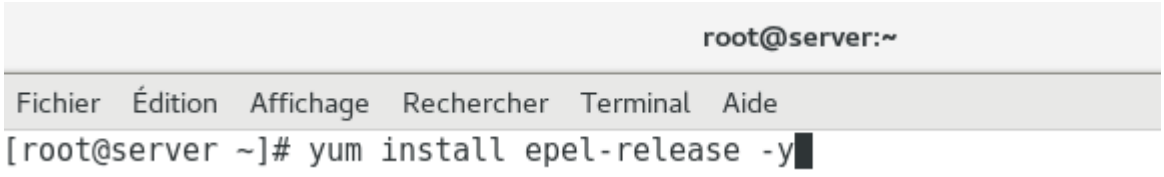
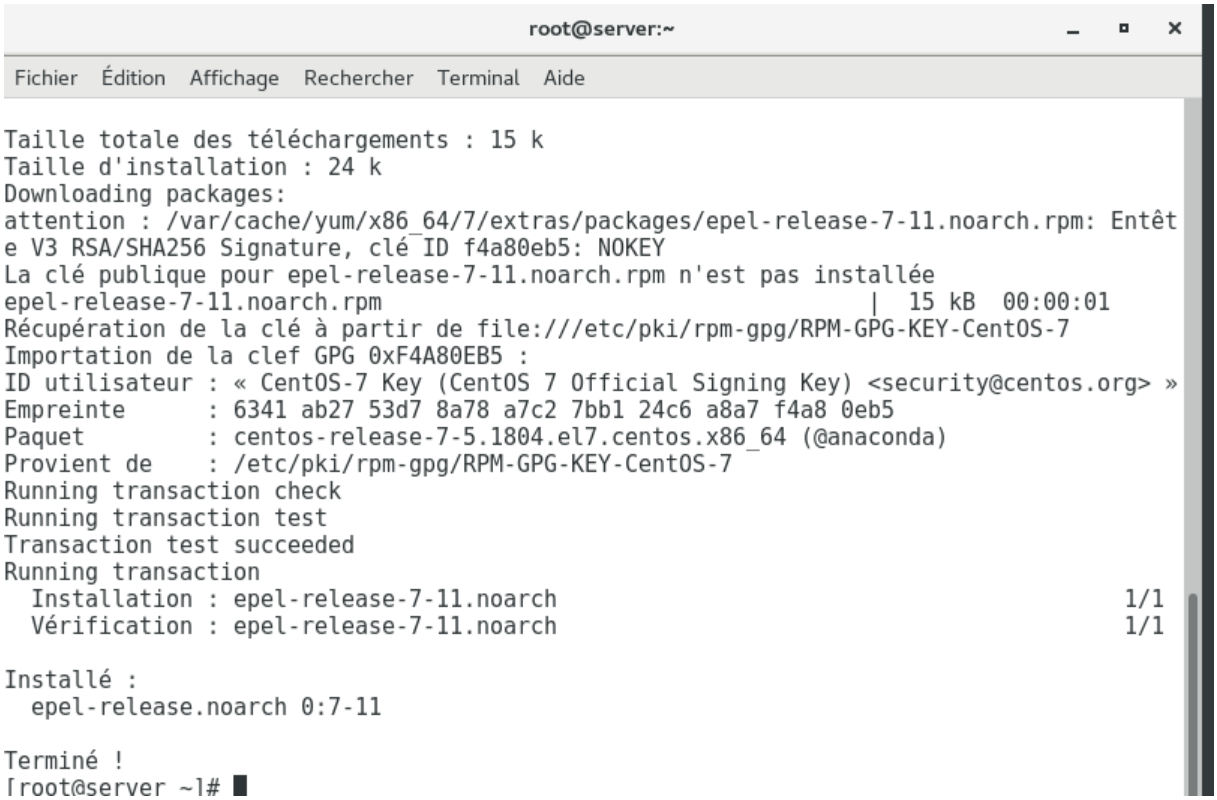
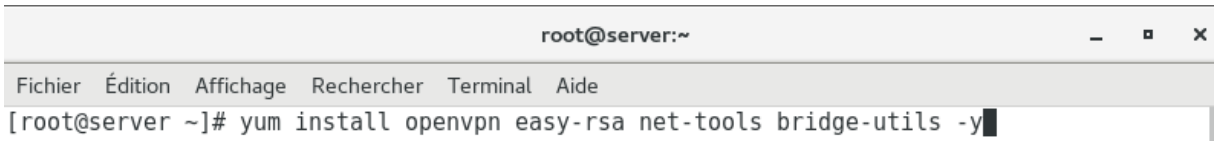
Pour installer le référentiel EPEL, saisissez la commande suivante :



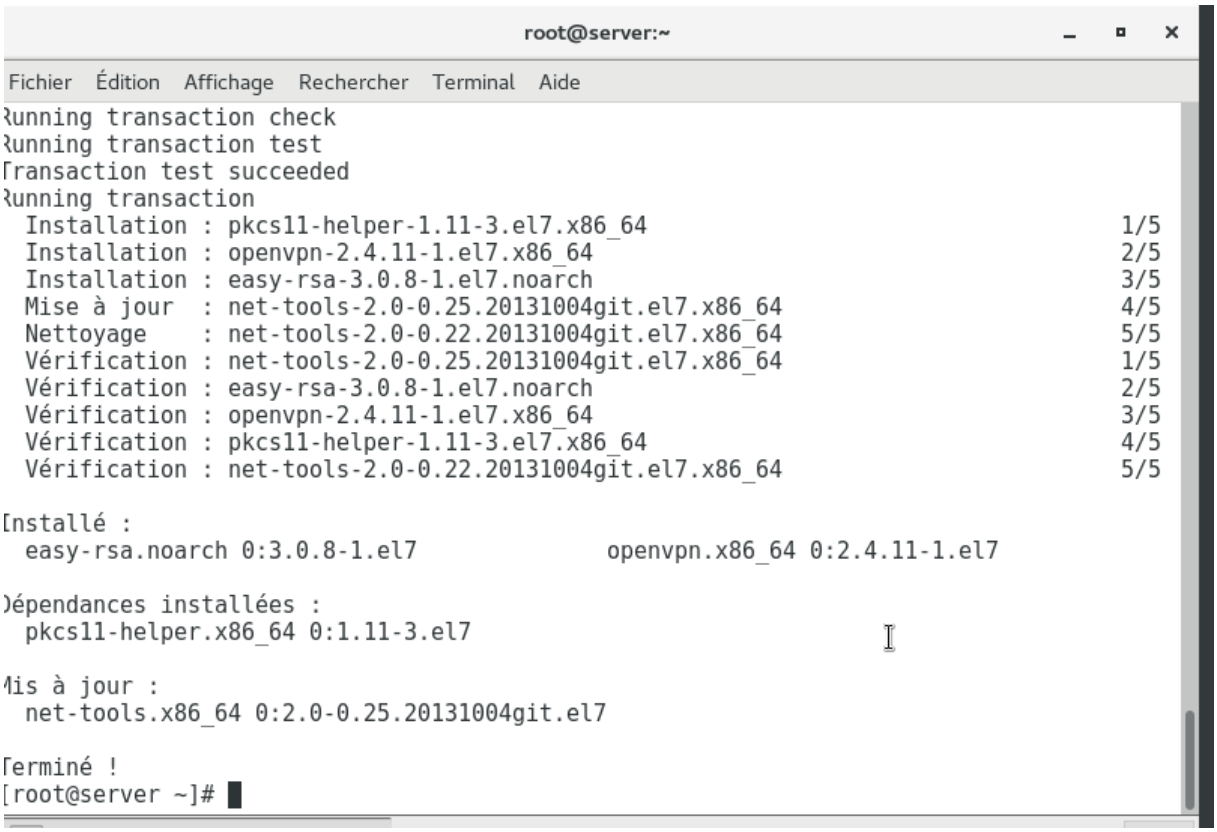
Vous obtiendrez l'écran comme ci-dessous



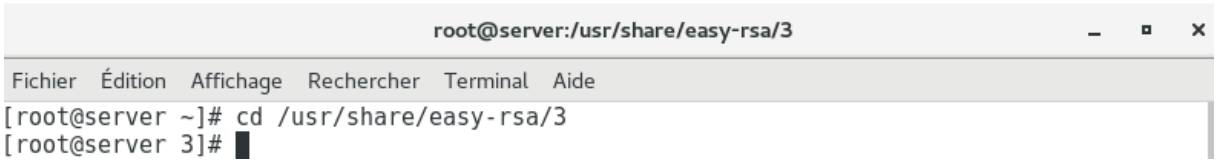
Une fois cette commande terminée. Nous devons également installer les paquets « Openvpn et easy-rsa » pour générer les paires de clés SSL que nous utiliserons pour sécuriser la connexion VPN :



