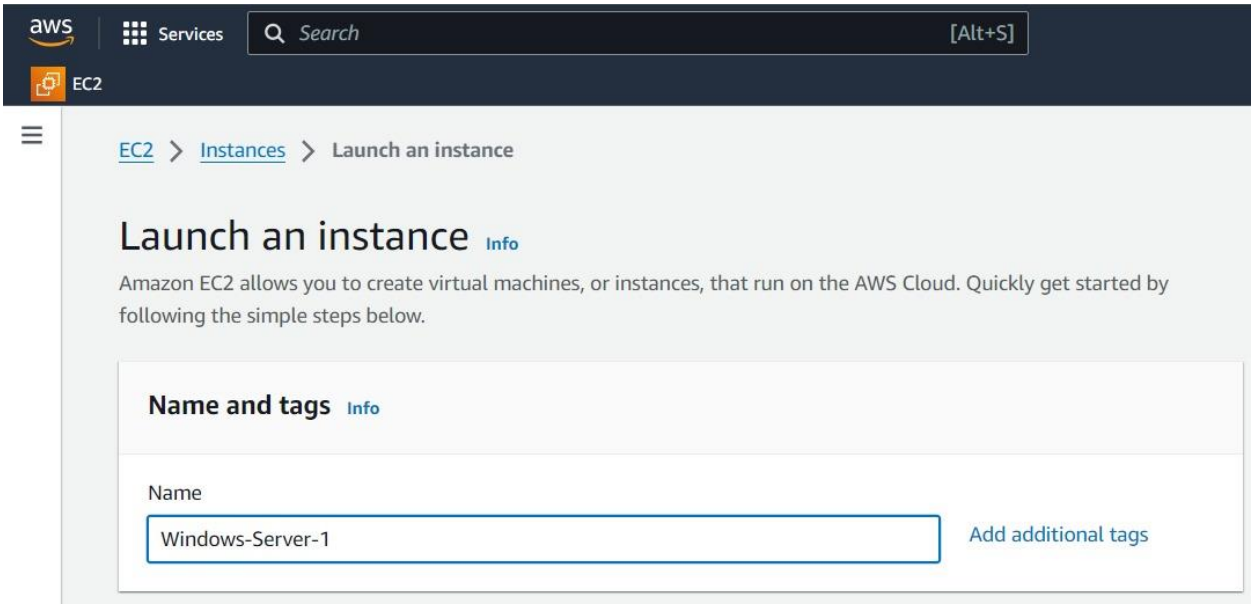
TASK 1

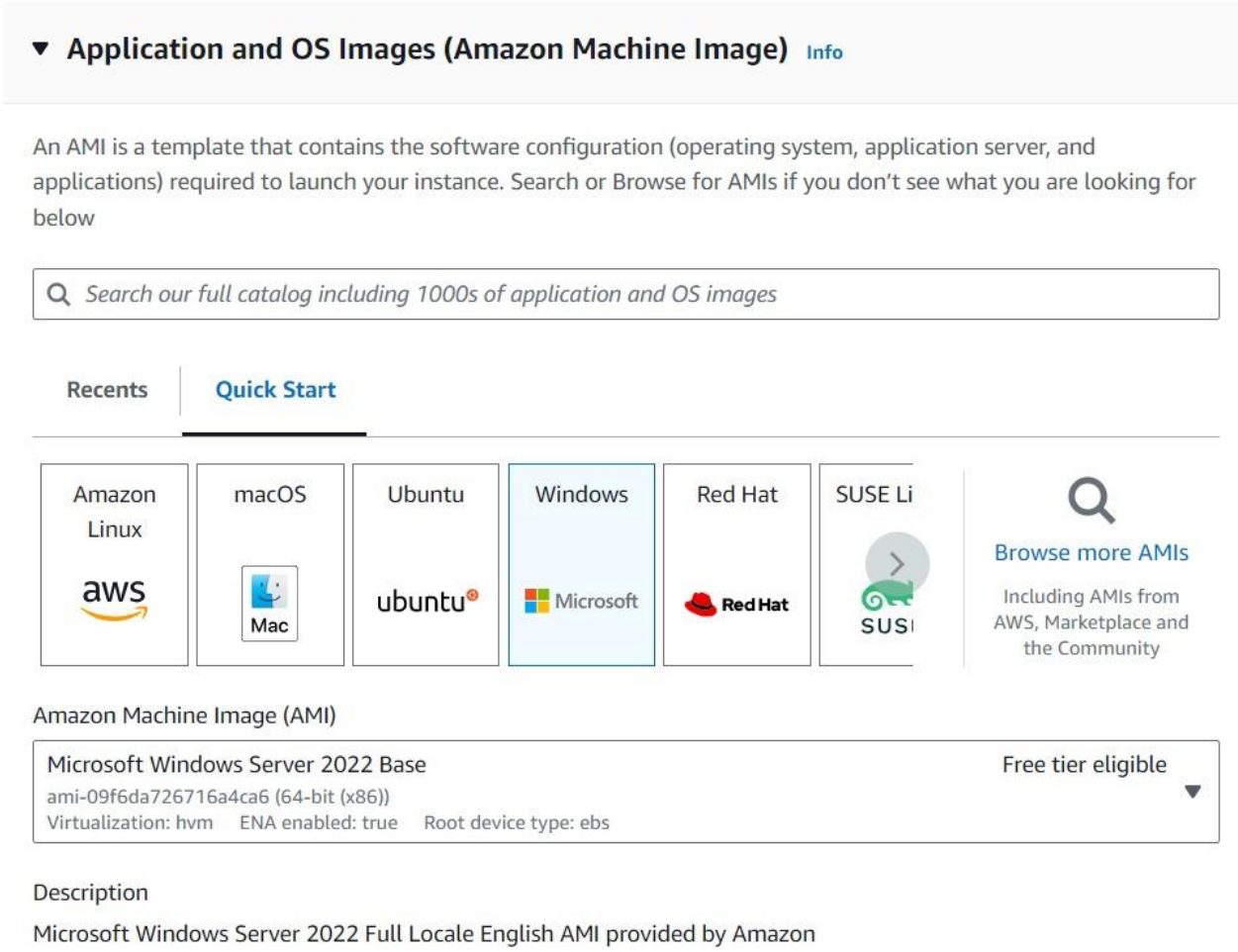
Aim: (A)Deploy a **Windows Instance** In **Another Windows Instance**

Steps:

1) Create an windows instance on EC2 **(Windows-Server-1)**

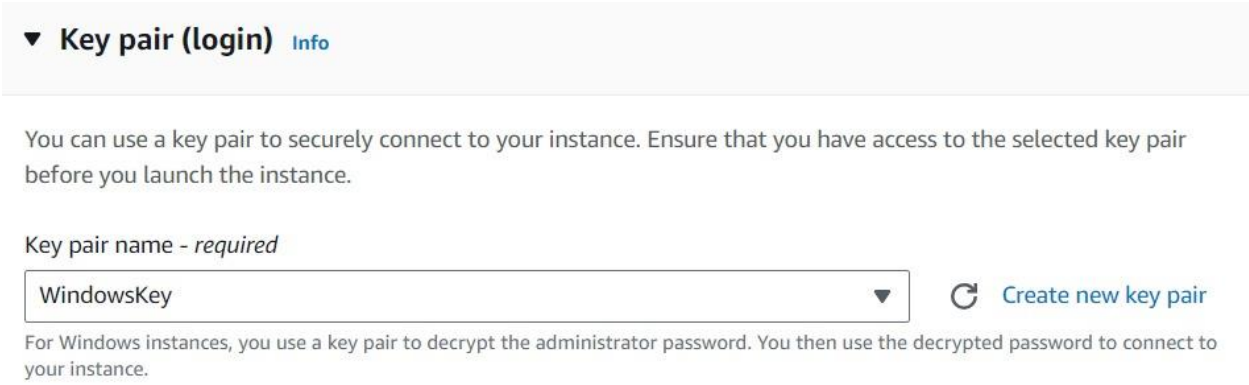


2) Select Amazon Machine Image (AMI) as Windows and Select Windows Server Base 2016 or Later

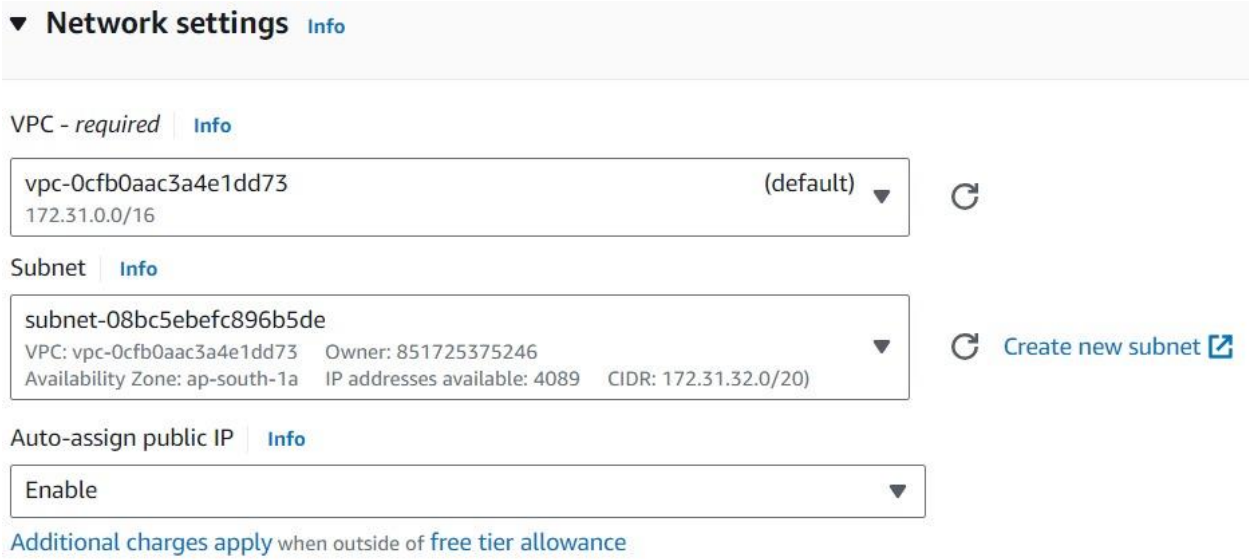


3) Choose Instance Type As Per Your Requirements

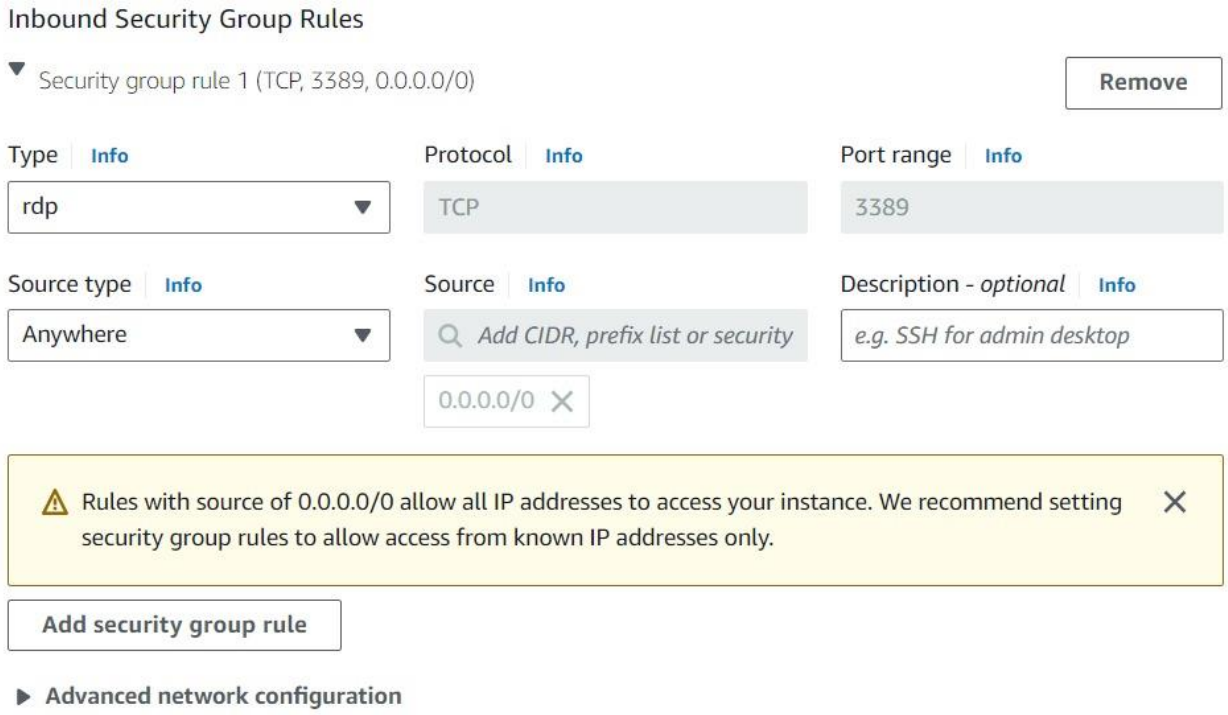
4) Create a Key Pair and Select It



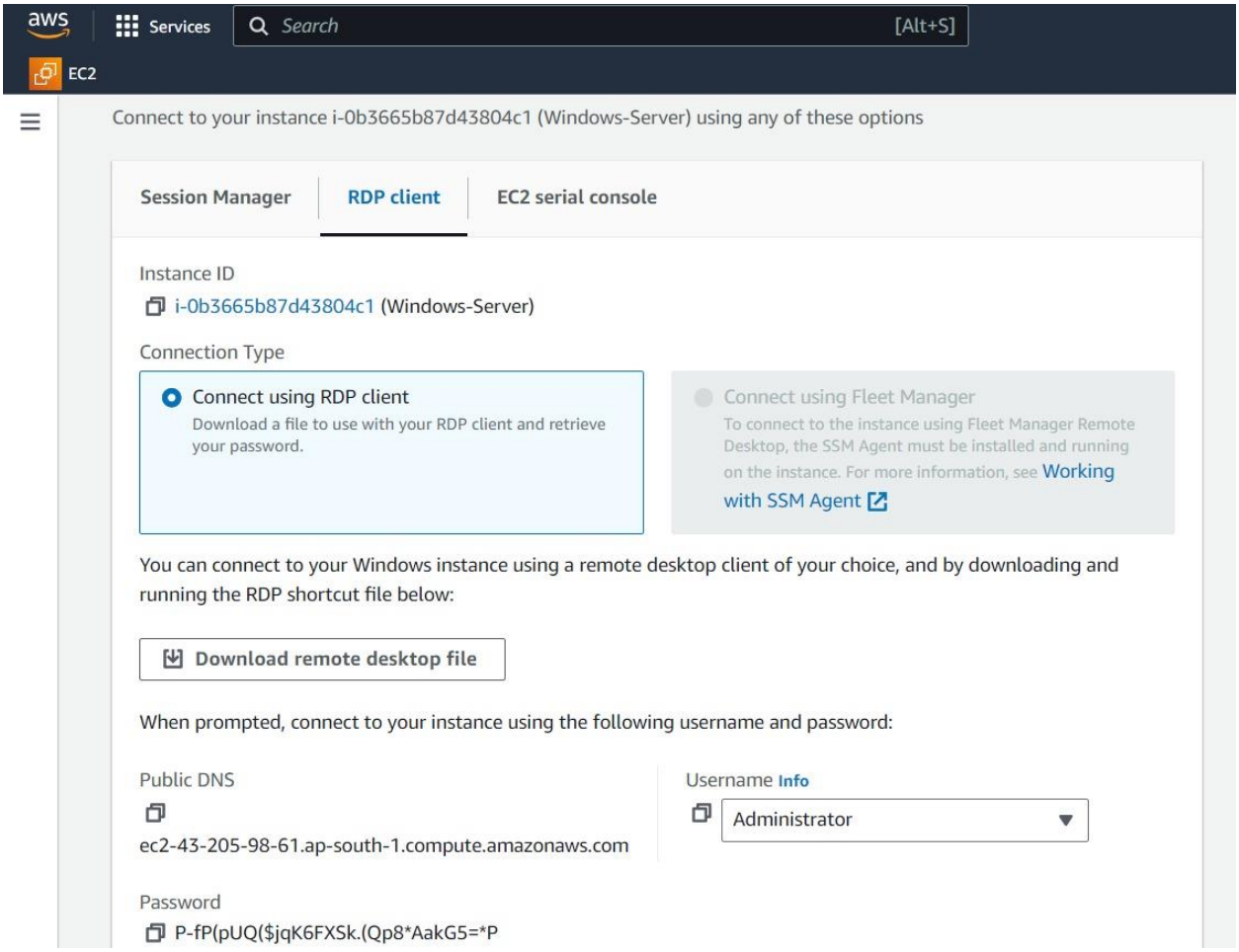
5) Edit Network Settings And Select Subnet : ap-south-1a OR ap-south-1b



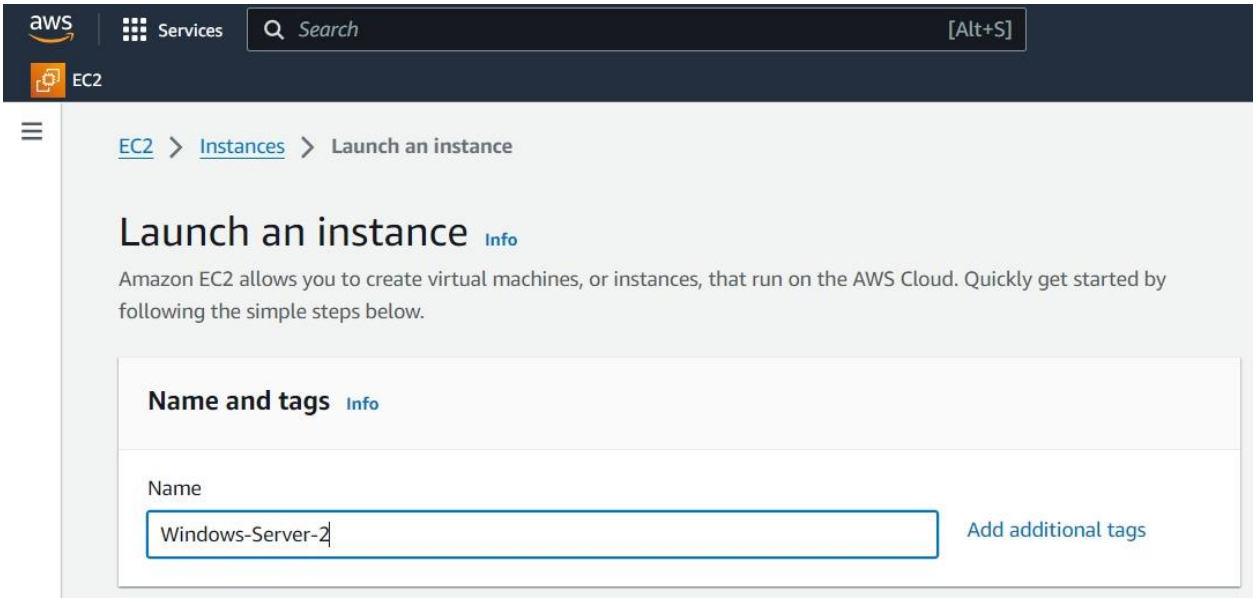
6) In Inbound Security Group Rules, Set Type To **“rdp”** and Source Type as “**Anywhere”**



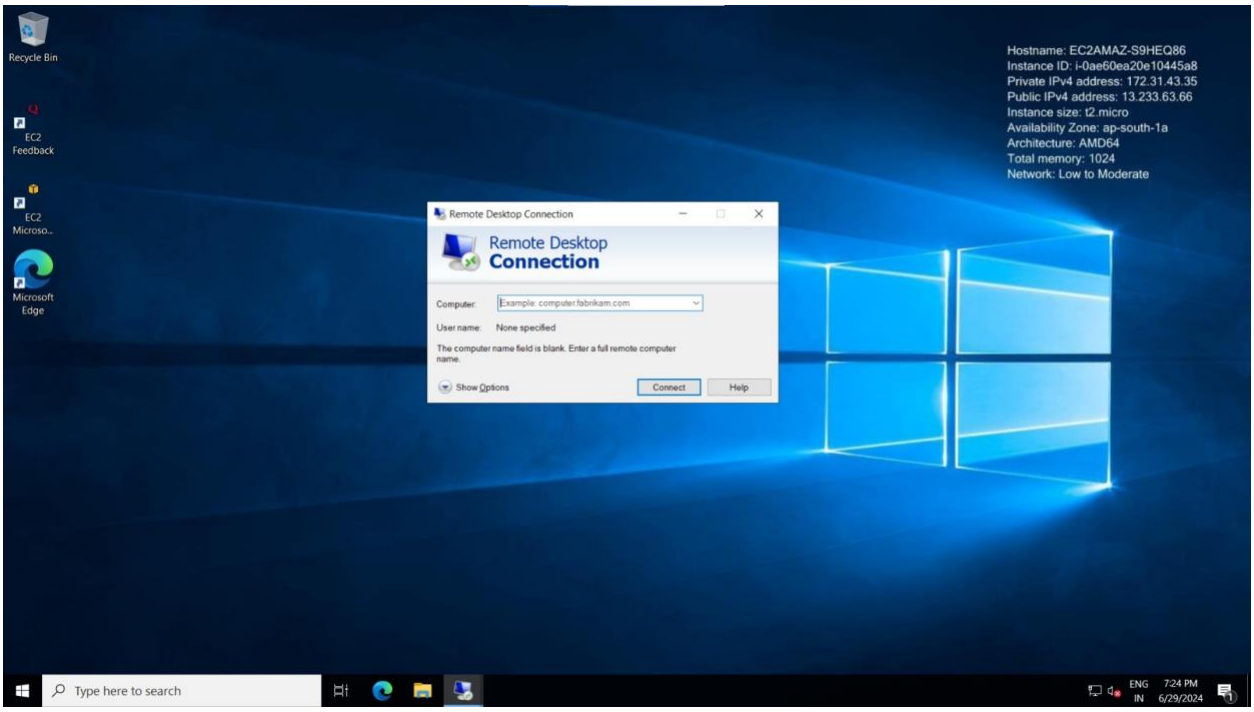
7) Get password from the created .pem key and use it to connect the rdp file and launch the Windows Instance



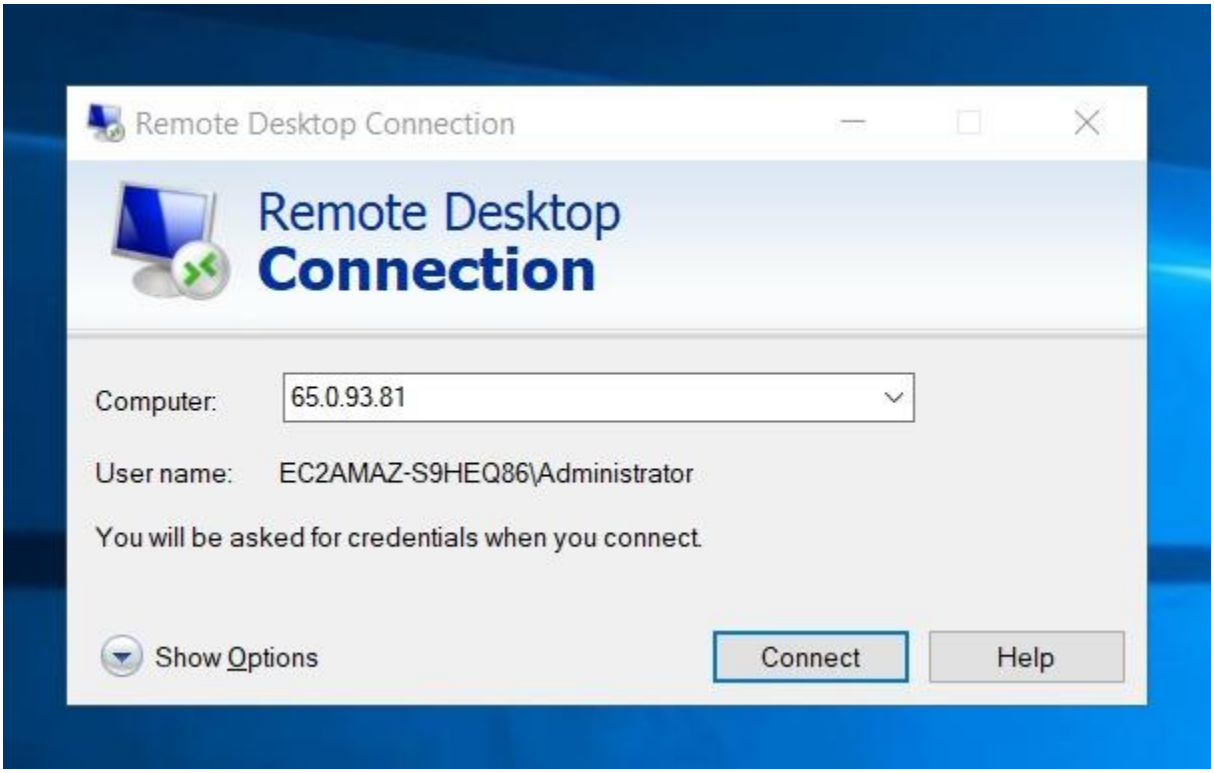
8) Now Create Another Windows Instance Using The Above Steps **(Windows-Server-2)**



