

# **Placement Empowerment Program**

## ***Cloud Computing and DevOps Centre***

### **Use Cloud Storage**

*TASK:- Create a storage bucket on your cloud platform and upload/download files. Configure access permissions for the bucket.*

Name:MADHU SMITHA

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.

## 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  
Click the "Create bucket" button.

Amazon S3 > Buckets

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

General purpose buckets | Directory buckets

General purpose buckets (4) 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="#">dev-trial</a>	Europe (Stockholm) eu-north-1	<a href="#">View analyzer for eu-north-1</a>	January 19, 2025, 11:11:20 (UTC+05:30)
<a href="#">madhu.html</a>	Europe (Stockholm) eu-north-1	<a href="#">View analyzer for eu-north-1</a>	February 1, 2025, 16:44:46 (UTC+05:30)
<a href="#">smitha-bucket</a>	Europe (Stockholm) eu-north-1	<a href="#">View analyzer for eu-north-1</a>	January 30, 2025, 11:06:34 (UTC+05:30)

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

## Step 2 :

Open your newly created bucket from the S3 console.

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

samplebucket999 [Info](#)

[Objects](#) | [Properties](#) | [Permissions](#) | [Metrics](#) | [Management](#) | [Access Points](#)

#### 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](#)

☐ Show versions

< 1 >

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	<a href="#">index.html</a>	html	February 1, 2025, 12:31:46 (UTC+05:30)	691.0 B	Standard

## Step 3 :

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

Upload: status

Close

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

**Summary**

**Destination**  
s3://madhu.html

**Succeeded**  
✔ 1 file, 776.0 B (100.00%)

**Failed**  
✖ 0 files, 0 B (0%)

- Files and folders
- Configuration

**Files and folders** (1 total, 776.0 B)

< 1 >

## Step 4 :

Amazon S3 > Buckets > madhu.html > Edit Block public access (bucket settings)

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

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

## Step 5 :

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

```

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 }

```

## Welcome to My Sample Page

[Home](#) [About](#) [Services](#) [Contact](#)

### Main Content

This is the main content area. Here, you can add your articles, blog posts, or any other information you want to share with your visitors.

### Sidebar

This is the sidebar area. You can place additional links or information here.

# Step6:



## **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.