Date – 08 Dec 2025 Preeti

AWS Client VPN – Step-by-Step Implementation Guide

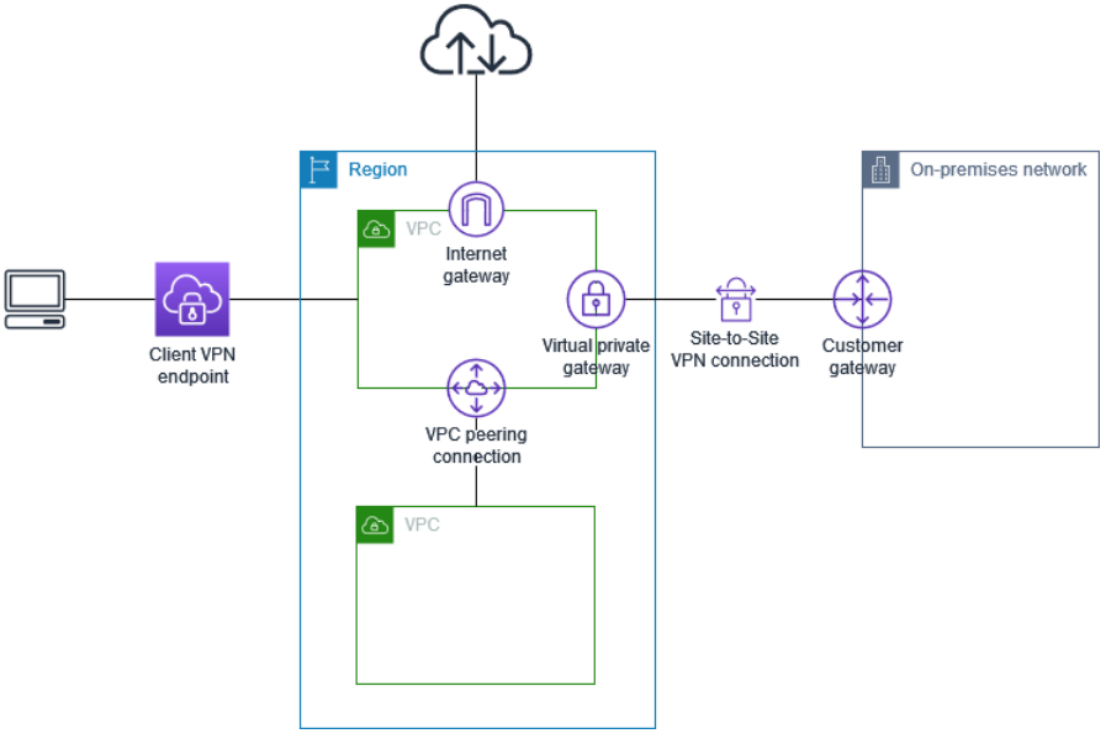
Contents

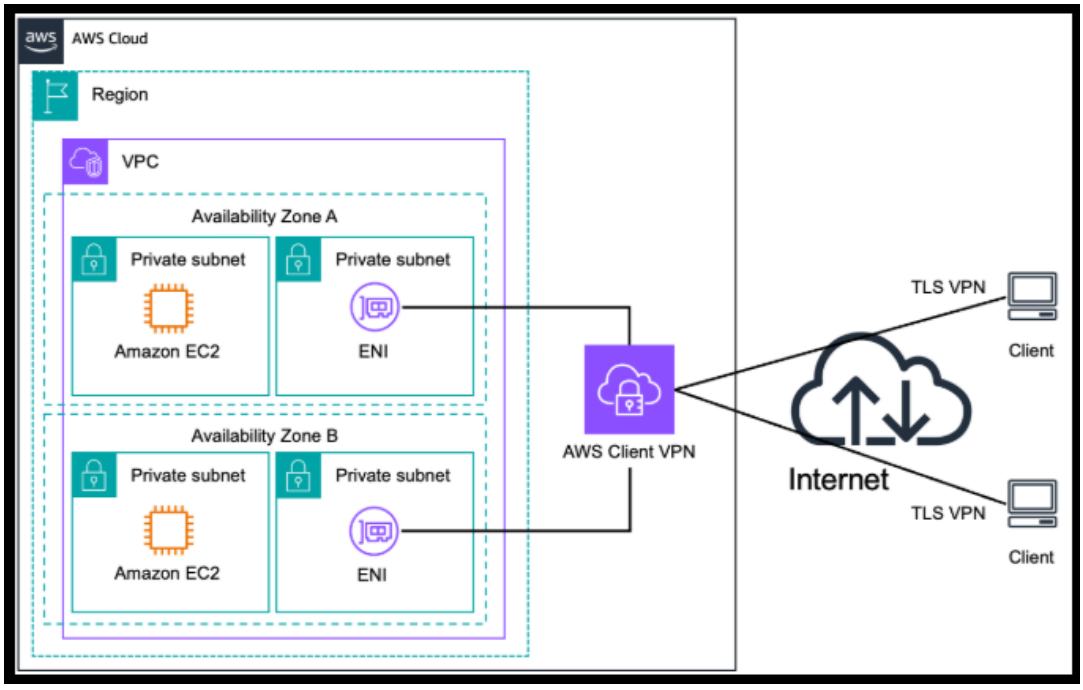
What is AWS Client VPN?

AWS Client VPN is a managed client-based VPN service that enables you to securely access your AWS resources and resources in your on-premises network. With Client VPN, you can access your resources from any location using an **OpenVPN-based VPN client.**

1. Architecture Overview

AWS Client VPN provides secure remote access to private EC2 resources inside a VPC using OpenVPN tunnels.

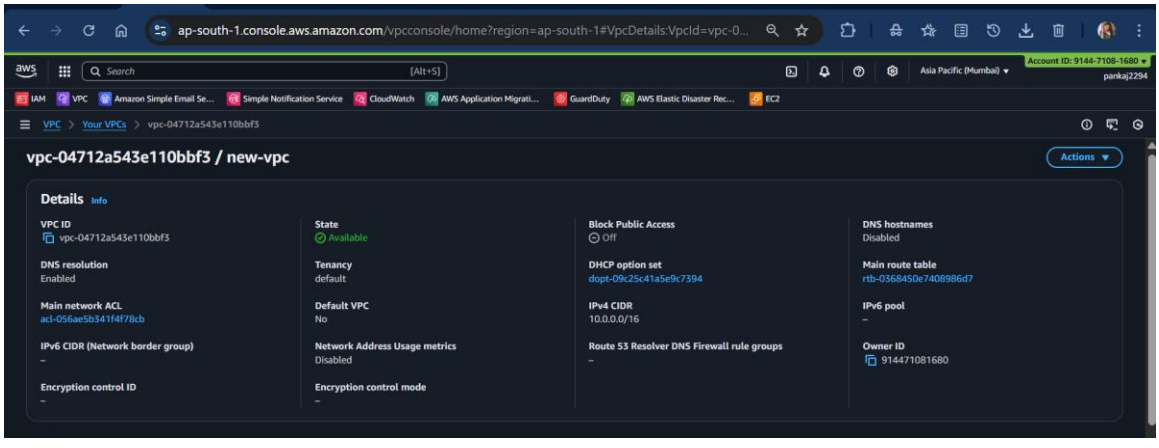


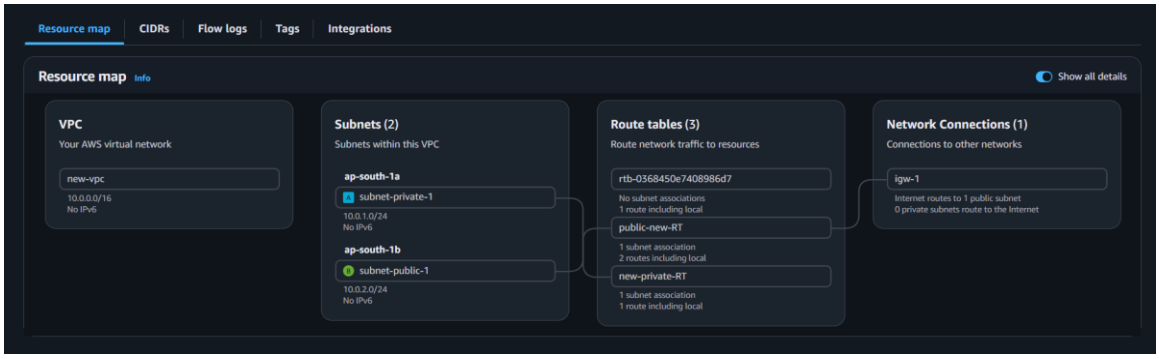


2. Prerequisites

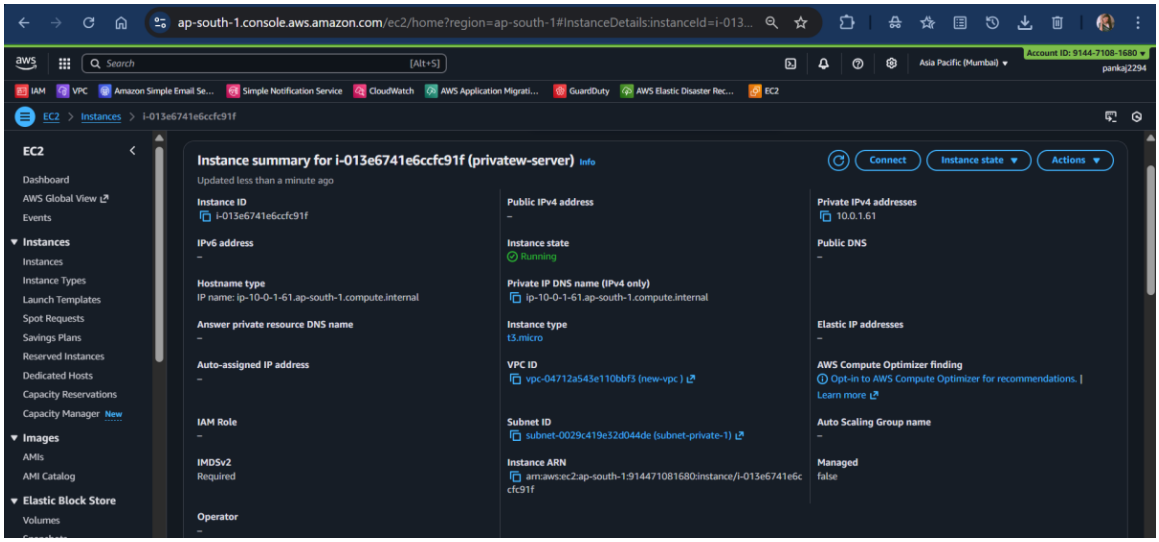
- AWS Account
- VPC (CIDR- 10.0.0.0/16)
- Public + Private Subnets
- Private EC2 instance with security port – VPN CIDR allow
- EasyRSA for certificate creation
- Enable mutual authentication for AWS Client VPN
- OpenVPN or AWS VPN Client

3. VPC Architecture overview:





Private EC2 Instance for test connectivity .

