

# RÉSUMÉ THÉORIQUE – FILIÈRE INFRASTRUCTURE DIGITALE

## M205-Administration réseau sous linux

120 heures

# SOMMAIRE


1. Présentation de protocole FTP
2. Description des ports et modes multiples de FTP
3. Installation et manipulation de serveur vsftpd
4. Options de configurations
5. Démarrage de multiples instances de vsftpd
6. Sécurité FTP
7. Travaux pratiques




# 01 - Présentation de protocole FTP

## Introduction et définition

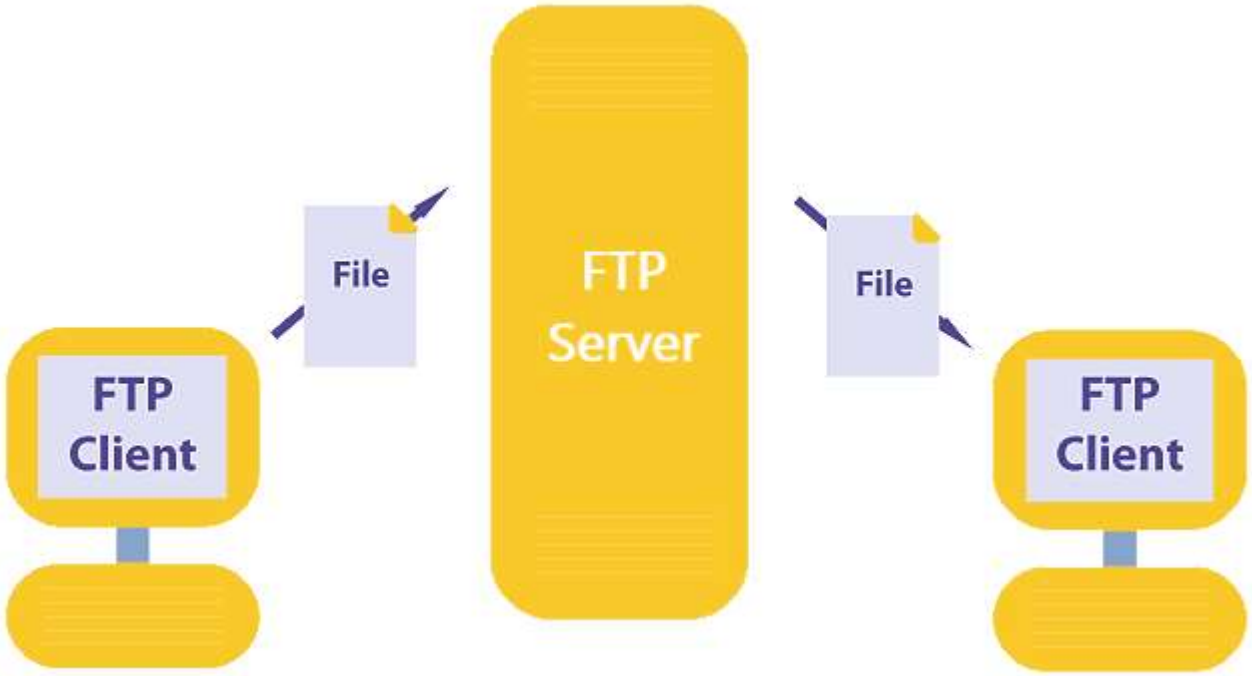
**File Transfer Protocol** (protocole de transfert de fichier, ou **FTP**), est un protocole de communication destiné au partage de fichiers sur un réseau TCP/IP.

- Il permet, depuis un ordinateur, de copier des fichiers vers un autre ordinateur du réseau, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur.
- La mise en place du protocole FTP date de 1971, date à laquelle un mécanisme de transfert de fichiers (décrit dans le RFC 114) entre les machines du MIT (Massachussetts Institute of Technology) avait été mis au point.
- Plusieurs RFC viennent compléter cette spécification, comme la RFC 2228 de juin 1997 pour l'ajout d'extensions de sécurité ou la RFC 2428 de septembre 1998 qui ajoute la prise en charge du protocole IPv6 et définit un nouveau type de mode passif.

Copyright - Tout droit réservé - OFPPT

# 01 - Présentation de protocole FTP

## Introduction et définition



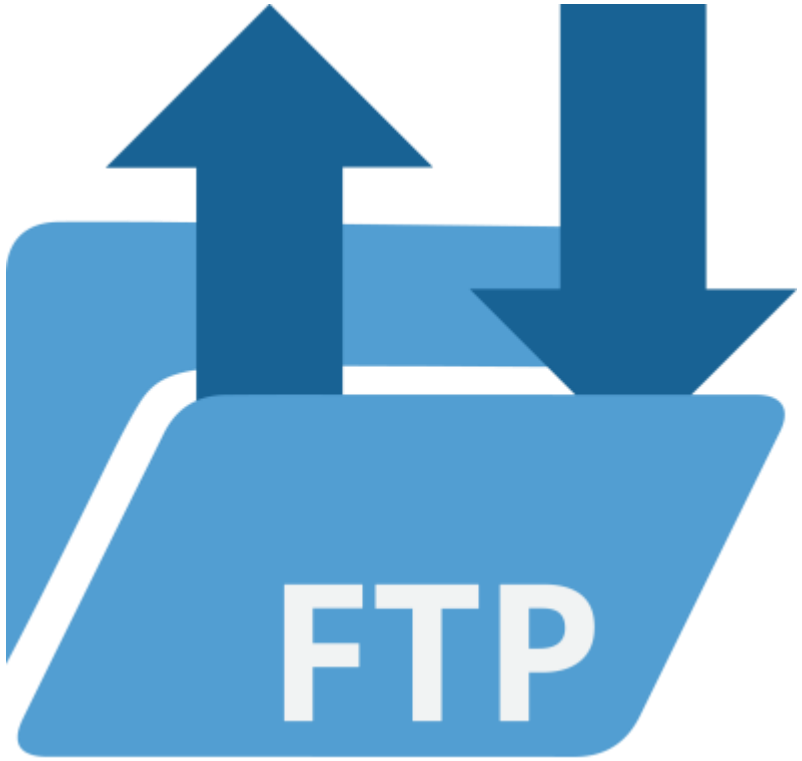

- En pratique, le serveur est un ordinateur sur lequel fonctionne un **logiciel**, maniable aussi en **ligne de commande**, lui-même appelé serveur FTP, qui rend publique une arborescence de fichiers similaire à un système de fichiers UNIX.
- Ce qui rend FTP **non sécurisé**, c'est que tout ce qui est envoyé entre le client et le serveur FTP se fait en texte clair. Le protocole FTP a été créé à une époque où la plupart des communications informatiques se faisaient sur des réseaux privés, lignes téléphoniques ou par ligne commutée, où le cryptage n'était pas considéré comme critique.
- Si vous utilisez FTP sur un réseau public, quelqu'un reniflant la ligne n'importe où entre le client et le serveur pourra voir non seulement les données transférées mais aussi le processus d'authentification (informations de connexion et de mot de passe).

Copyright - Tout droit réservé - OFPPT

# 01 - Présentation de protocole FTP

## Introduction et définition

- Ainsi, FTP n'est pas bon pour partager des fichiers en privé (utilisez des commandes SSH telles que **sftp**, **scp** ou **rsync** si vous avez besoin de transferts de fichiers privés et cryptés). Cependant, si vous partagez des documents publics, des référentiels de logiciels open source ou d'autres données librement disponibles, FTP est un bon choix.
- Quel que soit le système d'exploitation que les utilisateurs utilisent, ils disposent sûrement d'une application de transfert de fichiers FTP pour obtenir les fichiers que vous proposez à partir de votre serveur FTP.
- Lorsque les utilisateurs s'authentifient auprès d'un serveur FTP sous Linux, leurs noms d'utilisateur et mots de passe sont authentifiés par rapport aux comptes d'utilisateur et mots de passe Linux standard. Il existe également un compte spécial non authentifié utilisé par le serveur FTP appelé **anonymous**. Le compte anonymous est accessible à tous car il ne nécessite pas de mot de passe valide.
- En fait, le terme serveur FTP anonyme est souvent utilisé pour décrire un serveur FTP public qui ne nécessite pas (ni même n'autorise) l'authentification d'un compte utilisateur légitime.

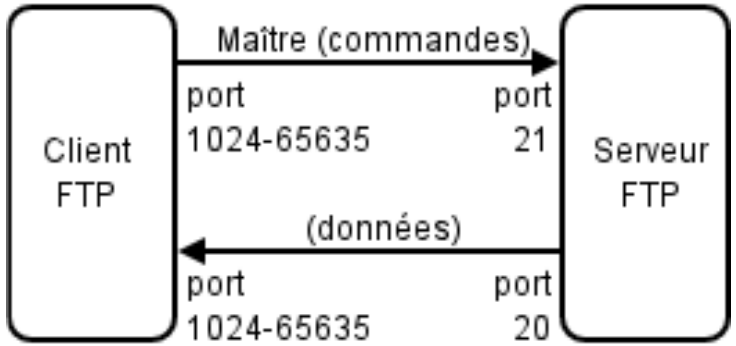



Copyright - Tout droit réservé - OFPPT

# 02 - Description des ports et modes multiples de FTP

## Explication: mode actif

- Après la phase d'authentification (sur le port de contrôle, port **TCP 21**), une deuxième connexion est établie entre le client et le serveur. FTP prend en charge les types de connexion **actifs** et **passifs**.

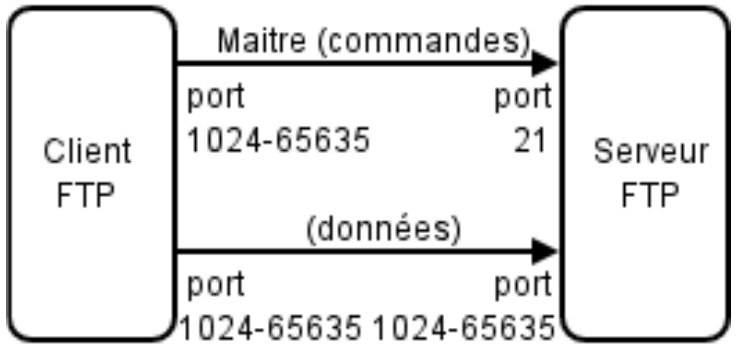



- En mode actif, c'est le **client FTP** qui détermine le port de connexion à utiliser pour permettre le transfert des données. Ainsi, pour que l'échange des données puisse se faire, le serveur FTP initialisera la connexion de son port de données **(port 20)** vers le port spécifié par le client.
- Le client devra alors configurer son pare-feu pour autoriser les nouvelles connexions entrantes afin que l'échange des données se fasse. De plus, il peut s'avérer problématique pour les utilisateurs essayant d'accéder à des serveurs FTP lorsque ces utilisateurs sont derrière une passerelle NAT. Étant donnée la façon dont fonctionne le NAT, le serveur FTP lance la connexion de données en se connectant à l'adresse externe de la passerelle NAT sur le port choisi. Certaines passerelles NAT n'ayant pas de correspondance pour le paquet reçu dans la table d'état, le paquet sera ignoré et ne sera pas délivré au client.

