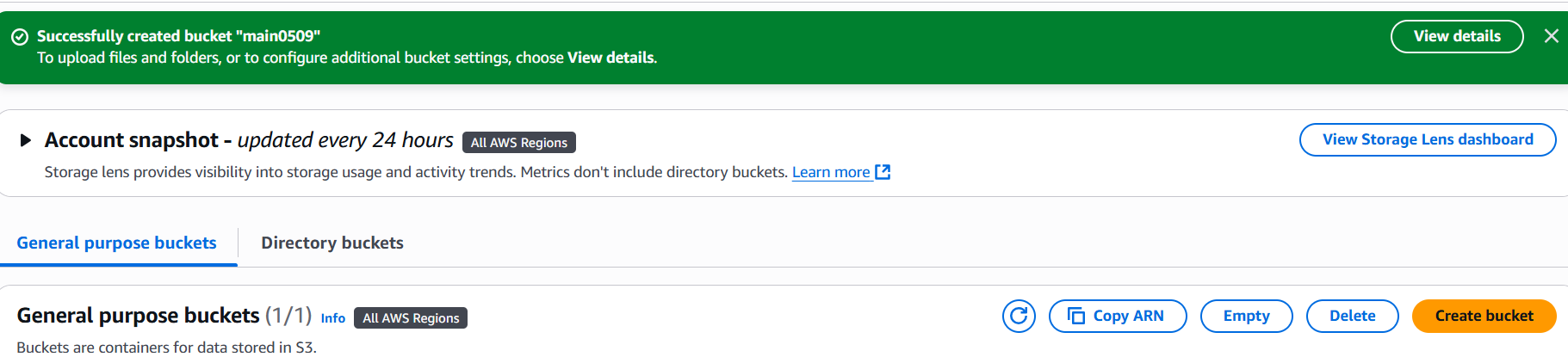
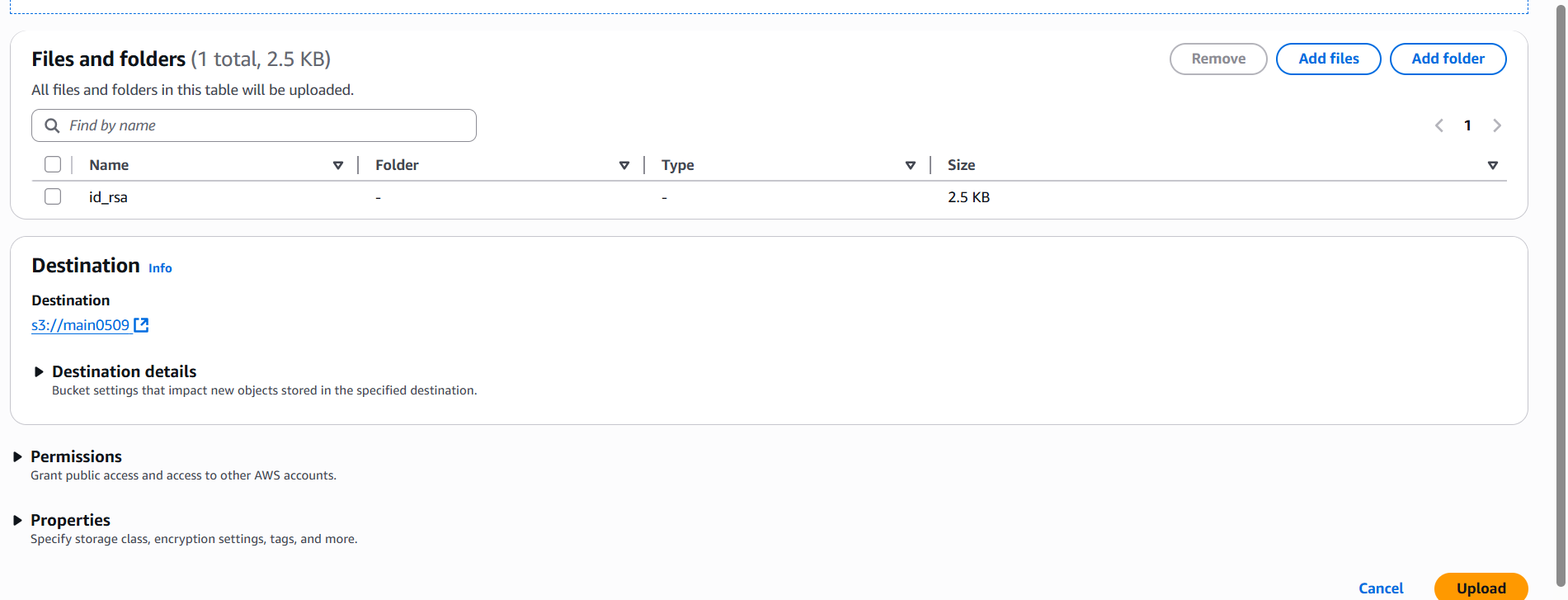
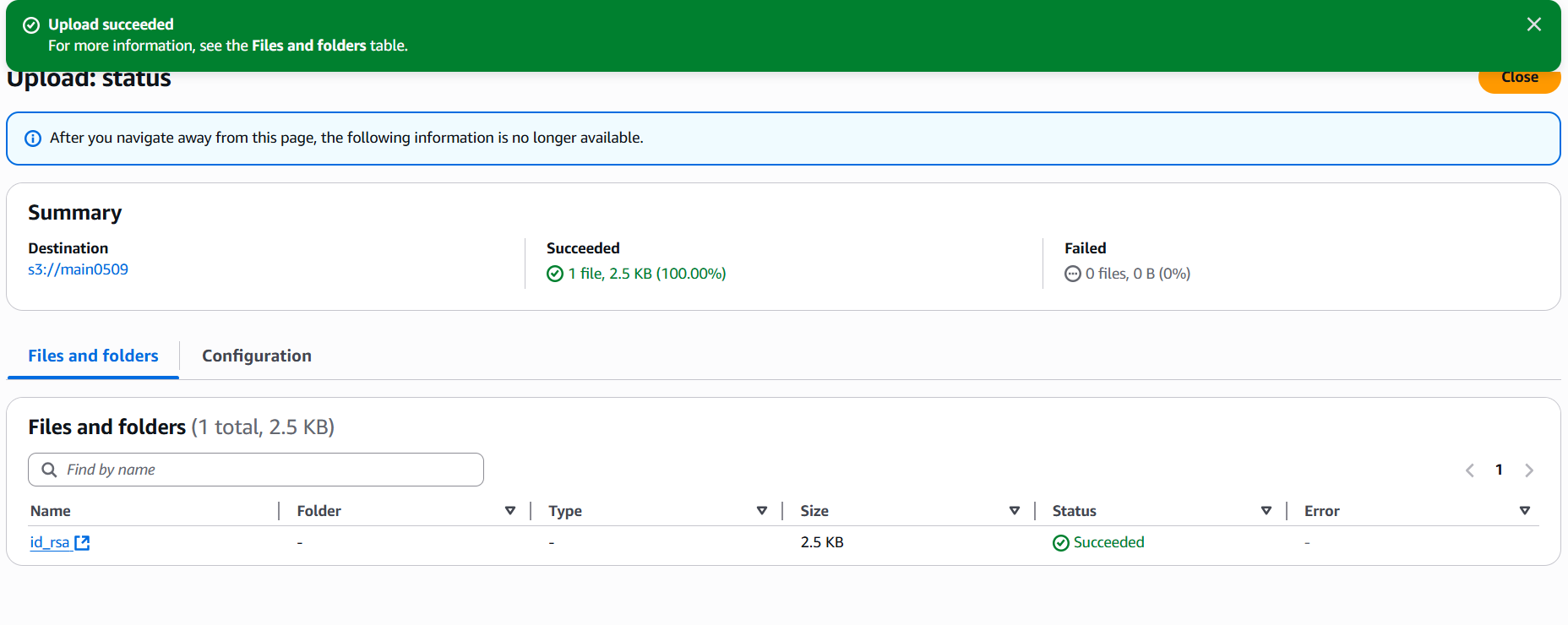
1. Create s3 bucket and upload some objects to s3.

Create an S3 Bucket:  
Sign in to the AWS Management Console.  
Click "Create bucket".  
Fill in:  
Bucket name: Must be globally unique (e.g., 1bucket-shravani)  
Region: Choose a region close to you  
Leave other settings as default  
Click "Create bucket"

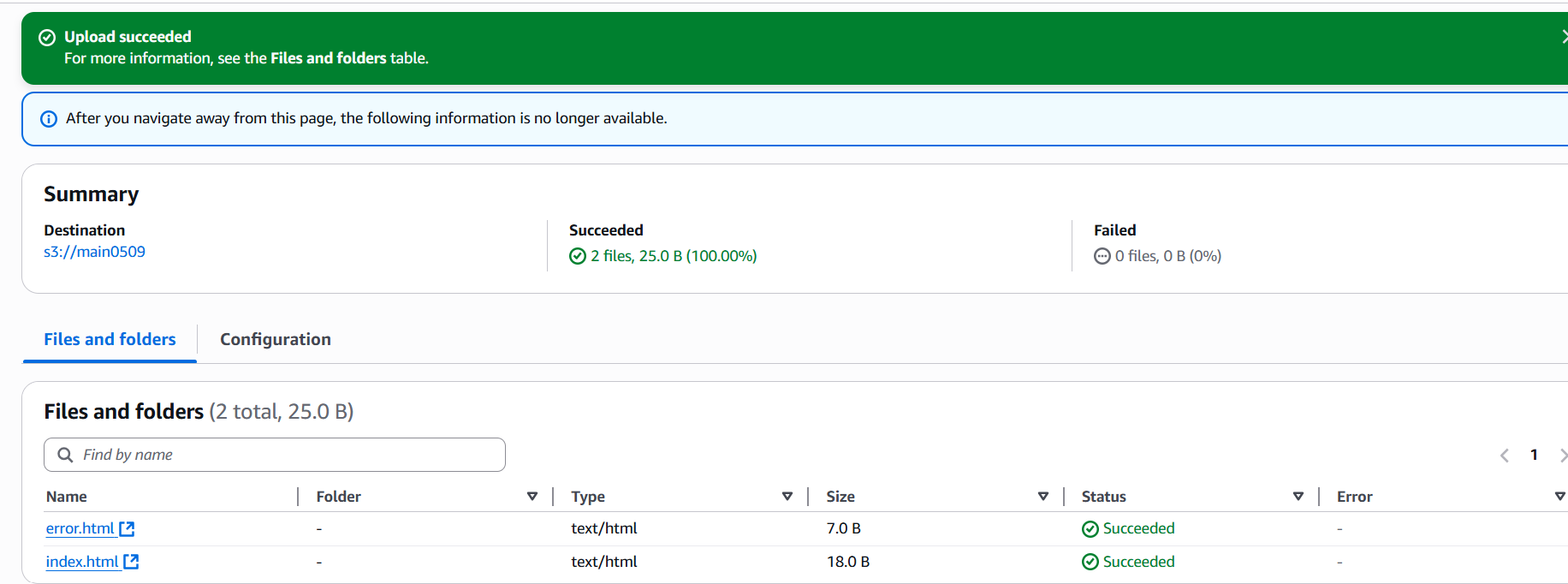
  
Upload Objects:  
Open the bucket by clicking its name.  
Click "Upload"  
Choose files from your computer  
Click "Upload"

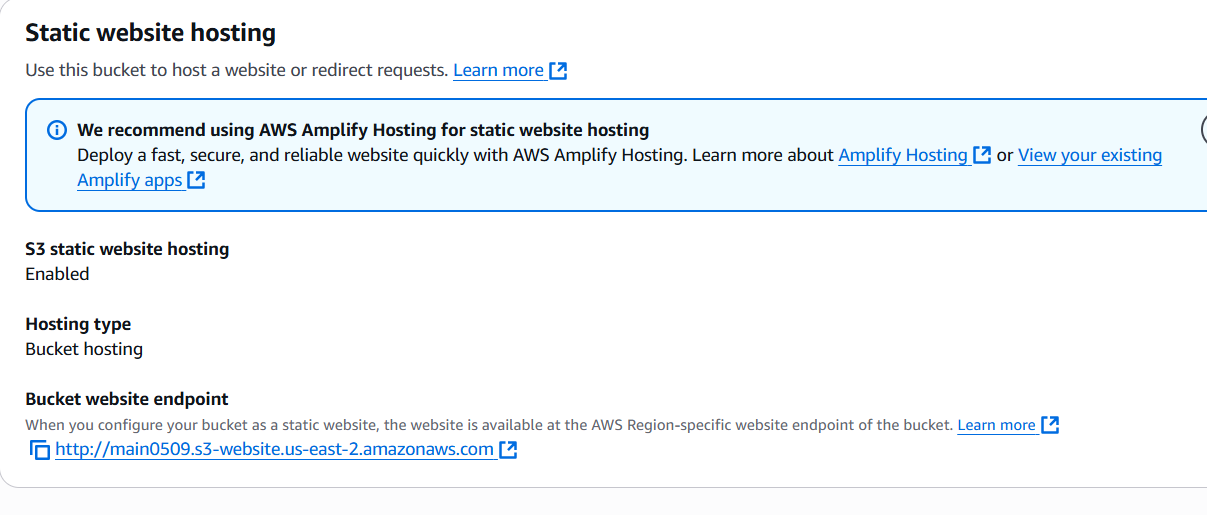


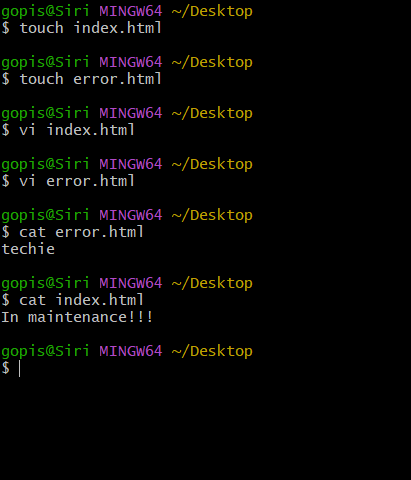


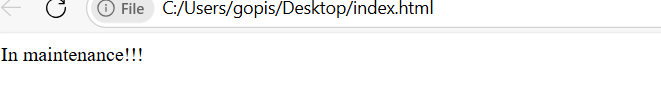
1. Deploy static website in s3 bucket.

