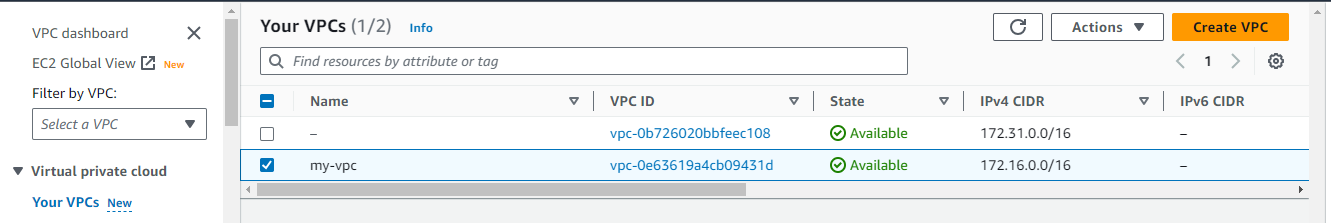
**AWS Client VPN Documentation**

🡺

Step 1:-

Do firstly login aws account and go to VPC session.

And create your VPC and Then gave it subnet ranges.



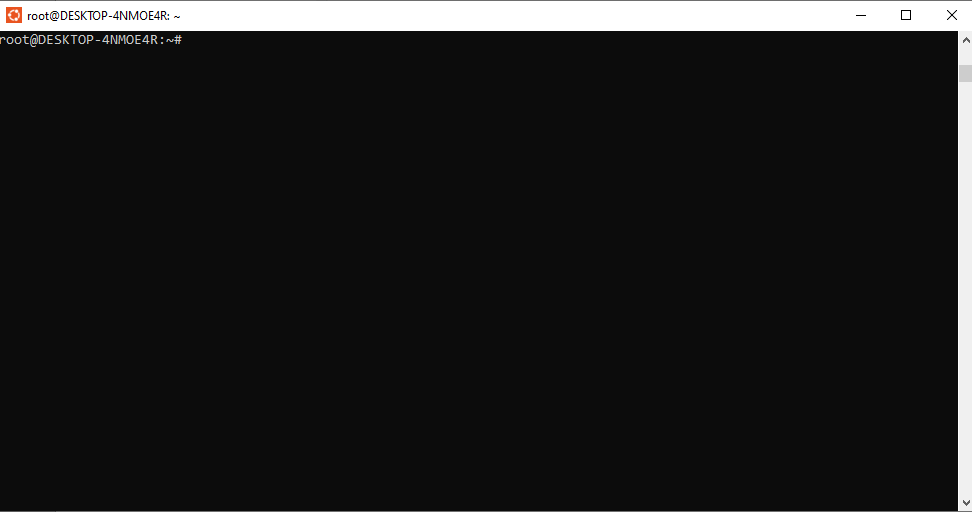
Step 2:-

now you have to gave private access to your client by client-VPN so go to on premises server.

this is link to configure the SSL certificate by cli so go to following link get commands.

<https://docs.aws.amazon.com/vpn/latest/clientvpn-admin/mutual.html>

see following I was login to my on premises machine to create server and client certificate.

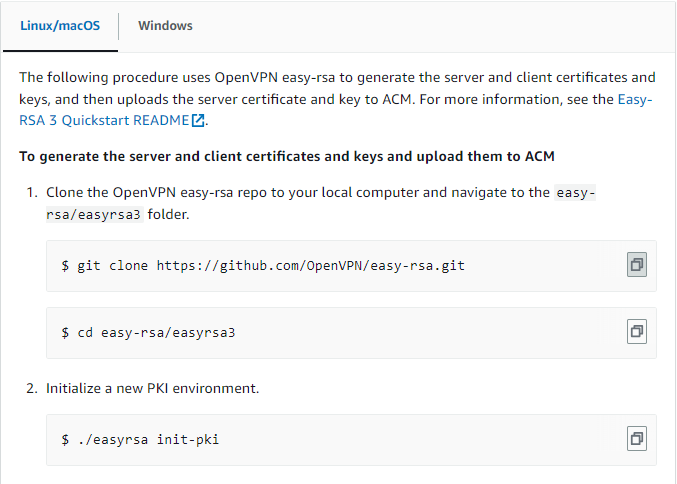


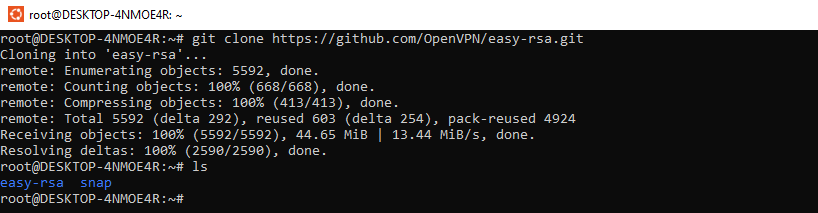
Step 3:-

Click on that link so there was two types you can create certificate of server and client.

I choose LINUX so first copy the firsts command to download openVPN package.

See the following ss I was download openVPN package on my machine.

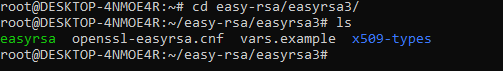




Step 4:-

Now you have to go to navigate to the easy-rsa/easyrsa3 folder.

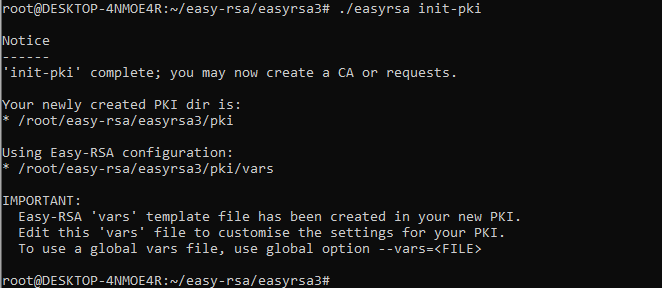
Run command #cd easy-rsa/easyrsa3



Step 5:-

After that you have initialize PKI environment so run command for that

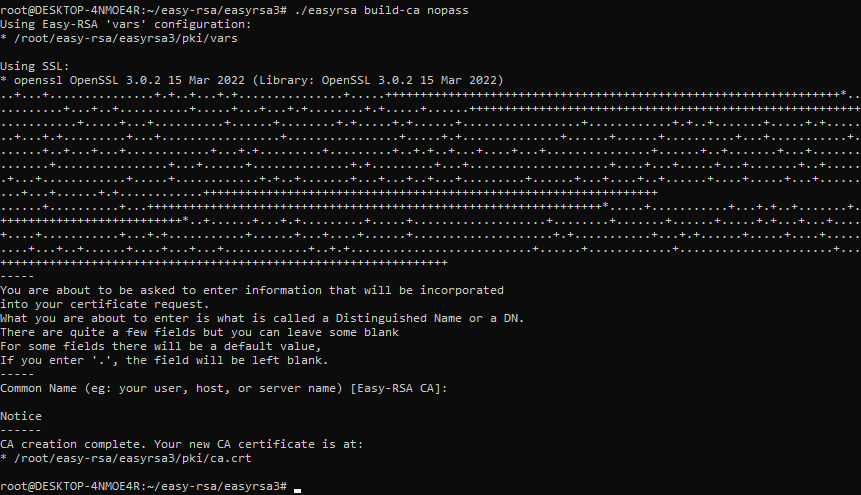
# ./easyrsa init-pki



Step 6:-

To build a new certificate authority (CA), run this command and follow the prompts.

