

Simple Storage Services (S3)

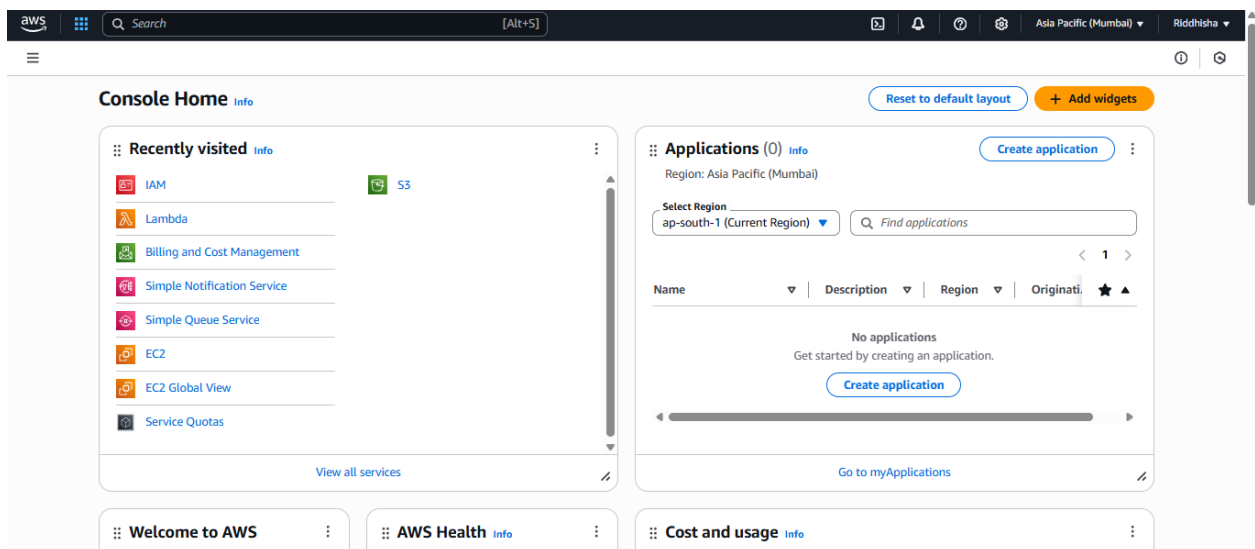
Introduction:

- Amazon Simple Storage Service (Amazon S3) is a cloud-based object storage service that helps you store and manage any amount of data. It offers high scalability, strong security, and fast performance, making it ideal for businesses of all sizes.
- You can use "Amazon S3" to store data for many purposes like "websites", "mobile apps", "backups", "archives", "data lakes", "IoT devices", and "big data analytics". It is also useful for restoring lost data and running enterprise-level applications.
- S3 includes tools to help you manage your files better. You can organize your data, control who can access it, and set rules that match your business or legal needs. It is a flexible and reliable solution for storing data safely in the cloud.

Step by Step Instructions:

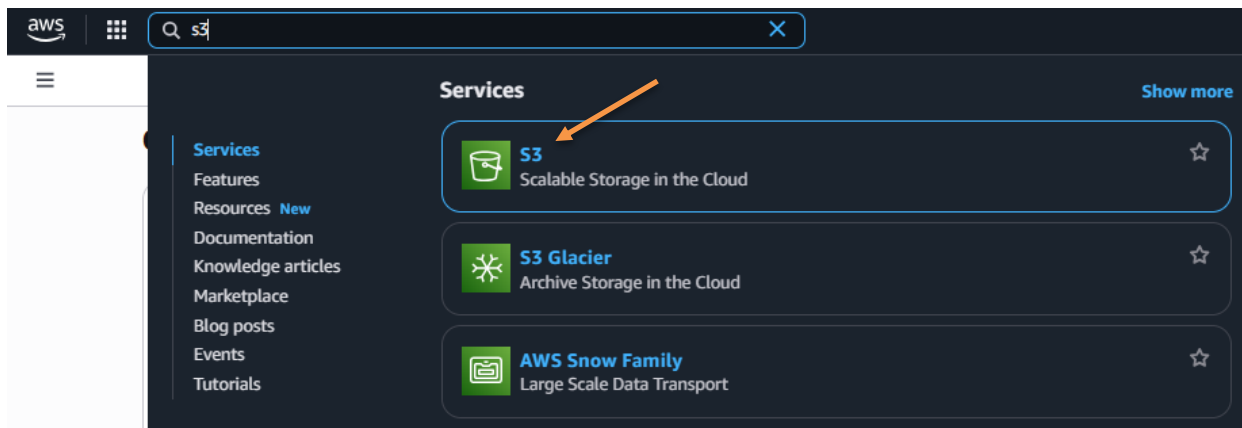
Step 1:

- Search “AWS Management Console” on Google.
- Click on “AWS Console Sign In | Amazon Web Services” and the home screen of AWS website will open.

