



OFPPT

مكتب التكوين المهني وإنعاش الشغل

Office de la Formation Professionnelle
et de la Promotion du Travail

Complexe de Formation dans les Métiers des Nouvelles Technologies de l'Information, de
l'Offshoring et de l'Electronique -Oujda

Module : Administration d'un Réseau sous Linux

**Installation et configuration du serveur VSFTP
sous Centos**

Formatrice : ZITI Iham

Sommaire

| | |
|---|----|
| 1. Présentation | 3 |
| 2. VSFTPD..... | 3 |
| 3. Installation..... | 3 |
| 4. Configuration..... | 4 |
| 5. Utilisateur Linux..... | 4 |
| ftpusers et user_list..... | 6 |
| 6. Test (client)..... | 6 |
| 6.1 Commande ftp..... | 6 |
| 6.2 File Zilla (Windows) | 7 |
| 6.3 Navigateur | 8 |
| 7. Utilisateur virtuel (Format berkeley)..... | 8 |
| 8. Référence | 10 |

1. Présentation

Le FTP (File Transfer Protocol) ou protocole de transfert de fichiers est un protocole de communication dédié à l'échange informatique de fichiers sur un réseau TCP/IP. Il intervient au niveau de la couche application du modèle OSI (couche n°7) et utilise TCP comme protocole de transport.

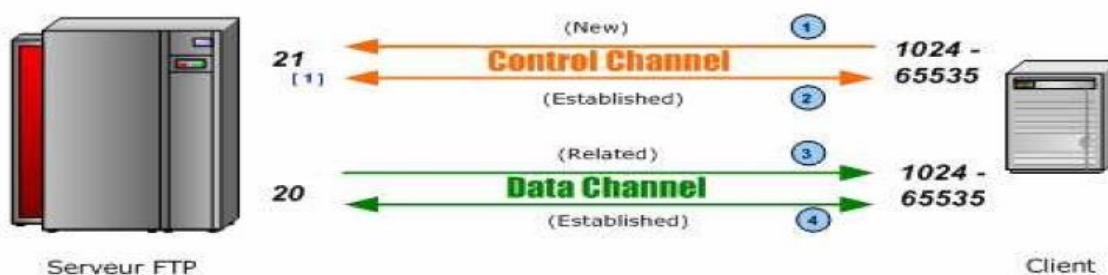
FTP est un protocole orienté connexion. C'est-à-dire qu'il y a trois étapes :

- Etablir une connexion entre le site local et le site distant
- Effectuer les traitements désirés
- Fermer la connexion

FTP utilise deux connexions TCP pour transférer un fichier :

- Une connexion de contrôle.
- Une connexion de transfert de données.

Pour la connexion de contrôle, le numéro de port utilisé par le serveur ftp est 21. Pour la connexion de transfert de données, le numéro de port utilisé par le serveur ftp est 20. Le client, quand à lui, obtient un numéro de port dynamiquement.



2. VSFTPD

vsftpd est un daemon FTP très léger, rapide et sécurisé. Il peut gérer des services FTP de tous types. Vsftpd est un serveur FTP conçu avec la problématique d'une sécurité maximale. Il fait ce que l'on appelle du FTPS ou encore SFTP c'est-à-dire qu'il utilise le protocole SSL/TLS pour la sécurisation des données

3. Installation

vsftpd étant le serveur FTP choisi par défaut par Fedora, celui-ci est directement accessible via yum ou **dnf** :

```
#dnf install vsftpd
```

Une fois l'installation effectuée, pour que le serveur se lance automatiquement au démarrage :

```
#systemctl enable vsftpd.service
```

Pour démarrer et stopper le service, les commandes respectives sont :

```
# systemctl start vsftpd.service
# systemctl stop vsftpd.service
```

Normalement votre système doit déjà avoir un utilisateur ftp et un groupe ftp :

```
$ grep ftp /etc/group
$ grep ftp /etc/passwd
```

4. Configuration

Le fichier de configuration de vsftpd se trouve dans le répertoire `/etc/vsftpd/` et se nomme `vsftpd.conf`

Il y a plusieurs façon de gérer l'utilisateur ftp:

- En créant un utilisateur linux pour chaque espace ftp.
- en utilisant une base de donnée de type Berkeley (mode utilisateurs virtuels)

5. Utilisateur Linux

Créer une sauvegarde du fichier de configuration `/etc/vsftpd.conf` , en cas de problème cela peut toujours être utile

```
#cp -i /etc/vsftpd.conf /etc/vsftpd.conf_BACKUP
```

Editer le fichier de configuration `/etc/vsftpd.conf` pour vérifier et modifier certains paramètres.

