Karthik Pradeep Hegadi

2KE20CS032

Assignment 35

Understood. To follow the provided instructions and create the files/directory using the same name and case as provided in the task steps, please provide me with the specific names and case instructions for the files/directory you want to create.

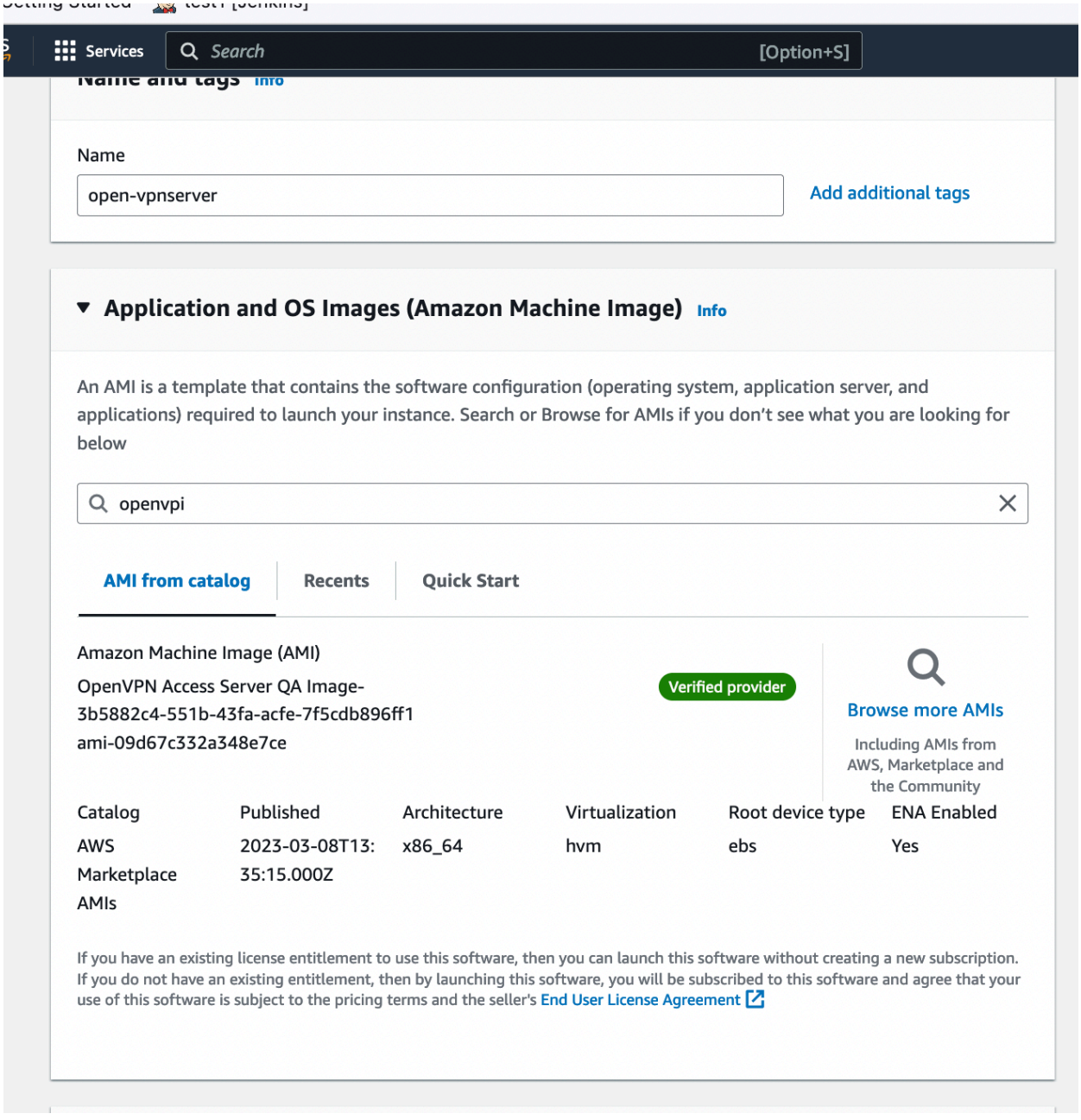
AWS

==========

Assignment:3 VPN server configuration in AWS

==========

1. Navigate EC2 -> Launch instance



2. In the AWS marketplace search text "openvpn" you will find the results. Select the first Image "OpenVPN Access Server”

