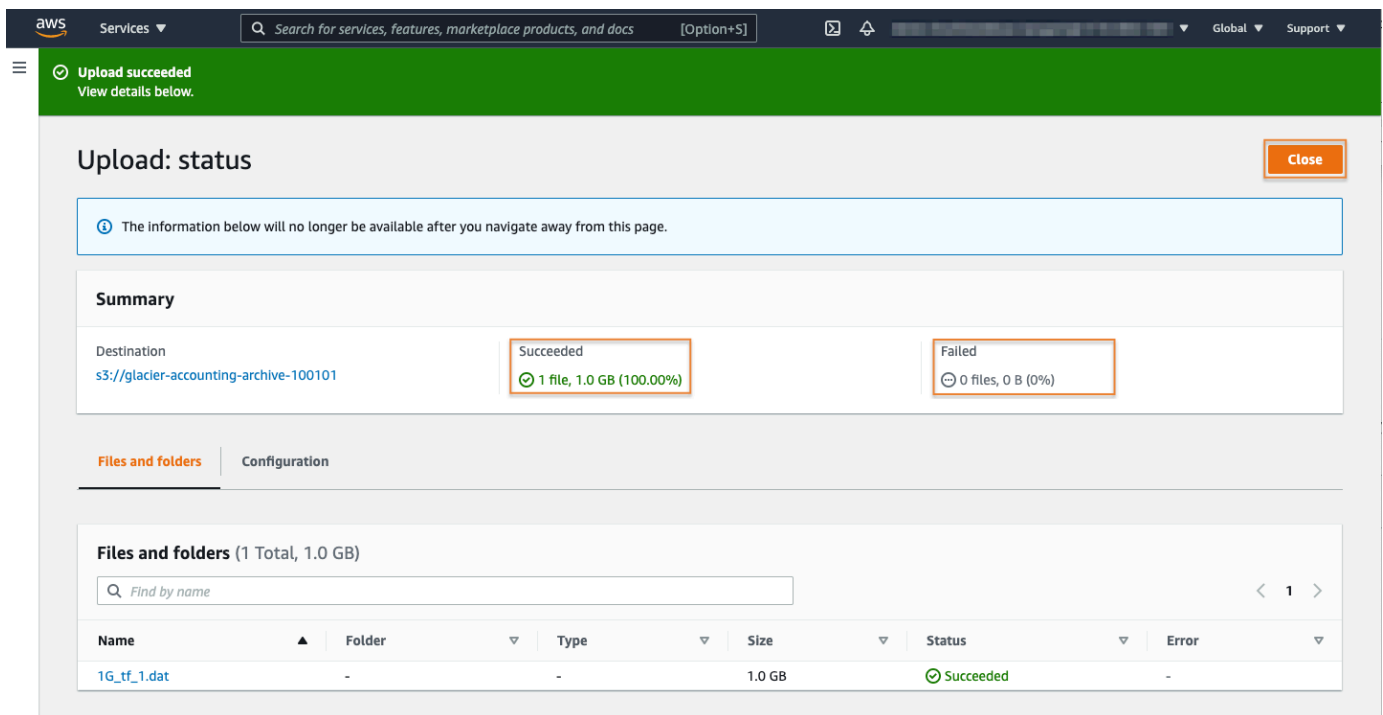
A banner will be displayed providing you with details of the file's upload status.



## 6. Confirm the upload completed

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.



## Step 3: Restore your data

Now that you have successfully uploaded your data to S3 Glacier Deep Archive, let's go over the process of restoring your data.

**Note**

the process of restoring your data before it can be accessed, is required for data that is stored in the S3 Glacier Flexible Retrieval and S3 Glacier Deep Archive storage classes. Data stored in the S3 Glacier Instant Retrieval storage class does not require this restore request prior to being accessed. You can learn more about S3 Glacier Instant Retrieval [here](#).

## 1. Select the object to restore

If you have logged out of your AWS Management Console session, log back in.

- Navigate to the [S3 console](#) and select the **Buckets** menu option.
- From the list of available buckets, select the bucket name of the bucket you have created for this exercise.
- From the **Objects** menu, select the name of the test file you just uploaded.

