Andhra Pradesh State Skill Development Corporation

Skill AP
APSSDC

Skill AP
Learn Anytime Anywhere
Andhra Pradesh State Skill Development Corporation

AWS CLOUD COMPUTING

CONFIGURATION OF THE PUBLIC SUBNET

Configuration of the Public Subnet

Public Subnet

Instances in Public Subnet can be accessible From the Internet, which means traffic From the Internet can hit a machine/Instance/Service in Public Subnet. You normally keep things like Load Balancers, Web Servers in Public Subnet. So when you create them, you add name Public in front of them to keep them separate from others and, it doesn't matter you enabled Auto-assign Public IPv4, but every time you choose the Public Subnet that you marked Public, you have to check or enable Auto-assign Public IPv4 option when you launch an instance of EC2 or RDS/Service. But it's better if you enable Auto-assign Public IPv4 and Subnet level to make it properly Public because this is the reason you are making difference and using Public-Private concept, so whenever you launch any service/Instance/machine in Public Subnet, it will be able to accessible From the Internet and To the Internet, means, You can hit the service/Instance over the Internet and can download updates and packages in the service/Instance as well.

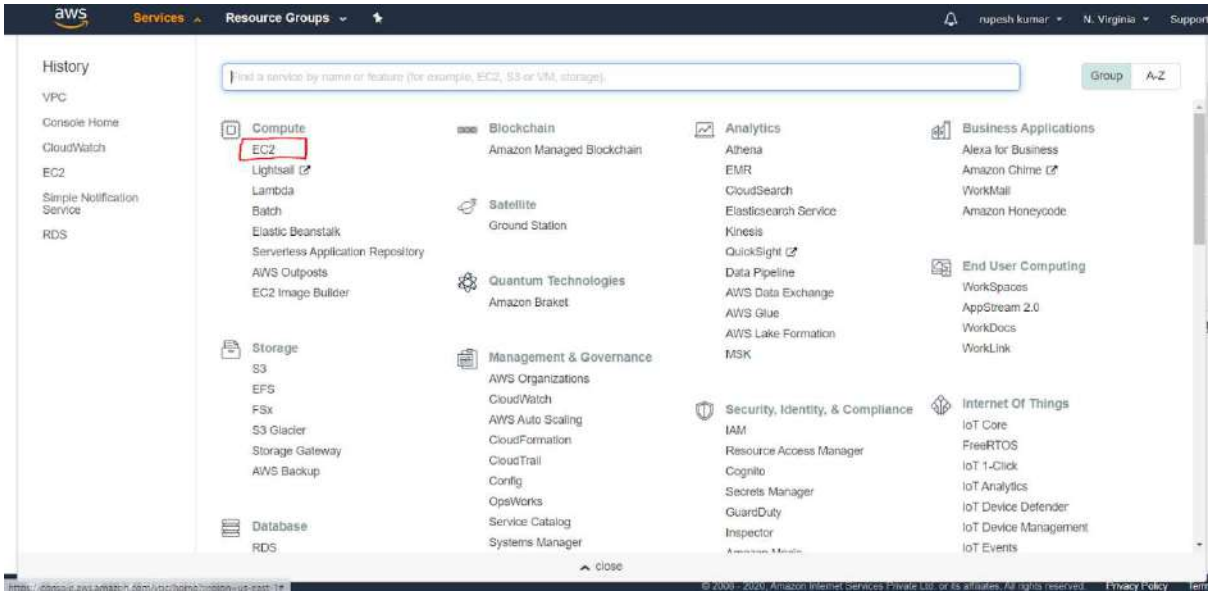
Private Subnet

Instances in Private Subnet cannot be accessible From the Internet. E.g. you can put Database Server, Redis Server or these kinds of other services in a Private Subnet and no one can access it From the Internet. It would be accessible only via Instances/machines/Services in Public Subnet (Web server, ELB, etc). Because it doesn't have a Public IP enabled option and also, we marked it as Private for the specific use as explained, for security and unwanted access over the Internet. This is good for architecture level security to avoid loopholes. To access this Private Subnet services/Instances, you have to add allow rule in Security group and add proper routes in the route table.

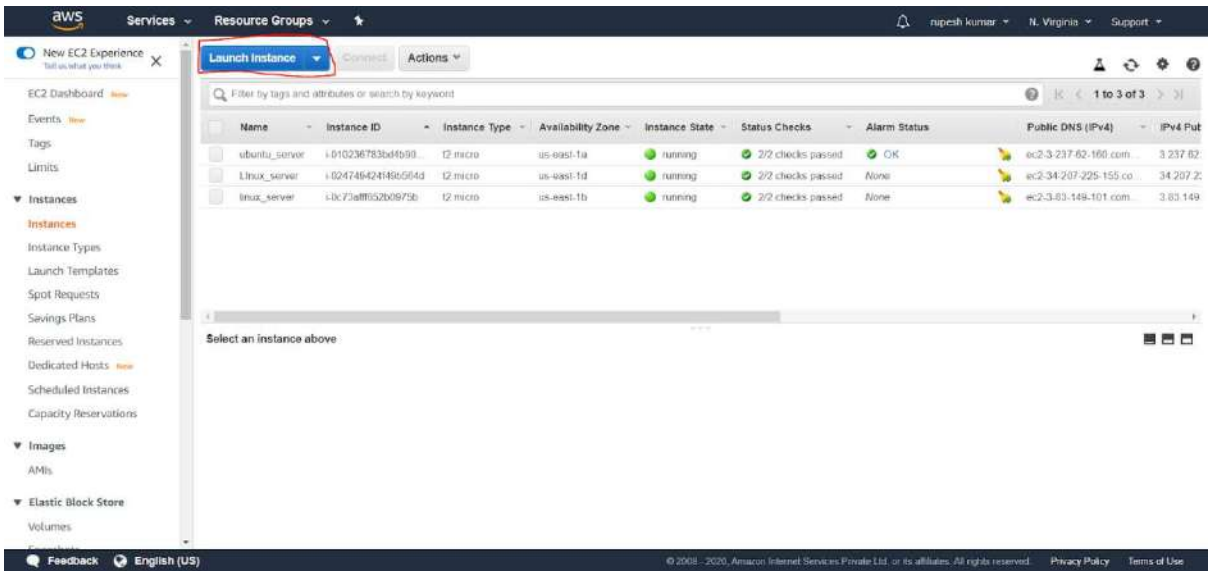
To Connect Linux Instance in Public Subnet

Launch Linux instance in public subnet → Example_pub_subnet

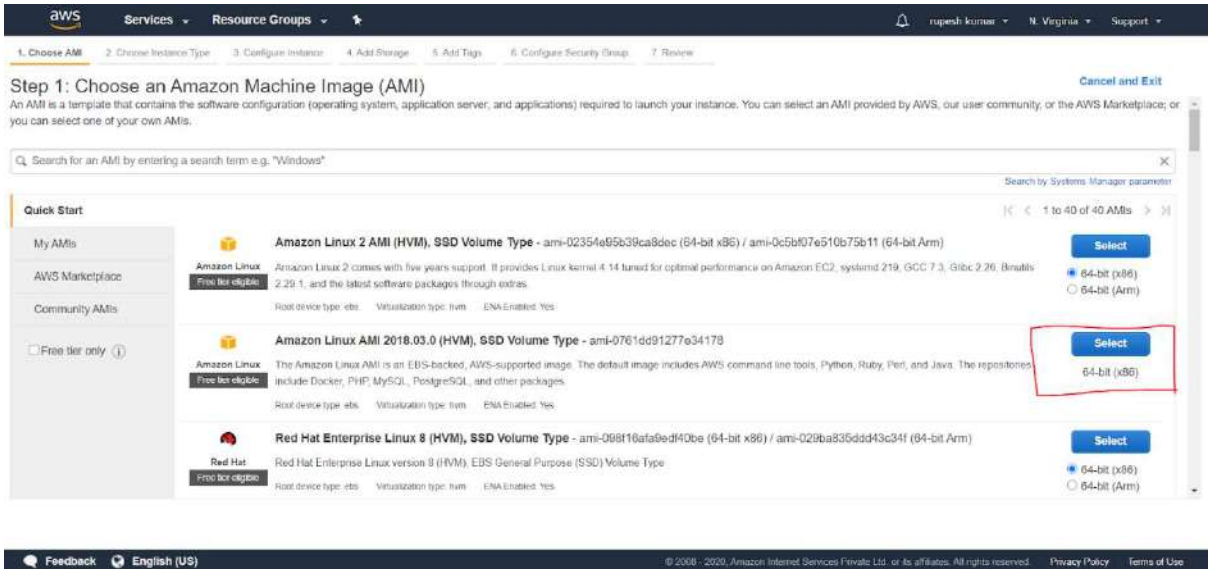
Open the AWS console
Click on Services
Select EC2



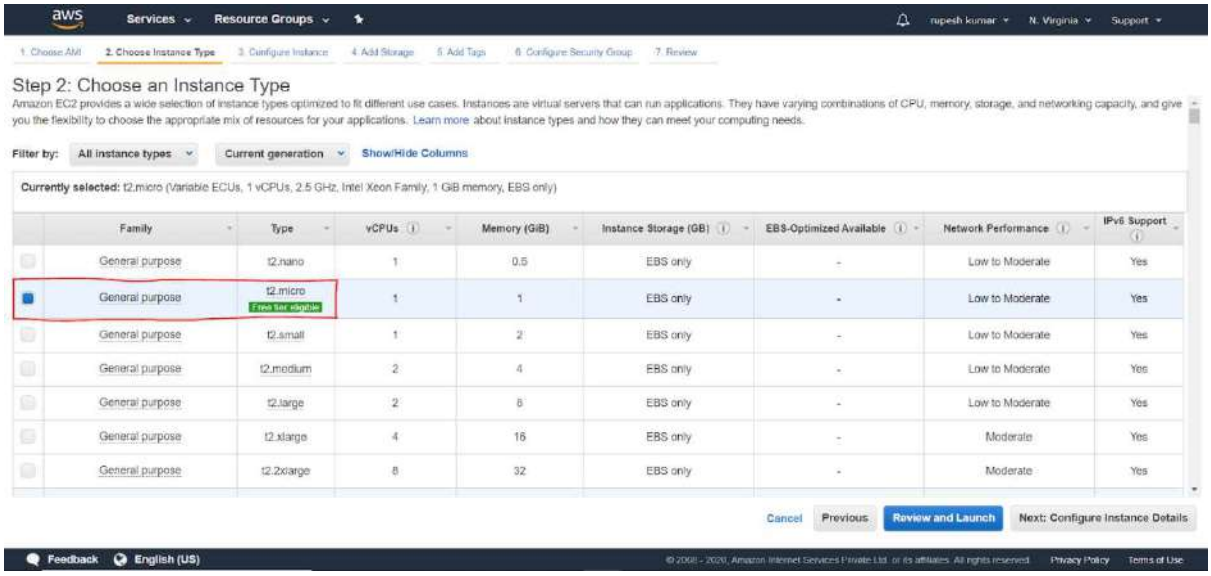
Click on Instances
Click on "Launch Instance" button



On the “Choose an Amazon Machine Image (AMI)” page
Select AMI “**Amazon Linux AMI 2018.03.0 (HVM), SSD Volume Type** - ami-0761dd91277e34178”
Click on select button

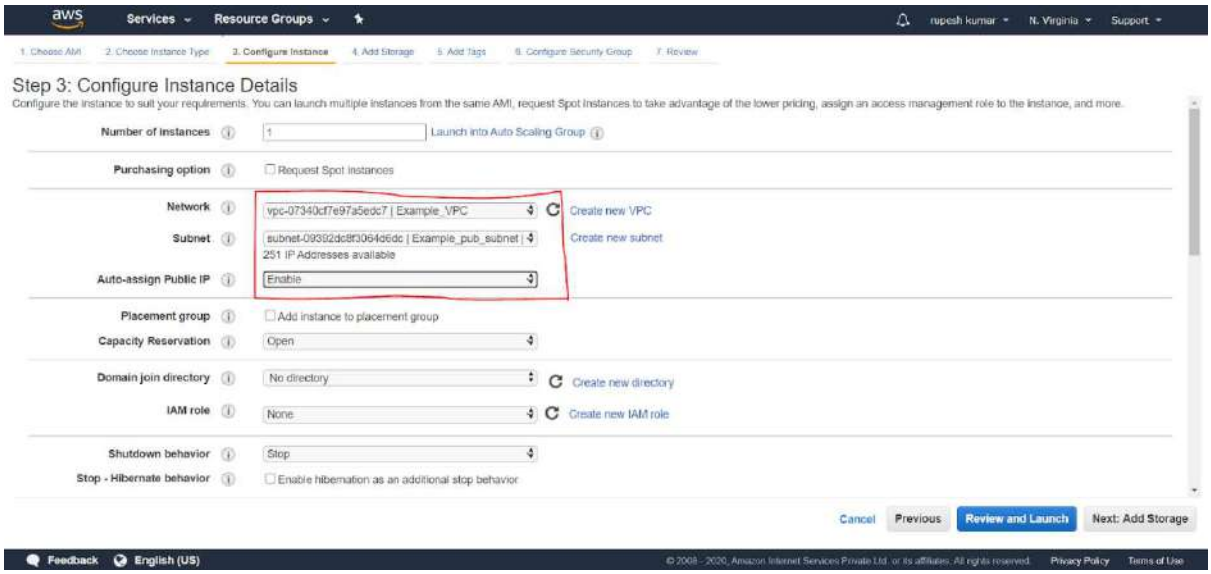


On the “Choose an instance Type” page
Select “General purpose”
Type → t2.micro
Click on “Next: Configure Instance Details”

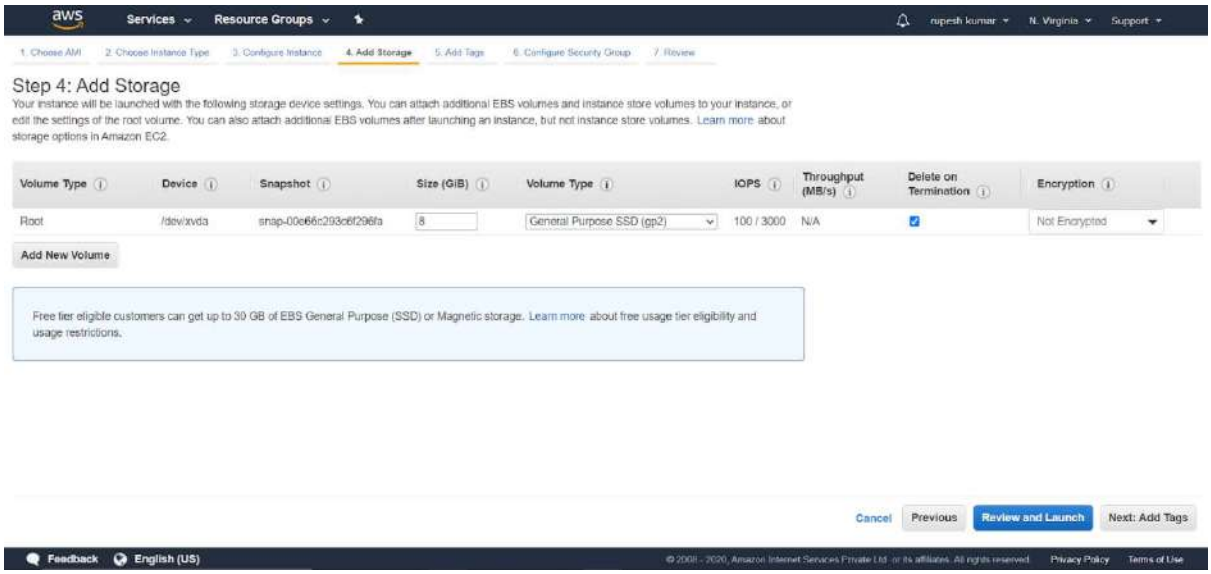


On the “Configuration Instance Details” page

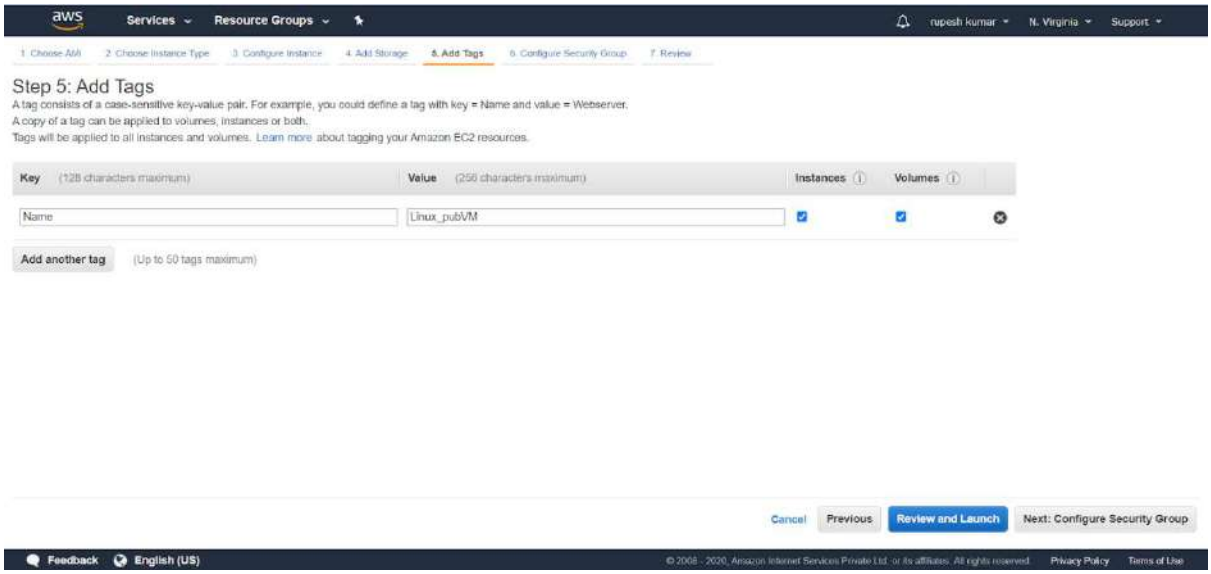
Number of instances → 1
Network → Example_VPC
Subnet → Example_pub_subnet
Auto-assign Public IP → Enable



