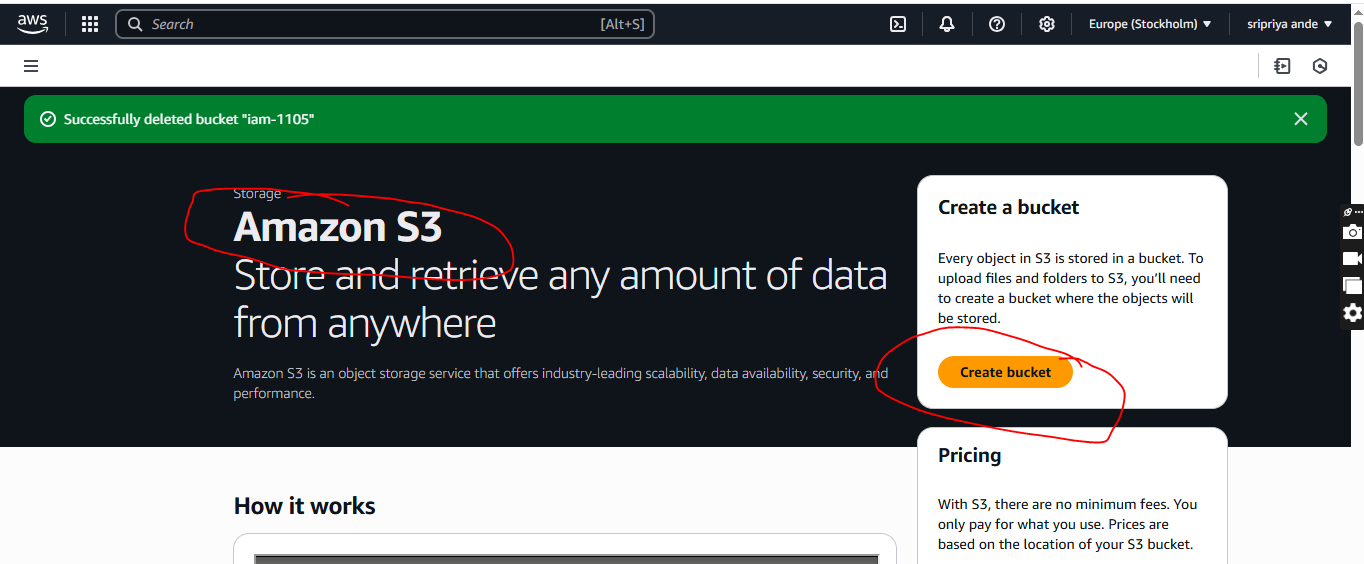
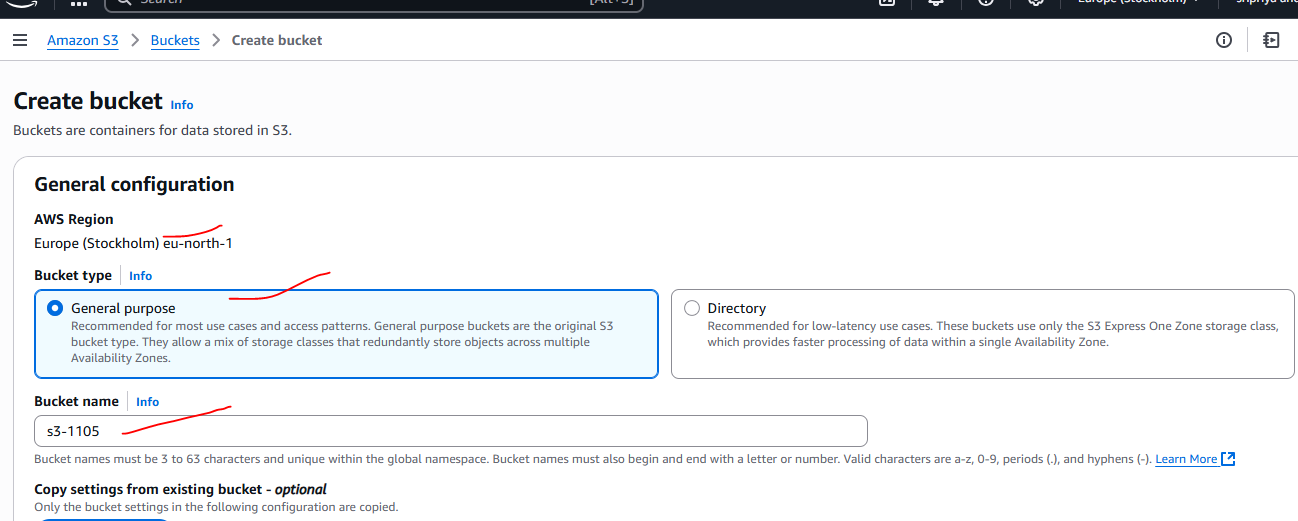
**13/05/2025**

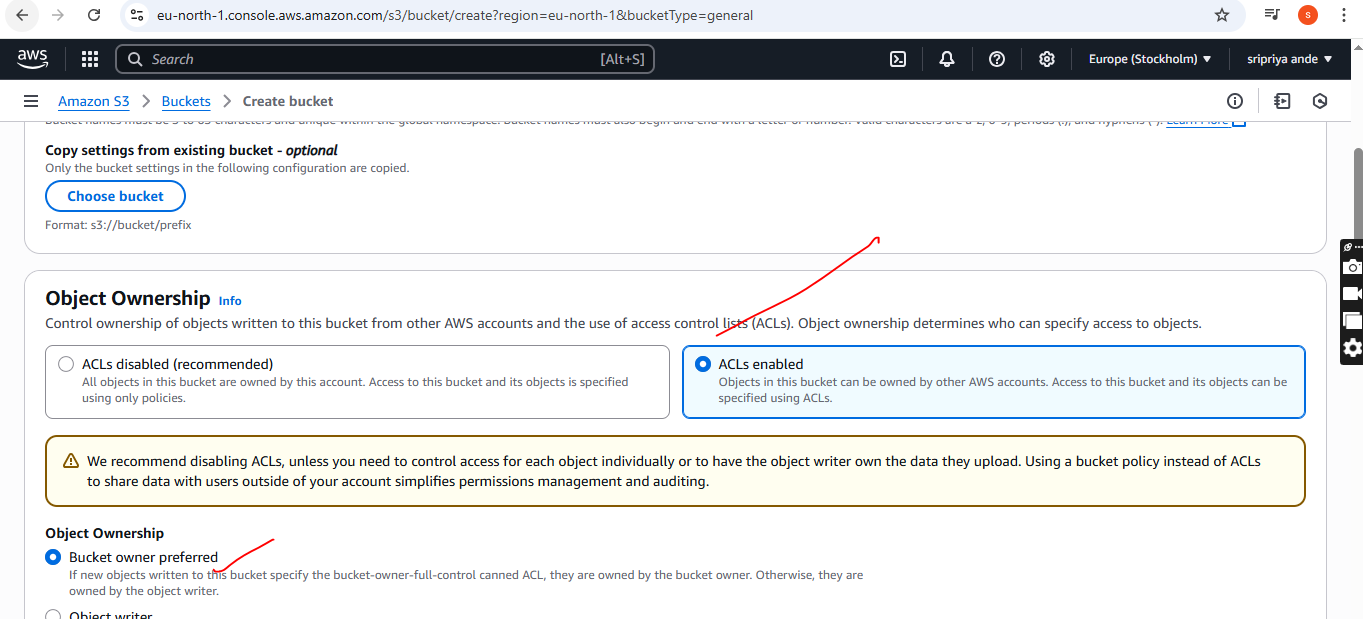
**Task on s3:  
================**

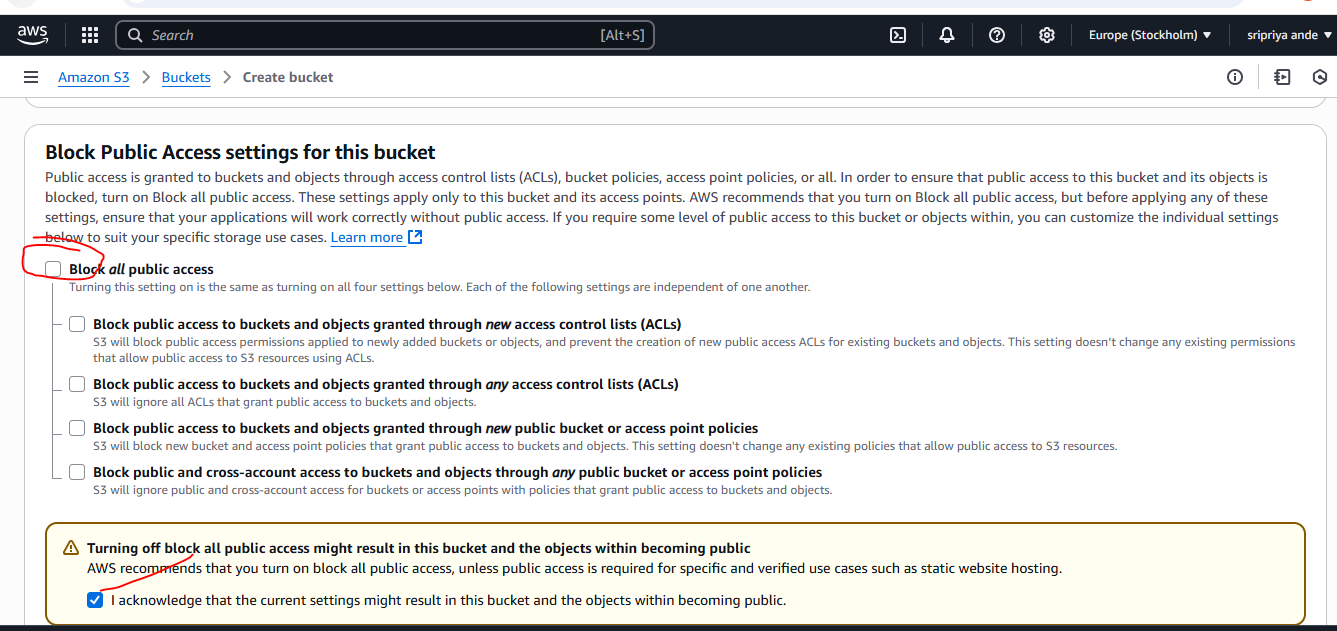
1. **Create s3 bucket and upload some objects to s3.**

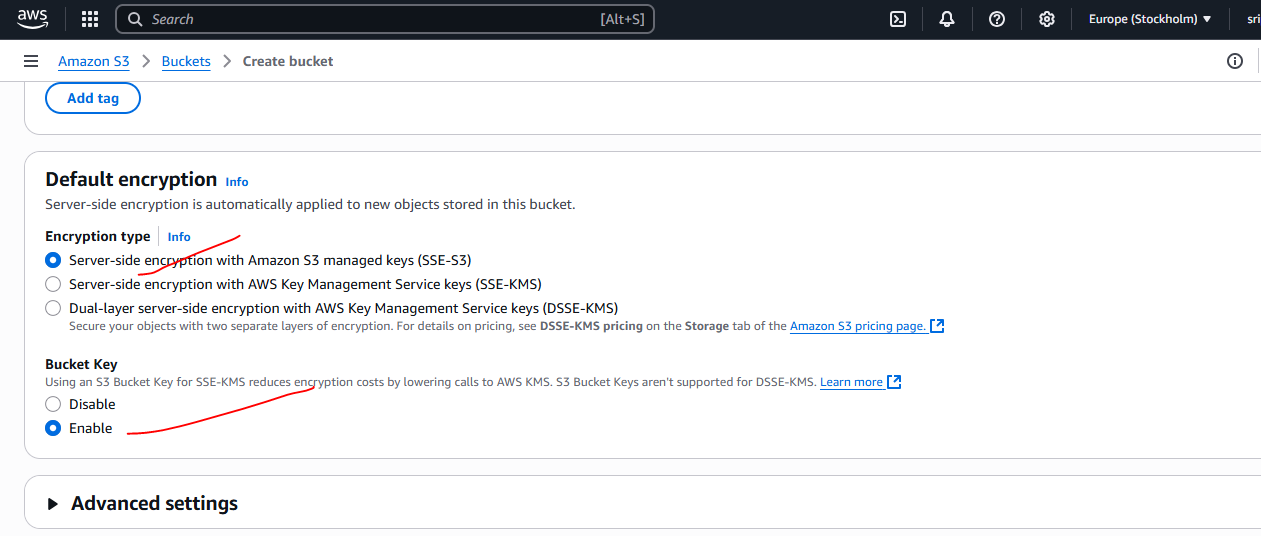
* Open Aws console--->serach for s3 bucket
* Click Create s3 bucket
* Select regio
* bucket type as general purpose
* Bucket name should be unique
* Object ownership as ACL’s enable (if we choose disable we won’t have access to object)
* unCheck box
* Click on Create bucket
* Now bucket is created then click on add files and upload any document.
* Now object has been uploaded
* Click on the object you find url copy and paste in browser
* If it shows any error
* Go to object and make public using url and save
* Now refresh page you can see the uploaded object

