

UNIVERSIDAD DE COSTA RICA

FACULTAD DE INGENIERÍA

ESCUELA DE CIENCIAS DE LA
COMPUTACIÓN E INFORMÁTICA

CI-0138 – Integración de Infraestructura de TI
Prof. Ricardo Villalón

Infraestructura de red de un servicio de TI

Elaborado por:

Hellen Fernández Jiménez B42525

I Semestre del 2021

Índice

Descripción del servicio	2
1. Diseño de infraestructura de red de un servicio de TI	2
1.1.Direccionamiento ip	2
1.2 Topología	3
2. Actualizar ESXi 6.7	3
3. Imagen base	10
1. Descripción de la imagen base	10
2. Prerrequisitos de instalación	10
3. Localización del equipo.	10
4. Características de hardware del equipo.	10
5. Pasos realizados para llegar a la imagen base	10
5.1 Cambie el hostname de la máquina	10
5.2 Asigne una dirección ip	12
5.3 Actualice el sistema	17
5.4 Instale el editor de texto nano	17
5.5 Instale net-tools	18
5.6 Instale iptables	19
5.7 Deshabilite el servicio remoto para usuario root	20
6. Agregue una interfaz a una máquina virtual	23
7. Exporte la imagen base	34
8. Cree los servidores de acuerdo a la imagen base	35
4. Cree red privada	38
5. Implementación de servicios	40
Instale apache	40
2. Instale MariaDB	41
3. Configure MariaDB	43
4.Instale PHP	49
5. Instale Wordpress	51
7. Configure Wordpress	53
8. Gestione de Wordpress	56
6. Gestión y restricción de accesos	59
1.Active iptables	59
2. Configure iptables en Base de datos	61
3. Configure iptables en servidor apache	62

Infraestructura de red de un servicio de TI

Descripción del servicio

Este documento está realizado con la intención de describir el diseño, instalación y configuración de la infraestructura de un servicio de TI mediante máquinas Centos7 aprovisionadas mediante un servicio de almacenamiento SAN que fue desarrollado anteriormente así como almacenamiento NAS, ambos en ESXi 6.7.3. En este trabajo, se va a brindar un servicio web en Wordpress utilizando un servidor apache con su respectiva base de datos MariaDB. Este servicio va a tener distintos niveles de comunicación entre ellos, hacia los clientes y de gestión, lo cual va a estar realizado bajo un direccionamiento específico de acuerdo al diseño propuesto.

1. Diseño de infraestructura de red de un servicio de TI

1.1. Direccionamiento ip

Para la establecer el servicio, se plantea el siguiente direccionamiento ip para los servicios ofrecidos:

Base de datos		
Interfaz	Direcciones ip	Servicio
ens224	192.168.5.2	Conexión privada con servidor apache
ens192	172.24.133.5	Configurada para gestión SSH

Servidor Web		
Interfaz	Direcciones IP	Servicio
ens224	192.168.5.3	Conexión privada con servidor de base de datos.
ens192	172.24.133.7	Dirección para servidor apache.
ens256	172.24.133.6	Exclusiva para gestión a través de SSH

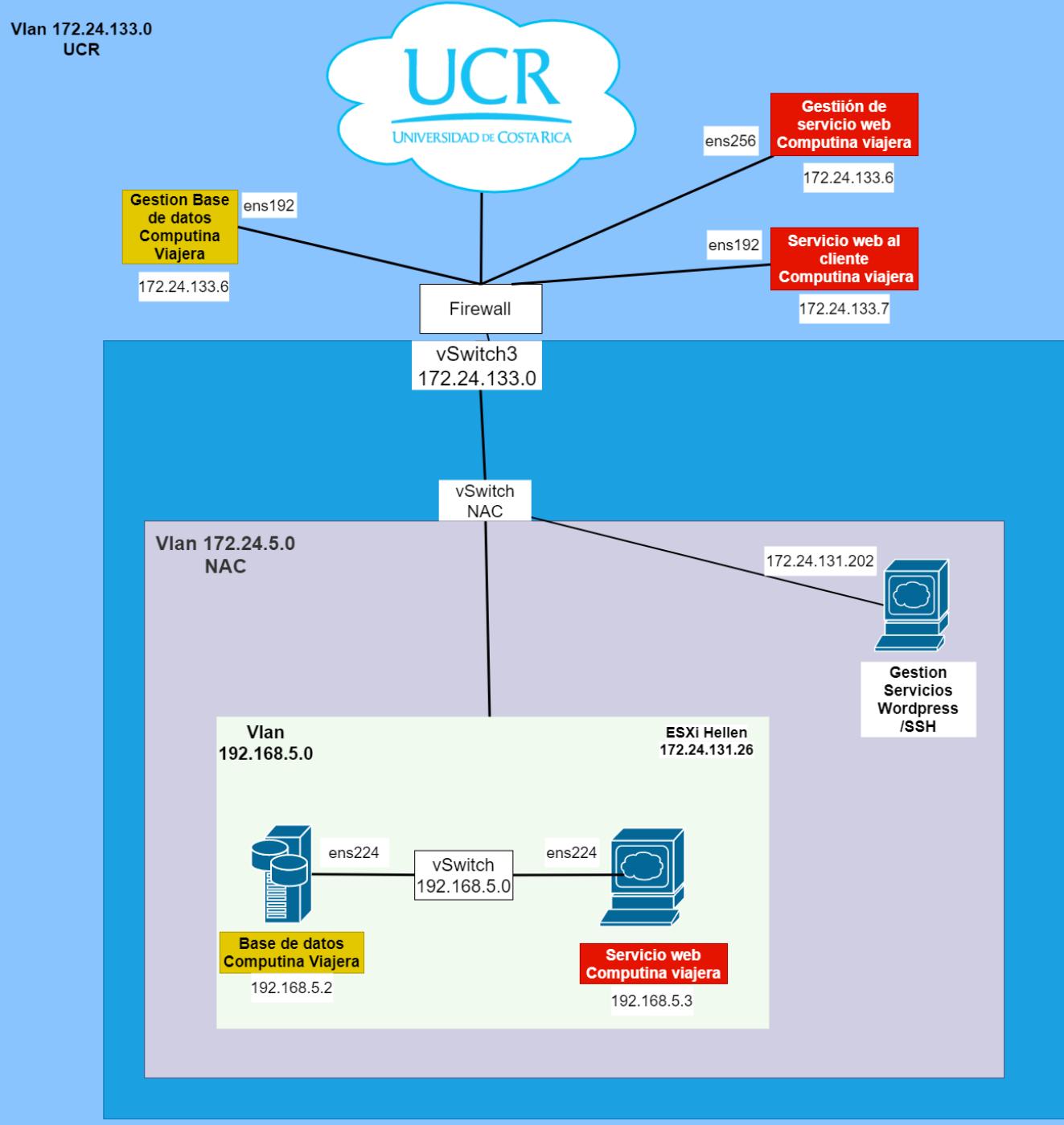
Para gestionar el servicio de Wordpress se estará utilizando una máquina reservada en el VCL de tipo Ubuntu, con nombre de reserva "soredes".

Máquina para gestión de Wordpress	
Direcciones IP	Servicio
172.24.131.202	Máquina para gestión de Wordpress.

1.2 Topología

Se plantea la siguiente topología para la implementación de los servicios de acuerdo al direccionamiento antes planteado. Aclaración: los servicios que tienen el mismo color: rojo o amarillo, corresponden a una misma máquina física, esto quiso representar en qué lugar del diagrama se encuentra el direccionamiento..

Arquitectura mini centro de datos con sus servicios



2. Actualizar ESXi 6.7

Actualizar el ESXi es algo esencial ya que las actualizaciones proveen una mejor protección con respecto a la versión base ya que se corrigen errores y vulnerabilidades que surgieron en la versión base instalada.

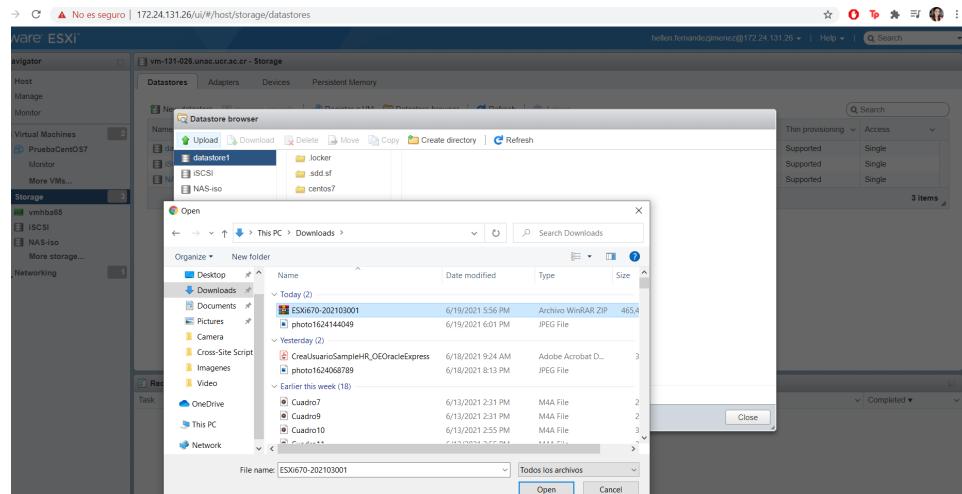
1. Entrar al esxi y poner en modo mantenimiento el equipo, además apagar todas las máquinas virtuales.
2. Verificar la versión de esxi que está en uso.

3. Crear una cuenta de Vmware.
4. Iniciar sesión y acceder al siguiente enlace, buscar el parche para la versión de esxi 6.7.0 que es la que está instalada actualmente y descargarlo.

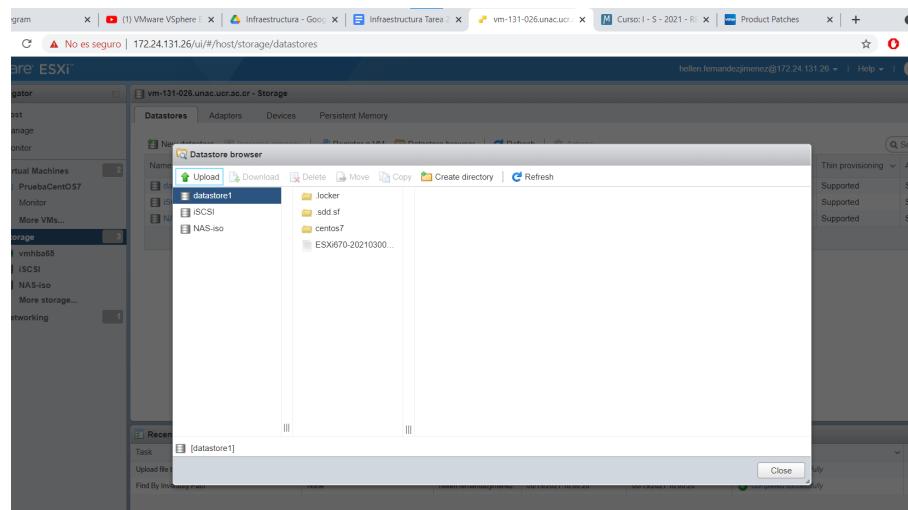
<https://my.vmware.com/group/vmware/patch#search>

5. Ir a Storage, Datastore browser.

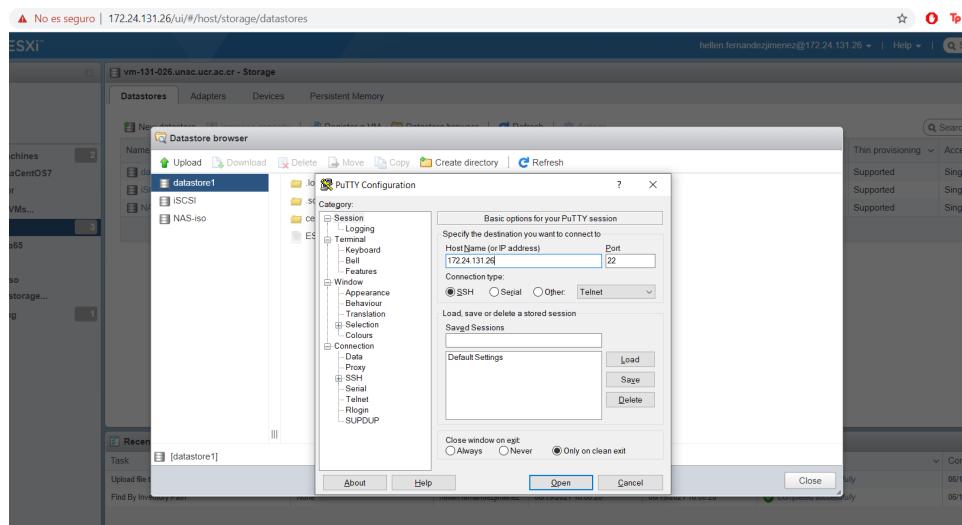
6. Seleccionar upload y seleccionar el zip que contiene el parche.



