

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

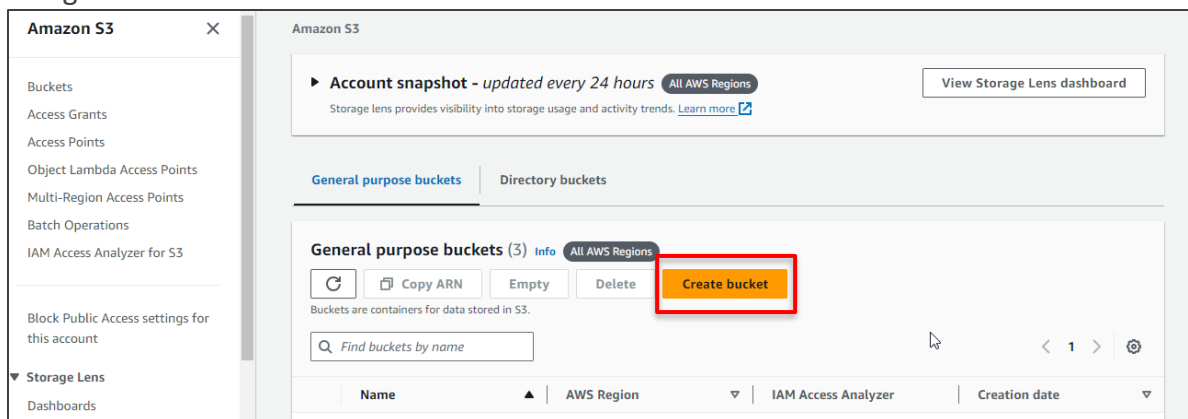
Prerequisites: AWS account with an S3 bucket created

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

General configuration

AWS Region
US East (N. Virginia) us-east-1

Bucket type [Info](#)

☒ **General purpose**
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

☐ **Directory - New**
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name [Info](#)
my-sse-demo-test

Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)

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

Format: s3://bucket/prefix

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)

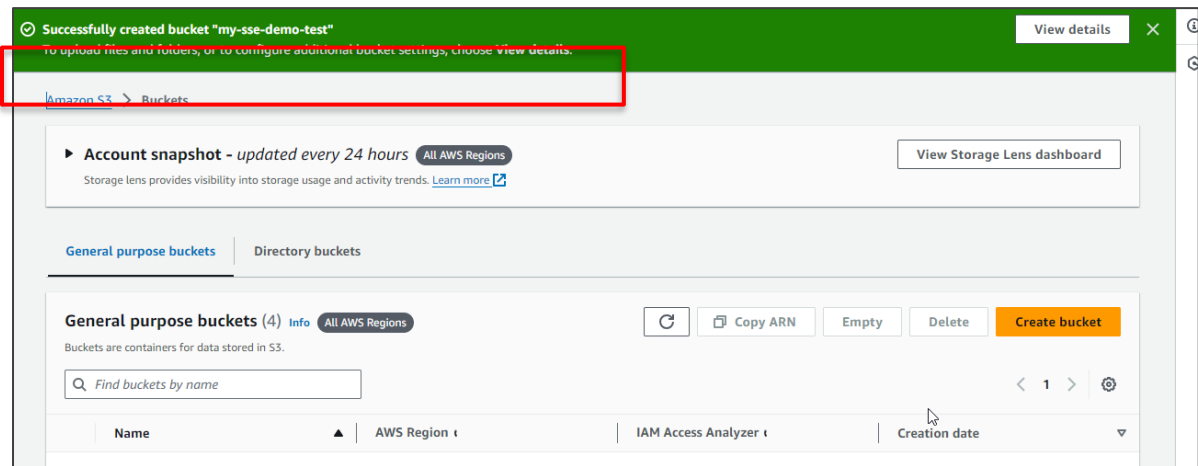
☐ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see [DSSE-KMS pricing](#) on the [Storage](#) tab of the [Amazon S3 pricing page](#).

