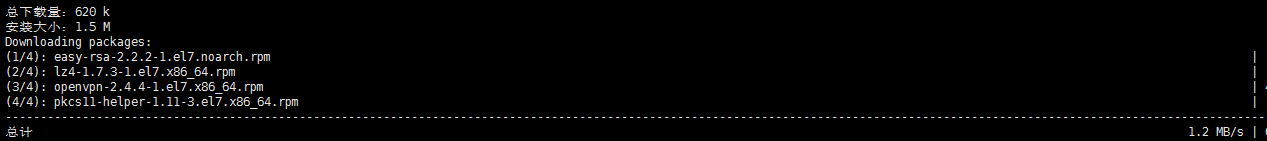
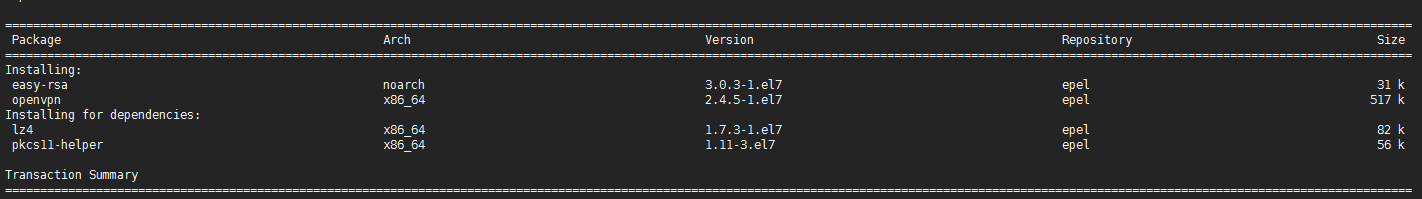
emmmm，前段时间把公司用的 vpn 换掉了，换成了 openvpn，刚开始用的是 tcp 协议，没有用 udp，然而，之前在家里连接到 VPN 之后向服务器传东西慢的有点夸张，只有 20 几 K，忍无可忍，无需再忍，就前几天把协议从 tcp 切换到了 udp 协议，经过测试没有问题，传输速率提升了 N 倍，但是这个 vpn 不止我们研发部门在用，而财务的也在用，他们外出有时候需要连接内部的财务服务器，下午找我说外出连接 vpn 之后连不到财务的服务器了，之前还行，最后经过确认是 vpn 的问题，使用 tcp 协议的时候就可以正常连接，而且换到 udp 协议之后就不行了，这个有点蛋疼，难不成再换回 tcp 的？不太现实，所以准备新装一套专给财务用，说搞就搞，但是情况和我之前搞不太一样了，具体如下。  
老



新

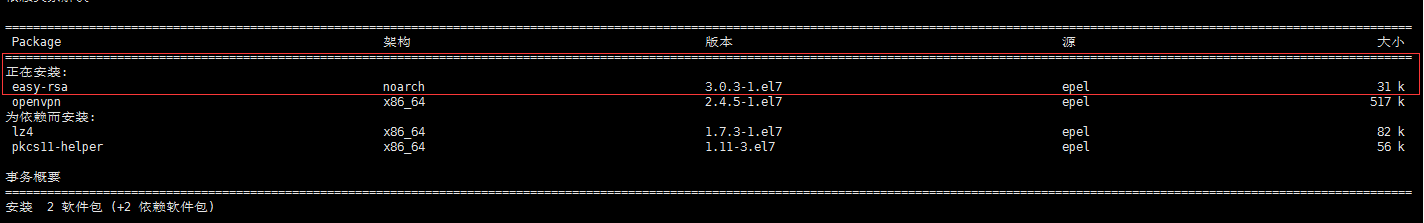


easy-rsa 的版本从之前的 2.2 直接窜到了 3.0，也都是用 yum 装的，貌似是更新了吧，今晚有点事要加班，就顺便琢磨了一下，配置和之前完全不一样了，还有点麻烦，具体如下，本篇文章写得不完整，这是针对 3.0 生成证书，2.2 完整版点[这里](https://blog.rj-bai.com/post/132.html)，而且这篇文章没怎么贴图，如果你看这晕就Ctrl+F查找 localhost，也就是我主机名，兴许看着没那么晕，哈哈。