7. Se verá de la siguiente forma:



8. Posteriormente, se inicia una sesión de SSH desde putty hacia el ESXi.



9. Se inicia sesión con las credenciales de esxi:

```
172.24.131.26 - PuTTY

login as: hellen.fernandezjimenez
Keyboard-interactive authentication prompts from server:
Password:
End of keyboard-interactive prompts from server
Access denied
Keyboard-interactive authentication prompts from server:
Password:
End of keyboard-interactive prompts from server
the time and date of this login have been sent to the system logs.

WARNING:
All commands run on the ESXi shell are logged and may be included in
support bundles. Do not provide passwords directly on the command line.
Most tools can prompt for secrets or accept them from standard input.

VMware offers supported, powerful system administration tools. Please
see www.vmware.com/go/sysadmintools for details.

The ESXi Shell can be disabled by an administrative user. See the
Sphere Security documentation for more information.
could not chdir to home directory /home/hellen.fernandezjimenez: No such file or
directory
hellen.fernandezjimenez@vm-131-026:~] 
```

10. Verificar el nombre del profile con el comando:

```
esxcli software sources profile list -d  
/vmfs/volumes/datastore1/ESXi670-202103001.zip
```

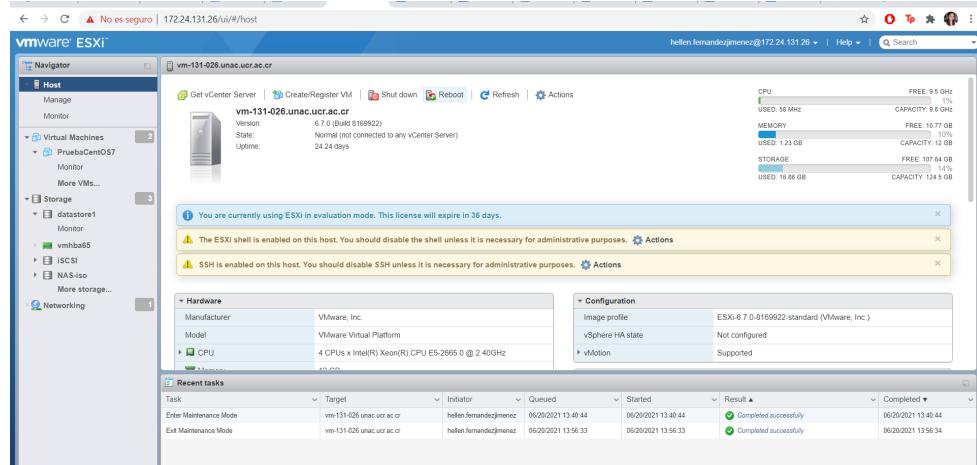
Cabe aclarar que ESXi670-202103001.zip es el nombre del zip del parche que fue cargado al storage1 desde la interfaz gráfica.

[hellen.fernandezjimenez@vm-131-026:~] esxcli software sources profile list -d /vmfs/volumes/datastore1/ESXi 670-202103001.zip				
Name	Vendor	Acceptance Level	Creation Time	Modification Time
ESXi-6.7.0-20210301001s-standard	VMware, Inc.	PartnerSupported	2021-03-04T10:17:40	2021-03-04T10:17:40
ESXi-6.7.0-20210301001s-no-tools	VMware, Inc.	PartnerSupported	2021-03-04T10:17:40	2021-03-04T10:17:40
ESXi-6.7.0-20210304001-standard	VMware, Inc.	PartnerSupported	2021-03-04T10:17:40	2021-03-04T10:17:40
ESXi-6.7.0-20210304001-no-tools	VMware, Inc.	PartnerSupported	2021-03-04T10:17:40	2021-03-04T10:17:40

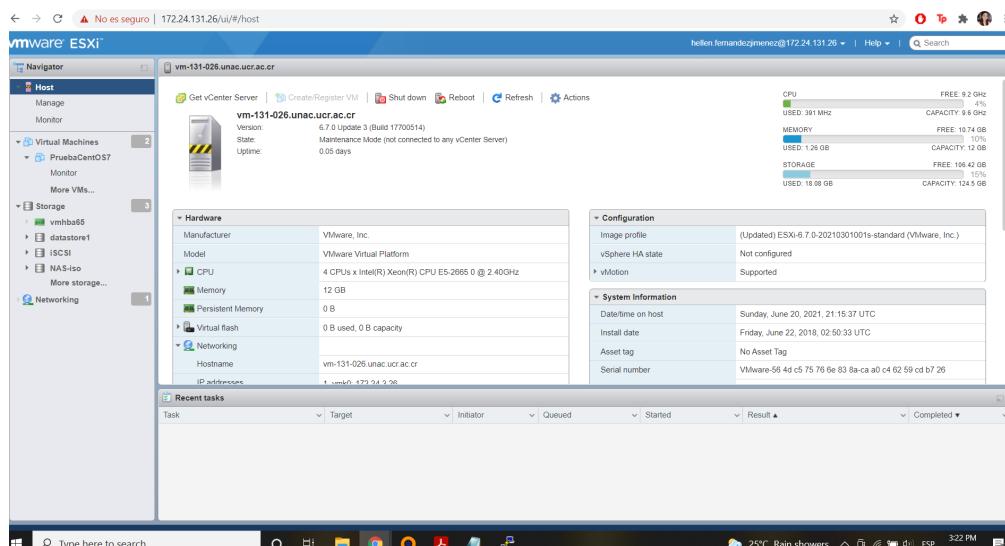
11. Para actualizar con el parche que fue descargado se utiliza el comando:

```
esxcli software profile update -d  
/vmfs/volumes/datastore1/ESXi670-202103001.zip -p  
ESXi-6.7.0-20210301001s-standard
```

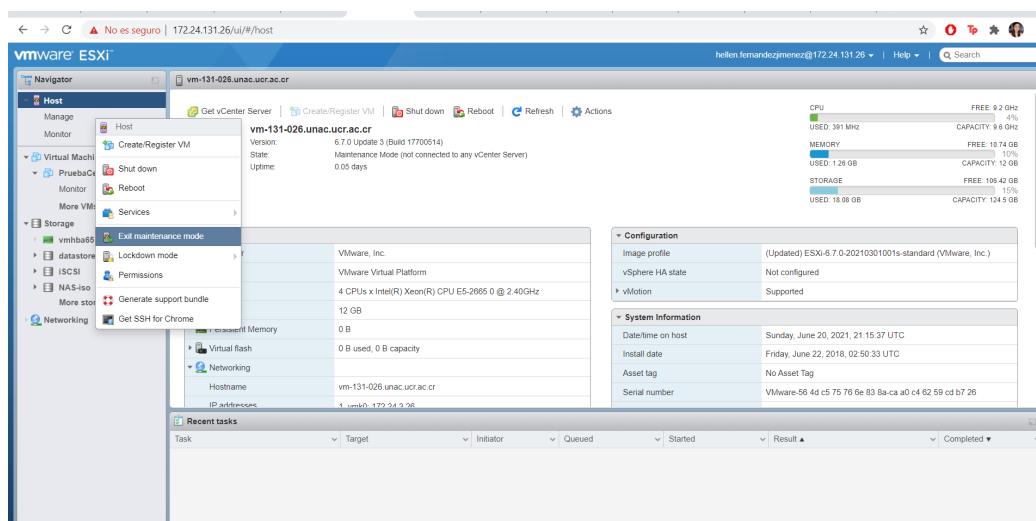
12. Se hace reboot.



13. Al ingresar nuevamente se puede observar como cambió la versión a 6.7.0 Update3



14. Se sale del modo mantenimiento y ya estaría instalada la última versión del parche publicada para esxi versión 6.7.



En este momento el estado de los virtual switches es el siguiente:

Name	Port groups	Uplinks	Type
vSwitch0	2	1	Standard vSwitch
vSwitch1	1	1	Standard vSwitch
vSwitch2	1	2	Standard vSwitch

En el cual se encuentran las vmnic2 y la vmnic3

Se le va a eliminar una de las nics al vSwitch2 para separar los accesos que tendrán los port groups en esos switches.

Para eso se da click en Edit settings y se verá de la siguiente forma y se dará click a la x del Uplink 1, porque en este caso se quiere que sólo esté la vmnic2 como Uplink:

vSwitch2

Add uplink | Edit settings | Refresh | Actions

vSwitch2

Type: Standard vSwitch
Port groups: 1
Uplinks:

Edit standard virtual switch - vSwitch2

Add uplink

MTU	1500
Uplink 1	vmnic3 - Up, 10000 mbps
Uplink 2	vmnic2 - Up, 10000 mbps

▼ vSwitch Details

- MTU
- Ports
- Link discovery
- Attached VMs
- Beacon interval

▼ NIC teaming policy

- Notify switches
- Policy
- Reverse policy
- Fallback

Recent tasks

Task

Save Cancel

Esto se verá de la siguiente forma, y posteriormente se le da click a la opción save:

172.24.131.26/ui/#/host/networking/vswitches/vSwitch2

hellen.fernandezjmenez@172.24.131.26 | Help | Search

vSwitch2

Add uplink | Edit settings | Refresh | Actions

vSwitch2

Type: Standard vSwitch
Port groups: 1
Uplinks:

Edit standard virtual switch - vSwitch2

Add uplink

MTU	1500
Uplink 1	vmnic2 - Up, 10000 mbps

▼ vSwitch Details

- MTU
- Ports
- Link discovery
- Attached VMs
- Beacon interval

▼ NIC teaming policy

- Notify switches
- Policy
- Reverse policy
- Fallback

Recent tasks

Task

Save Cancel

3. Imagen base

1. Descripción de la imagen base

Esta será la imagen de la máquina virtual que será utilizada como punto de partida para que a partir de la configuración que esta contenga, sea exportada y utilizada para los distintos servicios que ofrecidos en el centro de datos.

2. Prerrequisitos de instalación

Para realizar esta imagen base, debe estar instalado el .iso del de CentOS-7-x86_64-Minimal-2009, que se encuentra en el almacenamiento NAS.

3. Localización del equipo.

Este equipo se encontrará en la sección de Storage como parte del ISCSI

4. Características de hardware del equipo.

5. Pasos realizados para llegar a la imagen base

5.1 Cambie el hostname de la máquina

Que cada máquina tenga un nombre distinto de host es de suma importancia ya que esto va a ser de utilidad en caso de que se presenten problemas y se deseé identificar cuál de las máquinas es la que está dando problemas. Esto debe ser realizado en cada una de las máquinas ya que cada máquina debe tener su nombre único para los efectos antes expuestos. Para realizarlo se debe seguir la siguiente secuencia de pasos:

1. Revise el hostname existente:

```
# hostnamectl
```

```
hellen.fernandezjimenez@172.24.131.26 | Help | Search

ImagenBase

2. Reconfigure the baseurl/etc. for the repository, to point to a working upstream. This is most often useful if you are using a newer distribution release than is supported by the repository (and the packages for the previous distribution release still work).

3. Run the command with the repository temporarily disabled
   yum --disablerepo=<repoid> ...

4. Disable the repository permanently, so yum won't use it by default. Yum will then just ignore the repository until you permanently enable it again or use --enablerepo for temporary usage:

   yum-config-manager --disable <repoid>
   or
   subscription-manager repos --disable=<repoid>

5. Configure the failing repository to be skipped, if it is unavailable.
   Note that yum will try to contact the repo. when it runs most commands, so will have to try and fail each time (and thus, yum will be much slower). If it is a very temporary problem though, this is often a nice compromise:

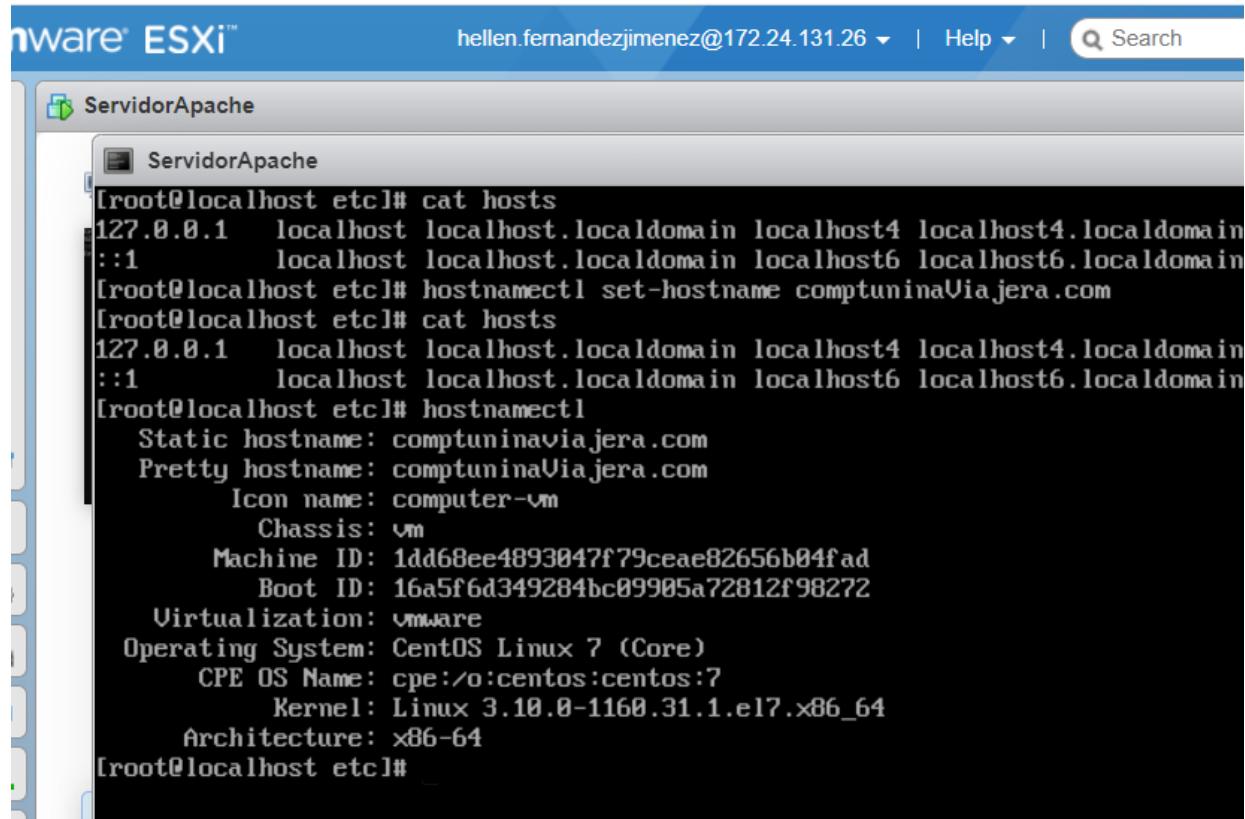
   yum-config-manager --save --setopt=<repoid>.skip_if_unavailable=true

Cannot find a valid baseurl for repo: base/7/x86_64
[root@localhost ~]# hostnamectl
  Static hostname: localhost.localdomain
    Icon name: computer-vm
      Chassis: vm
    Machine ID: 1dd68ee4893047f79ceae82656b04fad
      Boot ID: a51e44220434448f86a232d516f25d64
Virtualization: vmware
Operating System: CentOS Linux 7 (Core)
    CPE OS Name: cpe:/o:centos:centos:7
      Kernel: Linux 3.10.0-1160.el7.x86_64
Architecture: x86-64
[root@localhost ~]#
```

Como se puede observar, actualmente el hostname es localhost.

2. Cambie a un nuevo nombre estático:

```
# hostnamectl set-hostname computinaViajera.com
```



5.2 Asigne una dirección ip

Para poder realizar la configuración inicial, es importante que la máquina tenga acceso a internet debido a que deben poder instalar paquetes necesarios y actualizaciones para esta imagen base. Para esto, se deben realizar los siguientes pasos:

1. Revise las interfaces con las que cuenta el sistema.

```
# ip a
```

```

← → C ⚠ No es seguro | 172.24.131.26/ui/#/console/9
root@localhost /]# ip a
: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 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
: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:29:d5:c3 brd ff:ff:ff:ff:ff:ff
root@localhost /]#

```

En este caso se va a configurar ens192 para que tenga salida a internet, esto es crucial para poder instalar paquetes necesarios de esta imagen base.

2. Diríjase a la configuración de scripts mediante el siguiente comando:

```
# cd /etc/sysconfig/network-script
# ls
```

```

[hellen.fernandez.jimenez@localhost ~]$ cd /etc/sysconfig/network-scripts
[hellen.fernandez.jimenez@localhost network-scripts]$ ls
ifcfg-ens192  ifdown-ip6   ifdown-Team    ifup-eth      ifup-post      ifup-tunnel
ifcfg-lo      ifdown-isdn  ifdown-TeamPort  ifup-ppp      ifup-ppp       ifup-wireless
ifdown        ifdown-post  ifdown-tunnel   ifup-ip6      ifup-routes   init.ipv6-global
ifdown-bnep   ifdown-ppp   ifup          ifup-isdn     ifup-sit      network-functions
ifdown-eth    ifdown-routes ifup-aliases   ifup-plip    ifup-Team     network-functions-ipv6
ifdown-ipp   ifdown-sit   ifup-bnep     ifup-plusb   ifup-TeamPort
[hellen.fernandez.jimenez@localhost network-scripts]$ _

```

Como se puede observar, en este lugar se encuentra la configuración de red de la interfaz de ifcfg-ens192

3. Modifique la configuración de red con la siguiente información:

IPADDR	172.24.133.5
NETMASK	255.255.255.0
GATEWAY	172.24.133.1
DNS	8.8.8.8
ONBOOT	yes
BOOTPROTO	static

Este direccionamiento es consistente con el bloque de direcciones ip que se me fue asignado, y como la red 172.24.133.0 tiene acceso a internet, también se le debe asignar el DNS a 8.8.8.8 que corresponde al servidor DNS de Google. Cabe recalcar que es de suma importancia que sea modificado el parámetro BOOTPROTO, debido a que si este no se modifica, en algunas ocasiones hay conexión y ping y en otras no, además de que no permite el acceso a internet. Este fue un error que se me presentó y fue debido a que está tratando de obtener direcciones por medio de DHCP cuando más bien el objetivo es asignar direccionamiento estático.

Modifique la configuración de red para esa interfaz :

```
# vi ifcfg-ens192
```

Y modifique el archivo, de manera que quede de la siguiente forma:

ImagenBase

TYPE=Ethernet
IPADDR=172.24.133.5
NETMASK=255.255.255.0
GATEWAY=172.24.133.1
DNS1=8.8.8.8
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=static
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=ens192
e UUID=3db520e6-1757-4e1f-8f53-80d5def58b40
DEVICE=ens192
ONBOOT=yes
PREFIX=24

Acl

Q

"ifcfg-ens192" 20L, 370C

Para guardar la configuración y salir escriba:

:wq

4. Reinicie la conexión a la red con el comando:

```
# systemctl restart network
```

5. Verifique la configuración haya sido correctamente almacenada:

```
# cat ifcfg-ens192
```

The screenshot shows a terminal window titled "ImagenBase" with the title bar "hellen.fernandezjimenez@172.24.131.26". The window contains the following command output:

```
[hellen.fernandezjimenez@localhost network-scripts]$ cat ifcfg-ens192
TYPE=Ethernet
IPADDR=172.24.133.5
NETMASK=255.255.255.0
GATEWAY=172.24.133.1
DNS=8.8.8.8
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=dhcp
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=ens192
UUID=3db520e6-1757-4e1f-8f53-80d5def58b40
DEVICE=ens192
ONBOOT=yes
[hellen.fernandezjimenez@localhost network-scripts]$
```

6. Pruebe que exista acceso a la dirección ip del servidor DNS que en este caso es el de google:

```
ping 8.8.8.8
```

The screenshot shows a terminal window titled "ImagenBase" with the title bar "hellen.fernandezjimenez@172.24.131.26". The window contains the following command output:

```
[hellen.fernandezjimenez@localhost network-scripts]$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=115 time=66.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=115 time=63.6 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=115 time=63.4 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=115 time=63.4 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=115 time=63.3 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=115 time=63.6 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=115 time=63.4 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=115 time=63.7 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=115 time=63.3 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=115 time=63.6 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=115 time=63.6 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=115 time=63.5 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=115 time=63.7 ms
```

Para salir: CTRL+C

7. Pruebe que funcione el ping al gateway:

The screenshot shows a terminal window titled "ImagenBase" with the title bar "hellen.fernandezjimenez@172.24.131.26". The window contains the following command output:

```
[root@localhost hellen.fernandezjimenez]# ping 172.24.133.1
PING 172.24.133.1 (172.24.133.1) 56(84) bytes of data.
64 bytes from 172.24.133.1: icmp_seq=1 ttl=255 time=2.67 ms
64 bytes from 172.24.133.1: icmp_seq=2 ttl=255 time=1.27 ms
64 bytes from 172.24.133.1: icmp_seq=3 ttl=255 time=1.33 ms
64 bytes from 172.24.133.1: icmp_seq=4 ttl=255 time=1.10 ms
64 bytes from 172.24.133.1: icmp_seq=5 ttl=255 time=1.18 ms
64 bytes from 172.24.133.1: icmp_seq=6 ttl=255 time=1.20 ms
```

8. Haga ping a google.com para verificar que el servidor DNS funcione correctamente:

```
# ping google.com
```

```
hware ESXi hellen.fernandezjmenez@172.24.131.26 | Help | Search
[ImgenBase]
[root@localhost network-scripts]# ping google.com
PING google.com (142.250.217.206) 56(84) bytes of data.
64 bytes from mia07s61-in-f14.1e100.net (142.250.217.206): icmp_seq=1 ttl=115 time=63.5 ms
64 bytes from mia07s61-in-f14.1e100.net (142.250.217.206): icmp_seq=2 ttl=115 time=63.6 ms
64 bytes from mia07s61-in-f14.1e100.net (142.250.217.206): icmp_seq=3 ttl=115 time=63.7 ms
64 bytes from mia07s61-in-f14.1e100.net (142.250.217.206): icmp_seq=4 ttl=115 time=63.8 ms
```

9. Revise que la interfaz esté correctamente conectada y que posee dirección ip adecuada con los siguientes comandos:

10.

```
# nmcli
```

Debe mostrar connected to interfaz.

```
hware ESXi hellen.fernandezjmenez@172.24.131.26 | Help | Search
[ImgenBase]
[root@localhost network-scripts]# nmcli
ens192: connected to ens192
    "VMnet3"
      ethernet (vmnet3), 00:0c:29:29:d5:c3, hw, mtu 1500
      ip4 default
      inet4 172.24.133.5/24
      route4 172.24.133.0/24
      route4 0.0.0.0/0
      inet6 fe80::5965:c580:fc3e:5e8d/64
      route6 fe80::/64
      route6 ff00::/8

lo: unmanaged
    "lo"
      loopback (unknown), 00:00:00:00:00:00, sw, mtu 65536

DNS configuration:
  servers: 8.8.8.8
  interface: ens192

Use "nmcli device show" to get complete information about known devices and
"nmcli connection show" to get an overview on active connection profiles.

Consult nmcli(1) and nmcli-examples(?) manual pages for complete usage details.
[root@localhost network-scripts]#
```

```
# ip a
```

```
helen.fernandezjmenez@172.24.131.26 | Help | Search
[ImgenBase]
[root@localhost network-scripts]# ip a
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: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:29:d5:c3 brd ff:ff:ff:ff:ff:ff
    inet 172.24.133.5/24 brd 172.24.133.255 scope global noprefixroute ens192
        valid_lft forever preferred_lft forever
    inet6 fe80::5965:c580:fc3e:5e8d/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[root@localhost network-scripts]#
```

5.3 Actualice el sistema

1. Actualizar el sistema frecuentemente con el comando.

```
# yum update -y
```

A screenshot of a terminal window titled 'ImagenBase'. The URL in the address bar is 'hellen.fernandezjimenez@172.24.131.26'. The command entered is '[root@localhost network-scripts]# yum update -y'.

