Lesson 04 Demo 06

Demonstrating Server-Side Encryption Using S3 and KMS

Objective: To demonstrate the utilization of Amazon S3 buckets with different server-side encryption options: SSE-S3 and SSE-KMS

Tools required: None

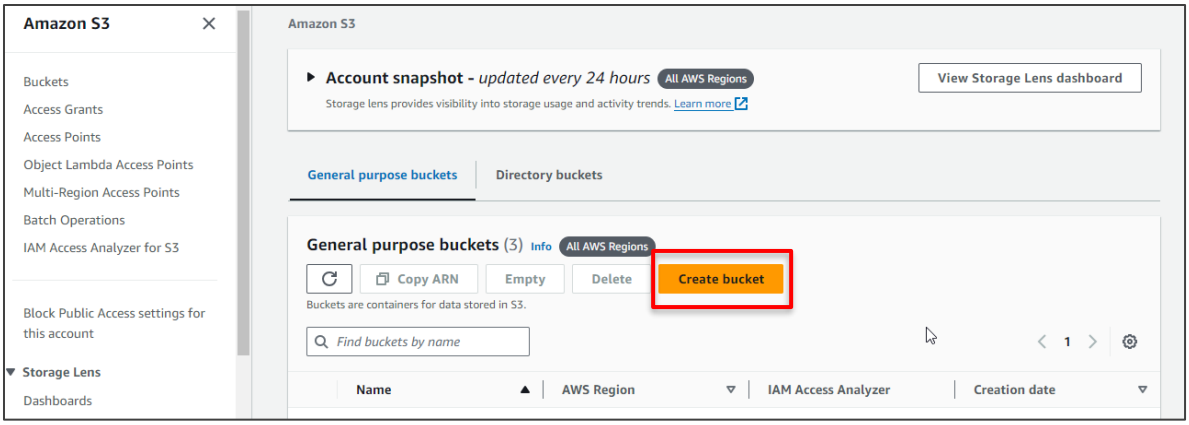
Prerequisites: AWS account with an S3 bucket created

Steps to be followed:

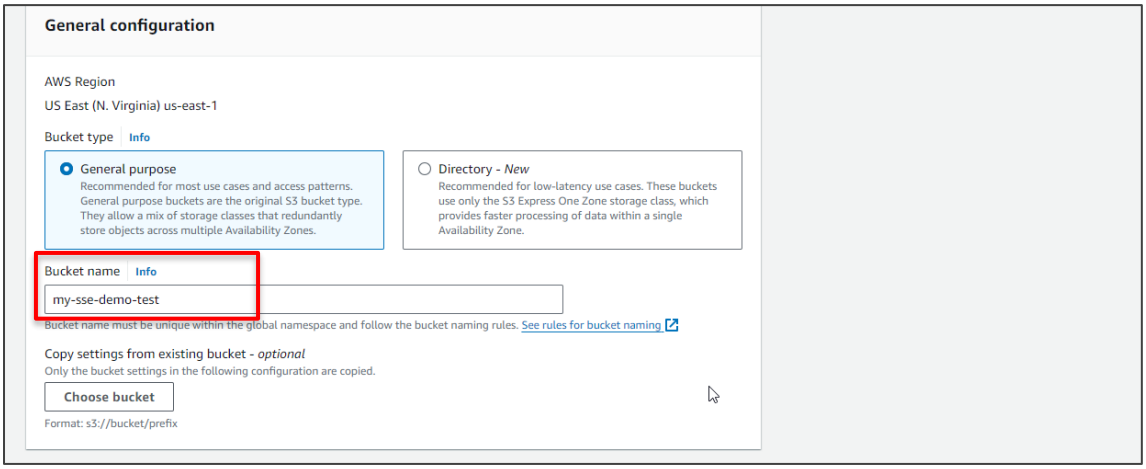
1. Create an S3 bucket with SSE-S3 encryption
2. Create a Key Management Service (KMS) key
3. Create an S3 bucket with SSE-KMS encryption

Step 1: Create an S3 bucket with SSE-S3 encryption

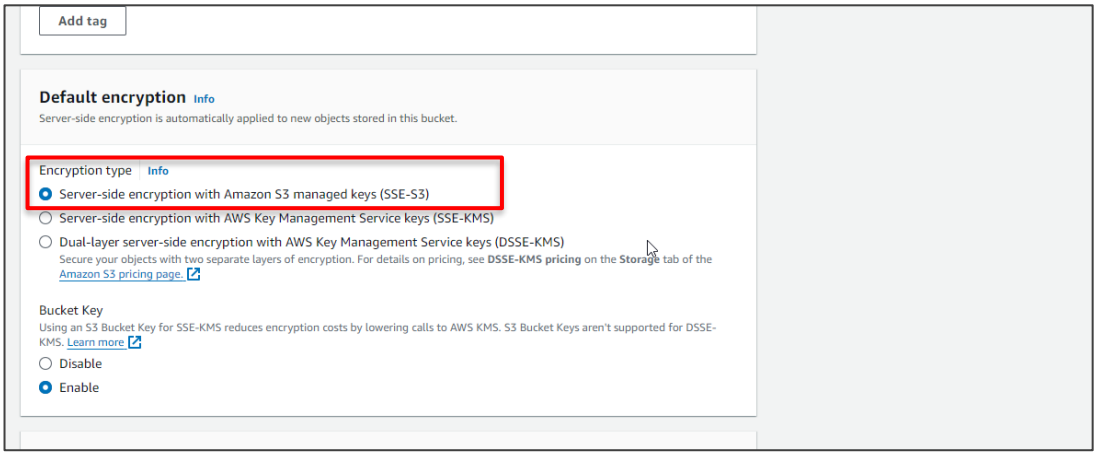
1.1 Navigate to **Amazon S3** and click on **Create bucket**



