

Placement Empowerment Program

Cloud Computing and DevOps Centre

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

Name: Mohana Priya M

Department: CSE

Introduction

This Proof of Concept (PoC) demonstrates the use of **AWS S3 (Simple Storage Service)** to create a storage bucket, upload and download files, and configure access permissions for secure file sharing. AWS S3 is a highly scalable and durable cloud storage service that enables users to store large amounts of data with high availability and low latency. This PoC walks through the essential tasks of working with S3, providing hands-on experience for managing cloud storage.

Overview

AWS S3 is a widely used cloud storage service offered by Amazon Web Services that allows users to store, manage, and retrieve data objects at scale. The storage structure is based on **buckets** where data is stored in the form of **objects**. This PoC focuses on creating an S3 bucket, uploading files to the bucket, downloading files, and configuring access controls to manage who can access the data stored in the bucket.

The process involves:

- 1. Creating an S3 bucket:** A container that holds data objects.
- 2. Uploading files:** Storing files (like documents, images, or any binary data) in the S3 bucket.
- 3. Downloading files:** Retrieving data from the S3 bucket to local systems.
- 4. Configuring access permissions:** Managing security through access policies, including making files publicly accessible or securing them for private access.

Objectives:

The primary objectives of this PoC are:

- 1. Learn how to create and manage S3 storage buckets:** Understand how to set up a cloud storage solution.
- 2. Upload and download files:** Get hands-on experience with managing data in the cloud by transferring files to and from S3.
- 3. Configure access permissions:** Explore how to manage access to the S3 bucket, including setting public or private access levels to the data stored.
- 4. Understand the key features of AWS S3:** Familiarize with the fundamental concepts of AWS S3, such as durability, scalability, and security.

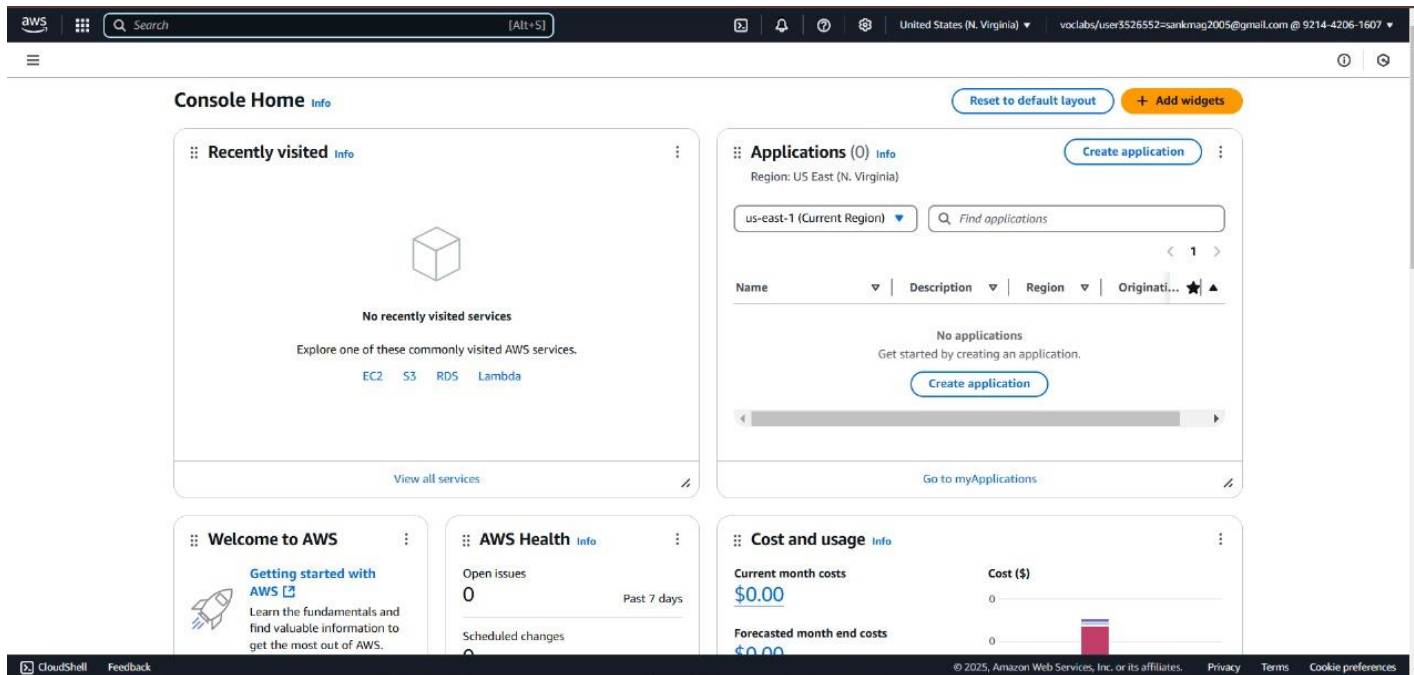
Importance:

