

Pour installer le référentiel EPEL, saisissez la commande suivante :

```
root@server:~  
Fichier Édition Affichage Rechercher Terminal Aide  
[root@server ~]# yum install epel-release -y
```

Vous obtiendrez l'écran comme ci-dessous

```
root@server:~  
Fichier Édition Affichage Rechercher Terminal Aide  
  
Taille totale des téléchargements : 15 k  
Taille d'installation : 24 k  
Downloading packages:  
attention : /var/cache/yum/x86_64/7/extras/packages/epel-release-7-11.noarch.rpm: Entête V3 RSA/SHA256 Signature, clé ID f4a80eb5: NOKEY  
La clé publique pour epel-release-7-11.noarch.rpm n'est pas installée  
epel-release-7-11.noarch.rpm | 15 kB 00:00:01  
Récupération de la clé à partir de file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7  
Importation de la clef GPG 0xF4A80EB5 :  
ID utilisateur : « CentOS-7 Key (CentOS 7 Official Signing Key) <security@centos.org> »  
Empreinte : 6341 ab27 53d7 8a78 a7c2 7bb1 24c6 a8a7 f4a8 0eb5  
Paquet : centos-release-7-5.1804.el7.centos.x86_64 (@anaconda)  
Provient de : /etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7  
Running transaction check  
Running transaction test  
Transaction test succeeded  
Running transaction  
  Installation : epel-release-7-11.noarch 1/1  
    Vérification : epel-release-7-11.noarch 1/1  
  
Installé :  
  epel-release.noarch 0:7-11  
  
Terminé !  
[root@server ~]#
```

Une fois cette commande terminée. Nous devons également installer les paquets « Openvpn et easy-rsa » pour générer les paires de clés SSL que nous utiliserons pour sécuriser la connexion VPN :

```
root@server:~  
Fichier Édition Affichage Rechercher Terminal Aide  
[root@server ~]# yum install openvpn easy-rsa net-tools bridge-utils -y
```

Vous obtiendrez l'écran comme ci-dessous :

```
root@server:~ Fichier Édition Affichage Rechercher Terminal Aide
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installation : pkcs11-helper-1.11-3.el7.x86_64 1/5
  Installation : openvpn-2.4.11-1.el7.x86_64 2/5
  Installation : easy-rsa-3.0.8-1.el7.noarch 3/5
  Mise à jour : net-tools-2.0-0.25.20131004git.el7.x86_64 4/5
  Nettoyage   : net-tools-2.0-0.22.20131004git.el7.x86_64 5/5
  Vérification : net-tools-2.0-0.25.20131004git.el7.x86_64 1/5
  Vérification : easy-rsa-3.0.8-1.el7.noarch 2/5
  Vérification : openvpn-2.4.11-1.el7.x86_64 3/5
  Vérification : pkcs11-helper-1.11-3.el7.x86_64 4/5
  Vérification : net-tools-2.0-0.22.20131004git.el7.x86_64 5/5

[Installé :
  easy-rsa.noarch 0:3.0.8-1.el7           openvpn.x86_64 0:2.4.11-1.el7

]Dépendances installées :
  pkcs11-helper.x86_64 0:1.11-3.el7

[Mis à jour :
  net-tools.x86_64 0:2.0-0.25.20131004git.el7

Terminé !
[root@server ~]#
```

Il faut se positionner dans répertoire « 3 » avec la commande : cd /usr/share/easy-rsa/3

```
root@server:/usr/share/easy-rsa/3 Fichier Édition Affichage Rechercher Terminal Aide
[root@server ~]# cd /usr/share/easy-rsa/3
[root@server 3]#
```

Après avoir positionné dans répertoire il faut initialiser le « PKI » avec la commande suivante :

```
root@server:/usr/share/easy-rsa/3 Fichier Édition Affichage Rechercher Terminal Aide
[root@server 3]# ./easyrsa init-pki

init-pki complete; you may now create a CA or requests.
Your newly created PKI dir is: /usr/share/easy-rsa/3/pki

[root@server 3]#
```

Création de certificat d'autorité avec la commande « ./easyrsa build-ca » et il va vous demander de saisir Passphrase et vous saisissez le mot de passe

```
root@server:/usr/share/easy-rsa/3
Fichier Édition Affichage Rechercher Terminal Aide
[root@server 3]# ./easyrsa build-ca
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]:
CA creation complete and you may now import and sign cert requests.
Your new CA certificate file for publishing is at:
/usr/share/easy-rsa/3/pki/ca.crt

[root@server 3]#
```

Le certificat d'autorité a été bien créé.

