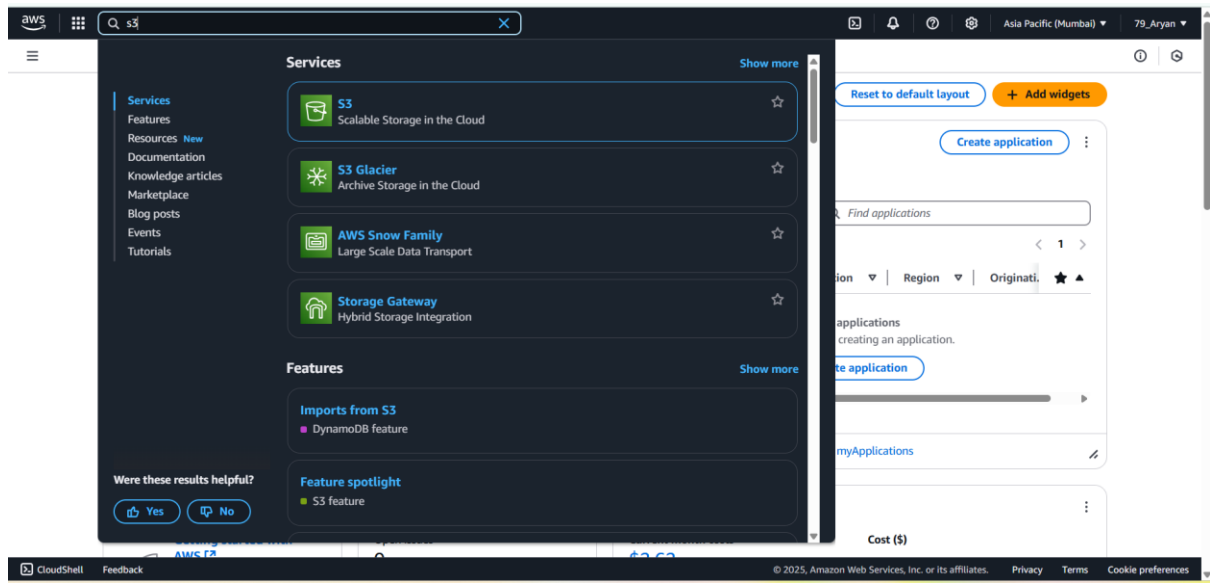


Assignment No:04

Title: Create a private bucket in in AWS. Upload a file and check whether you can access the file or not

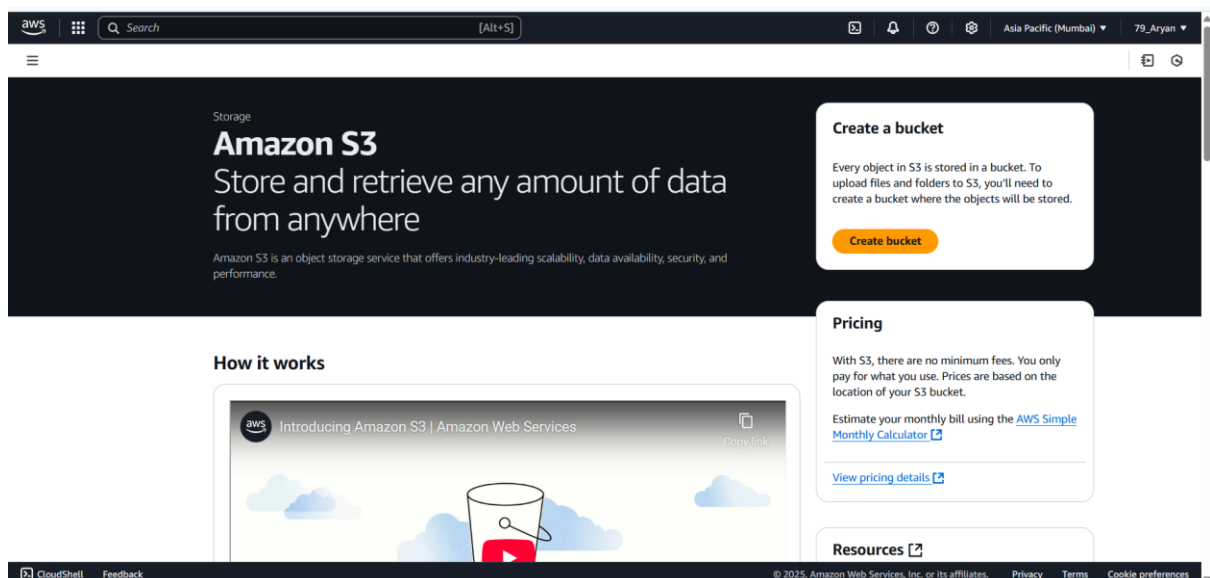
Step-1:

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.