- 1. Scalable Storage:** AWS S3 allows users to store large amounts of data without worrying about capacity limitations.
- 2. Cost-Effective:** With a pay-as-you-go pricing model, it's affordable and only charges for the storage used.
- 3. High Durability:** S3 ensures 99.999999999% durability, making it ideal for backup and disaster recovery.
- 4. Security:** Provides strong access controls via IAM, bucket policies, and encryption to secure data.
- 5. Global Access:** Enables easy access to data from anywhere in the world, supporting remote work and global operations.

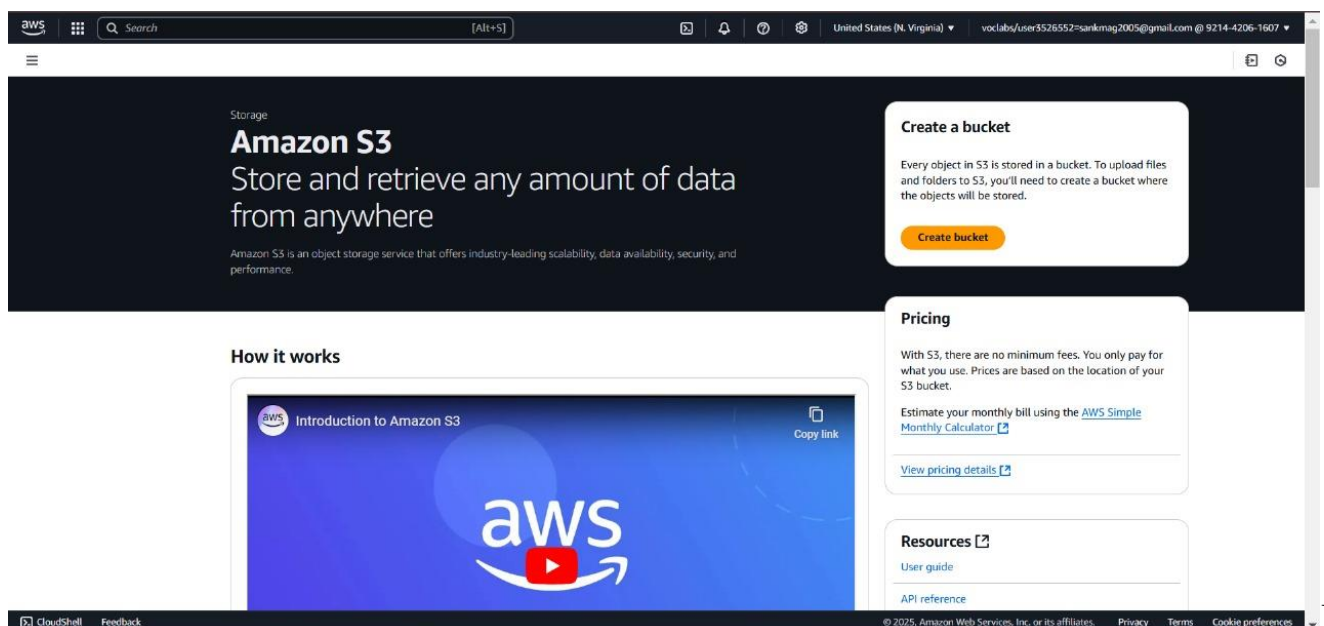
Step-by-Step Overview:

Step 1:

1. Go to [AWS Management Console](#).
2. Enter your username and password to log in.



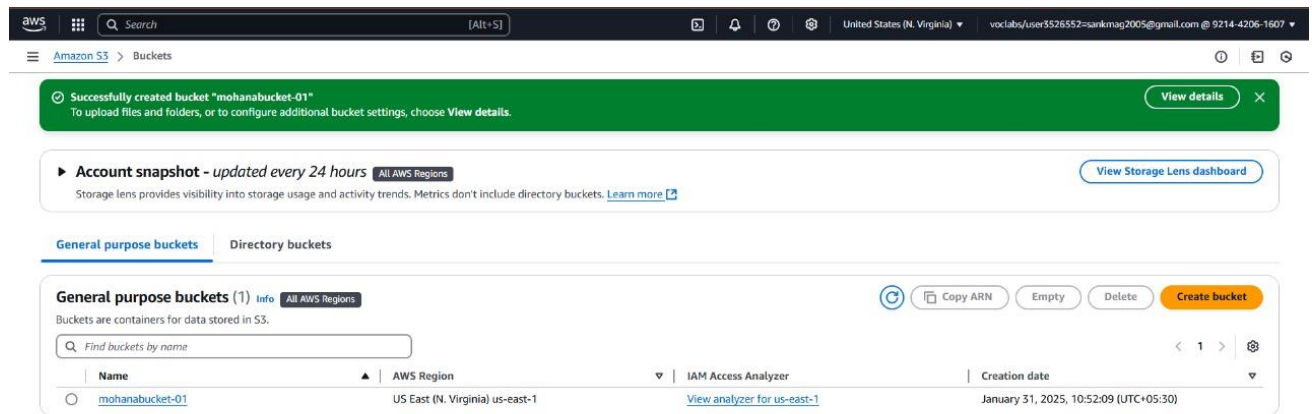
Step 2:



In the top search bar, type **S3** and select it from the search results.

Step 3:

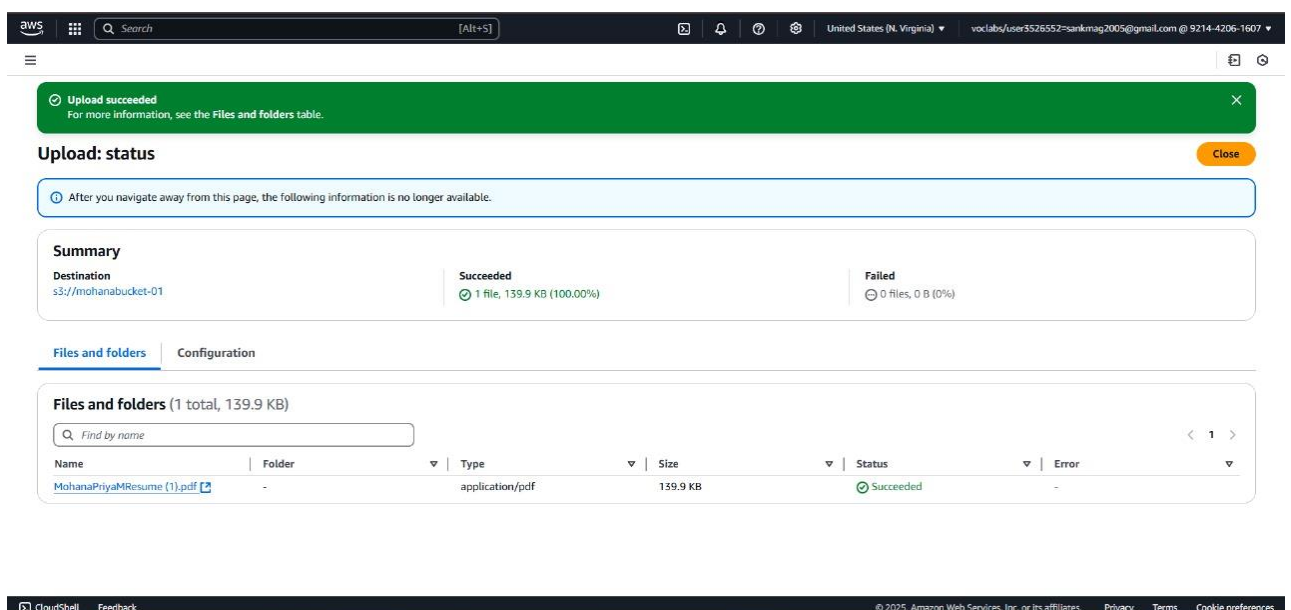
Click **Create bucket**.