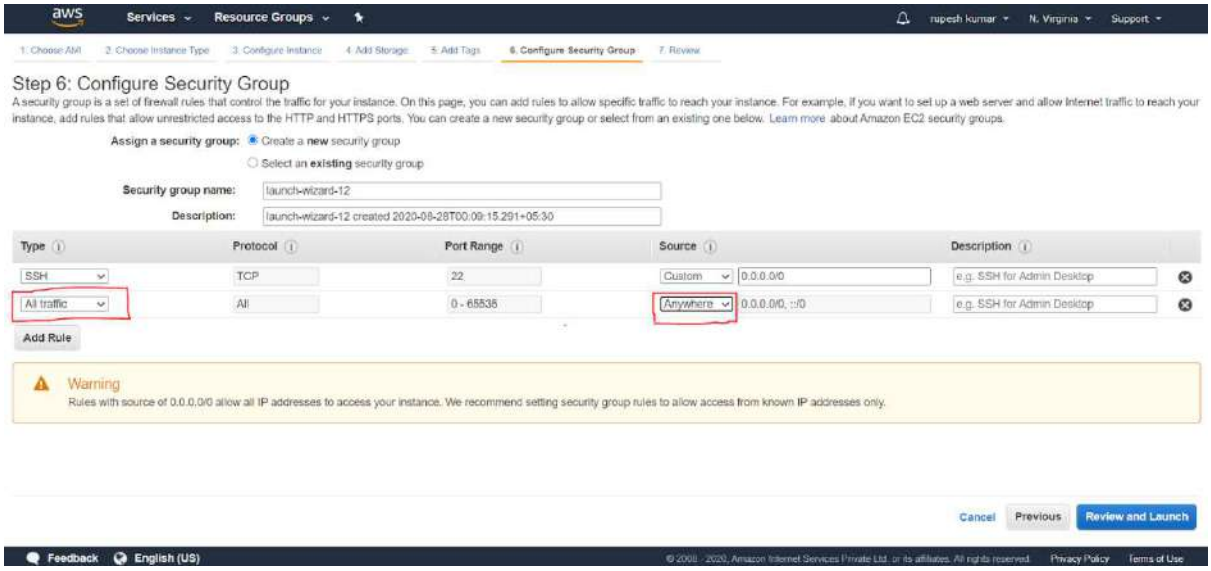
On the “Add storage” page
Leave the values as default
Click on “Next: Add Tags” button



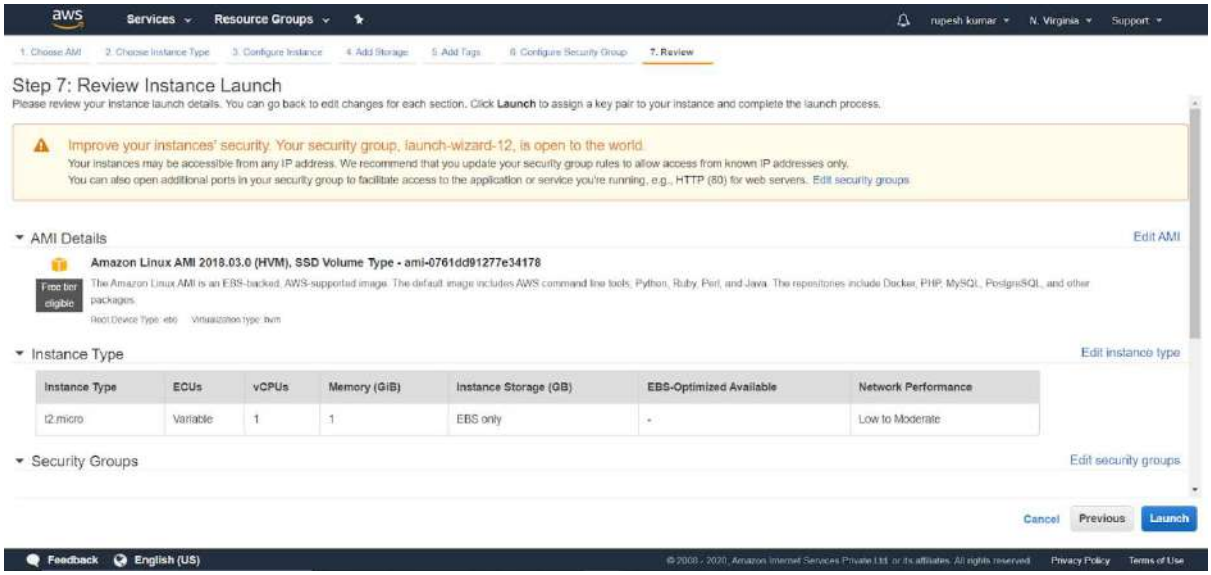
On the “Add Tags” page
Key → Name
Value → Linux_pubVM
Click on “Next Configuration Security Group” button



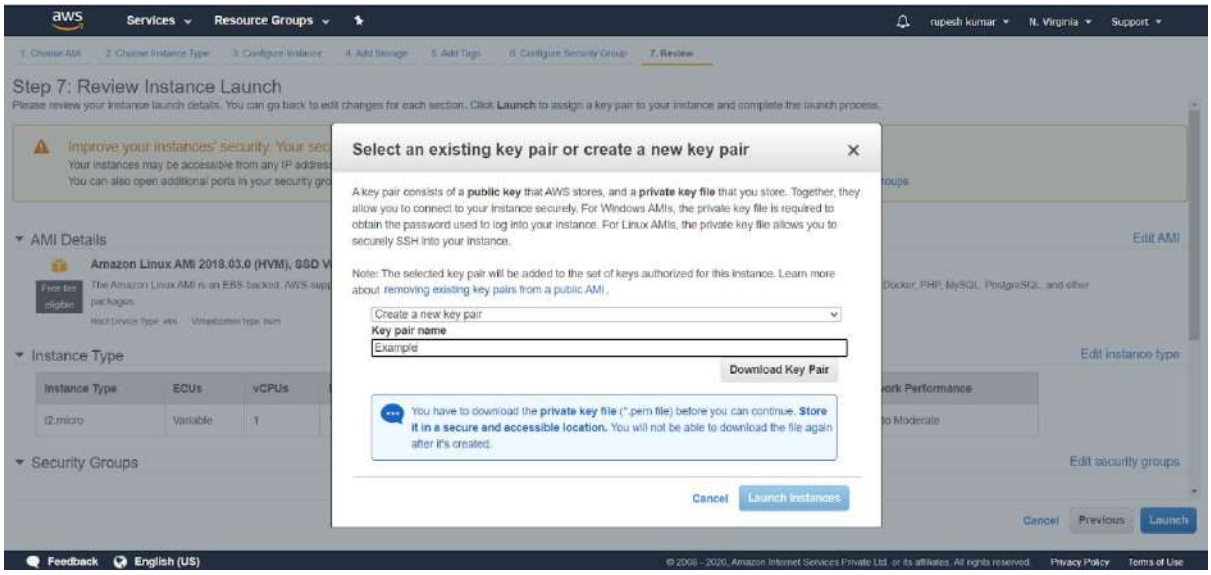
On the “Configuration Security Group” page
Assign a security group → Create a new security group
Click on Add rule and select All traffic
For All traffic rule types select the source to Anywhere
Click on Review and Launch button



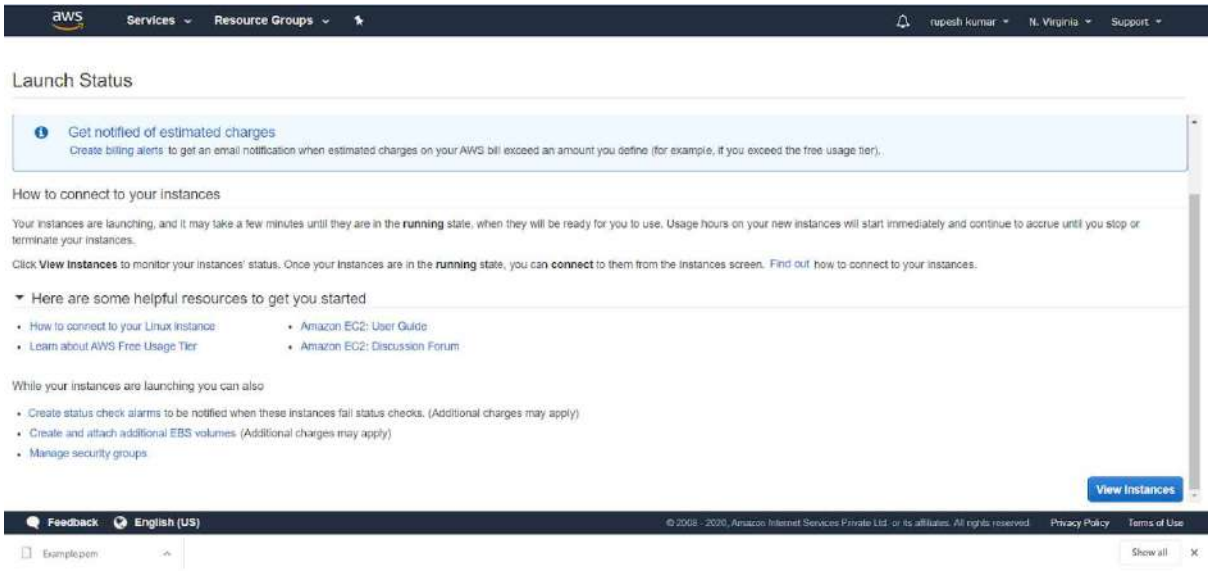
On the “Review Instance Launch” page
Click on Launch button



