SSH-KEYGEN

L'eina SSH-KEYGEN permet generar parells de claus (privada-pública) per ficar-los al directori de configuració i no haver d'identificar-se amb usuari i password:

El primer que haurem de fer és assegurar-nos que tenim, **a l'arxiu de configuració de la màquina servidor**, que està a /etc/ssh/sshd_config, les configuracions necessàries per no haver d'entrar claus:

RSAAuthentication yes
PubkeyAuthentication yes
AuthorizedKeysFile %h/.ssh/authorized_keys cal descomentar aquestes línies

jo havia posat /root/.ssh/authorized_keys però no era correcte ja que només funcionaria si el client remot és el root. Funciona si posem:

%h/.ssh/authorized_keys

I també amb:

.ssh/authorized_keys (que és com venia per defecte a l'arxiu)

OJO: qualsevol actualització a l'arxiu de configuració del servidor, per assegurar-nos que funciona, caldrà fer un restart de sshd tant al client com al servidor

Després generarem les claus **a la màquina client** utilitzant:

ssh-keygen –t opció opció pot ser rsa, rsa1 o dsa

(jo he posat dsa)

Genera un arxiu, per defecte /root/.ssh/id_sda amb la clau privada. Es pot posar clau de pas. Aquest arxiu ha de romandre al client, també genera un altre arxiu amb la clau pública que és el que hem d'enviar al servidor (/root/.ssh/id_dsa.pub)

Copiarem l'arxiu de claus públiques generat (/root/.ssh/id_dsa.pub), al servidor amb el nom authorized_keys, que serà l'arxiu que aquest reconeixerà sense entrar password. Per tant, **a la màquina client** farem:

scp /root/.ssh/id_dsa.pub **root@192.168.1.1**:/root/.ssh/authorized_keys

Entrem com a root a la màquina servidor i copio l'arxiu de claus públiques, suposant que 192.168.1.1 és la màquina servidor

exit

Ara, a la màquina servidor seria convenient comprovar que la còpia realment ha produït una actualització del fitxer authorized_keys.

Fet això, només ens quedarà reiniciar ssh a les dues màquines (/etc/rc.d/init.d/sshd restart **a client i a servidor**). (potser no calgui)

A partir d'aquest moment, podrem iniciar la sessió SSH des del client contra el servidor i aquest no ens demanarà password. Caldrà anar amb compte amb això, ja que si algú ens suplanta, no necessitarà conèixer les passwords.