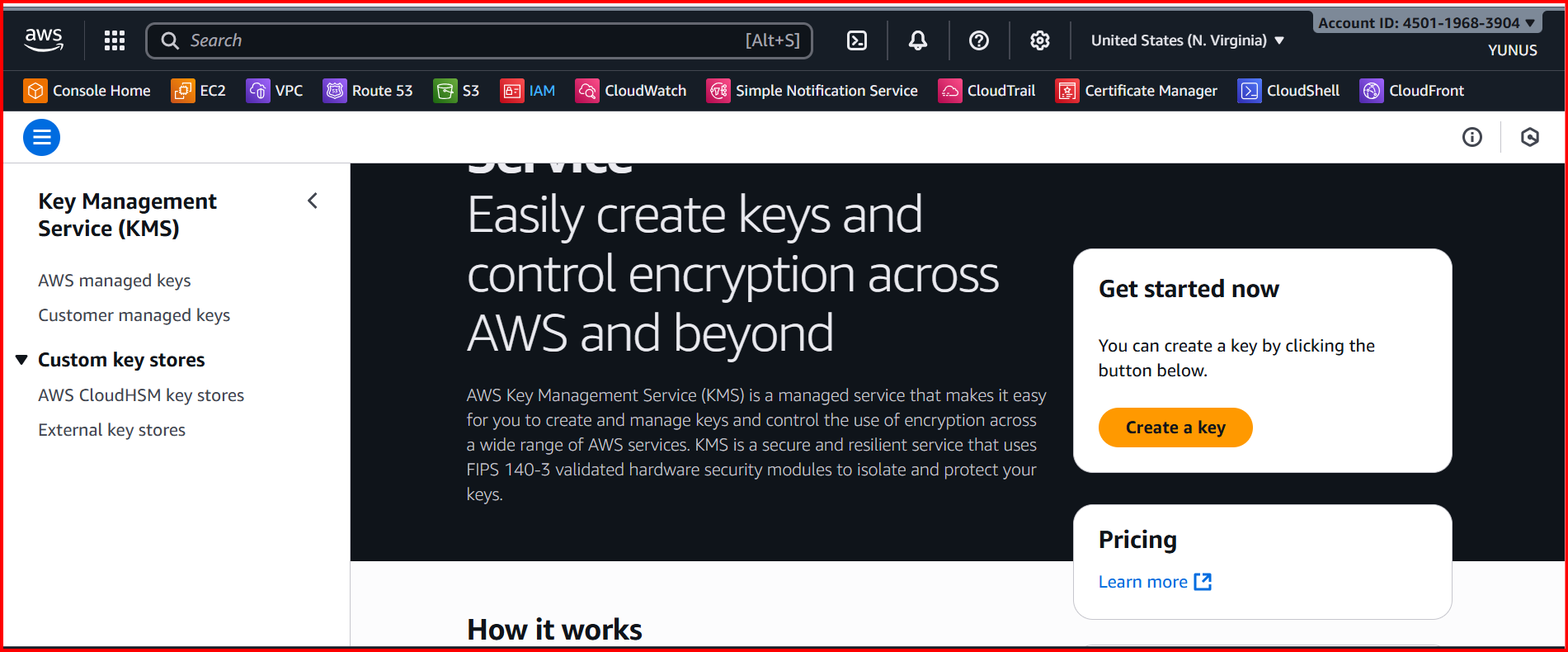
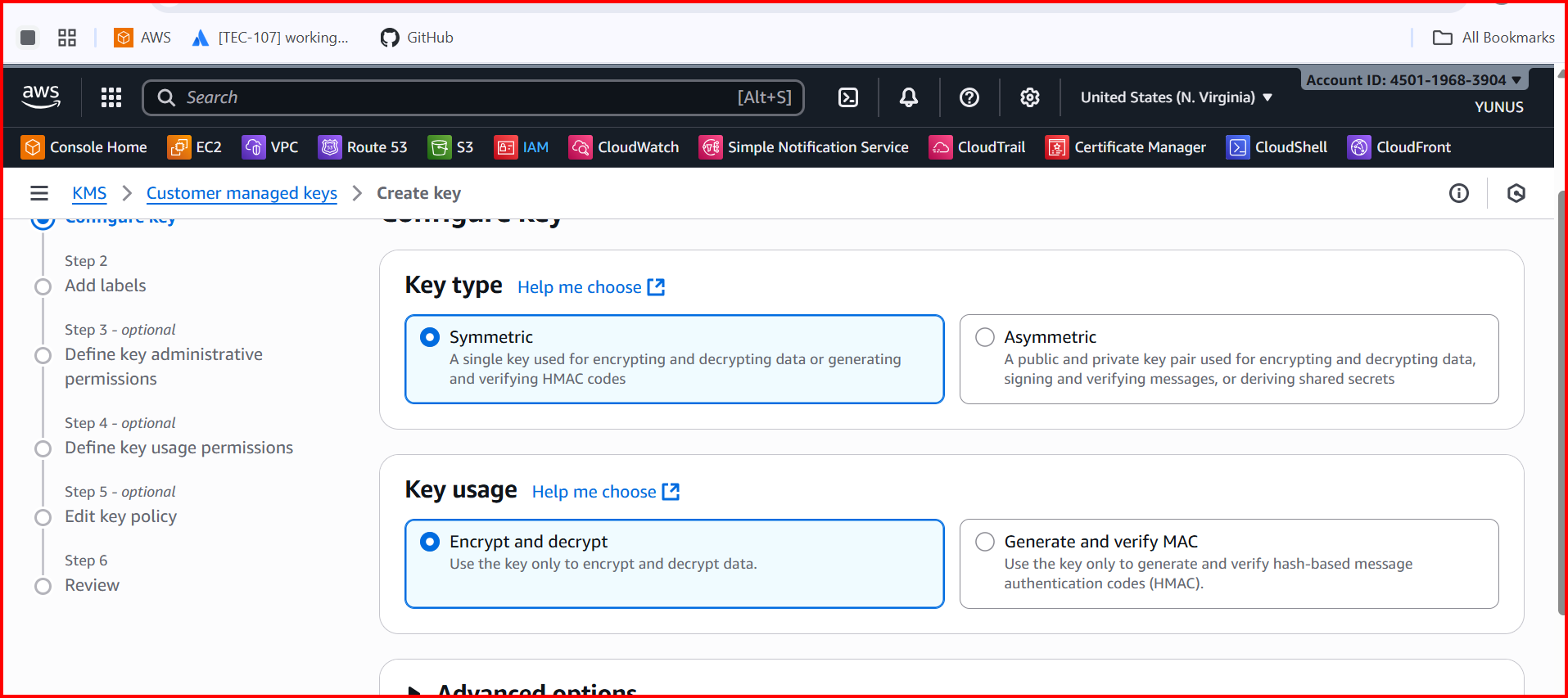
**AWS KMS**

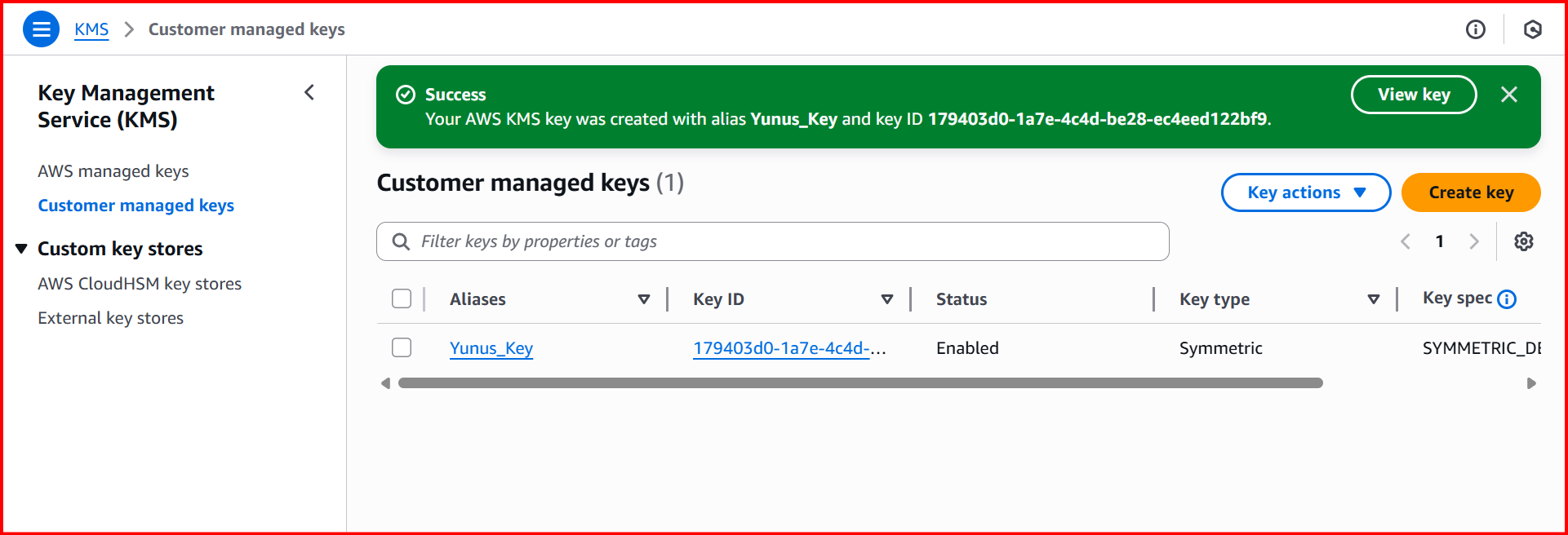
**Console → Key Management Service → Customer managed keys → Create key.**