On the “Select an existing key pair or create a new key pair” page
Select Create a new key pair
Key pair name → Example
Click on the Download Key Pair
Click on “Launch Instance” button

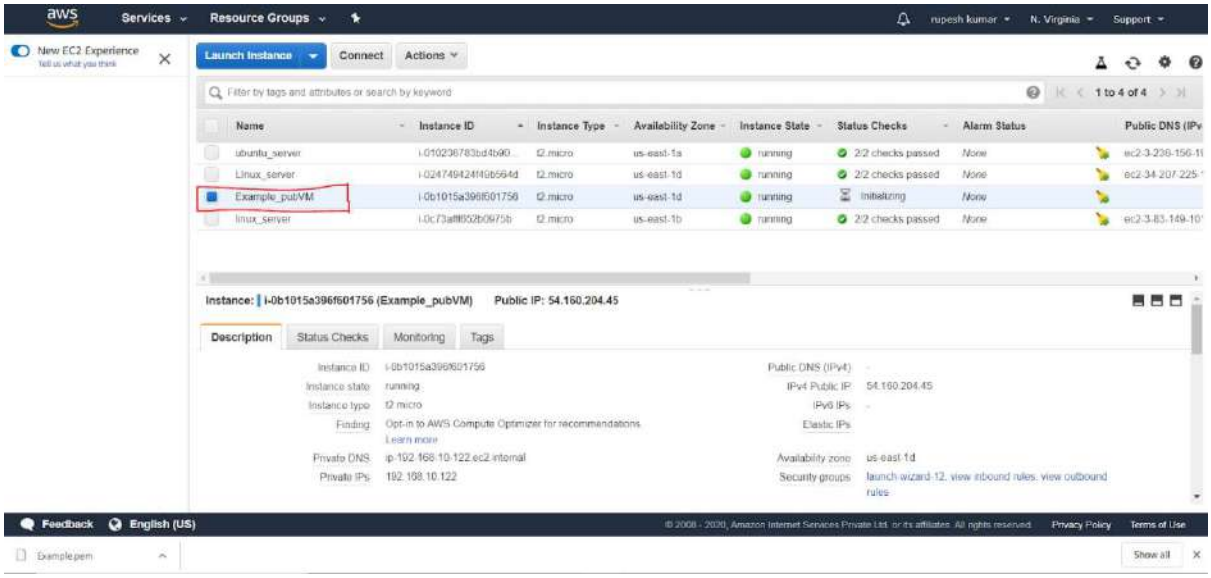


Click the summary
Click on View Instance button

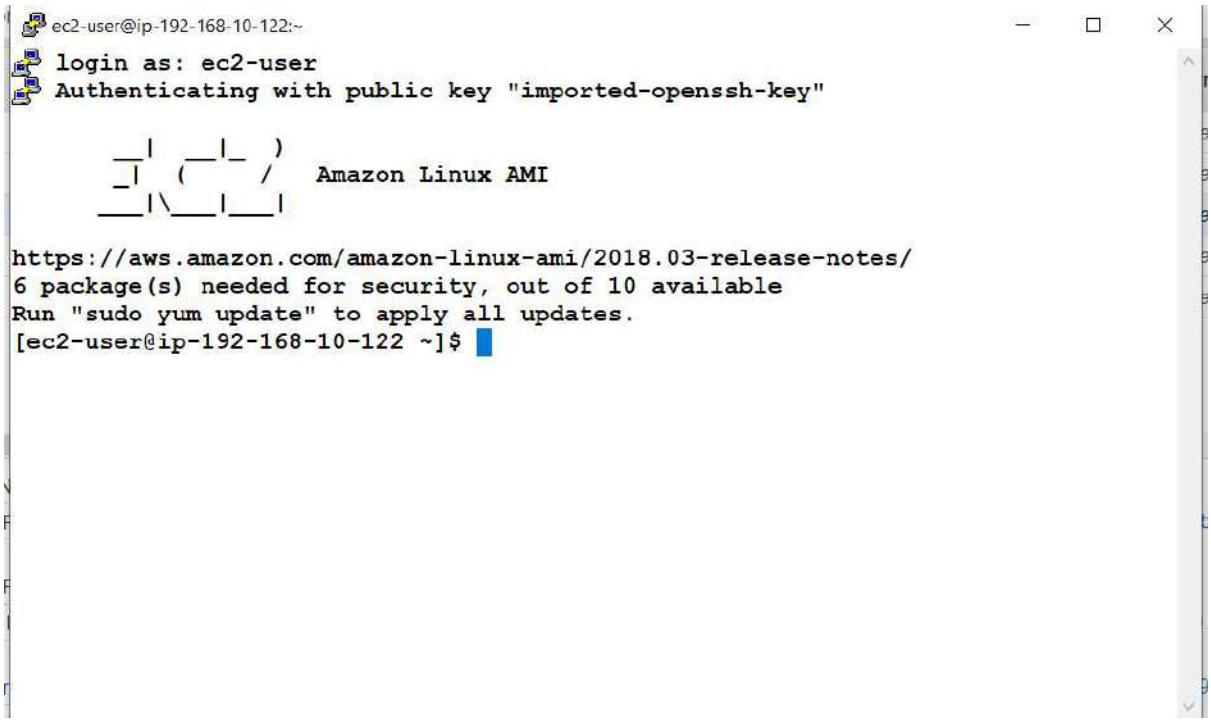


Verification

Linux instance in public subnet is launched



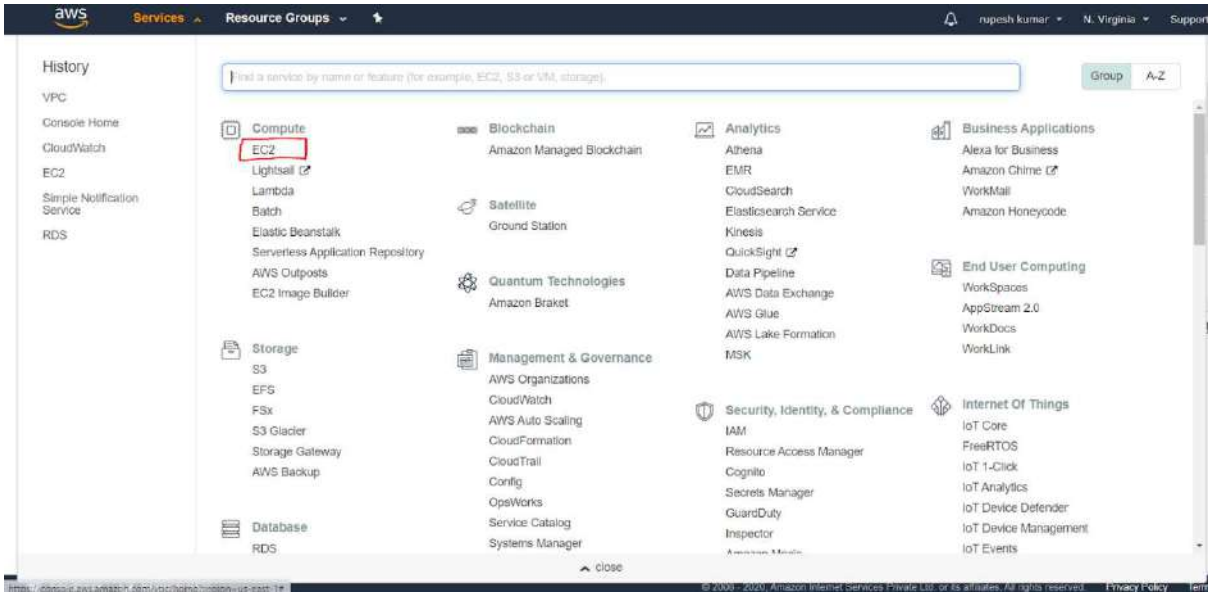
Now connect instance in public subnet using ssh



