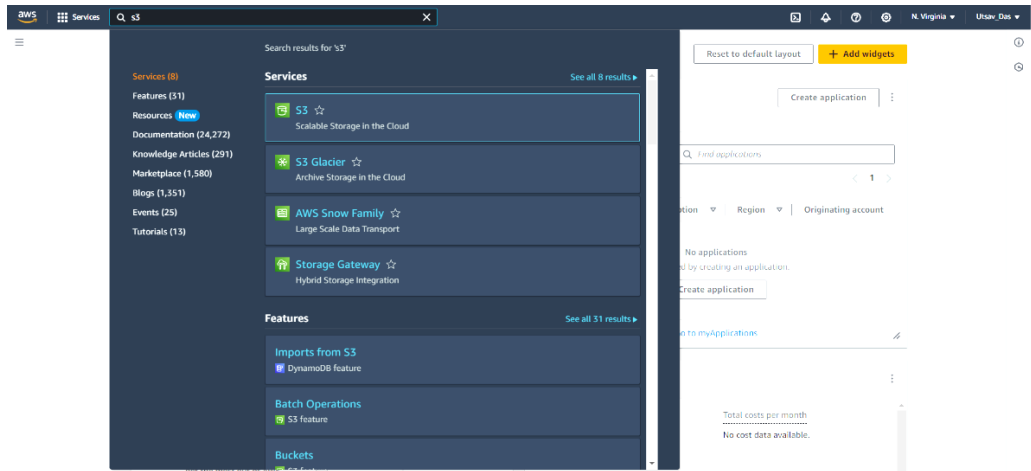


Assignment – 4

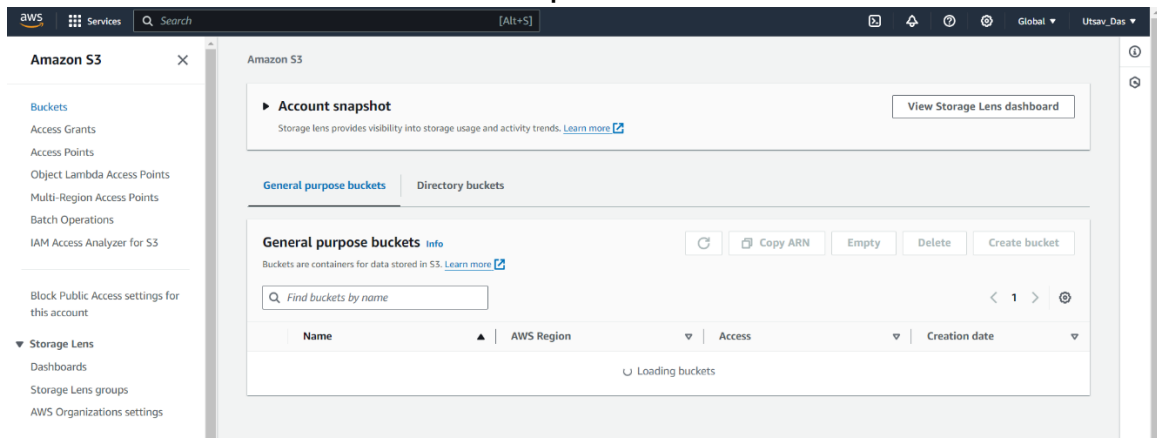
Problem Statement:

Create a private bucket in AWS Upload a file and check by reassigned URL whether you can access the file or not.

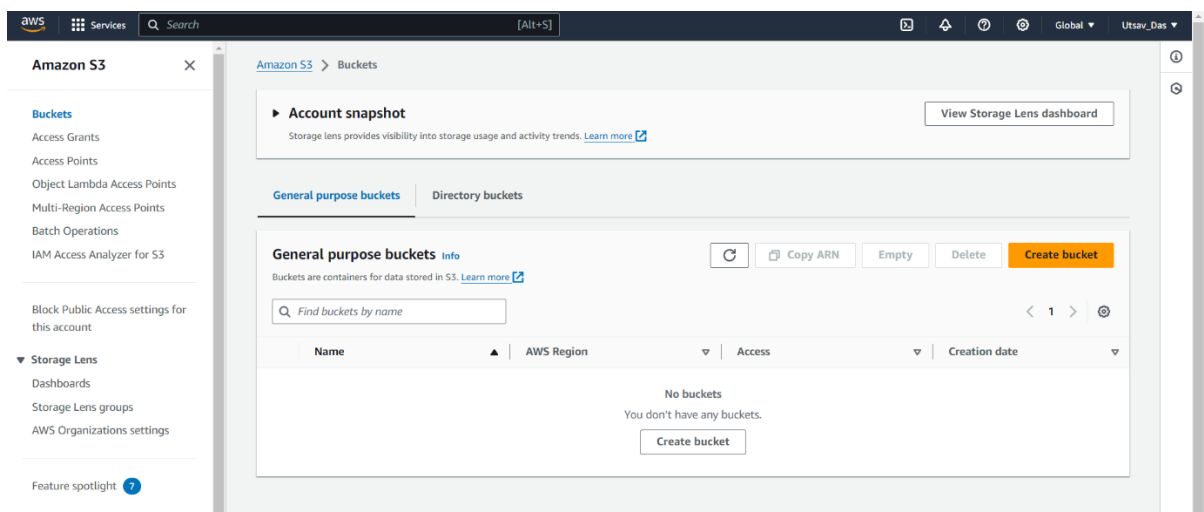
1) Search S3 in search bar and click on it.



2) Now click on Buckets in left side panel.



3) Now click on Create bucket.



- 4) Select AWS region Mumbai and give bucket name and remember this name should be unique as it is global. ACLs(Access Control List) is disabled. We have also kept 'Block all public access' checked. Now click on Create bucket.

The screenshot shows the 'Create bucket' page in the AWS Management Console. The 'General configuration' section is active, showing the 'AWS Region' set to 'Asia Pacific (Mumbai) ap-south-1' and the 'Bucket name' as 'mybucket770'. Below this, there are options for 'Copy settings from existing bucket - optional' and a 'Choose bucket' button. To the right, the 'Object Ownership' section shows 'ACLs disabled (recommended)' selected. The 'Block Public Access settings for this bucket' section has 'Block all public access' checked. At the bottom, there are 'Cancel' and 'Create bucket' buttons.

Create bucket [info](#)

Buckets are containers for data stored in S3. [Learn more](#)

General configuration

AWS Region

Asia Pacific (Mumbai) ap-south-1

Bucket name [info](#)

mybucket770

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 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)

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

Advanced settings

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

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

- 5) Click on newly created bucket.

The screenshot shows the 'Buckets' page in the AWS Management Console. A green banner at the top indicates 'Successfully created bucket "mybucket770"'. Below this, there's a 'View details' button. The 'General purpose buckets' section is active, showing a list of buckets. The newly created bucket 'mybucket770' is listed with the region 'Asia Pacific (Mumbai) ap-south-1', access 'Bucket and objects not public', and creation date 'February 18, 2024, 15:47:59 (UTC+05:30)'.

Successfully created bucket "mybucket770"

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

[View Storage Lens dashboard](#)

Account snapshot

Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

General purpose buckets | Directory buckets

General purpose buckets (1) [info](#)

Buckets are containers for data stored in S3. [Learn more](#)

[Find buckets by name](#)

Name	AWS Region	Access	Creation date
mybucket770	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	February 18, 2024, 15:47:59 (UTC+05:30)

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

- 6) Click on Upload.

The screenshot shows the 'mybucket770' page in the AWS Management Console. The 'Objects' tab is active, showing a list of objects. The 'Upload' button is visible in the top right corner of the 'Objects' section.

mybucket770 [info](#)

[Objects](#) | [Properties](#) | [Permissions](#) | [Metrics](#) | [Management](#) | [Access Points](#)

Objects (0) [info](#)

[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](#)

