|  |  |
| --- | --- |
| Ftp Server APK 1.32 Download for Android – Download Ftp Server APK Latest  Version - APKFab.com | **Service FTP vsFTPd** |

# Service FTP

## Introduction

Le protocole de transfert de fichier (FTP) existe depuis longtemps.   
C'est un **protocole réseau simple pour le partage de fichiers entre systèmes**. Il est principalement utilisé pour partager des **documents publics sur un réseau**.

Lors d’une connexion à un service FTP, son **processus d'authentification peut obliger à lui attribuer un nom d'utilisateur** et un **mot de passe valides**.   
Une fois authentifié, en fonction de la configuration du service FTP, on pourra essentiellement **rechercher et télécharger (ou téléverser) des fichiers**.

**Attention** …  
En utilisant des **informations de compte et des mots de passe** pour se connecter à un service FTP, il est important de savoir qu’**elles ne sont généralement pas chiffrées**.   
Cela signifie que toute personne utilisant une application de détection de réseau, telle que Wireshark, verra le **nom d'utilisateur et le mot de passe vers serveur FTP en clair**.   
Il est préférable d’utiliser **Secure FTP (SFTP), qui chiffre FTP à l’aide d’openSSH**.

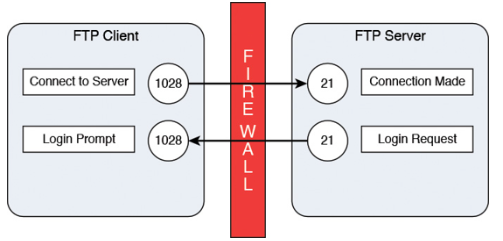
Il est plus courant de configurer un service FTP pour un accès anonyme et d’**autoriser** **uniquement les téléchargements** **de fichiers**.   
Avec un **accès FTP anonyme**, au lieu d’un nom d’utilisateur attribué individuellement, un nom d’utilisateur général, tel que **anonymous** ou **ftp**, est utilisé. Il se peut qu'**aucun** **mot** **de** **passe** ne soit requis ou qu'une demande d'adresse de courriel ne soit demandée (bien que l'adresse de courriel ne soit pas vérifiée).

### Connexions passives et actives

FTP utilise généralement **deux ports TCP** …  
le **port de données** et le **port de commande**.

* Le **port de commande** est utilisé pour envoyer des commandes et gérer les réponses aux commandes ;
* Le **port de données** est utilisé pour le transport des données de fichier.

Il est important de savoir que FTP utilise **deux modes de fonctionnement … passif et actif**.   
Le mode utilisé détermine comment une connexion est établie.   
Le **mode passif cause moins de problèmes** (comme décrit sous peu), il est donc le plus populaire des deux.



Une fois cette **connexion initiale établie**, des **actions supplémentaires sont effectuées**.

L'utilisateur est invité à **entrer un nom d'utilisateur** et un **mot de passe pour se connecter** au serveur FTP.

Une fois que l'utilisateur est connecté avec succès, **tout transfert de données** (téléchargement de fichiers, par exemple) a lieu sur des **ports différents**. …

* Sur le serveur, le **port TCP 20 est utilisé**.
* Sur le client, le **numéro de port est supérieur au port de connexion**.

Ainsi, pour l'exemple de la figure précédente, il s'agit du port 1028.

# vsFTPd

Le protocole FTP est **un des plus anciens protocoles de la couche application** encore en utilisation aujourd'hui.

La première spécification du protocole tel qu'on l'utilise aujourd'hui **date de 1980 (RFC959, mis à jour en 1985)**, mais les **bases de son mécanisme remontent à 1971 (RFC114)**.

Il existe plusieurs implémentations de FTP, mais **une des plus répandues sur linux est vsftpd** (v*ery secure FTP daemon*), du fait qu'elle offre beaucoup d’options pour contrôler les accès.

Pour bien comprendre ces options, il est important de connaître deux aspects des systèmes de fichiers avec linux   
la **notion de chroot** et les **masques de permissions**(*umask*).

