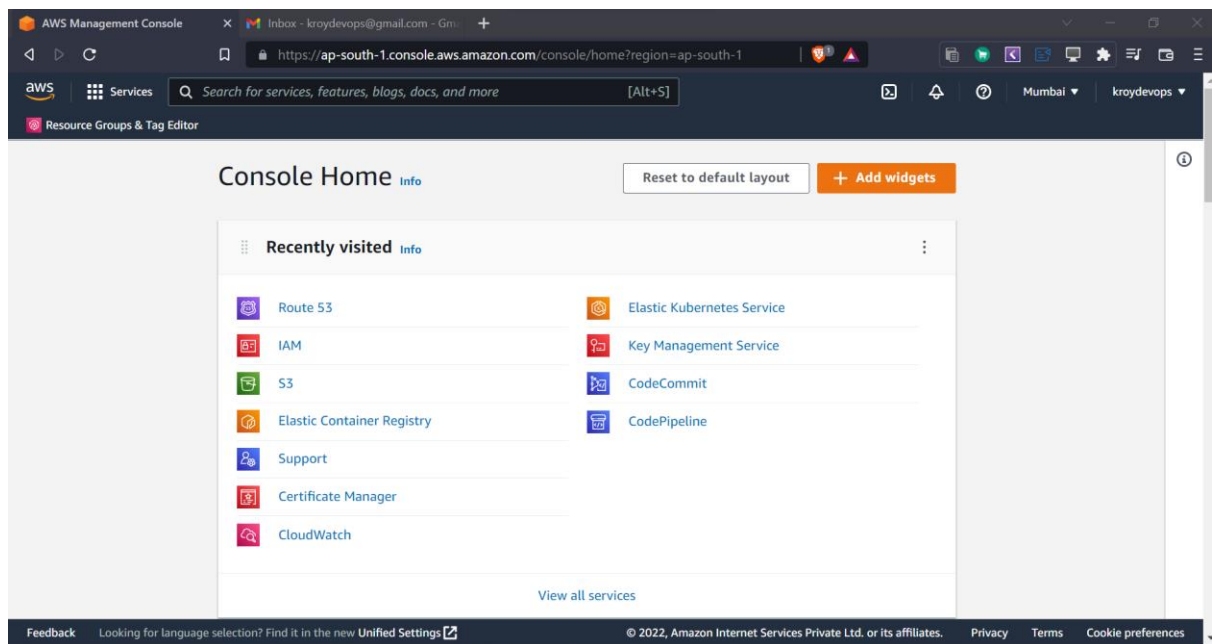


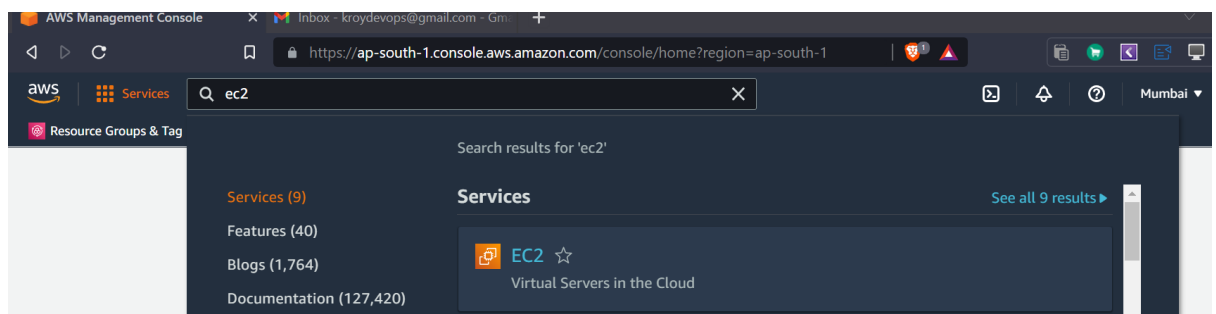
Learn how to launch an EC2 instance (linux) on aws account.

Steps:-

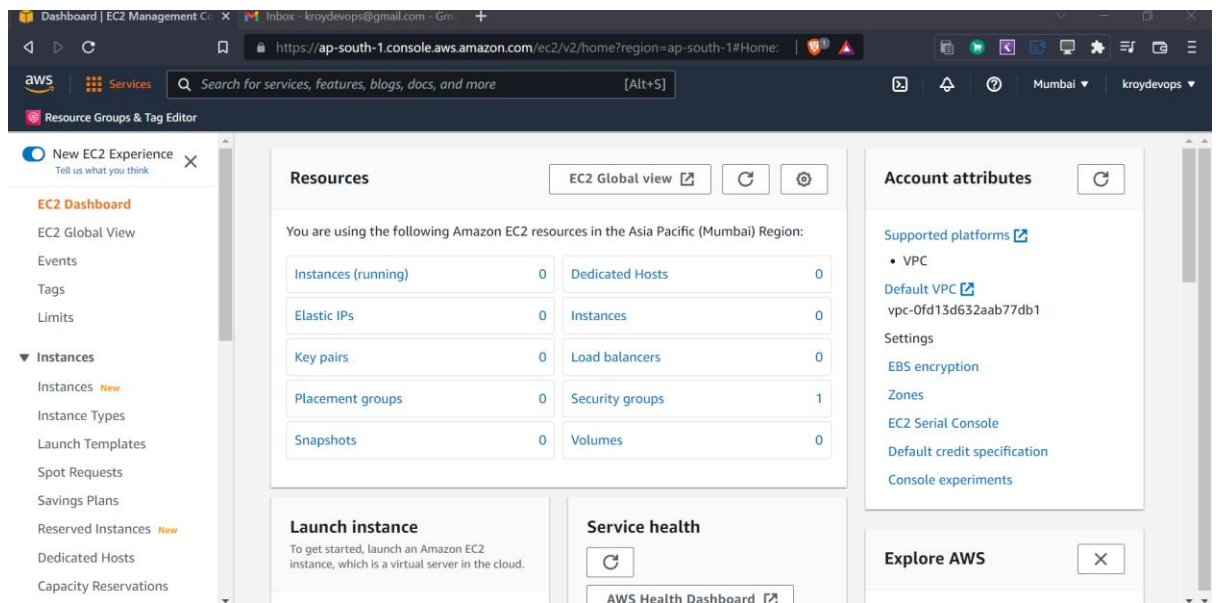
1. Sign in to aws console.



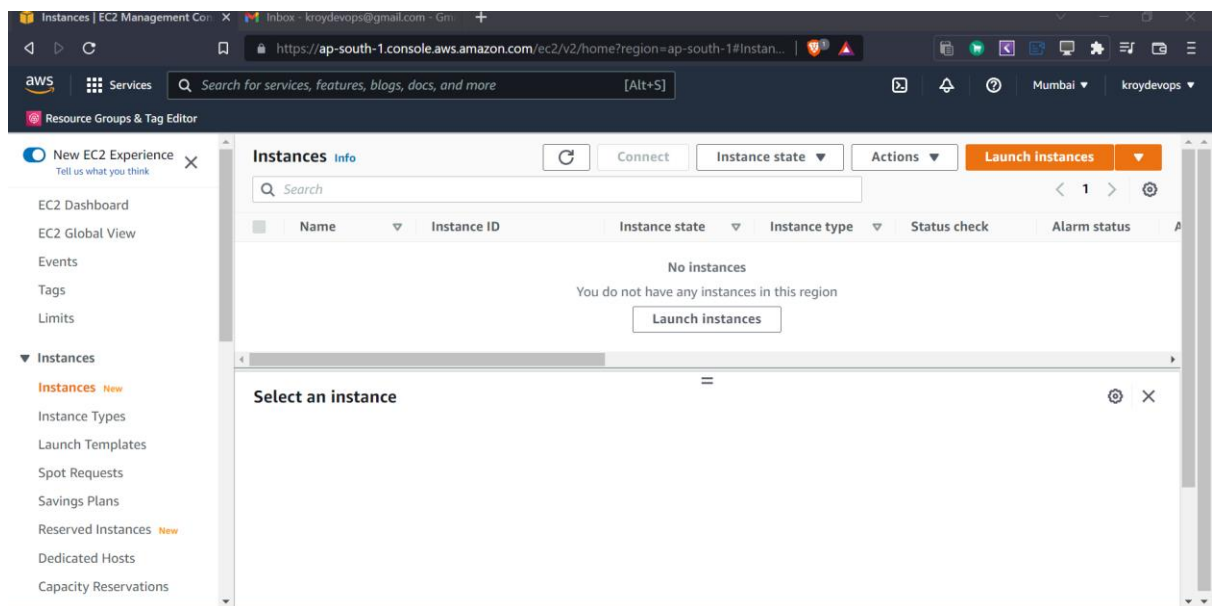
2. Search EC2 and then click enter.



