

Comment configurer des clés SSH sur un système Linux



Si vous voulez exporter des fichiers en SCP, vous avez la fainéantise de saisir le mot de passe d'une machine Linux ou que vous souhaitez sécurisé plus l'authentification SSH voici comment générer un certificat RSA pour vous simplifiez la vie.

Avant tous, vérifié dans le fichier de configuration `/etc/ssh/sshd_config` de SSH que ces options sont comme suite :

```
RSAAuthentication yes
PubkeyAuthentication yes
AuthorizedKeysFile      %h/.ssh/authorized_keys
```

Génération du certificat RSA

La commande `ssh-keygen` permet de générer notre certificat

```
ssh-keygen -t rsa
```



Si vous ne voulez pas de passphrase, mais que vous voulez un certificat RSA saisir la touche <entrée>

passphrase

Si vous avez mis une passphrase, les étapes en dessous vous permettrons d'éviter de ressaisir celle-ci.



les étapes en dessous sont à répéter à chaque que fois que vous vous loguez

```
ssh-agent $SHELL
ssh-add #attention demande de la passphrase
```

export du certificat (ssh-copy-id)

```
ssh-copy-id -i ~/.ssh/id_rsa.pud <usr>@<IP>
```

L'export du certificat "id_rsa.pud" vers la machine <IP>, il sera mis dans le répertoire home du login <usr>, un nouveau répertoire `.ssh` sera créé (s'il n'existe pas déjà), dedans un fichier `authorized_keys` sera créé (s'il n'existe pas déjà).

export du certificat manuel

Pour la méthode manuel, il faut d'abord exporter le certificat vers notre machine <IP>.

```
scp /home/<usr>/.ssh/id_rsa.pub <usr>@<IP>:/home/<usr>/.ssh/
```

Connectez vous sur la machine <IP> et changer le nom du fichier

```
mv /home/<usr>/.ssh/id_rsa.pub /home/<usr>/.ssh/authorized_keys  
chown <usr>:<usr> /home/<usr>/.ssh/authorized_keys
```

Si le repertoire .ssh n'existe pas sur la machine <IP> distante:

```
scp /home/<usr>/.ssh/id_rsa.pub <usr>@<IP>:/home/<usr>/
```

Connectez vous sur la machine <IP> avec le login <usr>:

```
mv /home/<usr>/id_rsa.pub /home/<usr>/authorized_keys  
mkdir /home/<usr>/.ssh  
chown <usr>:<usr> /home/<usr>/.ssh  
mv /home/<usr>/id_rsa.pub /home/<usr>/.ssh/authorized_keys  
chown <usr>:<usr> /home/<usr>/.ssh/authorized_keys
```

From:

<https://www.ksh-linux.info/> - **Know Sharing**

Permanent link:

<https://www.ksh-linux.info/systeme/certificat-rsa-sur-un-serveur-openssh>

Last update: **12/11/2016 20:00**

