
UD07

Conexión SSH desde terminal remoto



Índice

- [Introducción.](#)
- [Instalación de OpenSSH Server.](#)
- [Configuración de OpenSSH Server.](#)
- [Conexión desde terminal remoto.](#)
- [Conexión desde máquina anfitriona.](#)
 - [Reenvío de puertos en modo NAT.](#)
 - [Reenvío de puertos en modo Red NAT.](#)



Introducción





Introducción

- En un entorno en **producción**, lo normal es que **no podemos administrar** nuestro servidor conectados **físicamente** al mismo.
- Pueden existir **distintas razones** para ello, como:
 - **No tenemos un acceso** cómodo al equipo. Suele ocurrir cuando se encuentra en una sala de servidores con características especiales.
 - **No dispone de pantalla ni teclado** desde los que trabajar. Suele ocurrir cuando el servidor se encuentra instalado en un rack.
- Existen **distintos protocolos y herramientas** para poder conectarnos y **administrar de forma remota** un equipo.
- Una de estas opciones es instalar un **servidor SSH**, que recibe su nombre del **protocolo** de comunicaciones que utiliza, también **llamado SSH** (Secure Shell).



Introducción

- Utilizando el **protocolo SSH** (Secure Shell) podemos **conectarnos** a un servidor **desde un cliente de una forma sencilla y razonablemente segura**.
- Mediante SSH podremos controlar de forma remota un ordenador (normalmente un servidor) donde hayamos instalado con antelación el software que ofrece el servicio SSH, **por ejemplo OpenSSH, que es la versión abierta y libre del protocolo SSH**.
- El **protocolo SSH cifra toda la información** que viaja entre el cliente y el servidor. Este dato es particularmente **importante** cuando utilizamos **Internet** como vía de acceso.



Instalación de OpenSSH Server





Instalación de OpenSSH Server

- Como hemos indicado, para poder establecer una conexión SSH con nuestro servidor, lo **primero será instalar un servidor SSH**, por ejemplo, **OpenSSH**.
- Sin embargo, durante la **instalación de Ubuntu Server 20.04** autorizamos la instalación de **OpenSSH Server**. En ese caso, no tenemos que instalar nada adicional en nuestro servidor.

```
SSH Setup [ Help ]

You can choose to install the OpenSSH server package to enable secure remote
access to your server.

[X] Install OpenSSH server

Import SSH identity: [ No ▼ ]
You can import your SSH keys from GitHub or Launchpad.

Import Username:

[X] Allow password authentication over SSH

[ Done ]
[ Back ]
```



Instalación de OpenSSH Server

- Si no lo hubiéramos instalado durante el proceso de instalación del sistema operativo, podríamos **instarlo posteriormente ejecutando el comando:**

`sudo apt install open-ssh server`

- Para **comprobar el estado** en el que se encuentra el **servicio ssh** utilizamos el comando:

`sudo systemctl status ssh`

- Existen **otros comandos** que también debemos conocer:
 - **`sudo systemctl enable ssh`**: habilita el servicio SSH
 - **`sudo systemctl start ssh`**: inicia el servicio SSH
 - **`sudo service ssh restart`**: reinicio el servicio SSH
 - **`sudo ufw allow ssh`**: habilita regla en firewall para tráfico servicio SSH.

Instalación de OpenSSH Server



```
SERVER-1 (Instalación inicial) [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
smr@server-1:~$ sudo systemctl status ssh
• ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
  Active: active (running) since Tue 2023-12-26 09:28:57 UTC; 43min ago
    Docs: man:sshd(8)
           man:sshd_config(5)
  Main PID: 732 (sshd)
    Tasks: 1 (limit: 4595)
  Memory: 4.4M
  CGroup: /system.slice/ssh.service
          └─732 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

dic 26 09:44:37 server-1 sshd[1449]: Invalid user smr1 from 10.0.2.15 port 55208
dic 26 09:44:43 server-1 sshd[1449]: pam_unix(sshd:auth): check pass; user unknown
dic 26 09:44:43 server-1 sshd[1449]: pam_unix(sshd:auth): authentication failure; logname= uid=0 eu
dic 26 09:44:46 server-1 sshd[1449]: Failed password for invalid user smr1 from 10.0.2.15 port 5520
dic 26 09:44:50 server-1 sshd[1449]: pam_unix(sshd:auth): check pass; user unknown
dic 26 09:44:51 server-1 sshd[1449]: Failed password for invalid user smr1 from 10.0.2.15 port 5520
dic 26 09:44:59 server-1 sshd[1449]: Connection closed by invalid user smr1 10.0.2.15 port 55208 [p
dic 26 09:44:59 server-1 sshd[1449]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=s
dic 26 09:45:05 server-1 sshd[1452]: Accepted password for smr from 10.0.2.15 port 46416 ssh2
dic 26 09:45:05 server-1 sshd[1452]: pam_unix(sshd:session): session opened for user smr by (uid=0)
smr@server-1:~$
```



Configuración de OpenSSH Server





Configuración de OpenSSH Server

- El servido SSH se **configura** a través del fichero **/etc/ssh/sshd_config**
- Una **configuración de seguridad** importante es **cambiar el puerto** para el servidor SSH, que por **defecto** es el **puerto 22**.
- Puedes configurar **cualquier puerto que no esté siendo utilizado** por otro servicio. Lo normal es utilizar un puerto alto (mayor de 1000).
- Otra posible configuración sería **especificar los usuarios** que pueden conectarse por SSH.
- A continuación, vamos a cambiar **configurar el puerto 2200** como puerto de conexión para el servidor SSH.

```
smr@server-1:~$ sudo nano /etc/ssh/sshd_config
```

SERVER-1 (Instalación inicial) [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

GNU nano 4.8 /etc/ssh/sshd_config

\$OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp \$

This is the sshd server system-wide configuration file. See

sshd_config(5) for more information.