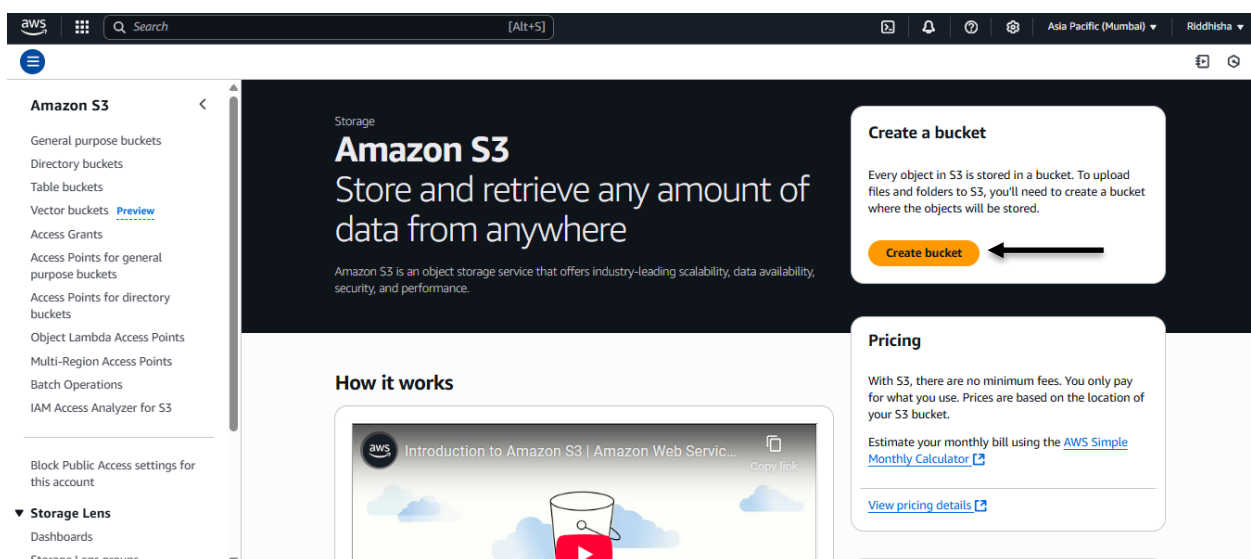


Step 2:

- Search for “S3” and open it.
- Then select any region (e.g. Mumbai).

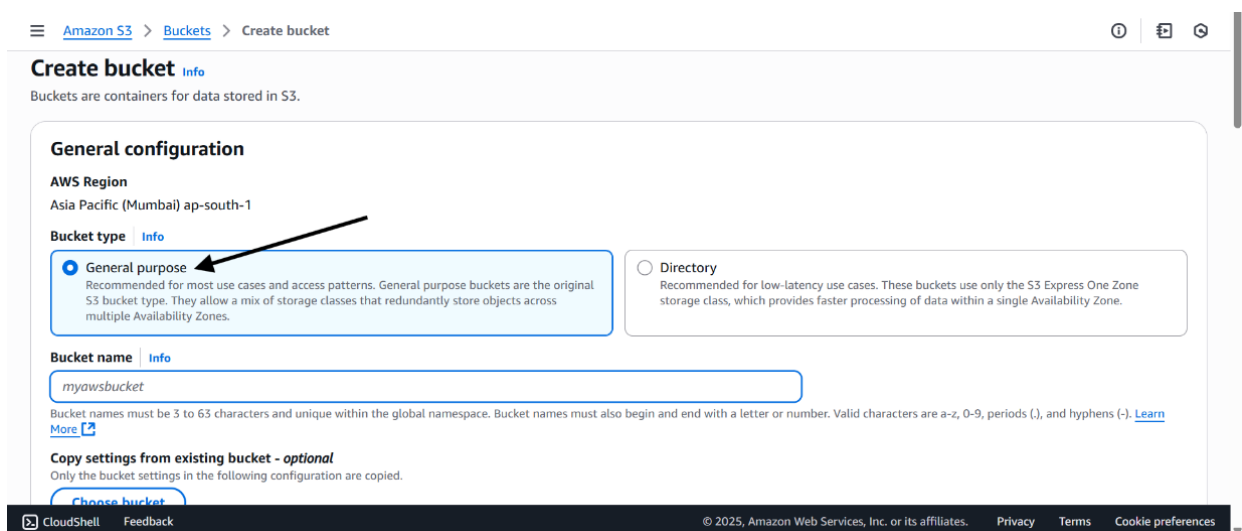


- Click on “Create Bucket”.



Step 3:

- Select Bucket Type - General purpose.



- Give a name to the bucket.
- In the “Object Ownership”, choose “ACL disabled”.

Bucket name [Info](#)

bucket5567568

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](#)

- This will create a private bucket.

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

- In “Bucket Versioning”, choose “Disable”.

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

- Click on “Create bucket”.

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

- The bucket is successfully created.

General purpose buckets (1/2) [Info](#)

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

Buckets are containers for data stored in S3.

Find buckets by name
 < 1 >
⚙️

	Name ▲	AWS Region ▼	Creation date ▼
<input checked="" type="radio"/>	bucket5567568	Asia Pacific (Mumbai) ap-south-1	July 18, 2025, 23:21:15 (UTC+05:30)

Step 4:

- Select the bucket you just created.
- Click on bucket name.

Name	AWS Region	Creation date
bucket5567568	Asia Pacific (Mumbai) ap-south-1	July 18, 2025, 23:21:15 (UTC+05:30)

- Then click on “Upload”.

Amazon S3 > Buckets > bucket5567568

bucket5567568 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](#)

Find objects by prefix

Name	Type	Last modified	Size	Storage class
No objects				
You don't have any objects in this bucket.				

[Upload](#)

Step 5:

- Click on add files.

Amazon S3 > Buckets > bucket5567568 > 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](#).

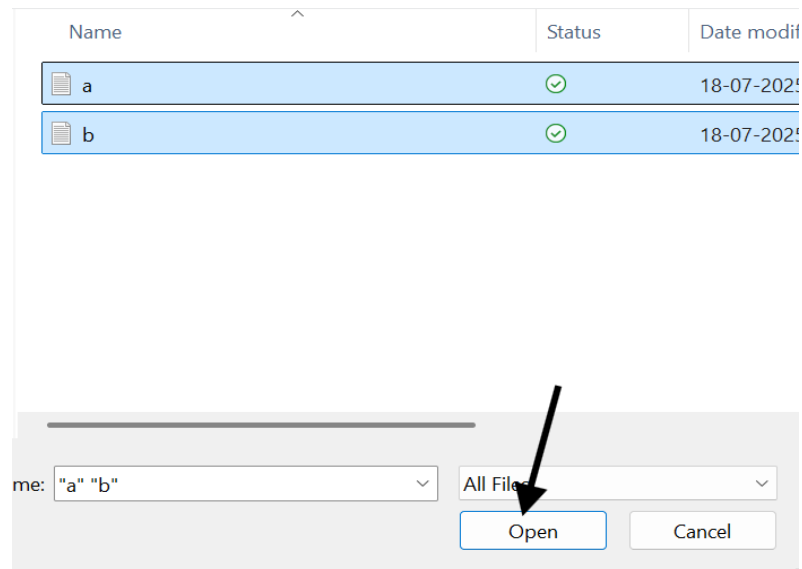
Files and folders (0) [Remove](#) [Add files](#) [Add folder](#)

All files and folders in this table will be uploaded.

Find by name

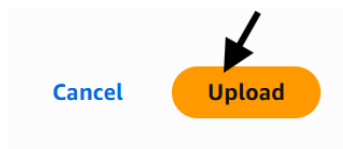
Name	Folder	Type	Size
No files or folders			
You have not chosen any files or folders to upload.			

- It opens for selecting files.
- Select files and upload it.

