Accés remot amb SSH

SSH (Secure Shell) és un programa de login remot que permet una transmissió segura de qualsevol tipus de dades: passwords, sessions de login, fitxers, sessions X remotes, comandes d'administració, etc.

La seva seguretat s'aconsegueix mitjançant l'ús de criptografia. Tota la comunicació és encriptada i autentificada de forma transparent per a l'usuari. Aquesta eina és molt més potent i segura que les anteriors eines de Telnet i altres basades en connexió TCP.

SSH ofereix una autentificació més robusta d'usuaris i hosts, que la tradicionalment oferida basada en adreces IP i noms de màquines.
Major privacitat per a l'usuari degut a l'ús de canals d'encriptació.
Ssh estableix un entorn protegit contra atacs típics

Instal·lació

El paquet consta d'un client i un servidor que s'instal·len al mateix temps.
Podem trobar la versió en paquets tar que caldrà instal·lar i compilar (make, make install,...) però en el cas de Red Hat, disposem de paquets RPM que només haurem d'instal·lar

A conseqüència de l'instal·lació, trobarem a */usr/local/bin* tots els clients (**ssh**, **scp**, **sftp**, **ssh-agent**, etc.) i a */usr/local/sbin* el servidor (**sshd**), amb les proteccions adecuades.

En aquesta versió de Fedora (7), podrem comprovar que tant client com servidor ja estaran instal·lats.

Configuració del servidor

A la versió SSH1 els arxius de configuració del sistema estaven a /etc.
A la versió SSH2, es troben a /etc/ssh i són:

/etc/ssh/sshd_config	Configuració del servidor
/etc/ssh/ssh_config	Configuració del client

A nivell de client, l'ordre de preferència en l'avaluació de les opcions d'arranc, és:
Opcions de línia de comandes
Opcions especificades al fitxer $HOME/.ssh/config
Opcions especificades a /etc/ssh/ssh_config.
Si la versió compilada que utilitzem inclou la llibreria wrapper, caldrà configurar també els fitxers
/etc/hosts.allow
/etc/hosts.deny

Opcions més rellevant de configuració del servidor (fitxer /etc/ssh/sshd_config)

La configuració per defecte d'aquest fitxer és acceptable. De totes formes, s'aconsella modificar les opcions PermitRootLogin i PermitEmptyPassword de forma que quedin:

```
PermitRootLogin  no
PermitEmptyPasswords no
```

D'aquesta forma no deixarem al root connectar-se via ssh ni realitzar logins que no corresponguin a un compte del sistema.

També pot ser útil configurar l'opció SyslogFacility per anar guardant-nos qui està realitzant connexions amb SSH.

També puc posar les directives:

allow users
deny users
allow groups
deny groups

que em permetran indicar els usuaris i/o grups que vull deixar treballar i els que no.

Execució del servidor

A Fedora el servidor SSH ja està activat. També es pot activar i desactivar des de l'entorn gràfic.

Podrem arrencar el servidor SSH mitjançant:

```
# Arranc del servidor ssh
/usr/local/sbin/sshd
```

o amb el seu script: /etc/rc.d/init.d/sshd start/stop/restart/status

El client SSH s'arrenca mitjançant:

```
ssh -l usuari altramaquina

slogin usuari@altramaquina
```

Autentificació per password

SSH permet autentificar a un usuari utilitzant la seva password del sistema Linux. Cal comentar que el password no viatja mai tal qual per la xarxa. Amb SSH evitarem el perill de que la nostra password sigui capturada per possibles "sniffers" a la xarxa.

Podem cridar ssh per obrir una sessió remota a una màquina (p.e. remot):

```
% ssh remot
Accepting host remot key without checking.
usuari's password:
```

També podem executar una única comanda al servidor:

```
% ssh remot pwd
Accepting host remot key without checking.
usuario's password:
/home/usuari
```

També ens ofereix la possibilitat de connectar-nos a un usuari amb un altre usuari:

```
% ssh remot -l altre_usu
        (opció més corrent)
```

Les claus de servidor

Cada servidor de SSH té associat un parell de claus, la pública i la privada. Aquestes claus s'utilitzen per identificar el servidor davant de l'usuari; d'aquesta forma s'evita que una altra màquina (possiblement hostil) pugui suplantar-lo.

