

**2018**

SSH

Despliegue de aplicaciones web

Andrei García Cuadra

Contenido

[1. bis 2](#_Toc504648894)

[2. Conexión por terminal desde linux 2](#_Toc504648895)

[3. Utilizando scopy (scp) 3](#_Toc504648896)

[4. Utilizando secure ftp (sftp) 4](#_Toc504648897)

[5. Conexión con certificado 5](#_Toc504648898)

[6. Cambiar certificado rsa a openssh 6](#_Toc504648899)

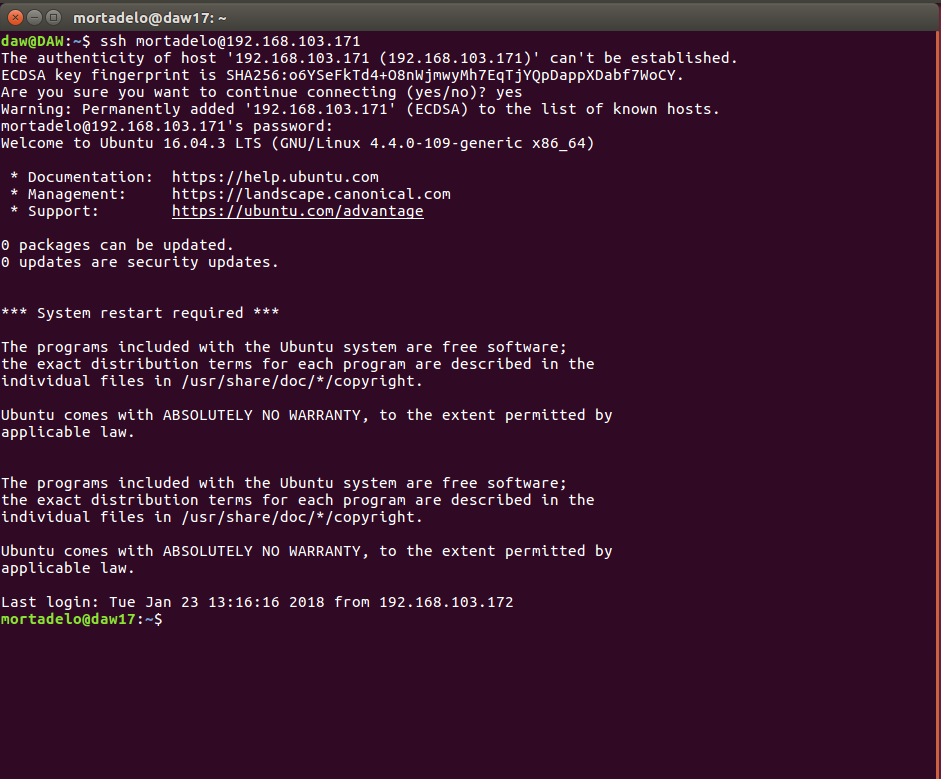
# bis

NOTA IMPORTANTE: PARA QUE LOS COMANDOS FUNCIONEN CORRECTAMENTE SE HA DE SUSTITUIR LA VARIABLE COMPLETA. LA SINTAXIS DE UNA VARIABLE ES SIMPLE, ESTÁ COMPRENDIDA ENTRE <>, TENIENDO QUE SUSTITUIR TAMBIÉN ESTOS CARACTERES.

# Conexión por terminal desde linux

Para la conexión a un terminal remoto vía SSH utilizando un Ubuntu de escritorio (en nuestro caso), para ello, podemos utilizar los siguientes comandos (reemplazando usuario y host donde corresponda, siendo <host> la dirección de nuestro servidor y <usuario> el usuario de conexión):

* **ssh <host>**
* **ssh <usuario>@<host>**



# Utilizando scopy (scp)

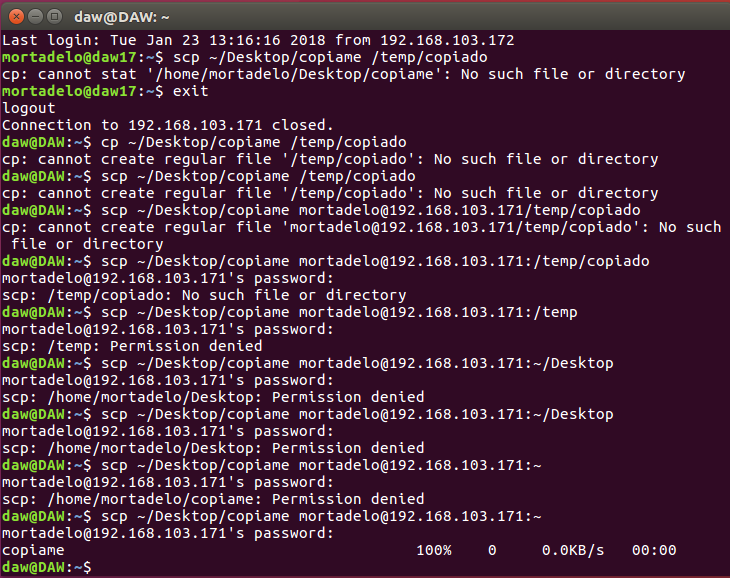
Este comando se utiliza para transferir un archivo desde el equipo local a uno ajeno, conectándonos por SSH. Para ello, podemos utilizar los siguientes comandos:

* **scp <origen> <destino>**

Sirve para copiar archivos entre La sintaxis de este método es básica: sólo debemos reemplazar origen por la ubicación del archivo local y destino por la ubicación de destino en el servidor. Es una sintaxis simple pero debemos estar conectados en la máquina a través del terminal ssh.

* **scp <origen> <usuario>@<host>:<destino>**

Permite copiar un archivo desde el equipo local a uno, el cual hemos ingresado su usuario y host previo a la ubicación del archivo que deseamos copiar. Es una sintaxis más avanzada. Debemos estar desconectados de la terminal SSH al ejecutarlo.

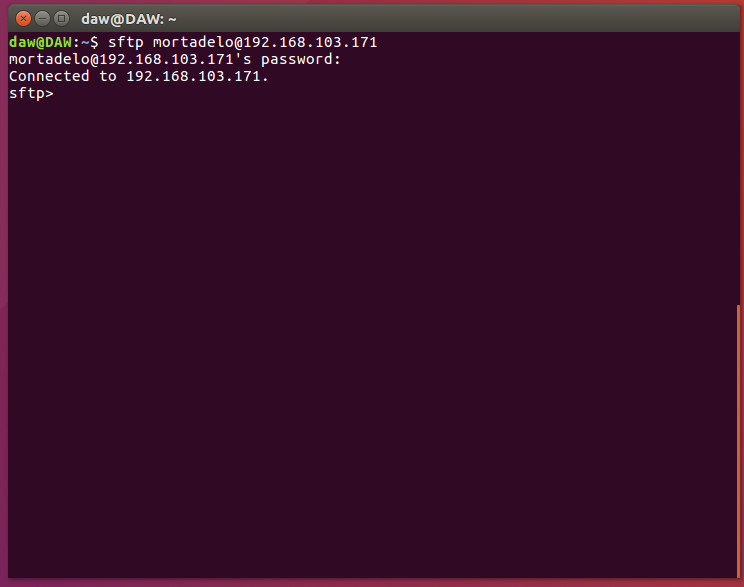


NOTA: Los errores de permisos fueron subsanados desde el servidor, ya que pertenecían a root (los cree como tal). Como se puede apreciar, finalmente el archivo fue copiado satisfactoriamente.

# Utilizando secure ftp (sftp)

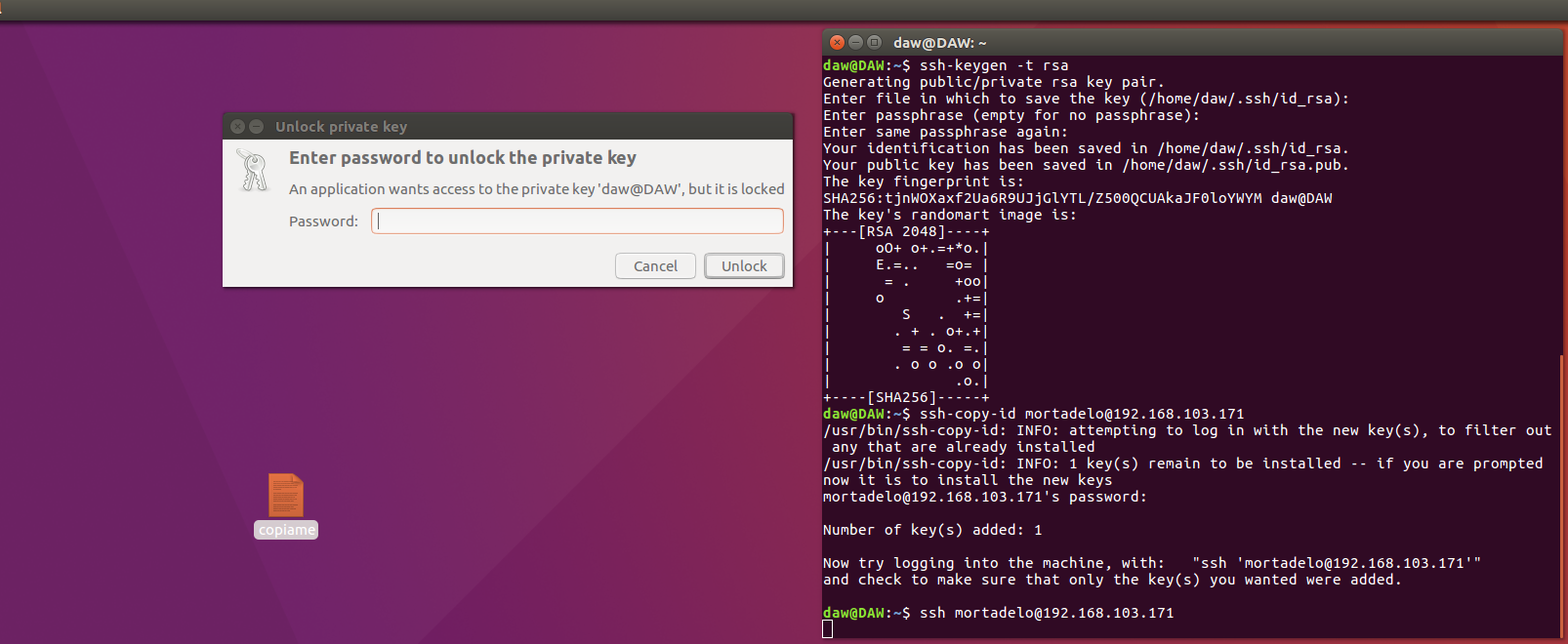
Para conectarnos utilizando el ftp seguro (encriptado), simplemente debemos ejecutar el siguiente comando, sustituyendo usuario y host donde corresponda:

* **stfp <host>**
* **sftp <usuario>@<host>**



# Conexión con certificado

Con este paso generaremos una clave para que sólo nos podamos conectar utilizando este archivo de encriptación, aumentando considerablemente la seguridad. Como se puede ver en la primera imagen, si tenemos la clave nos solicita su contraseña, la cual ya está en uso por el servidor para el usuario mortadelo. De este modo, podemos subir las claves para un determinado usuario o para todos.



1. Generar la clave privada en la máquina cliente

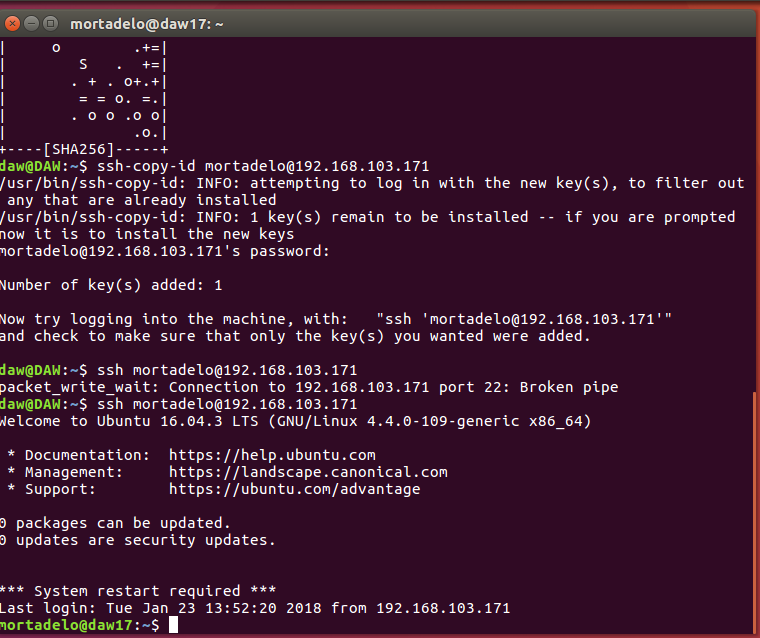
**ssh-keygen -t rsa**

1. Seleccionar ubicación de la clave

El programa nos solicitará la ubicación. Por defecto, se ubicará en el directorio home del usuario actual.

1. Introducimos la contraseña para la clave que hemos generado
2. Enviar esta clave al servidor para un determinado usuario (o para todos, omitiendo el usuario).

**ssh-copy-id <usuario>@<host>**

1. **Una vez introducida la contraseña, ya estaremos en el terminal.**

# 6. Cambiar certificado rsa a openssh

Para renovar los certificados de OpenSSH, seguimos el procedimiento:

1. Eliminamos los certificados antiguos

**rm -v /etc/ssh/ssh\_host\_\***

1. Reconfiguramos el servidor para que renueve las claves

**dpkg-reconfigure openssh-server**

1. Reiniciamos el servicio SSH

**service ssh restart**

Y ya estarían renovadas nuestras claves de OpenSSH.

