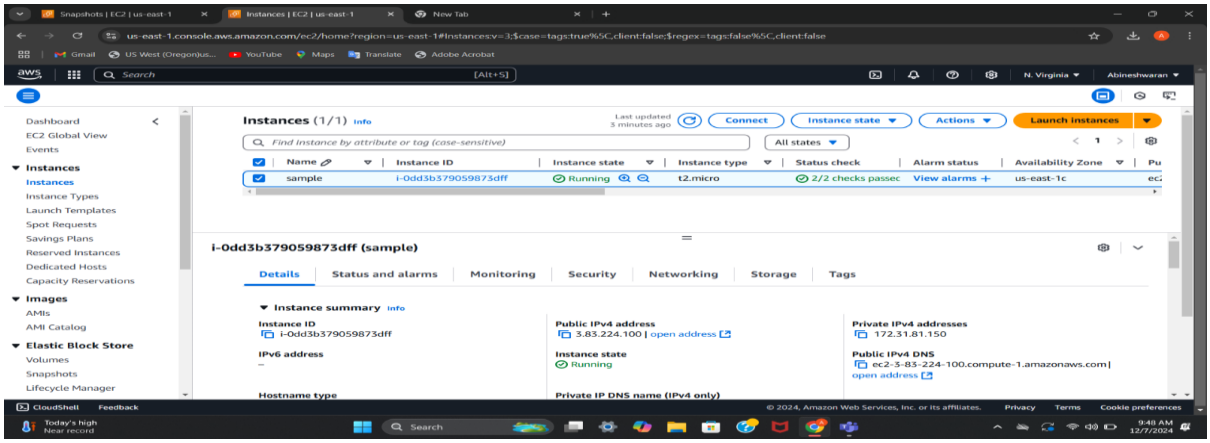
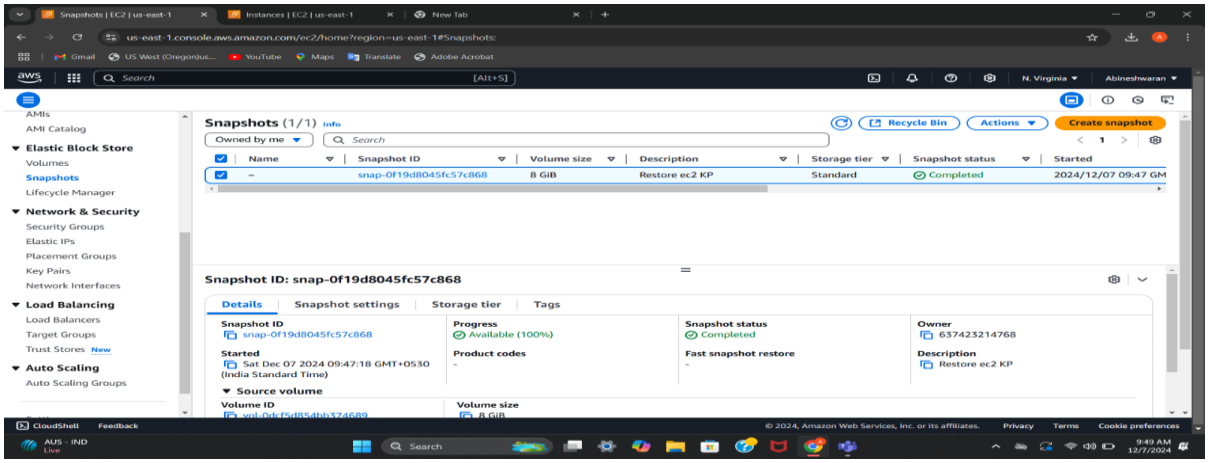
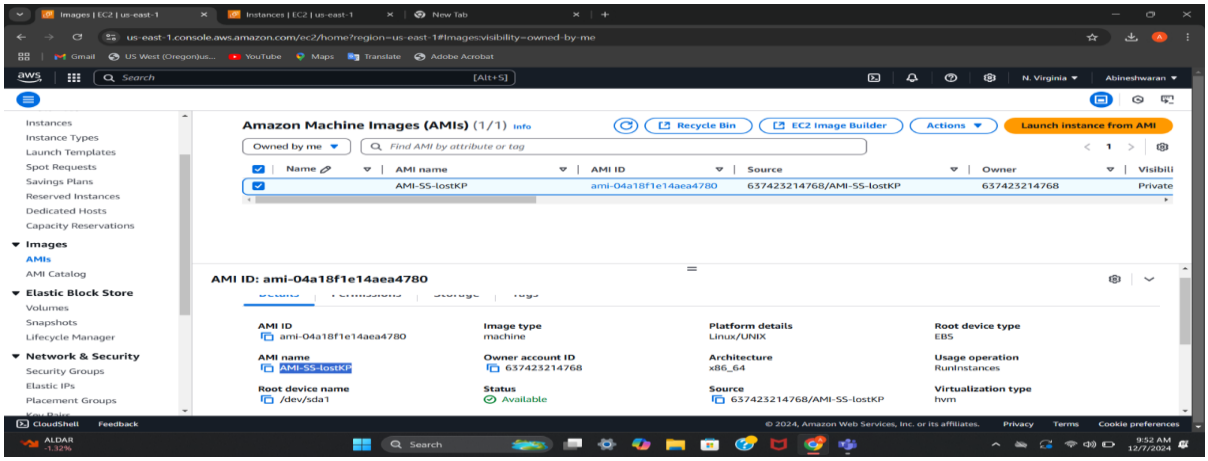
1) How to recover the ec2 instance, if you lost the key pair