A screenshot of a terminal window titled 'ImagenBase'. The URL in the address bar is 'hellen.fernandezjimenez@172.24.131.26'. The command entered is '[root@localhost network-scripts]# yum update -y'. The output shows numerous package updates:

```
libmount.x86_64 0:2.23.2-65.el7_9.1
libmountd1.x86_64 0:2.23.2-65.el7_9.1
libnfsidr.x86_64 0:2.23.2-65.el7_9.1
libnux-firmware.march 0:28288421-08.git78c8348.e17_9
lom2.x86_64 7:2.02.107.6.e17_9.5
lom2-1libs.x86_64 7:2.02.107.6.e17_9.5
microcode_ctl.x86_64 2.2.1-73.9.e17_9
nspr.x86_64 0:4.25.0-2.e17_9
nss.x86_64 0:3.53.1-7.e17_9
nss-softokn.x86_64 0:3.53.1-6.e17_9
nss-softokn-freebl.x86_64 0:3.53.1-6.e17_9
nss-sysinit.x86_64 0:3.53.1-7.e17_9
nss-tools.x86_64 0:3.53.1-7.e17_9
nss-util.x86_64 0:3.53.1-1.e17_9
openldap.x86_64 0:2.4.44-23.e17_9
openssl.x86_64 1:1.0.2k-21.e17_9
openssl-libs.x86_64 1:1.0.2k-21.e17_9
python.x86_64 0:2.7.5-98.el7
python-firewall.noarch 0:0.6.3-13.el7_9
python-l1bs.x86_64 0:2.7.5-98.el7
python-perf.x86_64 0:3.18.0-1160.31.1.el7
rsyslog.x86_64 0:8.24.0-57.e17_9.1
selinux-policy.march 0:3.13.1-268.el7_9.2
selinux-policy-targeted.noarch 0:3.13.1-268.el7_9.2
sudo.x86_64 0:1.8.23-18.e17_9.1
systemd.x86_64 0:219-78.e17_9.3
systemd-l1bs.x86_64 0:219-78.e17_9.3
systemd-sysv.x86_64 0:219-78.e17_9.3
tuned.noarch 0:2.11.0-11.e17_9
tzdata.noarch 0:2821a-1.e17_9
Complete!
[root@localhost network-scripts]#
```

5.4 Instale el editor de texto nano

Nano es un editor de texto más amigable con el usuario que vi. Por lo cual le podría facilitar al administrador modificar archivos.

Para realizar la instalación del editor de texto nano escriba:

```
# yum install nano -y
```

A screenshot of a terminal window titled 'ImagenBase'. The URL in the address bar is 'hellen.fernandezjimenez@172.24.131.26'. The command entered is '[root@localhost network-scripts]# yum install -y nano'.

```

[ 172.24.131.26/ui/#/host/vms/9
hellen
ImagenBase
Loading mirror speeds from cached hostfile
 * base: mirrors.ucr.ac.cr
 * updates: mirrors.ucr.ac.cr
Resolving Dependencies
--> Running transaction check
--> Package nano.x86_64 0:2.3.1-10.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package           Arch      Version        Repository      Size
=====
Installing:
nano              x86_64   2.3.1-10.el7    base            448 k

Transaction Summary
=====
Install 1 Package

Total download size: 448 k
Installed size: 1.6 M
Downloading packages:
nano-2.3.1-10.el7.x86_64.rpm          | 448 kB  00:00:08
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : nano-2.3.1-10.el7.x86_64
  Verifying  : nano-2.3.1-10.el7.x86_64
  Installed:
    nano.x86_64 0:2.3.1-10.el7

Complete!
[root@localhost network-scripts]# 

```

5.5 Instale net-tools

Este paquete contiene una colección de programas que forman la base de trabajo de red en linux. Algunos de los programas más importantes que este contiene junto con sus respectivas funcionalidades son:

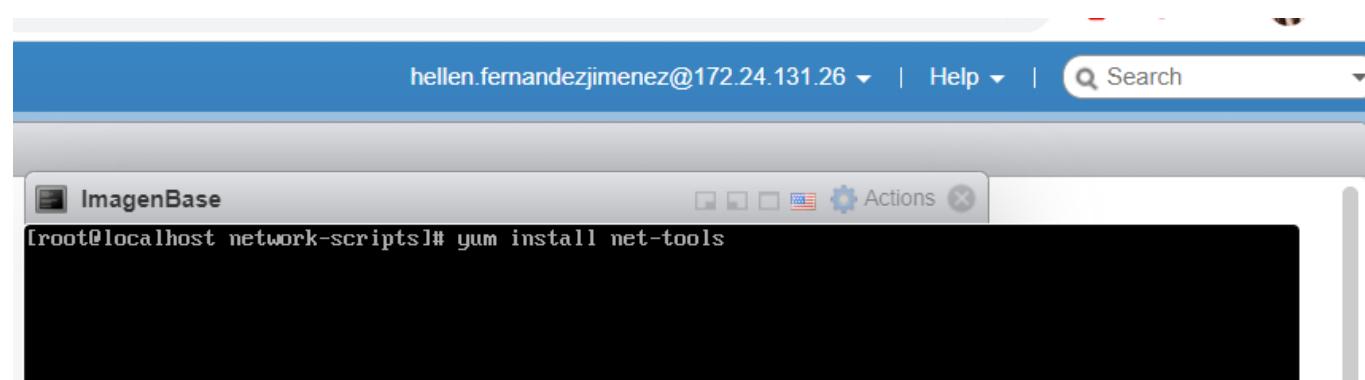
- **arp** se usa para manipular la caché ARP del núcleo, usualmente para añadir o borrar una entrada o volcar la caché completa.
- **dnsdomainname** muestra el nombre del dominio DNS del sistema.
- **domainname** muestra o establece el nombre del dominio NIS/YP del sistema.
- **hostname** muestra o establece el nombre del sistema actual.
- **ifconfig** es la utilidad principal usada para configurar las interfaces de red.
- **nameif** nombra interfaces de red basándose en las direcciones MAC.
- **netstat** se usa para mostrar las conexiones de red, tablas de encaminamiento y estadísticas de las interfaces.
- **nisdomainname** hace lo mismo que domainname.
- **route** se usa para manipular la tabla de encaminamiento IP.

Tomado de:

<http://www.escomposlinux.org/lfs-es/lfs-es-5.0/appendixa/net-tools.html>

Para instalarlo, escriba el comando:

```
#yum install net-tools -y
```



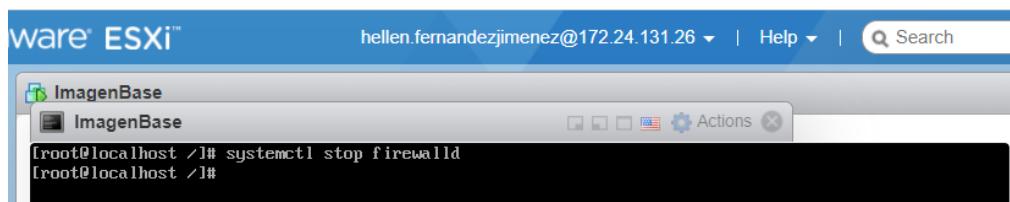
5.6 Instale iptables

Este será el servicio que permitirá establecer controles de acceso y nateo a través de reglas que se implementarán.

Para instalar iptables primero se debe deshabilitar FirewallD que es la solución de Firewall que viene por defecto en la instalación de Centos7 Minimal. Para esto:

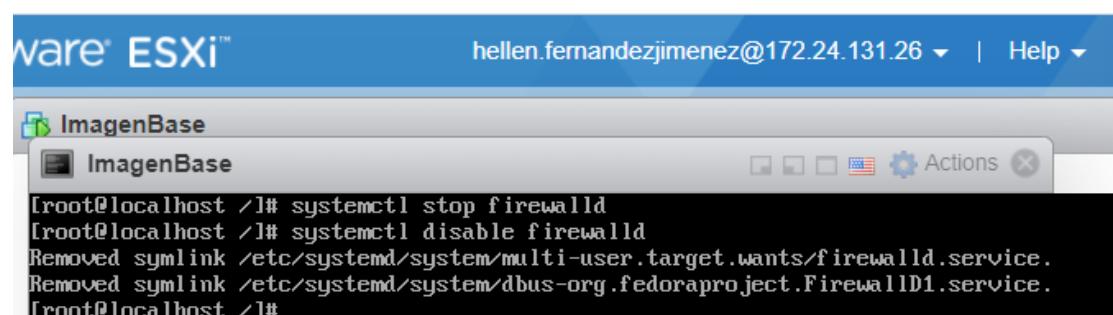
1. Detenga el servicio de FirewallD:

```
# systemctl stop firewalld
```



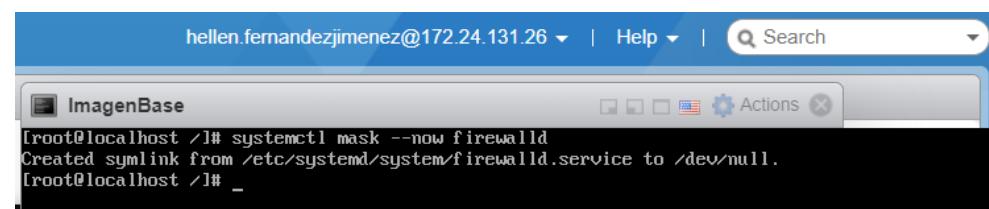
2. Des habilite que FirewallD inicie automáticamente cuando se le haga boot al sistema:

```
# systemctl disable firewalld
```



3. Prevenga que el servicio de FirewallD sea iniciado por otros servicios:

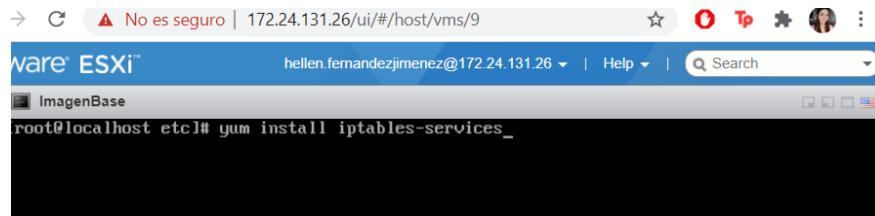
```
# systemctl mask --now firewalld
```



Ahora instale iptables:

4. Descargue el paquete de iptables-service:

```
# yum install iptables-services -y
```



```
[root@localhost ~]# yum install iptables-services -y
iptables-services-1.7.2-33.el7.x86_64.i686
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : iptables-services-1.4.21-35.el7.x86_64
  Verifying : iptables-services-1.4.21-35.el7.x86_64

Installed:
  iptables-services.x86_64 0:1.4.21-35.el7

Complete!
[root@localhost ~]#
```

5. Inicie el servicio de iptables en caso de ser necesario. En este caso aún no se va a iniciar iptables hasta que el servicio que se va a ofrecer esté en funcionamiento.

```
# systemctl start iptables
# systemctl start ip6tables
```

6. Habilite que el servicio se inicie automáticamente cuando el sistema bootea:

```
# systemctl enable iptables
# systemctl enable ip6tables
```

7. Revise el estado de iptables:

```
# systemctl status iptables
# systemctl status ip6tables
```

8. Para revisar las reglas que están actualmente en iptables utilice el siguiente comando:

```
# iptables -nvL
# ip6tables -nvL
```

Tomado de:

<https://linuxize.com/post/how-to-install-iptables-on-centos-7/>

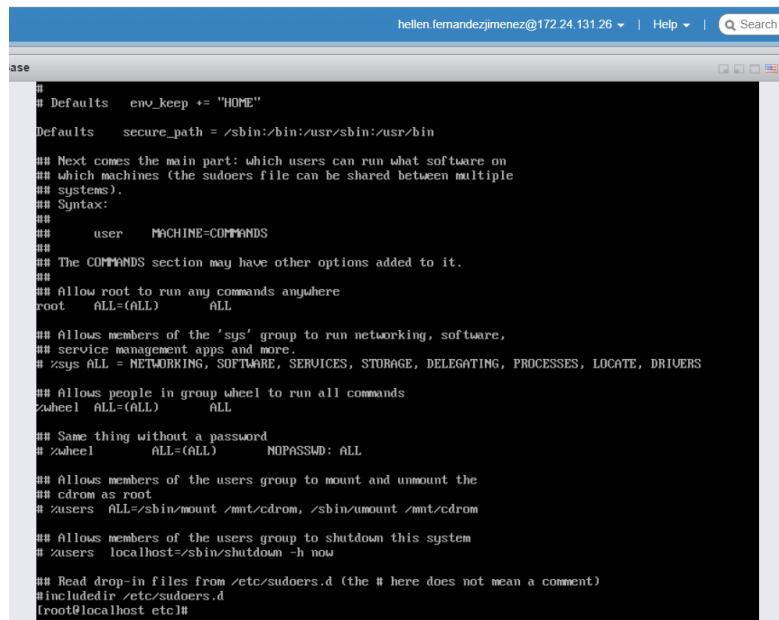
5.7 Deshabilite el servicio remoto para usuario root

Deshabilitar que el usuario root tenga acceso a ssh reduce el riesgo de que un atacante tome control de la máquina con estos privilegios ya que estos privilegios se le van a dar a otro usuario.

