

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: HARSHINI A

Department: CSE

Introduction

In this (PoC), we will explore AWS S3 (Simple Storage Service) to understand its functionality as a reliable cloud storage solution. The task involves creating an S3 bucket, uploading and downloading files, and configuring access permissions to manage who can access the stored data. This PoC demonstrates S3's versatility in securely storing and retrieving files, both publicly and privately. We will also set bucket policies to control access and test public URLs for hosted files. By completing this task, we gain hands-on experience with S3 and its key features, such as scalability, security, and cost-efficiency.

Objective

The goal of this project is to:

1. Understand AWS S3 Basics: Learn how to create, configure, and manage an S3 bucket for cloud storage.
2. File Operations: Gain hands-on experience in uploading, downloading, and managing files within the S3 bucket.
3. Access Control: Configure bucket policies and permissions to manage secure and public access to stored data.

Importance of S3

Foundation for Advanced Use Cases: Learning how to handle S3 storage is a stepping stone for mastering cloud computing and deploying large-scale applications.

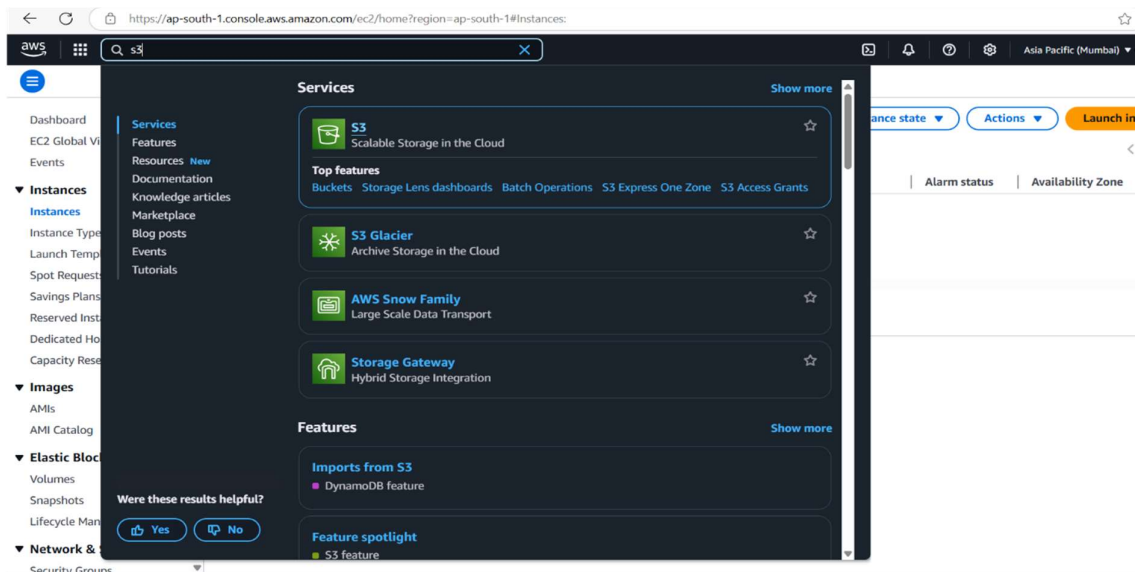
Hands-On Learning of Cloud Storage: AWS S3 provides a practical platform to learn cloud storage concepts, enabling users to create buckets, upload/download files, and manage data at scale.

Data Security and Access Control: By configuring bucket policies and permissions, users can secure their data and manage who can access it.

Step-by-Step Overview

Step 1:

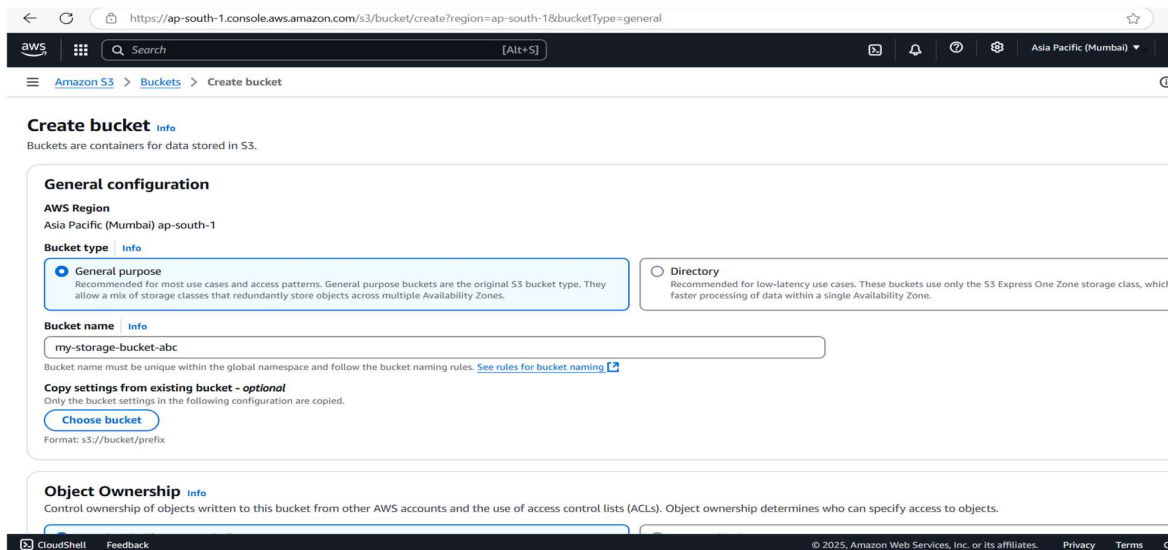
Go to the AWS Management Console, Search for and click on S3



Step 2 :

Click the "Create bucket" button.

Enter a unique bucket name (e.g., my-storage-bucket-123).



Step 3 :

Leave "Block all public access" enabled for now (you can modify it later).

The screenshot shows the 'Create bucket' page in the Amazon S3 console. The breadcrumb navigation is 'Amazon S3 > Buckets > Create bucket'. The page title is 'Object Ownership' with an 'info' icon. A description states: '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.'

There are two radio button options for 'Object Ownership':

- 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.

Below these options, it says 'Object Ownership: Bucket owner enforced'.

The next section is 'Block Public Access settings for this bucket'. It explains that public access is granted through ACLs, bucket policies, access point policies, or all. It recommends turning on 'Block all public access' before applying any of these settings.

The 'Block all public access' checkbox is checked. Below it, four sub-settings are listed, all of which are also checked:

- 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.
- 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.
- 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.

The footer of the console shows 'CloudShell', 'Feedback', and copyright information for Amazon Web Services, Inc. or its affiliates.

Step 4:

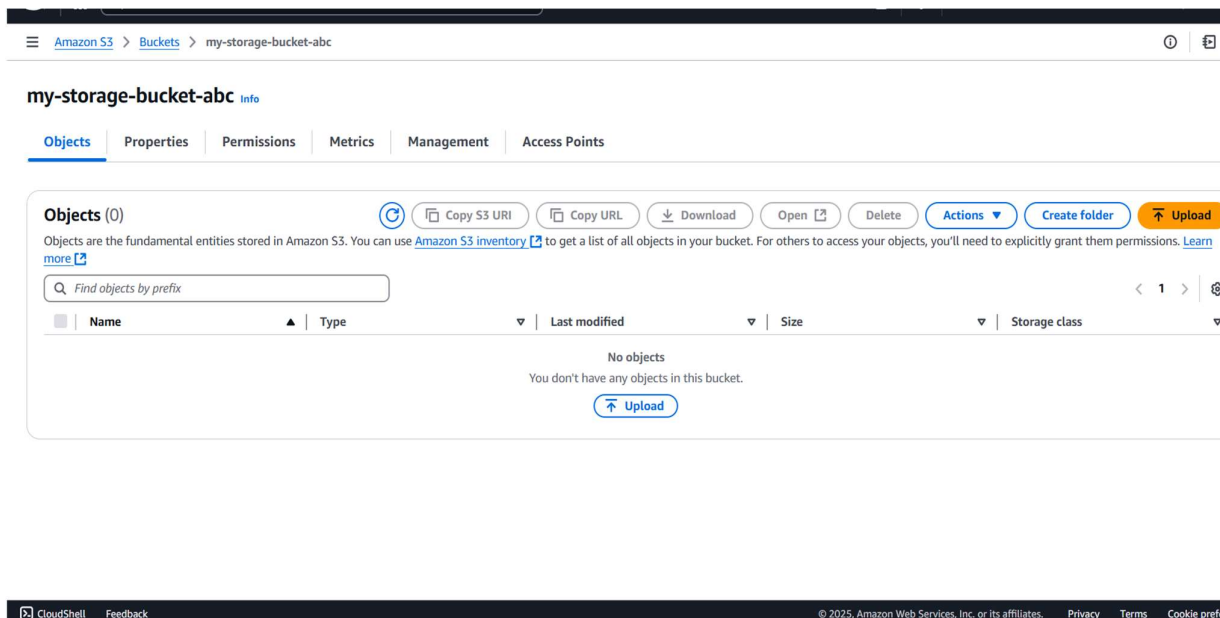
Click "Create bucket".