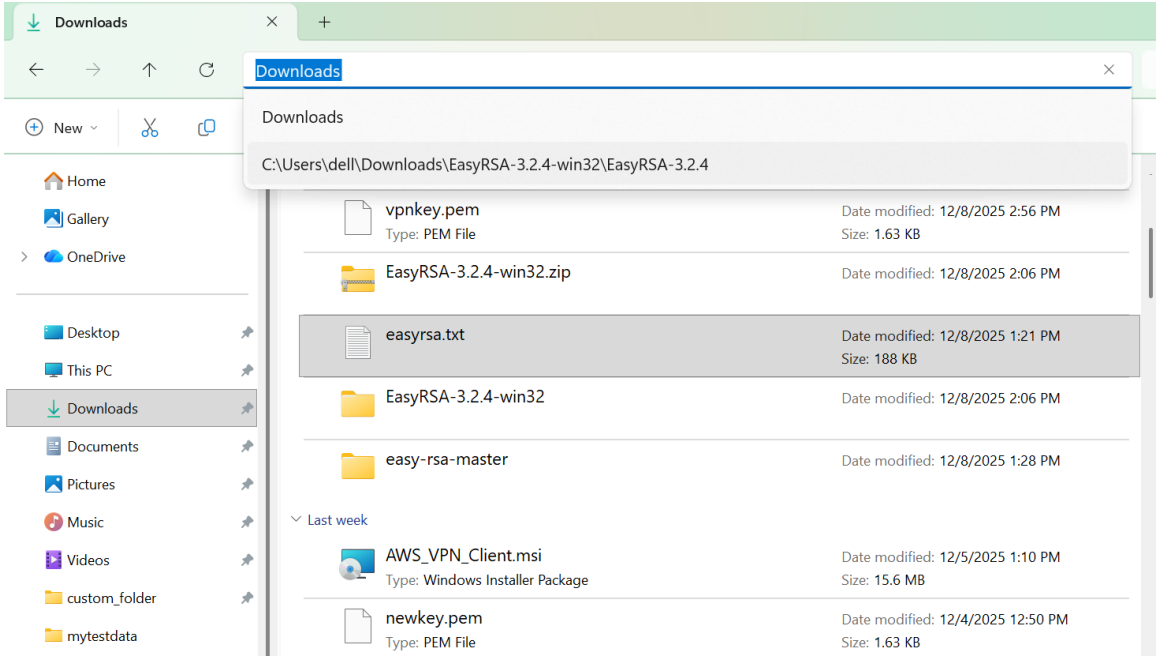


4. Create Server & Certificate Creation Using EasyRSA

To generate server and client certificates and keys and upload them to ACM.

Open the EasyRSA releases page and download the ZIP file for your version of Windows and extract it. https://github.com/OpenVPN/easy-rsa/releases

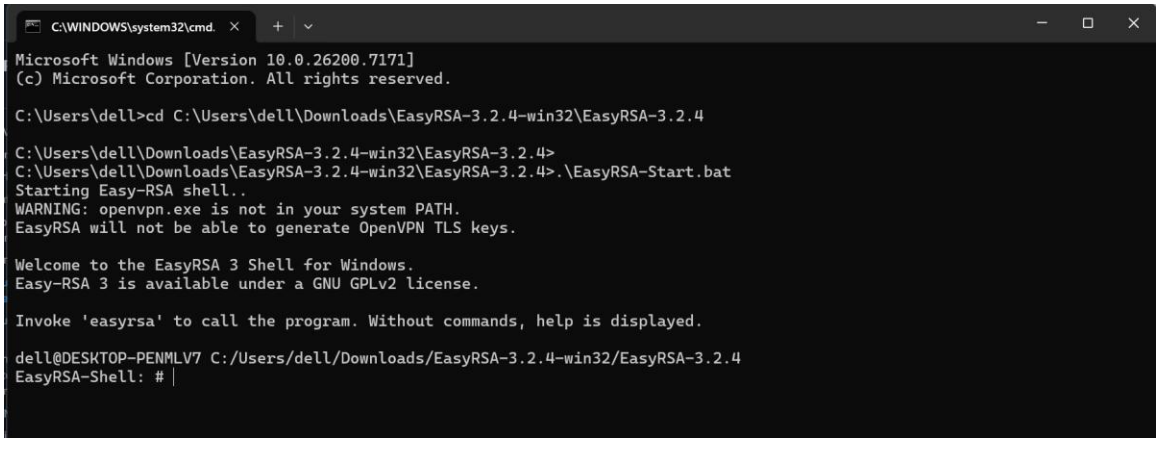
Open a command prompt and navigate to the location that the EasyRSA-3.x folder was extracted to.



4.1 Install EasyRSA (Windows)

Extract EasyRSA folder – open **PowerShell inside the folder**.

#.\EasyRSA-Start.bat



4.2 Initialize PKI environment.

#./easyrsa init-pki

```
dell@DESKTOP-PENMLV7 C:/Users/dell/Downloads/EasyRSA-3.2.4-win32/EasyRSA-3.2.4
EasyRSA-Shell: # ./easyrsa init-pki

WARNING!!!

You are about to remove the EASYRSA_PKI at:
* C:/Users/dell/Downloads/EasyRSA-3.2.4-win32/EasyRSA-3.2.4/pki

and initialize a fresh PKI here.

Type the word 'yes' to continue, or any other input to abort.
  Confirm removal:
```

Type: yes

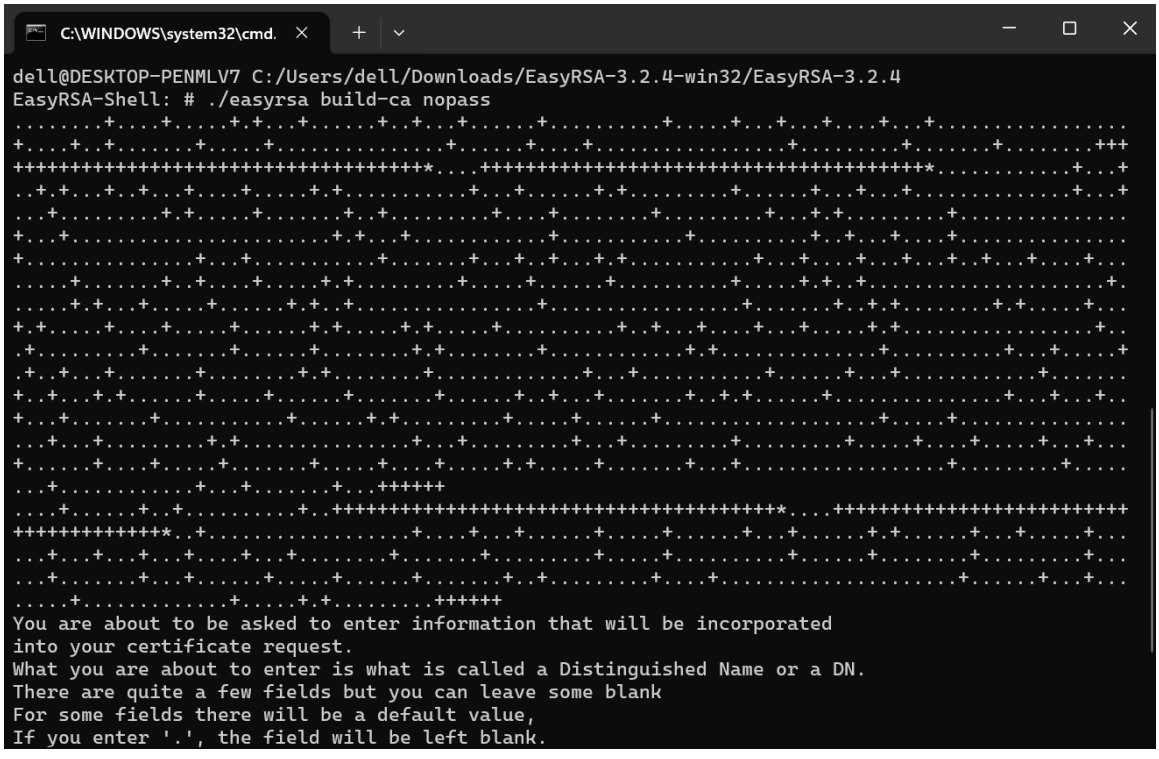
```
Notice
------
'init-pki' complete; you may now create a CA or requests.

Your newly created PKI dir is:
* C:/Users/dell/Downloads/EasyRSA-3.2.4-win32/EasyRSA-3.2.4/pki

Using Easy-RSA configuration:
* undefined
dell@DESKTOP-PENMLV7 C:/Users/dell/Downloads/EasyRSA-3.2.4-win32/EasyRSA-3.2.4
EasyRSA-Shell: #
```

4.3 Build CA

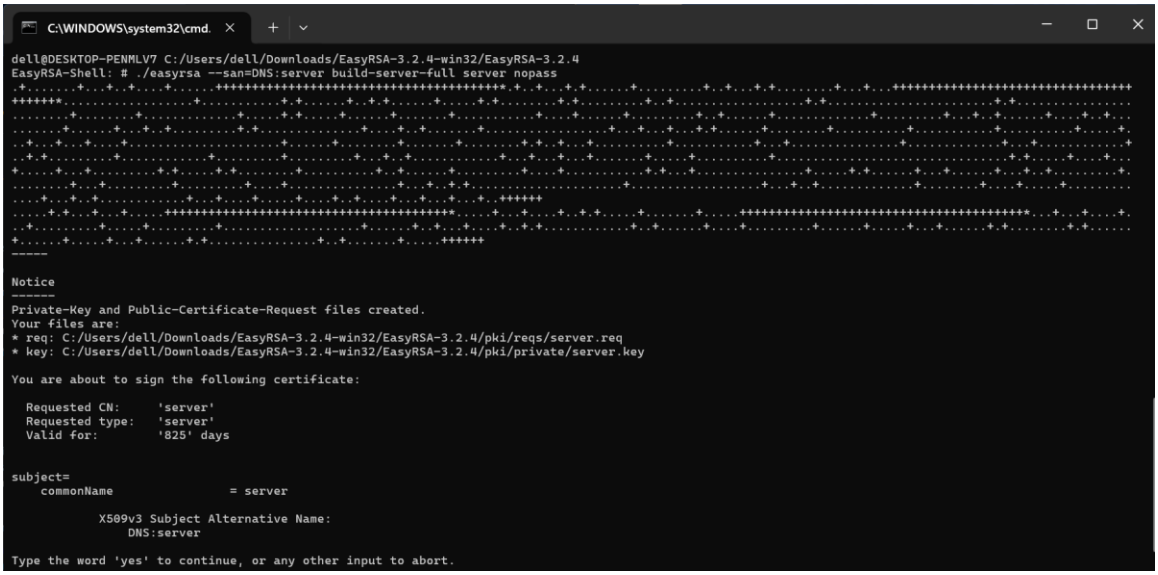
#./easyrsa build-ca



Enter a CA name (example: Server-CA).

