Delete MFA

# generate root access keys

aws configure --profile root-mfa-delete-demo

# enable mfa delete

aws s3api put-bucket-versioning --bucket {name} --versioning-configuration Status=Enabled,MFADelete=Enabled --mfa "arn-of-mfa-device mfa-code" --profile root-mfa-delete-demo

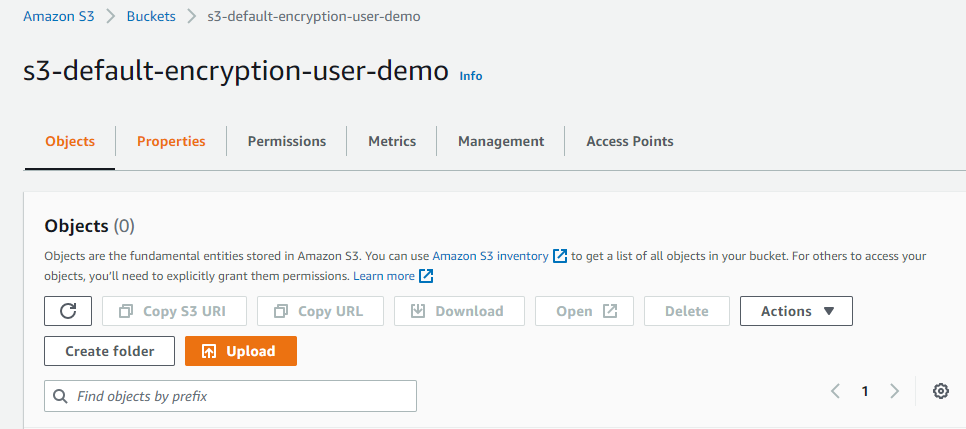
# disable mfa delete

aws s3api put-bucket-versioning --bucket {name} --versioning-configuration Status=Enabled,MFADelete=Disabled --mfa "arn-of-mfa-device mfa-code" --profile root-mfa-delete-demo

# delete the root credentials in the IAM console!!!

Default encryption

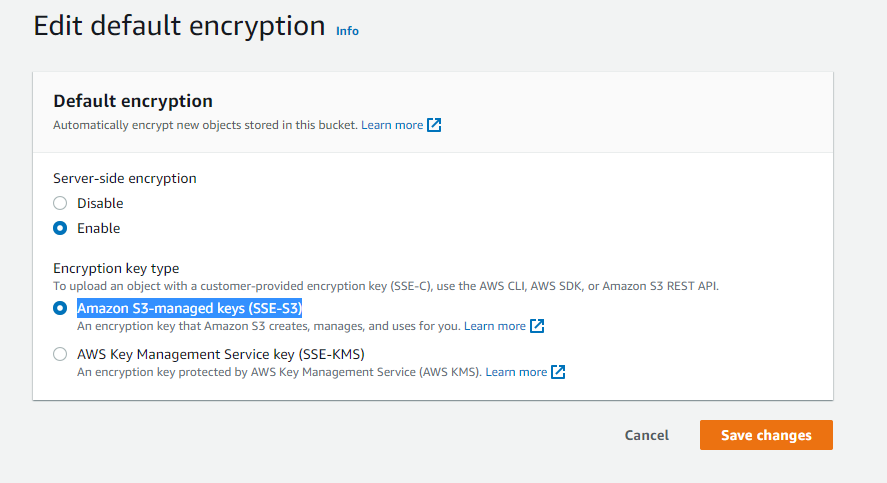
Create s3 bucket



Go to properties under bucket

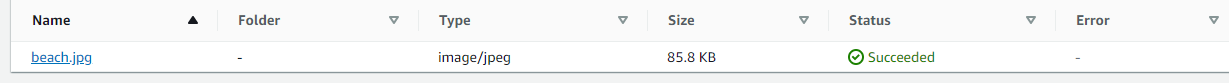
Edit default encryption





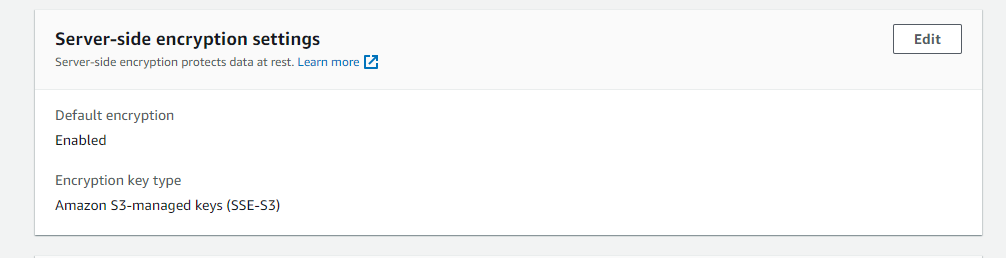
Go to Object and Add file with default

Open beach.jpg

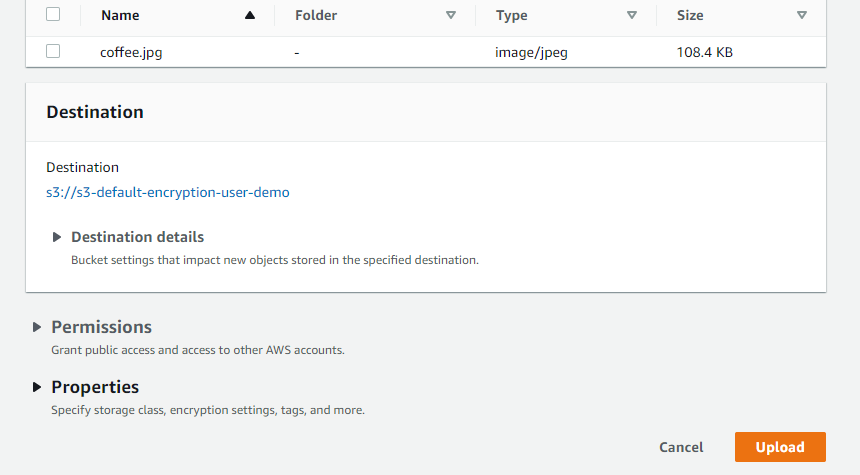


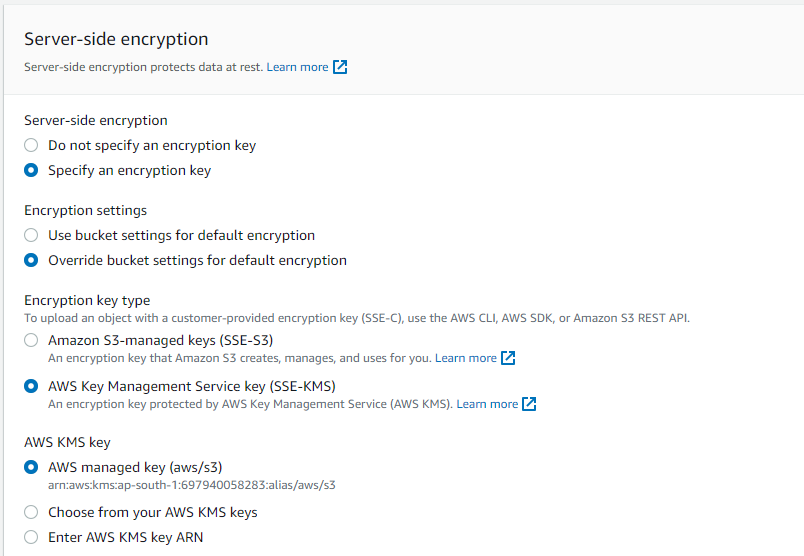
Under file properties

Add properties



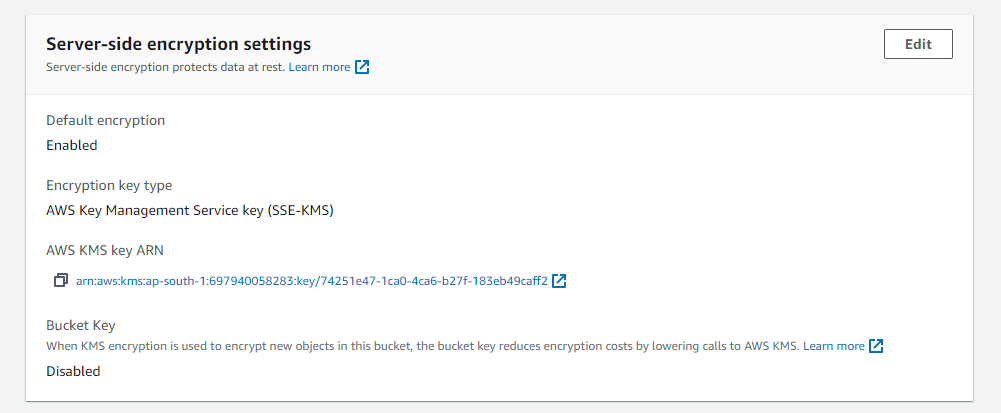
Upload another file





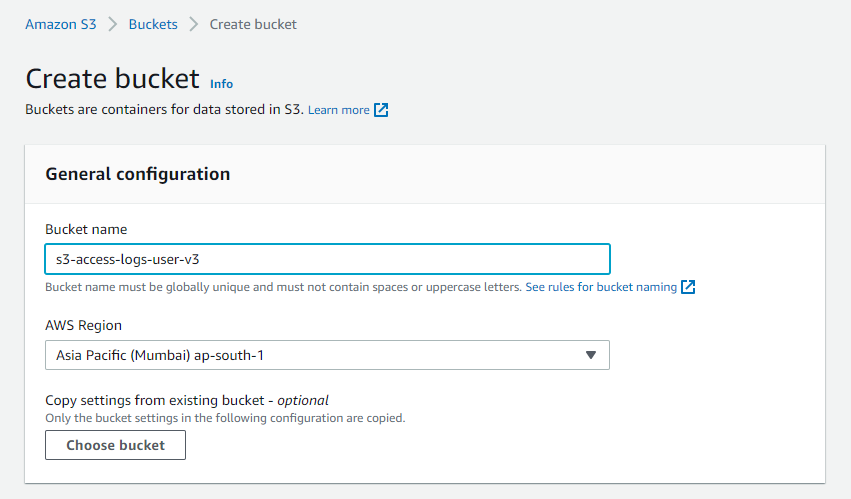
Open file

You will see



Access logs

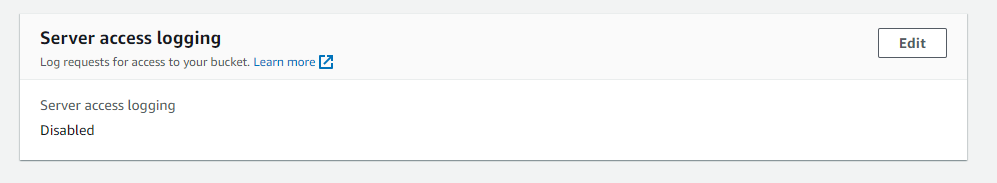
Create bucket

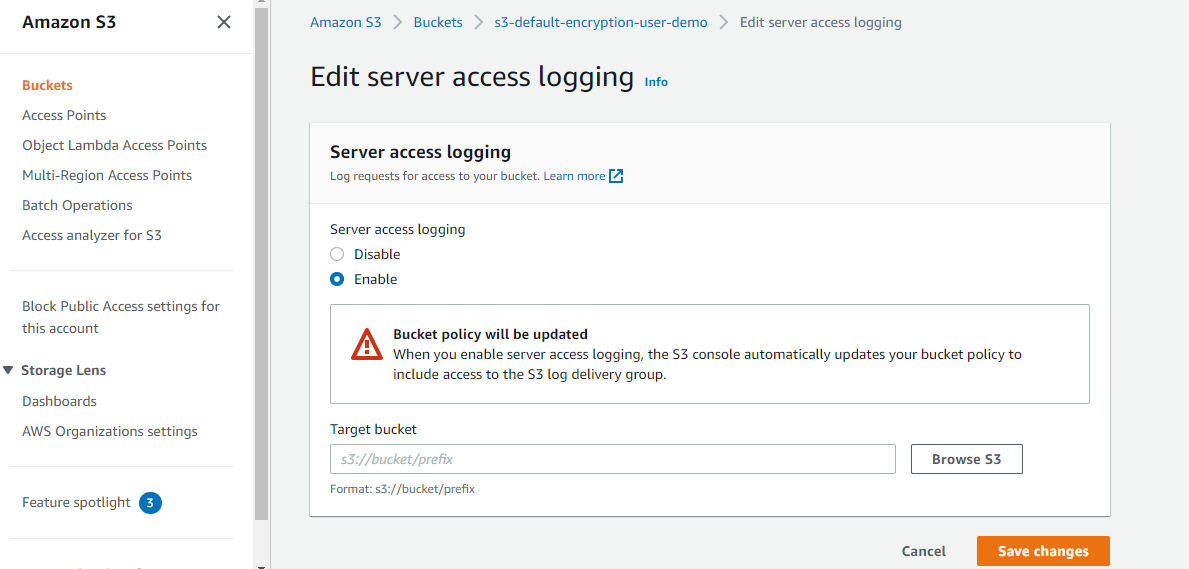


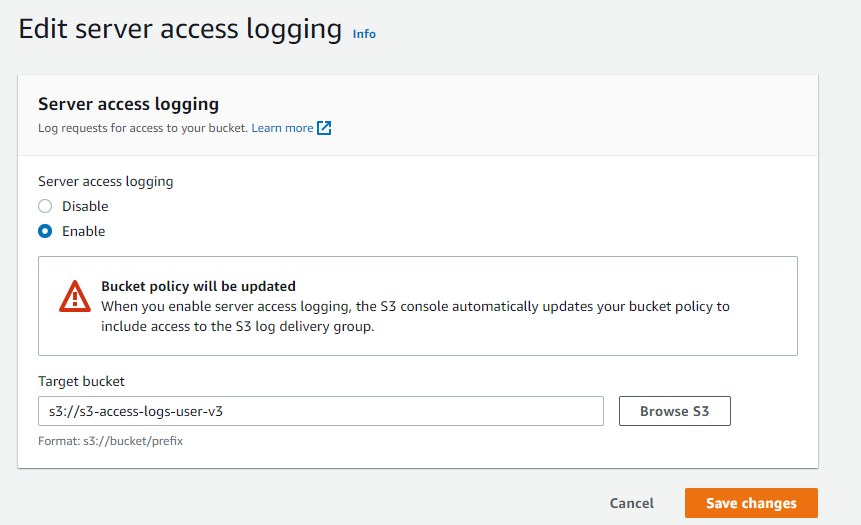
Create or use another bucket

Under properties

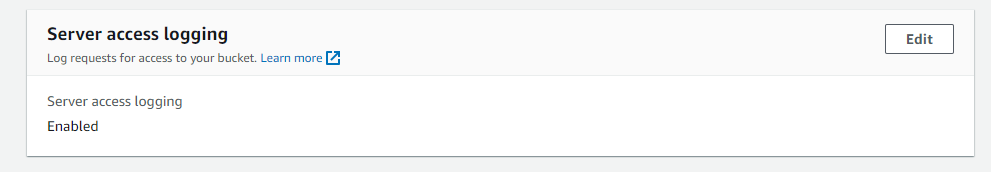
Edit server access logging



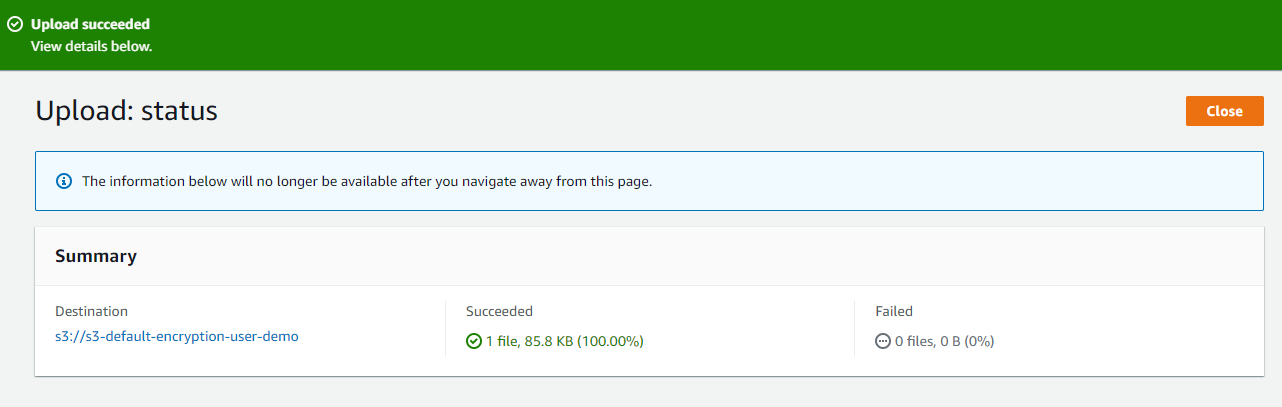




Now my s3 server is enable

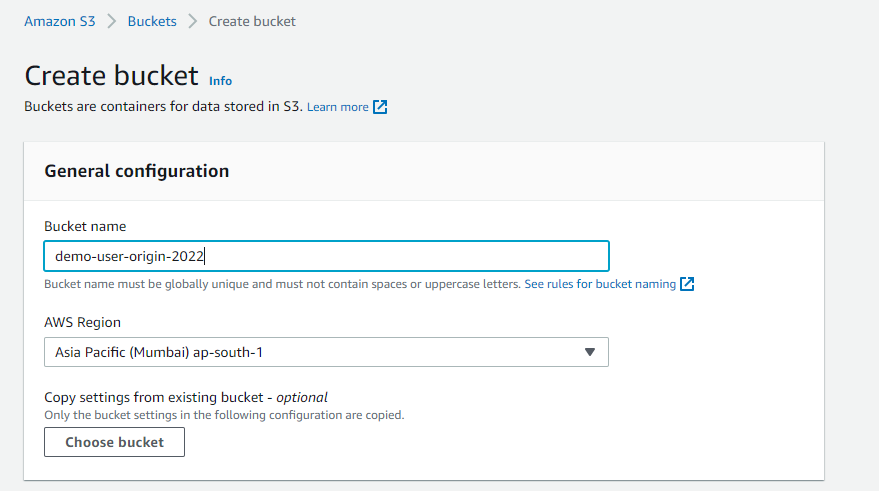


Add file on this bucket

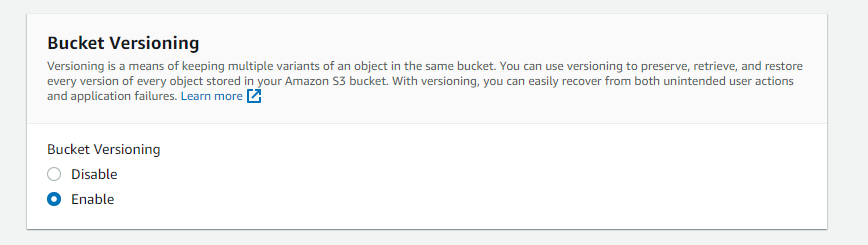


All your activities is recorded in first bucket

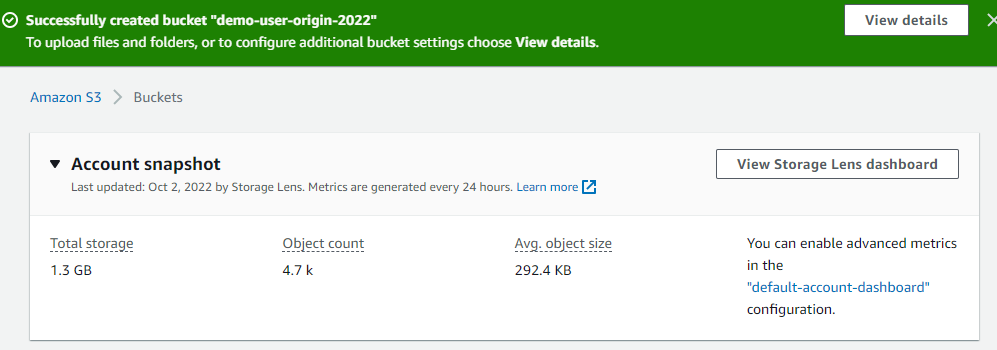
**Replication**



Enable versioning



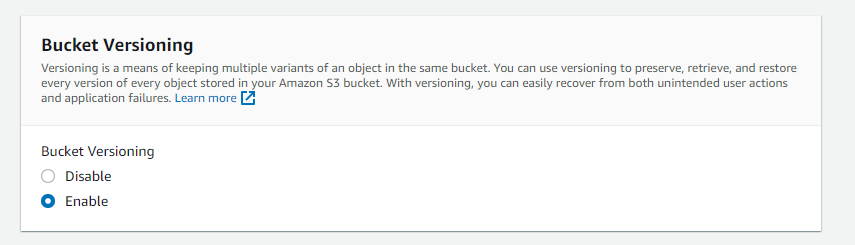
The create bucket



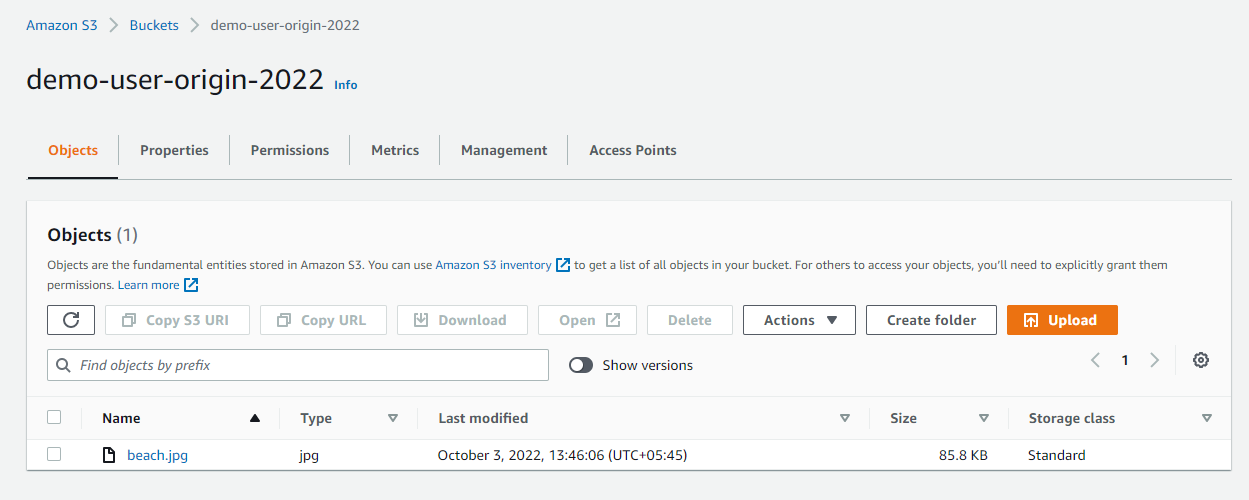
Again create a second bucket in different region