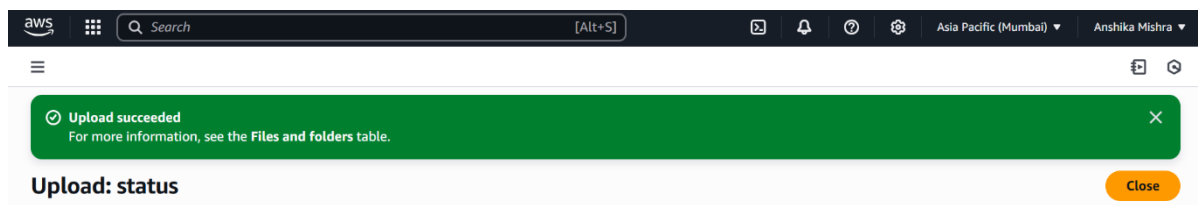


Step 6:

- Then finally click on “upload”.



- Now it shows that upload is succeeded so, you can close.



For public access:

Step1:

- Click on “S3”.
- Click on “Create Bucket” and similarly, create a bucket like you created before.
- Uncheck the “Block all public access” option.

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.

- Scroll down and check the “I acknowledge that the current settings might result in this bucket and the objects within becoming public” option.

Turning off block all public access might result in this bucket and the objects within becoming public
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☒ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

- In the “Object Ownership”, choose “ACL enabled”.

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.

We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.

Object Ownership

- ☒ **Bucket owner preferred**
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.
- ☐ **Object writer**
The object writer remains the object owner.

If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. [Learn more](#)

- In the “Bucket Versioning”, choose “Disable”.

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

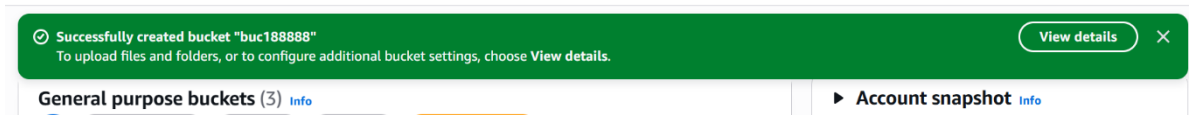
- ☒ **Disable**
- ☐ **Enable**

Step 2:

- Click on “Create Bucket”.



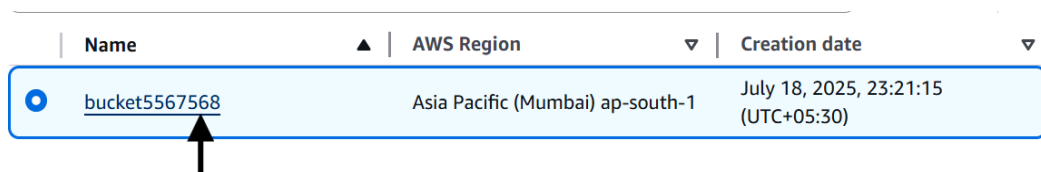
- Bucket is successfully created and this time, it is public.



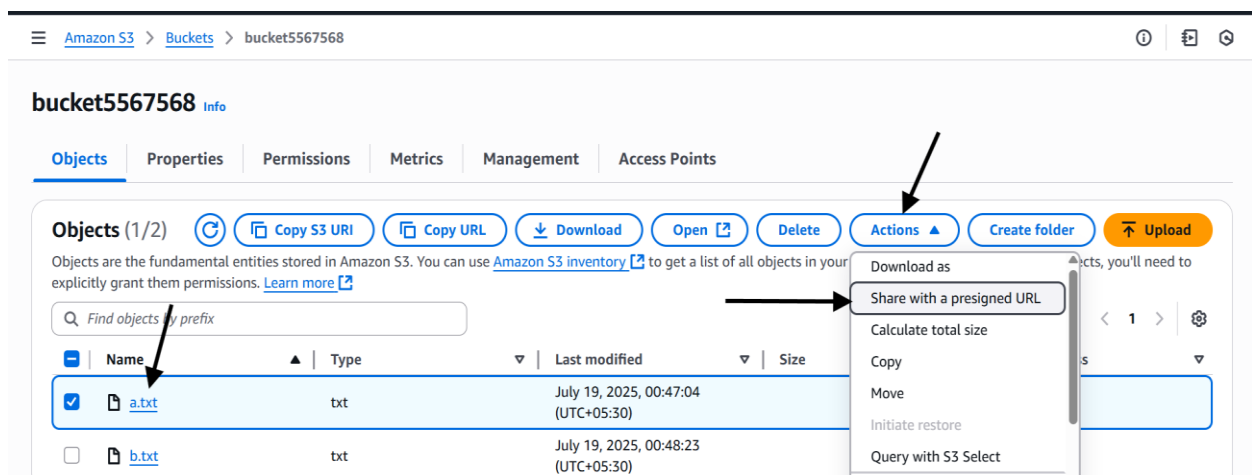
For private access:

Step 1:

- Open bucket, click on bucket name.



- Now, select text file and go to “Actions”.
- Click on “Share with a presigned URL”.



Step 2:

- Now, type time interval and then click on “Create presigned URL”.

Share "a.txt" with a presigned URL

Presigned URLs are used to grant access to an object for a limited time. [Learn more](#)

Anyone can access the object with this presigned URL until it expires, even if the bucket, and object are private.

Time interval until the presigned URL expires

Using the S3 console, you can share an object with a presigned URL for up to 12 hours or until your session expires. To create a presigned URL with a longer time interval, use the AWS CLI or AWS SDK. Time intervals for presigned URLs can be restricted by your IAM policy.

- ☒ Minutes
☐ Hours

Number of minutes

Must be a whole number between 1 and 720.

After you create the presigned URL, it's automatically copied to your clipboard.

Cancel

Create presigned URL

- Now, copy presigned URL.

A presigned URL for "a.txt" has been created and copied to your clipboard.

Copy presigned URL

- Now you can share the copied URL with anyone and only they can view your bucket .
- This URL is valid for 2 minutes only.

For changing storage class:

Step 1:

- Select file, go to "Actions".

Objects (1/2)



Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

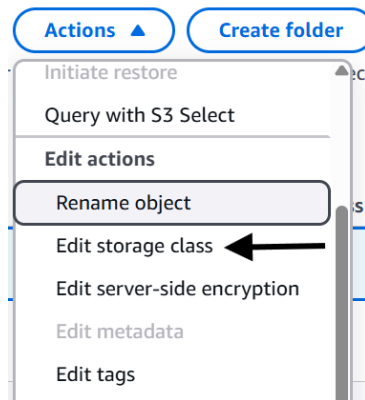
Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Find objects by prefix

< 1 > ⚙

	Name	Type	Last modified	Size	Storage class
<input checked="" type="checkbox"/>	a.txt	txt	July 19, 2025, 01:39:27 (UTC+05:30)	19.0 B	Standard

- Then, go to "Edit storage class".



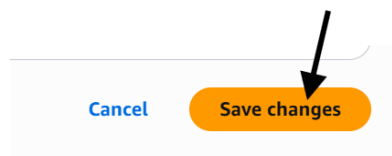
- Select “Standard-IA” in Storage class.

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	Min billable object size	Monitoring and auto-tiering fees	
<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	-	-	Per-object fees apply for objects >= 128 KB	-
<input checked="" type="radio"/>	Standard-IA	Infrequently accessed data (once a month) with milliseconds access	≥ 3	30 days	128 KB	-	P a
<input type="radio"/>	One Zone-IA	Recreateable, infrequently accessed data (once a month) with milliseconds access	1	30 days	128 KB	-	P a
<input type="radio"/>	Glacier Instant	Long-lived archive data accessed once a	≥ 3	90 days	128 KB	-	P

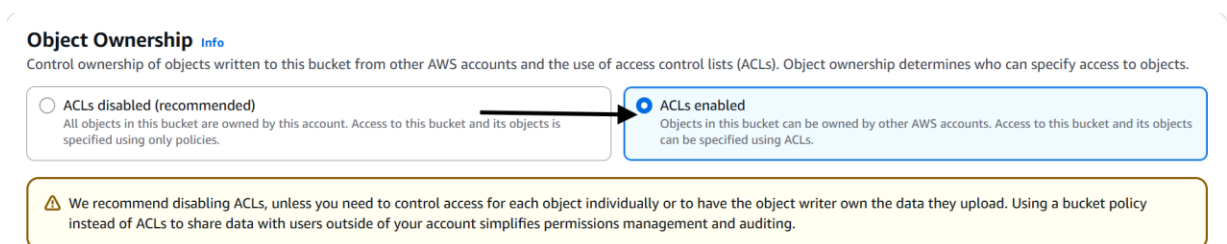
- Now, finally click on save changes.



