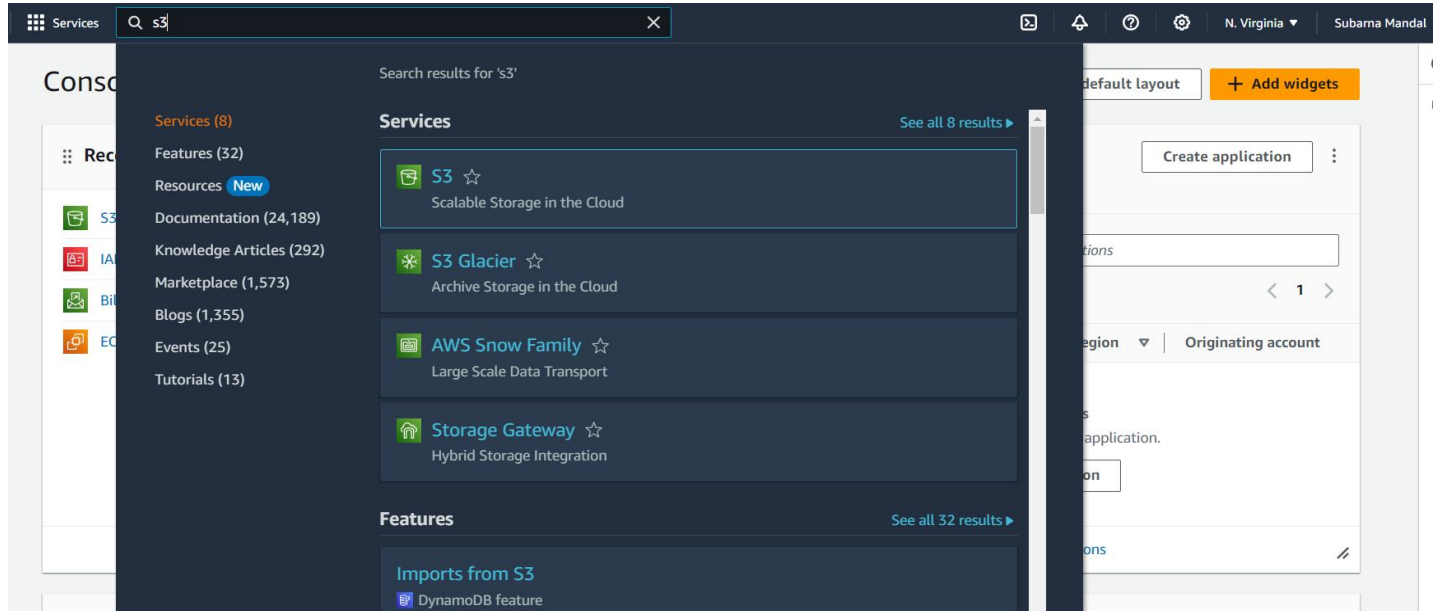


Assignment : 4

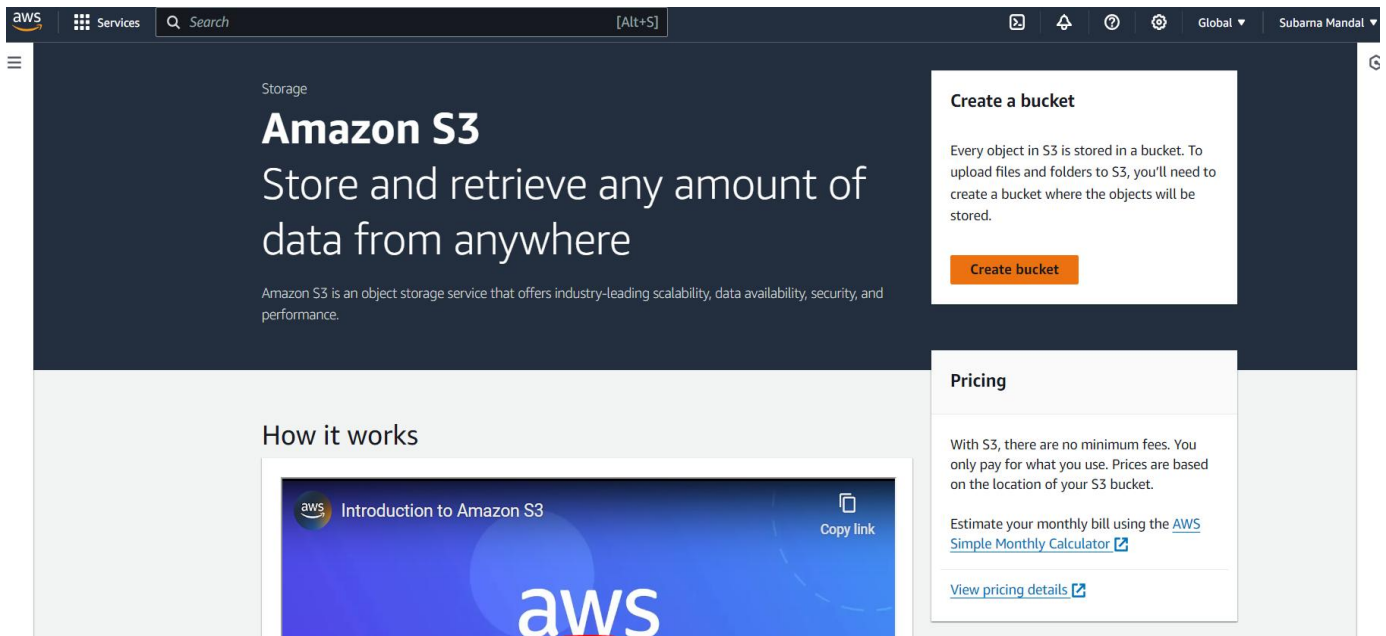
Statement : Create a private bucket in AWS. Upload a file and check by reassigned URL whether you can access the file or not.

Steps---

1. First sign in to your AWS account and search for “S3” (Simple Storage Services - where we will create the Bucket) in the search bar.



2. Now click in “Create Bucket” option.



3. Now set the configuration of the bucket -
 - i. Bucket name
 - ii. AWS Region
 - iii. Object Ownership information (ACLs disabled)
 - iv. Check all public access blockAfter filling click on “Create Bucket” option.

Create bucket

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

General configuration

AWS Region

Asia Pacific (Mumbai) ap-south-1

Bucket name

bucket1

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

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.

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

You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

No tags associated with this bucket.

Add tag

Default encryption

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type

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

4. you can see the bucket is successfully created. Next click on the <Bucket name>.

The screenshot shows the AWS Management Console interface. At the top, a green notification banner states "Successfully created bucket 'anonymous'" with a "View details" button. Below this, the breadcrumb navigation shows "Amazon S3 > Buckets". The "Account snapshot" section is visible. The "General purpose buckets" tab is selected, showing a list of buckets. The table below contains one entry:

| Name | AWS Region | Access | Creation date |
|-----------|----------------------------------|-------------------------------|--|
| anonymous | Asia Pacific (Mumbai) ap-south-1 | Bucket and objects not public | February 7, 2024, 18:01:18 (UTC+05:30) |

5. Click on the "Upload" option.

The screenshot shows the AWS Management Console interface for the "anonymous" bucket. The breadcrumb navigation shows "Amazon S3 > Buckets > anonymous". The "anonymous" bucket details page is displayed, with the "Objects" tab selected. The "Objects (0)" section shows a list of objects, but it is empty. The "Upload" button is visible in the top right corner of the "Objects" section.

6. Click "Add files" and upload a file.

The screenshot shows the AWS Management Console interface for the "anonymous" bucket. The "Add files" dialog box is open, showing a list of files and folders to be uploaded. The "Files and folders" section shows a table with one entry:

| Name | Folder | Type |
|-----------|--------|------------|
| loker.jpg | - | image/jpeg |

The "Destination" section shows the destination is "s3://anonymous". The "Permissions" and "Properties" sections are also visible. The "Upload" button is at the bottom right.

7. File is uploaded. Now click on the <uploaded file name >

Upload: status

The information below will no longer be available after you navigate away from this page.

