

原创

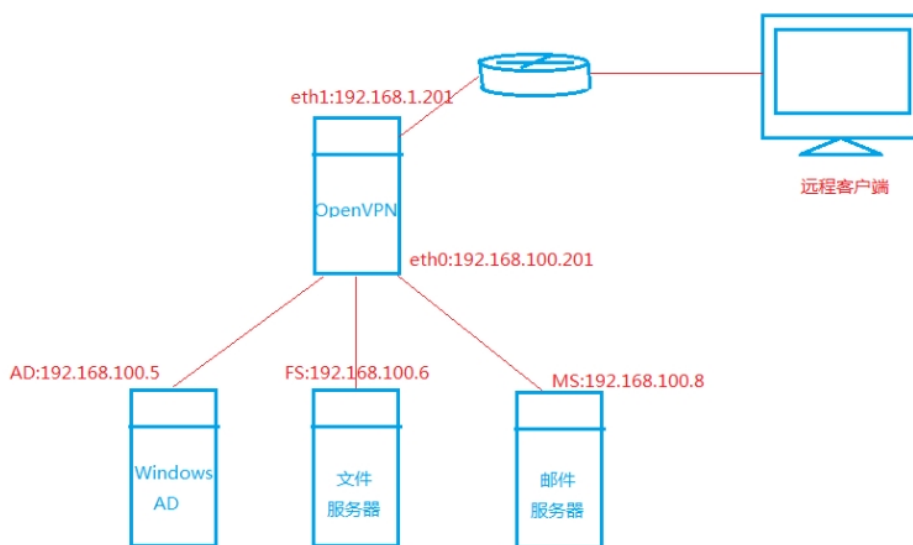
# CentOS 6.5基于Openxxx的xxx服务器构建



rong341233

[关注](#)

2014-04-29 10:37:10 5582人阅读 2人评论



外部用户透过路由器从open\*\*\*服务器映射出的1194端口，连接xxx服务器，从而访问公司内部服务。

<http://down.51cto.com/data/1142891>

这里我已经有将open\*\*\*软件进行打包(包含了open\*\*\*-2.3.3.tar.gz服务器安装包 open\*\*\* 32/64位客户端 lzo-2.0.6.tar.gz依赖包 easy-rsa证书制作工具)

## 1.时间校对

开始没有对时，导致后来无法联入xxx

```
yum -y install unzip pam-devel ntpdate openssl openssl-devel
#unzip用于解压软件
#pam-devel是安装open***必要的依赖包
#ntpdate是网络校时工具
```

```
ntpdate time.nist.gov
echo "/usr/sbin/ntpdate time.nist.gov" >> /etc/rc.local
echo "* */2 * * * /usr/sbin/ntpdate time.nist.gov" >> /etc/crontab
```

## 2.lzo的安装

```
unzip open***-2.3.3.zip
```

```
cd open***-2.3.3
tar zxvf lzo-2.06.tar.gz
cd lzo-2.06
./configure --prefix=/usr
make && make install
/sbin/ldconfig
cd ..
```

### 3.open\*\*\*的安装

```
mkdir -p /data/open***/conf
#用于存放配置文件
mkdir -p /data/open***/log
#用于存放open***日志
mkdir -p /data/open***/easy-rsa
#用于存放密钥生成工具及密钥
tar zxvf open***-2.3.3.tar.gz
cd open***-2.3.3
./configure --prefix=/data/open***
make && make install
cp sample/sample-config-files/server.conf /data/open***/conf/
#拷贝实例配置文件
cd ..
```

### 4.easy-rsa的解压

```
unzip easy-rsa.zip
cd easy-rsa/2.0/
cp -rf * /data/open***/easy-rsa/
cd /data/open***/easy-rsa/
chmod +x *
```

### 5.修改vars文件

```
vim vars
export KEY_SIZE=2048
export CA_EXPIRE=3650
export KEY_EXPIRE=365
export KEY_COUNTRY="CN"
export KEY_PROVINCE="GD"
export KEY_CITY="ShenZhen"      城市随便填一个即可
export KEY_ORG="Example INC"    组织单位
export KEY_EMAIL="ca@example.com" 邮箱地址可以随便填写
export KEY_OU="Manager"        组织容器可以随便填写
export KEY_NAME="xxxService"   名称可以随便填写
```

```
export KEY_SIZE=2048
#加密的位数，越大越安全，但是时间更长，也增加CPU负担
# In how many days should the root CA key expire?
export CA_EXPIRE=3650
#根证书的有效期，这个可以相应的设的时间长些，这里为10年
# In how many days should certificates expire?
export KEY_EXPIRE=365
#密钥的有效期，根据公司安全进行设置，半年或一年，不宜设的太长
# These are the default values for fields
# which will be placed in the certificate.
# Don't leave any of these fields blank.
export KEY_COUNTRY="CN" 国家
export KEY_PROVINCE="GD" 省份
export KEY_CITY="ShenZhen" 城市
export KEY_ORG="Example INC" 组织
export KEY_EMAIL="ca@example.com" 邮箱
export KEY_OU="Manager" 容器

# X509 Subject Field
export KEY_NAME="VPNService" 名称
```

```
source vars
#使之生效
```