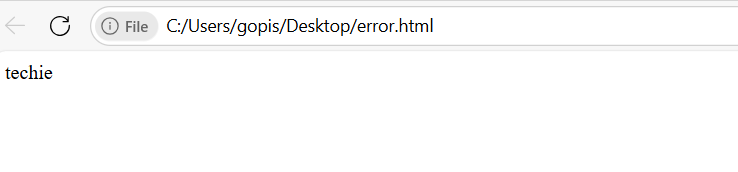
Click on the existing bucket and Upload Website Files  
index.html (homepage)  
error.html (custom error page)  
Upload Files:  
Open the bucket.  
Click "Upload" > Add files.  
Upload index.html and error.html



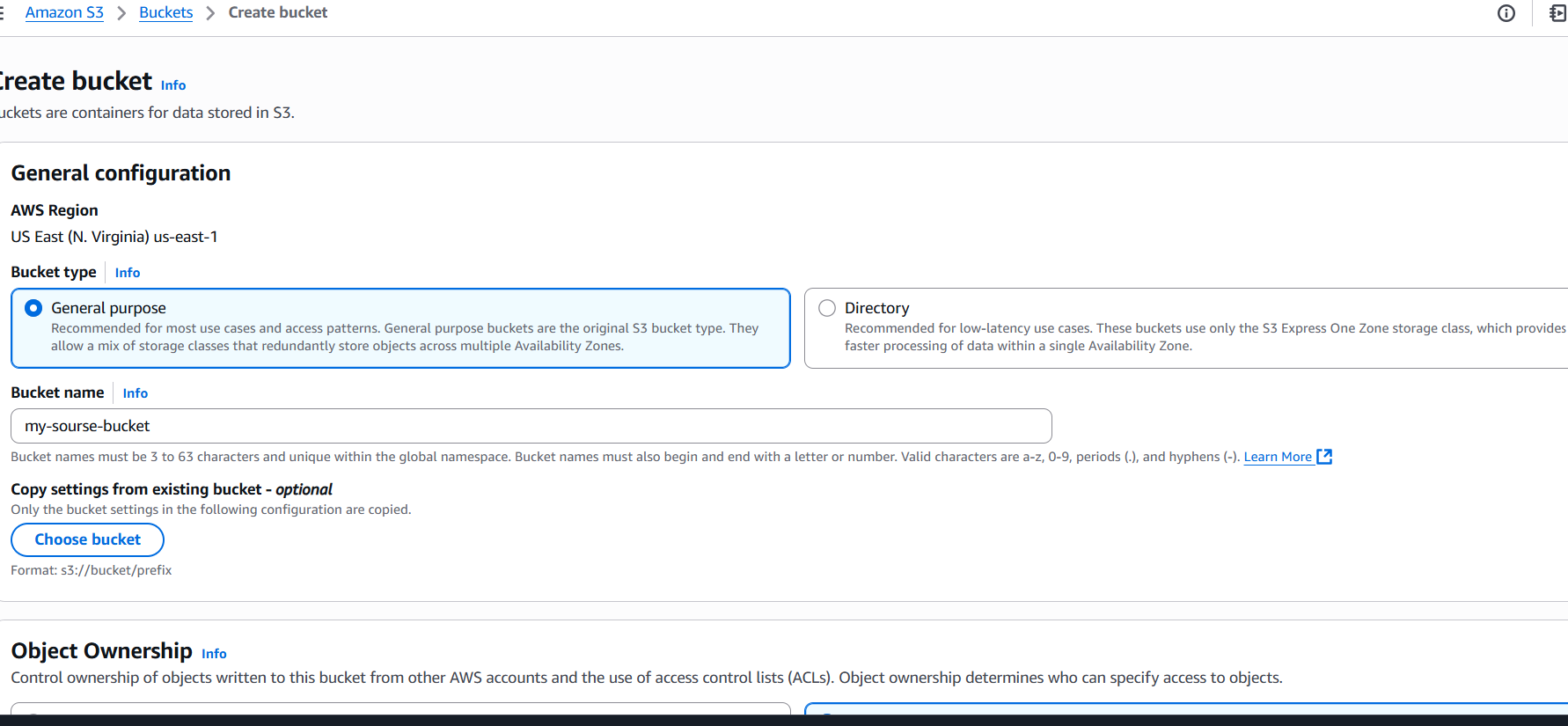


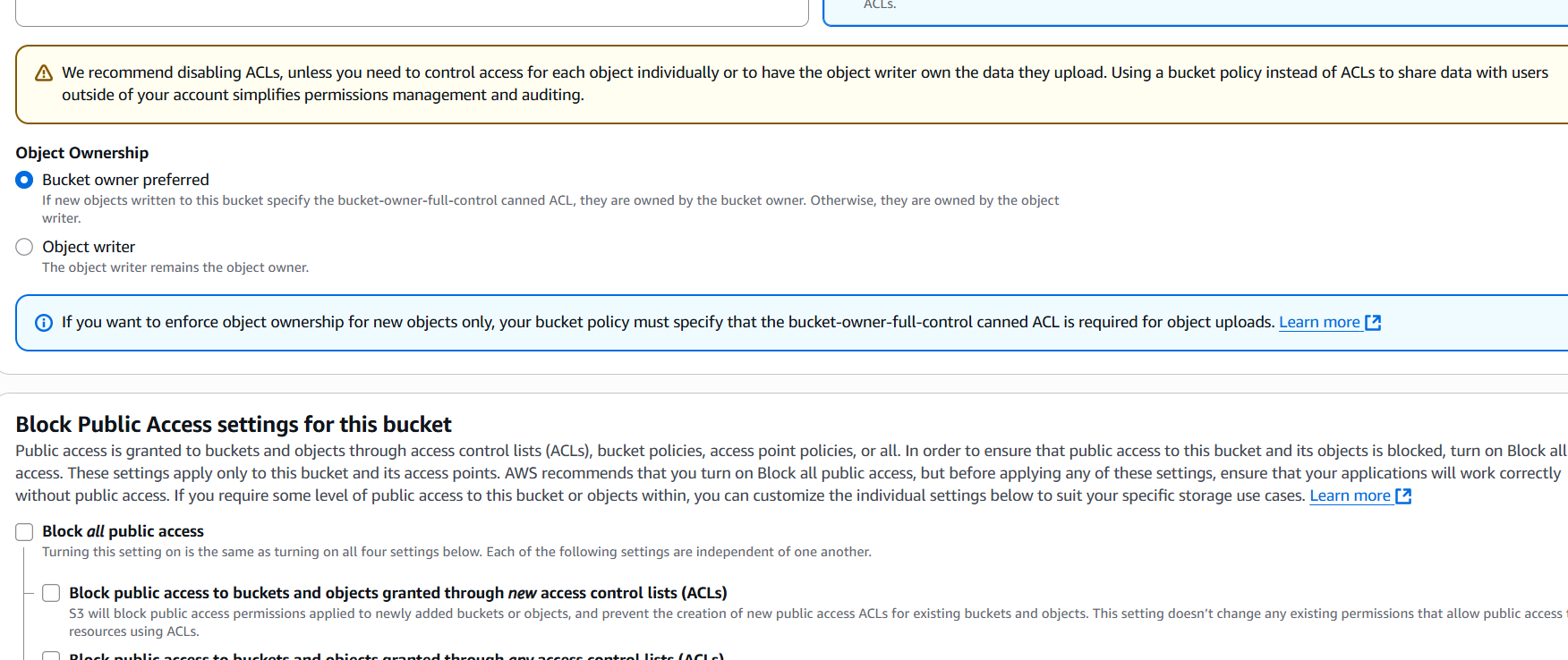


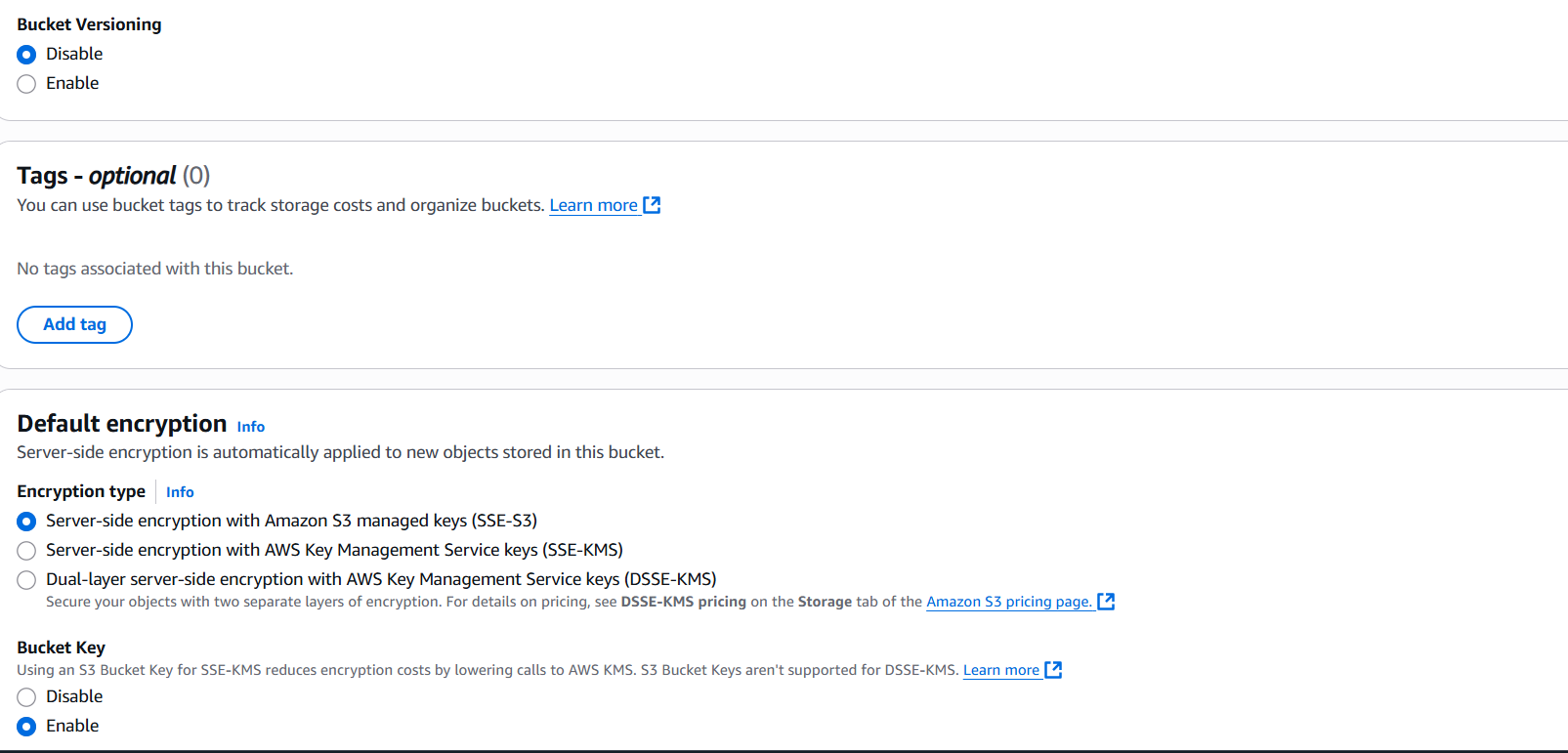


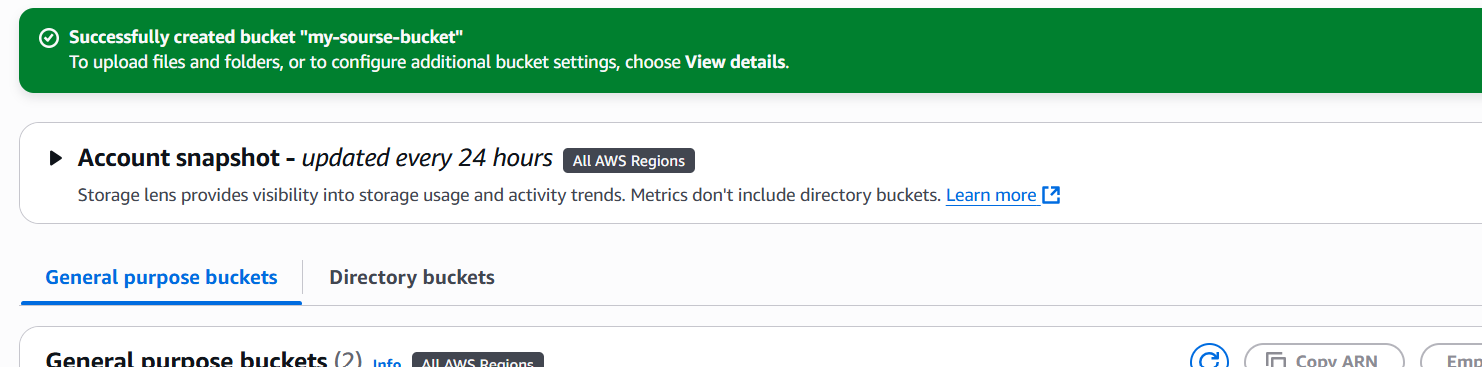


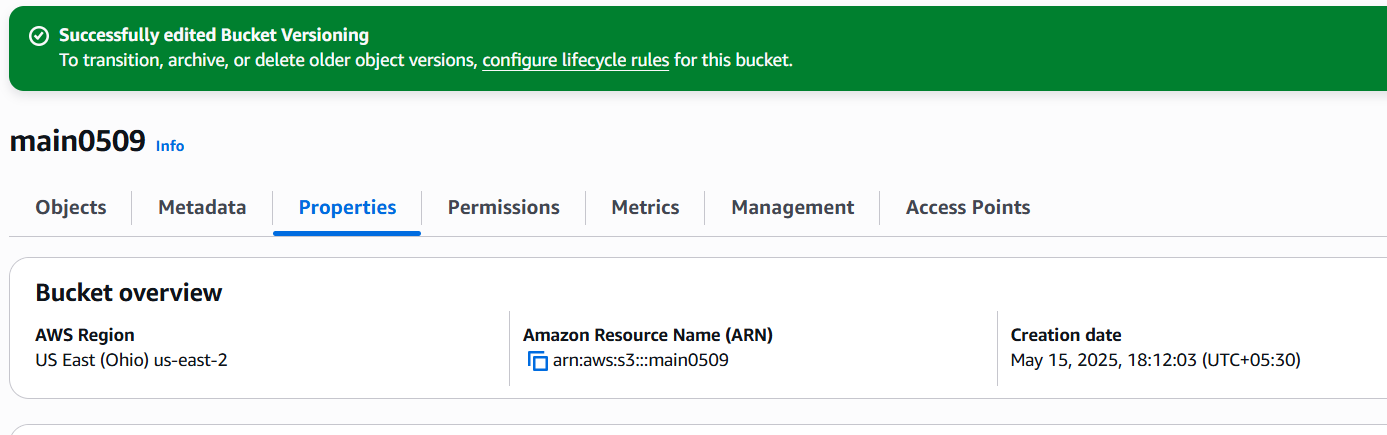
1. Enable cross region s3 buckets.

