Connexion sécurisée avec le protocole FTP

FTPS

2015-10-10

Objectif du tutoriel : Établir une connexion chiffrée avec le serveur FTP de Cassiopea afin de sécuriser vos transferts de données.

Public cible du tutoriel : les administrateurs du site utilisant le FTP

Durée moyenne du tutoriel : 8 minutes

Niveau de technicité : Très simple

1. Préalable : installer un client FTP

Ce tutoriel s'appuiera sur l'utilisation de FileZilla[1] comme client ftp. Ce programme est disponible pour différentes plate-formes. S'il n'est pas déjà installé, téléchargez la dernière version de FileZilla pour votre système opérateur ici : https://filezilla-project.org/download.php . Veillez également à maintenir votre système opérateur à jour afin d'optimiser votre sécurité en ligne.

Installer FileZilla en suivant les instructions ici : https://wiki.filezilla-project.org/Client_Installation (instructions en anglais).

Éléments nécessaire pour votre connexion

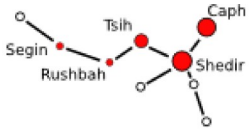
Pour établir une connexion sécurisée, vous devez être en possession de l'identifiant (login) et mot de passe fournis par les administrateurs des serveurs de Cassiopea.

2. Connexion

Établir une connexion classique

Ceci peut vous servir de test dans le cas où la connexion sécurisée ne fonctionne pas. Pour activer une connexion classique avec un serveur FTP, vous devez remplir les quatre champs suivants (dans

1 Testé avec la version 3.9 sur Linux Debian



FileZilla ces quatre champs se trouvent en haut de la fenêtre, sous les menus) :

- Le nom d'hôte : il s'agit de l'adresse du serveur, ici « ftp.cassiopea.org »
- votre identifiant
- votre mot de passe
- le numéro de port : nous utilisons le numéro de port par défaut (21).

Après avoir appuyé sur « Enter » ou cliquer sur « Connexion rapide », vous devriez établir une connexion avec nos serveurs. Si vous obtenez une erreur à ce stade, vérifiez l'orthographe des différents éléments et le numéro de port. Si l'erreur persiste, contacter un administrateur des serveurs cassiopéens.

Si la connexion est établie, vous pouvez échanger des données avec les serveurs mais elles transitent de manière non sécurisée (non chiffrée) sur le réseau. De plus votre identifiant et votre mot de passe transitent aussi en clair sur le réseau, ce qui facilite les piratages.