3. After clicking on ec2 you will land to this page.



4. Click on “instances new” on the left hand side .



5. Click on launch instances and then enter name and number of instances

The screenshot shows the 'Launch an instance' page in the AWS Management Console. The breadcrumb navigation is 'EC2 > Instances > Launch an instance'. The main heading is 'Launch an instance' with an 'Info' link. Below it, a sub-header 'Name and tags' has an 'Info' link. A text input field contains 'Linux-ec2', and there is a link 'Add additional tags'. Below this, a section 'Application and OS Images (Amazon Machine Image)' has an 'Info' link and a description of AMIs. On the right, a 'Summary' panel shows 'Number of instances' set to 1, 'Software Image (AMI)' as 'Amazon Linux 2 Kernel 5.10 AMI...', 'Virtual server type (instance type)' as 't2.micro', 'Firewall (security group)' as 'New security group', and 'Storage (volumes)' as '1 volume(s) - 8 GiB'.

6. Now choose amazon linux AMI, you can choose any images which you want to use but some of the images don't come in free tier.

The screenshot shows the 'Quick Start' section for 'My AMIs'. It features a row of AMI categories: Amazon Linux, macOS, Ubuntu, Windows, and Red Hat. The 'Amazon Linux' category is selected. Below this, the 'Amazon Machine Image (AMI)' section displays 'Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type' with AMI IDs and a 'Free tier eligible' label. The 'Description' section shows 'Amazon Linux 2 Kernel 5.10 AMI 2.0.20221103.3 x86_64 HVM gp2'. The 'Architecture' dropdown is set to '64-bit (x86)', and the 'AMI ID' is 'ami-0b0dcb5067f052a63'. A 'Verified provider' badge is visible.

7. Choose the instance type, here we are choosing t2.micro because it comes under the free tier

The screenshot shows the 'Instance type' selection section. The 'Instance type' dropdown is set to 't2.micro', which is highlighted with a red underline. To the right, a 'Free tier eligible' label is also underlined in red. Below the dropdown, details for the 't2.micro' instance type are listed: 'Family: t2', '1 vCPU', '1 GiB Memory', 'On-Demand Linux pricing: 0.0116 USD per Hour', and 'On-Demand Windows pricing: 0.0162 USD per Hour'. A 'Compare instance types' link is visible on the right.


8. Now create a key pair for you machine , it's like a password setup for your newly launched instance.

▼ **Key pair (login)** [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.


Key pair name - *required*

Select ▼

 [Create new key pair](#)

Create key pair ×

Key pairs allow you to connect to your instance securely.

Enter the name of the key pair below. 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](#) 

Key pair name

linuxnovkey

The name can include upto 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 (Not supported for Windows instances)

Private key file format

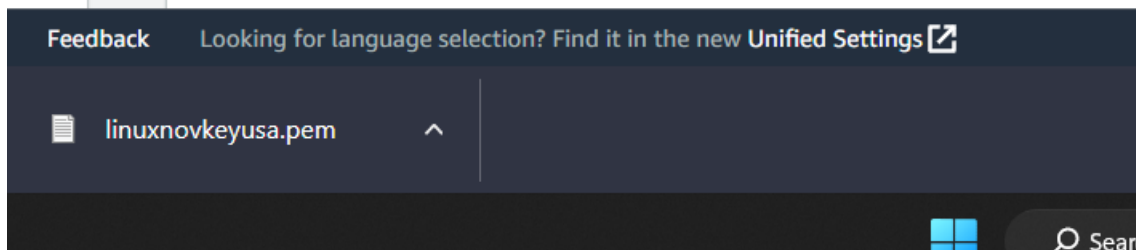
☒ **.pem**
For use with OpenSSH

☐ **.ppk**
For use with PuTTY

Cancel

Create key pair

No preference (Default subnet in any availability zone)



9. Check network settings

▼ Network settings [Info](#)

Edit

Network [Info](#)

vpc-0f052792f7d9078a1

Subnet [Info](#)

No preference (Default subnet in any availability zone)

Auto-assign public IP [Info](#)

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-19' 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

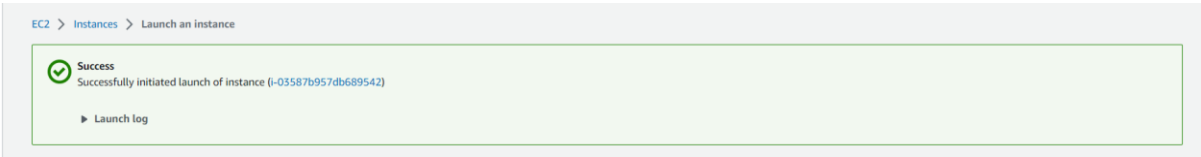
☐ Allow HTTP traffic from the internet

To set up an endpoint, for example when creating a web server

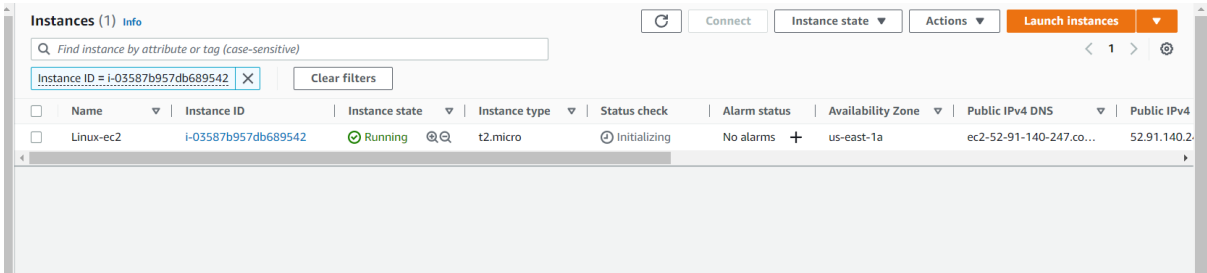
 Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

×

10. Now click on Launch.



11. Now click on instance ID



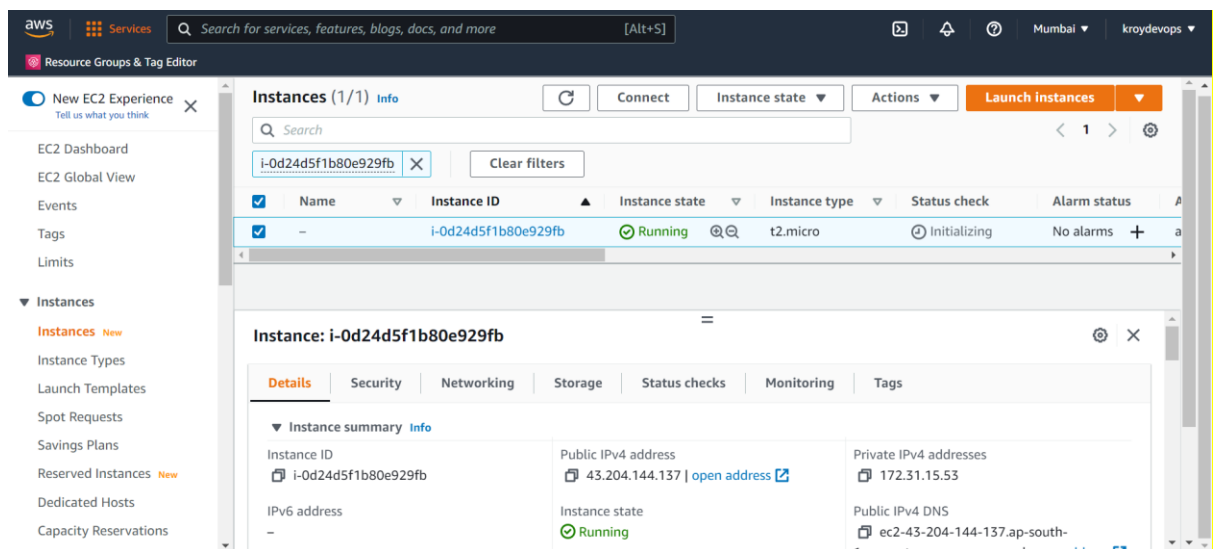
Now our Instance is up and running.

There are many ways to connect to our new launched ec2-instance.