Step 1: Take the snapshot of the current state of the ec2 instance



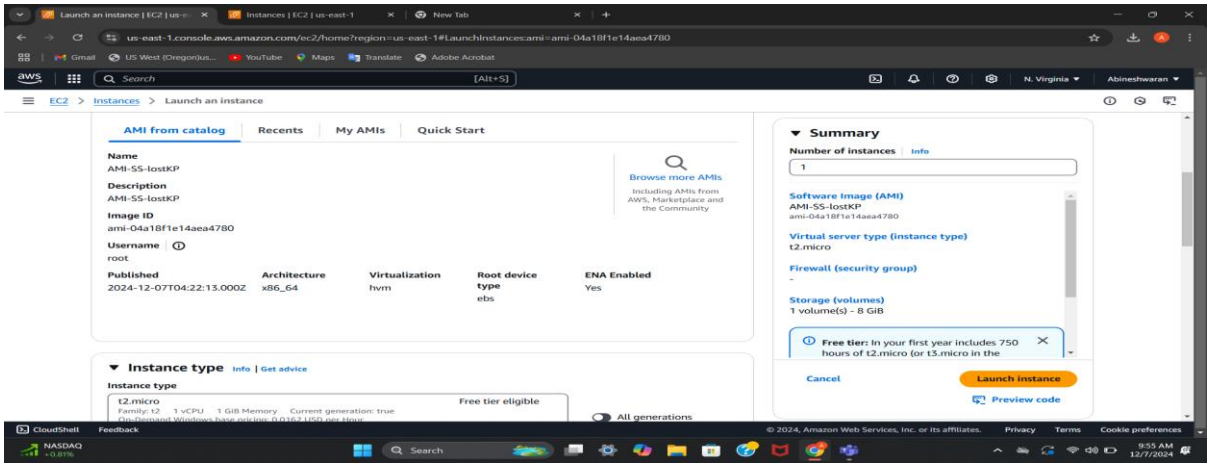


Step 2: Create an AMI from the Snapshot created.



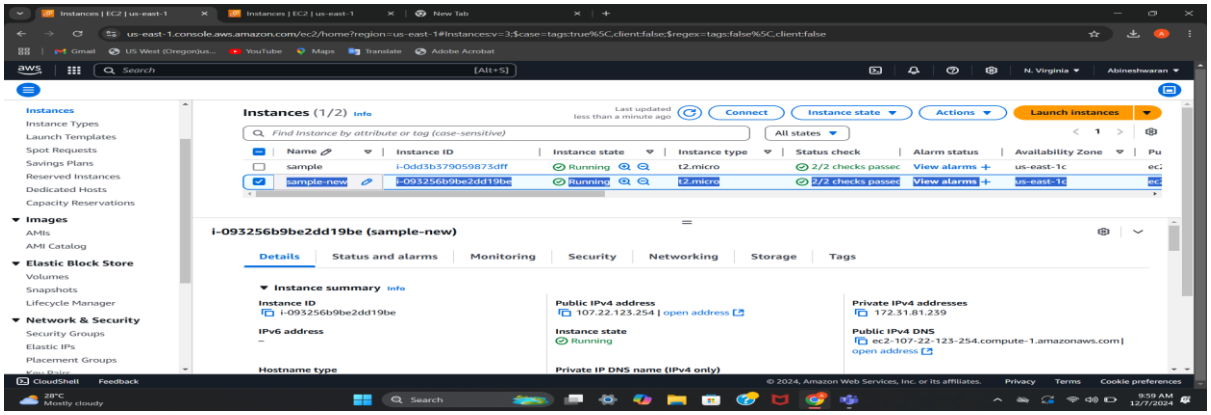
After creating an AMI from a snapshot, you can launch a new EC2 instance using this AMI. This newly created instance will be a copy of the original instance from which the snapshot was taken, including its software configuration, data, and settings

Step 3: Create a new EC2 Instance from the AMI created and create a new key pair to login to the EC2 Instance.

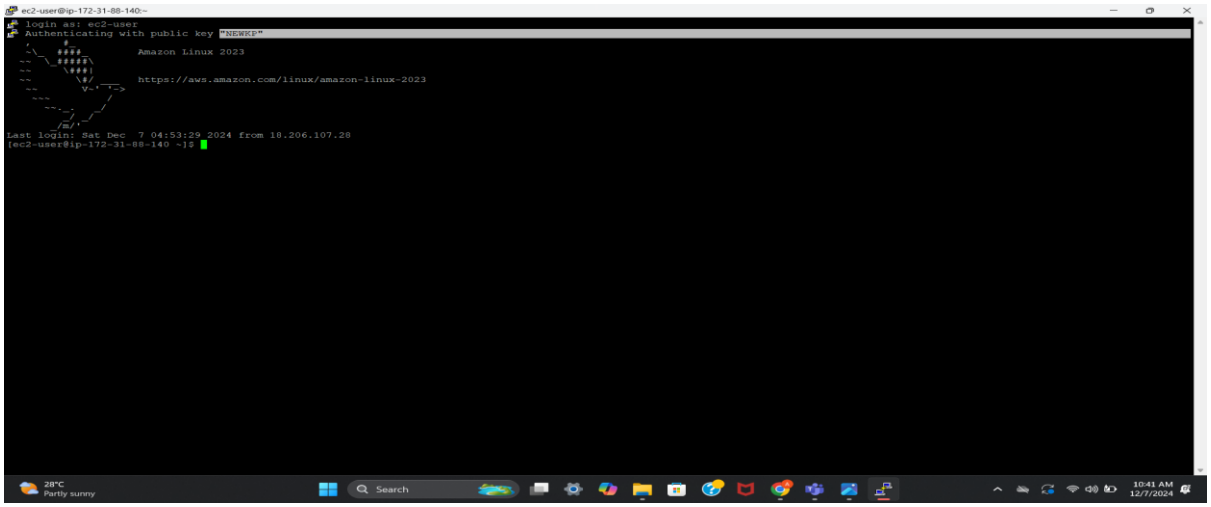


created with new keypair of name as **NEWKP** and created **sample_new** instance

Step 4: Login to the New EC2 Instance with the new Key Pair.

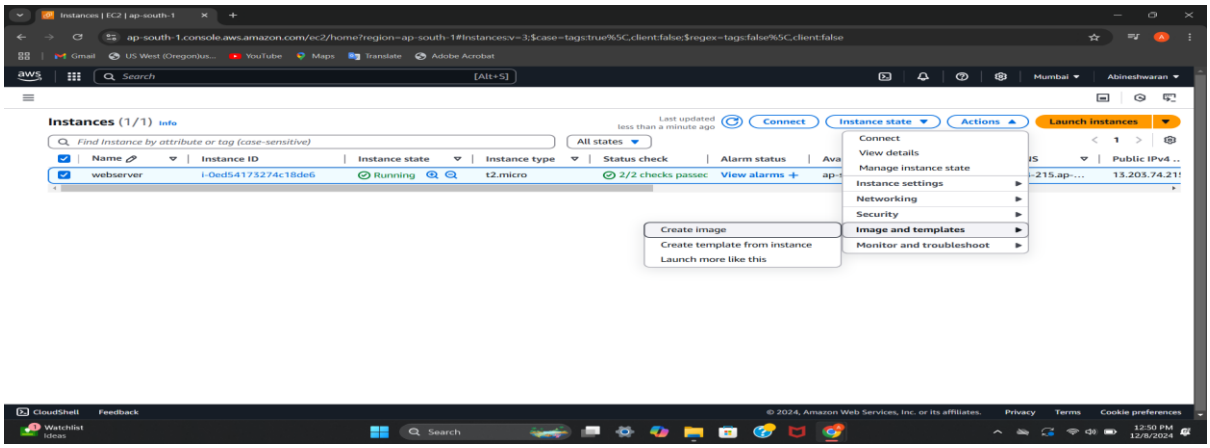


Now connect the ec2instance with new key pair

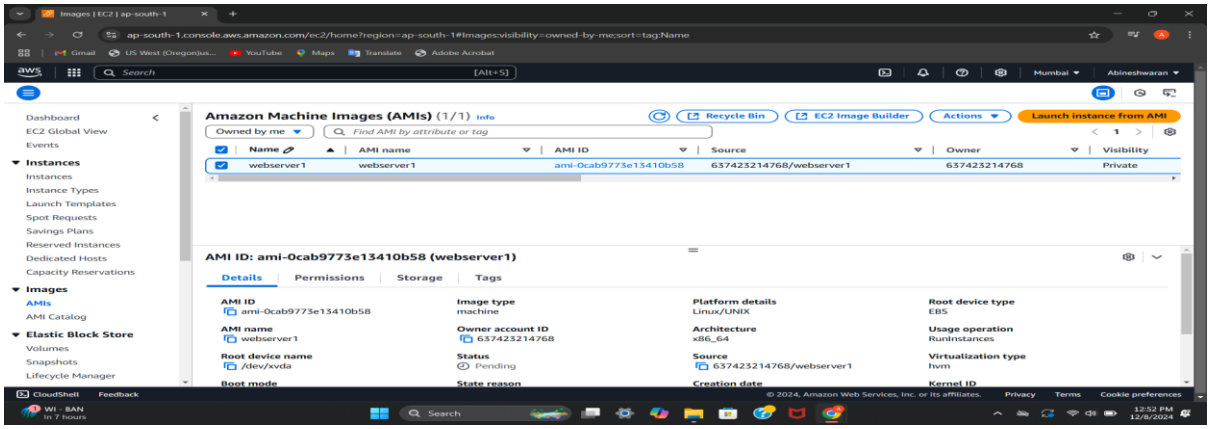


Successfully created the new key pair to recover the ec2 instance,

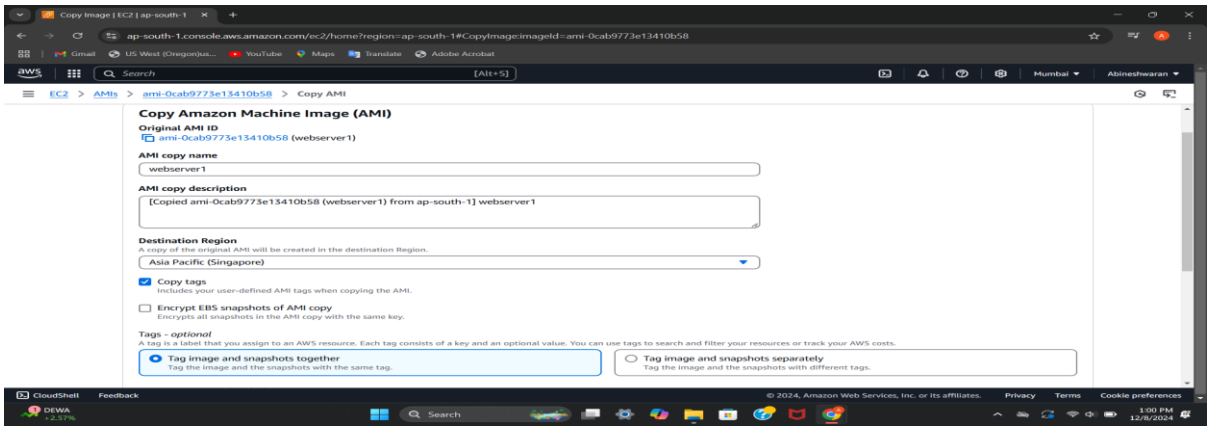
2) Migrate your AMI to Mumbai to Singapore Region



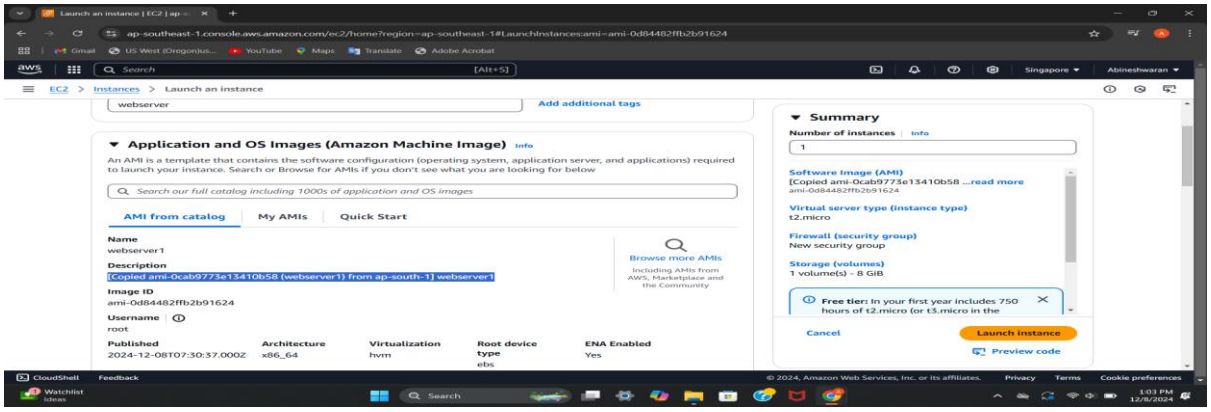
Created the ec2 instance with the name **WEBSERVER** and creating the image by using the option create image in Mumbai region



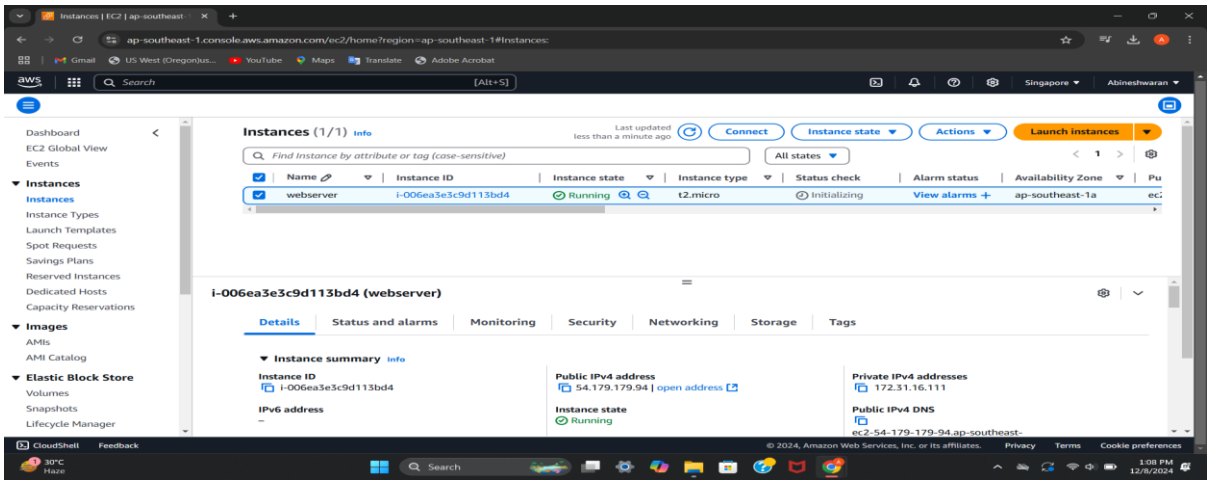
Then now copying the AMI for Migrate AMI to Mumbai to Singapore Region



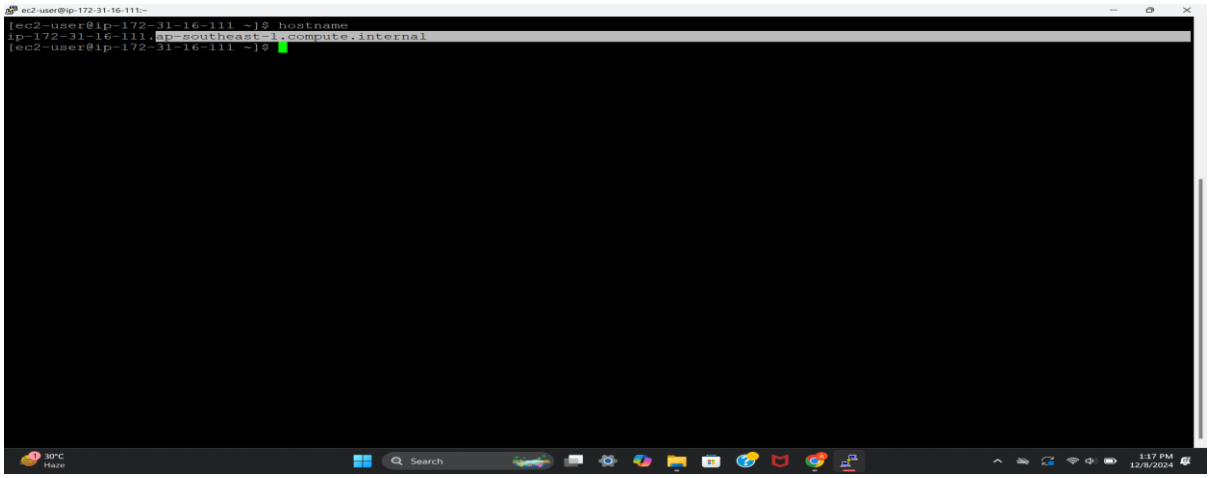
The Ami launched in Singapore region and the create the new ec2 with Mumbai region Ami



Launch the new instance of copied AMI

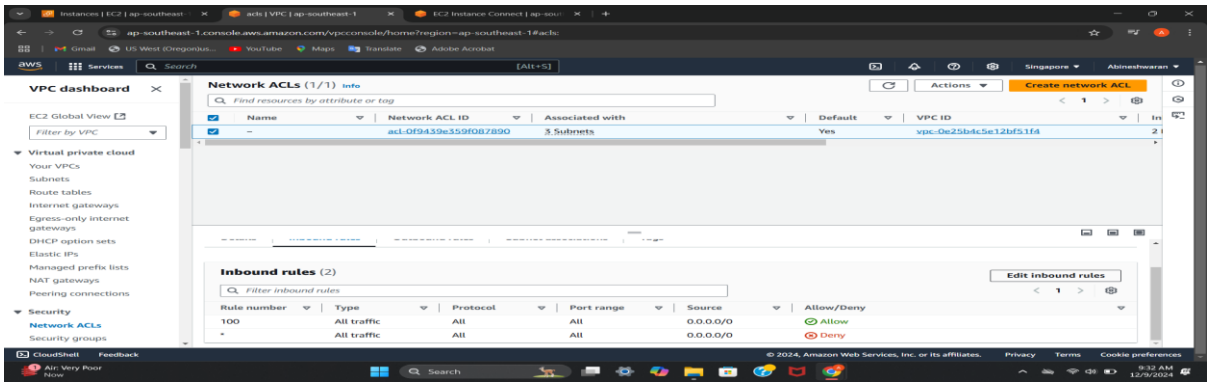


The new ec2 instance created in the Singapore region by the copied AMI of Mumbai region, and then connect the ec2 instance with putty, check the hostname of region

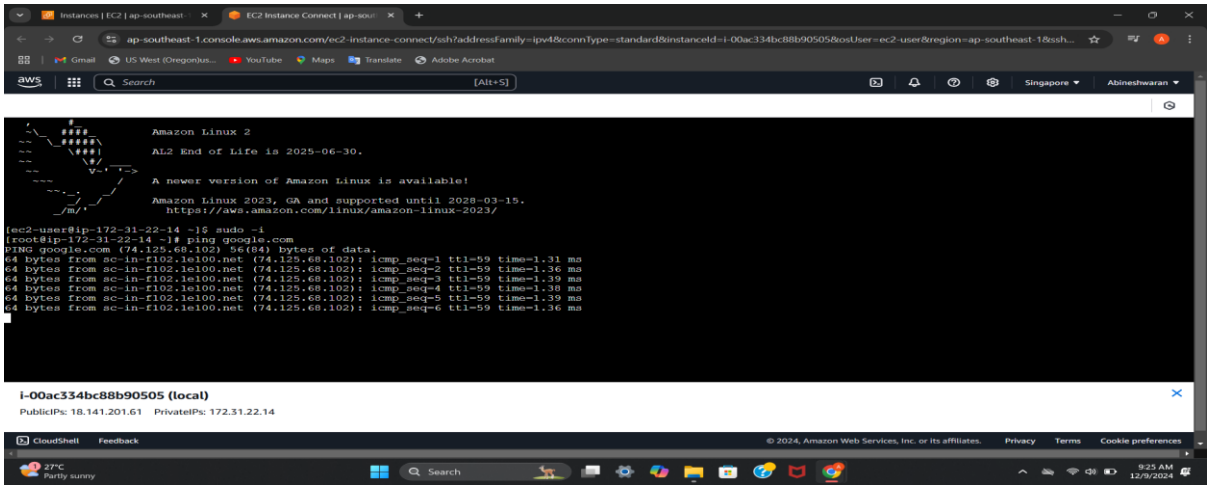


successfully connected with **ap-southeast-1 of** Singapore region, by Migrate AMI of Mumbai region

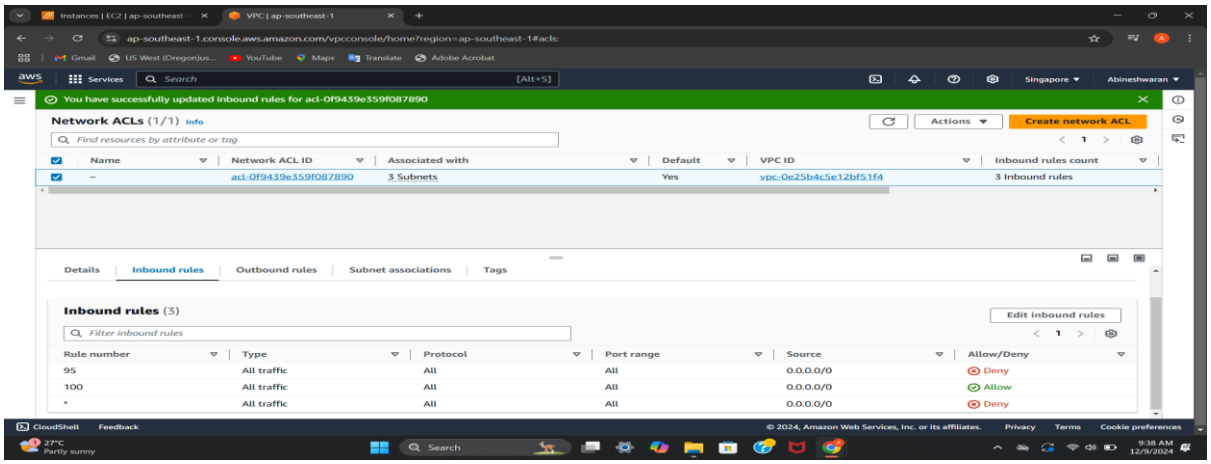
3) Block your ip address in NACL to restrict SSH Access



Created the ec2 instance and checked the internet flow on the instance before changing the rules



