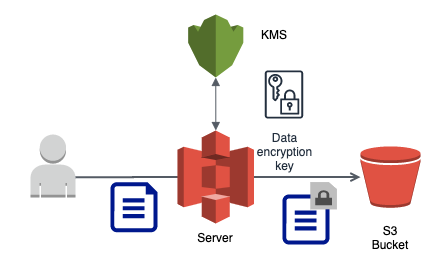
## **Configuring AWS S3 and KMS for Restricted Data Access**

****

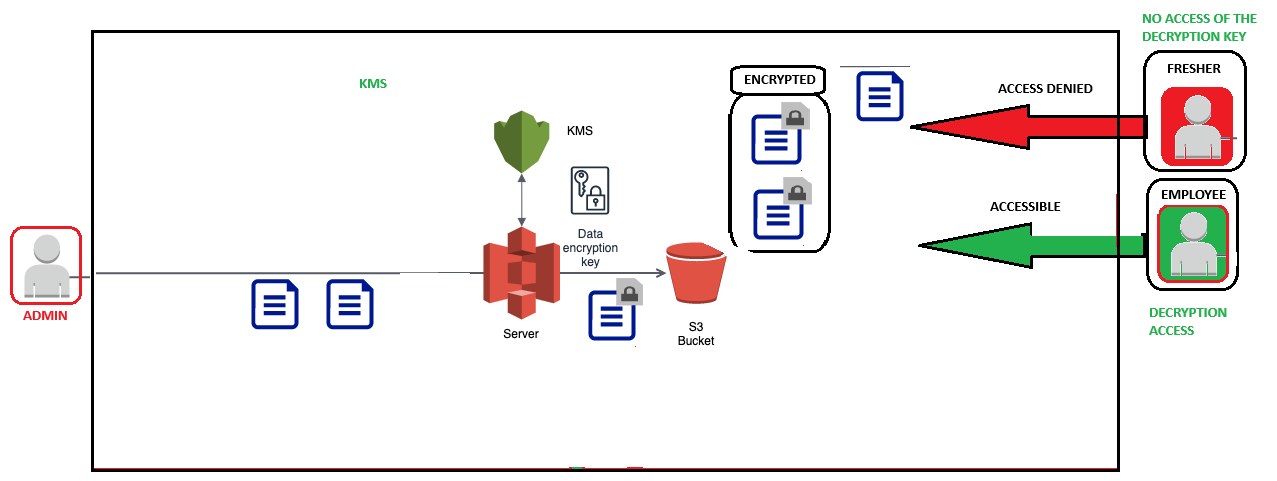
#### **Introduction**

This documentation provides a comprehensive guide to setting up a secure AWS environment using Amazon S3 for storage and AWS Key Management Service (KMS) for encryption. The scenario outlines creating two IAM users with S3 read-only access and configuring selective encryption on S3 objects using a symmetric KMS key.

#### **Objective**

The primary goal is to securely store data in an S3 bucket where:

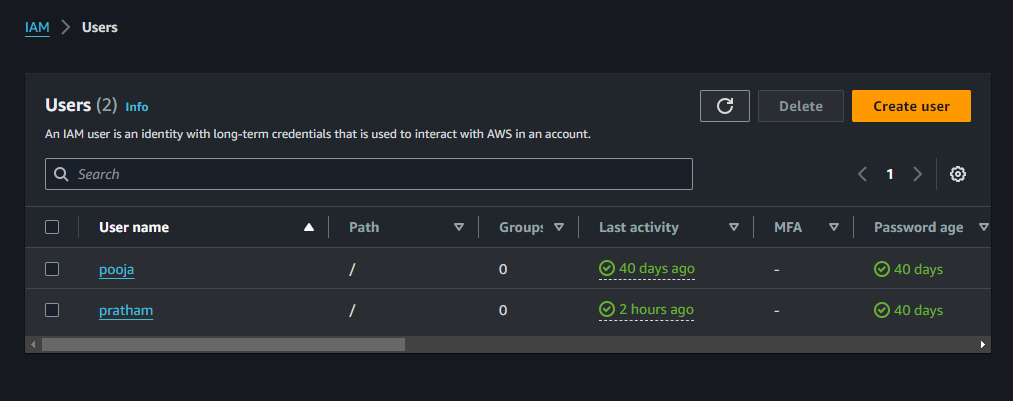
* Two IAM users (USER1 and USER2) have read-only access to all objects in the bucket.
* Some objects are encrypted using a symmetric KMS key, which both Admin and User1 can decrypt.
* The setup ensures compliance with security policies while enabling effective data access and protection.



