login as: root

root@10.10.10.128's password:

Last login: Tue Jun 20 17:40:21 2023

[root@master ~]# sestatus

SELinux status: enabled

SELinuxfs mount: /sys/fs/selinux

SELinux root directory: /etc/selinux

Loaded policy name: targeted

Current mode: enforcing

Mode from config file: enforcing

Policy MLS status: enabled

Policy deny\_unknown status: allowed

Max kernel policy version: 31

Similar command is: 'setenforce'

[root@master ~]# setenforce 0

[root@master ~]# vi /etc/selinux/config

[root@master ~]# cat /proc/sys/net/ipv4/ip\_forward

1

[root@master ~]# vi /etc/sysctl.conf

net.ipv4.ip\_forward=1

[root@master ~]# yum install epel-release -y

Loaded plugins: fastestmirror, langpacks

Loading mirror speeds from cached hostfile

\* base: mirrors.nxtgen.com

\* extras: mirrors.nxtgen.com

\* updates: centos.excellmedia.net

Resolving Dependencies

--> Running transaction check

---> Package epel-release.noarch 0:7-11 will be installed

--> Finished Dependency Resolution

Dependencies Resolved

=========================================================================================================

Package Arch Version Repository Size

=========================================================================================================

Installing:

epel-release noarch 7-11 extras 15 k

Transaction Summary

=========================================================================================================

Install 1 Package

Total download size: 15 k

Installed size: 24 k

Downloading packages:

epel-release-7-11.noarch.rpm | 15 kB 00:00:00

Running transaction check

Running transaction test

Transaction test succeeded

Running transaction

Installing : epel-release-7-11.noarch 1/1

Verifying : epel-release-7-11.noarch 1/1

Installed:

epel-release.noarch 0:7-11

Complete!

[root@master ~]# yum install openvpn -y

Loaded plugins: fastestmirror, langpacks

Loading mirror speeds from cached hostfile

\* base: mirrors.nxtgen.com

\* epel: repo.extreme-ix.org

\* extras: mirrors.nxtgen.com

\* updates: centos.excellmedia.net

Resolving Dependencies

--> Running transaction check

---> Package openvpn.x86\_64 0:2.4.12-1.el7 will be installed

--> Processing Dependency: libpkcs11-helper.so.1()(64bit) for package: openvpn-2.4.12-1.el7.x86\_64

--> Running transaction check

---> Package pkcs11-helper.x86\_64 0:1.11-3.el7 will be installed

--> Finished Dependency Resolution

Dependencies Resolved

=========================================================================================================

Package Arch Version Repository Size

=========================================================================================================

Installing:

openvpn x86\_64 2.4.12-1.el7 epel 529 k

Installing for dependencies:

pkcs11-helper x86\_64 1.11-3.el7 epel 56 k

Transaction Summary

=========================================================================================================

Install 1 Package (+1 Dependent package)

Total download size: 585 k

Installed size: 1.4 M

Downloading packages:

warning: /var/cache/yum/x86\_64/7/epel/packages/openvpn-2.4.12-1.el7.x86\_64.rpm: Header V4 RSA/SHA256 Sign ature, key ID 352c64e5: NOKEY

Public key for openvpn-2.4.12-1.el7.x86\_64.rpm is not installed

(1/2): openvpn-2.4.12-1.el7.x86\_64.rpm | 529 kB 00:00:00

(2/2): pkcs11-helper-1.11-3.el7.x86\_64.rpm | 56 kB 00:00:02

---------------------------------------------------------------------------------------------------------

Total 267 kB/s | 585 kB 00:00:02

Retrieving key from file:///etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL-7

Importing GPG key 0x352C64E5:

Userid : "Fedora EPEL (7) <epel@fedoraproject.org>"

Fingerprint: 91e9 7d7c 4a5e 96f1 7f3e 888f 6a2f aea2 352c 64e5

Package : epel-release-7-11.noarch (@extras)

From : /etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL-7

Running transaction check

Running transaction test

Transaction test succeeded

Running transaction

Installing : pkcs11-helper-1.11-3.el7.x86\_64 1/2

Installing : openvpn-2.4.12-1.el7.x86\_64 2/2

Verifying : openvpn-2.4.12-1.el7.x86\_64 1/2

Verifying : pkcs11-helper-1.11-3.el7.x86\_64 2/2

Installed:

openvpn.x86\_64 0:2.4.12-1.el7

Dependency Installed:

pkcs11-helper.x86\_64 0:1.11-3.el7

Complete!

