**Placement Empowerment Program**

***Cloud Computing and DevOps Centre***

**Using Cloud Storage**

Create a storage bucket on your cloud platform and upload/download files. Configure access permissions for the bucket.

Name: SIVAKUMAR C Department: AML



**Introduction and Overview**

Cloud storage services, like AWS S3 (Simple Storage Service), offer scalable, secure, and cost-effective solutions for storing and managing data. S3 provides a variety of features, including the ability to upload, download, and configure access control for files. This document outlines the process of creating an S3 bucket in AWS, uploading and downloading files, and configuring permissions to secure access to the stored data.

**Objectives**

* To create a storage bucket in AWS S3.
* To upload and download files to/from the S3 bucket.
* To configure access permissions for the S3 bucket to control who can access the stored data.

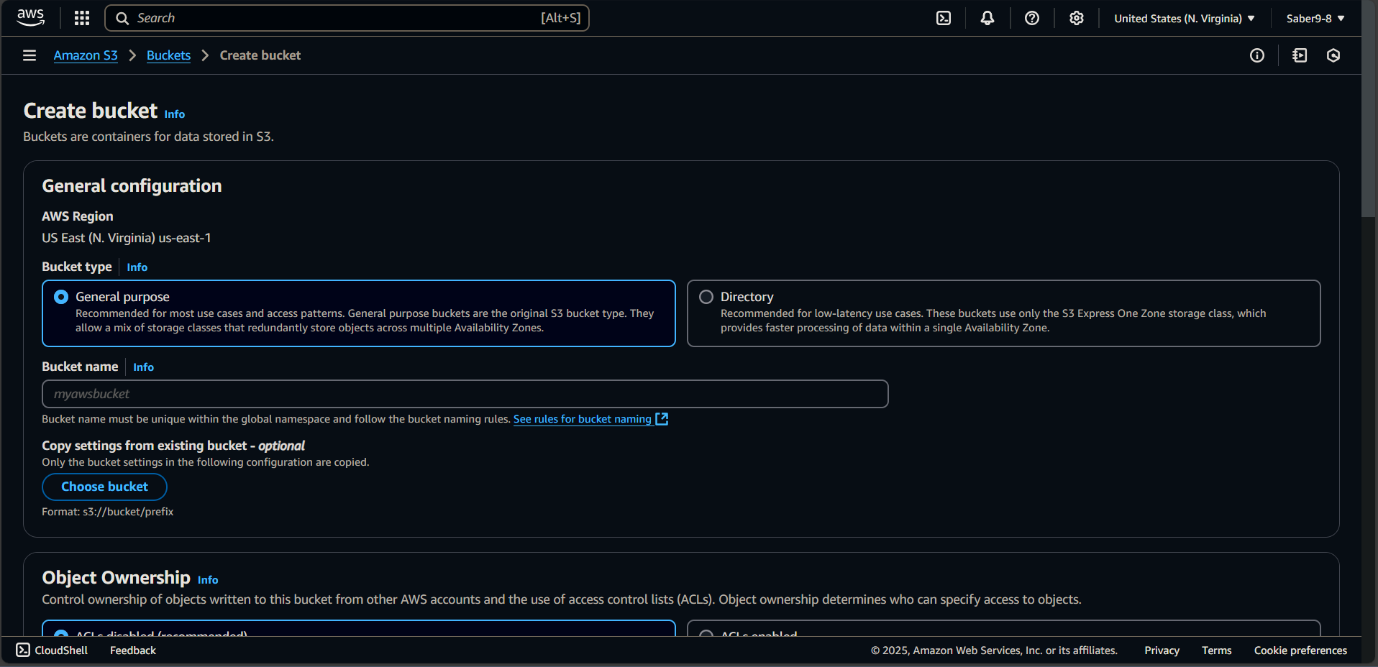
**Importance**

* **Scalability:** AWS S3 offers infinite scalability for storing data, enabling businesses to store vast amounts of information without worrying about running out of space.
* **Accessibility:** Files stored in S3 can be accessed from anywhere, making it ideal for cloud-based applications and backup solutions.
* **Security:** With S3’s access control mechanisms, you can ensure that only authorized users or applications can access your data.
* **Cost-Effectiveness:** AWS S3 uses a pay-as-you-go pricing model, allowing users to pay only for what they use, making it highly cost-effective for large-scale storage needs.
* **Data Durability:** AWS S3 offers 99.999999999% durability, ensuring that your data is safe and protected from failure.

