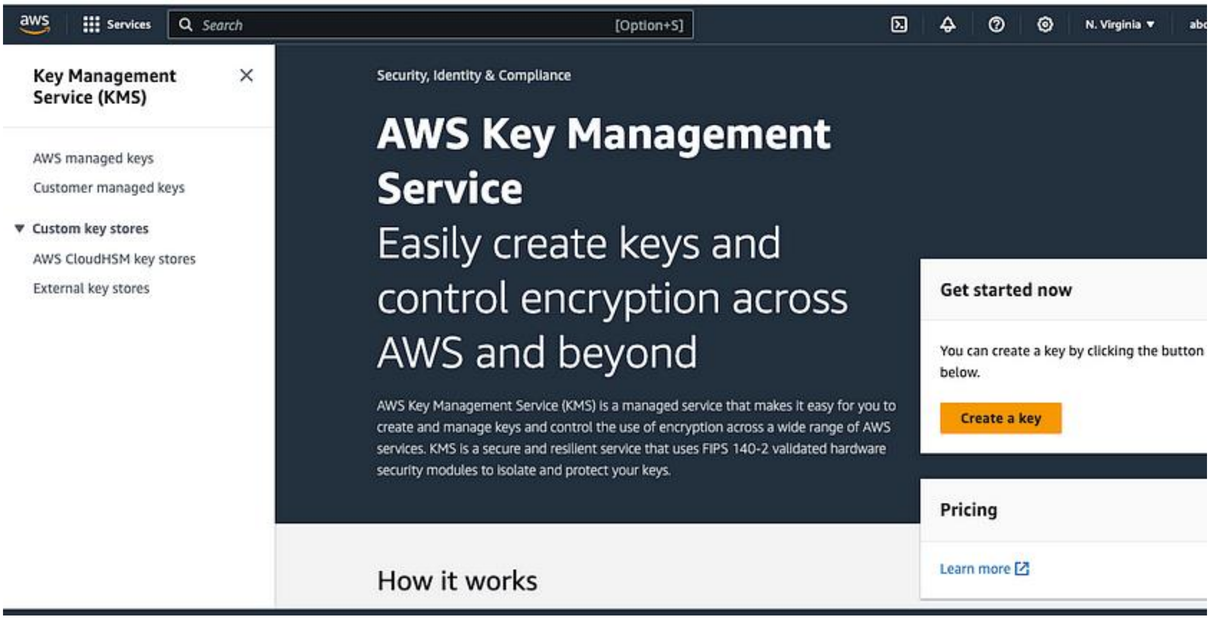
1. Log into your aws account.

2. Search for KMS service and click on it.

3. Click on the “create a key” orange button on the console.



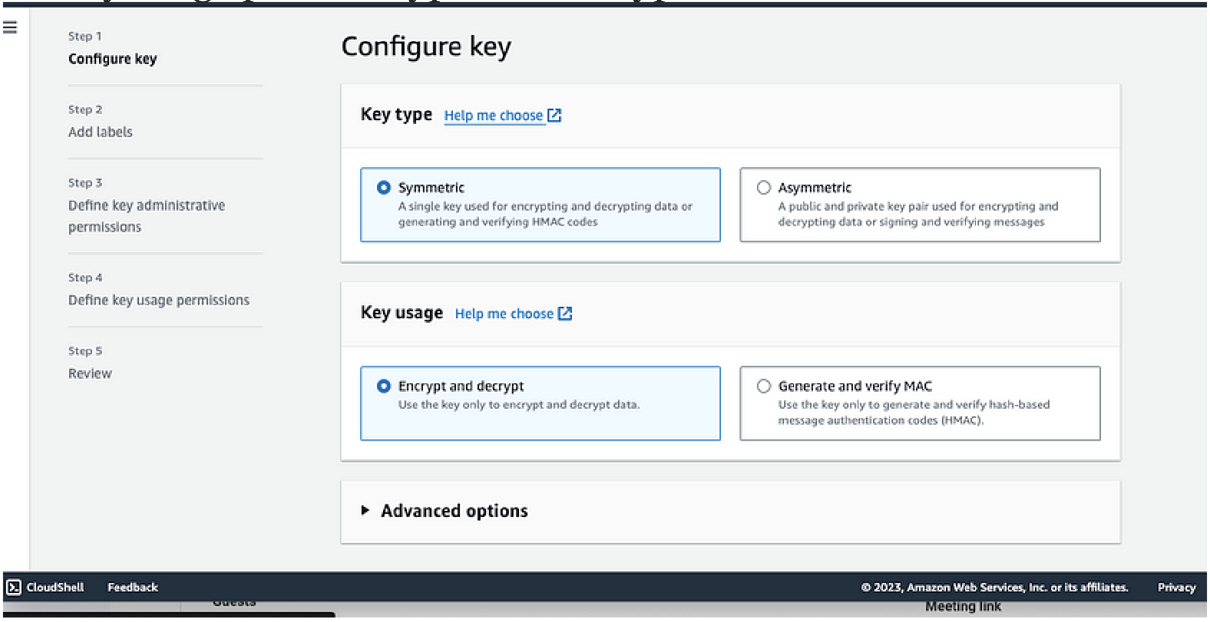
AWS Key Management Service

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.

You can create a key by clicking the button below.

4. Create Customer Managed Key. Pick Symmetric for key type and for key usage pick Encrypt and Decrypt. Then Click Next.



Configure key

Key type

● 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

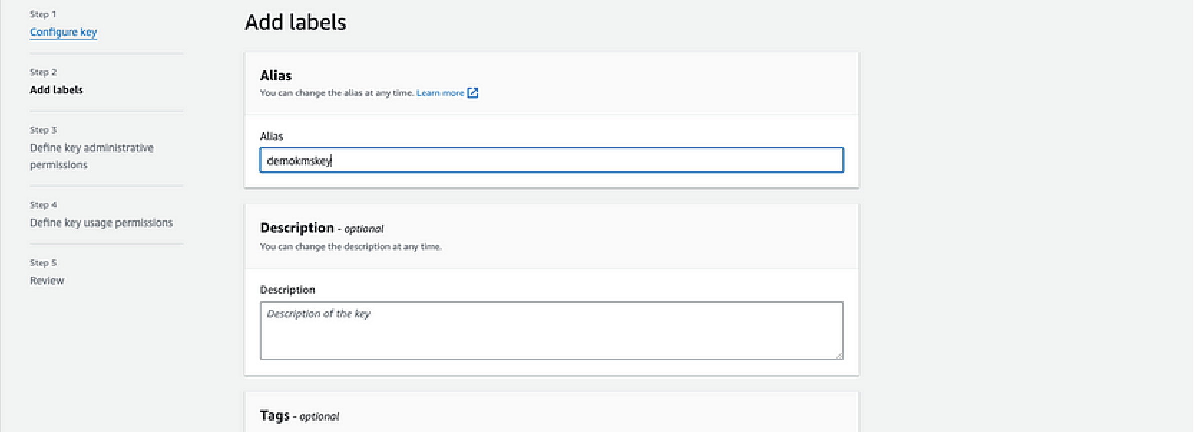
● Encrypt and decrypt
Use the key only to encrypt and decrypt data.

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

© 2023, Amazon Web Services, Inc. or its affiliates.

5. You will need to give this Customer Managed Key an alias name.

I named mine demokmskey. Feel free to give your CMK key a basic name as well. We will use this alias name later. After typing your alias name click next


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: demokmskey

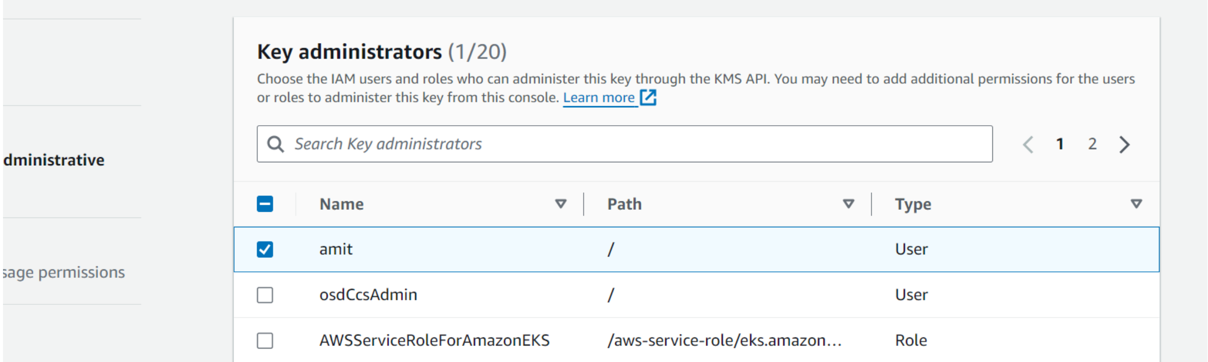
Description - optional

You can change the description at any time.