[root@master ~]# cd /etc/open

openldap/ openvpn/

[root@master ~]# cd /etc/openvpn/

[root@master openvpn]# wget https://github.com/OpenVPN/easy-rsa/releases/download/v3.0.6/EasyRSA-unix-v3. 0.6.tgz

--2023-07-03 10:24:55-- https://github.com/OpenVPN/easy-rsa/releases/download/v3.0.6/EasyRSA-unix-v3.0.6 .tgz

Resolving github.com (github.com)... 20.207.73.82

Connecting to github.com (github.com)|20.207.73.82|:443... connected.

HTTP request sent, awaiting response... 302 Found

Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/4519663/8d46db80-2 66e-11e9-85e3-7de4dbee40d9?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20230 703%2Fus-east-1%2Fs3%2Faws4\_request&X-Amz-Date=20230703T050304Z&X-Amz-Expires=300&X-Amz-Signature=20e92a5 28837d5b8afc035e1c19c0ea3ff0762cb52f8170ebc9626956a107804&X-Amz-SignedHeaders=host&actor\_id=0&key\_id=0&re po\_id=4519663&response-content-disposition=attachment%3B%20filename%3DEasyRSA-unix-v3.0.6.tgz&response-co ntent-type=application%2Foctet-stream [following]

--2023-07-03 10:24:55-- https://objects.githubusercontent.com/github-production-release-asset-2e65be/451 9663/8d46db80-266e-11e9-85e3-7de4dbee40d9?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4C SVEH53A%2F20230703%2Fus-east-1%2Fs3%2Faws4\_request&X-Amz-Date=20230703T050304Z&X-Amz-Expires=300&X-Amz-Si gnature=20e92a528837d5b8afc035e1c19c0ea3ff0762cb52f8170ebc9626956a107804&X-Amz-SignedHeaders=host&actor\_i d=0&key\_id=0&repo\_id=4519663&response-content-disposition=attachment%3B%20filename%3DEasyRSA-unix-v3.0.6. tgz&response-content-type=application%2Foctet-stream

Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.111.133, 185.199.109.1 33, 185.199.110.133, ...

Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.111.133|:443... conne cted.

HTTP request sent, awaiting response... 200 OK

Length: 40840 (40K) [application/octet-stream]

Saving to: ‘EasyRSA-unix-v3.0.6.tgz’

100%[===============================================================>] 40,840 --.-K/s in 0.006s

2023-07-03 10:24:56 (6.68 MB/s) - ‘EasyRSA-unix-v3.0.6.tgz’ saved [40840/40840]

[root@master openvpn]# ls

client EasyRSA-unix-v3.0.6.tgz server

[root@master openvpn]# tar -xvzf EasyRSA-unix-v3.0.6.tgz

EasyRSA-v3.0.6/

EasyRSA-v3.0.6/easyrsa

EasyRSA-v3.0.6/openssl-easyrsa.cnf

EasyRSA-v3.0.6/vars.example

EasyRSA-v3.0.6/x509-types/

EasyRSA-v3.0.6/gpl-2.0.txt

EasyRSA-v3.0.6/mktemp.txt

EasyRSA-v3.0.6/COPYING.md

EasyRSA-v3.0.6/ChangeLog

EasyRSA-v3.0.6/README.md

EasyRSA-v3.0.6/README.quickstart.md

EasyRSA-v3.0.6/doc/

EasyRSA-v3.0.6/doc/EasyRSA-Advanced.md

EasyRSA-v3.0.6/doc/EasyRSA-Readme.md

EasyRSA-v3.0.6/doc/EasyRSA-Upgrade-Notes.md

EasyRSA-v3.0.6/doc/Hacking.md

EasyRSA-v3.0.6/doc/Intro-To-PKI.md

EasyRSA-v3.0.6/x509-types/COMMON

EasyRSA-v3.0.6/x509-types/ca

EasyRSA-v3.0.6/x509-types/client

EasyRSA-v3.0.6/x509-types/code-signing

EasyRSA-v3.0.6/x509-types/server

EasyRSA-v3.0.6/x509-types/serverClient

[root@master openvpn]# mv EasyRSA-v3.0.6 easy-rsa

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

[root@master easy-rsa]# cat vars.example

# Easy-RSA 3 parameter settings

# NOTE: If you installed Easy-RSA from your distro's package manager, don't edit

# this file in place -- instead, you should copy the entire easy-rsa directory

# to another location so future upgrades don't wipe out your changes.

# HOW TO USE THIS FILE

#

# vars.example contains built-in examples to Easy-RSA settings. You MUST name

# this file 'vars' if you want it to be used as a configuration file. If you do

# not, it WILL NOT be automatically read when you call easyrsa commands.

#

# It is not necessary to use this config file unless you wish to change

# operational defaults. These defaults should be fine for many uses without the

# need to copy and edit the 'vars' file.

#

# All of the editable settings are shown commented and start with the command

# 'set\_var' -- this means any set\_var command that is uncommented has been

# modified by the user. If you're happy with a default, there is no need to

# define the value to its default.

# NOTES FOR WINDOWS USERS

#

# Paths for Windows \*MUST\* use forward slashes, or optionally double-esscaped

# backslashes (single forward slashes are recommended.) This means your path to

# the openssl binary might look like this:

# "C:/Program Files/OpenSSL-Win32/bin/openssl.exe"

# A little housekeeping: DON'T EDIT THIS SECTION

#

# Easy-RSA 3.x doesn't source into the environment directly.

# Complain if a user tries to do this:

if [ -z "$EASYRSA\_CALLER" ]; then

echo "You appear to be sourcing an Easy-RSA 'vars' file." >&2

echo "This is no longer necessary and is disallowed. See the section called" >&2

echo "'How to use this file' near the top comments for more details." >&2

return 1

fi

# DO YOUR EDITS BELOW THIS POINT

# This variable is used as the base location of configuration files needed by

# easyrsa. More specific variables for specific files (e.g., EASYRSA\_SSL\_CONF)

# may override this default.

#

# The default value of this variable is the location of the easyrsa script

# itself, which is also where the configuration files are located in the

# easy-rsa tree.

#set\_var EASYRSA "${0%/\*}"

# If your OpenSSL command is not in the system PATH, you will need to define the

# path to it here. Normally this means a full path to the executable, otherwise

# you could have left it undefined here and the shown default would be used.

#

# Windows users, remember to use paths with forward-slashes (or escaped

# back-slashes.) Windows users should declare the full path to the openssl

# binary here if it is not in their system PATH.

#set\_var EASYRSA\_OPENSSL "openssl"

#

# This sample is in Windows syntax -- edit it for your path if not using PATH:

#set\_var EASYRSA\_OPENSSL "C:/Program Files/OpenSSL-Win32/bin/openssl.exe"

# Edit this variable to point to your soon-to-be-created key directory. By

# default, this will be "$PWD/pki" (i.e. the "pki" subdirectory of the

# directory you are currently in).

#

# WARNING: init-pki will do a rm -rf on this directory so make sure you define

# it correctly! (Interactive mode will prompt before acting.)

#set\_var EASYRSA\_PKI "$PWD/pki"

# Define X509 DN mode.

# This is used to adjust what elements are included in the Subject field as the DN

# (this is the "Distinguished Name.")

# Note that in cn\_only mode the Organizational fields further below aren't used.

#

# Choices are:

# cn\_only - use just a CN value

# org - use the "traditional" Country/Province/City/Org/OU/email/CN format

#set\_var EASYRSA\_DN "cn\_only"

# Organizational fields (used with 'org' mode and ignored in 'cn\_only' mode.)

# These are the default values for fields which will be placed in the

# certificate. Don't leave any of these fields blank, although interactively

# you may omit any specific field by typing the "." symbol (not valid for

# email.)

#set\_var EASYRSA\_REQ\_COUNTRY "US"

#set\_var EASYRSA\_REQ\_PROVINCE "California"

#set\_var EASYRSA\_REQ\_CITY "San Francisco"

#set\_var EASYRSA\_REQ\_ORG "Copyleft Certificate Co"

#set\_var EASYRSA\_REQ\_EMAIL "me@example.net"

#set\_var EASYRSA\_REQ\_OU "My Organizational Unit"

