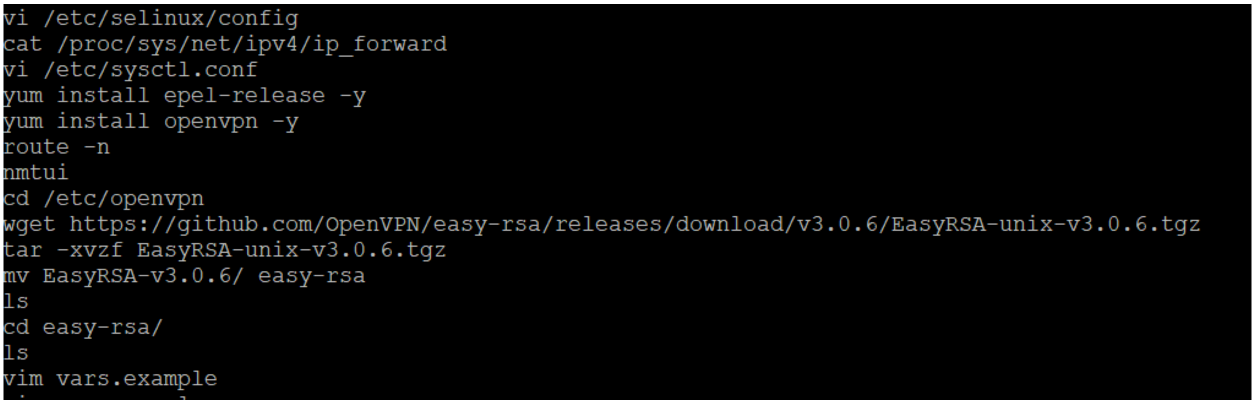
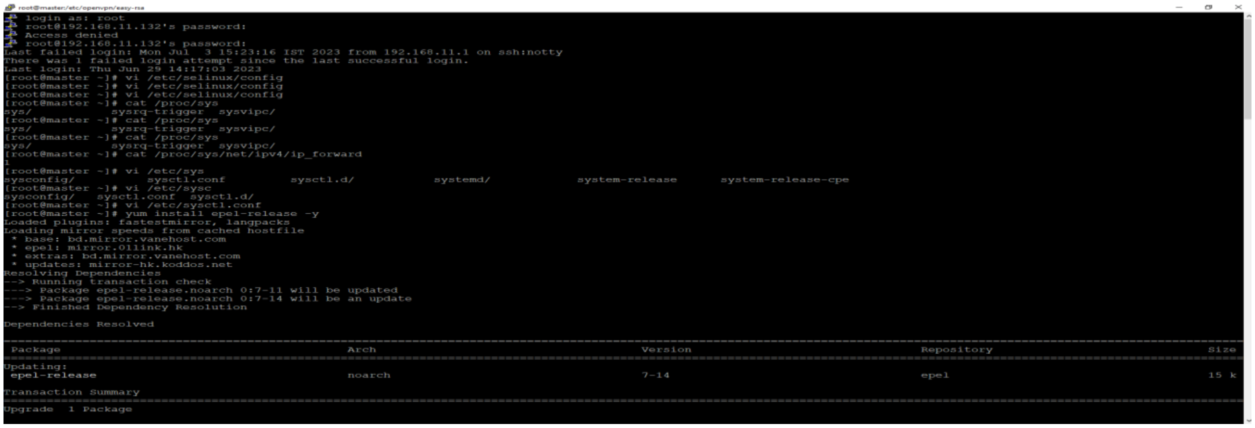
Q2)..openvpn configure…

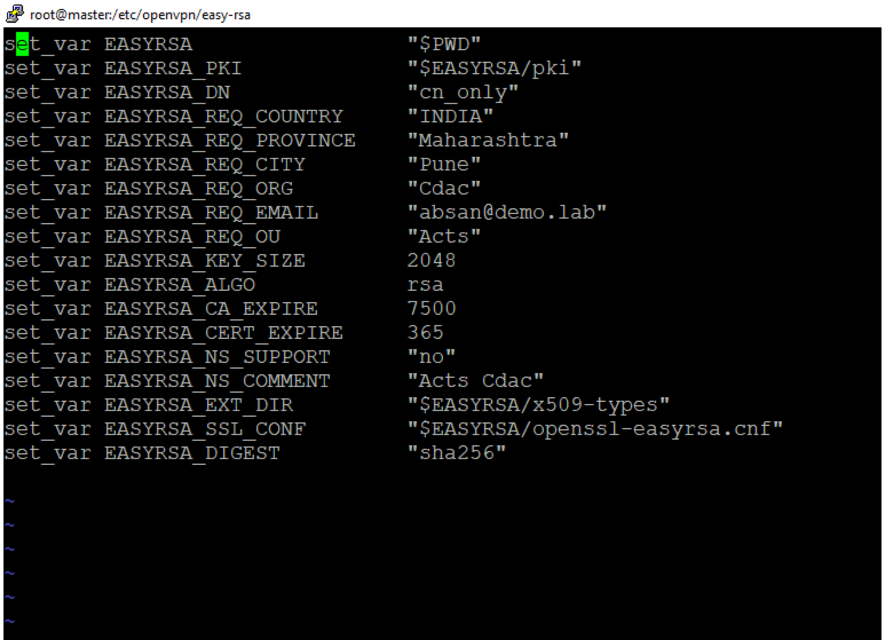


```
vi /etc/selinux/config
cat /proc/sys/net/ipv4/ip_forward
vi /etc/sysctl.conf
yum install epel-release -y
yum install openvpn -y
route -n
nmtui
cd /etc/openvpn
wget https://github.com/OpenVPN/easy-rsa/releases/download/v3.0.6/EasyRSA-unix-v3.0.6.tgz
tar -xvzf EasyRSA-unix-v3.0.6.tgz
mv EasyRSA-v3.0.6/ easy-rsa
ls
cd easy-rsa/
ls
vim vars.example
```

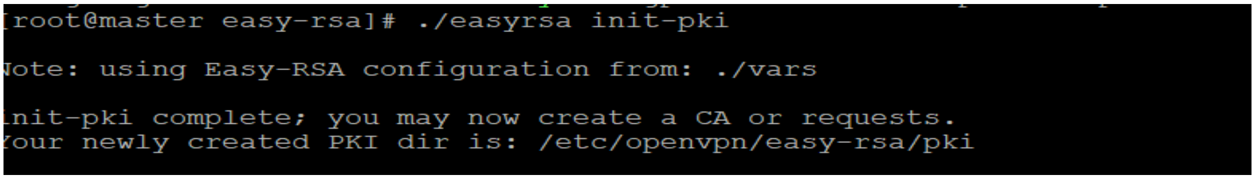


```
 login as: root
 root@192.168.11.132's password:
 Access denied
 root@192.168.11.132's password:
Last failed login: Mon Jul  3 15:23:16 IST 2023 from 192.168.11.1 on ssh:notty
There was 1 failed login attempt since the last successful login.
Last login: Thu Jun 29 14:17:03 2023
[root@master ~]# vi /etc/selinux/config
[root@master ~]# vi /etc/selinux/config
[root@master ~]# vi /etc/selinux/config
[root@master ~]# cat /proc/sys
sys/           sysrq-trigger  sysvipc/
[root@master ~]# cat /proc/sys
sys/           sysrq-trigger  sysvipc/
[root@master ~]# cat /proc/sys
sys/           sysrq-trigger  sysvipc/
[root@master ~]# cat /proc/sys/net/ipv4/ip_forward
1
[root@master ~]# vi /etc/sys
sysconfig/          sysctl.conf         sysctl.d/           systemd/            system-release      system-release-cpe
[root@master ~]# vi /etc/sysc
sysconfig/   sysctl.conf  sysctl.d/
[root@master ~]# vi /etc/sysctl.conf
[root@master ~]# yum install epel-release -y
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: bd.mirror.vanehost.com
 * epel: mirror.01link.hk
 * extras: bd.mirror.vanehost.com
 * updates: mirror-hk.koddos.net
Resolving Dependencies
--> Running transaction check
---> Package epel-release.noarch 0:7-11 will be updated
---> Package epel-release.noarch 0:7-14 will be an update
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================================================================
 Package                         Arch                         Version                          Repository                  Size
================================================================================================================================
Updating:
 epel-release                    noarch                       7-14                             epel                        15 k

Transaction Summary
================================================================================================================================
Upgrade  1 Package
```

