Name : Nakul Lahode

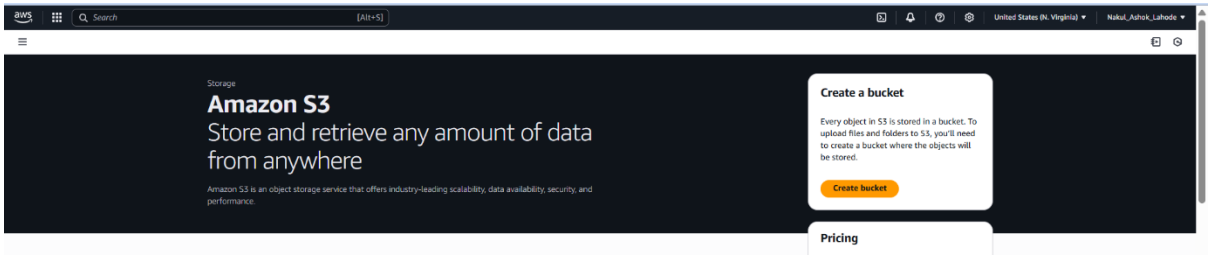
Task- 01 : Create and configure cloud storage on AWS S3 or Google Cloud Storage by setting up a bucket with example files uploaded and access permissions properly configured.

Overview of AWS S3 :

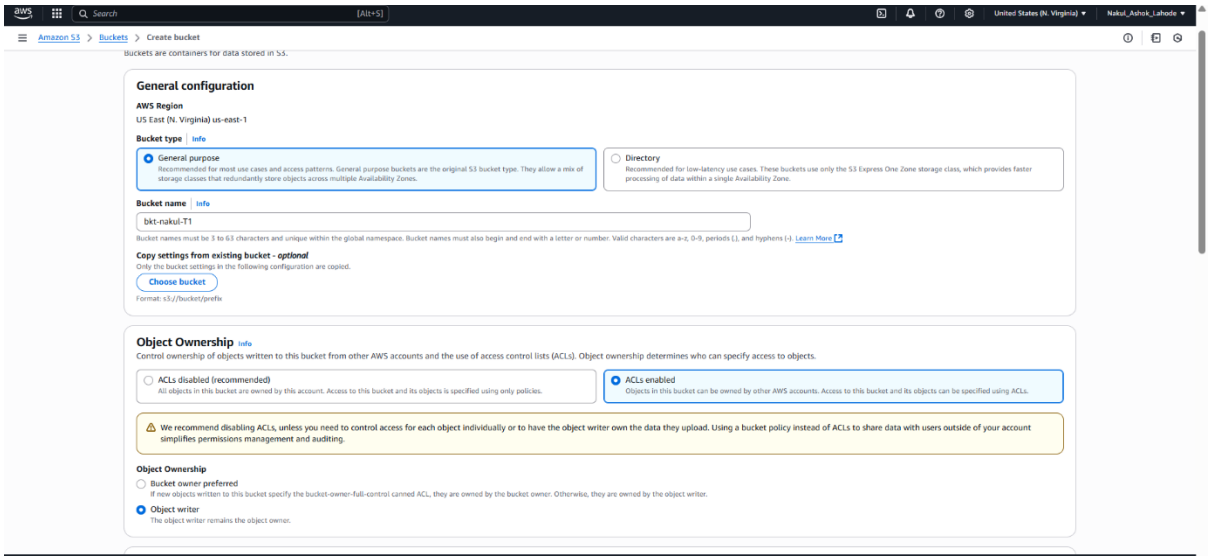
1. **Scalable Object Storage**
    - Amazon S3 provides highly scalable, reliable, and low-latency object storage for any amount of data. Data is stored in buckets as individual objects with unique keys.
2. **High Durability & Availability**
    - Offers **99.999999999% durability** by replicating data across multiple **Availability Zones (AZs)**, ensuring reliable data protection.
3. **Flexible Storage Classes**
    - Multiple classes like **Standard**, **Intelligent-Tiering**, **Infrequent Access (IA)**, and **Glacier** help reduce costs based on data access patterns.
4. **Robust Security & Access Control**
    - Includes **encryption (SSE-S3, SSE-KMS)**, **IAM policies**, **bucket policies**, **ACLs**, and **Block Public Access** settings for secure data storage.
5. **Versioning & Lifecycle Management**
    - Supports **object versioning** for recovery and auditing, and **lifecycle rules** to automatically transition or delete data over time.
6. **Integration with AWS Services**
    - Seamlessly integrates with **Lambda**, **Athena**, **CloudFront**, **CloudTrail**, and others for automation, analytics, and content delivery.
7. **Use Cases & Cost-Effectiveness**
    - Ideal for **backup**, **static website hosting**, **media storage**, and **big data**. It uses a **pay-as-you-go model** based on storage, requests, and data transfer.

