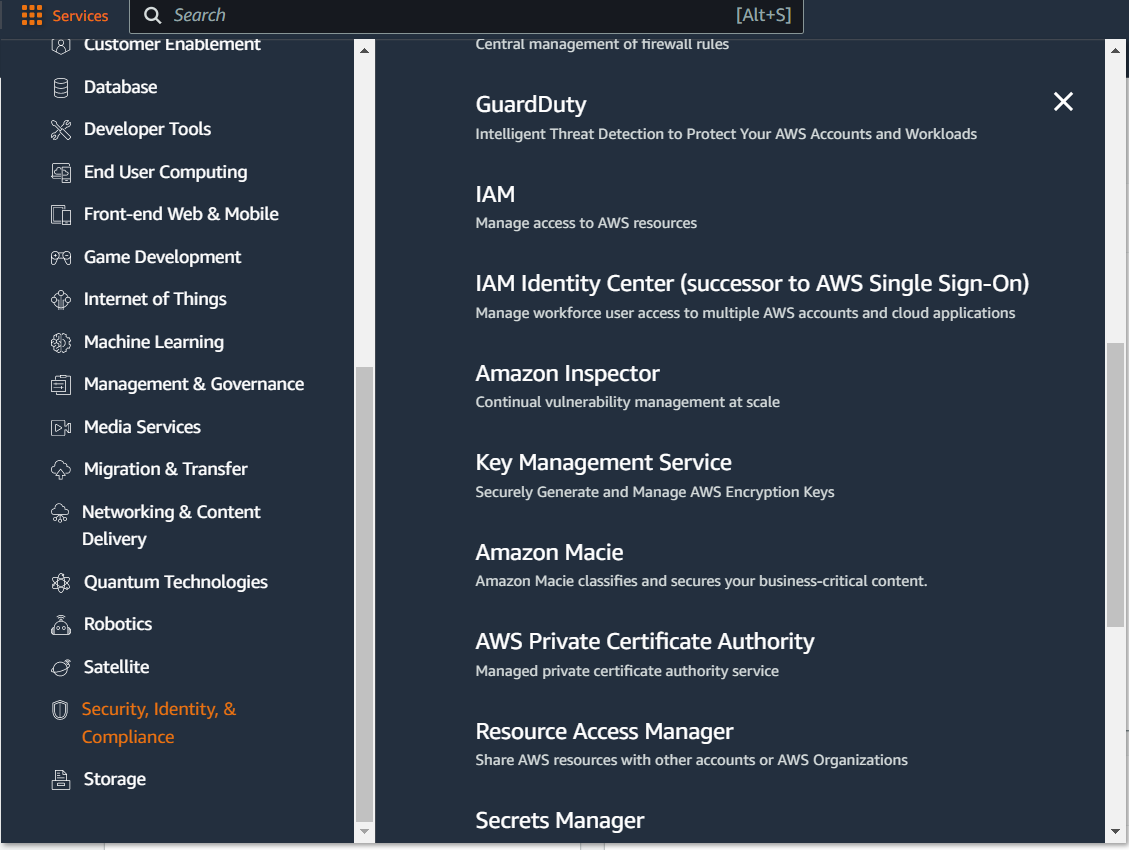
**Introduction to AWS Key Management Service**

In this lab, we will cover the following

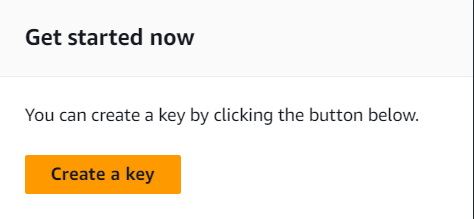
* Create an Encryption Key.
* Create an S3 bucket with CloudTrail logging functions.
* Encrypt data stored in a S3 bucket using an encryption key.
* Monitoring encryption key usage using CloudTrail.
* Manage encryption keys for users and roles.

**1. Create an Encryption Key.**

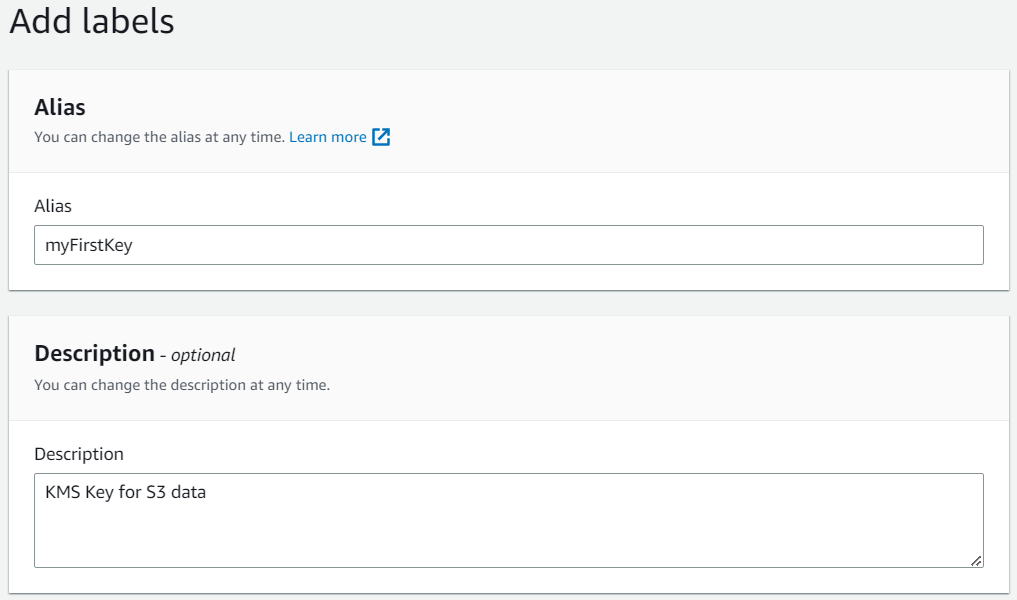
- we start off by navigating to the top left corner of Services -> scroll down to Security, Identity, & Compliance and select Key Management Service:



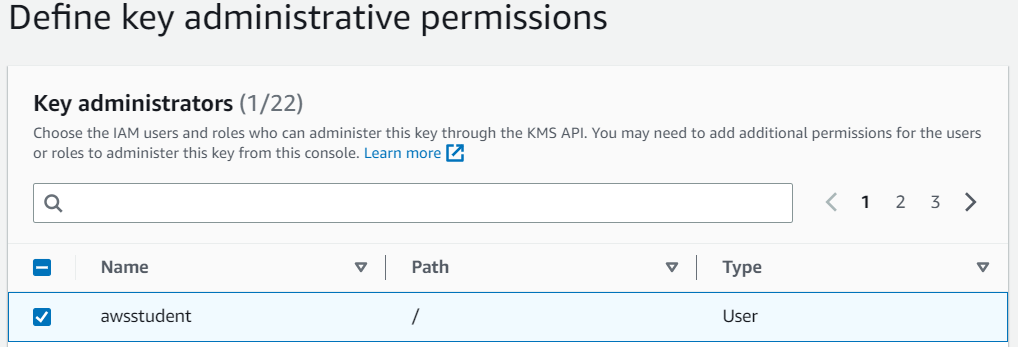
- on the next screen -> Create a key:

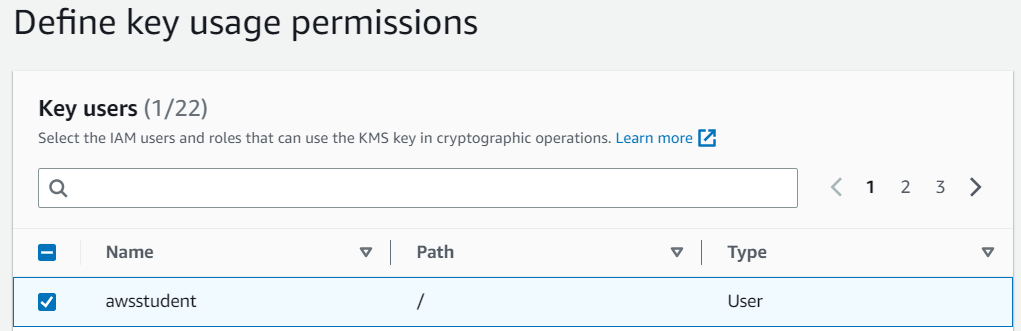


- we add some labels:



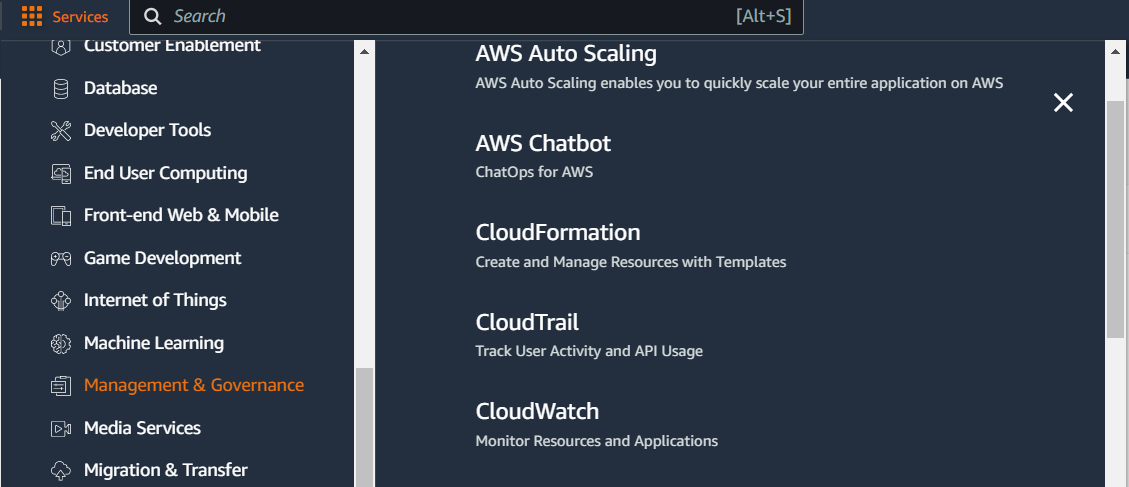
- on the next page, we add our user that we are logged in for administrative permissions and usage permissions:



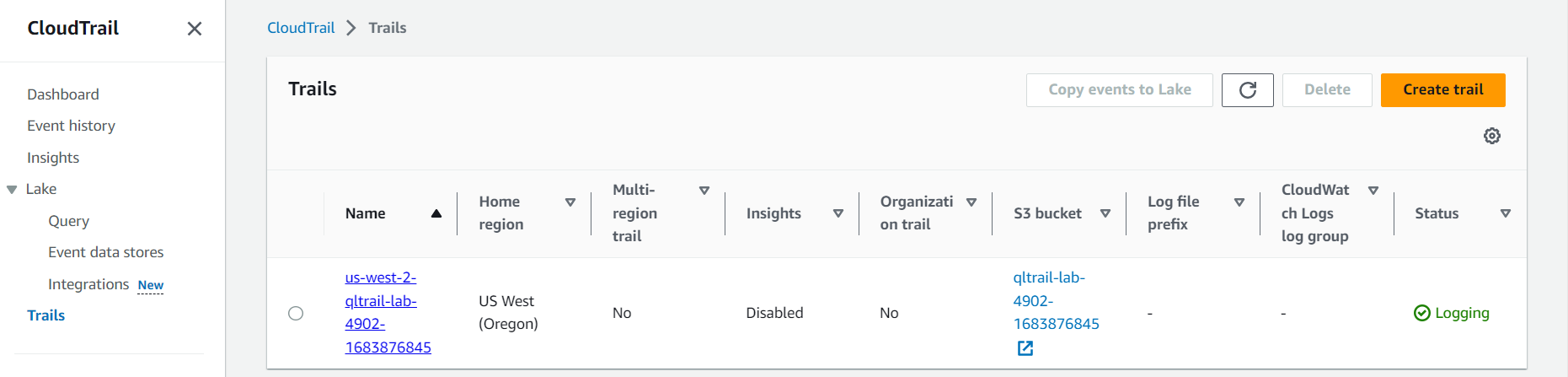


- on the next page, review the policy and click Finish. Copy the Key ID on the final screen that will show up after clicking Finish.

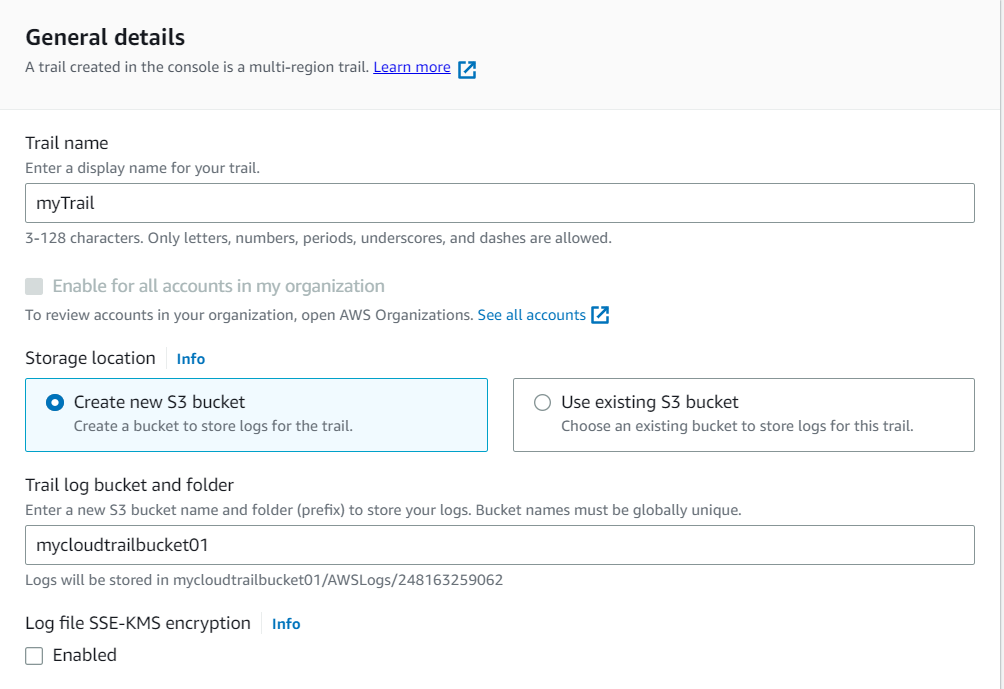
**2. Configure CloudTrail to Store Logs In An S3 Bucket.**

- from Services again -> Management and Governance, and click CloudTrail:

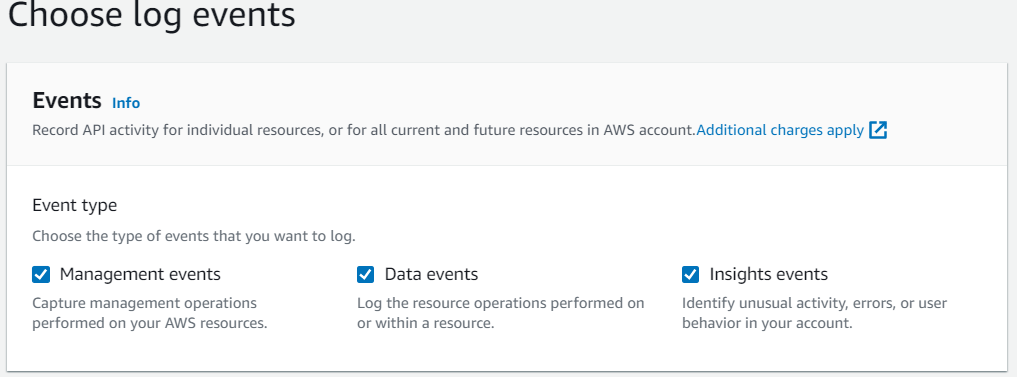
- from the left side panel, click and Trails -> Create trail:

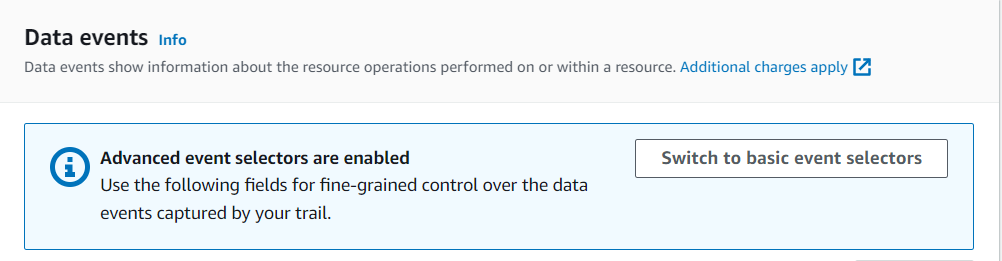


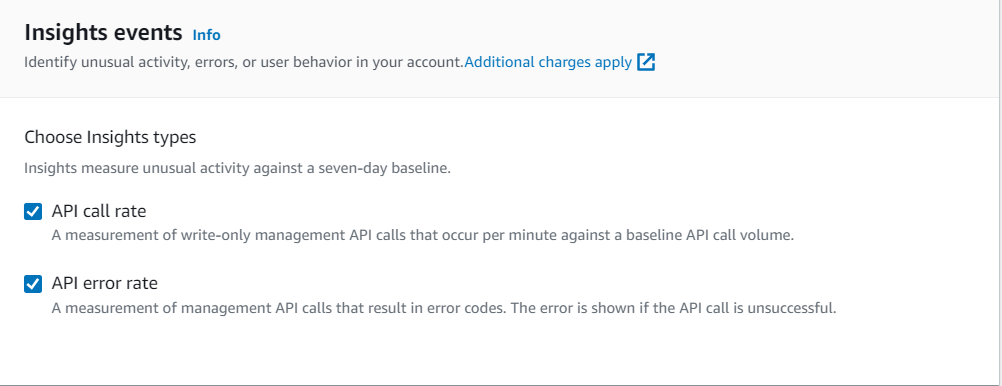
- define some settings and click Next:



- a bit more settings, and on the last page click Create Trail:



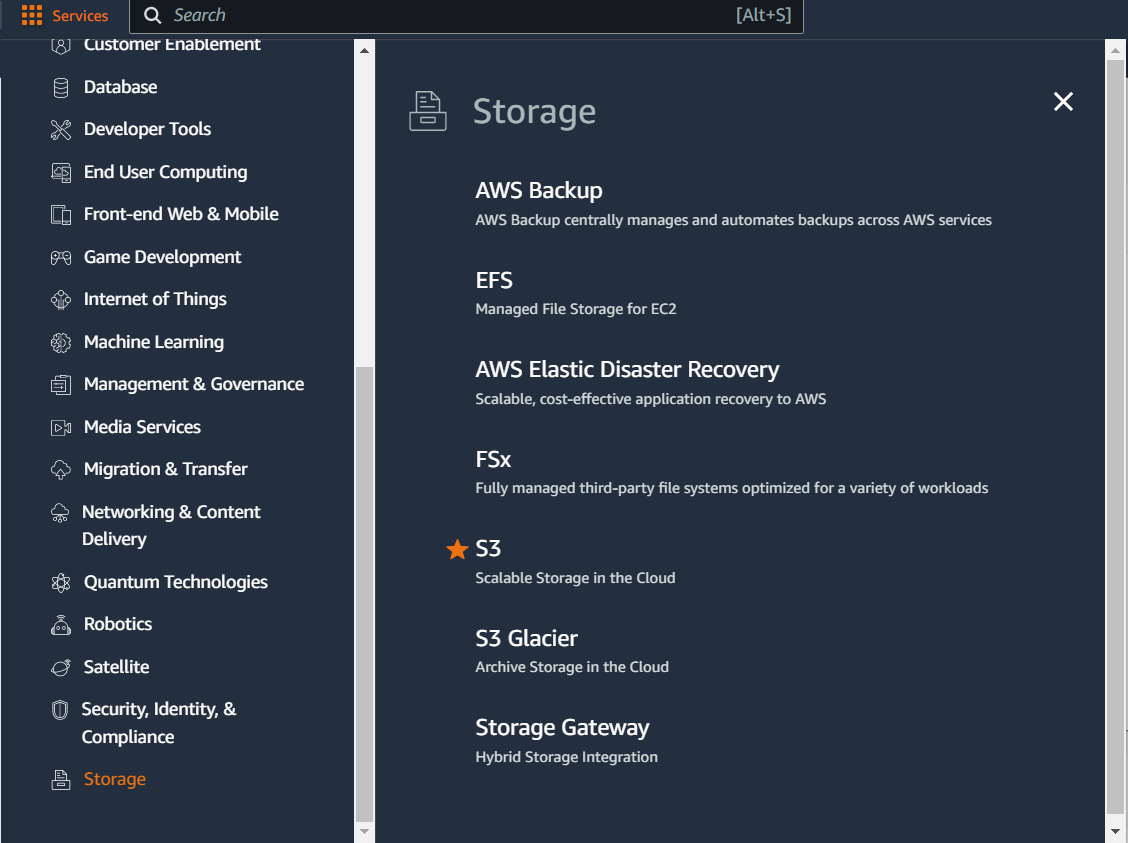


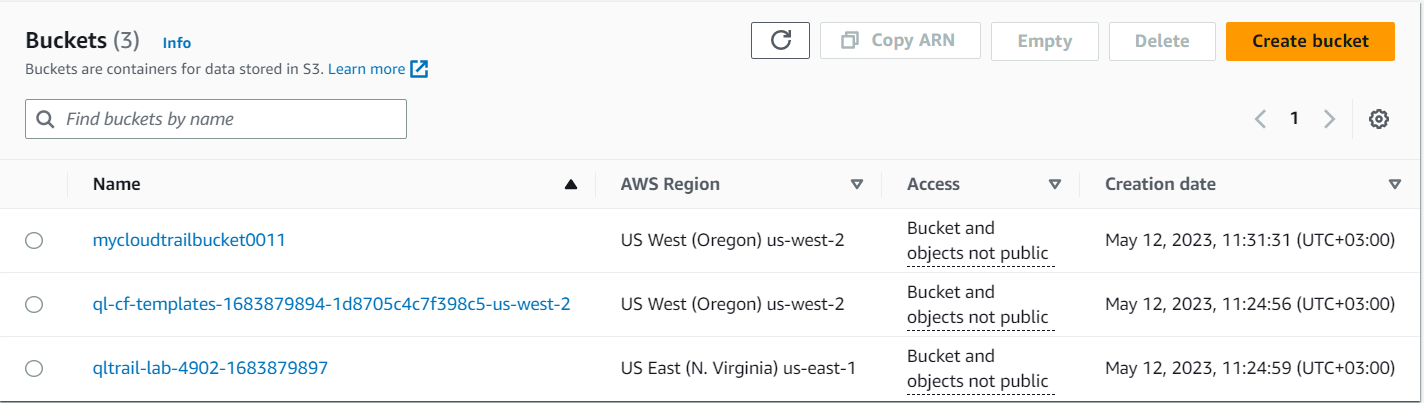


- I renamed the Trail to myTrail1 and bucket name to – mycloudtrailbucket0011, as the previous default one already existed.