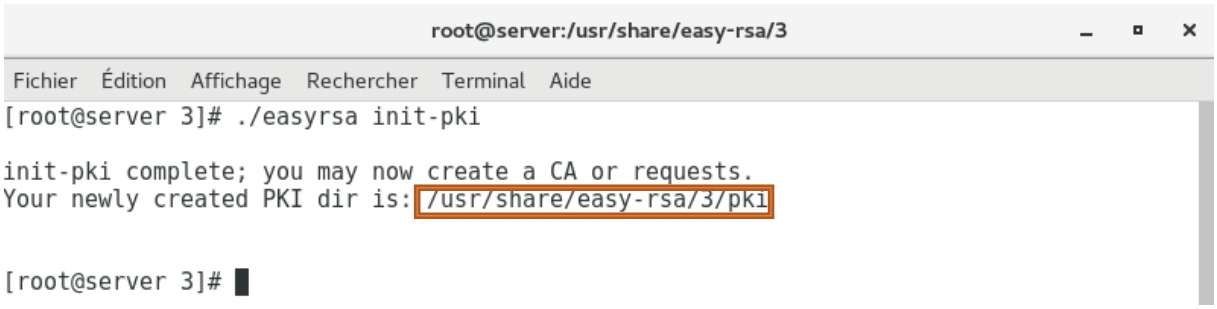
Vous obtiendrez l'écran comme ci-dessous :



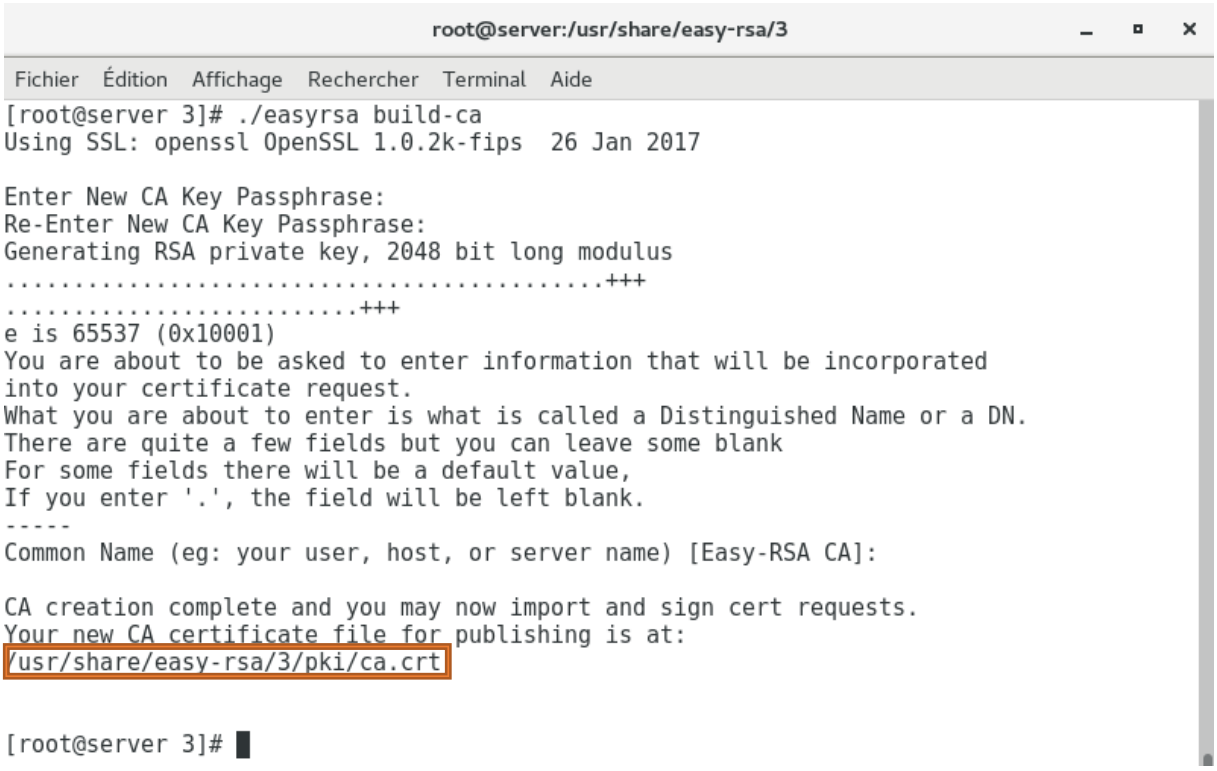
Il faut se positionner dans répertoire « 3 » avec la commande : cd /usr/share/easy-rsa/3



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

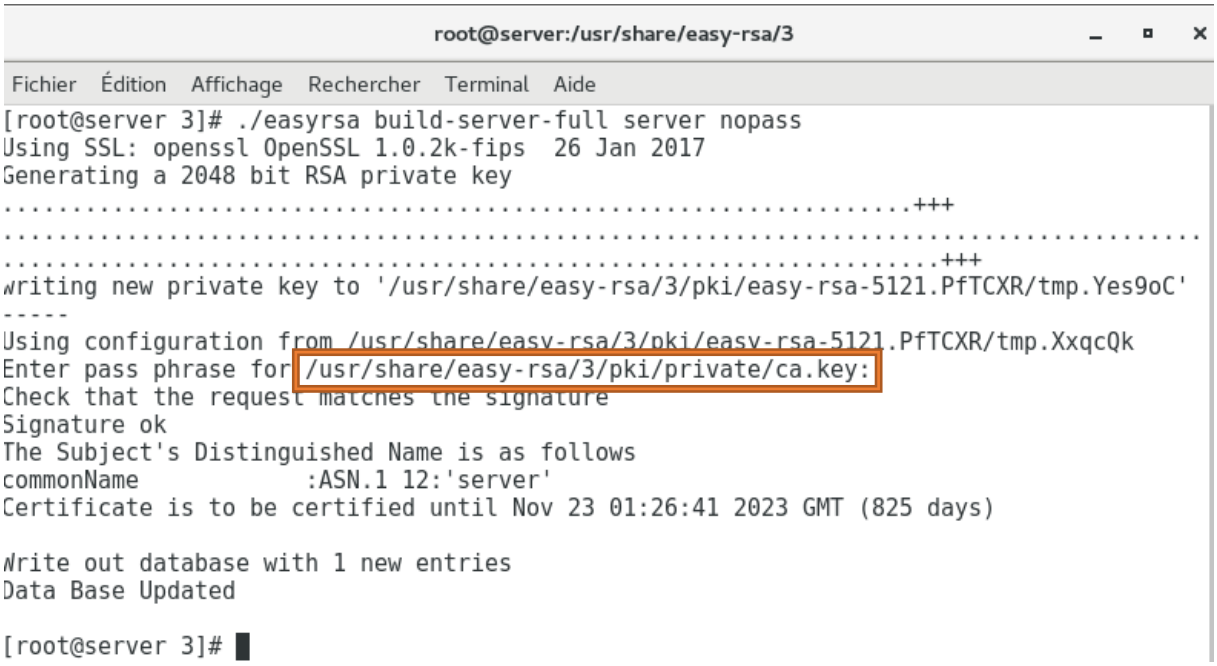


Création de certificat d'autorité avec la commande «. /easyrsa build-ca » et il va vous demander de saisir Passphrase et vous saisissez le mot de passe

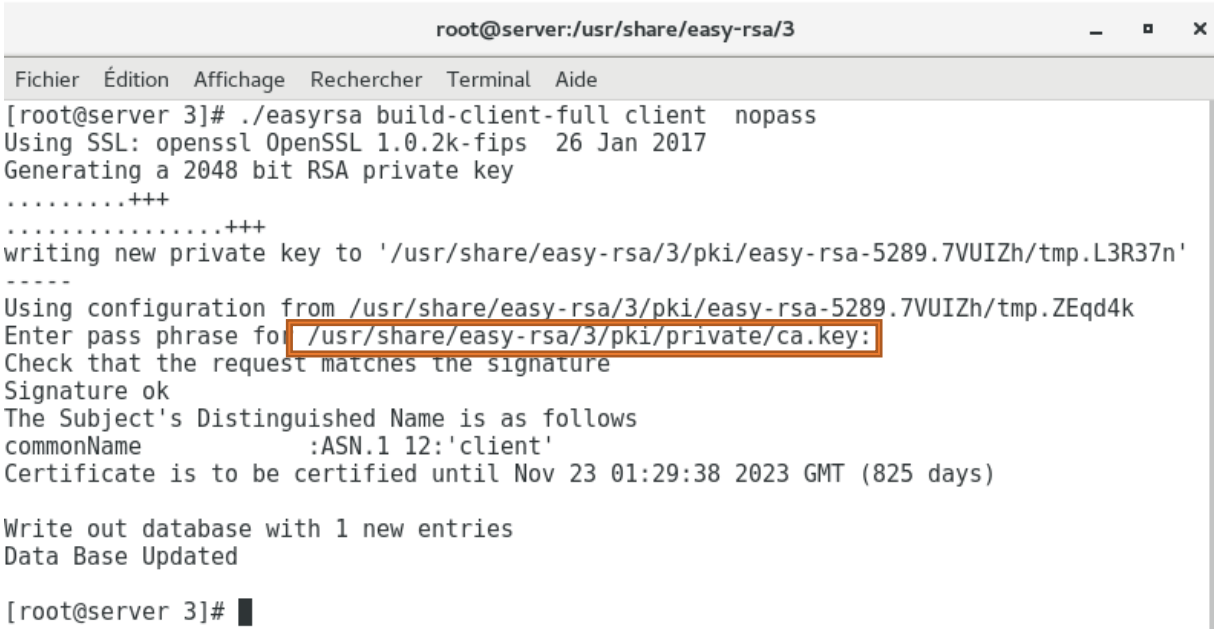


Le certificat d'autorité a été bien crée.

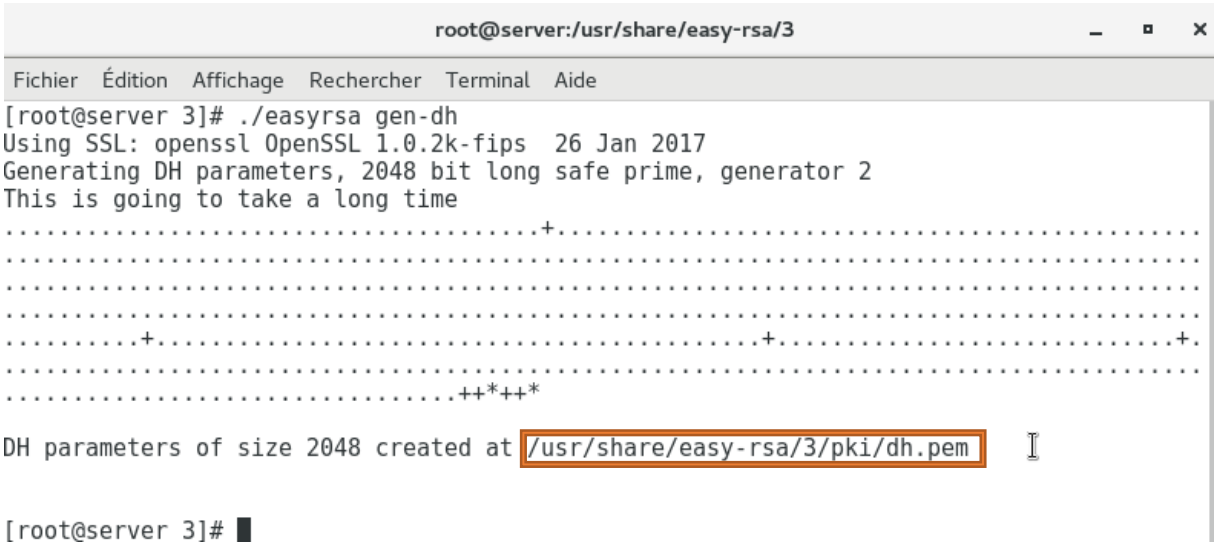
La capture ci-dessous nous montre la création de certificat pour le serveur.



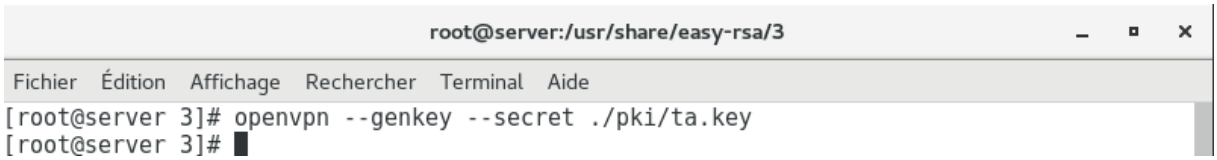
La création de certificat pour le client



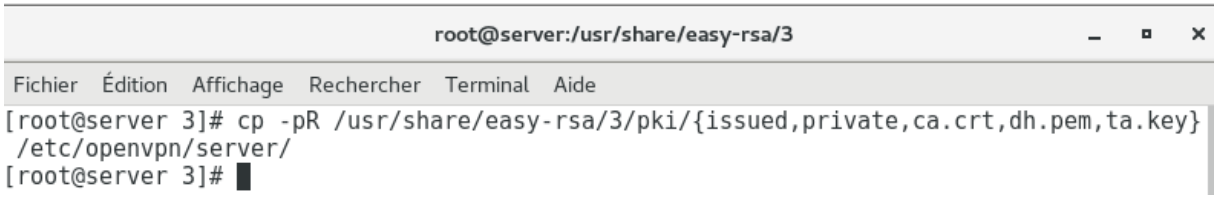
Générer le paramètre de Diffie-Hellman avec la commande suivante :



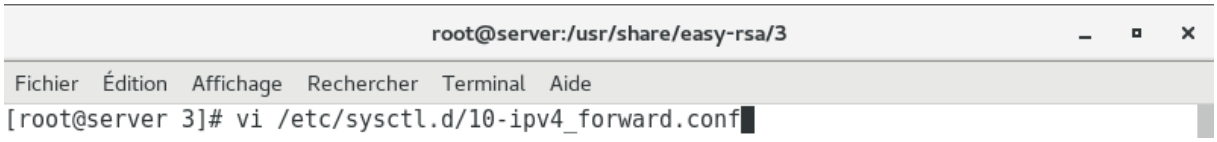
Création de la clé avec la commande suivante :



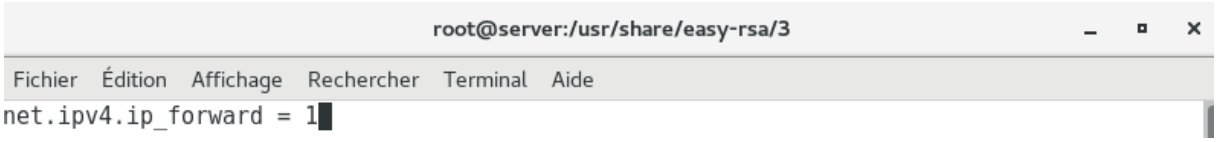
Copiez les certificats dans le répertoire « /etc/openvpn/server/ »



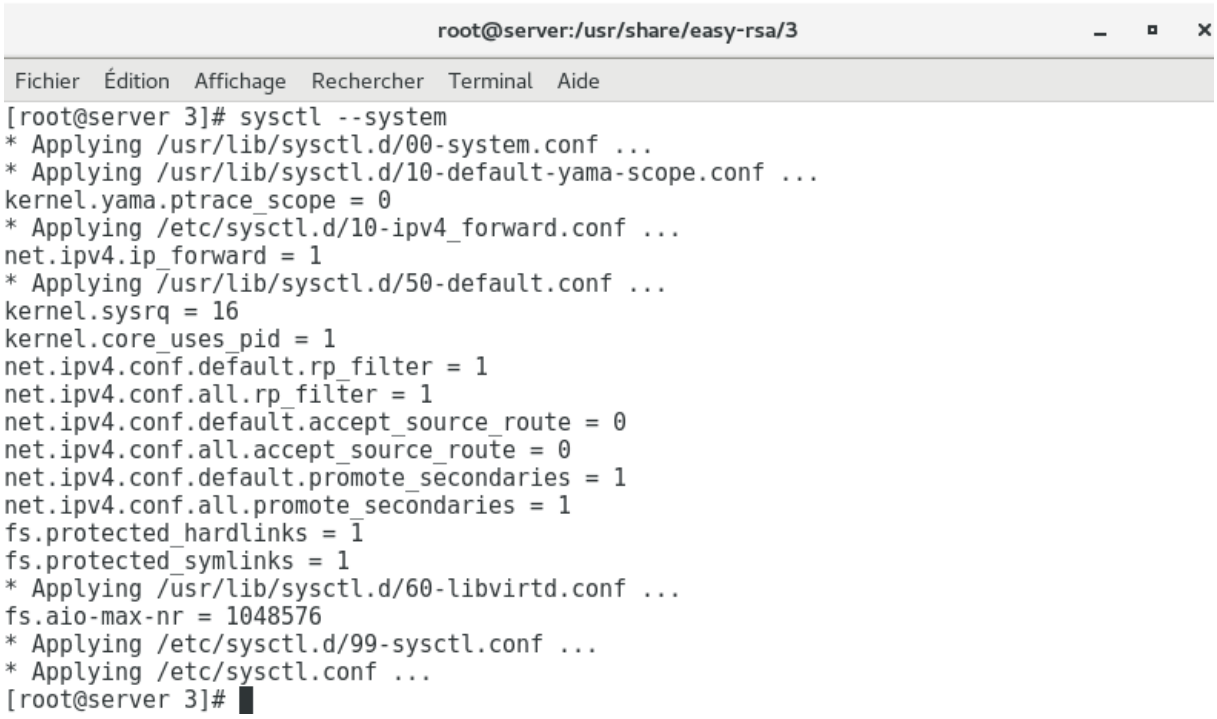
La capture ci-dessous nous montre l'activation de routage



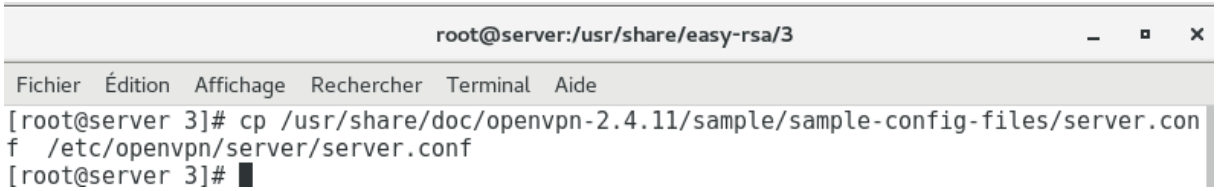
Après avoir édité le fichier « 10-ipv4_forward.conf » puis ajouté ce code « net.ipv4.ip_forward=1 »



Activez le routage avec la commande « sysctl –system »

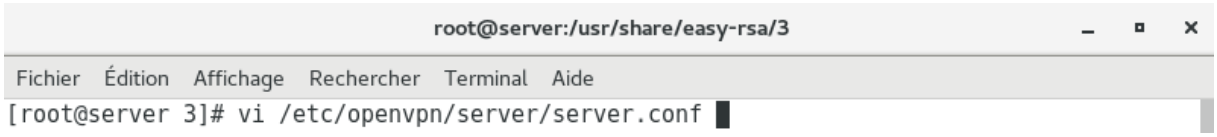


Copiez le fichier de configuration dans /etc/openvpn/server/server.conf

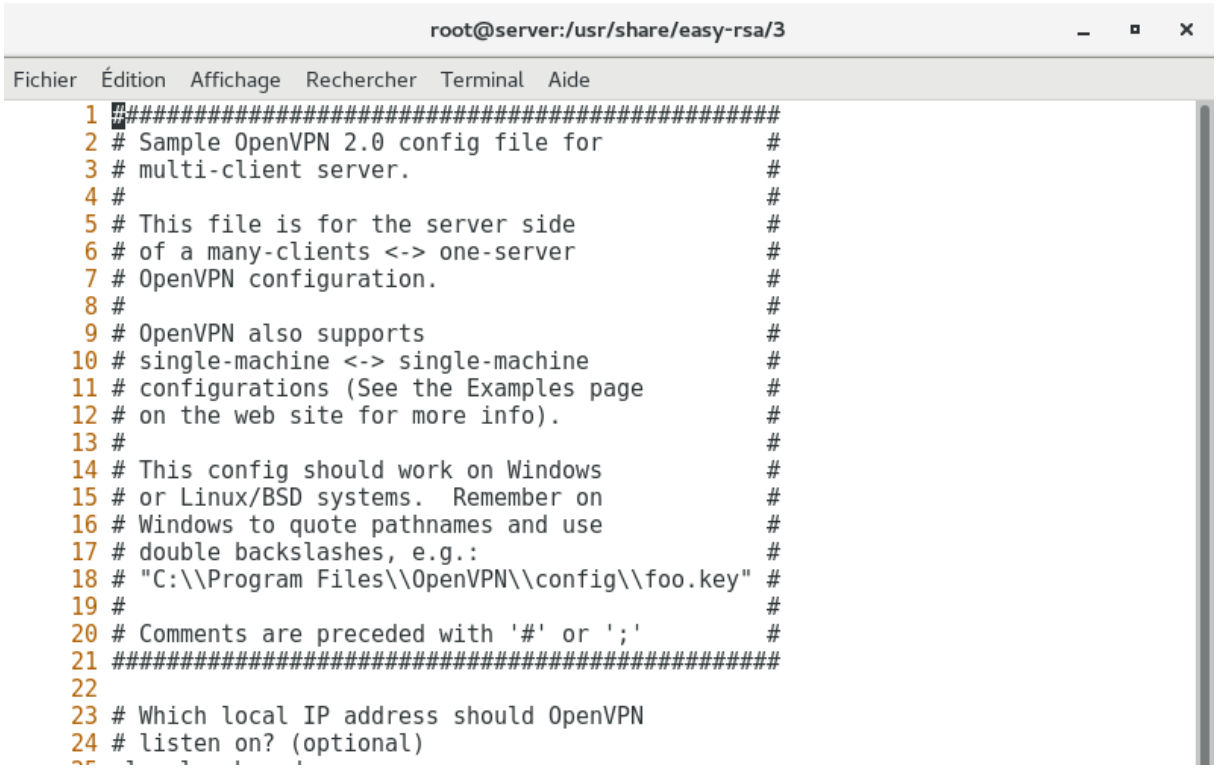


Après avoir terminé la copie passons l'édition du fichier de configuration avec la commande suivante :

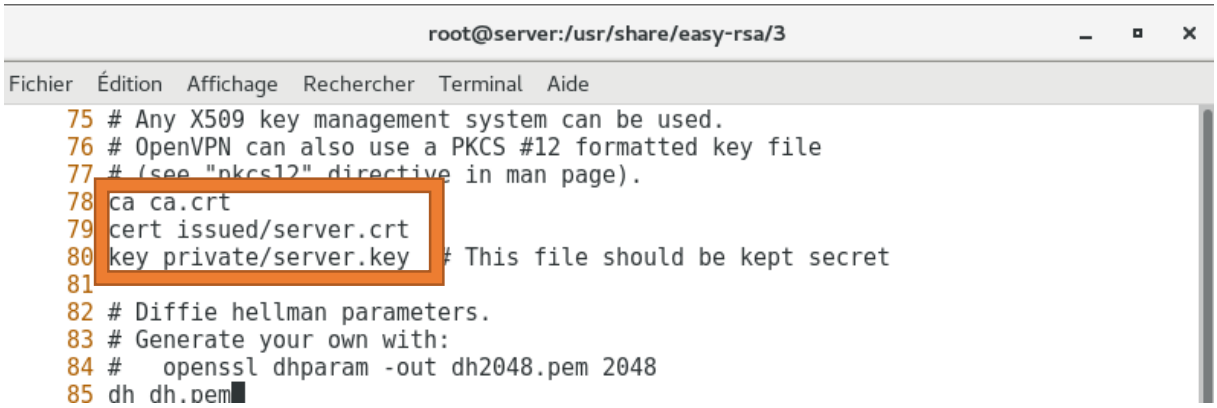
Vi /etc/openvpn/server/server.conf



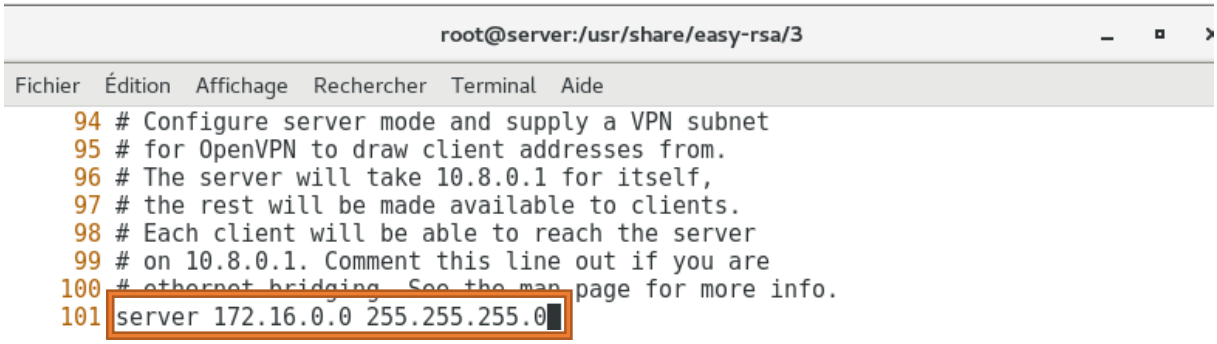
Vous obtiendrez comme l'écran ci-dessous



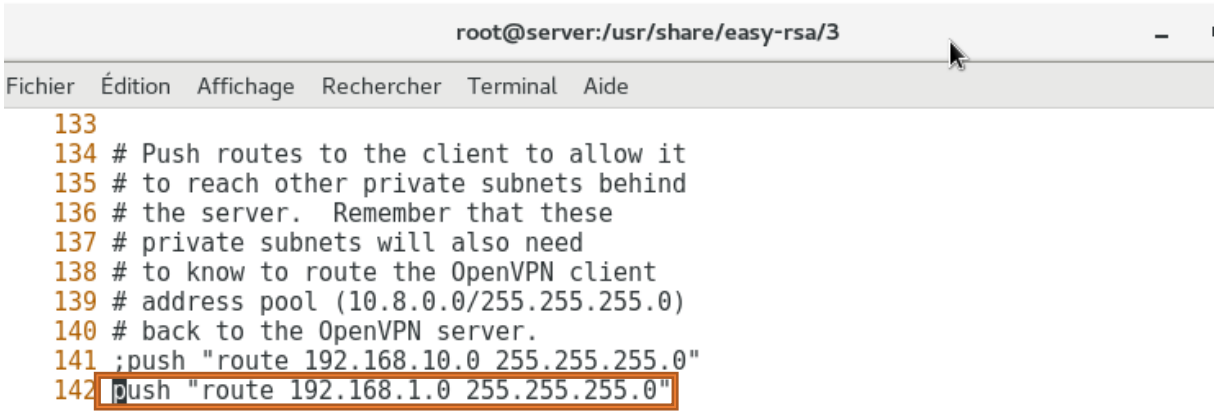
Repérez la ligne 79 vous mettez « cert issued/server.crt » la ligne 80 « key private/server.key » et la ligne 85 « dh dh.pem »



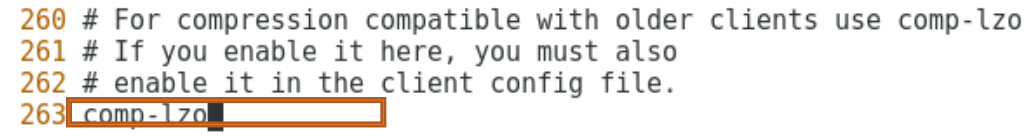
Repérez la ligne 101 puis déclarez votre adresse virtuelle « server 172.16.0.0 255.255.255.0 »



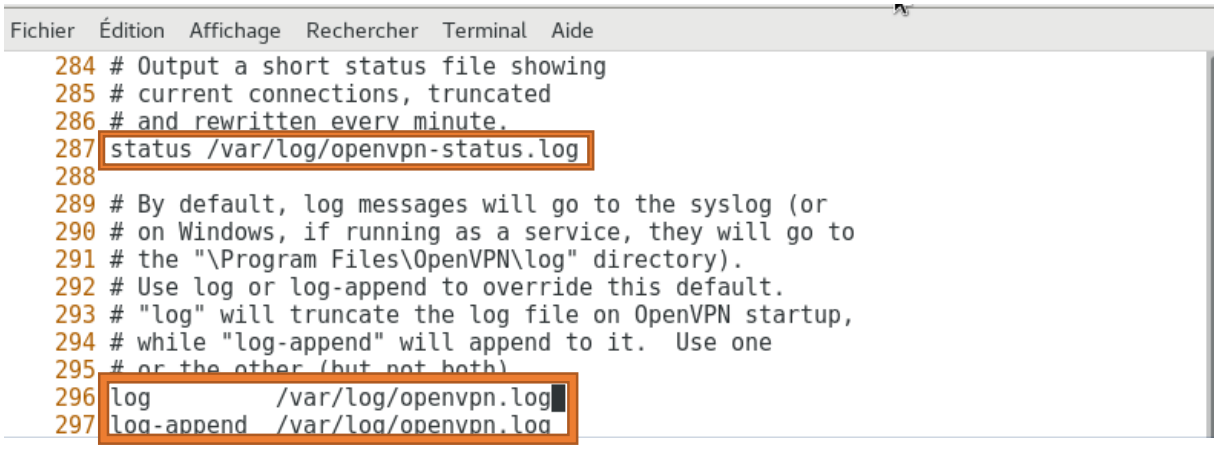
Repérez la ligne 142 puis définir votre adresse reseau et le masque



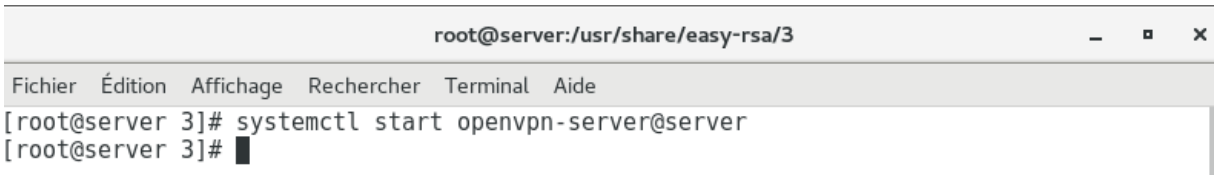
Repérez la ligne 263 puis de commenter



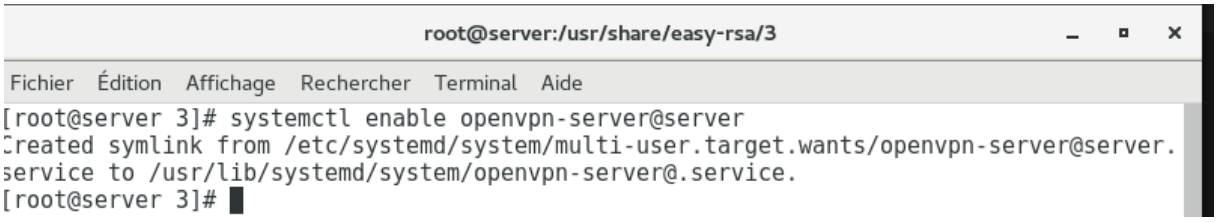
Repérez la ligne 287,296 et la ligne 297 c'est par rapport à la journalisation.



Redémarrez le service « openvpn » avec la commande suivante :



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



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"
   CGroup: /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
```

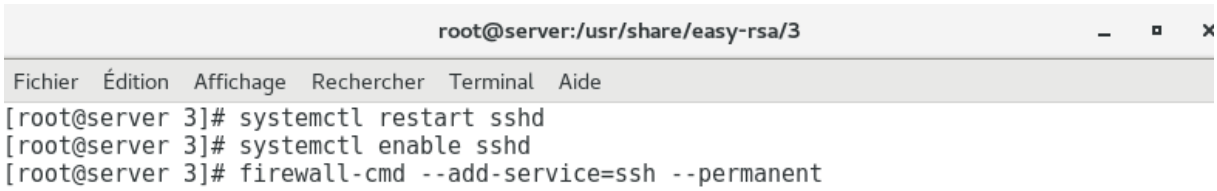
Repérez la ligne 17 puis de commenter

```
Fichier Édition Affichage Rechercher Terminal Aide
    17 Port 22
    18 #AddressFamily any
    19 #ListenAddress 0.0.0.0
    20 #ListenAddress ::
```

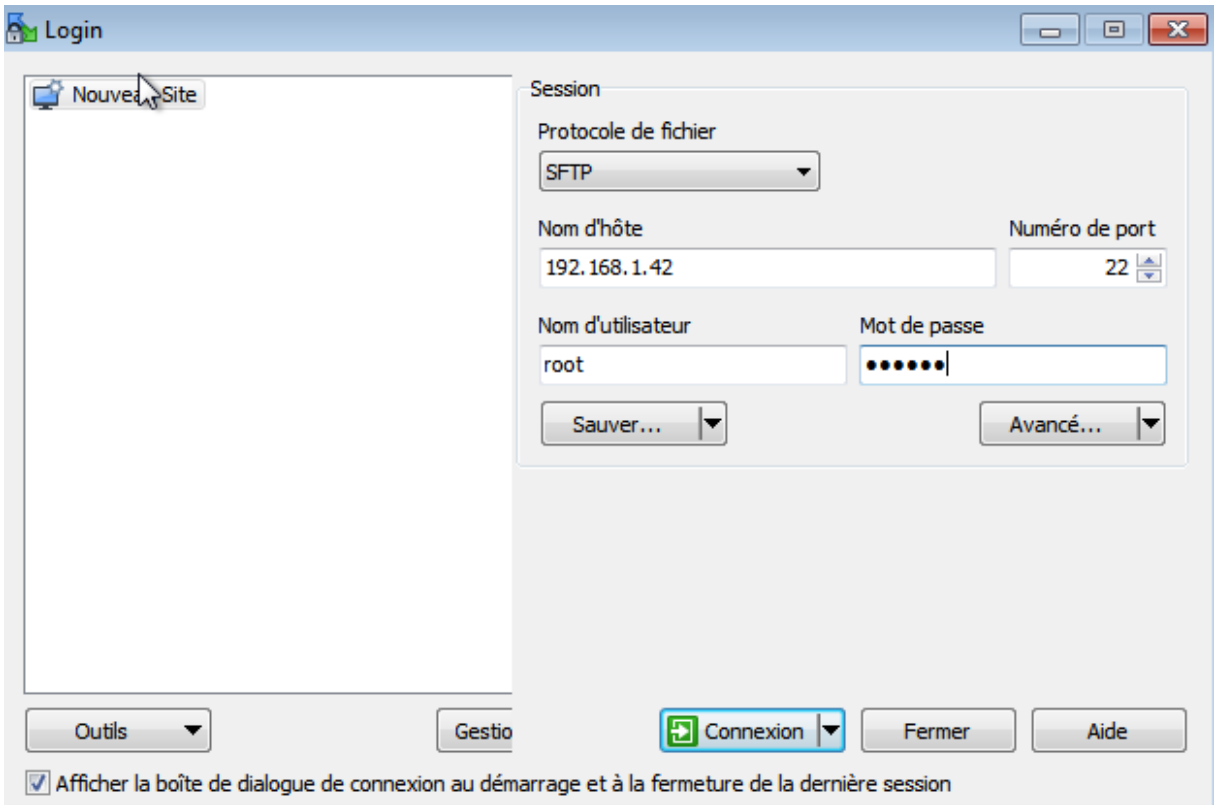
Repérez la ligne 38 puis de commenter

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

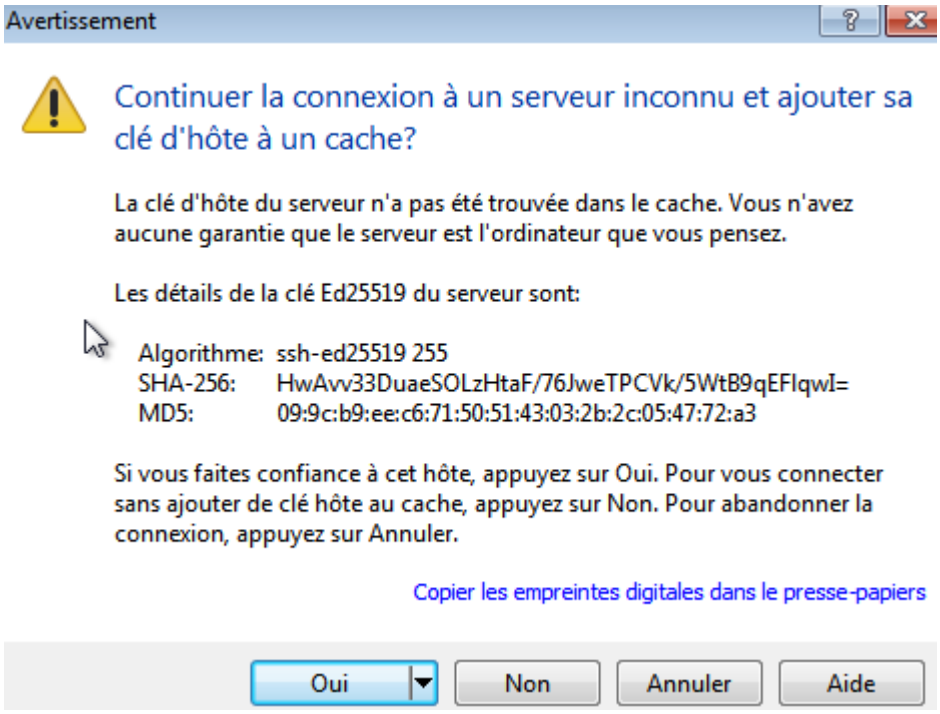
Redémarrez le service SSH avec la commande « systemctl restart sshd »

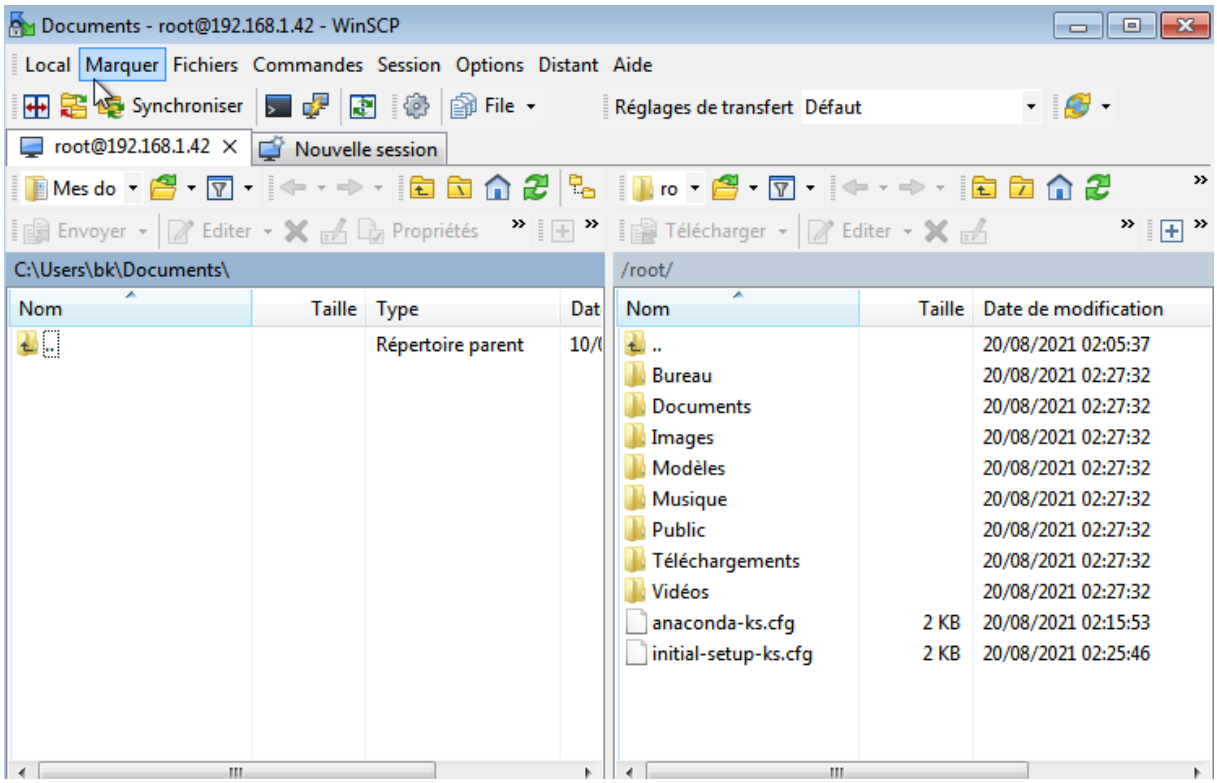


Allez sur la machine client connectez avec un logiciel WinSCP

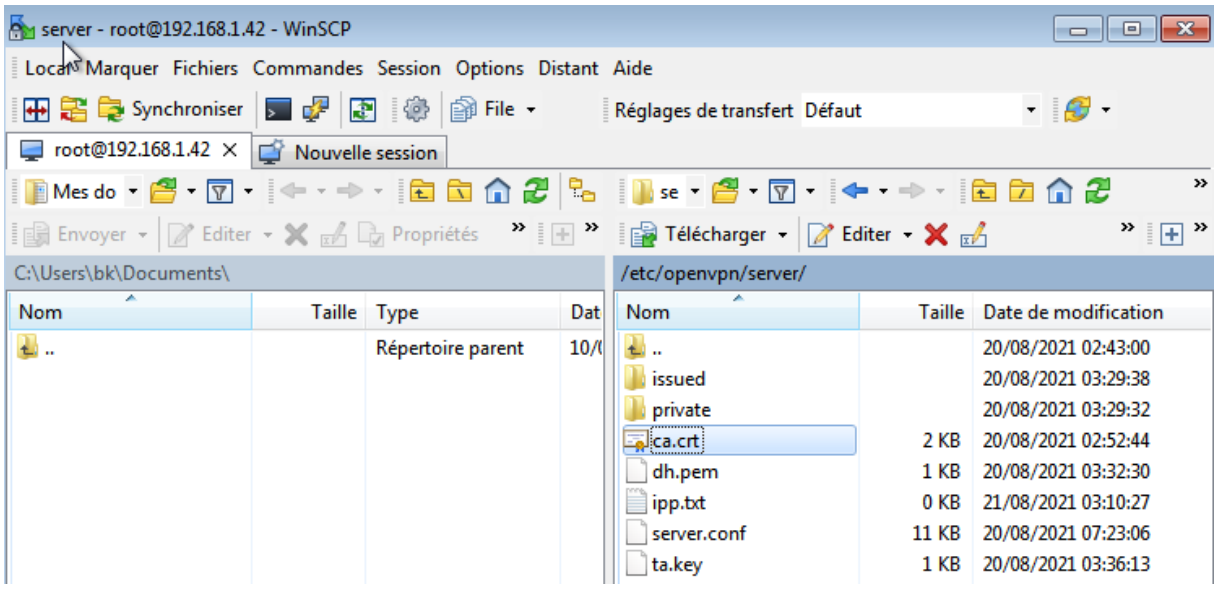


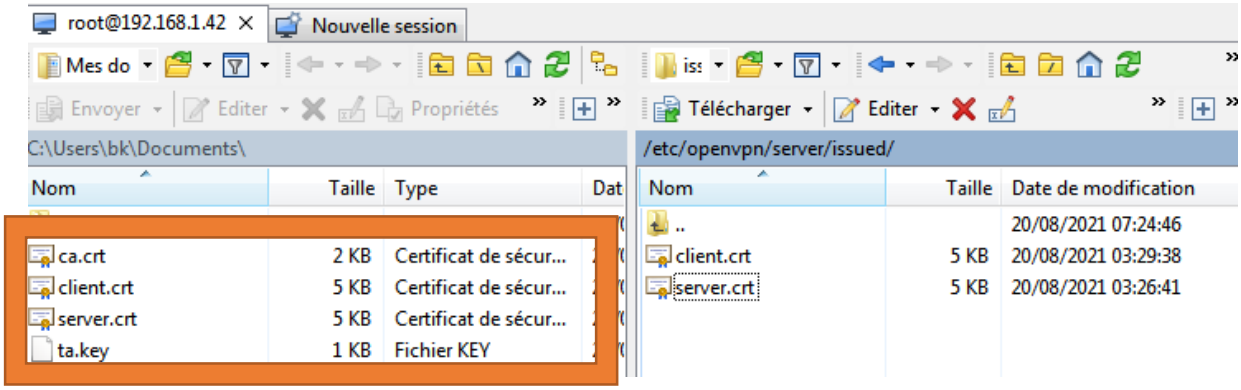
Une fois connectée vous obtiendrez l'écran ci-dessous

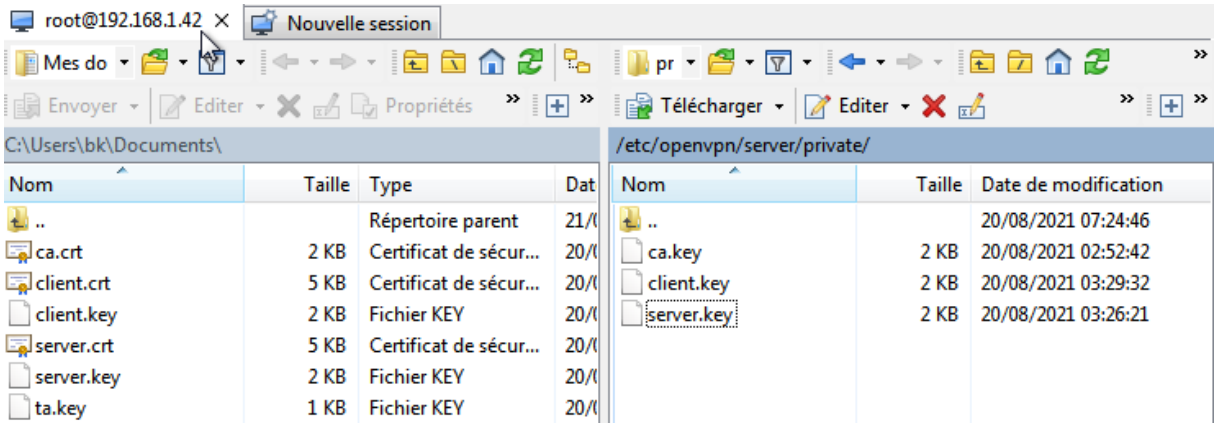




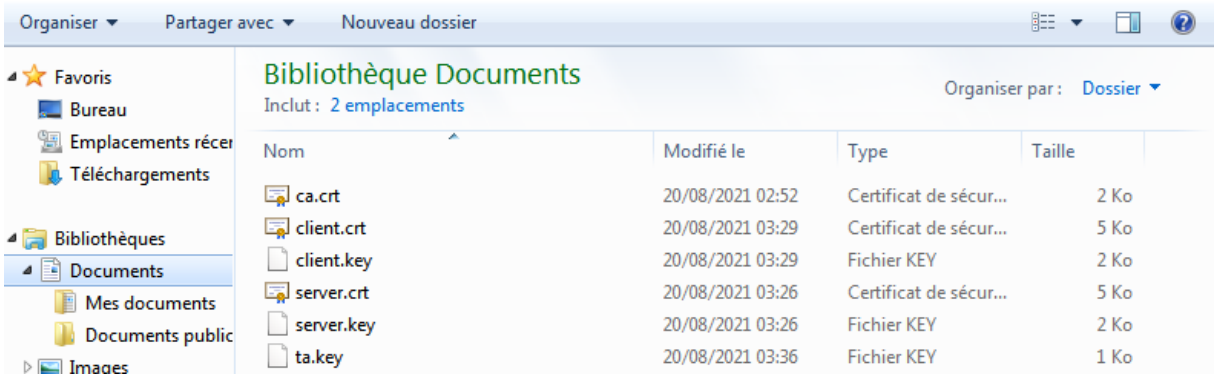
Copiez les certificats et les clés sur la machine cliente



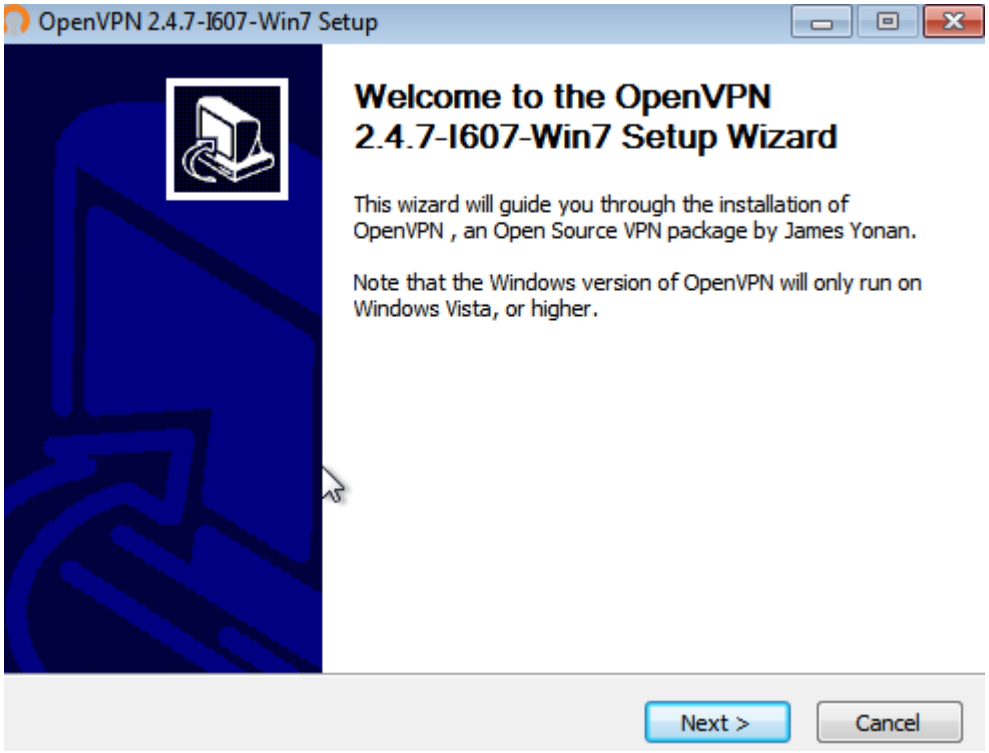




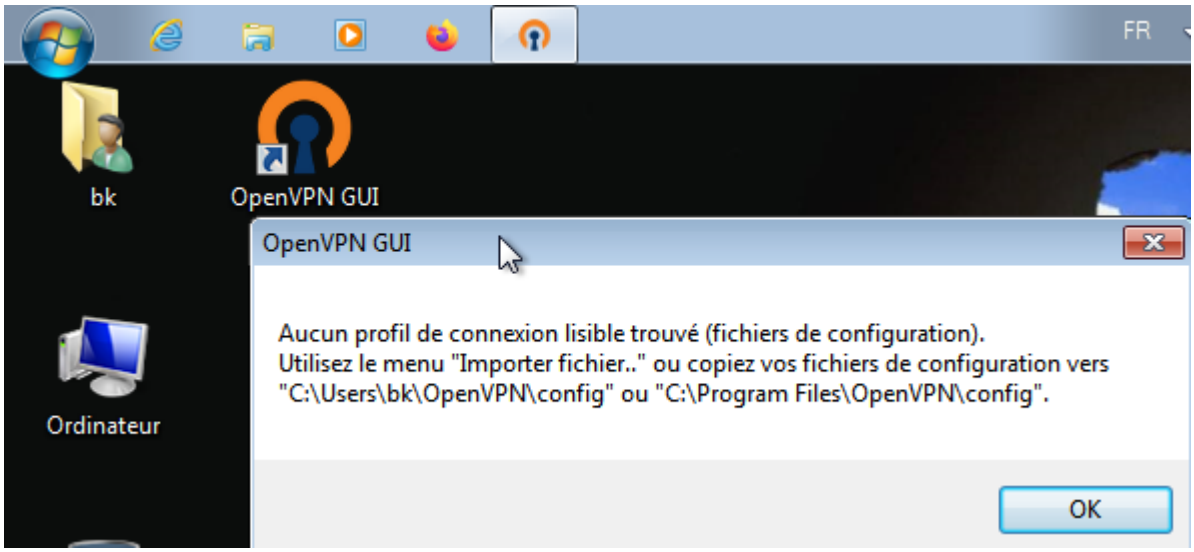
