

## **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: Hema S

Department: ECE



## 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.

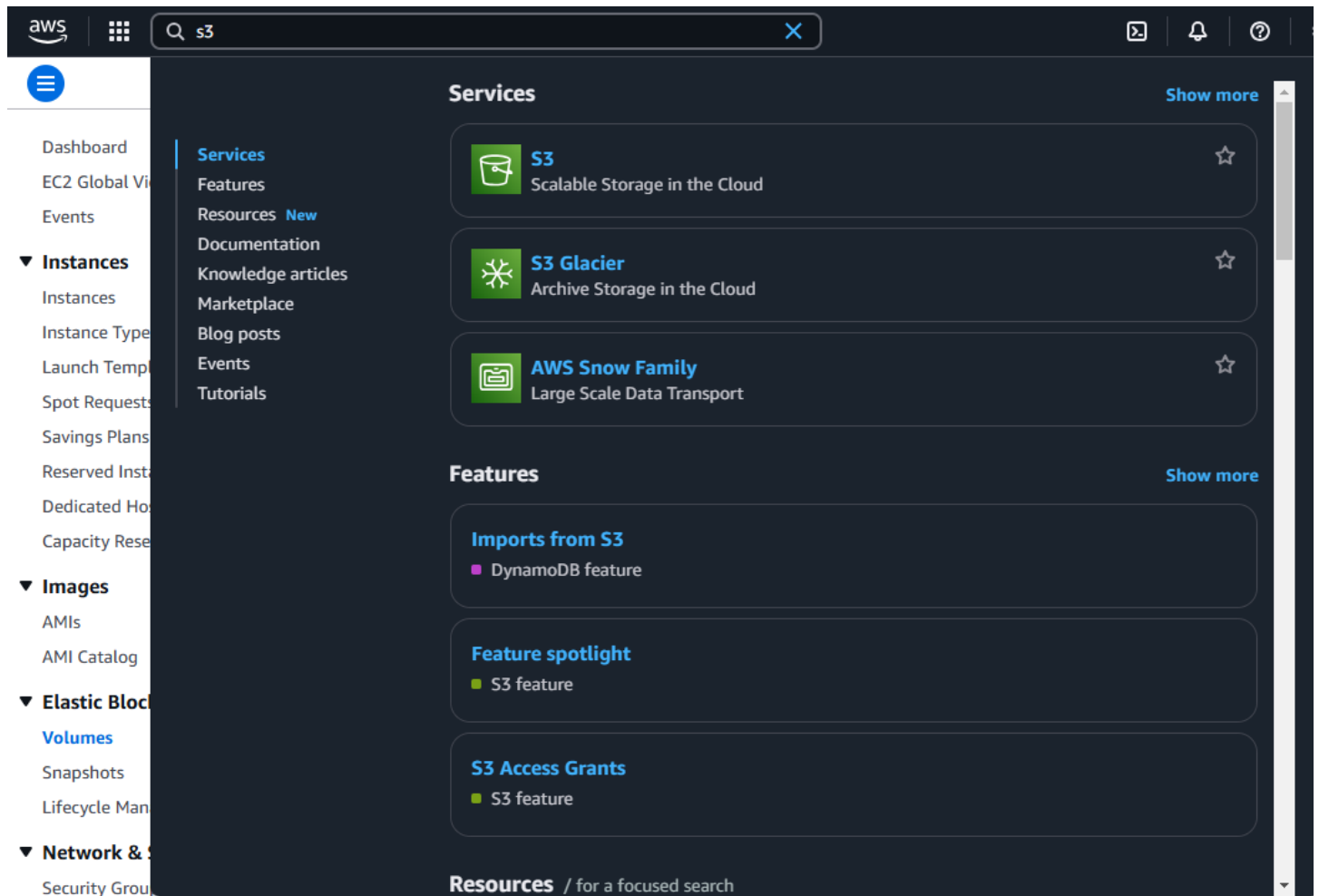
**Hands-On Learning of Cloud Storage:** AWS S3 provides a practical platform to learn cloud storage concepts, enabling users to create buckets, upload/download files, and manage data at scale.

**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).



[Alt+S]



United States (N. Virginia) ▼

Hema S ▼

Amazon S3 > Buckets > Create bucket

1 2 3

## 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](#)  
  
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.



Search



ENG IN



23:23  
04-02-2025



## Step 3 :

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

**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  
☐ Enable

## Step 4 :

Click "Create bucket".

**Successfully created bucket "hema-0212"**  
To upload files and folders, or to configure additional bucket settings, choose [View details](#).

**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

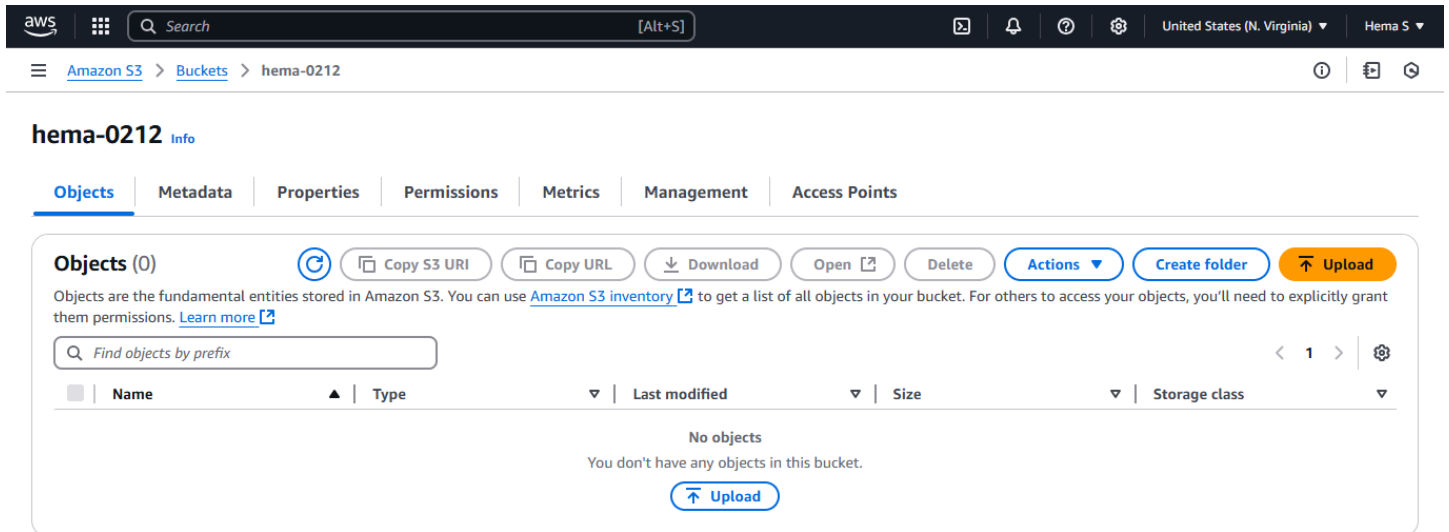
**General purpose buckets (1)** All AWS Regions

Buckets are containers for data stored in S3.

Name	AWS Region	IAM Access Analyzer	Creation date
<a href="#">hema-0212</a>	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	February 4, 2025, 23:25:11 (UTC+05:30)

## 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.

aws

Search

[Alt+S]

United States (N. Virginia)

Hema S

Amazon S3

Buckets

hema-0212

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, 73.6 KB)

Remove

Add files

Add folder

All files and folders in this table will be uploaded.

Find by name

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	WhatsApp Image 2024-09-22 at 20.34.4...	-	image/jpeg	73.6 KB

Destination

Info

Destination

[s3://hema-0212](#)

Destination details

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

Permissions

Grant public access and access to other AWS accounts.

aws

Search

[Alt+S]

United States (N. Virginia)

Hema S

Upload succeeded

For more information, see the Files and folders table.

