

Découvrir et configurer le protocole SFTP avec MySecureShell

Par jtraulle



www.openclassrooms.com

Sommaire

Sommaire	2
Découvrir et configurer le protocole SFTP avec MySecureShell	3
Pourquoi déployer cette solution ?	3
Dans quels cas pouvez vous déployer cette solution et quels sont ses avantages ?	3
Prérequis et Objectifs	4
Permettre l'accès en SSH	4
Installation et paramétrage de MySecureShell	5
Installation de MySecureShell	5
Ajouter un utilisateur	6
Modifier le shell de cet utilisateur	6
Configurer MySecureShell pour l'utilisateur	6
Partager	7



Découvrir et configurer le protocole SFTP avec MySecureShell

Par



jtraulle

Mise à jour : 28/08/2012

Difficulté : Facile 



Bonjour à tous !

Dans ce tutoriel, je vous proposerai tout d'abord une introduction au protocole SFTP puis je vous expliquerai comment restreindre l'accès d'un utilisateur à son seul dossier `/home/user` à l'aide de l'excellent MySecureShell.

Sommaire du tutoriel :



- [Pourquoi déployer cette solution ?](#)
- [Prérequis et Objectifs](#)
- [Permettre l'accès en SSH](#)
- [Installation et paramétrage de MySecureShell](#)

Pourquoi déployer cette solution ?

Dans quels cas pouvez vous déployer cette solution et quels sont ses avantages ?

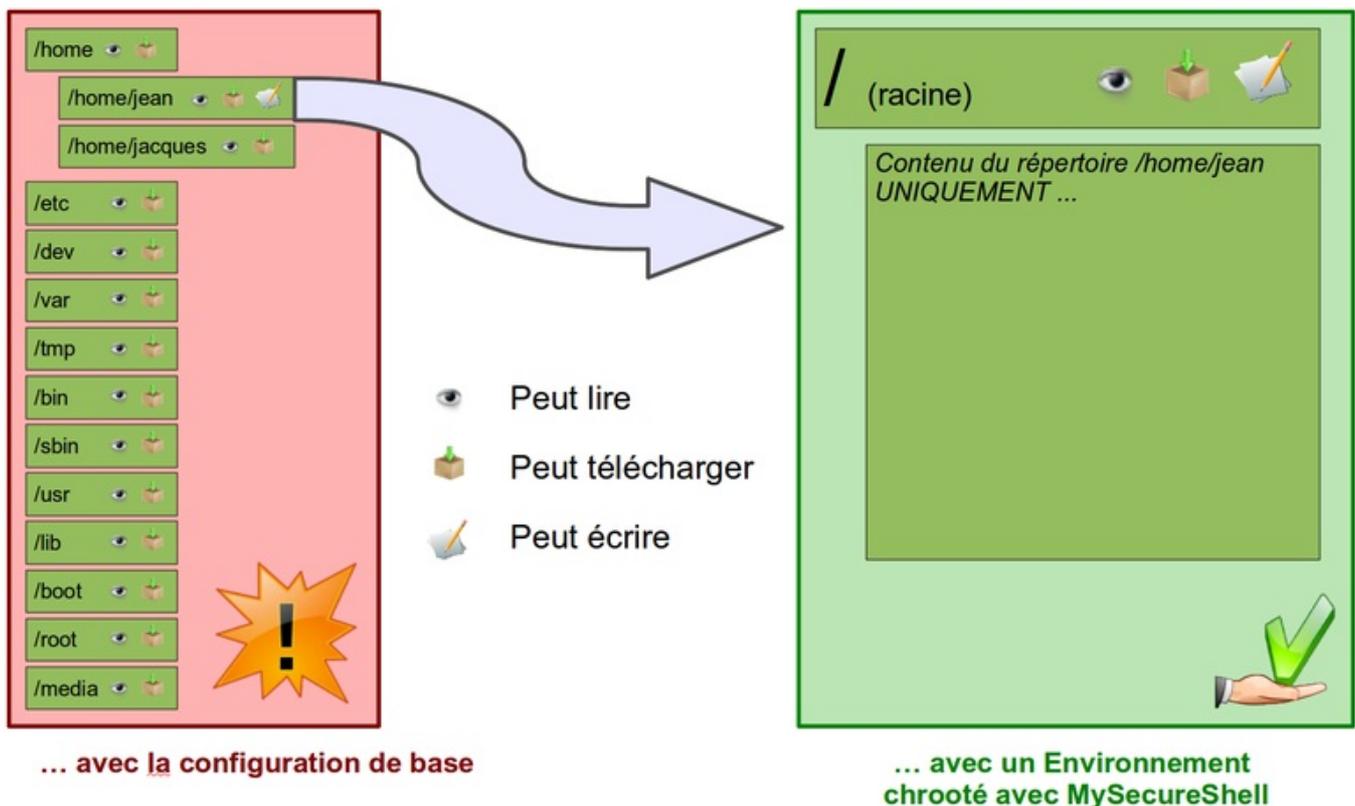
Tout d'abord, je dois dire que ce tutoriel s'adresse avant tout aux personnes disposant d'un serveur dédié sous GNU/Linux. C'est à dire une machine (un PC de bureau fait très bien l'affaire) allumée en permanence et faisant office de serveur familial avec une distribution GNU/Linux installée dessus. Sur cette machine vous pouvez installer tout un tas de logiciels permettant d'améliorer la convergence numérique de la maison. Ainsi si vous avez plusieurs PC à la maison, vous pouvez stocker vos documents uniquement sur cette machine dédiée par exemple.

Ensuite, vous pouvez avoir envie de partager vos fichiers avec de la famille (photos des petits enfants pour les grands parents) par exemple mais vous pouvez souhaiter qu'ils n'accèdent qu'à une certaine partie du disque dur.

Il faut donc restreindre l'utilisateur à un dossier donné du système. A la connexion ce sera ce dossier d'affiché par défaut et il n'aura pas la possibilité de remonter à la racine du système ...

MySecureShell permet de faire ceci et nous allons voir ensemble comment mettre en place cette solution. Maintenant, prenons un exemple pour que cela soit plus concret ...

Lors de la connexion de l'utilisateur jean ...



Avec la configuration de base, jean a accès à tout le système en lecture ! Il lui est de même possible de télécharger tous les fichiers du système !

Lorsque jean se connectera, seul son répertoire home sera accessible. Il n'aura pas la possibilité de remonter dans l'arborescence car la racine contiendra uniquement son home.

Prérequis et Objectifs



Tout d'abord, avant de commencer, vous devez maîtriser quelques notions. Voici les compétences requises avant la lecture de ce tutoriel :

- Posséder un serveur avec une distribution linux installée (pour le tuto, je prendrai comme référence une Debian Lenny)
- Avoir des connaissances minimales au niveau des systèmes GNU/Linux, notamment utiliser l'éditeur de fichiers GNU nano.
Si vous n'avez pas les bases, je vous recommande la lecture de ce chapitre du tutoriel [Reprennez le contrôle avec Linux !](#) de M@teo21 : Nano, l'éditeur de texte du débutant.



A la fin de ce tutoriel, vous devriez être capable :

- d'ajouter des utilisateurs pour faire du SFTP
- de modifier le shell d'un utilisateur
- de configurer MySecureShell pour un utilisateur
- d'accéder à distance à un dossier du système de fichier et uniquement à ce dossier en utilisant le protocole de transfert SFTP

Permettre l'accès en SSH

SFTP est un protocole de transfert sécurisé par SSH. Il permet de transférer des fichiers tout en bénéficiant des avantages de SSH (cryptage de tous les échanges).

Le protocole SFTP et SSH sont intimement liés puisque SFTP veut en réalité dire SSH File Transfert Protocole. SFTP n'est qu'en réalité une surcouche à SSH. L'installation de SSH est donc requise pour pouvoir accéder à son serveur via le protocole SFTP.

Après avoir réalisé une installation toute fraîche de Debian Lenny, par défaut, il n'est pas possible de se connecter à distance via le protocole SSH. Nous allons donc installer SSH.

Code : Console

```
aptitude install ssh
```

A partir de là, tous les utilisateurs du système Debian Lenny peuvent se connecter en SSH et en SFTP au serveur. Ils peuvent de même, remonter à la racine et voir tout les fichiers du système. En revanche, ils ne peuvent pas modifier les fichiers ne leur appartenant pas (la gestion des droits GNU/Linux reste active).

Cela pose cependant de graves problèmes car même s'ils ne pourront pas modifier les fichiers ne leur appartenant pas, ces utilisateurs pourront télécharger tout les fichiers du système et donc les lire par la suite.

Nous allons donc voir maintenant comment restreindre l'utilisateur à son dossier contenu dans le /home (technique du chroot).

Installation et paramétrage de MySecureShell

Citation

MySecureShell est un shell qui va permettre d'ajouter plusieurs fonctionnalités à sftp-server et qui va se rapprocher des grands serveurs ftp tel que ProFtpd.

Les avantages de MySecureShell sont qu'il s'appuie sur le protocole très sécurisé appelé SSH et qu'il permet un cryptage complet des données et des requêtes émises. Il est très simple à installer, à utiliser et hautement configurable.

Voilà comment est décrit MySecureShell sur [son site officiel](#).

Le gros avantage pour nous, c'est qu'il va nous permettre de restreindre l'utilisateur à son dossier personnel.

Installation de MySecureShell

Je vais maintenant détailler la procédure d'installation de MySecureShell

Modifier le fichier sources.list

Comme la dernière version de MySecureShell n'est pas forcément dans les dépôts, on ajoute une source externe. Commencez par éditer le fichier sources.list :

Code : Console

```
nano /etc/sources.list
```

A la fin du fichier, ajoutez :

Code : Autre

```
deb http://mysecureshell.free.fr/repository/index.php/debian testing main  
deb-  
src http://mysecureshell.free.fr/repository/index.php/debian testing main
```

Puis, fermez nano en tapant Ctrl+X, O et Entrer.

Recharger la liste des paquets

Comme nous venons d'ajouter un dépôt, nous devons actualiser la liste des paquets. Pour cela, tapez

Code : Console

```
aptitude update
```

Installer MySecureShell

Nous pouvons maintenant installer MySecureShell :

Code : Console

```
aptitude install mysecureshell
```

Ajouter un utilisateur

Pour l'exemple, mon utilisateur s'appellera joyre

Code : Console

```
adduser joyre
```

Modifier le shell de cet utilisateur

Pour que l'utilisateur, utilise par défaut MySecureShell lors de sa connection, nous allons devoir modifier le fichier `/etc/passwd` avec nano.

Code : Console

```
nano /etc/passwd
```

Dans le fichier `/etc/passwd`, vous allez retrouver toujours le même schéma pour tous les utilisateurs :

Citation : /etc/passwd

```
noutilisateur:x:guidutilisateur:guidgroupe::/home/utilisateur:shellutilise
```

Identifiez l'utilisateur dont vous voulez restreindre l'accès à son dossier. Son pseudo débute la ligne à modifier. Une fois que vous avez trouvé, remplacez `/bin/bash` par `/bin/MySecureShell`.

Si je prend un exemple : je veux restreindre l'utilisateur joyre

- j'avais avant `joyre:x:1000:1000::/home/joyre:/bin/bash`
- je le remplace par `joyre:x:1000:1000::/home/joyre:/bin/MySecureShell`

Maintenant que la ligne est modifié, nous pouvons enregistrer et fermer nano (Ctrl+X, O et Entrer)

Configurer MySecureShell pour l'utilisateur

Pour le moment, l'utilisateur est forcé d'utiliser MySecureShell mais celui ci n'est pas configuré. Il ne peut donc rien faire. Nous allons donc devoir paramétrer MySecureShell pour l'utilisateur en modifiant le fichier `/etc/ssh/sftp_config` avec nano.

Code : Console

```
nano /etc/ssh/sftp_config
```

Vous allez maintenant copier/coller le code suivant dans votre fichier `/etc/ssh/sftp_config` (qui est normalement vide).

Code : Autre

```
<User pseudoarestreindre>
Home /home/pseudoarestreindre
StayAtHome true
VirtualChroot true
LimitConnectionByUser 3
LimitConnectionByIP 3
HideNoAccess true
DefaultRights 0604 0705
IgnoreHidden true
</User>
```

Il vous faudra remplacer dans ce code `pseudoarestreindre` par le pseudo dont vous souhaitez restreindre l'accès.

Je vais maintenant expliquer les arguments contenus dans ce code :

- `<User pseudoarestreindre> [...] </User>` : La directive `User` est destinée à affecter des directives à une seule personne. L'utilisateur doit être créé sur la machine pour qu'il fonctionne sur MySecureShell (ce que nous avons fait précédemment)
- `Home` : C'est le dossier où seront redirigés les utilisateurs lors de la connexion au serveur.
- `StayAtHome` : L'utilisateur connecté ne peut remonter au dessus du dossier `Home` qui lui a été attribué.
- `VirtualChroot` : Chroot l'utilisateur authentifié, `"/` s'affichera pour lui comme le répertoire par défaut.
- `LimitConnectionByUser` : Limite le nombre de connexions simultanées par utilisateurs.
- `LimitConnectionByIP` : Limite le nombre de connexions simultanées par IP.
- `HideNoAccess` : Cache les fichiers/répertoires auxquels l'utilisateur, le groupe ou autre, n'ont pas accès.
- `DefaultRights` : Définit les droits pour les fichiers et les répertoires créés par l'utilisateur.
- `IgnoreHidden` : Masque les fichiers cachés à l'utilisateur (cette option peut être intéressante mais pensez à la désactiver si vous manipulez des fichiers `.htaccess` par exemple).

Voilà, ce tutoriel est désormais terminé, j'espère qu'il vous aura été utile dans la mise en place de l'accès SFTP de votre serveur.

Je vous rappelle que ce tutoriel est publié sous licence **Creative Commons Paternité 2.0 France**.

Dans le cadre de cette licence, vous avez le droit (et je vous encourage vivement à l'exercer) de reproduire, distribuer et communiquer cette création au public et de la modifier.

En contrepartie, vous devez citer le nom de l'auteur original (jtraulle, <http://facilinux.fr>) (mais pas d'une manière qui suggérerait que je vous soutiens ou que j'approuve votre utilisation de ce tutoriel).

Partager