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](#)

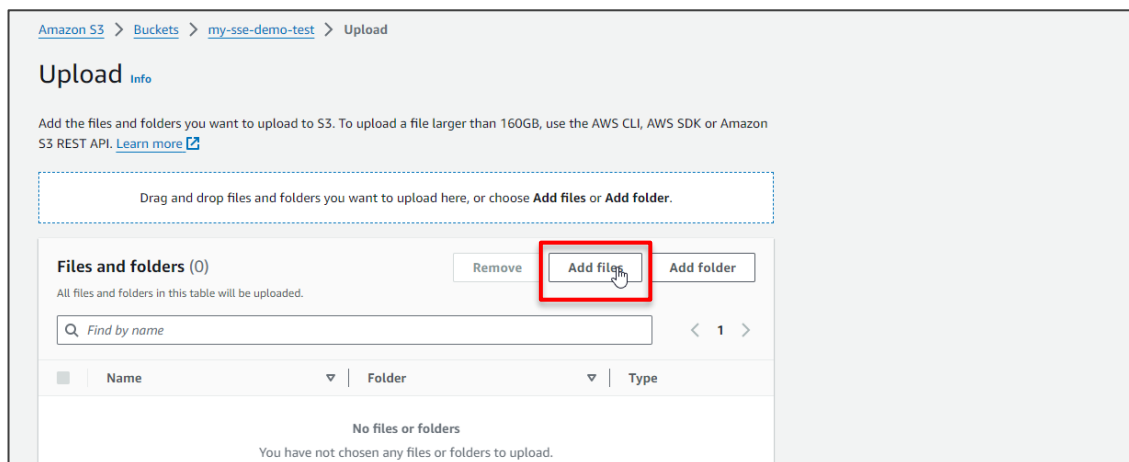
☐ Disable

☒ Enable

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



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



Upload succeeded
View details below.

Destination

s3://my-sse-demo-test

Succeeded

1 file, 4.9 KB (100.00%)

Failed

0 files, 0 B (0%)

Files and folders

Configuration

Files and folders (1 Total, 4.9 KB)

< 1 >

Name	Folder	Type	Size	Status	Error
348s.jpg	-	image/jpeg	4.9 KB	Succeeded	-

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

[Amazon S3](#) > [Buckets](#) > my-sse-demo-test

my-sse-demo-test

Info

Objects

Properties

Permissions

Metrics

Management

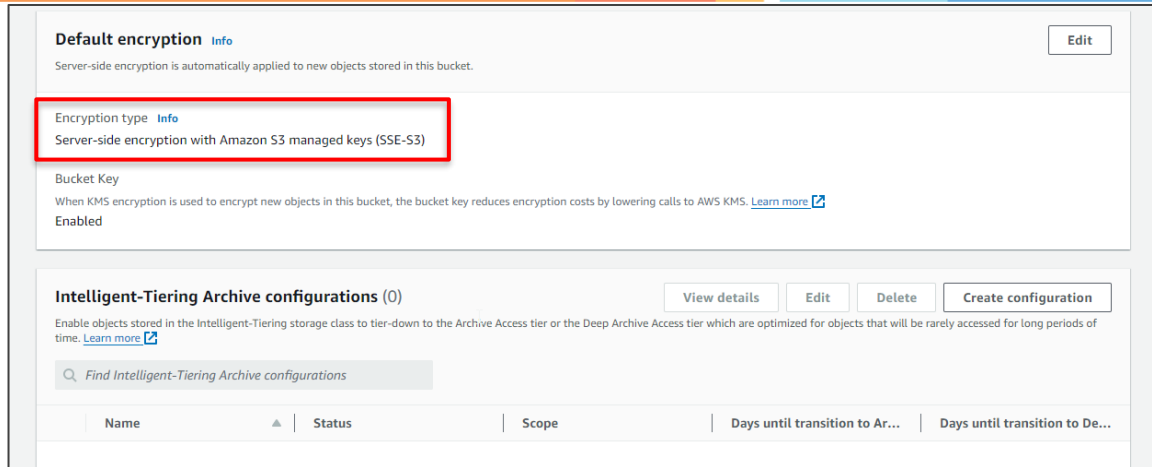
Access Points

Bucket overview

<div>AWS Region</div> <div>US East (N. Virginia) us-east-1</div>	<div>Amazon Resource Name (ARN)</div> <div> arn:aws:s3:::my-sse-demo-test</div>	<div>Creation date</div> <div>August 9, 2024, 18:18:06 (UTC+05:30)</div>
--	---	--

