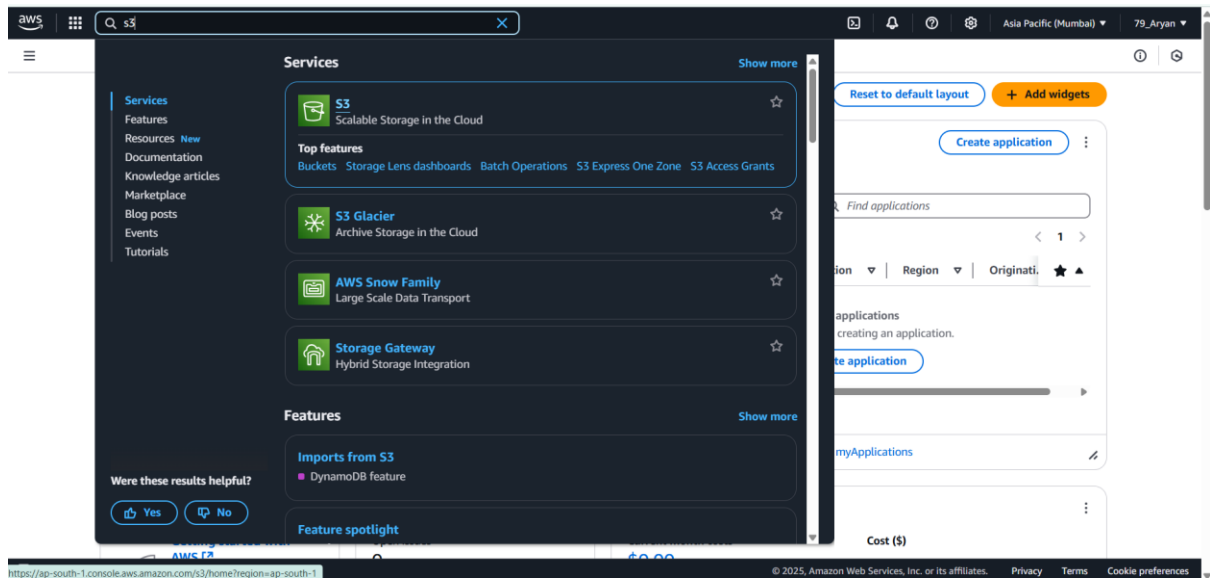# Assignment No:06

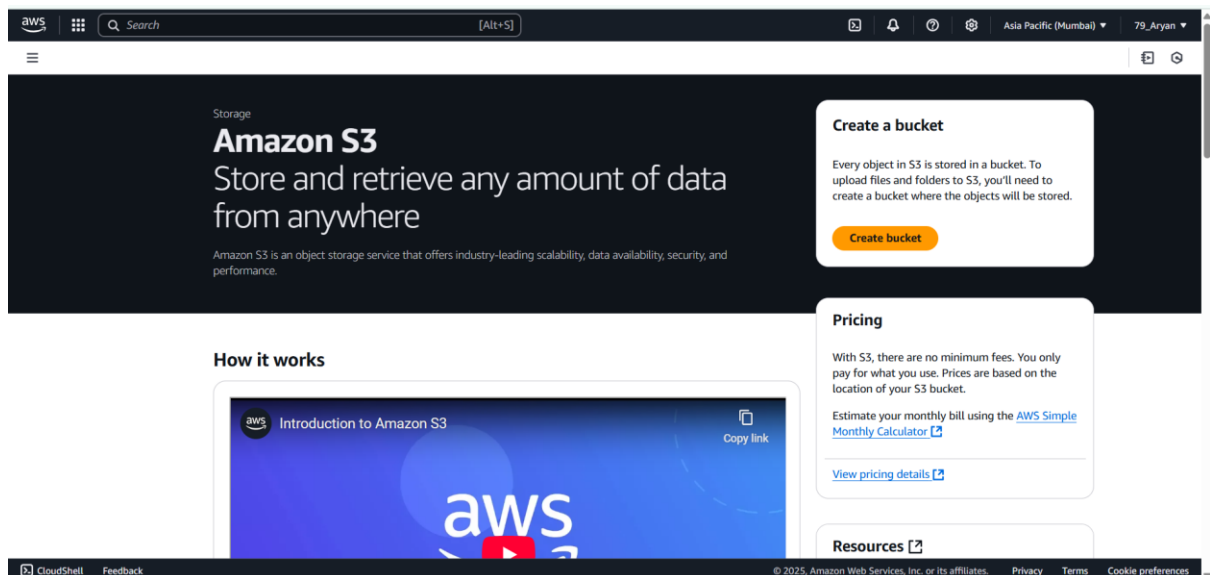## Title: Upload a static website on S3.

