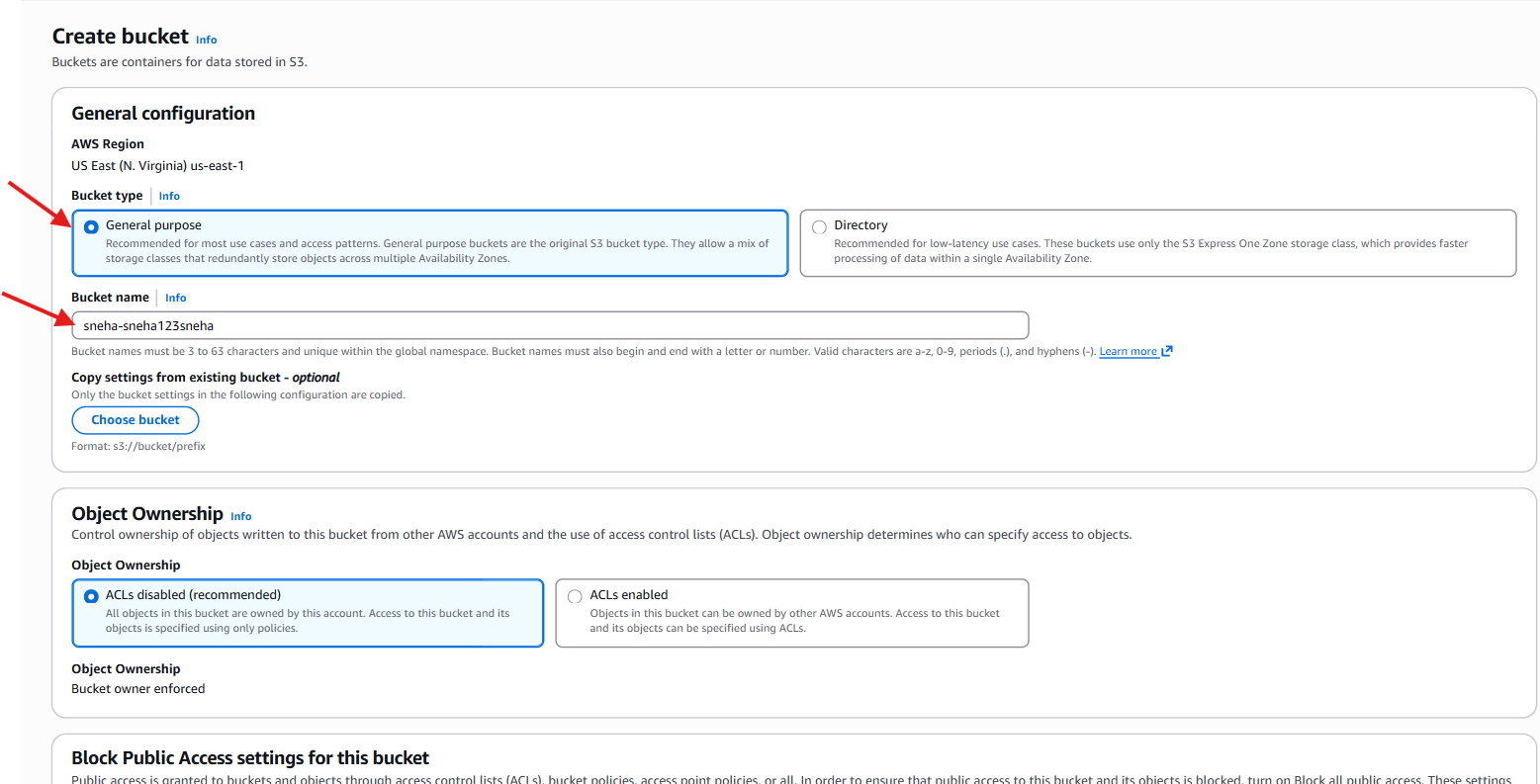
S3 TASK-01

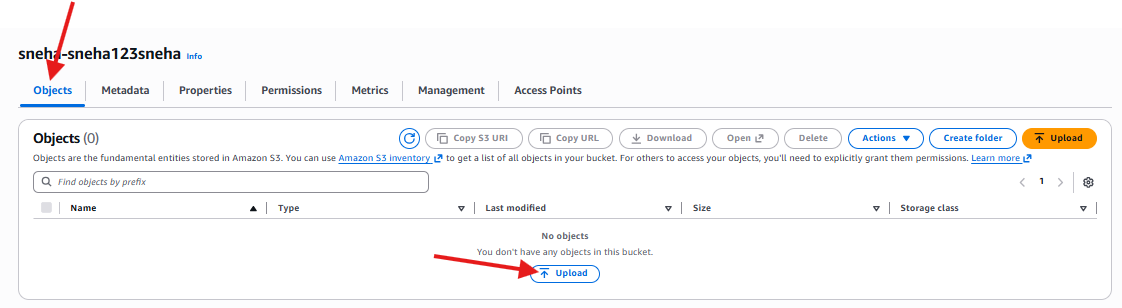
1. Create an S3 bucket and upload some objects to S3.