En este caso, los permisos de sudo se le van a dar al usuario: hellen.fernandezjimenez que ya está creado en esta máquina.

1. Verifique el estado de el archivo sudoers

```
# cat /etc/sudoers
```



```
hellen.fernandezjimenez@172.24.131.26 ~ | Help | Search

[ase

## Defaults env_keep += "HOME"
Defaults secure_path = /sbin:/bin:/usr/sbin:/usr/bin

## Next comes the main part: which users can run what software on
## which machines (the sudoers file can be shared between multiple
## systems).
## Syntax:
##
##     user    MACHINE=COMMANDS
##
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
root    ALL=(ALL)      ALL

## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOCATE, DRIVERS
# %sys ALL=(ALL)      ALL

## Allows people in group wheel to run all commands
%wheel  ALL=(ALL)      ALL

## Same thing without a password
# %wheel    ALL=(ALL)      NOPASSWD: ALL

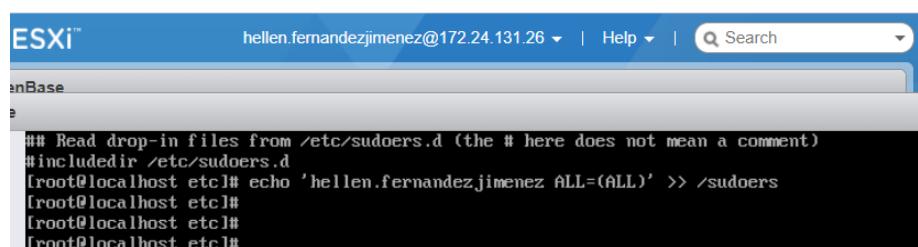
## Allows members of the users group to mount and umount the
## cdrom as root
# %users  ALL=/sbin/mount /mnt/cdrom, /sbin/umount /mnt/cdrom
# %users  ALL=(ALL)      ALL

## Allows members of the users group to shutdown this system
# %users  localhost=/sbin/shutdown -h now

## Read drop-in files from /etc/sudoers.d (the # here does not mean a comment)
#includedir /etc/sudoers.d
[root@localhost etc]#
```

2. Asigne permisos para el usuario:

```
# echo 'hellen.fernandezjimenez ALL=(ALL) ALL' >> /sudoers
```



```
ESXi™          hellen.fernandezjimenez@172.24.131.26 ~ | Help | Search

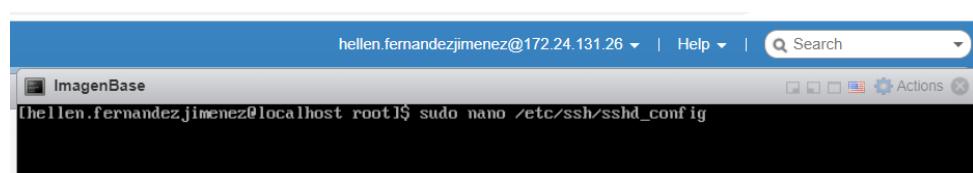
[enBase

[

## Read drop-in files from /etc/sudoers.d (the # here does not mean a comment)
#includedir /etc/sudoers.d
[root@localhost etc]# echo 'hellen.fernandezjimenez ALL=(ALL)' >> /sudoers
[root@localhost etc]#
[root@localhost etc]#
[root@localhost etc]#
```

3. Ahora deshabilitar ssh para el root:

```
# nano /etc/ssh/sshd_config
```



```
hellen.fernandezjimenez@172.24.131.26 ~ | Help | Search

[ImagenBase
[hellen.fernandezjimenez@localhost root]$ sudo nano /etc/ssh/sshd_config
```

4. Note que está una cláusula que dice:

```
#PermitRootLogin yes
```

```

#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

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

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile      .ssh/authorized_keys
#AuthorizedPrincipalsFile none

07:26:45 Get Help   07:26:45 WriteOut   07:26:45 Read File   07:26:45 Prev Page   07:26:45 Cut Text   07:26:45 Cur Pos
07:26:45 Exit   07:26:45 Justify   07:26:45 Where Is   07:26:45 Next Page   07:26:45 UnCut Text   07:26:45 To Spell

```

5. Modifique esta cláusula a no, de la siguiente manera:

```
#PermitRootLogin no
```

```

#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

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

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin no_
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile      .ssh/authorized_keys
#AuthorizedPrincipalsFile none

16:26:45 Get Help   16:26:45 WriteOut   16:26:45 Read File   16:26:45 Prev Page   16:26:45 Cut Text   16:26:45 Cur Pos
16:26:45 Exit   16:26:45 Justify   16:26:45 Where Is   16:26:45 Next Page   16:26:45 UnCut Text   16:26:45 To Spell

```

Para guardar los cambios Ctrl+O Ctrl+X

6. Reiniciar ssh:

El tutorial indica una forma de reiniciar el servicio, sin embargo esta no funciona, para esto mediante otro tutorial se encontró otra forma de reiniciarlo:

```
# systemctl restart sshd.service
```

```
[root@localhost bin]# systemctl restart sshd.service
[root@localhost bin]#
```

Tutorial para configuracion de ssh Tomado de:

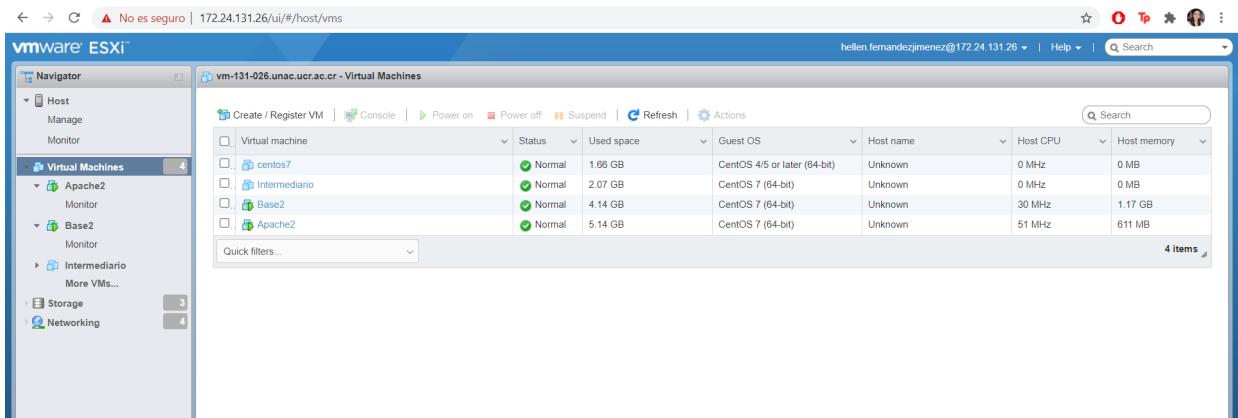
<https://mediatemple.net/community/products/dv/204643810/how-do-i-disable-ssh-login-for-the-root-user>

Tutorial para reiniciar el servicio:

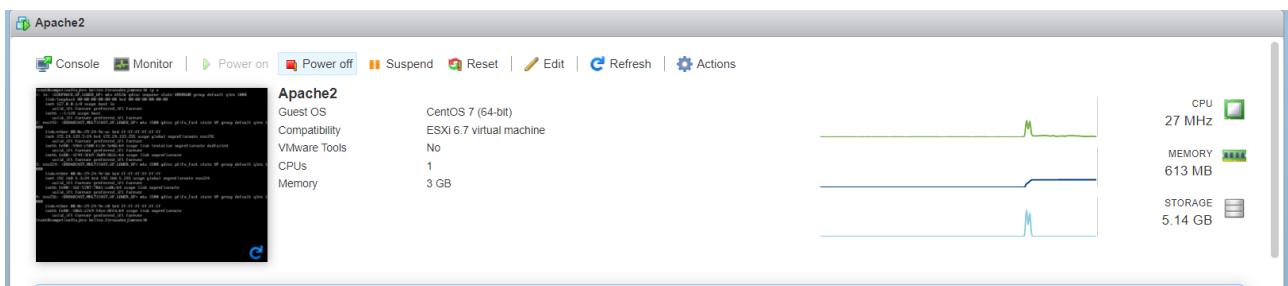
<https://globedrill.com/how-to-start-stop-restart-ssh-service-on-centos-7-redhat-7-servers/>

6. Agregue una interfaz a una máquina virtual

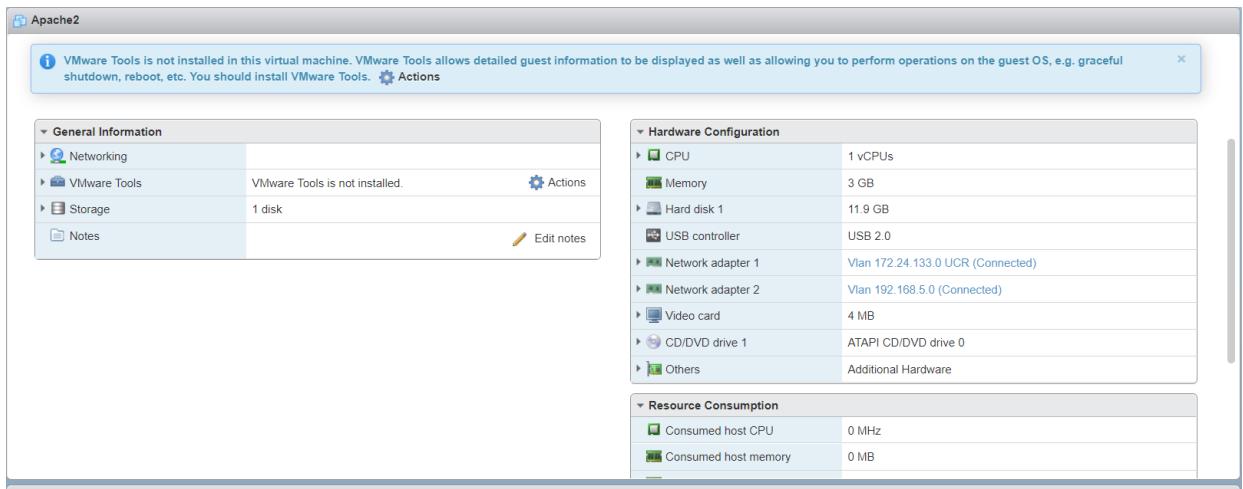
- Observe las interfaces que están actualmente en la máquina virtual dirigiéndose a virtual machines:



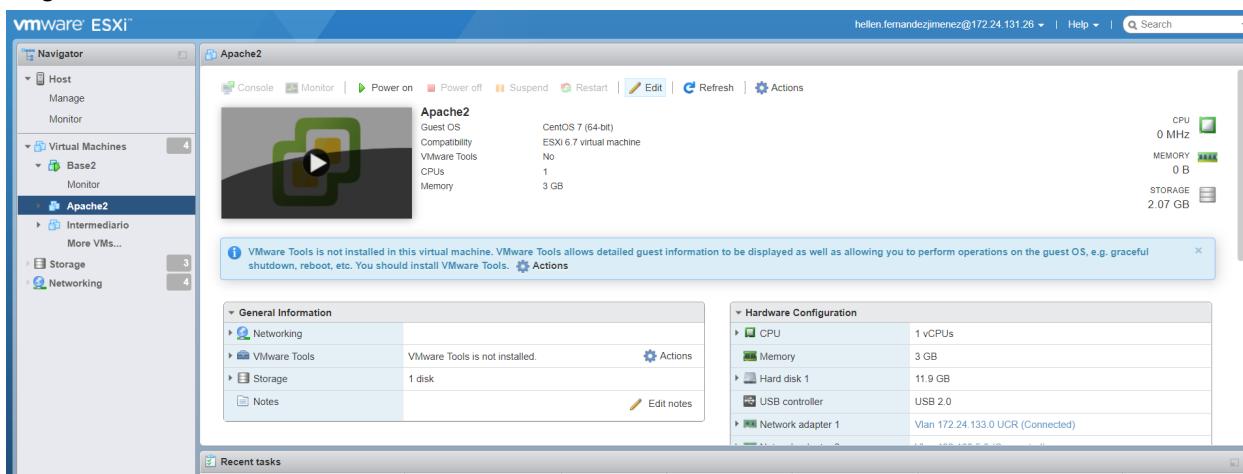
- Haga click en el nombre de la máquina a la cual le desea agregar una interfaz de red y haga click en Power off.



