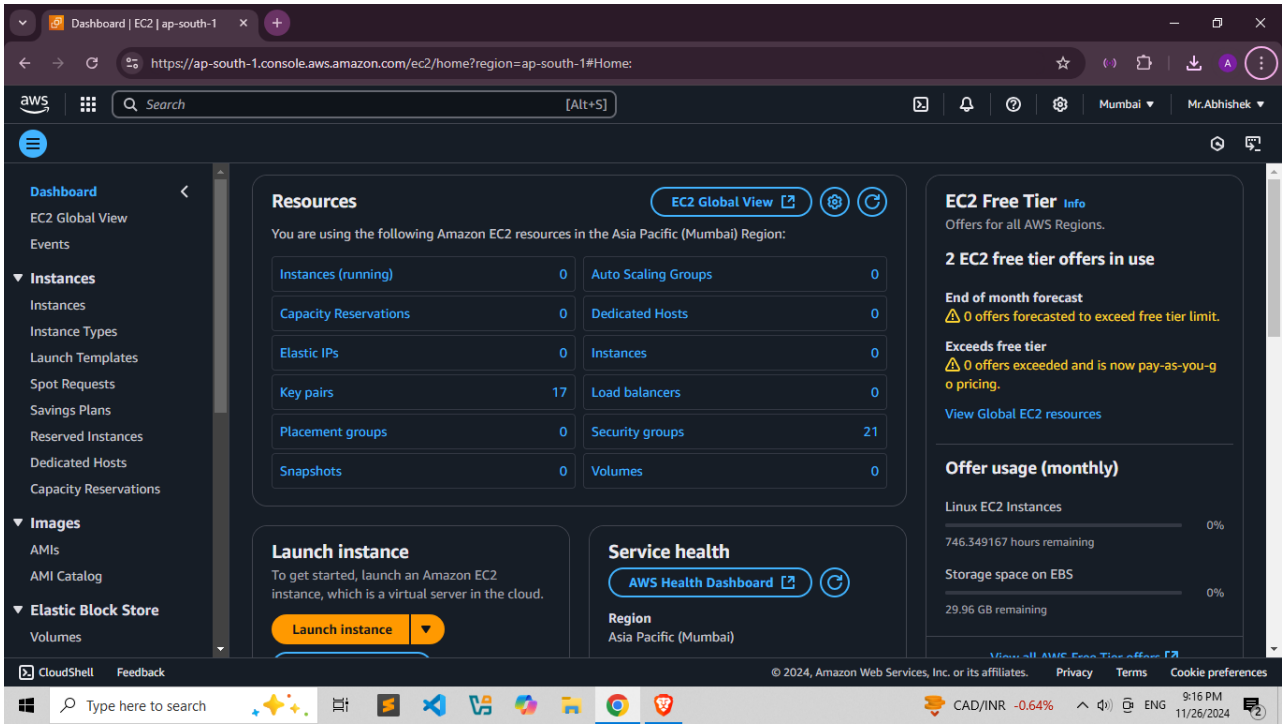
Host Static Website on EC2 Instance using Linux (AMI)

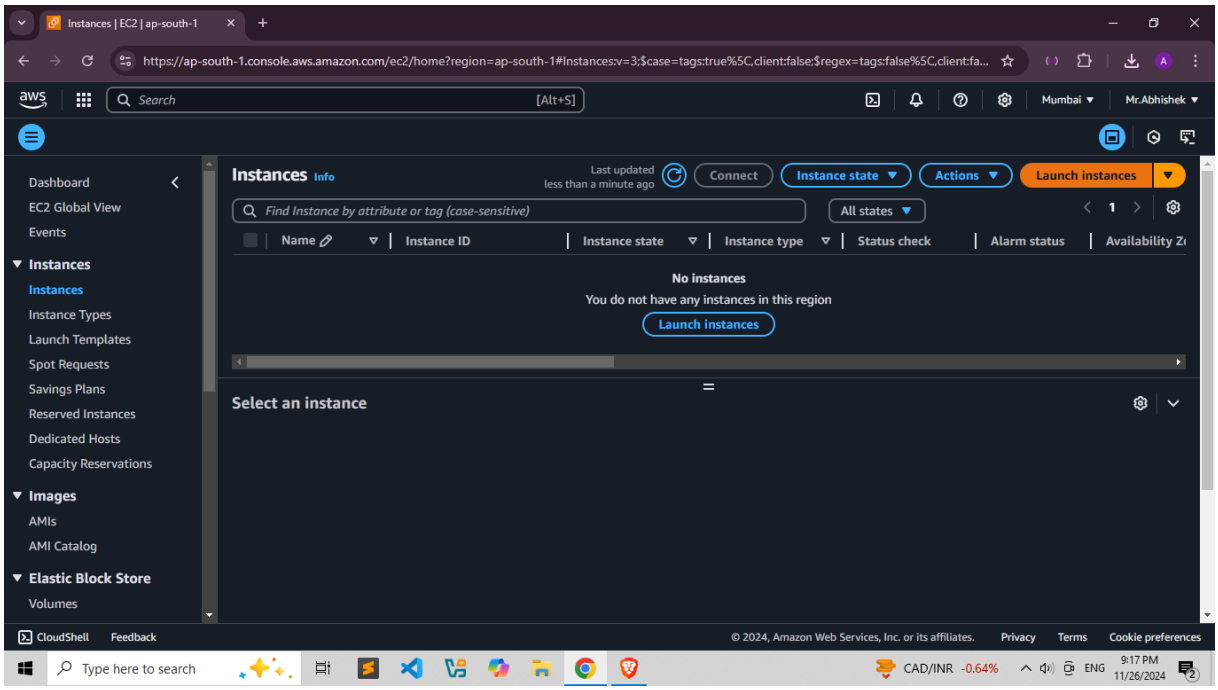
Step 1: Navigate to the EC2 Dashboard

- From the AWS Console, locate the **Services** menu in the top navigation bar.
- Select **EC2** under the "Compute" category. This will take you to the EC2 Dashboard.



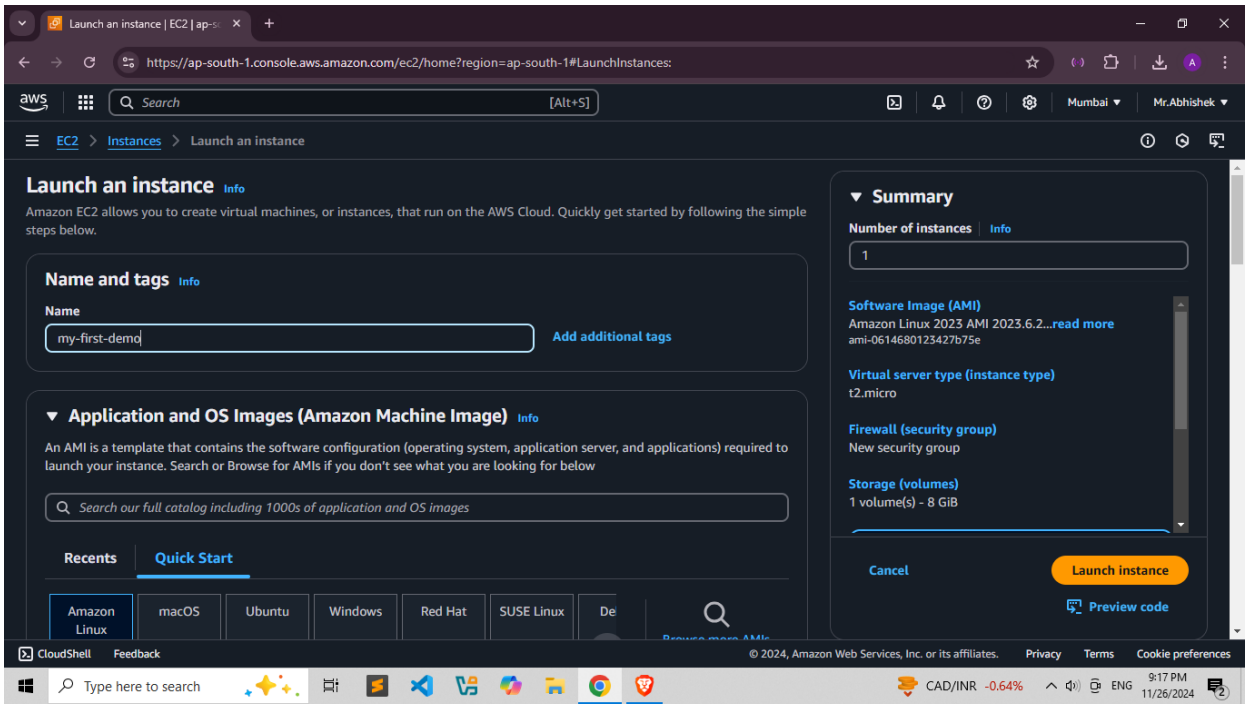
Step 2: Click on 'Launch Instances'

- On the EC2 Dashboard, click the **Launch Instances** button. This will start the instance creation wizard.



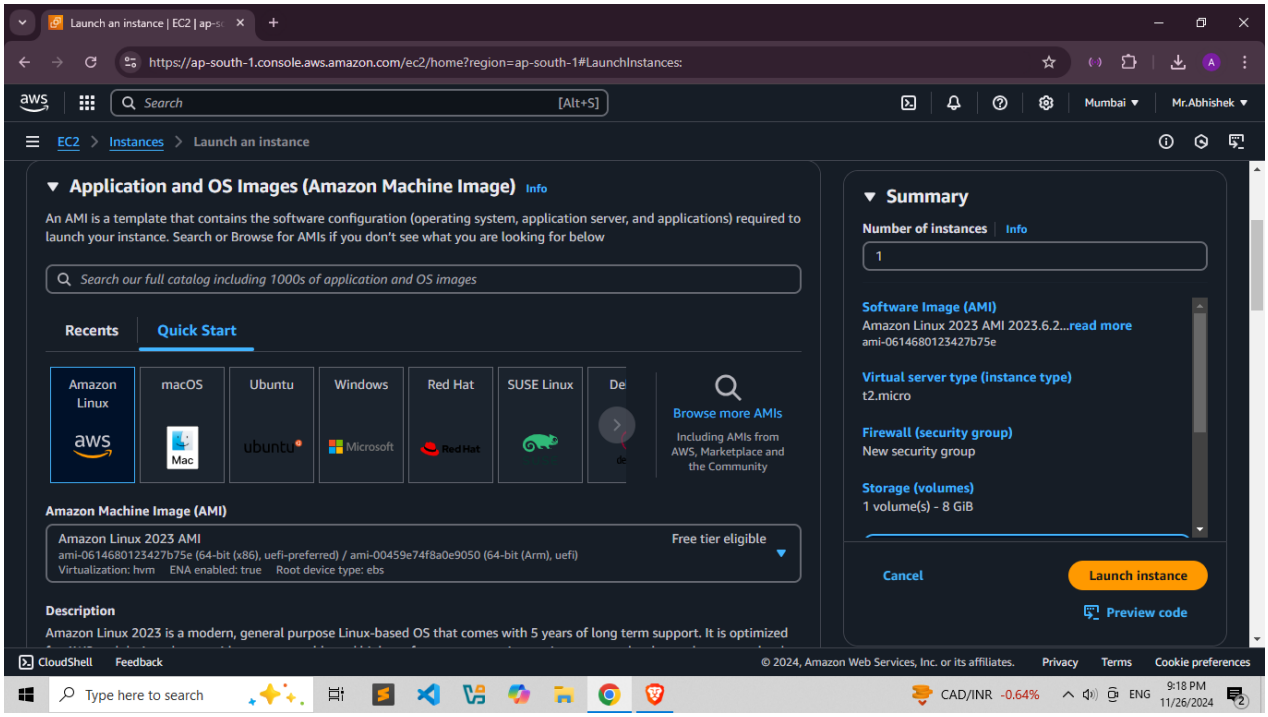
Step 3: Add Name and Tags

- Add tags to your instance for better management and identification.
  - Example: `Key: Name, Value: MyInstance`.



Step 4: Choose an Amazon Machine Image (AMI)

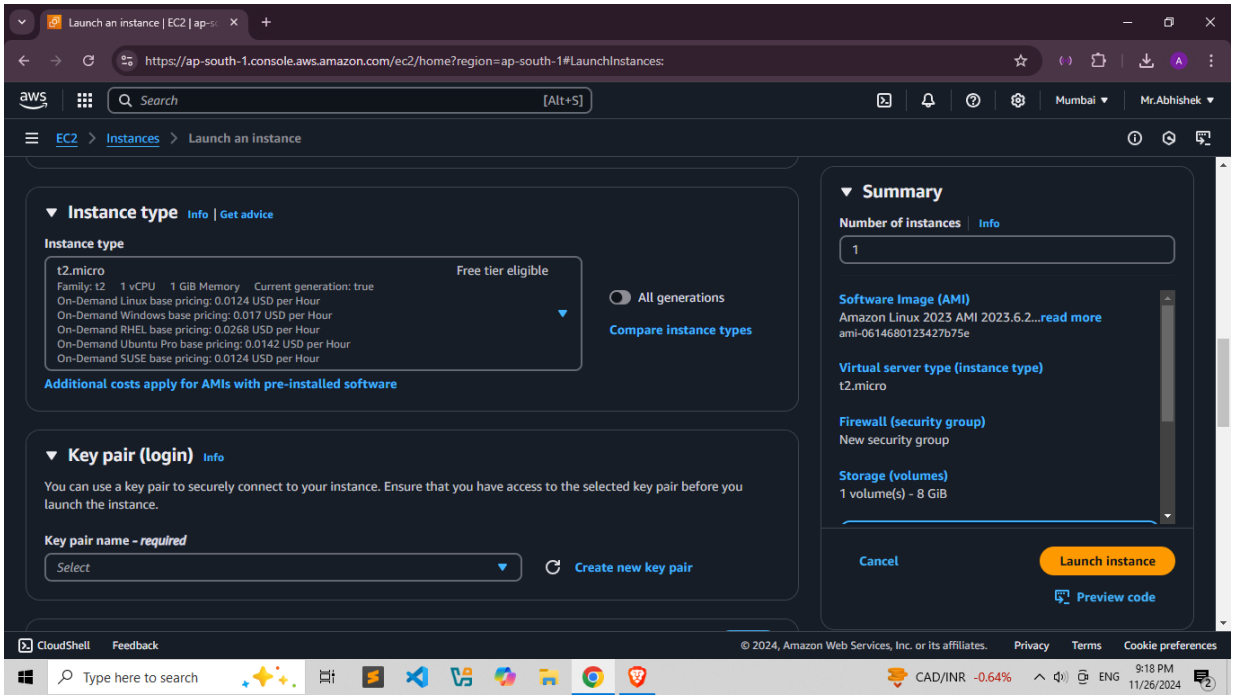
- Select an **AMI**, which is a pre-configured virtual machine template.
  - Examples:
    - **Amazon Linux 2 AMI** (Free-tier eligible).
    - **Ubuntu Server**.
    - **Windows Server** (if you need a Windows environment).
- Choose an AMI that suits your requirements for the operating system and software packages.



Step 5: Choose an Instance Type

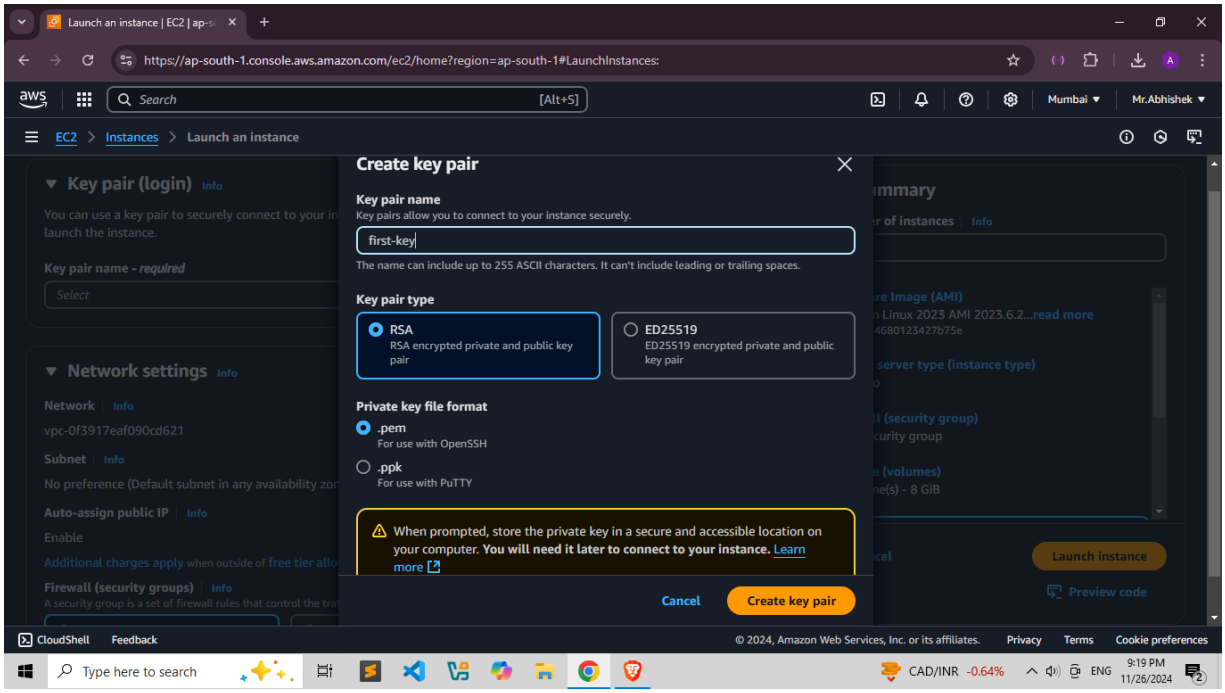
Select the instance type based on your performance needs (CPU, memory, storage, etc.).

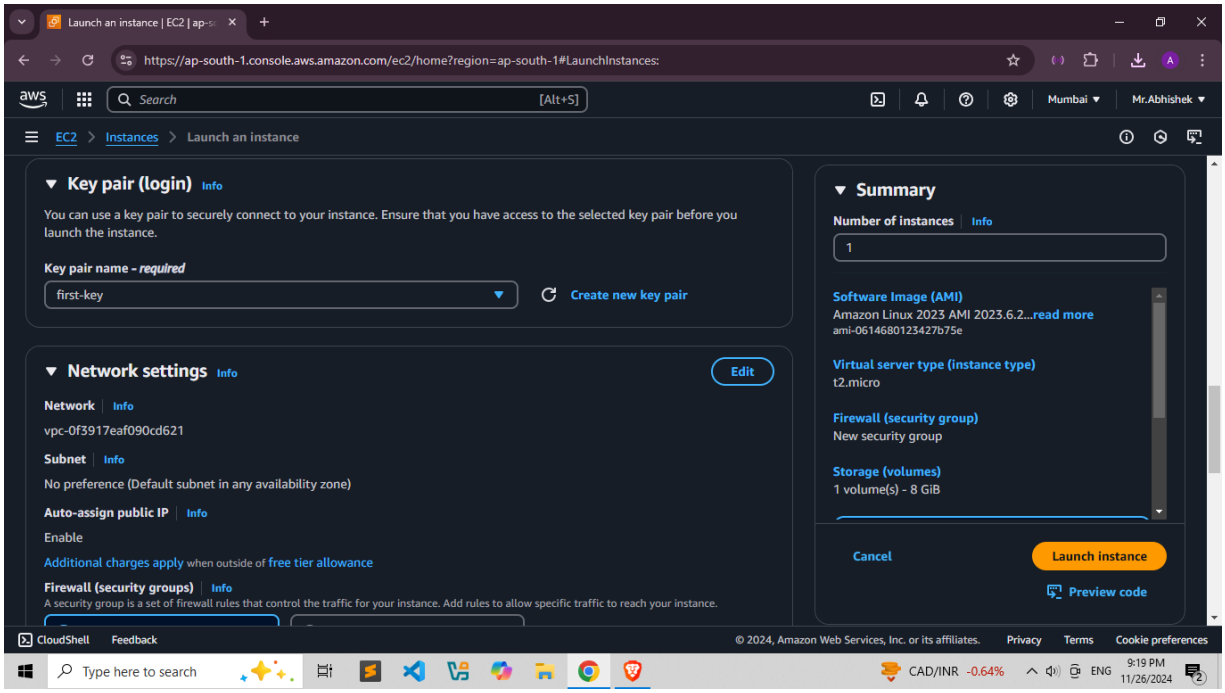
- For free-tier eligible users, choose **t2.micro** or **t3.micro**.



Step 6: Key Pair Creation

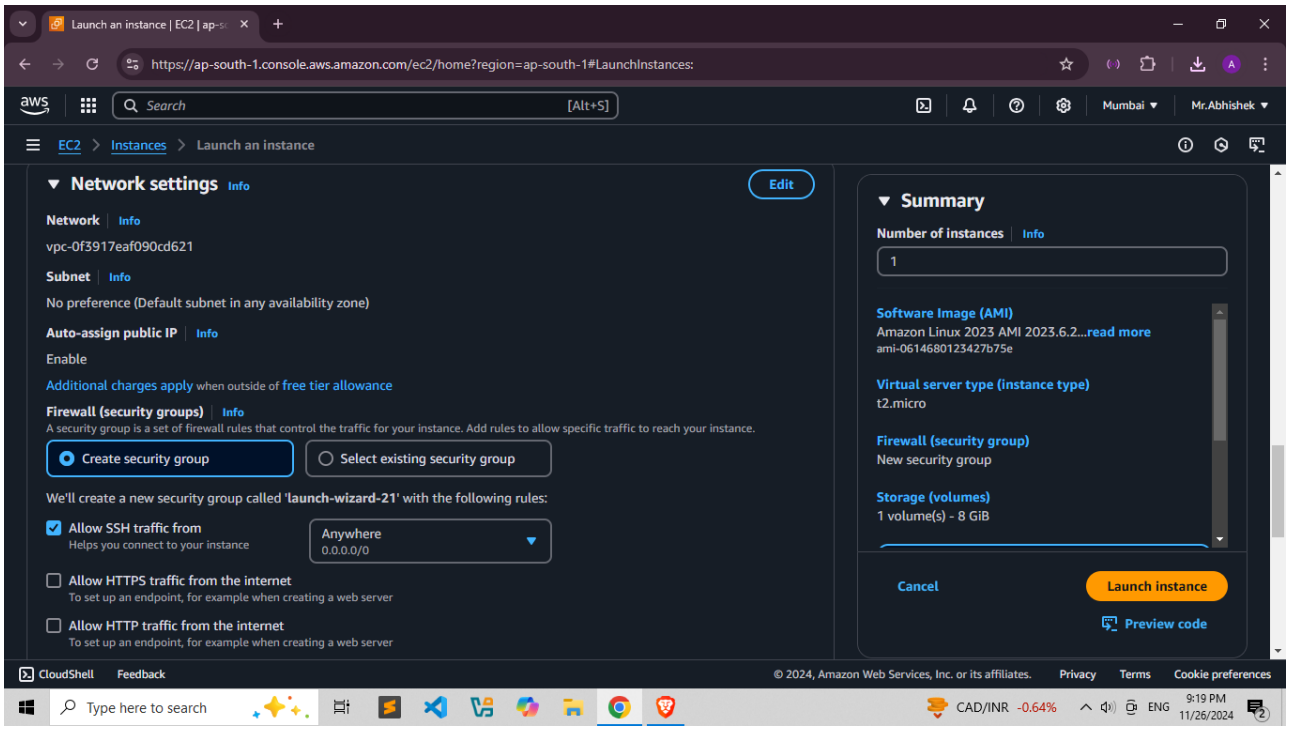
- When prompted, create a new key pair or use an existing one for SSH access:
  - Download the private key file (`.pem`) if creating a new key pair.
  -





