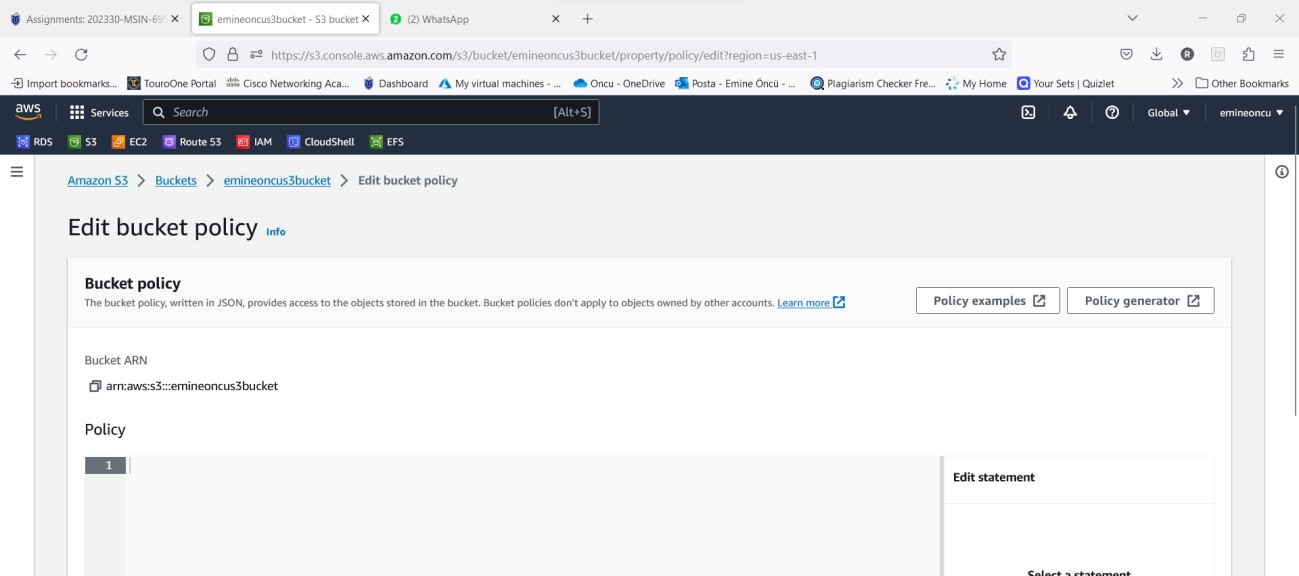
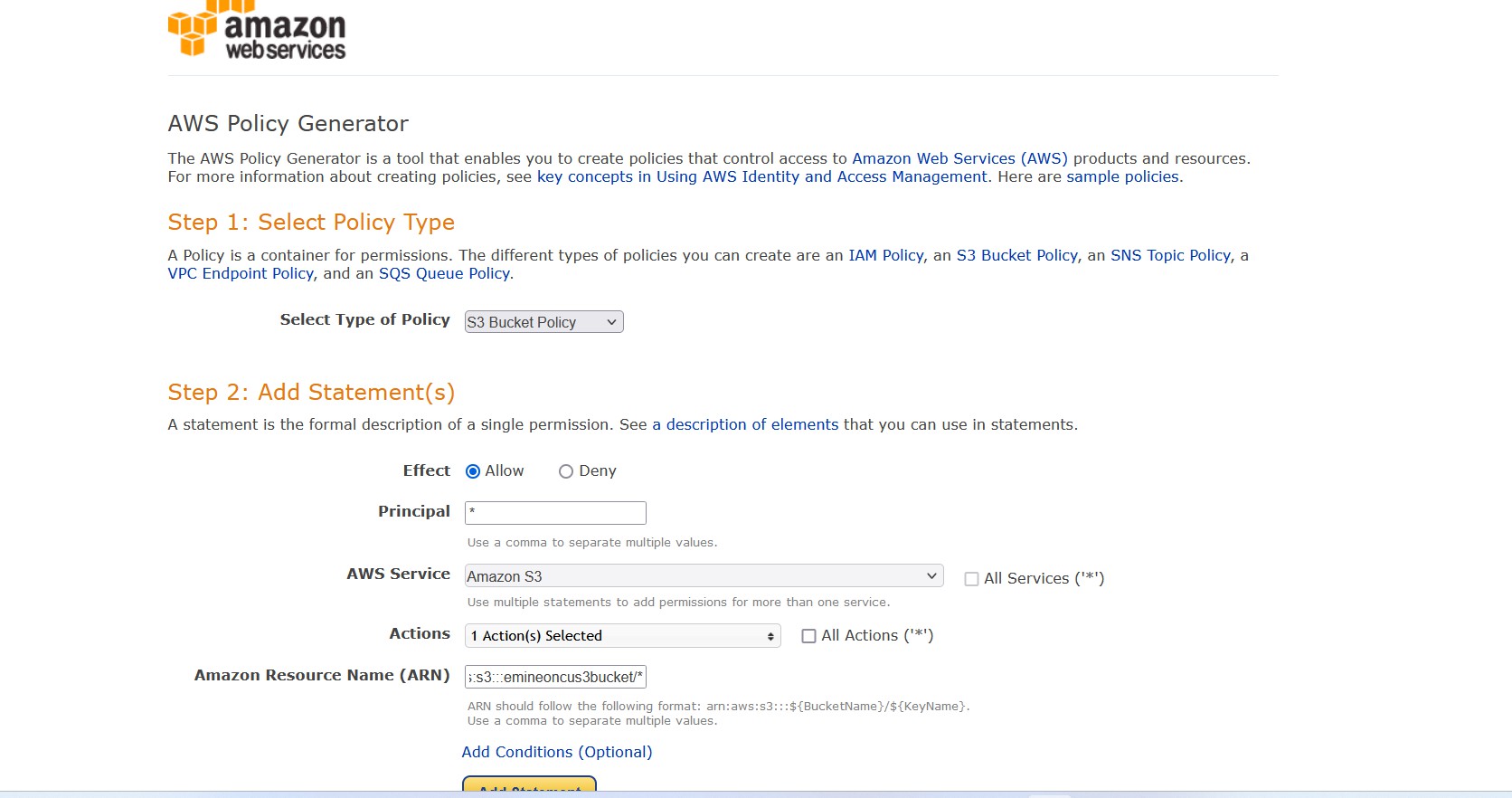


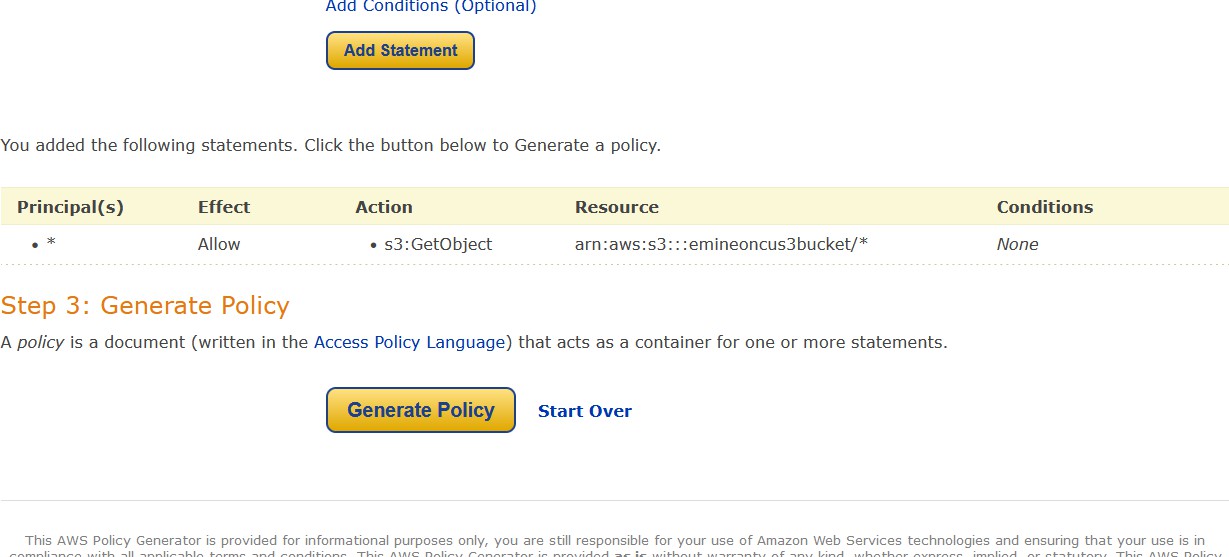
To make your **S3 bucket available publicly**, there are 2 settings to be done:

1. **Uncheck with ‘Block public access’**

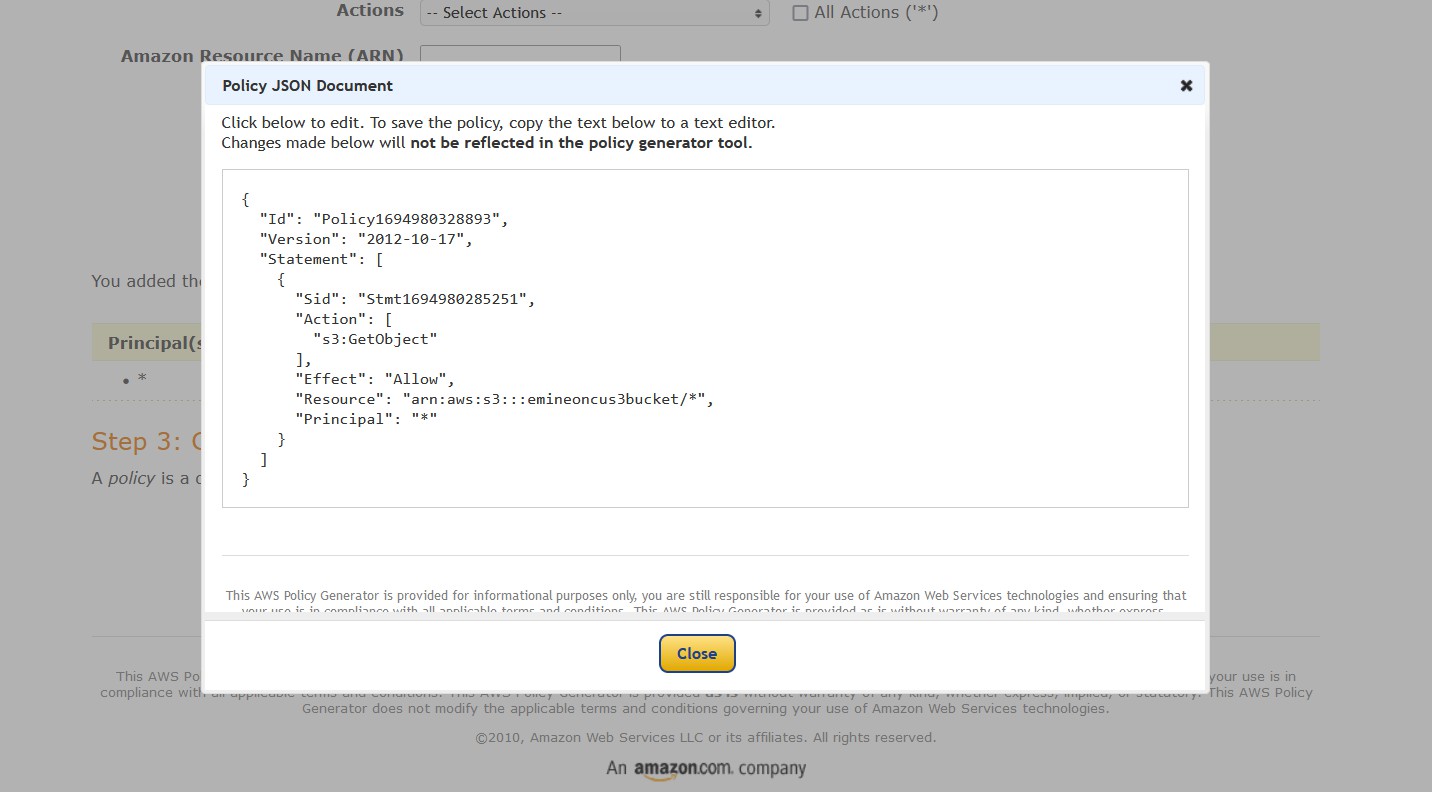


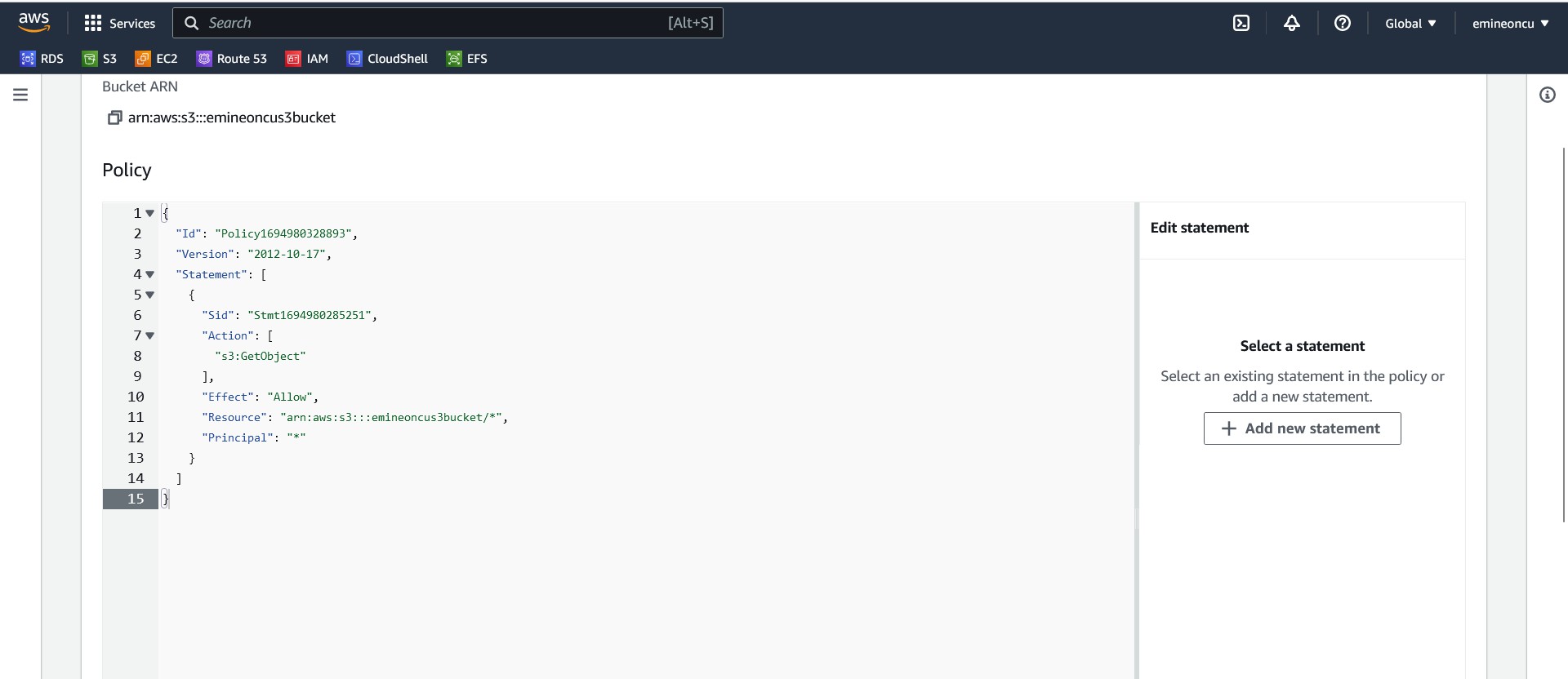
1. **Edit bucket policy to allow public access**



