Debian: Configuration serveur SFTP + chroot

Explication pour mettre en place un serveur SFTP avec chroot. Le but étant de permettre à un utilisateur de se connecter à une machine via SFTP (transfert de fichier via SSH) et qu'il ait uniquement accès à son dossier personnel qu'il lui est dédié.
Cela étant très utile dans le cas d'un serveur Web, où l'ont veut donner uniquement accès au dossier web à un utilisateur, sans qu'il puisse accéder au reste du système.
Dans cette documentation, la configuration est pour debian, mais elle fonctionne sur d'autres distributions.

Pré-requis

Il faut s'assurer que le serveur SSH est installé (la plupart du temps il est déjà installé):

```
apt installe openssh-{client,server} openssh-sftp-server
```

Configuration et mise en place

Dans un premier temps, on va créer notre arborescence. Notre utilisateur s'appellera **luc** et son dossier home sera dans `/var/sftp/luc`

Création dossier /var/sftp, et affectations droits à root:

```
mkdir /var/sftp
chown root:root /var/sftp
chmod 755  /var/sftp
```

On créer le groupe sftpusers:

```
groupadd sftpusers
```

Création utilisateur sftp (luc), son dossier HOME dans /var/sftp, et sans shell "nologin":

```
useradd -g sftpusers -m -d /var/sftp/luc -s /sbin/nologin luc
```

Il faut lui définir un mot de passe:

```
passwd luc
```

On met les droits root sur son dossier home, sinon le chroot ne fonctionnera pas:

```
chown root:root /var/sftp/luc
```

Notre utilisateur ne pourra pas créer de fichiers et dossier dans son home, car les droits sont assignés à root. On va donc créer un sous dossier, où il aura tous les droits:

```
mkdir /var/sftp/luc/data
chown -R luc:sftpusers /var/sftp/luc/data
```

Configuration service sshd

Nous allons créer une règles dans notre service SSH, afin que les utilisateurs du groupe **sftpusers** puissent seulement se connecter en sftp sur notre machine, et qu'ils aient uniquement accès à leur dossier, via chroot

Sur debian, on va créer un fichier `sftp_users.conf` dans `/etc/ssh/sshd_config.d/`:

```
Match group sftpusers
ChrootDirectory /var/sftp/%u
X11Forwarding no
AllowTcpForwarding no
Forcecommand internal-sftp
```

On redémarre le service, pour prise en compte:

```
systemctl restart ssh
```

Test connexion:

```
sftp luc@IP_MACHINE
```

Si c'est OK, après saisie du mot de passe:

```
Connected to localhost.
sftp> ls
data
```

On peut aussi utiliser un client graphique (winscp, filezilla, nautilus...) pour se connecter.

Liens

lt.fr - Installer et configurer un serveur SFTP

how-to-set-up-sftp-chroot-jail

Revision #2
Created 5 May 2025 13:41:27 by Lauris_Adm

Updated 20 May 2025 08:34:09 by Lauris_Adm