

## Lesson 04 Demo 08

### Creating and Deleting Keys with Amazon KMS

**Objectives:** To create and delete customer-managed keys using Amazon KMS

**Tools required:** None

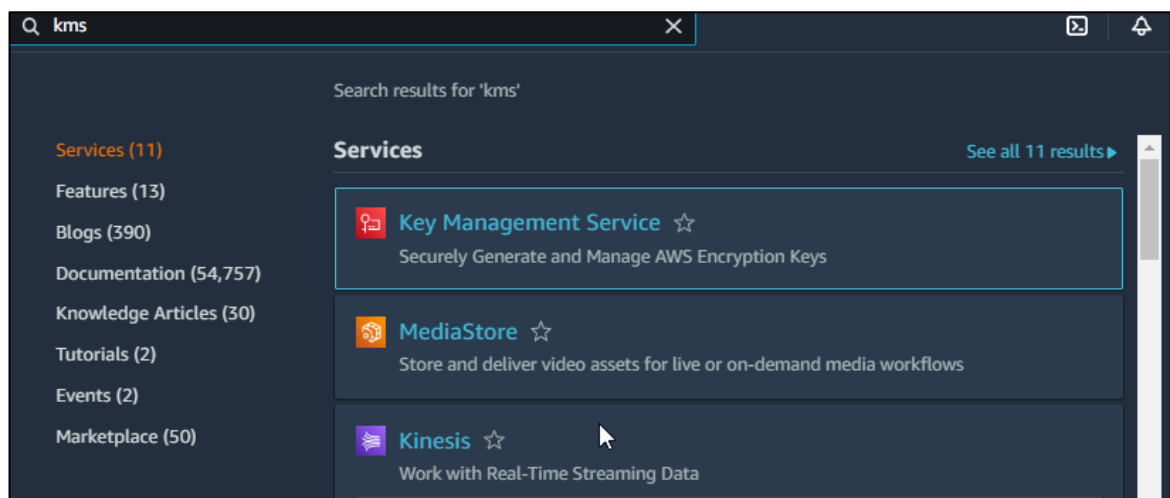
**Prerequisites:** AWS account with an S3 bucket created

Steps to be followed:

1. Create a customer-managed key
2. Delete a customer-managed key

#### Step 1: Create a customer-managed key

- 1.1 Access the AWS Management Console homepage, search for **Key Management Service**, and select it



## 1.2 Click on **Create a key**

Security, Identity & Compliance

# AWS Key Management Service

## Easily create keys and control encryption across AWS and beyond

AWS Key Management Service (KMS) is a managed service that makes it easy for you to create and manage keys and control the use of encryption across a wide range of AWS services. KMS is a secure and resilient service that uses FIPS 140-2 validated hardware security modules to isolate and protect your keys.

**Get started now**

You can create a key by clicking the button below.

**Create a key**

## 1.3 Configure the key using default settings, and proceed to the next step

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

### Configure key

**Key type** [Help me choose](#)

☒ **Symmetric**  
A single key used for encrypting and decrypting data or generating and verifying HMAC codes

☐ **Asymmetric**  
A public and private key pair used for encrypting and decrypting data or signing and verifying messages

**Key usage** [Help me choose](#)

☒ **Encrypt and decrypt**  
Use the key only to encrypt and decrypt data.

☐ **Generate and verify MAC**  
Use the key only to generate and verify hash-based message authentication codes (HMAC).

1.4 Choose **KMS** for Key material origin and **Single-Region key** for Regionality, and 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

1.5 Enter **CMK-demo** as the **Alias** name

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

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

Description - optional

## 1.6 Select the username associated with your AWS Lab as **Key administrators**

### Define key administrative permissions

**Key administrators**  
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](#)

< 1 >

<input type="checkbox"/>	Name	Path	Type
<input type="checkbox"/>	dev-admin	/	User
<input checked="" type="checkbox"/>	odl_user_687241	/	User
<input type="checkbox"/>	user1-13	/	User
<input type="checkbox"/>	user23	/	User
<input type="checkbox"/>	AWSServiceRoleForAutoScaling	/aws-service-role/autoscaling.amazonaws.com/	Role
<input type="checkbox"/>	AWSServiceRoleForOrganizations	/aws-service-role/organizations.amazonaws.com/	Role

## 1.7 Check **Allow key administrators to delete this key** and click **Next**

<input type="checkbox"/>	AWSServiceRoleForTrustedAdvisor	role/trustedadvisor.amazonaws.com/	Role
<input type="checkbox"/>	OrganizationAccountAccessRole	/	Role

### Key deletion

☒ Allow key administrators to delete this key.

