



Configuration d'un serveur FTP sur Linux (CENTOS)

Équipe de rédaction et d'approbation		
NGANSOP NJANOU ULRICH SOSTAIRE	Stagiaire (Admin Junior Réseau Informatique) EVOLV IZSOFTWARES GROUP Ltd	Date: 15 janvier 2025
GILDAS FOTSO TABAFO	Stagiaire (Admin Junior Réseau Informatique) EVOLV IZSOFTWARES GROUP Ltd	Date: 15 janvier 2025
Beryl Ngonga	Encadreur professionnelle - EVOLV IZSOFTWARES GROUP Ltd	Date de fin :
Sommaire des révisions		
Historique de Révision	Description générale	Date approuvée
0.0.0	Document, version 0	

Résumé des prérequis

- Adresse IP statique configurée.
- Pare-feu configuré pour autoriser le trafic FTP.
- SELinux configuré (si activé).
- Certificat SSL/TLS généré (pour FTPS).
- Utilisateur FTP et répertoire dédié créés.
- Système à jour.

Prérequis pour la configuration d'un serveur FTP sur CentOS

Avant de configurer un serveur FTP sur CentOS, assurez-vous que les éléments suivants sont en place :

1. Adressage IP et réseau

- **Adresse IP statique** : Veillez à ce que votre serveur CentOS soit configuré avec une adresse IP statique. Pour vérifier l'adresse IP, utilisez la commande suivante et suivez les instructions :

```
1 nmtui
```

- **DNS ou fichier hosts** : Lorsque vous utilisez un nom de domaine, il est essentiel de vérifier qu'il est correctement configuré dans votre DNS. Si ce n'est pas le cas, vous avez la possibilité d'ajouter une entrée dans le fichier `/etc/hosts` sur le client FTP, afin de lier l'adresse IP du serveur à un nom d'hôte.

2. Accès root ou utilisateur avec privilèges [↗](#)

- Pour installer et configurer les services FTP, vous devez disposer d'un accès **root** ou d'un utilisateur ayant des privilèges **sudo**.

3. Mise à jour du système [↗](#)

- Avant d'installer un serveur FTP, il est essentiel de mettre à jour votre système CentOS afin de garantir que tous les paquets soient à jour :

```
1 sudo yum update -y
```

4. Pare-feu (Firewall) [↗](#)

- Le pare-feu doit être configuré pour autoriser le trafic FTP. Sur CentOS, `firewalld` est généralement utilisé. Ouvrez les ports nécessaires :

- **Port 21** pour FTP.
- **Port 20** pour le mode actif FTP (si nécessaire).
- **Port 990** pour FTPS.
- **Port 22** pour SFTP (si vous utilisez SSH).

Exécutez les commandes suivantes pour ouvrir les ports :

```
1 sudo firewall-cmd --permanent --add-port=21/tcp
2 sudo firewall-cmd --permanent --add-port=20/tcp
3 sudo firewall-cmd --permanent --add-port=990/tcp
4 sudo firewall-cmd --permanent --add-port=22/tcp
5 sudo firewall-cmd --reload
```

5. SELinux (si activé) [↗](#)

- Si SELinux est activé sur votre système, vous devez configurer les règles pour autoriser le service FTP. Exécutez les commandes suivantes :

```
1 sudo setsebool -P ftpd_full_access on
2 sudo setsebool -P ftp_home_dir on
```

- Si vous souhaitez désactiver SELinux, il vous suffit d'accéder au répertoire `/etc/selinux/config/`. Ensuite, remplacez "**enforcing**" par "**permissive**" dans le fichier de configuration.

```
1 nano /etc/selinux/config
```

7. Utilisateur FTP [↗](#)

- Préparez un utilisateur dédié pour le serveur FTP. Cet utilisateur aura accès au répertoire FTP. Par exemple :

```
1 sudo adduser ftpuser
2 sudo passwd ftpuser
```

8. Répertoire FTP [↗](#)

- Si un répertoire dédié pour le serveur FTP a déjà été créé (`sudo mkdir /var/ftp`), il est important de définir les permissions appropriées :

```
1 sudo chown ftpuser:ftpuser /var/ftp
2 sudo chmod 755 /var/ftp
```

9. Vérification de la connectivité [↗](#)

- Assurez-vous que le serveur est accessible depuis le réseau. Vous pouvez utiliser la commande `ping` ou un outil comme `nmap` (`sudo yum install nmap -y`) pour vérifier que les ports FTP sont ouverts :

```
1 nmap -p 21,22,990 <adresse-ip-du-serveur>
```

```
[root@localhost ulrich]# nmap -p 21,22,990 192.168.2.5
Starting Nmap 7.92 ( https://nmap.org ) at 2025-02-11 17:15 EST
Nmap scan report for 00:0C:29:DD:C8:3E (192.168.2.5)
Host is up (0.00030s latency).

PORT      STATE SERVICE
21/tcp    closed ftp
22/tcp    open  ssh
990/tcp   closed ftps

Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
```

Interprétation des résultats

Port 21 (FTP) : Fermé

1. Cela signifie que le service FTP n'est pas actif sur votre serveur.
2. Si vous souhaitez utiliser FTP, vous devez :
 - Installer et configurer un serveur FTP (comme `vsftpd` ou `ProFTPD`).
 - Ouvrir le port **21** dans le pare-feu.

Port 22 (SSH) : Ouvert

1. Le port **22** est ouvert, ce qui signifie que le service SSH est actif.
 - SSH est utilisé pour accéder à votre serveur de manière sécurisée.
 - Si vous ne souhaitez pas utiliser SSH, vous pouvez le désactiver pour des raisons de sécurité.

Port 990 (FTPS) : Fermé

1. Le port **990** est fermé, ce qui signifie qu'aucun service FTPS (FTP over SSL/TLS) n'est actif.

⚠ REMARQUE : Certificat SSL/TLS (pour FTPS) - optionnel [↗](#)

- Si vous prévoyez d'utiliser FTPS (FTP over SSL/TLS), vous devez disposer d'un certificat SSL. Vous pouvez en générer un auto-signé avec les commandes suivantes :
- ```
1 sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/vsftpd.key -out /etc/
```

NB : En exécutant cette commande, il est possible que vous rencontriez une erreur, ce qui peut être normal. L'erreur que vous pourriez rencontrer pourrait indiquer que la commande `openssl` ne parvient pas à écrire le fichier de clé privée ( `/etc/ssl/private/vsftpd.key` ) car le répertoire `/etc/ssl/private` n'existe pas. Cela est fréquent sur certains systèmes où ce répertoire n'est pas créé par défaut.

## **Solution [↗](#)**

### 1. Créer le répertoire manquant :

Vous devez créer le répertoire `/etc/ssl/private` et définir les permissions appropriées pour qu'il soit accessible uniquement par l'utilisateur root.

```
1 sudo mkdir -p /etc/ssl/private
2 sudo chmod 700 /etc/ssl/private
```

- ## 2. Créer le répertoire pour le certificat :

```
1 sudo mkdir -p /etc/ssl/certs
2 sudo chmod 755 /etc/ssl/certs
```

```
1 sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/vsftpd.key -out /etc/
```

```
1 ls /etc/ssl/private/
2 ls /etc/ssl/certs/
```

## 2. Configurer vsftpd

Éditez le fichier de configuration de `vsftpd` :

```
1 sudo nano /etc/vsftpd.conf
```

Modifiez les paramètres suivants :

```
1 anonymous_enable=NO
2 local_enable=YES
3 write_enable=YES
4 chroot_local_user=YES
5 allow_writeable_chroot=YES
```

Pour activer FTPS (FTP over SSL/TLS), ajoutez les lignes suivantes :

```
1 ssl_enable=YES
2 rsa_cert_file=/etc/ssl/certs/vsftpd.pem
3 rsa_private_key_file=/etc/ssl/private/vsftpd.key
```

### 3. Créer un utilisateur FTP [↗](#)

Créez un utilisateur pour le serveur FTP :

```
1 sudo adduser Zetscore (votre-nom-d-utilisateur-ftp)
2 sudo passwd Zetscore (votre-nom-d-utilisateur-ftp)
```

### 4. Redémarrer vsftpd [↗](#)

Redémarrez le service `vsftpd` pour appliquer les modifications :

```
1 sudo systemctl restart vsftpd
2 sudo systemctl enable vsftpd
```

### 5. Tester l'accès FTP

## Méthode 1 : Tester le fonctionnement de notre serveur FTP en ligne de commande [↗](#)

Avec l'interface de commande CentOS, vous avez la possibilité de tester l'accès FTP sans difficulté. Il est possible d'utiliser des outils en ligne de commande pour se connecter au serveur FTP, transférer des fichiers et vérifier les permissions. Voici les étapes à suivre pour y parvenir :

#### **i** Étape 1 : Installer un client FTP en ligne de commande [↗](#)

Sur CentOS, vous pouvez utiliser `ftp` ou `lftp` pour vous connecter à un serveur FTP. Voici comment les installer :

##### 1. Installer `ftp` :

```
1 sudo yum install ftp -y
```

##### 2. Installer `lftp` (recommandé) :

- `lftp` est un client FTP plus puissant et plus convivial que `ftp`.

```
1 sudo yum install lftp -y
```

#### Étape 2 : Se connecter au serveur FTP [↗](#)

- Avec `ftp` : [↗](#)

### 1. Lancer le client FTP :

```
1 ftp 192.168.2.5
```

Remplacez `192.168.2.5` par l'adresse IP ou le nom de domaine de votre serveur FTP.

### 2. Entrer les informations de connexion :

- Vous serez invité à entrer le nom d'utilisateur et le mot de passe.
- Exemple :

```
1 Name (192.168.2.5:root): ftpuser
2 Password: *****
```

```
[root@localhost ulrich]# ftp 192.168.2.5
Connected to 192.168.2.5 (192.168.2.5).
220 (vsFTPd 3.0.5)
Name (192.168.2.5:root): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
ftp>
```

### 3. Naviguer et transférer des fichiers :

- Une fois connecté, vous pouvez utiliser les commandes FTP suivantes :
  - `ls` : Lister les fichiers et répertoires sur le serveur.
  - `cd <répertoire>` : Changer de répertoire sur le serveur.
  - `get <fichier>` : Télécharger un fichier du serveur vers votre machine locale.
  - `put <fichier>` : Envoyer un fichier de votre machine locale vers le serveur.
  - `quit` : Quitter la session FTP.

- Avec `lftp` :

### 1. Lancer `lftp` :

```
1 lftp ftp://ftpuser@192.168.2.5
```

Remplacez `ftpuser` par votre nom d'utilisateur FTP et `192.168.2.5` par l'adresse IP ou le nom de domaine de votre serveur.

### 2. Entrer le mot de passe :

- Vous serez invité à entrer le mot de passe de l'utilisateur FTP.

```
[root@localhost ulrich]# lftp ftp://ftpuser@192.168.2.5
Mot de passe :
lftp ftpuser@192.168.2.5:~> █
```


### 1. Naviguer et transférer des fichiers :

- Une fois connecté, vous pouvez utiliser les commandes suivantes :
  - `ls` : Lister les fichiers et répertoires.
  - `cd <répertoire>` : Changer de répertoire.
  - `get <fichier>` : Télécharger un fichier.
  - `put <fichier>` : Envoyer un fichier.
  - `mirror <répertoire>` : Télécharger un répertoire entier.
  - `quit` : Quitter la session.

### Étape 3 : Création de test complet, transfert de fichiers, etc.

```
[root@localhost ulrich]# lftp ftp://Zetscore@192.168.2.5
Mot de passe :
lftp Zetscore@192.168.2.5:~> ls
lftp Zetscore@192.168.2.5:~> |
```

Vous êtes actuellement dans le répertoire personnel de l'utilisateur `Zetscore` ( `/home/Zetscore` ), et ce répertoire semble vide (aucun fichier ou dossier n'est listé avec `ls` ). Voici comment créer un répertoire et un fichier, ainsi qu'une liste de tâches que vous pouvez effectuer avec votre utilisateur `Zetscore` sur le serveur FTP.

**Voici une liste de tâches que vous pouvez effectuer avec votre utilisateur `Zetscore` sur le serveur FTP :** 

#### 1. Créer un répertoire :

```
1 mkdir Data-Zetscore
```

#### 2. Créer un fichier :

```
1 echo "Ceci est un fichier de test." > fichier.txt
```

#### 3. Vérifier la création :

```
1 ls
```

#### 4. Naviguer dans le répertoire :

```
1 cd /home/Zetscore (mon_repertoire - utiliser pwd si vous voulez connaître votre repertoire)
```

#### 5. Envoyer un fichier dans le répertoire : la commande **put** ( permet d'envoyer le fichier vers le serveur )

```
1 put fichier.txt
```

#### 4. Revenir au répertoire parent :

```
1 cd ..
```

#### 5. Supprimer un fichier :

```
1 rm fichier.txt
```

#### 6. Quitter la session :

```
1 exit
```

### Étape 4 : Vérifier les permissions

#### 1. Vérifier les permissions des fichiers sur le serveur :

2. Utilisez la commande `ls -l` dans le client FTP pour afficher les permissions des fichiers :

```
1 ls -l
```

```
[root@localhost ulrich]# lftp ftp://Zetscore@192.168.2.5
Mot de passe :
lftp Zetscore@192.168.2.5:~> ls -l
drwxr-xr-x 2 1002 1002 6 Feb 11 23:39 Data-Zetscore
lftp Zetscore@192.168.2.5:~> |
```

- Cela montre les permissions ( `rw-r--r--` ), le propriétaire ( `Zetscore` ) et la taille du fichier.

## 2. Modifier les permissions (si nécessaire) :

- Si vous avez besoin de modifier les permissions, vous pouvez le faire directement sur le serveur via SSH :

```
1 chmod 755 fichier.txt
```

## Étape 5 : Déconnecter la session [↗](#)

### 1. Quitter le client FTP :

- Utilisez la commande `quit` pour fermer la session :

```
1 quit
```

## Methode 2 : Tester le fonctionnement de notre serveur FTP via l'interface graphique 'FileZilla' [↗](#)

Avec **FileZilla**, la gestion de votre serveur FTP devient simple et intuitive grâce à son interface graphique conviviale. Voici les étapes détaillées pour réaliser les mêmes tâches que celles effectuées en ligne de commande, mais cette fois-ci en utilisant **FileZilla**.

## [i](#) Étape 1 : Installer FileZilla sur CentOS [↗](#)

### 1. Ajouter le dépôt EPEL :

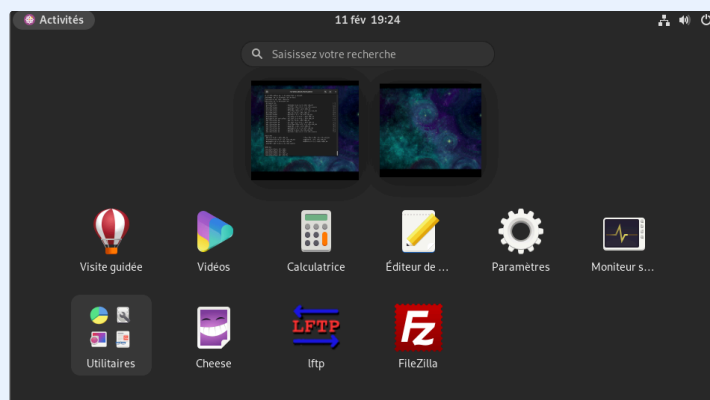
```
1 sudo yum install epel-release -y
```

### 2. Installer FileZilla :

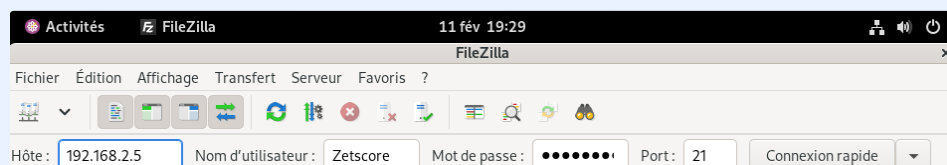
```
1 sudo yum install filezilla -y
```

### 3. Lancer FileZilla :

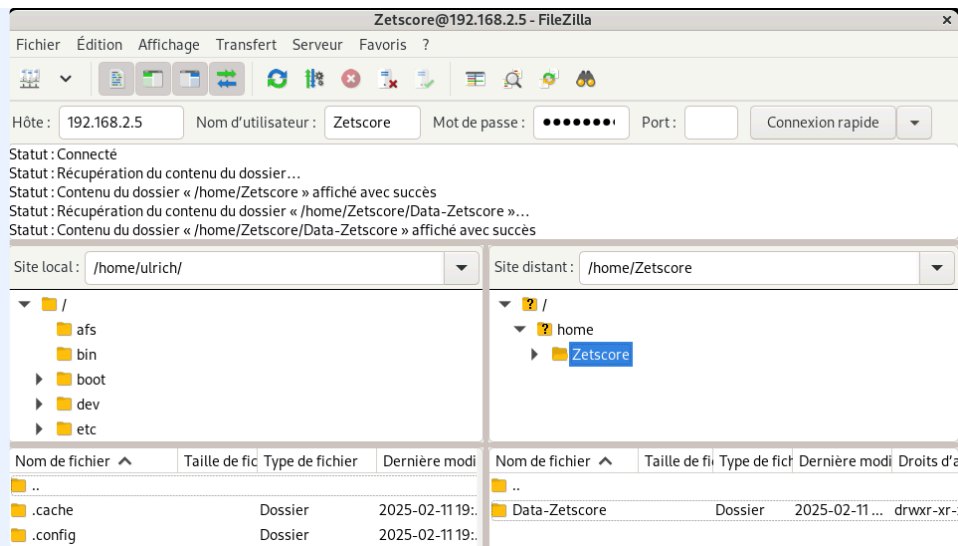
- Recherchez `FileZilla` dans le menu de votre environnement graphique.



1. Entrez les détails de connexion FTP/SFTP pour vous connecter à votre serveur.







✓ Contact des Auteurs

Pour toute question ou difficulté, n'hésitez pas à contacter les auteurs de ce document.

**Équipe Éditoriale :**

**Ulrich Sostaire Ngansop Njanou** (Administrateur Réseau Junior) - [ngansop2000@gmail.com](mailto:ngansop2000@gmail.com)

**Gildas Fotso Tabafu** (Administrateur Réseau Junior) - [gildastabafo@gmail.com](mailto:gildastabafo@gmail.com)