La capture ci-dessous nous montre la création de certificat pour le serveur.

```
root@server:/usr/share/easy-rsa/3
Fichier Édition Affichage Rechercher Terminal Aide
[root@server 3]# ./easyrsa build-server-full server nopass
Using SSL: openssl OpenSSL 1.0.2k-fips 26 Jan 2017
Generating a 2048 bit RSA private key
.....++++
.....+++
.....+++
writing new private key to '/usr/share/easy-rsa/3/pki/easy-rsa-5121.PfTCXR/tmp.Yes9oC'
-----
Using configuration from /usr/share/easy-rsa/3/pki/easy-rsa-5121.PfTCXR/tmp.XxqcQk
Enter pass phrase for /usr/share/easy-rsa/3/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:'server'
Certificate is to be certified until Nov 23 01:26:41 2023 GMT (825 days)

Write out database with 1 new entries
Data Base Updated

[root@server 3]#
```

La création de certificat pour le client

```
root@server:/usr/share/easy-rsa/3
Fichier Édition Affichage Rechercher Terminal Aide
[root@server 3]# ./easyrsa build-client-full client nopass
Using SSL: openssl OpenSSL 1.0.2k-fips 26 Jan 2017
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to '/usr/share/easy-rsa/3/pki/easy-rsa-5289.7VUIZh/tmp.L3R37n'
-----
Using configuration from /usr/share/easy-rsa/3/pki/easy-rsa-5289.7VUIZh/tmp.ZEqd4k
Enter pass phrase for /usr/share/easy-rsa/3/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 Nov 23 01:29:38 2023 GMT (825 days)

Write out database with 1 new entries
Data Base Updated

[root@server 3]#
```

Générer le paramètre de Diffie-Hellman avec la commande suivante :

Création de la clé av

```
Fichier Édition Affichage Rechercher Terminal Aide
[root@server 3]# openvpn --genkey --secret ./pki/ta.key
[root@server 3]#
```

Copiez les certificats dans le répertoire « /etc/openvpn/server/ »

```
root@server:/usr/share/easy-rsa/3 - □ ×
Fichier Édition Affichage Rechercher Terminal Aide
[root@server 3]# cp -pR /usr/share/easy-rsa/3/pki/{issued,private,ca.crt,dh.pem,ta.key}
/etc/openvpn/server/
[root@server 3]#
```

La capture ci-dessous nous montre l'activation de routage

```
root@server:/usr/share/easy-rsa/3
Fichier Édition Affichage Rechercher Terminal Aide
[root@server 3]# vi /etc/sysctl.d/10-ipv4_forward.conf
```

Après avoir édité le fichier « 10-ipv4_forward.conf » puis ajouté ce code « net.ipv4.ip_forward=1 »

```
root@server:/usr/share/easy-rsa/3
Fichier Édition Affichage Rechercher Terminal Aide
net.ipv4.ip_forward = 1
```

Activez le routage avec la commande « sysctl –system »

```
root@server:/usr/share/easy-rsa/3
Fichier Édition Affichage Rechercher Terminal Aide
[root@server 3]# sysctl --system
* Applying /usr/lib/sysctl.d/00-system.conf ...
* Applying /usr/lib/sysctl.d/10-default-yama-scope.conf ...
kernel.yama.ptrace_scope = 0
* Applying /etc/sysctl.d/10-ipv4_forward.conf ...
net.ipv4.ip_forward = 1
* Applying /usr/lib/sysctl.d/50-default.conf ...
kernel.sysrq = 16
kernel.core_uses_pid = 1
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.accept_source_route = 0
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.default.promote_secondaries = 1
net.ipv4.conf.all.promote_secondaries = 1
fs.protected_hardlinks = 1
fs.protected_symlinks = 1
* Applying /usr/lib/sysctl.d/60-libvirtd.conf ...
fs.aio-max-nr = 1048576
* Applying /etc/sysctl.d/99-sysctl.conf ...
* Applying /etc/sysctl.conf ...
[root@server 3]#
```

Copiez le fichier de configuration dans /etc/openvpn/server/server.conf

```
root@server:/usr/share/easy-rsa/3
Fichier Édition Affichage Rechercher Terminal Aide
[root@server 3]# cp /usr/share/doc/openvpn-2.4.11/sample/sample-config-files/server.conf /etc/openvpn/server/server.conf
[root@server 3]#
```

Après avoir terminé la copie passons l'édition du fichier de configuration avec la commande suivante :

Vi /etc/openvpn/server/server.conf

```
root@server:/usr/share/easy-rsa/3
Fichier Édition Affichage Rechercher Terminal Aide
[root@server 3]# vi /etc/openvpn/server/server.conf
```

Vous obtiendrez comme l'écran ci-dessous

```
root@server:/usr/share/easy-rsa/3
Fichier Édition Affichage Rechercher Terminal Aide
1 #####
2 # Sample OpenVPN 2.0 config file for #
3 # multi-client server. #
4 #
5 # This file is for the server side #
6 # of a many-clients <-> one-server #
7 # OpenVPN configuration. #
8 #
9 # OpenVPN also supports #
10 # single-machine <-> single-machine #
11 # configurations (See the Examples page #
12 # on the web site for more info). #
13 #
14 # This config should work on Windows #
15 # or Linux/BSD systems. Remember on #
16 # Windows to quote pathnames and use #
17 # double backslashes, e.g.: #
18 # "C:\\\\Program Files\\\\OpenVPN\\\\config\\\\foo.key" #
19 #
20 # Comments are preceded with '#' or ';' #
21 #####
22
23 # Which local IP address should OpenVPN
24 # listen on? (optional)
~
```

Repérez la ligne 79 vous mettez « cert issued/server.crt » la ligne 80 « key private/server.key » et la ligne 85 « dh dh.pem »

```
root@server:/usr/share/easy-rsa/3
Fichier Édition Affichage Rechercher Terminal Aide
75 # Any X509 key management system can be used.
76 # OpenVPN can also use a PKCS #12 formatted key file
77 # (see "pkcs12" directive in man page).
78 ca ca.crt
79 cert issued/server.crt
80 key private/server.key # This file should be kept secret
81
82 # Diffie hellman parameters.
83 # Generate your own with:
84 # openssl dhparam -out dh2048.pem 2048
85 dh dh.pem
```

