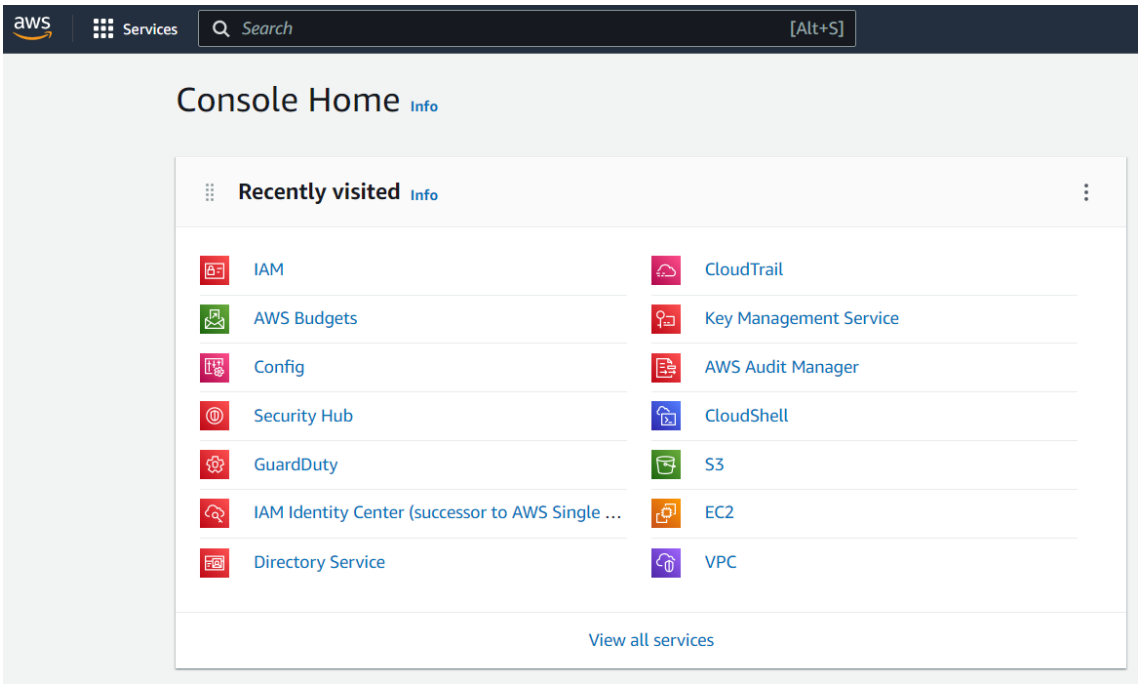
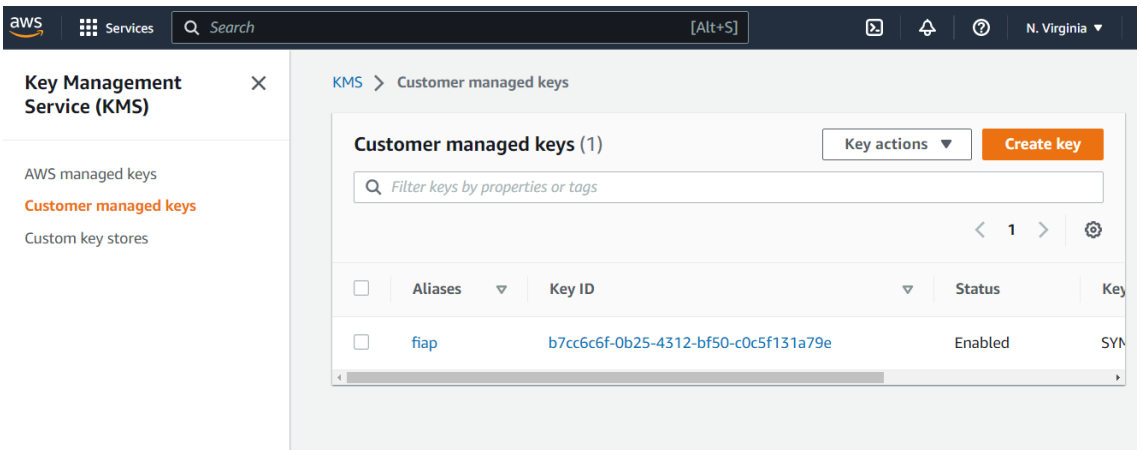
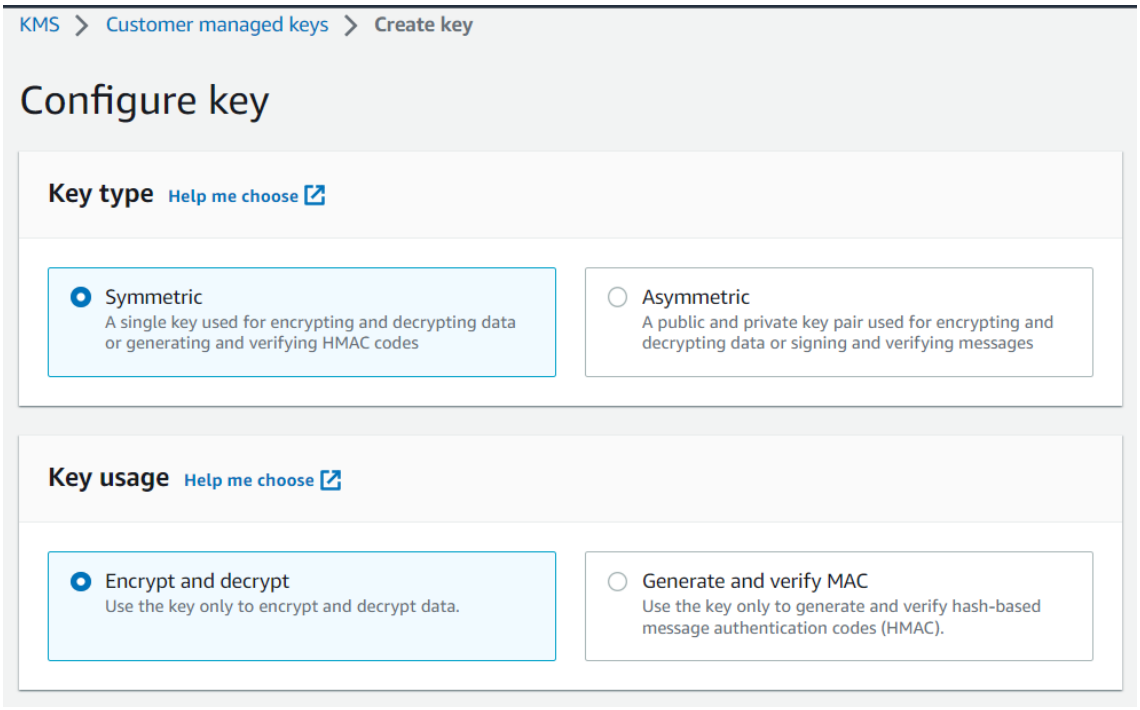
Laboratório 3: Criptografia usando o AWS KMS

