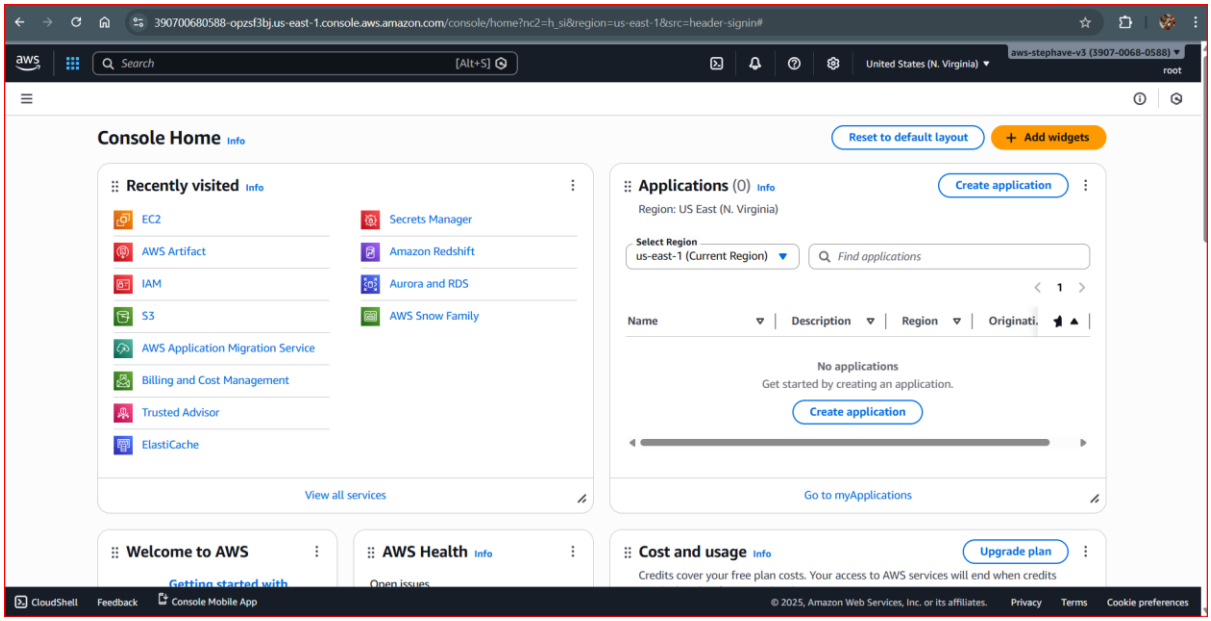
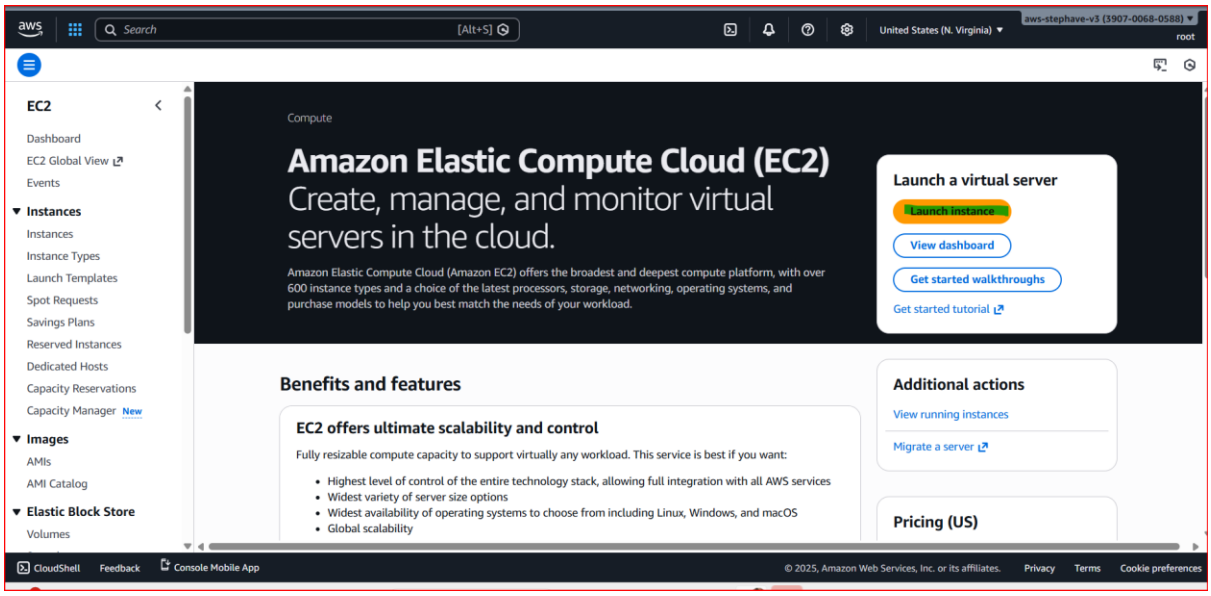
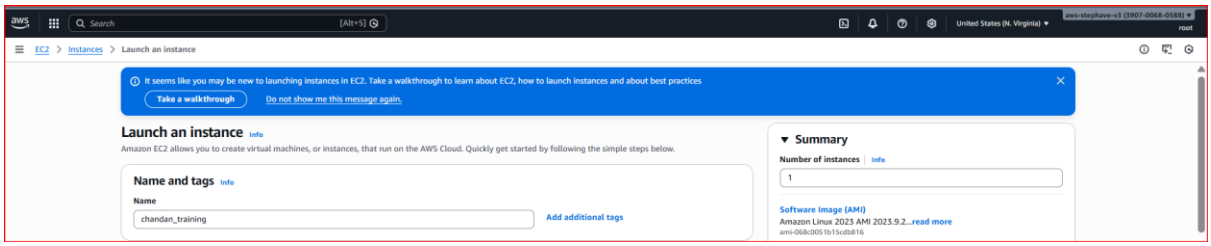
Login to AWS console



