

Acceso a un servidor dedicado a través de SSH

Introducción

El servidor de interfaz de comandos **Secure SHell** (SSH) está instalado en todos los servidores. De este modo puede conectarse al servidor de forma segura y tener un control total del servidor.

El acceso SSH le permite entrar en el shell del servidor de OVH y realizar tareas de administración :

- El shell más conocido y más utilizado para administrar un servidor Linux es BASH.
- En el caso de tener un servidor Windows, el shell utilizado es MS-DOS (Interfaz de línea de comandos).

Primera conexión

Para conectarse al servidor en SSH, necesita dos datos:

- ip de la máquina (o el nombre DNS equivalente)
- la contraseña "*root*" de la máquina

Necesitará también una utilidad para conectarse a SSH.

- En el caso de conectarse desde un ordenador con Linux, necesitará tener el paquete Open SSH instalado
- En el caso de conectarse desde un ordenador con Windows, necesitará tener el programa Putty instalado

Más información sobre Putty : [UtilizarPutty](#)

Ejemplo de conexión con Open SSH:

```
$ ssh root@nsxxxxx.ovh.net
The authenticity of host 'ns0000.ovh.net (213.186.32.1)' can't be
established.
RSA key fingerprint is a9:bb:55:35:86:4d:ca:81:7f:9e:2b:2c:79:10:96:3c.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ns0000.ovh.net,213.186.32.1' (RSA) to the
list of known hosts.
Password:
$
```

Una vez se ha conectado, su cliente SSH recibe una marca de seguridad **RSA key fingerprint** que identifica unívocamente el servidor al que está conectado.

Esta marca se verifica cada nueva conexión. Si cambia, se le informará del cambio y eso querrá decir que algo ha cambiado en el servidor. O bien la máquina ha sido reinstalada, o el servidor SSH ha sido reinstalado, o usted se conecta desde otra máquina.

A partir de la primera conexión debe aceptar la marca, que será almacenada en su puesto de trabajo por su cliente SSH.

Utilización del shell BASH

Una vez que ha conseguido entrar, puede ejecutar los comandos de Linux como si fuese su ordenador y con la seguridad que le proporciona el acceso SSH.

El acceso **root / admin** le permite tener acceso a todos los ficheros y con todos los permisos. Tenga mucho cuidado con las operaciones que realiza en el servidor con ese usuario.

Tiene disponible una pequeña guía que muestra lo que se puede hacer en Shell desde BASH en nuestra guía ShellBash.

Actualización

Por defecto su servidor dedicado provee acceso SSH en la última versión estable y segura.

No se olvide de mantenerlo actualizado si surgen nuevos fallos de seguridad, ya que es un elemento muy sensible del sistema.

Para saber la versión del programa gestor de SSH de su servidor puede introducir el comando **ssh -V**

```
# ssh -V
OpenSSH_3.7.1p2, SSH protocols 1.5/2.0, OpenSSL 0.9.6i [engine] Feb 19
2003
```

Si utiliza la distribución OVH Release, le aconsejamos actualizar su versión automáticamente usando nuestro sistema de Parches de actualización.

Hay una pequeña guía que describe el proceso en ReleasePatchSeguridad.

Estos parches corrigen automáticamente todos los fallos de seguridad conocidos hasta la fecha para su servidor dedicado.

Los errores

Error de protocolo con clientes SSH Windows

Si usted tiene la versión de ssh > 3.7, puede tener problemas de conexión con su máquina con los antiguos clientes SSH de Windows.

Para evitar estos problemas, puede descargar la última versión de su cliente SSH y forzar la conexión usando el protocolo SSHv2.

Si sigue sin poder conectar, le recomendamos que utilice el cliente PuttY : UtilizarPutty

En todos estos casos el problema no es de su servidor, sino de su cliente SSH.

Actualización incorrecta en la Release1 (Red Hat 7.2)

En la Release 1, si ha actualizado desde una version anterior a la 3.7.1p2, hay que introducir la opción **UsePAM yes** en el fichero `/etc/ssh/sshd_config`. Si no, no podrá volver a reconectar con su servidor.

Si con esta opción no consigue reiniciar el SSH, quiere decir que su versión no es la 3.7.1p2 y la actualización ha fallado.

En ambos casos, la solución pasa por arrancar su servidor en modo Rescue y modificar la configuración del fichero `/etc/ssh/sshd_config` con el valor correcto de **UsePAM**.

Más información sobre el modo Rescue : ModoRescue

Más información

: ShellBash :: Administración de un servidor a través de Bash

: UtilizarPutty :: Manual de uso de Putty

: ModoRescue :: Acceso al servidor en modo de rescate de emergencia