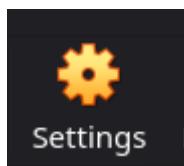


CONFIGURACIÓN DE SSH EN SERVIDORES LINUX VIRTUALES

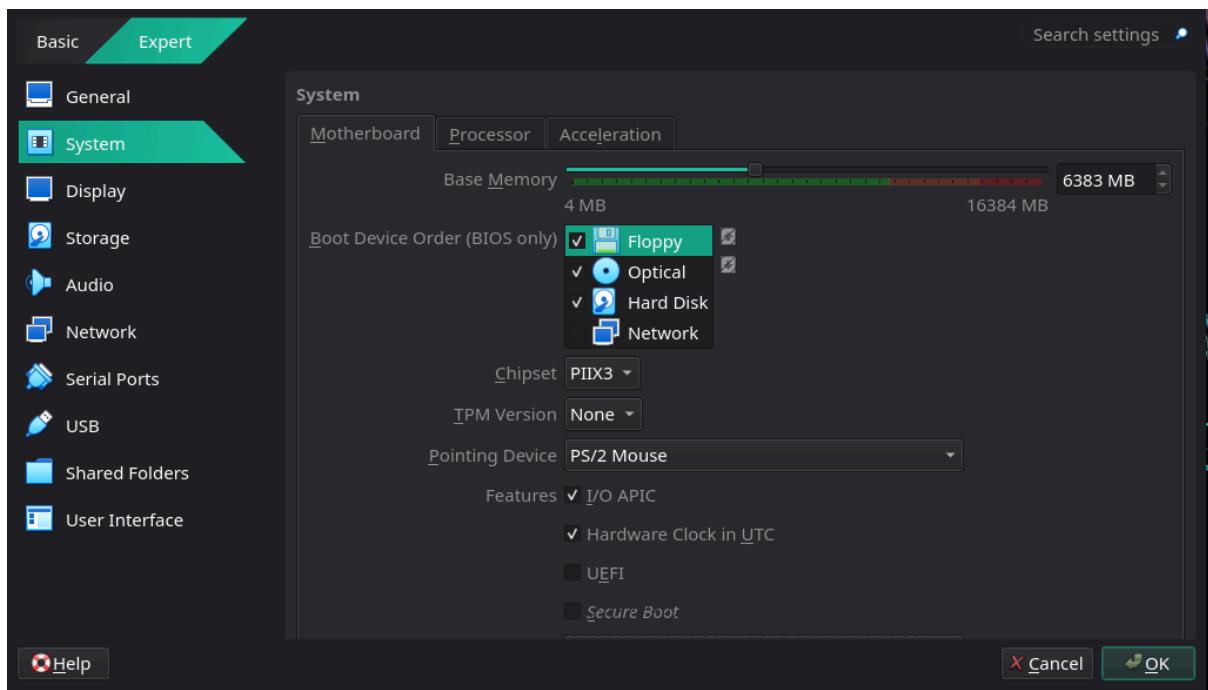
Luego de instalar servidores como Red Hat Enterprise Linux o Ubuntu, rara vez te vas a conectar desde el hypervisor/VirtualBox a los servidores para hacer configuraciones y con eso ahora vamos a configurar los servidores con un protocolo llamado SSH [Secure Shell Protocol, protocolo de red y una utilidad, cliente, software, un comando, que nos permite acceder de manera remota a un servidor]

Al configurar Ubuntu cuando pregunta si queremos instalar OpenSSH es para activar este protocolo, o al instalar Red Hat Enterprise Linux y le pusimos las herramientas de administración remota para Linux, instalara este SSH. SSH es como un pequeño servidor que se abre en el puerto 22 para que así nos podamos conectar a través de una IP, ahora vamos a VB para conectarnos a los servidores.