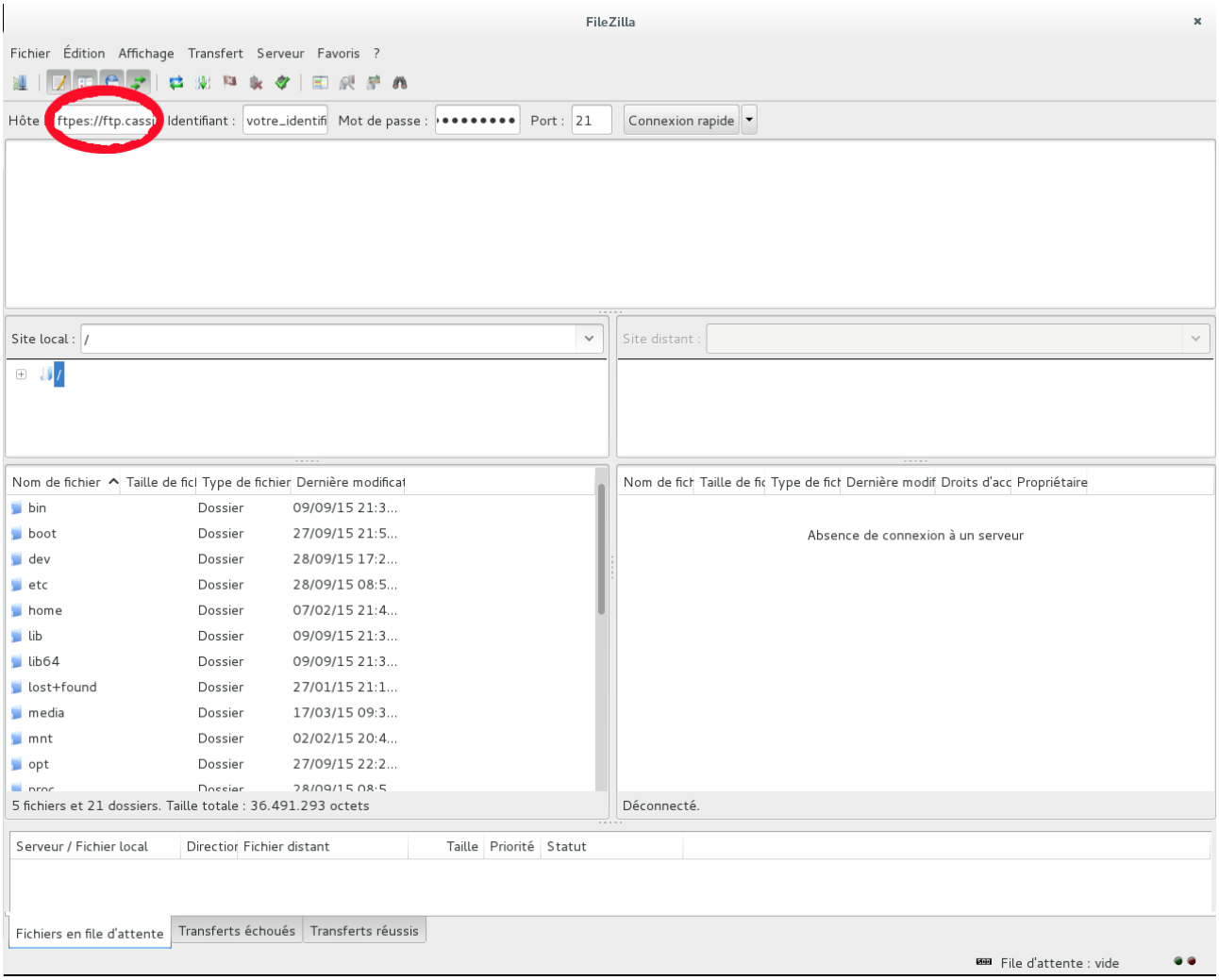
Qu'est-ce qu'un port de connexion

> La meilleure façon de vous représenter ce qu'est un port dans un ordinateur ou un serveur est de le comparer à un guichet dans une administration. Il ne suffit pas de connaître l'adresse de l'administration en question (ici l'adresse I.P. du serveur) mais également le bon guichet auquel s'adresser pour mener l'opération désirée. Les administrateurs systèmes attribuent un numéro de port pour chaque opération sur leur machine: réception de mail, de données Internet, échange de fichier, échange sécurisé, etc.. Ainsi, par exemple, le port 80 réceptionne par défaut les données de navigation Internet. Si vous envoyez des données au mauvais port, l'opération ne pourra pas être menée à bien : c'est comme si vous veniez renouveler votre carte d'identité à la commune mais que vous vous présentiez au guichet des cartes de stationnement ! Le port 21 est le port par défaut pour le protocole de transfert de fichier.

Établir une connexion sécurisée

Afin d'établir une connexion sécurisée, il est nécessaire de préciser le protocole souhaité. Par défaut, le protocole utilisé est le FTP (File Transfert Protocol), non sécurisé. Afin de sécuriser la connexion, ajoutez (dans le premier champ, avant le nom d'hôte) le protocole sous cette forme : « ftpes:// ». Les informations à fournir sont donc :

- Hôte : ftpes://ftp.cassiopea.org
- votre identifiant
- votre mot de passe
- Port : 21 (optionnel)



Lorsque vous vous connectez pour la première fois, vous devrez probablement accepter un certificat auto-signé de notre serveur. Nous ne payons en effet pas pour la signature par une autorité reconnue, car c'est relativement cher. Si vous avez des doutes sur l'authenticité du certificat, vous pouvez toujours contacter le support.

Qu'est-ce que le protocole FTPS ?

En déclarant le « ftpes:// » avant le nom du serveur, FileZilla va utiliser le protocole FTPS (FTP Secure) de manière explicite : dès sa connexion au serveur, il va passer une commande pour sécuriser les transferts de données (y compris les noms d'utilisateur et mot de passe). Cette commande (AUTH TLS) permet d'utiliser le système TLS. Ce système va chiffrer les données d'un bout à l'autre de l'échange, de la même manière que le « https:// » qui permet de sécuriser les échanges de données sur le web.

Ce système est différent du protocole SFTP qui fonctionne sur la base de SSH.

3. Vérifiez votre connexion

Une fois le certificat approuvé et lors des connexions suivantes, vous pourrez constater dans les message de FileZilla (première fenêtre sous les quatre champs) que la connexion est bien établie. Il devrait apparaître quelque chose comme ceci :

```
Statut : Résolution de l'adresse de ftp.cassiopea.org
Statut : Connexion à 92.243.20.228:21...
Statut : Connexion établie, attente du message d'accueil...
Réponse :     220 ProFTPD 1.3.4a Server (Cassiopea FTP server) [::ffff:92.243.20.228]
Commande :    AUTH TLS
Réponse :     234 AUTH TLS successful
Statut : Initialisation de TLS...
Statut : Vérification du certificat...
Commande :    USER votre_nom
Statut : Connexion TLS/SSL établie.
Réponse :     331 Password required for votre_nom
Commande :    PASS *********
Réponse :     230 User votre_nom logged in
```

La commande AUTH TLS est bien passée, la connexion est sécurisée. Le nom et le mot de passe sont transmis de manière chiffrée. Il ne reste plus qu'à transférer vos fichiers de manière tout aussi sécurisée !

FAQ

Pourquoi « ftpes:// » et pas « ftps:// » ?

Le « ftps:// » est l'ancienne méthode de connexion, moins souple. La nouvelle méthode permet de paramétrer plus finement ce qui doit être chiffré ou pas. Nous chiffrons tout (ce qui revient exactement à l'ancienne méthode).

Pourrais-je utiliser « sftp:// » ?

La configuration actuelle de nos serveurs n'autorise pas le protocole sftp avec authentification par mot de passe. Pour ne pas surcharger de travail les bénévoles maintenant nos serveurs, nous ne proposons pas aux membres l'authentification par clé publique. Le protocole FTPS avec TLS est suffisamment sûr pour les banques, il devrait l'être pour nos serveurs.

Qu'en est-il avec d'autres clients FTP ?

Sur d'autres clients FTP, la méthode pour obtenir une connexion sécurisée par FTPS peut varier. Cherchez dans les menus et options proposées comment l'activer.