

AWS Client VPN – Step-by-Step Implementation Guide

Contents

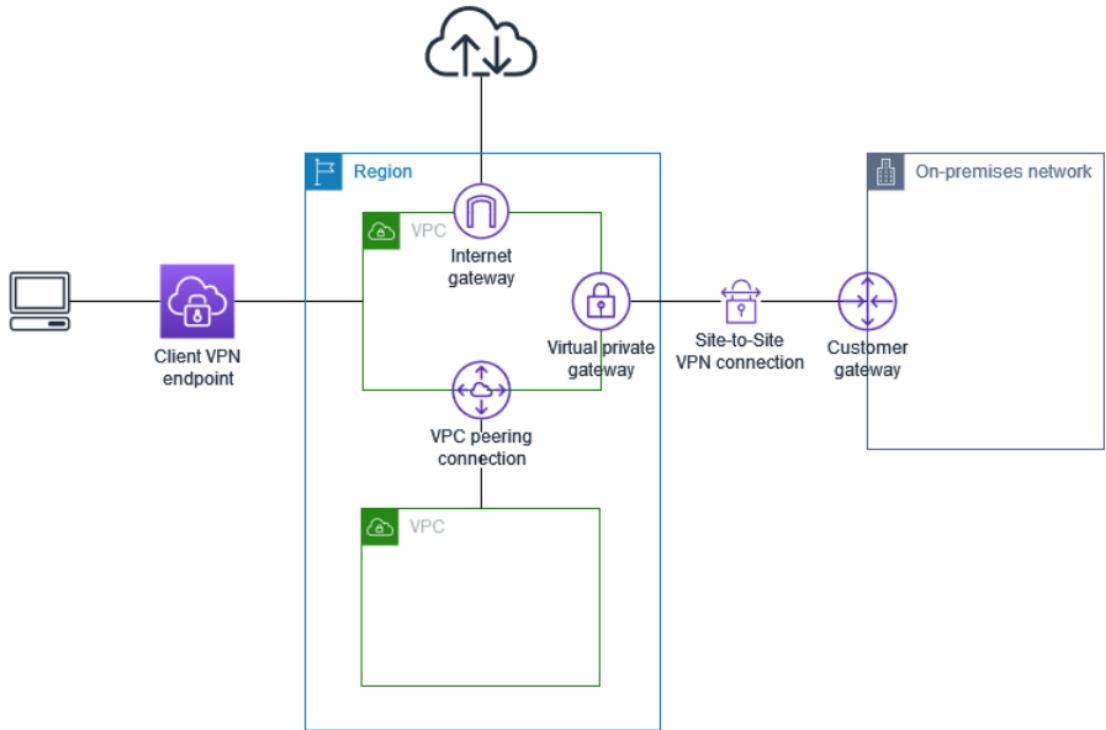
AWS Client VPN – Step-by-Step Implementation Guide	1
What is AWS Client VPN?.....	2
1. Architecture Overview	2
2. Prerequisites.....	3
3. VPC Architecture overview:	3
Private EC2 Instance for test connectivity	4
4. Create Server & Certificate Creation Using EasyRSA.....	4
4.1 Install EasyRSA (Windows).....	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 <i>Create AWS Client VPN Endpoint</i>	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

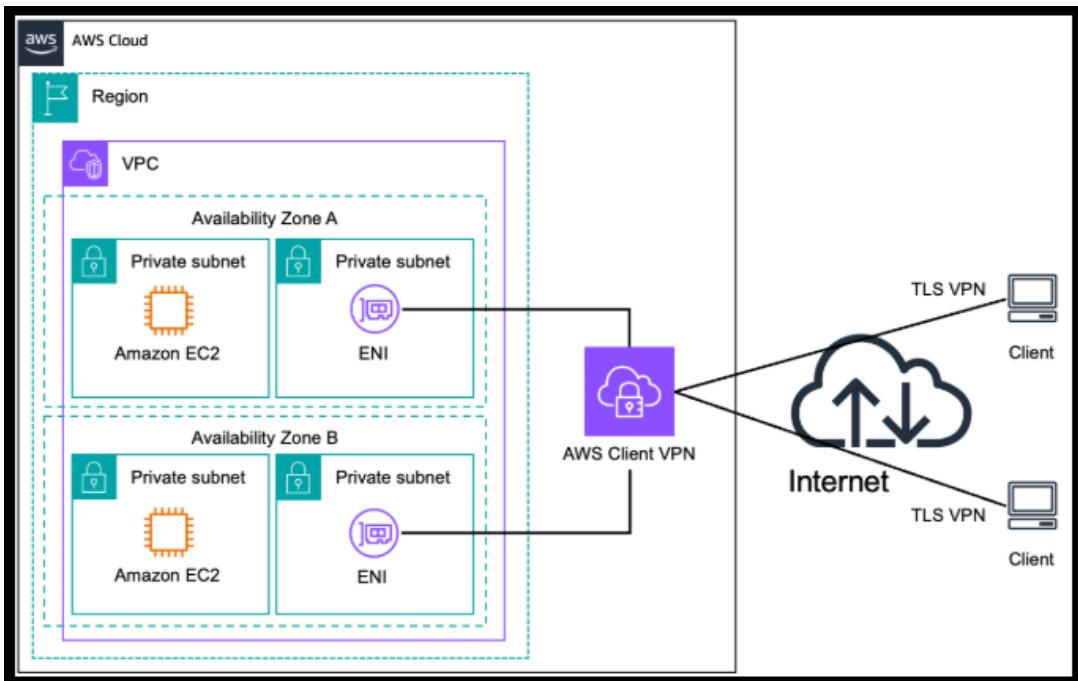
What is AWS Client VPN?

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:

The screenshot shows the AWS VPC console interface. At the top, the URL is ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#VpcDetails?VpcId=vpc-0... and the account information is Account ID: 914471081680, Region: Asia Pacific (Mumbai), User: pankaj2294. The navigation bar includes links for IAM, VPC, Amazon Simple Email Se..., Simple Notification Service, CloudWatch, AWS Application Migr..., GuardDuty, AWS Elastic Disaster Rec..., and EC2. The current view is under the VPC section, specifically for 'Your VPCs'.