Search

[Alt+S]

Amazon S3 > Buckets > Create bucket

(Info) [Share] [Refresh]

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](#)

aryanthree

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.

☒ 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.

[Alt+S]

[Amazon S3](#)
[Buckets](#)
[Create bucket](#)

Asia Pacific (Mumbai)
79_Aryan

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

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.

CloudShell
 [Feedback](#)

© 2025, Amazon Web Services, Inc. or its affiliates.
 [Privacy](#)
[Terms](#)
[Cookie preferences](#)

aws

Q Search

[Alt+S]

🔍 🔔 🗨️ 🌐

Asia Pacific (Mumbai) 79_Aryan

☰

Amazon S3 > Buckets > Create bucket

⌕ 🗨️

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.

[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 Amazon S3 pricing page](#)

CloudShell Feedback

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

Step-4:

Now click on the name of the created bucket.

aws Search [Alt+S] Asia Pacific (Mumbai) 79_Aryan

Amazon S3 > Buckets

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

Account snapshot - updated every 24 hours [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.

Find buckets by name

Name	AWS Region	IAM Access Analyzer	Creation date
aryanthree	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	April 8, 2025, 11:34:14 (UTC+05:30)

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

Step-5:

Click on upload to upload file.

aws Search [Alt+S] Asia Pacific (Mumbai) 79_Aryan

Amazon S3 > Buckets > aryanthree

aryanthree 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

Show versions

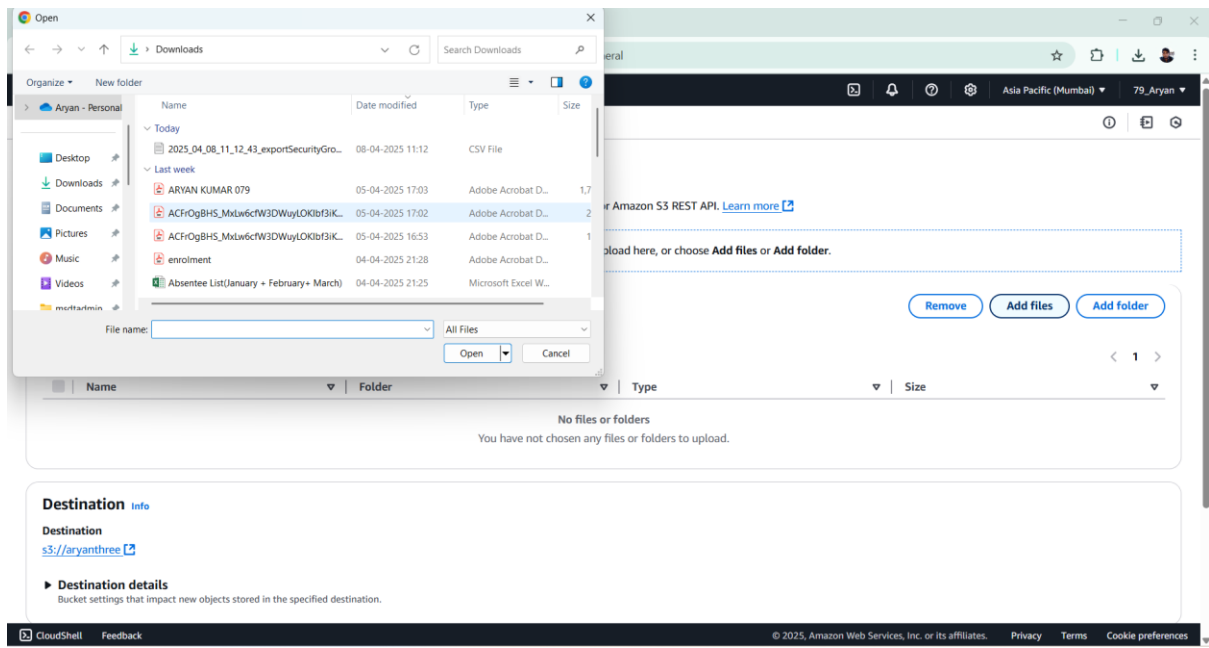
Name	Type	Last modified	Size	Storage class
No objects You don't have any objects in this bucket.				

Upload

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

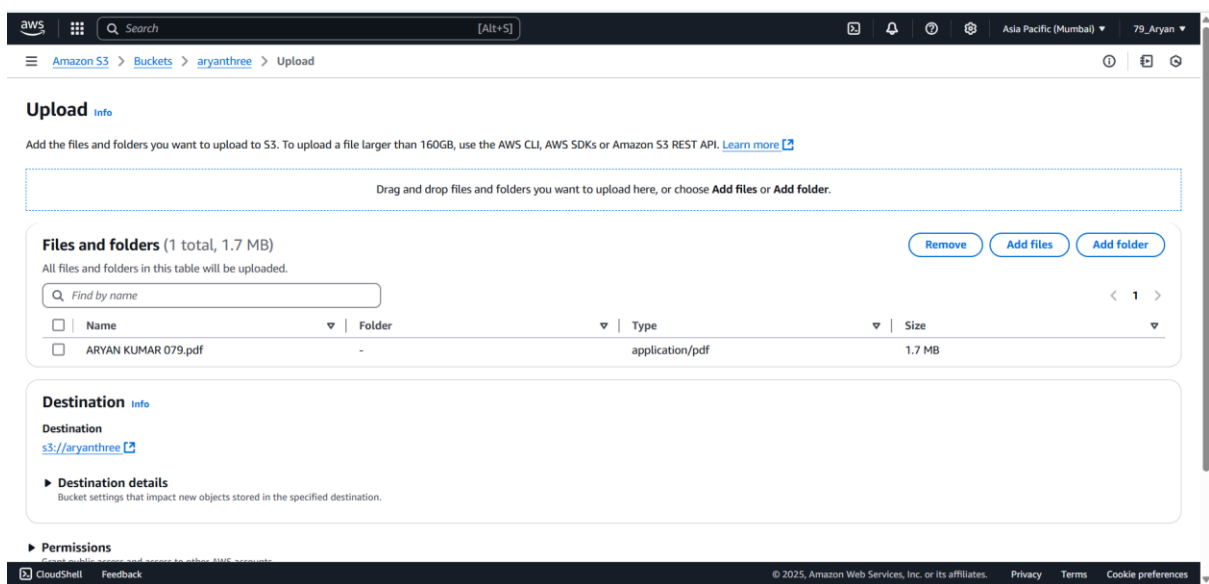
Step-6:

Select the file file to upload and click open. Then press upload



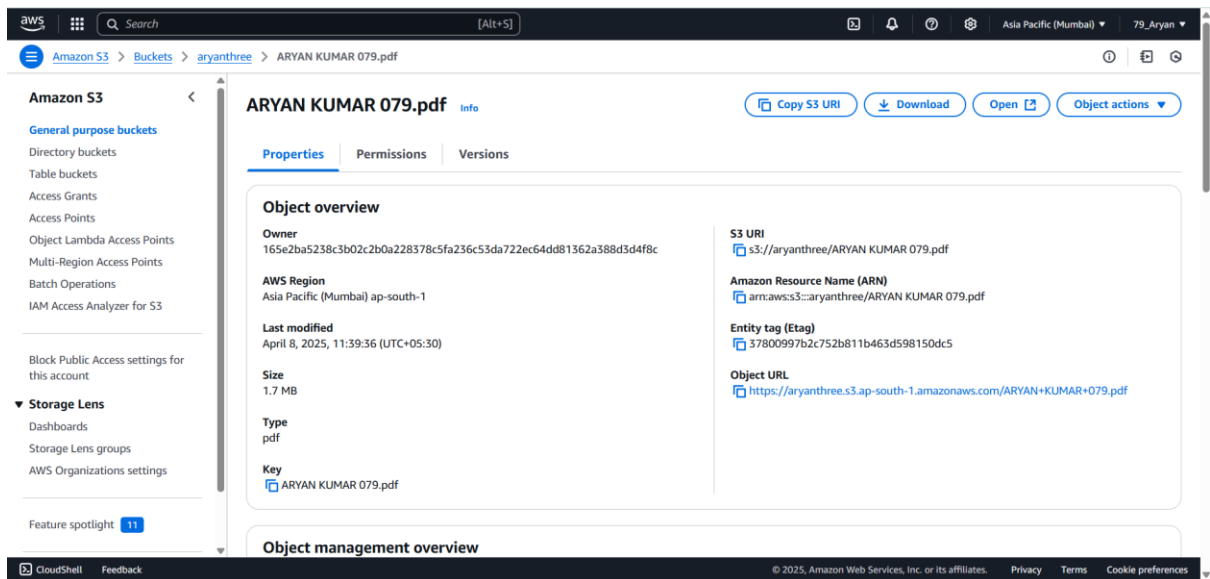
Step-7:

Now click on the name of the file uploaded



Step-8:

Copy the Object URL and open it in incognito mode.



Step-9:

The access is denied.