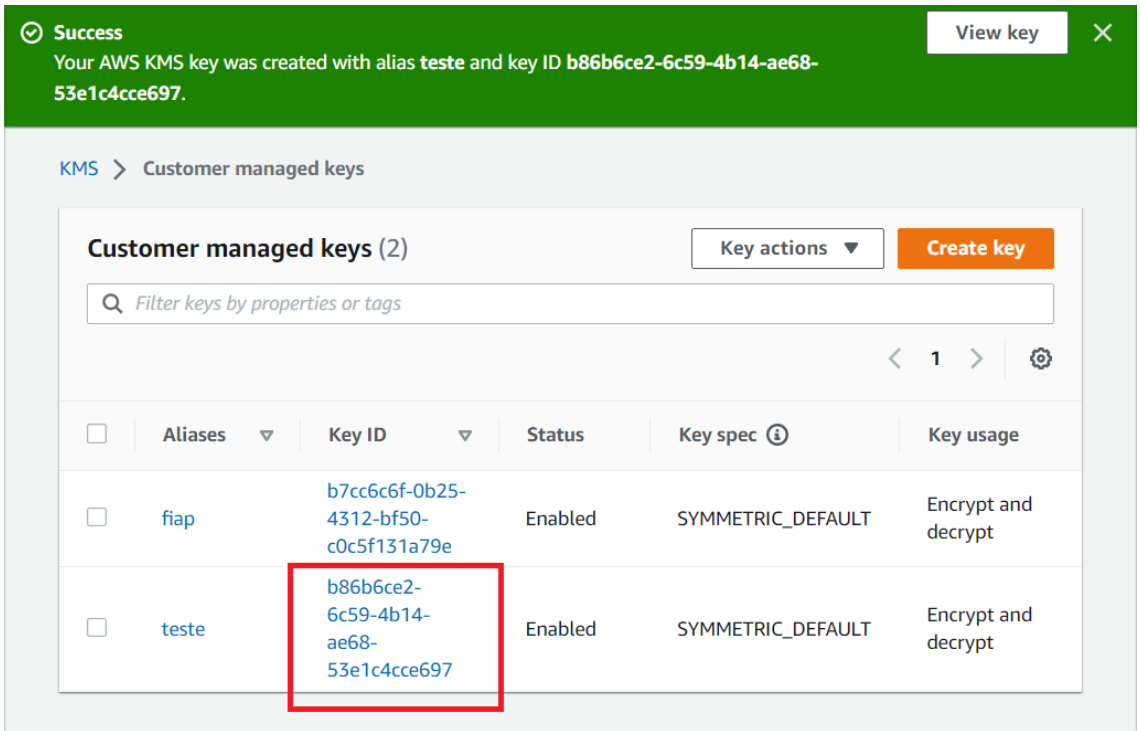
1)Acesse a sua conta da AWS.



