OPENVPN Server Installation and configuration Guide

OpenVPN is opensource SSL VPN solution. It encrypts all the network traffic and creates a tunnel between server and the client.

OpenVPN Installation On Ubuntu

1. Download OpenVPN shell script using below link

Unset

```
wget https://git.io/vpn -O openvpn-install.sh
```

2. After Downloading the script give execute permission to the script

Unset

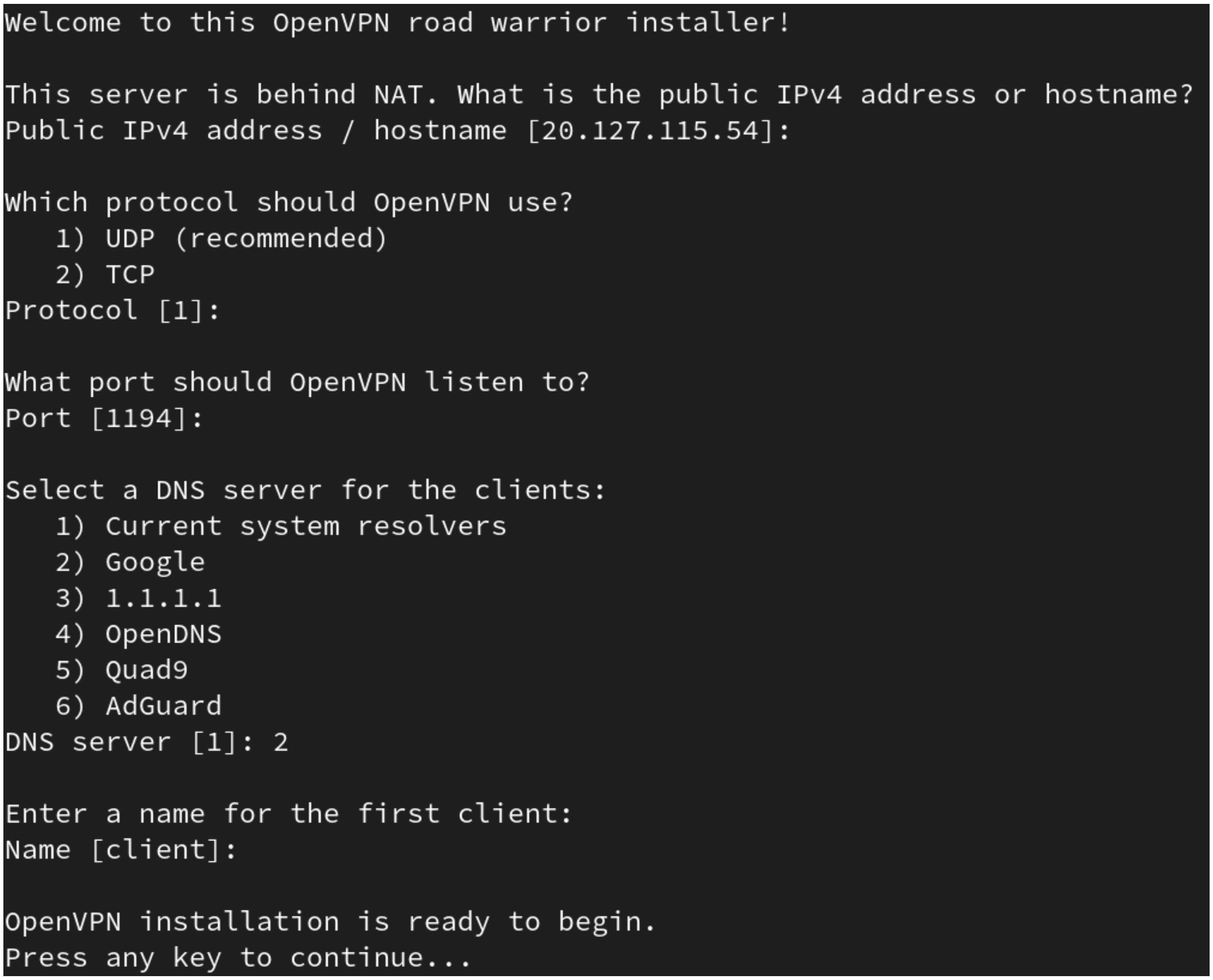
```
chmod +x openvpn-install.sh
```

3. Now execute the shell script to install OpenVPN server

Unset

```
./openvpn-install.sh
```

4. We need to fill up necessary arguments it will ask while installing and we need to choose respective values



```
Welcome to this OpenVPN road warrior installer!