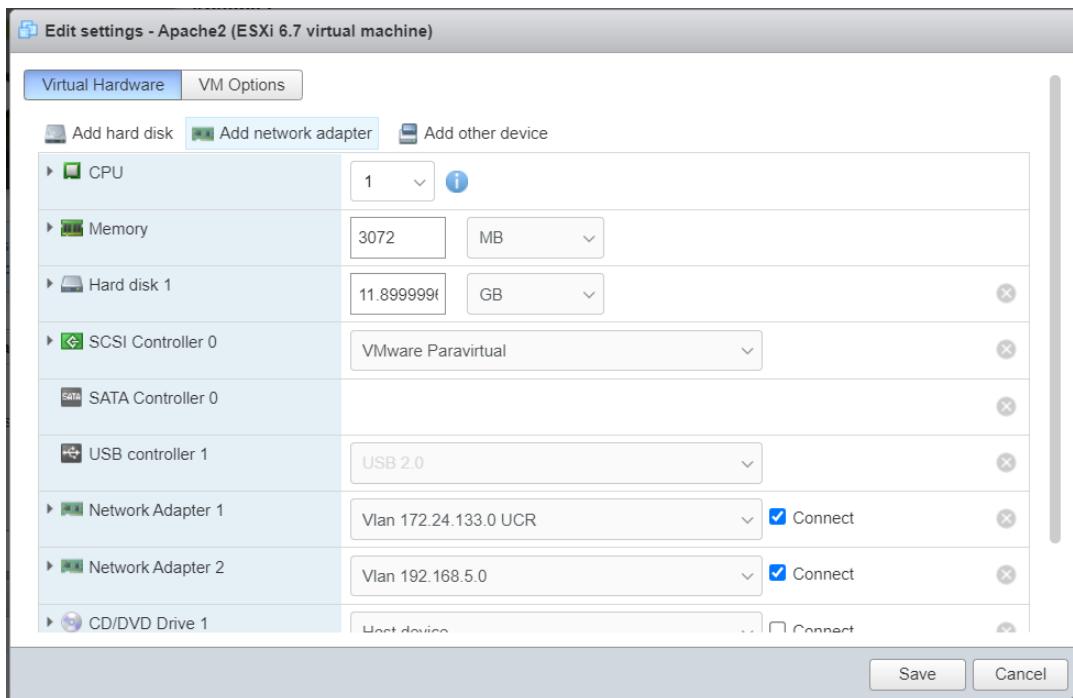
- Baje en esta misma ventana, observe las interfaces que están actualmente activas en donde dice Network adapter 1, network adapter 2:



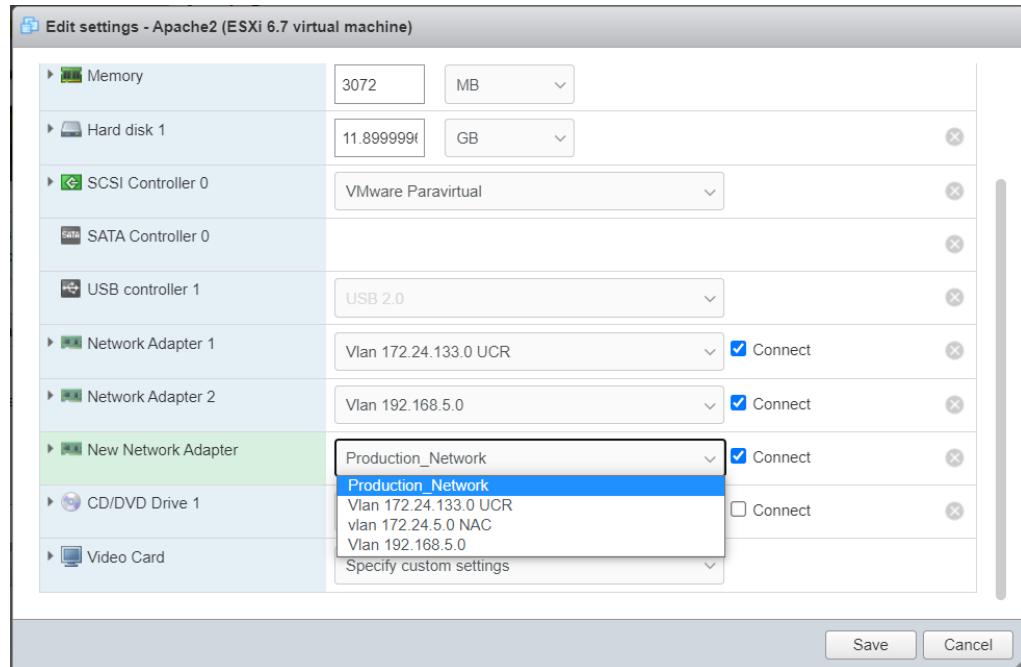
4. Haga click en Edit:



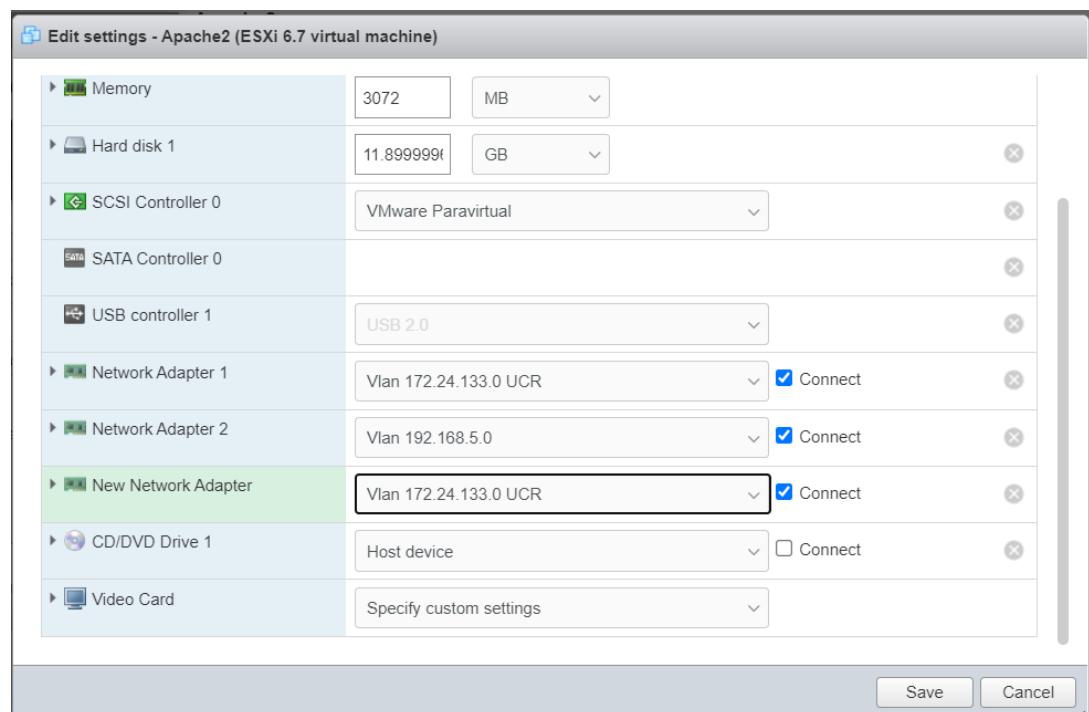
5. Haga click en Add network adapter:



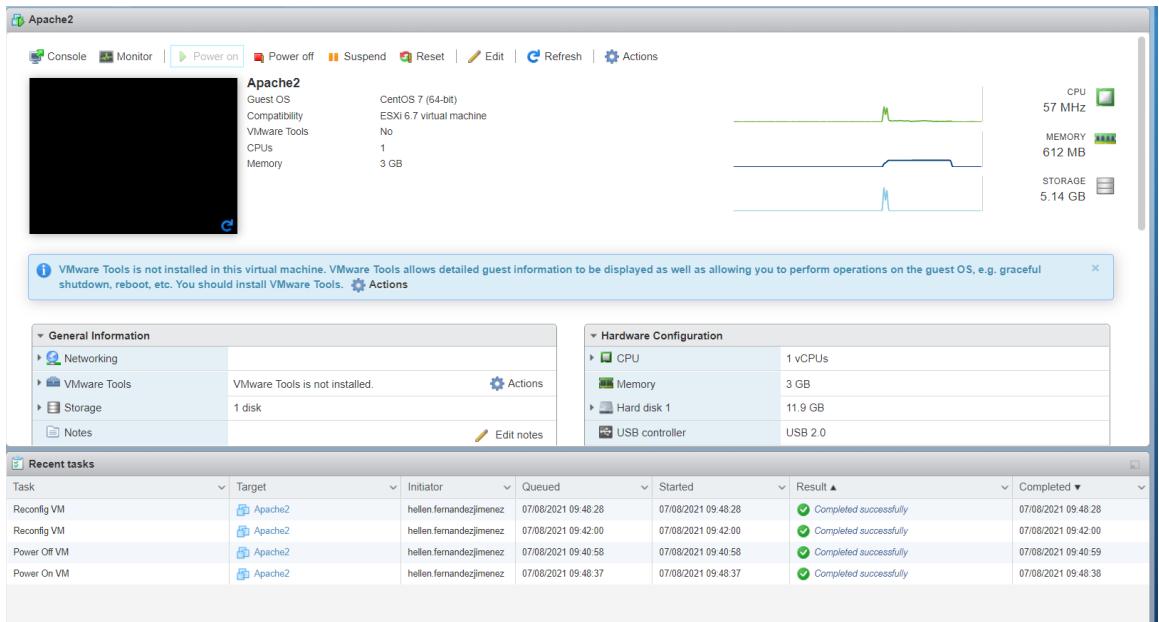
6. Seleccione el port group en el cual desea que esté la máquina.