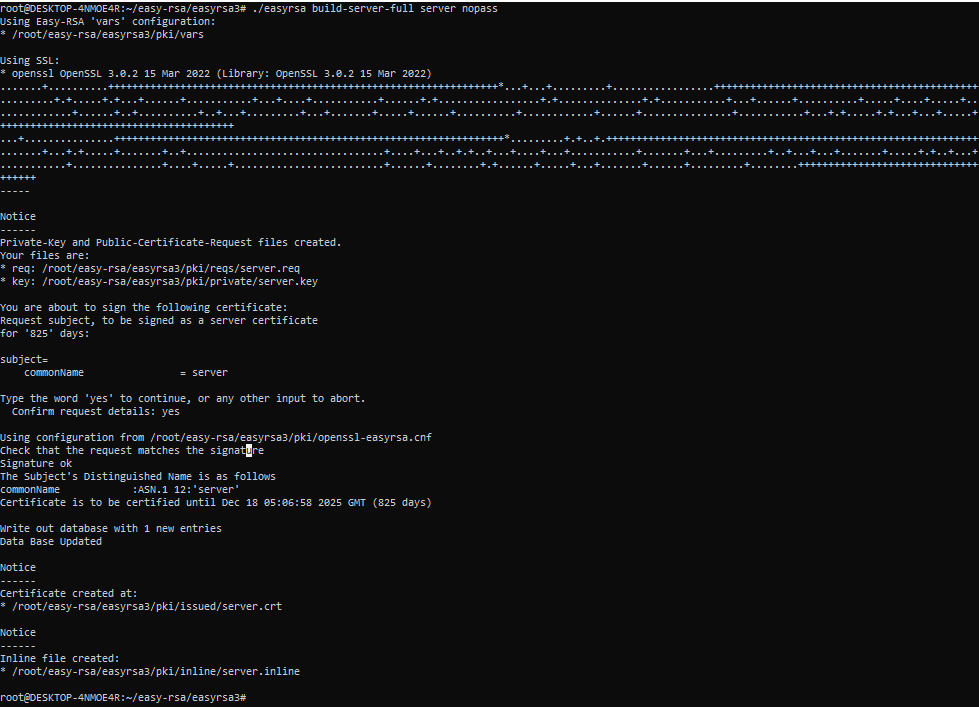
# ./easyrsa build-ca nopass



Step 7:-

After that Generate the server certificate and key. So run following command

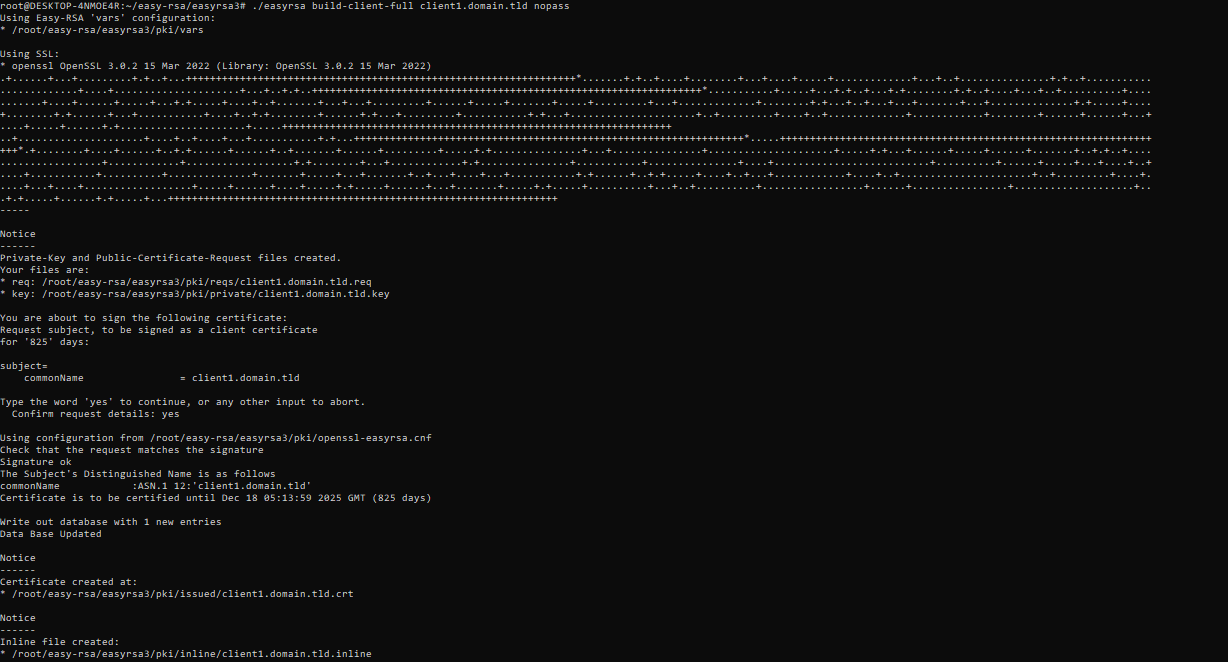
# ./easyrsa build-server-full server nopass



Step 8:-

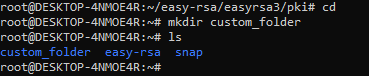
After that you have to Generate the client certificate and key. So run the following command

./easyrsa build-client-full client1.domain.tld nopass



Step 9:-

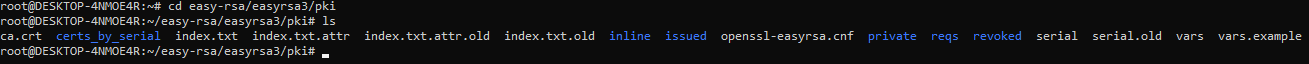
Now your key was stored in PKI directory with different places and different names so get that all certificates and keys to one folder. So first name one directory as name custom\_folder in users home directory.



Step 10:-

Now got directory PKI where the all keys and certificates was stored.

#cd easy-rsa/easyrsa3/pki



Step 11:-

After that copy one by one certificate and keys to custom\_folder directory.

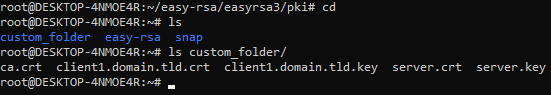






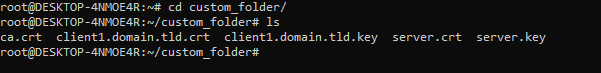






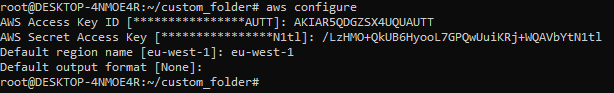
Step 12:-

Now go to cutom\_folder.



Step 13:-

Now we have to send certificate and keys to amazon certificate manager. Before that you have to aws configure of user which have permission or access of Amazon certificate manager service. And gave region name in which you to send certificate and key.



Step 14:-

After that send keys and certificate to ACM service.

