链滴

# OpenVPN 集成 LDAP 踩坑记

作者：cuijianzhe
原文链接：https://ld246.com/article/1589975805640
来源网站：链滴

# 自建vpn


需求：直接替换阿里云购买的SSL VPN，硬刚.....trollface
rollface trollface

openvpn版本：2.4.9-1.el7

ease-rsa版本：3.0.7-1.el7

openvpn-auth-ldap版本：2.0.3-17.el7

# 搭建过程

1. 安装openvpn和easy-rsa

yum install -y openvpn easy-rsa

2. 创建easy-rsa key 的存放位置

mkdir -p /etc/openvpn/easy-rsa/keys

3. 复制相关文件至Openvpn目录

```
cp /usr/share/doc/openvpn-2.4.9/sample/sample-config-files/server.conf /etc/openvpn
cp -rf /usr/share/easy-rsa/3.0/* /etc/openvpn/easy-rsa/
cp /etc/openvpn/easy-rsa/openssl-easyrsa.cnf /etc/openvpn/easy-rsa/openssl.cnf
```

4. **生成tls-auth文件**

```
openvpn --genkey --secret /etc/openvpn/ta.key
```

5. **创建CA，并设置密码：**

```
[root@cjz openvpn]# cd /etc/openvpn/easy-rsa/
[root@cjz easy-rsa]# ./easyrsa init-pki

init-pki complete; you may now create a CA or requests.
Your newly created PKI dir is: /etc/openvpn/easy-rsa/pki


[root@cjz easy-rsa]# ./easyrsa build-ca
Using SSL: openssl OpenSSL 1.0.2k-fips  26 Jan 2017

Enter New CA Key Passphrase:    #在此要输入ca的密码：（ca.com），需要输入两次。
Re-Enter New CA Key Passphrase:
Generating RSA private key, 2048 bit long modulus
........+++
..+++
e is 65537 (0x10001)
```

原文链接：OpenVPN 集成 LDAP 踩坑记

```
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]:limikeji  #此处要输入组织（Open××× CERTIFICATE AUTHORITY）

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/pki/ca.crt
```

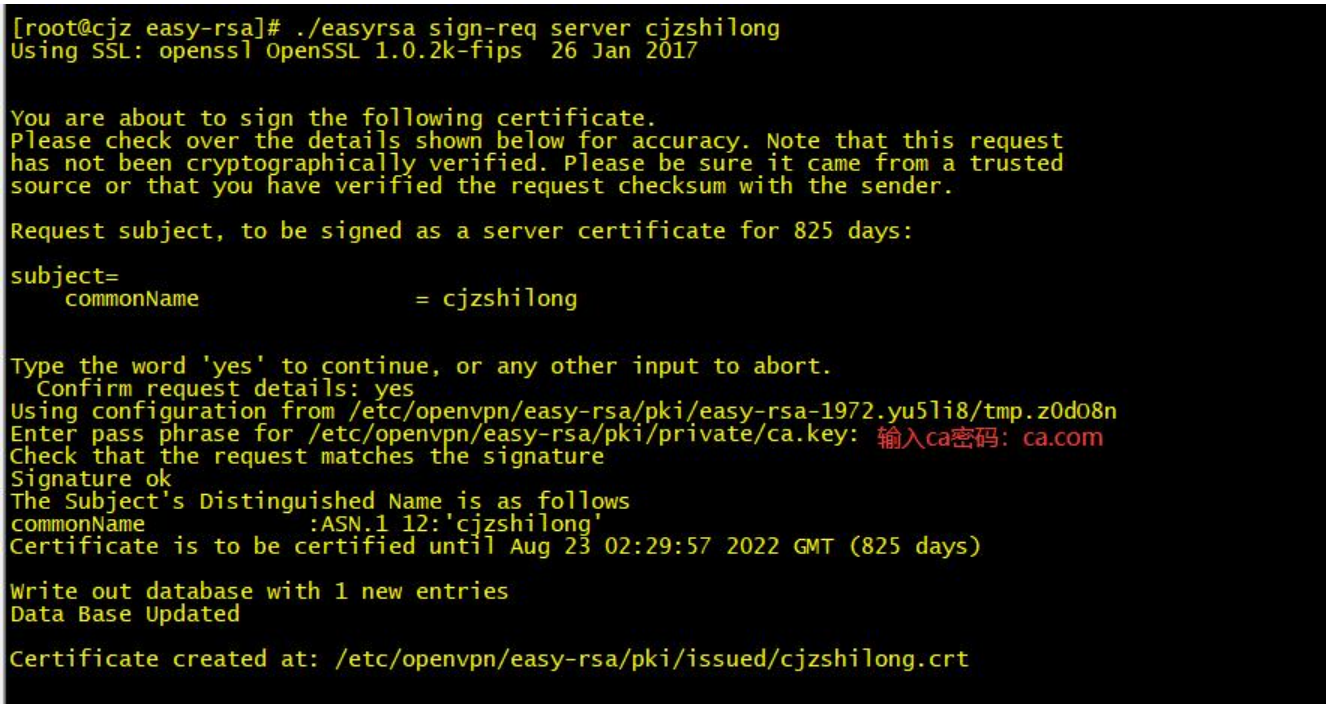
6. **创建服务端证书，生成请求，使用gen-req来生成req**

```
[root@cjz easy-rsa]# ./easyrsa gen-req cjzshilong
Using SSL: openssl OpenSSL 1.0.2k-fips  26 Jan 2017
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to '/etc/openvpn/easy-rsa/pki/easy-rsa-1945.QkcdZs/tmp.plZnLa'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
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) [cjzshilong]:

Keypair and certificate request completed. Your files are:
req: /etc/openvpn/easy-rsa/pki/reqs/cjzshilong.req
key: /etc/openvpn/easy-rsa/pki/private/cjzshilong.key
```

```
[root@cjz easy-rsa]# ./easyrsa gen-req cjzshilong
Using SSL: openssl OpenSSL 1.0.2k-fips  26 Jan 2017
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to '/etc/openvpn/easy-rsa/pki/easy-rsa-1945.QkcdZs/tmp.plZnLa'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase: 输入密码
-----
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) [cjzshilong]: 直接回车

Keypair and certificate request completed. Your files are:
req: /etc/openvpn/easy-rsa/pki/reqs/cjzshilong.req
key: /etc/openvpn/easy-rsa/pki/private/cjzshilong.key
```

7. **签发证书，签约服务端证书**

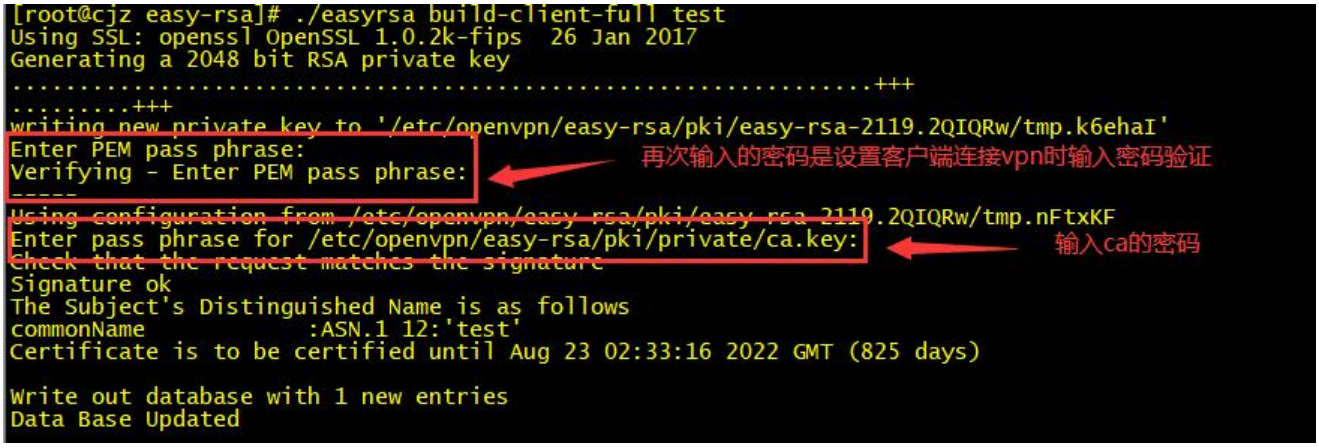
```
[root@cjz easy-rsa]# ./easyrsa sign-req server cjzshilong
Using SSL: openssl OpenSSL 1.0.2k-fips  26 Jan 2017


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 825 days:

subject=
    commonName                = cjzshilong


Type the word 'yes' to continue, or any other input to abort.
  Confirm request details: yes
Using configuration from /etc/openvpn/easy-rsa/pki/easy-rsa-1972.yu5li8/tmp.z0dO8n
Enter pass phrase for /etc/openvpn/easy-rsa/pki/private/ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'cjzshilong'
Certificate is to be certified until Aug 23 02:29:57 2022 GMT (825 days)

Write out database with 1 new entries
Data Base Updated

Certificate created at: /etc/openvpn/easy-rsa/pki/issued/cjzshilong.crt
```




