

ssh : logiciel permettant l'authentification sécurisée à un shell distant

YuGiOhJCJ

14 juin 2008

Table des matières

1	Avant propos...	2
2	Les exécutable	2
3	L'authentification par mot de passe	2
4	L'authentification par clé publique	2
5	L'utilisation de l'agent SSH	3
6	L'exécution de commandes	3
7	La copie de fichiers	3
8	Du FTP par SSH	4

1 Avant propos...

Cette documentation a été rédigée par YuGiOhJCJ. Vous lisez actuellement la version 20080614 qui est gratuite. Si vous souhaitez utiliser une partie de cette documentation pour vos créations, veuillez d'abord me contacter à yugiohjcj@free.fr. La version la plus récente de ce document est disponible à l'adresse <http://yugiohjcj.free.fr/>. Cette publication peut contenir certaines erreurs. N'hésitez pas à me les rapporter pour que j'effectue une correction.

La première version du document date du 11/11/2007. Voici les différentes mises à jours qui ont été apportées au document :

- 14/06/2008 - Correction du nom de fichier de la clé publique. Le fichier est nommé *id_rsa.pub* et pas *id_rsa* qui correspond plutôt à la clé privée.

2 Les exécutables

- ssh - Le client SSH
- scp - Le client pour la copie de fichiers par SSH
- sftp - Le client permettant de faire du FTP via SSH
- ssh-keygen - L'utilitaire permettant de générer les clés
- ssh-agent - L'utilitaire permettant d'éviter d'entrer sa passphrase
- ssh-add - L'utilitaire permettant d'ajouter une clé privée à SSH Agent
- sshd - Le serveur SSH

3 L'authentification par mot de passe

Pour vous authentifier par mot de passe à un serveur SSH, tapez cette commande :

```
ssh utilisateur@serveur
```

4 L'authentification par clé publique

Il est possible de s'authentifier par clé publique. Cela donne un premier avantage de sécurité : ne pas faire circuler sur le réseau votre mot de passe UNIX. De plus, en passant par le SSH Agent, plus besoin d'entrer de passphrase pour s'authentifier. Sur le client, vous devez créer vos clés :

```
ssh-keygen
```

Une passphrase vous sera demandée. Sur le serveur, vous devez copier la clé publique dans le fichier `/.ssh/authorized_keys` :

```
cat id_rsa.pub >> ~/.ssh/authorized_keys
```

Le serveur doit avoir activé l'authentification par clé publique sur le serveur :

```
/etc/ssh/sshd_config
```

```
PubkeyAuthentication yes
AuthorizedKeysFile      .ssh/authorized_keys
```

Ne pas oublier de relancer le serveur SSH après modification de ce fichier. Maintenant, l'authentification se fait ainsi :

```
ssh utilisateur@serveur
```

Votre passphrase vous sera demandée.

5 L'utilisation de l'agent SSH

Lors d'une connexion par clé publique à un serveur SSH, il vous est demandé la passphrase. Pour éviter qu'elle ne vous soit demandée à chaque authentification, vous devez utiliser l'Agent SSH :

```
ssh-agent
eval `ssh-agent`
ssh-add ~/.ssh/id_rsa
```

Essayez maintenant de vous authentifier à la machine distante :

```
ssh utilisateur@serveur
```

La passphrase ne vous est plus demandée. Aussi, sur le client, vous avez la possibilité d'utiliser l'option :

```
/etc/ssh/ssh_config
```

```
ForwardAgent yes
```

Avec cette configuration, vous pourrez effectuer plusieurs authentifications SSH sur une connexion SSH existante sans que l'on vous demande d'entrer de passphrase.

6 L'exécution de commandes

Il est possible d'exécuter une commande sur l'ordinateur distant :

```
ssh utilisateur@serveur ls /
```

7 La copie de fichiers

Vous pouvez utiliser scp, pour copier des fichiers via SSH :

```
scp utilisateur@serveur:~/fichier.txt ~/
```

8 Du FTP par SSH

Vous pouvez utiliser sftp, pour faire du FTP via SSH :

```
sftp utilisateur@serveur
```