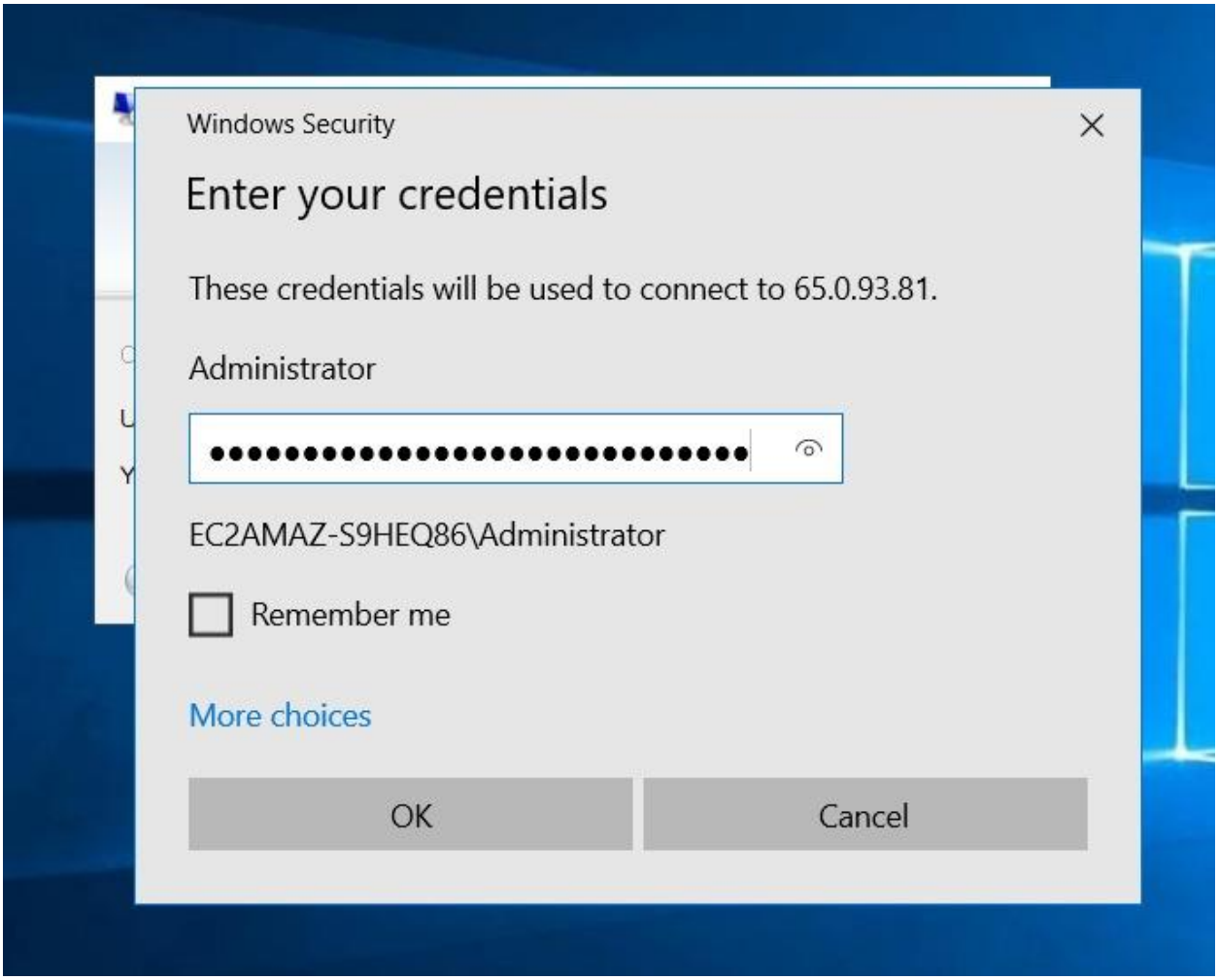
9) Now once the first instance**(Windows-Server-1)** is launched then type **"Remote Desktop Connection"** in Windows Seach Bar



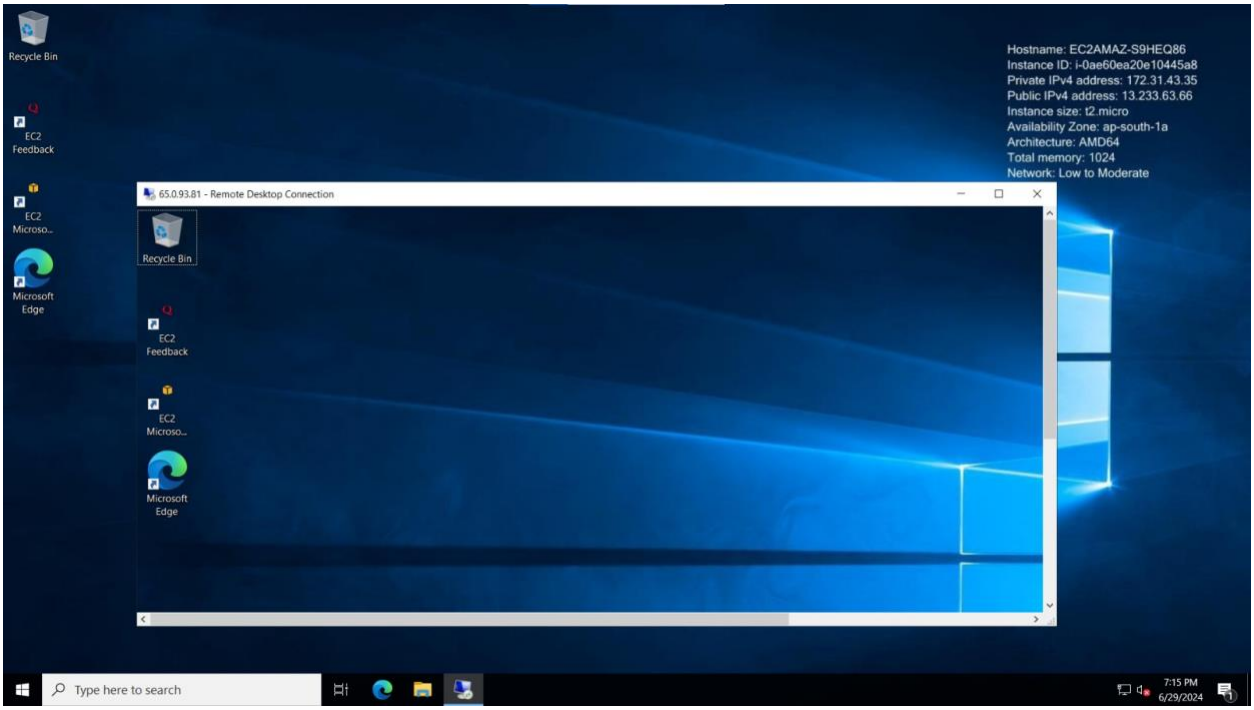
10) Now enter the Public IPv4 OR Public DNS of the Second Instance **(Windows-Server-2)** and click on **Connect**



11) Now Enter Username as **“Administrator”** and Password as your **decrypted .pem key** and click OK



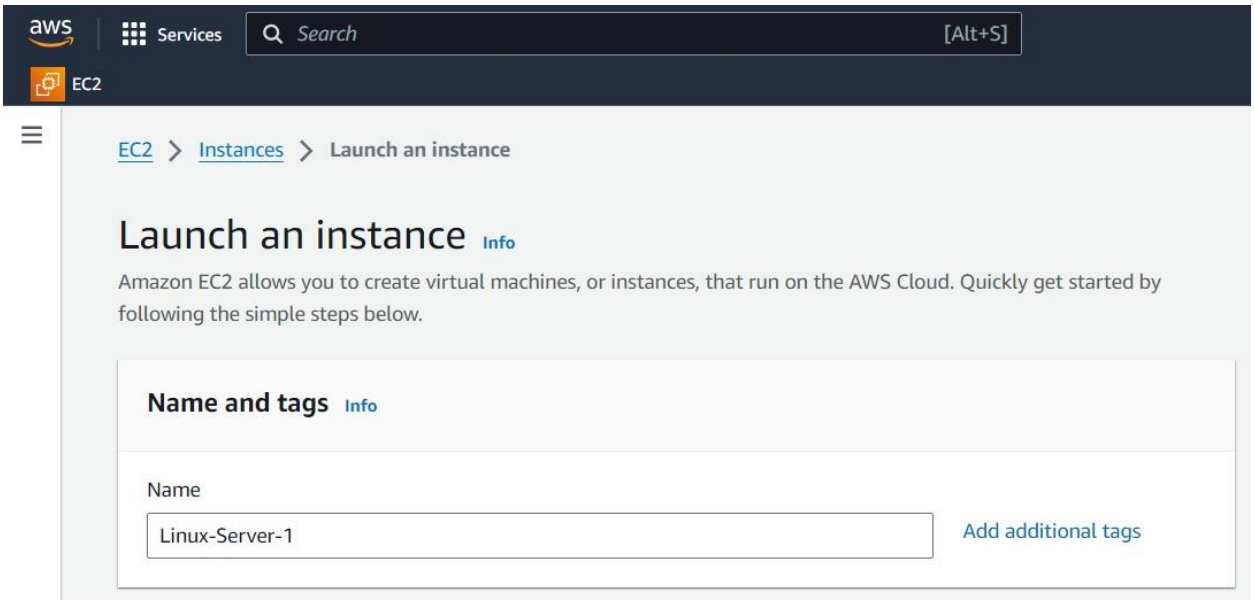
12)And Here is Your **Windows Instance** Inside **Another Windows Instance**



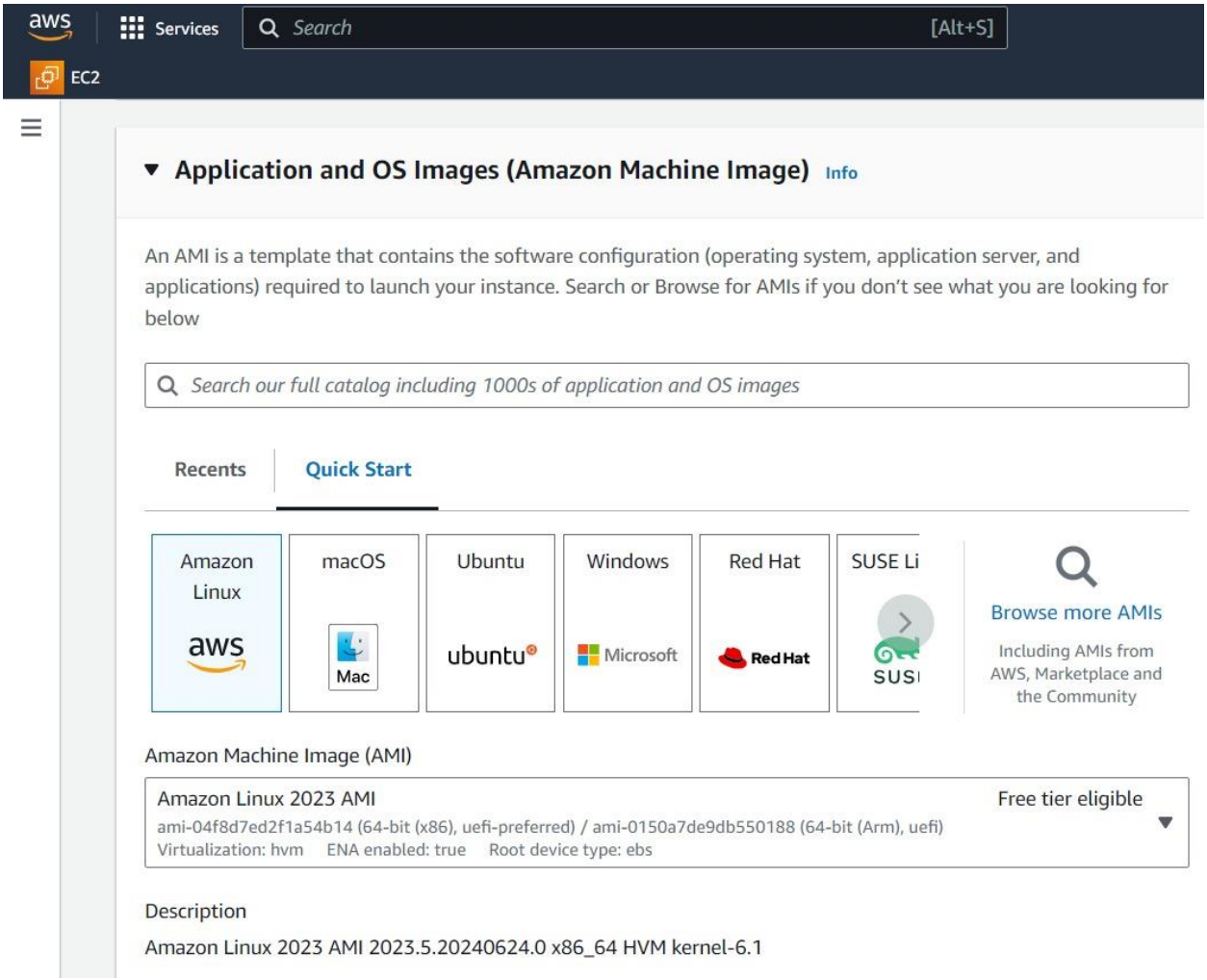
Aim: (B) Deploy a **Linux Instance** In **Another Linux Instance**

Steps:

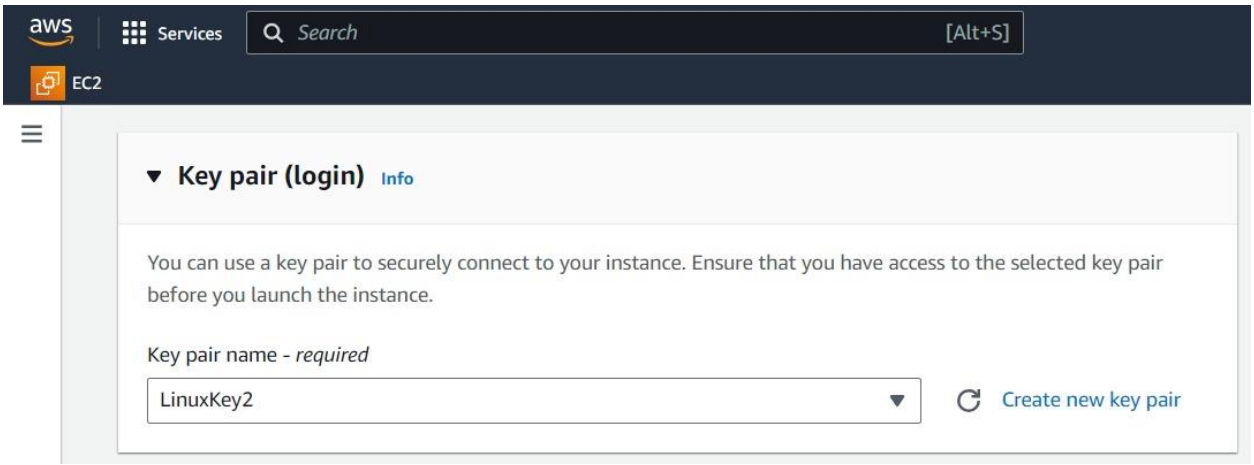
1) Create an linux instance on EC2 **(Linux-Server-1)**



