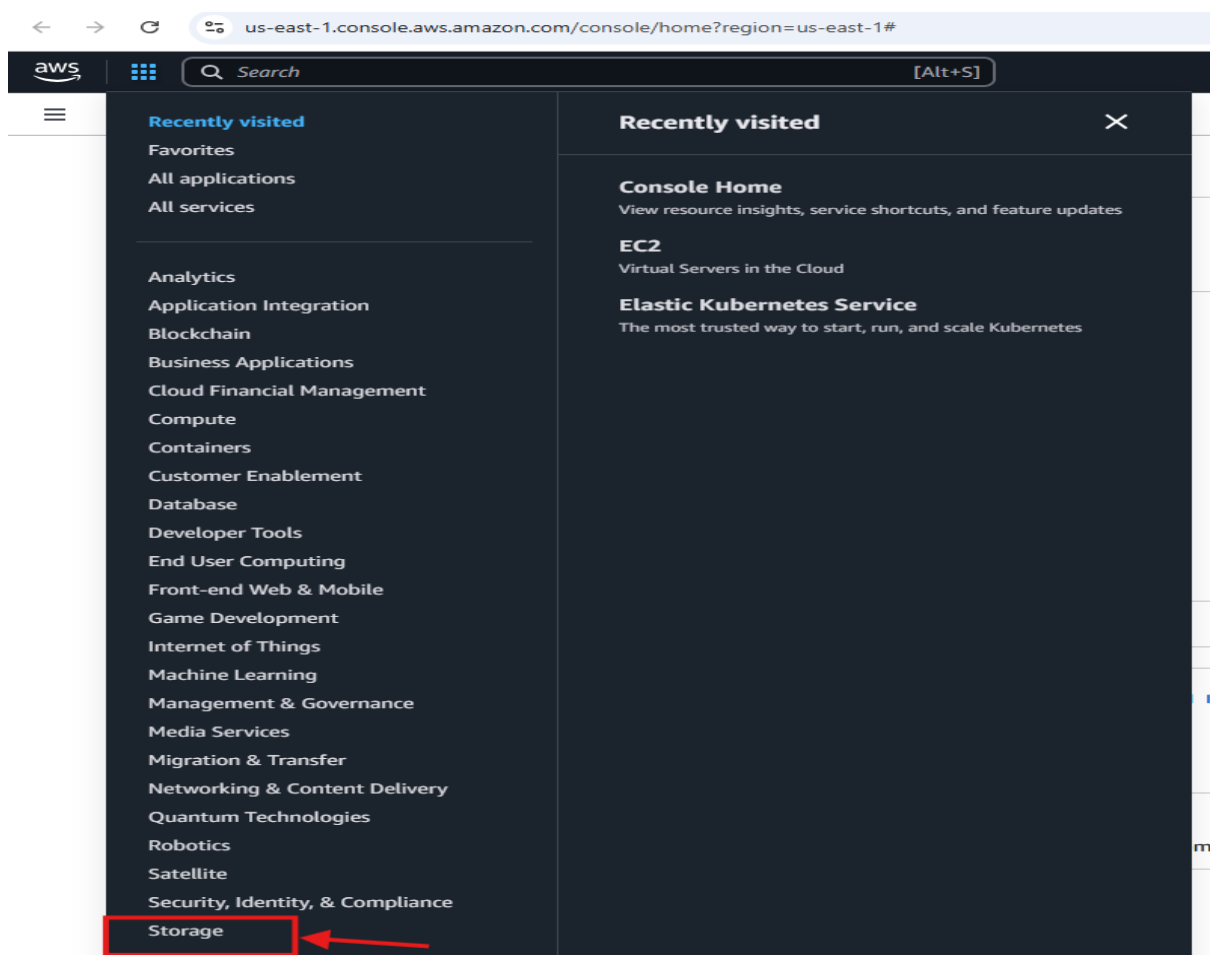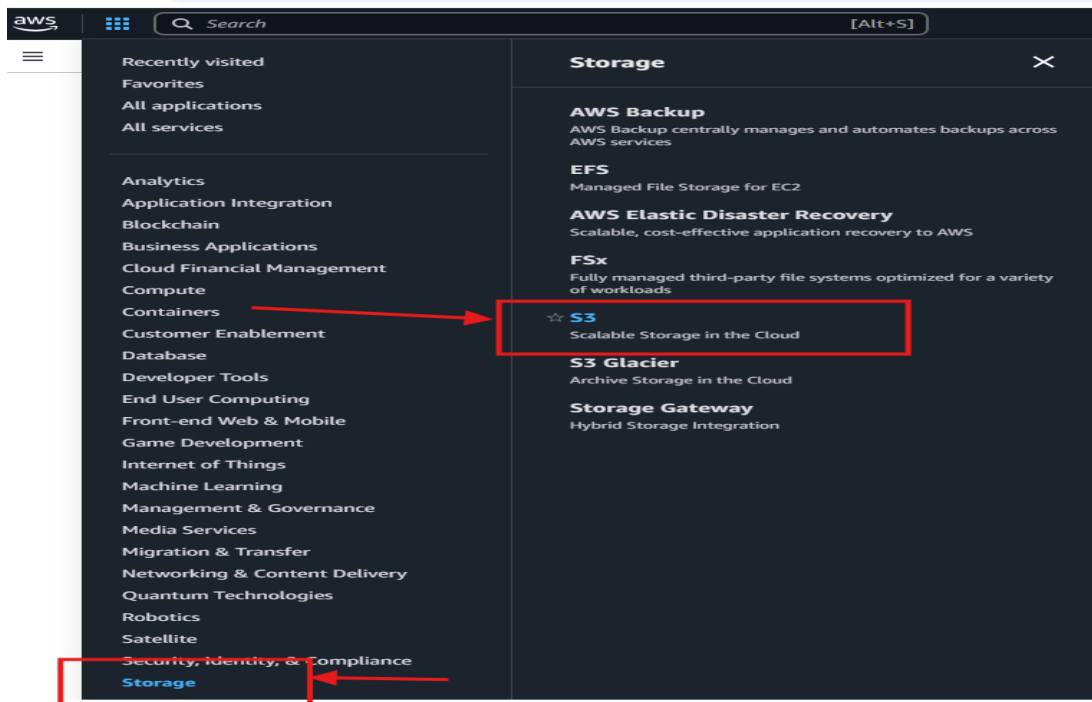# Week-4: Create and configure Amazon Simple Storage Service (Amazon S3)