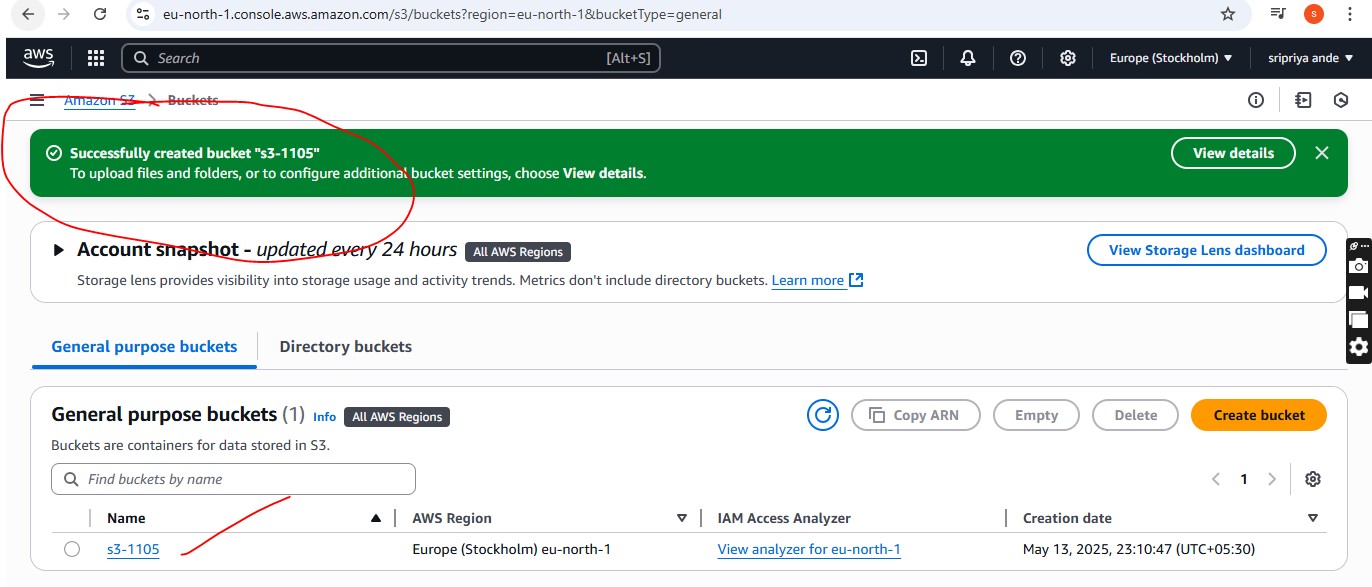




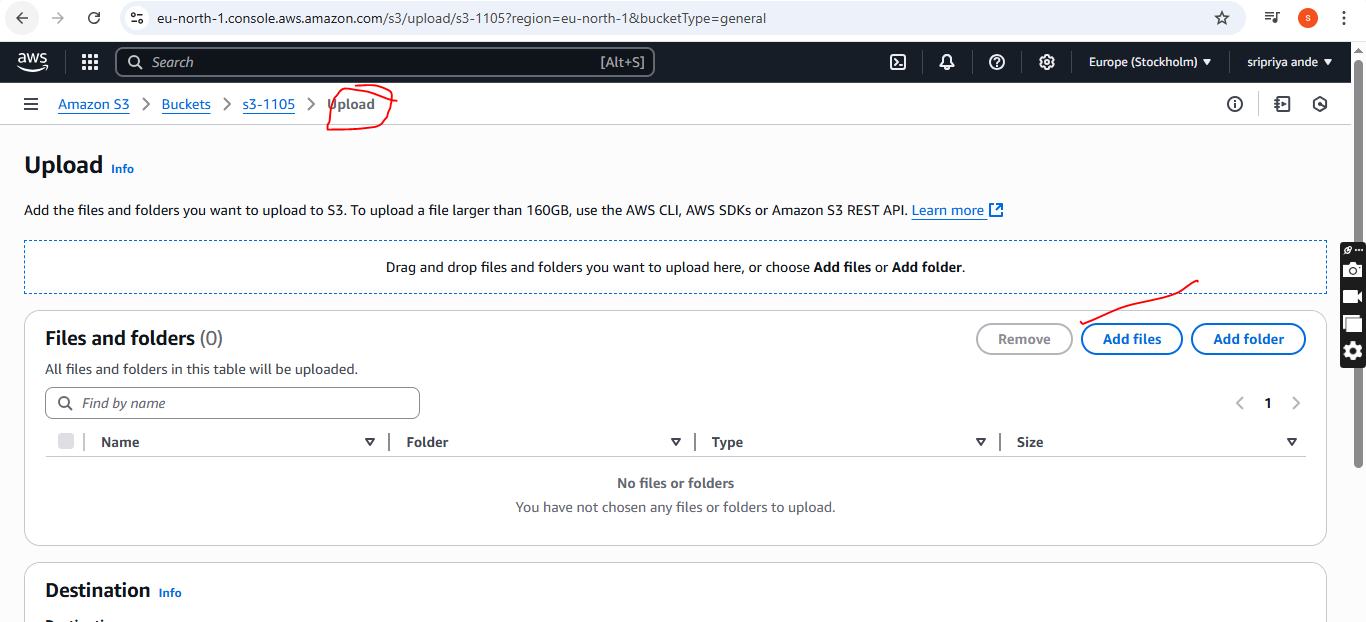


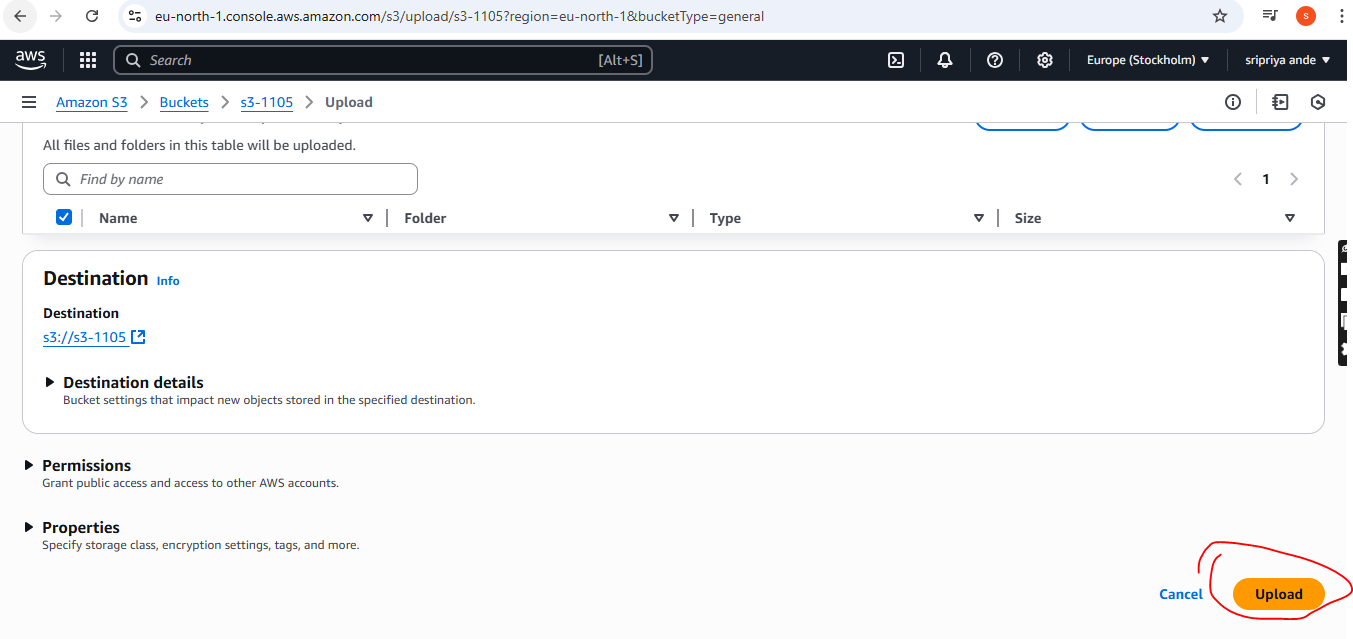


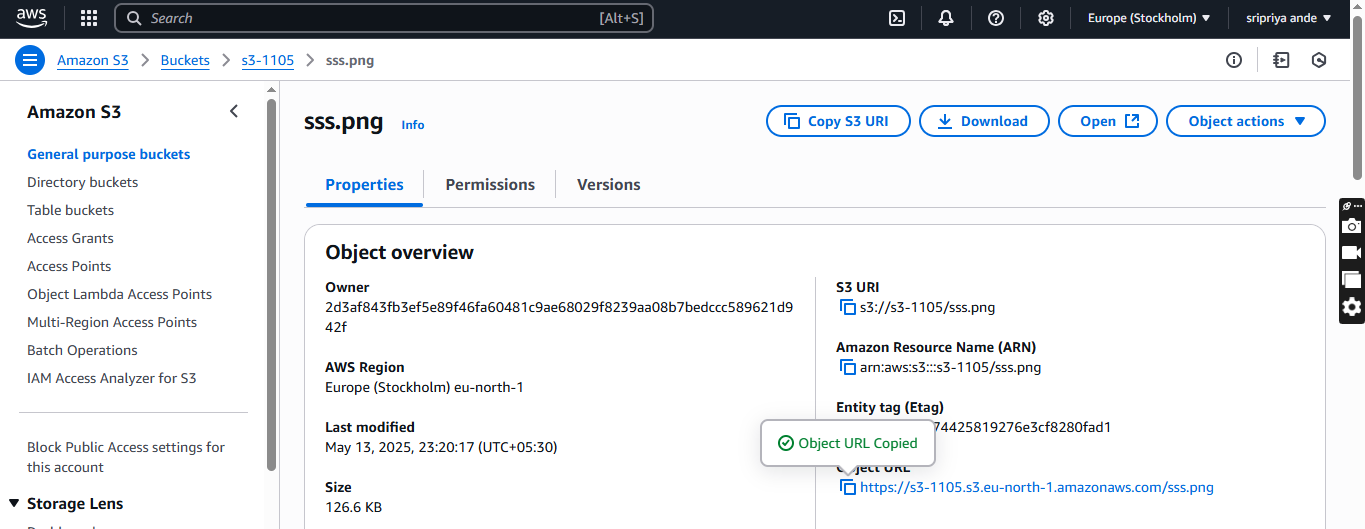


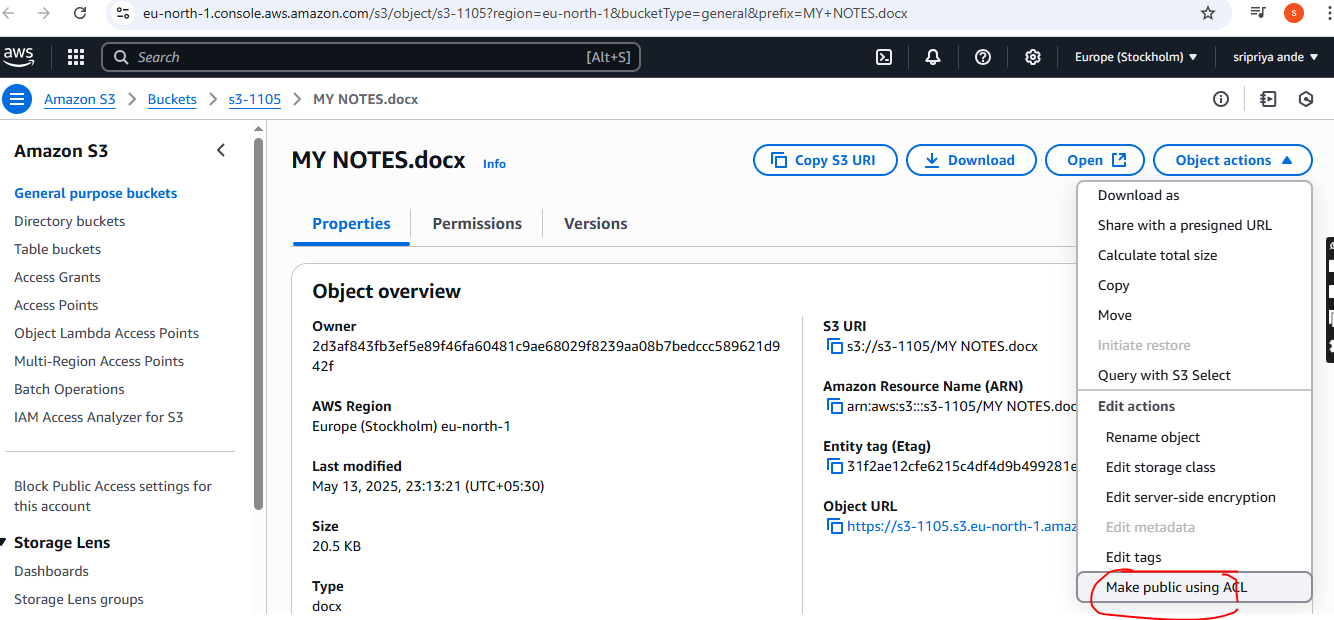
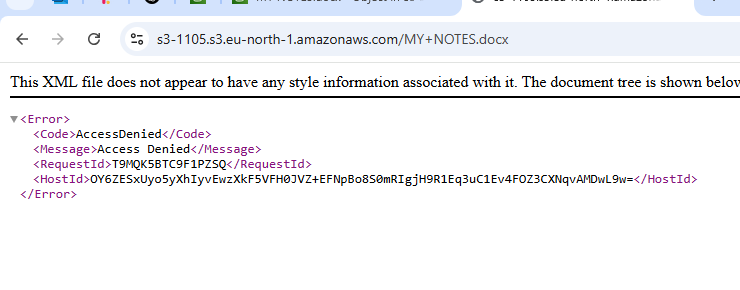


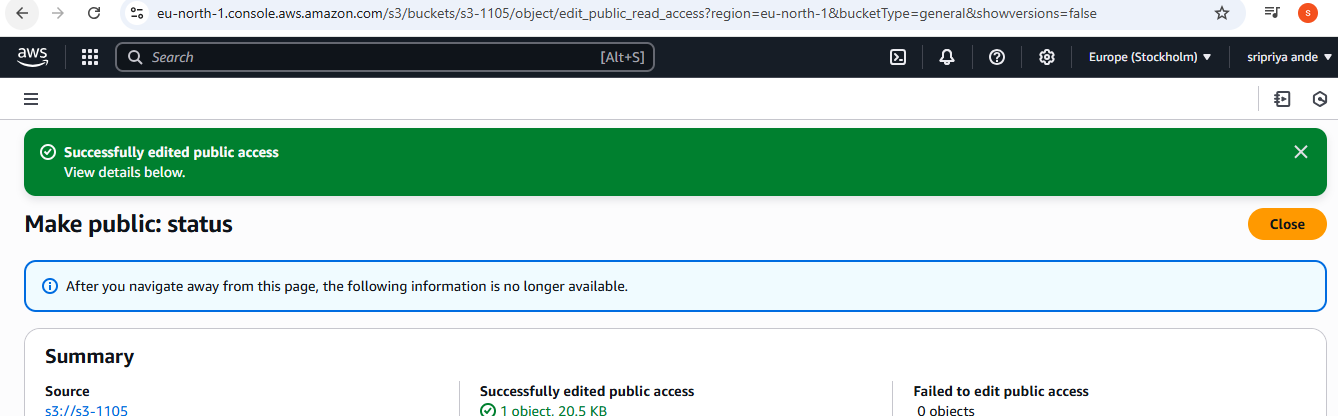


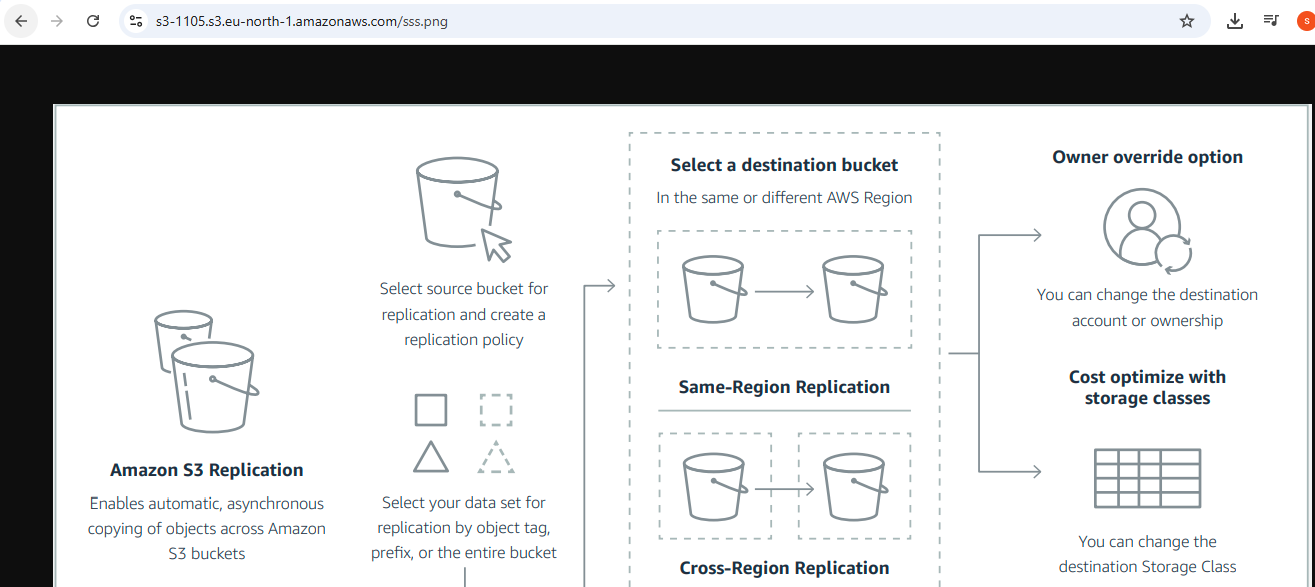












1. **Deploy static website in s3 bucket**.