The screenshot shows the Amazon S3 console after a bucket has been created. A green banner at the top says 'Successfully created bucket "my-storage-bucket-abc"'. Below this, there's a section for 'Account snapshot - updated every 24 hours' with a 'View Storage Lens dashboard' link.

The main content area is titled 'General purpose buckets' and 'Directory buckets'. Under 'General purpose buckets', there's a search bar and a table of buckets. The table has columns for 'Name', 'AWS Region', 'IAM Access Analyzer', and 'Creation date'. One bucket is listed: 'my-storage-bucket-abc' in the 'us-east-1' region, created on 'January 28, 2025, 17:48:33 (UTC+05:30)'. Above the table, there are buttons for 'Copy ARN', 'Empty', 'Delete', and 'Create bucket'.

Step 5:

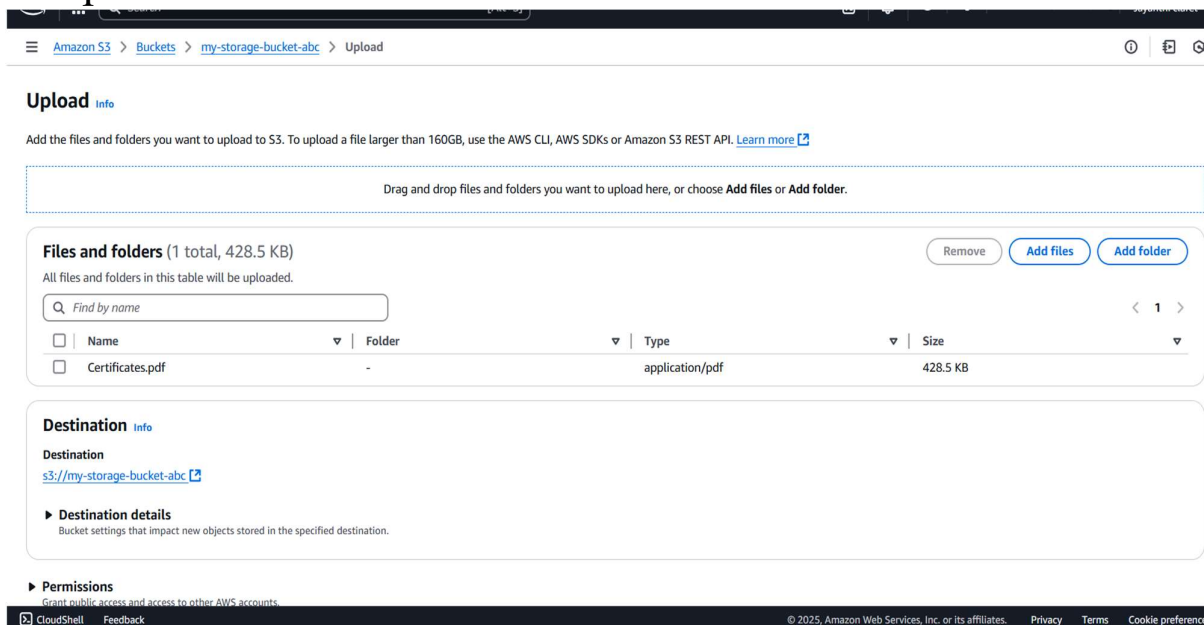
Open your newly created bucket from the S3 console.