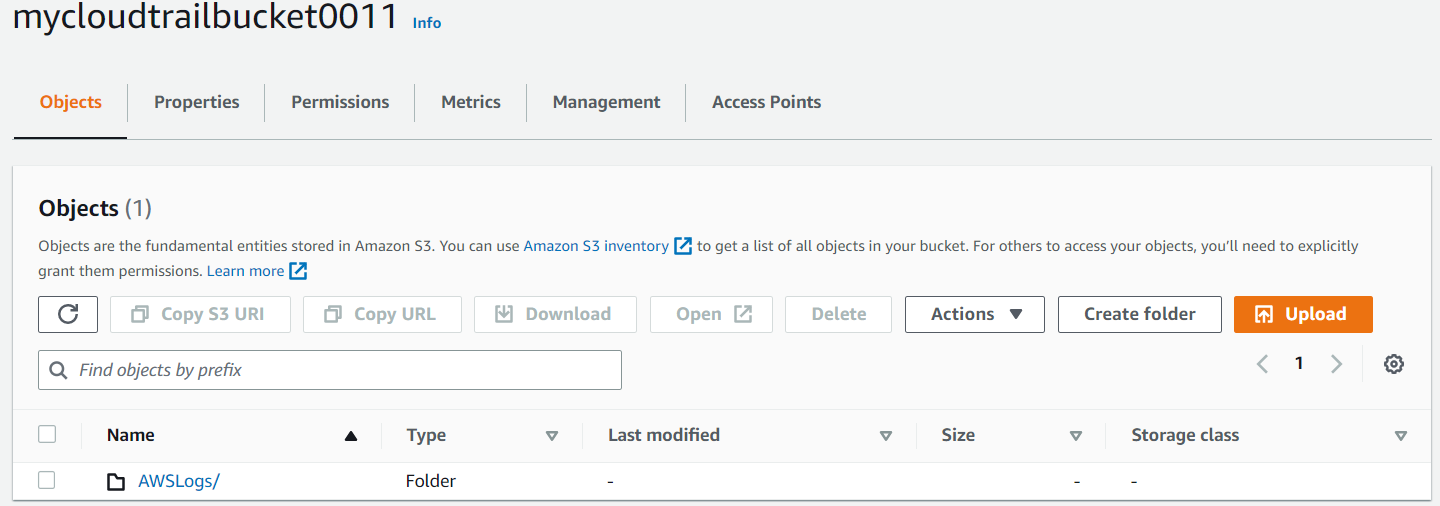
**3. Upload an Image to Your S3 Bucket And Encrypt It.**

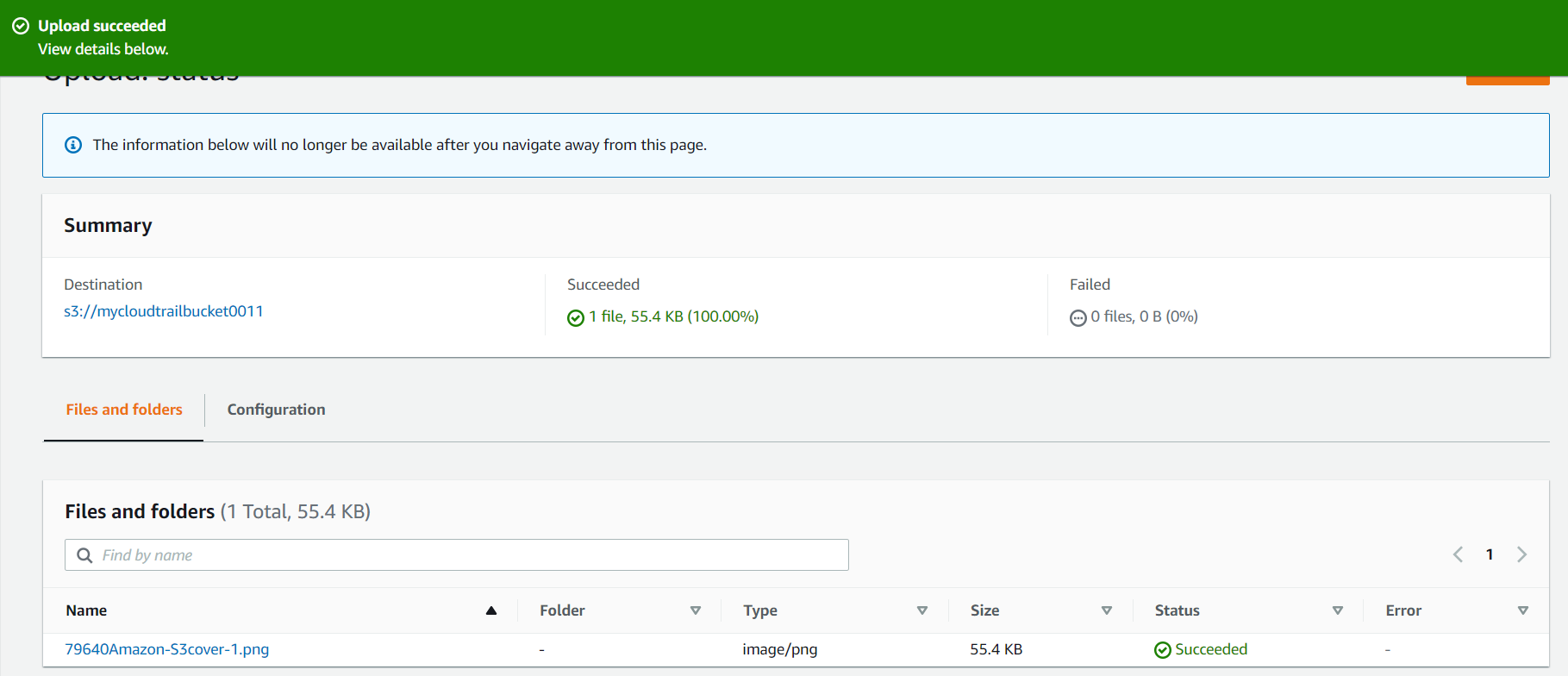
- from Services -> Storage -> select S3:



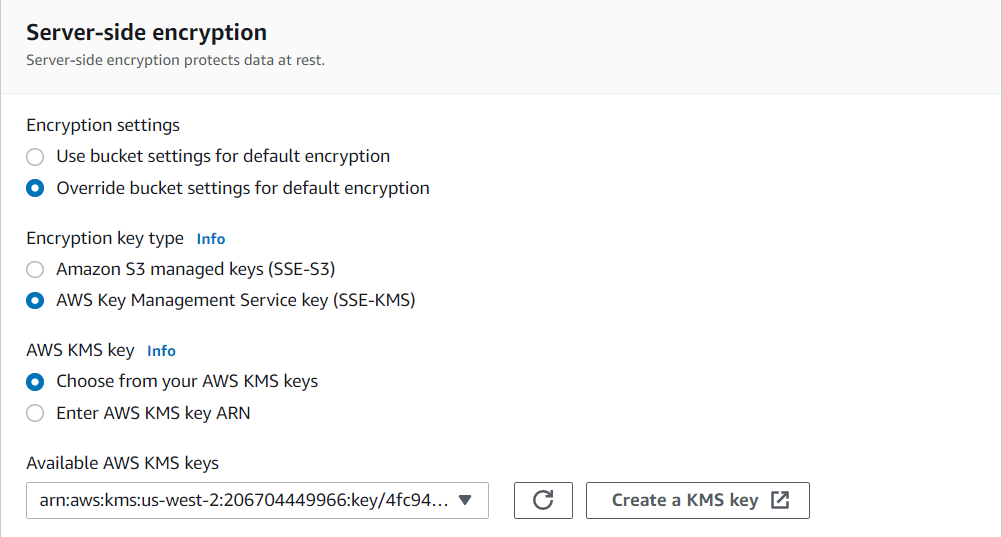
- select our mycloudtrailbucket0011:  


- and upload our random screenshot:



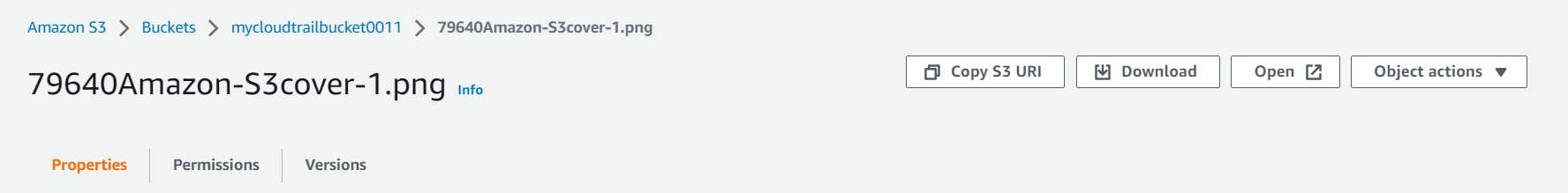


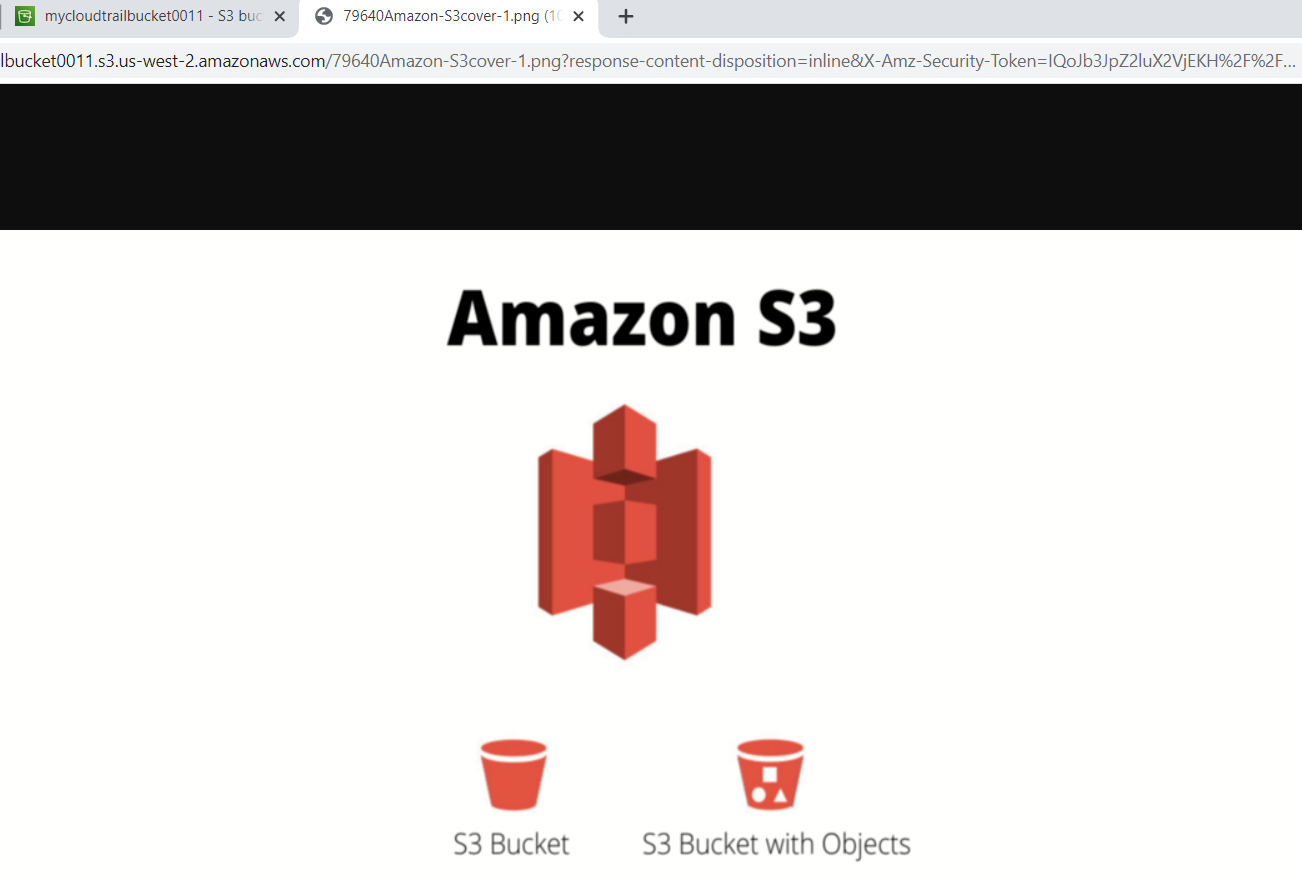
- we select our screenshot, and scroll down to Server-side encryption settings and specify the following and save the settings:



**4. Access The Encrypted Image.**

- we can now try accessing the image by selecting it and clicking Open:

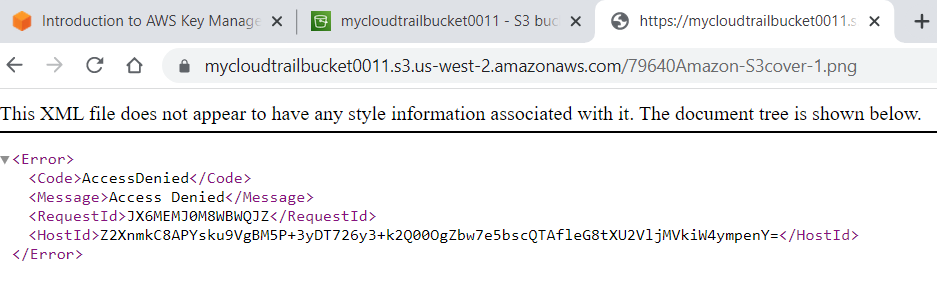




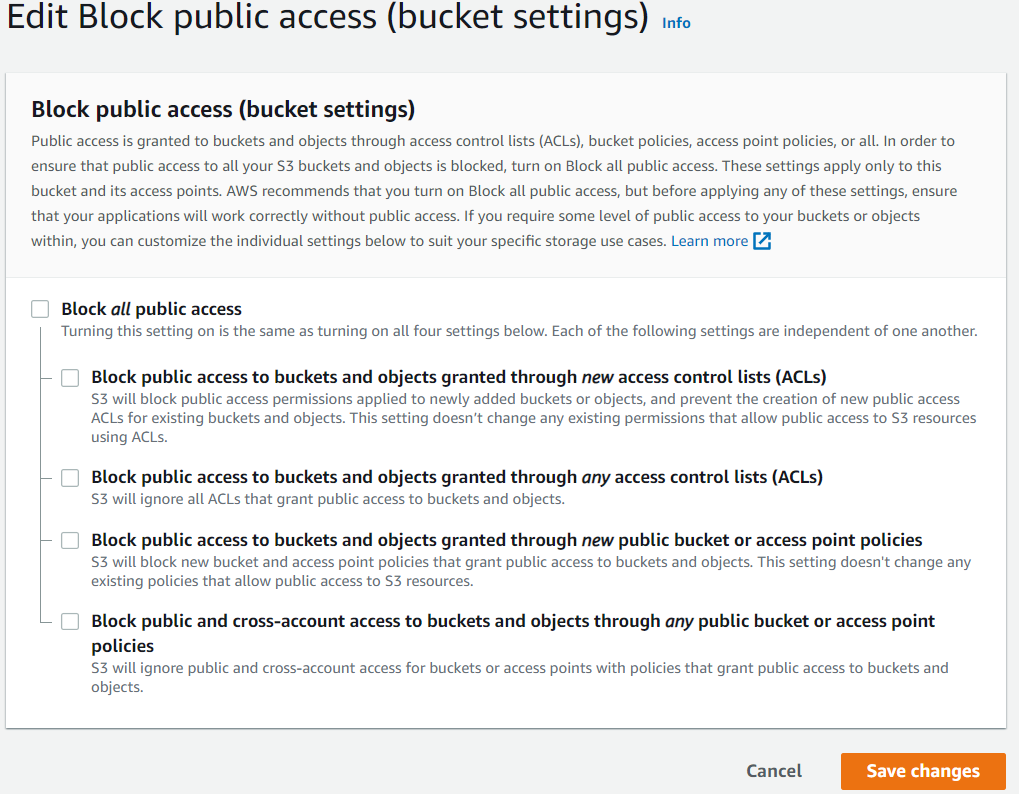
- however, if we try to access it through the object url:



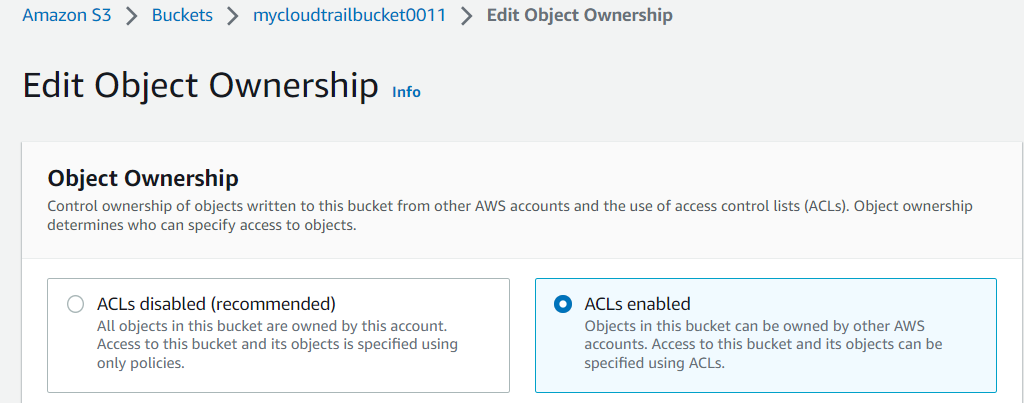
- we would receive an access denied message. This is expected, as by default public access is not allowed:



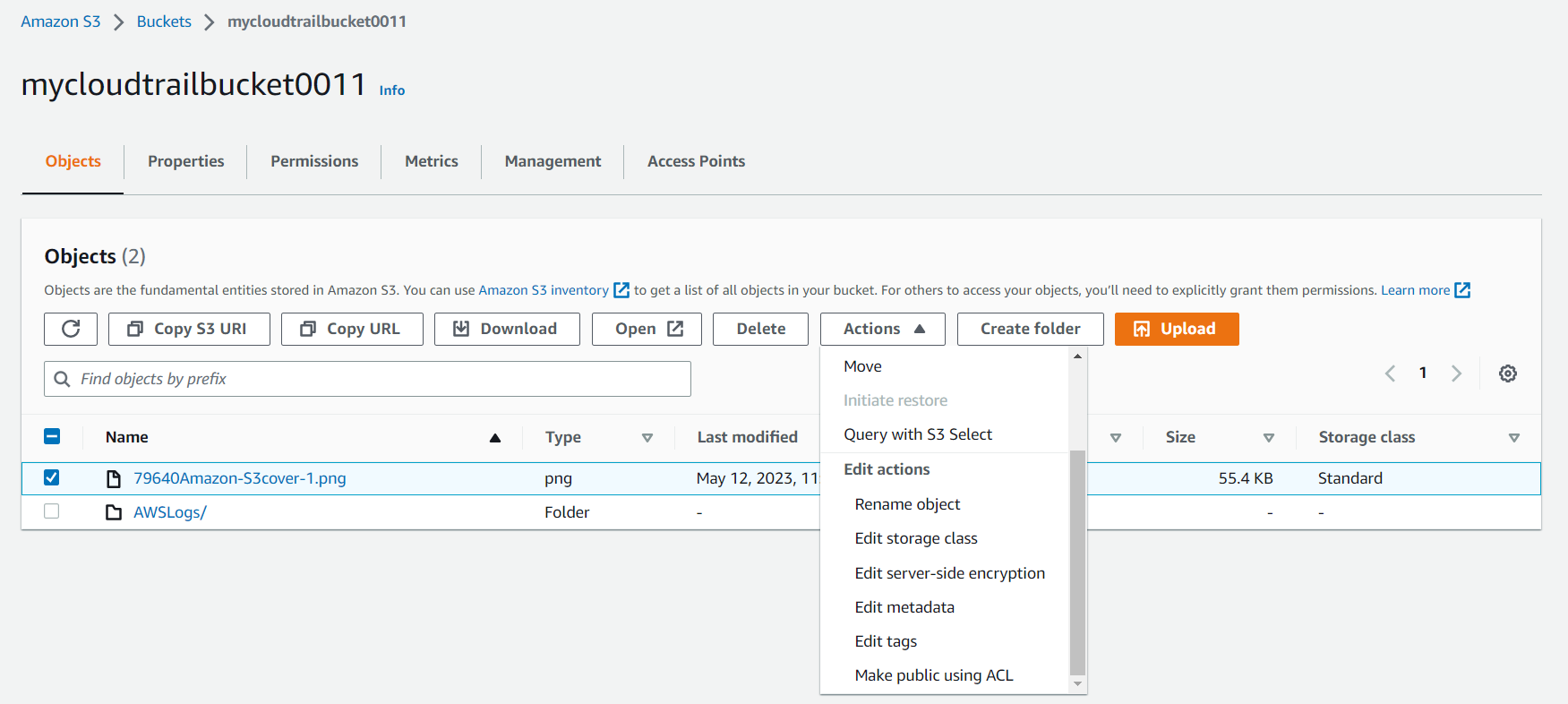
- we can edit this by selecting our bucket name -> Permissions -> and Edit Block public access:



- to enable the following setting (Make public via ACL), we first have to enable it by selecting the bucket name -> scroll down to Object Ownership -> Edit -> and ACLs enabled:

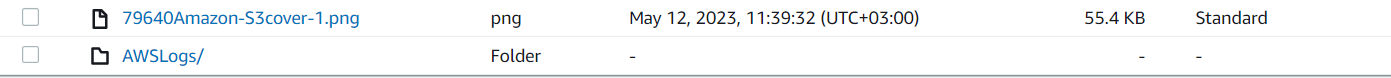


- return back to our image, select it -> Actions -> Make public via ACL:

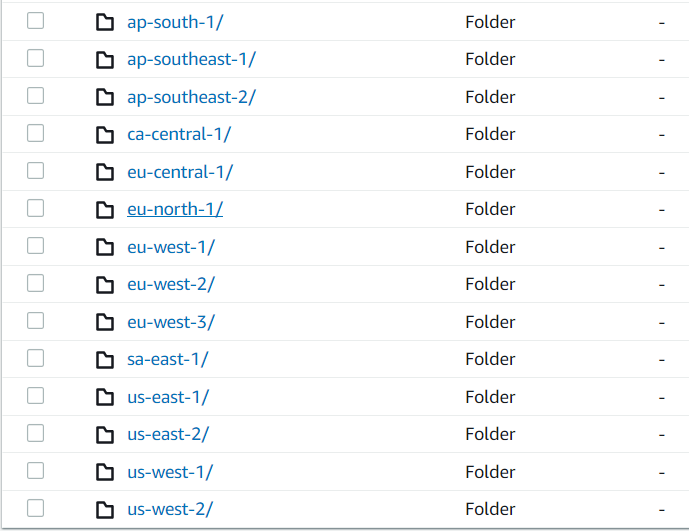


- and because the image is encrypted, we still cannot view it using the public link.

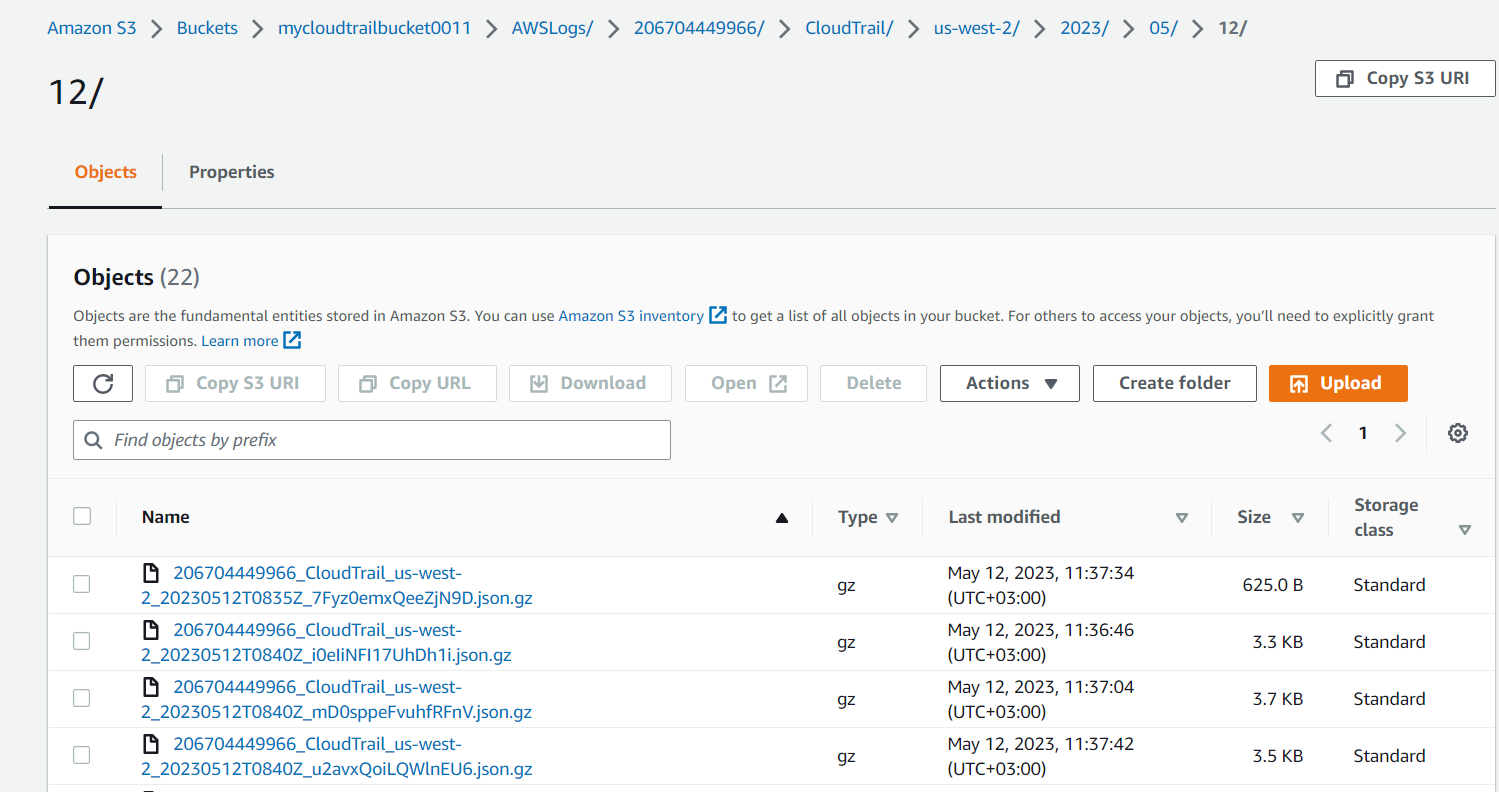
**5. Monitor KMS Activity Using CloudTrail Logs.**

- back to our bucket -> AWSLogs/ folder:  
  


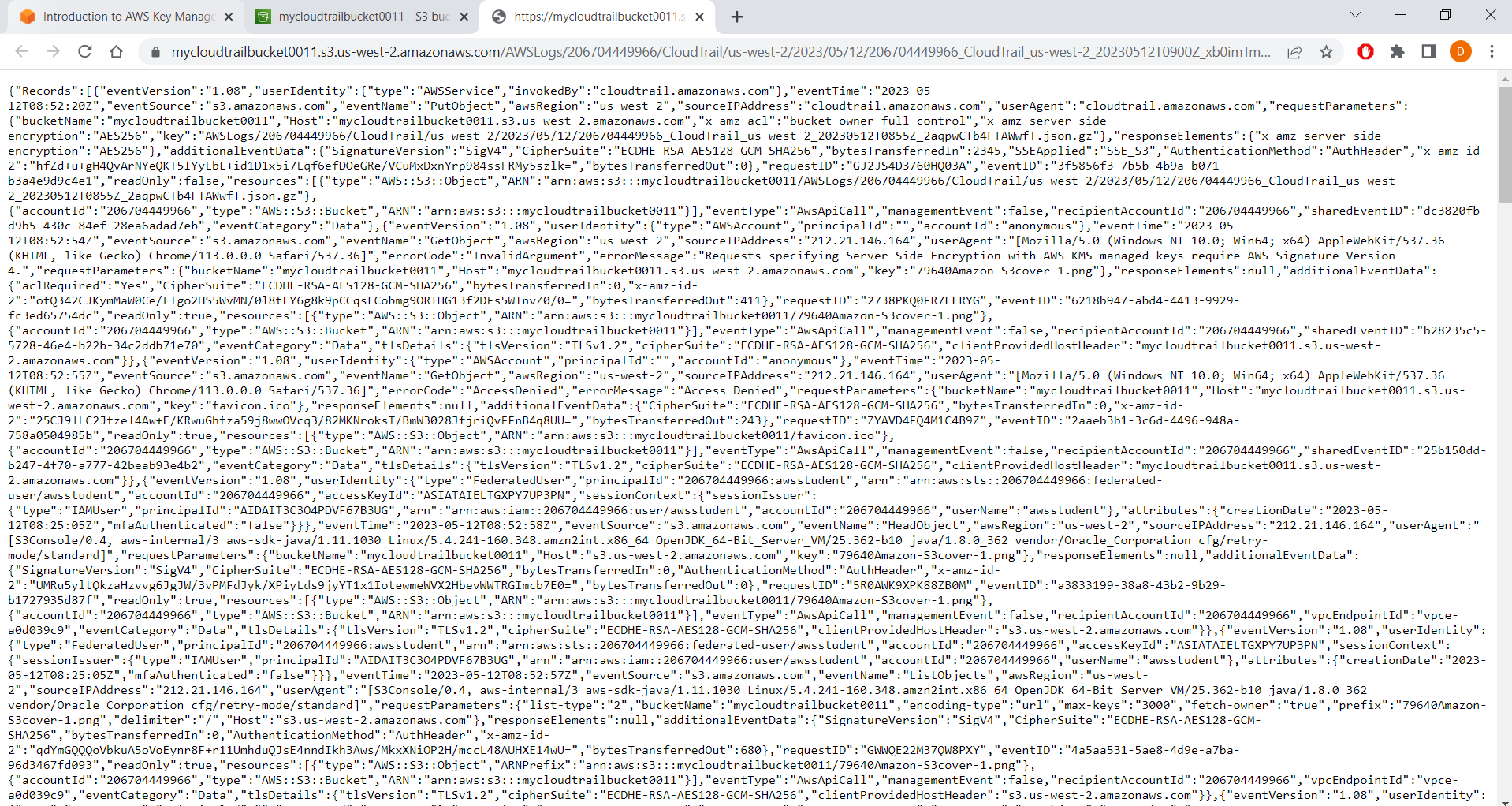
- go through the folders and select the region where we created our bucket (mine was us-west-2):



- going through the folders again, we reach the log files:



- we can select any of the log files -> and Open to see the actual logs (I selected the last one, not visible on the screen):  
  

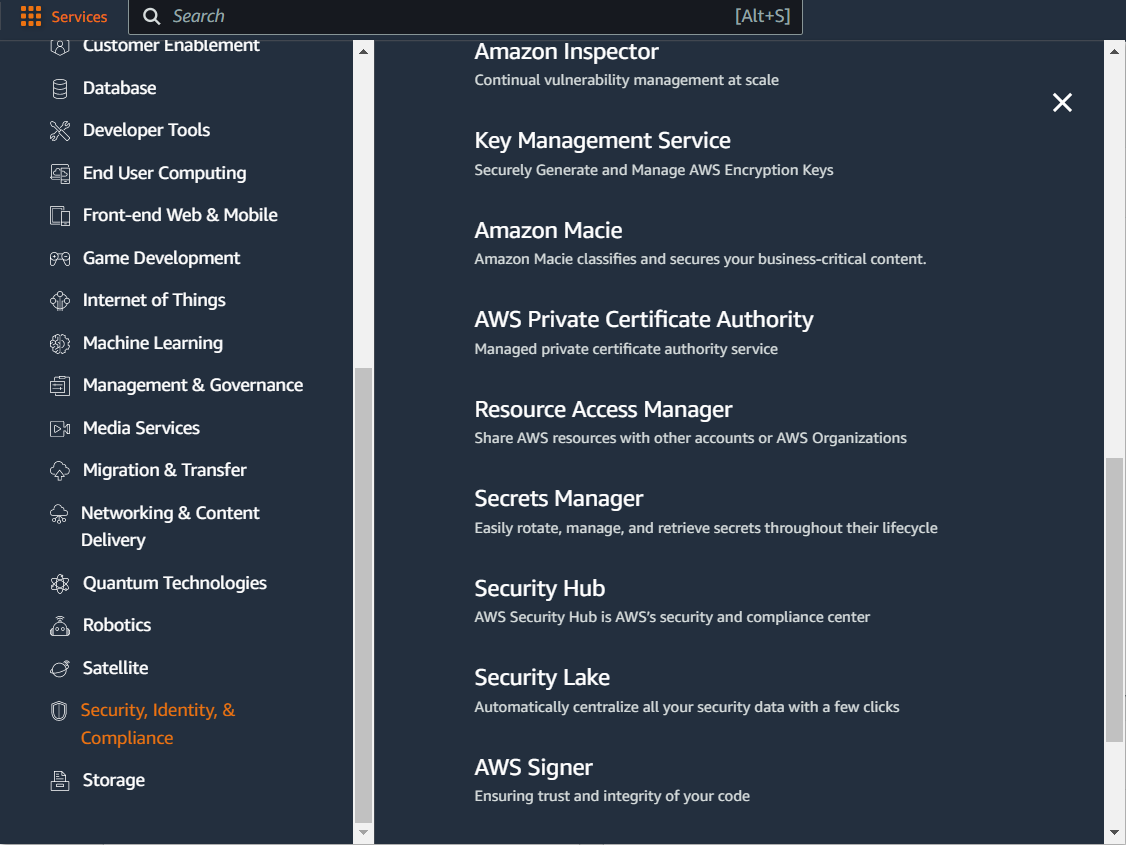



- and we can see that the name of the file we uploaded earlier is there (the encryption Key ID was not for me):

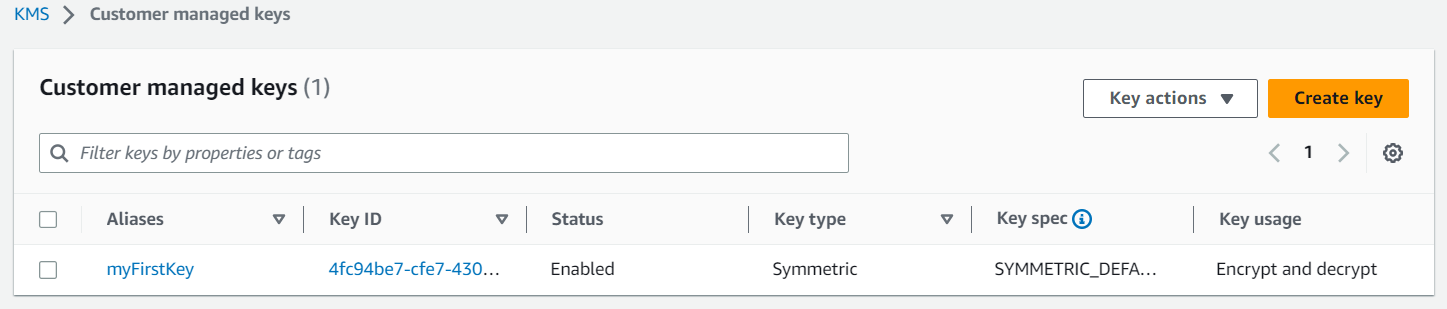


**6. Manage Encryption Keys.**

- again, in the Services -> scroll down to Security, Identity, & Compliance and select Key Management Service:

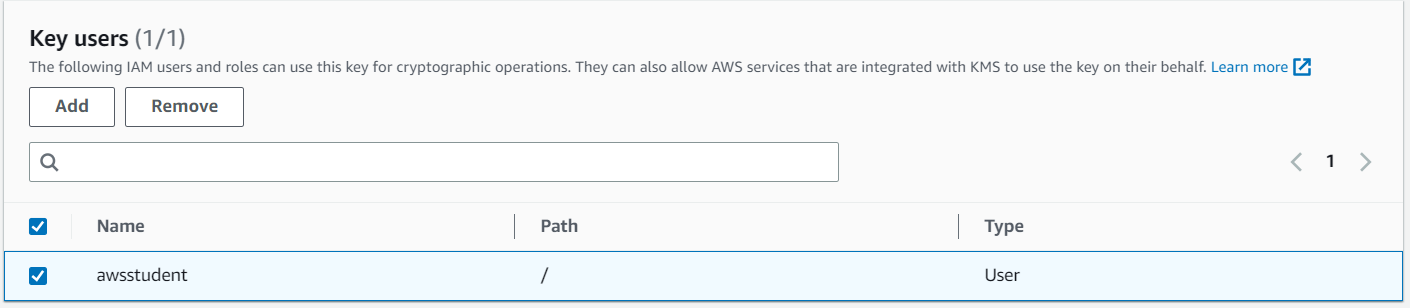


- select our key:



- here we can alter key description, Add or Remove Key Administrators and Key Users, allow external users to access the key and place the key into annual rotation.

- from the Key users section, we can remove the user or role that we are signed in with:



- from the same section, if we press Add, we can add our user again:

