

Week-3 Securing Cloud Storage

Name- Saish Dhiwar

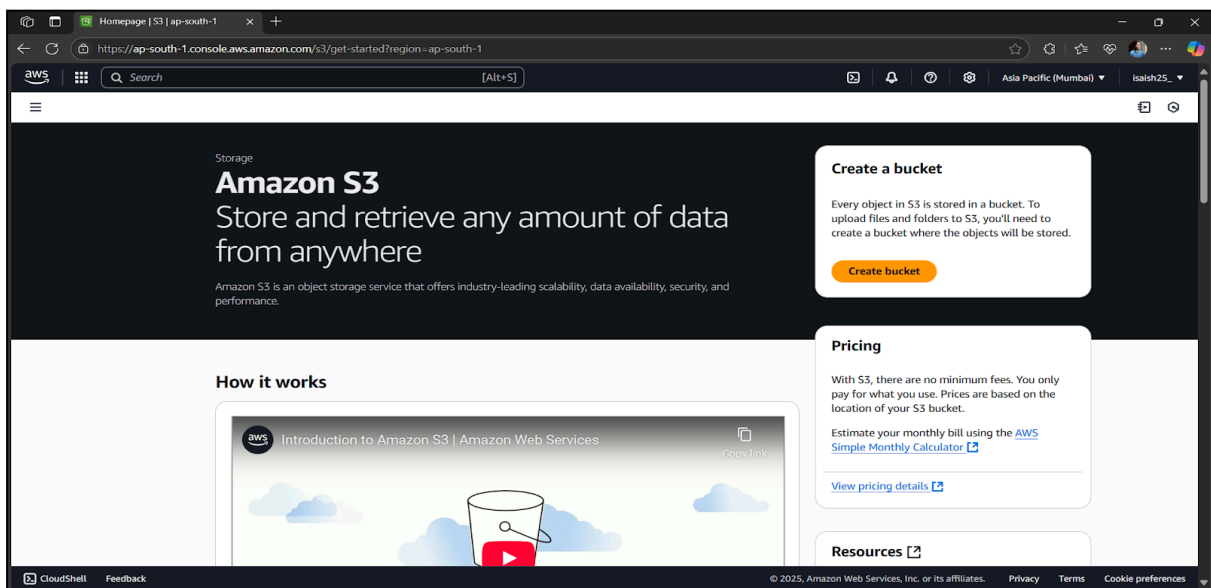
PRN- 2124UCSM2011

Email- saish.dhiwar_24ucs@sanjivani.edu.in

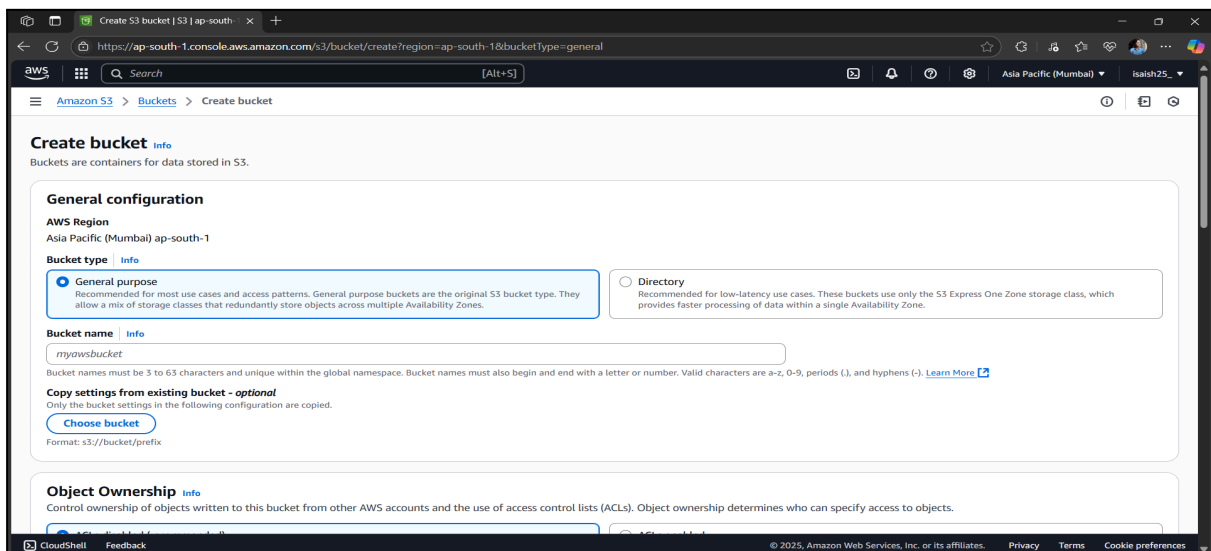
- Task-** 1) Set up an S3 bucket.
2) Apply access control policies.
3) Document security configurations.

Task 1- Steps to Set Up an S3 Bucket-

- 1) Logged in to the AWS Console.
2) Search S3 and then click.



- 3) Then click Create bucket Options.



4) Enter the Bucket name and select the Bucket type.

Amazon S3 > Buckets > Create bucket

Create bucket Info

Buckets are containers for data stored in S3.

General configuration

AWS Region
Asia Pacific (Mumbai) ap-south-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, which provides faster processing of data within a single Availability Zone.

Bucket name Info
bucket-1default encryption, block public access setting for this bucket
Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). [Learn More](#)

Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.
[Choose bucket](#)
Format: s3://bucket/prefix

5) Select the Object Ownership.

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

6) Block Public access setting for this bucket.

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.

7) Select Bucket versioning Enable, and then select Default encryption server-side encryption with Amazon S3 managed key(SSE-S3).

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning

☐ Disable

☒ **Enable**

Tags - optional (0)

You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

No tags associated with this bucket.

[Add new tag](#)

You can add up to 50 tags.

Default encryption Info

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type Info

☒ **Server-side encryption with Amazon S3 managed keys (SSE-S3)**

☐ Server-side encryption with AWS Key Management Service keys (SSE-KMS)

☐ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see [DSSE-KMS pricing on the Storage tab of the Amazon S3 pricing page](#).

8) Select Bucket key Enable, and then click the create bucket button.

Bucket Key
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

☐ Disable
☒ Enable

► **Advanced settings**

After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

Cancel Create bucket

9) Bucket Successfully Created.

Amazon S3 > Buckets

Successfully created bucket "2124ucsm2011"
To upload files and folders, or to configure additional bucket settings, choose [View details](#).

General purpose buckets All AWS Regions Directory buckets

General purpose buckets (1) Info [Copy ARN](#) Empty Delete Create bucket

Buckets are containers for data stored in S3.

Find buckets by name

Name	AWS Region	Creation date
2124ucsm2011	Asia Pacific (Mumbai) ap-south-1	July 17, 2025, 22:29:20 (UTC+05:30)

► **Account snapshot** Info [View dashboard](#)
Updated daily
Storage Lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets.

► **External access summary - new** Info
Updated daily
External access findings help you identify bucket permissions that allow public access or access from other AWS accounts.

Task 2- Steps to Apply Access Control Policies-

1) Open S3 > Bucket > 2124ucsm2011 > Permission.

Amazon S3 > Buckets > 2124ucsm2011

2124ucsm2011 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](#)

2) Scroll down and Click Edit.

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](#)

Public access is blocked because Block Public Access settings are turned on for this bucket
To determine which settings are turned on, check your Block Public Access settings for this bucket. Learn more about [using Amazon S3 Block Public Access](#)

3) Then write the following code to block public access, and save the policy.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "AllowOnlyOwner",
6       "Effect": "Deny",
7       "Principal": "*",
8       "Action": "s3:GetObject",
9       "Resource": "arn:aws:s3:::2124ucsm2011/*",
10      "Condition": {
11        "StringNotEquals": {
12          "aws:PrincipalAccount": "355433852359"
13        }
14      }
15    }
16  ]
17 }
18
```

4) Save the policy → Now, only the bucket owner's account can access the objects. All other access is denied.

Amazon S3 > Buckets > 2124ucsm2011

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](#)

Public access is blocked because Block Public Access settings are turned on for this bucket
To determine which settings are turned on, check your Block Public Access settings for this bucket. [Learn more about using Amazon S3 Block Public Access](#)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowOnlyOwner",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::2124ucsm2011/*",
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalAccount": "355433852359"
        }
      }
    }
  ]
}
```

[Copy](#)

Successfully edited bucket policy.

Access control list (ACL) [Edit](#)

Grant basic read/write permissions to other AWS accounts. [Learn more](#)

This bucket has the bucket owner enforced setting applied for Object Ownership
When `bucket_owner_enforced` is applied, use bucket policies to control access. [Learn more](#)

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account) Canonical ID: e8de8db760b57ea5702771838bbe4bda13b1f9a7422938eeb025a0981cb5452d	List, Write	Read, Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	-	-
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	-	-
S3 log delivery group Group: http://acs.amazonaws.com/groups/s3/LogDelivery	-	-

Task 3- Document security configurations.

1) Default encryption with Amazon S3 managed keys (SSE-S3) is enabled to protect all objects by default.

Default encryption [Info](#) [Edit](#)

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type [Info](#)
Server-side encryption with Amazon S3 managed keys (SSE-S3)

Bucket Key
When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. [Learn more](#)
Enabled

2) Versioning is enabled to keep all versions of objects for recovery and rollback.

Bucket VersioningEdit

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning
Enabled

Multi-factor authentication (MFA) delete
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](#)
Disabled

3) Access policy restricts object access to only the bucket owner's account.

Bucket policyEditDelete

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](#)

Public access is blocked because Block Public Access settings are turned on for this bucket
To determine which settings are turned on, check your Block Public Access settings for this bucket. Learn more about [using Amazon S3 Block Public Access](#)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowOnlyOwner",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::2124ucsm2011/*",
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalAccount": "355433852359"
        }
      }
    }
  ]
}
```

Copy

4) Public access is blocked using AWS's Block Public Access settings for added security.

Public access is blocked because Block Public Access settings are turned on for this bucket
To determine which settings are turned on, check your Block Public Access settings for this bucket. Learn more about [using Amazon S3 Block Public Access](#)