#### **KMS Exam Tips**



#### **CREATING A CMK**

#### Set Up CMK

Create alias and description. Choose key material option.



#### **Key Administrative Permissions**

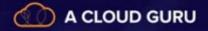
IAM users and roles that can administer (but not use) the key through the KMS API.



#### **Key Usage Permissions**

IAM users and roles that can use the key to encrypt and decrypt data.





#### **KMS 101**

## KMS Exam Tips

#### KMS COMPONENTS



#### **AWS-Managed CMK**

AWS-provided and AWS-managed CMK. Used on your behalf with the AWS services integrated with KMS.



#### **Customer-Managed CMK**

You create, own and manage yourself. Used to encrypt, decrypt files up to 4KB and generate the data key.



#### **Data Key**

Encryption key that you can use to encrypt data, including large amounts of data. You can use a CMK to generate, encrypt, and decrypt data keys.





### **Envelope Encryption**

Encrypting the key that encrypts our data.

The CMK is used to encrypt the data key (or envelope key).

The data key encrypts our data.

Used for encrypting anything over 4 KB.

By using envelope encryption this avoids sending all your data into KMS over the network.





#### aws kms encrypt

Encrypts plaintext into ciphertext by using a customer master key.



#### aws kms re-encrypt

Decrypts ciphertext and then reencrypts using a CMK that you specify. (e.g. when you change the CMK or manually rotate the CMK).



#### aws kms decrypt

Decrypts ciphertext that was encrypted by a customer master key.



#### aws kms enable-key-rotation

( ) A CLOUD GURU

Enables automatic key rotation every 365 days.

# **Exam Tips KMS API Calls**



#### aws kms generate-data-key

Uses the CMK to generate a data key to encrypt data using envelope encryption.