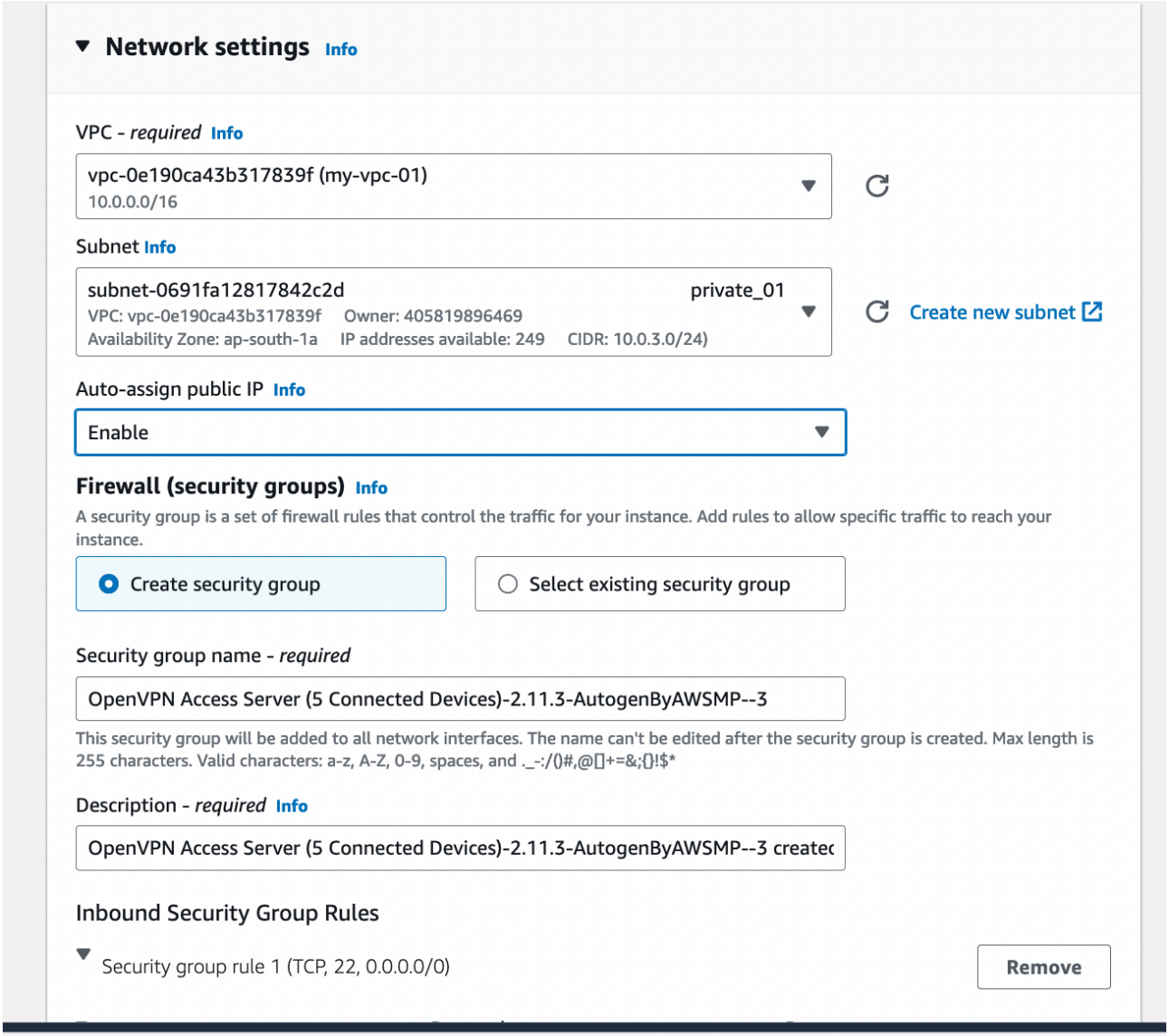
3. In the Instance type select "2.micro" and click config instance details4 Select your VPC, select the Public subnet that you have created previously, Auto Assign ip -> enable, host name -> Use subnet setting (Ip name) and click Add storage

5. Storage settings can be default, click Add tags

6. Add tag key as "Name" and provide the value and click configure security group (Note: The default settings allows all traffic for ssh, you can change to "mv IP" to be more secure)

7. Click "Review & Launch" and then click "Launch option" . Choose the existing keypair from the list that you generated and then click "Launch Instance

8. Verify your Instance is running



/awsmp-offer-legal-documents-prod-iad.s3.us-east-1.amazonaws.com/prod/arn:aws:catalog:us-east-1::offer/3ihdqli79...U5/2

9. Login to the VPN server (Note : you can either ssh from windows/linux machine where you have copied the private key, or you can use putty as well)

You need to use username as openvpnas instead of root

```
(base) kartikhegadi@Kartiks-MacBook-Air aws.02 % chmod 400 open_vpn.pem
(base) kartikhegadi@Kartiks-MacBook-Air aws.02 % ssh -i "open_vpn.pem" openvpnas@65.0.93.148
The authenticity of host '65.0.93.148 (65.0.93.148)' can't be established.
ED25519 key fingerprint is SHA256:4oad0V3ufSCTGhS8JemoM4rYt7MNy9qzL7K+nrM/OIA.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '65.0.93.148' (ED25519) to the list of known hosts.
Welcome to OpenVPN Access Server Appliance 2.11.3

  System information as of Sat Jan 28 04:18:28 UTC 2023
```

10. Once you try gave your username it prompts for configurations .Follow the screenshots and make changes Will this be the primary Access server node ? - Enter for default : ves

Please specify the network interface - Press Enter for default :

Press Enter for default [9431 : "click enter”

Press ENTER for the default[443] : "click enter"

Should client traffic be routed by default through VPN?

Press ENTER for default [no] : yes

Should client DNS traffic be routed by default through VPN? - “yes"

Use local authentication via internal DB? "Click enter”

Should private subnets be accessible to clients by default?

Press enter for EC2 default [yes]: "click enter”

