# 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 tout individu 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.

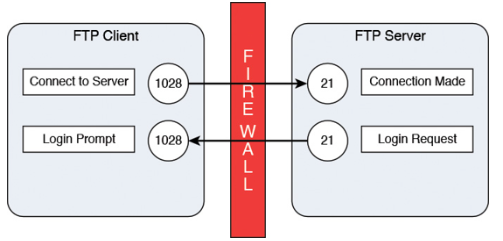
Il est plus courant de configurer un service FTP pour un accès anonyme et d’autoriser uniquement les téléchargements de fichiers. Avec un accès FTP anonyme, au lieu d’un nom d’utilisateur attribué individuellement, un nom d’utilisateur général, tel que **anonymous** ou **ftp**, est utilisé. Il se peut 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 20 est utilisé. Sur le client, le numéro de port est supérieur au port de connexion. Ainsi, pour l'exemple de la figure suivante, il s'agit du port 1029.

## Installation vsFTPd

Le service le plus utilisé sous Linux est vsFTPd.

Comme la plupart des applications sous Debian, son installation est simple …

**>> sudo apt update  
>> sudo apt upgrade -y  
>> sudo apt install vsftpd**

Afin de vérifier le statut de vsFTPd …  
**>> sudo systemctl status vsftpd.service**

## Directives du service FTP

Le fichier de configuration de vsFTPd permet de modifier le comportement du service FTP.

**Remarque** …  
Avant de modifier le fichier de configuration de vsFTPd, il est prudent d’en faire préalablement une copie …  
**>> sudo cp --verbose /etc/vsftpd.conf /etc/vsftpd.conf.original**.  
Il sera toujours possible de revenir en arrière en cas d’erreur.

Le tableau suivant présente les principales directives de configuration du fichier /etc/vsftpd.

|  |  |
| --- | --- |
| Directive | Description |
| **anon\_max\_rate** | Définit le débit, en octets par seconde, pouvant être transféré par des utilisateurs anonymes |
| **anon\_mkdir\_write\_enable** | Détermine si l'utilisateur anonyme peut créer des répertoires Si défini sur YES, pour que cela fonctionne correctement, la **directive write\_enable** doit également être définie sur YES et l'autorisation d'accès en écriture sur le répertoire parent doit être activée pour le compte d'utilisateur anonyme Ce booléen est défini sur **NO par défaut** |
| **anon\_other\_write\_enable** | Définit si l'utilisateur anonyme sera autorisé à effectuer des opérations sur les fichiers, telles que la suppression et le changement de nom de fichier Ce booléen est défini sur **NO par défaut** |
| **anon\_root** | Détermine le répertoire dans lequel l'utilisateur anonyme se connecte après une connexion au serveur FTP Si cette directive n’est pas définie, le répertoire utilisé est le répertoire de base du compte anonyme (voir ftp\_username) défini dans le fichier /etc/passwd Cette valeur de chaîne n'a **pas de valeur par défaut** |
| **anon\_world\_readable\_only** | Définit si l'utilisateur anonyme peut voir et télécharger des fichiers lisibles par tout le monde De cette manière, certains fichiers appartenant au compte anonyme (voir ftp\_username) peuvent être protégés des utilisateurs de serveurs FTP anonymes Ce booléen est défini sur **YES par défaut** |
| **anon\_upload\_enable** | Détermine si un utilisateur anonyme peut téléverser des fichiers sur le serveur FTP Si défini sur YES, pour que cela fonctionne correctement, la directive write\_enable doit également être définie sur YES et l’autorisation d’écriture sur le répertoire parent de l’emplacement de téléchargement doit être activée pour le compte utilisateur anonyme Ce booléen est défini sur **NO par défaut** |
| **anonymous\_enable** | Définit si le compte d'utilisateur anonyme est utilisé pour l'accès au serveur FTP Si seul un accès utilisateur anonyme est souhaité, cette directive doit être définie sur YES et la directive local\_enable sur NO Ce booléen est défini sur **YES par défaut** |
| **banner\_file** | Définitle message affiché avant la tentative de connexion Par défaut, le serveur vsftpd affiche ses informations de version … 220 (vsFTPd 2.0.5)  Cela peut entraîner des problèmes de sécurité car le fait de connaître la version d'un serveur peut fournir à un pirate informatique des informations lui permettant d'exploiter le serveur Au lieu d'afficher la version du serveur vsftpd, on doit envisage de créer un fichier avec un avertissement immédiat et de définir la directive banner\_file= pour qu'elle pointe vers ce fichier d'avertissement |
| **chown\_uploads** | Détermine si la propriété de tous les fichiers téléversés anonymes est remplacée par un nom d'utilisateur spécifié (voir chown\_username) Ce booléen est défini sur **NO par défaut** |
| **chown\_username** | Définit le nom d'utilisateur pour la propriété de tous les fichiers téléchargés anonymes Si défini, pour que cela fonctionne correctement, la directive chown\_uploads doit être définie sur YES Cette chaîne n'a **pas de valeur par défaut** |
| **chroot\_local\_user** | Détermine s'il faut placer les utilisateurs locaux accédant au service FTP dans une prison chroot en utilisant leur répertoire de base comme nouveau répertoire racine Ce booléen est défini sur NO par défaut |
| **chroot\_list\_enable** | Définit si une liste d'utilisateurs locaux est placée dans une prison chroot en utilisant leur répertoire de base comme nouveau répertoire racine Si défini sur YES et que chroot\_local\_user est défini sur YES, ceci active une liste (voir chroot\_list\_file) des utilisateurs ne pouvant pas être placés dans une prison chroot Si défini sur YES et que chroot\_local\_user est défini sur NO, ceci active la liste des utilisateurs qui doivent être placés dans une prison chroot Si défini sur YES, la directive chroot\_list\_file doit être définie pour que cela fonctionne correctement Ce booléen est défini sur **NO par défaut** |

