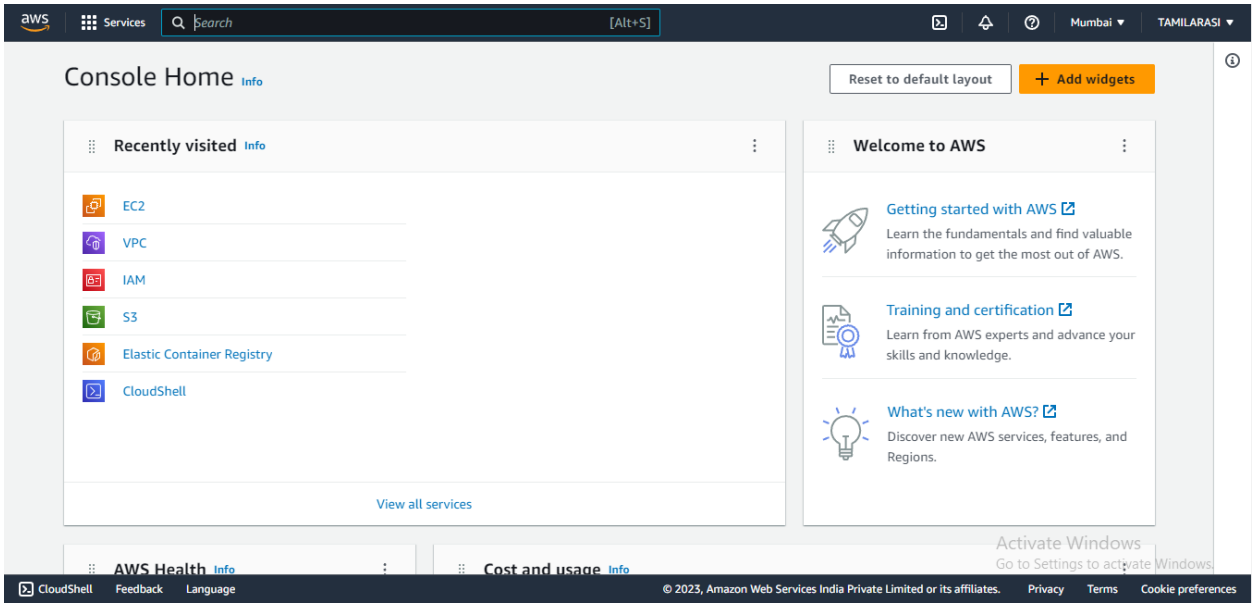
NAME :TAMILARASI
REG NO:727721EUCS163

AMAZON CLOUD COMPUTING

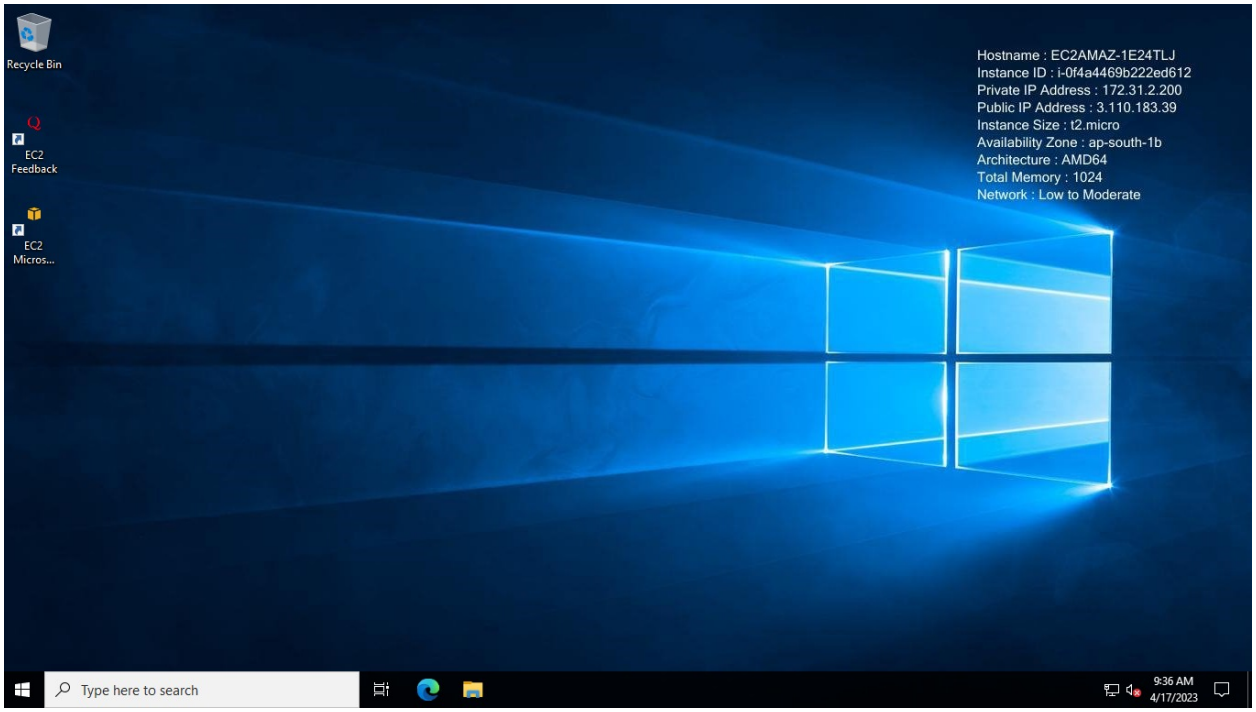
Day1:

1.Aws account creation:



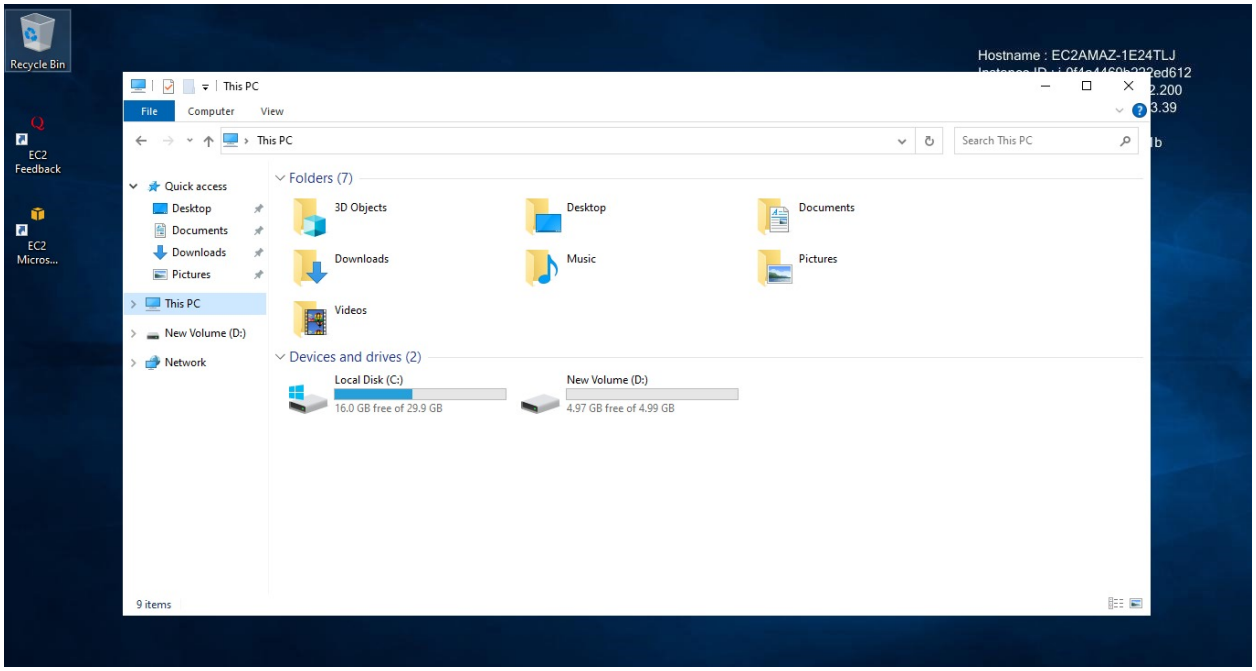
Day2:

Create a Windows EC2 instance with t2.micro Instance and show the remote connection of that EC2 Instance.

