CentOS-7 安装 OpenVPN

安装环境：CentOS-7.3 以上

安装

```
yum -y update
yum -y install epel-release
yum -y install openvpn easy-rsa

cp -r /usr/share/easy-rsa/ /etc/openvpn/easy-rsa
cd /etc/openvpn/easy-rsa/
\rm 3 3.0
cd 3.0.3/
find / -type f -name "vars.example" | xargs -i cp {} . && mv vars.example vars
```

生成 CA 证书

创建一个新的 PKI 和 CA

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

```
[root@pdh 3.0.3]# ./easyrsa init-pki

Note: using Easy-RSA configuration from: ./vars

init-pki complete; you may now create a CA or requests.
Your newly created PKI dir is: /etc/openvpn/easy-rsa/3.0.3/pki
```

创建新的 CA，不使用密码

```
./easyrsa build-ca nopass
```

```
[root@pdh 3.0.3]# ./easyrsa build-ca nopass

Note: using Easy-RSA configuration from: ./vars
Generating a 2048 bit RSA private key
.....................................................................................
.....................................................................................
.......................+++
.....................................................................................
.....................................................................................
.........................+++
writing new private key to '/etc/openvpn/easy-rsa/3.0.3/pki/private/ca.key.LH0B47lmgF'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [Easy-RSA CA]:
```

回车

```
Common Name (eg: your user, host, or server name) [Easy-RSA CA]:

CA creation complete and you may now import and sign cert requests.
Your new CA certificate file for publishing is at:
/etc/openvpn/easy-rsa/3.0.3/pki/ca.crt
```

创建服务端证书

```
./easyrsa gen-req server nopass
```

```
[root@pdh 3.0.3]# ./easyrsa gen-req server nopass

Note: using Easy-RSA configuration from: ./vars
Generating a 2048 bit RSA private key
..........+++
.........................................+++
writing new private key to '/etc/openvpn/easy-rsa/3.0.3/pki/private/server.key.rDLvTS5
Rsm'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [server]:
```

回车

```
Common Name (eg: your user, host, or server name) [server]:

Keypair and certificate request completed. Your files are:
req: /etc/openvpn/easy-rsa/3.0.3/pki/reqs/server.req
key: /etc/openvpn/easy-rsa/3.0.3/pki/private/server.key
```

签约服务端证书

```
./easyrsa sign server server
```

```
[root@pdh 3.0.3]# ./easyrsa sign server server

Note: using Easy-RSA configuration from: ./vars


You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.

Request subject, to be signed as a server certificate for 3650 days:

subject=
    commonName                = server


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

yes

创建 Diffie-Hellman

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

```
[root@pdh 3.0.3]# ./easyrsa gen-dh

Note: using Easy-RSA configuration from: ./vars
Generating DH parameters, 2048 bit long safe prime, generator 2
This is going to take a long time
.........................+.....................................................
.....................................................................................
...........+.........................................................................
.....................................................................................
.................................+...................................................
.....................................................................+...........
..+..................................................................++*++
*

DH parameters of size 2048 created at /etc/openvpn/easy-rsa/3.0.3/pki/dh.pem
```

整理证书

```
cd /etc/openvpn
cp easy-rsa/3.0.3/pki/dh.pem .
cp easy-rsa/3.0.3/pki/ca.crt .
cp easy-rsa/3.0.3/pki/issued/server.crt .
cp easy-rsa/3.0.3/pki/private/server.key .
```

创建客户端证书

```
cp -r /usr/share/easy-rsa/ /etc/openvpn/client
cd /etc/openvpn/client/easy-rsa/
\rm 3 3.0
cd 3.0.3/
find / -type f -name "vars.example" | xargs -i cp {} . && mv vars.example vars
```

创建新的 pki

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

```
[root@pdh 3.0.3]# ./easyrsa init-pki

Note: using Easy-RSA configuration from: ./vars

init-pki complete; you may now create a CA or requests.
Your newly created PKI dir is: /etc/openvpn/client/easy-rsa/3.0.3/pki
```

这步骤可以创建多个使用不同名字，每个客户端使用一个（如：`./easyrsa gen-req client2 nopass`）

