

OpenVPN Setup & Certificates

1. Install Easy-RSA

The first step in building an OpenVPN configuration is to establish a PKI (public key infrastructure). The PKI consists of:

- a separate certificate (also known as a public key) and private key for the server and each client, and
- a master Certificate Authority (CA) certificate and key which is used to sign each of the server and client certificates.

Install easy-rsa package on your Debian system with the following command:

```
# apt install easy-rsa
```

Create a directory where whole key structure will be stored:

```
# make-cadir /tmp/certs
# cd /tmp/certs
```

Edit the vars file to configure Certificate Authority (CA) variables:

```
#nano ./vars
-----
Uncomment:

set_var EASYRSA_KEY_SIZE          2048
set_var EASYRSA_REQ_COUNTRY       "NL"
set_var EASYRSA_REQ_PROVINCE      "Zuid-Holland"
set_var EASYRSA_REQ_CITY          "Rijnsburg"
set_var EASYRSA_REQ_ORG           "Oscar.de.Groot"
set_var EASYRSA_REQ_EMAIL         "oscar@oscardegroot.nl"
set_var EASYRSA_REQ_OU            "MySites"
```

Generate the required certificates and keys:

```
$ easyrsa init-pki
```

2. Create own CA certificate

```
$ easyrsa build-ca
```

3. Create Server Certificate & Key

Throughout this tutorial, the OpenVPN server's common name will be "MyServerName". Be sure to include the `nopass` option as well. Failing to do so will password-protect the request file, which could lead to permissions issues later on.

```
$ easyrsa gen-req MyServerName nopass
```

This will create a private key for the server and a certificate request file called `server.req`. Then sign the request by running `easyrsa` with the `sign-req` option, followed by the request type and the common name. The request type can either be client or server, so for the OpenVPN server's certificate request, be sure to use the server request type.

```
$ easyrsa sign-req server MyServerName
```

In the output, you'll be asked to verify that the request comes from a trusted source. Type `yes` and press `ENTER` to confirm this.

Generating Diffie-Hellman (DH) params

The Diffie-Hellman (DH) Algorithm is a key-exchange protocol that enables two parties communicating over public channel to establish a mutual secret without it being transmitted over the Internet. DH enables the two to use a public key to encrypt and decrypt their conversation or data using symmetric cryptography. After initializing a PKI, any entity can create DH params that needs them. DH key params can be generated with:

```
$ ./easyrsa gen-dh
```

This may take a few minutes to complete. Once it does, generate an HMAC signature to strengthen the server's TLS integrity verification capabilities:

```
$ openvpn --genkey --secret pki/ta.key
```

When the command finishes, copy the two new files to your `/etc/openvpn/` directory:

```
sudo cp ~/easy-rsa/ta.key /etc/openvpn/
sudo cp ~/easy-rsa/pki/dh.pem /etc/openvpn/
```

With that, all the certificate and key files needed by your server have been generated. You're ready to create the corresponding certificates and keys that your client machine will use to access your OpenVPN server.

Key Files

Now we will find our newly-generated keys and certificates in the `keys` subdirectory. Here is an

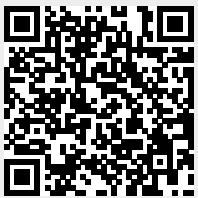
explanation of the relevant files:

| Filename | Needed By | Purpose |
|--------------------|--------------------------|---------------------------|
| ca.crt | server + all clients | Root CA certificate |
| ca.key | key signing machine only | Root CA key |
| dh{ <i>n</i> }.pem | server only | Diffie Hellman parameters |
| server.crt | server only | Server Certificate |
| server.key | server only | Server Key |
| client1.crt | client1 only | Client1 Certificate |
| client1.key | client1 only | Client1 Key |

Links

- https://wiki.debian.org/OpenVPN#OpenVPN_Overview
- <https://www.webhi.com/how-to/how-to-install-openvpn-server-on-linux-debian-11-12/>
- <https://www.digitalocean.com/community/tutorials/how-to-set-up-an-openvpn-server-on-debian-11>

From:
<https://wiki.oscardegroot.nl/> - **HomeWiki**



Permanent link:

<https://wiki.oscardegroot.nl/doku.php?id=networking:openvpn&rev=1723655213>

Last update: **2024/08/14 17:06**