Bucket name: Enter a unique name (e.g., mohana-s3-poc). Leave other settings as default (you can modify later).

Step 4:

Select your bucket from the list and Click **Upload** → **Add files**.



Choose the file(s) you want to upload from your local machine and Click **Upload**.

Step 5:

Navigate to the uploaded file inside your bucket.

Upload: status

After you navigate away from this page, the following information is no longer available.

Summary

Destination	Succeeded	Failed
s3://mohanabucket-01	1 file, 139.9 KB (100.00%)	0 files, 0 B (0%)

Files and folders (1 total, 139.9 KB)

Name	Folder	Type	Size	Status	Error
MohanaPriyaMResume (1).pdf	-	application/pdf	139.9 KB	Succeeded	-

Select the file and click **Download** from the **Actions** menu (or click the file name to download directly).

Step 6:

Navigate to the uploaded file. Click the file name → Go to the **Permissions** tab. Under **Public access**, click **Edit** → Enable public access → Save changes.

Block Public Access settings for this account

Use Amazon S3 Block public access settings to control the settings that allow public access to your data.

Block Public Access settings for this account

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 all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply account-wide for all current and future buckets and 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 your buckets or objects, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block all public access

- ☐ Off
- ☐ Block public access to buckets and objects granted through **new** access control lists (ACLs)
- ☐ Off
- ☐ Block public access to buckets and objects granted through **any** access control lists (ACLs)
- ☐ Off
- ☐ Block public access to buckets and objects granted through **new** public bucket or access point policies
- ☐ Off
- ☐ Block public and cross-account access to buckets and objects through **any** public bucket or access point policies
- ☐ Off

Step 7:

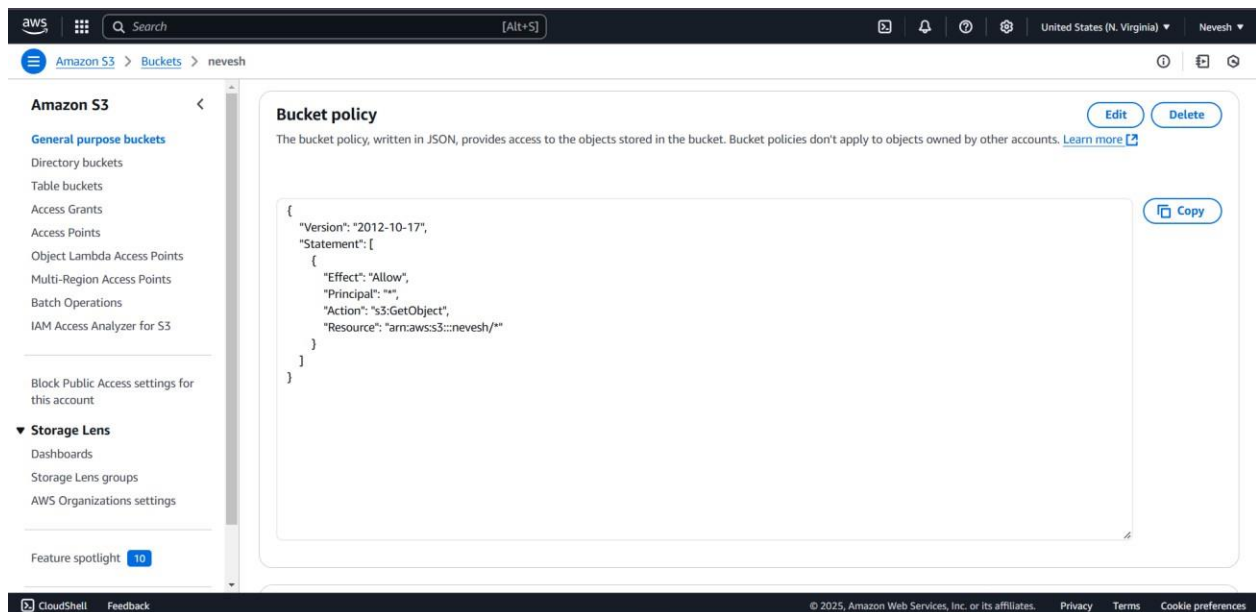
Go to the **Permissions** tab of your bucket.