Cancel
Previous
Next

1.8 Under **Define key usage permissions**, select the username of your AWS Lab, and click on **Next**

## Define key usage permissions

### This account

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_687241	/	User
<input type="checkbox"/>	user1-13	/	User
<input type="checkbox"/>	user23	/	User
<input type="checkbox"/>	AWSServiceRoleForAutoScaling	/aws-service-role/autoscaling.amazonaws.com/	Role
<input type="checkbox"/>	AWSServiceRoleForOrganizations	/aws-service-role/organizations.amazonaws.com/	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](#)

## 1.9 Scroll down to the **Key policy** tab, and click on **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 2: Delete a customer-managed key

### 2.1 Navigate to **Customer managed keys** and click on the created key

**Key Management Service (KMS)**

Success: 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)

Filter keys by properties or tags

Aliases	Key ID	Status	Key spec	Key usage
CMK-demo	35cb7076-5315-4d68-9d36-704e31f73d0c	Enabled	SYMMETRIC_DEFAULT	Encrypt and decrypt

### 2.2 Under **Key actions**, select **Schedule key deletion**

KMS > Customer managed keys > Key ID: 35cb7076-5315-4d68-9d36-704e31f73d0c

35cb7076-5315-4d68-9d36-704e31f73d0c

Key actions: Disable, Schedule key deletion

**General configuration**

Alias CMK-demo	Status Enabled	Creation date Jul 21, 2022 17:19 GMT+5:30
ARN arn:aws:kms:us-east-1:043805049749:key/35cb7076-5315-4d68-9d36-704e31f73d0c	Description -	Regionality Single Region

### 2.3 Under **Schedule key deletion**, add a number between **7** and **30** for the waiting period

**Schedule key deletion**

⚠️ Deleting a key makes all data encrypted under that key unrecoverable. [Learn more](#)

You can create an Amazon CloudWatch alarm that alerts you about any attempts to use the key(s) during the waiting period. [Learn more](#)

**Waiting period**

You can cancel deletion any time before the waiting period ends. After the waiting period ends, AWS KMS deletes the key(s). [Learn more](#)

Waiting period (in days)

7

Enter a waiting period between 7 and 30 days.

**Keys to delete**

The following keys will be scheduled for deletion.

Aliases	Key ID	Key usage	Regionality
CMK-demo	35cb7076-5315-4d68-9d36-704e31f73d0c	Encrypt and decrypt	Single Region

## 2.4 Confirm the deletion, and click on **Schedule deletion**

**Keys to delete**  
The following keys will be scheduled for deletion.

Aliases	Key ID	Key usage	Regionality
CMK-demo	35cb7076-5315-4d68-9d36-704e31f73d0c	Encrypt and decrypt	Single Region

**Confirmation**  
☒ Confirm that you want to schedule these keys for deletion after a 7 day waiting period.

Cancel
Schedule deletion

Successfully scheduled deletion for key `arn:aws:kms:us-east-1:043805049749:key/35cb7076-5315-4d68-9d36-704e31f73d0c`

X

KMS > Customer managed keys > Key ID: 35cb7076-5315-4d68-9d36-704e31f73d0c

35cb7076-5315-4d68-9d36-704e31f73d0c

Key actions
Edit

**General configuration**

Alias CMK-demo	Status Pending deletion	Creation date Jul 21, 2022 17:19 GMT+5:30
ARN <code>arn:aws:kms:us-east-1:043805049749:key/35cb7076-5315-4d68-9d36-704e31f73d0c</code>	Description -	Scheduled deletion date Jul 28, 2022 17:35 GMT+5:30
Regionality Single Region		

The key has been scheduled for deletion successfully.

**Note:** The key will be deleted after 7 days.

By following these steps, you have gained the ability to confidently manage cryptographic keys, ensuring robust security practices in your AWS environment.