8. **生成Windows客户端test用户**

```
[root@cjz easy-rsa]# ./easyrsa build-client-full test
Using SSL: openssl OpenSSL 1.0.2k-fips  26 Jan 2017
```

```
Generating a 2048 bit RSA private key
.....................................................................+++
.........+++
writing new private key to '/etc/openvpn/easy-rsa/pki/easy-rsa-2119.2QIQRw/tmp.k6ehaI'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
Using configuration from /etc/openvpn/easy-rsa/pki/easy-rsa-2119.2QIQRw/tmp.nFtxKF
Enter pass phrase for /etc/openvpn/easy-rsa/pki/private/ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'test'
Certificate is to be certified until Aug 23 02:33:16 2022 GMT (825 days)

Write out database with 1 new entries
Data Base Updated
```




注：生成客户端用户的时候会提示设置密码，可以直接回车密码为空，也可以输入密码，待客户端连时需要输入密码。

9. **查看客户端证书存放路径：**

```
ls -l /etc/openvpn/easy-rsa/pki/issued/test.crt
ls -l /etc/openvpn/easy-rsa/pki/private/test.key
```

10. **配置sysctl.com文件**

```
vim /etc/sysctl.conf
```

在末尾加入:net.ipv4.ip_forward=1

最后执行：

```
[root@cjz easy-rsa]# sysctl -p
```

11. **配置** /etc/openvpn/server.conf

```
port 1194   #端口：1194
proto udp  #协议使用：UDP
dev tun
ca /etc/openvpn/easy-rsa/pki/ca.crt  #此处配置的是绝对路径
cert /etc/openvpn/easy-rsa/pki/issued/limikeji-sa.crt
key /etc/openvpn/easy-rsa/pki/private/limikeji-sa.key  # This file should be kept secret
```

```
dh /etc/openvpn/easy-rsa/pki/dh.pem
server 10.8.0.0 255.255.255.0   #内网服务器虚拟地址
ifconfig-pool-persist ipp.txt
push "route 172.16.0.0 255.255.0.0"
push "redirect-gateway def1 bypass-dhcp"    #使客户端所有网络通信通过vpn
push "dhcp-option DNS 223.5.5.5"   #配置DNS
push "dhcp-option DNS 114.114.114.114"
keepalive 10 120
tls-auth /etc/openvpn/ta.key 0 # This file is secret
cipher AES-256-CBC
comp-lzo
max-clients 100  # 最大客户端连接数量
user openvpn
group openvpn
persist-key
persist-tun
status openvpn-status.log  # 状态日志
log-append  /var/log/openvpn/openvpn.log  # 开启OpenVpn日志
verb 3
mute 20
explicit-exit-notify 1
```