This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

The strategy used for options in the default sshd_config shipped with

OpenSSH is to specify options with their default value where

possible, but leave them commented. Uncommented options override the

default value.

Include /etc/ssh/sshd_config.d/*.conf

#Port 22

#AddressFamily any

#ListenAddress 0.0.0.0

#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key

#HostKey /etc/ssh/ssh_host_ecdsa_key

#HostKey /etc/ssh/ssh_host_ed25519_key

Ciphers and keying

#RekeyLimit default none

Logging

#SyslogFacility AUTH

#LogLevel INFO

Authentication:

#LoginGraceTime 2m

[Read 123 lines]

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo

^X Exit ^R Read File ^\ Replace ^U Paste Text ^T To Spell ^_ Go To Line M-E Redo

Puerto por defecto para el servicio SSH: 22

CTRL DERECHA

SERVER-1 (Instalación inicial) [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

GNU nano 4.8 /etc/ssh/sshd_config Modified

\$OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp \$

This is the sshd server system-wide configuration file. See

sshd_config(5) for more information.

This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

The strategy used for options in the default sshd_config shipped with

OpenSSH is to specify options with their default value where

possible, but leave them commented. Uncommented options override the

default value.

Include /etc/ssh/sshd_config.d/*.conf

Port 2200

#AddressFamily any

#ListenAddress 0.0.0.0

#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key

#HostKey /etc/ssh/ssh_host_ecdsa_key

#HostKey /etc/ssh/ssh_host_ed25519_key

Ciphers and keying

#RekeyLimit default none

Logging

#SyslogFacility AUTH

#LogLevel INFO

Authentication:

#LoginGraceTime 2m

[Read 123 lines]

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo

^X Exit ^R Read File ^\ Replace ^U Paste Text ^T To Spell ^_ Go To Line M-E Redo

CTRL DERECHA

Quitamos el carácter #, que indica que los que se escribe a continuación es sólo un comentario, y cambiamos el valor por 2200, que será el número de puerto que utilizará ahora el servidor SSH para sus conexiones.

CTRL + X (Salir)

SERVER-1 (Instalación inicial) [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

GNU nano 4.8 /etc/ssh/sshd_config Modified

\$OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp \$

This is the sshd server system-wide configuration file. See

sshd_config(5) for more information.

This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

The strategy used for options in the default sshd_config shipped with

OpenSSH is to specify options with their default value where

possible, but leave them commented. Uncommented options override the

default value.

Include /etc/ssh/sshd_config.d/*.conf

Port 2200

#AddressFamily any

#ListenAddress 0.0.0.0

#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key

#HostKey /etc/ssh/ssh_host_ecdsa_key

#HostKey /etc/ssh/ssh_host_ed25519_key

Ciphers and keying

#RekeyLimit default none

Logging

#SyslogFacility AUTH

#LogLevel INFO

Authentication:

#LoginGraceTime 2m

Save modified buffer?

Y Yes

N No ^C Cancel

y (Guardar cambios)

CTRL DERECHA

```
# $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

Port 2200
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
```

Intro (confirmar nombre del fichero)

File Name to Write: /etc/ssh/sshd_config

^G Get Help

M-D DOS Format

M-A Append

M-B Backup File

^C Cancel

M-M Mac Format

M-P Prepend

^T To Files


```
# $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

Port 2200
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m

smr@server-1:~$ _
```

Ya hemos modificado el
fichero de configuración del
servicio SSH

GNU nano 4.8 /etc/ssh/sshd_config

```
# $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

Port 2200
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
```

Para que los cambios tengan efectos, debemos reiniciar el servicio SSH

```
smr@server-1:~$ sudo service ssh restart _
```

```
# $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

Port 2200
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m

smr@server-1:~$ sudo service ssh restart
smr@server-1:~$
```

El servicio se ha reiniciado y
no nos muestra ningún error.



Conexión desde terminal remoto





Conexión desde terminal remoto

- Como es lógico, **para conectarnos a través del protocolo SSH a otro equipo**, necesitamos que ambas máquinas estén en la **misma red**.
- Además, necesitamos conocer las **credenciales de un usuario con permisos** para poder acceder al **equipo remoto**. Este usuario es el que utilizaremos para autenticarnos en el equipo remoto.
- Por ejemplo, supongamos que tenemos **dos máquina virtuales en la misma Red NAT**, correspondientes a nuestro **servidor** y una máquina con **Ubuntu Desktop**. En este caso, podremos conectarnos de forma remota a nuestro servidor.



Conexión desde terminal remoto

- **Para conectarnos de forma remota** a nuestro servidor, utilizamos el comando:

`ssh nombre_usuario@ip_servidor -p puerto`

- Donde:
 - **nombre_usuario**: es el usuario con el que nos vamos a autenticar en el equipo remoto. Si el usuario con el que queremos autenticarnos coincide con el que hemos utilizado para autenticarnos en nuestra terminal local, no haría falta indicarlo (`ssh @ip_servidor -p puerto`)
 - **ip_servidor**: es la dirección ip del equipo remoto al que queremos conectarnos.
 - **-p**: opción que se utiliza para especificar el puerto de conexión. Si el puerto de conexión es el 22, puerto por defecto para el servicio SSH, no sería necesaria incluir esta opción.
 - **puerto**: es el número de puerto que vamos a utilizar para la conexión SSH. Como hemos indicado, si se trata del puerto 22 por defecto, no es necesario incluir esta información.

