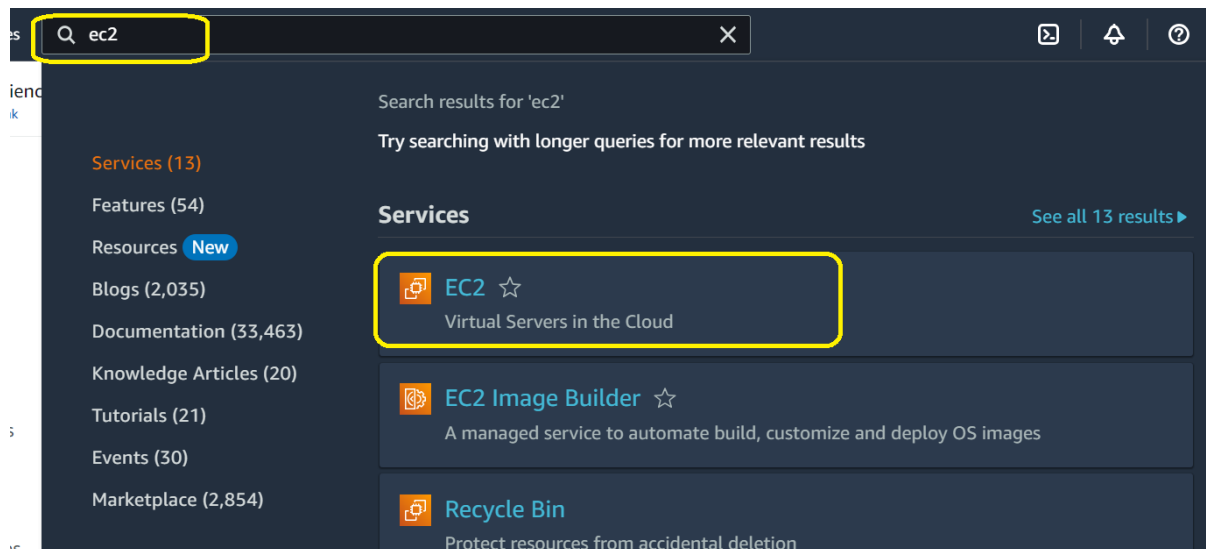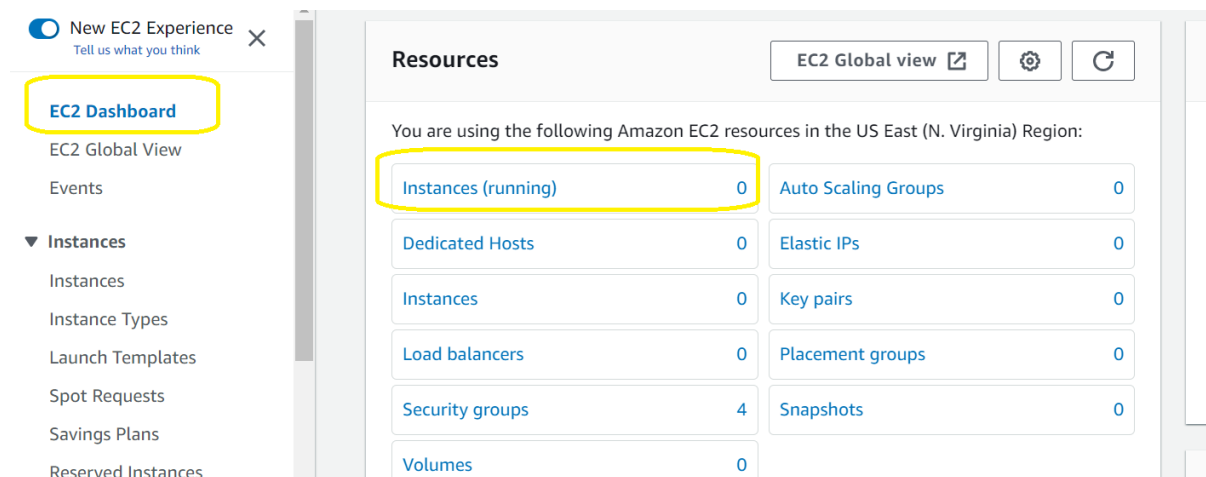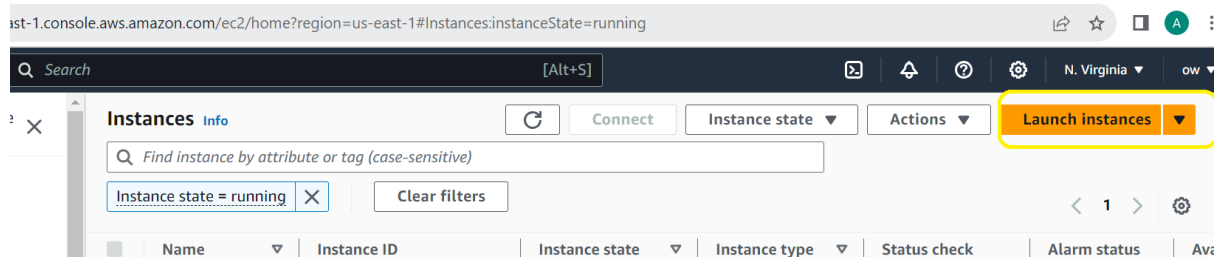1. Login to aws console
2. Search for ec2 and go to ec2 dashboard

