1. Introduction to S3

Amazon S3 (Simple Storage Service) is a scalable, secure object storage service that provides high durability and low-latency access to data. S3 is commonly used to store objects like backups, logs, media files, and web assets.

2. Creating an S3 Bucket

- Log in to AWS Console: Go to AWS Console and log in.
- **Navigate to S3:** In the search bar at the top, type “S3” and click on the S3 service to open it.
- **Create a Bucket:** Click on the Create bucket button.

- **Bucket name:** Enter a globally unique name for your bucket (e.g., my-unique-bucket-accno-region).
- **Region:** Select the AWS region closest to where you want your data to be stored (e.g., US East (N. Virginia)).
- **Bucket settings:** Leave the default settings unless you need special configurations like versioning, logging, or encryption.

- **Set Permissions:**
    - For now, leave the default Block all public access selected to keep your data private.
    - Click Create bucket.
- You've created your first S3 bucket. It's like a container that will hold your files.

3. Uploading Files to S3

- **Go to Your Bucket:** Click on the bucket you just created from the S3 console.
- Click on **Upload:**
    - Select Upload at the top of the page.
    - Click Add files and choose a file to upload from your computer.
- **Configure Permissions (Optional)**: You can set permissions to allow others to access the file or keep it private.
- **Start Upload:** Click Upload to upload the file to your bucket.
- Our file is now stored in S3. We can access it by clicking on the file name.

4. What is Object Storage?

Object storage in S3 means storing data as objects rather than files or blocks. Each object has:

- **Data:** The file itself.
- **Metadata:** Information like the file type, size, and custom tags.
- **Unique ID:** A unique identifier (key) for the object.

Real-life Example:

- Imagine uploading a photo. The photo is the data, the metadata could be the photo's resolution, file type, and upload date, and the key is the unique name you give it (e.g., vacation-photo.jpg).

5. S3 Storage Classes

Amazon S3 offers multiple storage classes based on how frequently data is accessed and how long you need to retain it. Here are some common ones:

Step-by-Step to Set Storage Class:

- When Uploading Files: During the upload process, you can select the Storage Class.
- Choose from:
  - **Standard:** High-frequency access (e.g., website files).
  - **Infrequent Access (IA):** For data that is accessed less frequently (e.g., backups).
  - **Glacier:** For archival data that you rarely need to access (e.g., compliance data).

- **Intelligent-Tiering:** Automatically moves data between frequent and infrequent access.

Real-life Example:

- **Standard** for frequently accessed website images.
- **Glacier** for storing old records or company archives that you rarely need.

MANISH BATRA

6. Enabling Versioning

Versioning allows you to keep multiple versions of an object in S3. This helps if you accidentally delete or overwrite files.

- **Step-by-Step to Enable Versioning:**
  - Go to your S3 bucket.
  - Click on the **Properties** tab.
  - Under **Bucket Versioning**, click Edit and select Enable.
  - Click Save changes.

Real-life Example:

- Imagine you accidentally delete or overwrite a file. With versioning, you can restore the previous version.

7. S3 Lifecycle Policies

Lifecycle policies automate the transition of data between storage classes and deletion of old objects. This is useful for managing costs.

- **Step-by-Step to Set Lifecycle Rule:**
  - Go to your S3 bucket.
  - Click on the **Management** tab.
  - Under Lifecycle rules, click Create lifecycle rule.
  - Name the rule (e.g., "Move logs to Glacier").
  - **Set the rule:**
    - Transition objects to Glacier after 30 days.
    - Delete objects after 365 days.
    - Click Create rule.

Real-life Example:

- **Logs:** Move logs to Glacier after 30 days for cheaper storage and delete them after 1 year.

8. Access Control (ACLs) and Permissions

You can manage access to your S3 bucket and its contents using **Access Control Lists (ACLs) or Bucket Policies**

- **Step-by-Step to Set Permissions:**
  - Go to your S3 bucket.
  - Click on **Permissions.**
  - Under **Bucket Policy** or **Access Control List**, you can:
    - Grant public access to files.
    - Grant specific users or roles permissions (Read, Write).

Real-life Example:

- You want to make a file publicly available, such as an image for your website. You'd set the file's ACL to public-read.

9. Encryption Options

Amazon S3 supports several types of encryption to protect your data at rest and in transit.

- **Types of Encryption:**
  - Server-Side Encryption (SSE): AWS handles encryption for you.
    - **SSE-S3:** Standard encryption managed by AWS.
    - **SSE-KMS:** Uses AWS Key Management Service for more control over encryption keys.
    - **SSE-C:** You manage the encryption keys.

Step-by-Step to Enable Encryption:

- During upload, under Encryption, choose the encryption type (e.g., SSE-S3).
- For SSE-KMS, you'll need to select a KMS key (can be the default key or custom).

Real-life Example:

- You want to ensure sensitive financial documents are encrypted at rest. Use SSE-KMS to control the encryption keys.

MANISH BATRA

10. Cross-Region Replication (CRR)

Cross-Region Replication (CRR) automatically replicates objects from one S3 bucket to another in a different region.

- **Step-by-Step to Enable CRR:**
  - Enable **Versioning** on both the source and destination buckets.
  - Go to the **Management** tab of your source bucket.
  - Click **Replication** → Add Rule.
  - Select the **destination** region and bucket.
  - Configure **replication** for specific objects or the entire bucket.

Real-life Example:

- You want to ensure data durability and availability in another region. Use CRR to replicate your data for disaster recovery.

11. S3 Event Notifications

You can configure event notifications to trigger actions when specific events occur in your S3 bucket (e.g., object uploads, deletions).

- **Step-by-Step to Set Up Event Notification:**
  - Go to your S3 bucket.
  - Click **Properties** → **Event Notifications** → Create **Event Notification.**
  - Select the **event type** (e.g., ObjectCreated).
  - Choose a destination (e.g., **SNS topic, Lambda function, SQS queue**).
  - Click **Save changes**.

Real-life Example:

- Whenever a file is uploaded, you might want to trigger a Lambda function that processes or resizes the file.

12. S3 Object Locking (Compliance)

S3 Object Locking helps ensure that objects cannot be deleted or overwritten for a fixed retention period. It's useful for compliance scenarios.

- **Step-by-Step to Enable Object Locking:**
  - Enable Versioning on your bucket.
  - Go to the Properties tab and enable Object Locking.
  - When uploading an object, you can set a retention period or apply a legal hold.

Real-life Example:

- You need to store financial records for 7 years and ensure they cannot be tampered with or deleted. Use Object Locking to enforce this retention period.

MANISH BATRA