En la comunicació entre client i servidor, cadascun tindrà la seva clau pública i la privada. Cadascun li envia a l'altre la clau pública i envia un missatge que codifica amb la clau privada. L'altre haurà de decodificar el missatge amb la clau pública que li va passar la màquina remota. Aquest missatge només es podrà interpretar correctament si la clau pública és la correcta. En cas contrari, es denegarà la connexió.

La clau pública rebuda del servidor es guardarà a /home/usuari/.ssh/hostkeys. Si el servidor modifica les seves claus (p.e. per una reinstal·lació del sistema operatiu), caldrà esborrar el fitxer que conté la clau del node remot (/home/.ssh/hostkeys).

Aquest procés es pot simplificar utilitzant l'agent d'autentificació (ssh-agent), que serà una eina encarregada de custodiar les meves passwords privades i donar-li al client SSH quan aquest ho necessiti. Per tant, a efectes pràctics, guanyarem haver d'entrar una única vegada la nostra password. Degut a que l'agent subministrarà la nostra password i no l'haurem d'entrar diverses vegades, caldrà assegurar-nos que ningú pugui fer-se amb la nostra sessió, ja que no necessitaria saber les passwords per accedir a servidors, l'agent ja les subministraria.

Aquests mecanismes de validació seran transparents als usuaris.

Arxius de configuració:

La informació de configuració SSH de tot el sistema s'emmagatzema al directori `/etc/ssh/`:

- `moduli` — Arxiu necessari per a l'intercanvi (clan Diffie-Hellman) que és imprescindible per a la construcció d'una capa de transport segur.
- `ssh_config` — Arxiu de configuració del client. No tindrà efecte si tenim un arxiu de configuració propi del client (a /home/usuari`/.ssh/config`).
- `sshd_config` — Arxiu de configuració del dimoni `sshd (servidor SSH)`.
- `ssh_host_dsa_key` — La clau privada DSA.
- `ssh_host_dsa_key.pub` — La clau pública DSA.
- `ssh_host_key` — La clau privada RSA (versió 1 de SSH).
- `ssh_host_key.pub` — La clau pública RSA (versió 1 de SSH).
- `ssh_host_rsa_key` — La clau privada RSA (versió 2 de SSH).
- `ssh_host_rsa_key.pub` — La clau pública RSA (versió 2 de SSH).

DSA, RSA1 i RSA2 són diferents algorismes d'encriptació que s'utilitzen a SSH.

La informació per a la configuració SSH del client s'emmagatzamerà al directori propi de l'usuari que actua com a client (/home/usuari/.ssh/):

- `authorized_keys` — Arxiu que conté la llista de claus públiques "autoritzades". Quan un client es connecta al servidor, el servidor valida al client chequejant la seva clau pública guardada en aquest arxiu.
- `id_dsa` — Clau privada DSA de l'usuari.
- `id_dsa.pub` — Clau pública DSA de l'usuari.
- `id_rsa` — Clau RSA privada (versió 2 de SSH).
- `id_rsa.pub` — Clau pública RSA (versió 2 de SSH).
- `identity` — Clau privada RSA (versió 1 de SSH).
- `identity.pub` — Clau pública RSA (versió 1 de SSH).
- `known_hosts` — Conté les claus de host DSA dels servidors SSH coneguts per l'usuari. Aquest arxiu és molt important per validar que el client es connecti al servidor correcte. Si volem que tots els usuaris coneguin els mateixos hosts, copiarem aquest arxiu al directori de configuració de SSH:

```
cp /home/usuari/.ssh/ssh_known_hosts   /etc/ssh/ssh_known_hosts
```