Add cerificate details

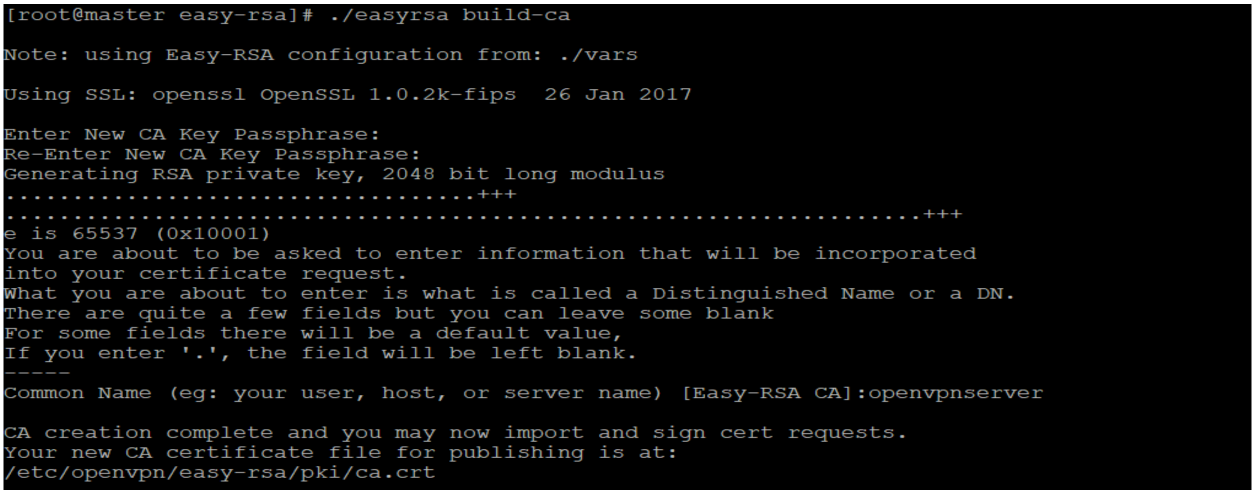


```
set_var EASYRSA                 "$PWD"
set_var EASYRSA_PKI             "$EASYRSA/pki"
set_var EASYRSA_DN              "cn_only"
set_var EASYRSA_REQ_COUNTRY     "INDIA"
set_var EASYRSA_REQ_PROVINCE    "Maharashtra"
set_var EASYRSA_REQ_CITY        "Pune"
set_var EASYRSA_REQ_ORG         "Cdac"
set_var EASYRSA_REQ_EMAIL       "absan@demo.lab"
set_var EASYRSA_REQ_OU          "Acts"
set_var EASYRSA_KEY_SIZE        2048
set_var EASYRSA_ALGO            rsa
set_var EASYRSA_CA_EXPIRE       7500
set_var EASYRSA_CERT_EXPIRE     365
set_var EASYRSA_NS_SUPPORT      "no"
set_var EASYRSA_NS_COMMENT      "Acts Cdac"
set_var EASYRSA_EXT_DIR         "$EASYRSA/x509-types"
set_var EASYRSA_SSL_CONF        "$EASYRSA/openssl-easyrsa.cnf"
set_var EASYRSA_DIGEST          "sha256"

~
~
~
~
~
~
```



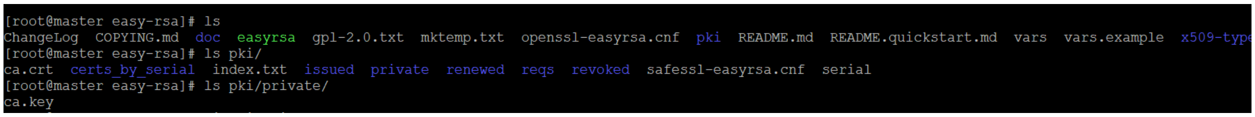
```
[root@master easy-rsa]# ./easyrsa init-pki

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/pki
```

Run Below command and enter the Password and Common Name



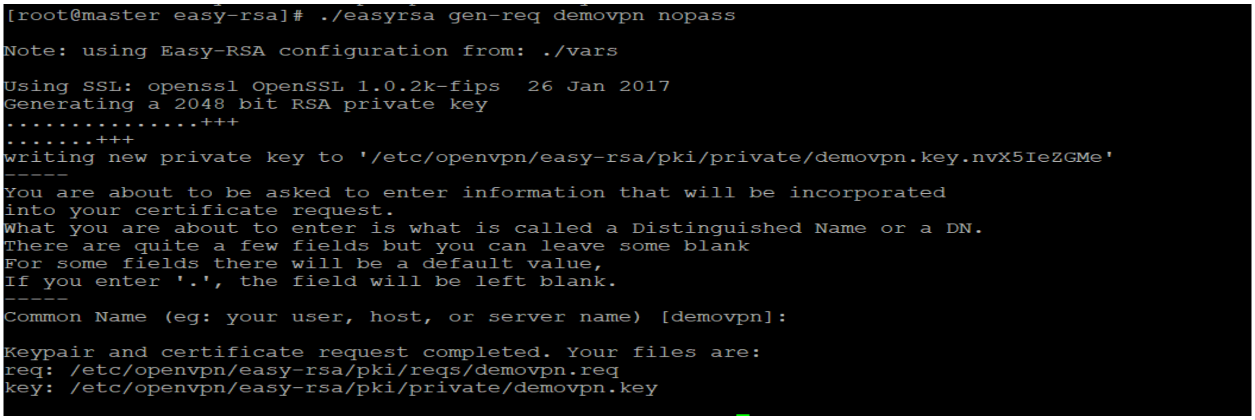
```
[root@master easy-rsa]# ./easyrsa build-ca

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

Using SSL: openssl OpenSSL 1.0.2k-fips  26 Jan 2017

Enter New CA Key Passphrase:
Re-Enter New CA Key Passphrase:
Generating RSA private key, 2048 bit long modulus
...................................+++
.....................................................................+++
e is 65537 (0x10001)
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]:openvpnserver

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
```

Now Check PVT key and Public key is generate, public key- ca.crt and Pvt key- ca.key