3. Ec2 dashboard→click on instances

4. Click on Launch instances

5.Provide a name and select ubuntu,

Select t2.medium instance type

Create new key pair

▼ 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

Provide name→RSA→.ppk (and click on create key pair) and it will **download one ppk file**

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

mykey

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

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 ↗

In network setting make sure auto-assign public ip is enabled

▼ Network settings Info

VPC - *required* Info

| vpc-05e85ba543a91205b | (default) |
| 172.31.0.0/16 | ▼ |

Subnet Info

| No preference | ▼ |

Auto-assign public IP Info

| Enable | ▼ |

Firewall (security groups) Info

In network setting→Create new security group

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

Security group name - *required*

| launch-wizard-4 |

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*

Description - *required* Info

| launch-wizard-4 created 2023-09-27T01:55:58.335Z |

Inbound Security Group Rules

Add security rule for ssh and jenkins

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0)   Remove

| Type Info | Protocol Info | Port range Info |
| ssh ▼ | TCP | 22 |

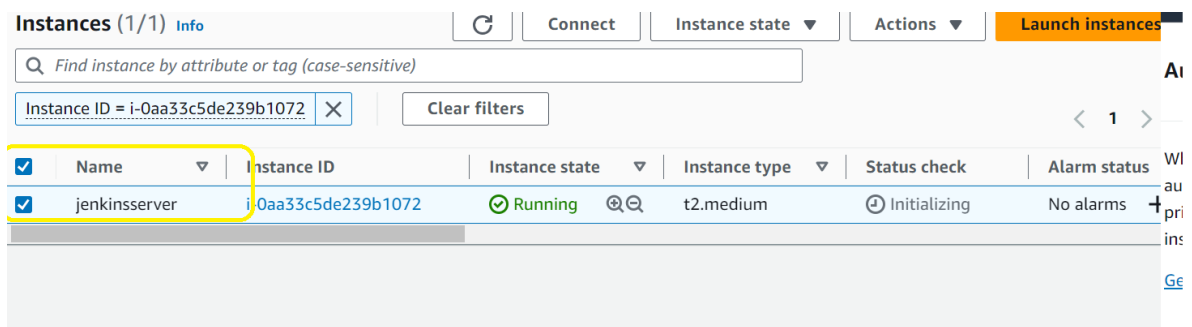| Source type Info | Source Info | Description - *optional* Info |
| Anywhere ▼ | 🔍 Add CIDR, prefix list or security ⊄ | e.g. SSH for admin desktop |
| | 0.0.0.0/0 ✕ | |

Add security group rule

In custom tcp provice source

Click on launch instance

Click on instance id

Select the instance id

Note down the public ip from details

Instance: i-0aa33c5de239b1072 (jenkinsserver)

| Details | Security | Networking | Storage | Status checks | Monitoring | Tags |

▼ Instance summary Info

Instance ID
📋 i-0aa33c5de239b1072 (jenkinsserver)

Public IPv4 address
📋 54.237.100.185 |open address ↗

Private IPv4 addresses
📋 172.31.56.233

IPv6 address

Instance state

Public IPv4 DNS

Download putty from putty.org

Download PuTTY

PuTTY is an SSH and telnet client, developed originally by Simon Tatham
Windows platform. PuTTY is open source software that is available with source
is developed and supported by a group of volunteers.

Download PuTTY

Go to Alternative Binaries and download

(Not sure whether you want the 32-bit or the 64-bit version? Read the FAQ entry.)

We also publish the latest PuTTY installers for all Windows architectures as a free-of-charge dov
we release them.