Step 1: Sign in to the AWS Management Console
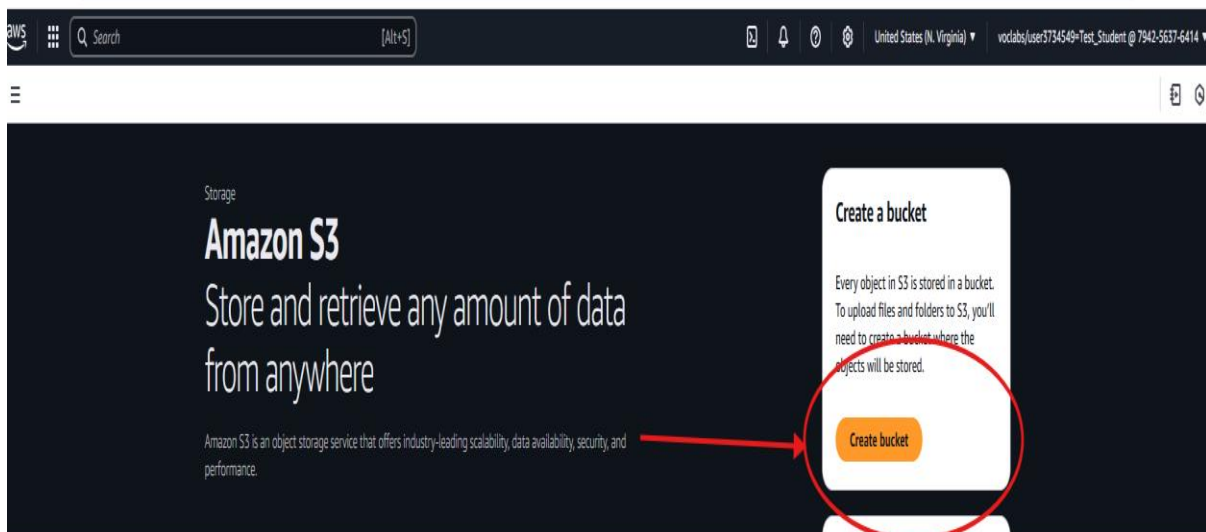
Step 2: Navigate to the S3 Service

Once you're logged in to the AWS Management Console, search for and select the S3 service. This will take you to the S3 dashboard, where you can manage your buckets and objects

Step 3: Create a New Bucket

To create a new bucket, click on the "Create bucket" button.

