

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: Jason Peniel Raj. S

Department : CSE

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.

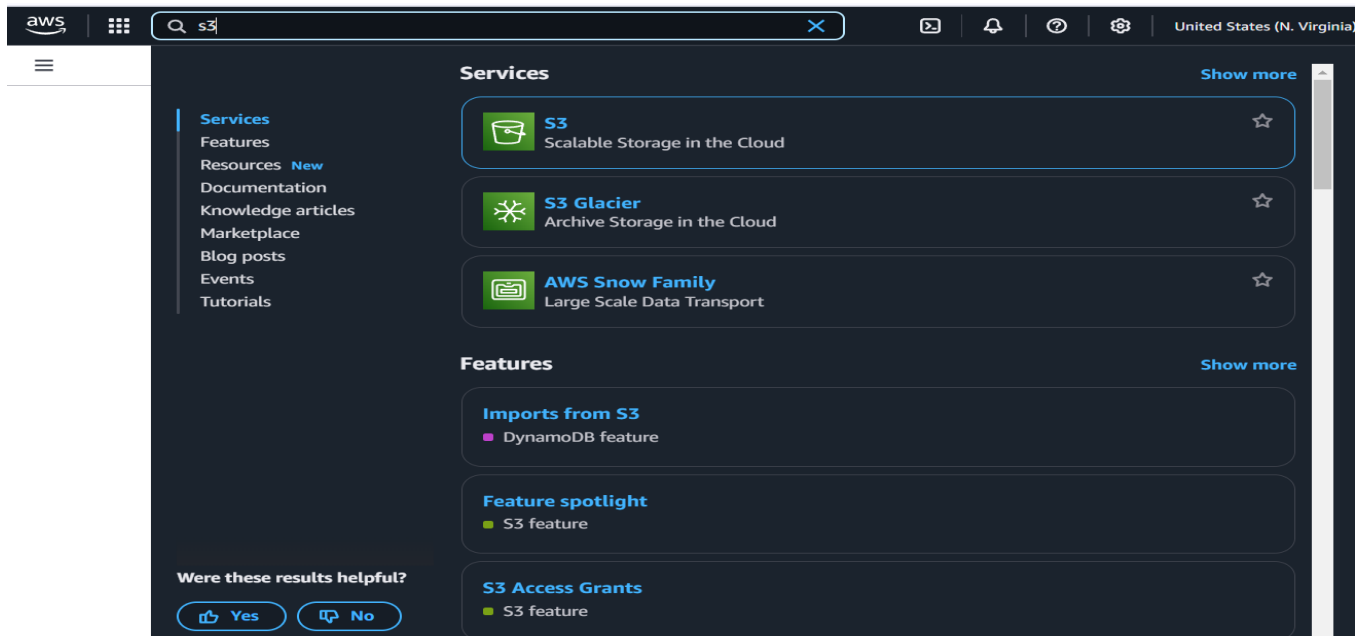
Hands-On Learning of Cloud Storage: AWS S3 provides a practical platform to learn cloud storage concepts, enabling users to create buckets, upload/download files, and manage data at scale.

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

Step1:

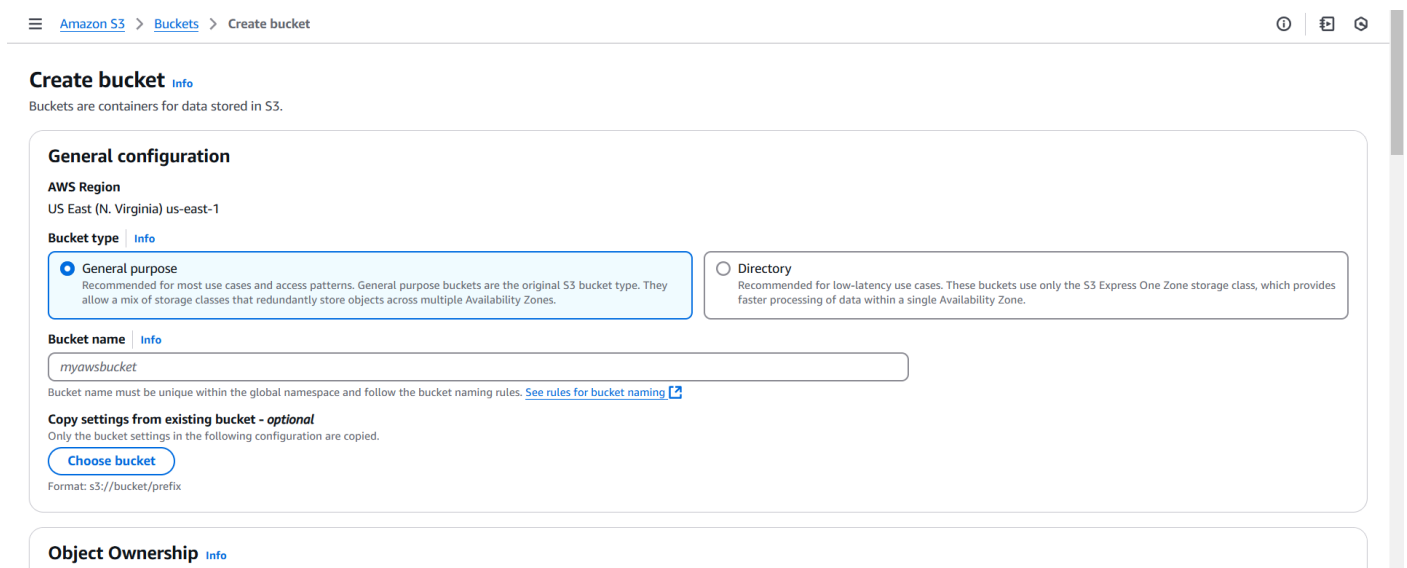
Go to the AWS Management Console, Search for and click on S3