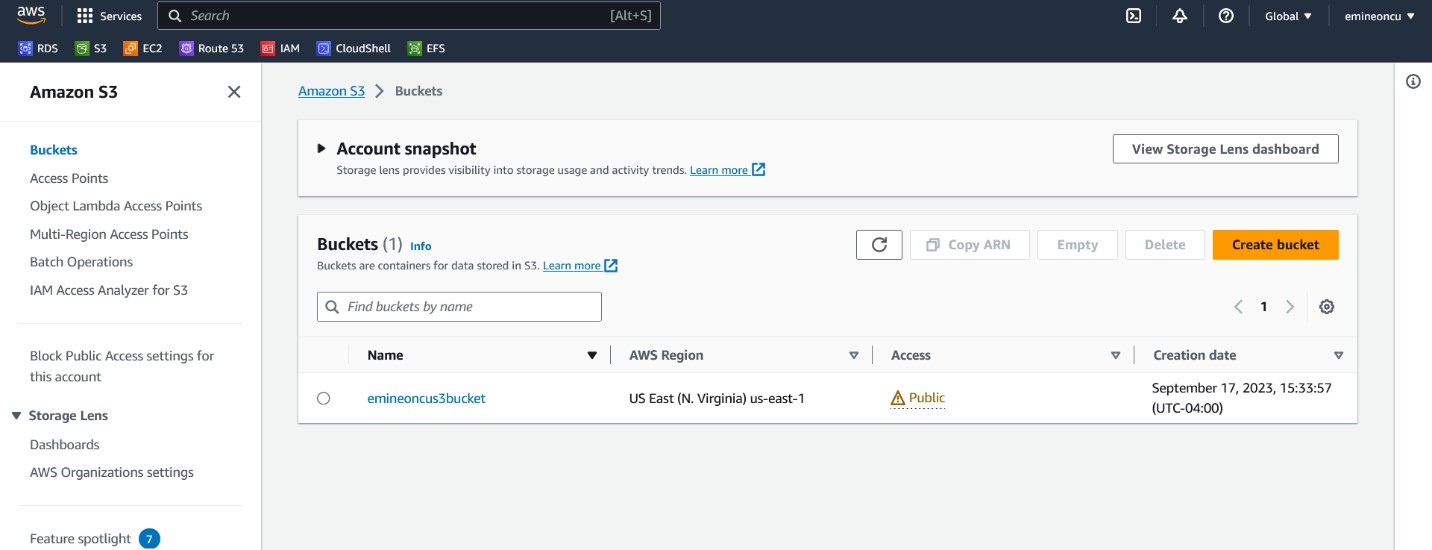


* + **Using Policy generation tool available within AWS console:**

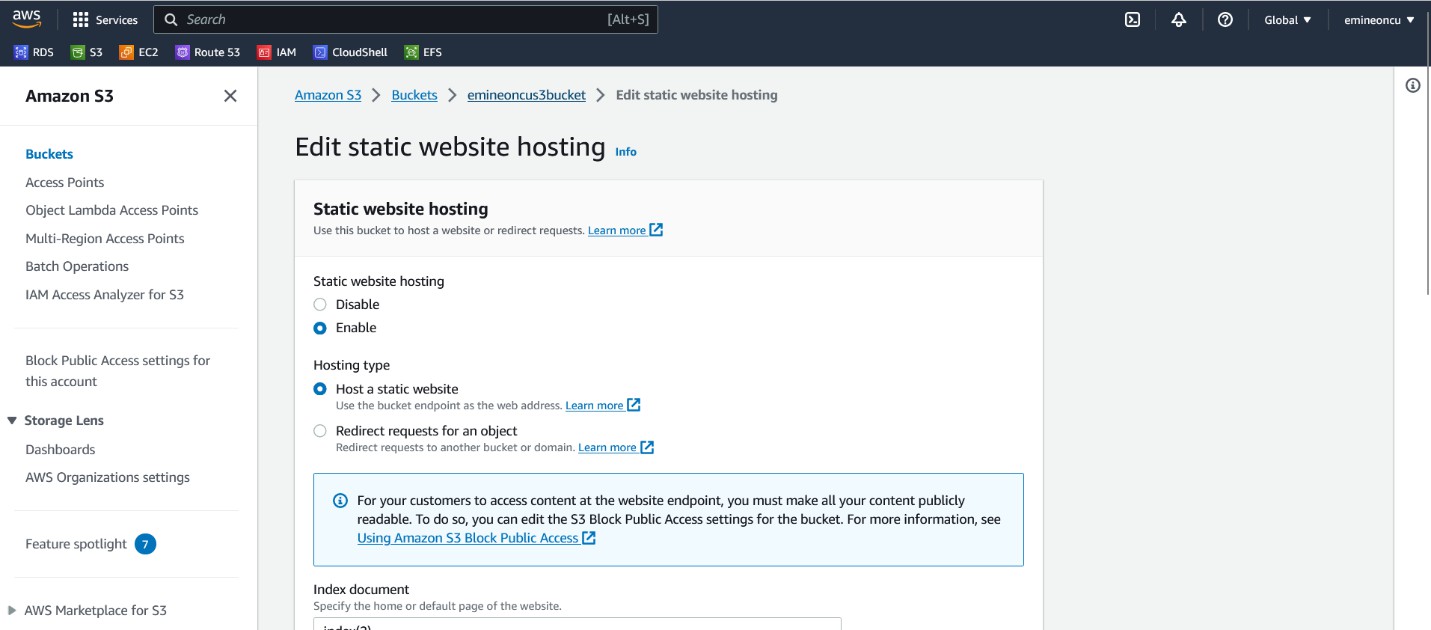


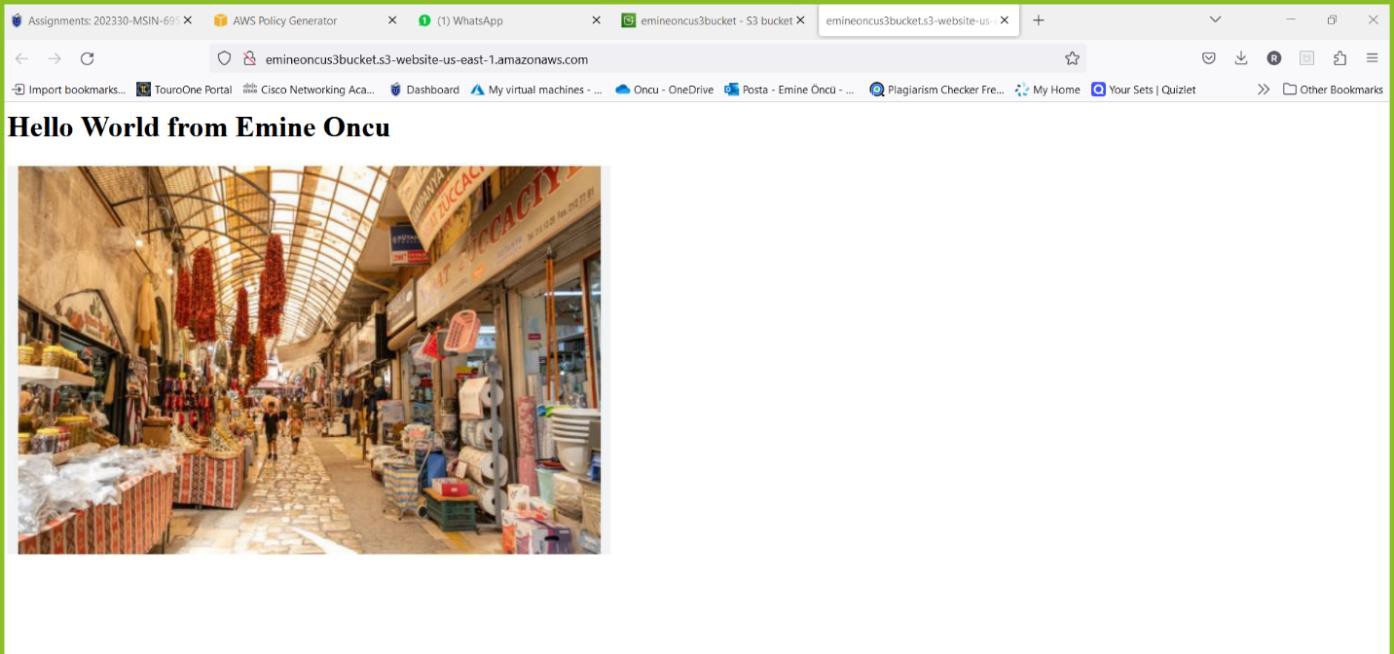


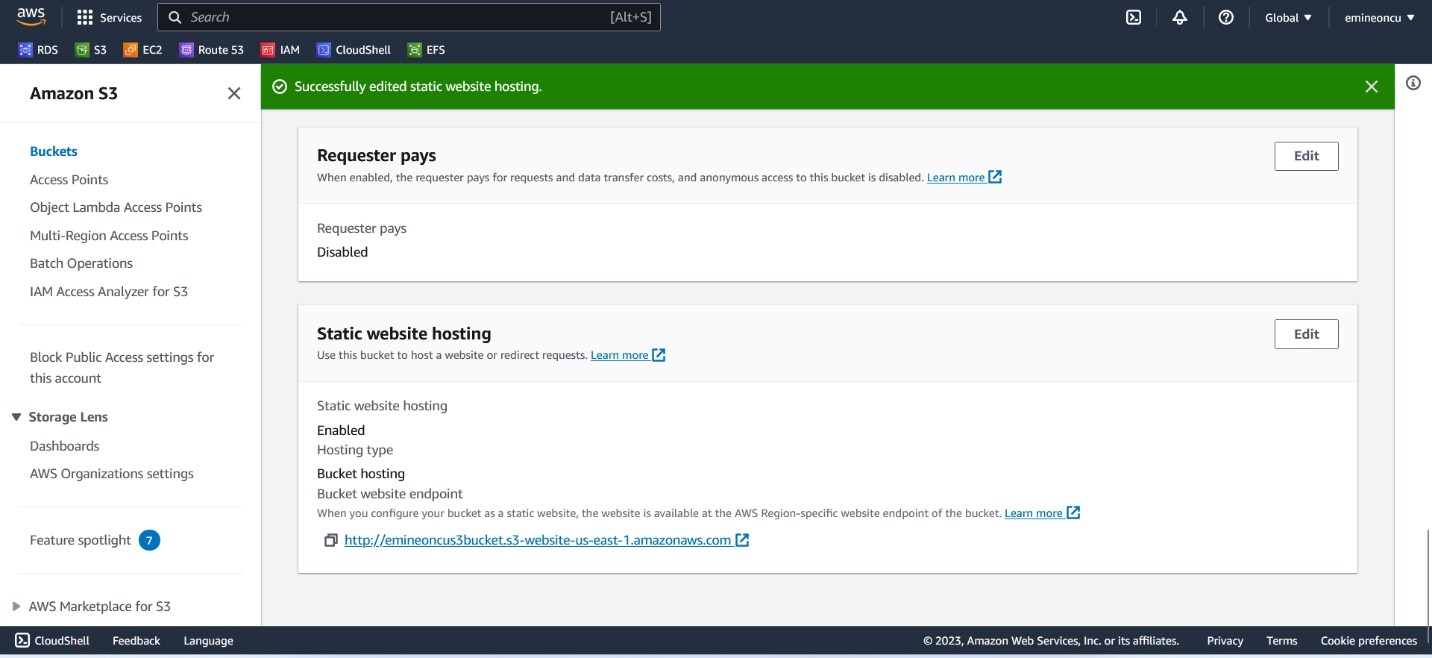