Step 1: Create a Bucket and Enable Static Website Hosting

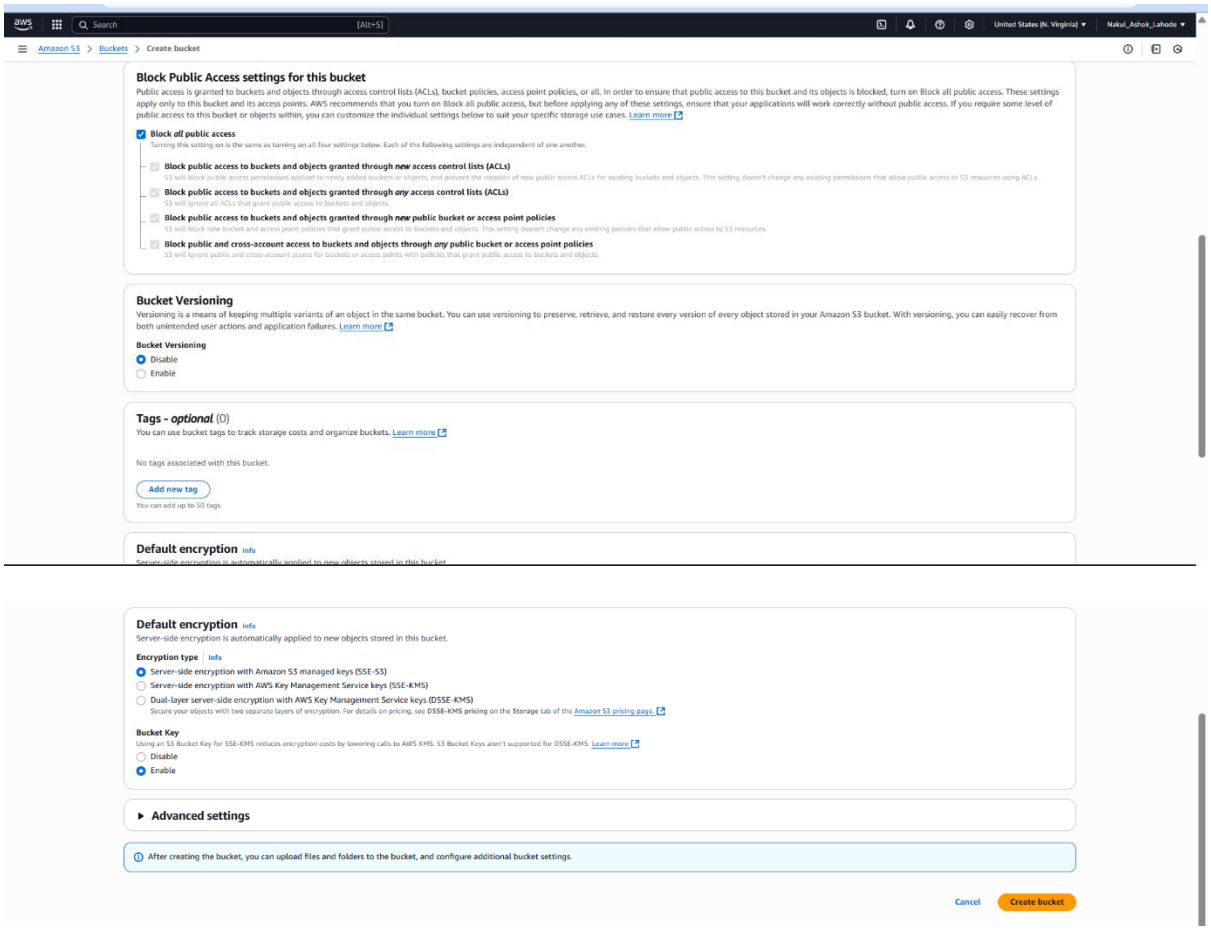
1. Log in to the AWS Management Console.
2. Navigate to **S3** under Services.
3. Click on **"Create bucket"**.