## 6.生成证书

```
./clean-all
#初始化
./build-ca
#创建根证书，一路回车即可
Generating a 2048 bit RSA private key
.....+++
.+++
writing new private key to 'ca.key'
-----
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.
-----
Country Name (2 letter code) [CN]:
State or Province Name (full name) [GD]:
Locality Name (eg, city) [ShenZhen]:
Organization Name (eg, company) [Example INC]:
Organizational Unit Name (eg, section) [Manager]:
Common Name (eg, your name or your server's hostname) [Example INC CA]:
Name [xxxService]:
Email Address [ca@example.com]:
```

## 创建服务器端密钥

```
./build-key-server server
Country Name (2 letter code) [CN]: #回车
State or Province Name (full name) [GD]: #回车
Locality Name (eg, city) [ShenZhen]: #回车
Organization Name (eg, company) [Example INC]: #回车
Organizational Unit Name (eg, section) [Manager]: #回车
Common Name (eg, your name or your server's hostname) [server]: #回车
Name [xxxService]: #回车
Email Address [ca@example.com]: #回车
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []: #回车
An optional company name []: #回车
Using configuration from /data/open***/easy-rsa/openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName          :PRINTABLE:'CN'
stateOrProvinceName  :PRINTABLE:'GD'
localityName         :PRINTABLE:'ShenZhen'
organizationName     :PRINTABLE:'Example INC'
organizationalUnitName:PRINTABLE:'Manager'
commonName           :PRINTABLE:'server'
name                 :PRINTABLE:'xxxService'
emailAddress         :IASSTRING:'ca@example.com'
Certificate is to be certified until May  5 02:35:08 2015 GMT (365 days)
Sign the certificate? [y/n]:y #输入y,回车
1 out of 1 certificate requests certified, commit? [y/n]y #输入y,回车
Write out database with 1 new entries
Data Base Updated
```

## 创建用户

```
./build-key client
#创建client用户
#方法和创建服务器密钥是一样的
```

## 创建Diffie-Hellman文件

```
./build-dh
```

## 7.配置open\*\*\*

```
#本机要侦听使用的IP地址
local 192.168.1.201
#使用的端口，默认1194
port 1194
#使用的协议，默认使用UDP，如果使用HTTP proxy，必须使用TCP协议
proto udp
#使用的设备可选tap和tun，tap是二层设备，支持链路层协议。
#tun是ip层的点对点协议，限制稍微多一些，建议使用tun,如果使用桥接的话，就必须使用tap
dev tun
#Openxxx使用的ROOT CA，使用build-ca生成的，用于验证客户证书是否合法
ca /data/open***/easy-rsa/keys/ca.crt
#Server使用的证书文件
cert /data/open***/easy-rsa/keys/server.crt
#Server使用的证书对应的key，注意文件的权限，防止被盗
key /data/open***/easy-rsa/keys/server.key # This file should be kept secret
#上面提到的生成的Diffie-Hellman文件
dh /data/open***/easy-rsa/keys/dh2048.pem
#防止注销用户登录
#crl-verify /data/open***/easy-rsa/keys/crl.pem
#客户端使用的地址、子网掩码
server 10.8.0.0 255.255.255.0
#用于记录某个Client获得的IP地址，类似于dhcpd.lease文件，
#防止open***重新启动后“忘记”Client曾经使用过的IP地址
ifconfig-pool-persist /data/open***/log/ipp.txt
#DHCP的DNS选项
push "dhcp-option DNS 114.114.114.114"
push "dhcp-option DNS 8.8.4.4"
#通过xxx Server往Client push路由，client通过pull指令获得Server push的所有选项并应用
push "route 192.168.100.0 255.255.255.0"
#如果可以让xxx Client之间相互访问直接通过open***程序转发，
#不用发送到tun或者tap设备后重新转发，优化Client to Client的访问效率
client-to-client
#如果Client使用的CA的Common Name有重复了，或者说客户都使用相同的CA
#和keys连接xxx，一定要打开这个选项，否则只允许一个人连接xxx，建议一人一个证书
duplicate-cn
#定义最大连接数
max-clients 10
#NAT后面使用xxx，如果xxx长时间不通信，NAT Session可能会失效，
#导致xxx连接丢失，为防止之类事情的发生，keepalive提供一个类似于ping的机制，
#下面表示每10秒通过xxx的Control通道ping对方，如果连续120秒无法ping通，
#认为连接丢失，并重新启动xxx，重新连接
#（对于mode server模式下的open***不会重新连接）。
keepalive 10 120
#对数据进行压缩，注意Server和Client一致
comp-lzo
#通过keepalive检测超时后，重新启动xxx，不重新读取keys，保留第一次使用的keys
persist-key
#通过keepalive检测超时后，重新启动xxx，一直保持tun或者tap设备是linkup的，
#否则网络连接会先linkdown然后linkup
```

```

persist-tun
#定期把open***的一些状态信息写到文件中，以便自己写程序计费或者进行其它操作
status /data/open***/log/open***-status.log
#和log一致，每次重新启动open***后保留原有的log信息，新信息追加到文件最后
log-append /data/open***/log/open***.log
#相当于debug level，具体查看manual
verb 3