****

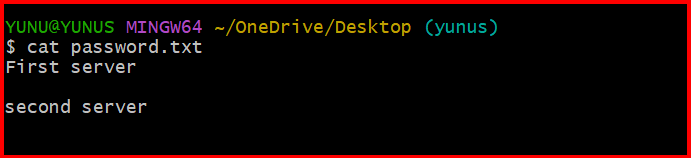
**Create a key**

****

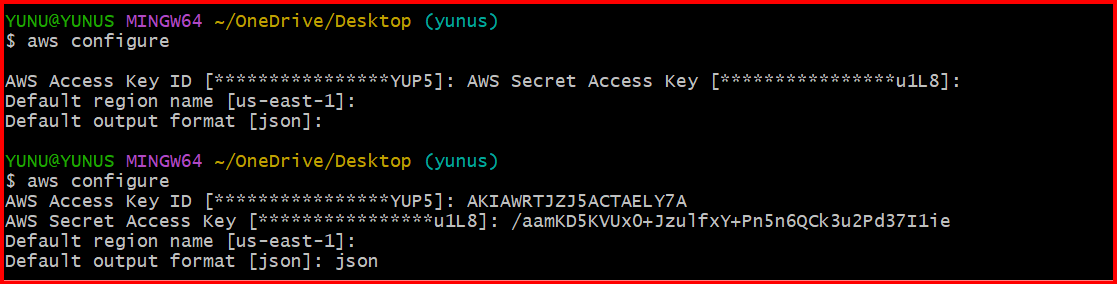
**Select the permissions**

****

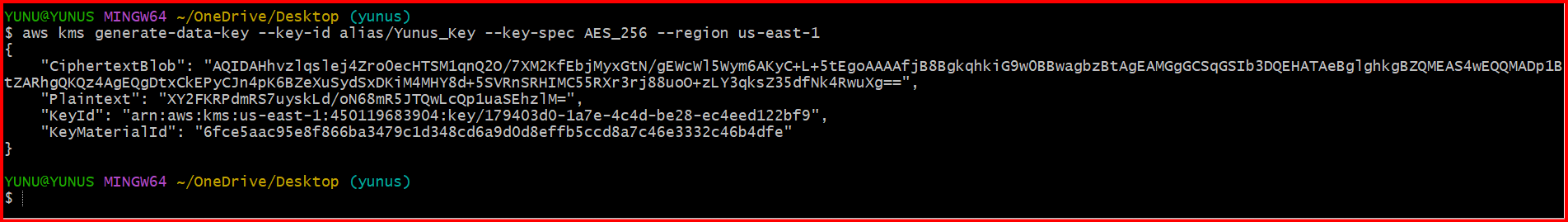
1. Open gitbash or any cli, creating a file with my aws accounts passwords or credentials