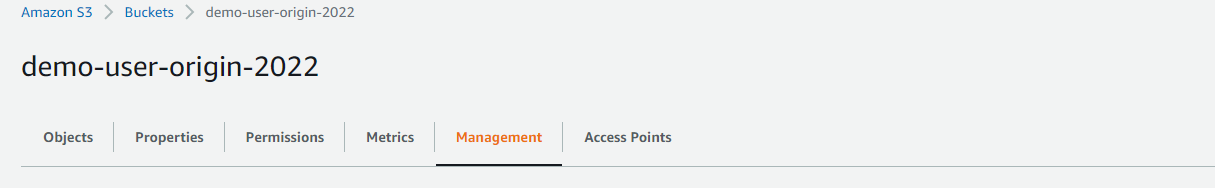
Enable region



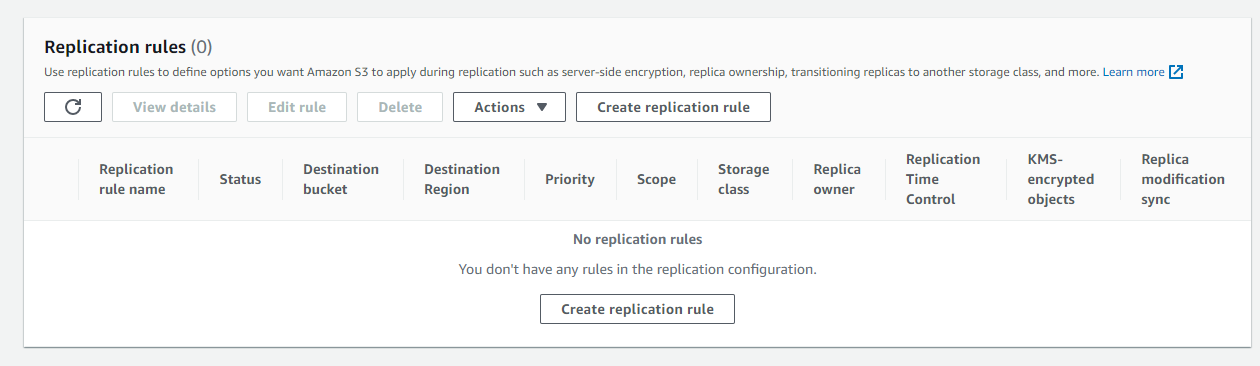
Go back to origin bucket



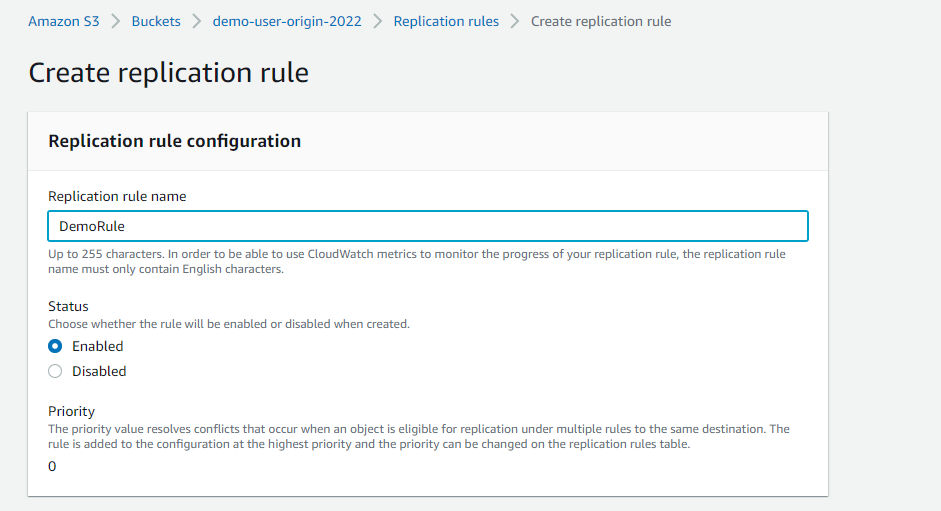
Go to management

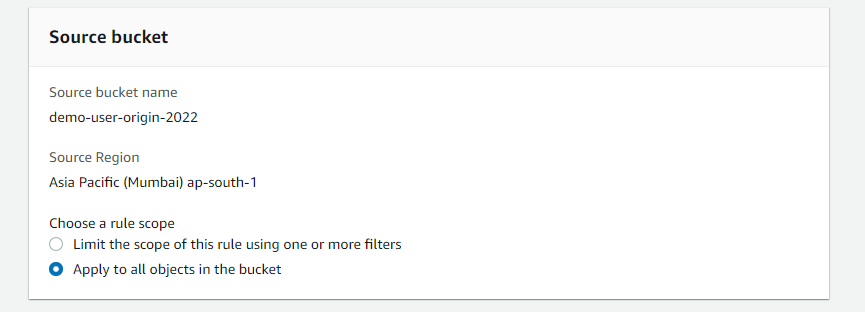


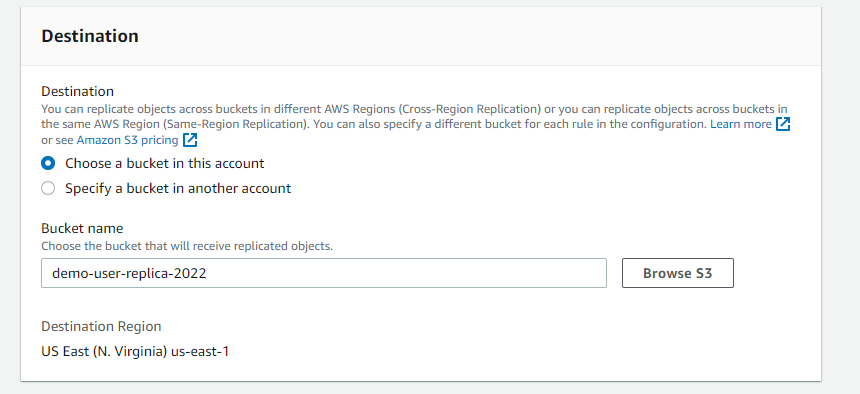
Go to replica rule



Click Create replication rule



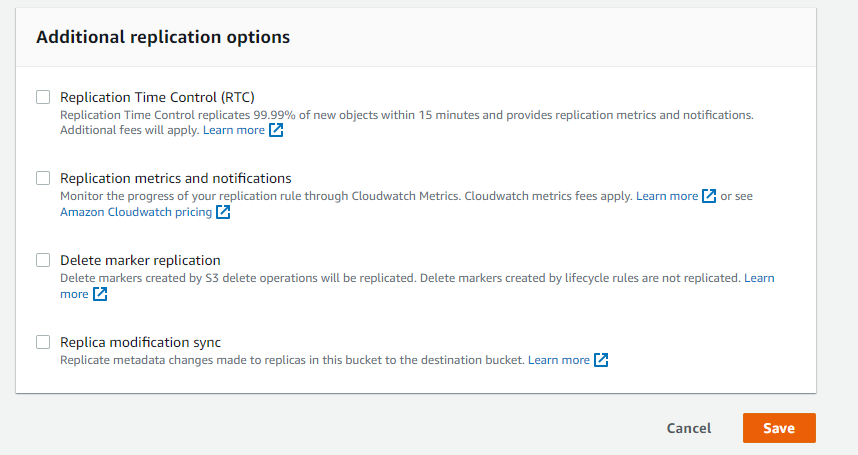


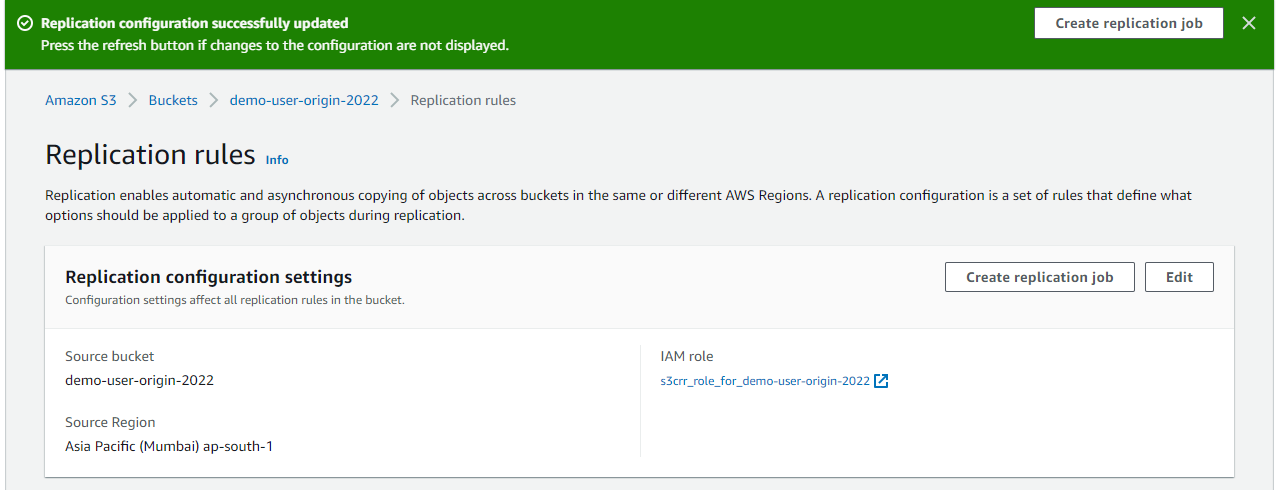


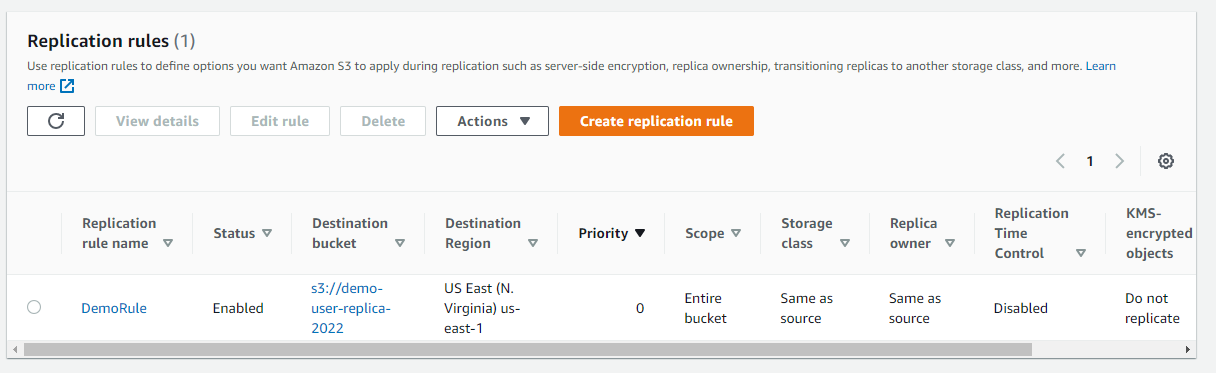


Keep encryption and additional options default

Keep save



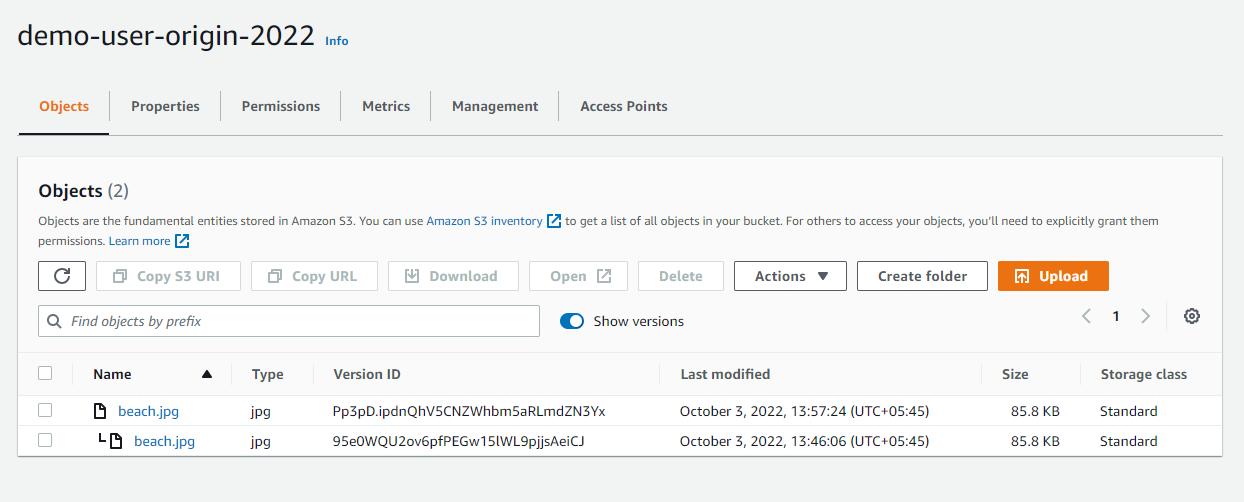




Go to origin bucket

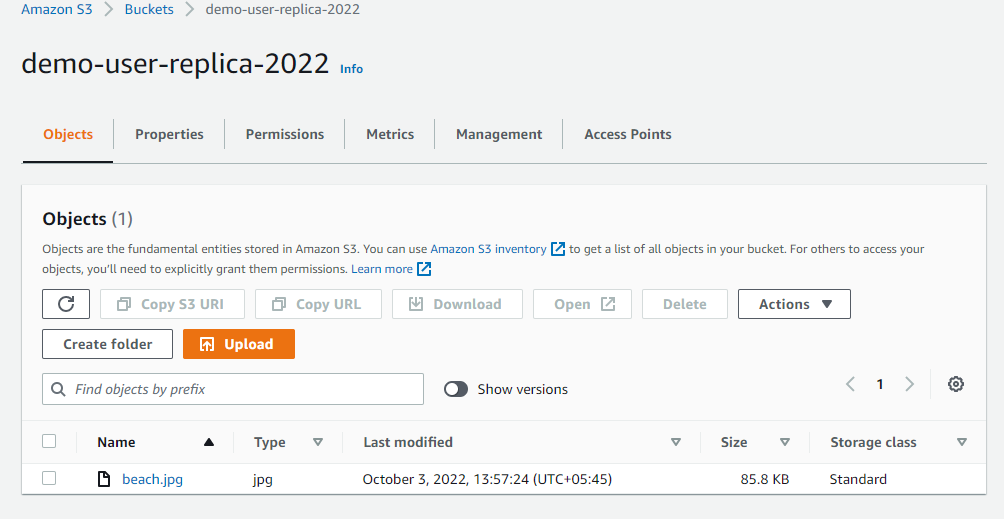


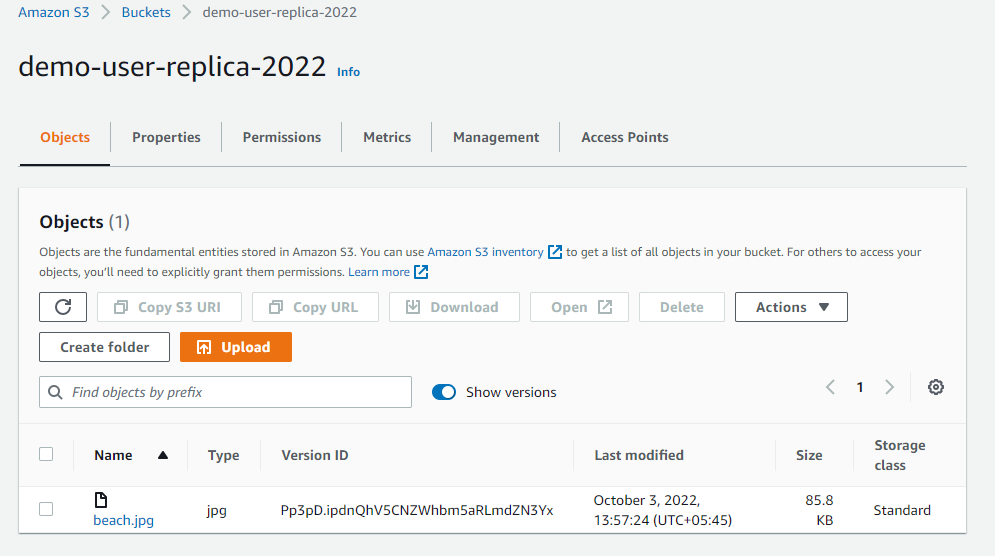
And upload file



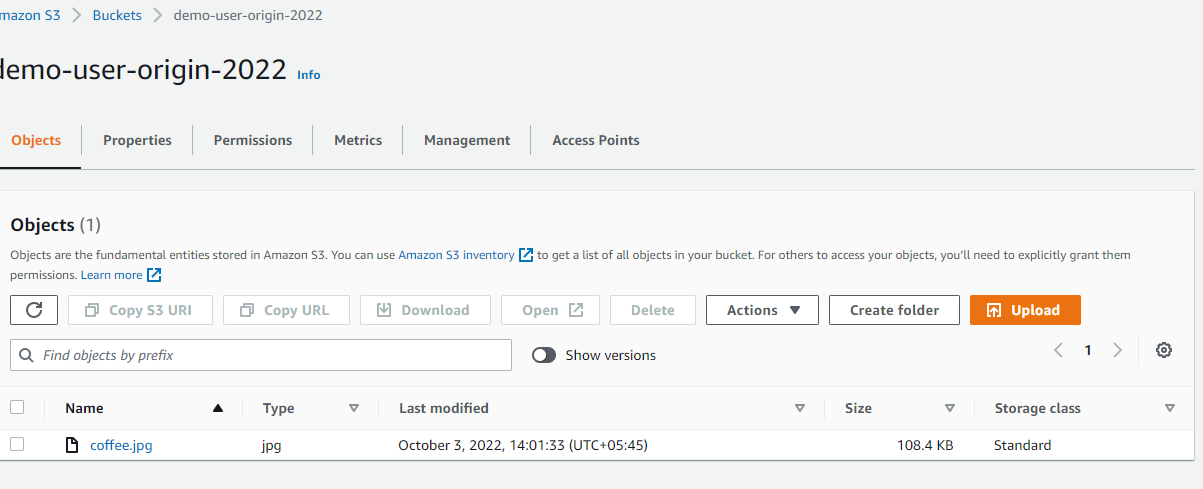
If you go to your replica bucket

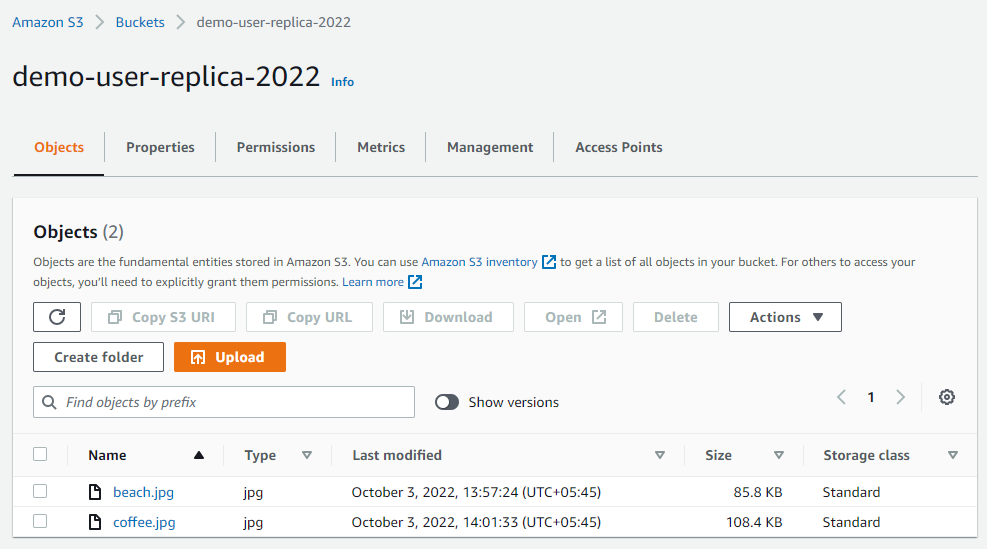
Same is also uploaded here with same version ID