# Choose a size in bits for your keypairs. The recommended value is 2048. Using

# 2048-bit keys is considered more than sufficient for many years into the

# future. Larger keysizes will slow down TLS negotiation and make key/DH param

# generation take much longer. Values up to 4096 should be accepted by most

# software. Only used when the crypto alg is rsa (see below.)

#set\_var EASYRSA\_KEY\_SIZE 2048

# The default crypto mode is rsa; ec can enable elliptic curve support.

# Note that not all software supports ECC, so use care when enabling it.

# Choices for crypto alg are: (each in lower-case)

# \* rsa

# \* ec

#set\_var EASYRSA\_ALGO rsa

# Define the named curve, used in ec mode only:

#set\_var EASYRSA\_CURVE secp384r1

# In how many days should the root CA key expire?

#set\_var EASYRSA\_CA\_EXPIRE 3650

# In how many days should certificates expire?

#set\_var EASYRSA\_CERT\_EXPIRE 1080

# How many days until the next CRL publish date? Note that the CRL can still be

# parsed after this timeframe passes. It is only used for an expected next

# publication date.

# How many days before its expiration date a certificate is allowed to be

# renewed?

#set\_var EASYRSA\_CERT\_RENEW 30

#set\_var EASYRSA\_CRL\_DAYS 180

# Support deprecated "Netscape" extensions? (choices "yes" or "no".) The default

# is "no" to discourage use of deprecated extensions. If you require this

# feature to use with --ns-cert-type, set this to "yes" here. This support

# should be replaced with the more modern --remote-cert-tls feature. If you do

# not use --ns-cert-type in your configs, it is safe (and recommended) to leave

# this defined to "no". When set to "yes", server-signed certs get the

# nsCertType=server attribute, and also get any NS\_COMMENT defined below in the

# nsComment field.

#set\_var EASYRSA\_NS\_SUPPORT "no"

# When NS\_SUPPORT is set to "yes", this field is added as the nsComment field.

# Set this blank to omit it. With NS\_SUPPORT set to "no" this field is ignored.

#set\_var EASYRSA\_NS\_COMMENT "Easy-RSA Generated Certificate"

# A temp file used to stage cert extensions during signing. The default should

# be fine for most users; however, some users might want an alternative under a

# RAM-based FS, such as /dev/shm or /tmp on some systems.

#set\_var EASYRSA\_TEMP\_FILE "$EASYRSA\_PKI/extensions.temp"

# !!

# NOTE: ADVANCED OPTIONS BELOW THIS POINT

# PLAY WITH THEM AT YOUR OWN RISK

# !!

# Broken shell command aliases: If you have a largely broken shell that is

# missing any of these POSIX-required commands used by Easy-RSA, you will need

# to define an alias to the proper path for the command. The symptom will be

# some form of a 'command not found' error from your shell. This means your

# shell is BROKEN, but you can hack around it here if you really need. These

# shown values are not defaults: it is up to you to know what you're doing if

# you touch these.

#

#alias awk="/alt/bin/awk"

#alias cat="/alt/bin/cat"

# X509 extensions directory:

# If you want to customize the X509 extensions used, set the directory to look

# for extensions here. Each cert type you sign must have a matching filename,

# and an optional file named 'COMMON' is included first when present. Note that

# when undefined here, default behaviour is to look in $EASYRSA\_PKI first, then

# fallback to $EASYRSA for the 'x509-types' dir. You may override this

# detection with an explicit dir here.

#

#set\_var EASYRSA\_EXT\_DIR "$EASYRSA/x509-types"

# OpenSSL config file:

# If you need to use a specific openssl config file, you can reference it here.

# Normally this file is auto-detected from a file named openssl-easyrsa.cnf from the

# EASYRSA\_PKI or EASYRSA dir (in that order.) NOTE that this file is Easy-RSA

# specific and you cannot just use a standard config file, so this is an

# advanced feature.

#set\_var EASYRSA\_SSL\_CONF "$EASYRSA/openssl-easyrsa.cnf"

# Default CN:

# This is best left alone. Interactively you will set this manually, and BATCH

# callers are expected to set this themselves.

#set\_var EASYRSA\_REQ\_CN "ChangeMe"

# Cryptographic digest to use.

# Do not change this default unless you understand the security implications.

# Valid choices include: md5, sha1, sha256, sha224, sha384, sha512

#set\_var EASYRSA\_DIGEST "sha256"

# Batch mode. Leave this disabled unless you intend to call Easy-RSA explicitly

# in batch mode without any user input, confirmation on dangerous operations,

# or most output. Setting this to any non-blank string enables batch mode.

#set\_var EASYRSA\_BATCH ""

[root@master easy-rsa]# vim vars

[root@master easy-rsa]# cat vars

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 "ACTS CDAC"

set\_var EASYRSA\_REQ\_EMAIL "admin@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]# ls

ChangeLog doc gpl-2.0.txt openssl-easyrsa.cnf README.quickstart.md vars.example

COPYING.md easyrsa mktemp.txt README.md vars x509-types

[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

[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: @1234

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]:vpn-server

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

[root@master easy-rsa]# ls

ChangeLog doc gpl-2.0.txt openssl-easyrsa.cnf README.md vars x509-types

COPYING.md easyrsa mktemp.txt pki README.quickstart.md vars.example

[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

[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.ioWnsS0F9z'

