**S3**

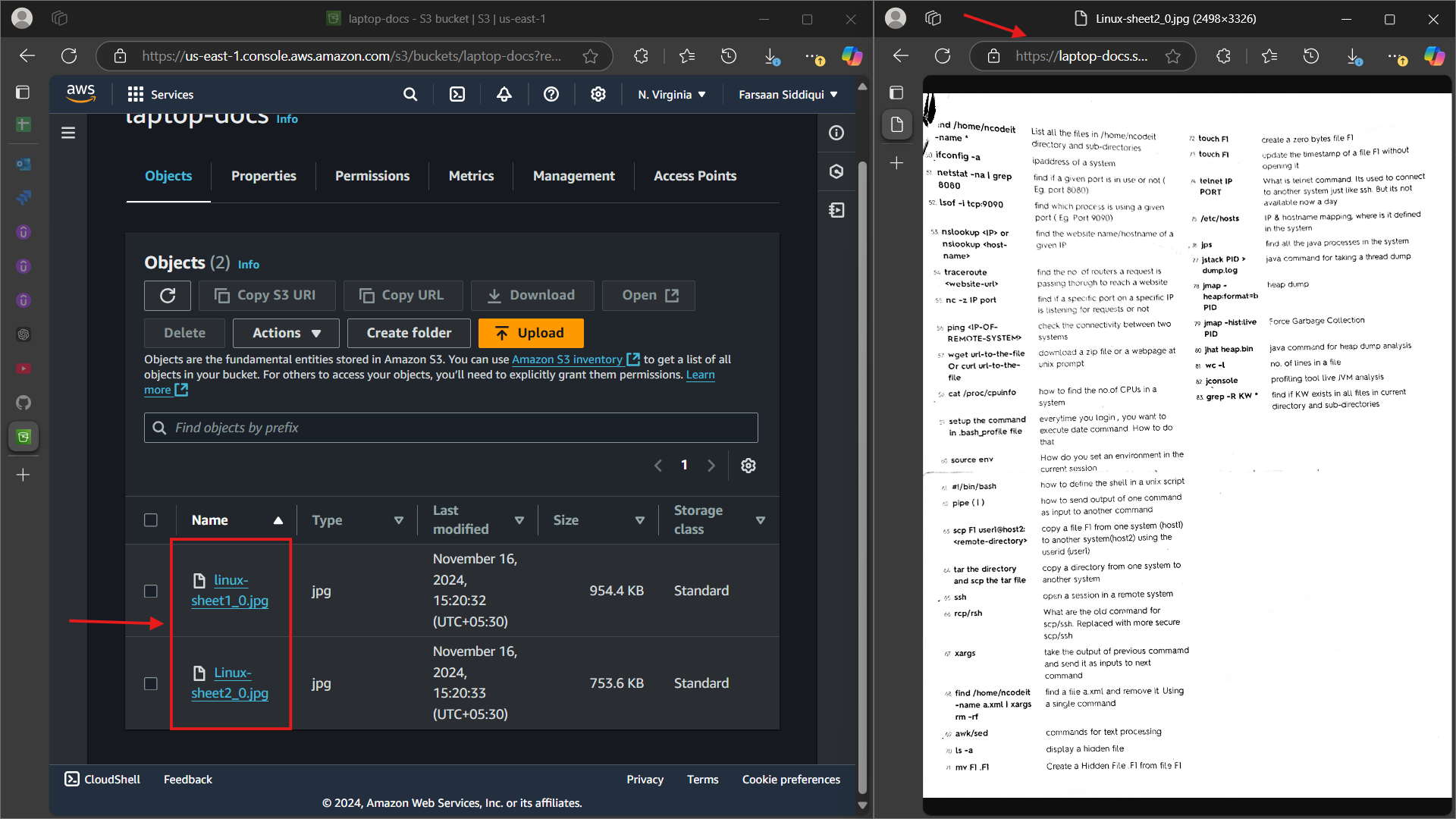
1. **Create s3 bucket and upload some objects to s3.**

\*go to s3 and create new bucket

\*select the created bucket and upload files from local machine those are called objects after uploaded

\*make sure the permissions are given as public accessable

\*copy the object url and test it in new window

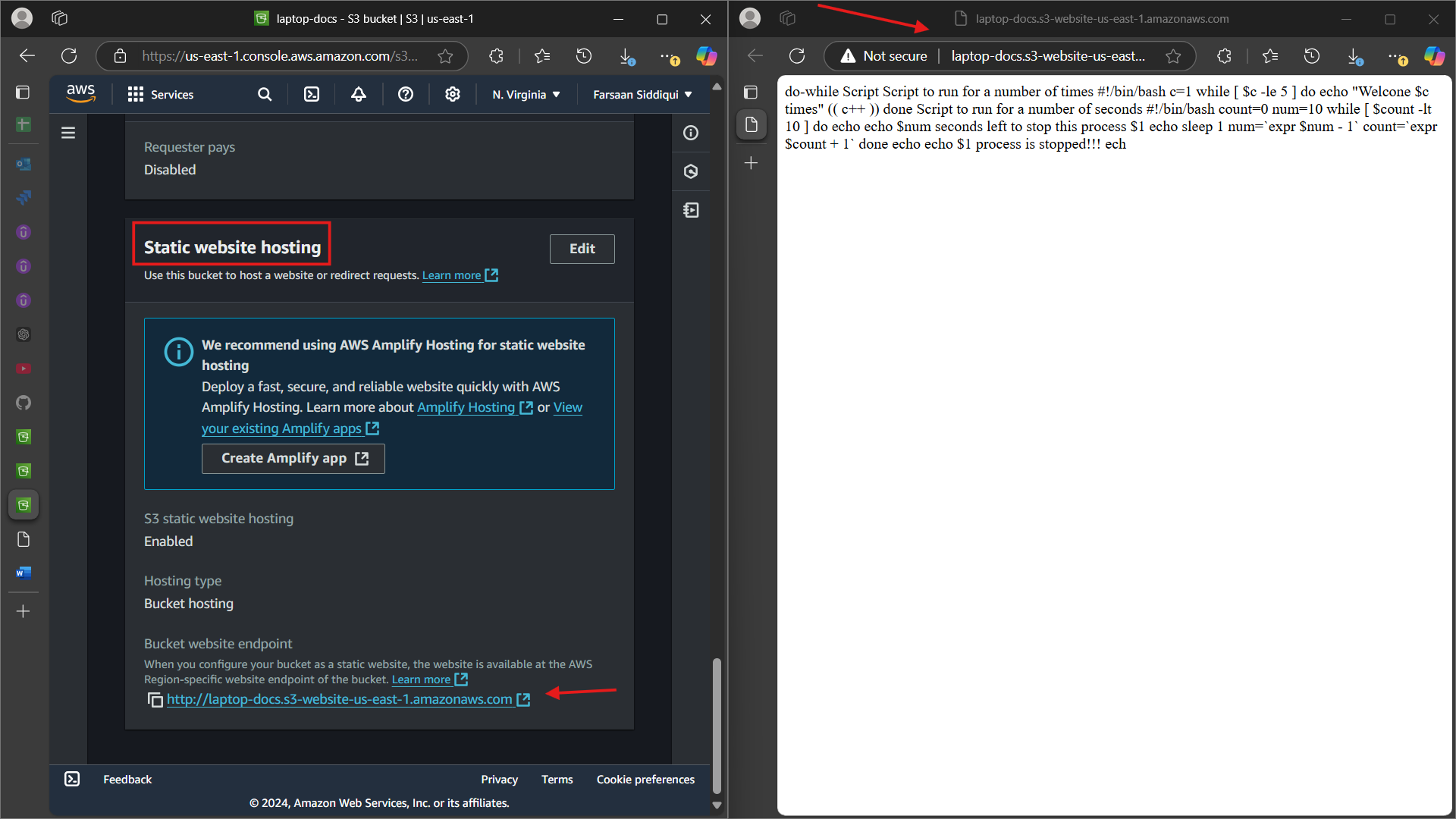
****

**2) Deploy static website in s3 bucket.**

\*go to bucket and select properties scrll all the way down edit static website hosting and add the web page name