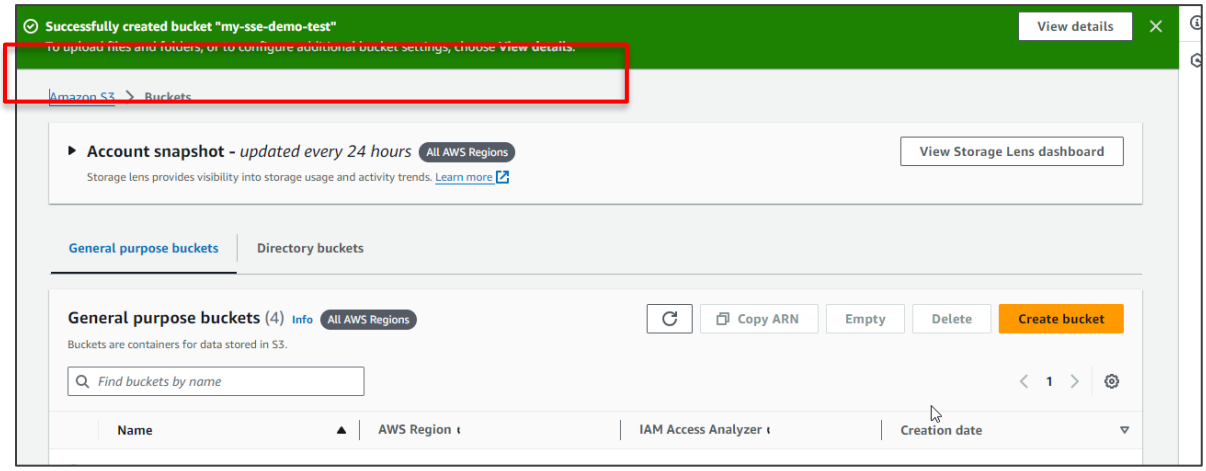
1.2 Enter the **Bucket name** as **my-sse-demo-test**



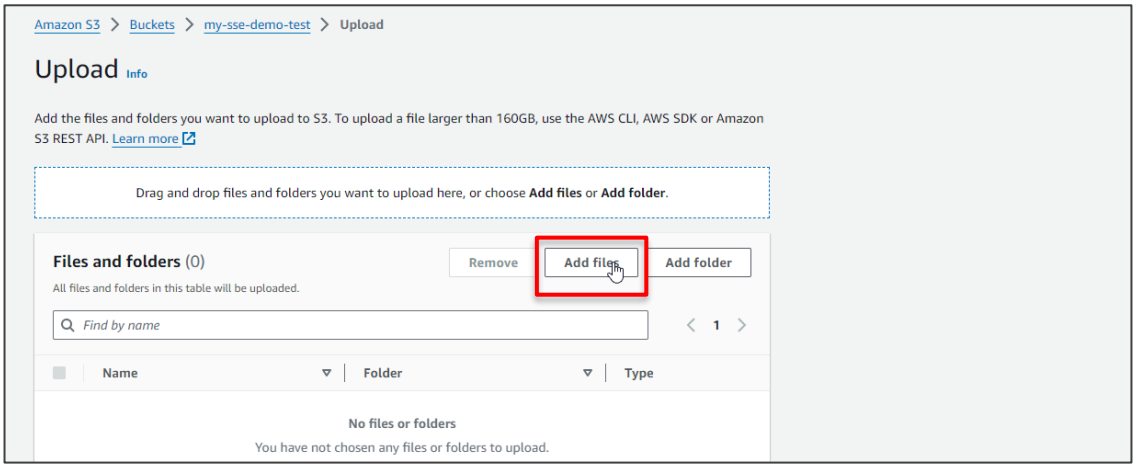
1.3 Select **Server-side encryption with Amazon S3 managed keys (SSE-S3)**