## chroot

Avec Linux, on peut **modifier la racine du système de fichiers pour un utilisateur**, ce qui revient à l'**enfermer dans un répertoire en l'empêchant de remonter dans la hiérarchie de fichiers**.   
On dit dans ce cas qu'on ***chroot* un utilisateur** ; ceci provient de la **commande *chroot*** (*change root*), qui a pour effet de donner à un utilisateur ou à un processus une racine différente de celle du système de fichiers.

Par exemple …

**/**

**|-- bin**

**|-- boot**

**|-- dev**

**|-- etc**

**| |-- apache2**

**| |-- apt**

**| |-- (...)**

**|-- home**

**| |-- alice**

**| |-- bob**

**|-- lib**

**|-- (...)**

La **racine normale du système de fichiers est /**.   
Dans le cas normal, les utilisateurs peuvent circuler dans tout le système de fichiers, et ne peuvent évidemment pas remonter plus haut que la racine.   
Toutefois, si on ***chroot* les utilisateurs alice et bob dans le répertoire /home**, ce sera leur racine, et ils **ne pourront pas aller ailleurs que dans /home et ses sous-répertoires**.

## Installation de vsftpd

Depuis un terminal, on lance la commande … **>>** sudoapt install vsftpd

Pour vérifier si le service est démarré …  
**>>** sudo systemctl status vsftpd.service  
**● vsftpd.service - vsftpd FTP server  
 Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor preset: enabled)  
 Active: active (running) since Mon 2022-03-14 09:32:28 EDT; 13s ago  
 Process: 2801 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCES>  
 Main PID: 2803 (vsftpd)  
 Tasks: 1 (limit: 4663)  
 Memory: 696.0K  
 CPU: 4ms  
 CGroup: /system.slice/vsftpd.service  
 └─2803 /usr/sbin/vsftpd /etc/vsftpd.conf**

Pour tester l'installation, on peut essayer de se connecter à partir d'un autre poste de travail sur le même réseau en mode anonyme (identifiant … **<Nom d’usager>**, mot de passe … **<Mot de passe>**) … **>>** ftp 192.168.1.100  
**Connected to 192.168.1.119.  
220 (vsFTPd 2.3.5)  
530 Please login with USER and PASS.  
530 Please login with USER and PASS.  
SSL not available  
Name (192.168.1.119:root):** anonymous  
**331 Please specify the password.  
Password:** …  
**230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp>**

**Remarque** …  
On remplace l’adresse IP (192.168.1.100) par la sienne.

## Utilisateurs

Avec vsftpd, les **utilisateurs FTP sont les utilisateurs du système**, c'est-à-dire que pour créer une compte FTP il faut en fait créer un compte système.   
Il existe aussi un **compte FTP public** (ou *anonyme*) qui **ne dispose par défaut que des droits de lecture**.  
Le répertoire racine (/) de ce compte *anonymous* est ***/srv/ftp***.

Toutefois l'installation de base de vsftpd, si on n’apporte aucune modification à la configuration, **n'autorise pas ces connexions anonymes**.

Pour permettre les connexions anonymes, en tant qu’utilisateur root, on **modifie la directive anonymous\_enable=NO** **pour** **YES** …  
**>>** sudo nano /etc/vsftpd.conf

Pour que la modification s’applique, il faut **recharger le fichier de configuration du service** …  
**>>** sudo systemctl reload vsftpd.service

**Remarque** …  
Il est aussi **possible de redémarrer le service** (sudo systemctl restart vsftpd.service) mais cela va couper les connexions existantes.

## Configuration de vsftpd

La configuration du service FTP est définie par une série de **directives spécifiées dans le fichier /etc/vsftpd.conf**.

La référence des **directives et leur valeurs possibles** sont **disponibles sur le web** ou encore à partir du terminal avec la **commande** man vsftpd.conf.