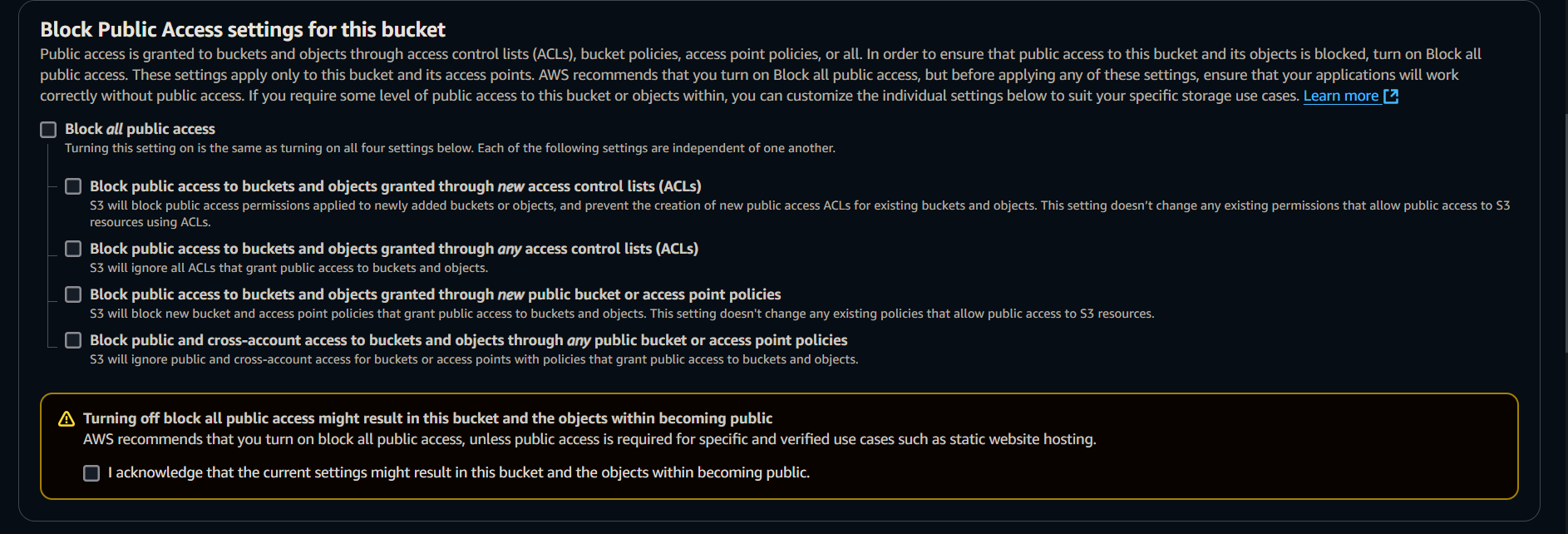
**STEPS:**

**STEP 1: Create a Storage Bucket in AWS S3**

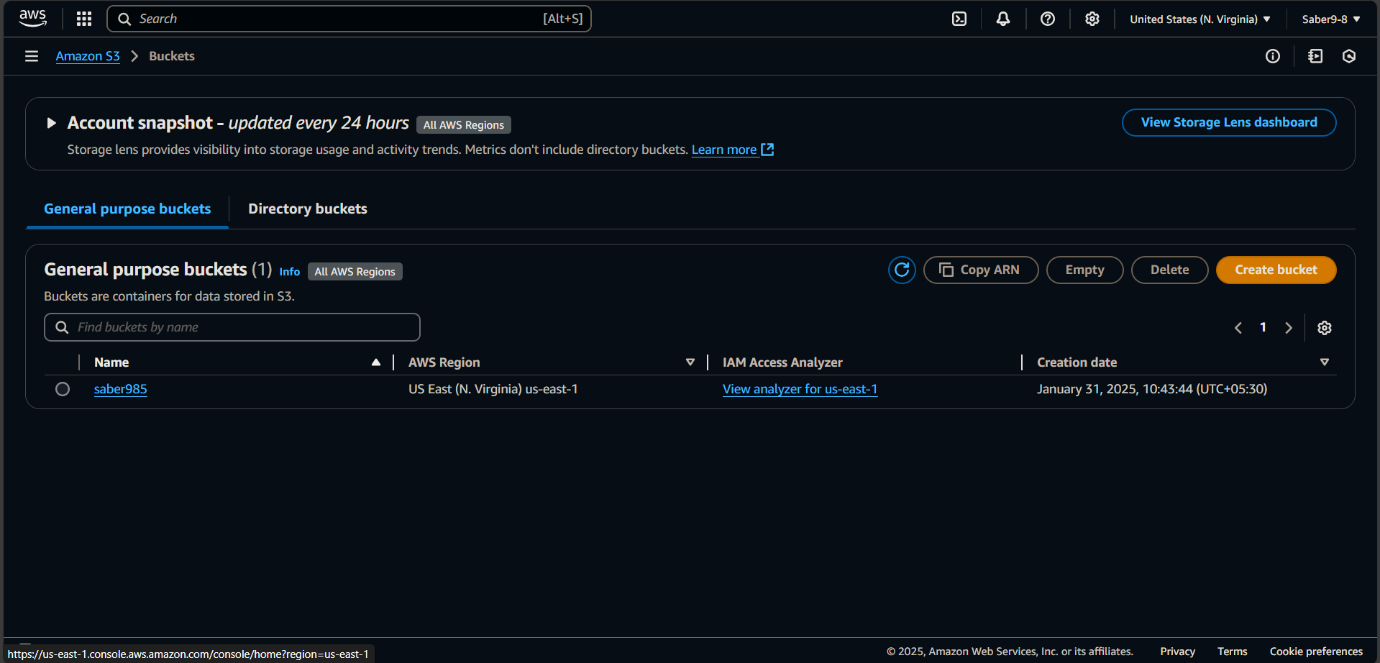
* Log in to the AWS Management Console and navigate to the S3 Dashboard.
* Click Create Bucket to start the process.



* Bucket Name: Enter a unique name for the bucket (e.g., my-example-bucket).
* Region Selection: Choose the AWS region where the bucket will be created (e.g., US East (N. Virginia)).
* Configure Options: Configure options like versioning, logging, and encryption if necessary.