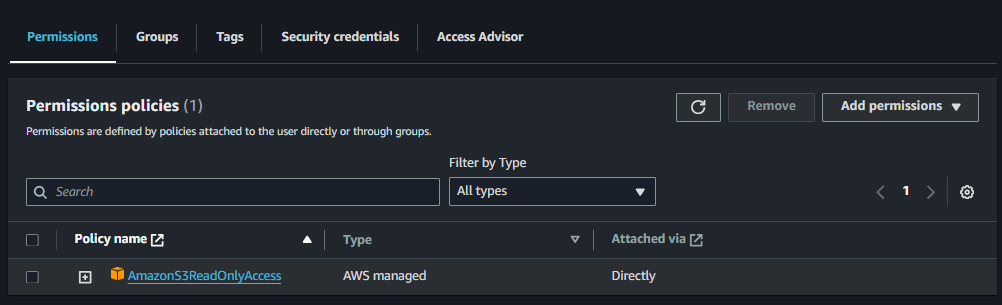
#### **Setup Configuration**

##### **Step 1: Creating IAM Users**

1. **Log in to AWS Management Console** and navigate to the IAM dashboard.
2. **Create two users (Admin and User1)**:
   * Click on “Add user”.

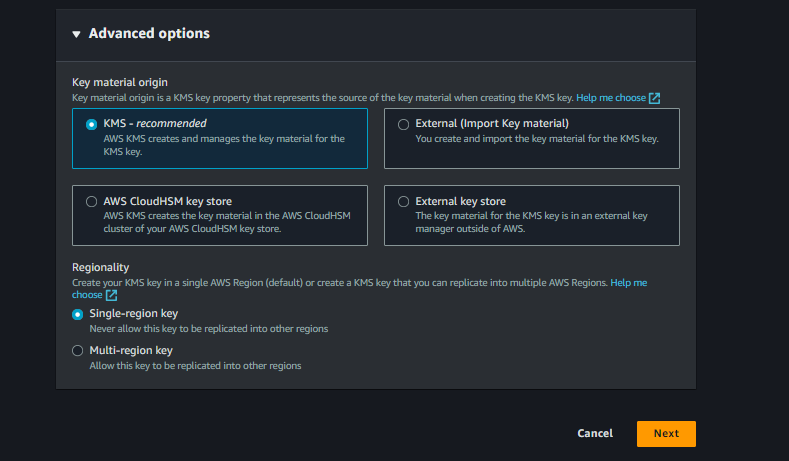
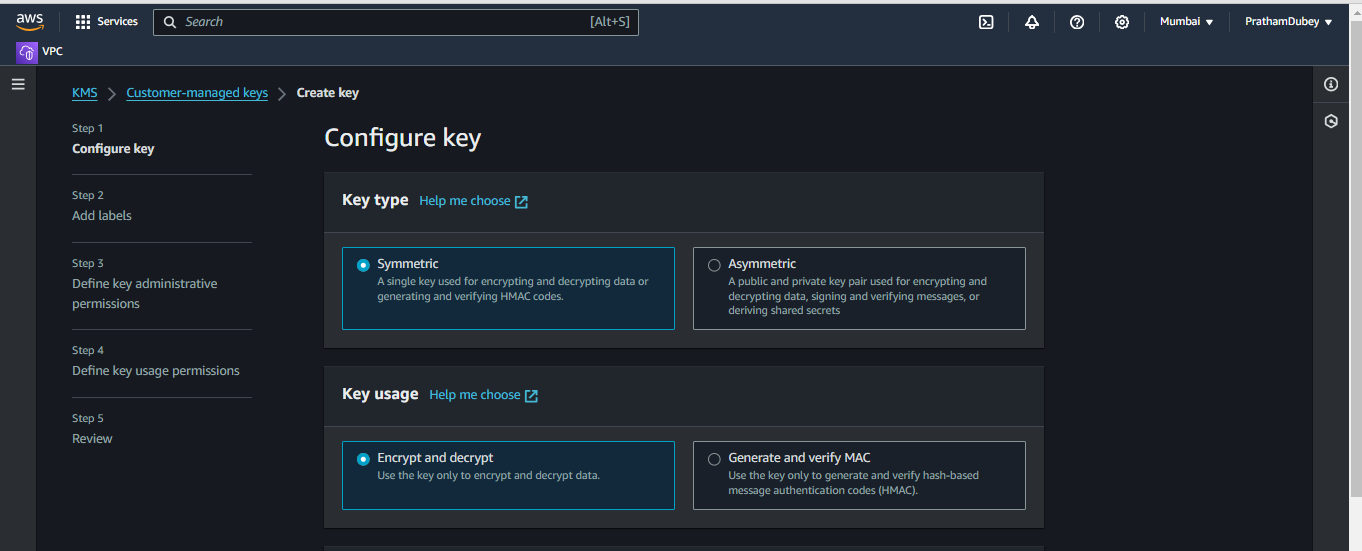


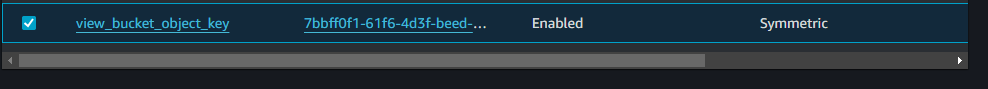
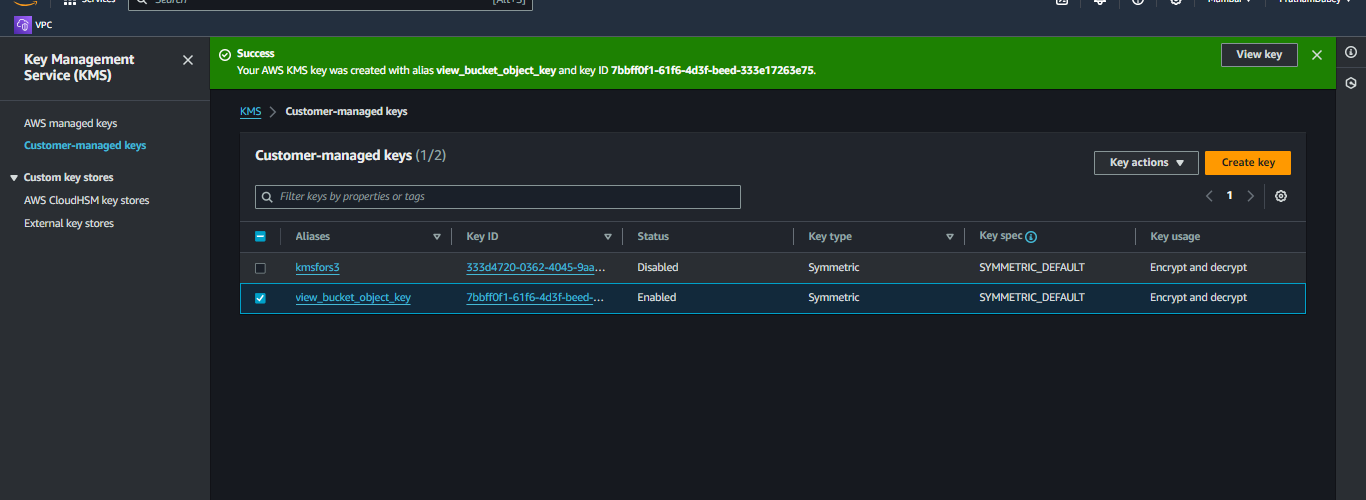
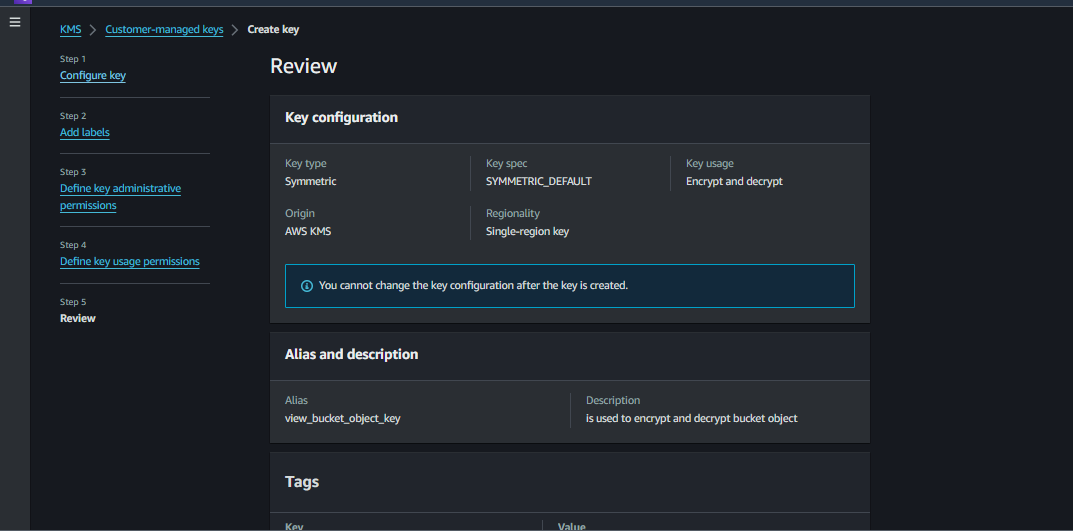
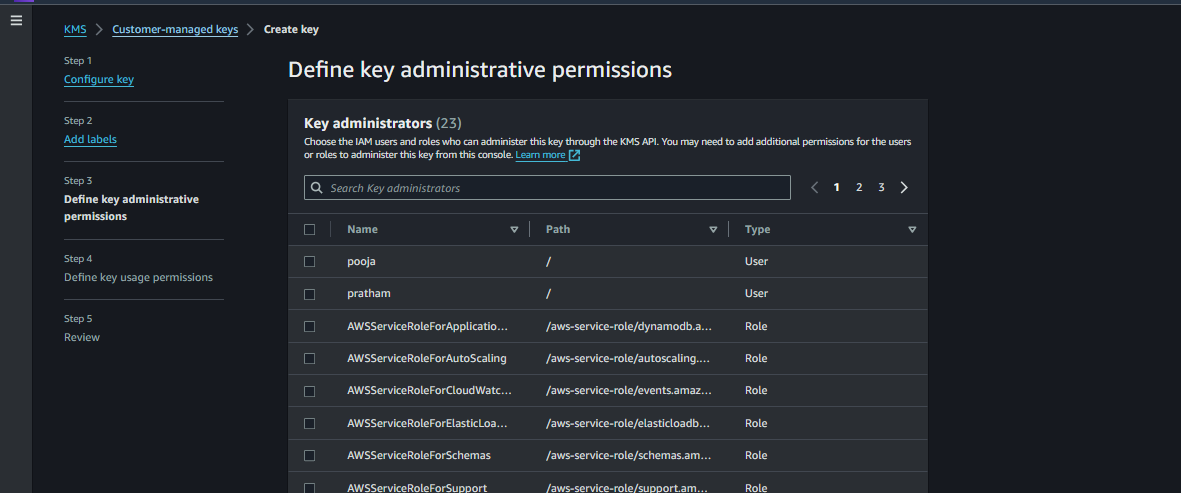
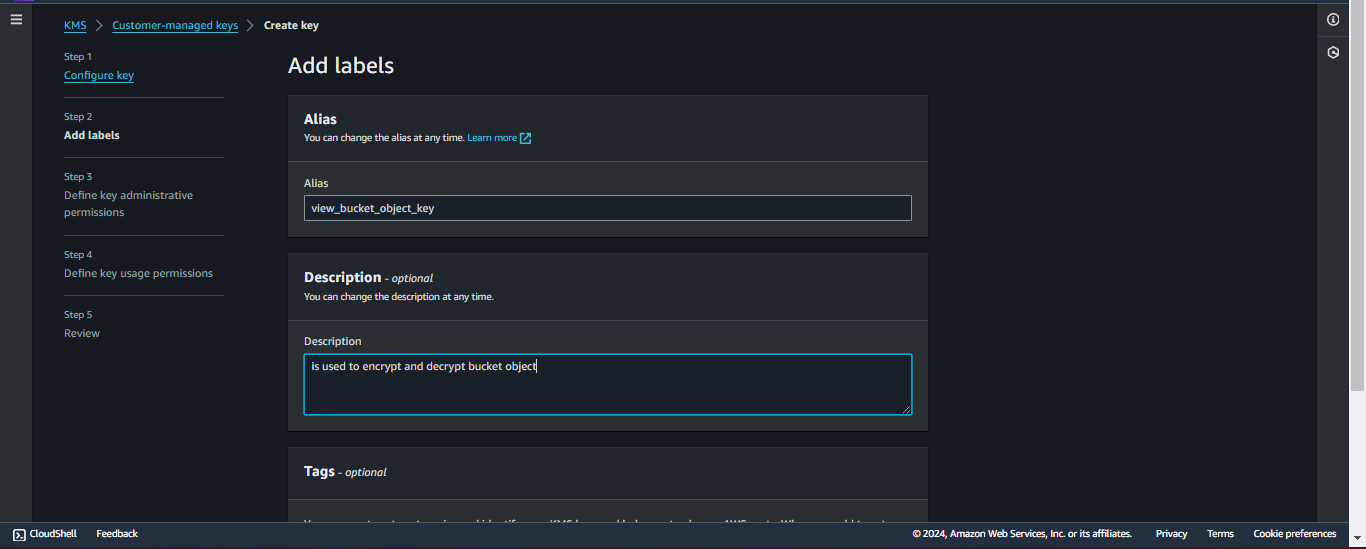
* + Enter user names and select both Programmatic and AWS Management Console access types.
  + Assign AmazonS3ReadOnlyAccess to ensure they have read-only access to S3 buckets.