You will be prompted to provide a unique name for your bucket. Keep in mind that the bucket name must be globally unique across all existing buckets in S3.

Create bucket Info
Buckets are containers for data stored in S3.

General configuration

AWS Region
US East (N. Virginia) us-east-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 us processing of data within a single Availability Zone.

Bucket name | Info

myawsbucket

Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming ↗

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 account

Object Ownership
Bucket owner enforced

Step 4: Configure Bucket Properties

After naming your bucket, you'll need to configure its properties. This includes selecting the region where your bucket will be located and setting up optional features such as versioning, logging, and tags. Choose the appropriate settings based on your requirements.

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 processing of data within a single Availability Zo

Bucket name | Info

Mru-sabitha

Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming ↗

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 t

○ **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 AV

Object Ownership
Bucket owner enforced

Step 5: Set Permissions

In this step, you can define access permissions for your bucket. AWS offers a flexible and granular access control mechanism using AWS Identity and Access Management (IAM) policies. You can specify who can access your bucket and what operations they can perform.

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 ensu 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 set public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn mo

☑ **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 a

   ☑ **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 allc

   ☑ **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 versio both unintended user actions and application failures. Learn more ↗

Bucket Versioning
◉ Disable
○ Enable

Tags - *optional* (0)

You can use bucket tags to track storage costs and organize buckets. Learn more ↗

No tags associated with this bucket.

(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

Step 6: Review and Create

Before creating the bucket, review the configuration settings you've made so far. Double-check the bucket name, region, properties, and permissions. If everything looks good, click on the "Create bucket" button to create your S3 bucket.

▶ **Advanced settings**

ⓘ After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

Cancel   **Create bucket**

Go to Settings to activate Windc

Step 7: Upload a file in S3 bucket

Now that you've created a bucket, you're ready to add an object to it. An object can be any kind of file: a document, a photo, a video, a music file, or other file type.

Successfully created bucket "mru-sabitha"
To upload files and folders, or to configure additional bucket settings, choose **View details**.

Account snapshot - *updated every 24 hours* All AWS Regions

Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. Learn more

General purpose buckets   Directory buckets

General purpose buckets (1) Info All AWS Regions
Buckets are containers for data stored in S3.

Name	AWS Region	IAM Access Analyzer	Creation date
mru-sabitha	US East (N. Virginia) us-east-1	View analyzer for us-east-1	January 31, 2025, 10:19:13 (UTC+05:30)

General purpose buckets (1) Info All AWS Regions

Buckets are containers for data stored in S3.

Name	AWS Region
mru-sabitha	US East (N. Virginia) us-east-1

In the Amazon S3 console, choose the bucket where you want to upload an object**, choose Upload**, and then choose **Add Files**

mru-sabitha Info

Objects   Metadata   Properties   Permissions   Metrics   Management   Access Points

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

Name	Type	Last modified	Size	Storage class

No objects
You don't have any objects in this bucket.

Upload

In the file selection dialog box, find the file that you want to upload, choose it, choose **Open**, and then choose **Start Upload**.