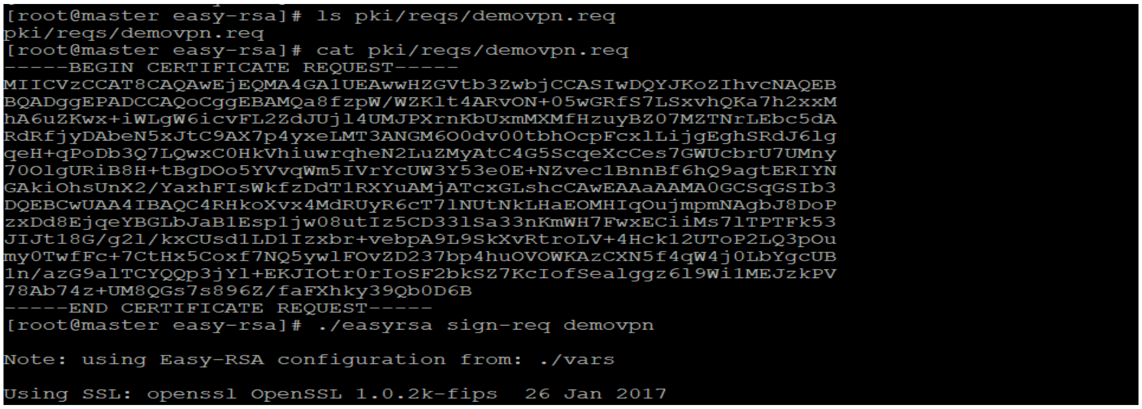


```
[root@master easy-rsa]# ls
ChangeLog  COPYING.md  doc  easyrsa  gpl-2.0.txt  mktemp.txt  openssl-easyrsa.cnf  pki  README.md  README.quickstart.md  vars  vars.example  x509-type
[root@master easy-rsa]# ls pki/
ca.crt  certs_by_serial  index.txt  issued  private  renewed  reqs  revoked  safessl-easyrsa.cnf  serial
[root@master easy-rsa]# ls pki/private/
ca.key
```

Now generate certificate for server ,give name as demovpn and then Enter while Asking For common Name

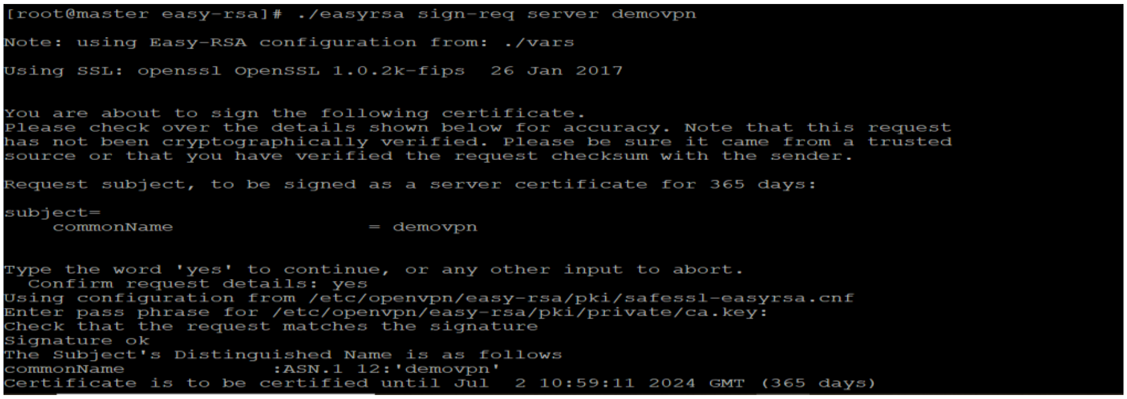


```
[root@master easy-rsa]# ./easyrsa gen-req demovpn nopass

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

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/private/demovpn.key.nvX5IeZGMe'
-----
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) [demovpn]:

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

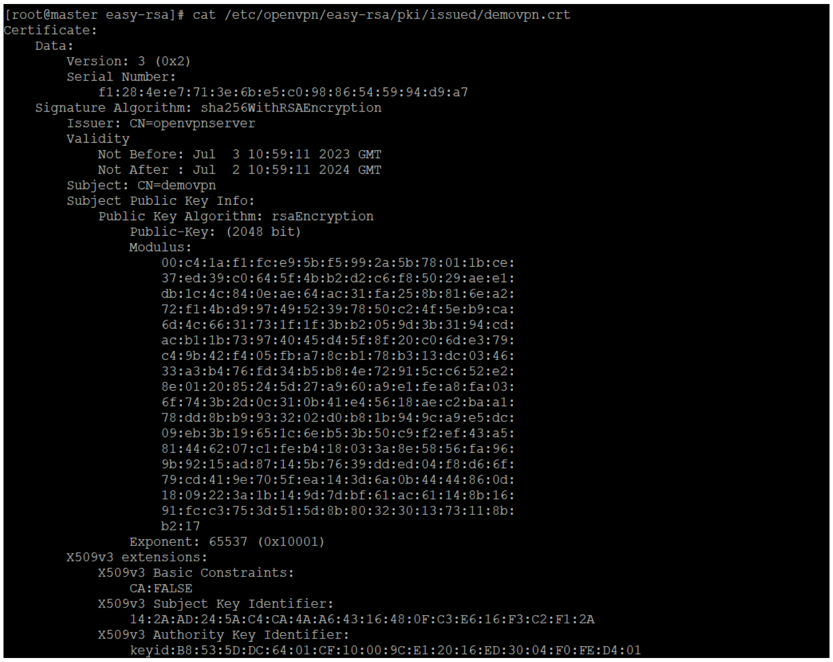


```
[root@master easy-rsa]# ls pki/reqs/demovpn.req
pki/reqs/demovpn.req
[root@master easy-rsa]# cat pki/reqs/demovpn.req
-----BEGIN CERTIFICATE REQUEST-----
MIICVzCCAT8CAQAwEjEQMA4GA1UEAwwHZGVtb3ZwbjCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBAMQa8fzpW/WZKlt4ARvON+05wGRfS7LSxvhQKa7h2xxM
hA6uZKwx+iWLgW6icvFL2ZdJUjl4UMJPXrnKbUxmMXMfHzuyBZ07MZTNrLEbc5dA
RdRfjyDAbeN5xJtC9AX7p4yxeLMT3ANGM6O0dv00tbhOcpFcxlLijgEghSRdJ6lg
qeH+qPoDb3Q7LQwxC0HkVhiuwrqheN2LuZMyAtC4G5ScqeXcCes7GWUcbrU7UMny
70OlgURiB8H+tBgDOo5YVvqWm5IVrYcUW3Y53e0E+NZvec1BnnBf6hQ9agtERIYN
GAkiOhsUnX2/YaxhFIsWkfzDdT1RXYuAMjATcxGLshcCAwEAAaAAMA0GCSqGSIb3
DQEBCwUAA4IBAQC4RHkoXvx4MdRUyR6cT7lNUtNkLHaEOMHIqOujmpmNAgbJ8DoP
zxDd8EjqeYBGLbJaB1Esp1jw08utIz5CD33lSa33nKmWH7FwxECiiMs7lTPTFk53
JIJt18G/g2l/kxCUsd1LD1Izxbr+vebpA9L9SkXvRtroLV+4Hck12UToP2LQ3pOu
my0TwfFc+7CtHx5Coxf7NQ5ywlFOvZD237bp4huOVOWKAzCXN5f4qW4j0LbYgcUB
1n/azG9alTCYQQp3jYl+EKJIOtr0rIoSF2bkSZ7KcIofSealggz6l9Wi1MEJzkPV
78Ab74z+UM8QGs7s896Z/faFXhky39Qb0D6B
-----END CERTIFICATE REQUEST-----
[root@master easy-rsa]# ./easyrsa sign-req demovpn