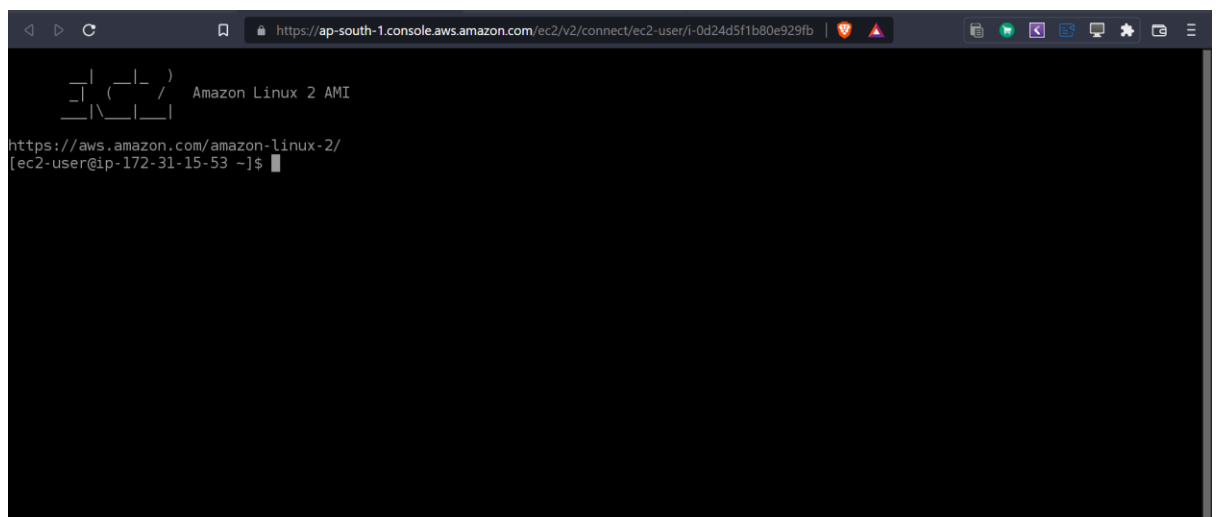
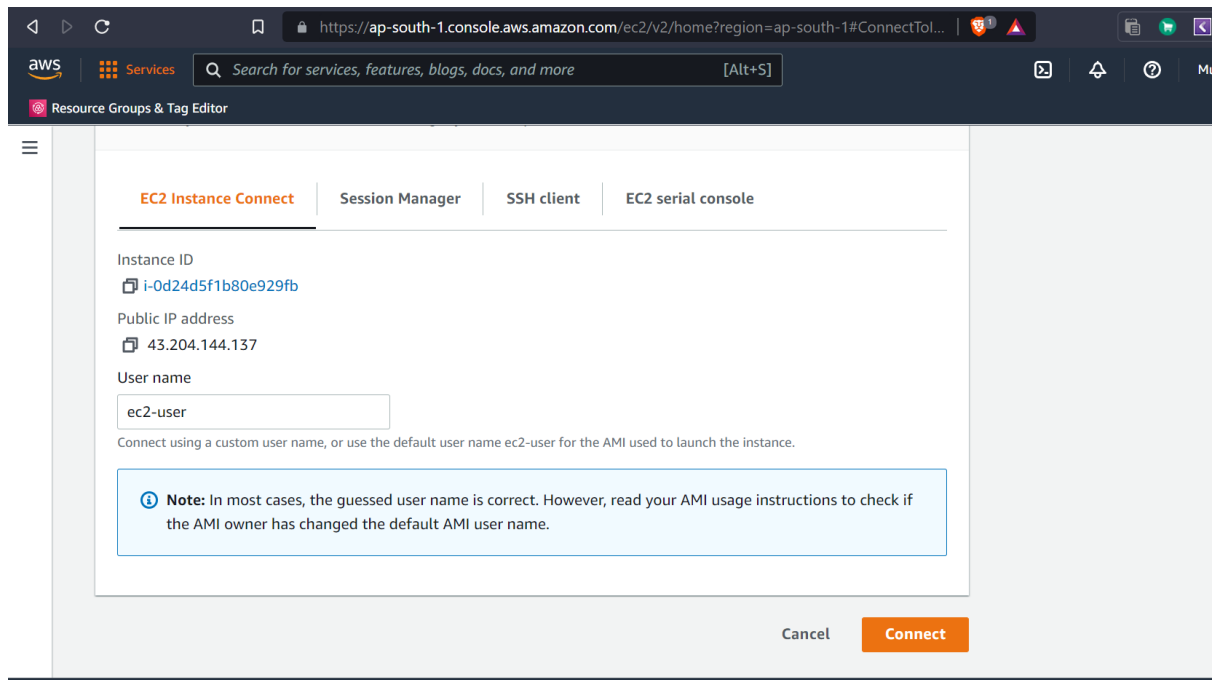
1. Direct connect from AWS (Browser access)
2. Using Putty (for windows people)
3. Using ssh (for linux or mac os people)

Direct connect (works only for some images like amazon and ubuntu)

1. Select the box of ec2-instance and click on connect written above.



2. Click on connect



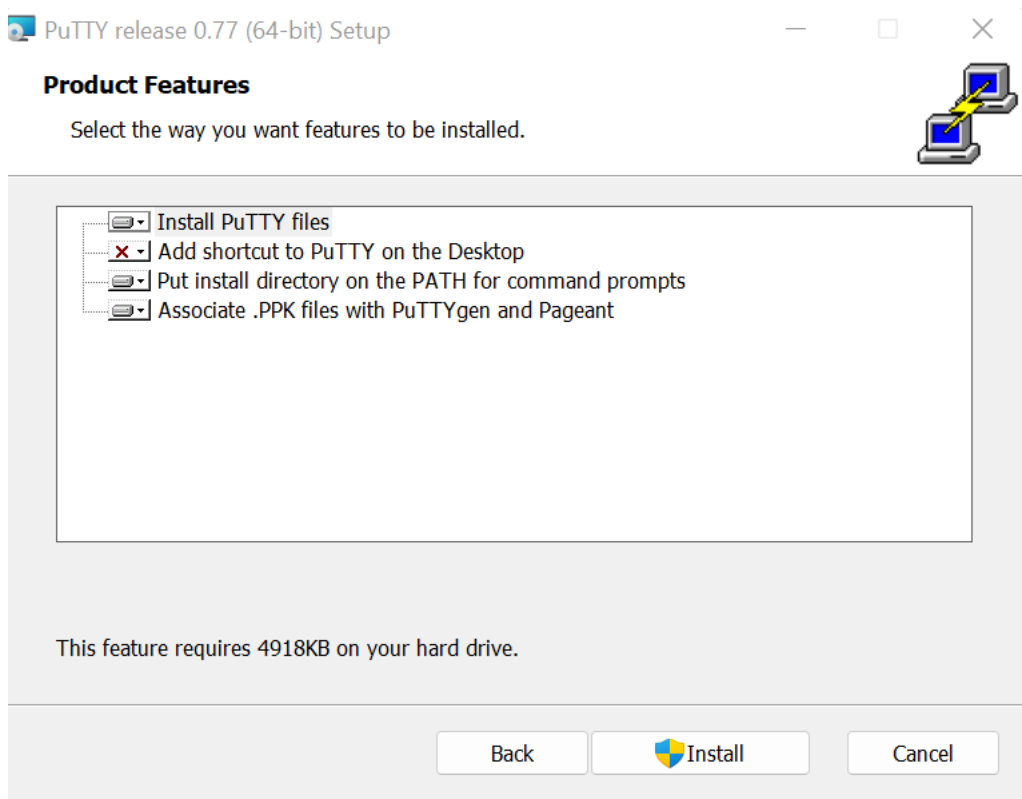
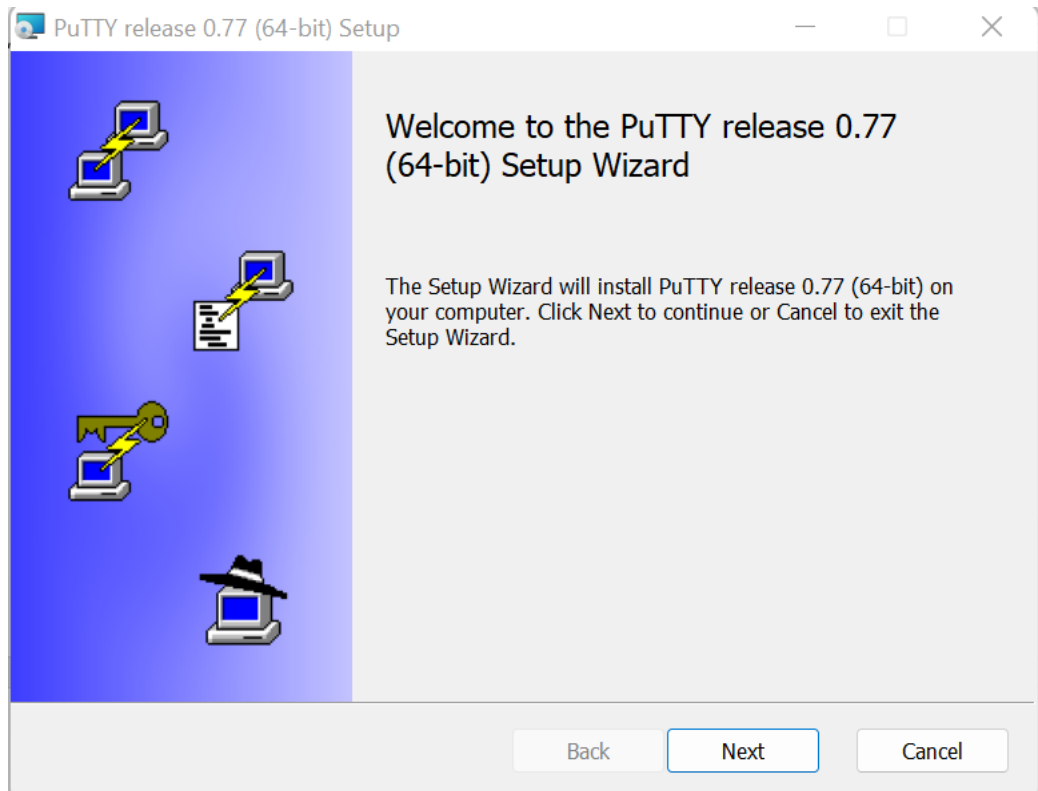
i-0d24d5f1b80e929fb