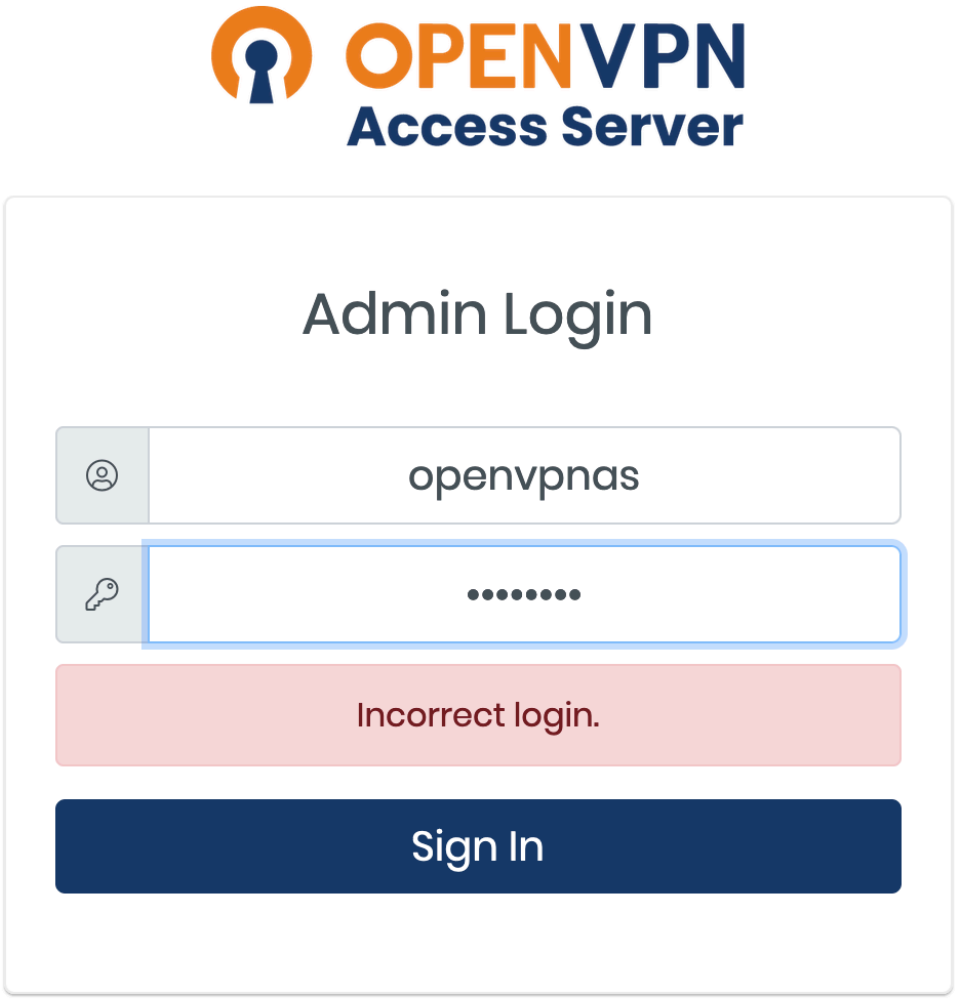
```
Please enter 'yes' to indicate your agreement [no]: yes

Once you provide a few initial configuration settings,
OpenVPN Access Server can be configured by accessing
its Admin Web UI using your Web browser.

Will this be the primary Access Server node?
(enter 'no' to configure as a backup or standby node)
> Press ENTER for default [yes]: yes

Please specify the network interface and IP address to be
used by the Admin Web UI:
(1) all interfaces: 0.0.0.0
(2) eth0: 10.0.1.48
Please enter the option number from the list above (1- 2).
> Press Enter for default [1]: 1
```

```
Please specify the TCP port number for the OpenVPN Daemon
[> Press ENTER for default [443]:

Should client traffic be routed by default through the VPN?
[> Press ENTER for default [no]: yes

Should client DNS traffic be routed by default through the VPN?
[> Press ENTER for default [no]: yes
Admin user authentication will be  local

Private subnets detected: ['10.0.0.0/16']

Should private subnets be accessible to clients by default?
[> Press ENTER for EC2 default [yes]: yes
```

```
Created symlink /etc/systemd/system/multi-user.target.wants/openvpnas.service
/lib/systemd/system/openvpnas.service.
Starting openvpnas...

NOTE: Your system clock must be correct for OpenVPN Access Server
to perform correctly.  Please ensure that your time and date
are correct on this system.

Initial Configuration Complete!

You can now continue configuring OpenVPN Access Server by
directing your Web browser to this URL:

https://65.0.93.148:943/admin
```

```
During normal operation, OpenVPN AS can be accessed via these URLs:
Admin  UI: https://65.0.93.148:943/admin
Client UI: https://65.0.93.148:943/
To login please use the "openvpn" account with "SQHJbgbeRF3E" password.

See the Release Notes for this release at:
   https://openvpn.net/vpn-server-resources/release-notes/

openvpnas@ip-10-0-1-48:~$ sudo passwd openvpn
passwd: user 'openvpn' does not exist
openvpnas@ip-10-0-1-48:~$ sudo passwd openvpnas
New password:
Retype new password:          lusy@123
passwd: password updated successfully
openvpnas@ip-10-0-1-48:~$     lusy@123
```