MSI ('Windows Installer')

64-bit x86:   putty-64bit-0.79-installer.msi   (signature)
64-bit Arm: putty-arm64-0.79-installer.msi   (signature)
32-bit x86:   putty-0.79-installer.msi   (signature)

Unix source archive

.tar.gz: putty-0.79.tar.gz   (signature)

Alternative binary files

The installer packages above will provide versions of all of these (except PuTTYtel and pterm),

(Not sure whether you want the 32-bit or the 64-bit version? Read the FAQ entry.)

putty.exe (the SSH and Telnet client itself)
64-bit x86:   putty.exe   (signature)
64-bit Arm: putty.exe   (signature)

Putty.exe

Open putty and provide public ip
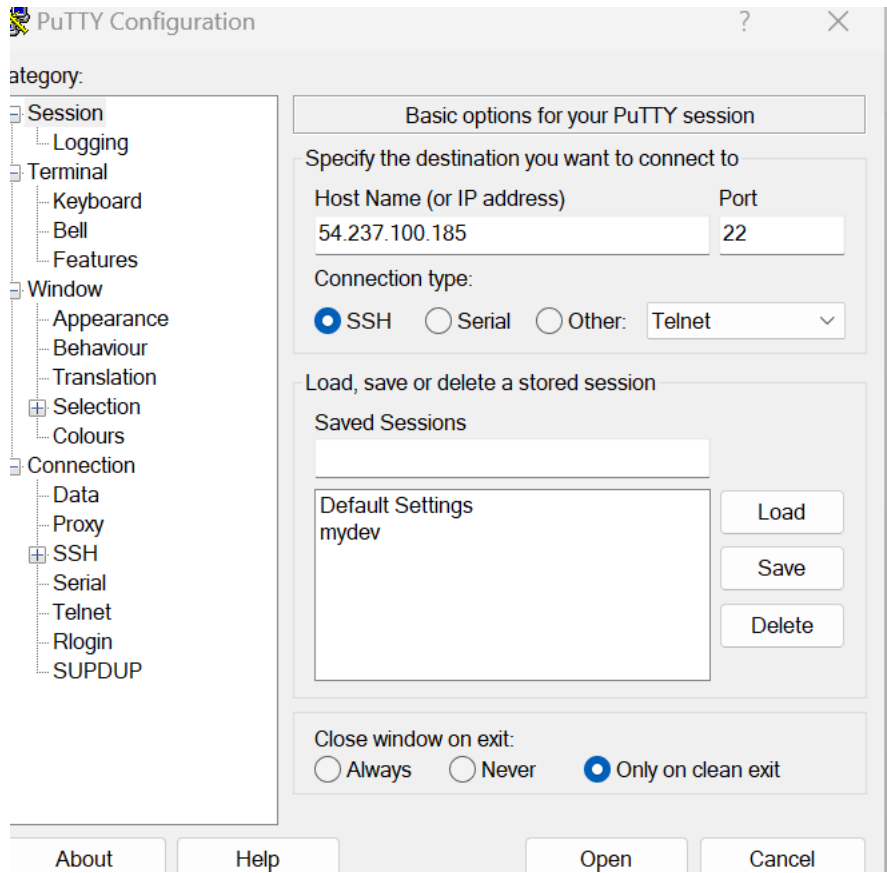
In putty→connection→ssh→auth→credentials

