

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: SUBASHINI P

Department: IT



Introduction and Overview

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 Storage Bucket(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.

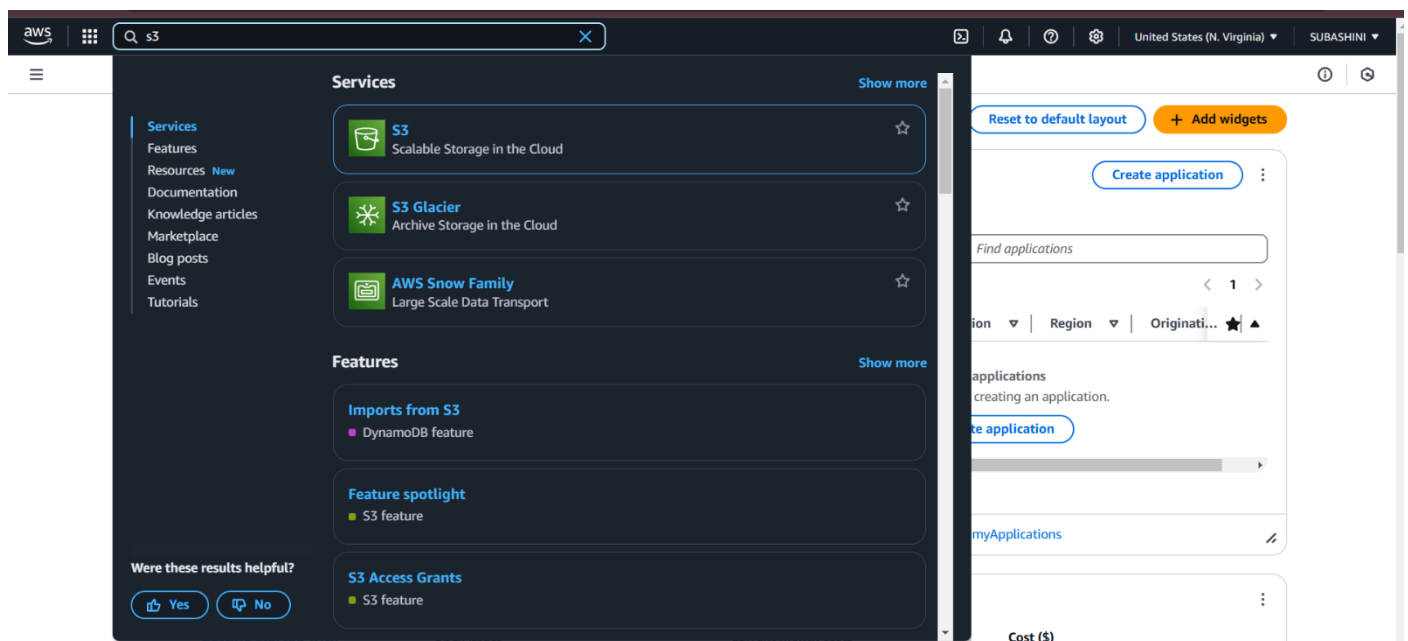
Hands-On Learning of Cloud Storage: AWS S3 provides a practical platform to learn cloud storage concepts, enabling users to create buckets, upload/download files, and manage data at scale.

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).

Amazon S3 > Buckets > Create bucket

Create bucket

Info

Buckets are containers for data stored in S3.

General configuration

AWS Region

US East (N. Virginia) us-east-1

Bucket type

Info

☒ General purpose

Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

☐ Directory

Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name

Info

storage-bucket

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

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.

Step 3 :

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

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

Step 4 :

Click "Create bucket".

Amazon S3 > Buckets

Account snapshot - updated every 24 hours All AWS Regions [View Storage Lens dashboard](#)

Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. [Learn more](#)

General purpose buckets | Directory buckets

General purpose buckets (5) All AWS Regions [Refresh](#) [Copy ARN](#) [Empty](#) [Delete](#) [Create bucket](#)

Buckets are containers for data stored in S3.

	Name	AWS Region	IAM Access Analyzer	Creation date
<input type="radio"/>	aws-easy-website25	Europe (Stockholm) eu-north-1	View analyzer for eu-north-1	January 11, 2025, 18:20:34 (UTC+05:30)
<input checked="" type="radio"/>	storage-bucket-25	US East (N. Virginia) us-east-1	View analyzer for us-east-1	February 3, 2025, 18:31:50 (UTC+05:30)
<input type="radio"/>	suba-25	Europe (Stockholm) eu-north-1	View analyzer for eu-north-1	February 2, 2025, 21:12:17 (UTC+05:30)
<input type="radio"/>	textract-console-us-west-1-4e4b5c1a-d457-457a-8280-dfd84a293a38	US West (N. California) us-west-1	View analyzer for us-west-1	January 22, 2025, 19:09:53 (UTC+05:30)
<input type="radio"/>	tom25	Europe (Stockholm) eu-north-1	View analyzer for eu-north-1	January 5, 2025, 17:28:19 (UTC+05:30)

Step 5 :

Open your newly created bucket from the S3 console.