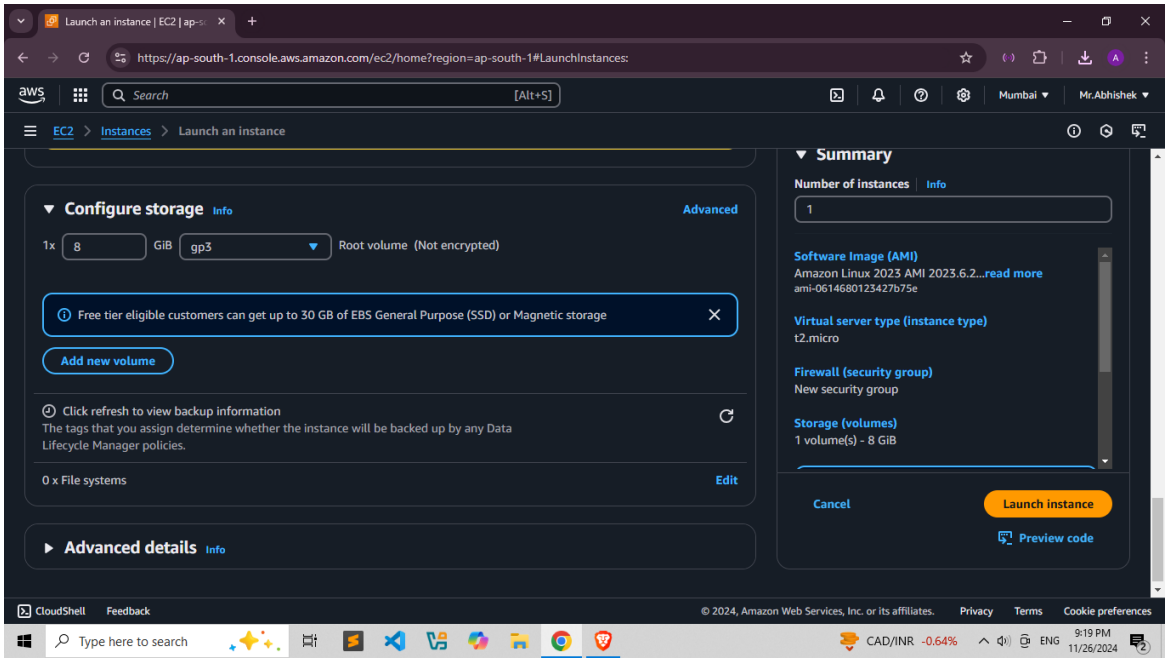
Step 7: Configure Instance Details

- Specify the details for your instance:
  - **Number of instances**: Default is 1.
  - **Network**: Select a Virtual Private Cloud (VPC).
  - **Subnet**: Choose a subnet for your instance.
  - **Auto-assign Public IP**: Enable this if you need internet access.
  - **IAM Role**: Assign an IAM role if necessary.
  - Advanced options: Configure placement groups, capacity reservations, etc.
- Click **Next** when done.



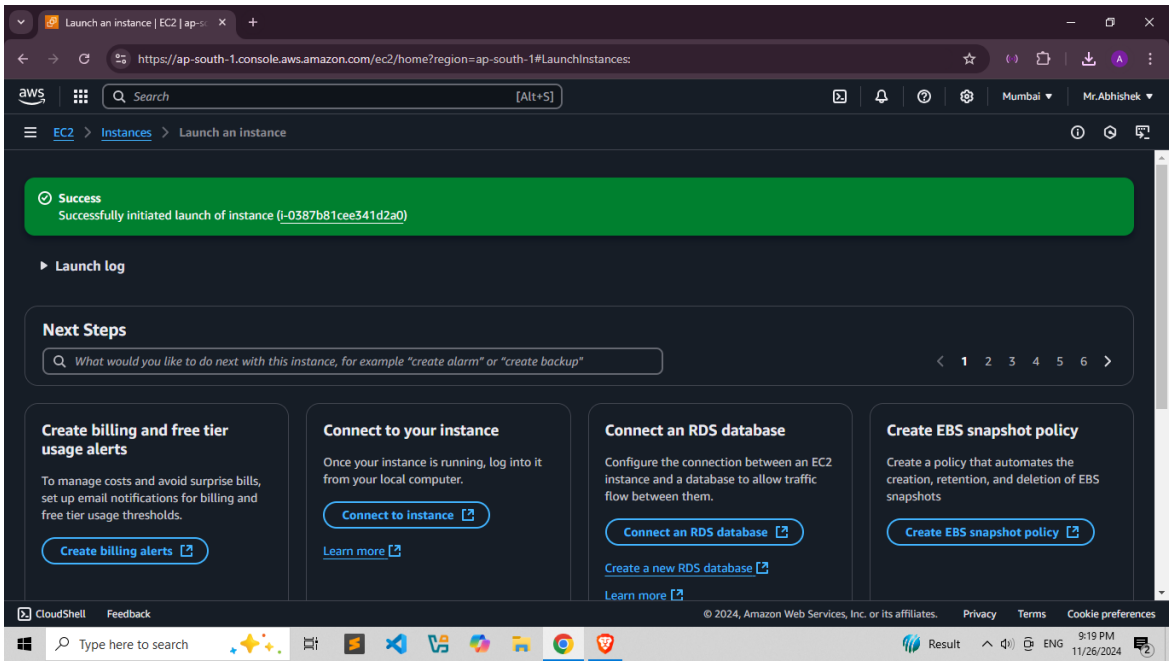
Step 8: Add Storage

- Configure the storage for your instance:
  - Root volume size (default is 8 GiB for Amazon Linux).
  - Add additional volumes if required.
  - Choose the storage type (e.g., General Purpose SSD).



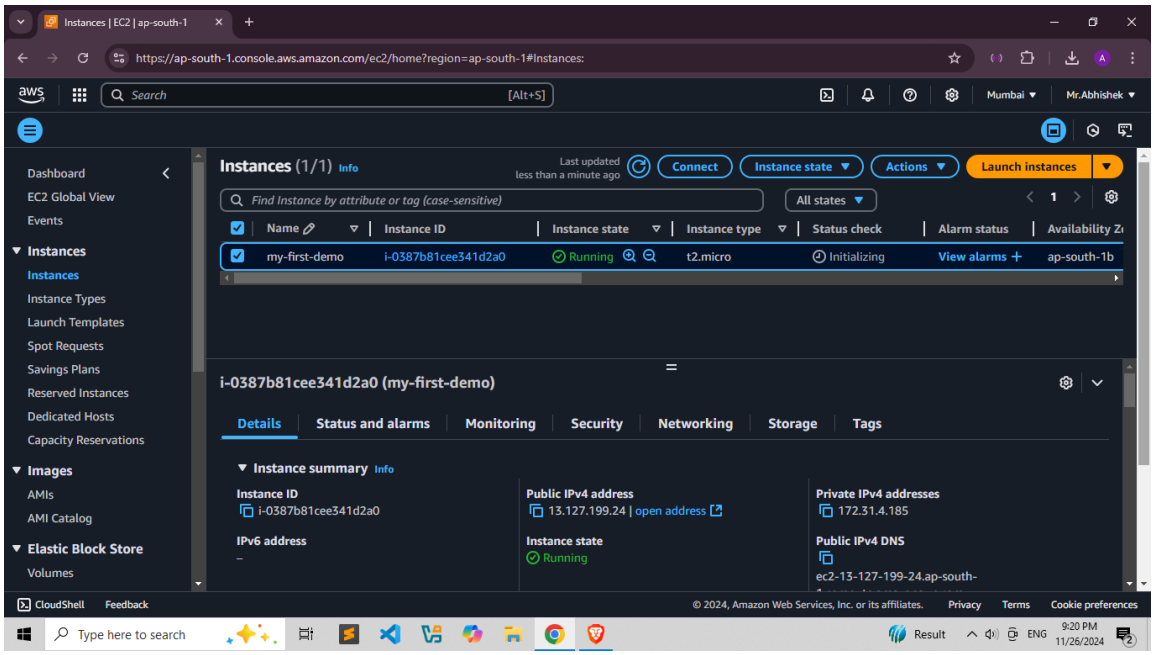
Step 9: Review and Launch

- Review all your configurations.
- If everything looks good, click **Launch**.



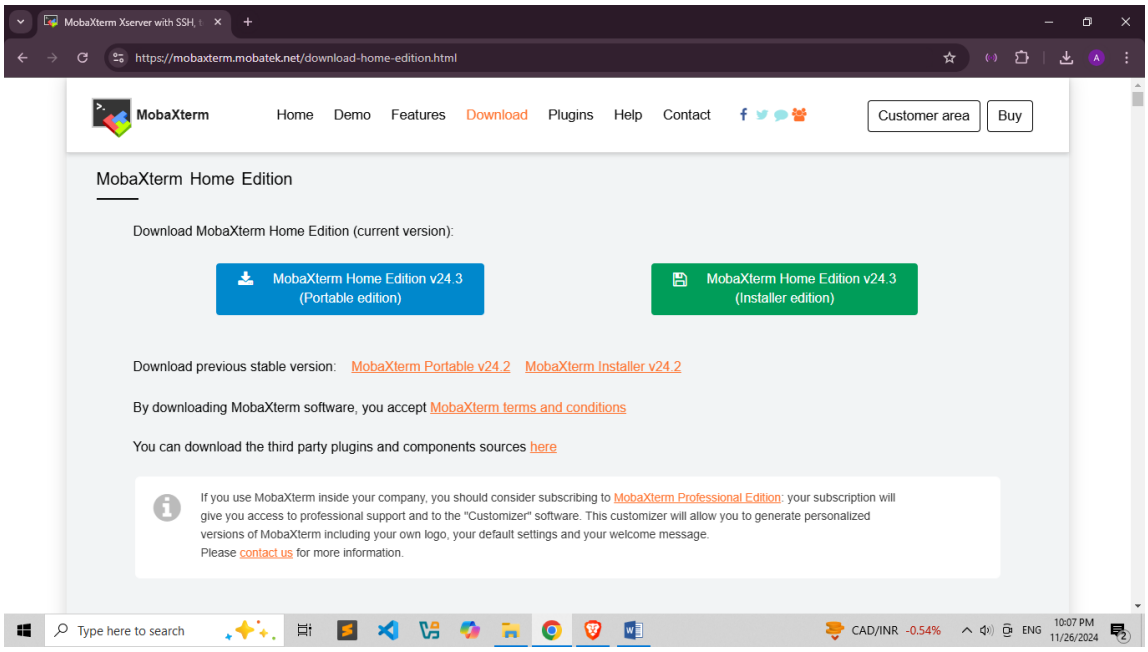
Step 10: Instance to Launch

- You will be redirected to a confirmation page.
- Click **View Instances** to go to the EC2 Dashboard and monitor the status of your instance.