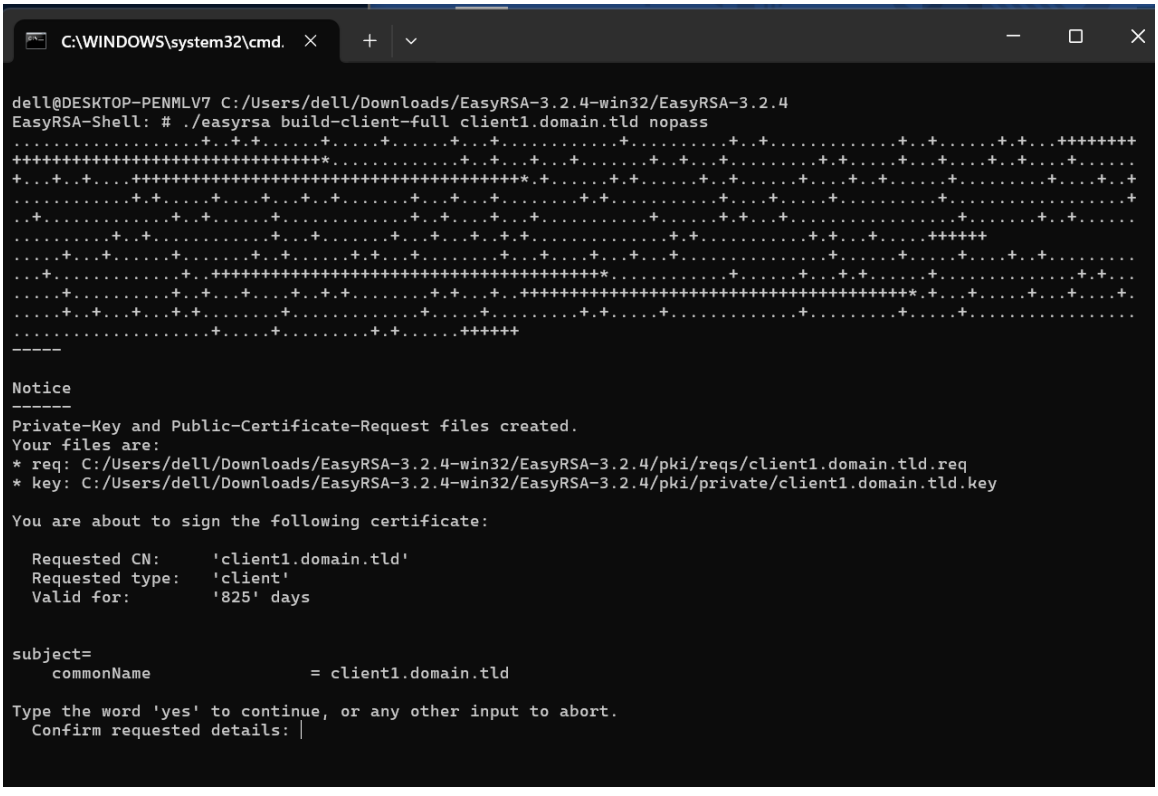
4.4 Generate Server Certificate and key

./easyrsa --san=DNS:server build-server-full server nopass

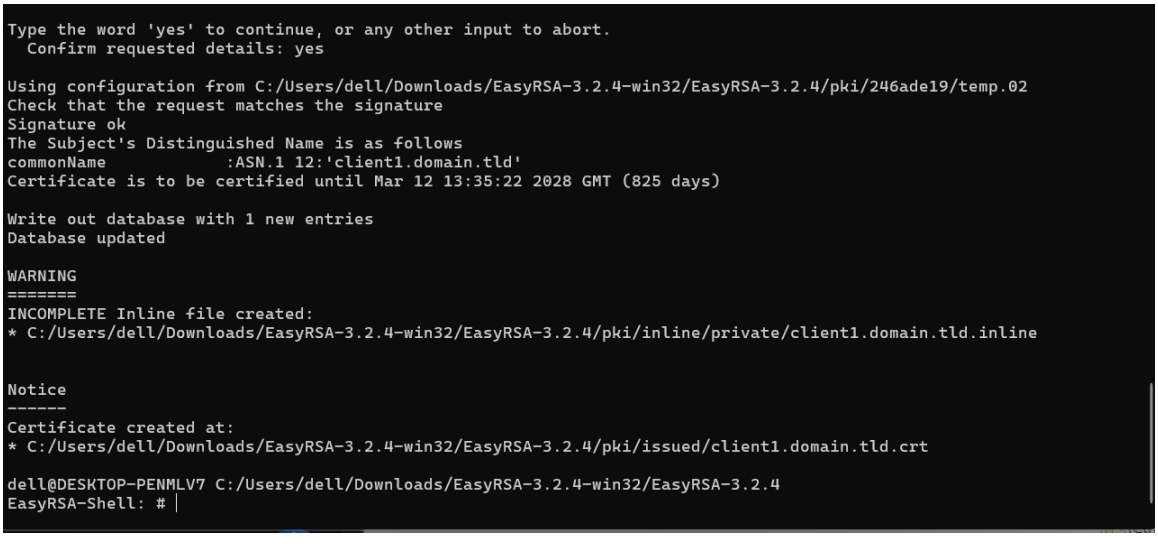


4.5 Generate Client Certificate and key

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



Type:yes



4.6 Exit the EasyRSA 3 shell.

exit

This creates:

- **server.crt**

- **server.key**
- **ca.crt**

Copy the server certificate and key and the client certificate and key to a custom folder and then navigate into the custom folder.

mkdir C:\custom_folder

copy pki\ca.crt C:\custom_folder

copy pki\issued\server.crt C:\custom_folder

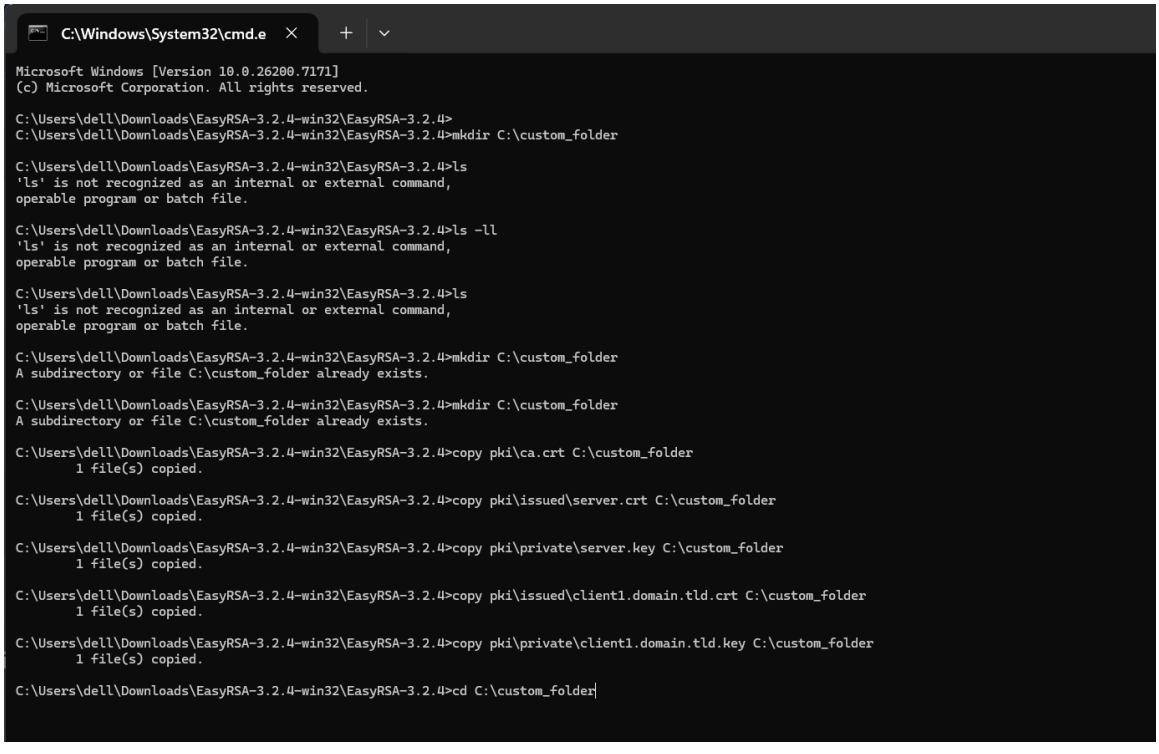
copy pki\private\server.key C:\custom_folder

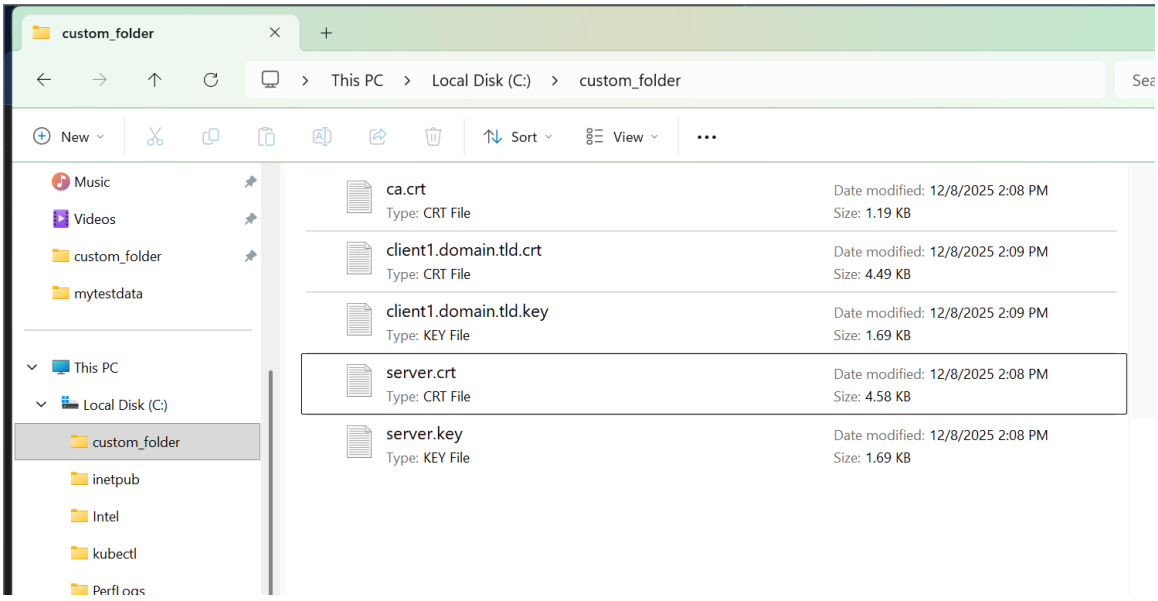
copy pki\issued\client1.domain.tld.crt C:\custom_folder

copy pki\private\client1.domain.tld.key C:\custom_folder

cd C:\custom_folder

Before you copy the certificates and keys, create the custom folder by using the mkdir command. The following example creates a custom folder in your C:\ drive.





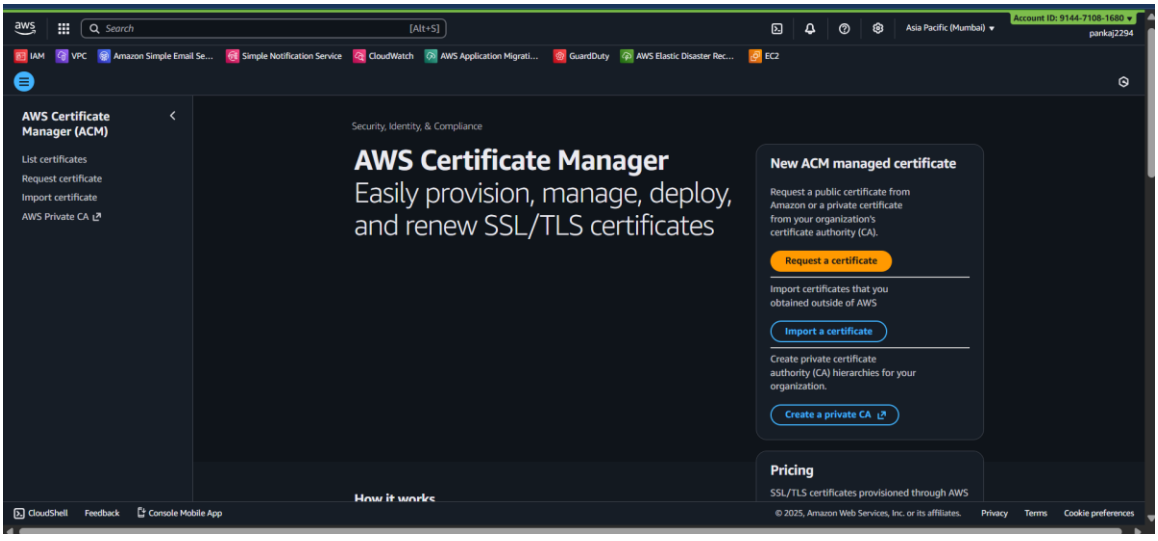
You can see in the above screenshot the custom folder has been created now and all copied files are there.

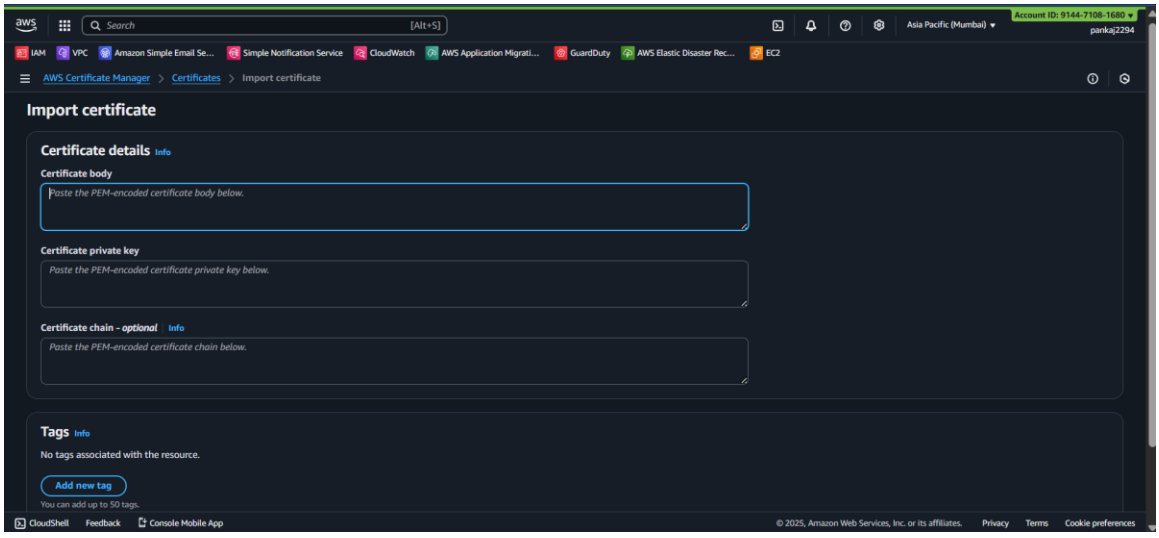
5. Import Certificates to AWS ACM

Go to :

AWS ACM – Click : **Import certificate**

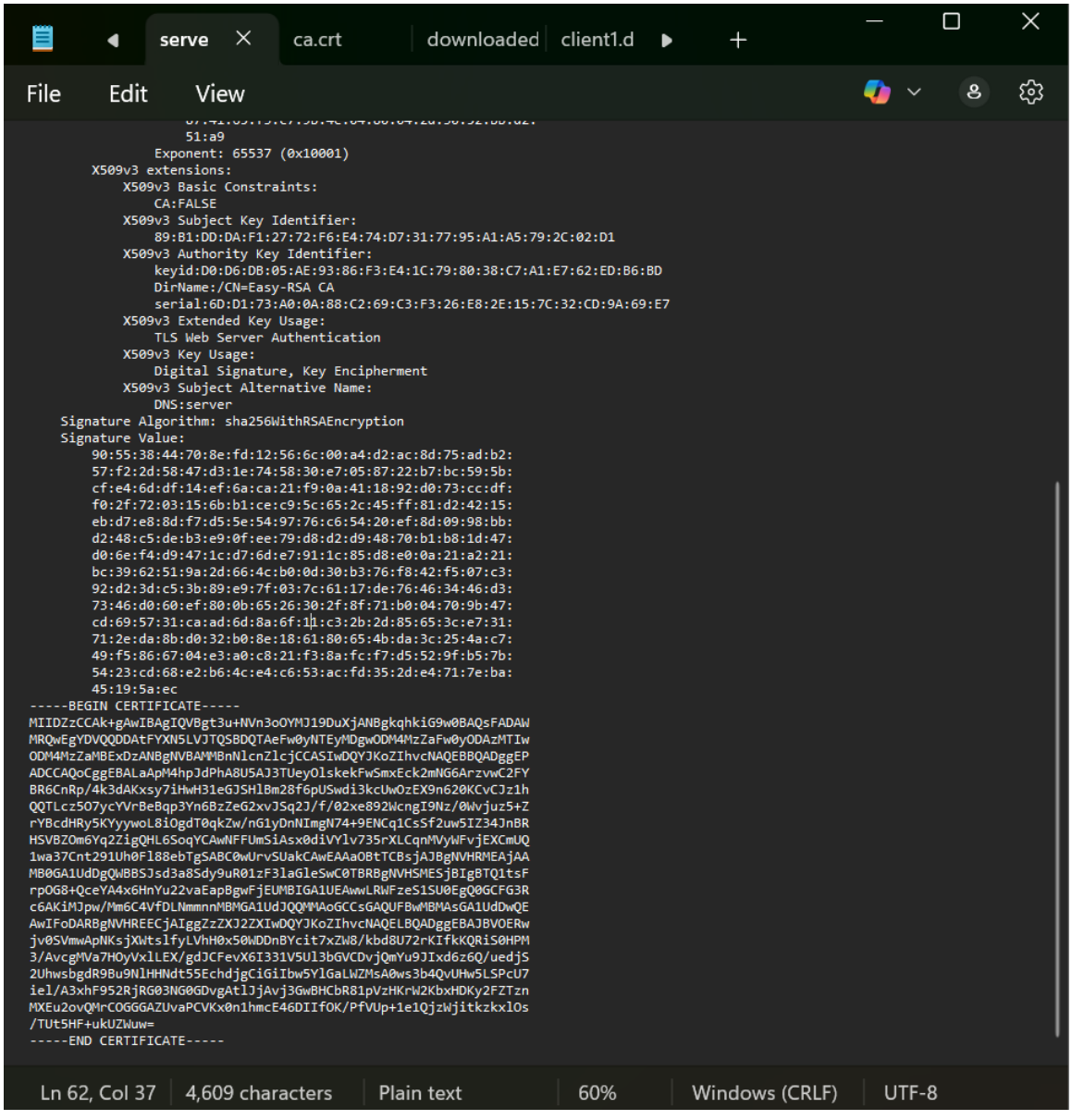
Upload server certificate & server.key, and ca.crt into ACM.