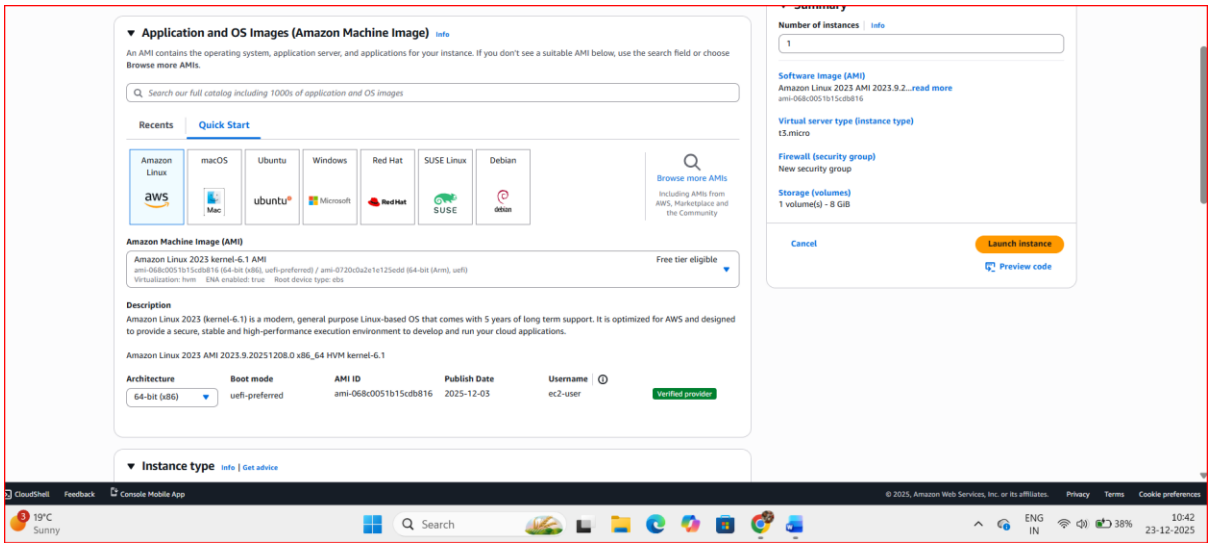
Select EC2 and click on Launch Instance



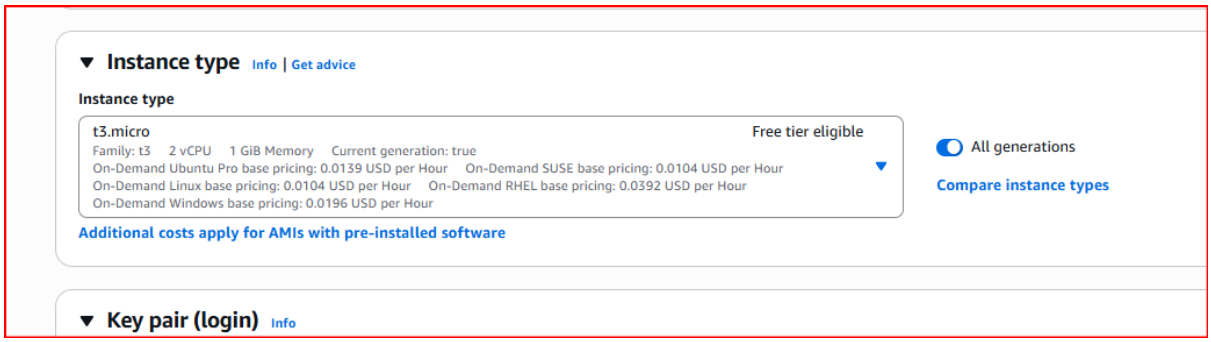
Give the name for your instance. Here we have named it as Chandan_Training



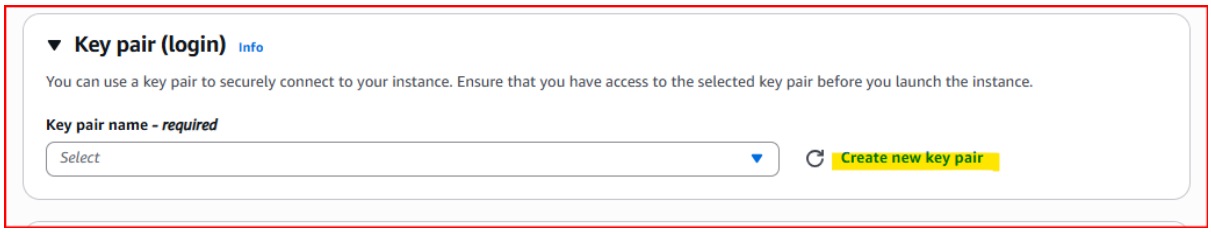
Select an operating system. For e.g select Amazon Linux.



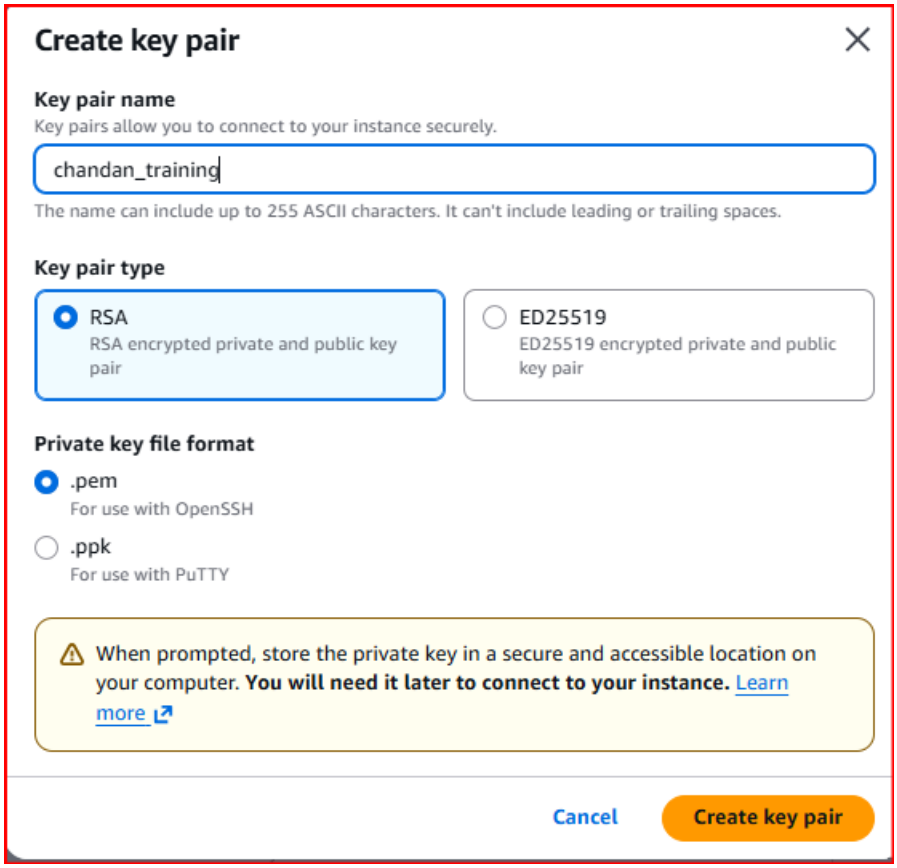
In instance type, Select t3.micro (Free tier eligible)