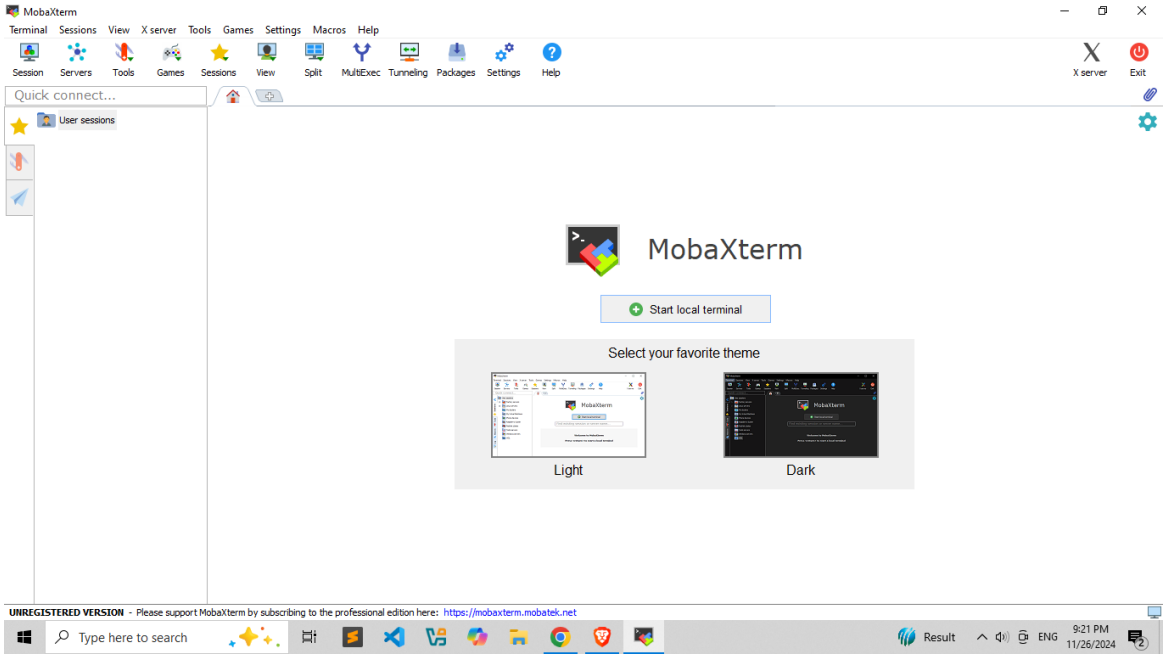
Step 11: Download and Install MobXStream

- Visit the official [MobXStream website](#) or any trusted download source.
- Install the application by following the on-screen instructions.



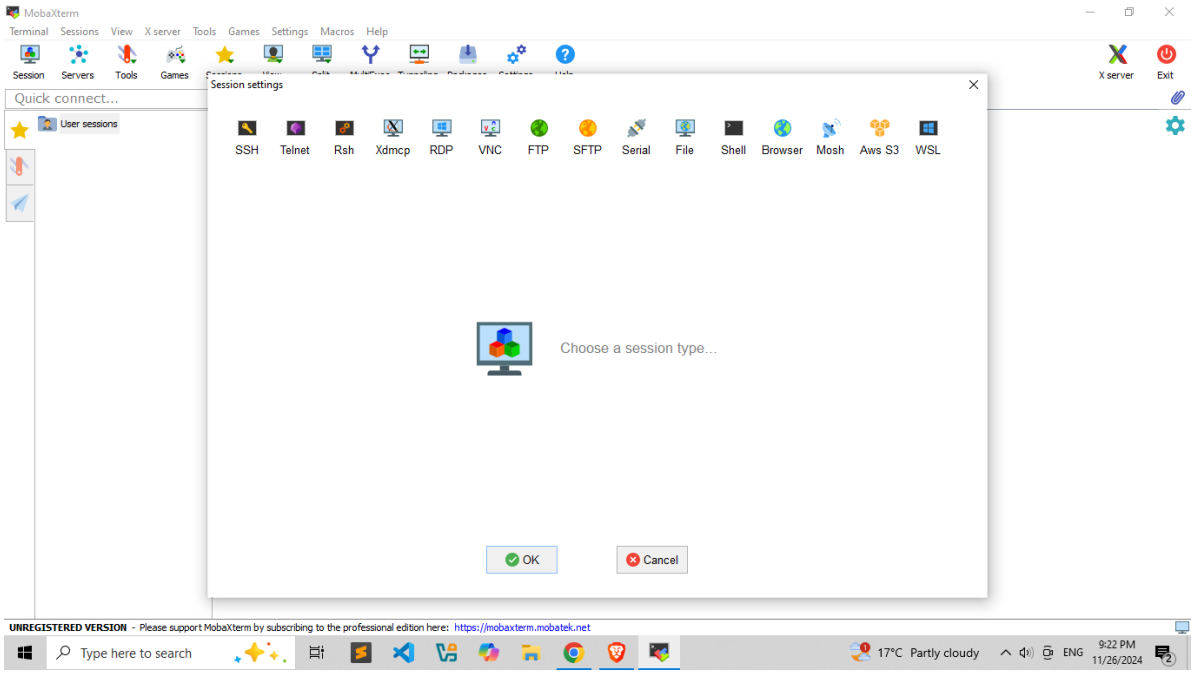
Step 12: Launch MobXStream

- Open the installed MobXStream application on your computer.



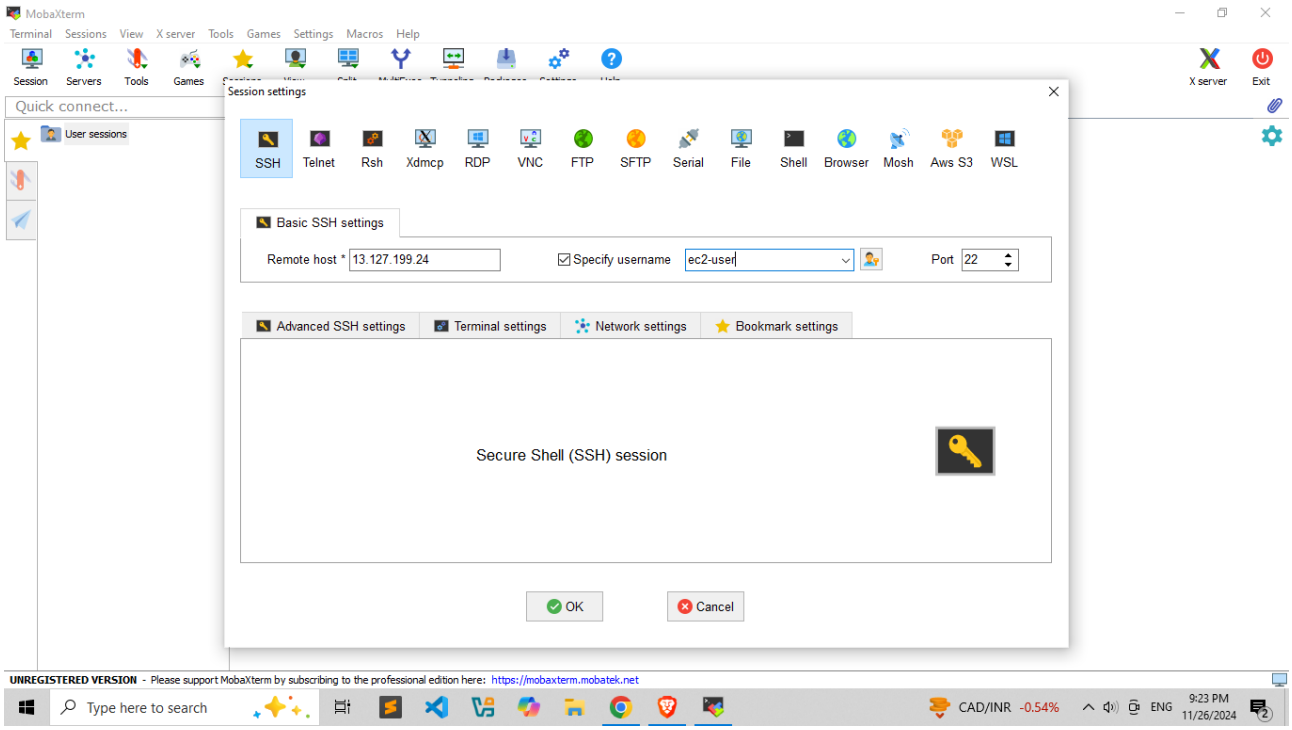
Step 13: Add a New Session in MobXStream

- Open MobXStream and click on the **Session** menu.
- Select **New Session** or similar (varies by version).



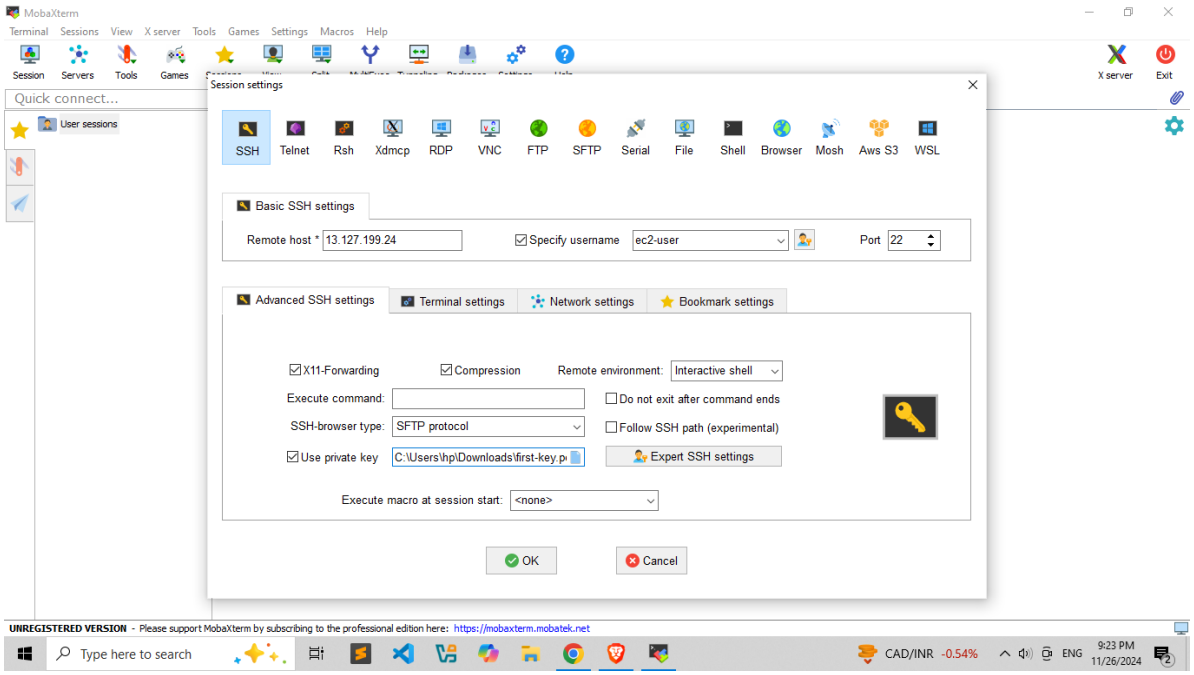
Step 14: Configure SSH Connection

- In the session settings, enter the following:
  - **Session Name**: Provide a descriptive name for your session (e.g., `My AWS EC2`).
  - **Host Name or IP Address**: Enter the **Public IP** of your EC2 instance.
  - **Port**: Set to **22** (default SSH port).
  - **Protocol**: Select **SSH**.