Step 8: Create Folder in S3 Bucket

Click on the "Create Folder" button to create a new folder in the selected bucket.
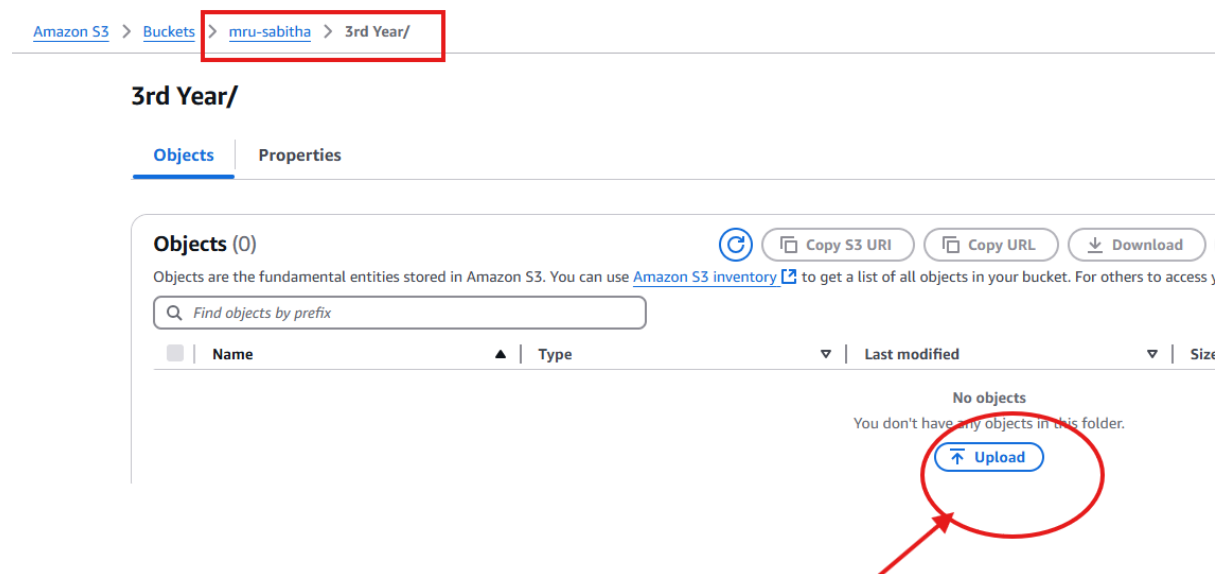

Enter Folder Name, Click on Create Folder.

Step 9: Upload the file in the Folder

Click on Folder Name in S3 Bucket, It will open the folder
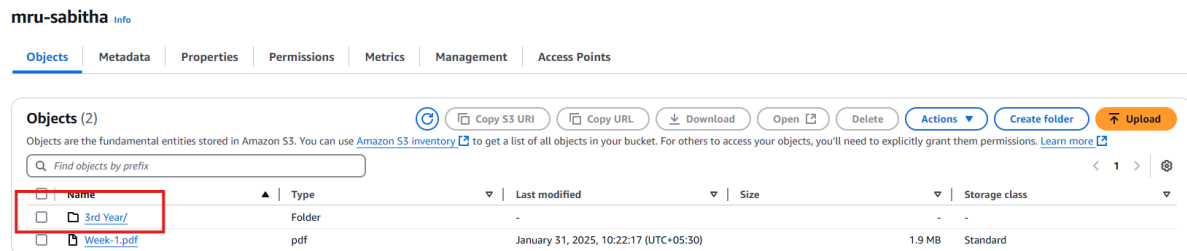
Click on upload, Click on Add files ->browse the file from your local system->Click on Upload

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)
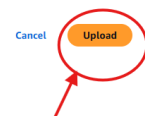
All files and folders in this table will be uploaded.

Remove | Add files | Add folder

Name ▽	Folder ▽	Type ▽	Size ▽

No files or folders

You have not chosen any files or folders to upload.

Destination Info

Destination

s3://mru-sabitha/3rd Year/ ⧉

▶ **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.

Cancel | Upload

Files and folders (1 total, 71.3 KB)

All files and folders in this table will be uploaded.

Remove | Add files | Add folder

Name ▽	Folder ▽	Type ▽	Size ▽
☐ sabitha.cse.jpg	-	image/jpeg	71.3 KB

Destination Info

Destination

s3://mru-sabitha/3rd Year/ ⧉

▶ **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.