12. **启动openvpn**

```
systemctl start openvpn@server
```

13. **查看状态：**

```
[root@cjz ~]# ps -aux | grep openvpn
openvpn  11941  0.0  0.1  77636  4940 ?        Ss   May19   0:01 /usr/sbin/openvpn --cd /etc/o
envpn/ --config server.conf
root     12992  0.0  0.0 112708   988 pts/2    S+   10:44   0:00 grep --color=auto openvpn
```

查看安装openvpn后的网卡状态：

```
[root@cjz ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group
efault qlen 1000
    link/ether 00:16:3e:10:39:70 brd ff:ff:ff:ff:ff:ff
    inet 172.16.16.55/24 brd 172.16.16.255 scope global dynamic eth0
       valid_lft 315295137sec preferred_lft 315295137sec
8: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state
NKNOWN group default qlen 100
    link/none
    inet 10.8.0.1 peer 10.8.0.2/32 scope global tun0
       valid_lft forever preferred_lft forever
```

# 客户端安装连接

windows 64 位的openvpn版本为：2.4.9 可以从官网上下载

下载链接：https://openvpn.net/community-downloads/

1. **客户端需要的证书文件：**

tese.crt test.key ca.crt ta.key

2. **创建一个存放客户端证书的文件夹，然后将客户端的证书下载到本地电脑**

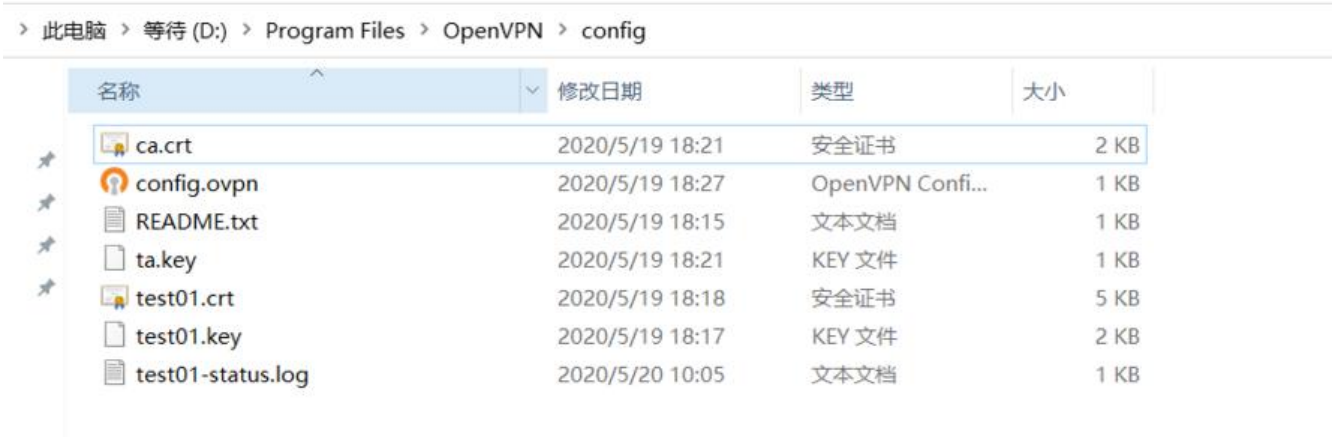
```
[root@cjz ~]# cd /etc/openvpn/client/
[root@cjz client]# ll
total 20
-rw------- 1 root root 1159 May 19 18:22 ca.crt
-rw------- 1 root root  636 May 19 18:22 ta.key
-rw------- 1 root root 4418 May 19 18:22 test.crt
-rw------- 1 root root 1834 May 19 18:22 test.key
```

3. **复制完成后，将客户端正在下载到本地电脑，在此不详细描述。**

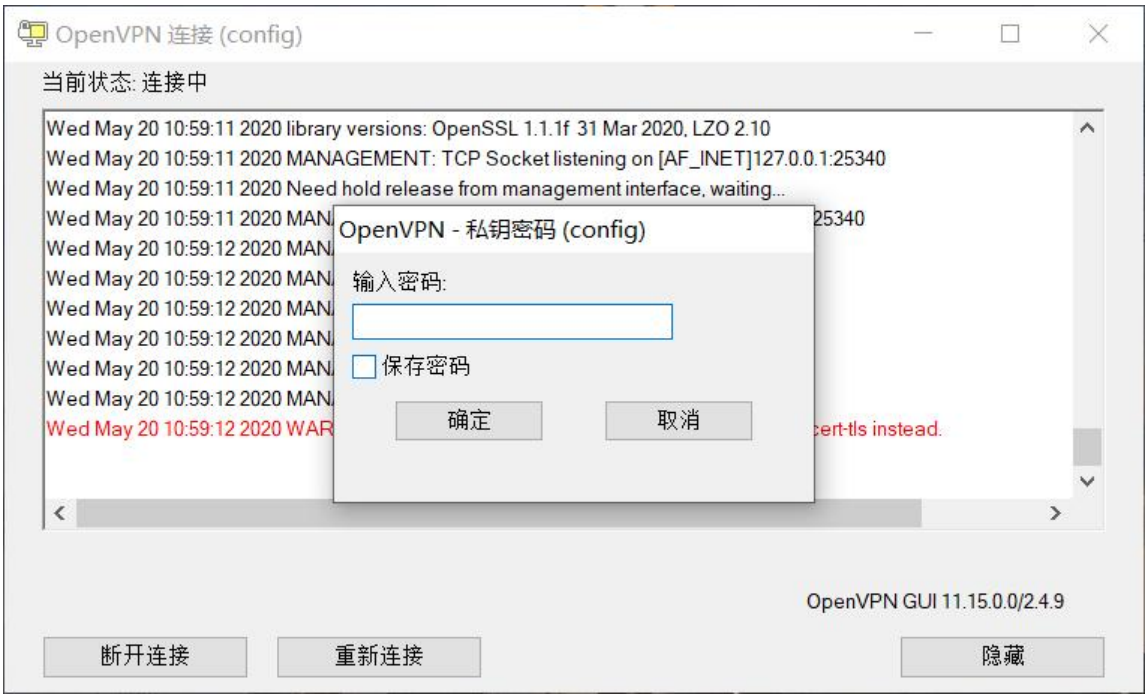
然后需要在本地电脑上创建客户端配置文件：config.ovpn ,具体配置信息如下：

```
client
dev tun
proto udp
resolv-retry infinite
nobind
remote 182.x.x.141 1194 #此处要更换成出口的公网IP地址
ns-cert-type server
comp-lzo
ca ca.crt
cert test01.crt
key test01.key
tls-auth ta.key 1
keepalive 10 120
persist-key
persist-tun
verb 5
redirect-gateway
route-method exe
route-delay 2
status test01-status.log
log-append test01.log
```

安装Openvpn 2.4.9 x86_64后，需要找到客户端安装目录下的config文件夹，清空config文件夹，后将客户端证书和客户端配置文件复制到config文件夹下




原文链接：OpenVPN 集成 LDAP 踩坑记





**直接对标阿里云SSL VPN** **trollface trollface**


# 其他

1. **如果生成证书时输错密码了（如test用户），报出如下错误：**

```
[root@cjz easy-rsa]# ./easyrsa build-client-full test01
Using SSL: openssl OpenSSL 1.0.2k-fips  26 Jan 2017

Easy-RSA error:

Request file already exists. Aborting build to avoid overwriting this file.
If you wish to continue, please use a different name or remove the file.
Matching file found at:  /etc/openvpn/easy-rsa/pki/reqs/test01.req
```

需要删除以为文件后，可继续创建

```
[root@cjz easy-rsa]# rm -f  /etc/openvpn/easy-rsa/pki/reqs/test01.req
[root@cjz easy-rsa]# rm -f  /etc/openvpn/easy-rsa/pki/private/test01.key
```

2. **撤销证书（test为例）**

撤销命令：revoke

```
./easyrsa revoke test
```

原文链接：OpenVPN 集成 LDAP 踩坑记

生成CRL文件（撤销证书的列表）

./easyrsa gen-crl

重启Openvpn服务生效

```
systemctl stop openvpn@server
systemctl start openvpn@server
```