Step-1:

Search S3 in the AWS management console.

Step-2:

Click on the S3 and click on create bucket.

Step-3:

Name the bucket the select all the necessary settings uncheck "block all public access" and enable bucket versioning.

Create bucket Info

Buckets are containers for data stored in S3.

General configuration

AWS Region
Asia Pacific (Mumbai) ap-south-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

aryankye

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.

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 ☒

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.

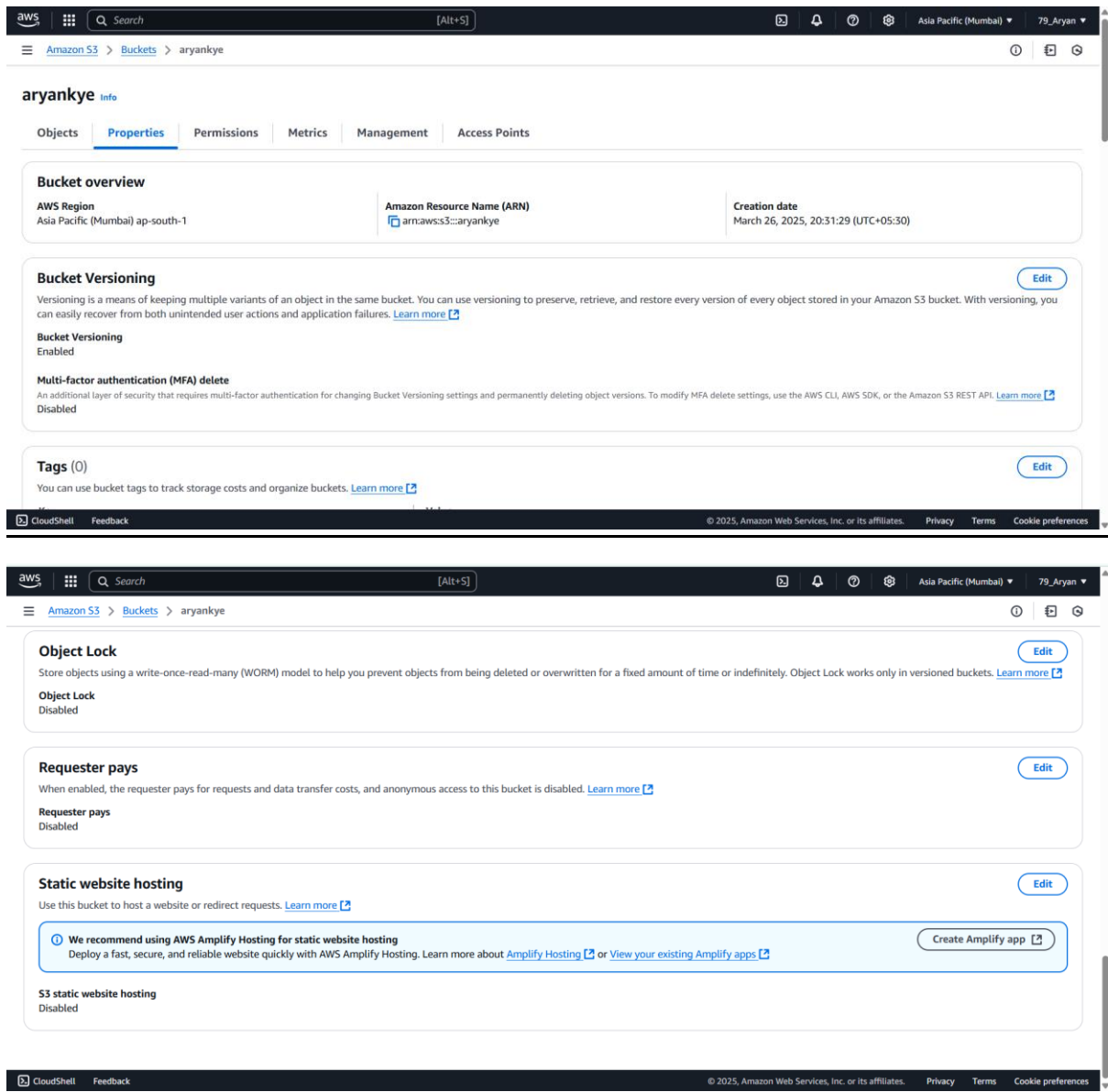☐ **Block public access to buckets and objects granted through any access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.

☐ **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.

⚠ **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.

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 (0)

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

No tags associated with this bucket.

Step-4:

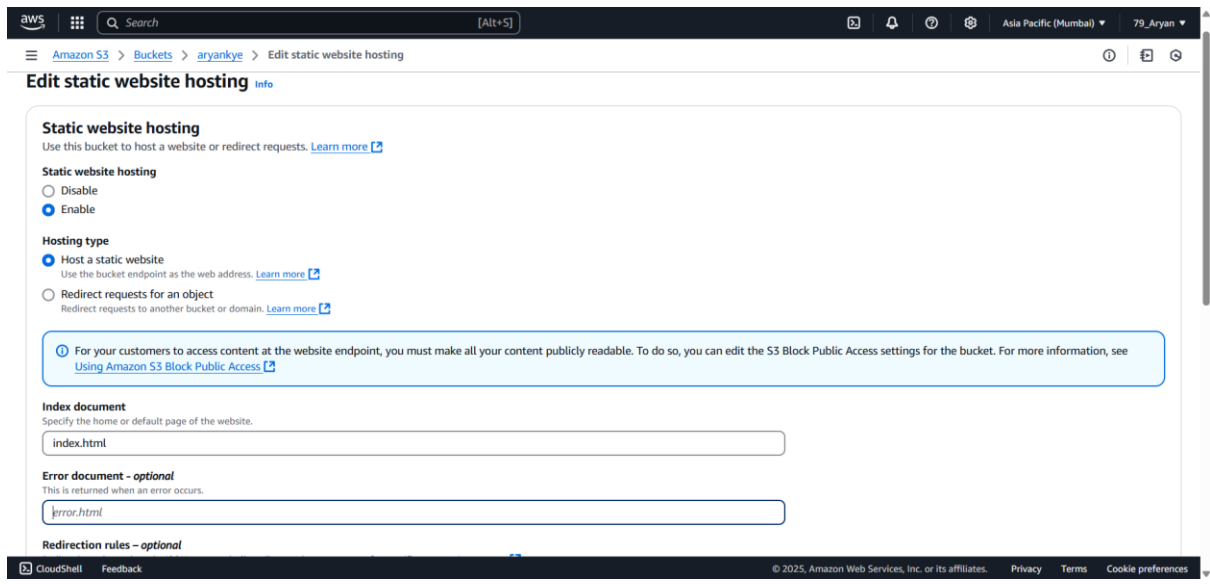Now click on the name of the created bucket.