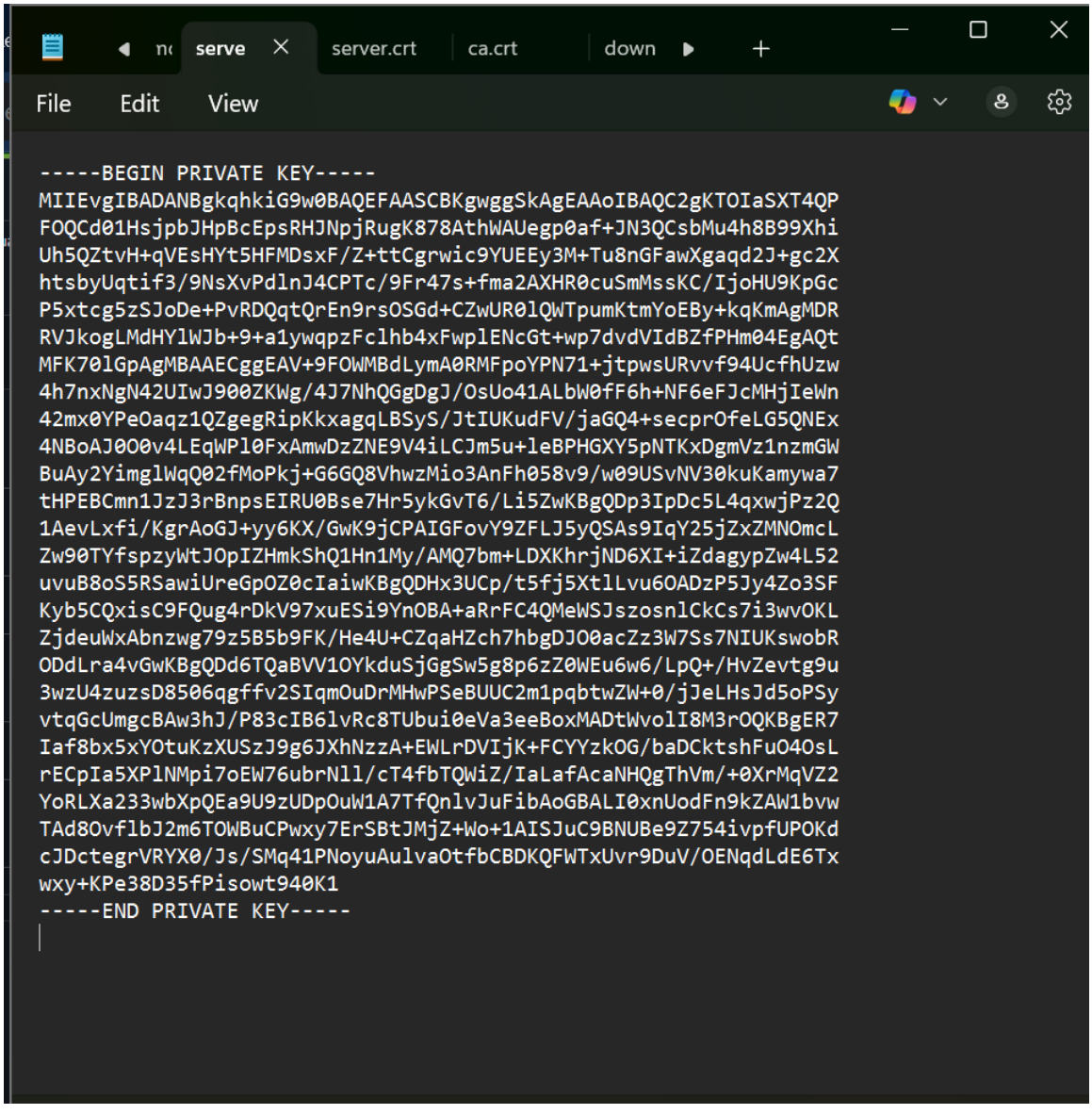


aws acm import-certificate \

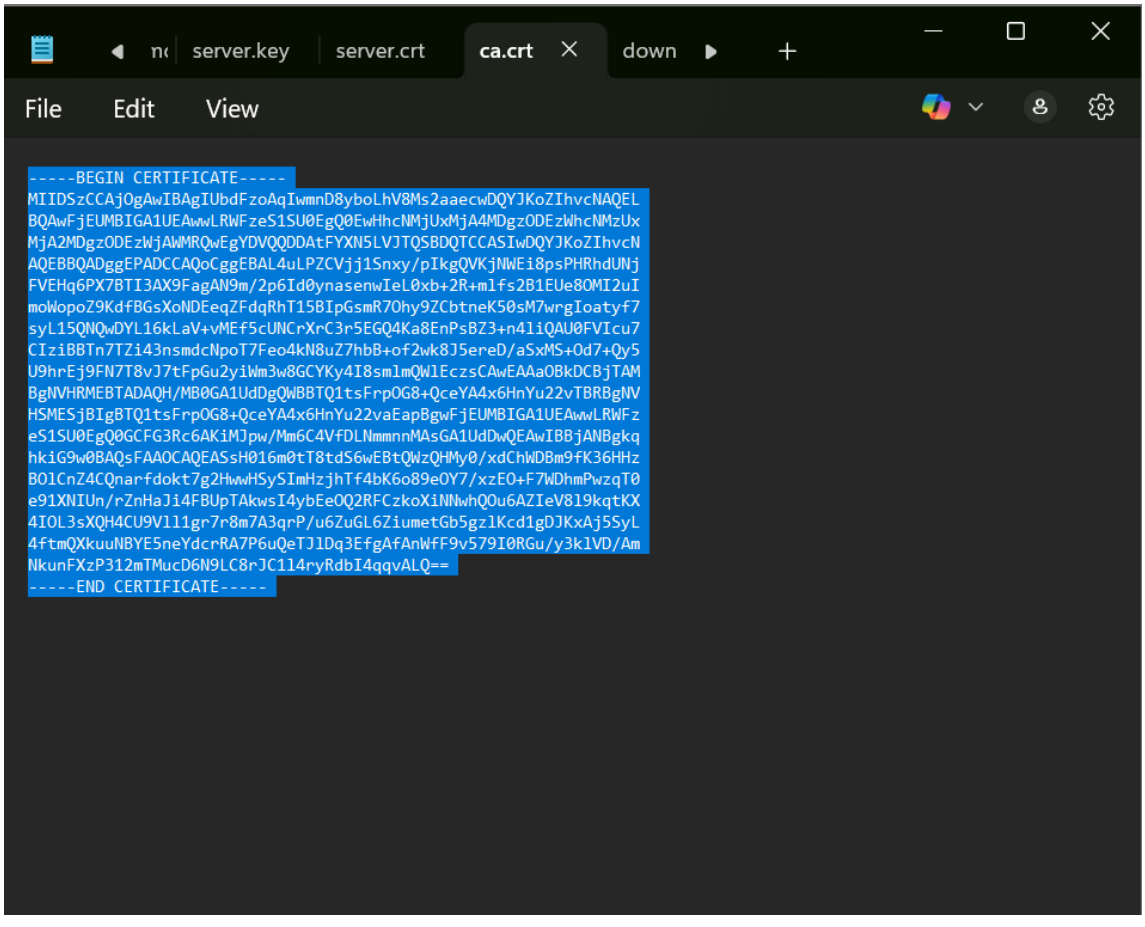
--certificate fileb://server.crt \



--private-key fileb://server.key \



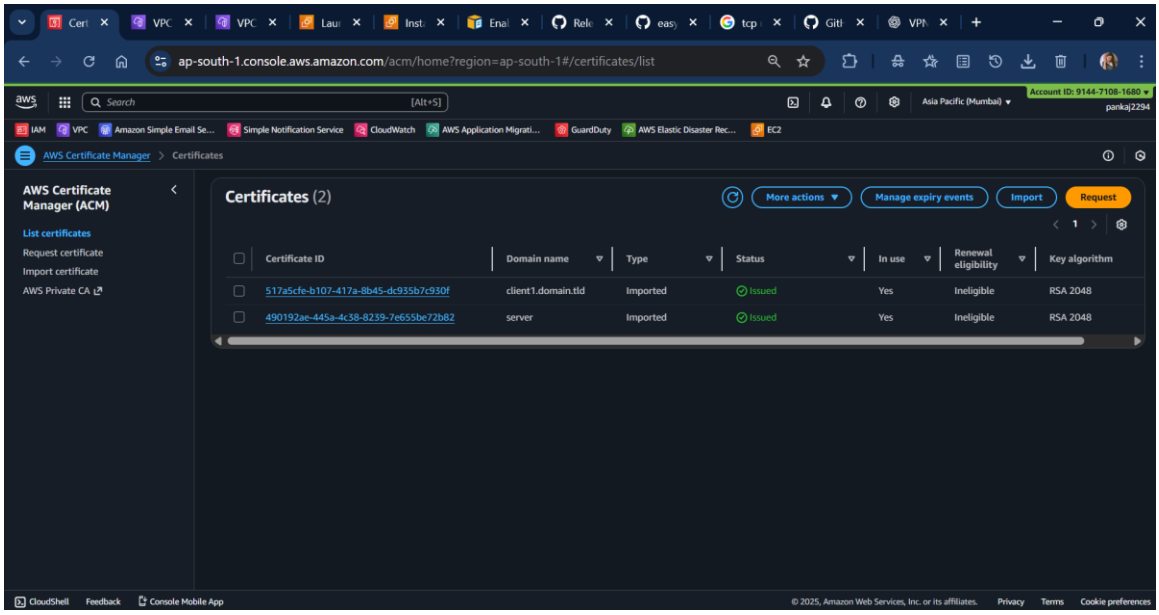
--certificate-chain fileb://ca.crt



Your server certificate has now successfully imported to your AWS ACM and now again repeat the same thing to import the Client Certificate.

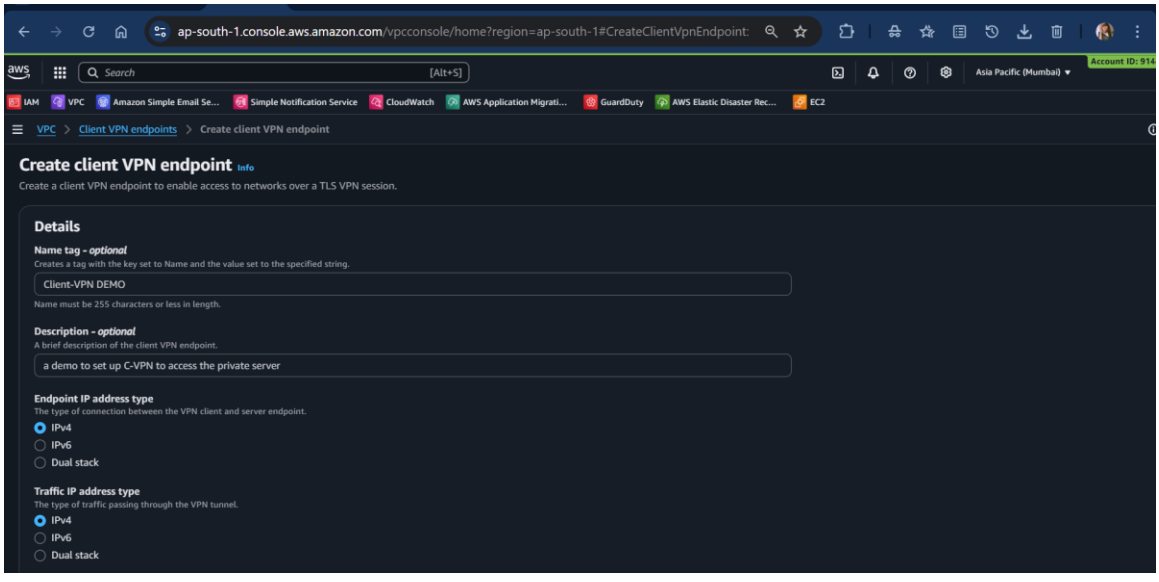
```
aws acm import-certificate \
  --certificate fileb://client1.domain.tld.crt \
  --private-key fileb://client1.domain.tld.key \
  --certificate-chain fileb://ca.crt
```

Field	File
Certificate body	server.crt
Certificate private key	server.key
Certificate chain	ca.crt



Here in the above screenshot of **AWS ACM imported certificates** you can see in the AWS ACM List Certificates dashboard.

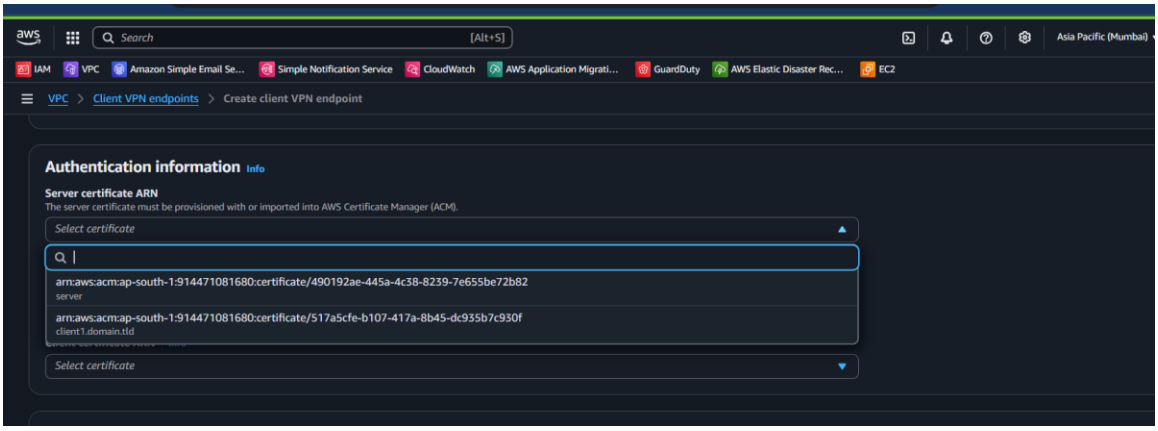
5.1 Create AWS Client VPN Endpoint



Use non-overlapping Client CIDR (Example: 192.168.100.0/22).