Step 2 :

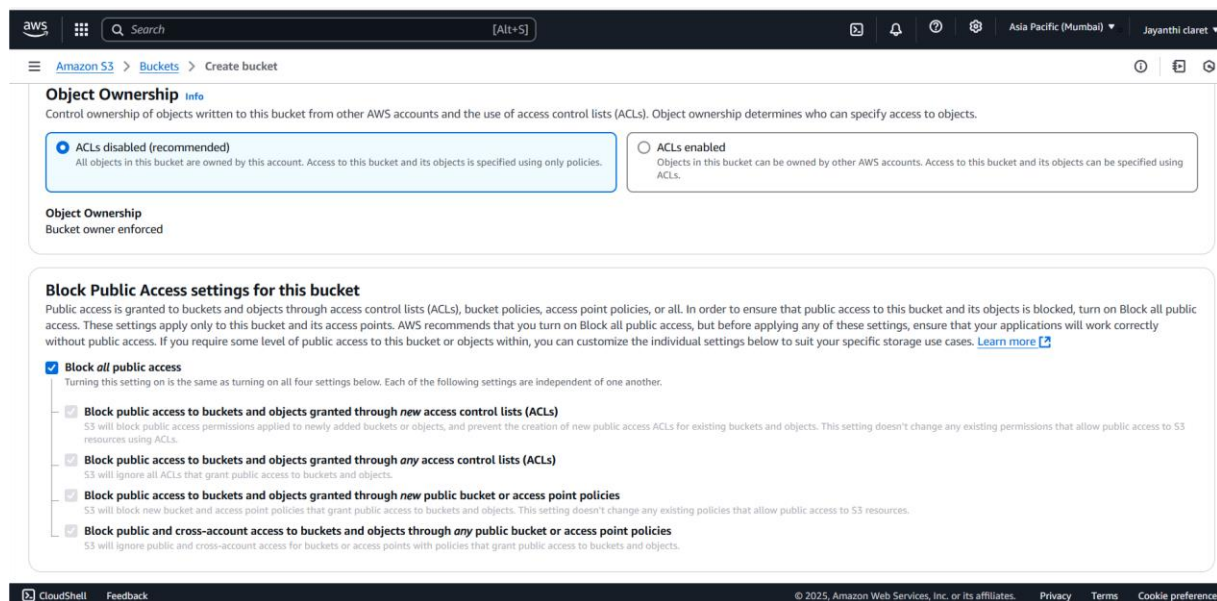
Click the "Create bucket" button.

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



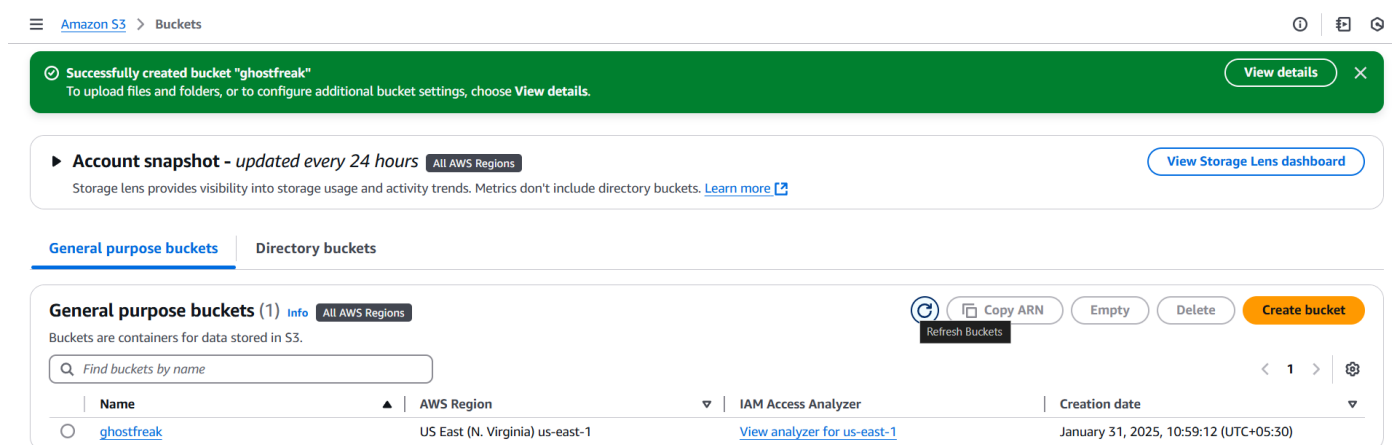
Step 3 :