```
./easyrsa gen-req client nopass
```

```
[root@pdh 3.0.3]# ./easyrsa gen-req client nopass

Note: using Easy-RSA configuration from: ./vars
Generating a 2048 bit RSA private key
.............+++
.......................+++
writing new private key to '/etc/openvpn/client/easy-rsa/3.0.3/pki/private/client.key.
qu34KSNQye'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [client]:
```

回车

```
Common Name (eg: your user, host, or server name) [client]:

Keypair and certificate request completed. Your files are:
req: /etc/openvpn/client/easy-rsa/3.0.3/pki/reqs/client.req
key: /etc/openvpn/client/easy-rsa/3.0.3/pki/private/client.key
```

签约客户端证书，如有多个请签约多个

```
cd /etc/openvpn/easy-rsa/3.0.3/
./easyrsa import-req /etc/openvpn/client/easy-rsa/3.0.3/pki/reqs/client.req client
```

```
[root@pdh 3.0.3]# ./easyrsa import-req /etc/openvpn/client/easy-rsa/3.0.3/pki/reqs/cli
ent.req client

Note: using Easy-RSA configuration from: ./vars

The request has been successfully imported with a short name of: client
You may now use this name to perform signing operations on this request.
```

```
./easyrsa sign client client
```

```
[root@pdh 3.0.3]# ./easyrsa sign client client

Note: using Easy-RSA configuration from: ./vars


You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.

Request subject, to be signed as a client certificate for 3650 days:

subject=
    commonName                = client


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

yes

整理证书

```
cd /etc/openvpn/client
cp /etc/openvpn/easy-rsa/3.0.3/pki/ca.crt .
```

```
cp /etc/openvpn/easy-rsa/3.0.3/pki/issued/client.crt .
cp /etc/openvpn/client/easy-rsa/3.0.3/pki/private/client.key .
```

配置文件

创建服务器配置文件

```
vi /etc/openvpn/server.conf
```

内容可以参考如下：

```
port 1194
proto tcp
dev tun

ca /etc/openvpn/ca.crt
cert /etc/openvpn/server.crt
key /etc/openvpn/server.key
dh /etc/openvpn/dh.pem

ifconfig-pool-persist /etc/openvpn/ipp.txt

server 10.8.0.0 255.255.255.0
push "route 10.8.0.0 255.255.255.0"
push "redirect-gateway def1 bypass-dhcp"
push "dhcp-option DNS 114.114.114.114"
push "dhcp-option DNS 8.8.8.8"
client-to-client
duplicate-cn # 同一个 vpn 账号允许同时多点登陆

keepalive 20 120
comp-lzo

user openvpn
group openvpn

persist-key
persist-tun
status   openvpn-status.log
log-append  openvpn.log
verb 1
mute 20
```

创建客户端配置文件

```
vi /etc/openvpn/client/client.ovpn
```

内容可以参考如下：

```
client
remote xx.xxx.xx.xx 1194
proto tcp
dev tun
comp-lzo
ca ca.crt
cert client.crt
key client.key
route-delay 2
route-method exe
redirect-gateway def1
dhcp-option DNS 8.8.8.8
dhcp-option DNS 8.8.4.4
dhcp-option DNS 4.2.2.1
dhcp-option DNS 4.2.2.2
verb 3
```

（注意：`remote xx.xxx.xx.xx 1194` 为服务端访问 IP 和端口）

启动 OpenVPN 和 iptables 策略

启动 OpenVPN

```
systemctl start openvpn@server
```

添加 iptables 策略

```
iptables -t nat -A INPUT -p udp -m state --state NEW -m udp --dport 1194 -j ACCEPT
iptables -t nat -A INPUT -p tcp -m state --state NEW -m tcp --dport 1194 -j ACCEPT
iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -j MASQUERADE
```