Conexión desde terminal remoto



```
Ubuntu_2204_LTS-1 (Instalación inicial + GA) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 26 de dic 11:26
juan@smr1-VirtualBox: ~
juan@smr1-VirtualBox:~$ ssh smr@10.0.2.254 -p 2200
```

```
Ubuntu_2204_LTS-1 (Instalación inicial + GA) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 26 de dic 11:26
juan@smr1-VirtualBox: ~
juan@smr1-VirtualBox:~$ ssh smr@10.0.2.254 -p 2200
The authenticity of host '[10.0.2.254]:2200 ([10.0.2.254]:2200)'
can't be established.
ED25519 key fingerprint is SHA256:L4Rpo80ZRewuRYOAYThp/IC3MrdLueV
YOSPnzaX0eQc.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint
])? 
```

```
Ubuntu_2204_LTS-1 (Instalación inicial + GA) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 26 de dic 11:26
juan@smr1-VirtualBox: ~
juan@smr1-VirtualBox:~$ ssh smr@10.0.2.254 -p 2200
The authenticity of host '[10.0.2.254]:2200 ([10.0.2.254]:2200)'
can't be established.
ED25519 key fingerprint is SHA256:L4Rpo80ZRewuRYOAYThp/IC3MrdLueV
YOSPnzaX0eQc.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint
])? yes
```

```
Ubuntu_2204_LTS-1 (Instalación inicial + GA) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 26 de dic 11:27
juan@smr1-VirtualBox: ~
juan@smr1-VirtualBox:~$ ssh smr@10.0.2.254 -p 2200
The authenticity of host '[10.0.2.254]:2200 ([10.0.2.254]:2200)'
can't be established.
ED25519 key fingerprint is SHA256:L4Rpo80ZRewuRYOAYThp/IC3MrdLueV
YOSPnzaX0eQc.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint
])? yes
Warning: Permanently added '[10.0.2.254]:2200' (ED25519) to the l
ist of known hosts.
smr@10.0.2.254's password: 
```

```
Ubuntu_2204_LTS-1 (Instalación inicial + GA) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 26 de dic 11:27
smr@server-1: ~
* Introducing Expanded Security Maintenance for Applications.
Receive updates to over 25,000 software packages with your
Ubuntu Pro subscription. Free for personal use.

https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.
0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
New release '22.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Dec 26 09:45:05 2023 from 10.0.2.15
smr@server-1:~$
```

Conexión desde terminal remoto



```
Ubuntu_2204_LTS-1 (Instalación inicial + GA) [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Actividades  Terminal  26 de dic 11:27
smr@server-1: ~
* Introducing Expanded Security Maintenance for Applications.
  Receive updates to over 25,000 software packages with your
  Ubuntu Pro subscription. Free for personal use.

  https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.
0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
New release '22.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Dec 26 09:45:05 2023 from 10.0.2.15
smr@server-1:~$
```




Conexión desde terminal remoto

- Como puedes observar, el **prompt ha cambiado**.
 - Antes: `juan@smr1-VirtualBox:~$`
 - Ahora: `smr@server-1:~$`
- Esto indica que estamos **autenticados** con el usuario **smr** en la máquina **server-1**.
- Ahora podemos **administrar la máquina server-1** (ejecutar comandos, crear carpetas y archivos, ...) **desde** la terminal que estamos ejecutando en la máquina con **Ubuntu Desktop**.

