

AWS Client VPN – Step-by-Step Implementation Guide

Contents

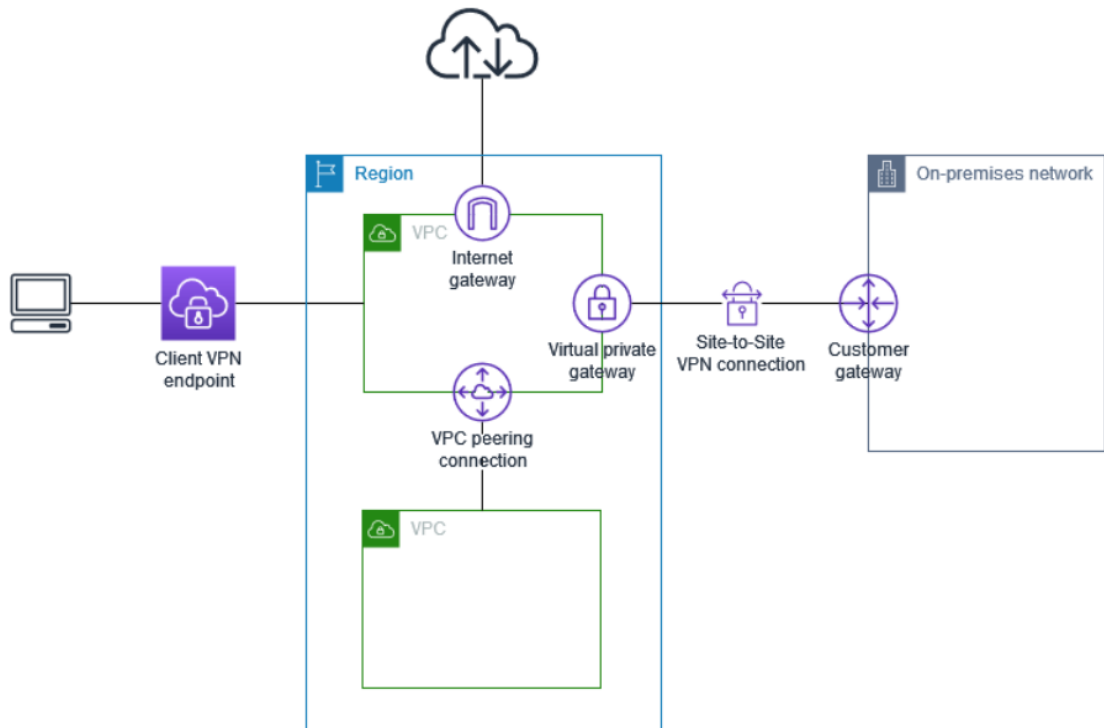
| | |
|---|----|
| AWS Client VPN – Step-by-Step Implementation Guide | 1 |
| What is AWS Client VPN? | 2 |
| 1. Architecture Overview | 2 |
| 2. Prerequisites | 3 |
| 3. VPC Architecture overview: | 3 |
| Private EC2 Instance for test connectivity | 4 |
| 4. Create Server & Certificate Creation Using EasyRSA | 4 |
| 4.1 Install EasyRSA (Windows) | 5 |
| 4.2 Initialize PKI environment | 5 |
| 4.3 Build CA | 6 |
| 4.4 Generate Server Certificate and key | 7 |
| 4.5 Generate Client Certificate and key | 7 |
| 4.6 Exit the EasyRSA 3 shell | 8 |
| 5. Import Certificates to AWS ACM | 10 |
| 5.1 Create AWS Client VPN Endpoint | 15 |
| 6. Associate Client VPN with a Subnet | 18 |
| 7. Authorization Rule | 19 |
| 8. Add Route to VPC | 20 |
| 9. Update Security Group on Private EC2 | 21 |
| 10. Download & Configure Client OVPN File | 21 |
| 11. Connect Using AWS VPN Client | 23 |
| Open AWS VPN Client → Import configuration → Connect | 23 |
| You should receive an IP from the pool: 192.168.100.x | 23 |
| 12. Validate Connectivity | 23 |
| 13. Troubleshooting | 25 |

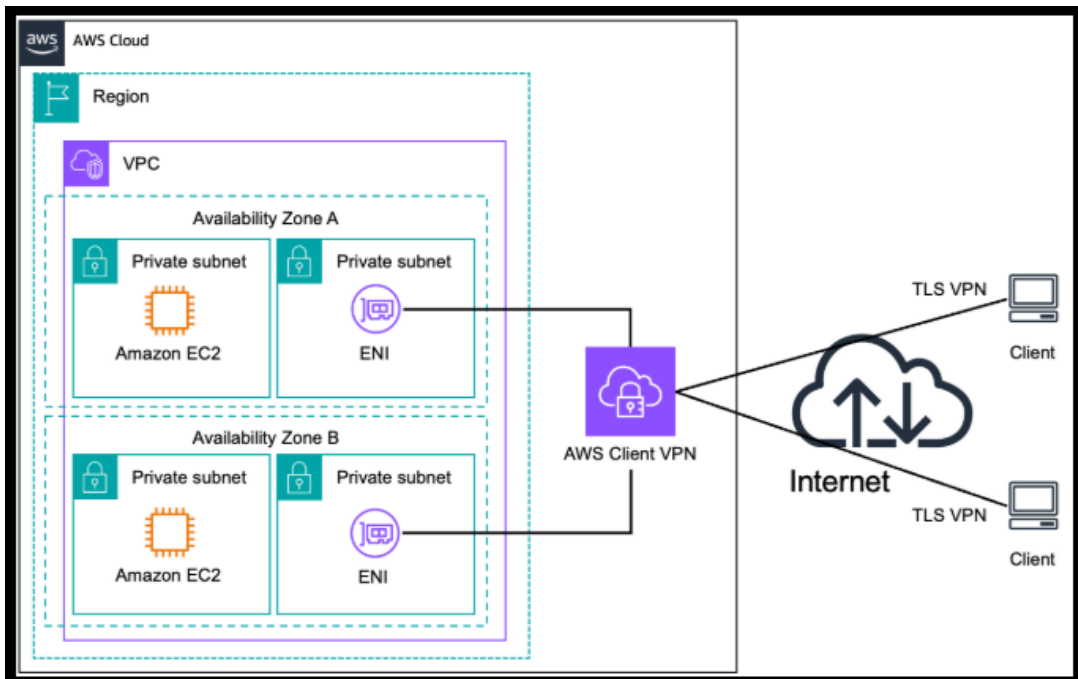
What is AWS Client VPN?

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.

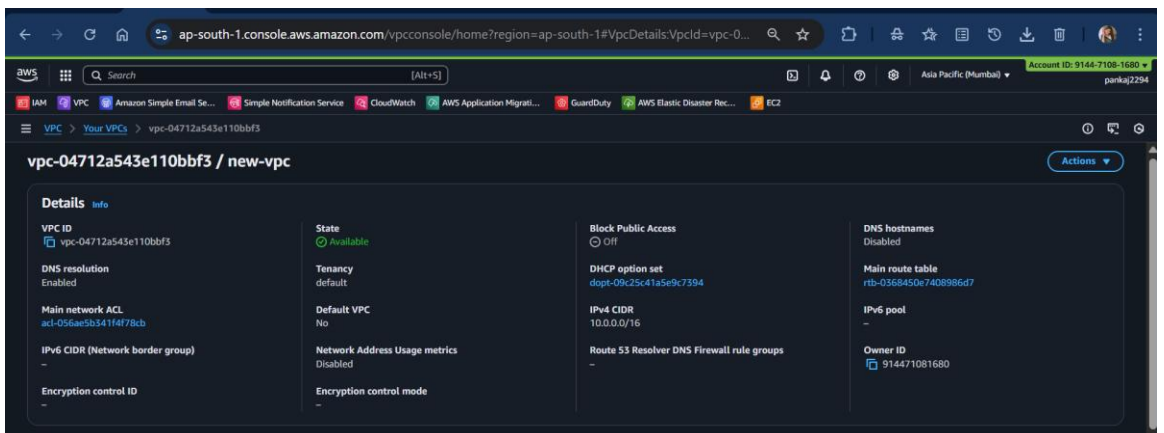


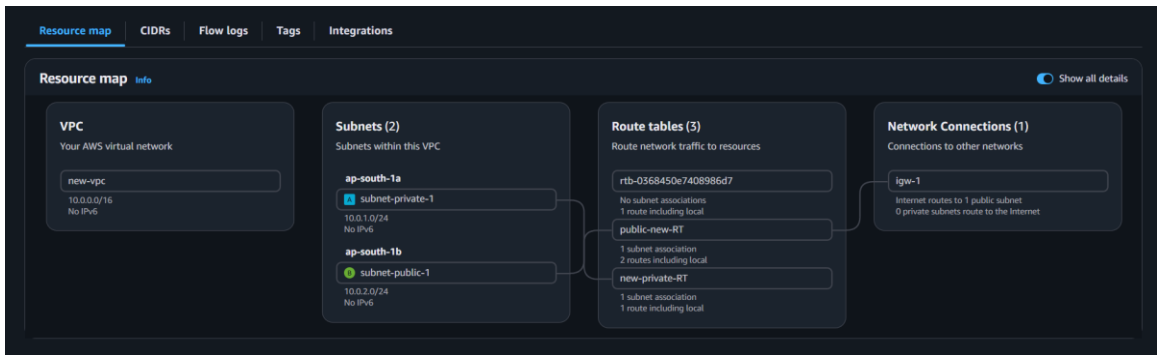


2. Prerequisites

- 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 .

