##### CentOS-7安装OpenVPN

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

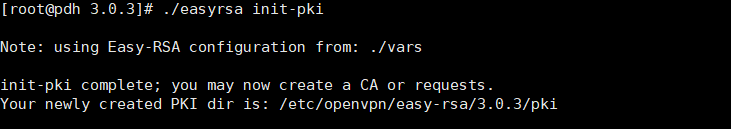
cd 3.0.3/

find / -type f -name "vars.example" | xargs -i cp {} . && mv vars.example vars

**生成CA证书**

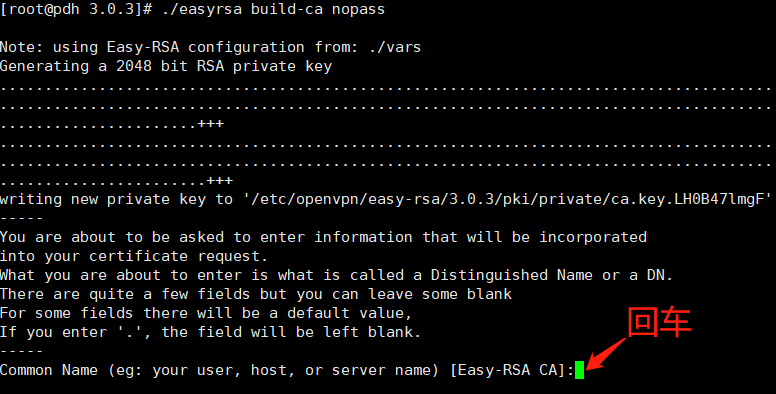
创建一个新的 PKI 和 CA

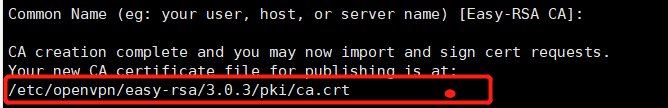
./easyrsa init-pki



创建新的CA，不使用密码

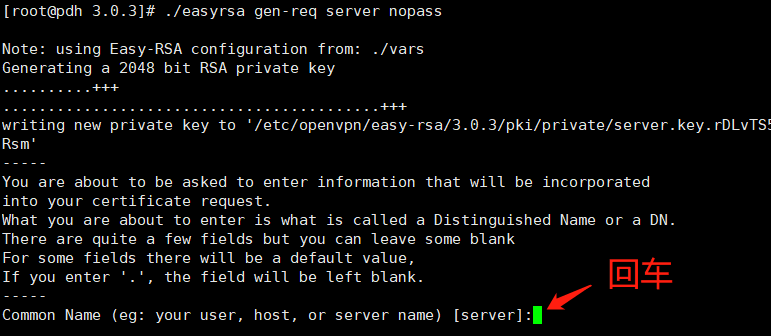
./easyrsa build-ca nopass

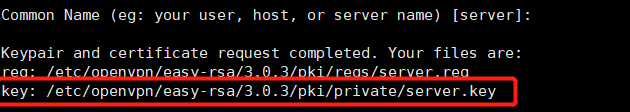




创建服务端证书

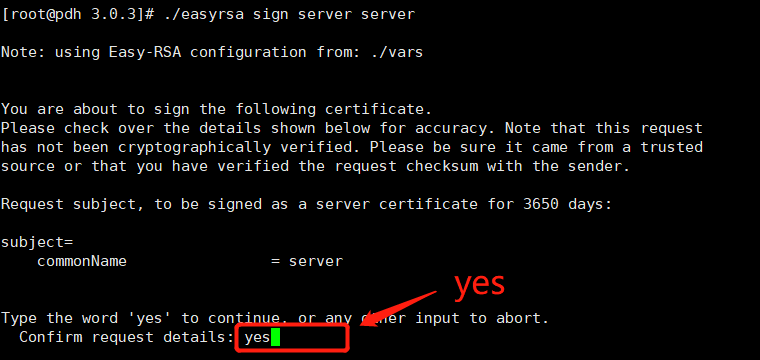
./easyrsa gen-req server nopass





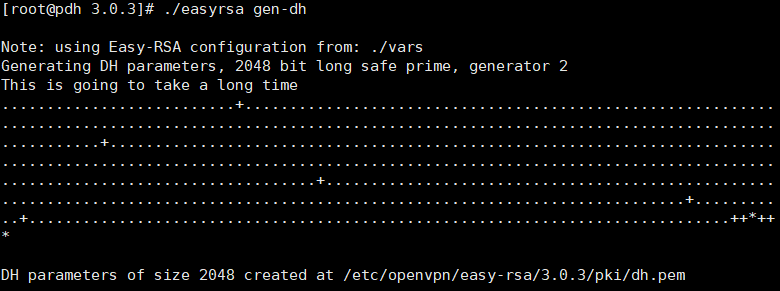
签约服务端证书

./easyrsa sign server server



创建 Diffie-Hellman

./easyrsa gen-dh



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/

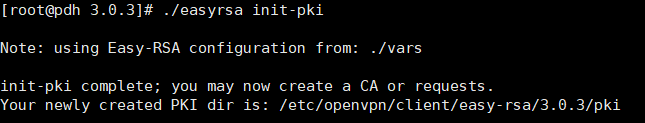
\rm 3 3.0

cd 3.0.3/

find / -type f -name "vars.example" | xargs -i cp {} . && mv vars.example vars

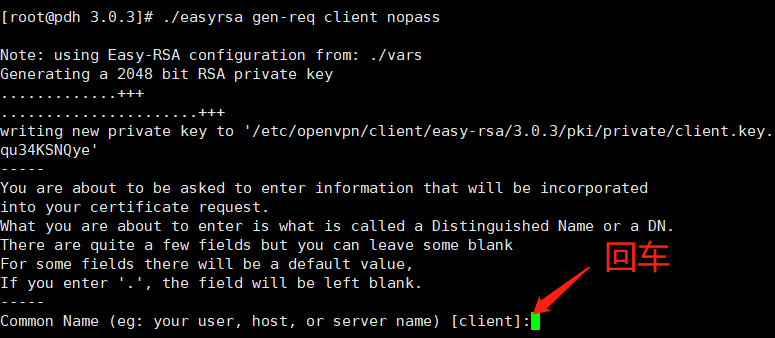
创建新的pki

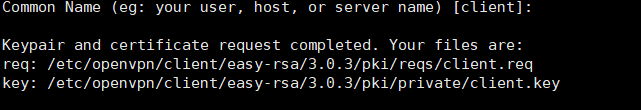
./easyrsa init-pki



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

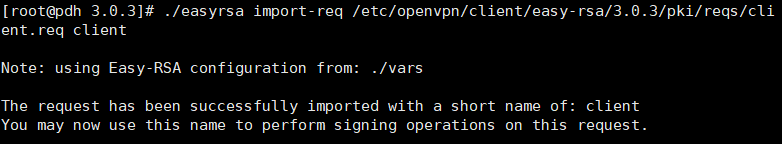




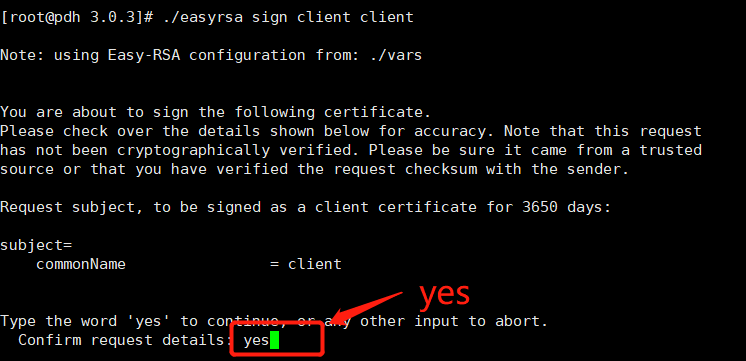
签约客户端证书，如有多个请签约多个

cd /etc/openvpn/easy-rsa/3.0.3/

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



./easyrsa sign client client



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 udp

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 39.106.153.182 1194

proto udp

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 39.106.153.182 1194 为服务器IP和端口，客户端为类linux操作系统时会有不同，详见：https://www.digitalocean.com/community/tutorials/how-to-set-up-an-openvpn-server-on-ubuntu-18-04）

**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 POSTROUTING -s 10.8.0.0/24 -j MASQUERADE

保存规则

service iptables save

开启转发

vi /etc/sysctl.conf

net.ipv4.ip\_forward = 1

查看一下系统参数

sysctl -p

开机启动

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

vi /etc/rc.d/rc.local

添加如下：

## 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

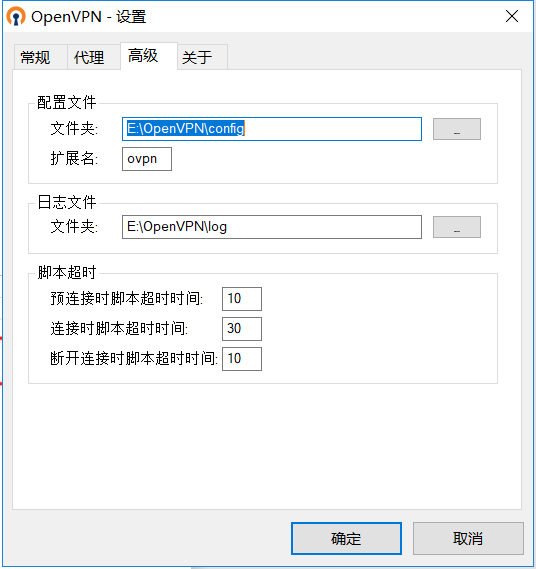
查看一下端口

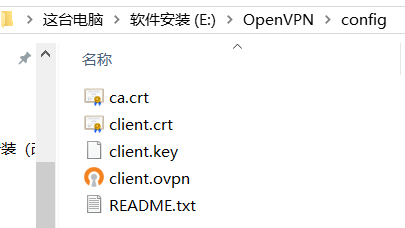
netstat -tunl | grep 1194



**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