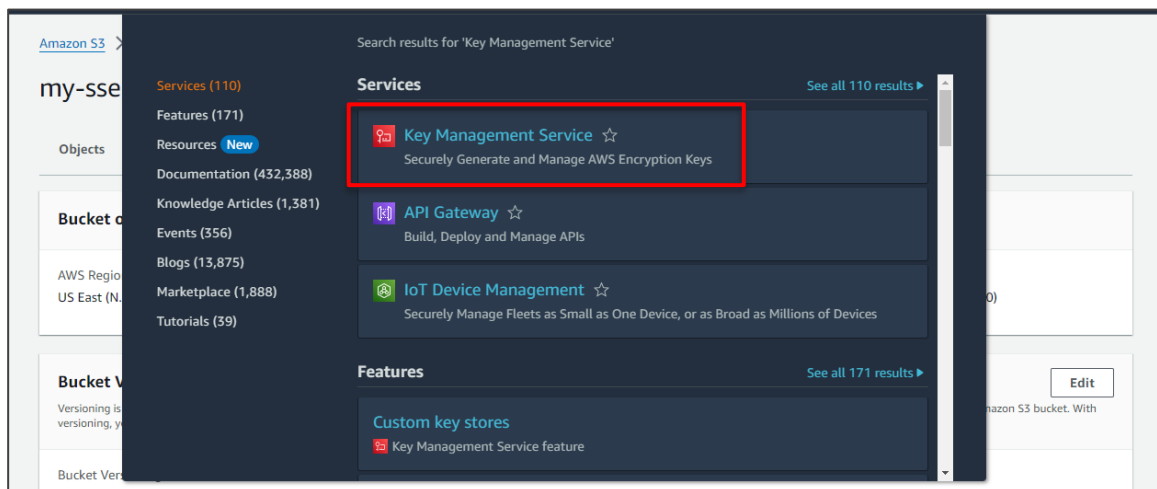
Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

