

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: Sabidhaa

Department : ADS

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.

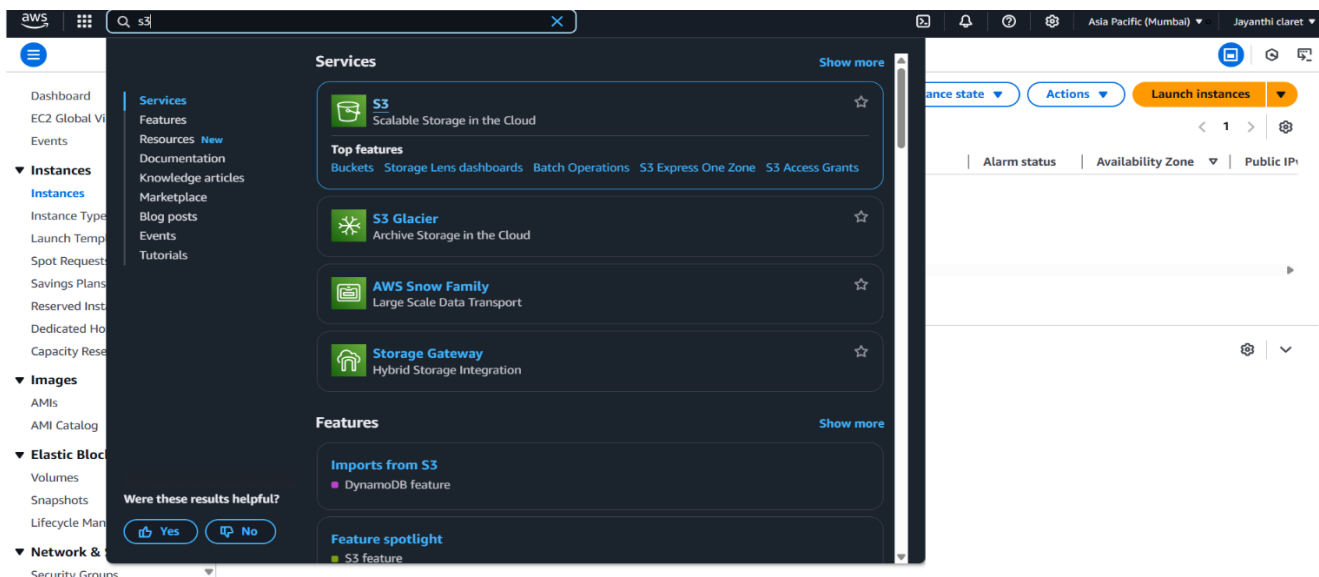
Hands-On Learning of Cloud Storage: AWS S3 provides a practical platform to learn cloud storage concepts, enabling users to create buckets, upload/download files, and manage data at scale.

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

Step 1:

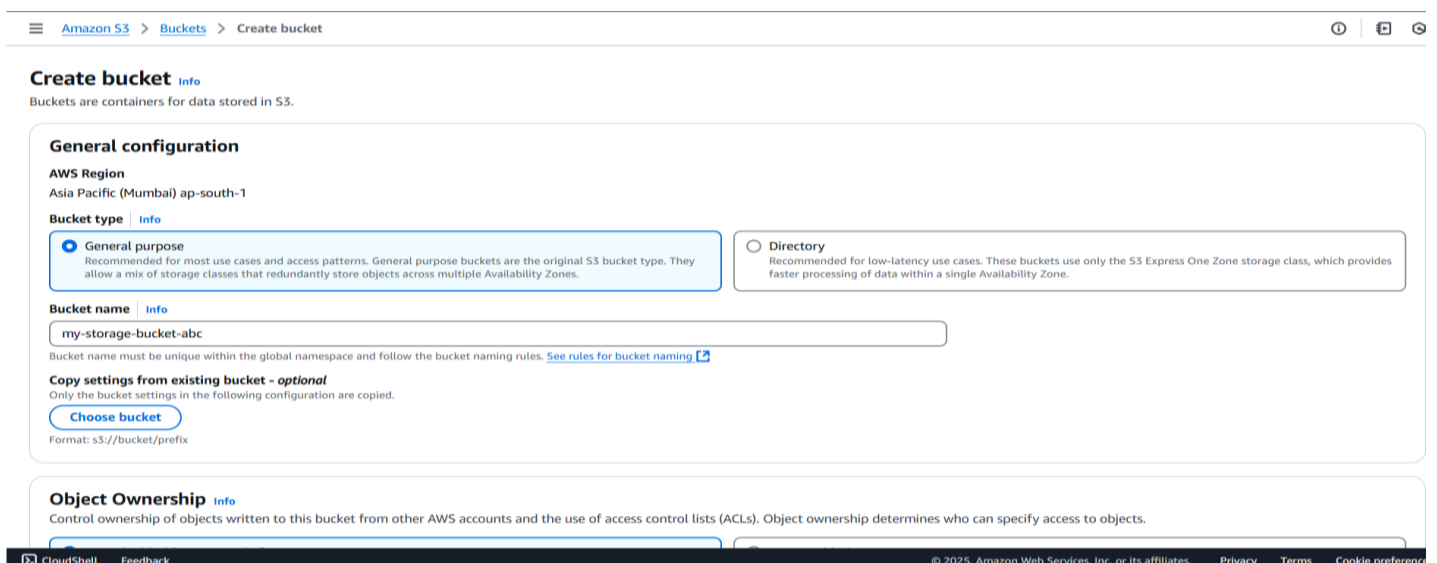
Go to the AWS Management Console, Search for and click on S3



