Lab Steps

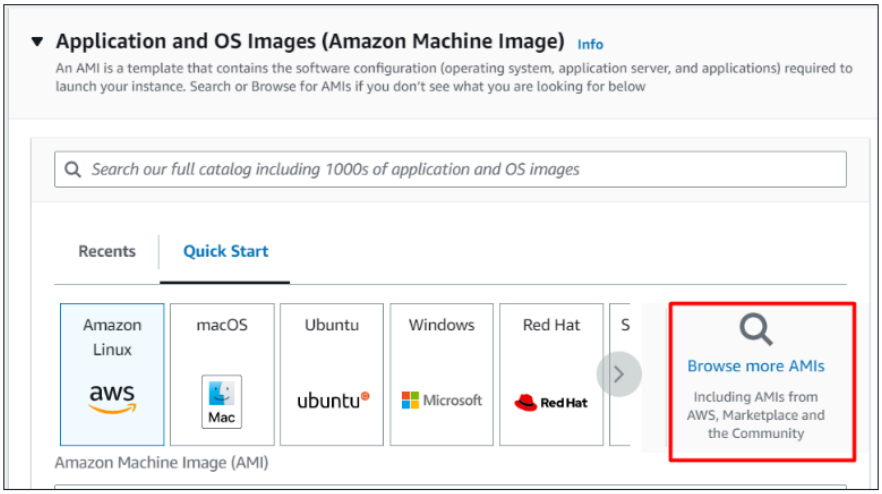
Task 1: Sign in to the AWS Management Console

1. Click on the **Open Console** button, and you will get redirected to AWS Console in a new browser tab.
2. On the AWS sign-in page,
    - Leave the Account ID as default. Never edit/remove the 12-digit Account ID present in the AWS Console. Otherwise, you cannot proceed with the lab.
    - Now copy your **User Name** and **Password** in the Lab Console to the **IAM Username and Password** in the AWS Console and click on the **Sign-in** button.
3. Once Signed In to the AWS Management Console, make the default AWS Region as **US East (N. Virginia) us-east-1.**

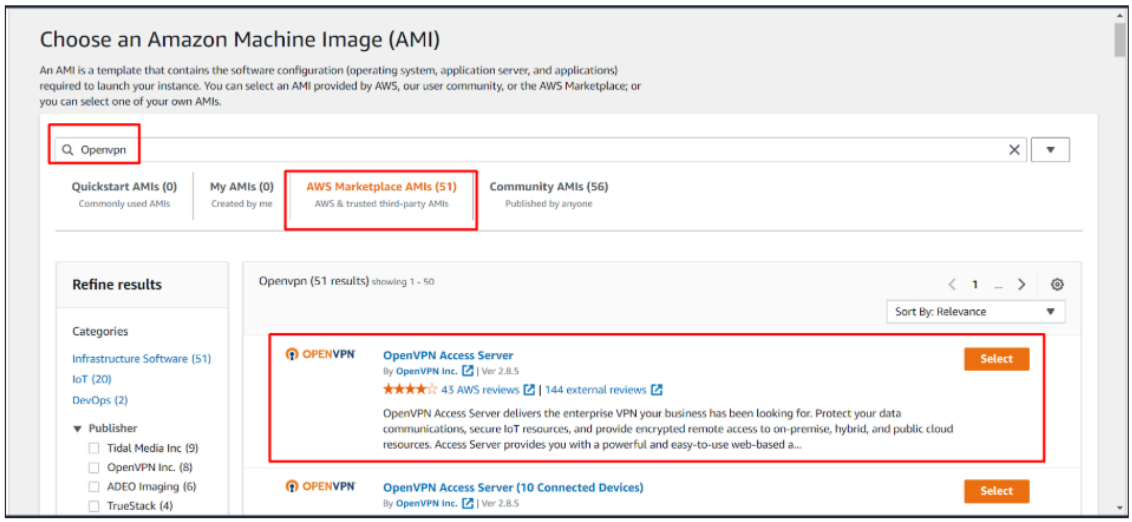
Task 2: Launching an EC2 Instance

In this task, we are going to create and launch an EC2 Instance with the required configurations.

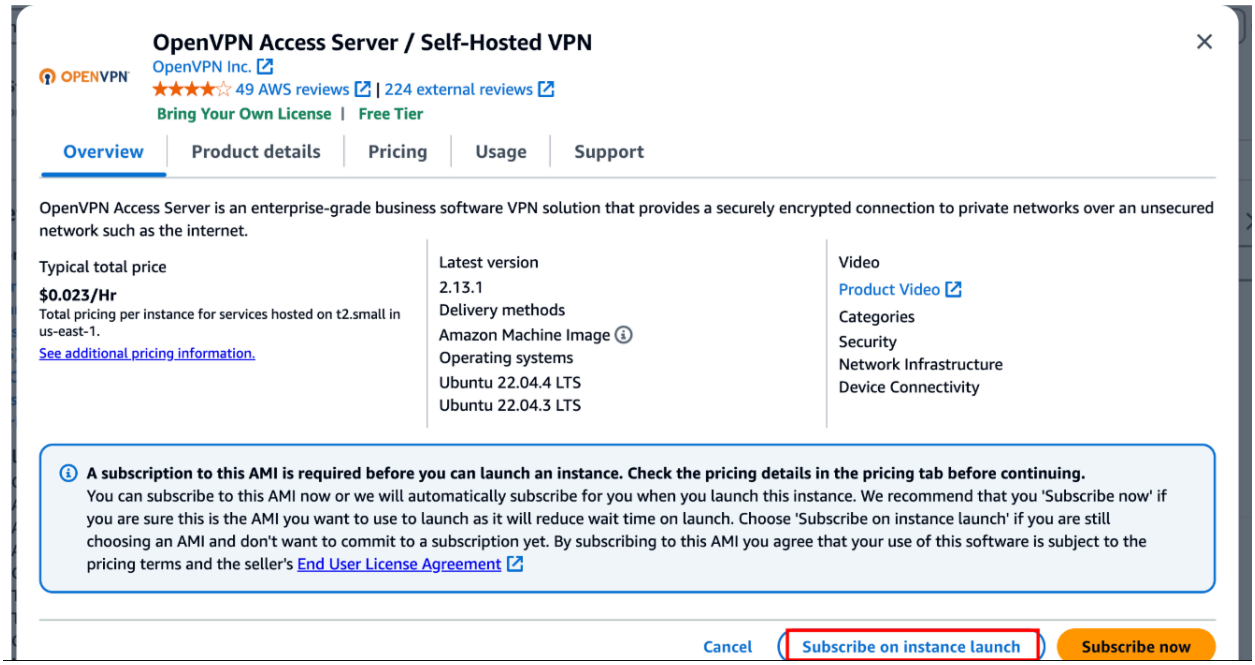
1. Make sure you are in the **N.Virginia** Region.
2. Navigate to **EC2** by clicking on the **Services** menu at the top, then click on **EC2** under **Compute** section.
3. Navigate to **Instances** on the left panel and click on the **Launch Instances** button.
4. Enter Name as **MyVPNServer**
5. **Choose an Amazon Machine Image (AMI):**
    - Click on **Browse more AMIs.**



- Search for **Openvpn** in the search box.
- Click on the **Select** button of the **OpenVPN Access Server**

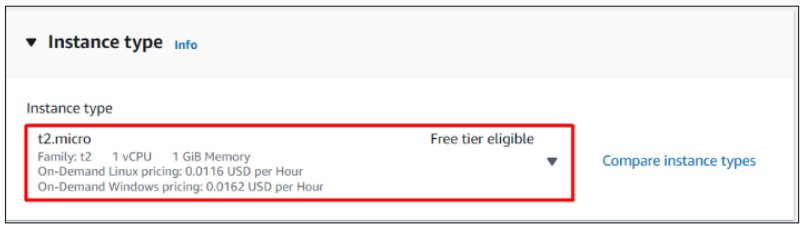


- Click on **subscribe on the instance launch**



- Click on the **Continue** button in the popup window.

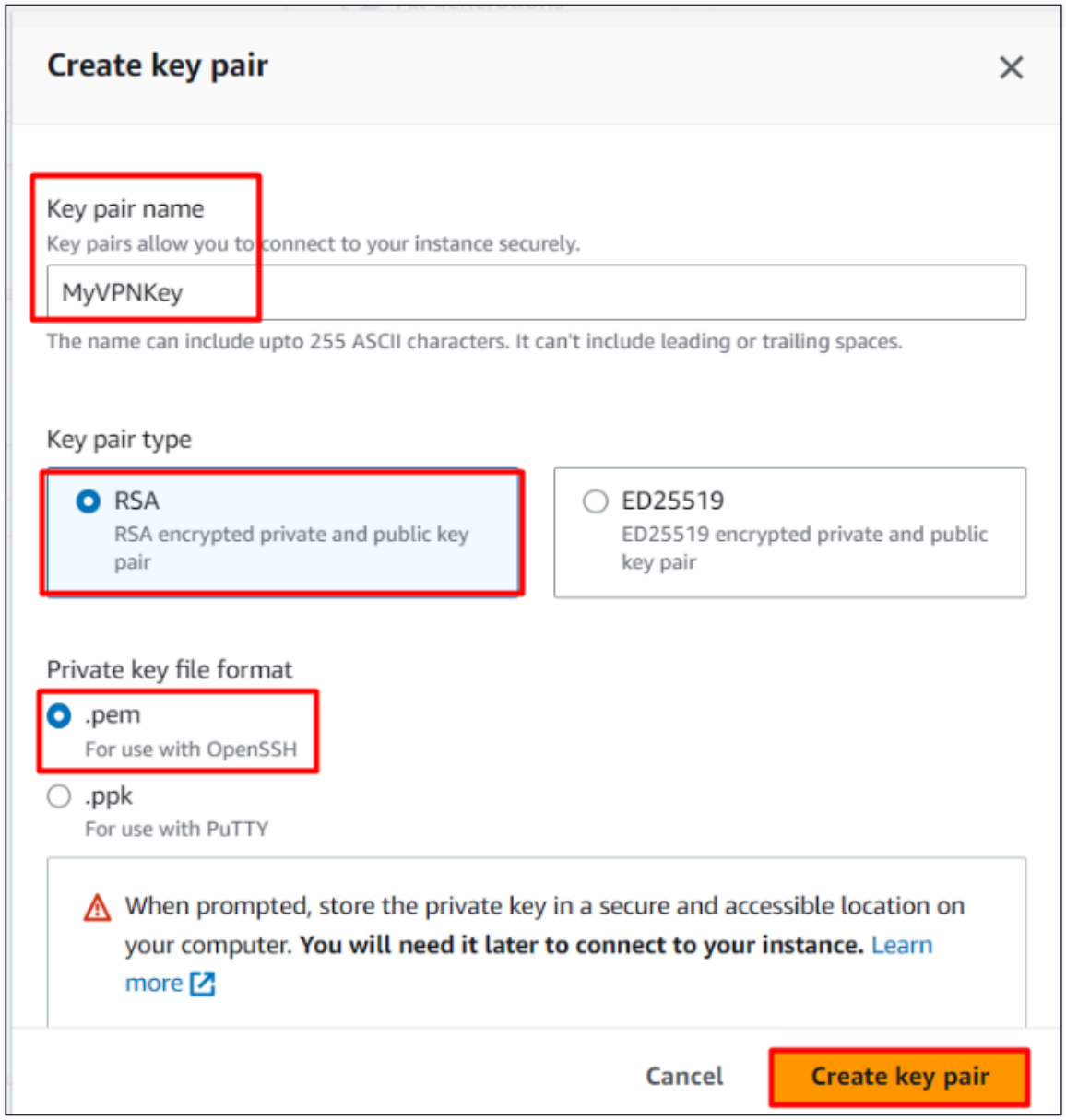
6. Choose an Instance Type: Enter **t2.micro**



Note: Make sure only t2.micro is selected, Else it won't be allowed to launch the EC2 Instance.

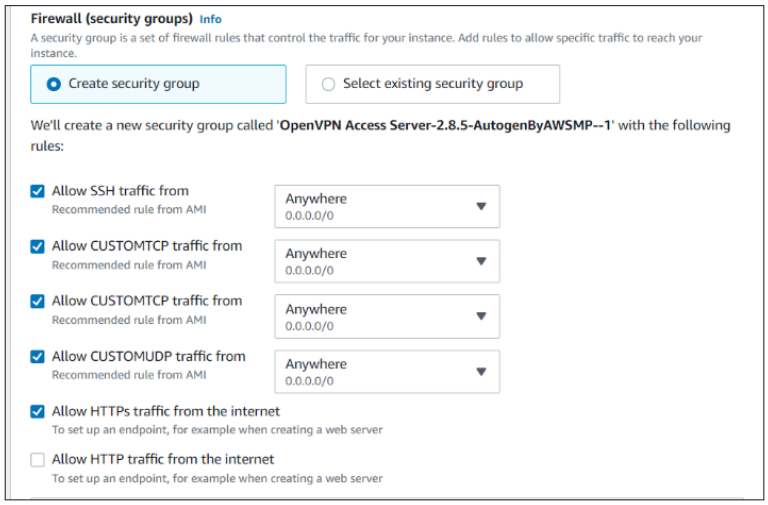
7. **Key Pair:** Choose **Create a new key Pair** hyperlink.

- Key pair name: Enter **MyVPNKey**
- Key Pair Type: Select **RSA**
- Private key file format: Select **.pem**
- Click on the **Create key pair** button to download the key to your local machine.


Create key pair
Key pair name
Key pairs allow you to connect to your instance securely.
MyVPNKey
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
Cancel
Create key pair

8. Under Network Settings:

- The following ports will be automatically enabled :

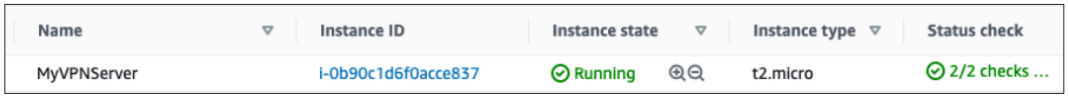


9. Now click on the **Launch Instances** button.

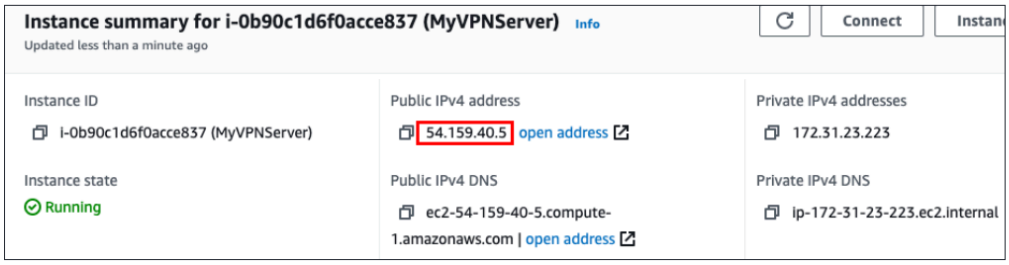
10. Launching a VPN Server may take a few minutes, you may see a message saying that the **Subscription** may take an hour to complete.

11. Scroll down and click on **View Instances** or click to navigate to the instance page

12. **Launch Status:** Your instance is now launching, wait for the complete initialization of the instance till the status changes to **Running.**



13. Now click on the **instance ID** and copy the IPv4 Public IP of this instance and place it in your text editor.



Task 3: SSH into EC2 Instance

- Please note, that the username is **root.** Change the hostname or username to **openvpnas**.
- Please follow the steps to SSH into EC2 Instance.

```
>ssh -i "vpnkey.pem" openvpnas@ec2-54-234-147-103.compute-1.amazonaws.com
Welcome to OpenVPN Access Server Appliance 2.11.3

  System information as of Tue Jun  6 07:39:45 UTC 2023

  System load:  0.00537109375     Processes:             100
  Usage of /:   30.2% of 7.57GB   Users logged in:       0
  Memory usage: 23%               IPv4 address for eth0: 172.31.82.100
  Swap usage:   0%
```

Task 4: Initialize the VPN Server

1. Please enter 'yes' to indicate your argument [no]: Enter **yes**
2. Will this be the primary Access Server node?
    - Press ENTER for default [yes]: Click the **[enter]** button.
3. Please specify the network interface and IP address to be
    - Press Enter for default [1]: Click the **[enter]** button.
4. What public/private type/algorithms do you want to use for the OpenVPN CA?
    - Press ENTER for default [rsa]: Click the **[enter]** button.
5. What key size do you want to use for the certificates?