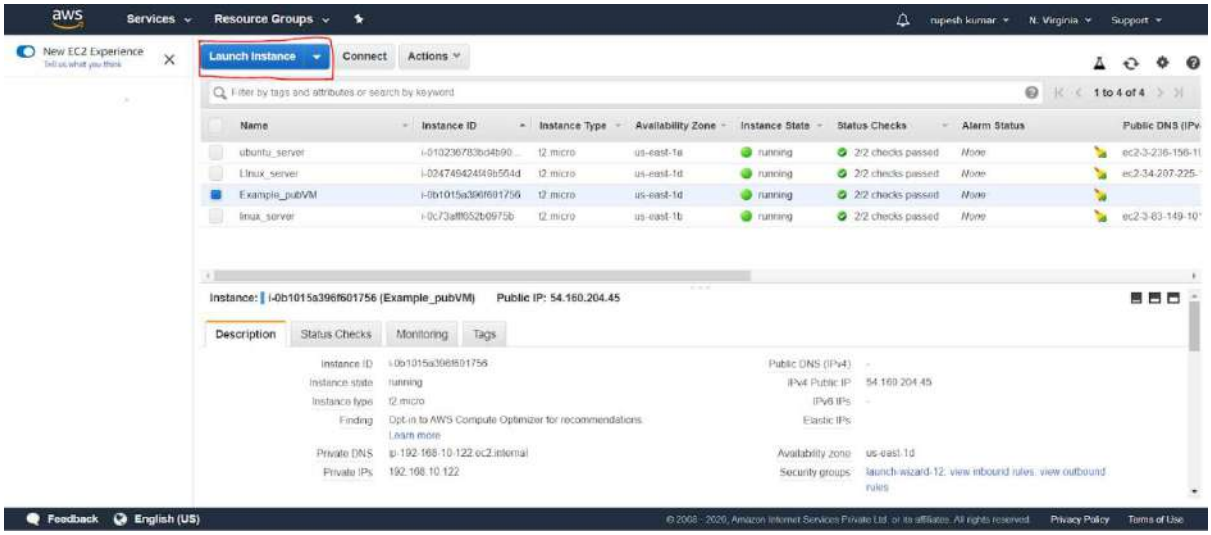
To Connect Linux Instance in Private Subnet

Launch Linux instance in private subnet → Example_pvt_sub
Open the AWS console
Click on Services

Click on EC2

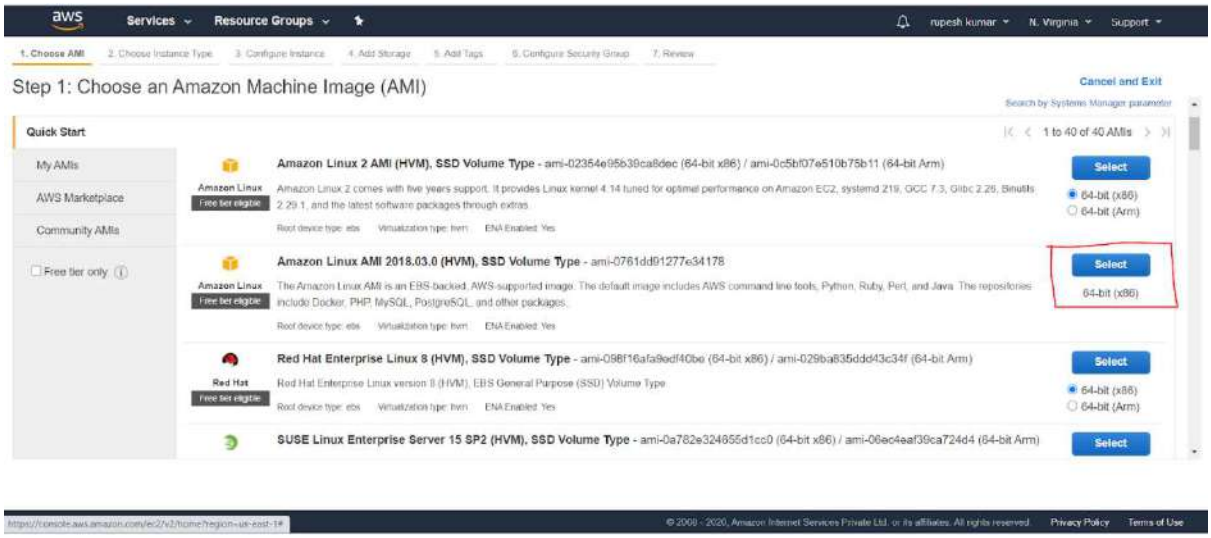


Click on Instances
Click on “Launch Instance” button

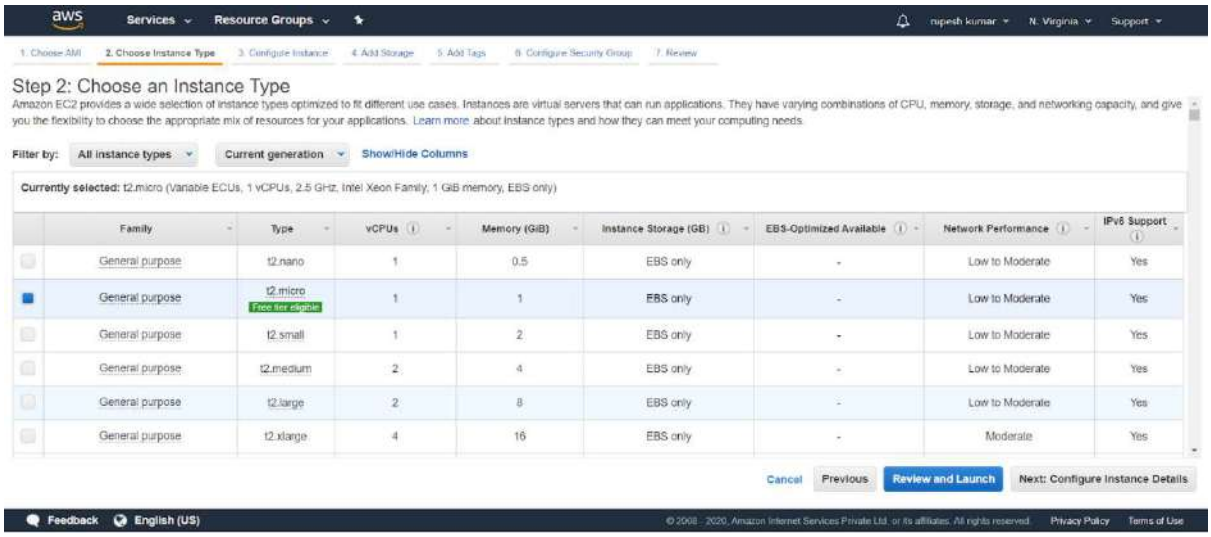


On the “Choose an Amazon Machine Image (AMI)” page
Select AMI “Amazon Linux AMI 2018.03.0 (HVM), SSD Volume Type - ami-0761dd91277e34178”

