Práctica 3 SSH

2º DAW – Dual Eric Moros Pérez

Tabla de contenido

[Definición 3](#_Toc1678584)

[Instalación 3](#_Toc1678585)

[Configuración 4](#_Toc1678586)

[Filtrado con el firewall 5](#_Toc1678587)

[Transferencia de archivos 6](#_Toc1678588)

# Definición

SSH (Secure Shell) es un protocolo para controlar servidores de forma remota cifrado de punto a punto.

Normalmente los servicios de este protocolo se ponen a la escucha en el puerto 22.

# Instalación

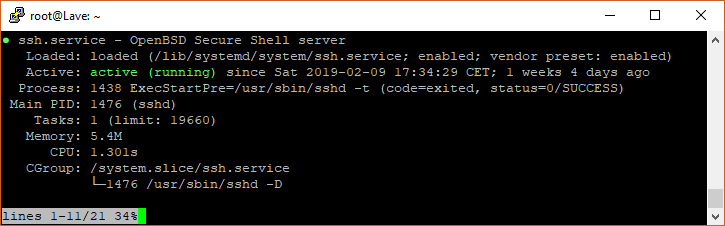
Ubuntu server por defecto ya tiene instalado el servicio/demonio del SSH, en caso de usar otra distribución parecida a Debian o Ubuntu y de que no realizara la instalación automáticamente pudes usar este comando:

sudo apt install openssh -y

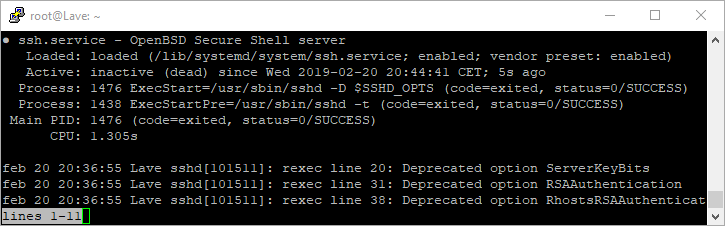
Si todo ha ido bien durante la instalación, puedes comprobar el estado actual del servicio con el siguiente comando:

sudo service ssh status

Tras lanzar el comando debería darte un resultado parecido a este:



Es posible que, en lugar de encontrártelo activo, aparezca inactivo/muerto:



En tal caso puedes arrancar el servicio lanza este comando (Para parar borra ***start*** y pon ***stop***):

sudo service ssh start

Si a partir de este momento, post comprobar el estado, no se encuentra el servicio activo, es posible que hayas tenido algún problema durante la instalación o que este documento se haya quedado obsoleto.

# Configuración

Puedes editar los parámetros del servicio/demonio en este archivo “***/etc/ssh/sshd\_config***”).

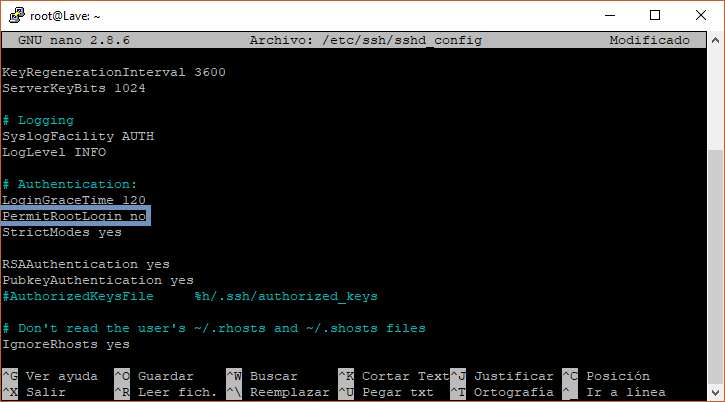
Ten cuidado al elegir el archivo a editar, existe un archivo llamado “~~ssh\_config~~” que no tiene nada que ver con las configuraciones que vamos a realizar y es muy fácil de confundir con el nuestro.

Si estás familiarizado con nano puedes lanzar este comando para editarlo:

***sudo nano /etc/ssh/sshd\_config***

Ubuntu y Debian por defecto deshabilitan la conexión por SHH con el usuario “root”, ya que consideran un fallo grabe de seguridad el que un usuario con capacidad omisiva total de los permisos pueda lanzar ordenes remotamente.

Si por alguna razón, tu servicio/demonio permite la conexión de este usuario y no te parece conveniente, puedes bloquearla modificando tu configuración como se resalta en la siguiente imagen:



Para aplicar los cambios ejecuta este comando:

***sudo service reload ssh reload***

Puedes comprobar si se ha aplicado correctamente haciendo un “status”. En caso de no haberse recargado correctamente la configuración revisa tu configuración.

# Filtrado con el firewall

Antiguamente se utilizaban los ficheros “***/etc/host.deny***” y “***/etc/host.allow***” para relizar un filtrado servicio/demonio por cliente/dirección, pero actualmente estos archivos se han quedado deprecados y se aplican reglas en el firewall del servidor porque es mucho más seguro y da mucha más soltura a la hora de crear reglas de acceso.

Para limitar la conexión por SSH con un filtro de lista blanca por IP tienes que aplicar las siguientes reglas.

Bloqueo de todo el tráfico entrante:

***sudo ufw default deny incoming***

Permiso de conexión exclusivo por el puerto 22 para la dirección IP “***192.168.1.123***” (En caso de haber modificado el puerto del servicio del SSH sustituye **22** por el modificado):

***sudo ufw allow from 192.168.1.123 to any port 22 proto tcp***

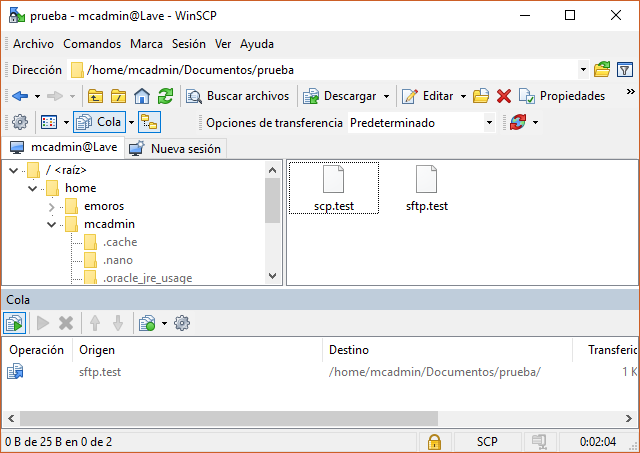
Habilitar el firewall:

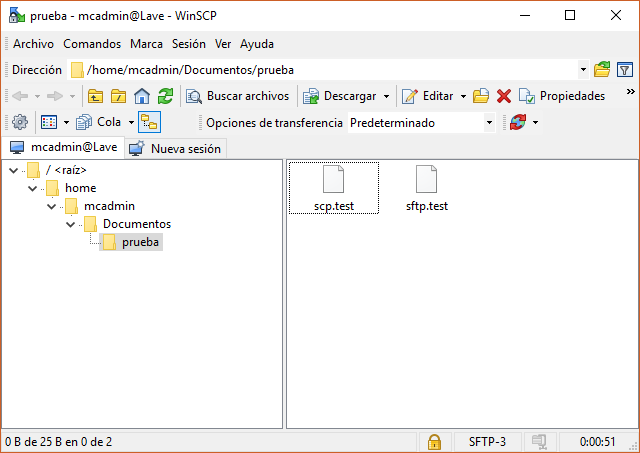
***sudo ufw enable***

Si haces un “status” debería de “ufw” verás las reglas aplicadas.

# Transferencia de archivos

Para realizar una transferencia de archivos por SSH podemos utilizar el protocolo SCP o SFTP, como diferencias principales SCP es más rápido que SFTP, pero SFTP tiene más aplicaciones que SCP, en lo relacionado a la seguridad ambos están bien preparados.





# Clave pública y privada

Hay veces que un usuario y una contraseña es insuficiente para mantener una seguridad elevada en los servidores, para aumentarla considerablemente se puede crear una clave publica y privada que sirvan como identificadores.

La clave publica es la identificación que se coloca en la máquina de destino.

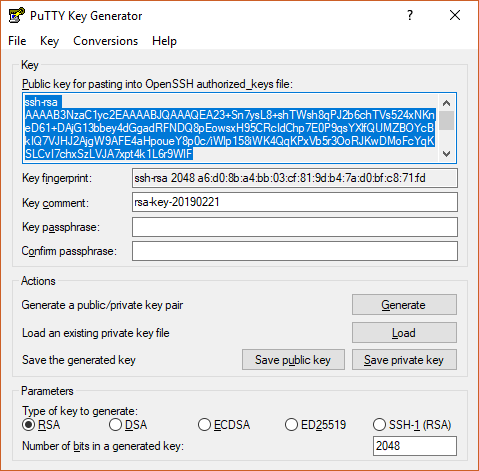
La clave priva es la identificación que se guardará el cliente para conectar al destino.

Siempre que la máquina destino contenga la clave pública del cliente y el cliente acceda con su clave privada se creará la conexión, en caso de que falte cualquiera de estas claves al realizar la petición de conexión se rechazara.

Es más sencillo de ver si te imaginas que la clave privada es una llave y la clave pública un candado que puedes poner a tu servidor. Sin candado da igual la llave que tengas y sin llave no puedes abrir el candado.

Nosotros para realizar la conexión desde Windows vamos a usar el cliente “PuTTY”.

Para crear las claves privadas puedes usar “PuTTy Key Generator”.

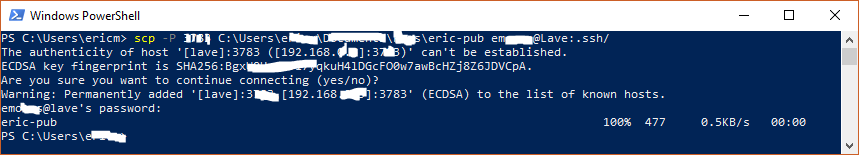


Guarda tus claves en un sitio seguro y accesible por ti mismo.

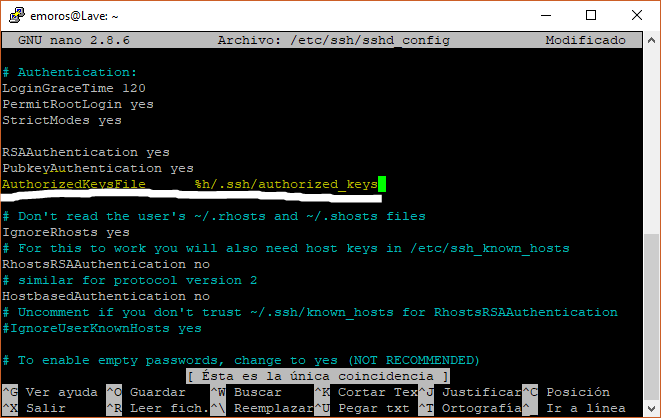
Sube la clave pública a tu servidor, para subirla puedes usar este comando desde PowerShell:

***scp C:\Users\youruser\keys\user-pub*** [**user@machine:.ssh/**](mailto:user@machine:.ssh/)

Si se ha relizado bien la tranmision deveria darte un resultado parecido al de esta imagen:



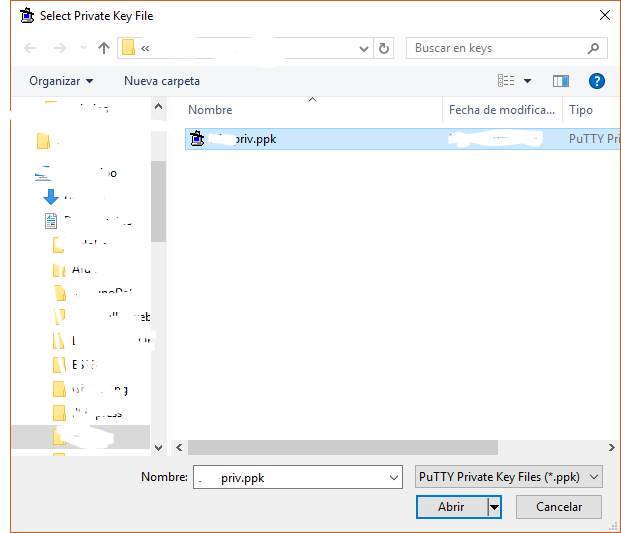
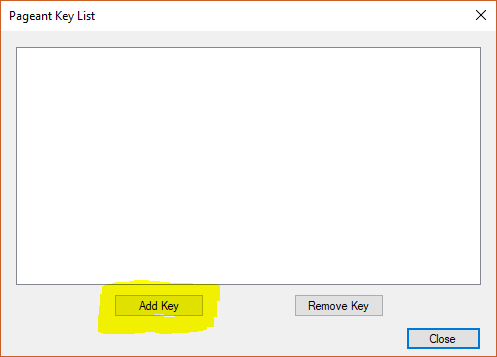
Aplica la siguiente configuración:

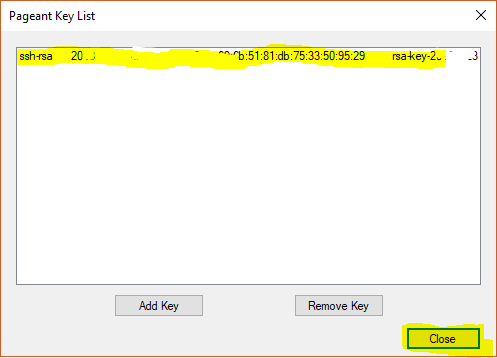


Pon ese nombre al archivo con tu clave y recarga el servicio.

Ahora ya podrás realizar la conexión utilizando tu clave privada.

Puesto que para realizar la conexión vamos a usar el programa “PuTTY” para añadir la clave privada a nuestra conexión debemos lanzar Pageant y añadir nuestra clave privada como en las siguientes imágenes:





Después tras realizar la conexión SSH debería conectarse sin problemas

