

SSH con contraseñas RSA

Escrito por Administrator
Viernes, 02 de Mayo de 2008 16:27

Con la utilización de contraseñas RSA eliminas la necesidad de tener que escribir la contraseña de un usuario determinado cada vez que te conectas a un maquina, permitiéndote, por ejemplo, poder automatizar procesos para los que antes necesitabas escribir la contraseña.

Hace algunos días me vi en la necesidad de automatizar las copia de archivos entre servidores utilizando la herramienta rsync (<http://rsync.samba.org/>), la cual permite copiar archivos entre maquinas y mantener espejos de archivos entre distintos servidores, el problema que tenia era que cada vez que me conectaba a la otra maquina como usuario root esta me pedía la contraseña, pero claro si lo que quieres es automatizar la tarea no puedes ir a escribir la contraseña cada vez que corras la tarea.

Esquema de los servidor

Servidor A : roble, desde este me conectare a alerce.

Servidor B : alerce, recibirá las conexiones desde roble, sin pedir contraseña.

Lo primero que necesitas es tener instalado OpenSSH(<http://openssh.com/es/>), en ambas maquinas, dentro de las utilidades que instala OpenSSH se encuentra una llamada ssh-keygen, la cual permite generar pares de claves, para comenzar debemos generar un par de claves RSA en la maquina llamada roble con el comando:

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

te preguntara por el nombre que tendrá el archivo de contraseñas y la ruta en la que quieres almacenarlo, por defecto es "/root/.ssh/id_rsa", una vez generados los dos archivos de claves (una es la clave privada y la otra la clave publica), debes copiar la clave publica al servidor que quieres conectarte sin escribir la contraseña, en este caso alerce, esto lo puedes hacer de varias formas yo uso scp (otra utilizada de ssh para copias de archivos entre servidores). Entonces estando en alerce escribo el comando:

```
scp root@roble:/root/.ssh/id_rsa.pub /root/.ssh
```

SSH con contraseñas RSA

Escrito por Administrator
Viernes, 02 de Mayo de 2008 16:27

me pedirá la clave del usuario root de la maquina roble, con esto copiare el archivo de clave publica desde la ubicación predeterminada, hacia el servidor alerce al directorio /root/.ssh Luego debo agregar la clave publica del servidor roble al archivos de claves publicas autorizadas del servidor alerce, esto lo hago con el comando:

```
cat id_rsa.pub >> authorized_keys
```

Ahora ya esta la clave en el listado de claves autorizadas del servidor alerce, solo falta configurar OpenSSH para que acepte este método de autenticación, para ellos se debe editar el archivo "/etc/ssh/sshd_config", se debe buscar la líneas siguientes y descomentariarlas (sacar el signo gato del principio) :

```
#RSAAuthentication yey
```

```
#PubkeyAuthentication yes
```

```
#AuthorizedKeysFile .ssh/authorized_keys
```

Una vez creadas o descomentariadas las líneas anteriores se debe reiniciar el servicio, de cualquiera de las formas siguientes:

```
./etc/rc.d/init.d/sshd restart ó  
service sshd restart
```

Espero que este artículo sea de ayuda para alguien.