Pour épurer le **fichier de configuration vsftpd.conf** …  
**>>** sudo mv –verbose /etc/vsftpd.conf /etc/vsftpd.conf.original   
Renommé 'vsftpd.conf' -> 'vsftpd.conf.original'  
**>>** sudo cat /etc/vsftpd.conf.original | egrep -v -e '^[[:blank:]]\*#|^$' | sudo tee /etc/vsftpd.conf

**Remarque** …  
On peut constater le résultat avec la commande cat /etc/vsftpd.conf.

### Autoriser les utilisateurs authentifiés en lecture/écriture

Par défaut, *vsftpd* est configuré pour n'autoriser que les **connexions anonymes et en lecture seule**; nous voulons que les utilisateurs du système puissent se connecter et déposer des fichiers sur le serveur. Dans le fichier de configuration, assurez-vous d'avoir les valeurs suivantes …

**# Empêcher les connexions anonymes  
anonymous\_enable=NO**

**# Activer les utilisateurs du système Linux (utilisateurs du fichier /etc/passwd)  
local\_enable=YES**

**# Activer la possibilité d'écriture de fichiers sur le ftp (et non seulement en lecture)  
write\_enable=YES**

Par défaut, la **valeur de umask dans vsftpd est 077**, ce qui est **très restrictif** - les utilisateurs qui déposent un fichier sur le serveur seront les seuls à pouvoir le lire… on ajoute donc aussi la ligne suivante …  
**# Modification du umask  
local\_umask=022**

Ensuite, on recharge le fichier de configuration du démon vsftpd afin de prendre en compte les modifications …  
**>>** sudo systemctl restart vsftpd.service

### Modifier le répertoire initial pour /srv/ftp

Après la connexion, les **utilisateurs anonymes se retrouvent dans le** **répertoire /srv/ftp**, et les **utilisateurs système se** **retrouvent dans leur répertoire personnel**.

On peut **modifier le répertoire initial des utilisateurs système** avec la directive **local\_root**.

Pour que tous les utilisateurs aient accès à **/srv/ftp**, ajoutez la ligne suivante dans le fichier de configuration …  
**# Modification du répertoire initial des utilisateurs système  
local\_root=/srv/ftp**

On recharge le fichier de configuration du démon vsftpd …  
**>>** sudo systemctl reload vsftpd.vsftpd

Pour vsFTPd, les **utilisateurs système peuvent librement circuler dans le système de fichiers** comme lors d'une session linux ordinaire (on essaie de faire **cd *..*** immédiatement après la connexion …).   
Pour des **raisons de sécurité**, il serait préférable de les **empêcher de sortir de leur répertoire initial** - on veut **éviter de** **rendre accessible les informations de configuration du serveur** (entre autres).

Dans vsftpd, la **directive chroot\_local\_user** permet de **limiter un utilisateur à son répertoire i**nitial.

On ajoute la ligne suivante au fichier de configuration …  
**chroot\_local\_user=YES**

vsFTPd requiert que les utilisateurs ne puissent pas écrire directement dans leur répertoire racine.   
Si on veut que les utilisateurs système puissent écrire des fichiers, c'est l'administrateur du serveur qui devra créer des sous‑répertoires dans le répertoire de *chroot*.

Toutefois, il est possible de modifier cet état en modifiant la **directive allow\_writeable\_chroot** et la positionner à **–** …  
**allow\_writeable\_chroot=YES**

## Gestion des utilisateurs

Il est possible de permettre ou de refuser aux utilisateurs de se connecter au serveur vsFTPd.

Pour ce faire on doit ajouter les directives suivantes dans le fichier /etc/vsftpd.conf …  
**userlist\_deny=NO  
userlist\_enable=YES  
userlist\_file=/etc/vsftpd.allowed\_users**

Par la suite on édite et on ajoute les utilisateurs qui peux se connecter dans ce fichier.

On recharge le fichier de configuration du démon vsftpd …  
**>>** sudo systemctl reload vsftpd.service

**Remarque** …  
S’il n’est pas autorisé, l’utilisateur recevra une erreur indiquant qu'il ne peut pas se connecter avant de saisir son mot de passe.