Ahora que vamos a encender los dos servidores a la vez, podemos bajarle los recursos a alguno, como RED HAT

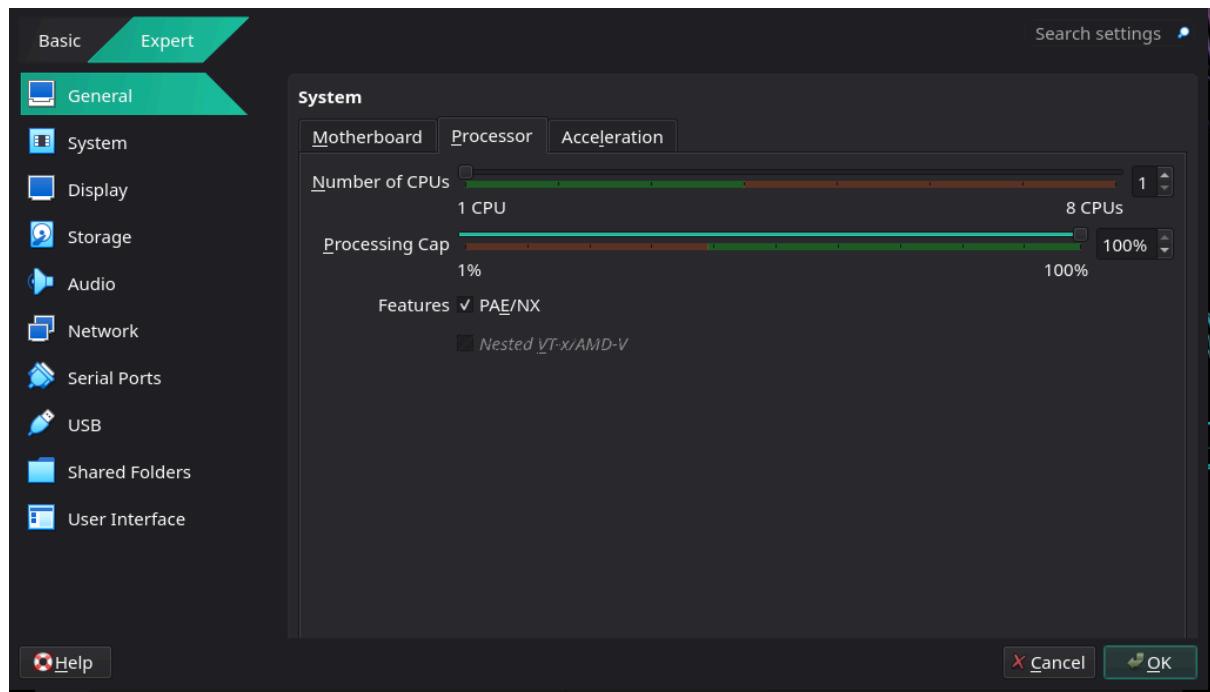


Le asignamos 6GB aproximadamente a nivel de memoria



y a nivel de procesador, bajarle los cores a 1

IMPORTANTE: ENCENDER 1 A 1 LOS SERVIDORES Y ANALIZAR SI TU HARDWARE ES COMPATIBLE, POR SI TU PC SE CRASHEA O SOBRECALIENTA



listo, iniciemos ambos servidores, en ubuntu probemos SSH escribiendo tal cual = ssh

```
ubuntu_server [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Ubuntu 24.04.3 LTS ubuntuserver tty1
Hint: Num Lock on
ubuntuserver login: cherry
Password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-88-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

System information as of Thu Dec 11 04:47:54 AM UTC 2025

System load: 0.03
Usage of /: 18.8% of 24.44GB
Memory usage: 9%
Swap usage: 0%
Processes: 114
Users logged in: 0
IPv4 address for enp0s3: 10.0.2.15
IPv6 address for enp0s3: fd17:625c:f037:2:a00:27ff:fedecdb6

Expanded Security Maintenance for Applications is not enabled.

37 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

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

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

cherry@ubuntuserver:~$ ssh
usage: ssh [-46aaCfGgKkMnqgTtVvXxYy] [-B bind_interface] [-b bind_address]
           [-c cipher_spec] [-D [bind_address]:port] [-E log_file]
           [-e escape_char] [-F configfile] [-I pkcs11] [-i identity_file]
           [-J destination] [-L address] [-l login_name] [-m mac_spec]
           [-o ctl_cmd] [-o option] [-P tag] [-p port] [-R address]
           [-S ctl_path] [-W host:port] [-w local_tun[:remote_tun]]
           destination [command [argument ...]]
           ssh [-Q query_option]
cherry@ubuntuserver:~$
```

sino, configuramos todo el servidor con el siguiente comando:
 sudo apt install openssh-server