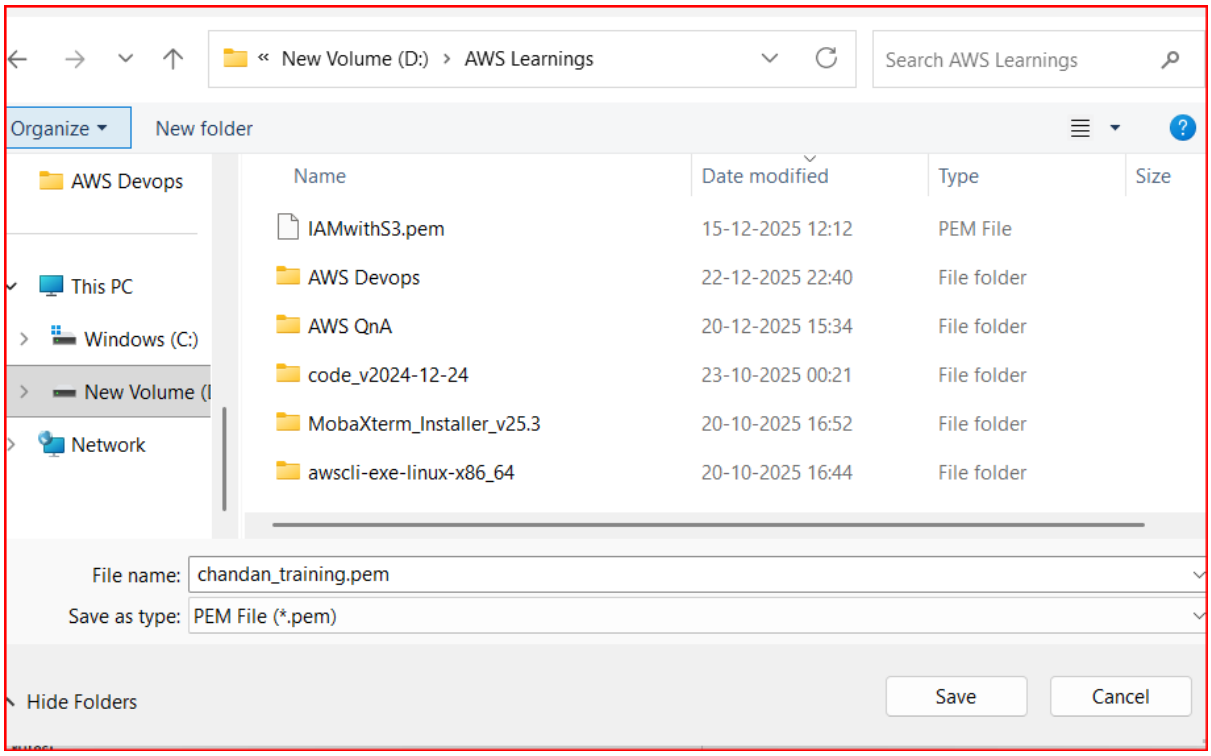
Click on Create Key pair



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

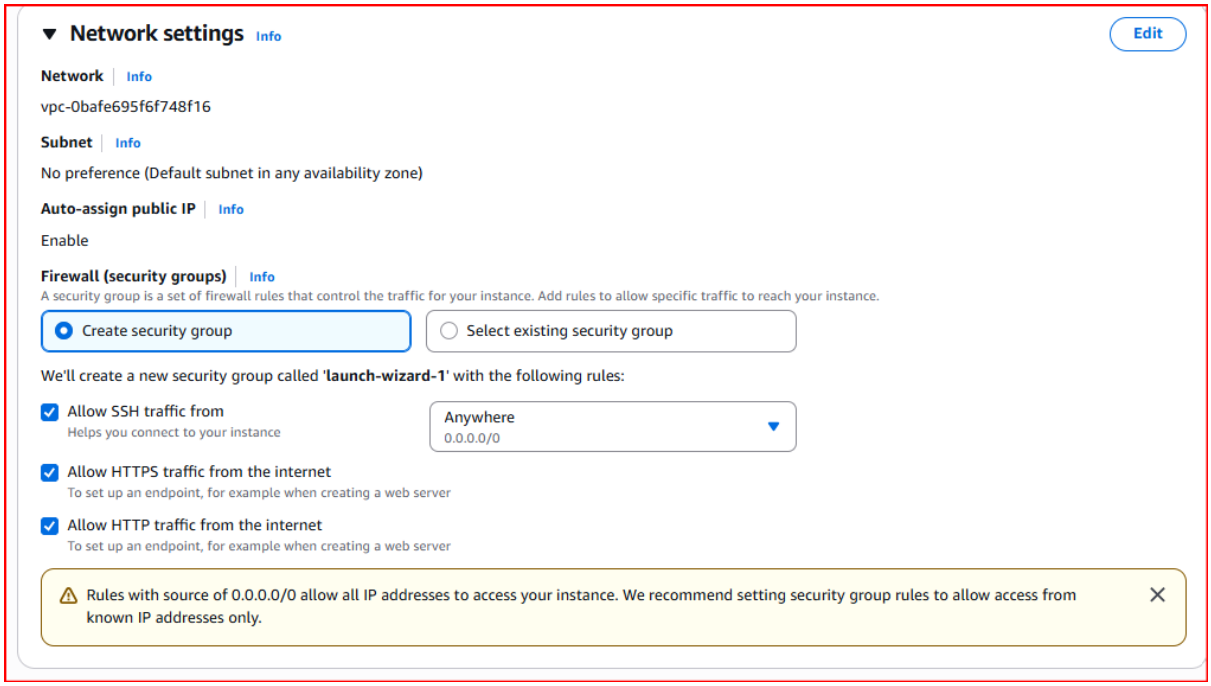


Key get generated and save it on your drive folder. Key pair get saved.



Network Setting

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

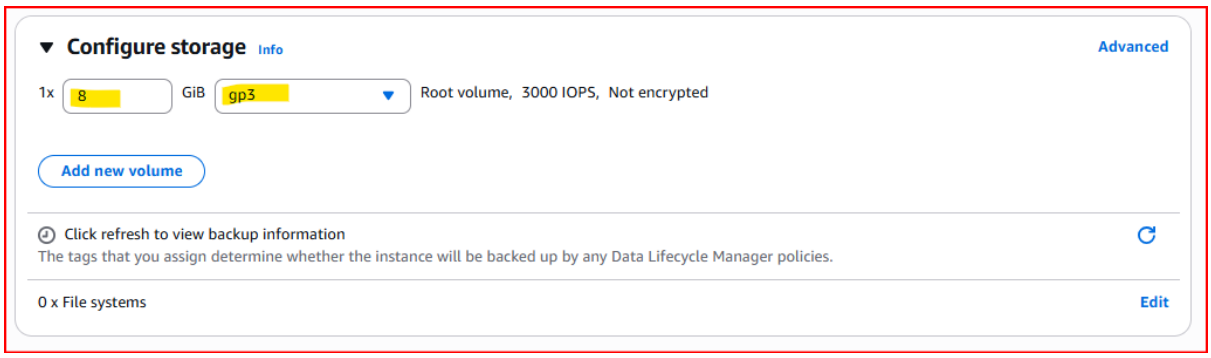


Note:- Security group either you can create new or select existing group if available.

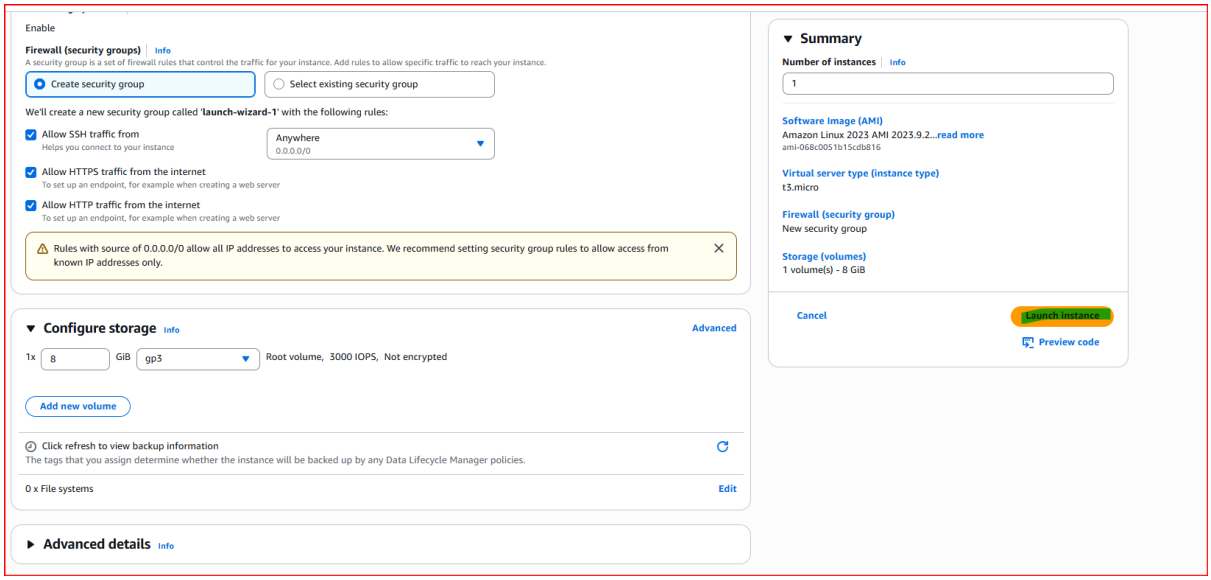
[AWS Security Groups are virtual firewalls for EC2 instances, controlling inbound/outbound traffic via stateful rules (allow by default for responses) based on protocol, port, and source/destination]