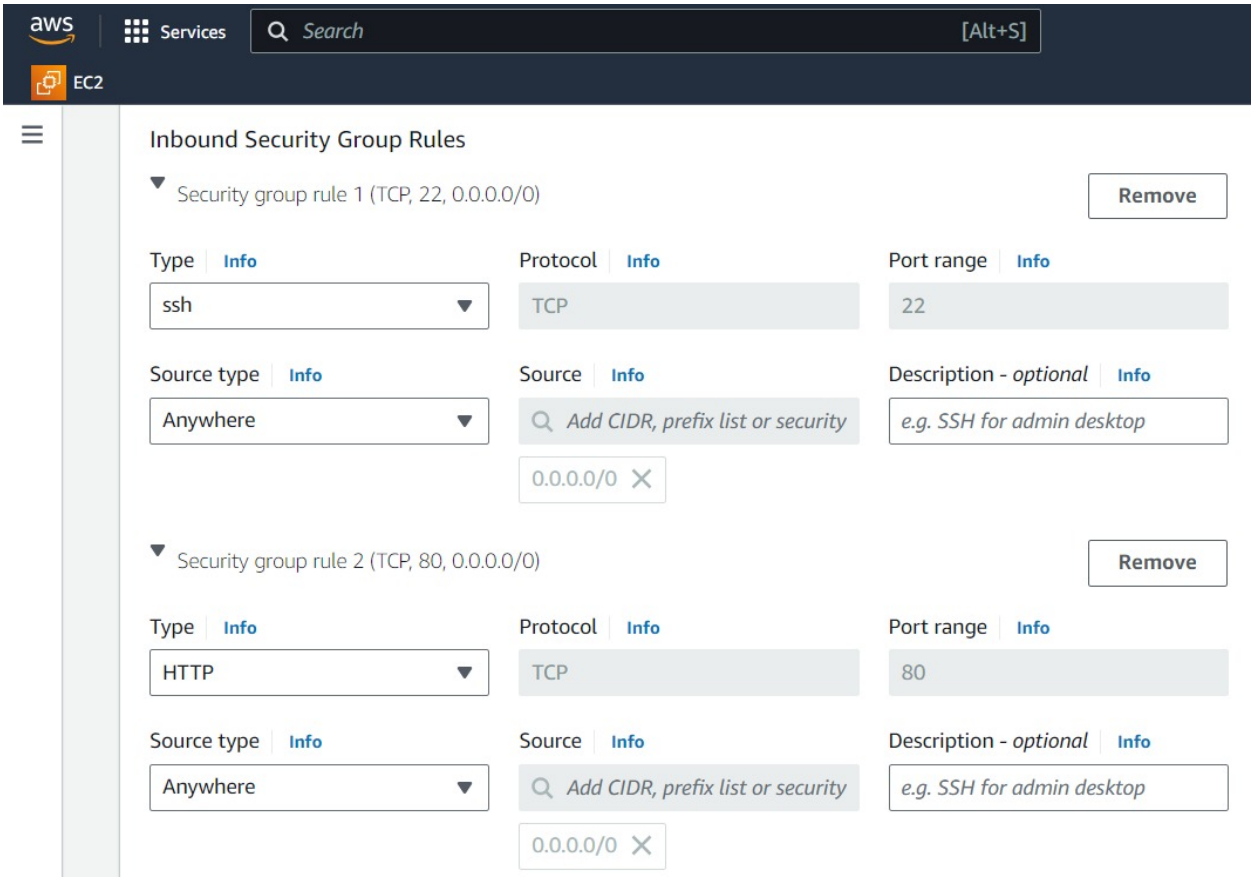
2) Select Amazon Machine Image (AMI) as Amazon Linux and Select Amazon Linux Server 2023



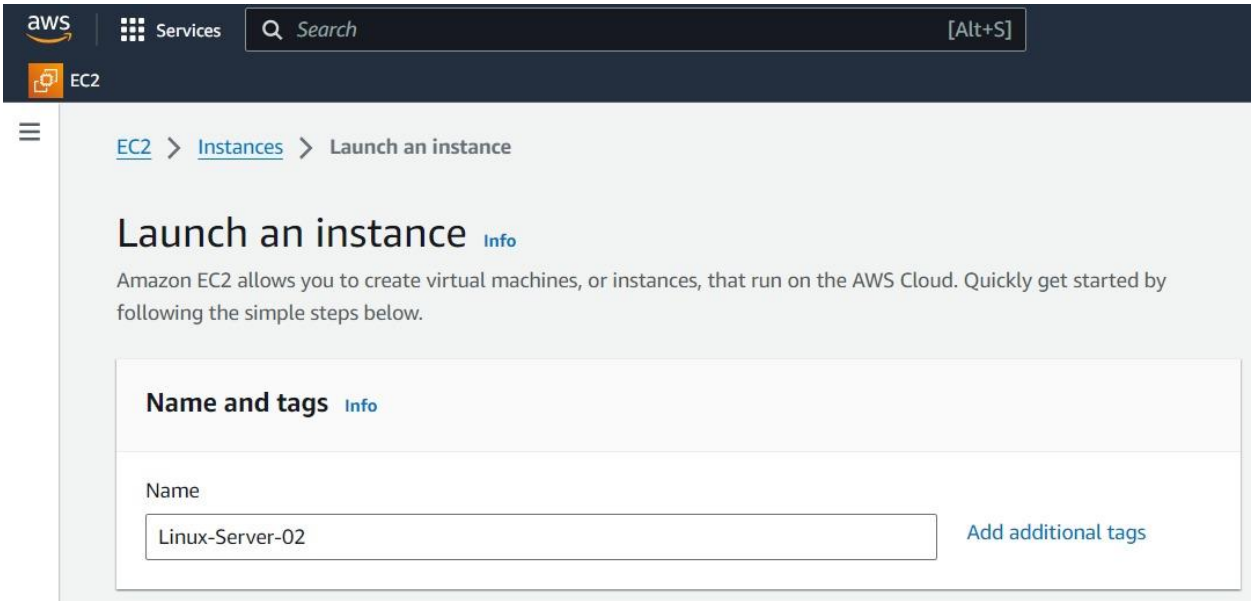
3) Create a Key Pair and Select It



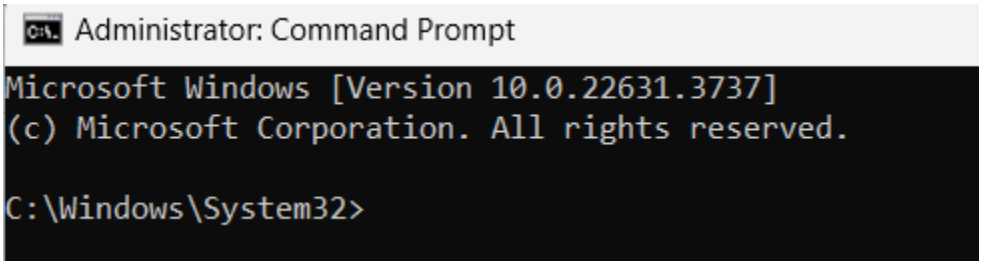
4) In Inbound Security Group Rules, Set Type To **“ssh”** and Source Type as “**Anywhere”** and Add New Security Group Set Type To **“http”** and Source Type as “**Anywhere”**



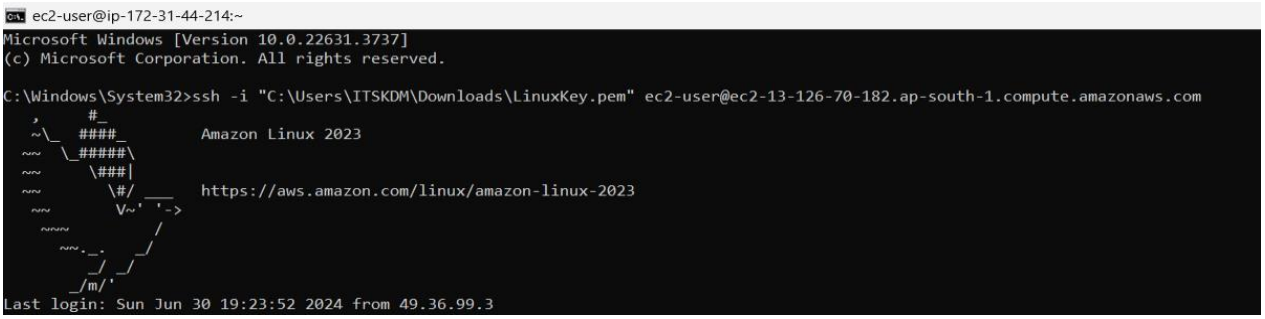
5) Now Launch This Instance **(Linux-Server-1)** and Create Another Linux Instance In EC2 **(Linux-Server-02)** following the above steps



6) Type **Command Prompt** and **Run as Administrator** on Your Local Computer



7) Now Run Your Linux Instance by Deploying it on Your **Command Prompt** by inserting the ssh client of the Public DNS with .pem key file location on your local computer



8) Now in this instance create a file using **touch** named as .pem key of your second instance and edit it file by using **vi** and paste the encrypted file contents in that file and close it and make sure to type command after editing the file [>**chmod 400 “filename”]** to ensure key is not publicly viewed

root@ip-172-31-47-231:/home/ec2-user


```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAoZFR0KA93MRemT6LqT8HEr0h37NAI1s+MTd9YCmCnzonv27l
DpcLRqTgd+9YauXvShuI5ryJ9m6ni812wKf7BIZ1H5GiNLY5FQHJvoXGthfx1jV7
66wPENXWw4e8fhg8qDhPsMk+AdaKEfmrVbFfOjQzFPN/yp0GVm00JxDZLbU4luJz
p7DDjUlkJ1KMdkjagB8A0UNz7qyfBxFdAn8xc2yWOX/69eV+bsowWcVsgdzR/TF+
JqZ4gsYa5GNxHE/T4UURZzWTmXIl6GyCSmM5LoSg7fqGjwShmcNrw3n9I1tyiADH
fPoofq9rGqJMcev8qbLw5+4VvXaRC9mU30hiCwIDAQABAoIBAFr9yZLyPATSPuiV
NfiKO4SNKb+fZvbCk0MKmjyHBD6CdRI19SCDZmFRx+0jyaridiJJYY95DUXRSeDN
RRz5PcBtrRarYSvImFtBV4pKMwAoehWGp5SxoQZ9N+eE0V4+biLbG95XZ+mHFtlK
v/iR3Syda0tYW1cTmhcgh2ec8ILxjVDVml44UsTSq8pcX7tTeJ/0HZGwnWj9S/8y
ogmIddgiEtv6RgwHSC0q1ELeYUT5AMRh0cia6h47rnHjAz2DvlEvrx0vADaofv1u
SB1iAyNMpGFdNl/JSs/o+0wPUASU7nMxjPIb555LbWoElzmSP2IHTbJ2vlj7T7IV
EG2jAdECgYEA8UQvOFzBGRNJaW3HkjlQSHR42ndaL+WC/14cADm5apXq9uu6W7Ag
b102b4Oh7FeLdPbKl9hbD9+i5anmHeP27NoXd9JXaGw7+kMsm7zS/hYW3sleypix
R/7rx317Jkwd1UcxgjGajrafYeduwg6+WH/eiI1K3X7lZ3vj7djnjDMCgYEAq28s
QY6gZQvhnAOHHtWfne5Kc9rtEOSD0bhvaAFqTXJlBLNT3zhcOFr8zXgPwoiBqtZK
OaN/ip2XE166E5CirLe/TxG4uboo3N/GBI9y+KWHY5d6Vt0ISqnRjOtxKhZNjYyb
I49o09PKgv/nHkg6jm5aN+owPkmciiLbuqmpeskCgYB5T/iSVYk+i4UZPvrfWnQ0
ymPOLb8qYDP7JZ3cuymxH0qy95qP6cKVXIA3mC9+ABL+L+10ZnR7Sc7FviUYGH0b
YRn1xMzwk6Og1dADSvGokwDS6tv/8MELW3HAsCaQ/iruB8ssFLcLVWZUuyLk7rbl
Fv6VGL5xGxJMc24LNUpQIwKBgGww7S0yZedfaDKdx1ieWO3CxRn4wEQ48zgXvbdV
rVDTMQ2WXwgw+YJXadQCQW/z1mGKe62EkalZa06+KZDPZtq52/J6rKoJ4mACmWWn
Ylepn5gqsPrA48q7AZR9wh1dlfQPGJmImA+XSecCuUlTLCFXY3iGQ4wLyM8k0Kct
C9iBAoGATLPaY6LgSVg886PBMAUqm/gOe4xZcG9s3uV0Wnga/TbxMbtGKx3Q6lZN
qh6xbz3iDp8PviYmaUpXd3Q06qPa7w9ECpKNYKNuEVwVgTWhp/dYg85TYBdPxSMZ
a+dBHV4KDvT3DooDhY2Qb3l8NtaYfT6MfmMTVlI0tnhS3QmesHo=
-----END RSA PRIVATE KEY-----
```

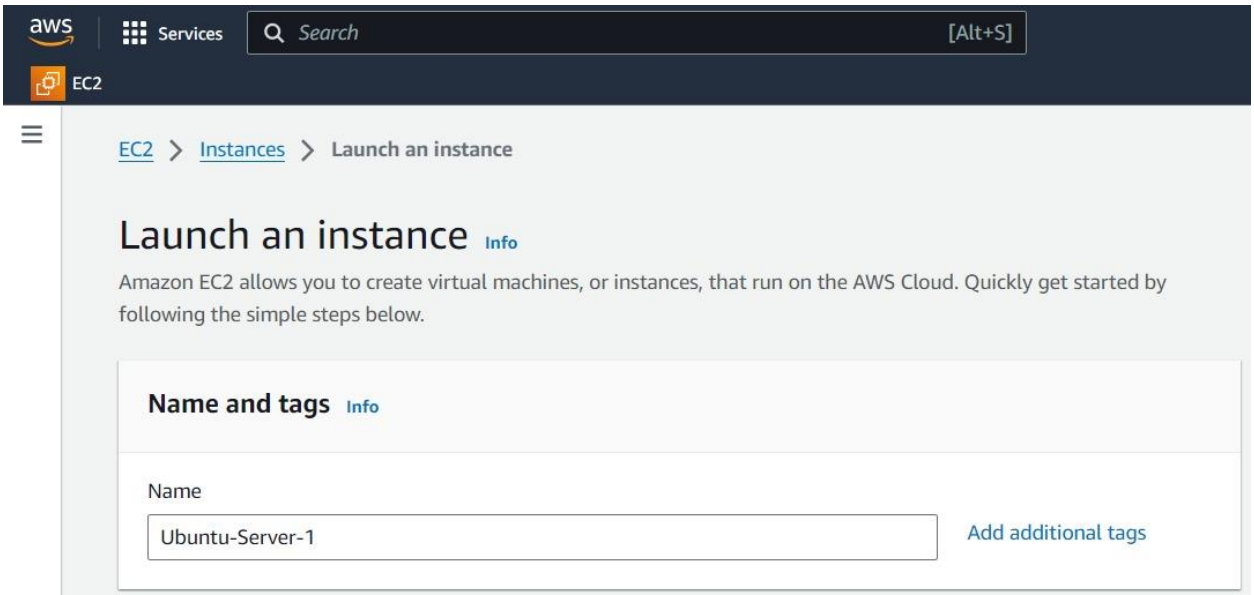
9) Now Run Your Second Linux Instance by Deploying it on Your **First Linux Instance** by inserting the ssh client of the Public DNS with .pem key file location on your instance computer and that's your Linux Instance Inside Another Linux Instance

```
ec2-user@ip-172-31-44-214:~
Microsoft Windows [Version 10.0.22631.3737]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>ssh -i "C:\Users\ITSKDM\Downloads\LinuxKey.pem" ec2-user@ec2-13-126-70-182.ap-south-1.compute.amazonaws.com
       #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Sun Jun 30 19:23:52 2024 from 49.36.99.3
[ec2-user@ip-172-31-47-231 ~]$ sudo su
[root@ip-172-31-47-231 ec2-user]# pwd
/home/ec2-user
[root@ip-172-31-47-231 ec2-user]# touch LinuxKey2.pem
[root@ip-172-31-47-231 ec2-user]# vi LinuxKey2.pem
[root@ip-172-31-47-231 ec2-user]# chmod 400 "LinuxKey2.pem"
[root@ip-172-31-47-231 ec2-user]# ssh -i "/home/ec2-user/LinuxKey2.pem" ec2-user@ec2-43-205-115-60.ap-south-1.compute.amazonaws.com
The authenticity of host 'ec2-43-205-115-60.ap-south-1.compute.amazonaws.com (172.31.44.214)' can't be established.
ED25519 key fingerprint is SHA256:I8ODQMMtXIGfgy2YA2d/+AYsK6jrg06QEPr3tqAfrGg.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-43-205-115-60.ap-south-1.compute.amazonaws.com' (ED25519) to the list of known hosts.
       #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-172-31-44-214 ~]$
```

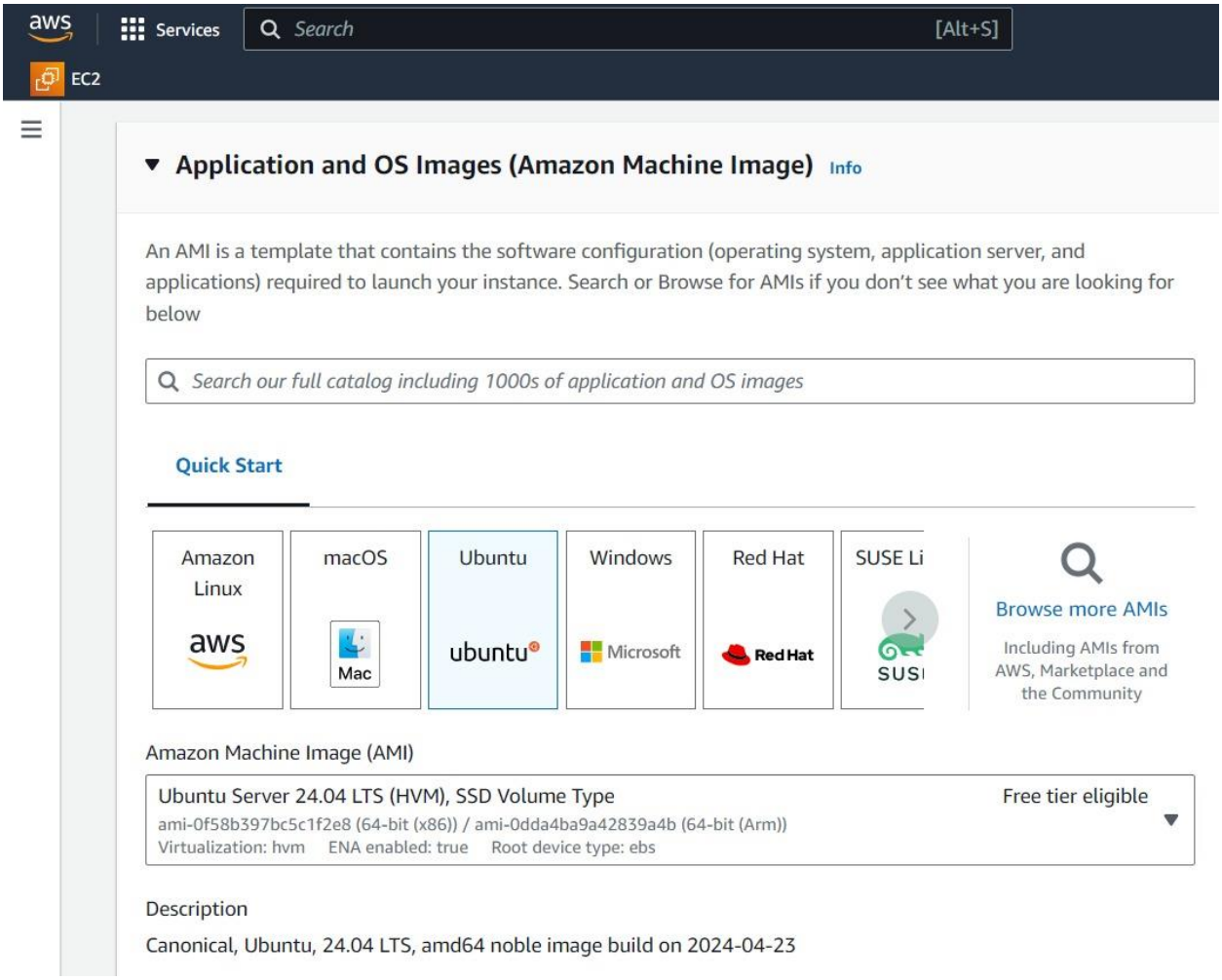
Aim: (C) Deploy a **Ubuntu Instance** In **Another Ubuntu Instance**

Steps:

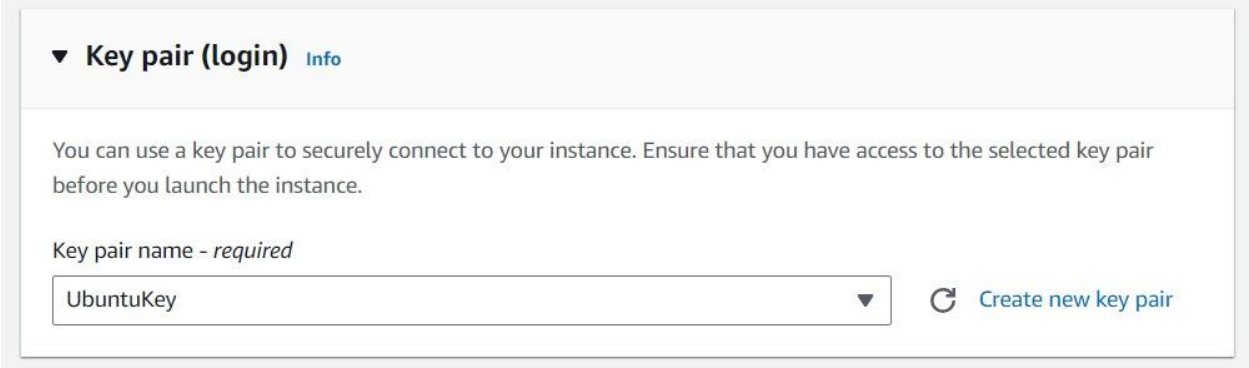
1) Create an ubuntu instance on EC2 **(Ubuntu-Server-1)**



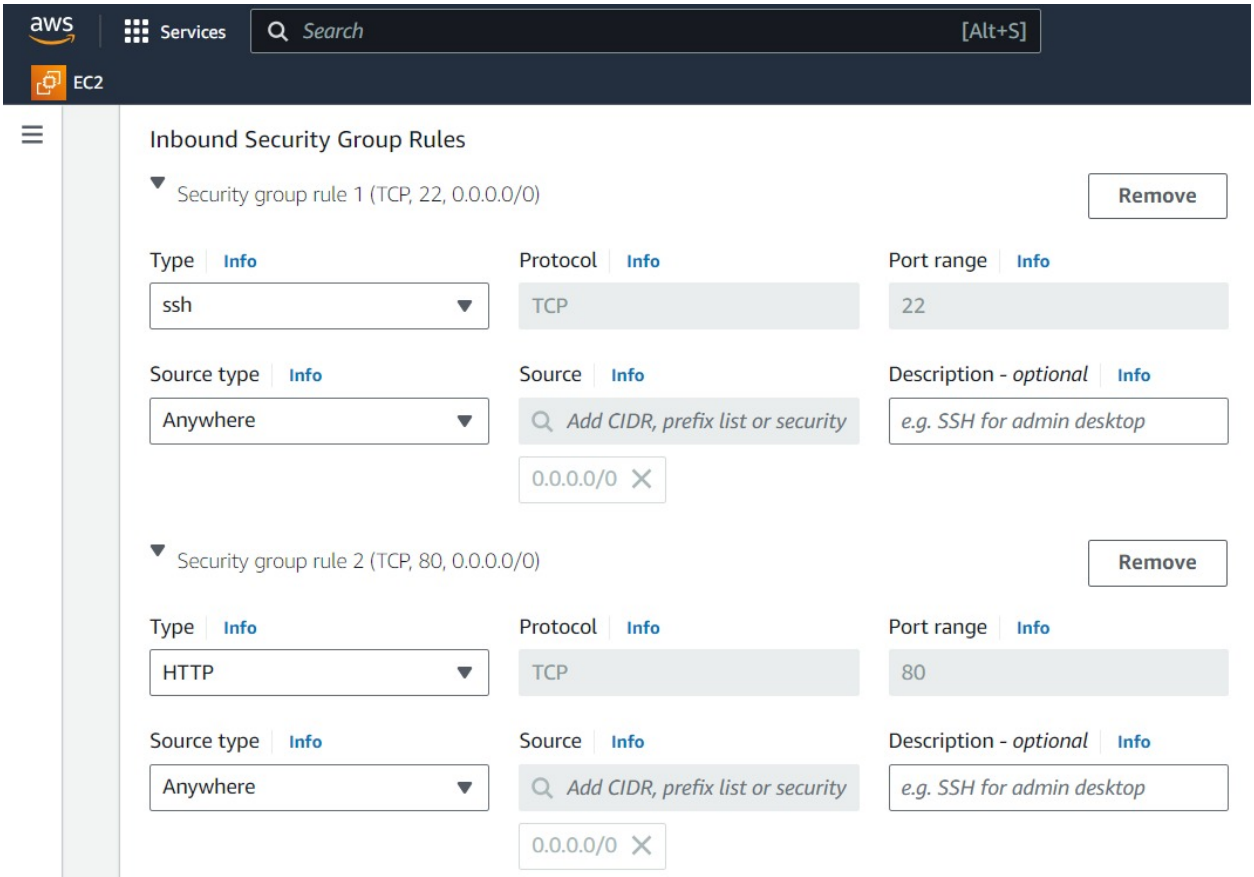
2) Select Amazon Machine Image (AMI) as Ubuntu and Select Ubuntu Server 24.04 LTS



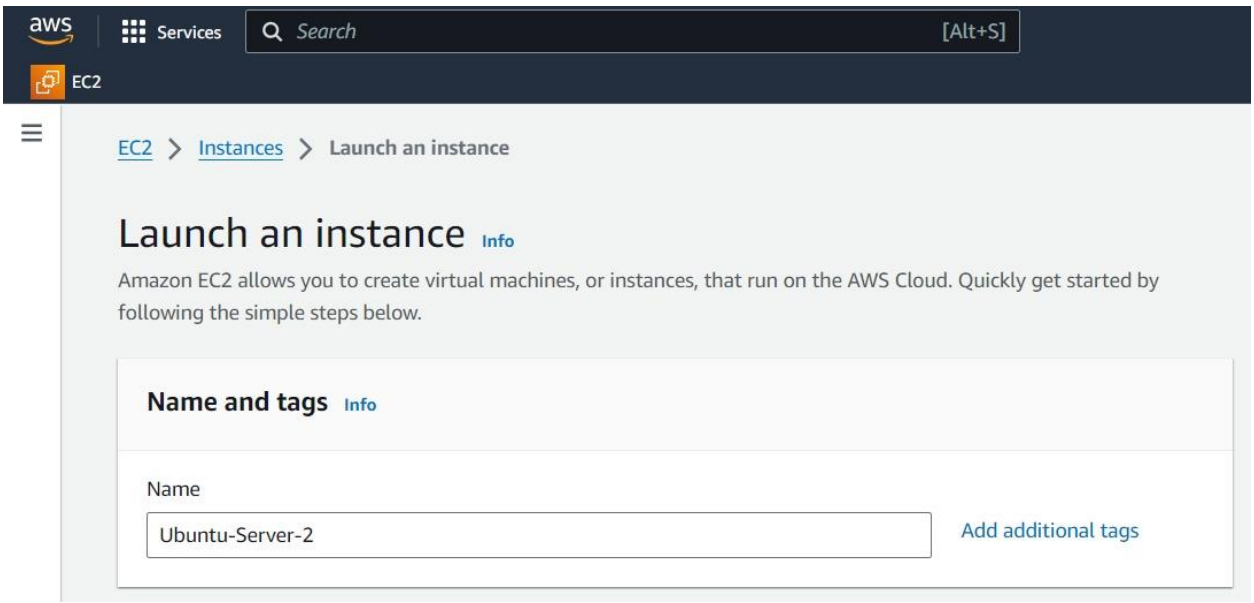
3) Create a Key Pair and Select It



4) In Inbound Security Group Rules, Set Type To **“ssh”** and Source Type as “**Anywhere”** and Add New Security Group Set Type To **“http”** and Source Type as “**Anywhere”**



5) Now Launch This Instance **(Ubuntu-Server-1)** and Create Another Instance In EC2 **(Ubuntu-Server-2)** following the above steps



6) Type **Command Prompt** and **Run as Administrator** on Your Local Computer

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.22631.3737]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>
```

7) Now Run Your Linux Instance by Deploying it on Your **Command Prompt** by inserting the ssh client of the Public DNS with .pem key file location on your local computer

```
Select ubuntu@ip-172-31-45-126: ~
Microsoft Windows [Version 10.0.22631.3737]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>ssh -i "C:\Users\ITSKDM\Downloads\UbuntuKey.pem" ubuntu@ec2-13-126-43-39.ap-south-1.compute.amazonaws.com
The authenticity of host 'ec2-13-126-43-39.ap-south-1.compute.amazonaws.com (13.126.43.39)' can't be established.
ED25519 key fingerprint is SHA256:6BMRbT4sRzkHMjbn0KnN33s66VnAejQpf6YlZIZMrQQ.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-13-126-43-39.ap-south-1.compute.amazonaws.com' (ED25519) to the list of known hosts.
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-1008-aws x86_64)

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

 System information as of Sun Jun 30 20:13:32 UTC 2024

  System load:  0.07              Processes:             108
  Usage of /:   23.2% of 6.71GB   Users logged in:       0
  Memory usage: 20%               IPv4 address for enX0: 172.31.34.227
  Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

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

ubuntu@ip-172-31-34-227:~$ sudo su
```

8) Now in this instance create a file using **touch** named as .pem key of your second instance and edit it file by using **vi** and paste the encrypted file contents in that file and close it and make sure to type command after editing the file [>**chmod 400 “filename”]** to ensure key is not publicly viewed

```
ubuntu@ip-172-31-34-227:~$ sudo su
root@ip-172-31-34-227:/home/ubuntu# touch UbuntuKey.pem
root@ip-172-31-34-227:/home/ubuntu# vi UbuntuKey.pem
root@ip-172-31-34-227:/home/ubuntu# root@ip-172-31-34-227:/home/ubuntu# chmod 400 "UbuntuKey.pem"
root@ip-172-31-34-227:/home/ubuntu# pwd
```

root@ip-172-31-34-227: /home/ubuntu


```
-----BEGIN RSA PRIVATE KEY-----
MIIEoQIBAAKCAQEAhRVRoAMpzTbdg6UICr5bqeqmSROvpDjpXa4QMM610aEKewqi
9rUoFDiqJFifLVuE79PcPL7+qoukOVxfzhmBHcTNJnzmoyJZ0YLk52T5p4J0+ybP
EUXtgzHu2AzyKZhbDMCv4bzRZi8t8GRLY+36zZgvsg831qKH3mTOeh1L+Oqzj+rt
OfHrYCCCGQSjzuxWe9fFKW/yx2qg7uaYHefNdq+bYaZoJ9KyvWb6EYAb/R3cQjdq
W00r7PZL4VqstLOb/raEHCVWVNAgU8AxG9fjzIPB3qbdSdeInj9nZTPHg7TW8xS4
hLhXf9UClWAV7zYFXac9gWnilZ0vEytbjZJ2QwIDAQABAoIBAF8EPJX5DDRXUsp1
3osFJB7pyLVuF74xX/ShnS+rtkaoKvp0OqvX5XiiiF+Q4n0Y1Y4BfkHkv6B2ONc3
a7OTpArkAvDSxjx8/xHF2baX8mM1kl3qdHbJrW05DmU0wQUPoRo2zJxoGj1RvAPh
J65+L83wNUV09hIJUuZmpMCtABwENQIVpSFKM2Ok4+Y/ULKa5MVvnWJAc1hOg6aY
OAQTFXxikMg5CNXHdRV20FYYzfokj/jPV9As7HLhCv/l3JXIWir16hvBM02cCb35
gUwstPvYl/ThtNFq9cjgh0yd/EuLoueJsJAzRxW0sasfaoPKX35PcT2XHFyaOzBA
hpxSRxkCgYEAzWfZzFV7ACd1Sv7Jg/eeBU0C3b5KbLhp80ztn7no6FDNYWafPVFR
ZcXYdKhWd8PeAJOVmybQ4Viup/65m05T601X6h4a/s5SJeDFpuhyvHOMstozQwHD
JxMW16qe73wVXp95b3uZDWBb4S2nsTHi6czm/bf6111OTC2zd9iv980CgYEApd0T
b6Zat4UcKfXFJonEBs51/0SZDIeQvpZQc08eBddHkqs7gmeMfs88KOONHgiID2NJ
jRKSRVxfgYV5Dg2yq9UwSbi8Xe7fwxTGeDPVMj41QtfGrvvRkmVxtadqGpPqCgcK
TLJJAsjtK9hX23ZMh6IRRhFKLff93vAmSGG+9k8CgYAsW7YMS5WBhgPtizJnnmzw
xh3NV0/pRLYUxdM3QEXNDc4cr7XJ3yrN6LkDEGuD97eUtkqDtBE96RHm07qvkG3N
DenjdFbuGg5hgbYNgntsuSN0aGzTlqjXYmb3cjBalZhj09q8uZtm6R1OdraVLKnN
RePIfRfdtJe5GdF9Gz19LQJ/G9wGZ7qJgknZcTLW6qI5Suti5n2fN3uN1HVrDfM8
F78RRpF8bWr3LlWgxT1zdpf4Qp1qvUdhSkU5xYelzbZ/TF2Cvt9IxH5bF2ll7MrI
BKhuScv0k2+4w95GOzzjlZNCvGxyTm+j09PsAnFUUIiOUjnmrN46l34QJmIwC/hf
GwKBgQCnbDNHiO0gCJWniYmnaIKdm4d3XP+nWwIZg5QzgAkRsxT5s/Vo1wUuD0it
w+PgdViTz6UJ252hw1II5TC30bSyHydyWSKnNgxu1pGeg8JrwgbxwHBnQVEQog8S
tep4sQCknGUFrXtmwWljQqNrngjvpFTsqBfrm+qsgAfH9246dw==
-----END RSA PRIVATE KEY-----
```

9) Now Run Your Second Ubuntu Instance by Deploying it on Your **First Ubuntu Instance** by inserting the ssh client of the Public DNS with .pem key file location on your instance computer and that's your Ubuntu Instance Inside Another Ubuntu Instanc

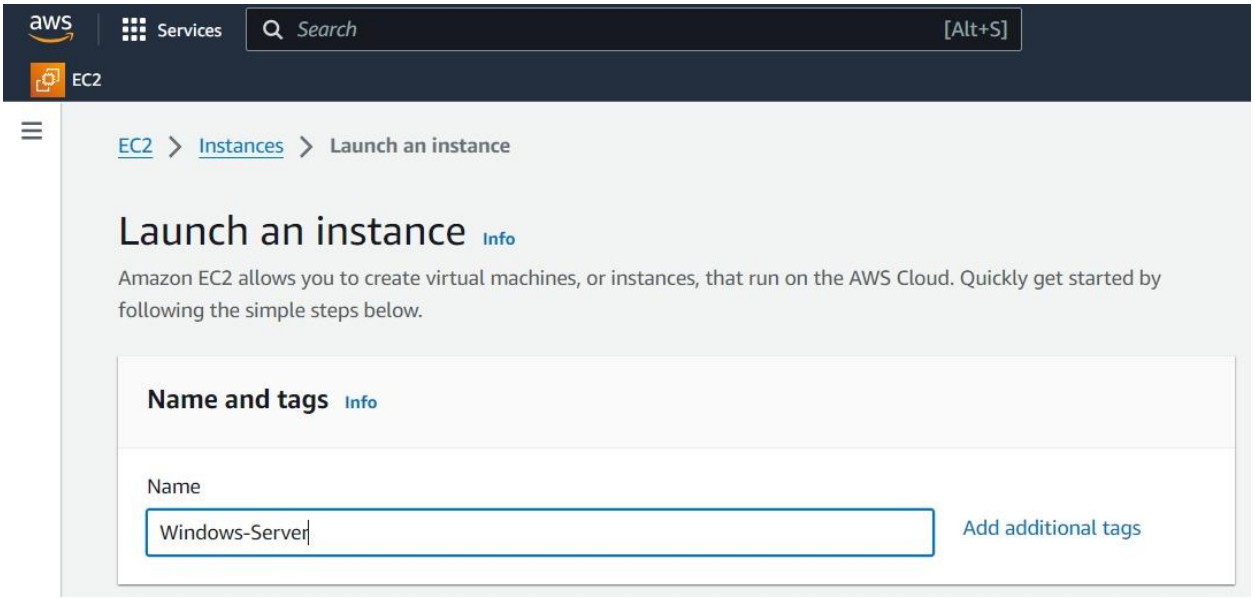
Select ubuntu@ip-172-31-45-126: ~

```
/home/ubuntu
root@ip-172-31-34-227:/home/ubuntu# ssh -i "/home/ubuntu/UbuntuKey.pem" ubuntu@ec2-13-127-35-53.ap-south-1.compute.amazonaws.com
The authenticity of host 'ec2-13-127-35-53.ap-south-1.compute.amazonaws.com (172.31.45.126)' can't be established.
ED25519 key fingerprint is SHA256:9gyujDEQvcICFKx7ZQRW/cWsUguMctqZ0G9cA8yw1oI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-13-127-35-53.ap-south-1.compute.amazonaws.com' (ED25519) to the list of known hosts.
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-1008-aws x86_64)

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

 System information as of Sun Jun 30 20:18:29 UTC 2024

  System load:  0.0               Processes:             104
  Usage of /:   23.2% of 6.71GB   Users logged in:       0
  Memory usage: 19%               IPv4 address for enX0: 172.31.45.126
  Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

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

ubuntu@ip-172-31-45-126:~$
```

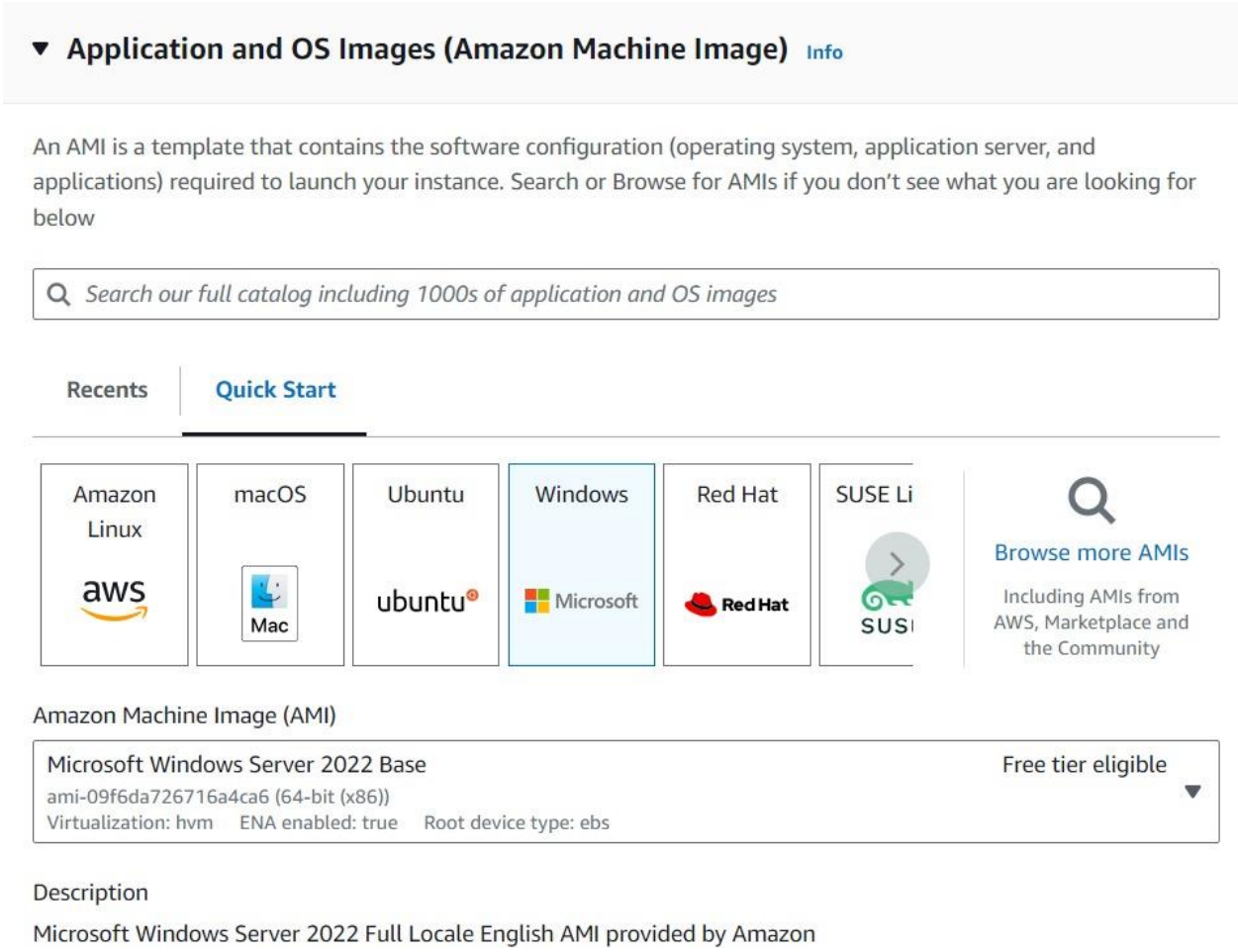
Aim: (D) Deploy a **Linux Instance** In **Windows Instance**

Steps:

1) Create an windows instance on EC2 **(Windows-Server)**

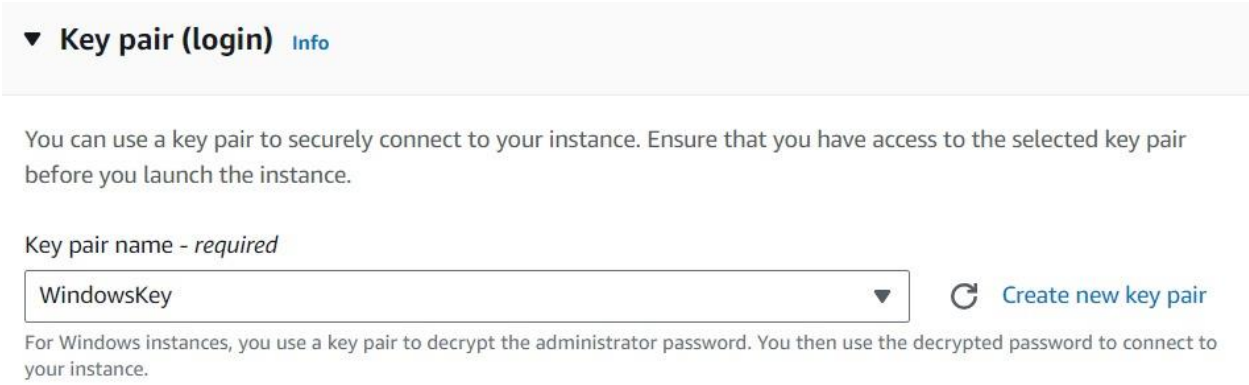


2) Select Amazon Machine Image (AMI) as Windows and Select Windows Server Base 2016 or Later

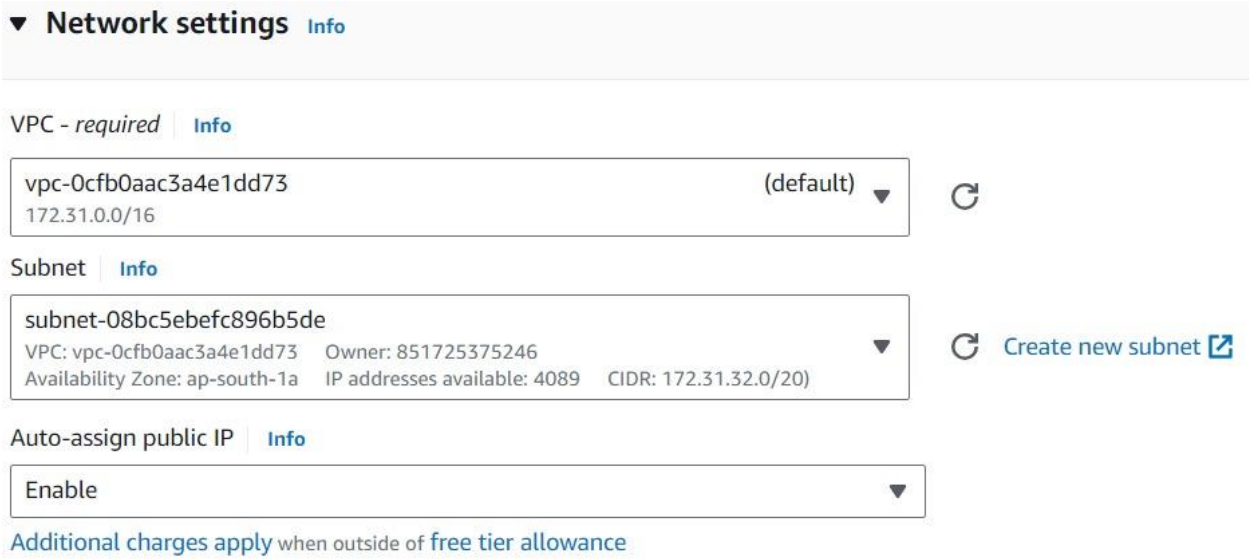


3) Choose Instance Type As Per Your Requirements

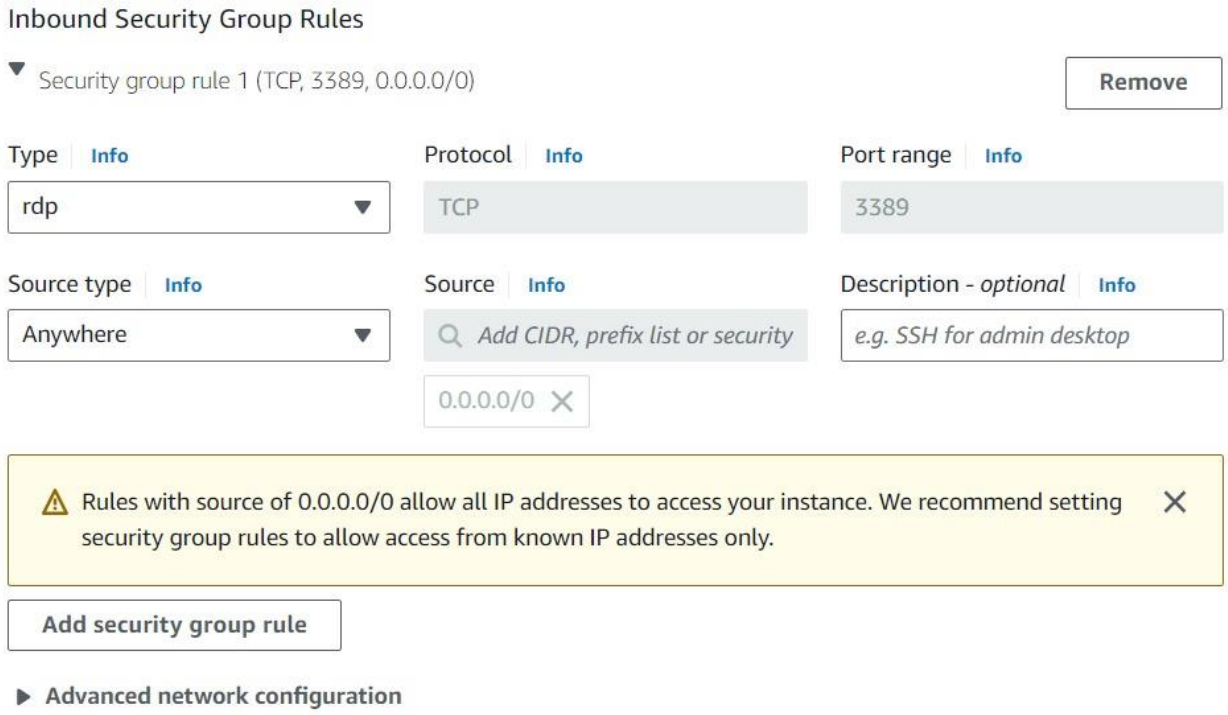
4) Create a Key Pair and Select It



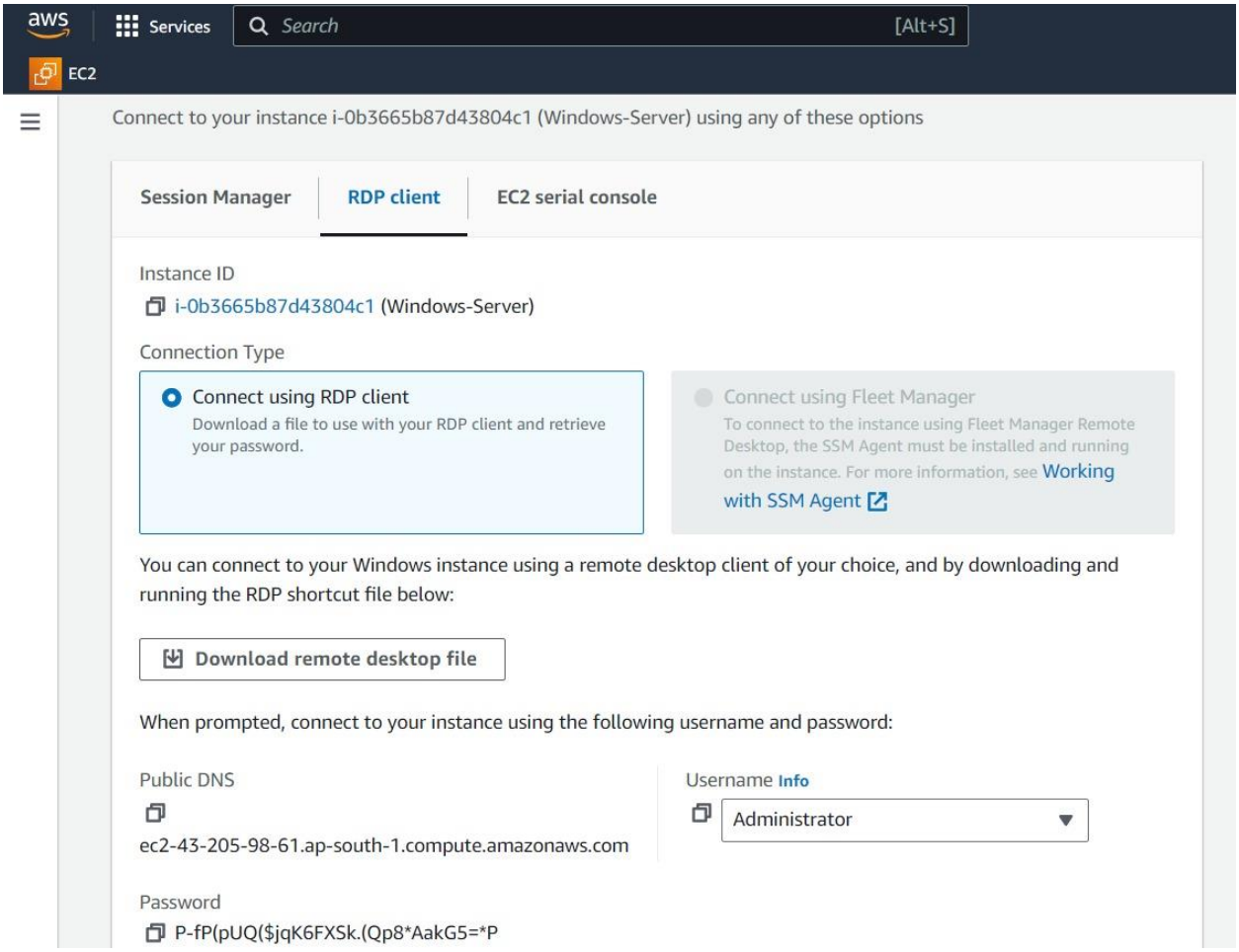
5) Edit Network Settings And Select Subnet : ap-south-1a OR ap-south-1b



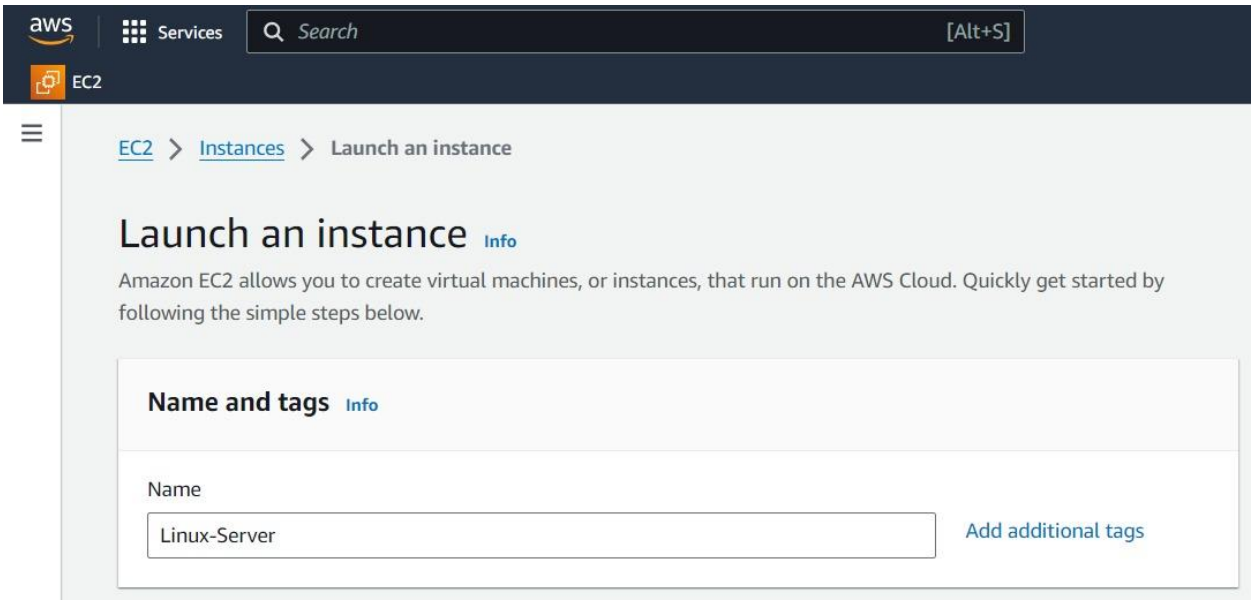
6) In Inbound Security Group Rules, Set Type To **“rdp”** and Source Type as “**Anywhere”**



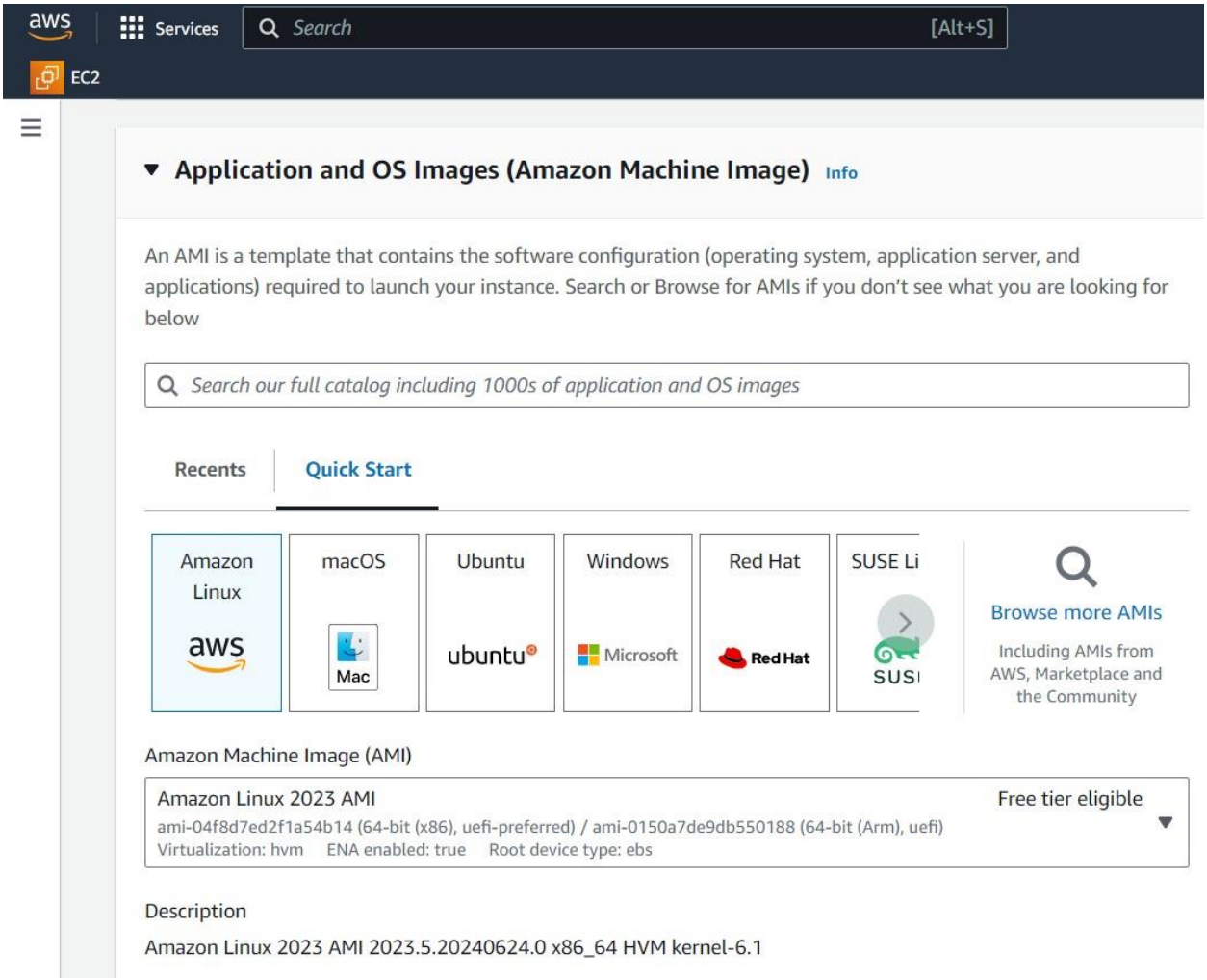
7) Get password from the created .pem key and use it to connect the rdp file and launch the Windows Instance



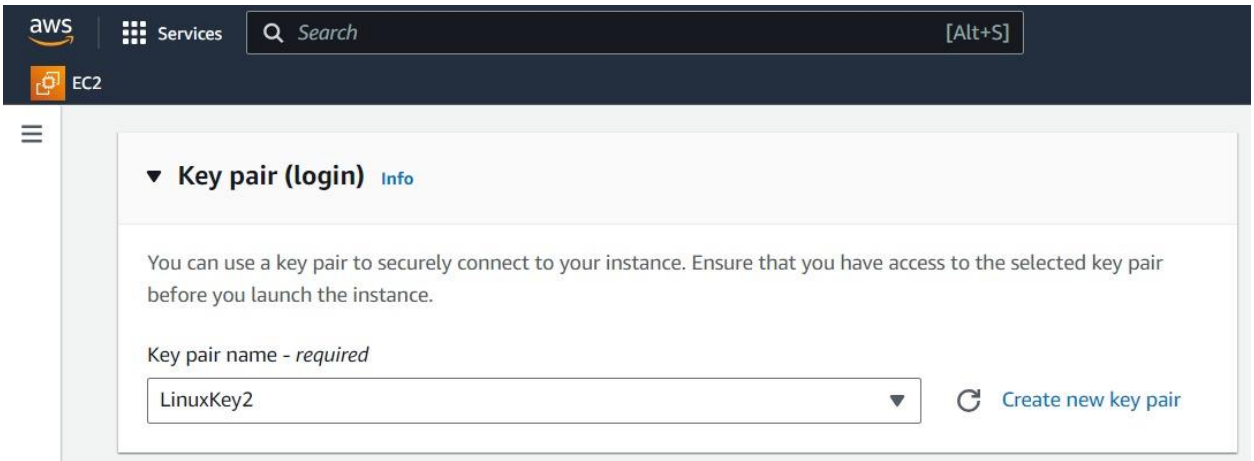
8) Now create a linux instance **(Linux-Server)**



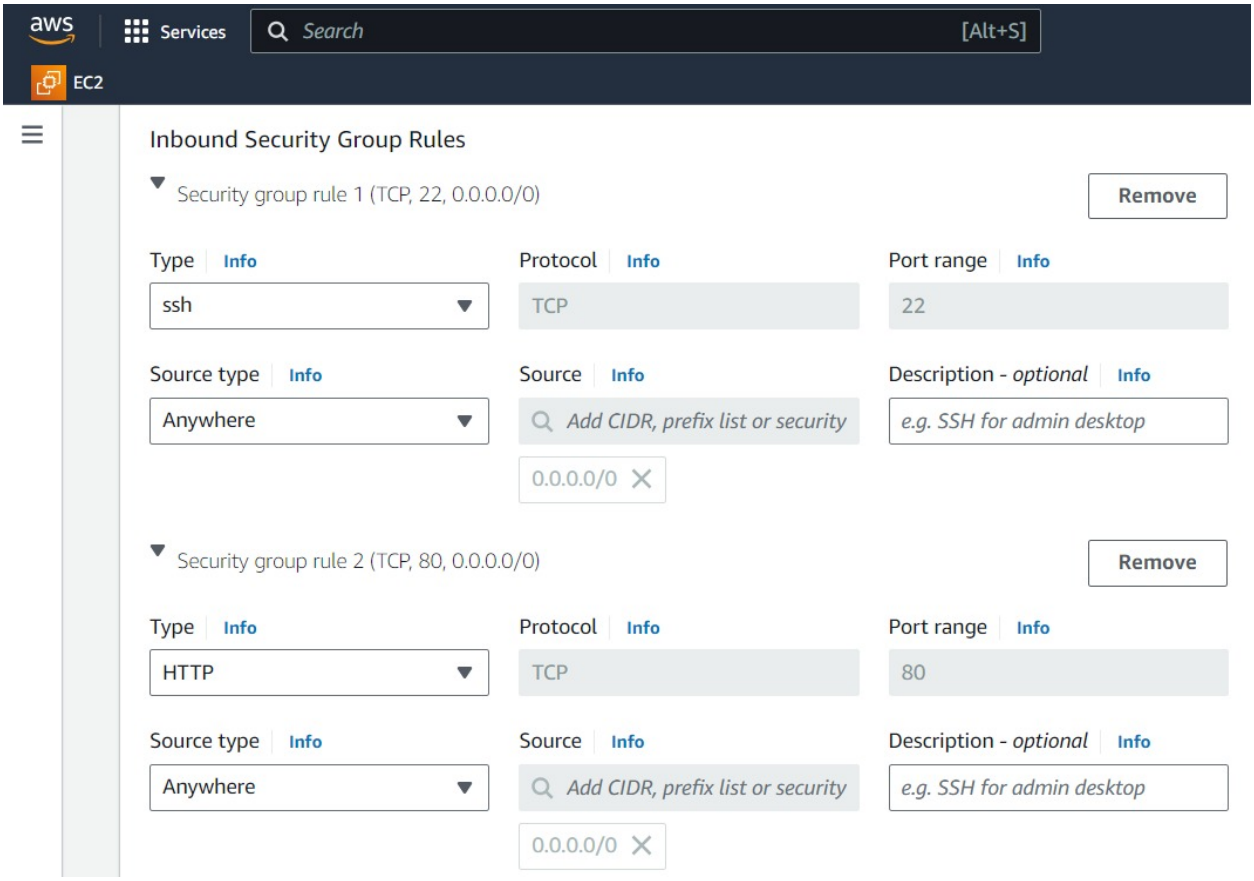
9) Select Amazon Machine Image (AMI) as Amazon Linux and Select Amazon Linux Server 2023



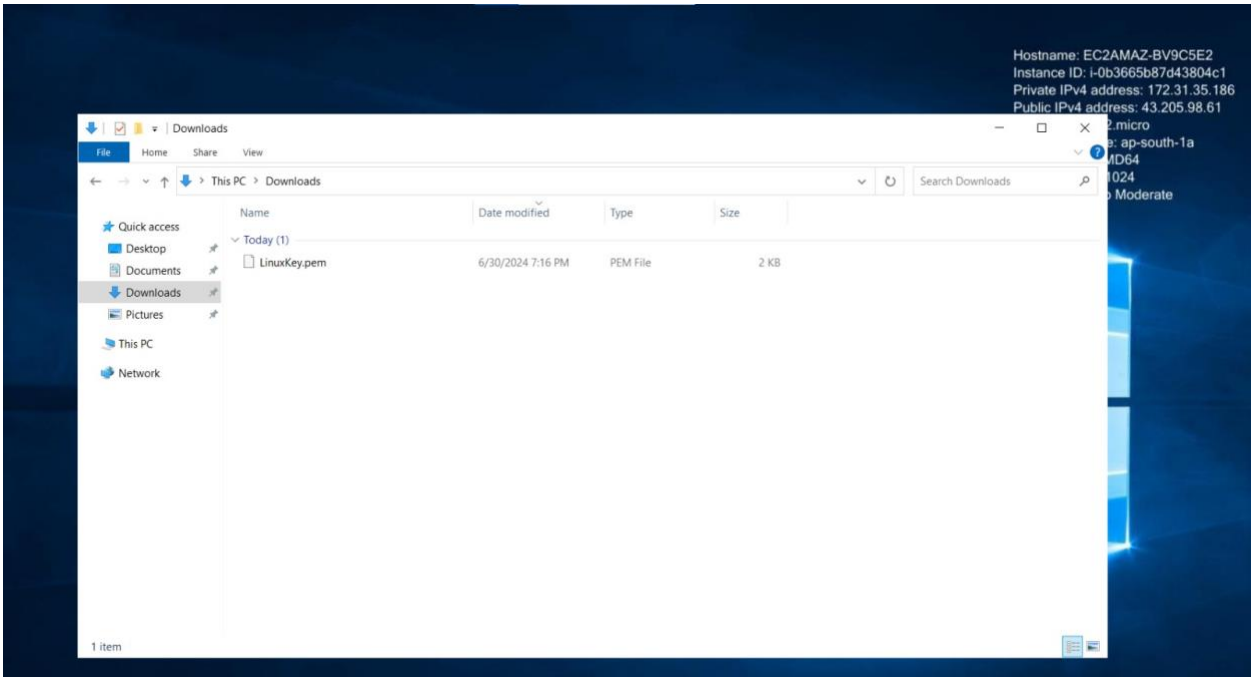
10) Create a Key Pair and Select It



11) In Inbound Security Group Rules, Set Type To **“ssh”** and Source Type as “**Anywhere”** and Add New Security Group Set Type To **“http”** and Source Type as “**Anywhere”** and Launch the instance.



12) Now Open The Windows Instance and Paste the .pem key of The Linux Instance



13) Now open command prompt in the Windows Instance and Change the directory where the .pem key is saved and Now Run Your **Linux Instance** by Deploying it on Your **Windows Instance** by inserting the ssh client of the Public DNS with .pem key file location on your instance computer and that's your Linux Instance Inside a Windows Instance.