

Serveur FTP

Systeme d'exploitation 2

Présenté par :

- Fatima-zahra Ait Benalla
- Fatima Es-sofyany
- Kawtar Herra

Encadré par :

Mr.Moukhafi

REMERCIEMENT

Mes remerciements vont à **Mr.Moukhafi** pour son encadrement et ses conseils précieux. Un grand merci également à mes collègues de classe pour leur collaboration et leur soutien tout au long du projet.

Ensemble, nous avons atteint nos objectifs et réussi à compléter ce projet avec succès.

Table des matières

Introduction :
Définition du FTP : 1
histoire du FTP : 1
Les types du ftp :
FTP : 4
FTPS : 4
SFTP : 4
Les modes FTP :
Mode actif : 6
Mode passif : 6
Modèle OSI : 7
Modèle TCP/IP : 7
Adresse IP : 9
Fragmentation : 9
Installation et Configuration FTP avec VSFTPD :
Installation: 12
sudo dnf install vsftpd 12
Activer serveur FTP : 12
sudo systemctl start vsftpd 12
sudo systemctl status vsftpd 12
Configuration : 13
Sudo vi /etc/vsftpd/vsftpd.conf 13
Réglage du pare-feu : 13
sudo useradd -m ftpuser 14
FileZilla Client : 14
Conclusion :

Introduction

Définition du FTP :

FTP est l'abréviation de File Transfer Protocol, Ce protocole de communication est utilisé pour l'échange de fichiers entre un serveur et un client. FTP est utile pour transférer des fichiers entre ordinateurs, que ce soit à distance ou au sein d'un réseau local, votre ordinateur personnel peut même faire office de serveur FTP. Il intervient au niveau de la couche application du modèle OSI (couche n°7) et utilise TCP comme protocole de transport.

Il s'inscrit dans un modèle client/serveur qui permet :

- Le téléchargement de fichiers depuis un serveur vers le client (Download)
- Le téléchargement de fichiers depuis le client vers un serveur (Upload),

C'est le protocole le plus sûr pour faire du téléchargement de fichiers, même si cette opération peut aussi être réalisée avec http.

FileZilla server est un exemple de serveur FTP open-source. Il est très puissant, pratique et fonctionne à merveille avec un client FileZilla.

Histoire du FTP :

L'histoire du File Transfer Protocol (FTP) remonte aux premiers jours de l'informatique et des réseaux. Voici une brève chronologie de son évolution :

- 1- Début (années 1970) : Le FTP a été développé dans les années 1970 par Abhay Bhushan, un étudiant du Massachusetts Institute of Technology (MIT). L'objectif était de permettre le transfert de fichiers entre différents ordinateurs connectés au réseau ARPANET, l'ancêtre d'Internet. La première spécification officielle du FTP a été publiée en 1971.
- 2- Normalisation (années 1980) : Au fur et à mesure que les réseaux informatiques se développaient, le FTP est devenu un standard de facto pour le transfert de fichiers. Dans les années 1980, il a été formalisé en tant que standard de l'Internet Engineering Task Force (IETF), avec la publication de la RFC 959 en 1985 détaillant le protocole FTP.
- 3- Extensions et améliorations (années 1990) : Au cours des années 1990, plusieurs extensions et améliorations ont été apportées au FTP pour accroître ses fonctionnalités et sa sécurité. Parmi celles-ci, on trouve l'introduction de FTP sécurisé (FTPS) qui utilise SSL/TLS pour le chiffrement des données.

- 4- L'arrivée de l'Internet (années 1990-2000) : Avec la popularisation de l'Internet grand public, le FTP est devenu un outil essentiel pour le partage de fichiers et la gestion de sites web. Les clients FTP graphiques ont été développés, facilitant l'accès et la manipulation des fichiers pour les utilisateurs non techniques.
- 5- Évolution vers des alternatives (années 2000 à nos jours) : Bien que le FTP soit toujours largement utilisé, des alternatives plus modernes ont émergé au fil du temps. Des protocoles tels que SFTP (SSH File Transfer Protocol) et des services de stockage cloud ont gagné en popularité en raison de leur sécurité améliorée et de leur facilité d'utilisation.
- 6- Persistance (à ce jour) : Malgré l'émergence de nouvelles technologies, le FTP demeure pertinent dans de nombreux scénarios. Il est souvent utilisé dans des environnements professionnels et industriels où la simplicité et la fiabilité sont prioritaires.

Les types du ftp

FTP :

- La version standard qui nous connaissons, non sécurisé.
- Fonctionne sur deux canaux distincts, l'un pour le contrôle (commandes) et l'autre pour les données.

FTPS :

FTPS est une extension sécurisée du protocole FTP. FTPS utilise le chiffrement SSL/TLS pour sécuriser la communication entre le client FTP et le serveur FTP. Il existe deux modes principaux de FTPS :

- La methode implicite : la connexion sécurisée est établie dès le début. Le client FTPS se connecte au port spécifique généralement le port 990 du serveur FTP, et la connexion est automatiquement sécurisée via SSL/TLS.
- La methode explicite : le client FTPS initie une connexion non sécurisée au serveur FTPS sur le port 21, ensuite le client envoie une commande spéciale (SSL/TLS) pour demander une connexion sécurisée, si le serveur accepte, la connexion rend sécurisé. le client et le serveur négocient le démarrage de la session sécurisée à l'aide du protocole STARTTLS (pour TLS) ou du protocole de commande PROT (pour SSL).

SFTP :

SFTP (SSH File Transfer Protocol ou Secure File Transfer Protocol) est un protocole distinct du FTP. Contrairement à FTP et FTPS, SFTP n'est pas lié à FTP mais utilise SSH (Secure Shell) pour fournir un canal sécurisé de transfert de fichiers.

Parmi les caractéristiques importantes de SFTP :

1- Sécurité par défaut :

SFTP chiffre toutes les données pendant la transmission, ce qui signifie que la confidentialité et l'intégrité des données sont assurées par défaut.

2- Canal unique :

SFTP utilise un seul canal (généralement sur le port 22) pour les commandes et le transfert de données, simplifiant ainsi la configuration réseau par rapport à FTP qui utilise des canaux séparés pour les commandes et les données.

Les modes FTP

Mode actif :

Dans session contrôle le client ftp envoie une demande de connexion au serveur ftp. Les commandes FTP (par exemple, USER, PASS, LIST, RETR) sont envoyées du client vers le serveur, et les réponses du serveur (par exemple, 220 Welcome, 331 Password required) sont renvoyées au client sur le même canal (généralement sur le port 21).

Dans session de donnée le serveur initie une connexion sur le port de données 20 vers le port de données spécifié (high port non réservé) par le client pour le transfert des fichiers. Certains pare-feux peuvent bloquer ces connexions entrantes, provoquant des échecs de transfert de données. Cela peut nécessiter une configuration manuelle du pare-feu. Le mode passif est souvent une solution plus simple dans des environnements où le mode actif rencontre des problèmes

Mode passif :

Dans session contrôle comme Mode actif.

Dans session donnée le client initie une connexion sur le port de donnée spécifié (high port) au serveur ftp, le client envoie la commande PASV (Passive) au serveur. La commande PASV demande au serveur de passer en mode passif. Le serveur répond à la commande PASV en indiquant une adresse IP et un numéro de port pour la connexion de données passives. Le client utilise l'adresse IP et le port fournis par le serveur pour établir une connexion de données avec le serveur.

Modèle OSI

Modèle TCP/IP

Couche Transport (4) : Cette couche assure la fiabilité du transfert de bout en bout des données, en fractionnant les données en paquets plus petits si nécessaire et en gérant les erreurs :

- Segmentation :
 - numéro de port
 - numéro de Séquence
- Contrôle de flux.
- Contrôle des erreurs.

Faisant l'encapsulation en passant de la couche transport à la couche Réseau en ajoutant IP destinataire et IP source, et la donnée devienne un paquet.

Couche Réseau (3) : Responsable du routage des données à travers le réseau, elle détermine le meilleur chemin pour les données entre l'émetteur et le destinataire.

Couche Liaison (2) : Elle assure la transmission fiable des données à travers un lien physique, en détectant et corrigeant les erreurs.

-En ajoutant l'adresse Mac source et destinataire

Modèle TCP/IP

On donne un exemple sur le modèle TCP/IP pour très bien comprendre, Commenant avec une requête « www.dijon.fr » qui va être traduit par GET qui signifie obtenir suivie de l'adresse du site web sous forme d'IP.

L'encapsulation est commencée

La couche transport va ajouter un entête :

- Le port source : numéro qui identifie les application, 1337 identifie notre navigateur web
- Le port 80 : identifier une application du serveur web

Le segment est encapsulé par la couche Internet en ajoutant IP Destination : du serveur qui héberge la page web et IP Source

Le paquet est encapsulé par la couche Réseau en ajoutant un entête de l'adresse MAC de la carte réseau Destination du prochain routeur et MAC Source de la carte de notre ordinateur.

Donc le message est arrivé au destinataire mais comment l'expéditeur va savoir, pour cela les ports sont inverses, numéro du message augmente pour faire suite au message précédent et le flag va utiliser : ACK : acknowledgment of receipt, accusé de réception, bien reçu, c'est seulement l'enveloppe qui va voyager et non la donnée.

Adresse IP

Fragmentation

Adresse IP : numéro d'identification unique à chaque périphérique faisant partie d'un même réseau informatique utilisant Internet Protocol, 2 versions sont disponibles :

- **IPV4 :** qui peut être divisé en 2 parties, partie Réseau et partie Hôte

-partie Réseau : identifiant du réseau auquel appartient la machine

-Hôte : identifiant de la machine elle-même.

A savoir qu'on a 4,3 Milliards d'IP de IPV4.

Les Classes d'adresse IP :

- Classe A : peut marcher avec une entreprise ou grande société
- Classe B : peut marcher avec les petites entreprises.
- Classe C : peut marcher avec petites organisation ou les maisons, et c'est la classe la plus utilisée.

- **IPV6 :**

- IPV6 a été développé pour répondre aux limitations d'adressage d'IPv4 et apporte des améliorations en termes d'espace d'adressage.....

-Les adresses IPv6 sont représentées en notation hexadécimale et sont structurées en huit groupes de quatre chiffres hexadécimaux, séparés par des deux-points. Par exemple, une adresse IPv6 typique ressemble à ceci : 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

La fragmentation est le processus de division de données en fragments plus petits pour permettre leur transmission sur des réseaux avec des contraintes de taille.

Installation et Configuration FTP avec VSFTPD

On va installer VSFTPD, qui signifie "Very Secure FTP Daemon", est un serveur FTP open-source populaire utilisé pour transférer des fichiers entre un client et un serveur sur un réseau.

Installation:

Il suffit d'installer le paquet vsftpd :

sudo dnf install vsftpd

```
[aitbenalla@fedora ~]$ sudo systemctl status vsftpd
[sudo] Mot de passe de aitbenalla :
Unit vsftpd.service could not be found.
[aitbenalla@fedora ~]$ sudo dnf install vsftpd
Dernière vérification de l'expiration des métadonnées effectuée il y a 2:22:32 le sam. 18 nov. 2023 10:14:39.
Dépendances résolues.
=====
Paquet          Architecture  Version      Dépôt        Taille
=====
Installation:
vsftpd          x86_64       3.0.5-4.fc38 updates      168 k
=====
Résumé de la transaction
=====
Installer 1 Paquet

Taille totale des téléchargements : 168 k
Taille des paquets installés : 348 k
Voulez-vous continuer ? [o/N] : o
Téléchargement des paquets :

Voulez-vous continuer ? [o/N] : o
Téléchargement des paquets :
vsftpd-3.0.5-4.fc38.x86_64.rpm          97 kB/s | 168 kB    00:01
-----
Total                                9.3 kB/s | 168 kB    00:18
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-3.0.5-4.fc38.x86_64 1/1
Exécution du scriptlet: vsftpd-3.0.5-4.fc38.x86_64 1/1
Vérification de : vsftpd-3.0.5-4.fc38.x86_64 1/1
Installé:
vsftpd-3.0.5-4.fc38.x86_64
Terminé !
[aitbenalla@fedora ~]$
```

Activer serveur FTP :

Démarrer le serveur par la commande :

sudo systemctl start vsftpd

Pour vérifier l'activation du FTP on utilise la commande suivante :

sudo systemctl status vsftpd


```
[aitbenalla@fedora ~]$ sudo systemctl start vsftpd
[aitbenalla@fedora ~]$ sudo systemctl status vsftpd
● vsftpd.service - Vsftpd ftp daemon
   Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; disabled; preset: disabled)
   Drop-In: /usr/lib/systemd/system/service.d
            └─10-timeout-abort.conf
   Active: active (running) since Sat 2023-11-18 12:40:42 +01; 3s ago
     Process: 8799 ExecStart=/usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf (code=exited, status=0/SUCCESS)
    Main PID: 8800 (vsftpd)
       Tasks: 1 (limit: 2296)
      Memory: 900.0K
         CPU: 6ms
      CGroup: /system.slice/vsftpd.service
              └─8800 /usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf

nov. 18 12:40:42 fedora systemd[1]: Starting vsftpd.service - Vsftpd ftp daemon...
nov. 18 12:40:42 fedora systemd[1]: Started vsftpd.service - Vsftpd ftp daemon.
[aitbenalla@fedora ~]$
```

Configuration :

La configuration de vsftpd est réalisée à partir du fichier "vsftpd.conf".

Sudo vi /etc/vsftpd/vsftpd.conf

Le fichier vsftpd.conf propose un grand nombre d'options dont les plus importantes sont :

- Listen : permet de définir si le démon est en standalone (YES) ou dirigé par(x) inetd (NO)
- anonymous_enable : permet d'accepter les connexions anonymes
- local_enable : autorise les personnes à s'identifier avec un compte utilisateur local
- write_enable : donne la permission d'écriture
- chroot_local_user : permet de "chrooter" la connexion de l'utilisateur
- allow_writeable_chroot : autorise l'écriture pour les utilisateurs "chrootés"

La configuration par défaut de vsftpd est très restrictive:

- Le compte anonyme n'est pas autorisé à se connecter au serveur (anonymous_enable=NO)
- Les utilisateurs ne peuvent accéder qu'à leur compte, et en lecture seule (local_enable=YES)

Réglage du pare-feu :

- Pour utiliser le mode actif

```
[aitbenalla@fedora ~]$ sudo firewall-cmd --add-service=ftp --permanent
success
[aitbenalla@fedora ~]$ sudo systemctl restart vsftpd
[aitbenalla@fedora ~]$ sudo firewall-cmd reload
usage: 'firewall-cmd --help' for usage information or see firewall-cmd(1) man page
firewall-cmd: error: unrecognized arguments: reload
[aitbenalla@fedora ~]$ sudo firewall-cmd --reload
success
[aitbenalla@fedora ~]$ sudo systemctl restart vsftpd
```

- Pour le mode passif

```
# Example config file /etc/vsftpd/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
# Allow anonymous FTP? (Beware - allowed by default if you comment this out).
anonymous_enable=YES
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES

pasv_enable=YES

#
# Default umask for local users is 077. You may wish to change this to 022.
```

On peut créer un utilisateur

sudo useradd -m ftpuser

-m : Cette option crée automatiquement un répertoire personnel (home directory) pour le nouvel utilisateur. Le répertoire personnel est généralement créé dans le répertoire /home et porte le même nom que l'utilisateur.

```
[aitbenalla@fedora ~]$ sudo useradd -m ftpuser
[aitbenalla@fedora ~]$ sudo passwd ftpuser
Changement de mot de passe pour l'utilisateur ftpuser.
Nouveau mot de passe :
MOT DE PASSE INCORRECT : Le mot de passe ne passe pas la vérification dans le di
ctionnaire - basé sur un mot du dictionnaire
Retapez le nouveau mot de passe :
passwd : mise à jour réussie de tous les jetons d'authentification.
[aitbenalla@fedora ~]$
```

FileZilla Client :

FileZilla Client est une application logicielle qui permet aux utilisateurs de se connecter à des serveurs FTP pour transférer des fichiers.

ftpuser@192.168.56.102 - FileZilla

Statut : Transfert de fichier réussi, 330 octets transférés en 1 seconde
 Statut : Récupération du contenu du dossier « / »...
 Statut : Contenu du dossier « / » affiché avec succès
 Statut : Déconnecté du serveur
 Statut : Connexion interrompue par le serveur

Site local : C:\Users\aitbe\Desktop\ Site distant : /

Nom de fichier	Taille d...	Type de fich...	Dernière m...
..			
office		Dossier de f...	20/10/2023...
a.txt	330	Document t...	09/11/2023...
desktop.ini	282	Paramètres ...	20/10/2023...
Eclipse IDE for J...	1 095	Raccourci	22/10/2023...
FTP.docx	19 880	Document ...	05/11/2023...
Les commande...	14 111	Document ...	02/11/2023...
passwor.txt	59	Document t...	08/11/2023...
Telegram.Ink	1 032	Raccourci	17/11/2023...

élection de 1 fichier. Taille totale : 330 octets

Nom de fichier	Taille ...	Type d...	Dernière ...	Droits ...	Proprié...
..					
a.txt	330	Docu...	21/11/20...	-rw-r--...	1001 1...

1 fichier. Taille totale : 330 octets

serveur / Fichier local | Dire... | Fichier distant | Taille | Prio... | Statut

Ou Juste entrer avec compte anonymous

Hôte : 192.168.56.106 Nom d'utilisateur : Mot de passe : Port : Connexion rapide

Statut : Connexion à 192.168.56.106:21...
 Statut : Connexion établie, attente du message d'accueil...
 Statut : Serveur non sécurisé, celui-ci ne prend pas en charge FTP sur TLS.

Site local : C:\Users\aitbe\Desktop\ Site distant :

Connexion FTP non sécurisée

Ce serveur ne gère pas FTP sur TLS.
 Si vous continuez, votre mot de passe et vos fichiers seront envoyés en clair sur Internet.

Hôte : 192.168.56.106
 Port : 21
☐ Toujours autoriser FTP non sécurisé pour ce serveur.

OK Annuler

9 fichiers et 2 dossiers. Taille totale : 247 314 octets

Déconnecté.

Serveur / Fichier local | Dire... | Fichier distant | Taille | Prio... | Statut

Hôte : 192.168.56.106 Nom d'utilisateur : Mot de passe : Port : [Connexion rapide](#)

Statut : Connexion établie, attente du message d'accueil...
 Statut : Serveur non sécurisé, celui-ci ne prend pas en charge FTP sur TLS.
 Statut : Connecté
 Statut : Récupération du contenu du dossier...
 Statut : Contenu du dossier « / » affiché avec succès

Site local : C:\Users\aitbe\Desktop\ Site distant : /

- Desktop
- Documents
- Downloads
- eclipse
- eclipse-workspace
- Favorites

- /
- pub

Nom de fichier	Taille d...	Type de fich...	Dernière m...	Nom de fichier	Taille ...	Type d...	Dernière ...	Droits ...	Proprié...
..				..					
JEE		Dossier de f...	11/12/2023...	pub		Dossie...	22/07/20...	drwxr-...	0 0
office		Dossier de f...	20/10/2023...						
a.txt	330	Document t...	27/11/2023...						
desktop.ini	282	Paramètres ...	20/10/2023...						
Eclipse IDE for J...	1 095	Raccourci	22/10/2023...						
java.txt	74	Document t...	07/12/2023...						
Les commande...	14 111	Document ...	02/11/2023...						
passwor.txt	59	Document t...	08/11/2023...						

9 fichiers et 2 dossiers. Taille totale : 247 314 octets 1 dossier

Conclusion :

Le FTP demeure un pilier fondamental pour les transferts de fichiers, offrant une combinaison de simplicité et de fiabilité. Que ce soit à travers l'histoire du protocole, les types de FTP disponibles, les modes de transmission, les modèles OSI et TCP/IP, ou les aspects pratiques de l'installation et de la configuration, ce rapport offre une vue complète du FTP et de son rôle essentiel dans les communications informatiques modernes.