Bucket Versioning:

Step 1:

- Create a bucket like you did before.
- In the “Object Ownership”, choose “ACL enabled”.



- Uncheck “Block all public access” option.

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.

- Scroll down and check the “I acknowledge that the current settings might result in this bucket and the objects within becoming public” option.

⚠ **Turning off block all public access might result in this bucket and the objects within becoming public**
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☒ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

- In “Bucket Versioning”, choose “Enable”.

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use it to recover from both unintended user actions and malware. Amazon S3 buckets can be configured to allow any number of versions of an object to be stored.

Bucket Versioning

☐ Disable

☒ **Enable** ←

Step 2:

- Go to “Advanced Settings” and “Enable” the Object Lock.
- Check on the acknowledgement.

▼ 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.

- Click on “Create Bucket”.



Step 3:

- Select the bucket and click on bucket name.

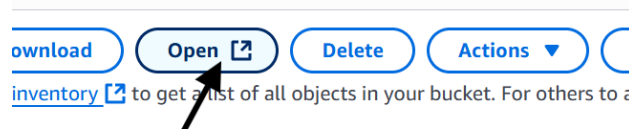
	Name	AWS Region	Creation date
<input checked="" type="radio"/>	<u>bucket5567568</u>	Asia Pacific (Mumbai) ap-south-1	July 18, 2025, 23:21:15 (UTC+05:30)

- Go to files and select a file.
- Open it on the browser.

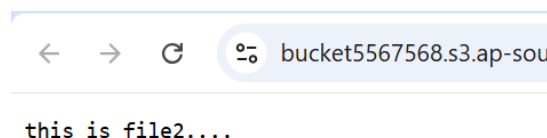
Objects (1/2) [Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#) [Actions](#)

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 other actions, you can explicitly grant them permissions. [Learn more](#)

	Name	Type	Last modified	Size
<input type="checkbox"/>	a.txt	txt	July 19, 2025, 01:52:34 (UTC+05:30)	19.0
<input checked="" type="checkbox"/>	b.txt	txt	July 19, 2025, 00:48:23 (UTC+05:30)	17.0





- The file is open and you can check the text it shows.

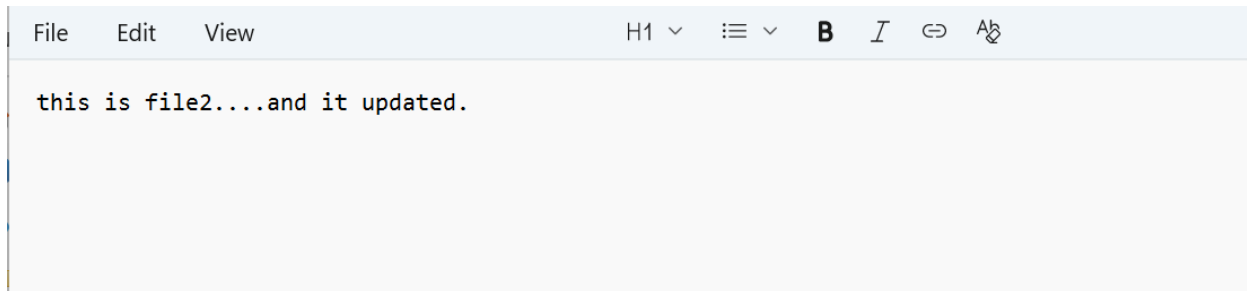


Step 4:

- Go to file explorer and open the same file.

