

## **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:** Jeffersen Godfrey A 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:**

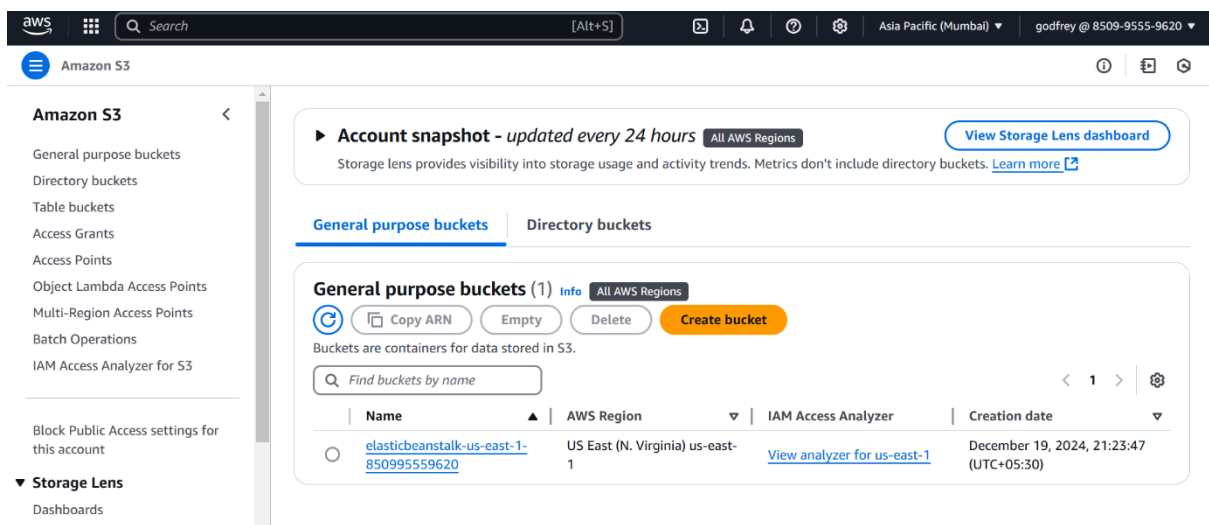
- 1. Scalable Storage:** AWS S3 allows users to store large amounts of data without worrying about capacity limitations.
- 2. Cost-Effective:** With a pay-as-you-go pricing model, it's affordable and only charges for the storage used.
- 3. High Durability:** S3 ensures 99.999999999% durability, making 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:

Go to [AWS Management Console](#).

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



## Step 2:

Click **Create bucket**.

**Bucket name:** Enter a unique name

Leave other settings as default (you can modify later).

aws [Search] [Alt+S] Asia Pacific (Mumbai) godfrey @ 8509-9555-9620

Amazon S3 > Buckets

Successfully created bucket "defo-02"  
To upload files and folders, or to configure additional bucket settings, choose [View details](#).

Account snapshot - updated every 24 hours All AWS Regions  
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 (2) Info All AWS Regions  
Buckets are containers for data stored in S3.

Find buckets by name

Name	AWS Region	IAM Access Analyzer	Creation date
<a href="#">defo-02</a>	Asia Pacific (Mumbai) ap-south-1	<a href="#">View analyzer for ap-south-1</a>	January 30, 2025, 21:28:44 (UTC+05:30)
<a href="#">elasticbeanstalk-us-east-1-850995559620</a>	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	December 19, 2024, 21:23:47 (UTC+05:30)

## Step 3:

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**.

Upload succeeded  
For more information, see the [Files and folders](#) table.

Summary

Destination <a href="#">s3://defo-02</a>	Succeeded ✔ 1 file, 222.9 KB (100.00%)	Failed ✖ 0 files, 0 B (0%)
---	---	-------------------------------

Files and folders Configuration

Files and folders (1 total, 222.9 KB)

Find by name

Name	Folder	Type	Size	Status	Error
<a href="#">AWS 1.pdf</a>	-	application/pdf	222.9 KB	✔ Succeeded	-

## Step 4:

Navigate to the uploaded file inside your bucket.

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

The screenshot shows the Amazon S3 console interface. At the top, a green notification bar states "Upload succeeded". Below this, the breadcrumb navigation shows "Amazon S3 > Buckets > defo-02". The bucket name "defo-02" is displayed with an "Info" link. A tabbed interface shows "Objects" as the active tab, with other tabs for "Properties", "Permissions", "Metrics", "Management", and "Access Points". The "Objects" section shows a list of objects with a search bar and pagination controls. The table contains one object: "AWS 1.pdf", which is a PDF file, 222.9 KB in size, and was last modified on January 30, 2025, at 21:29:49 (UTC+05:30). The storage class is "Standard". Above the table, there are buttons for "Copy S3 URI", "Copy URL", "Download", "Open", "Delete", "Actions", "Create folder", and "Upload".