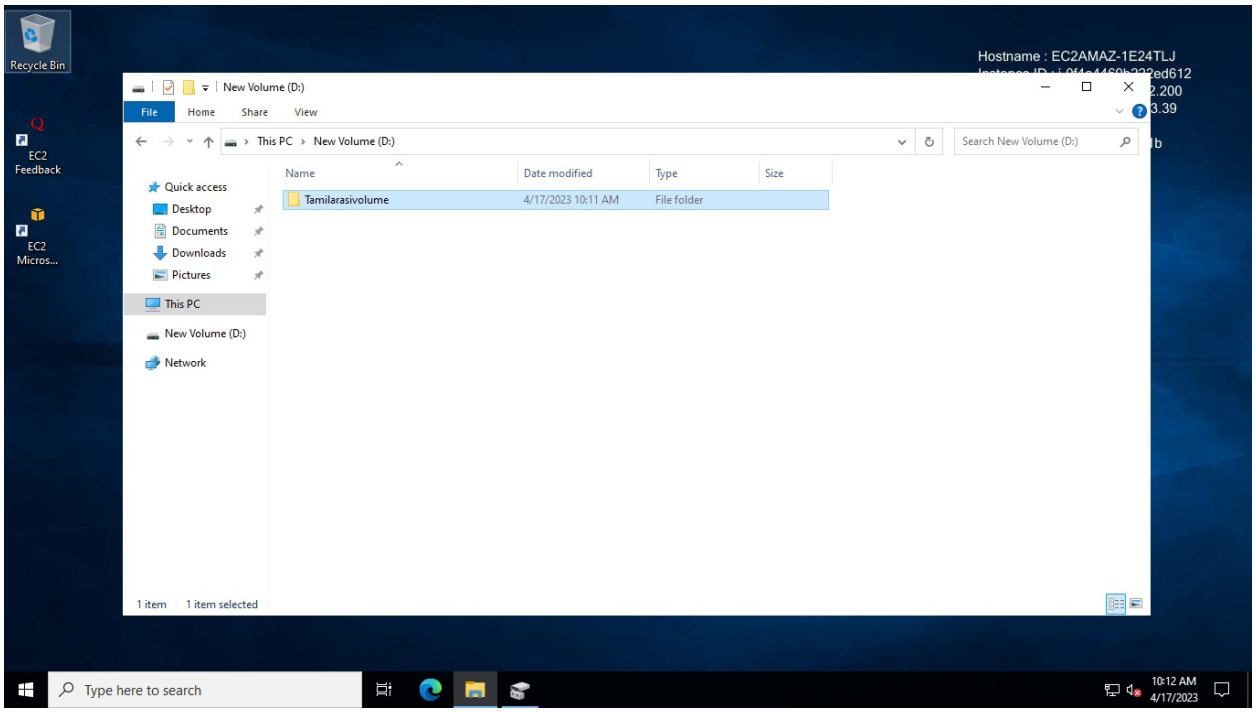


2.

Create an EBS volume of 5 GB and attach to a windows EC2 instance and make partition of that EBS volume.



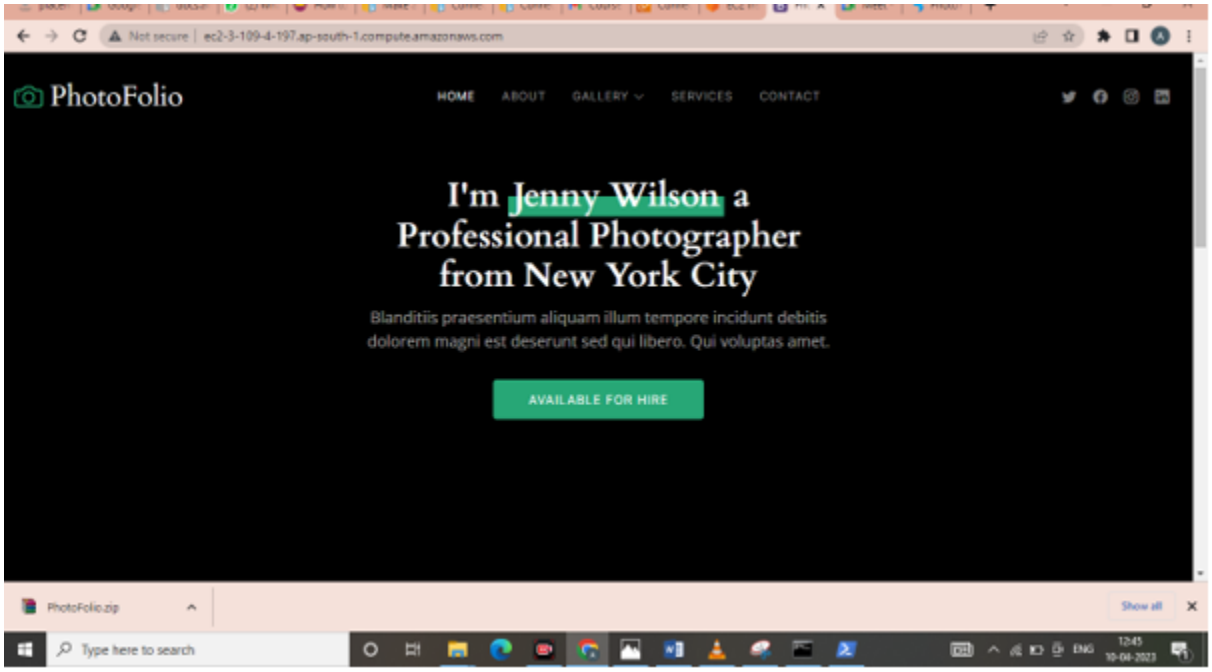
3.Create some files and folders into 5 GB EBS volume of the previous exercise and take a snapshot of that EBS volume.

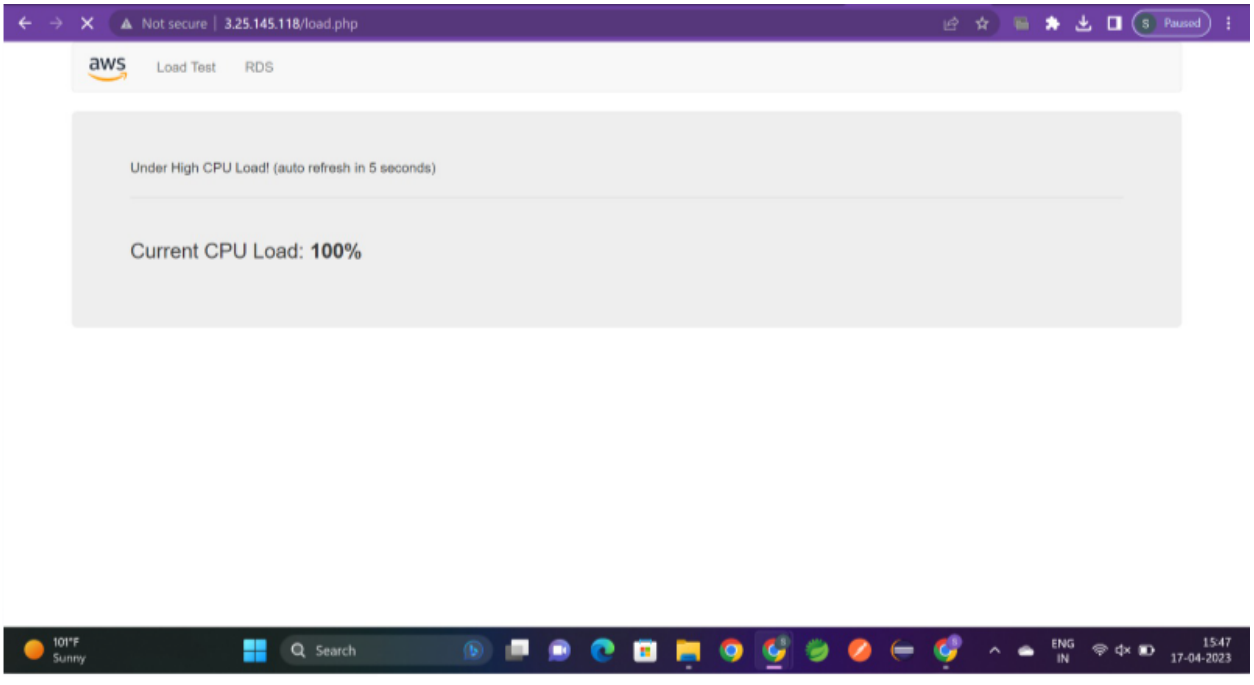


4.