3. **防火墙开放1194端口，阿里云需要在ESC的安全组中添加策略，开放1194端口。要不然映射后也问不了(同时如果为了访问其他网段的机器，需要在专有网络中添加路由)**

4. **如果连接OpenVPN没问题的话，但是访问Internet却不行，这是需要开启虚拟网段进行nat转发**

5.

```
#开启NAT转发
iptables -I FORWARD -j ACCEPT   ###开启所有转发
iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE
```

# OpenVPN集成LDAP

OpenVPN服务端集成的OpenLDAP认证，这样能够使客户端用户在连接VPN时直接使用统一的OpenDAP账号

# 安装openvpn-auth-ldap

yum install openvpn-auth-ldap -y

主要会安装 /usr/lib64/openvpn/plugin/lib/openvpn-auth-ldap.so文件，和生成 /etc/openvpn/auth/ldap.conf文件。

**配置 vim /etc/openvpn/auth/ldap.conf**

```
<LDAP>
   URL         ldap://172.16.16.4:389
   BindDN          cn=manager,dc=limikeji,dc=com
   Password    limikeji.com
   Timeout         15
   TLSEnable    no
   FollowReferrals no
</LDAP>

<Authorization>
   BaseDN          "dc=limikeji,dc=com"
   SearchFilter    "uid=%u"
   RequireGroup    false
   <Group>
      BaseDN         "ou=group,dc=limikeji,dc=com"
      SearchFilter     "cn=chanpinyanfabu"
      MemberAttribute     uniqueMember
   </Group>
</Authorization>
```

注意上面的ldap.conf中如果设置 RequireGroup true以及Group的配置实际我们期望是必须是LDAP

的名称为vpn的组下的用户才可以登录VPN。但根据这个ISSUE，当前2.0.3的openvpn-auth-ldap不持。因此如果只想限制LDAP中某些用户可以使用VPN的话，只能设置 RequireGroup fals，然后可在SearchFilter中做一些文章，比如(&(uid=%u)(ou=vpn))即只有用户的ou字段为(vpn)的才可以。

**配置 /etc/openvpn/server.conf，添加如下：**

```
...
plugin /usr/lib64/openvpn/plugin/lib/openvpn-auth-ldap.so "/etc/openvpn/auth/ldap.conf"
client-cert-not-required
...
```

- 使用了上面安装的openvpn-auth-ldap认证插件
- client-cert-not-requir不再需要客户端证书，将改为使用OpenLDAP中的用户认证

## 客户端配置：

```
client
dev tun
proto udp
resolv-retry infinite
nobind
remote 182.x.x.141 1194 #此处要更换成出口的公网IP地址
ns-cert-type server
comp-lzo
ca ca.crt
;cert test01.crt
;key test01.key
tls-auth ta.key 1
keepalive 10 120
persist-key
persist-tun
verb 5
auth-user-pass
redirect-gateway
route-method exe
route-delay 2
status OpenVpnClient-status.log
log-append test01.log
```

- 上面的配置注释掉了 cert client.crt和 ;key client.key不再需要客户端证书client.crt和秘钥client.key
- ns-cert-type server和 auth-user-pass是新加入的配置开启了用户名密码认证

此时集成LDAP的OpenVPN客户端认证文件目录如下：


原文链接：OpenVPN 集成 LDAP 踩坑记

**配置参考： doge**

1. http://majinlei.com/2018/11/04/Centos7-2-OpenVPN-2-4-4-easy-rsa-3-0-%E6%9C%8D%E%8A%A1%E5%99%A8%E6%90%AD%E5%BB%BA%E6%95%99%E7%A8%8B/
2. https://i4t.com/4481.html
3. https://open.weave.pub/install_openvpn
4. https://blog.frognew.com/2017/09/openvpn-integration-ldap.html

**LDAP配置参考：heart_eyes**

https://github.com/threerings/openvpn-auth-ldap/wiki/Configuration

https://github.com/threerings/openvpn-auth-ldap

**FQA:innocent**

https://forums.openvpn.net/viewtopic.php?t=2156