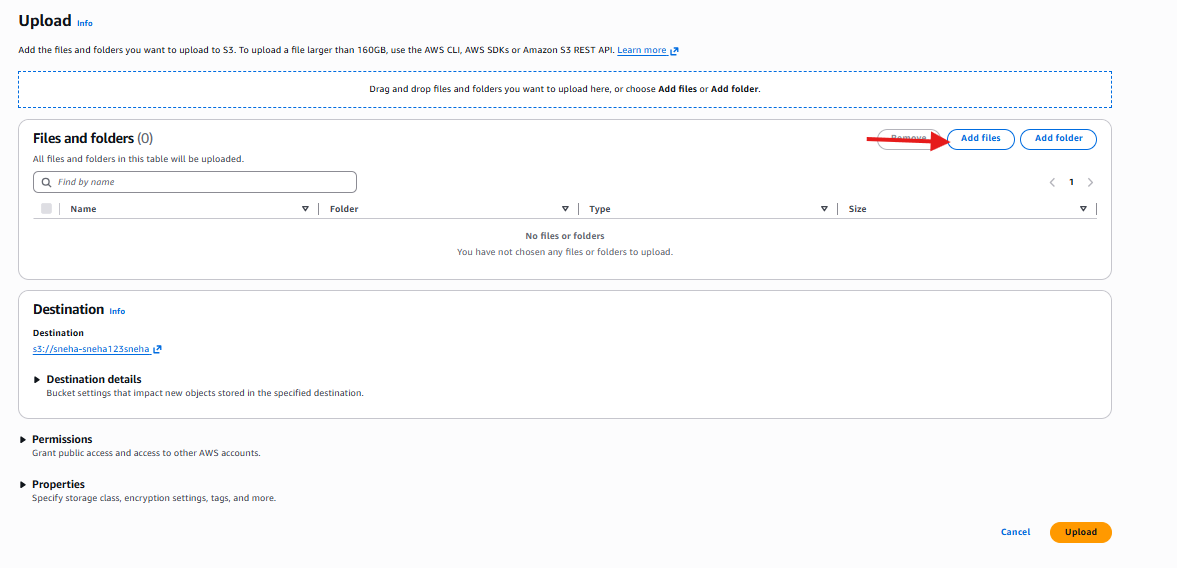
Successful bucket is created



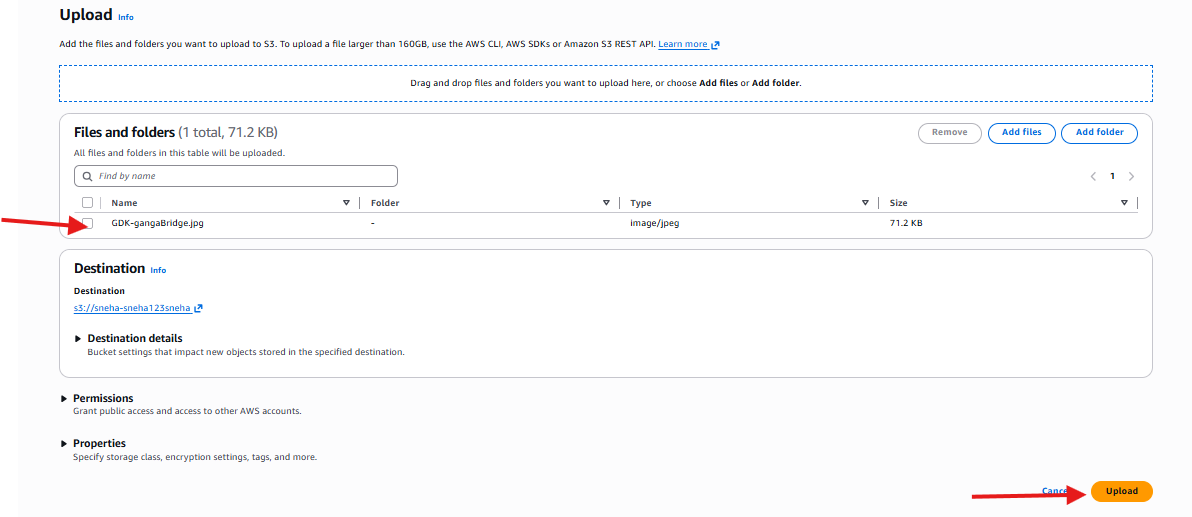
Hear you can upload the file



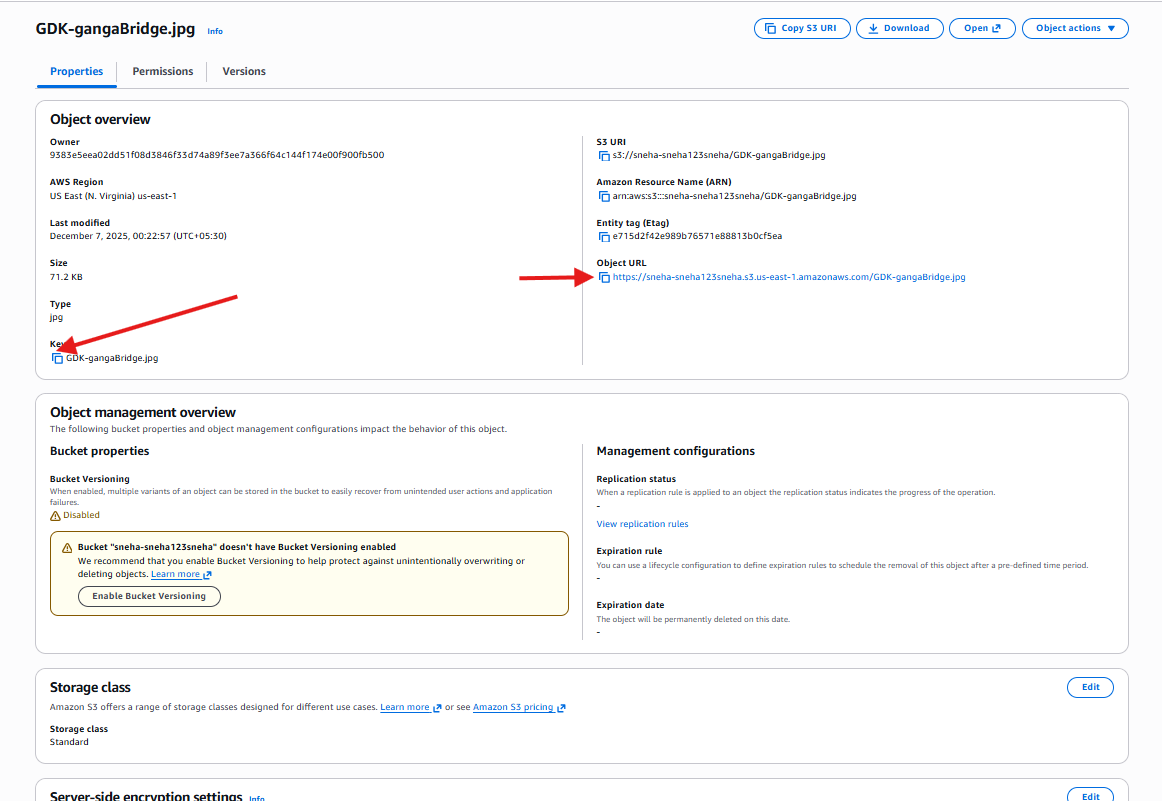
Hear you can add the file



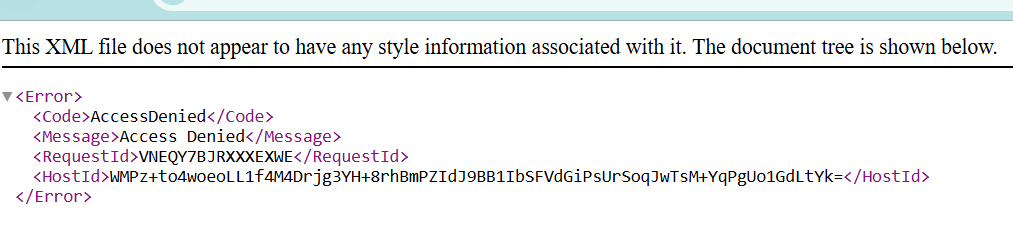
Added the file and uploaded

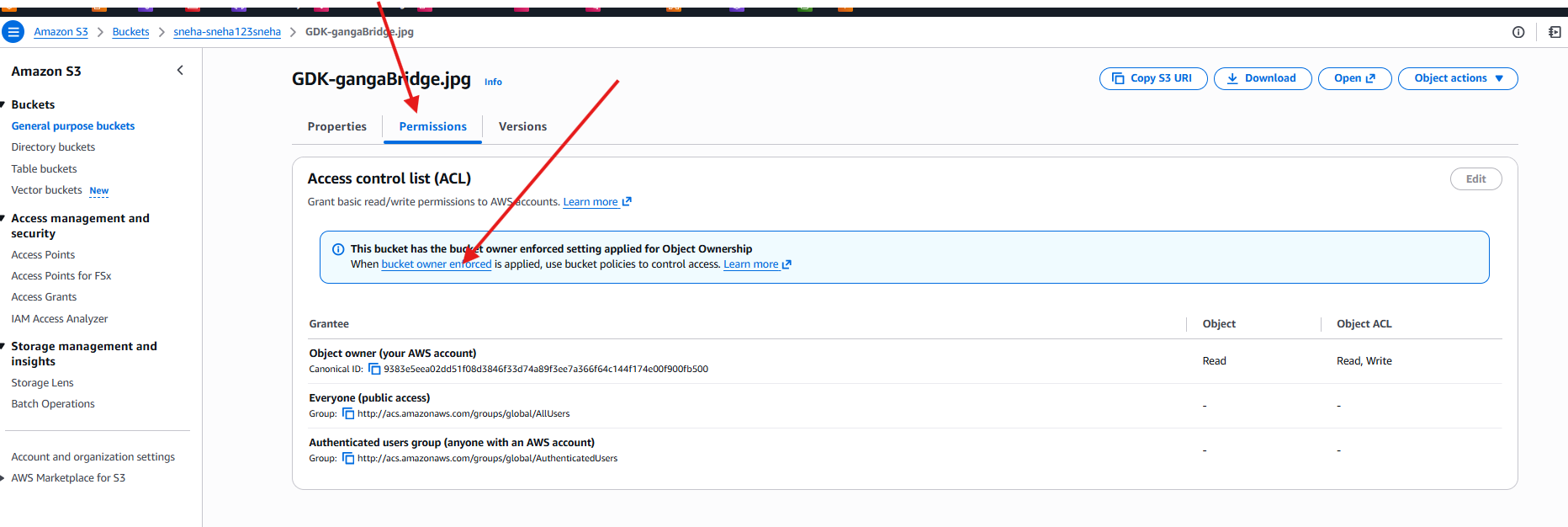


Go to the object overview

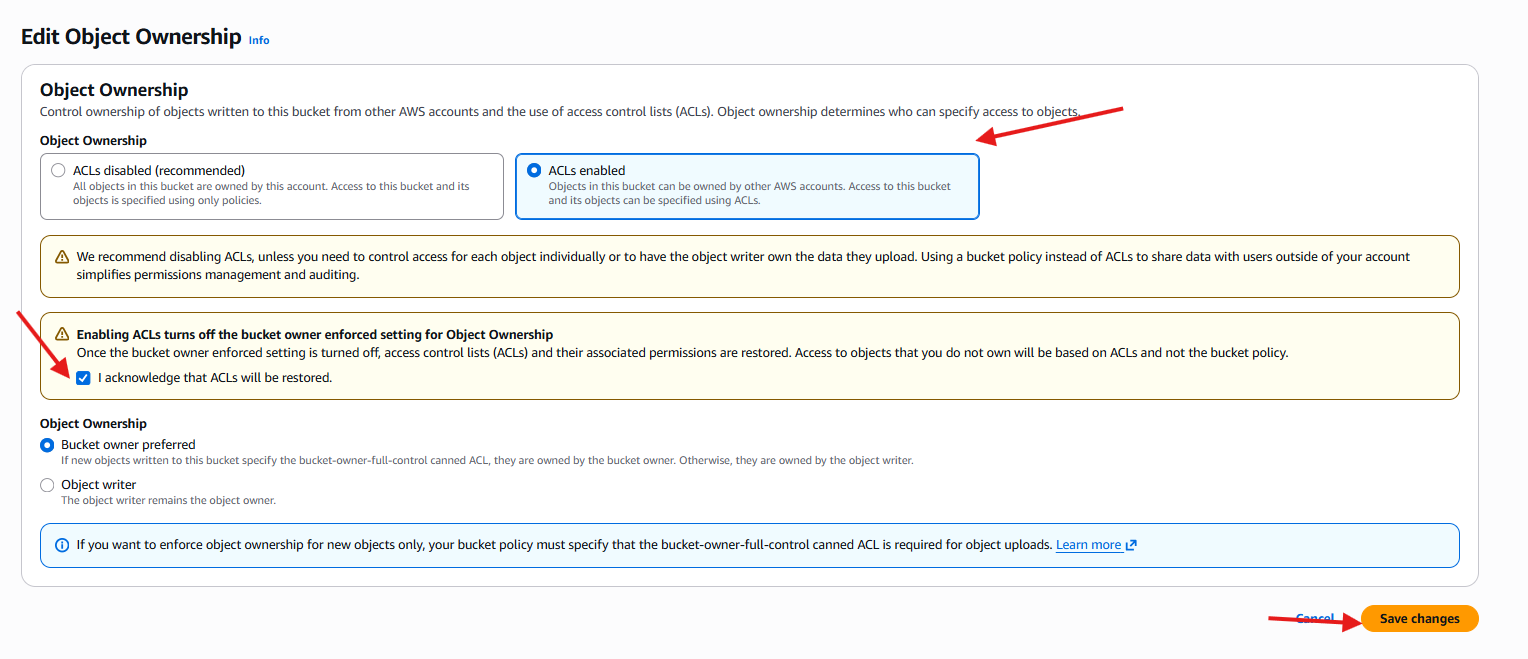


It’s getting error with xml format

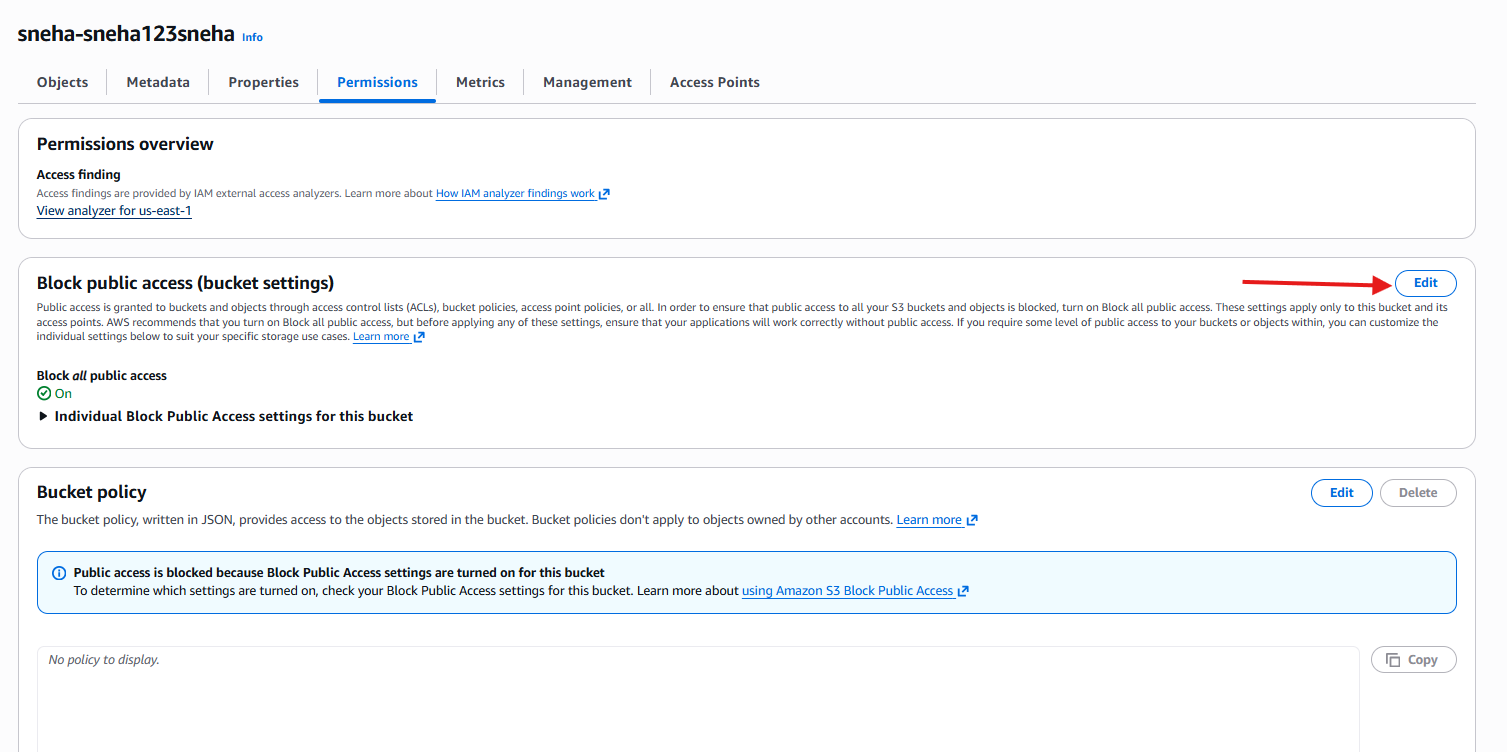


Go to the permissions and enable 

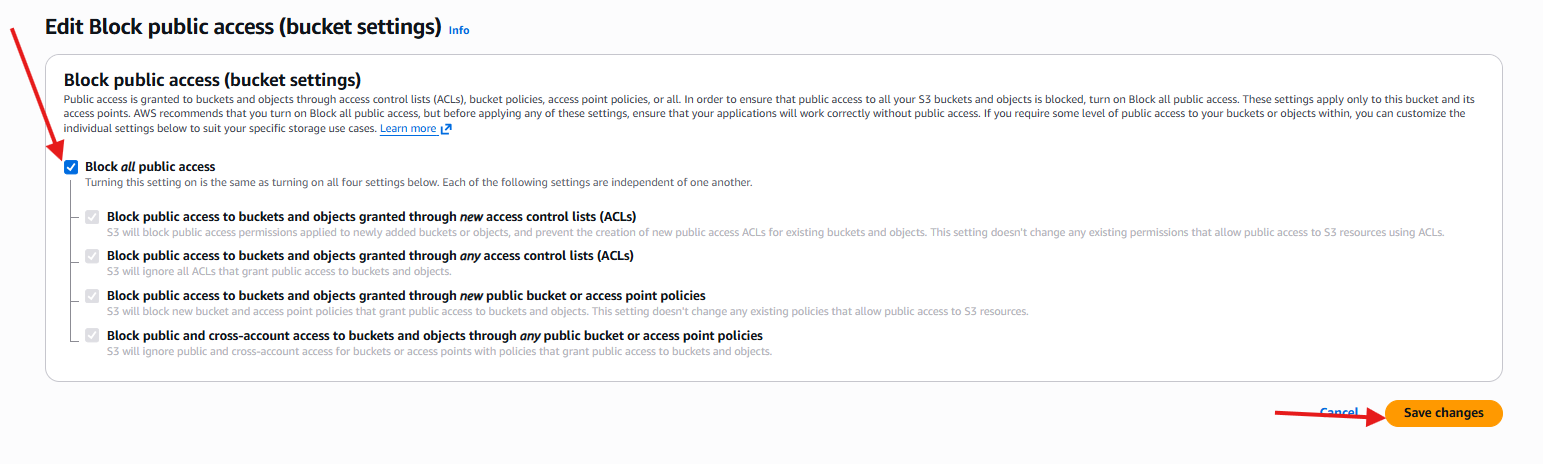