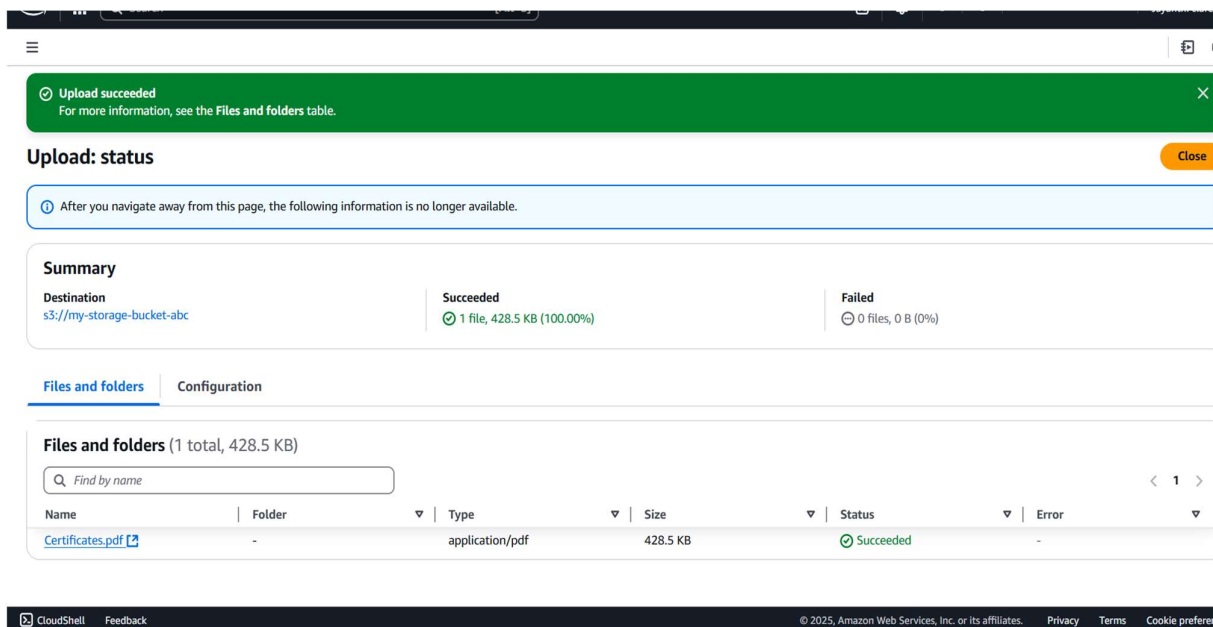


Step 6 :

Click "Upload" and then,

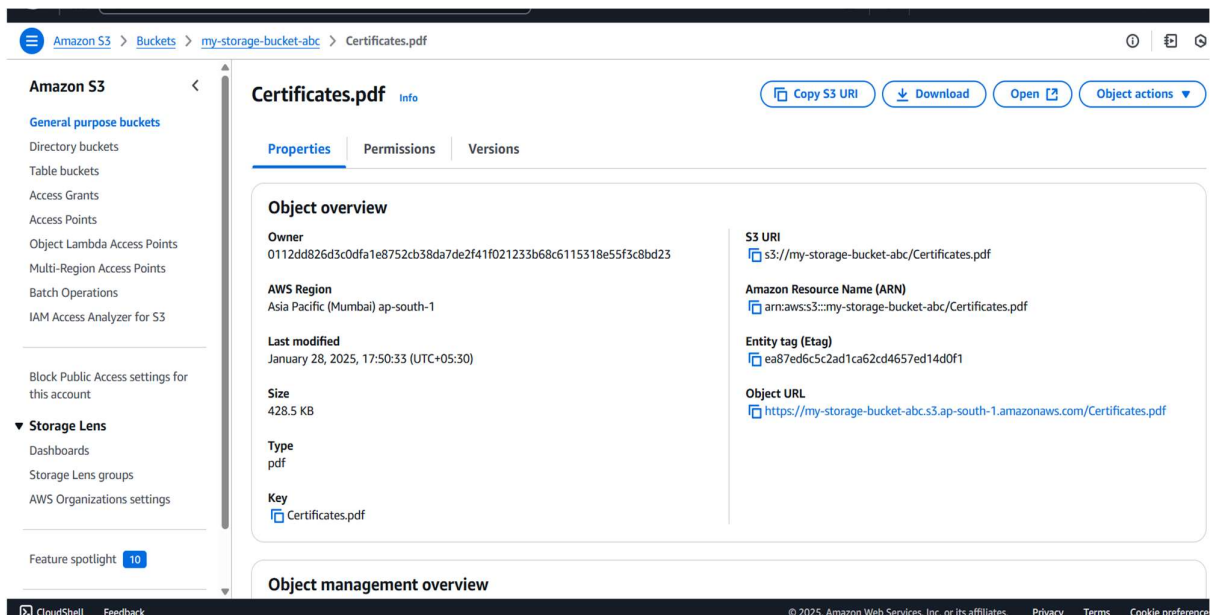
Drag and drop your file(s) or use the Add files button. Click Upload to complete.