The screenshot shows the AWS Management Console for the 'ap-south-1' region. The left sidebar shows the navigation menu with 'EC2' selected. The main content area displays the 'Instance summary for i-013e6741e6ccfc91f (privatew-server)'. The instance is in the 'Running' state.

| Instance ID | Public IPv4 address | Private IPv4 addresses |
|---------------------|---------------------|------------------------|
| i-013e6741e6ccfc91f | - | 10.0.1.61 |

| IP address | Instance state | Private IP DNS name (IPv4 only) |
|------------|----------------|--|
| - | Running | ip-10-0-1-61.ap-south-1.compute.internal |

| Hostname type | Instance type | VPC ID |
|---|---------------|---------------------------------|
| IP name: ip-10-0-1-61.ap-south-1.compute.internal | t3.micro | vpc-04712a543e110bbf3 (new-vpc) |

| Answer private resource DNS name | Subnet ID | Instance ARN |
|----------------------------------|---|---|
| - | subnet-0029c419e32d044de (subnet-private-1) | arn:aws:ec2:ap-south-1:914471081680:instance/i-013e6741e6cfc91f |

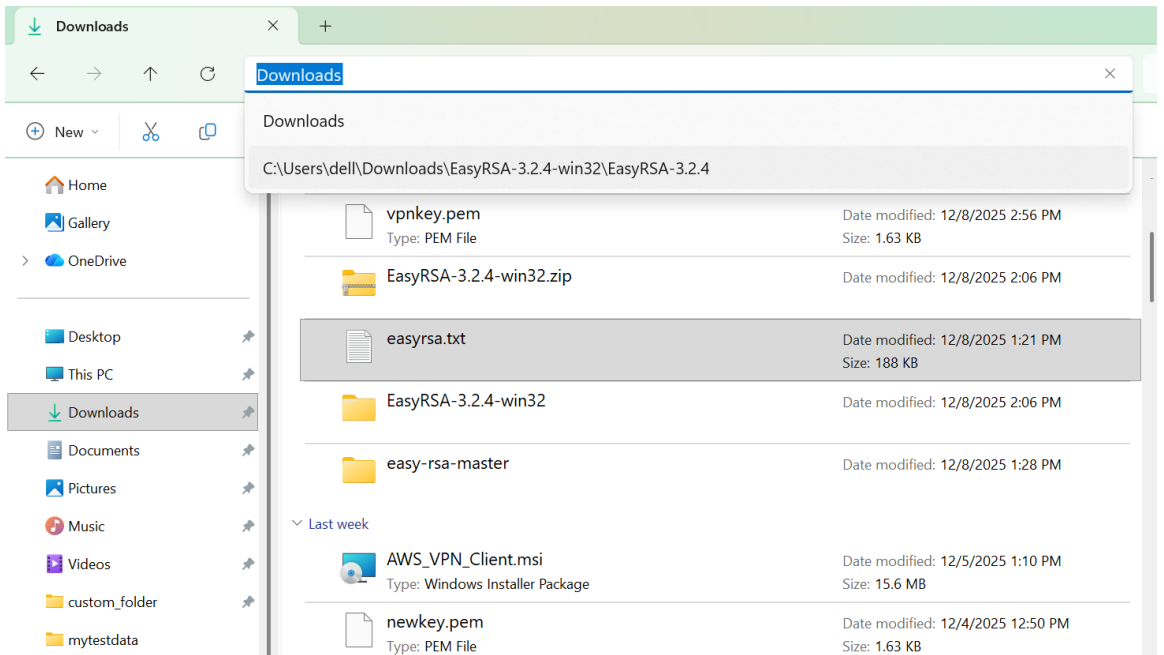
| Auto-assigned IP address | Operator | Managed |
|--------------------------|----------|---------|
| - | - | false |

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
```

```
C:\WINDOWS\system32\cmd. x + v
Microsoft Windows [Version 10.0.26200.7171]
(c) Microsoft Corporation. All rights reserved.

C:\Users\dell>cd C:\Users\dell\Downloads\EasyRSA-3.2.4-win32\EasyRSA-3.2.4
C:\Users\dell\Downloads\EasyRSA-3.2.4-win32\EasyRSA-3.2.4>
C:\Users\dell\Downloads\EasyRSA-3.2.4-win32\EasyRSA-3.2.4>.\EasyRSA-Start.bat
Starting Easy-RSA shell..
WARNING: openssl.exe is not in your system PATH.
EasyRSA will not be able to generate OpenVPN TLS keys.

Welcome to the EasyRSA 3 Shell for Windows.
Easy-RSA 3 is available under a GNU GPLv2 license.

Invoke 'easyrsa' to call the program. Without commands, help is displayed.
dell@DESKTOP-PENMLV7 C:\Users\dell\Downloads\EasyRSA-3.2.4-win32\EasyRSA-3.2.4
EasyRSA-Shell: # |
```

4.2 Initialize PKI environment.

```
#./easyrsa init-pki
```


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

4.4 Generate Server Certificate and key

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

[illegible]

4.5 Generate Client Certificate and key

```
./easysrsa build-client-full client1.domain.tld nopass
```


- 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.

```
C:\Windows\System32\cmd.e  X  +  v
Microsoft Windows [Version 10.0.26200.7171]
(c) Microsoft Corporation. All rights reserved.

C:\Users\de11\Downloads\EasyRSA-3.2.4-win32\EasyRSA-3.2.4>
C:\Users\de11\Downloads\EasyRSA-3.2.4-win32\EasyRSA-3.2.4>mkdir C:\custom_folder

C:\Users\de11\Downloads\EasyRSA-3.2.4-win32\EasyRSA-3.2.4>ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\de11\Downloads\EasyRSA-3.2.4-win32\EasyRSA-3.2.4>ls -ll
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\de11\Downloads\EasyRSA-3.2.4-win32\EasyRSA-3.2.4>ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\de11\Downloads\EasyRSA-3.2.4-win32\EasyRSA-3.2.4>mkdir C:\custom_folder
A subdirectory or file C:\custom_folder already exists.

C:\Users\de11\Downloads\EasyRSA-3.2.4-win32\EasyRSA-3.2.4>mkdir C:\custom_folder
A subdirectory or file C:\custom_folder already exists.

C:\Users\de11\Downloads\EasyRSA-3.2.4-win32\EasyRSA-3.2.4>copy pki\ca.crt C:\custom_folder
1 file(s) copied.

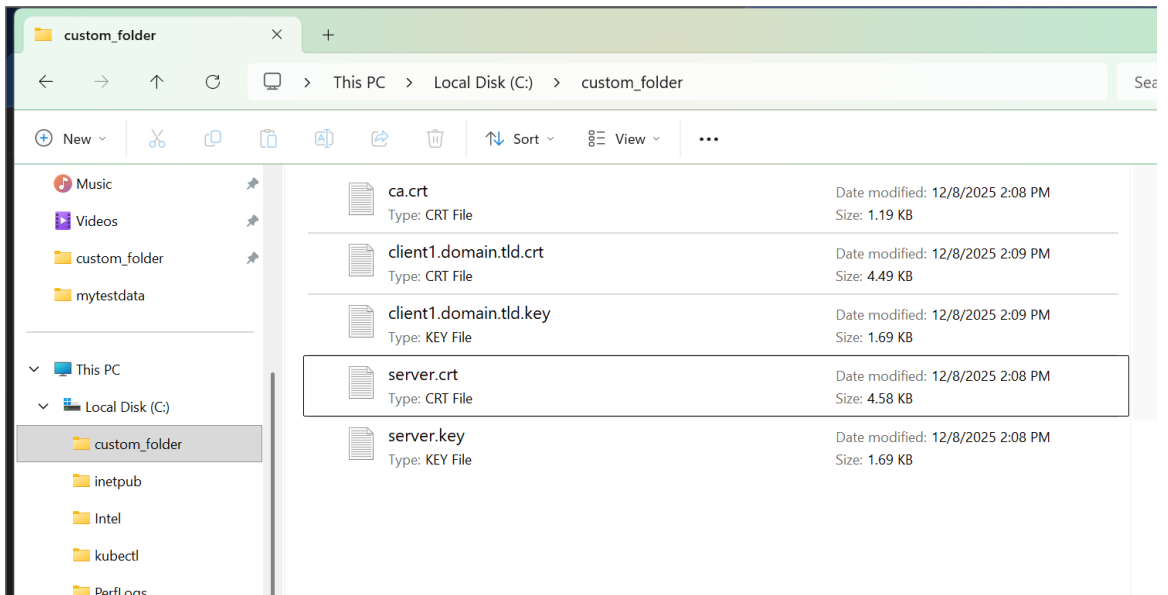
C:\Users\de11\Downloads\EasyRSA-3.2.4-win32\EasyRSA-3.2.4>copy pki\issued\server.crt C:\custom_folder
1 file(s) copied.

C:\Users\de11\Downloads\EasyRSA-3.2.4-win32\EasyRSA-3.2.4>copy pki\private\server.key C:\custom_folder
1 file(s) copied.

C:\Users\de11\Downloads\EasyRSA-3.2.4-win32\EasyRSA-3.2.4>copy pki\issued\client1.domain.tld.crt C:\custom_folder
1 file(s) copied.

C:\Users\de11\Downloads\EasyRSA-3.2.4-win32\EasyRSA-3.2.4>copy pki\private\client1.domain.tld.key C:\custom_folder
1 file(s) copied.

C:\Users\de11\Downloads\EasyRSA-3.2.4-win32\EasyRSA-3.2.4>cd C:\custom_folder
```



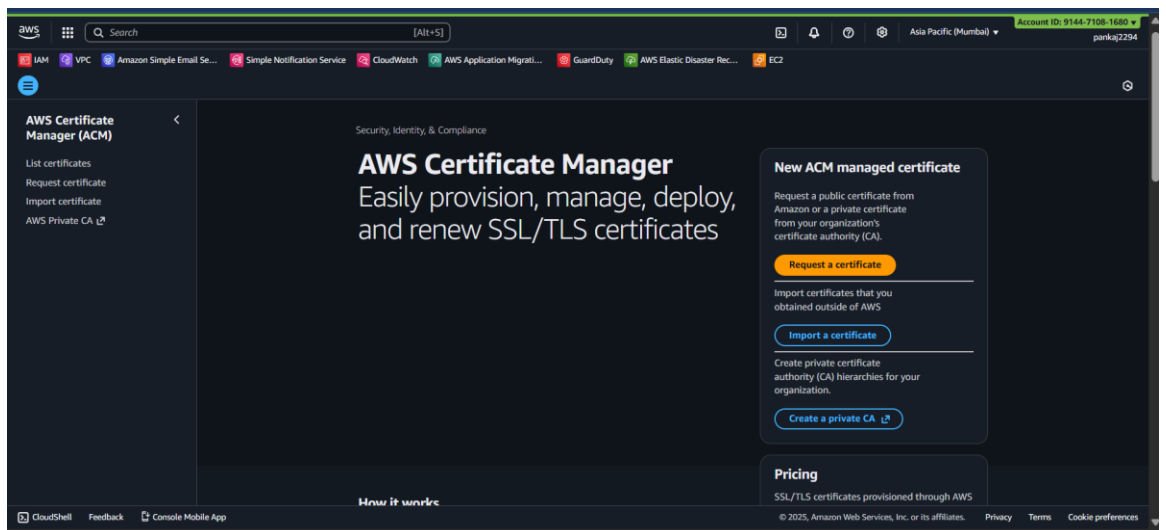
You can see in the above screenshot the custom folder has been created now and all copied files are there.

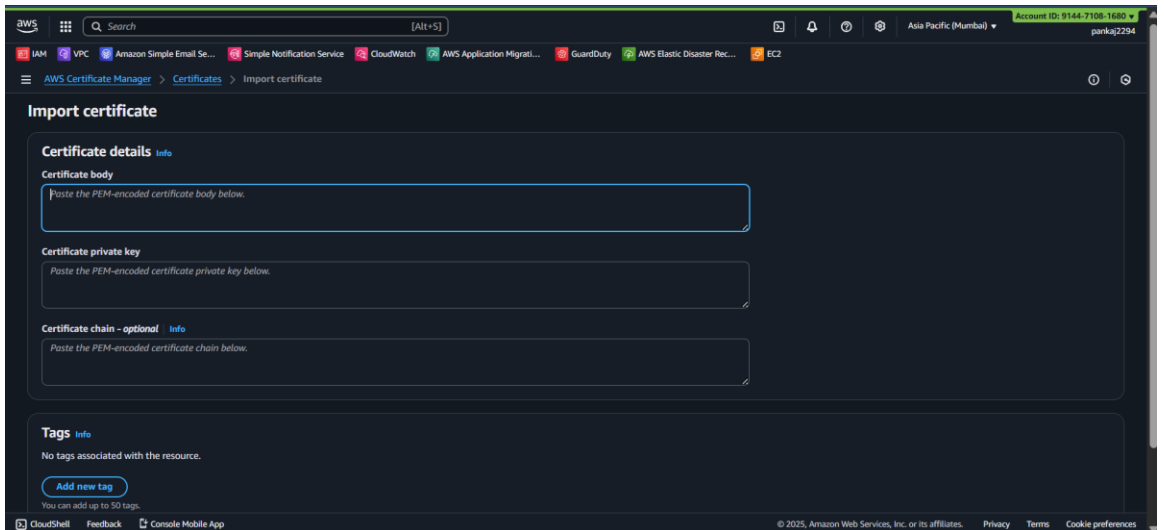
5. Import Certificates to AWS ACM

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 \  