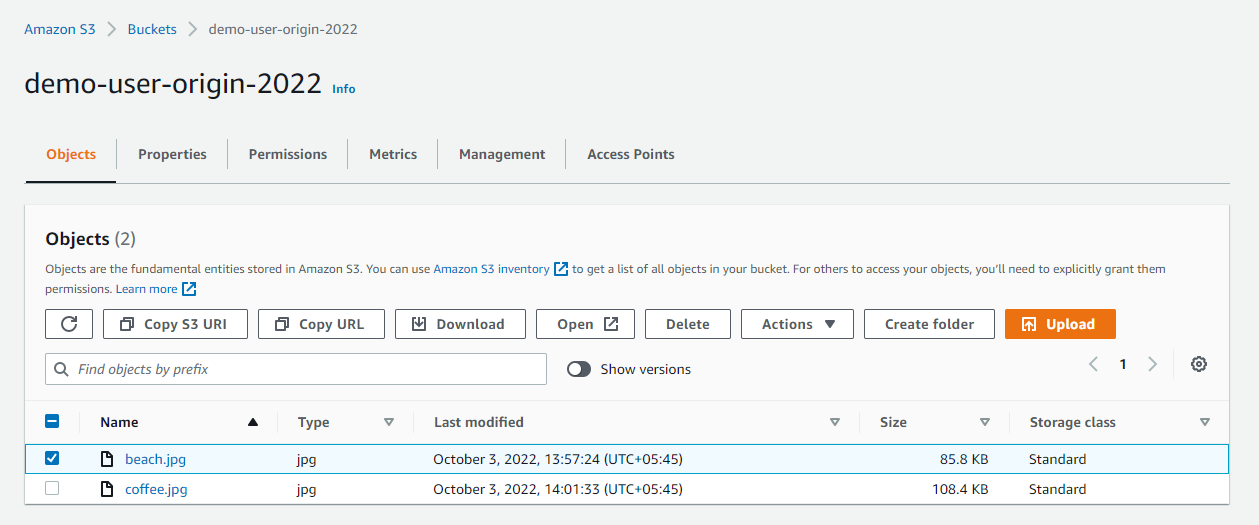




If you delete object , this will not be replicated.

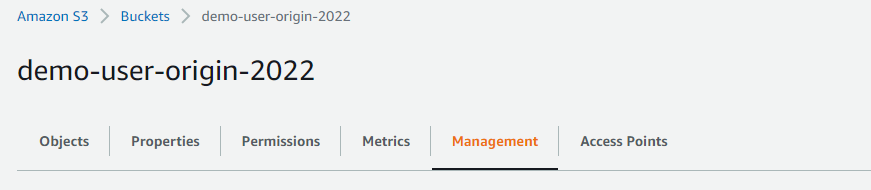


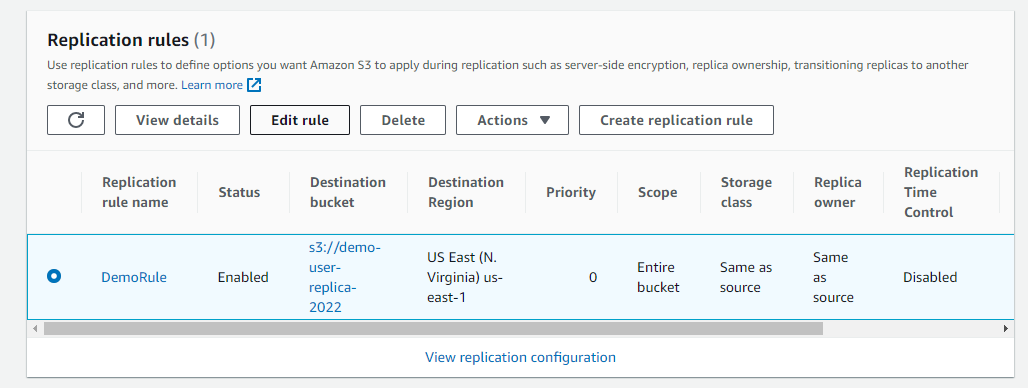




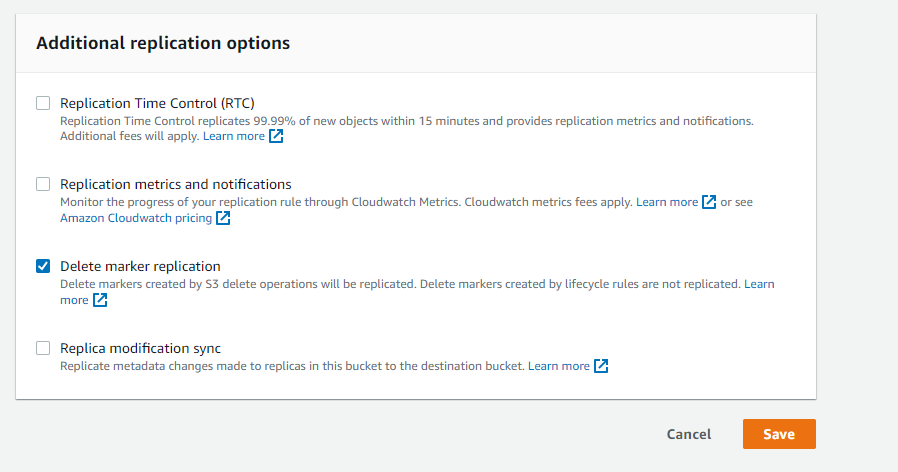
Edit rule on origin bucket management

demo-user-origin-2022

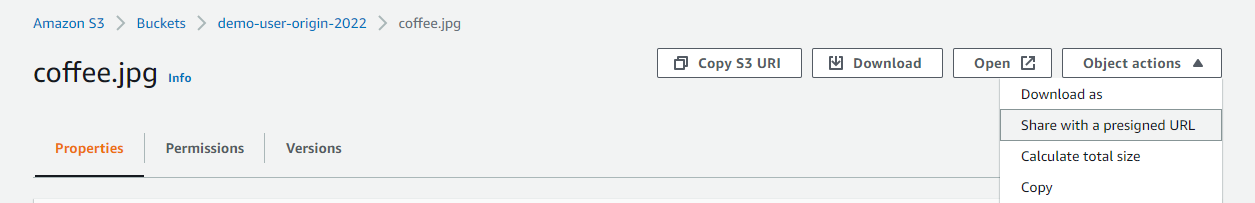


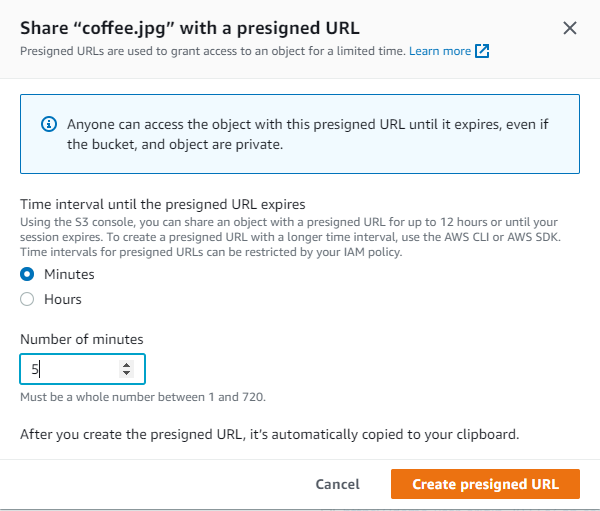


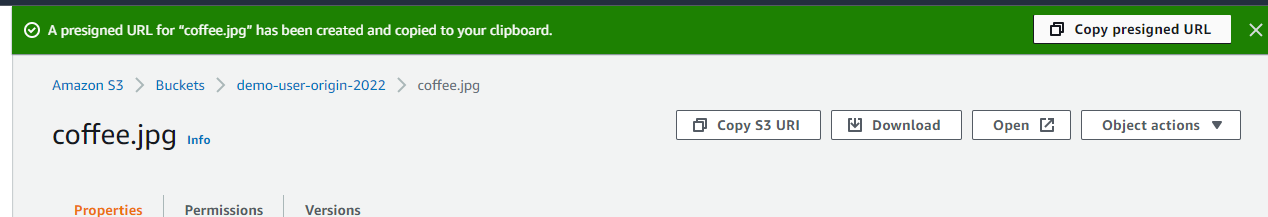
Highlight **delete marker replication** and **click save.**



**S3 Presigned URL**

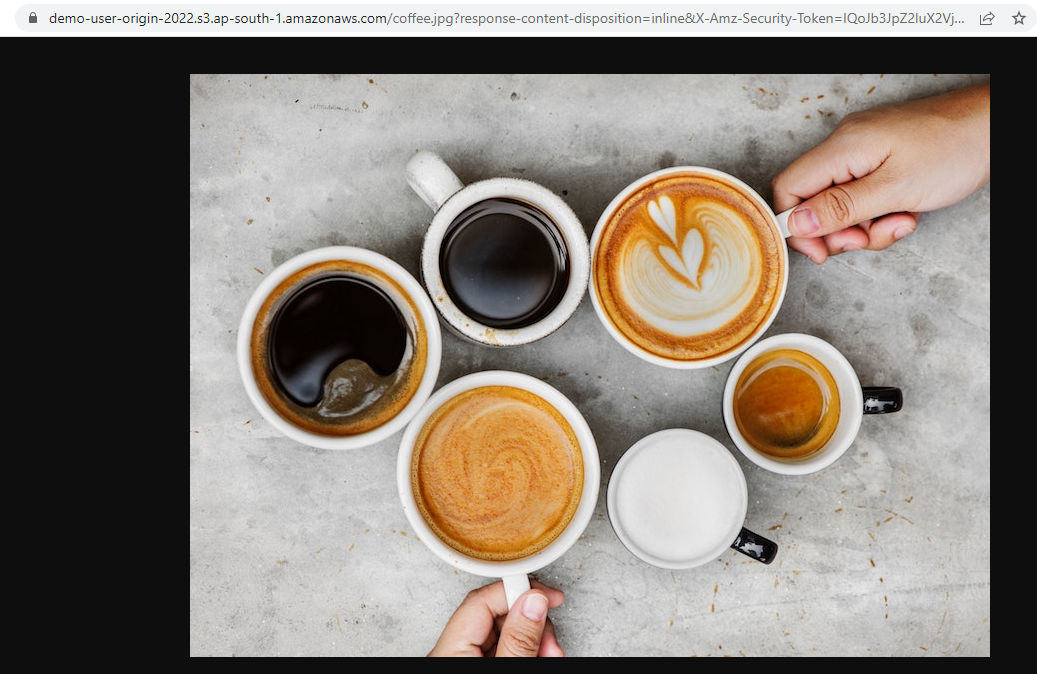






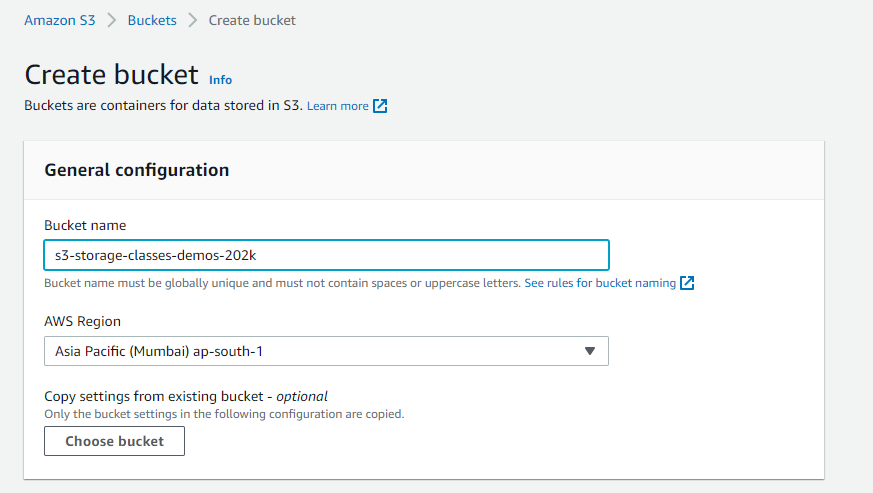
**Copy presigned URL and paste it**

**Anyone can access**

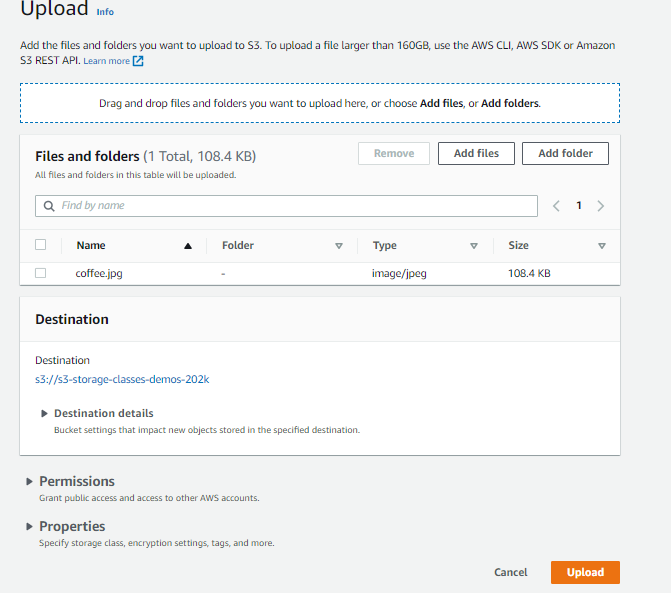


**Storages classes and Glaciers**

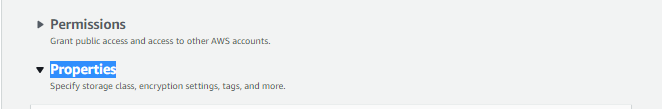
**Create s3 bucket**

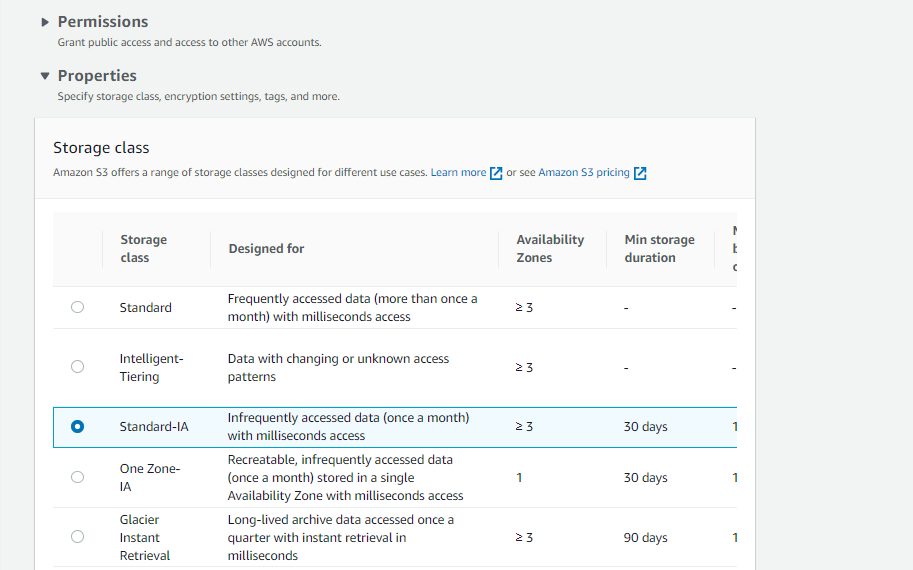


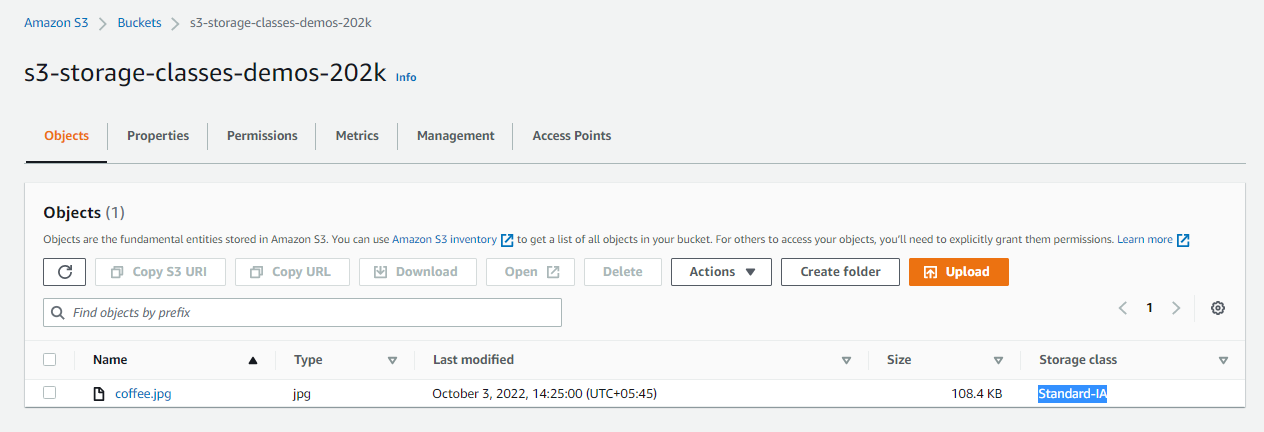
**Upload file**



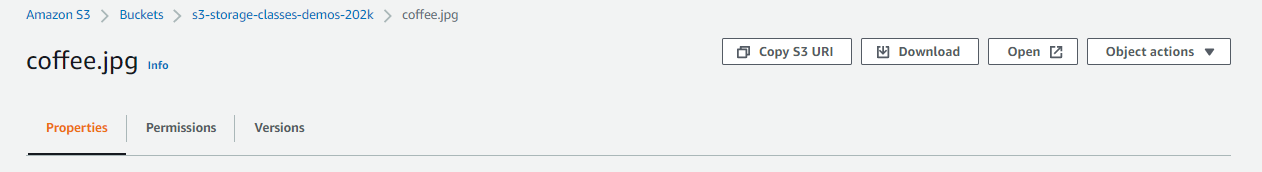
**Go to properties**





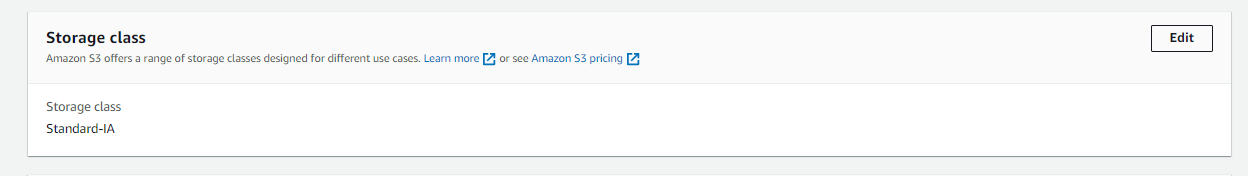


**Go to properties on file**

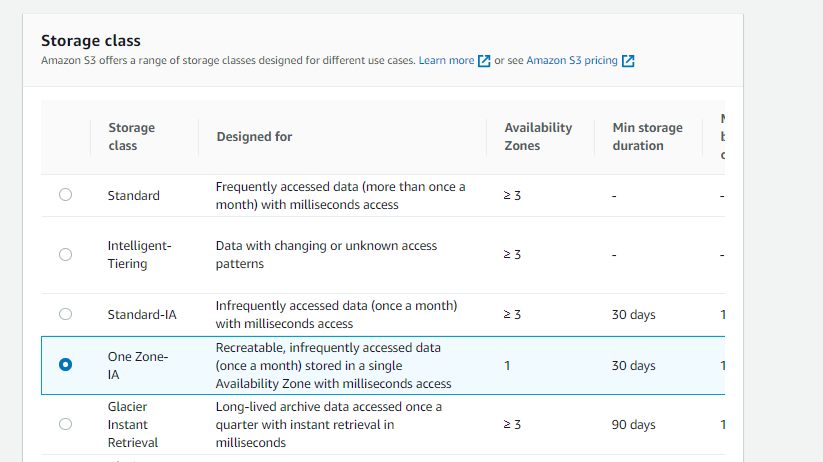


**Scroll down**

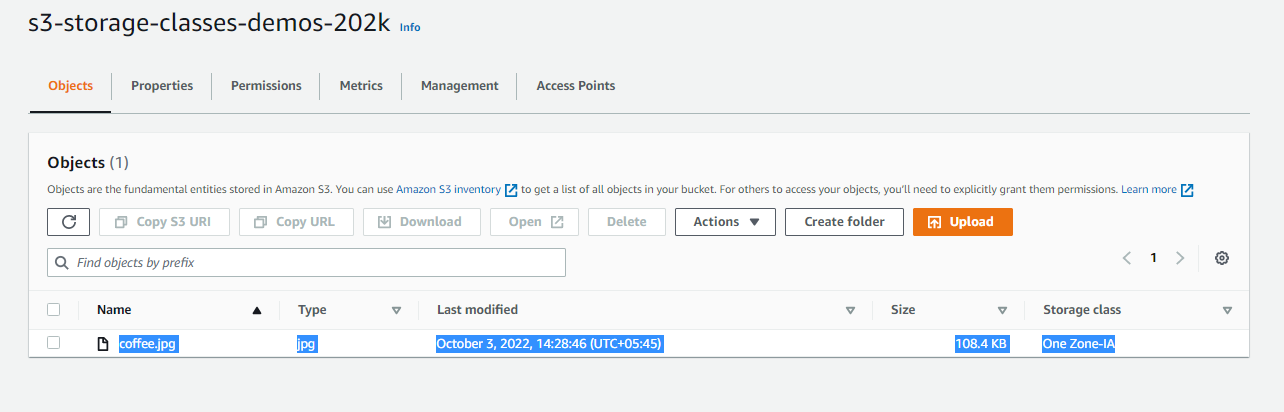
**Go top Storage class**

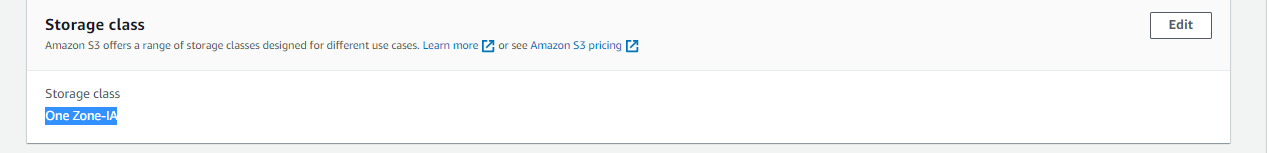


Select One Zone IA

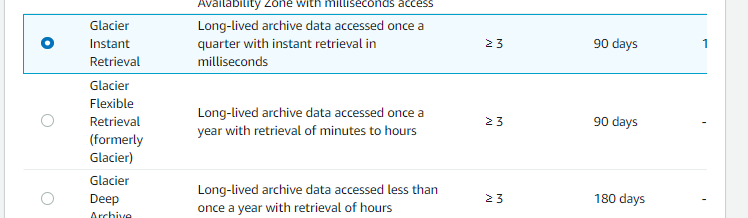


output



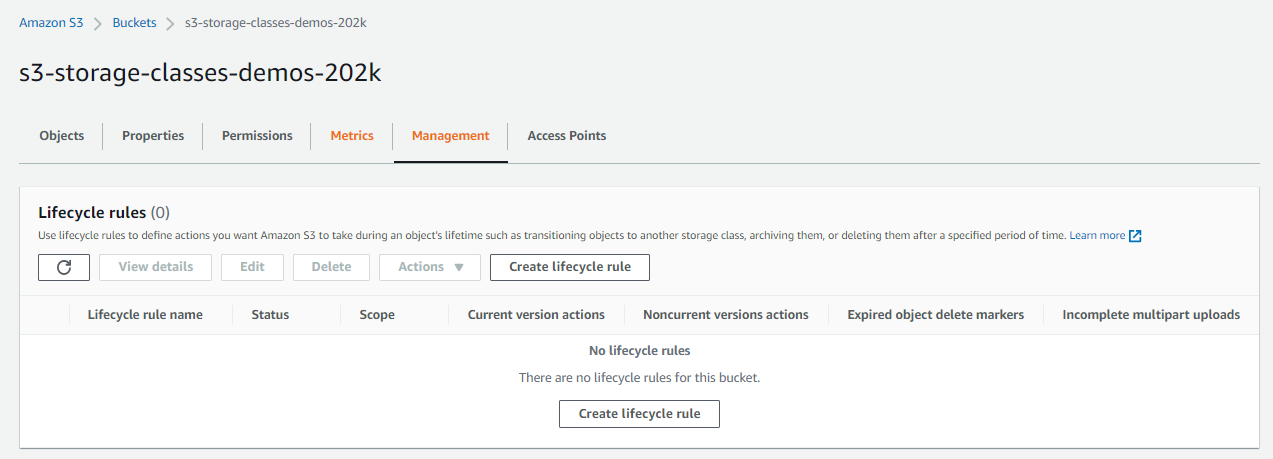


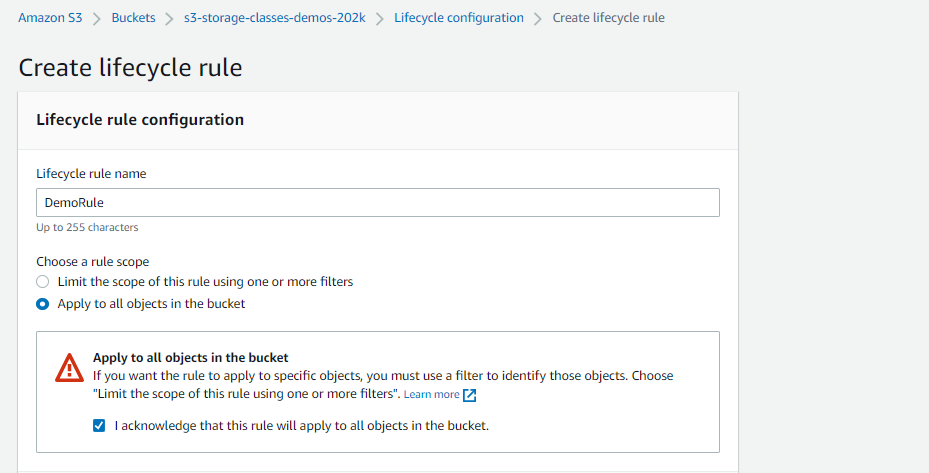
Same as choose

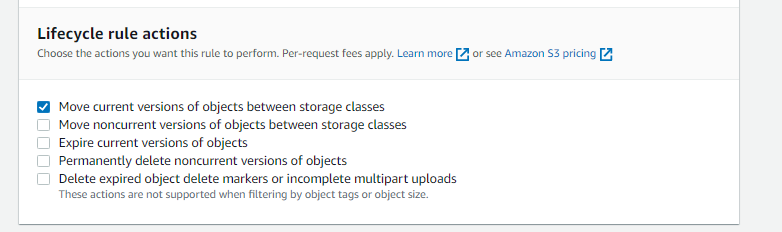


Go back to bucket

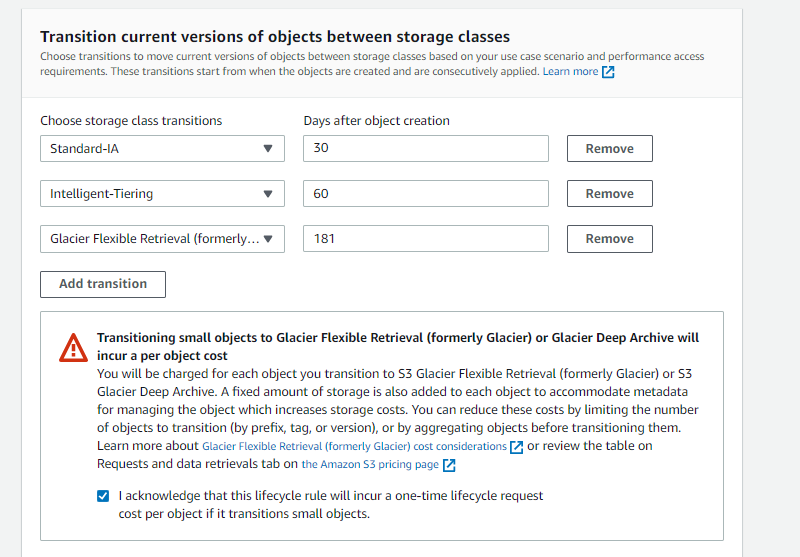
Create lifecycle rule



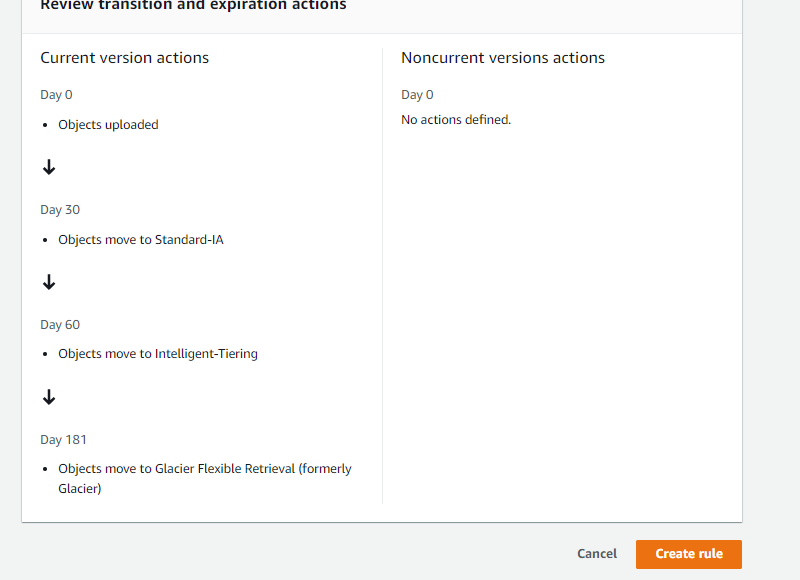




Add transition

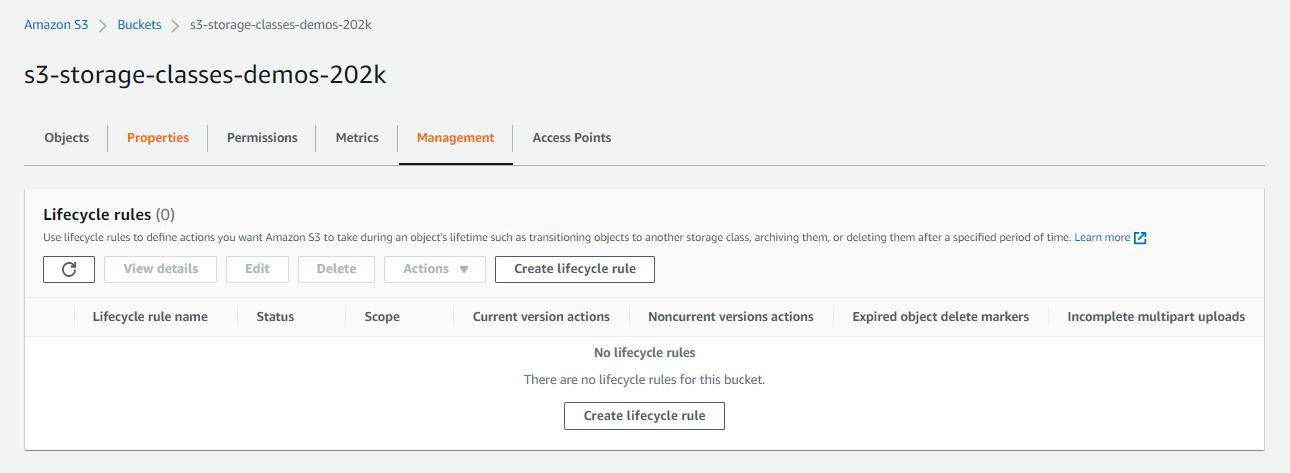


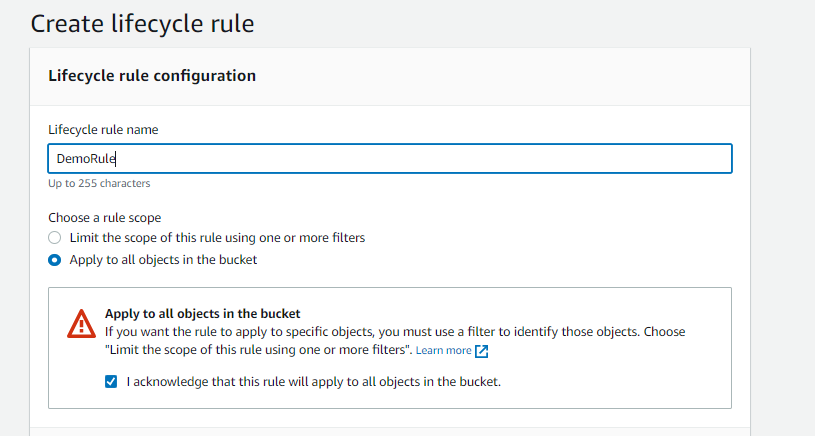
Then create rule

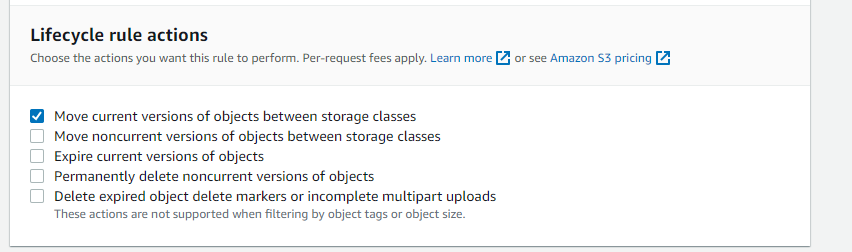


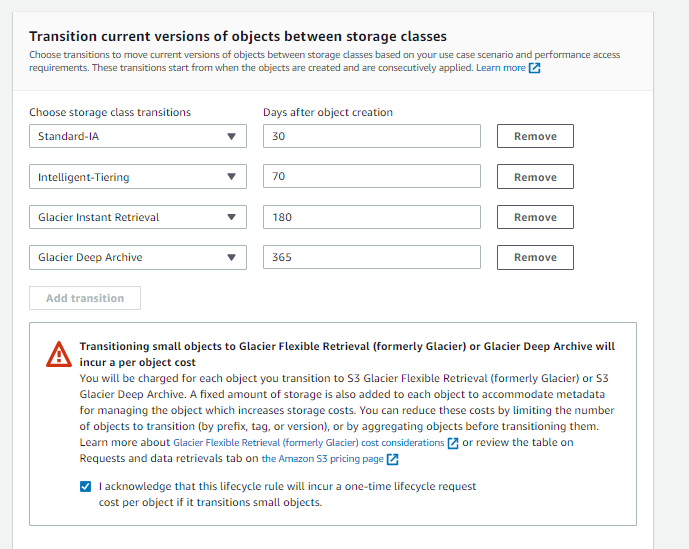
**Life Cycle Rules**

Go to management on bucket and create life cycle rule

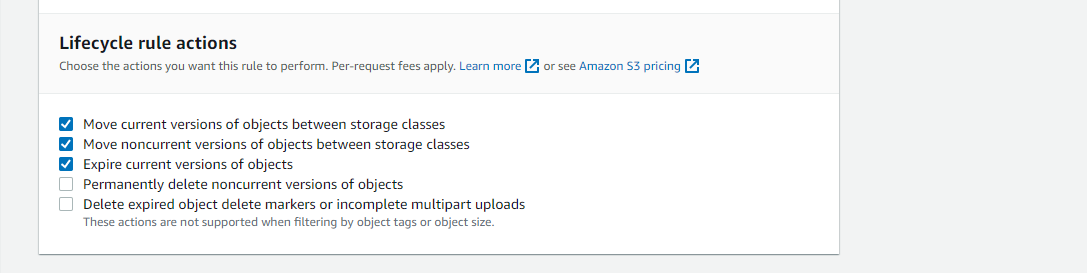


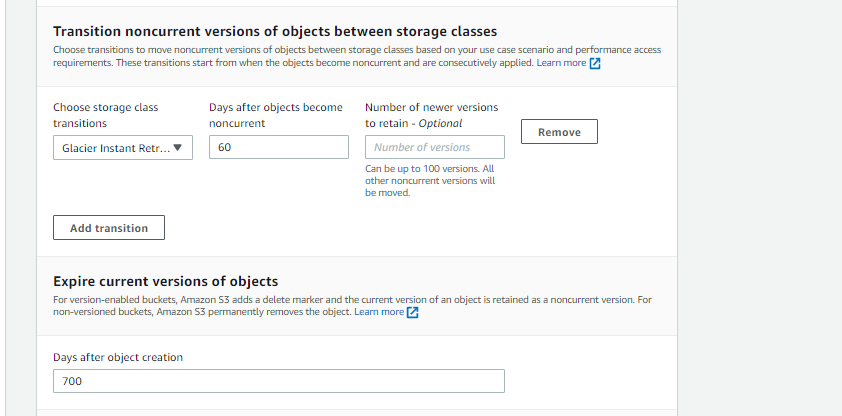


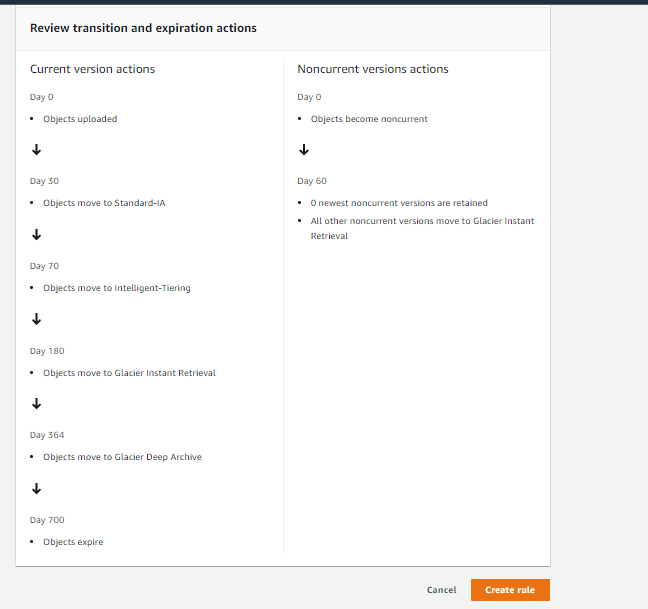


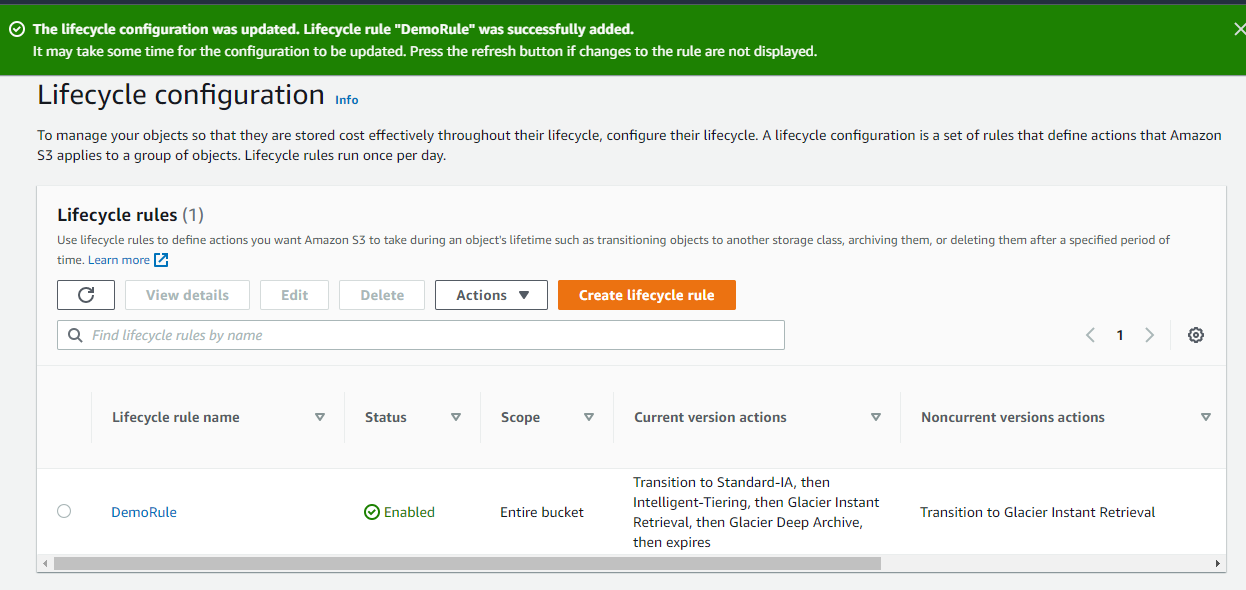


**Add two more**



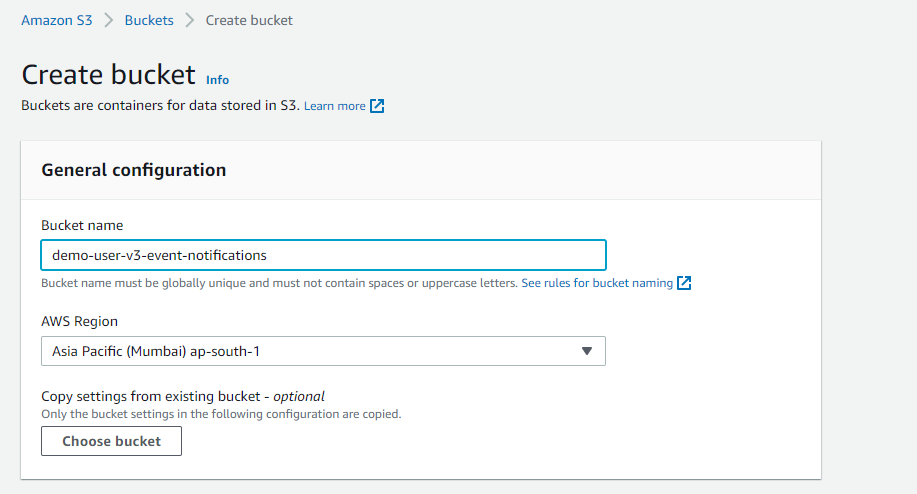




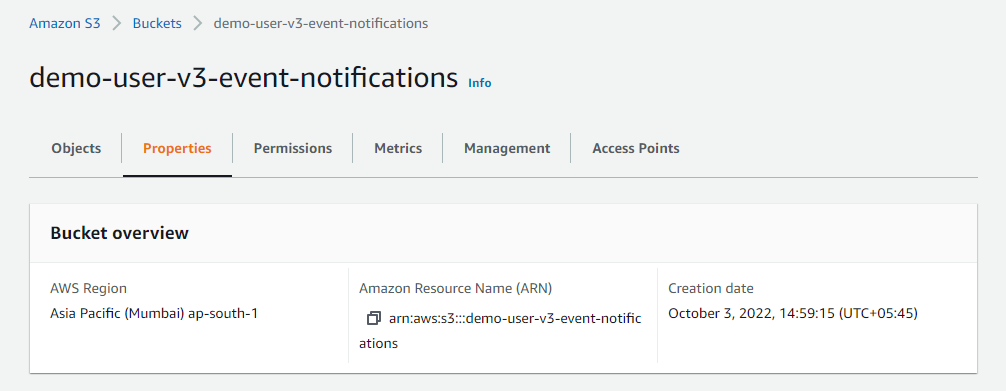


**S3 event Notification**

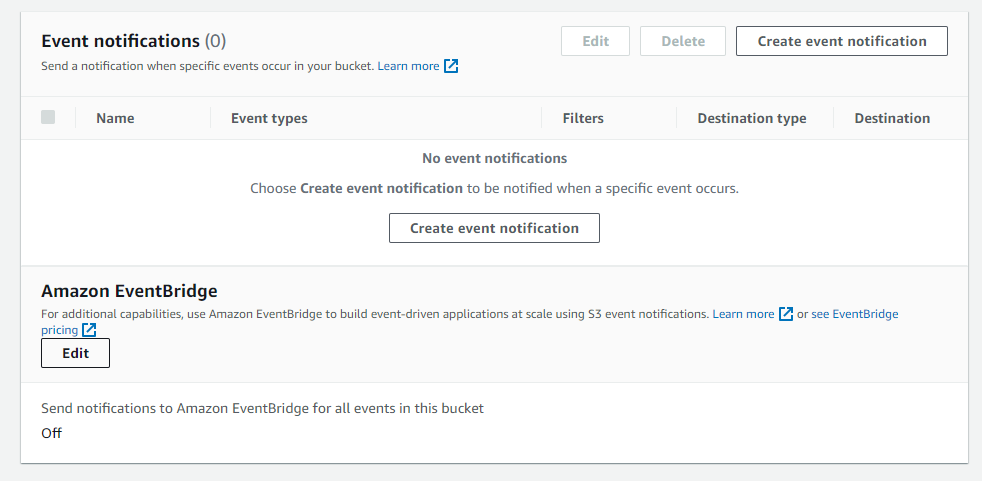
**Create s3 bucket**

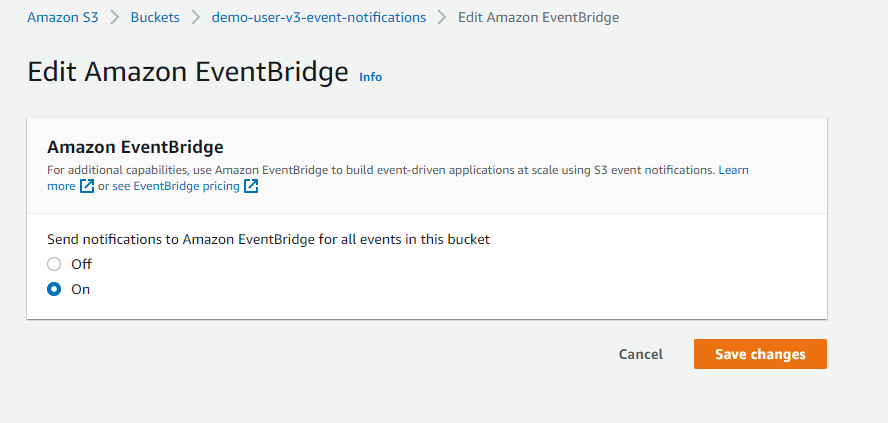


**Go to properties**

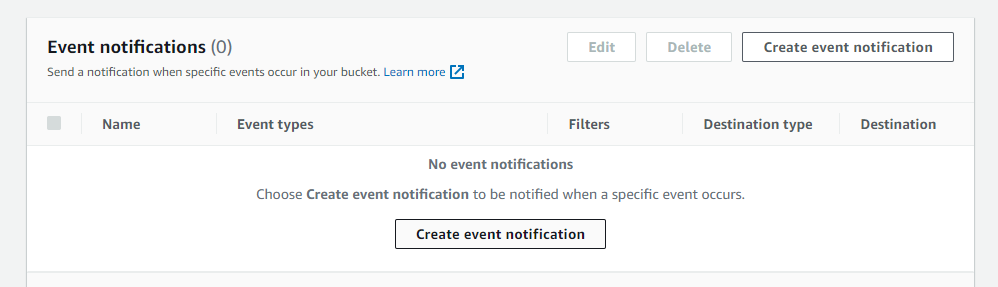


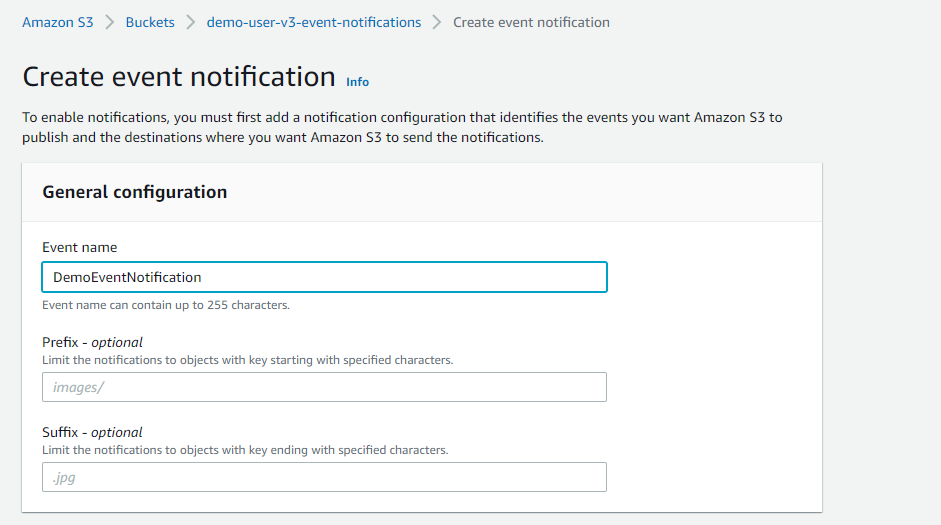
**Edit Amazon Event Bridge**



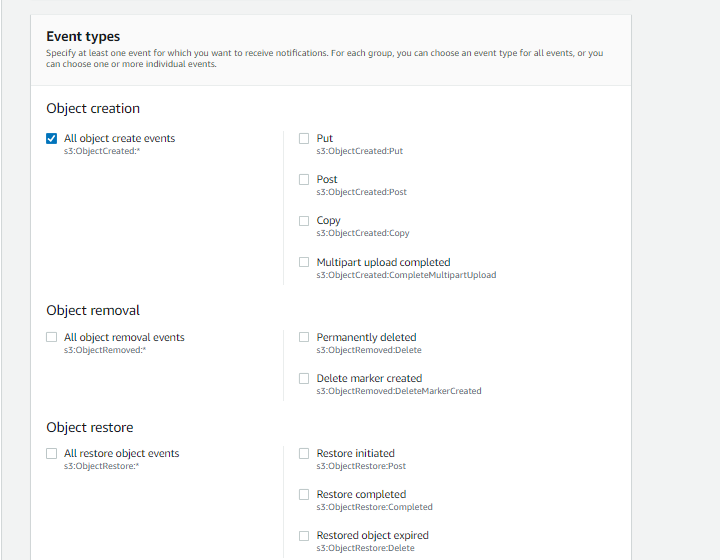


**Again Go to properties on bucket**

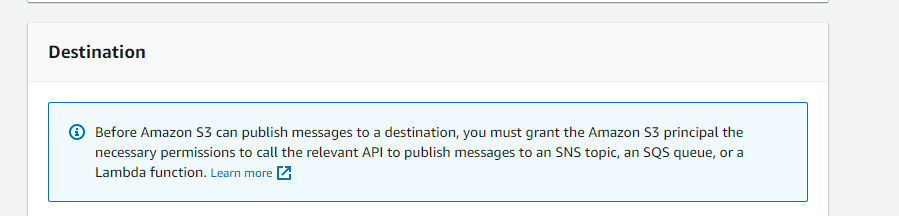




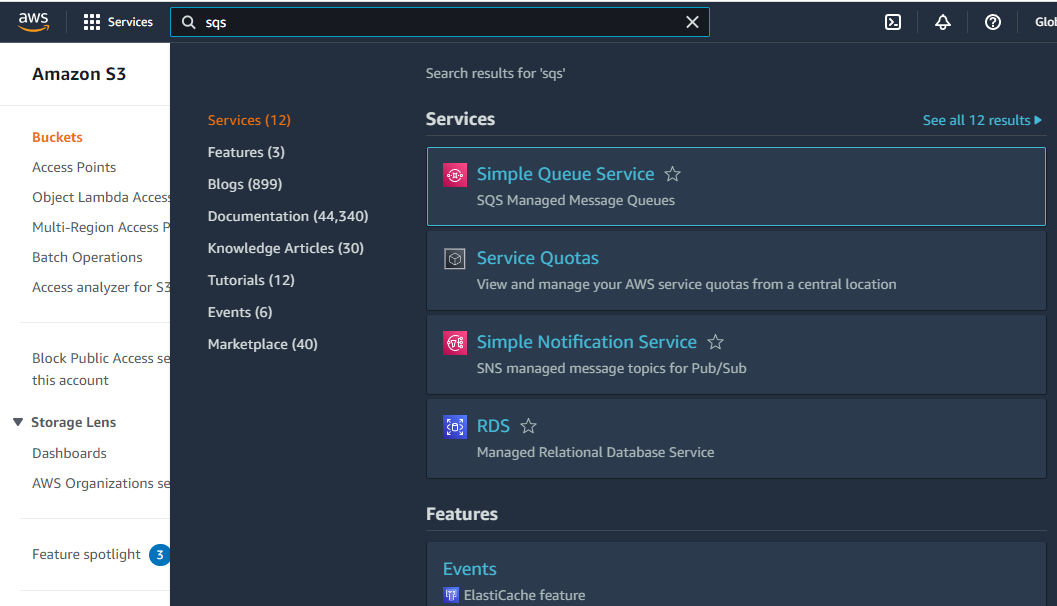
**Choose event type**

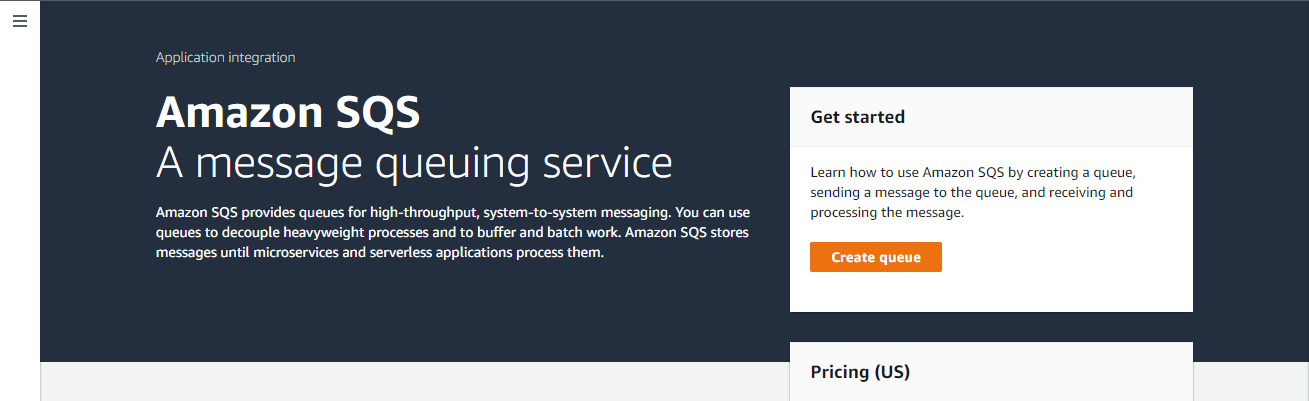


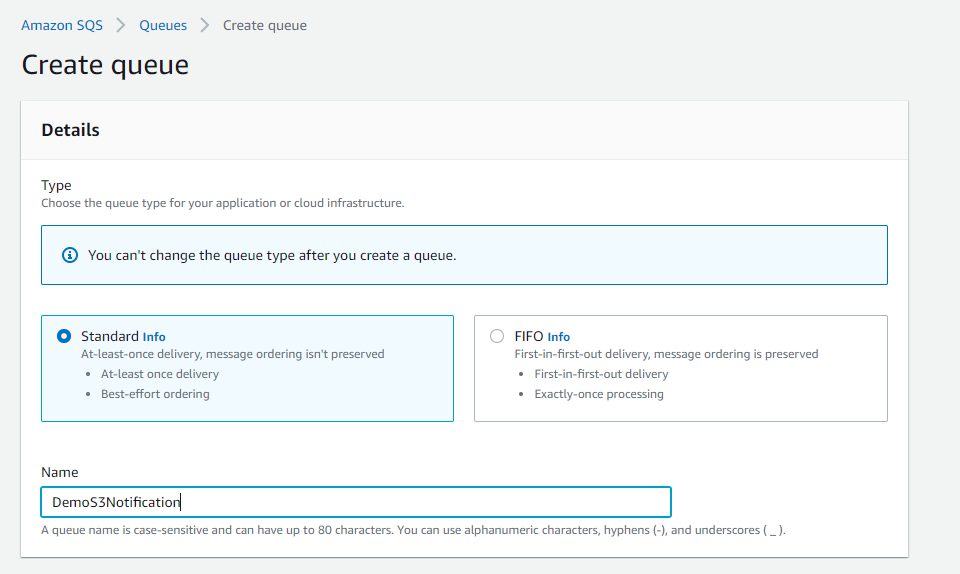