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

Using SSL: openssl OpenSSL 1.0.2k-fips  26 Jan 2017
```

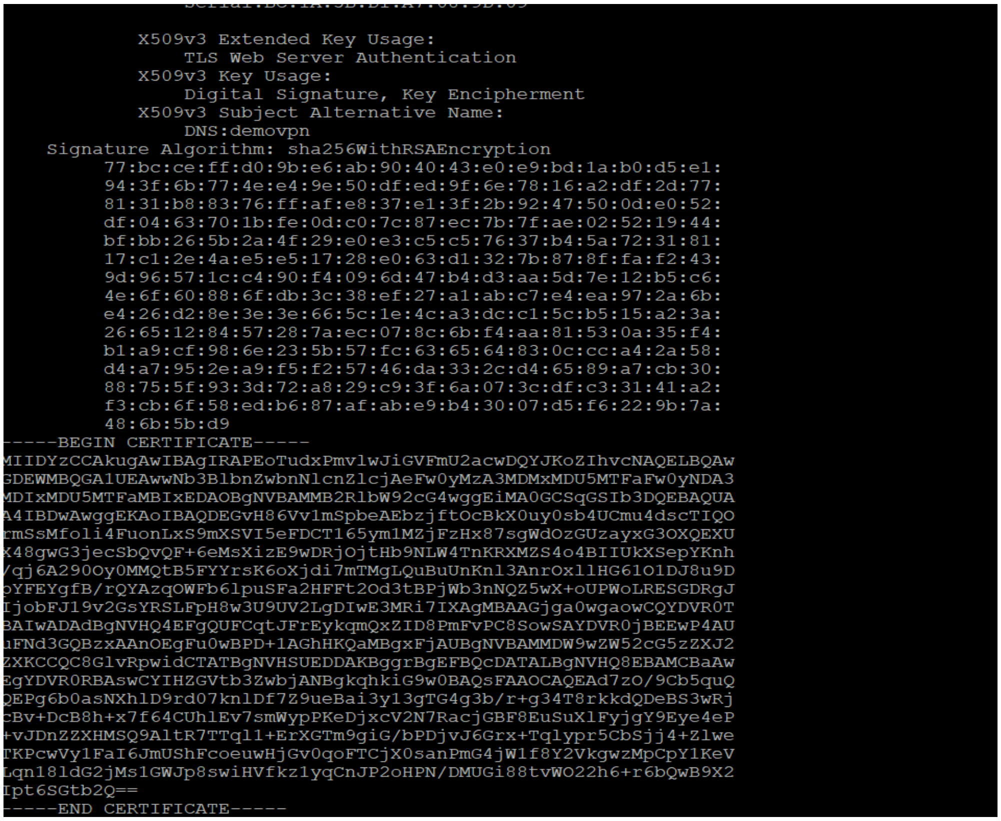
Sign the Server Key Using CA



```
[root@master easy-rsa]# ./easyrsa sign-req server demovpn

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

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 365 days:

subject=
    commonName                = demovpn


Type the word 'yes' to continue, or any other input to abort.
  Confirm request details: yes
Using configuration from /etc/openvpn/easy-rsa/pki/safessl-easyrsa.cnf
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:'demovpn'
Certificate is to be certified until Jul  2 10:59:11 2024 GMT (365 days)
```

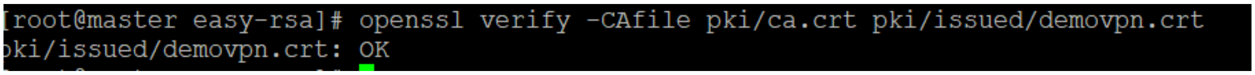


