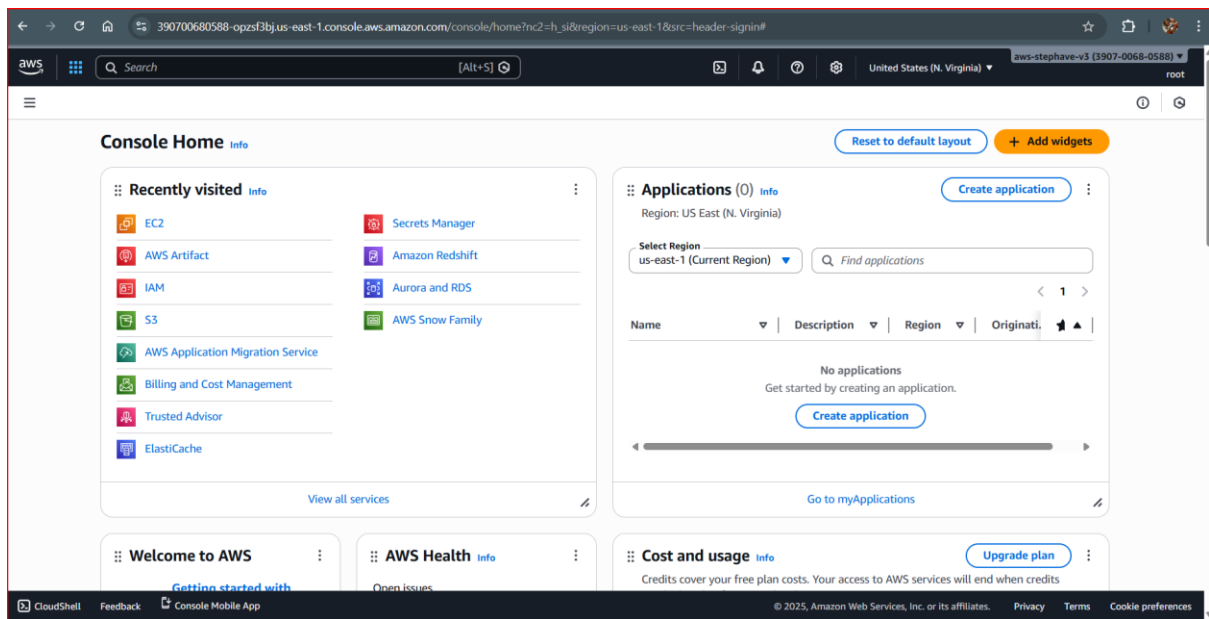
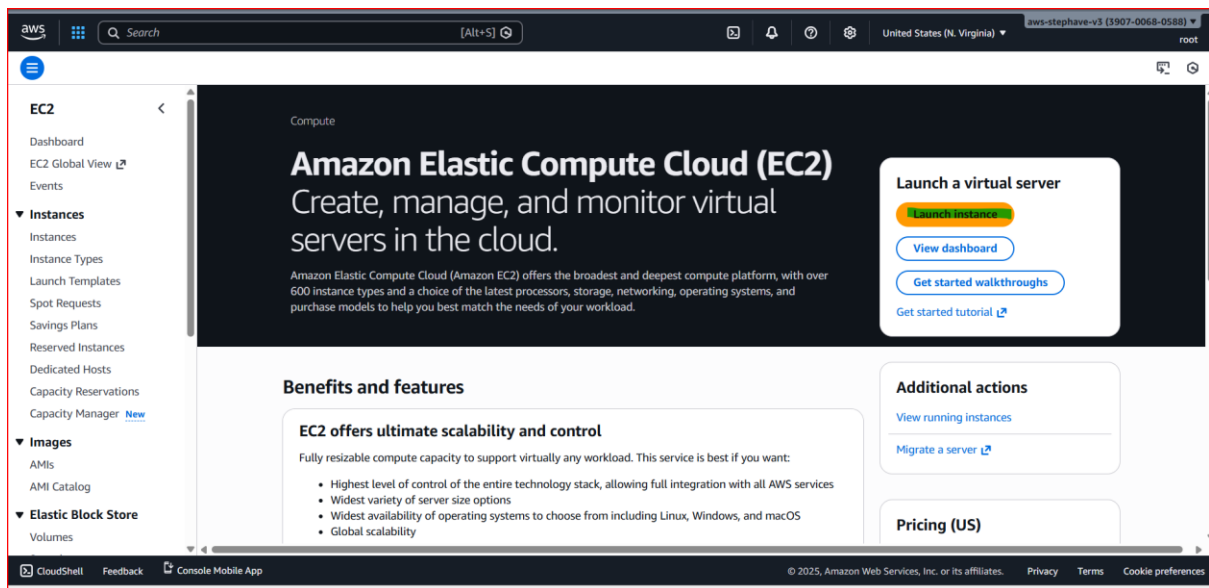