* + **Bucket is now publicly accessible:**

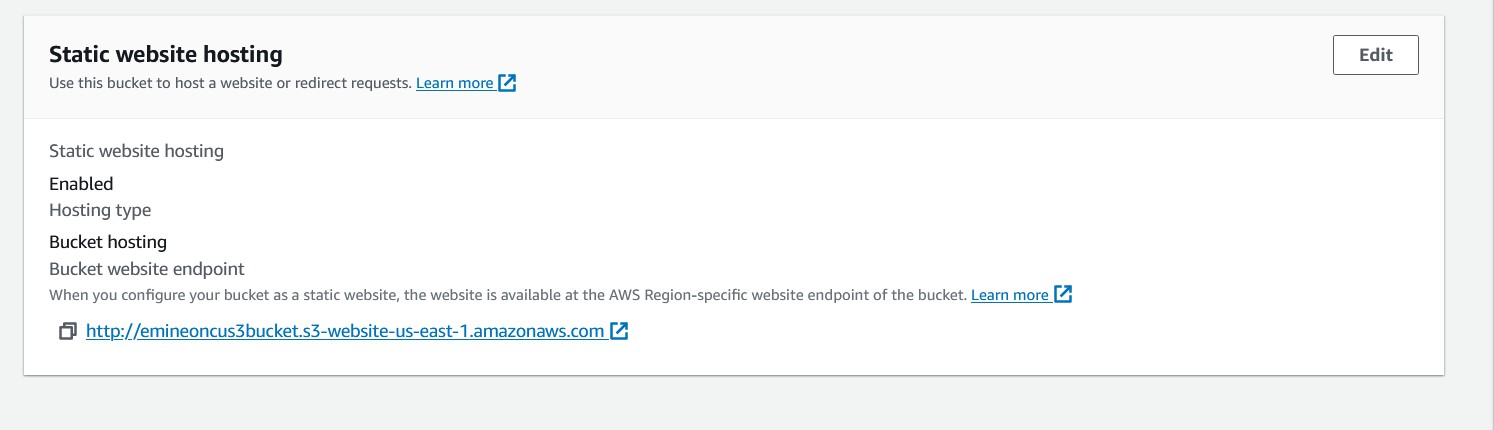


* + **Hosting a static website using S3:**





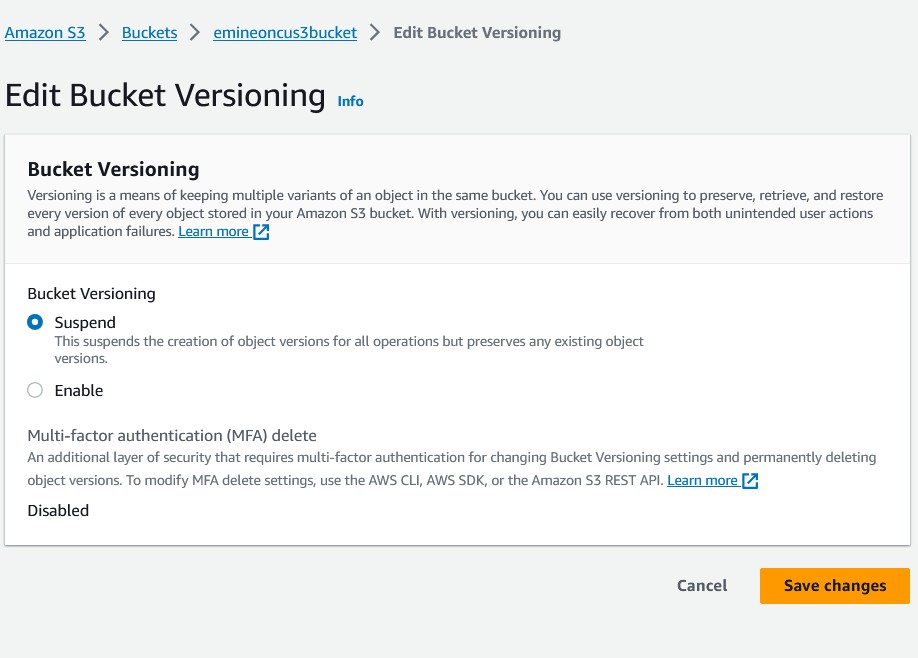
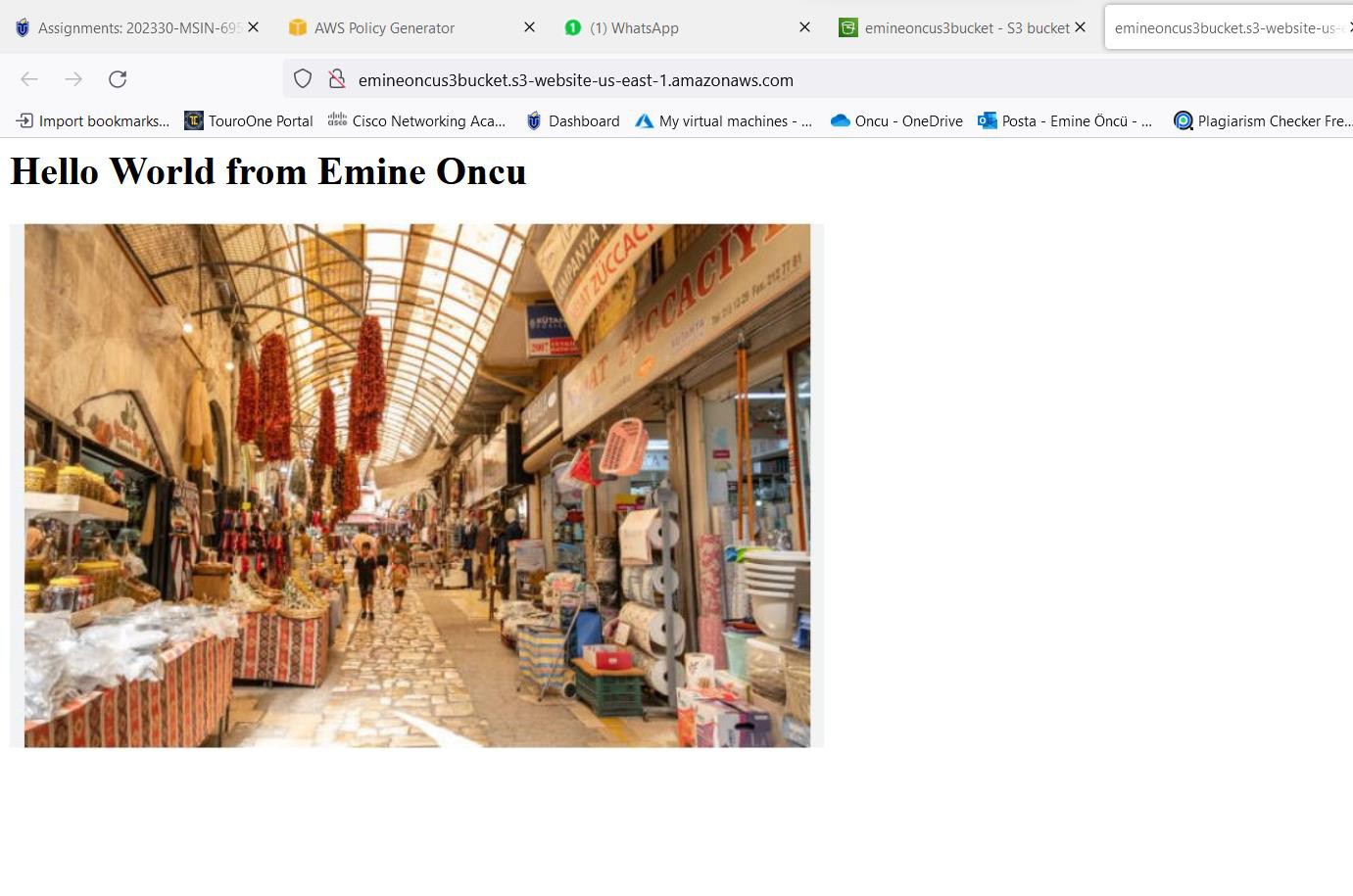


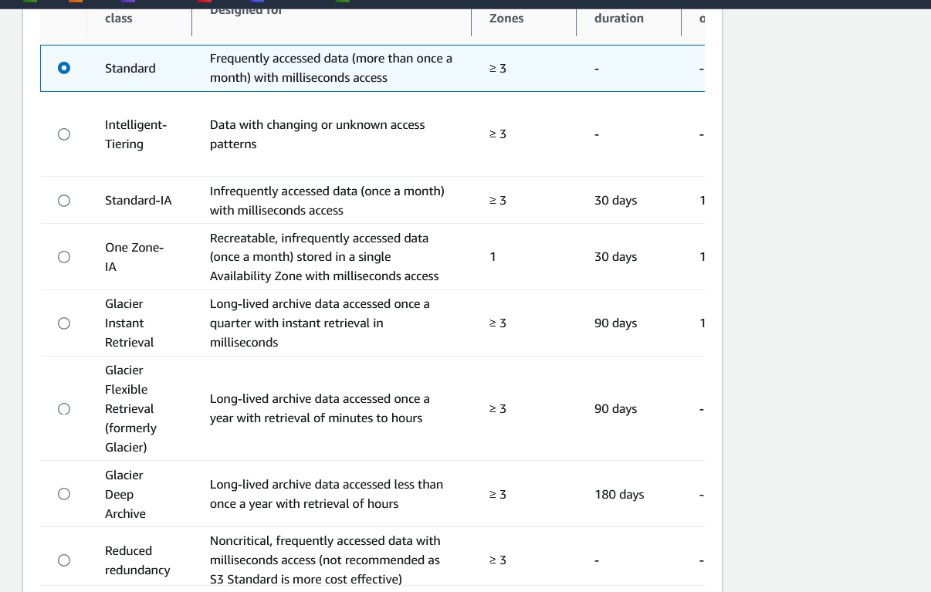


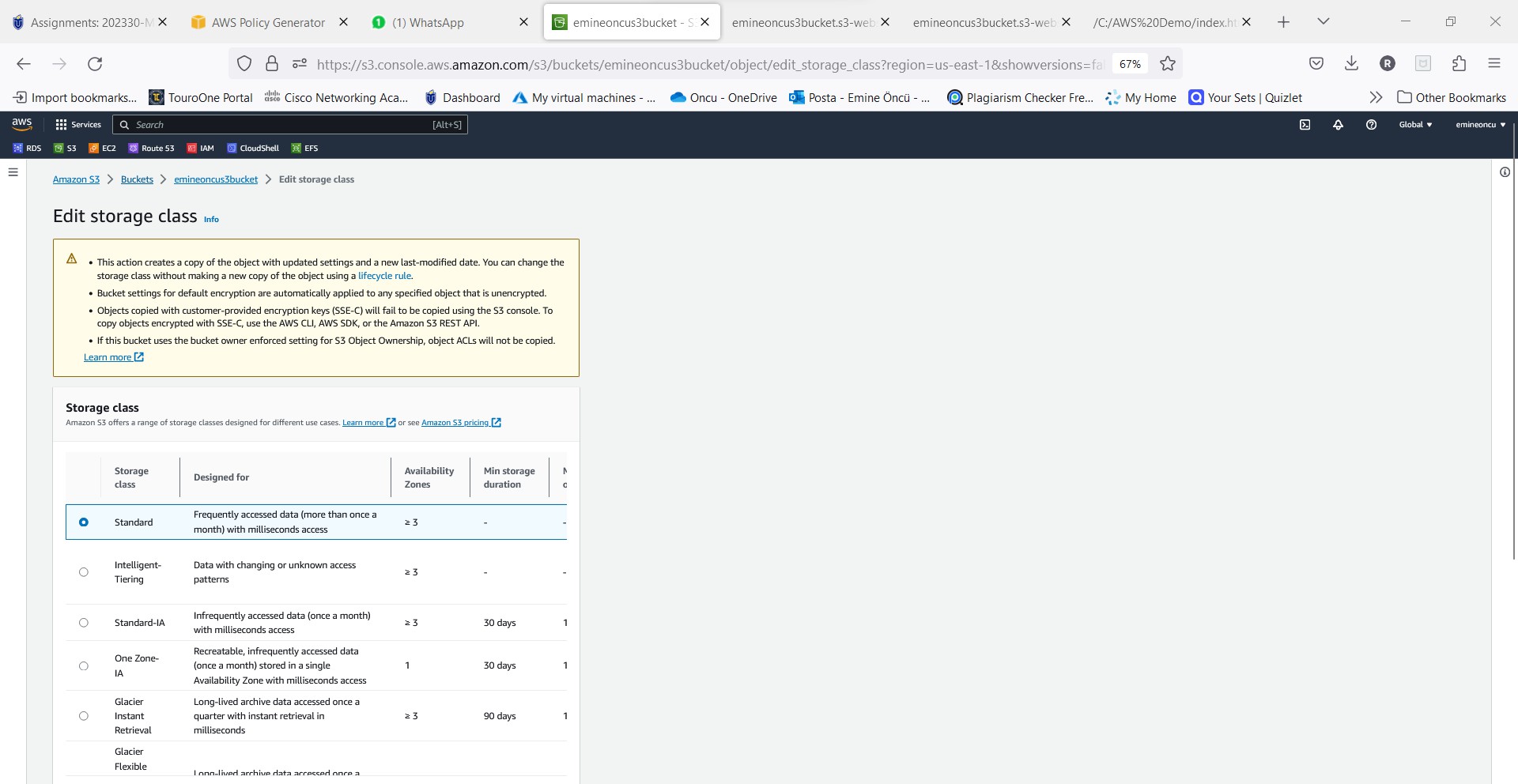
**CHAPTER 3**

**Demonstrate use of Simple Storage Service [S3] Bucket in AWS**

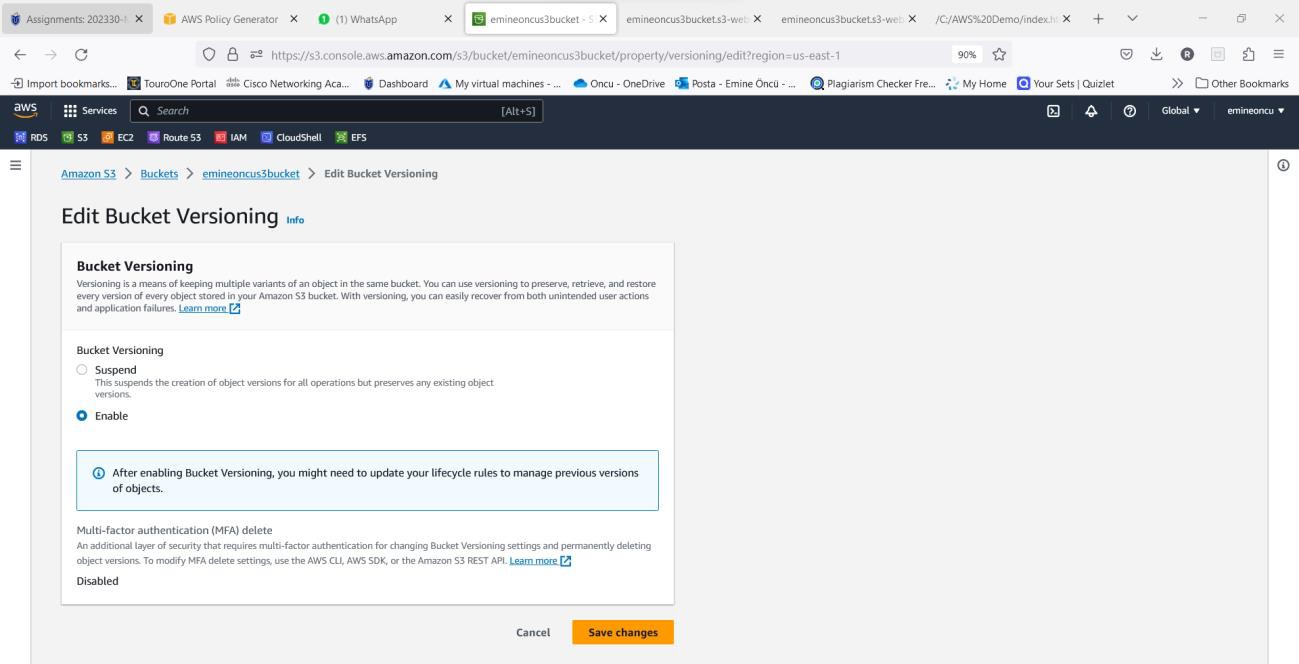
* + **Changing S3 storage class**



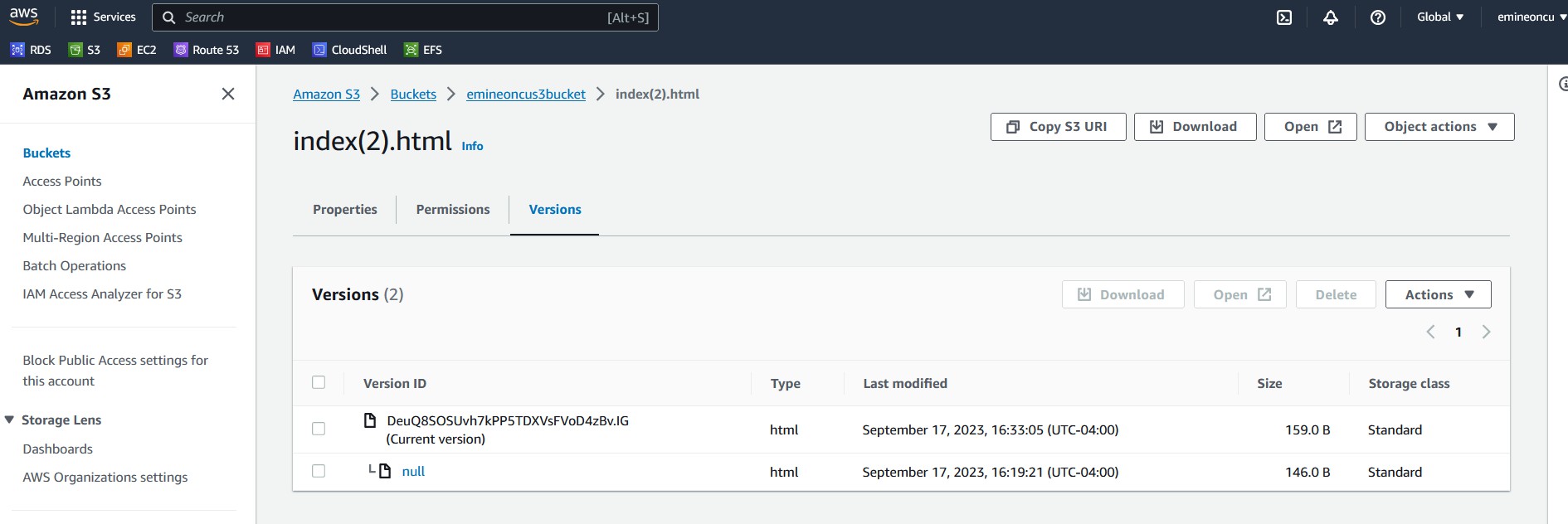




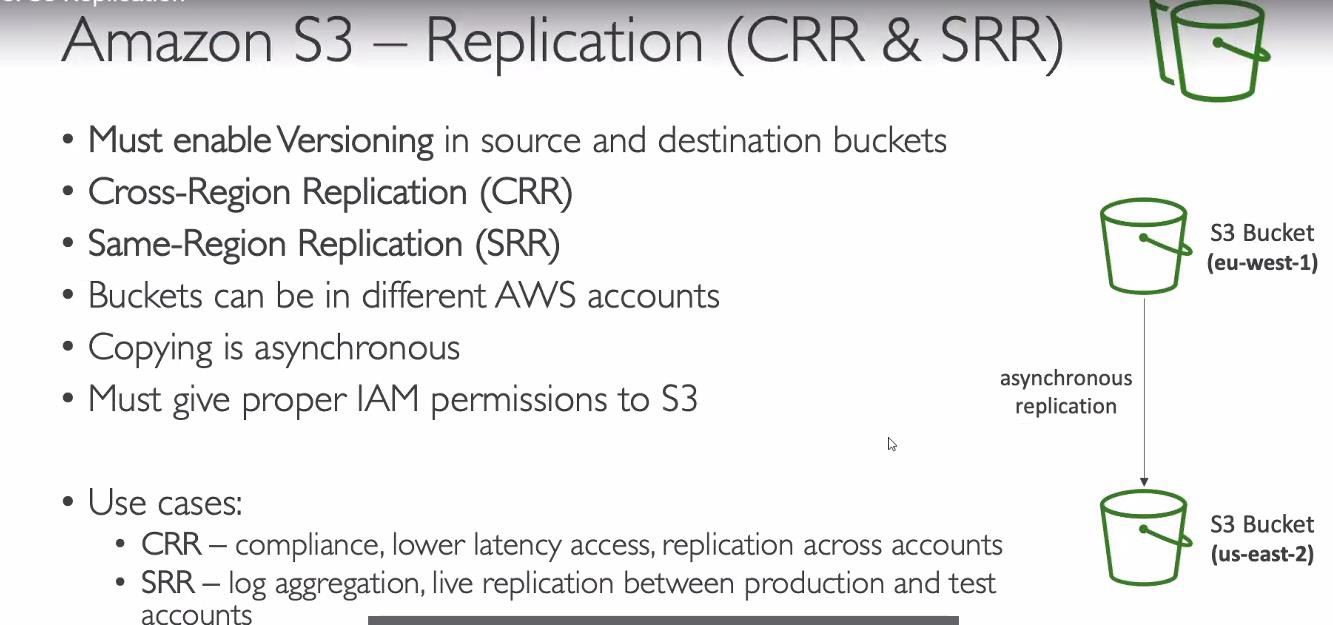
* + **Enabling Bucket versioning: Allows us to maintain multiple versions of a file.**



