EL KHATIT Zouhair, L3 ASR
N° : 20072486

Projet Administration Réseaux

Thème : SFTP & SCPOnly

I- SFTP (Secure File Transfer Protocol) :

Introduction:

Le SFTP permet de transférer des fichiers par une connexion sécurisée utilisant le protocole SSH. SFTP peut effectuer les mêmes opérations que le FTP.

Du côté du client, on peut :

- Supprimer et créer des fichiers
- Envoyer et recevoir des fichiers
- Déplacer et renommer des fichiers

Du côté du serveur, on peut :

- Gérer l'espace alloué à chaque client
- Administrer les accès de chaque utilisateur sur chaque fichier ou dossier
- Ajouter, supprimer, modifier les paramètres de chaque groupe ou utilisateur.

Il est important de noter que le SFTP n'est pas une simple connexion FTP passant par un tunnel SSH : Du côté du serveur, on lance sftp-server, qui utilise OpenSSH. Du côté client on utilise un client SFTP graphique ou en ligne de commande. Dans cet article, on utilisera RSSH, un shell restreint qui va faciliter et sécuriser d'avantage l'utilisation du SFTP.

Installation des Logiciels nécessaires :

- **Sous une Machine Linux/Unix :**

Installation de OpenSSH :

OpenSSH est installé nativement sur les principales distributions Linux. Il doit être installé sur la machine cliente et serveur. Si OpenSSH n'est pas installé sur votre ordinateur, tapez les commandes suivantes (après avoir configuré la connexion internet) :

- **Sur Mandriva :** # urpmi open-ssh
- **Sur Fedora** : # yum install open-ssh
- **Sur Debian :** # apt-get install open-ssh

Installation de RSSH :

Rssh est un shell restreint qui va sécuriser et faciliter l'utilisation du SFTP. Grâce à RSSH, l'utilisateur distant pourra uniquement échanger, supprimer, modifier des fichiers : il ne pourra exécuter de commandes à distance, susceptibles d'exploiter des failles de sécurité.

- **Sur Mandriva :** # urpmi rssh
- **Sur Fedora : #** yum install rssh
- **Sur Debian :** # apt-get install rssh

Pour les autres, téléchargez les sources disponibles sur le lien : http://sourceforge.net/projects/rssh/

Pour compiler les utilisez la procédure suivante :

```
$ tar -fvzx rssh-xxx.tar.gz
$ cd rssh-xxx
$ ./configure --orefix=/usr --sysconfdir=/etc
$ make
$ su
# make install
```

Le xxx présente le N° de version.

Configuration du Serveur :

Configuration de rssh

Rssh est un shell (restreint). Il faut donc s'assurer qu'il soit présent dans le fichier /etc/shells :

```
$ cat /etc/shells
```

Si il n'est pas présent, ajouter la ligne suivante au fichier à l'aide de votre éditeur de texte favori :

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

Il faut maintenant éditer le fichier de configuration de rssh :

On déplace le fichier de configuration présent, puis on en créé un vide :

```
# mv /etc/rssh.conf /etc/rssh.conf.old
# touch /etc/rssh.conf
```

On édite le nouveau fichier /etc/rssh.conf en le remplissant comme ceci :

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

Maintenant, le shell rssh se limitera à l'utilisation du sftp.

CHROOT de la Connexion SFTP :

Cette partie s'adresse à ceux qui veulent chrooté la connexion SFTP. Pour les autres, passez directement à l'étape suivante. Le Chroot permettra ici de restreindre l'accès d'un utilisateur (pour en savoir plus, lisez l'article sur le lien : http://lea-linux.org/cached/index/Admin-admin_env-chroot.html). Par exemple, on décide de chrooter un utilisateur dans /home : cet utilisateur verra /home comme son répertoire racine, et ne pourra aller au-delà. L'inconvénient de cette manière, c'est que tout les fichiers nécessaires doivent être inclus dans le dossier chrooté.

Préparation du dossier chrooté

On télécharge le fichier mkdep, puis on lui attribue le droit d'exécution, mkdep permet de copier automatiquement un fichier donné ainsi que ses librairies dans le dossier chrooté cible :

```
./mkdep <fichier à copier> <dossier chrooté>
```

C'est parti : on copie tous les fichiers cités plus hauts :

```
$su
# ./mkdep /usr/bin/rssh /home
```

#./mkdep /usr/bin/sftp /home
#./mkdep /usr/libexec/rssh_chroot_helper /home
#./mkdep /usr/libexec/sftp-server /home
#./mkdep /usr/bin/scp /home

Il ne reste plus maintenant qu'à modifier la configuration du fichier /etc/rssh.conf en ajoutant la ligne : chrootpath="/home"

L'utilisateur sera maintenant connecté dans le répertoire /home.

Création d'un utilisateur :

Maintenant que rssh est configuré, il faut l'associer à un utilisateur. Généralement, lorsqu'on créer un nouvel utilisateur, on lui attribu le shell "bash". Ici on lui attribura le shell "rssh". Exemple : on veut créer un utilisateur "toto" restreint à l'utilisation du sftp. On utilise la commande adduser. Lorsque Shell [/bin/bash] apparait, tapez /usr/bin/rssh. N'oubliez pas de lui créer un mot de passe : *#passwd toto*

Connexion au serveur SFTP :

Maintenant que le compte "toto" est créé, essayons de nous logger avec :

```
#su toto
```

Linux vous répondra ceci :

```
This account is restricted by rssh.
Allowed commands: sftp
If you believe this is in error, please contact your system administrator.
```

C'est tout à fait normal, étant donné que rssh accepte uniquement une connexion sftp!
Essayons maintenant de nous y connecter avec le client sftp :

```
$ sftp toto@localhost
Connecting to localhost...
toto@localhost's password:
sftp>
```

Une fois connecté :

- Pour uploader un fichier : sftp> put le_fichier
- Pour downloader un fichier : sftp> get le_fichier

Quelques Options utiles :

- help : permet de lister les commandes disponibles
- pwd : affiche le nom du répertoire courant sur le FTP
- ls : permet de lister le contenu du répertoire courant côté FTP
- cd : permet de se déplacer dans l'arborescence du FTP
- mkdir : créé un répertoire sur le FTP
- delete et rm : effacent un fichier sur le FTP
- 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
- quit : pour quitter la session en cours

Remarque : Si vous avez configuré RSSH pour une connexion chrootée, vous remarquerez que l'utilisateur ne peut aller au-delà de sa "cage".

La ligne de commande étant peu maniable, il est pratique d'utiliser des clients SFTP graphiques :

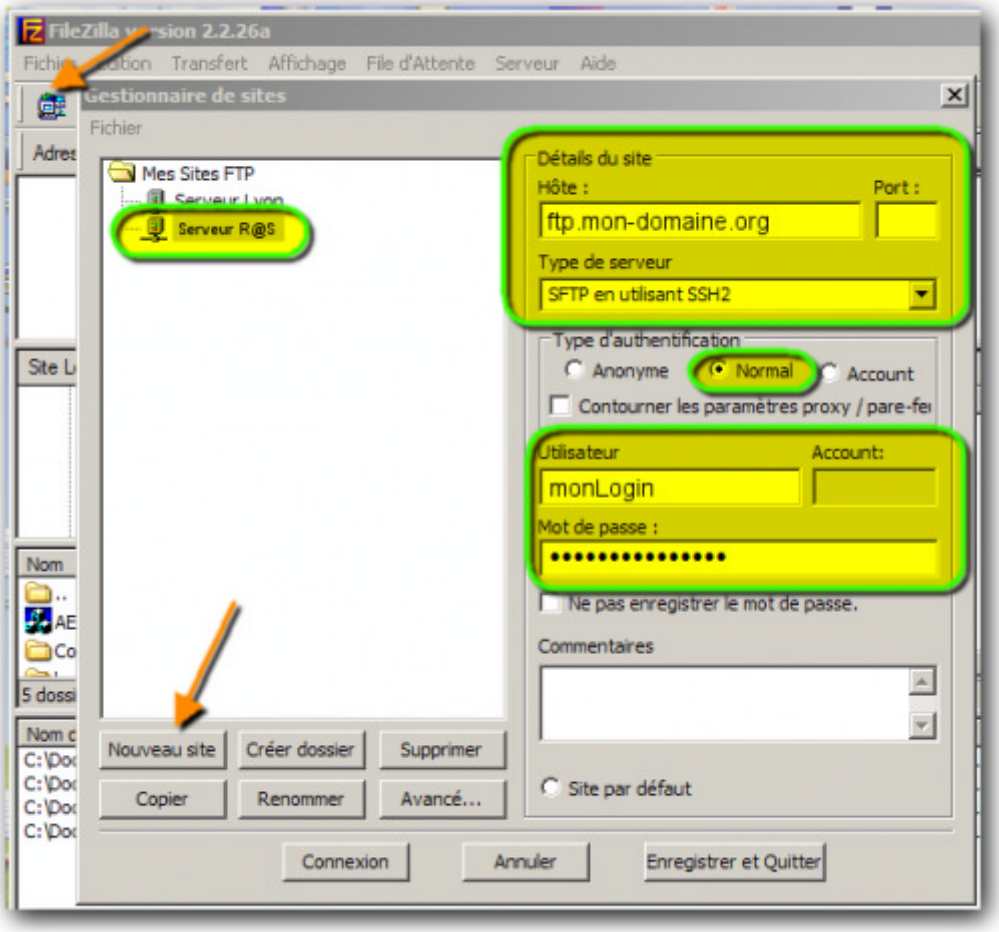
- WinSCP pour Windows (client SFTP).
- DreamWeaver sous Windows.
- Filezilla pour Windows, MAC et Linux (client FTP et SFTP).
- GFTP sous une machine LINUX.
- Cyberduck sous Mac OSX

Remarque : les clients FTP ne supportent pas le SFTP.

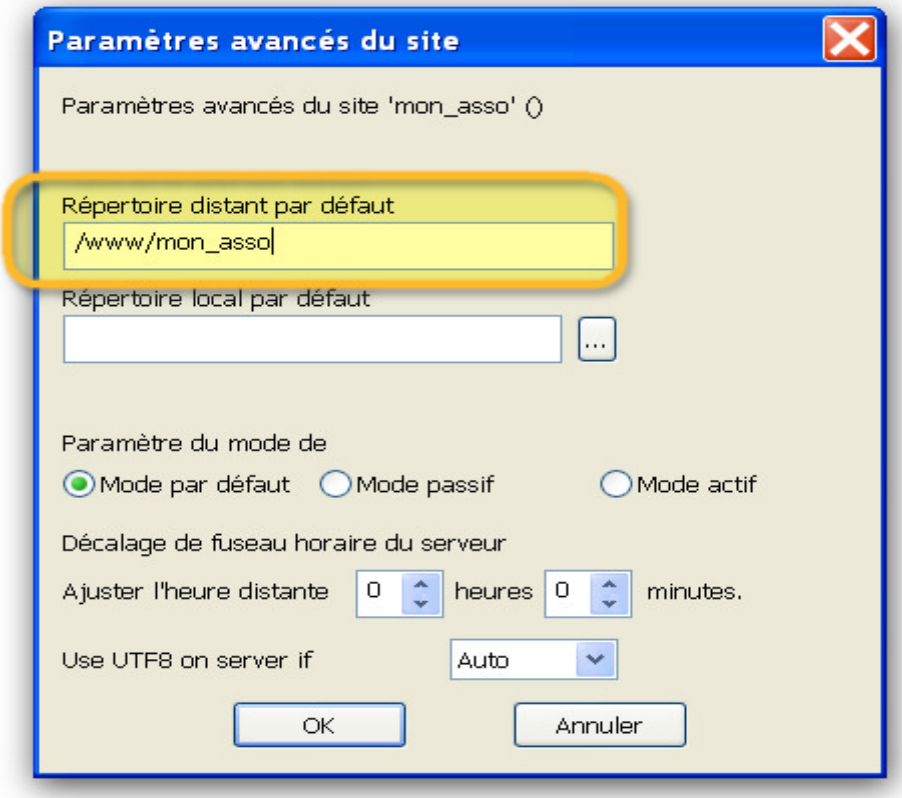
- **Sous Une Machine Windows :**
  on va voir l'installation et la config de SFTP sous Windows avec deux fameux outils : Filezilla et WinScp.

  - ***Filezilla :***
    Pour Télécharger ce logiciel, allez à cette adresse :
    http://filezilla-project.org/download.php

L'image suivante montre comment configurer Filezilla à utiliser SFTP :



allez dans le gestionnaire de sites,
- cliquez sur "Nouveau site"
- donnez lui un nom et remplissez les informations en vous inspirant du modèle ci-dessus
- cliquez sur "Avancé", et indiquez le répertoire initial (par exemple : /www/asso).

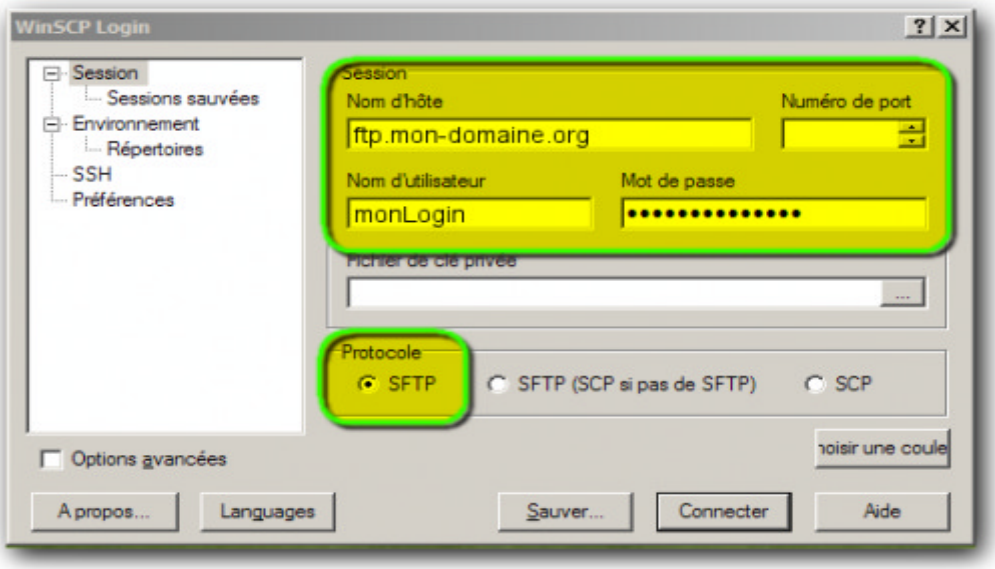


OK

- **Enregistrez**
- testez

- ***WinScp :***

- Vous pouvez télécharger Winscp à cette adresse http://winscp.net/download/winscp38... le paquet multilingue (en particulier le français)
- L'interface ressemble beaucoup à celle de WsFtp. Le paramétrage est à faire selon le modèle suivant :



Conclusion :

Le SFTP est une bonne alternative au FTP, plus sécurisée, mais aussi plus configurable : en effet, si ce tutorial nous montre uniquement comment créer un compte SFTP, les possibilités de configuration du serveur sont très importantes : Les ACL, les quotas,... permettent de moduler complètement l'accès de chaque utilisateur. Vous trouverez toutes ces possibilités dans la rubrique "Administrer" du wiki ;) .

II- SCPOnly :

Introduction:

scponly est une sorte d'interpréteur de commandes alternatif pour les administrateurs système qui désirent donner à des utilisateurs distants des accès en lecture et en écriture à des fichiers locaux, sans avoir à fournir les privilèges d'exécution distants. En fait, il restreint les commandes disponibles aux utilisateurs de Scp et Sftp. Fontionnellement, il se décrit plus comme un encapsuleur de l'application la plus sécurisée qu'est ssh.

Installation et Configuration sous Linux :

1- Installation :

- **Sous Debian :** apt-get install scponly
- **Sous Mandriva :** urmpi scponly
- **Sous Fedora :** yum install scponly

Pour les autres télécharger le package sur le lien : http://www.sublimation.org/scponly/

2- Configuration :

On positionne le *setuid bit* (ce n'est pas fait automatiquement à l'installation):

Chmod u+s /usr/sbin/scponly

C'est le moment de configurer notre cage (*jail*). Pour cela on va utiliser un script fourni par le paquet Debian. On copie ce script et on le décompresse:

Cp /usr/share/doc/scponly/setup_chroot/setup_chroot.sh.gz

gunzip setup_chroot.sh.gz

et enfin on l'exécute: *sh ./setup_chroot.sh*.

Le répertoire de dépôt sera le même pour tout le monde, alors on positionne les droits en conséquence pour que tout le monde puisse écrire: *chmod 1777 /home/scponly/incoming*. Il nous reste à créer l'entrée pour */dev/null*: mkdir /home/scponly/dev : *mknod -m 666 /home/scponly/dev/null c 1 3*

Pour transférer des utilisateurs déjà présents sur scponly, il suffit d'éditer le fichier */etc/passwd* et de définir comme répertoire maison: */home/scponly* et comme shell: */usr/sbin/scponlyc*.

Pour créer un nouvel utilisateur, il suffit d'utiliser la commande magique:

*useradd -g **gid_sshusers** -d /home/scponly -s /usr/sbin/scponlyc -c "toto ASR" toto*

Puis de lui donner un mot de passe grâce à la commande: *passwd toto*

Pour connaître l'identifiant du groupe *sshusers **(gid_sshusers)***, il suffit de jeter un coup d'oeil dans le fichier */etc/groups*. Pour supprimer un compte, il faut utiliser la commande:

deluser toto.

Remarque : Pour les utilisateurs de Windows, il faut savoir que scponly est parfaitement compatible avec WinScp.

Bibliographie

- Documentation SFTP :
- http://doc.ubuntu-fr.org/serveur/mysecureshell_sftp-server
- http://perso.univ-rennes1.fr/pascal.gentil/docs/unix/unix.reseaux.html
- Documentation SFTP et RSSH :
- http://file.trustonme.net/documentation/318.pdf
- Site Internet de scponly :
- http://www.sublimation.org/scponly
- Bulletin de sécurité Gentoo GLSA-200512-17 du 17 décembre 2005 :
- http://www.gentoo.org/security/en/glsa/glsa-200512-17.xml
- Bulletin de sécurité de FreeBSD du 22 décembre 2005 :
- http://www.vuxml.org/freebsd/index.html