This server is behind NAT. What is the public IPv4 address or hostname?
Public IPv4 address / hostname [20.127.115.54]:

Which protocol should OpenVPN use?
   1) UDP (recommended)
   2) TCP
Protocol [1]:

What port should OpenVPN listen to?
Port [1194]:

Select a DNS server for the clients:
   1) Current system resolvers
   2) Google
   3) 1.1.1.1
   4) OpenDNS
   5) Quad9
   6) AdGuard
DNS server [1]: 2

Enter a name for the first client:
Name [client]:

OpenVPN installation is ready to begin.
Press any key to continue...
```

5. Now install OpenVPN Authentication Module

Unset

```
apt-get install openvpn-auth-ldap
```

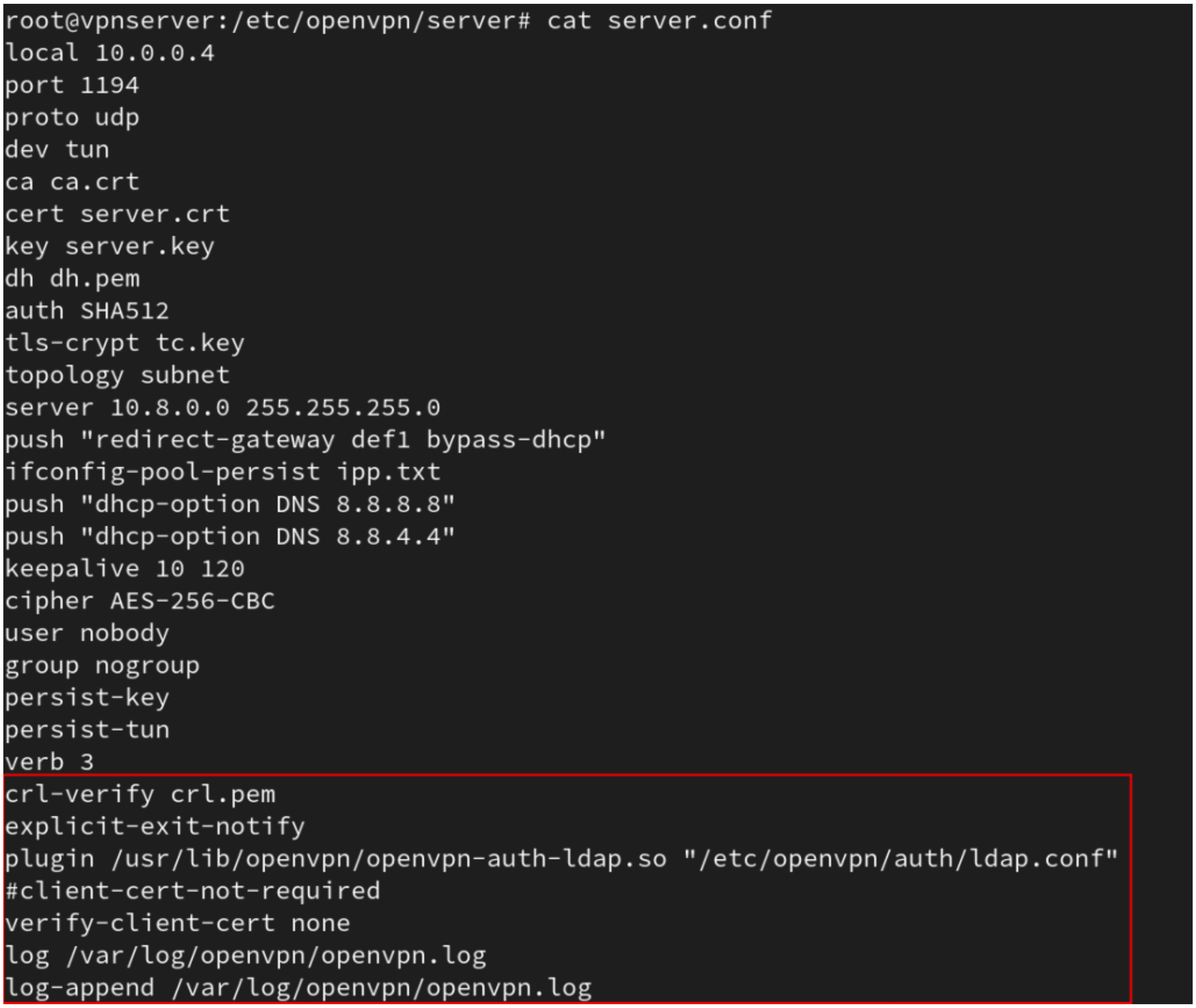
6. Now open file /etc/openvpn/server/server.conf and make below changes to the file.