ACL enable



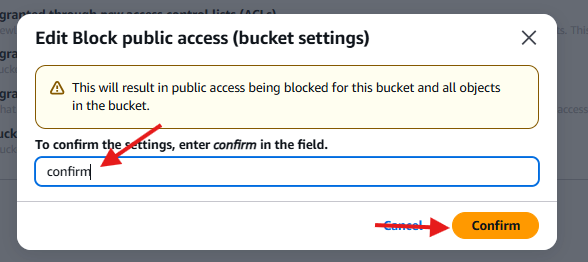
Go to the edits



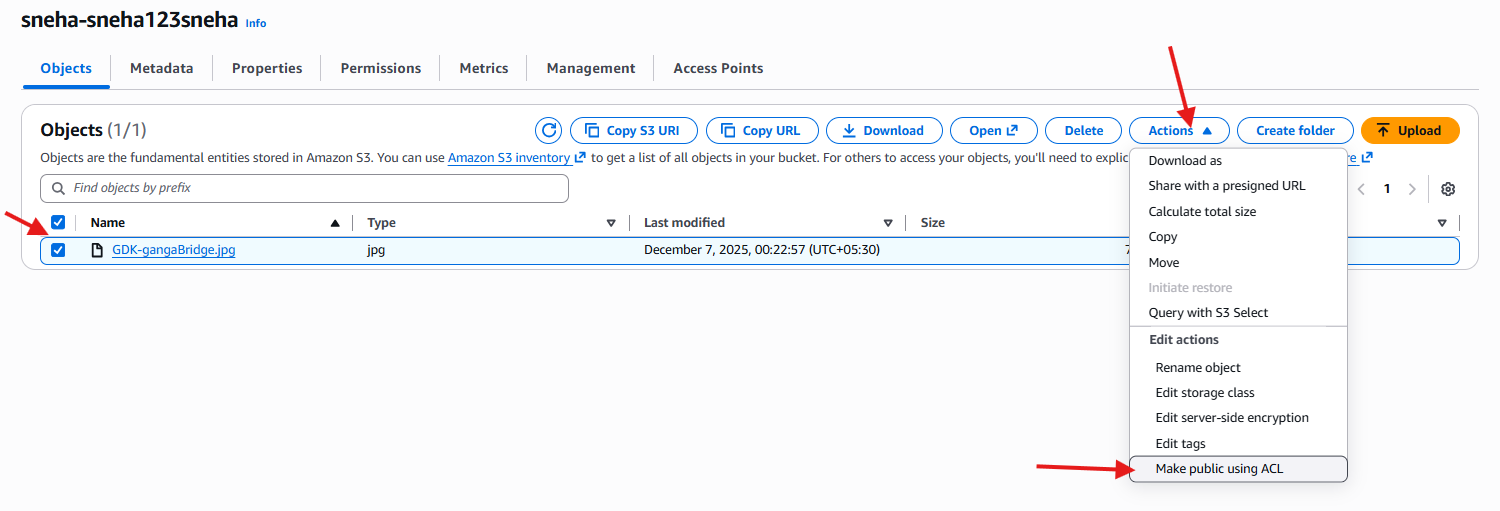
Enable public access



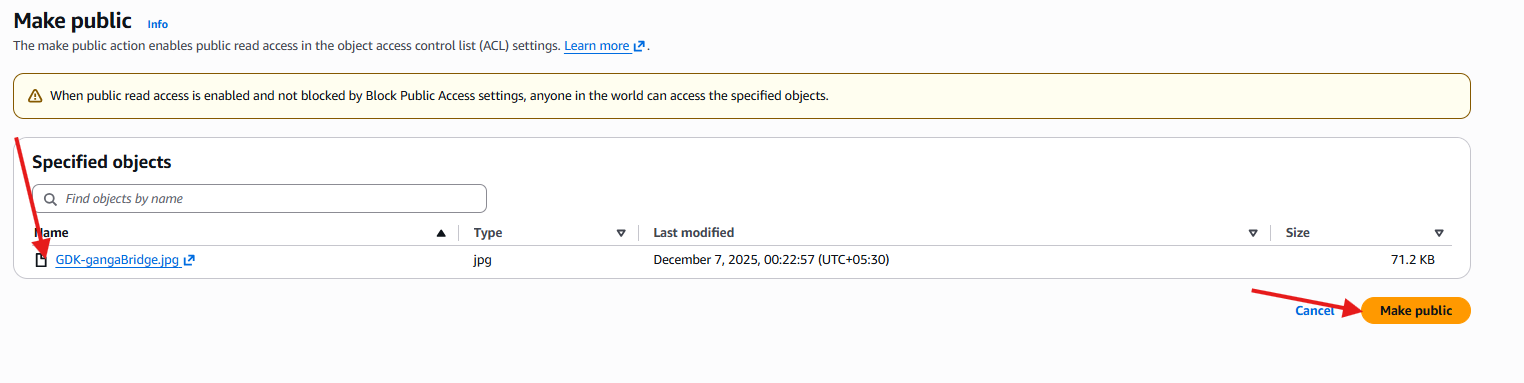
Confirm



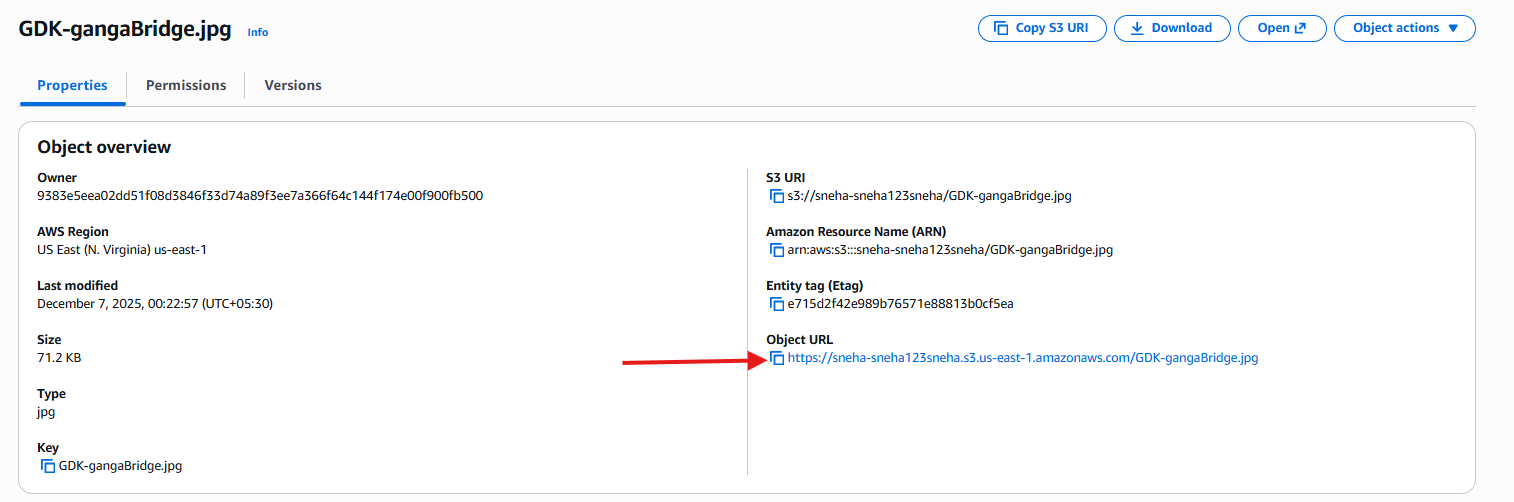
Go to the objects select the file and go to the actions and make public using ACL



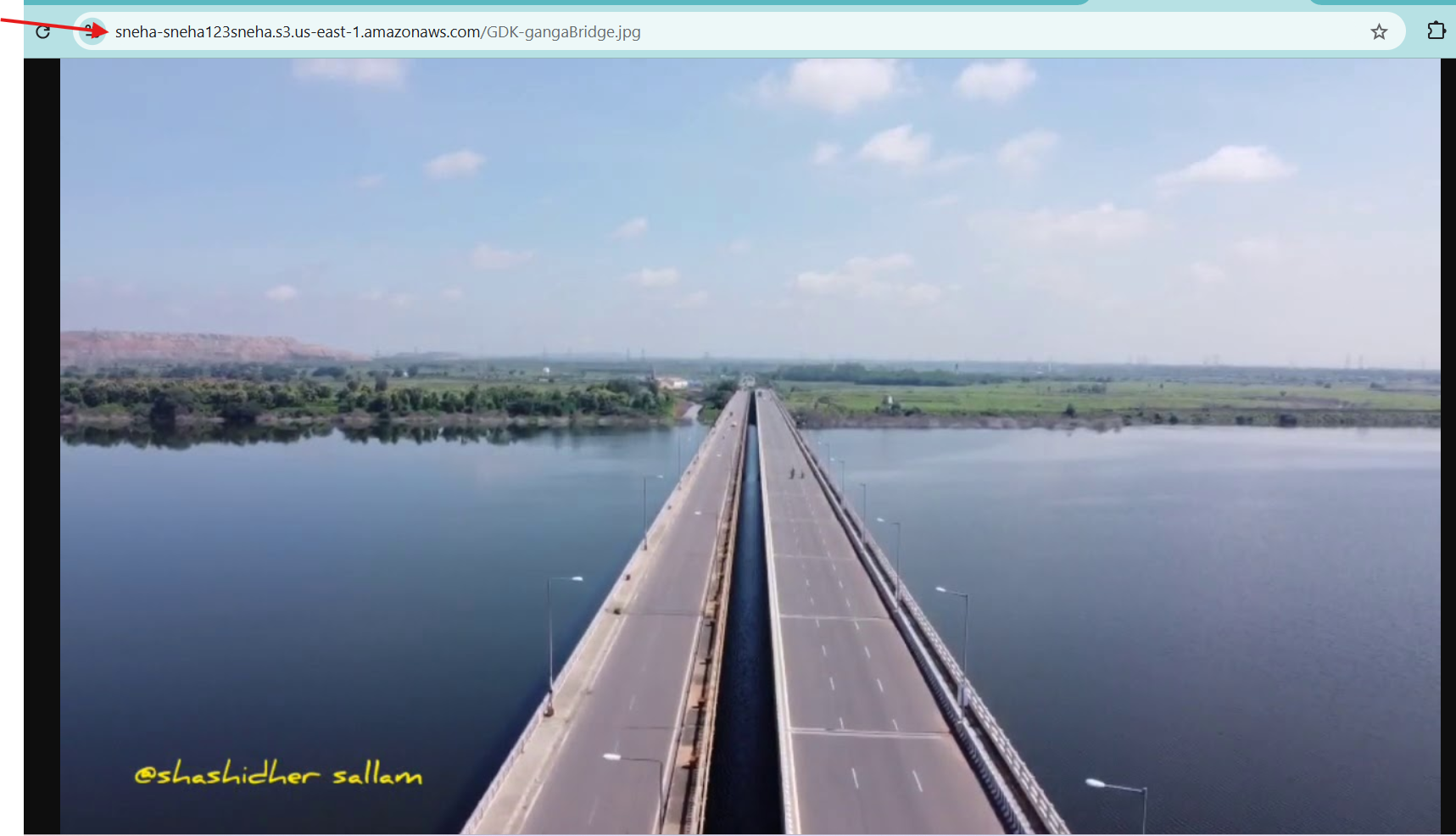
Make it public



Select the URL



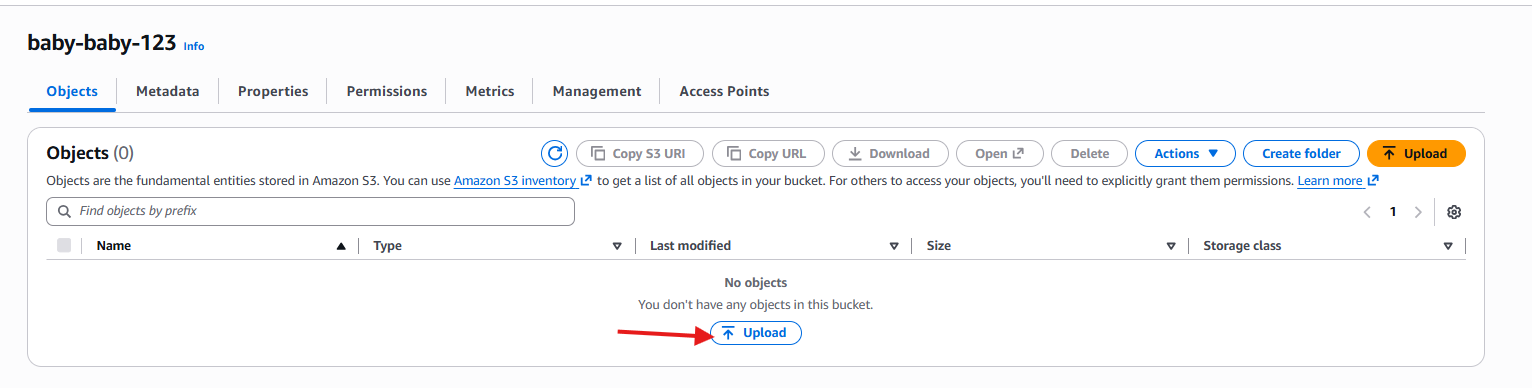
This is my S3 buck URL



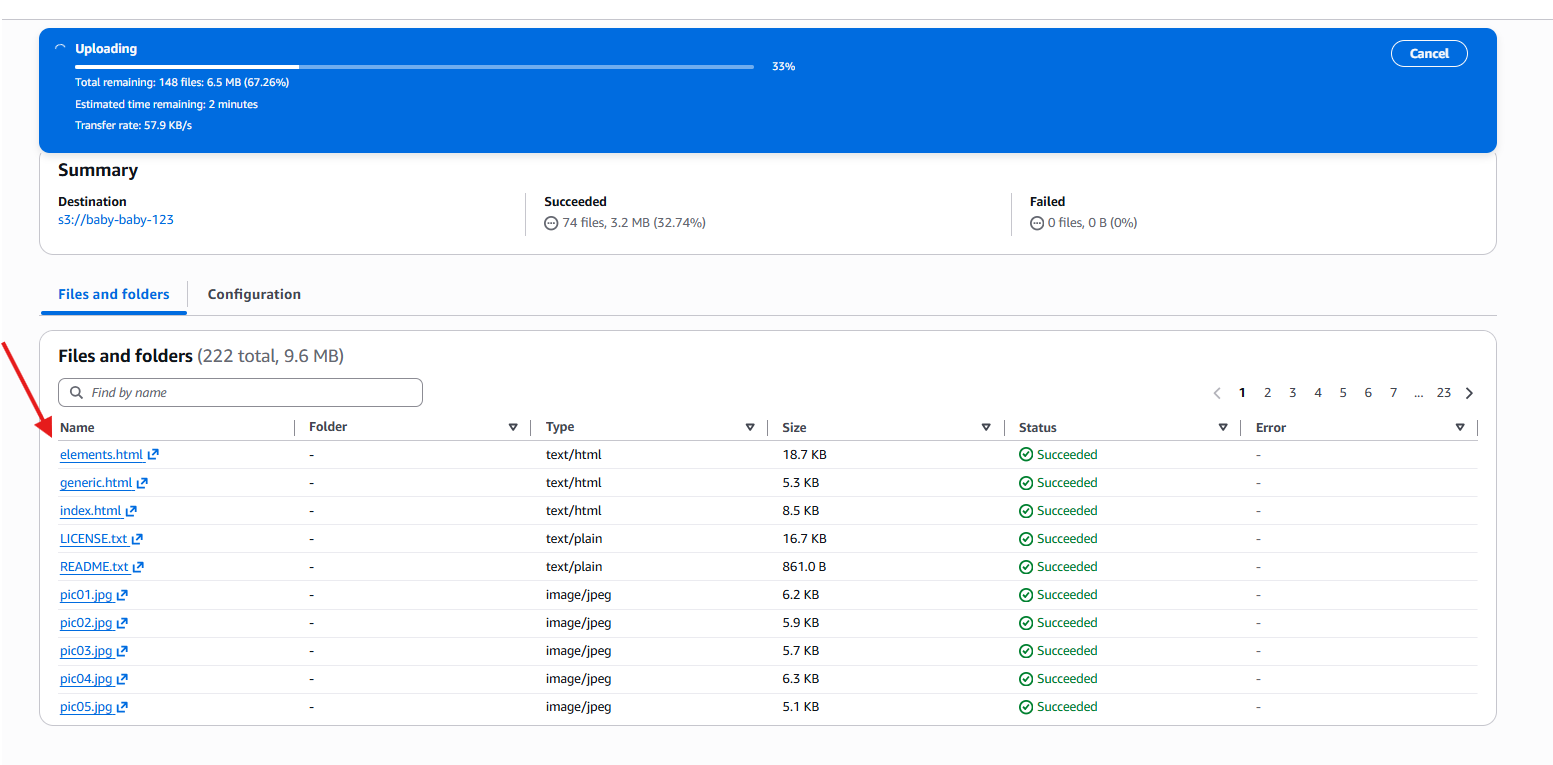
1. Deploy a static website in the S3 bucket.

Create one S3 bucket

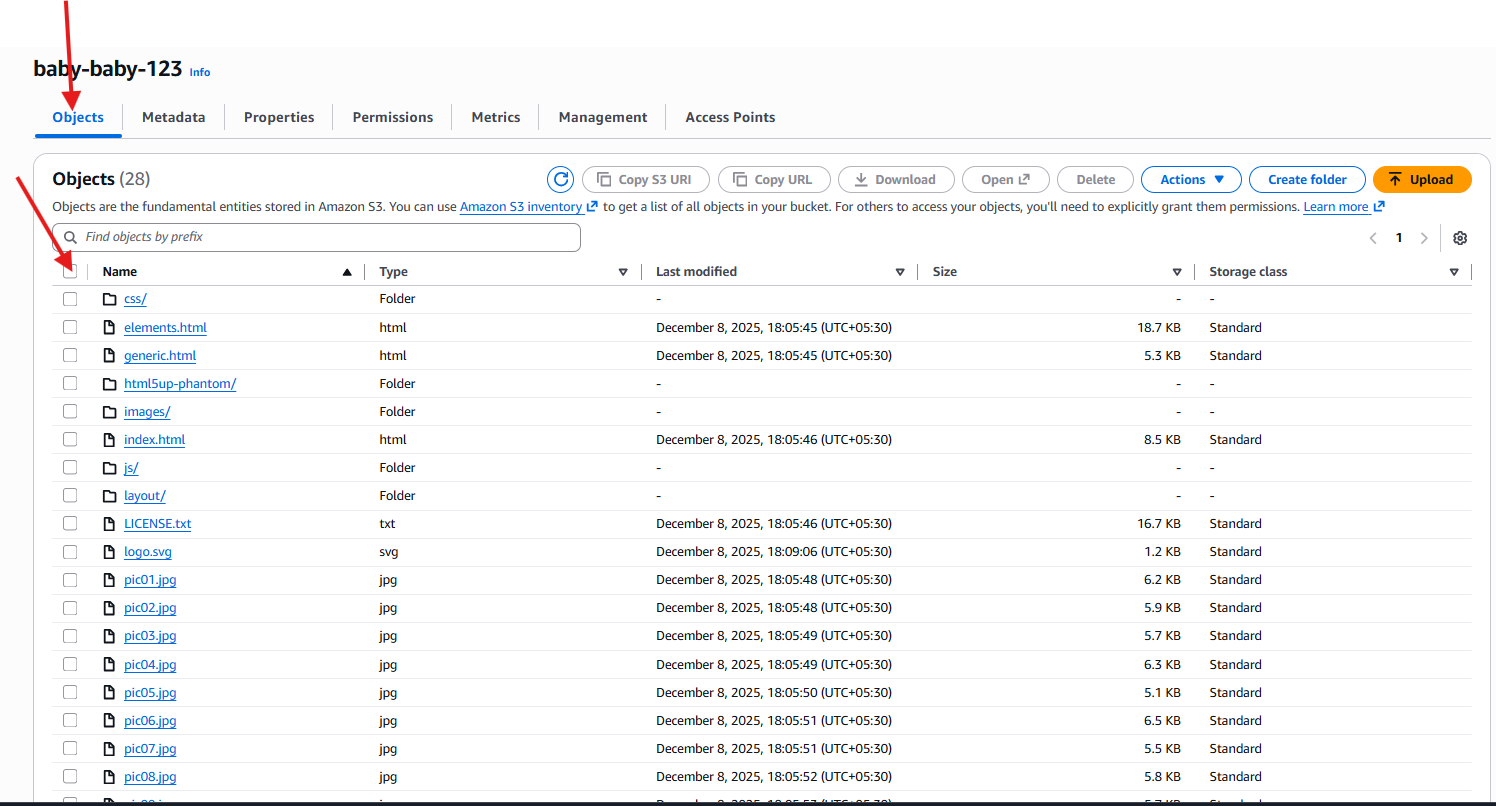
Upload the file



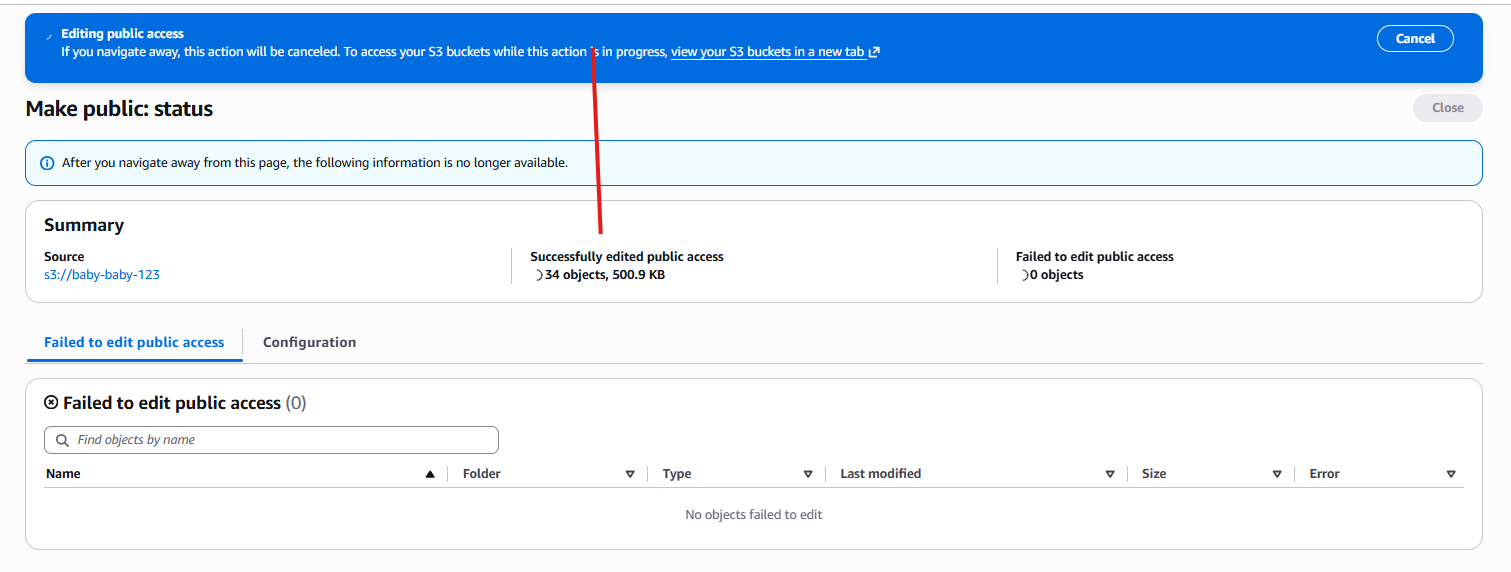
Upload a files and folder



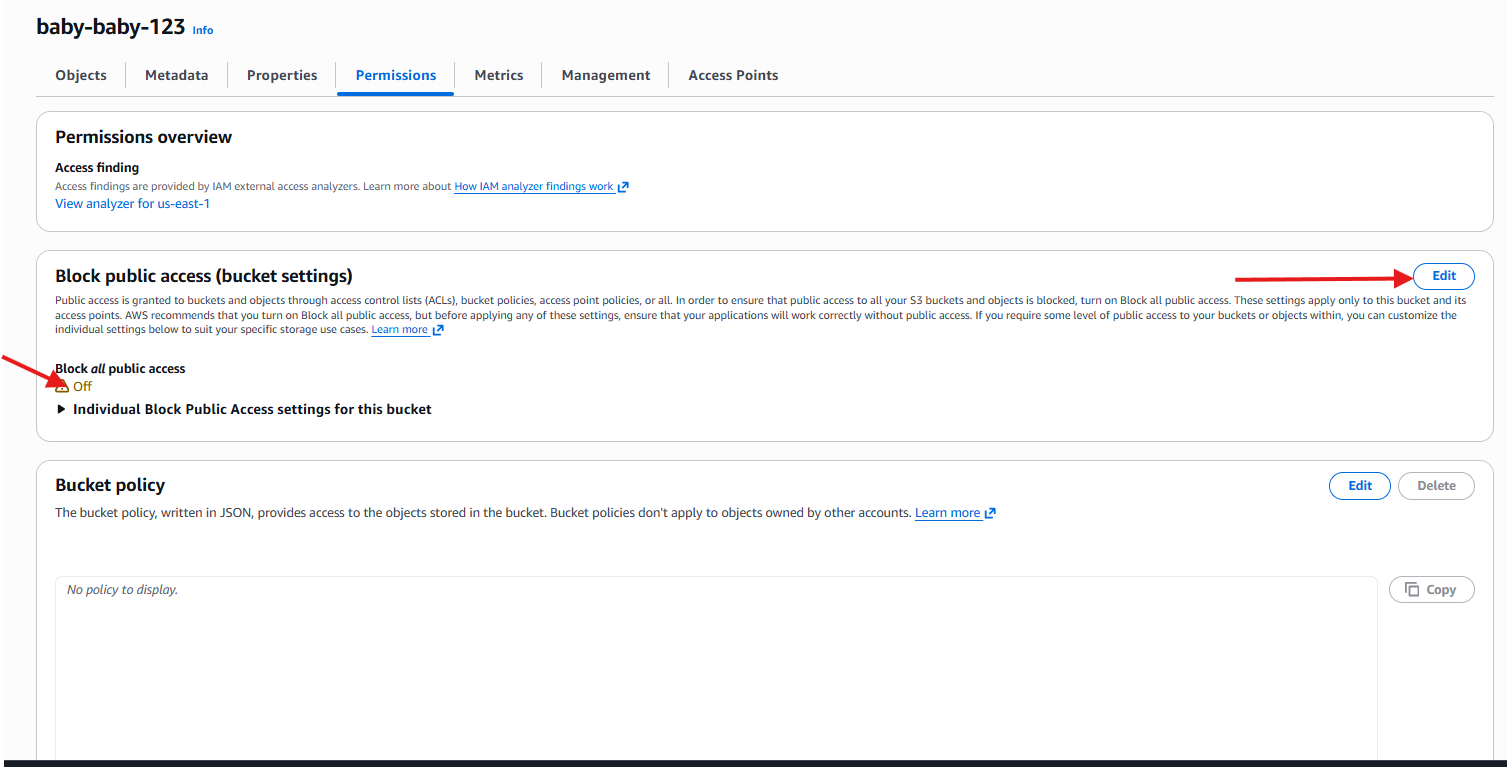
Objects has been uploaded successfully

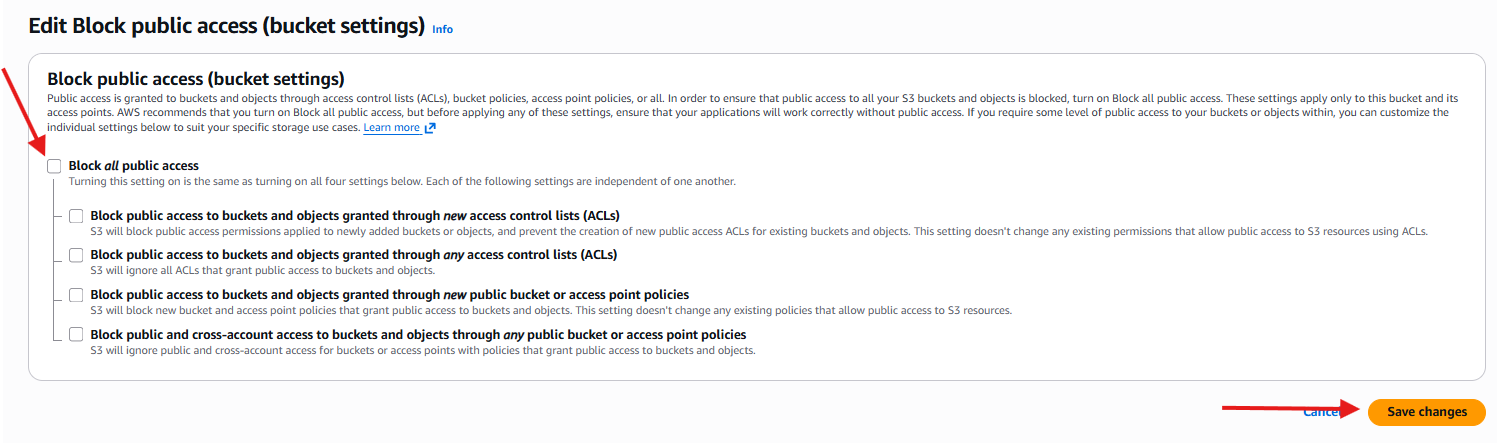


Give the permissions

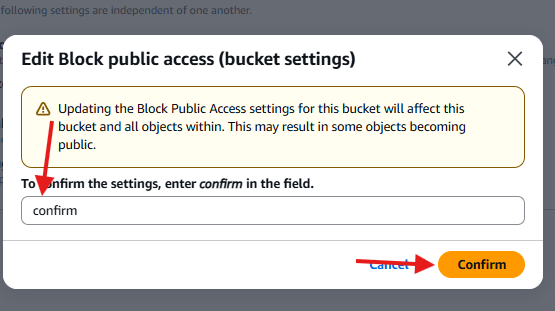


Give the public access

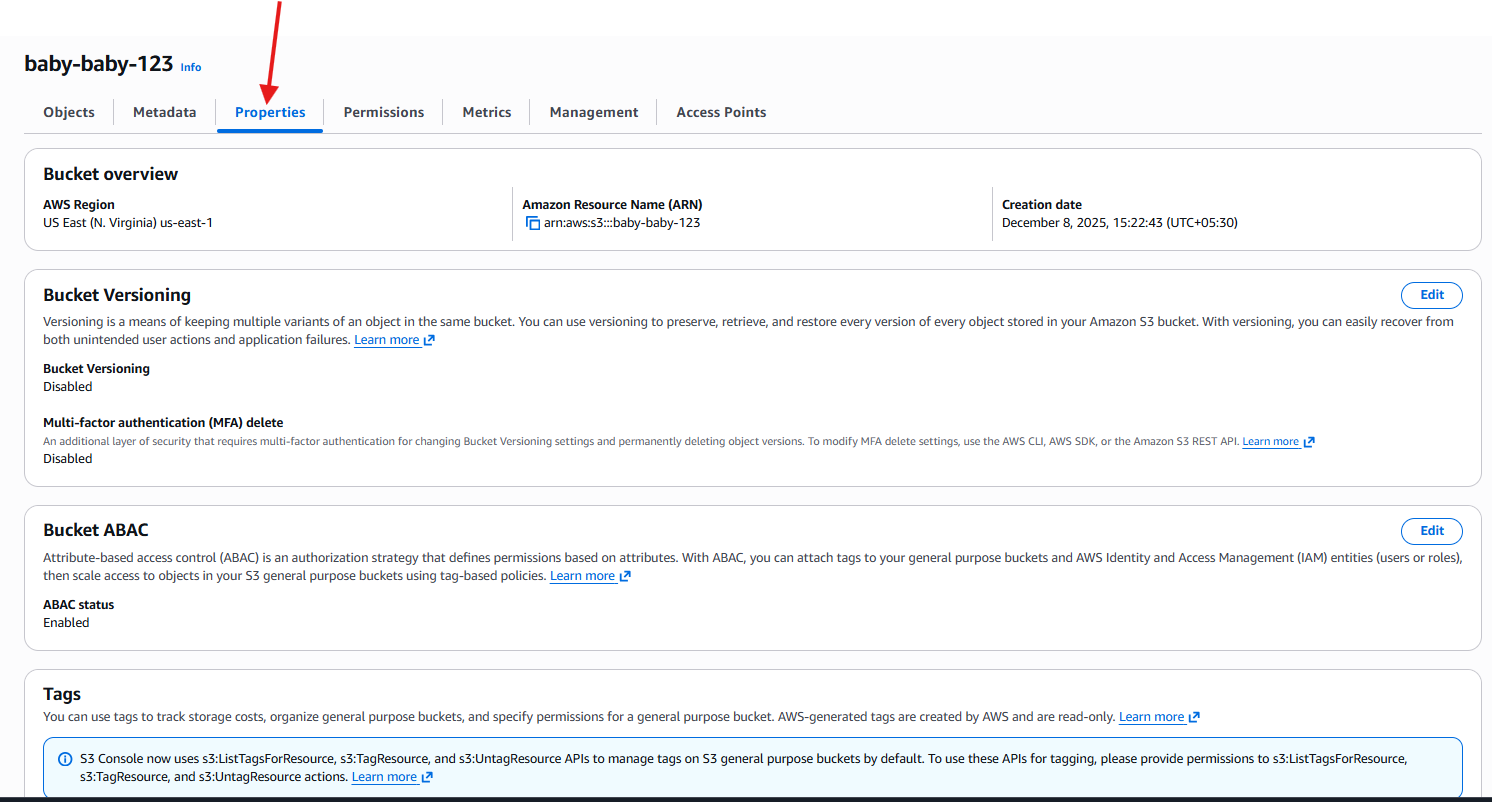




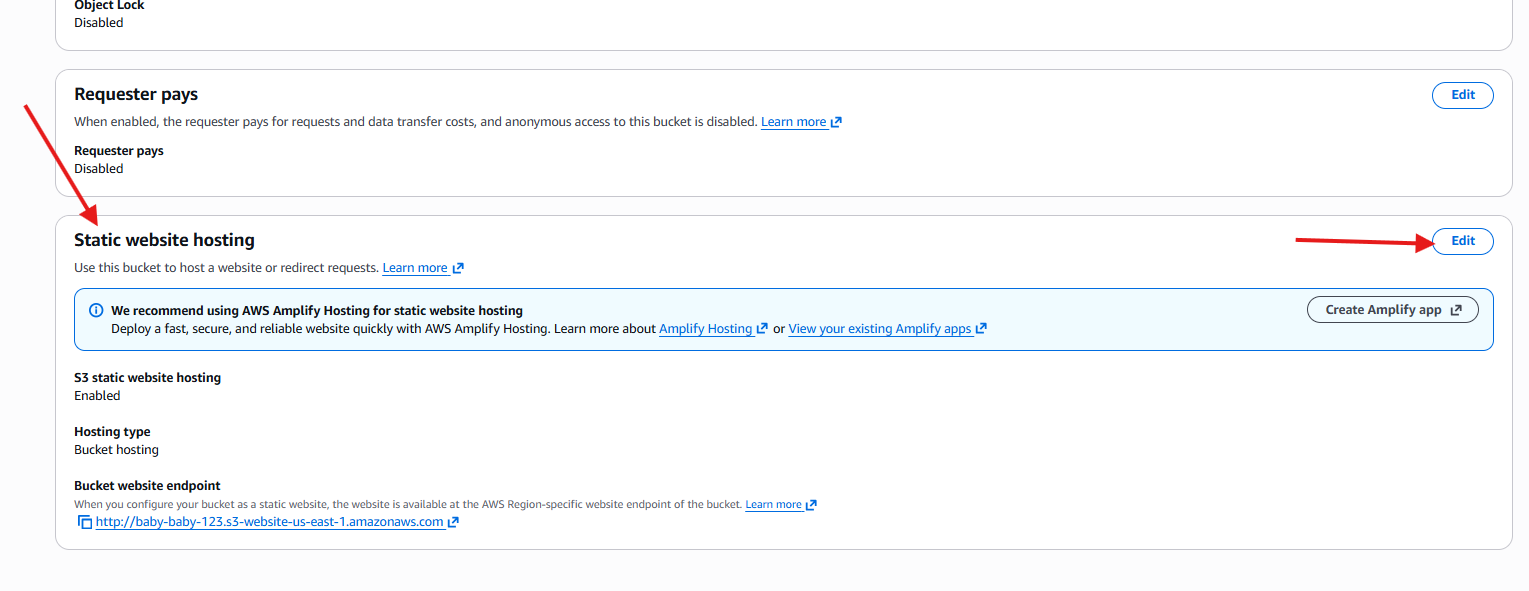
Confirm



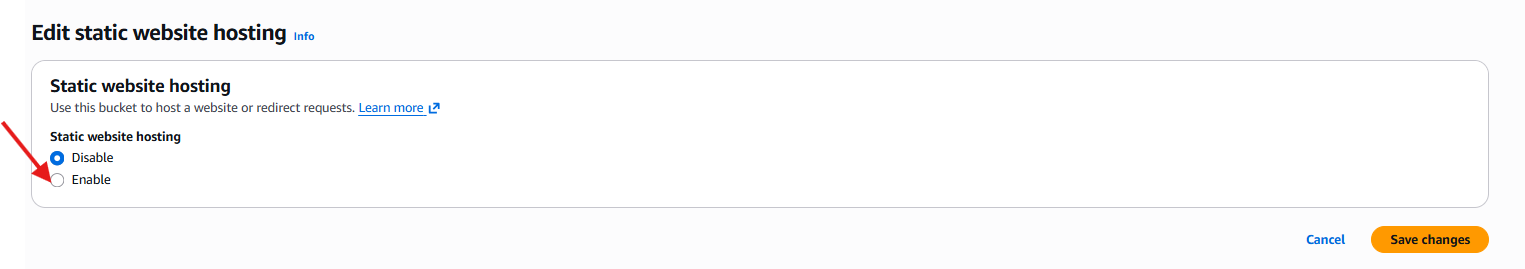
Go to the properties there is a statice website



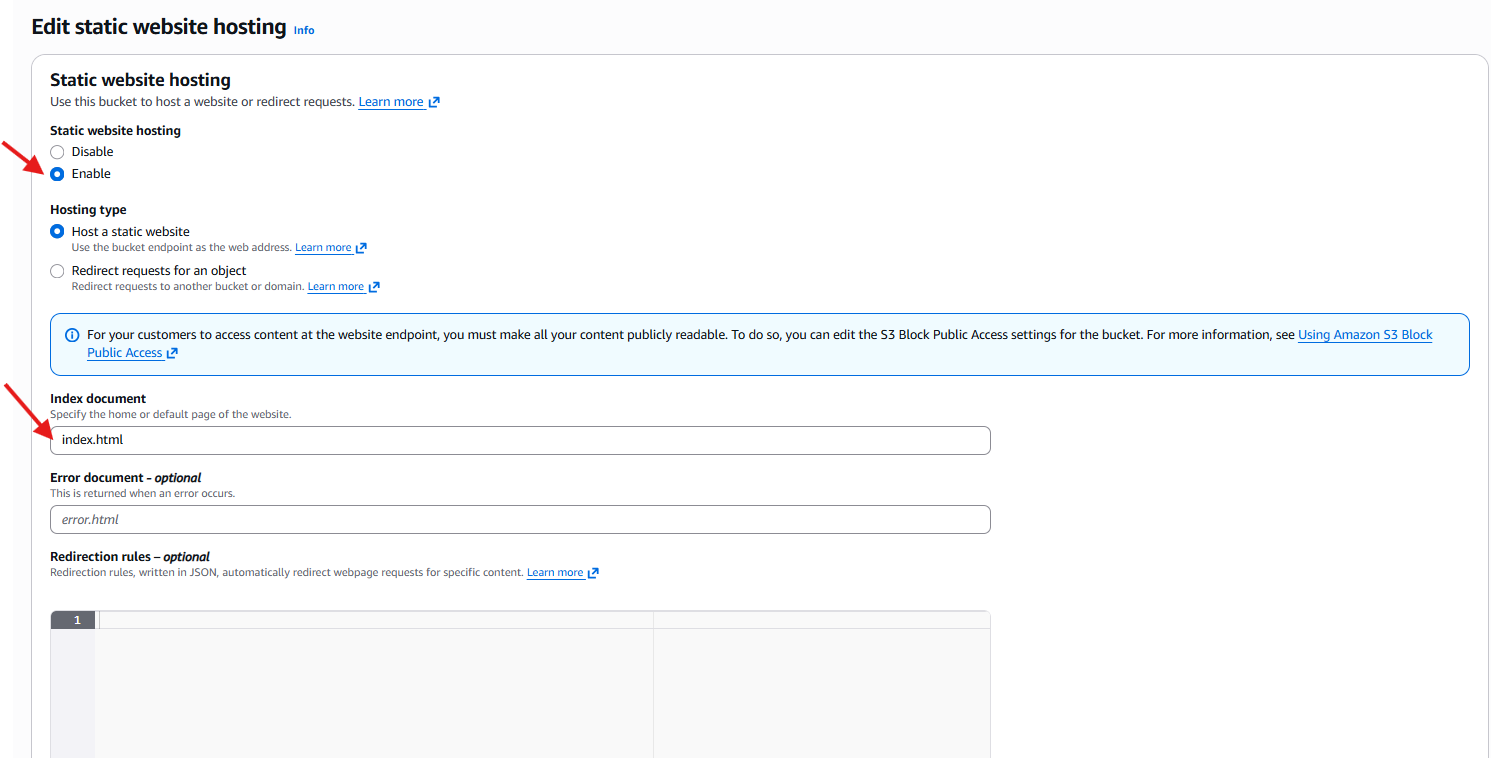
Static website host edit it



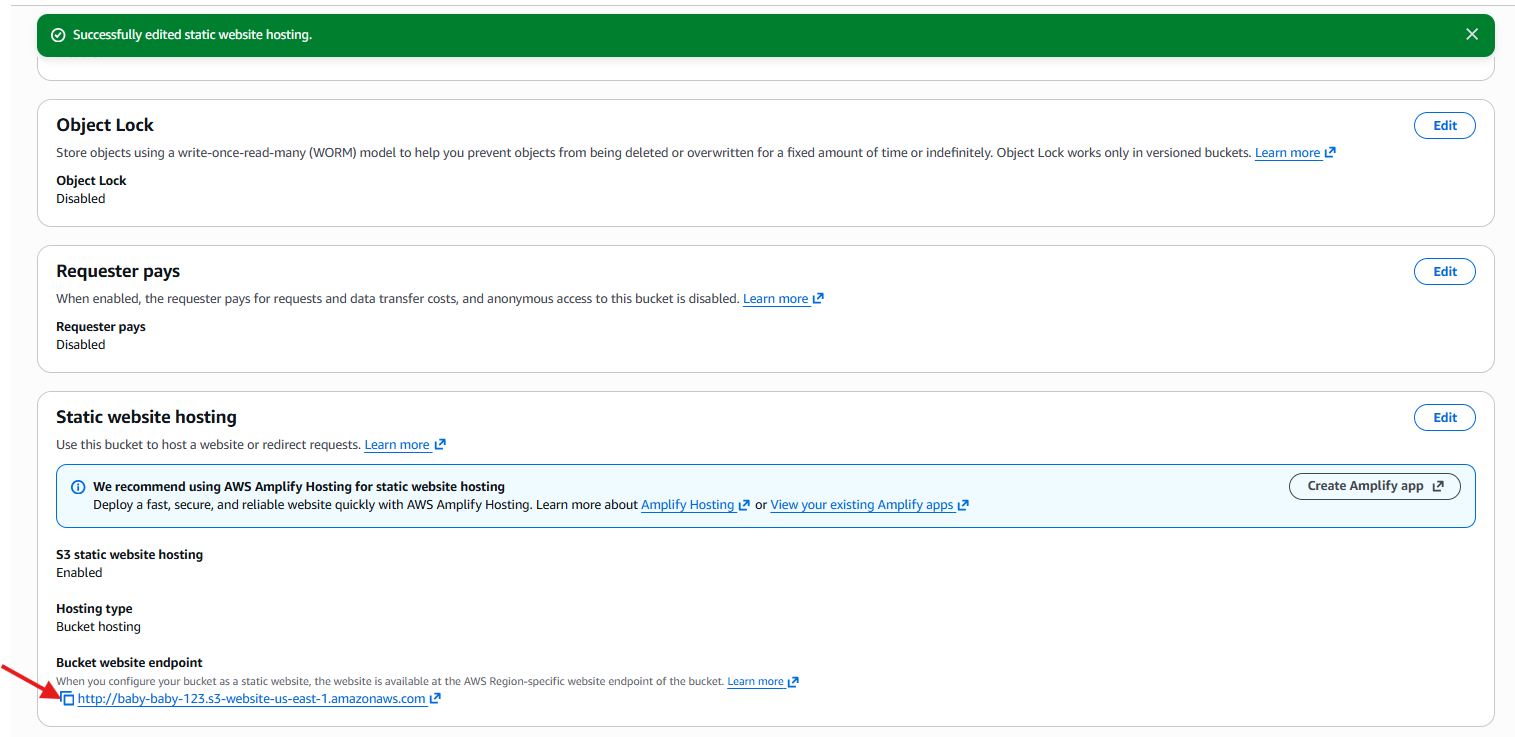
Hear it is showing disable then we can enable it



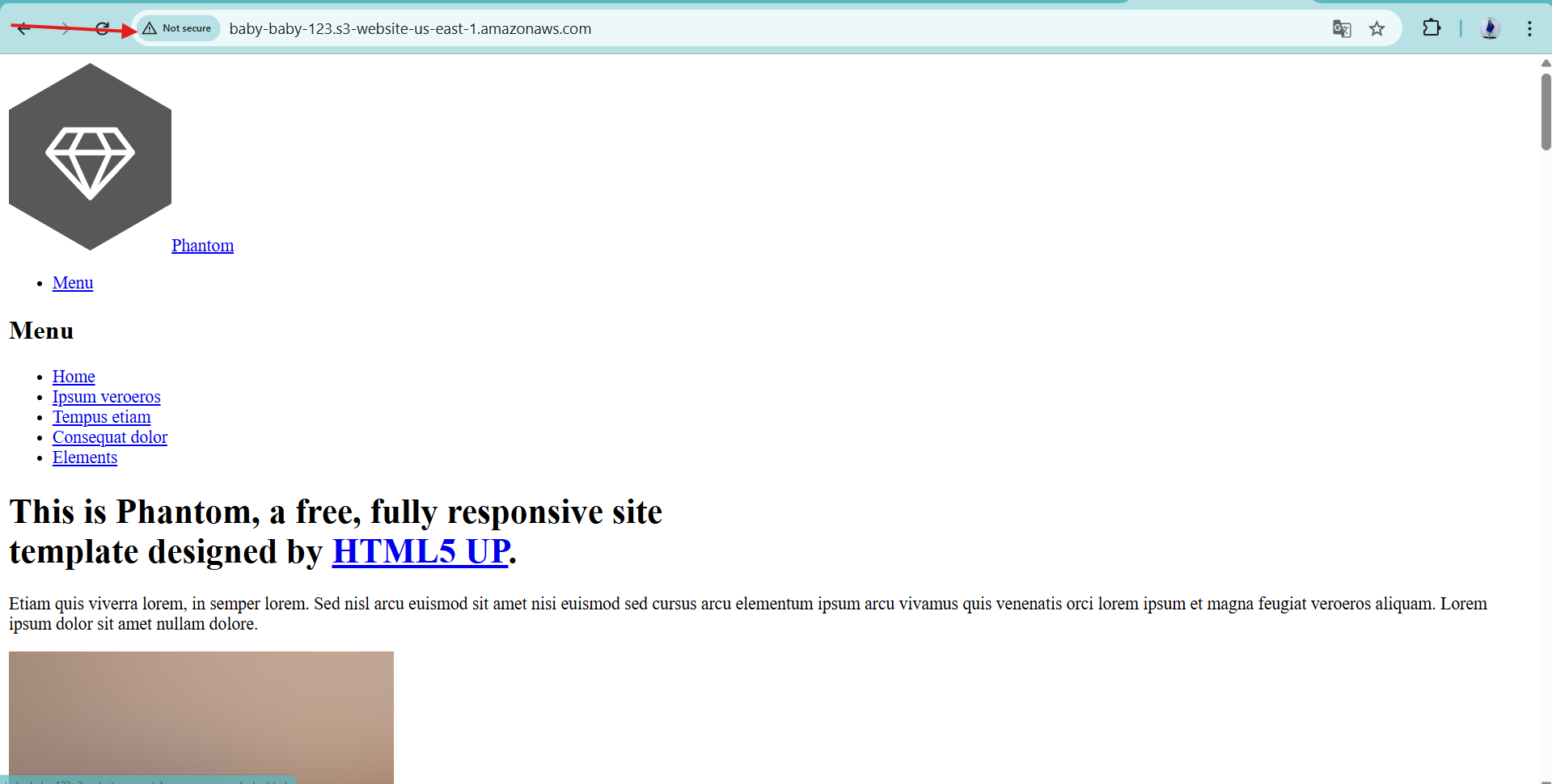
Don’t change enaything but index document should be name as index.html



