**RESUMEN SSH**

INSTALACION Y CONFIGURACION

* Instalación
  + apt-get install openssh-server
* Archivo de configuración
  + /etc/ssh/sshd\_config
* Reiniciación del servicio

start

* + /etc/init.d/ssh stop

restart

PARAMETROS DE CONFIGURACION

* LoginGraceTime (tiempo en segundos que tiene un cliente para conectarse)
* MaxAuthTries n (intentos de login fallidos)
* MaxStartups n (máximo de conexiones no identificadas simultaneas)
* PermitRootLogin (impide que se conecte root)
* Texto de bienvenida:

-modifica el archivo /etc/issue.net con el texto de bienvenida

-descomenta la línea Banner /etc/issue.net del fichero /etc/ssh/sshd\_config

-reinicia el servidor /etc/init.d/ssh restart

* Por defecto, el servidor SSH permitirá a cualquier usuario acceder siempre que tenga cuenta en el server.
* Para limitar los usuarios remotos a conectarse podemos optar por:
* AllowUsers nombre\_usuario Puede conectarse desde cualquier equipo.
* AllowUsers nombre\_usuario@IP\_equipo Puede conectarse el usuario únicamente desde IP\_equipo

COMANDOS SSH

* El comando **ssh** es un sustituto seguro de los comandos rlogin,rsh y telnet.

Este comando permite **iniciar sesión a través del shell hacía el servidor y ejecutar comandos en el servidor**.

El **formato del comando ssh** es:

**ssh [username@]servername [comando]**

**ssh [ -l username] servername [comando]**

* Uso del comando **scp**. Acceso por rcp

El comando scp puede ser **utilizado para transferir ficheros** entre máquinas bajo una conexión **segura y encriptada**. Este comando es similar a rcp.

**Formato** para **transferir** un **fichero local del cliente** **a** un sistema remoto en **el servidor**:

**scp localfile username@servername:newremotefile**

**Formato** para **transferir** un **fichero remoto del servidor** **a** un sistema local en **el cliente**:

**scp username@servername:remotefile newlocalfile**

Podemos usar estas opciones:

**-p** Especifica el puerto para realizar la conexión, debes utilizar en el caso de que utilice un puerto diferente al 22. ( scp -p 222 alumno@adequipo313:directorio1/\* directo )

**-r** Copia recursivamente los directorios especificados ,es decir, los subdirectorios con sus archivos. (scp -r alumno@adequipo313:directorio1/\* directorio)

* Uso del comando **sftp**. Acceso por ftp.

La utilidad **sftp** puede ser usada **para abrir una sesión segura e interactiva de FTP**. Es similar a ftp a excepción de que este utiliza seguridad de conexión **encriptada**. Una vez autentificado, podrás utilizar un conjunto de comandos similar al conjunto de comandos utilizado por el comando FTP.

El **formato del comando sftp** es:

sftp username@servername

* **Montar por ssh.**

Es posible montar sistemas de ficheros remotos en el servidor a través de NFS y SAMBA. Pero si te resulta más cómodo, también puedes montar sistemas de ficheros a través del servicio SSH, para ello:

1.- Instalar el paquete sshfs

# apt-get install ssh

2.-Realizar el montaje

# sshfs /mnt/fs 192.168.1.133:/datos /aux

Siendo /aux la carpeta local donde se monta el directorio remoto /datos del servidor 192.168.1.133