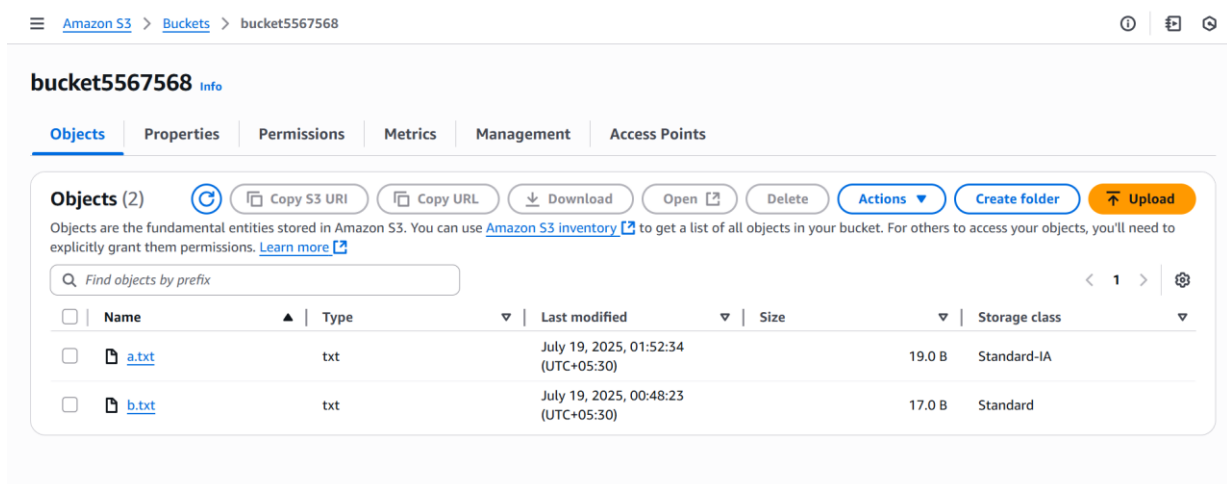
Name	Status	Date modified	Type	Size
 a	✓	18-07-2025 23:37	Text Document	1 KB
 b	✓	18-07-2025 23:37	Text Document	1 KB

- Make changes in the file and save it.

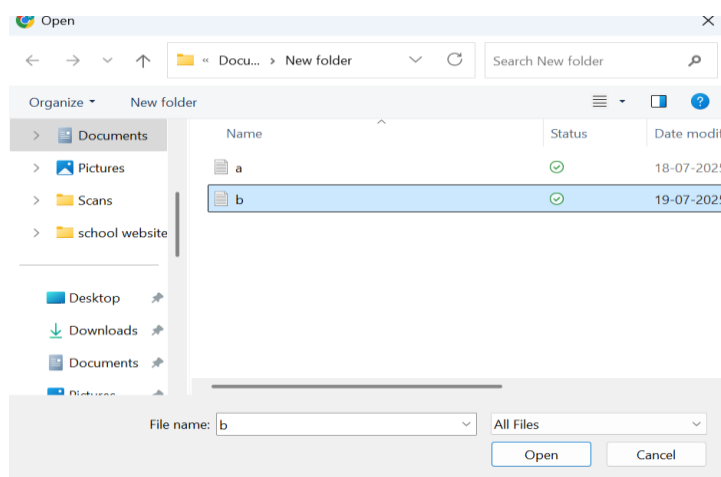


Step 5:

- Open the bucket and go to files.



- Upload the same file again i.e. "b.txt".
- Click on "Upload".



Cancel Upload

Step 6:

- Now you can see that there is no change.

Amazon S3 > Buckets > bucket5567568

bucket5567568 Info

Objects Properties Permissions Metrics Management Access Points

Objects (2)

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 >

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	a.txt	txt	July 19, 2025, 02:49:59 (UTC+05:30)	19.0 B	Standard
<input type="checkbox"/>	b.txt	txt	July 19, 2025, 02:51:00 (UTC+05:30)	17.0 B	Standard

- Click on "Show versions" and it will show all the versions of the files uploaded in the bucket.

Objects (3)

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 >

<input type="checkbox"/>	Name	Type	Version ID	Last modified	Size	Storage class
<input type="checkbox"/>	a.txt	txt	QXTBa7DDtWr2lWD8eR Fdot3Dwf1MyHUL	July 19, 2025, 02:49:59 (UTC+05:30)	19.0 B	Standard
<input type="checkbox"/>	b.txt	txt	0a7MDA3.RKR2pBr6u_B 9o_7KdNzh2L0	July 19, 2025, 02:54:01 (UTC+05:30)	32.0 B	Standard
<input type="checkbox"/>	b.txt	txt	kxg2yFYhHwM8KGcMP0s K9f5flkyNGfZv	July 19, 2025, 02:51:00 (UTC+05:30)	17.0 B	Standard

- Select updated file and open it.