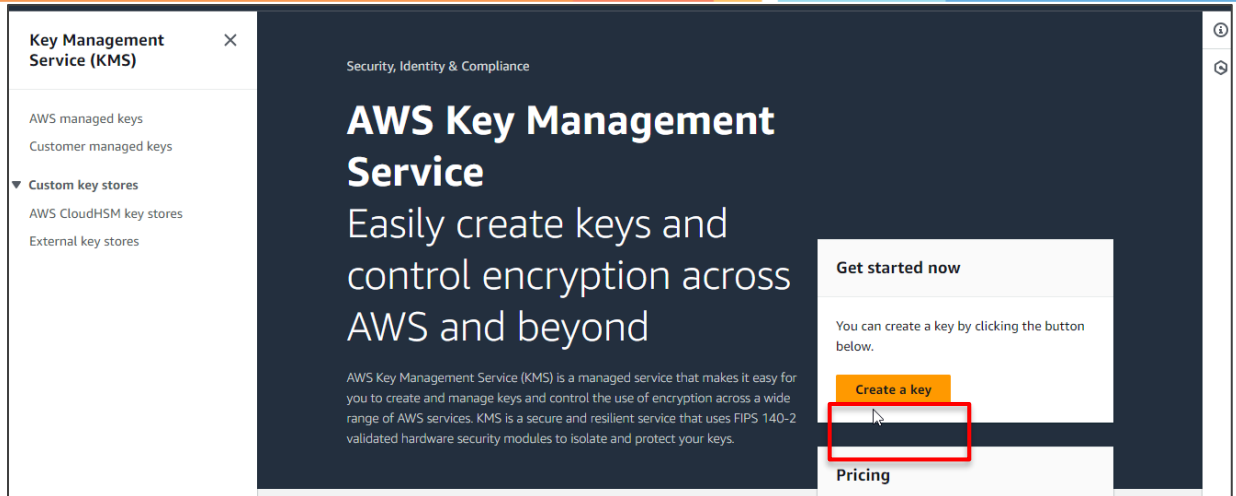


Step 2: Create a Key Management Service (KMS) key

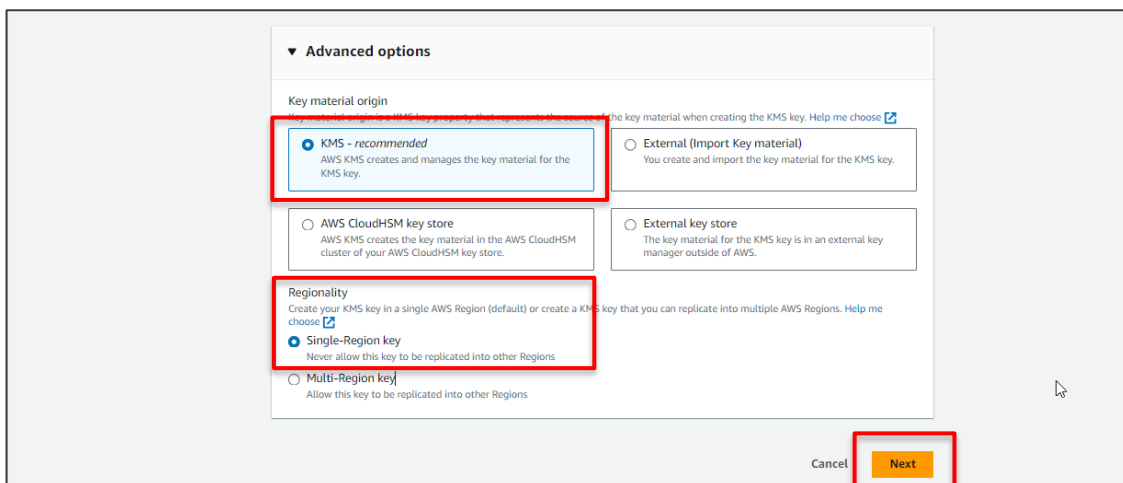
2.1 Access the AWS Management Console, search for **Key Management Service**, and select it



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

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

Add labels

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

Alias
CMK-demo

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

Description
Description of the key

2.5 Click on **Next**

Step 4
Define key usage permissions

Step 5
Review

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

Description
Description of the key

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**

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 administrative permissions

Key administrators (1/11)
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](#)

Search Key administrators

	Name	Path	Type
<input type="checkbox"/>	dev-admin	/	User
<input checked="" type="checkbox"/>	odl_user_1422073	/	User
<input type="checkbox"/>	AWSServiceRoleForAmazonIns...	/aws-service-role/inspector.a...	Role
<input type="checkbox"/>	AWSServiceRoleForApplicatio...	/aws-service-role/dynamodb.a...	Role
<input type="checkbox"/>	AWSServiceRoleForConfig	/aws-service-role/config.amaz...	Role
<input type="checkbox"/>	AWSServiceRoleForOrganizati...	/aws-service-role/organization...	Role
<input type="checkbox"/>	AWSServiceRoleForRedshift	/aws-service-role/redshift.am...	Role

Review

<input type="checkbox"/>	AWSServiceRoleForAmazonIns...	/aws-service-role/inspector.a...	Role
<input type="checkbox"/>	AWSServiceRoleForApplicatio...	/aws-service-role/dynamodb.a...	Role
<input type="checkbox"/>	AWSServiceRoleForConfig	/aws-service-role/config.amaz...	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 (1/11)
Select the IAM users and roles that can use the KMS key in cryptographic operations. [Learn more](#)

Search Key users

<input type="checkbox"/>	Name	Path	Type
<input type="checkbox"/>	dev-admin	/	User
<input checked="" type="checkbox"/>	odl_user_1422073	/	User
<input type="checkbox"/>	AWSServiceRoleForAmazonIns...	/aws-service-role/inspector.a...	Role
<input type="checkbox"/>	AWSServiceRoleForApplicatio...	/aws-service-role/dynamodb.a...	Role
<input type="checkbox"/>	AWSServiceRoleForConfig	/aws-service-role/config.amaz...	Role
<input type="checkbox"/>	AWSServiceRoleForOrganizati...	/aws-service-role/organization...	Role

