

# openvpn

February 5, 2024

```
[ ]: import getpass
import os
!rm pass.txt
password = getpass.getpass()
f=open("pass.txt","w")
f.write(password)
f.close()
!sudo -S apt update < pass.txt
!sudo -S apt upgrade -y < pass.txt
!sudo -S apt install easy-rsa openvpn gcc make perl linux-headers-$(uname -r)
↵-y < pass.txt
!sudo -S cp pass.txt /etc/openvpn/server
```

.....

```
Atteint :1 http://gb.archive.ubuntu.com/ubuntu jammy InRelease
Atteint :2 http://gb.archive.ubuntu.com/ubuntu jammy-updates InRelease
Atteint :3 http://gb.archive.ubuntu.com/ubuntu jammy-backports InRelease
Atteint :4 http://security.ubuntu.com/ubuntu jammy-security InRelease
```

```

Lecture des listes de paquets... Fait[33m
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Tous les paquets sont à jour.
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Calcul de la mise à jour... Fait
Get more security updates through Ubuntu Pro with 'esm-apps' enabled:
    libjs-jquery-ui python3-scipy
Learn more about Ubuntu Pro at https://ubuntu.com/pro
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
gcc est déjà la version la plus récente (4:11.2.0-1ubuntu1).
make est déjà la version la plus récente (4.3-4.1build1).
easy-rsa est déjà la version la plus récente (3.0.8-1ubuntu1).
linux-headers-6.5.0-15-generic est déjà la version la plus récente
(6.5.0-15.15~22.04.1).
openvpn est déjà la version la plus récente (2.5.9-0ubuntu0.22.04.2).
perl est déjà la version la plus récente (5.34.0-3ubuntu1.3).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
[sudo] Mot de passe de vboxuser :

```

```

[1]: !sudo -S mkdir -p /etc/openvpn/easy-rsa < pass.txt
    !sudo -S cp -r /usr/share/easy-rsa/* /etc/openvpn/easy-rsa/ < pass.txt

```

```

[sudo] Mot de passe de vboxuser : [sudo] Mot de passe de vboxuser :

```

```

[2]: !ls /etc/openvpn/easy-rsa

```

```

easyrsa openssl-easyrsa.cnf pki toto.txt vars vars.example x509-types

```

```

[3]: import subprocess
    subprocess.run("""cat <<EOF > vars

```

```

export KEY_COUNTRY="FR"
export KEY_PROVINCE="FR"
export KEY_CITY="Perpignan"
export KEY_ORG="UPVD"
export KEY_EMAIL="bastienbaranoff@gmail.com"
export KEY_CN=MyVPN
export KEY_NAME=MyVPN
export KEY_OU=MyVPN
export EASYRSA_ALGO "ec"
export EASYRSA_DIGEST "sha512"
export EASYRSA_BATCH=1
EOF
""", shell=True)
!sudo -S cp vars /etc/openvpn/easy-rsa/ < pass.txt

```

[sudo] Mot de passe de vboxuser :

```

[4]: !cd /etc/openvpn/easy-rsa/ && ls && source vars
!cd /etc/openvpn/server && sudo -S /etc/openvpn/easy-rsa/easyrsa init-pki < ~/
↳TP1/pass.txt
!cd /etc/openvpn/server && sudo -S /etc/openvpn/easy-rsa/easyrsa build-ca
↳nopass < ~/TP1/pass.txt
!cd /etc/openvpn/server && sudo -S /etc/openvpn/easy-rsa/easyrsa gen-dh < ~/TP1/
↳pass.txt
!cd /etc/openvpn/server && sudo -S /etc/openvpn/easy-rsa/easyrsa gen-req .
↳nopass < ~/TP1/pass.txt

```

```
easyrsa openssl-easyrsa.cnf pki toto.txt vars vars.example x509-types
```

[sudo] Mot de passe de vboxuser :

[sudo] Mot de passe de vboxuser : Using SSL: openssl OpenSSL 3.0.2 15 Mar 2022  
(Library: OpenSSL 3.0.2 15 Mar 2022)

[sudo] Mot de passe de vboxuser : Using SSL: openssl OpenSSL 3.0.2 15 Mar 2022  
(Library: OpenSSL 3.0.2 15 Mar 2022)

Generating DH parameters, 2048 bit long safe prime

```

...+...+...
...
...
...
...
+...+...+...
...+...
...+...+...
...+...
...
...
...

```

...+...+...+...  
 ...+...+...  
 ...+...+...  
 ...+...+...  
 ...  
 ...  
 ...  
 ...  
 ...  
 ...+...  
 ...  
 ...  
 ...+...  
 ...+...  
 ...+...+...  
 ...+...  
 ...+...  
 ...  
 ...  
 ...  
 ...+...  
 ...  
 ...+...  
 ...  
 ...+...  
 ...  
 ...+...+...+...  
 ...+...+...+...  
 ...+...  
 ...  
 ...+...+...  
 ...  
 ...+...  
 ...  
 ...  
 ...  
 ...+...  
 ...  
 ...  
 ...  
 ...  
 ...+...+...  
 ...+...  
 ...  
 ...  
 ...  
 ...+...+...  
 ...+...  
 ...  
 ...

...  
 ...+...  
 ...+...  
 ...  
 ...  
 ...  
 ...+ . . +...+...  
 ...  
 ...+...+...  
 ...+...  
 ...+...  
 ...+...  
 ...  
 ...+...  
 ...+ . . +...+...  
 ...+...  
 ...+...  
 ...  
 ...+...  
 ...  
 ...+...  
 ...+...  
 ...  
 ...+...  
 ...+...  
 ...+...+...  
 ...+...  
 ...+...+...  
 ...  
 ...  
 ...+...+ . .  
 ...+...+...  
 ...  
 ...+...  
 ...+...+...+...  
 ...  
 ...  
 ...+...  
 ...+...  
 ...+...+...  
 ...+...+...  
 ...+...+ . .  
 ...+...  
 ...  
 ...+...+...  
 ...+...  
 ...+...  
 ...+...

$$\begin{array}{c}
+_{...} +_{...} \\
... \\
... \\
... \\
... +_{...} \\
... \\
... +_{...} +_{...} \\
... +_{...} \\
... \\
... +_{...} \\
... +_{...} \\
... \\
... +_{...} \\
... +_{...} \\
... \\
... +_{...} \\
... +_{...} \\
... \\
... +_{...} \quad . \quad +_{...} \\
... \\
... \\
... +_{...} \\
... +_{...} \\
... \\
... +_{...} \\
... +_{...} \\
... +_{...} +_{...} \\
... \\
... +_{...} \quad . \quad +_{...} +_{...} +_{...} \\
... \\
... \\
... \\
... +_{...} \\
... \\
... +_{...} \\
... +_{...} \\
... \\
... +_{...} \\
... \\
... \\
... +_{...} +_{...} \\
...
\end{array}$$

...+...  
 ...+...+...  
 ...+...  
 ...  
 ...  
 ...+...  
 ...  
 ...  
 ...+...  
 ...  
 ...  
 ...+...  
 ...+...  
 ...+ . .  
 ...  
 ...+...  
 ...+...  
 ...+...  
 ...  
 ...  
 ...  
 ...  
 ...  
 . . +...+...  
 ...  
 ...+...+...+...+...+ . +...+...+...  
 ...  
 ...  
 ...  
 ...+...+...+...+...  
 ...  
 ...+...  
 ...+...  
 +...  
 ...+...  
 ...  
 ...  
 ...  
 ...+...  
 ...+...+...  
 ...+...  
 ...  
 . +...+...  
 ...  
 ...  
 ...+...  
 ...+...+...  
 ...+...  
 ...

...  
 ...+...  
 ...+...  
 ...  
 ...+...  
 ...  
 ...+...+...  
 ...  
 ...+...  
 ...+...  
 ...  
 ...+...+...  
 ...+...  
 ...  
 ...  
 ...  
 ...  
 ...  
 ...  
 ...+...  
 ...+...  
 ...  
 ...+...  
 ...  
 ...  
 ...  
 ...+...+...  
 ...  
 ...  
 ...+...  
 ...+...  
 ...  
 ...  
 ...  
 ...+...  
 ...  
 ...  
 ...+...  
 ...+...  
 ...+...  
 ...+...  
 ...  
 ...  
 ...  
 ...  
 ...  
 ...+...  
 ...+...  
 ...+...  
 ...



```

...
...
...+...
...
...+...
...+...+...
...
...
...
...
...
...+...
...
...+...
...
...+...
...+*****
+*****
+*****
[sudo] Mot de passe de vboxuser : Using SSL: openssl OpenSSL 3.0.2 15 Mar 2022
(Library: OpenSSL 3.0.2 15 Mar 2022)
.+...+*****+.
...+.+.+*****+.
...+...+.+.+...+.+.+...+
+
...+.+...+
*...+...+...+
+++++*...+...+...+...+.+.+.+
...+...+...+...+...+.+...
.+...+...+...+...
...+.+.+...+...+.+...+...+...
...+...+...+...+.+.+...+...+.
...+.+...+...+.+.+...+...+
+...+.+...+.+.+...+...+.+.+...+
...+...+...+.+.+...+...+.+...+
...+...+...+.+.+...+...+...
...+...+...+...+...+...+...+

```

```
[5]: !cd /etc/openssl/easy-rsa/ && ls && source vars
      !sudo -S /etc/openssl/easy-rsa/easyrsa init-pki /etc/openssl/server < pass.txt
      !sudo -S /etc/openssl/easy-rsa/easyrsa build-ca /etc/openssl/server nopass <
      ↪pass.txt
```

```
!sudo -S /etc/openvpn/easy-rsa/easyrsa gen-dh /etc/openvpn/server < pass.txt
```

```
easyrsa openssl-easyrsa.cnf pki toto.txt vars vars.example x509-types
[sudo] Mot de passe de vboxuser :
[sudo] Mot de passe de vboxuser : Using SSL: openssl OpenSSL 3.0.2 15 Mar 2022
(Library: OpenSSL 3.0.2 15 Mar 2022)
```

```
[sudo] Mot de passe de vboxuser : Using SSL: openssl OpenSSL 3.0.2 15 Mar 2022
(Library: OpenSSL 3.0.2 15 Mar 2022)
Generating DH parameters, 2048 bit long safe prime
```

```
...
...
...
...+...
...+...
...
...
...+...
...
...+...
...
...+...+...+...
...+...
...+...
...+...
. +...+...
...+...
...+...+...
...
...
+...
...
...
...
...
. +...+...
...
...+...+...+...
...
+...+...
. +...+...
...+ .
...
...
...+...
...
+...+...
```

$\dots + \dots + \dots$   
 $\dots + \dots$   
 $\dots$   
 $\dots + \dots$   
 $\dots + \dots + \dots$   
 $\dots$   
 $\dots + \dots$   
 $\dots$   
 $\dots$   
 $\dots$   
 $\dots + \dots$   
 $\dots + \dots$   
 $\dots$   
 $\dots$   
 $\dots$   
 $\dots$   
 $\dots$   
 $\dots$   
 $\dots + \dots + \dots$   
 $\dots + \dots$   
 $\dots$   
 $\dots$   
 $\dots$   
 $\dots$   
 $\dots$   
 $\dots$   
 $\dots + \dots + \dots + \dots$   
 $\dots$   
 $\dots$   
 $\dots$   
 $\dots$   
 $\dots + \dots$   
 $\dots$   
 $\dots$   
 $\dots + \dots + \dots$   
 $\dots +$   
 $\dots + \dots$   
 $\dots$   
 $\dots + \dots + \dots$   
 $\dots$   
 $\dots + \dots$   
 $\dots + \dots$   
 $\dots + \dots + \dots$   
 $\dots$   
 $\dots + \dots$   
 $\dots$   
 $\dots$   
 $\dots$   
 $\dots + \dots + \dots$   
 $\dots$   
 $\dots$   
 $\dots$

$\dots + \dots$   
 $\dots$   
 $\dots + \dots$   
 $\dots$   
 $\dots + \dots + \dots$   
 $\dots + \dots$   
 $\dots + \dots$   
 $\dots + \dots + \dots$   
 $\dots + \dots + \dots + \dots + \dots$   
 $\dots + \dots$   
 $\dots + \dots$   
 $\dots + \dots$   
 $\dots$   
 $\dots + \dots + \dots$   
 $\dots + \dots + \dots + \dots$   
 $\dots + \dots + \dots$   
 $\dots$   
 $\dots + \dots + \dots + \dots$   
 $\dots + \dots + \dots$   
 $\dots$   
 $\dots$   
 $\dots$   
 $\dots$   
 $\dots + \dots$   
 $\dots + \dots + \dots + \dots$   
 $\dots + \dots$   
 $\dots + \dots$   
 $\dots + \dots$   
 $\dots$   
 $\dots + \dots$   
 $\dots + \dots + \dots$   
 $\dots$   
 $\dots + \dots$   
 $\dots + \dots$   
 $\dots + \dots$   
 $\dots$   
 $\dots$   
 $\dots$   
 $\dots$   
 $\dots + \dots + \dots$   
 $\dots$   
 $\dots$   
 $\dots + \dots + \dots$   
 $\dots + \dots$

$\dots$   
 $\dots + \dots$   
 $\dots$   
 $\dots$   
 $\dots$   
 $\dots + \dots$   
 $\dots + \dots$   
 $\dots$   
 $\dots$   
 $\dots + \dots$   
 $\dots$   
 $\dots + \dots$   
 $\dots$   
 $\dots$   
 $\dots + \dots$   
 $\dots + \dots$   
 $\dots + \dots + \dots$   
 $\dots + \dots + \dots$   
 $\dots + \dots$   
 $\dots + \dots$   
 $\dots$   
 $\dots$   
 $\dots$   
 $\dots + \dots$   
 $\dots + \dots$   
 $\dots$   
 $\dots + \dots + \dots + \dots$   
 $\dots$   
 $\dots + \dots + \dots$   
 $\dots + \dots$   
 $\dots + \dots$   
 $\dots + \dots$   
 $\dots + \dots$   
 $\dots$   
 $\dots + \dots +$   
 $\dots$   
 $\dots + \dots + \dots$   
 $\dots$   
 $\dots + \dots$   
 $\dots$   
 $\dots + \dots + \dots$   
 $\dots + \dots + \dots$   
 $\dots + \dots$   
 $\dots$   
 $\dots + \dots$   
 $\dots + \dots$   
 $\dots + \dots$   
 $\dots + \dots$

[illegible]

```
[7]: !sudo -S rm /etc/openvpn/server/pki/reqs/..req < pass.txt
      !sudo -S rm /etc/openvpn/server/pki/private/..key < pass.txt
      !sudo -S rm /etc/openvpn/server/pki/issued/..crt < pass.txt
```

```
!cd /etc/openvpn/server && sudo -S /etc/openvpn/easy-rsa/easyrsa_
↪build-server-full . nopass < ~/TP1/pass.txt
```

```
[sudo] Mot de passe de vboxuser : [sudo] Mot de passe de vboxuser : [sudo] Mot
de passe de vboxuser : rm: impossible de supprimer
'/etc/openvpn/server/pki/issued/..crt': Aucun fichier ou dossier de ce type
[sudo] Mot de passe de vboxuser : Using SSL: openssl OpenSSL 3.0.2 15 Mar 2022
(Library: OpenSSL 3.0.2 15 Mar 2022)
```

```
...+...+...+...+...+...+...+...+...+...+
...+++++*...
.+...+...+++++*..
...+...+...+...+...+...+...+...+...+...
...+...+...+...+...+...+...+...+...
..+...+...+...+...+...+...+...+...+...
..+...+...+...+...+...+...+...+...+...
..+...+...+...+...+...+...+...+...+...
.+...+...+...+...+...+...+...+...+...
...+...+...+...+...+...+...+...+...+...
..+...+...+...+...+...+...+...+...+...
..+...+...+...+...+...+...+...+...+...
...+...+...+...+...+...+...+...+...+...
+...+...+...+...+...+...+...+...+...+...
+...+...+...+...+...+...+...+...+...+...
+++++
.+...+...+...+...+...+...+...+...+...+...
...+...+...+...+...+...+...+...+...+...+...
+++++*...+...+...+...+...+...+...+...
...+++++*...
+...+...+...+...+...+...+...+...+...+...
.+...+...+...+...+...+...+...+...+...+...
+.+...+...+...+...+...+...+...+...+...+...
+++++
-----
```

```
Using configuration from /etc/openvpn/server/pki/easy-
rsa-27531.Z8UioP/tmp.5UOHU6
40273853DF7F0000:error:0700006C:configuration file routines:NCONF_get_string:no
value:../crypto/conf/conf_lib.c:315:group=<NULL> name=unique_subject
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName          :ASN.1 12:'. '
Certificate is to be certified until May  9 22:19:15 2026 GMT (825 days)
```

```
Write out database with 1 new entries
Data Base Updated
```

[ ]: