

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

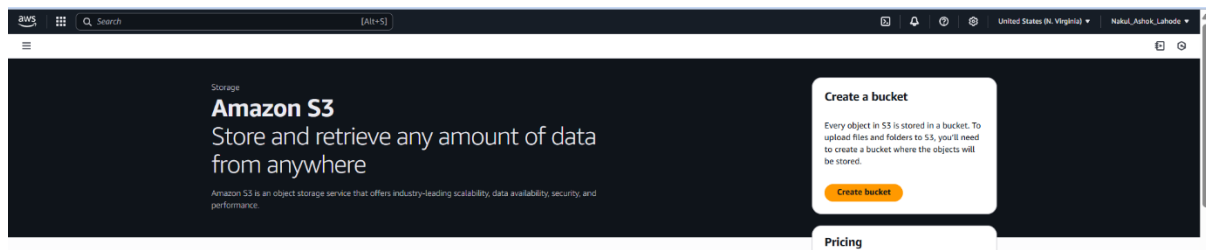
- Seamlessly integrates with **Lambda**, **Athena**, **CloudFront**, **CloudTrail**, and others for automation, analytics, and content delivery.

7. Use Cases & Cost-Effectiveness

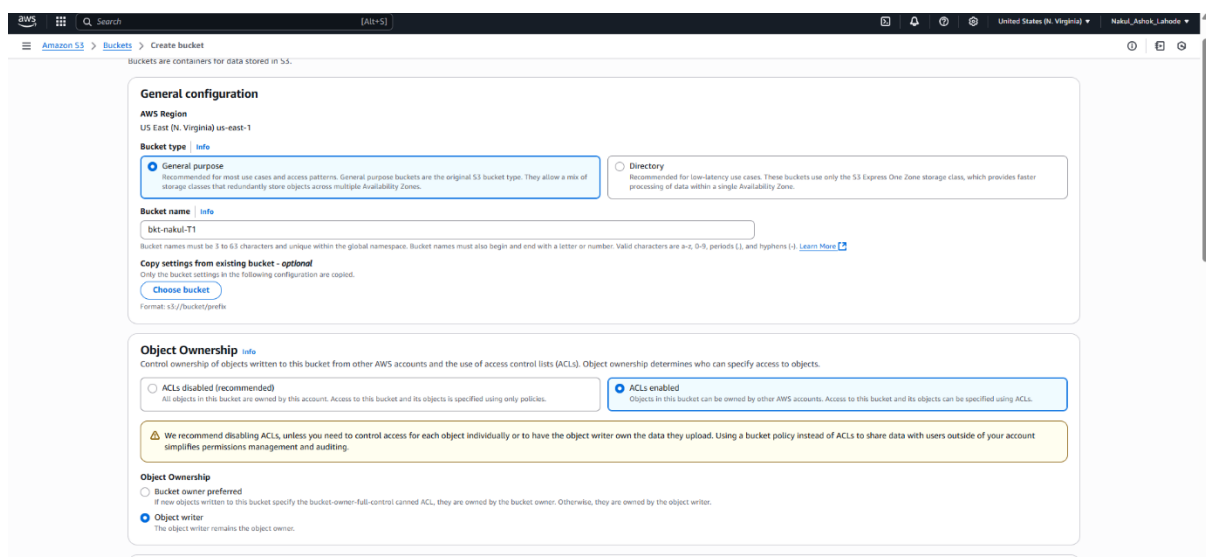
- Ideal for **backup**, **static website hosting**, **media storage**, and **big data**. It uses a **pay-as-you-go model** based on storage, requests, and data transfer.

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)”**.

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 granted to newly created 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 does not 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 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](#).

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](#)

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”**.

bkt-nakul-t1 [info](#)

[Objects](#) [Metadata](#) [Properties](#) [Permissions](#) [Metrics](#) [Management](#) [Access Points](#)

Objects (0)

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](#)

Name	Type	Last modified	Size	Storage class
No objects				

You don't have any objects in this bucket.

[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.

Destination
s3://bkt-nakul-t1

Destination details
Bucket settings that impact new objects stored in the specified destination.

Permissions
Grant public access and access to other AWS accounts.

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

☐ AWS recommends using S3 bucket policies or IAM policies for access control. [Learn more](#)

Access control list (ACL)
☒ Choose from predefined ACLs
☐ Specify individual ACL permissions

Predefined ACLs
☒ Private (recommended)
Only the object owner will have read and write access.
☐ Grant public-read access
Anyone in the world will be able to access the specified objects. The object owner will have read and write access. [Learn more](#)

Properties
Specify storage class, encryption settings, tags, and more.

Storage class [info](#)
Amazon S3 offers a range of storage classes designed for different use cases. [Learn more](#) or see [Amazon S3 pricing](#)

Storage class	Designed for	Bucket type	Availability Zones	Min storage duration	Min billable object size	Monitoring and auto-tiering fees	Retrieval fees
<input checked="" type="radio"/> Standard	Frequently accessed data (more than once a month) with milliseconds access	General purpose	> 3	-	-	-	-

Per-object

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.

Edit Block public access (bucket settings) [info](#)

Block public access (bucket settings)
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 case. [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 assigned to newly created buckets or objects.
- ☐ 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 bucket policies
S3 will block new bucket and access point policies that grant public access to buckets and objects.
- ☐ Block public and cross-account access to buckets and objects through existing permissions that allow public access to S3 resources using ACLs.
S3 will ignore public and cross-account access for buckets or objects owned by you.

Edit Block public access (bucket settings)

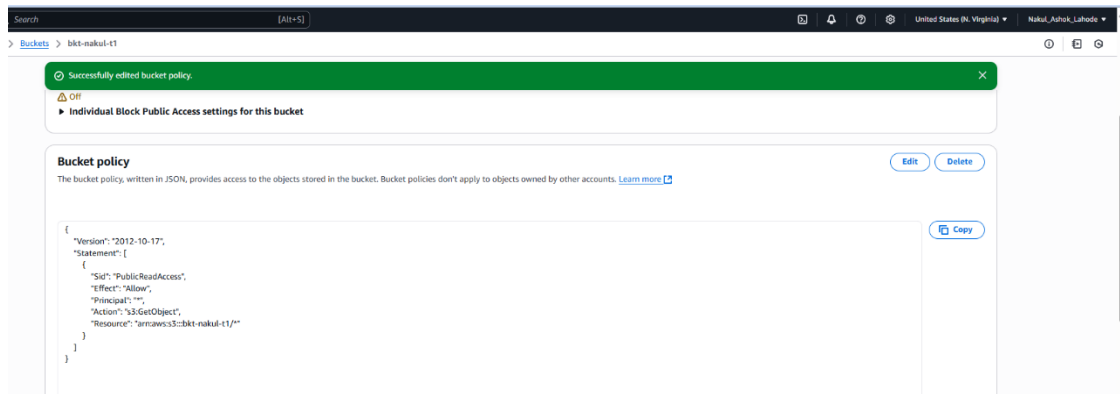
Updating the Block Public Access settings for this bucket will affect this bucket and all objects within. This may result in some objects becoming public.

To confirm the settings, enter confirm in the field.

confirm

Cancel 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**.