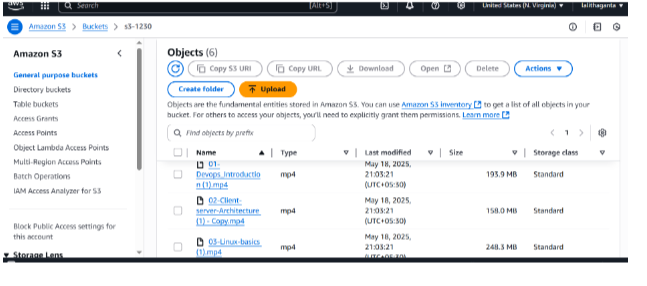


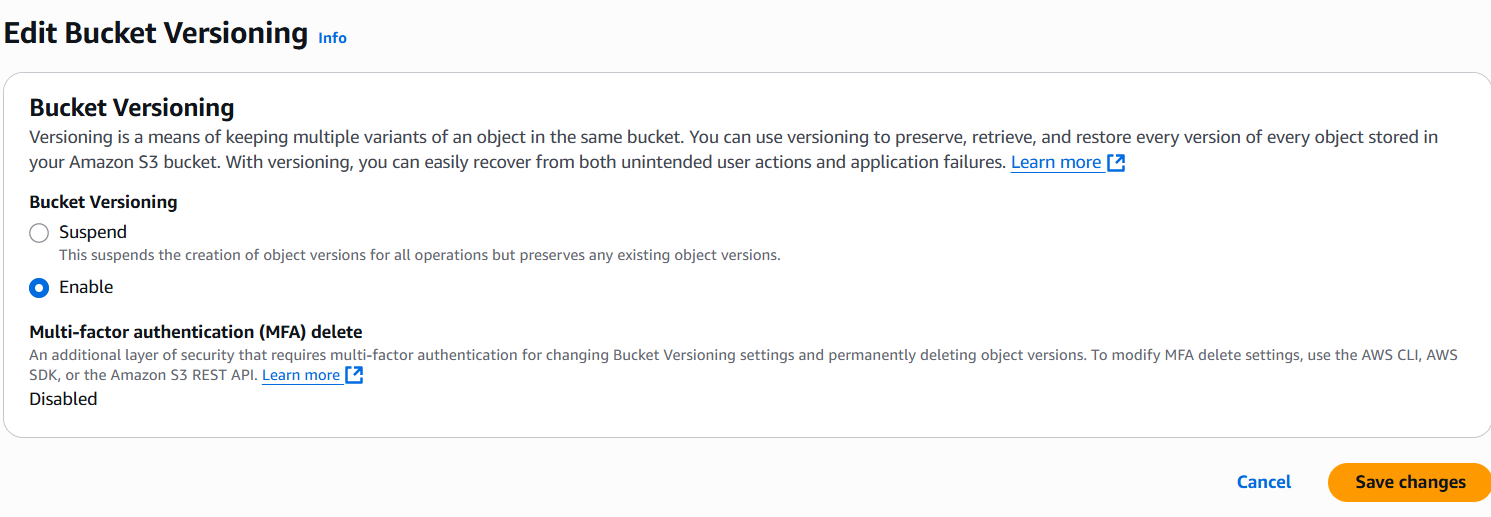


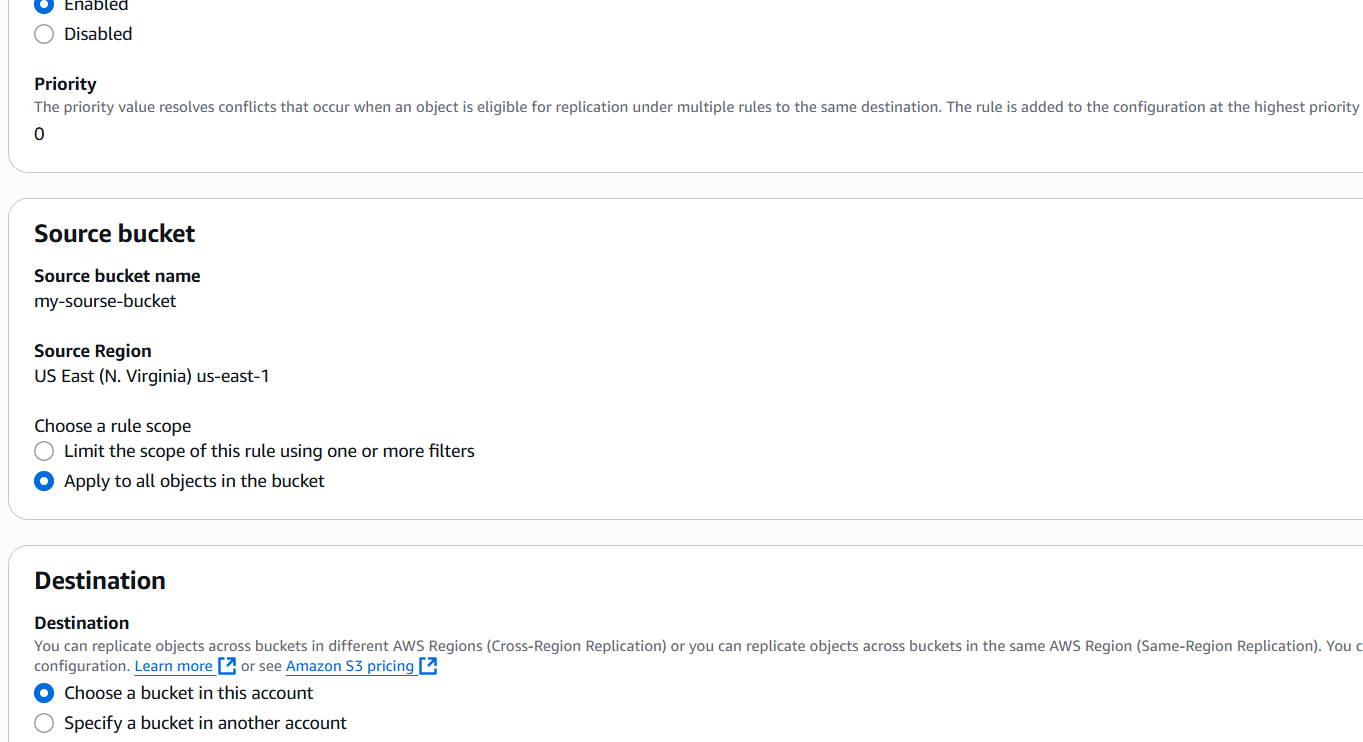


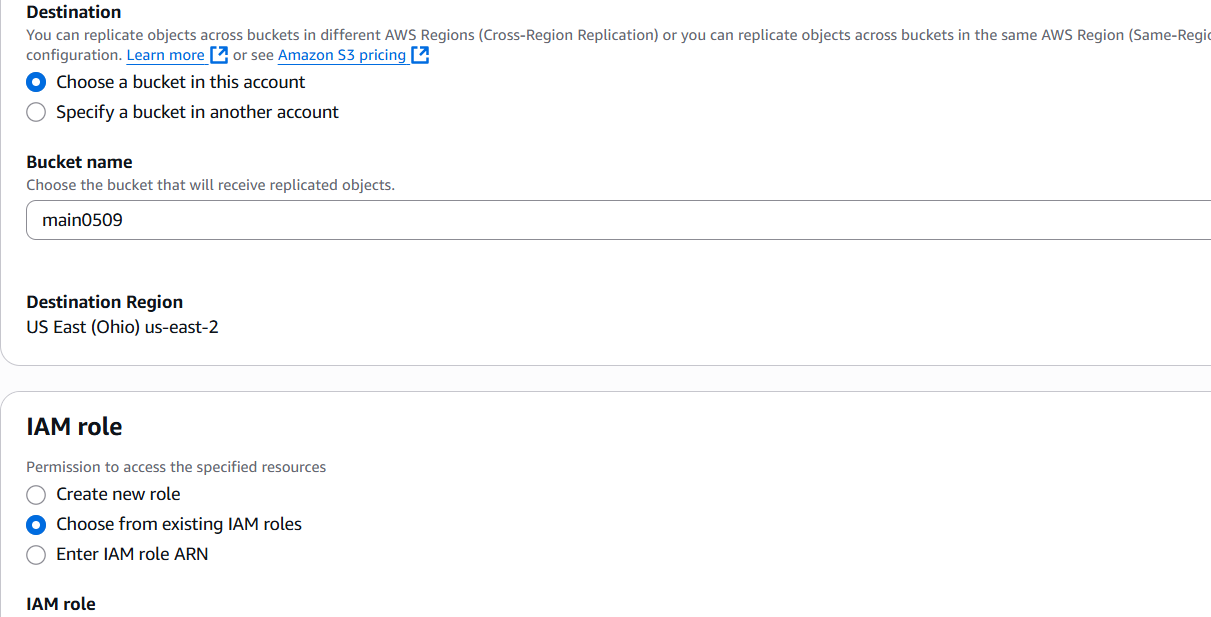


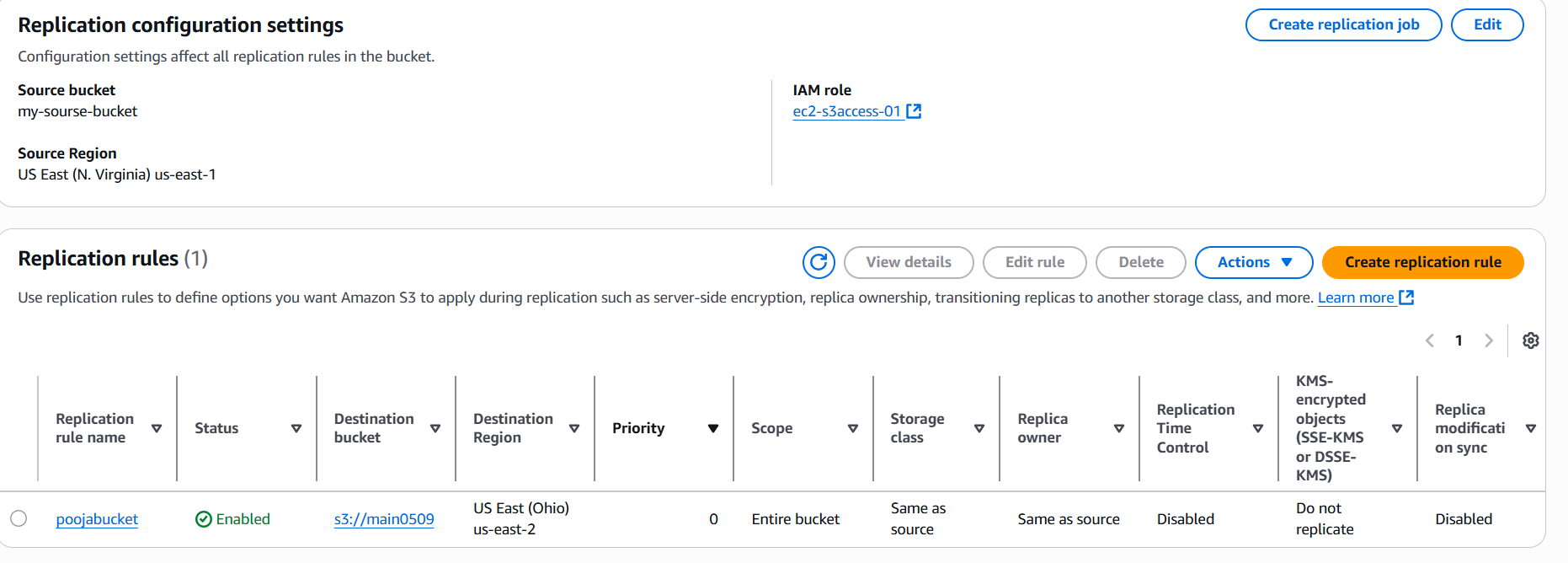








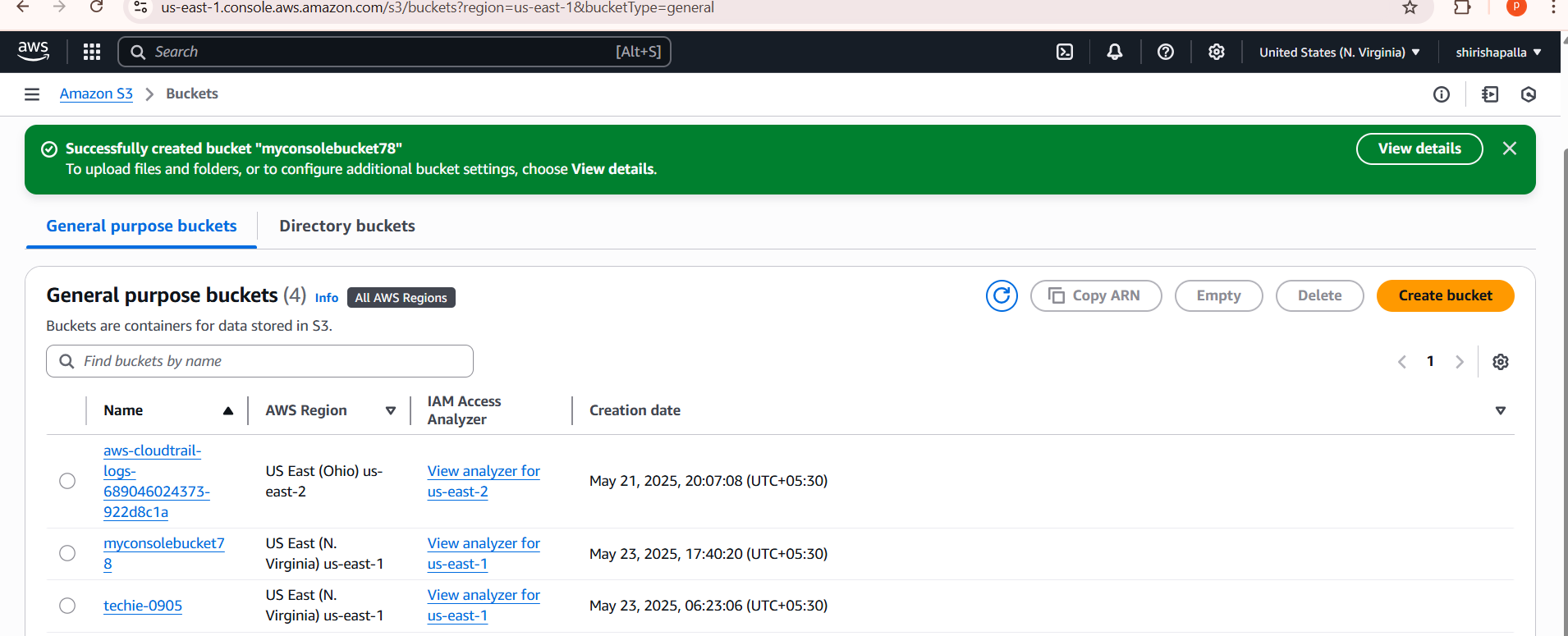




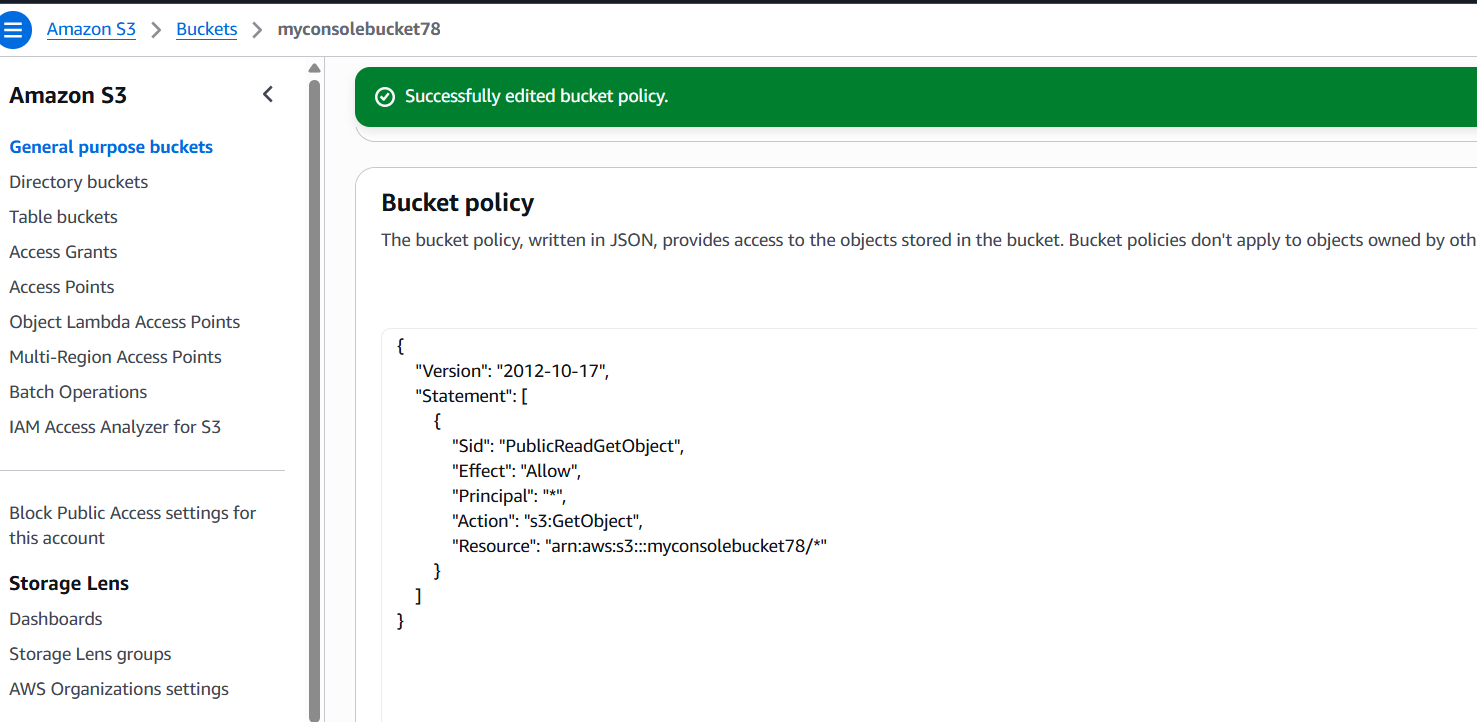
4)Configure bucket policy, only Admin user can see the objects of s3 bucket.

Step 1: Select the Bucket  
1. Log in to the AWS Management Console.  
2. Navigate to the S3 dashboard

3. Select the bucket (e.g., myconsolebucket78)



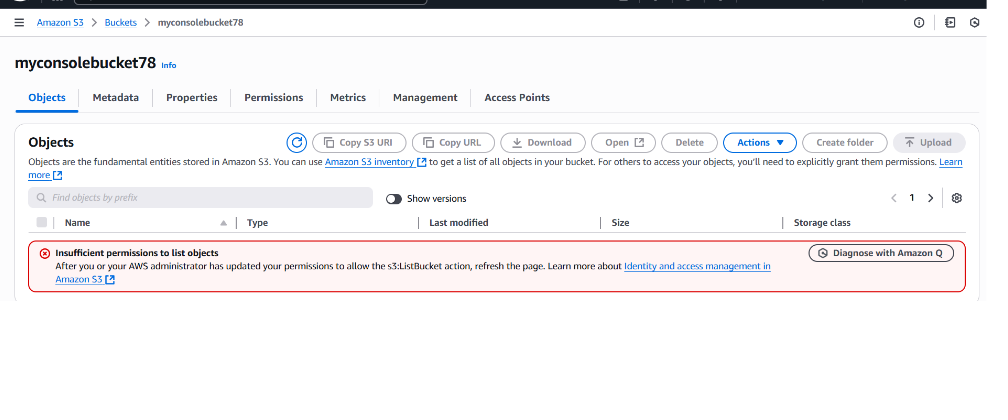
Step 2: Edit Bucket Policy  
1. Click "Permissions" and then "Bucket policy".  
2. Click "Edit



Step 3: Configure and save the Policy

1. In the policy document, add the following  
2. Click "Save changes" to apply the bucket policy.  
{  
 "Version": "2012-10-17",  
 "Statement": [  
 {  
 "Sid": "AllowOnlyRootAccess",  
 "Effect": "Allow",  
 "Principal": {  
 "AWS": "arn:aws:iam:: 689046024373:root"  
 },  
 "Action": "s3:\*",  
 "Resource": [  
 "arn:aws:s3:::myconsolebucket78",  
 "arn:aws:s3:::myconsolebucket78/\*"  
 ]  
 },  
 {  
 "Sid": "DenyAllOthers",  
 "Effect": "Deny",  
 "Principal": "\*",  
 "Action": "s3:\*",  
 "Resource": [  
 "arn:aws:s3:::myconsolebucket78",  
 "arn:aws:s3:::myconsolebucket78/\*"  
 ],  
 "Condition": {  
 "StringNotEquals": {  
 "aws:PrincipalArn": "arn:aws:iam:: 689046024373:root"  
 }  
 }  
 }  
 ]

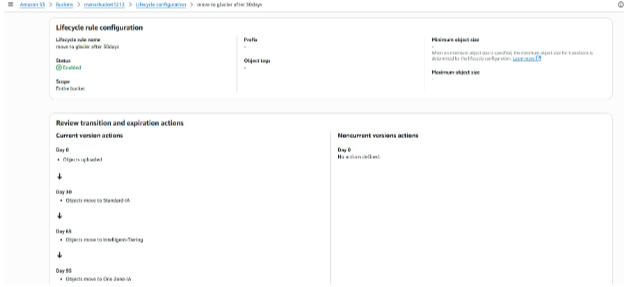
}



5) Setup lifecycle policies to automatically transition or delete objects based on specific criteria.

Go to the S3 Console: Log in to the AWS Management Console   
and navigate to the S3 service.  
• Select the S3 Bucket: Choose the bucket where you want to   
apply the lifecycle policy.