```
[root@master easy-rsa]# cat /etc/openvpn/easy-rsa/pki/issued/demovpn.crt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            f1:28:4e:e7:71:3e:6b:e5:c0:98:86:54:59:94:d9:a7
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=openvpnserver
        Validity
            Not Before: Jul  3 10:59:11 2023 GMT
            Not After : Jul  2 10:59:11 2024 GMT
        Subject: CN=demovpn
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c4:1a:f1:fc:e9:5b:f5:99:2a:5b:78:01:1b:ce:
                    37:ed:39:c0:64:5f:4b:b2:d2:c6:f8:50:29:ae:e1:
                    db:1c:4c:84:0e:ae:64:ac:31:fa:25:8b:81:6e:a2:
                    72:f1:4b:d9:97:49:52:39:78:50:c2:4f:5e:b9:ca:
                    6d:4c:66:31:73:1f:1f:3b:b2:05:9d:3b:31:94:cd:
                    ac:b1:1b:73:97:40:45:d4:5f:8f:20:c0:6d:e3:79:
                    c4:9b:42:f4:05:fb:a7:8c:b1:78:b3:13:dc:03:46:
                    33:a3:b4:76:fd:34:b5:b8:4e:72:91:5c:c6:52:e2:
                    8e:01:20:85:24:5d:27:a9:60:a9:e1:fe:a8:fa:03:
                    6f:74:3b:2d:0c:31:0b:41:e4:56:18:ae:c2:ba:a1:
                    78:dd:8b:b9:93:32:02:d0:b8:1b:94:9c:a9:e5:dc:
                    09:eb:3b:19:65:1c:6e:b5:3b:50:c9:f2:ef:43:a5:
                    81:44:62:07:c1:fe:b4:18:03:3a:8e:58:56:fa:96:
                    9b:92:15:ad:87:14:5b:76:39:dd:ed:04:f8:d6:6f:
                    79:cd:41:9e:70:5f:ea:14:3d:6a:0b:44:44:86:0d:
                    18:09:22:3a:1b:14:9d:7d:bf:61:ac:61:14:8b:16:
                    91:fc:c3:75:3d:51:5d:8b:80:32:30:13:73:11:8b:
                    b2:17
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Subject Key Identifier:
                14:2A:AD:24:5A:C4:CA:4A:A6:43:16:48:0F:C3:E6:16:F3:C2:F1:2A
            X509v3 Authority Key Identifier:
                keyid:B8:53:5D:DC:64:01:CF:10:00:9C:E1:20:16:ED:30:04:F0:FE:D4:01
```



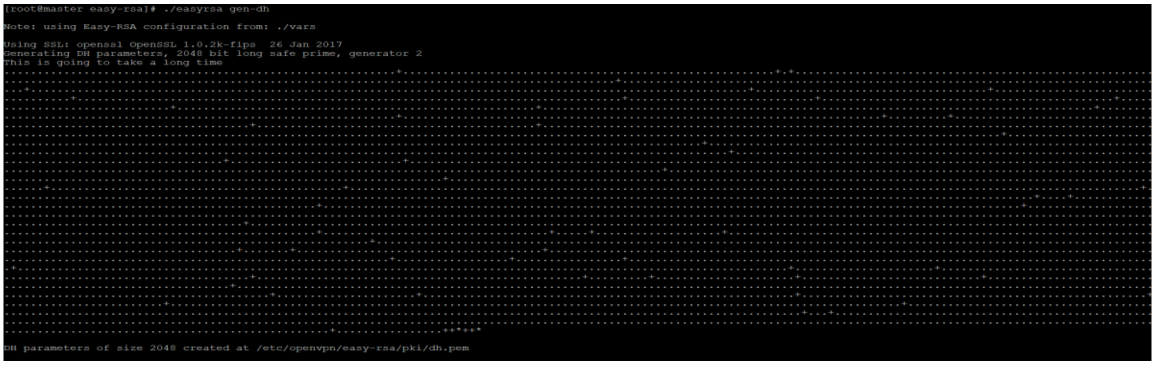
```
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Key Usage:
                Digital Signature, Key Encipherment
            X509v3 Subject Alternative Name:
                DNS:demovpn
    Signature Algorithm: sha256WithRSAEncryption
         77:bc:ce:ff:d0:9b:e6:ab:90:40:43:e0:e9:bd:1a:b0:d5:e1:
         94:3f:6b:77:4e:e4:9e:50:df:ed:9f:6e:78:16:a2:df:2d:77:
         81:31:b8:83:76:ff:af:e8:37:e1:3f:2b:92:47:50:0d:e0:52:
         df:04:63:70:1b:fe:0d:c0:7c:87:ec:7b:7f:ae:02:52:19:44:
         bf:bb:26:5b:2a:4f:29:e0:e3:c5:c5:76:37:b4:5a:72:31:81:
         17:c1:2e:4a:e5:e5:17:28:e0:63:d1:32:7b:87:8f:fa:f2:43:
         9d:96:57:1c:c4:90:f4:09:6d:47:b4:d3:aa:5d:7e:12:b5:c6:
         4e:6f:60:88:6f:db:3c:38:ef:27:a1:ab:c7:e4:ea:97:2a:6b:
         e4:26:d2:8e:3e:3e:66:5c:1e:4c:a3:dc:c1:5c:b5:15:a2:3a:
         26:65:12:84:57:28:7a:ec:07:8c:6b:f4:aa:81:53:0a:35:f4:
         b1:a9:cf:98:6e:23:5b:57:fc:63:65:64:83:0c:cc:a4:2a:58:
         d4:a7:95:2e:a9:f5:f2:57:46:da:33:2c:d4:65:89:a7:cb:30:
         88:75:5f:93:3d:72:a8:29:c9:3f:6a:07:3c:df:c3:31:41:a2:
         f3:cb:6f:58:ed:b6:87:af:ab:e9:b4:30:07:d5:f6:22:9b:7a:
         48:6b:5b:d9
-----BEGIN CERTIFICATE-----
MIIDYzCCAkugAwIBAgIRAPEoTudxPmvlwJiGVFmU2acwDQYJKoZIhvcNAQELBQAw
GDEWMBQGA1UEAwwNb3BlbnZwbnNlcnZlcjAeFw0yMzA3MDMxMDU5MTFaFw0yNDA3
MDIxMDU5MTFaMBIxEDAOBgNVBAMMB2RlbW92cG4wggEiMA0GCSqGSIb3DQEBAQUA
A4IBDwAwggEKAoIBAQDEGvH86Vv1mSpbeAEbzjftOcBkX0uy0sb4UCmu4dscTIQO
rmSsMfoli4FuonLxS9mXSVI5eFDCT165ym1MZjFzHx87sgWdOzGUzayxG3OXQEXU
X48gwG3jecSbQvQF+6eMsXizE9wDRjOjtHb9NLW4TnKRXMZS4o4BIIUkXSepYKnh
/qj6A29OOy0MMQtB5FYYrsK6oXjdi7mTMgLQuBuUnKnl3AnrOxllHG61O1DJ8u9D
oYFEYgfB/rQYAzqOWFb6lpuSFa2HFFt2Od3tBPjWb3nNQZ5wX+oUPWoLRESGDRgJ
IjobFJ19v2GsYRSLFpH8w3U9UV2LgDIwE3MRi7IXAgMBAAGjga0wgaowCQYDVR0T
BAIwADAdBgNVHQ4EFgQUFCqtJFrEykqmQxZID8PmFvPC8SowSAYDVR0jBEEwP4AU
uFNd3GQBzxAAnOEgFu0wBPD+1AGhHKQaMBgxFjAUBgNVBAMMDW9wZW52cG5zZXJ2
ZXKCCQC8GlvRpwidCTATBgNVHSUEDDAKBggrBgEFBQcDATALBgNVHQ8EBAMCBaAw
EgYDVR0RBAswCYIHZGVtb3ZwbjANBgkqhkiG9w0BAQsFAAOCAQEAd7zO/9Cb5quQ
QEPg6b0asNXhlD9rd07knlDf7Z9ueBai3yl3gTG4g3b/r+g34T8rkkdQDeBS3wRj
cBv+DcB8h+x7f64CUhlEv7smWypPKeDjxcV2N7RacjGBF8EuSuXlFyjgY9Eye4eP
+vJDnZZXHMSQ9AltR7TTql1+ErXGTm9giG/bPDjvJ6Grx+Tqlypr5CbSjj4+Zlwe
TKPcwVy1FaI6JmUShFcoeuwHjGv0qoFTCjX0sanPmG4jW1f8Y2VkgwzMpCpY1KeV
Lqn18ldG2jMs1GWJp8swiHVfkz1yqCnJP2oHPN/DMUGi88tvWO22h6+r6bQwB9X2
Ipt6SGtb2Q==
-----END CERTIFICATE-----
```

verify the generated certificate file with the following command



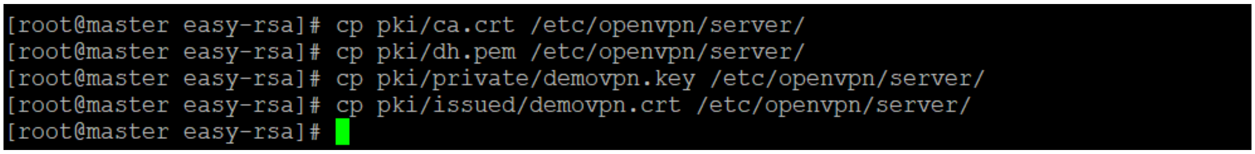
```
[root@master easy-rsa]# openssl verify -CAfile pki/ca.crt pki/issued/demovpn.crt
pki/issued/demovpn.crt: OK
```

Next, run the following command to generate a strong Diffie-Hellman key to use for the key exchange



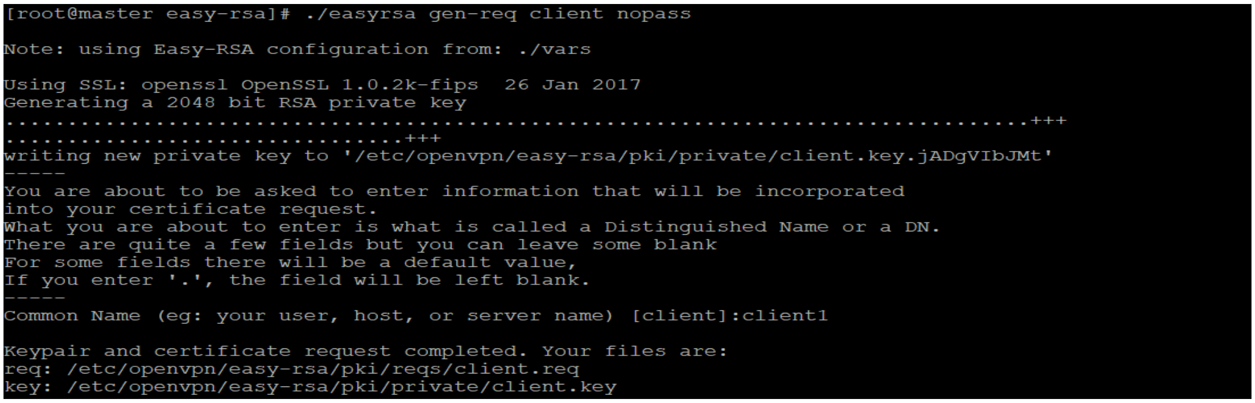
```
[root@master easy-rsa]# ./easyrsa gen-dh