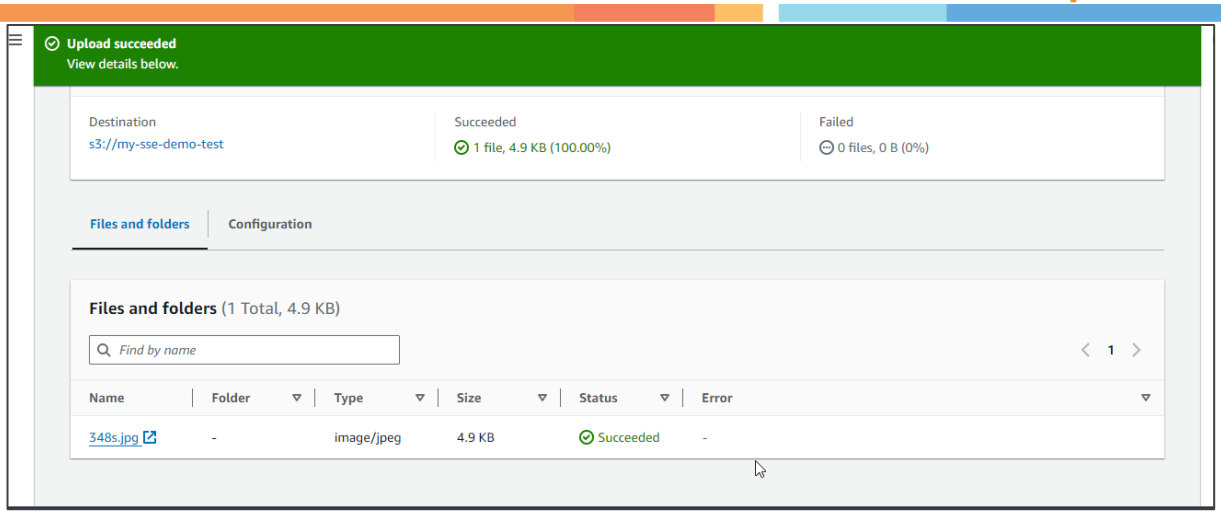


1.4 Verify successful creation of the bucket named **my-sse-demo-test**

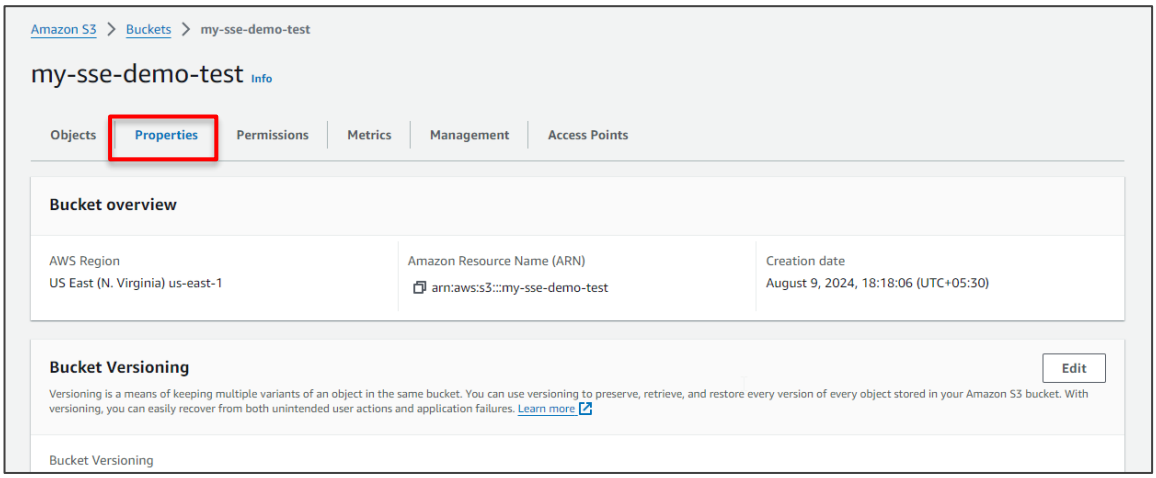


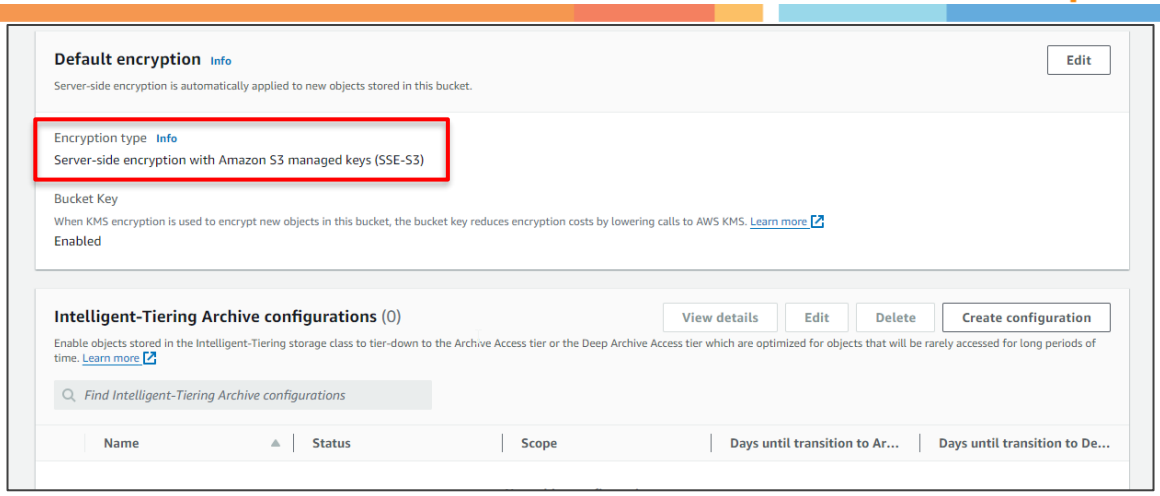
1.5 Upload a file by clicking **Add files**





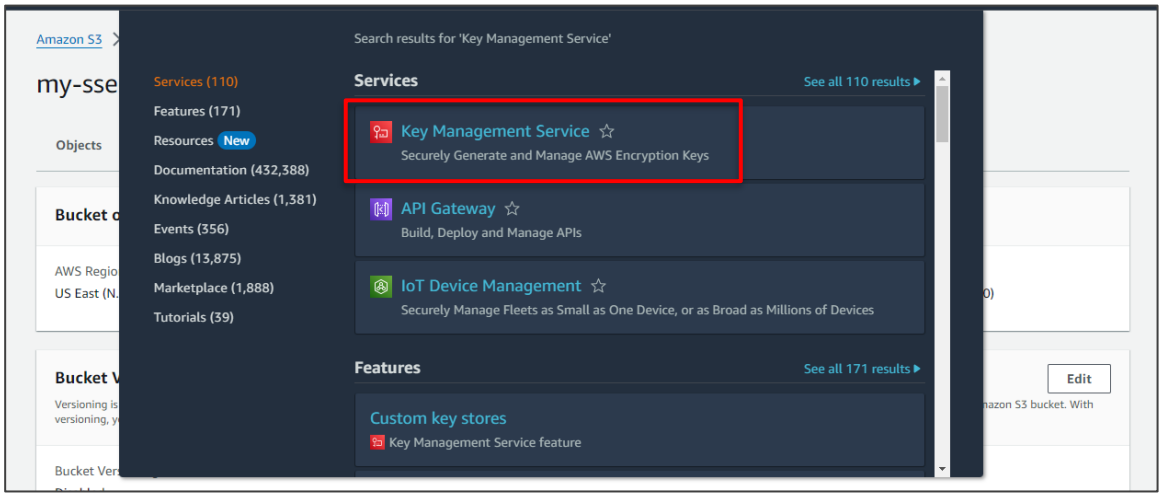
1.6 Confirm encryption status by navigating to the **Properties** tab



