

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**

Amazon S3 > Buckets > Create bucket

Create bucket [Info](#)

Buckets are containers for data stored in S3. [Learn more](#)

General configuration

Bucket name

Bucket name must be unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

AWS Region

Copy settings from existing bucket - *optional*
Only the bucket settings in the following configuration are copied.

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

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

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

🟢 **Successfully created bucket "my-sse-demo-test"** View details
 To upload files and folders, or to configure additional bucket settings choose [View details](#).

Amazon S3 > Buckets

▼ **Account snapshot** View Storage Lens dashboard
 Last updated: Jul 20, 2022 by Storage Lens. Metrics are generated every 24 hours. [Learn more](#)

Total storage	Object count	Avg. object size
101.0 KB	4	25.3 KB

You can enable advanced metrics in the "default-account-dashboard" configuration.

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

Amazon S3 > Buckets > my-sse-demo-test > Upload

Upload Info

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose **Add files**, or **Add folders**.

Files and folders (1 Total, 113.0 KB) Remove **Add files** Add folder
 All files and folders in this table will be uploaded.

🔍 Find by name < 1 >

<input type="checkbox"/>	Name ▲	Folder ▼	Type ▼	Size ▼
<input type="checkbox"/>	Simplilearn.JPG	-	image/jpeg	113.0 KB

Destination

Destination
[s3://my-sse-demo-test](#)

Upload succeeded
View details below.

The information below will no longer be available after you navigate away from this page.

Summary

Destination s3://my-sse-demo-test	Succeeded 1 file, 113.0 KB (100.00%)	Failed 0 files, 0 B (0%)
--------------------------------------	---	-----------------------------

Files and folders | Configuration

Files and folders (1 Total, 113.0 KB)

Find by name

Name	Folder	Type	Size	Status
Simplilearn.JPG	-	image/jpeg	113.0 KB	Succeeded

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

Amazon S3 > Buckets > my-sse-demo-test > Screenshot (1).png

Screenshot (1).png Info

Copy S3 URI Download Open Object actions

Properties | Permissions | Versions

Object overview

Owner simplilearnlabs282 AWS Region US East (N. Virginia) us-east-1 Last modified August 2, 2023, 15:28:28 (UTC+05:30) Size 209.2 KB Type	S3 URI s3://my-sse-demo-test/Screenshot (1).png Amazon Resource Name (ARN) arn:aws:s3:::my-sse-demo-test/Screenshot (1).png Entity tag (Etag) 7c83e179b5d8b62b4223ae8e5f5aade3 Object URL https://my-sse-demo-test.s3.amazonaws.com/Screenshot+1).png
--	--

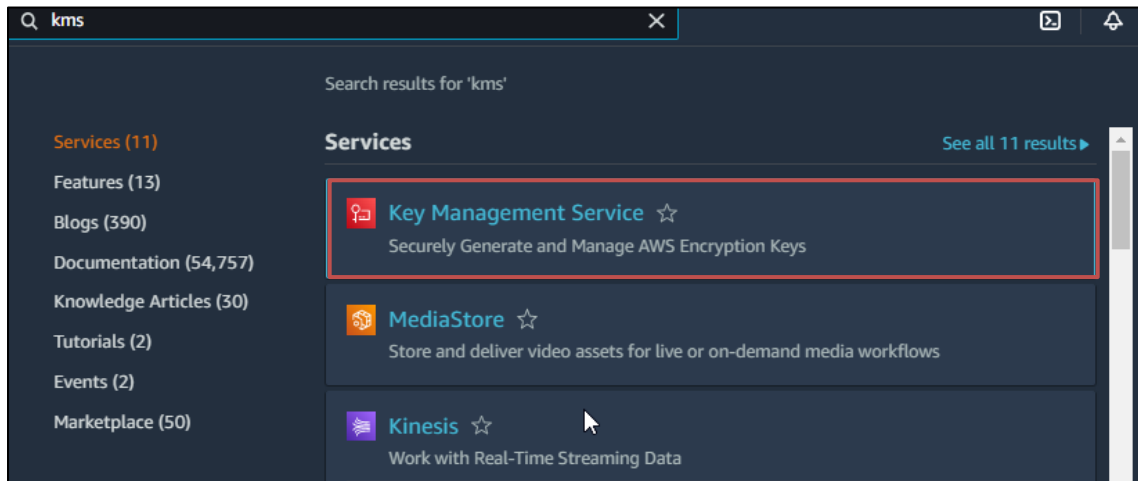
Server-side encryption settings Info

Server-side encryption protects data at rest.

Encryption type Info
Server-side encryption with Amazon S3 managed keys (SSE-S3)

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**

▼ **Advanced options**

Key material origin
Key material origin is a KMS key property that represents the source of the key material when creating the KMS key. [Help me choose](#)

☒ **KMS - recommended**
AWS KMS creates and manages the key material for the KMS key.

☐ **External (Import Key material)**
You create and import the key material for the KMS key.

☐ **AWS CloudHSM key store**
AWS KMS creates the key material in the AWS CloudHSM cluster of your AWS CloudHSM key store.

☐ **External key store**
The key material for the KMS key is in an external key manager outside of AWS.

Regionality
Create your KMS key in a single AWS Region (default) or create a KMS key that you can replicate into multiple AWS Regions. [Help me choose](#)

☒ **Single-Region key**
Never allow this key to be replicated into other Regions

☐ **Multi-Region key**
Allow this key to be replicated into other Regions

Cancel

Next

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

Step 1

Configure key

Step 2

Add labels

Step 3

Define key administrative permissions

Step 4

Define key usage permissions

Step 5

Review

Add labels
You can change the alias at any time. [Learn more](#)

Alias

CMK-demo

Description - optional
You can change the description at any time.

Description - optional
Description of the key

2.5 Click on **Next**

Tags - optional

You can use tags to categorize and identify your KMS keys and help you track your AWS costs. When you add tags to AWS resources, AWS generates a cost allocation report for each tag. [Learn more](#)

This key has no tags.

Add tag

You can add up to 50 more tags.

Cancel Previous **Next**

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

Step 2
[Add labels](#)

Step 3
Define key administrative permissions

Step 4
Define key usage permissions

Step 5
Review

Key administrators (1/9)

Choose the IAM users and roles who can administer this key through the KMS API. You may need to add additional permissions for the users or roles to administer this key from this console. [Learn more](#)

Q

	Name	Path	Type
<input type="checkbox"/>	dev-admin	/	User
<input checked="" type="checkbox"/>	odl_user_1032406	/	User
<input type="checkbox"/>	AWSServiceRoleForApplicatio...	/aws-service-role/dynamodb.a...	Role
<input type="checkbox"/>	AWSServiceRoleForAWScloud9	/aws-service-role/cloud9.ama...	Role
<input type="checkbox"/>	AWSServiceRoleForOrganizati...	/aws-service-role/organization...	Role
<input type="checkbox"/>	AWSServiceRoleForRedshift	/aws-service-role/redshift.am...	Role
<input type="checkbox"/>	AWSServiceRoleForSupport	/aws-service-role/support.am...	Role
<input type="checkbox"/>	AWSServiceRoleForTrustedAd...	/aws-service-role/trustedadvis...	Role
<input type="checkbox"/>	OrganizationAccountAccessRole	/	Role

Key deletion

☒ Allow key administrators to delete this key.

Cancel Previous **Next**

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

KMS > Customer managed keys > Create key

Step 1
Configure key

Step 2
Add labels

Step 3
Define key administrative permissions

Step 4
Define key usage permissions

Step 5
Review

Define key usage permissions

Key users (1/9)
Select the IAM users and roles that can use the KMS key in cryptographic operations. [Learn more](#)

< 1 >

<input type="checkbox"/>	Name	Path	Type
<input type="checkbox"/>	dev-admin	/	User
<input checked="" type="checkbox"/>	odl_user_1032406	/	User
<input type="checkbox"/>	AWSServiceRoleForApplicatio...	/aws-service-role/dynamodb.a...	Role
<input type="checkbox"/>	AWSServiceRoleForAWSCloud9	/aws-service-role/cloud9.ama...	Role
<input type="checkbox"/>	AWSServiceRoleForOrganizati...	/aws-service-role/organization...	Role
<input type="checkbox"/>	AWSServiceRoleForRedshift	/aws-service-role/redshift.am...	Role
<input type="checkbox"/>	AWSServiceRoleForSupport	/aws-service-role/support.am...	Role
<input type="checkbox"/>	AWSServiceRoleForTrustedAd...	/aws-service-role/trustedadv...	Role
<input type="checkbox"/>	OrganizationAccountAccessRole	/	Role

Other AWS accounts

Specify the AWS accounts that can use this key. Administrators of the accounts you specify are responsible for managing the permissions that allow their IAM users and roles to use this key. [Learn more](#)

Cancel Previous **Next**

2.8 Click on **Next**

Other AWS accounts

Specify the AWS accounts that can use this key. Administrators of the accounts you specify are responsible for managing the permissions that allow their IAM users and roles to use this key. [Learn more](#)

Cancel Previous **Next**

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

Key policy

To change this policy, return to previous steps or edit the text here.

```

1 {
2   "Id": "key-consolepolicy-3",
3   "Version": "2012-10-17",
4   "Statement": [
5     {
6       "Sid": "Enable IAM User Permissions",
7       "Effect": "Allow",
8       "Principal": {
9         "AWS": "arn:aws:iam::043805049749:root"
10      },
11       "Action": "kms:*",
12       "Resource": "*"
13     },
14     {
15       "Sid": "Allow access for Key Administrators",

```

Cancel
Previous
Finish

Success
View key

Your AWS KMS key was created with alias **CMK-demo** and key ID **35cb7076-5315-4d68-9d36-704e31f73d0c**.

KMS > Customer managed keys

Customer managed keys (1)
Key actions
Create key

Filter keys by properties or tags

<input type="checkbox"/>	Aliases	Key ID	Status	Key spec	Key usage
<input type="checkbox"/>	CMK-demo	35cb7076-5315-4d68-9d36-704e31f73d0c	Enabled	SYMMETRIC_DEFAULT	Encrypt and decrypt

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

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

3.1 Repeat steps 1.1 and 1.2 to create a new bucket

3.2 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**

3.3 Click **Create bucket**

Successfully created bucket "my-sse-kms-demo-test"
To upload files and folders, or to configure additional bucket settings choose [View details](#).

Amazon S3 > Buckets

Account snapshot
Last updated: Jul 10, 2022 by Storage Lens. Metrics are generated every 24 hours. [Learn more](#)

[View Storage Lens dashboard](#)

Total storage	Object count	Avg. object size	
24.9 KB	1	24.9 KB	You can enable advanced metrics in the "default-account-dashboard" configuration.

Buckets (2) [Info](#)

Buckets are containers for data stored in S3. [Learn more](#)

	Name	AWS Region	Access	Creation date
<input type="radio"/>	my-sse-demo-test	US East (N. Virginia) us-east-1	Bucket and objects not public	July 21, 2022, 16:58:36 (UTC+05:30)
<input checked="" type="radio"/>	my-sse-kms-demo-test	US East (N. Virginia) us-east-1	Bucket and objects not public	July 21, 2022, 17:20:53 (UTC+05:30)

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

3.4 Upload a file using **Add files**

Amazon S3 > Buckets > my-sse-demo-test > Upload

Upload [Info](#)

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose **Add files**, or **Add folders**.

Files and folders (1 Total, 113.0 KB) [Remove](#) [Add files](#) [Add folder](#)

All files and folders in this table will be uploaded.

	Name	Folder	Type	Size
<input type="checkbox"/>	Simplilearn.JPG	-	image/jpeg	113.0 KB

Destination

Destination
[s3://my-sse-demo-test](#)

✓ **Upload succeeded**
View details below.

Upload: status

❗ The information below will no longer be available after you navigate away from this page.

Summary

<p>Destination</p> <p>s3://my-sse-kms-demo-test</p>	<p>Succeeded</p> <p>✓ 1 file, 113.0 KB (100.00%)</p>
---	--

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

Amazon S3 > Buckets > my-sse-demo-test > Simplilearn.JPG

Simplilearn.JPG Info

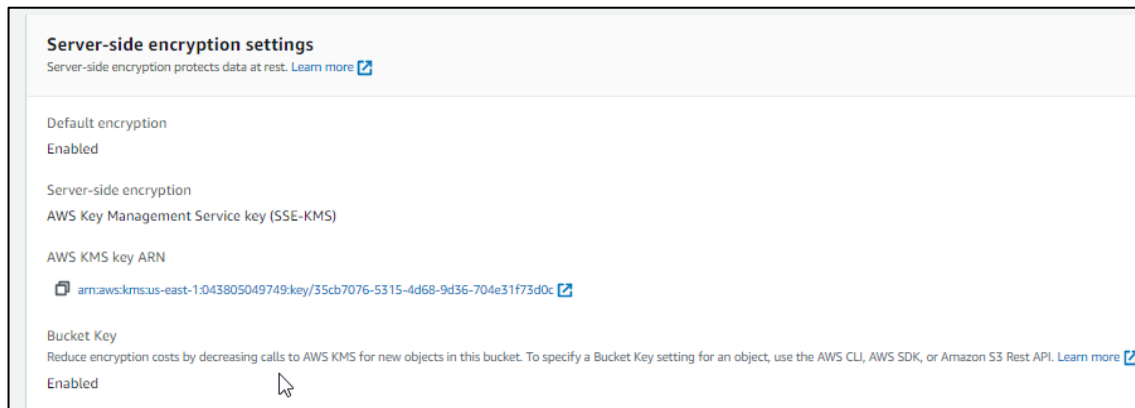
Copy S3 URI
Download

Properties

Permissions
Versions

Object overview

<p>Owner</p> <p>simplilearnlabs119</p> <p>AWS Region</p> <p>US East (N. Virginia) us-east-1</p> <p>Last modified</p> <p>July 21, 2022, 17:00:42 (UTC+05:30)</p> <p>Size</p> <p>113.0 KB</p> <p>Type</p> <p>JPG</p> <p>Key</p> <p> Simplilearn.JPG</p>	<p>S3 URI</p> <p> s3://my-sse-demo-test/Simplilearn.JPG</p> <p>Amazon Resource Name (ARN)</p> <p> arn:aws:s3:::my-sse-demo-test/Simplilearn.JPG</p> <p>Entity tag (Etag)</p> <p> a8a7f49c69cbcd0b6d6b0ee1f3b13a0f</p> <p>Object URL</p> <p> https://my-sse-demo-test.s3.amazonaws.com/Simplilearn.JPG</p>
---	---



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