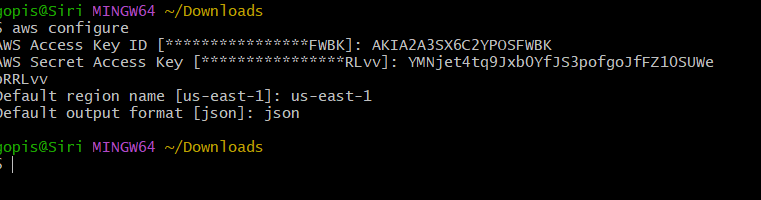
• Navigate to the "Management" Tab: In the bucket settings, go  
to the "Management" tab.  
• Create a Lifecycle Rule: Under the "Lifecycle rules" section,   
click on "Create lifecycle rule."  
• Define Rule Name and Scope:  
•Enter a name for your rule.  
•Specify whether the rule applies to all objects or a specific   
prefix/tag.  
• Define Transitions and Expirations:  
•Transition actions: Move objects to another storage class, like   
Glacier or Deep Archive, after a specified number of days.  
•Expiration actions: Automatically delete objects after they reach   
a certain age (e.g., 30 days).  
• Review and Save: Review your settings and create the lifecycle   
rule.



1. Push some objects in s3 using AWS CLI.

Step 1: Install and Configure AWS CLI

1. Ensure you have AWS CLI installed on your machine, using command aws --version.



Step 2: Create a File to Upload



#!/bin/bash

# Define your variables

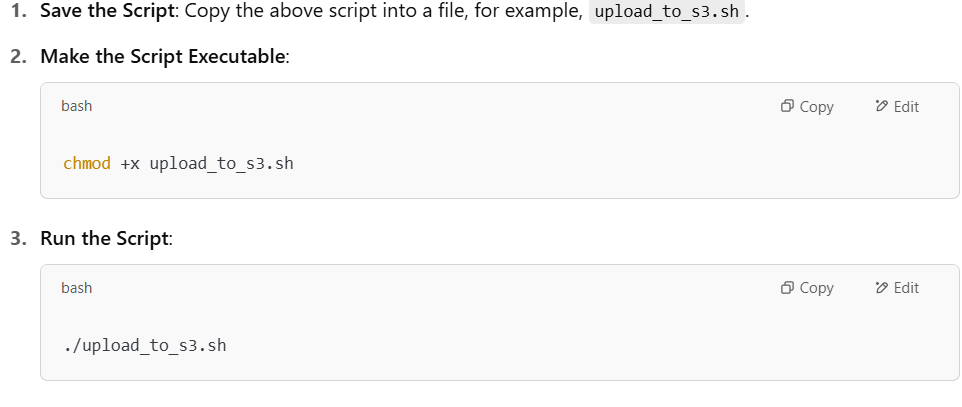
LOCAL\_DIR="/path/to/local/files" # Replace with your local directory path

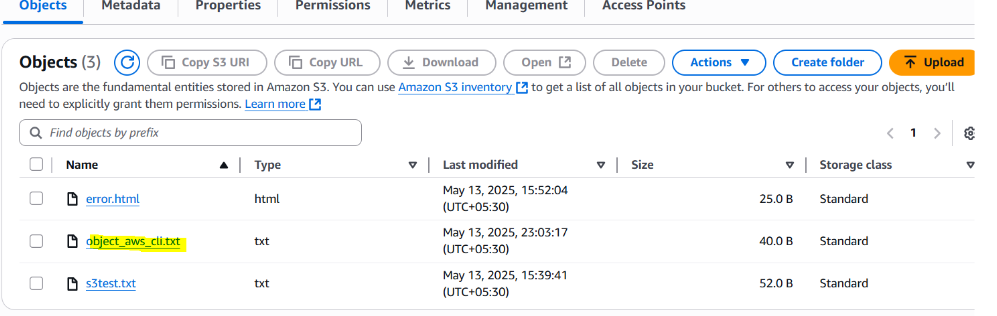
S3\_BUCKET="your-s3-bucket-name" # Replace with your S3 bucket name

S3\_PATH="optional/path/in/bucket" # Replace with your desired S3 path or leave empty

# Upload files to S3

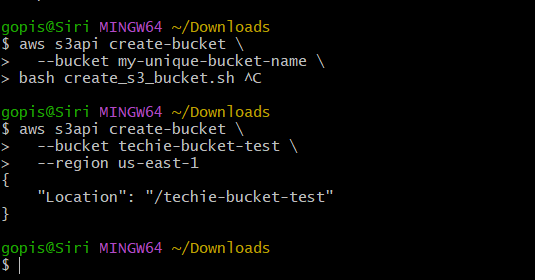
aws s3 cp "$LOCAL\_DIR" "s3://$S3\_BUCKET/$S3\_PATH" –recursive

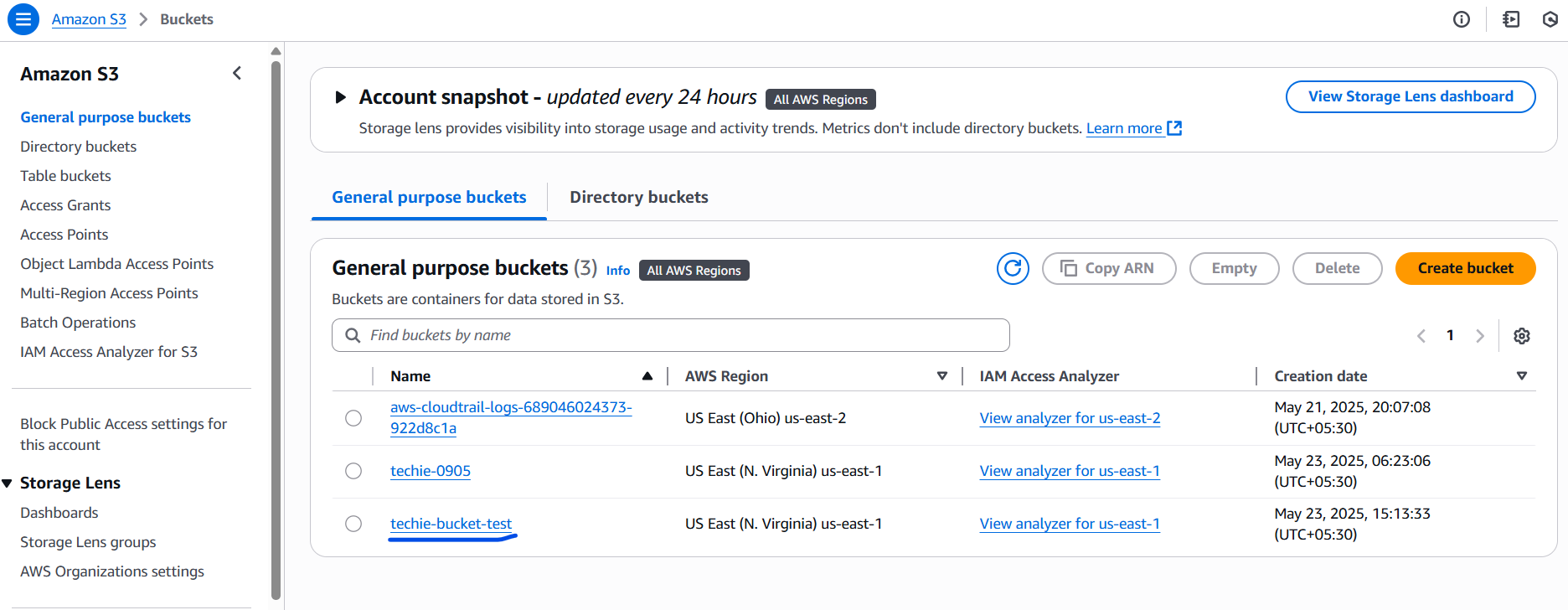




7) Write a bash script to create s3 bucket.

1. **Install AWS CLI**: Ensure that the AWS CLI is installed on your system.
2. **Configure AWS CLI**: Run aws configure to set up your AWS credentials and default region.
3. **Permissions**: Ensure that your IAM user or role has the necessary permissions to create S3 buckets.





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

