

Procédure d'installation et d'utilisation Serveur FTP

Sommaire :

Objectif de la procédure :.....	1
1) Installation de ProFTPD.....	1
2) Création et mise en place d'un certificat à l'aide d'OpenSSL :.....	4
Création d'une clé privé :.....	4
Création d'un certificat X509 :.....	4
Configuration de ProFTPD avec SSL/TLS :.....	5
Tests depuis une machine client :.....	6
Tests avec un utilisateur connu :.....	6
Tests avec un utilisateur inconnu :.....	8
Procédure d'utilisation :.....	9
Pour accéder au service FTP avec Filezilla (sur Ubuntu Desktop) :.....	9
Pour accéder au service FTP avec l'explorateur de fichiers sur Ubuntu Desktop :.....	10
Pour accéder au service FTP en ligne de commande sous Linux :.....	11

Objectif de la procédure :

L'objectif de cette procédure est de permettre une installation sécurisée d'un serveur FTP sur une machine Ubuntu Live Server. Les mesures de sécurité mises en place inclues l'utilisation de SSL/TLS qui vont permettre la mise en place d'un système de certificat et de clé privée/publique.

Une procédure d'utilisation est également disponible à la fin de ce document.

1) Installation de ProFTPD

- Dans un premier temps, il faut disposer d'une machine Ubuntu Server à jour, pour cela utiliser les commandes suivantes : « sudo -i » pour passer en mode root puis « apt update » et « apt upgrade » afin de mettre à jour les paquets.

- Installer ProFTPD avec la commande « apt-get install proftpd »

- Modifier le fichier de configuration proftpd avec la commande suivante : « nano /etc/proftpd/proftpd.conf »

- Une fois dans le fichier de configuration de proftpd, renommer le serveur en « serverftp » :

```
ServerName "serverftp"
```

- Dans le fichier de configuration proftpd.conf changer la ligne DefaultRoot en retirant le # au début et changer le répertoire par défaut du serveur de la manière suivante :

```
# Use this to jail all users in their homes  
DefaultRoot /home/FTP/
```

- Sauvegarder les changements avec un ctrl+O puis valider avec la touche Entrée. Enfin quitter avec ctrl+X

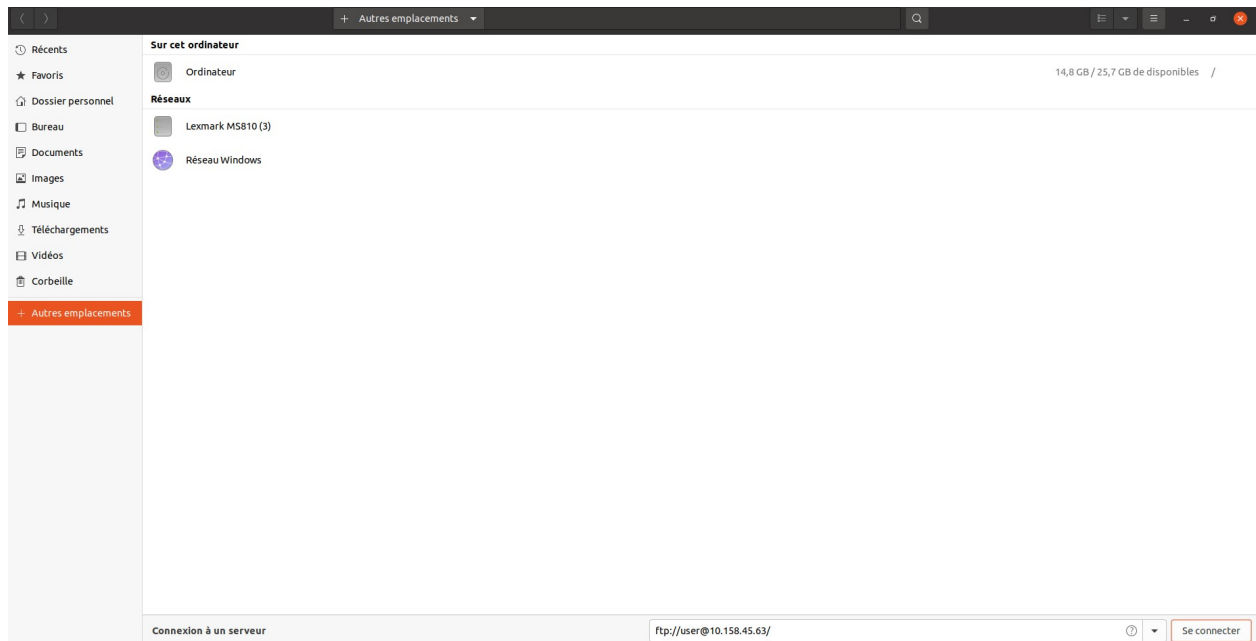
- Se rendre dans le répertoire /home/ avec la commande « cd /home »

- Dans ce répertoire, créer le dossier FTP avec la commande « mkdir FTP » puis changer le propriétaire du répertoire avec la commande « chown user:user /home/FTP/ » afin que l'utilisateur est la possibilité d'apporter des modifications dans ce dernier.

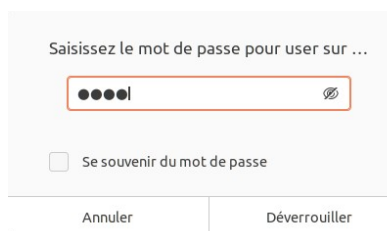
- Relancer le service proftpd avec la commande « systemctl restart proftpd » afin d'appliquer les changements effectués dans le fichier de configuration.

- Tester la connexion au serveur FTP depuis une autre machine (qui servira de machine client -ici une machine Ubuntu Desktop ») avec le compte user (dans le but de vérifier si une connexion sans certificat fonctionne, on ne va pas essayer d'ajouter un certificat sans être sûr qu'une connexion normale fonctionne correctement au préalable, comme ça en cas de problème futur, on saura que la connexion sans certificat fonctionnait correctement et ainsi que le problème est causé par autre chose).

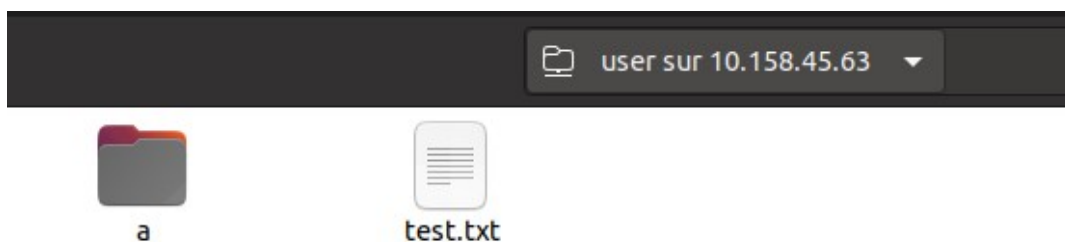
- Sur la machine client, ouvrir l'explorateur de fichiers et sélectionner « autre emplacements » comme montré ci-dessous et renseigner les informations suivantes : « ftp://user@10.158.45.63/ » (ce qui correspond respectivement à l'utilisateur que l'on va utiliser pour s'authentifier et à l'adresse IP du serveur FTP)



- Lors de la première connexion, le mot de passe de l'utilisateur choisi est demandé et il est possible par la suite de l'enregistrer ou non en prévision de nouvelles connexions.



