

INTRODUCCIÓN AL SSH (Secure Shell)

SSH es un protocolo que facilita las **conexiones entre dos sistemas**. A diferencia de otros protocolos de comunicación, **SSH encripta los datos que envía** para hacer imposible que alguien pueda acceder a la información que se está enviando y recibiendo, con una encriptación robusta de 128 bits. El nombre de **SSH** viene de **Secure SHell**. Por defecto **ssh usa el puerto 22**, aunque esto es configurable.

Con una **conexión ssh** podremos acceder a una máquina que tenga instalado y activo un **servidor ssh**. Normalmente accederemos vía terminal, con acceso a la Shell y a todos los comandos disponibles en el sistema de la máquina a la que estamos **conectados remotamente**.

En Ubuntu el **cliente ssh** viene instalado por defecto, si quisiésemos **instalar el servidor ssh** para poder conectarnos a nuestro equipo desde otros sólo tendríamos que escribir:

sudo apt-get install ssh (u openssh-server).

Para **conectarnos mediante ssh a una máquina remota** (que tiene que tener instalado un servidor ssh) simplemente tendremos que escribir el siguiente comando en el terminal:

ssh [<usuario>@]<hostname>[:<puerto>]

usuario: Hay que especificar el usuario siempre que el nombre sea diferente al usuario que estamos usando en la máquina local, tiene que ser un nombre de usuario válido en la máquina remota.

hostname: Puede ser una dirección IP, un dominio, un hostname interno, etc.

puerto: Si el puerto de escucha de la máquina remota no es el habitual (el **puerto 22**) tendremos que especificarlo.

A continuación unos **ejemplos** de diferentes maneras con las que podríamos conectarnos a una máquina remota con un **túnel ssh**:

ssh google.com

ssh 192.168.1.2

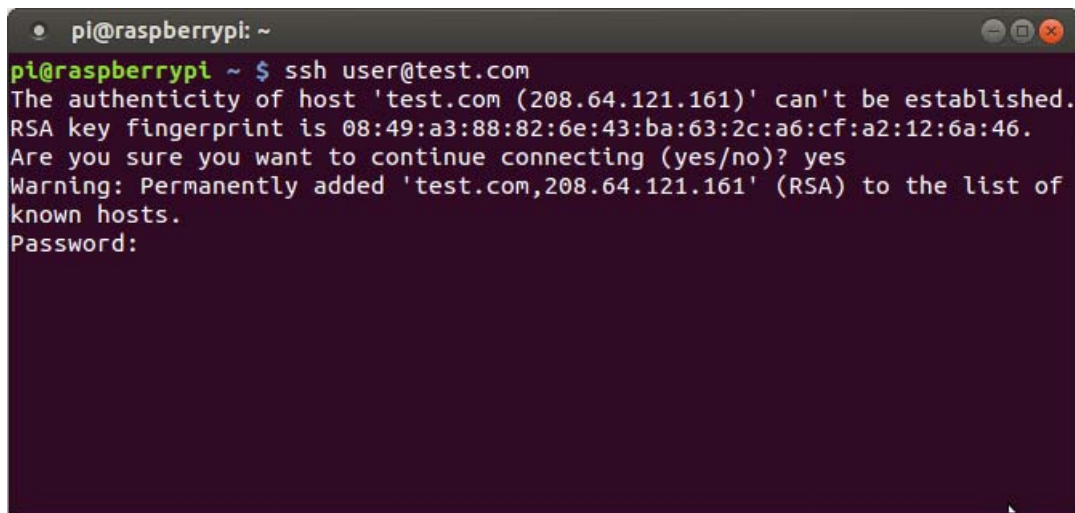
ssh user@192.168.1.2

ssh user@google.com

ssh user@192.168.1.2:2222

Al intentarnos **conectar a un servidor ssh**, nos pedirá una contraseña que será la del usuario en el equipo remoto y que tendremos que escribir (recordad que en Linux no aparecen asteriscos o puntos cuando escribimos una contraseña en la línea de comandos). Si el usuario y la contraseña son correctos accederemos vía ssh a la máquina remota.

También nos preguntará si confiamos en la **autenticidad del host**, la primera vez que nos intentemos conectar a él. Si por lo que sea el host cambia e intentamos volver a conectarnos con el host, ssh nos avisará y no nos dejará conectarnos, una sencilla solución es borrar el archivo: `~/.ssh/known_hosts` (en nuestra carpeta home).

A terminal window titled 'pi@raspberrypi: ~' with a dark purple background. The prompt is 'pi@raspberrypi ~ \$'. The user has entered 'ssh user@test.com'. The terminal displays the following text: 'The authenticity of host 'test.com (208.64.121.161)' can't be established. RSA key fingerprint is 08:49:a3:88:82:6e:43:ba:63:2c:a6:cf:a2:12:6a:46. Are you sure you want to continue connecting (yes/no)? yes'. The user has responded with 'yes'. The terminal then shows 'Warning: Permanently added 'test.com,208.64.121.161' (RSA) to the list of known hosts.' and 'Password:'. The cursor is on the next line.

```
pi@raspberrypi ~ $ ssh user@test.com
The authenticity of host 'test.com (208.64.121.161)' can't be established.
RSA key fingerprint is 08:49:a3:88:82:6e:43:ba:63:2c:a6:cf:a2:12:6a:46.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'test.com,208.64.121.161' (RSA) to the list of
known hosts.
Password:
```

Una vez conectados, es lo mismo que si hubiésemos abierto un terminal en la máquina remota, pudiendo cambiar, modificar y ejecutar lo que queramos desde la línea de comandos. De este modo podemos trabajar, apagar la máquina, reiniciarla, etc, desde cualquier sitio.

Arrancar el demonio SSH

Si queremos que nuestra máquina disponga de un servidor SSH debemos arrancar el servicio correspondiente. El servicio SSH se puede encontrar en el directorio `/etc/init.d` junto a otros muchos servicios de Linux. También es posible encontrarlo usualmente en `/usr/sbin/sshd`. Para arrancarlo basta con ejecutar el comando:

`/etc/init.d/sshd start [stop | reload | force-reload | restart]`

Archivos de configuración

El directorio donde se encuentra instalado es `/etc/ssh`. En este directorio encontramos entre otros archivos:

- `sshd_config`: archivo de configuración del servidor SSH
- `ssh_config`: archivo de configuración del cliente SSH
- `ssh_host_*_key`: clave privada de la máquina (* *puede ser rsa o dsa*)
- `ssh_host_*_key.pub`: clave pública de la máquina (* *puede ser rsa o dsa*).