**安装软件包展开目录**

环境就是新装 CentOS7.4，使用阿里云的 epel 源和常规源，不知道别的源有没有更新这个包，不废话，直接安装软件包。

[root@localhost ~]# yum -y install openvpn easy-rsa



看这里，如果是 2.2 的，直接去看[这里](https://blog.rj-bai.com/post/132.html)吧。

**配置 easy-rsa-3.0展开目录**

**复制文件展开目录**

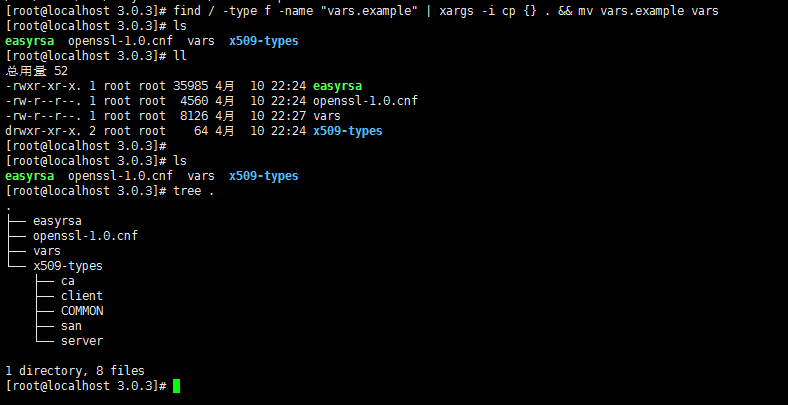
[root@localhost ~]# cp -r /usr/share/easy-rsa/ /etc/openvpn/easy-rsa

[root@localhost ~]# cd /etc/openvpn/easy-rsa/

[root@localhost easy-rsa]# \rm 3 3.0

[root@localhost easy-rsa]# cd 3.0.3/

[root@localhost 3.0.3]# find / -type f -name "vars.example" | xargs -i cp {} . && mv vars.example vars



这里说明一下，正常来说easy-rsa-3.0.3安装完之后，vars.example文件在/usr/share/doc/easy-rsa-3.0.3/目录，至于有些人说找不到这个文件，我暂时还没遇到过，可能你的安装方式和我不一致，或版本不同，不做深究，过。

**创建一个新的 PKI 和 CA展开目录**

[root@localhost 3.0.3]# pwd

/etc/openvpn/easy-rsa/3.0.3

[root@localhost 3.0.3]# ./easyrsa init-pki #创建空的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

[root@localhost 3.0.3]# ./easyrsa build-ca nopass #创建新的CA，不使用密码

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.pClvaQ1GLD'

-----

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

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

**创建服务端证书展开目录**

[root@localhost 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.wy7Q0fuG6A'

-----

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

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

**签约服务端证书展开目录**

[root@localhost 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

Using configuration **from** ./openssl-1.0.cnf

Check that the request matches the signature

Signature ok

The Subject's Distinguished Name is as follows

commonName :ASN.1 12:'server'

Certificate is to be certified until Apr 7 14:54:08 2028 GMT (3650 days)

Write out database with 1 new entries

Data Base Updated

Certificate created at: /etc/openvpn/easy-rsa/3.0.3/pki/issued/server.crt

**创建 Diffie-Hellman展开目录**

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

............................................................

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

到这里服务端的证书就创建完了，然后创建客户端的证书。

**创建客户端证书展开目录**

**复制文件展开目录**

[root@localhost ~]# cp -r /usr/share/easy-rsa/ /etc/openvpn/client/easy-rsa

[root@localhost ~]# cd /etc/openvpn/client/easy-rsa/

[root@localhost easy-rsa]# \rm 3 3.0

[root@localhost easy-rsa]# cd 3.0.3/

[root@localhost 3.0.3]# find / -type f -name "vars.example" | xargs -i cp {} . && mv vars.example vars

**生成证书展开目录**

[root@localhost 3.0.3]# pwd

/etc/openvpn/client/easy-rsa/3.0.3

[root@localhost 3.0.3]# ./easyrsa init-pki #创建新的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

[root@localhost 3.0.3]# ./easyrsa gen-req dalin nopass #客户证书名为大林，木有密码

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/dalin.key.FkrLzXH9Bm'

-----

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) [dalin]: 回车

Keypair and certificate request completed. Your files are:

req: /etc/openvpn/client/easy-rsa/3.0.3/pki/reqs/dalin.req

key: /etc/openvpn/client/easy-rsa/3.0.3/pki/**private**/dalin.key

**最后签约客户端证书展开目录**

[root@localhost 3.0.3]# cd /etc/openvpn/easy-rsa/3.0.3/

[root@localhost 3.0.3]# pwd

/etc/openvpn/easy-rsa/3.0.3

[root@localhost 3.0.3]# ./easyrsa import-req /etc/openvpn/client/easy-rsa/3.0.3/pki/reqs/dalin.req dalin

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

The request has been successfully imported with a short name of: dalin

You may now use **this** name to perform signing operations on **this** request.

[root@localhost 3.0.3]# ./easyrsa sign client dalin

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 = dalin

Type the word 'yes' to **continue**, **or** any other input to abort.

Confirm request details: yes

Using configuration **from** ./openssl-1.0.cnf

Check that the request matches the signature

Signature ok

The Subject's Distinguished Name is as follows

commonName :ASN.1 12:'dalin'

Certificate is to be certified until Apr 8 01:54:57 2028 GMT (3650 days)

Write out database with 1 new entries

Data Base Updated

Certificate created at: /etc/openvpn/easy-rsa/3.0.3/pki/issued/dalin.crt

**整理证书展开目录**

现在所有的证书都已经生成完了，下面来整理一下。

**服务端所需要的文件展开目录**

[root@localhost ~]# mkdir /etc/openvpn/certs

[root@localhost ~]# cd /etc/openvpn/certs/

[root@localhost certs]# cp /etc/openvpn/easy-rsa/3.0.3/pki/dh.pem .

[root@localhost certs]# cp /etc/openvpn/easy-rsa/3.0.3/pki/ca.crt .

[root@localhost certs]# cp /etc/openvpn/easy-rsa/3.0.3/pki/issued/server.crt .

[root@localhost certs]# cp /etc/openvpn/easy-rsa/3.0.3/pki/private/server.key .

[root@localhost certs]# ll

总用量 20

-rw-------. 1 root root 1172 4月 11 10:02 ca.crt

-rw-------. 1 root root 424 4月 11 10:03 dh.pem

-rw-------. 1 root root 4547 4月 11 10:03 server.crt

-rw-------. 1 root root 1704 4月 11 10:02 server.key

**客户端所需的文件展开目录**

[root@localhost certs]# mkdir /etc/openvpn/client/dalin/

[root@localhost certs]# cp /etc/openvpn/easy-rsa/3.0.3/pki/ca.crt /etc/openvpn/client/dalin/

[root@localhost certs]# cp /etc/openvpn/easy-rsa/3.0.3/pki/issued/dalin.crt /etc/openvpn/client/dalin/

[root@localhost certs]# cp /etc/openvpn/client/easy-rsa/3.0.3/pki/private/dalin.key /etc/openvpn/client/dalin/

[root@localhost certs]# ll /etc/openvpn/client/dalin/

总用量 16

-rw-------. 1 root root 1172 4月 11 10:07 ca.crt

-rw-------. 1 root root 4431 4月 11 10:08 dalin.crt

-rw-------. 1 root root 1704 4月 11 10:08 dalin.key

其实这三个文件就够了，之前全下载下来是因为方便，然而这次懒得弄了，哈哈，编写服务端配置文件。顺便提一下再添加用户在./easyrsa gen-req这里开始就行了, 像是吊销用户证书的命令都自己用./easyrsa --help去看吧，[GitHub](https://github.com/OpenVPN/easy-rsa/blob/v3.0.5/README.quickstart.md)项目地址

**服务器配置文件展开目录**

[root@localhost ~]# vim /etc/openvpn/server.conf

**local** 192.168.1.113

port 1194

proto tcp

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

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

server 17.166.221.0 255.255.255.0

**push** "route 192.168.1.0 255.255.255.0"

**push** "redirect-gateway def1 bypass-dhcp"

**push** "dhcp-option DNS 223.5.5.5"

**push** "dhcp-option DNS 223.6.6.6"

client-to-client

keepalive 20 120

comp-lzo

#duplicate-cn

user openvpn

group openvpn

persist-key

persist-tun

status openvpn-status.log

**log**-append openvpn.log

verb 1

mute 20

**启动服务展开目录**

启动服务

[root@localhost ~]# systemctl start openvpn@server

然后接下来的请看[这里](https://blog.rj-bai.com/post/132.html#menu_index_11)吧，从配置 iptables 及转发开始，懒得写了。

**吊销证书展开目录**

最近被游客问到如何去吊销证书，所以在这里就加一下，正常情况下证书就是一人一个，下面栗子，注销名为dalin的证书。

[root@openvpn ~]# cd /etc/openvpn/easy-rsa/

[root@openvpn easy-rsa]# ./easyrsa revoke dalin

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

Please confirm you wish to revoke the certificate with the following subject:

subject=

commonName = dalin

Type the word 'yes' to **continue**, or any other input to abort.

Continue with revocation: yes

Using configuration **from** /etc/openvpn/easy-rsa/openssl-1.0.cnf

Revoking Certificate 06.

Data Base Updated

IMPORTANT!!!

Revocation was successful. You must run gen-crl and upload a CRL to your

infrastructure **in** order to prevent the revoked cert **from** being accepted.

[root@openvpn easy-rsa]# ./easyrsa gen-crl

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

Using configuration **from** /etc/openvpn/easy-rsa/openssl-1.0.cnf

An updated CRL has been created.

CRL file: /etc/openvpn/easy-rsa/pki/crl.pem

执行上述命令后用户证书不会被删除，只是更新了crl.pem文件，可以看到上面的提示，文件位置在/etc/openvpn/easy-rsa/pki/crl.pem，查看所有证书的的信息，阔以这样去看。

[root@openvpn easy-rsa]# find /etc/openvpn/ -type f -name "index.txt" | xargs cat

V 280825082643Z 01 unknown /CN=server

R 280826061455Z 181211135800Z 03 unknown /CN=dalin

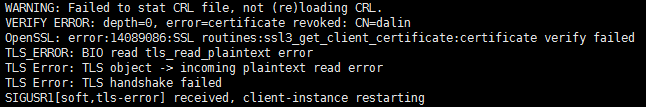
列举了两个作对比，V为可用，R为注销，现在dalin的证书还是能连接到服务器，现在需要告知服务端crl.pem的位置, 下面修改配置文件。

[root@openvpn easy-rsa]# vim /etc/openvpn/server.conf

crl-verify /etc/openvpn/easy-rsa/pki/crl.pem

[root@openvpn easy-rsa]# systemctl restart openvpn@server

这样就可以了，dalin现在就无法连接到服务器了，服务端日志。



emmmm，效果达到了，我还得重新生成一下，因为我要用，当然还叫dalin，这种情况建议将被吊销的证书删掉之后再生成新的。

[root@openvpn easy-rsa]# cd /etc/openvpn/

[root@openvpn openvpn]# find . -type f -name "dalin.\*" | xargs rm