Copyright - Tout droit réservé - OFPPT

# 02 - Description des ports et modes multiples de FTP

## Explication: mode passif

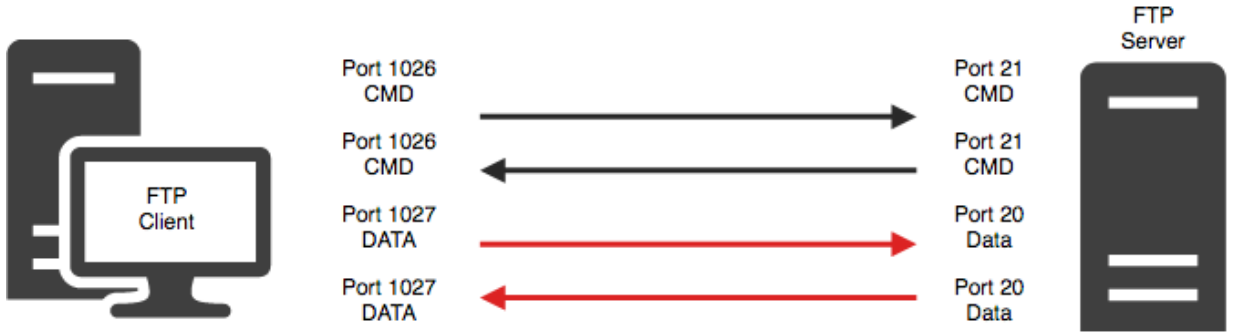



- En mode passif, le serveur FTP détermine lui-même le port de connexion à utiliser pour permettre le transfert des données (data connexion) et le communique au client. En cas de présence d'un pare-feu devant le serveur, celui-ci devra être configuré pour autoriser la connexion de données.
- L'avantage de ce mode est que le serveur FTP n'initialise aucune connexion. Ce mode fonctionne sans problème avec des clients derrière une passerelle NAT. Dans les nouvelles implémentations, le client initialise et communique directement par le **port 21** du serveur ; cela permet de simplifier les configurations des pare-feu serveur.

Copyright - Tout droit réservé - OFPPT

# 02 - Description des ports et modes multiples de FTP

## Explication

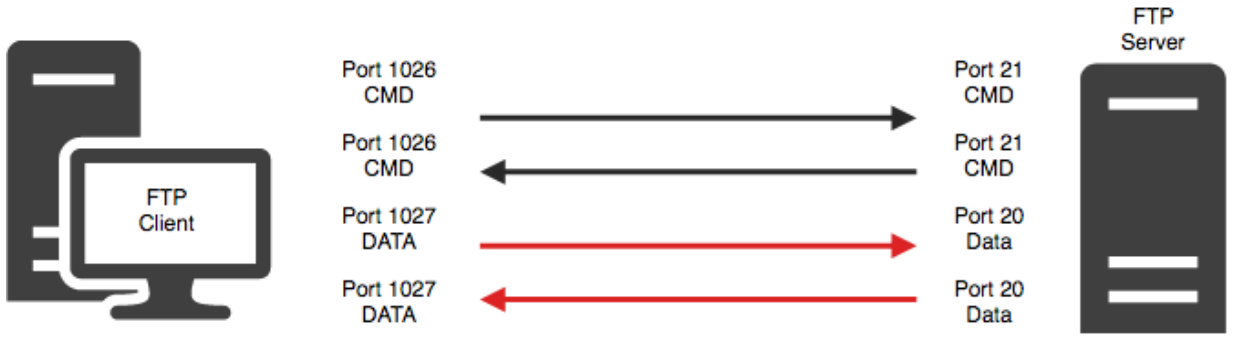



- De nombreux navigateurs prennent en charge le mode FTP passif afin que si le client dispose d'un pare-feu, il ne bloque pas le port de données que le serveur FTP pourrait utiliser en mode actif.
- La prise en charge du mode passif nécessite un travail supplémentaire sur le pare-feu du serveur pour permettre des connexions aléatoires aux ports supérieurs à 1023 sur le serveur.
- Une fois la connexion établie entre le client et le serveur, le répertoire actuel du client est établi. Pour l'utilisateur anonyme, le répertoire **/var/ftp** est le répertoire personnel pour **Fedora**, et c'est **/srv/ftp** pour **Ubuntu** et la plupart des distributions basées sur Debian. L'utilisateur anonyme ne peut pas sortir de la structure du répertoire /var/ftp.
- Si un utilisateur régulier, disons AHMED, se connecte au serveur FTP, **/home/ahmed** est le répertoire actuel de ahmed, mais ce dernier peut passer à n'importe quelle partie du système de fichiers pour lequel il **a l'autorisation**.
- Les clients FTP orientés commandes (tels que les commandes lftp et ftp) passent en mode interactif une fois connectés au serveur. À partir de **l'invite de commande** qui s'affiche, vous pouvez exécuter de nombreuses commandes similaires à celles que vous utiliseriez à partir du **shell**.