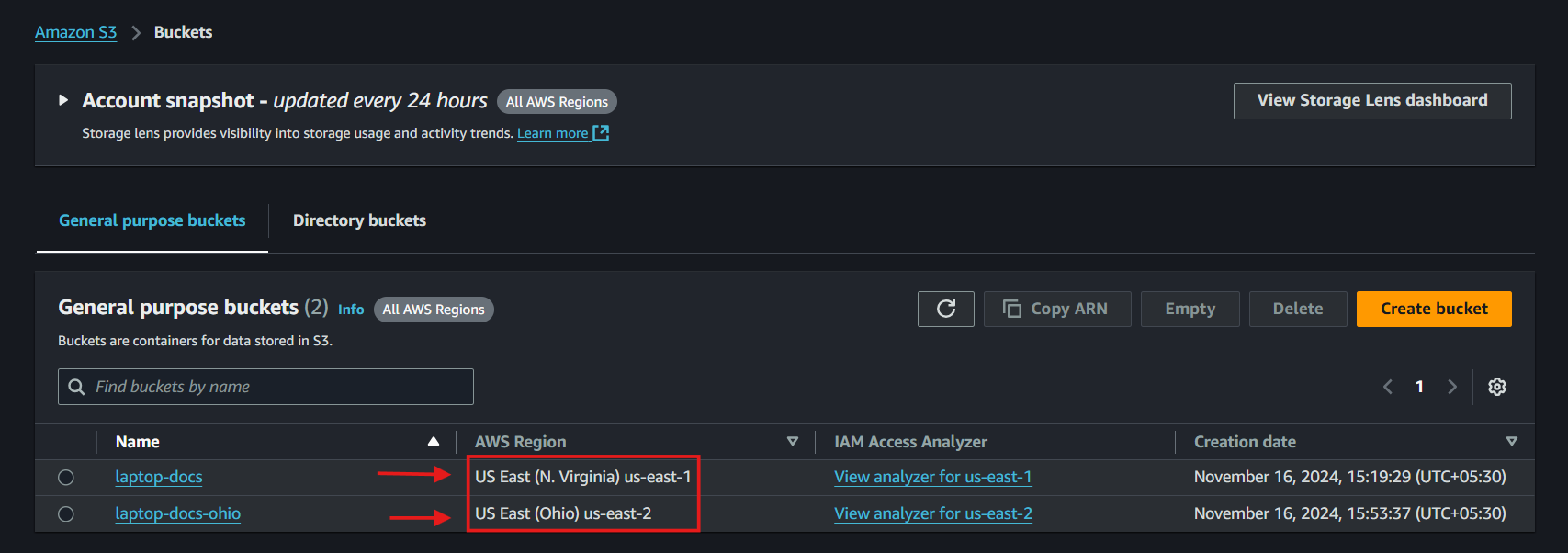
\*go to objects and upload the web page filr there with the same name and allow acl permission as public

\*now with the bucket url test the page

****

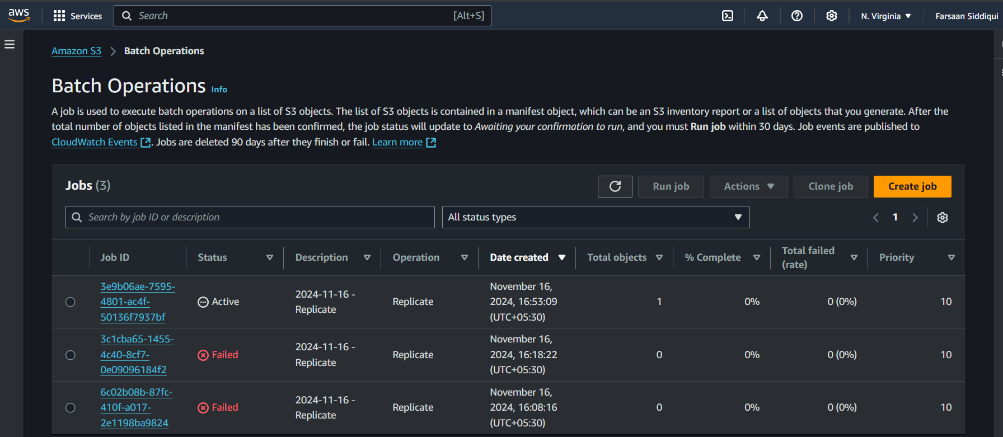
**3) Enable cross region replication on s3 buckets.**