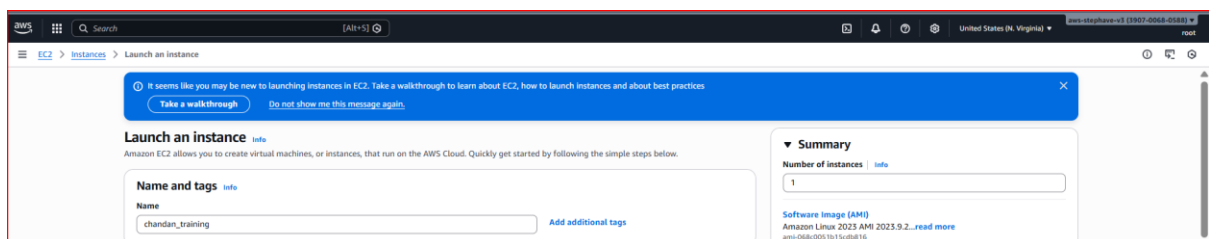
Login to AWS console



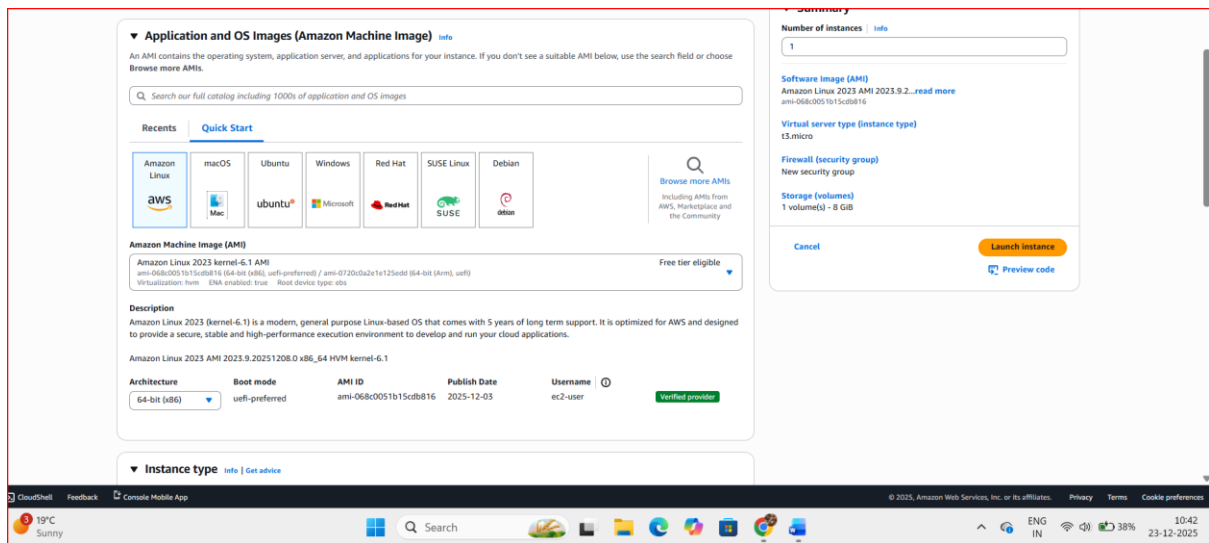
Select EC2 and click on Launch Instance



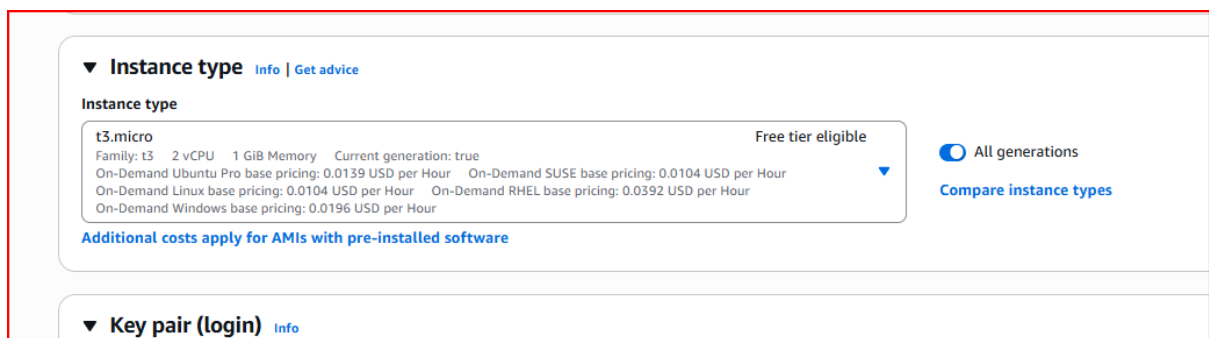
Give the name for your instance. Here we have named it as Chandan_Training



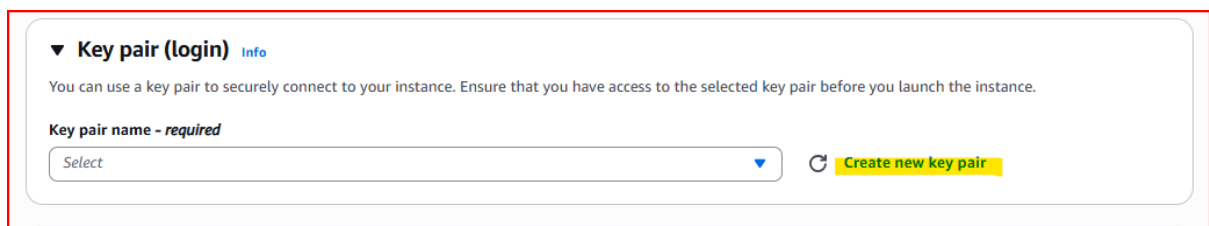
Select an operating system. For e.g select Amazon Linux.



In instance type, Select t3.micro (Free tier eligible)



Click on Create Key pair



Enter keypair name which you can easily remember->key pair type- keypair file format. For this one I have selected .pem and click on create key pair

Create key pair

Key pair name
Key pairs allow you to connect to your instance securely.

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

☒ **RSA**
RSA encrypted private and public key pair

☐ **ED25519**
ED25519 encrypted private and public key pair

Private key file format

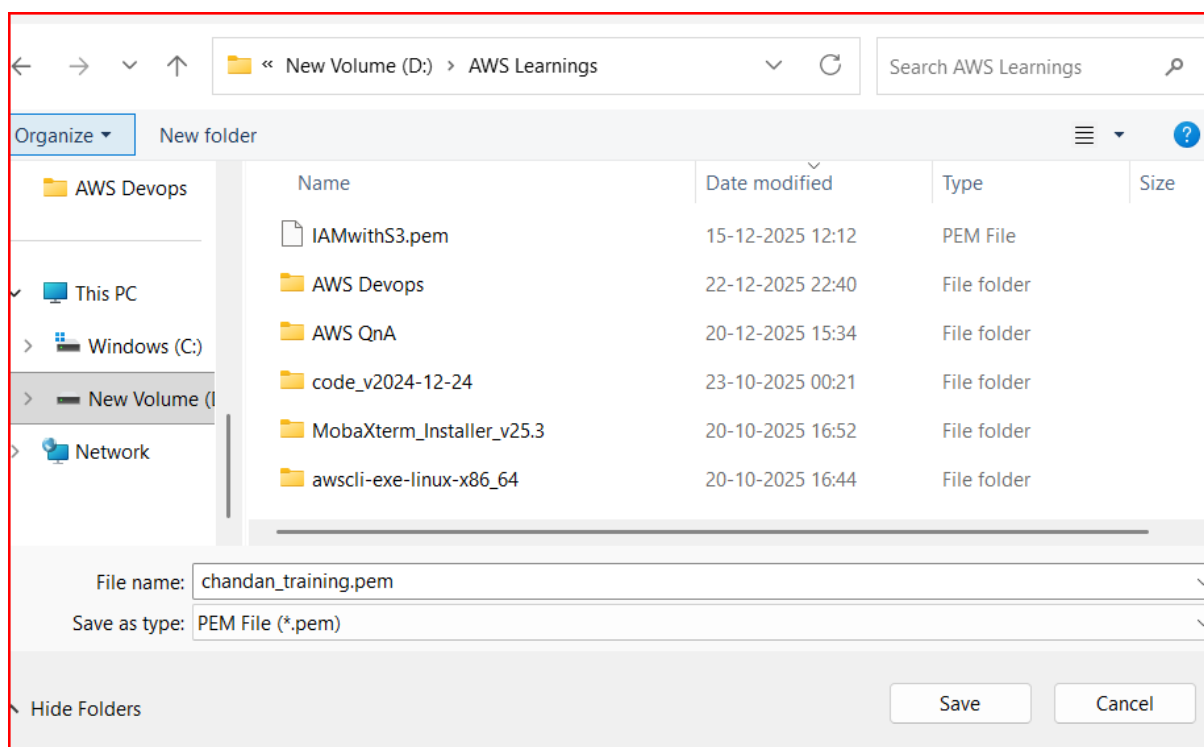
☒ **.pem**
For use with OpenSSH

☐ **.ppk**
For use with PuTTY

⚠ When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** [Learn more](#)