Amazon S3 > Buckets > storage-bucket-25

storage-bucket-25 Info

Objects | Metadata | Properties | Permissions | Metrics | Management | Access Points

Objects (0) [Refresh](#) [Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#) [Actions](#) [Create folder](#) [Upload](#)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

	Name	Type	Last modified	Size	Storage class
No objects You don't have any objects in this bucket.					

[Upload](#)

Step 6 :

Click "Upload" and then,

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

Amazon S3 > Buckets > storage-bucket-25 > 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 SDKs or Amazon S3 REST API. [Learn more](#)

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

Files and folders (1 total, 242.9 KB)

All files and folders in this table will be uploaded.

Find by name

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	Screenshot 2025-01-24 193907.png	-	image/png	242.9 KB

Remove

Add files

Add folder

Destination Info

Destination

[s3://storage-bucket-25](#)

Destination details

Bucket settings that impact new objects stored in the specified destination.

Permissions

aws

Search

[Alt+S]

United States (N. Virginia)

SUBASHINI

Upload succeeded

For more information, see the Files and folders table.

Close

Upload: status

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

Summary

Destination

[s3://storage-bucket-25](#)

Succeeded

1 file, 242.9 KB (100.00%)

Failed

0 files, 0 B (0%)

Files and folders

Configuration

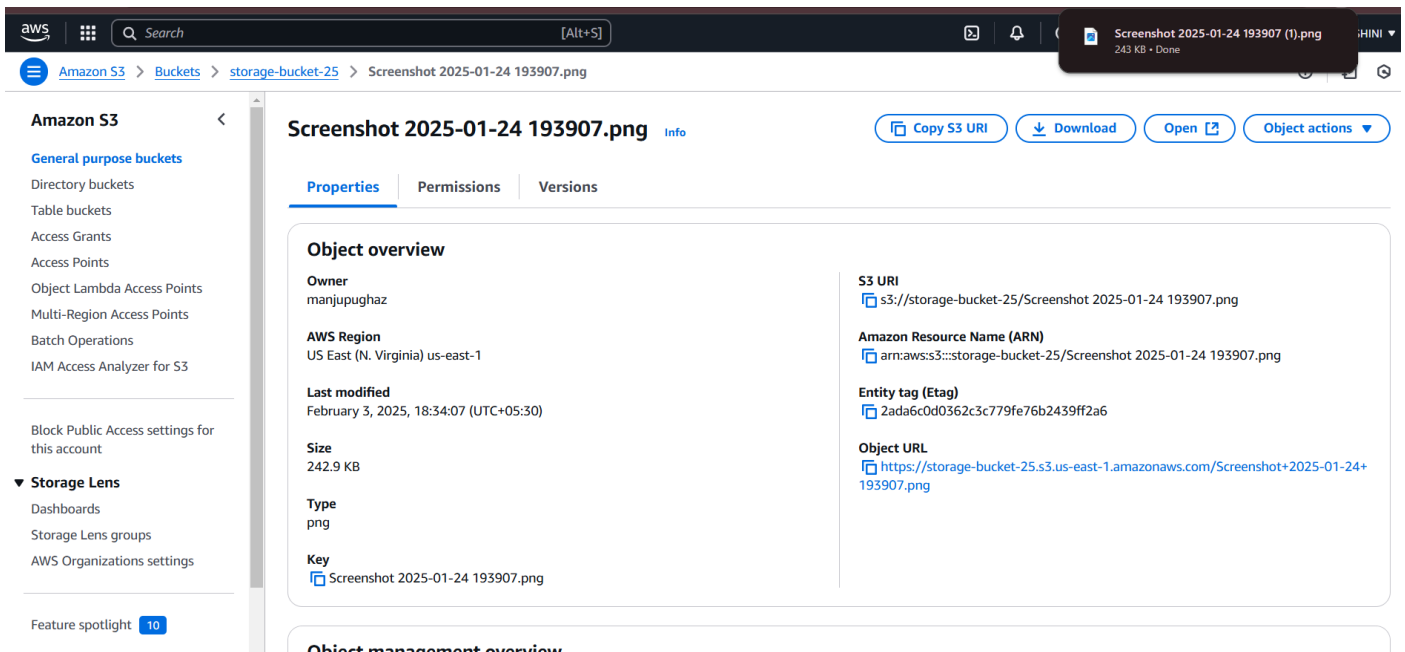
Files and folders (1 total, 242.9 KB)

Find by name

Name	Folder	Type	Size	Status	Error
Screenshot 2025-01-24 193907....	-	image/png	242.9 KB	Succeeded	-

Step 7 :