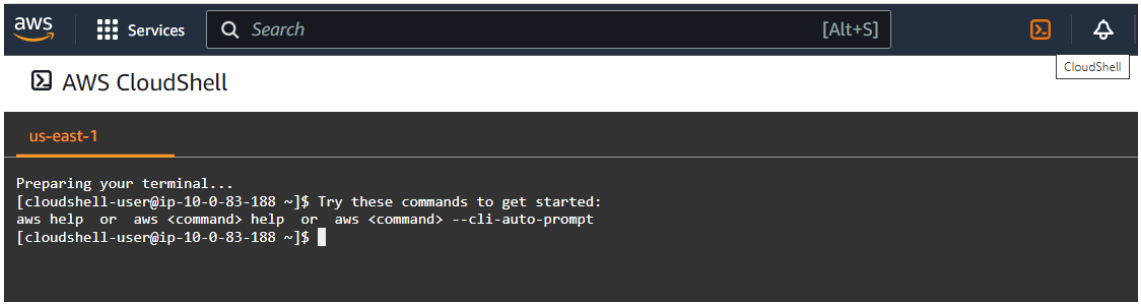
2)Acesse o serviço KMS e crie uma chave simétrica. Anote o ID da chave.







3)Acesse o cloud shell



4)Crie um arquivo chamado senha.txt. Coloque um texto super secreto dentro dele.

5)Execute o seguinte comando no cloud shell:

aws kms encrypt --key-id b7cc6c6f-0b25-4312-bf50-c0c5f131a79e --plaintext fileb://senha.txt --output text --query CiphertextBlob --region us-east-1 > senha.base64

cat senha.base64 | base64 --decode > Encrypteddatafile

6)Apague os arquivos criados, exceto o "Encryteddatafile". Perceba que não restaram arquivos para ler. Somente o arquivo binário do arquivo criptografado.

Este arquivo foi criptografado com algoritmo simétrico AES-256.

7)Volte ao cloud shell e execute o seguinte comando:

aws kms decrypt --ciphertext-blob fileb://Encrypteddatafile --output text --query Plaintext > Decrypteddatafile.base64

cat Decrypteddatafile.base64 | base64 --decode > Decrypteddatafile.txt

8)Abra e leia o arquivo.