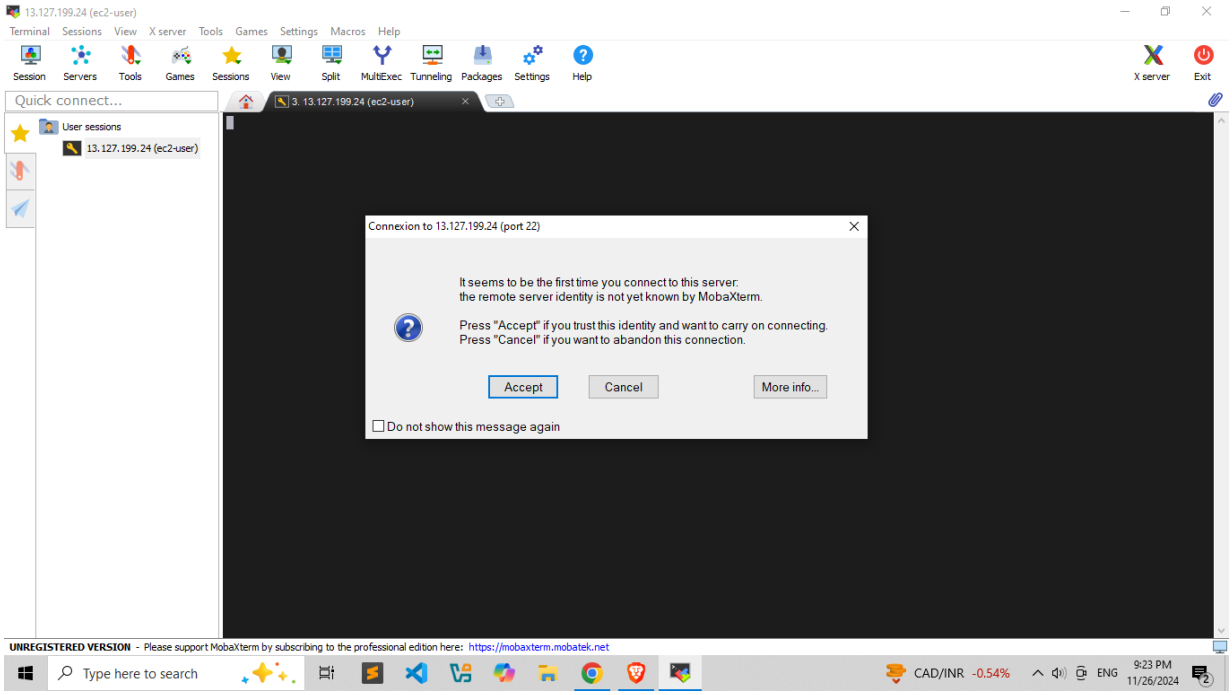
Step 15: Authenticate with the Key Pair

Private Key File: Browse and upload the .pem key pair file.

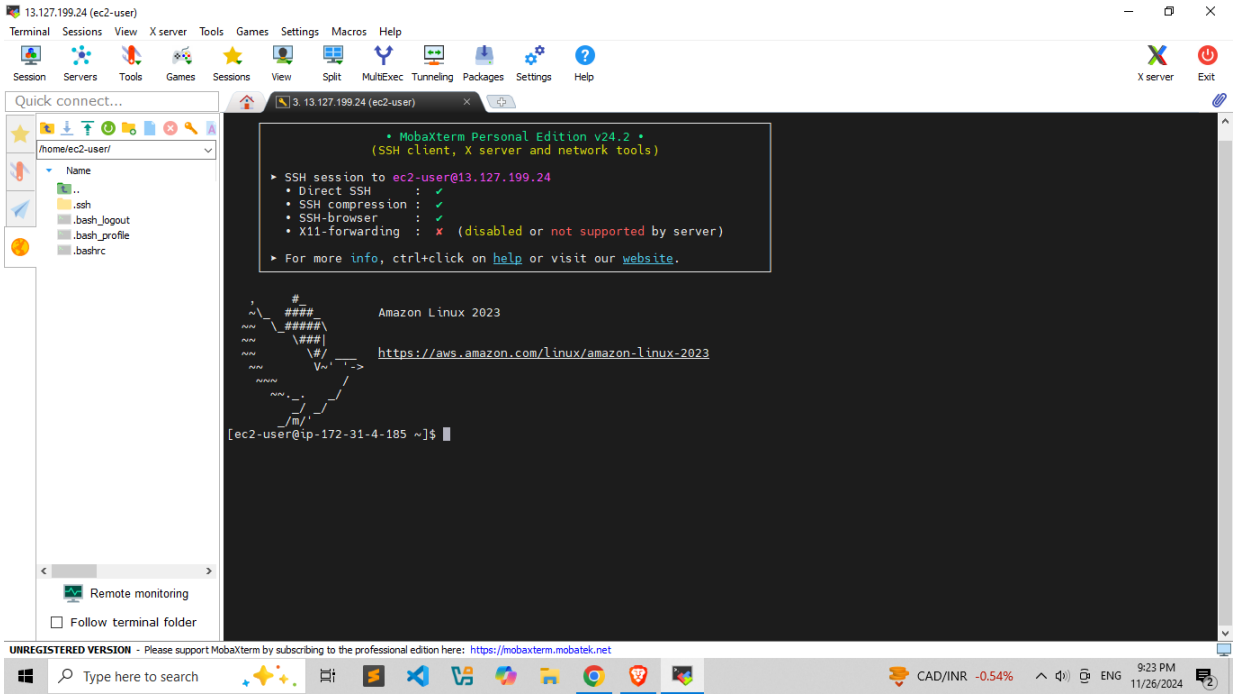


Step 16: Save and Connect

- Save the session settings.
- Double-click the saved session to initiate the connection.

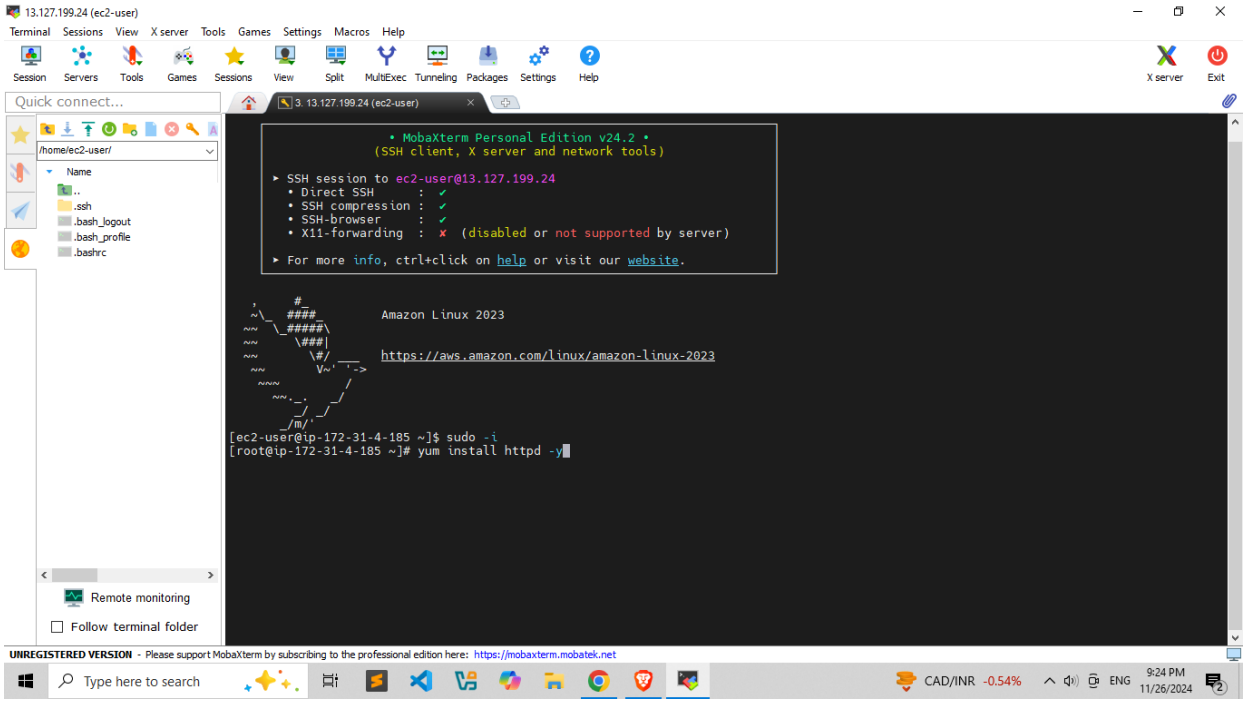


Step 17: Once connected, a terminal or remote desktop interface will appear (depending on your instance setup and MobXStream features).



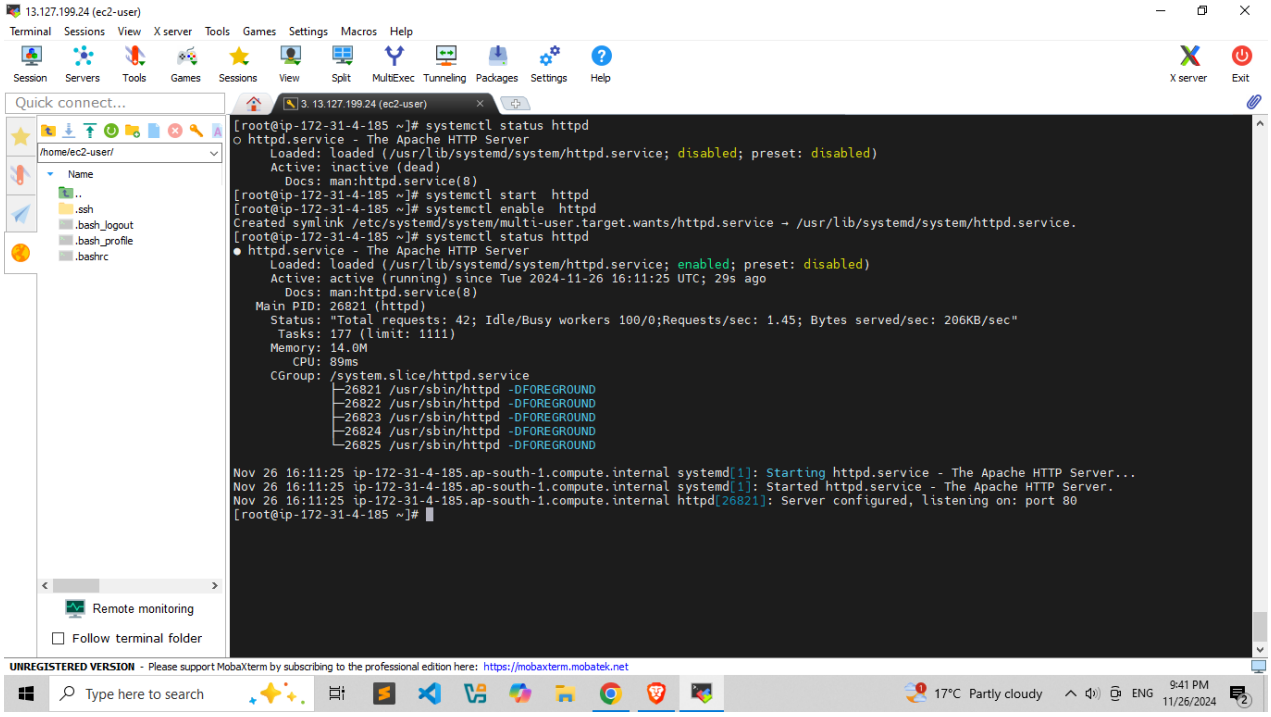
Step 18: Update the instance and install Apache:

yum install -y httpd



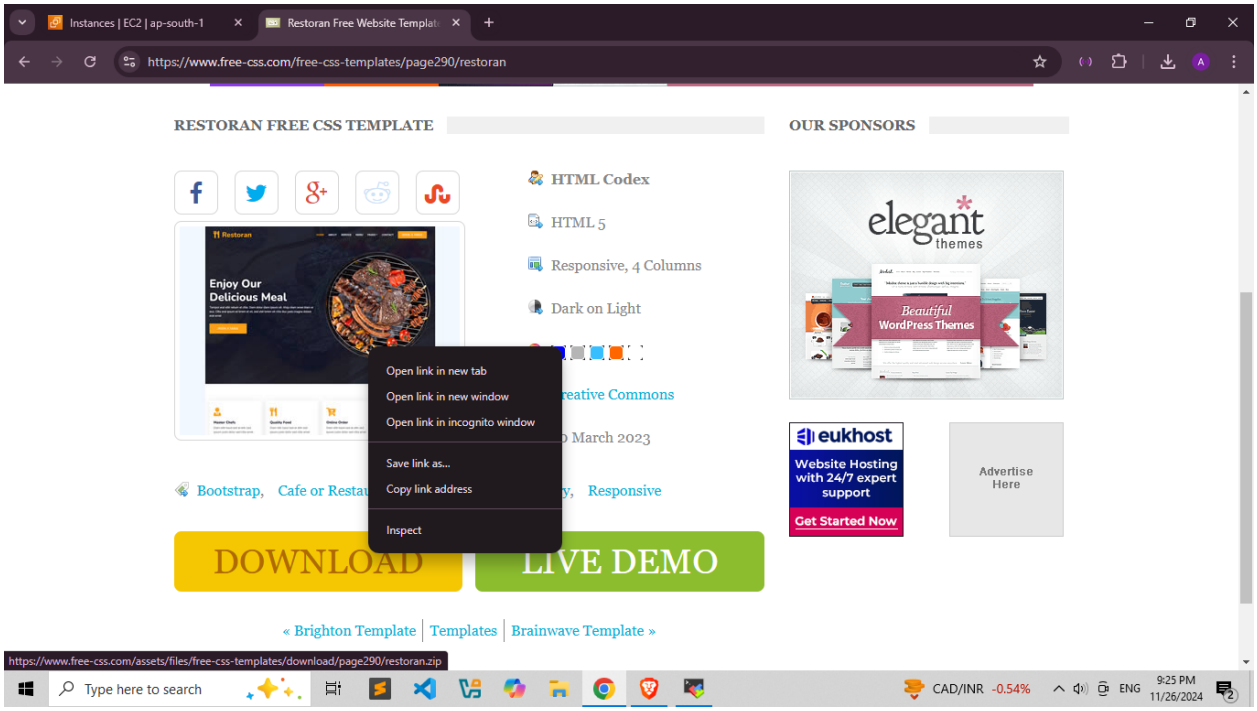
Step 19:Install Apache Web Server

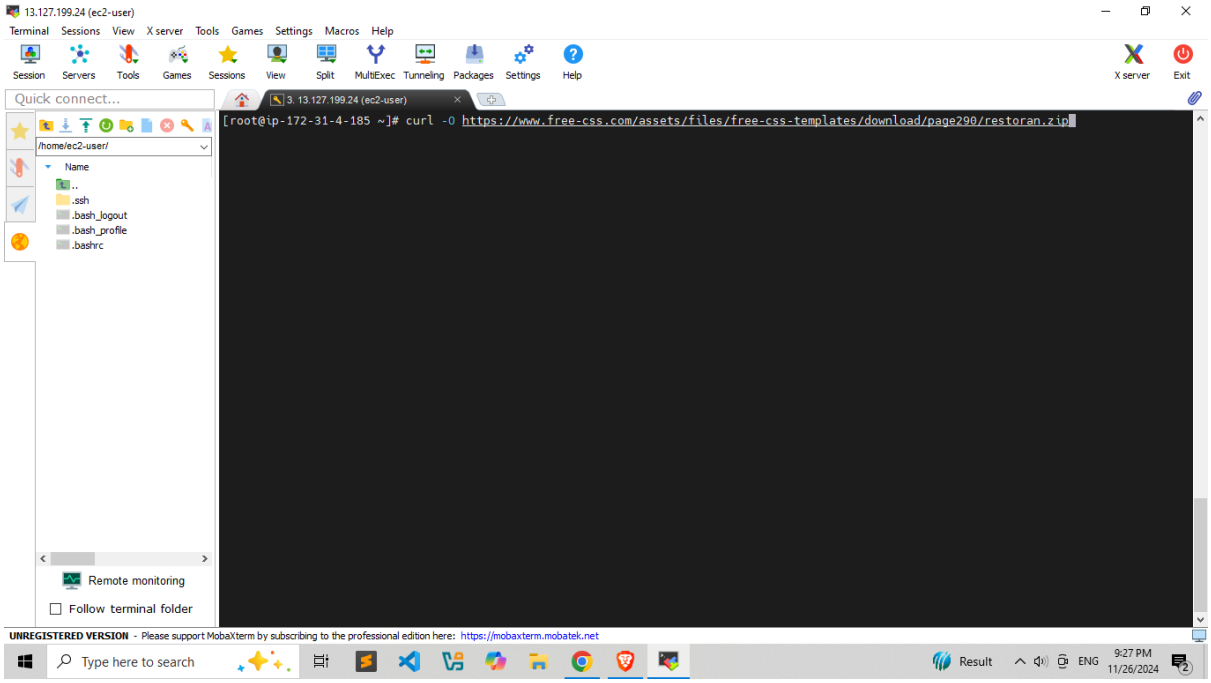
- Start and enable Apache service: **systemctl start httpd** and **systemctl enable httpd**

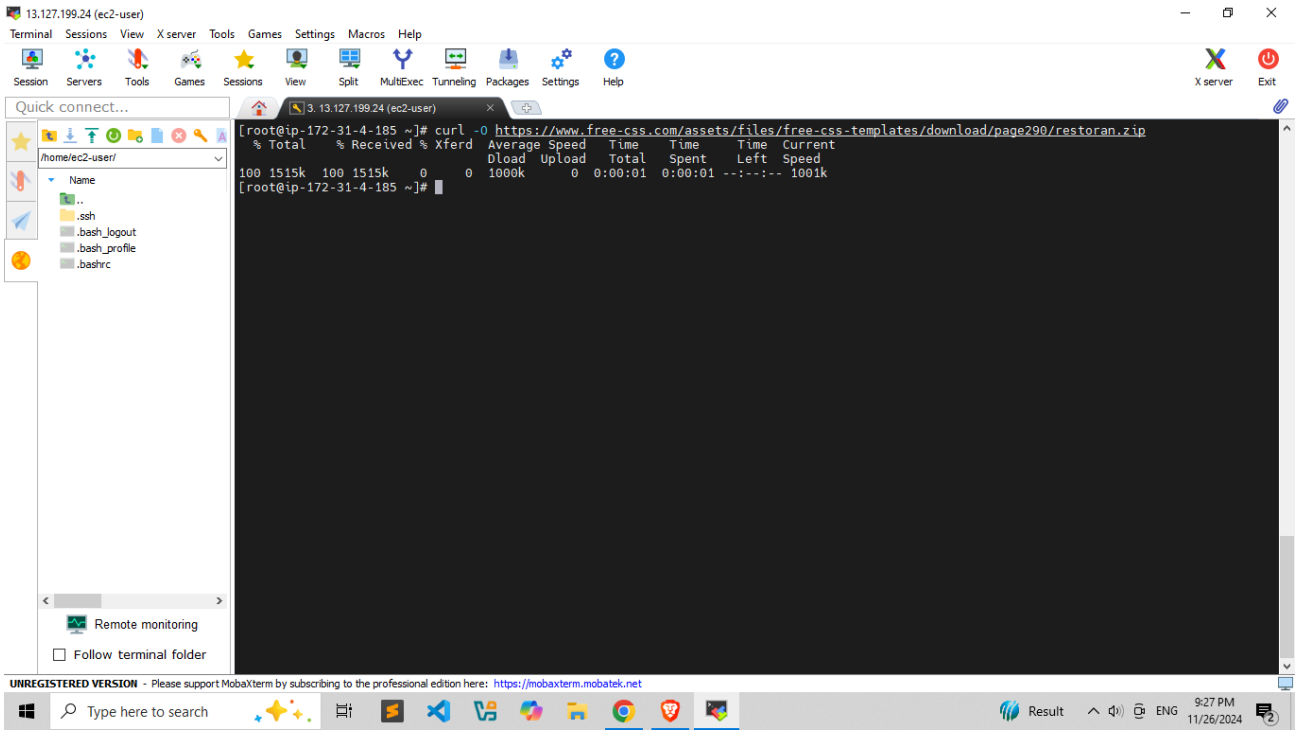


Step 20:Download the Free CSS Template

- On your local machine, download a free static website template from websites like:

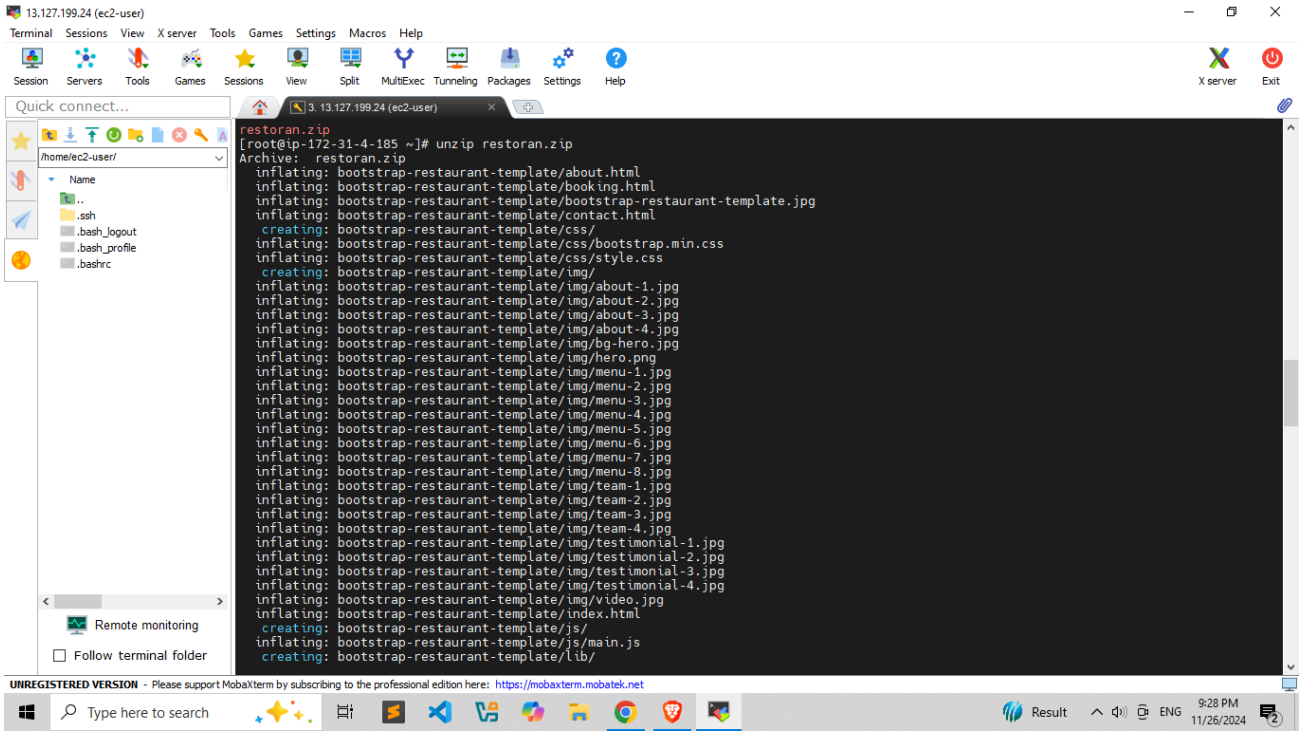


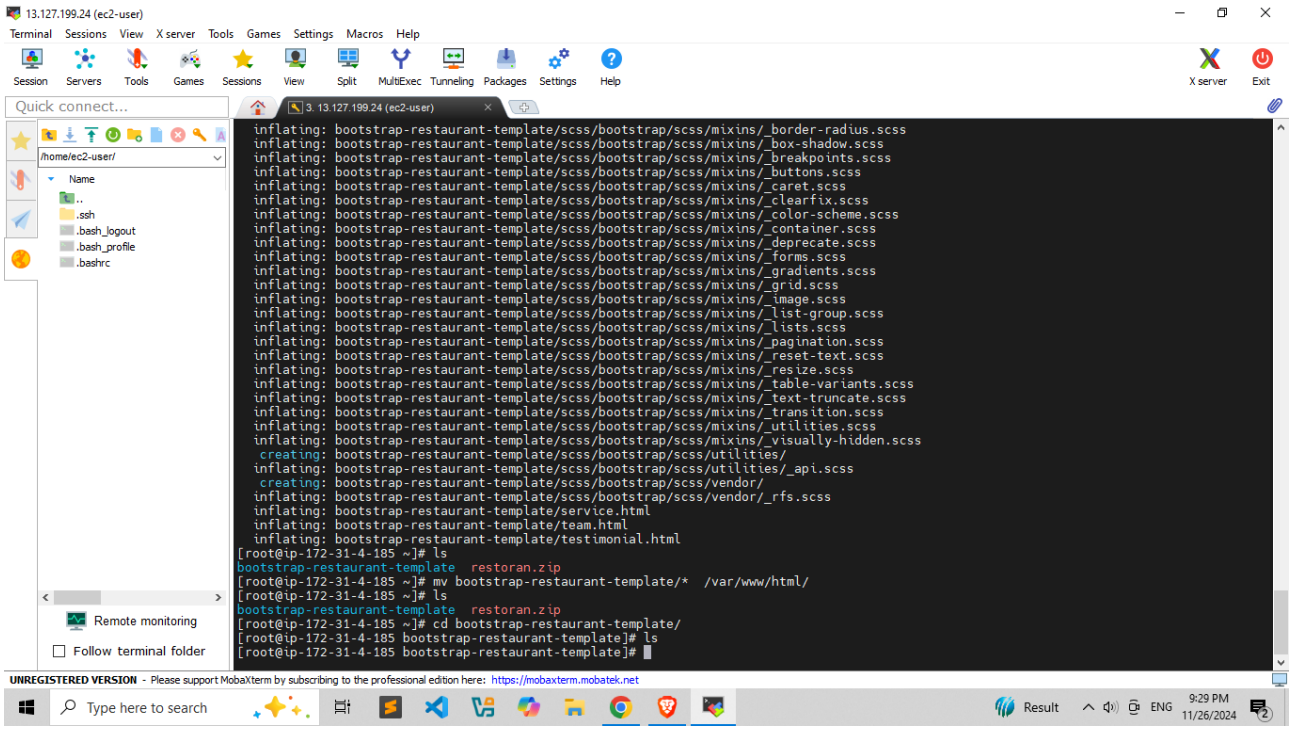

13.127.199.24 (ec2-user)
Terminal Sessions View X server Tools Games Settings Macros Help
Quick connect...
3. 13.127.199.24 (ec2-user)
[root@ip-172-31-4-185 ~]# curl -O https://www.free-css.com/assets/files/free-css-templates/download/page290/restoran.zip
/home/ec2-user/
Name
..
.ssh
.bash_logout
.bash_profile
.bashrc
Remote monitoring
Follow terminal folder
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
Result
ENG
9:27 PM
11/26/2024


13.127.199.24 (ec2-user)
Terminal Sessions View X server Tools Games Settings Macros Help
Quick connect...
3. 13.127.199.24 (ec2-user)
[root@ip-172-31-4-185 ~]# curl -O https://www.free-css.com/assets/files/free-css-templates/download/page290/restoran.zip
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 1515k 100 1515k 0 0 1000k 0 0:00:01 0:00:01 --:--:-- 1001k
[root@ip-172-31-4-185 ~]#
/home/ec2-user/
Name
..
.ssh
.bash_logout
.bash_profile
.bashrc
Remote monitoring
Follow terminal folder
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
Result
ENG
9:27 PM
11/26/2024

Step 21: Extract the Template

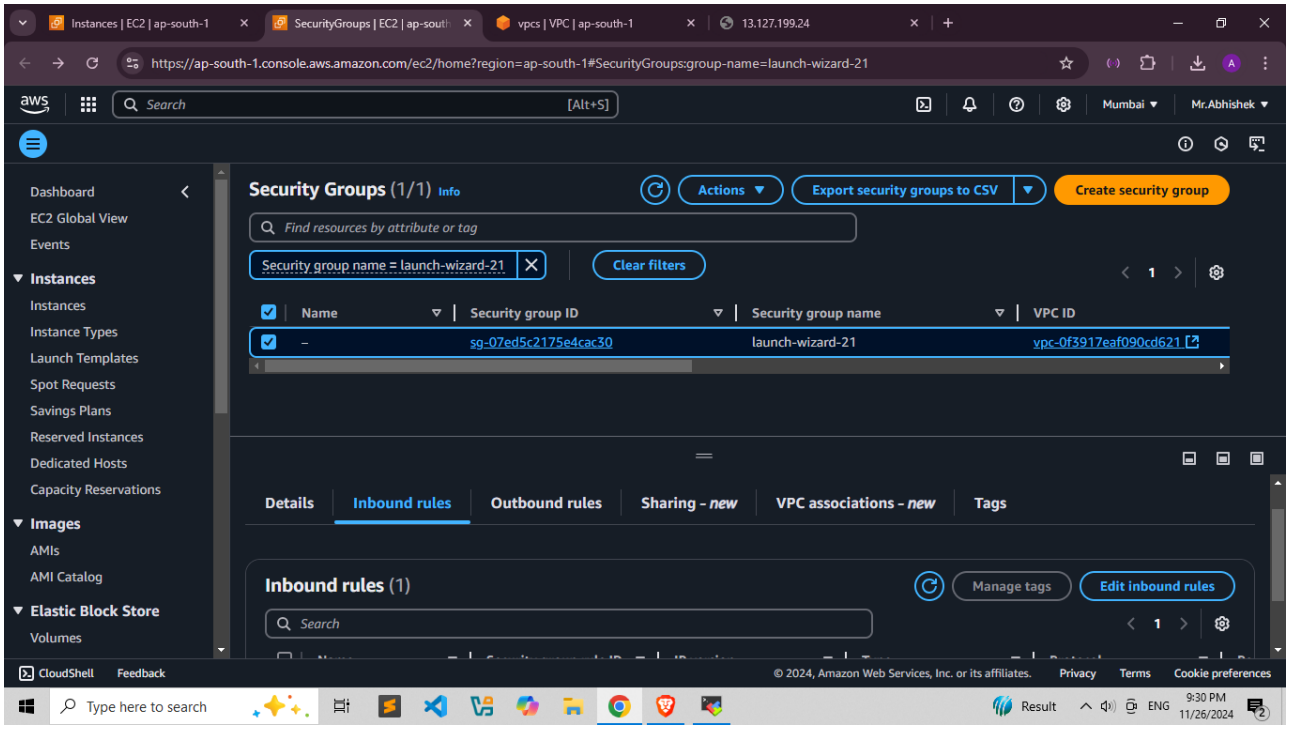
- Extract the `.zip` file on your local machine.
- Verify that the folder contains static files like:
  - `index.html`
  - Folders for `css`, `js`, `images`, etc.

