

Name: Ashwini Shetty

Roll No: A063

SapId: 86062300005

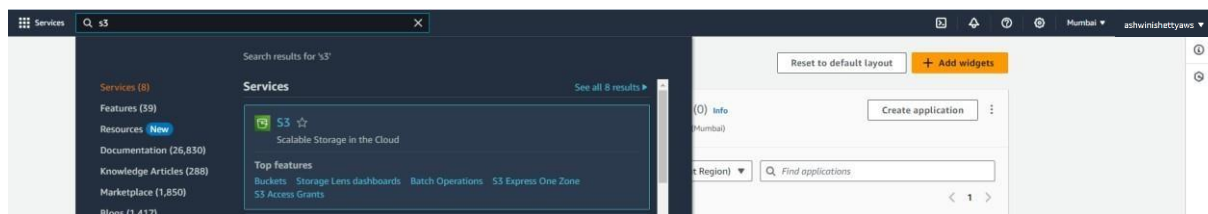
MSc SDS Batch 2

Cloud Computing Practical 2

1) Uploading a file, video, etc

Steps:

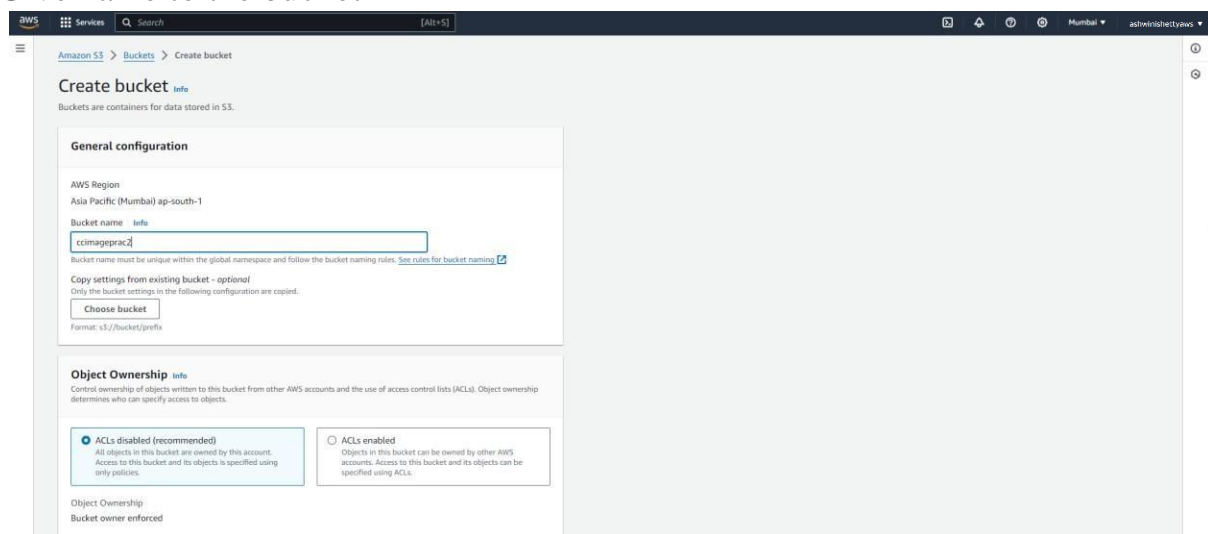
Open Amazon Web Services (AWS) and login in the services. Search S3 on the search tab. Click on S3.



Then Click on Create Bucket



Give name to the bucket



Please ensure that you click on block all parties if it is not turned on and let the others options be in default.

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

Then click on Create Bucket.

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 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

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

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

Click on ccimageprac2 i.e the name of the bucket here.

Successfully created bucket "ccimageprac2"

To upload files and folders, or to configure additional bucket settings, choose [View details](#).

[View Storage Lens dashboard](#)

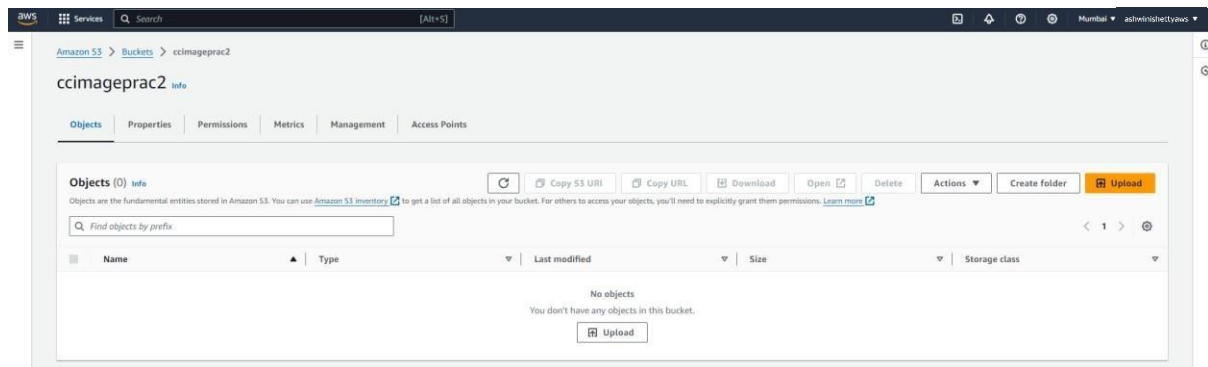
General purpose buckets | Directory buckets