Cancel | Upload

File will be Uploaded Successfully in the folder

✓ **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://mru-sabitha/3rd Year/

Succeeded
✓ 1 file, 71.3 KB (100.00%)

Failed
⊖ 0 files, 0 B (0%)

Files and folders | Configuration
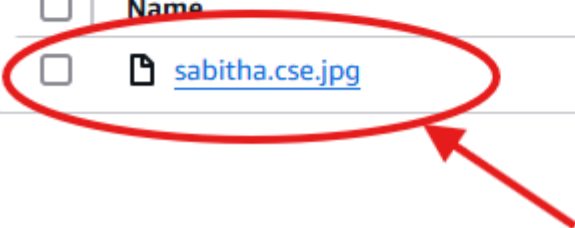
Files and folders (1 total, 71.3 KB)

Name	Folder ▽	Type ▽	Size ▽	Status ▽	Error ▽
sabitha.cse.jpg ⧉	-	image/jpeg	71.3 KB	✓ Succeeded	-

3rd Year/

Objects | **Properties**

Objects (1)

Objects are the fundamental entities stored in Amazon S3. You can use Amaz

🔍 Find objects by prefix

☐	Name	▲	Type
☐	📄 sabitha.cse.jpg		jpg

Now that you've added an object to a folder, you can open and view it in a browser. You can also download the object to your local computer.
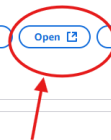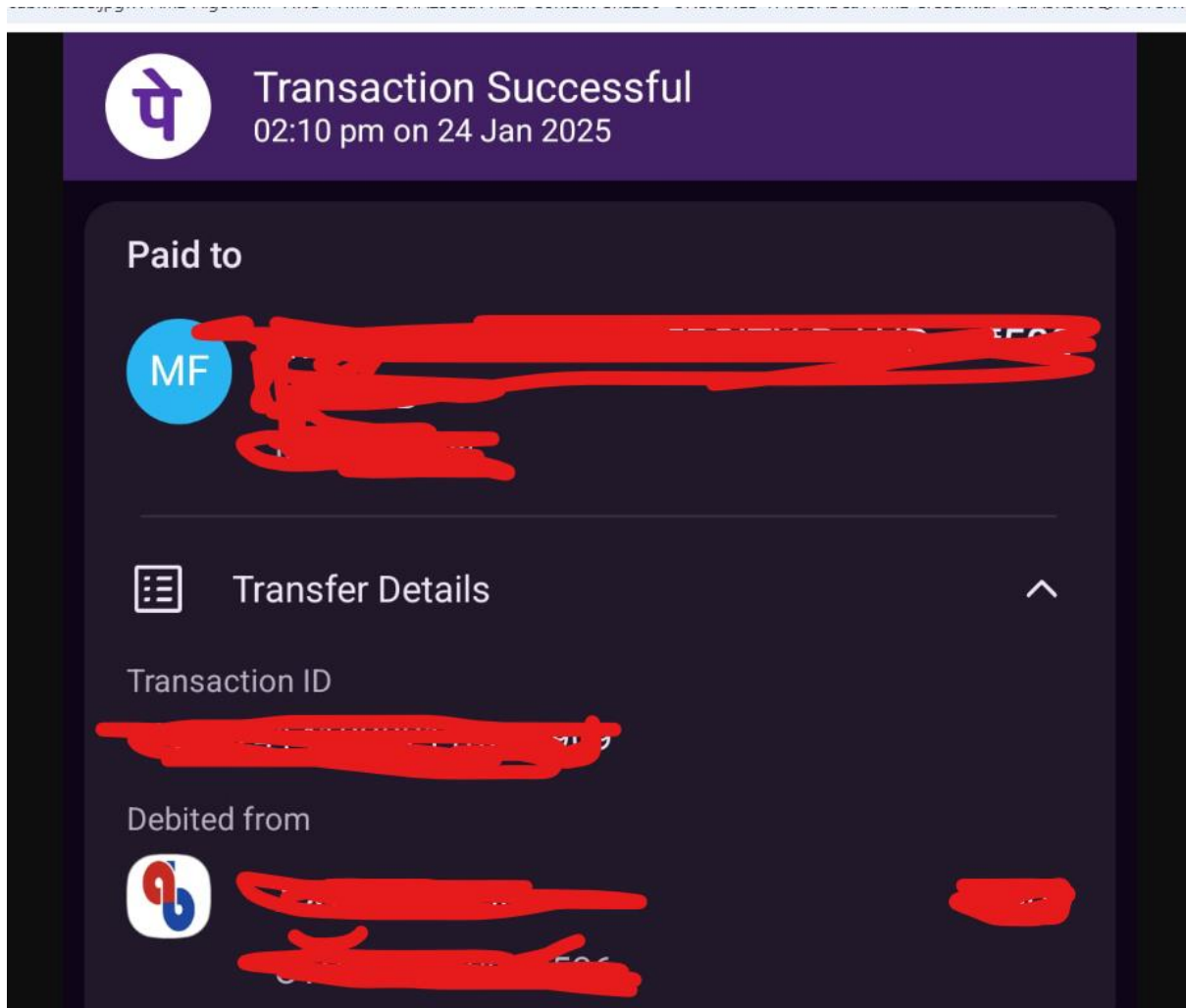
Click on File Name->Click Open

