SSH_Intro_v01

Facundo Navarro

26 de diciembre de 2018

1. SSH - Introducción

SSH o Secure Shell, es un protocolo de administración para acceder de forma remota a un servidor privado, el acceso se grarantiza mediante el uso de una clave pública y una clave privada mediante un cifrado criptográfico asimétrico tambien llamado criptografía de clave pública o criptografía de dos claves. El método consiste en crear un par de llaves, que mediante los métodos criptógraficos se garantiza que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

La clave pública se puede entregar a cualquier persona y es la que permanece en el servidor, la otra clave es la clave privada y el propietario debe guardarla de modo que nadie tenga acceso a ella.

1.1. Generación de par de claves SSH en sistemas UNIX

Un par de llaves SSH puede ser generado ejecuando el comando *ssh-keygen* dentro de la terminal, el cual por defecto usa seguridad 2048-bit RSA, luego de presionado se pedirá que se indique un nombre de archivo como asi también la ruta, si se deja vacío el mismo se guardará en la ruta */home/usuario/.ssh/* con el nombre *id_rsa* (clave privada) e *id_rsa.pub* (clave pública), como se puede observar en las imágenes 1 y 2.

De igual manera se recomienda utilizar la encirptación de 4096 bits, como asi también no dejar en blanco la *passphrase* para la clave privada de forma que por cualquier motivo se obtenga la clave privada esta quede encriptada con la *passphrase* y no pueda ser utilizada, cabe aclarar que esta contraseña no la debe proporcionar por ningun motivo, en caso de olvido se deberá generar un nuevo par de claves, el comando recomendado a ejecutar es el siguiente:

```
$ ssh-keygen -f <filename> -t rsa -b 4096 -C "email@dominio.com"
```

-f especifica el nombre del archivo como así también la ruta en donde se guardará.

-t indica el algoritmo a utilizar.

-b indica el tamaño o cantidad de bits.

-C es importante añadir un comentario acorde de manera de identificar el propietario de la clave pública por parte del administrador en caso de extravío.

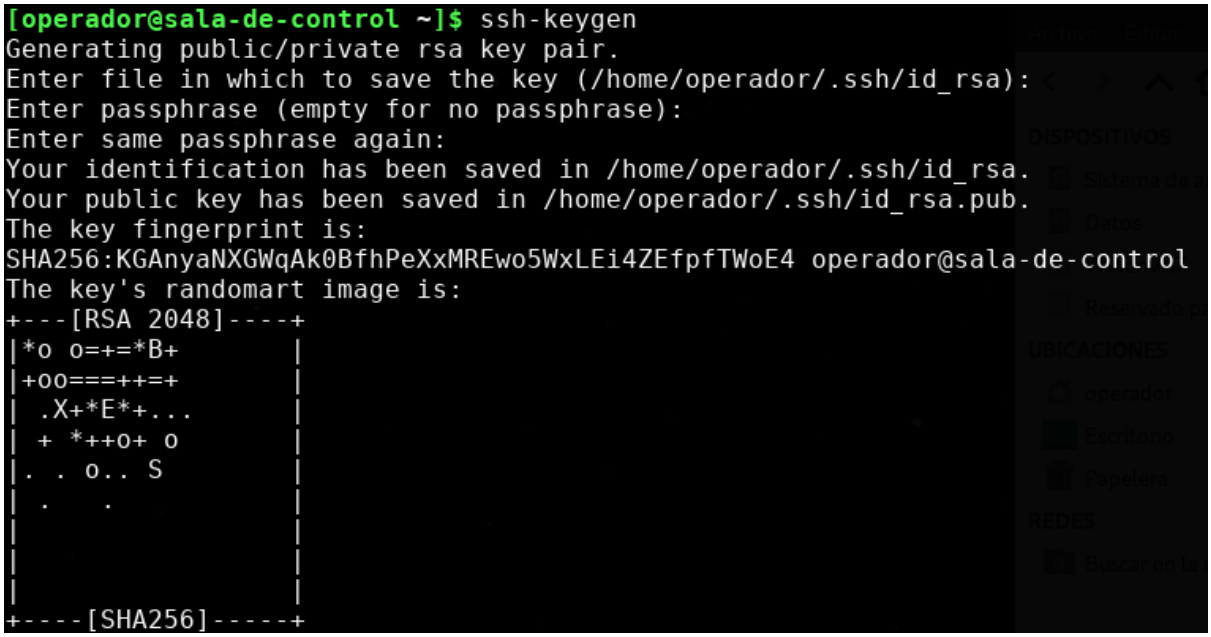

Figura 1: Salida terminal dejando vacío tanto el nombre del archivo como el *passphrase*

Figura 2: Directorio en $HOME/.ssh/ se ve las claves *id_rsa* e *id_rsa.pub*

Figura 3:

En la imagen 3 se puede observar el procedimiento completo, en primer lugar creamos un directorio llamado *llave_cluster*, luego se ejecuta el comando dado previamente reemplazando adecuadamente con nuestros datos, el nombre que elegí para el par de llaves es *fnavarro*

En la imagen 4 se ve que se crearon dentro del directorio especificado, un archivo *fnavarro* (clave privada) y otro de mismo nombre pero de extensión *.pub* (clave pública).

```
[operador@sala-de-control ~]$ cd llave_cluster/ && ls -l && pwd
total 8
-rw------- 1 operador operador 3434 dic 26 15:43 fnavarro
-rw-r--r-- 1 operador operador  745 dic 26 15:43 fnavarro.pub
/home/operador/llave_cluster
```

Figura 4: Par de llaves creadas acorde al parametro **-f**

1.2. Accediendo al Cluster Navira

Una vez que se han generado y enviado la clave pública al administrador *(it.ing@ucc.edu.ar)* y este le haya confirmado la creación de su usuario, se podra acceder al cluster por SSH desde la terminal de la siguiente manera:

```
$ ssh <usuario>@navira.cidie.ucc.edu.ar -p 2230
```

es impresindible la bandera **-p 2230** ya que es el puerto asignado por parte de servicio técnico para el acceso desde el exterior.

```
[operador@sala-de-control ~]$ ssh fnavarro@navira.cidie.ucc.edu.ar -p 2230
Last login: Wed Dec 26 09:50:20 2018 from 10.0.100.117

                    ooooo      ooo       .o.       oooooo     oooo ooooo ooooooooo.          .o.
                    `888b.     `8'      .888.       `888.     .8'  `888' `888   `Y88.       .888.
                     8 `88b.    8      .8"888.       `888.   .8'    888   888   .d88'      .8"888.
                     8   `88b.  8     .8' `888.       `888. .8'     888   888ooo88P'     .8' `888.
                     8     `88b.8    .88ooo8888.       `888.8'      888   888`88b.      .88ooo8888.
                     8       `888   .8'     `888.       `888'       888   888  `88b.   .8'     `888.
                    o8o        `8  o88o     o88888o       `8'       o8888o o888o  o888o o88o     o88888o

                                                en Universidad Catolica de Cordoba
             ======================================== ATENCION ========================================

             ============================================================================================

             * En construccion...;
             * Cualquier duda, consulta o sugerencia enviar mail a:
               it.ing@ucc.edu.ar

##############################################################################################################

[16:00][head@fnavarro ~]$
```

Figura 5: