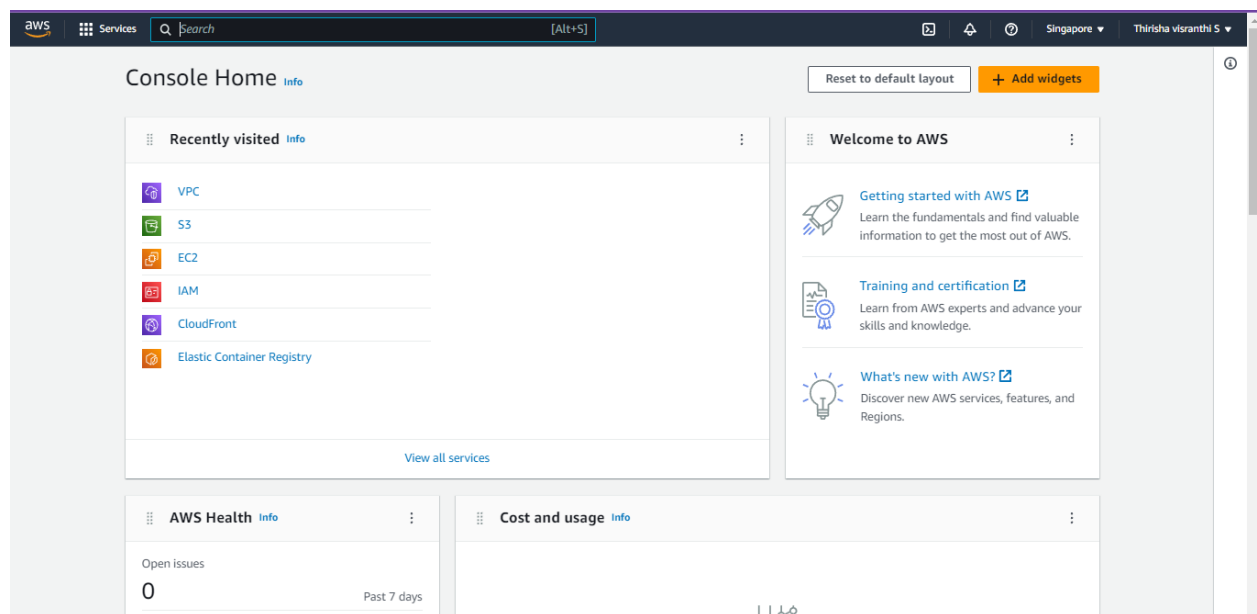


**NAME :THIRISHA VISRANTHI**  
**REG NO:727721EUCS170**

## **AMAZON CLOUD COMPUTING**

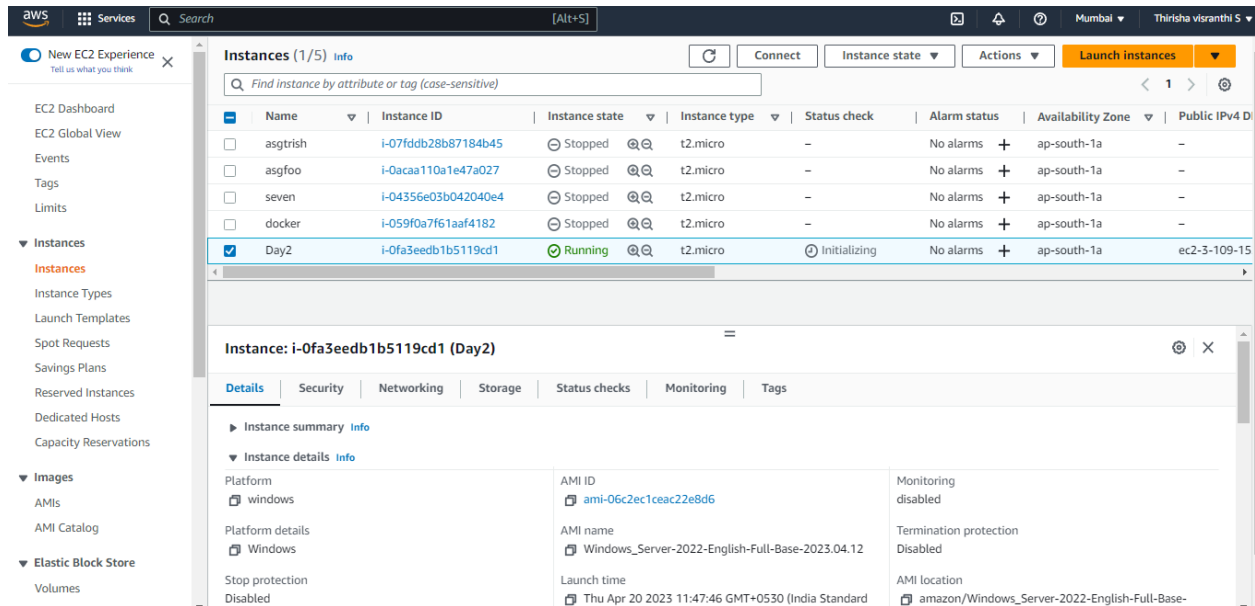
### **Day1:**

#### **1.Aws account creation:**

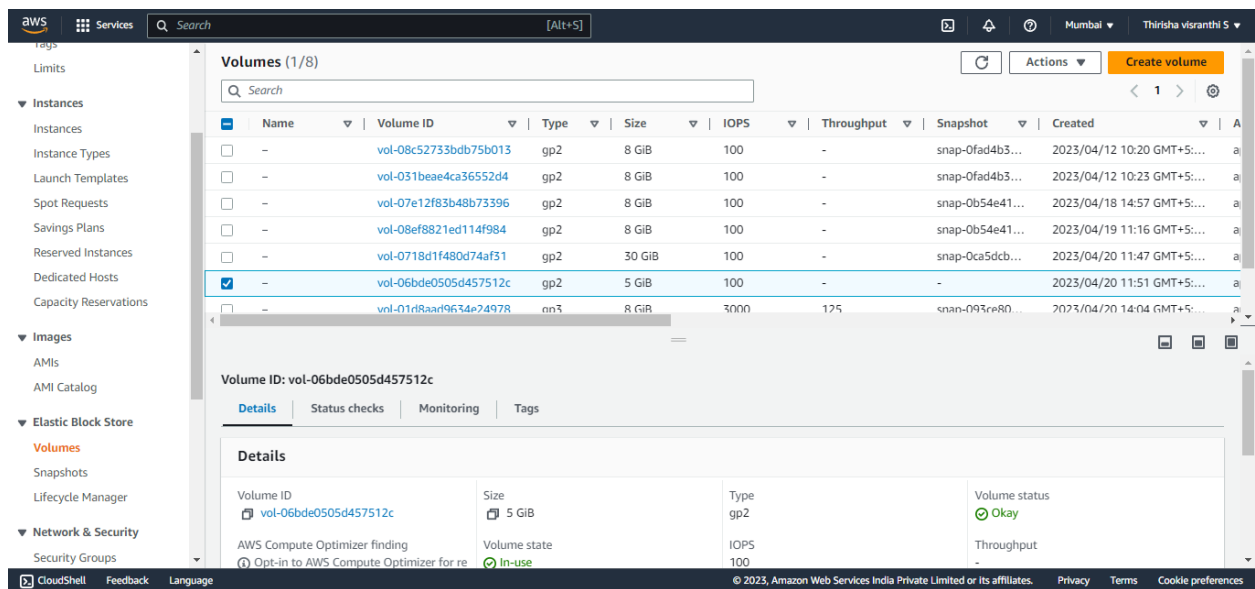


### **Day2:**

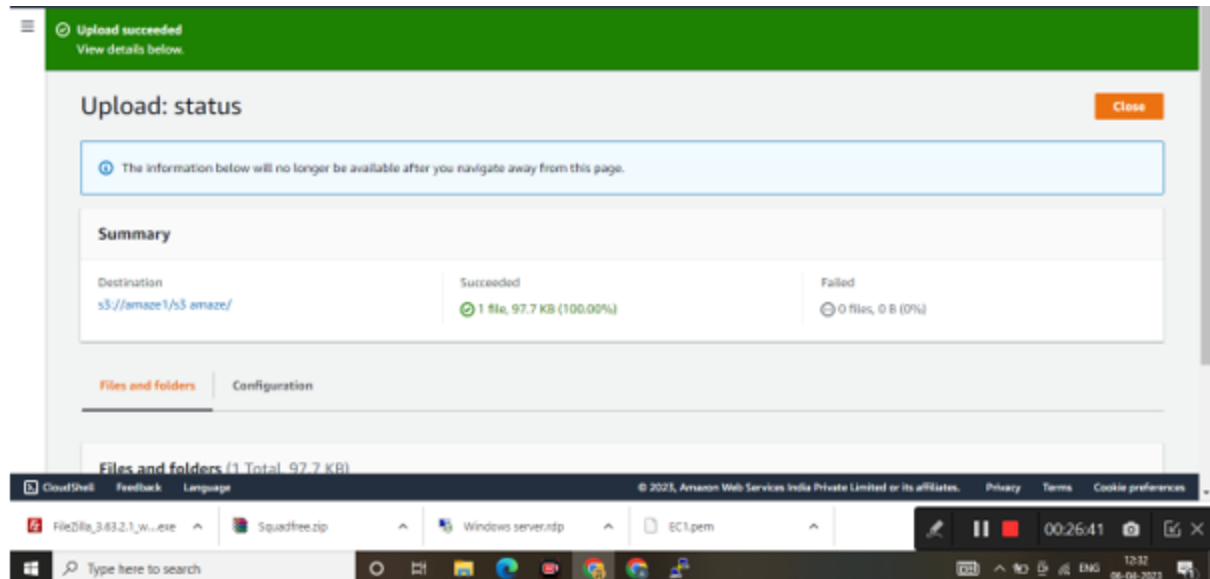
Create a Windows EC2 instance with t2.micro Instance and show the remote connection of that EC2 Instance.



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.

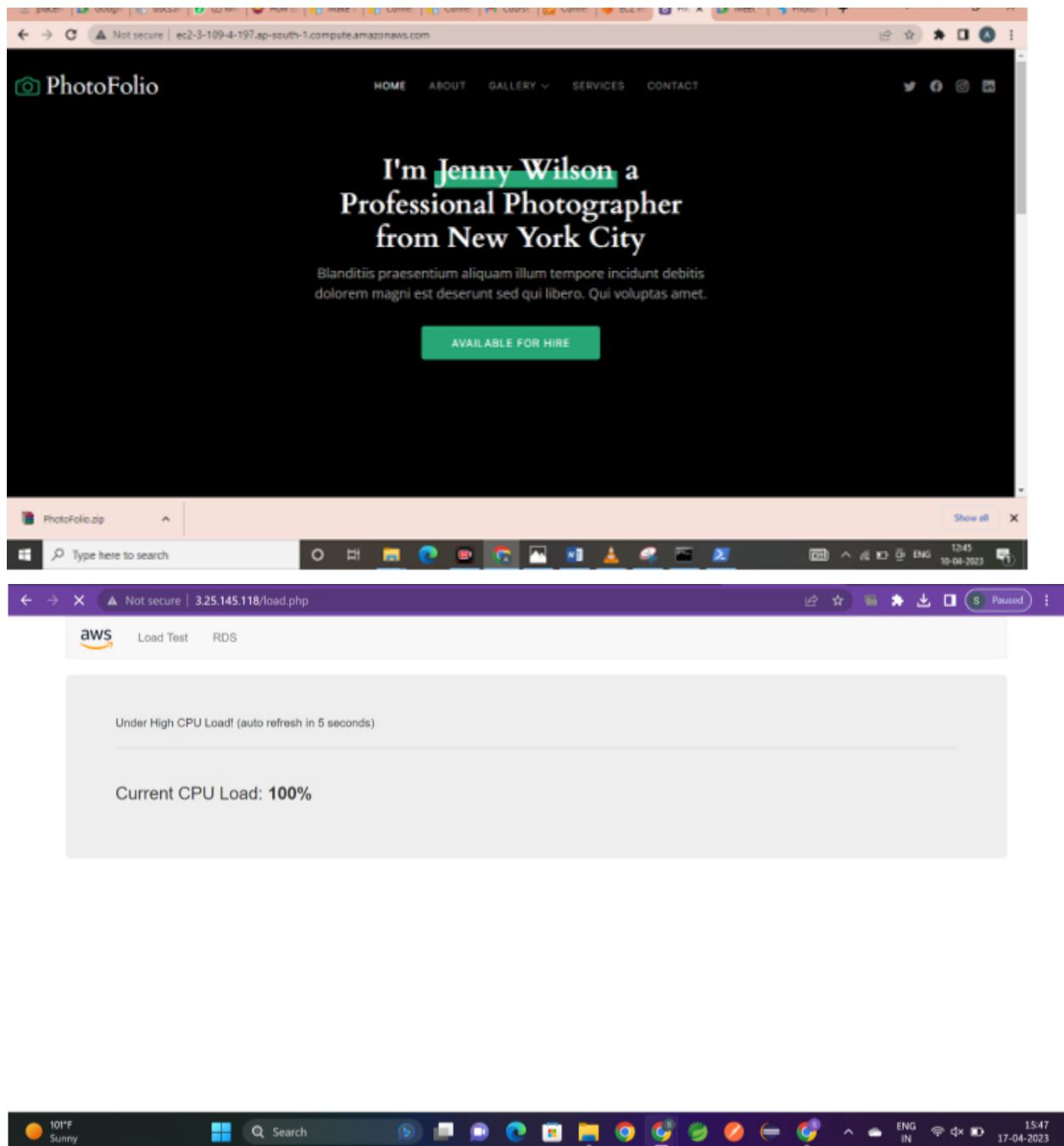


4.

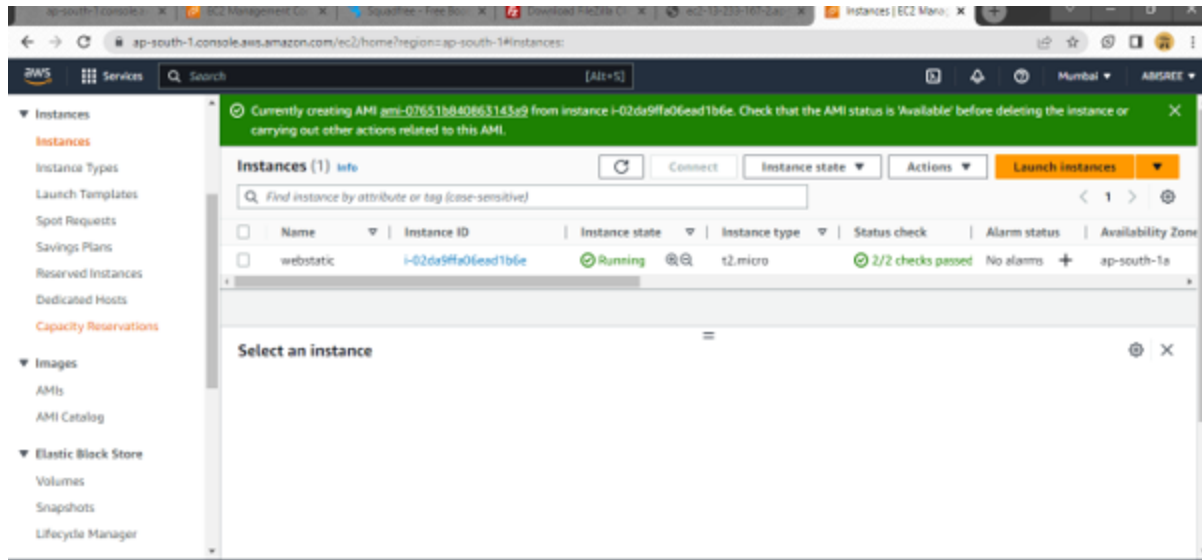
Create a Linux EC2 instance with t2.micro Instance and show the remote connection of that EC2 Instance.



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

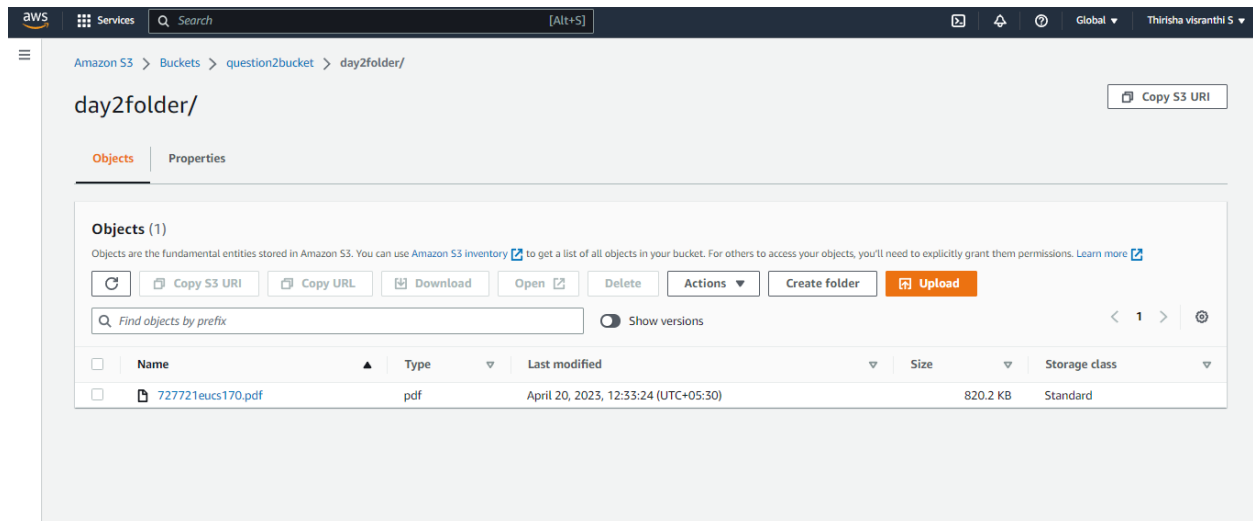


6. Create Image(MyAMI) of the linux Webserver(from the previous exercise) and launch new EC2 instance from the created Image(MyAMI)

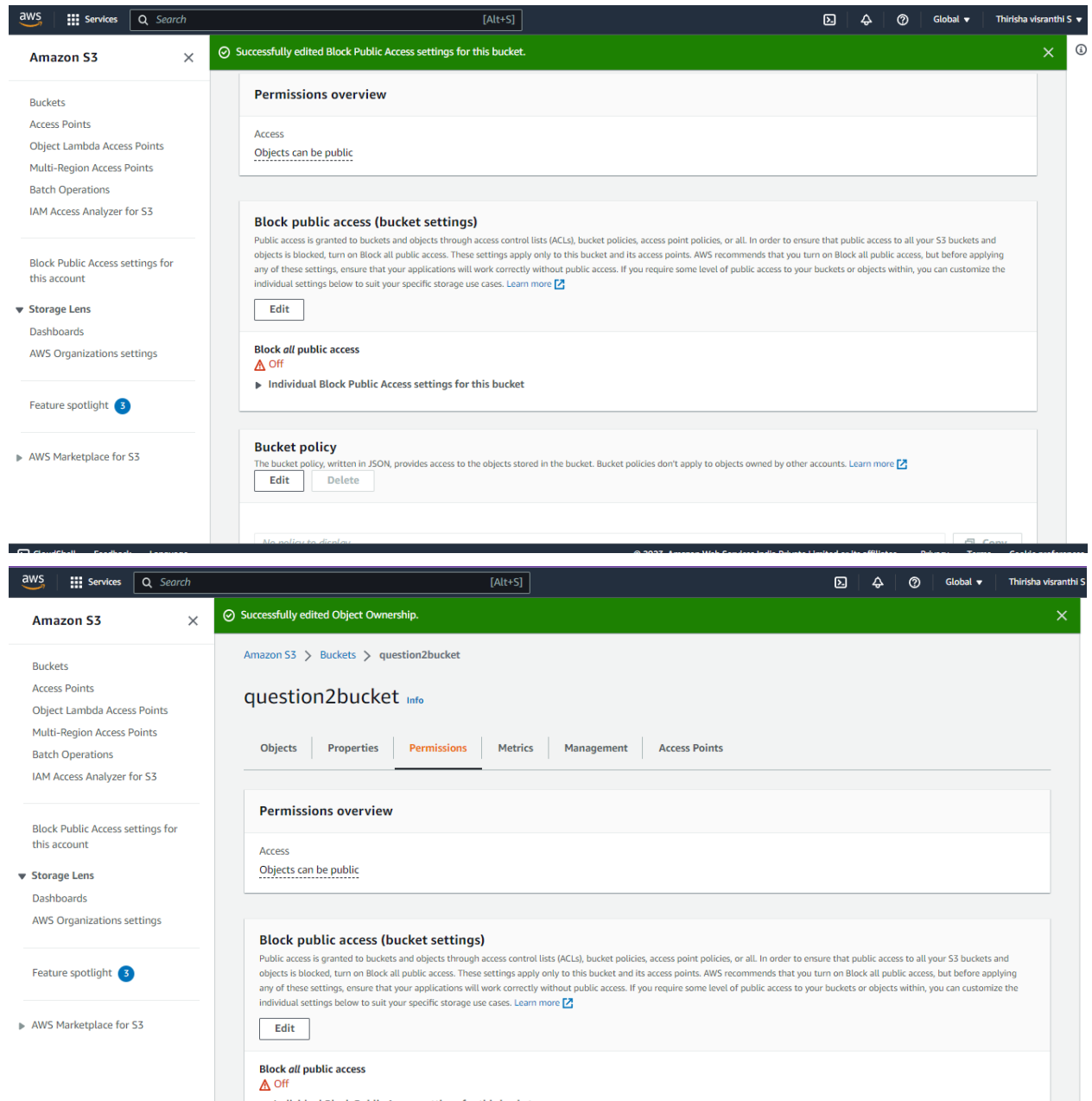


## Day3

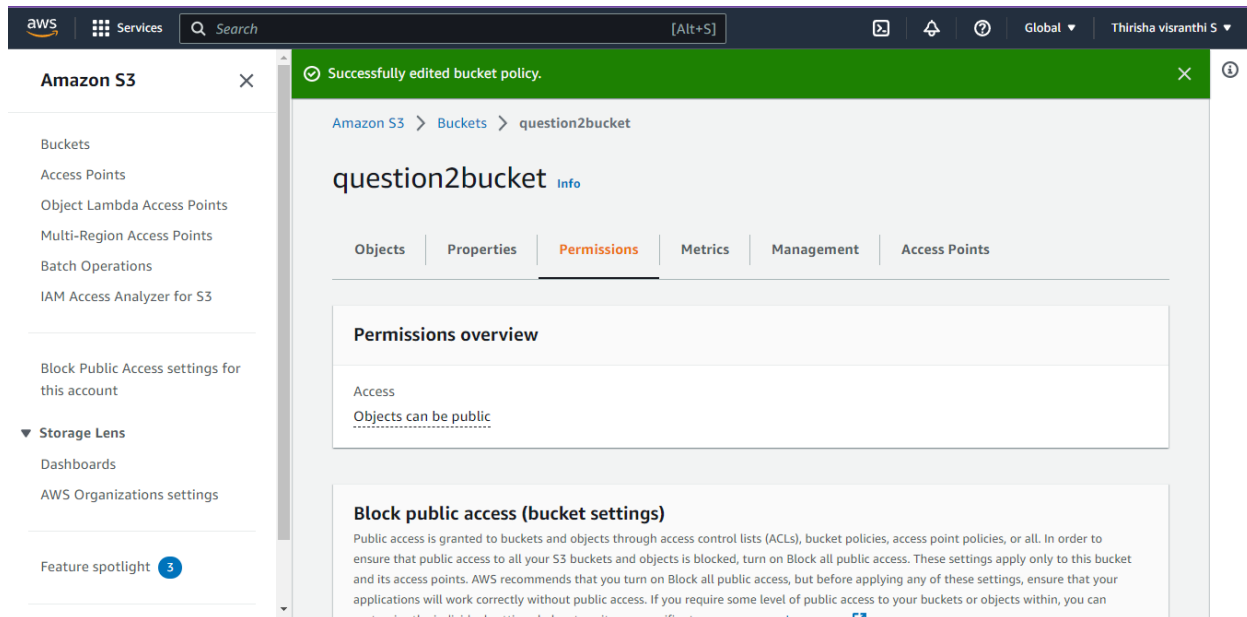
1.Create a S3 Bucket and create a folder in the bucket and upload a file in the folder.



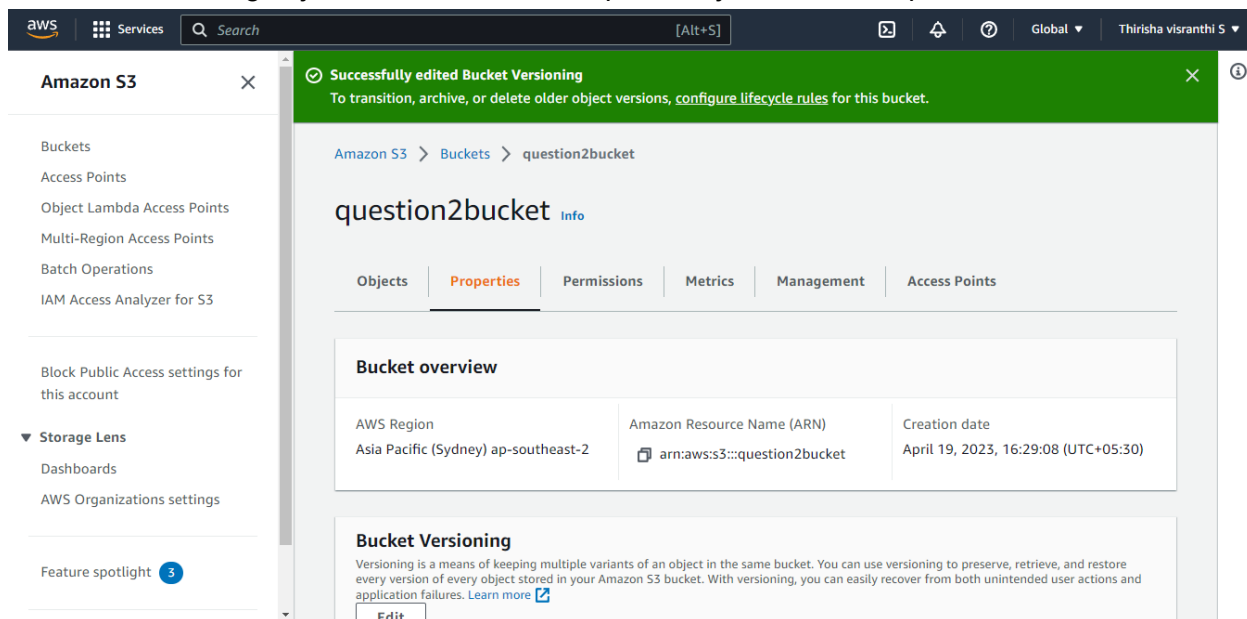
2.Disable "Block Public Access" for the bucket and enable public read access for a file.