* Go to s3 bucket
* In s3 bucket go to properties(scroll down)
* You will find static website hosting
* Now it is disable mode click on and change it to enable
* Set as host type is Host a static website.
* Now go to git bash and create 2 files with .html one for index document and error document
* Select created files in s3 page
* Paste this policy in json in permission--->bucket policy

{

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

"Statement": [

{

"Sid": "PublicReadGetObject",

"Effect": "Allow",

"Principal": "\*",

"Action":"s3:GetObject",

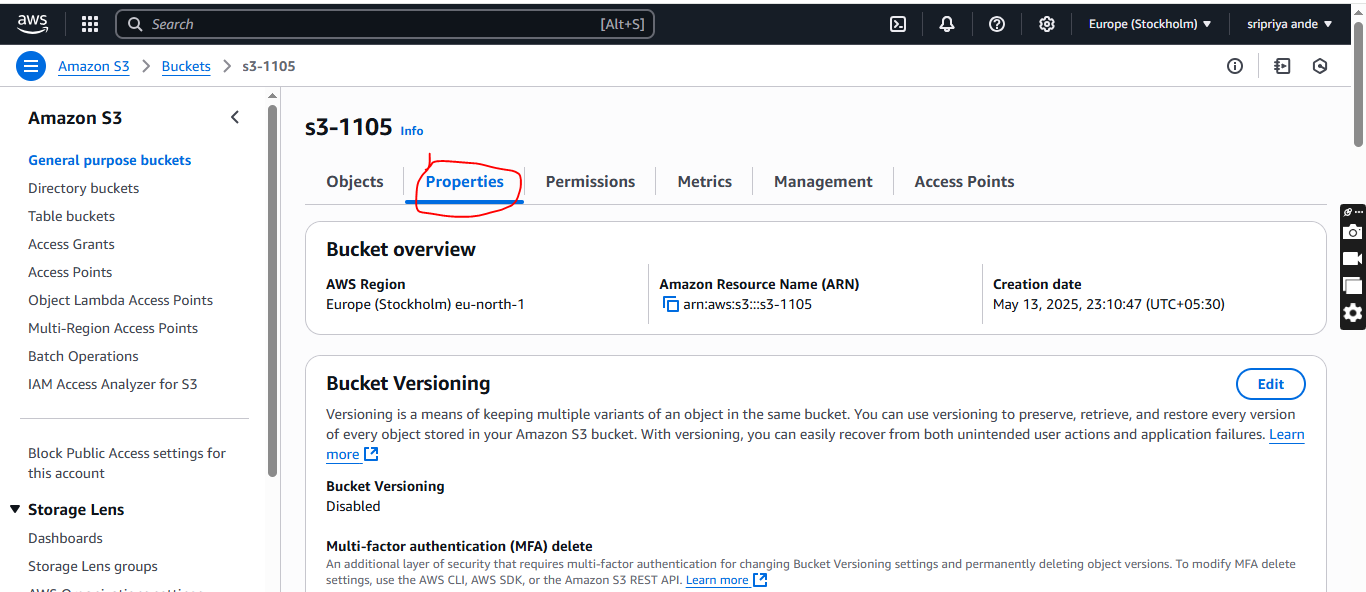
"Resource":"arn:aws:s3:::s3-1105/\*"

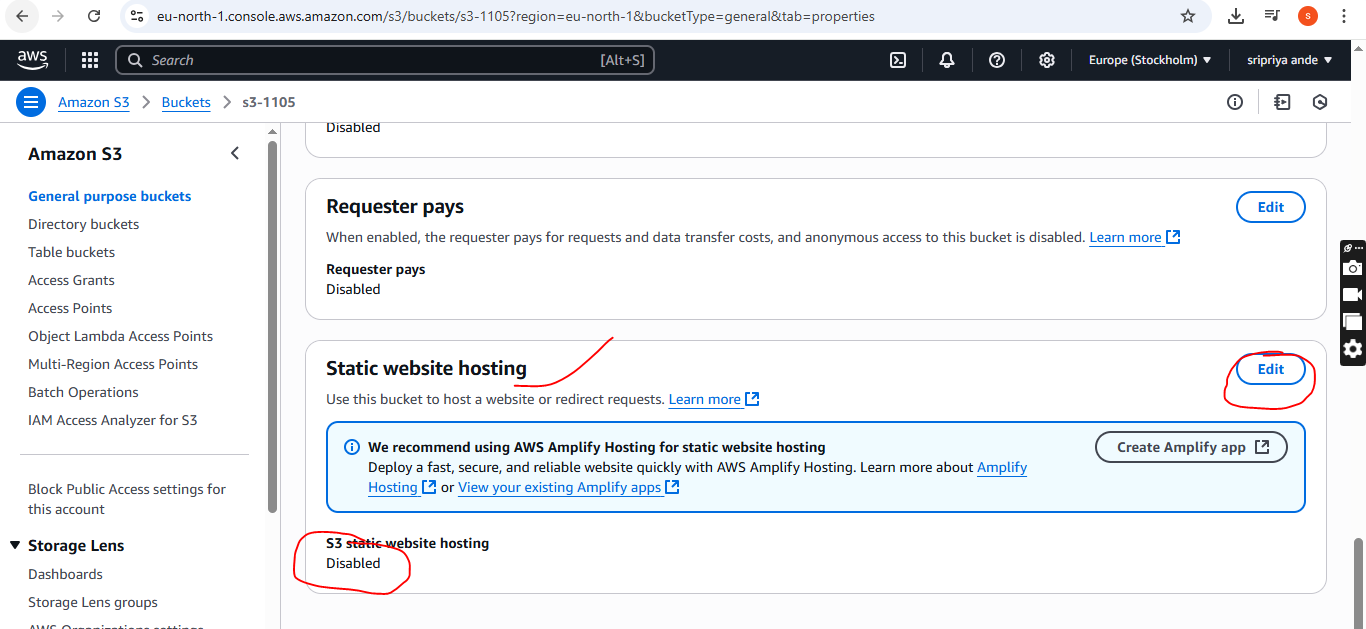
}

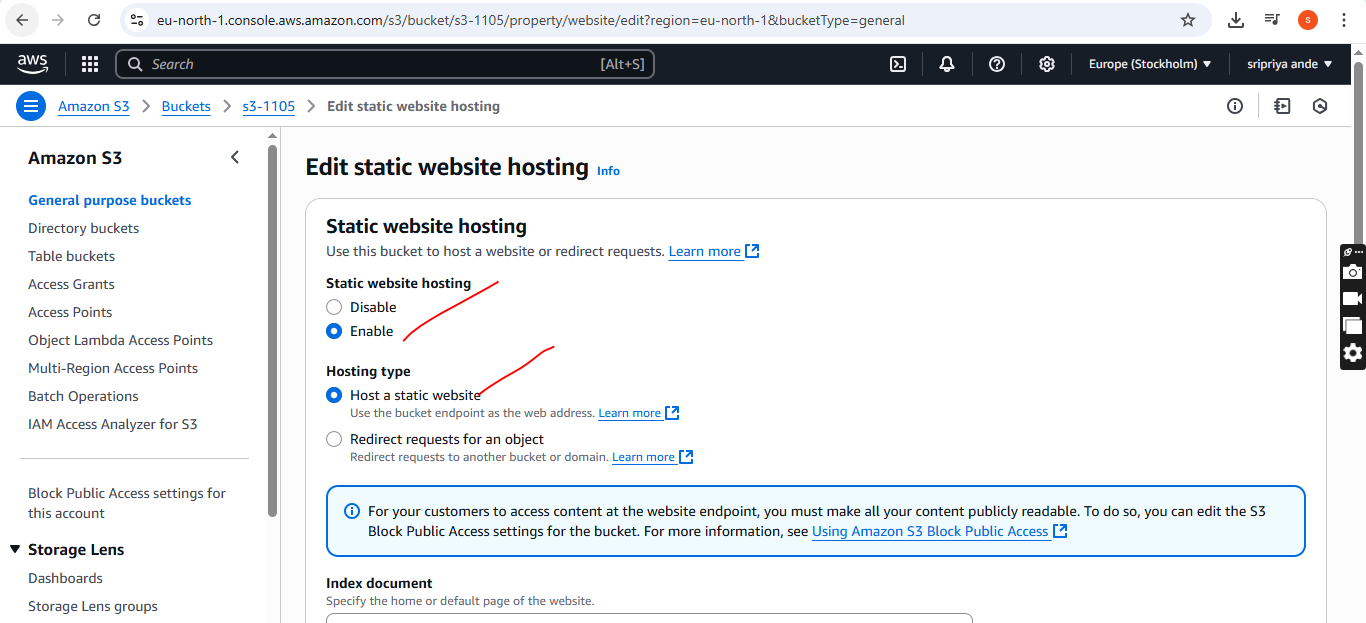
]

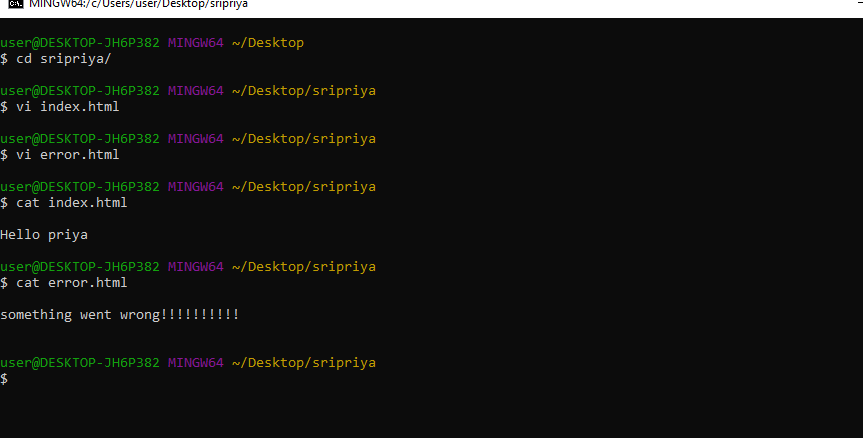
}

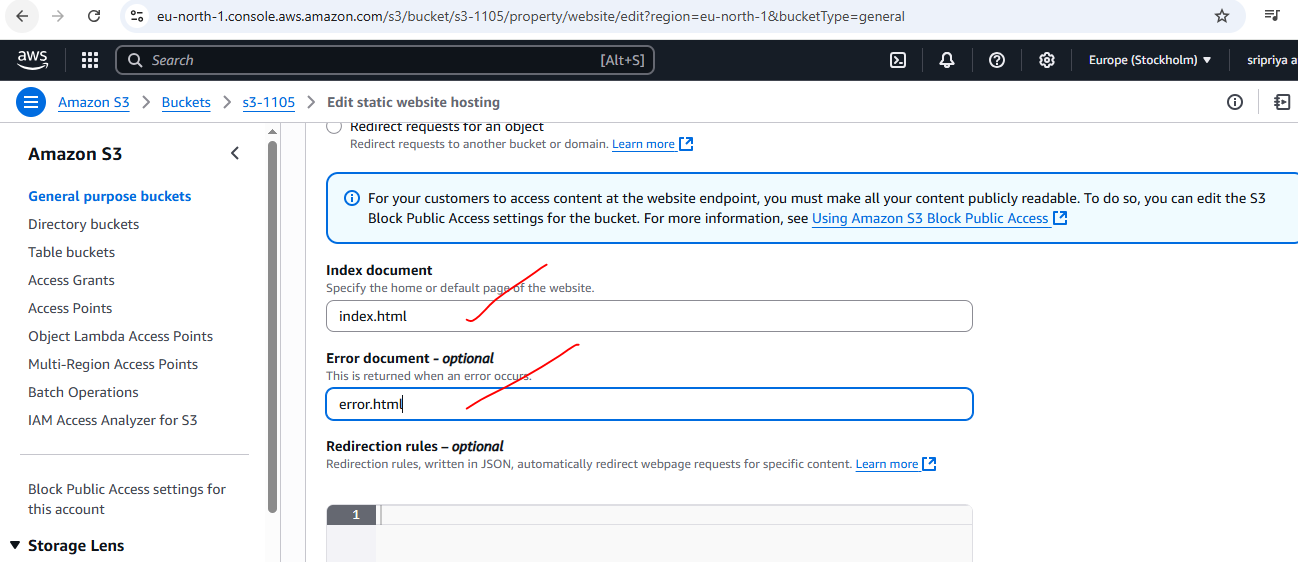
* Save changes
* Now add both files in s3 bucket --->upload
* NOw in s3 bucket properties we can see bucket URL
* Copy and paste in browser
* You will see the output

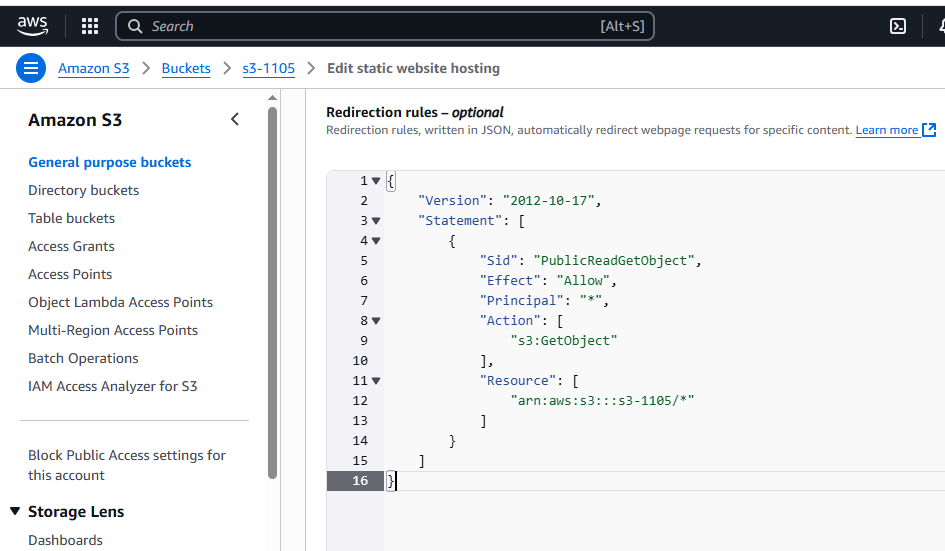


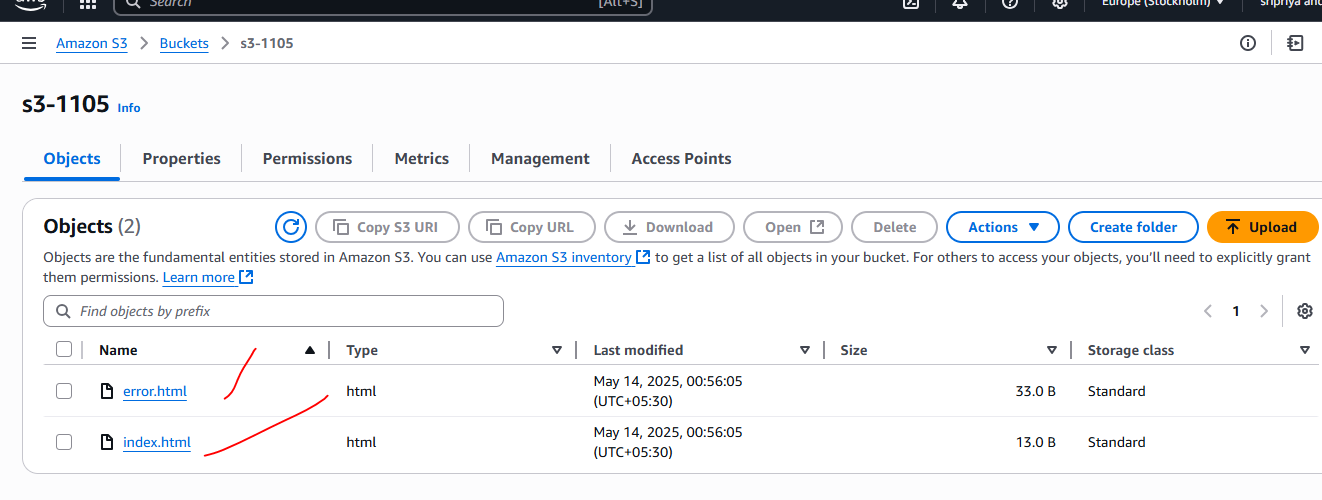


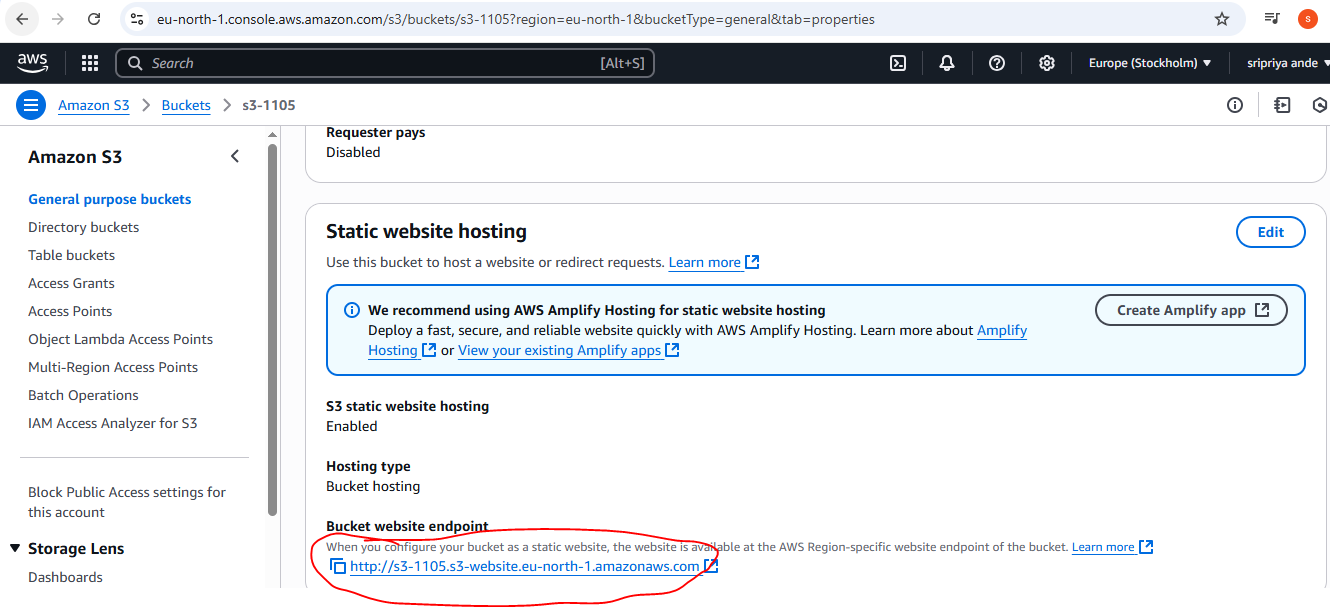


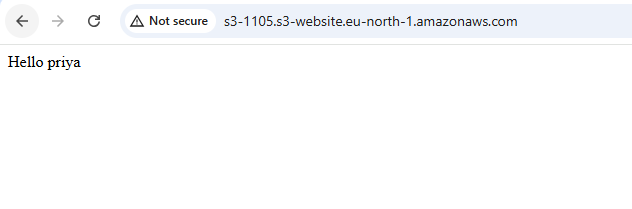












1. **Enable cross region replication on s3 buckets.**

step 1 Create Source and Destination Buckets

Go to the S3 Console.