Unset

```
local 172.31.45.56

port 1194
```

```
proto udp

dev tun

ca ca.crt

cert server.crt

key server.key

dh dh.pem

auth SHA512

tls-crypt tc.key

topology subnet

server 10.8.0.0 255.255.255.0

push "redirect-gateway def1 bypass-dhcp"

ifconfig-pool-persist ipp.txt

push "dhcp-option DNS 8.8.8.8"

push "dhcp-option DNS 8.8.4.4"

keepalive 10 120

cipher AES-256-CBC

user nobody

group nogroup

persist-key

persist-tun
```

```
verb 3

crl-verify crl.pem

explicit-exit-notify

plugin /usr/lib/openvpn/openvpn-auth-ldap.so "/etc/openvpn/auth/ldap.conf"

#client-cert-not-required

verify-client-cert none

log /var/log/openvpn/openvpn.log

log-append /var/log/openvpn/openvpn.log
```



```
root@vpnserver:/etc/openvpn/server# cat server.conf
local 10.0.0.4
port 1194
proto udp
dev tun
ca ca.crt
cert server.crt
key server.key
dh dh.pem
auth SHA512
tls-crypt tc.key
topology subnet
server 10.8.0.0 255.255.255.0
push "redirect-gateway def1 bypass-dhcp"
ifconfig-pool-persist ipp.txt
push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 8.8.4.4"
keepalive 10 120
cipher AES-256-CBC
user nobody
group nogroup
persist-key
persist-tun
verb 3
crl-verify crl.pem
explicit-exit-notify
plugin /usr/lib/openvpn/openvpn-auth-ldap.so "/etc/openvpn/auth/ldap.conf"
#client-cert-not-required
verify-client-cert none
log /var/log/openvpn/openvpn.log
log-append /var/log/openvpn/openvpn.log
```

Also, make sure that plugin /usr/lib/openvpn/openvpn-auth-ldap.so is present. if not then find that file openvpn-auth-ldap.so and copy paste that file into /usr/lib/openvpn/ directory