Instance has internet flow by ping google

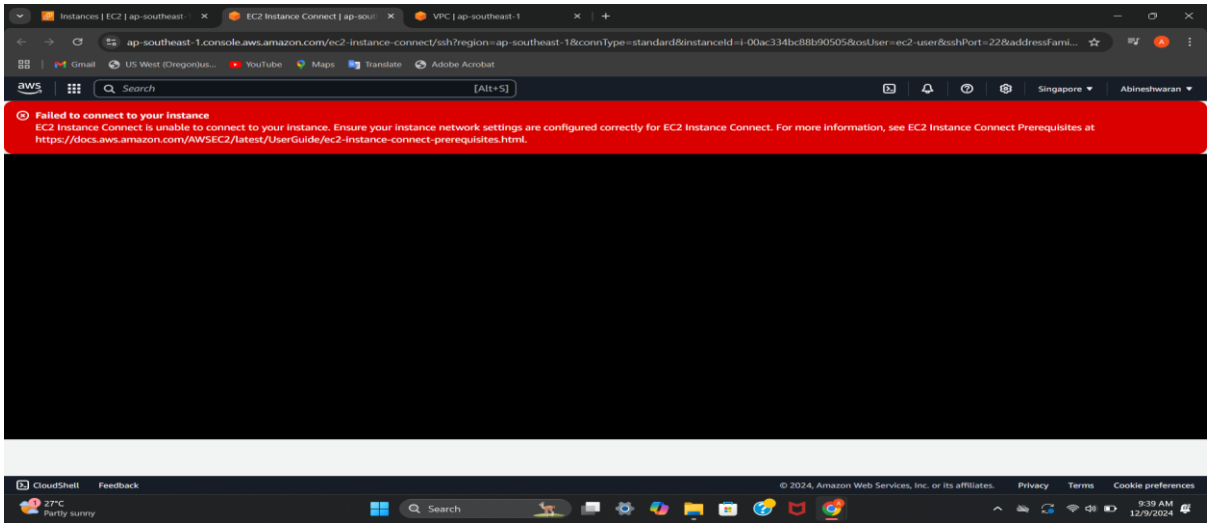


Restricts SSH access to your EC2 instance, you can create a new inbound rule in your Network ACL (NACL) with the following specifications:

1. **Rule Number:** 95
2. **Type:** All Traffic

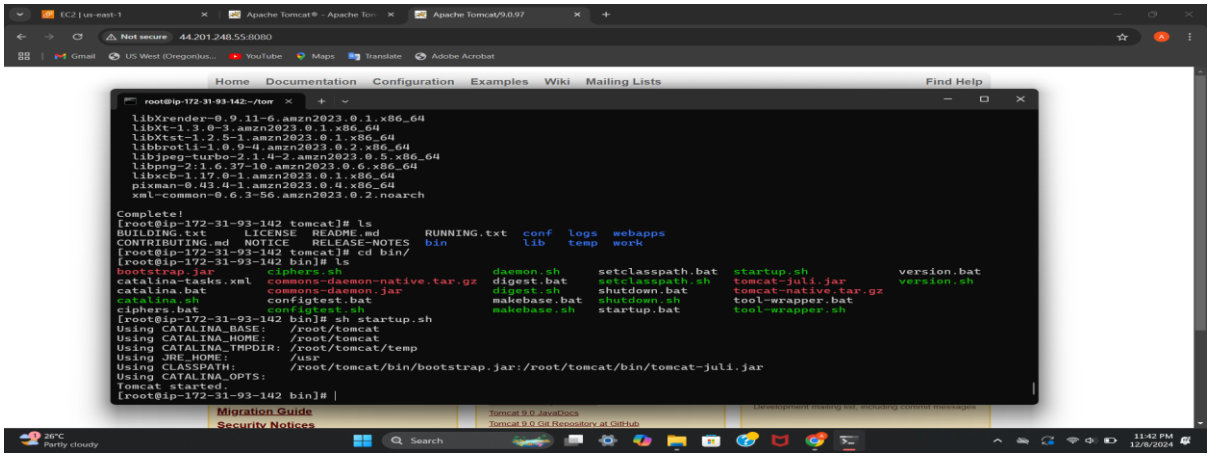
3. **Action:** Deny
4. **Protocol:** -1 (All Protocols)
5. **Port Range:** All Ports
6. **Source CIDR Blocks:** The IP address or range of IP addresses you want to block.

Once you've added this rule, save the changes to your NACL. This will effectively block SSH access from the specified IP addresses, preventing unauthorized access to your instance.



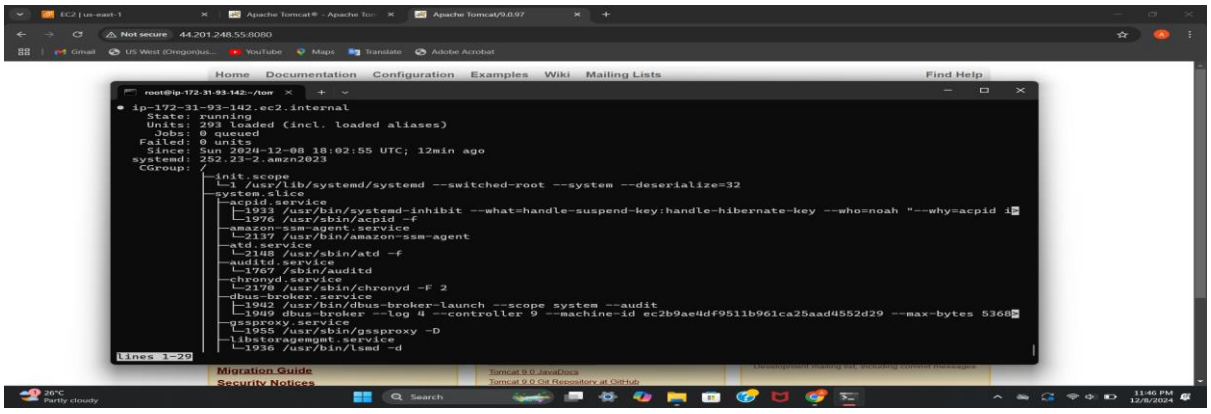
Successfully blocked your IP address in the Network Access Control List (NACL) to restrict SSH access. As a result, you will be unable to connect to your EC2 instance via SSH.

4) Run httpd in the back end by using systemctl commands



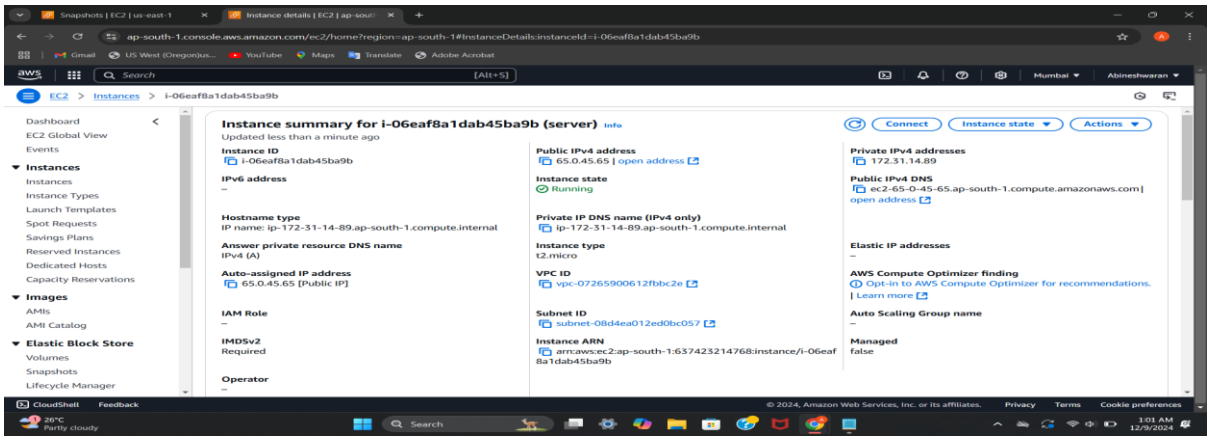
Launch an EC2 Instance: Create a new EC2 instance with an appropriate operating system (e.g., Amazon Linux 2) and security group configuration to allow SSH and HTTP traffic.

1. **Install Apache HTTP Server:** Use the package manager (e.g., `yum` or `apt`) to install the Apache HTTP server.
2. **Install Java:** Install the desired Java version (e.g., OpenJDK or Oracle JDK) using the package manager.
3. **Configure Apache:** Configure Apache to serve your web applications. This may involve creating virtual hosts, configuring SSL, and other customizations.
4. **Deploy Your Web Applications:** Deploy your Java web applications to the EC2 instance, either as standalone applications or using a web server like Tomcat.
5. **To connect to your EC2 instance and Apache web server:**
6. **SSH into the EC2 Instance:** Use the SSH client to connect to your EC2 instance using its public IP address and security key pair.
7. **Access the Apache Web Server:** Once you're connected, you can access the Apache web server running on the instance by visiting its IP address or domain name in a web browser.

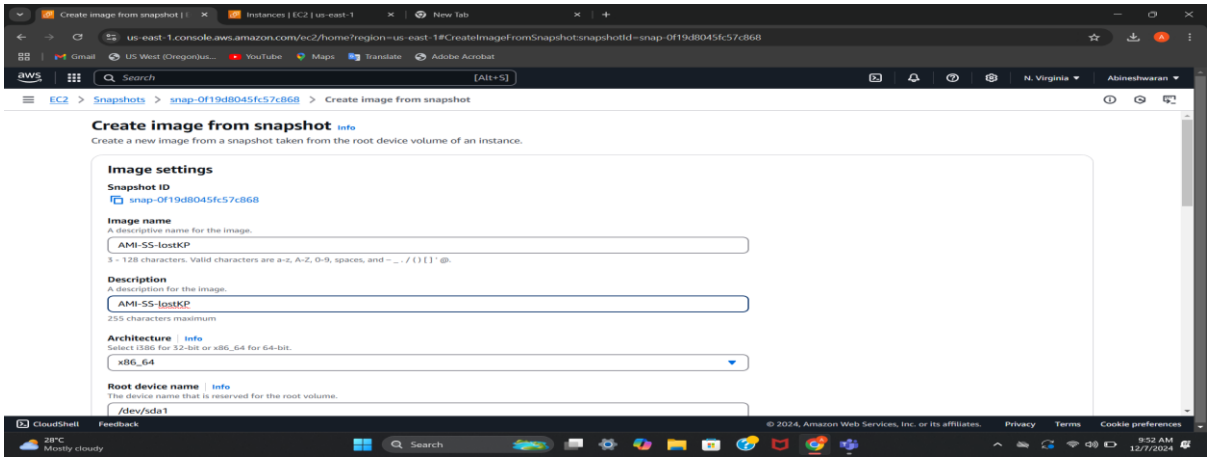


successfully set up and access your Apache web server on your EC2 instance by Run httpd in the back end by using systemctl commands

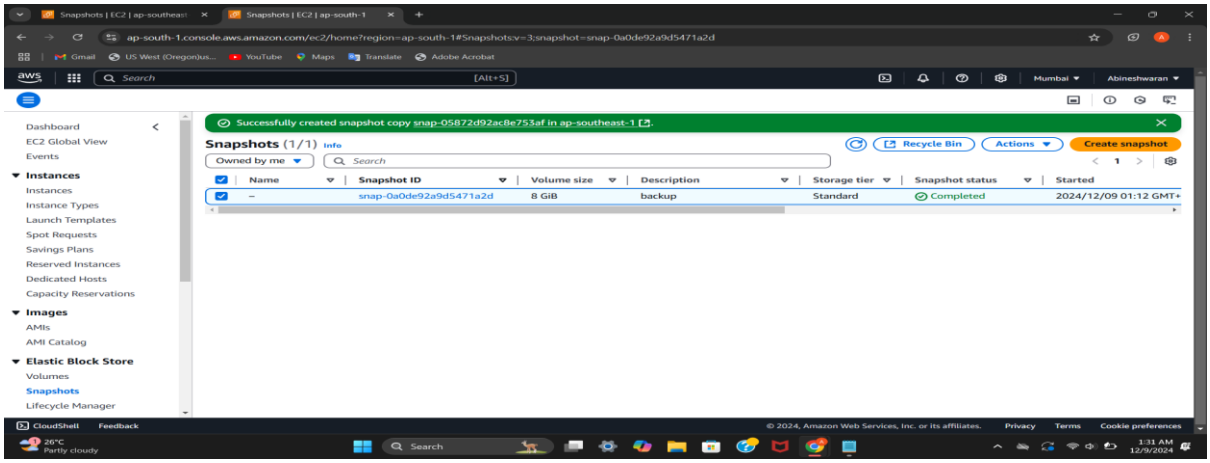
5) Backup your ebs volume by taking snapshot and check is it possible to migrate to another region



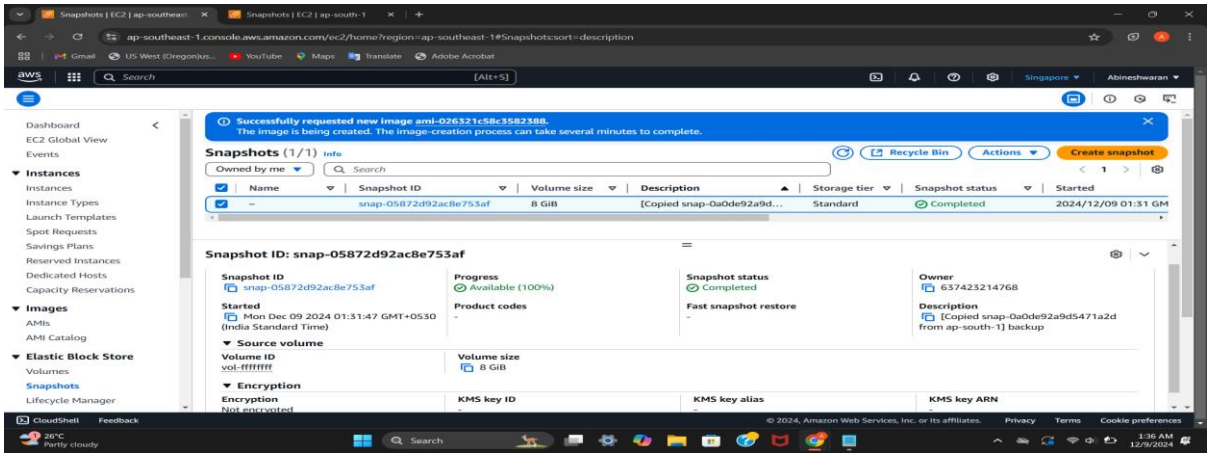
created the ec2 instance of Mumbai region and backup the ebs volume, then migrate to Singapore region



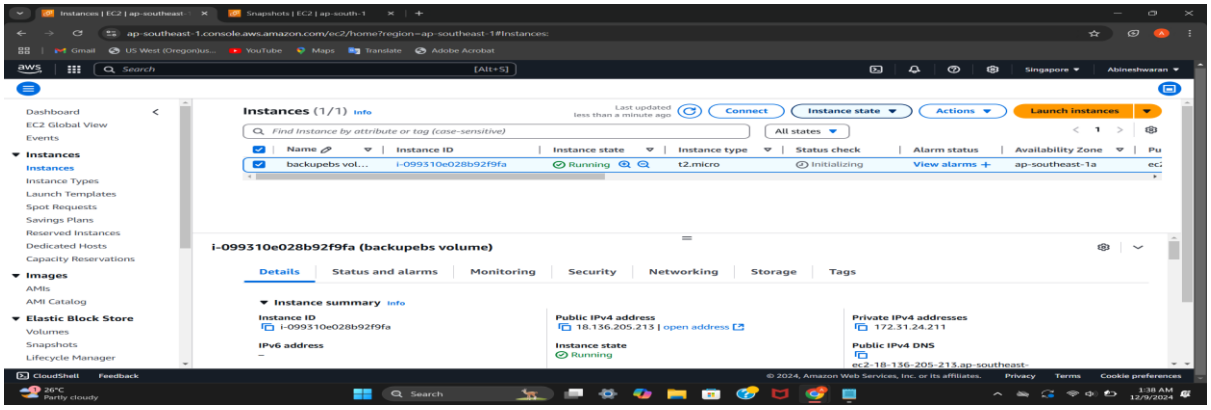
Backup the EBS volume by taking the snapshot of volume



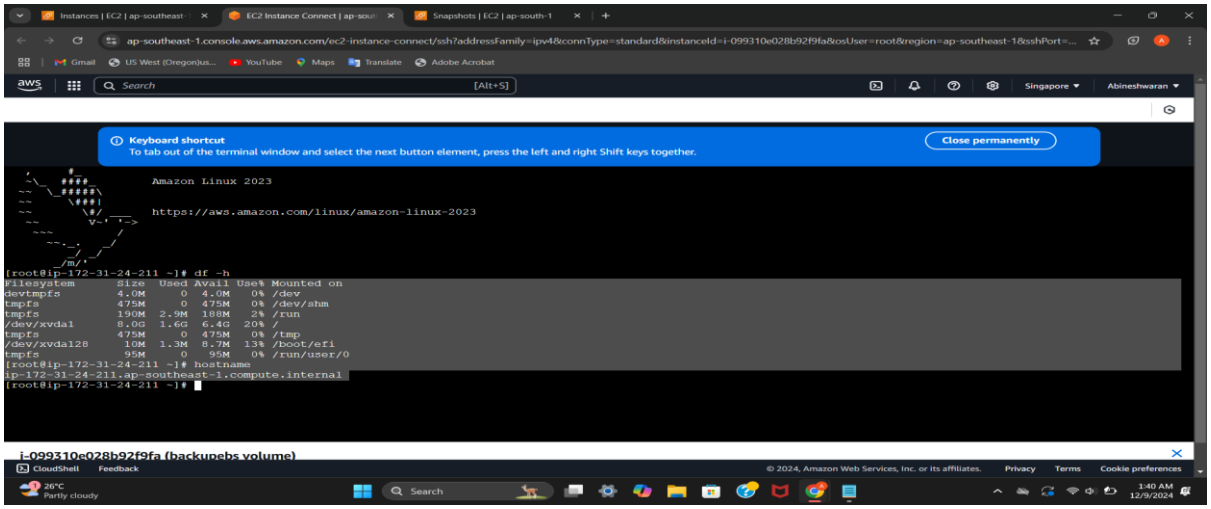
create the copy of snapshot by using the option copy snapshot and selected the region of Singapore as ap-southeast-1, create the snapshot



now check the Singapore region of snapshot and create the Ami by using the copied snapshot of Mumbai region and launch the instance by the snap copy AMI image



Now connect instance and check the volume of hostname



successfully back up an EBS volume by taking a snapshot. Additionally, migrate this volume from the Mumbai region to the Singapore region