- Press ENTER for default [2048]: Click the **[enter]** button.

6. What public/private type/algorithms do you want to use for the self-signed web certificate?

   - Press ENTER for default [rsa]: Click the **[enter]** button.

7. What key size do you want to use for the certificates?

   - Press ENTER for default [2048]: Click the **[enter]** button.

8. Please specify the port number for the Admin Web UI.

   - Press ENTER for default [943]: Click the **[enter]** button.

9. Please specify the TCP port number for the OpenVPN Daemon

   - Press ENTER for default [443]: Click the **[enter]** button.

10. Should client traffic be routed by default through the VPN?

    - Press ENTER for default [no]: Click the **[enter]** button.

11. Should client DNS traffic be routed by default through the VPN?

    - Press ENTER for default [no]: Click the **[enter]** button.

12. Should private subnets be accessible to clients by default?

- Press ENTER for default [yes]: Click the **[enter]** button.

13. Do you wish to log in to the Admin UI as "openvpn"?

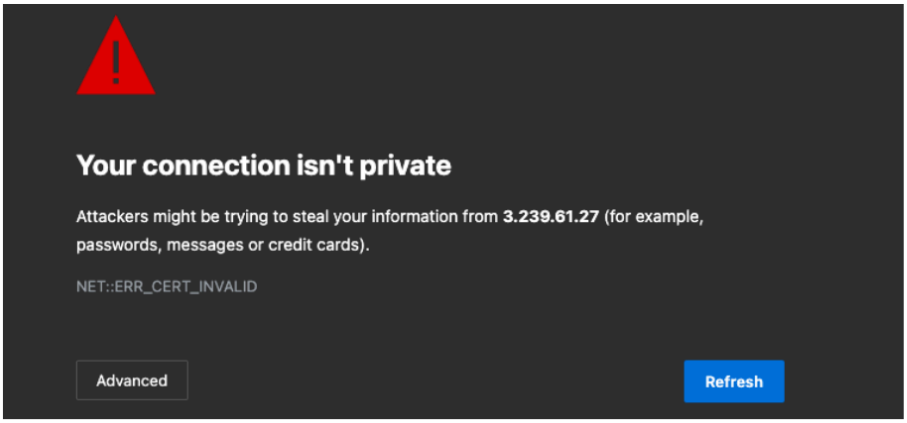
- Press ENTER for default [yes]: Click the **[enter]** button.
- Type a password for the 'openvpn' account: Enter **Whizvpn123@** and press **[enter]** and then enter the same password to confirm the password.

14. Please specify your Activation key (or leave blank to specify later): Click the **[enter]** button.

```
Initial Configuration Complete!

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

https://100.24.42.33:943/admin

During normal operation, OpenVPN AS can be accessed via these URLs:
Admin  UI: https://100.24.42.33:943/admin
Client UI: https://100.24.42.33:943/
To login please use the "openvpn" account with  the password you specified during the setup.

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

15. Now login as administrator, open Google Chrome and paste the following URL

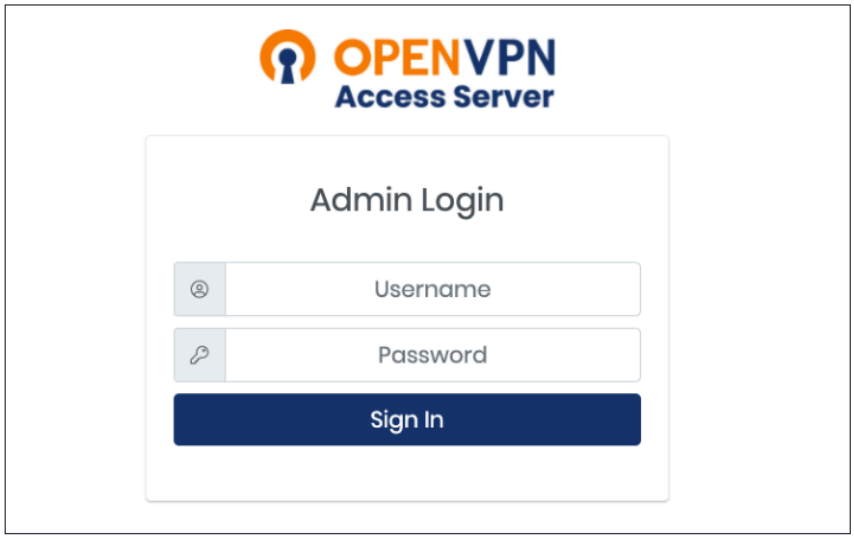
- Syntax : https://<IPv4 Public IP>:943/admin/
- Example: https://3.239.61.27:943/admin/
- Now you will get a Warning message **Your connection isn't private**, this is because we are not using any SSL certificate for this connection.



- Click on the **Advanced** Button and see if you have a **proceed to website** option then click on the link.
- If you see the below message instead, then type **thisisunsafe** on the keyboard and the page will automatically reload.

You cannot visit 100.26.97.202 at the moment because the website sent scrambled credentials that Google Chrome cannot process. Network errors and attacks are usually temporary, so this page will probably work later.

- You will see a login page like this :



16. Login to the VPN Admin page :

    - Username: Enter **openvpn**
    - Password: Enter **Whizvpn123@**
    - Now click on the **Sign in** button.

17. Now On the License Agreement page click on the **Agree** button.

18. Click on the **VPN Settings** option in the left-side menu.

19. To make sure all the internet traffic goes through the VPN, Under **Routing**

    - Should client Internet traffic be routed through the VPN? : Switch the button to **Yes**

20. Now scroll down and click on the **Save settings** button.

Task 5: Connect to the VPN

1. Open a new tab in the Google Chrome browser.
2. Paste the url **https://**<IPv4 Public IP>**/** Example : https://100.26.97.202/

3. Login to the VPN User Page :

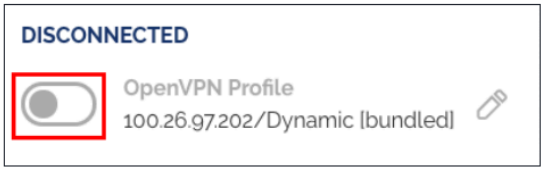
- Username: Enter **openvpn**
- Password: Enter **Whizvpn123@**
- Now click on the **Sign in** button.

4. Now, based on which operating system you are using, download the VPN connector and install it on your local machine.

5. Open the OpenVPNConnector application and if you see **Onboarding Tour**, just close it.

6. Now again, agree to the terms and conditions.

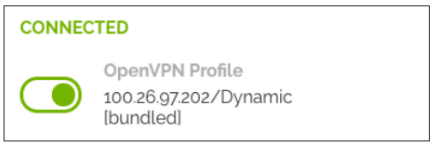
7. You will be able to see a pre-configured VPN profile, turn on this connection.



8. Now again enter the username and password.

- Username: Enter **openvpn**
- Password: Enter **Whizvpn123@**
- Click on the **OK** button.

9. Now you are connected to the VPN



10. Now you can start browsing using a VPN connection.

DO You Know?

OpenVPN is widely used and trusted by organizations and individuals worldwide for its robust security features, including encryption, authentication, and data integrity. It provides a flexible and scalable solution for establishing secure connections, making it suitable for various use cases, such as remote access to corporate networks, securing public Wi-Fi connections, and creating secure communication channels between different cloud environments.

Completion and Conclusion

1. You have successfully created and launched the Amazon EC2 Instance.
2. You have successfully logged into an EC2 instance by SSH.
3. You have successfully Initialized the VPN Server.
4. You have successfully connected to the VPN.