By following command ,

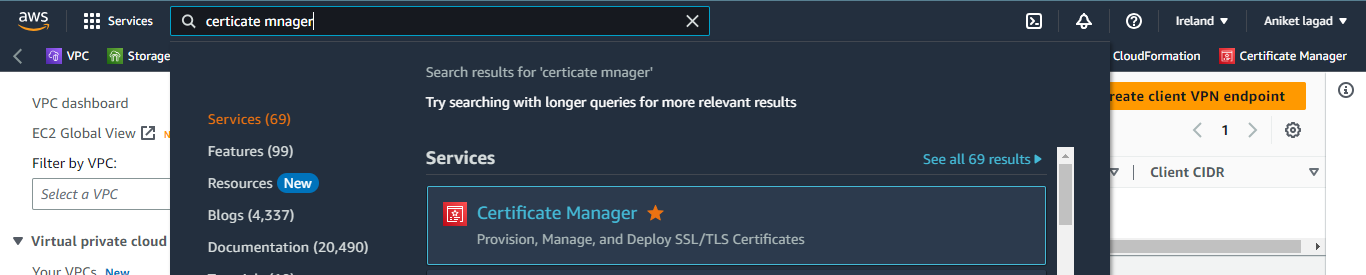
aws acm import-certificate --certificate fileb://server.crt --private-key fileb://server.key --certificate-chain fileb://ca.crt (this command for send sever key and certificate)

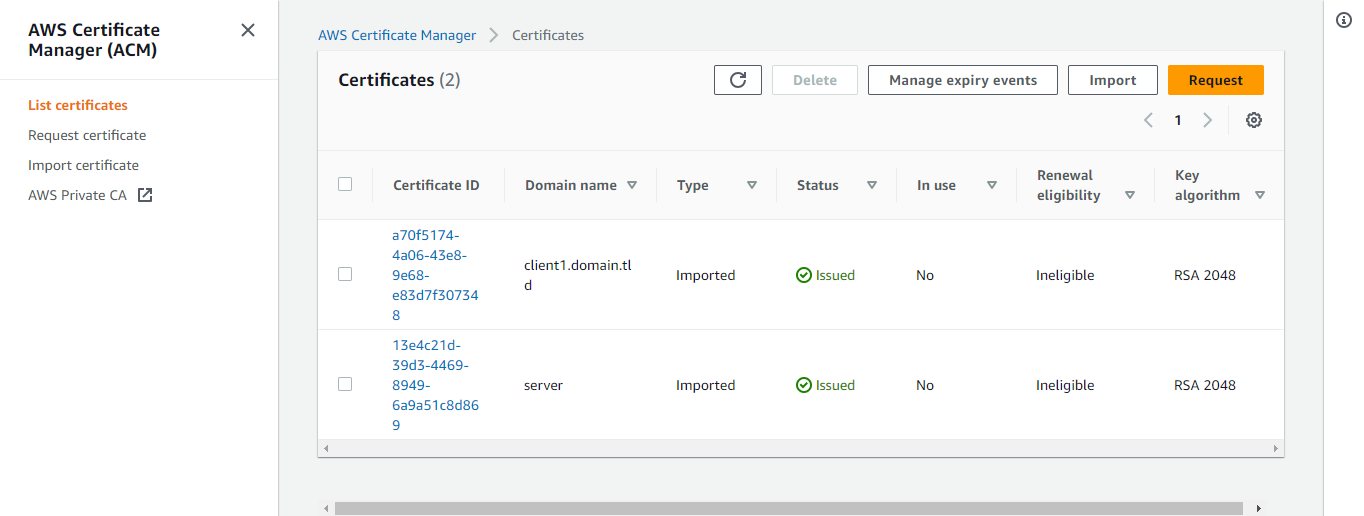
aws acm import-certificate --certificate fileb://client1.domain.tld.crt --private-key fileb://client1.domain.tld.key --certificate-chain fileb://ca.crt (this command for send client key and certificate)



Step 15:-

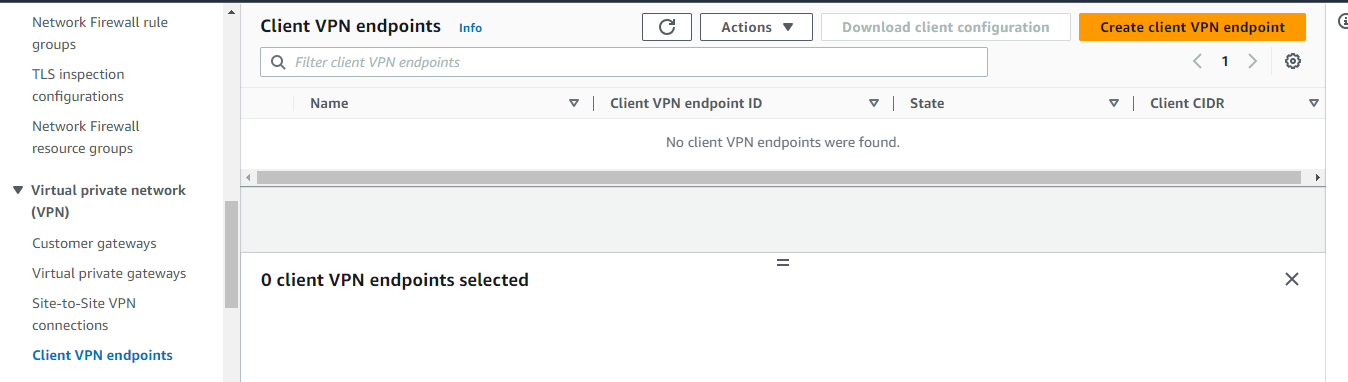
Now go aws console and search certificate manager service and then check there certificate was uploaded or not.