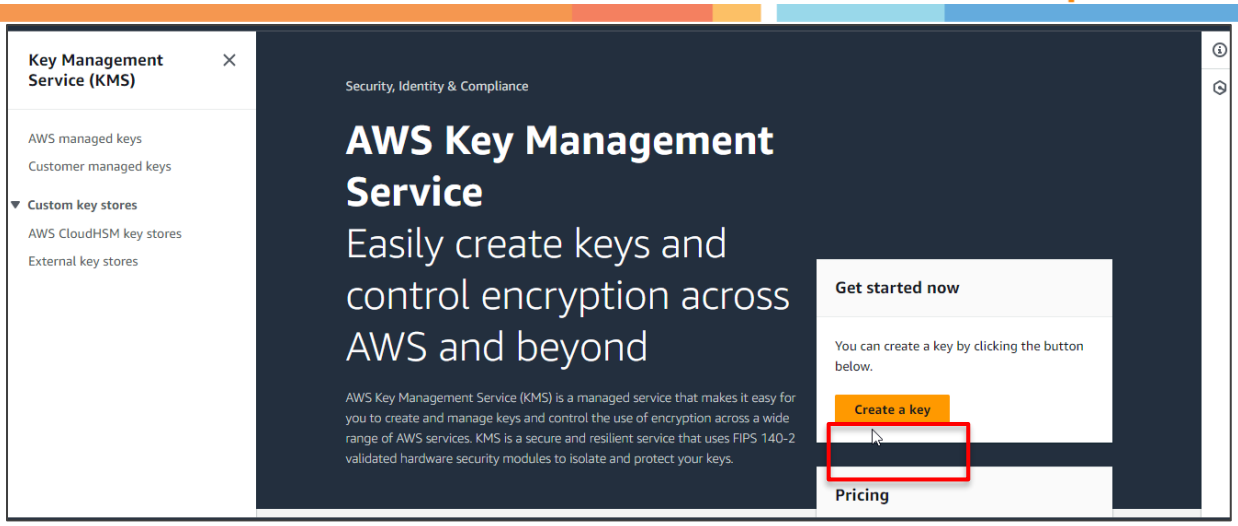


Step 2: Create a Key Management Service (KMS) key

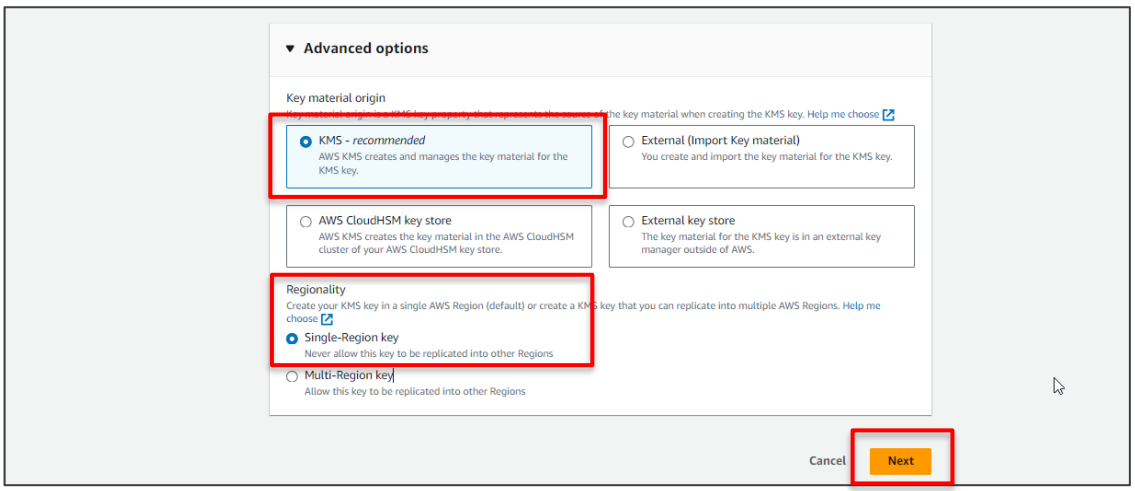
2.1 Access the AWS Management Console, search for **Key Management Service**, and select it



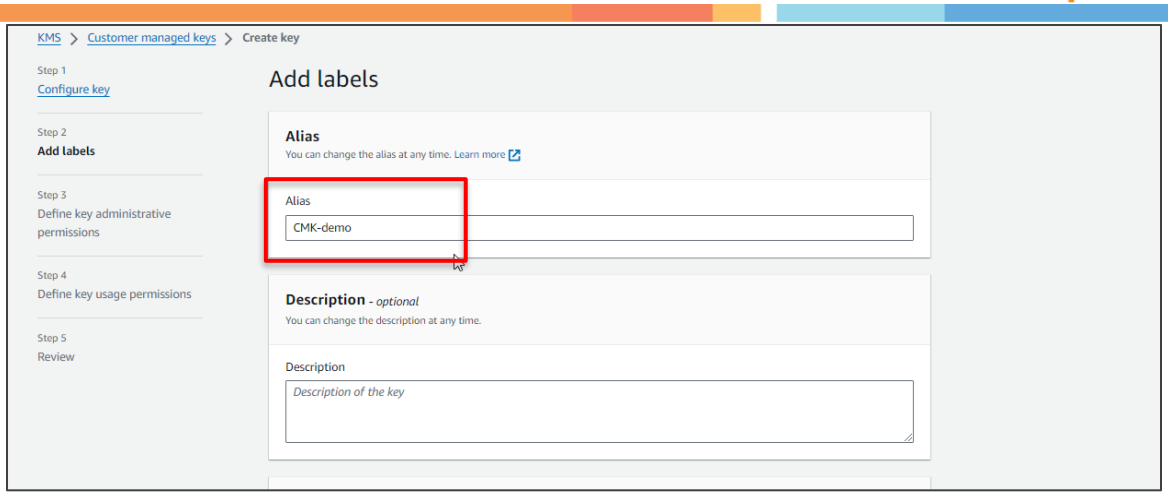
2.2 Choose **Key Management Service** and select **Create a key**



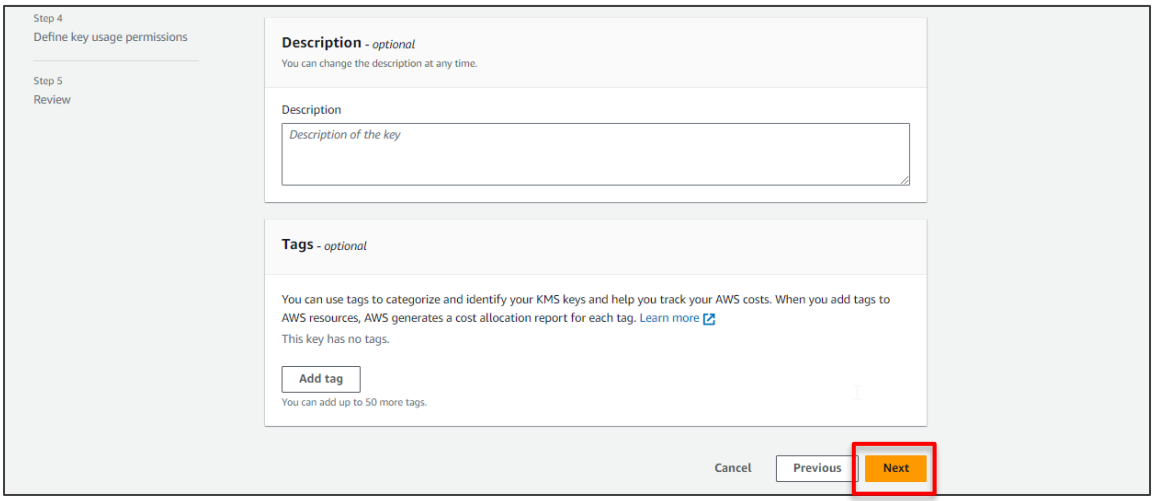
2.3 Select **KMS** from **Key material origin**, select **Single-Region key** from **Regionality**, and then click on **Next**



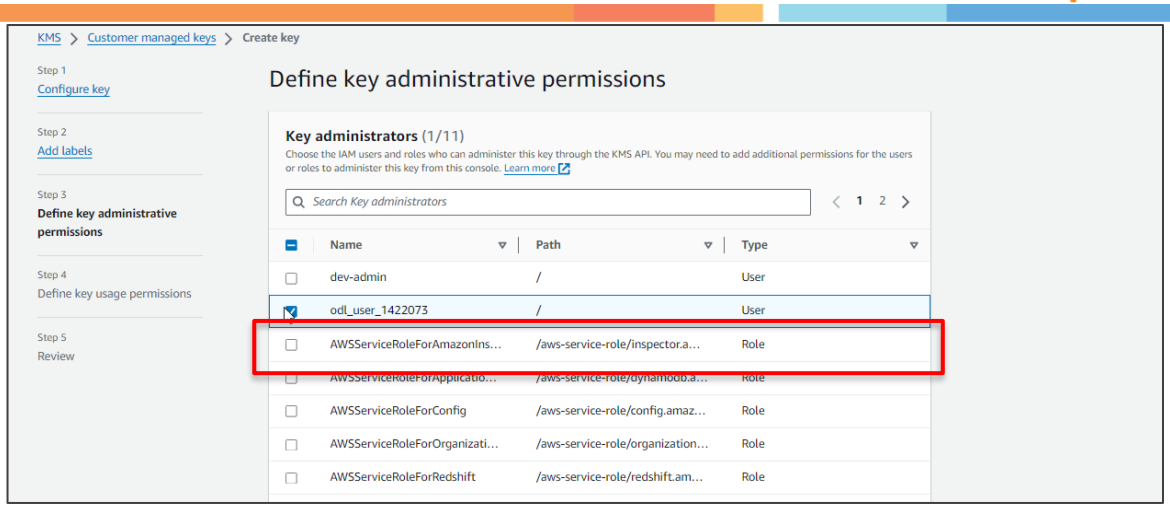
2.4 Enter the name as **CMK-demo** in Alias