sabitha.cse.jpg Info

[Copy S3 URI] [↓ Download] [Open ☑] [Object actions ▼]

Properties | Permissions | Versions

Object overview

Owner
awslabsc0w3898468t1645879782

AWS Region
US East (N. Virginia) us-east-1

Last modified
January 31, 2025, 10:27:48 (UTC+05:30)

Size
71.3 KB

Type
jpg

Key
📋 3rd Year/sabitha.cse.jpg

S3 URI
📋 s3://mru-sabitha/3rd Year/sabitha.cse.jpg

Amazon Resource Name (ARN)
📋 arn:aws:s3:::mru-sabitha/3rd Year/sabitha.cse.jpg

Entity tag (Etag)
📋 578f9cbda57ff7dcdddc34e7f1e5959a

Object URL
📋 https://mru-sabitha.s3.us-east-1.amazonaws.com/3rd+Year/sabitha.cse.jpg

Transaction Successful
02:10 pm on 24 Jan 2025

Paid to

MF

Transfer Details

Transaction ID

Debited from

## Retaining multiple versions of objects with S3 Versioning

Versioning in Amazon S3 is a means of keeping multiple variants of an object in the same bucket. You can use the S3 Versioning feature to preserve, retrieve, and restore every version of every object stored in your buckets. With versioning you can recover more easily from both unintended user actions and application failures. After versioning is enabled for a bucket, if Amazon S3 receives multiple write requests for the same object simultaneously, it stores all of those objects.

Versioning-enabled buckets can help you recover objects from accidental deletion or overwrite.

Step 1: Then on the Amazon S3 page click on create a bucket.
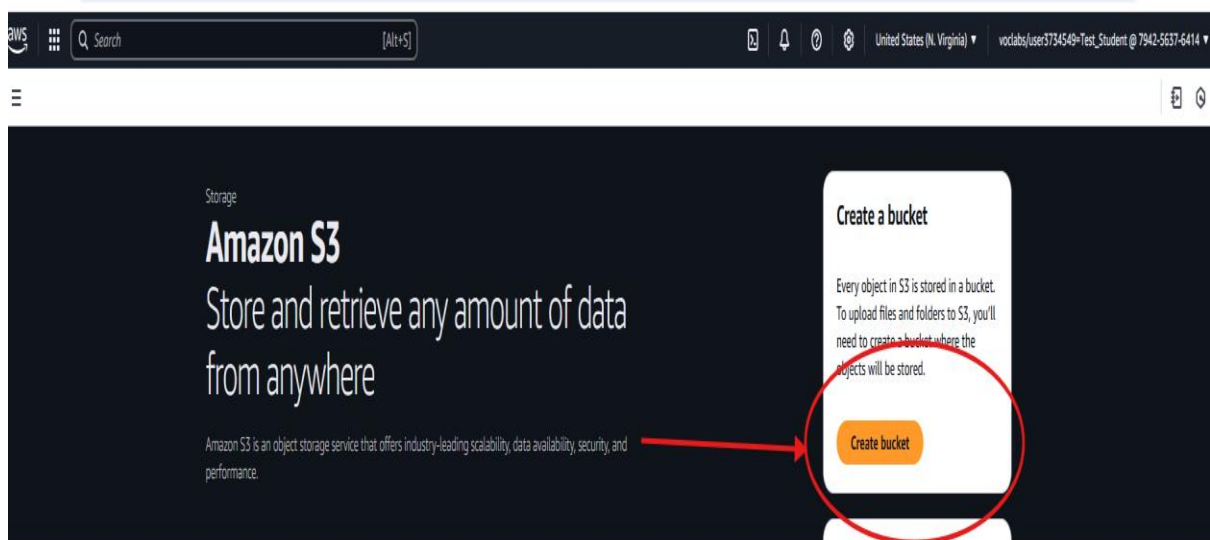
Step 2: In create bucket page, Give the bucket a Name
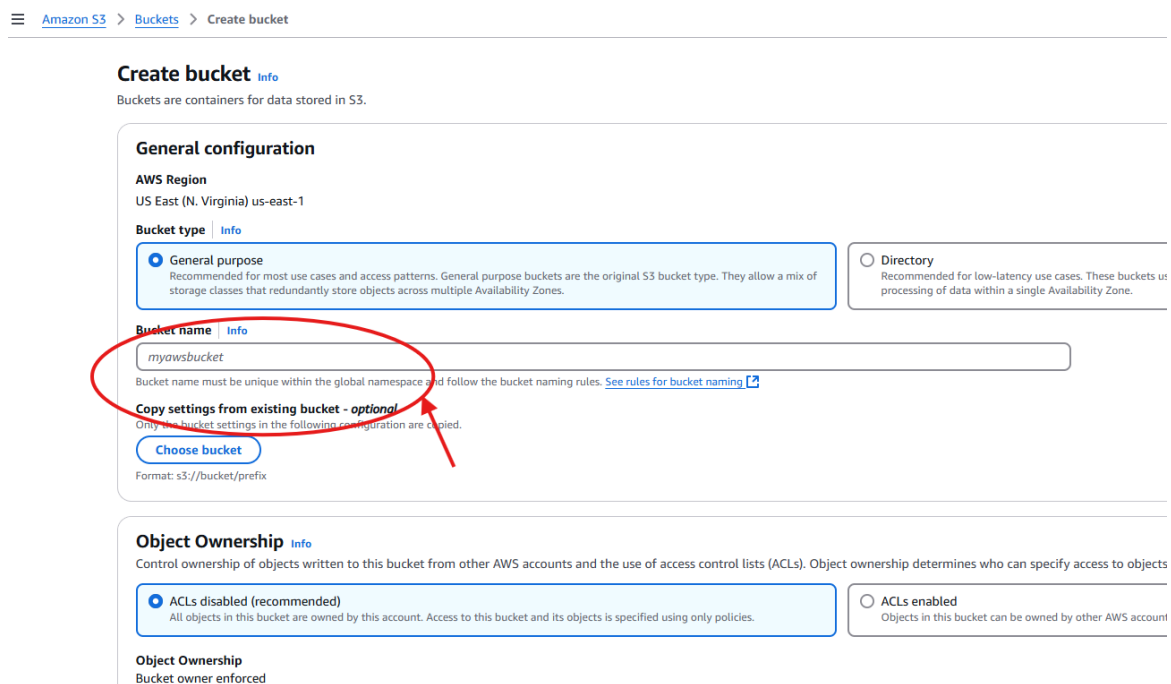
NOTE: name must be unique and should not contain any space or uppercase letter)

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 processing of data within a single Availability Zo

Bucket name | Info

Mru-sabitha

Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming

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 t

○ **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 AV

Object Ownership
Bucket owner enforced

Step 3: ACLs disabled Enable or Block Public Access Bucket

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 ensu 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 set public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn mo

☑ **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 a

☑ **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 allo

☑ **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.