Scroll down to **Bucket Policy** and click **Edit**.

Add the following example policy to make all files in the bucket publicly accessible:

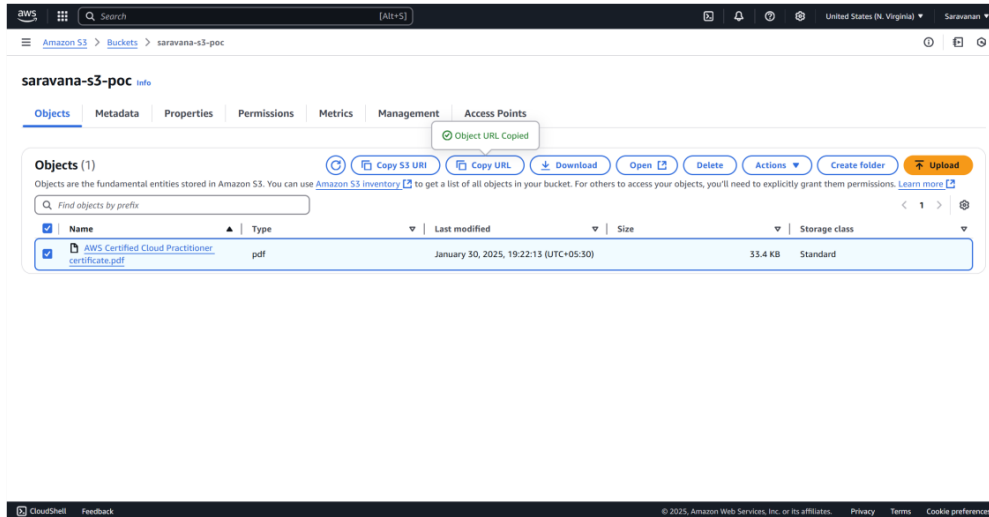
Replace YOUR_BUCKET_NAME with your bucket name.

Save the policy.



Step 8:

Copy the Url in Copy URL option



Step 9:



Paste the link in the new tab and you can see the uploaded file.

Outcomes:

By completing this PoC of setting up an S3 bucket, uploading/downloading files, and configuring access permissions, you will:

- 1. Create and Manage an S3 Bucket:** Learn how to set up an S3 bucket for storing and managing objects in the cloud.
- 2. Upload and Download Files:** Gain hands-on experience in transferring files to and from the cloud securely and efficiently.
- 3. Configure Access Permissions:** Understand how to apply bucket policies and permissions to control access to your data.
- 4. Enhance Data Security:** Implement best practices for securing your data using AWS S3's access controls and encryption options.
- 5. Experience AWS S3 Features:** Explore key S3 capabilities such as scalability, durability, and accessibility for real-world applications.

This PoC will provide a solid foundation for working with AWS S3 and understanding its role in modern cloud architectures.