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

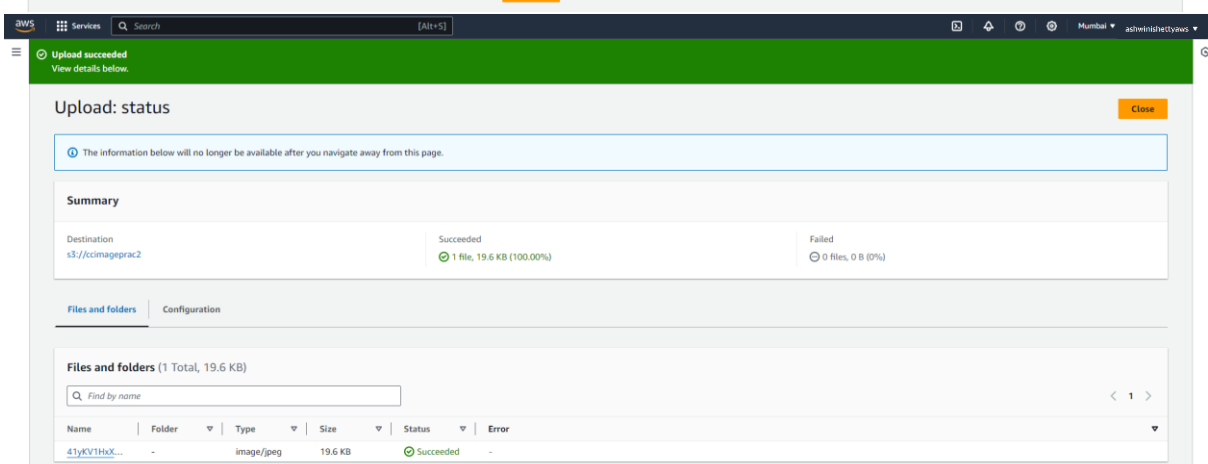
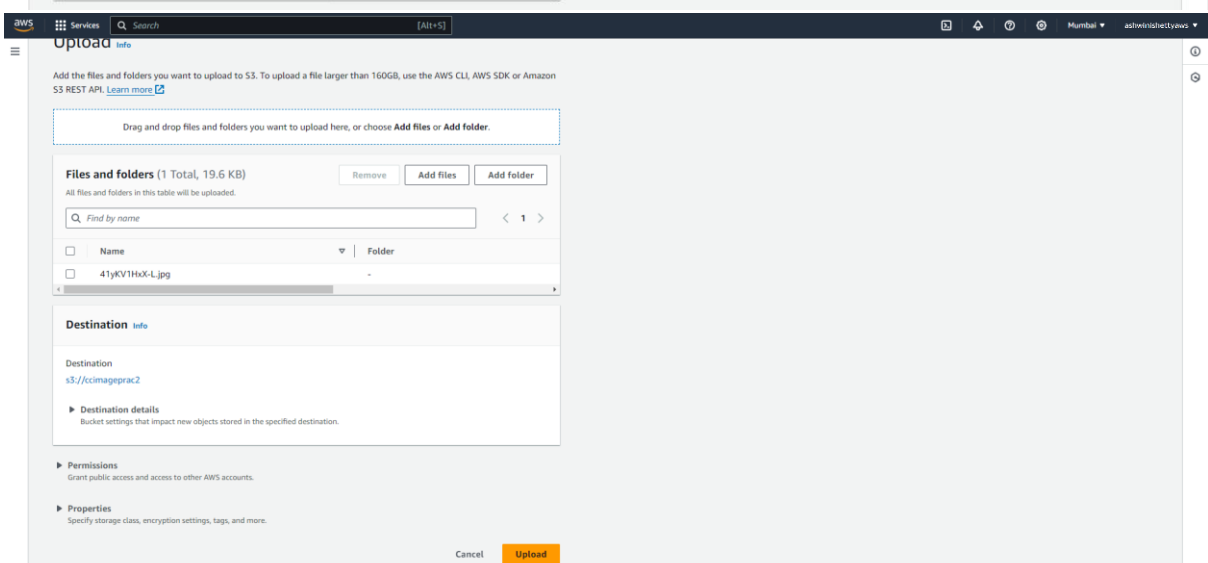
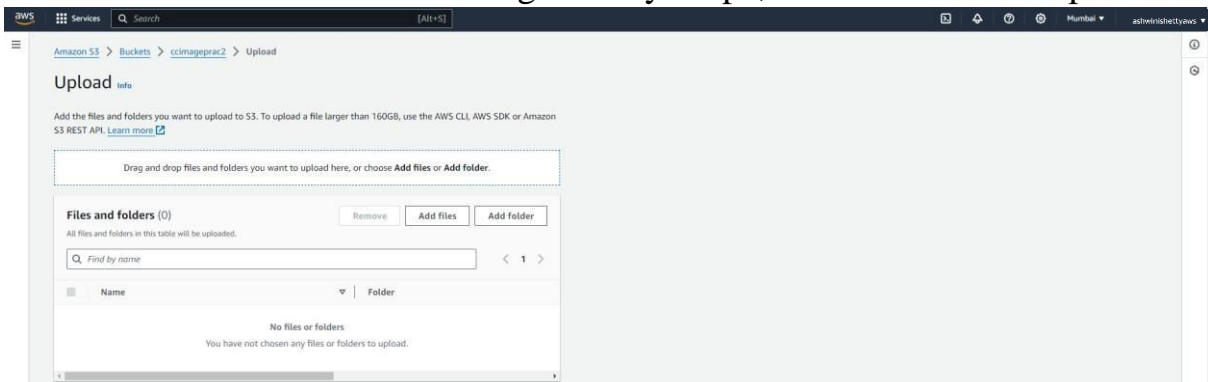
Buckets are containers for data stored in S3.