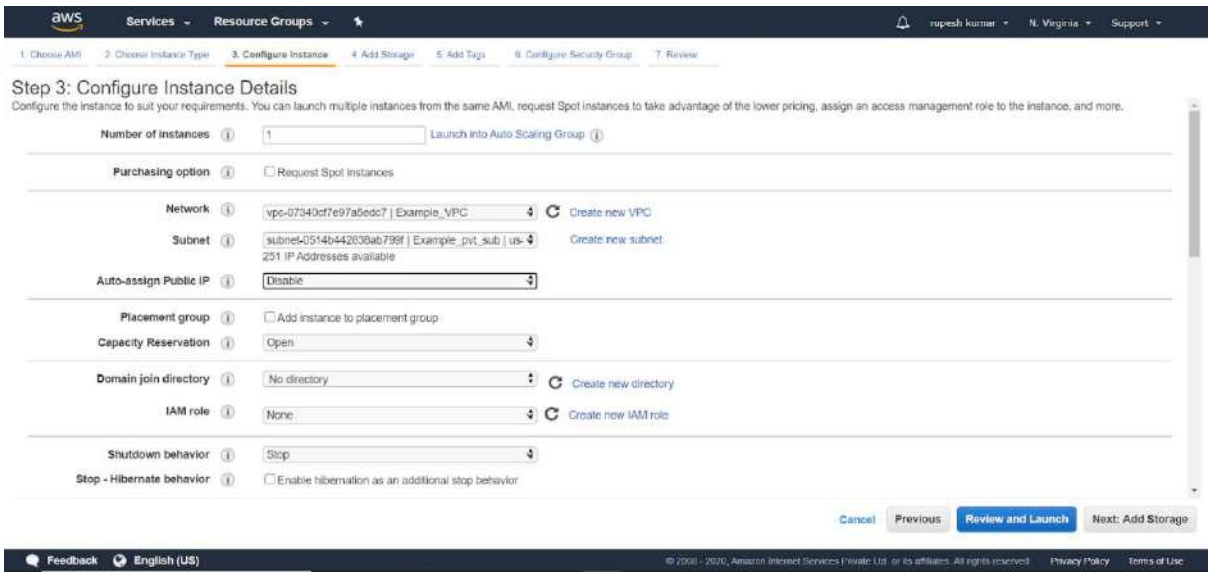
Click on Select button



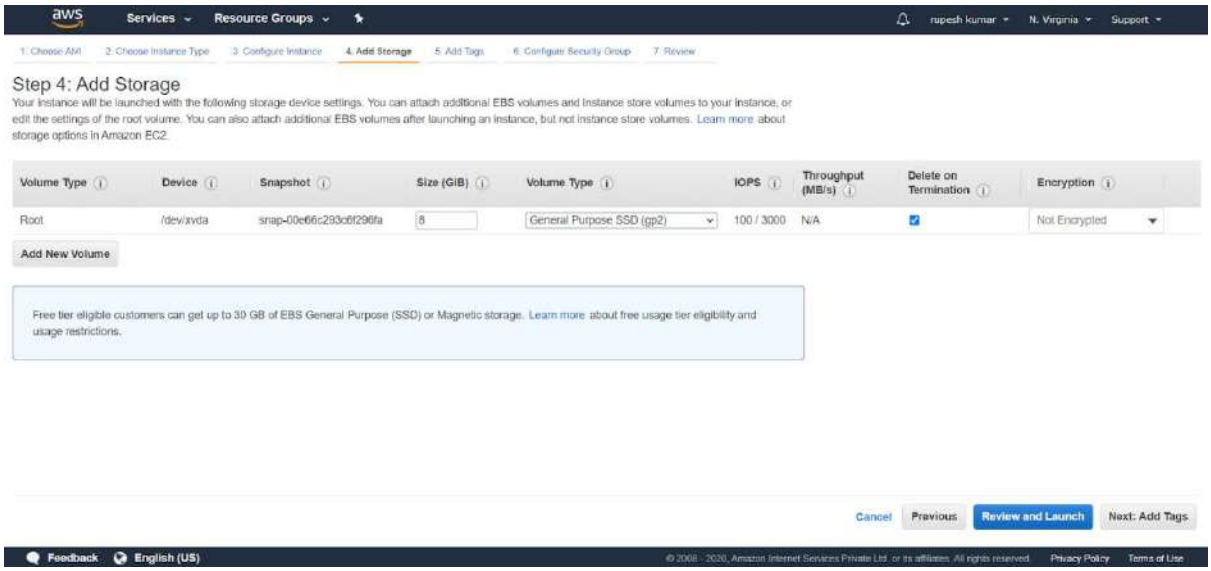
On the "Choose an instance Type" page
Select "General purpose"
Type → t2.micro
Click on "Next: Configure Instance Details" button



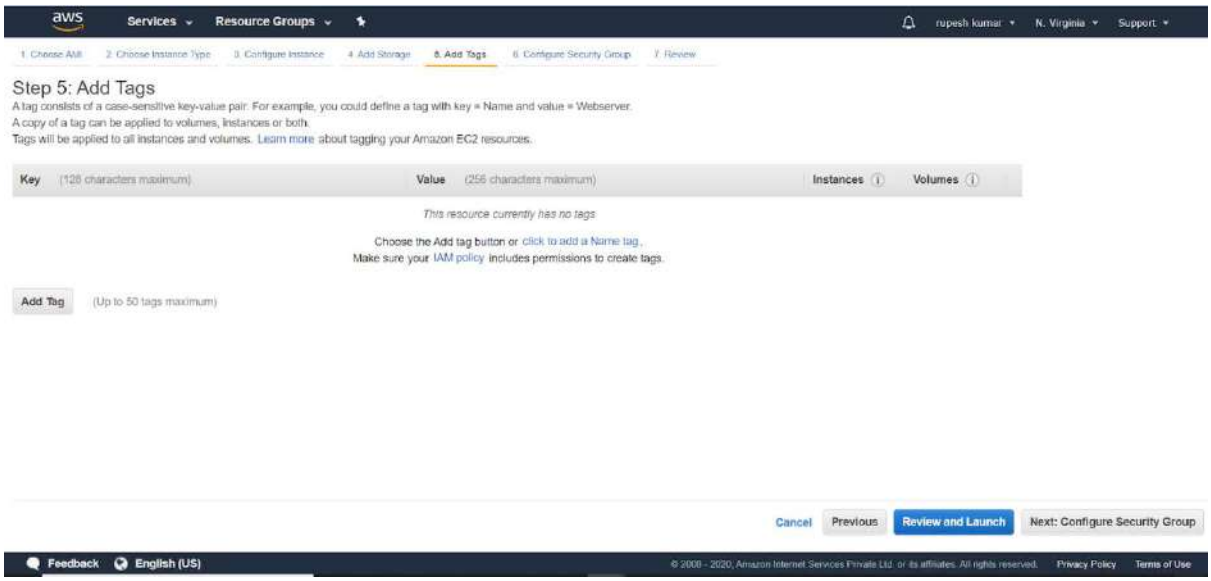
On the “Configuration Instance Details” page
Number of instances → 1
Network → Example_VPC
Subnet → Example_pvt_sub
Auto-assign Public IP → Disable



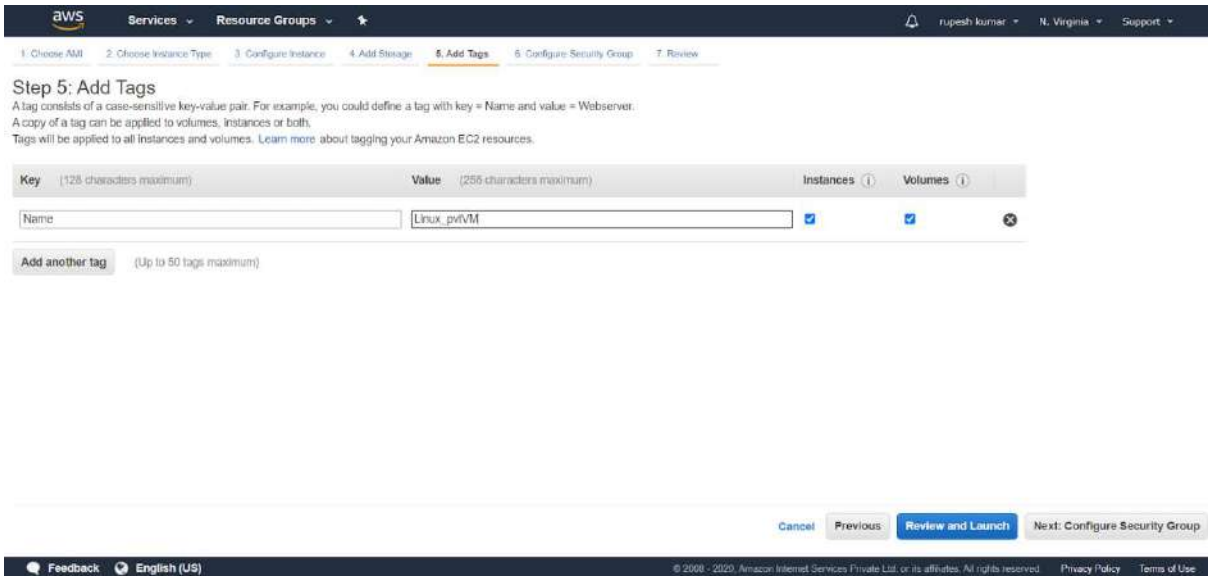
On the “Add Storage” page
Leave the value as default
Click on “Next: Add Tags” button