The screenshot shows the Amazon S3 console interface. On the left, the 'Buckets' menu is highlighted. The main area displays the bucket 'glacier-accounting-archive-100101'. The 'Objects' tab is selected, showing a list of objects. The object '1G\_tf\_1.dat' is highlighted in the list. The object details show it is a 'dat' file, 1.0 GB in size, and stored in the 'Glacier Deep Archive' storage class. The 'Last modified' date is May 12, 2021, 09:32:33 (UTC-04:00).

Name	Type	Last modified	Size	Storage class
1G_tf_1.dat	dat	May 12, 2021, 09:32:33 (UTC-04:00)	1.0 GB	Glacier Deep Archive

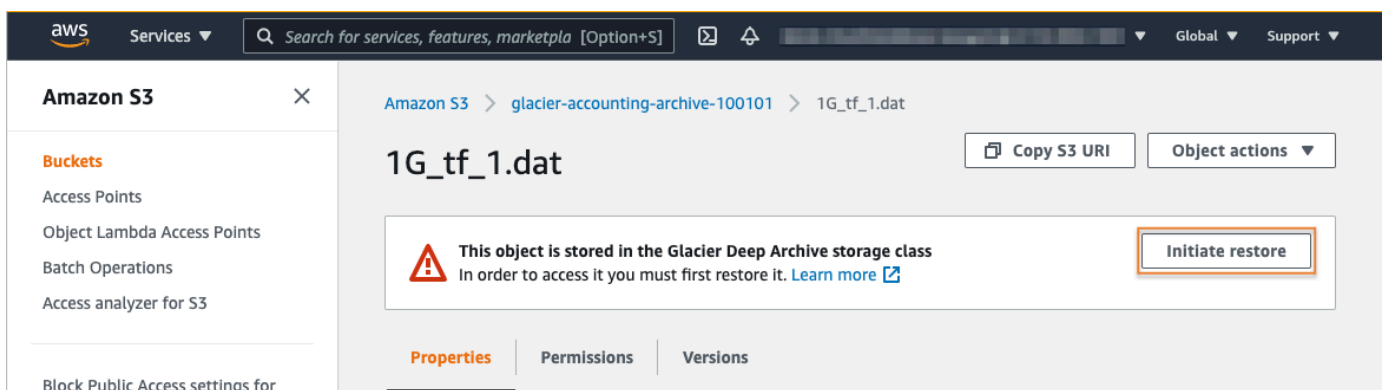
## 2. Initiate the restore

After selecting your test file's name, you will be presented with a banner indicating that your object is stored in the S3 Glacier Deep Archive 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.

### Note

The restore process will create a copy of your archived data and will store that copy in the S3 Standard storage class. During the restore initiation process you will set the number of days that you wish to have your data available. During this time period, you will incur applicable storage charges for your data in both the archive storage class as well as in the active storage class.



### 3. Configure the restore

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. Data stored in the Amazon S3 Glacier Flexible Retrieval storage class will additionally have an option to select expedited retrieval. [More information about restore options can be found here.](#)

For this exercise, choose the **Standard retrieval** option. Then, select the **Initiate restore** button to continue.

**Amazon S3** ×

Amazon S3 > glacier-accounting-archive-100101 > Initiate restore

## Initiate restore

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 Deep Archive

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.

5

Number of days must be a positive integer.

*The restored copy will be available until approximately 05-31-2021.*

**Retrieval tier**

☐ Bulk retrieval  
Typically within 48 hours.

☒ **Standard retrieval**  
Typically within 12 hours.

### Specified objects

Find objects by name

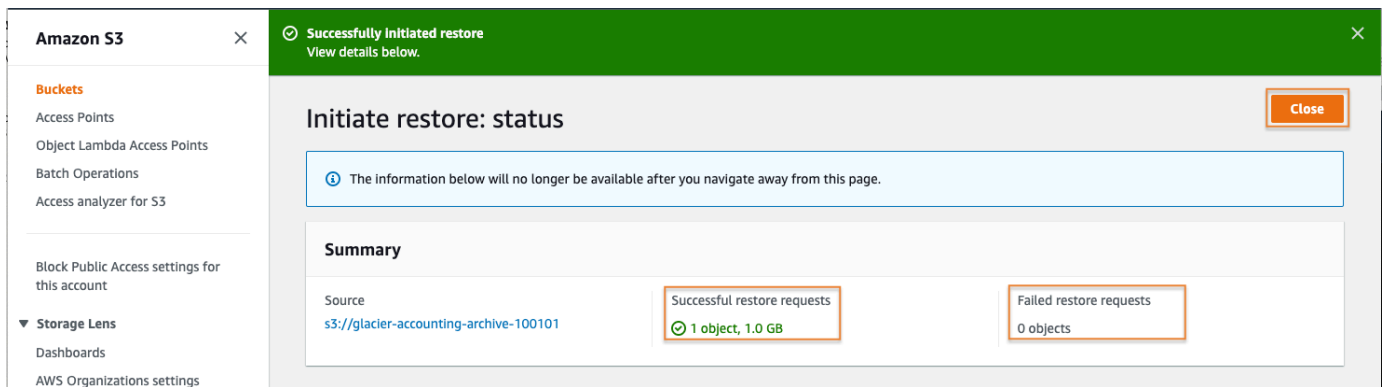
Name	Version ID	Type	Last modified	Size	Storage class	Intelligent-Tiering Access
1G_tf_1.dat	-	dat	May 12, 2021, 09:32:33 (UTC-04:00)	1.0 GB	Glacier Deep Archive	-

