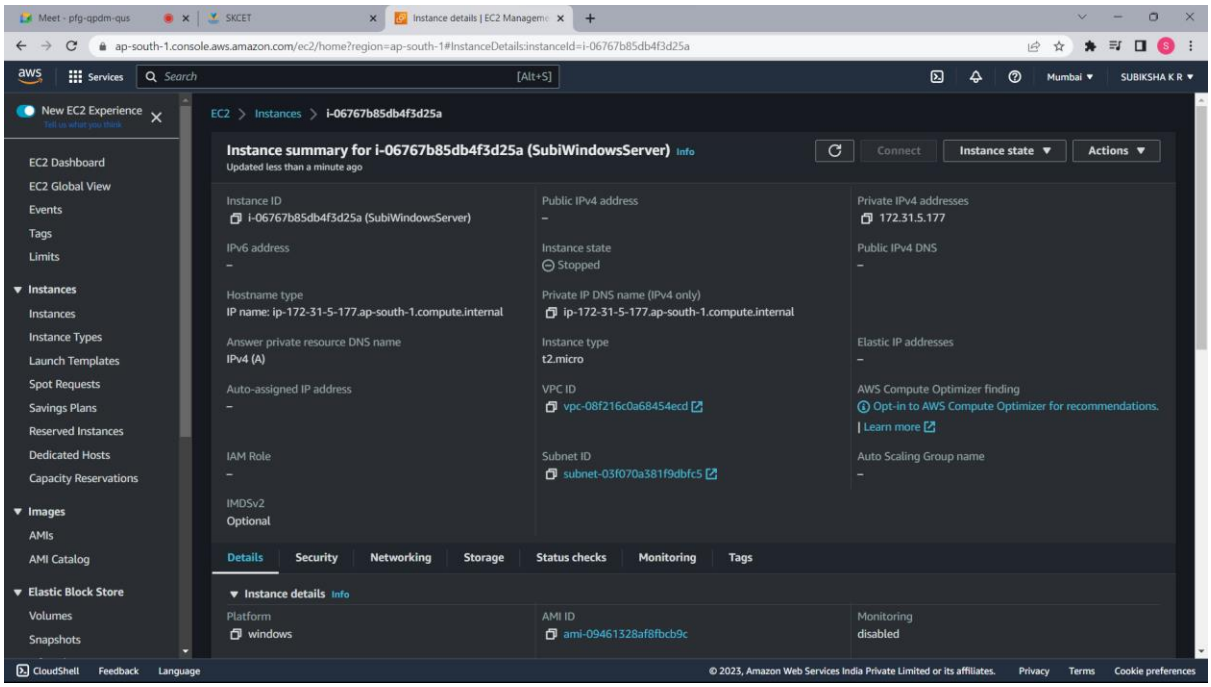
CLOUD COMPUTING

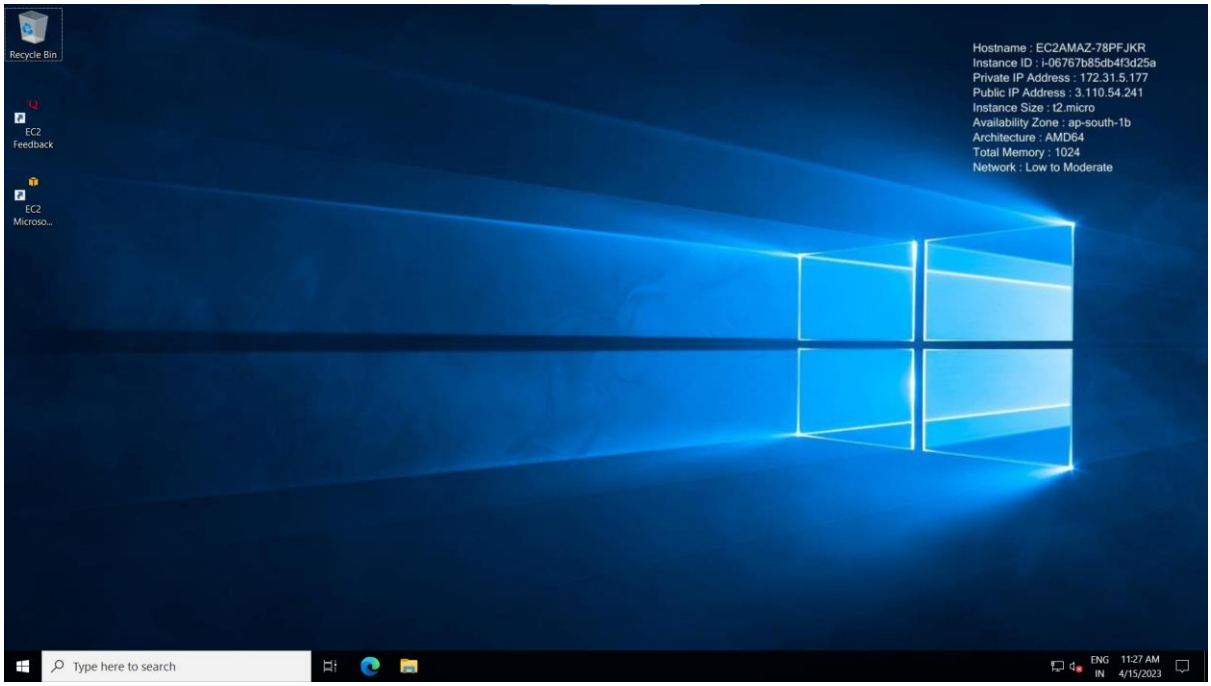
NAME: SUBIKSHA KR

ROLL NO: 727721eucs154

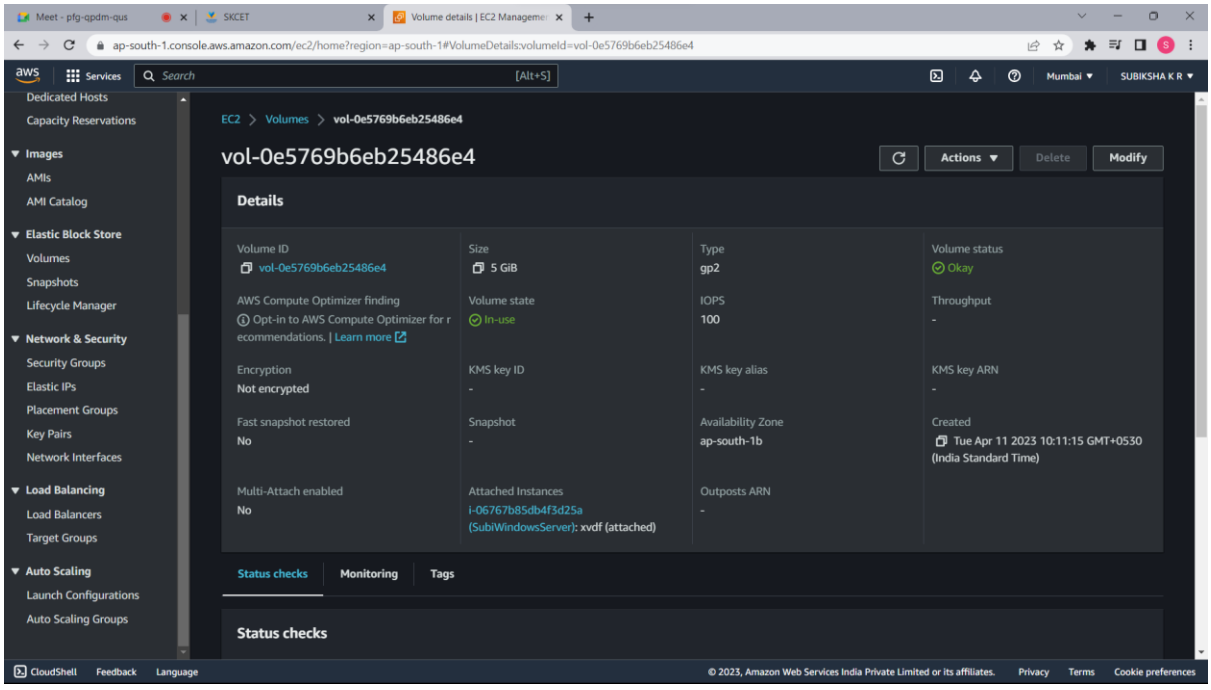
DAY 2

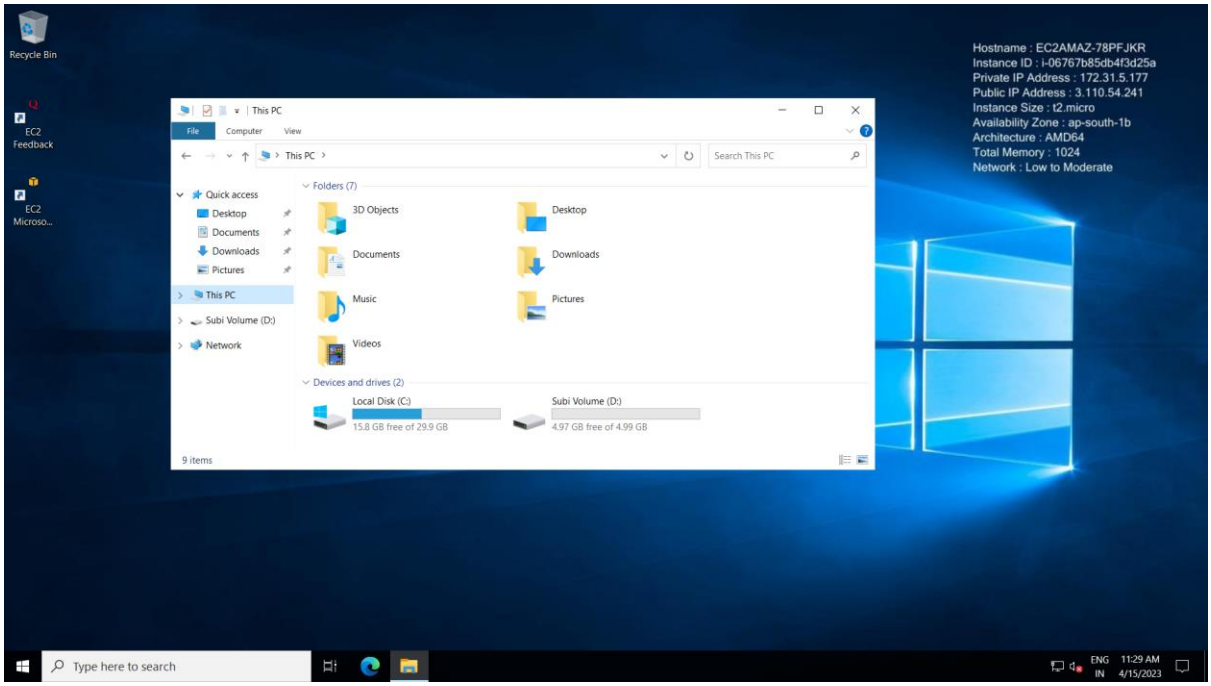
1)Create a Windows EC2 instance with t2.micro Instance and show the remote connection of that EC2 Instance.



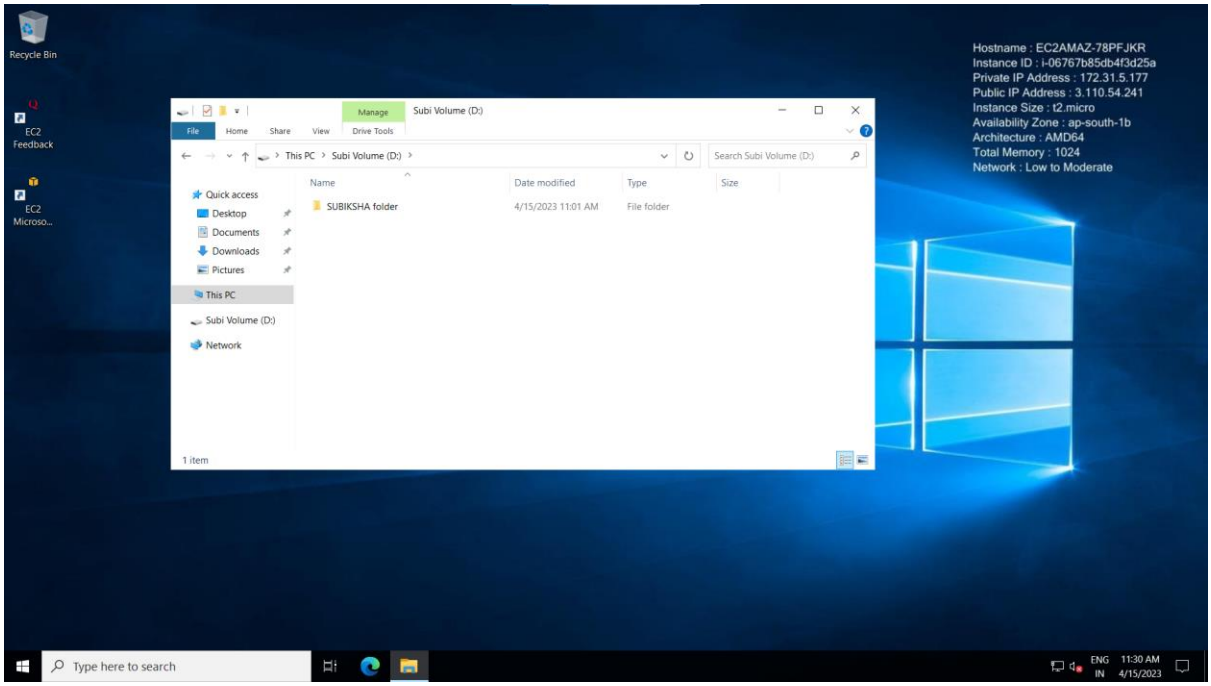


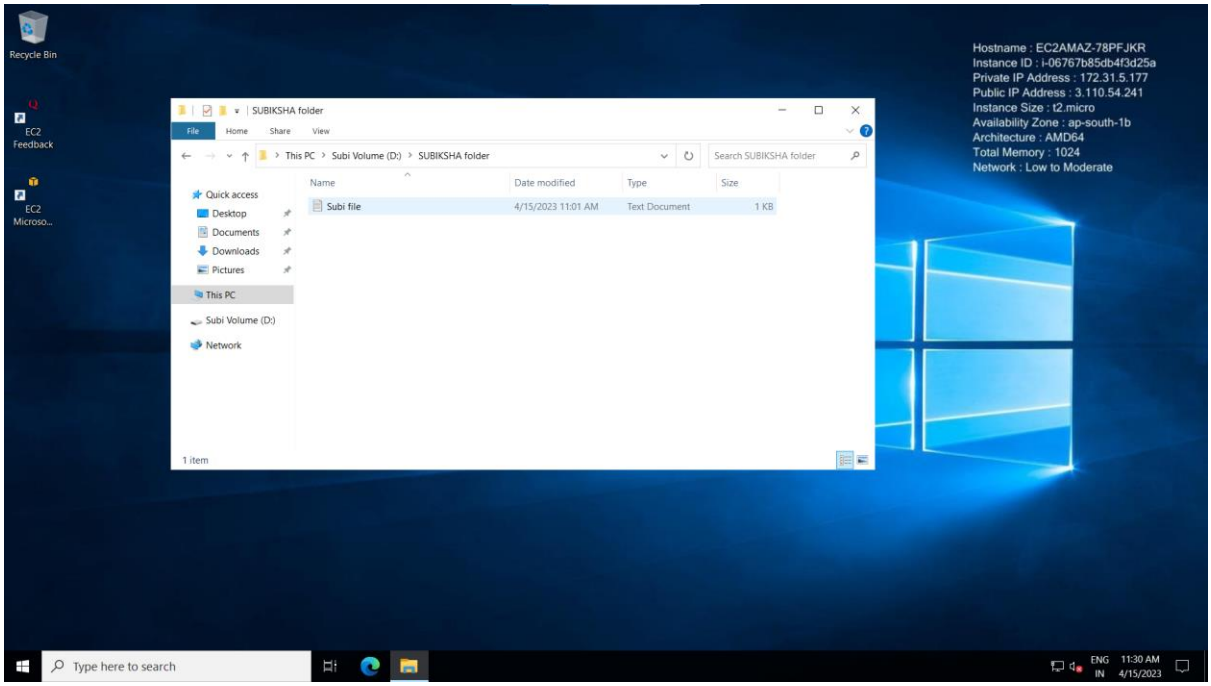
2)Create an EBS volume of 5 GB and attach to a windows EC2 instance and make partition of that EBS volume.

