

# **CRÉATION SERVEUR FTP AVEC PROFTP ET** **SSL/TLS**

## **Table des matières**

1) Installation des paquets nécessaires.....	2
2) Création d'une clé privée.....	2
3) Création d'un certificat.....	2
4) Configuration des différents fichiers.....	3
5) Tests avec FileZilla (utilisateur connu).....	5
5) Tests avec FileZilla (utilisateur inconnu).....	6
6) Tests avec l'exportateur de fichier Ubuntu (utilisateur connu).....	7
.....	8
Dans l'emplacement « Connexion à un serveur » on se connecte avec la commande suivante :.....	8
7) Tests avec l'exportateur de fichier Ubuntu (utilisateur inconnu).....	10
Dans l'emplacement « Connexion à un serveur » on se connecte avec la commande suivante :.....	10
8) Tests en ligne de commande (utilisateur connu).....	11
9) Tests en ligne de commande (utilisateur inconnu).....	11

L'objectif de cette procédure est de créer un serveur FTP sécurisé avec SSL/TLS sur une machine serveur Ubuntu 20.04

Prérequis :

- Machine serveur Ubuntu 20.04
- Machine client Ubuntu Desktop

## 1) Installation des paquets nécessaires

- Commencer par mettre à jour sa machine :

```
apt update && apt upgrade -y
```

- Installation de Proftpd et openssl

```
apt install proftpd openssl
```

## 2) Création d'une clé privée

- Se rendre dans le dossier SSL :

```
cd /etc/ssl
```

- Créer un répertoire personnalisé pour créer sa clé :

```
cd mesCles  
mkdir mesCles
```

- Se rendre dans le dossier et créer la clé :

```
openssl genrsa -out macle.key 4096
```

On a créer notre clé notre clé privée on va maintenant créer notre certificat

## 3) Création d'un certificat

- Se rendre dans le dossier SSL :

```
cd /etc/ssl
```

- Créer un répertoire personnalisé pour créer son certificat :

```
mkdir mesCertifs
```

- Se rendre dans le dossier et créer la clé :

```
cd mesCertifs  
openssl req -new -key ../mesCles/macle.key -out monCertif.csr
```

```
openssl x509 -req -days 365 -in monCertif.csr -signkey ../mesCles/macle.key -out monCertif.crt
```

Ne pas oublier de modifier les chemins de la clé et du certificat dans le fichier `tls.conf` :

```
TLRSACertificateFile      /etc/ssl/mesCertifs/monCertif.crt
TLRSACertificateKeyFile    /etc/ssl/mesCles/macle.key
```

## 4) Configuration des différents fichiers

- Pour effectuer les tests on va créer un dossier pour le serveur FTP :

```
cd /home
```

```
mkdir FTP
```

- On va maintenant lui donner les droits :

```
cd /home/FTP
```

```
chmod 777 /home/FTP
```

- Vérifier dans le fichier `/etc/proftpd/modules.conf` que TLS est activé :

```
LoadModule mod_tls.c
```

- Décommenter la ligne suivante dans le fichier `proftpd.conf` pour inclure le fichier de configuration :

```
nano /etc/proftpd/proftpd.conf
```

```
Include /etc/proftpd/tls.conf
```

- On va également décommenter la ligne et la modifier comme ceci :

```
DefaultRoot /home/FTP/
```

On va se rendre dans le fichier `tls.conf` afin de le configurer comme ceci :

**`nano /etc/proftpd/tls.conf`**

```
#
# Proftpd sample configuration for FTPS connections.
#
# Note that FTPS impose some limitations in NAT traversing.
# See http://www.castaglia.org/proftpd/doc/contrib/ProFTPD-mini-HOWTO-TLS.html
# for more information.
#
<IfModule mod_tls.c>
  TLSEngine               on
  TLSLog                  /var/log/proftpd/tls.log
  TLSProtocol              SSLv23
#
# Server SSL certificate. You can generate a self-signed certificate using
# a command like:
#
# openssl req -x509 -newkey rsa:1024 \
#             -keyout /etc/ssl/private/proftpd.key -out /etc/ssl/certs/proftpd.crt \
#             -nodes -days 365
#
# The proftpd.key file must be readable by root only. The other file can be
# readable by anyone.
#
# chmod 0600 /etc/ssl/private/proftpd.key
# chmod 0640 /etc/ssl/private/proftpd.key
#
TLRSACertificateFile       /etc/ssl/mesCertifs/monCertif.crt
TLRSACertificateKeyFile    /etc/ssl/mesCles/macle.key
#
# CA the server trusts...
# TLSCACertificateFile     /etc/ssl/certs/CA.pem
# ...or avoid CA cert and be verbose
# TLSOptions               NoCertRequest EnableDiags
# ... or the same with relaxed session use for some clients (e.g. FireFtp)
# TLSOptions               NoCertRequest EnableDiags NoSessionReuseRequired
```

- On redémarre le service `proftpd` :

**`systemctl restart proftpd`**

Pour les tests on va créer un autre utilisateur qui lui n'es pas censé avoir accès au serveur :

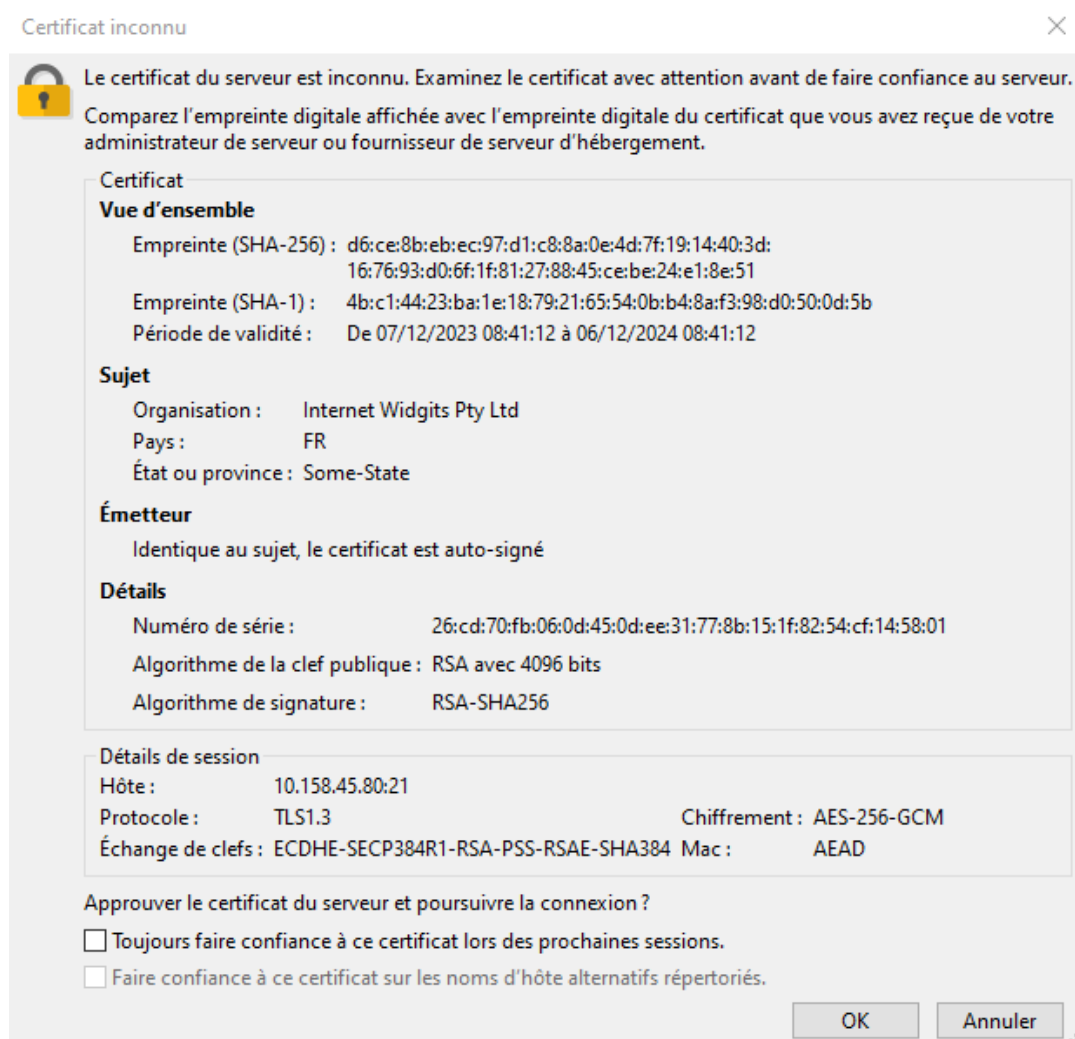
**`useradd marie -p marie`**

## 5) Tests avec FileZilla (utilisateur connu)

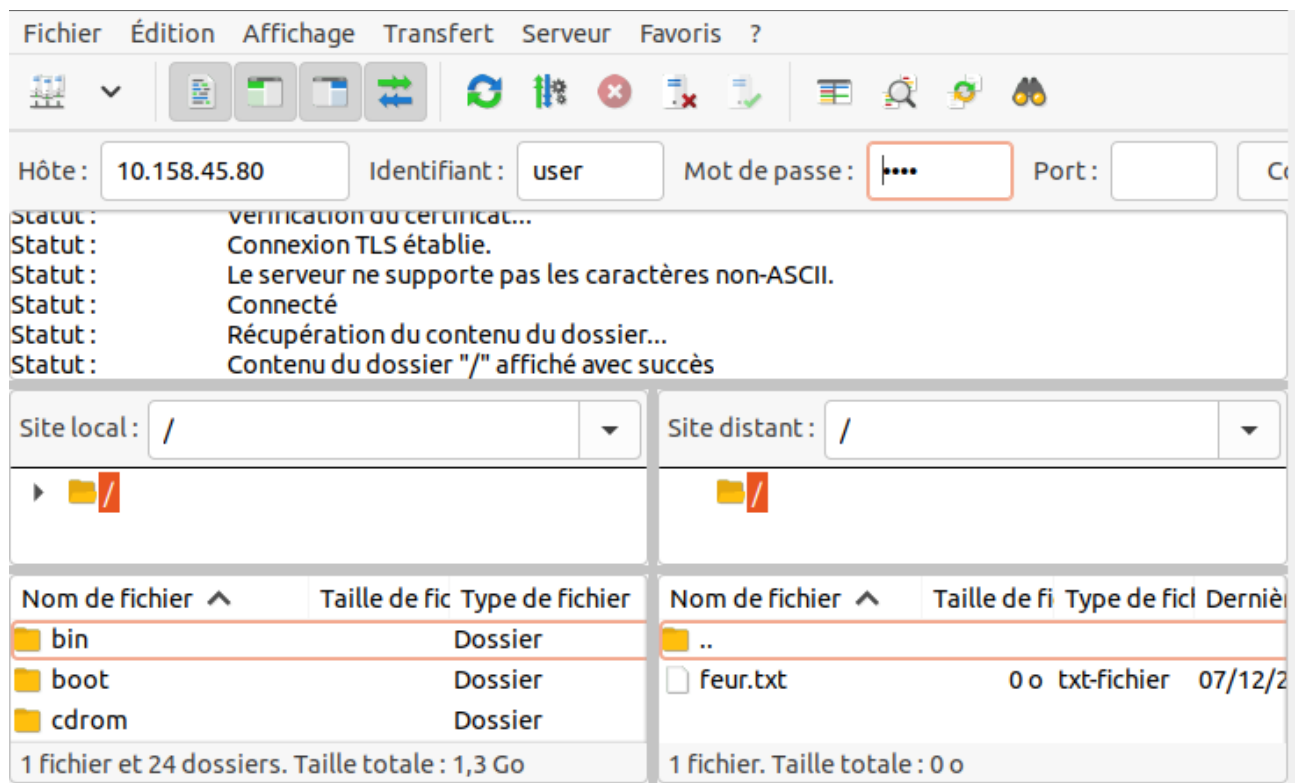
On ouvre FileZilla puis on indique le nom du serveur, le nom d'utilisateur (user) et le mot de passe (user):

Hôte :	10.158.45.80	Identifiant :	user	Mot de passe :	....
--------	--------------	---------------	------	----------------	------

On clique sur connexion puis le message concernant le certificat apparaît :



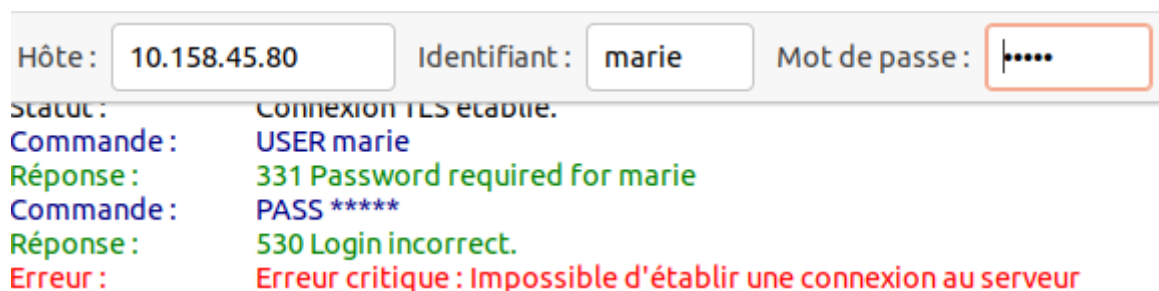
## Résultat :



On remarque que le fichier « feur.txt » est présent, ce qui prouve donc que cela marche

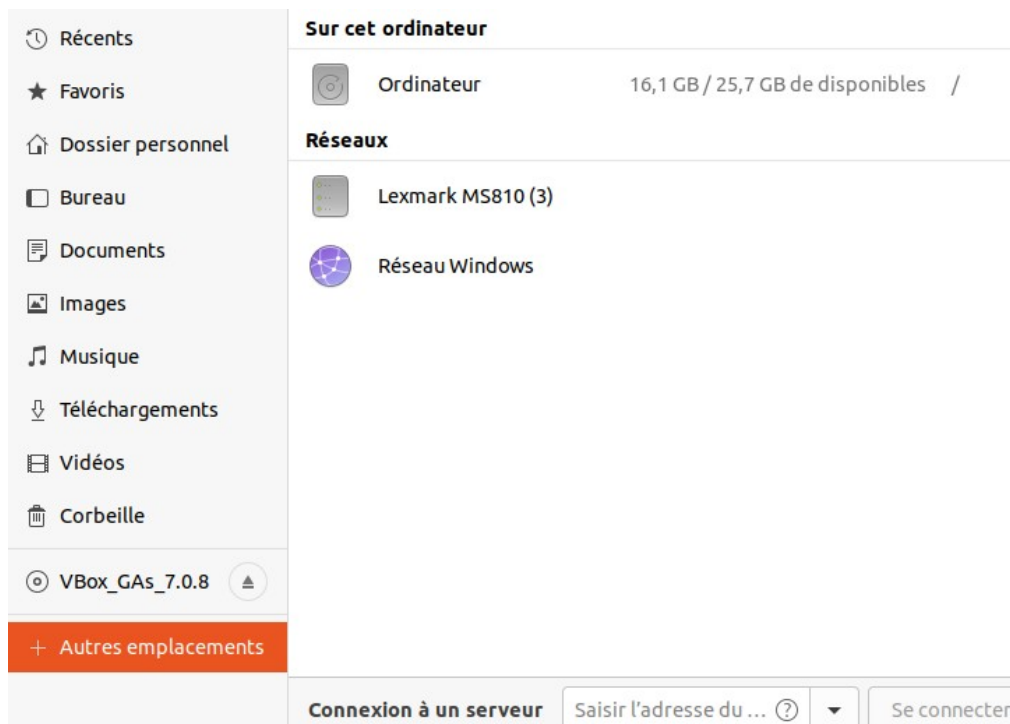
## 5) Tests avec FileZilla (utilisateur inconnu)

On ouvre FileZilla puis on indique le nom du serveur, le nom d'utilisateur et le mot de passe :



## 6) Tests avec l'exportateur de fichier Ubuntu (utilisateur connu)

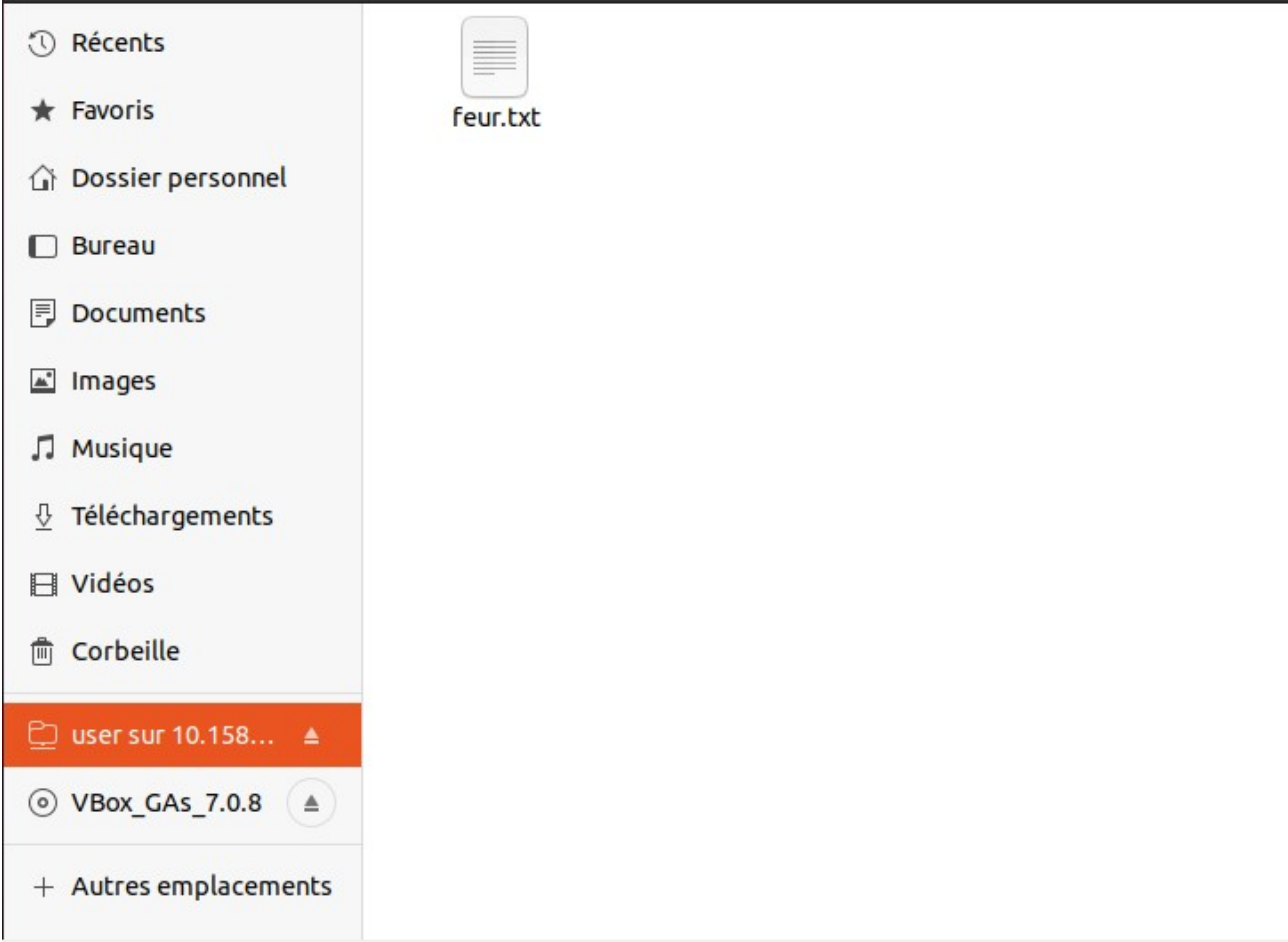
On se rend dans l'explorateur de fichiers Ubuntu puis on clique sur « Autres emplacements »



Dans l'emplacement « Connexion à un serveur » on se connecte avec la commande suivante :

<ftp://user@10.158.45.80/>

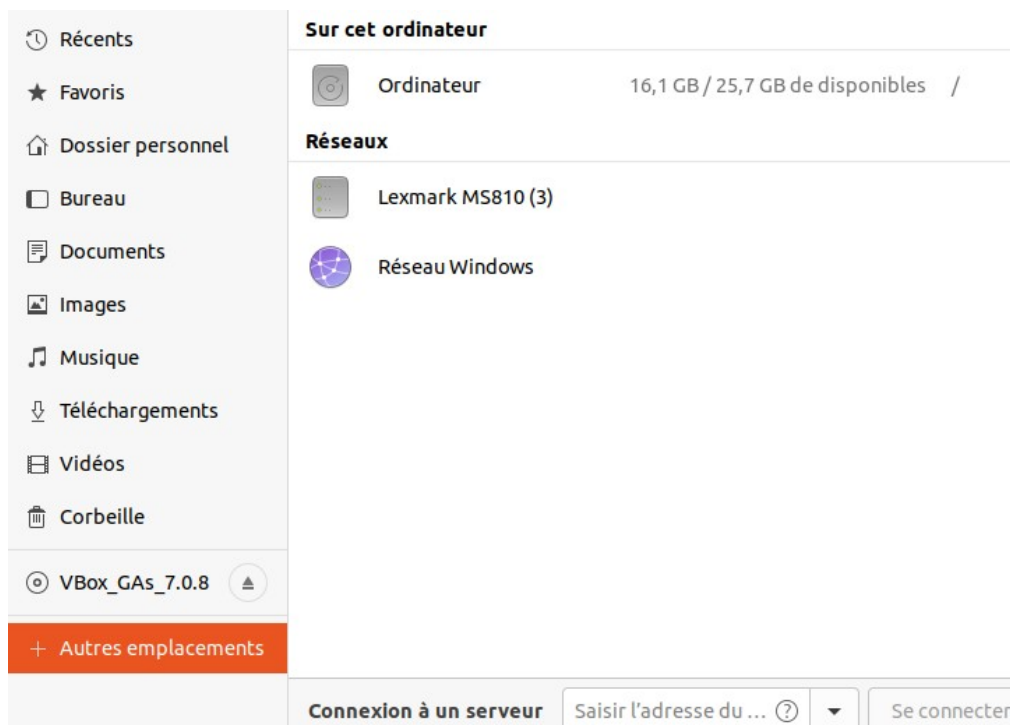
On entre le mot de passe (user) et on accède bien au serveur





## 7) Tests avec l'exportateur de fichier Ubuntu (utilisateur inconnu)

On se rend dans l'explorateur de fichiers Ubuntu puis on clique sur « Autres emplacements »



Dans l'emplacement « Connexion à un serveur » on se connecte avec la commande suivante :

<ftp://marie@10.158.45.80/>

On rentre le mot de passe et on se rend compte que le compte marie ne peut pas accéder au serveur

## 8) Tests en ligne de commande (utilisateur connu)

Dans un terminal on rentre la commande suivante :

**ftp <ip du serveur>**

```
user@user-VirtualBox:~$ ftp 10.158.45.80
Connected to 10.158.45.80.
220 ProFTPD Server (Debian) [::ffff:10.158.45.80]
Name (10.158.45.80:user):
```

On rentre le nom d'utilisateur (user) et le mot de passe (user) et on voit que l'on peut bien se connecter :

```
230 User user logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

## 9) Tests en ligne de commande (utilisateur inconnu)

On refait la même manipulation en mettant en nom d'utilisateur marie et son mot de passe marie :

```
530 Login incorrect.
Login failed.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Cela ne fonctionne pas ce qui est normal