5.3 Server Certificate ARN

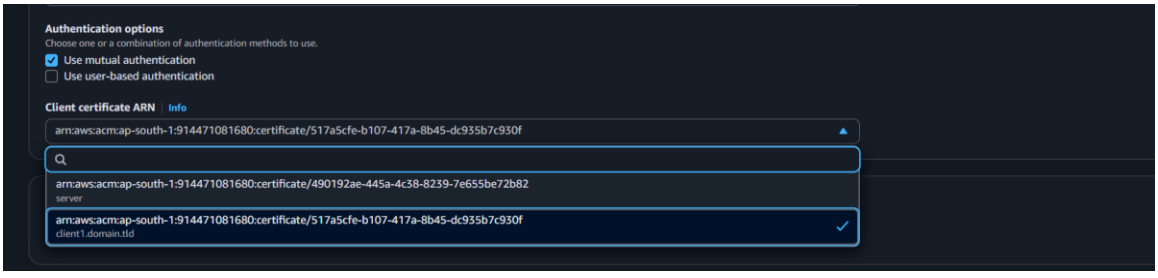
Select server certificate from ACM.



Paste ACM ARN.

5.4 Authentication

- Mutual authentication
- Upload Client CA (ca.crt)



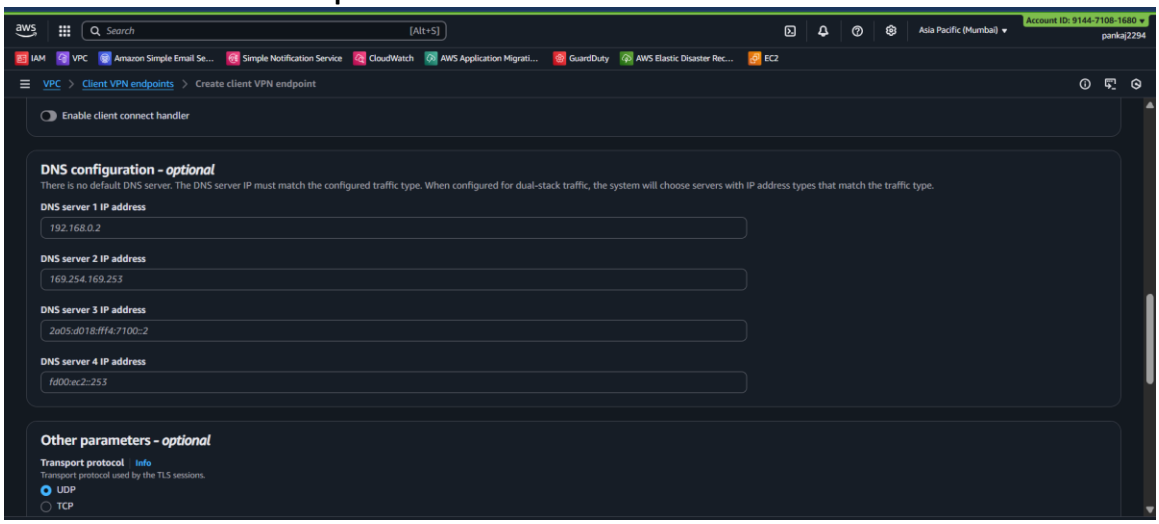
5.5 Connection Logging

Optional.

5.6 DNS Servers

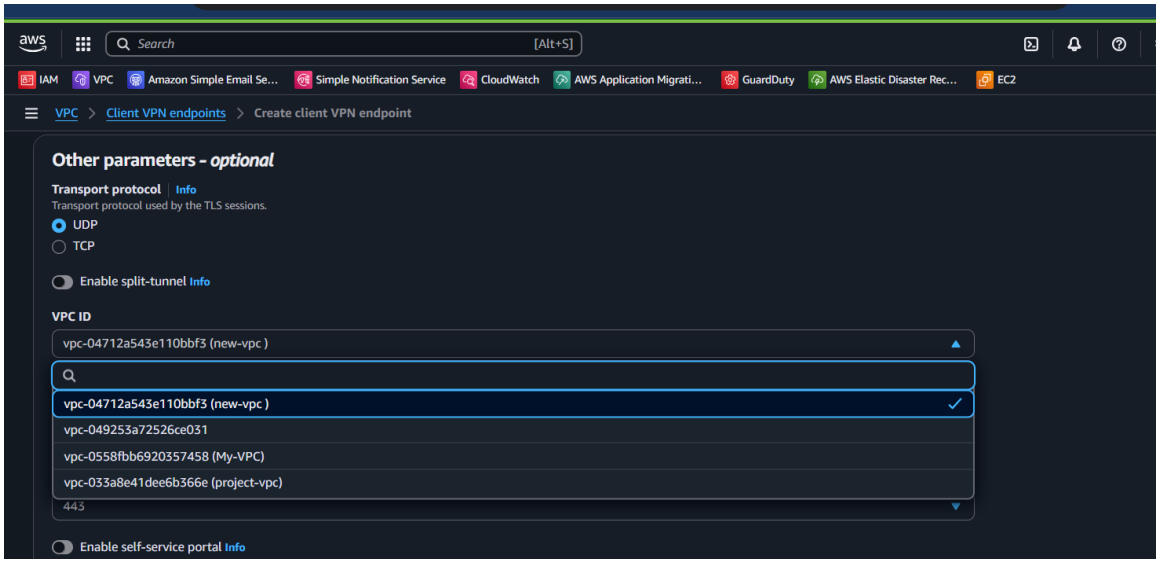
Use:

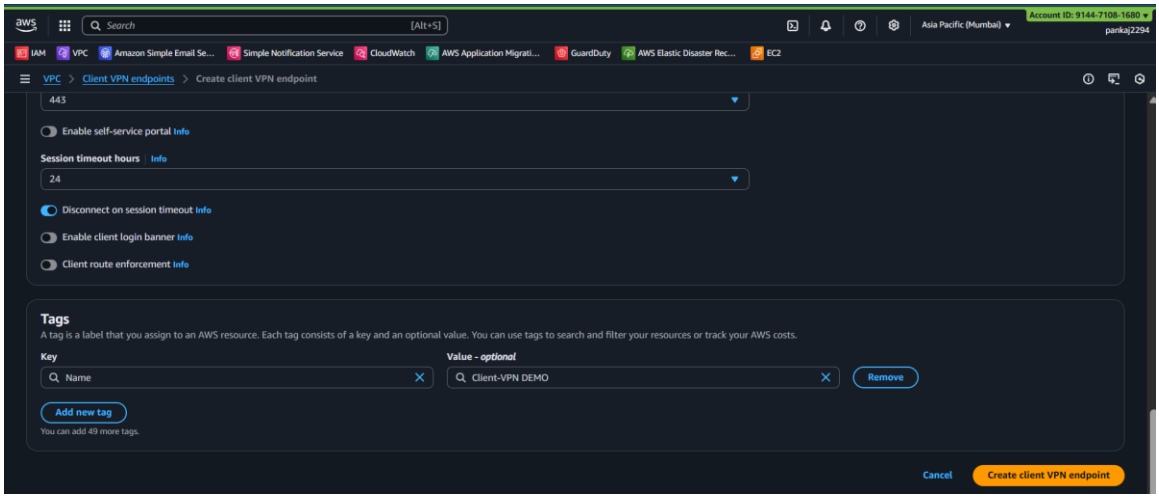
8.8.8.8
Click **Create Client VPN Endpoint**.



5.6 Others Parameters—Opti0nal

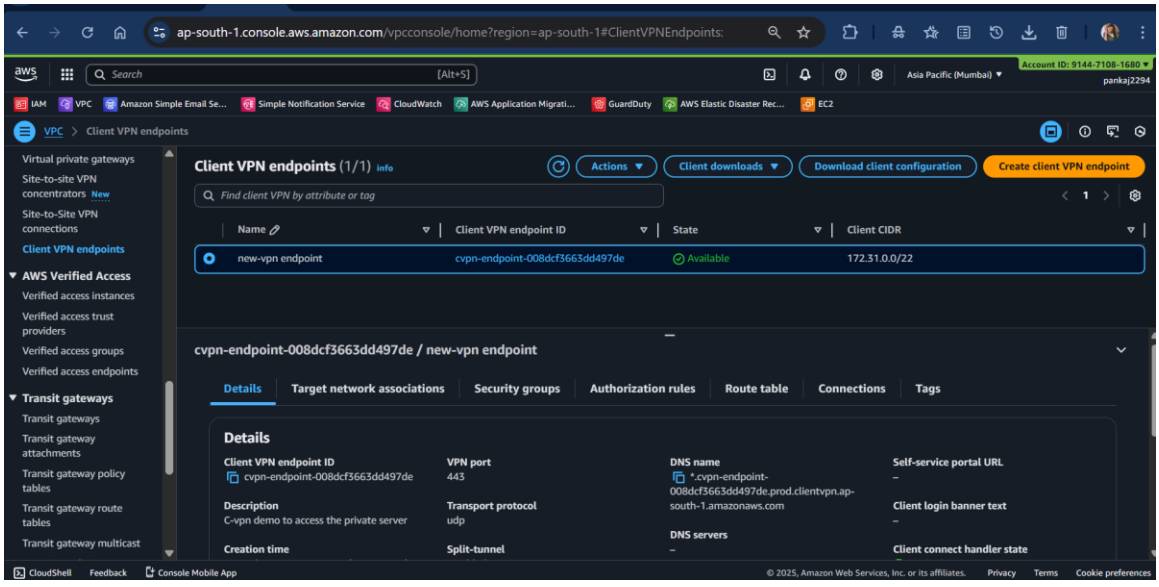
5.7 Now choose your VPC.





Now click on – Create Client VPN Endpoint.

After a while it will show you in Active state.



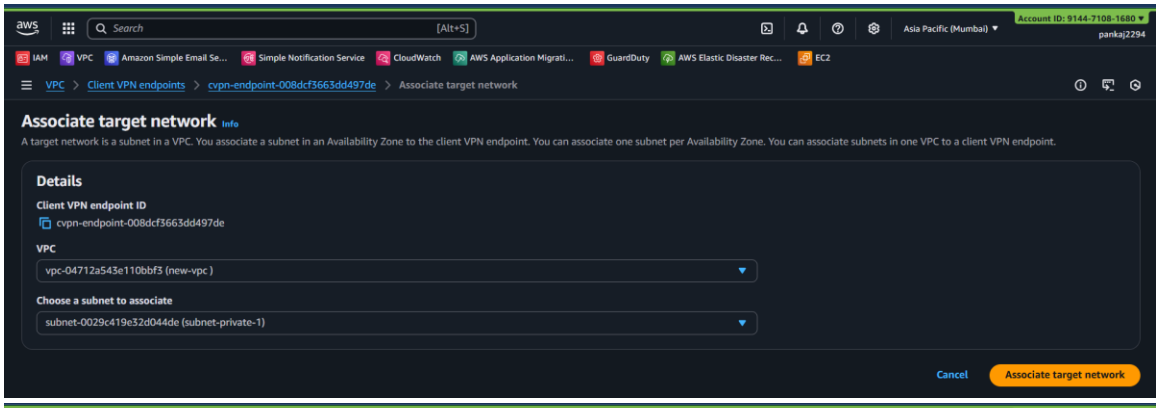
Go to page down and click on tabs and then add some required details:

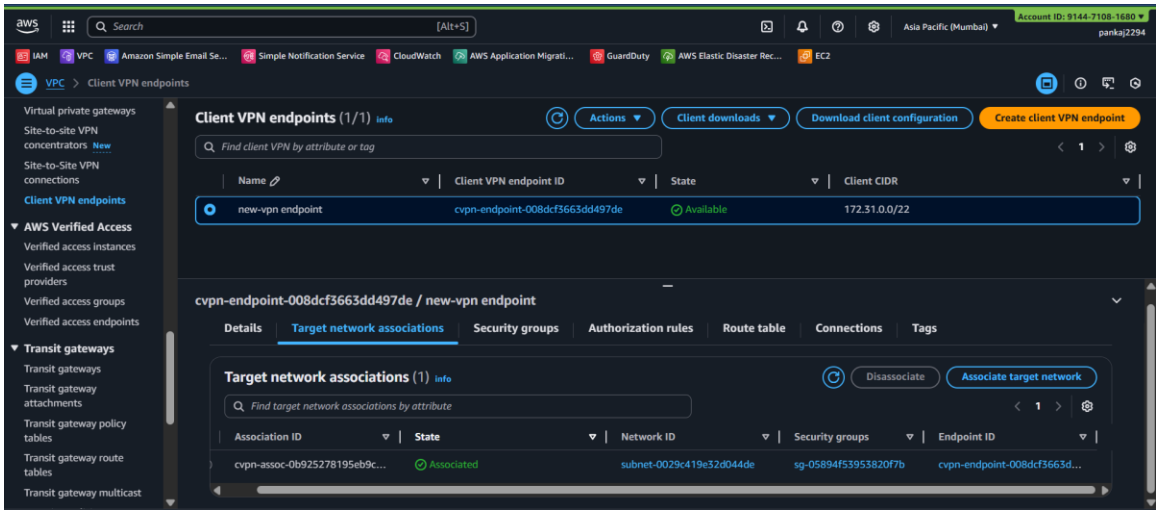
6. Associate Client VPN with a Subnet

Associate endpoint with a public subnet.

Go to:

Client VPN Tabs – Target Network Associations → Associate





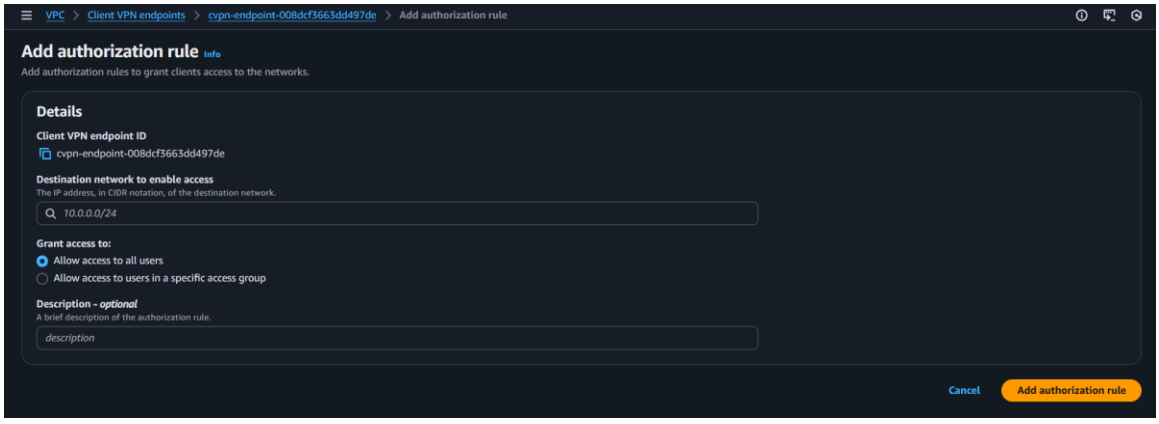
7. Authorization Rule

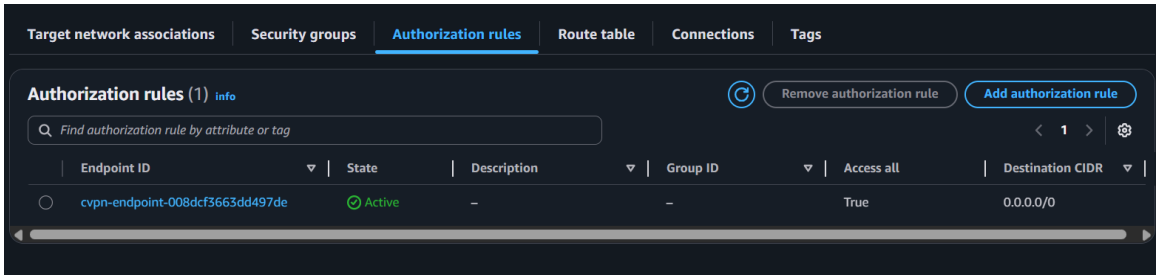
Allow access to 10.0.0.0/16.

Go to:

Client VPN --- Authorization Rules --- Add

- Destination CIDR: 10.0.0.0/16
- Access: Allow
- Group: allow-everyone





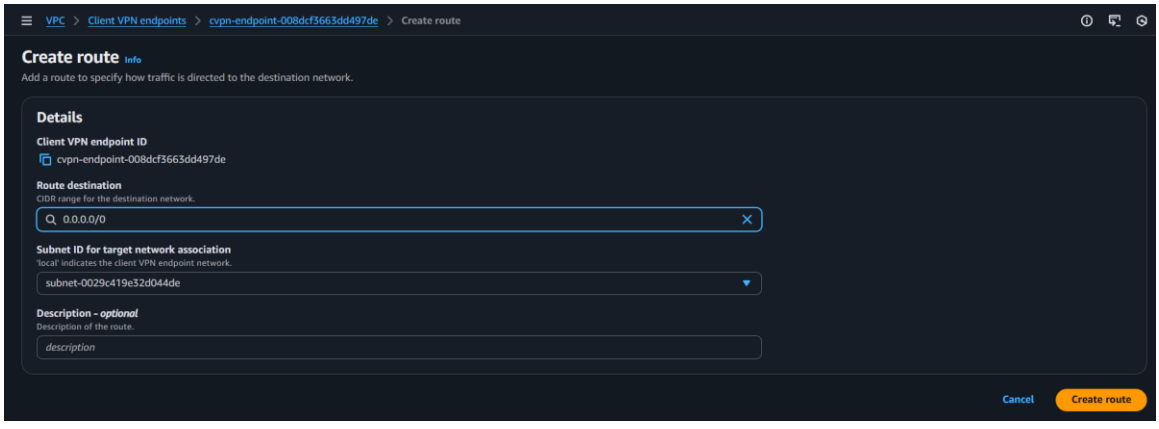
8. Add Route to VPC

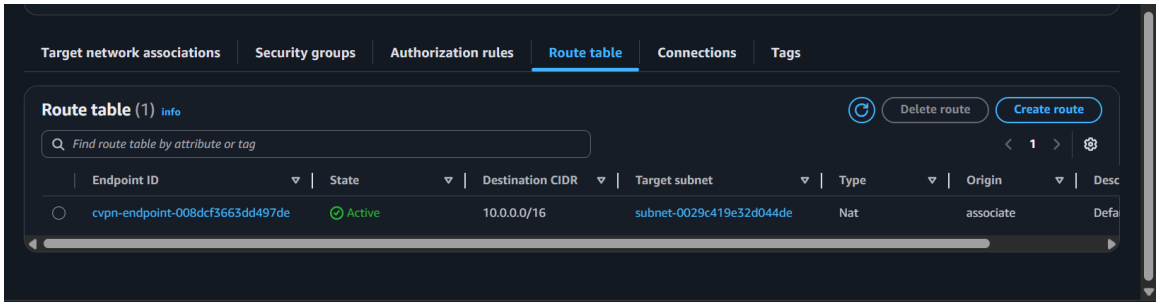
Go to:

Client VPN - Routes - Add route

Route destination: 10.0.0.0/16

Target: associated subnet.





9. Update Security Group on Private EC2

Add this rule:

Allow SSH from Client VPN CIDR (192.168.100.0/22).

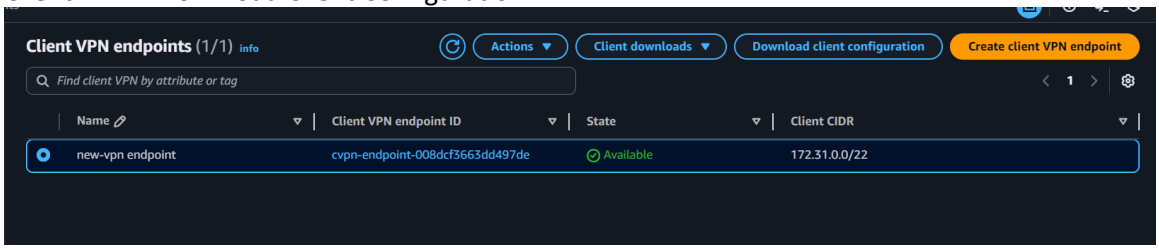
- Type: SSH
- Source: 192.168.100.0/22 (your Client CIDR)

This is required — without it you get **Request timed out**.

10. Download & Configure Client OVPN File

Go to:

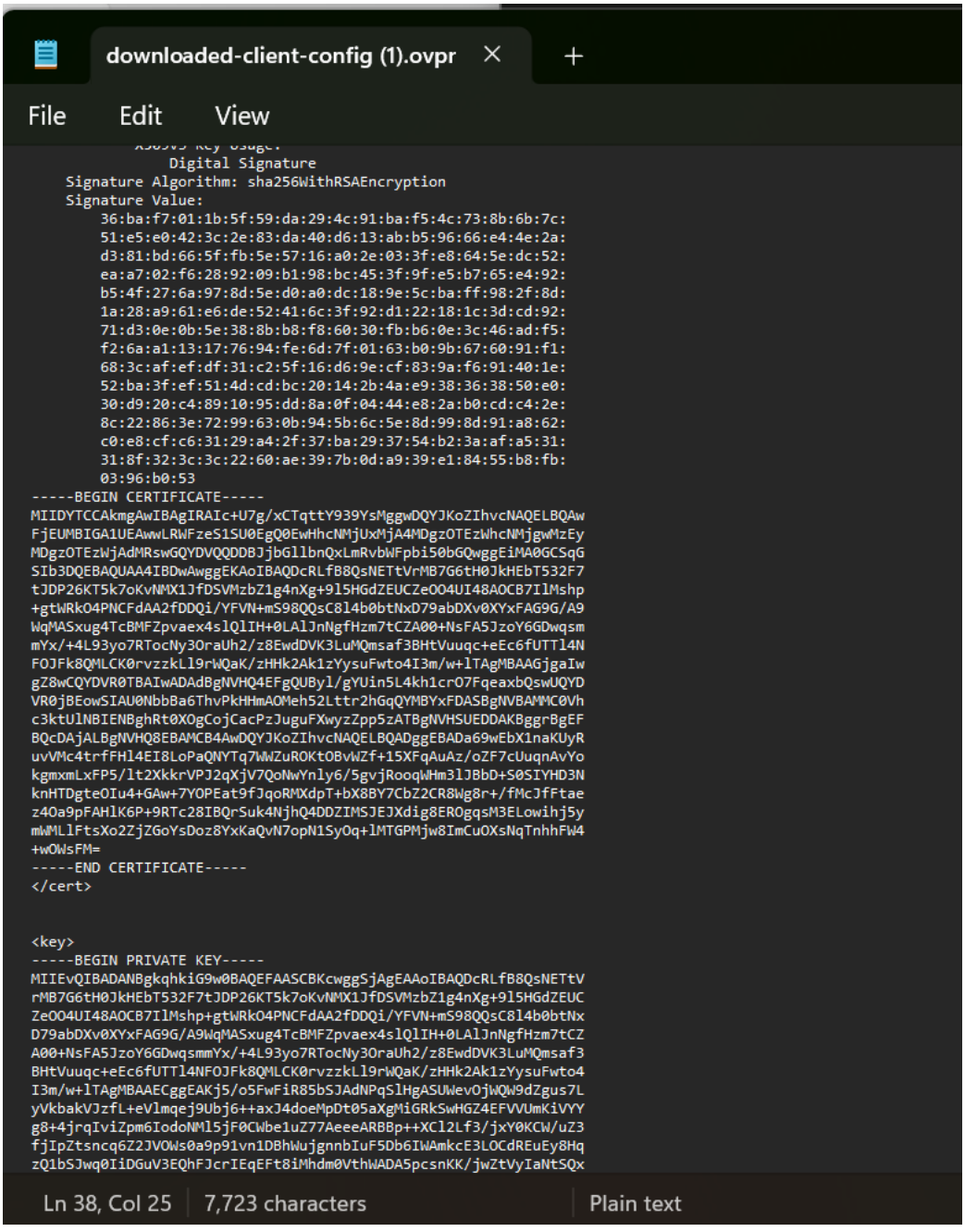
Client VPN – Download Client Configuration