**In order to go destination**



**First go to SQS**

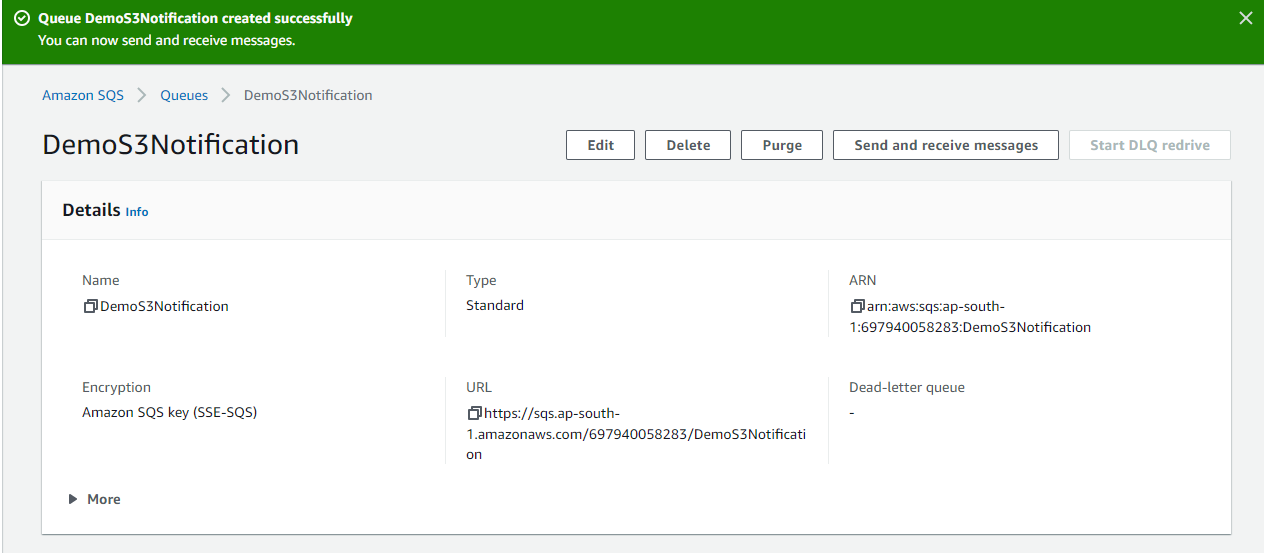




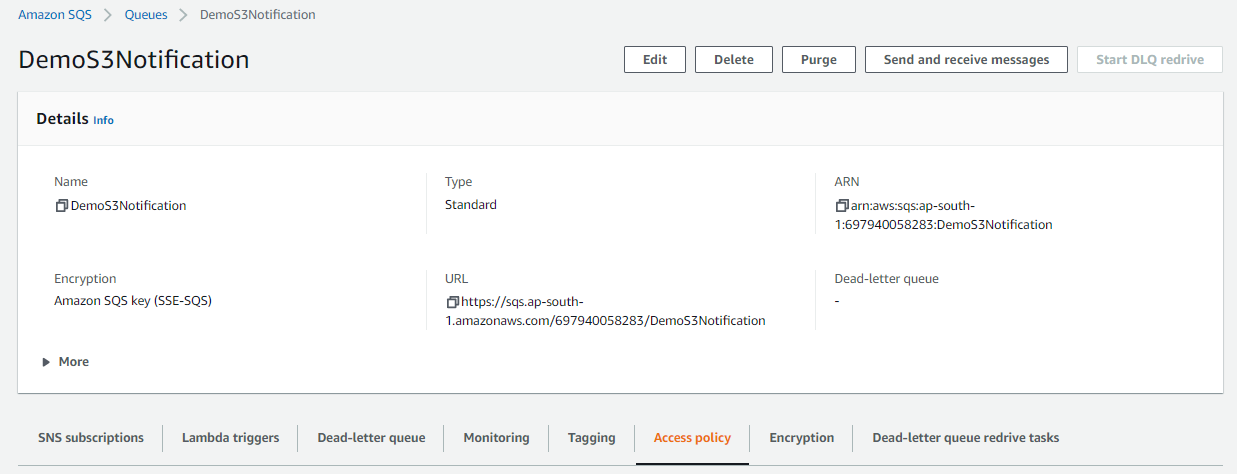


**Keep other options default**

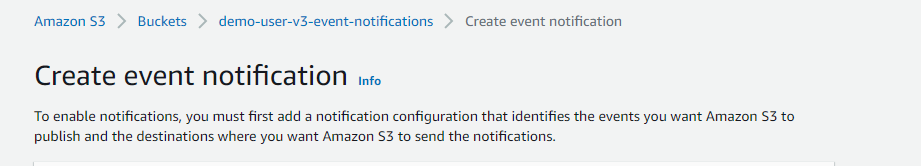
**Click create queque**

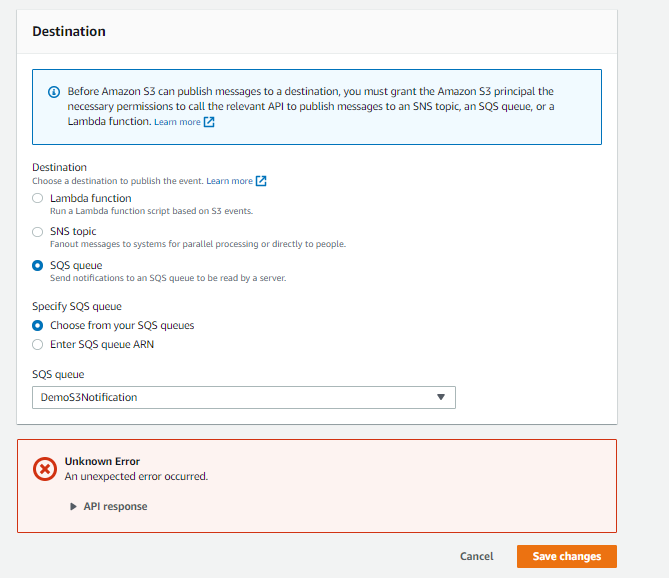


**Go to ACCESSPOLICY**



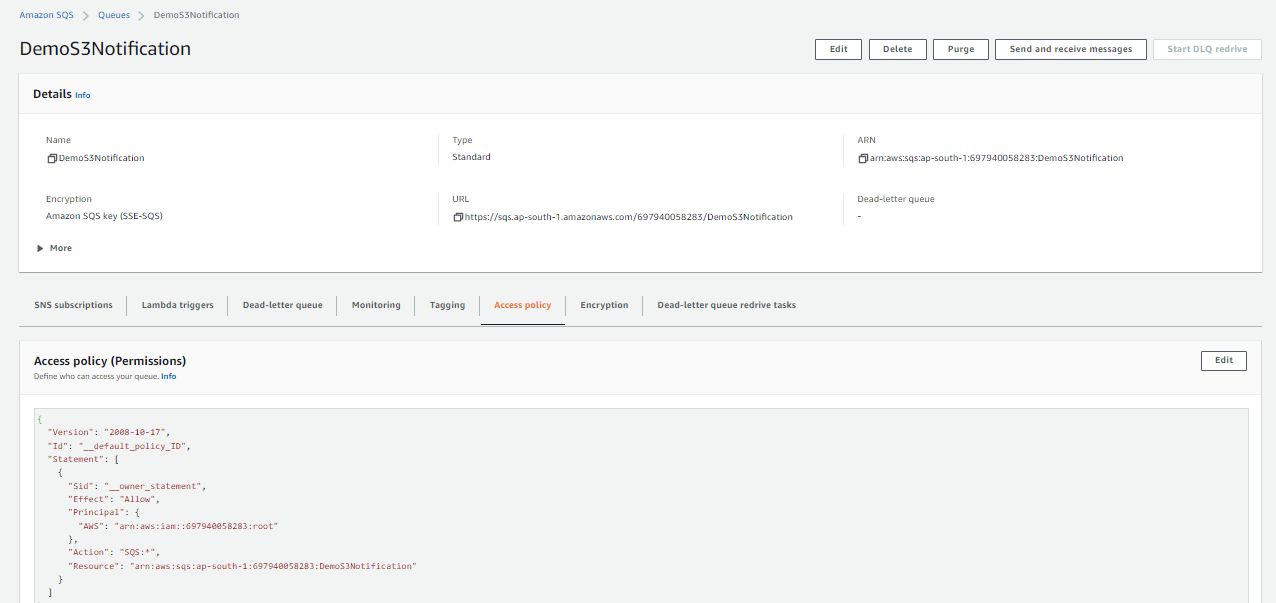
**Now refresh page**





**You will get this error**

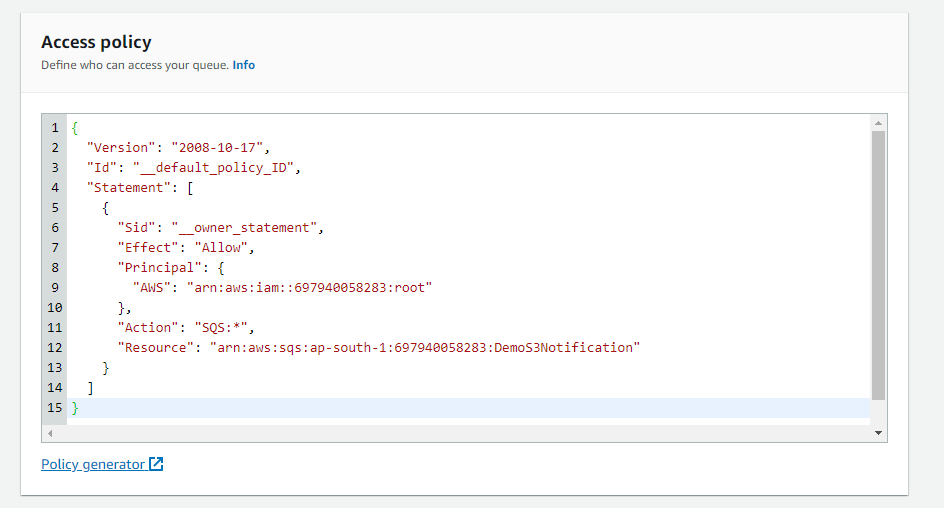
**Because access policy doesnot allow.**



**Go to edit change policy**



**Click policy generator**



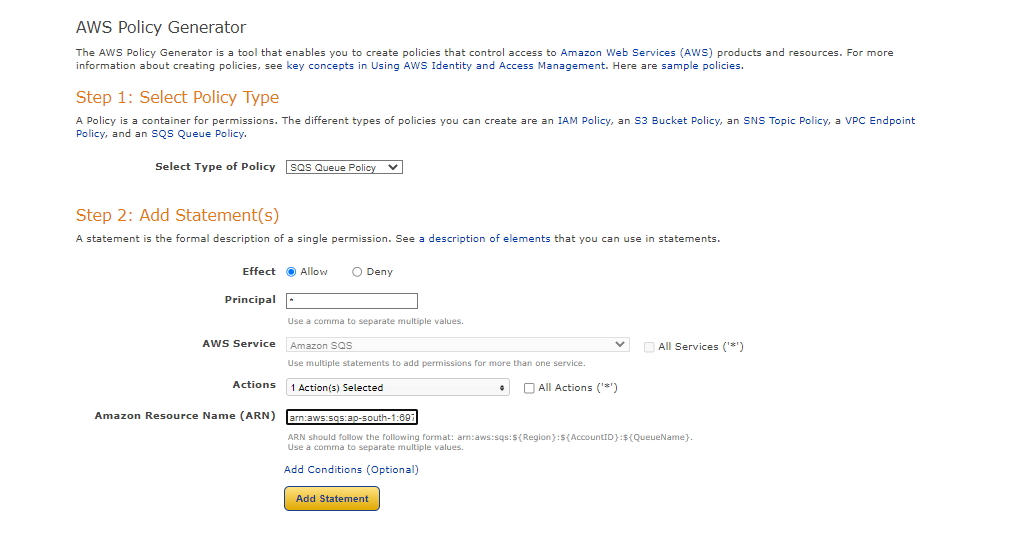
**Effect: Allow**

**Principal: \***

**Actions: Send Message**

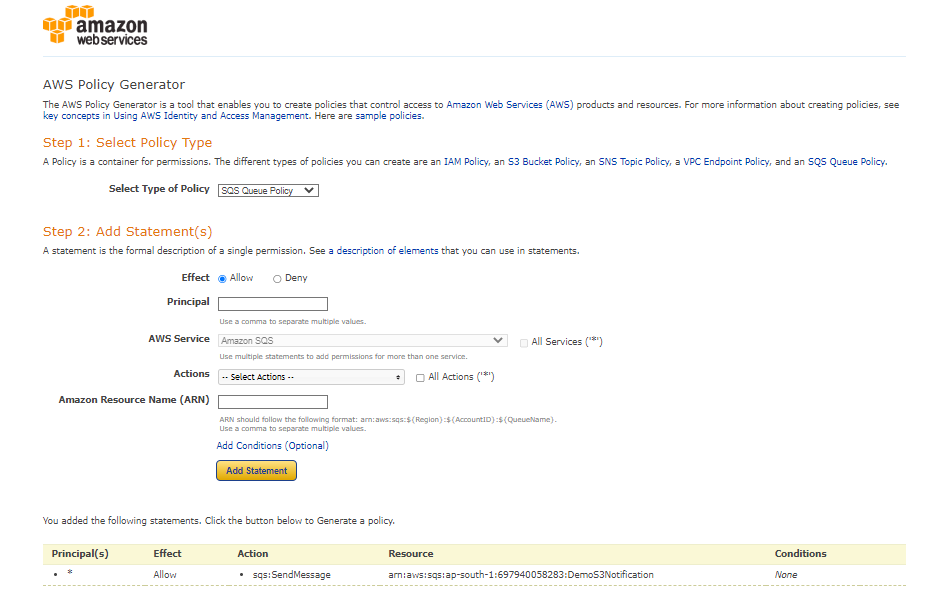
**Copy ARN**



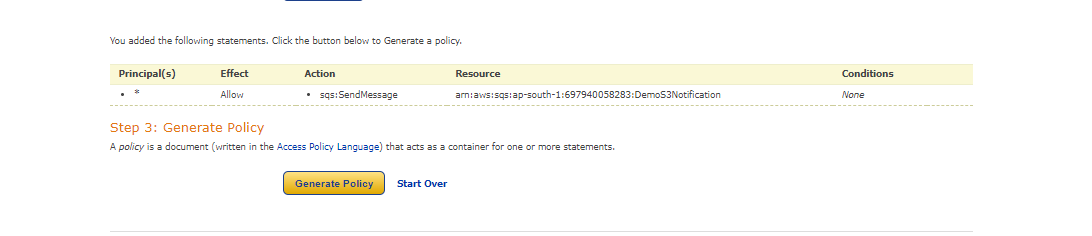


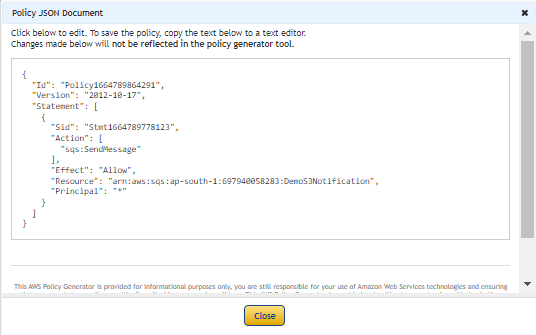
**Once fillup click Add statement**

**Output**

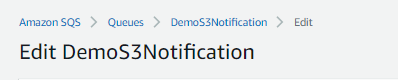


**Click generate policy**



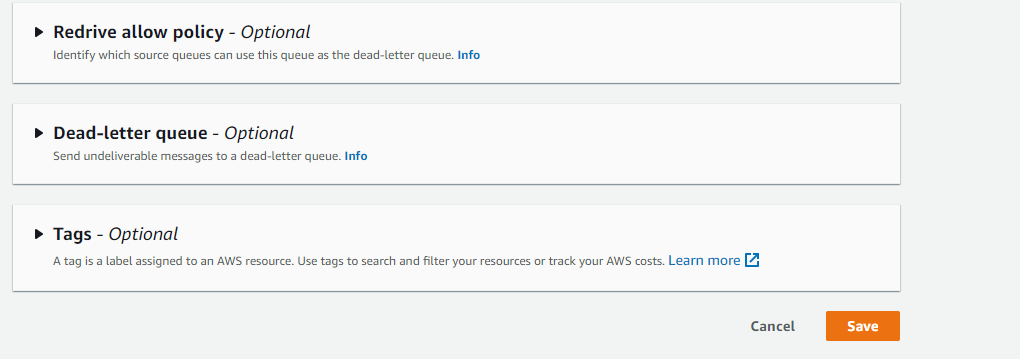


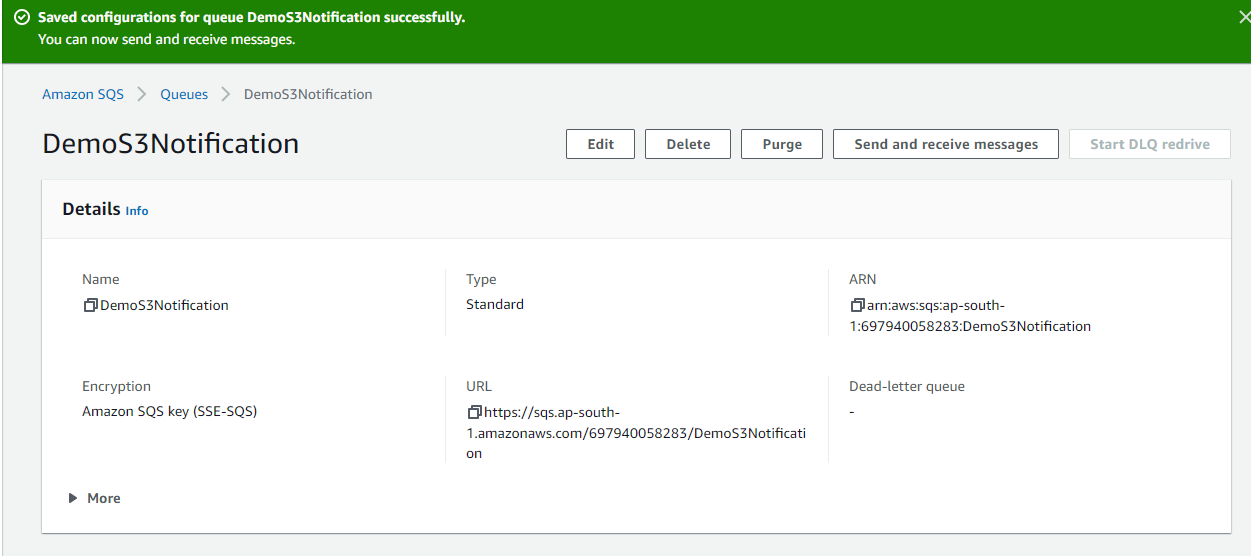
**Copyand paste this policy Edit DemoS3Notification**