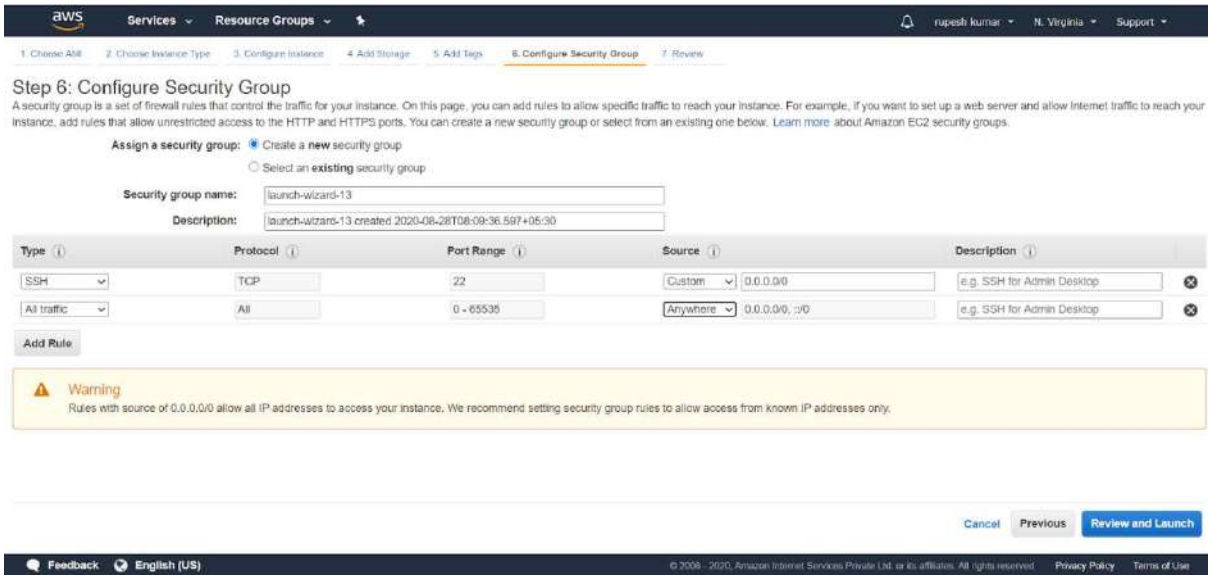
Click on Add Tag



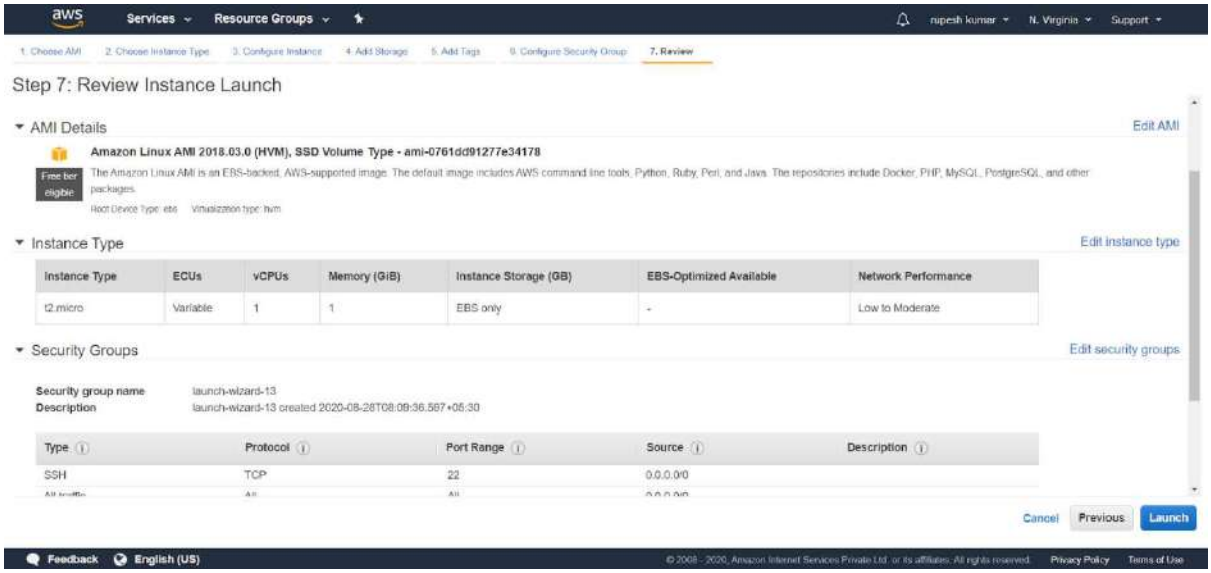
On the "Add Tags" page
Key → Name
Value → Example_pvtVM
Click on "Next: Configure Security Group" button



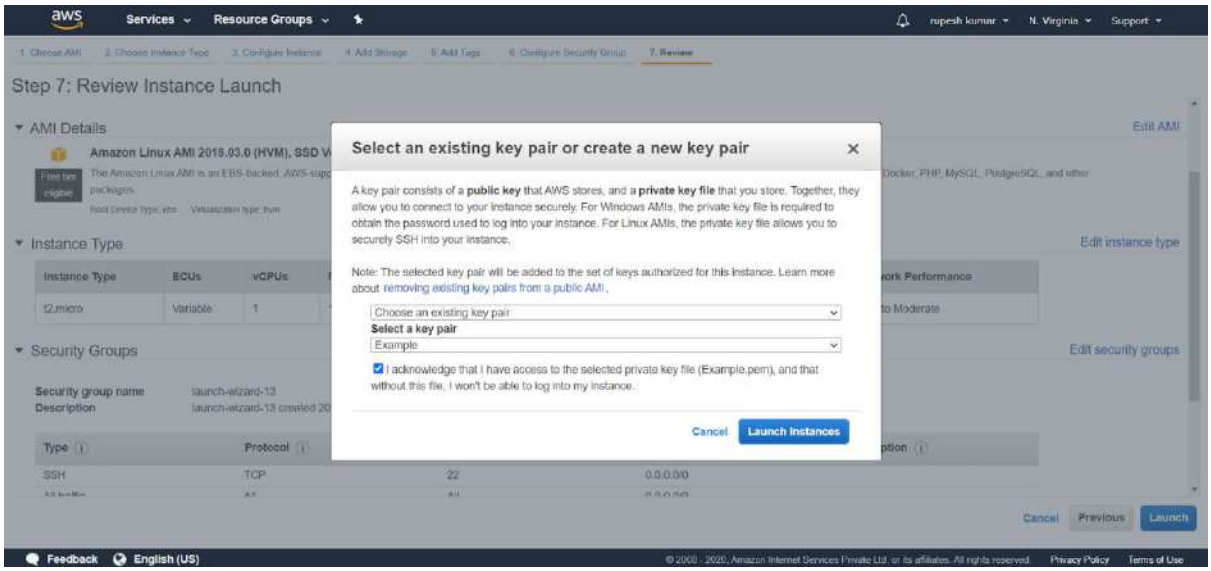
On the “Configuration Security Group” page
Assign a security group → Create a new security group
Click on Add Rule and select all traffic
For all traffic select the source to Anywhere
Click on “Review and Launch” button



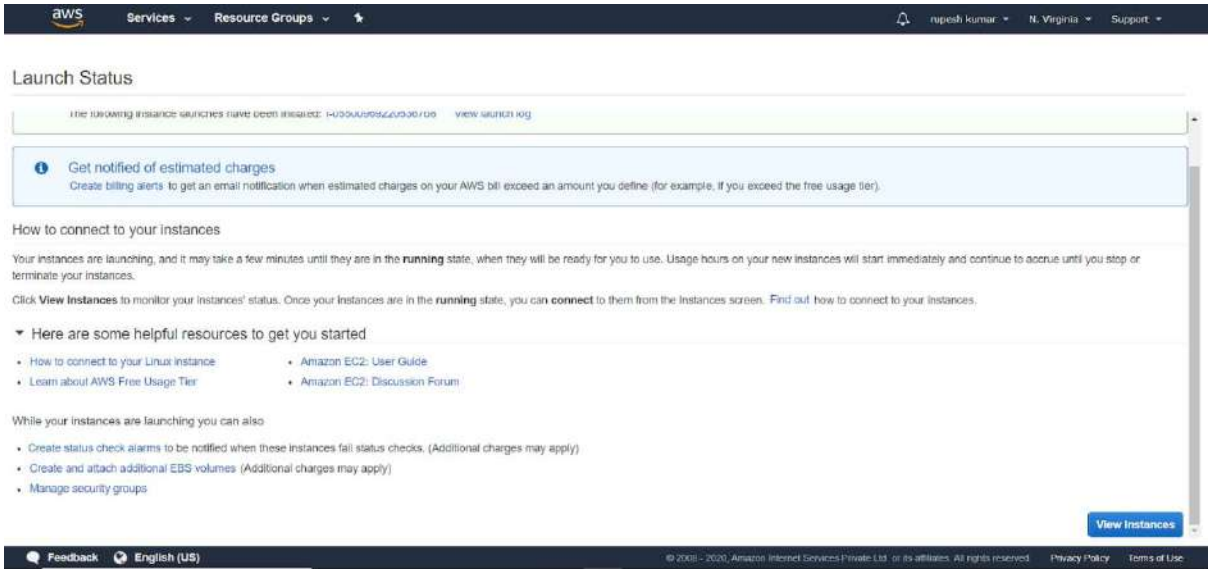
On the “Review Instance Launch” page
Click on Launch button



On the “Select an existing key pair or create a new key pair” box
Select existing key pair
Key pair name → Example
Click on “Launch Instance” button