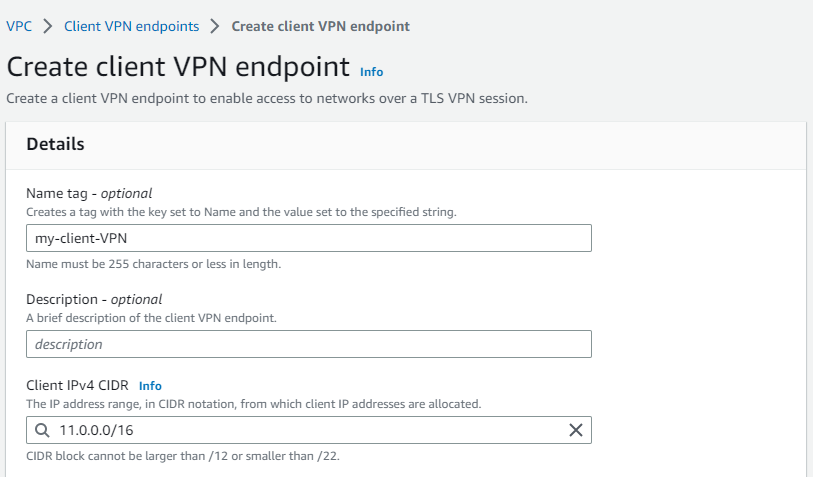
Step 16:-

Now go to your vpc service and in VPC got VPN session and click on client endpoint. And next click on create client VPN endpoint.



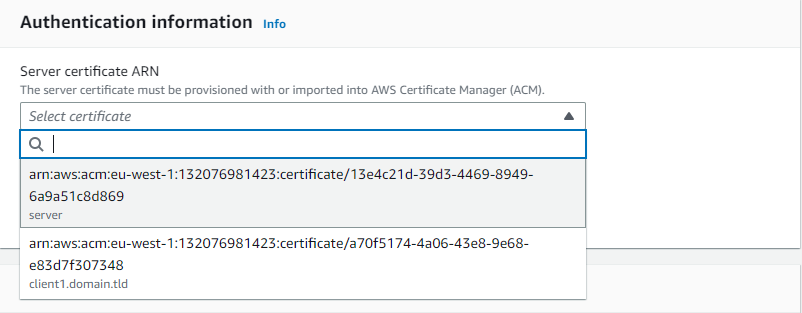
Step 17:-

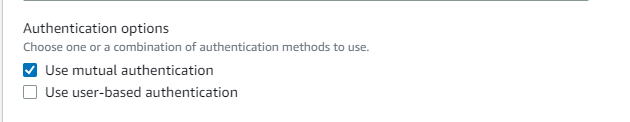
After that you will see the create client VPN endpoint setting so gave it name first and then gave it description if you want to gave and then gave IP range any but remember one thing gave ip range different from VPC IP.

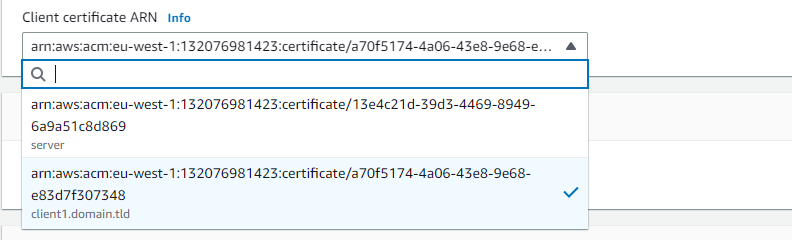


Step 18:-

Then now your have to select sever certificate ARN and then as server certificate select and after that next select authentication option is use mutual authentication and then select client certificate ARN and scroll down.

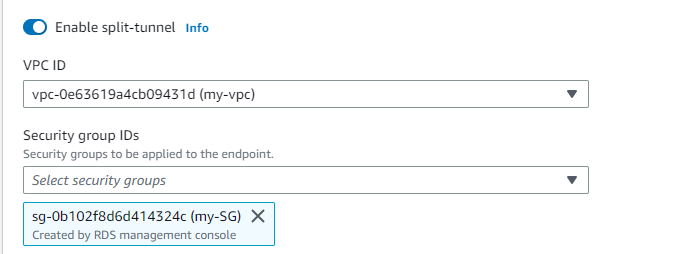






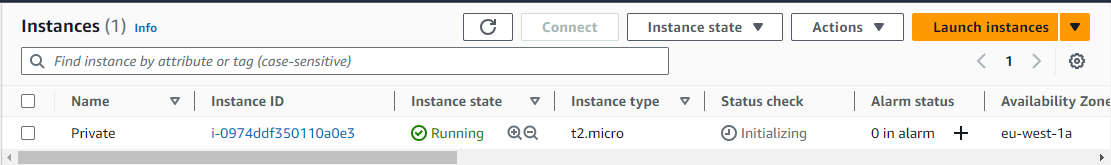
Step 19:-

And now select enable split-tunnel and then select your VPC and after that select security group. and then click on create client VPN endpoint. Wait for 10 to 15 minute to active. Till that active setting up other.