```

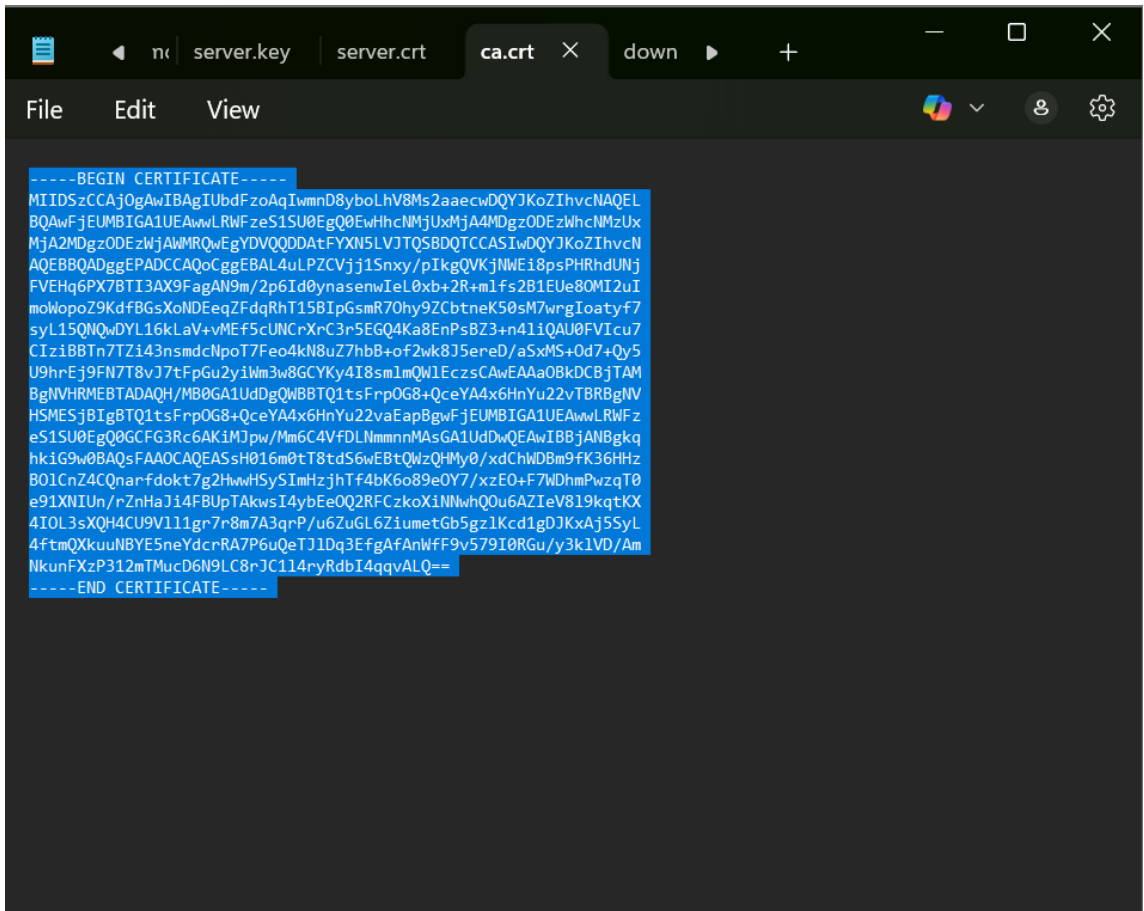
```
51:a9
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
X509v3 Subject Key Identifier:
89:81:DD:DA:F1:27:72:F6:E4:74:D7:31:77:95:A1:A5:79:2C:02:D1
X509v3 Authority Key Identifier:
keyid:D0:D6:D8:05:AE:93:86:F3:E4:1C:79:80:38:C7:A1:E7:62:ED:B6:8D
DirName:/CN=Easy-RSA CA
serial:6D:D1:73:0A:0A:88:C2:69:C3:F3:26:E8:2E:15:7C:32:CD:9A:69:E7
X509v3 Extended Key Usage:
TLS Web Server Authentication
X509v3 Key Usage:
Digital Signature, Key Encipherment
X509v3 Subject Alternative Name:
DNS:server
Signature Algorithm: sha256WithRSAEncryption
Signature Value:
90:55:38:44:70:8e:fd:12:56:6c:00:a4:d2:ac:8d:75:ad:b2:
57:f2:2d:58:47:d3:1e:74:58:30:e7:05:87:22:b7:bc:59:5b:
cf:e4:6d:df:14:ef:6a:ca:21:f9:0a:41:18:92:d0:73:cc:df:
f0:2f:72:03:15:6b:b1:ce:c9:5c:65:2c:45:ff:81:d2:42:15:
eb:d7:e8:8d:f7:d5:5e:54:97:76:c6:54:20:ef:8d:09:98:bb:
d2:48:c5:de:b3:e9:0f:ee:79:d8:d2:d9:48:70:b1:b8:1d:47:
d0:6e:f4:d9:47:1c:d7:6d:e7:91:1c:85:d8:e0:0a:21:a2:21:
bc:39:62:51:9a:2d:66:4c:b0:0d:30:b3:76:f8:42:f5:07:c3:
92:d2:3d:c5:3b:89:e9:7f:03:7c:61:17:de:76:46:34:46:d3:
73:46:d0:60:ef:80:0b:65:26:30:2f:8f:71:b0:04:70:9b:47:
cd:69:57:31:ca:ad:6d:8a:6f:11:c3:2b:2d:85:65:3c:e7:31:
71:2e:da:8b:d0:32:b0:8e:18:61:80:65:4b:da:3c:25:4a:c7:
49:f5:86:67:04:e3:a0:c8:21:f3:8a:fc:f7:d5:52:9f:b5:7b:
54:23:cd:68:e2:b6:4c:e4:c6:53:ac:fd:35:2d:e4:71:7e:ba:
45:19:5a:ec
-----BEGIN CERTIFICATE-----
MIIDZzCCAkgAwIBAgIQVBgt3u+NVn3oOYMj19DuXjANBgkqhkiG9w0BAQsFADAW
MRQwEgYDVQDDAtFYXN5LVJ1TQ5BDQTAeFw0yNTEyMDgwODM4MzZaFw0yODAzMTIw
ODM4MzZaMBExDzANBgNVBAMwBmN1cnZlcjCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBALaApM4hpJdPhA8U5A13TUey01skekFwSmxEck2mMG6ArzvwC2FY
BR6CnRp/4k3dAKxxy7iHwH31eGJSH18m28f6pUswd13kcUwOzEX9n620KCVcjz1h
QQTLCz507ycYVrBeBqp3Yn68zZeG2xvJSq2J/f/02xe892WcngI9Nz/0Wvjuz5+Z
rYBcdHRy5KYyywoL8i0gdT0qkZw/nG1yDnImgn74+9ENCq1CsSf2uw5IZ34JnBR
HSVBZ0m6Yq2ZiGQHL6SoqYCAwNFFUmSiAsx0diV1v735rXLCqnMvYwFvjEXCmUQ
1wa37Cnt291U0f188ebTgSABC0wUrvSUakCAwEAa08tTCBsJAjBglNVHRMjAA
MB0GA1UdDgQwBBBSjd3a8Sdy9uR01zF31aG1eSwC0TBRBgNVHSMESjB1BGTQ1tsF
rp0G8+QceYA4x6HnYu22vaEapBgfjEUMBIGA1UEAwwLRWfzeS1SU0EgQ0GCFG3R
c6AK1Mjpw/Mm6C4VfDLNmmnnHBNGA1UdJQQwMAoGCCsGAQUFBwMBMAcGA1UdDwQE
AwIFoDARBgNVHRECjAIGgzZzXJ2ZXIwDQYJKoZIhvcNAQELBQADggEBAJBVOERw
jv0SVmmApNKsJXWtsIfyLVhH0x50wDDnBYcit7xZW8/kbd8U72rKIfkKQRiS0HPM
3/AvvcMva7H0yVx1LEX/gdJCFevX6I331V5U13bGVCDvjQmYu9JIXd6z6Q/uedjS
2UhwsgbdR9Bu9N1HHndt55EchdjgCiG1Ibw5Y1GaLWZMsA0ws3b4QvUhw5LSPcU7
ie1/A3xhF952RjRG03NG0GdvGAt1JjAvj3GwBHCbR81pVzHKrW2KbxHDKy2FTzn
MXEu2ovQMrCOGGAZUvaPCVKx0n1hmcE46DIIFOK/PfVUp+1e1QjzWjitzkx10s
/Tut5HF+ukUZWuu=
-----END CERTIFICATE-----
```

Ln 62, Col 37 | 4,609 characters | Plain text | 60% | Windows (CRLF) | UTF-8

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

```
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBAgEAAoIBAQC2gKTOIaSXT4QP
FOQCd01HsjpbJHpBcEpsRHJNpjRugK878AthWAUegp0af+JN3QCsbMu4h8B99Xhi
Uh5QZtvH+qVEsHYt5HFMDsxF/Z+ttCgrwic9YUEEy3M+Tu8nGFawXgaqd2J+gc2X
htsbyUqtif3/9NsXvPdlnJ4CPTc/9Fr47s+fma2AXHR0cuSmMssKC/IjoHU9KpGc
P5xtcg5zSJoDe+PvRDQqtQrEn9rsOSGd+CZWUR0lQWTpumKtmYoEBY+kqKmAqMDR
RVJkogLMdHYlWJb+9+a1ywqpzFclhb4xFwplEncGt+wp7dvdVIdBZfPHm04EgAQ
tMFK70lGpAgMBAAECggEAV+9FOWMBdLymA0RMFpoYPN71+jtpwsURvvf94UcfhUzw
4h7nXNgN42UIwJ900ZKwg/4J7NhQGgDgJ/OsUo41ALbW0fF6h+NF6eFJcMHjIeWn
42mx0YPe0aq1QZgegRipKkxagqLBSyS/JtIUkudFV/jaGQ4+secprOfELG5QNE
4NB0AJ000v4LEqWPl0FxAmdZNE9V4iLCJm5u+leBPHGXY5pNTKxDgmVz1nzmGW
BuAy2YimglWqQ02fMoPkj+G6GQ8VhwzMio3AnFh058v9/w09USvNV30kuKamywa7
tHPEBCmn1JzJ3rBnpsEIRU0Bse7Hr5ykGvT6/Li5ZwKBgQDp3IpDc5L4qxwJpZ2Q
1AevLxfi/KgrAoGJ+yy6KX/GwK9jCPAIGFovY9ZFLJ5yQSA9IqY25jZxZMN0mcL
Zw90TYfspzyWtJOpIZHmkShQ1Hn1My/AMQ7bm+LDXKhrjND6XI+iZdagypZw4L52
uvuB8oS5RSawiUreGpOZ0cIaiwKBgQDHx3UCp/t5fj5Xt1LvU60ADzP5Jy4Z03SF
Kyb5CQxisC9FQug4rDkV97xuESi9Yn0BA+aRrFC4QMewSJsosn1CkCs7i3wvOKL
ZjdeUwXAbnzwg79z5B5b9FK/He4U+CZqaHZch7hbgDJ00acZz3W7Ss7NIUKswobR
ODdLra4vGwKBgQDd6TQaBVV10YkduSjGgSw5g8p6zZ0WEu6w6/LpQ+/HvZevtg9U
3wzU4zuzsD8506qgffv2SIqmOuDrMHwPSeBUUC2m1pqbtwZW+0/jJeLHsJd5oPSy
vtqGcUmgcBAw3hJ/P83cIB61vRc8TUbuioeVa3eeBoxMADtWvolI8M3rOQKBgER7
Iaf8bx5xY0tuKzXUSzJ9g6JXhNzzA+EWLrDVIjK+FCYYzkOG/baDcktshFu040sL
rECpIa5XP1NMpi7oEW76ubrN1l/cT4fbTQWiZ/IaLafAcaNHQgThVm/+0XrMqVZ2
YoRLXa233wbXpQEa9U9zUDpOuW1A7TfQnlvJuFibAoGBALi0xnUodFn9kZAW1bvw
TAd80vflbJ2m6TOWBuCPwxy7ErSBtJMjZ+Wo+1AISJuC9BNUBe9Z754ivpFUPOKd
cJDctegrVRYX0/Js/SMq41PNoyuAulva0tfbCBKQFWTxUvr9DuV/OENqdLdE6Tx
wxy+KPe38D35fPisowt940K1
-----END PRIVATE KEY-----
```