2.8 Click on Next

<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

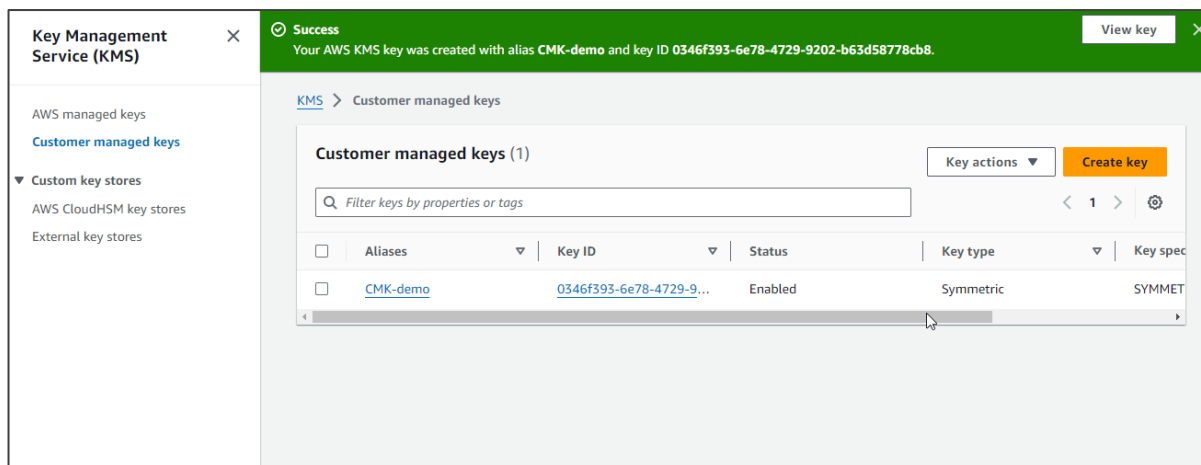
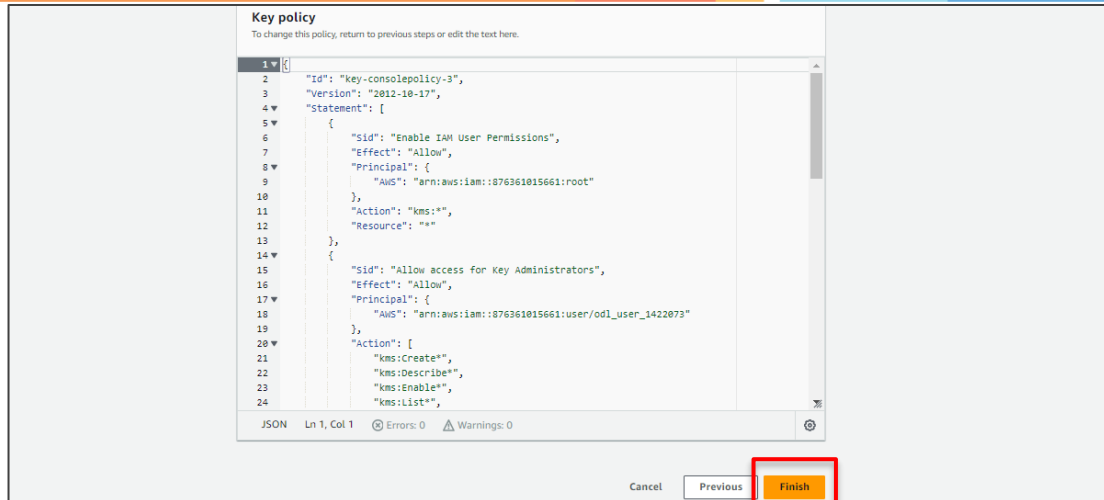
Other AWS accounts

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](#)

[Add another AWS account](#)

Cancel Previous **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**

Amazon S3 > Buckets > my-sse-demo-test > Edit default encryption

Edit default encryption [Info](#)

Default encryption
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](#).