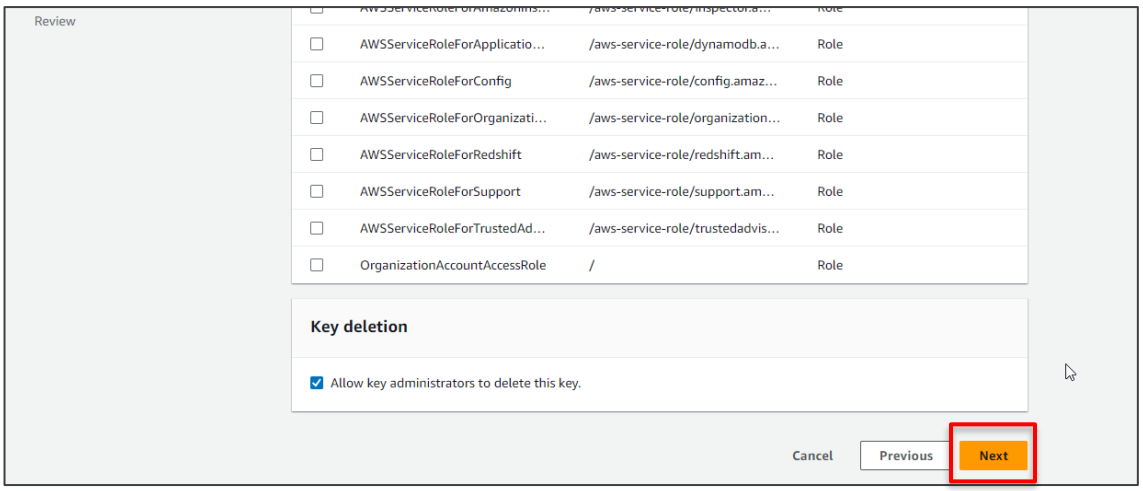


2.5 Click on **Next**

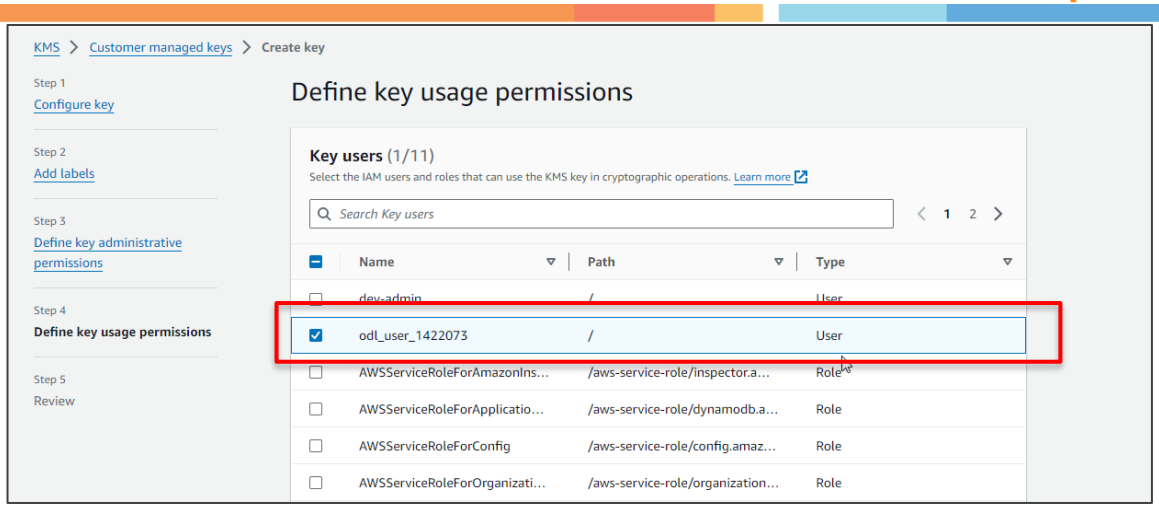


2.6 Select your AWS Lab username as key administrator, allow key deletion access, and click **Next**

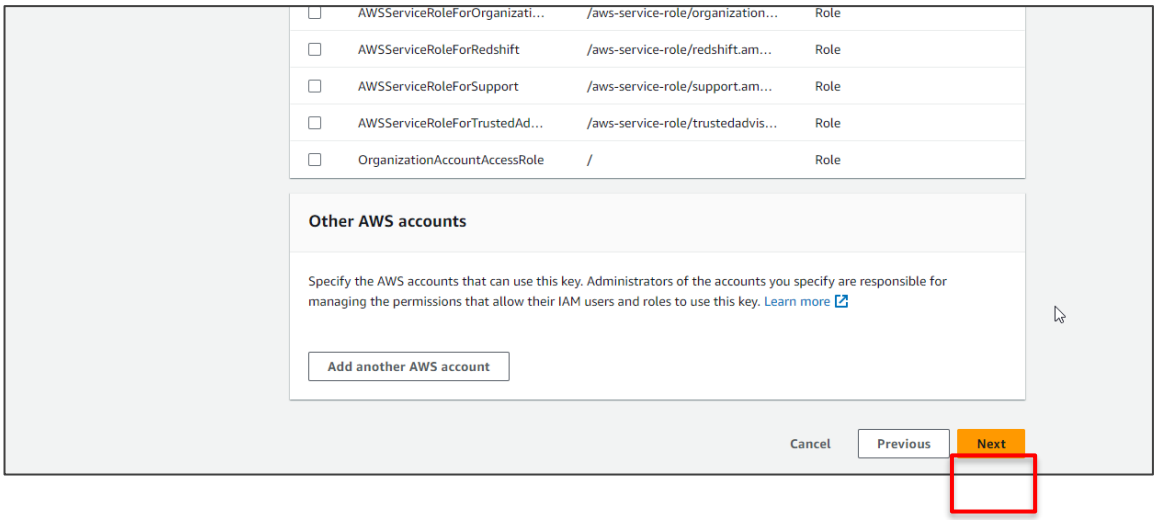




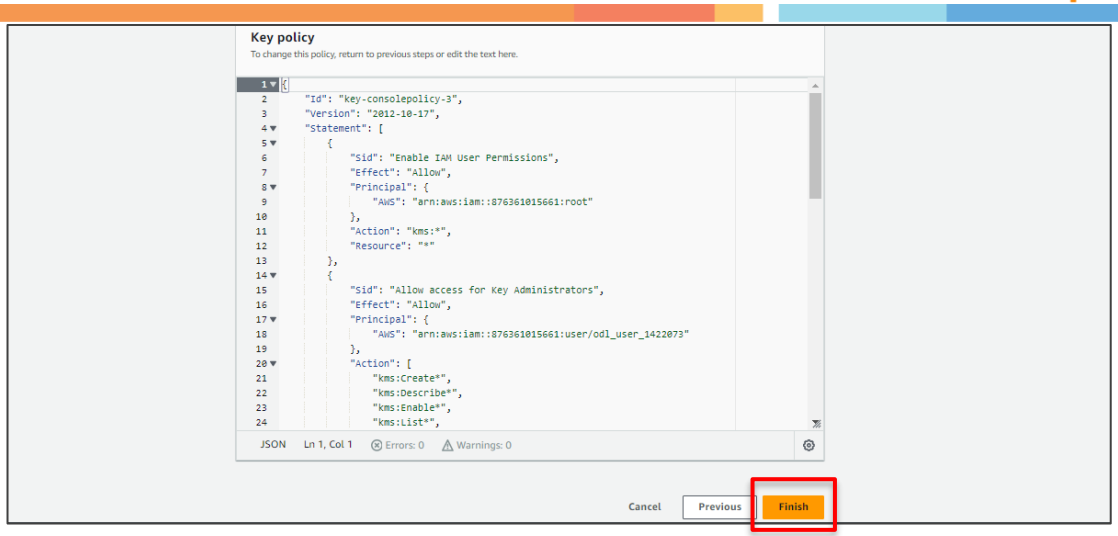