11. Now you are logged in as "**openvpnas**" user

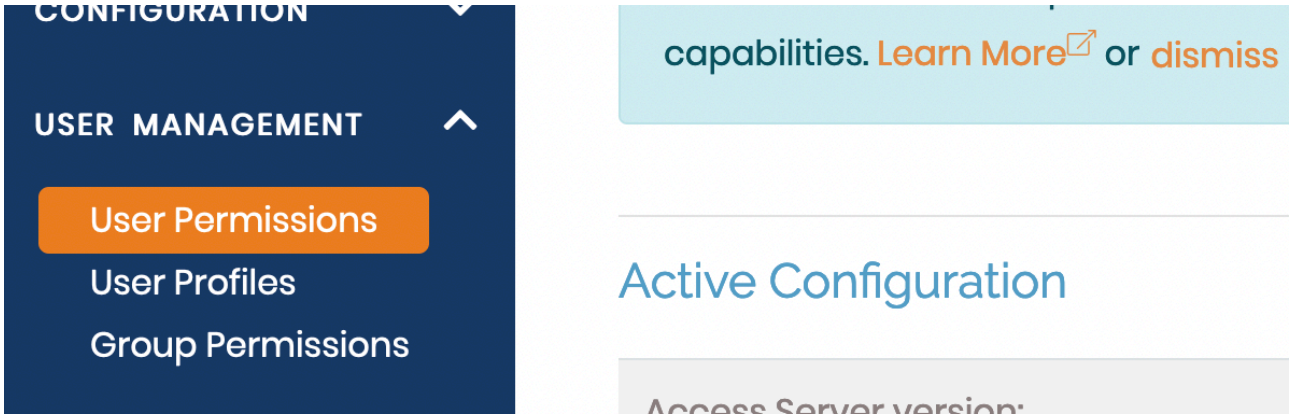


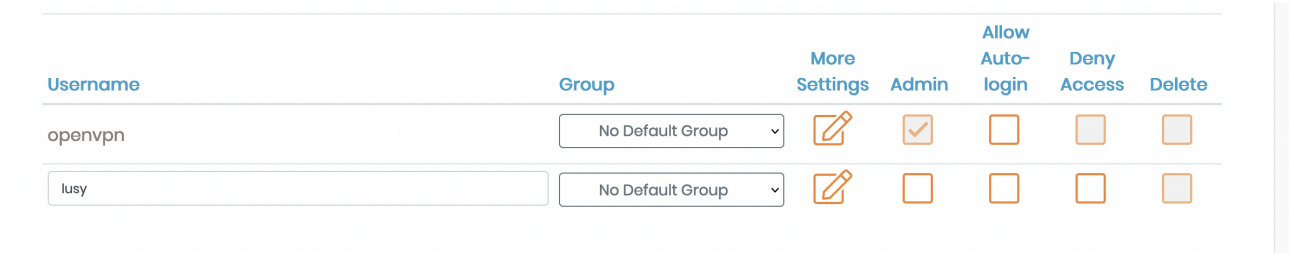
12. In order to login to the VPN server in GUI you need to login as user "openvpn". Generate

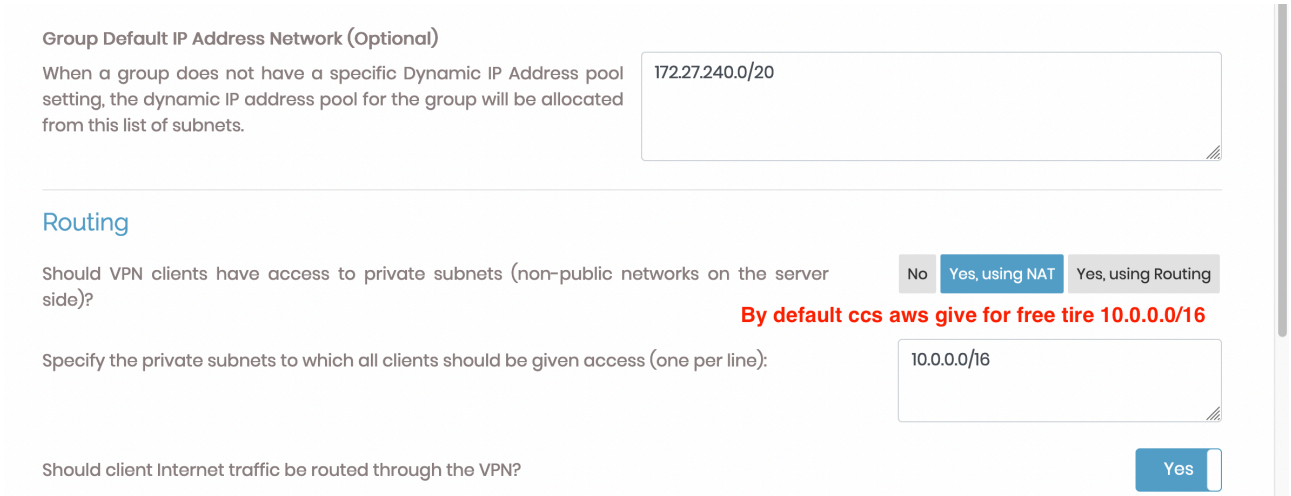
the new password for openvon user

Run the command "sudo passwd openvpn" and change the password

(note : give a strong password as it needs to be secured)