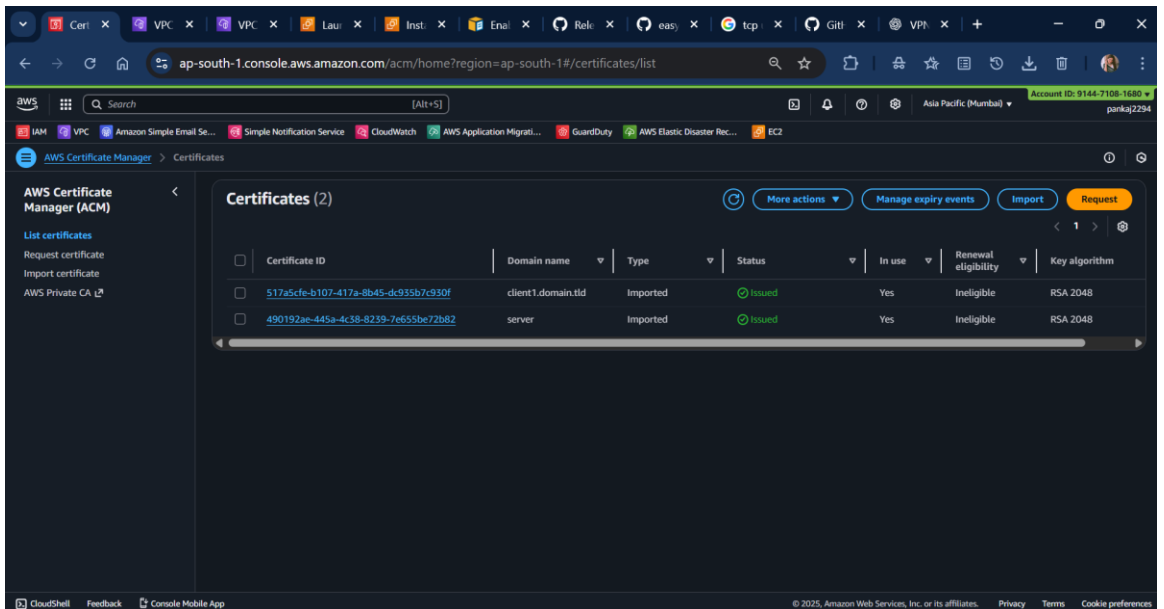
--certificate-chain fileb://ca.crt



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

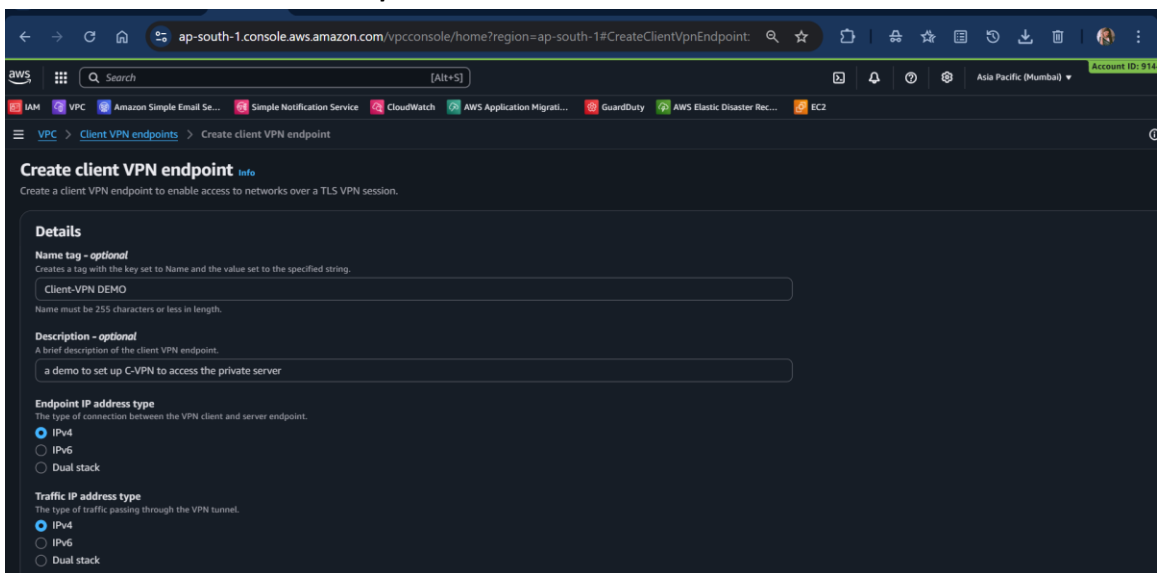
```
aws acm import-certificate \  
  --certificate fileb://client1.domain.tld.crt \  
  --private-key fileb://client1.domain.tld.key \  
  --certificate-chain fileb://ca.crt
```

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

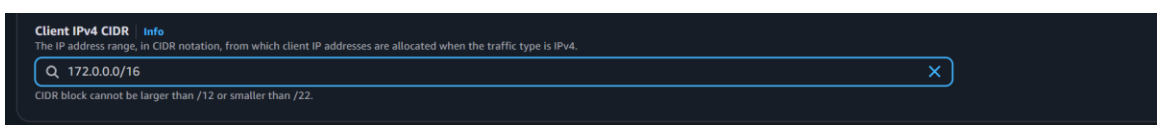


Here in the above screenshot of **AWS ACM imported certificates** you can see in the AWS ACM List Certificates dashboard.

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.

The screenshot shows the AWS Management Console interface for creating a client VPN endpoint. The 'Authentication information' section is active, and the 'Server certificate ARN' field is selected. A dropdown menu displays two certificate ARNs: one for a server certificate and one for a client certificate. The server certificate is selected.

Paste ACM ARN.

5.4 Authentication

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

The screenshot shows the 'Authentication options' section of the AWS Management Console. The 'Use mutual authentication' checkbox is checked. The 'Client certificate ARN' field is selected, and a dropdown menu displays two certificate ARNs: one for a server certificate and one for a client certificate. The client certificate is selected.

5.5 Connection Logging

Optional.

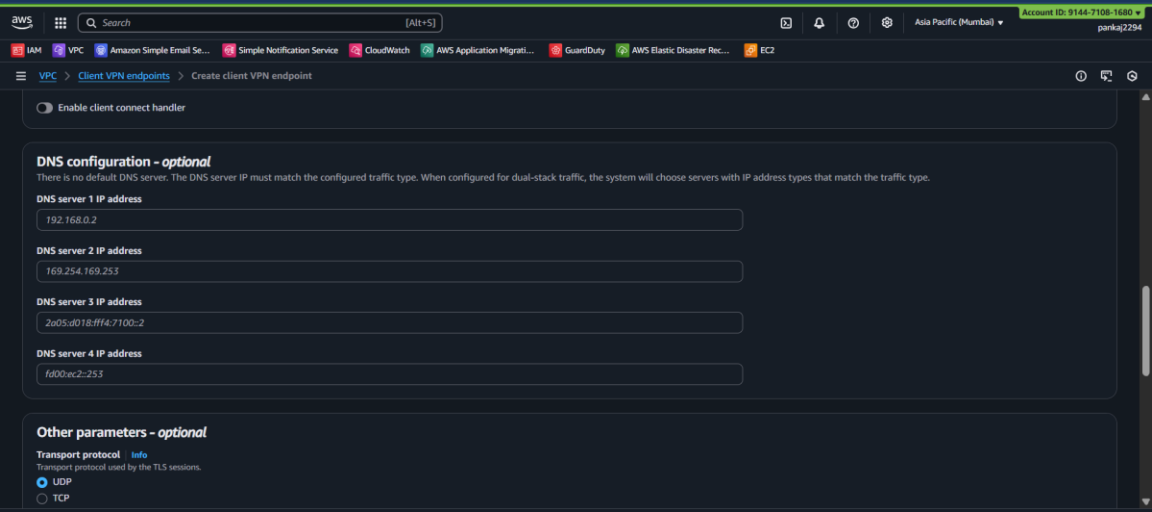
The screenshot shows the 'Connection logging' section of the AWS Management Console. The 'Enable log details on client connections' checkbox is checked. The 'CloudWatch logs log group name' field is selected, and a dropdown menu displays 'Select log group'. The 'CloudWatch logs log stream name - optional' field is also selected, and a dropdown menu displays 'Select log stream'.