Remarque: les commentaires dans ce fichier commencent par le caractère # (dièse), donc les paramètres écrits après # seront ignorés.

```
#Pas de connexions en mode anonymous
anonymous_enable=NO
#Spécifie le port sur lequel vsftpd doit être à l'écoute de connexions réseau.
listen_port=21
#Autoriser les utilisateurs locaux puissent se connecter
local_enable=YES

#Autoriser les utilisateurs à remonter des fichiers sur le serveur
write_enable=YES

#Fixer le masque local a 022 (les fichiers remontés auront des droits en 755)
local_umask=022
```

```
# Refus des droits d'écriture pour les anonymes (et donc utilisateurs virtuels)
anon_upload_enable=NO

# pas de création de répertoire
anon_mkdir_write_enable=NO

# pas de création, suppression, renommage de répertoire ...
anon_other_write_enable=NO

# Les actions des utilisateurs soient logees
xferlog_enable=YES

# Les logs seront enregistrés dans le fichier /var/log/vsftpd.log
xferlog_file=/var/log/vsftpd.log

#Temps avant déconnexion sur une session inactive
idle_session_timeout=600

#Temps avant déconnexion sur une session active
data_connection_timeout=120
# Nombre maximum de connexion simultanée
max_clients=50

# Nombre maximum de connexion venant de la même IP
max_per_ip=4

# Les transferts en ASCII sont souvent source de confusions
ascii_upload_enable=NO
ascii_download_enable=NO

# Banniere de bienvenue
ftpd_banner=Bienvenue sur mon ftp perso

# Limiter les utilisateurs a leur repertoire
chroot_local_user=YES
chroot_list_enable=NO
allow_writeable_chroot=YES

# Les heures d'enregistrement des fichiers seront affichees a l'heure locale
use_localtime=YES

#Le serveur fonctionne en mode standalone
listen=YES
listen_ipv6=NO

# verifie que la commande PORT provienne bien du port 20 de la machine cliente
connect_from_port_20=YES

# Par securite, on interdit la commande ABOR
async_abor_enable=NO
```

ftusers et user_list

Ces deux fichiers ont la même vocation : interdire des utilisateurs. En effet, ils contiennent tous les deux une liste d'utilisateurs pour lesquels le serveur FTP refusera toute connexion.

- Le premier (ftusers) est utilisé via PAM dans la configuration par défaut faite sur Fedora. A la connexion d'un utilisateur, PAM vient lire ce fichier et si l'identifiant de connexion utilisé est dans ce fichier, la connexion est refusée.
- Le second (user_list) est utilisé directement par vsftpd. Il peut avoir deux usages : soit les seuls utilisateurs contenus dans ce fichier ont le droit de se connecter, soit l'accès leurs est systématiquement refusé.

Par exemple pour refuser les utilisateurs du fichier « user_list » il faut modifier les lignes suivante :

```
# Fichier de users
userlist_file=/etc/vsftpd/user_list // Pour la version Centos7 nous avons pas besoin d'ajouter
cette ligne
# Chargement de la liste userlist_file
userlist_enable=YES
```

6. Test (client)

Les logiciels clients sont nombreux, certains sont en ligne de commande (par exemple la commande ftp, implémentée en standard sous de nombreux systèmes d'exploitation), mais une grande majorité permet de manipuler des fichiers sous une interface graphique (FileZilla,gFTP,AxyFTP par exemple), rendant les transferts de fichiers plus conviviaux.

6.1 Commande ftp

- Se connecter à un serveur FTP

```
$ftp Nom Serveur FTP (ou Adresse IP)
```

- Explorer et voir la liste

Utiliser la commande ls

```
>ls
```

- Navigation

Utiliser la commande pwd

```
>pwd
```

- Accéder à un dossier

Utiliser la commande cd

```
>cd nom du dossier
```

- Lister le dossier local courant

Utiliser la commande !pwd

```
>!pwd
```

- Changer le répertoire local

Utiliser la commande lcd

```
>lcd
```

- Télécharger des fichiers

Vérifier l'emplacement local après utiliser la commande get

```
>get nom fichier
```

Pour télécharger plus d'un fichier utiliser la commande mget (multi get)

```
>mget fichier1 fichier2 fichier3
```

- Uploader des fichiers

Vérifier l'emplacement local après utiliser la commande put

```
>put nom fichier
```

La commande put s'utilise comme get, donc la commande mput permet d'uploader plusieurs fichiers

6.2 File Zilla (Windows)

- Hôte : utiliser le nom du domaine ou adresse ip du serveur
- Identifiant : Utilisateur FTP
- Mot de passe : Le mot de passe de l'utilisateur FTP
- Port ” – le port de données du serveur FTP. le port par défaut d'un FTP est 21 , cependant, ce champ n'est pas obligatoire.

6.3 Navigateur

Nous pouvons utiliser le navigateur Web pour réaliser de tels transferts de fichiers. Dans la barre d'adresse, au lieu d'une adresse http://, tapez ftp:// suivi de l'adresse du serveur FTP que vous souhaitez utiliser.

Si le serveur accepte d'être contacté depuis un navigateur Web, vous voyez alors apparaître une fenêtre de dialogue. Entrez alors votre nom et mot de passe. Cliquez ensuite sur Ouvrir une session.