**Click save**

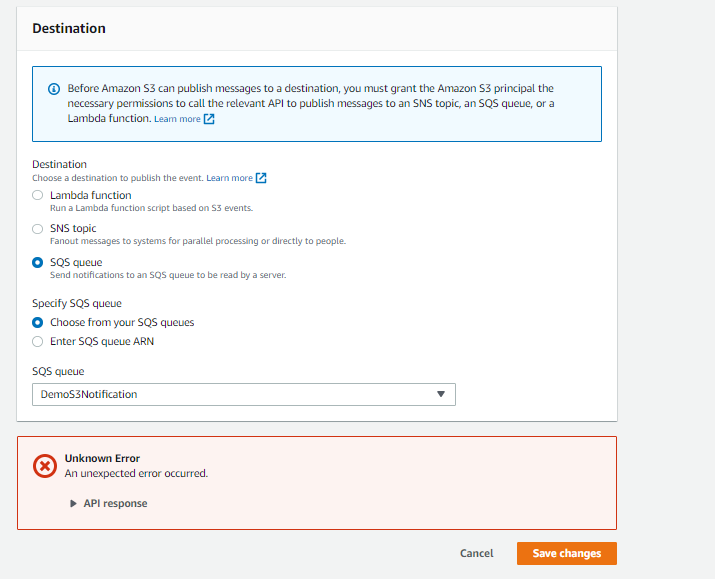




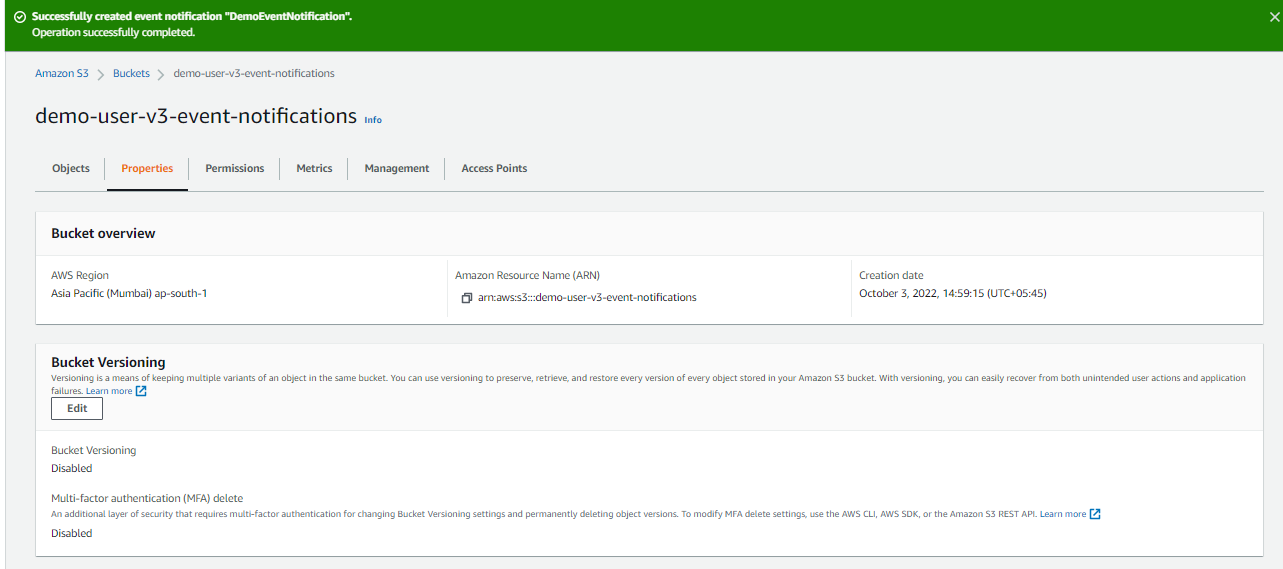
**Now Access policy has been updated.**

**Go back to** Create event notification

**Click save changes**

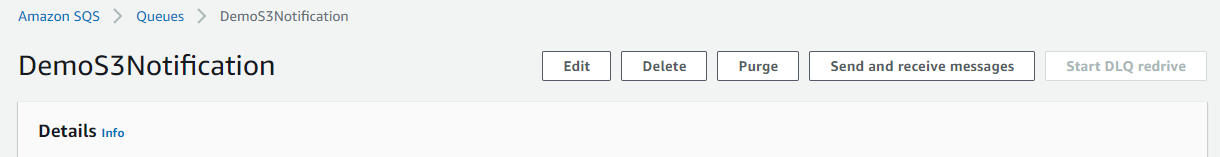


**Successfully completed**

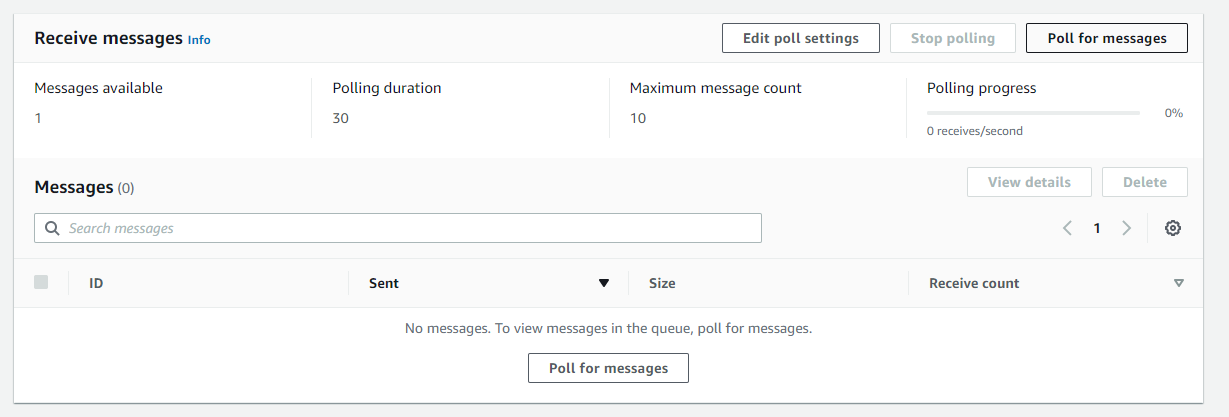


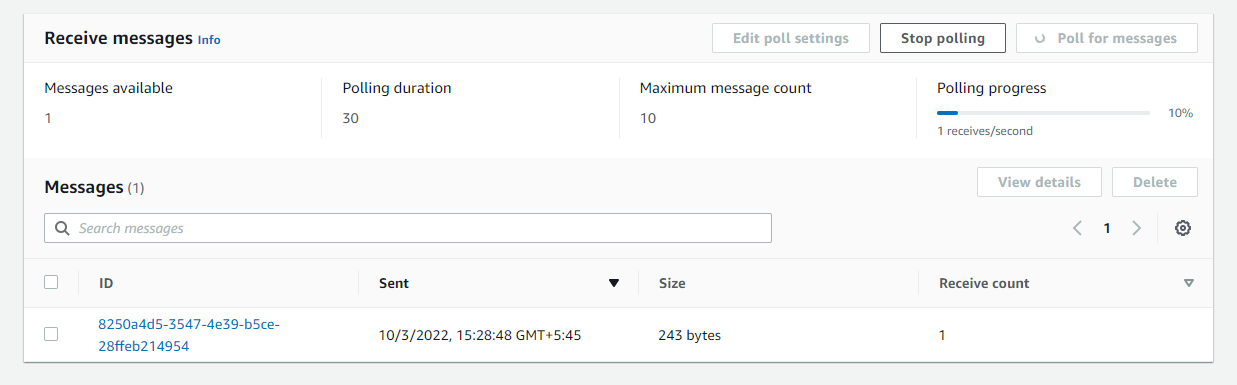
**Go back to sqs**

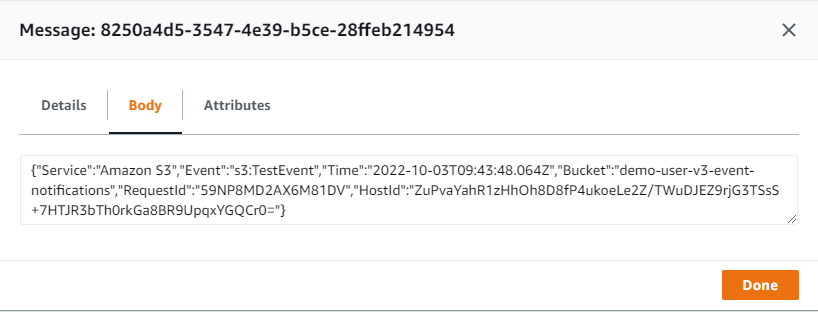
**Click send and receive messages**



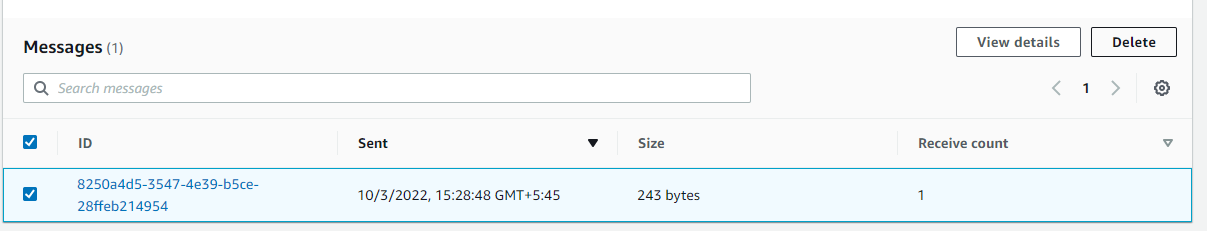
**Click for poll for messages**





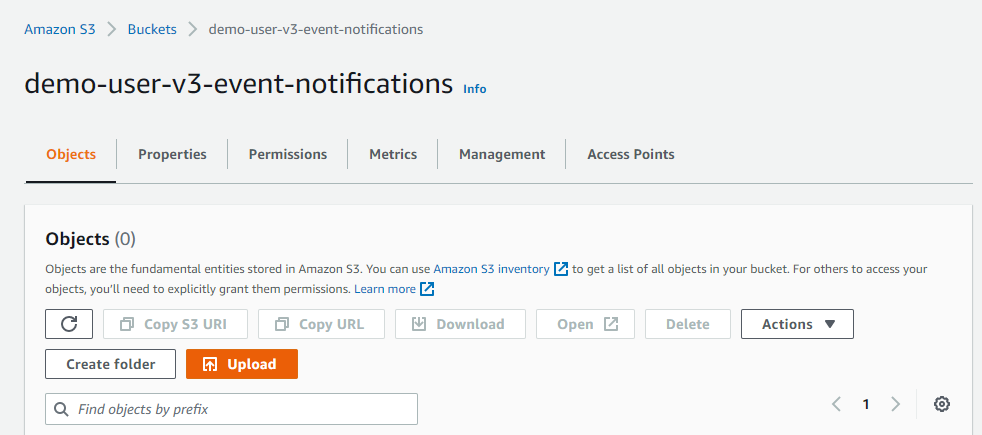


**Delete**

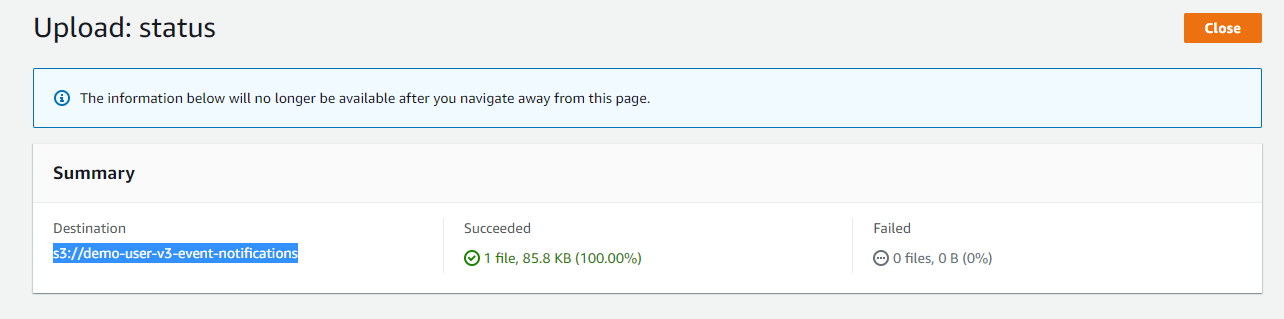


**Lets test whether sqs notification is working or not.**

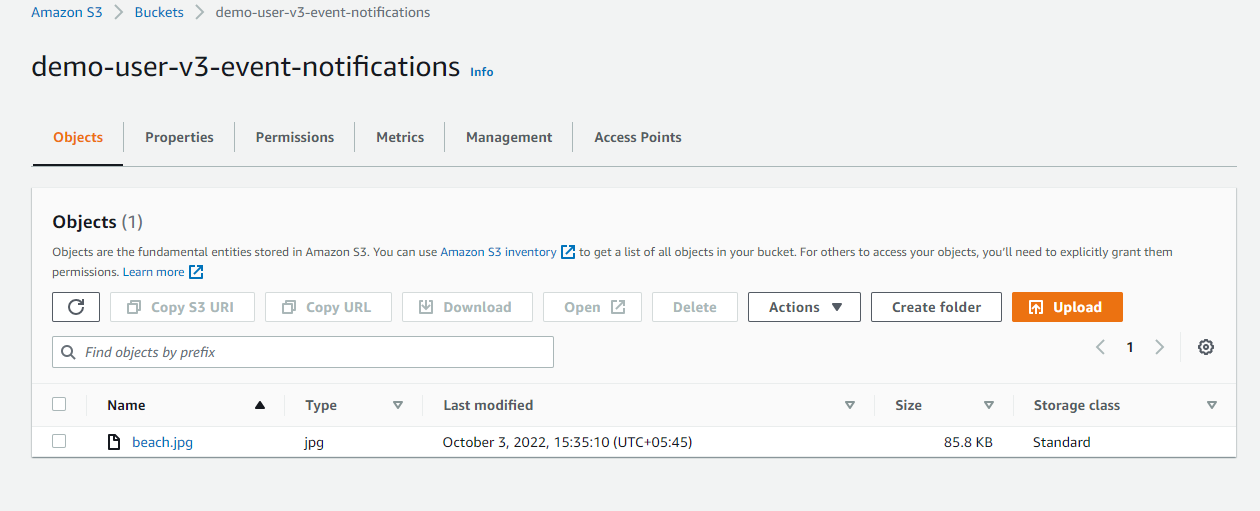
**Go back to s3 bucket and upload file**