Copyright - Tout droit réservé - OFPPT

# 02 - Description des ports et modes multiples de FTP

## Explication




- Vous pouvez utiliser **pwd** pour voir votre répertoire actuel, **ls** pour lister le contenu du répertoire et **cd** pour changer de répertoire. Lorsque vous voyez un fichier que vous voulez, vous utilisez les commandes **GET** et **PUT** pour télécharger des fichiers ou les charger sur le serveur, respectivement.
- Avec des outils graphiques pour accéder aux serveurs FTP (comme un navigateur Web), vous tapez l'**URL** du site que vous souhaitez visiter (**comme ftp://docs.example.com**) dans la zone d'emplacement du navigateur. Si vous n'ajoutez pas de nom d'utilisateur ou de mot de passe, une connexion anonyme est établie et le contenu du répertoire d'accueil du site est affiché. Cliquez sur les liens vers les répertoires pour accéder à ces répertoires. Cliquez sur les liens vers les fichiers pour afficher ou télécharger ces fichiers sur votre système local.

Copyright - Tout droit réservé - OFPPT

# 03 - Installation et manipulation de serveur vsftpd

## Installation




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

```
Dépendances résolues.
================================================================================
 Paquet                  Architecture            Version                 Dépôt                    Taille
================================================================================
Installation:
 vsftpd                  x86_64                  3.0.3-46.fc35           updates                  158 k

Résumé de la transaction
================================================================================
Installer  1 Paquet

Taille totale des téléchargements : 158 k
Taille des paquets installés : 348 k
Voulez-vous continuer ? [o/N] : o
Téléchargement des paquets :
vsftpd-3.0.3-46.fc35.x86_64.rpm                                 127 kB/s | 158 kB     00:01
--------------------------------------------------------------------------------
Total                                                            73 kB/s | 158 kB     00:02
Test de la transaction
La vérification de la transaction a réussi.
Lancement de la transaction de test
Transaction de test réussie.
Exécution de la transaction
  Préparation          :                                                          1/1
  Installation         : vsftpd-3.0.3-46.fc35.x86_64                              1/1
  Exécution du scriptlet: vsftpd-3.0.3-46.fc35.x86_64                             1/1
  Vérification de      : vsftpd-3.0.3-46.fc35.x86_64                              1/1

Installé:
  vsftpd-3.0.3-46.fc35.x86_64

Terminé !
```

Copyright - Tout droit réservé - OFPPT

# 03 - Installation et manipulation de serveur vsftpd

## Installation




- 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**

```
[root@fedorasrv ~]# systemctl enable vsftpd.service
Created symlink /etc/systemd/system/multi-user.target.wants/vsftpd.service → /usr/lib/systemd/system/vsftpd.service.
[root@fedorasrv ~]# systemctl start vsftpd.service
[root@fedorasrv ~]# systemctl status vsftpd.service
● vsftpd.service - Vsftpd ftp daemon
     Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled; vendor preset: disabled)
     Active: active (running) since Wed 2022-03-30 15:22:58 +00; 7s ago
    Process: 212302 ExecStart=/usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf (code=exited, status=0/SUCCESS)
   Main PID: 212303 (vsftpd)
      Tasks: 1 (limit: 4569)
     Memory: 552.0K
        CPU: 5ms
     CGroup: /system.slice/vsftpd.service
             └─212303 /usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf

mars 30 15:22:58 fedorasrv systemd[1]: Starting Vsftpd ftp daemon...
mars 30 15:22:58 fedorasrv systemd[1]: Started Vsftpd ftp daemon.
```

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

```
[root@fedorasrv ~]# cat /etc/passwd | grep ftp
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
[root@fedorasrv ~]# cat /etc/group | grep ftp
ftp:x:50:
```

Copyright - Tout droit réservé - OFPPT

# 03 - Installation et manipulation de serveur vsftpd

## Configuration




- Une fois l'installation est faite, on passe à la configuration. Dans le répertoire /etc/vsftpd/ on trouve les éléments suivants:

```
[root@fedorasrv ~]# ls -l /etc/vsftpd/
total 20
-rw-------. 1 root root  125 13 oct.  16:26 ftpusers
-rw-------. 1 root root  361 13 oct.  16:26 user_list
-rw-------. 1 root root 5077 30 mars  15:47 vsftpd.conf
```

- Le fichier **vsftpd.conf** est le fichier de configuration principale
- **ftpusers** 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. Pourquoi deux fichiers (au contenu identique) ?
    - **Ftpusers** 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.
    - **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.

```
# vsftpd userlist
# If userlist_deny=NO, only allow users in this file
# If userlist_deny=YES (default), never allow users in this file, and
# do not even prompt for a password.
# Note that the default vsftpd pam config also checks /etc/vsftpd/ftpusers
# for users that are denied.
root
bin
daemon
adm
lp
sync
shutdown
halt
mail
news
uucp
operator
games
nobody
```

Copyright - Tout droit réservé - OFPPT

# 03 - Installation et manipulation de serveur vsftpd

## Configuration




Après on passe à la configuration du fichier principal:

- **On écoute sur le port 21/tcp ;**
- **On est en standalone ;**
- **On refuse les utilisateurs anonymes ;**
- **On accepte les utilisateurs système et les utilisateurs virtuels ;**
- **Les utilisateurs virtuels sont mappés sur l'utilisateur système "ftp" ;**
- **Les utilisateurs n'ont aucun droit d'écriture par défaut ;**
- **Ils sont chrootés dans /var/ftp/ ;**
- **/etc/vsftpd/user_list contiendra la liste des utilisateurs refusés (pour lesquels on ne demandera même pas le mot de passe).**
- **…**

```
anonymous_enable=NO
local_enable=YES
write_enable=NO
local_umask=022
dirmessage_enable=YES
xferlog_enable=YES
connect_from_port_20=YES
listen_port=21
listen=YES
ftpd_banner="Bienvenue chef"
xferlog_std_format=YES
anon_upload_enable=NO
anon_mkdir_write_enable=NO
anon_other_write_enable=NO
chroot_local_user=YES
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd/chroot_list
listen_ipv6=YES
pam_service_name=vsftpd
userlist_enable=YES
pasv_min_port=3000
pasv_max_port=3500
max_clients=50
max_per_ip=4
```

Copyright - Tout droit réservé - OFPPT

# 03 - Installation et manipulation de serveur vsftpd

## tests

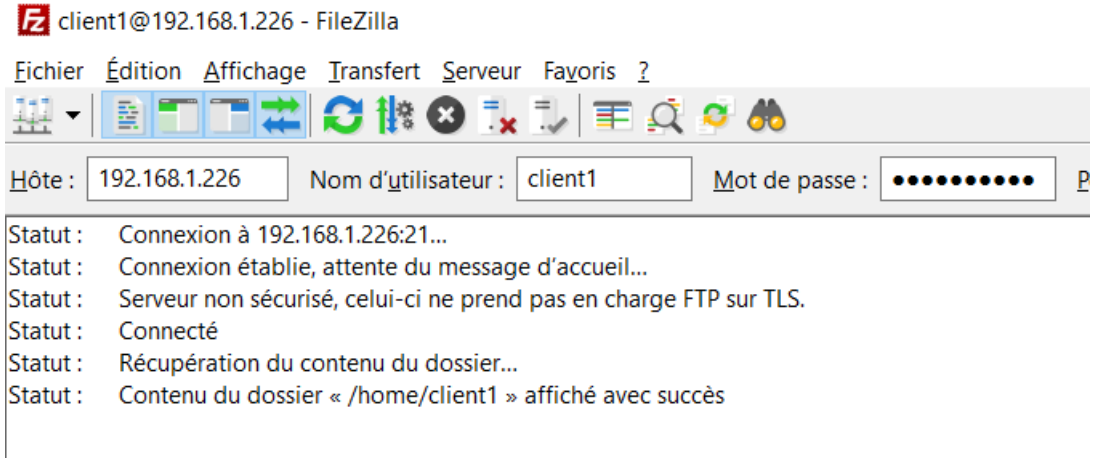



- Maintenant, on va autoriser les ports de communication ainsi que l'intervalle des ports qu'on aura besoin:

```
# firewall-cmd --add-port=21/tcp --add-port=3000-3500/tcp --permanent
# systemctl restart firewalld.service
```

- Pour accéder au serveur on utilise un outil comme **filezilla** ou via l'invite de commande:

```
C:\WINDOWS\system32>ftp 192.168.1.226
Connecté à 192.168.1.226.
220 (vsFTPd 3.0.3)
200 Always in UTF8 mode.
Utilisateur (192.168.1.226:(none)) : client1
331 Please specify the password.
Mot de passe :
230 Login successful.
ftp>
```




Copyright - Tout droit réservé - OFPPT

# 04 - Options de configurations

## Options pour le démon




Toute configuration de vsftpd est traitée par son fichier de configuration, /etc/vsftpd/vsftpd.conf. Chaque directive apparaît sur sa propre ligne au sein du fichier et suit le format suivant :

**<directive>=<value>**

La liste ci-dessous représente les directives les plus importantes dans /etc/vsftpd/vsftpd.conf :

**Les directives contrôlant le comportement général du démon vsftpd.**

- **listen** — Lorsque cette option est activée, vsftpd est exécuté en mode autonome.
- **listen_ipv6** — Lorsque cette option est activée, vsftpd est exécuté en mode autonome, mais n'écoute que l'interface de connexion (ou socket) IPv6. Cette directive ne peut pas être utilisée de concert avec la directive listen.
- **session_support** — Lorsque cette option est activée, vsftpd tente de maintenir les sessions de connexion pour chaque utilisateur par le biais de modules d'authentification enfichables (ou PAM). Si l'ouverture de sessions n'est pas nécessaire, la désactivation de cette option permet à vsftpd de tourner avec moins de processus et avec des privilèges moindres.