## Paramètres de configuration utiles

Il peut être intéressant de modifier les directives suivantes …

* **userlist\_enable (YES ou NO)**Si **userlist\_enable=YES** et **userlist\_deny=YES**, le fichier userlist\_file spécifie les usagers bloqués  
  Si **userlist\_enable=YES** et **userlist\_deny=NO**, le fichier userlist\_file spécifie les usagers autorisés ;
* **chroot\_local\_users (YES ou NO)**Si **chroot\_local\_users=NO** et **chroot\_list\_enable=NO**, les utilisateurs locaux sont libres  
  Si **chroot\_local\_users=NO** et **chroot\_list\_enable=YES**, chroot\_list\_file définit les utilisateurs *chrootés*  
  Si **chroot\_local\_users=YES** et **chroot\_list\_enable=NO** les utilisateurs locaux sont *chrootés*  
  Si **chroot\_local\_users=YES** et **chroot\_list\_enable=YES**, chroot\_list\_file définit les utilisateurs libre ;
* **anon\_root**Permet de définir le répertoire où se retrouvera l’utilisateur anonyme après sa connexion ;
* **local\_root**Permet de définir le répertoire où se retrouvera l’utilisateur local après sa connexion ;  
  Si **chroot\_local\_user=YES**, il ne pourra pas en sortir ;
* **anon\_upload\_enable (YES ou NO)**Autorise l’utilisateur anonyme à déposer des fichiers sur le serveur ;
* **no\_anon\_passwd (YES ou NO)**Permet de spécifier si la connexion anonyme nécessite un mot de passe ou non ;
* **dual\_log\_enable (YES ou NO)**Permet d’enregistrer les deux types de journaux, un dans le ficher vsftpd\_log\_file et l’autre dans xferlog\_file ;
* **xferlog\_enable(YES ou NO)**Active la journalisation, pour un seul type de journal ;
* **xferlog\_std\_format (YES ou NO)  
  YES** : le journal normal est écrit dans le fichier spécifié par vsftpd\_log\_file  
  **NO** : le journal suivant le standard xferlog est écrit dans le fichier spécifié par xferlog\_file.

## Rappel – Commandes client

|  |  |
| --- | --- |
| Commande | Résultat |
| ! | Permet d’ouvrir un *shell* *bash* temporaire durant une session ftp.  «exit » revient à la ligne de commande ftp. |
| ls, ls -l, cd, pwd, mkdir, chmod | Commandes similaires à leur équivalent *bash*. |
| binary | Spécifie un mode de transfert binaire. |
| ascii | Spécifie un mode de transfert texte. |
| put, mput | Dépose un ou plusieurs fichiers sur le serveur. |
| get, mget | Télécharge un ou plusieurs fichiers du serveur. |
| delete, mdelete | Supprime un ou plusieurs fichiers du serveur. |
| help + *commande* | Affiche une brève description de la commande. *Help* seul affiche la liste des commandes possible. |

## umask

Tous les fichiers et répertoires créés dans un système de fichiers Unix/Linux se font attribuer un ensemble de permissions.

Ces permissions affectent trois ensembles d'utilisateurs …

* L’utilisateur propriétaire ;
* Le groupe propriétaire ;
* Les autres utilisateurs et groupes.

Les droits de chacun sur les fichiers consistent à pouvoir le lire, le modifier ou l’exécuter.   
Par exemple, pour la commande ls -l, on obtient la sortie suivante …  
**drwxr-xr-x 2 olivier olivier 4096 Sep 24 02:03 doc  
-rw-r--r-- 1 olivier olivier 161 Sep 24 02:05 proc1  
drwxr-xr-x 2 olivier olivier 4096 Sep 24 02:03 scripts**

Dans la colonne des droits d’accès, le **d** initial signifie que l’élément est un répertoire; les autres éléments correspondent aux droits de lecture (**r**), écriture (**w**) ou exécution (**x**) pour (respectivement) le propriétaire, le groupe et les autres.