Create a Linux EC2 instance with t2.micro Instance and show the remote connection of that EC2 Instance.

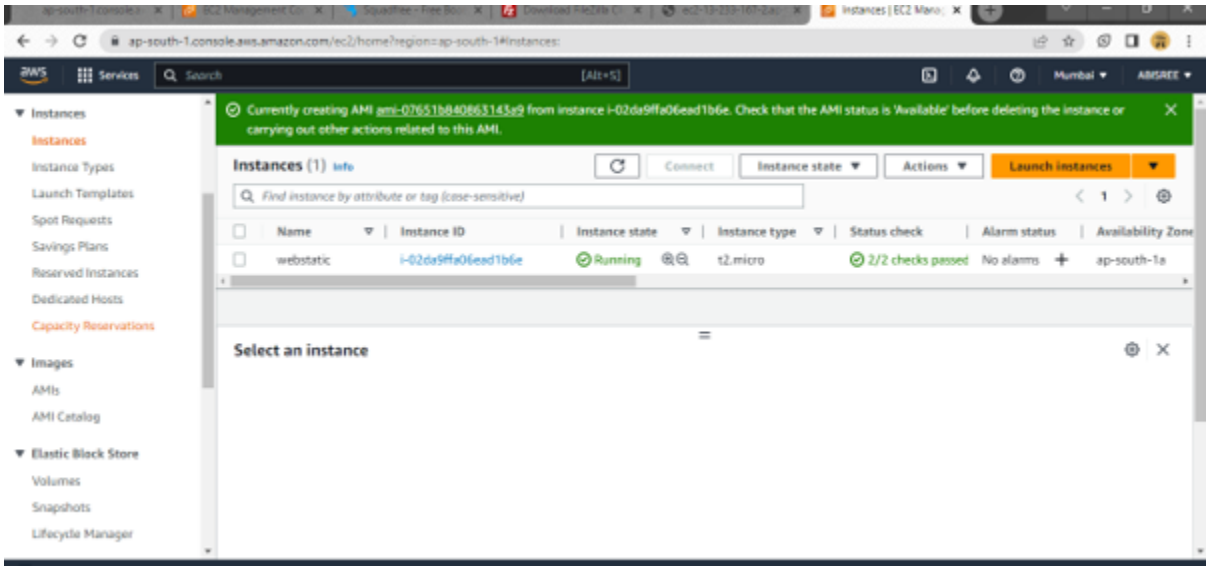
5.Install, Start and Enable the httpd webservice in that Linux EC2 Instance, then host a static website in EC2.





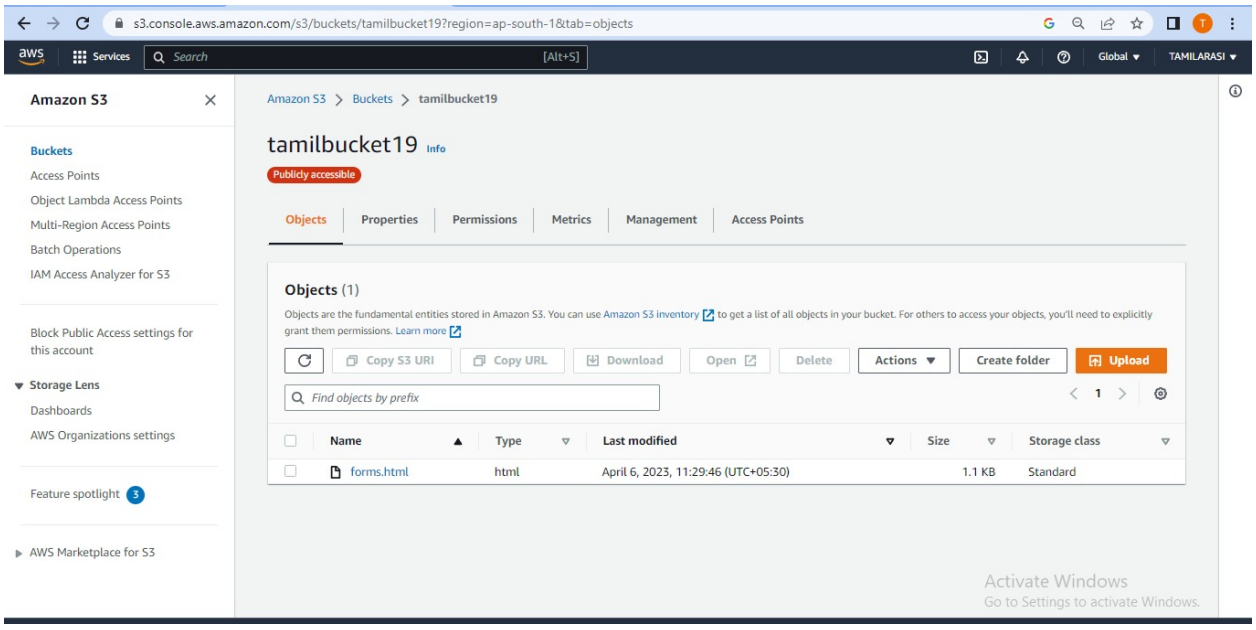
6.

Create Image(MyAMI) of the linux Webserver(from the previous exercise) and launch new EC2 instance from the created Image(MyAMI)

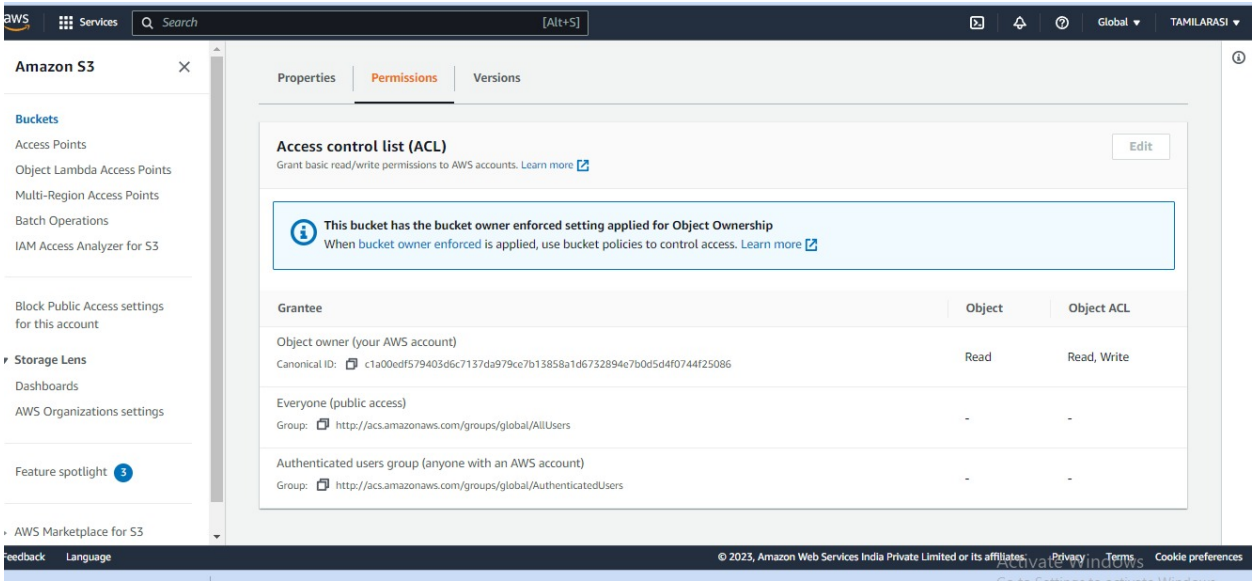


Day3

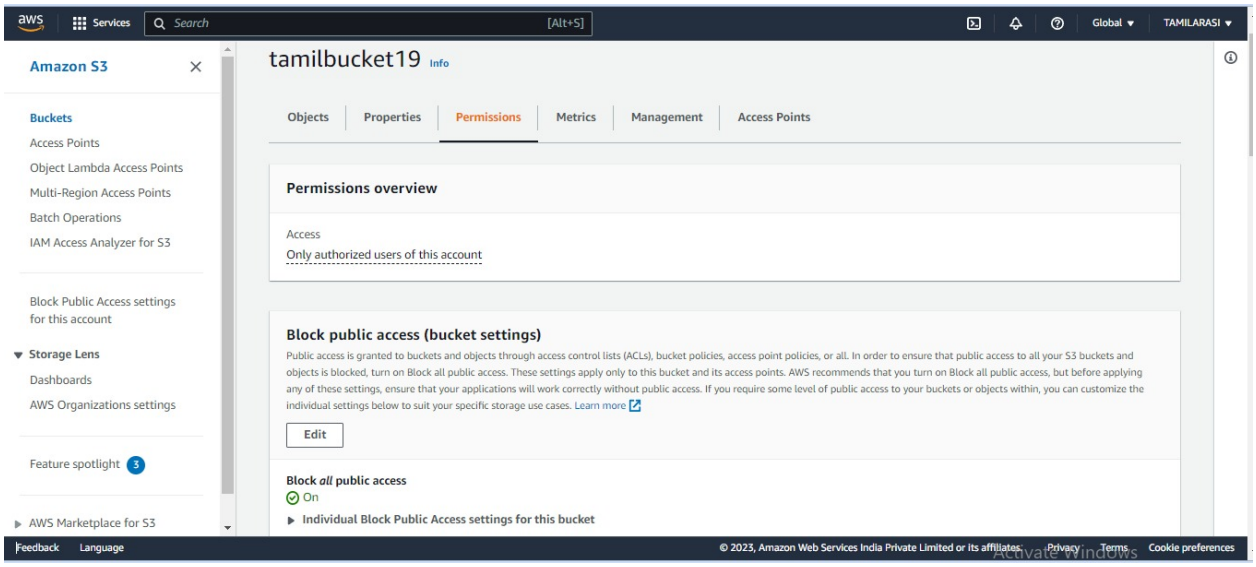
1.Create a S3 Bucket and create a folder in the bucket and upload a file in the folder.



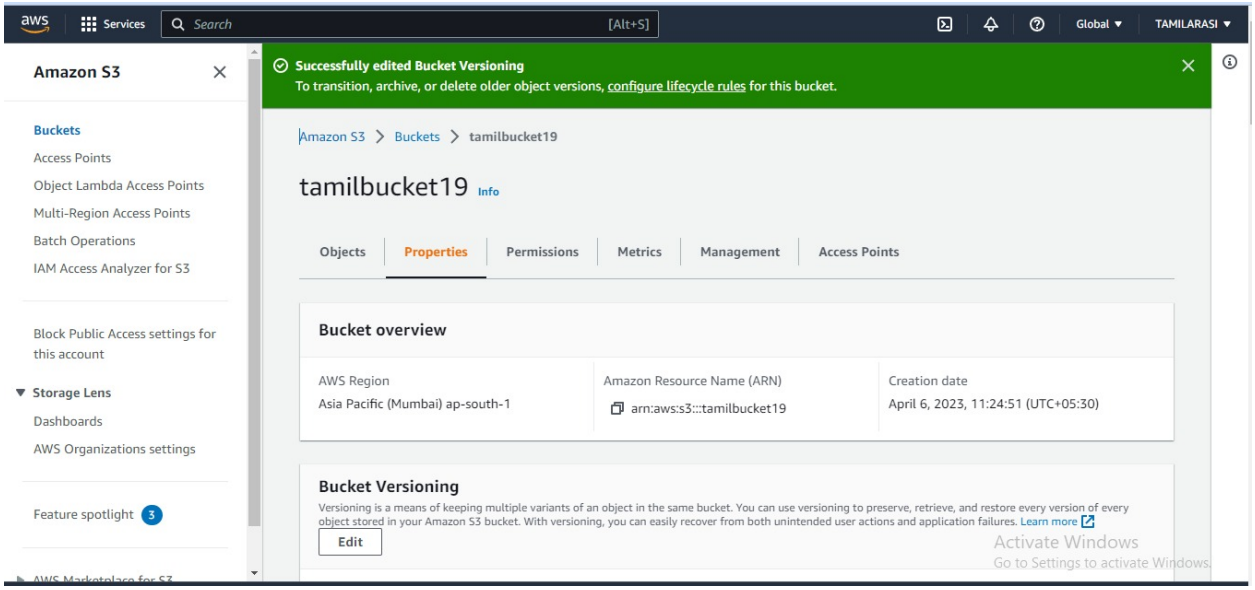
2.Disable "Block Public Access" for the bucket and enable public read access for a file.



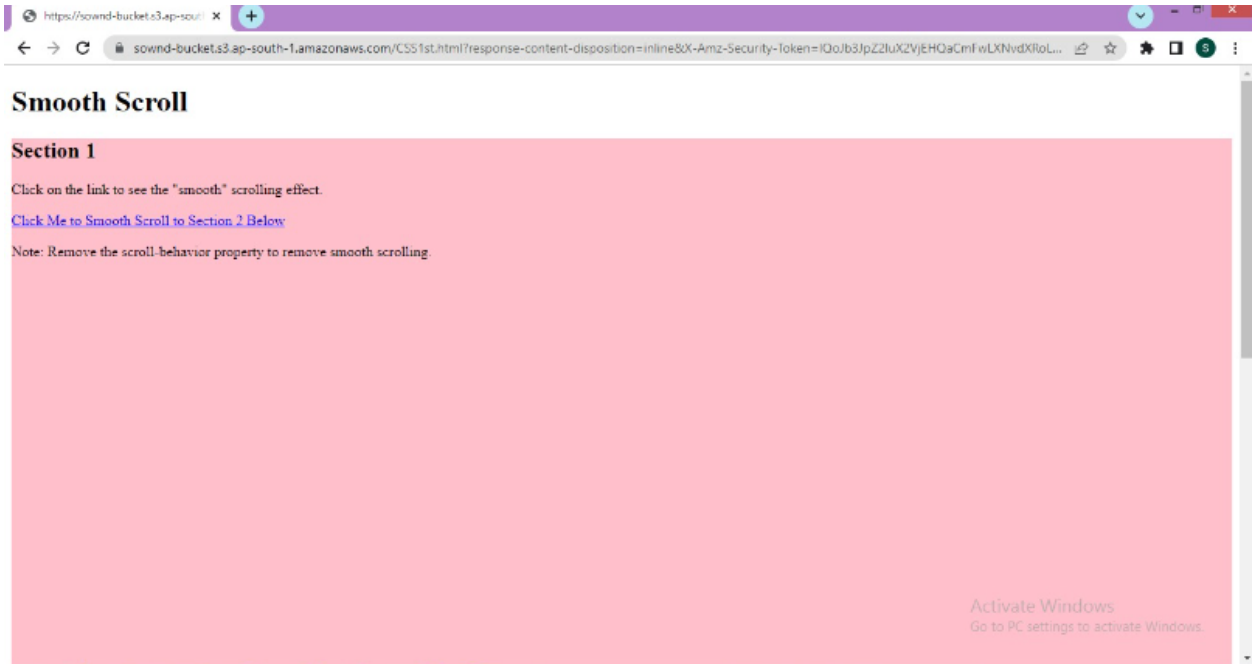
3.Create a bucket policy which should deny to read objects under a folder of a bucket.



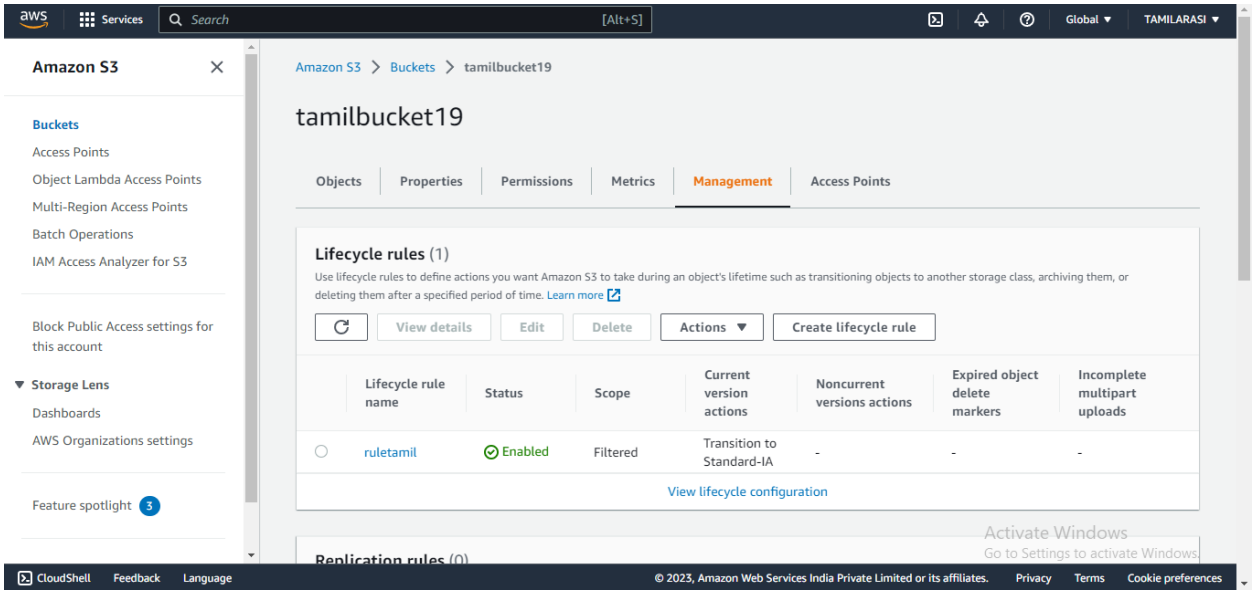
4.Enable versioning objects for a bucket and upload objects with multiple versions of it.



5.Host a static webpage in a bucket itself by using static website hosting feature of it.

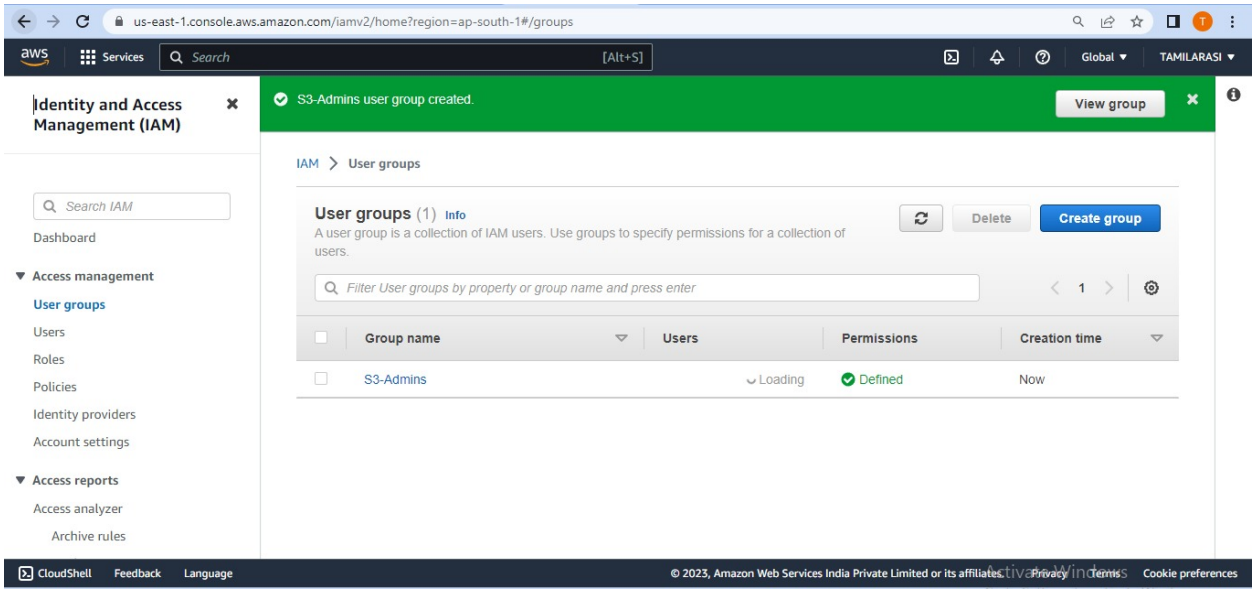


6.Enable a lifecycle management rule between various storage classes for a S3 bucket.

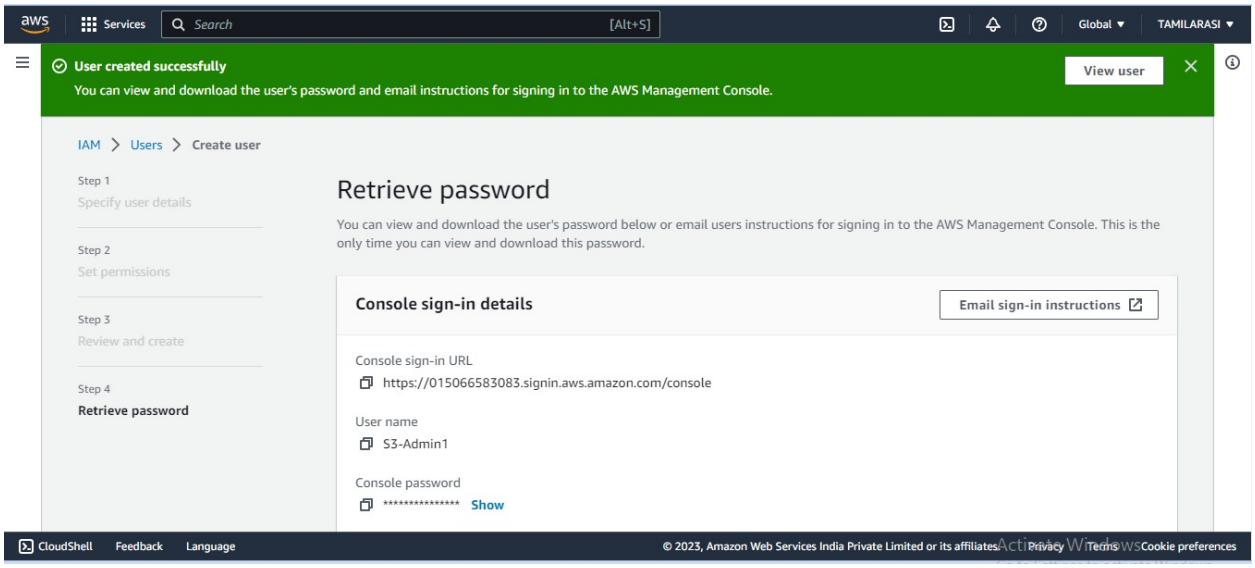


Day:4

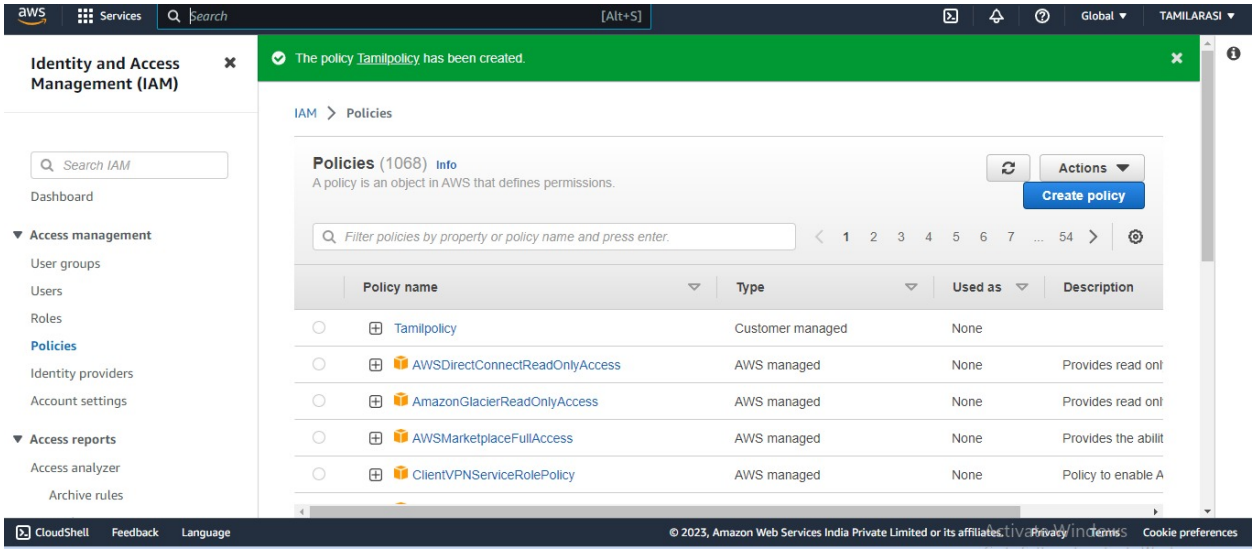
1.Create an IAM group called as ‘S3-Admins’ with ‘AmazonS3FullAccess’.



2.Create an IAM user called as ‘S3Admin1’ and add it to the ‘S3-Admins’ group.

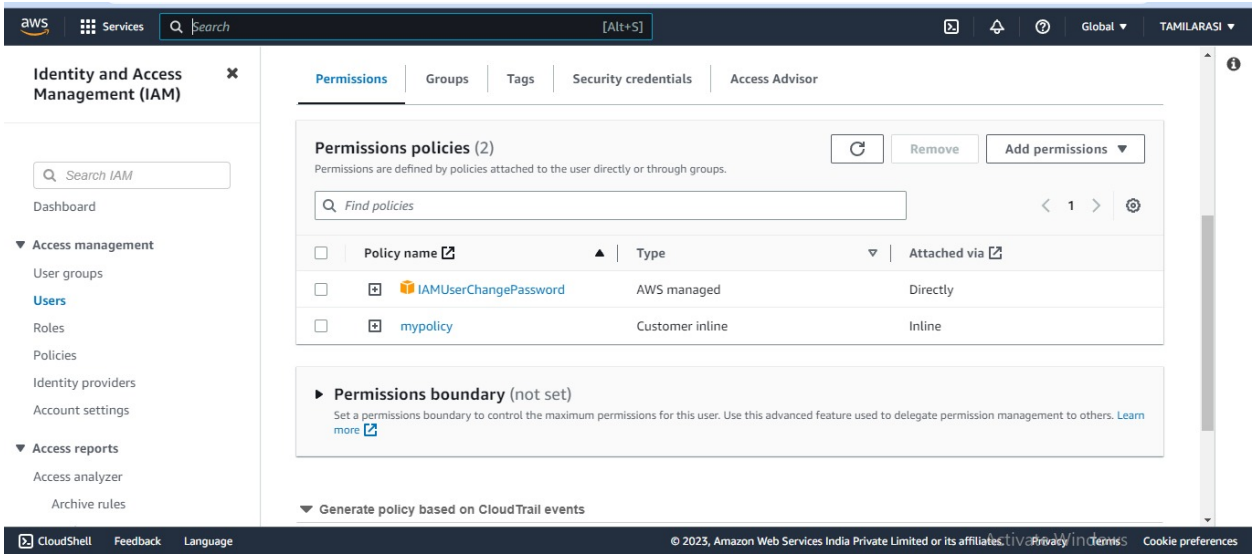


3.Attach an IAM custom policy to the ‘S3-Admins’ group which should deny to delete objects.

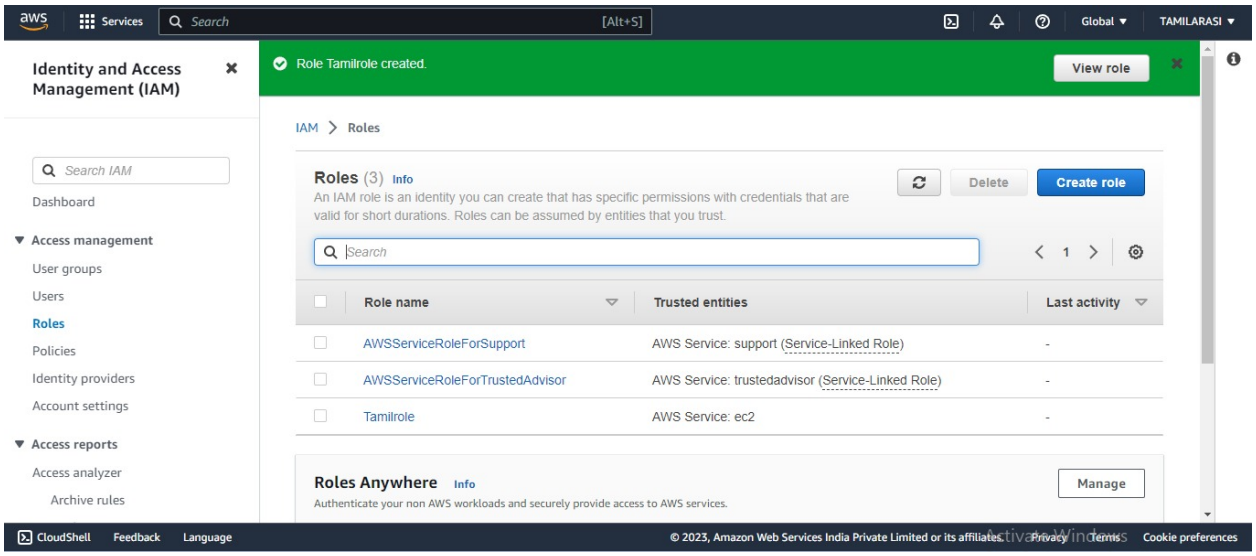


4.