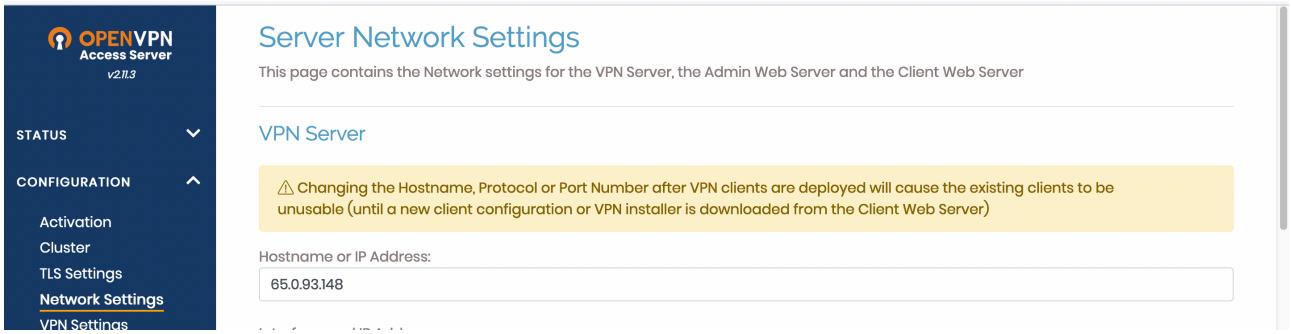


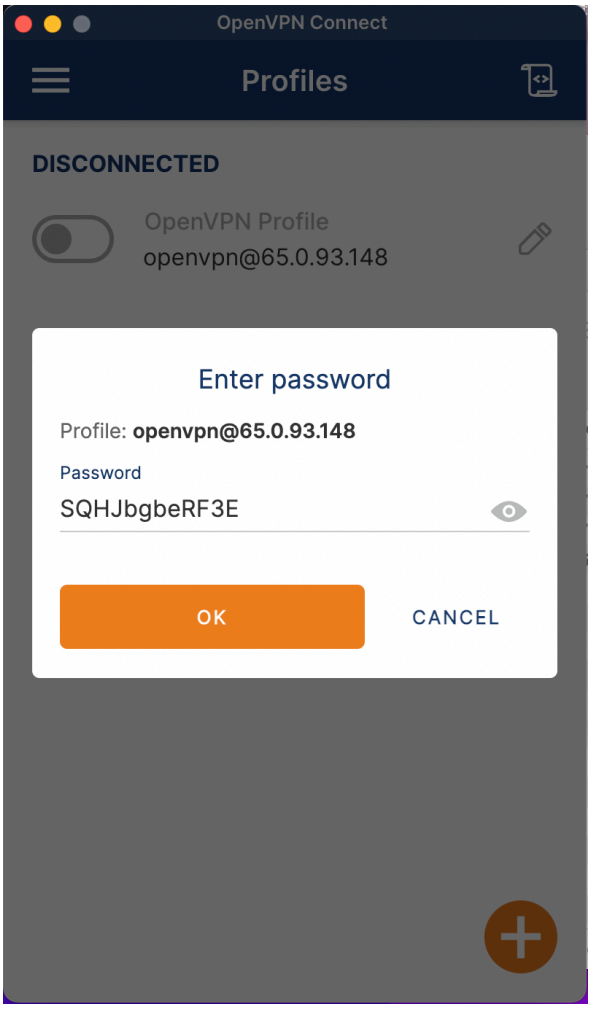


13. Now login to the web GUI using your public Ip https://"yourvpnip", login using your openvon username and password

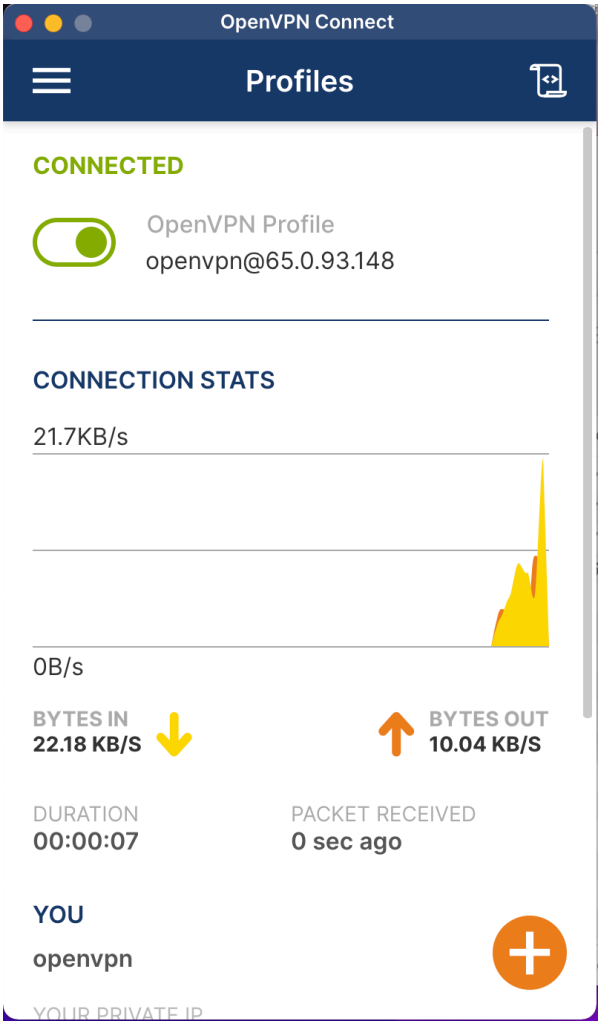
14. You can download openvpn connect for client if this prompt appears for you, if not You can download it separately(This is for windows)

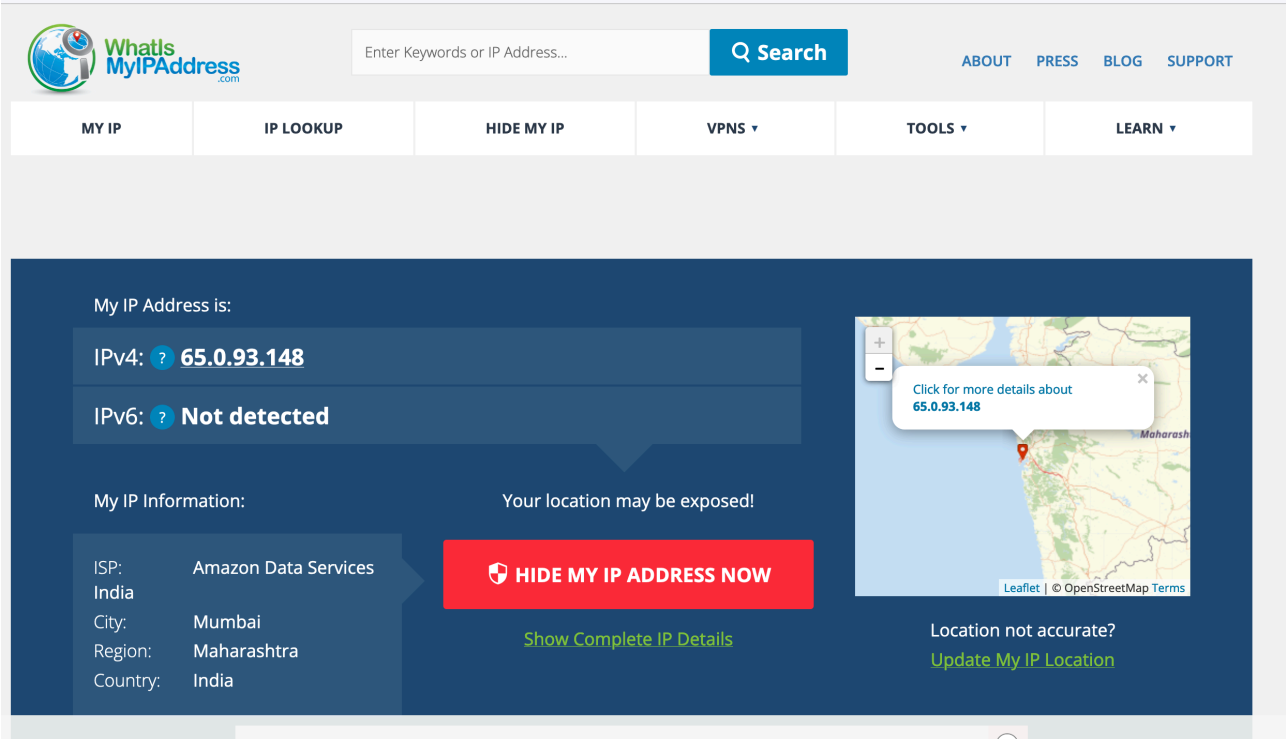
Please refer end of the document if you want to configure OpenVpn client in your Linuxmachine





14. You can create customized users in this settings





15. Navigate to configuration -> VPN settings -> configure the routing

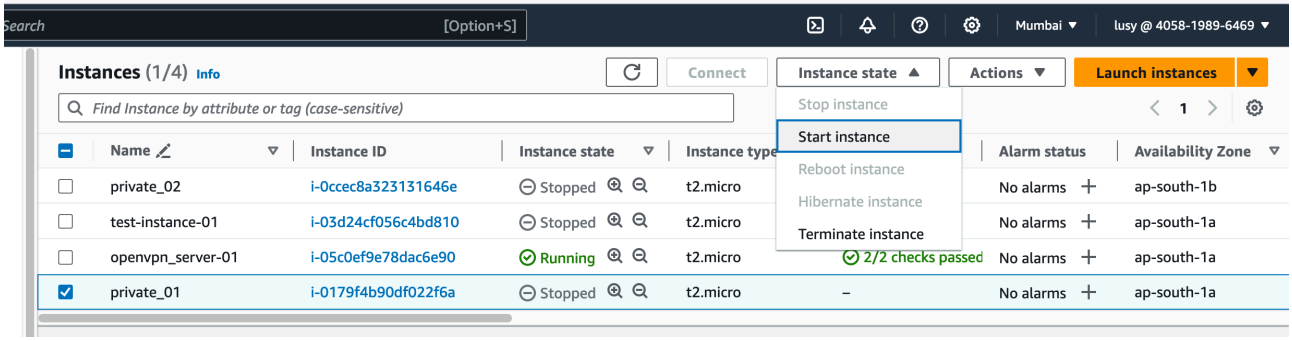
Specify the private subnets -> you can give your private subnet range in the field

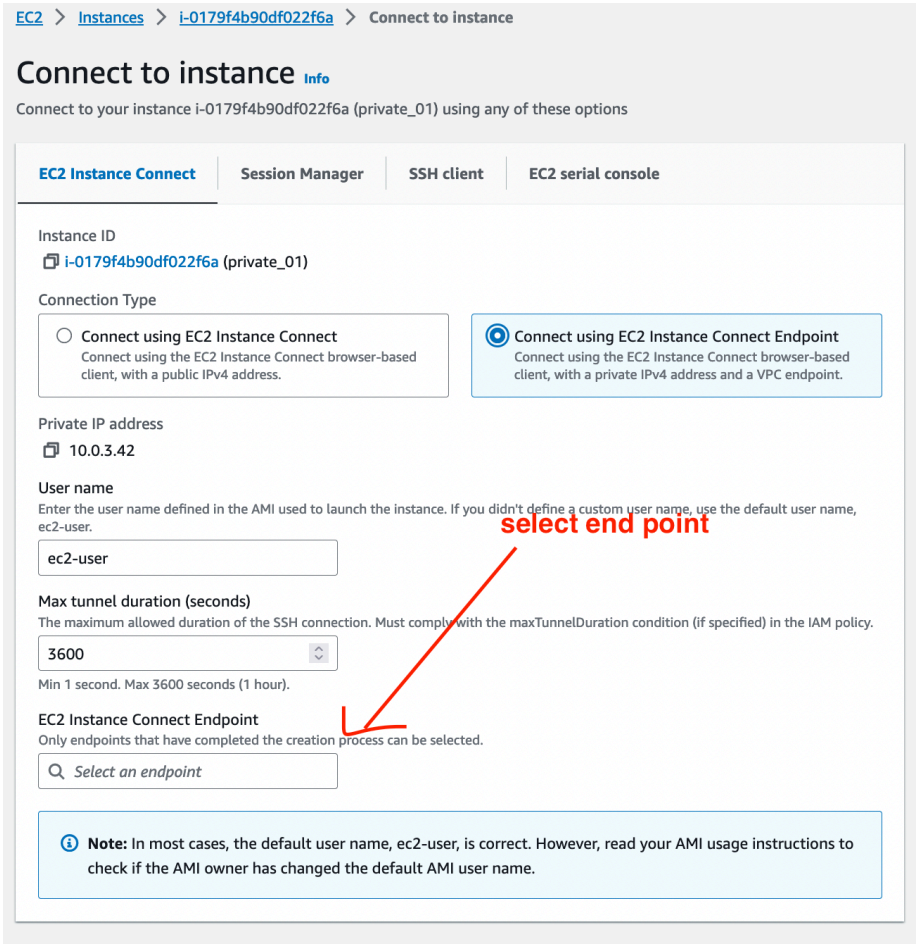
(YES I CHANGED) (I forgot to take screenshot)

16. Click on save changes

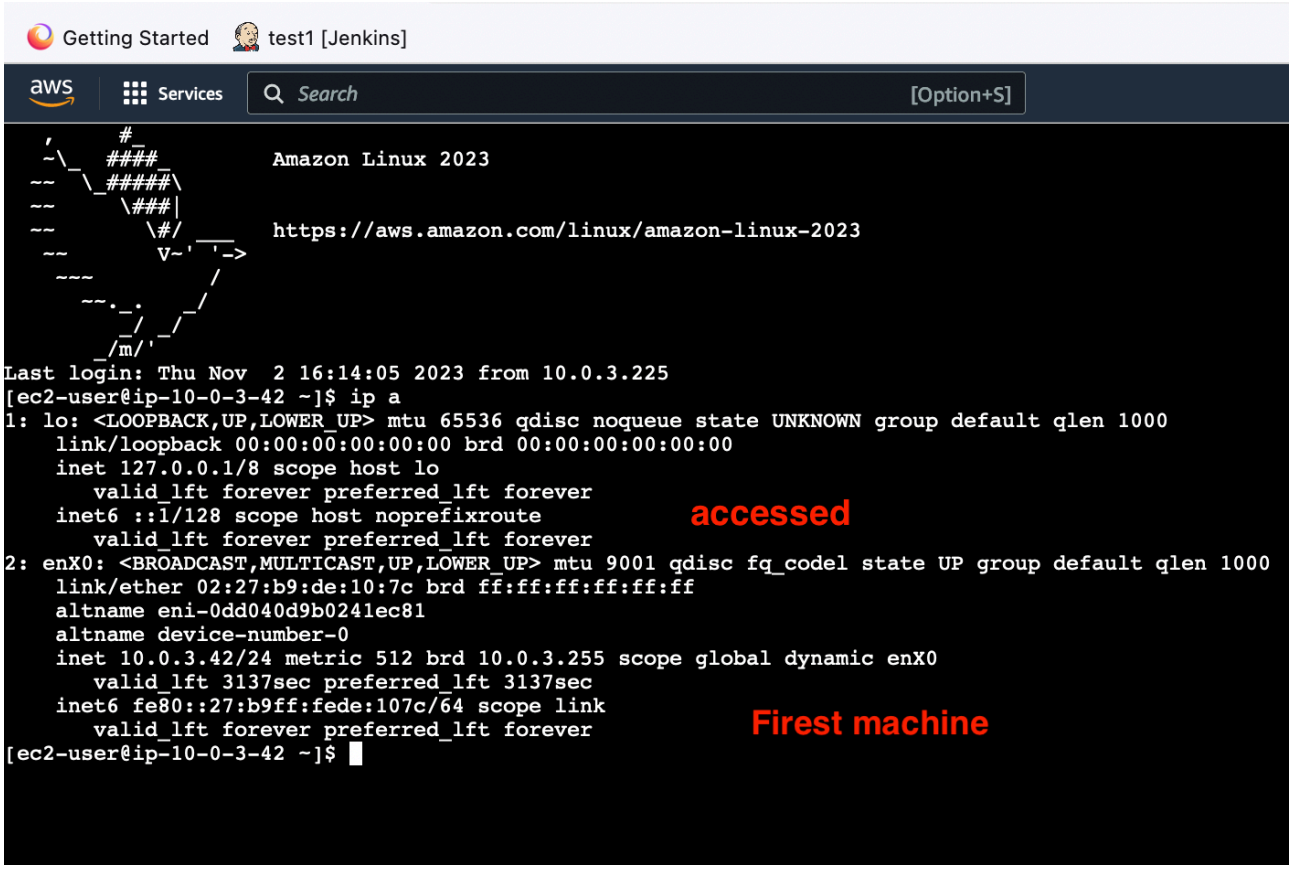
Note : Everytime when your public ip got

17. Now you need to connect to the VPN network using VPN connect , launch "open vpn connect from your windows" . You need to import the profile using the VPN url. Once you did you can connect using your username password

