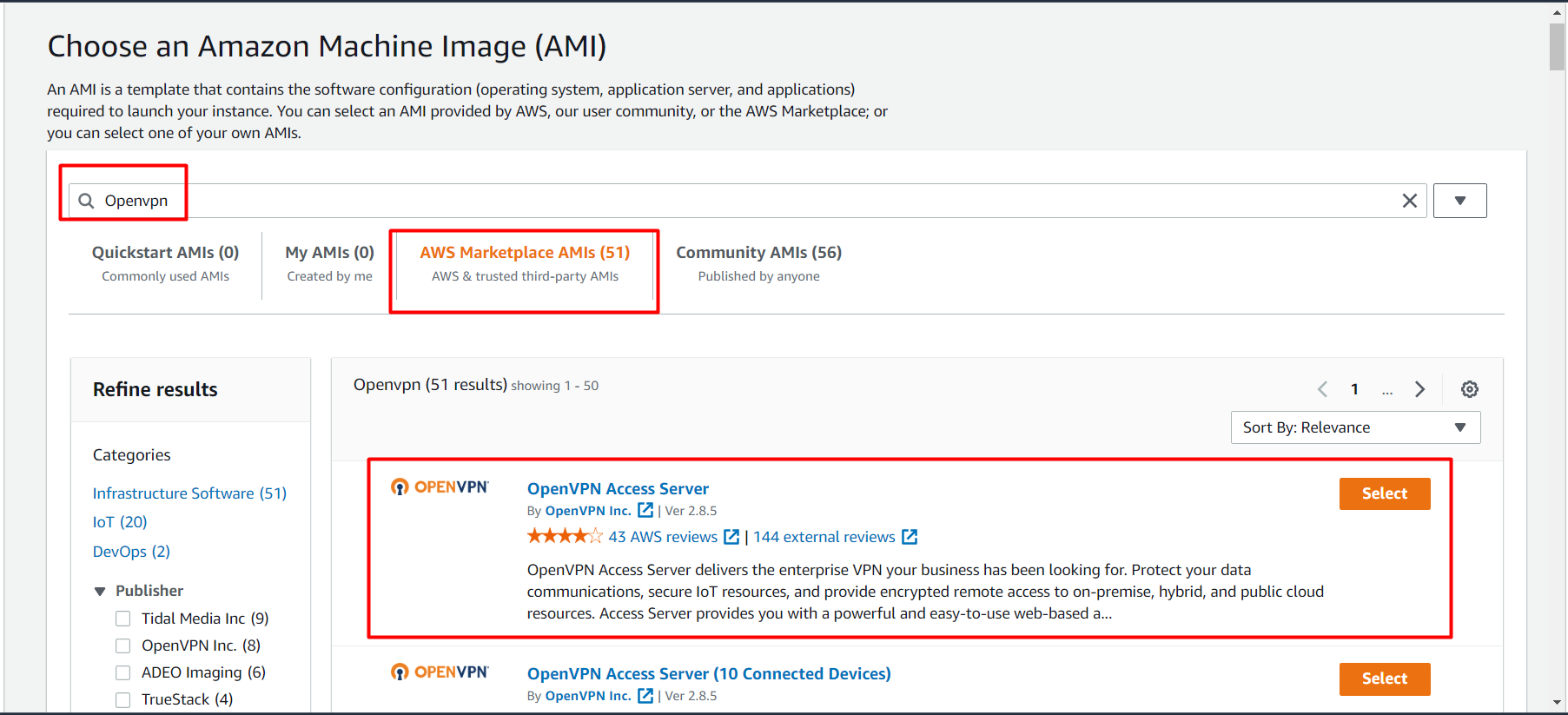
**Lab Steps**

Task 1: Sign in to AWS Management Console

1. Click on the  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 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.**

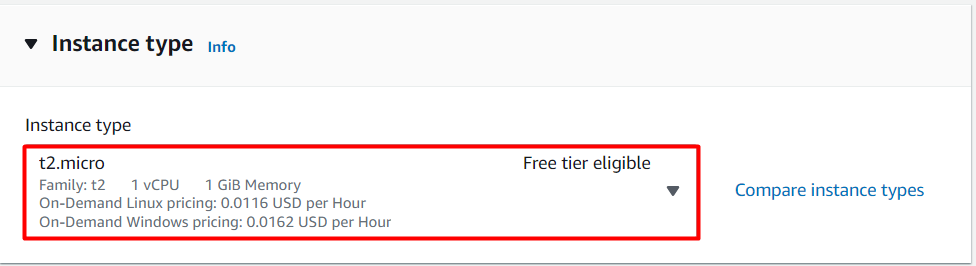
Task 2: Launching an EC2 Instance

1. Make sure you are in the **N.Virginia** Region.
2. Navigate to **EC2** by clicking on the **Services** menu in the top, then click on **EC2** under **Compute** section.
3. Navigate to  on the left panel and click on 
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 .