Donc le fichier ***proc1*** peut être lu et modifié par son propriétaire, mais uniquement lu par le groupe et le reste du monde.

Les permissions d’un type d’utilisateur sont représentées par une séquence de trois *bits*, dont la valeur décimale peut donc être de 0 à 7 (3 bits : 23 = 8 valeurs possibles).

Le droit de lecture correspond au premier bit, d'écriture au second, et d’exécution au troisième :

|  |  |  |
| --- | --- | --- |
| **0** | **0** | **0** |

lecture

exécution

écriture

Si on convertit ces valeurs binaires en décimal, on a …  
 **4** lecture  
 **2** écriture   
 **1** exécution

Pour définir un droit d’accès d'un type d'utilisateur à l'aide d'un seul nombre décimal, on fait la somme de ces valeurs : par exemple « r-x » (lecture et exécution) correspond aux trois bits 1,0,1, donc à **4+1=5** (notez que «101» en binaire est le nombre 5…).   
Le nombre 5 signifie donc que le type d'utilisateur donné a les droits de lecture et d'exécution sur le fichier.

Afin de définir les droits d’accès pour tous (le propriétaire, le groupe et les autres), on fait donc trois sommes, par exemple :

**rwxr-xr-x**

**7 5 5**

Lorsqu'un utilisateur crée des répertoires ou des fichiers, les permissions attribuées par défaut sont les suivantes …

* répertoires : 777
* fichiers : 666

On peut modifier ces permissions par défaut en modifiant le masque de permissions associé à chaque utilisateur. Le masque est une suite de trois nombres qu'on doit soustraire à 777 dans le cas des répertoires et à 666 dans le cas des fichiers.

Par exemple …

|  |  |  |
| --- | --- | --- |
|  | répertoire | fichier |
|  | 777 | 666 |
| masque | 022 | 022 |
| résultat | 755 | 644 |
| rwxr-xr-x | rw-r--r-- |

|  |  |  |
| --- | --- | --- |
|  | répertoire | fichier |
|  | 777 | 666 |
| masque | 077 | 077 |
| résultat | 700 | 600 |
| rwx------ | rw------ |

On peut spécifier le masque d'un utilisateur dans le fichier **.profile** de son répertoire personnel avec la directive suivante …  
**umask 022**

# Exercice – Configuration du service FTP

On veut éviter que des connexions restent inutilement ouvertes.   
Comment configurer *vsftpd* pour que la connexion soit automatiquement fermée après 30 secondes si l'utilisateur ne fait rien ?

|  |
| --- |
|  |
|  |
|  |

Créez sur le serveur les 3 utilisateurs Alice, Bob et Charles.

|  |
| --- |
|  |
|  |
|  |
|  |

Comment configurer *vsftpd* afin d’interdire l'accès FTP à Alice uniquement ?

|  |
| --- |
|  |
|  |
|  |

Comment configurer *vsftpd* afin de permettre l'accès ftp à Alice uniquement ?

|  |
| --- |
|  |
|  |
|  |

Configurez le service pour que les utilisateurs nommés dans /etc/vsftpd/acces\_restreint et l’utilisateur anonyme soient « chrootés » dans le répertoire /home/public.

|  |
| --- |
|  |
|  |
|  |

Activez la journalisation des transferts au format standard dans le fichier /var/log/ftp.log.

|  |
| --- |
|  |
|  |
|  |

# Exercice – Utilisation de FTP

### Ouverture d’une session FTP

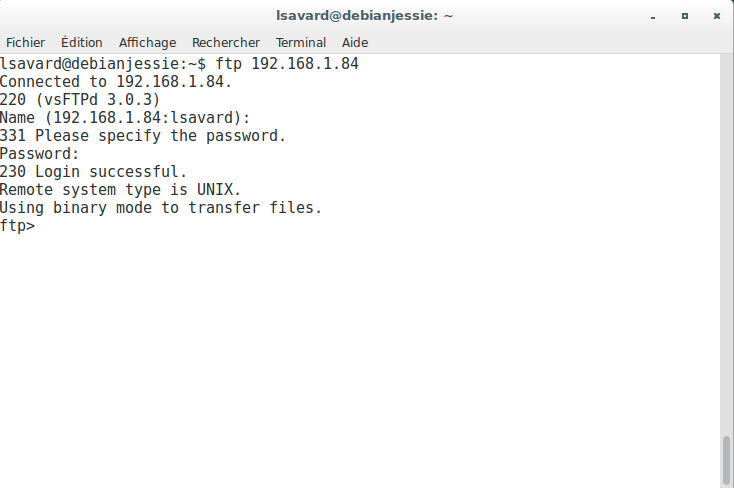
À partir d’une console …

Ouvrir une session FTP

|  |
| --- |
|  |

Établir une connexion avec votre serveur FTP (l’adresse est celle de votre serveur)

|  |
| --- |
|  |



### Création des fichiers et répertoires de travail

Créer cinq fichiers dont les noms sont …

* travail.doc
* semaine.txt
* mercredi.txt
* document.rtf
* demain.doc

Le contenu de ces fichiers n’a pas d’importance.

|  |
| --- |
|  |
|  |
|  |
|  |
|  |

Créer un répertoire tempo à la racine de votre espace FTP.

|  |
| --- |
|  |

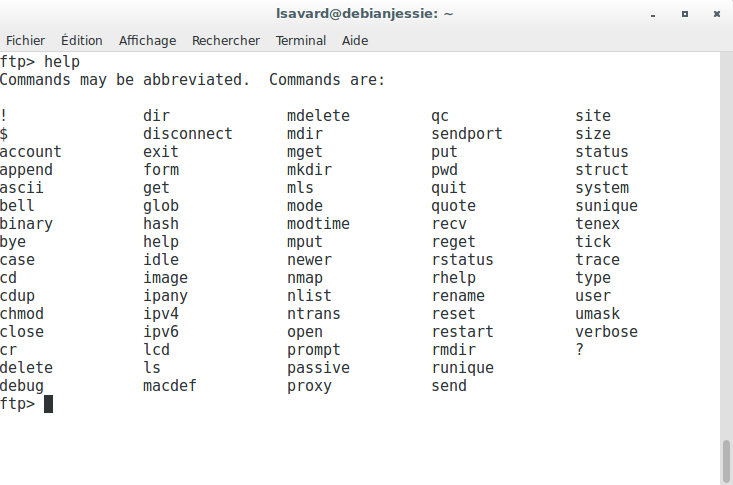
Créer un répertoire document dans le répertoire tempo.

|  |
| --- |
|  |

Créer un dossier sur votre disque dur nommé transfert.

|  |
| --- |
|  |

### Manipulation de base



Téléverser dans la racine de votre espace FTP le fichier travail.doc ;

|  |
| --- |
|  |

Téléverser dans le répertoire tempo (en une seule commande) les fichiers dont le suffixe est .txt ;

|  |
| --- |
|  |

Déplacer le curseur dans le répertoire document ;

|  |
| --- |
|  |

Téléverser dans le répertoire document (en une seule commande) les fichiers qui débutent par la lettre d ;

|  |
| --- |
|  |

Afficher la liste des fichiers du répertoire tempo ;

|  |
| --- |
|  |

Afficher la liste des fichiers du répertoire document ;

|  |
| --- |
|  |

Télécharger le document document.rtf (du répertoire documents) dans votre nouveau répertoire transferts ;

|  |
| --- |
|  |

Supprimer le fichier semaine.txt du répertoire tempo ;

|  |
| --- |
|  |

Supprimer le fichier document.rtf du répertoire document ;

|  |
| --- |
|  |

Fermer la connexion ;

|  |
| --- |
|  |

Fermez la session FTP.

|  |
| --- |
|  |