4. Configure the bucket settings:
    - Choose a unique **bucket name**.
    - Select **"General purpose"** as the bucket type.
    - Enable **ACLs (Access Control Lists)** under **Object Ownership**.



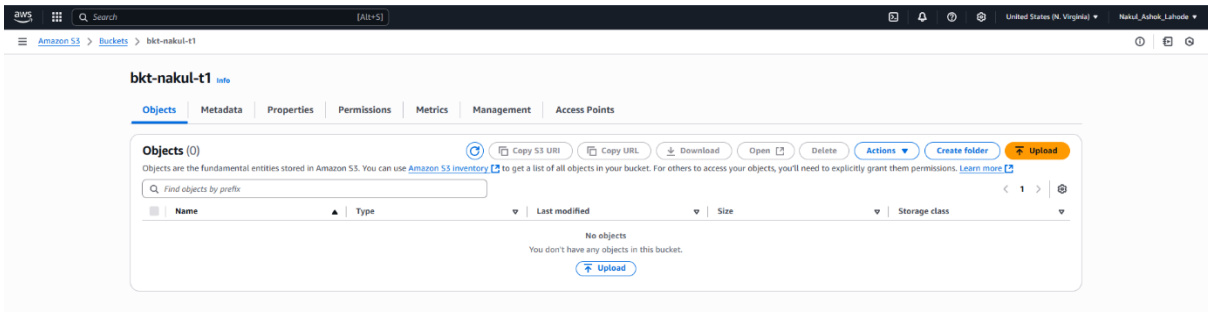
    - Set object ownership to **"Object writer"**.
    - **Block all public access** initially.
    - Choose **"Server-side encryption with Amazon S3 managed key (SSE-S3)"**.



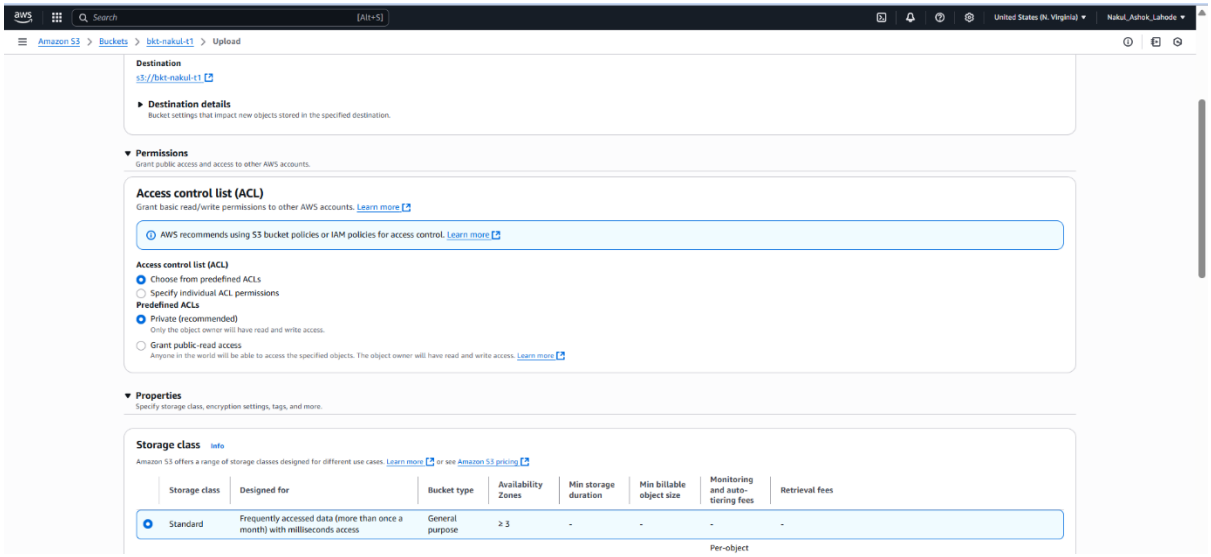
5. Click **Create bucket** to finalize setup.