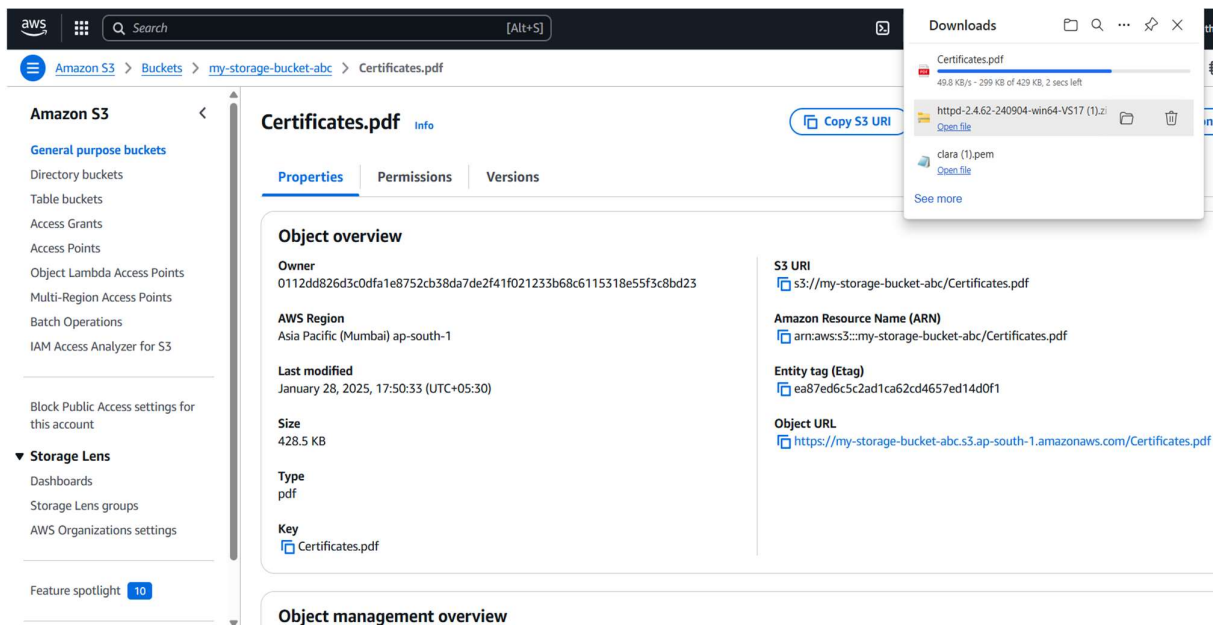




Step 7:

Go to the uploaded file in your bucket. Click the file name to open its details. Select Download to save the file locally.

