**Openvpn+system accout 认证**

本次配置环境centos 7

Yum源配置好，可以选择阿里云源

安装依赖包

yum install -y lzo lzo-devel openssl openssl-devel pam pam-develyum install -y pkcs11-helper pkcs11-helper-devel

安装openvpn服务

wget [http://oss.aliyuncs.com/aliyunecs/openvpn-2.2.2.tar.gz](http://oss.aliyuncs.com/aliyunecs/openvpn-2.2.2.tar.gz?spm=5176.7742521.0.0.cUaCX1&file=openvpn-2.2.2.tar.gz)

使用rpmbuild 将源码包编译成rpm包来进行安装

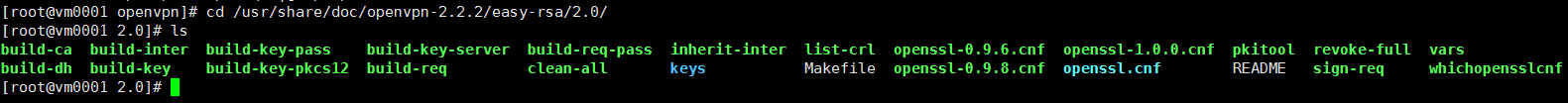
Rpmbuild –tb openvpn-2.2.2.tar.gz

编译完成后会在编译完成以后会在 /root/rpmbuild/RPMS/x86\_64 目录下生成 openvpn-2.2.2-1.x86\_64.rpm 安装包

初始化KPI

cd /usr/share/doc/openvpn-2.2.2/easy-rsa/2.0

进入到 /usr/share/doc/openvpn-2.2.2/easy-rsa/2.0 目录下，找到 vars 证书环境文件，修改以下几行 export 定义的参数值



export KEY\_COUNTRY="CN"

export KEY\_CITY="ShangHai"

export KEY\_PROVINCE="ShangHai"

export KEY\_ORG="pyyx"

export KEY\_EMAIL="huanghuajin@pyyx.com"

export KEY\_EMAIL=mail@host.domain

export KEY\_CN=changeme

export KEY\_NAME=changeme

export KEY\_OU=changeme

export PKCS11\_MODULE\_PATH=changeme

export PKCS11\_PIN=1234

上述参数的值可以自定义设置，对配置无影响

生成服务端证书

清楚并删除leys目录下的所有key

ln -s openssl-1.0.0.cnf openssl.cnf

source ./vars

./clean-all

生成CA证书

./build-ca

生成服务器证书，pyyx是自定义的名字，完成后在keys目录下保存pyyx.csr 、pyyx.crt、pyyx.key三个文件

./build-key-server pyyx

创建用户密钥与证书

./build-key pyyxuser

生成 Diffie Hellman参 数

./build-dh

执行了./build-dh后，会在 keys 目录下生成 dh 参数文件 dh1024.pem。该文件客户端验证的时候会用到

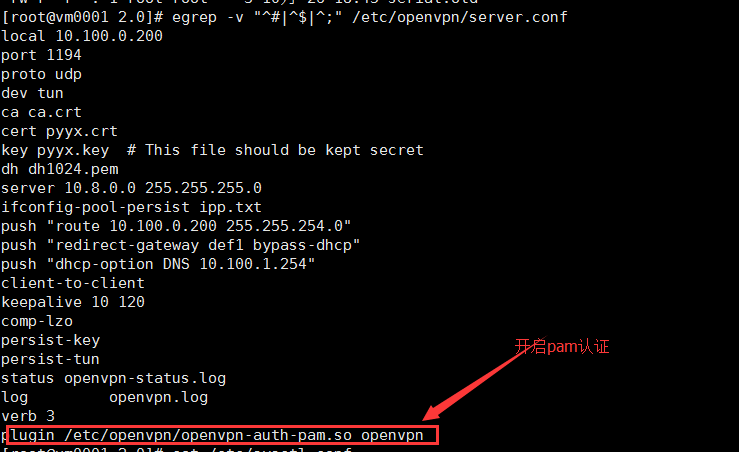
将 /usr/share/doc/openvpn-2.2.2/easy-rsa/2.0/keys 目录下的所有文件复制到 /etc/openvpn下

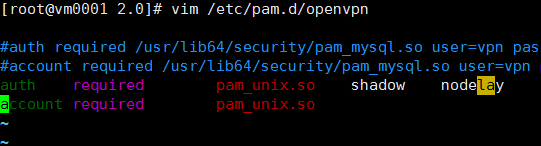
cp -a /usr/share/doc/openvpn-2.2.2/easy-rsa/2.0/keys/\* /etc/openvpn/

复制 openvpn 服务端配置文件 server.conf 到 /etc/openvpn/ 目录下

cp -a /usr/share/doc/openvpn-2.2.2/sample-config-files/server.conf /etc/openvpn/

配置内容如下





**开启路由转发**

**[root@vm0001 2.0]# cat /etc/sysctl.conf**

**# System default settings live in /usr/lib/sysctl.d/00-system.conf.**

**# To override those settings, enter new settings here, or in an /etc/sysctl.d/<name>.conf file**

**#**

**# For more information, see sysctl.conf(5) and sysctl.d(5).**

**net.ipv4.ip\_forward = 1**

**systemctl –p 使内核参数生效**

**添加iptables规则(centos6)**

**Iptables –t nat –A POSTROUTING –s 10.100.0.0/23 –j MASQUERADE**

**Service iptables save**

**Centos7**

**Firewall-cmd –add-service openvpn**

**Firewall-cmd –permanent –add-service openvpn**

**检查**

**[root@vm0001 2.0]# firewall-cmd --list-services**

**dhcpv6-client openvpn radius ssh**

**添加masquerade**

**Firewall-cmd –add-masquerade**

**Firewall-cmd –permanent –add-masquerade**

**Firewall-cmd –query-masquerade**

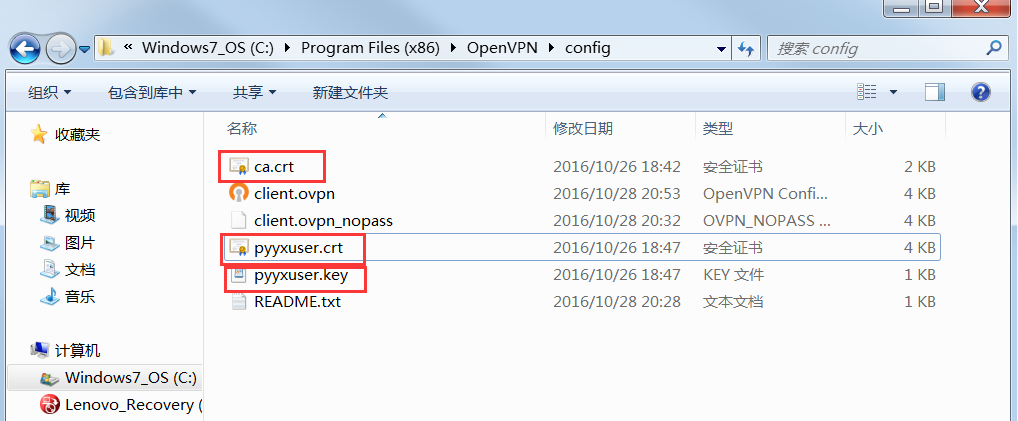
**启动openvpn**

**Service openvpn start**

**查看1194端口是否在监听**

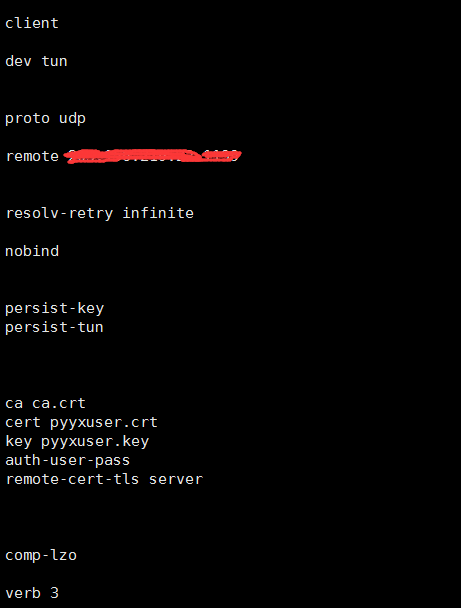
**Windows客户端配置**

**安装openvpn客户端**



**将红色部分的几个文件传到windows客户端对应路径**

**编辑client.ovpn**



**安卓客户端**

**https://play.google.com/store/apps/details?id=net.openvpn.openvpn**

**ios客户端**

**到app stone下载OpenVPN Connect**