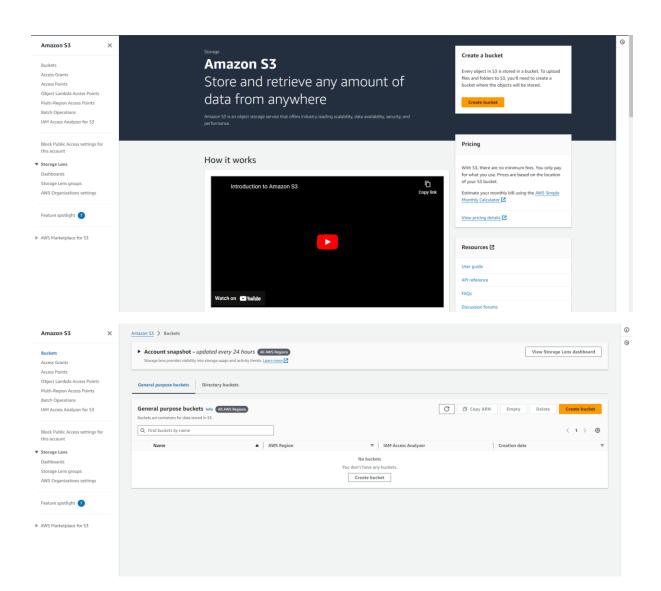
# **CLOUD COMPUTING**

# PRACTICAL 2

NAME: BHARVI CHAVDA

**ROLL NO.: A006** 

SAP ID: 86062300028



# **General configuration**

**AWS Region** 

Asia Pacific (Mumbai) ap-south-1

Bucket name Info

mybucket1277

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

# 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.

 $\_$   $extbf{Z}$  Block public access to buckets and objects granted through  $\emph{new}$  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.

#### **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 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)
- O Server-side encryption with AWS Key Management Service keys (SSE-KMS)
- O 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

- Disable
- Enable



