

Thomas

Session 2022 / 2023

SRENG

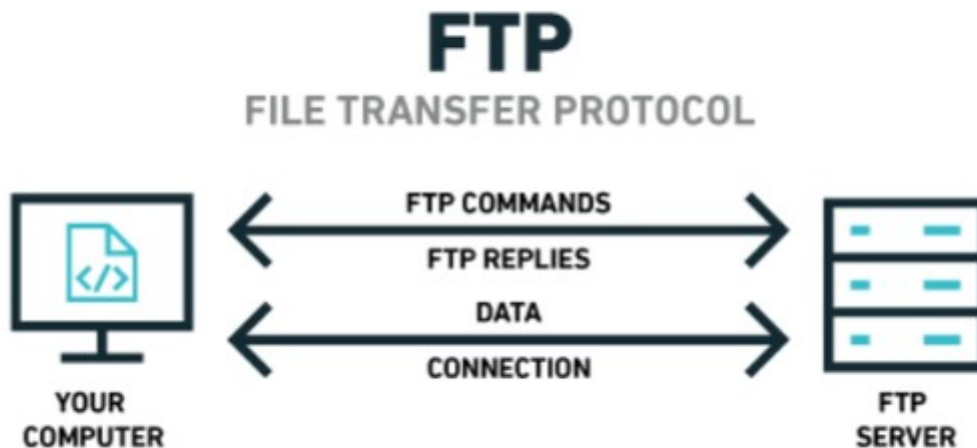
Étienne

RIDOUX

BTS SIO option SISR

Installation et configuration du serveur FTP

Définition : Le **serveur FTP** permet de transférer des fichiers par Internet ou par le biais d'un réseau informatique local. Toute personne en ayant l'autorisation, peut télécharger et envoyer des fichiers sur un ordinateur distant faisant fonctionner un tel serveur. Le port par défaut et le plus souvent utilisé est le port 21.



Pour Linux, il existe différents serveurs FTP, dont la plupart sont open source et se trouvent généralement dans la gestion des paquets de la distribution respective.

L'installation s'effectue donc de manière habituelle via le terminal et avec la commande suivante :

```
sudo apt-get install proftpd
```

Après l'installation, vous pouvez commencer à configurer ProFTPD. Le fichier de configuration **proftpd.conf** qui est nécessaire, se trouve dans `/etc/proftpd/`. Pour l'éditer, il suffit de l'ouvrir avec **l'éditeur de votre choix**. Avec le programme standard Debian nano, cela peut être fait par exemple en utilisant la commande de terminal suivante :

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

Avant d'entrer dans le détail de la configuration de votre serveur FTP sous Debian, vous devez tout d'abord ajuster la configuration de base. Il s'agit de paramètres élémentaires tels que la spécification du nom d'hôte ou du répertoire du serveur que vous souhaitez mettre à disposition pour le chargement et le téléchargement des fichiers. Vous disposez aussi de diverses options de configuration qui se réfèrent à des utilisateurs FTP potentiels, comme le montre l'exemple de configuration suivant :

```
# Spécification du nom d'hôte et du message de bienvenue
ServerName "nom d'hôte/adresse IP"
DisplayLogin "La connexion au serveur FTP sous Debian s'est effectuée avec succès !"

# Instructions générales de connexion
<Global>
  # Autoriser l'accès uniquement avec les interfaces systèmes, qui sont dans /etc/shells définie
  RequireValidShell on
  # Refuser la connexion root
  RootLogin off
  # Spécifie le répertoire FTP auquel l'utilisateur est autorisé à accéder
  DefaultRoot état
</Global>

# Définir les utilisateurs/groupes d'utilisateurs autorisés pour la connexion FT
<Limit LOGIN>
  # L'enregistrement n'est possible que pour les utilisateurs du groupe de référence ftpuser
  # Au lieu d'une longue liste, le groupe autorisé est simplement nié (!)
  DenyGroup !ftpuser
</Limit>
```

Dans cette configuration de base, les utilisateurs ont accès à un répertoire spécifique. Cela a du sens, par exemple, s'ils sont impliqués dans la maintenance d'un site Web et ont donc besoin de **droits d'accès étendus**. Cependant, si la fonction du serveur FTP Linux est d'offrir aux utilisateurs un seul emplacement pour leurs fichiers, vous devez configurer ProFTPD de sorte que l'accès au **répertoire d'origine** soit restreint :

DefaultRoot ~

À la suite de ces modifications, on relance le processus de à l'aide de cette commande :

```
sudo /etc/init.d/proftpd reload
```

CRÉATION D'UN UTILISATEUR FTP

Lorsque vous créez un nouvel utilisateur ProFTPD, vous devez toujours définir */bin/false* comme l'interface système (Shell) de connexion. De cette façon, vous vous assurez que l'utilisateur ne peut accéder qu'au serveur FTP et non à l'ensemble du système. Utilisez la commande de terminal suivante pour entrer */bin/false* dans le fichier des interfaces système (Shells) autorisées :

```
sudo echo "/bin/false" >> /etc/shells
```