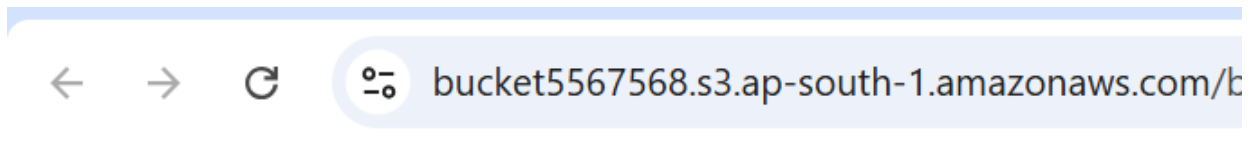
Objects (1/2)

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](#)

< 1 >

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	a.txt	txt	July 19, 2025, 01:52:34 (UTC+05:30)	19.0 B	Standard-IA
<input checked="" type="checkbox"/>	b.txt	txt	July 19, 2025, 02:03:35 (UTC+05:30)	32.0 B	Standard

- Now, you can see the updated file with text.

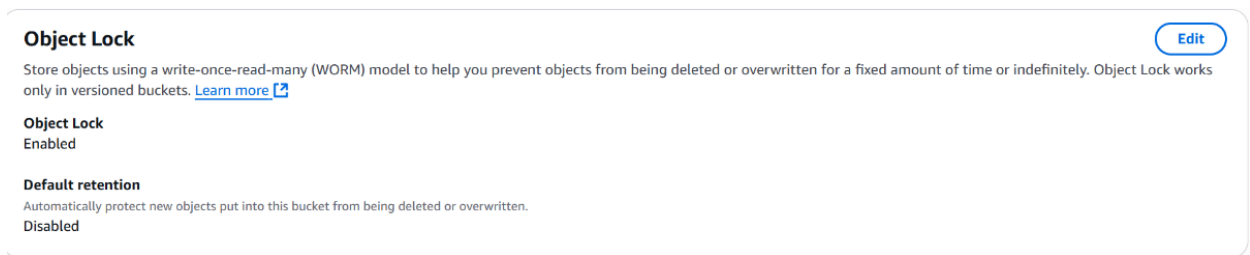


this is file2....and it updated.

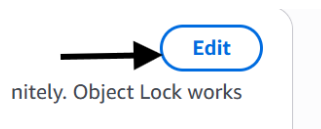
For retention mode:

Step 1:

- Go to “Object lock”.

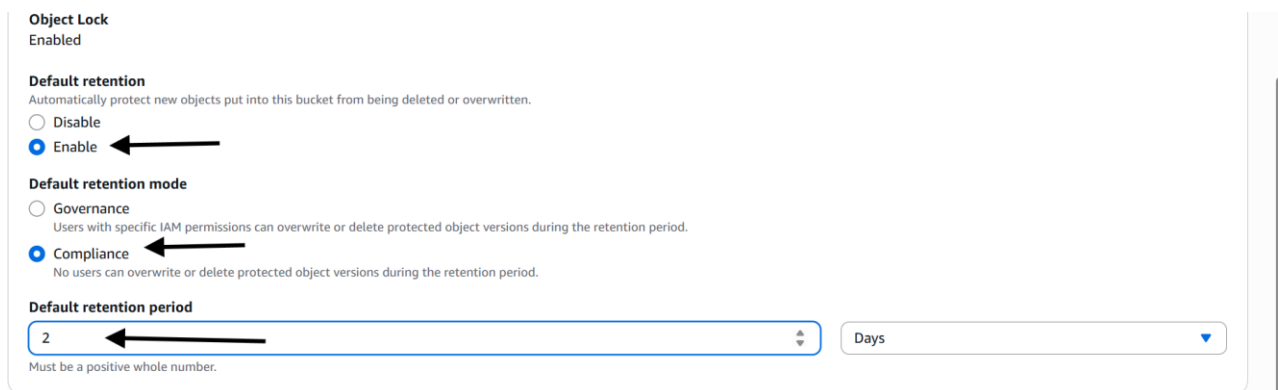


- Click on “edit”.



Step 2:

- “Enable” Default retention.
- Select “Compliance” in “Default retention mode”.
- Set “Default retention period”.



- Click on “Save Changes”.



- Type “confirm”.
- Then click on “Enable compliance mode”.

