

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: Swathika K

Department : AML

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

Click the "Create bucket" button.

Enter a unique bucket name (samplebucket).

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

Click "Create bucket".

Step 5 :

Open your newly created bucket from the S3 console.

Click "Upload" and then,

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

The screenshot shows the AWS S3 console interface for the 'samplebucket555' bucket. The breadcrumb navigation at the top reads 'Amazon S3 > Buckets > samplebucket555 > Upload'. The main heading is 'Upload' with an 'Info' link. Below this, a message states: '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](#)'. A large dashed box contains the instruction: 'Drag and drop files and folders you want to upload here, or choose **Add files** or **Add folder**.' Below this is a section titled 'Files and folders (1 total, 2.3 KB)' with a 'Remove' button and 'Add files' and 'Add folder' buttons. A search bar labeled 'Find by name' is present. A table lists the files to be uploaded:

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	index.html	-	text/html	2.3 KB

Below the table is a 'Destination' section with an 'Info' link. It shows the destination as 's3://samplebucket555'. There is a 'Destination details' link. At the bottom, there are sections for 'Permissions' (Grant public access and access to other AWS accounts) and 'Properties'.

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.

The screenshot displays the AWS S3 console interface. At the top, a green notification bar states "Upload succeeded" with a link to view the "Files and folders" table. Below this, the "Upload: status" section shows a warning that information may be lost if the user navigates away. The "Summary" section provides a breakdown: Destination is "s3://samplebucket555", 1 file (2.3 KB) was successfully uploaded (100.00%), and 0 files (0 B) failed (0%). The "Files and folders" tab is active, showing a table with one entry: "index.html" (2.3 KB, text/html) with a status of "Succeeded".

Name	Folder	Type	Size	Status	Error
index.html	-	text/html	2.3 KB	Succeeded	-

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.

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](#)**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 Off[► Individual Block Public Access settings for this bucket](#)

Step 9 :

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 }
```

Edit bucket policy [Info](#)

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 other accounts. [Learn more](#)

Bucket ARN

arn:aws:s3::samplebucket555

Policy

```
1 ▼ {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": "*",
7       "Action": "s3:GetObject",
8       "Resource": "arn:aws:s3:::samplebucket555/*"
9     }
10  ]
11 }
12
```

Step 10:

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

[index.html](#) [Info](#)

Info

Copy S3 URI

Download

Open 

Object actions ▼

Properties

Permissions

Versions

Object overview

Owner

awslabsc0w6611856t1698219193

AWS Region

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

Last modified

January 31, 2025, 10:52:20 (UTC+05:30)

Size

2.3 KB


Type

html

Key

[index.html](#)

S3 URI

 s3://samplebucket555/index.html

Amazon Resource Name (ARN)

```
arn:aws:s3:::samplebucket555/index.html
```

Entity tag (Etag)

Entity tag (Etag) 1b0837c9895cfd945dbb2c4

✔ Object URL Copied

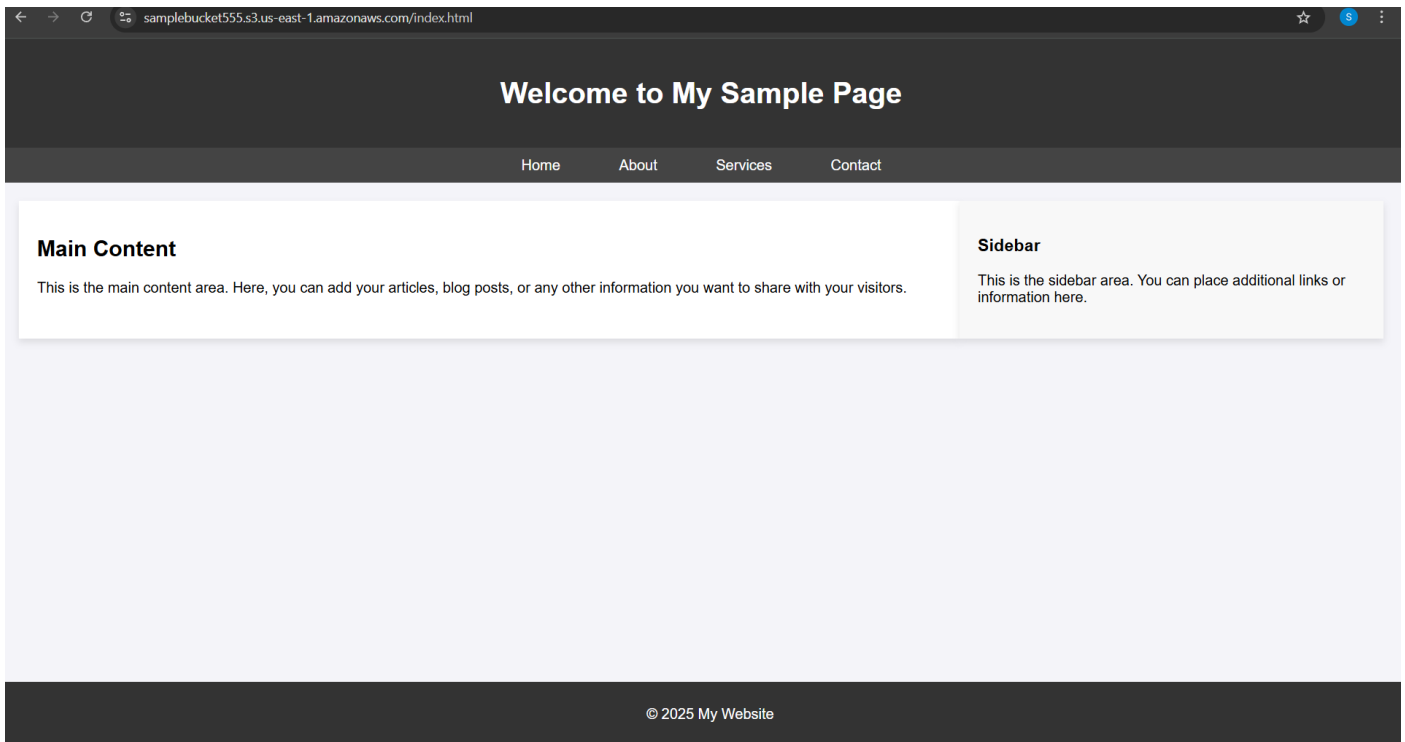
<https://samplebucket555.s3.us-east-1.amazonaws.com/index.html>

Object management overview

The following bucket properties and object management configurations impact the behavior of this object.

Bucket properties

Management configurations



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.