Les fichiers copiés se trouvent dans le dossier Documents sur la capture suivante :



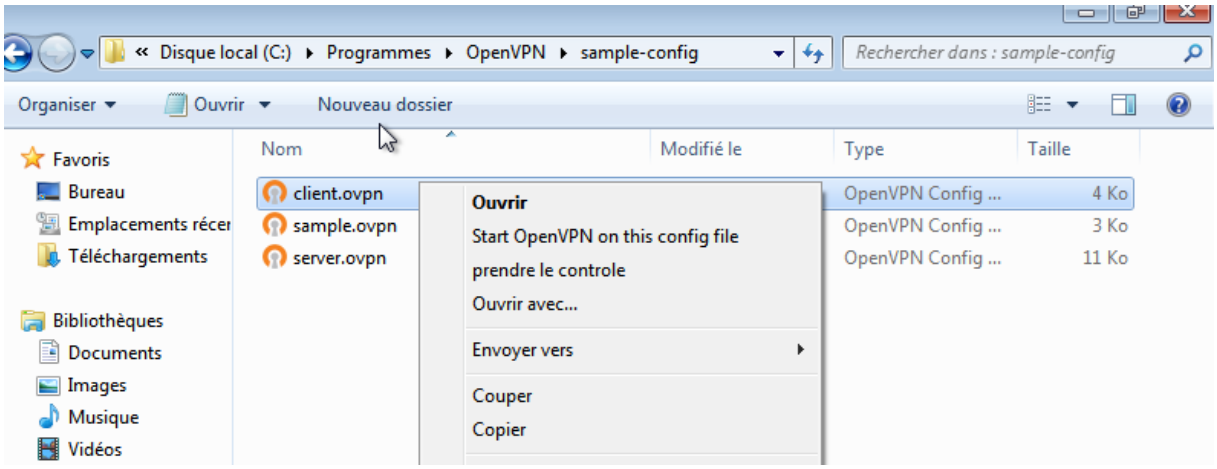
L'installation de logiciel « OpenVPN » au niveau du client



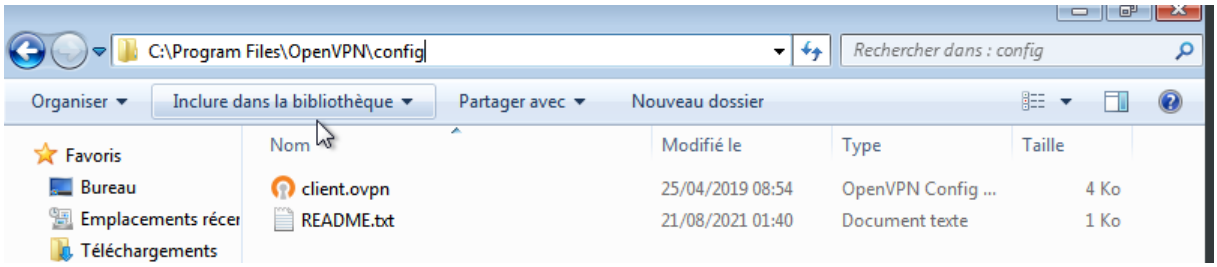
Après avoir terminé l'installation « OpenVPN » vous obtiendrez la capture ci-dessous.



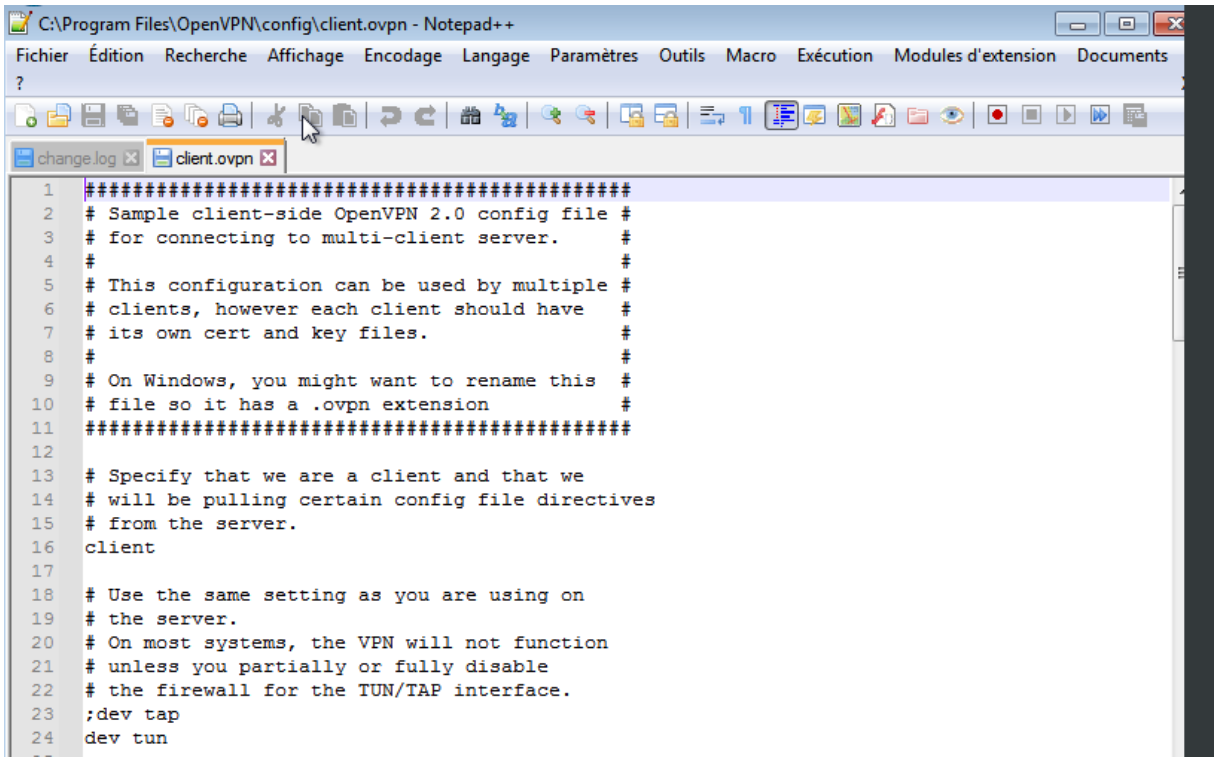
Copiez le fichier « client.ovpn »



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



Edition du fichier client.ovpn



Repérez la ligne 121 puis de commenter

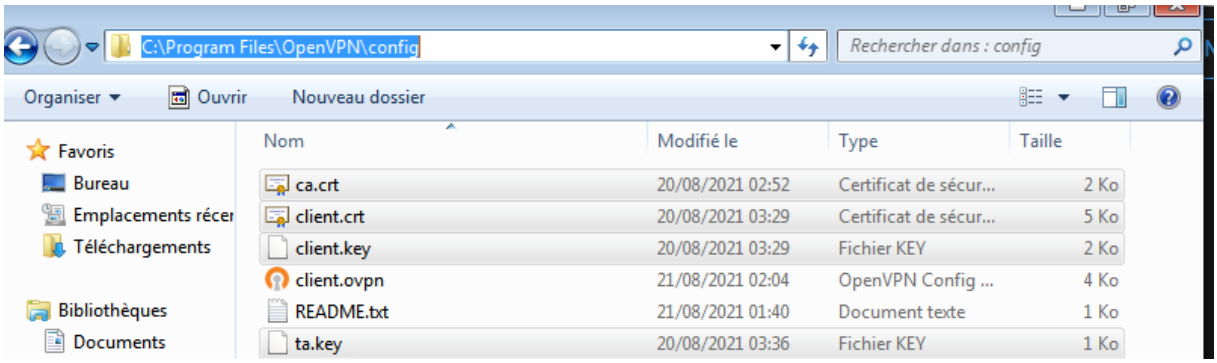
```
118  # Enable compression on the VPN link.
119  # Don't enable this unless it is also
120  # enabled in the server config file.
121  comp-lzo
```

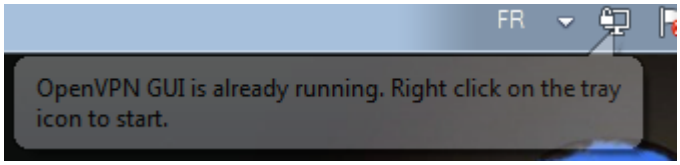
Repérez la ligne 42 puis ajoutez @ IP du serveur

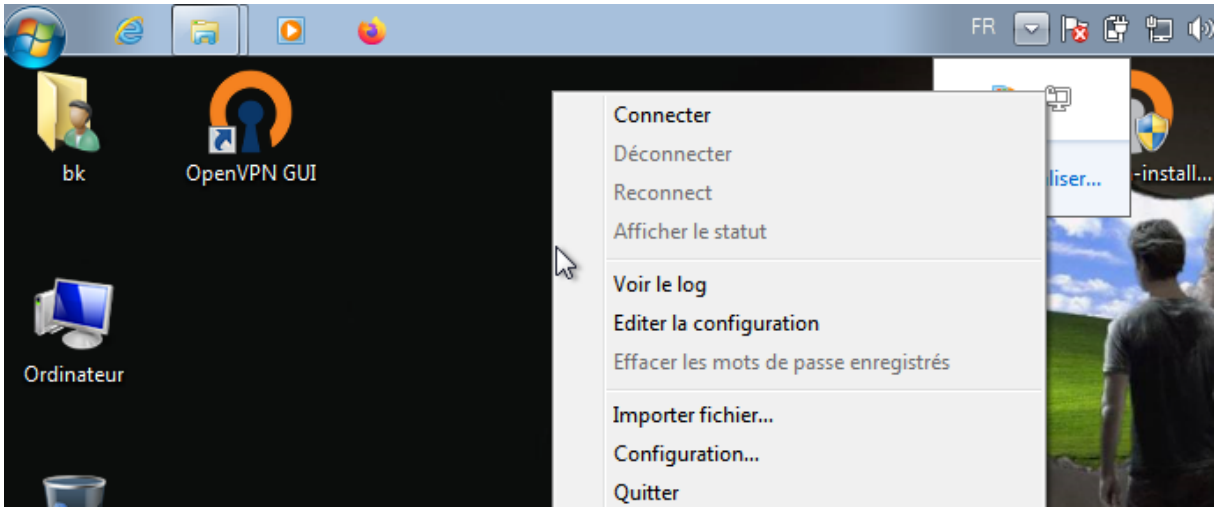
change.log | client.ovpn