-----

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

BQADggEPADCCAQoCggEBAK/8eojAmYKd4ioWMBYT4sUmMONNz3S+AU0p/sQrv1yX

Kzi0sMeNv+clMBSvFHgwT5C7hFHAd918j8b55Nwy8YApjYP/exaofMDWnW8foEHz

U9xmM1TPzZU5cuboXa5ZeiMZYMDo4TvshxHm77Z8gIMiia11wKsmXQDcOc4rcdcY

wKPeQ7/dhZqINXhwO26wb14z3ikR6lZ0S81cWTXId90OaLxrmLDnK2QrTbUoYCqh

yGqD+nenL88DKsEMMmFF3rOpaL6VLALuOfrxd/RGCtjN6AaoxAxhJ943SW77waVW

mJVVq8yxgDtNp3pXe6lPaVDHwUj/aZ/TuC+GRSjcpJ0CAwEAAaAAMA0GCSqGSIb3

DQEBCwUAA4IBAQANjhyVFmZ6oYFXjBvoZyp2eJBuHXt4zB11V36UJMEg3Hq3juPV

J49+DvIPT+X79l7qe+dQLemcWkO6rC08cwPiErIxCIlq707x+M9WYXsvWHYYoia3

2m8PXs7bXTT31rXh7ATcNTjk7msU5VIOWLtsthtWzIAXN5ZNFszhWJuWMEtTtTEF

NQhVdENxyTkkYMsE0cZYM+4mHDcYBhDFaZBaVSEbQy3fKTvMgOr7kqWiEVTz/mCu

wMCSc6uH5IROk7lcBibuYlloeC4JYpXoz0Pw6vaCM0Lgzno+MCUl90tCk5rGqO+/

7aiR3ksqTfgVhUK5sbnSUH0b5qGv1V5xaOdY

-----END CERTIFICATE REQUEST-----

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

Yes 🡪 ca.key : @1234

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 05:27:19 2024 GMT (365 days)

Write out database with 1 new entries

Data Base Updated

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

[root@master easy-rsa]# cat pki/issued/demovpn.crt

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

97:1b:4a:b8:79:ec:c4:94:9e:b6:c5:0a:d3:b6:56:c4

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=vpn-server

Validity

Not Before: Jul 3 05:27:19 2023 GMT

Not After : Jul 2 05:27:19 2024 GMT

Subject: CN=demovpn

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

00:af:fc:7a:88:c0:99:82:9d:e2:2a:16:30:16:13:

e2:c5:26:30:e3:4d:cf:74:be:01:4d:29:fe:c4:2b:

bf:5c:97:2b:38:b4:b0:c7:8d:bf:e7:25:30:14:af:

14:78:30:4f:90:bb:84:51:c0:77:dd:7c:8f:c6:f9:

e4:dc:32:f1:80:29:8d:83:ff:7b:16:a8:7c:c0:d6:

9d:6f:1f:a0:41:f3:53:dc:66:33:54:cf:cd:95:39:

72:e6:e8:5d:ae:59:7a:23:19:60:c0:e8:e1:3b:ec:

87:11:e6:ef:b6:7c:80:83:22:89:ad:75:c0:ab:26:

5d:00:dc:39:ce:2b:71:d7:18:c0:a3:de:43:bf:dd:

85:9a:88:35:78:70:3b:6e:b0:6f:5e:33:de:29:11:

ea:56:74:4b:cd:5c:59:35:c8:77:dd:0e:68:bc:6b:

98:b0:e7:2b:64:2b:4d:b5:28:60:2a:a1:c8:6a:83:

fa:77:a7:2f:cf:03:2a:c1:0c:32:61:45:de:b3:a9:

68:be:95:2c:02:ee:39:fa:f1:77:f4:46:0a:d8:cd:

e8:06:a8:c4:0c:61:27:de:37:49:6e:fb:c1:a5:56:

98:95:55:ab:cc:b1:80:3b:4d:a7:7a:57:7b:a9:4f:

69:50:c7:c1:48:ff:69:9f:d3:b8:2f:86:45:28:dc:

a4:9d

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints:

CA:FALSE

X509v3 Subject Key Identifier:

B5:AB:41:03:90:FE:88:94:CE:6F:A1:D5:6A:B8:B9:EB:3B:90:16:D2

X509v3 Authority Key Identifier:

keyid:C6:18:D4:C8:1E:35:38:F4:C8:86:01:07:98:BD:5C:C0:63:C8:7E:E5

DirName:/CN=vpn-server

serial:CD:26:C7:A0:AA:2B:D4:E1

X509v3 Extended Key Usage:

TLS Web Server Authentication

X509v3 Key Usage:

Digital Signature, Key Encipherment

X509v3 Subject Alternative Name:

DNS:demovpn

Signature Algorithm: sha256WithRSAEncryption

35:30:f3:a9:aa:bf:77:b6:bf:aa:30:b4:7e:9c:f7:08:ce:5c:

90:b0:30:6a:8c:a2:67:03:97:0d:39:01:b4:1f:e9:13:40:52:

16:f0:83:29:56:a9:57:55:92:cf:13:57:8d:fb:c6:d9:af:82:

75:75:d8:74:22:89:92:ea:59:6f:36:2d:b0:db:c2:66:68:30:

21:87:98:e3:92:53:1a:f5:fd:58:84:16:52:80:7a:f0:a2:d3:

06:2a:d4:07:5c:35:76:a3:3e:9f:45:c6:cd:ce:ae:3e:7d:dd:

d4:48:52:d5:b7:23:2a:24:3c:df:1e:f4:38:fd:24:7a:78:07:

37:39:eb:3c:d1:0a:85:f9:6f:4e:1e:4c:4a:85:87:ec:60:1e:

73:1a:e5:c2:af:57:a5:79:4e:e5:4a:4f:cc:8a:53:79:a3:5b:

fd:0d:f1:e5:f1:f4:2d:40:5c:76:0b:c4:59:30:0d:2c:83:7e:

be:0e:6a:1c:49:04:c3:aa:c4:c2:d7:c7:10:25:8d:78:76:d5:

46:9d:cf:b9:68:f5:d6:3d:fa:36:3b:e9:1e:6d:9d:57:42:6e:

6b:08:66:dc:3e:3a:9a:1f:ef:7c:89:0a:96:54:66:48:e1:bc:

76:e5:db:5c:ac:5d:4b:9a:fd:29:1b:6e:87:b0:f4:cb:76:9d:

a8:53:ba:b1

-----BEGIN CERTIFICATE-----

MIIDXTCCAkWgAwIBAgIRAJcbSrh57MSUnrbFCtO2VsQwDQYJKoZIhvcNAQELBQAw

FTETMBEGA1UEAwwKdnBuLXNlcnZlcjAeFw0yMzA3MDMwNTI3MTlaFw0yNDA3MDIw

NTI3MTlaMBIxEDAOBgNVBAMMB2RlbW92cG4wggEiMA0GCSqGSIb3DQEBAQUAA4IB

DwAwggEKAoIBAQCv/HqIwJmCneIqFjAWE+LFJjDjTc90vgFNKf7EK79clys4tLDH

jb/nJTAUrxR4ME+Qu4RRwHfdfI/G+eTcMvGAKY2D/3sWqHzA1p1vH6BB81PcZjNU

z82VOXLm6F2uWXojGWDA6OE77IcR5u+2fICDIomtdcCrJl0A3DnOK3HXGMCj3kO/

3YWaiDV4cDtusG9eM94pEepWdEvNXFk1yHfdDmi8a5iw5ytkK021KGAqochqg/p3

py/PAyrBDDJhRd6zqWi+lSwC7jn68Xf0RgrYzegGqMQMYSfeN0lu+8GlVpiVVavM

sYA7Tad6V3upT2lQx8FI/2mf07gvhkUo3KSdAgMBAAGjgaowgacwCQYDVR0TBAIw

ADAdBgNVHQ4EFgQUtatBA5D+iJTOb6HVari56zuQFtIwRQYDVR0jBD4wPIAUxhjU

yB41OPTIhgEHmL1cwGPIfuWhGaQXMBUxEzARBgNVBAMMCnZwbi1zZXJ2ZXKCCQDN

JsegqivU4TATBgNVHSUEDDAKBggrBgEFBQcDATALBgNVHQ8EBAMCBaAwEgYDVR0R

BAswCYIHZGVtb3ZwbjANBgkqhkiG9w0BAQsFAAOCAQEANTDzqaq/d7a/qjC0fpz3

CM5ckLAwaoyiZwOXDTkBtB/pE0BSFvCDKVapV1WSzxNXjfvG2a+CdXXYdCKJkupZ

bzYtsNvCZmgwIYeY45JTGvX9WIQWUoB68KLTBirUB1w1dqM+n0XGzc6uPn3d1EhS

1bcjKiQ83x70OP0kengHNznrPNEKhflvTh5MSoWH7GAecxrlwq9XpXlO5UpPzIpT

eaNb/Q3x5fH0LUBcdgvEWTANLIN+vg5qHEkEw6rEwtfHECWNeHbVRp3PuWj11j36

NjvpHm2dV0Juawhm3D46mh/vfIkKllRmSOG8duXbXKxdS5r9KRtuh7D0y3adqFO6

sQ==

-----END CERTIFICATE-----

[root@master easy-rsa]#

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

pki/issued/demovpn.crt: OK

[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

[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]# ./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.5xWM3KSGsm'

-----

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]:client

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

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

Yes 🡪 @1234

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 = client

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:'client'

Certificate is to be certified until Jul 2 06:29:54 2024 GMT (365 days)

Write out database with 1 new entries

Data Base Updated

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

[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.7Te1rdAOQy'

-----

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]:jeery

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

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 = jeery

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:'jeery'

Certificate is to be certified until Jul 2 06:33:29 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

[root@master easy-rsa]# ./easyrsa gen-req indra 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/indra.key.J7Ki0FC5AK'

-----

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) [indra]:indra

Keypair and certificate request completed. Your files are:

req: /etc/openvpn/easy-rsa/pki/reqs/indra.req

key: /etc/openvpn/easy-rsa/pki/private/indra.key

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

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 = indra

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:'indra'

Certificate is to be certified until Jul 2 06:34:15 2024 GMT (365 days)

Write out database with 1 new entries

Data Base Updated

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

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

[root@master easy-rsa]# ls /etc/openvpn/client/

ca.crt

[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]# ls /etc/openvpn/client/

ca.crt client.crt client.key

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

port 1194

proto udp

dev tun

ca /etc/openvpn/server/ca.crt

cert /etc/openvpn/server/hpcsa1.crt

key /etc/openvpn/server/hpcsa1.key

dh /etc/openvpn/server/dh.pem

server 10.8.0.0 255.255.255.0

push "route 10.10.10.0 255.255.255.0"

#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

[root@master easy-rsa]# systemctl start openvpn-server@server

[root@master easy-rsa]# 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 easy-rsa]# systemctl status openvpn-server@server

● openvpn-server@server.service - OpenVPN service for server

Loaded: loaded (/usr/lib/systemd/system/openvpn-server@.service; enabled; vendor preset: disabled)

Active: active (running) since Mon 2023-07-03 12:30:37 IST; 20s ago

Docs: man:openvpn(8)

https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage

https://community.openvpn.net/openvpn/wiki/HOWTO

Main PID: 1401 (openvpn)

Status: "Initialization Sequence Completed"

CGroup: /system.slice/system-openvpn\x2dserver.slice/openvpn-server@server.service

└─1401 /usr/sbin/openvpn --status /run/openvpn-server/status-server.log --status-version 2 --suppress-timestamps...

Jul 03 12:30:37 master systemd[1]: Starting OpenVPN service for server...

Jul 03 12:30:37 master systemd[1]: Started OpenVPN service for server.

[root@master easy-rsa]# systemctl start firewalld.service

[root@master easy-rsa]# systemctl enable firewalld.service

Created symlink from /etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service to /usr/lib/systemd/system/firewalld.service.

Created symlink from /etc/systemd/system/multi-user.target.wants/firewalld.service to /usr/lib/systemd/system/firewalld.service.

[root@master easy-rsa]# firewall-cmd --permanent --add-service=openvpn

success

[root@master easy-rsa]# firewall-cmd --permanent --zone=trusted --add-service=openvpn

success

[root@master easy-rsa]# firewall-cmd --permanent --zone=trusted --add-interface=tun0

success

[root@master easy-rsa]# firewall-cmd --add-masquerade

success

[root@master easy-rsa]# firewall-cmd --permanent --add-masquerade

success

[root@master easy-rsa]# tecadmin=$(ip route get 8.8.8.8 | awk 'NR==1 {print $(NF-2)}')

[root@master easy-rsa]# ip route get 8.8.8.8

8.8.8.8 via 192.168.15.2 dev ens33 src 192.168.15.151

cache

[root@master easy-rsa]# firewall-cmd --permanent --direct --passthrough ipv4 -t nat -A POSTROUTING -s 10.8.0.0/24 -o ens33 -j MASQUERADE

success

[root@master easy-rsa]# firewall-cmd --reload

success

[root@master easy-rsa]# vim /etc/openvpn/client/client.ovpn

client

dev tun

proto udp

remote 192.168.15.189(server nat ip) 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

[root@master easy-rsa]# vim /etc/openvpn/client/client.ovpn

[root@master easy-rsa]# scp -r root@192.168.15.161:/etc/openvpn/client .

The authenticity of host '192.168.15.161 (192.168.15.161)' can't be established.

ECDSA key fingerprint is SHA256:vLMUl0ZblhAE5iXWIABnvnJKNpTC1gLelyc0RWcKv9E.

