**To generate the server and client certificates and keys and upload them to ACM**

1. Clone the OpenVPN easy-rsa repo to your local computer.

$ git clone https://github.com/OpenVPN/easy-rsa.git

1. Navigate into the easy-rsa/easyrsa3 folder in your local repo.

$ cd easy-rsa/easyrsa3

1. Initialize a new PKI environment.

$ ./easyrsa init-pki

1. Build a new certificate authority (CA).

$ ./easyrsa build-ca nopass

Follow the prompts to build the CA.

1. Generate the server certificate and key.

$ ./easyrsa build-server-full server nopass

1. Generate the client certificate and key.

Make sure to save the client certificate and the client private key because you will need them when you configure the client.

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

You can optionally repeat this step for each client (end user) that requires a client certificate and key.

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

$ mkdir ~/*custom\_folder*/

$ cp pki/ca.crt ~/*custom\_folder*/

$ cp pki/issued/server.crt ~/*custom\_folder*/

$ cp pki/private/server.key ~/*custom\_folder*/

$ cp pki/issued/client1.domain.tld.crt ~/*custom\_folder*

$ cp pki/private/client1.domain.tld.key ~/*custom\_folder*/

$ cd ~/*custom\_folder*/

1. Upload the server certificate and key to ACM.

$ aws acm import-certificate --certificate file://server.crt --private-key file://server.key --certificate-chain file://ca.crt --region *region*

**Note**

Be sure to upload the certificate and key in the same Region in which you intend to create the Client VPN endpoint.

1. Upload the client certificate and key to ACM.

$ aws acm import-certificate --certificate file://client1.domain.tld.crt --private-key file://client1.domain.tld.key --certificate-chain file://ca.crt --region *region*

**Note**

Be sure to upload the certificate and key in the same Region in which you intend to create the Client VPN endpoint.

Authorization

Client VPN supports two types of authorization: security groups and network-based authorization (using authorization rules).