\*create two buckets in different region



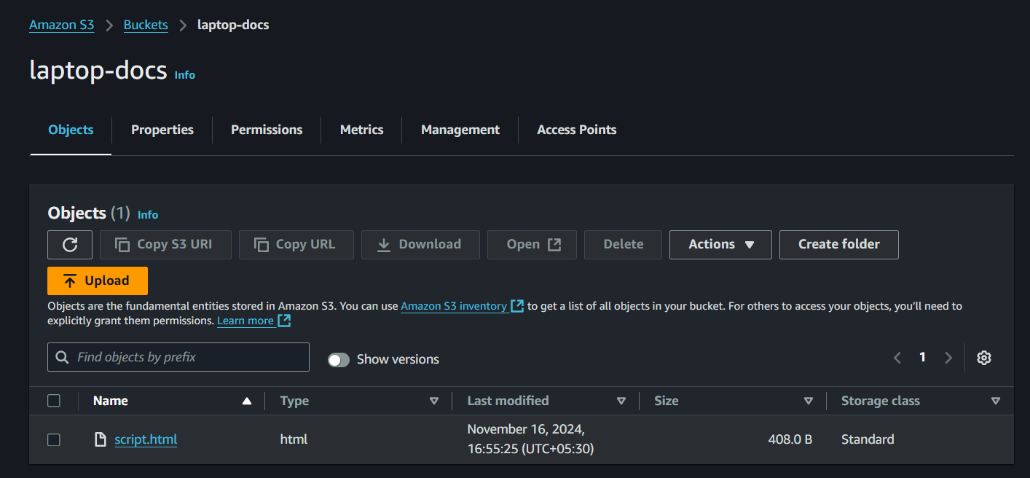
\*select the source bucket and go to management>create relication rule and follow the steps

(at the point of role just select create new role and it will create a json format role )

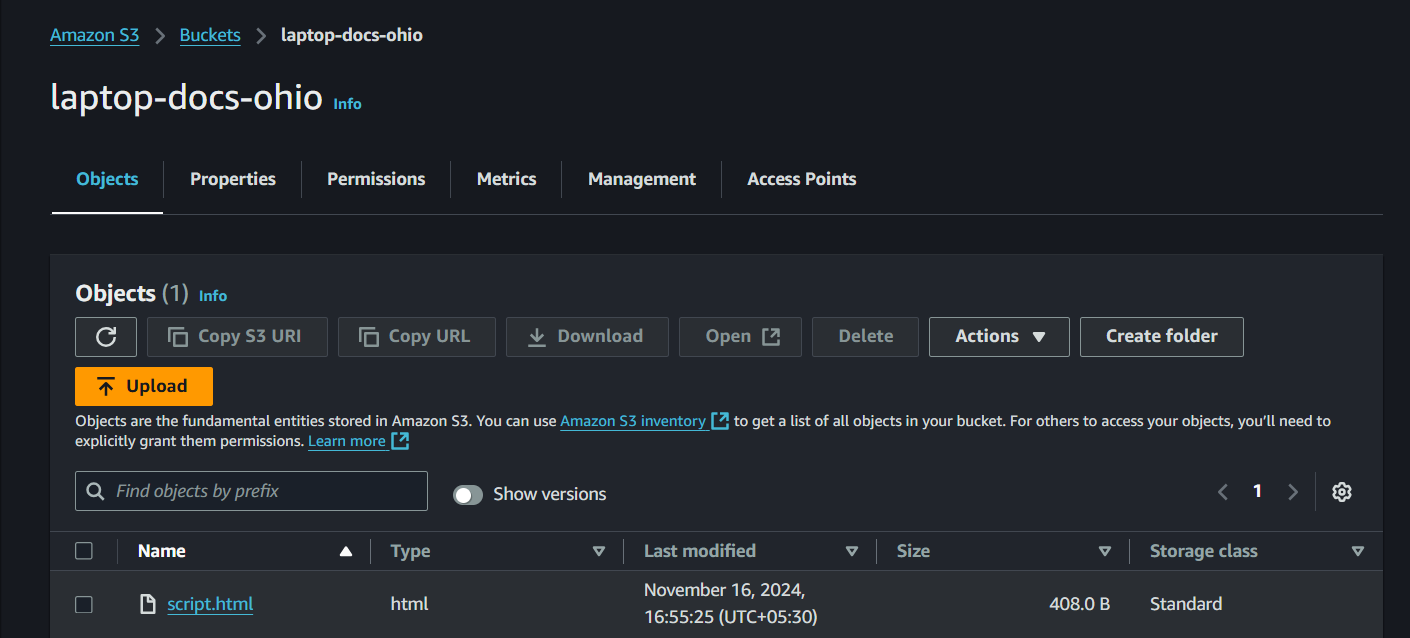


\*now add a file in source bucket and check the destination bucket if the file is replicated or not.

>>source bucket

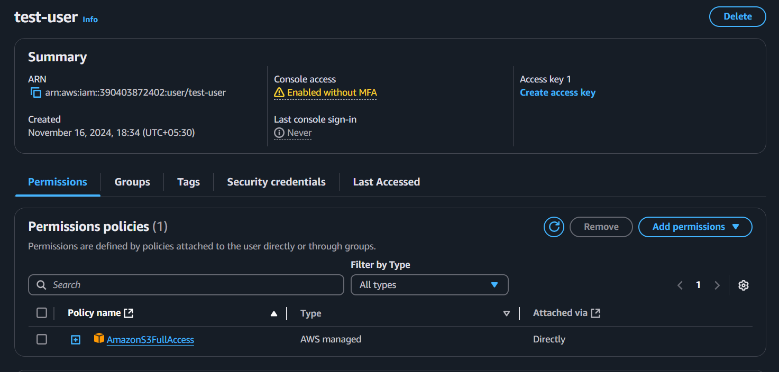
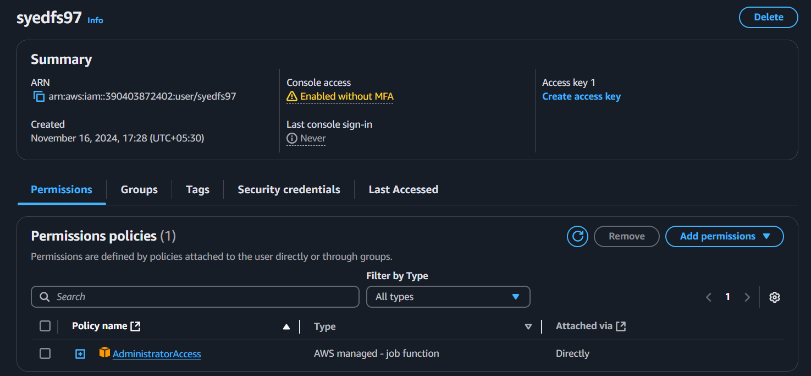


>>destination bucket



**4) Configure bucket policy,only Admin user can see the objects of s3 bucket.**

\*creating two users 1.with admin access 2.with full s3 acess.

\*now add the policy to bucket for which only admin can access the objects

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Deny",

"Principal": "\*",

"Action": "s3:\*",

"Resource": [

"arn:aws:s3:::laptop-docs-ohio",

"arn:aws:s3:::laptop-docs-ohio/\*"

],

"Condition": {

"StringNotEquals": {

"aws:userid": "arn:aws:iam::390403872402:user/syedfs97"

}

}

},

{

"Effect": "Allow",

"Principal": {

"AWS": "arn:aws:iam::390403872402:user/syedfs97"

},

"Action": "s3:\*",

"Resource": [

"arn:aws:s3:::laptop-docs-ohio",

"arn:aws:s3:::laptop-docs-ohio/\*"

