

## SSH

SSH est installé sur toutes les machines. Il permet de se connecter sur la machine de manière sécurisée et avoir un contrôle total de celle-ci.

### Clients ssh

- sous windows :

Putty (gratuit) <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>. Pour en savoir plus, consultez Utilisation de Putty.

SecureCRT (payant) <http://www.vandyke.com/products/securecrt/>.

- sous mac :

<http://directory.google.com/Top/Computers/Internet/Protocols/SSH/Clients/Macintosh/>  
Terminal est livré avec Mac OS X, il est toujours installé systématiquement sur le disque.

[http://pro.wanadoo.fr/chombier/MacSSH/SSH\\_info.html](http://pro.wanadoo.fr/chombier/MacSSH/SSH_info.html)

<http://sourceforge.net/projects/macssh/>.

- sous linux :

openssh (gratuit) <http://www.openssh.org>.

### Première connexion

Pour se connecter sur la machine en ssh, il faut avoir 2 informations :

- ip de la machine (ou le nom de la machine),
- le mot de passe root de la machine.

Exemple de connexion avec openssh :

```
$ ssh root@bmw
The authenticity of host 'bmw (213.186.32.1)' can't be established.
RSA key fingerprint is a9:bb:55:35:86:4d:ca:81:7f:9e:2b:2c:79:10:96:3c.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'bmw,213.186.32.1' (RSA) to the list of known hosts.
Password:
$
```

Lors de la connexion votre client ssh reçoit **RSA key fingerprint** qui est une empreinte du serveur sur lequel vous vous connectez. Cette empreinte est vérifiée à chaque nouvelle connexion. Si elle change vous allez être informé et ça veut dire que quelque chose a changé sur la machine. Soit la machine a été réinstallée, soit le serveur ssh a été réinstallé, soit vous vous connectez sur une autre machine.

Lors de la première connexion vous devez accepter l'empreinte qui sera enregistrée sur votre poste de travail par votre client ssh.

**Ensuite alors ?**

Vous avez un petit guide sur ce qu'on peut faire en shell sous bash : Administrer la machine en ssh (shell sous bash).

**Mise à jour**

Lorsque vous mettez à jour ssh sur votre machine n'oubliez pas de redemarrer telnet. Telnet est une version non sécurisée de ssh. De plus telnet ne permet pas directement une connexion en root. Mais c'est une roue de secours. Pour savoir la version de votre ssh sur la machine il suffit de taper ssh -V.

```
# ssh -V
```

```
OpenSSH_3.7.1p2, SSH protocols 1.5/2.0, OpenSSL 0.9.6i engine Feb 19 2003
```

Les versions d'OpenSSH < à 3.7.1p2 sont hackables. Nous vous conseillons de mettre à jour votre machine si ce n'est toujours pas le cas. Voici un guide à ce propos : Tout sur les releases OVH.

Attention: à partir de la 3.7.1p2 il faut mettre l'option UsePAM à yes dans /etc/ssh/sshd\_config sinon vous ne pourrez pas vous reconnecter sur la machine. Si avec cette option votre ssh ne redemarre plus cela signifie que vous n'êtes pas en 3.7.1p2 (la mise à jour a raté).

**Les erreurs**

Si vous êtes en ssh > 3.7, vous pouvez avoir des problèmes de connexion sur votre machine avec les anciens clients ssh sous windows. Pour éviter ces problèmes il faut télécharger la dernière version de votre client ssh. Pour Putty, il faut forcer la connexion en SSH2. (Voir le guide suivant à ce sujet : Utilisation de Putty. Pour SecureCRT, il faut configurer l'authentification primaire en 'password'. Dans tous les cas le problème ne vient pas de la machine mais bien de votre client ssh.