Name	Type	Last modified	Size	Storage class
<a href="#">AWS 1.pdf</a>	pdf	January 30, 2025, 21:29:49 (UTC+05:30)	222.9 KB	Standard

## Step 5:

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

The screenshot shows the "Permissions" tab in the Amazon S3 console for the "defo-02" bucket. The breadcrumb navigation is "Amazon S3 > Buckets > defo-02". The "Permissions" tab is active, showing a "Permissions overview" section with an "Access finding" link. Below this, the "Block public access (bucket settings)" section is visible, with an "Edit" button. The "Block all public access" setting is currently "On" (indicated by a green checkmark). The text below the setting states: "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 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 your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more".

**Block public access (bucket settings)** [Edit](#)

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 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 your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

**Block all public access**  
On

► Individual Block Public Access settings for this bucket

## Edit Block public access (bucket settings) [Info](#)

### Block public access (bucket settings)

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 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 your buckets 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.

[Cancel](#)[Save changes](#)

## Step 6:

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.


## Edit bucket policy [Info](#)

### Bucket policy

[Policy examples](#)[Policy generator](#)

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](#)

#### Bucket ARN

 arn:aws:s3:::defo-02

#### Policy

1

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement



aws [Search] [Alt+S]

Amazon S3 > Buckets > defo-02 > Edit bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by

**Bucket ARN**  
arn:aws:s3:::defo-02

**Policy**

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

## Step 7:

Copy the Url in Copy URL option

Amazon S3 > Buckets > defo-02

defo-02 Info

Objects Properties Permissions Metrics Management Access Points

Object URL Copied

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

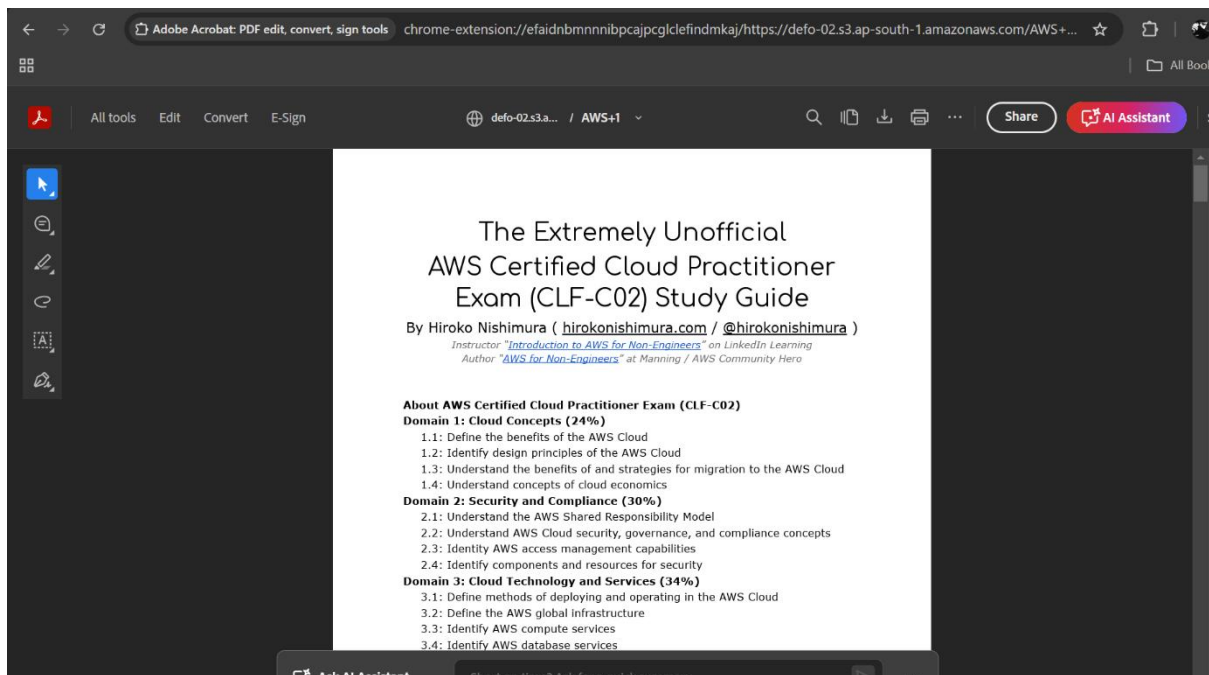
Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Find objects by prefix

<input checked="" type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input checked="" type="checkbox"/>	<a href="#">AWS 1.pdf</a>	pdf	January 30, 2025, 21:29:49 (UTC+05:30)	222.9 KB	Standard

## Step 9:

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



## OUTCOME:

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.