

OpenSSH



Este artigo está en construción. Os autores do mesmo están traballando nel.

Se queres axudar á súa realización ou, simplemente, queres facer algún tipo de comentario, envía un mail a un dos autores que aparecen no pé deste artigo."

Sumario

- 1 Introducción ao servidor OpenSSH
- 2 Instalación do servidor SSH
- 3 Arrancar o servidor SSH
- 4 Agregar seguridade ao servidor SSH
 - ♦ 4.1 Cambiar o porto por defecto
- 5 Conexión dende un PC con Windows
- 6 Exemplos conexión SSH

Introdución ao servidor OpenSSH

OpenSSH (*Secure Shell*, Entorno Seguro) é un paquete que contén un grupo de programas para a transferencia remota segura:

- **scp** (*Secure Copy*, Copia segura).
- **ssh** (*Secure Shell*, Intérprete de comandos seguro).
- **sftp** (SSH *file transfer protocol*, Protocolo de transferencia de arquivos sobre SSH).

ssh é a ferramenta a elixir para a administración remota do sistema. Poderemos iniciar sesión en sistemas remotos e executalos coma si estivésenos fisicamente neles. O inicio de sesión e os datos cífranse e compróbase se os arquivos enviados foron alterados durante a transferencia.

En realidade SSH non é un intérprete de comandos, SSH é un protocolo. Hai dúas versións incompatibles entre si: **SSH-1** e **SSH-2**.

Na actualidade emprégase SSH-2 que está descrito en 5 documentos:

- ♦ **SSH Assigned Numbers** (RFC 4250)
- ♦ **SSH Protocol Architecture** (RFC 4251)
- ♦ **SSH Authentication Protocol** (RFC 4252)
- ♦ **SSH Transport Layer Protocol** (RFC 4253)
- ♦ **SSH Connection Protocol** (RFC 4254)

Instalación do servidor SSH

Instalamos o servidor **OpenSSH**. Por exemplo, para instalalo nunha distribución Ubuntu:

```
# apt-get install openssh-server
```

Arrancar o servidor SSH

O demo de SSH é **sshd**. Para iniciar sshd:

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

Para deter sshd:

```
# /etc/init.d/sshd stop
```

Así e todo, o mellor é comprobar os nomes dos arquivos *init*, pois poden variar segundo a distribución.

Agregar seguridade ao servidor SSH

[Enlace de interese para a distribución Ubuntu](#).

É interesante aumentar a seguridade do servidor, para iso editaremos o arquivo `/etc/ssh/sshd_config` e cambiaremos ou engadiremos as seguintes liñas:

Cambiar o porto por defecto

Por defecto o SSH escoita no porto 22, é interesante cambialo por un que só nos saibamos. Por exemplo, para facer que escoite no porto 1122 engadiremos a directiva **Port**:

```
Port 1122
```

Conexión dende un PC con Windows

O mellor neste caso é empregar o software [PuTTY](#).

O único que hai que facer é descargalo, instalalo e executalo. Despois debe de escribirse o nome, ou a IP, do ordenador ó que se quere conectar, e logo facer clic en Open.

O programa é un executable (putty.exe), colle en calquera disquete e pode executarse dende unha memoria USB, disquete ou similar.

Para acceder dende Windows tamén poderíamos utilizar o [Cygwin](#).

- **Ligazón de Interese:** [Putty para plataformas Windows e UNIX](#)

Exemplos conexión SSH

Ligazón [Exemplos](#)