Repérez la ligne 101 puis déclarez votre adresse virtuelle « server 172.16.0.0 255.255.255.0 »

```
root@server:/usr/share/easy-rsa/3
Fichier Édition Affichage Rechercher Terminal Aide
94 # Configure server mode and supply a VPN subnet
95 # for OpenVPN to draw client addresses from.
96 # The server will take 10.8.0.1 for itself,
97 # the rest will be made available to clients.
98 # Each client will be able to reach the server
99 # on 10.8.0.1. Comment this line out if you are
100 # ethernet bridging. See the man page for more info.
101 server 172.16.0.0 255.255.255.0
```

Repérez la ligne 142 puis définir votre adresse réseau et le masque

```
root@server:/usr/share/easy-rsa/3
Fichier Édition Affichage Rechercher Terminal Aide
133
134 # Push routes to the client to allow it
135 # to reach other private subnets behind
136 # the server. Remember that these
137 # private subnets will also need
138 # to know to route the OpenVPN client
139 # address pool (10.8.0.0/255.255.255.0)
140 # back to the OpenVPN server.
141 ;push "route 192.168.10.0 255.255.255.0"
142 push "route 192.168.1.0 255.255.255.0"
```

Repérez la ligne 263 puis de commenter

```
260 # For compression compatible with older clients use comp-lzo
261 # If you enable it here, you must also
262 # enable it in the client config file.
263 comp-lzo
```

Repérez la ligne 287,296 et la ligne 297 c'est par rapport à la journalisation.

```
Fichier Édition Affichage Rechercher Terminal Aide
284 # Output a short status file showing
285 # current connections, truncated
286 # and rewritten every minute.
287 status /var/log/openvpn-status.log
288
289 # By default, log messages will go to the syslog (or
290 # on Windows, if running as a service, they will go to
291 # the "\Program Files\OpenVPN\log" directory).
292 # Use log or log-append to override this default.
293 # "log" will truncate the log file on OpenVPN startup,
294 # while "log-append" will append to it. Use one
295 # or the other (but not both)
296 log      /var/log/openvpn.log
297 log-append /var/log/openvpn.log
```

Redémarrez le service « openvpn » avec la commande suivante :

```
root@server:/usr/share/easy-rsa/3
Fichier Édition Affichage Rechercher Terminal Aide
[root@server 3]# systemctl start openvpn-server@server
[root@server 3]#
```

Activez le service au démarrage avec la commande « systemctl enable openvpn-server@server »

```
root@server:/usr/share/easy-rsa/3
Fichier Édition Affichage Rechercher Terminal Aide
[root@server 3]# 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@server 3]#
```

Ajoutez le service dans le pare-feu

```
root@server:/usr/share/easy-rsa/3
Fichier Édition Affichage Rechercher Terminal Aide
[root@server 3]# firewall-cmd --add-port=1194/udp --permanent
success
[root@server 3]# firewall-cmd --reload
success
[root@server 3]#
```

Vérification l'état du service

```
root@server:/usr/share/easy-rsa/3
Fichier Édition Affichage Rechercher Terminal Aide
[root@server 3]# systemctl status openvpn-server@server
● openvpn-server@server.service - OpenVPN service for server
   Loaded: loaded (/usr/lib/systemd/system/openvpn-server@.service; enabled; vendor pre
   set: disabled)
     Active: active (running) since ven. 2021-08-20 05:24:46 GMT; 6min ago
       Docs: man:openvpn(8)
              https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage
              https://community.openvpn.net/openvpn/wiki/HOWTO
     Main PID: 520 (openvpn)
        Status: "Initialization Sequence Completed"
       CGroub: /system.slice/system-openvpn\x2dserver.slice/openvpn-server@server.service
              └─520 /usr/sbin/openvpn --status /run/openvpn-server/status-server.log ----
août 20 05:24:46 server systemd[1]: Starting OpenVPN service for server...
août 20 05:24:46 server systemd[1]: Started OpenVPN service for server.
[root@server 3]#
```

Configuration le service SSH

```
root@server:/usr/share/easy-rsa/3
Fichier Édition Affichage Rechercher Terminal Aide
[root@server 3]# vi /etc/ssh/sshd_config
```

Repérez la ligne 17 puis de commenter

```
17 Port 22
18 #AddressFamily any
19 #ListenAddress 0.0.0.0
20 #ListenAddress ::
```

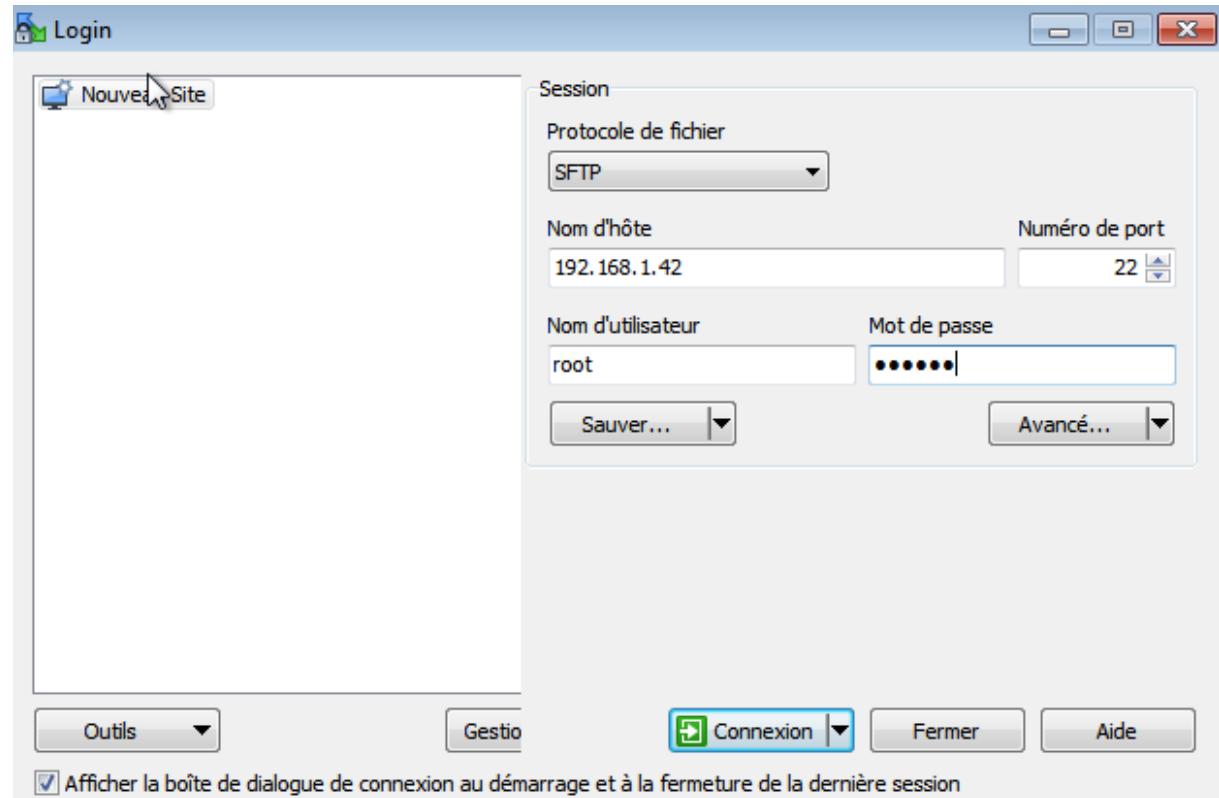
Repérez la ligne 38 puis de commenter

```
37 #LoginGraceTime 2m
38 PermitRootLogin yes
39 #StrictModes yes
40 #MaxAuthTries 6
41 #MaxSessions 10
```

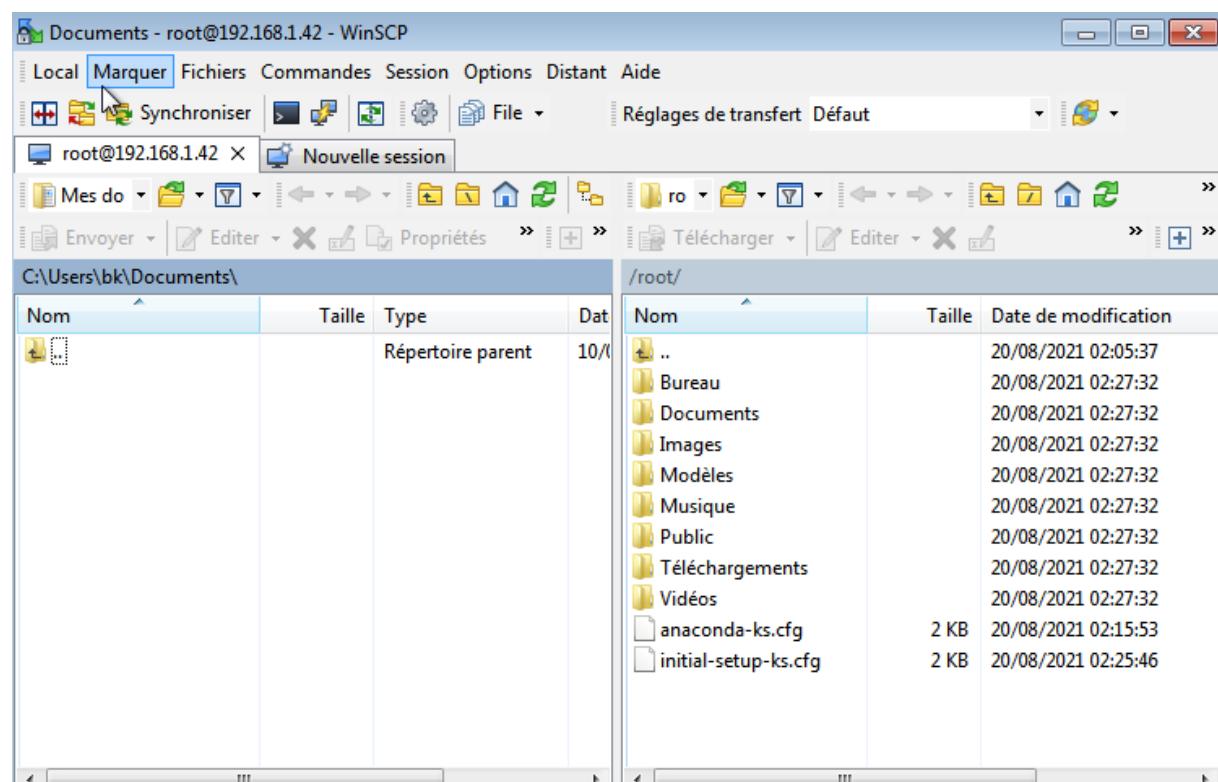
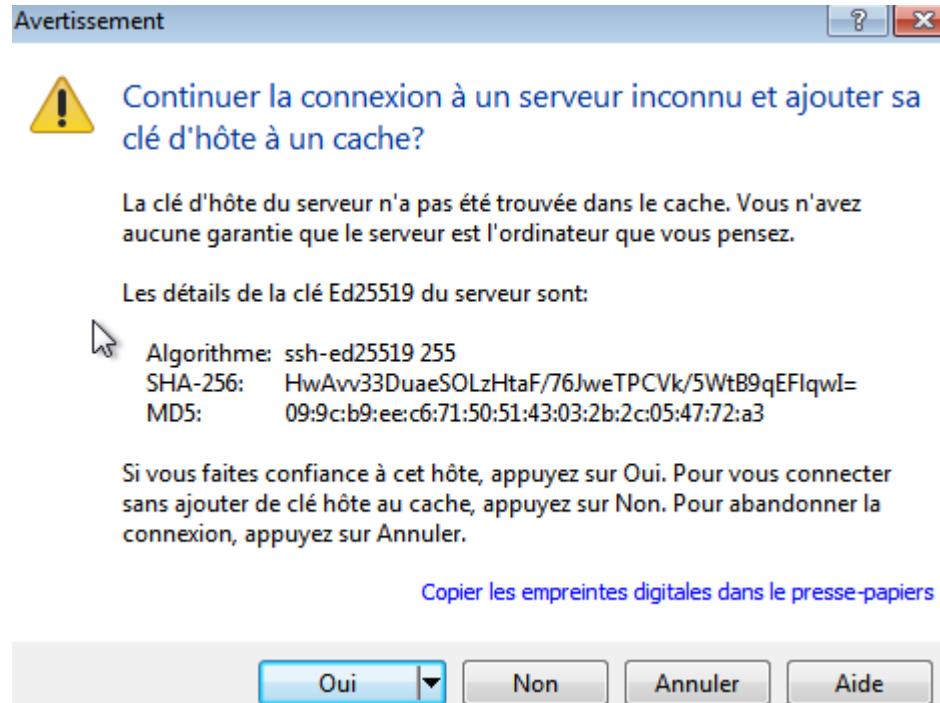
Redémarrez le service SSH avec la commande « systemctl restart sshd »

```
root@server:/usr/share/easy-rsa/3
Fichier Édition Affichage Rechercher Terminal Aide
[root@server 3]# systemctl restart sshd
[root@server 3]# systemctl enable sshd
[root@server 3]# firewall-cmd --add-service=ssh --permanent
```