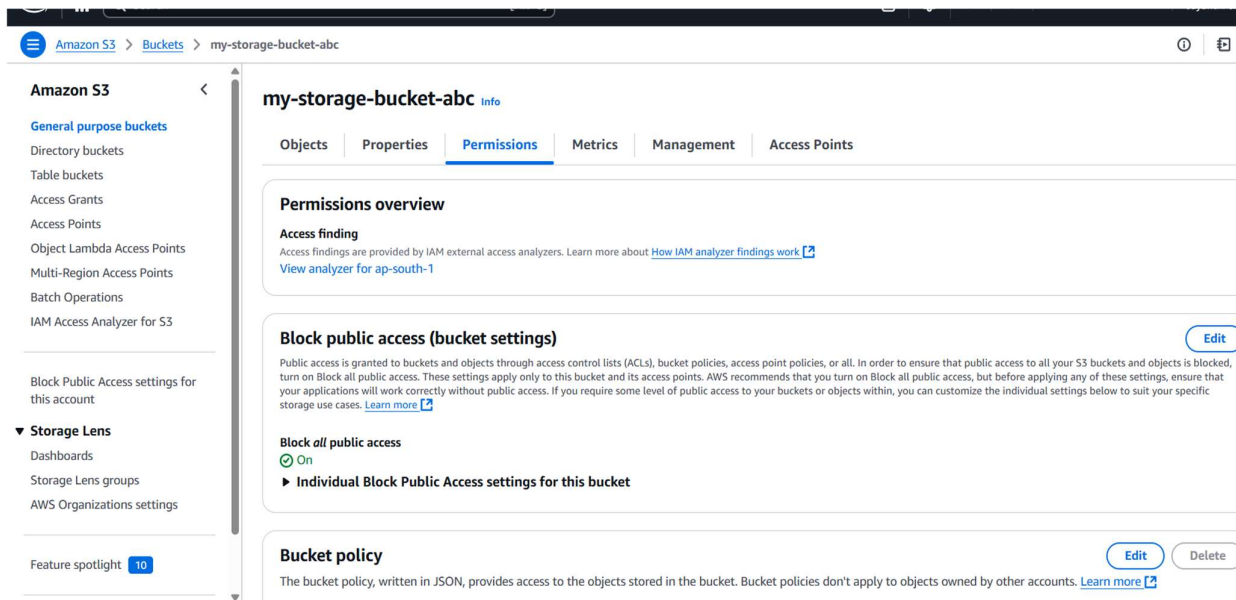


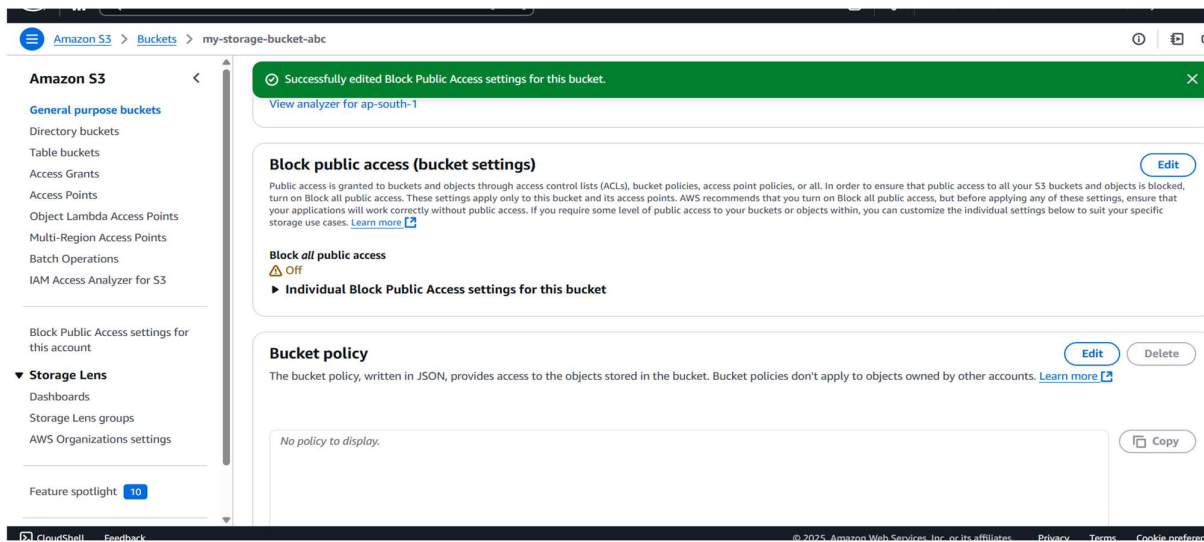


Step 8 :

Open your bucket and navigate to the "Permissions" tab.

