

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: Akshaya 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.

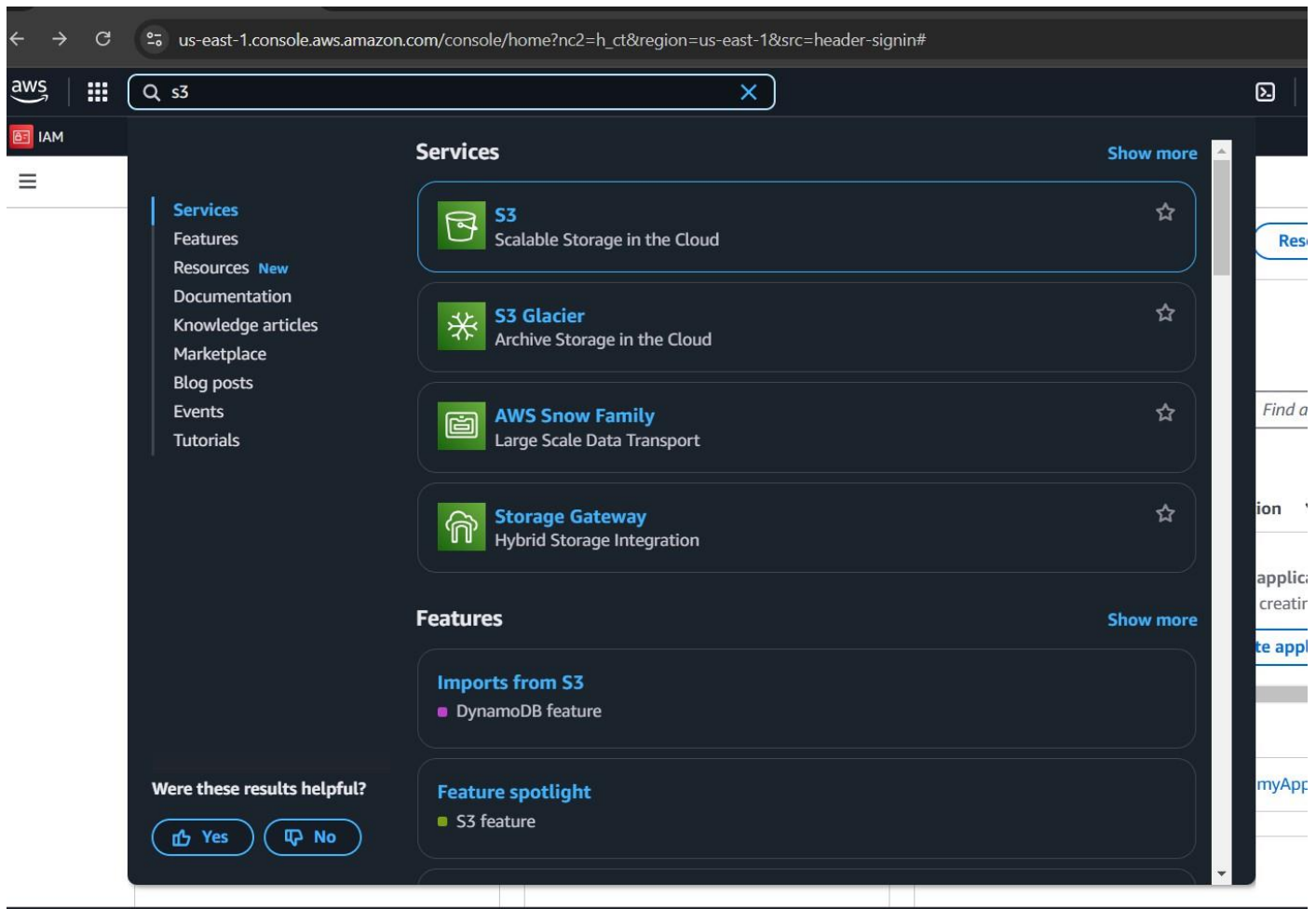
Hands-On Learning of Cloud Storage: AWS S3 provides a practical platform to learn cloud storage concepts, enabling users to create buckets, upload/download files, and manage data at scale.

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).

Create bucket [Info](#)

Buckets are containers for data stored in S3.

General configuration

AWS Region

Europe (Stockholm) eu-north-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 for 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

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.

Step 4 :

Click "Create bucket".

Successfully created bucket "akshu224"
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](#)

View Sto

General purpose buckets

Directory buckets

General purpose buckets (4) Info All AWS Regions

Refresh Copy ARN Empty Delete

Buckets are containers for data stored in S3.

Find buckets by name

Name	AWS Region	IAM Access Analyzer	Creation date
akshu224	Europe (Stockholm) eu-north-1	View analyzer for eu-north-1	February 4, 2025, 11:36:37

Step 5 :