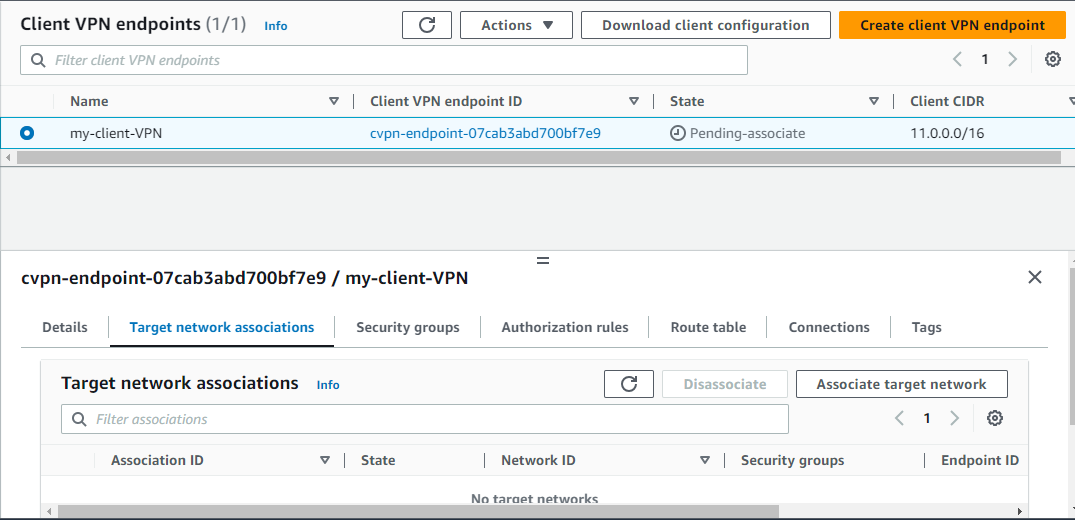
Step 10:-

Now launch private instance to check connection was created or not when process was done. So first go to ec2 service and create a private instance with your selected VPC. And in security group instance add all ICMP ipv4 address this port is used for ping.



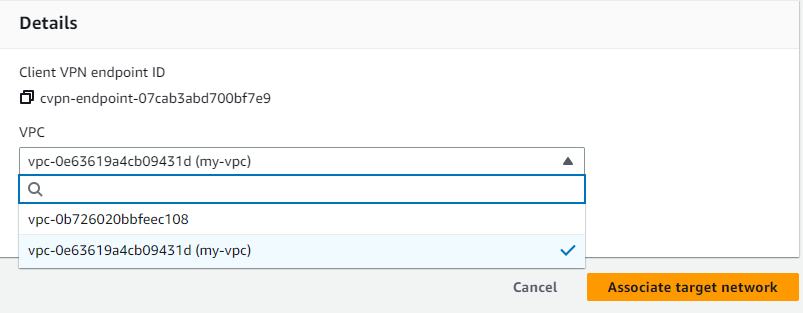
Step 11:-

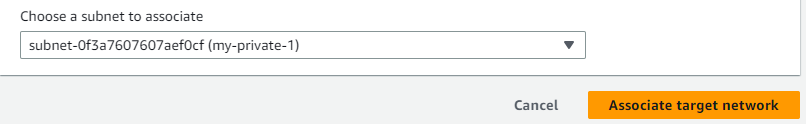
After that select your created client VPN endpoint and then click on option target network association to associate subnets to create connection with them with the help of VPN.



Step 12:-

Now you will see the information of associate target network and then first select your vpc and then select subnet which you have to create instance or subnet which you have create connection. And then click on associate target network.

