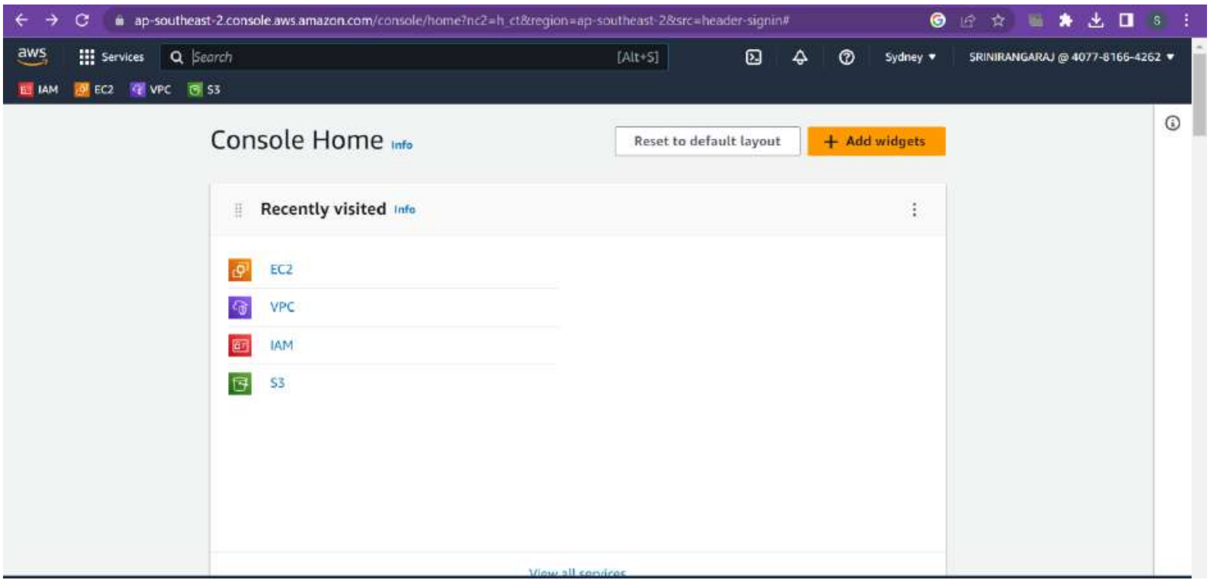
CLOUD COMPUTING

NAME : SRINI R
ROLL NO : 727721EUCS152

DAY-1:

1.AWS account creation



ap-southeast-2.console.aws.amazon.com/console/home?nc2=h_ct&region=ap-southeast-2&src=header-signin#

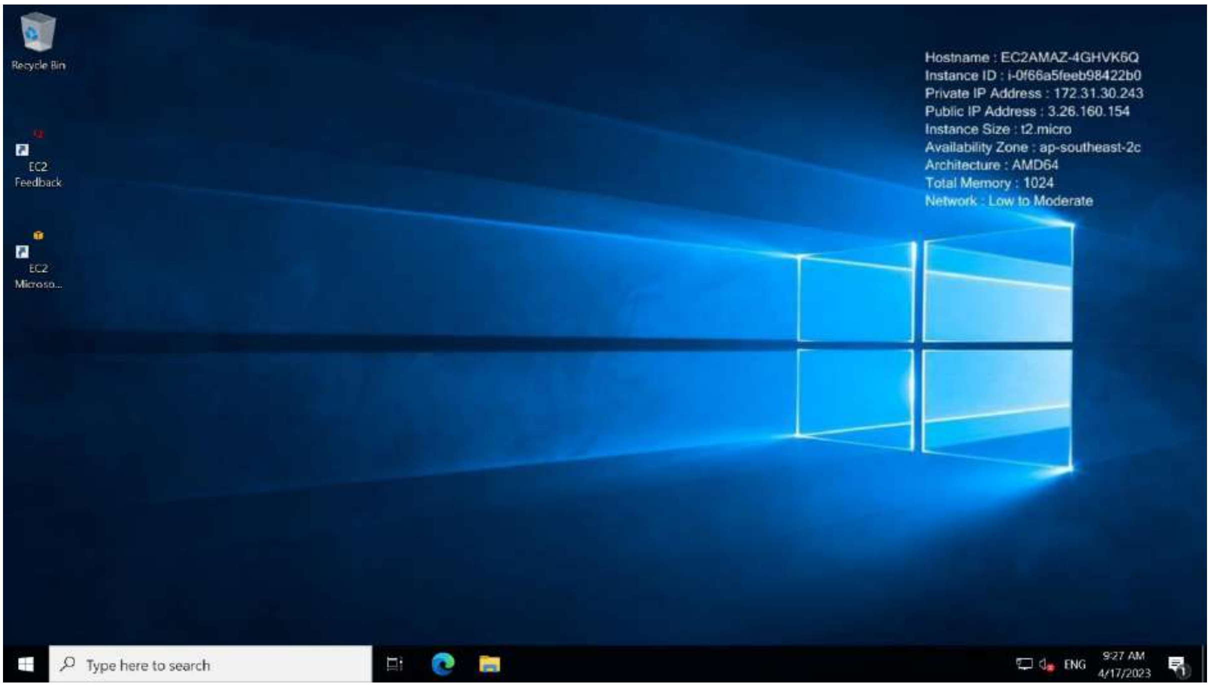
SRINIRANGARAJ @ 4077-8166-4262

CLOUD COMPUTING

NAME : SRINI R
ROLL NO : 727721EUCS152

DAY-2:

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

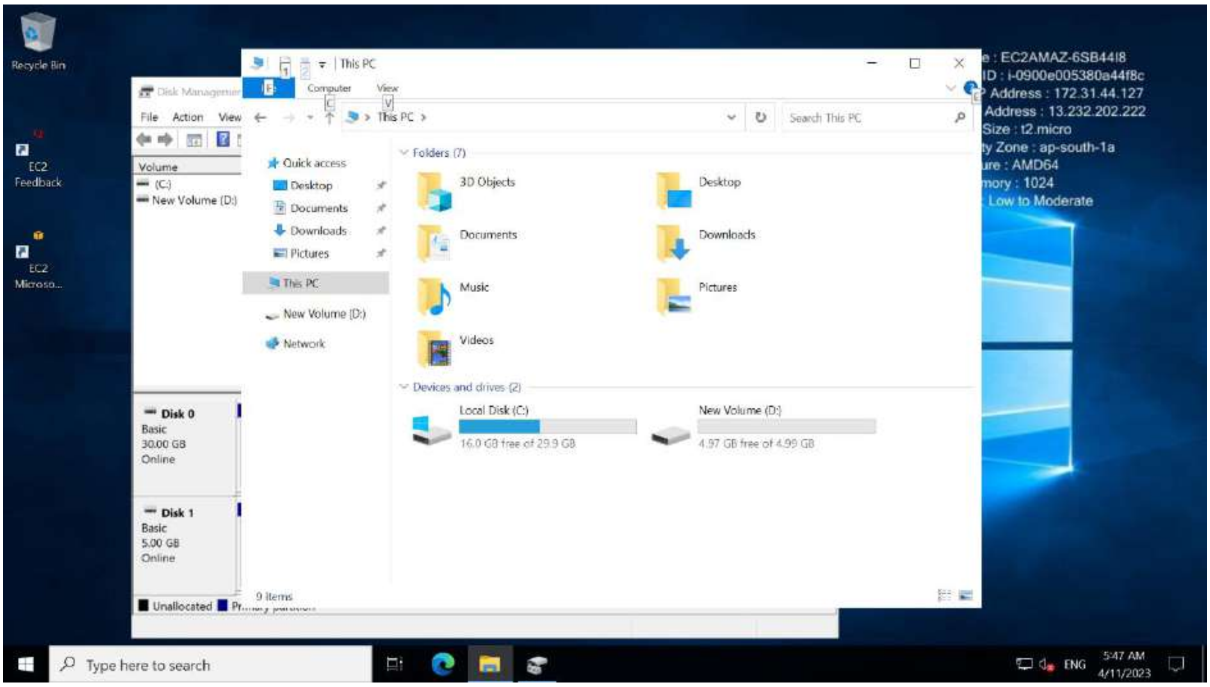


Hostname : EC2AMAZ-4GHVK6Q
Instance ID : i-0f66a5feeb98422b0
Private IP Address : 172.31.30.243
Public IP Address : 3.26.160.154
Instance Size : t2.micro
Availability Zone : ap-southeast-2c
Architecture : AMD64
Total Memory : 1024
Network : Low to Moderate

CLOUD COMPUTING

NAME : SRINI R
ROLL NO : 727721EUCS152

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



e : EC2AMAZ-6SB44I8
ID : i-0900e005380a44f8c
P Address : 172.31.44.127
Address : 13.232.202.222
Size : t2.micro
ty Zone : ap-south-1a
ure : AMD64
mory : 1024
Low to Moderate

Disk 0
Basic
30.00 GB
Online

Disk 1
Basic
5.00 GB
Online

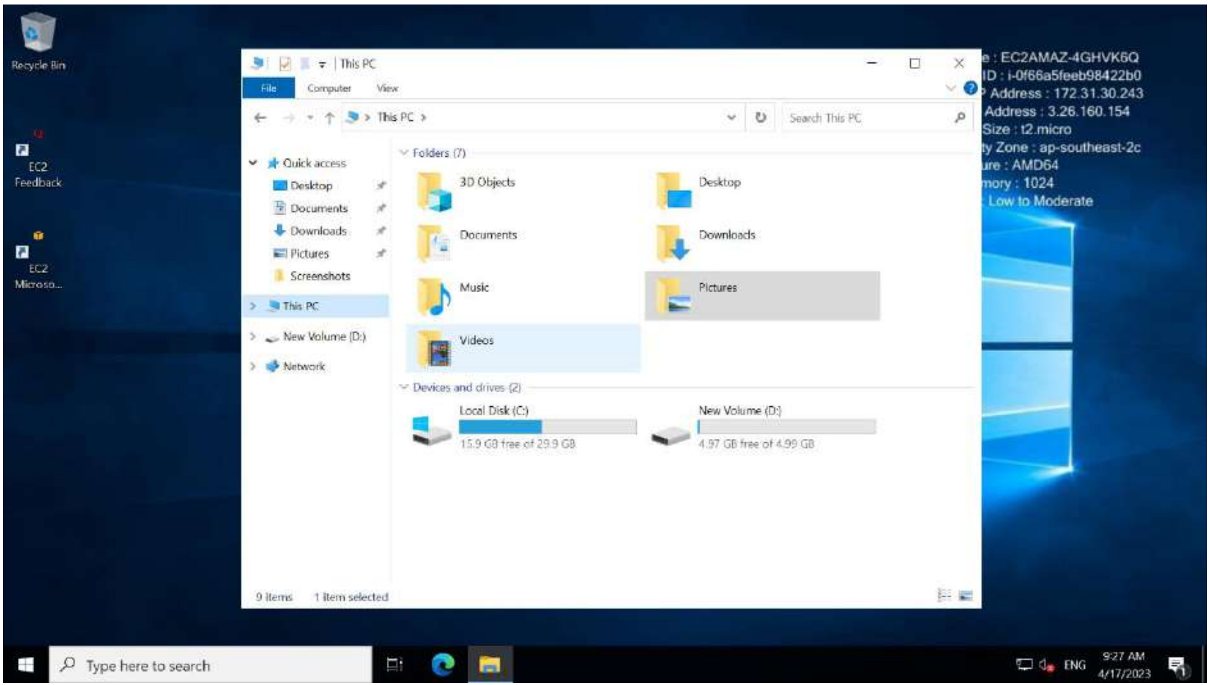
Local Disk (C:) 16.0 GB free of 29.9 GB

New Volume (D:) 4.97 GB free of 4.99 GB

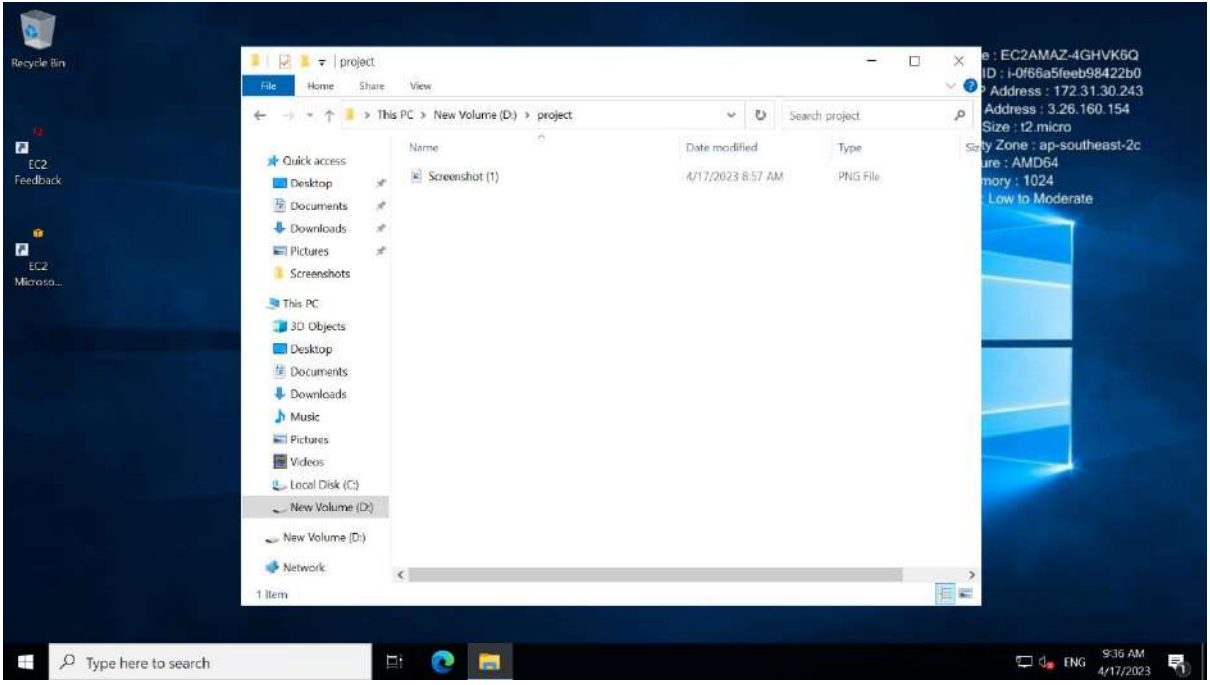
3. Create some files and folders into 5 GB EBS volume of the previous exercise and take a snapshot of that EBS volume.

CLOUD COMPUTING

NAME : SRINI R
ROLL NO : 727721EUCS152



e : EC2AMAZ-4GHVK6Q
ID : i-0f66a5feeb98422b0
Address : 172.31.30.243
Address : 3.26.160.154
Size : t2.micro
ty Zone : ap-southeast-2c
ure : AMD64
mory : 1024
Low to Moderate



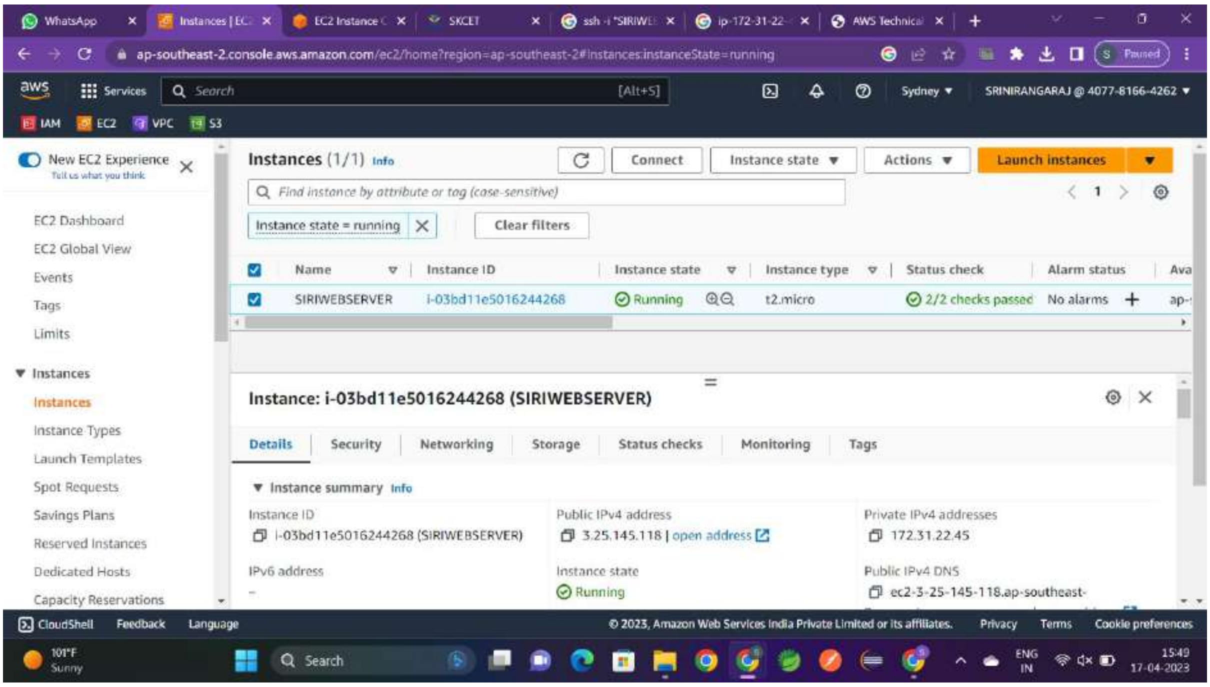
Name	Date modified	Type
Screenshot (1)	4/17/2023 8:57 AM	PNG File

e : EC2AMAZ-4GHVK6Q
ID : i-0f66a5feeb98422b0
Address : 172.31.30.243
Address : 3.26.160.154
Size : t2.micro
ty Zone : ap-southeast-2c
ure : AMD64
mory : 1024
Low to Moderate

CLOUD COMPUTING

NAME : SRINI R
ROLL NO : 727721EUCS152

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



Instances (1/1)

Instance state = running

Name	Instance ID	Instance state	Instance type	Status check	Alarm status
SIRIWEBSERVER	i-03bd11e5016244268	Running	t2.micro	2/2 checks passed	No alarms

Instance: i-03bd11e5016244268 (SIRIWEBSERVER)

Instance summary

Instance ID: i-03bd11e5016244268 (SIRIWEBSERVER)

Public IPv4 address: 3.25.145.118 | open address

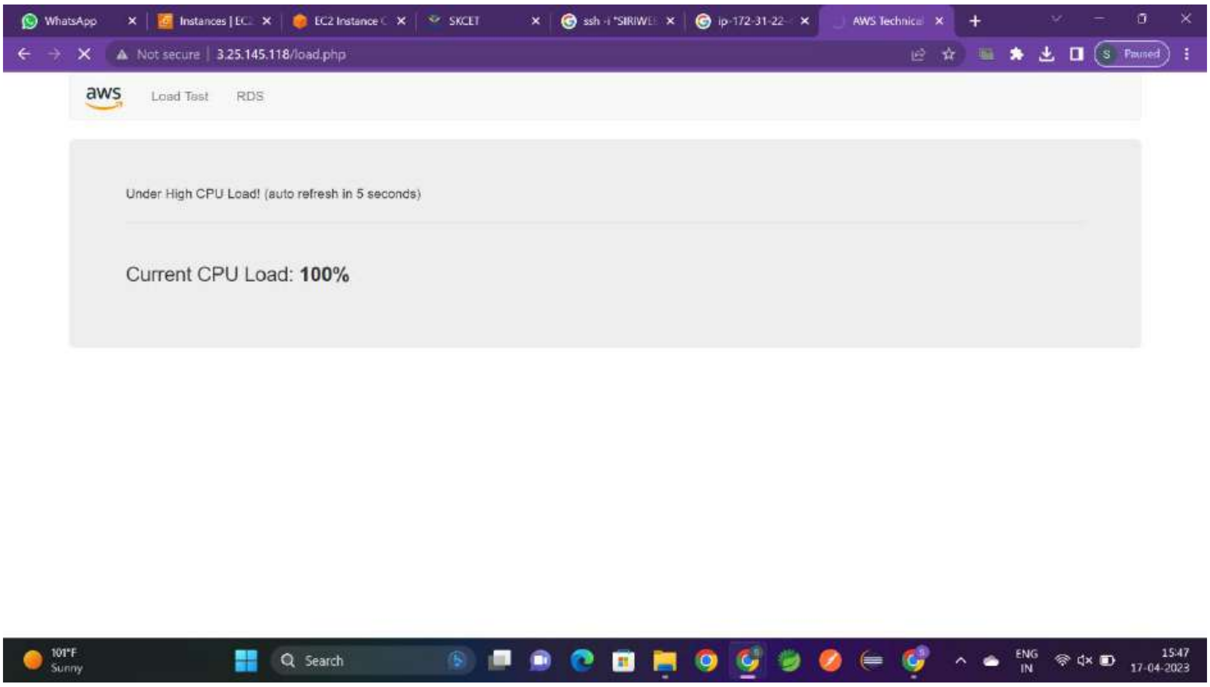
Private IPv4 addresses: 172.31.22.45

IPv6 address: –

Instance state: Running

Public IPv4 DNS: ec2-3-25-145-118.ap-southeast-

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



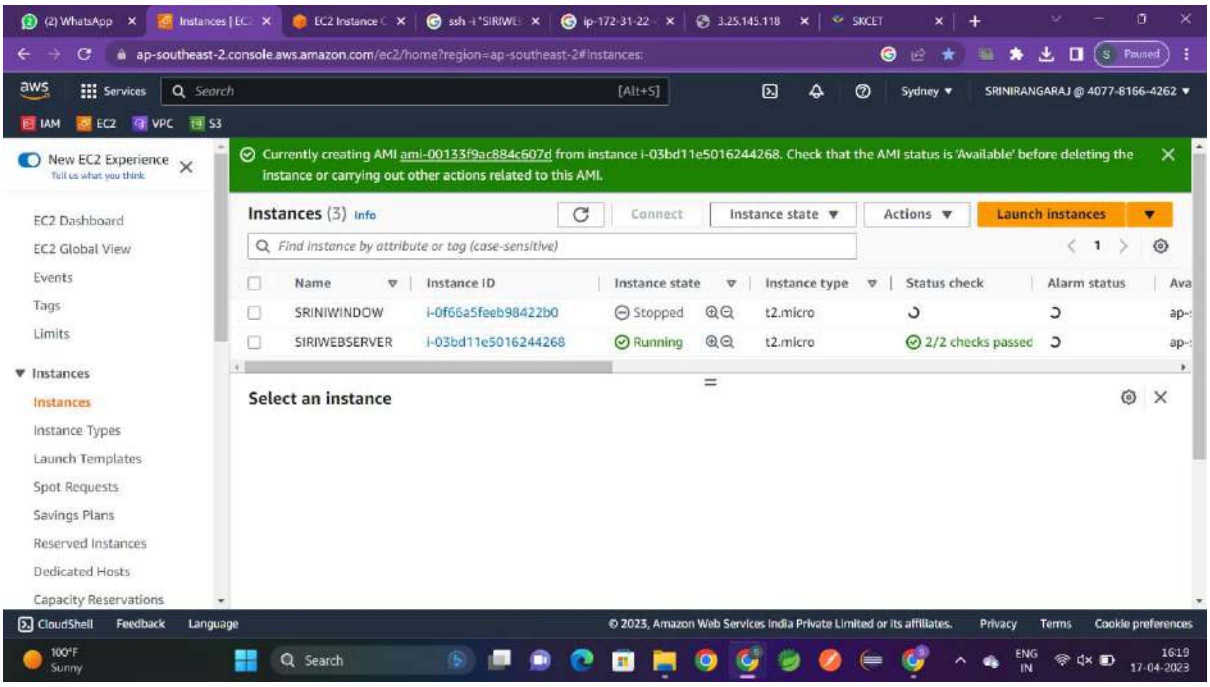
Under High CPU Load! (auto refresh in 5 seconds)

Current CPU Load: **100%**

CLOUD COMPUTING

NAME : SRINI R
ROLL NO : 727721EUCS152

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



Currently creating AMI ami-00133f9ac884c607d from instance i-03bd11e5016244268. Check that the AMI status is 'Available' before deleting the instance or carrying out other actions related to this AMI.