Create a source bucket (e.g., sourcebucket-sri05 in eu-north-1 and enable versioning.

Create a destination bucket (e.g., destinationbucket-priya05 in us-east-2 another region and enable versioning.

step 2: Enable Replication on Source Bucket

Open the source bucket.

Go to the “Management” tab.

Scroll to “Replication rules” and click “Create replication rule".

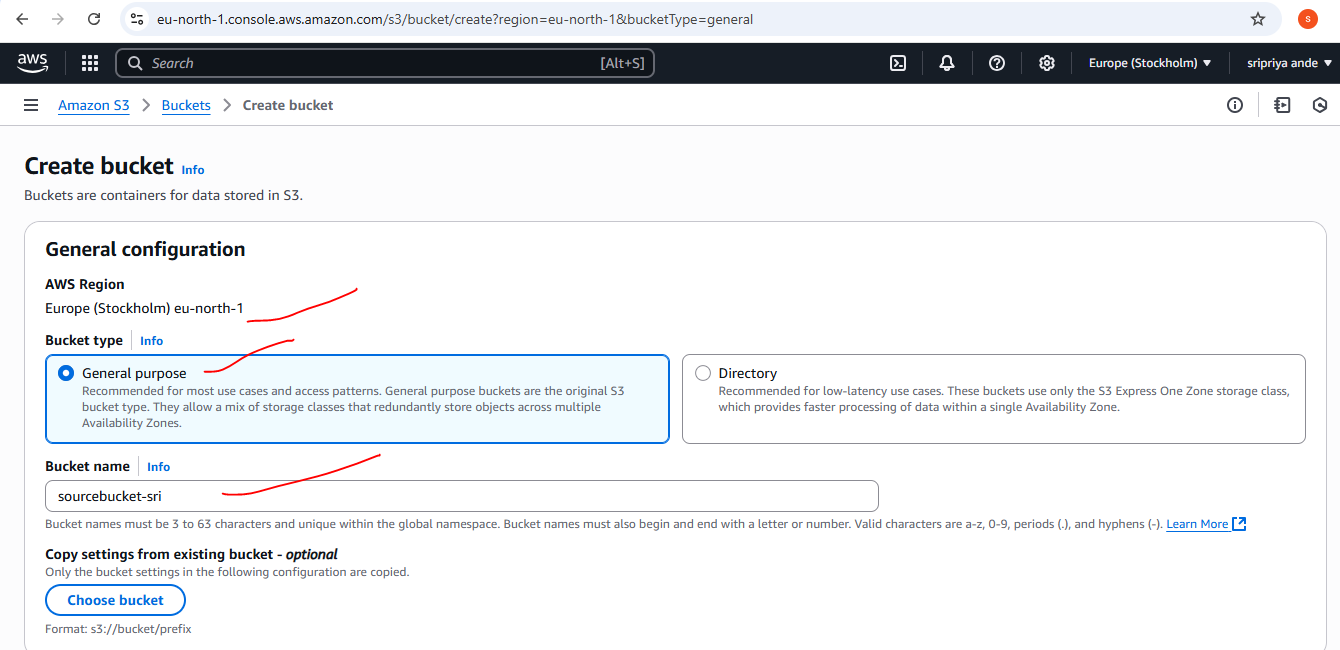
step 3: Configure the Rule

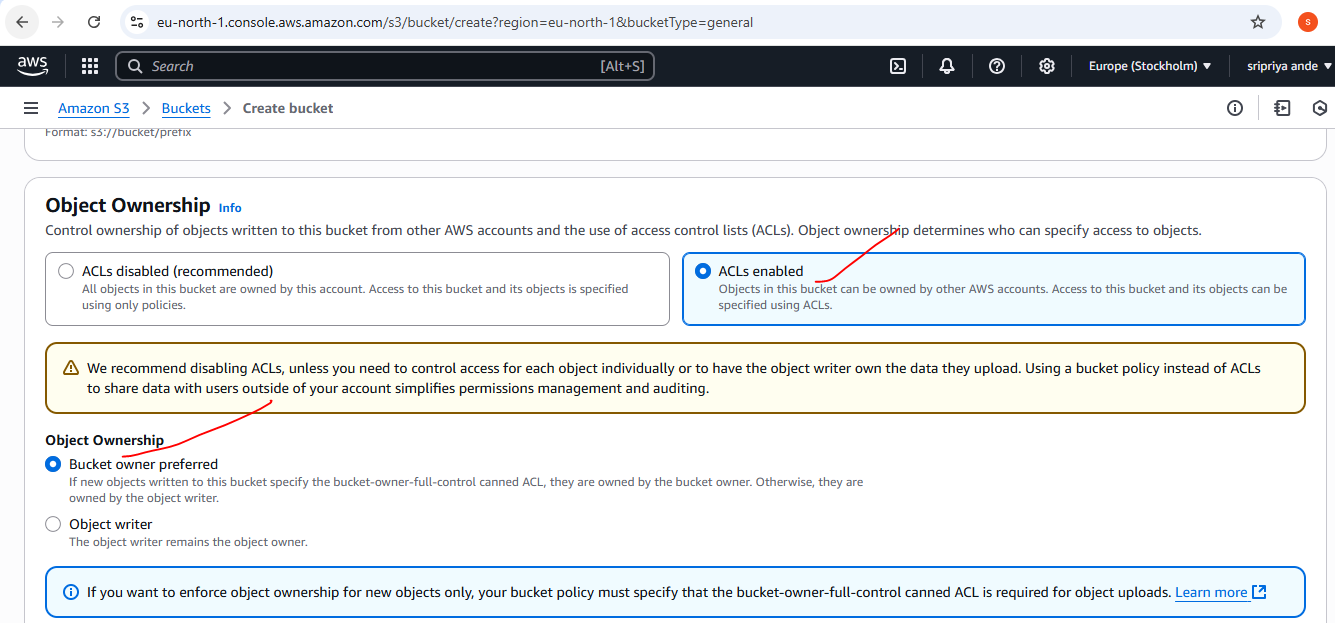
Rule name: Any name (e.g., replicate-to-ohio)

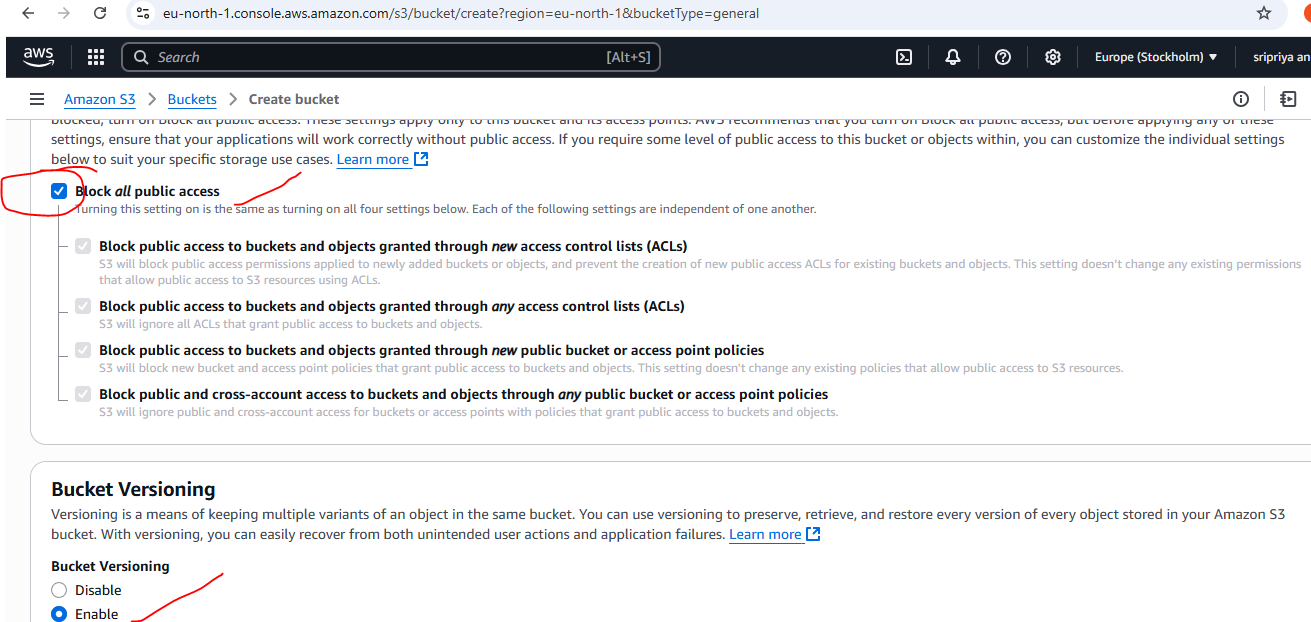
Status: Keep it as enabled

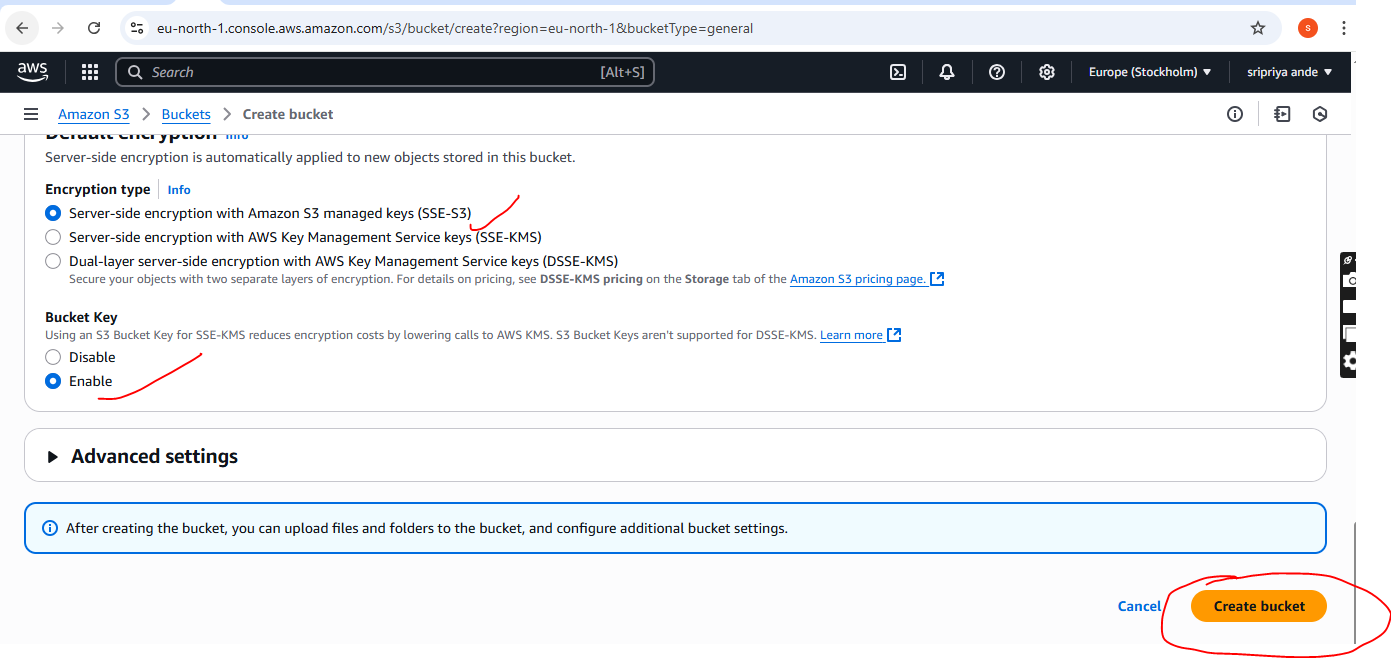
Scope:

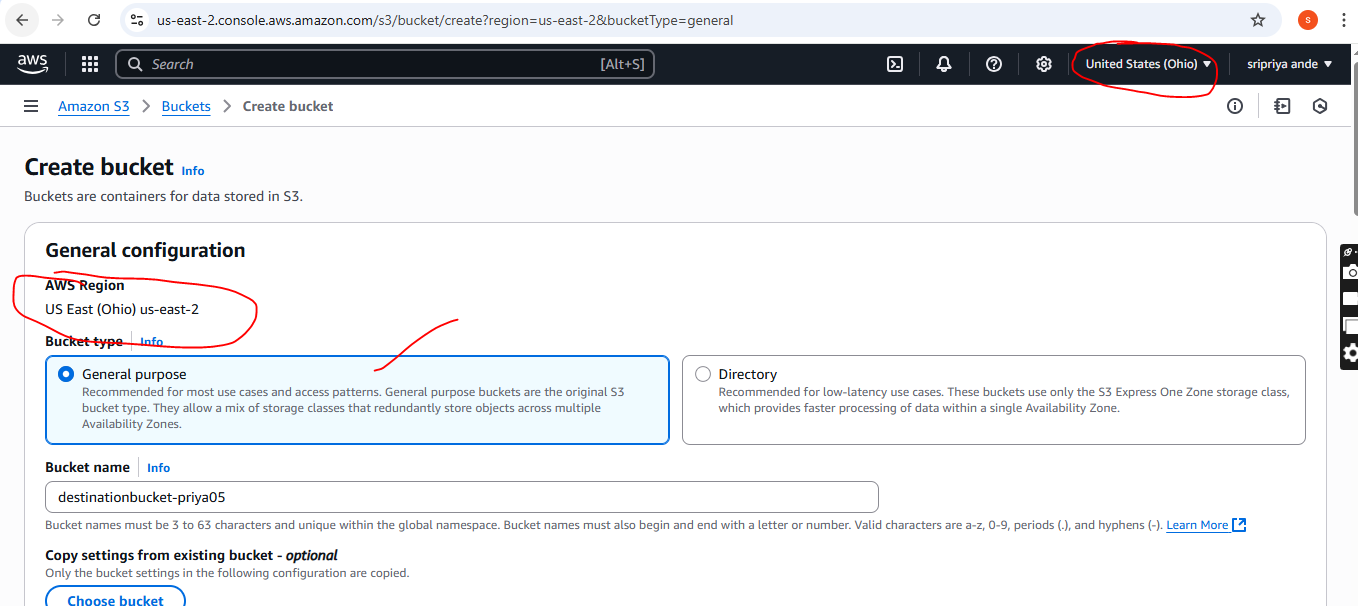
Choose “This rule applies to all objects in the bucket”