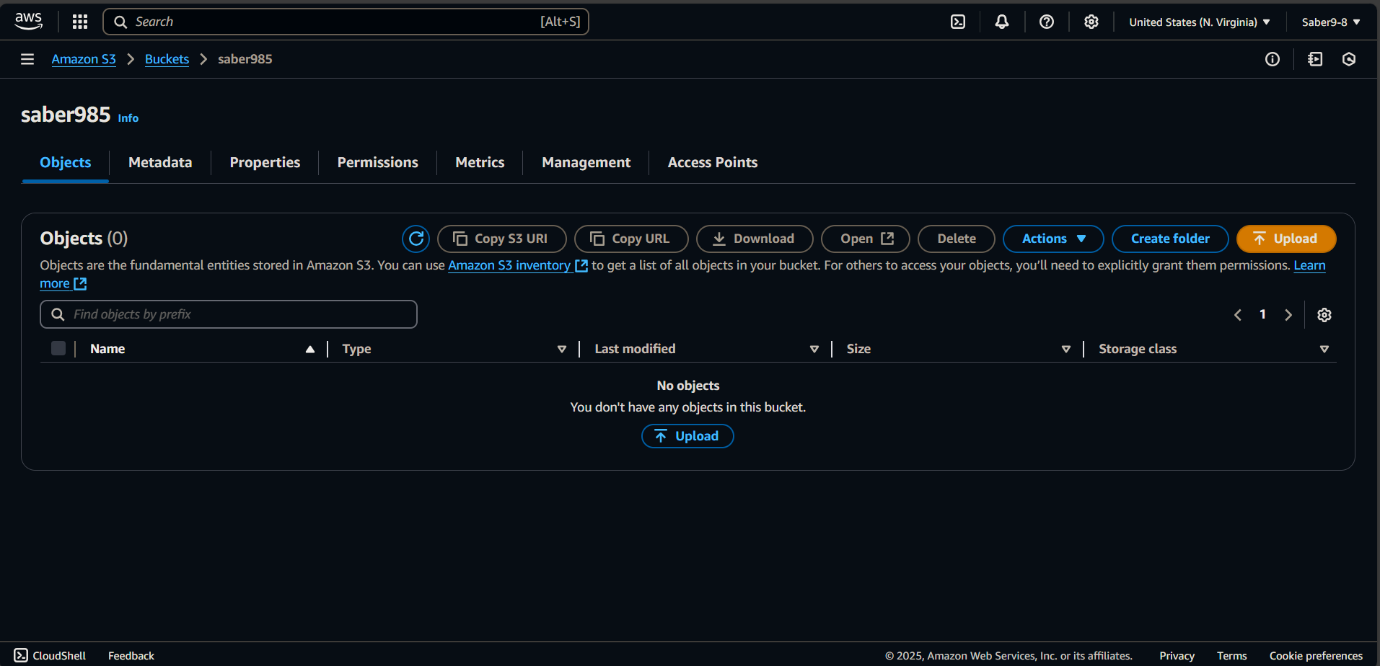


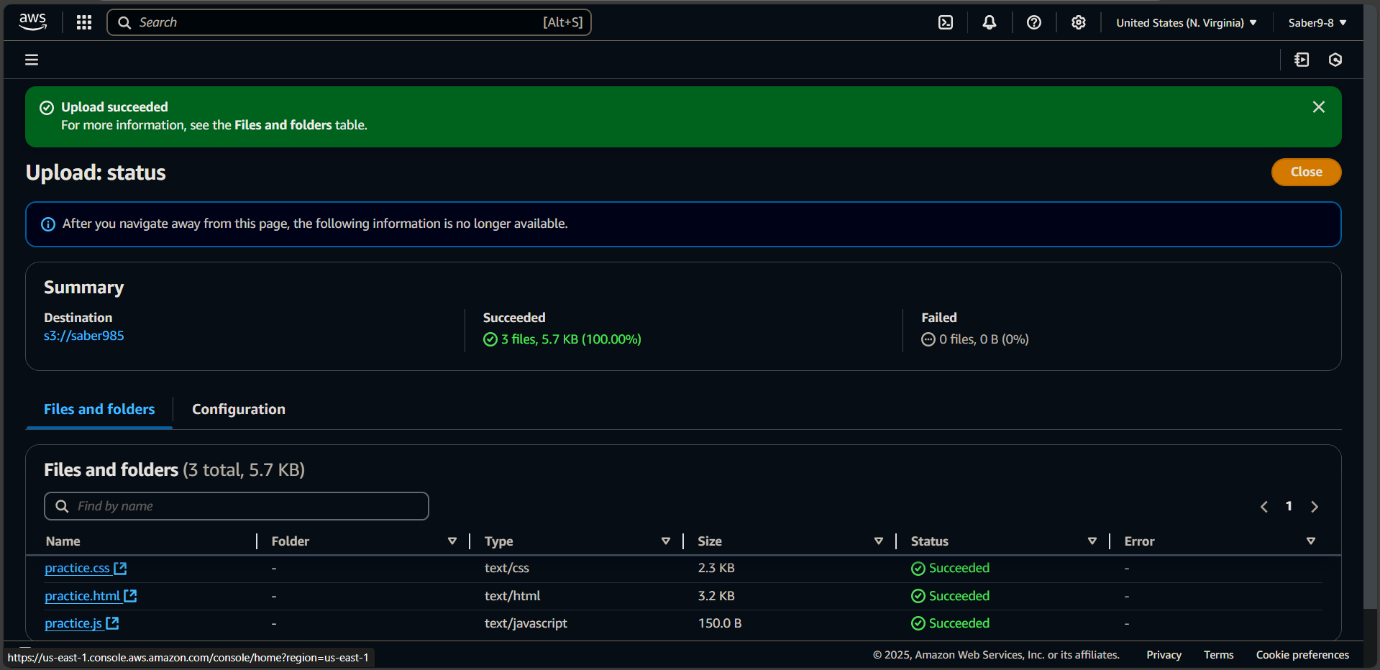
* Set Permissions: Ensure the correct permissions are set during the bucket creation. You can leave the default settings or adjust them based on your security needs.
* Click Create to complete the bucket creation process.



**STEP 2: Upload Files to the S3 Bucket**

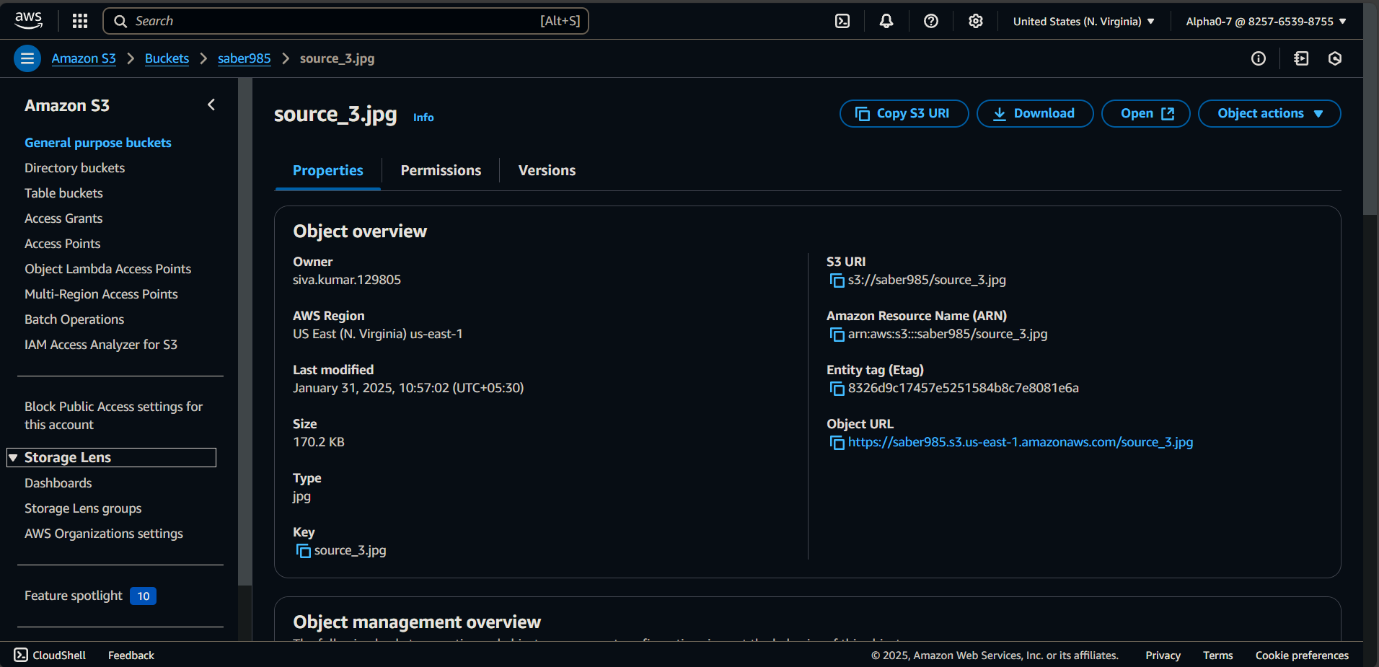
* Navigate to the S3 Dashboard, then select the bucket you just created.



