

Assignment No: 4

Problem Statement: Create a private bucket in AWS. Upload a file and check by reassigned URL whether you can access the file or not.

Solution:

1. At first go to the s3 bucket and click on create bucket option.
2. Give a name to the bucket.
3. Keeping all other option as default, just create the 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](#)
archak890bucket

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

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

Tags - optional (0)
You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

No tags associated with this bucket.

[Add tag](#)

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](#).

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](#)

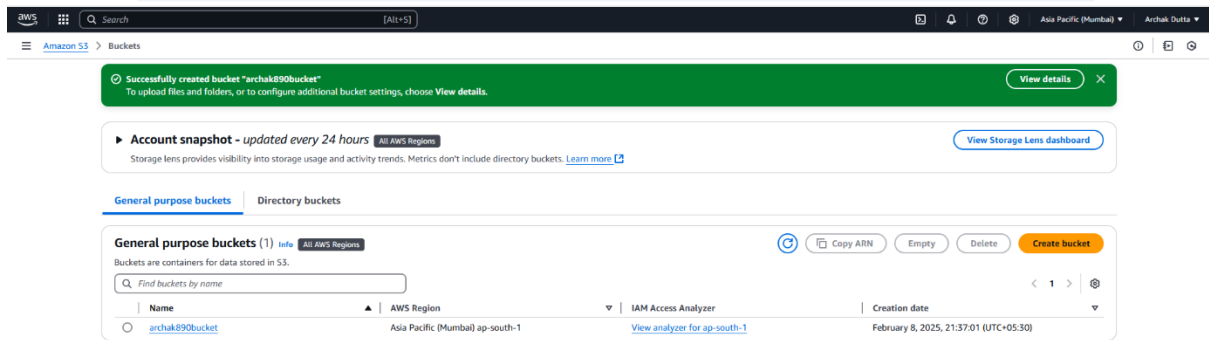
☒ **Enable**

☐ **Disable**

Advanced settings

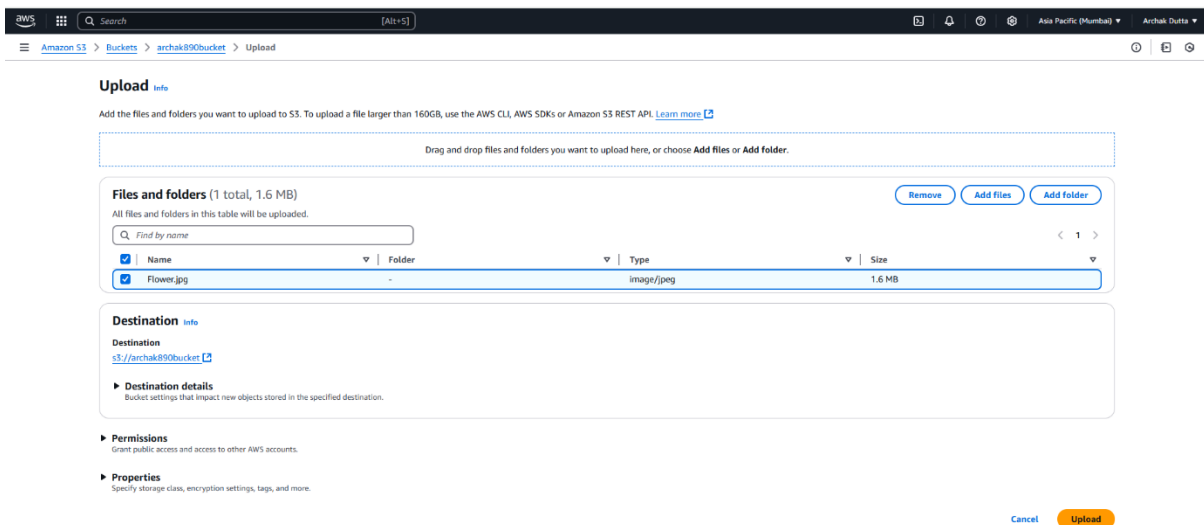
After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

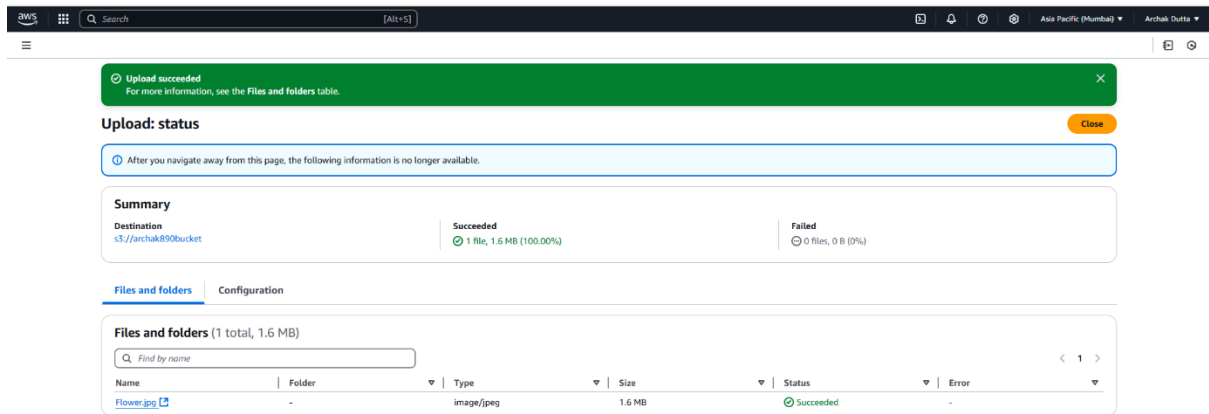
[Cancel](#) [Create bucket](#)



4.Go to the created bucket and click on the upload option.

5.And upload a file(.jpg,.png,.pdf etc) in the bucket.





6. Then tick the bucket and copy the URL to check whether it is working or not.

7. But it is not working.



8. So if we want to give access to this private bucket we can create a preassigned URL for some given amount of time.

9. Then, we can use this URL to access the file for the permissible amount of time.

10. Hence, a private bucket is created.

