Security in the cloud

Assignment-2

KMS

Assignment Brief

|  |  |
| --- | --- |
| Student Name/ID Number | Yazan Atary / 22034818 |
| **Course Title** | **Security in the cloud** |
| Academic Year | 2023/24 |
| **Assignment Title** | **KMS** |
| Issue Date | **4-21-2024** |
| Submission Date | **4-21-2024** |
| IV Name & Date |  |

|  |
| --- |
| **Submission Format** |
| The submission is in this form as clear screen shot under every question.  You can use this website to add your screen shots to the PDF file : <https://www.ilovepdf.com/blog/how-to-insert-an-image-into-pdf> |

1

AWS Key Management Service (KMS)

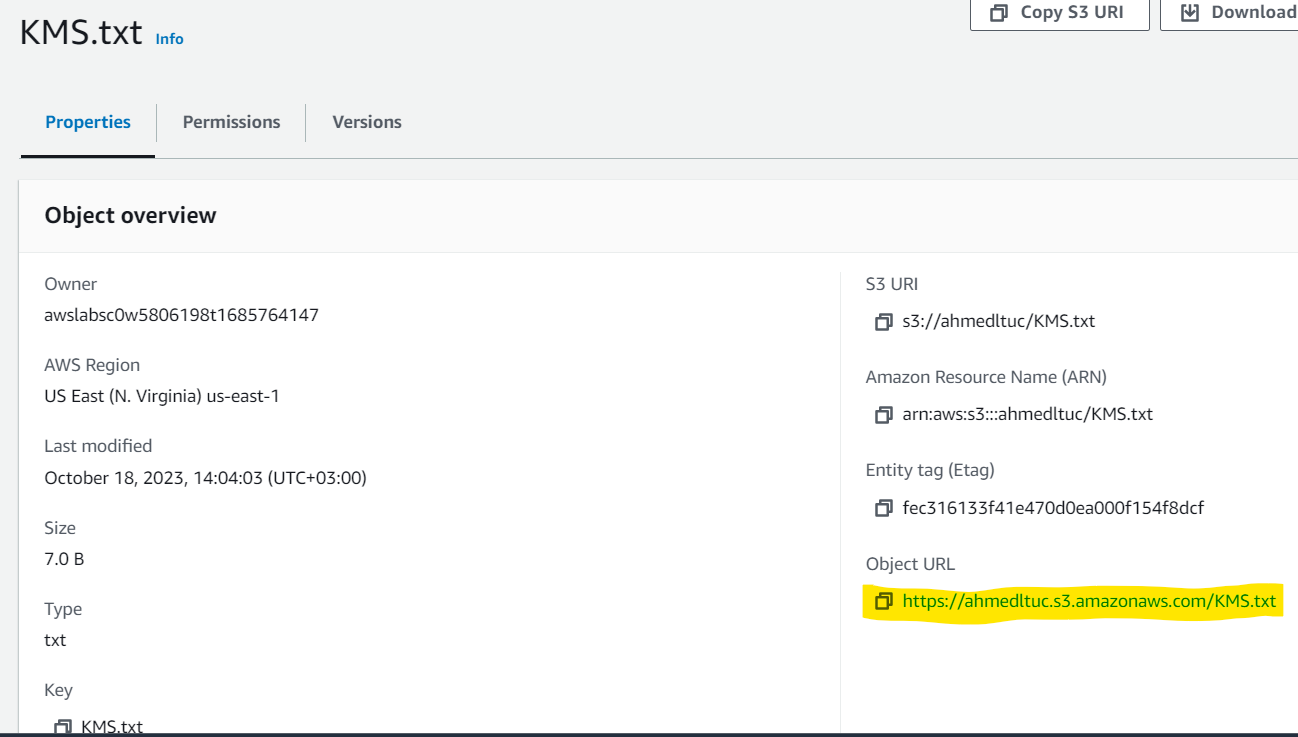
(Managed service that makes it easy for you to create and manage keys and control the use of encryption across a wide range of AWS services. KMS is a secure and resilient service that uses FIPS 140-2 validated hardware security modules to isolate and protect your keys).

1. Create S3 bucket on AWS

* Go to S3 service, then create bucket.
* Name the bucket, ACLs enabled.
* Unclick “block all public access, check “I acknowledge that the current settings might result in this bucket and the objects within becoming public”.
* Bucket versioning “enable”.
* Create bucket.
* Open your bucket, upload, add files, and then add your files.
* Go to properties inside your uploaded file.
* Inside your bucket , permissions , bucket policy , edit ,
* Copy ARN, press on “policy generator”.
* Select type of policy “S3 bucket policy”.
* Select Effect “allow”, and fill principal “\*”.
* from Actions choose “Get object”.(to allow object permission)
* Paste the copied URL on Amazon Resource Name (ARN).
* Press on “add statement” then press on “Generate Policy”.
* Copy the “Policy JSON Document “code.
* Go to edit bucket policy again then paste the copied “Policy JSON Document “code inside it, and **“add /\* beside the name of your bucket inside JSON Document Code** “to allow all object in this bucket”.

As shown below

* Save changes.
* Inside your uploaded file, Open URL object, it will open now.



Share your screen shot

A screenshot of a computer

Description automatically generated

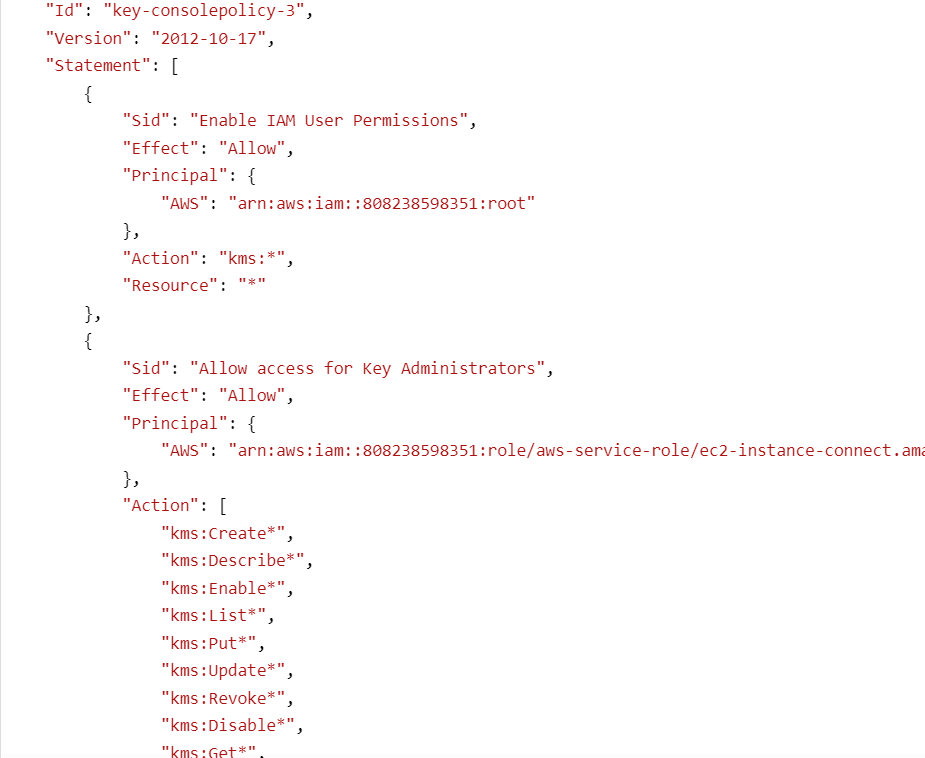
A screenshot of a computer

Description automatically generated

2

1. Create a key on AWS:

* Step1: Go to services and choose KMS.
* From the left side choose “customer managed keys”.
* Press on create key.
* Choose symmetric.
* From advanced options, choose key material origin “KMS” then next.
* Step2: give a name, then next.
* Step3: choose the required key administration as “EC2instance” then next.
* Step4: Define key usage permissions as “EC2instance” then next.
* Scroll down till reach key policy, as shown, you can read and check the main commands and modify it based on your needs and requests, then finish.



3

* Open your created key, you can add another key administrations inside it, modify the policies.

Share your screen shot

A screenshot of a computer

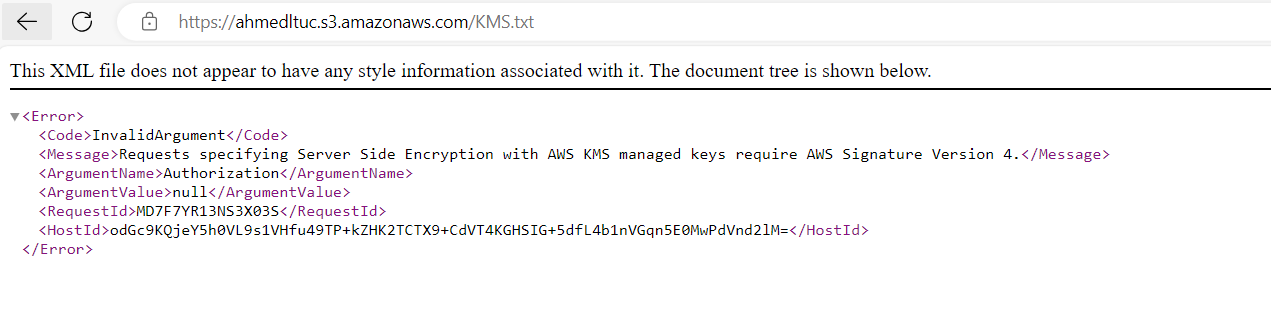
Description automatically generated

A screenshot of a computer

Description automatically generated

1. Encrypt your file :

* To encrypt this file: go to your file, from “object actions” edit server side encryption, from Encryption settings, choose “Override bucket settings for default encryption”.
* From Encryption type, choose “Server-side encryption with AWS Key Management Service keys (SSE-KMS)”.
* From AWS KMS key, Choose from your AWS KMS keys, choose your Available AWS KMS keys.
* Save changes, that means your file encrypted now, you can copy your object URL on browser, it will show that your file encrypted by your key as shown.



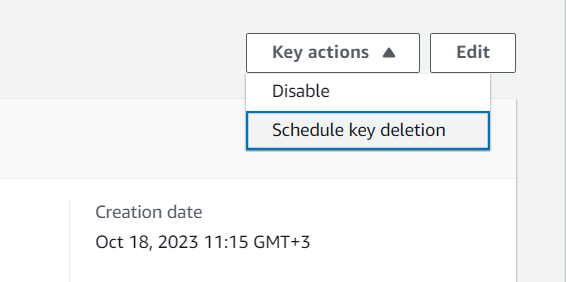
Share your screen shot

A screen shot of a computer

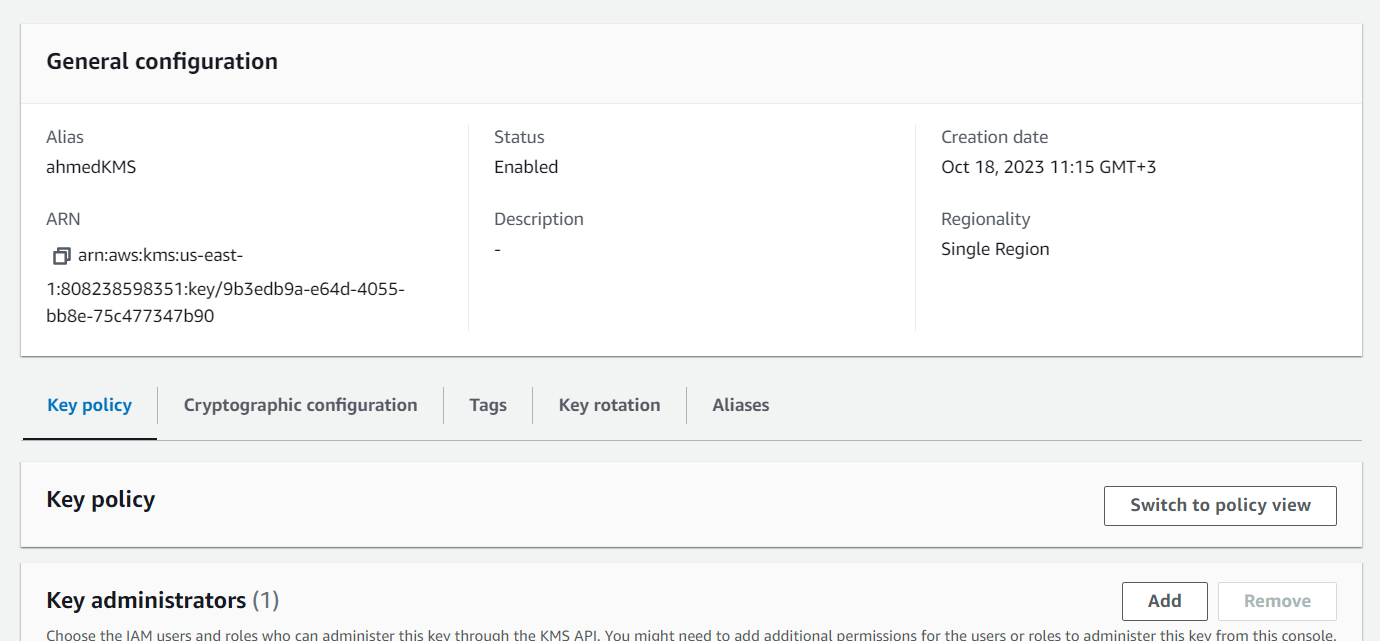
Description automatically generated

1. Delete your key :

* You can delete it from “key actions”, go to KMS then “schedule key deletion”,
* Make waiting period 7 days, then confirm deletion, then press “schedule deletion”.



5



Share your screen shot

A screenshot of a computer

Description automatically generated

6