链滴

OpenVPN 服务 SHELL 自动化部署脚本

作者：Carey

原文链接：https://ld246.com/article/1611668213504

来源网站：链滴

```
#!/bin/bash
#
#**********************************************************************
#Author:zhangzhuo
#QQ: 1191400158
#Date: 2021-01-26
#FileName：  openvpn_install.sh
#URL: [https://www.zhangzhuo.ltd](https://www.zhangzhuo.ltd)
#Description：  The test script
#Copyright (C): 2021 All rights reserved
#**********************************************************************
openvpn_install(){
while :;do
    read -p "请输入OpenVPN服务器公网IP: " IP
    { echo $IP | grep -E "^(([1-9]?[0-9]|1[0-9](#)|2[0-4](#)|25[0-5]).){3}([1-9]?[0-9]|1[0-9](#)|2[0-4
(#)|25[0-5])$">/dev/null; } && break || echo "请输入正确的IP地址！"
done

while :;do
    read -p "请输入内网的网络地址如(192.168.10.0): " NET
    { echo $NET | grep -E "^(([1-9]?[0-9]|1[0-9](#)|2[0-4](#)|25[0-5]).){3}([1-9]?[0-9]|1[0-9](#)|2[0
4](#)|25[0-5])$">/dev/null; } && break || echo "请输入正确的网络地址！"
done

while :;do
    read -p "请输入内网的子网掩码如(255.255.255.0): " MASK
    { echo $MASK | grep -E "^(([1-9]?[0-9]|1[0-9](#)|2[0-4](#)|25[0-5]).){3}([1-9]?[0-9]|1[0-9](#)|2
0-4](#)|25[0-5])$">/dev/null; } && break || echo "请输入正确的子网掩码！"
done

centos_Version                          #版本centos版本区分，centos8缺少server文件
yum install -y openvpn easy-rsa       #安装
```

```
rpm -ql openvpn &>/dev/null || { echo "openvpn服务安装失败请检查YUM是否配置EPEL源";exit ;

rpm -ql easy-rsa &>/dev/null || { echo "easy-rsa服务安装失败请检查YUM是否配置EPEL源";exit ;}

#准备服务器端证书环境
cp -r /usr/share/easy-rsa/ /etc/openvpn/easy-rsa-server
#修改vars配置文件
cp /usr/share/doc/easy-rsa/vars.example /etc/openvpn/easy-rsa-server/3/vars
#修改CA自签证书有效期
sed -ri 's/.*(set_var EASYRSA_CA_EXPIRE).*/\1 36500/' /etc/openvpn/easy-rsa-server/3/vars
#修改openvpn服务器证书有效期
sed -ri 's/.*(set_var EASYRSA_CERT_EXPIRE).*/\1 3650/' /etc/openvpn/easy-rsa-server/3/vars

cd /etc/openvpn/easy-rsa-server/3
#初始化PKI生成PKI相关目录和文件
./easyrsa init-pki
#创建CA机构
echo -e "\n" | ./easyrsa build-ca nopass
#创建openvpn服务器证书并颁发
echo -e "\n" | ./easyrsa gen-req server nopass
echo -e "yes\n" | ./easyrsa sign server server
#创建Diffie-Hellman算法
./easyrsa gen-dh

#准备客户端证书环境
cp -r /usr/share/easy-rsa/ /etc/openvpn/easy-rsa-client
cp /usr/share/doc/easy-rsa/vars.example /etc/openvpn/easy-rsa-client/3/vars
cd /etc/openvpn/easy-rsa-client/3
./easyrsa init-pki

#修改客户端证书有效期，根据自己的实际情况可修改
sed -ri 's/.*(set_var EASYRSA_CERT_EXPIRE).*/\1 180/' /etc/openvpn/easy-rsa-client/3/vars

#CA和服务器证书复制到openvpn服务的目录
mkdir /etc/openvpn/certs
cp /etc/openvpn/easy-rsa-server/3/pki/ca.crt /etc/openvpn/certs/
cp /etc/openvpn/easy-rsa-server/3/pki/issued/server.crt /etc/openvpn/certs/
cp /etc/openvpn/easy-rsa-server/3/pki/private/server.key /etc/openvpn/certs/
cp /etc/openvpn/easy-rsa-server/3/pki/dh.pem /etc/openvpn/certs/
openvpn --genkey --secret /etc/openvpn/certs/ta.key

#准备客户端配置文件
mkdir /etc/openvpn/client-file
cp /etc/openvpn/certs/{ca.crt,dh.pem,ta.key} /etc/openvpn/client-file
cat <<EOF >/etc/openvpn/client-file/client.ovpn
client
dev tun
proto tcp
remote server-ip 1194
resolv-retry infinite
nobind
#persist-key
#persist-tun
ca ca.crt
```

```
cert client.crt
key client.key
remote-cert-tls server
#tls-auth ta.key 1
cipher AES-256-CBC
verb 3
compress lz4-v2
tls-auth ta.key 1
EOF
sed -ri "s/(server-ip)/$IP/" /etc/openvpn/client-file/client.ovpn

#生成证书吊销列表
cd /etc/openvpn/easy-rsa-server/3
./easyrsa gen-crl

#创建openvpn日志目录
mkdir /var/log/openvpn
chown openvpn: /var/log/openvpn/

#生成openvpn服务器配置文件
cat <<EOF >/etc/openvpn/server.conf
port 1194
proto tcp
#pexplicit-exit-notify 1
dev tun
ca /etc/openvpn/certs/ca.crt
cert /etc/openvpn/certs/server.crt
key /etc/openvpn/certs/server.key
dh /etc/openvpn/certs/dh.pem
server 10.0.0.0 255.255.255.0
push "route network"
keepalive 10 120
cipher AES-256-CBC
compress lz4-v2
push "compress lz4-v2"
;comp-lzo
max-clients 2048
user openvpn
group openvpn
status /var/log/openvpn/openvpn-status.log
log-append /var/log/openvpn/openvpn.log
verb 3
mute 20
tls-auth /etc/openvpn/certs/ta.key 0
crl-verify /etc/openvpn/easy-rsa-server/3/pki/crl.pem
EOF
sed -ri "s/(network)/$NET $MASK/" /etc/openvpn/server.conf

#添加iptables规则和内核参数
echo net.ipv4.ip_forward = 1 >>/etc/sysctl.conf
sysctl -p
echo "iptables -t nat -APOSTROUTING -s 10.0.0.0/24 -j MASQUERADE" >>/etc/rc.d/rc.local
chmod +x /etc/rc.d/rc.local
/etc/rc.d/rc.local
```

```
#启动openvpn服务
systemctl daemon-reload
systemctl enable --now openvpn@server
echo -e "\033[1;31m服务安装完成，已经启动！\033[0m"
}

#centos系统版本区分
centos_Version(){
Version=`grep -Eo "[0-9].[0-9]" /etc/redhat-release | tr '.' '%' | tr '\n' % |cut -d% -f 1`
if [ $Version = 8 ];then
cat <<EOF >/lib/systemd/system/openvpn@.service
[Unit]
Description=OpenVPN Robust And Highly Flexible Tunneling Application On %I
After=network.target

[Service]
Type=notify
PrivateTmp=true
ExecStart=/usr/sbin/openvpn --cd /etc/openvpn/ --config %i.conf

[Install]
WantedBy=multi-user.target
EOF
chmod 644 /lib/systemd/system/openvpn@.service
fi
}

issue(){
while :;do
   read -p "请输入创建证书的人名全拼如(zhangzhuo):" REQ_NAME
   ls -ld /etc/openvpn/client/$REQ_NAME &>/dev/null && echo "用户已经存在" || break
done
read -p "私钥是否设置密码(1设置，其他为不设置)" A
if [ ! $A = 1 ];then
NOPASS=nopass
fi
#生成证书申请文件
cd /etc/openvpn/easy-rsa-client/3
echo -e "\n" | ./easyrsa gen-req $REQ_NAME $NOPASS
#导入申请文件到CA
cd /etc/openvpn/easy-rsa-server/3
./easyrsa import-req /etc/openvpn/easy-rsa-client/3/pki/reqs/$REQ_NAME.req $REQ_NAME
#颁发
echo -e "yes\n" | ./easyrsa sign client $REQ_NAME
#创建用户客户端配置文件
mkdir /etc/openvpn/client/$REQ_NAME
cp /etc/openvpn/easy-rsa-server/3/pki/issued/${REQ_NAME}.crt /etc/openvpn/client/${REQ_
AME}
cp /etc/openvpn/easy-rsa-client/3/pki/private/${REQ_NAME}.key /etc/openvpn/client/${REQ
NAME}
cp /etc/openvpn/client-file/* /etc/openvpn/client/${REQ_NAME}
mv /etc/openvpn/client/${REQ_NAME}/${REQ_NAME}.crt /etc/openvpn/client/${REQ_NAME}/
lient.crt
```

```
mv /etc/openvpn/client/${REQ_NAME}/${REQ_NAME}.key /etc/openvpn/client/${REQ_NAME}
client.key
cd /etc/openvpn/client/${REQ_NAME}/
#打包用户客户端配置文件
tar -cf ${REQ_NAME}.tar *
cp ${REQ_NAME}.tar  /root/
echo -e "\033[1;31m用户客户端配置文件已经生成，已经打包放置到root目录下\033[0m"
echo -e "\033[1;31m原本的文件在/etc/openvpn/client/文件夹下\033[0m"
}


revoked(){
echo `ls /etc/openvpn/client/`
while :;do
read -p "请输入要吊销的用户名:" NAME
ls -ld /etc/openvpn/client/$NAME &>/dev/null && { rm -rf /etc/openvpn/client/$NAME;break
 } || echo "没有这个用户请重新输入！"
done
cd /etc/openvpn/easy-rsa-server/3
echo -e "yes\n" | ./easyrsa revoke $NAME
./easyrsa gen-crl

systemctl restart openvpn@server
}

PS3="请选择相应的编号(1-4):"
MENU="
安装OpenVPN服务
给用户颁发证书
吊销用户证书
退出
"
select menu in $MENU;do
case $REPLY in
1)
    openvpn_install
    ;;
2)
    issue
    ;;
3)
    revoked
    ;;
4)
    break
    ;;
*)
    echo -e "\e[1;31m输入错误,请输入正确的数字(1-3)!\e[0m"
    ;;
esac
done
```

脚本功能

- 可以实现在Centos7和8系统部署openvpn服务,部署完成后CA证书100年，openvpn证书10年
- 可以自动实现客户端证书颁发，有效期180天
- 脚本具体过程脚本中有注释

原文链接：OpenVPN 服务 SHELL 自动化部署脚本