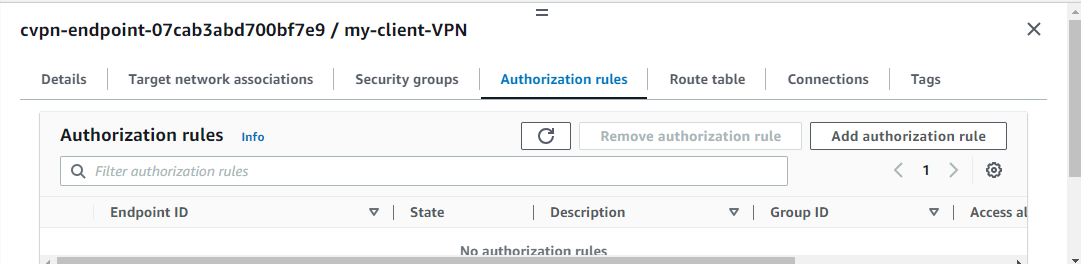


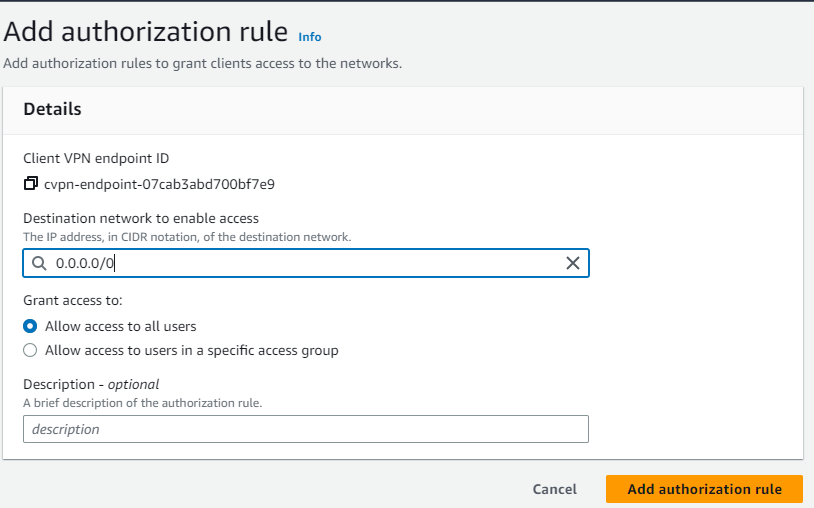


Step 13:-

Now select option authorization rule and click on add authorization rule.

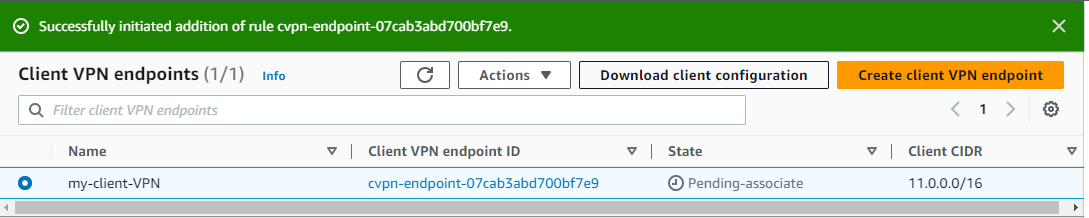
After that you will see add authorization rule setting so first gave IP address of destination but I will select 0.0.0.0/0 and then select allow access to all users so any one can connect with my instance. And then click on add authorization rule.

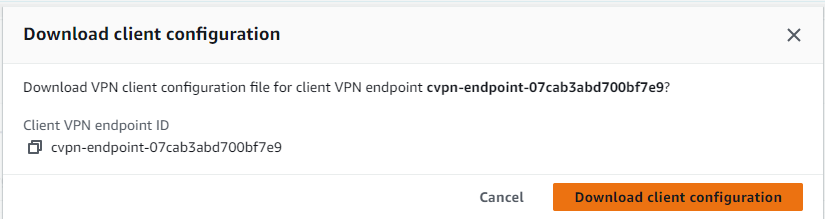




Step 14:-

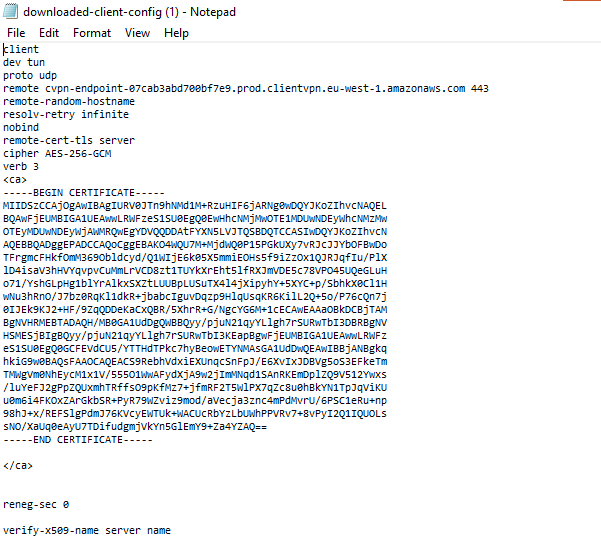
After that download client configuration so we can add in that certification of client to add in that keys. And then click on download. After that that configuration was download on your windows.





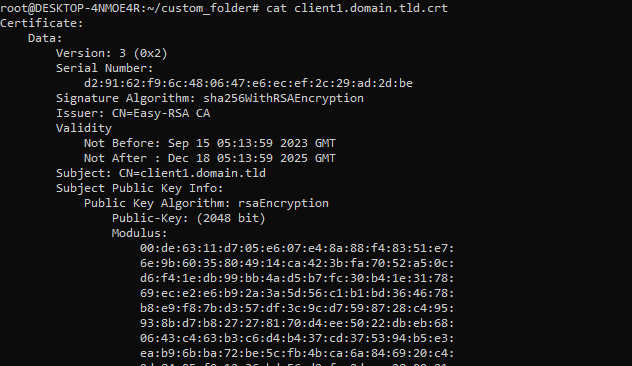
Step 15:-

Open that downloaded configuration file. You will see the certificate of sever so after </ca> this you have to open <cert> and then hit enter and then close</cert>. and in the middle of open and close “cert” you have to paste the certificate which you have crated on premises machine. So go to on premises.