Unset

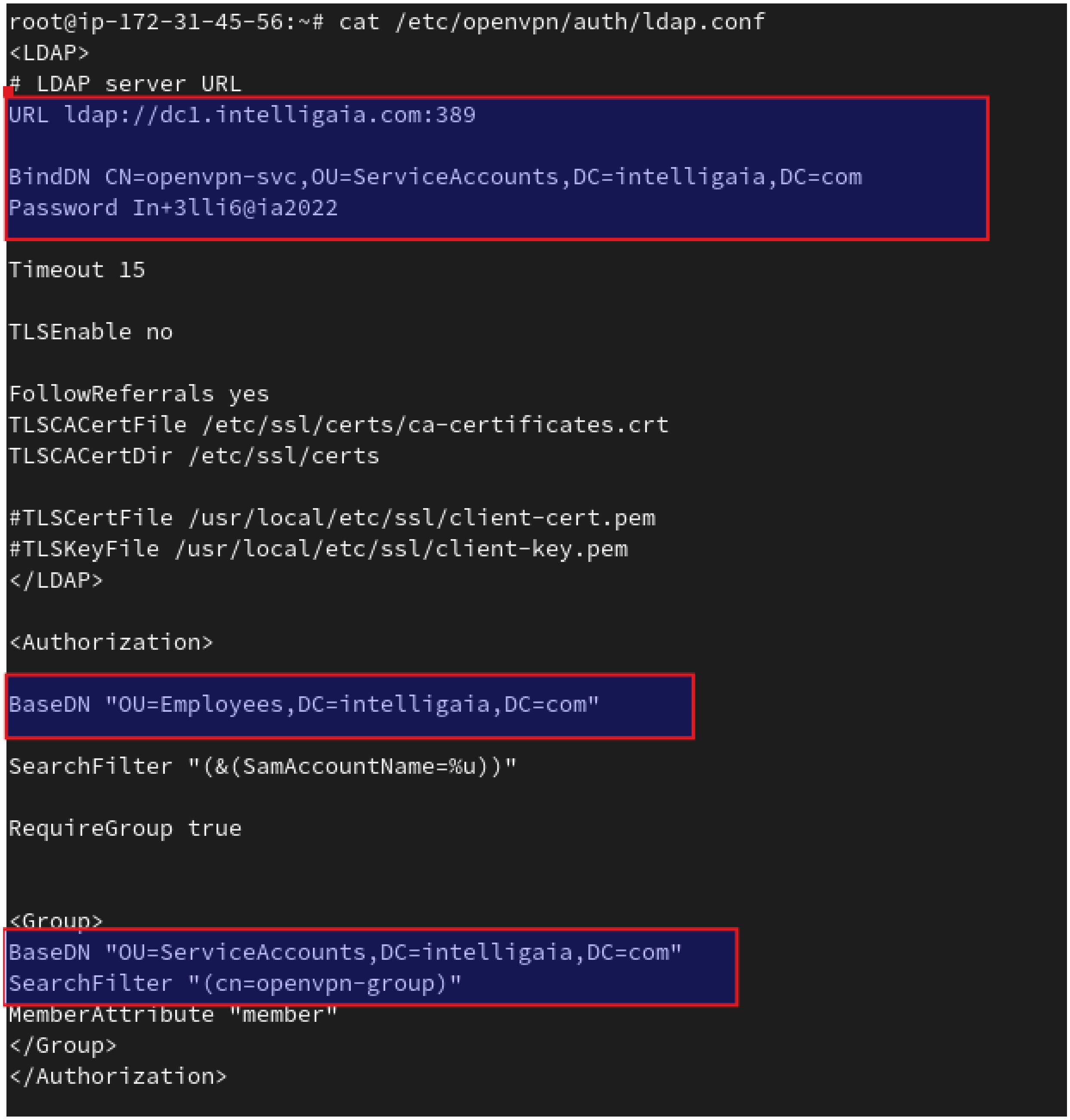
```
ls /usr/lib/openvpn/openvpn-auth-ldap.so
find / -type f -name openvpn-auth-ldap.so
```

7. Verify that the file /etc/openvpn/auth/ldap.conf is present. if not then create this file as below

Unset

```
<LDAP>
# LDAP server URL
URL ldap://dc1.intelligaia.com:389

BindDN
CN=openvpn-svc,OU=ServiceAccounts,DC=intelligaia,DC=com
Password In+3lli6@ia2022

Timeout 15

TLSEnable no

FollowReferrals yes
TLSCACertFile /etc/ssl/certs/ca-certificates.crt
TLSCACertDir /etc/ssl/certs

#TLSCertFile /usr/local/etc/ssl/client-cert.pem
#TLSKeyFile /usr/local/etc/ssl/client-key.pem
</LDAP>

<Authorization>

BaseDN "OU=Employees,DC=intelligaia,DC=com"

SearchFilter "(&(SamAccountName=%u))"

RequireGroup true


<Group>
BaseDN "OU=ServiceAccounts,DC=intelligaia,DC=com"
SearchFilter "(cn=openvpn-group)"
MemberAttribute "member"
</Group>
```

```
</Authorization>
```



```
root@ip-172-31-45-56:~# cat /etc/openvpn/auth/ldap.conf
<LDAP>
# LDAP server URL
URL ldap://dc1.intelligaia.com:389

BindDN CN=openvpn-svc,OU=ServiceAccounts,DC=intelligaia,DC=com
Password In+3lli6@ia2022

Timeout 15

TLSEnable no

FollowReferrals yes
TLSCACertFile /etc/ssl/certs/ca-certificates.crt
TLSCACertDir /etc/ssl/certs

#TLSCertFile /usr/local/etc/ssl/client-cert.pem
#TLSKeyFile /usr/local/etc/ssl/client-key.pem
</LDAP>

<Authorization>

BaseDN "OU=Employees,DC=intelligaia,DC=com"

SearchFilter "(&(SamAccountName=%u))"

RequireGroup true


<Group>
BaseDN "OU=ServiceAccounts,DC=intelligaia,DC=com"
SearchFilter "(cn=openvpn-group)"
MemberAttribute "member"
</Group>
</Authorization>
```