Step 2: Upload a File to the Bucket

1. Open the newly created bucket.
2. Click on **“Upload”**.

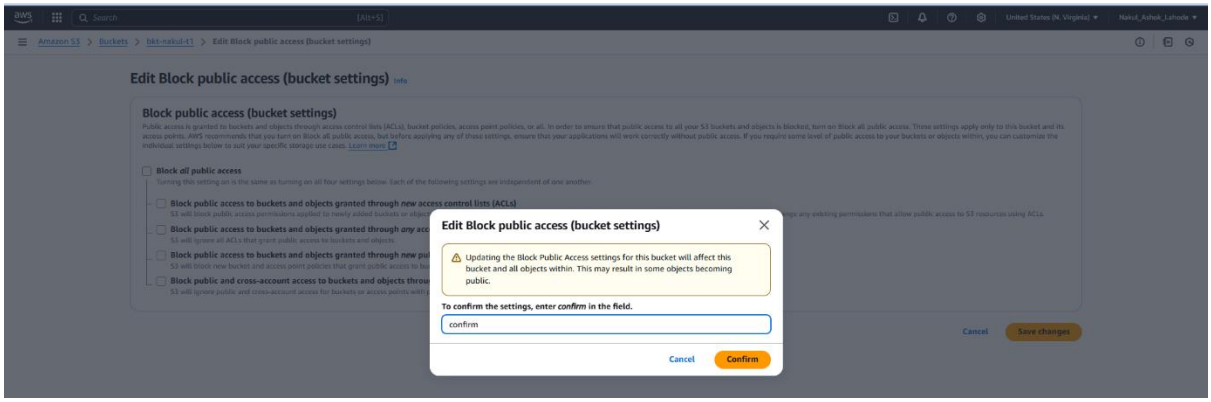


3. Select the file to be uploaded.
4. Choose desired **ACLs** and **Storage class** during upload.
5. Click **Upload** to complete the file upload process.

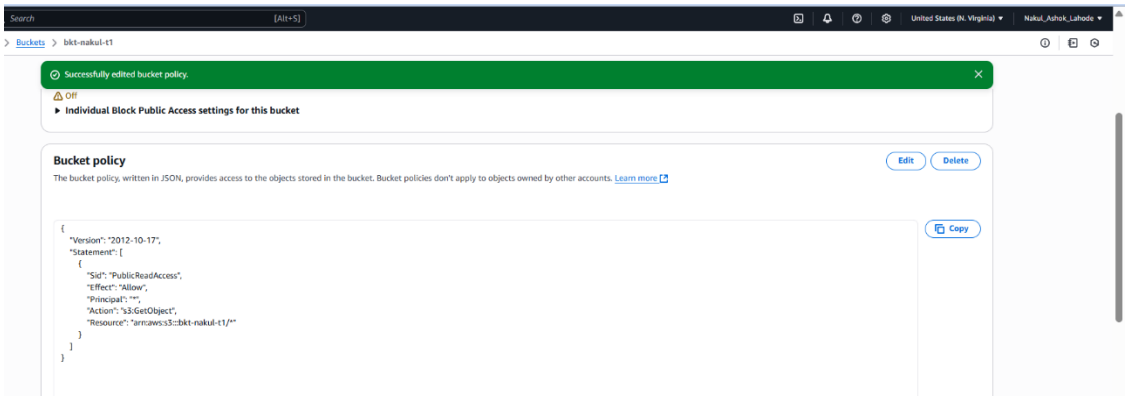


Step 3: Modify Bucket Permissions

1. Select the bucket and navigate to **Permissions**.
2. Under **Block public access (bucket settings)**, disable the block and save changes.



3. Open the **Bucket Policy** editor and write a policy to allow **public read access**.



- Save the policy changes.

Step 4: Access the File Publicly

1. Navigate to the uploaded file within the bucket.
2. Copy the **Object URL**.
3. Paste it in a browser to verify **public read access**.