Then static website will give the bucket static URL

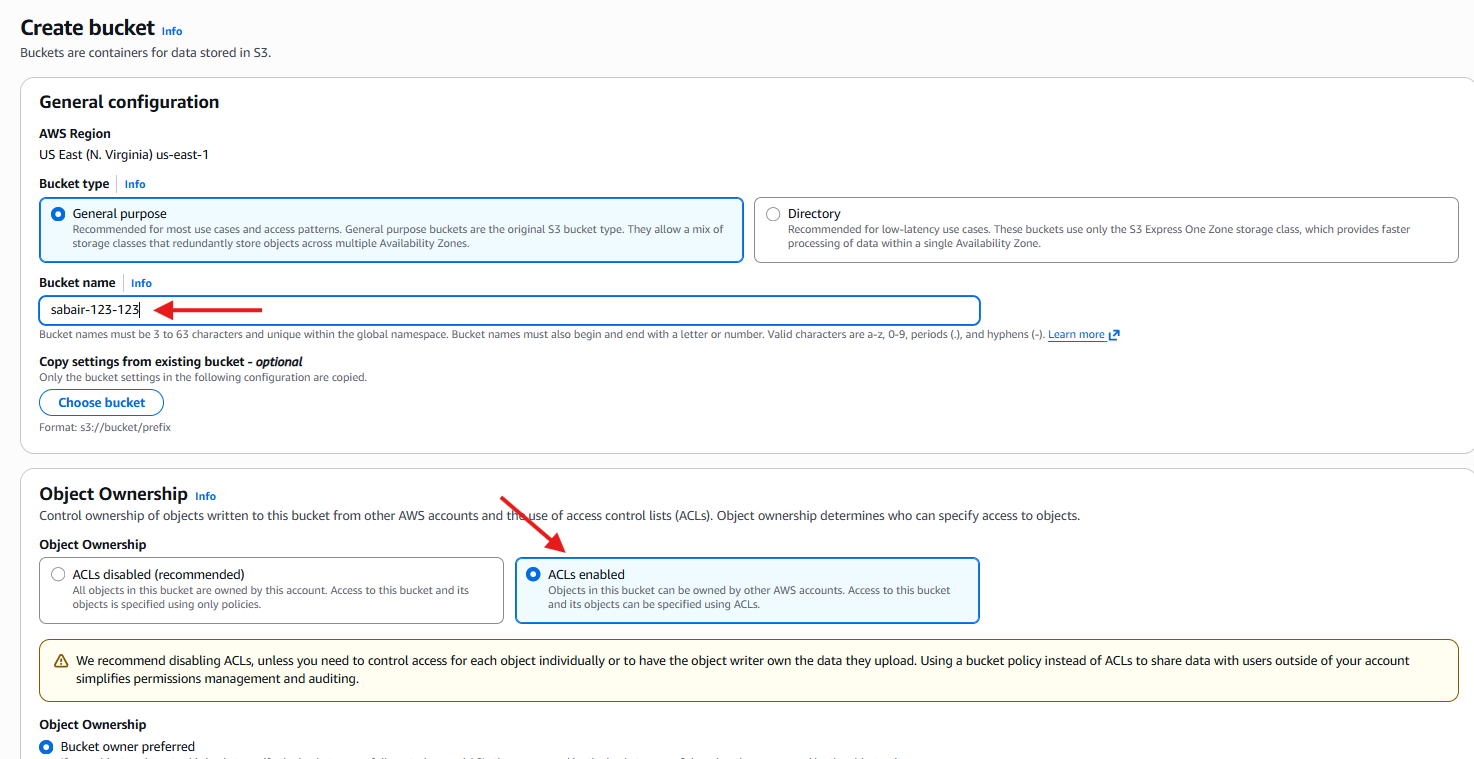


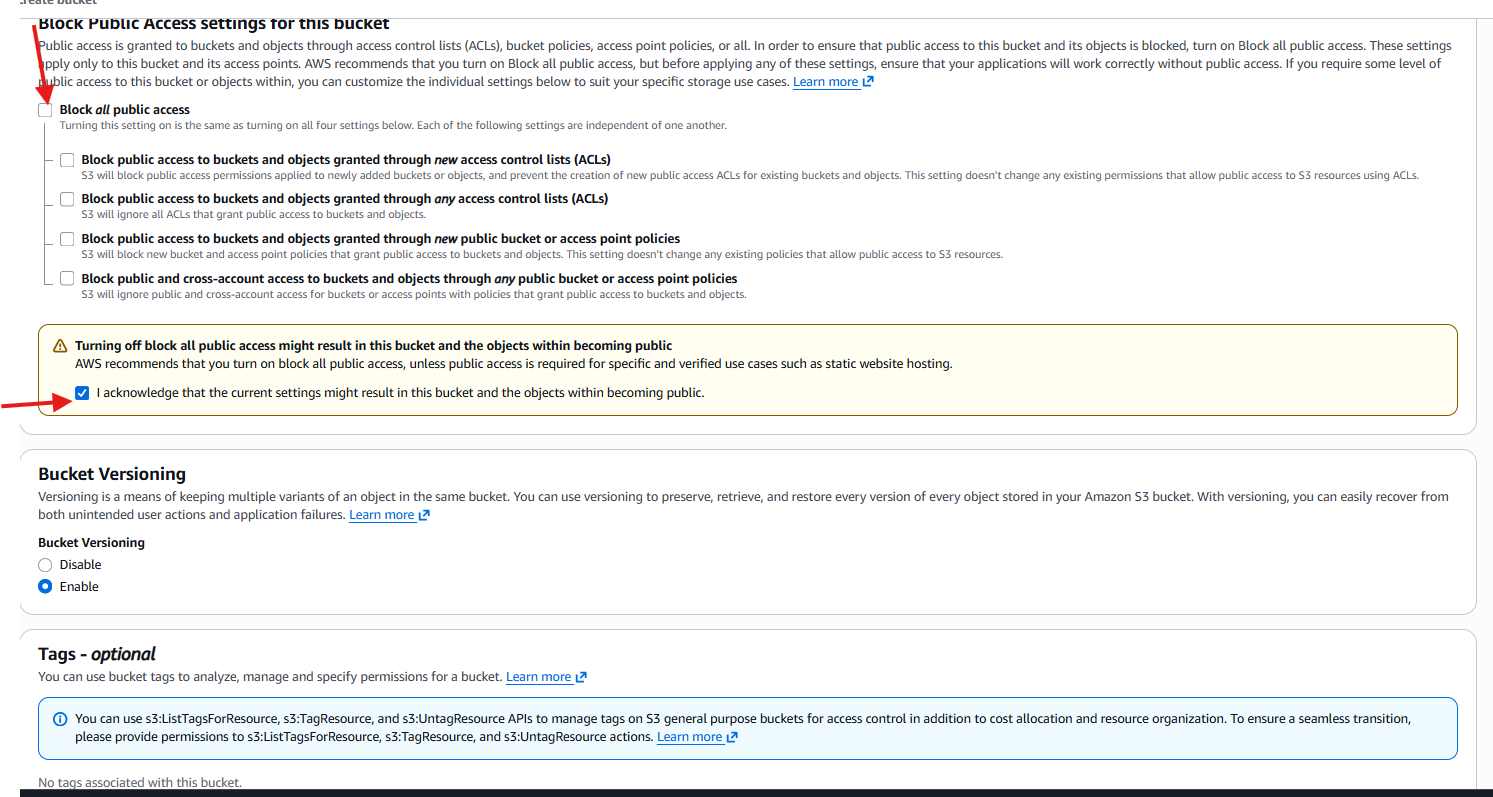
Copy the URL and browse



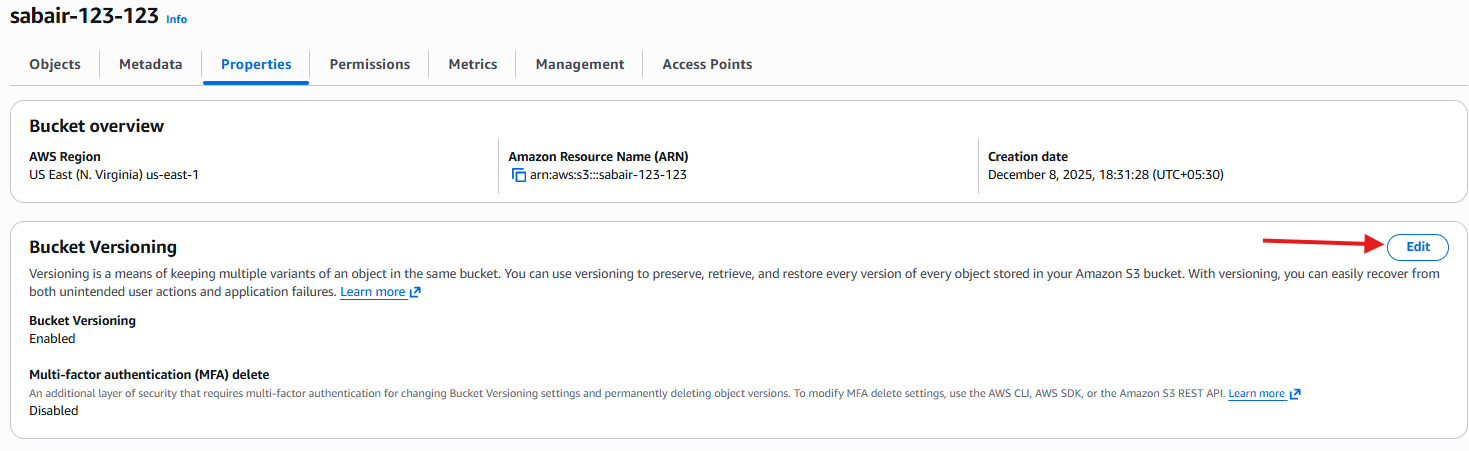
1. Enable cross-region replication on S3 buckets.

Create one buck and enable the ACLs and give the public access

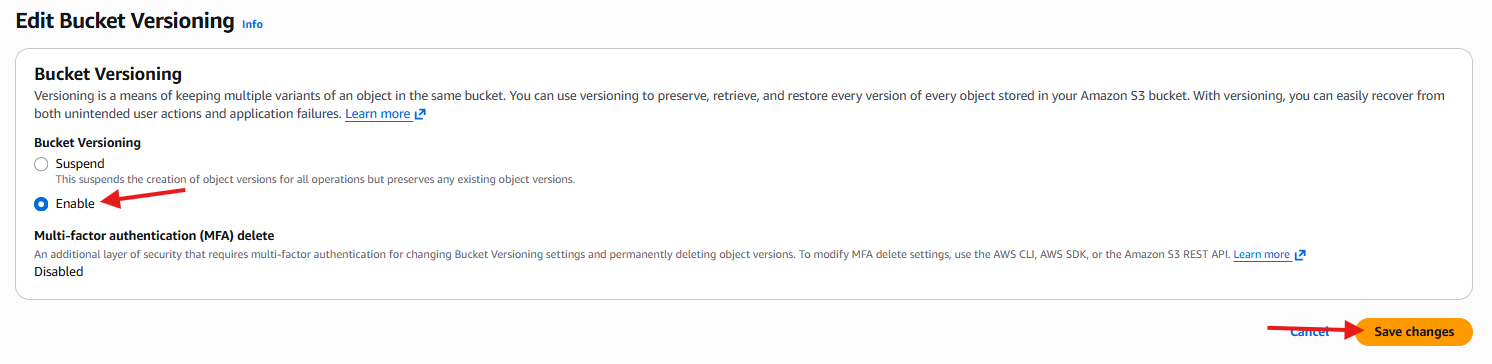




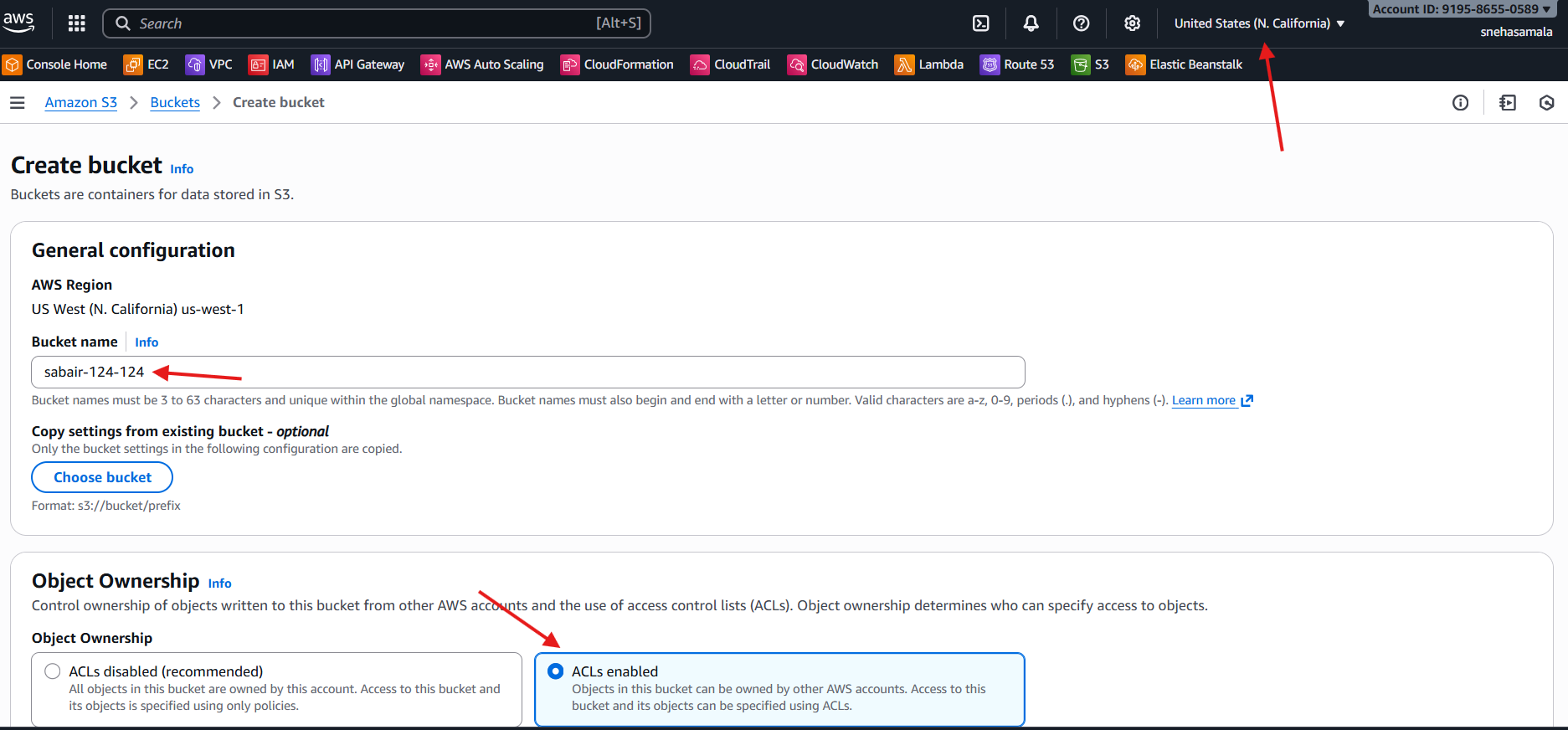
Go to the bucket versioning



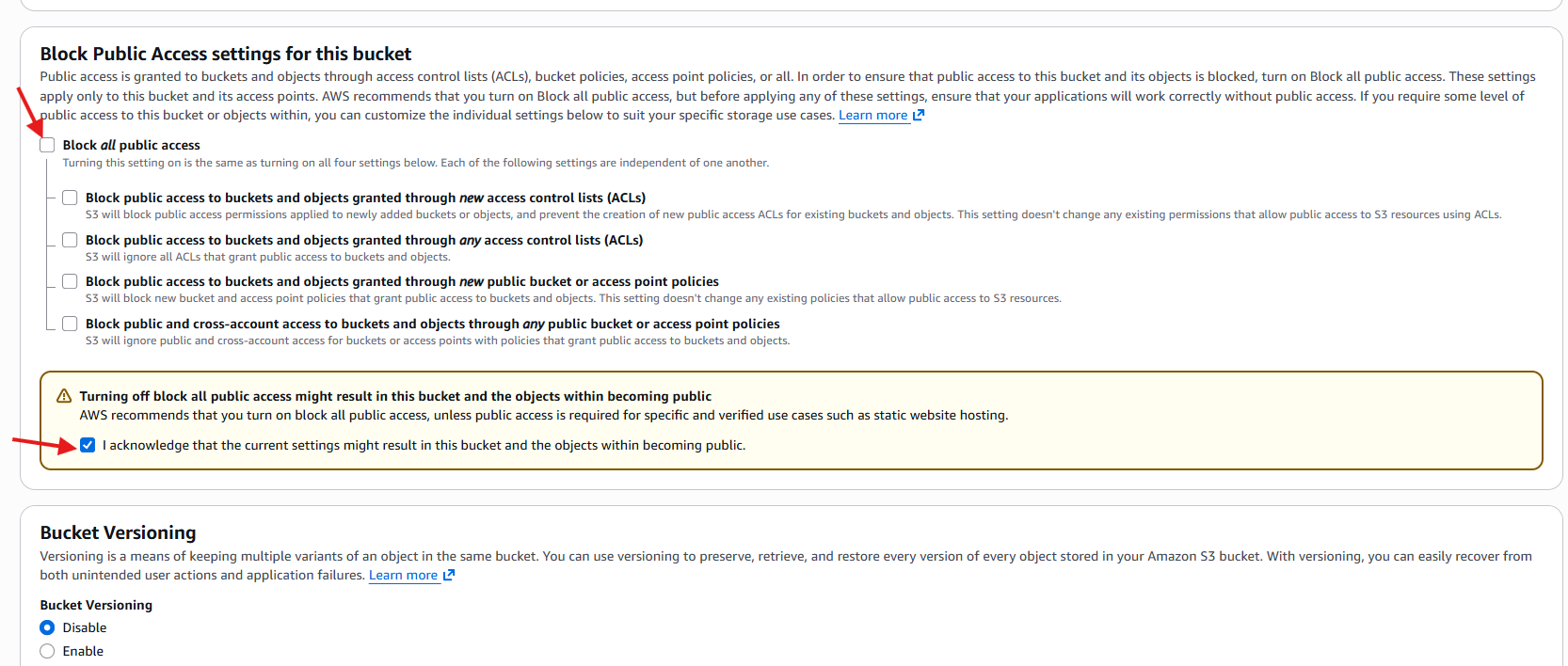
Enable the versioning and save changes



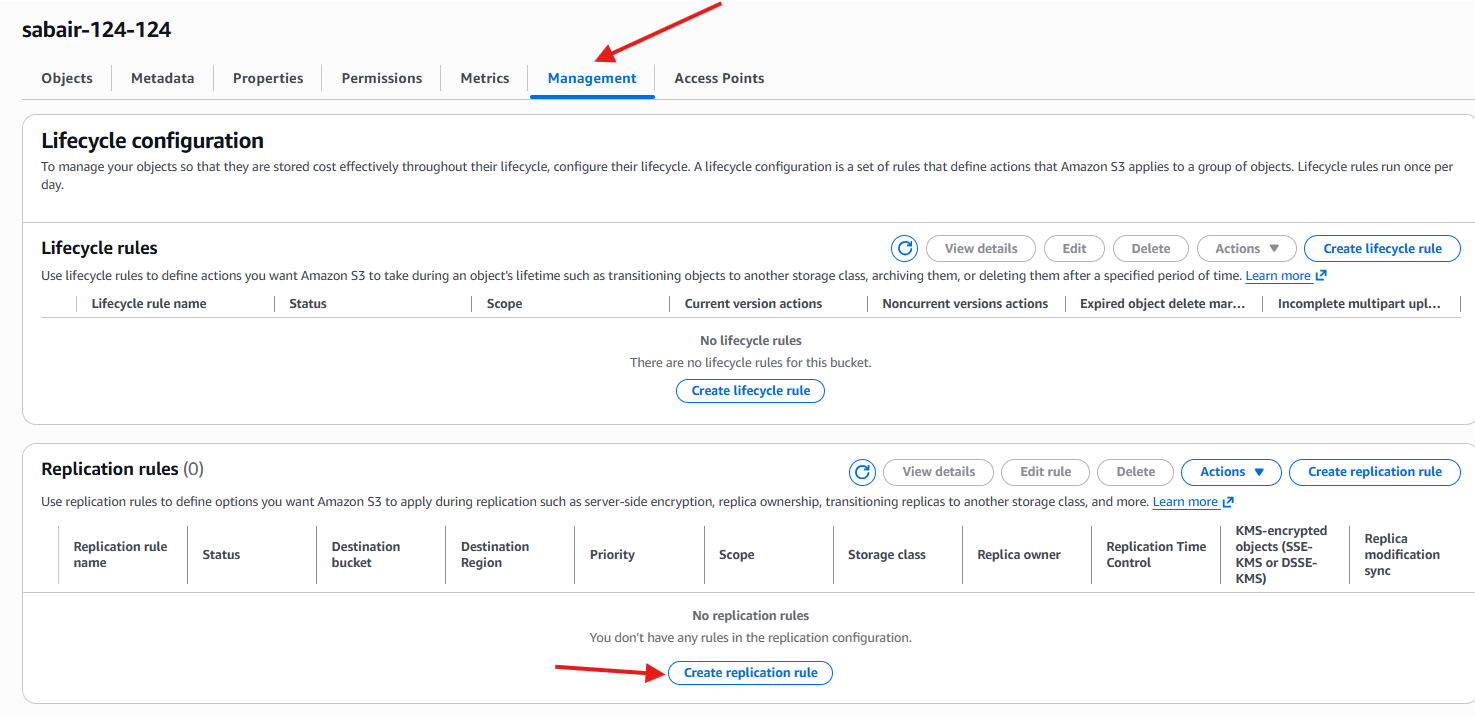
Create another bucket in another region (California)



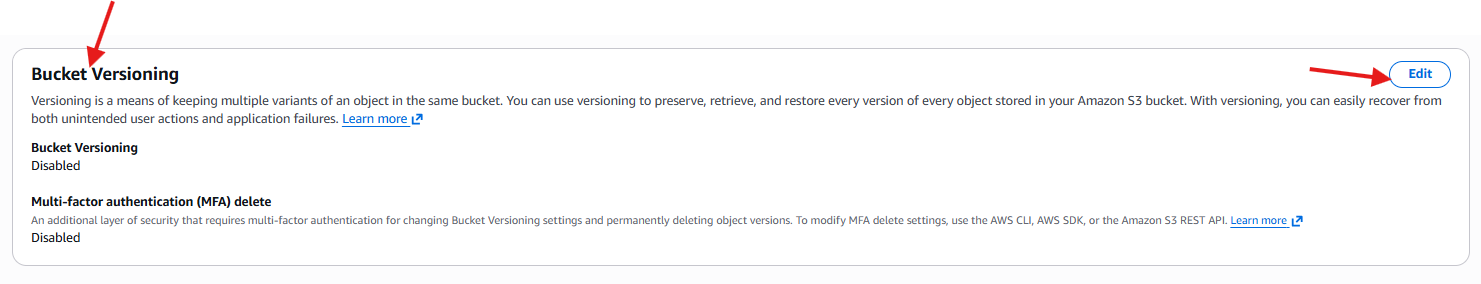
Allow all [public access



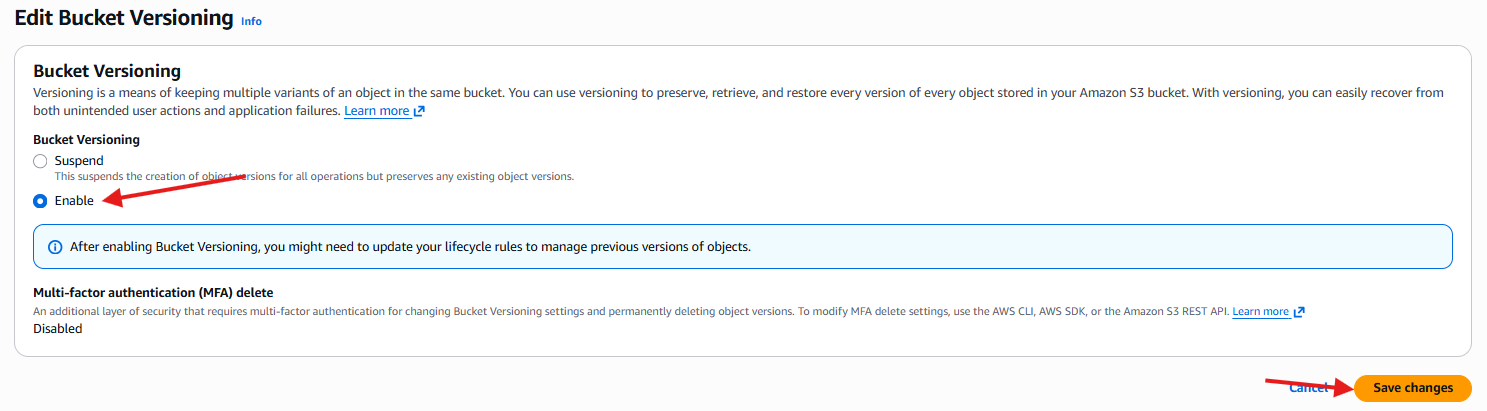
Go to the management and create the replication