Instances (3)

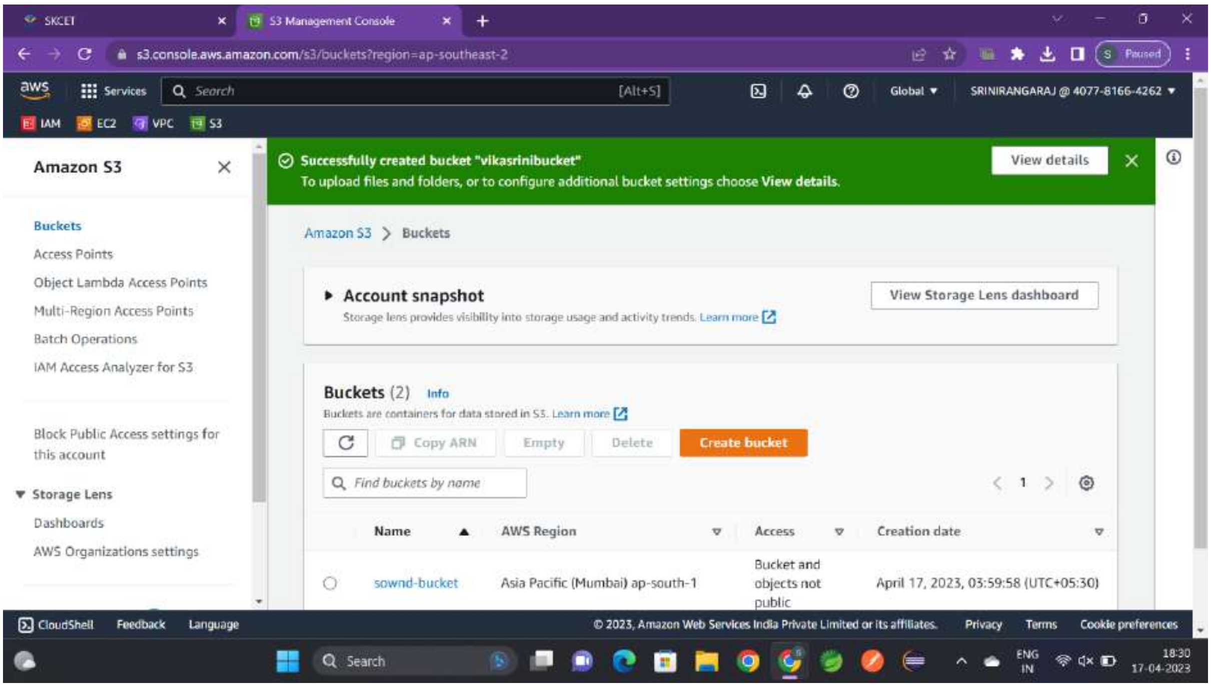
Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Ava
SRINIWINDOW	i-0f66a5feeb98422b0	Stopped	t2.micro			ap-
SIRIWEBSERVER	i-03bd11e5016244268	Running	t2.micro	2/2 checks passed		ap-

DAY-3:

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

CLOUD COMPUTING

NAME : SRINI R
ROLL NO : 727721EUCS152



s3.console.aws.amazon.com/s3/buckets?region=ap-southeast-2

Successfully created bucket "vikasrinibucket"
To upload files and folders, or to configure additional bucket settings choose **View details**.

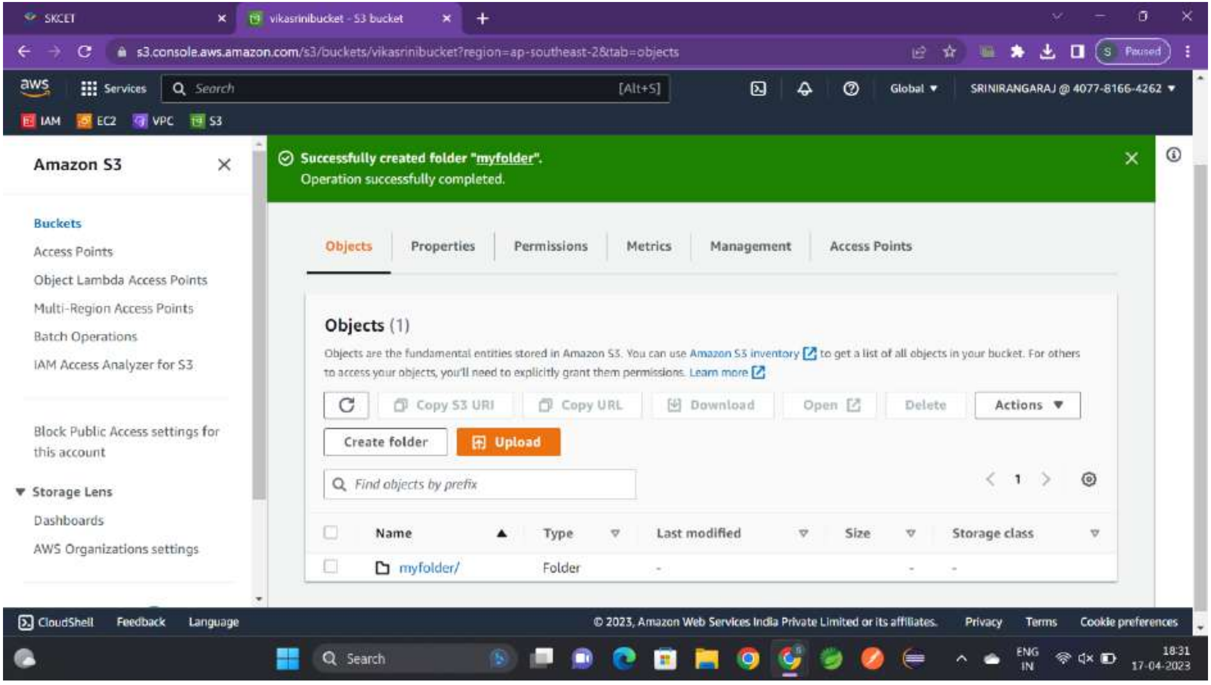
Amazon S3 > Buckets

Account snapshot
Storage lens provides visibility into storage usage and activity trends. Learn more

Buckets (2) Info
Buckets are containers for data stored in S3. Learn more

Name	AWS Region	Access	Creation date
sownd-bucket	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	April 17, 2023, 03:59:58 (UTC+05:30)

© 2023, Amazon Web Services India Private Limited or its affiliates.



s3.console.aws.amazon.com/s3/buckets/vikasrinibucket?region=ap-southeast-2&tab=objects

Successfully created folder "myfolder".
Operation successfully completed.

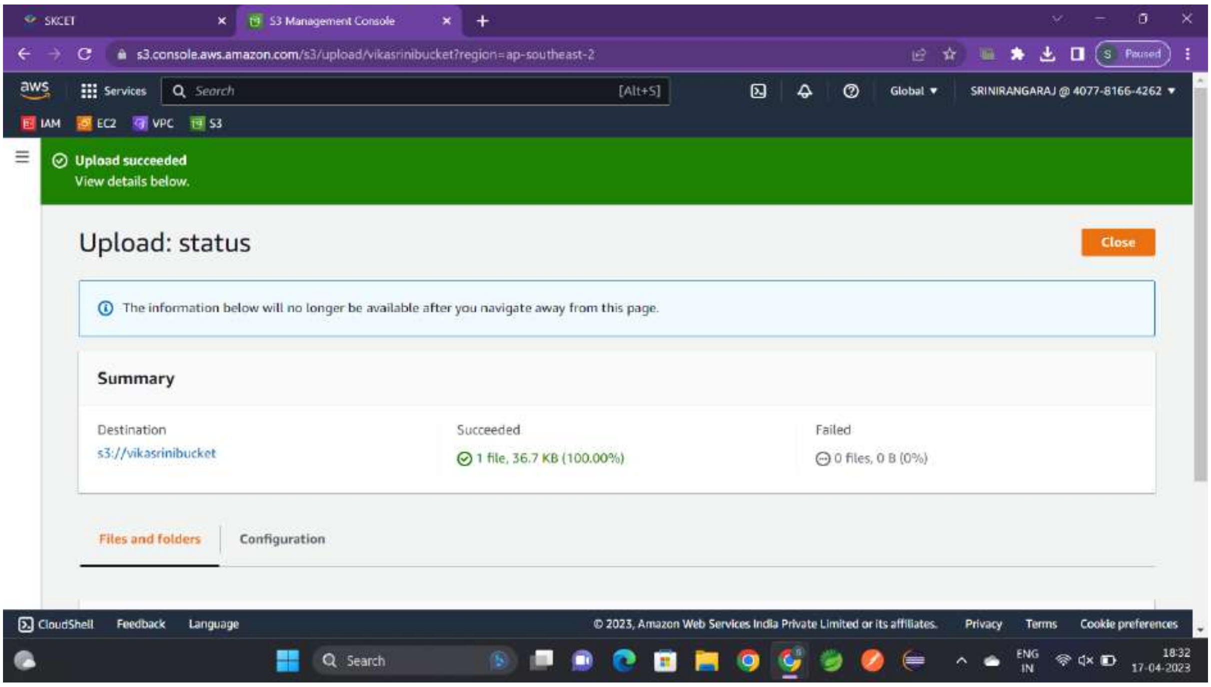
Objects (1)
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Name	Type	Last modified	Size	Storage class
myfolder/	Folder	-	-	-

© 2023, Amazon Web Services India Private Limited or its affiliates.

CLOUD COMPUTING

NAME : SRINI R
ROLL NO : 727721EUCS152



Upload succeeded
View details below.

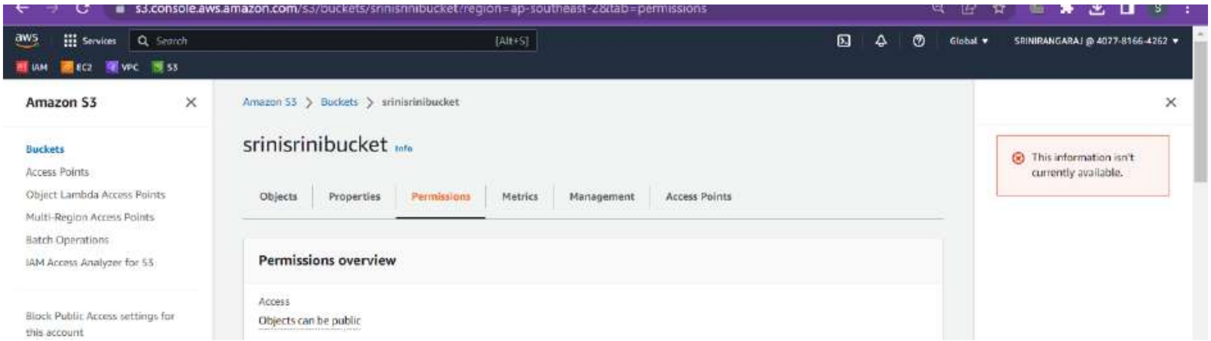
Upload: status

The information below will no longer be available after you navigate away from this page.

Summary

Destination	Succeeded	Failed
s3://vikasrinibucket	1 file, 36.7 KB (100.00%)	0 files, 0 B (0%)

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


s3.console.aws.amazon.com/s3/buckets/srinisrinibucket?region=ap-southeast-2&tab=permissions
aws
Services
Search
[Alt+S]
Global
SRINIRANGARAJ @ 4077-8166-4262
IAM
EC2
VPC
S3
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
Amazon S3
Buckets
srinisrinibucket
Info
Objects
Properties
Permissions
Metrics
Management
Access Points

srinisrinibucket

Permissions overview

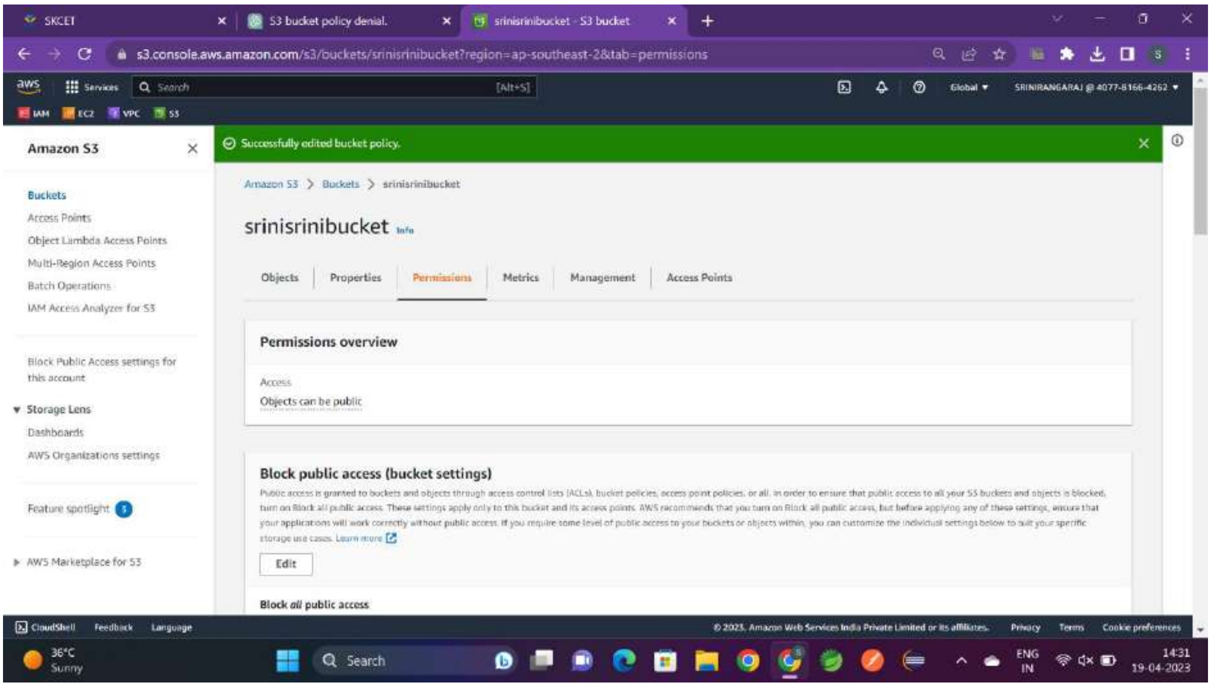
Access
Objects can be public

This information isn't currently available.

CLOUD COMPUTING

NAME : SRINI R
ROLL NO : 727721EUCS152

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


SKCET
S3 bucket policy denial.
srinisrinibucket - S3 bucket
s3.console.aws.amazon.com/s3/buckets/srinisrinibucket?region=ap-southeast-2&tab=permissions
Services
Search
[Alt+S]
Global
SRINIRANGARAJ @ 4077-8166-4262
IAM
EC2
VPC
S3
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 > srinisrinibucket
Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Edit
CloudShell
Feedback
Language
Privacy
Terms
Cookie preferences
36°C
Sunny
Search
ENG
IN
14:31
19-04-2023

Successfully edited bucket policy.

srinisrinibucket

Permissions overview

Access
Objects can be public

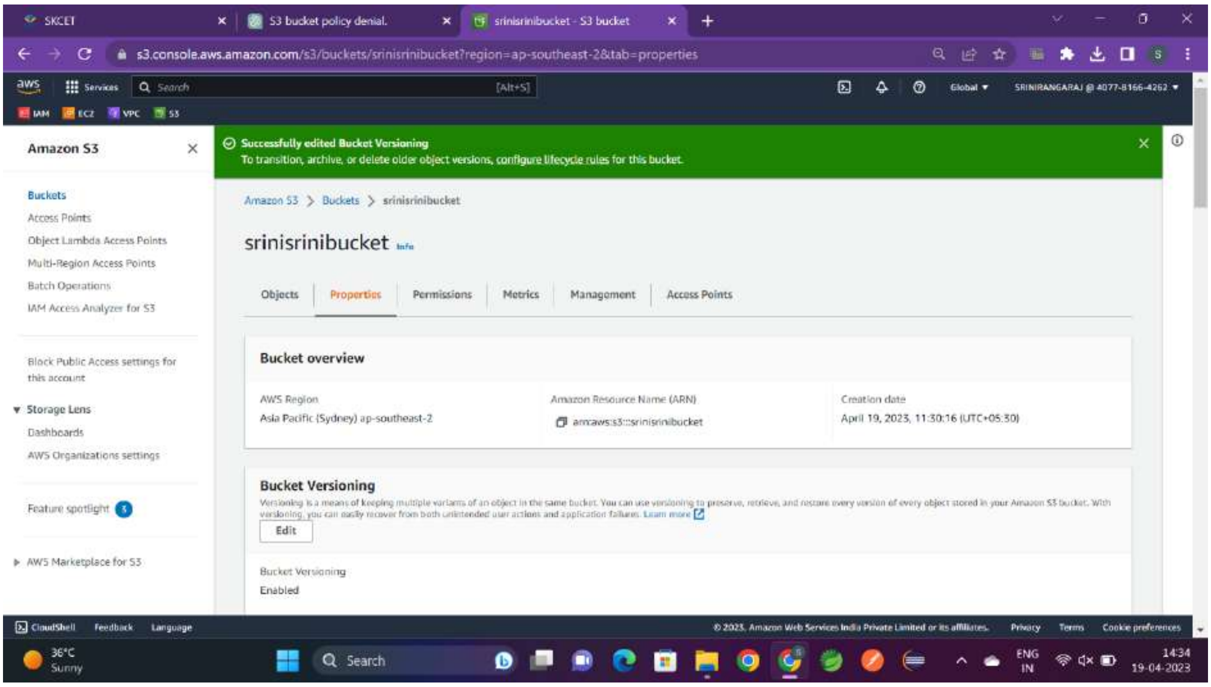
Block public access (bucket settings)

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

Block *all* public access

© 2023, Amazon Web Services India Private Limited or its affiliates.

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


SKCET
S3 bucket policy denial.
srinisrinibucket - S3 bucket
s3.console.aws.amazon.com/s3/buckets/srinisrinibucket?region=ap-southeast-2&tab=properties
Services
Search
[Alt+S]
Global
SRINIRANGARAJ @ 4077-8166-4262
IAM
EC2
VPC
S3
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 > srinisrinibucket
Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Edit
CloudShell
Feedback
Language
Privacy
Terms
Cookie preferences
36°C
Sunny
Search
ENG
IN
14:34
19-04-2023

Successfully edited Bucket Versioning
To transition, archive, or delete older object versions, configure lifecycle rules for this bucket.

srinisrinibucket

Bucket overview

AWS Region	Amazon Resource Name (ARN)	Creation date
Asia Pacific (Sydney) ap-southeast-2	arn:aws:s3:::srinisrinibucket	April 19, 2023, 11:30:16 (UTC+05:30)

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more

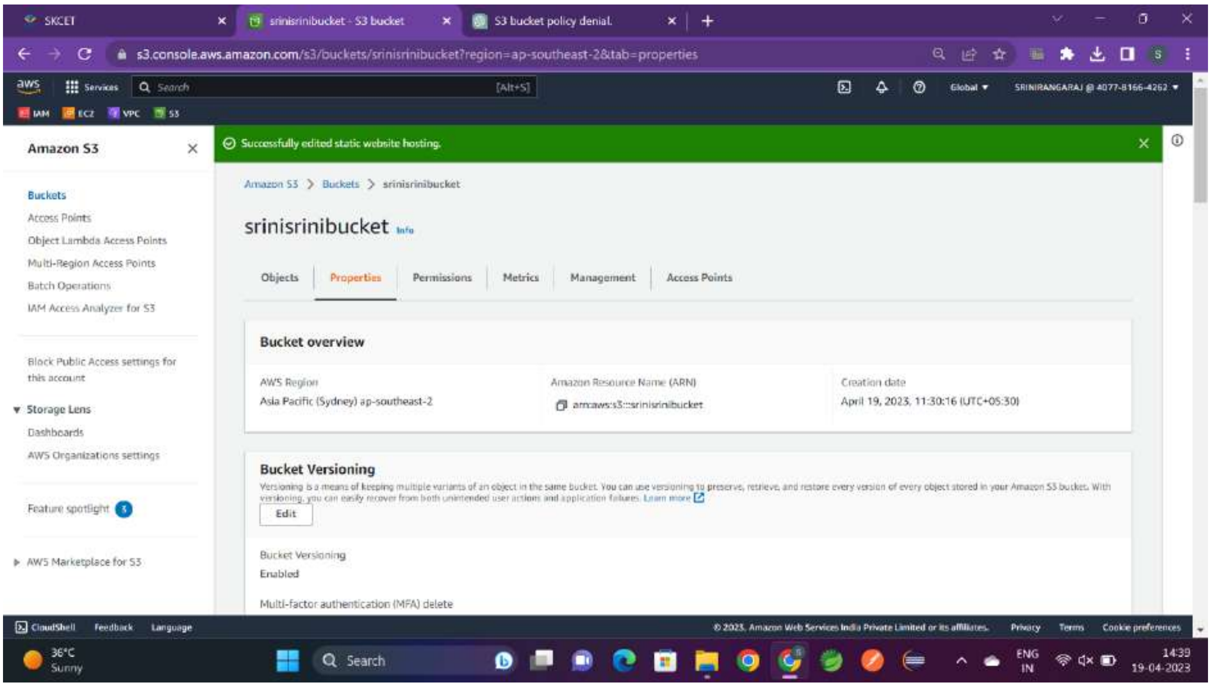
Bucket Versioning
Enabled

© 2023, Amazon Web Services India Private Limited or its affiliates.

CLOUD COMPUTING

NAME : SRINI R
ROLL NO : 727721EUCS152

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



s3.console.aws.amazon.com/s3/buckets/srinisrinibucket?region=ap-southeast-2&tab=properties

Successfully edited static website hosting.

Amazon S3 > Buckets > srinisrinibucket

srinisrinibucket

Bucket overview

AWS Region: Asia Pacific (Sydney) ap-southeast-2

Amazon Resource Name (ARN): arn:aws:s3:::srinisrinibucket

Creation date: April 19, 2023, 11:30:16 (UTC+05:30)

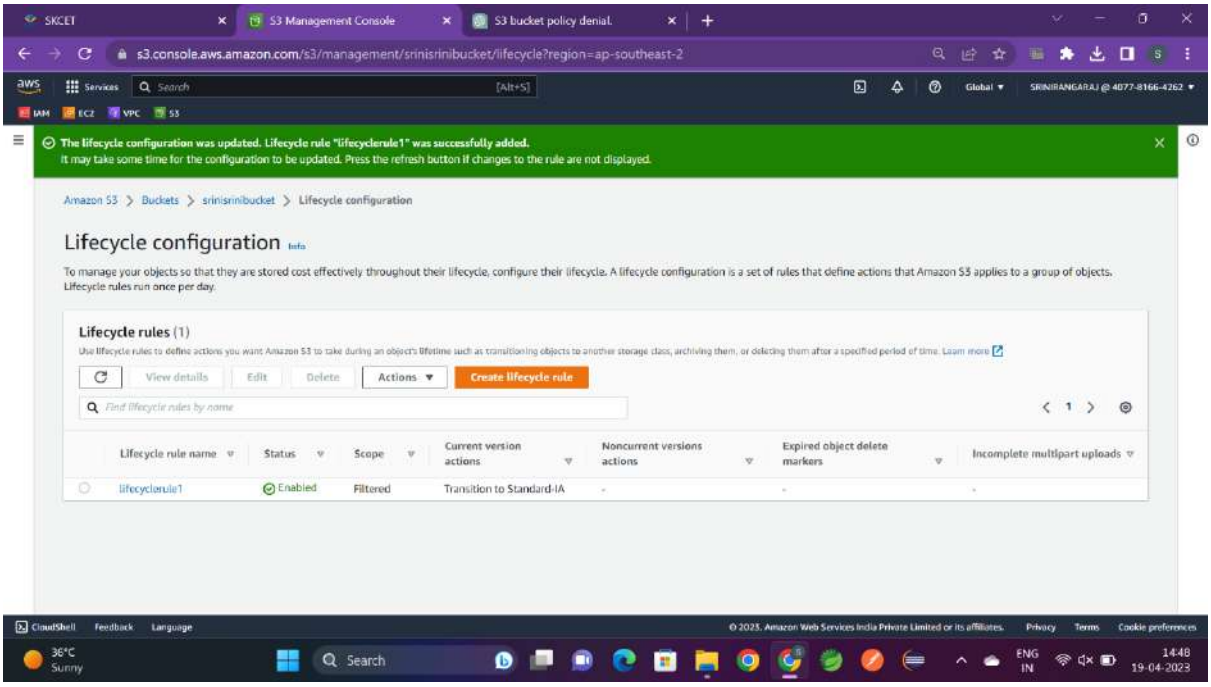
Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 buckets. With versioning, you can easily recover from both unintended user actions and application failures. Learn more

Bucket Versioning: Enabled

Multi-factor authentication (MFA) delete

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



s3.console.aws.amazon.com/s3/management/srinisrinibucket/lifecycle?region=ap-southeast-2

The lifecycle configuration was updated. Lifecycle rule "lifecyclerule1" was successfully added.
It may take some time for the configuration to be updated. Press the refresh button if changes to the rule are not displayed.

Amazon S3 > Buckets > srinisrinibucket > Lifecycle configuration

Lifecycle configuration

To manage your objects so that they are stored cost effectively throughout their lifecycle, configure their lifecycle. A lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects. Lifecycle rules run once per day.

Lifecycle rules (1)

Use lifecycle rules to define actions you want Amazon S3 to take during an object's lifetime such as transitioning objects to another storage class, archiving them, or deleting them after a specified period of time. Learn more

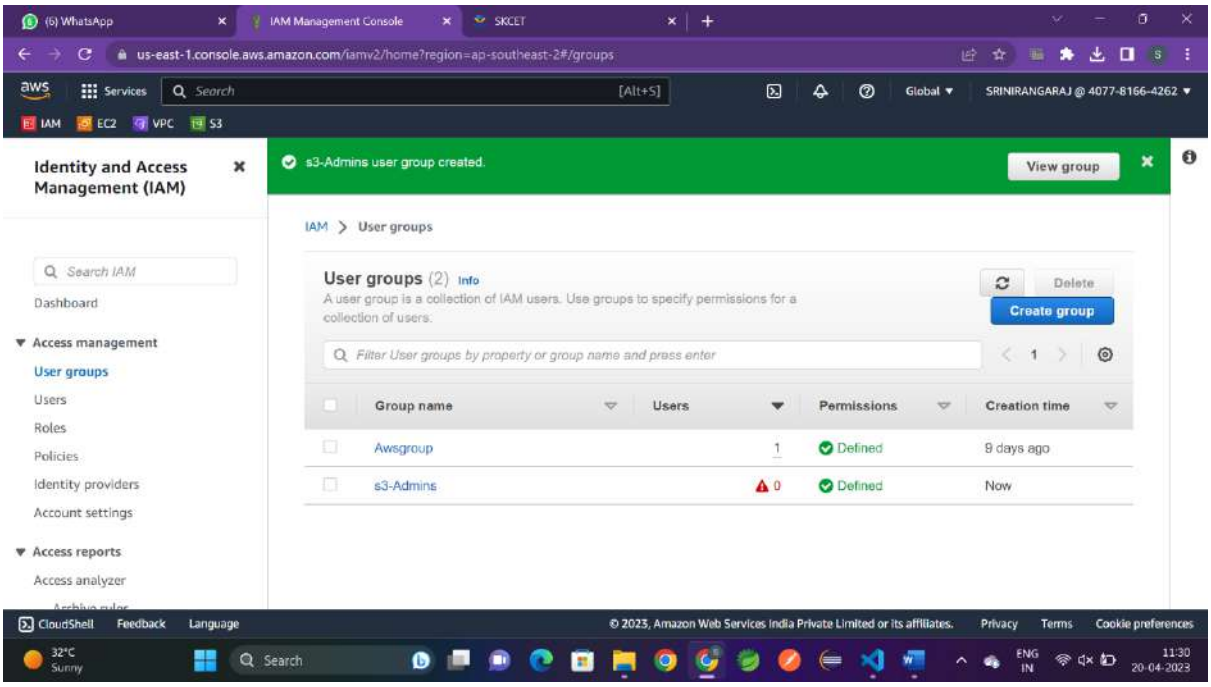
	Lifecycle rule name	Status	Scope	Current version actions	Noncurrent versions actions	Expired object delete markers	Incomplete multipart uploads
○	lifecyclerule1	✓ Enabled	Filtered	Transition to Standard-IA	-	-	-

CLOUD COMPUTING

NAME : SRINI R
ROLL NO : 727721EUCS152

DAY-4:

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



s3-Admins user group created.

IAM > User groups

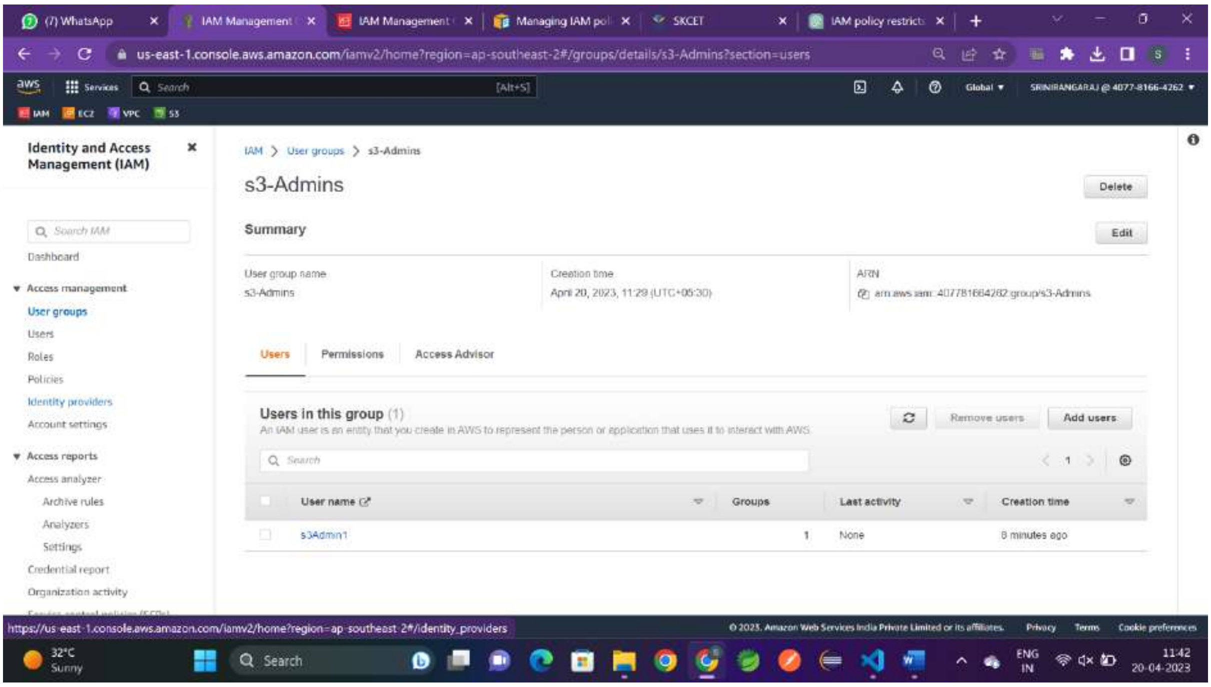
User groups (2) Info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Filter User groups by property or group name and press enter

Group name	Users	Permissions	Creation time
Awsgroup	1	Defined	9 days ago
s3-Admins	0	Defined	Now

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



IAM > User groups > s3-Admins

s3-Admins

Summary

User group name: s3-Admins

Creation time: April 20, 2023, 11:29 (UTC+05:30)

ARN: arn:aws:iam::407781664262:group/s3-Admins

Users in this group (1)

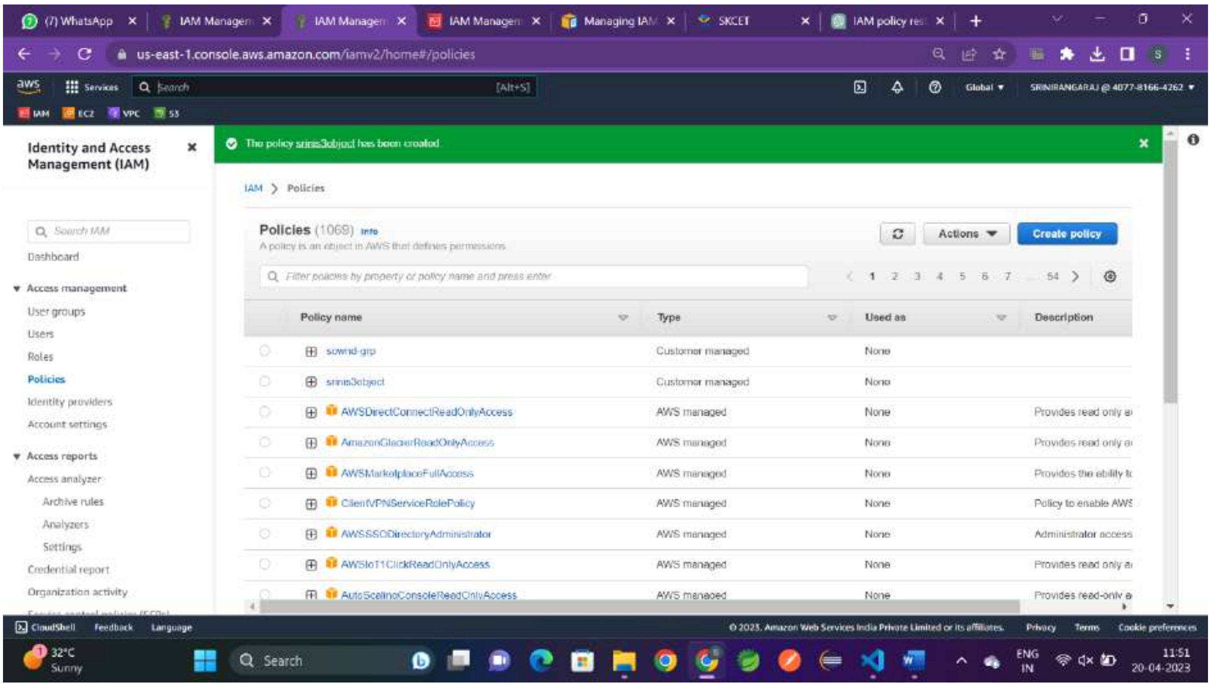
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

User name	Groups	Last activity	Creation time
s3Admin1	1	None	8 minutes ago

CLOUD COMPUTING

NAME : SRINI R
ROLL NO : 727721EUCS152

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



us-east-1.console.aws.amazon.com/iamv2/home#/policies

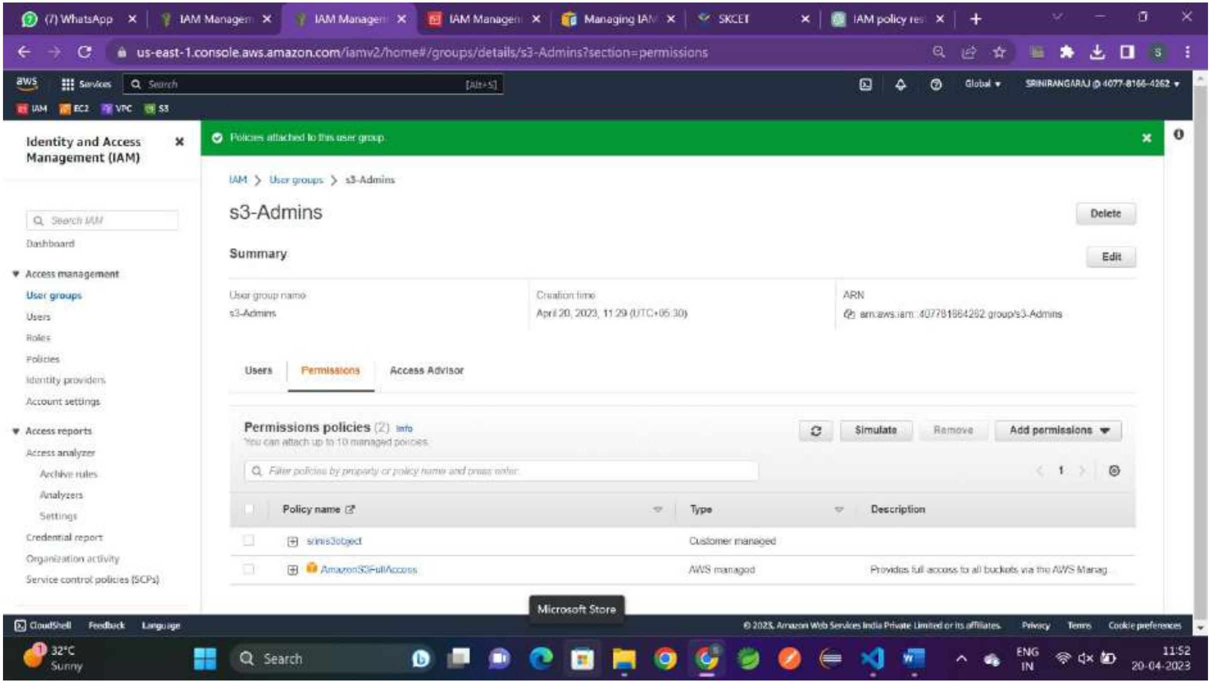
The policy srinis3object has been created

IAM > Policies

Policies (1069) Info

A policy is an object in AWS that defines permissions

	Policy name	Type	Used as	Description
○	sownd-grp	Customer managed	None	
○	srinis3object	Customer managed	None	
○	AWSDirectConnectReadOnlyAccess	AWS managed	None	Provides read only a
○	AmazonGlacierReadOnlyAccess	AWS managed	None	Provides read only a
○	AWSMarketplaceFullAccess	AWS managed	None	Provides the ability t
○	ClientVPNServiceRolePolicy	AWS managed	None	Policy to enable AWS
○	AWSSSODirectoryAdministrator	AWS managed	None	Administrator access
○	AWSIoT1ClickReadOnlyAccess	AWS managed	None	Provides read only a
○	AutoScalingConsoleReadOnlyAccess	AWS managed	None	Provides read-only a



us-east-1.console.aws.amazon.com/iamv2/home#/groups/details/s3-Admins?section=permissions

Policies attached to this user group.

IAM > User groups > s3-Admins

s3-Admins

Summary

User group name	Creation time	ARN
s3-Admins	April 20, 2023, 11:29 (UTC+05:30)	arn:aws:iam::407781864262:group/s3-Admins

Permissions policies (2) Info

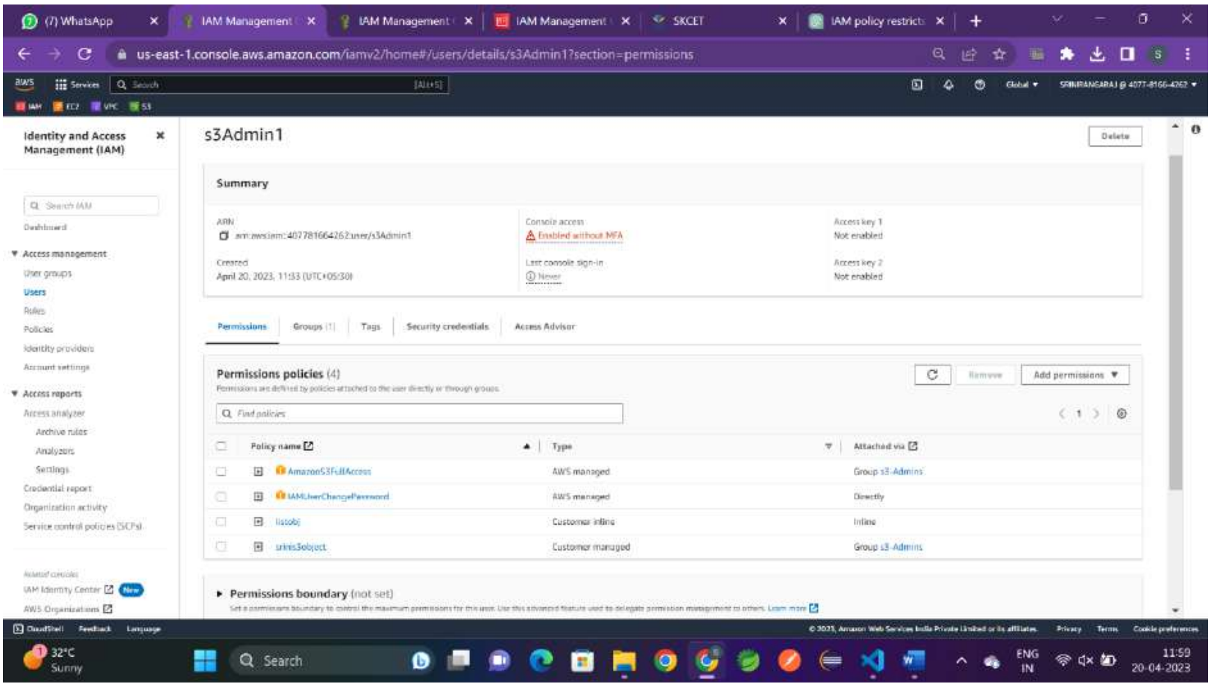
You can attach up to 10 managed policies.

	Policy name	Type	Description
□	srinis3object	Customer managed	
□	AmazonS3FullAccess	AWS managed	Provides full access to all buckets via the AWS Manag

CLOUD COMPUTING

NAME : SRINI R
ROLL NO : 727721EUCS152

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



us-east-1.console.aws.amazon.com/iamv2/home#/users/details/s3Admin1?section=permissions

s3Admin1

Summary

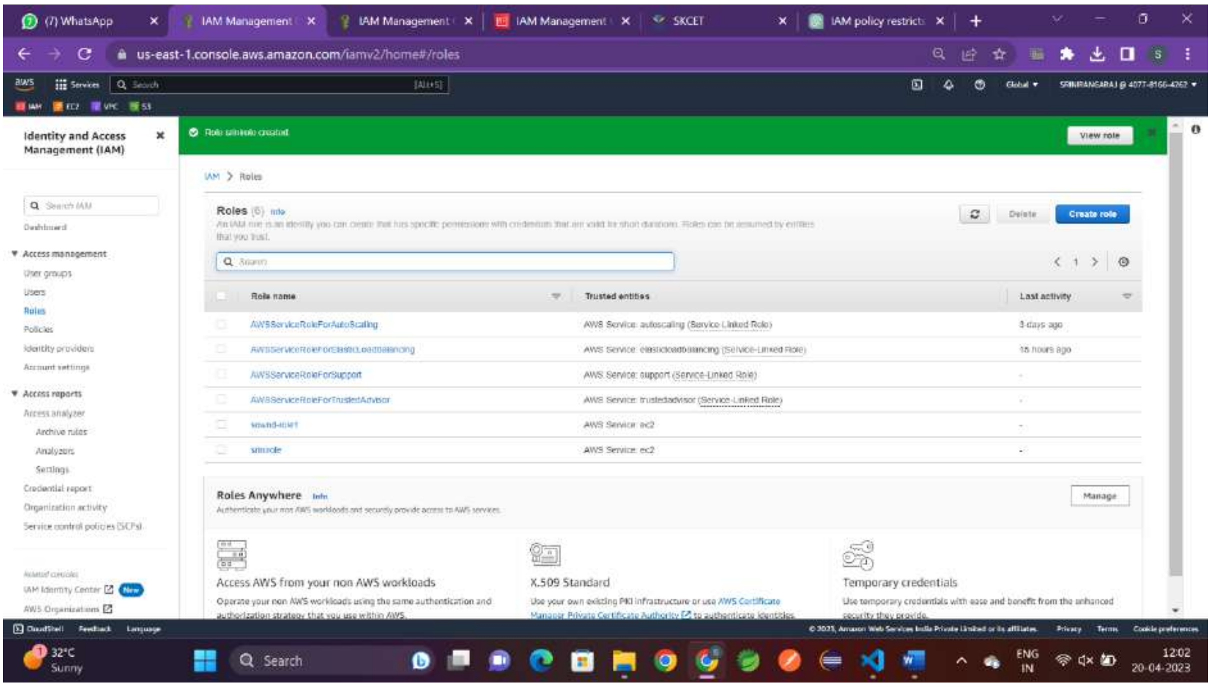
ARN: arn:aws:iam::407781664262:user/s3Admin1
Created: April 20, 2023, 11:53 (UTC+05:30)
Console access: Enabled without MFA
Last console sign-in: Never
Access key 1: Not enabled
Access key 2: Not enabled

Permissions policies (4)

Policy name	Type	Attached via
AmazonS3FullAccess	AWS managed	Group s3-Admins
IAMUserChangePassword	AWS managed	Directly
listobj	Customer inline	Inline
srinis3object	Customer managed	Group s3-Admins

Permissions boundary (not set)

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



us-east-1.console.aws.amazon.com/iamv2/home#/roles

Role srinirole created

IAM > Roles

Roles (6)

Role name	Trusted entities	Last activity
AWSServiceRoleForAutoScaling	AWS Service: autoscaling (Service-Linked Role)	3 days ago
AWSServiceRoleForElasticLoadBalancing	AWS Service: elasticloadbalancing (Service-Linked Role)	18 hours ago
AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-
[illegible]	AWS Service: ec2	-
srinirole	AWS Service: ec2	-

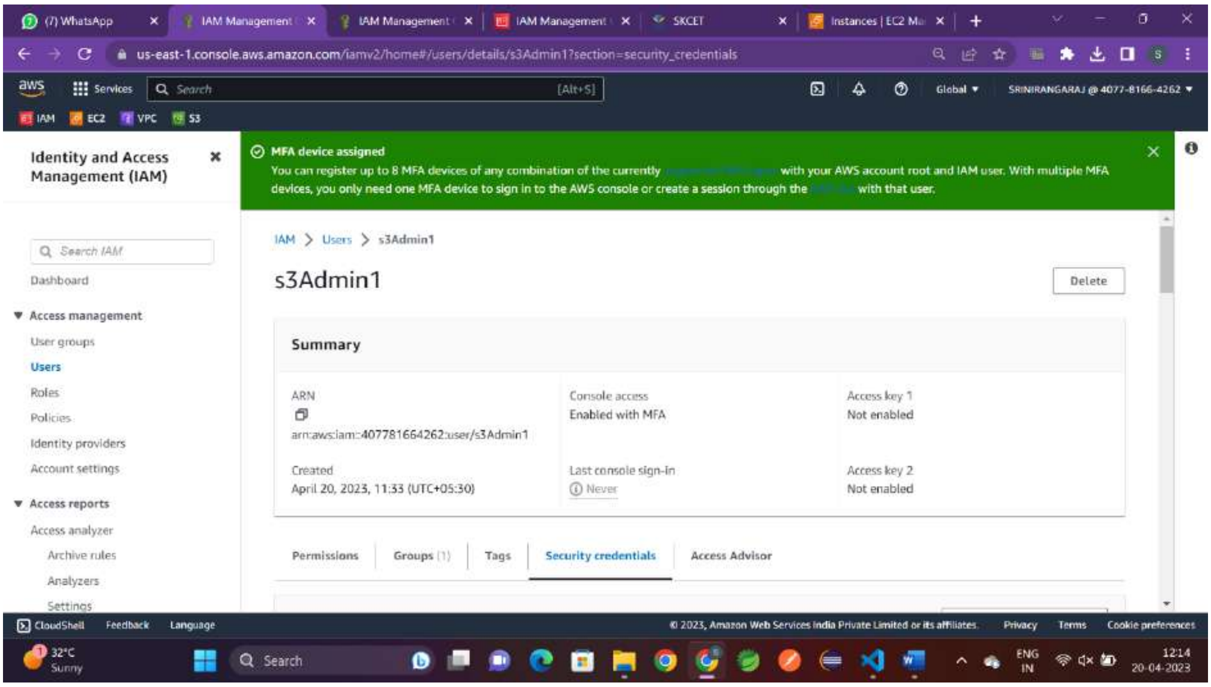
Roles Anywhere

Access AWS from your non AWS workloads
X.509 Standard
Temporary credentials

CLOUD COMPUTING

NAME : SRINI R
ROLL NO : 727721EUCS152

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



us-east-1.console.aws.amazon.com/iamv2/home#/users/details/s3Admin1?section=security_credentials

MFA device assigned
You can register up to 8 MFA devices of any combination of the currently [illegible] 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 [illegible] with that user.

IAM > Users > s3Admin1

s3Admin1

Summary

ARN
arn:aws:iam::407781664262:user/s3Admin1

Created
April 20, 2023, 11:33 (UTC+05:30)

Console access
Enabled with MFA

Last console sign-in
Never

Access key 1
Not enabled

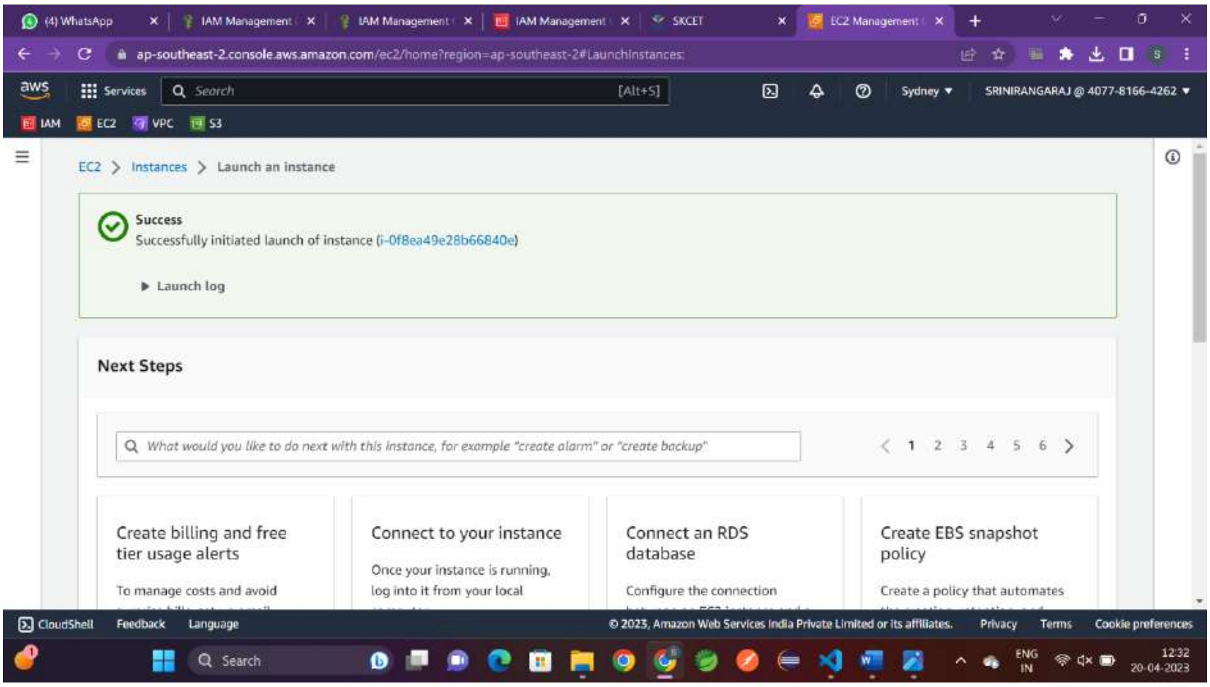
Access key 2
Not enabled

CLOUD COMPUTING

NAME : SRINI R
ROLL NO : 727721EUCS152

DAY-5:

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

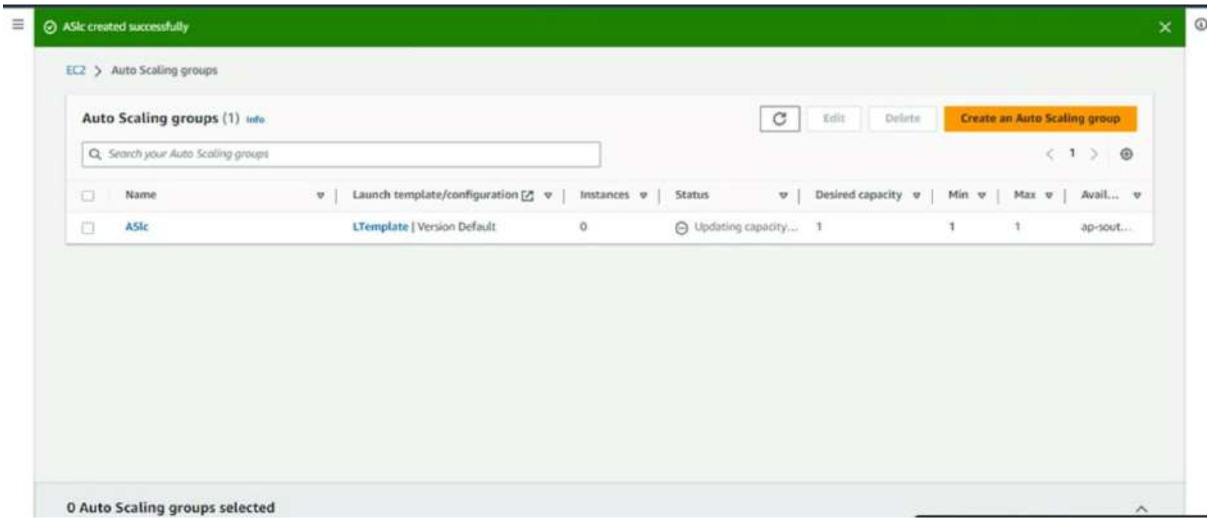


EC2 > Instances > Launch an instance

Success
Successfully initiated launch of instance (i-0f8ea49e28b66840e)

Launch log
Next Steps
What would you like to do next with this instance, for example "create alarm" or "create backup"
Create billing and free tier usage alerts
To manage costs and avoid
Connect to your instance
Once your instance is running, log into it from your local
Connect an RDS database
Configure the connection
Create EBS snapshot policy
Create a policy that automates

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



ASlc created successfully

EC2 > Auto Scaling groups
Auto Scaling groups (1) Info
Edit
Delete
Create an Auto Scaling group
Search your Auto Scaling groups

	Name	Launch template/configuration	Instances	Status	Desired capacity	Min	Max	Avail...
□	ASlc	LTemplate | Version Default	0	Updating capacity...	1	1	1	ap-sout...

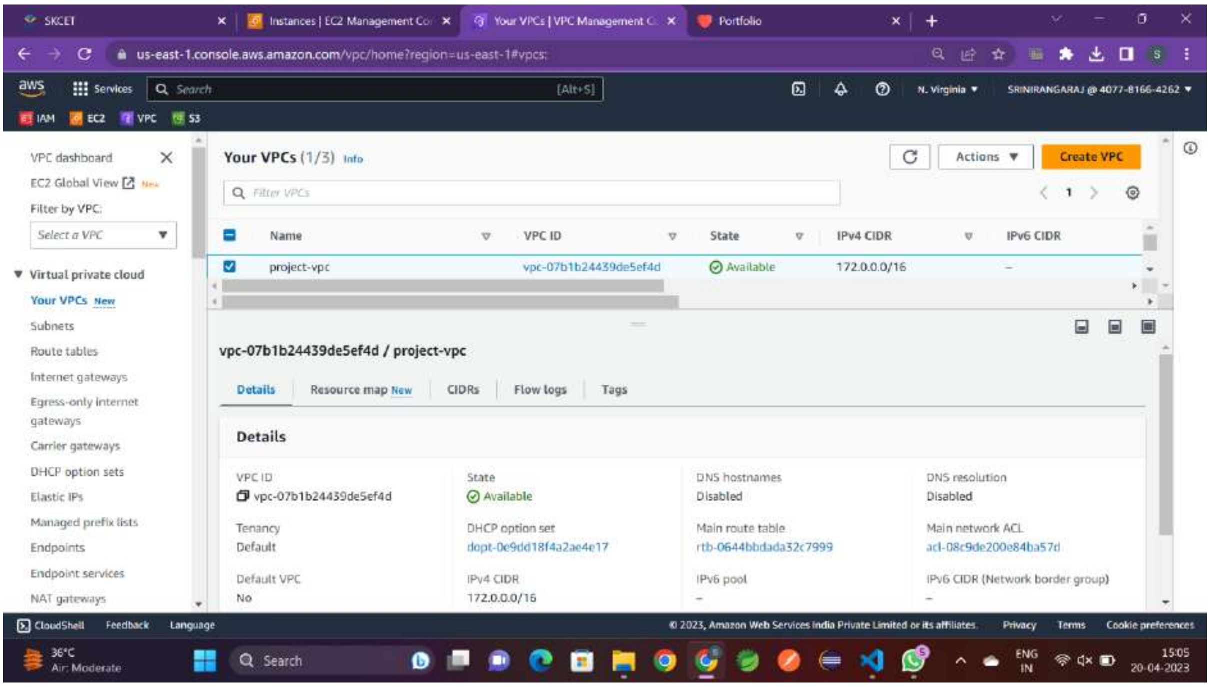
0 Auto Scaling groups selected

CLOUD COMPUTING

NAME : SRINI R
ROLL NO : 727721EUCS152

DAY-6:

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



Your VPCs (1/3) Info

☑	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR
☑	project-vpc	vpc-07b1b24439de5ef4d	✓ Available	172.0.0.0/16	–

vpc-07b1b24439de5ef4d / project-vpc

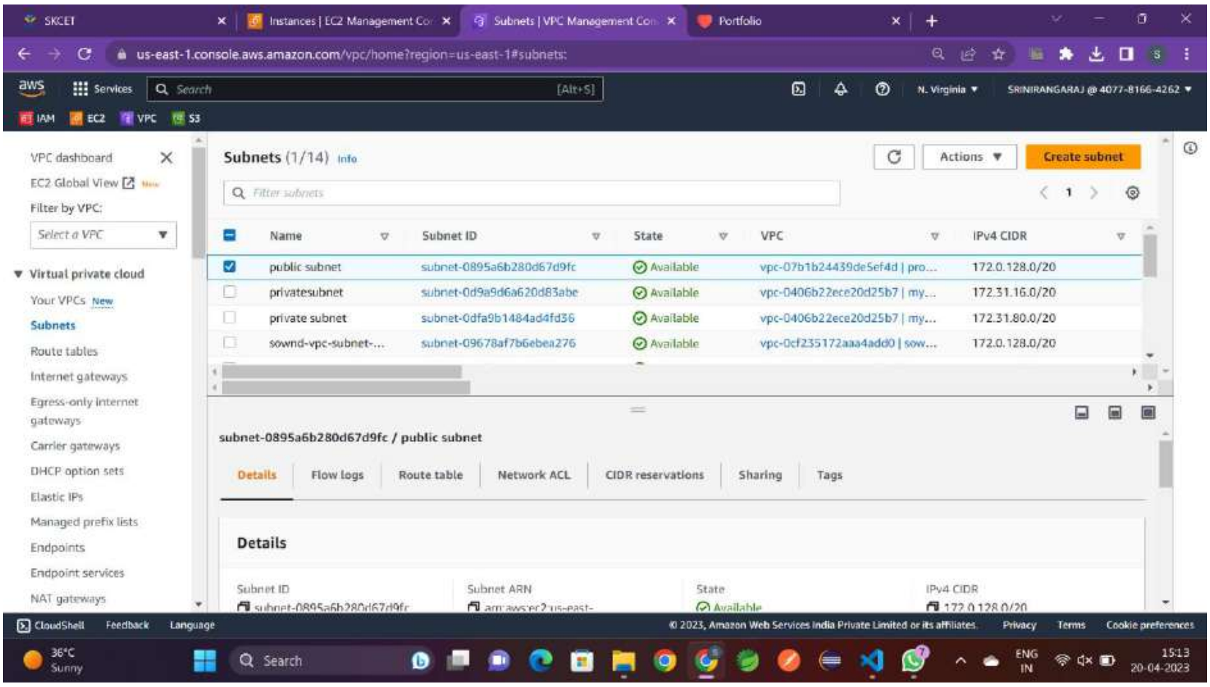
Details

VPC ID vpc-07b1b24439de5ef4d	State ✓ Available	DNS hostnames Disabled	DNS resolution Disabled
Tenancy Default	DHCP option set dopt-0e9dd18f4a2ae4e17	Main route table rtb-0644bbdada32c7999	Main network ACL acl-08c9de200e84ba57d
Default VPC No	IPv4 CIDR 172.0.0.0/16	IPv6 pool –	IPv6 CIDR (Network border group) –

CLOUD COMPUTING

NAME : SRINI R
ROLL NO : 727721EUCS152

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

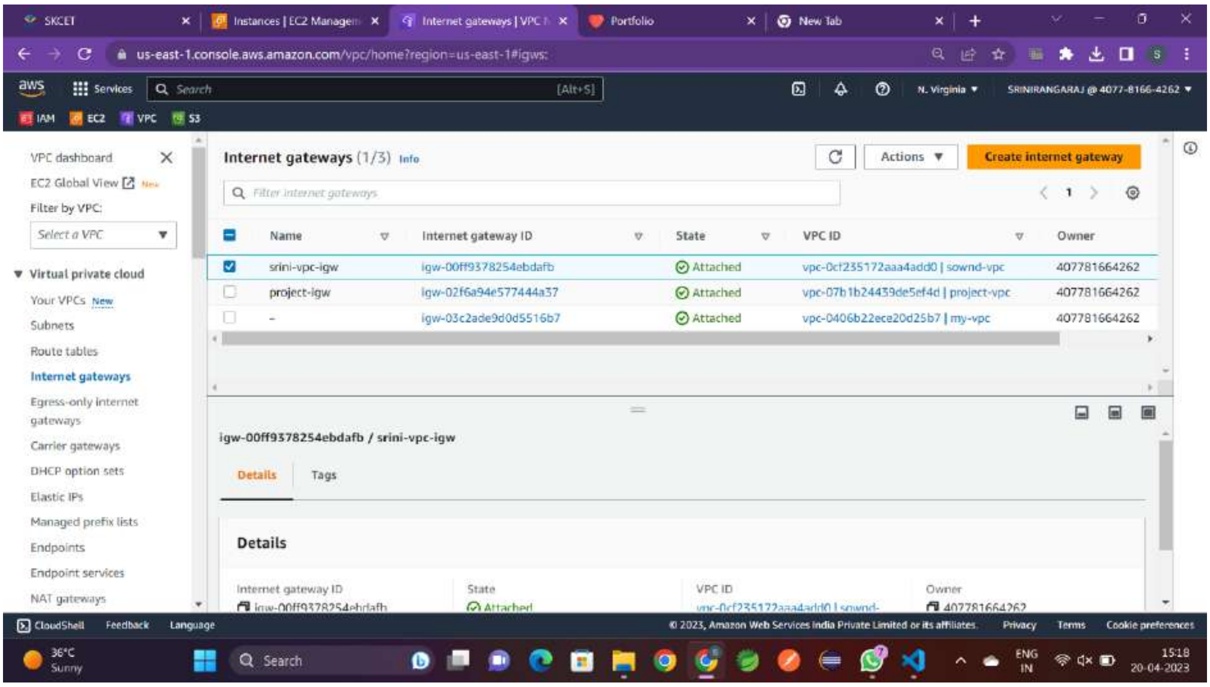


Subnets (1/14)

☐	Name	Subnet ID	State	VPC	IPv4 CIDR
☑	public subnet	subnet-0895a6b280d67d9fc	Available	vpc-07b1b24439de5ef4d | pro...	172.0.128.0/20
☐	privatesubnet	subnet-0d9a9d6a620d83abe	Available	vpc-0406b22ece20d25b7 | my...	172.31.16.0/20
☐	private subnet	subnet-0dfa9b1484ad4fd36	Available	vpc-0406b22ece20d25b7 | my...	172.31.80.0/20
☐	sownd-vpc-subnet-...	subnet-09678af7b6ebea276	Available	vpc-0cf235172aaa4add0 | sow...	172.0.128.0/20

subnet-0895a6b280d67d9fc / public subnet

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



Internet gateways (1/3)

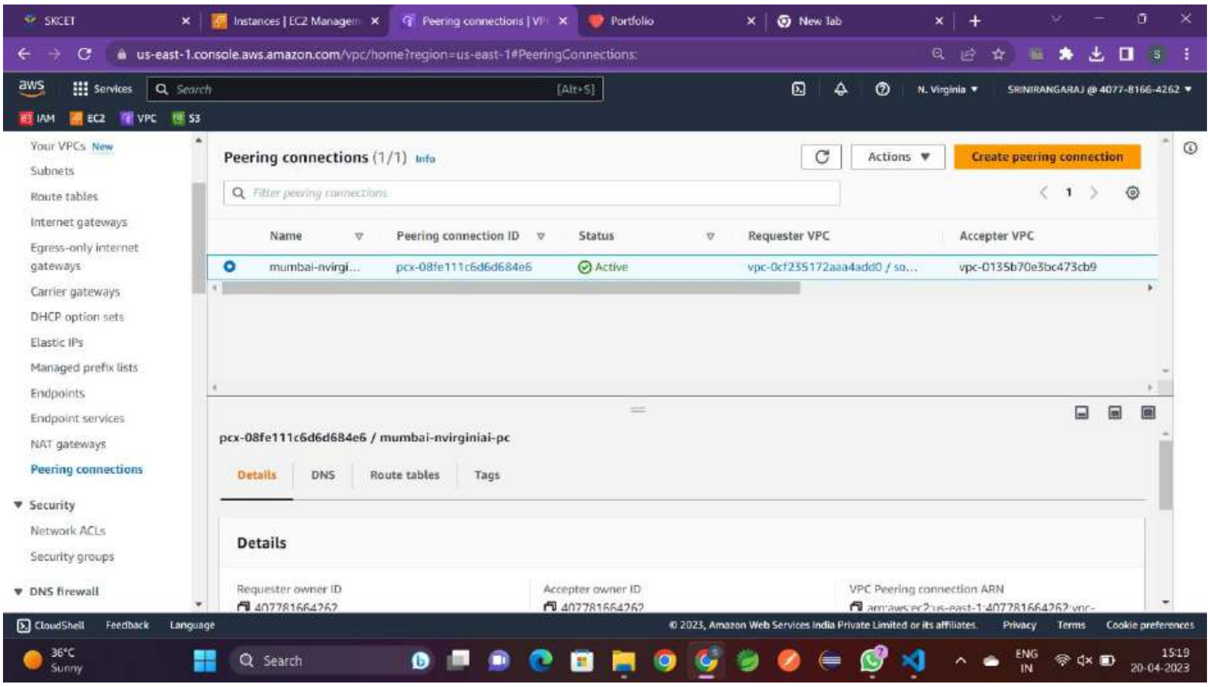
☐	Name	Internet gateway ID	State	VPC ID	Owner
☑	srini-vpc-igw	igw-00ff9378254ebdafb	Attached	vpc-0cf235172aaa4add0 | sownd-vpc	407781664262
☐	project-igw	igw-02f6a94e577444a37	Attached	vpc-07b1b24439de5ef4d | project-vpc	407781664262
☐	–	igw-03c2ade9d0d5516b7	Attached	vpc-0406b22ece20d25b7 | my-vpc	407781664262

igw-00ff9378254ebdafb / srini-vpc-igw

CLOUD COMPUTING

NAME : SRINI R
ROLL NO : 727721EUCS152

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



us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#PeeringConnections:

Peering connections (1/1)

	Name	Peering connection ID	Status	Requester VPC	Accepter VPC
●	mumbai-nvirgi...	pcx-08fe111c6d6d684e6	Active	vpc-0cf235172aaa4add0 / so...	vpc-0135b70e3bc473cb9

pcx-08fe111c6d6d684e6 / mumbai-nvirginiai-pc

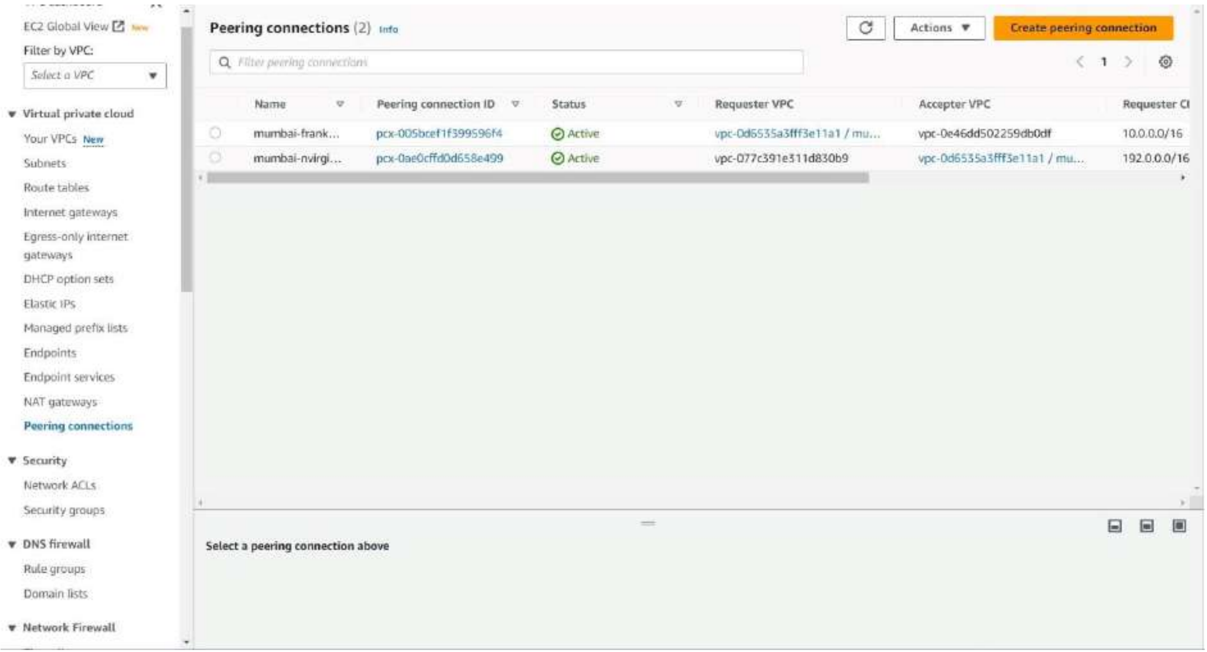
Details

Requester owner ID	Accepter owner ID	VPC Peering connection ARN
407781664262	407781664262	arn:aws:ec2:us-east-1:407781664262:vpc-

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

CLOUD COMPUTING

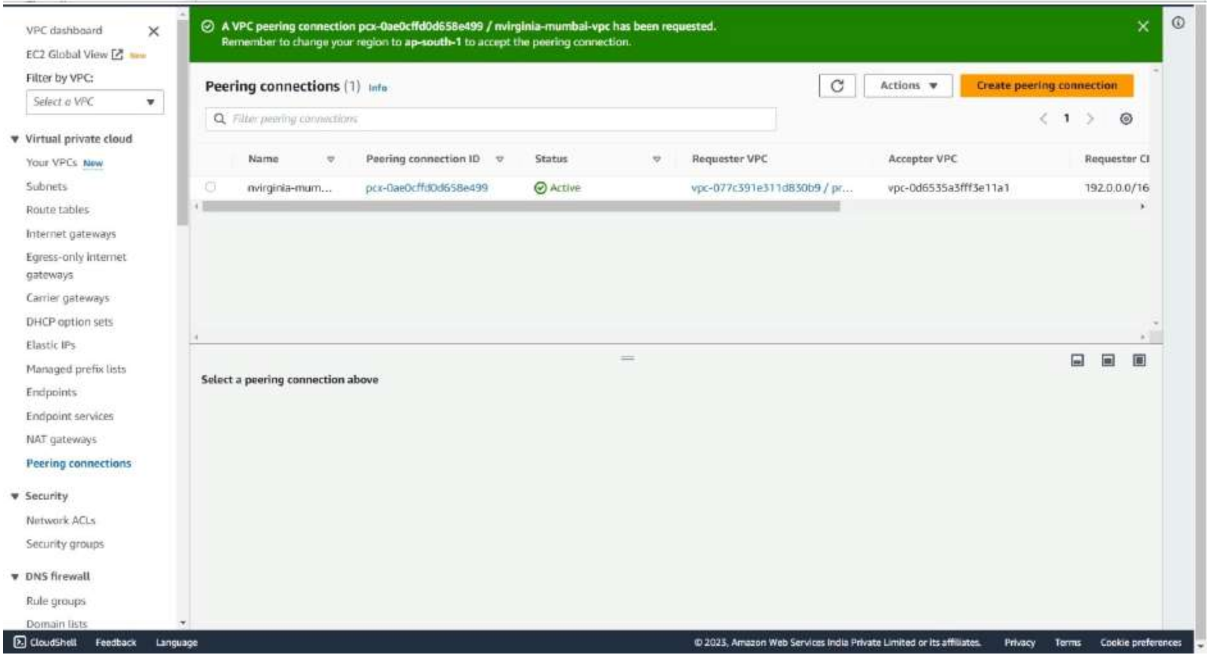
NAME : SRINI R
ROLL NO : 727721EUCS152



Peering connections (2) Info

	Name	Peering connection ID	Status	Requester VPC	Accepter VPC	Requester CI
○	mumbai-frank...	pcx-005bcef1f399596f4	✓ Active	vpc-0d6535a3fff3e11a1 / mu...	vpc-0e46dd502259db0df	10.0.0.0/16
○	mumbai-nvirgi...	pcx-0ae0cffd0d658e499	✓ Active	vpc-077c391e311d830b9	vpc-0d6535a3fff3e11a1 / mu...	192.0.0.0/16

Select a peering connection above



A VPC peering connection pcx-0ae0cffd0d658e499 / nvirginia-mumbai-vpc has been requested.
Remember to change your region to **ap-south-1** to accept the peering connection.

Peering connections (1) Info

	Name	Peering connection ID	Status	Requester VPC	Accepter VPC	Requester CI
○	nvirginia-mum...	pcx-0ae0cffd0d658e499	✓ Active	vpc-077c391e311d830b9 / pr...	vpc-0d6535a3fff3e11a1	192.0.0.0/16

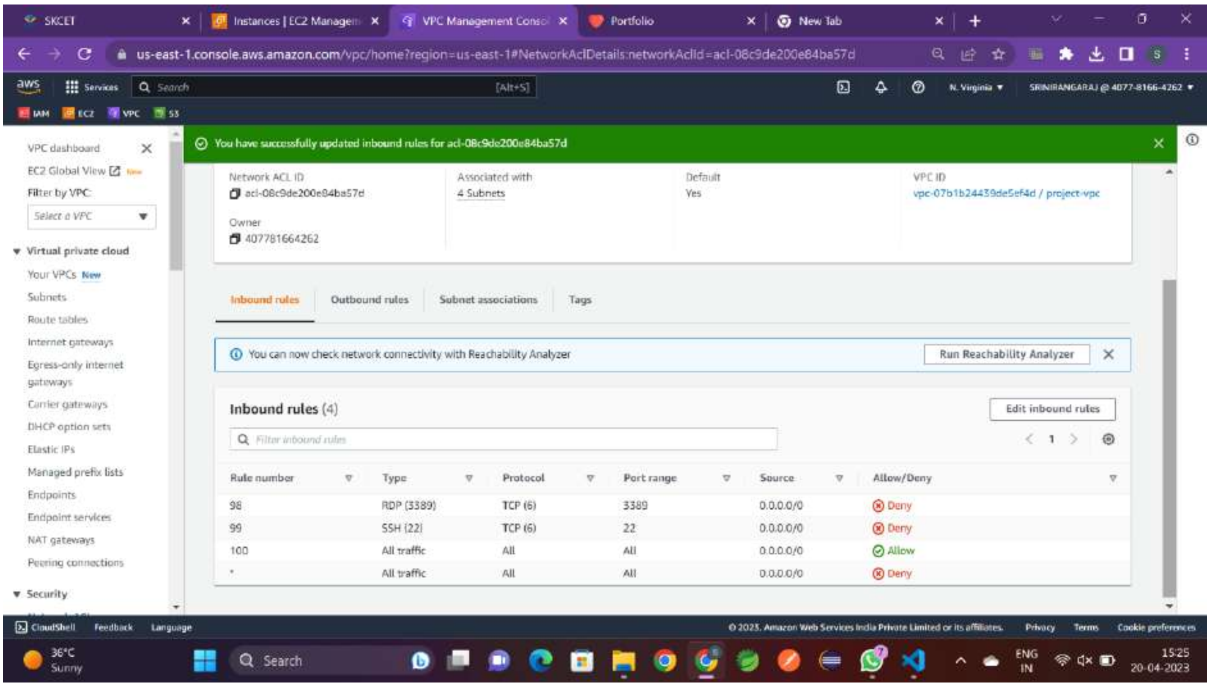
Select a peering connection above

© 2023, Amazon Web Services India Private Limited or its affiliates.

CLOUD COMPUTING

NAME : SRINI R
ROLL NO : 727721EUCS152

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



You have successfully updated inbound rules for acl-08c9de200e84ba57d

Network ACL ID: acl-08c9de200e84ba57d
Associated with: 4 Subnets
Default: Yes
VPC ID: vpc-07b1b24439de5ef4d / project-vpc
Owner: 407781664262

You can now check network connectivity with Reachability Analyzer

Inbound rules (4)

Rule number	Type	Protocol	Port range	Source	Allow/Deny
98	RDP (3389)	TCP (6)	3389	0.0.0.0/0	Deny
99	SSH (22)	TCP (6)	22	0.0.0.0/0	Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#NetworkAclDetails:networkAclId=acl-08c9de200e84ba57d
Inbound rules
Outbound rules
Subnet associations
Tags
Run Reachability Analyzer
Edit inbound rules
VPC dashboard
Virtual private cloud
Security
N. Virginia
15:25
20-04-2023