2.7 Under **Define key usage permissions**, select your AWS Lab username, and click **Next**

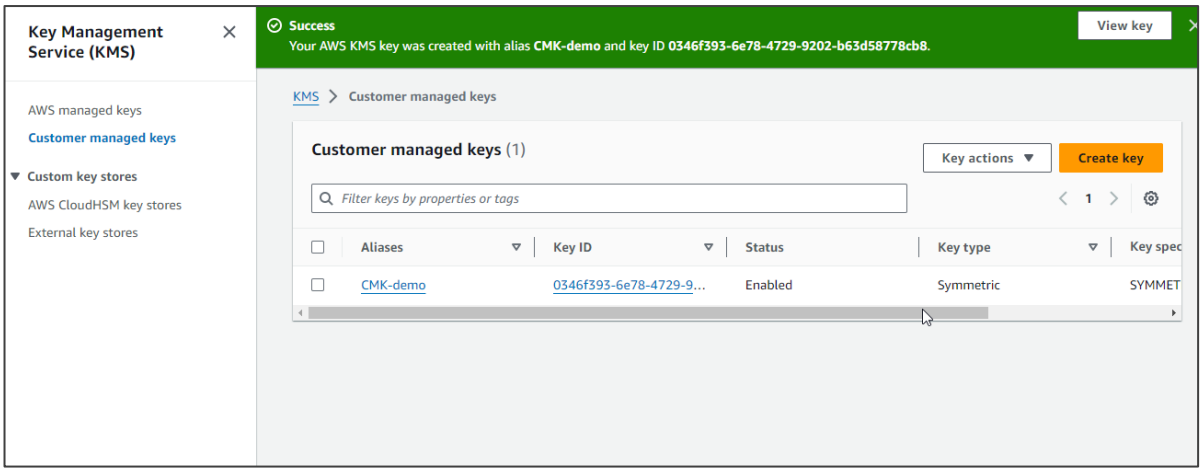


2.8 Click on **Next**



2.9 Scroll down to the **Key policy** tab and finalize by clicking **Finish**



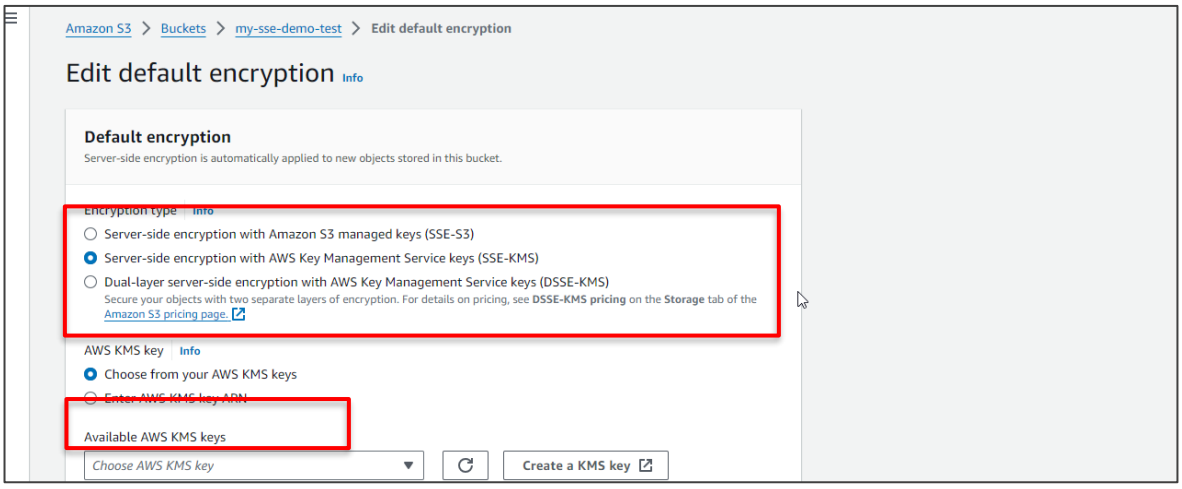


The **KMS key** has been successfully created.