Step-5:

Open the properties and scroll down to Static website hosting then click on edit.
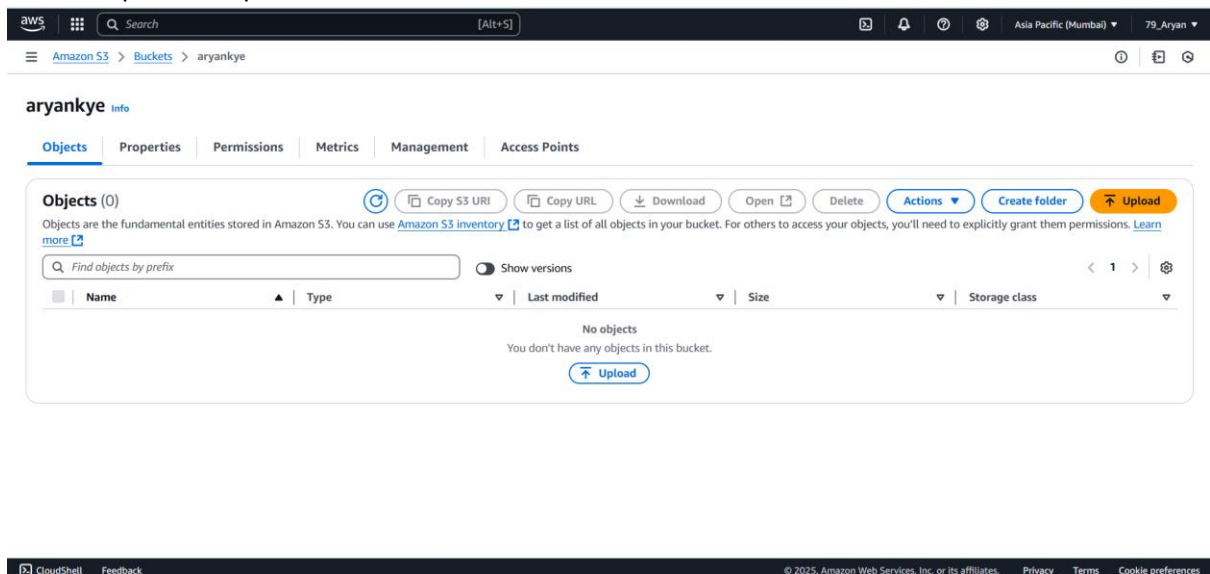
Step-5:

Click on enable and give the name of the home page in index document and Next page in error document click save changes.

Step-5:

Click on upload to upload file.

Step-6:

Select the files to be uploaded and click on open.

Step-7:

Now click on the name of the file uploaded

Step-8:

Open the permissions and edit

Step-9:

Edit the ACL set everyone to read.

Step-8:

Copy the Object URL of the home page and open it in incognito mode.

≡ Amazon S3 > Buckets > aryankye > Index.html ⓘ ⊕ ⊘

⊘ Successfully edited access control list for object "Index.html". ✕

Index.html ⓘ

Copy S3 URI | ⬇ Download | Open ↗ | Object actions ▾

Properties | Permissions | Versions

Object overview

Owner
165e2ba5238c3b02c2b0a228378c5fa236c53da722ec64dd81362a388d3d4f8c

AWS Region
Asia Pacific (Mumbai) ap-south-1

Last modified
March 27, 2025, 11:40:24 (UTC+05:30)

Size
230.0 B

Type
html

Key
⧉ Index.html

S3 URI
⧉ s3://aryankye/Index.html

Amazon Resource Name (ARN)
⧉ arn:aws:s3:::aryankye/Index.html

Entity tag (Etag)
⧉ 0fd4edf7899cb54ecec9ace3f0416789

Object URL
⧉ https://aryankye.s3.ap-south-1.amazonaws.com/Index.html

⧉ CloudShell   Feedback   © 2025, Amazon Web Services, Inc. or its affiliates.   Privacy   Terms   Cookie preferences

Step-10:

Open the permissions and click on edit.

This is a Heading

This is a paragraph.

Google Next

This is Next

This is a Next