

SUPPRIMER UNE ENTREE SSH DANS LE FICHIER « KNOWN_HOSTS »

En vous connectant en SSH à une machine (serveur Debian par exemple) que vous venez de réinstaller, vous risquez d'avoir le message suivant sur le poste client :

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@  WARNING : REMOTE HOST IDENTIFICATION HAS CHANGED !  @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY !
Someone could be eavesdropping on you right now (man-in-the-middle attack) !
It is also possible that a host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
f6:fe:f0:1c:4c:25:96:f9:08:8f:97:02:60:90:38:8e
Please contact your system administrator.
Add correct host key in /Users/prof/.ssh/known_hosts to get rid of this message.
Offending RSA key in /Users/prof/.ssh/known_hosts:9
RSA host key for 192.168.1.20 has changed and you have requested strict checking.
Host key verification failed.
```

Ce problème vient du fait que la clé a été modifiée sur le serveur sur lequel vous voulez accéder en SSH.

Vous devez exécuter la commande ci-dessous pour supprimer l'ancienne clé du fichier « known_hosts » :

- Ouvrez l'invite de commande en mode administrateur sur l'ordinateur depuis lequel vous voulez lancer SSH
- Saisissez la commande suivante :

ssh-keygen -R ip_du_serveur (ou nom du serveur)