ECDSA key fingerprint is MD5:d1:a9:b7:3d:22:e4:d4:f3:37:83:c0:ac:d5:8a:95:68.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '192.168.15.161' (ECDSA) to the list of known hosts.

root@192.168.15.161's password:

scp: /etc/openvpn/client: No such file or directory

[root@master easy-rsa]# scp -r /etc/openvpn/client/ [root@192.168.15.161(client](mailto:root@192.168.15.161(client) ip):/root

root@192.168.15.161's password:

ca.crt 100% 1168 1.2MB/s 00:00

client.crt 100% 4430 6.3MB/s 00:00

client.key 100% 1704 4.2MB/s 00:00

client.ovpn 100% 406 1.1MB/s 00:00

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

[root@master server]# vi server.conf

[root@master server]# cat 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 "route 10.10.10.0 255.255.255.0"

#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

[root@master server]# systemctl restart 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; enabled; vendor preset: disabled)

Active: active (running) since Mon 2023-07-03 15:16:21 IST; 8s ago

Docs: man:openvpn(8)

https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage

https://community.openvpn.net/openvpn/wiki/HOWTO

Main PID: 5548 (openvpn)

Status: "Initialization Sequence Completed"

CGroup: /system.slice/system-openvpn\x2dserver.slice/openvpn-server@server.service

└─5548 /usr/sbin/openvpn --status /run/openvpn-server/status-server.log --status-version 2 --suppress-timestamps...

Jul 03 15:16:21 master systemd[1]: Starting OpenVPN service for server...

Jul 03 15:16:21 master systemd[1]: Started OpenVPN service for server.

[root@master server]#

History

345 setenforce 0

346 vi /etc/selinux/config

347 cat /proc/sys/net/ipv4/ip\_forward

348 vi /etc/sysctl.conf

349 yum install epel-release -y

350 yum install openvpn -y

351 cd /etc/openvpn/

352 wget https://github.com/OpenVPN/easy-rsa/releases/download/v3.0.6/EasyRSA-unix-v3.0.6.tgz

353 ls

354 tar -xvzf EasyRSA-unix-v3.0.6.tgz

355 mv EasyRSA-v3.0.6 easy-rsa

356 cd easy-rsa/

357 cat vars.example

358 vim vars

359 cat vars

360 ls

361 ./easyrsa init-pki

362 ./easyrsa build-ca

363 ls

364 ls pki

365 ls pki/private/

366 ./easyrsa gen-req demovpn nopass

367 ls pki/reqs/demovpn.req

368 cat pki/reqs/demovpn.req

369 ./easyrsa sign-req server demovpn

370 cat pki/issued/demovpn.crt

371 openssl verify -CAfile pki/ca.crt pki/issued/demovpn.crt

372 ./easyrsa gen-dh

373 cp pki/ca.crt /etc/openvpn/server/

374 cp pki/dh.pem /etc/openvpn/server/

375 cp pki/private/demovpn.key /etc/openvpn/server/

376 cp pki/issued/demovpn.crt /etc/openvpn/server/

377 ./easyrsa gen-req client nopass

378 ./easyrsa sign-req client client

379\*

380 ./easyrsa sign-req client jerry

381 ./easyrsa gen-req indra nopass

382 ./easyrsa sign-req client indra

383 cp pki/ca.crt /etc/openvpn/client/

384 ls /etc/openvpn/client/

385 cp pki/issued/client.crt /etc/openvpn/client/

386 cp pki/private/client.key /etc/openvpn/client/

387 ls /etc/openvpn/client/

388 vi /etc/openvpn/server/server.conf

389 systemctl start openvpn-server@server

390 systemctl enable openvpn-server@server

391 systemctl status openvpn-server@server

392 systemctl start firewalld.service

393 systemctl enable firewalld.service

394 firewall-cmd --permanent --add-service=openvpn

395 firewall-cmd --permanent --zone=trusted --add-service=openvpn

396 firewall-cmd --permanent --zone=trusted --add-interface=tun0

397 firewall-cmd --add-masquerade

398 firewall-cmd --permanent --add-masquerade

399 tecadmin=$(ip route get 8.8.8.8 | awk 'NR==1 {print $(NF-2)}')

400 ip route get 8.8.8.8

401 firewall-cmd --permanent --direct --passthrough ipv4 -t nat -A POSTROUTING -s 10.8.0.0/24 -o ens33 -j MASQUERADE

402 firewall-cmd --reload

403 vim /etc/openvpn/client/client.ovpn

404 scp -r root@192.168.15.161:/etc/openvpn/client .

405 scp -r /etc/openvpn/client/ root@192.168.15.161:/root

406 cd /etc/openvpn/server/

407 vi server.conf

408 cat server.conf

409 systemctl restart openvpn-server@server

410 systemctl status openvpn-server@server

411 history