- Une fois connecté, il est possible de créer de nouveaux dossiers et fichiers ainsi que de modifier le contenu de ceux-ci depuis la machine client. On peut vérifier que le transfert de fichiers a lieu entre les 2 machines en effectuant la commande « ls » dans le répertoire « FTP » sur la machine serveurftp.



```
root@serveurftp:/home/FTP# ls
a  test.txt
root@serveurftp:/home/FTP#
```

2) Création et mise en place d'un certificat à l'aide d'OpenSSL :

Création d'une clé privé :

- Se rendre dans le répertoire /etc/ssl avec la commande « cd /etc/ssl »
- Créer un dossier « CLES » avec la commande « mkdir CLES »
- Se rendre dans le dossier nouvellement créé avec la commande « cd CLES »
- Créer une nouvelle clé avec la commande « openssl genrsa -out cleftp.key 4096 »

Création d'un certificat X509 :

- Retourner dans le répertoire /etc/ssl avec la commande « cd /etc/ssl »
- Créer un répertoire « CERTIFICATS » avec la commande « mkdir CERTIFICATS » et se rendre dans ce dossier avec la commande « cd CERTIFICATS »
- Créer un nouveau certificat avec les commandes « openssl req -new -key ../CLES/cleftp.key -out certiftp.csr » et « openssl x509 -req -days 365 -in certiftp.csr -signkey ../CLES/cleftp.key -out certiftp.crt »

Exemple d'informations à renseigner lors de la création du certificat :

```
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:France
Locality Name (eg, city) []:Nevers
Organization Name (eg, company) [Internet Widgits Pty Ltd]:FTP INC
Organizational Unit Name (eg, section) []:FTP 1
Common Name (e.g. server FQDN or YOUR name) []:FTP CERTIF
Email Address []:.

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:.
An optional company name []:.
```

Configuration de ProFTPD avec SSL/TLS :

- Utiliser la commande « nano /etc/proftpd/modules.conf » pour vérifier si TLS est bien activé, comme on peut le voir ci-dessous, la ligne est bien présente par défaut

```
LoadModule mod_ctrls_admin.c
LoadModule mod_tls.c
```

- Utiliser la commande « nano /etc/proftpd/proftpd.conf » afin de dé-commenter la ligne « Include /etc/proftpd/tls.conf » comme suit :

```
# This is used for FTPS connections
#
Include /etc/proftpd/tls.conf
```

- Utiliser la commande « nano /etc/proftpd/tls.conf » afin de vérifier quels éléments de configuration sont renseignés dedans et éventuellement dé-commenter les éléments qui nous intéressent pour notre usage ainsi que renseigner le chemin de la clé et du certificat comme suit :

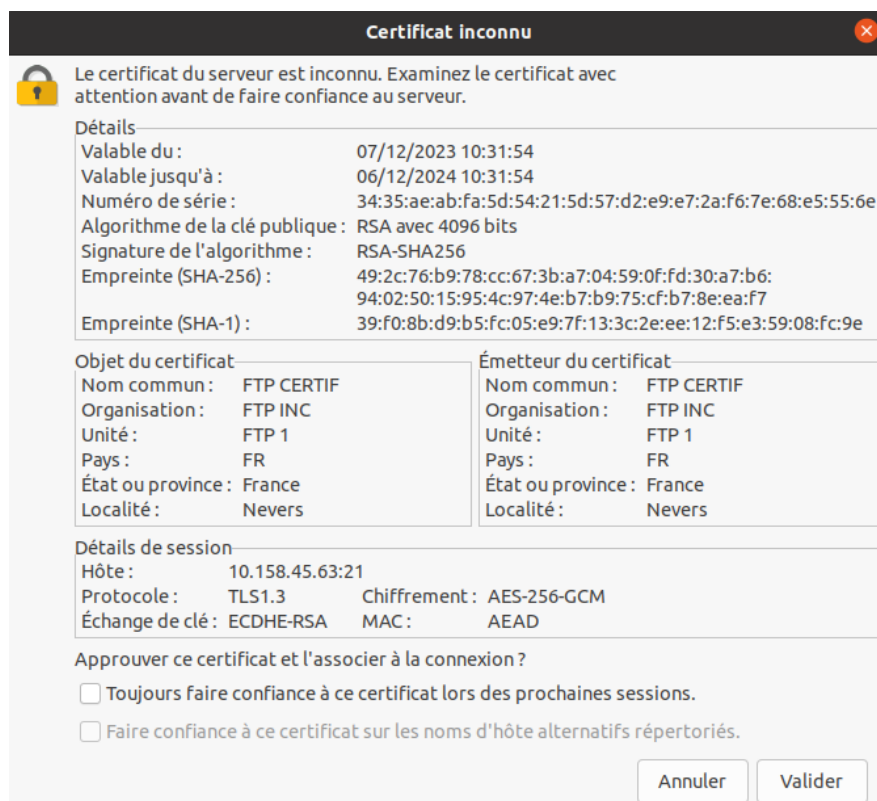
```
<IfModule mod_tls.c>
TLSEngine                                on
TLSLog                                   /var/log/proftpd/tls.log
TLSProtocol                              SSLv23
#
# Server SSL certificate. You can generate a self-signed certificate using
# a command like:
#
# openssl req -x509 -newkey 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
#
TLSRSACertificateFile                    /etc/ssl/CERTIFICATS/certiftp.crt
TLSRSACertificateKeyFile                 /etc/ssl/CLES/cleftp.key
#
# CA the server trusts...
# TLSCACertificateFile [redacted] /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
#
# Per default drop connection if client tries to start a renegotiate
# This is a fix for CVE-2009-3555 but could break some clients.
#
# TLSOptions [redacted] AllowClientRenegotiations
#
# Authenticate clients that want to use FTP over TLS?
#
TLSVerifyClient                         off
#
# Are clients required to use FTP over TLS when talking to this server?
#
# TLSRequired                            on
#
# Allow SSL/TLS renegotiations when the client requests them, but
# do not force the renegotiations. Some clients do not support
# SSL/TLS renegotiations; when mod_tls forces a renegotiation, these
# clients will close the data connection, or there will be a timeout
# on an idle data connection.
#
# TLSRenegotiate                         required off
</IfModule>
```