Unset

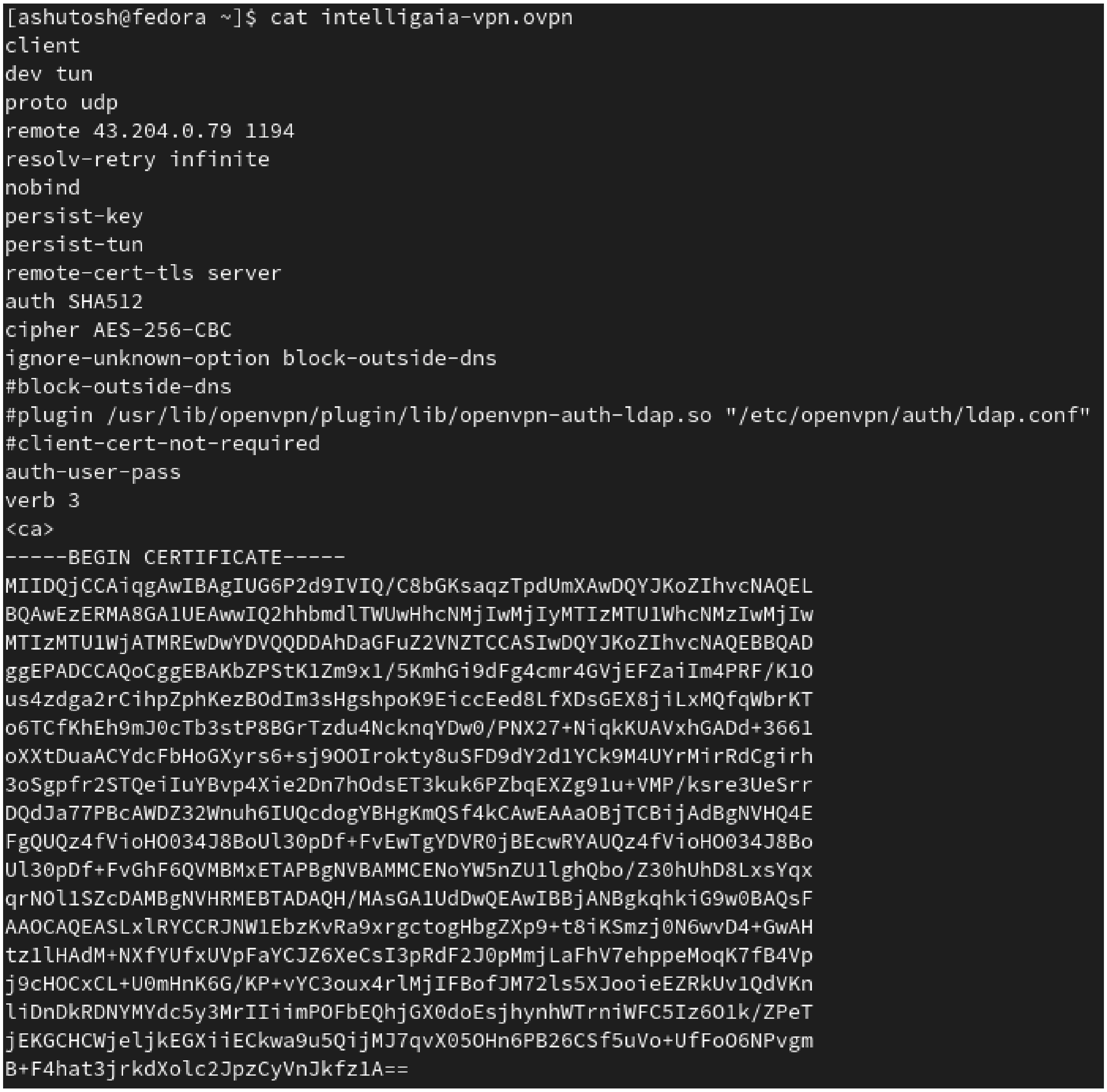
```
Note: DC Name : intelligaia.com
       Service Account name : openvpn-svc
       Openvpn Groupd  : openvpn-group
```

8. Now open the intelligaia-vpn.ovpn file or .ovpn file that we got in the first step and make few changes(Add ldap-auth) in that file and then use that file for connecting the VPN.