Step 16:-

Copy all data of that certificate and then go to that client configuration file and paste in the open and close <cert>.







Step 17:-

Now you have to same as it open and close key after the </cert>.

Open <key> and then close </keys> and then go to on premises and then cat client key and the copy all and paste between the open and close <key>. And then save the file as it is.



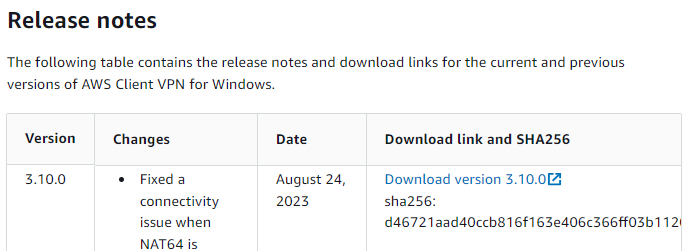


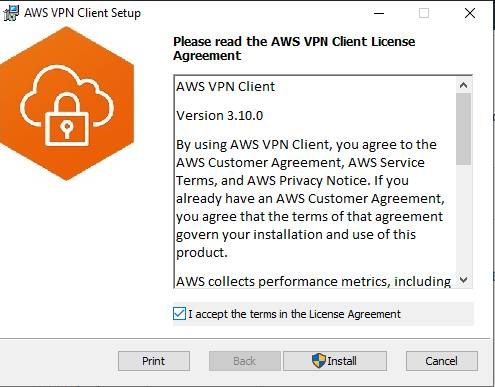
Step 18:-

Now your created client VPC endpoint was active so download VPN connection application on any where I was choose as windows. For download the VPN application click on following link.

https://docs.aws.amazon.com/vpn/latest/clientvpn-user/client-vpn-connect-windows.html

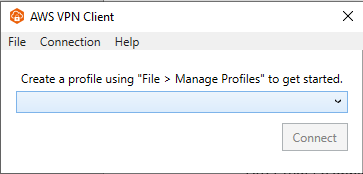
when you open this link scroll down and you have see the option release notes in that click on download version which you want. And wait for download. And then install it on windows.

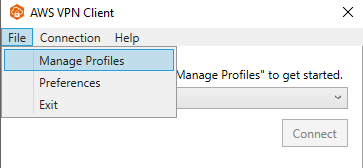




Step 19:-

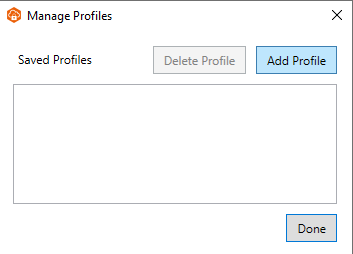
After that go application session of windows and search of VPN application and click on it to open. When AWS VPN client application open then click on Ffile option in the left side and then click on manage profile.

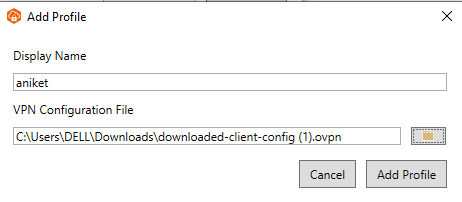


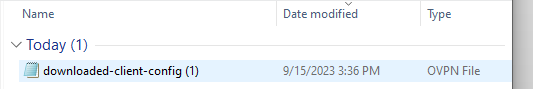


Step 20:-

Now click on add profile. And then gave display name and then select VPN configuration file which we have downloaded and edit with adding key and certificate in it. And after that click on add profile. And then click on done manage profile.

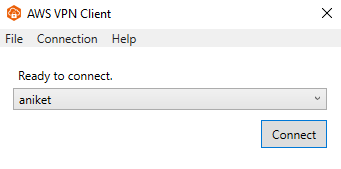


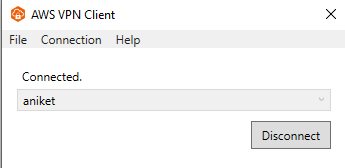




Step 21:-

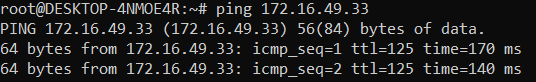
Now select your VPN display name and click on connect.

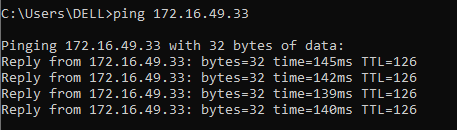




Step 22:-

When VPN connected then go CMD or on premises machine and ping the your instance private IP which instance we have launched in associated subnets with vpn client endpoint.





\*\*\*THE END\*\*\*