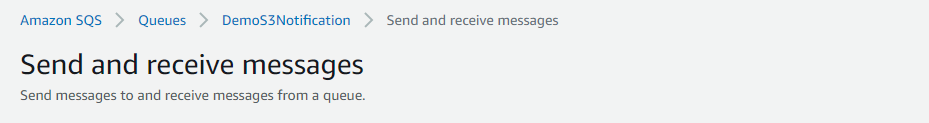
**Go to s3 bucket**



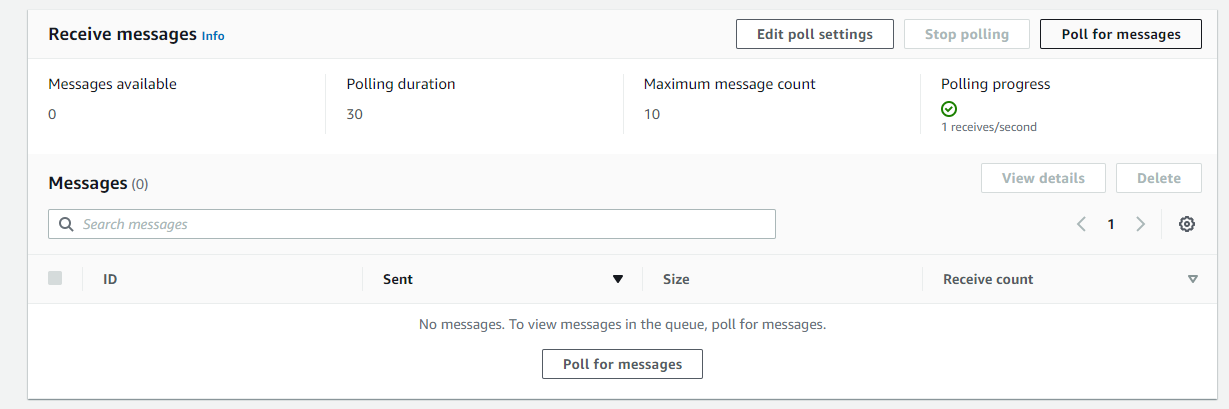
**File has been uploaded**



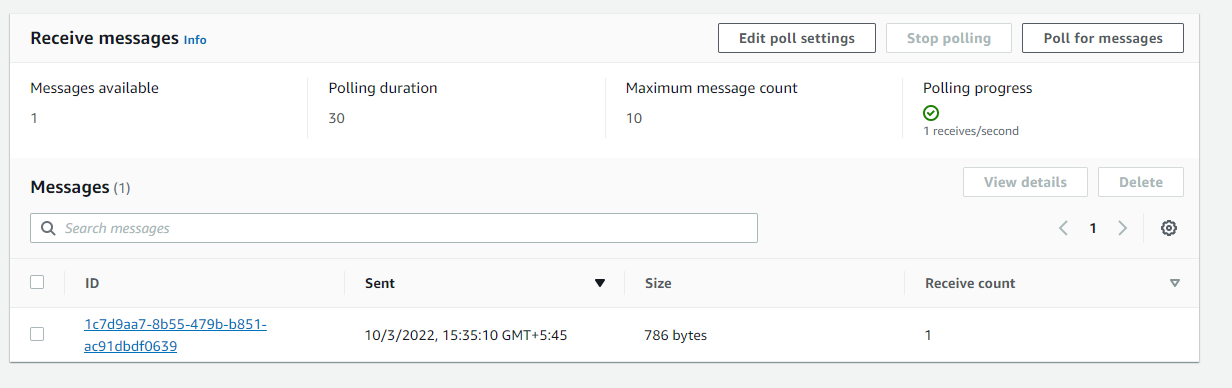
**Go to SQS**



**Click poll for message**

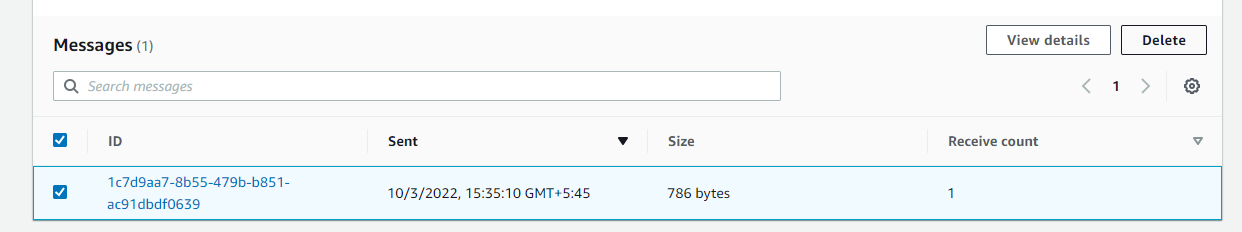


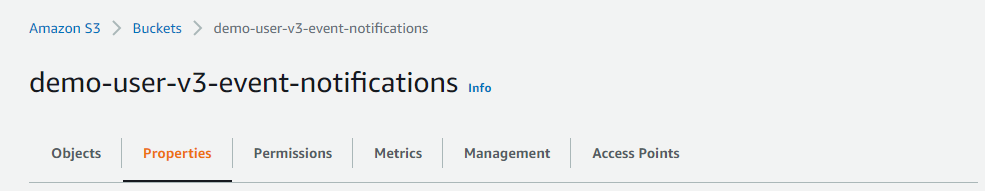
**Open message**

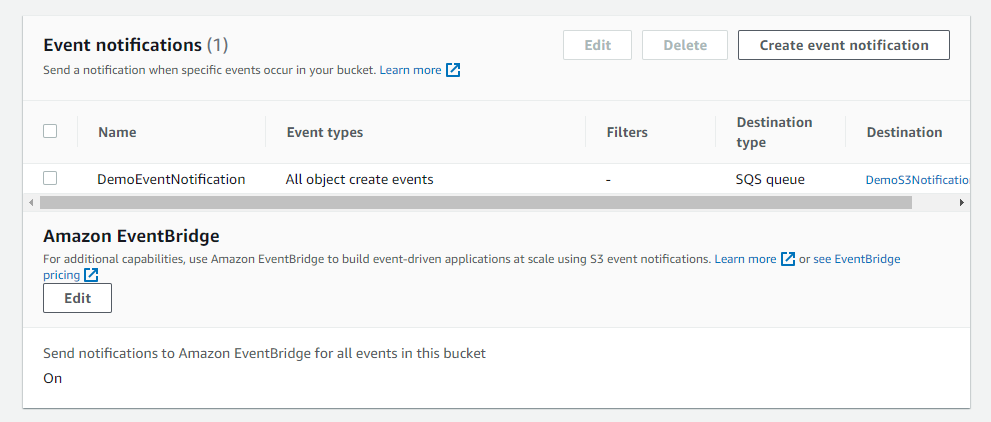




**Click delete**

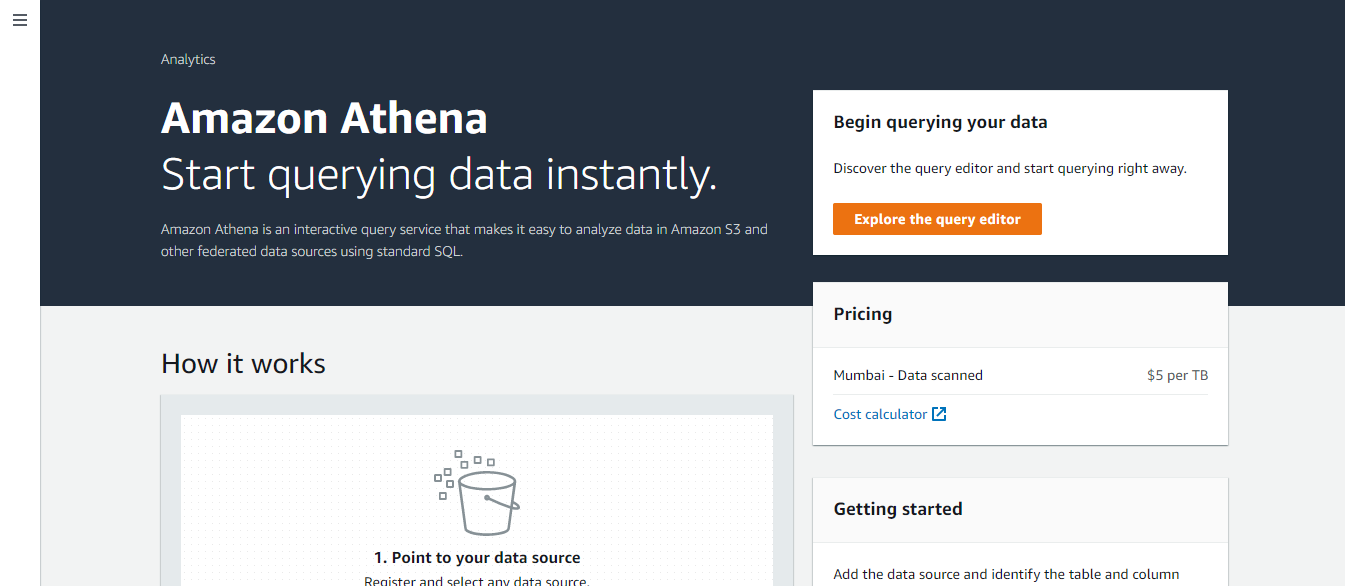




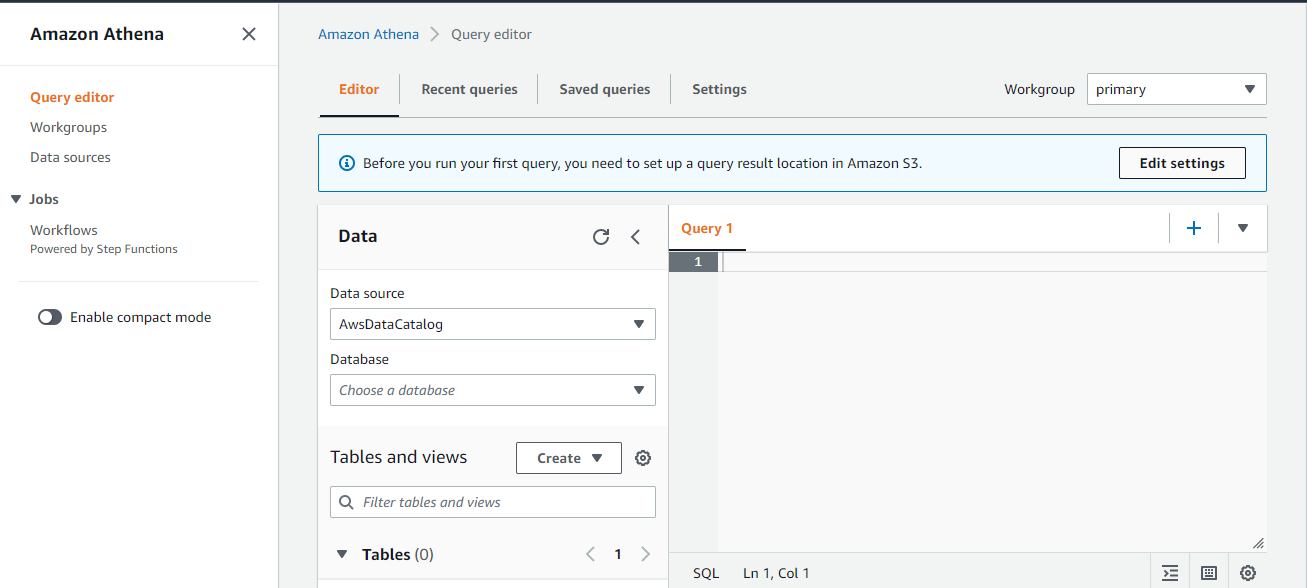


**Athena Demo**

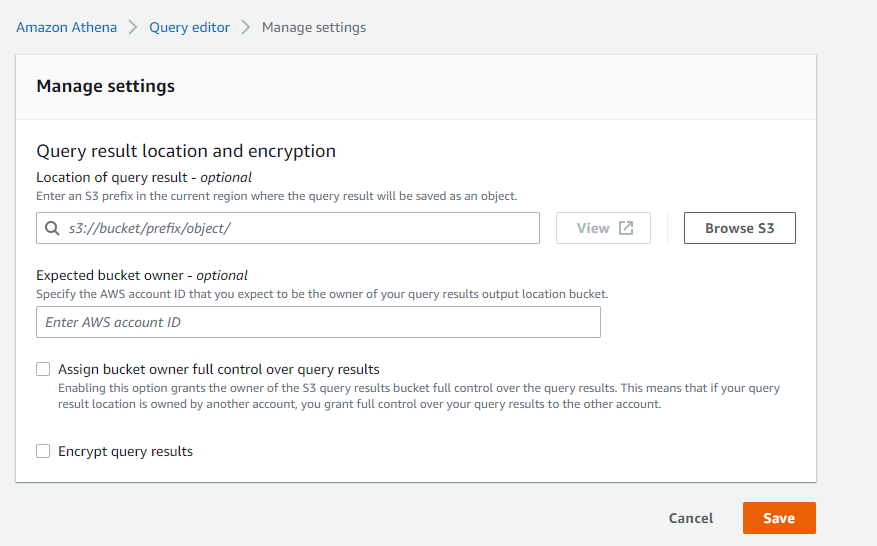
**Go to Amazon Athena on aws console**



**Click edit settings**



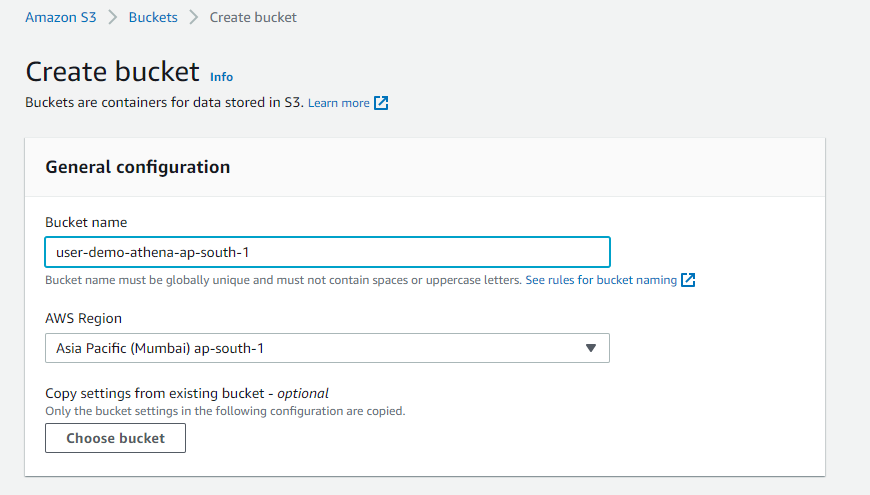
**Click save**



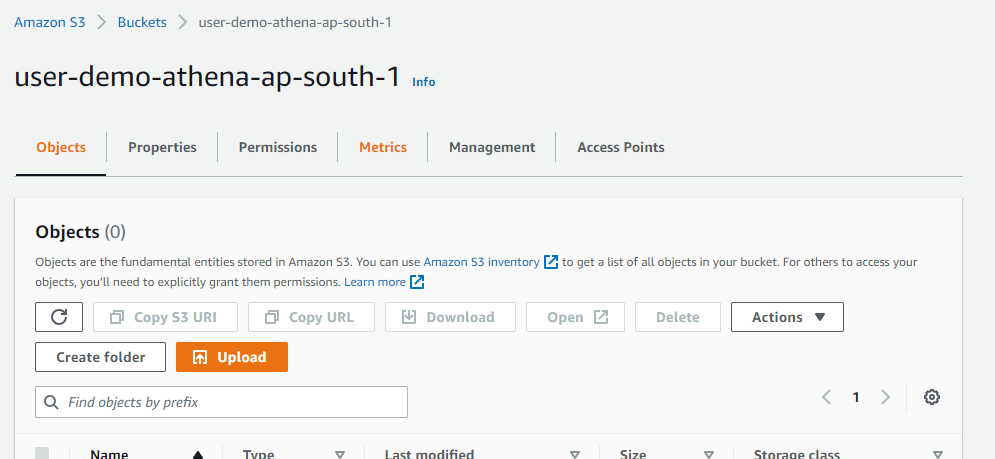
**Click manage**

**Specify location**

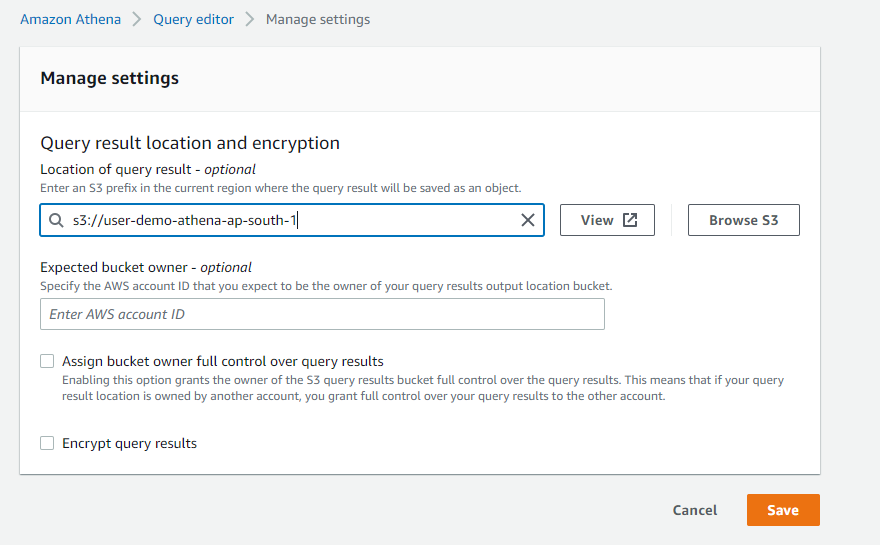
**First create s3 bucket**

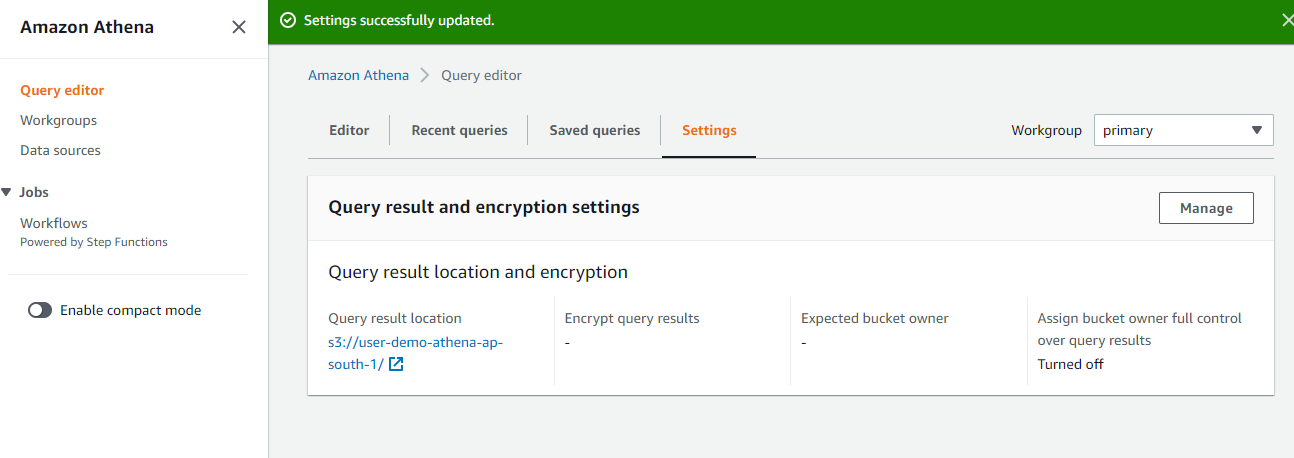


**Bucket has been created**

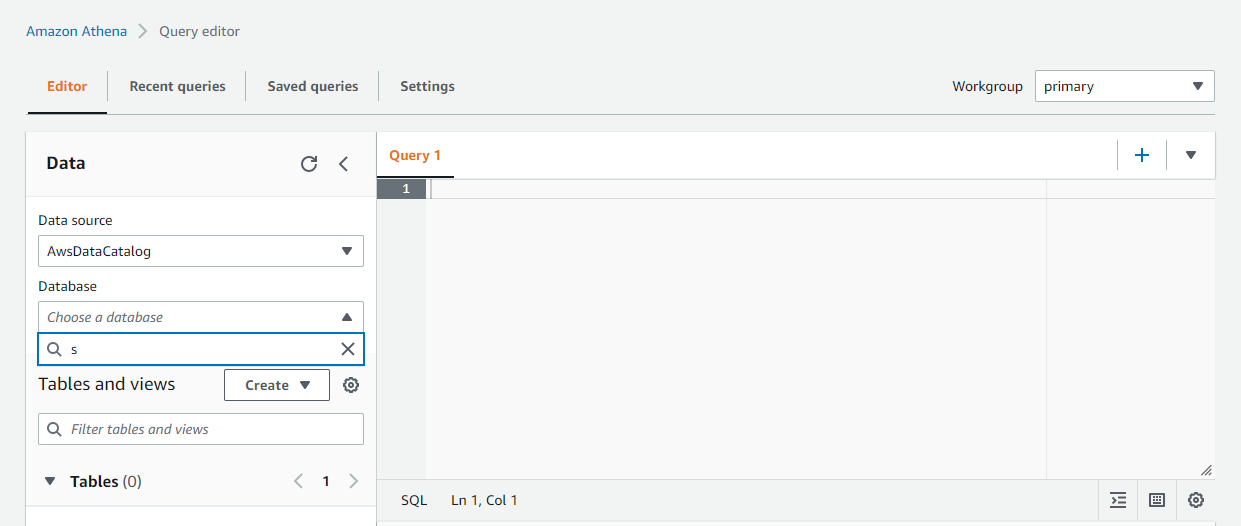


**Copy bucket name and paste in athena**

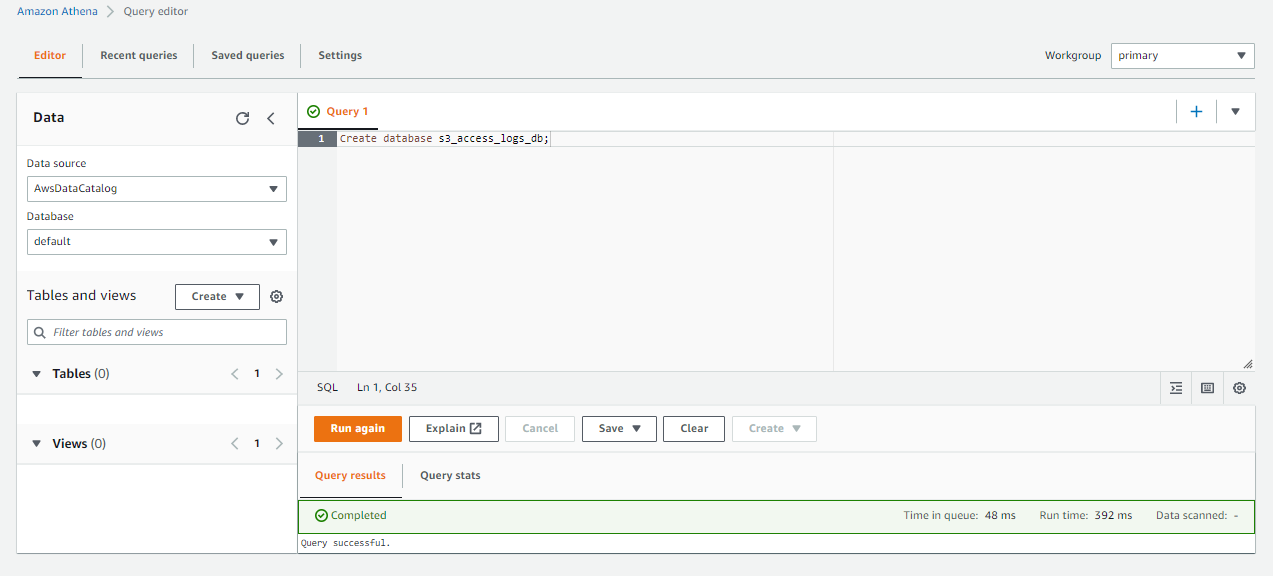


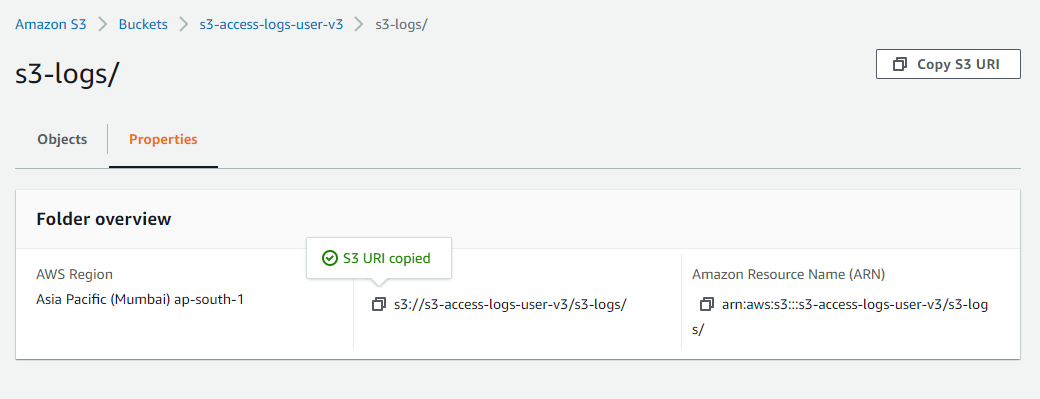


**Go back to athena dashboard**

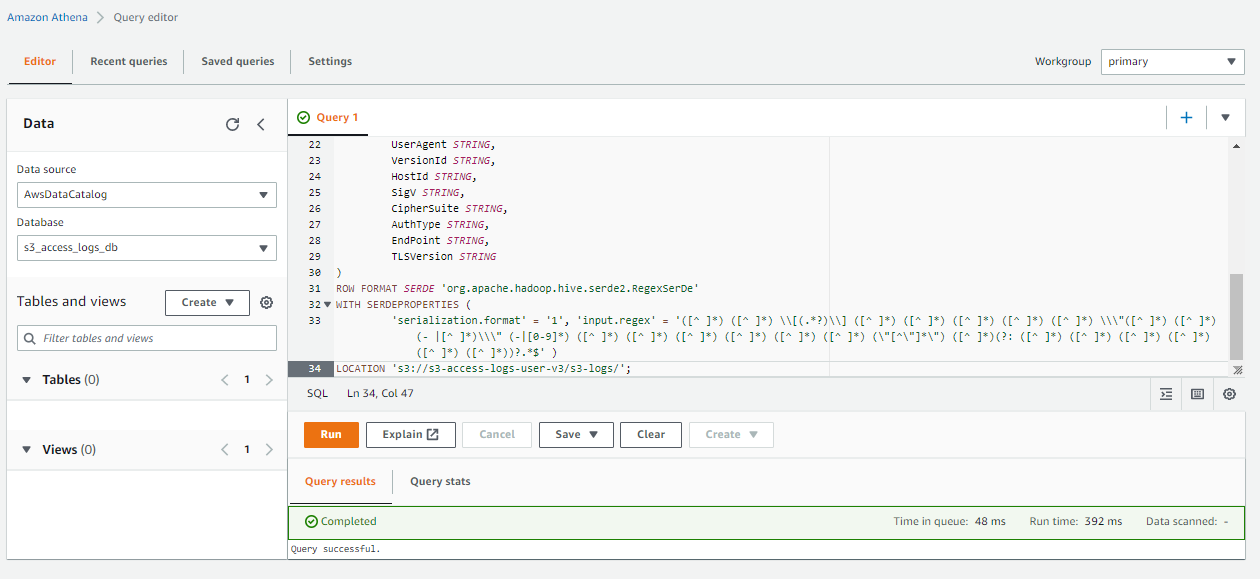


**Run code**





**Again, run the code**



**Query is run**