|  |  |
| --- | --- |
| Directive | Description |
| **chroot\_list\_file** | Désigne le fichier contenant la liste des utilisateurs à être ou non placés dans une prison chroot en utilisant leur répertoire de base comme nouveau répertoire racine Si elle est définie, pour que cela fonctionne correctement, la directive chroot\_list\_enable doit être définie sur YES La valeur par défaut de cette directive **dépend de la distribution** |
| **dir\_message\_enable** | Permet d’afficher le contenu du fichier **.message** lors de l’accès à un répertoire  Cela peut être utile afin d’avertir les usagers anonymes d’un usage correct du serveur FTP Ce booléen est défini sur **YES par défaut** |
| **ftp\_banner** | Définit un un petit message de pré-connexion? Au lieu d'utiliser un fichier, on utilise simplement **ftpd\_banner=Message** |
| **ftp\_username** | Définit le nom d'utilisateur du compte anonyme à utiliser pour les connexions anonymes La valeur par défaut de cette directive est ftp |
| **listen** | Détermine si le vsftpd opère est en mode autonome et est démarré via un service d’initialisation (YES) ou géré via le démon xinetd (NO) Dans les deux cas, il n’écoute que la communication IPv4 Ce booléen est défini sur **NO par défaut** |
| **listen\_ipv6** | Détermine si vsftpd s'exécute en mode autonome et est démarré via un service d'initialisation (YES) ou géré via le démon xinetd (NO) Dans les deux cas, il n’écoute que la communication IPv6 Ce booléen est défini sur **NO par défaut** |
| **local\_enable** | Définit si les connexions locales au service FTP sont autorisées ou non Si défini sur YES, les comptes d'utilisateurs répertoriés dans /etc/passwd (également appelés non anonymes) peuvent être utilisés pour se connecter au service FTP Ce booléen est défini sur **NO par défaut** |
| **local\_max\_rate** | Définit le débit, en octets par seconde, pouvant être transféré par les utilisateurs réguliers |
| **log\_ftp\_protocol** | Détermine si toutes les requêtes et réponses FTP sont consignées Ce booléen est défini sur **NO par défaut** |
| **max\_client** | Limite le nombre de clients FTP pouvant se connecter au serveur en même temps Ceci est utile pour prévenir les attaques DDoS |
| **max\_per\_ip** | Limite le nombre de clients FTP pouvant se connecter à partir d'une seule adresse IP Ceci est important lorsque la directive max\_clients est utilisée pour empêcher un utilisateur d’utiliser toutes les connexions possibles |
| **userlist\_enable** | Définit si un fichier de liste de noms d'utilisateurs est chargé et vérifié lorsqu'un utilisateur tente de se connecter Si la valeur est définie sur YES, tout utilisateur figurant dans le fichier de liste de noms d'utilisateurs se voit refuser l'accès avant toute tentative de mot de passe De plus, si cette option est définie sur YES, la directive userlist\_file doit être définie sur un fichier de liste de noms d'utilisateurs pour que cela fonctionne correctement Ce booléen est défini sur **NO par défaut** |
| **userlist\_file** | Désigne le fichier contenant la liste de noms d'utilisateurs à qui l'accès est refusé lors d'une tentative de connexion La valeur par défaut de cette directive **dépend de la distribution** |
| **write\_enable** | Définit si un utilisateur FTP peut émettre des commandes pour modifier le système de fichiers, telles que le téléversement ou la suppression de fichiers Ce booléen est défini sur **NO par défaut** |

De nombreuses **directives du fichier vsftpd.conf sont interdépendantes**.   
En outre, le fait que l’on utilise une directive particulière ou un ensemble d’entre elles dépend de ce que l’on essaie d’accomplir.

Si on souhaite afficher toutes les directives vftpd.conf, on peut le faire à l’aide de la page de manuel.

### Accès avec nom d'utilisateur et mot de passe

Configurer un serveur FTP vsftpd qui accepte les noms d'utilisateur et les mots de passe pour accéder aux fichiers est assez simple.

Tout d’abord, dans le **fichier vsftpd.conf**, on vérifie certaines directives.   
La **directive local\_enable** doit être définie sur YES …

**>> grep enable /etc/vsftpd.conf | grep -v '#'**anonymous\_enable=NO  
local\_enable=YES  
dirmessage\_enable=YES  
xferlog\_enable=YES  
ssl\_enable=NO

Si on doit apporter des modifications au fichier vsftpd.conf, on effectue d’abord une copie de sauvegarde.   
(Cela est toujours une bonne idée.)   
Une fois vos modifications terminées, on redémarre le service …

**>> sudo systemctl restart vsftpd.service**

Ensuite, un compte d'utilisateur FTP est ajouté.   
Ici, un utilisateur tuxftp est ajouté un compte et un mot de passe au système du serveur FTP …

**>> sudo useradd -d /home/tuxftp -m tuxftp  
>> sudo passwd tuxftp**

Comme cet utilisateur est un utilisateur FTP et ne devrait pas avoir un accès complet au système, le shell par défaut du compte est remplacé par /usr/sbin/nologin (sur certaines distributions, ce shell est /sbin/nologin) …  
**>> sudo usermod -s /usr/sbin/nologin tuxftp**