The main content area displays the details of a VPC named 'new-vpc'. The VPC ID is listed as vpc-04712a543e110bbf3. The VPC status is 'Available'. Other details shown include:

- State:** Available
- Tenancy:** default
- Default VPC:** No
- Network Address Usage metrics:** Disabled
- Encryption control mode:** -
- Block Public Access:** Off
- DHCP option set:** dopt-09c25c41a5e9c7394
- IPv4 CIDR:** 10.0.0.0/16
- Route 53 Resolver DNS Firewall rule groups:** -
- DNS hostnames:** Disabled
- Main route table:** rtb-0368450e7408986d7
- IPv6 pool:** -
- Owner ID:** 914471081680

At the bottom right of the details card, there is an 'Actions' button.



Private EC2 Instance for test connectivity .

The screenshot shows the AWS EC2 Instances details page for instance 'i-013e6741e6ccfc91f'. The left sidebar shows navigation options like Dashboard, AWS Global View, Events, Instances, Images, and Elastic Block Store. The main content area displays the following details:

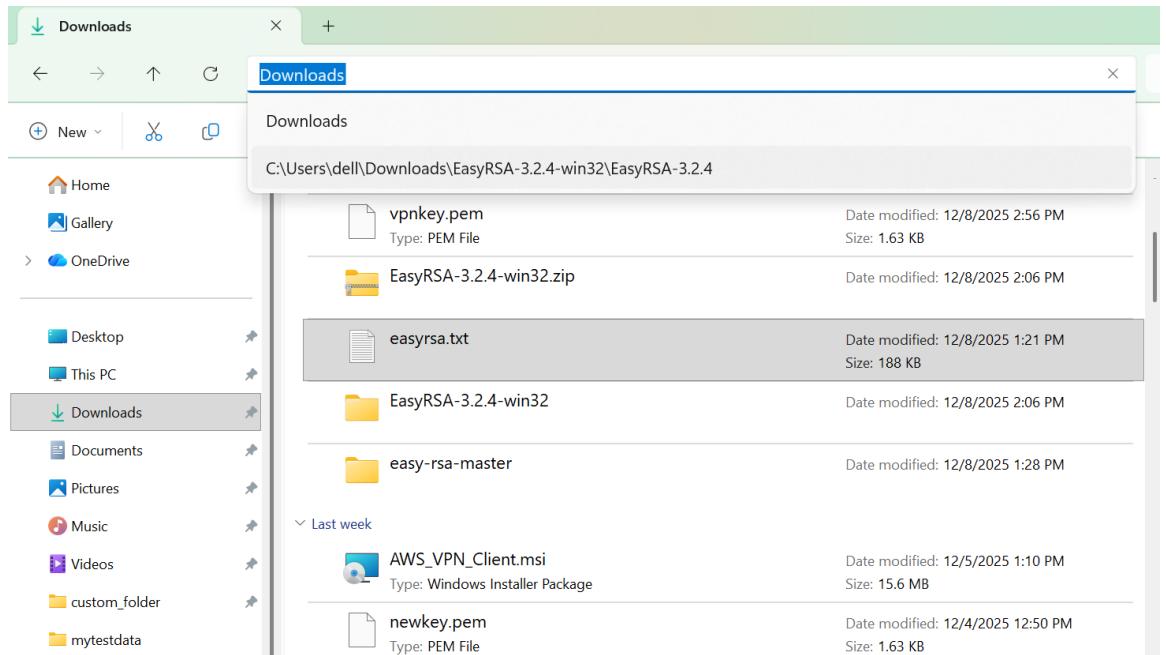
Instance summary for i-013e6741e6ccfc91f (privatew-server)	
Updated less than a minute ago	
Instance ID	i-013e6741e6ccfc91f
IPv6 address	-
Hostname type	IP name: ip-10-0-1-61.ap-south-1.compute.internal
Answer private resource DNS name	-
Auto-assigned IP address	-
IAM Role	-
IMDSv2	Required
Operator	-
Public IPv4 address	-
Instance state	Running
Private IP DNS name (IPv4 only)	ip-10-0-1-61.ap-south-1.compute.internal
Instance type	t3.micro
VPC ID	vpc-04712a543e110bbf3 (new-vpc)
Subnet ID	subnet-0029:419e32d044de (subnet-private-1)
Instance ARN	arn:aws:ec2:ap-south-1:914471081680:instance/i-013e6741e6ccfc91f
Private IPv4 addresses	10.0.1.61
Public DNS	-
Elastic IP addresses	-
AWS Compute Optimizer finding	Opt-in to AWS Compute Optimizer for recommendations. Learn more
Auto Scaling Group name	-
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 + ▾
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>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>.\EasyRSA-Start.bat
Starting Easy-RSA shell..
WARNING: openvpn.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
```

```
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

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

Type:yes

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

Using configuration from C:/Users/dell/Downloads/EasyRSA-3.2.4-win32/EasyRSA-3.2.4/pki/246ade19/temp.02
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName :ASN.1 12:'client1.domain.tld'
Certificate is to be certified until Mar 12 13:35:22 2028 GMT (825 days)

Write out database with 1 new entries
Database updated

WARNING
=====
INCOMPLETE Inline file created:
* C:/Users/dell/Downloads/EasyRSA-3.2.4-win32/EasyRSA-3.2.4/pki/inline/private/client1.domain.tld.inline

Notice
-----
Certificate created at:
* C:/Users/dell/Downloads/EasyRSA-3.2.4-win32/EasyRSA-3.2.4/pki/issued/client1.domain.tld.crt

dell@DESKTOP-PENMLV7 C:/Users/dell/Downloads/EasyRSA-3.2.4-win32/EasyRSA-3.2.4
EasyRSA-Shell: # |
```

4.6 Exit the EasyRSA 3 shell.

exit

This creates:

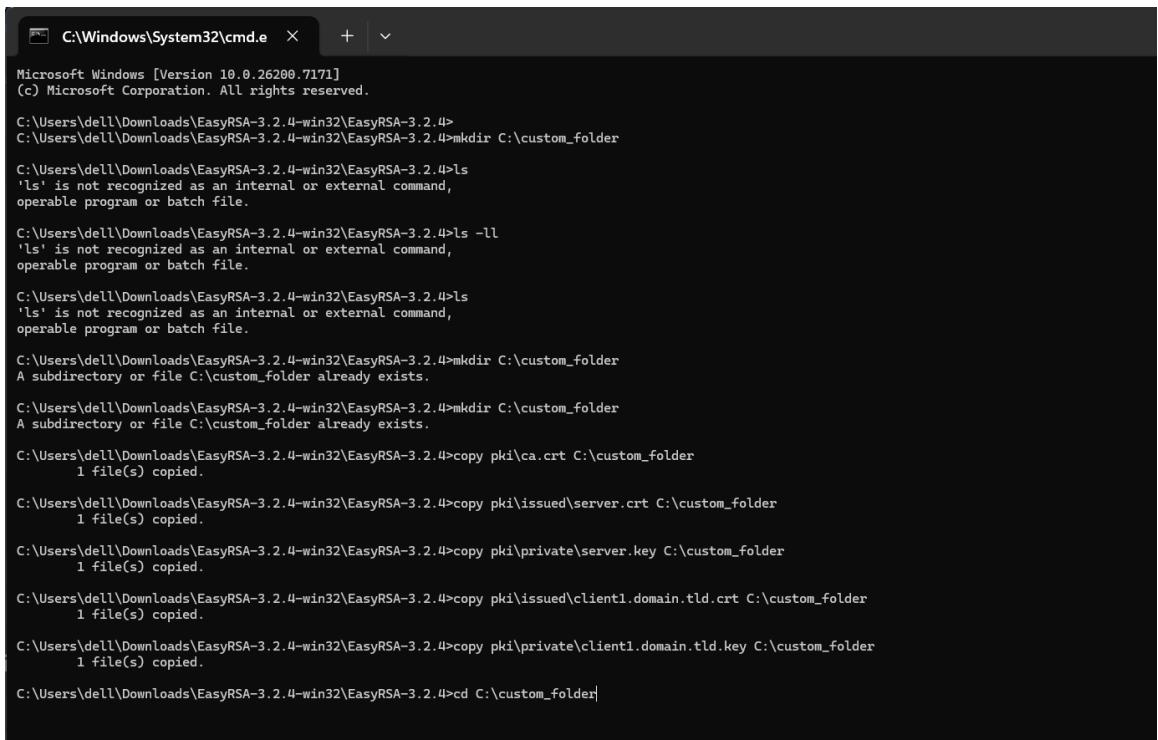
- server.crt

- **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.



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

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

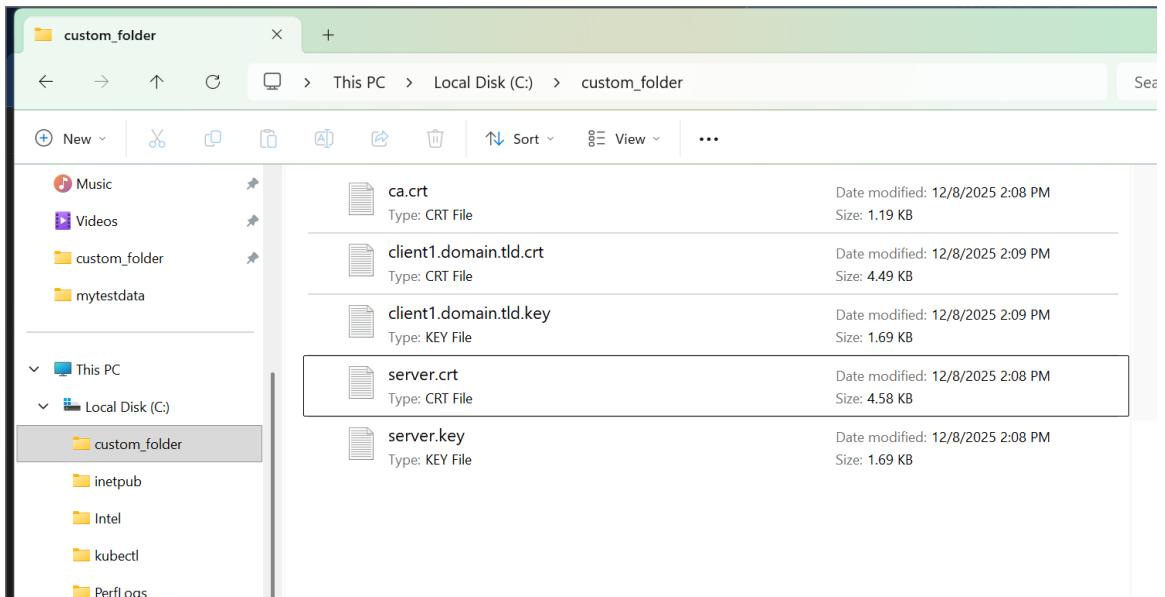
C:\Users\dell\Downloads\EasyRSA-3.2.4-win32\EasyRSA-3.2.4>copy pki\issued\server.crt C:\custom_folder
1 file(s) copied.

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

C:\Users\dell\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\dell\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\dell\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.

A screenshot of the AWS Certificate Manager (ACM) console. The top navigation bar includes links for IAM, VPC, Amazon Simple Email Service, Simple Notification Service, CloudWatch, AWS Application Migration, GuardDuty, AWS Elastic Disaster Recovery, and EC2. The main heading is 'AWS Certificate Manager' with the subtext 'Easily provision, manage, deploy, and renew SSL/TLS certificates'. On the left, a sidebar lists 'AWS Certificate Manager (ACM)' with options for 'List certificates', 'Request certificate', 'Import certificate', and 'AWS Private CA'. A central callout box titled 'New ACM managed certificate' contains three buttons: 'Request a certificate', 'Import a certificate', and 'Create a private CA'. Below this, a 'Pricing' section states 'SSL/TLS certificates provisioned through AWS'. At the bottom, there are links for 'CloudShell', 'Feedback', 'Console Mobile App', and copyright information: '© 2025, Amazon Web Services, Inc. or its affiliates.' and 'Privacy Terms Cookie preferences'.

The screenshot shows the AWS Certificate Manager interface. At the top, there's a navigation bar with links like IAM, VPC, Amazon Simple Email Service, Simple Notification Service, CloudWatch, AWS Application Migration Service, GuardDuty, AWS Elastic Disaster Recovery, and EC2. The main title is 'Import certificate'. Below it, there are three input fields: 'Certificate body', 'Certificate private key', and 'Certificate chain - optional'. Each field has a placeholder text: 'Paste the PEM-encoded certificate body below.', 'Paste the PEM-encoded certificate private key below.', and 'Paste the PEM-encoded certificate chain below.' respectively. There's also a 'Tags' section with a note 'No tags associated with the resource.' and a button 'Add new tag'. At the bottom, there are links for CloudShell, Feedback, and Console Mobile App, along with copyright information: '© 2025, Amazon Web Services, Inc. or its affiliates.' and links for Privacy, Terms, and Cookie preferences.