AWS KMS key [Info](#)

- ☒ Choose from your AWS KMS keys
- ☐ Enter AWS KMS key ARN

Available AWS KMS keys

Choose AWS KMS key

3.2 Click **Save changes**

AWS KMS key [Info](#)

- ☒ Choose from your AWS KMS keys
- ☐ Enter AWS KMS key ARN

Available AWS KMS keys

arn:aws:kms:us-east-1:876361015661:key/0346f...

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

Warning: Changing the default encryption settings might cause in-progress replication and Batch Replication jobs to fail. These jobs might fail because of missing AWS KMS permissions on the IAM role that's specified in the replication configuration. If you change the default encryption settings, make sure that this IAM role has the necessary AWS KMS permissions. [Learn more](#)

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



Successfully edited default encryption. Objects uploaded, modified, or copied into this bucket will inherit this encryption configuration unless otherwise specified.

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

my-sse-demo-test [Info](#)

Objects | **Properties** | Permissions | Metrics | Management | Access Points

Bucket overview

AWS Region US East (N. Virginia) us-east-1	Amazon Resource Name (ARN) arn:aws:s3:::my-sse-demo-test	Creation date August 9, 2024, 18:18:06 (UTC+05:30)
---	---	---

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

[Edit](#)

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

Account snapshot - updated every 24 hours [All AWS Regions](#) [View Storage Lens dashboard](#)
Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

General purpose buckets | Directory buckets

General purpose buckets (2) [Info](#) [All AWS Regions](#)

Buckets are containers for data stored in S3.

[Refresh](#) [Copy ARN](#) [Empty](#) [Delete](#) [Create bucket](#)

	Name	AWS Region	IAM Access Analyzer	Creation date
<input type="radio"/>	my-sse-demo-test	US East (N. Virginia) us-east-1	View analyzer for us-east-1	August 9, 2024, 18:18:06 (UTC+05:30)
<input type="radio"/>	my-sse-kms-demo-test	US East (N. Virginia) us-east-1	View analyzer for us-east-1	August 9, 2024, 18:51:36 (UTC+05:30)

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

3.3 Upload a file using Add files

Amazon S3 > Buckets > my-sse-kms-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 folder](#).

Files and folders (0) [Remove](#) [Add files](#) [Add folder](#)

All files and folders in this table will be uploaded.

[Refresh](#) [Copy ARN](#) [Empty](#) [Delete](#) [Create bucket](#)

<input type="checkbox"/>	Name	Folder	Type
No files or folders You have not chosen any files or folders to upload.			

Upload succeeded
View details below.

Destination
s3://my-sse-kms-demo-test

Succeeded
 1 file, 4.9 KB (100.00%)

Failed
 0 files, 0 B (0%)

Files and folders | Configuration

Files and folders (1 Total, 4.9 KB)

Find by name

< 1 >

Name	Folder	Type	Size	Status	Error
348s.jpg	-	image/jpeg	4.9 KB	Succeeded	-

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

[Amazon S3](#) > [Buckets](#) > my-sse-kms-demo-test

my-sse-kms-demo-test
[Info](#)

Objects | **Properties** | Permissions | Metrics | Management | Access Points

Bucket overview

AWS Region US East (N. Virginia) us-east-1	Amazon Resource Name (ARN) arn:aws:s3::my-sse-kms-demo-test	Creation date August 9, 2024, 18:51:36 (UTC+05:30)
---	--	---

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning

Edit

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)

Bucket Key

When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. [Learn more](#)

Enabled

Intelligent-Tiering Archive configurations (0)

[View details](#)
[Edit](#)
[Delete](#)
[Create configuration](#)

Enable objects stored in the Intelligent-Tiering storage class to tier-down to the Archive Access tier or the Deep Archive Access tier which are optimized for objects that will be rarely accessed for long periods of time. [Learn more](#)

Find Intelligent-Tiering Archive configurations

Name	Status	Scope	Days until transition to Ar...	Days until transition to De...

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