Name	AWS Region	IAM Access Analyzer	Creation date
ccimageprac2	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	July 27, 2024, 17:02:28 (UTC+05:30)

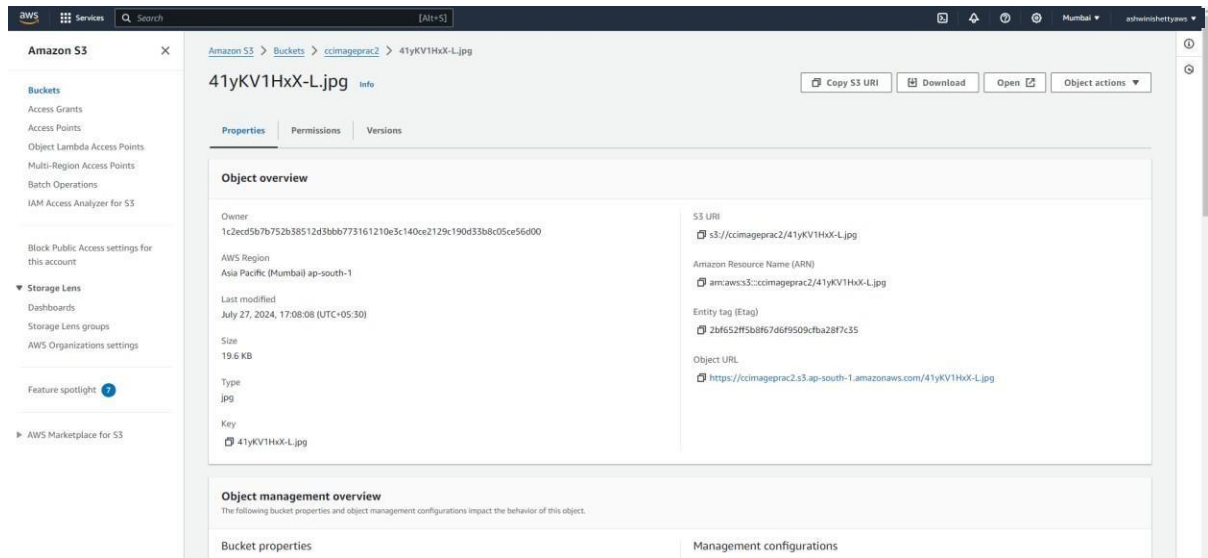
Click on Upload.



Click on Add files and add the image from your pc, and then click on Upload button.



Now you have successfully uploaded the image and to check your image click on the link inside the Name of the Files and Folders.



Click on the open button then you will get the uploaded image.



Uploading a static website:

Click on Create other bucket for creating another bucket for creating an html webpage that will open in the AWS. Proceed the above process again.

This is a Heading

This is a paragraph.