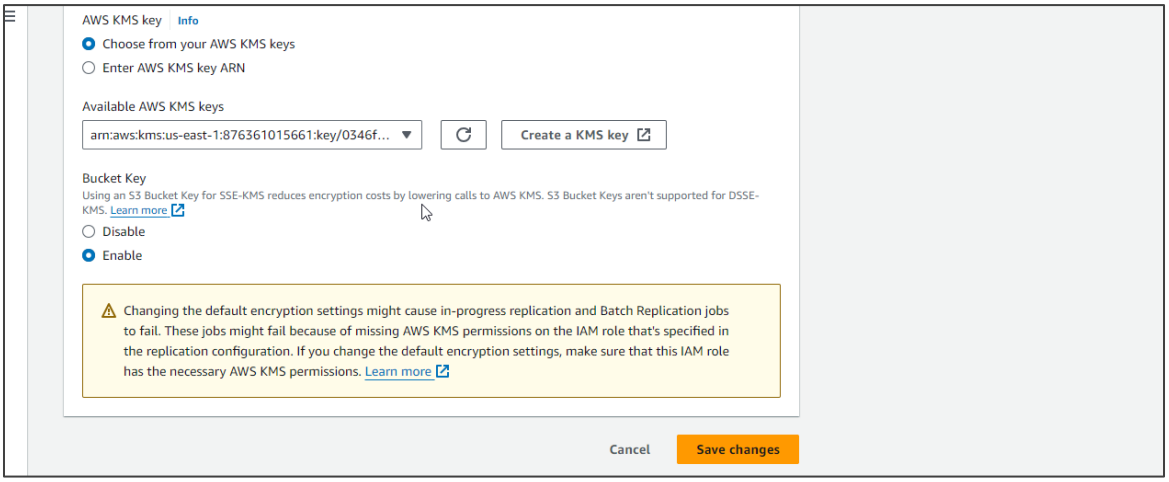
Note: Repeat steps 1.1 and 1.2 to create a new bucket

Step 3: Create an S3 bucket with SSE-KMS encryption

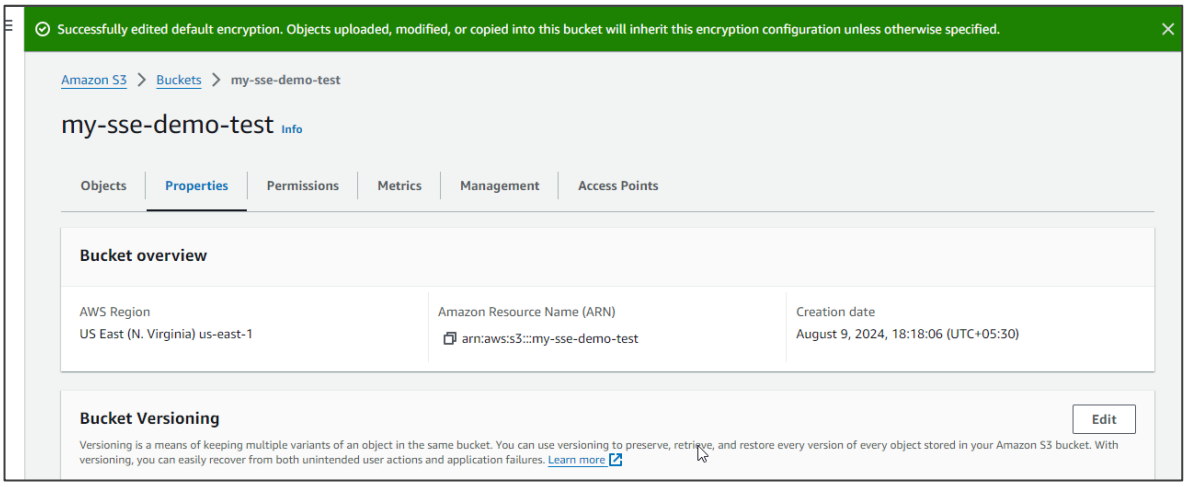
3.1 Enable default encryption by selecting the key type as **AWS Key Management Service key (SSE-KMS)**, then click on **Choose from your AWS KMS keys**

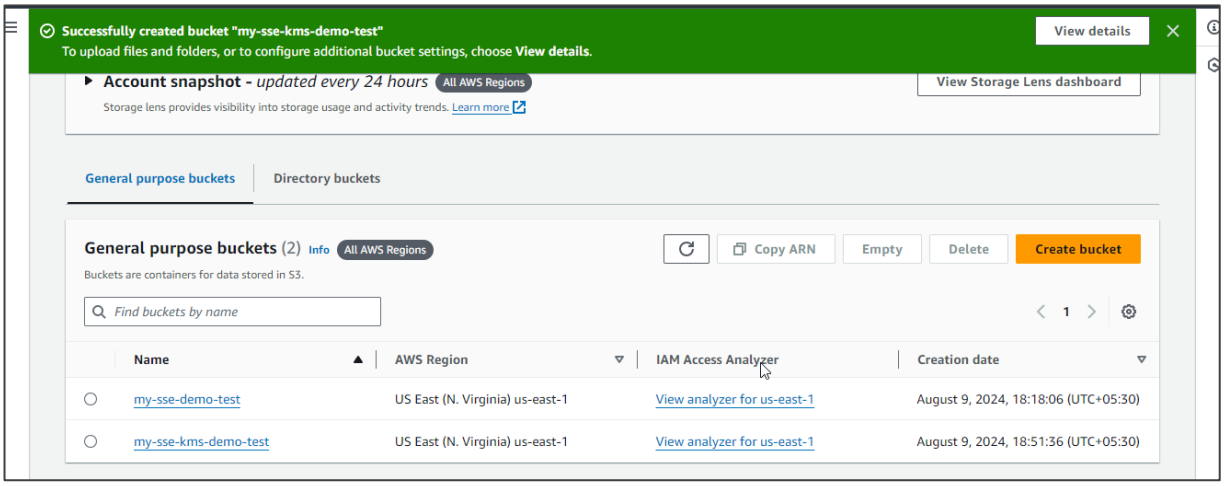


3.2 Click **Save changes**



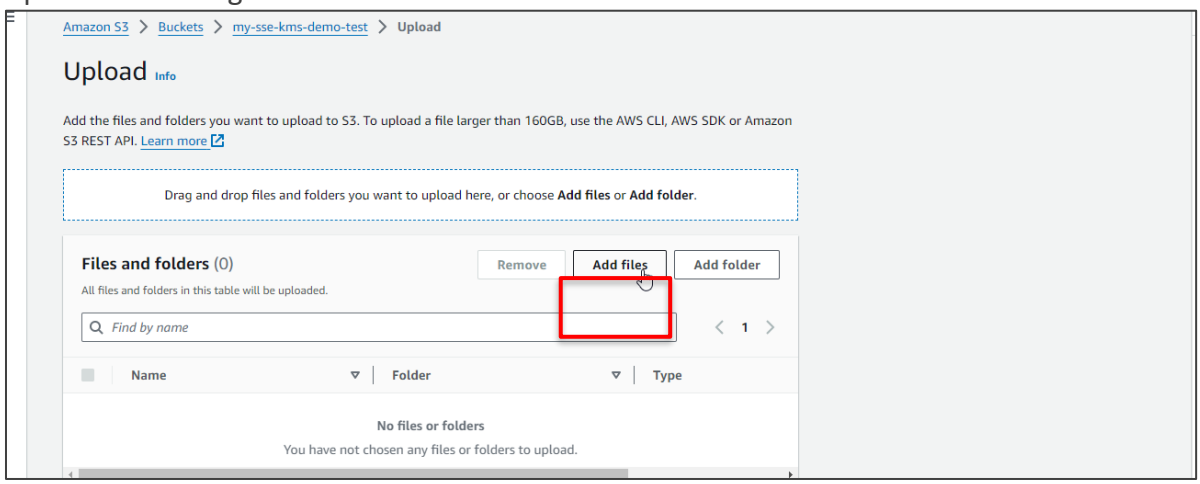
Note: Repeat steps 1.1 and 1.2 to create a new bucket