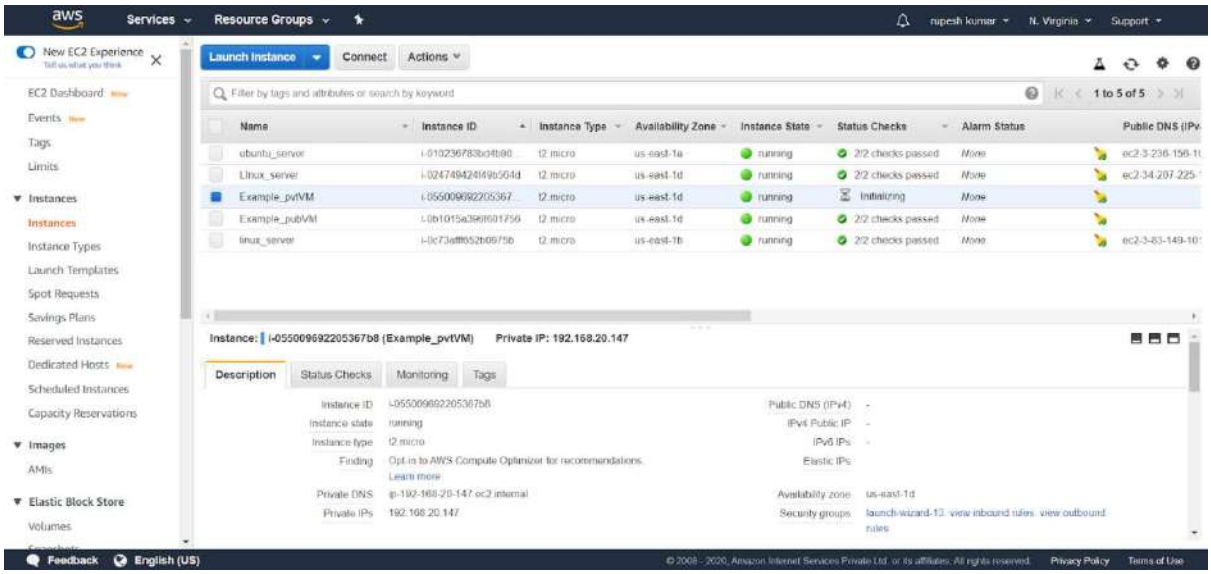


Check the summary
Click on View Instance button



Verification

Linux instance in public subnet is launched



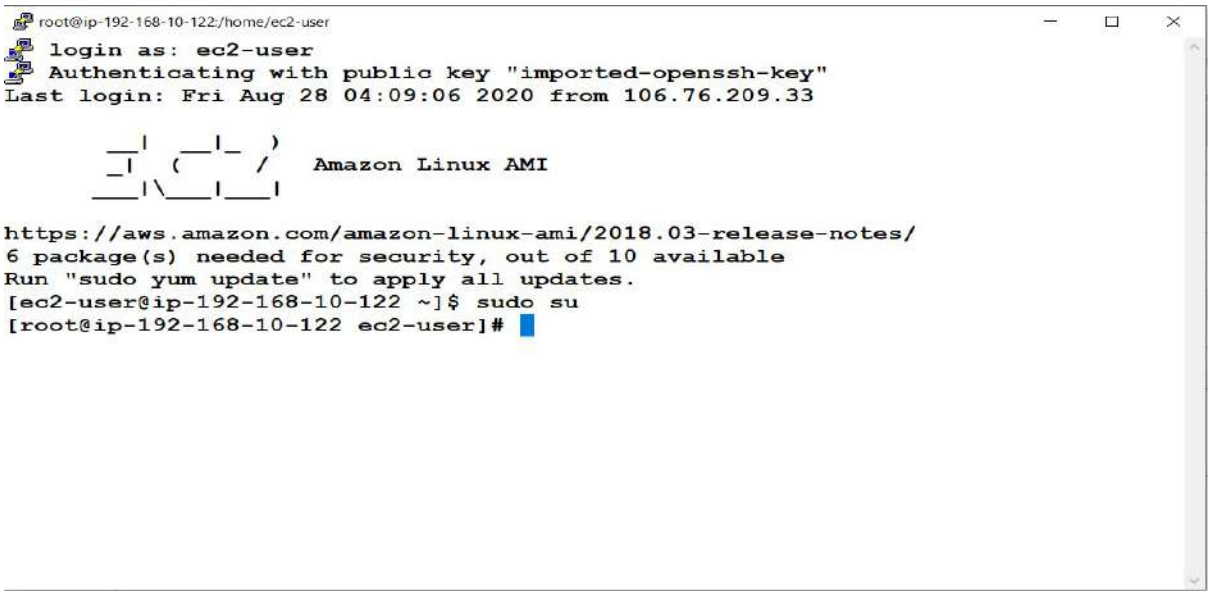
To connect to Linux private instance

First copy the key to Linux instance in public subnet

Now connect to Linux instance in public

Then connect to Linux instance in private

Connect to the Linux instance in public



Now connect to the Linux instance in private subnet using the private ip, the command is Ssh -i ec2-user@192.168.20.147

```
root@ip-192-168-10-122:/home/ec2-user
login as: ec2-user
Authenticating with public key "imported-openssh-key"
Last login: Fri Aug 28 04:09:06 2020 from 106.76.209.33

       __|  __|_  )
       _|  (     /   Amazon Linux AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/
6 package(s) needed for security, out of 10 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-192-168-10-122 ~]$ sudo su
[root@ip-192-168-10-122 ec2-user]# ssh -i ec2-user@192.168.20.147
Warning: Identity file ec2-user@192.168.20.147 not accessible: No such file or d
irectory.
usage: ssh [-1246AaCfGgKkMNnqsTtVvXxYy] [-b bind_address] [-c cipher_spec]
           [-D [bind_address:]port] [-E log_file] [-e escape_char]
           [-F configfile] [-I pkcs11] [-i identity_file]
           [-J [user@]host[:port]] [-L address] [-l login_name] [-m mac_spec]
           [-O ctl_cmd] [-o option] [-p port] [-Q query_option] [-R address]
           [-S ctl_path] [-W host:port] [-w local_tun[:remote_tun]]
           [user@]hostname [command]
[root@ip-192-168-10-122 ec2-user]#
```

It gives the error message, now add the key pair related to the private subnet Linux instance and add the content of the keypair.
nano example.pem

```
root@ip-192-168-10-122:/home/ec2-user
  GNU nano 2.5.3              File: example.pem

-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAkJaggB6GT06RLNSuOEtr3RW1SFJLFeFKwvLCHQauyptiZfaWU3IS+Eft2ef3
NGLw7Ks06B2n3ZpzzHoHhgdTIjh9N5p/UvsKf3vJml3WJ7Jwe2IV8qe7pa/ZdvUGk+PcF2VW2OtT
JQsofHBrjVZmaRE1xP45OUJKVNS1nRuHX1Xwc/Ck6vA9y1yYAV+OFNatPRRNIBk0nUy5JY0SZQkE
b/pW577eNnQ4jyYD6YHTd31A1xd+fe5LtTGpYHg5PmAgNY0p2svKYSY3sLfqcVeDBanB9IVt5p/u
+3SFVoA4vIJI8kCCBAIdtxxwTzBcj9k3NHFCzUetPEyyOBUeVI6jzwIDAQABAoIBAG+FjtRjNusy
yW0PujU3j0HecTbAKqP8uoJ1Zd2niuhBQ3sr4DUKtrEEIeRCM/0XF4ckYtFqF1Ep0Y100hrByZCK
i6J4qx5g/W7pFs3W9Nh3nKS+OfmJAIZChXRod6NYTC1Lg9oaYG4hFiAtQfepHaKKoLOJ9q9Afz7B
NjewxRB1daQ1W9kKkq1R4+1ZiY4IBj6edvGnv99HuZMzoSa8+MUXTRd2FNMrO4e5YjeNY8VfgTqc
HF1UG3E4BWOMDQA0UqJvHk+X8uq88gb8G37yjGI1j43bQ9+Pw2ikNMfR7kZrXEZbwG5agUbdjm5a
DrqDz3PJejLo9qm8u0CQnab0LqkCgYEA6NppDG2vYoL++uDjEObwFA1G0qIOEv7QdEOJ/MMv+vdm
1kJd3Dh9kdYkl7wjAvWlnznVp2/VeIFUREzDGX1ke4tLyjkz8TLL901UUQ2KuFssuxDRAbtPpkYq
CQKs4UhDRYjtlwxHFGy+cvmy8J+Ergptuwrz7hIIkTAnbNH7jgUCgYEAnvYTjiVQJwgGVoH+a+ly
j8YZoQBbX7vUn4p6YSpwXRGRKefSqVQVTCQjXpb8NtRTHlBy6gYonzw2sn+gpBNP83P7RLm+clMn
+81MlYpmijZxc2633NUiegsegmeStZgk9/zRs2+j/Cv95Cd80Y2NM5KmSjMN/KSuPklV9ozPfsMC
gYAFta1Tv7DIQpwL/M20kWUbqMOu0Ih10Me9whY1G3gmuEBMuO3iQ4RYuh6F1fhpzyozgFCL3YMn
hExTrGowSri7Csxd9g8e//beZm7p2eIn6RxsrdniJ/ypAB1xxR4GHCaCIvxocsWfa5cz7ImFuvOe
7OSJ7JfUo56QKNUepvt7HQKBgE+m0F+utL4KGFrqoljiTiRayGbTbfXHgaA73FypzknkTo/n+Lge
SNmxVgPEtjanJ8sN1rcLRPmdS28f4pe0kaBU4ngqdpKEtolG8vQPuJfS9gA4X2sJZVAwGCaRzYKu
                    [ Read 23 lines ]
^G Get Help  ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line
```

Now run the command to connect to the Linux instance in the private subnet

```
root@ip-192-168-10-122:/home/ec2-user
[root@ip-192-168-10-122 ec2-user]# nano example.pem
[root@ip-192-168-10-122 ec2-user]# ssh -i example.pem ec2-user@192.168.20.147
```

After running the command, the prompt was changed from the public subnet to the private subnet

```
ec2-user@ip-192-168-20-147:~
[root@ip-192-168-10-122 ec2-user]# nano example.pem
[root@ip-192-168-10-122 ec2-user]# ssh -i example.pem ec2-user@192.168.20.147
Last login: Fri Aug 28 04:11:51 2020 from 192.168.10.122

       __|  __|_  )
       _|  (     /   Amazon Linux AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/
[ec2-user@ip-192-168-20-147 ~]$
```

Now we are successfully connected to the private subnet.