Add the client certificate and key inside the .ovpn file:

<cert>
(client1.crt content)
</cert>

<key>
(client1.key content)
</key>



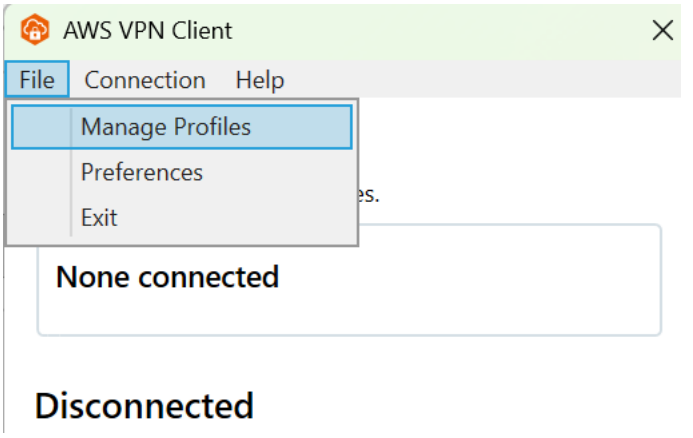
Ln 38, Col 25 | 7,723 characters | Plain text

Save.

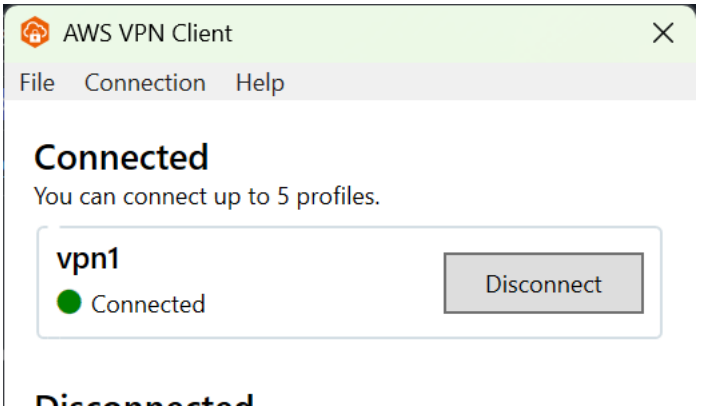
Insert client certificate and key inside the .ovpn file.

11. Connect Using AWS VPN Client

Open AWS VPN Client → Import configuration → Connect.

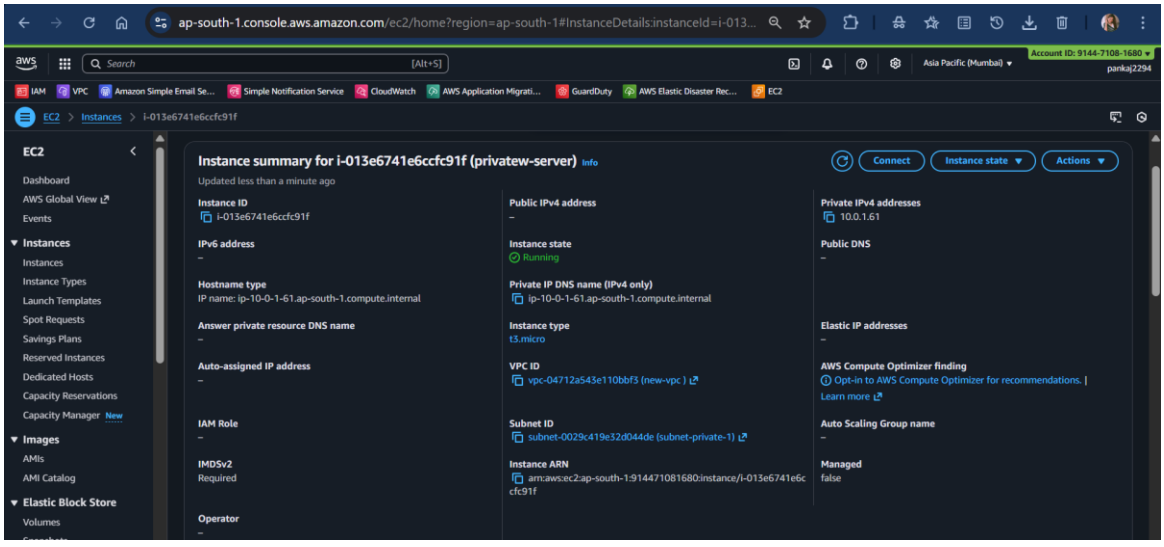


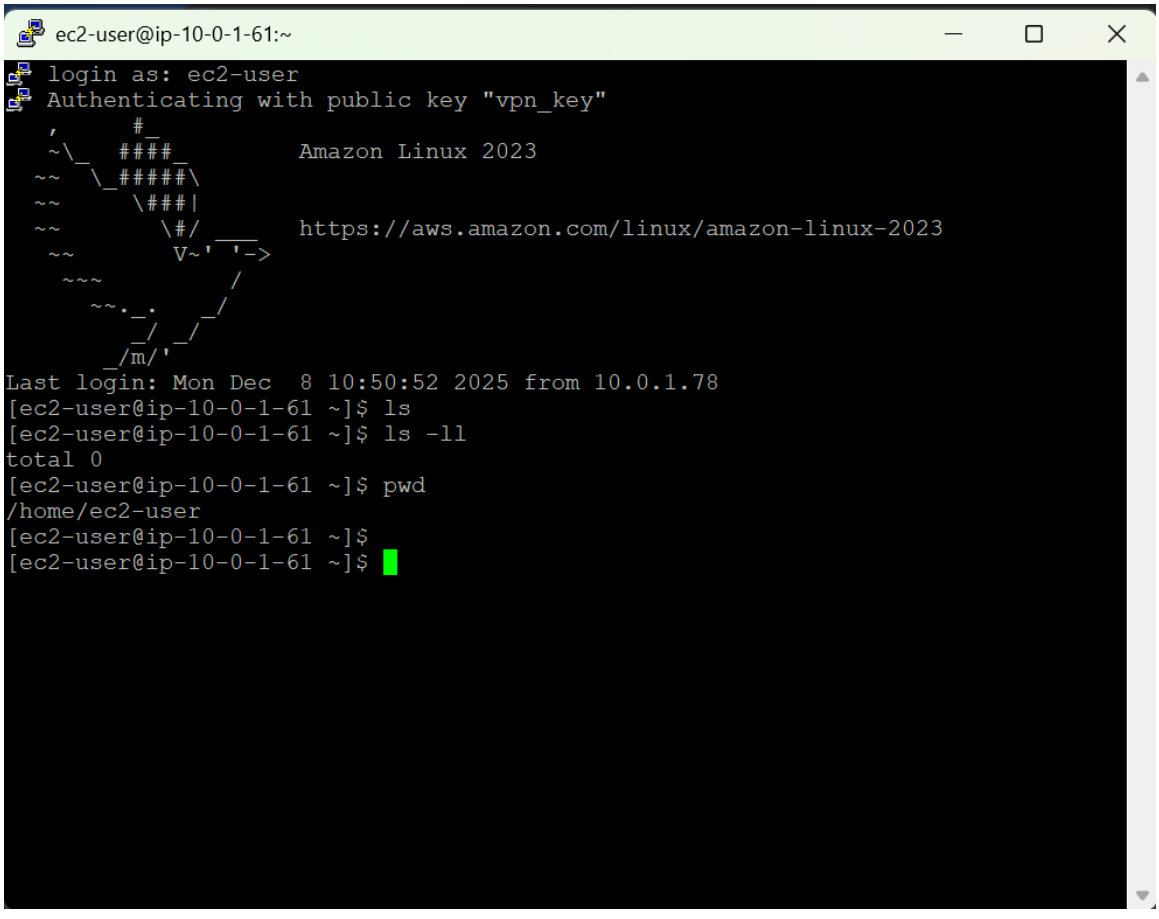
You should receive an IP from the pool: 192.168.100.x



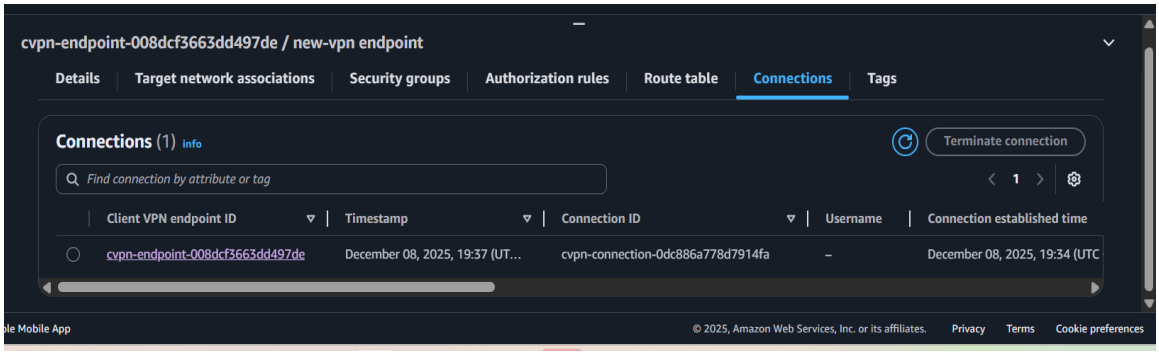
12. Validate Connectivity

Ping and SSH putty to private EC2 via private IP.





If it connects — VPN is working.



13. Troubleshooting

Common issues: CIDR overlap, missing routes, SG/NACL blocks.

Certificate errors: Re-import certificates or rebuild with EasyRSA.

VPN connects but no access: Check authorization rules.
