

Assignment – 4

Problem Statement: -

Create a Private Bucket in AWS. Upload a file & checked by presigned URL that you access or not.

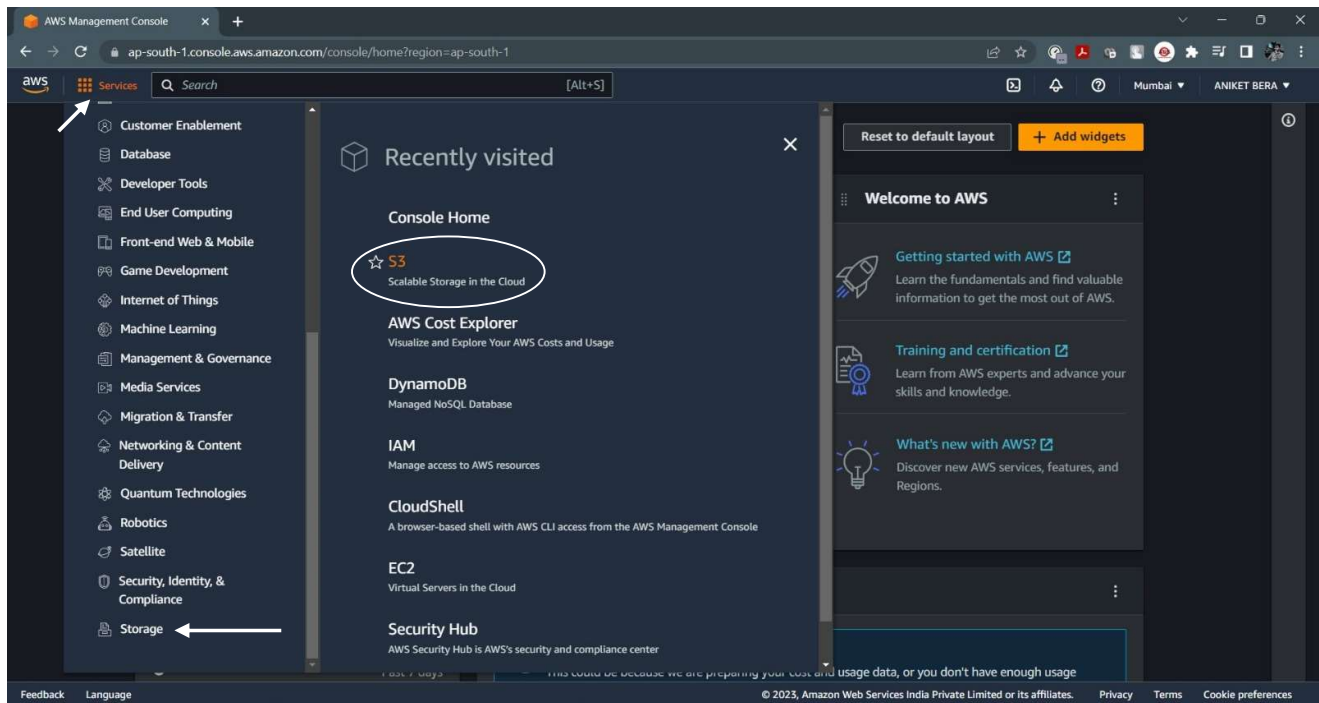
Steps for create a Private Bucket & check uploaded file presigned URL: -

1. Open the **Amazon Web Services** (<https://aws.amazon.com/console/>) home page.
2. Log in your **AWS Management Console** account.
3. Go **Services** and click on **Storage**.
4. Next go to **S3** (*Scalable Storage in the Cloud*).
5. Now click on **Create bucket**.
6. In **General configuration** give a **Bucket name**, choose **ACLs disabled**, **Block all public access** and no need to change rest of the configuration (default setting).
7. **Complete Private Bucket creation**.
8. Now double click on *private bucket name*.
9. For uploading a file in bucket go **Upload** option.
10. After that open an upload window; then **Add files** and continue with **Upload** option.
11. **Complete file uploading**.
12. Now double click on uploaded file; go **Object actions** then click on **Share with a Presigned URL**. Set *time interval until the presigned URL expires* and continue with **Create presigned URL**.
13. Now copy object URL and paste it another web browser (incognito mode option is better for testing the URL).

Observation: -

URL shows “**This XML file does not appear to have any style information associated with it. The document tree.**”. File content can't access.

Some snapshots of above process: -



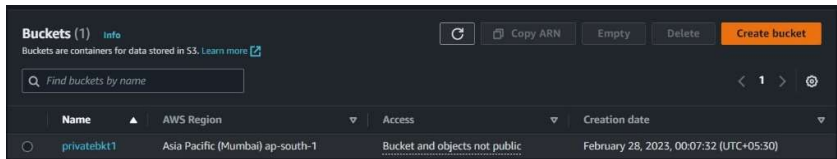
Step 1: Go **Services** -> **Storage** -> **S3**

Create a bucket

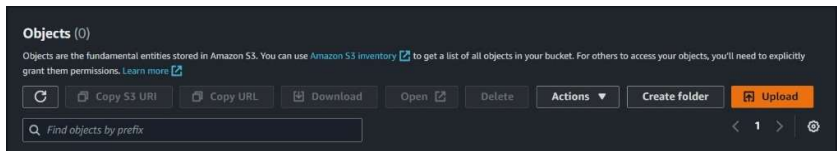
Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.