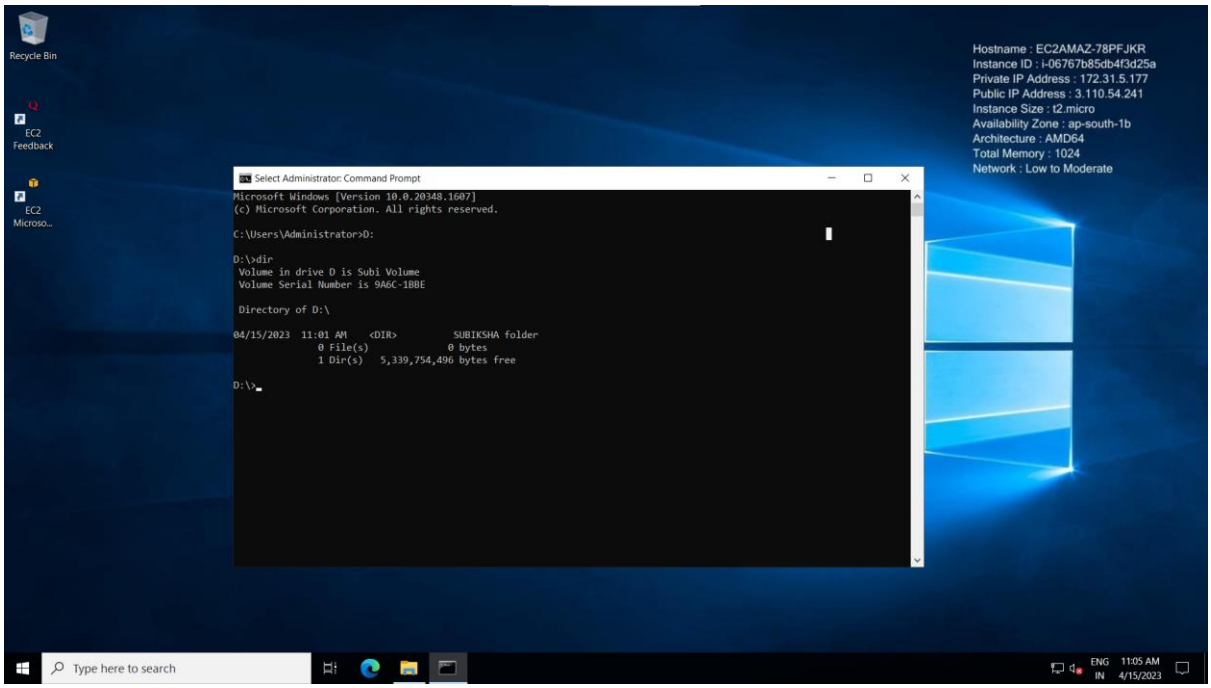




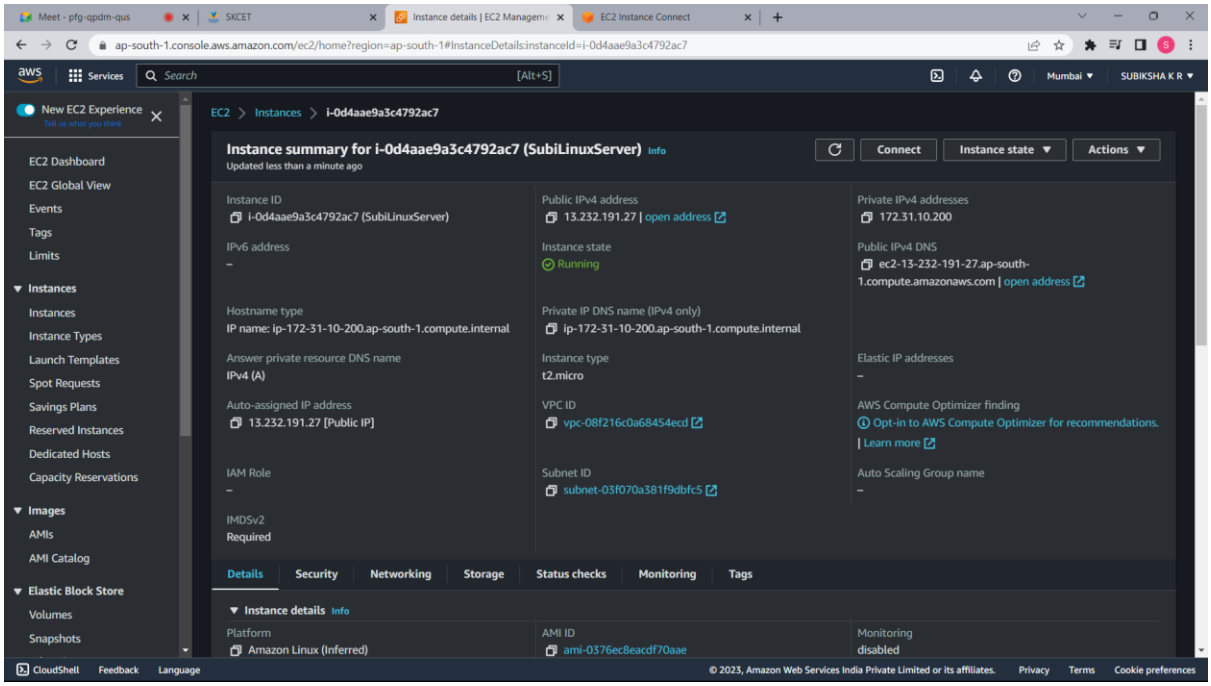
3)Create some files and folders into 5 GB EBS volume of the previous exercise and take a snapshot of that EBS volume.

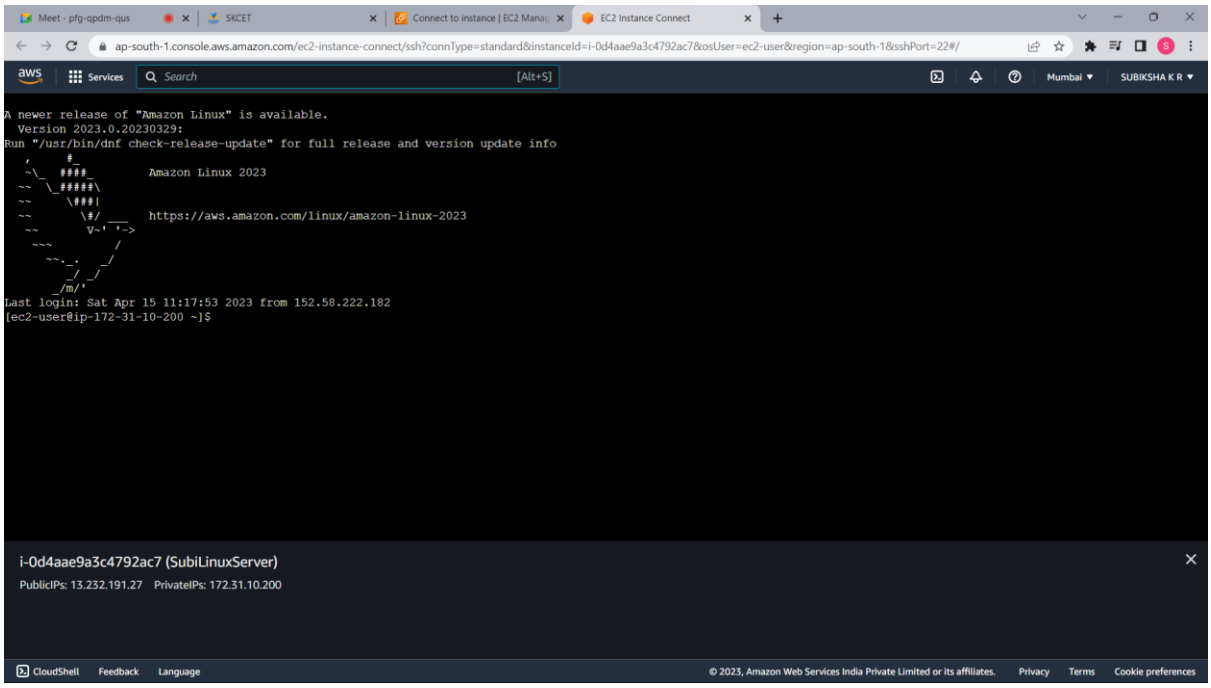




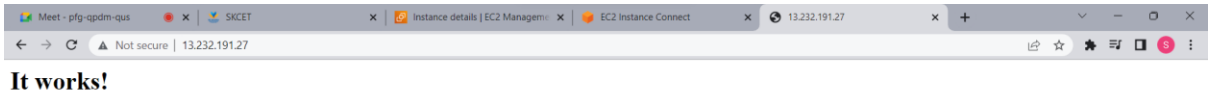


4) Create a Linux EC2 instance with t2.micro Instance and show the remote connection of that EC2 Instance.



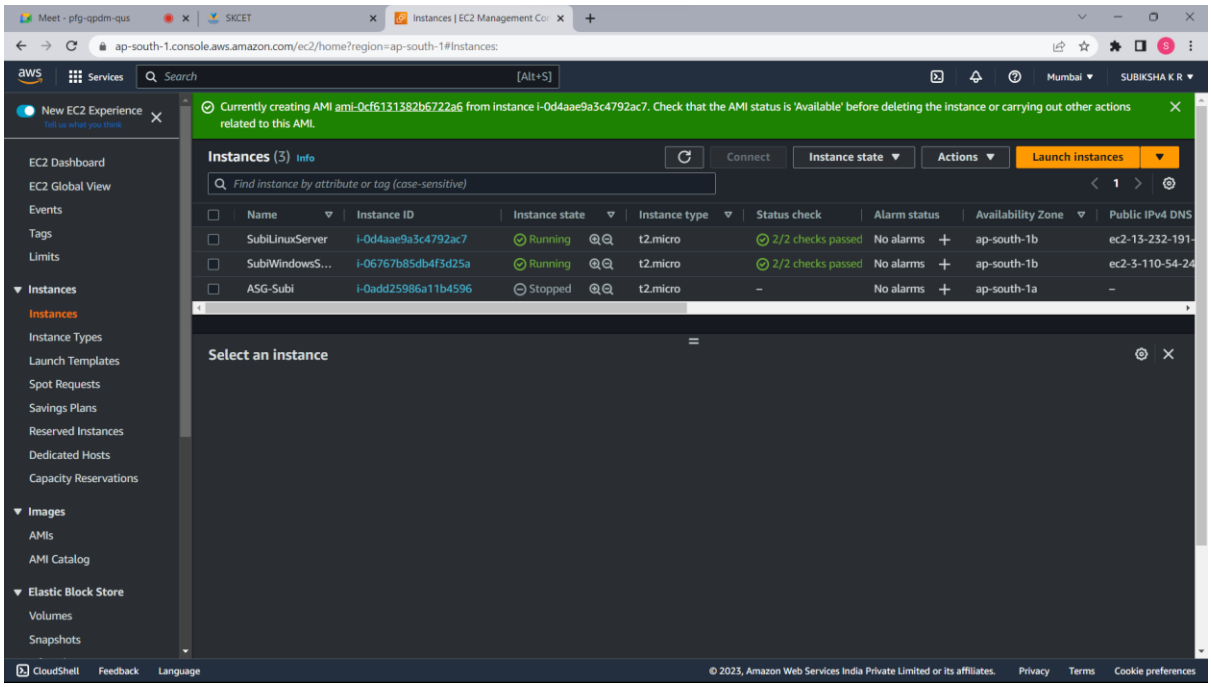


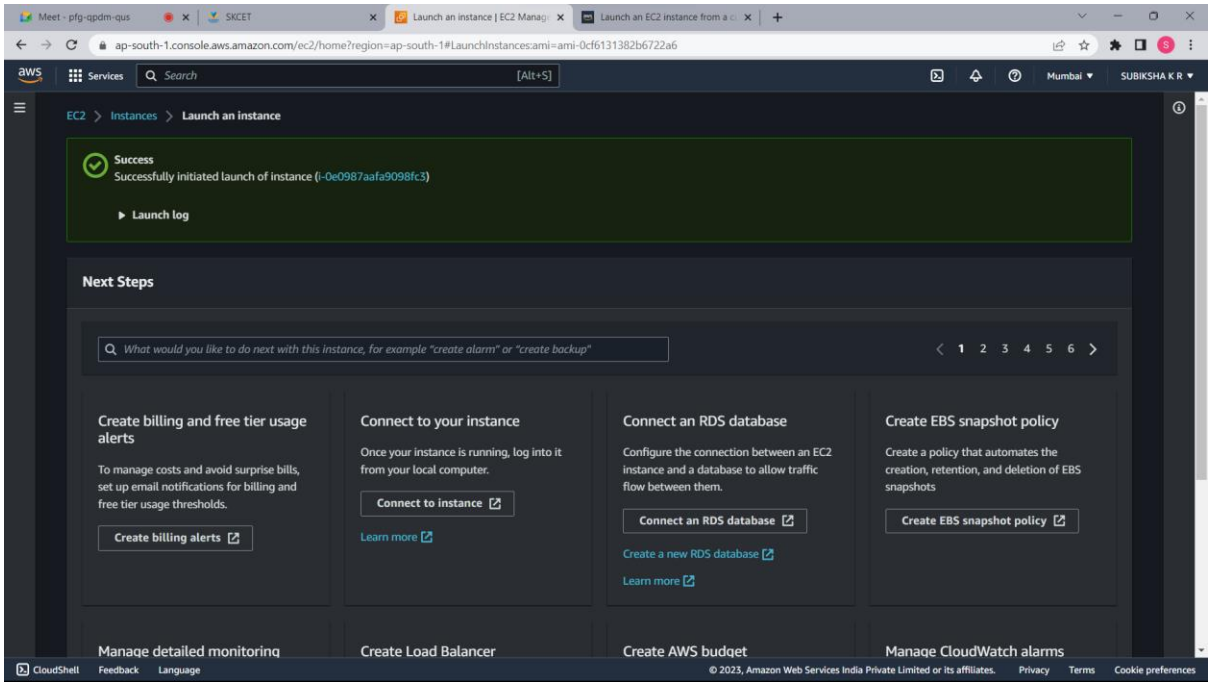
5) Install, Start and Enable the httpd webservice in that Linux EC2 Instance, then host a static website in EC2.



---

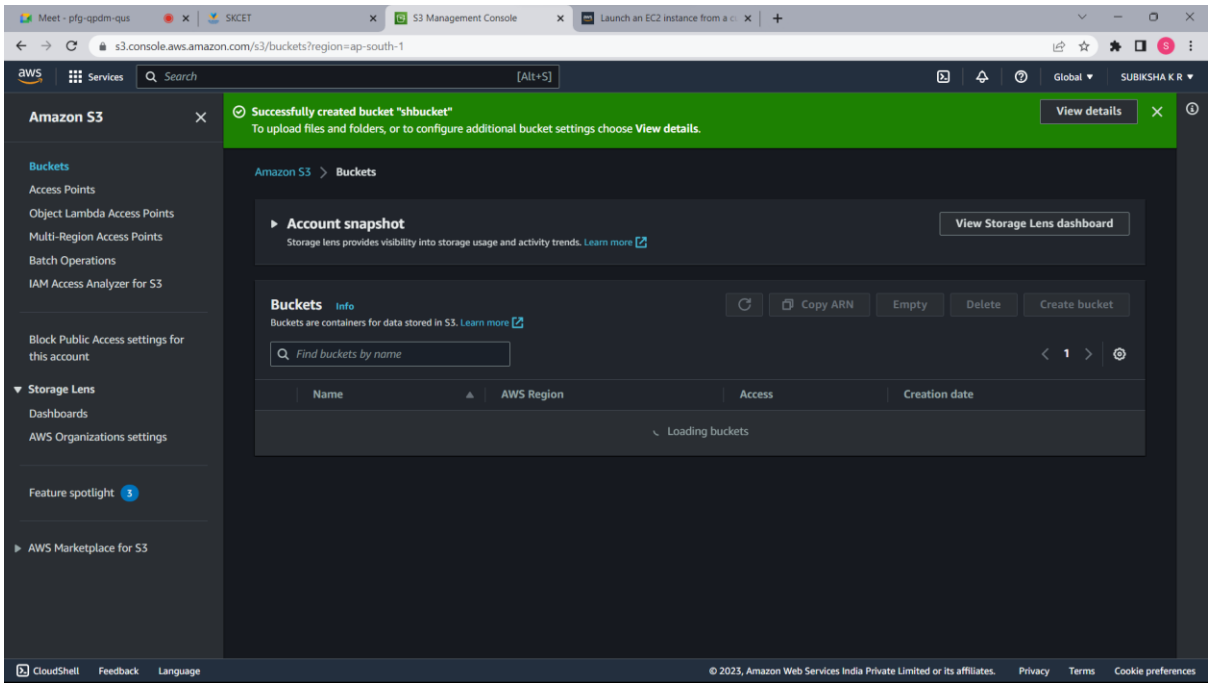
6) Create Image(MyAMI) of the linux Webserver(from the previous exercise) and launch new EC2 instance from the created Image(MyAMI)