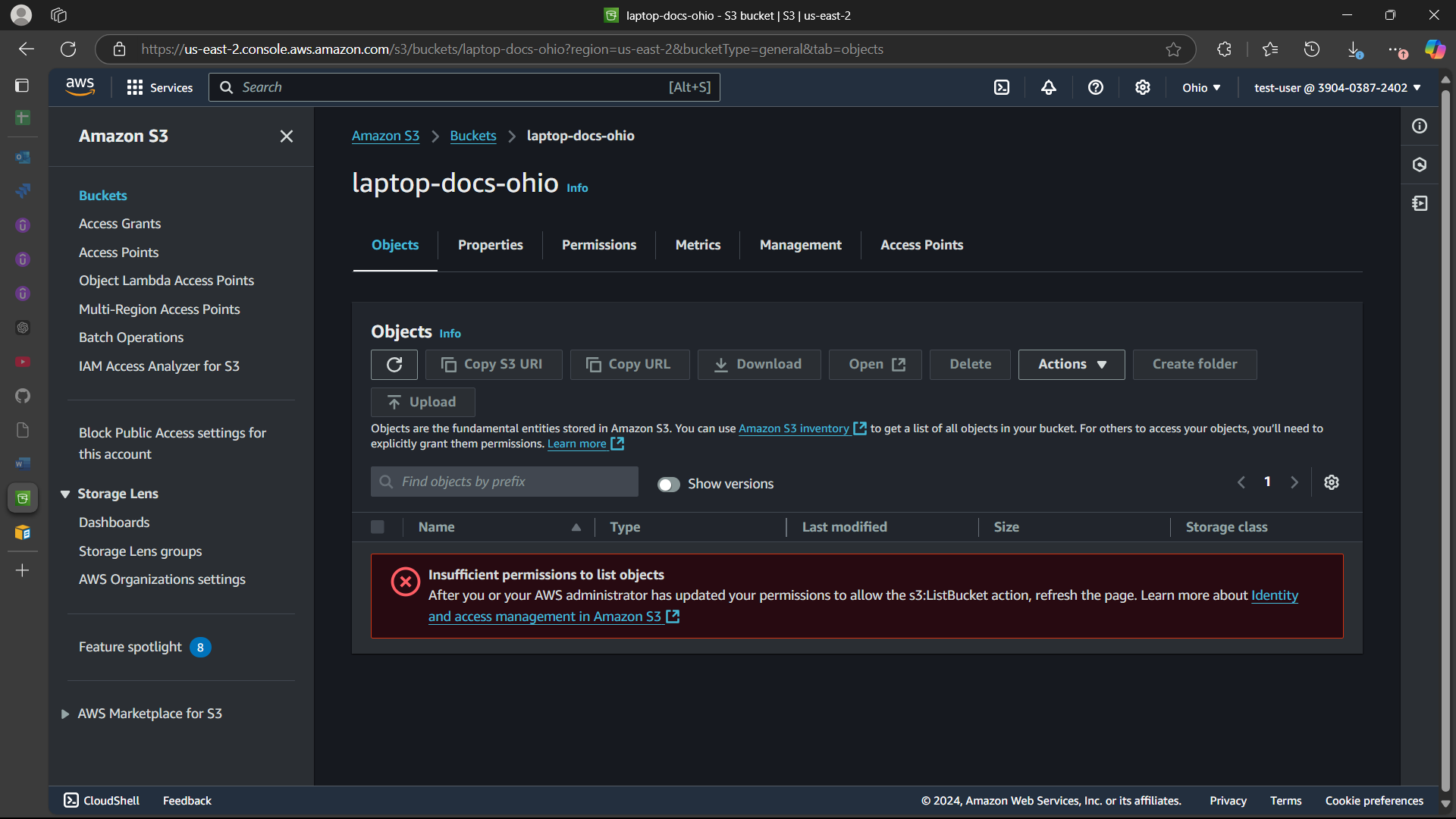
]

}

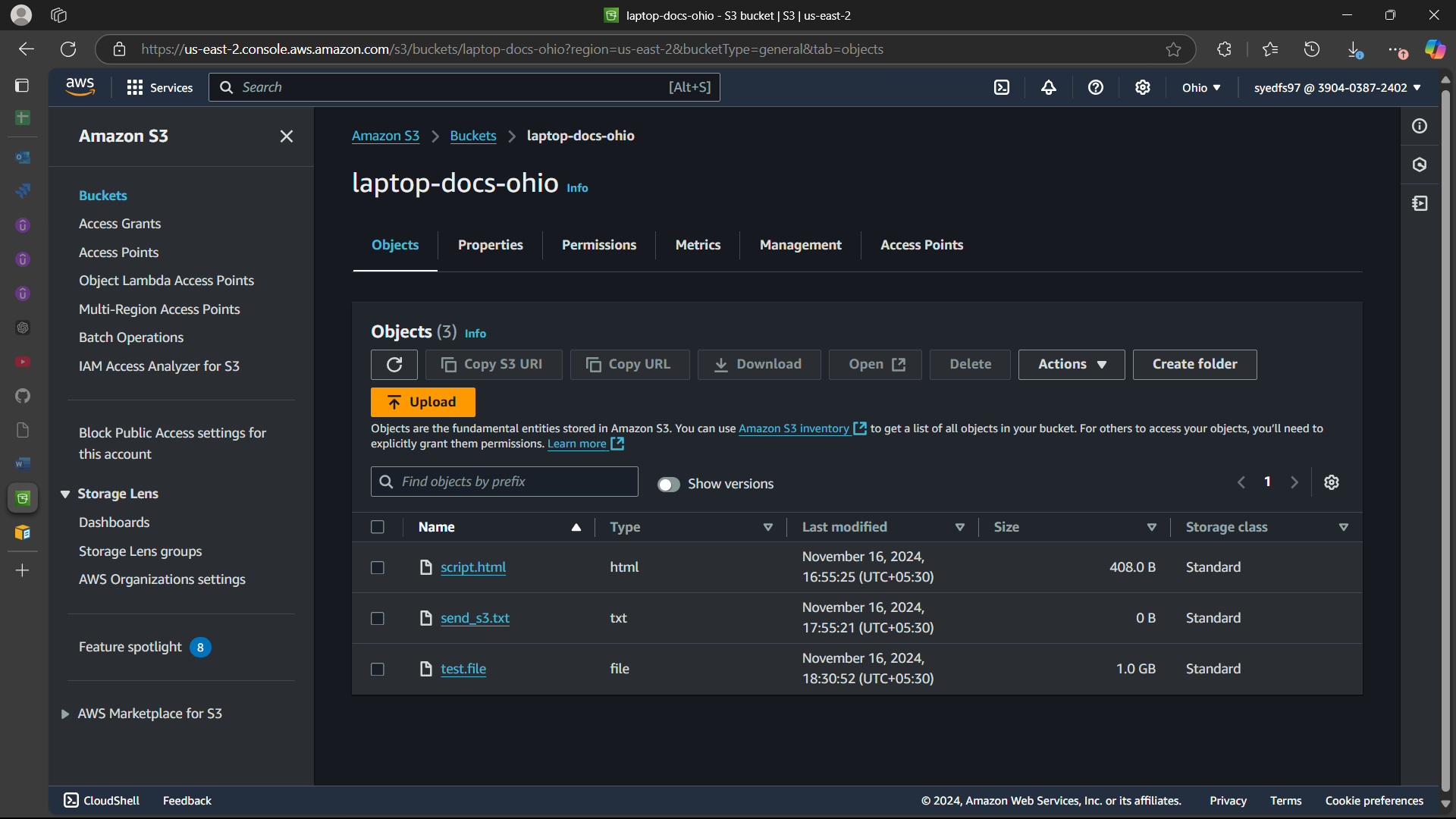
]