Step 2 :

Click the "Create bucket" button.

Enter a unique bucket name (e.g., my-storage-bucket-123).



Step 3 :

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

Amazon S3 > Buckets > Create bucket

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.

ACLs disabled (recommended)

All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

ACLs enabled

Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Object Ownership

Bucket owner enforced

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.

CloudShell Feedback

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

Step 4 :

Click "Create bucket".

Amazon S3 > Buckets

Successfully created bucket "my-storage-bucket-abc"

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) info

All AWS Regions

Refresh

Copy ARN

Empty

Delete

Create bucket

Buckets are containers for data stored in S3.

Find buckets by name

< 1 >

Settings

Name

▲

AWS Region

▼

IAM Access Analyzer

▼

Creation date

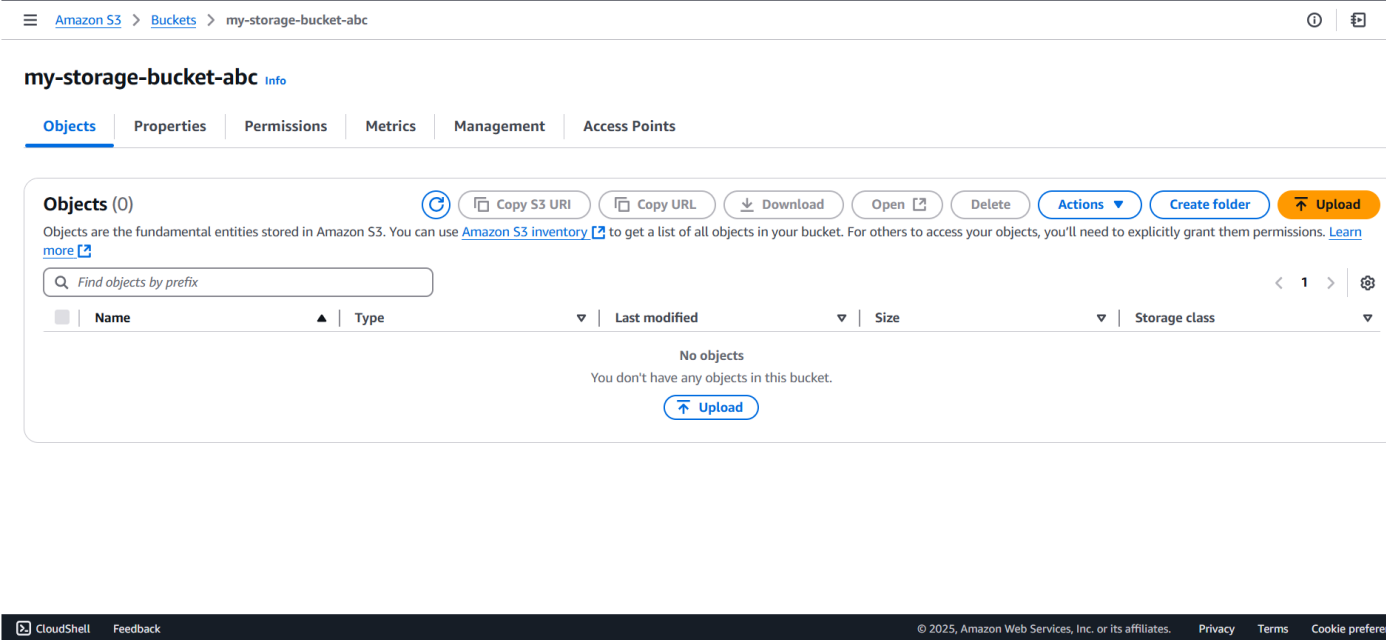
▼

my-storage-bucket-abc

January 28, 2025, 17:48:33 (UTC+05:30)