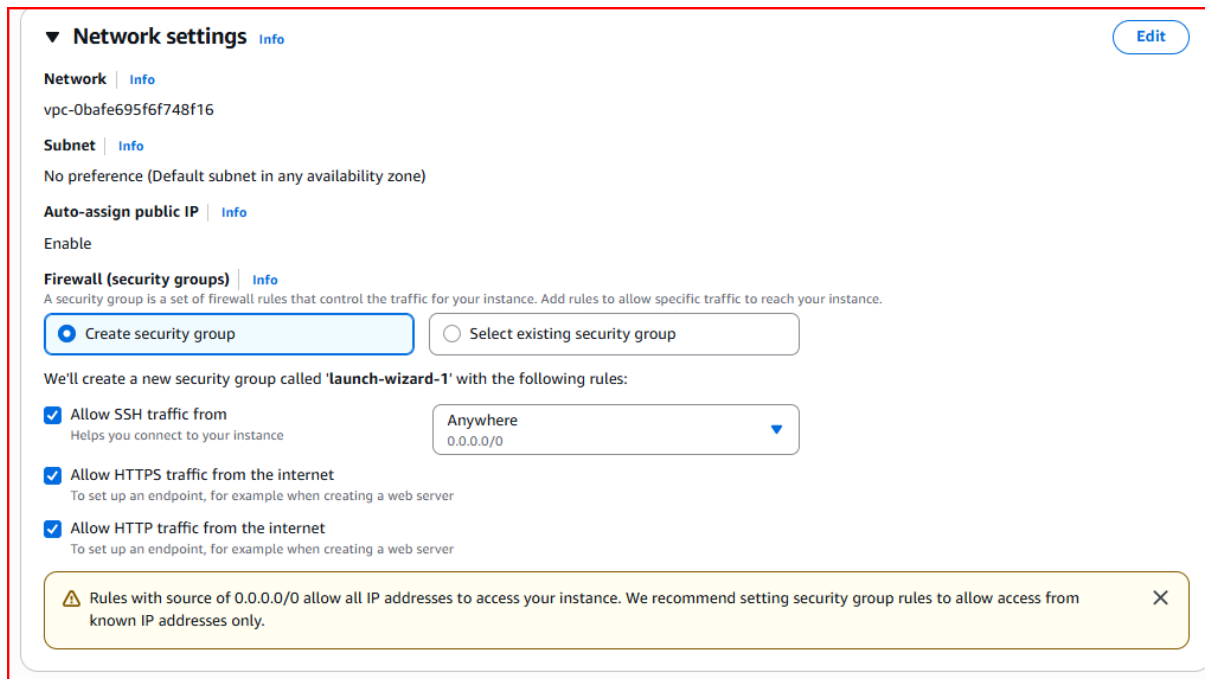
Cancel Create key pair

Key get generated and save it on your drive folder. Key pair get saved.



Network Setting

You can enable all ports for learning purpose where port allowed traffic



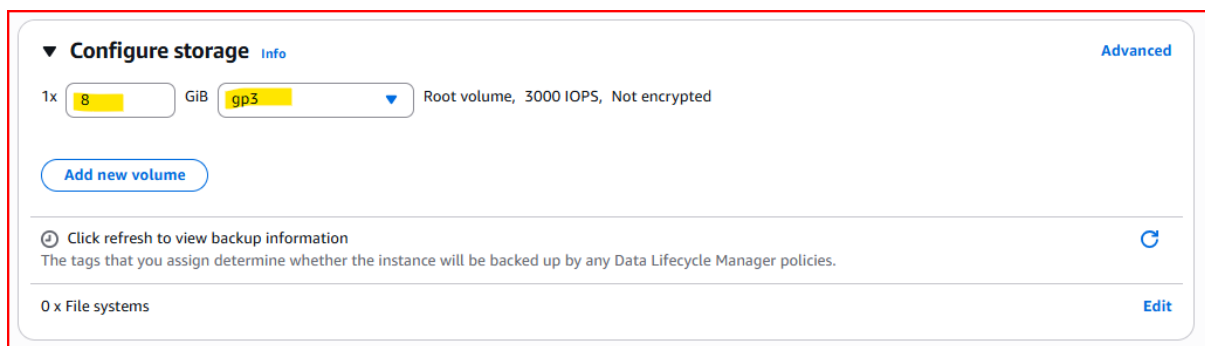
The screenshot shows the 'Network settings' section of an AWS console. It includes fields for 'Network' (vpc-0baf695f6f748f16), 'Subnet' (No preference), and 'Auto-assign public IP' (Enable). The 'Firewall (security groups)' section is active, showing options to 'Create security group' or 'Select existing security group'. Below, it lists rules for 'launch-wizard-1': 'Allow SSH traffic from Anywhere', 'Allow HTTPS traffic from the internet', and 'Allow HTTP traffic from the internet'. A warning message at the bottom states: 'Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.'

Note:- Security group either you can create new or select existing group if available.

[AWS [Security Groups](#) are virtual firewalls for EC2 instances, controlling inbound/outbound traffic via stateful rules (allow by default for responses) based on protocol, port, and source/destination]

Storage Configuration

Storage configuration in AWS EC2 involves choosing from several options to meet different requirements for persistence, performance, and scalability. The primary storage types are **Amazon Elastic Block Store (EBS)** and **Instance Store**, which can be complemented by other AWS storage services like Amazon S3, EFS, and FSx.



The screenshot shows the 'Configure storage' section of an AWS console. It displays a configuration for 1x 8 GiB gp3 Root volume, 3000 IOPS, Not encrypted. There is an 'Add new volume' button. Below, there is a section for backup information with a refresh icon and a note: 'Click refresh to view backup information. The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.' At the bottom, it shows '0 x File systems' and an 'Edit' button.

Click on Launch Instance

Enable

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group
 ☐ Select existing security group

We'll create a new security group called 'launch-wizard-1' with the following rules:

☒ Allow SSH traffic from
Helps you connect to your instance
Anywhere
0.0.0.0/0

☒ Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server

☒ Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Configure storage [Info](#)

1x 8 GiB gp3 Root volume, 3000 IOPS, Not encrypted

[Add new volume](#)

Click refresh to view backup information
The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems

Advanced details [Info](#)

Summary

Number of instances [Info](#)

1

Software image (AMI)
Amazon Linux 2023 AMI 2023.9.2...[read more](#)
ami-058c0051a15c0b1e16

Virtual server type (instance type)
t3.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

Cancel [Launch instance](#) [Preview code](#)

To verify instance status go EC2-> View All Instances -> You will be able to see your new instance.

EC2

Dashboard

EC2 Global View

Events

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

Capacity Manager [New](#)

Images

AMIs

AMI Catalog

Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

Network & Security

Security Groups

Elastic IPs

Placement Groups

Key Pairs

Network Interfaces

Instances (2) [Info](#)

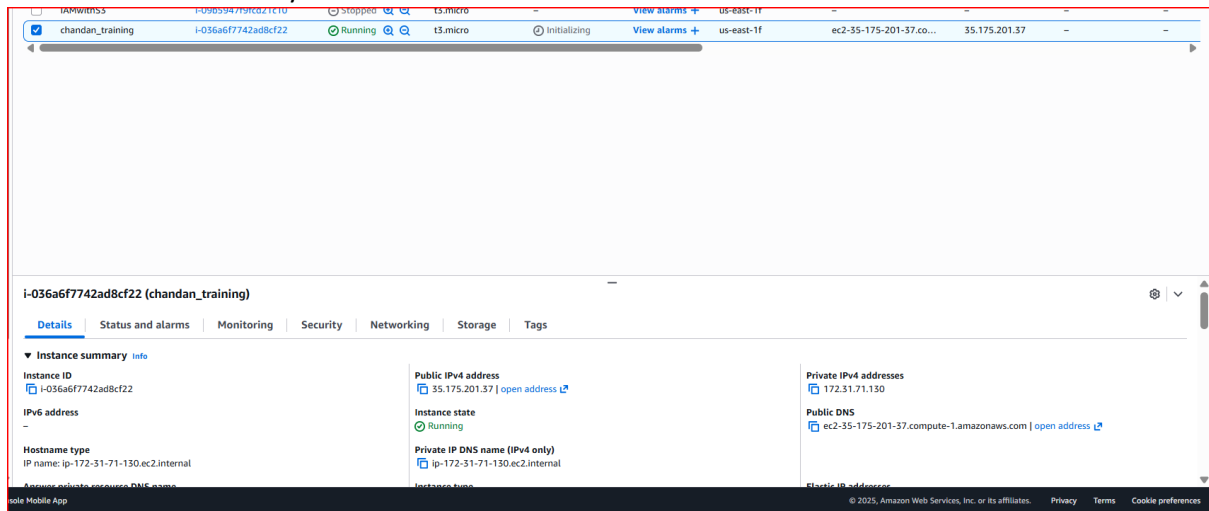
Find Instance by attribute or tag (case-sensitive)

All states

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs
IAMwidth53	i-0960947f9fcd21c10	Stopped	t3.micro			us-east-1f				
chandan_training	i-036a6f7742ad8cf22	Running	t3.micro	Initializing		us-east-1f	ec2-35-175-201-37.co...	35.175.201.37		

Select an instance

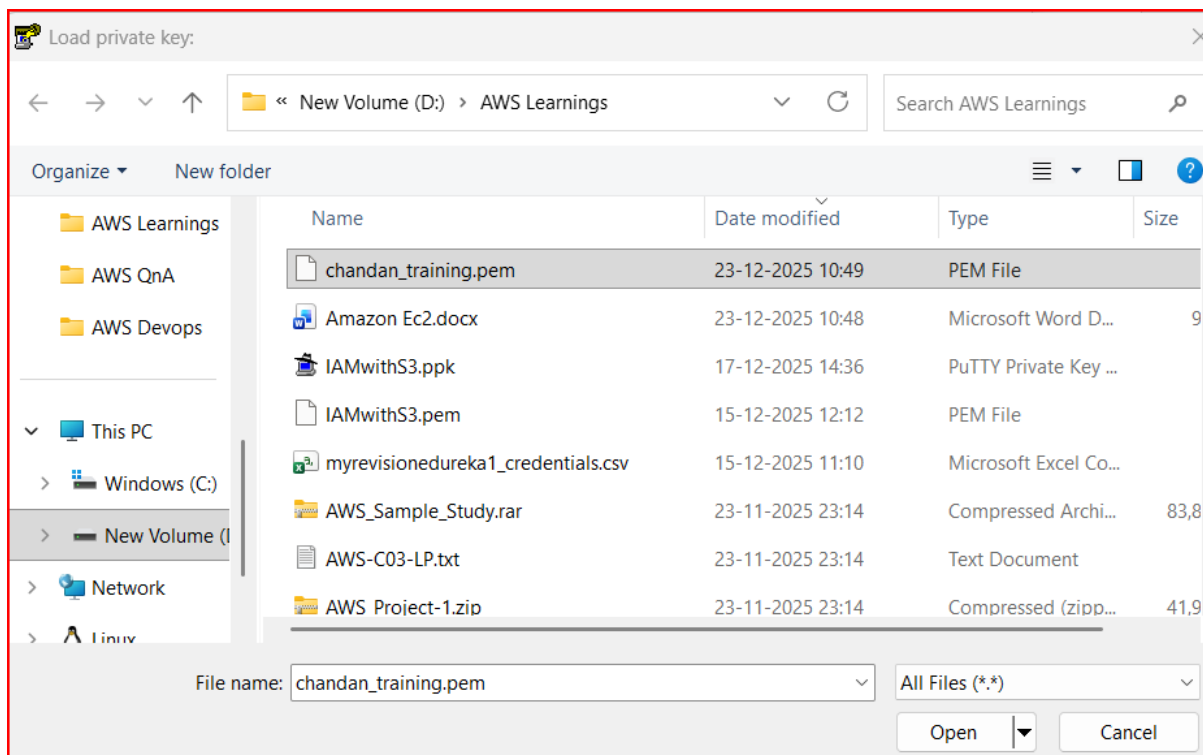
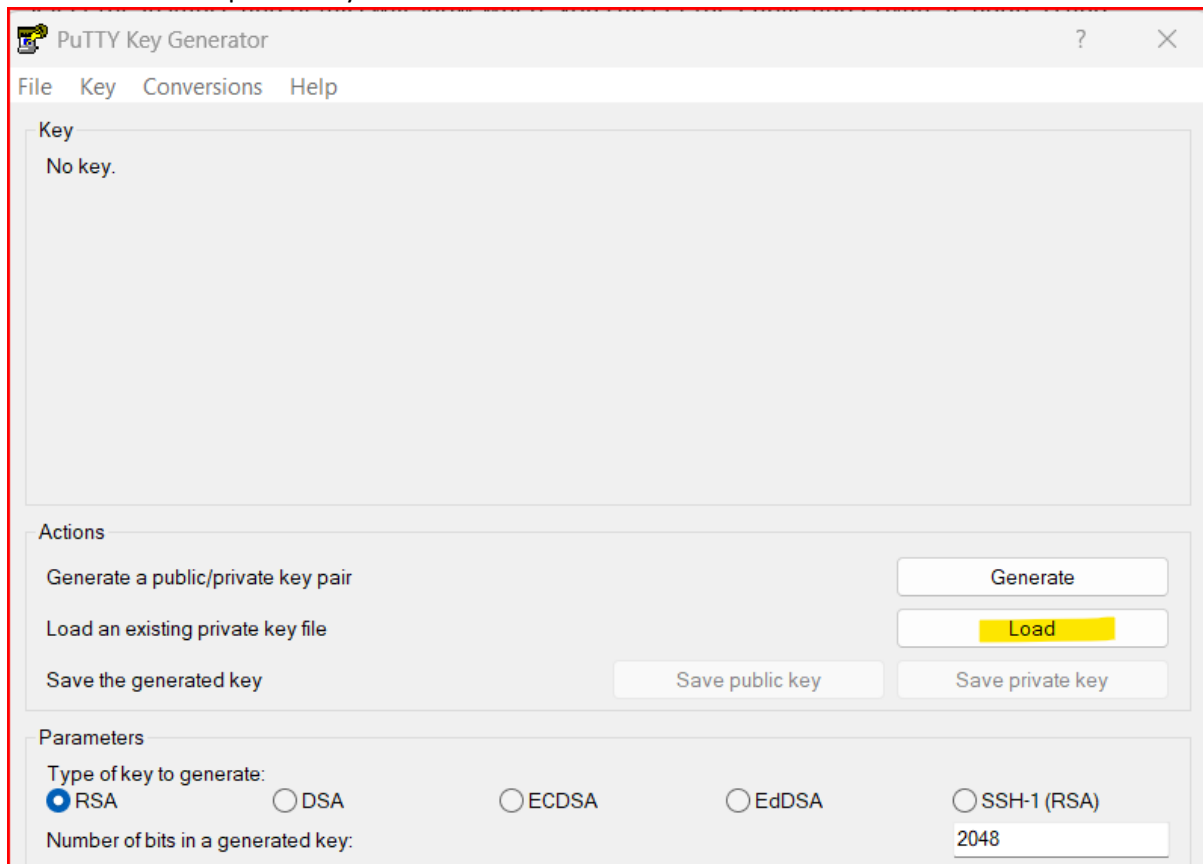
Select the instance and details will show where you can get the Public and Private IP address and other details related to your instance.

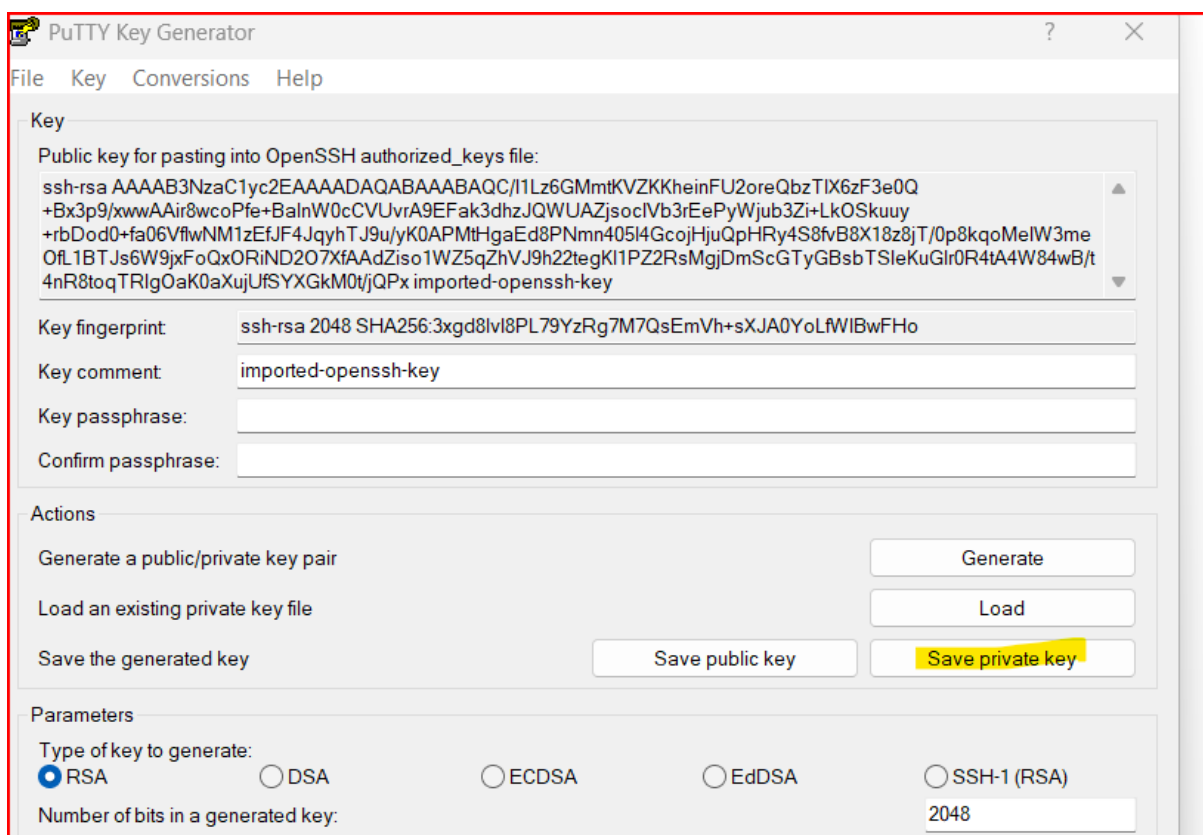
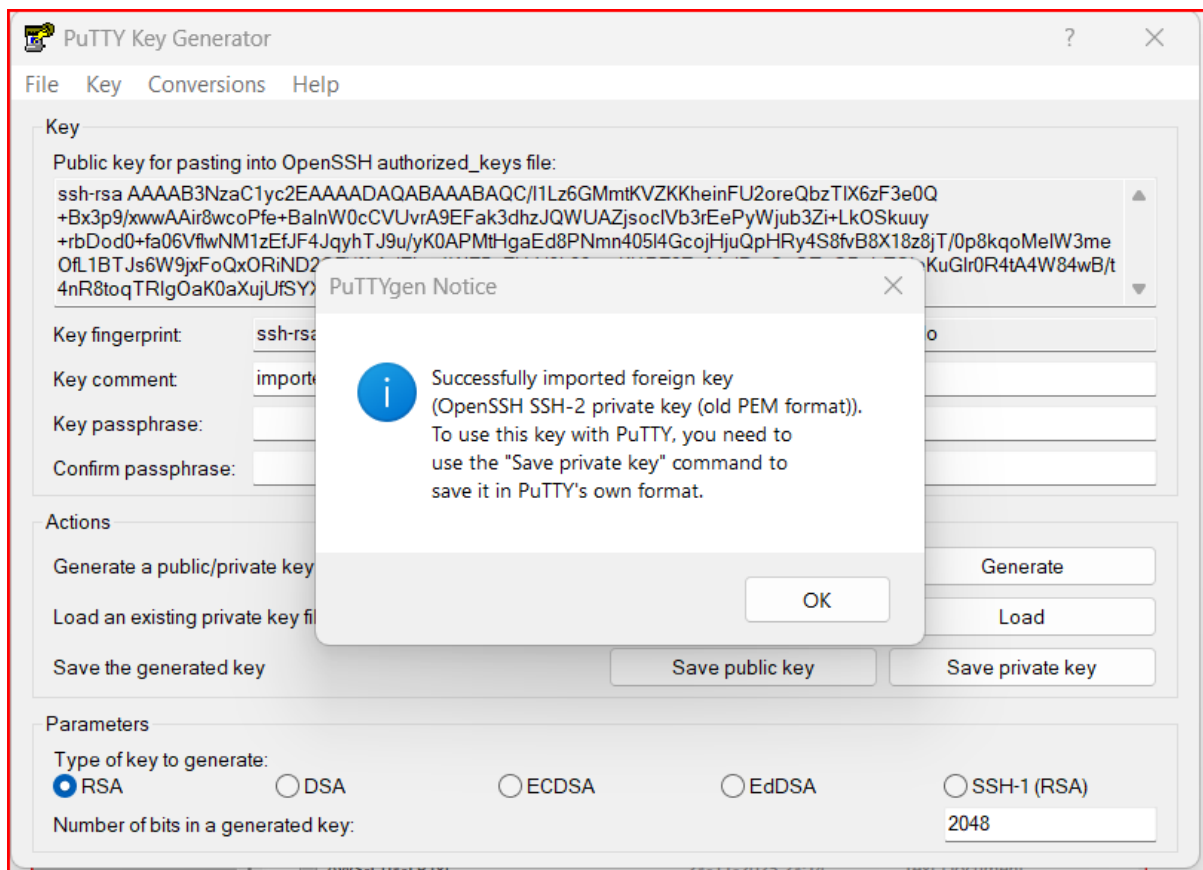


Get Public IP or DNS name to connect it through internet. Also note the Instance Id to connect through CLI.

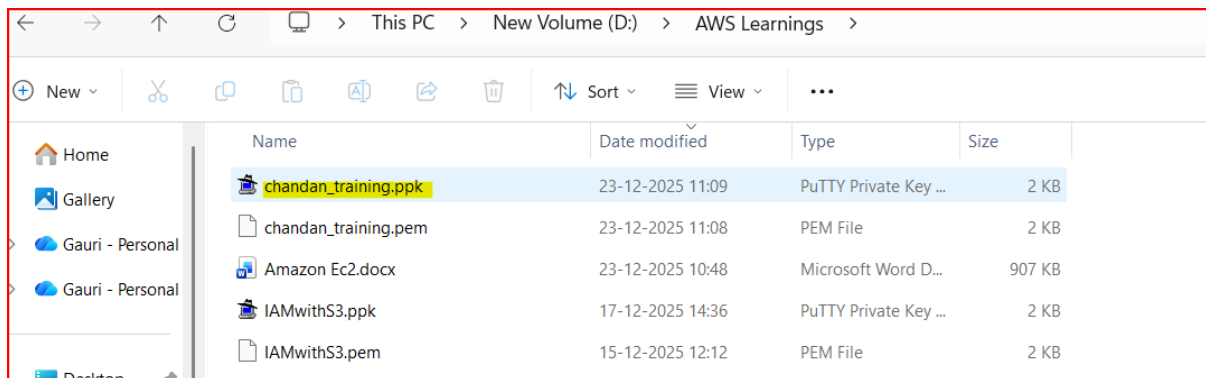
Download PuTTY through <https://www.putty.org> and install it. In your task bar of your local system, search for PuTTYgen and select it. PuTTYgen dialogue box appears, then select Load option. Search for the key pair file which would be in the .pem format and open it.

Click on “Load”, make file type as “All Files”, select the downloaded .pem file to convert it to .ppk file, and click on “Save private key”.



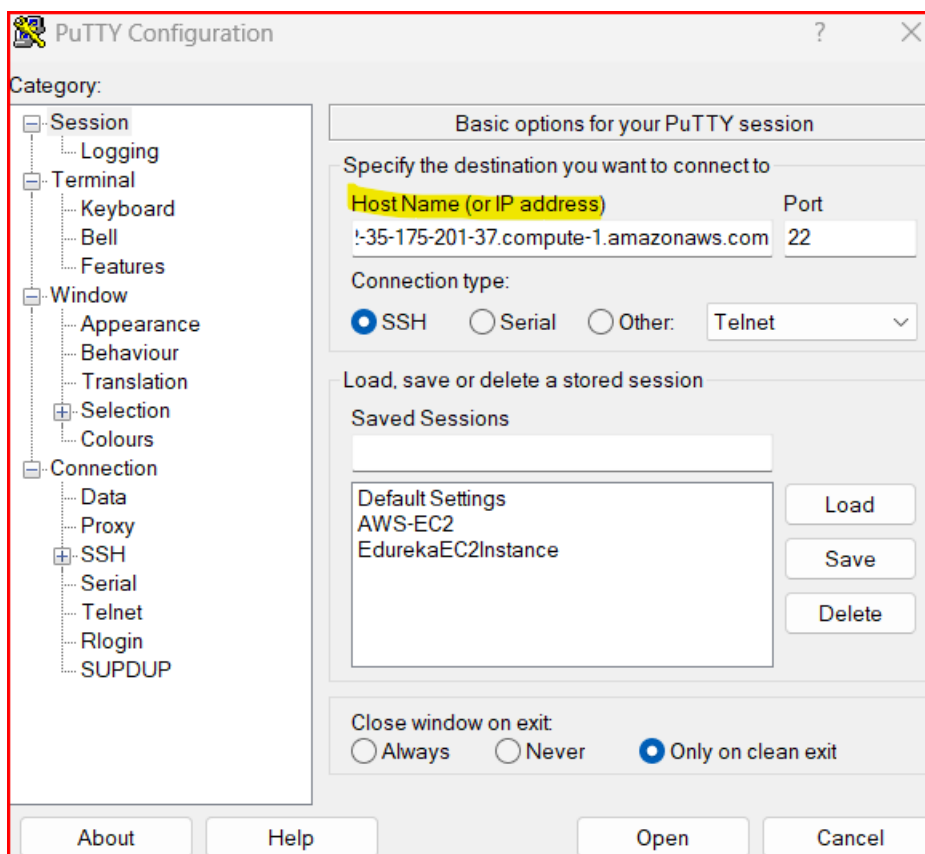


While saving the key change the file extension name from .pem to .ppk and key will be saved in .ppk format

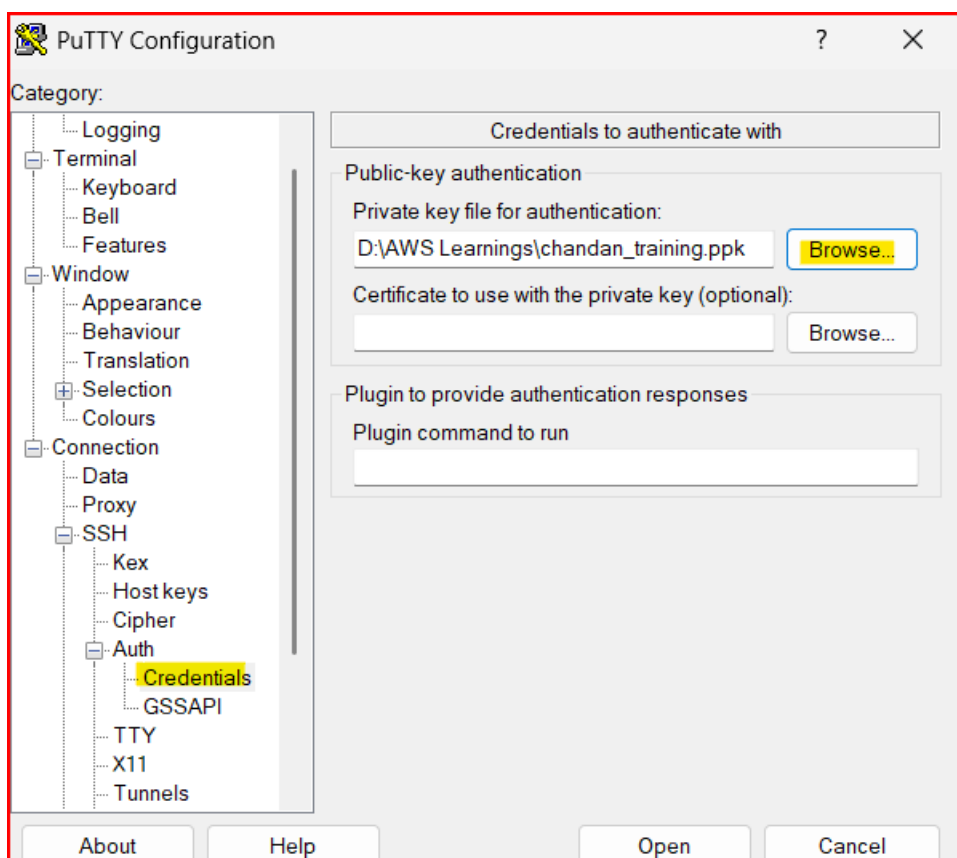
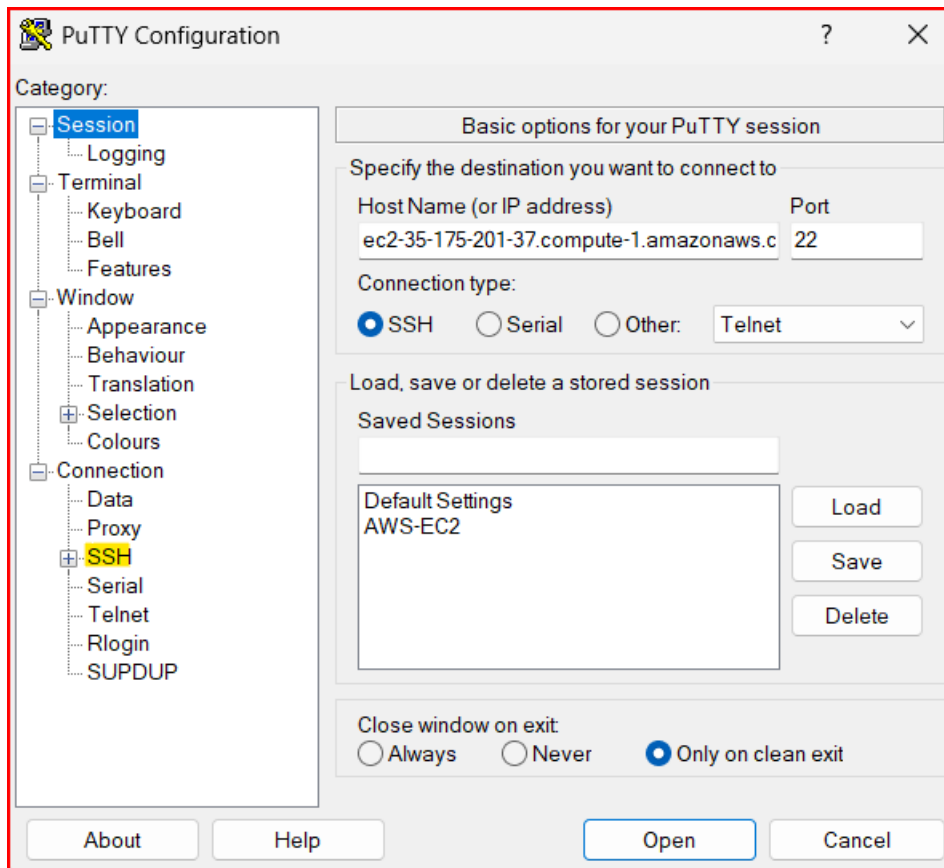


Now we are going to connect the EC2 instance through SSH. For this first copy the DNS name or Public IP.

Open the Putty app and paste the copied Instance DNS/ IP address in Host name.



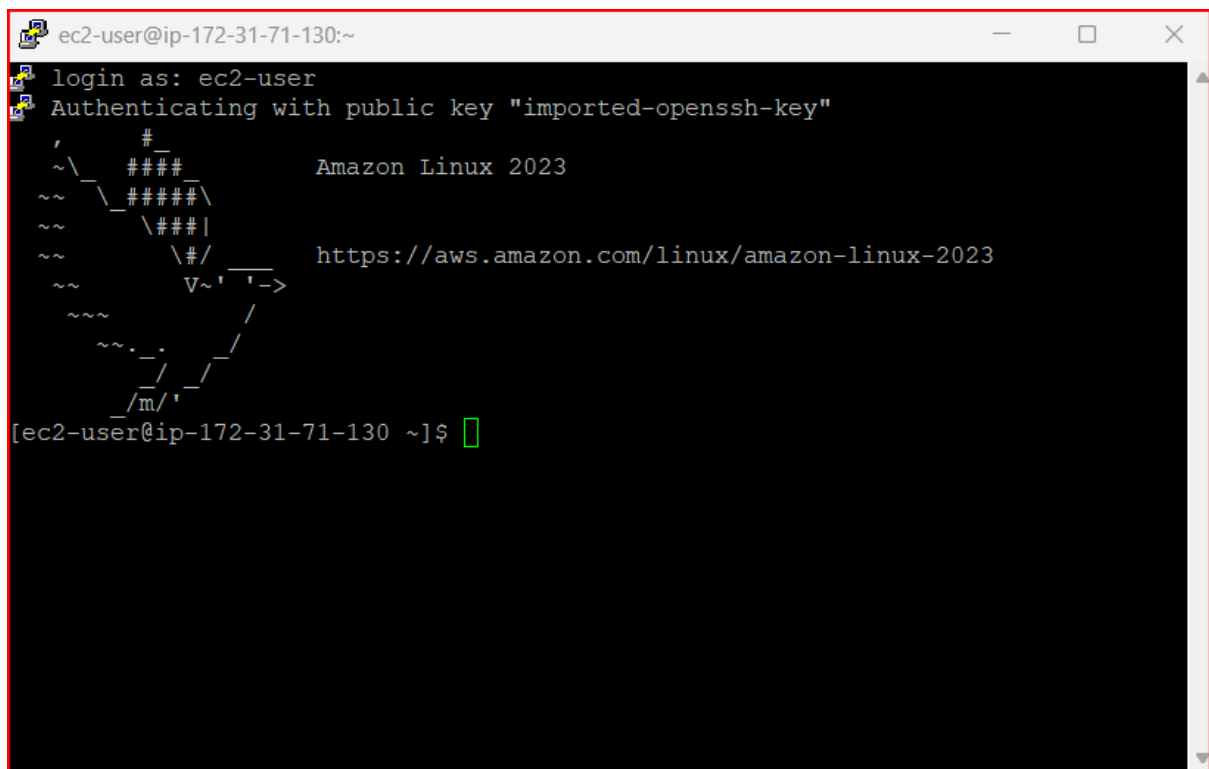
Click on highlighted SSH-> AUTH-> Credential-> Browse private key-> Click to Open



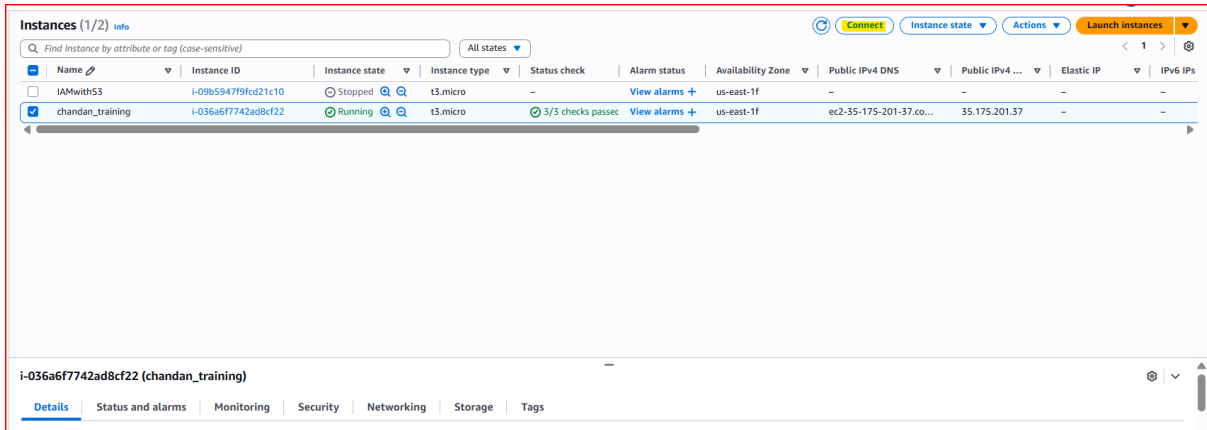
Below terminal will open



To login and start working with your instance type the User Name of instance. For Amazon Linux user will be ec2-user and for ubuntu user name will be ubuntu

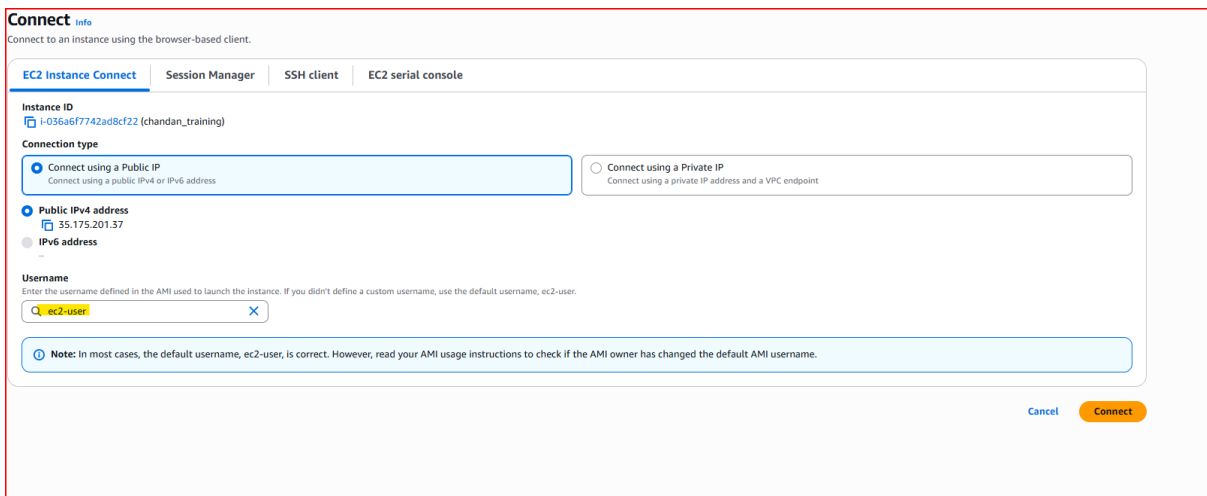


To get your user name you can click on connect



The screenshot shows the AWS Management Console 'Instances' page. At the top, there are buttons for 'Connect', 'Instance state', 'Actions', and 'Launch instances'. Below these is a search bar and a table of instances. The table has columns for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, Public IPv4 DNS, Public IPv4 ..., Elastic IP, and IPv6 IPs. The instance 'chandan_training' with ID 'i-036a6f7742ad8cf22' is in the 'Running' state. Below the table, there is a section for 'i-036a6f7742ad8cf22 (chandan_training)' with tabs for Details, Status and alarms, Monitoring, Security, Networking, Storage, and Tags.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs
IAMwithS3	i-09b5947f9fd21c10	Stopped	t3.micro	3/3 checks passed	View alarms +	us-east-1f	-	-	-	-
chandan_training	i-036a6f7742ad8cf22	Running	t3.micro	3/3 checks passed	View alarms +	us-east-1f	ec2-35-175-201-37.co...	35.175.201.37	-	-



The screenshot shows the 'Connect' page in the AWS Management Console. It has tabs for 'EC2 Instance Connect', 'Session Manager', 'SSH client', and 'EC2 serial console'. The 'EC2 Instance Connect' tab is selected. It shows the 'Instance ID' as 'i-036a6f7742ad8cf22 (chandan_training)'. Under 'Connection type', there are two options: 'Connect using a Public IP' (selected) and 'Connect using a Private IP'. The 'Public IP v4 address' is '35.175.201.37'. Under 'Username', the default 'ec2-user' is entered. A note states: 'In most cases, the default username, ec2-user, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.' At the bottom right, there are 'Cancel' and 'Connect' buttons.

We have successfully connected to our Amazon Linux Instance using SSH