Upload: status

Close

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

Summary

Destination

[s3://hema-0212](#)

Succeeded

1 file, 73.6 KB (100.00%)

Failed

0 files, 0 B (0%)

Files and folders

Configuration

Files and folders (1 total, 73.6 KB)

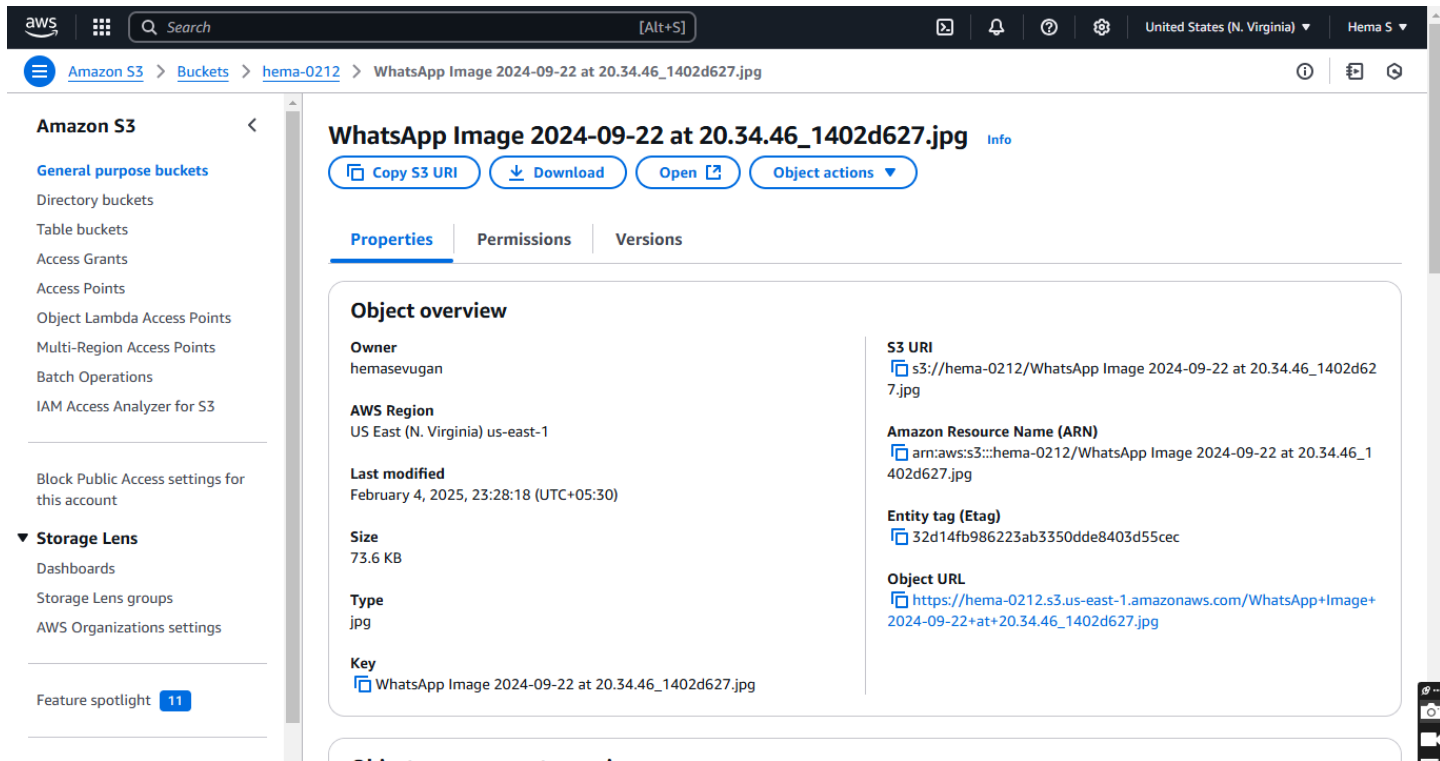
Find by name

Name	Folder	Type	Size	Status	Error
<a href="#">WhatsApp Image 2024-09-2...</a>	-	image/jpeg	73.6 KB	Succeeded	-

Step 7 :