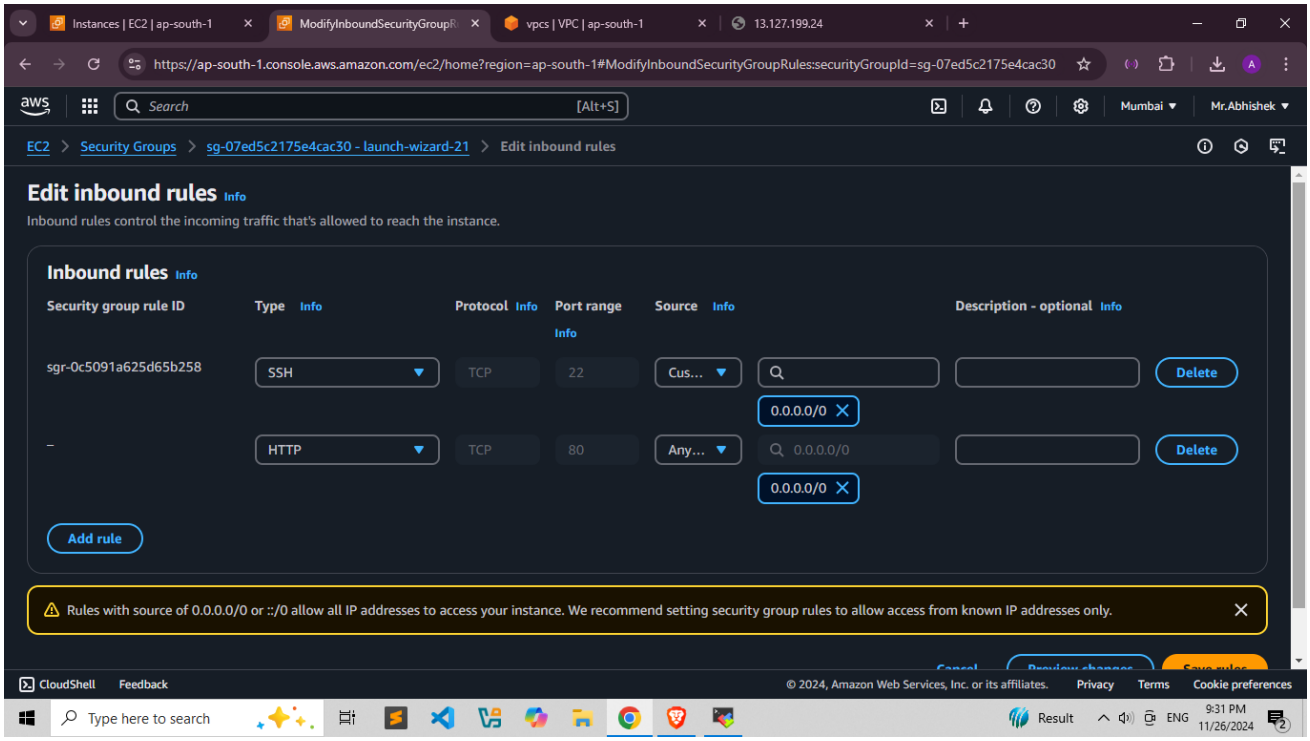


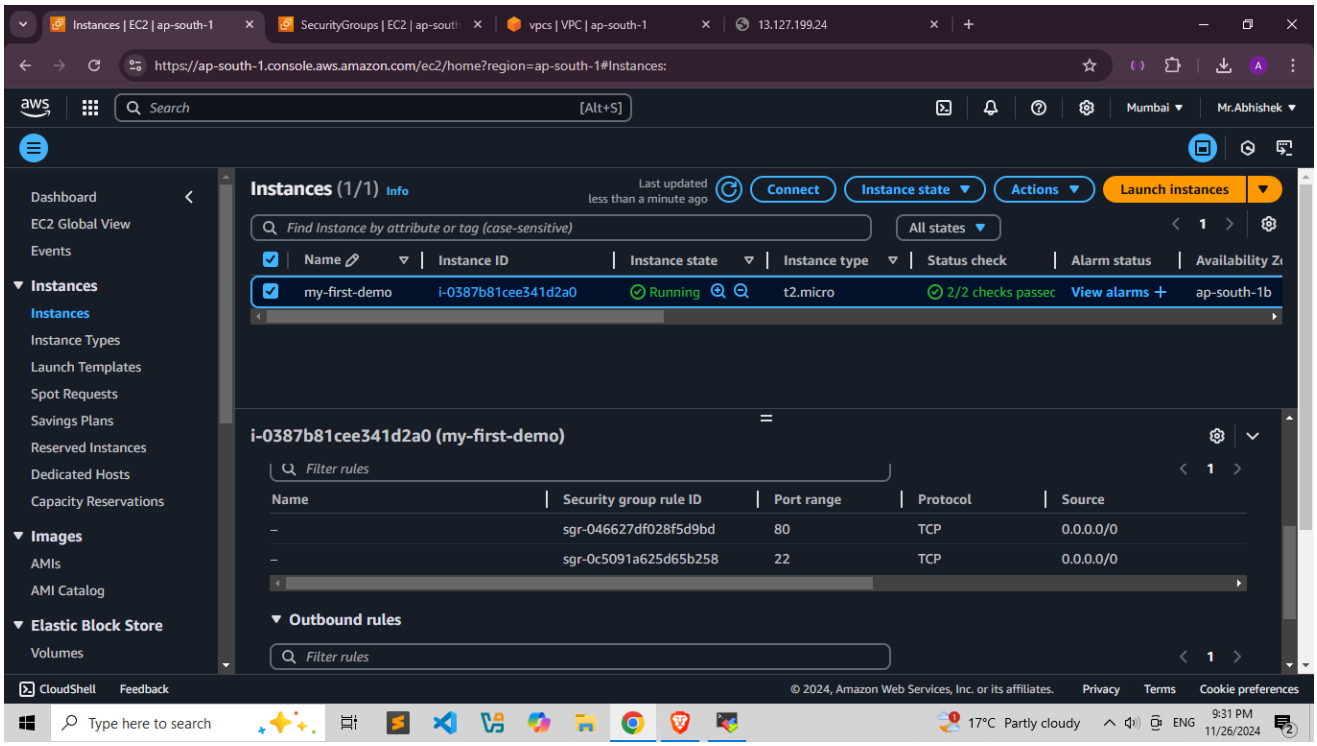


Step 22: Steps to Add HTTP Inbound Rule

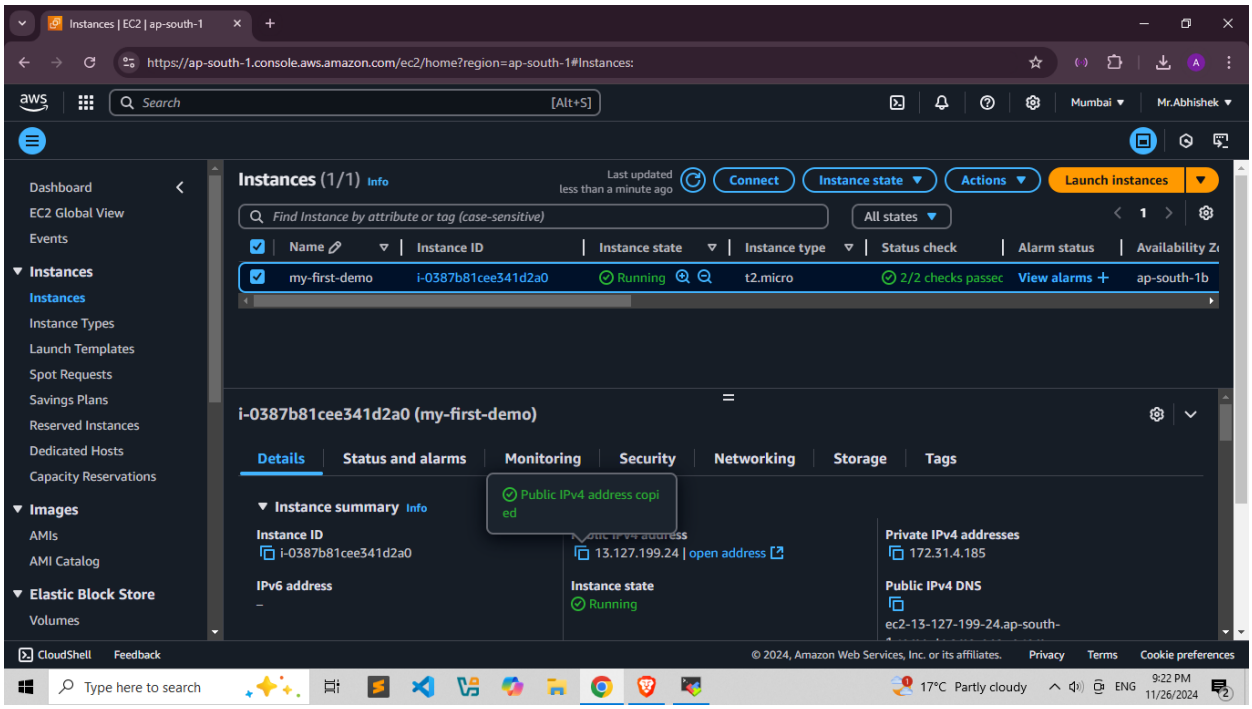
1. **Go to Security Groups**
   - From the EC2 Dashboard, click **Security Groups** in the left-hand menu.
2. **Select Your Security Group**
   - Find and select the Security Group associated with your EC2 instance.
3. **Edit Inbound Rules**
   - Click on the **Inbound Rules** tab and then click the **Edit inbound rules** button.
4. **Add HTTP Rule**
   - Click **Add Rule** and configure:
     - **Type**: HTTP
     - **Protocol**: TCP
     - **Port Range**: 80
     - **Source**: Anywhere (0.0.0.0/0) or My IP (for restricted access).



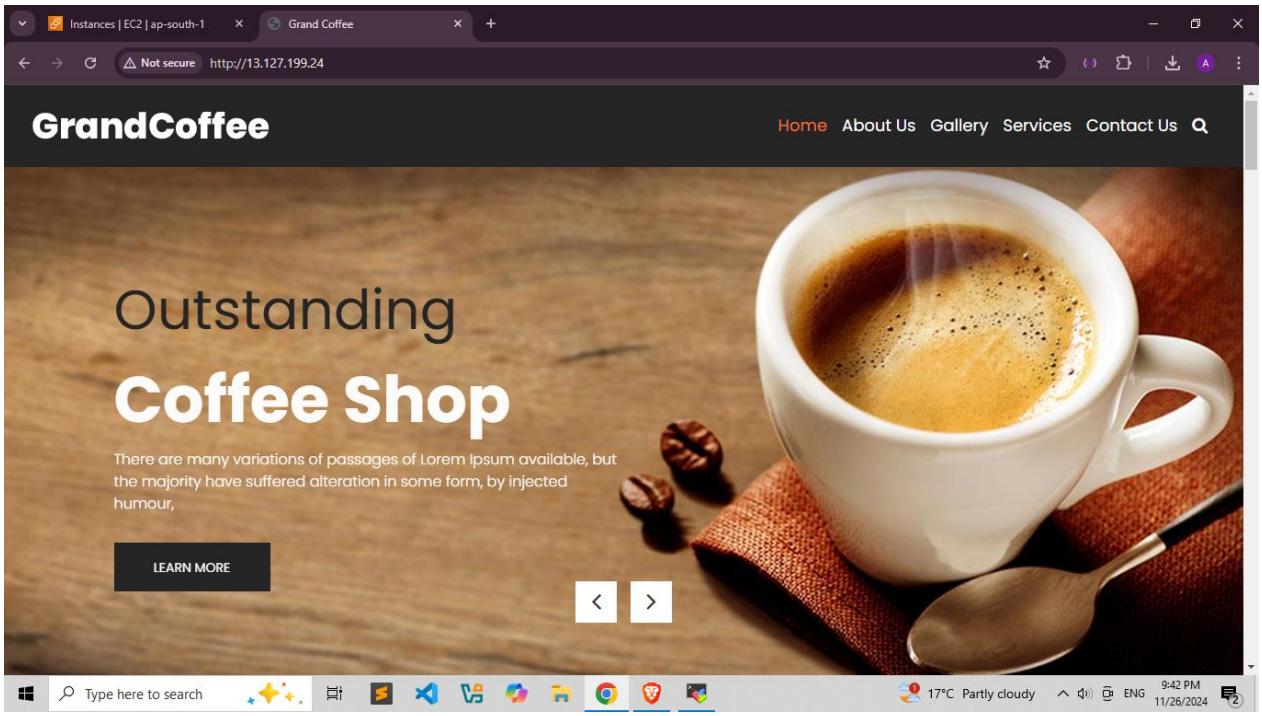

Instances | EC2 | ap-south-1
ModifyInboundSecurityGroupR
vpcs | VPC | ap-south-1
13.127.199.24
https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#ModifyInboundSecurityGroupRules:securityGroupId=sg-07ed5c2175e4cac30
Search
[Alt+S]
Mumbai
Mr.Abhishek
EC2 > Security Groups > sg-07ed5c2175e4cac30 - launch-wizard-21 > Edit inbound rules
Edit inbound rules Info
Inbound rules control the incoming traffic that's allowed to reach the instance.
Inbound rules Info
Security group rule ID
Type Info
Protocol Info
Port range Info
Source Info
Description - optional Info
sgr-0c5091a625d65b258
SSH
TCP
22
Cus...
0.0.0.0/0
Delete
HTTP
TCP
80
Any...
0.0.0.0/0
Delete
Add rule
Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
Result
ENG
9:31 PM
11/26/2024


Instances | EC2 | ap-south-1
SecurityGroups | EC2 | ap-south
vpcs | VPC | ap-south-1
13.127.199.24
https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#Instances:
Search
[Alt+S]
Mumbai
Mr.Abhishek
Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Instances (1/1) Info
Last updated less than a minute ago
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zo
my-first-demo
i-0387b81cee341d2a0
Running
t2.micro
2/2 checks passed
View alarms +
ap-south-1b
i-0387b81cee341d2a0 (my-first-demo)
Filter rules
Name
Security group rule ID
Port range
Protocol
Source
sgr-046627df028f5d9bd
80
TCP
0.0.0.0/0
sgr-0c5091a625d65b258
22
TCP
0.0.0.0/0
Outbound rules
Filter rules
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
17°C Partly cloudy
ENG
9:31 PM
11/26/2024

Step 22: Copy the Public IP address from instance details paste to the other new tab:



Step 23: View the Website Host in Public ip address 13.127.199.24



Step 24: Select instance and in the right corner click on **Instant State** and Select **Terminate(delete) instance**.