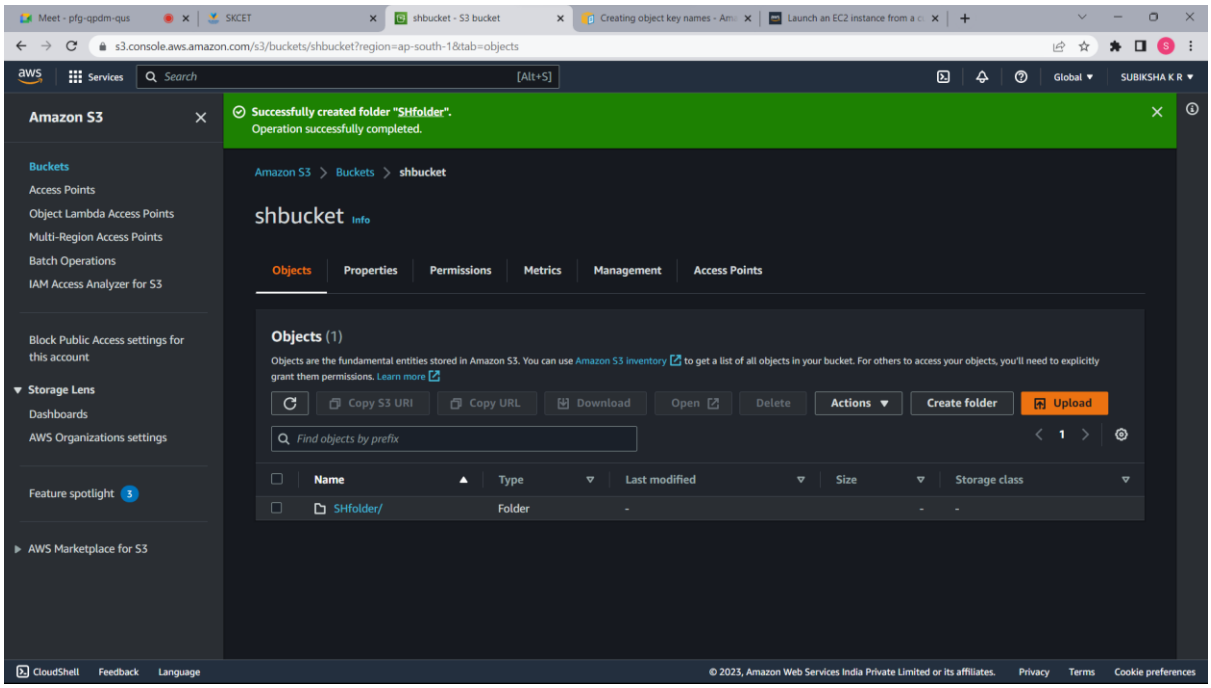


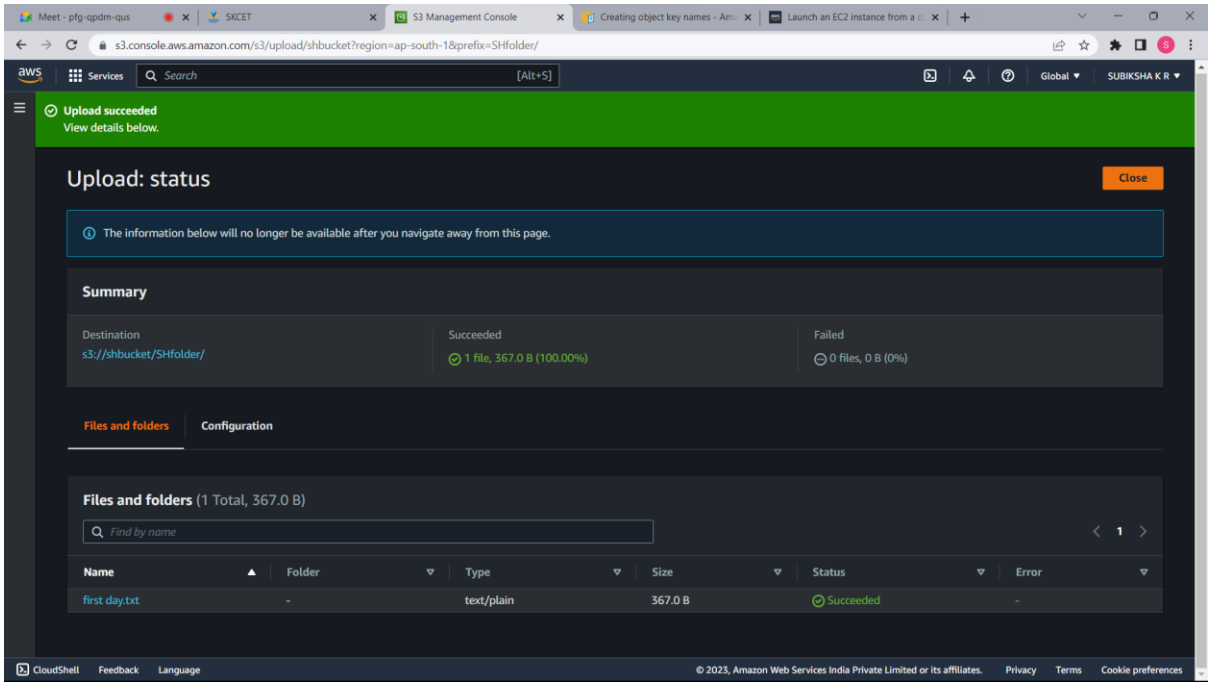

Meet - pfg-qpdm-qus
SKCET
Launch an instance | EC2 Manag
Launch an EC2 instance from a c
ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:ami=ami-0cf6131382b6722a6
Services
Search
[Alt+S]
Mumbai
SUBIKSHA K R
EC2 > Instances > Launch an instance
Success
Successfully initiated launch of instance (i-0e0987aafa9098fc3)
Launch log
Next Steps
What would you like to do next with this instance, for example "create alarm" or "create backup"
1 2 3 4 5 6
Create billing and free tier usage alerts
To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.
Create billing alerts
Connect to your instance
Once your instance is running, log into it from your local computer.
Connect to instance
Learn more
Connect an RDS database
Configure the connection between an EC2 instance and a database to allow traffic flow between them.
Connect an RDS database
Create a new RDS database
Learn more
Create EBS snapshot policy
Create a policy that automates the creation, retention, and deletion of EBS snapshots
Create EBS snapshot policy
Manage detailed monitoring
Create Load Balancer
Create AWS budget
Manage CloudWatch alarms
CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences

DAY 3

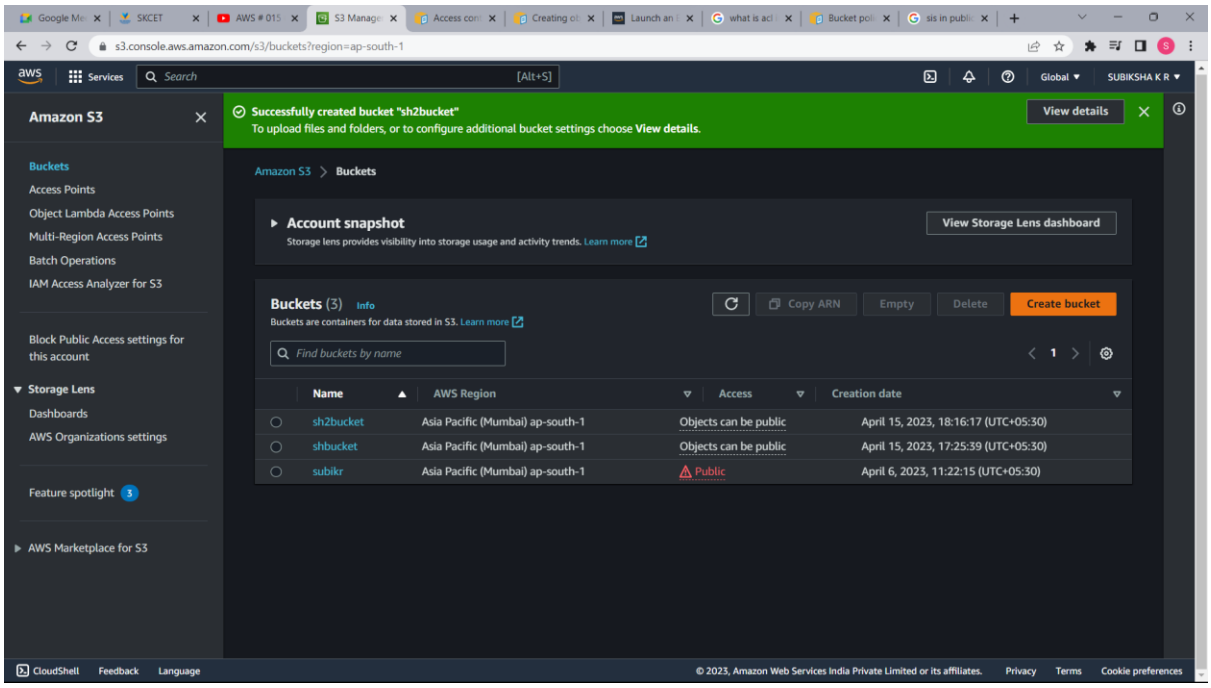
1) Create a S3 Bucket and create a folder in the bucket and upload a file in the folder.

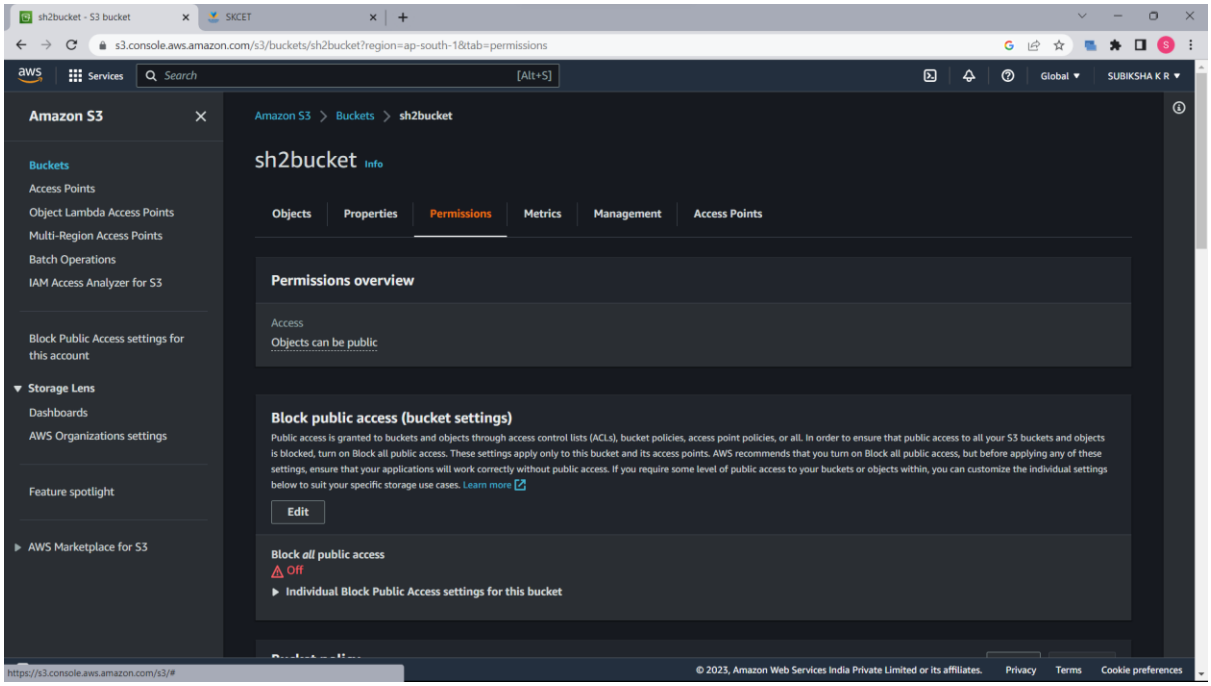


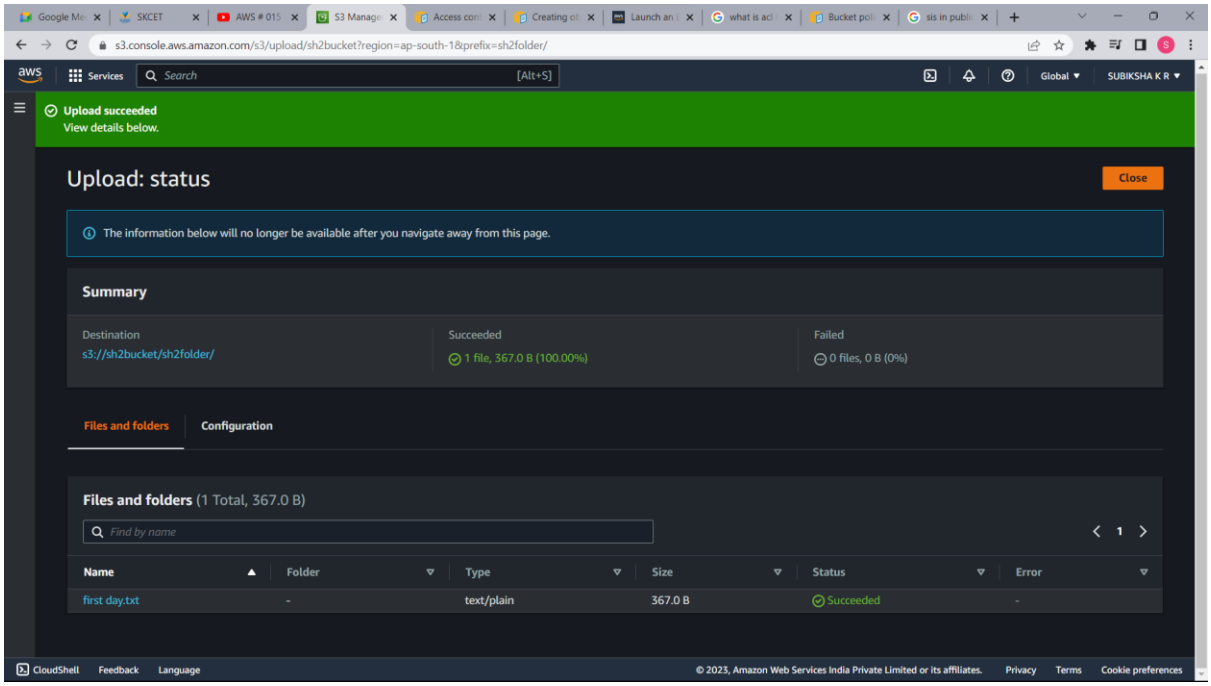


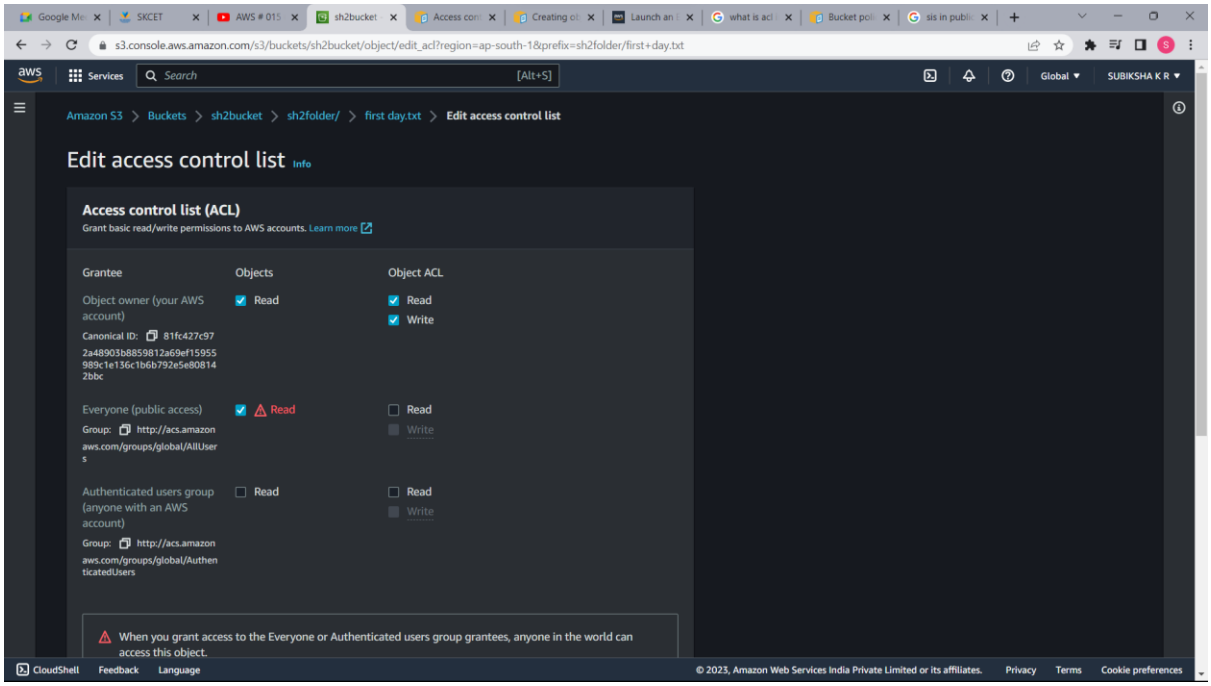


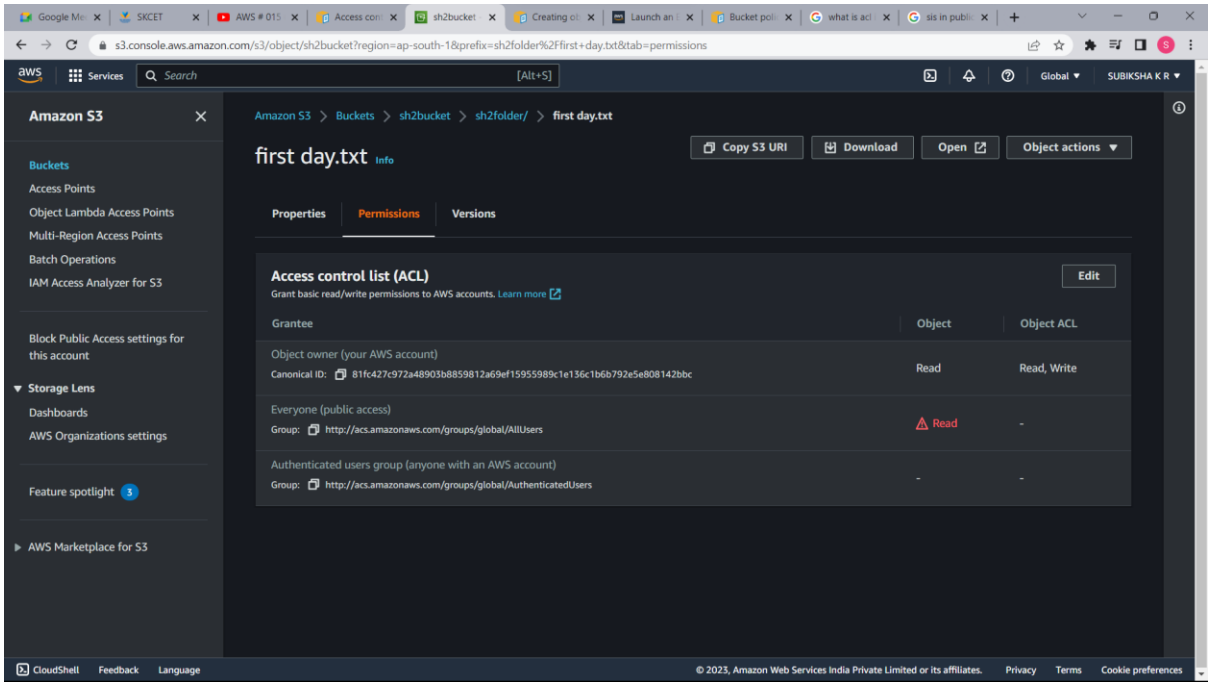
2) Disable "Block Public Access" for the bucket and enable public read access for a file.



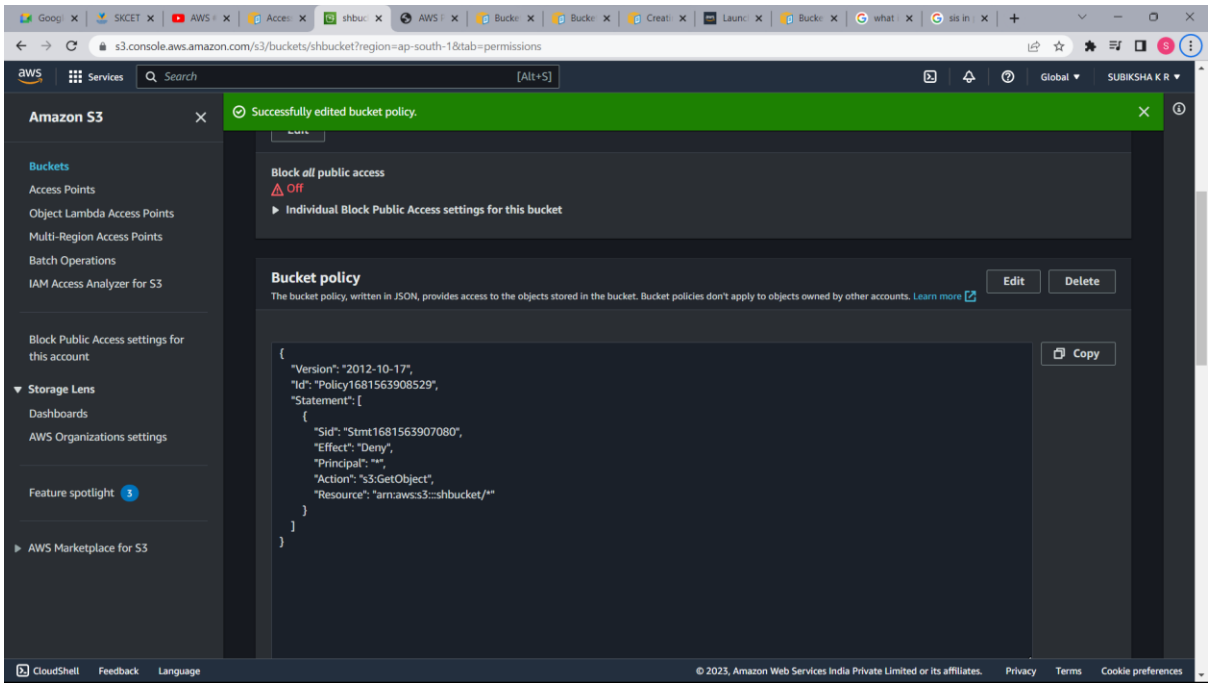

sh2bucket - S3 bucket
SKCET
s3.console.aws.amazon.com/s3/buckets/sh2bucket?region=ap-south-1&tab=permissions
Services
Search
[Alt+S]
Global
SUBIKSHA K R
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
Amazon S3 > Buckets > sh2bucket
sh2bucket Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Permissions overview
Access
Objects can be public
Block public access (bucket settings)
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more
Edit
Block all public access
Off
Individual Block Public Access settings for this bucket
https://s3.console.aws.amazon.com/s3/#
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences


s3.console.aws.amazon.com/s3/upload/sh2bucket?region=ap-south-1&prefix=sh2folder/
Services
Search
[Alt+S]
Global
SUBIKSHA K R
Upload succeeded
View details below.
Upload: status
Close
The information below will no longer be available after you navigate away from this page.
Summary
Destination
s3://sh2bucket/sh2folder/
Succeeded
1 file, 367.0 B (100.00%)
Failed
0 files, 0 B (0%)
Files and folders
Configuration
Files and folders (1 Total, 367.0 B)
Find by name
1
Name
Folder
Type
Size
Status
Error
first day.txt
-
text/plain
367.0 B
Succeeded
-
CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences

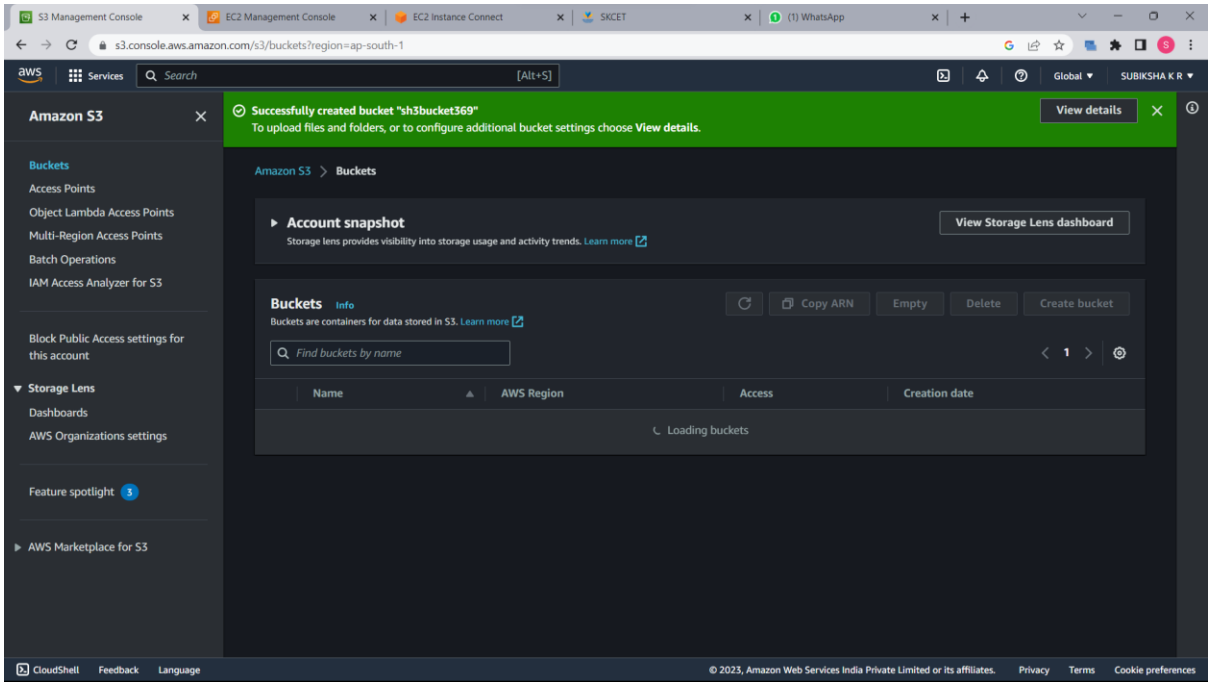

s3.console.aws.amazon.com/s3/buckets/sh2bucket/object/edit_acl?region=ap-south-1&prefix=sh2folder/first+day.txt
Services
Search
[Alt+S]
Global
SUBIKSHA K R
Amazon S3 > Buckets > sh2bucket > sh2folder/ > first day.txt > Edit access control list
Edit access control list Info
Access control list (ACL)
Grant basic read/write permissions to AWS accounts. Learn more
Grantee
Objects
Object ACL
Object owner (your AWS account)
Canonical ID: 81fc427c97 2a48903b8859812a69ef15955 989c1e136c1b6b792e5e80814 2bbc
Read
Read
Write
Everyone (public access)
Group: http://acs.amazon aws.com/groups/global/AllUser s
Read
Read
Write
Authenticated users group (anyone with an AWS account)
Group: http://acs.amazon aws.com/groups/global/Authen ticatedUsers
Read
Read
Write
When you grant access to the Everyone or Authenticated users group grantees, anyone in the world can access this object.
CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences

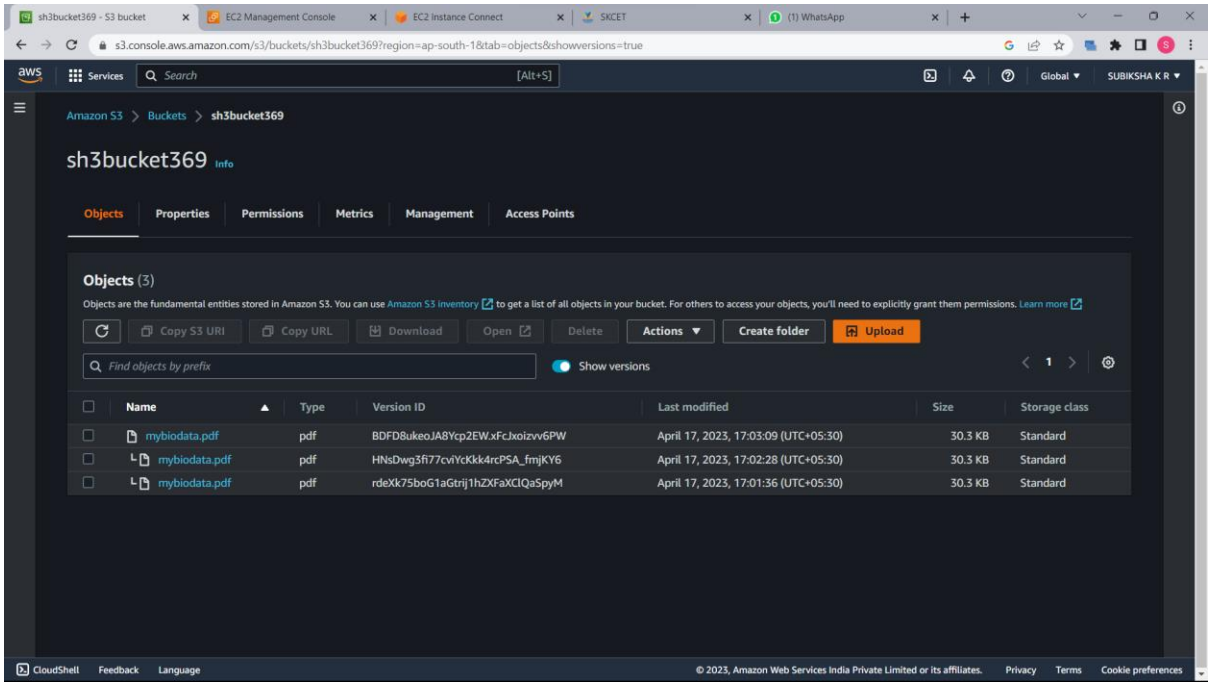

s3.console.aws.amazon.com/s3/object/sh2bucket?region=ap-south-1&prefix=sh2folder%2Ffirst+day.txt&tab=permissions
Services
Search
[Alt+S]
Global
SUBIKSHA K R
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight 3
AWS Marketplace for S3
Amazon S3 > Buckets > sh2bucket > sh2folder/ > first day.txt
first day.txt Info
Copy S3 URI
Download
Open
Object actions
Properties
Permissions
Versions
Access control list (ACL)
Grant basic read/write permissions to AWS accounts. Learn more
Edit
Grantee
Object
Object ACL
Object owner (your AWS account)
Canonical ID: 81fc427c972a48903b8859812a69ef15955989c1e136c1b6b792e5e808142bbc
Read
Read, Write
Everyone (public access)
Group: http://acs.amazonaws.com/groups/global/AllUsers
Read
-
Authenticated users group (anyone with an AWS account)
Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers
-
-
CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences

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

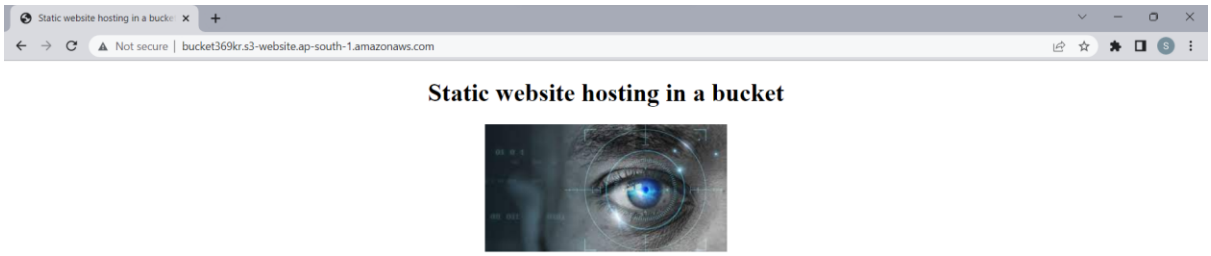


4) Enable versioning objects for a bucket and upload objects with multiple versions of it.

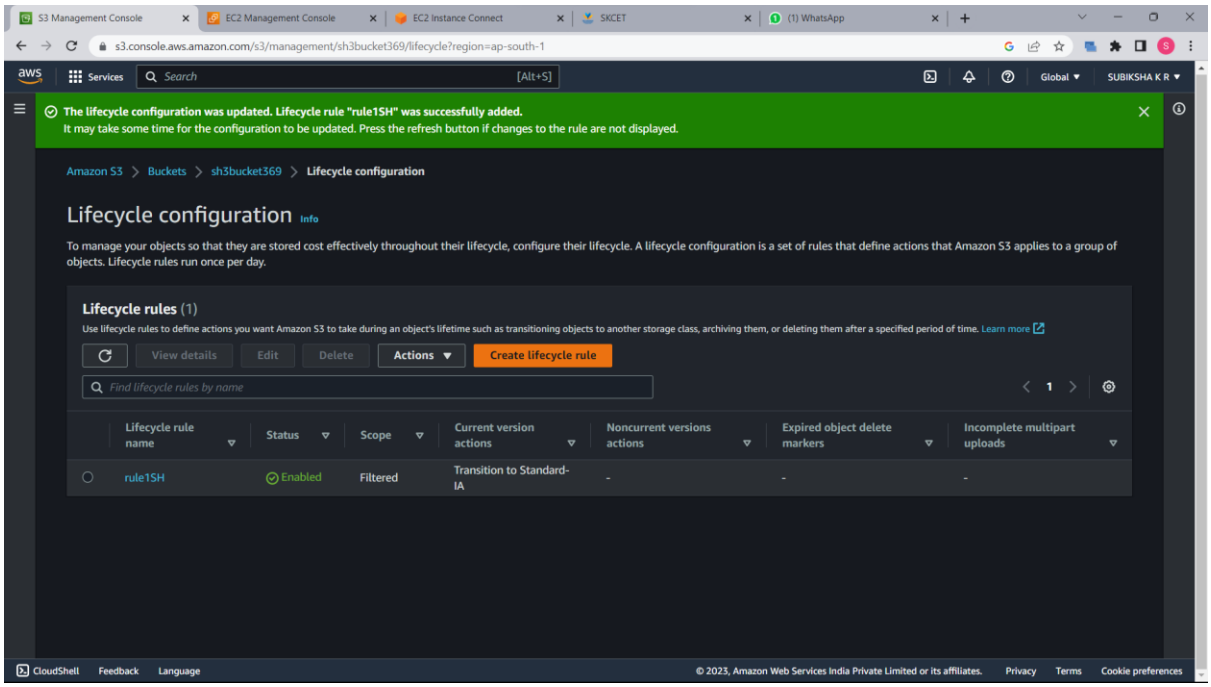




5) Host a static webpage in a bucket itself by using static website hosting feature of it.

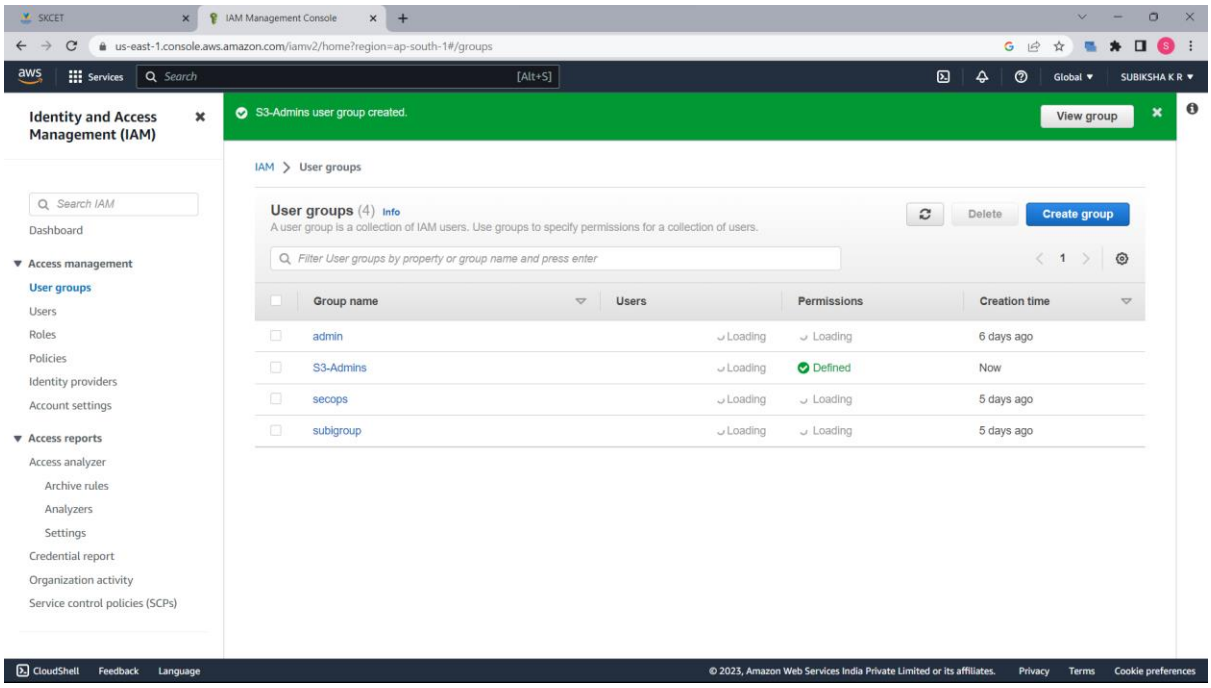


6) Enable a lifecycle management rule between various storage classes for a S3 bucket.

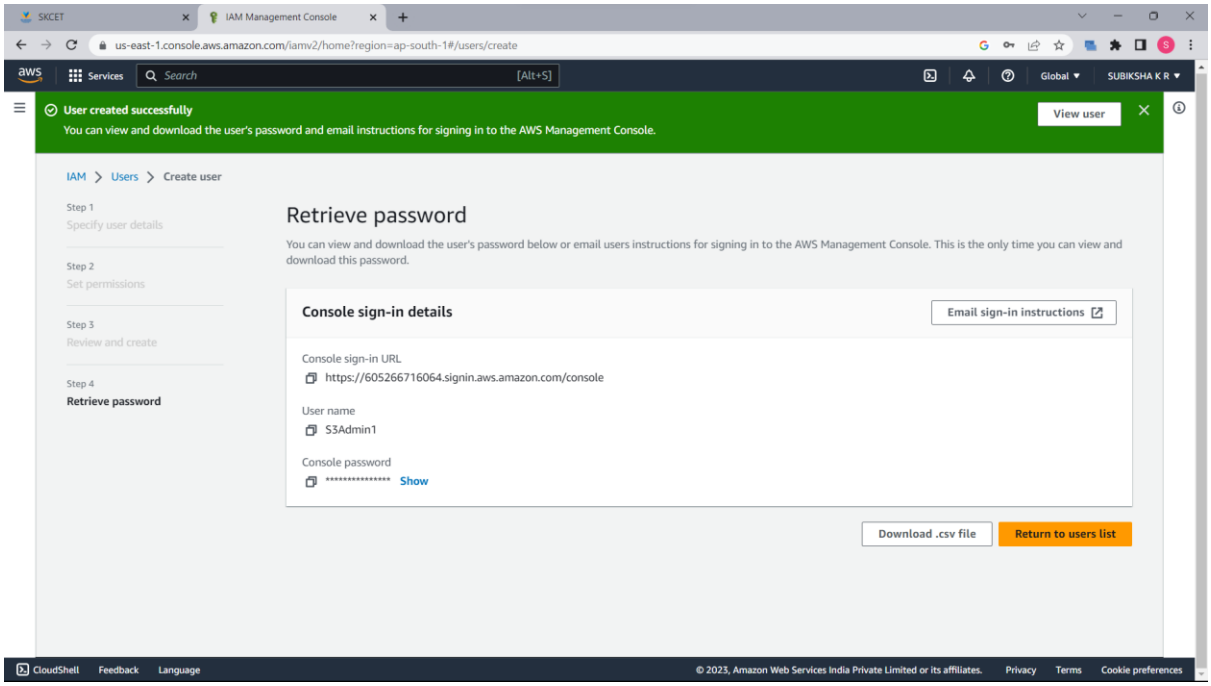


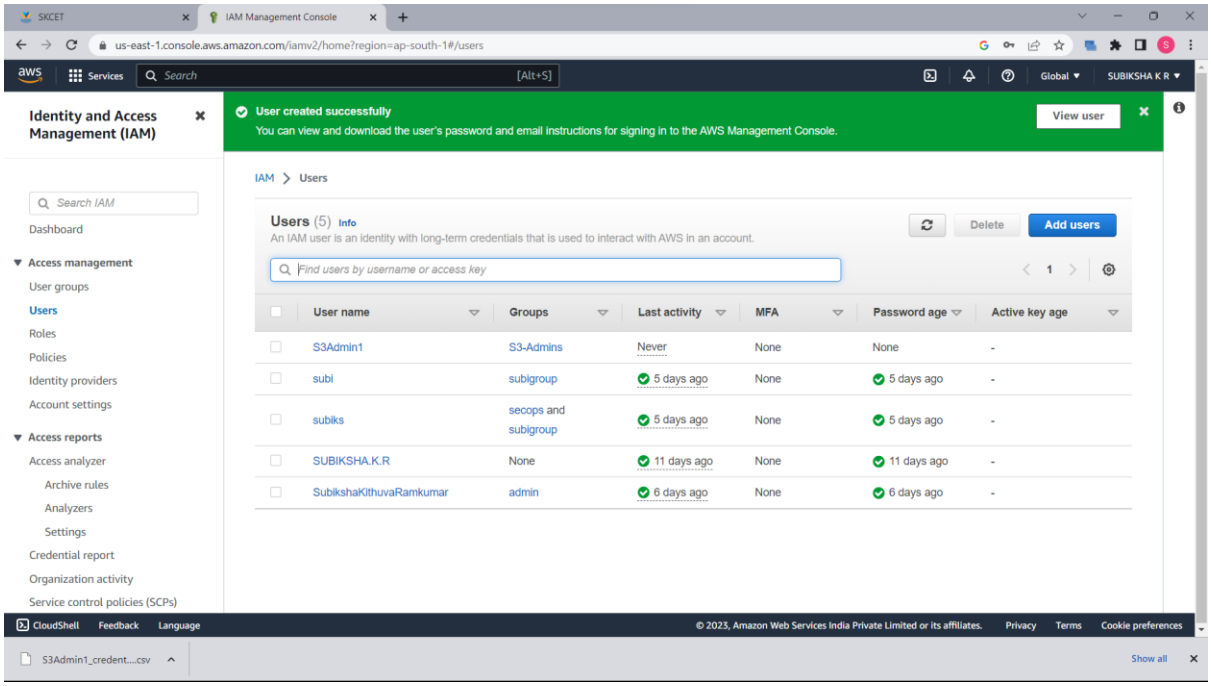
DAY 4

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

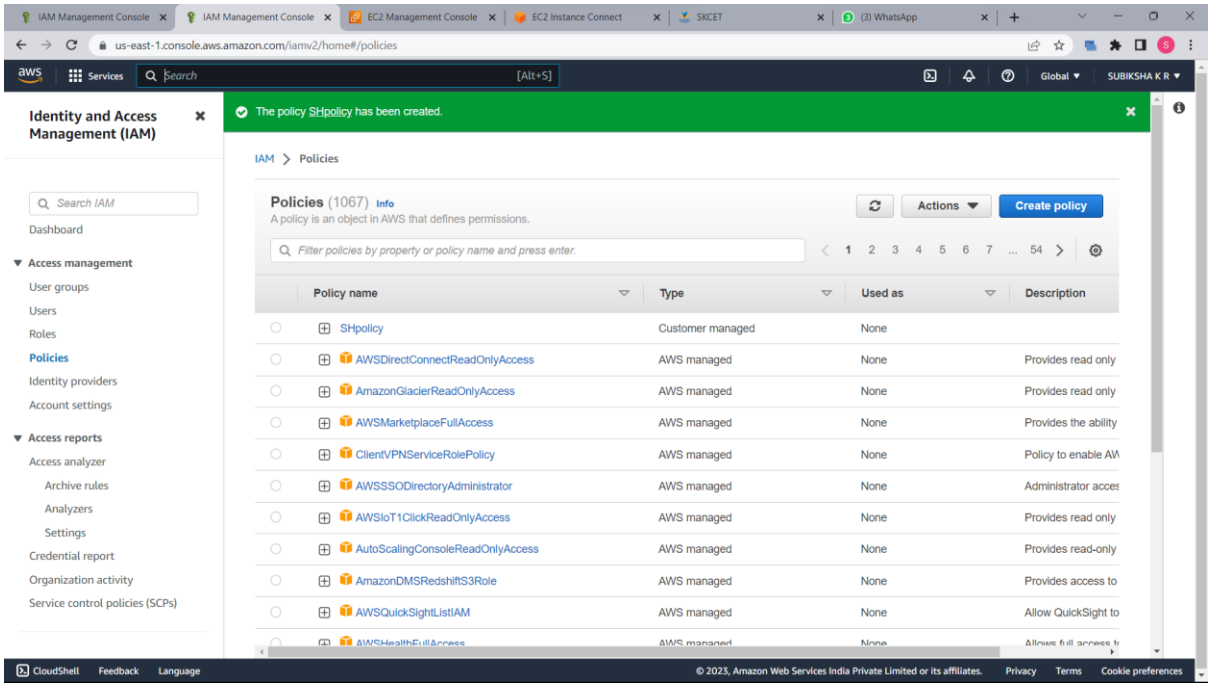


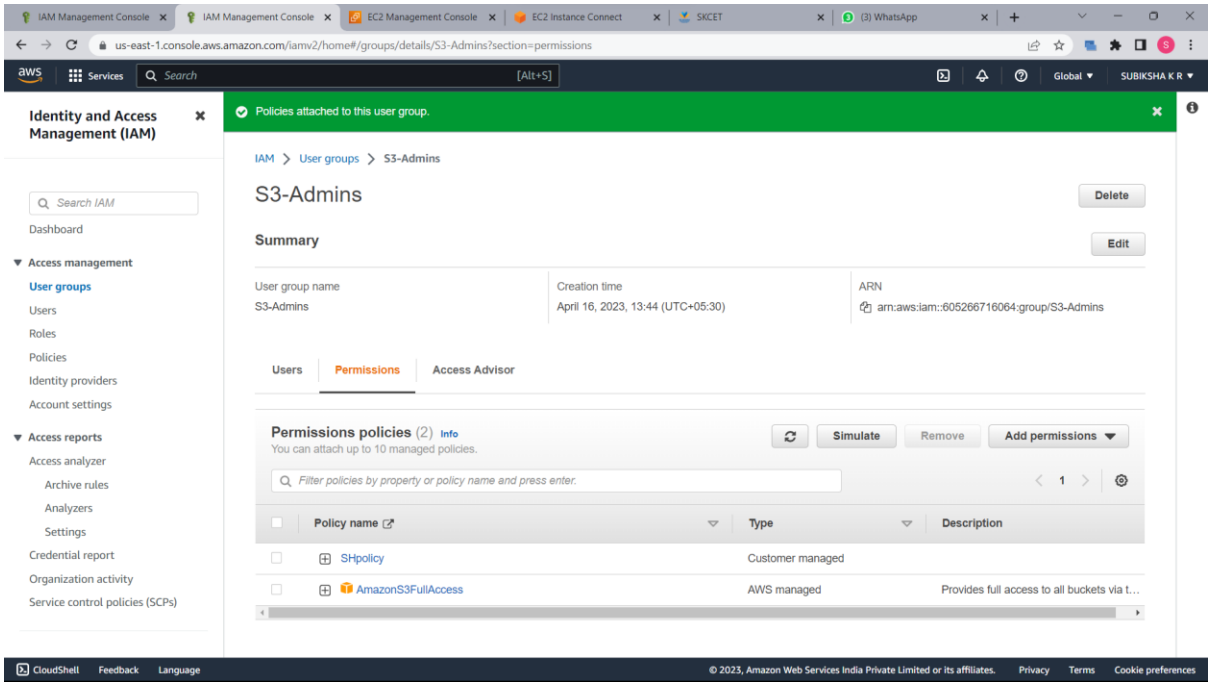
2) Create an IAM user called as ‘S3Admin1’ and add it to the ‘S3-Admins’ group.



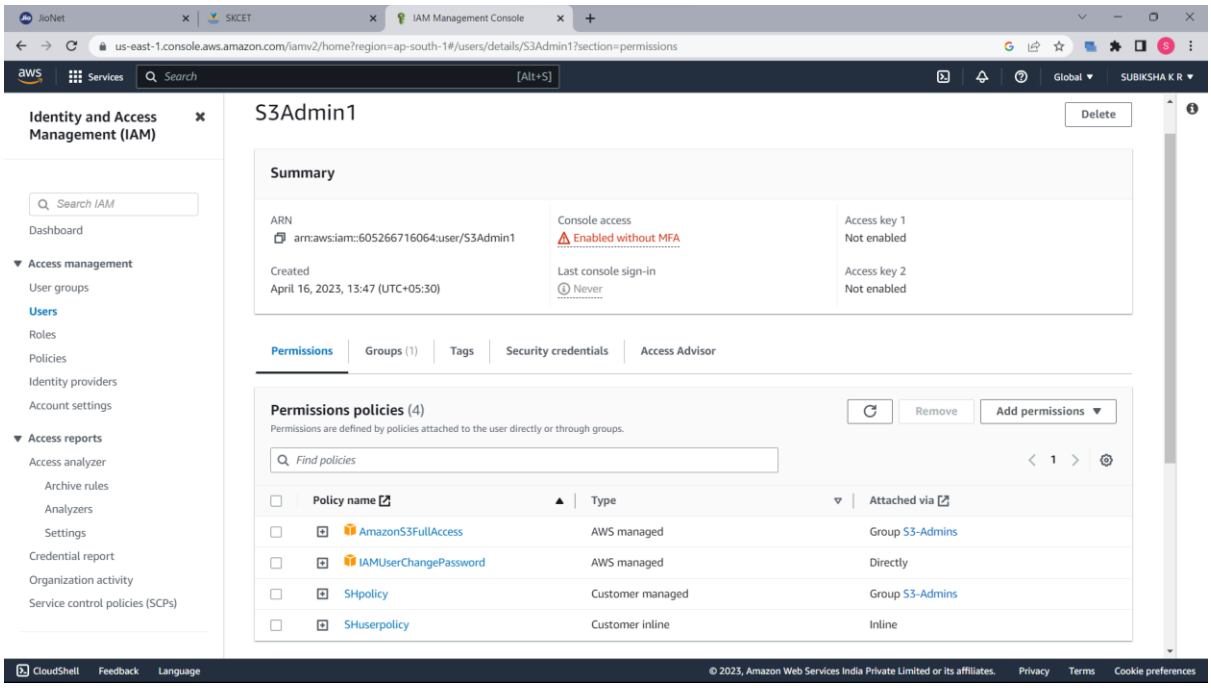


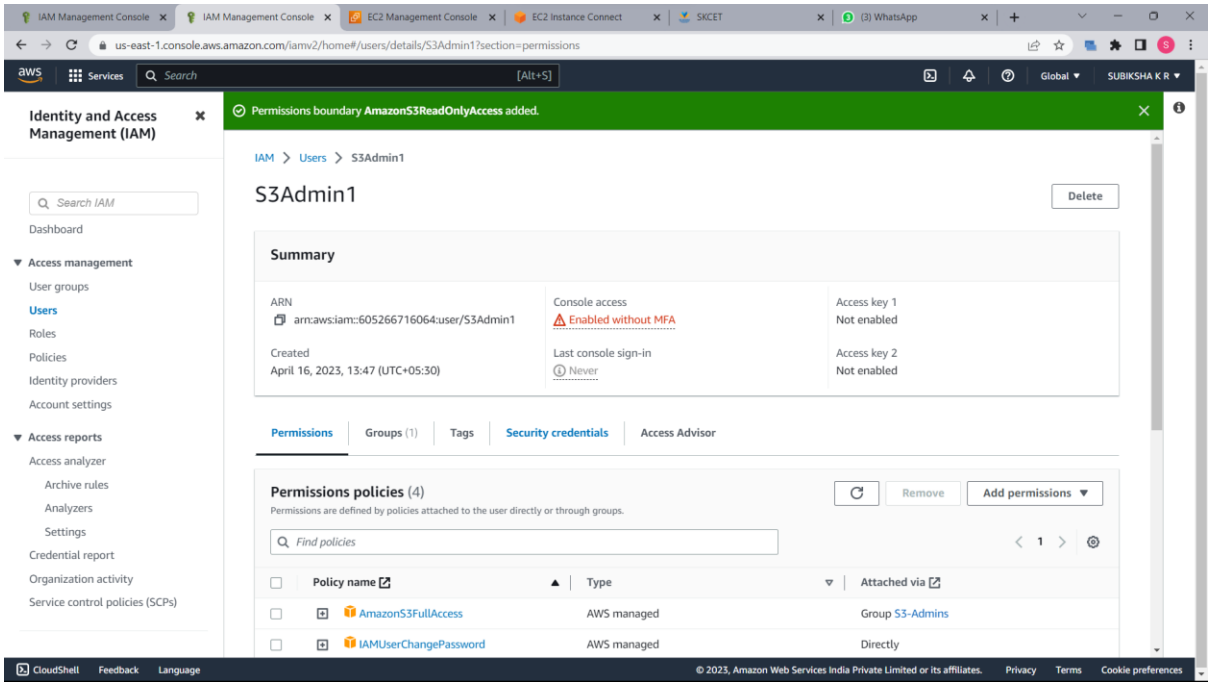
3)Attach an IAM custom policy to the 'S3-Admins' group which should deny to delete objects.



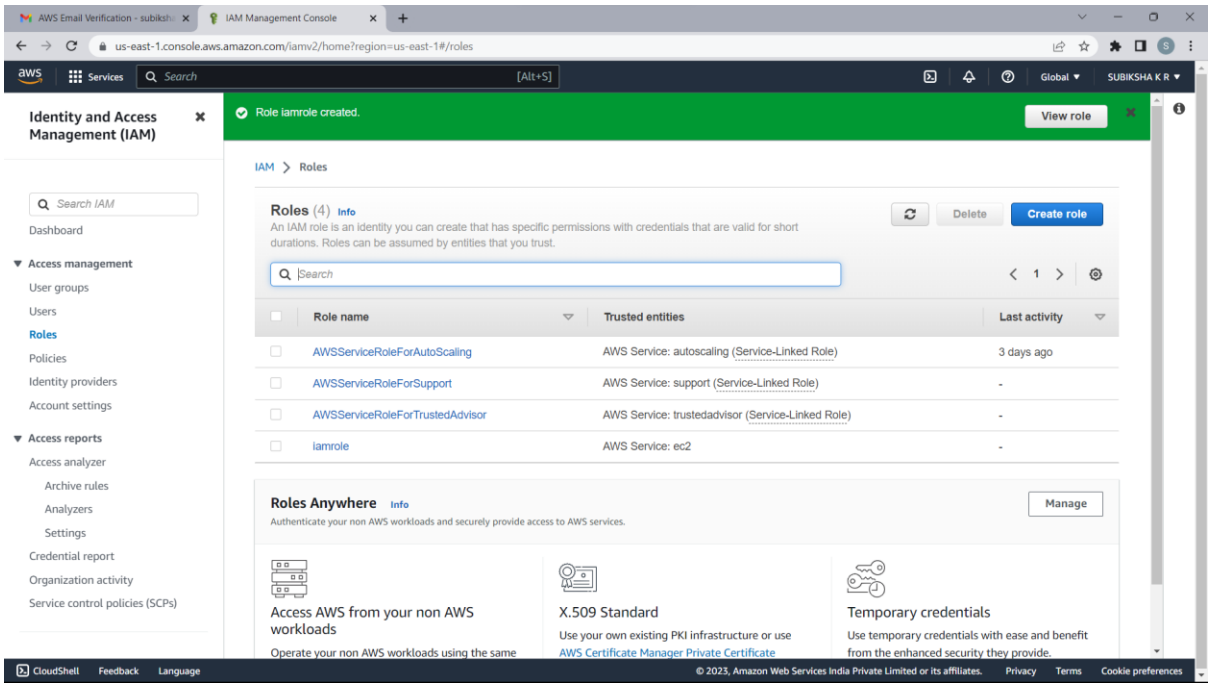


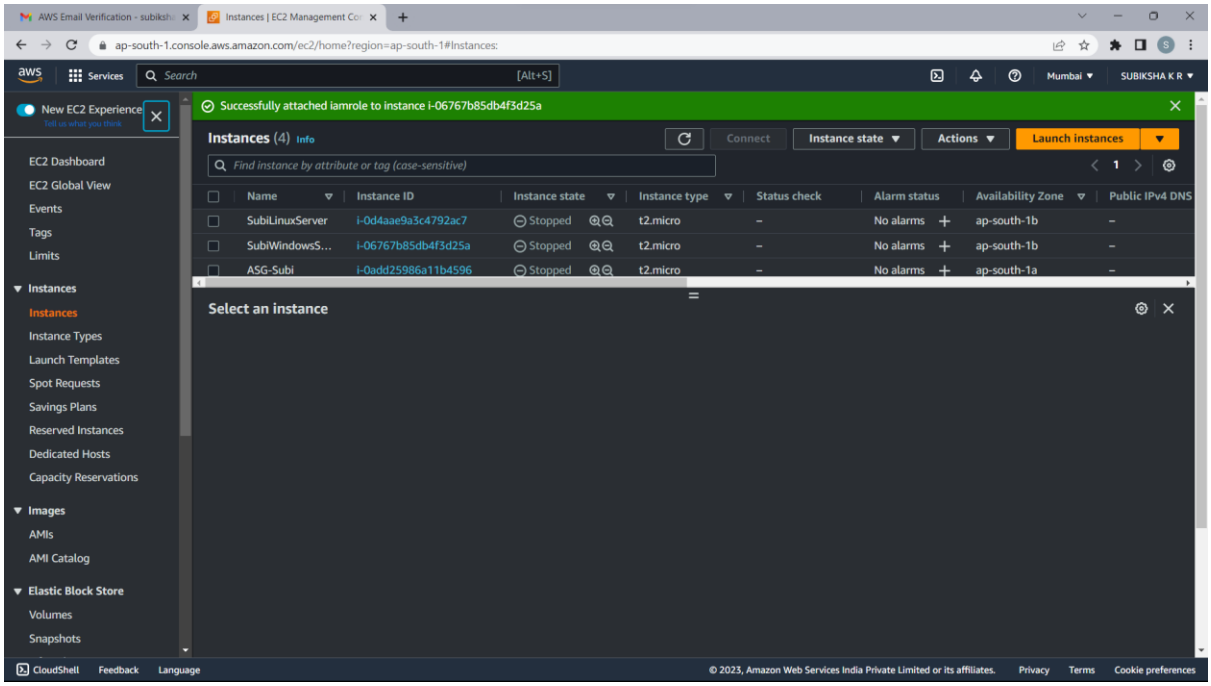
4) Create an Inline policy for an IAM user and set some permission boundary for that user.



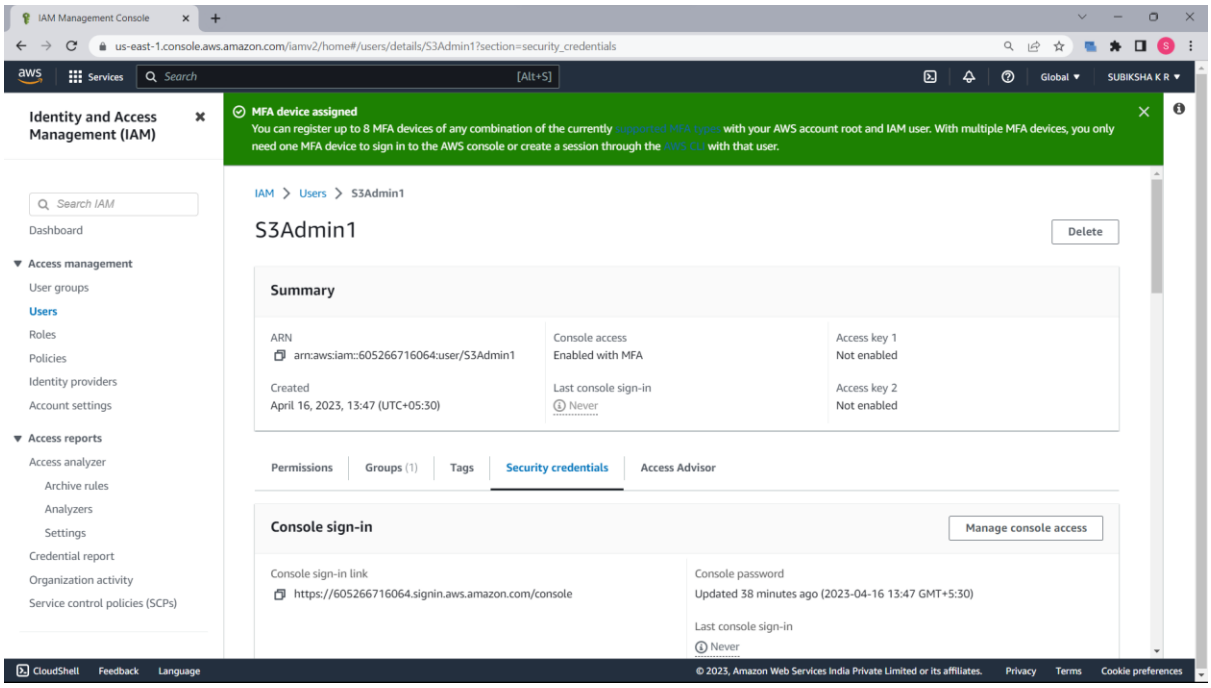


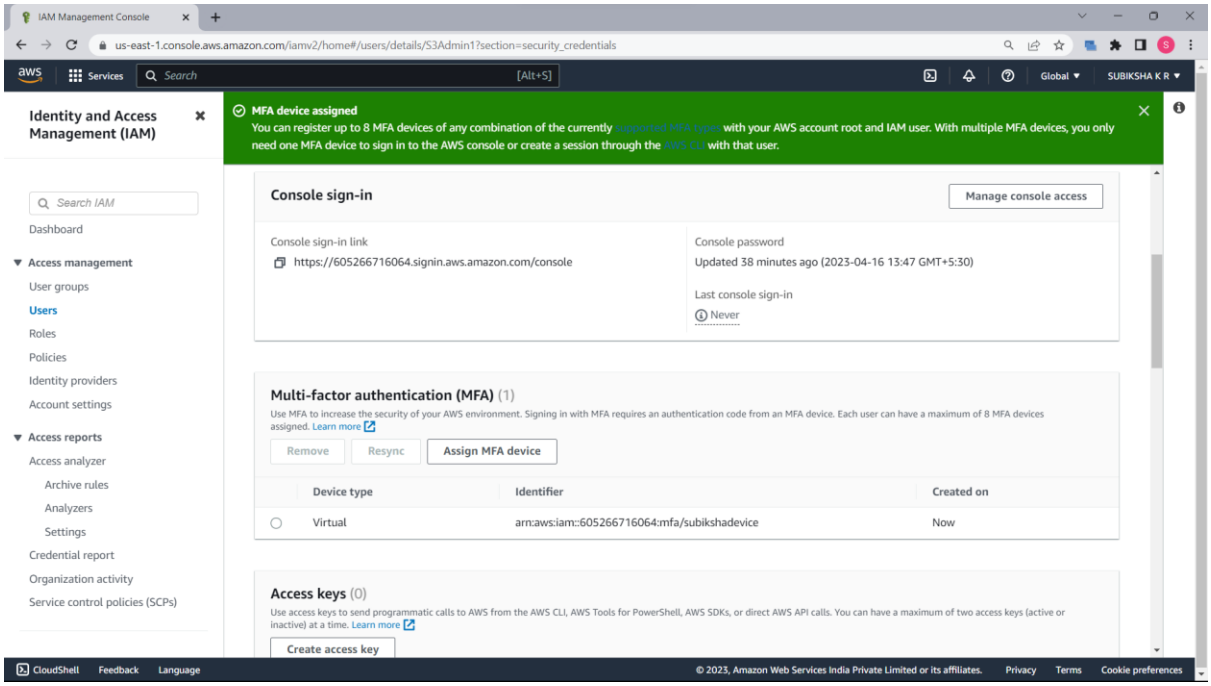
5) Create an IAM role with ‘AmazonS3FullAccess’ and attach the role to an EC2 instance.

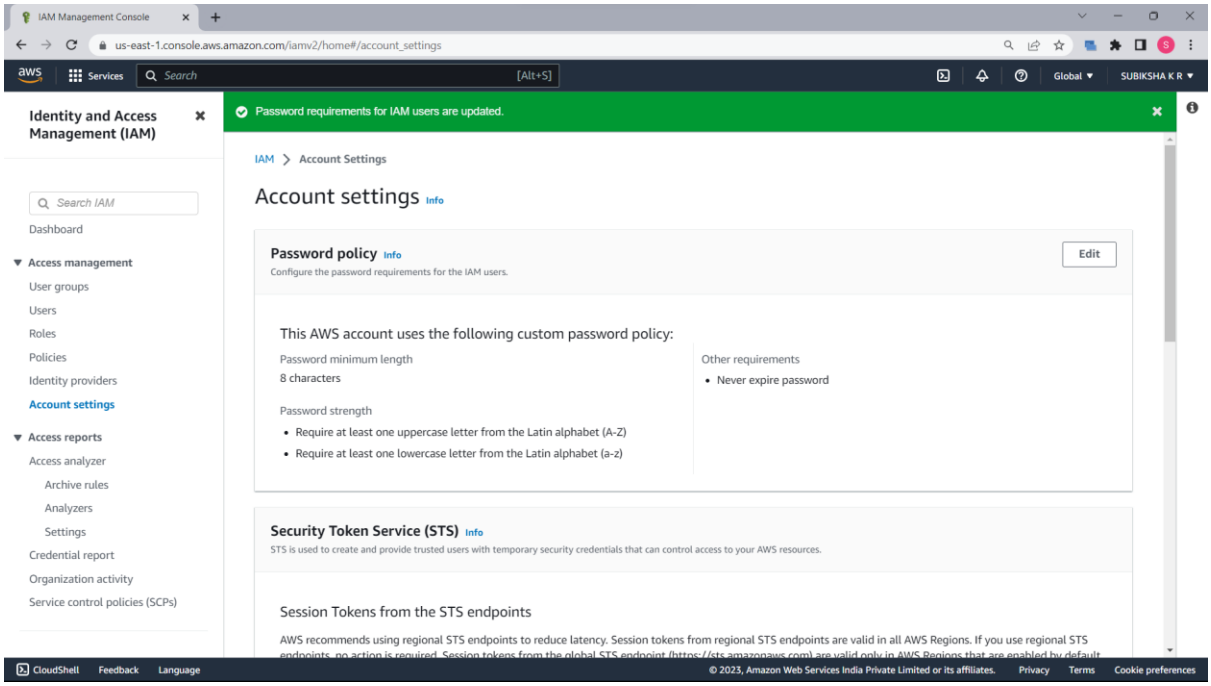




6)Activate MFA for an IAM user and Set some Password Policies such as 1 uppercase, 1 lowercase etc.

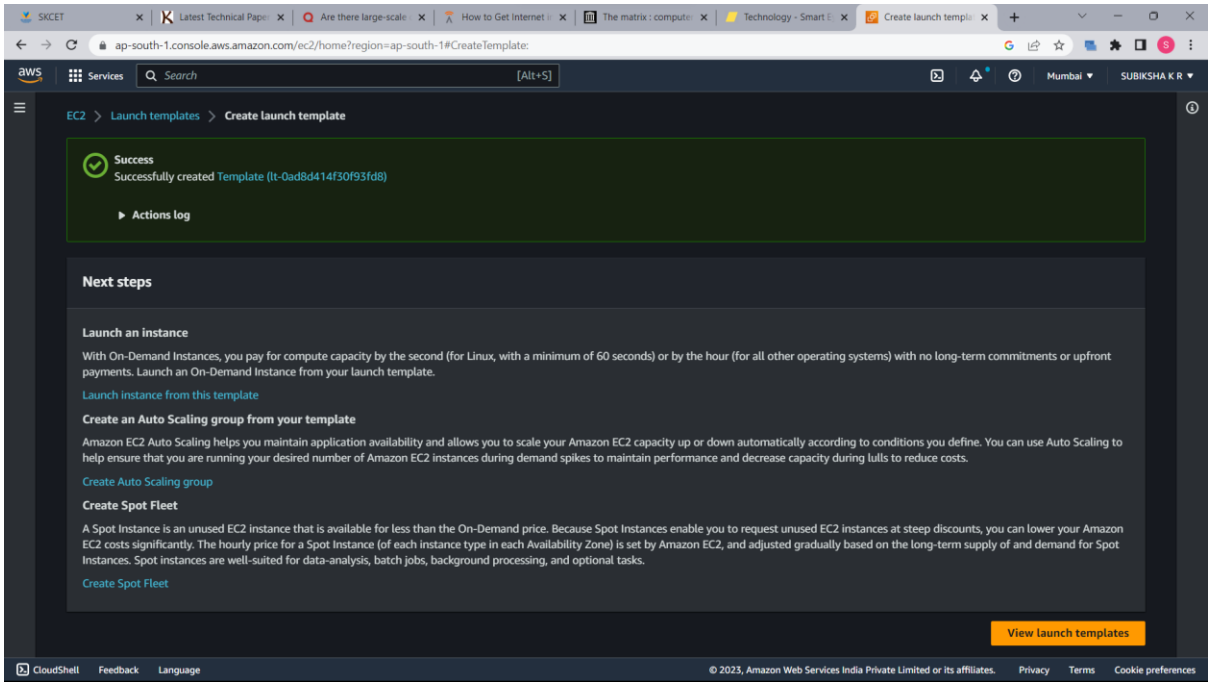


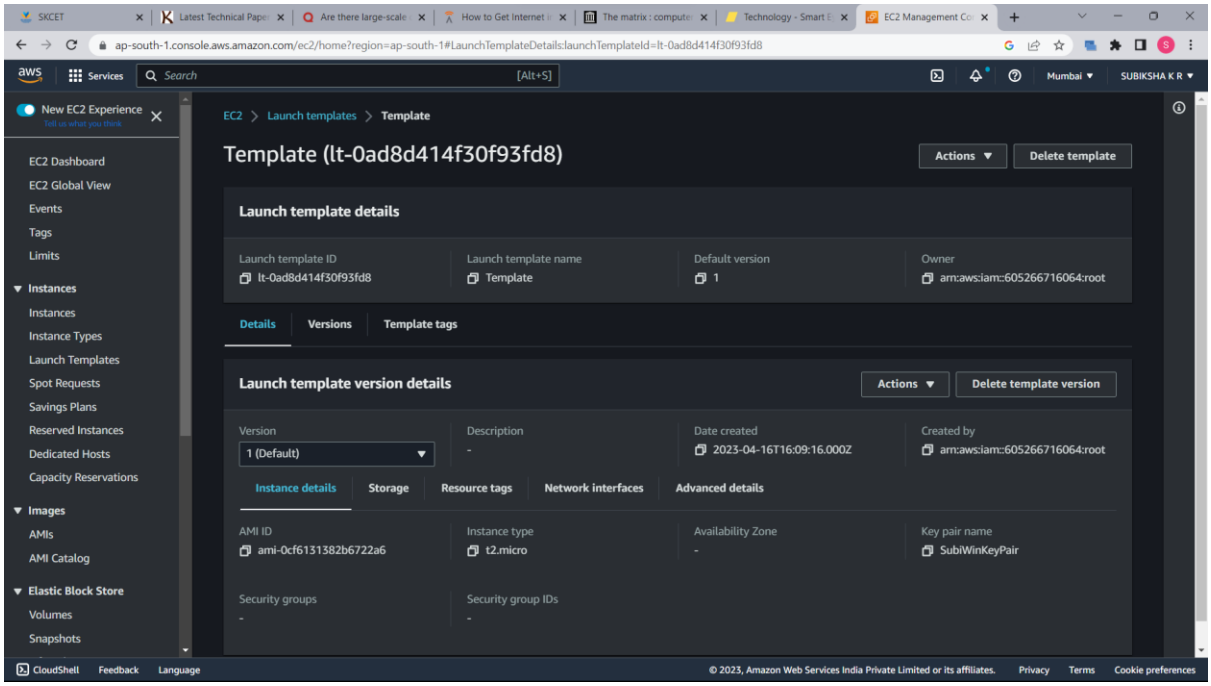

IAM Management Console
us-east-1.console.aws.amazon.com/iamv2/home#/users/details/S3Admin1?section=security_credentials
Services
Search
[Alt+S]
Global
SUBIKSHA K R
Identity and Access Management (IAM)
MFA device assigned
You can register up to 8 MFA devices of any combination of the currently supported MFA types with your AWS account root and IAM user. With multiple MFA devices, you only need one MFA device to sign in to the AWS console or create a session through the AWS CLI with that user.
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
Console sign-in
Manage console access
Console sign-in link
https://605266716064.signin.aws.amazon.com/console
Console password
Updated 38 minutes ago (2023-04-16 13:47 GMT+5:30)
Last console sign-in
Never
Multi-factor authentication (MFA) (1)
Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more
Remove
Resync
Assign MFA device
Device type
Identifier
Created on
Virtual
arn:aws:iam::605266716064:mfa/subikshadevice
Now
Access keys (0)
Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. Learn more
Create access key
CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences


IAM Management Console
us-east-1.console.aws.amazon.com/iamv2/home#/account_settings
Services
Search
[Alt+S]
Global
SUBIKSHA K R
Identity and Access Management (IAM)
Password requirements for IAM users are updated.
IAM > Account Settings
Account settings Info
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
Password policy Info
Configure the password requirements for the IAM users.
Edit
This AWS account uses the following custom password policy:
Password minimum length
8 characters
Password strength
Require at least one uppercase letter from the Latin alphabet (A-Z)
Require at least one lowercase letter from the Latin alphabet (a-z)
Other requirements
Never expire password
Security Token Service (STS) Info
STS is used to create and provide trusted users with temporary security credentials that can control access to your AWS resources.
Session Tokens from the STS endpoints
AWS recommends using regional STS endpoints to reduce latency. Session tokens from regional STS endpoints are valid in all AWS Regions. If you use regional STS
CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences

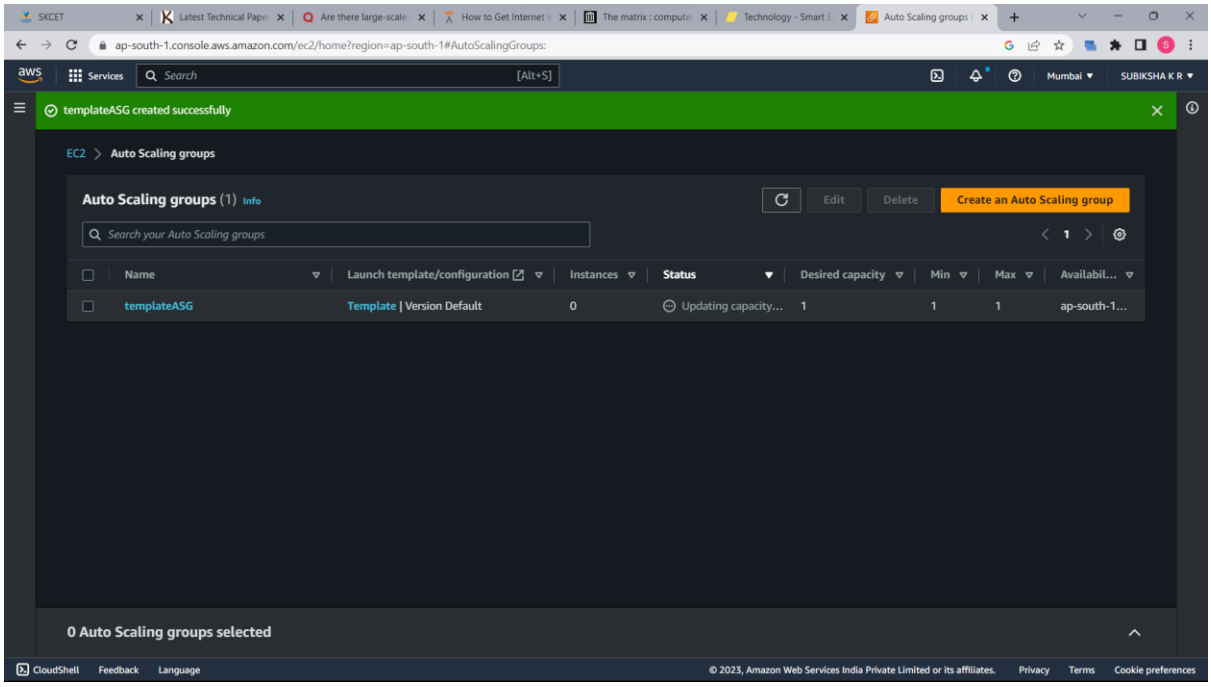
Day5

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



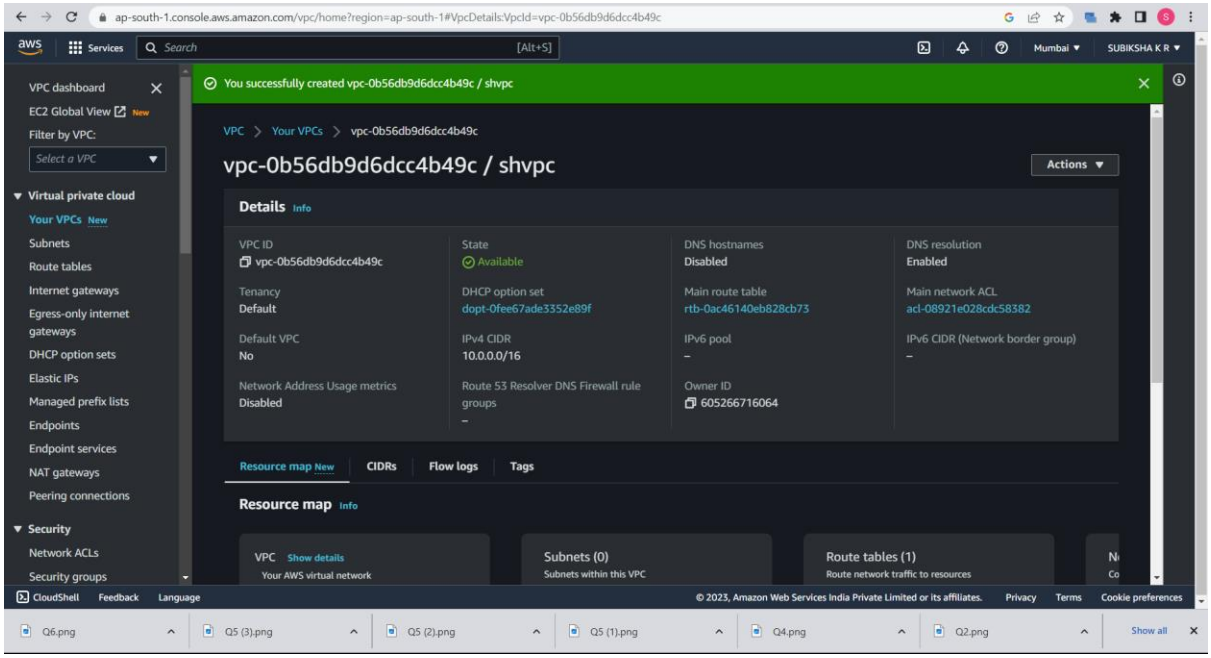


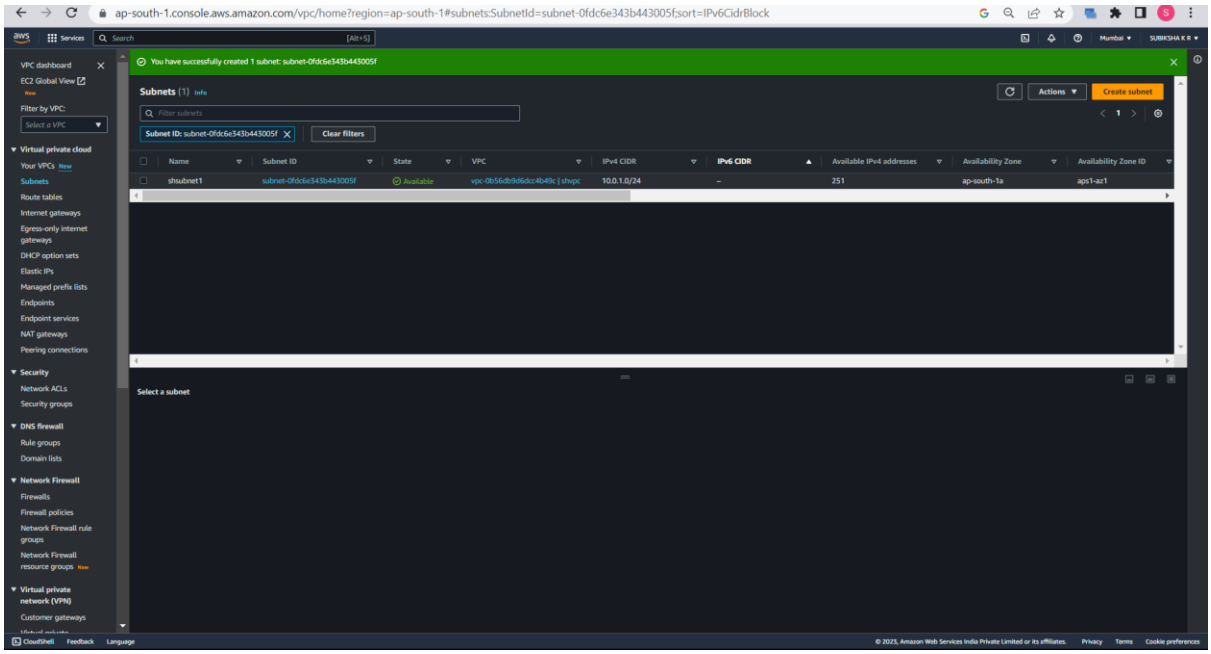
2) Create an autoscaling group with the above-created launch template

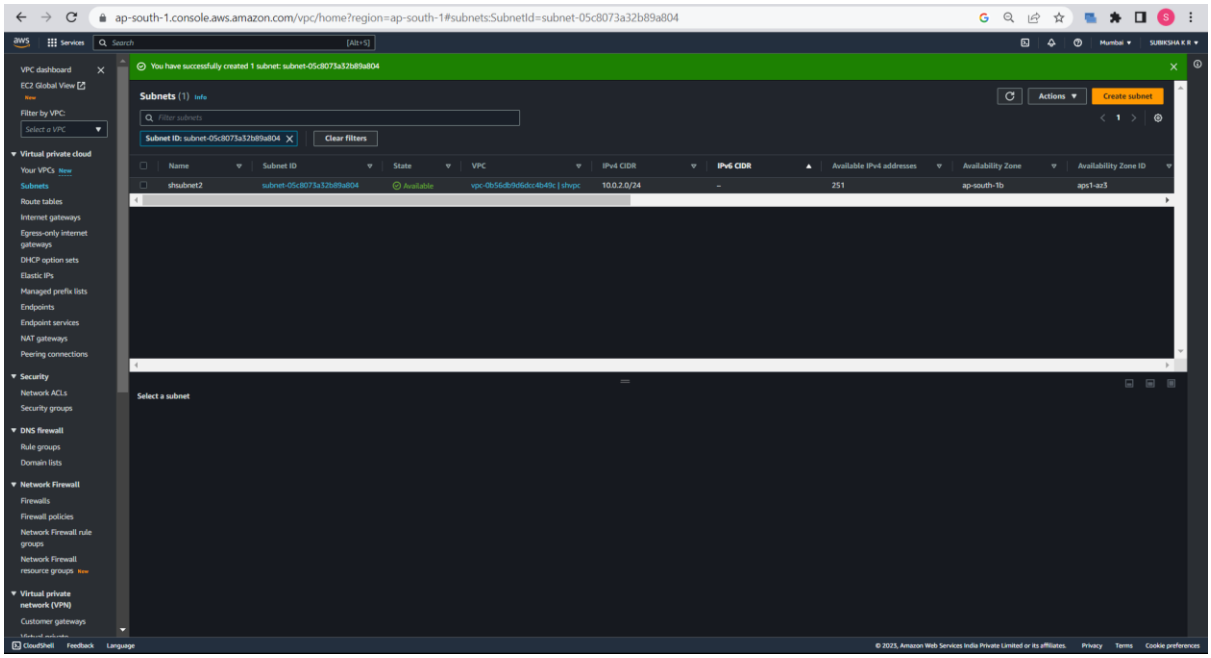


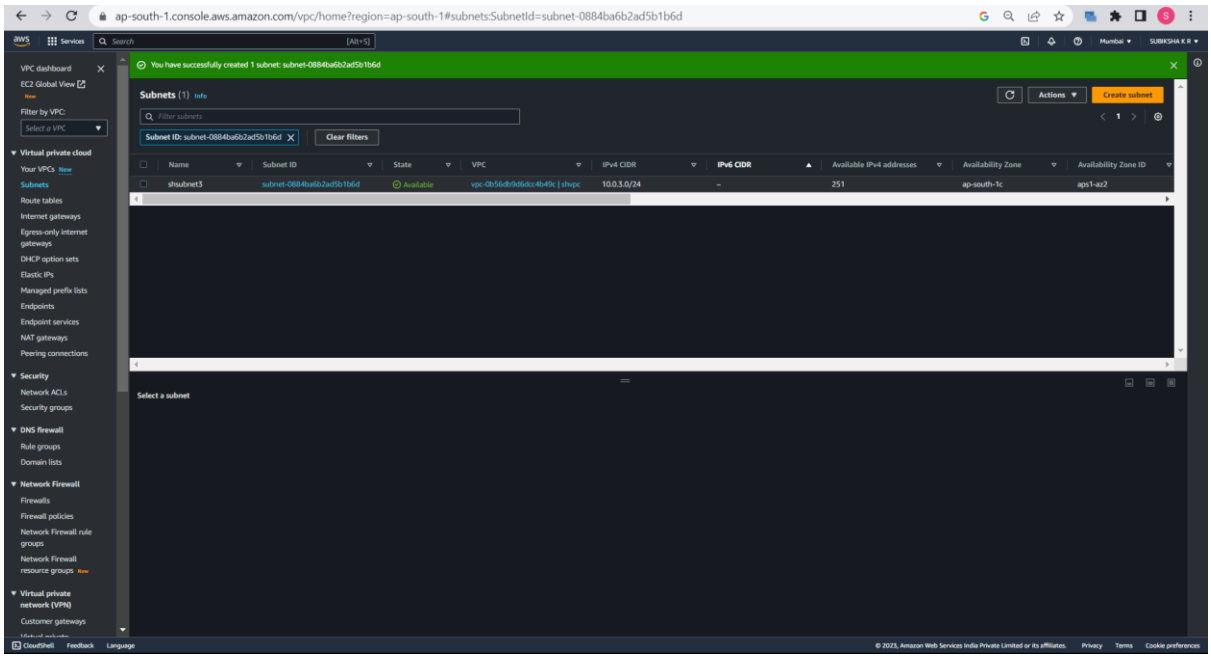
Day6

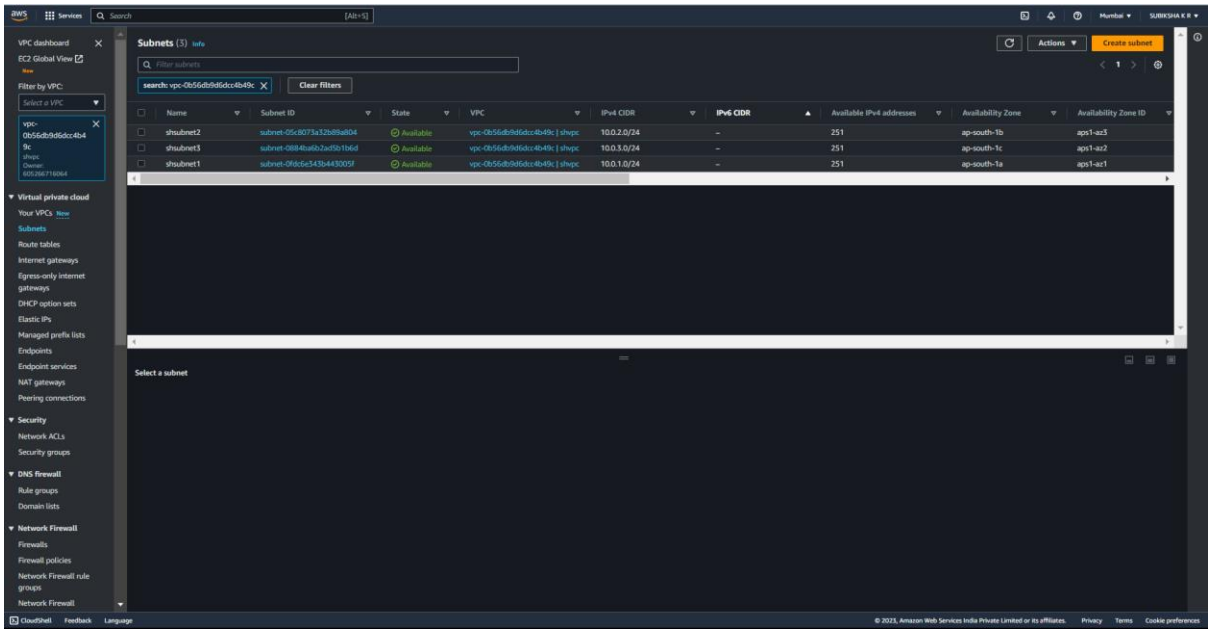
1) Create a vpc with multiple subnets(atleast 1 subnet in each zone)



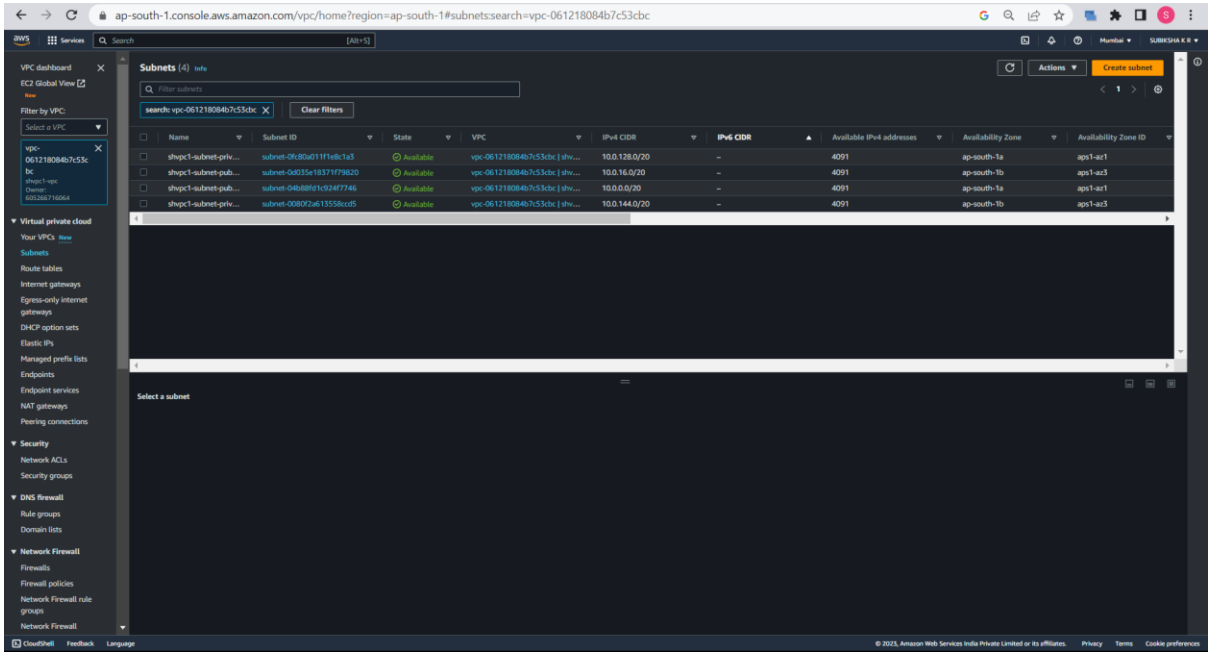



ap-south-1.console.aws.amazon.com/vpc/home?region=ap-south-1#subnets:SubnetId=subnet-05c8073a32b89a804
You have successfully created 1 subnet: subnet-05c8073a32b89a804
Subnets (1) Info
Actions
Create subnet
Subnet ID: subnet-05c8073a32b89a804
Clear filters
Name
Subnet ID
State
VPC
IPv4 CIDR
IPv6 CIDR
Available IPv4 addresses
Availability Zone
Availability Zone ID
shsubnet2
subnet-05c8073a32b89a804
Available
vpc-0b56db9d6dcc4b49c | shvpc
10.0.2.0/24
–
251
ap-south-1b
aps1-az3
Select a subnet

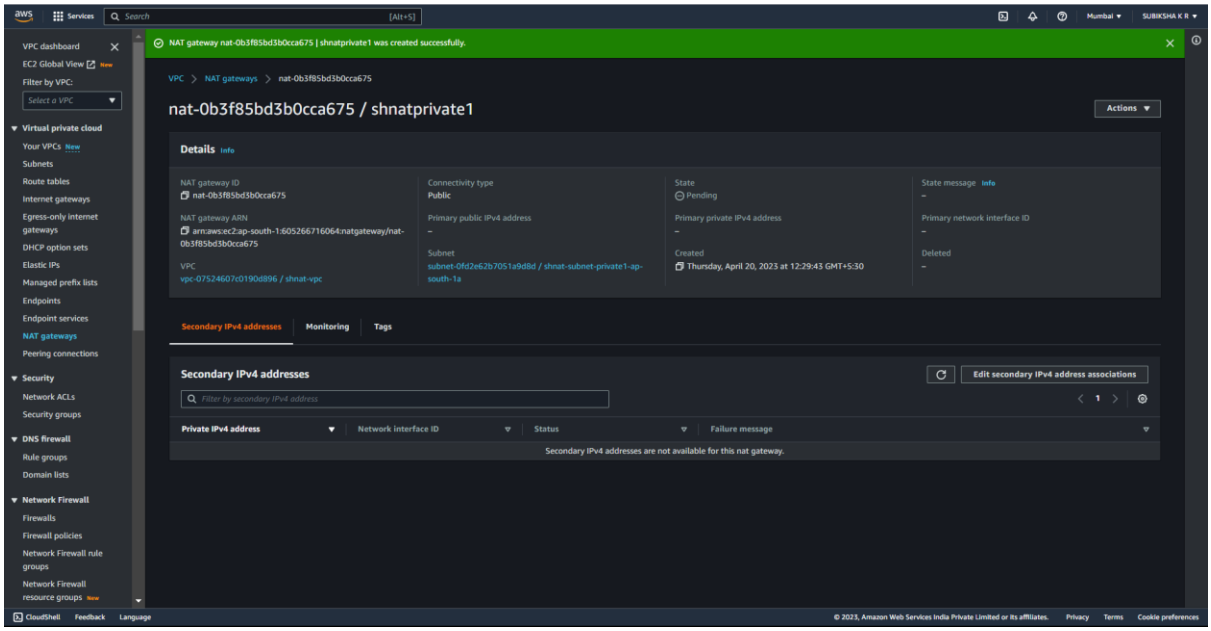

ap-south-1.console.aws.amazon.com/vpc/home?region=ap-south-1#subnets:SubnetId=subnet-0884ba6b2ad5b1b6d
You have successfully created 1 subnet: subnet-0884ba6b2ad5b1b6d
Subnets (1) Info
Actions
Create subnet
Subnet ID: subnet-0884ba6b2ad5b1b6d
Clear filters
Name
Subnet ID
State
VPC
IPv4 CIDR
IPv6 CIDR
Available IPv4 addresses
Availability Zone
Availability Zone ID
shsubnet3
subnet-0884ba6b2ad5b1b6d
Available
vpc-0b56db9d6dcc4b49c | shvpc
10.0.3.0/24
–
251
ap-south-1c
aps1-az2
Select a subnet

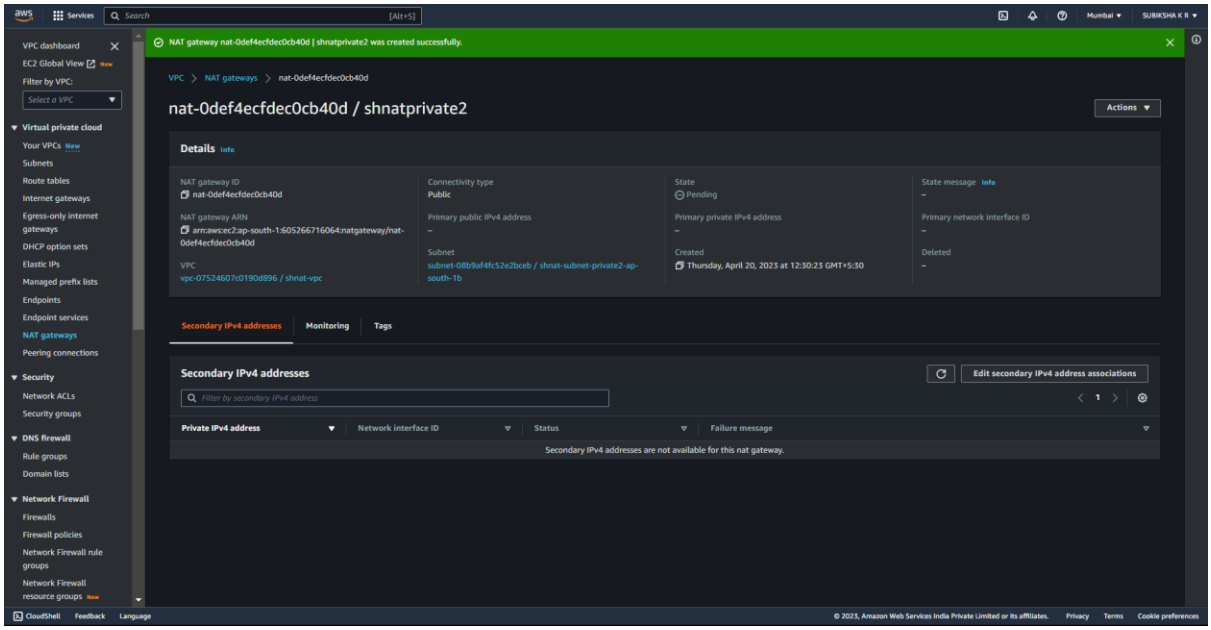


2) Make 1 public subnet and 2 private subnets in the created VPC

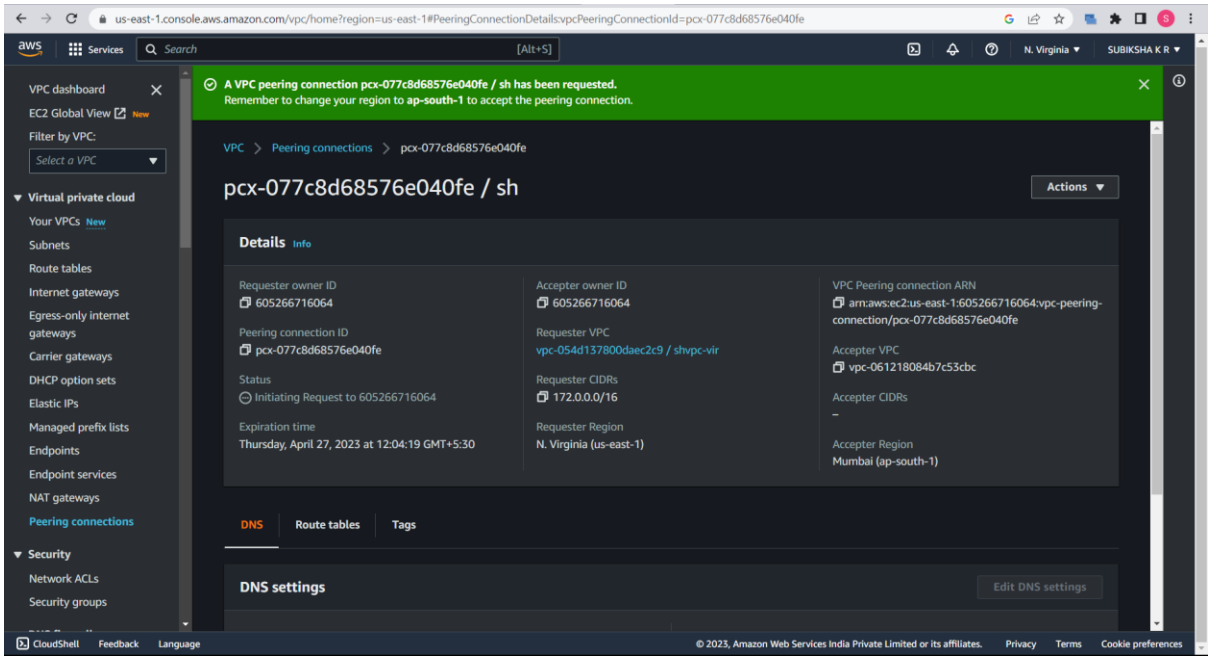


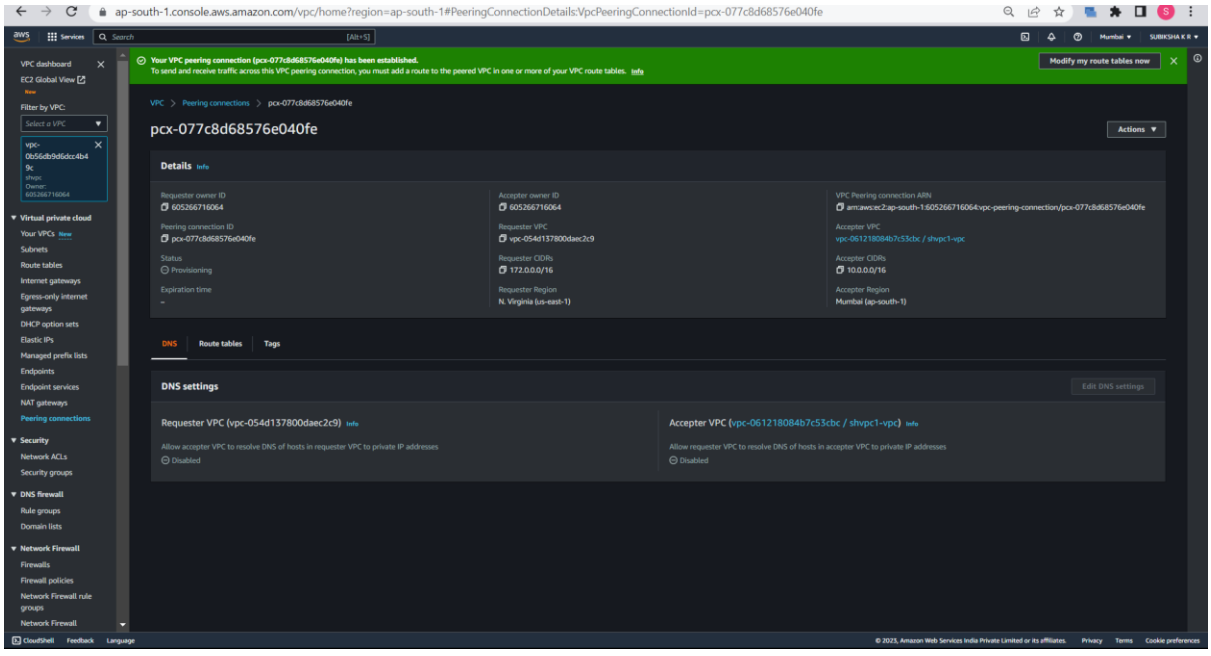
3) Make internet connection using NAT gateway for the 2 private subnets.



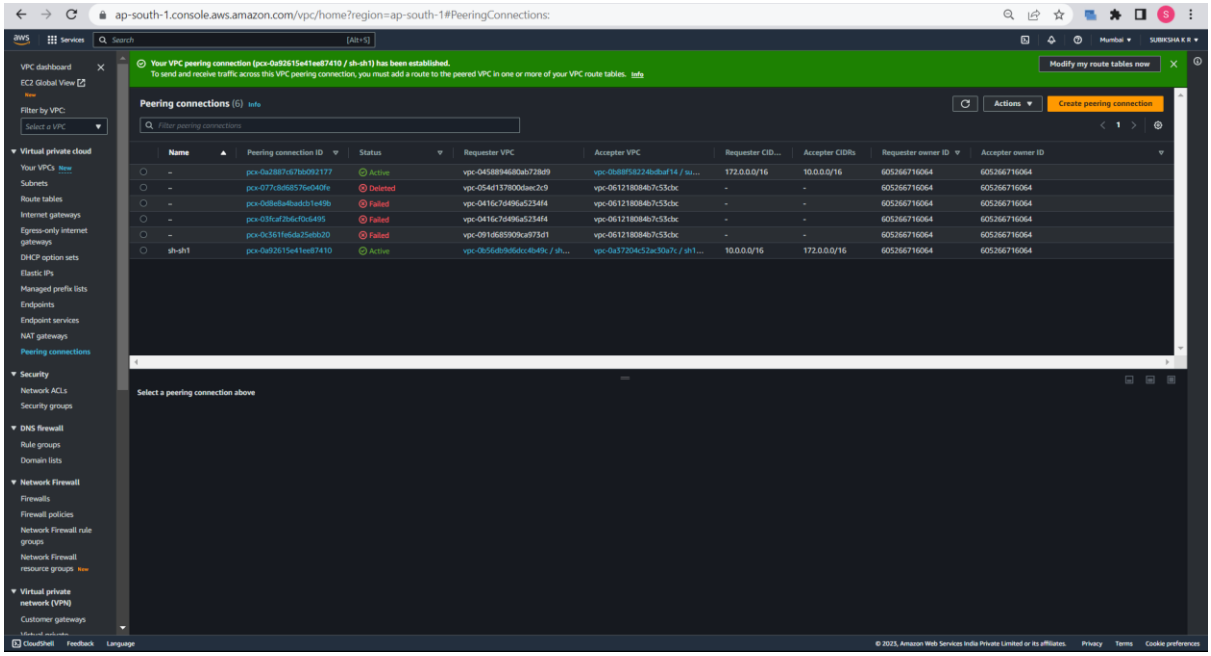


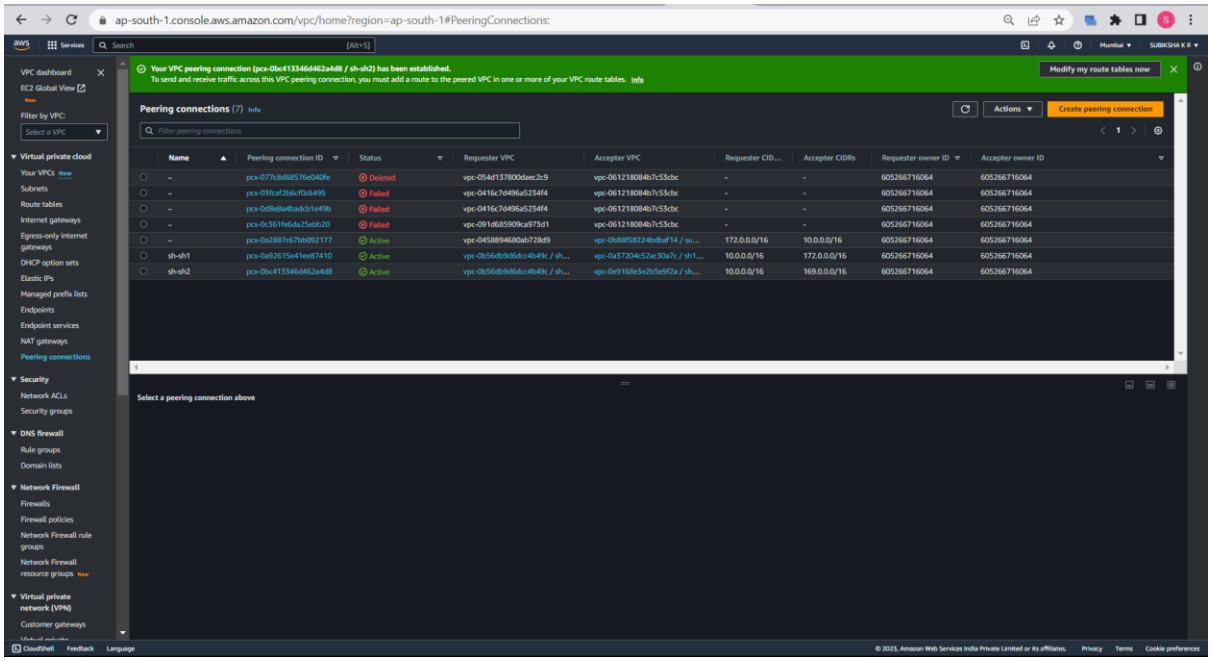
4) Create a VPC peering connetion between 2 different VPCs from 2 different regions.

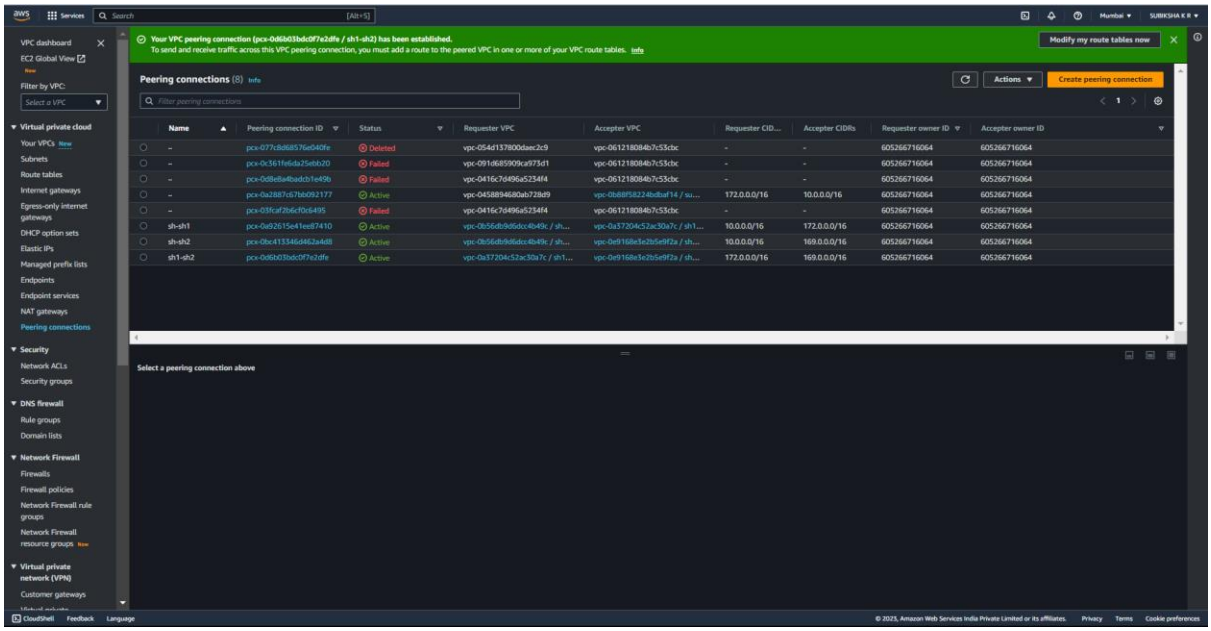




5) Create VPC peering connetions for 3 different VPCs from the same region







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