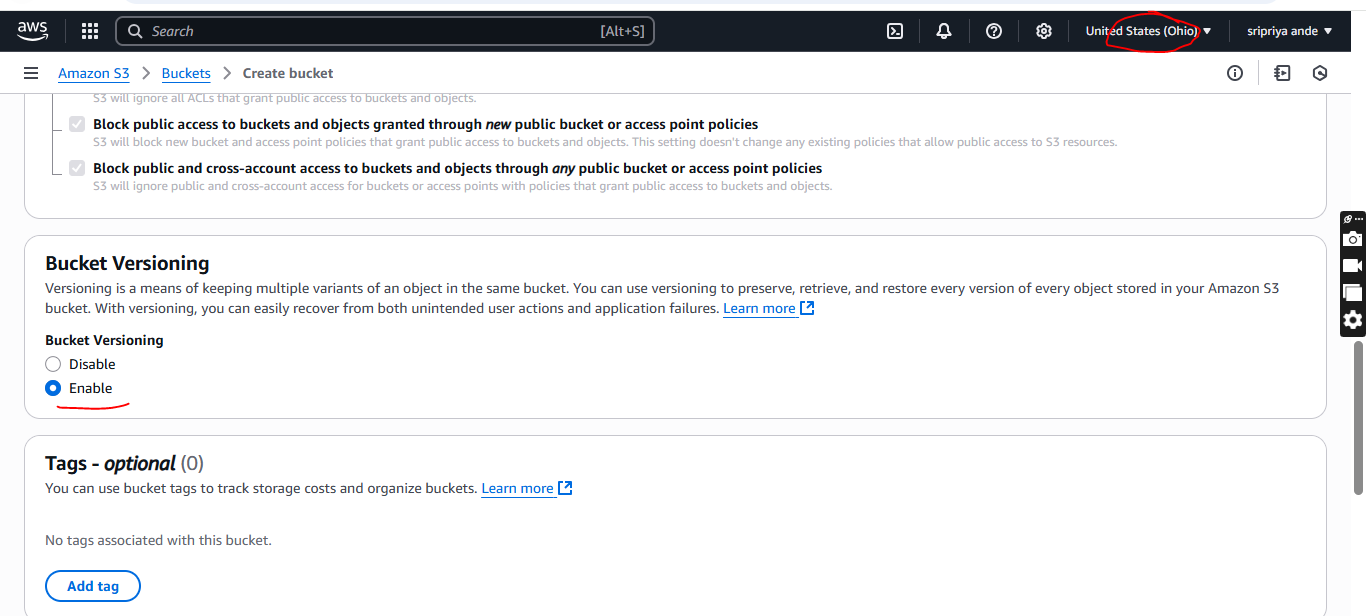


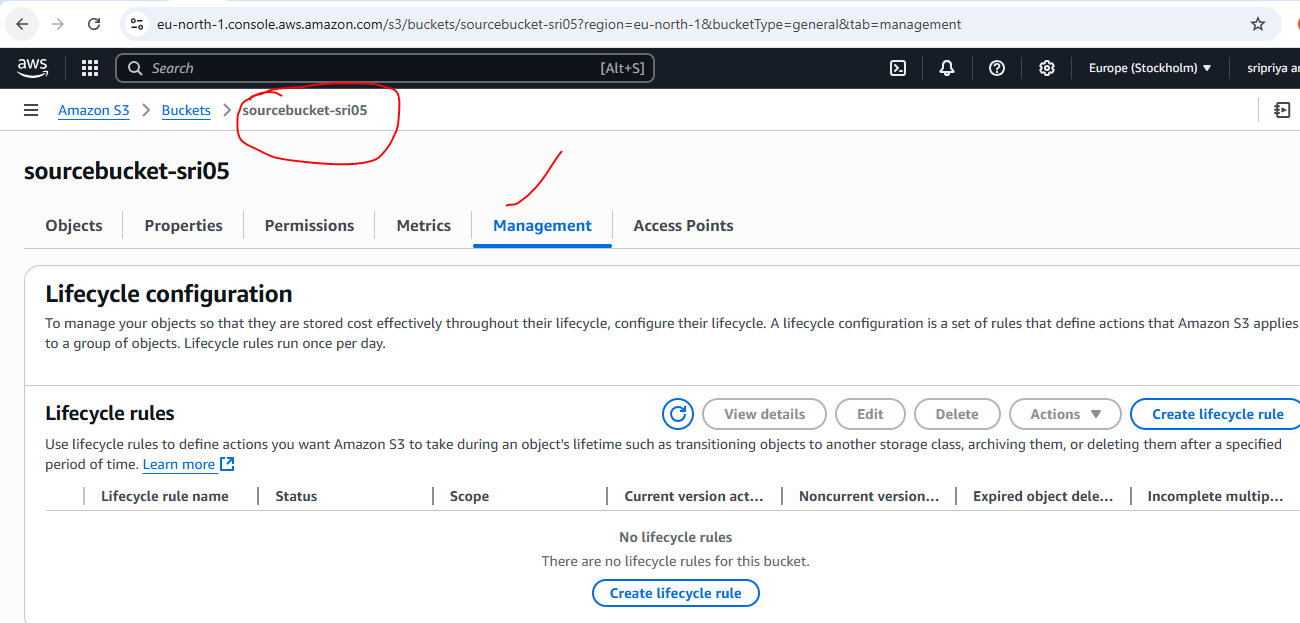


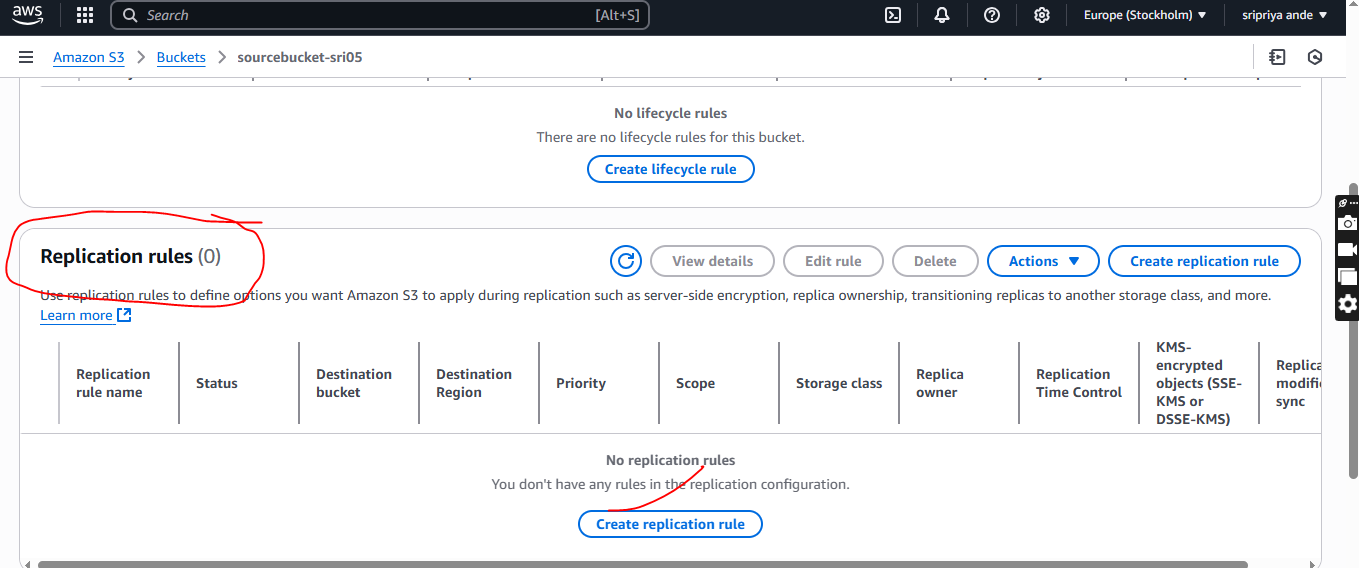


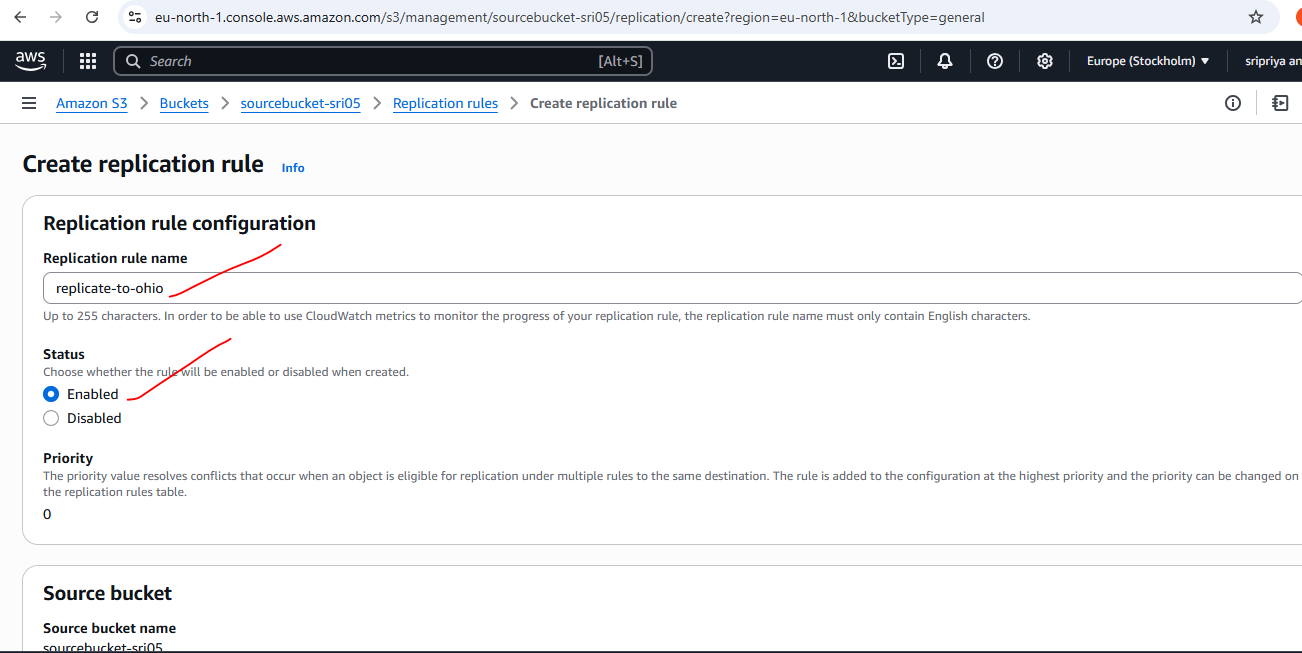


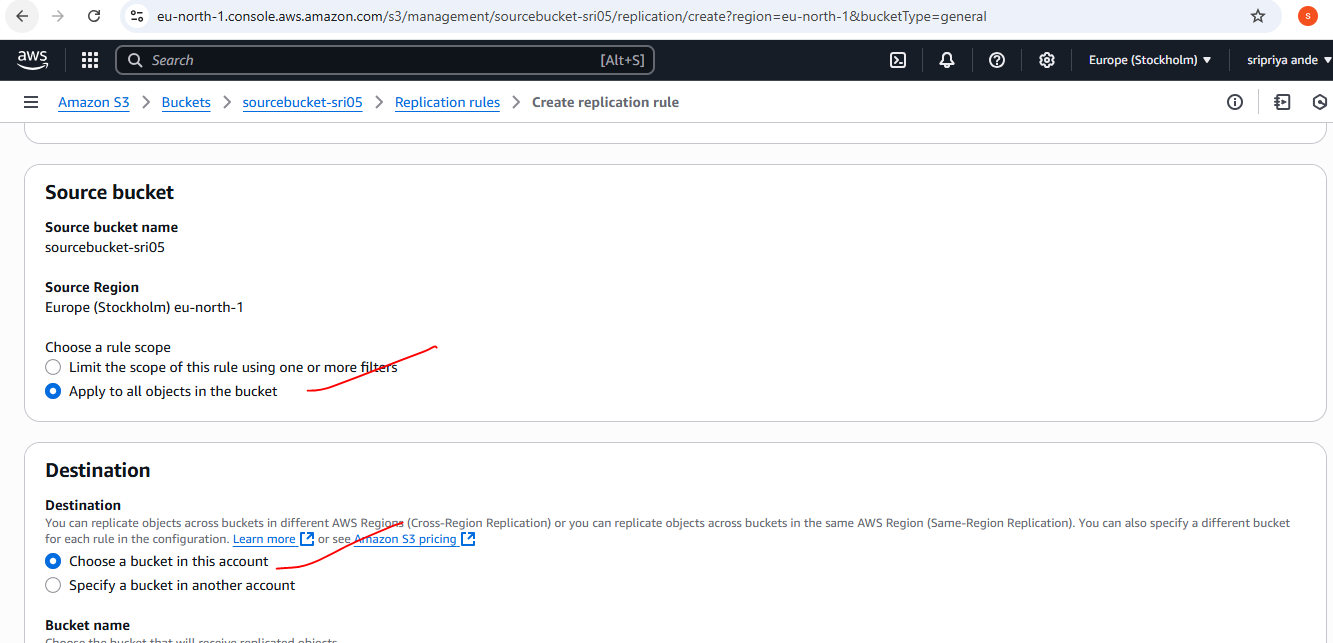


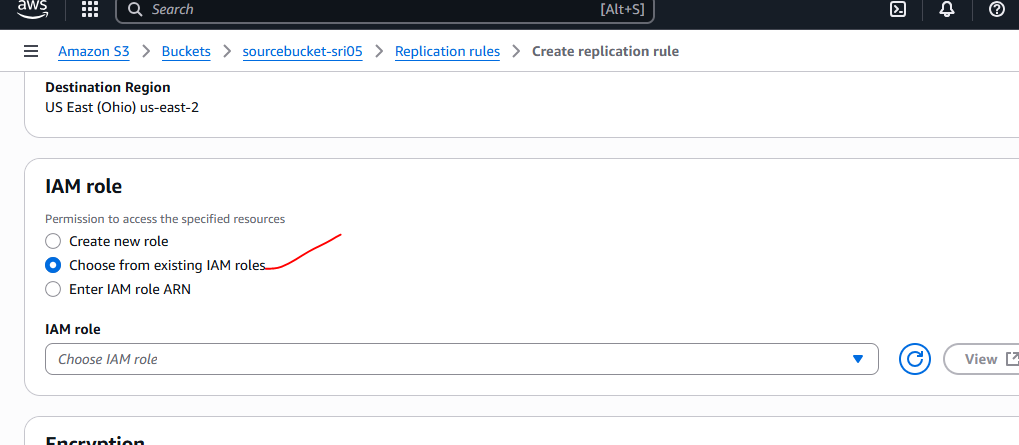


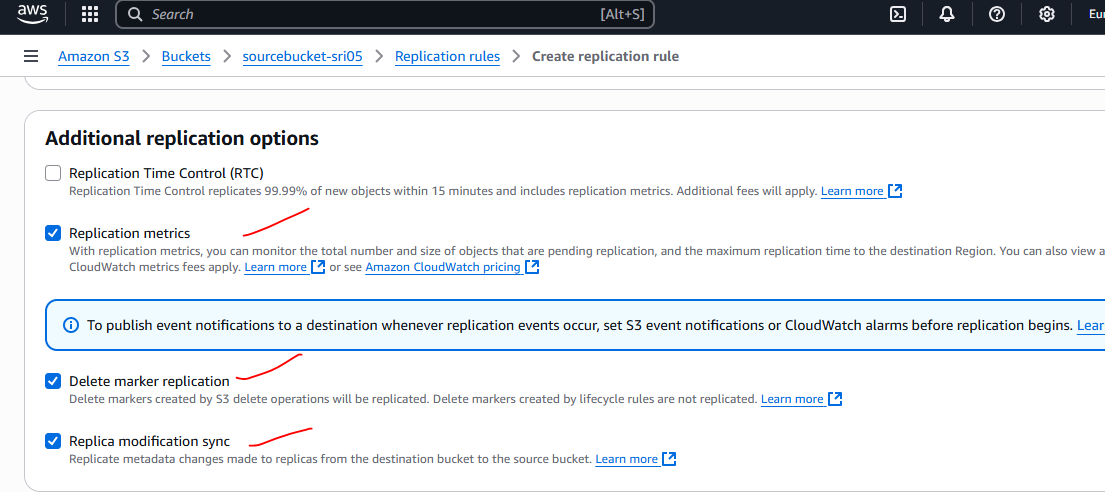


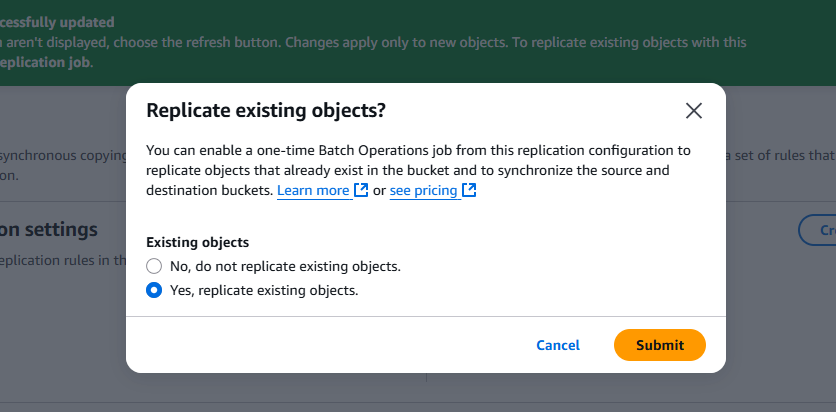


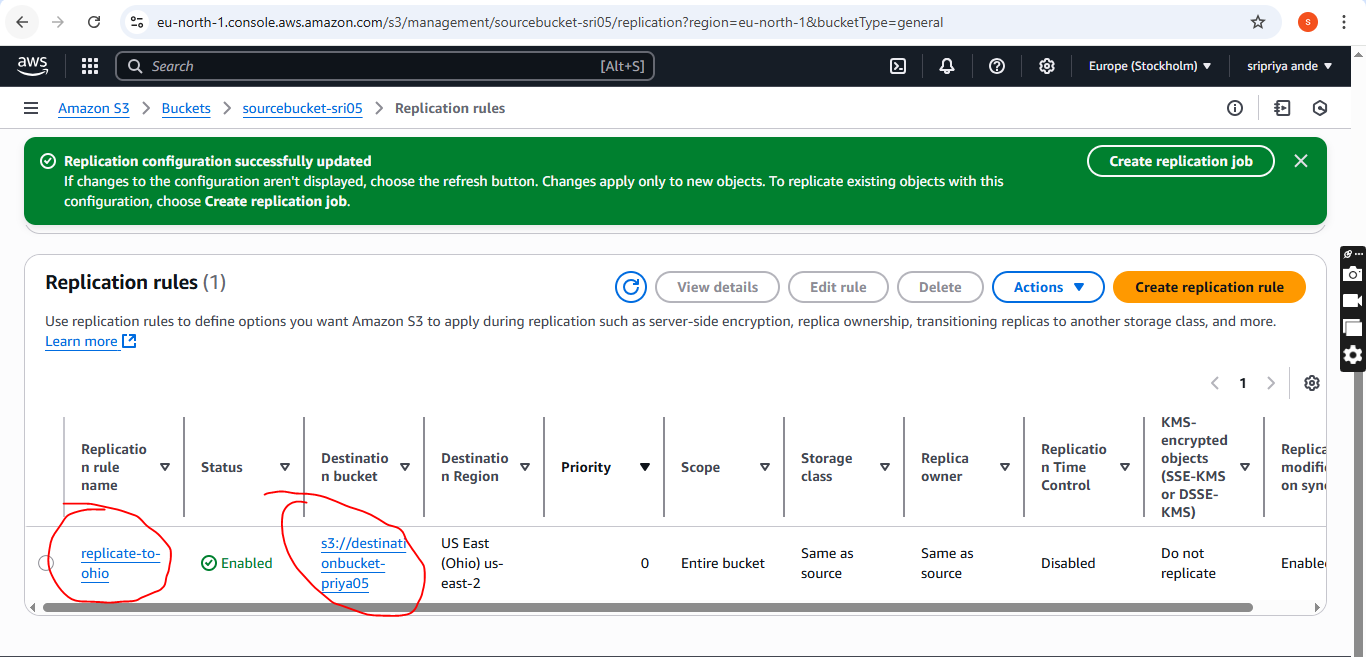












1. **Configure bucket policy,only Admin user can see the objects of s3 bucket.**

You must know the ARN of the Admin user.

You can find it in the IAM console or using:

aws iam get-user --user-name test

Example ARN:

arn:aws:iam::750471539774:user/test

Bucket already exists.

Step 1: Open AWS Console → S3 → Your Bucket

Go to the S3 console.

Click on your bucket name.

Go to the Permissions tab.

Scroll down to Bucket policy and click Edit.

Step 2: Add Bucket Policy

{

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

"Statement": [

{

"Sid": "AllowtestOnlyAccess",

"Effect": "Allow",

"Principal": {

"AWS": "arn:aws:iam::750471539774:user/test

"

},

"Action": "s3:\*",

"Resource": [

"arn:aws:s3:::s3-0803",

"arn:aws:s3:::s3-0803/\*"

]

}

]

}

Only Admin user will have access — all others will be denied, unless they have specific IAM permissions.

Step 3: Save the Policy

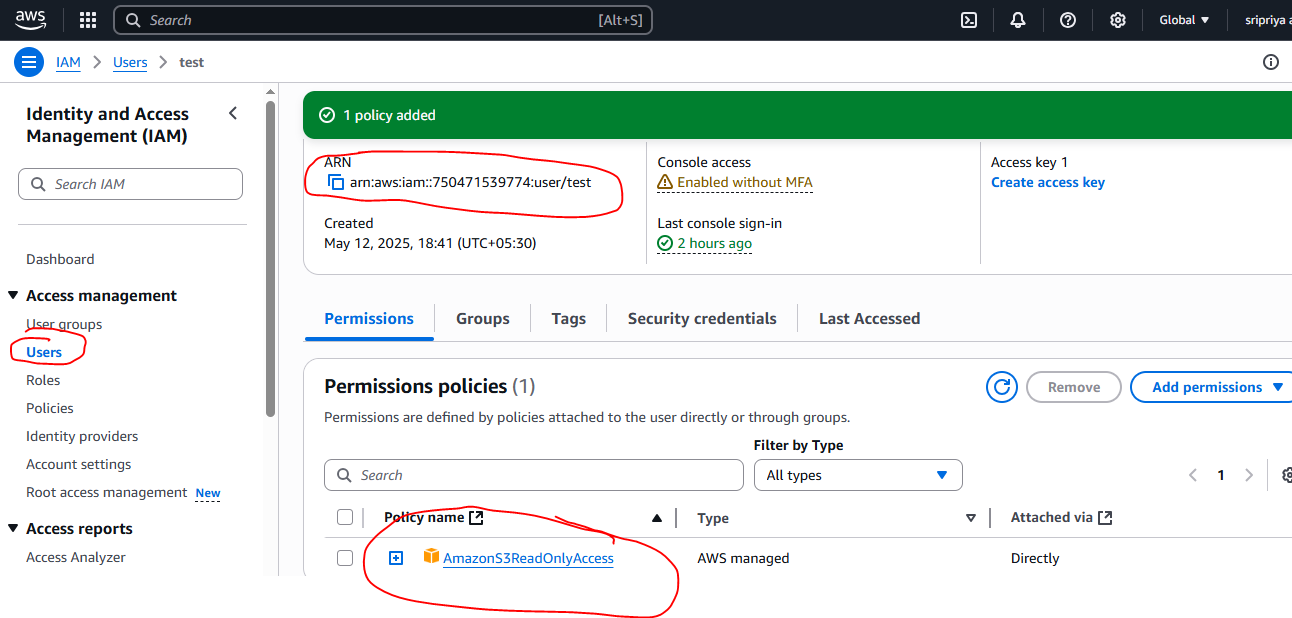
Click Save changes after pasting the policy.

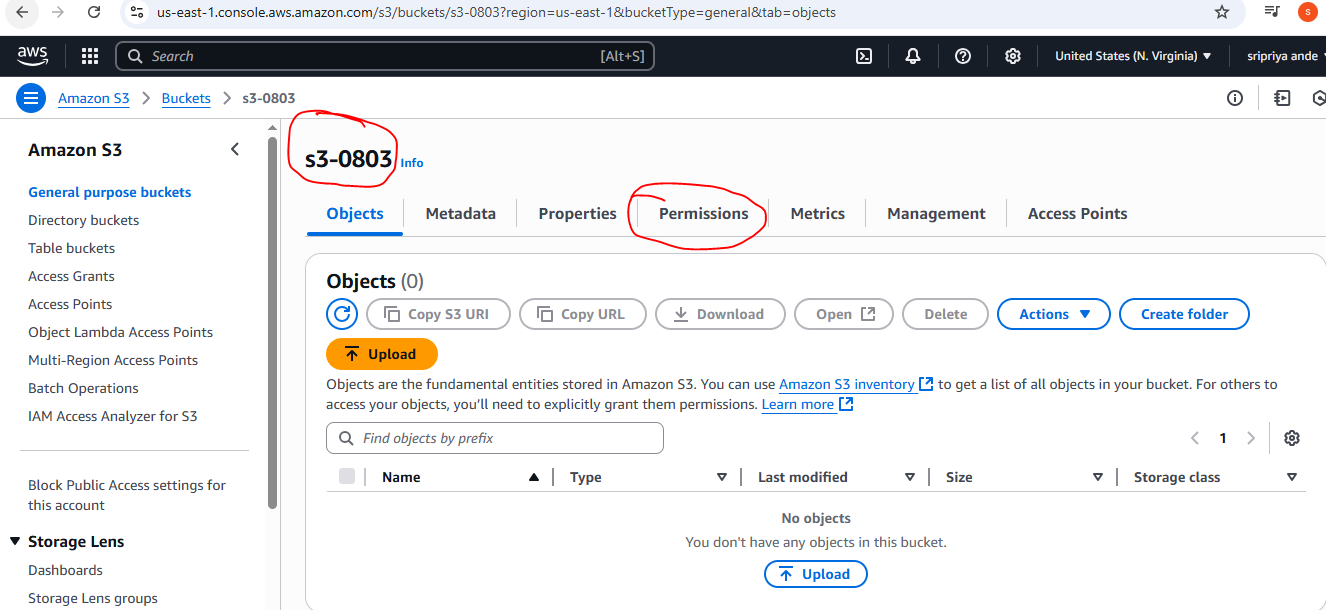
Validate Permissions

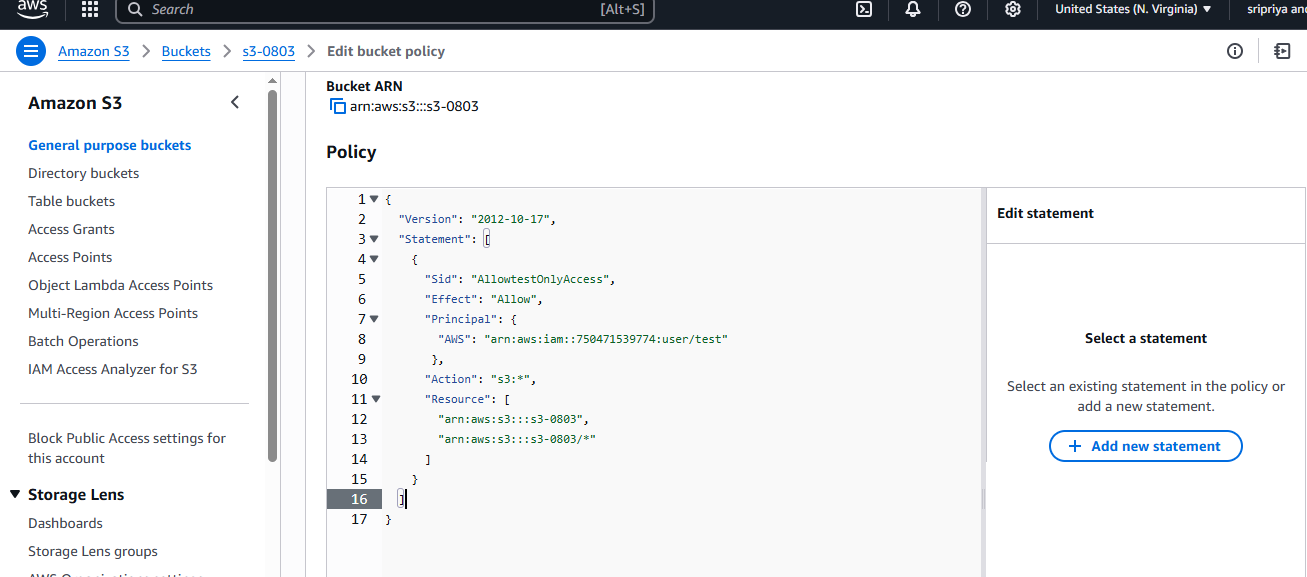
You can test access with:

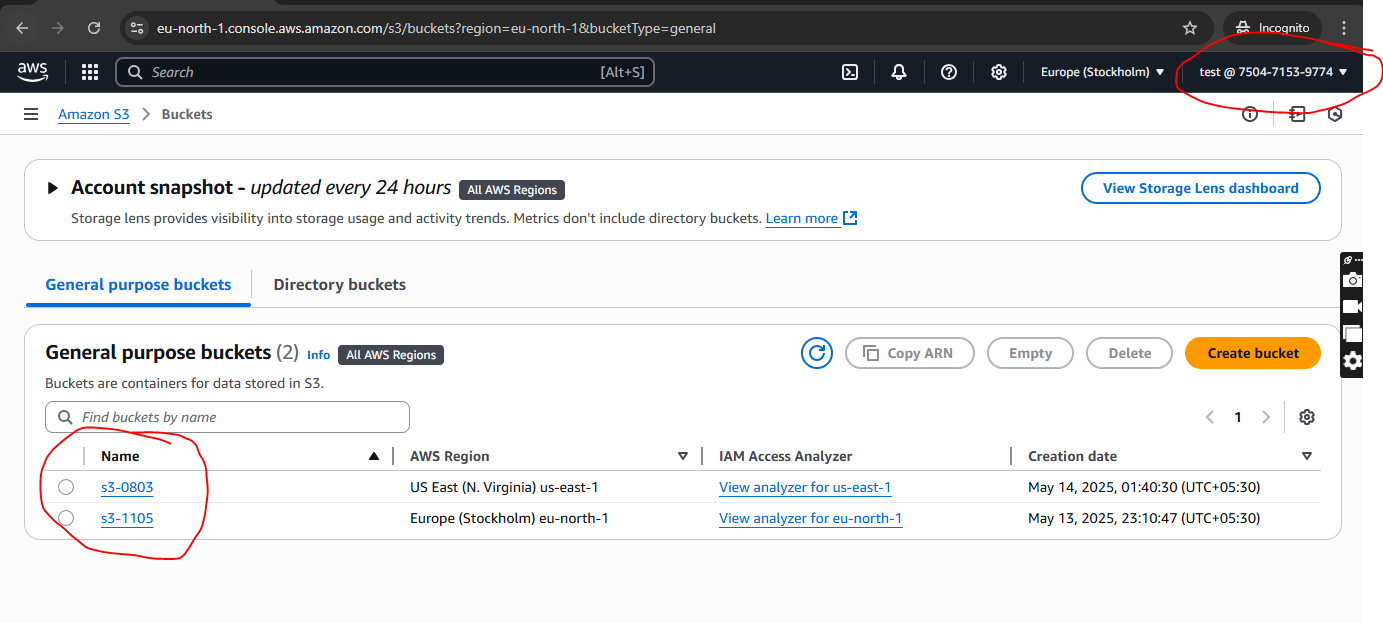
aws s3 ls s3:// --profile test-profile











1. **Setup lifecycle policies to automatically transition or delete objects based on specific criteria.**

Step 1: Go to the S3 Console

Open: https://s3.console.aws.amazon.com

Select your bucket (e.g., s3-0803)

Step 2: Choose the “Management” tab

Click Lifecycle rules

Click Create lifecycle rule

Step 3: Set Lifecycle Rule Details

Name: e.g., transition-delete-rule

Scope: Apply to all objects or specific prefix/tags

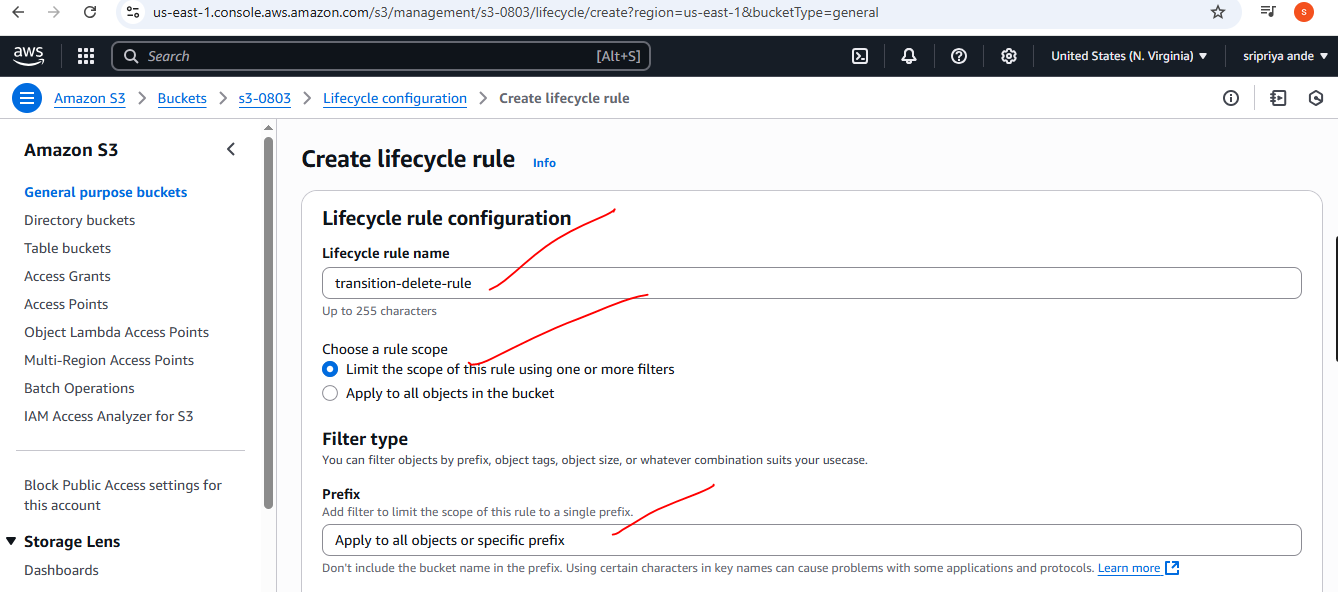
Step 4: Add Transitions (optional)