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



Step 4 :

Click "Create bucket".



Step 5 :

Open your newly created bucket from the S3 console.

Amazon S3 > Buckets > ghostfreak

ghostfreak

Info

ObjectsMetadataPropertiesPermissionsMetricsManagementAccess Points

Objects (0)

Copy S3 URICopy URLDownloadOpenDeleteActionsCreate folderUpload

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

< 1 >

NameTypeLast modifiedSizeStorage 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.

https://ap-south-1.console.aws.amazon.com/s3/upload/my-storage-bucket-abc?region=ap-south-1&bucketType=general

aws

Search

[Alt+S]

Asia Pacific (Mumbai)

Jayanthi claret

Amazon S3 > Buckets > my-storage-bucket-abc > 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, 428.5 KB)

RemoveAdd filesAdd folder

All files and folders in this table will be uploaded.

Find by name

< 1 >

NameFolderTypeSize

Certificates.pdf-

application/pdf428.5 KB

Destination

Info

Destination

[s3://my-storage-bucket-abc](#)

Destination details

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

Permissions

Grant public access and access to other AWS accounts.

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. PrivacyTermsCookie preferences

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://ghostfreak

Succeeded

1 file, 439.0 KB (100.00%)

Failed

0 files, 0 B (0%)

Files and folders

Configuration

Files and folders (1 total, 439.0 KB)

Find by name

< 1 >

Name	Folder	Type	Size	Status	Error
Screenshot 2024-06-13 115225...	-	image/png	439.0 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.

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

Amazon S3 > Buckets > ghostfreak > Screenshot 2024-06-13 115225.png

Screenshot 2024-06-13 115225.png Info

Copy S3 URI

Download

Open

Object actions

Properties

Permissions

Versions

Object overview

Owner
awslabsc0w6613678t1698227449

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

Last modified
January 31, 2025, 11:00:55 (UTC+05:30)

Size
439.0 KB

Type
png

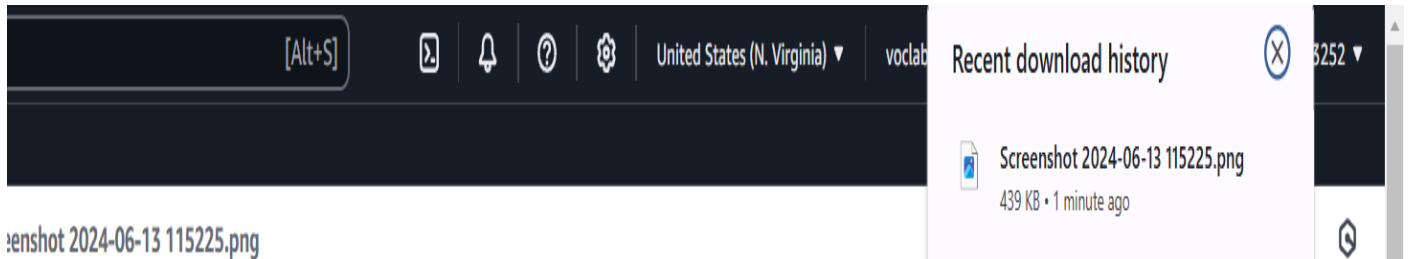
Key
Screenshot 2024-06-13 115225.png

S3 URI
s3://ghostfreak/Screenshot 2024-06-13 115225.png

Amazon Resource Name (ARN)
arn:aws:s3::ghostfreak/Screenshot 2024-06-13 115225.png

Entity tag (Etag)
528bf5600381e61f0d33a56ce906fa93

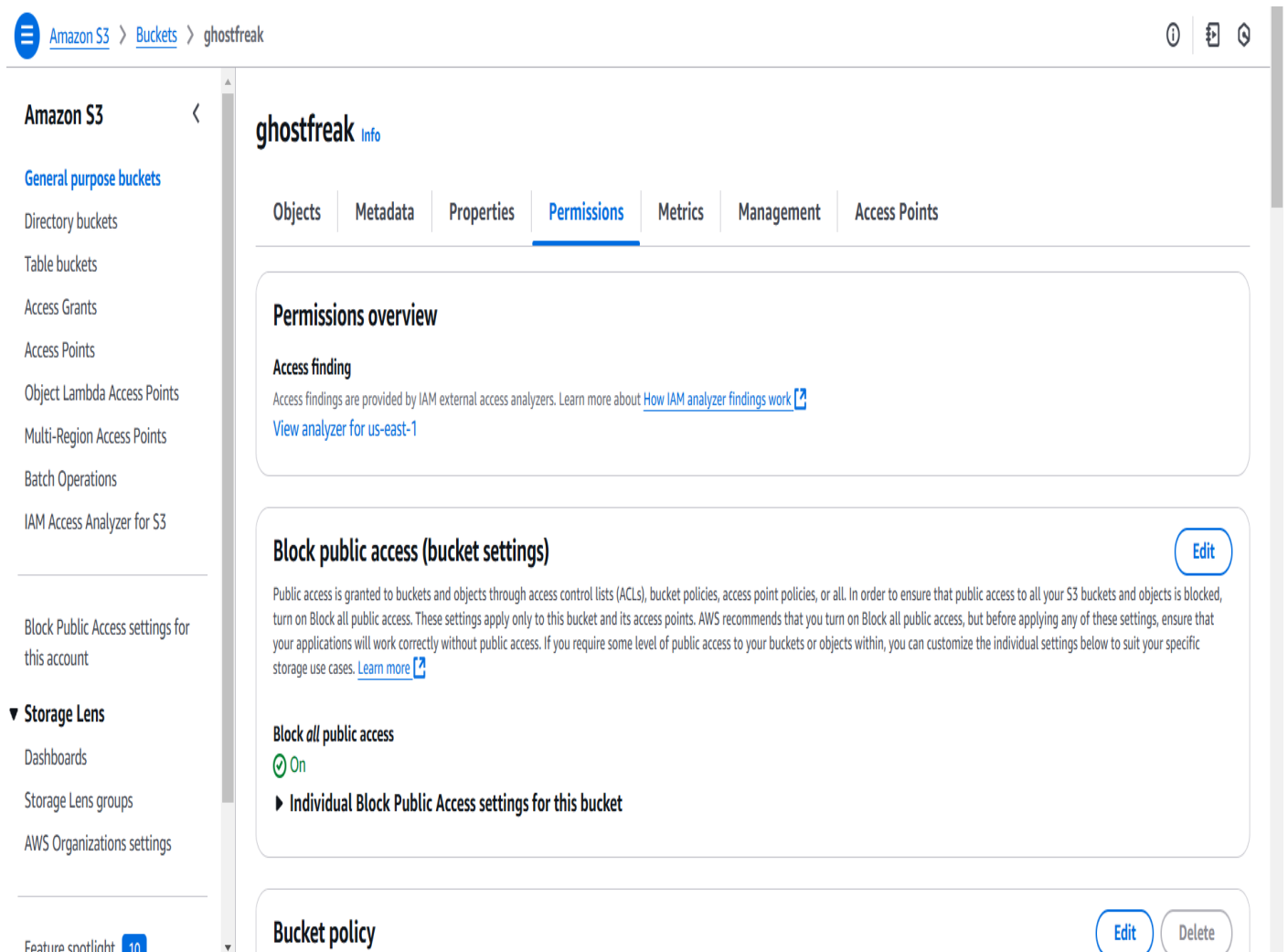
Object URL
<https://ghostfreak.s3.us-east-1.amazonaws.com/Screenshot+2024-06-13+115225.png>



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.



☐ **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.


Cancel

Save changes

Step 9 :

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

Bucket ARN

 arn:aws:s3:::ghostfreak

Policy

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


Successfully edited bucket policy.

Bucket policy

EditDelete

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

```
{  "Version": "2012-10-17",  "Statement": [    {      "Effect": "Allow",      "Principal": "*",      "Action": "s3:GetObject",      "Resource": "arn:aws:s3:::ghostfreak/*"    }  ]}
```

Copy

Step10:

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

ObjectsMetadataPropertiesPermissionsMetricsManagementAccess Points

Object URL Copied

Objects (1)

Copy S3 URICopy URLDownloadOpenDeleteActionsCreate folderUpload

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 2024-06-13 115225.png	png	January 31, 2025, 11:00:55 (UTC+05:30)	439.0 KB	Standard



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.