Public IPs: 43.204.144.137 Private IPs: 172.31.15.53

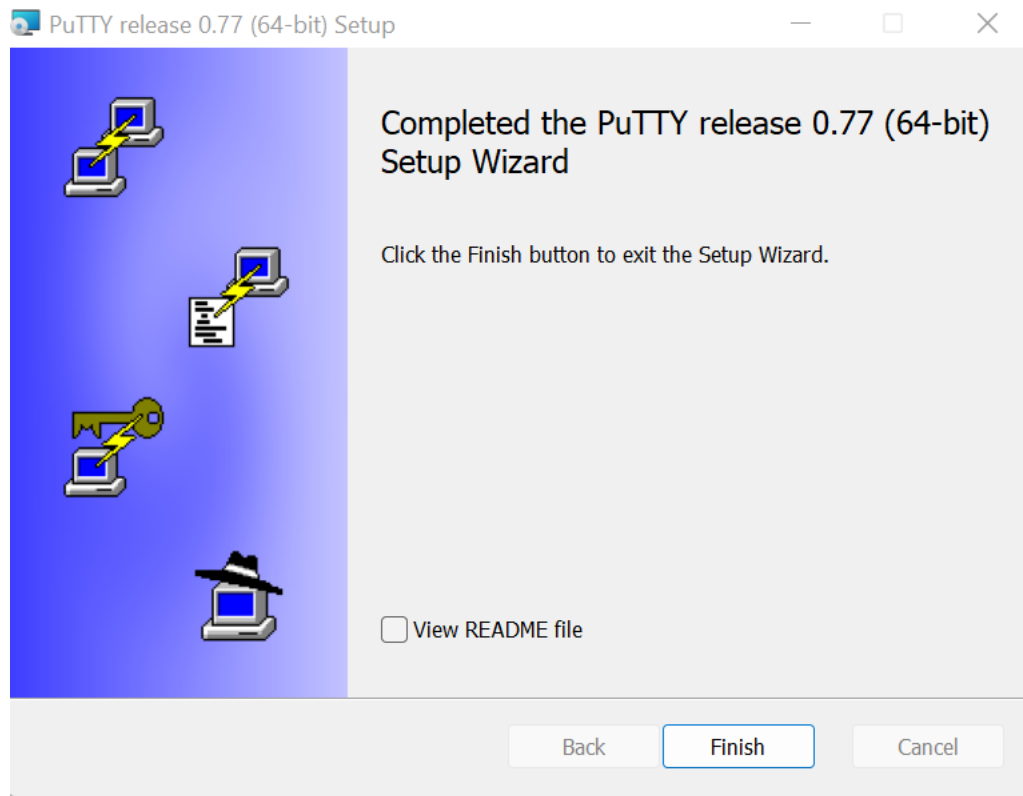
Will open terminal in new tab.

Using Putty for windows user

1. Download Putty from this link:- [putty link](#)
2. Install the application by clicking next next.

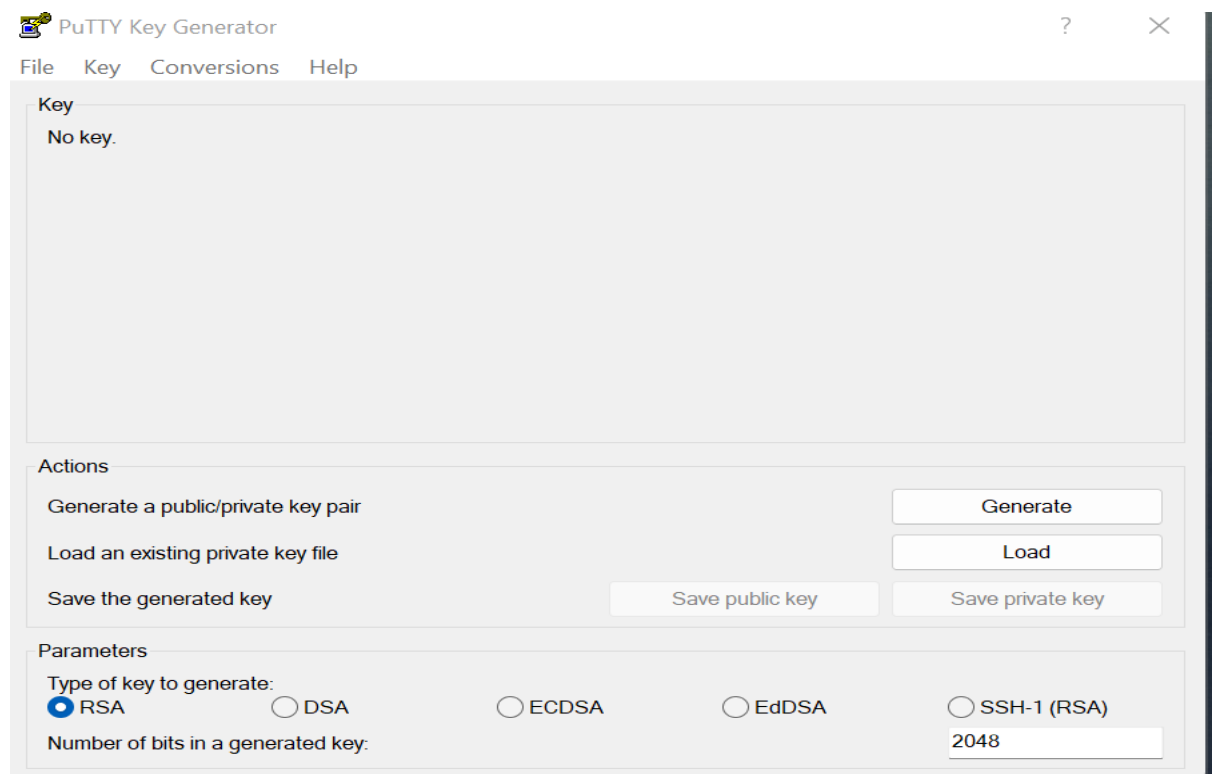


Click on install

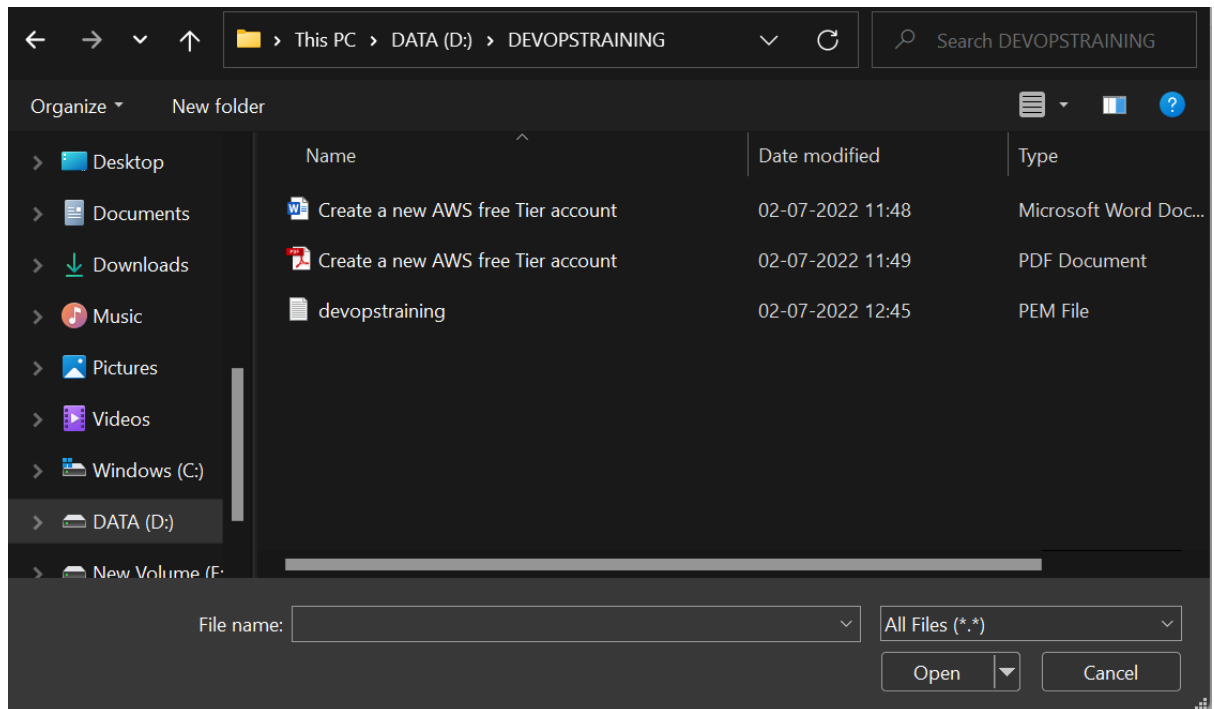


Click on finish

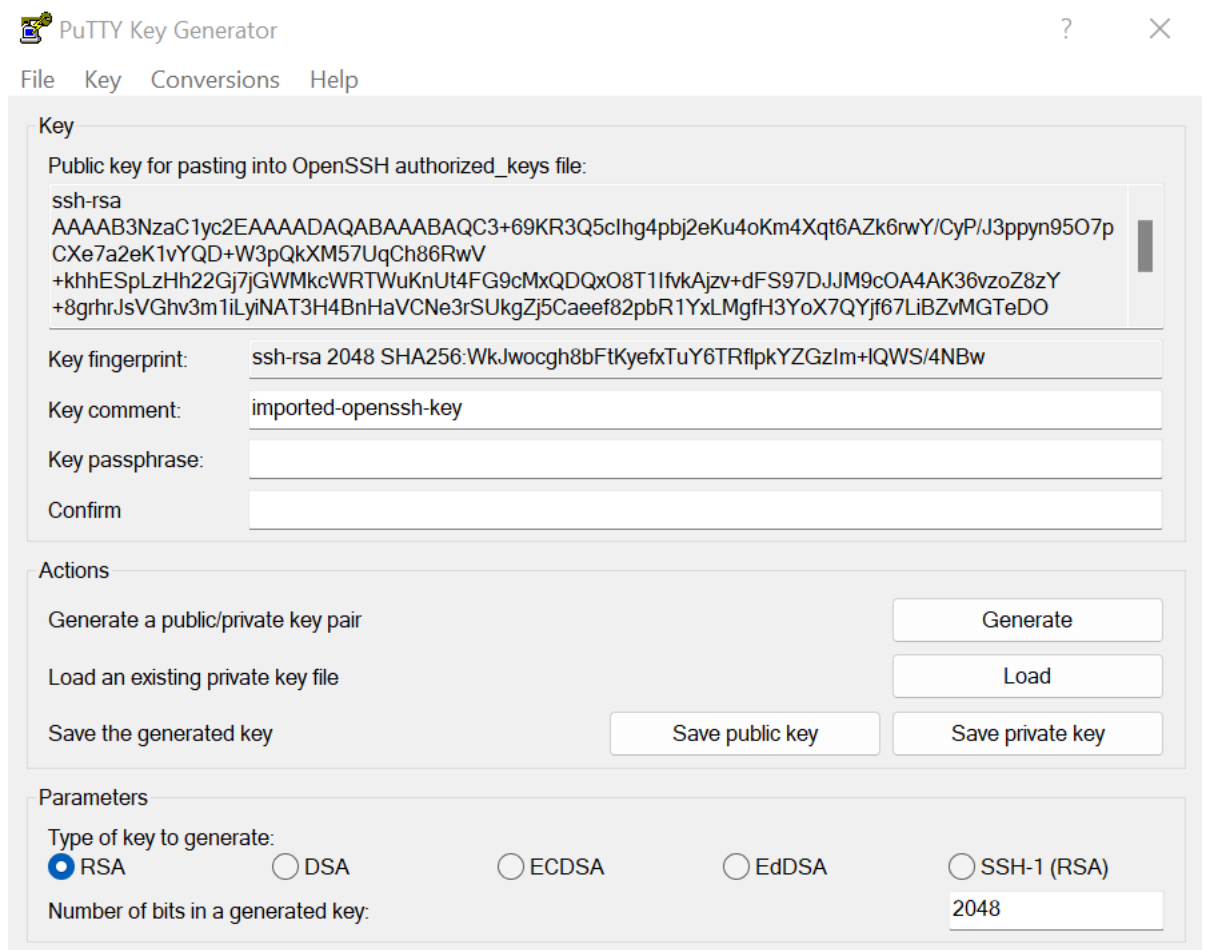
3. Now search “puttygen” in windows search section and open it.



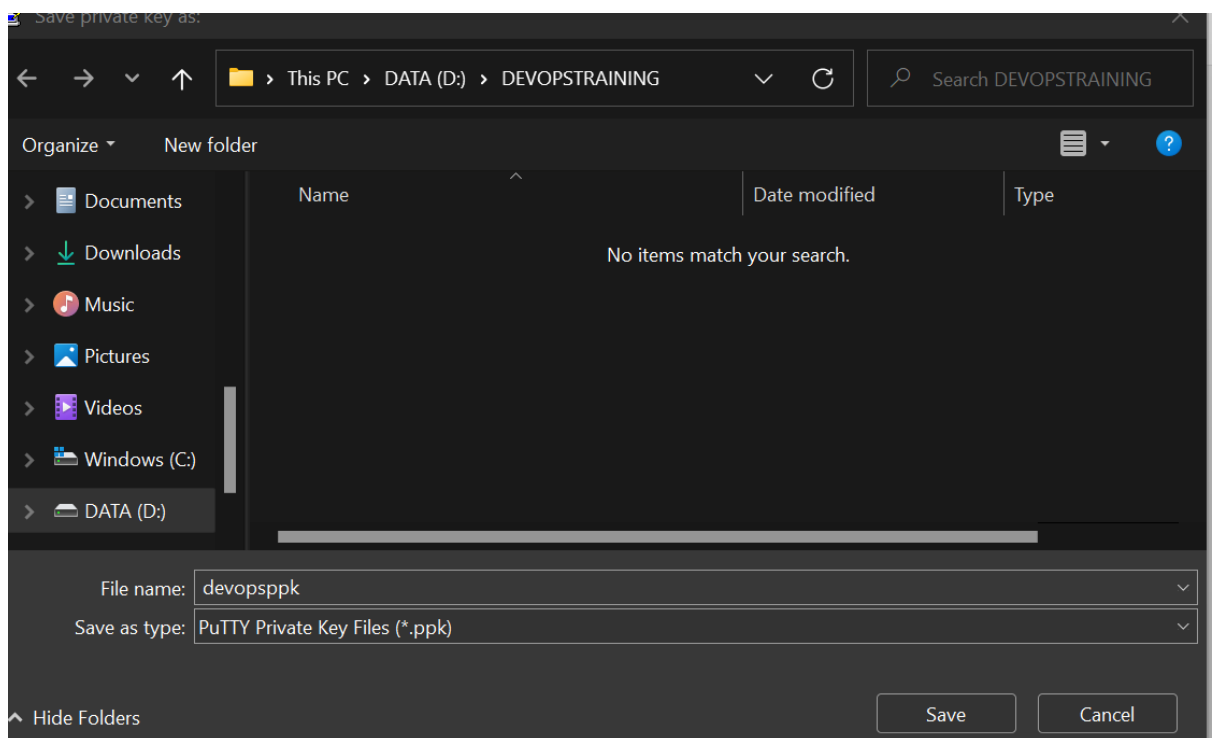
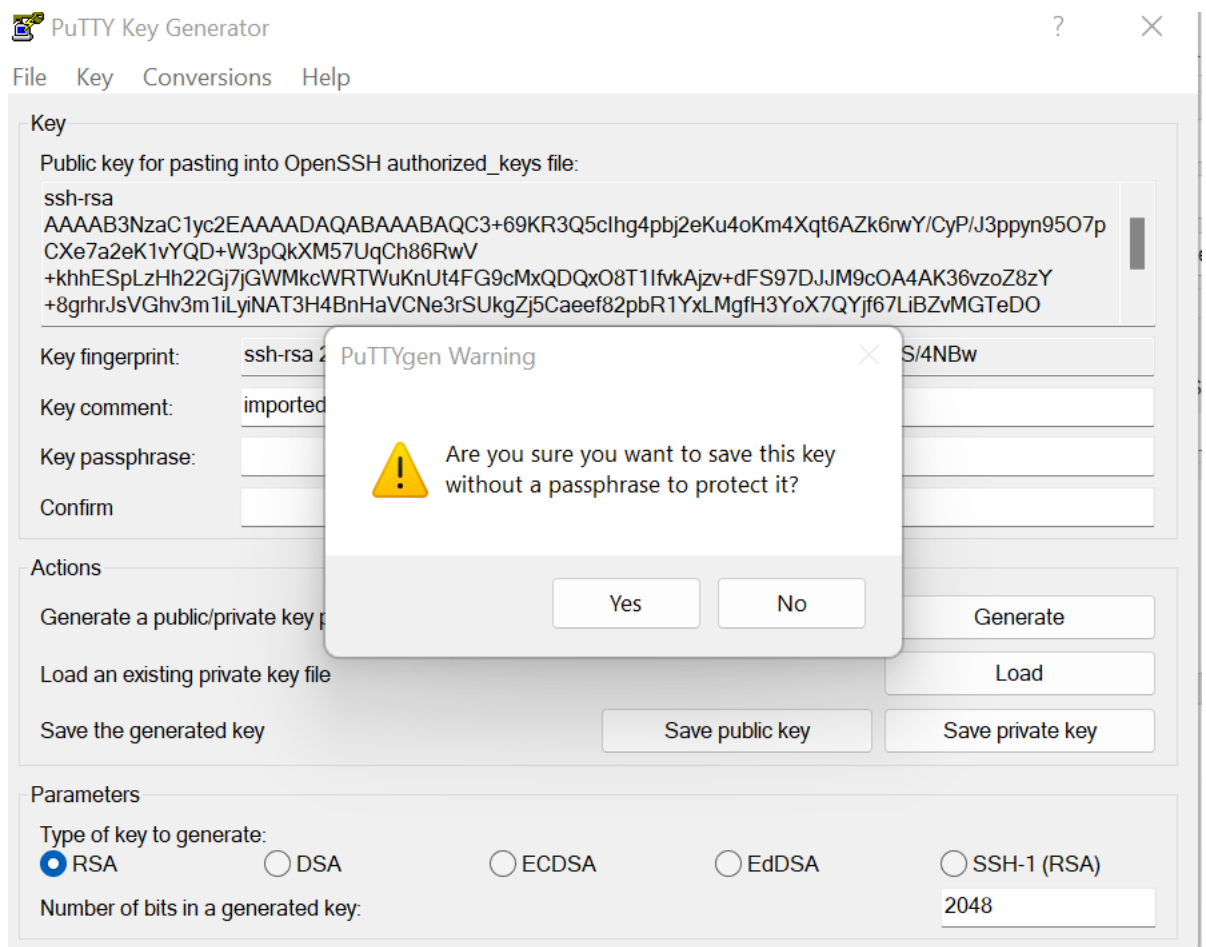
- Now click on load and open that folder where .pem key file is downloaded while launching ec2 instance and choose file types to all.



- Select devopstraining.pem file and click open

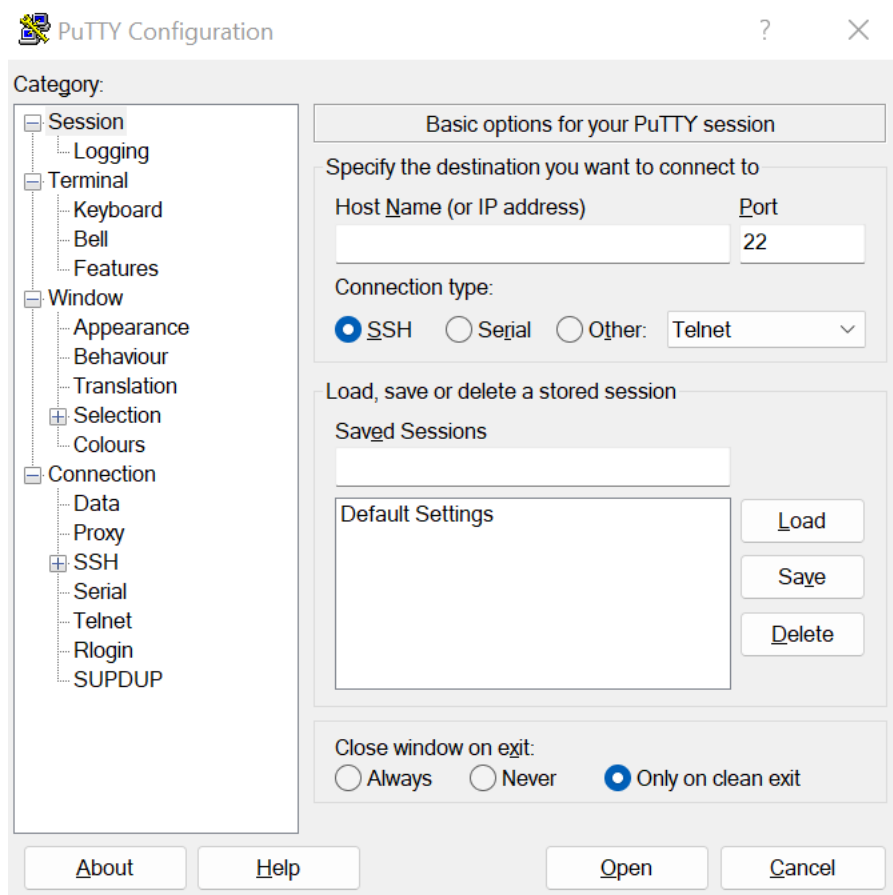


6. Click on save private key

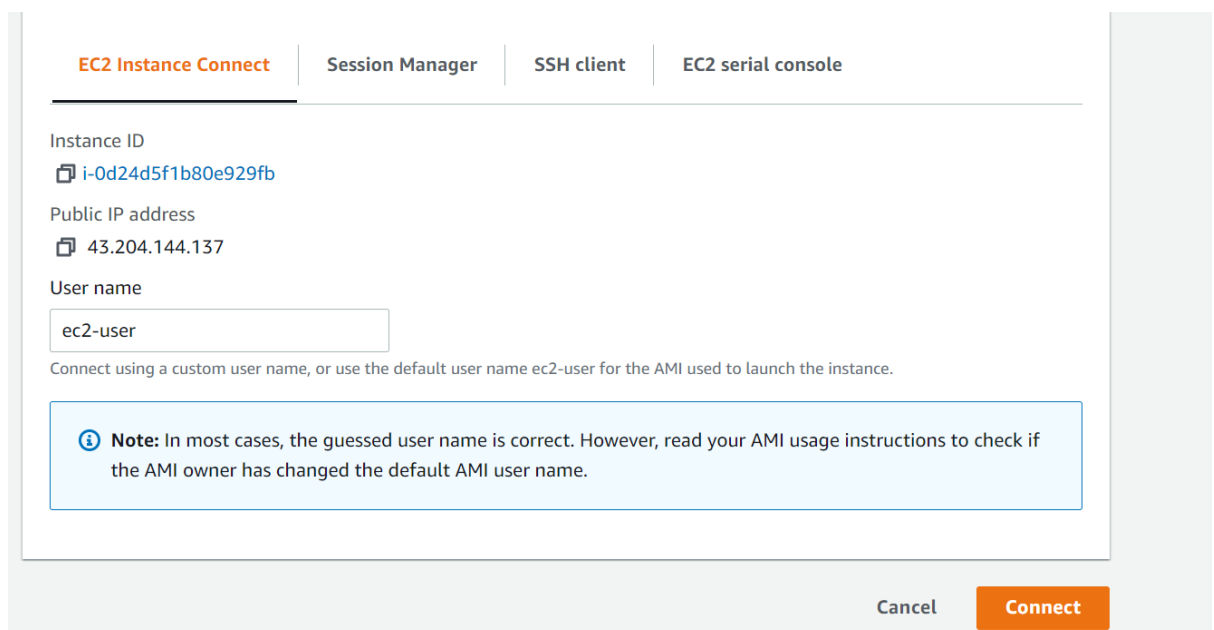


Click save.

7. Now open putty



8. In host name write “username@public-IP”



9. Here username is “ec2-user” and public-ip is “43.204.144.137”. will be different in your case.

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)

ec2-user@43.204.144.137

Port

22

Connection type:

☒ SSH

☐ Serial

☐ Other:

Telnet

Load, save or delete a stored session

Saved Sessions

Default Settings

Load

Save

Delete

Close window on exit:

☐ Always

☐ Never

☒ Only on clean exit

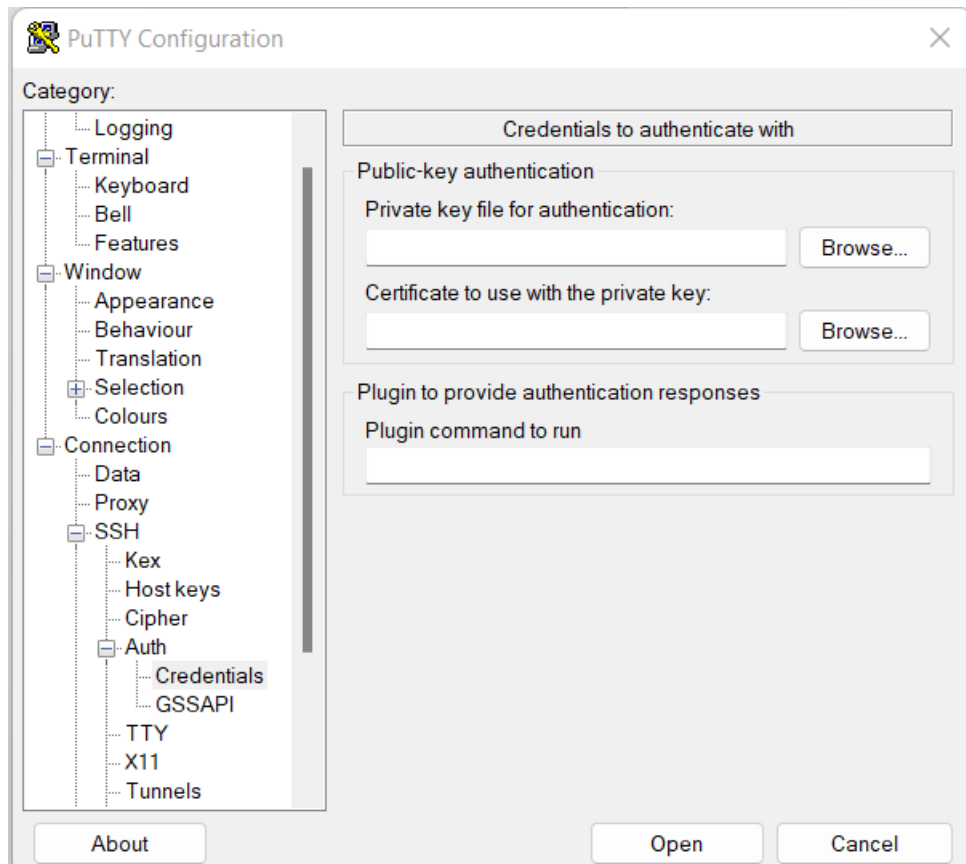
About

Help

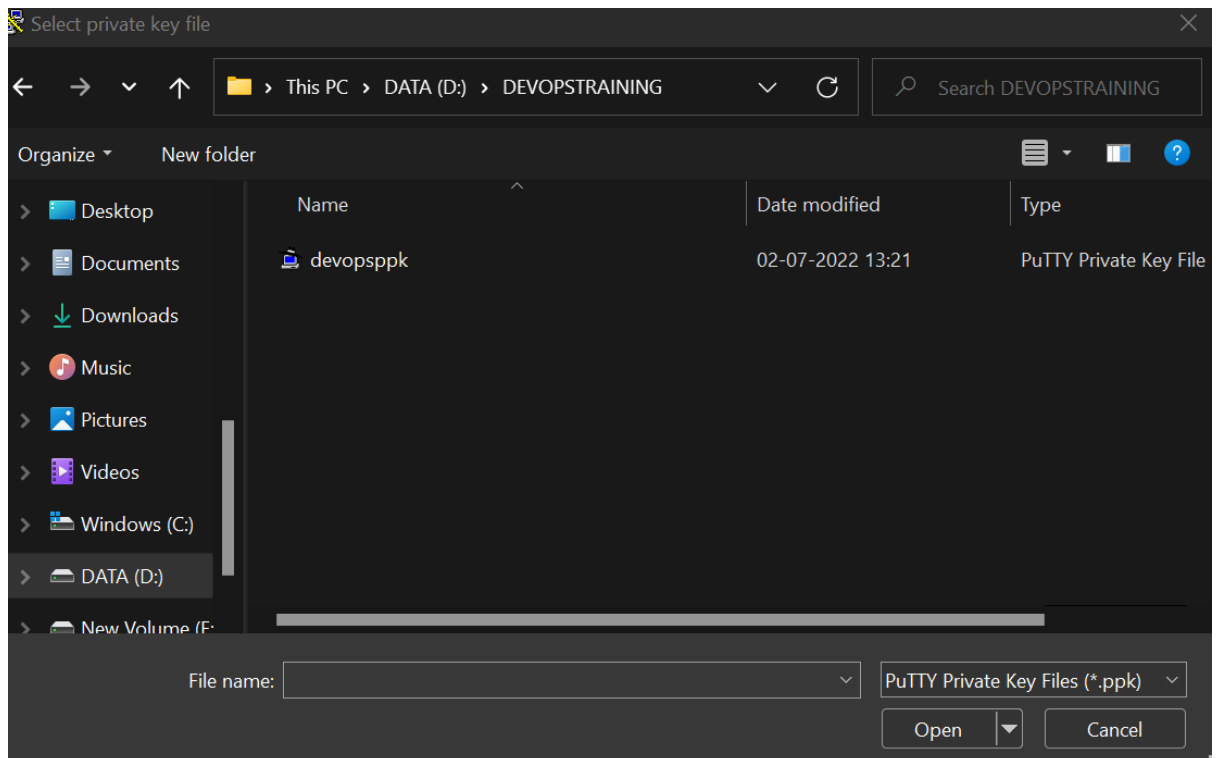
Open

Cancel

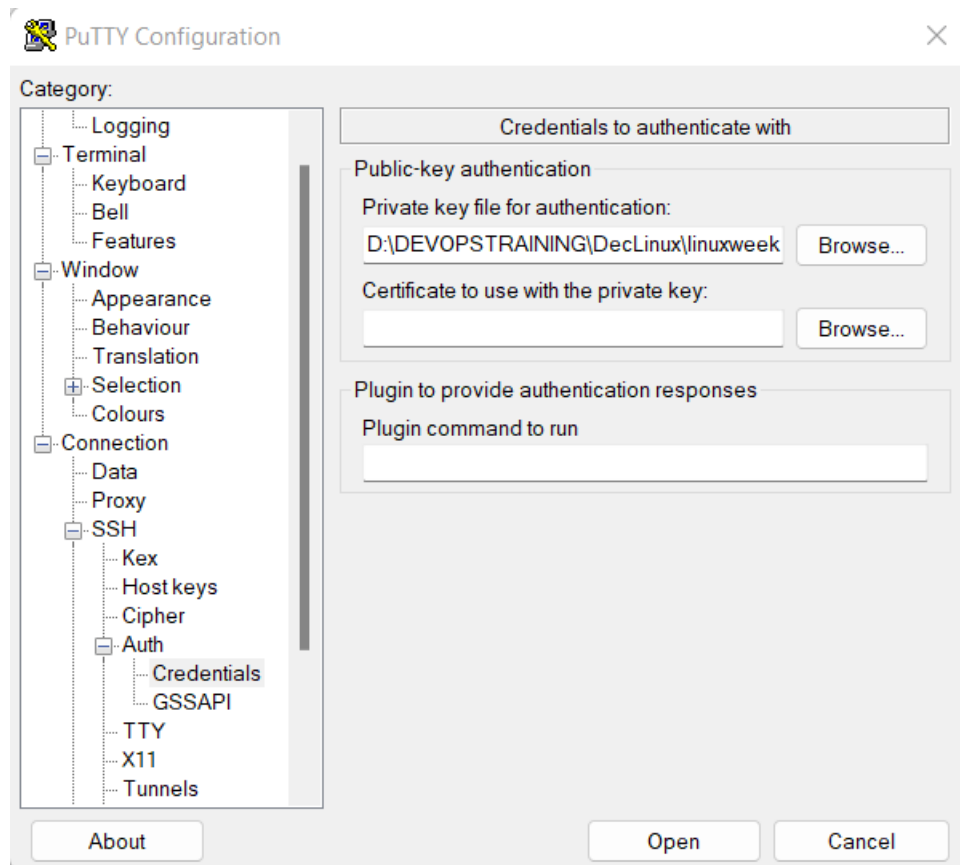
Click on ssh and then auth and then credentials



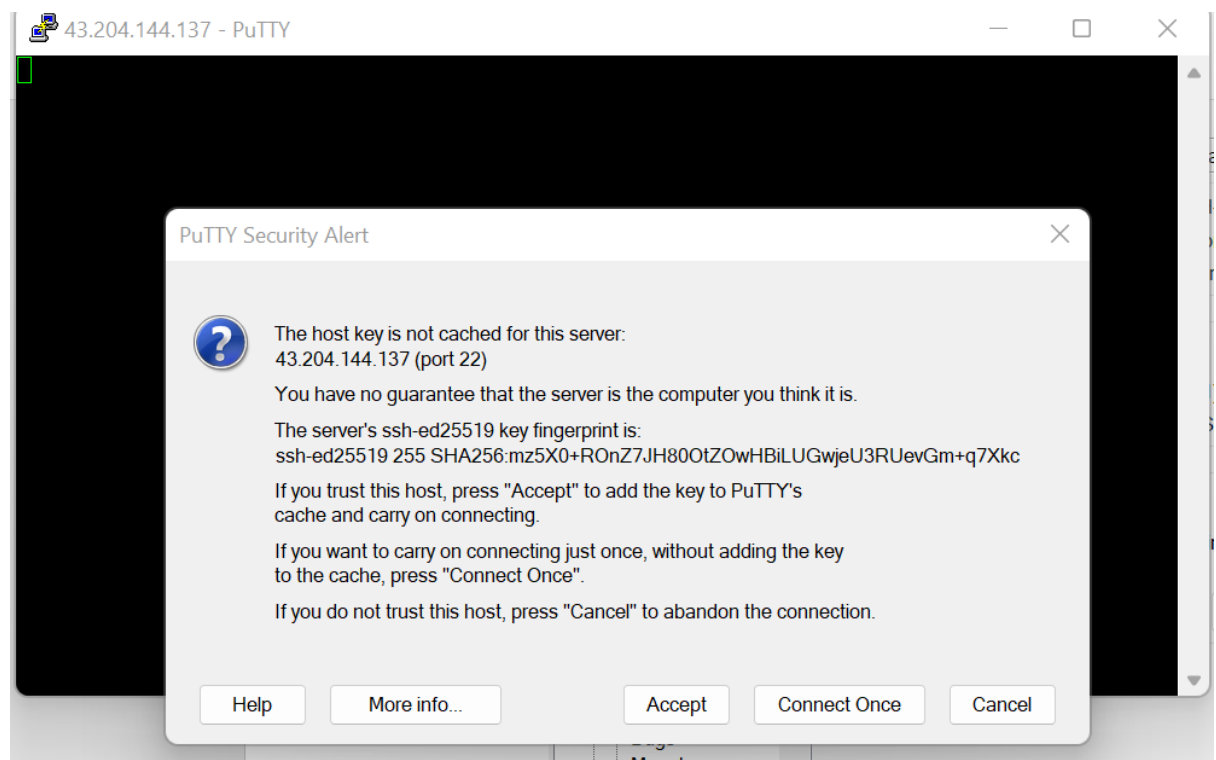
Then click on browse and select the ppk file earlier we saved.



Now select and open



Now click on open



Click on Accept.


```
ec2-user@ip-172-31-15-53:~  
Using username "ec2-user".  
Authenticating with public key "imported-openssh-key"  
Last login: Sat Jul  2 07:28:34 2022 from ec2-13-233-177-0.ap-south-1.compute.am  
amazonaws.com  
  
      _|_  _|_  )  
      _|_ ( _|_ /  Amazon Linux 2 AMI  
      _|_ \ _|_ |  
  
https://aws.amazon.com/amazon-linux-2/  
[ec2-user@ip-172-31-15-53 ~]$
```

Connect to ec2 instance successfully.

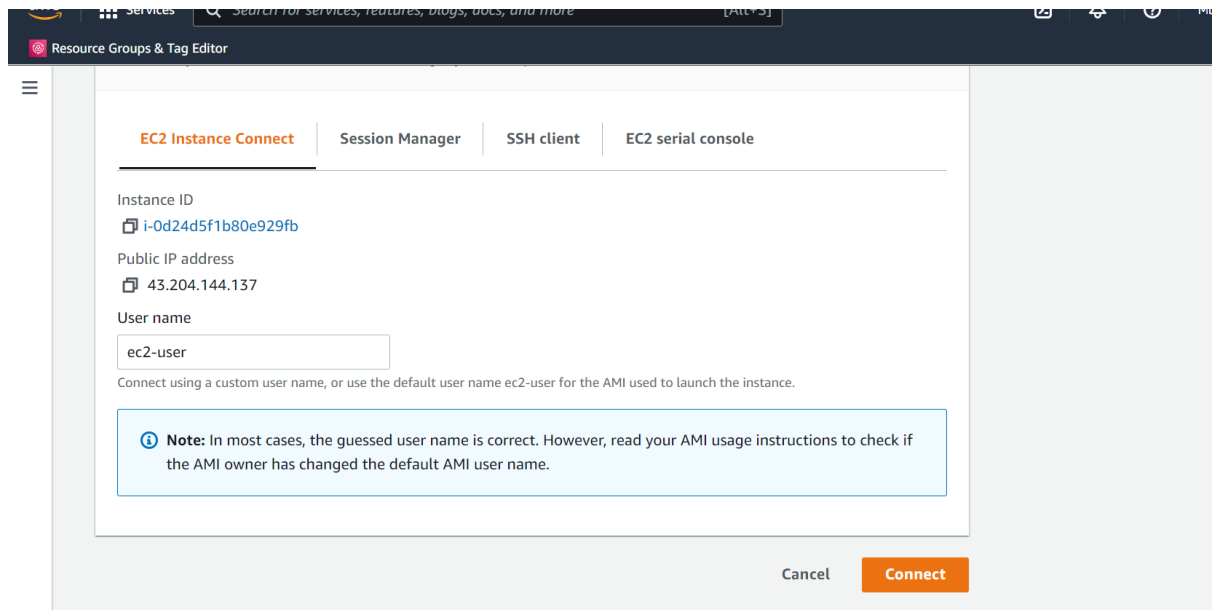
Using ssh (for linux or mac os people)

1. Open terminal and go to folder where you downloaded the .pem file while creating aws ec2-instance.

```
kishan@kishan-HP: ~/devopstraining  
kishan@kishan-HP:~$ cd devopstraining/  
kishan@kishan-HP:~/devopstraining$ ls  
devopstraining.pem  
kishan@kishan-HP:~/devopstraining$
```

In my case I stored my .pem file in DEVOPSTRaining folder.

2. Now go to aws console and click on connect like we done previously in direct browser connection.



Click on SSH Client

EC2 Instance Connect | Session Manager | **SSH client** | EC2 serial console

Instance ID
i-0d24d5f1b80e929fb

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is devopstraining.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
chmod 400 devopstraining.pem
4. Connect to your instance using its Public DNS:
ec2-43-204-144-137.ap-south-1.compute.amazonaws.com

Example:
ssh -i "devopstraining.pem" ec2-user@ec2-43-204-144-137.ap-south-1.compute.amazonaws.com

Note: In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

3. Now run command written in step3 : chmod 400 devopstraining.pem

```

ishan@kishan-HP:~$ cd devopstraining/
ishan@kishan-HP:~/devopstraining$ ls
devopstraining.pem
ishan@kishan-HP:~/devopstraining$ chmod 400 devopstraining.pem
ishan@kishan-HP:~/devopstraining$

```

4. Now run the command written in example of aws console.

EC2 Instance Connect	Session Manager	SSH client	EC2 serial console
<p>Instance ID i-0d24d5f1b80e929fb</p> <ol style="list-style-type: none"> 1. Open an SSH client. 2. Locate your private key file. The key used to launch this instance is devopstraining.pem 3. Run this command, if necessary, to ensure your key is not publicly viewable. <pre>chmod 400 devopstraining.pem</pre> 4. Connect to your instance using its Public DNS: <pre>ec2-43-204-144-137.ap-south-1.compute.amazonaws.com</pre> <p>Example: <pre>ssh -i "devopstraining.pem" ec2-user@ec2-43-204-144-137.ap-south-1.compute.amazonaws.com</pre></p> <div style="border: 1px solid #007bff; padding: 10px; margin-top: 10px;"> <p>Note: In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.</p> </div>			

```

ishan@kishan-HP:~/devopstraining$ ssh -i "devopstraining.pem" ec2-user@ec2-43-204-144-137.ap-south-1.compute.amazonaws.com
The authenticity of host 'ec2-43-204-144-137.ap-south-1.compute.amazonaws.com (43.204.144.137)' can't be established.
ECDSA key fingerprint is SHA256:edmyRh+c9/ucrm65iIvJvNEi65IvnlmXsPKrHoKk2wA.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-43-204-144-137.ap-south-1.compute.amazonaws.com,43.204.144.137' (ECDSA) to the list of known hosts.
Last login: Sat Jul 2 07:57:25 2022 from 43.230.42.116

 _ _ | _ _ | _ _ |
 _ | ( _ _ | / Amazon Linux 2 AMI
 _ | \ _ _ | _ _ |

https://aws.amazon.com/amazon-linux-2/
ec2-user@ip-172-31-15-53 ~]$

```

Connected..

Hence we completed all the popular ways to connect to our ec2-instance.

Regards: kishan ray