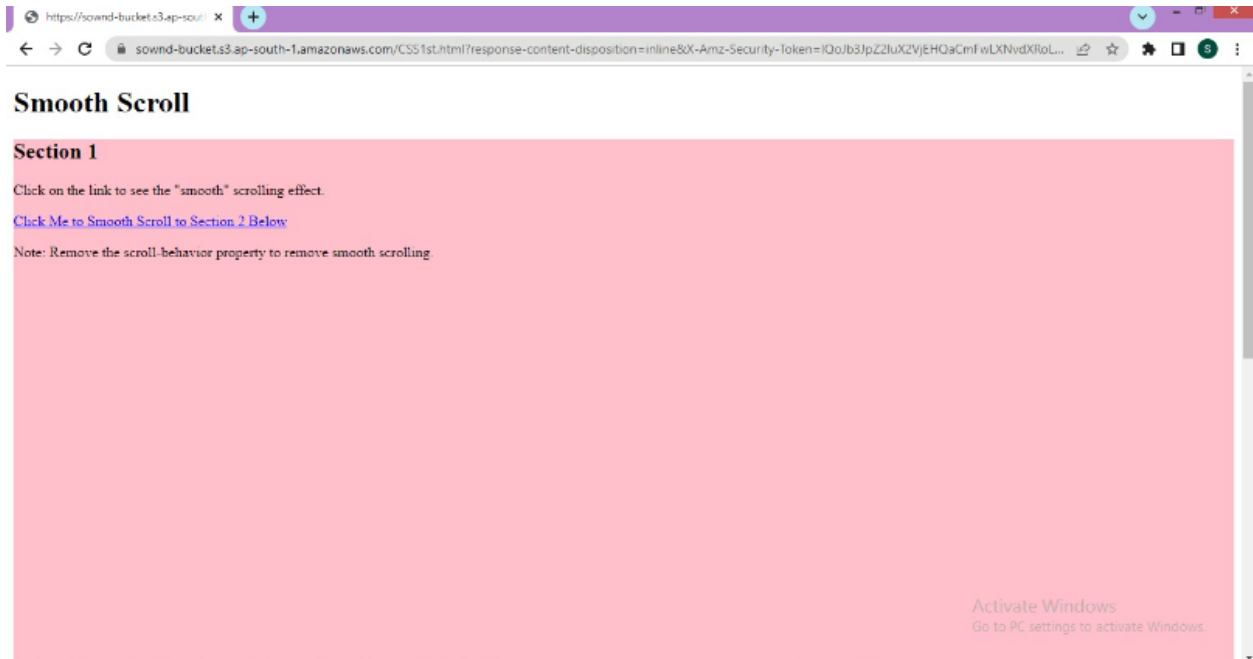
3. Create a bucket policy which should deny to read objects under a folder of a bucket.



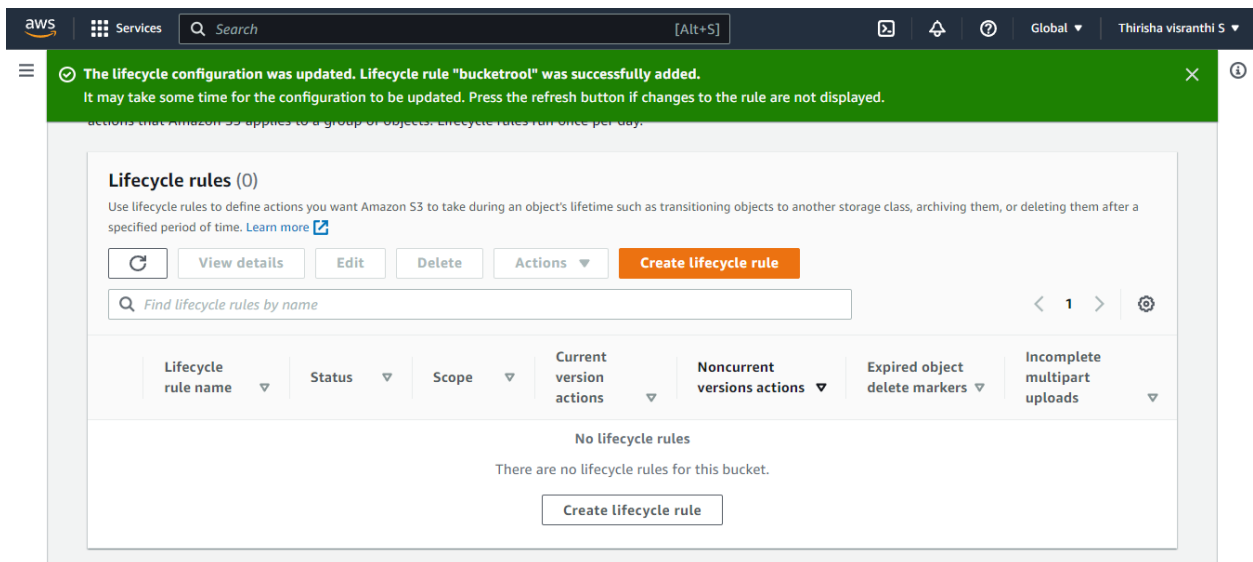
4.Enable versioning objects for a bucket and upload objects with multiple versions of it.



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'.



aws Services Search [Alt+S] Global Thirisha Visranthi S

**Identity and Access Management (IAM)**

Search IAM

Dashboard

▼ Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

▼ Access reports

- Access analyzer
- Archive rules
- Analizers
- Settings
- Credential report
- Organization activity

**S3-Admins user group created.** View group

**User groups** (3) 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
<input type="checkbox"/>	itsmine	3	Defined	10 days ago
<input type="checkbox"/>	S3-Admins	⌵ Loading	Defined	Now
<input type="checkbox"/>	safty	1	Defined	10 days ago

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

aws Services Search [Alt+S] Global Thirisha Visranthi S

**Identity and Access Management (IAM)**

Search IAM

Dashboard

▼ Access management

- User groups
- Users**
- Roles
- Policies
- Identity providers
- Account settings

▼ Access reports

- Access analyzer
- Archive rules
- Analizers
- Settings
- Credential report
- Organization activity

**User created successfully** View user

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

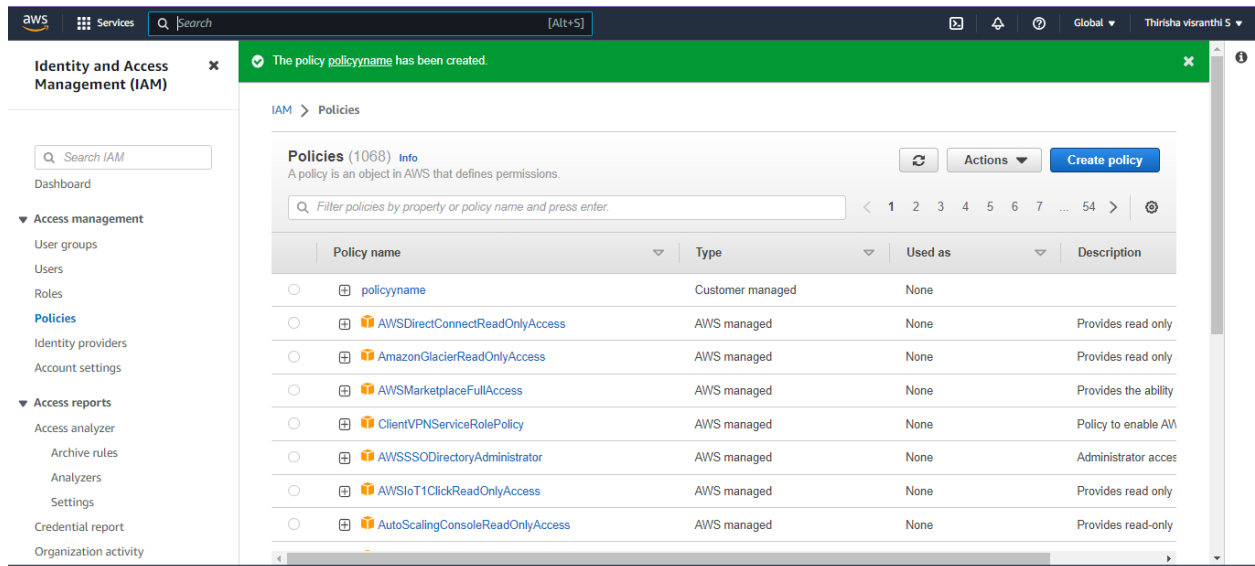
**Users** (Selected 1/4) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

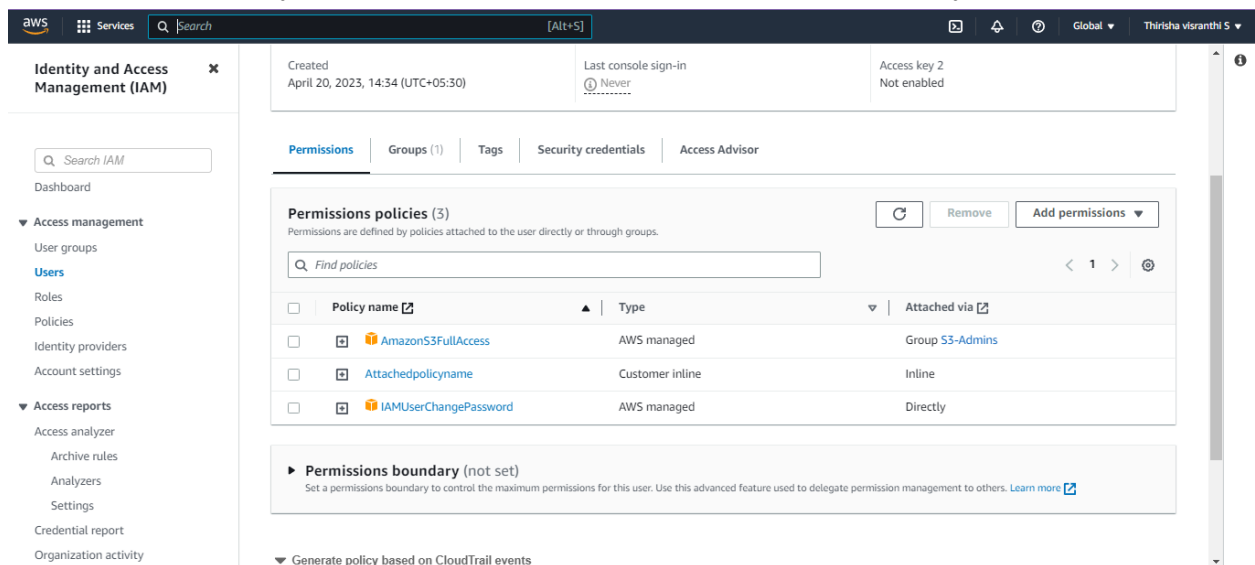
Find users by username or access key

	User name	Groups	Last activity	MFA	Password age	Active key age
<input type="checkbox"/>	room	itsmine	Never	None	10 days ago	-
<input type="checkbox"/>	roomgala	itsmine	Never	None	10 days ago	-
<input checked="" type="checkbox"/>	S3Admin1	S3-Admins	Never	None	None	-
<input type="checkbox"/>	safe	safty and itsmine	Never	None	10 days ago	-

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.

The screenshot shows the AWS IAM console interface. On the left is a navigation sidebar with 'Identity and Access Management (IAM)' selected. The main content area displays the 'creatorole' role configuration. At the top, there are 'Delete' and 'Edit' buttons. Below is a 'Summary' section with a table of key information:

Creation date April 20, 2023, 14:50 (UTC+05:30)	ARN arn:aws:iam::221350325039:role/creatorole	Instance profile ARN arn:aws:iam::221350325039:instance-profile/creatorole
Last activity None	Maximum session duration 1 hour	

Below the summary is a tabbed interface with 'Permissions' selected. It shows 'Permissions policies (1)' and a search bar. At the bottom, there is a table with columns for 'Policy name', 'Type', and 'Description'.

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

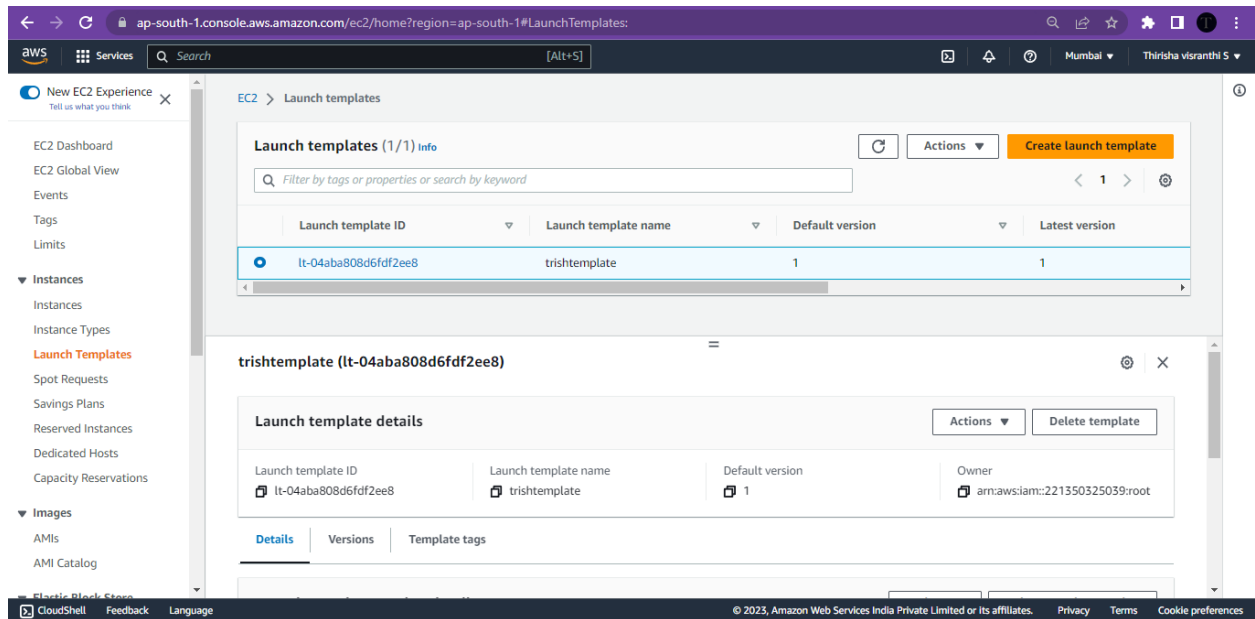
The screenshot shows the AWS IAM console interface. A green banner at the top states 'MFA device assigned'. The main content area displays the 'S3Admin1' user configuration. At the top, there is a 'Delete' button. Below is a 'Summary' section with a table of key information:

ARN arn:aws:iam::221350325039:user/S3Admin1	Console access Enabled with MFA	Access key 1 Not enabled
Created April 20, 2023, 14:34 (UTC+05:30)	Last console sign-in Never	Access key 2 Not enabled

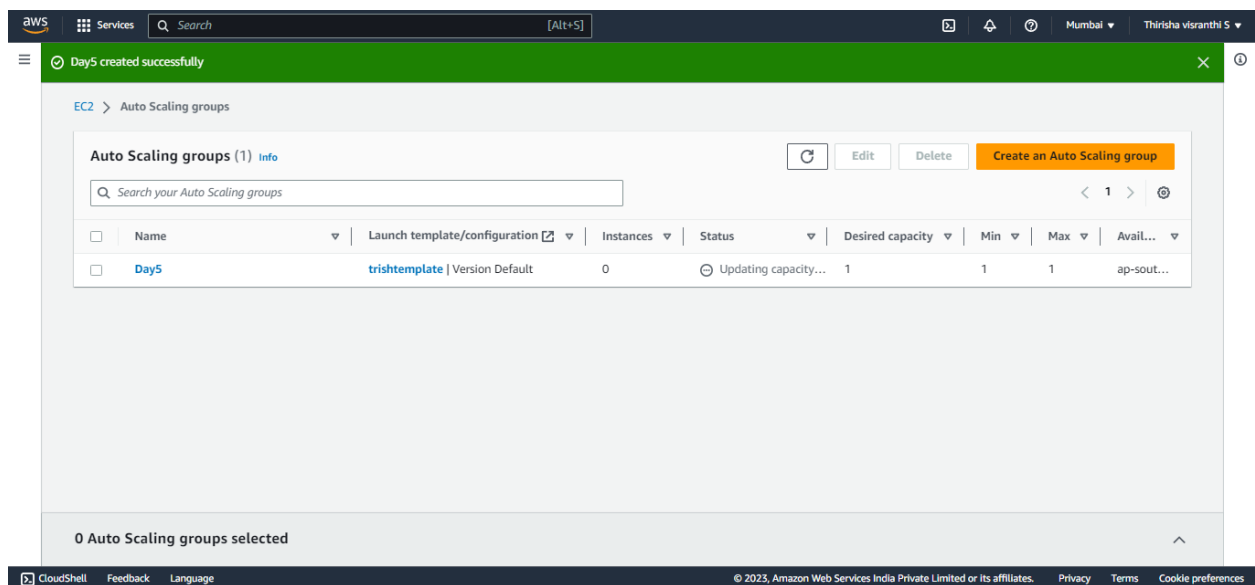
Below the summary is a tabbed interface with 'Security credentials' selected. It shows 'Console sign-in' and a 'Manage console access' button. At the bottom, there is a table with columns for 'Console sign-in link' and 'Console password'.

## Day 5:

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



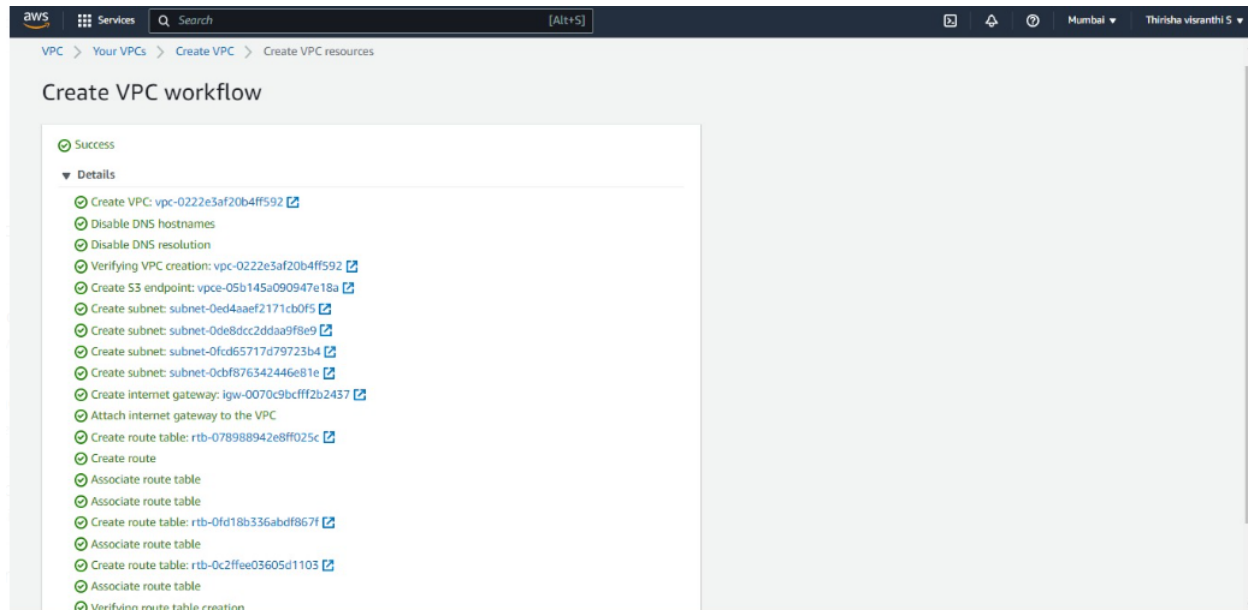
2.Create an autoscaling group with the above-created launch template



## Day:6

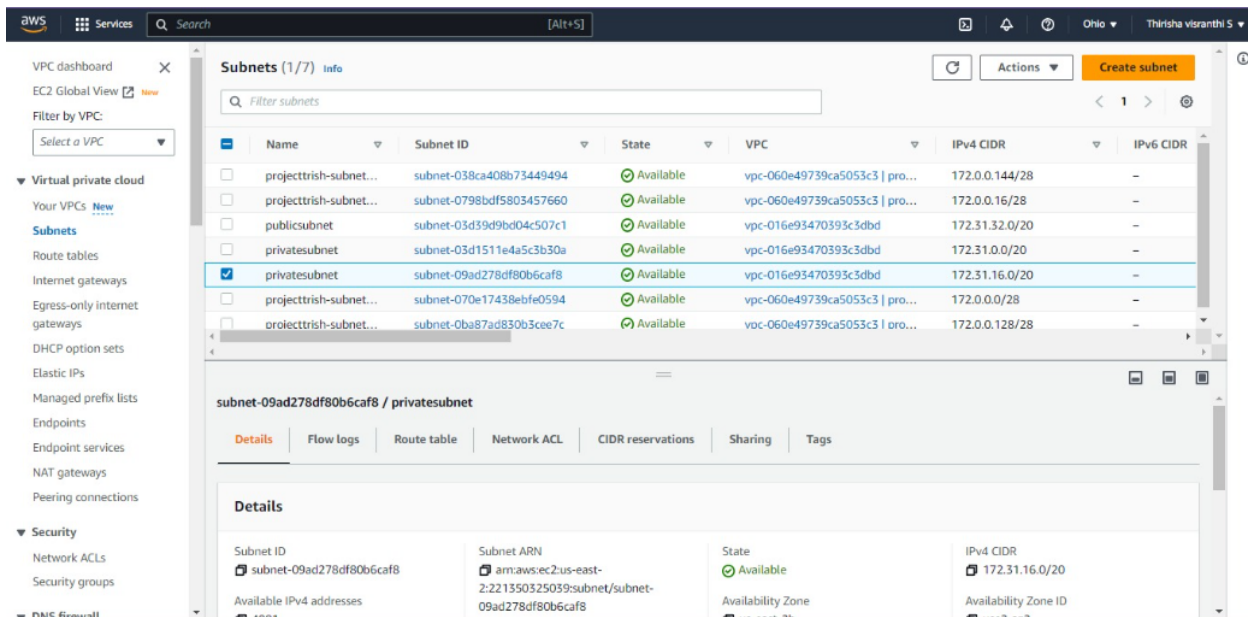
Qst:1

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.

VPC > NAT gateways > Create NAT gateway

## Create NAT gateway [Info](#)

A highly available, managed Network Address Translation (NAT) service that instances in private subnets can use to connect to services in other VPCs, on-premises networks, or the internet.

### NAT gateway settings

**Name - optional**  
Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

**Subnet**  
Select a subnet in which to create the NAT gateway.

**Connectivity type**  
Select a connectivity type for the NAT gateway.

☒ Public  
☐ Private

**Elastic IP allocation ID [Info](#)**  
Assign an Elastic IP address to the NAT gateway.

Activate Windows  
Go to PC settings to activate Windows.

Qst:4

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

aws Services Search [Alt+S] Ohio Thirisha Visranthi S

VPC dashboard EC2 Global View [New](#)

Filter by VPC:

- Virtual private cloud
  - Your VPCs [New](#)
  - Subnets
  - Route tables
  - Internet gateways
  - Egress-only internet gateways
  - DHCP option sets
  - Elastic IPs
  - Managed prefix lists
  - Endpoints
  - Endpoint services
  - NAT gateways
  - Peering connections**
- Security
  - Network ACLs
  - Security groups

**A VPC peering connection pcx-07bb47e728f142abc / Myvpcname has been requested.**  
Remember to change your region to **ap-south-1** to accept the peering connection.

VPC > Peering connections > pcx-07bb47e728f142abc

### pcx-07bb47e728f142abc / Myvpcname [Actions](#)

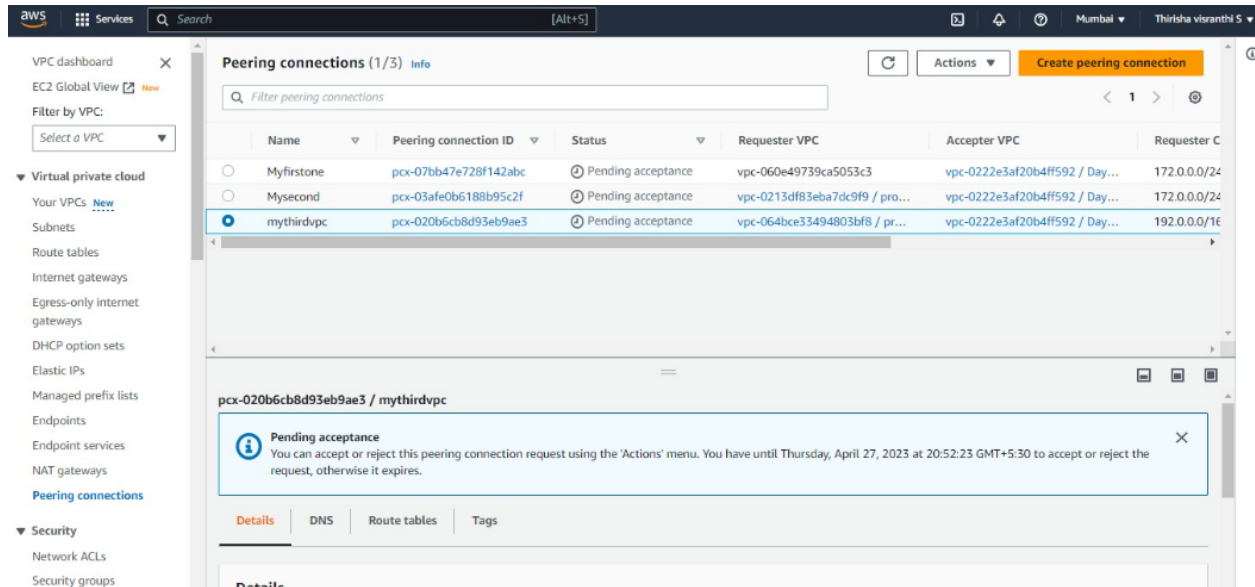
#### Details [Info](#)

Requester owner ID 221350325039	Accepter owner ID 221350325039	VPC Peering connection ARN arn:aws:ec2:us-east-2:221350325039:vpc-peering-connection/pcx-07bb47e728f142abc
Peering connection ID pcx-07bb47e728f142abc	Requester VPC vpc-060e49739ca5053c3 / projecttrish-vpc	Accepter VPC vpc-0222e3af20b4ff592
Status Initiating Request to 221350325039	Requester CIDRs 172.0.0.0/24	Accepter CIDRs -
Expiration time Thursday, April 27, 2023 at 20:35:55 GMT+5:30	Requester Region Ohio (us-east-2)	Accepter Region Mumbai (ap-south-1)

**DNS settings** [Edit DNS settings](#)

[DNS](#) [Route tables](#) [Tags](#)

Qst5:Create VPC peering connections 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