Copyright - Tout droit réservé - OFPPT

# 04 - Options de configurations

## Options de connexion et contrôles d'accès




**Les directives qui contrôlent le comportement de connexion et les mécanismes de contrôle d'accès.**

- **anonymous_enable** — Lorsque cette option est activée, des utilisateurs anonymes sont autorisés à se connecter. Les noms d'utilisateurs anonymes (dits anonymous) et ftp sont acceptés.
- **banner_file** — Spécifie le fichier contenant le texte affiché lorsqu'une connexion est établie avec le serveur . Cette option écrase tout texte spécifié dans la directive ftpd_banner.
- **ftpd_banner** — Lorsque cette option est activée, la chaîne spécifiée dans cette directive est affichée lorsque qu'une connexion au serveur est établie. Cette option peut être annulé par la directive banner_file.
- **local_enable** — Lorsque cette option est activée, les utilisateurs locaux sont autorisés à se connecter au système.
- **userlist_enable** — Lorsque cette option est activée, les utilisateurs mentionnés dans le fichier spécifiés par la directive userlist_file se voient refuser l'accès. Étant donné que l'accès est refusé avant même que le client ne puisse saisir son mot de passe, les utilisateurs n'ont pas la possibilité de soumettre des mots de passe non-cryptés sur le réseau.
- **userlist_file** — Spécifie le fichier référencé par vsftpd lorsque la directive userlist_enable est activée. La valeur par défaut est /etc/vsftpd.user_list ; cette dernière est créée durant l'installation.
- …

Copyright - Tout droit réservé - OFPPT

# 04 - Options de configurations

## Options pour les utilisateurs anonymes




**Les directives qui contrôlent l'accès des utilisateurs anonymes au serveur. Pour utiliser ces options, la valeur de la directive anonymous_enable doit être YES.**

- **anon_mkdir_write_enable** — Lorsque cette option est activée de concert avec la directive write_enable, des utilisateurs anonymes sont autorisés à créer de nouveaux répertoires au sein du répertoire parent qui a des permissions en écriture.
- **anon_root** — Spécifie le répertoire que vsftpd utilise après la connexion d'un utilisateur anonyme.
- **anon_upload_enable** — Lorsque cette option est activée de concert avec la directive write_enable, des utilisateurs anonymes sont autorisés à télécharger vers le serveur des fichiers dans un répertoire parent doté de permissions en écriture.
- **anon_world_readable_only** — Lorsque cette option est activée, des utilisateurs anonymes sont autorisés à télécharger des fichiers lisibles par tout un chacun.
- **ftp_username** — Spécifie le compte de l'utilisateur local (énoncé dans /etc/passwd) employé pour l'utilisateur FTP anonyme. Le répertoire personnel spécifié dans /etc/passwd pour l'utilisateur est le répertoire root de l'utilisateur FTP anonyme.
- **no_anon_password** — Lorsque cette option est activée, l'utilisateur anonyme ne doit pas saisir de mot de passe.

Copyright - Tout droit réservé - OFPPT

# 04 - Options de configurations

## Options pour les utilisateurs locaux




**Les directives caractérisant la manière selon laquelle les utilisateurs locaux ont accès au serveur. Pour utiliser ces options, la directive local_enable doit avoir la valeur YES.**

- **chroot_list_enable** — Lorsque cette option est activée, les utilisateurs locaux énumérés dans le fichier qui est spécifié dans la directive chroot_list_file, sont placés dans une prison chroot dès qu'ils se connectent. Si cette option est activée de concert avec la directive chroot_local_user, les utilisateurs locaux énumérés dans le fichier qui est spécifié dans la directive chroot_list_file ne sont pas placés dans une prison chroot lors de la connexion.
- **chroot_list_file** — Spécifie le fichier contenant une liste des utilisateurs locaux référencés lorsque la valeur de la directive chroot_list_enable est YES. La valeur par défaut est /etc/vsftpd.chroot_list.
- **chroot_local_user** — Lorsque cette option est activée, les utilisateurs locaux opèrent dans l'environnement chrooté de leur répertoire personnel après leur connexion.
- **local_root** — Spécifie le répertoire que vsftpd utilise après la connexion d'un utilisateur local.
- **local_umask** — Spécifie la valeur donnée à umask pour la création de fichiers. Notez que la valeur par défaut se présente sous la forme octale (un système numérique en base huit), qui inclut un préfixe "0". Sinon la valeur est traitée comme un entier à base 10.

Copyright - Tout droit réservé - OFPPT

# 04 - Options de configurations

## Options pour les répertoires




**Les directives ayant un impact sur les répertoires.**

- **dirlist_enable** — Lorsque cette option est activée, les utilisateurs sont autorisés à visionner les listes de répertoires.
- **dirmessage_enable** — Lorsque cette option est activée, un message apparaît chaque fois qu'un utilisateur ouvre un répertoire avec un fichier message. Ce message se trouve dans le répertoire qui est ouvert. Le nom de ce fichier est spécifié dans la directive message_file et part défaut prend la valeur .message.
- **force_dot_files** — Lorsque cette option est activée, les fichiers commençant par un point (.) sont inclus dans les listes de répertoires, à l'exception des fichiers . et ...
- **hide_ids** — Lorsque cette option est activée, toutes les listes de répertoires font apparaître ftp comme l'utilisateur et le groupe de chaque fichier.
- **message_file** — Spécifie le nom du fichier message lorsque la directive dirmessage_enable est utilisée. La valeur par défaut est .message.
- **text_userdb_names** — Lorsque cette option est activée, des noms d'utilisateurs et noms de groupes test sont utilisés au lieu des entrées UID et GID. L'activation de cette option peut entraîner un ralentissement des performances du serveur.
- **use_localtime** — Lorsque cette option est activée, les listes de répertoires révèlent l'heure locale de l'ordinateur au lieu de l'heure GMT.