en red hat, hacemos lo mismo, escribimos
ssh

```
Red Hat Enterprise Linux 9.6 (Plow)
Kernel 5.14.0-570.62.1.el9_6.x86_64 on an x86_64

Activate the web console with: systemctl enable --now cockpit.socket

localhost login: cherry
Password:
Last login: Wed Dec 10 20:59:07 on ttym1
[cherry@localhost ~]$ ssh
usage: ssh [-t6AuCfGgKkMnqsTtUXXYy] [-B bind_interface]
           [-b bind_address] [-c cipher_spec] [-D [bind_address:]port]
           [-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]
           [-i identity_file] [-J [user@]host[:port]] [-L address]
           [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
           [-Q query_option] [-R address] [-S ctl_path] [-W host:port]
           [-w local_tun[:remote_tun]] destination [command]

You can find some explanations for typical errors at this link:
  https://red.ht/support_rhel_ssh
[cherry@localhost ~]$
```

ahora si queremos verificar específicamente que el servicio está corriendo, usamos el comando

systemctl

esto es para monitorear procesos, ver status de un proceso, específicamente de DEMONIOS

lo que necesitamos específicamente es ver si esta corriendo ese demonio de SSH con el siguiente comando

systemctl status sshd

a 'ssh' le agregamos la 'd' al final, para especificar que es un demonio, ya que no se llama simplemente 'ssh' como tal

```
[cherry@localhost ~]$ 
[cherry@localhost ~]$ 
[cherry@localhost ~]$ systemctl status sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: enabled)
   Active: active (running) since Wed 2025-12-10 22:44:10 CST; 15min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
 Main PID: 795 (sshd)
   Tasks: 1 (limit: 37475)
     Memory: 2.9M
        CPU: 10ms
      CGroup: /system.slice/sshd.service
              └─795 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Dec 10 22:44:10 localhost.localdomain systemd[1]: Starting OpenSSH server daemon...
Dec 10 22:44:10 localhost.localdomain sshd[795]: Server listening on 0.0.0.0 port 22.
Dec 10 22:44:10 localhost.localdomain sshd[795]: Server listening on :: port 22.
Dec 10 22:44:10 localhost.localdomain systemd[1]: Started OpenSSH server daemon.
[cherry@localhost ~]$ _
```

con esto podemos ver que está corriendo y los logs, así como tambien nos dice que el servidor está escuchando en el puerto 22

LISTO, significa que en RED HAT el servicio está corriendo

ahora verifiquemos en ubuntu

Jelena Palavecino
student • hace un año

Si cuando ejecutan `systemctl status sshd` en ubuntu y les aparece el error **Unit sshd.service could not be found**. prueben primero fijándose si OpenSSH está instalado con :

```
dpkg -l | grep openssh
```Si no aparece alguna salida relacionada con
openssh-server, significa que no está instalado.
```

Entonces, toca instalarlo con :

```
```js
sudo apt install openssh-server
```Una vez instalado, verifiquen el estado del
servicio con:
```

```
```js
sudo apt install openssh-server
```Si les aparece así (disabled):
```

Tienen que habilitarlo con el comando:

```
```js
sudo systemctl start ssh
sudo systemctl enable ssh
```Y listo una vez hecho esto, ejecuten de nuevo
`systemcl status sshd` y ya no les a a salir el
error. :)
```

```
cherry@ubuntuserver:~$ systemctl status sshd
● ssh.service - OpenBSD Secure Shell server
 Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
 Active: active (running) since Thu 2025-12-11 05:23:34 UTC; 1min 10s ago
TriggeredBy: ● ssh.socket
 Docs: man:sshd(8)
 man:ssh_config(5)
 Main PID: 1326 (sshd)
 Tasks: 1 (limit: 2267)
 Memory: 2.1M (peak: 2.3M)
 CPU: 28ms
 CGroup: /system.slice/ssh.service
 └─1326 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Dec 11 05:23:34 ubuntuserver systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Dec 11 05:23:34 ubuntuserver sshd[1326]: Server listening on 0.0.0.0 port 22.
Dec 11 05:23:34 ubuntuserver sshd[1326]: Server listening on :: port 22.
Dec 11 05:23:34 ubuntuserver systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
cherry@ubuntuserver:~$ _
```

y listo tambien en los logs de la parte de abajo aparece que esta escuchando en el puerto 22

y listo, ahora accederemos a cada uno de esos servicios

IMPORTANTE: hacer la conexion de puentes, porque facilita muchas cosas a nivel local, sobre todo si nos queremos conectar

ip address

con esto compartimos la misma interfaz que tenemos de red en nuestra computadora, de nuestro host a nuestras maquinas virtuales

```
cherry@ubuntuserver:~$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
 link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
 inet 127.0.0.1/8 scope host lo
 valid_lft forever preferred_lft forever
 inet6 ::1/128 scope host noprefixroute
 valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
 link/ether 08:00:27:de:cdb6 brd ff:ff:ff:ff:ff:ff
 inet 10.0.2.15/24 metric 100 brd 10.0.2.255 scope global dynamic enp0s3
 valid_lft 82926sec preferred_lft 82926sec
 inet6 fd17:625c:f037:2:a00:27ff:fedecdb6/64 scope global dynamic mngtmpaddr noprefixroute
 valid_lft 86216sec preferred_lft 14216sec
 inet6 fe80::a00:27ff:fedecdb6/64 scope link
 valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
 link/ether 08:00:27:2f:17:8a brd ff:ff:ff:ff:ff:ff
 inet 192.168.1.26/24 metric 100 brd 192.168.1.255 scope global dynamic enp0s8
 valid_lft 82928sec preferred_lft 82928sec
 inet6 2800:98:1a0c:193:a00:27ff:fe2f:178a/64 scope global dynamic mngtmpaddr noprefixroute
 valid_lft 258963sec preferred_lft 172563sec
 inet6 fe80::a00:27ff:fe2f:178a/64 scope link
 valid_lft forever preferred_lft forever
cherry@ubuntuserver:~$
```

el dispositivo 1, que es el loopback que es un dispositivo virtual

el que estamos buscando empieza con 'en' que es el 2, y dice broadcast multicast, abajo luego de link/ether, aparece una linea que dice 'inet' la cual es basicamente la nuestra IP de nuestra intranet.

```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
 link/ether 08:00:27:de:cdb6 brd ff:ff:ff:ff:ff:ff
 inet 10.0.2.15/24 metric 100 brd 10.0.2.255 scope global dynamic enp0s3
 valid_lft 82926sec preferred_lft 82926sec
 inet6 fd17:625c:f037:2:a00:27ff:fedecdb6/64 scope global dynamic mngtmpaddr noprefixroute
 valid_lft 86216sec preferred_lft 14216sec
 inet6 fe80::a00:27ff:fedecdb6/64 scope link
 valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
```

observemos la IP

```
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
 link/ether 08:00:27:2f:17:8a brd ff:ff:ff:ff:ff:ff
 inet 192.168.1.26/24 metric 100 brd 192.168.1.255 scope global dynamic enp0s8
 valid_lft 82928sec preferred_lft 82928sec
 inet6 2800:98:1a0c:193:a00:27ff:fe2f:178a/64 scope global dynamic mngtmpaddr noprefixroute
 valid_lft 258963sec preferred_lft 172563sec
 inet6 fe80::a00:27ff:fe2f:178a/64 scope link
 valid_lft forever preferred_lft forever
cherry@ubuntuserver:~$ _
```

SSH además de que es un protocolo de red, también es un cliente, y para acceder a él, podemos, desde la terminal de nuestra computadora [fuera de virtual box] con esta IP que nos dió, podremos acceder con este comando

ssh username@IP

[que veremos a continuacion]

nuestra terminal [que es la linea de comandos] del sistema operativo ya tiene un cliente de SSH instalado por defecto

para conectarnos a SSH a nuestro servidor, es poner nuestras credenciales de usuario e IP:

```
~ (36.334s)
ssh cherry@192.168.1.26

~ (36.334s)
ssh cherry@192.168.1.26

ED25519 key fingerprint is SHA256:Mih1lGv9odSMII3uMriWQWwdTJ49ylq3LUhCiYo5yzo.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.26' (ED25519) to the list of known hosts.
cherry@192.168.1.26's password:

cherry@ubuntuserver:~ (0.104s)
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-88-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

System information as of Thu Dec 11 06:00:02 AM UTC 2025

System load: 0.01
Usage of /: 19.0% of 24.44GB
Memory usage: 11%
Swap usage: 0%
Processes: 120
Users logged in: 1

✉️ cherry@ubuntuserver 📂 ~
Warp anything e.g. Deploy my React app to Vercel and set up environment variables

Expanded Security Maintenance for Applications is not enabled.