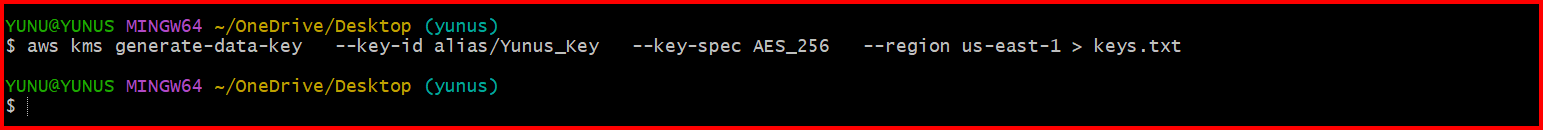
Configure the AWS



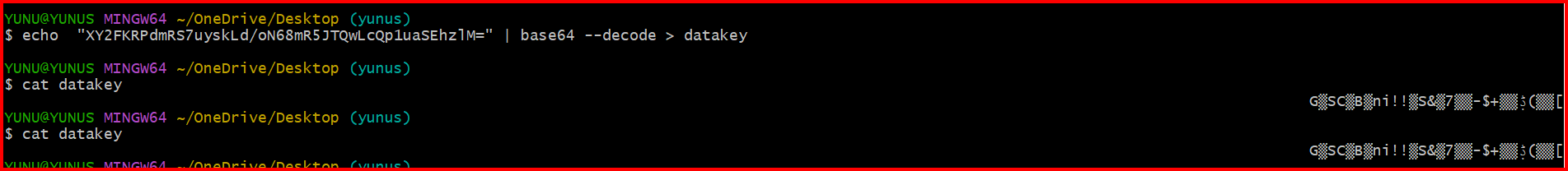
**aws kms generate-data-key --key-id alias/Yunus\_key --key-spec AES\_256 --region us-east-1**

****

KMS returned:  
● Plaintext (base64): the raw 256-bit data key, encoded  
● CiphertextBlob (base64): the same data key, encrypted under your   
CMK  
● KeyId: which CMK was used  
I redirected the JSON to keys.txt for reuse:  
aws kms generate-data-key --key-id alias/Yunus\_key --key-spec AES\_256 –region us-east-1 > keys.txt

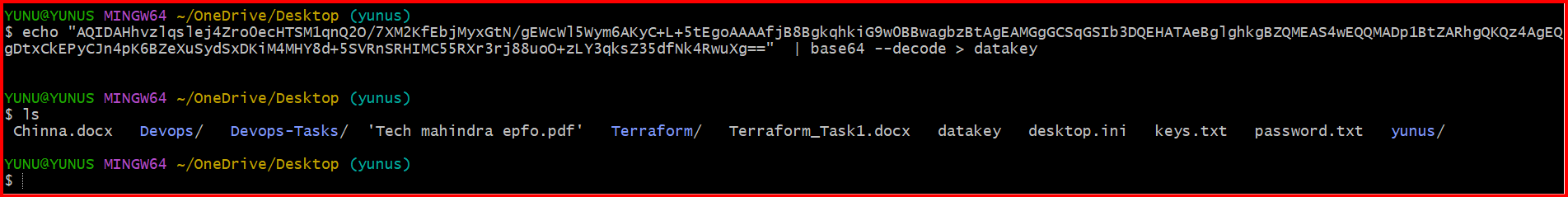
****

Create a binary file with the plaintext DEK  
● You base64-decoded the Plaintext into datakey (binary):  
● datakey looks like gibberish in cat because it’s raw bytes   
(expected)

****

Create a binary file with the encrypted DEK  
● You base64-decoded the CiphertextBlob into encrypted-  
datakey:  
● This file is safe to store next to your ciphertext. It can only be turned   
back into the plaintext key by KMS (and only if caller is authorized)

Echo “copy the ciphertextbob” | base64 --decode > encrypted-datakey



****