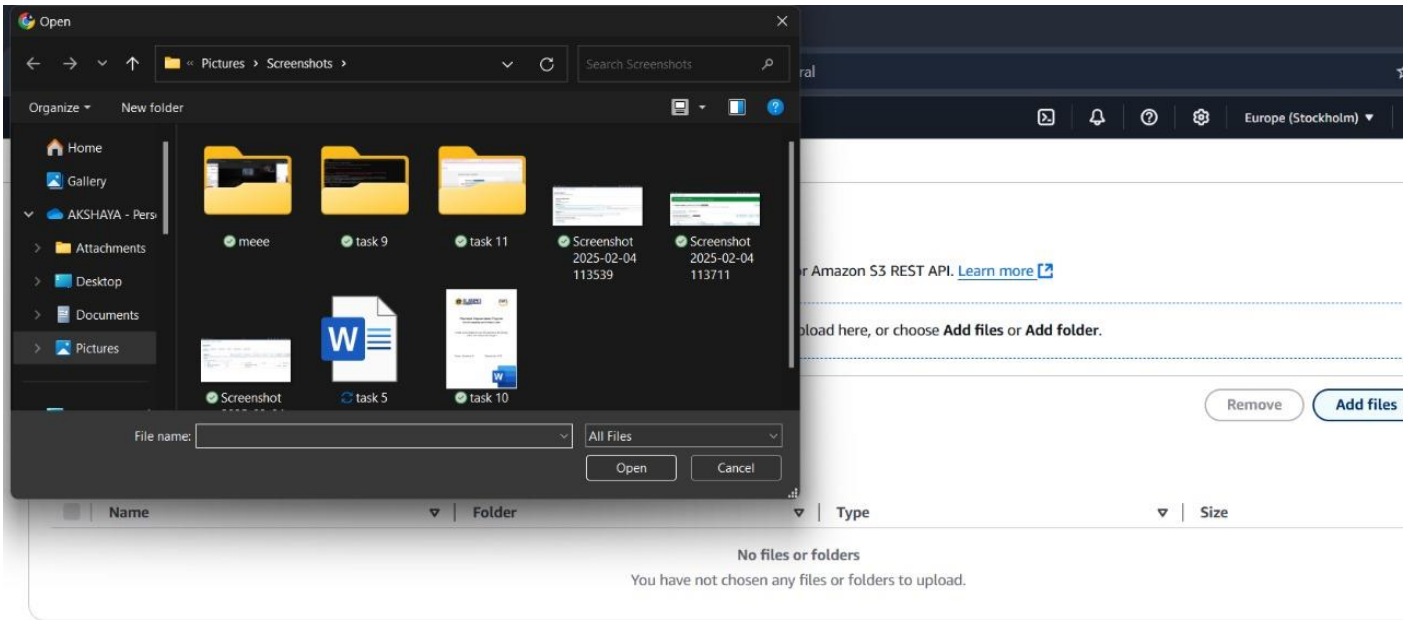
Open your newly created bucket from the S3 console.

The screenshot shows the AWS S3 console interface. At the top, the navigation bar includes the AWS logo, a search bar, and the region 'Europe (Stockholm)'. The breadcrumb trail indicates the path: Amazon S3 > Buckets > akshu224 > 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 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 (0)' with a 'Remove' button and an 'Add files' button. A message says: 'All files and folders in this table will be uploaded.' There is a search bar with the placeholder 'Find by name'. Below the search bar is a table header with columns: Name, Folder, Type, and Size. The table body is empty, displaying the message: 'No files or folders' and 'You have not chosen any files or folders to upload.' Below the 'Files and folders' section is the 'Destination' section with an 'Info' link. It shows the destination as 's3://akshu224' with a copy icon. A section titled 'Destination details' is expanded, showing the text: 'Bucket settings that impact new objects stored in the specified destination.'

Step 6 :

Click "Upload" and then,

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









Destination [Info](#)

Destination

[7:13:33.334](#)

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.

  [Alt+S]     Europe (Stockholm) ▼

Amazon S3 > Buckets > akshu224 > Screenshot 2025-02-04 113539.png

Screenshot 2025-02-04 113539.png Info

[Copy S3 URI](#) [Download](#) [Open](#)

Properties

Permissions

Versions

Object overview


Owner
5f0f6cd84837f1538a6e6397e248d2b14685f026c29108aba73cae44169df7b4


AWS Region
Europe (Stockholm) eu-north-1


Last modified
February 4, 2025, 11:38:08 (UTC+05:30)


Size
115.5 KB


Type
png

Key
 Screenshot 2025-02-04 113539.png

S3 URI
 s3://akshu224/Screenshot 2025-02-04 113539.png

Amazon Resource Name (ARN)
 arn:aws:s3:::akshu224/Screenshot 2025-02-04 113539.png

Entity tag (Etag)
 1df696ebcc874ea17d58ff9e53ab2aac

Object URL
 <https://akshu224.s3.eu-north-1.amazonaws.com/Screenshot+2025-02-04+113539.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.

Permissions overview

Access finding

Access findings are provided by IAM external access analyzers. Learn more about [How IAM analyzer findings work](#) [View analyzer for us-east-1](#)

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](#) [View analyzer for us-east-1](#)

Block all public access

On

► Individual Block Public Access settings for this bucket

[View analyzer for us-east-1](#)

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.

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:::dasan03

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 }
```

Edit statement

Select a statement

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

aws

Search

[Alt+S]

Amazon S3

Buckets

akshu224

Edit bucket policy

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:::akshu224

Policy

1

{

2

"Version": "2012-10-17",

3

"Statement": [

4

{

5

"Effect": "Allow",

6

"Principal": "*",

7

"Action": "s3:GetObject",

8

"Resource": "arn:aws:s3:::akshu224/*"

9

}

10

]

11

}

Step10:

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

aws

Search

[Alt+S]

Europe (Stockholm)

Amazon S3

Buckets

akshu224

akshu224

Info

Objects

Properties

Permissions

Metrics

Management

Access Points

Objects (1)

Copy S3 URI

Copy URL

Download

Open


Delete

Actions

Create folder

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 the [more](#)

Find objects by prefix

<input checked="" type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input checked="" type="checkbox"/>	 Screenshot 2025-02-04 113539.png	png	February 4, 2025, 11:38:08 (UTC+05:30)	115.5 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.