* Inside the bucket, click the Upload button.
* Select Add Files and choose the files you want to upload from your local system.
* After selecting the files, click Upload to start the upload process. 
* You’ll see a progress bar that indicates the upload status. Once completed, the files will be stored in the bucket.

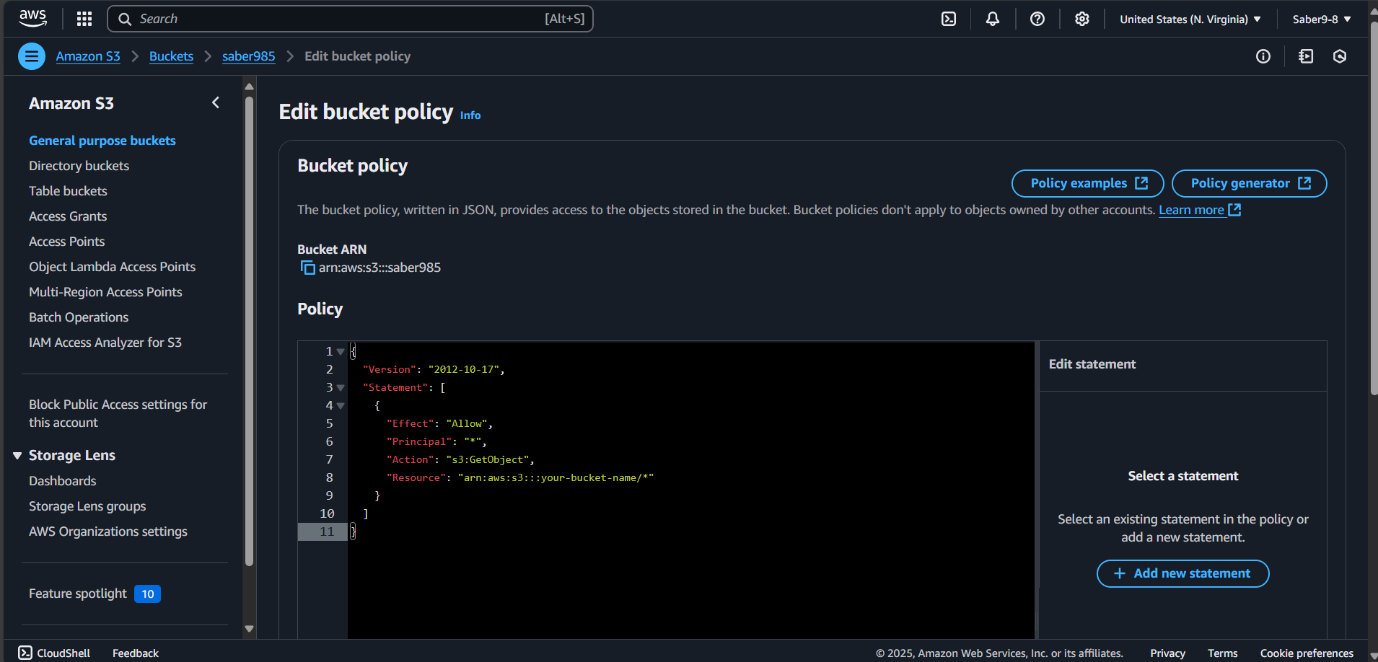
**STEP 3: Download Files from the S3 Bucket**

1. In the **S3 Dashboard**, go to the bucket that contains the files you want to download.
2. Browse through the files, and click the **checkbox** next to the file you want to download.
3. Click **Download** to download the selected file to your local system.



**STEP 4: Configure Access Permissions for the S3 Bucket**

* In the S3 Dashboard, select the bucket you want to configure access permissions for.
* Go to the Permissions tab in the bucket details.
* Bucket Policy:
  1. You can configure bucket-wide permissions by adding a bucket policy. Click Bucket Policy and write a JSON policy that defines who can access the bucket and what actions they can perform (e.g., read, write).



**STEP 5: Test Access Permissions**

* After configuring the permissions, test the access control by trying to open the file using the object URL.
* Ensure that only the intended users have the appropriate access.