保存规则

```
service iptables save
```

开启转发

```
vi /etc/sysctl.conf
```

修改下面一行参数为：

```
net.ipv4.ip_forward = 1
```

（如果没有，则添加进去）

查看一下系统参数

```
sysctl -p
```

配置开机启动

```
chmod u+x /etc/rc.d/rc.local
vi /etc/rc.d/rc.local
```

添加如下内容：

```
## OpenVPN
systemctl restart openvpn@server
systemctl restart iptables.service
iptables -F
iptables -t nat -A POSTROUTING -s 10.8.0.0/24  -j MASQUERADE
sysctl -p
```

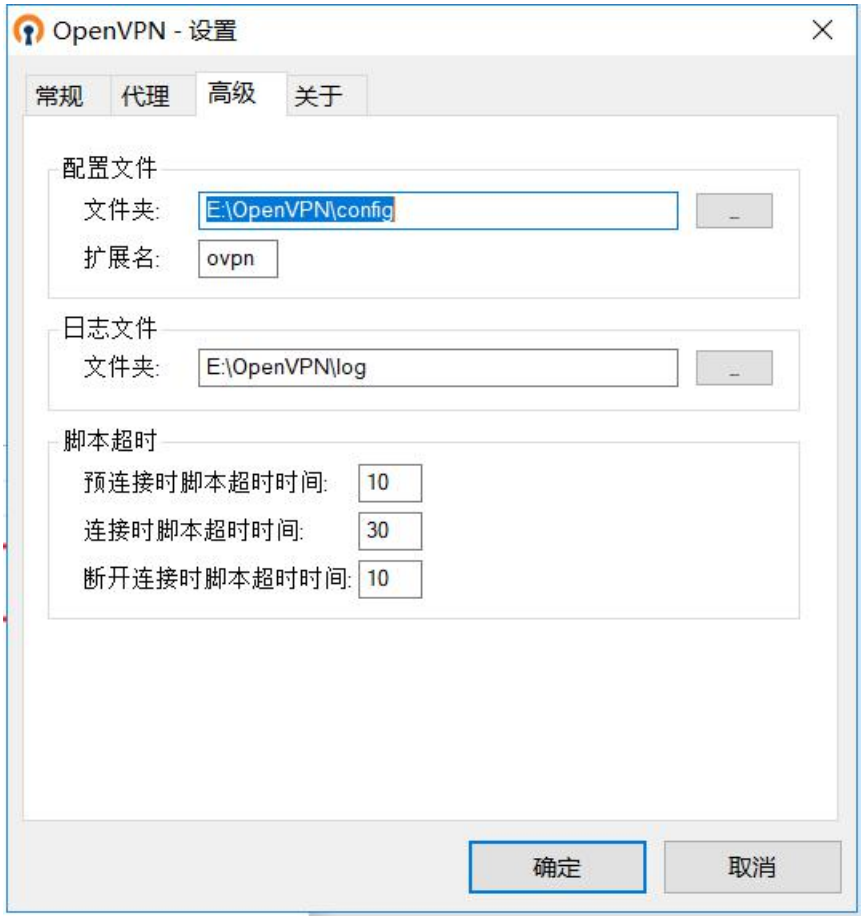
查看一下端口

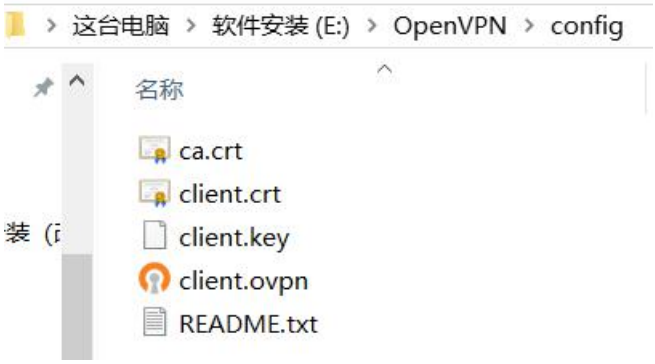
```
netstat -tunl | grep 1194
```

```
[root@pdh client]# netstat -tunl | grep 1194
udp        0      0 0.0.0.0:1194            0.0.0.0:*
```

用客户端连接一下

将创建的客户端配置文件和证书放入对应位置（右下角图标，右键选项配置位置）





然后右键右下角图标，连接。或者双击启动。绿色状态表示已连接。