}

\*now test with both the accounts to access the objects of bucket

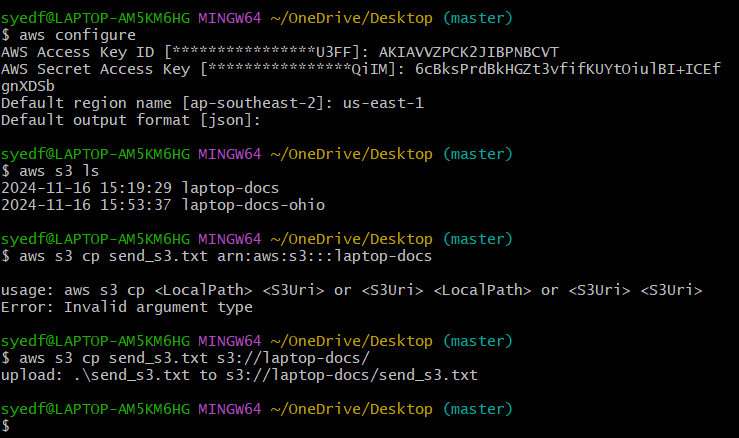


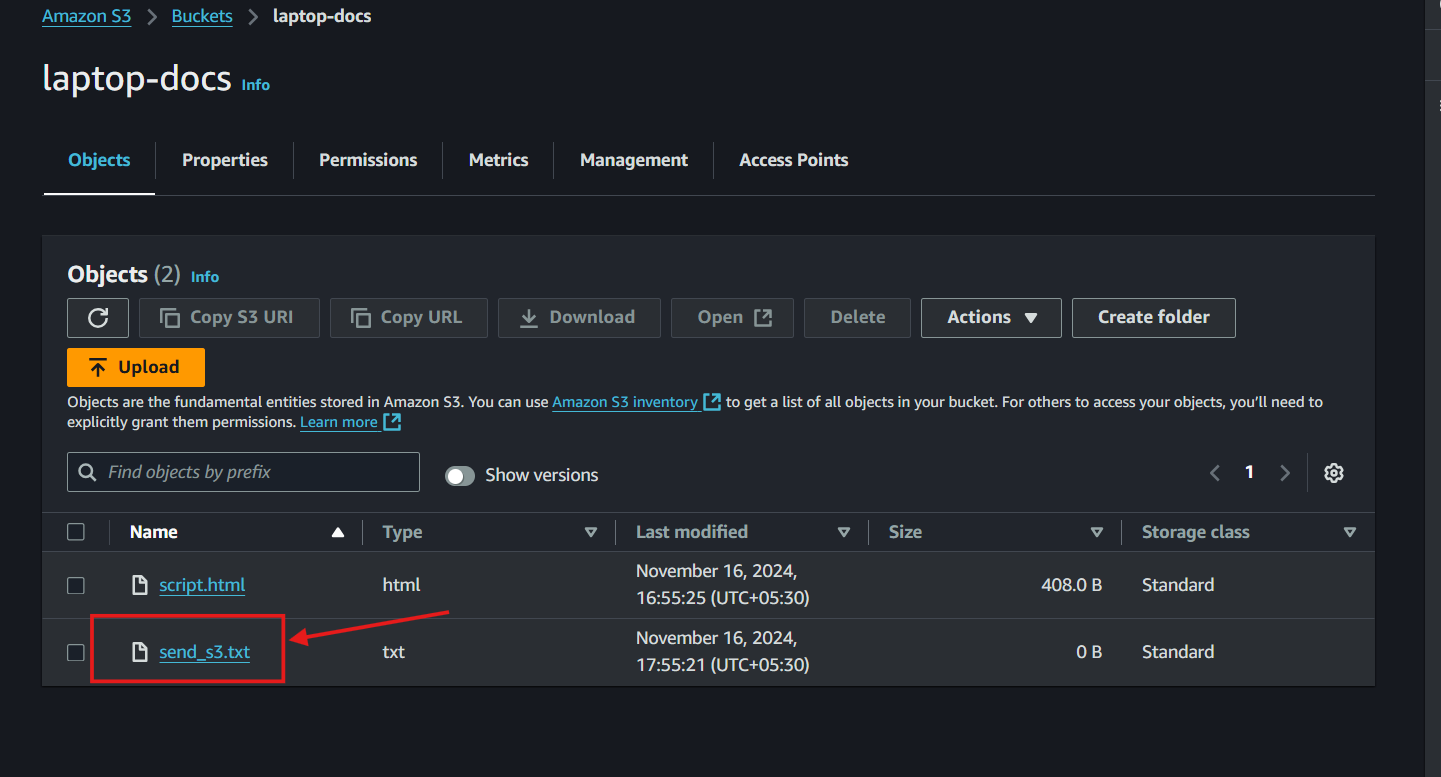
\*access denied from test-user with full s3 access



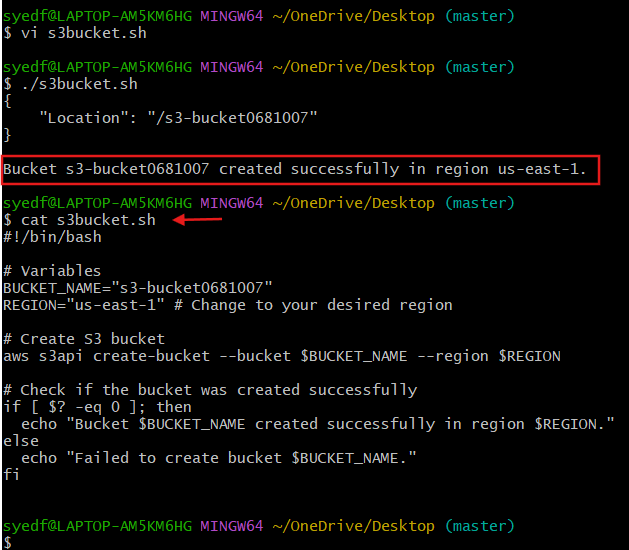
\*syedfs97 with full admin access can see the objects of bucket

**6) Push some objects in s3 using AWS CLI.**

****

****

**7) Write a bash script to create s3 bucket.**

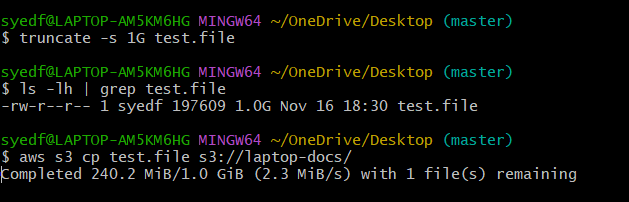
****

****

**8) Upload one 1 gb of file to s3 using cli.**

\*createing 1gb file

\*uploading it to s3 bucket

****

\*checking the bucket