43 updates can be applied immediately.
2 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

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

con eso podemos logearnos de manera remota a un servidor linux

EN LA INDUSTRIA asi te conectas a terminales o servidores remotos

Te darán un usuario, una IP y hay que poner luego la contraseña

Hay otros mecanismos de autenticación que puedes investigar, como configurar una llave SSH para repositorios de github y asi es como servidores linux realmente están en todo

PARA SABER QUE YO REALMENTE ESTOY EN MI SERVIDOR

- vamos a crear un archivo

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

cherry@ubuntuserver:~ (0.018s)
touch hello_remote.txt

cherry@ubuntuserver ~ (0.016s)
pwd
/home/cherry

cherry@ubuntuserver ~ (0.02s)
ls
hello_remote.txt
```

y podremos ver que detectó nuestro archivo y todos los demás

```
cherry@ubuntuserver ~ (0.018s)
ll
total 36
drwxr-x--- 4 cherry cherry 4096 Dec 11 06:18 ./
drwxr-xr-x 3 root root 4096 Dec 6 06:49 ../
-rw----- 1 cherry cherry 30 Dec 11 06:19 .bash_history
-rw-r--r-- 1 cherry cherry 220 Mar 31 2024 .bash_logout
-rw-r--r-- 1 cherry cherry 3771 Mar 31 2024 .bashrc
drwx----- 2 cherry cherry 4096 Dec 6 06:53 .cache/
-rw-rw-r-- 1 cherry cherry 0 Dec 11 06:18 hello_remote.txt
-rw----- 1 cherry cherry 20 Dec 11 05:24 .lesshst
-rw-r--r-- 1 cherry cherry 807 Mar 31 2024 .profile
drwx----- 2 cherry cherry 4096 Dec 6 06:50 .ssh/
-rw-r--r-- 1 cherry cherry 0 Dec 11 05:17 .sudo_as_admin_successful
```

ahora si me voy a la sesión que tengo en mi servidor virtualizado y revisamos si tenemos el archivo que hicimos desde nuestra computadora, fuera del hypervisor

```
0]cherry@ubuntuserver:~$ ls
hello_remote.txt
96]cherry@ubuntuserver:~$ ls -la
total 36
 (drwxr-x--- 4 cherry cherry 4096 Dec 11 06:18 .
 drwxr-xr-x 3 root root 4096 Dec 6 06:49 ..
 -rw----- 1 cherry cherry 33 Dec 11 06:19 .bash_history
 -rw-r--r-- 1 cherry cherry 220 Mar 31 2024 .bash_logout
 -rw-r--r-- 1 cherry cherry 3771 Mar 31 2024 .bashrc
 drwx----- 2 cherry cherry 4096 Dec 6 06:53 .cache
 -rw-rw-r-- 1 cherry cherry 0 Dec 11 06:18 hello_remote.txt
 -rw----- 1 cherry cherry 20 Dec 11 05:24 .lesshist
 -rw-r--r-- 1 cherry cherry 807 Mar 31 2024 .profile
 drwx----- 2 cherry cherry 4096 Dec 6 06:50 .ssh
 -rw-r--r-- 1 cherry cherry 0 Dec 11 05:17 .sudo_as_admin_successful
cherry@ubuntuserver:~$ _
```

aparecerá nuestro archivo

Así accedemos de manera “remota” [entre comillas porque esta configuración es local]  
Para que un servidor linux pueda funcionar a lo largo del internet se debe hacer una  
configuración a nivel de IP pública o asignársele una IP a la cual se le pueda acceder y  
obviamente de SSH se pueden hacer muchas configuraciones a nivel de firewall, usuarios...  
Puede haber una serie específica de SSH por su amplitud

En este caso se explorará lo básico para ver como se conecta al servidor

ahora vamos a hacer las pruebas con RED HAT, haciendo exactamente lo mismo

## CONEXIÓN EN RED HAT

Vamos a buscar la dirección IP de nuestra máquina con  
ip address

```
[cherry@localhost ~]$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
 link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
 inet 127.0.0.1/8 scope host lo
 valid_lft forever preferred_lft forever
 inet6 ::1/128 scope host
 valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
 link/ether 08:00:27:56:59:e3 brd ff:ff:ff:ff:ff:ff
 inet 192.168.1.28 brd 192.168.1.255 scope global dynamic noprefixroute enp0s3
 valid_lft 79897sec preferred_lft 79897sec
 inet6 2800:98:1a0c:193:a00:27ff:fe56:59e3/64 scope global dynamic noprefixroute
 valid_lft 259117sec preferred_lft 122717sec
 inet6 fe80::a00:27ff:fe56:59e3/64 scope link noprefixroute
 valid_lft forever preferred_lft forever
[cherry@localhost ~]$ _
```

Esta asignación de IPs es normalmente con DHCP, que son IPs dinámicas locales, basicamente es la forma en que nuestro computador las asigna