```
aws acm import-certificate \
--certificate fileb://server.crt \
```

The screenshot shows a terminal window with the following details:

- Tab titles: serve, ca.crt, downloaded, client1.d
- File menu: File, Edit, View
- Toolbar icons: a folder icon, a refresh icon, a save icon, a plus icon, a settings gear icon.

The main content area displays the text of a certificate file:

```
51:a9
    Exponent: 65537 (0x10001)
X509v3 extensions:
    X509v3 Basic Constraints:
        CA:FALSE
    X509v3 Subject Key Identifier:
        89:1:D:D:A:F:1:27:72:F:6:E:4:7:D:7:31:77:95:A:1:A:5:79:2:C:0:2:D1
    X509v3 Authority Key Identifier:
        keyid:D:0:D:D:B:0:5:AE:93:86:F:3:E:4:1:C:79:80:38:C:7:A:1:E:7:6:2:ED:B:6:BD
        DirName:/CN=Easy-RSA CA
        serial:60:D1:73:A:0:A:88:C:2:69:C:3:F:3:26:E:8:2:E:15:7:C:32:CD:9:A: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:
90:55:38:44:70:8:fd:12:56:6:c:00:a4:d2:ac:8d:75:ad:b2:
57:f:2:2d:58:47:d:3:1:e:74:58:30:e:7:05:87:22:b7:bc:59:5b:
cf:e:4:6:d:df:14:ef:6:a:ca:21:f:9:0:a:41:18:92:d:0:73:cc:df:
f:0:2:f:72:0:3:15:6:b:1:c:e:2:9:5:c:65:2:c:45:ff:81:d:2:42:15:
eb:d:7:e:8:d:7:f:5:5:e:54:97:76:c:6:54:20:ef:8:d:09:98:bb:
d:2:48:c:5:de:b:3:e:9:0:f:ee:79:d:8:d:2:d:9:48:70:b:1:b:8:1:d:47:
d:0:6:e:4:9:47:1:c:d:7:6:d:7:9:1:1:c:85:d:8:e:0:a:2:1:a:2:21:
bc:39:62:51:9:a:2:d:66:4:c:b:0:d:30:b:3:76:f:8:42:f:5:07:c:3:
92:d:2:3:d:5:3:b:89:e:9:7:0:3:7:c:61:17:de:76:46:34:46:d:3:
73:46:d:0:60:e:f:80:0:b:65:26:30:2:f:8f:71:b:0:4:7:0:9b:47:
cd:69:57:31:c:a:ad:6:d:8:a:6:f:1:l:c:3:2:b:2d:85:65:3:c:e:7:31:
71:2:e:da:8:b:0:32:b:0:8:e:18:61:80:65:4:b:da:3:c:25:4:a:c:7:
49:f:5:86:67:04:e:3:a:0:c:8:21:f:3:8:a:fc:f:7:d:5:2:9:f:b:5:7:b:
54:23:cd:68:e:2:b:6:4:c:4:g:53:ac:fd:35:2:d:e:4:7:1:b:a:
45:19:5:a:ec
-----BEGIN CERTIFICATE-----
MIIDZzCCAk+gAwIBAgIQBgt3u+NvN3oOYMj19DuXjANBgkqhkiG9w0BAQsFADAW
MRQwEgYDVQDQDAEFTYXN5LVJTSQSBQDQTAefWv0yNTEyIDgwODM4HzzaFw0yODAzMTIw
ODM4NzZmBEbzANBwNBAMBnNlcnz1cJCGASTiwQDYKoZIhvcNAQEBBQxDggEP
ADCCAQoCggFBALaAp4hpJdpHA8U5A3TUEyOlskekFwSmxEck2mNG6ArzvwC2FY
BR6CnR/4K3dAKxsy7iHwH31eGJSHLbm2f6puSwdi3kcUw0zEX9n620KCVCj1h
QQTLCz507ycYVrBe8ap3Yn68zZeG2xvJ5q23/f/02xe892wcn9Nz/0WvjuZs+Z
rYBcdHrYQYyywol830gdT0qkZw/n61yDnNImgN74+9ENCq1Cs+f2uwS1Z34Jn8R
HSVbRyM6YqZigQH6SsQyCAwNFFUm5iAsxzd1Ylvt735XLcqMvYwFvjEXcmUQ
1wa37Cn291Uh0f188ebtgSABC0wUrSuUakCwEAaaObtTCbs:jA8gNVHREmAjAA
MB0G1AUdgQNBBSSd3a8Sdy9uR01zf3laGleSwC0TB8gNWHSMESjBIg8TQ1tsF
rp0G8qeYA4x6HnYu22vaEapBwgFjEUMBiGA1UEAwLRLFzeS1SU0Eg00GCFg3R
c6AK1Mjpw/MmC4VfDLNmnnmMBMGAl1udJQ0IMAoGCCsGAQUFBwIBMAgA1udQwQE
AwF0dARBgVMHREECjAIggzzXJ22X1wQDYKoZIhvcNAQELBQAdggEBAJBV0ERw
jv0SVmwApKksjXWts1fyLvhHo50WDnBYcit7xZw8/kbd8U72rKifkkQRiS0HPM
3/AvcgMw7H0yVx1LEX/gdJCFevX6I33V5U13bGVCDvjoMyu9Jxld6:60:uedj5
2UhwsbgDR9buN1HNd55EchdjgC1Gibw5Y1GaLWZMsA0ws3b4QvUhw5LSPcU7
iEl/A3xhF952RjrG03N60GDvgAt1jAvj3Gw8HCbR81pVzHKrW2KbxHDKy2FZTzn
MXEu2ovQMrC0GGGAZUvaPCVKx0n1hmcE46D1If0/PFvUp+le10jzwjitzkx10s
/TUt5HF+ukUZlw=
-----END CERTIFICATE-----
```

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

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