Create bucket

Step 2: Create bucket



Step 4: Complete Private Bucket creation



Step 5: Upload a file

Amazon S3 > Buckets > Create bucket

Create bucket Info

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

General configuration

Bucket name

Bucket name must be globally unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

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

Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.
Choose bucket

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

Upcoming permission changes to disable ACLs
Starting in April 2023, to disable ACLs when creating buckets by using the S3 console, you will no longer need the `s3:PutBucketOwnershipControls` permission. [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 is 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.

Upcoming permission changes to enable all Block Public Access settings
Starting in April 2023, to enable all Block Public Access settings when creating buckets by using the S3 console, you will no longer need the `s3:PutBucketPublicAccessBlock` permission. [Learn more](#)

Cancel Create bucket

Step 3: Configuration of bucket

Amazon S3 > Buckets > privatebkt1 > Upload

Upload Info

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose **Add files**, or **Add folders**.

Files and folders (0)

All files and folders in this table will be uploaded.

<input checked="" type="checkbox"/>	Name	Folder	Type	Size
<input checked="" type="checkbox"/>	Assignment1.pdf	-	application/pdf	976.3 KB

Destination

Destination
`s3://privatebkt1`

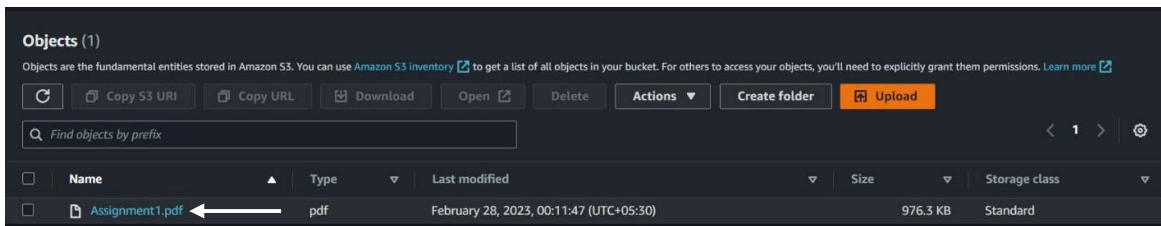
Destination details
Bucket settings that require new objects stored in the specified destination.

Permissions
Grant public access and access to other AWS accounts.

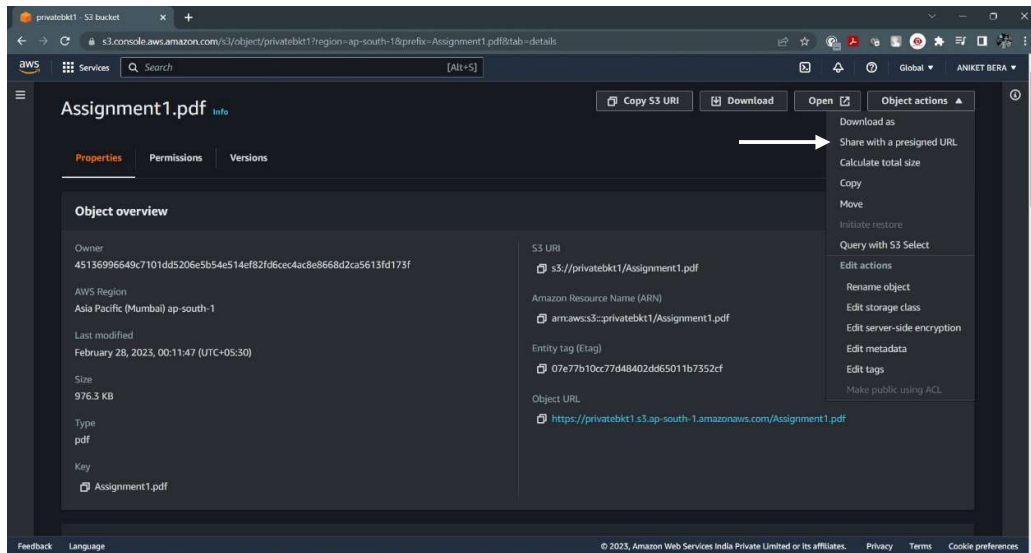
Properties
Specify storage class, encryption settings, tags, and more.

Cancel Upload

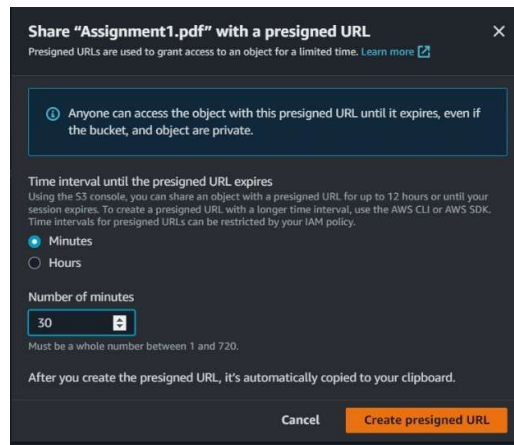
Step 6: Add files & upload



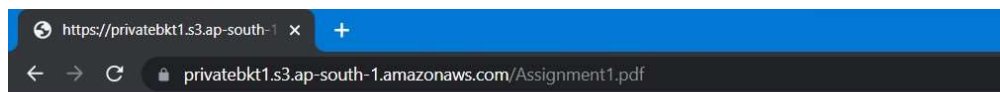
Step 7: Double click on uploaded file



Step 8: Share with a presigned URL



Step 9: Set time interval of presigned URL



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>Z5F7HR4B6SAYZD0K</RequestId>
  <HostId>D3ncITzFxi0DW2saifgilcoNwHmbV89CD++fTPTaEkjw0jz5nJrNjIyNPChemDeCsyhSSiusa+c</HostId>
</Error>
```

Step 10: Copy & paste object URL