

0.1 SFTP : Transfert de fichiers sécurisé

Le sftp est une amélioration du ftp qui fonctionne au-dessus d'un tunnel ssh. Pour que ça fonctionne il faut que le PC distant ait installé sftp-server et que le PC local dispose de la commande sftp. Ce qu'il faut savoir c'est que quand vous lancez une connexion sftp, une connexion ssh est initiée sur le serveur et c'est elle qui lance sftp-server. De plus, comme sftp-server est lancé depuis ssh, aucun privilège root n'est requis. Notez également qu'en sftp, toutes les commandes habituelles de ftp sont acceptées.

0.1.1 1. Installation des logiciels nécessaires

0.1.2 1.1 Installation d'OpenSSH

Sur la machine cliente et sur la machine serveur installez SSH comme indiqué installation de SSH¹

0.1.3 1.2 Installation de rssh

rssh est un shell restreint qui s'utilise avec OpenSSH et permet de faire uniquement du scp ou du sftp.

- Les utilisateurs de Mandriva, tapez : # urpmi rssh
- Les utilisateurs de Fedora, tapez : # yum install rssh
- Les utilisateurs de Debian, tapez : # apt-get install rssh
- Pour les autres :

Téléchargez les sources² et installez-les comme suite :

```
$ tar -xzf /où_est/rssh-xxx.tar.gz
$ cd rssh-xxx/
$ ./configure --prefix=/usr --sysconfdir=/etc
$ make
$ su
# make
```

0.1.4 2. Configuration du serveur

0.1.5 2.1 Fichier de configuration

Editez le fichier /etc/shells et assurez-vous d'avoir la ligne suivante :

```
/usr/bin/rssh
```

Nettoyez votre fichier /etc/rssh.conf comme suite :

```
# cd /etc/
# mv rssh.conf rssh.conf.old
# sed /#/d rssh.conf.old > rssh.conf
```

Maintenant éditez-le avec votre éditeur favori et assurez-vous qu'il ressemble à ceci :

¹<http://www.trustonme.net/didactels/111.html>

²<http://www.pizzashack.org/rssh/>

```
logfacility = LOG_USER
allowsftp
umask = 022
```

0.1.6 2.2 Chroot de l'environnement

Cette partie concerne les personnes qui souhaitent chrooter leurs utilisateurs. Si ce n'est pas votre cas, passez au 2.3. Le chroot est une technique qui permet de déplacer la racine du système pour enfermer l'utilisateur dans un dossier. Dans notre cas ce sera "/home". L'avantage de cette technique est que toutes les actions des utilisateurs du sftp n'auront d'impact que sur cet univers clos. Mais pour que ça fonctionne il faut que tout ce dont auront besoin les utilisateurs soit accessible dans cet univers. Préparons maintenant le chroot en copiant les exécutables dont auront besoin les utilisateurs du sftp dans le dossier "/home".

```
# cd /home
# mkdir -p usr/bin
# cp /usr/bin/sftp usr/bin
# cp /usr/bin/scp usr/bin
# cp /usr/bin/rsync usr/bin
# mkdir -p usr/libexec
# cp /usr/libexec/rsync_helper usr/libexec
# cp /usr/libexec/sftp-server usr/libexec
# mkdir lib
# mkdir usr/lib
```

Les exécutables peuvent ne pas être à ces endroits chez vous, alors adaptez ! Déterminons maintenant les dépendances de sftp :

```
# ldd /usr/bin/sftp
```

Vous devrez avoir quelque chose comme ceci (il peut y avoir des variations) :

```
linux-gate.so.1 => (0xffffe000)
libresolv.so.2 => /lib/libresolv.so.2 (0x4002d000)
libcrypto.so.0 => /usr/lib/libcrypto.so.0 (0x40041000)
libutil.so.1 => /lib/libutil.so.1 (0x40140000)
libz.so.1 => /usr/lib/libz.so.1 (0x40144000)
libnsl.so.1 => /lib/libnsl.so.1 (0x40155000)
libcrypt.so.1 => /lib/libcrypt.so.1 (0x4016b000)
libc.so.6 => /lib/libc.so.6 (0x40199000)
libdl.so.2 => /lib/libdl.so.2 (0x402b7000)
/lib/ld-linux.so.2 (0x40000000)
```

Vous devez copier les dépendances qui sont dans /lib dans /home/lib et celles de /usr/lib dans /home/usr/lib en respectant l'arborescence. Un exemple :

```
# cd /home
# cp /lib/libresolv.so.2 lib/
```

Quand vous aurez fini vous devrez taper :

```
# ldd /usr/bin/rssh
# ldd /usr/libexec/rssh_chroot_helper
# ldd /usr/libexec/sftp-servers
# ldd /usr/bin/scp
```

et copier toutes les dépendances correspondantes dans /home, comme vous l'avez fait pour /usr/bin/sftp. Finissez en ajoutant la ligne :

```
chrootpath="/home"
```

à la fin du fichier /etc/rssh.conf.

0.1.7 2.3 Gestion des utilisateurs

Créez maintenant les utilisateurs autorisés à faire du sftp et autorisés à ne faire que du sftp. Pour fixer les idées, je vais créer l'utilisateur toto et lui attribuer comme dossier personnel /home/toto :

```
# adduser -home /home/toto -shell /usr/bin/rssh toto
```

Vérifier que l'utilisateur toto a bien rssh comme shell :

```
# su - toto
```

Vous devriez avoir quelque chose comme ça :

```
This account is restricted to sftp only.
```

```
If you believe this is in error, please contact your system administrator
```

0.1.8 3. Connexion au serveur sftp

Vous pouvez tester en local :

```
$ sftp toto@localhost
```

Après avoir entré le mot de passe, vous devriez obtenir ceci :

```
sftp>
```

Et tester en réseau :

```
$ sftp toto@IP_du_Serveur
```

Si vous obtenez l'invite sftp> , c'est gagné ! sinon vérifiez que vous avez bien copié toutes les dépendances dans l'environnement de chroot. Si vous ne souhaitez plus utiliser l'environnement chrooté, il suffit d'enlever la ligne :

```
chrootpath="/home"
```

du fichier /etc/rssh.conf.

0.1.9 4. Utilisation de sftp

Pour vous connecter, à un PC distant, il suffit de taper :

```
$ sftp toto@IP_du_Serveur
```

Une fois connecté :

```
- Pour uploader un fichier : sftp> put le_fichier
```

```
- Pour downloader un fichier : sftp> get le_fichier
```

Quelques commandes utiles :

- **help** : permet de lister les commandes disponibles
- **quit** : pour quitter la session en cours
- **get** : récupère un fichier présent sur le serveur FTP et le place sur votre machine
- **put** : transfère un fichier de votre disque dur vers le serveur
- **ls** : permet de lister le contenu du répertoire courant côté FTP
- **cd** : permet de se déplacer dans l'arborescence du FTP
- **pwd** : affiche le nom du répertoire courant sur le FTP
- **delete** et **rm** : effacent un fichier sur le FTP
- **mkdir** : crée un répertoire sur le FTP

Attention : Pour ceux qui ont une allergie chronique au mode console et qui frise l'embolie cérébrale quand ils entendent les mots lignes de commandes, il existe des logiciels avec GUI qui gèrent le sftp, par exemple GFTP ou LFTP alors plus d'excuses.