Step 5 :

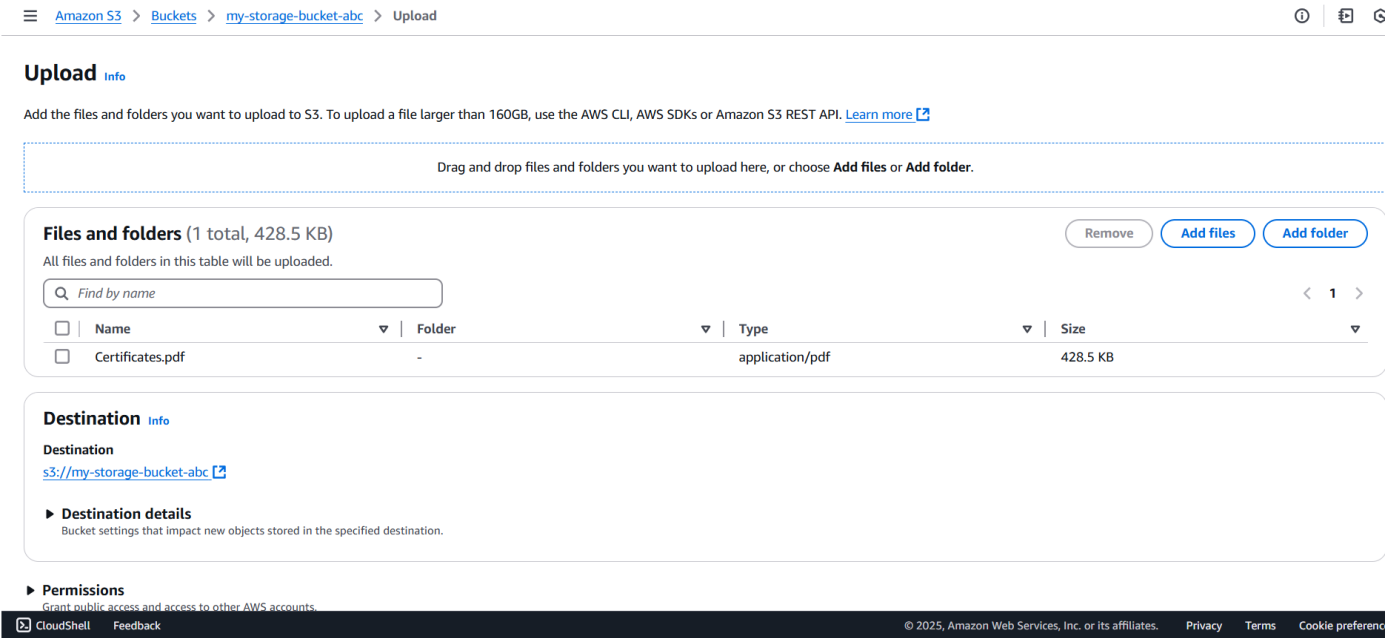
Open your newly created bucket from the S3 console.



Step 6 :

Click "Upload" and then,

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



☰

🔍

🟢 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://my-storage-bucket-abc

Succeeded

🟢 1 file, 428.5 KB (100.00%)

Failed

🔴 0 files, 0 B (0%)

Files and folders

Configuration

Files and folders (1 total, 428.5 KB)

🔍 Find by name

< 1 >

Name	Folder	Type	Size	Status	Error
Certificates.pdf	-	application/pdf	428.5 KB	🟢 Succeeded	-

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preference

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.