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

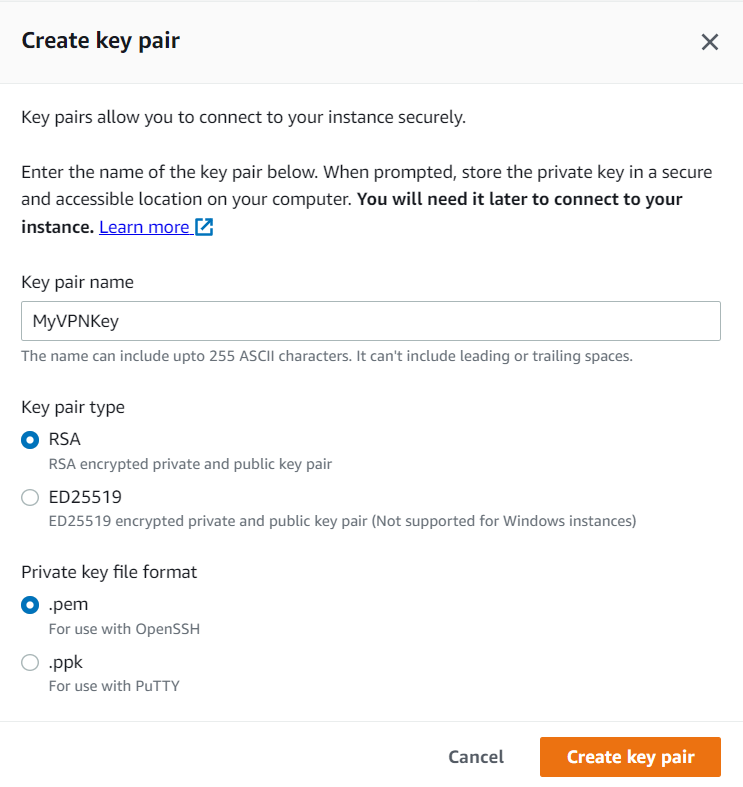
1. Choose an Instance Type: Enter **t2.micro**



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

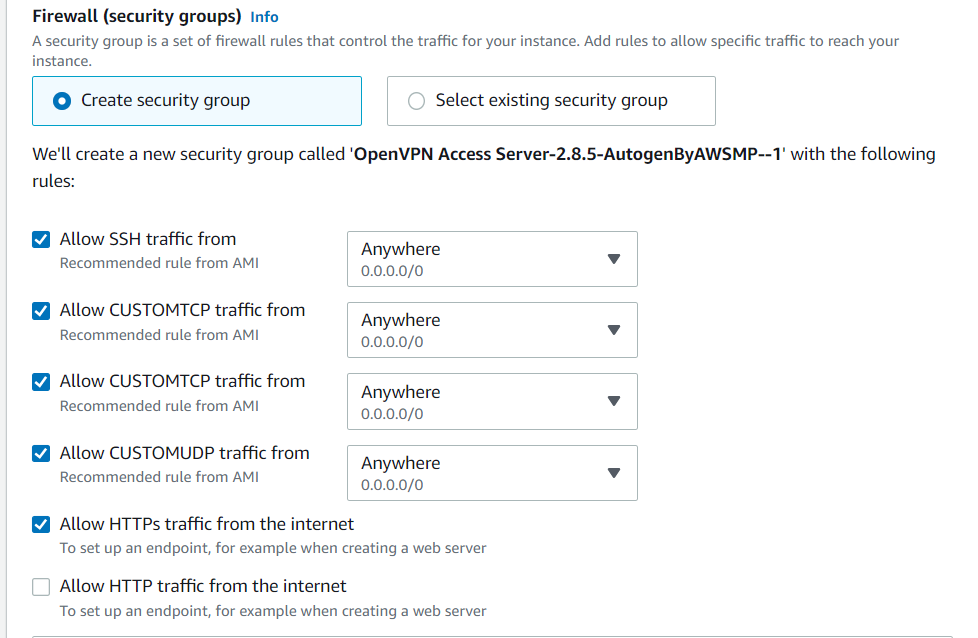
6.  **Key Pair :**Choose **Create a new key Pair** from the dropdown list.

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



         7. Under Network Settings , Click on **Edit**button.

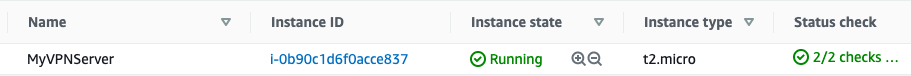
* The following ports will be automatically enabled :



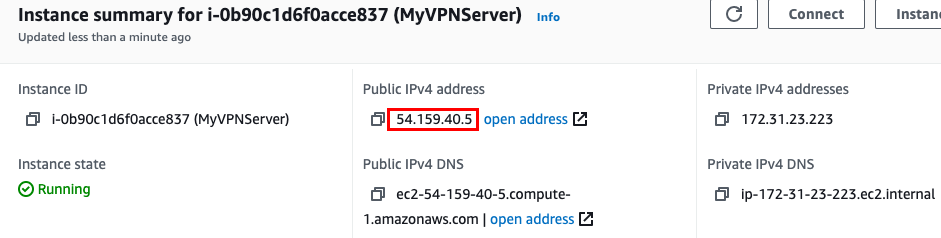
     8. Now click on the **Launch Instances** button.

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

1. Scroll down and click on **View Instances**or click to navigate to the instance page
2. **Launch Status:** Your instance is now launching, wait for complete initialization of instance till status change to .



    12. 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

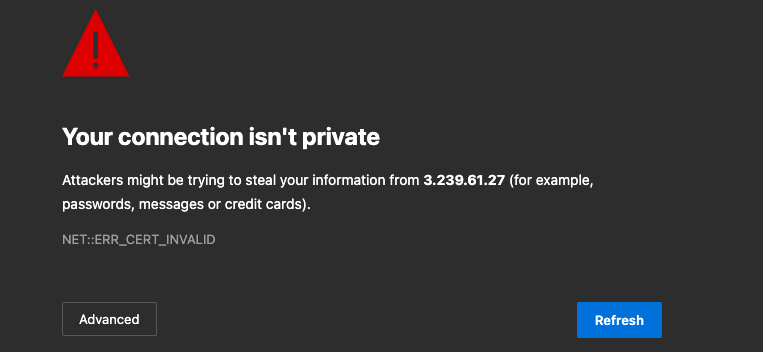
* Please note the username is **root**
* Please follow the steps to [SSH into EC2 Instance](https://www.whizlabs.com/labs/support-document/ssh-into-ec-instance).

Task 4: Initialize the VPN Server

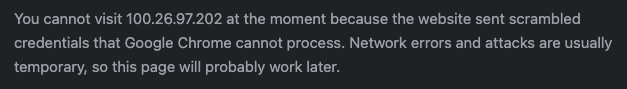
1.  : Enter **yes**
2. Will this be the primary Access Server node?
   *  : Click the **[enter]** button.
3. Please enter the option number from the list above (1-2).
   *  : Click the **[enter]** button.
4. Please specify the port number for the Admin Web UI.
   *  : Click the **[enter]** button.
5. Please specify the TCP port number for the OpenVPN Daemon
   *  : Click the **[enter]** button.
6. Should client traffic be routed by default through the VPN?
   *  : Click the **[enter]** button.
7. Should client DNS traffic be routed by default through the VPN?
   *  : Click the **[enter]** button.
8. Use local authentication via internal DB?
   *  : Click the **[enter]** button.
9. Should private subnets be accessible to clients by default?
   *  : Click the **[enter]** button.
10. Do you wish to login to the Admin UI as "openvpn"?
    *  : Click the **[enter]** button.
11.  : Click the **[enter]** button.
12. Once the configuration is completed, you will be automatically logged out the server connection. Next time to login you should use **openvpnas** as user name instead of **root**.
13. Now again [SSH into EC2 Instance](https://www.whizlabs.com/labs/support-document/ssh-into-ec-instance) but the user name is **openvpnas**
    * **Note** : when you create the EC2 instance the initial password to SSH into the instance is **root**, later when you configure the VPN in the above step the username  is changed to **openvpnas**
14. Set a login password
    * sudo passwd openvpn
    * Enter new UNIX password :  Enter **whizlabsvpn**
    * Retype new UNIX password : Enter **whizlabsvpn**
    * **Note** : **openvpn** is the default user login name present in the server to connect to the VPN and we set **whizlabsvpn** as its password.
15. Now login as administrator, open Google Chrome and paste the following url
    * Syntax :

