



Connexion SSH via clef RSA & ssh-keygen

>>> Client Linux Debian

Description :

Dans ce cours nous allons apprendre à installer SSH et à le configurer pour qu'il utilise des clefs RSA à la place des mots de passe.

Connexion SSH via clef RSA & ssh-keygen

>>> Client Linux Debian

Sommaire :

- I) Introduction
- II) Installation de SSH
 - 1) Installation et configuration de SSH
 - 2) Création de l'utilisateur
 - 3) Création des clefs RSA
 - 4) Copie de la clef publique sur le serveur
 - 5) Redémarrage du service SSH
- III) Test de connexion

I) Introduction

L'utilisation de clef RSA vous permet d'augmenter la sécurité au niveau de l'administration à distance de vos serveurs.

Avant de commencer, voici quelques informations concernant ma maquette :

- Adresse IP du serveur : 172.16.1.35
- Adresse IP du client : 172.16.1.34
- OS Debian 8.6

II) Installation de SSH

1) Installation et configuration de SSH

- Commencez par installer "SSH" :

```
aptitude -y install ssh
```

- Une fois installé ouvrez votre éditeur préféré (pour moi VIM) et éditez le fichier "/etc/ssh/sshd_config" :

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

- Modifiez la ligne ci-dessous :

```
AuthorizedKeysFile %h/.ssh/authorized_keys
```

Enregistrez et quittez mais ne redémarrez pas votre serveur, ni le service SSH.

2) Création de l'utilisateur

Nous allons créer un nouvel utilisateur sur le serveur ET sur le client.

- Sur le serveur :

```
root@serveur:~# adduser vthymme
Ajout de l'utilisateur « vthymme »...
Ajout du nouveau groupe « vthymme » (1001)...
Ajout du nouvel utilisateur « vthymme » (1001) avec le groupe « vthymme »...
Création du répertoire personnel « /home/vthymme »...
Copie des fichiers depuis « /etc/skel »...
Entrez le nouveau mot de passe UNIX :
Retapez le nouveau mot de passe UNIX :
passwd : le mot de passe a été mis à jour avec succès
Modification des informations relatives à l'utilisateur vthymme
Entrez la nouvelle valeur ou « Entrée » pour conserver la valeur proposée
Nom complet []: Vincent thymme
N° de bureau []:
Téléphone professionnel []:
Téléphone personnel []:
Autre []:
Ces informations sont-elles correctes ? [0/n]
```

- Sur le client :

```
root@client:~# adduser vthymme
Ajout de l'utilisateur « vthymme »...
Ajout du nouveau groupe « vthymme » (1001)...
Ajout du nouvel utilisateur « vthymme » (1001) avec le groupe « vthymme »...
Création du répertoire personnel « /home/vthymme »...
Copie des fichiers depuis « /etc/skel »...
Entrez le nouveau mot de passe UNIX :
Retapez le nouveau mot de passe UNIX :
passwd : le mot de passe a été mis à jour avec succès
Modification des informations relatives à l'utilisateur vthymme
Entrez la nouvelle valeur ou « Entrée » pour conserver la valeur proposée
Nom complet []: Vincent thymme
N° de bureau []:
Téléphone professionnel []:
Téléphone personnel []:
Autre []:
Ces informations sont-elles correctes ? [0/n]
```

3) Création des clefs RSA

- Sur votre client Debian, connectez-vous avec l'utilisateur "**vthymme**".
- Ouvrez un terminal
- Tapez la commande suivante pour générer les clefs publique et privé :

```
ssh-keygen
```

- Vous devez obtenir ceci :

```
Generating public/private rsa key pair.
Enter file in which to save the key (/home/vthymme/.ssh/id_rsa):
Created directory '/home/vthymme/.ssh'.
Enter passphrase (empty for no passphrase):
```

```
Enter same passphrase again:
Your identification has been saved in /home/vthymme/.ssh/id_rsa.
Your public key has been saved in /home/vthymme/.ssh/id_rsa.pub.
The key fingerprint is:
da:85:b3:30:51:be:3b:c1:21:0f:4f:ea:1b:af:2c:a7 vthymme@debian
The key's randomart image is:
+---[RSA 2048]-----+
| . |
| o |
| ++ |
| X + |
| + S . |
| . = * |
| + = |
| ...+ . |
| E+... |
+-----+
```

4) Copie de la clef publique sur le serveur

Vous devez maintenant copier la clef publique sur le serveur.

- Depuis le terminal du client, tapez la commande suivante :

```
ssh-copy-id vthymme@172.16.1.35
```

- Vous devez obtenir ceci :

```
The authenticity of host '172.16.1.35 (172.16.1.35)' can't be established.
ECDSA key fingerprint is ea:df:62:5b:11:8f:c6:60:aa:10:99:0f:b9:4f:94:1d.
Are you sure you want to continue connecting (yes/no)? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are
already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to
install the new keys
vthymme@172.16.1.35's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'vthymme@172.16.1.35'"
and check to make sure that only the key(s) you wanted were added.
```

- On vous demande si vous voulez vous connecter. Répondez **"Yes"**.
- On vous demande ensuite le mot de passe du compte vthymme (sur le serveur).

5) Redémarrage du service SSH

- Retournez sur le serveur pour redémarrer le service "SSH" :

```
service ssh restart
```

III) Test de connexion

- Sur le serveur, tapez la commande suivante pour vérifier la présence de la clef publique du compte vthymme :

```
cat /home/vthymme/.ssh/authorized_keys
```

- Vous devez obtenir ceci :

```
ssh-rsa  
AAAAB3NzaC1yc2EAAAADAQABAAQ=CpzbbLein0t0h6kABo5gFoJH0CC69Xqw9kgucQjk8GtmkryKnrruwpHtc+5jzPHfKM2d  
PH90AfmqJ0geWLEbzGSTVIB50QHATJ+rEdFkZ4G9XE9c+V0F7ga/r9hRgLnSuKKp9m2719Dd+95gwRUwQKAGgypGab+TYoY1/  
TSsiQeCGmkN8C3VPNUb3y5cCgeBfwnyiHA9LrY3yNmfvGAq+RJGaCIQRAw9ABAIRZdPcg2zuhL11gfDVhFhJUbwra3iBR9BskL  
/5TG5UGzpwrfJqI9AfQ+k9y7aSQbbzz5F80RZj5qHC+JhvTMIuB+6WiWyhEX5Tm7wsVwpEo7bfSuSx vthymme@debia
```

- Sur le client, tapez la commande suivante pour vous connecter en SSH. Si vous avez bien suivi la procédure, vous devriez être connecté sans avoir tapé de mot de passe.

```
ssh vthymme@172.16.1.35
```

22 mai 2017 -- N.Salmon -- article_325.pdf



Idum