7. Utilisateur virtuel (Format berkeley)

Comme la plupart des autres serveurs FTP (ProFTPD, pure-ftpd), vsftpd gère les utilisateurs virtuels, c'est-à-dire la possibilité de créer des comptes utilisateurs sans que ceux-ci ne soient des utilisateurs système (ils sont en fait tous "mappés" sur un utilisateur système dédié à cela). La particularité de vsftpd est qu'il utilise PAM pour l'authentification des utilisateurs. Nous avons donc autant de possibilités d'authentification que PAM en propose.

Dans le cours nous allons traiter le format **Format berkeley**

Installer la base de données Berkeley (db4)

Dans cette méthode, nous utilisons la base de données Berkeley (db4 (version4) pour stocker les noms d'utilisateurs virtuels avec leurs mots de passe.) Installez d' **abord le paquet db4-utils** s'il n'est pas installé:

```
#yum install db4-utils db4
```

Créer un fichier de base de données pour les utilisateurs virtuels

Créez d'abord un fichier texte et entrez les noms d'utilisateurs virtuels et leurs mots de passe un par un. Ensuite, créez le fichier db à partir du fichier texte brut. Ce fichier doit se terminer par un retour à la ligne.

Par exemple, je crée un fichier texte brut appelé **login.txt** dans le répertoire **/etc/vsftpd** avec le nom d'utilisateur **ilham** et **amina** le mot de passe **mdpilham** et **ofppt** :

```
ilham
mdpilham
amina
ofppt
~
```

Exécutez la commande suivante pour créer un fichier de base de données:

```
#db_load -T -t hash -f login.txt login.db
#chmod 600 login.db
```


Configuration du PAM

Editez le fichier `/etc/pam.d/vsftpd`, commenter toutes les lignes existantes et ajouter les lignes suivantes :

```
auth    required    pam_userdb.so db=/etc/vsftpd/login
account required    pam_userdb.so db=/etc/vsftpd/login
session required    pam_loginuid.so
```

```
#%PAM-1.0
auth    required    pam_userdb.so db=/etc/vsftpd/login
account required    pam_userdb.so db=/etc/vsftpd/login
#session optional    pam_keyinit.so force revoke
#auth    required    pam_listfile.so item=user sense=deny file=/etc/vsftpd/ftpusers onerr=succeed
#auth    required    pam_shells.so
#auth    include     password-auth
#account include     password-auth
session required    pam_loginuid.so
#session include     password-auth
~
```

Configuration VSFTPD

Editez le fichier `/etc/vsftpd/vsftpd.conf`

```
#vi /etc/vsftpd/vsftpd.conf
```

Assurez-vous d'avoir ajouté ou modifié les lignes suivantes, comme indiqué ci-dessous:

```
# On autorise les connexions des utilisateurs locaux. C'est indispensable
# pour que les utilisateurs virtuels (mappés sur un utilisateur local)
# puissent se connecter (les "vrais" utilisateurs locaux sont ensuite désactivés)
# avec le fichier user_list
local_enable=YES

## Activer les utilisateurs virtuels
guest_enable = yes

## Les utilisateurs virtuels utiliseront les mêmes autorisations que les utilisateurs anonymes
virtual_use_local_privs = yes

# Décommentez ceci pour activer n'importe quelle forme de commande d'écriture FTP.
write_enable = yes

## Nom du fichier PAM
pam_service_name = vsftpd

## Home Directory pour les utilisateurs virtuels
user_sub_token= $ USER
local_root = / home/ftp/$ USER

# Vous pouvez spécifier une liste explicite d'utilisateurs locaux à chroot () à leur domicile
# répertoire. Si chroot_local_user est YES, alors cette liste devient une liste de
# utilisateurs à ne pas chrooter ().
chroot_local_user = yes
```

```
## Masquer les ID de l'utilisateur
hide_ids = yes
```

Enregistrez et quittez le fichier.

Créez maintenant des répertoires personnels pour les utilisateurs virtuels:

```
# mkdir /home/vftp
# mkdir -p /home/vftp/{amina,ilham}
# chown -R ftp:ftp /home/vftp
```

```
[root@localhost vsftpd]# ls -l /home/
total 12
drwxr-xr-x  3 ftp  ftp  4096  3 déc.  19:45 ftp
```

Démarrer ou redémarrer le service vsftpd:

```
[root@localhost vsftpd]# systemctl restart vsftpd
```

Test

Essayez de vous connecter au serveur FTP en utilisant l'utilisateur virtuel **amina** avec le mot de passe **ofppt** :

```
[root@localhost vsftpd]# ftp localhost
Connected to localhost (127.0.0.1).
220 Welcome to blah FTP service.
Name (localhost:root): amina
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
227 Entering Passive Mode (127,0,0,1,61,22).
150 Here comes the directory listing.
226 Directory send OK.
ftp> pwd
257 "/home/ftp/amina" is the current directory
ftp> █
```

8. Référence

<https://www.cyberciti.biz/tips/centos-redhat-vsftpd-ftp-with-virtual-users.html>

https://doc.fedora-fr.org/wiki/Vsftpd:_Installation_et_configuration

<https://openclassrooms.com/courses/les-bases-du-ftp-sous-ms-dos>