5.6 DNS Servers

Use:

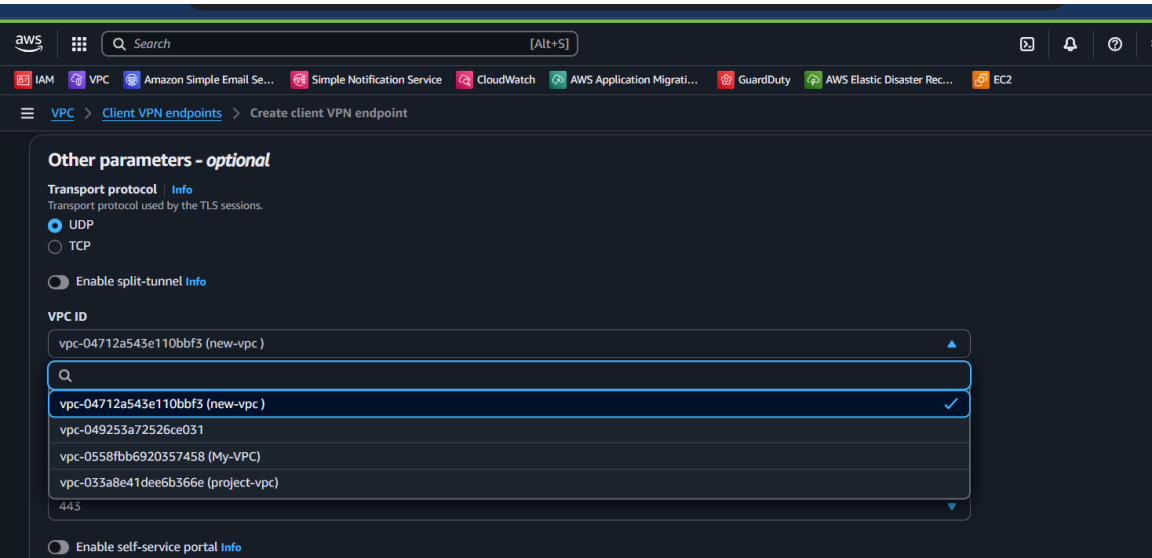
8.8.8.8

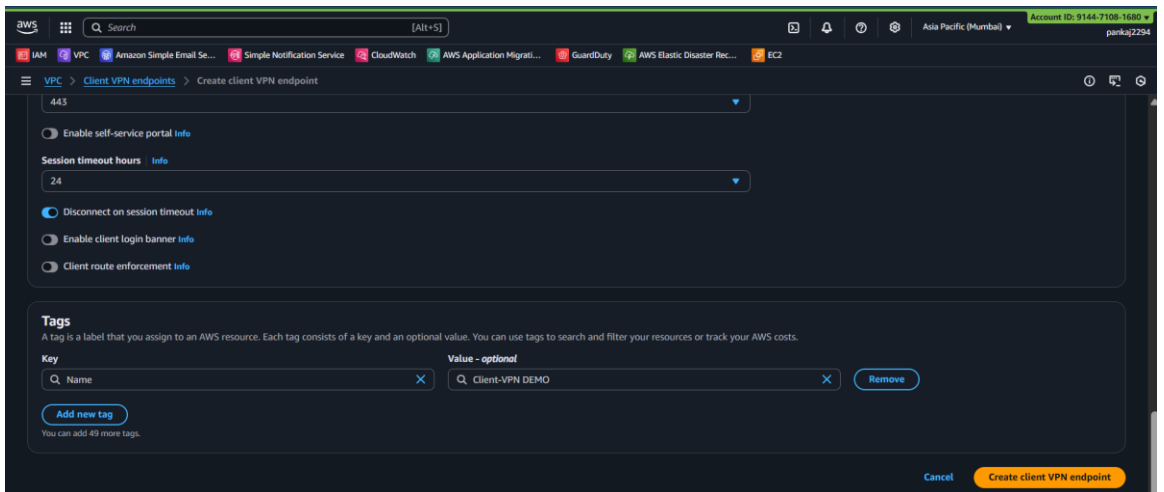
Click **Create Client VPN Endpoint**.



5.6 Others Parameters—Optional

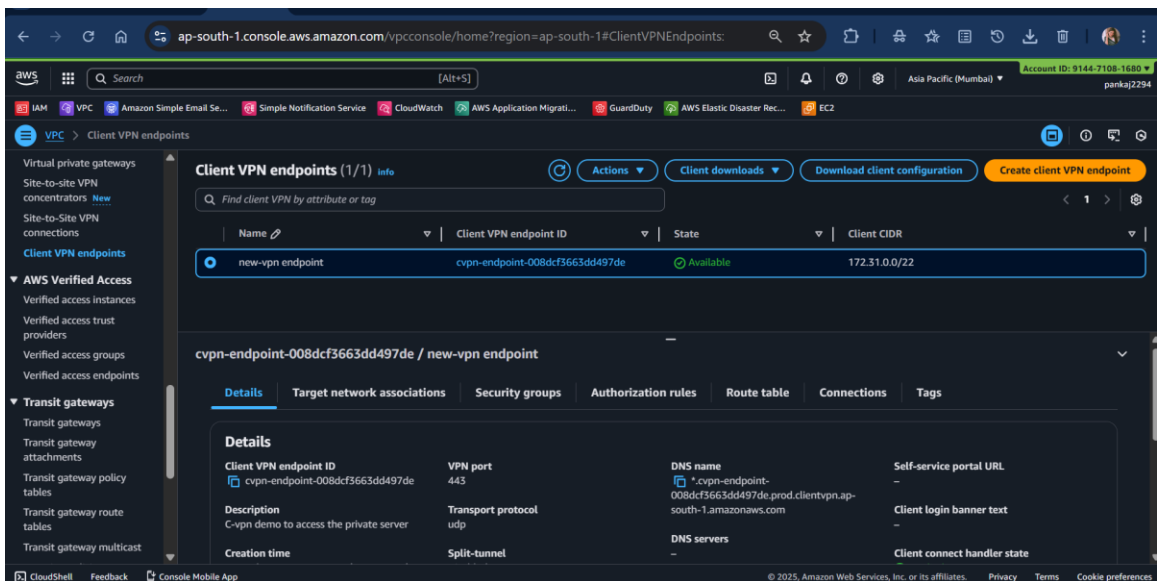
5.7 Now choose your VPC.





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

Associate target network info

A target network is a subnet in a VPC. You associate a subnet in an Availability Zone to the client VPN endpoint. You can associate one subnet per Availability Zone. You can associate subnets in one VPC to a client VPN endpoint.

Details

Client VPN endpoint ID
cvpn-endpoint-008dcf3663dd497de

VPC
vpc-04712a543e110bbf3 (new-vpc)

Choose a subnet to associate
subnet-0029c419e32d044de (subnet-private-1)

Cancel Associate target network

Client VPN endpoints (1/1) info

Find client VPN by attribute or tag

| Name | Client VPN endpoint ID | State | Client CIDR |
|------------------|---------------------------------|-----------|---------------|
| new-vpn endpoint | cvpn-endpoint-008dcf3663dd497de | Available | 172.31.0.0/22 |

cvpn-endpoint-008dcf3663dd497de / new-vpn endpoint

Details Target network associations Security groups Authorization rules Route table Connections Tags

Target network associations (1) info

Find target network associations by attribute

| Association ID | State | Network ID | Security groups | Endpoint ID |
|-------------------------------|------------|--------------------------|----------------------|-------------------------------|
| cvpn-assoc-0b925278195eb9c... | Associated | subnet-0029c419e32d044de | sg-05894f53953820f7b | cvpn-endpoint-008dcf3663dd... |

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

VPC > Client VPN endpoints > cvpn-endpoint-008dcf3663dd497de > Add authorization rule

Add authorization rule info

Add authorization rules to grant clients access to the networks.