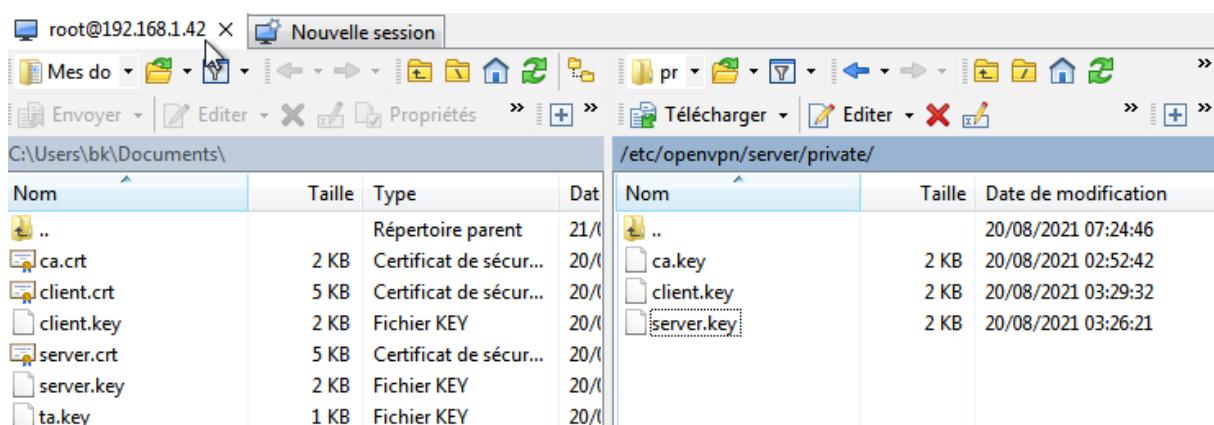
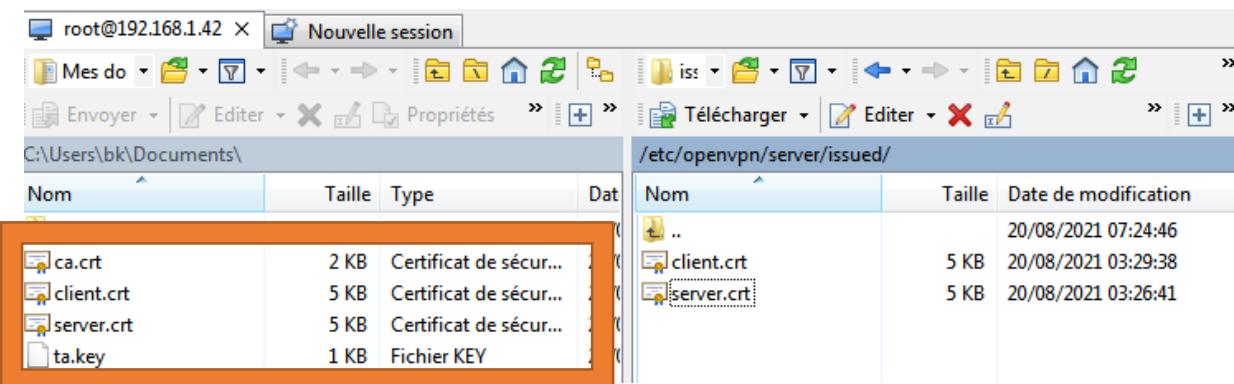
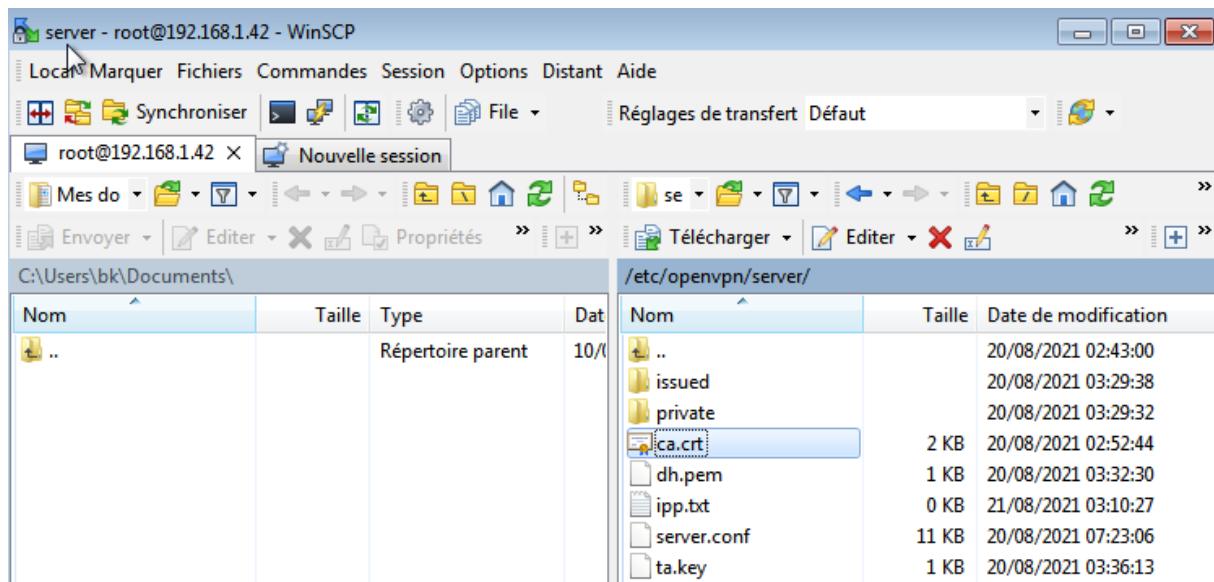
Allez sur la machine client connectez avec un logiciel WinSCP



Une fois connectée vous obtiendrez l'écran ci-dessous



Copiez les certificats et les clés sur la machine cliente



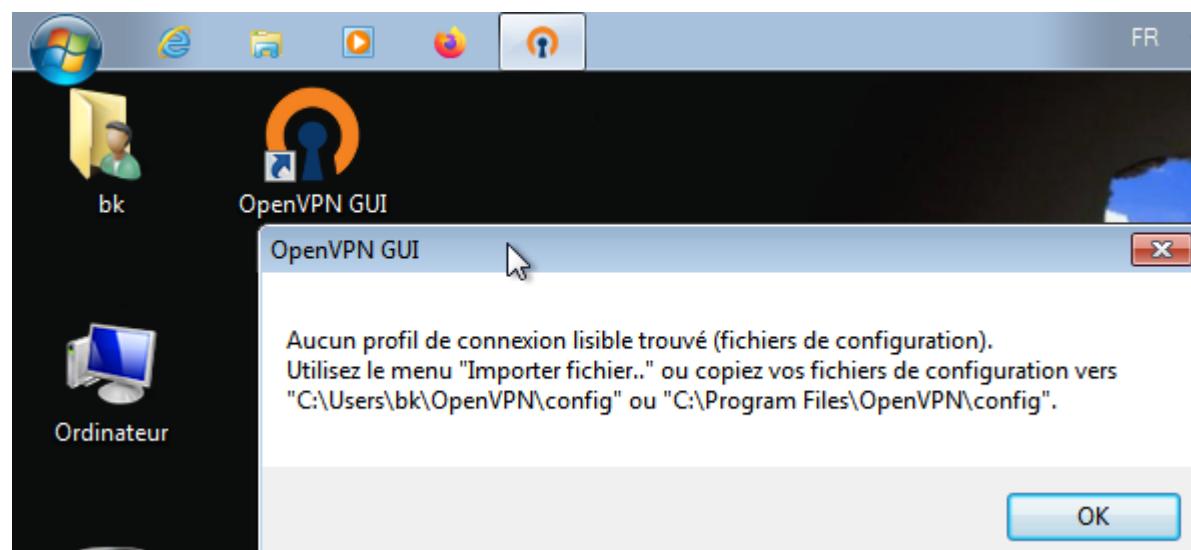
Les fichiers copiés se trouvent dans le dossier Documents sur la capture suivante :