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

Using SSL: openssl OpenSSL 1.0.2k-fips  26 Jan 2017
Generating DH parameters, 2048 bit long safe prime, generator 2
This is going to take a long time

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

After creating all certificate files, copy them to the /etc/openvpn/server/ directory



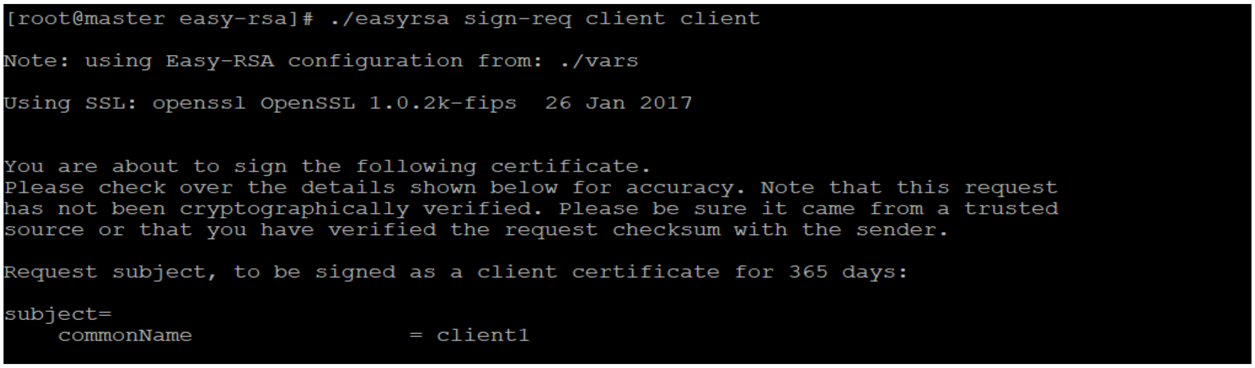
```
[root@master easy-rsa]# cp pki/ca.crt /etc/openvpn/server/
[root@master easy-rsa]# cp pki/dh.pem /etc/openvpn/server/
[root@master easy-rsa]# cp pki/private/demovpn.key /etc/openvpn/server/
[root@master easy-rsa]# cp pki/issued/demovpn.crt /etc/openvpn/server/
[root@master easy-rsa]# 
```

run the following command to build the client key file, Enter the Common name as the clients host name



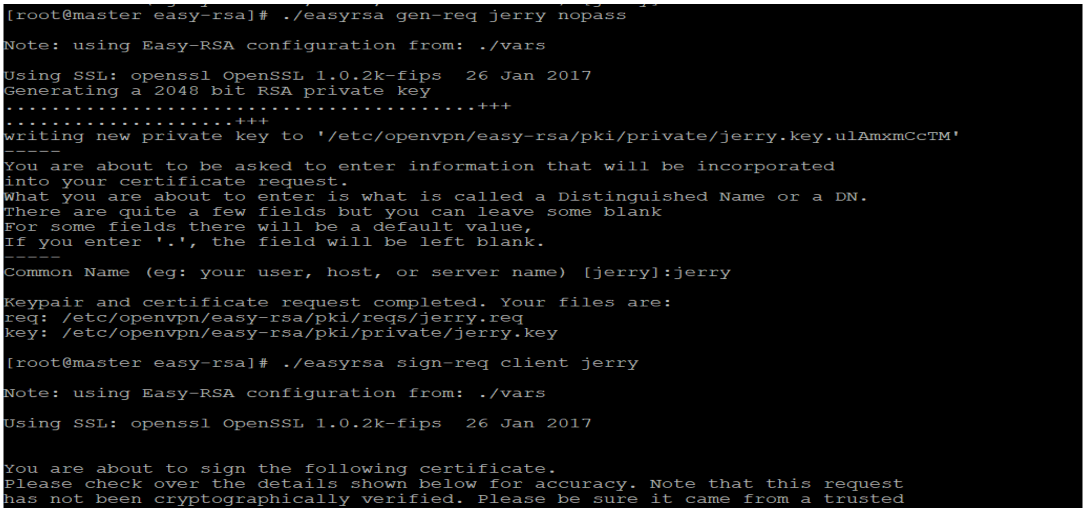
```
[root@master easy-rsa]# ./easyrsa gen-req client nopass

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

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/private/client.key.jADgVIbJMt'
-----
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) [client]:client1

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

sign the client key using your CA certificate: say yes and enter the password

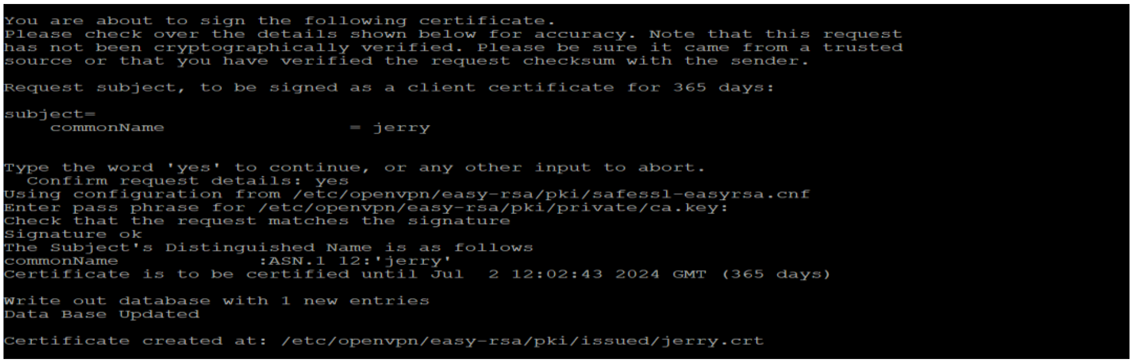


```
[root@master easy-rsa]# ./easyrsa sign-req client client

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

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 client certificate for 365 days:

subject=
    commonName                = client1
```

Now Create Certificate For New User Jerry

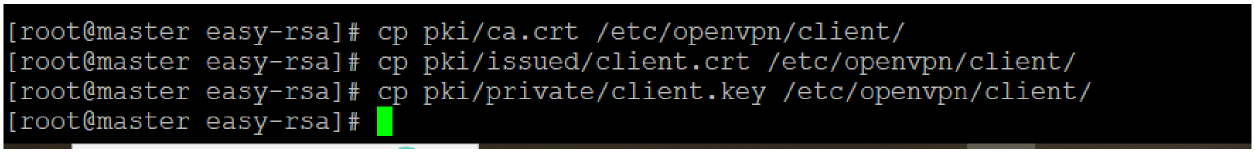


```
[root@master easy-rsa]# ./easyrsa gen-req jerry nopass

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

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/private/jerry.key.ulAmxmCcTM'
-----
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) [jerry]:jerry

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

[root@master easy-rsa]# ./easyrsa sign-req client jerry

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

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
```



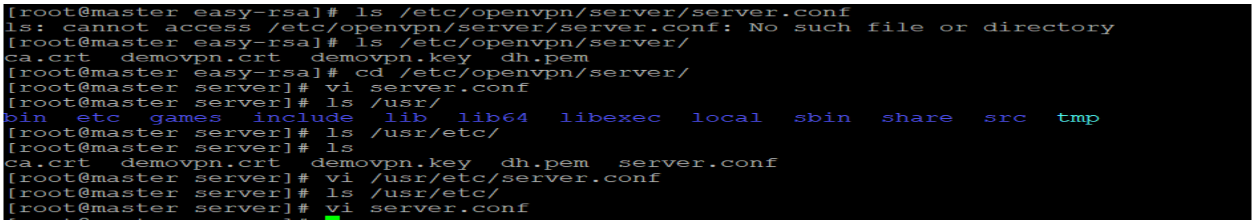
```
You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.