```
-----BEGIN PRIVATE KEY-----  
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKggSkAgEAAoIBAQC2gKTOIaSXT4QP  
FOQCd01HsjpbJHpBcEpsRHJNpjRugK878AthlAUegp0af+JN3QCsMu4h8B99Xhi  
Uh5QZtvH+qVEsHYt5HFMDsxF/Z+ttCgrwic9YUEy3M+Tu8nGFawXgaqd2J+gc2X  
htsbyUqtif3/9NsXvPdlnJ4CPTc/9Fr47s+fma2AXHR0cuSmMssKC/IjoHU9KpGc  
P5xtcg5zSJ0De+PvRDQqtQrEn9rsOSGd+CZwUR01QWTpumKtmYoEBy+kqKmAgMDR  
RVJkogLMdHY1WJb+9+a1ywqpzFclhb4xFwp1ENcGt+wp7dvdVIdBZfPHm04EgAQt  
MFK701GpAgMBAAECggEAV+9F0wMBdLymA0RMFpoYPN71+jtpwsURvvf94UcfhUzw  
4h7nxNgN42UIwJ900ZKwg/4J7NhQGgDgJ/OsUo41ALbW0ff6h+NF6eFJcMHjIeWn  
42mx0YPeOaqz1QZgegRipKkxagqLBsyS/JtIUKudFV/jaGQ4+secpr0feLG5QNE  
4NBoAJ000v4LEqWP10FxAmwDzZNE9V4iLCJm5u+leBPHGXY5pNTKxDgmVz1nzmGW  
BuAy2Yimg1WqQ02fMoPkj+G6GQ8VhwzMio3AnFh058v9/w09USvNV30kuKamywa7  
tHPEBCmn1JzJ3rBnpsEIRU0Bse7Hr5ykGvT6/Li5ZwKBgQDp3IpDc5L4qxwjPz2Q  
1AevLxfi/KgrAoGJ+yy6KX/GwK9jCPAIGFovY9ZFLJ5yQSA9IqY25jZxZMNOmcL  
Zw90TYfspzyWtJOpIZHmkShQ1Hn1My/AMQ7bm+LDXKhrjND6XI+iZdagypZw4L52  
uvuB8oS5RSawiUreGpOZ0cIaiwKBgQDHx3UCp/t5fj5Xt1Lvu60ADzP5Jy4Zo3SF  
Kyb5CQxisC9FQug4rDkV97xuESi9YnOBA+aRrFC4QMeWSJszosn1CkCs7i3wvOKL  
ZjdeuWxAbnwzg79z5B5b9FK/He4U+CZqaHZch7hbgDJ00acZz3W7Ss7NIUKswobR  
ODdLra4vGwKBgQD6TQaBV10YkdusjGgSw5g8p6zz0WEu6w6/LpQ+/HvZevtg9u  
3wzU4zuzsD8506qgffv2SIqmOuDrMhwPSeBUUC2m1pqbtwZW+0/jJeLhsJd5oPSy  
vtqGcUmgcBAw3hJ/P83cIB61vRc8TUbui0eVa3eeBoxMADtWvolI8M3r0QKBgER7  
Iaf8bx5xY0tuKzXUszJ9g6JXhNzzA+EWLrDVIjk+FCYYzkOG/baDCKtshFu04OsL  
rECpIa5XP1NMpi7oEW76ubrN11/cT4fbTQwiz/IaLafAcaNHQgThVm/+0XrMqVZ2  
YoRLXa233wbXpQEa9U9zUDp0uW1AT7fQnlvJuFibAoGBALI0xnUodFn9kZAW1bvw  
TAd80vf1bJ2m6TOWBuCPwxy7ErSBtJMjZ+Wo+1AISJuC9BNUBe9Z754ivpfUPOKd  
cJDctegrVRYX0/Js/SMq41PNoyuAulva0tfbCBDKQFWTxUvr9DuV/OENqdLdE6Tx  
wxy+KPe38D35fPisowt940K1  
-----END PRIVATE KEY-----  
|
```

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