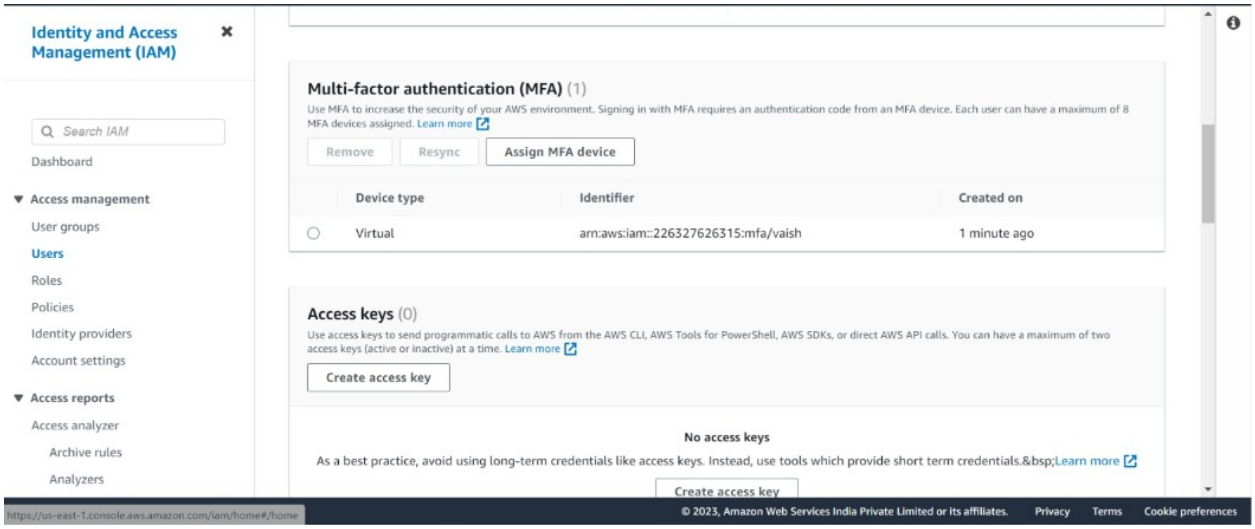
Create an Inline policy for an IAM user and set some permission boundary for that user.



5.Create an IAM role with ‘AmazonS3FullAccess’ and attach the role to an EC2 instance.

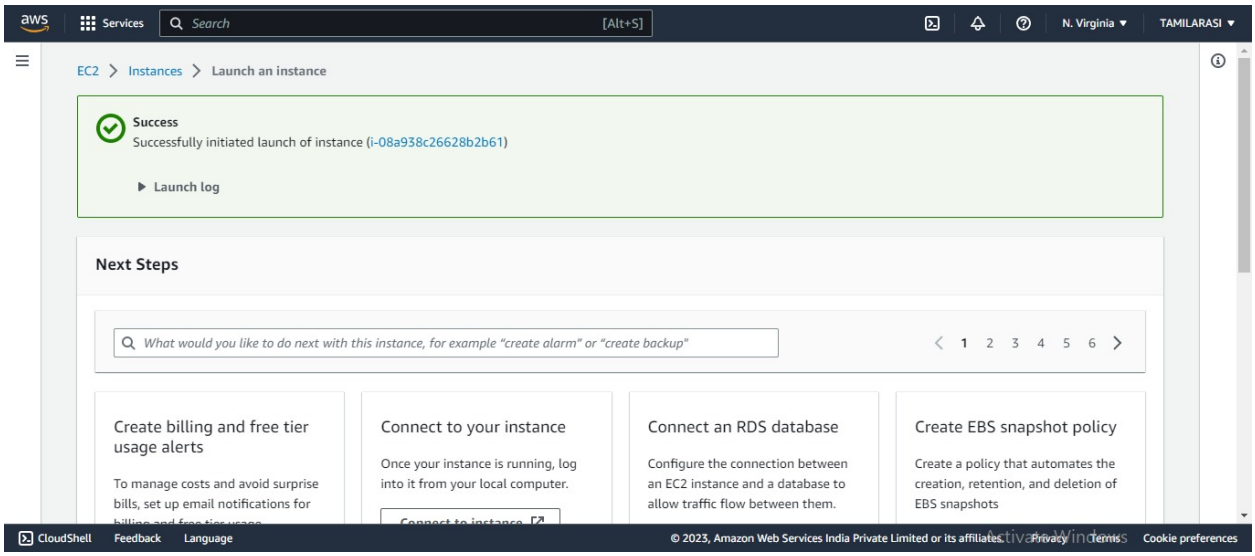


6.Activate MFA for an IAM user and Set some Password Policies such as 1 uppercase, 1 lowercase etc



Day 5:

1.Create a launch template with a custom AMI and t2.micro instance type

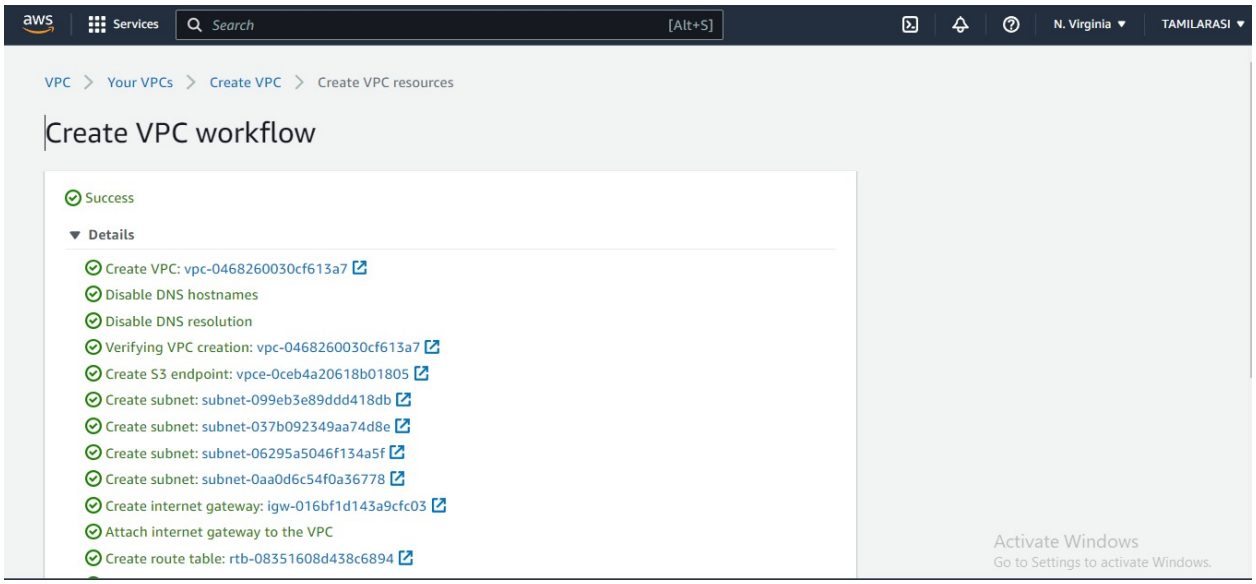


2.Create an autoscaling group with the above-created launch template

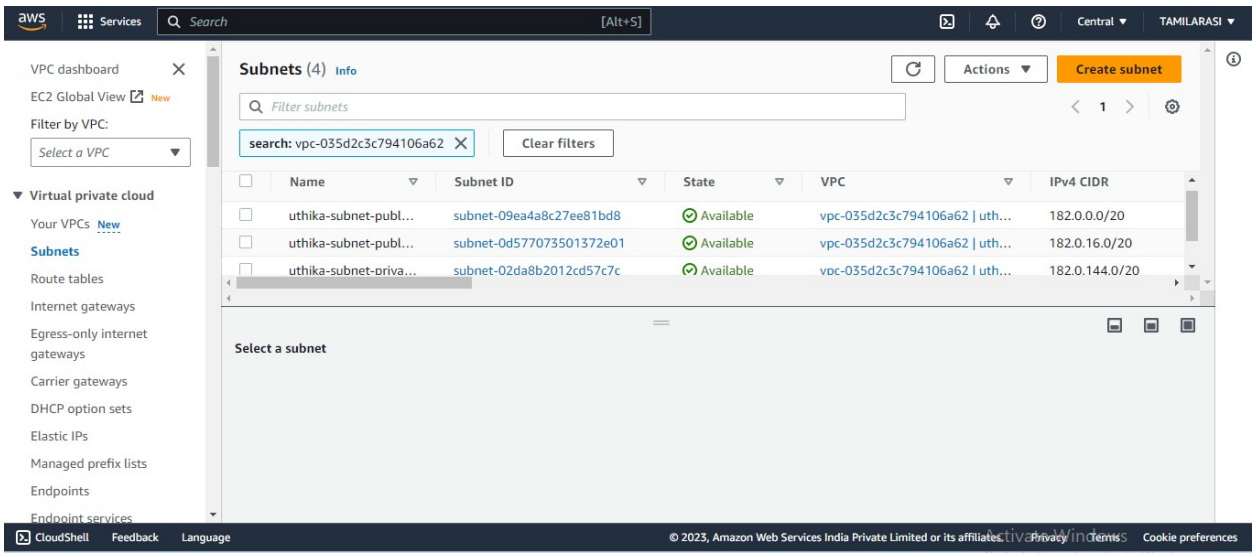
Day:6

Qst:1

Create a vpc with multiple subnets(atleast 1 subnet in each zone)