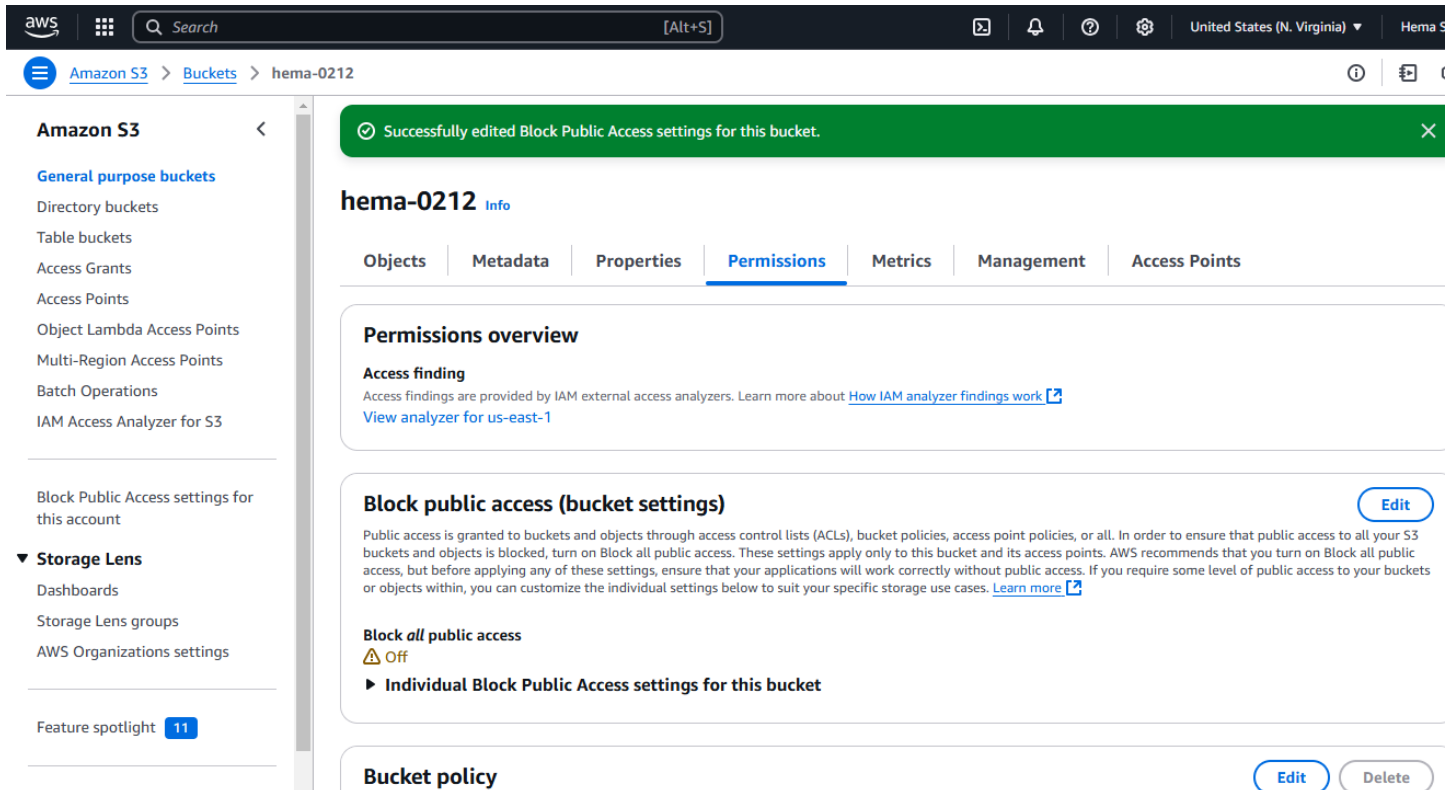
Go to the uploaded file in your bucket. Click the file name to open its details. Select Download to save the file locally.



## 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.

#### Edit bucket policy

---

#### Policy

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "PublicReadGetObject",  
6       "Effect": "Allow",  
7       "Principal": "*",  
8       "Action": "s3:GetObject",  
9       "Resource": "arn:aws:s3:::hema-0212/*"  
10    }  
11  ]  
12 }  
13 }
```

## Step10:

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

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 11

hema-0212

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

Objects (1/1)


- 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

< 1 >

<input checked="" type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input checked="" type="checkbox"/>	<div><div></div><div><a href="#">WhatsApp Image</a> 2024-09-22 at 20.34.46_1402d627.jpg</div></div>	jpg	February 4, 2025, 23:28:18 (UTC+05:30)	73.6 KB	Standard

Hema S

**Certificate of Completion for**

AWS Academy Graduate - AWS Academy Cloud Foundations

**Course hours completed**

20 hours

**Issued on**

02/01/2025

**Digital badge**

<https://www.credly.com/go/fXnlTHN5>

## 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.