Vous pouvez ensuite créer un premier utilisateur :

```
sudo adduser user1 --shell /bin/false --home /home/user1
```

Dans cet exemple, vous créez un compte utilisateur avec le nom « user1 » et créez son répertoire d'origine dans la même étape. Enfin, attribuez un **mot de passe** pour le nouveau compte utilisateur et confirmez le profil. Pour que cet utilisateur nouvellement créé puisse se connecter au serveur FTP de Debian et télécharger des fichiers dans son répertoire exclusif, spécifiez enfin son répertoire d'origine dans le fichier **proftpd.conf** :

```
1 <Directory /home /user1>
2     Umask 022
3     AllowOverride off
4     <Limit LOGIN>
5         AllowUser user1
6         DenyAll
7     </Limit>
8     <Limit ALL>
9         AllowUser user1
10        DenyAll
11    </Limit>
12 </Directory>
```

CONFIGURATION DU CHIFFREMENT SSL/TLS

Le protocole FTP transfère à la fois les informations de connexion et les données envoyées **en texte clair**. Si vous souhaitez configurer un serveur ProFTPD privé qui ne doit pas être accessible à tous, il est donc recommandé de **chiffrer la connexion**. La solution la plus répandue est le chiffrement via SSL/TLS, que vous pouvez mettre en place en peu d'efforts et en utilisant le **logiciel gratuit OpenSSL**. La boîte à outils cryptographiques est incluse et déjà installée par défaut dans la gestion des paquets Debian. De manière alternative, l'installation peut être réalisée de la manière habituelle :

```
apt-get install openssl
```

Utilisez ensuite OpenSSL, pour créer un certificat. Comme vous devez le stocker quelque part, créer d'abord **le dossier approprié dans le répertoire ProFTPD** :

```
mkdir /etc/proftpd/ssl
```

Générez maintenant le **certificat** (*proftpd.cert.pem*) et la **clef** (*proftpd.key.pem*) avec une durée de vie d'un an pour votre serveur FTP Linux en spécifiant cet emplacement et en utilisant la commande suivante :

```
openssl req -new -x509 -days 365 -nodes -out /etc/proftpd/ssl/proftpd.cert.pem -keyout /etc/proftpd/ssl/proftpd.key.pem
```

Après avoir créé votre propre certificat et votre clef privée, vous devez activer la technologie de chiffrement pour le serveur ProFTPD. Pour cela, le logiciel du serveur FTP sur Debian fournit le module **mod_tls**, qui est installé par défaut mais désactivé. Pour l'activation, des ajustements supplémentaires dans le fichier *proftpd.conf* sont nécessaires. Ouvrez le fichier de configuration et recherchez l'entrée suivante :

```
<IfModule mod_tls.c>
```

```
TLSEngine off
```

```
</IfModule>
```

Assigner la valeur „on“ à la directive TLS Engine et étendre enfin la section comme suit :

```
1 <IfModule mod_tls.c>
2   TLSEngine      on
3   TLSLog         /var/log/proftpd/tls.log
4   TLSProtocol    TLSv1 TLSv1.1 TLSv1.2
5   TLSRSACertificateFile /etc/proftpd/ssl/proftpd.cert.pem
6   TLSRSACertificateKeyFile /etc/proftpd/ssl/proftpd.key.pem
7   TLSVerifyClient off
8   TLSRequired    on
9 </IfModule>
```

De cette manière, vous avez non seulement activé le chiffrement SSL/TLS pour votre serveur FTP sur Debian, mais vous avez aussi effectué les paramètres les plus importants au cours de la même étape. **Le fichier log pour l'enregistrement des connexions FTP** (*TLSLog*) est défini de la même manière que les chemins d'accès au certificat (*TLSRSACertificateFile*) et à la clef (*TLSRSACertificateKeyFile*). Les versions de protocole possibles (protocole TLS) sont aussi indiquées. Les deux dernières lignes signifient enfin que le module ne vérifie pas les certificats présentés par le client (*TLSVerifyClient*) et que le **chiffrement est une condition de base** pour établir une connexion (*TLSRequired*). Après le redémarrage du serveur ProFTPD, les nouveaux paramètres prennent effet :

```
sudo /etc/init.d/proftpd restart
```

SE CONNECTER AU SERVEUR PROFTPD

Si vous avez activé SSL/TLS pour ProFTPD (comme recommandé dans ce tutoriel sur le serveur FTP sous Debian), les utilisateurs ont besoin **d'un client FTP qui supporte les connexions chiffrées**. L'un des représentants les plus importants est FileZilla qui n'est pas seulement disponible pour Debian et d'autres distributions Linux, mais aussi pour macOS et Windows. Ainsi, le programme open source est la solution optimale pour vous et tous les autres utilisateurs d'**accéder au serveur FTP à partir de différentes plateformes**.