Storage Configuration

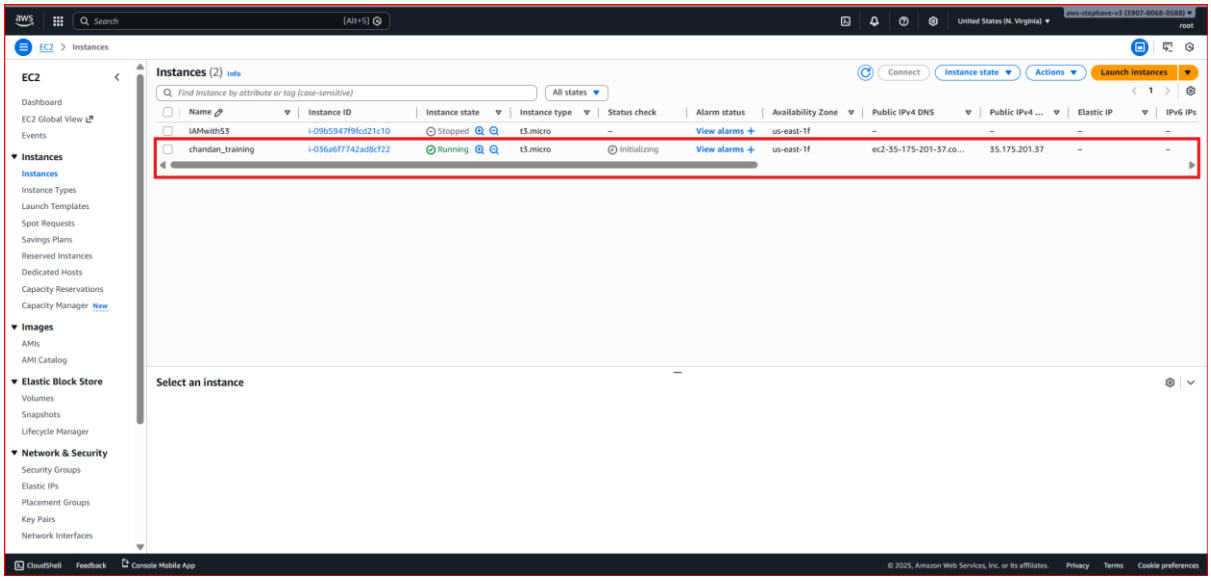
Storage configuration in AWS EC2 involves choosing from several options to meet different requirements for persistence, performance, and scalability. The primary storage types are **Amazon Elastic Block Store (EBS)** and **Instance Store**, which can be complemented by other AWS storage services like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



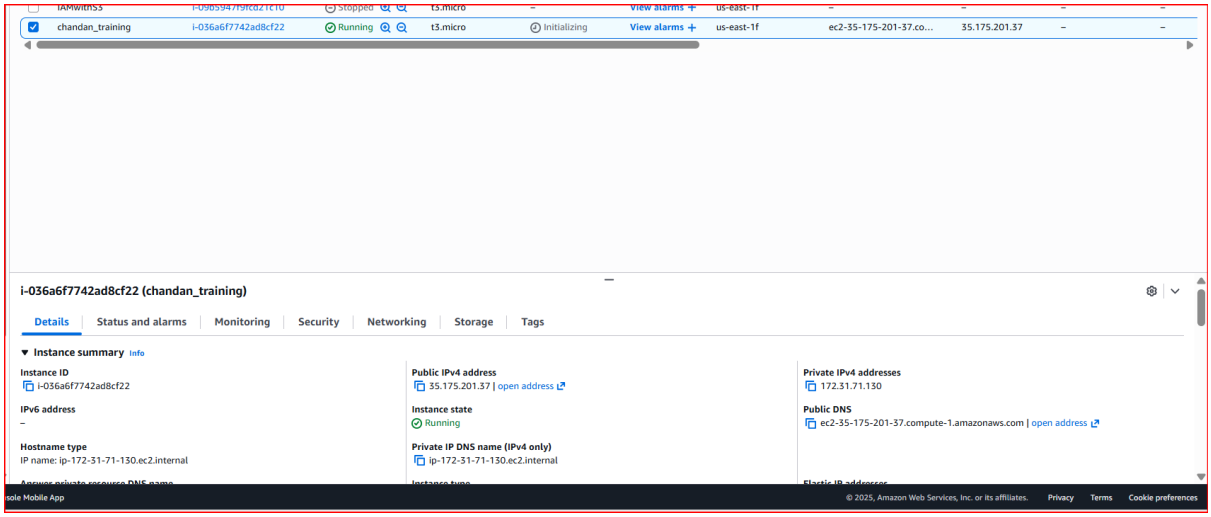
Click on Launch Instance



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



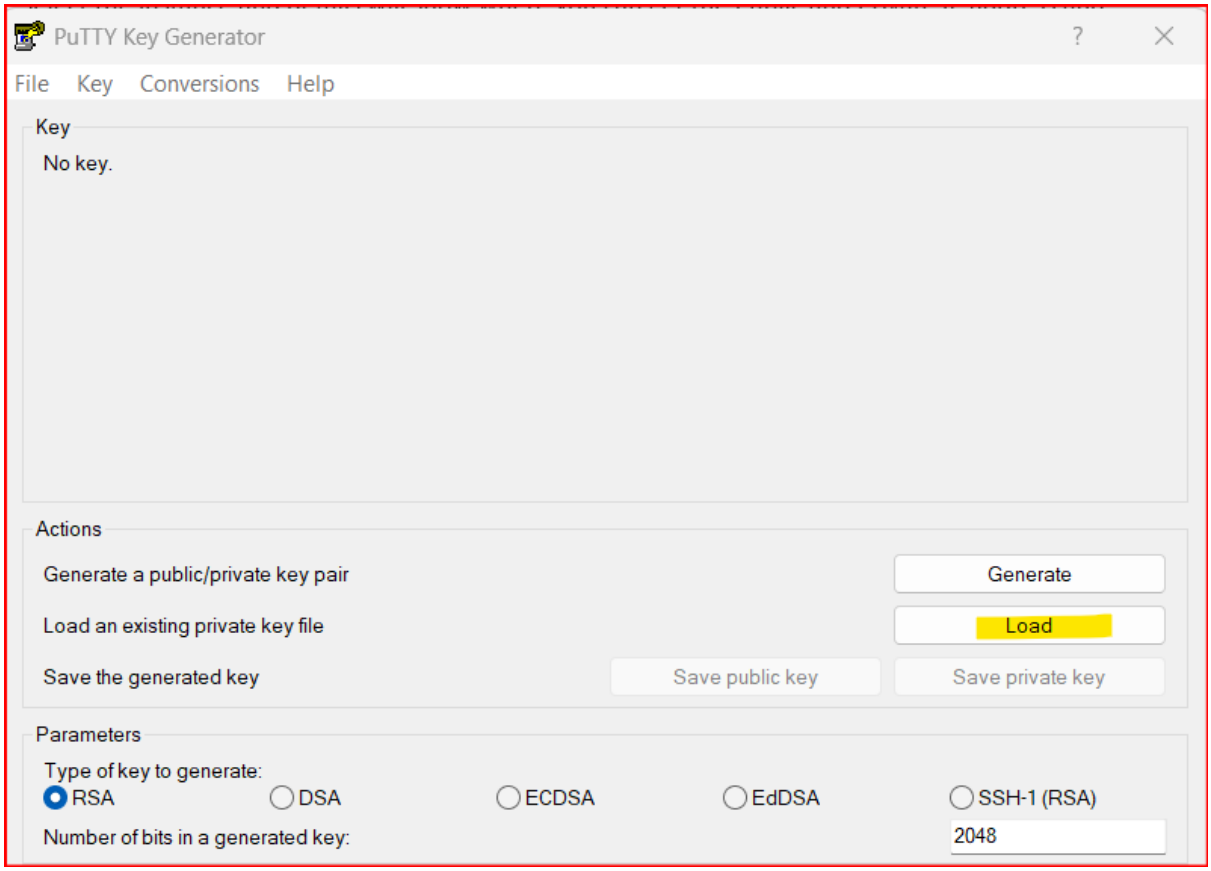
Select the instance and details will show where you can get the Public and Private IP address and other details related to your instance.