Bibliothèque Documents			
Inclut : 2 emplacements			
Nom	Modifié le	Type	Taille
ca.crt	20/08/2021 02:52	Certificat de sécur...	2 Ko
client.crt	20/08/2021 03:29	Certificat de sécur...	5 Ko
client.key	20/08/2021 03:29	Fichier KEY	2 Ko
server.crt	20/08/2021 03:26	Certificat de sécur...	5 Ko
server.key	20/08/2021 03:26	Fichier KEY	2 Ko
ta.key	20/08/2021 03:36	Fichier KEY	1 Ko

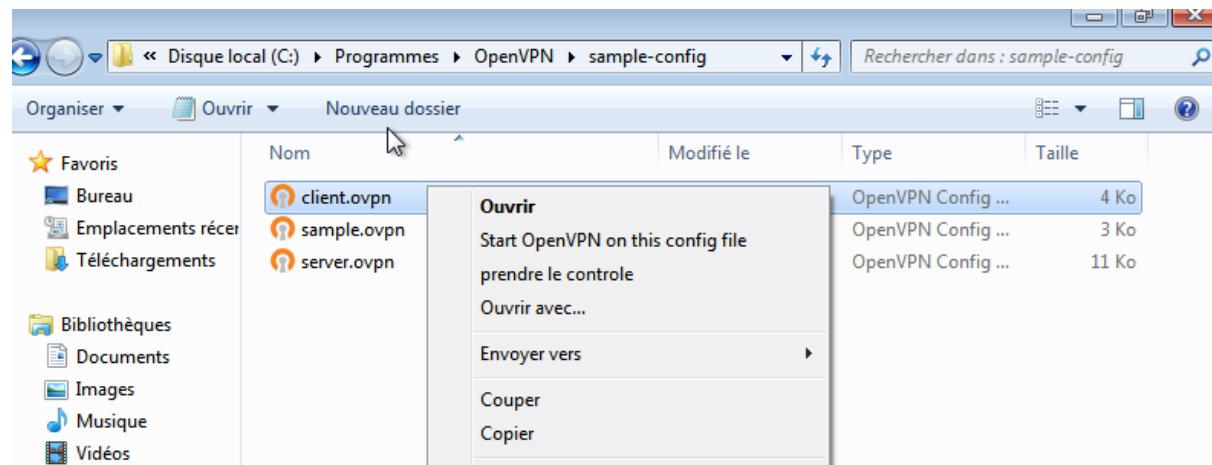
L'installation de logiciel « OpenVPN » au niveau du client



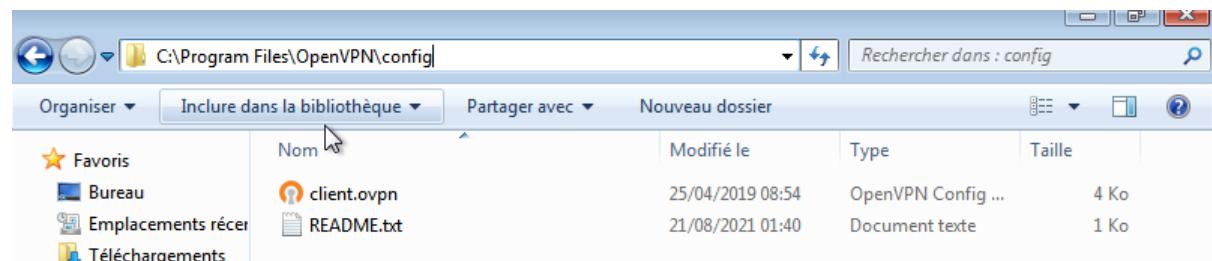
Après avoir terminé l'installation « OpenVPN » vous obtiendrez la capture ci-dessous.



Copiez le fichier « client.ovpn »



Collez le fichier « client.ovpn » dans le dossier « config »



Édition du fichier client.ovpn

```

1 #####
2 # Sample client-side OpenVPN 2.0 config file #
3 # for connecting to multi-client server. #
4 #
5 # This configuration can be used by multiple #
6 # clients, however each client should have #
7 # its own cert and key files. #
8 #
9 # On Windows, you might want to rename this #
10 # file so it has a .ovpn extension #
11 #####
12
13 # Specify that we are a client and that we
14 # will be pulling certain config file directives
15 # from the server.
16 client
17
18 # Use the same setting as you are using on
19 # the server.
20 # On most systems, the VPN will not function
21 # unless you partially or fully disable
22 # the firewall for the TUN/TAP interface.
23 ;dev tap
24 dev tun