☰

Amazon S3

Buckets

my-storage-bucket-abc

Certificates.pdf

🔍

🔍

🔄

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 10

Certificates.pdf

Info

📄 Copy S3 URI

📄 Download

📄 Open

📄 Object actions

Properties

Permissions

Versions

Object overview

Owner

0112dd826d3c0dfa1e8752cb38da7de2f41f021233b68c6115318e55f3c8bd23

AWS Region

Asia Pacific (Mumbai) ap-south-1

Last modified

January 28, 2025, 17:50:33 (UTC+05:30)

Size

428.5 KB

Type

pdf

Key

📄 Certificates.pdf

S3 URI

📄 s3://my-storage-bucket-abc/Certificates.pdf

Amazon Resource Name (ARN)

📄 arn:aws:s3:::my-storage-bucket-abc/Certificates.pdf

Entity tag (Etag)

📄 ea87ed6c5c2ad1ca62cd4657ed14d0f1

Object URL

📄 <https://my-storage-bucket-abc.s3.ap-south-1.amazonaws.com/Certificates.pdf>

Object management overview

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preference

Amazon S3 > Buckets > my-storage-bucket-abc > Certificates.pdf

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
- Storage Lens
 - Dashboards
 - Storage Lens groups
 - AWS Organizations settings
- Feature spotlight 10

Certificates.pdf Info

Copy S3 URI

Properties Permissions Versions

Object overview

Owner
0112dd826d3c0dfa1e8752cb38da7de2f41f021233b68c6115318e55f3c8bd23

AWS Region
Asia Pacific (Mumbai) ap-south-1

Last modified
January 28, 2025, 17:50:33 (UTC+05:30)

Size
428.5 KB

Type
pdf

Key
Certificates.pdf

S3 URI
s3://my-storage-bucket-abc/Certificates.pdf

Amazon Resource Name (ARN)
arn:aws:s3:::my-storage-bucket-abc/Certificates.pdf

Entity tag (Etag)
ea87ed6c5c2ad1ca62cd4657ed14d0f1

Object URL
https://my-storage-bucket-abc.s3.ap-south-1.amazonaws.com/Certificates.pdf

Object management overview

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.

Amazon S3 > Buckets > my-storage-bucket-abc

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
- Storage Lens
 - Dashboards
 - Storage Lens groups
 - AWS Organizations settings
- Feature spotlight 10

my-storage-bucket-abc Info

Objects Properties **Permissions** Metrics Management Access Points

Permissions overview

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

Block public access (bucket settings) Edit

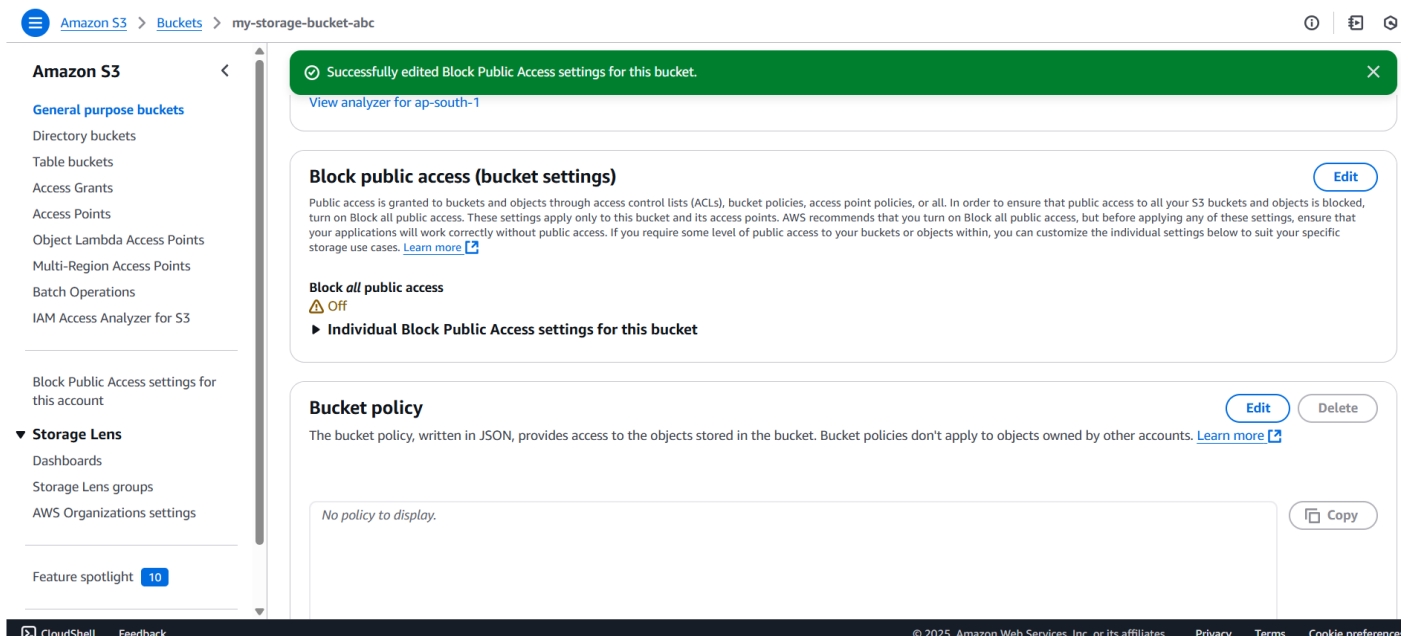
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access 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
On