Details

Client VPN endpoint ID
cvpn-endpoint-008dcf3663dd497de

Destination network to enable access
The IP address, in CIDR notation, of the destination network.

Grant access to:
☒ Allow access to all users
☐ Allow access to users in a specific access group

Description - optional
A brief description of the authorization rule.

Cancel Add authorization rule

Target network associations Security groups **Authorization rules** Route table Connections Tags

Authorization rules (1) info

Find authorization rule by attribute or tag

Remove authorization rule Add authorization rule

| Endpoint ID | State | Description | Group ID | Access all | Destination CIDR |
|---------------------------------|--------|-------------|----------|------------|------------------|
| cvpn-endpoint-008dcf3663dd497de | Active | - | - | True | 0.0.0.0/0 |

8. Add Route to VPC

Go to:

Client VPN - Routes - Add route

Route destination: 10.0.0.0/16

Target: associated subnet.

VPC > Client VPN endpoints > cvpn-endpoint-008dcf3663dd497de > Create route

Create route info

Add a route to specify how traffic is directed to the destination network.

Details

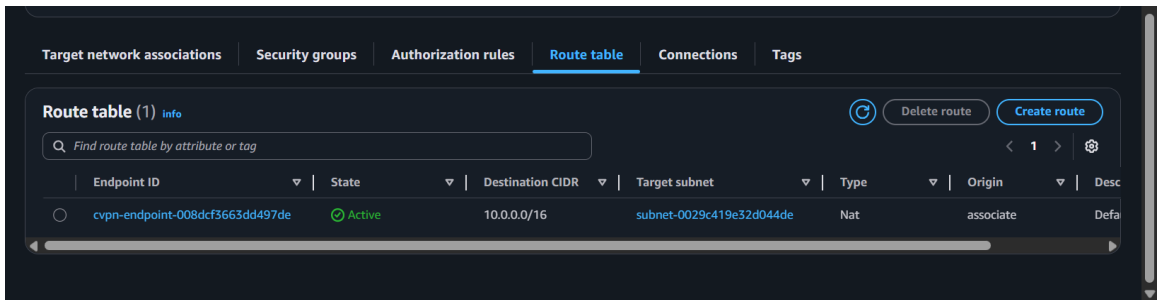
Client VPN endpoint ID
cvpn-endpoint-008dcf3663dd497de

Route destination
CIDR range for the destination network.

Subnet ID for target network association
local indicates the client VPN endpoint network.

Description - optional
Description of the route.

Cancel Create route



9. Update Security Group on Private EC2

Add this rule:

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

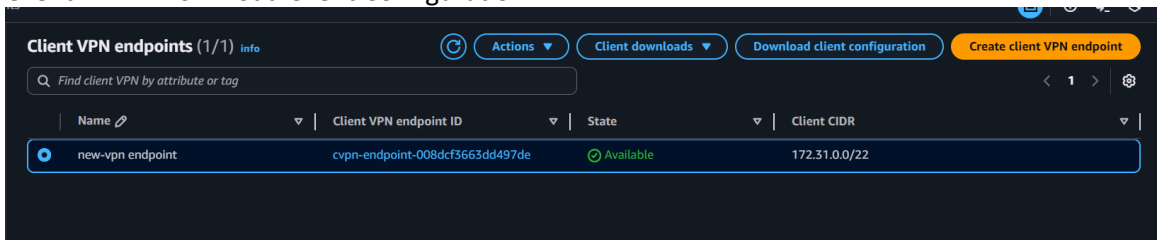
- Type: SSH
- Source: 192.168.100.0/22 (your Client CIDR)

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>
```

downloaded-client-config (1).ovpr

File Edit View

```
-----BEGIN CERTIFICATE-----
MIIDYTCACmAwIAAgIRAIc+U7g/xCTqtY939YsMggwDQYJKoZIhvcNAQELBQAw
FjEUMBIGA1UEAwRLRWZzeS1SU0EgQ0EwHhcNMjUxMjA4MDgzOTEzWWhcNMjgwMzEy
MDgzOTEzWjAdMRswGQYDVQDD8jbjG1bnQxLmRvbWVpb150bGQwggEiMA0GCSqG
S1B3DQEBAQUAA4IBDwAwggEKAoIBAQCdRLfB8QsNETtVrMB7G6tH0JkHEbT532F7
tJDP26KT5k7oKvNMx1JfDSVMzbZ1g4nXg+915HGdZEUCZe004UI48AOCB7IIMshp
+gtWRk04PNCfDAA2fDDQ1/YFVN+mS98QQsC814b0btNxD79abDXv0XYxFAG9G/A9
WqMASxug4TcBMFZpvaex4s1Q1IH+0LA1JnNgfHzm7tCZA00+NsfASJzoY6GDwqsm
mYx/+4L93yo7RTocNy30raUh2/z8EwdDVk3LuMQmsaf3BHtVuuqc+eEc6FUTT14N
FOJFk8QMLCK0rvzckL19rWQaK/zHHk2Ak1zYysuFwto4I3m/w+1TAGMBAAGjgaIw
gZ8wCQYDVROTBAlwADAdBgNVHQ4EFgQUByl/gYUin5L4kh1cr07FqeaxbQswUQYD
VR0jBEowIAU0NbbBa6ThvPKHhMA0Meh52Ltr2hgQYMBYxFDASBGNVBAWMC0Vh
c3ktULNBIENBghRt0X0GCojCacPzJuguFXwyzZpp5zATBgNVHUEDAKBggrBgEF
BQcDAjAlBgNVHQ8EBAMCB4AwDQYJKoZIhvcNAQELBQADggEBADa69wEbX1naKUyR
uvVMc4trfFh14EI8LoPaQNYTq7WmZuR0Kt0BvWZf+15XFqAuAz/oZF7CUuqnAvYo
kgmxmLxFP5/1t2XkkrVPJ2qXjV7QoNwYnIy6/5gvjRooqihm31J8bd+S05IYHD3N
knHTDgteOIu4+GAw+7Y0PEat9fJqoRmXdpT+bX8BY7CbZ2CR8Wg8r+/fMcJfFtae
z40a9pFAH1K6P+9RTc28IBQr-Suk4NjhQ4DDZIMSJEJXdiG8ER0GqsM3ELowihj5y
mkMLlFtsXo2ZjZGoYsDoz8YxKaQvN7opN1SyOq+1MTGPMjw8ImCuOXsNqTnhhFW4
+uOWsFM=
-----END CERTIFICATE-----

</cert>

<key>
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQCdRLfB8QsNETtV
rMB7G6tH0JkHEbT532F7tJDP26KT5k7oKvNMx1JfDSVMzbZ1g4nXg+915HGdZEUC
Ze004UI48AOCB7IIMshp+gtWRk04PNCfDAA2fDDQ1/YFVN+mS98QQsC814b0btNxD
79abDXv0XYxFAG9G/A9WqMASxug4TcBMFZpvaex4s1Q1IH+0LA1JnNgfHzm7tCZ
A00+NsfASJzoY6GDwqsmmYx/+4L93yo7RTocNy30raUh2/z8EwdDVk3LuMQmsaf3
BHtVuuqc+eEc6FUTT14NFOJFk8QMLCK0rvzckL19rWQaK/zHHk2Ak1zYysuFwto4
I3m/w+1TAGMBAAGjEAKj5/o5FwF1R85bSjAdNPqSLHgASUwevOjwQW9dZgus7L
yVkbakVJzfl+eVlmqeJ9Ubj6+axJ4doeMpDt05aXgMiGRkSwHGZ4EFVUUmK1VYy
g8+4jrqIviZpm6IodoNM15jF0Cwbe1uZ77AeeeARBBp++XCL2Lf3/jxY0KCK/uZ3
fjIpZtsncq6Z23VOWs0a9p91vn1DBHwujgnnbIuF5Db6IwAmkcE3LOCdREuEy8Hq
zQ1bSjwq0IiDGv3EQhFJcrIEqEFt8iMhdm0VthWADA5pcsnKK/jwZTvYIaTnTSQx
-----END PRIVATE KEY-----