Description: Description of the key

Tags - optional

6. Pick a key administrator for this key. To make things easy I will choose the user that I am currently logged in with. We created a user during the pre-req .

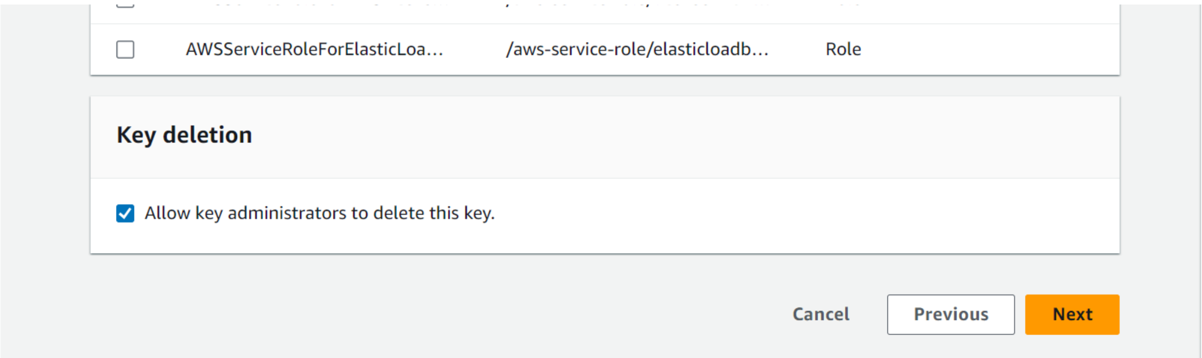


Key administrators (1/20)

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

	Name	Path	Type
☑	amit	/	User
□	osdCcsAdmin	/	User
□	AWSServiceRoleForAmazonEKS	/aws-service-role/eks.amazon...	Role

7. Ensure the key deletion box is checked, then click next.

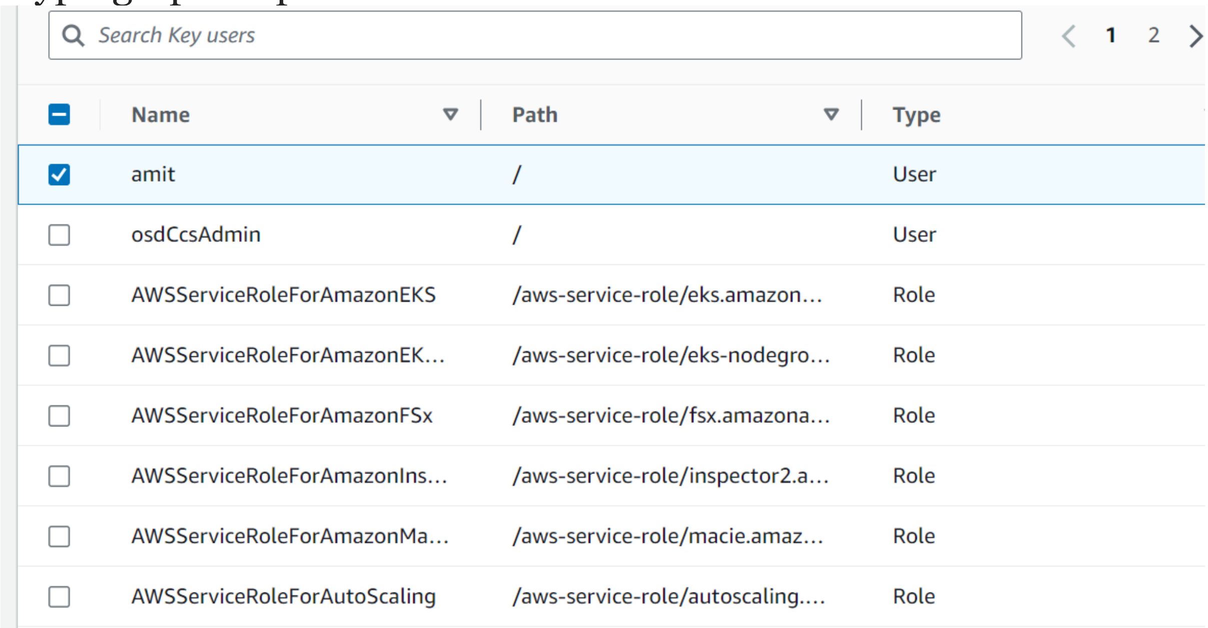


□	AWSServiceRoleForElasticLoa…	/aws-service-role/elasticloadb…	Role

Key deletion

☑ Allow key administrators to delete this key.

8. For key usage permissions pick the same user picked from the previous . This is permission on who can use the kms key for cryptographic operations.



▬	Name	Path	Type
☑	amit	/	User
□	osdCcsAdmin	/	User
□	AWSServiceRoleForAmazonEKS	/aws-service-role/eks.amazon…	Role
□	AWSServiceRoleForAmazonEK…	/aws-service-role/eks-nodegro…	Role
□	AWSServiceRoleForAmazonFSx	/aws-service-role/fsx.amazona…	Role
□	AWSServiceRoleForAmazonIns…	/aws-service-role/inspector2.a…	Role
□	AWSServiceRoleForAmazonMa…	/aws-service-role/macie.amaz…	Role
□	AWSServiceRoleForAutoScaling	/aws-service-role/autoscaling.…	Role

9. Click next. Now you will be at the review stage. Click finish at the bottom right.

10. You now have a kms key.

Using the CMK for encryption and Decryption

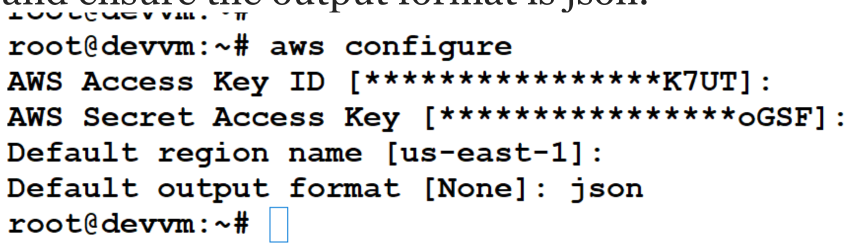
1. Open up your terminal

2. Create a folder called kmslab

mkdir kmslab

3. Navigate to this folder in the command line.

4. Make sure you have aws cli configured by running "aws configure" on the command line. Configure your credentials regions and ensure the output format is json.

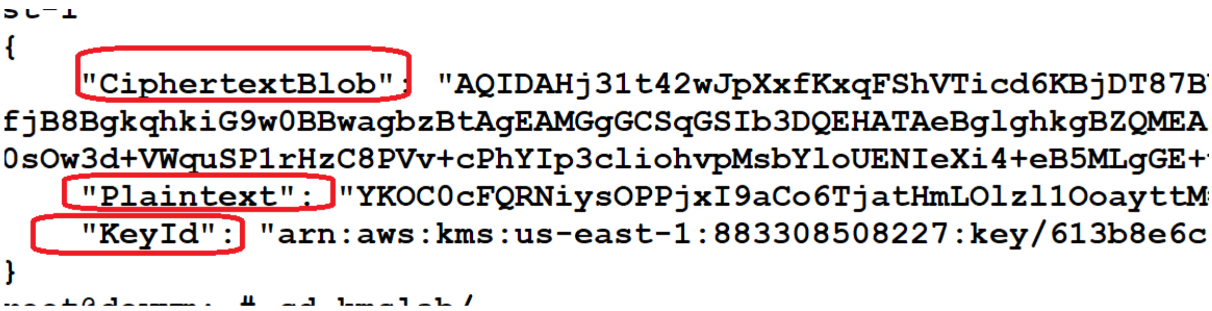


```
root@devvm:~# aws configure
AWS Access Key ID [****************K7UT]:
AWS Secret Access Key [****************oGSF]:
Default region name [us-east-1]:
Default output format [None]: json
root@devvm:~#
```

5. Run this aws cli command and ensure that you change the alias and the region to the alias you created originally as well as the region you created that cmk. For my case, my alias is called demokmskey and the region is us-east-1.

Run "aws kms generate-data-key --key-id alias/demokmskey --key-spec AES_256 --region us-east-1"

6. After running that command you should get a ciphetextblob, plaintext, and a key id listed.



```
st-1
{
    "CiphertextBlob": "AQIDAHj31t42wJpXxfKxqFShVTicd6KBjDT87B
fjB8BgkqhkiG9w0BBwagbzBtAgEAMGgGCSqGSIb3DQEHATAeBglghkgBZQMEA
0sOw3d+VWquSP1rHzC8PVv+cPhYIp3cliohvpMsbYloUENIeXi4+eB5MLgGE+
    "Plaintext": "YKOC0cFQRNiysOPPjxI9aCo6TjatHmLOlzl1OoayttM
    "KeyId": "arn:aws:kms:us-east-1:883308508227:key/613b8e6c
}
```