Conexión desde terminal remoto

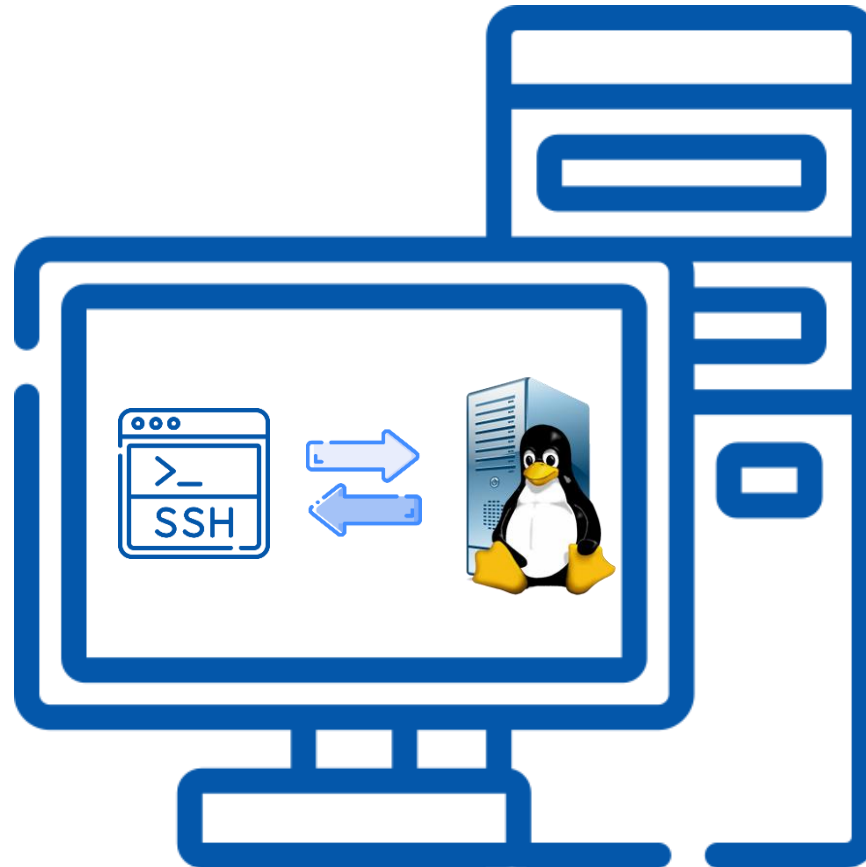


- Para **cerrar la conexión SSH** es suficiente con ejecutar el comando **exit**.
- Como puedes observar, el **prompt vuelve a cambiar** mostrando de nuevo ahora: **juan@smr1-VirtualBox:~\$**

```
Ubuntu_2204_LTS-1 (Instalación inicial + GA) [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Actividades  Terminal  26 de dic 11:36
juan@smr1-VirtualBox: ~
https://ubuntu.com/pro
Expanded Security Maintenance for Applications is not enabled.
0 updates can be applied immediately.
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
New release '22.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
Last login: Tue Dec 26 09:45:05 2023 from 10.0.2.15
smr@server-1:~$ exit
logout
Connection to 10.0.2.254 closed.
juan@smr1-VirtualBox:~$
```



Conexión desde máquina anfitriona





Conexión desde máquina anfitriona

- Una **opción muy útil** cuando trabajamos con máquinas virtuales es poder **conectarnos de forma remota** a un servidor virtual **desde nuestra máquina anfitriona**.
- Para ello, utilizamos el **protocolo SSH**, tal como hemos visto anteriormente.
- Esta conexión puede ser **incluso** desde un equipo **anfitrión** con **Windows** y un **servidor virtual Server Linux**, como vamos a mostrar a continuación.

```
C:\Users\FJCP>ssh smr@10.0.2.15 -p 2200
ssh: connect to host 10.0.2.15 port 2200: Connection timed out
C:\Users\FJCP>
```

Conexión SSH desde nuestra máquina anfitrión
(Windows 10) a máquina remota (con
adaptador de red NAT)

¿Qué ha fallado?



Conexión desde máquina anfitriona

- Para poder **conectarnos desde un terminal a un equipo remoto**, ambas máquinas deben estar en la **misma red**. Por tanto, para poder conectar nuestra máquina anfitrión a la máquina virtual de nuestro servidor, ambos equipos deberían estar en la misma red.
- Para que esto sea posible, deberíamos configurar el **adaptador de red de la máquina virtual** de nuestro servidor en modo **Adaptador puente o Adaptador sólo anfitrión**. Sin embargo, estas **opciones no son adecuadas** por:
 - **Adaptador puente**: tendremos conexión entre la máquina anfitrión y la máquina virtual de nuestro servidor pero, además, tendrán **conexión con todos los posibles equipos en la red del anfitrión**, como pueden ser todos los equipos del aula.
 - **Adaptador solo anfitrión**: tendremos una red formada sólo por el anfitrión y las posibles máquinas virtuales que se están ejecutando en el mismo, pero **no tendremos salida a internet**.



Conexión desde máquina anfitriona

- La **solución** para poder administrar nuestra máquina virtual correspondiente a nuestro servidor desde nuestra máquina anfitriona, será utilizar el **reenvío de puertos**.
- El reenvío de puertos se puede realizar en VirtualBox con una **adaptador de red configurado en modo NAT o Red NAT**.
- A continuación, vamos a mostrar **cómo se configura en ambos casos** el reenvío de puertos utilizando el **puerto modificado, 2200**, como puerto para las **conexiones SSH** de nuestra máquina virtual.

Conexión desde máquina anfitriona

Reenvío de puertos en modo NAT



Oracle VM VirtualBox Administrator

Archivo Máquina Ayuda

Herramientas

Nueva Añadir Configuración Descartar Mostrar

> Linux

> Windows

SERVER-1 (Instalación...) Corriendo

General

Nombre: SERVER-1
Sistema operativo: Ubuntu (64-bit)

Sistema

Memoria base: 4096 MB
Procesadores: 2
Orden de arranque: Óptica, Disco duro
Aceleración: Paginación anidada, Paravirtualización KVM

Pantalla

Memoria de vídeo: 16 MB
Controlador gráfico: VMSVGA
Servidor de escritorio remoto: Inhabilitado
Grabación: Inhabilitado

Almacenamiento

Controlador: IDE
Dispositivo IDE secundario 0: [Unidad óptica] Vacío
Controlador: SATA
Puerto SATA 0: SERVER-1.vdi (Normal, 50,00 GB)

Audio

Controlador de anfitrión: Predeterminado
Controlador: ICH AC97

Red

Adaptador 1: Intel PRO/1000 MT Desktop (NAT)

USB

Controlador USB: OHCI, EHCI
Filtros de dispositivos: 0 (0 activo)

Carpetas compartidas

Ninguno

Descripción

Ninguno

SERVER-1 - Configuración

General Sistema Pantalla Almacenamiento Audio Red Puertos serie USB Carpetas compartidas Interfaz de usuario

Red

Adaptador 1 Adaptador 2 Adaptador 3 Adaptador 4

☒ Habilitar adaptador de red

Conectado a: NAT

Nombre:

Avanzado

SERVER-1 - Configuración

General Sistema Pantalla Almacenamiento Audio Red Puertos serie USB Carpetas compartidas Interfaz de usuario

Red

Adaptador 1 Adaptador 2 Adaptador 3 Adaptador 4

☒ Habilitar adaptador de red

Conectado a: NAT

Nombre:

Avanzado

Tipo de adaptador: Intel PRO/1000 MT Desktop (82540EM)

Modo promiscuo: Denegar

Dirección MAC: 080027D5F6D7

☒ Cable conectado

Reenvío de puertos

Aceptar Cancelar Ayuda



Conexión desde máquina anfitriona

Reenvío de puertos en modo NAT

Reglas de reenvío de puertos

Nombre	Protocolo	IP anfitrión	Puerto anfitrión	IP invitado	Puerto invitado
Rule 1	TCP		0		0

Reglas de reenvío de puertos

Nombre	Protocolo	IP anfitrión	Puerto anfitrión	IP invitado	Puerto invitado
SSH	TCP		2222		2200

2222: puerto que vamos a utilizar en el anfitrión (puede ser cualquier que no esté siendo utilizado)
2200: puerto configurado en el servicio SSH del servidor (máquina virtual)

Aceptar Cancelar



Conexión desde máquina anfitriona

Reenvío de puertos en modo NAT

- Lo que hará este reenvío de puertos será que, cualquier conexión que se pretenda establecer a través del puerto 2222 del anfitrión, será redirigida al puerto 2200 de la máquina virtual con adaptador de red NAT.
- Como hemos configurado el **puerto 2200** para el servicio SSH en la máquina virtual, **todo lo que llegue** a la misma **a ese puerto** será gestionado por el servicio SSH del **servidor OpenSSH**.
- Por tanto, podremos establecer una **conexión SSH** entre anfitrión y servidor virtual, **sin necesidad de estar en la misma red**.
- A través de esta conexión SSH podemos **administrar nuestro servidor virtual desde el Símbolo del sistema** (Windows) o **Terminal** (Linux) de nuestro anfitrión.

```
Símbolo del sistema

C:\Users\FJCP>ssh smr@127.0.0.1 -p 2222
```

Intentamos establecer conexión SSH con el equipo local a través del puerto 2222. El reenvío de puertos enviará todos los paquetes recibidos por ese puerto al puerto 2200 de la máquina virtual con adaptador NAT.

```
Símbolo del sistema - ssh smr@127.0.0.1 -p 2222

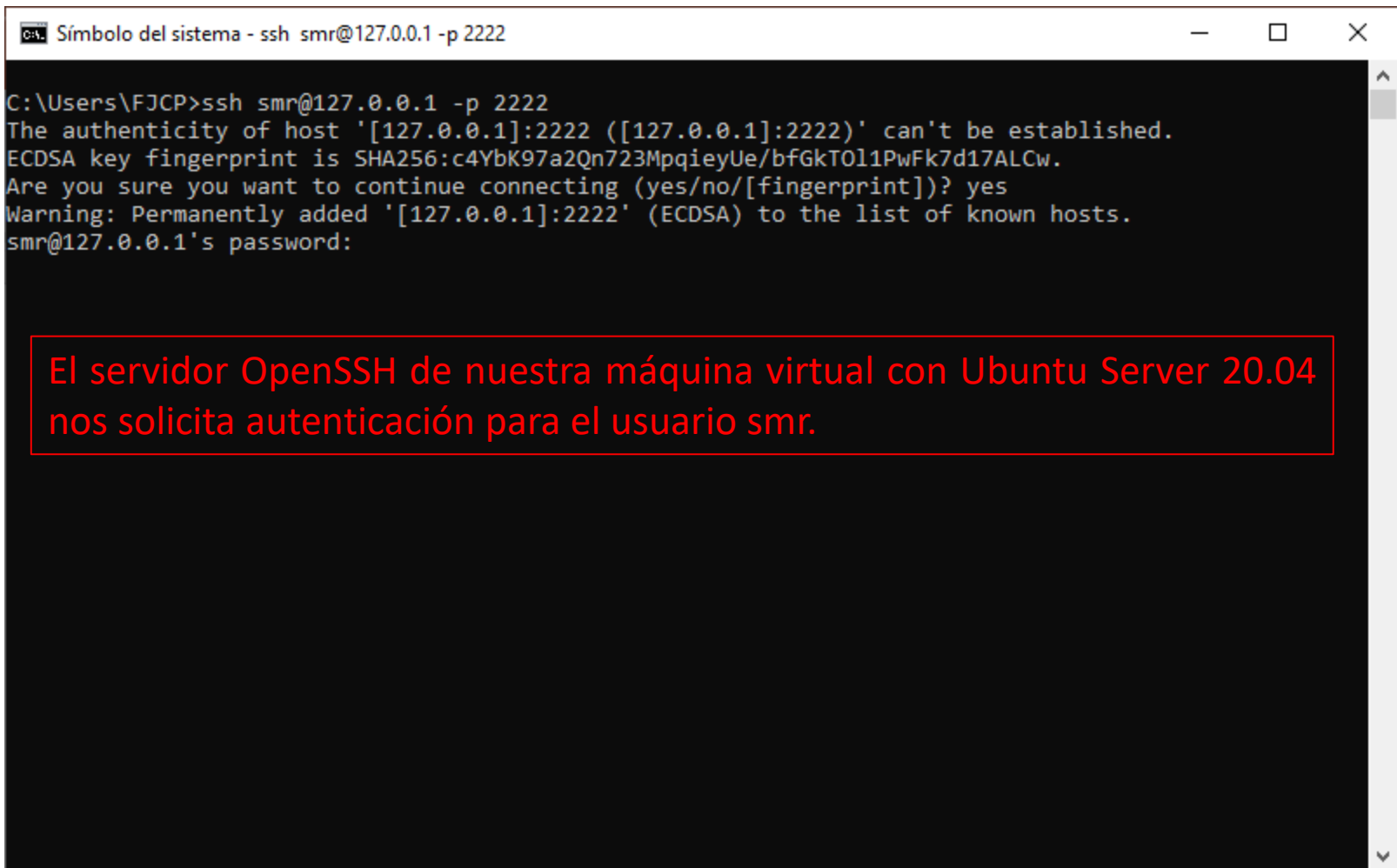
C:\Users\FJCP>ssh smr@127.0.0.1 -p 2222
The authenticity of host '[127.0.0.1]:2222 ([127.0.0.1]:2222)' can't be established.
ECDSA key fingerprint is SHA256:c4YbK97a2Qn723MpqiyeUe/bfGkT0l1PwFk7d17ALCw.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

La primera vez que realicemos conexión SSH se importan las claves y nos solicita confirmación.

```
Símbolo del sistema - ssh smr@127.0.0.1 -p 2222

C:\Users\FJCP>ssh smr@127.0.0.1 -p 2222
The authenticity of host '[127.0.0.1]:2222 ([127.0.0.1]:2222)' can't be established.
ECDSA key fingerprint is SHA256:c4YbK97a2Qn723MpqiyeUe/bfGkT0l1PwFk7d17ALCw.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

Aceptamos para poder establecer la conexión SSH.

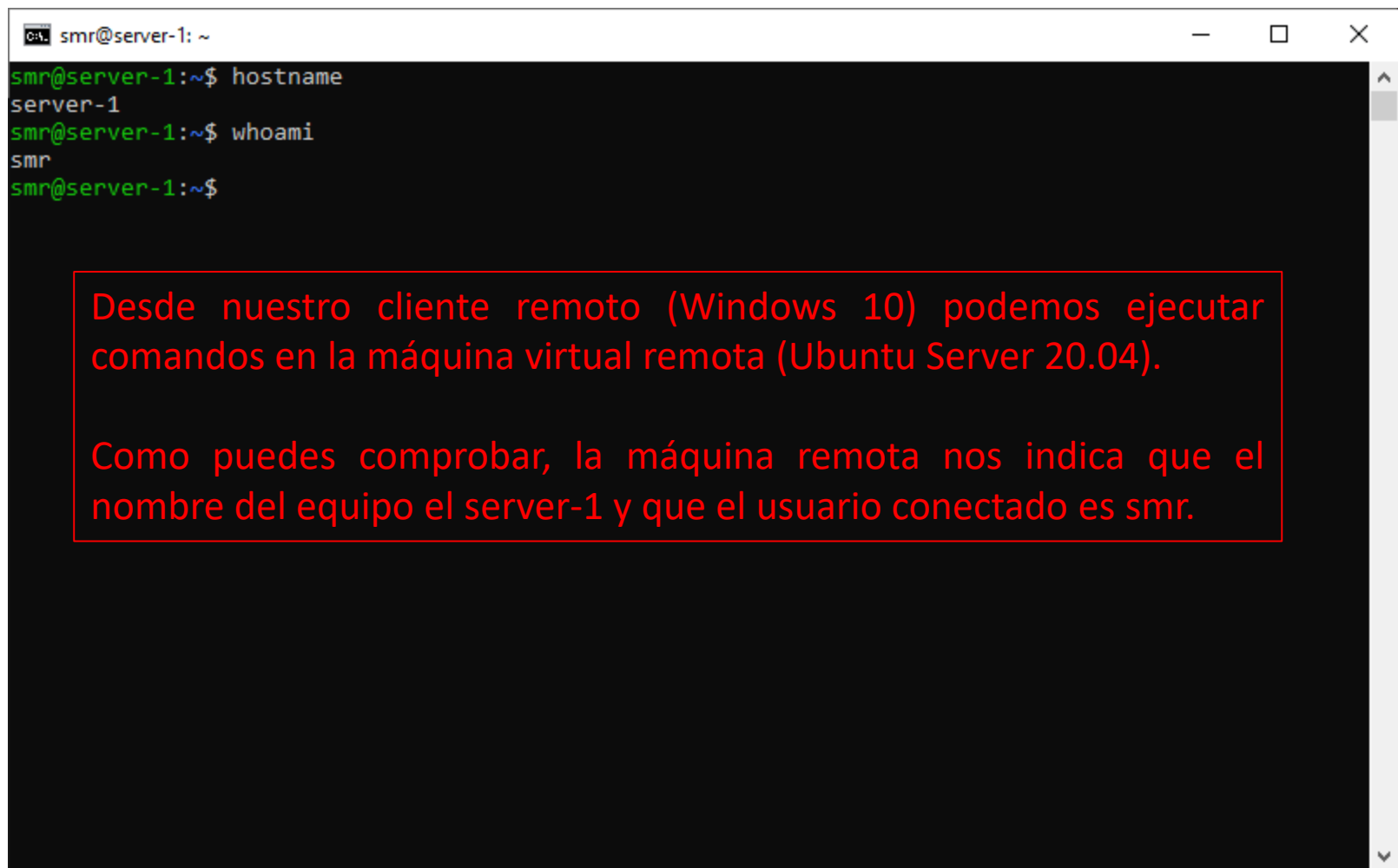


```
C:\Users\FJCP>ssh smr@127.0.0.1 -p 2222
The authenticity of host '[127.0.0.1]:2222 ([127.0.0.1]:2222)' can't be established.
ECDSA key fingerprint is SHA256:c4YbK97a2Qn723MpqiyeUe/bfGkT0l1PwFk7d17ALCw.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[127.0.0.1]:2222' (ECDSA) to the list of known hosts.
smr@127.0.0.1's password:
```

El servidor OpenSSH de nuestra máquina virtual con Ubuntu Server 20.04 nos solicita autenticación para el usuario smr.

```
smr@server-1: ~  
  
System load: 0.08      Processes: 127  
Usage of /home: 0.0% of 19.51GB  Users logged in: 1  
Memory usage: 6%      IPv4 address for enp0s3: 10.0.2.15  
Swap usage: 0%  
  
* Introducing Expanded Security Maintenance for Applications.  
Receive updates to over 25,000 software packages with your  
Ubuntu Pro subscription. Free for personal use.  
  
https://ubuntu.com/pro  
  
Expanded Security Maintenance for Applications is not enabled.  
  
0 updates can be applied immediately.  
  
Enable ESM Apps to receive additional future security updates.  
See https://ubuntu.com/esm or run: sudo pro status  
  
The list of available updates is more than a week old.  
To check for new updates run: sudo apt update  
New release '22.04.3 LTS' available.  
Run 'do-release-upgrade' to upgrade to it.  
  
Last login: Sun Dec 24 16:17:58 2023 from 10.0.2.2  
smr@server-1:~$
```

Si la autenticación es correcta
(password) la conexión queda
establecida.

A terminal window titled 'smr@server-1: ~' with standard window controls. It shows a sequence of commands and their outputs: 'hostname' returns 'server-1', and 'whoami' returns 'smr'.

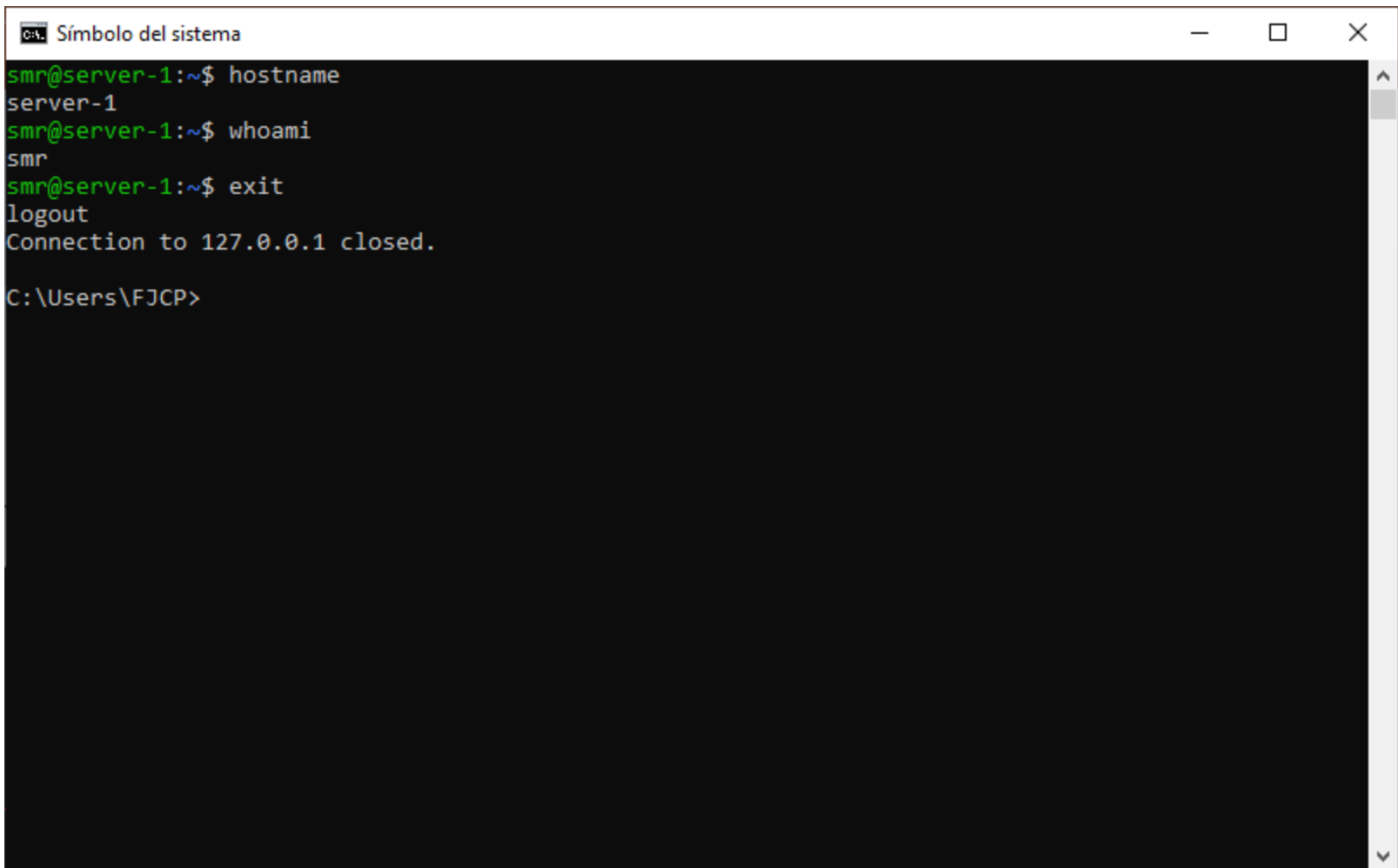
```
smr@server-1: ~  
smr@server-1:~$ hostname  
server-1  
smr@server-1:~$ whoami  
smr  
smr@server-1:~$
```

Desde nuestro cliente remoto (Windows 10) podemos ejecutar comandos en la máquina virtual remota (Ubuntu Server 20.04).