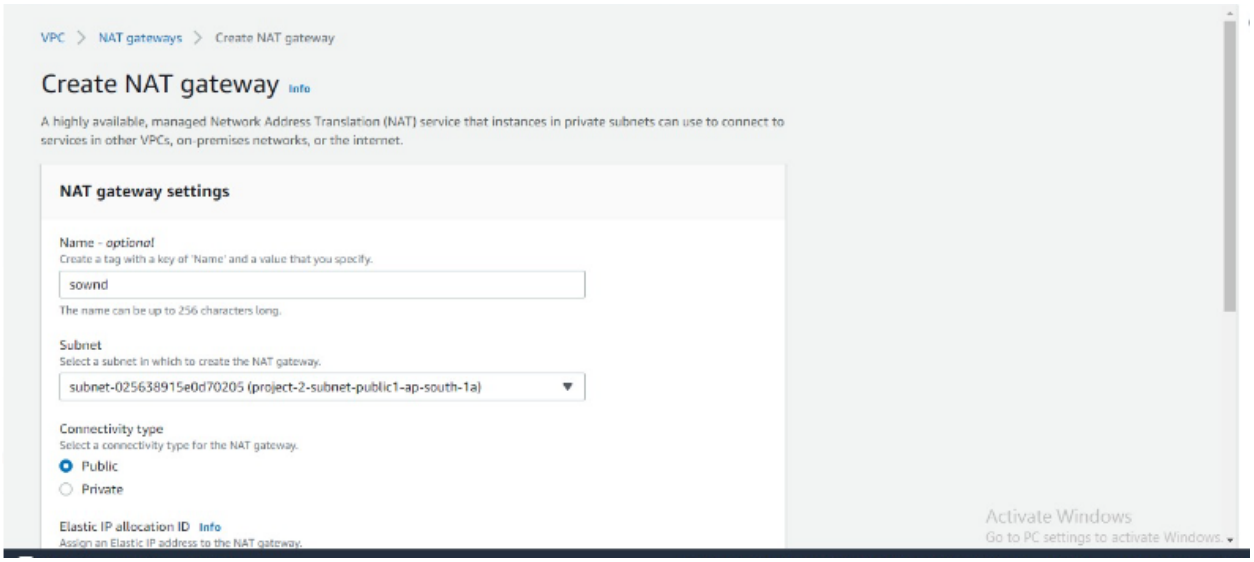


Qst:2
Make 1 public subnet and 2 private subnets in the created VPC



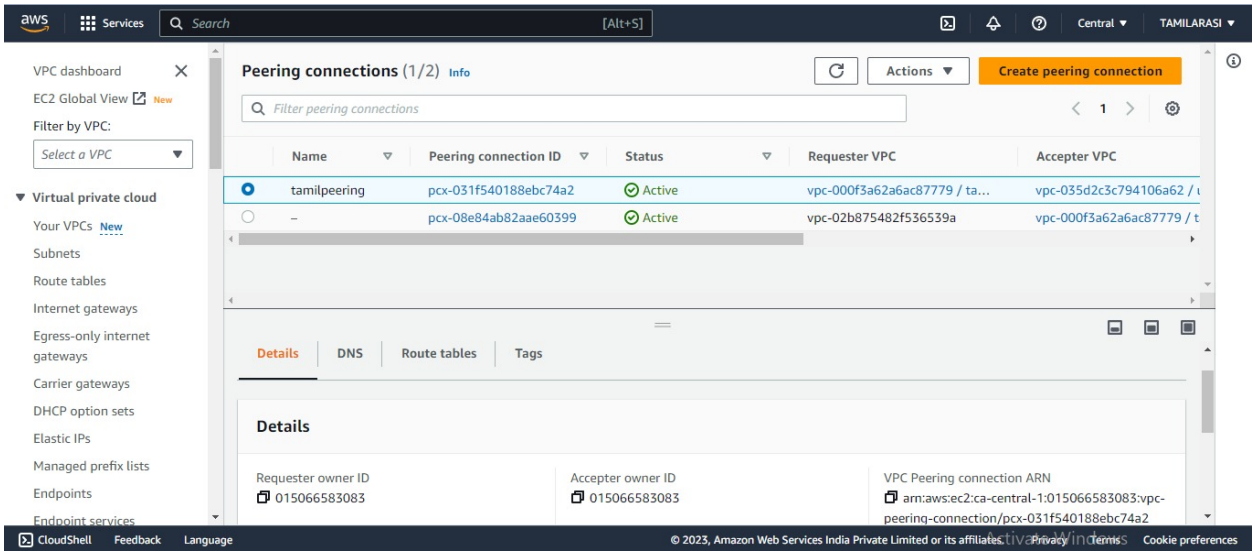
Qst3

Make internet connection using NAT gateway for the 2 private subnets.

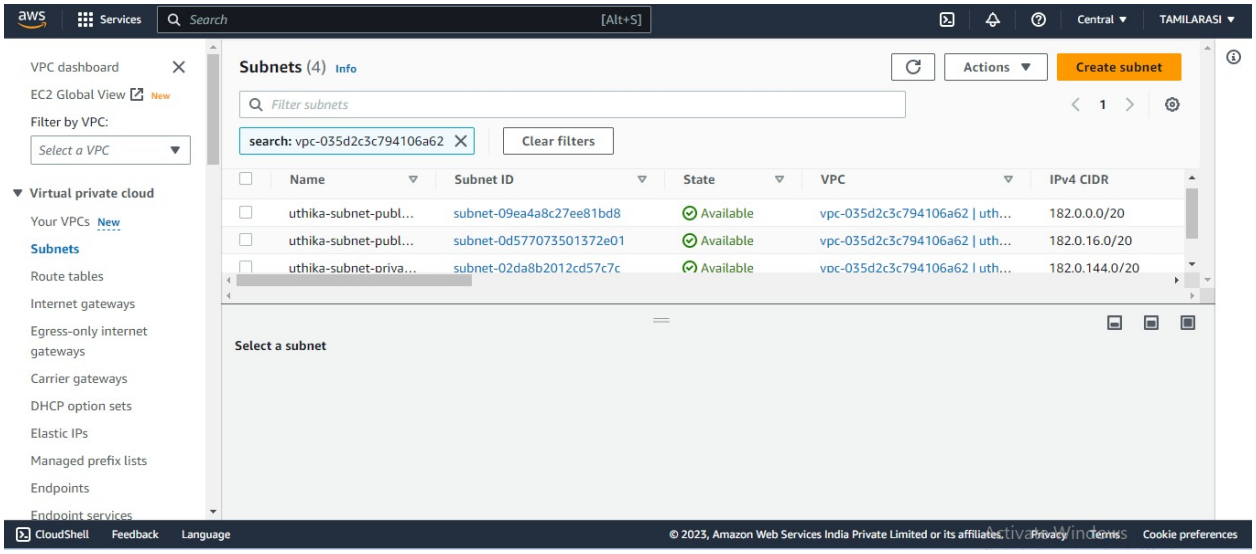


Qst:4

Create a VPC peering connetion between 2 different VPCs from 2 different regions.



Qst5:Create VPC peering connetions for 3 different VPCs from the same region



QSt6

Add security rules in the VPC's NACL which should deny RDP, SSH from the public network

1