- Redémarrer le service ProFTPD avec la commande suivante : « `systemctl restart proftpd` » afin de prendre en compte les changements.

Tests depuis une machine client :

Tests avec un utilisateur connu :

- Lorsque l'on essaye de se connecter au serveur FTP depuis la machine client en utilisant Filezilla, le certificat s'affiche comme prévu et l'option de faire confiance ou non au certificat est également disponible sur cette même fenêtre :



- Lors de la connexion un message d'erreur apparaît disant qu'il est impossible de récupérer le contenu du dossier, pour fixer ce problème, modifier le fichier `tls.conf` avec la commande « `nano /etc/proftpd/tls.conf` » et dé-commenter la ligne suivante :

```
TLSOptions NoCertRequest EnableDiags NoSessionReuseRequired
```

Le message d'erreur :

Hôte : 10.158.45.63 Identifiant : user Mot de passe : Port : Connexion rapide ▼

Commande : PASV
 Réponse : 227 Entering Passive Mode (10,158,45,63,168,195).
 Commande : LIST
 Réponse : 150 Opening BINARY mode data connection for file list
 Réponse : 425 Unable to build data connection: Operation not permitted
 Erreur : Impossible de récupérer le contenu du dossier

Site local : /home/user/ Site distant : /

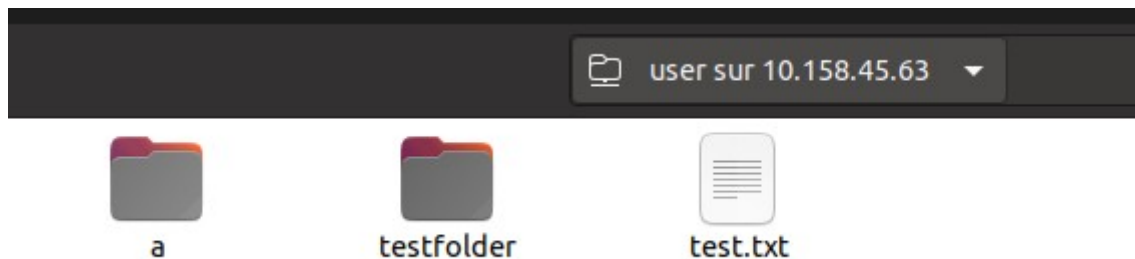
Une fois la modification effectuée :

