

ACCESO REMOTO AL SISTEMA. SSH

Es un protocolo que permite conectarse a un servidor de forma segura. Ofrece los siguientes servicios:

- acceso a terminal
- copia de ficheros
- ftp seguro

El protocolo ssh garantiza que la conexión se realiza desde los equipos deseados, para lo que usa certificados, y establece una comunicación cifrada entre el cliente y el servidor.

En Linux el servidor ssh más utilizado es OpenSSH www.openssh.org

INSTALACIÓN Y CONFIGURACIÓN DE SSH

Instalación: `#apt-get install ssh`

Fichero de configuración: `/etc/ssh/sshd_config` Algunos parámetros

<code>Port 22</code>	Puerto en el que trabaja ssh. Por defecto trabaja en el puerto 22.
<code>ListenAddress 0.0.0.0</code>	Dirección en la que atiende peticiones. Por defecto, responde por todas las interfaces del sistema
<code>PermitRootLogin no</code>	Indica si se permite o no el acceso al usuario root al servidor
<code>AllowUser susana profe</code> <code>AllowUsers susana@192.168.1.201</code>	Permite restringir el acceso a los usuarios del sistema. AllowUsers indica los usuarios que pueden acceder al sistema. Se puede indicar el equipo anfitrión desde el que pueden conectarse
<code>PrintMotd yes</code> <code>Banner /etc/issue.net</code>	Mensajes de entrada y conexión
<code>IgnoreUserKnownHosts no</code> <code>GatewayPorts no</code> <code>AllowTcpForwarding yes</code>	Configuración de seguridad y control de acceso
<code>Subsystem sftp /usr/lib/openssh/sftp-server</code>	Uso de subsistemas para otras aplicaciones, por ejemplo FTP

Iniciar el servicio

`#/etc/init.d/ssh start`

UTILIZACIÓN DEL SERVICIO SSH - FTP

Conectarse a un servidor remoto desde un terminal linux usando ssh

Por defecto, Ubuntu instala el cliente ssh

Sintaxis: `$ssh IP_equipo_remoto`

Ej: `$ssh 192.168.1.101`

Por defecto, se conecta con el usuario del cliente. Para indicar el usuario de conexión:

Sintaxis: `$ssh usuario@equipo`

donde:

usuario: usuario de conexión

equipo: IP del equipo remoto

Ej: `$ssh profesor@192.168.1.101`

Para conectarse a servidores Linux desde clientes Windows se utilizan aplicaciones como:

Putty o ssh Secure shell

scp

scp realiza la copia remota de ficheros entre dos equipos. Un cliente ejecuta scp y un servidor que permite el acceso ssh

Sintaxis:

`$scp fichero local usuario@ip_equipo_remoto:/directorio_remoto`

donde:

fichero local: Fichero a copiar.

usuario: Usuario con el que va a acceder al sistema remoto.

equipo_remoto: Equipo al que se va a copiar el fichero.

directorio_remoto: Directorio destino del sistema de ficheros del equipo remoto.

Ej: `scp fichero1.txt profesor@192.168.1.101:/home/profesor`

sftp

Protocolo de transferencia de ficheros segura. Realiza ftp utilizando ssh como transporte.

Sintaxis: `$ sftp usuario@equipo_remoto`

Ej: `sftp profesor@192.168.1.101`

*Para hacer FTP desde clientes Windows se utilizan aplicaciones como: **psftp** (comandos), **Filezilla** (entorno gráfico)*

Comandos de sftp

lcd directorio_local	Cambia de directorio en el equipo local
get fichero_remoto	Coger un fichero del equipo remoto para copiar en el equipo local
mget ficheros_remoto	Coger múltiples ficheros del equipo remoto para copiarlos en el equipo local
put fichero_local	Poner un fichero del equipo local en el equipo remoto
mput ficheros_locales	Poner múltiples ficheros del equipo local en el equipo remoto
quit	salir

...Otros comandos de ficheros de Linux se pueden usar en sftp Ver [enlace](#)

Es necesario definir en la configuración de ssh el servicio sftp, para ello en `/etc/ssh/sshd_config` tiene que aparecer la línea:

`subsystem sftp /usr/lib/sftp-server`