```
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
```

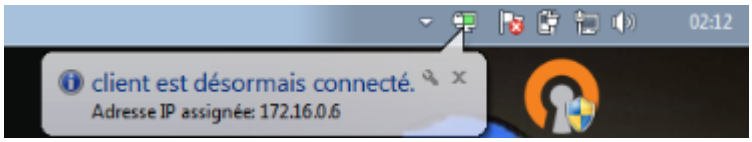
Copiez les certificats et clés dans le dossier config

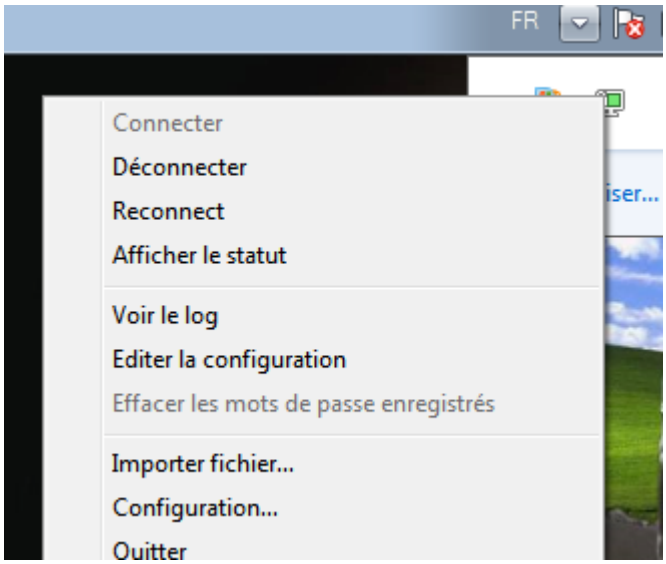






Le client est maintenant connecté





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