Como puedes comprobar, la máquina remota nos indica que el nombre del equipo es server-1 y que el usuario conectado es smr.

```
smr@server-1: ~  
smr@server-1:~$ hostname  
server-1  
smr@server-1:~$ whoami  
smr  
smr@server-1:~$ exit
```

Para terminar la conexión, utilizamos el comando exit



```
C:\> Símbolo del sistema
smr@server-1:~$ hostname
server-1
smr@server-1:~$ whoami
smr
smr@server-1:~$ exit
logout
Connection to 127.0.0.1 closed.
C:\Users\FJCP>
```









Conexión desde máquina anfitriona

Reenvío de puertos en modo Red NAT

- En **modo Red NAT** el reenvío de puertos se realiza en la **configuración de la red** ya que podemos tener distintas redes NAT con distintos reenvíos de puertos.
- Además, en **NAT** **no fue necesario indicar a qué equipo** se redirigiría el tráfico. Tan solo se indicó el puerto de destino en la máquina remota. Esto es lógico porque en NAT sólo tenemos un equipo y no existe posibilidad de error.
- En **Red NAT** **podemos tener múltiples equipos**, de modo que debemos indicar a qué **equipo debe redirigirse el tráfico** para la conexión SSH.

Herramientas

- > Linux
- > Windows
-  **SERVER-1** (Instalación inicial)
 Corriendo

 Crear
  Eliminar
  Propiedades

Redes solo-anfitrión Redes NAT Redes en la nube

Nombre	Prefijo IPv4	Prefijo IPv6	Servidor DHCP
RN1	192.168.200.0/24	fd17:625c:f037:a8c8::/64	Habilitado
RN2	10.0.2.0/24	fd17:625c:f037:2::/64	Habilitado

Opciones generales **Reenvío de puertos**

Nombre:

Prefijo IPv4:

☒ Habilitar DHCP

☐ Habilitar IPv6

Prefijo IPv6:

☐ Anunciar ruta por defecto IPv6

Aplicar Restaurar

ArchivoMáquinaRedAyuda

Herramientas

> Linux

> Windows

64

SERVER-1 (Instalación inicial)

Corriendo

Crear

Eliminar

Propiedades

Redes solo-anfitriónRedes NATRedes en la nube



Nombre	Prefijo IPv4	Prefijo IPv6	Servidor DHCP
RN1	192.168.200.0/24	fd17:625c:f037:a8c8::/64	Habilitado
RN2	10.0.2.0/24	fd17:625c:f037:2::/64	Habilitado

Opciones generalesReenvío de puertos



IPv4IPv6




Nombre	Protocolo	IP anfitrión	Puerto anfitrión	IP invitado	Puerto invitado

AplicarRestaurar

 **Herramientas** 

- > Linux
- > Windows

 **SERVER-1** (Instalación inicial)
 Corriendo

 Crear  Eliminar  Propiedades

- Redes solo-anfitrión Redes NAT Redes en la nube

Nombre	Prefijo IPv4	Prefijo IPv6	Servidor DHCP
RN1	192.168.200.0/24	fd17:625c:f037:a8c8::/64	Habilitado
RN2	10.0.2.0/24	fd17:625c:f037:2::/64	Habilitado

- Opciones generales Reenvío de puertos

IPv4 IPv6

Nombre	Protocolo	IP anfitrión	Puerto anfitrión	IP invitado	Puerto invitado
Rule 1	TCP		0	10.0.2.0	0

Aplicar Restaurar

Nombre	Prefijo IPv4	Prefijo IPv6	Servidor DHCP
RN1	192.168.200.0/24	fd17:625c:f037:a8c8::/64	Habilitado
RN2	10.0.2.0/24	fd17:625c:f037:2::/64	Habilitado

Debemos indicar los puertos del equipo anfitrión (2222) y del equipo virtual (2200), tal como hicimos antes.

Ahora, también hay que indicar la IP del equipo virtual con el que queremos establecer la conexión SSH. En este ejemplo suponemos que la dirección IP estática del servidor es 10.0.2.254.

IPv4




IPv6

Nombre	Protocolo	IP anfitrión	Puerto anfitrión	IP invitado	Puerto invitado
SSH	TCP		2222	10.0.2.254	2200








Aplicar

Restaurar

 **Herramientas**  

- > Linux
- > Windows

 **SERVER-1** (Instalación inicial)
 Corriendo

 Crear  Eliminar  Propiedades

- Redes solo-anfitrión Redes NAT Redes en la nube

Nombre	Prefijo IPv4	Prefijo IPv6	Servidor DHCP
RN1	192.168.200.0/24	fd17:625c:f037:a8c8::/64	Habilitado
RN2	10.0.2.0/24	fd17:625c:f037:2::/64	Habilitado

Reenvío de puertos establecidos.

- Opciones generales Reenvío de puertos

- IPv4 IPv6

Nombre	Protocolo	IP anfitrión	Puerto anfitrión	IP invitado	Puerto invitado
SSH	TCP		2222	10.0.2.254	2200



Conexión desde máquina anfitriona

Reenvío de puertos en modo Red NAT

- Una vez configurado el envío de puertos, la **forma de realizar la conexión es la misma** que hemos visto en el caso de adaptador con **configuración NAT**.