```
-----BEGIN CERTIFICATE-----  
MIIDSzCCAjOgAwIBAgIUbFdFzoAqIwmnD8yoLhV8Ms2aaecwDQYJKoZIhvcaNAQEL  
BQAwFjEUMBIGA1UEAwvLRWFzeS1SU0EgQ0EwHhcNMjUxMjA4MDgzODEzWhcNMzUx  
MjA2MDgzODEzLkjAWMRQwEgYDVQDDAtFYXN5LVJTQSBQTCASIwDQYJKoZIhvCN  
AQEBBQADggEPADCCAQcggEBAL4uLPZCVjj1Sny/pIkqQVKjNWEl8psPHRhdUNj  
FVEhqGPX7BT13AX9FagANm/2p6tD0ynasenwIeL0xb+2R+m1fs2B1Eue8OMI2uI  
moWopoZ9KdfBGsXoNDeqZFdqRhT15B1pGsmR70hy9ZCbtneK50sM7wrgIoatyf7  
syL15QNQwDYL16kLaV+vMEf5cUNCrXrC3r5EGQ4Ka8EnPsBZ3+n4liQAU0FVICu7  
C1ziBBTn7Tz143nsmdNpoT7Feo4kN8uZ7hb8+of2wk8J5ereD/asxMs+od7+Qy5  
U9hnEj9FM7T8vJ7tFpGu2yiWm3w8CYKy418sm1mQ1EczsCAwEAa0BkDCBjTAM  
BgNVHRMEBTADAQH/MB0GA1UdDgQVBHQ1tsFrp0G8+QceYA4x6HnYu22vaEapBgvFjEUMBIGA1UEAwvLRWFz  
eS1SU0EgQ0GCFG3Rc6AK1Mjpw/Mm6C4VfdLNmmmnMasGA1UdDwQEAwIBBjANBqk  
hkiG9w0BAQsFAAOCAQEASsH016m0t8td56wEBtQwQHMy0/xdChlDBm9fK36Hz  
B01CnZ4CQnarfdokt7g2HwHsyzImHzjhTF4bk6o89eOY7/xzE0+F7wDhmPwzqT0  
e91XNIUn/rZnHaJi4FBUpTAKwsI4ybEe0Q2RFCzkoXiNNwhQ0u6AZIE819kqtKX  
4IOl3sxQH4CU9V111gr7r8m7A3qrP/u6ZuGL6ziumetGb5gz1Kcd1gDJKxAj5SyL  
4ftmQXkuuNBYE5neYdcrRA7P6uQeTJ1Dq3EfgAfAnWFF9v579I0RGu/y3k1VD/Am  
NkunFXzP312mTMucD6N9LC8rJC114ryRdbI4qqvALQ==  
-----END CERTIFICATE-----
```

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

The screenshot shows the AWS Certificate Manager (ACM) interface. On the left, there's a sidebar with options like 'List certificates', 'Request certificate', 'Import certificate', and 'AWS Private CA'. The main area is titled 'Certificates (2)' and lists two entries:

Certificate ID	Domain name	Type	Status	In use	Renewal eligibility	Key algorithm
517a5cfe-b107-417a-8b45-d935b7c930f	client1.domain.tld	Imported	Issued	Yes	Ineligible	RSA 2048
490192ae-445a-4c38-8239-7e655be72b82	server	Imported	Issued	Yes	Ineligible	RSA 2048

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

The screenshot shows the 'Create client VPN endpoint' configuration page. It has several sections:

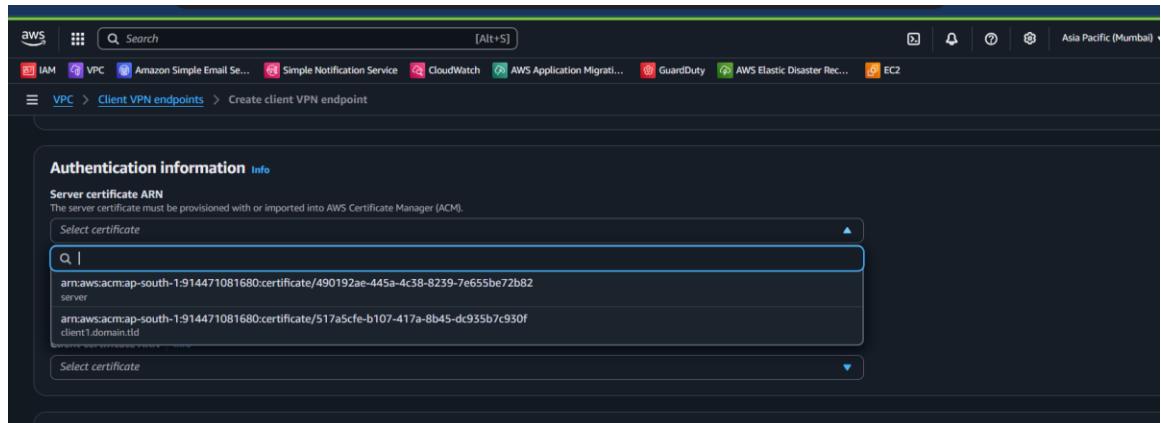
- Details**:
 - Name tag - optional**: A field containing 'Client-VPN DEMO'.
 - Description - optional**: A field containing 'a demo to set up C-VPN to access the private server'.
- Endpoint IP address type**: A section where 'IPv4' is selected.
- Traffic IP address type**: A section where 'IPv4' is selected.

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

The screenshot shows a modal or input field for 'Client IPv4 CIDR'. It contains the following text:
Client IPv4 CIDR [Info](#)
The IP address range, in CIDR notation, from which client IP addresses are allocated when the traffic type is IPv4.
CIDR block cannot be larger than /12 or smaller than /22.
Input field: 172.0.0.0/16

5.3 Server Certificate ARN

Select server certificate from ACM.



Authentication information Info

Server certificate ARN

The server certificate must be provisioned with or imported into AWS Certificate Manager (ACM).

Select certificate

arnaws:acm:ap-south-1:914471081680:certificate/490192ae-445a-4c38-8239-7e655be72b82
server

arnaws:acm:ap-south-1:914471081680:certificate/517a5cf-b107-417a-8b45-dc935b7c930f
client1.domain.tld

Select certificate

Paste ACM ARN.

5.4 Authentication

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



Authentication options

Choose one or a combination of authentication methods to use.

Use mutual authentication

Use user-based authentication

Client certificate ARN Info

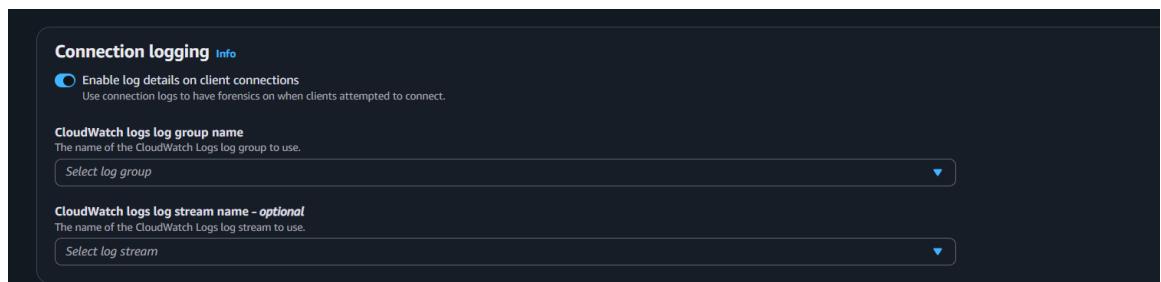
arnaws:acm:ap-south-1:914471081680:certificate/517a5cf-b107-417a-8b45-dc935b7c930f

arnaws:acm:ap-south-1:914471081680:certificate/490192ae-445a-4c38-8239-7e655be72b82
server

arnaws:acm:ap-south-1:914471081680:certificate/517a5cf-b107-417a-8b45-dc935b7c930f
client1.domain.tld

5.5 Connection Logging

Optional.



Connection logging Info

Enable log details on client connections

Use connection logs to have forensics on when clients attempted to connect.

CloudWatch logs log group name

The name of the CloudWatch Logs log group to use.

Select log group

CloudWatch logs log stream name - optional

The name of the CloudWatch Logs log stream to use.

Select log stream

5.6 DNS Servers

Use:

8.8.8.8

Click Create Client VPN Endpoint.

The screenshot shows the 'Create client VPN endpoint' page in the AWS VPC console. Under the 'DNS configuration - optional' section, there are four input fields for DNS server IP addresses: 'DNS server 1 IP address' (192.168.0.2), 'DNS server 2 IP address' (169.254.169.253), 'DNS server 3 IP address' (2a05:d018:ff4:7100:2), and 'DNS server 4 IP address' (fd00:ec2::253). Below this, the 'Other parameters - optional' section includes a 'Transport protocol' dropdown set to 'UDP' (selected with a blue radio button) and an 'Enable client connect handler' checkbox which is unchecked.

5.6 Others Parameters—Opti0nal

5.7 Now choose your VPC.

The screenshot shows the 'Create client VPN endpoint' page in the AWS VPC console. Under the 'VPC ID' section, a dropdown menu lists several VPC IDs: 'vpc-04712a543e110bbf3 (new-vpc)' (selected with a blue background), 'vpc-04712a543e72526ce031', 'vpc-049253a72526ce031', 'vpc-0558fb6920357458 (My-VPC)', and 'vpc-033a8e41dee6b366e (project-vpc)'. At the bottom of the page, there is an 'Enable self-service portal' checkbox which is unchecked.

Account ID: 9144-7108-1680 panika2294

VPC > Client VPN endpoints > Create client VPN endpoint

443

Enable self-service portal Info

Session timeout hours Info

Disconnect on session timeout Info

Enable client login banner Info

Client route enforcement Info

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key Value - optional

Add new tag

You can add 49 more tags.

Create client VPN endpoint

Now click on – Create Client VPN Endpoint.

After a while it will show you in Active state.

ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#ClientVPNEndpoints

VPC > Client VPN endpoints

Client VPN endpoints (1 / 1) info

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

cvpn-endpoint-008dcf3663dd497de / new-vpn endpoint

Details	Target network associations	Security groups	Authorization rules	Route table	Connections	Tags
Details Client VPN endpoint ID: cvpn-endpoint-008dcf3663dd497de Description: C-vpn demo to access the private server Creation time: Split-tunnel	VPN port: 443 Transport protocol: udp	DNS name: *.cvpn-endpoint-008dcf3663dd497de.prod.clientvpn.ap-south-1.amazonaws.com DNS servers: -	Self-service portal URL: - Client login banner text: - Client connect handler 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)

Associate target network

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

Association ID	State	Network ID	Security groups	Endpoint ID
cvpn-assoc-0b925278195eb9...	Associated	subnet-0029c419e32d044de	sg-05894f5395820f7b	cvpn-endpoint-008dcf3663d...

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 > vpn-endpoint-008dcf3663dd497de > Add authorization rule

Add authorization rule Info

Add authorization rules to grant clients access to the networks.

Details

Client VPN endpoint ID
vpn-endpoint-008dcf3663dd497de

Destination network to enable access
The IP address, in CIDR notation, of the destination network.
Q 10.0.0.0/24

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.
description

[Cancel](#) [Add authorization rule](#)

Target network associations	Security groups	Authorization rules	Route table	Connections	Tags
Authorization rules (1) <small>Info</small>					
 Remove authorization rule Add authorization rule					
 Find authorization rule by attribute or tag					
<input type="radio"/> vpn-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 > vpn-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
vpn-endpoint-008dcf3663dd497de

Route destination
CIDR range for the destination network.
Q 0.0.0.0/0

Subnet ID for target network association
'local' indicates the client VPN endpoint network.
subnet-0029c419e32d044de

Description - optional
Description of the route.
description

[Cancel](#) [Create route](#)

Target network associations	Security groups	Authorization rules	Route table	Connections	Tags
Route table (1) Info					

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

Client VPN endpoints (1/1) Info				Actions ▾	Client downloads ▾	Download client configuration	Create client VPN endpoint
Find client VPN by attribute or tag							
Name	Client VPN endpoint ID	State	Client CIDR				

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 X +

File Edit View

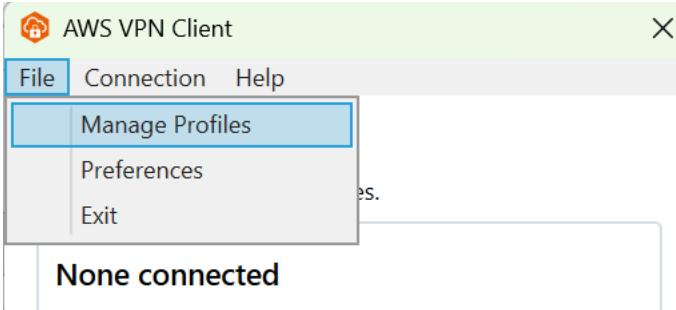
```
-----key-----  
Digital Signature  
Signature Algorithm: sha256WithRSAEncryption  
Signature Value:  
36:ba:f7:01:1b:5f:59:da:29:4c:91:ba:f5:4c:73:8b:6b:7c:  
51:e5:e0:42:3c:2e:83:da:40:d6:13:ab:b5:96:66:e4:4e:2a:  
d3:81:bd:66:5f:fb:5e:57:16:a0:2e:03:3f:e8:64:5e:dc:52:  
ea:a7:02:f6:28:92:09:b1:98:bc:45:3f:9f:e5:b7:65:e4:92:  
b5:4f:27:6a:97:8d:5e:d0:a0:dc:18:9e:5c:ba:ff:98:2f:8d:  
1a:28:a9:61:e6:de:52:41:6c:3f:92:d1:22:18:1c:3d:cd:92:  
71:d3:0e:0b:5e:38:8b:b8:f8:60:30:fb:b6:0e:3c:46:ad:f5:  
f2:6a:a1:13:17:76:94:fe:6d:7f:01:63:b0:9b:67:60:91:f1:  
68:3c:af:ef:df:31:c2:5f:16:d6:9e:cf:83:9a:f6:91:40:e1:  
52:ba:3f:ef:51:4d:cd:bc:20:14:2b:4a:e9:38:36:38:50:e0:  
30:d9:20:c4:89:10:95:dd:8a:0f:04:44:e8:2a:b0:cd:c4:2e:  
8c:22:86:3e:72:99:63:0b:94:5b:6c:5e:8d:99:8d:91:a8:62:  
c0:e8:cf:c6:31:29:a4:2f:37:ba:29:37:54:b2:3a:af:a5:31:  
31:8f:32:3c:3c:22:60:ae:39:7b:0d:a9:39:e1:84:55:b8:fb:  
03:96:b0:53  
-----BEGIN CERTIFICATE-----  
MIIDYTCACKmgAwIBAgIRAIc+U7g/xCTqttY939YsMggwDQYJKoZIhvNAQELBQA  
wFjEUMBTGA1UEAwuLRWfzeS1SU0Ego0EwHhcNMjUxMjA4MDgzOTEzhcNMjgwMzEy  
MdgzOTEzwjAdMRswGQYDVQODDBJjbG1lnbnQxLmRvbWFpbis0bGQwggEiMA0GCSqG  
S1b3DQEBAQUAA4IBDwAwggEKAoIBAQDcRLFBQsNETtvrMB7G6tH0JkHebT532F7  
tJDP26KT5k7okvNNX1fDSVMzbZ1g4nXg+915HgDEUCZe004UI48AOCB71lMshp  
+gtwRk04PNCFdAA2fDDQi/YFVN+mS98QQcs814b0btNxD79abDXvxFYxFAG96/A9  
WqMASxug4tC8MFZpvaeax4s1QlIH+0LA1JnNgfHzm7tCZA00+NsfASJzoY66Dwqs  
mYx/+4L93yo7RTocNy30raUh2/z8EwdDVK3LuMQmsaf3BHTVuuc+eEc6fUTTl4N  
FOJFk8QMLCK0rvzzkL19rwQak/zHHk2Ak1zYysuFwto4I3m/w+1TAG#BAAgjgaIw  
gZ8wCQYDVROTBAlwADBgNVHQ4EFgQUBy1/gYuin5L4kh1crO7FqeaxbQswuQYD  
VR0JBewwSIAU0NbBbaGThPkHhmAoMeh52Ltr2hGqQMYBxFDASBgNVBAMC0Vh  
c3ktu1NBIEBghRt0X0gCojCacPzJuguFxwy:Zpp5zATBgNVHSUEDDAKBgrBgfEF  
BQcDAjALBgNVHQ8EBAMCB4AwDQYJKoZIhvNAQELBQADggEBAdaa69wEbX1naKUyR  
uvV7c4trfFH14ET8loPaQNYTq7WwZuR0KtOBwZf715XfqAuAz/oF7cUlupnAvYo  
kgmxmLxFP5/ltxXkrVPj2qXjV7QoNwNny6/5gvjRooqlHm3lJ8BD+S05IYHD3N  
knHTDgte0tu4+Gw+7Y0PEat9fJqoRMXdpT+b8BY7cbZ2CR8lg8r+/fMcJfftae  
z40a9pFAH1K6P+9RTc28IBQRsuk4NjhQ4DDZIMSJEJXdig8ER0gqsM3ElLowihj5y  
mlwML1FtsXo2ZjZGoYsDoz8YXkaQvN7opN1syQ+1MT6PMjw8ImCuOXsNqTnhhFW4  
+wOWsFm=  
-----END CERTIFICATE-----  
</cert>  
  