Go to the bucket versioning and edit

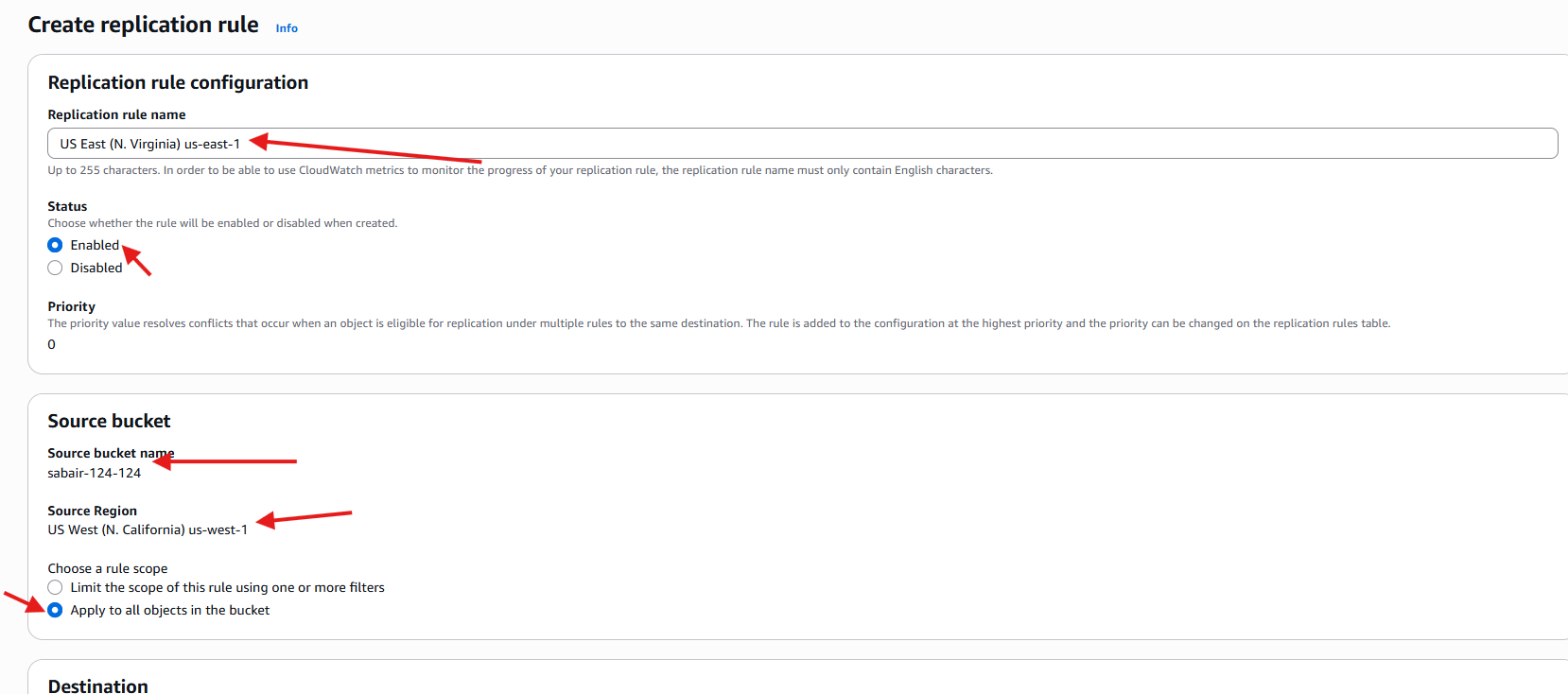


Enable the bucket



Replace the configuration

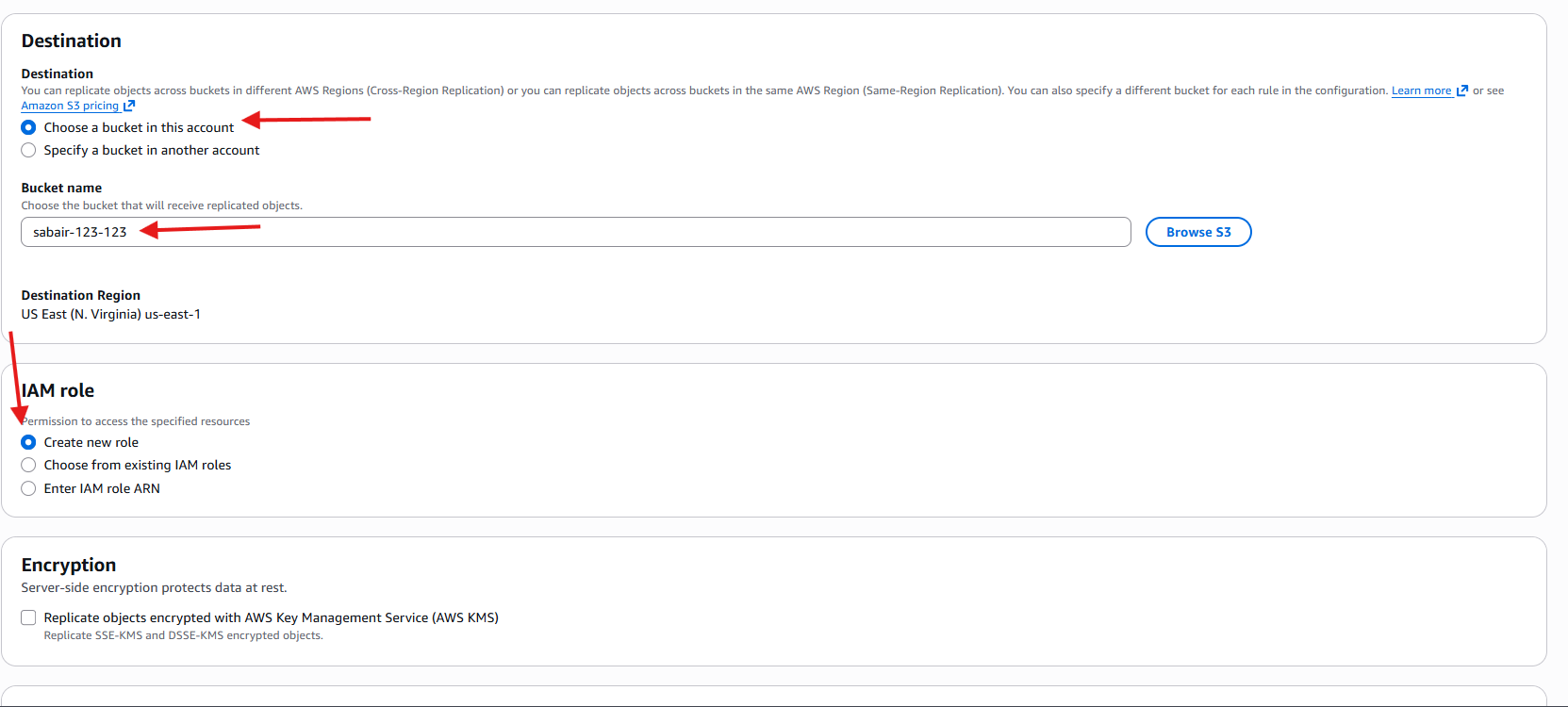
Enable 🡪 status 🡪 source🡪sabair-124-124🡪apply all the objects in the bucket

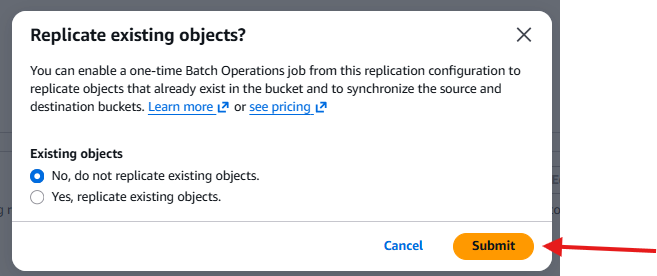


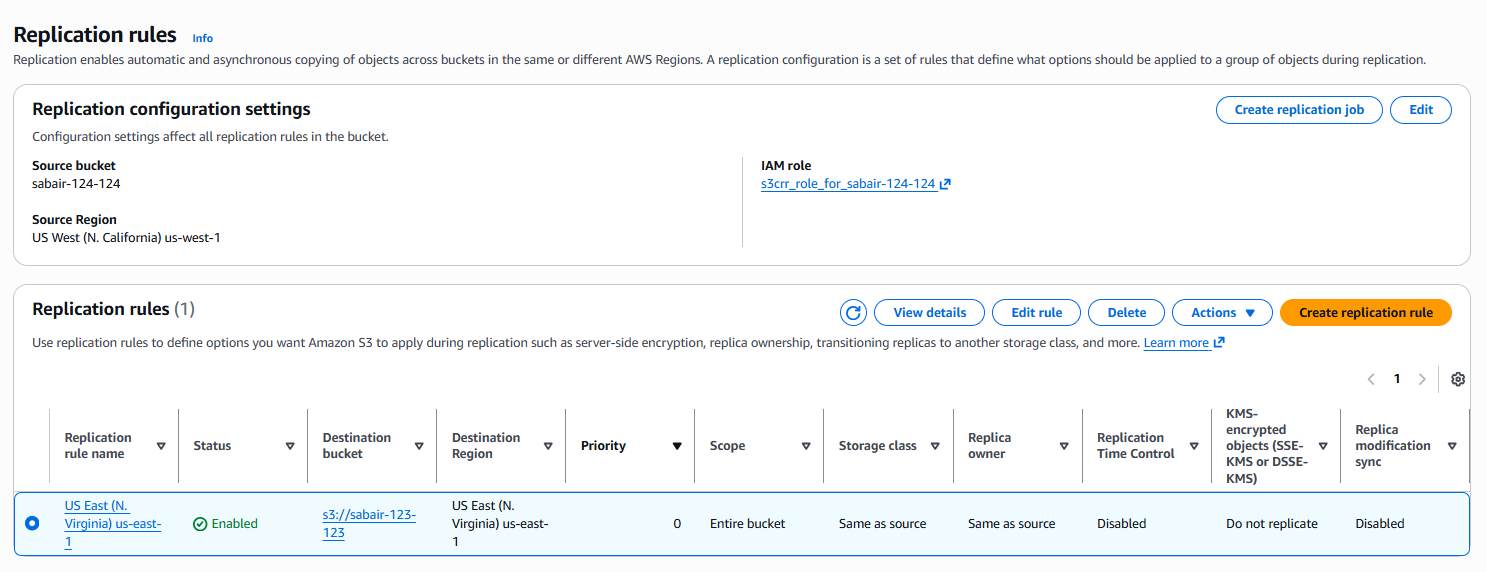
Destination🡪choose a bucket in this account

Bucket name 🡪sabair-123-123

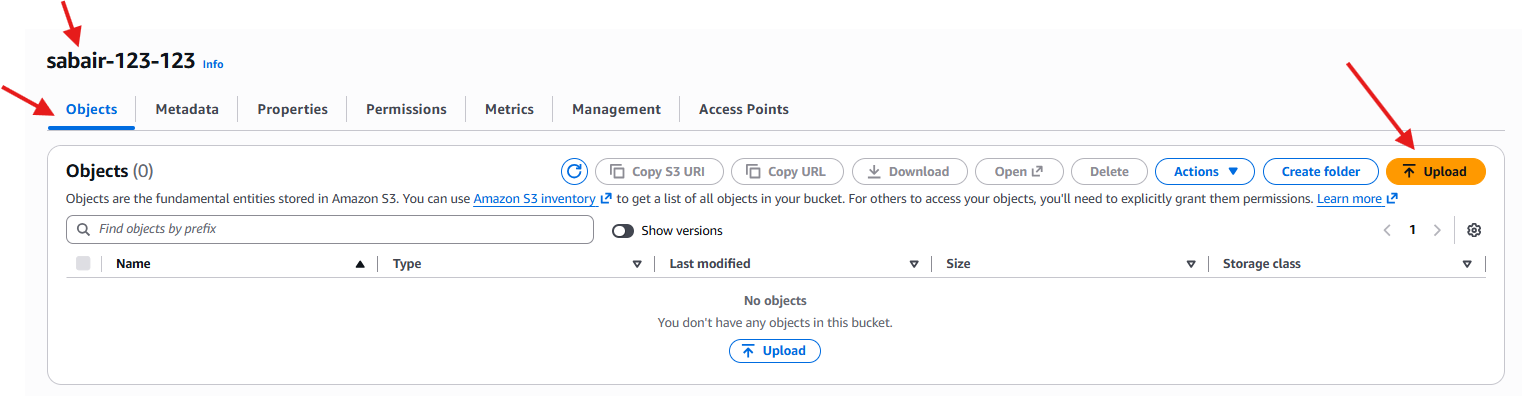
IAM role 🡪 create new role



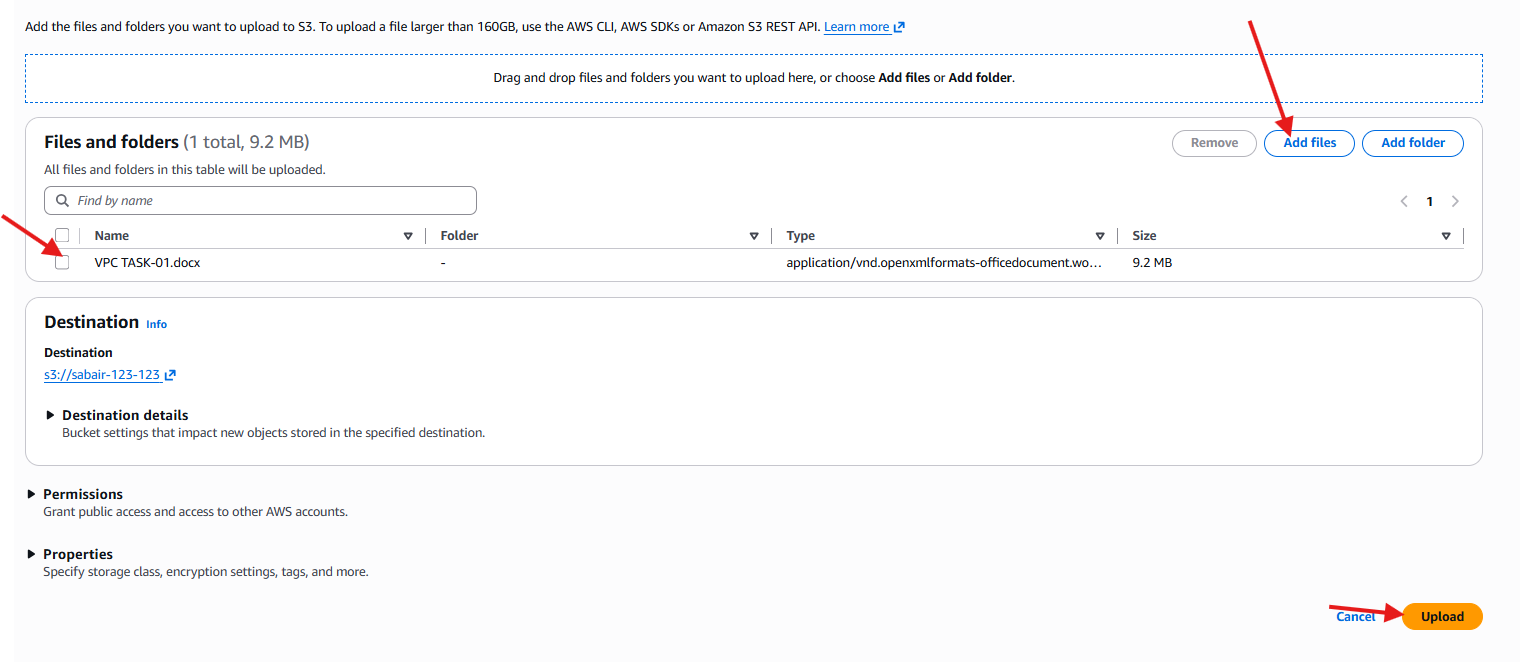




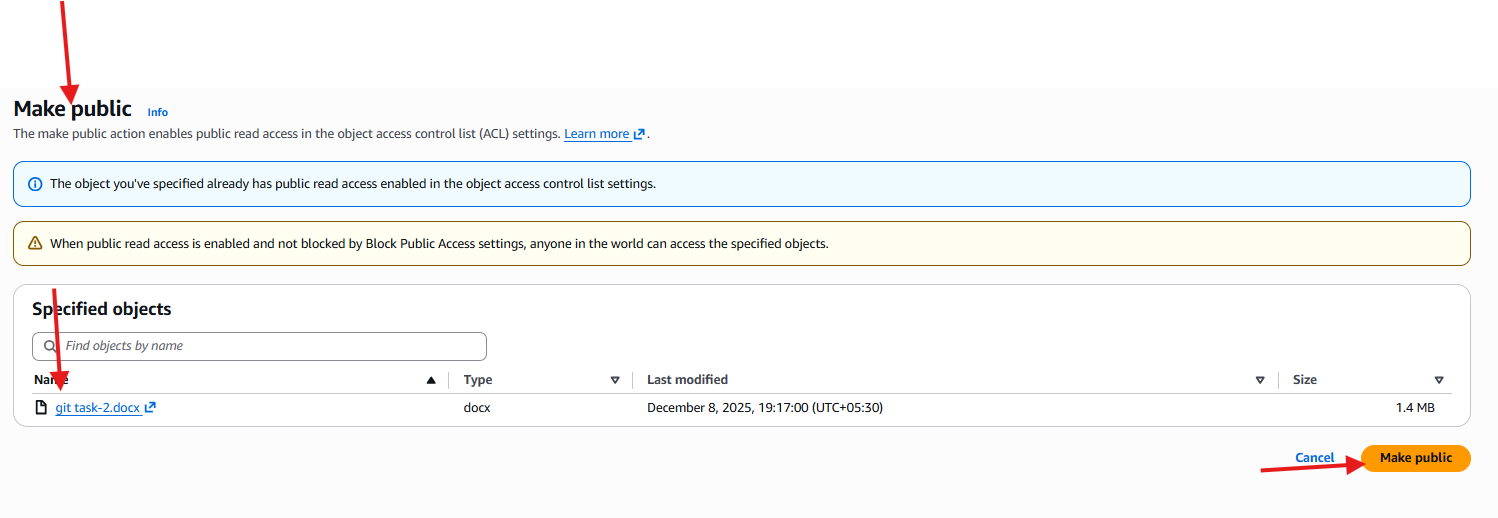
Go to the another region and select the bucket click the objects



Upload the file

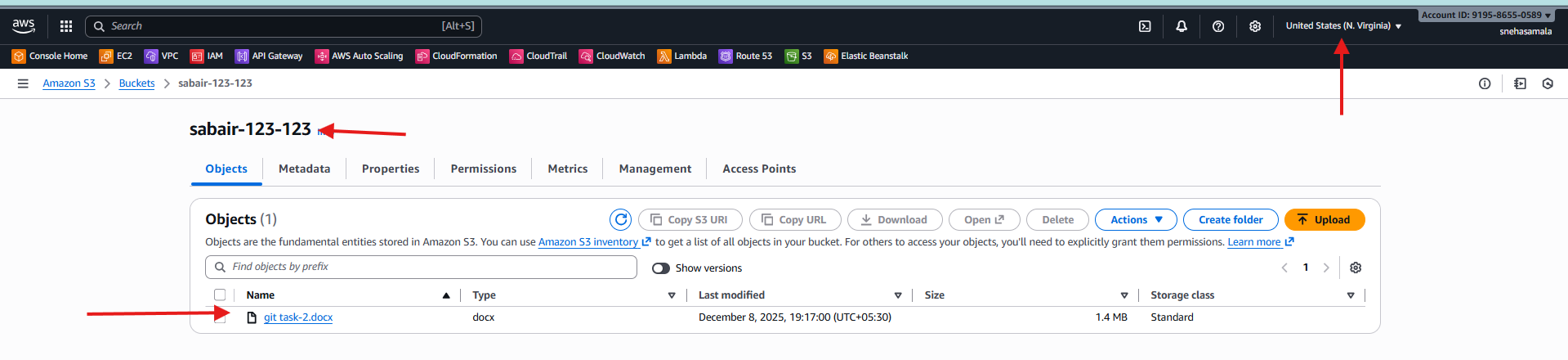


Make it public



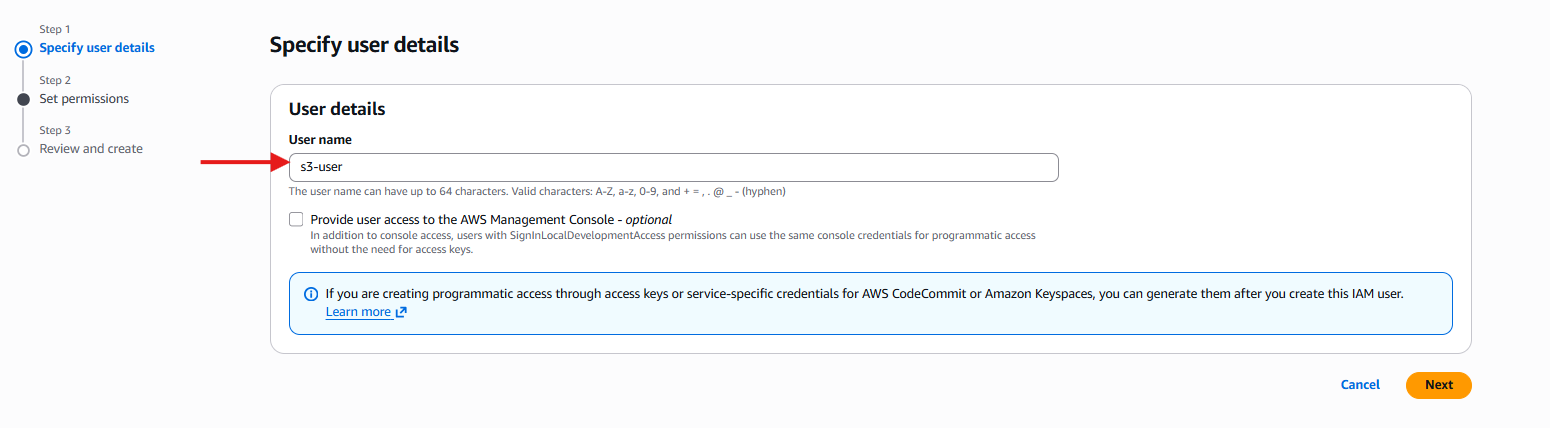


Change the region and go to the bucket and check in the object

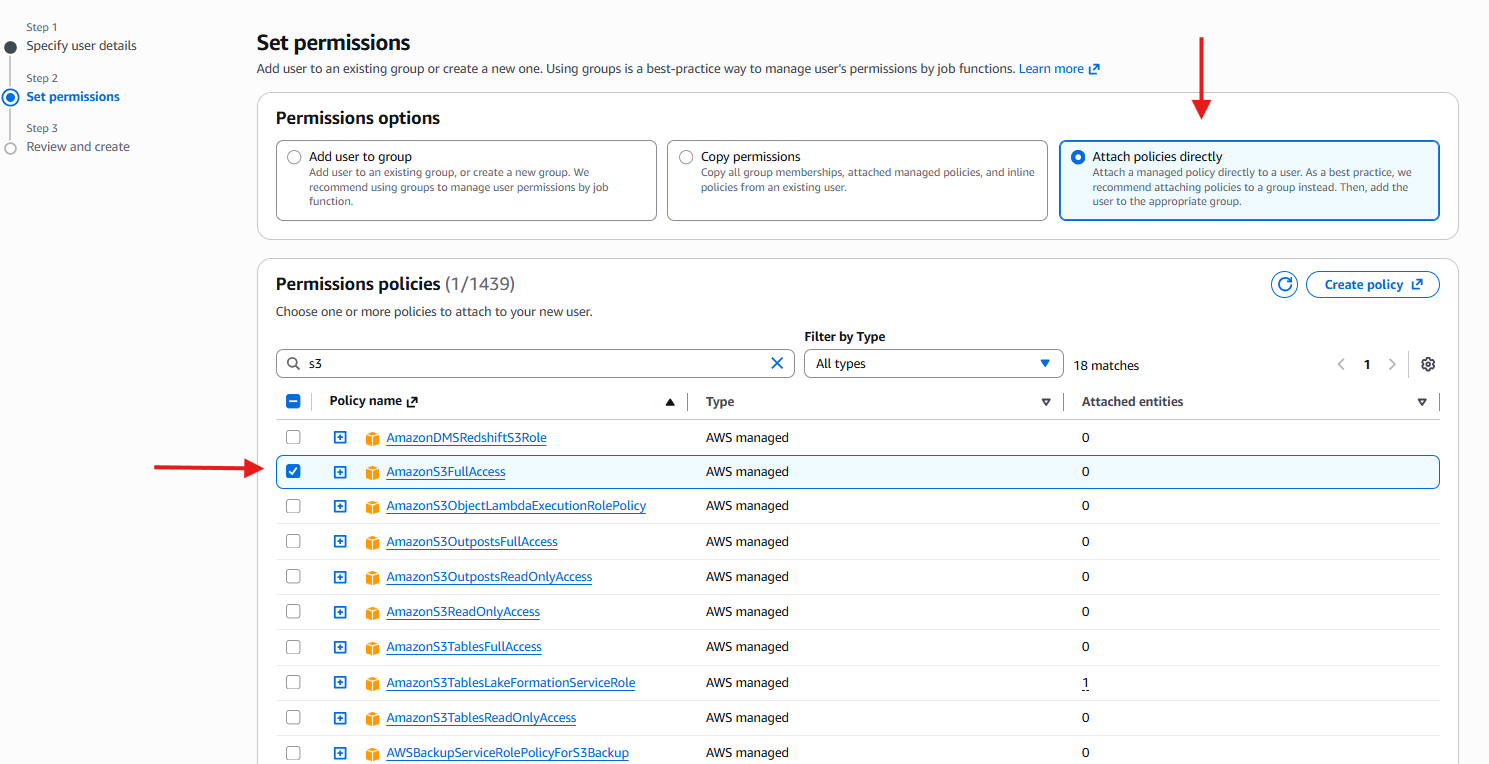


1. Configure a bucket policy so only the Admin user can see the objects of the S3 bucket.

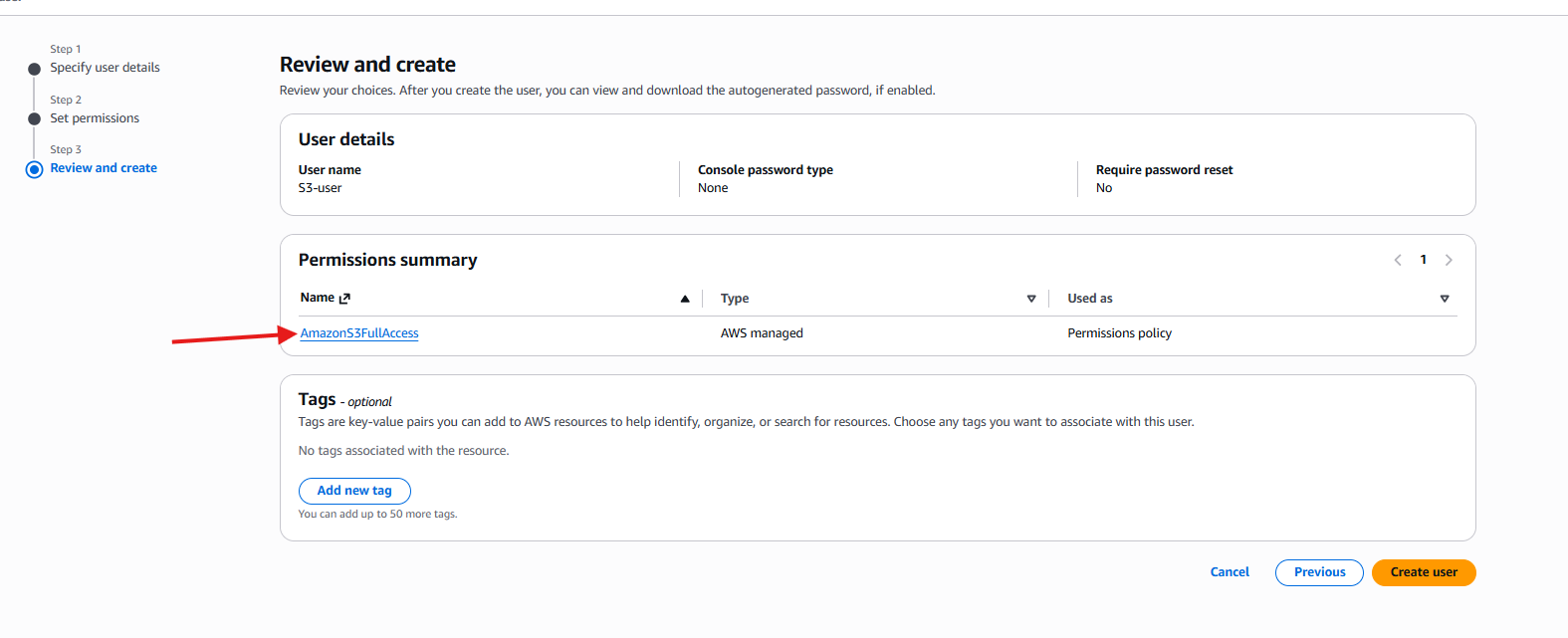
Go to IAM and create the user and give the full access to the s3 bucket