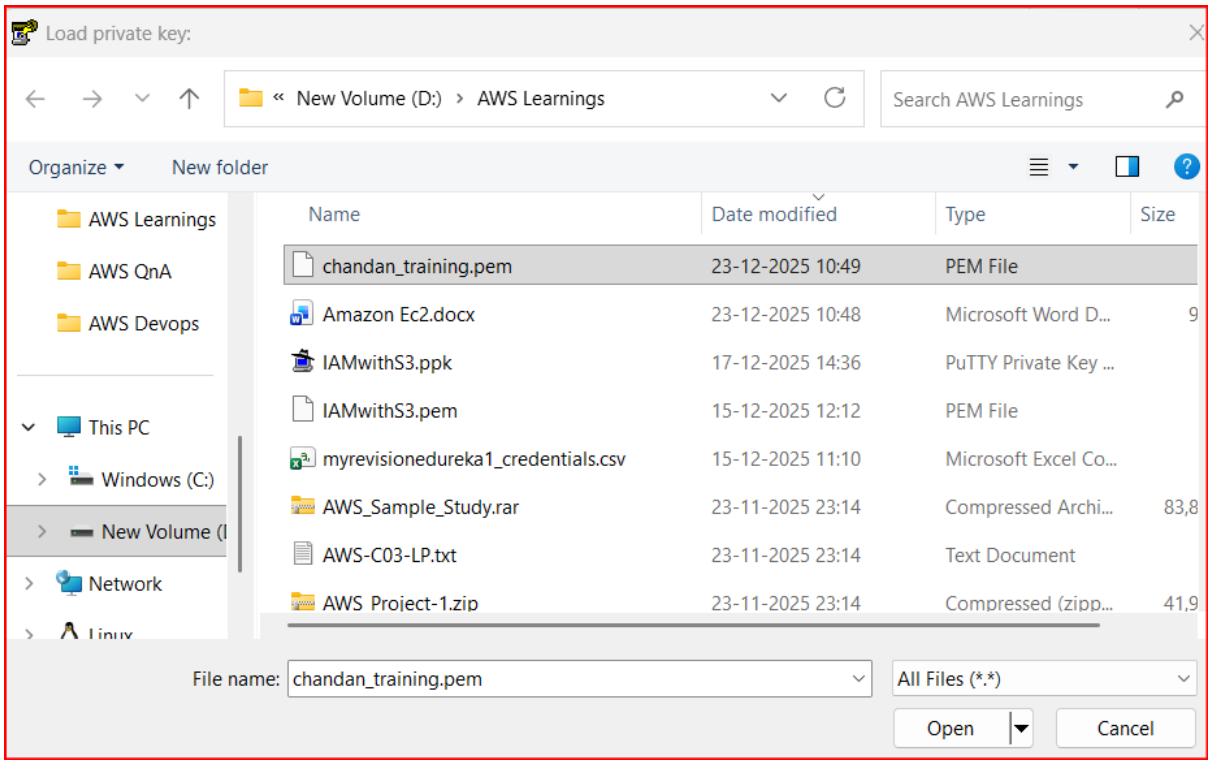


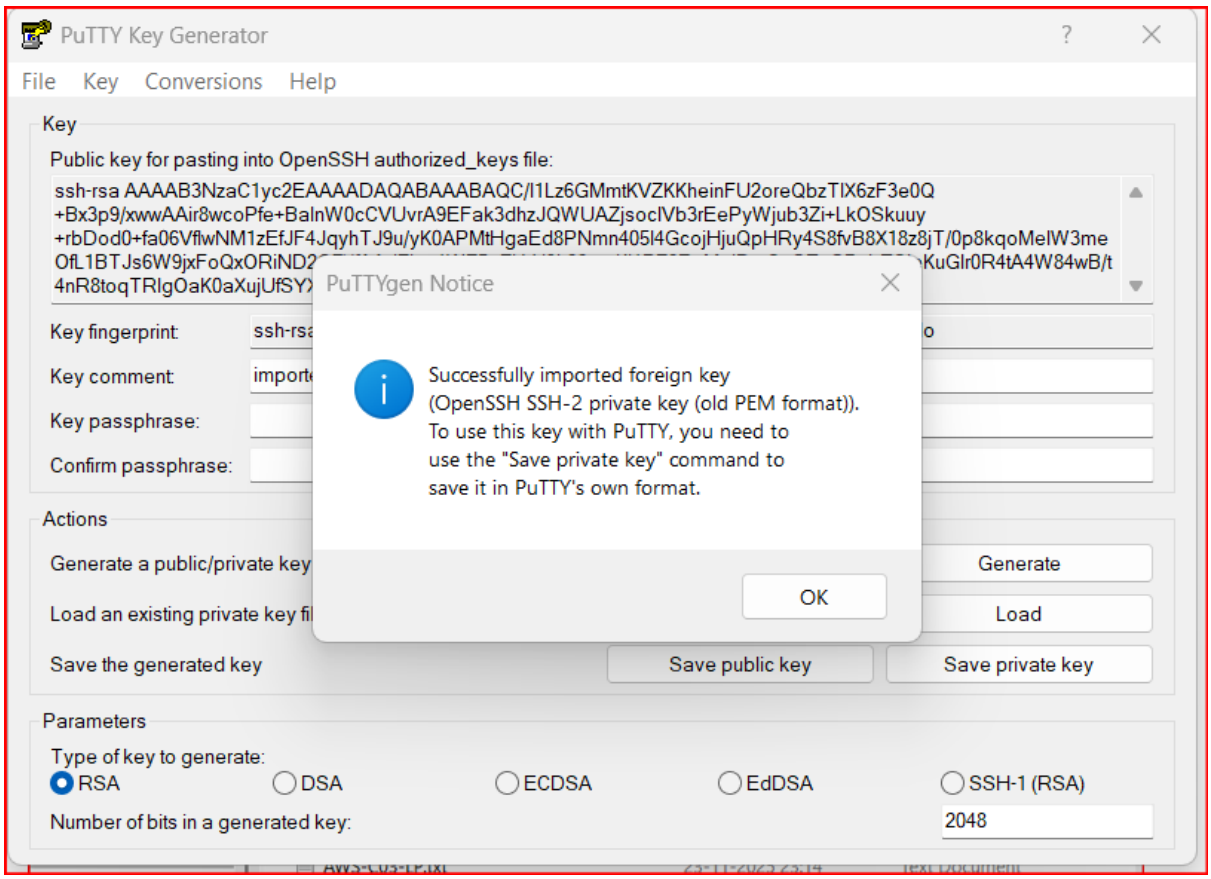
Get Public IP or DNS name to connect it through internet. Also note the Instance Id to connect through CLI.

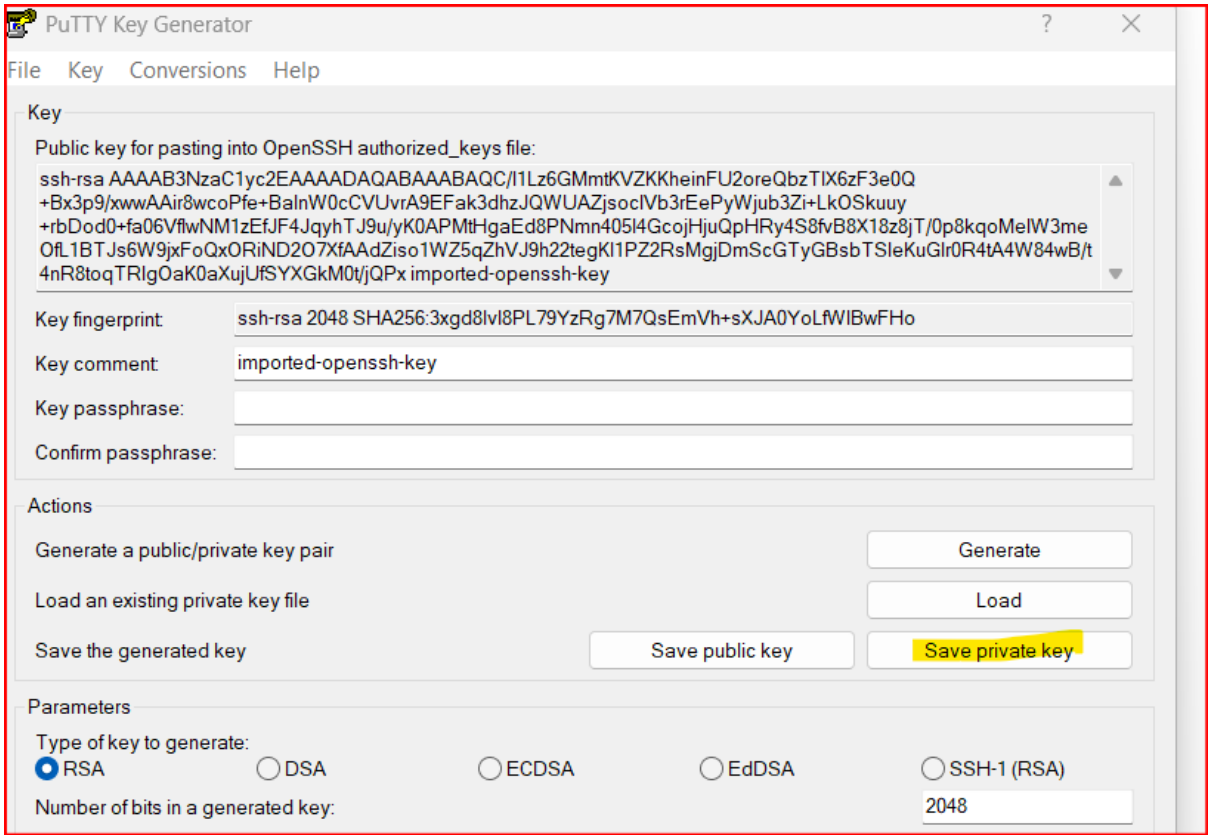
Download PuTTy through https://www.putty.org and install it. In your task bar of your local system, search for PuTTygen and select it. PuTTygen dialogue box appears, then select Load option. Search for the key pair file which would be in the .pem format and open it.

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”.

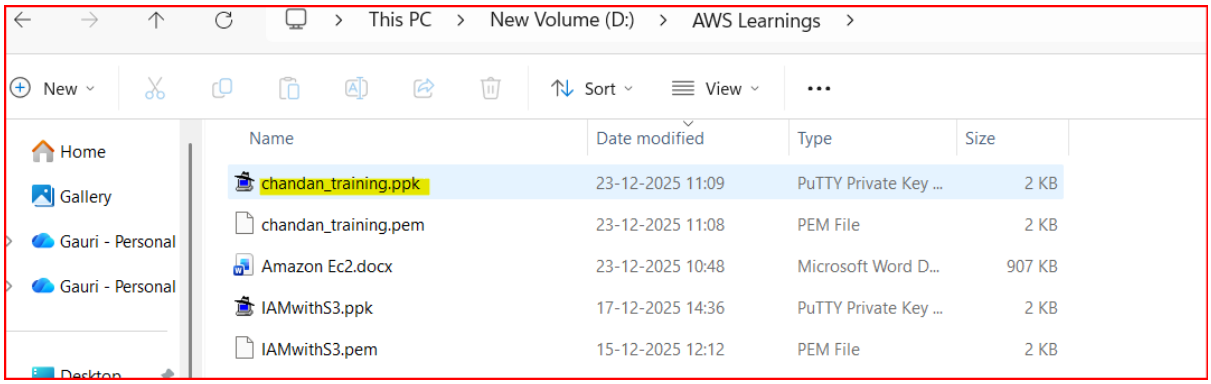





PuTTY Key Generator
File Key Conversions Help
Key
Public key for pasting into OpenSSH authorized_keys file:
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC/l1Lz6GMmtKVZKKheinFU2oreQbzTlX6zF3e0Q
+Bx3p9/xwwAAir8wcoPfe+BalnW0cCVUvrA9EFak3dhzJQWUAZjsoclVb3rEePyWjub3Zi+LkOSkuuy
+rbDod0+fa06VflwNM1zEfJF4JqyhTJ9u/yK0APMtHgaEd8PNmn405l4GcojHjuQpHRy4S8fvB8X18z8jT/0p8kqoMelW3me
OfL1BTJs6W9jxFoQxORiND2
KuGlr0R4tA4W84wB/t
4nR8toqTRIgOaK0aXujUfSY
Key fingerprint:
Key comment:
Key passphrase:
Confirm passphrase:
Actions
Generate a public/private key
Load an existing private key fi
Save the generated key
Generate
Load
Save public key
Save private key
Parameters
Type of key to generate:
RSA DSA ECDSA EdDSA SSH-1 (RSA)
Number of bits in a generated key:
2048
PuTTYgen Notice
Successfully imported foreign key
(OpenSSH SSH-2 private key (old PEM format)).
To use this key with PuTTY, you need to
use the "Save private key" command to
save it in PuTTY's own format.
OK

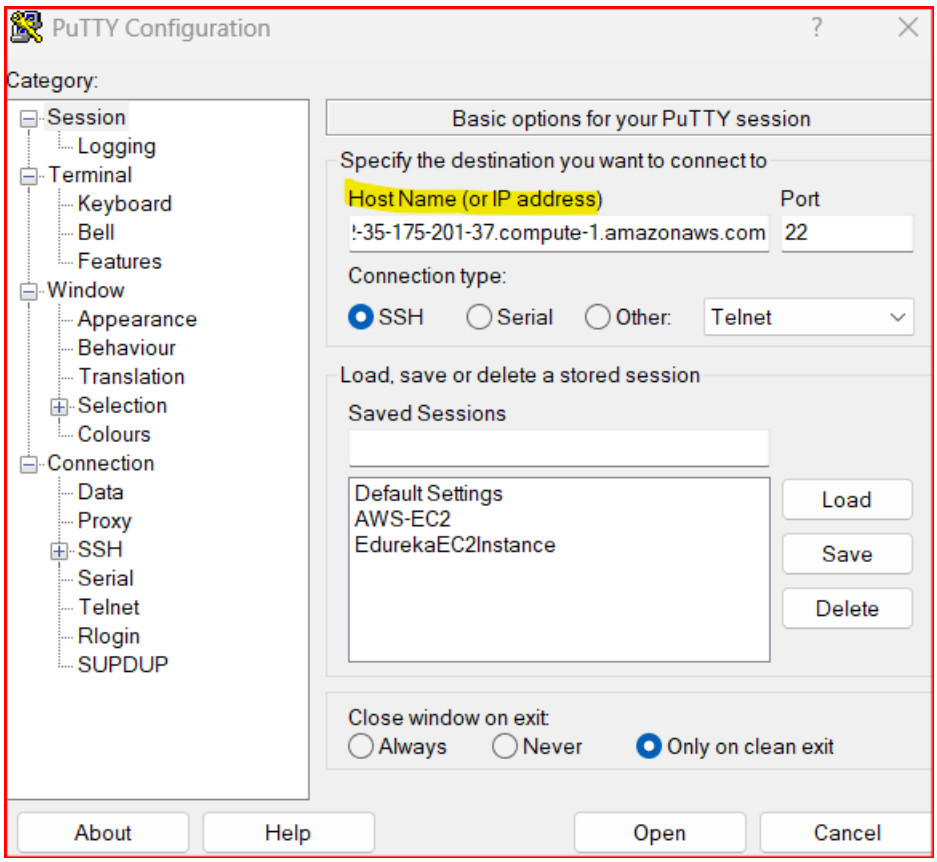

PuTTY Key Generator
File Key Conversions Help
Key
Public key for pasting into OpenSSH authorized_keys file:
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC/l1Lz6GMmtKVZKKheinFU2oreQbzTlX6zF3e0Q
+Bx3p9/xwwAAir8wcoPfe+BalnW0cCVUvrA9EFak3dhzJQWUAZjsoclVb3rEePyWjub3Zi+LkOSkuuy
+rbDod0+fa06VflwNM1zEfJF4JqyhTJ9u/yK0APMtHgaEd8PNmn405l4GcojHjuQpHRy4S8fvB8X18z8jT/0p8kqoMelW3me
OfL1BTJs6W9jxFoQxORiND2O7XfAAdZiso1WZ5qZhVJ9h22tegKl1PZ2RsMgjDmScGTyGBsbTSleKuGlr0R4tA4W84wB/t
4nR8toqTRIgOaK0aXujUfSYXGkM0t/jQPx imported-openssh-key
Key fingerprint:
ssh-rsa 2048 SHA256:3xgd8lvl8PL79YzRg7M7QsEmVh+sXJA0YoLfWIBwFHo
Key comment:
imported-openssh-key
Key passphrase:
Confirm passphrase:
Actions
Generate a public/private key pair
Load an existing private key file
Save the generated key
Generate
Load
Save public key
Save private key
Parameters
Type of key to generate:
RSA DSA ECDSA EdDSA SSH-1 (RSA)
Number of bits in a generated key:
2048

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

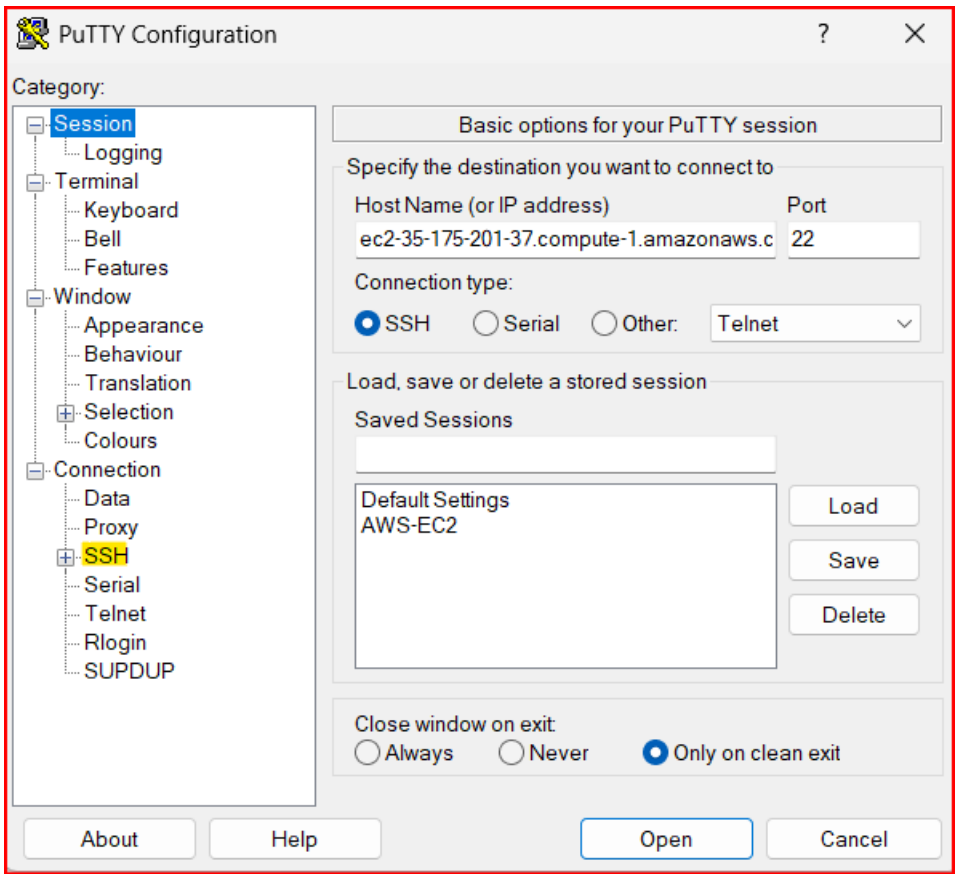


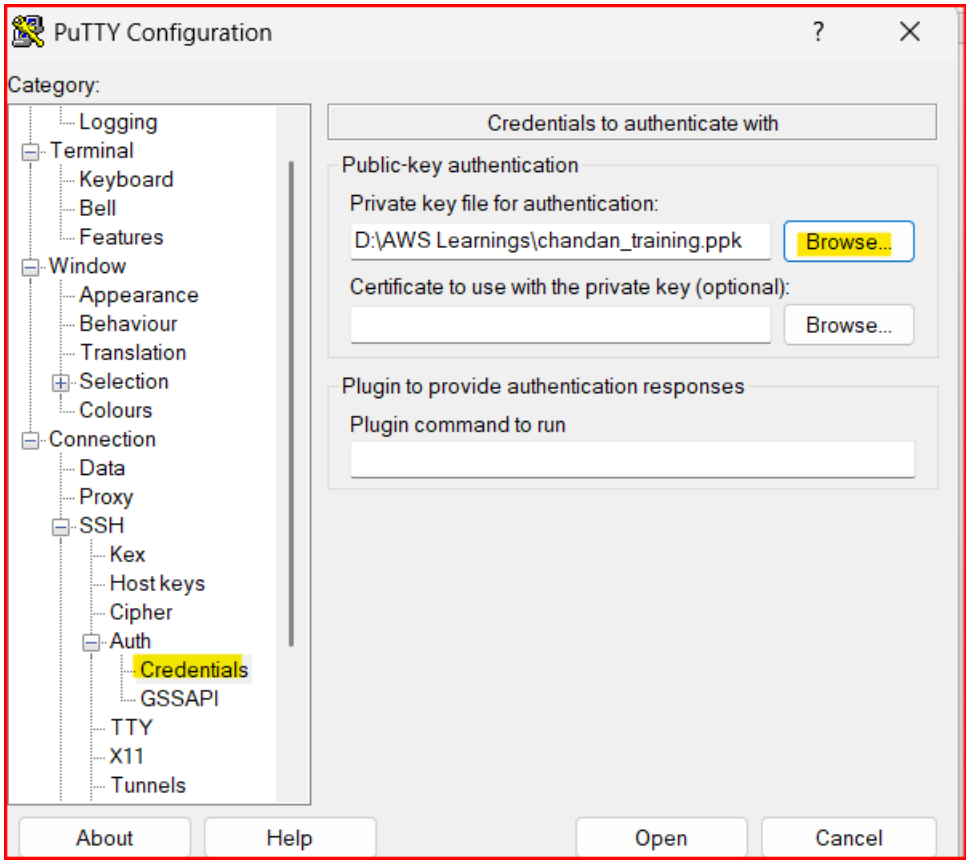
Now we are going to connect the EC2 instance through SSH. For this first copy the DNS name or Public IP.

