

Resumen comandos SSH

Configuración OpenSSH-Server

Instalar los paquetes necesarios

```
apt install openssh-server
```

Verificar el estado del servidor

```
systemctl status ssh
```

Permitir SSH a través del firewall

```
ufw allow ssh
```

Uso de SSH

Autenticación con usuario y contraseña

Abrir shell remota

```
ssh usuario@maquina -p <puerto>
```

Ejecutar comando directamente sin abrir shell

```
ssh usuario@maquina -p <puerto> <comando>
```

Si no se indica el puerto se utilizará el **puerto 22**, por defecto del protocolo SSH.

Autenticación con clave pública

Generar claves

```
ssh-keygen -t <algoritmo>
```

Copiar clave publica al servidor remoto

```
#Linux/MacOS:  
ssh-copy-id -i <ruta_fichero_identidad> usuario@maquina  
  
#Windows:  
type <fichero_clave_pub> | ssh usuario@maquina "cat >> .ssh/authorized_keys"
```

Abrir shell remota

```
ssh usuario@maquina -p <puerto>
```

Abrir shell remota indicando una clave privada concreta

```
ssh -i <ruta_clave_privada> usuario@maquina -p <puerto>
```

Regenerar archivo de clave pública a partir de clave privada

```
ssh-keygen -y -f <archivo_clave_privada> >> <nuevo_archivo.pub>
```

Añadir passphrase a una clave privada ya existente

```
ssh-keygen -p -f <archivo_clave_privada>
```

SSH-Agent

Verificar que se encuentra disponible el proceso SSH-Agent

```
# Opción 1  
env | grep SSH  
  
# Opción 2  
ps aux | grep ssh-agent
```

Agregar una clave a la gestión de SSH-Agent

```
ssh-add <ruta_fichero_clave_privada>
```

Comprobar la lista de identidades

```
ssh-add -l
```

Eliminar todas las identidades

```
ssh-add -D
```

Configuración

Comprobar si una maquina está registrada en `known_hosts`

```
ssh-keygen -F maquina:<puerto>
```

Eliminar la clave pública de un servidor remoto

```
ssh-keygen -R maquina:<puerto>
```

Indicar explícitamente una **parámetro de configuración**

```
ssh -o "<parametro> <valor>" usuario@maquina
```

Ficheros relevantes de configuración:

Cliente

- `~/.ssh/known_host` Servidores remotos conocidos
- `~/.ssh/config` Configuración del cliente SSH para el usuario
- `/etc/ssh/ssh_config` Configuración del cliente SSH global, para todos los usuarios

Servidor

- `/etc/ssh/sshd_config` Archivo de configuración del servicio SSH
- `~/.ssh/authorized_keys` Archivo que almacena las claves públicas de los clientes que pueden conectar mediante este método de autenticación

Obtener todos los **parámetros** (explícitos e implícitos) del servicio SSH

```
sshd -T
```

Transferencia de ficheros

Transferencia de ficheros mediante **scp**

```
scp usuario@maquina_origen:ruta usuario@maquina_destino:ruta
```

Transferencia **recursiva** de ficheros mediante **scp**

```
scp -r usuario@maquina_origen:directorio usuario@maquina_destino:ruta
```

Abrir shell para transferencia de archivos mediante **sftp**

```
sftp usuario@maquina
```

Túneles SSH

Redirigir servicio desde una maquina inaccesible, a través de un **túnel SSH**

```
ssh -L <puerto_local>:<direccion_M1>:<puerto_M1> <usuario>:<direccion_M2> -N
```