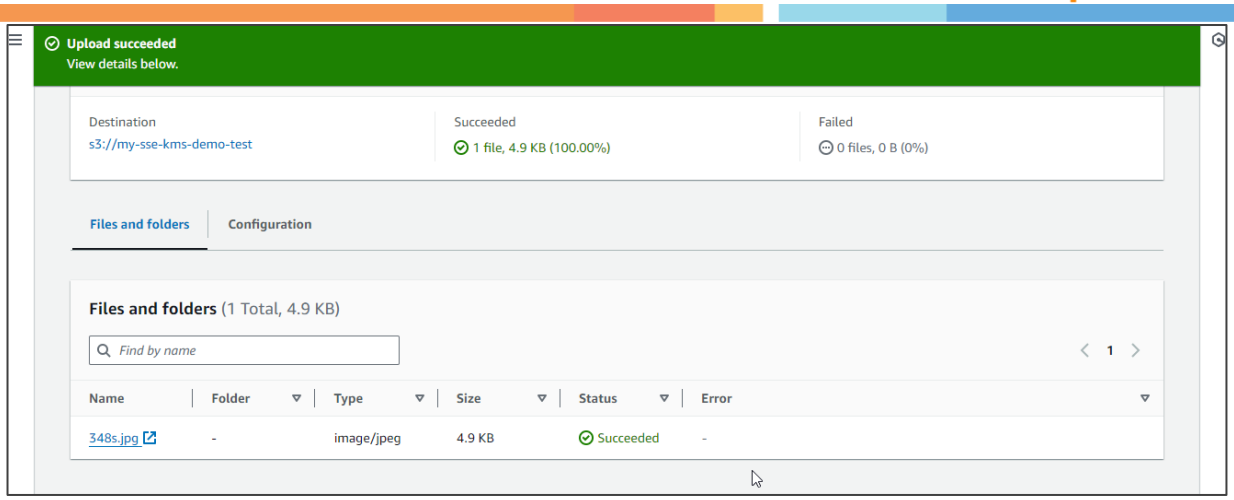




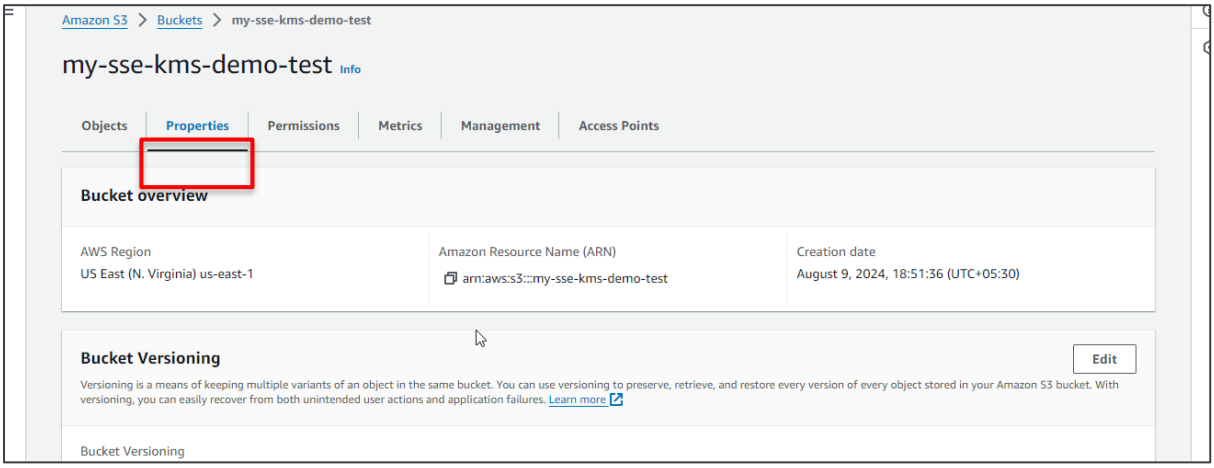
A bucket named **my-sse-kms-demo-test** has been successfully created.

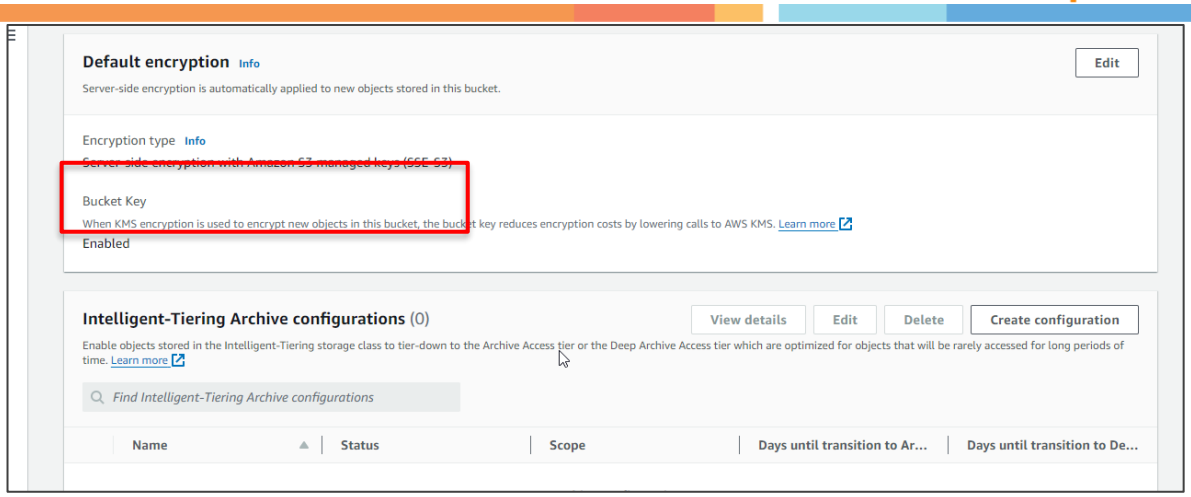
3.3 Upload a file using **Add files**





3.4 Confirm encryption status by clicking the uploaded file and navigating to the **Properties** tab





By following these steps, you have effectively implemented robust server-side encryption using Amazon S3 and KMS, ensuring optimal security for your stored data.