Votre soumission a été envoyée avec succès! *Fermer*

Vous vous êtes désabonné avec succès! *Fermer*

Recherche sur les documen Soumettre

Serveur FTP

Le protocole de transfert de fichiers (FTP) est un protocole TCP pour le téléchargement de fichiers entre ordinateurs. Dans le passé, il a également été utilisé pour le téléchargement mais, comme cette méthode n'utilise pas le cryptage, les informations d'identification de l'utilisateur ainsi que les données transférées dans le clair et sont facilement interceptées. Donc, si vous cherchez ici un moyen de télécharger et de télécharger des fichiers en toute sécurité, voir le Documentation OpenSSH à la place.

FTP fonctionne sur un modèle client / serveur. Le composant serveur est appelé un *Démon FTP*. Il écoute en continu les demandes FTP des clients distants. Lorsqu'une demande est reçue, elle gère la connexion et configure la connexion. Pendant la durée de la session, il exécute l'une des commandes envoyées par le client FTP.

L'accès à un serveur FTP peut être géré de deux manières:

- Anonyme
- Authentifié

En mode anonyme, les clients distants peuvent accéder au serveur FTP en utilisant le compte utilisateur par défaut appelé “ anonyme ” ou “ ftp ” et en envoyant une adresse e-mail comme mot de passe. En mode Authentifié, un utilisateur doit avoir un compte et un mot de passe. Ce dernier choix est très peu sûr et ne doit pas être utilisé sauf dans des circonstances particulières. Si vous cherchez à transférer des fichiers en toute sécurité, consultez SFTP dans la section sur OpenSSH-Server. L'accès des utilisateurs aux répertoires et fichiers du serveur FTP dépend des autorisations définies pour le compte utilisé lors de la connexion. En règle générale, le démon FTP masquera le répertoire racine du serveur FTP et le modifiera dans le répertoire FTP Home. Cela masque le reste du système de fichiers des sessions distantes.

vsftpd - Installation du serveur FTP

vsftpd est un démon FTP disponible en Ubuntu. Il est facile à installer, à configurer et à entretenir. Pour installer vsftpd, vous pouvez exécuter la commande suivante:

```
sudo apt install vsftpd
```

Configuration FTP anonyme

Par défaut, vsftpd est *ne pas* configuré pour permettre un téléchargement anonyme. Si vous souhaitez activer le téléchargement anonyme, modifiez `/etc/vsftpd.conf` en changeant:

```
anonymous_enable=YES
```

Pendant l'installation a *ftp* l'utilisateur est créé avec un répertoire personnel de `/srv/ftp`. Il s'agit du répertoire FTP par défaut.

Si vous souhaitez modifier cet emplacement, à `/srv/files/ftp` par exemple, créez simplement un répertoire dans un autre emplacement et modifiez le *ftp* répertoire personnel de l'utilisateur:

```
sudo mkdir -p /srv/files/ftp
sudo usermod -d /srv/files/ftp ftp
```

Après avoir effectué le redémarrage de la modification, vsftpd:

```
sudo systemctl restart vsftpd.service
```

Enfin, copiez tous les fichiers et répertoires que vous souhaitez rendre disponibles via FTP anonyme `/srv/files/ftp`, ou `/srv/ftp` si vous souhaitez utiliser la valeur par défaut.

Configuration FTP authentifiée par l'utilisateur

Par défaut, vsftpd est configuré pour authentifier les utilisateurs du système et leur permettre de télécharger des fichiers. Si vous souhaitez que les utilisateurs puissent télécharger des fichiers, modifiez `/etc/vsftpd.conf`:

```
write_enable=YES
```

Maintenant, redémarrez vsftpd:

```
sudo systemctl restart vsftpd.service
```

Maintenant, lorsque les utilisateurs du système se connectent à FTP, ils démarrent dans leur *à la maison* répertoires où ils peuvent télécharger, télécharger, créer des répertoires, etc.