Enabling versioning:

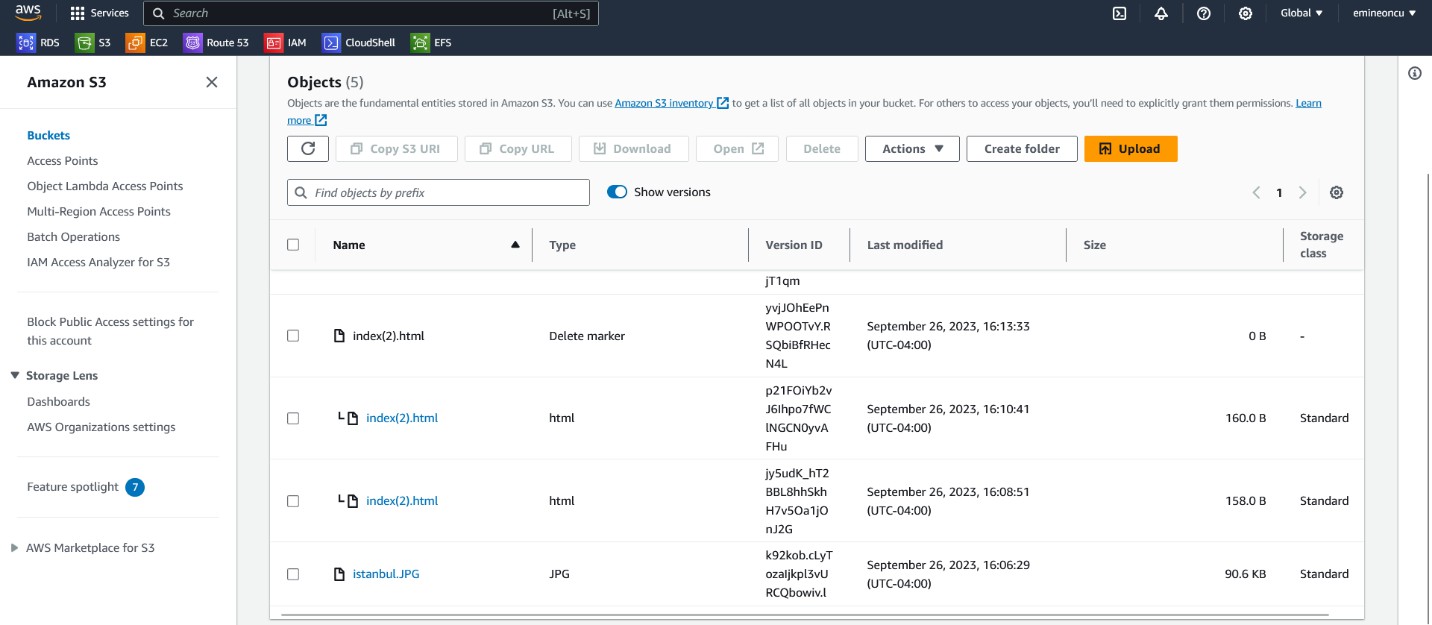


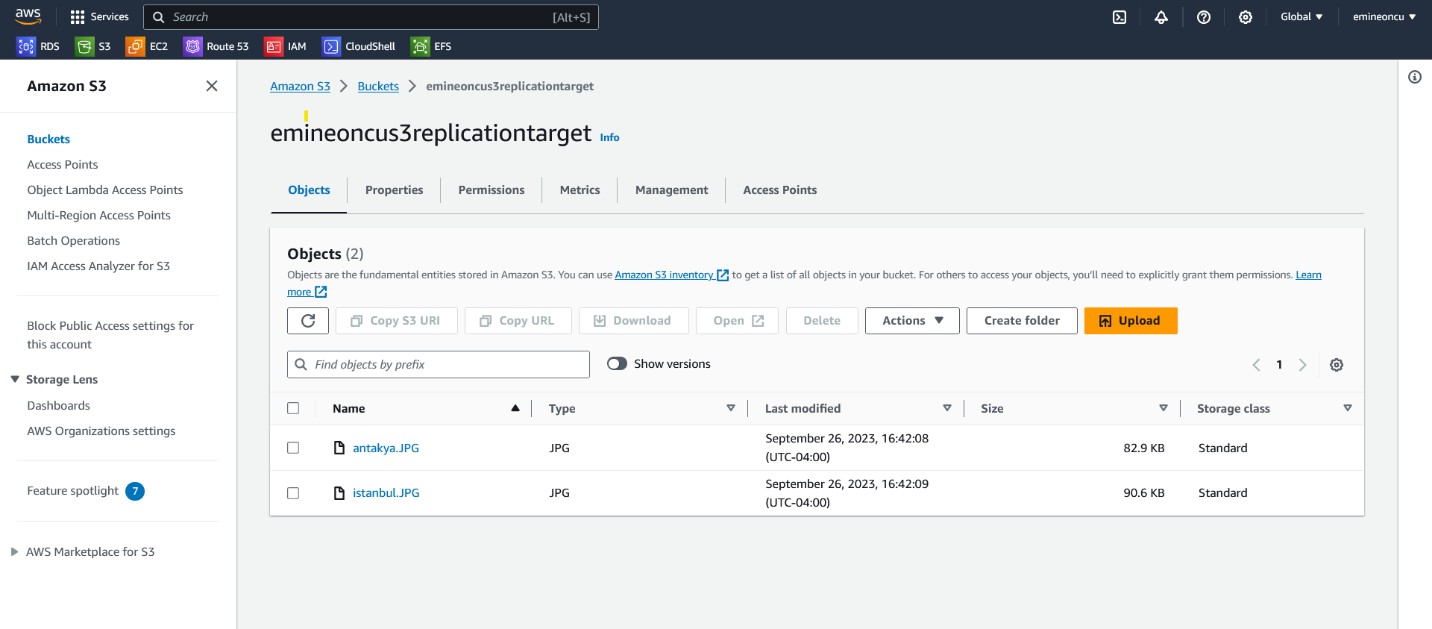
* + **Previous version of index.html and New version of index.html**
  + **Replication and Encryption Part**



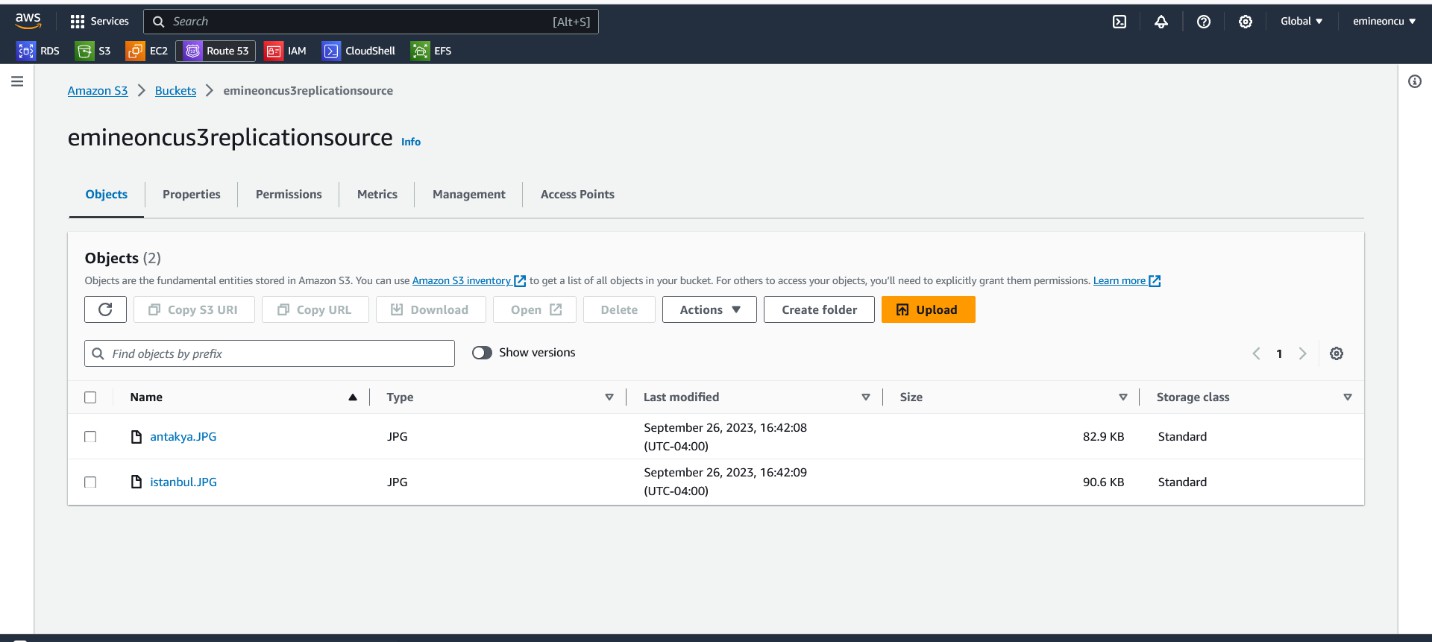
* + **After versioning the file if you delete it, AWS will set a “Delete Marker” on the file, but you**

can still obtain the file by moving the “Show Version” slider.