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



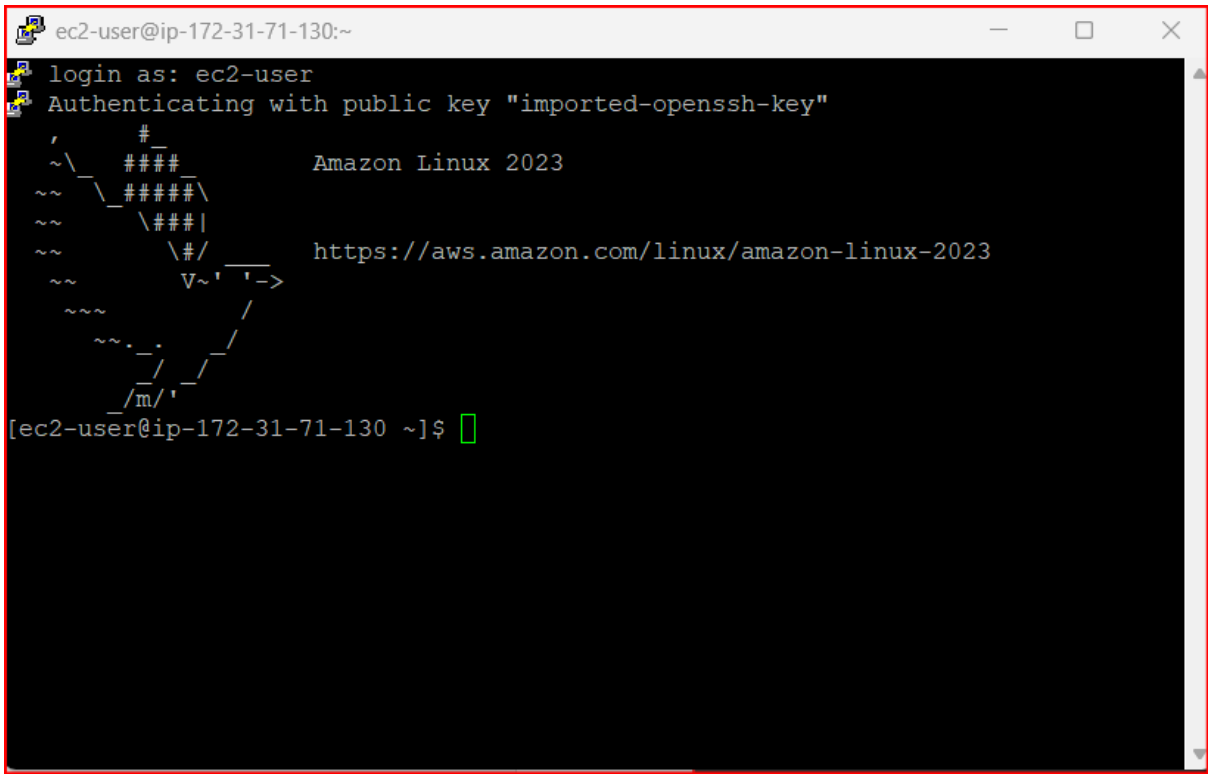
Click on highlighted SSH-> AUTH-> Credential-> Browse private key-> Click to Open


PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
SSH
Serial
Telnet
Rlogin
SUPDUP
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
ec2-35-175-201-37.compute-1.amazonaws.c
22
Connection type:
SSH
Serial
Other:
Telnet
Load, save or delete a stored session
Saved Sessions
Default Settings
AWS-EC2
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Help
Open
Cancel

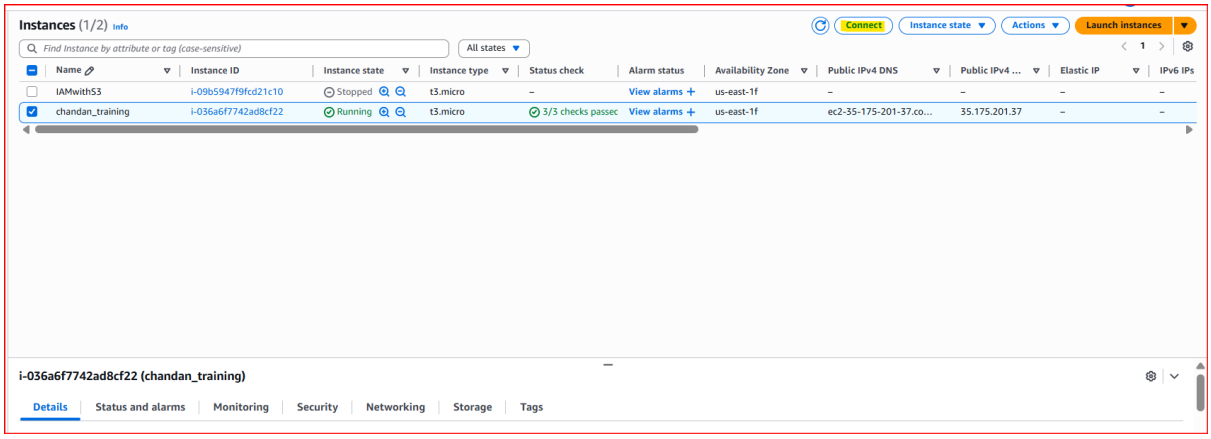

PuTTY Configuration
Category:
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
SSH
Kex
Host keys
Cipher
Auth
Credentials
GSSAPI
TTY
X11
Tunnels
Credentials to authenticate with
Public-key authentication
Private key file for authentication:
D:\AWS Learnings\chandan_training.ppk
Browse...
Certificate to use with the private key (optional):
Browse...
Plugin to provide authentication responses
Plugin command to run
About
Help
Open
Cancel

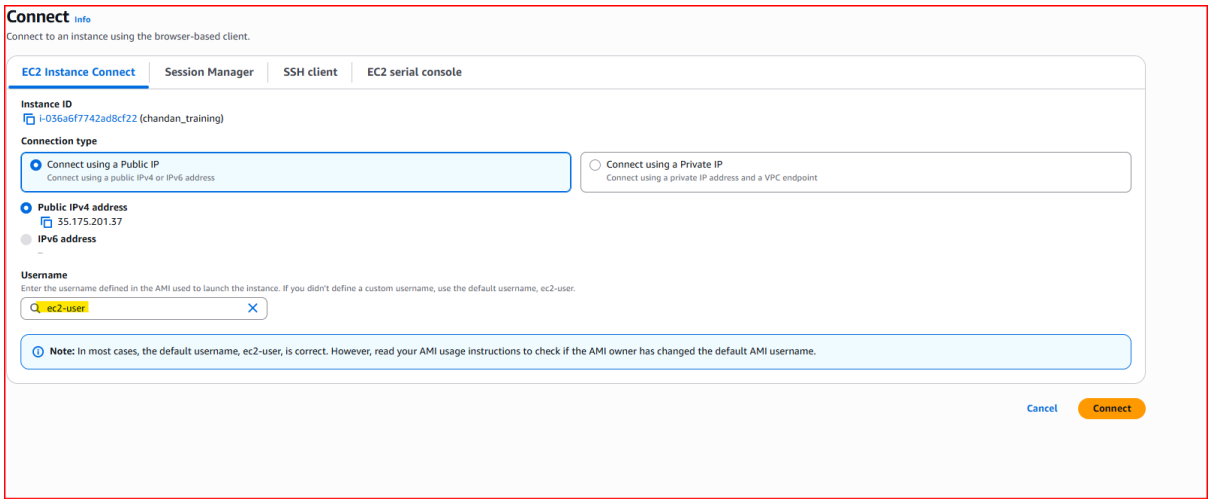
Below termial will open

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





We have successfully connected to our Amazon Linux Instance using SSH