Copyright - Tout droit réservé - OFPPT

# 04 - Options de configurations

## Options pour le transfert de fichiers




**Les directives ayant un impact sur les fichiers.**

- **download_enable** — Lorsque cette option est activée, le téléchargement de fichiers est autorisé.
- **chown_uploads** — Lorsque cette option est activée, tous les fichiers téléléchargés vers les serveur par des utilisateurs anonymes deviennent la propriété de l'utilisateur spécifié dans la directive chown_username.
- **chown_username** — Spécifie la propriété de fichiers téléchargés anonymement vers le serveur si la directive chown_uploads est activée. La valeur par défaut est root.
- **write_enable** — Lorsque cette option est activée, les commandes FTP permettant de modifier le système de fichiers sont permises, telles que DELE, RNFR et STOR.

Copyright - Tout droit réservé - OFPPT

# 04 - Options de configurations

## Options de journalisation




**Les directives ayant un impact sur le comportement de journalisation de vsftpd.**

- **dual_log_enable** — Lorsque cette option est activée de concert avec xferlog_enable, vsftpd enregistre deux fichiers simultanément : un journal compatible avec wu-ftpd dans le fichier spécifiée dans la directive xferlog_file (par défaut /var/log/xferlog) et un fichier journal vsftpd standard spécifié dans la directive vsftpd_log_file (par défaut /var/log/vsftpd.log). La valeur par défaut est NO.
- **log_ftp_protocol** — Lorsque cette option est activée de concert avec xferlog_enable et lorsque xferlog_std_format a pour valeur NO, toutes les commandes et réponses FTP sont journalisées. Cette directive est très utilisée lors d'opérations de débogage.
- **syslog_enable** — Lorsque cette option est activée de concert avec xferlog_enable, toute journalisation normalement enregistrée dans le fichier journal standard vsftpd spécifié dans la directive vsftpd_log_file (par défaut /var/log/vsftpd.log) est envoyée à l'enregistreur du système sous le service FTPD.
- **vsftpd_log_file** — Spécifie le fichier journal vsftpd. Pour que ce fichier soit utilisé, xferlog_enable doit être activée et xferlog_std_format doit avoir pour valeur NO ou, si la valeur de xferlog_std_format est YES, l'activation dedual_log_enable est nécessaire. Il est important de noter ici que si syslog_enable a pour valeur YES, le journal du système est utilisé à la place du fichier spécifié dans cette directive. La valeur par défaut est /var/log/vsftpd.log.

Copyright - Tout droit réservé - OFPPT

# 04 - Options de configurations

## Options de journalisation




- **xferlog_enable** — Lorsque cette commande est activée, vsftpd journalise les connexions (seulement au format vsftpd) et les informations de transfert de fichiers dans le fichier journal spécifié dans la directive vsftpd_log_file (par défaut /var/log/vsftpd.log). Si xferlog_std_format a pour valeur YES, les informations de transfert de fichiers sont journalisées mais les connexions elles ne le sont pas et le fichier spécifié dans xferlog_file (par défaut /var/log/xferlog) est utilisé à la place. Il est important de noter ici que les fichiers journaux aussi bien que les formats de journaux sont utilisés si la valeur de dual_log_enable est YES.
- **xferlog_file** — Spécifie le fichier journal compatible avec wu-ftpd. Pour que ce fichier soit utilisé, xferlog_enable doit être activé et la valeur de xferlog_std_format doit être YES. Elle est également utilisée si la valeur de dual_log_enable est YES. La valeur par défaut est /var/log/xferlog.
- **xferlog_std_format** — Lorsque cette option est activée de concert avec xferlog_enable, seul un journal de transfert de fichiers compatible avec wu-ftpd est enregistré dans le fichier spécifié dans la directive xferlog_file (par défaut /var/log/xferlog). Il est important de noter ici que ce fichier journalise seulement les transferts de fichiers et n'enregistre pas les connexions au serveur.

Copyright - Tout droit réservé - OFPPT

# 04 - Options de configurations

## Options réseau




**Les directives ayant un impact sur la manière dont vsftpd interagit avec le réseau.**

- **accept_timeout** — Spécifie la durée donnée à un client utilisant une connexion passive pour se connecter. La valeur par défaut est 60.
- **connect_from_port_20** Lorsque cette option est activée, vsftpd tourne avec suffisamment de privilèges pour ouvrir le port 20 sur le serveur lors des transferts de données en mode actif. La désactivation de cette option permet à vsftpd de tourner avec moins de privilèges, mais cette option peut-être incompatible avec certains clients FTP.
- **connect_timeout** — Spécifie la durée maximale exprimée en secondes, donnée à un client utilisant un mode actif pour répondre à une connexion de données. La valeur par défaut est 60.
- **data_connection_timeout** — Spécifie la durée maximale exprimée en secondes, pendant laquelle les transferts de données peuvent s'arrêter. Une fois cette durée écoulée, la connexion au client distant est fermée. La valeur par défaut est 300.
- **ftp_data_port** — Spécifie le port utilisé pour les connexions actives aux données lorsque connect_from_port_20 a pour valeur YES. La valeur par défaut est 20.
- **listen_address** — Spécifie l'adresse IP sur laquelle vsftpd doit être à l'écoute de connexions réseau.
- **listen_port** — Spécifie le port sur lequel vsftpd doit être à l'écoute de connexions réseau. La valeur par défaut est 21.
- **max_clients** — Spécifie le nombre maximal de clients autorisés à se connecter simultanément au serveur lorsqu'il tourne en mode autonome. Toute connexion client supplémentaire provoquerait un message d'erreur. La valeur par défaut est 0, ce qui ne limite pas les connexions.