<key>  
-----BEGIN PRIVATE KEY-----  
MIIEvQTBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDcRLfB8QsNETtV  
rMB7G6tH0JkHebT532F7tJDP26KT5k7oKvNMk1JfDSVMzbZ1g4nXg+915HgDEUC  
Ze004UI48AOCB71lMshp+gtwRk04PNCFdAA2fDQ1/YFVN+mS98QQcs814b0btNx  
D79abDXv0XYxFAG96/A9MqMASxug4tC8MFZpvaeax4s1QlIH+0LA1JnNgfHzm7tCZ  
A00+NsfASJzoY66DwqsnnmYx/+4L93yo7RTocNy30raUh2/z8EwdDVK3LuMQmsaf3  
BHTVuuc+eEc6fUTTl4NF0Fk8QMLCK0rvzzkL19rwQak/zHHk2Ak1zYysuFwto4  
I3m/w+1TAG#BAAgjgaIw85b5JAdNPqS1hgASUlev0jW09dzgsu7L  
yVkbakVJzfL+eVlmqeojUbj6++axJ4doemDt05axgMiGRkswHGZ4EFVVUmKiVY  
g8+4jrQiv1Zpm6IdoM15jF0Clwe1uZ77aeeeARBBp+XC12Lf3/jxY0KCW/uZ3  
fjIpZtsncg6Z2JW0Vs0a9p91vn10BhlwUjgnnbIuF5Db6IWAmkcE3LOCdREuEyBhq  
zQ1bSJwq0IiDGuV3E9hFJcrIEqEFt81MhdmoVthWA5pcsnKK/jwZtVyaNTSQx  
-----END PRIVATE KEY-----  
Ln 38, Col 25 | 7,723 characters | Plain text
```

Save.

Insert client certificate and key inside the .ovpn file.

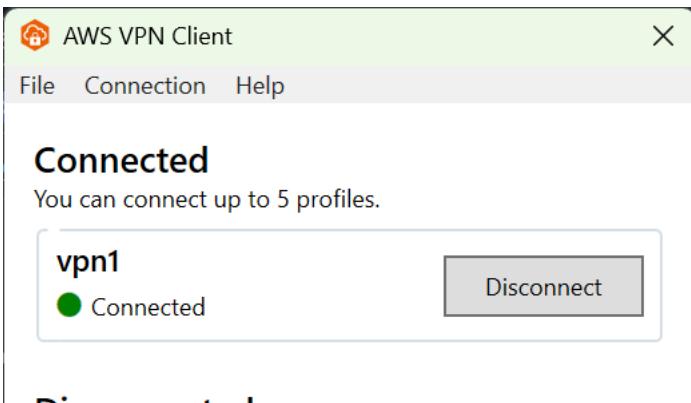
11. Connect Using AWS VPN Client

Open AWS VPN Client → Import configuration → Connect.



Disconnected

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.

The screenshot shows the AWS EC2 Instances details page for an instance named i-013e6741e6ccfc91f. The instance is currently running. Key details include its Public IPv4 address (10.0.1.61), Private IP DNS name (ip-10-0-1-61.ap-south-1.compute.internal), and VPC ID (vpc-04712a543e110bbf3). The instance is associated with a subnet (subnet-0029c419e32d044de) and an IAM Role. The instance type is t3.micro, and it is part of a new-vpc network. The instance has an Auto-assigned IP address and is connected to a VPC interface (eni-013e6741e6ccfc91f). The instance summary also lists its Private IPv4 address (10.0.1.61), Public DNS (ip-10-0-1-61.ap-south-1.compute.internal), and its association with an Auto Scaling Group.

