

首页 » 杂乱文章 » 正文

easy-rsa-3.0在openvpn下的配置

2018-04-10 | 杂乱文章 | 暂无评论 | 2268 次阅读

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

```
总下载量: 620 k
安装大小: 1.5 M
Downloading packages:
(1/4): easy-rsa-2.2.2-1.el7.noarch.rpm
(2/4): lz4-1.7.3-1.el7.x86_64.rpm
(3/4): openvpn-2.4.4-1.el7.x86_64.rpm
(4/4): pkcs11-helper-1.11-3.el7.x86_64.rpm
-----
总计                                     1.2 MB/s |
```

新

Package	Arch	Version	Repository	Size
Installing:				
easy-rsa	noarch	3.0.3-1.el7	epel	31 k
openvpn	x86_64	2.4.5-1.el7	epel	517 k
Installing for dependencies:				
lz4	x86_64	1.7.3-1.el7	epel	82 k
pkcs11-helper	x86_64	1.11-3.el7	epel	56 k
Transaction Summary				

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](#)，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，请先关闭 **selinux**，且睁大您的眼睛仔细看，有些地方是需要输入 **yes** 的，别给我直接按回车。

安装软件包

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
```

easy-rsa	noarch	3.0.3-1.el7	epel	31 k
openvpn	x86_64	2.4.5-1.el7	epel	517 k
为依赖而安装:				
lz4	x86_64	1.7.3-1.el7	epel	82 k
pkcs11-helper	x86_64	1.11-3.el7	epel	56 k
事务概要				
安装 2 软件包 (+2 依赖软件包)				

看这里，如果是2.2的，直接去看[这里](#)吧。

配置easy-rsa-3.0

复制文件

```
[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 \
```

```
[root@localhost 3.0.3]# find / -type f -name "vars.example" | xargs -i cp {} . && mv vars.example vars
[root@localhost 3.0.3]# ls
easyrsa  openssl-1.0.cnf  vars  x509-types
[root@localhost 3.0.3]# ll
总用量 52
-rwxr-xr-x. 1 root root 35985 4月 10 22:24 easyrsa
-rw-r--r--. 1 root root 4560 4月 10 22:24 openssl-1.0.cnf
-rw-r--r--. 1 root root 8126 4月 10 22:27 vars
drwxr-xr-x. 2 root root 64 4月 10 22:24 x509-types
[root@localhost 3.0.3]#
[root@localhost 3.0.3]# ls
easyrsa  openssl-1.0.cnf  vars  x509-types
[root@localhost 3.0.3]# tree .
.
├── easyrsa
├── openssl-1.0.cnf
├── vars
└── x509-types
    ├── ca
    ├── client
    ├── COMMON
    ├── san
    └── server

1 directory, 8 files
[root@localhost 3.0.3]#
```

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

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
```

```
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:
```

创建服务端证书

```
[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

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



```
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/openssl/easy-rsa/3.0.3/pki/issued/server.crt
```

创建Diffie-Hellman

```
[root@localhost 3.0.3]# ./easysrsa gen-dh
.....
DH parameters of size 2048 created at /etc/openssl/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

复制文件

```
[root@localhost ~]# cp -r /usr/share/easy-rsa/ /etc/openssl/client/easy-rsa
[root@localhost ~]# cd /etc/openssl/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 \
```

生成证书

```
[root@localhost 3.0.3]# pwd
/etc/openssl/client/easy-rsa/3.0.3
[root@localhost 3.0.3]# ./easysrsa 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/openssl/client/easy-rsa/3.0.3/pki
[root@localhost 3.0.3]# ./easysrsa 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/openssl/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.

最后签约客户端证书

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

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=

整理证书

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

```
[root@localhost ~]# mkdir /etc/openssl/certs
[root@localhost ~]# cd /etc/openssl/certs/
[root@localhost certs]# cp /etc/openssl/easy-rsa/3.0.3/pki/dh.pem .
[root@localhost certs]# cp /etc/openssl/easy-rsa/3.0.3/pki/ca.crt .
[root@localhost certs]# cp /etc/openssl/easy-rsa/3.0.3/pki/issued/server.crt .
[root@localhost certs]# cp /etc/openssl/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

```
[root@localhost certs]# mkdir /etc/openssl/client/dalin/
[root@localhost certs]# cp /etc/openssl/easy-rsa/3.0.3/pki/ca.crt /etc/openssl/client/dalin/
[root@localhost certs]# cp /etc/openssl/easy-rsa/3.0.3/pki/issued/dalin.crt /etc/openssl/client/dalin/
[root@localhost certs]# cp /etc/openssl/easy-rsa/3.0.3/pki/private/dalin.key /etc/openssl/client/dalin/
```

```
-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](#)项目地址

服务器配置文件

```
[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
```

启动服务

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

然后接下来的请看[这里](#)吧，从配置iptables及转发开始，懒得写了。

吊销证书

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
```

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，可以这样去看。

```
[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。

```
WARNING: Failed to stat CRL file, not (re)loading CRL.
VERIFY ERROR: depth=0, error=certificate revoked: CN=dalin
OpenSSL: error:14089086:SSL routines:ssl3_get_client_certificate:certificate verify failed
TLS_ERROR: BIO read tls_read_plaintext error
TLS Error: TLS object -> incoming plaintext read error
TLS Error: TLS handshake failed
SIGUSR1[soft,tls-error] received, client-instance restarting
```

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
```

打赏: [微信](#), [支付宝](#)

标签: [vpn](#)



上一篇: [利用qshell同步七牛云存储数据到本地服务器](#)

下一篇: [docker入门及实践](#)