```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
 link/ether 08:00:27:56:59:e3 brd ff:ff:ff:ff:ff:ff
 inet 192.168.1.28/24 brd 192.168.1.255 scope global d
 valid_lft 79897sec preferred_lft 79897sec
```

En este caso es 192.168.1.28 en la puerta 24

Nos conectamos desde nuestra computadora, fuera del hypervisor

```
~ (15.929s)
ssh cherry@192.168.1.28
The authenticity of host '192.168.1.28 (192.168.1.28)' can't be established.
ED25519 key fingerprint is SHA256:l60cFJH5zykRAEcXdfw3TG3zT9LxHefnGT6HitI29wU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.28' (ED25519) to the list of known hosts.
cherry@192.168.1.28's password:
```

el mensaje es que si se desea establecer la firma SSH en este host para que sepan que accediste [escribimos: yes]

luego ingresamos nuestra clave y listo, estamos en nuestro servidor directamente de RED HAT

probamos creando un archivo remoto

```
cherry@localhost.localdomain:~ (0.02s)
touch rhel_remote.txt

cherry@localhost.localdomain ~ (0.023s)
ls -la

total 20
drwx----- 2 cherry cherry 122 Dec 11 00:42 .
drwxr-xr-x 3 root root 20 Dec 10 20:27 ..
-rw----- 1 cherry cherry 75 Dec 11 00:42 .bash_history
-rw-r--r-- 1 cherry cherry 18 Feb 15 2024 .bash_logout
-rw-r--r-- 1 cherry cherry 141 Feb 15 2024 .bash_profile
-rw-r--r-- 1 cherry cherry 492 Feb 15 2024 .bashrc
-rw----- 1 cherry cherry 20 Dec 10 23:00 .lessht
-rw-r--r-- 1 cherry cherry 0 Dec 11 00:42 rhel_remote.txt
```

Luego verificamos en la maquina virtual con el comando

```
ls -l
```

```
[cherry@localhost ~]$ ls -l
total 0
-rw-r--r-- 1 cherry cherry 0 Dec 11 00:42 rhel_remote.txt
[cherry@localhost ~]$
```

y ya tenemos nuestro RHEL remoto

ya hemos configurado nuestros servidores linux de manera “remota” [en comillas porque solo alcanzan al dominio de nuestra máquina, osea que si queremos conectarnos de la maquina de nuestro vecino a través de internet, no va a funcionar, pero es una buena práctica para irse familiarizando en cómo sucede EN LA INDUSTRIA, para acceder a un servidor remoto

EL ESTÁNDAR EN LA INDUSTRIA ES SSH, aunque existen mas formas para acceder a un servidor remoto. Existen software de acceso remoto, directamente a nivel de interfaz gráfica como TEAMVIEWER, que es muy usado entre SYS ADMINS, en general existe mucho software para resolver el problema del acceso remoto

Otra forma de poder acceder de manera remota a un servidor, es por ejemplo, si te metes a tu GOOGLE CLOUD, o a tu CONSOLA DE AZURE, o a la CONSOLA DE AMAZON, estas incluso ya tienen terminales directamente a nivel de navegador, osea que como tu ya estás logueado, simplemente ya tienes acceso a la instancia o al servidor que hayas creado

Y LISTO, CON ESTO YA SE TIENE UNA IDEA DE COMO LOGEAR A UN SERVIDOR REMOTO

CUANDO APAGAMOS CON  
poweroff

en la terminal fuera del hypervisor aparece algo como

```
Broadcast message from cherry@localhost on tty1 (Thu 2025-12-11 00:56:12 CST):
The system will power off now!
Connection to 192.168.1.28 closed by remote host.
Connection to 192.168.1.28 closed.
```

```
Broadcast message from cherry@ubuntuserver on tty1 (Thu 2025-12-11 06:56:23 UTC):
The system will power off now!
Connection to 192.168.1.26 closed by remote host.
Connection to 192.168.1.26 closed.
```

que se desconecta