Map the ppk file

And click on open

Click on accept

PuTTY Security Alert

The host key is not cached for this server:
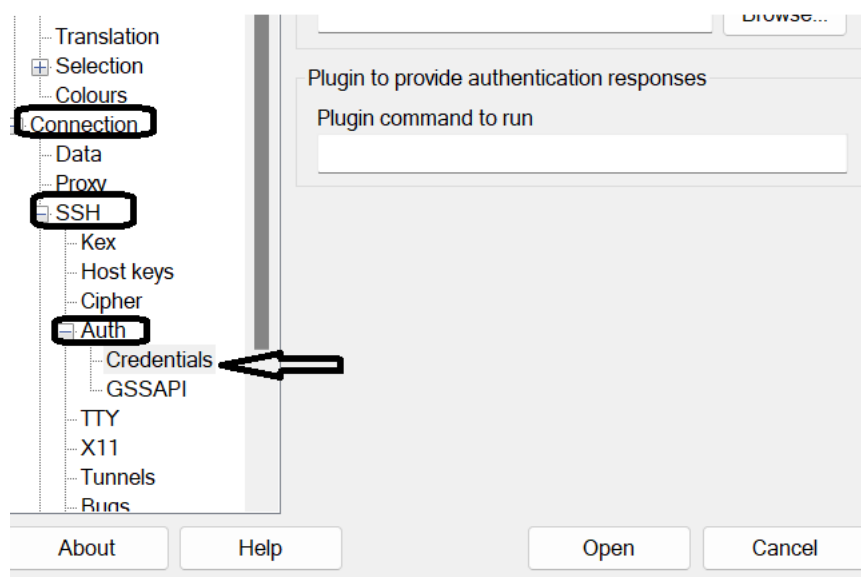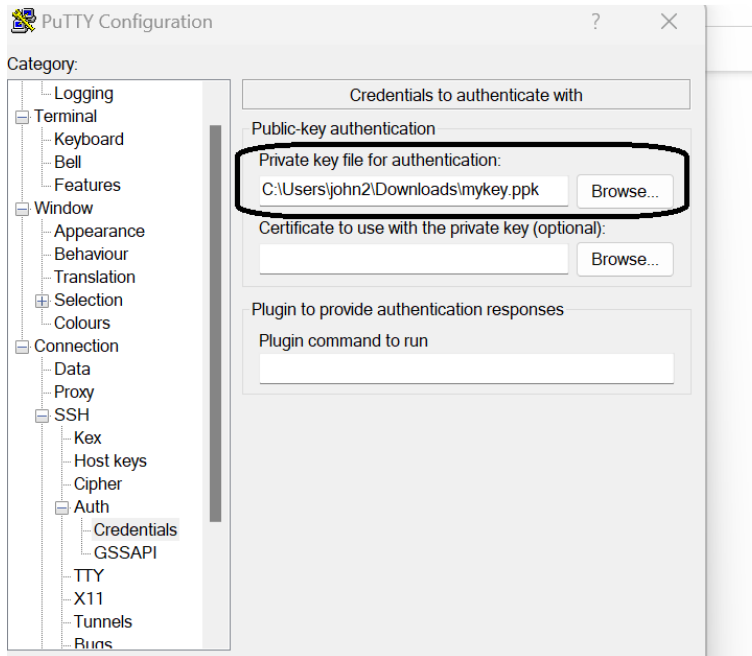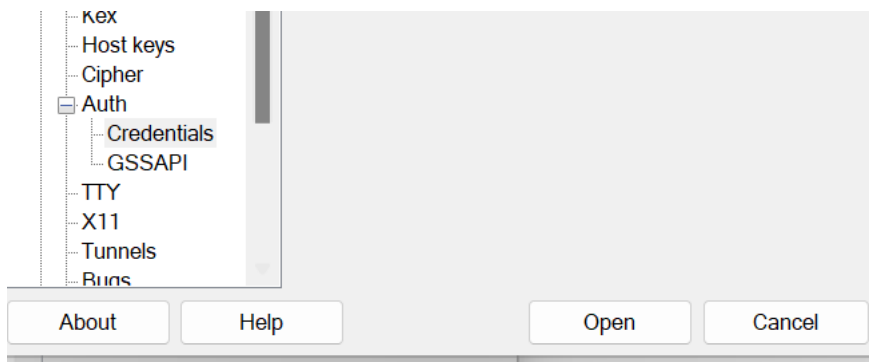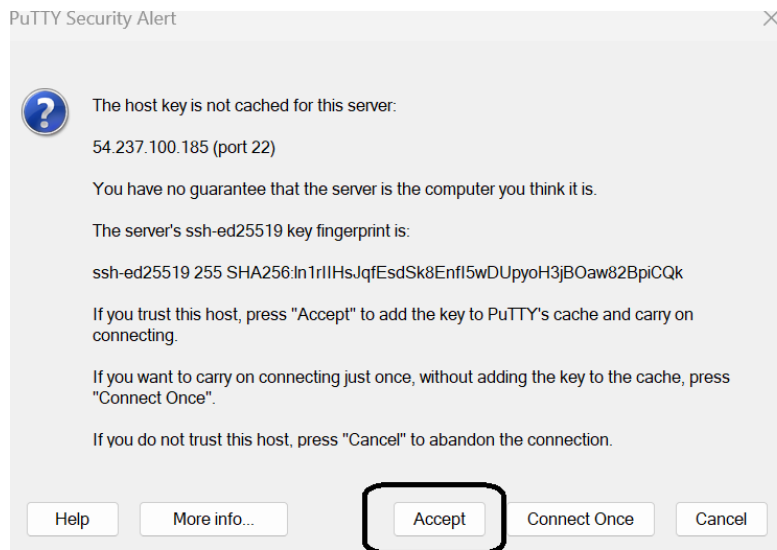
54.237.100.185 (port 22)

You have no guarantee that the server is the computer you think it is.

The server's ssh-ed25519 key fingerprint is:

ssh-ed25519 255 SHA256:ln1rlIHsJqfEsdSk8Enfl5wDUpyoH3jBOaw82BpiCQk

If you trust this host, press "Accept" to add the key to PuTTY's cache and carry on connecting.

If you want to carry on connecting just once, without adding the key to the cache, press "Connect Once".

If you do not trust this host, press "Cancel" to abandon the connection.

| Help | More info... | Accept | Connect Once | Cancel |

Provide the username : ubuntu


```
login as: ubuntu
Authenticating with public key "mykey"
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.19.0-1025-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Sep 27 03:02:42 UTC 2023

  System load:  0 080078125        Processes:        106
```

Login as root

sudo su root


```
To run a command as administrator (user "root"), use "
See "man sudo_root" for details.

ubuntu@ip-172-31-56-233:~$ sudo su root
root@ip-172-31-56-233:/home/ubuntu#
```