Step 4: Versioning -> Select Enable

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 obje both unintended user actions and application failures. Learn more

Bucket Versioning
○ Disable
● Enable

Default Encryption

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

Step 4: Click on your created bucket>>Click on upload>>Upload any file
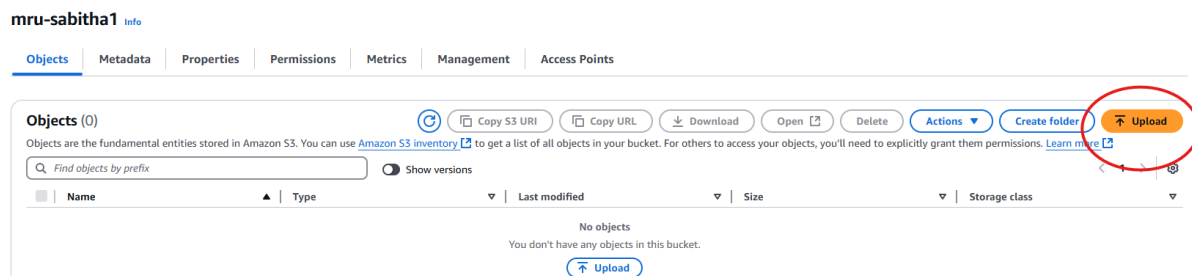
Upload the Object
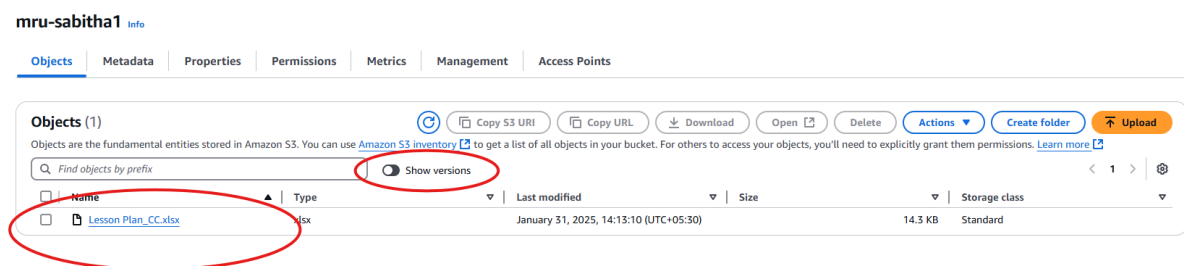
Step 5: To find the Versioning of object enable the Show Version option

mru-sabitha1 Info

Objects	Metadata	Properties	Permissions	Metrics	Management	Access Points

Objects (1)   Copy S3 URI   Copy URL   Download   Open ☐

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 nee

Find objects by prefix   ⬤ Show versions

☐	Name	▲	Type	Version ID	Last modified	Size
☐	Lesson Plan_CC.xlsx		xlsx	6rH0vsmwM MkNNEA6Lpk sAVf8QT6Ds8 79	January 31, 2025, 14:13:10 (UTC+05:30)	

Upload the same file again into bucket

Files and folders (1 total, 14.3 KB)

All files and folders in this table will be uploaded.

Find by name

☐	Name	▽	Folder	▽	Type
☐	Lesson Plan_CC.xlsx		-		application/vnd.openxmlformats-officedocun

Destination Info

Destination

s3://mru-sabitha1 ☐

▶ **Destination details**

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

mru-sabitha1 Info

Objects	Metadata	Properties	Permissions	Metrics	Management	Access Points

Objects (1)   Copy S3 URI   Copy URL   Download

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 ac

Find objects by prefix   ○ Show versions

☐	Name	▲	Type	Last modified	▽
☐	Lesson Plan_CC.xlsx		xlsx	January 31, 2025, 14:16:53 (UTC+05:30)	

✓ Enable Shoe version option you will find Version of object

✓ Multiple Files will be available in bucket when you uploading same file multiple times with different version id

Delete Data from S3 Bucket

In the Bucket name list, choose the name of the bucket that you want to delete an object from.

Select the object and then choose Delete.

To confirm deletion of the objects list under Specified objects in the Delete objects? text box, enter permanently delete.

mru-sabitha1 Info

Objects | Metadata | 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

	Name ▲	Type	Version ID	Last modified	Size	Storage class
☐	📄 Lesson Plan_CC.xlsx	xlsx	6rH0vsmwMMkNNEA6LpksAVf8QT6Ds879	January 31, 2025, 14:13:10 (UTC+05:30)	14.3 KB	Standard

Objects (1)

Copy S3 URI | Copy URL | Download | Open | Delete | Actions ▼ | Create folder | Upload

	Name ▲	Type	Version ID	Last modified	Size	Storage class
☐	📄 Lesson Plan_CC.xlsx	xlsx			14.3 KB	Standard