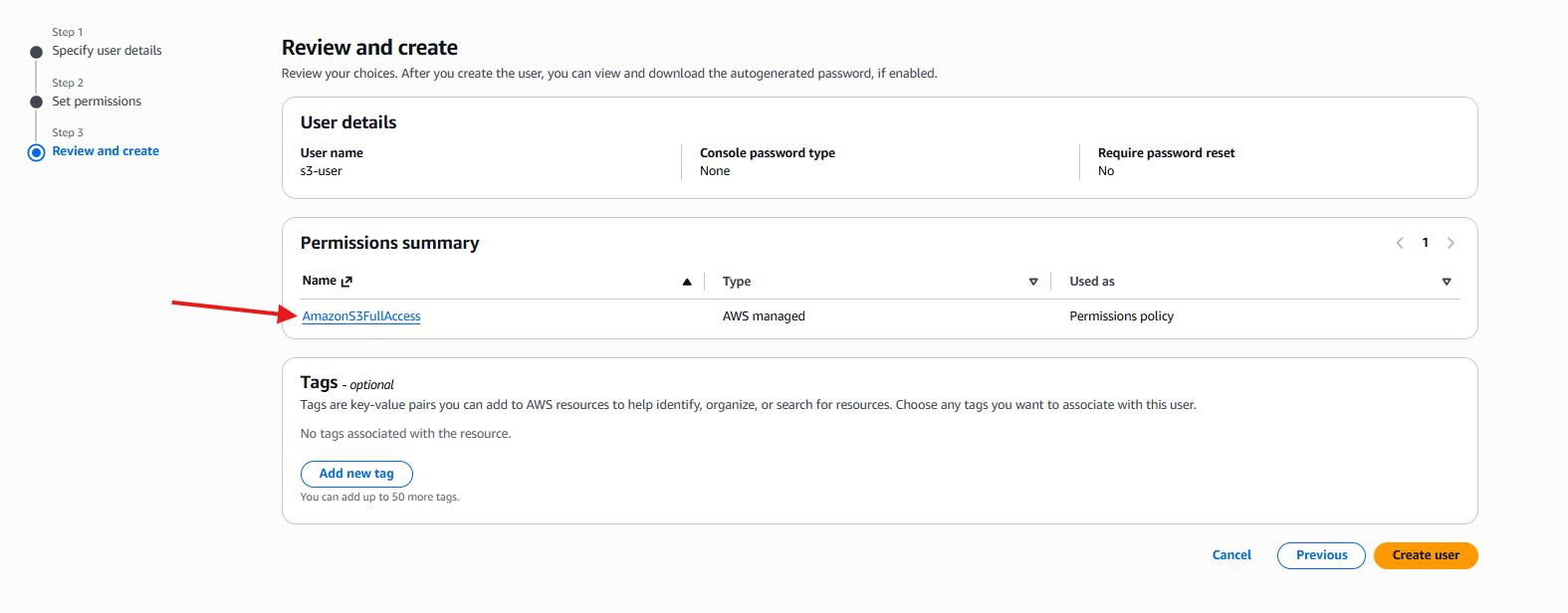


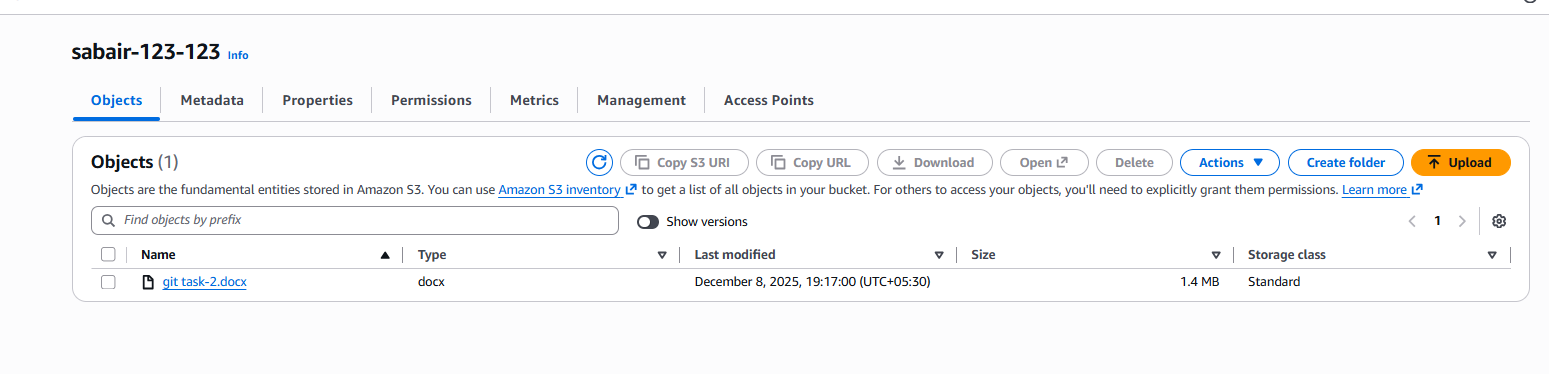
Change the policiey

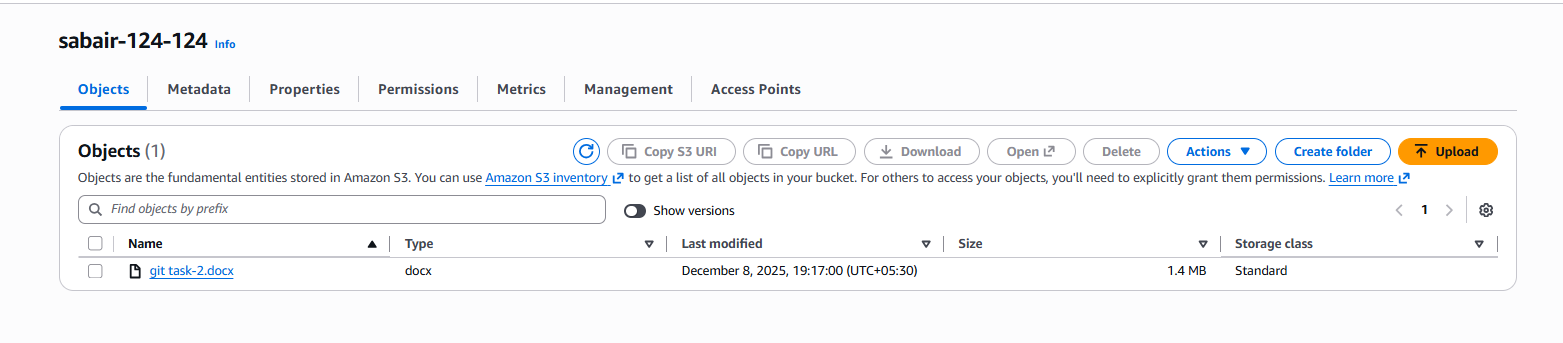


Successfully access is got



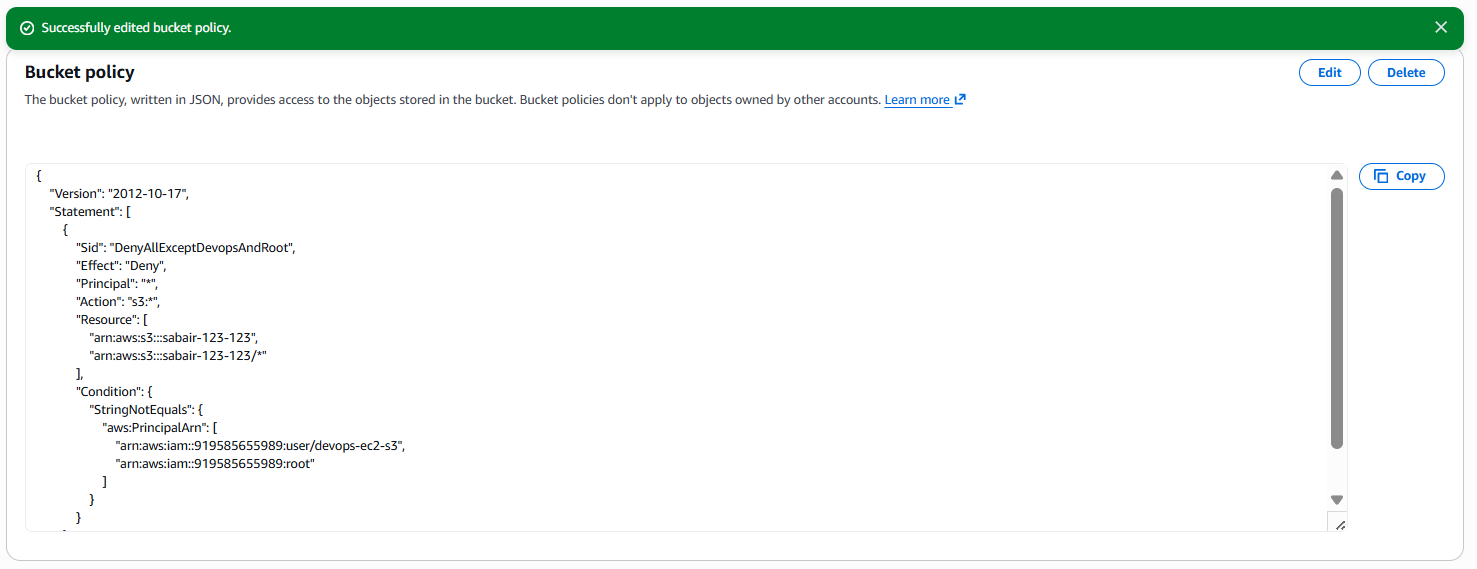






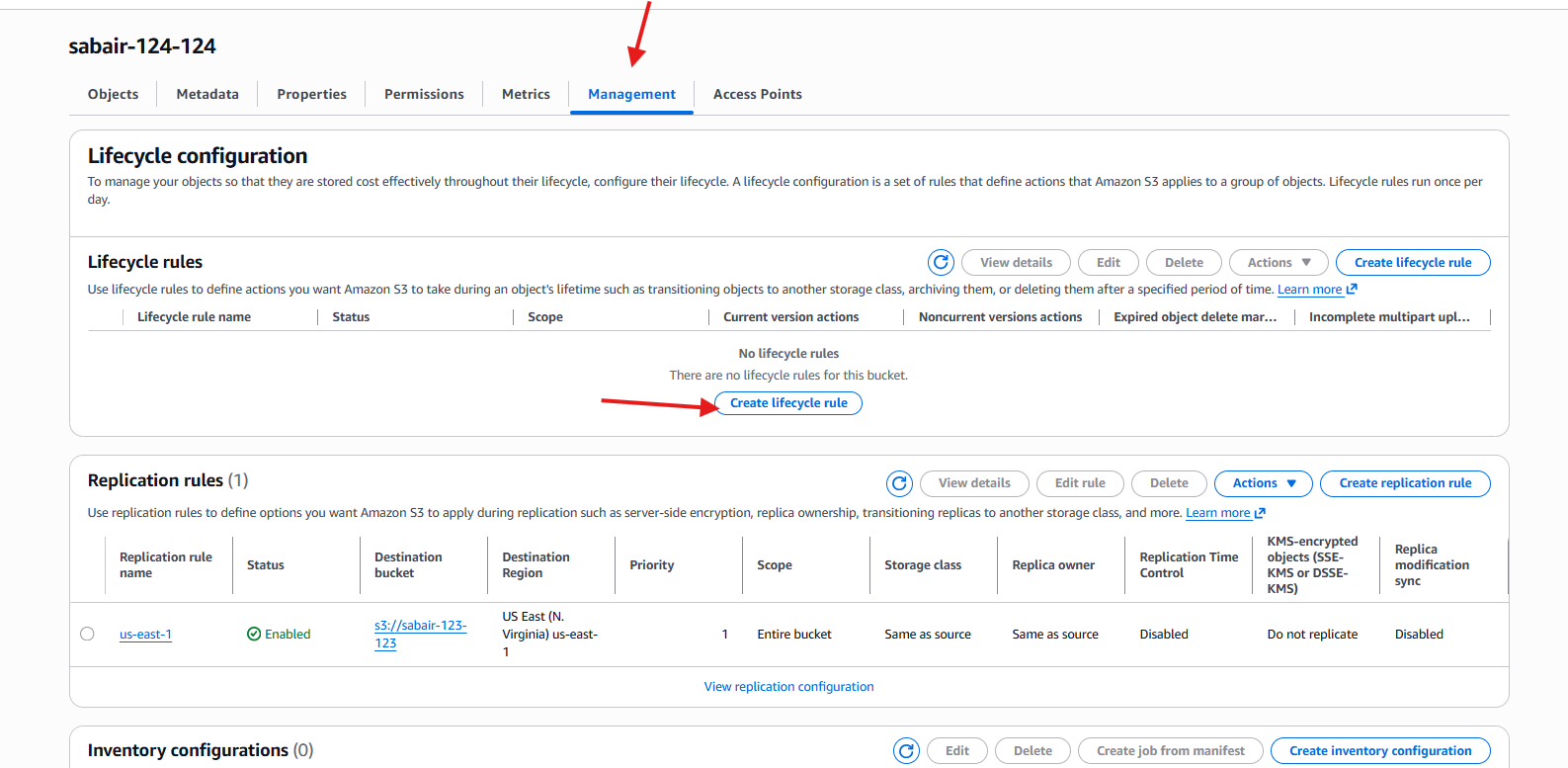
Go to the permissions and bucket policy



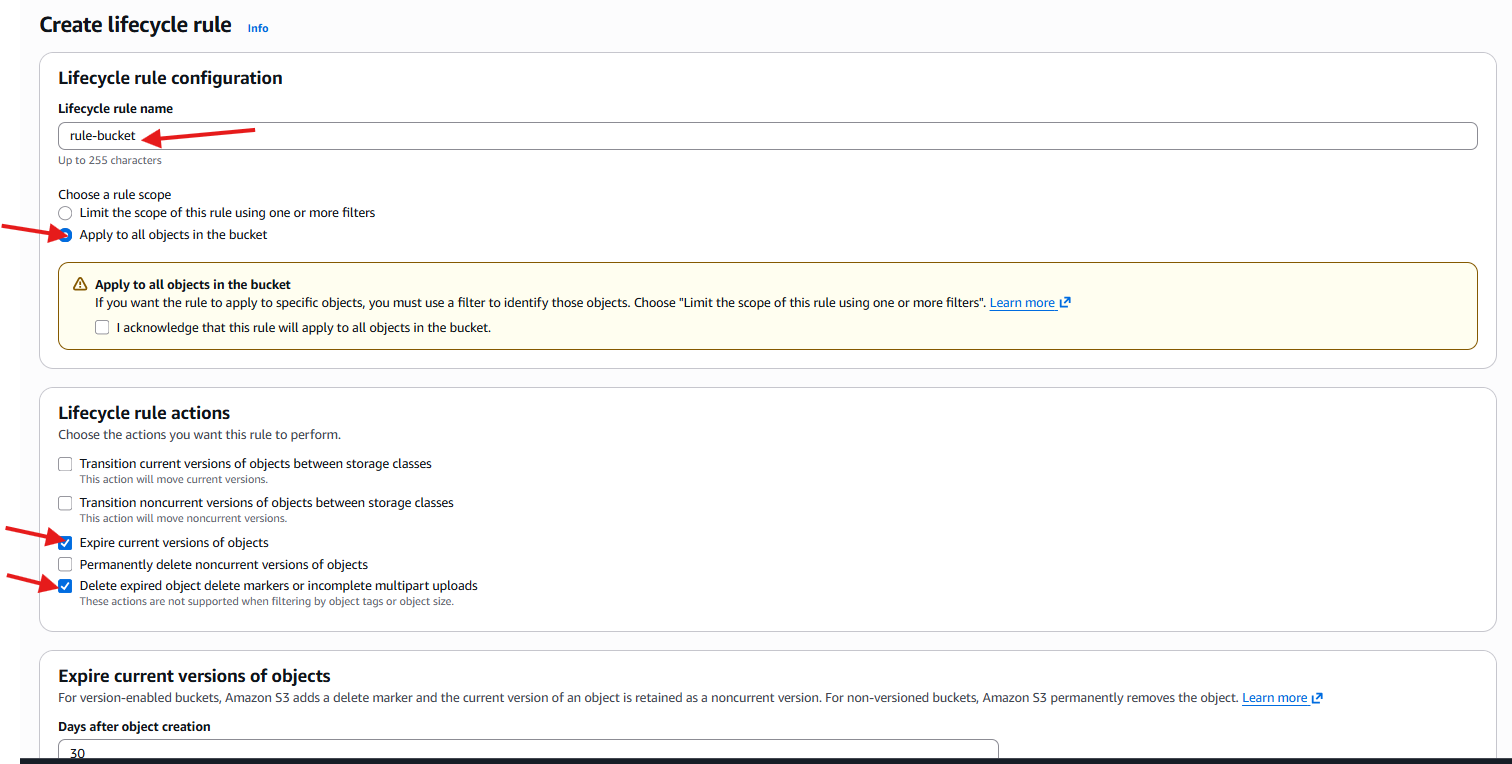


1. Set up lifecycle policies to automatically transition or delete objects based on specific criteria.

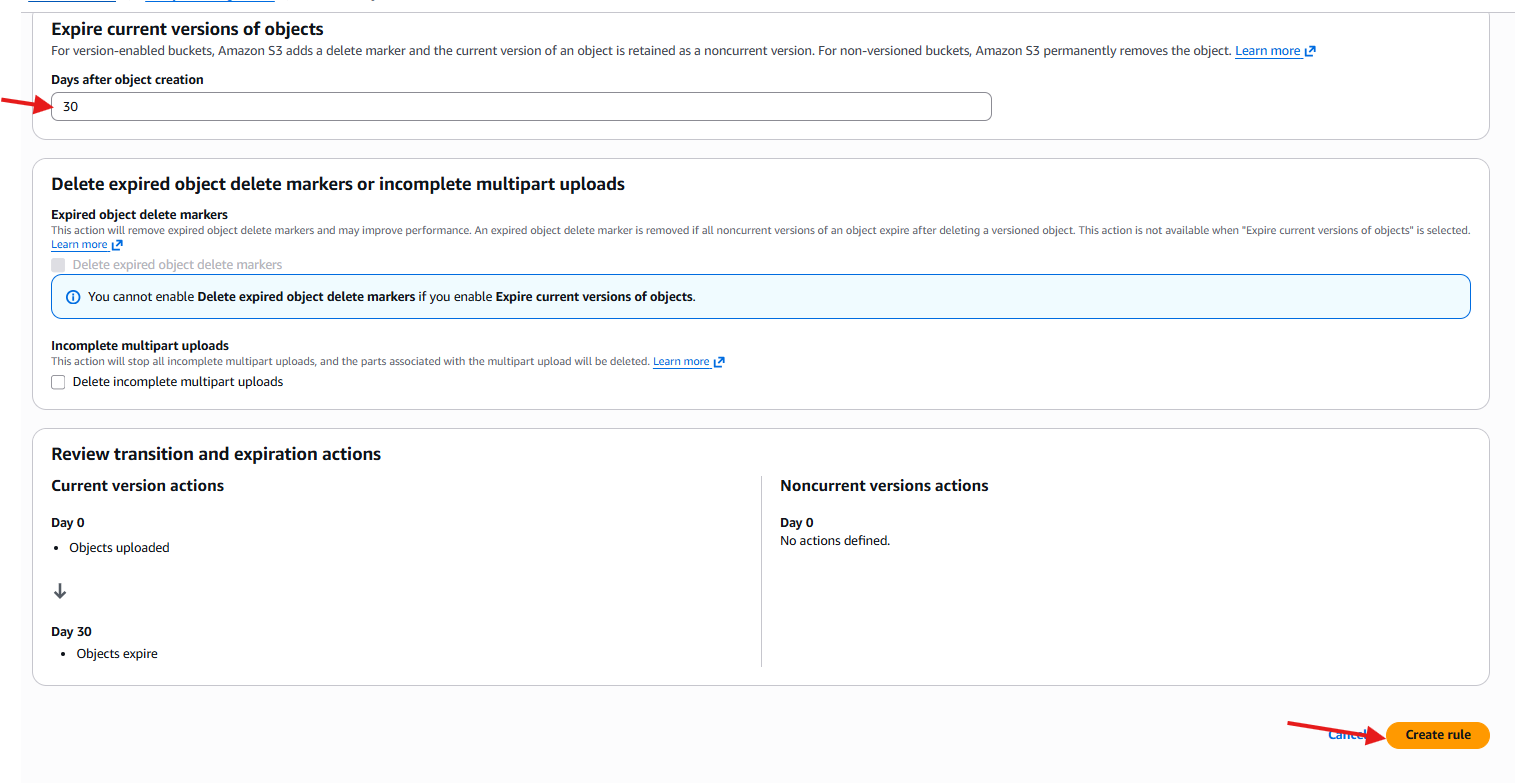
Go to the bucket and management 🡪create life cycle



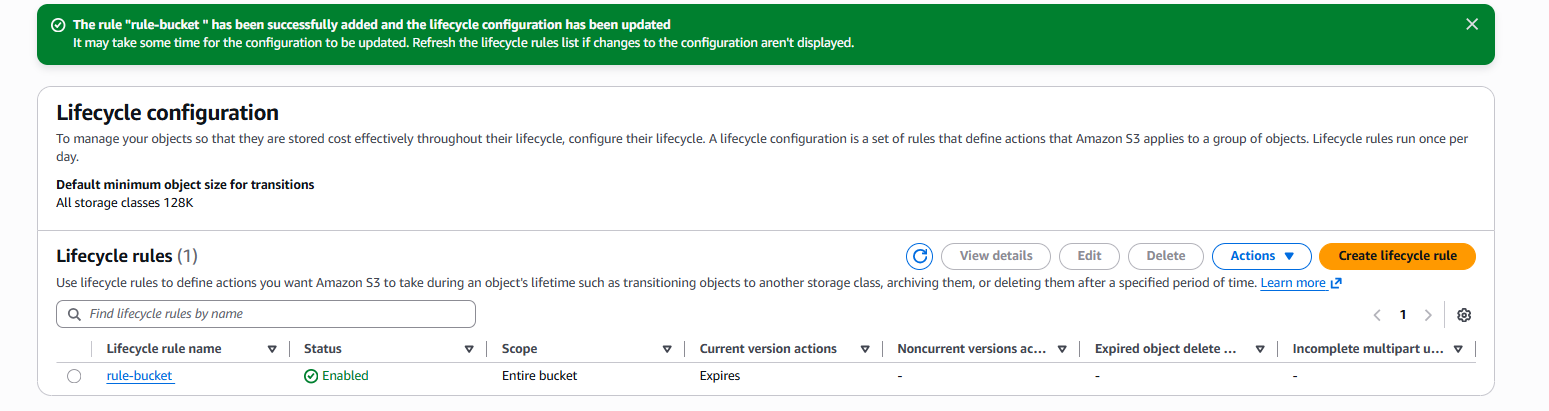
LIFEcycele🡪apply to all objects🡪enable and delete🡪



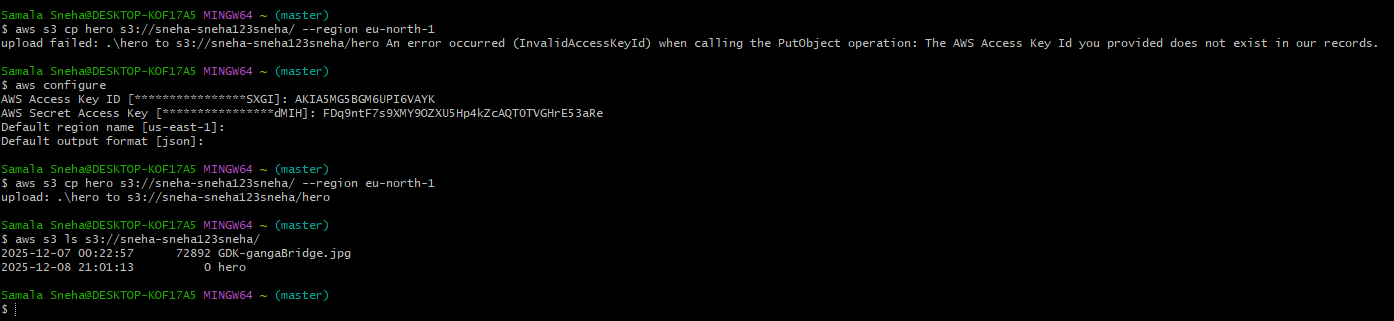
Expires in 30 days



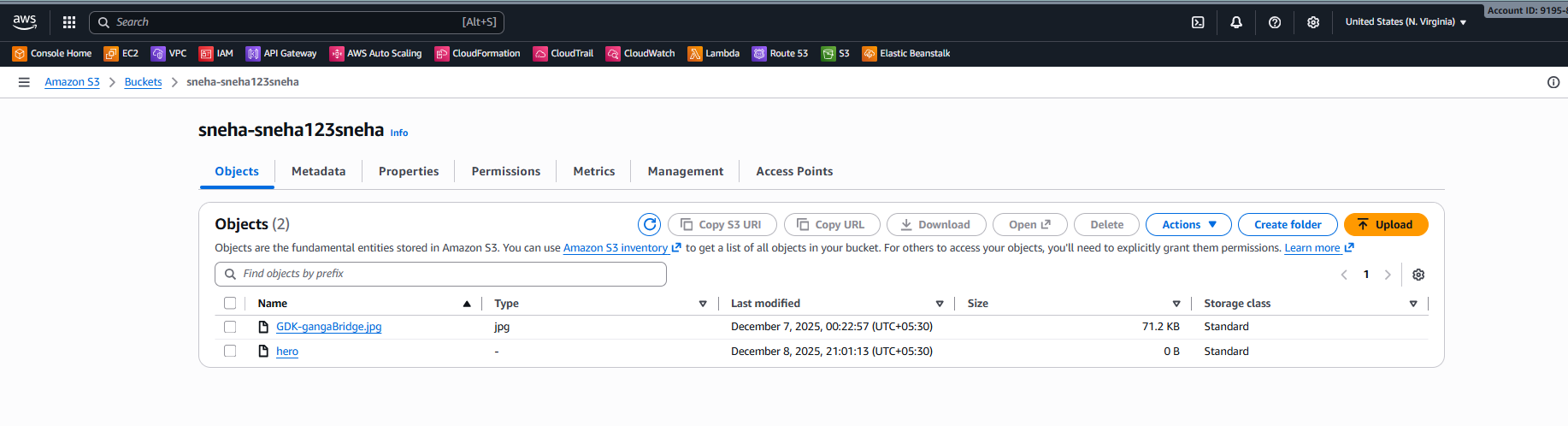
Successfully life cycle configuration is created



1. Push some objects to S3 using the AWS CLI.



I have pushed one object to s3

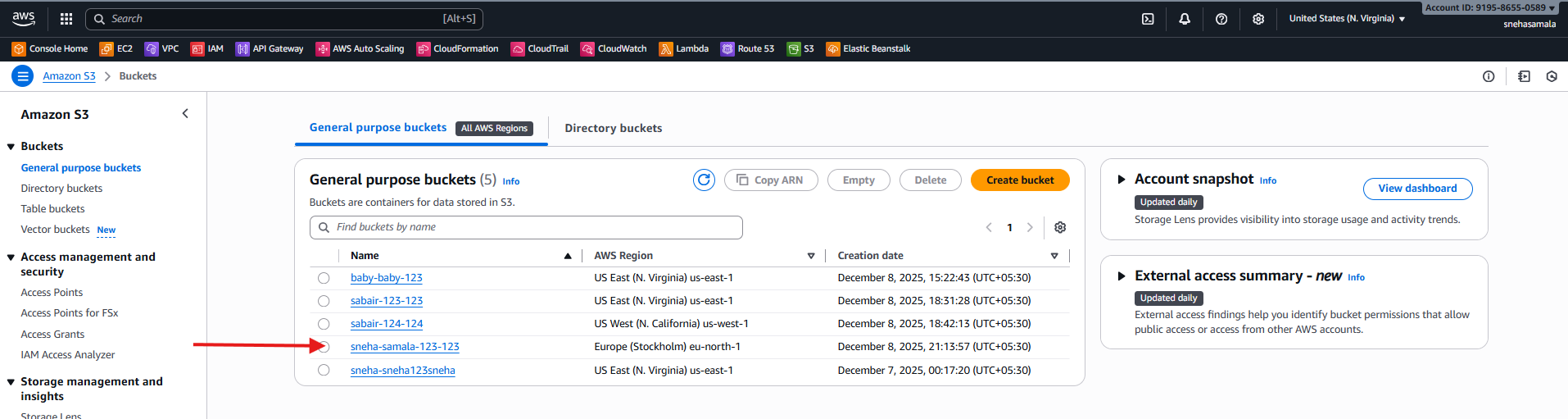


1. Write a Bash script to create an S3 bucket.

Creating the script to create the buket

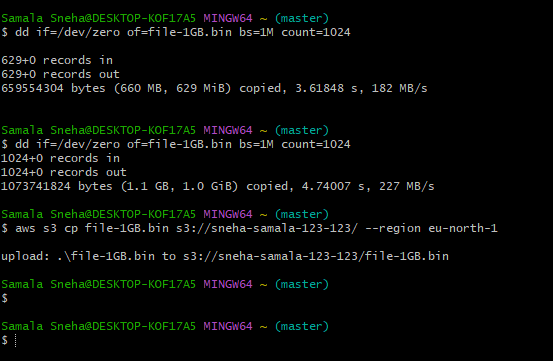


Success fully bucket is created



1. Upload a 1 GB file to S3 using the CLI.

Uploaded the 1gb file in CLI



Successfully file is uploaded