Hôte : 10.158.45.63 Identifiant : user Mot de passe : Port : Connexion rapide ▼

Statut : vérification du certificat...
 Statut : Connexion TLS établie.
 Statut : Le serveur ne supporte pas les caractères non-ASCII.
 Statut : Connecté
 Statut : Récupération du contenu du dossier...
 Statut : Contenu du dossier "/" affiché avec succès

Site local : /home/user/ Site distant : /

- La connexion depuis l'explorateur de fichiers linux n'a pas de problèmes pour se connecter au serveur FTP (même sans modifier la ligne comme pour Filezilla)

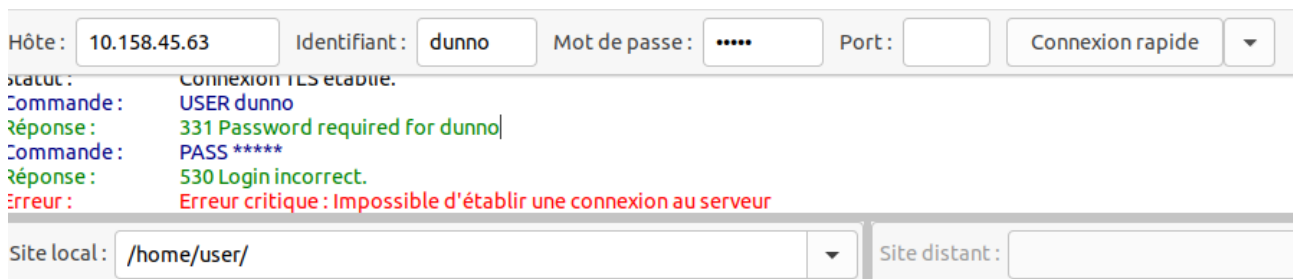


- De même, la connexion et l'utilisation du serveur FTP fonctionne correctement en ligne de commande :

```
user@client-linux-ubuntu:~$ ftp 10.158.45.63
Connected to 10.158.45.63.
220 ProFTPD Server (serverftp) [::ffff:10.158.45.63]
Name (10.158.45.63:user): user
331 Password required for user
Password:
230 User user logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
drwxr-xr-x  2 user  user    4096 Dec  7 08:45 a
drwxr-xr-x  2 user  user    4096 Dec  7 09:58 testfolder
-rw-r--r--  1 user  user      9 Dec  7 08:50 test.txt
226 Transfer complete
ftp>
```

Tests avec un utilisateur inconnu :

- La connexion est censée échouer avec tous les utilisateurs inconnus, dans Filezilla, le message suivant s'affiche en cas de tentative de connexion avec un utilisateur inconnu :



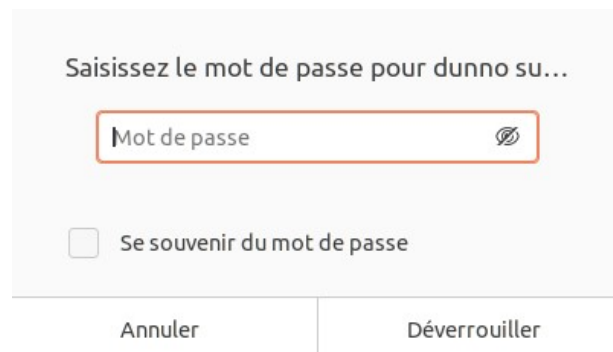
The screenshot shows the FileZilla interface. At the top, there are input fields for 'Hôte' (10.158.45.63), 'Identifiant' (dunno), 'Mot de passe' (masked with dots), and 'Port'. A 'Connexion rapide' button is on the right. Below these, the 'statut' section shows a log of commands and responses: 'Connexion TLS établie.', 'Commande: USER dunno', 'Réponse: 331 Password required for dunno|', 'Commande: PASS *****', 'Réponse: 530 Login incorrect.', and 'Erreur: Erreur critique: Impossible d'établir une connexion au serveur'. At the bottom, there are fields for 'Site local' (/home/user/) and 'Site distant'.

- Depuis l'explorateur de fichiers cela donne :



The screenshot shows the FileZilla file explorer. The address bar contains 'ftp://dunno@10.158.45.63/'. To the right of the address bar is a question mark icon and a dropdown arrow. A 'Se connecter' button is located to the right of the address bar.

- On reste bloqué sur l'écran du mot de passe tant que l'on renseigne des informations d'utilisateurs inconnus



The screenshot shows a password prompt dialog box. The title is 'Saisissez le mot de passe pour dunno su...'. There is a text input field labeled 'Mot de passe' with a red border and a small icon to its right. Below the input field is a checkbox labeled 'Se souvenir du mot de passe'. At the bottom, there are two buttons: 'Annuler' and 'Déverrouiller'.

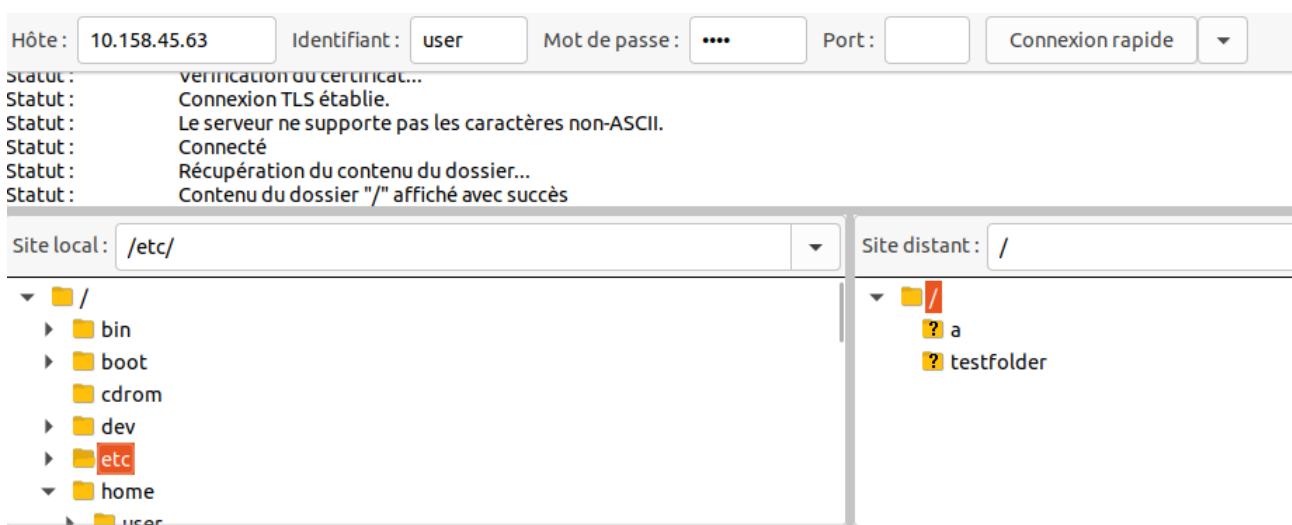
- En ligne de commande, on obtient l'erreur suivante et l'on a pas accès aux commandes tant que l'on ne se connecte pas avec un utilisateur valide :


```
user@client-linux-ubuntu:~$ ftp 10.158.45.63
Connected to 10.158.45.63.
220 ProFTPD Server (serverftp) [::ffff:10.158.45.63]
Name (10.158.45.63:user): dunno
331 Password required for dunno
Password:
530 Login incorrect.
Login failed.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
530 Please login with USER and PASS
ftp: bind: Address already in use
ftp>
```

Procédure d'utilisation :