Summary

| | | |
|-------------------------------|--|-----------------------------|
| Destination s3://anonymous | Succeeded 1 file, 41.5 KB (100.00%) | Failed 0 files, 0 B (0%) |
|-------------------------------|--|-----------------------------|

Files and folders (1 Total, 41.5 KB)

| Name | Folder | Type | Size | Status | Error |
|-----------|--------|------------|---------|-----------|-------|
| joker.jpg | - | image/jpeg | 41.5 KB | Succeeded | - |

8. Copy the object URL from this .

joker.jpg

Object overview

| | |
|---|---|
| Owner 216e13a6df37bc01c1f68de70f85823cfa478d84dc4a1532d9a5017cb9ce6bb2 | S3 URI s3://anonymous/joker.jpg |
| AWS Region Asia Pacific (Mumbai) ap-south-1 | Amazon Resource Name (ARN) arn:aws:s3:::anonymous/joker.jpg |
| Last modified February 7, 2024, 18:10:09 (UTC+05:30) | Entity tag (Etag) 7f479e500e2acaffb5dc467eba4f830 |
| Size 41.5 KB | Object URL https://anonymous.s3.ap-south-1.amazonaws.com/joker.jpg |
| Type jpg | |
| Key joker.jpg | |

9. Open the URL in another browser. It will show access denied.

anonymous1.s3.ap-south-1.ama

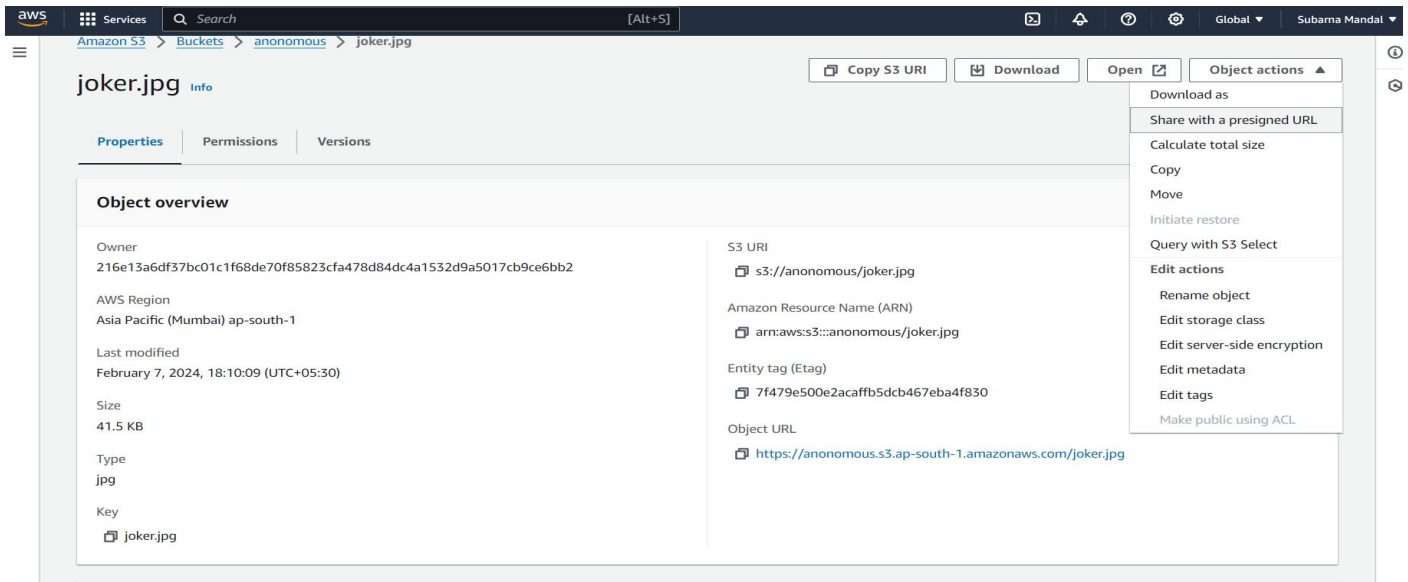
Settings

https://anonymous1.s3.ap-south-1.amazonaws.com/WhatsApp+Image+2024-02-04+at+00.27.41_599b46e1.jpg

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<?xml version="1.0" encoding="UTF-8" ?>
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>82T7FYTEQWHY75Y6</RequestId>
  <HostId>pSNqw6YhxXdDGPRtH51TkrI6c4hSW/bQ3DwSu0Hxc60iQNZe+ErVEN934+ tq1w/nzN7NsFT1IdM2f9mOQJQug==</HostId>
</Error>
```

10. Now click on “Object actions” and select “Share with a presigned URL” option.



11. Now set the number of minutes (here 1 minutes) and click on “Create presigned URL”.

Share “joker.jpg” 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

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. Next copy the Presigned URL and paste it on another browser. The file will be visible for the given time.