► Individual Block Public Access settings for this bucket

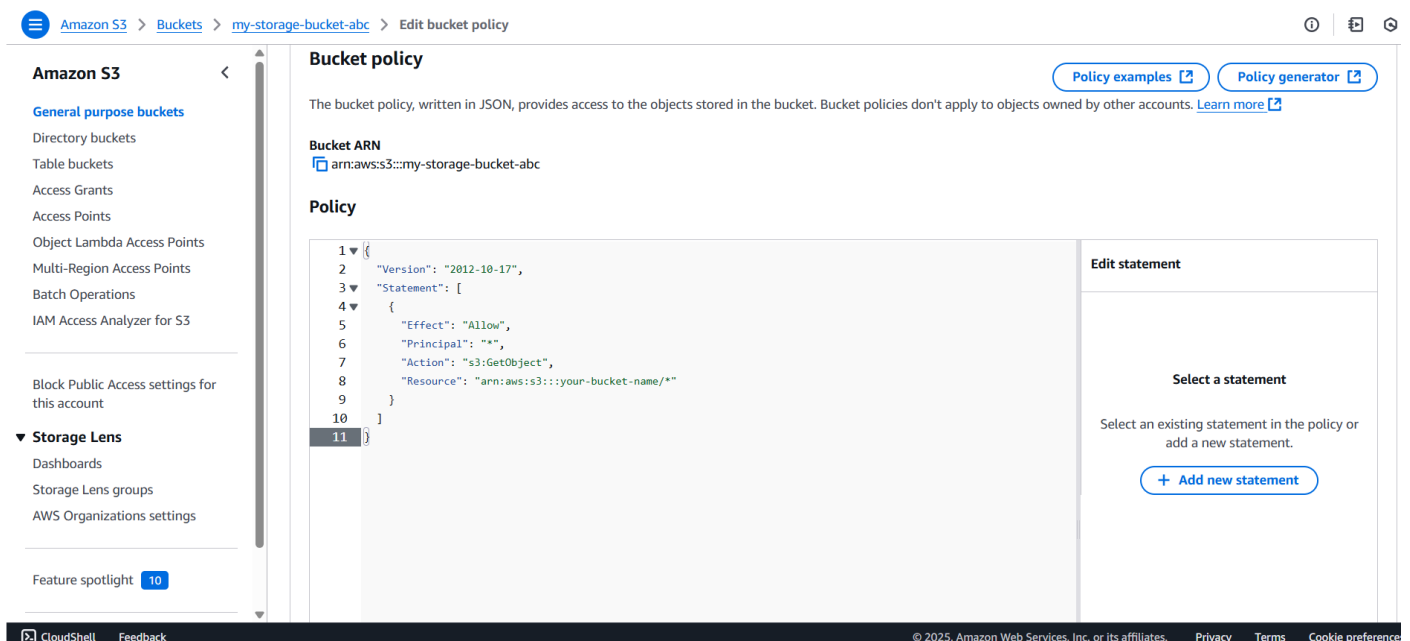
Bucket policy Edit Delete

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](#)



Step 9 :

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



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 10

Successfully edited bucket policy.

Bucket policy

Edit

Delete

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](#)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::my-storage-bucket-abc/*"
    }
  ]
}
```

Copy

Step10:

Use the 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 10

my-storage-bucket-abc

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

< 1 >

<input checked="" type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input checked="" type="checkbox"/>	Certificates.pdf	pdf	January 28, 2025, 17:50:33 (UTC+05:30)	428.5 KB	Standard

CloudShell

Feedback

© 2025 Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)



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.