</key>
```

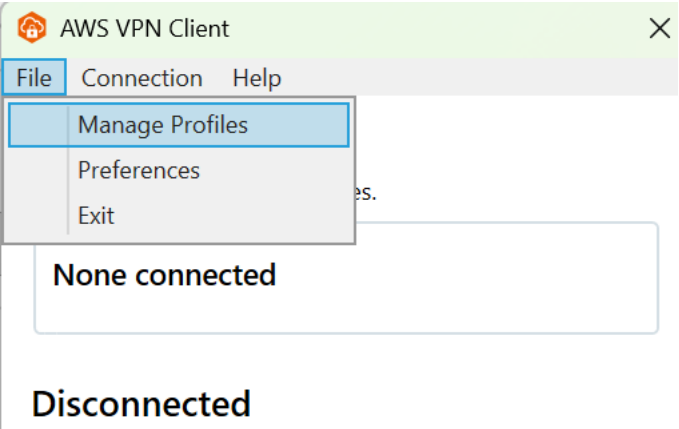
Ln 38, Col 25 | 7,723 characters | Plain text

Save.

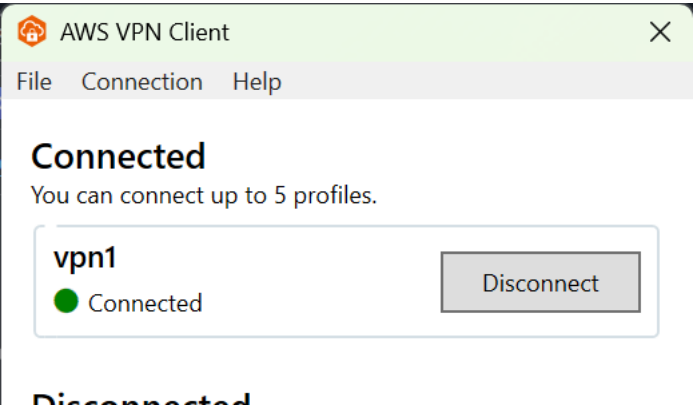
Insert client certificate and key inside the .ovpn file.

11. Connect Using AWS VPN Client

Open AWS VPN Client → Import configuration → Connect.

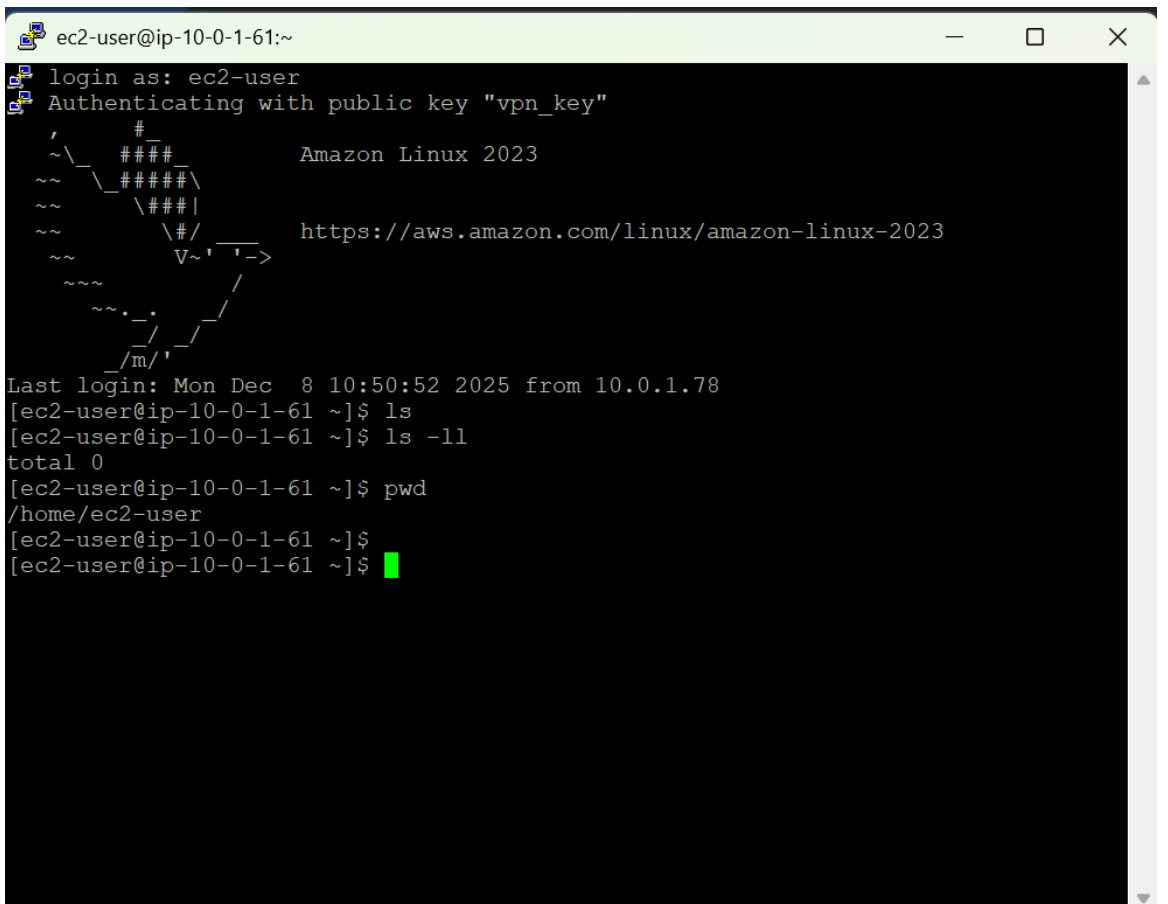
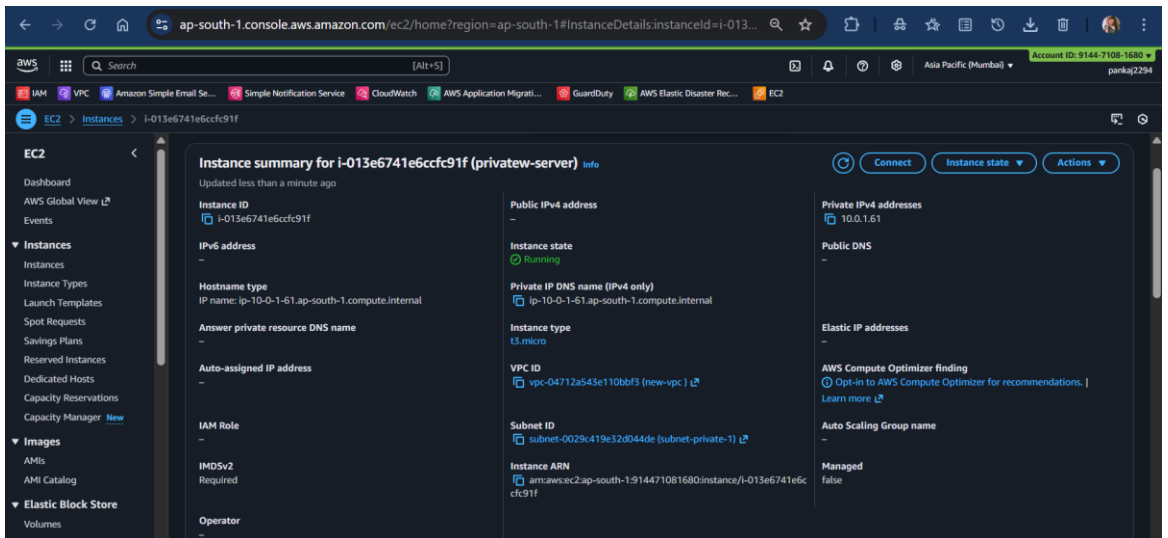


You should receive an IP from the pool: 192.168.100.x

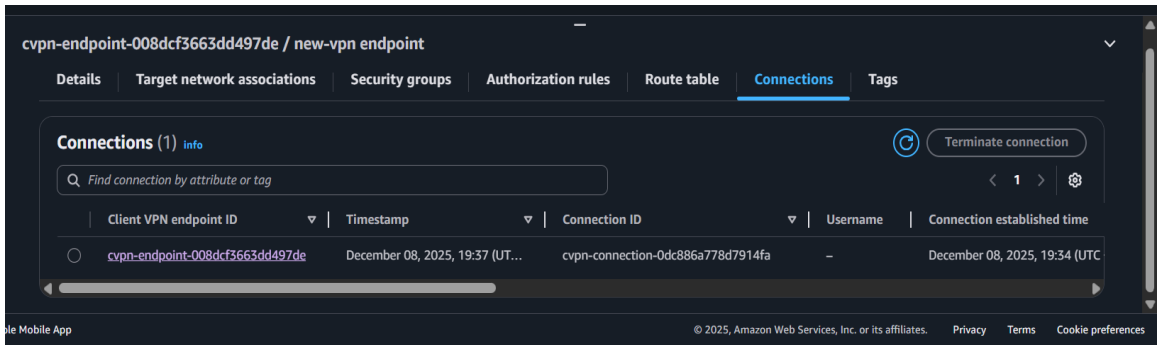


12. Validate Connectivity

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.