Request subject, to be signed as a client certificate for 365 days:

subject=
    commonName                = jerry


Type the word 'yes' to continue, or any other input to abort.
  Confirm request details: yes
Using configuration from /etc/openvpn/easy-rsa/pki/safessl-easyrsa.cnf
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:'jerry'
Certificate is to be certified until Jul  2 12:02:43 2024 GMT (365 days)

Write out database with 1 new entries
Data Base Updated

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

copy all client certificate and key file to the /etc/openvpn/client/ directory:

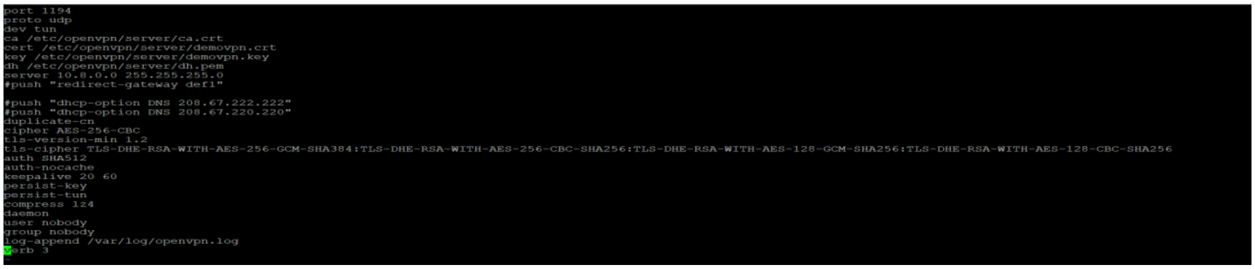


```
[root@master easy-rsa]# cp pki/ca.crt /etc/openvpn/client/
[root@master easy-rsa]# cp pki/issued/client.crt /etc/openvpn/client/
[root@master easy-rsa]# cp pki/private/client.key /etc/openvpn/client/
[root@master easy-rsa]# 
```

create a new OpenVPN configuration file inside /etc/openvpn/client/ directory:

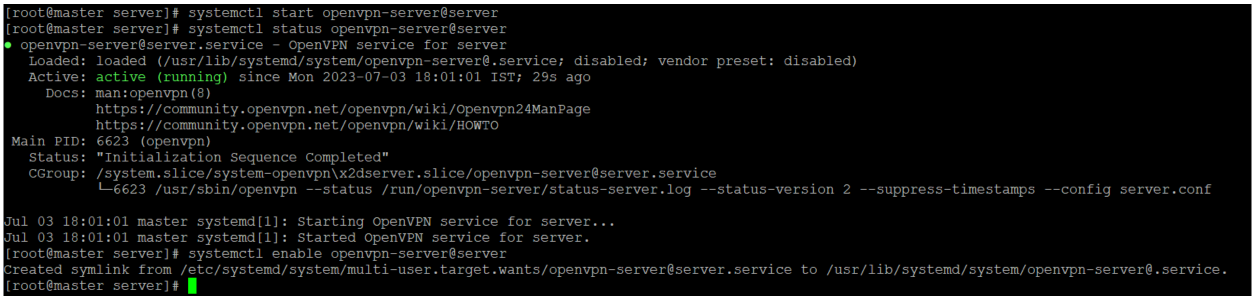


```
[root@master easy-rsa]# ls /etc/openvpn/server/server.conf
ls: cannot access /etc/openvpn/server/server.conf: No such file or directory
[root@master easy-rsa]# ls /etc/openvpn/server/
ca.crt  demovpn.crt  demovpn.key  dh.pem
[root@master easy-rsa]# cd /etc/openvpn/server/
[root@master server]# vi server.conf
[root@master server]# ls /usr/
bin  etc  games  include  lib  lib64  libexec  local  sbin  share  src  tmp
[root@master server]# ls /usr/etc/
[root@master server]# ls
ca.crt  demovpn.crt  demovpn.key  dh.pem  server.conf
[root@master server]# vi /usr/etc/server.conf
[root@master server]# ls /usr/etc/
[root@master server]# vi server.conf
```



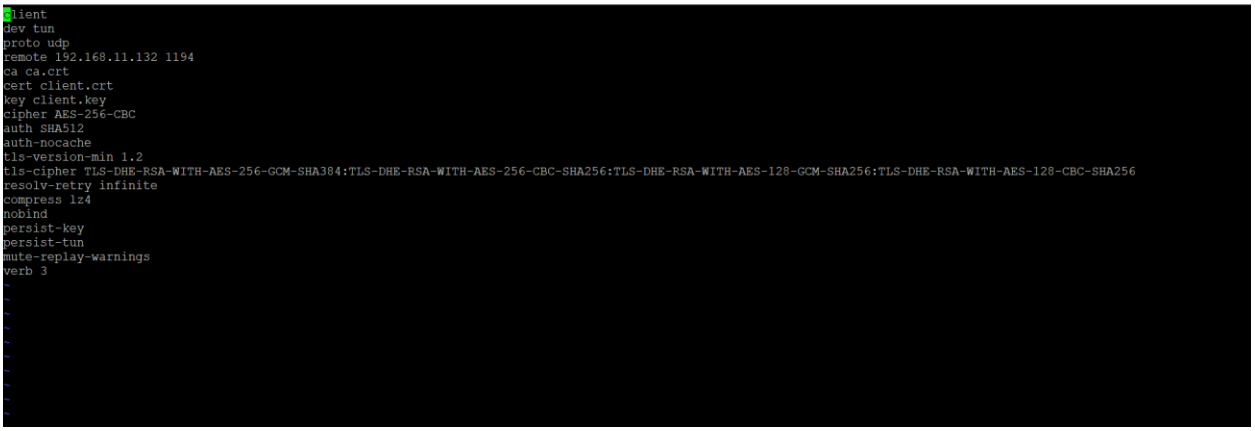
```
port 1194
proto udp
dev tun
ca /etc/openvpn/server/ca.crt
cert /etc/openvpn/server/demovpn.crt
key /etc/openvpn/server/demovpn.key
dh /etc/openvpn/server/dh.pem
server 10.8.0.0 255.255.255.0
#push "redirect-gateway def1"

#push "dhcp-option DNS 208.67.222.222"
#push "dhcp-option DNS 208.67.220.220"
duplicate-cn
cipher AES-256-CBC
tls-version-min 1.2
tls-cipher TLS-DHE-RSA-WITH-AES-256-GCM-SHA384:TLS-DHE-RSA-WITH-AES-256-CBC-SHA256:TLS-DHE-RSA-WITH-AES-128-GCM-SHA256:TLS-DHE-RSA-WITH-AES-128-CBC-SHA256
auth SHA512
auth-nocache
keepalive 20 60
persist-key
persist-tun
compress lz4
daemon
user nobody
group nobody
log-append /var/log/openvpn.log
verb 3
```