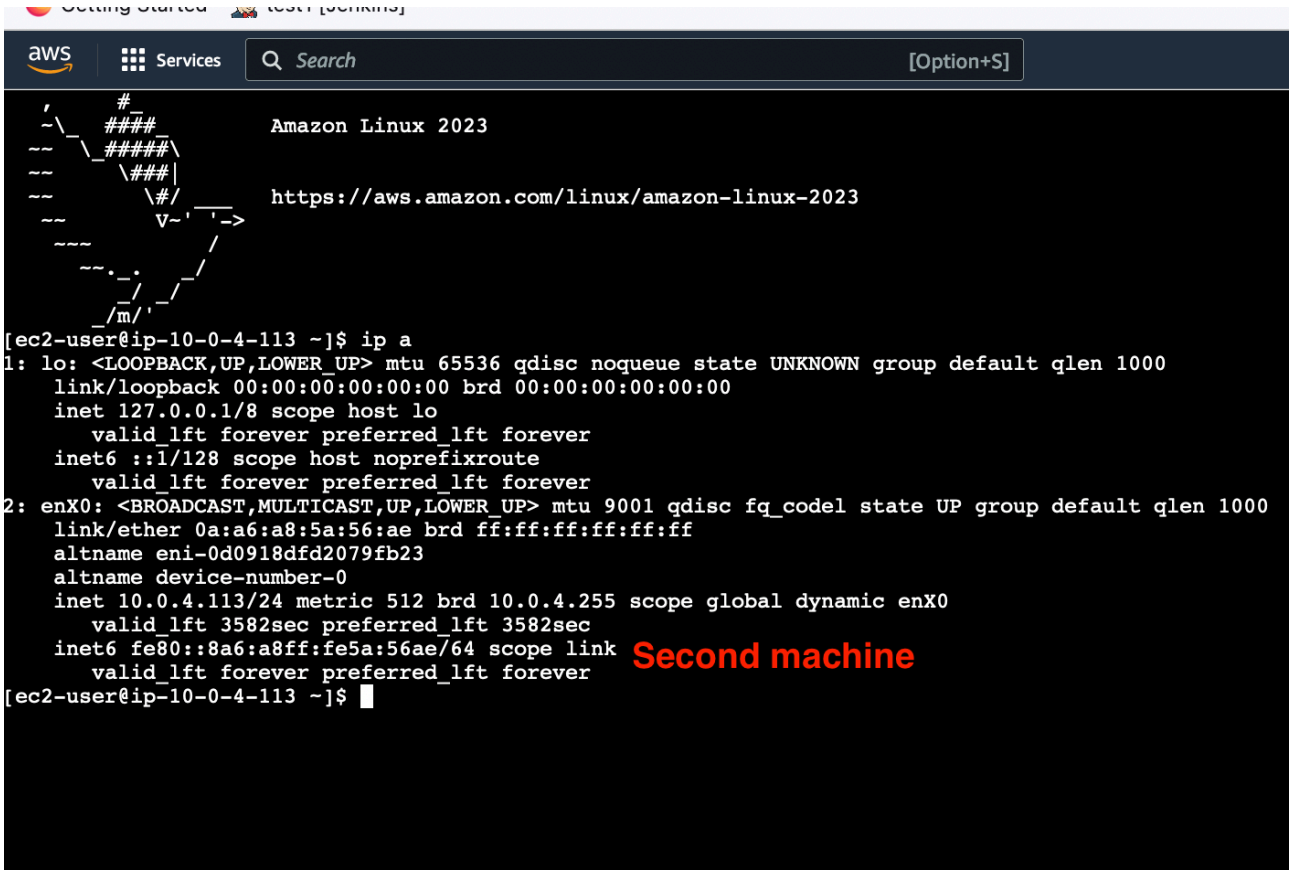




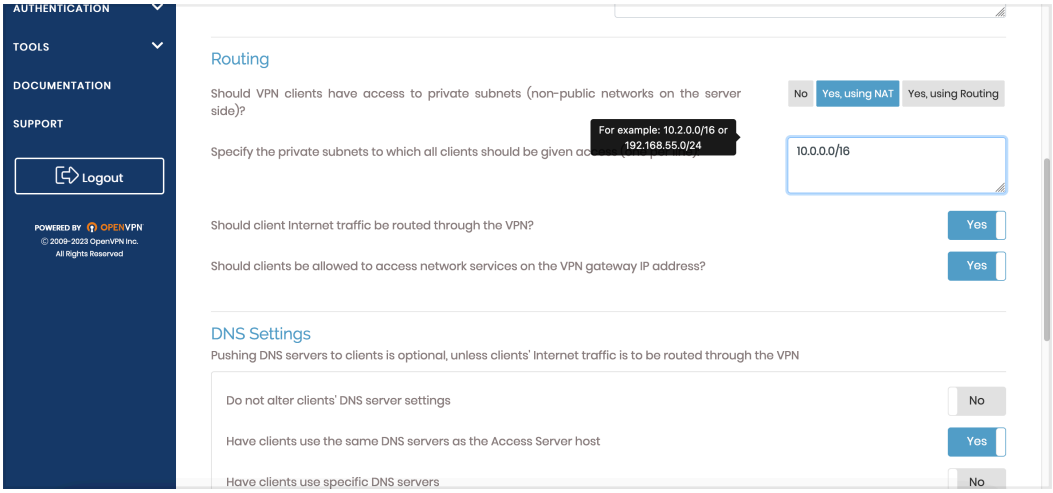
PRIVATE INSTANCE-1



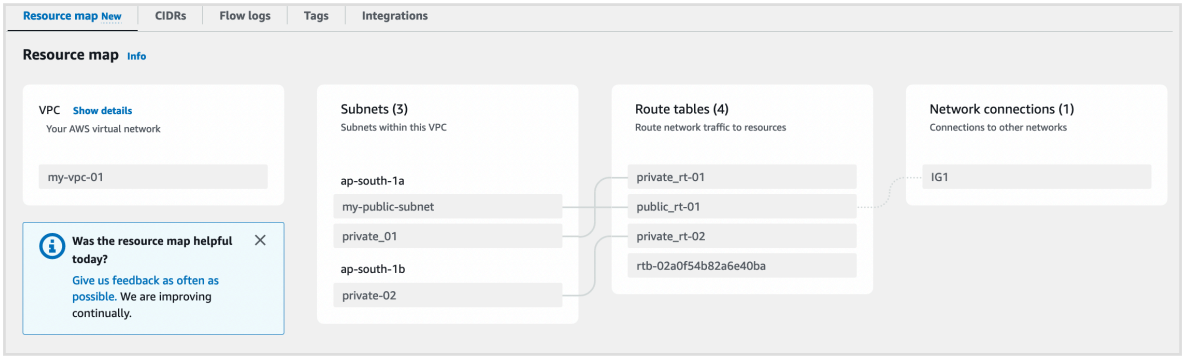
PRIVATE INSTANCE-2



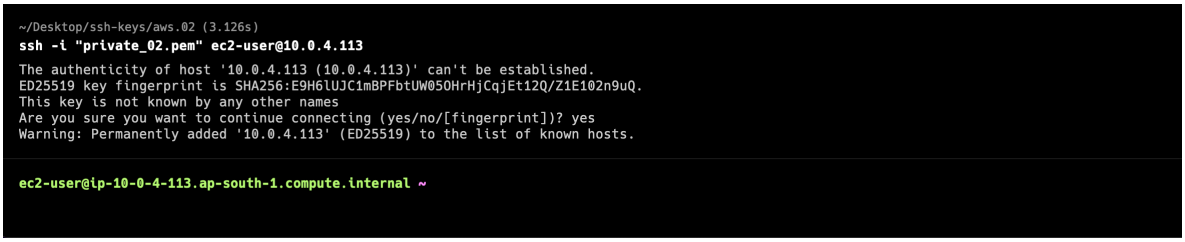
we can see our **private IP range**



My VPC



Instance 1 (private)



Instance 2 (private)


~/Desktop/ssh-keys/aws.02 (3.873s)
ssh -i "private_01.pem" ec2-user@10.0.3.42
The authenticity of host '10.0.3.42 (10.0.3.42)' can't be established.
ED25519 key fingerprint is SHA256:9xsDcrmMz4+GsYNUHCUyrQZEAiWhJWjH9f4Pfmhz3iY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.3.42' (ED25519) to the list of known hosts.
ec2-user@ip-10-0-3-42.ap-south-1.compute.internal ~