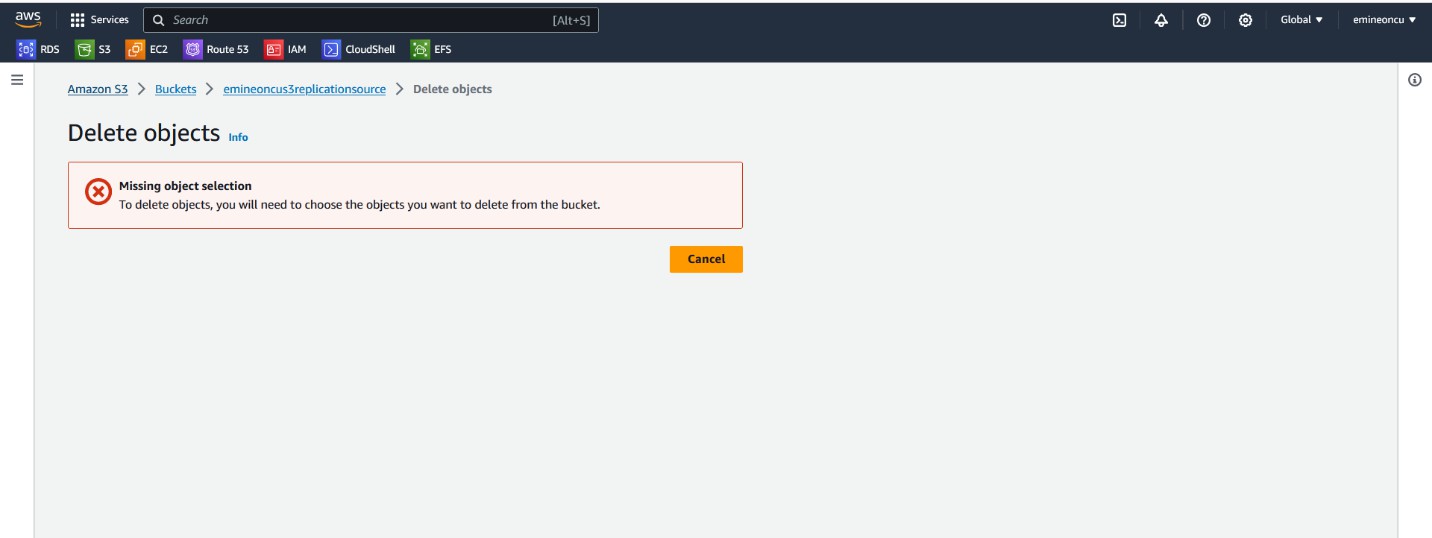


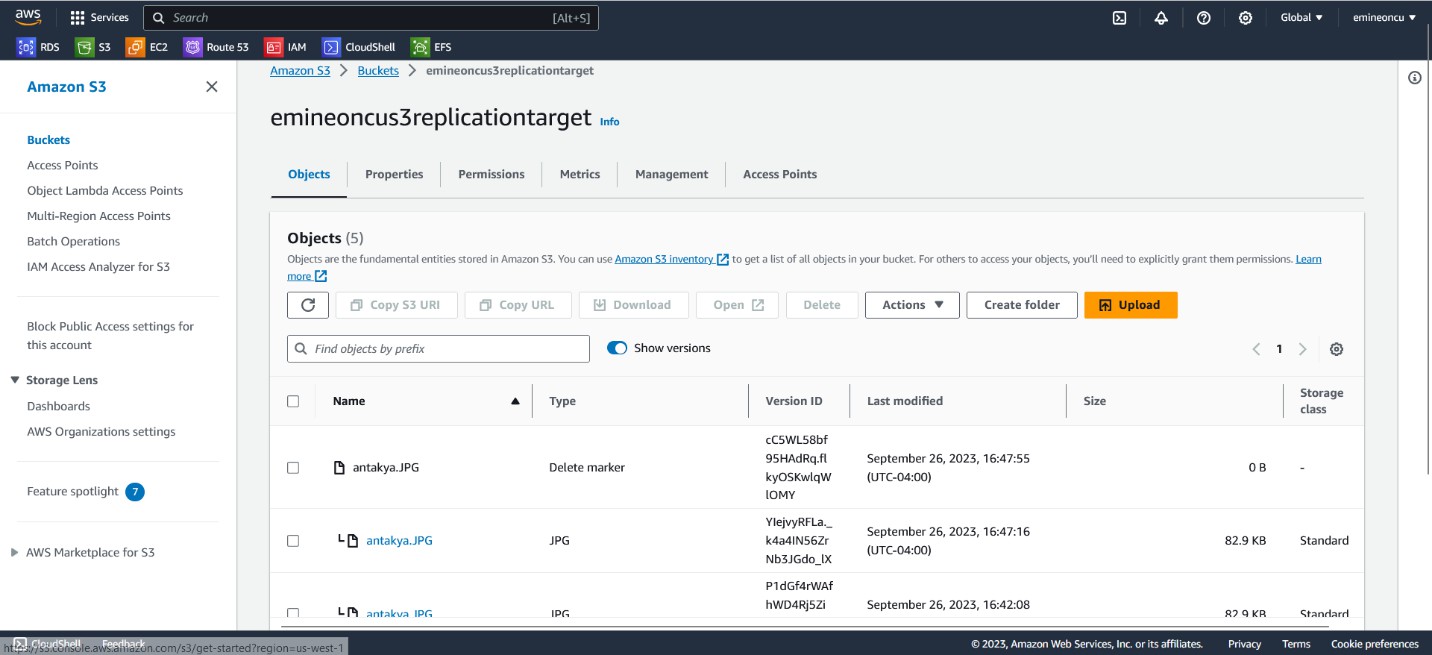


* + **The same two files are now available in the Target bucket.**



* + **When two files were uploaded to the Source bucket**
  + **Enabling the ‘Delete Marker’ replication on Source bucket.**

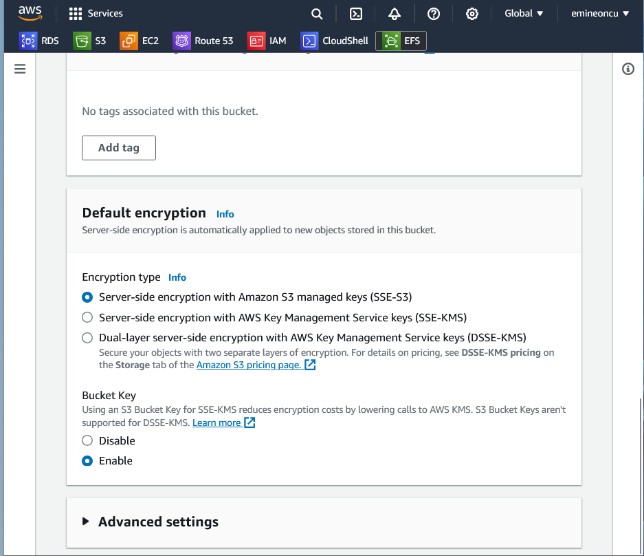




* + **Will ensure the file gets deleted from the target bucket as well along with the ‘Delete Marker’**

being replicated to the target bucket.

* + **Encryption Part**



* + **Applying default encryption to my S3 bucket. Helps protect data, especially sensitive data.**