https://<IPv4 Public IP>:943/admin/

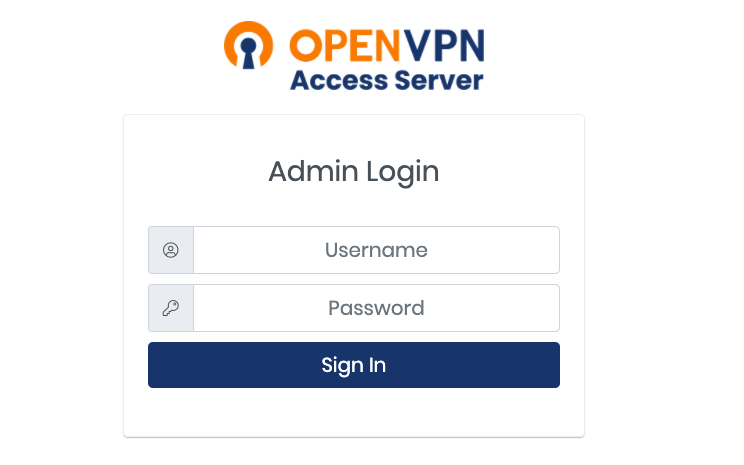
* + Example : https://3.239.61.27:943/admin/
  + Now you will get a Warning message **Your connection isn't private**, this is because we are not using any SSL certificate for this connection.



* Click on the  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** in the keyboard and the page will automatically reload.



* You will see a login page like this :



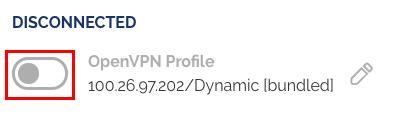
1. Login to the VPN Admin page :
   * Username : Enter ***openvpn***
   * Password : Enter ***whizlabsvpn***
   * Now click on the 
2. Now In the License Agreement page click on the 
3. Click on the  option in the left side menu.
4. To make sure all the internet traffic goes through the VPN, Under 
   * Should client Internet traffic be routed through the VPN? : Switch the button to **Yes**



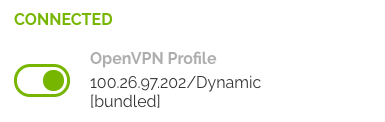
1. Now scroll down and click on the 

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 ***whizlabsvpn***
   * Now click on the 
4. Now Based on which Operating system you are using download the VPN connector and install it in your local machine.
5. Open the OpenVPNConnector application and if you see  just close it.
6. Now again Agree the terms and conditions.
7. You will be able to see a pre configured VPN profile, turn on this connection.



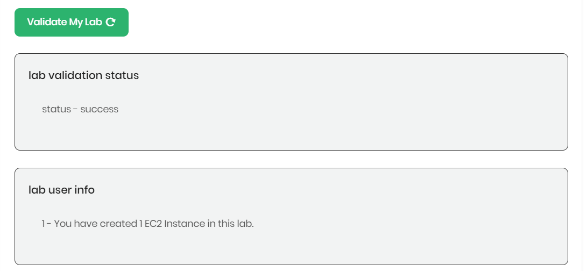
1. Now again enter the username and password.
   * Username : Enter ***openvpn***
   * Password : Enter ***whizlabsvpn***
   * Click on the  button.
2. Now you are connected to the VPN



1. Now you can start browsing using VPN connection.

Task 6: Validation Test

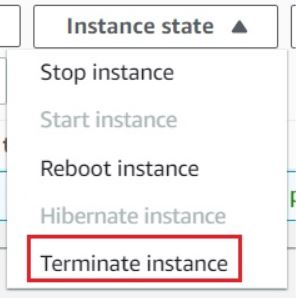
1. Once the lab steps are completed, please click on the  button on the left side panel.
2. This will validate the resources in the AWS account and displays whether you have completed this lab successfully or not.
3. Sample output :



**Task 7: Delete AWS Resources**

Delete EC2 Instance

1. Make sure you are in the **US East (N. Virginia)**Region.
2. Navigate to **EC2** by clicking on the **Services** menu in the top, then click on **EC2** under **Compute** section.
3. Now select the EC2 instance that you have created, click on **Instance State** and click on the **Terminate** **instance**option.



1. Click on **Terminate** button and your EC2 will start terminating.

**Completion and Conclusion**

1. You have successfully created and launched 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.

**End Lab**