##### **Step 2: Setting Up AWS KMS**

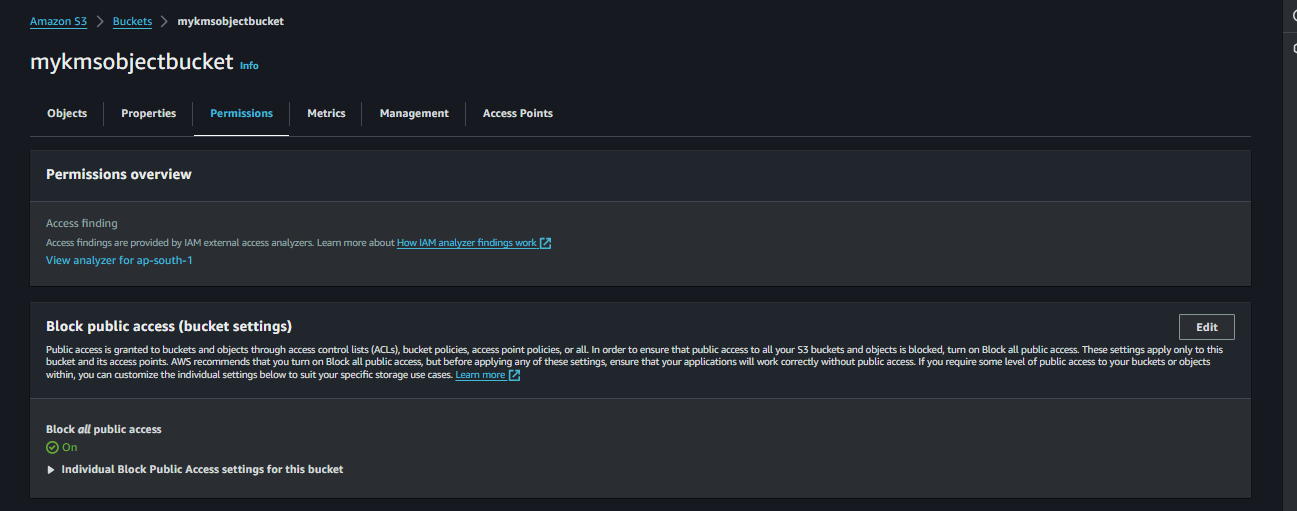
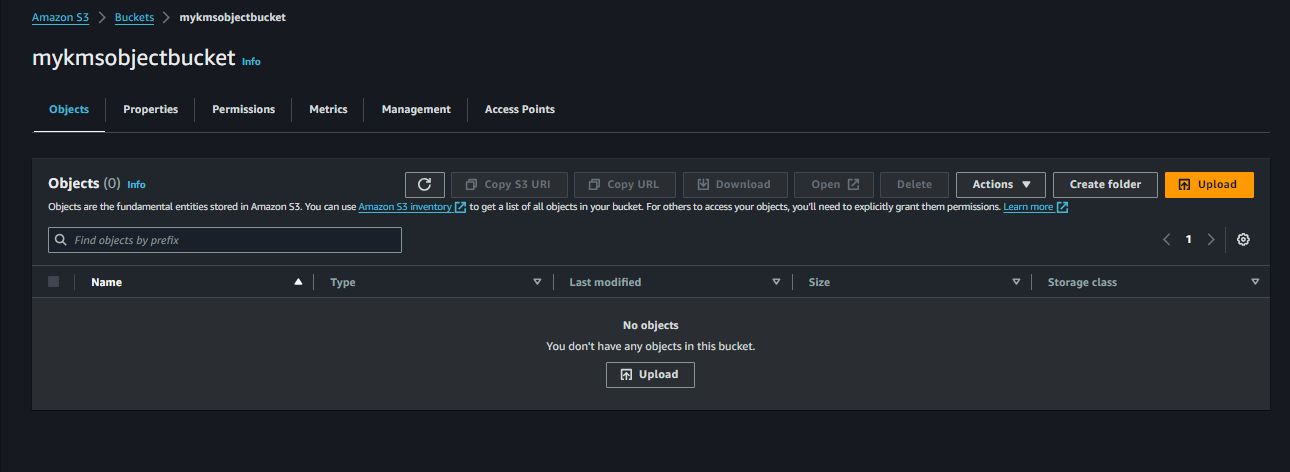
1. **Navigate to the KMS section** in the IAM dashboard.
2. **Create a new symmetric key**:
   * Choose “Create a key” and select “Symmetric”.
   * Set an alias and description for the key.
   * Configure permissions to allow only Admin and User1 to use this key for decryption purposes.