Note: Do not share this intelligaia-vpn.ovpn file with anybody outside the organisation

Unset

```
#block-outside-dns
auth-user-pass
```



```
[ashutosh@fedora ~]$ cat intelligaia-vpn.ovpn
client
dev tun
proto udp
remote 43.204.0.79 1194
resolv-retry infinite
nobind
persist-key
persist-tun
remote-cert-tls server
auth SHA512
cipher AES-256-CBC
ignore-unknown-option block-outside-dns
#block-outside-dns
#plugin /usr/lib/openvpn/plugin/lib/openvpn-auth-ldap.so "/etc/openvpn/auth/ldap.conf"
#client-cert-not-required
auth-user-pass
verb 3
<ca>
-----BEGIN CERTIFICATE-----
MIIDQjCCAiqgAwIBAgIUG6P2d9IVIQ/C8bGKsaqzTpdUmXAwDQYJKoZIhvcNAQEL
BQAwEzERMA8GA1UEAwwIQ2hhbmdlTWUwHhcNMjIwMjIyMTIzMTU1WhcNMzIwMjIw
MTIzMTU1WjATMREwDwYDVQQDDAhDaGFuZ2VNZTCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAKbZPStK1Zm9x1/5KmhGi9dFg4cmr4GVjEFZaiIm4PRF/K1O
us4zdga2rCihpZphKezBOdIm3sHgshpoK9EiccEed8LfXDsGEX8jiLxMQfqWbrKT
o6TCfKhEh9mJ0cTb3stP8BGrTzdu4NcknqYDw0/PNX27+NiqkKUAVxhGADd+3661
oXXtDuaACYdcFbHoGXyrs6+sj9OOIrokty8uSFD9dY2d1YCk9M4UYrMirRdCgirh
3oSgpfr2STQeiIuYBvp4Xie2Dn7hOdsET3kuk6PZbqEXZg91u+VMP/ksre3UeSrr
DQdJa77PBcAWDZ32Wnuh6IUQcdogYBHgKmQSf4kCAwEAAaOBjTCBijAdBgNVHQ4E
FgQUQz4fVioHO034J8BoUl30pDf+FvEwTgYDVR0jBEcwRYAUQz4fVioHO034J8Bo
Ul30pDf+FvGhF6QVMBMxETAPBgNVBAMMCENoYW5nZU1lghQbo/Z30hUhD8LxsYqx
qrNOl1SZcDAMBgNVHRMEBTADAQH/MAsGA1UdDwQEAwIBBjANBgkqhkiG9w0BAQsF
AAOCAQEASLxlRYCCRJNW1EbzKvRa9xrgctogHbgZXp9+t8iKSmzj0N6wvD4+GwAH
tz1lHAdM+NXfYUfxUVpFaYCJZ6XeCsI3pRdF2J0pMmjLaFhV7ehppeMoqK7fB4Vp
j9cHOCxCL+U0mHnK6G/KP+vYC3oux4rlMjIFBofJM72ls5XJooieEZRkUv1QdVKn
liDnDkRDNYMYdc5y3MrIIiimPOFbEQhjGX0doEsjhynhWTrniWFC5Iz6O1k/ZPeT
jEKGCHCWjeljkEGXiiECkwa9u5QijMJ7qvX05OHn6PB26CSf5uVo+UfFoO6NPvgm
B+F4hat3jrkdXolc2JpzCyVnJkfz1A==
```

9. Now, restart the openvpn service and see if you get any errors. if you don’t get any errors then telnet and see if you're able to telnet port 389

```
Unset
systemctl restart openvpn-server@server.service
telnet dc1.intelligaia.com 389
```

The Openvpn server is installed and configured with Active directory successfully