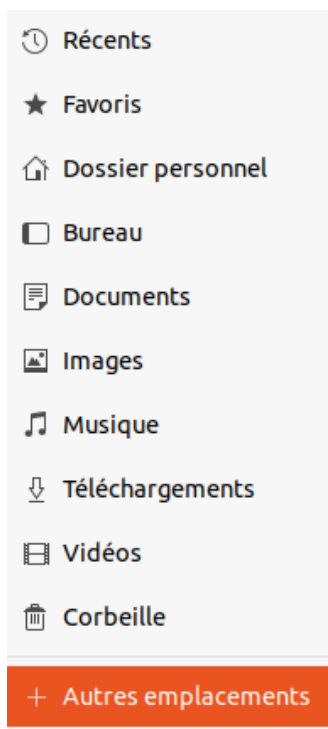
Pour accéder au service FTP avec Filezilla (sur Ubuntu Desktop) :

- Installer le paquet Filezilla avec la commande « apt-get install filezilla » dans le terminal
- Ouvrir filezilla avec la commande « filezilla »
- Dans l'interface qui s'ouvre renseigner l'adresse IP du serveur FTP ainsi qu'un nom d'utilisateur et son mot de passe associé connus du serveur FTP (renseigner le port n'est pas obligatoire)

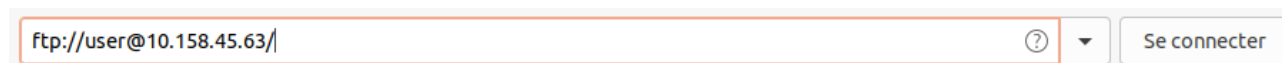


Pour accéder au service FTP avec l'explorateur de fichiers sur Ubuntu Desktop :

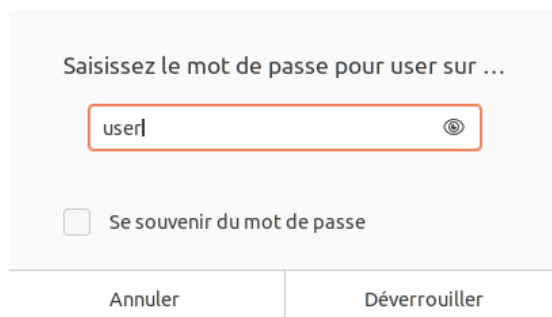
- Ouvrir l'explorateur de fichier et se rendre dans l'onglet « autres emplacements » :



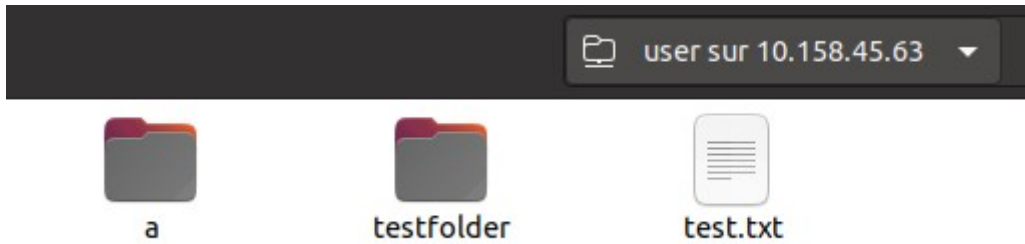
- Dans « Autres emplacements » renseigner la commande « ftp://user@10.158.45.63/ » (user est ici l'utilisateur que l'on souhaite utiliser et l'adresse ip correspond à celle du serveur FTP)



- Dans la fenêtre qui apparaît ensuite, renseigner le mot de passe et choisir ou non d'enregistrer le mot de passe en prévision de futures connexions puis cliquer sur « déverrouiller »



- On accède ensuite au serveur FTP :



Pour accéder au service FTP en ligne de commande sous Linux :

- Dans le terminal, utiliser la commande « `ftp 10.158.45.63` » (à nouveau, l'adresse IP correspond à celle du serveur FTP)

- On nous demande alors de renseigner un nom d'utilisateur :

```
user@client-linux-ubuntu:~$ ftp 10.158.45.63
Connected to 10.158.45.63.
220 ProFTPD Server (serverftp) [::ffff:10.158.45.63]
Name (10.158.45.63:user):
```

- Puis un mot de passe :

```
Name (10.158.45.63:user): user
331 Password required for user
Password:
```

- Une fois ce dernier renseigné, nous avons accès au serveur FTP et aux commandes associés.

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