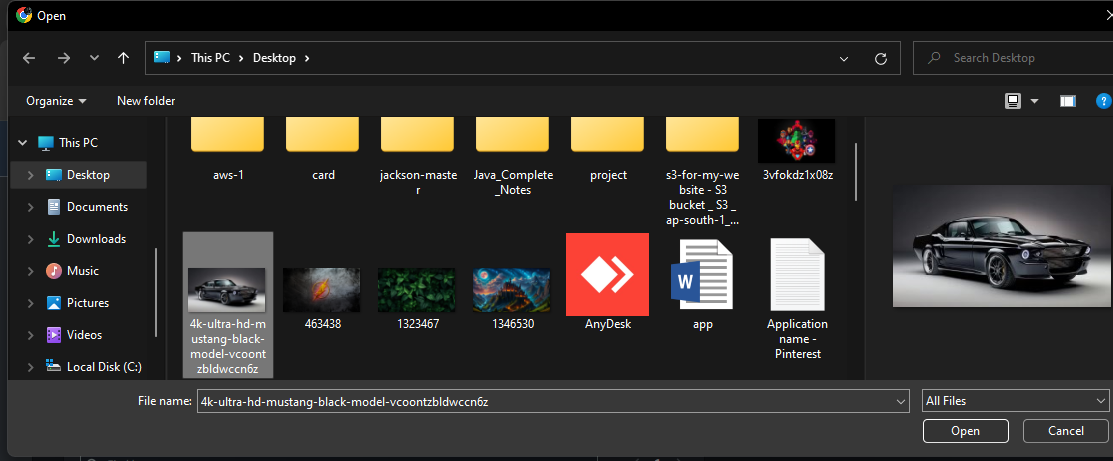




##### **Step 3: Creating and Configuring an S3 Bucket**

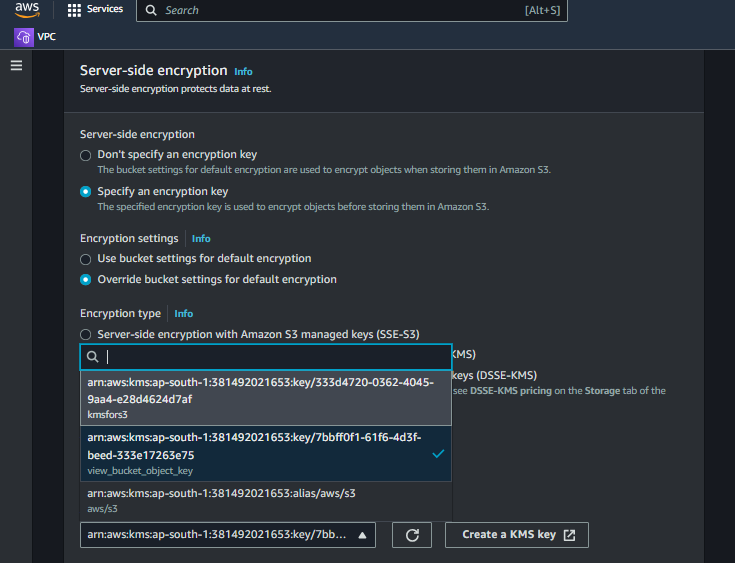
1. **Go to the S3 service** in the AWS Management Console.
2. **Create a new bucket**:
   * Click “Create bucket”.
   * Follow the setup to name the bucket and select the appropriate region.
   * Ensure all public access is blocked to enhance security.





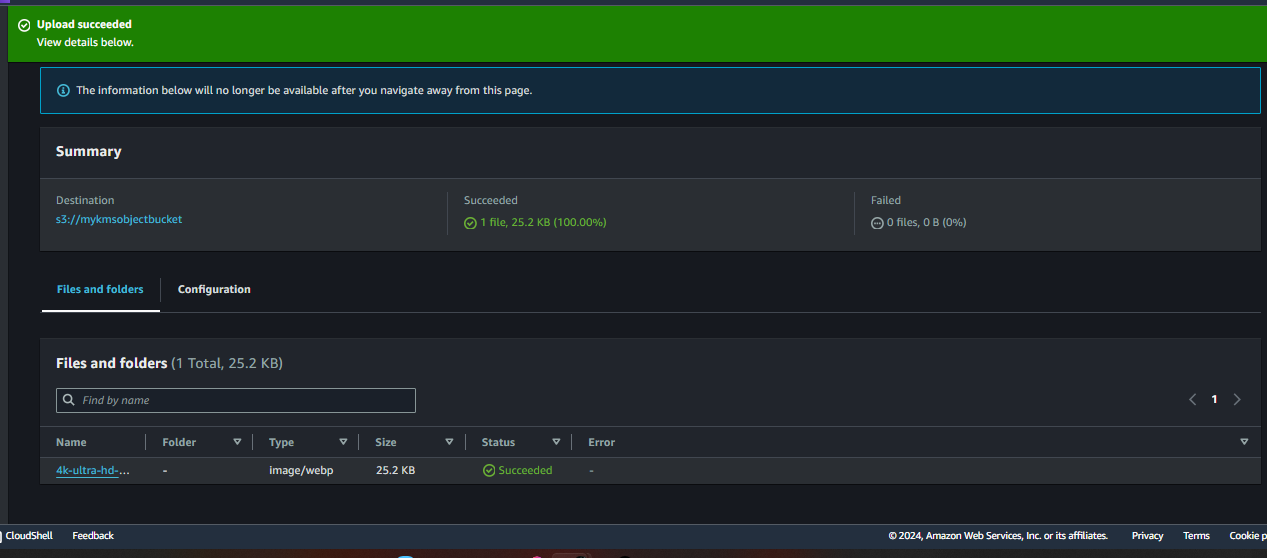
##### **Step 4: Configuring Encryption on S3 Objects**

1. **Manually encrypt specific objects using the KMS key**:
   * During the upload process, select the encryption option.
   * Choose the previously created KMS key for encryption to secure sensitive files.



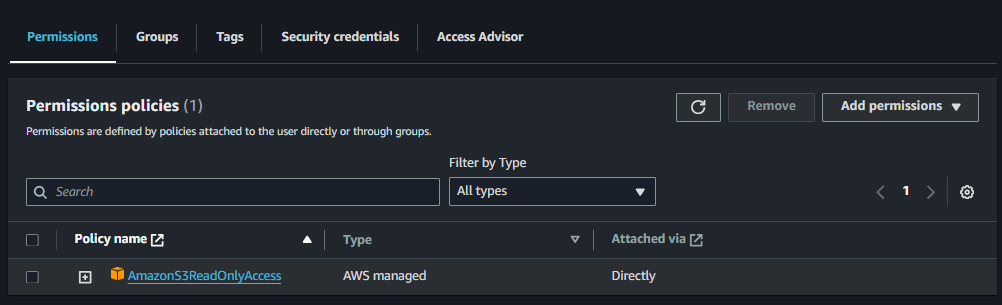
##### **Step 5: Uploading Data**

1. **Upload both encrypted and non-encrypted objects**:
   * Admin, as the primary user, should upload files to the S3 bucket.
   * Selectively apply encryption to sensitive files during the upload.