```

## 8.启动open\*\*\*服务

```
/data/open***/sbin/open*** --config /data/open***/conf/server.conf &
```

查看是否启动成功

```

[root@xxxServer easy-rsa]# netstat -ntlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID
tcp        0      0 0.0.0.0:22             0.0.0.0:*               LISTEN      801
tcp        0      0 :::22                  :::*                    LISTEN      801
udp        0      0 0.0.0.0:1194           0.0.0.0:*               16

```

可以看到1194端口已经启动，说明open\*\*\*启动成功

## 9.注销证书

同事离职了，需要将证书进行注销

```

#注销账户test
/data/open***/easy-rsa/revoke-full test
Using configuration from /data/open***/easy-rsa/openssl-1.0.0.cnf
Revoking Certificate 03.
Data Base Updated
Using configuration from /data/open***/easy-rsa/openssl-1.0.0.cnf
lushare.crt: C = CN, ST = GD, L = ShenZhen, O = Example INC, OU = Manager, CN = test, not before=Jan 1 00:00:00 2019, not after=Jan 1 00:00:00 2020, error 23 at 0 depth lookup:certificate revoked
#error 23说明证书已经注销

```

这个时候还是可以利用此证书登录服务器的，在/data/open\*\*\*/conf/server.conf下增加一行

```
crl-verify /data/open***/easy-rsa/keys/crl.pem
```

再重启下open\*\*\*服务即可

```

killall open***
/data/open***/sbin/open*** --config /data/open***/conf/server.conf &

```

这个时候open\*\*\*下的test账户已经不能登录服务器了

## 10.修改/etc/sysctl.conf

```

vim /etc/sysctl.conf
将下面值修改为1，开启Linux ip跳转
net.ipv4.ip_forward = 1
#保存后执行
sysctl -p

```

## 11.防火墙修改

```

iptables -F
iptables -X
iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -A INPUT -i lo -j ACCEPT

```

```






iptables -A OUTPUT -o lo -j ACCEPT
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -p udp --dport 1194 -j ACCEPT
#对IP进行转发
iptables -t nat -A POSTROUTING -o eth0 -s 10.8.0.0/24 -j MASQUERADE
iptables -t nat -A POSTROUTING -o eth1 -s 10.8.0.0/24 -j MASQUERADE
service iptables save
service iptables restart

```

或者上面的也可以改成




```
iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -d 192.168.1.0/24 -o eth0 -j SNAT --to-source
```

## 12.客户端安装配置

 easy-rsa.zip	4/23/2014 8:35 ...	压缩(zip)文件...	28 KB
 lzo-2.06.tar.gz	4/23/2014 8:35 ...	GZ 文件	570 KB
 openvpn-2.3.3.tar.gz	4/23/2014 8:30 ...	GZ 文件	1,134 KB
 openvpn-install-2.3.3-1002-i686.exe	4/23/2014 8:31 ...	应用程序	1,639 KB
 openvpn-install-2.3.3-1002-x86_64.exe	4/23/2014 8:31 ...	应用程序	1,723 KB

里面有一个32位的安装客户端，也有一个64位的，按需安装即可

，安装完成后，将C:\Program Files\Open×××\sample-config(我这里安装在C:\Program Files\Open×××)目录下的client.o\*\*\*

名称	修改日期	类型	大小
 client.ovpn	4/14/2014 8:48 ...	OpenVPN Confi...	4 KB
 sample.ovpn	4/14/2014 8:48 ...	OpenVPN Confi...	4 KB
 server.ovpn	4/14/2014 8:48 ...	OpenVPN Confi...	11 KB

拷贝到C:\Program Files\Open×××\config

修改client.o\*\*\*

```

client
dev tun      #设备类型tun、tap根据服务器来设置
proto udp    #所使用的协议有udp、tcp根据服务器来设置
remote 192.168.100.201 1194  #主服务器
#remote 250.250.250.250 1194  #备用服务器
#remote-random      #开启服务器的轮询，如果设置了多台服务器的话
resolv-retry infinite
nobind
;user nobody
;group nobody
persist-key
persist-tun
ca ca.crt      #ca证书是从服务器上下载来的
cert client.crt  #生成的客户端证书
key client.key  #服务器上生成的密码
ns-cert-type server
comp-lzo      #压缩类型
verb 3

```

注意：如果是win7/win8的话需要使用管理员权限运行，否则是无法增加路由的

如果公司使用的是ADSL动态IP上网的话，如果要提供服务的话可以使用花生壳（不推荐，相当不稳定），建议自己申请域名使用DNSPOD进行动态解析，设置详情可以查看

<http://fengwan.blog.51cto.com/508652/1404534>