Copyright - Tout droit réservé - OFPPT

# 04 - Options de configurations

## Options réseau




- **max_per_ip** — Spécifie le nombre maximal de clients autorisés à se connecter depuis l'adresse IP source.
- **pasv_address** — Spécifie l'adresse IP utilisée pour l'adresse IP publique du serveur aux serveurs se trouvant derrière des pare-feu NAT (Network Address Translation). Cette option permet à vsftpd de fournir la bonne adresse de retour pour des connexions en mode passif.
- **pasv_enable** — Lorsque cette option est activée, les connexions en mode passif ne sont pas permises. La valeur par défaut est YES.
- **pasv_max_port** — Spécifie le port le plus élevé possible qui est envoyé aux clients FTP pour des connexions en mode passif. Ce paramètre est utilisé pour limiter la plage de ports afin que les règles de pare-feu soient faciles à créer. La valeur par défaut est 0, ce qui ne limite pas la plage des ports passifs les plus élevés. La valeur ne doit pas dépasser 65535.
- **pasv_min_port** — Spécifie le port le plus bas possible qui est envoyé au client FTP pour des connexions en mode passif. Ce paramètre est utilisé pour limiter la plage de ports afin que les règles de pare-feu soient faciles à créer. La valeur par défaut est 0, ce qui ne limite pas la plage des ports passifs les plus bas. La valeur ne doit pas être inférieure à 1024.
- **pasv_promiscuous** — Lorsque cette option est activée, les connexions aux données ne sont pas analysées pour vérifier qu'elles proviennent bien de la même adresse IP. Ce paramètre est seulement utile pour certains types de tunnellisation.
- **port_enable** — Lorsque cette option est activée, les connexions en mode actif ne sont pas permises.

Copyright - Tout droit réservé - OFPPT

# 05 - Démarrage de multiples instances de vsftpd

## Configuration




- Parfois, un ordinateur est utilisé pour fournir de multiples domaines FTP. Cette technique est appelée **multihoming** (aussi appelée **hébergement multi-domaines**). Une possibilité d'effectuer du multihoming à l'aide de vsftpd consiste à exécuter de multiples copies du démon, chacune disposant de son propre fichier de configuration.
- Pour ce faire, assignez d'abord les adresses IP appropriées aux périphériques réseau des périphériques réseau du système. Ensuite, assurez-vous que le serveur DNS pour les domaines FTP est bien configuré pour référencer le bon ordinateur.
- Pour que vsftpd réponde à des requêtes sur des adresses IP, il est nécessaire que de multiples copies du démon tournent. La première copie doit être exécutée à l'aide des initscripts de vsftpd. Cette copie utilise le fichier de configuration standard, /etc/vsftpd/vsftpd.conf.
- Chaque site FTP supplémentaire doit avoir un fichier de configuration portant un nom unique dans le répertoire /etc/vsftpd/, comme /etc/vsftpd/**vsftpd-site-2.conf**. Chaque fichier de configuration ne doit être lisible et modifiable que par le super-utilisateur. Au sein de chaque fichier de configuration relatif à chaque serveur FTP écoutant sur un réseau IPv4, la directive suivante doit être unique :
    - **listen_address=@IPV4**

Copyright - Tout droit réservé - OFPPT

# 05 - Démarrage de multiples instances de vsftpd

## Configuration




- Une fois que chaque serveur supplémentaire est doté d'un fichier de configuration, le démon vsftpd doit être exécuté depuis une invite du shell root à l'aide de la commande suivante :

  **#vsftpd /etc/vsftpd/ vsftpd-site-2.conf &**

- Parmi d'autres directives pouvant faire l'objet de modifications sur une base individuelle pour chaque serveur figurent :
  - **anon_root**
  - **local_root**
  - **vsftpd_log_file**
  - **xferlog_file**

Copyright - Tout droit réservé - OFPPT

# 06 - Sécurité FTP

## explication




Le protocole de transfert de fichiers a été créé à l'origine sans aucune précaution de sécurité. Au moment du développement, Internet était encore à ses débuts et la cybercriminalité n'existait pas. Maintenant, l'utilisation du FTP est associée à de nombreux risques de sécurité, car toutes les informations transférées sont non chiffrées. C'est pourquoi deux variantes plus sûres ont été développées, qui sont depuis lors en concurrence l'une avec l'autre **: FTPS** et **SFTP.**

- Le protocole FTPS est **le FTP avec SSL**. La connexion est donc établie en combinaison avec Secure Sockets Layer (SSL) ou Transport Layer Security (**TLS**). L'échange de données est chiffré.
- Le protocole de transfert de fichiers **SSH** (**SFTP**) utilise quant à lui Secure Shell (SSH) pour le transfert sécurisé de fichiers. La connexion est également chiffrée. Mais alors que le FTPS nécessite deux connexions, le SFTP ne s'en sort qu'avec une.

Copyright - Tout droit réservé - OFPPT