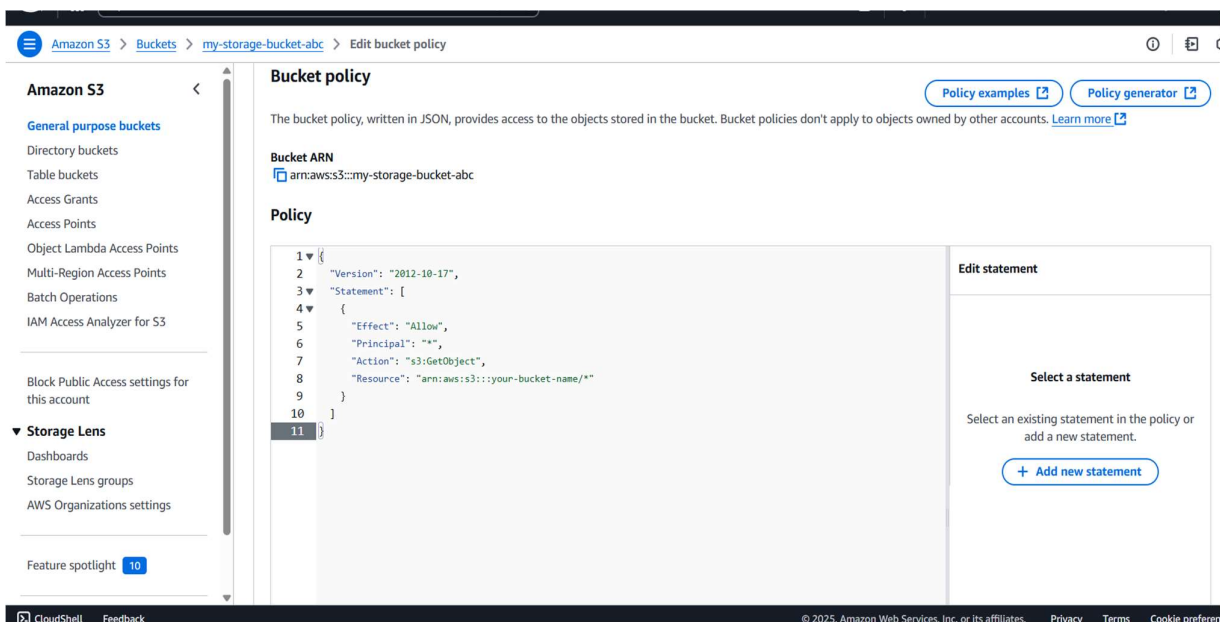
Under Block public access, click Edit and uncheck "Block all public access". Confirm by typing "confirm" and save.

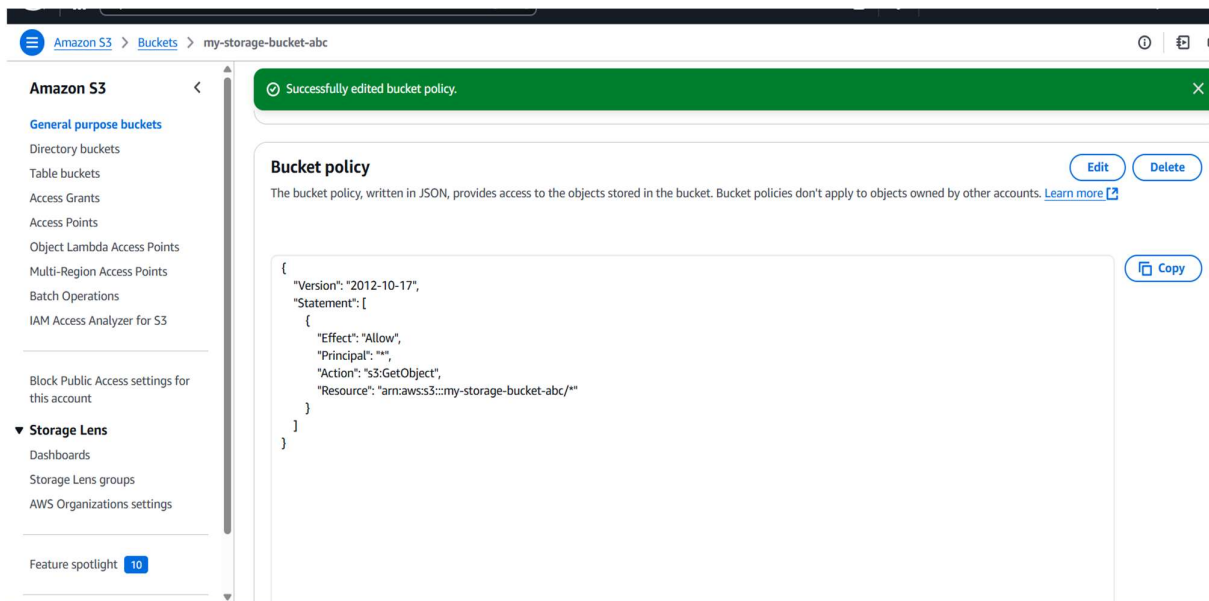




Step 9:

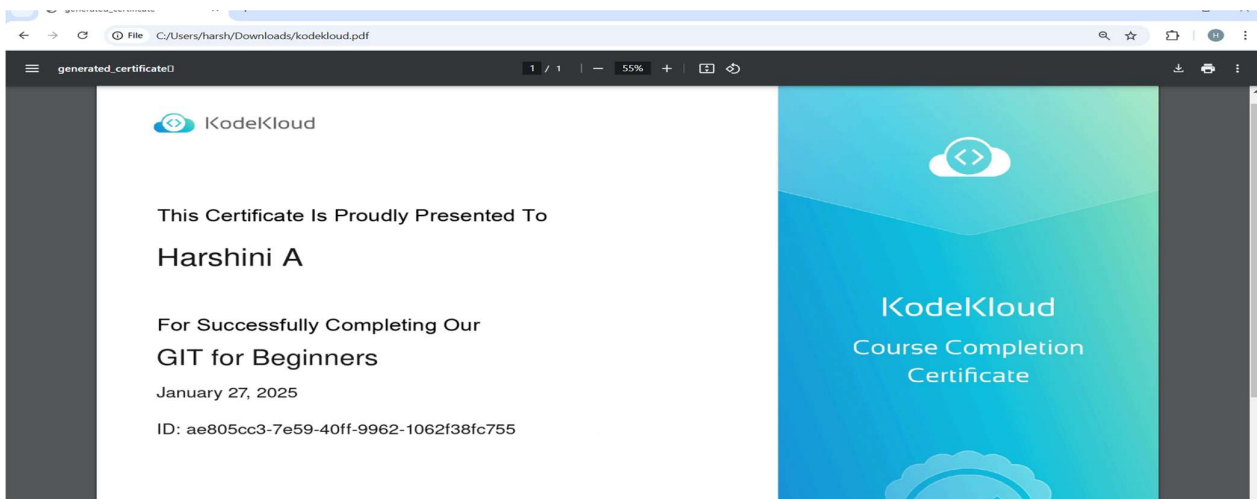
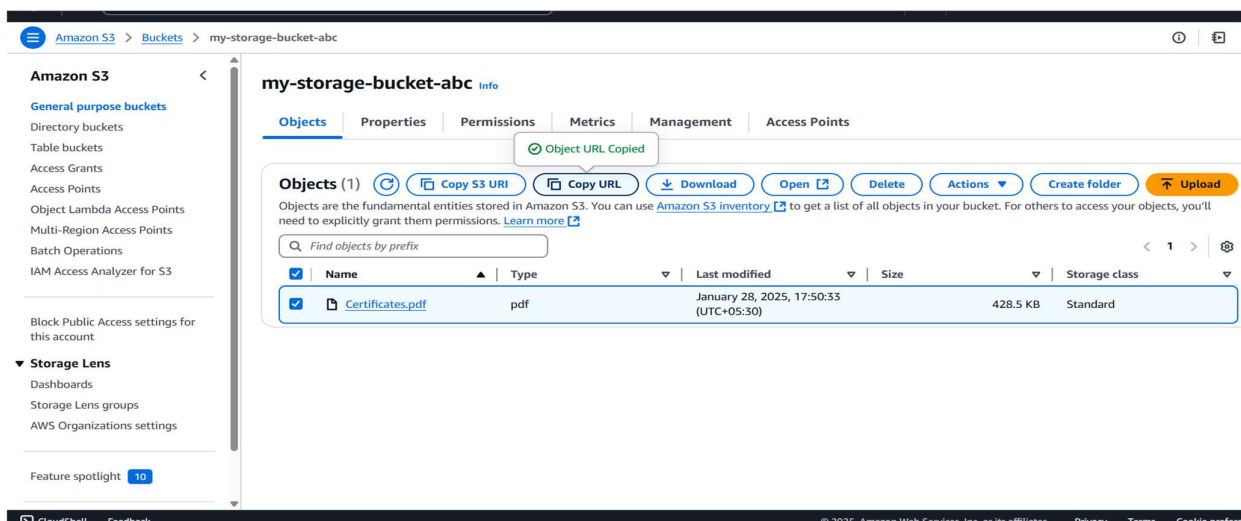
In the "Permissions" tab, scroll to Bucket Policy and click Edit. Replace your-bucket-name with your actual bucket name. Save changes.





Step10:

Use the S3 bucket URL or public file URL to test access permissions.



Expected Outcome

By completing this POC, you will:

1. Successfully create an AWS S3 bucket and perform file upload/download operations.
2. Configure and validate access permissions, ensuring secure or public access as needed.
3. Gain a solid understanding of S3's functionality, enabling its use in real-world cloud-based applications.