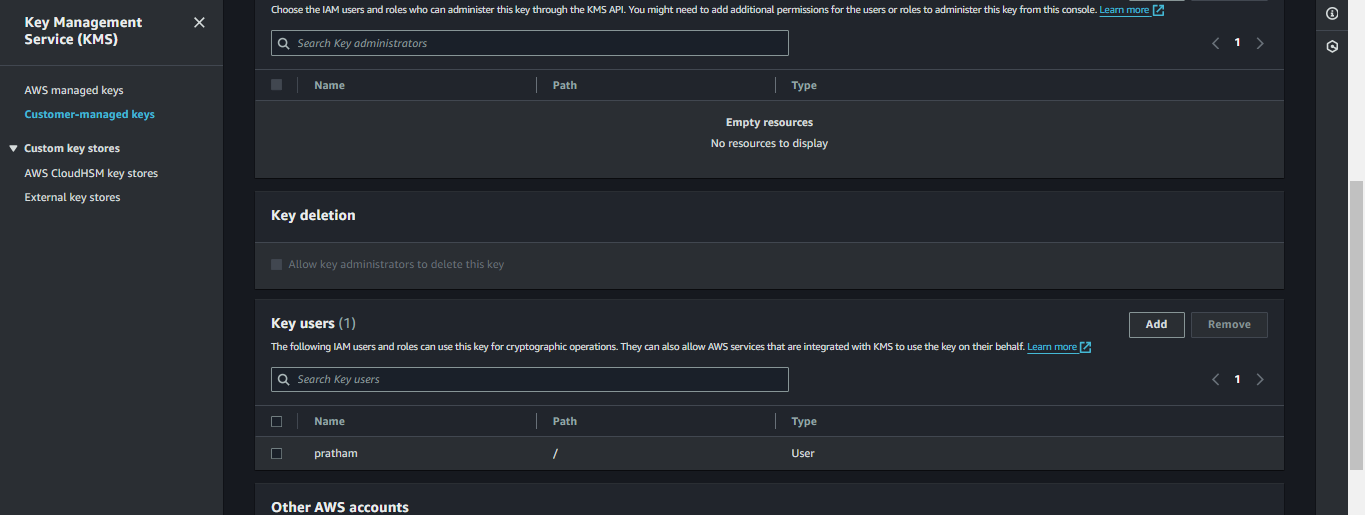
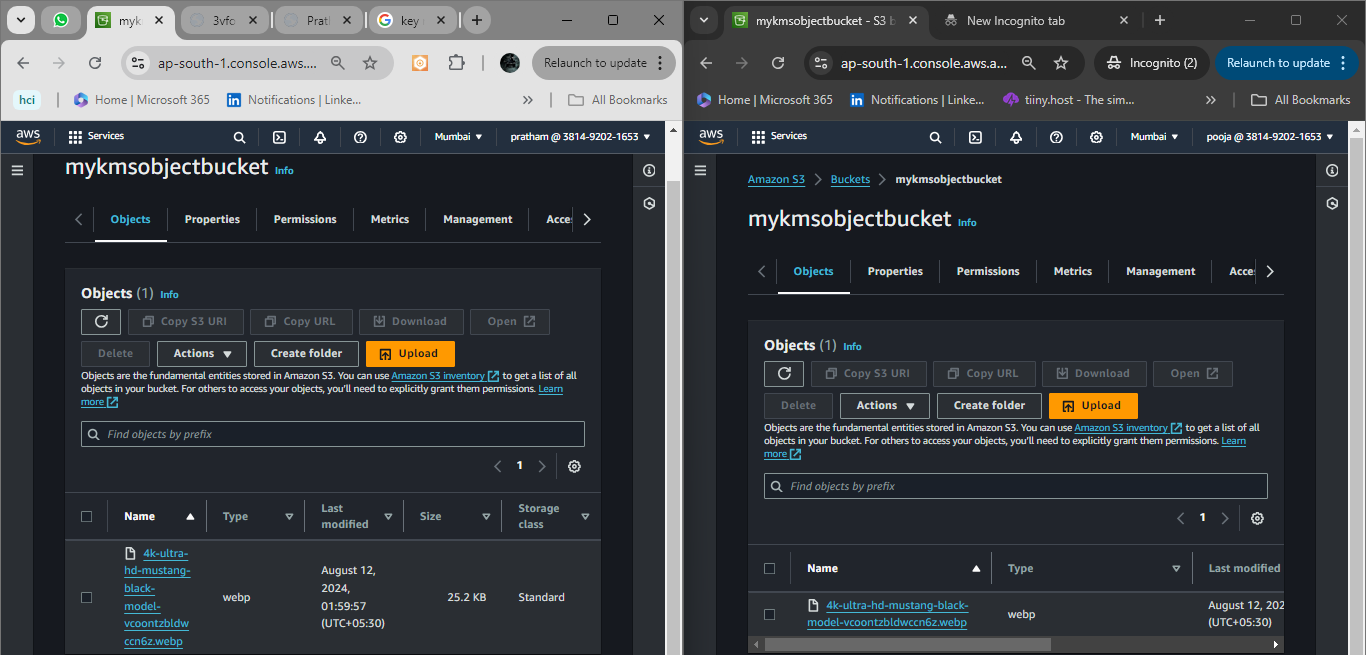


#### **User Access and Permissions**

* **Configure IAM roles and policies** to ensure that both user1 and User2 can read all objects.



* **Set decryption permissions** using the KMS key for both user1 to access encrypted files securely.

****

#### 

#### **Conclusion**

organizations can effectively manage data security in AWS using S3 and KMS. The read-only access coupled with selective encryption provides a robust security framework while maintaining straightforward access for authorized users.

Working Video:-

<https://drive.google.com/file/d/1XEwvvXeMgrEI4aP_0JhcydF1bkv470NM/view?usp=drive_link>