**Lesson 4 Demo 6**

**Server-side Encryption Using S3 and KMS**

**Objectives:** To create a Server-side Encryption using S3 and KMS

**Prerequisites:** AWS account with an S3 bucket created

**Steps to be followed:**

1. Creating an S3 bucket by enabling SSE-S3 encryption
2. Creating a KMS
3. Creating a S3 bucket by enabling SSE-KMS encryption

**Step** **1:** **Creating an S3 bucket by enabling SSE-S3 encryption**

1. Go to the Amazon S3 management console home page and create a bucket

Graphical user interface, text, application, email

Description automatically generated

1. Enable the **Default encryption** by choosing the key type as **Amazon S3-managed keys (SSE-S3)** and click on **Create bucket:**

Graphical user interface, text, application, email

Description automatically generated

A **Bucket** named **my-sse-demo-test** has been successfully created

Graphical user interface, text, application

Description automatically generated

1. Upload an object by clicking on **Add files** tab:

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

1. Click on the uploaded file and navigate to the **properties tab** to verify if the encryption is enabled

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

**Step** **2:** **Creating a KMS**

* 1. Go to the AWS management console home page and search for **Key Management Service** **(KMS):**

Graphical user interface, application

Description automatically generated

* 1. Choose the **Key Management Service** and click on **Create a key** tab

Graphical user interface, text

Description automatically generated

* 1. Configure the key with the default options as shown in the screenshots below and click on **Next:**

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

**Note:** Please make sure that you are providing an alias that can be changed at any point in time.

* 1. Under the **key administrator’s** option, select the username of your AWS Lab, allow the access to delete the key, and click on **Next:**

Graphical user interface, text, application, table, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

* 1. Under the **key usage permissions**, select the username of your AWS Lab and click on **Next:**

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

* 1. Scroll down to the **Key policy** tab and click on the **Finish** tab**:**

Graphical user interface, text, application, email

Description automatically generated

**KMS key** has been successfully created

Graphical user interface, text, application

Description automatically generated

**Step** **3:** **Creating an S3 bucket by enabling SSE-KMS encryption**

* 1. Repeat the bucket creation steps from 1.1
  2. Enable the **Default encryption** by selecting the key type as **AWS key Management Service key (SSE-KMS):**

Graphical user interface, text, application, email

Description automatically generated

* 1. Choose the **AWS KMS key** created and click on Create bucket**:**

Graphical user interface, text, application, email

Description automatically generated

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

Graphical user interface, text, application

Description automatically generated

3.5 Upload an object by clicking on **Add files** tab:

Graphical user interface, text, application, email

Description automatically generated

3.6 Click on the uploaded file and navigate to the **properties tab** to verify, if the encryption is enabled:

Graphical user interface, text, application, email

Description automatically generated

Hence proved, both SSE-S3 and SSE-KMS Encryption have been successfully enabled for the buckets created.