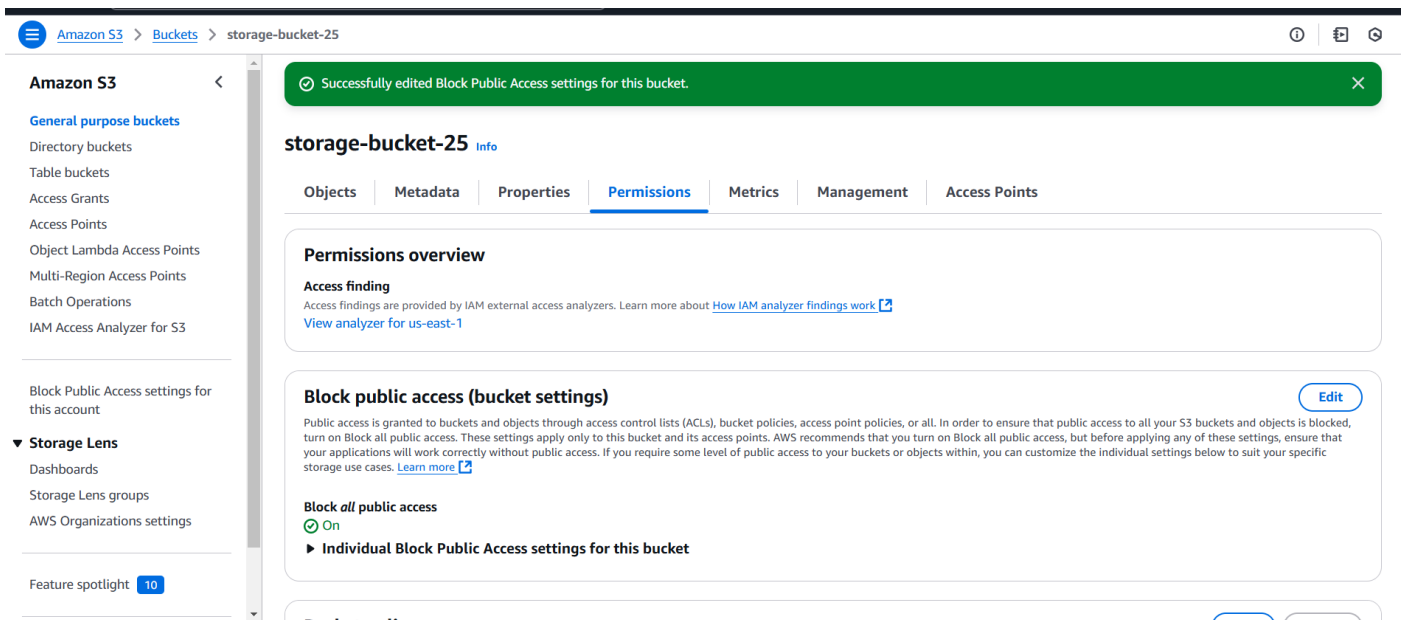
Go to the uploaded file in your bucket. Click the file name to open its details. Select Download to save the file locally.



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.

The screenshot shows the 'Edit bucket policy' page in the Amazon S3 console. The left sidebar contains navigation links for 'Amazon S3', 'General purpose buckets', 'Directory buckets', 'Table buckets', 'Access Grants', 'Access Points', 'Object Lambda Access Points', 'Multi-Region Access Points', 'Batch Operations', 'IAM Access Analyzer for S3', 'Block Public Access settings for this account', 'Storage Lens', 'Dashboards', 'Storage Lens groups', 'AWS Organizations settings', and 'Feature spotlight'. The main content area shows the bucket policy for 'storage-bucket-25'. The policy is written in JSON and includes a single statement that allows the 'GetObject' action on the bucket. The 'Edit statement' panel on the right is empty, showing a 'Select a statement' message and an 'Add new statement' button.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": "*",
7       "Action": "s3:GetObject",
8       "Resource": "arn:aws:s3:::storage-bucket-25*"
9     }
10  ]
11 }
12
```

The screenshot shows the 'Permissions' tab for 'storage-bucket-25' in the Amazon S3 console. A green banner at the top indicates 'Successfully edited bucket policy.' The 'Permissions' tab is selected, showing the 'Permissions overview' section. This section includes 'Access finding' and 'Block public access (bucket settings)'. The 'Block public access' settings are currently 'On', and there is an 'Edit' button next to it. The 'Individual Block Public Access settings for this bucket' section is also visible.

Step10:

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

aws [Search] [Alt+S] United States (N. Virginia) SUBASHINI

Amazon S3 > Buckets > storage-bucket-25

Amazon S3

General purpose buckets

- Directory buckets
- Table buckets
- Access Grants
- Access Points
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- IAM Access Analyzer for S3

Block Public Access settings for this account

▼ Storage Lens

- Dashboards
- Storage Lens groups
- AWS Organizations settings

Feature spotlight 10

storage-bucket-25 Info


Objects Metadata Properties Permissions Metrics Management Access Points

Object URL Copied

Objects (1) Copy S3 URI Copy URL Download Open Delete Actions Create folder Upload

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Find objects by prefix

<input checked="" type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input checked="" type="checkbox"/>	 Screenshot 2025-01-24 193907.png	png	February 3, 2025, 18:34:07 (UTC+05:30)	242.9 KB	Standard



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.