```
ec2-user@ip-10-0-1-61:~  
login as: ec2-user  
Authenticating with public key "vpn_key"  
' #  
~\ _ #####_ Amazon Linux 2023  
~~ \#####\ |  
~~ \###|  
~~ \#/ https://aws.amazon.com/linux/amazon-linux-2023  
~~ V~' .-'>  
~~ /  
~~ ._. /  
~/m/' /  
Last login: Mon Dec 8 10:50:52 2025 from 10.0.1.78  
[ec2-user@ip-10-0-1-61 ~]$ ls  
[ec2-user@ip-10-0-1-61 ~]$ ls -ll  
total 0  
[ec2-user@ip-10-0-1-61 ~]$ pwd  
/home/ec2-user  
[ec2-user@ip-10-0-1-61 ~]$  
[ec2-user@ip-10-0-1-61 ~]$
```

If it connects — VPN is working.

cvpn-endpoint-008dcf3663dd497de / new-vpn endpoint

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

Connections (1) [Info](#)

Find connection by attribute or tag

Client VPN endpoint ID	Timestamp	Connection ID	Username	Connection established time
cvpn-endpoint-008dcf3663dd497de	December 08, 2025, 19:37 (UT...)	cvpn-connection-0dc886a778d7914fa	-	December 08, 2025, 19:34 (UTC)

Terminate connection

< 1 > ⚙

Mobile App © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

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.