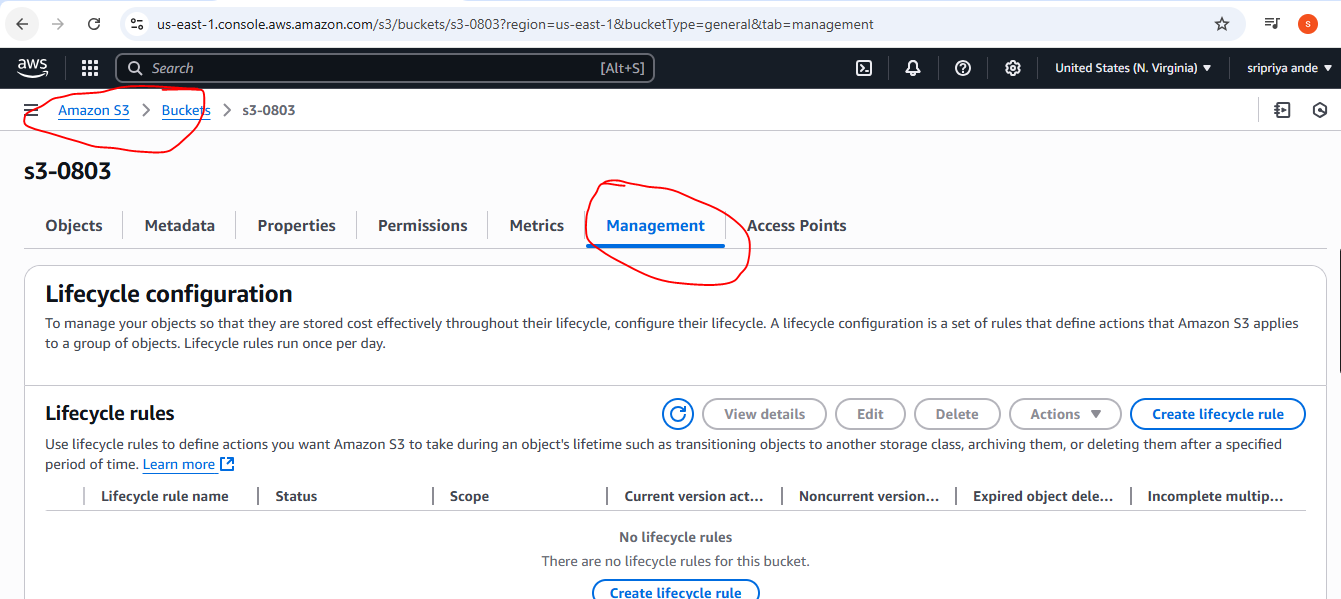
Example:

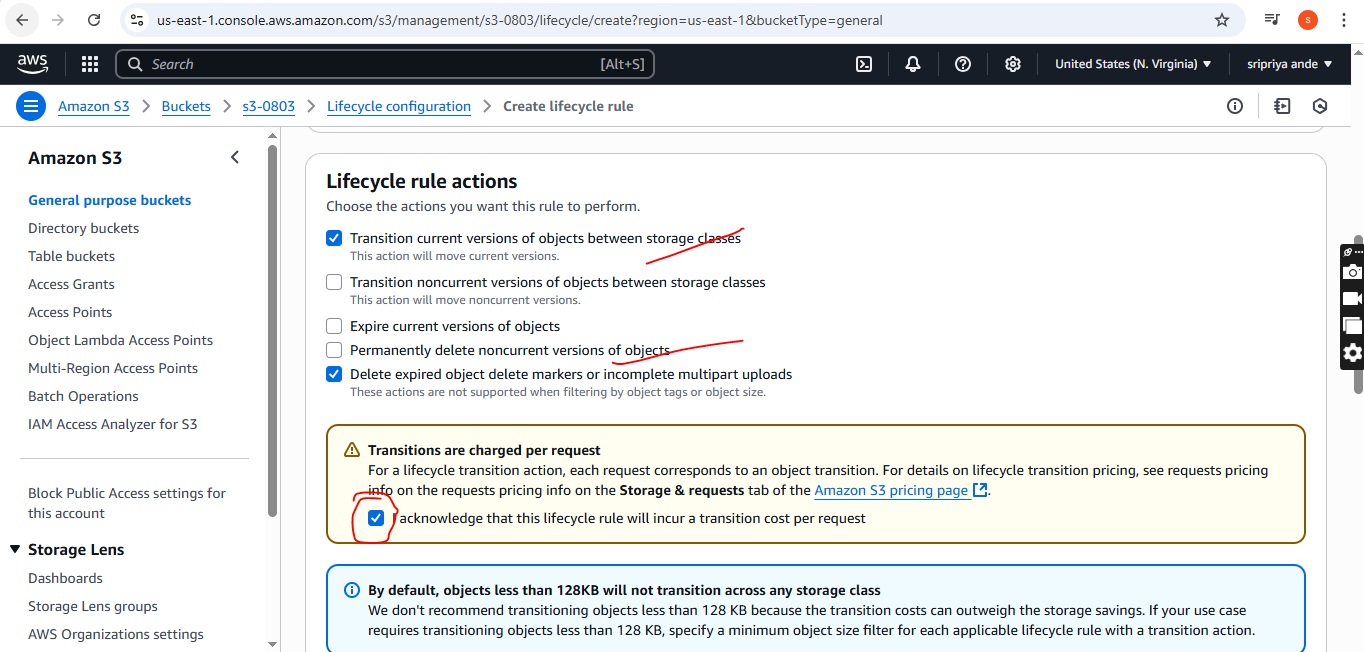
Transition objects to Standard-IA after 30 days

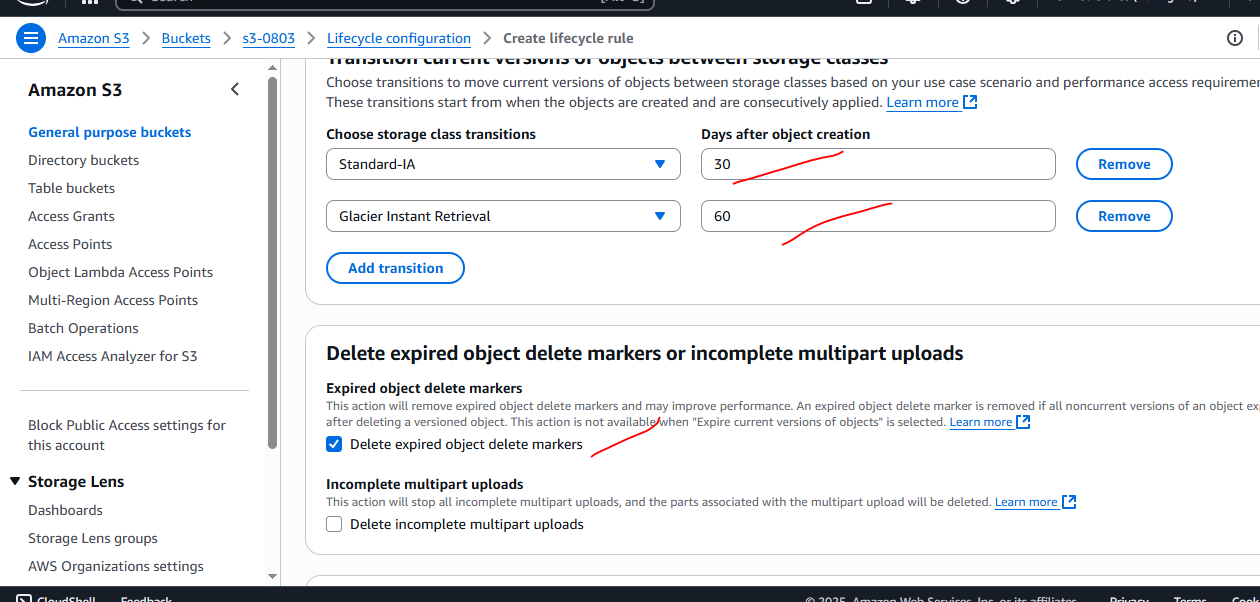
Transition to Glacier after 90 days

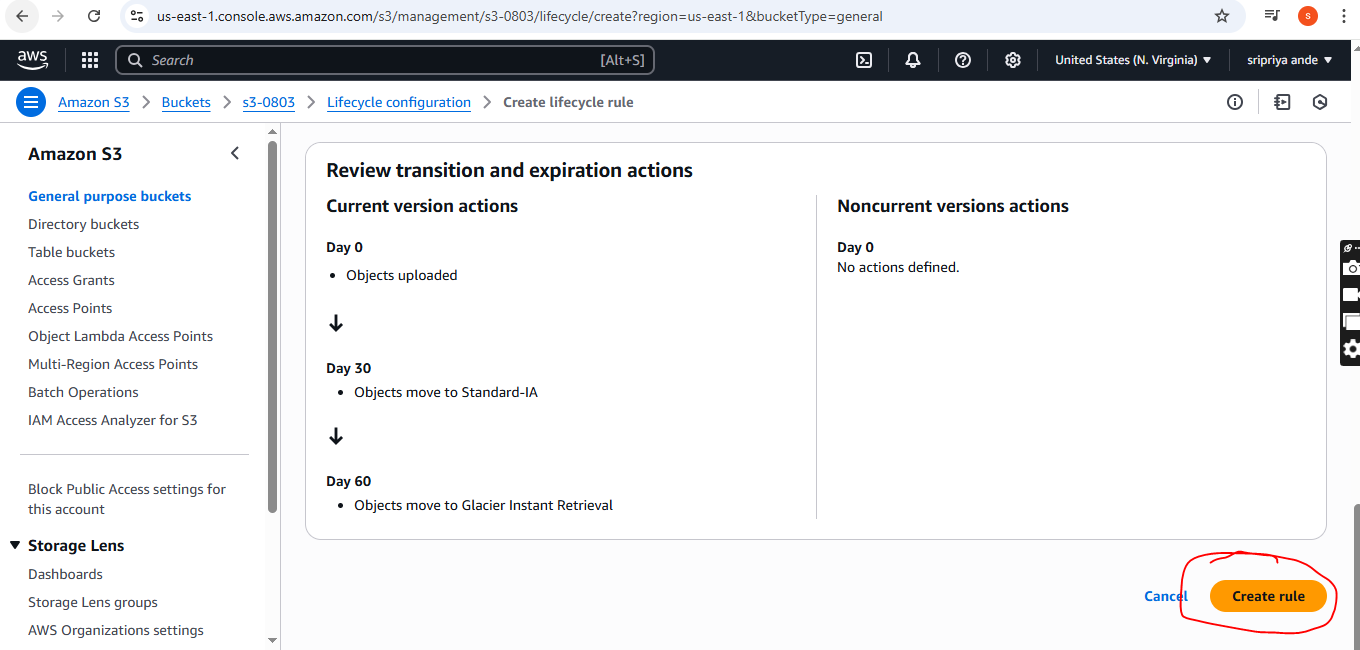
Step 5: Save the rule











1. **Push some objects in s3 using AWS CLI.**

AWS CLI installed

Check: aws --version

If not installed: Download AWS CLI

Configured AWS CLI

Run: aws configure

Enter:

AWS Access Key ID

AWS Secret Access Key

Region (e.g., us-east-1)

Output format (default: json)

Create a test file

echo "Hello from AWS CLI!" > test.txt

Upload a file to S3

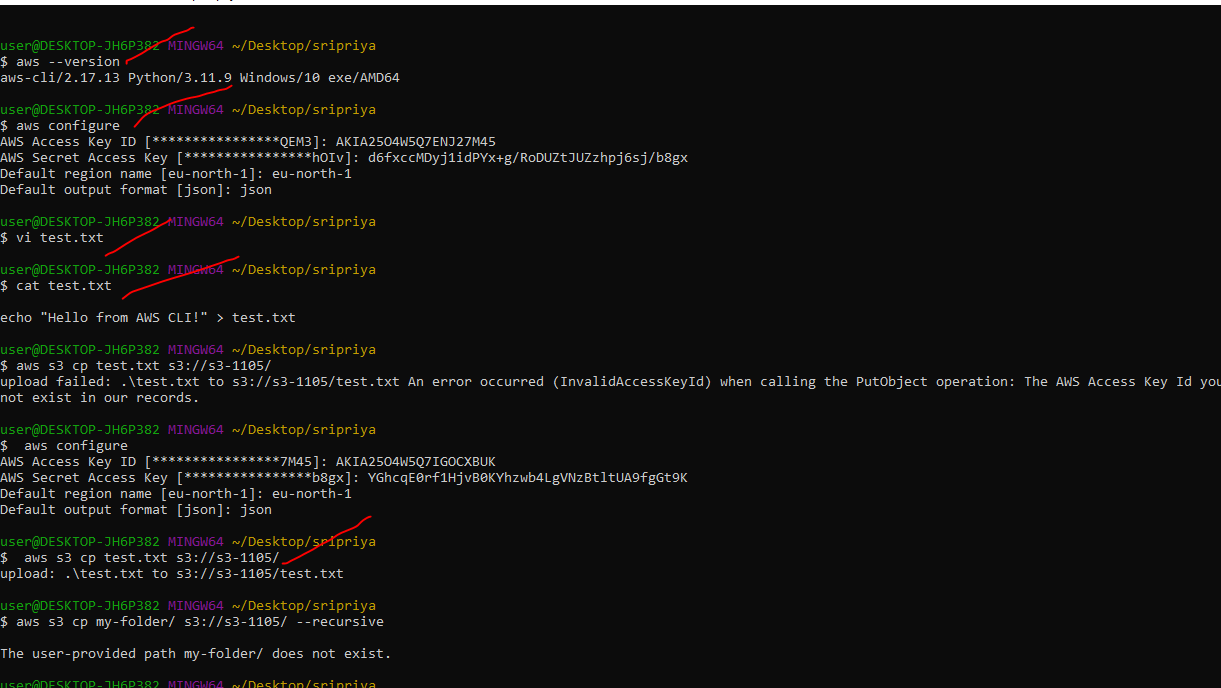
aws s3 cp test.txt s3://s3-1105/

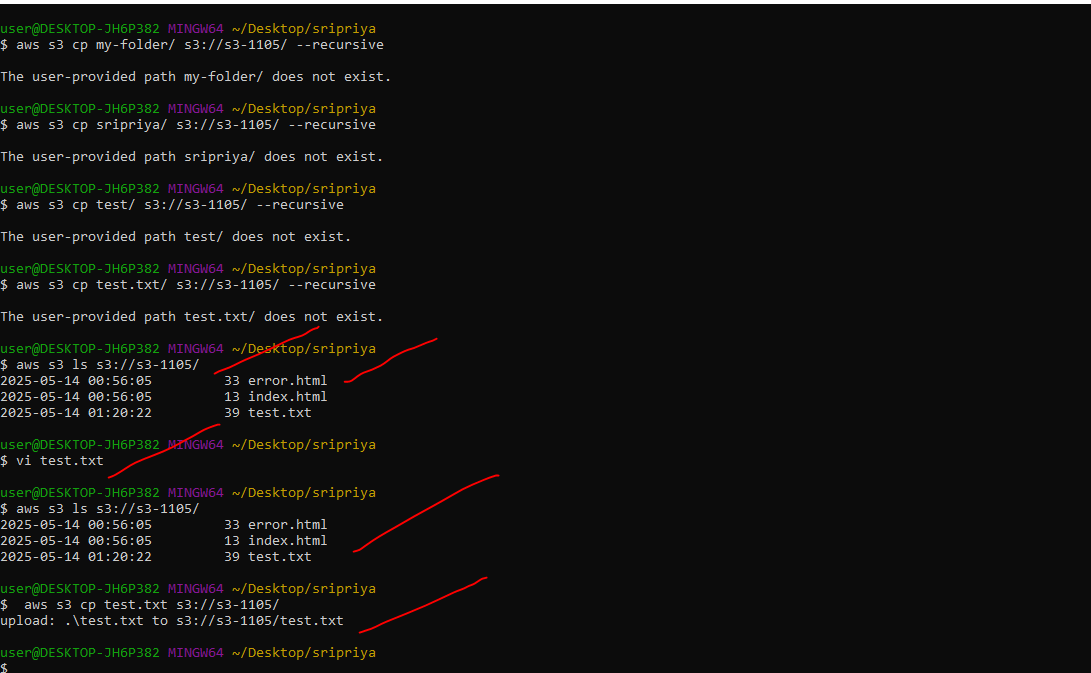
Replace your-bucket-name with your actual S3 bucket name.