```

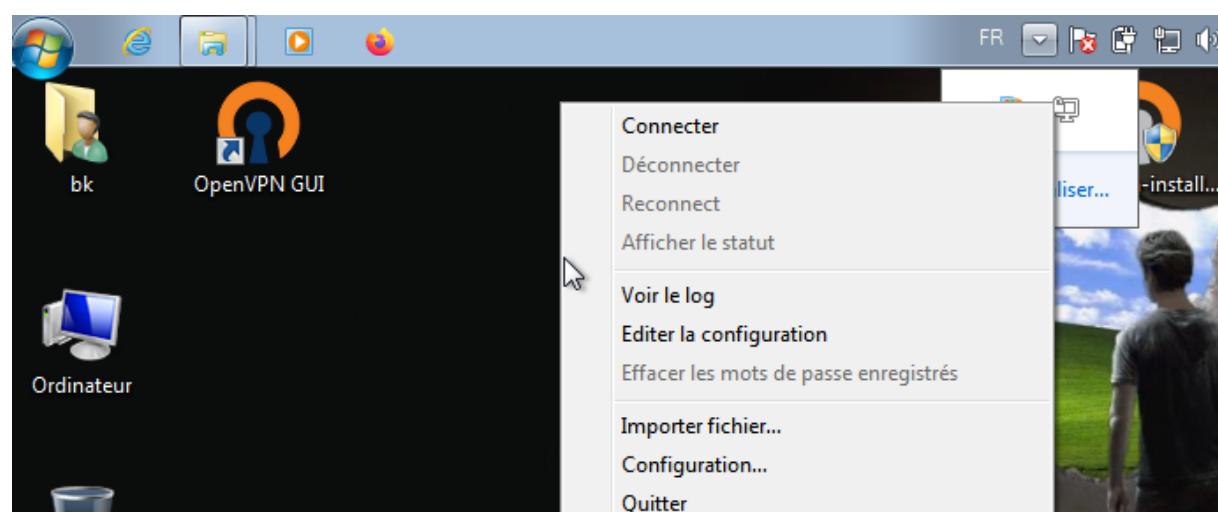
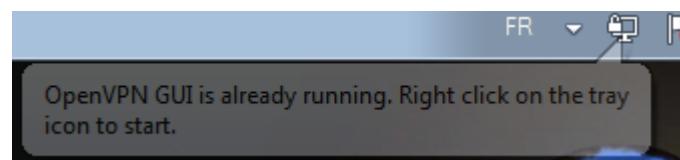
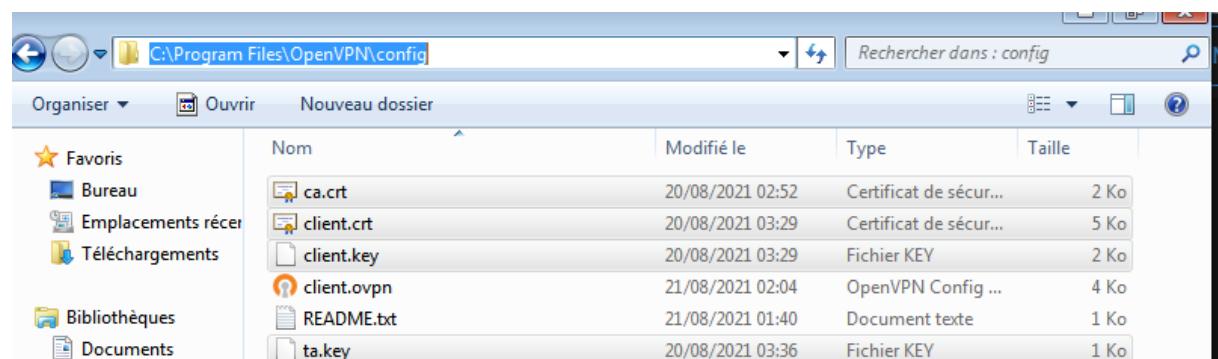
Repérez la ligne 121 puis de commenter

```
118 # Enable compression on the VPN link.
119 # Don't enable this unless it is also
120 # enabled in the server config file.
121 comp-lzo
```

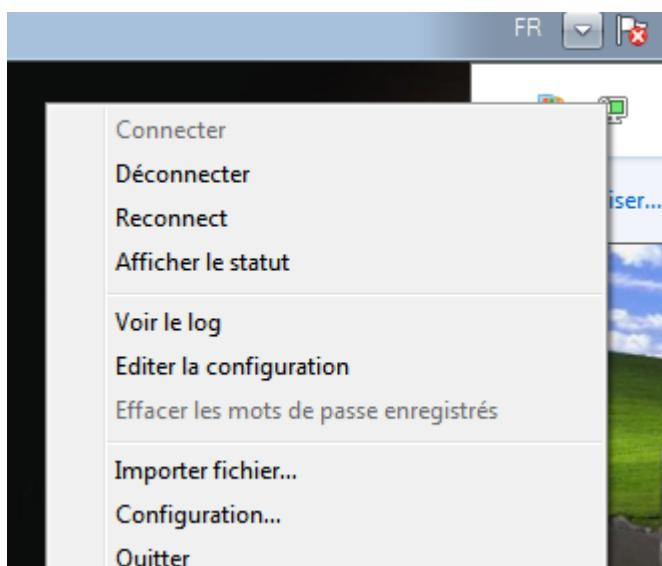
Repérez la ligne 42 puis ajoutez @ IP du serveur

```
38
39 # The hostname/IP and port of the server.
40 # You can have multiple remote entries
41 # to load balance between the servers.
42 remote 192.168.1.42 1194
43 ;remote my-server-2 1194
```

Copiez les certificats et clés dans le dossier config



Le client est maintenant connecté



Dans ce rapport je vous ai montré comment installer et configurer le VPN sur centos7.