Check the status of openvpn server



```
[root@master server]# systemctl start openvpn-server@server
[root@master server]# systemctl status openvpn-server@server
● openvpn-server@server.service - OpenVPN service for server
   Loaded: loaded (/usr/lib/systemd/system/openvpn-server@.service; disabled; vendor preset: disabled)
   Active: active (running) since Mon 2023-07-03 18:01:01 IST; 29s ago
     Docs: man:openvpn(8)
           https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage
           https://community.openvpn.net/openvpn/wiki/HOWTO
 Main PID: 6623 (openvpn)
   Status: "Initialization Sequence Completed"
   CGroup: /system.slice/system-openvpn\x2dserver.slice/openvpn-server@server.service
           └─6623 /usr/sbin/openvpn --status /run/openvpn-server/status-server.log --status-version 2 --suppress-timestamps --config server.conf

Jul 03 18:01:01 master systemd[1]: Starting OpenVPN service for server...
Jul 03 18:01:01 master systemd[1]: Started OpenVPN service for server.
[root@master server]# systemctl enable openvpn-server@server
Created symlink from /etc/systemd/system/multi-user.target.wants/openvpn-server@server.service to /usr/lib/systemd/system/openvpn-server@.service.
[root@master server]# 
```

vi /etc/openvpn/client/client.ovpn



```
client
dev tun
proto udp
remote 192.168.11.132 1194
ca ca.crt
cert client.crt
key client.key
cipher AES-256-CBC
auth SHA512
auth-nocache
tls-version-min 1.2
tls-cipher TLS-DHE-RSA-WITH-AES-256-GCM-SHA384:TLS-DHE-RSA-WITH-AES-256-CBC-SHA256:TLS-DHE-RSA-WITH-AES-128-GCM-SHA256:TLS-DHE-RSA-WITH-AES-128-CBC-SHA256
resolv-retry infinite
compress lz4
nobind
persist-key
persist-tun
mute-replay-warnings
verb 3
~
~
~
~
~
~
~
~
~
~
```

Install epelrelease and openvpn on linux client

Yum install epel-release –y

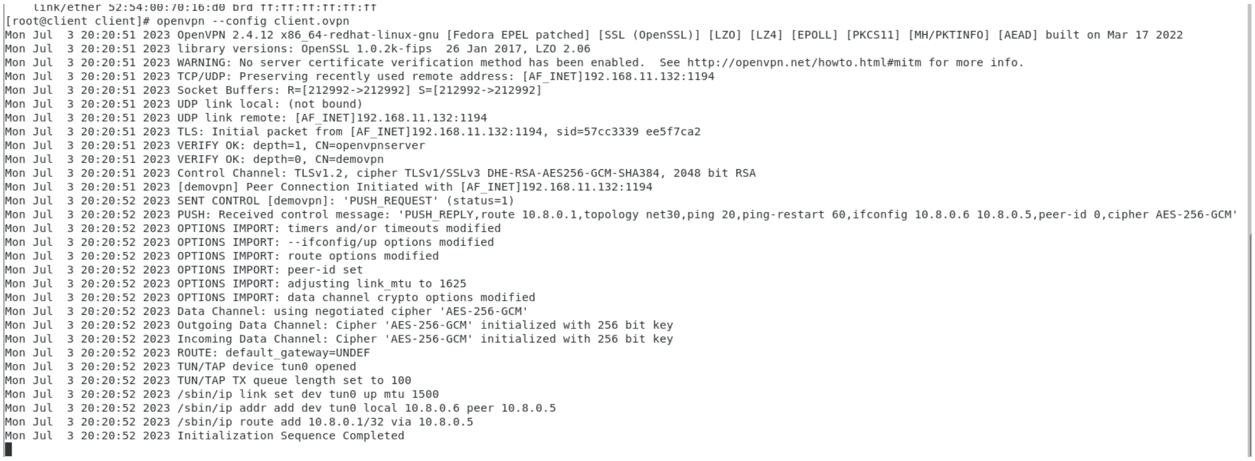
Yum install openvpn -y

Ifup ens33 ifdown ens33

Systemctl restart NetworkManager

Now try to ping windows ip and access webpage it should be unaccessible.

Give #ip a check for tun0 network adapter then run this command openvpn –config client.ovpn



```
    link/ether 52:54:00:70:16:d0 brd ff:ff:ff:ff:ff:ff
[root@client client]# openvpn --config client.ovpn
Mon Jul  3 20:20:51 2023 OpenVPN 2.4.12 x86_64-redhat-linux-gnu [Fedora EPEL patched] [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Mar 17 2022
Mon Jul  3 20:20:51 2023 library versions: OpenSSL 1.0.2k-fips  26 Jan 2017, LZO 2.06
Mon Jul  3 20:20:51 2023 WARNING: No server certificate verification method has been enabled.  See http://openvpn.net/howto.html#mitm for more info.
Mon Jul  3 20:20:51 2023 TCP/UDP: Preserving recently used remote address: [AF_INET]192.168.11.132:1194
Mon Jul  3 20:20:51 2023 Socket Buffers: R=[212992->212992] S=[212992->212992]
Mon Jul  3 20:20:51 2023 UDP link local: (not bound)
Mon Jul  3 20:20:51 2023 UDP link remote: [AF_INET]192.168.11.132:1194
Mon Jul  3 20:20:51 2023 TLS: Initial packet from [AF_INET]192.168.11.132:1194, sid=57cc3339 ee5f7ca2
Mon Jul  3 20:20:51 2023 VERIFY OK: depth=1, CN=openvpnserver
Mon Jul  3 20:20:51 2023 VERIFY OK: depth=0, CN=demovpn
Mon Jul  3 20:20:51 2023 Control Channel: TLSv1.2, cipher TLSv1/SSLv3 DHE-RSA-AES256-GCM-SHA384, 2048 bit RSA
Mon Jul  3 20:20:51 2023 [demovpn] Peer Connection Initiated with [AF_INET]192.168.11.132:1194
Mon Jul  3 20:20:52 2023 SENT CONTROL [demovpn]: 'PUSH_REQUEST' (status=1)
Mon Jul  3 20:20:52 2023 PUSH: Received control message: 'PUSH_REPLY,route 10.8.0.1,topology net30,ping 20,ping-restart 60,ifconfig 10.8.0.6 10.8.0.5,peer-id 0,cipher AES-256-GCM'
Mon Jul  3 20:20:52 2023 OPTIONS IMPORT: timers and/or timeouts modified
Mon Jul  3 20:20:52 2023 OPTIONS IMPORT: --ifconfig/up options modified
Mon Jul  3 20:20:52 2023 OPTIONS IMPORT: route options modified
Mon Jul  3 20:20:52 2023 OPTIONS IMPORT: peer-id set
Mon Jul  3 20:20:52 2023 OPTIONS IMPORT: adjusting link_mtu to 1625
Mon Jul  3 20:20:52 2023 OPTIONS IMPORT: data channel crypto options modified
Mon Jul  3 20:20:52 2023 Data Channel: using negotiated cipher 'AES-256-GCM'
Mon Jul  3 20:20:52 2023 Outgoing Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
Mon Jul  3 20:20:52 2023 Incoming Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
Mon Jul  3 20:20:52 2023 ROUTE: default_gateway=UNDEF
Mon Jul  3 20:20:52 2023 TUN/TAP device tun0 opened
Mon Jul  3 20:20:52 2023 TUN/TAP TX queue length set to 100
Mon Jul  3 20:20:52 2023 /sbin/ip link set dev tun0 up mtu 1500
Mon Jul  3 20:20:52 2023 /sbin/ip addr add dev tun0 local 10.8.0.6 peer 10.8.0.5
Mon Jul  3 20:20:52 2023 /sbin/ip route add 10.8.0.1/32 via 10.8.0.5
Mon Jul  3 20:20:52 2023 Initialization Sequence Completed
```