Cancel **Initiate restore**

#### 4. Wait for the restore to complete

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.

For this standard restore from S3 Glacier Deep Archive, you will need to wait about 12 hours for the temporary object to be restored to the Amazon S3 Standard-IA storage class. S3 Event notifications support alerting when an object restore event has completed. [More information about S3 Event notifications can be found in the Amazon S3 documentation here.](#)



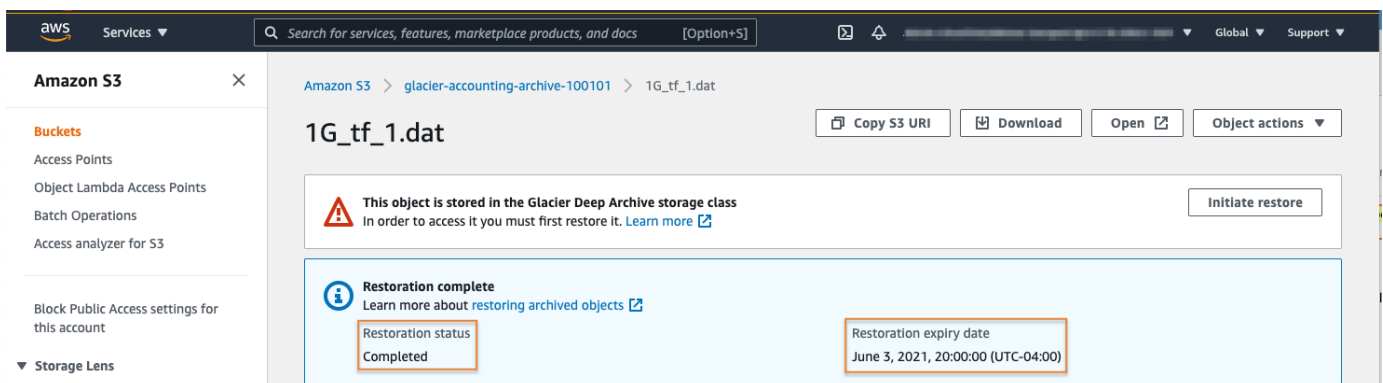
## 5. Verify restore has completed

Now you can verify that your object has been restored. After waiting about twelve hours for the restore operation to complete, log back into your [S3 console](#).

Select **Buckets** from the left rail menu, and select the name of your bucket to view its contents. From the **Objects** section, 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.



## Clean up resources

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

1. Delete your test object
  - a. If you have logged out of your AWS Management Console session, log back in.
  - b. Navigate to the [S3 console](#) and select the **Buckets** menu option.
  - c. First you will need to delete the test object from your test bucket. Select the **name** of the bucket you have been working with for this tutorial.
  - d. Put a check mark in the checkbox to the left of your test object name, then select the **Delete** button.
  - e. 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.
  - f. Then, select the **Delete object** button to continue. Next, you will be presented with a banner indicating if the deletion has been successful.
2. Delete your test bucket
  - a. Finally, you need to delete the test bucket you have created. Return to the list of buckets in your account.
  - b. Select the radio button to the left of the bucket you created for this tutorial, and then select the **Delete** button.
  - c. 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**.

## Congratulations!

You have learned how to create an Amazon S3 bucket, upload objects to the Amazon S3 Glacier and S3 Glacier Deep Archive storage classes, and how to restore your objects so that they can be easily retrieved.