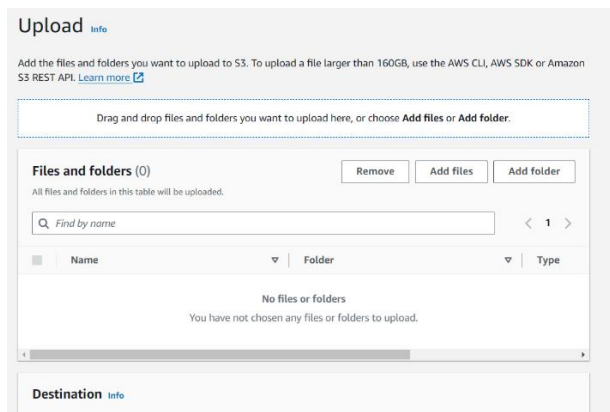
[Find objects by prefix](#)

Name	Type	Last modified	Size	Storage class
No objects				

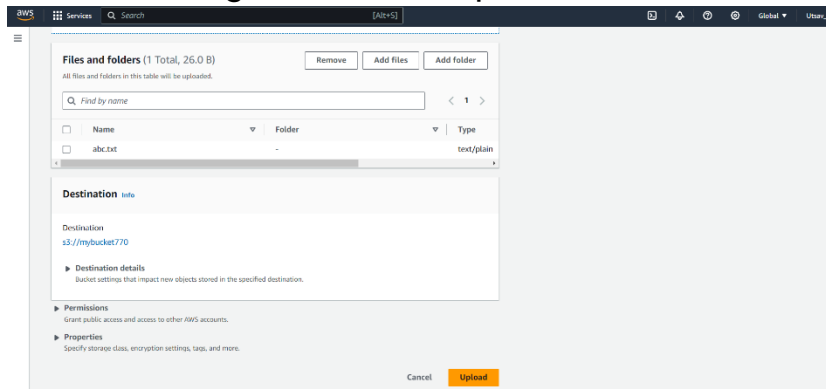
You don't have any objects in this bucket.

[Upload](#)

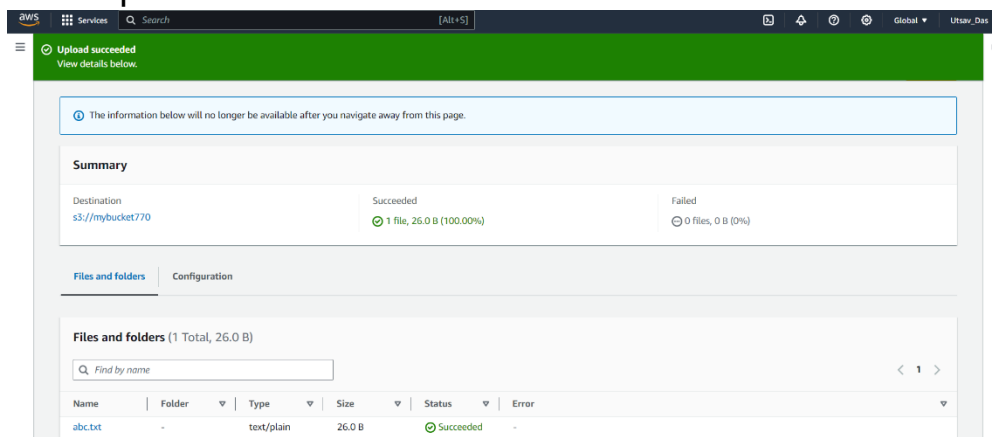
7) Click on Add files.



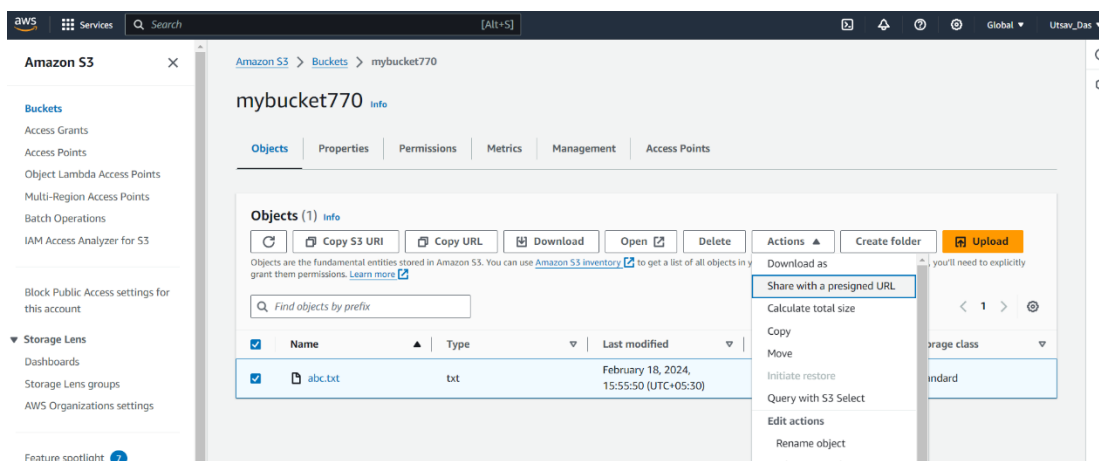
8) After selecting file click on Upload.



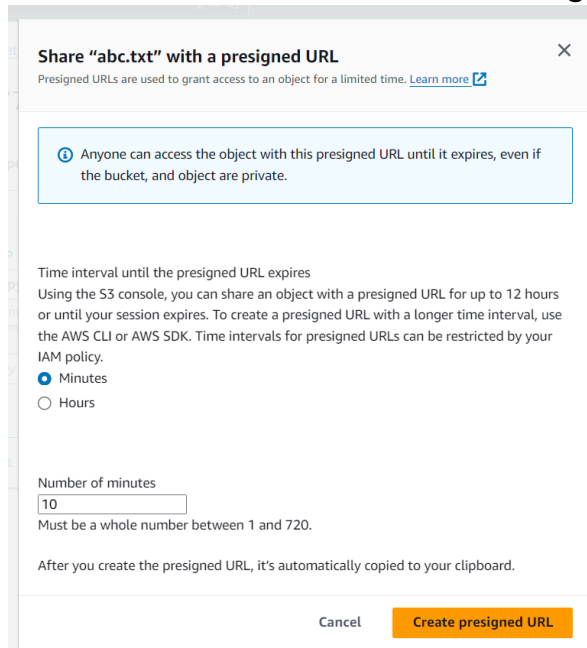
9) Now Upload has succeeded. Click on Close.



10) Go back to Buckets. Click on bucket name and click on checkbox of uploaded file name. Click on Actions dropdown and click on 'Share with a Presigned URL'.



11) Select time intervals for presigned URL as Minute. And give number of minutes and click on Create Presigned URL.



The screenshot shows the 'Share "abc.txt" with a presigned URL' dialog in the AWS S3 console. It includes a warning that anyone can access the object until it expires. The 'Time interval until the presigned URL expires' section has 'Minutes' selected. The 'Number of minutes' input field is set to '10'. At the bottom, there are 'Cancel' and 'Create presigned URL' buttons.

Share "abc.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

10

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

12) Now paste and enter this URL in new tab and as we have given 10 minutes time interval so after 10 minutes no one can access it again.



The screenshot shows a browser's address bar with a long, complex URL. The URL starts with 'https://mybucket770.s3.ap-south-1.amazonaws.com/abc.txt?' and includes various query parameters like 'response-content-disposition=inline&X-Amz-Security-Token=IQoJb3JpZ2luX2VjEBEaCmFwLXNvdXRoLTEiRzBFaIEAqDI9...'.

<Amz-Credential=ASIACTKATNUA7UBIIROE%2F20240218%2Fap-south-1%2Fs3%2Faws4_request&X-Amz-Signature=73d21ed2a6b1b173b5e8b1d7d3e89d7a638609e8d79f5afe95a7f781c3455daa|

https://mybucket770.s3.ap-south-1.amazonaws.com/abc.txt?response-content-disposition=inline&X-Amz-Security-Token=IQoJb3JpZ2luX2VjEBEaCmFwLXNvdXRoLTEiRzBFaIEAqDI9...

https://mybucket770.s3.ap-south-1.amazonaws.com/abc.txt?response-content-disposition=inline&X-Amz-Security-Token=IQoJb3JpZ2luX2VjEBEaCmFwLXNvdXRoLTEiRzBFaIEAqDI95i5kRMaqSBzQ...