De même, par défaut, les utilisateurs anonymes ne sont pas autorisés à télécharger des fichiers sur le serveur FTP. Pour modifier ce paramètre, vous devez décommenter

la ligne suivante et redémarrer vsftpd:

```
anon_upload_enable=YES
```

> **Avertissement**
>
> L'activation du téléchargement FTP anonyme peut être un risque de sécurité extrême. Il est préférable de ne pas activer le téléchargement anonyme sur des serveurs accessibles directement depuis Internet.

Le fichier de configuration se compose de nombreux paramètres de configuration. Les informations sur chaque paramètre sont disponibles dans le fichier de configuration. Alternativement, vous pouvez vous référer à la page de manuel, `man 5 vsftpd.conf` pour les détails de chaque paramètre.

Sécurisation FTP

Il y a des options dans `/etc/vsftpd.conf` pour aider à rendre vsftpd plus sécurisé. Par exemple, les utilisateurs peuvent être limités à leurs répertoires personnels en ne se compatissant pas:

```
chroot_local_user=YES
```

Vous pouvez également limiter une liste spécifique d'utilisateurs à leurs répertoires personnels:

```
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd.chroot_list
```

Après avoir décommenté les options ci-dessus, créez un `/etc/vsftpd.chroot_list` contenant une liste d'utilisateurs un par ligne. Redémarrez ensuite vsftpd:

```
sudo systemctl restart vsftpd.service
```

Aussi, le `/etc/ftpusers` fichier est une liste d'utilisateurs qui sont *refusé* Accès FTP. La liste par défaut comprend root, daemon, noon, etc. Pour désactiver l'accès FTP pour d'autres utilisateurs, ajoutez-les simplement à la liste.

FTP peut également être crypté à l'aide *FTPS*. Différent de *SFTP*, *FTPS* est FTP sur Secure Socket Layer (SSL). *SFTP* est une session de type FTP sur un crypté *SSH* connexion. Une différence majeure est que les utilisateurs de SFTP doivent avoir un *coquille* compte sur le système, au lieu d'un *nologine* coquille. Fournir à tous les utilisateurs un shell peut ne pas être idéal pour certains environnements, tels qu'un

hôte Web partagé. Cependant, il est possible de restreindre ces comptes au SFTP uniquement et de désactiver l'interaction shell.

Pour configurer *FTPS*, modifier `/etc/vsftpd.conf` et en bas ajouter:

```
ssl_enable=YES
```

Notez également le certificat et les options clés:

```
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
```

Par défaut, ces options sont définies sur le certificat et la clé fournis par le package ssl-cert. Dans un environnement de production, ceux-ci doivent être remplacés par un certificat et une clé générés pour l'hôte spécifique. Pour plus d'informations sur les certificats, voir **Sécurité - Certificats**.

Maintenant, redémarrez vsftpd et les utilisateurs non anonymes seront obligés d'utiliser *FTPS*:

```
sudo systemctl restart vsftpd.service
```

Pour permettre aux utilisateurs avec un shell de `/usr/sbin/nologin` accès à FTP, mais sans accès shell, modifier `/etc/shells` ajoutant le *nologine* coque:

```
# /etc/shells: valid login shells
/bin/csh
/bin/sh
/usr/bin/es
/usr/bin/ksh
/bin/ksh
/usr/bin/rc
/usr/bin/tcsh
/bin/tcsh
/usr/bin/esh
/bin/dash
/bin/bash
/bin/rbash
/usr/bin/screen
/usr/sbin/nologin
```

Ceci est nécessaire car, par défaut, vsftpd utilise PAM pour l'authentification, et le `/etc/pam.d/vsftpd` le fichier de configuration contient:

```
auth    required        pam_shells.so
```

Le *coquillages* Le module PAM restreint l'accès aux coques répertoriées dans le `/etc/shells` fichier.

Most popular FTP clients can be configured to connect using FTPS. The lftp command line FTP client has the ability to use FTPS as well.

References

- See the vsftpd website <http://vsftpd.beasts.org/vsftpd_conf.html> for more information.

Previous Domain Name Service (DNS) Next iSCSI

Last updated 2 years ago. Help improve this document in the forum <https://discourse.ubuntu.com/t/service-ftp/11319> .