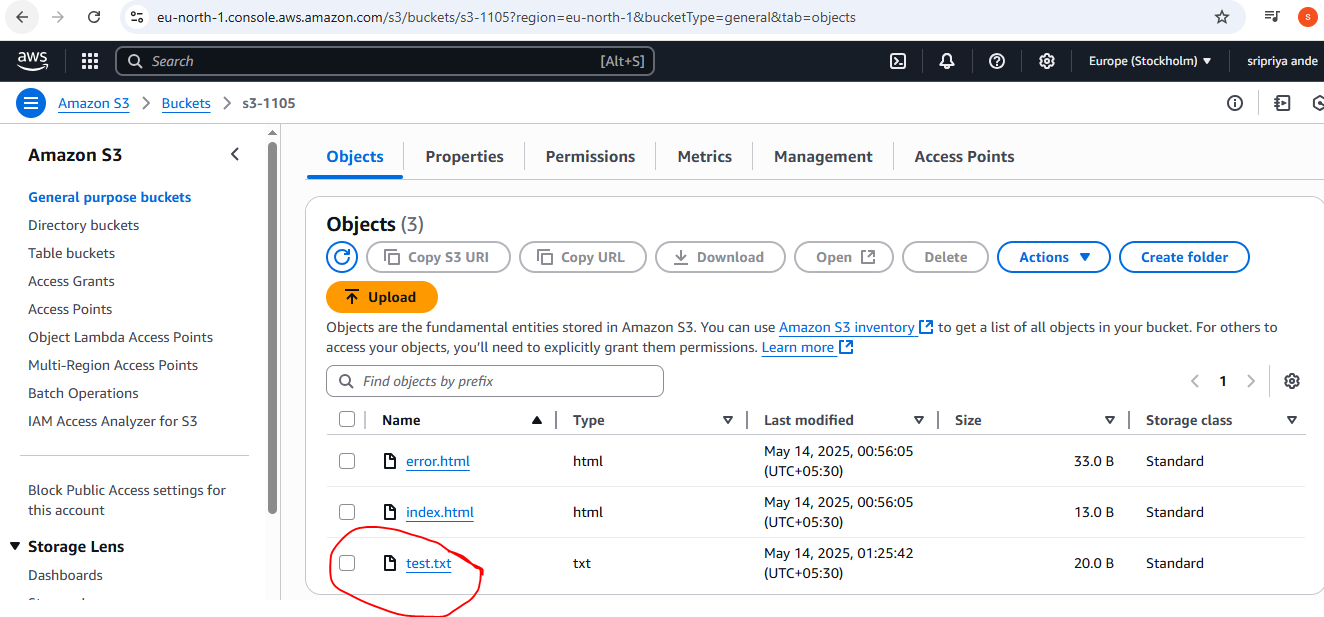
Upload an entire folder

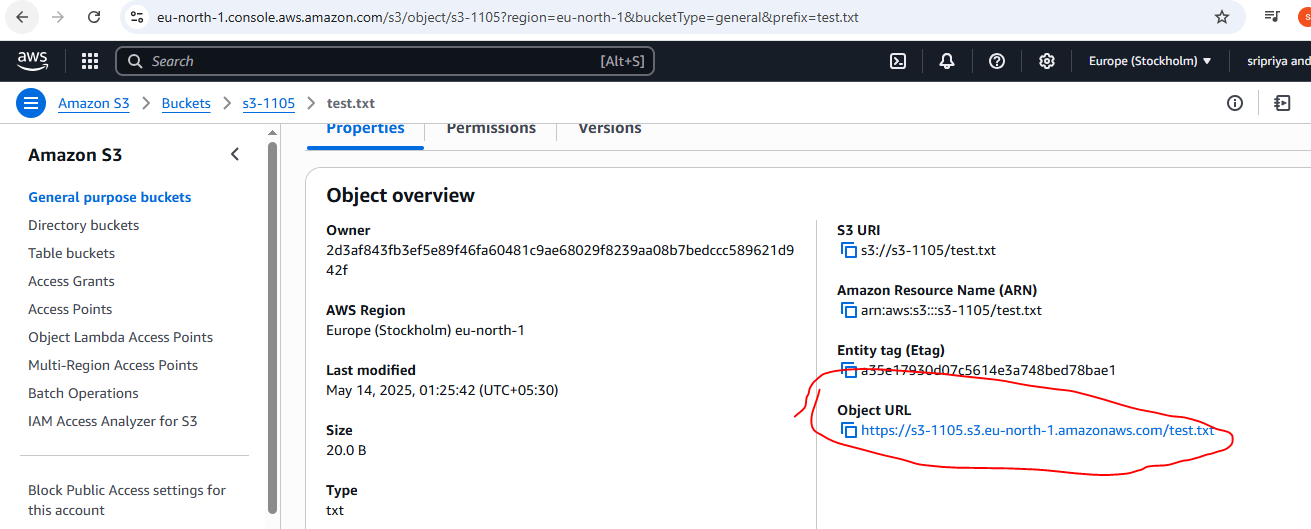
aws s3 ls s3://s3-1105/

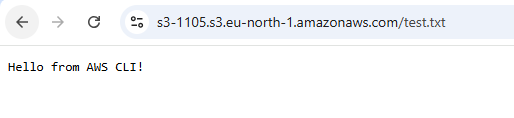
This lists all objects in your bucket.











1. **Write a bash script to create s3 bucket.**

AWS CLI installed (aws --version)

AWS CLI configured (aws configure)

IAM user must have s3:CreateBucket permission.

Step-by-Step Script to Create S3 Bucket

Step 1: Create a new bash script file

vi s3-0803.sh

Step 2: Add the following script

#!/bin/bash

# Ask user for bucket name and region

read -p "Enter a unique S3 bucket name: " BUCKET\_NAME

read -p "Enter AWS region (e.g., us-east-1): " REGION

# Create the bucket

echo "Creating S3 bucket: $BUCKET\_NAME in region: $REGION"

# Use different syntax for us-east-1 (no LocationConstraint)

if [ "$REGION" == "us-east-1" ]; then

aws s3api create-bucket --bucket "$BUCKET\_NAME" --region "$REGION"

else

aws s3api create-bucket --bucket "$BUCKET\_NAME" \

--region "$REGION" \

--create-bucket-configuration LocationConstraint="$REGION"

fi

# Confirm creation

if [ $? -eq 0 ]; then

echo "Bucket '$BUCKET\_NAME' created successfully."

else

echo "Failed to create bucket. Please check the name and permissions."

fi

Step 3: Save and exit

Press CTRL + O, then Enter to save

Press CTRL + X to exit

Step 4: Make the script executable

chmod +x s3-0803.sh

Step 5: Run the script

./s3-0803.sh

enter:

Bucket name (must be unique globally)

AWS region (like us-east-1, ap-south-1, etc.)

Example Run:

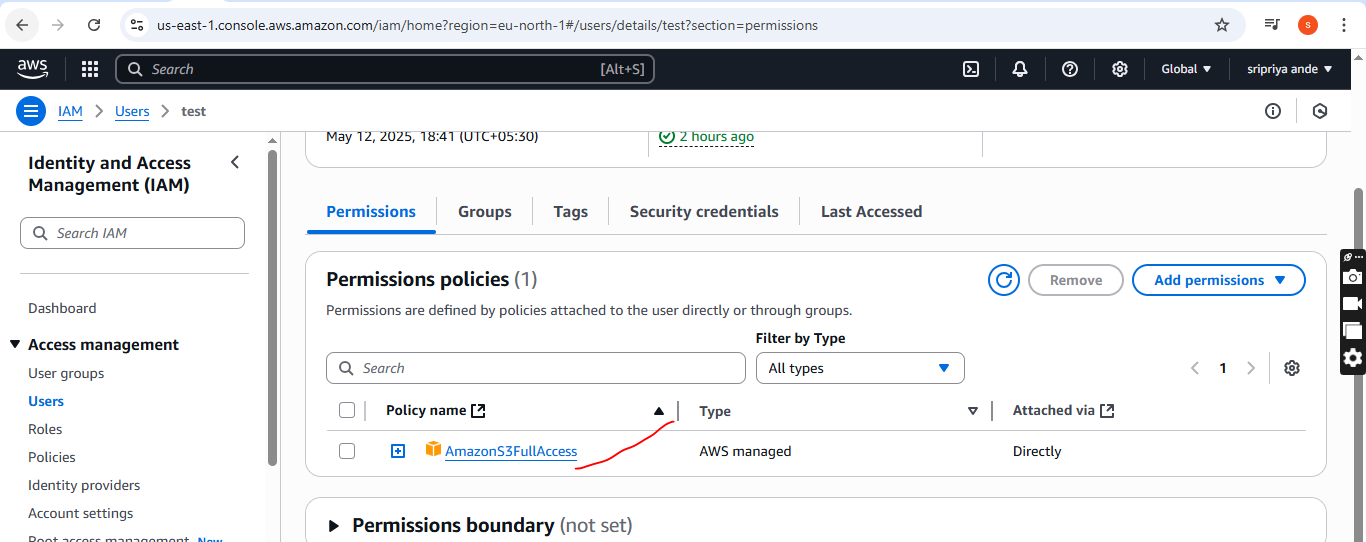
Enter a unique S3 bucket name:

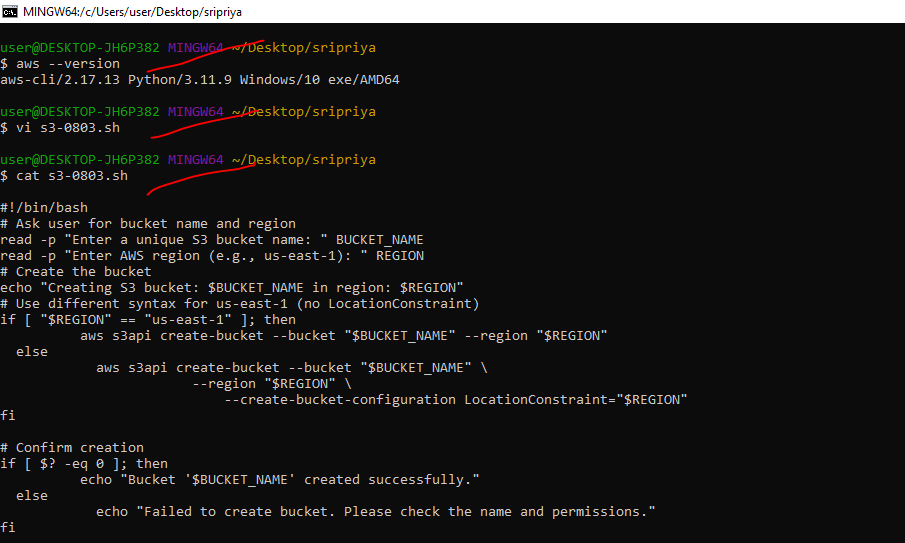
Enter AWS region (e.g., us-east-1):

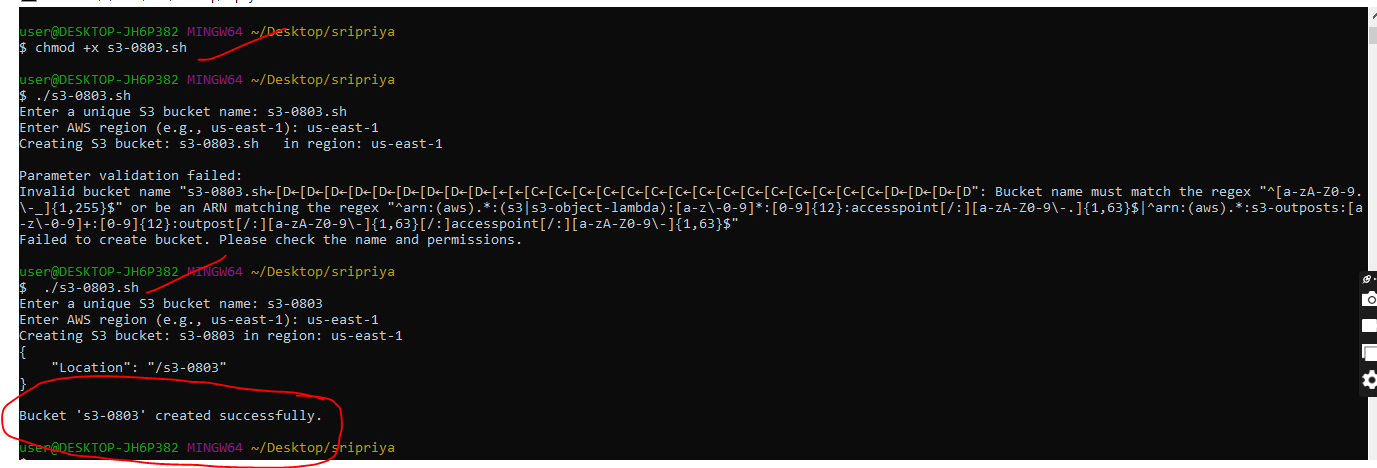
Creating S3 bucket:

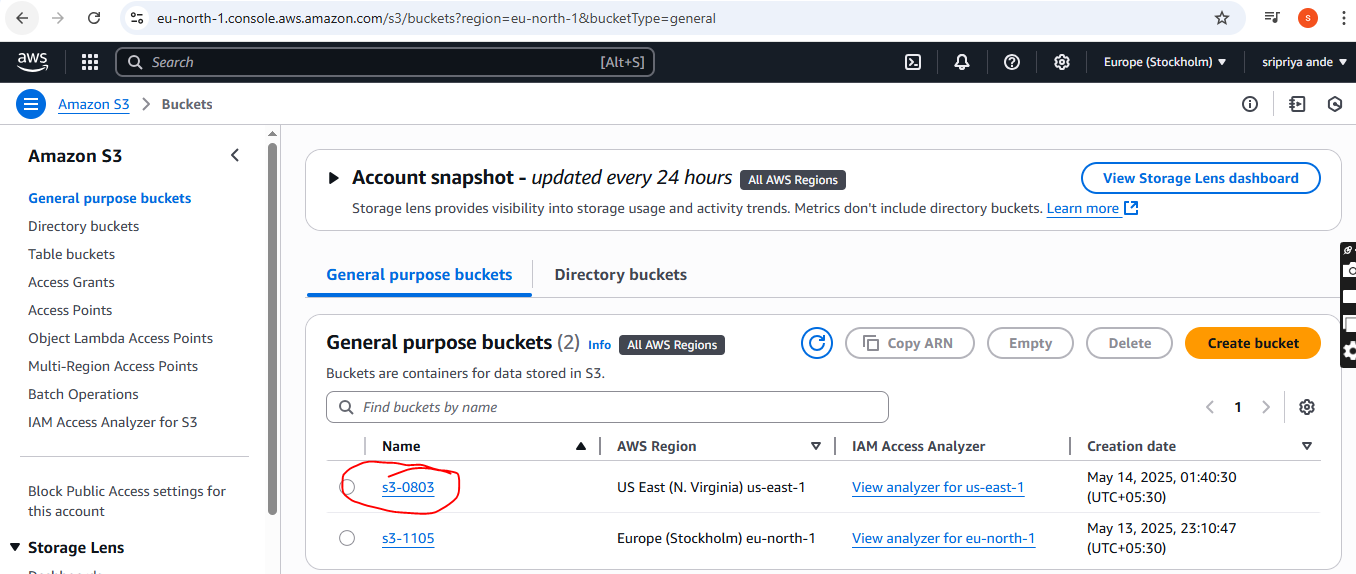
in region:

Bucket ' 'created successfully.









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

Step 1: Create a 1 GB dummy file (if you don't already have one)

You can use the dd command to generate a dummy 1 GB file:

**dd if=/dev/zero of=sample-1gb-file.bin bs=1M count=1024**

of=sample-1gb-file.bin is the output file name

bs=1M means 1 MB block size

count=1024 means 1024 blocks → 1 GB

Step 2: Upload the file to S3 using the AWS CLI

**aws s3 cp sample-1gb-file.bin s3://s3-0803/**

Replace your-bucket-name with your actual S3 bucket name.

If you're using a specific profile (e.g., test), use:

**aws s3 cp sample-1gb-file.bin s3://s3-0803/ --profile test**