7. Haga click en save:



8. Encienda nuevamente la máquina, entre en la pantalla e inicie sesión:



9. Verifique las interfaces existentes y observe la interfaz que no tiene dirección ip agregada, esta es la que fue recientemente añadida:

ip a

```
[root@computinaViajera hellen.fernandez.jimenez]# ip a
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: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:24:9e:ac brd ff:ff:ff:ff:ff:ff
        inet 172.24.133.7/24 brd 172.24.133.255 scope global noprefixroute ens192
            valid_lft forever preferred_lft forever
            inet6 fe80::5965:c580:fc3e:5e8d%ens192 brd ff:ff:ff:ff:ff:ff
                valid_lft forever preferred_lft forever
                inet6 fe80::1f44:3f69:3b09:862c%ens192 brd ff:ff:ff:ff:ff:ff
                    valid_lft forever preferred_lft forever
3: ens224: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:24:9e:b6 brd ff:ff:ff:ff:ff:ff
        inet 192.168.5.3/24 brd 192.168.5.255 scope global noprefixroute ens224
            valid_lft forever preferred_lft forever
            inet6 fe80::16f:5707:70a1:ca0%ens224 brd ff:ff:ff:ff:ff:ff
                valid_lft forever preferred_lft forever
4: ens256: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:24:9e:c0 brd ff:ff:ff:ff:ff:ff
        inet6 fe80::1865:a7e9:54ce:8ffd%ens256 brd ff:ff:ff:ff:ff:ff
            valid_lft forever preferred_lft forever
[root@computinaViajera hellen.fernandez.jimenez]# _
```

Observe la interfaz 4 con nombre ens256

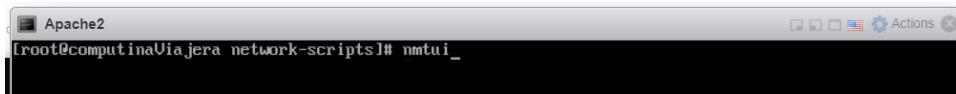
10. Muévase a la carpeta de network scripts y revise los scripts que ya existen mediante los comandos:

```
# cd /etc/sysconfig/network-scripts
# ls
```

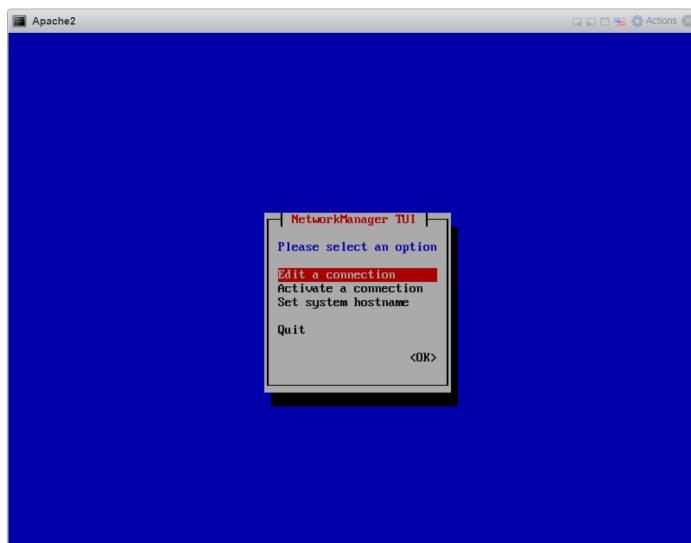
```
[root@computinaViajera hellen.fernandez.jimenez]# cd /etc/sysconfig/network-scripts
[root@computinaViajera network-scripts]# ls
ifcfg-ens192  ifdown-ippp    ifdown-sit      ifup-bnep    ifup-plusb   ifup-TeamPort
ifcfg-ens224  ifdown-ipv6    ifdown-Team     ifup-eth     ifup-post    ifup-tunnel
ifcfg-lo      ifdown-isdn    ifdown-TeamPort ifup-ippp    ifup-ppp     ifup-wireless
ifdown        ifdown-post   ifdown-tunnel  ifup-ipv6   ifup-routes  init.ipv6-global
ifdown-bnep   ifdown-ppp    ifup          ifup-isdn   ifup-sit    network-functions
ifdown-eth    ifdown-routes ifup-aliases   ifup-plip   ifup-Team   network-functions-ipv6
[root@computinaViajera network-scripts]# _
```

11. Acceda a la herramienta nmtui mediante el comando:

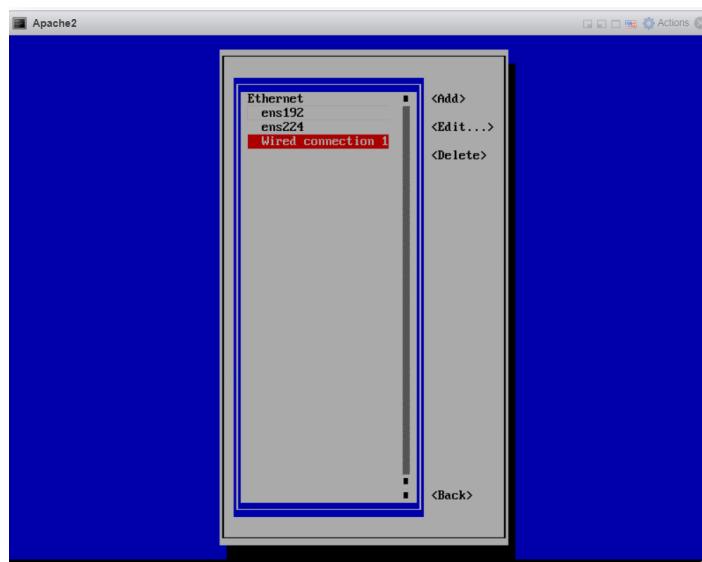
```
#nmtui
```



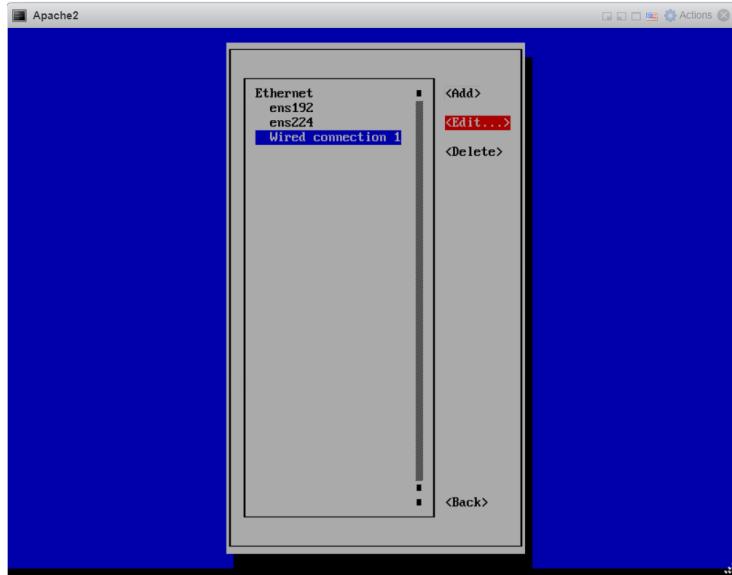
12. Seleccione Edit a connection dandole enter:



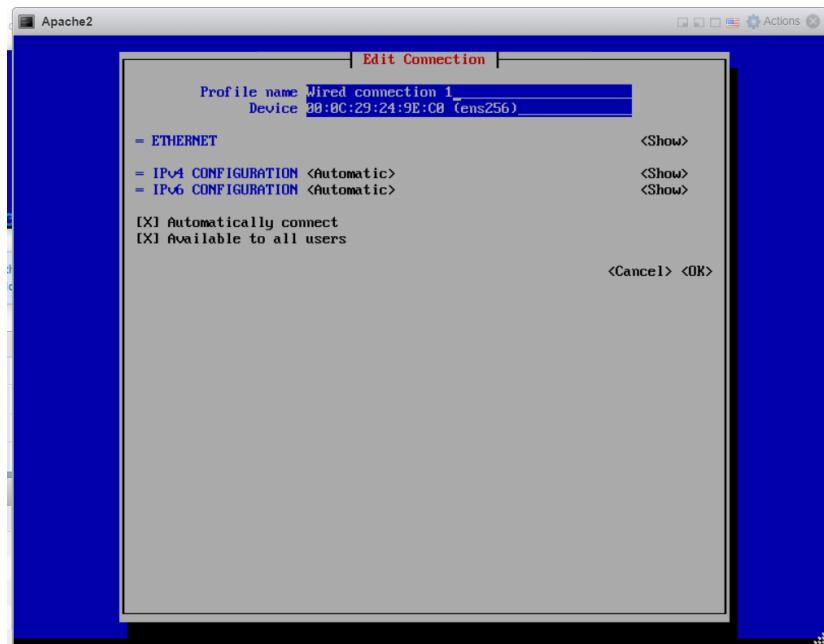
13. Baje hasta llegar a la opción Wired connection 1:



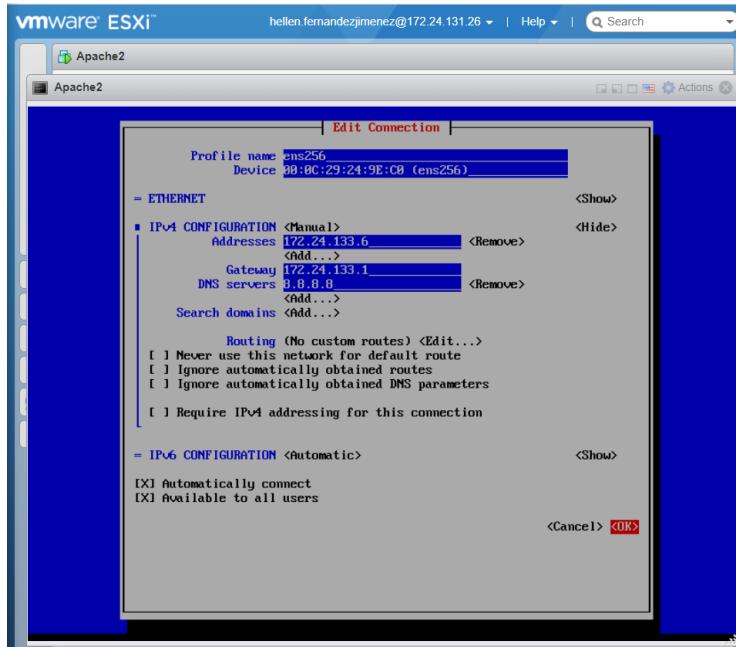
14. Pulse la flecha de su teclado que apunta hacia la derecha, y baje hasta llegar a la opción Edit y pulse enter:



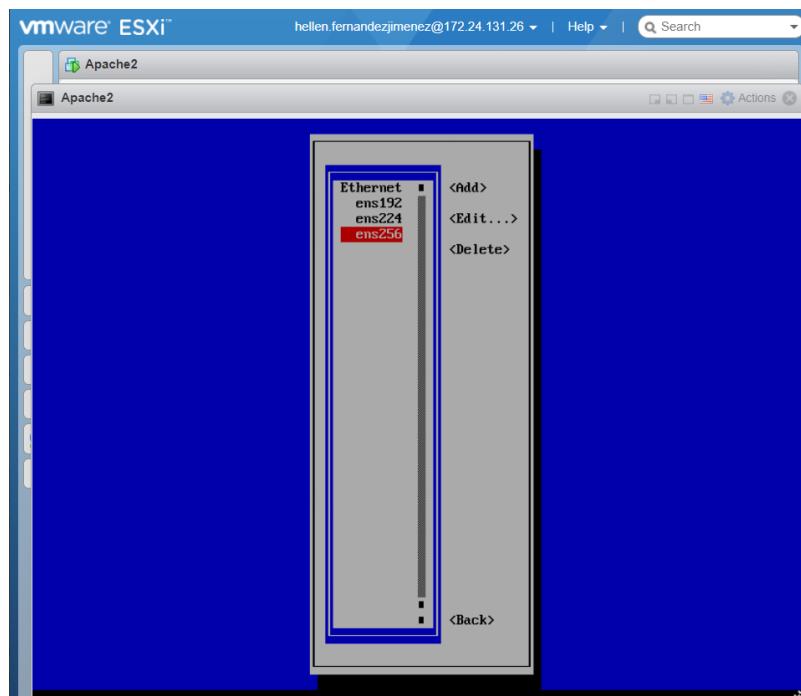
15. Cambie el nombre en Profile name, borrando el que está, y poniéndole el nombre de la interfaz, en este caso ens256:



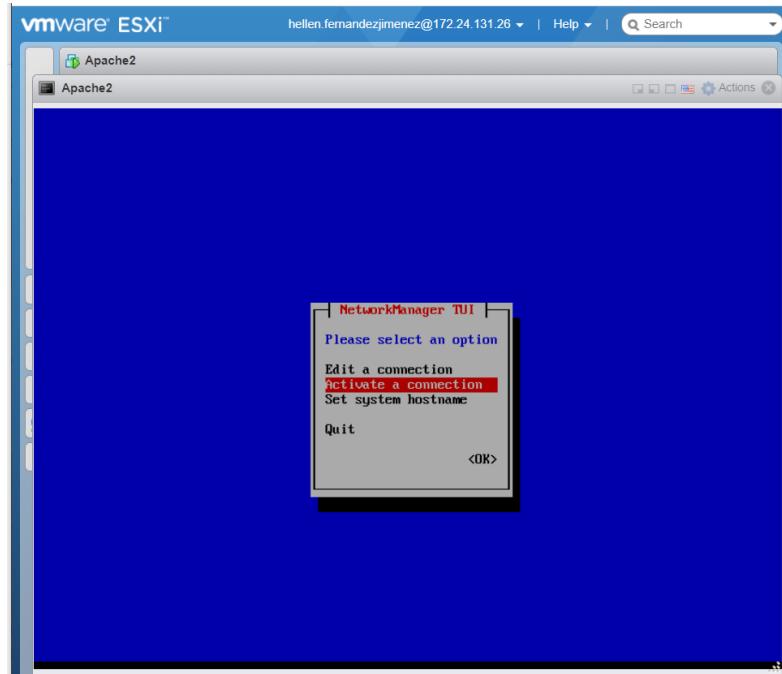
16. Baje a IPv4 Configuration y seleccione Manual, y a la derecha seleccione show y configúralo de la siguiente forma y seleccione OK:



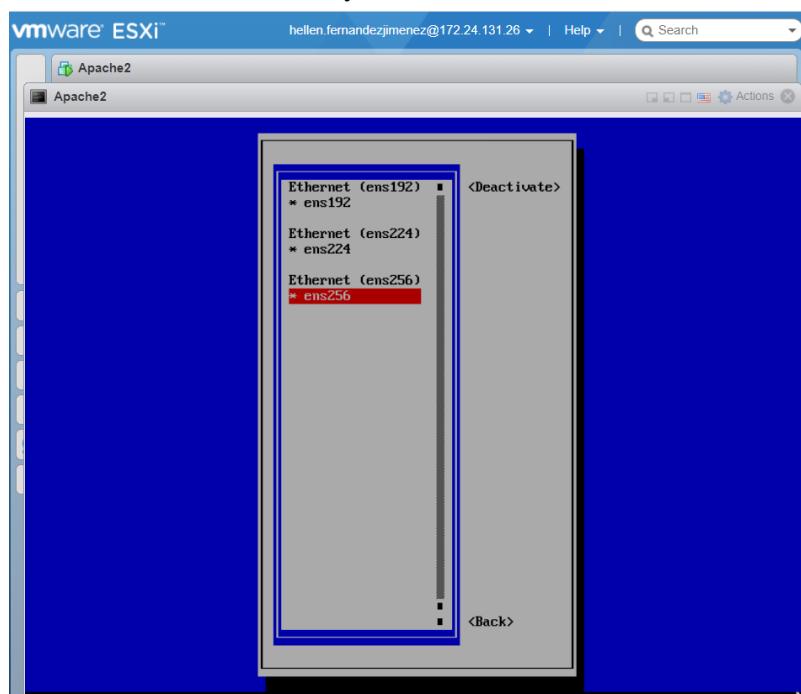
17. En esta pantalla, seleccione Back:



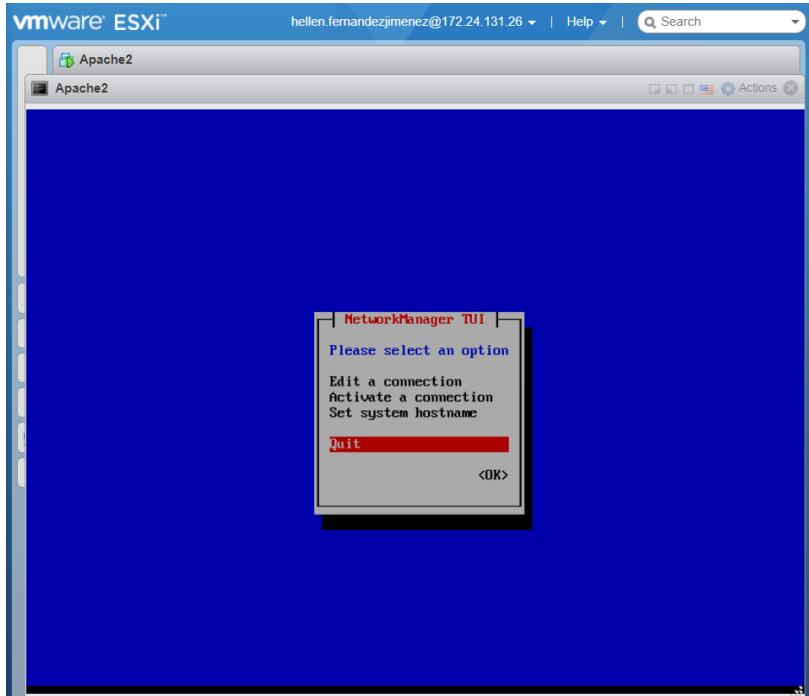
18. Seleccione activa Connection:



19. En caso de que esté desactivada la interfaz que se acaba de configurar, actívela:
En este caso, se activó automáticamente y seleccione Back.



20. Seleccione Quit



21. Verifique que todas las interfaces estén conectadas con sus respectivas ip mediante el comando:

```
#nmcli
```

Presione q para salir una vez que fue verificado.

```

ens192: connected to ens192
    "VMware VMNET3"
    ethernet (vmnet3), 00:0C:29:24:9E:AC, hw, mtu 1500
    ip4 default
    inet4 172.24.133.7/24
    route4 172.24.133.0/24
    route4 0.0.0.0/0
    route6 fe80::1f44:3f69:3b89:862c/64
    inet6 fe80::5965:c580:fc3e:5e0d/64
    route6 fe80::/64
    route6 ff00::/8

ens224: connected to ens224
    "VMware VMNET3"
    ethernet (vmnet3), 00:0C:29:24:9E:B6, hw, mtu 1500
    inet4 192.168.5.3/24
    route4 192.168.5.0/24
    route6 fe80::1f67:5707:70d1:ca06/64
    route6 fe80::/64
    route6 ff00::/8

ens256: connected to ens256
    "VMware VMNET3"
    ethernet (vmnet3), 00:0C:29:24:9E:C8, hw, mtu 1500
    inet4 172.24.133.6/16
    route4 172.24.0.0/16
    route4 0.0.0.0/0
    route6 fe80::1065:a7e9:54ce:8ffd/64
    route6 fe80::/64
    route6 ff00::/8

lo: unmanaged
    "lo"
    loopback (unknown), 00:00:00:00:00:00, sw, mtu 65536

DNS configuration:
lines 1-36

```

22. Como se puede observar, aún se encuentra en esta ruta:

```

[root@computinaViajera network-scripts]# pwd
/etc/sysconfig/network-scripts
[root@computinaViajera network-scripts]#

```

23. Liste los archivos de configuración nuevamente mediante el comando:

```
# ls
```

Note como ahora si se encuentra el archivo de configuración de la interfaz 256:

```
Apache2 Actions
[root@computinaViajera network-scripts]# pwd
/etc/sysconfig/network-scripts
[root@computinaViajera network-scripts]# ls
ifcfg-ens192  ifdown-ipp  ifdown-Team   ifup-ipp  ifup-routes      network-functions
ifcfg-ens224  ifdown-ipv6  ifdown-TeamPort  ifup-ipv6  ifup-sit       network-functions-ipv6
ifcfg-ens256  ifdown-isdn  ifdown-tunnel  ifup-isdn  ifup-Team
ifcfg-lo      ifdown-post  ifup          ifup-plip  ifup-TeamPort
ifdown        ifdown-ppp   ifup-aliases   ifup-plusb ifup-tunnel
ifdown-bnep   ifdown-routes ifup-bnep    ifup-post   ifup-wireless
ifdown-eth    ifdown-sit   ifup-eth     ifup-ppp   init.ipv6-global
[root@computinaViajera network-scripts]#
```

24. Observa la configuración que ya está:

```
# cat ifcfg-ens256
```

```
Apache2 Actions
[root@computinaViajera network-scripts]# ls
ifcfg-ens192  ifdown-ipp  ifdown-Team   ifup-ipp  ifup-routes      network-functions
ifcfg-ens224  ifdown-ipv6  ifdown-TeamPort  ifup-ipv6  ifup-sit       network-functions-ipv6
ifcfg-ens256  ifdown-isdn  ifdown-tunnel  ifup-isdn  ifup-Team
ifcfg-lo      ifdown-post  ifup          ifup-plip  ifup-TeamPort
ifdown        ifdown-ppp   ifup-aliases   ifup-plusb ifup-tunnel
ifdown-bnep   ifdown-routes ifup-bnep    ifup-post   ifup-wireless
ifdown-eth    ifdown-sit   ifup-eth     ifup-ppp   init.ipv6-global
[root@computinaViajera network-scripts]# cat ifcfg-ens256
HWADDR=00:0C:29:24:9E:C8
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=none
IPADDR=172.24.133.6
PREFIX=16
GATEWAY=172.24.133.1
DNS1=8.8.8.8
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=ens256
UUID=0a044ca7-e207-3ae2-9fff-da9429ce5c57
ONBOOT=yes
AUTOCONNECT_PRIORITY=-999
[root@computinaViajera network-scripts]# _
```

25. Modifique el parámetro BOOTPROTO a static de la siguiente forma:

```
# nano ifcfg-ens256
```

```
GNU nano 2.3.1          File: ifcfg-ens256          Modified

HWADDR=00:0C:29:24:9E:C0
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=static
IPADDR=172.24.133.6
PREFIX=16
GATEWAY=172.24.133.1
DNS1=8.8.8.8
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=ens256
UUID=0a044ca7-e207-3ae2-9fff-da9429ce5c57
ONBOOT=yes
AUTOCONNECT_PRIORITY=-999
```

Get Help WriteOut Read File Prev Page Cut Text Cur Pos
Exit Justify Where Is Next Page UnCut Text To Spell

26. Verifique se se guardaron los cambios:

```
# cat ifcfg-ens256
```

```
[root@computinaViajera network-scripts]# cat ifcfg-ens256
HWADDR=00:0C:29:24:9E:C0
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=static
IPADDR=172.24.133.6
PREFIX=16
GATEWAY=172.24.133.1
DNS1=8.8.8.8
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=ens256
UUID=0a044ca7-e207-3ae2-9fff-da9429ce5c57
ONBOOT=yes
AUTOCONNECT_PRIORITY=-999
```

27. Reinicie el servicio de red:

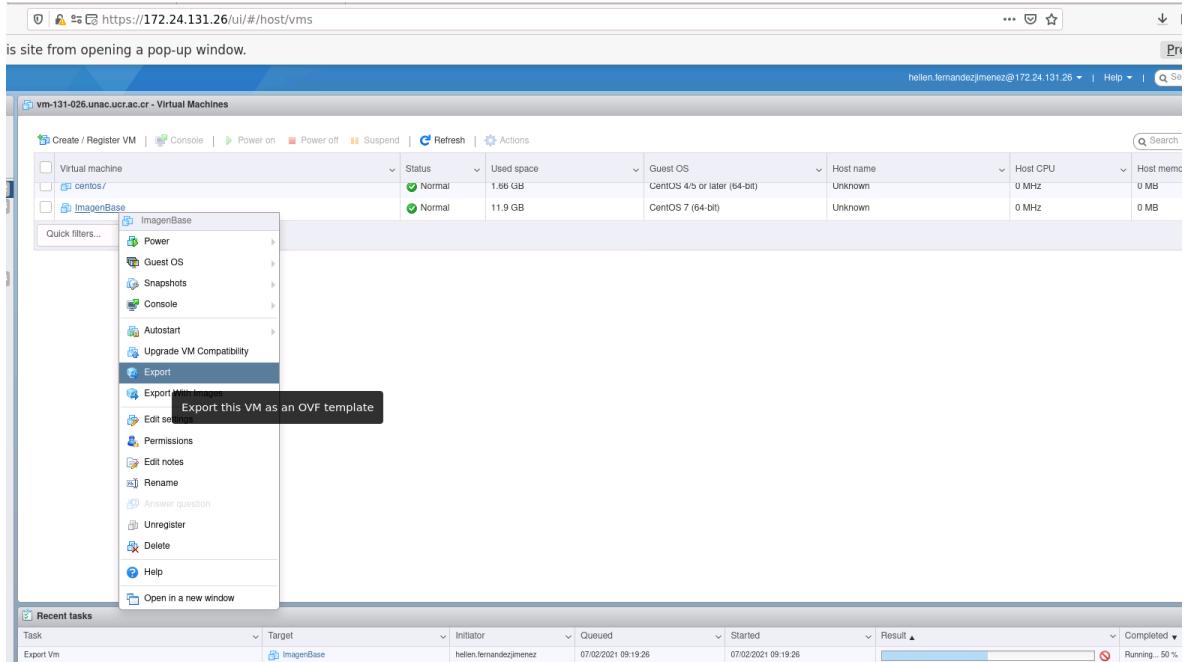
```
[root@computinaViajera network-scripts]# systemctl restart network
[root@computinaViajera network-scripts]# _
```

7. Exporte la imagen base

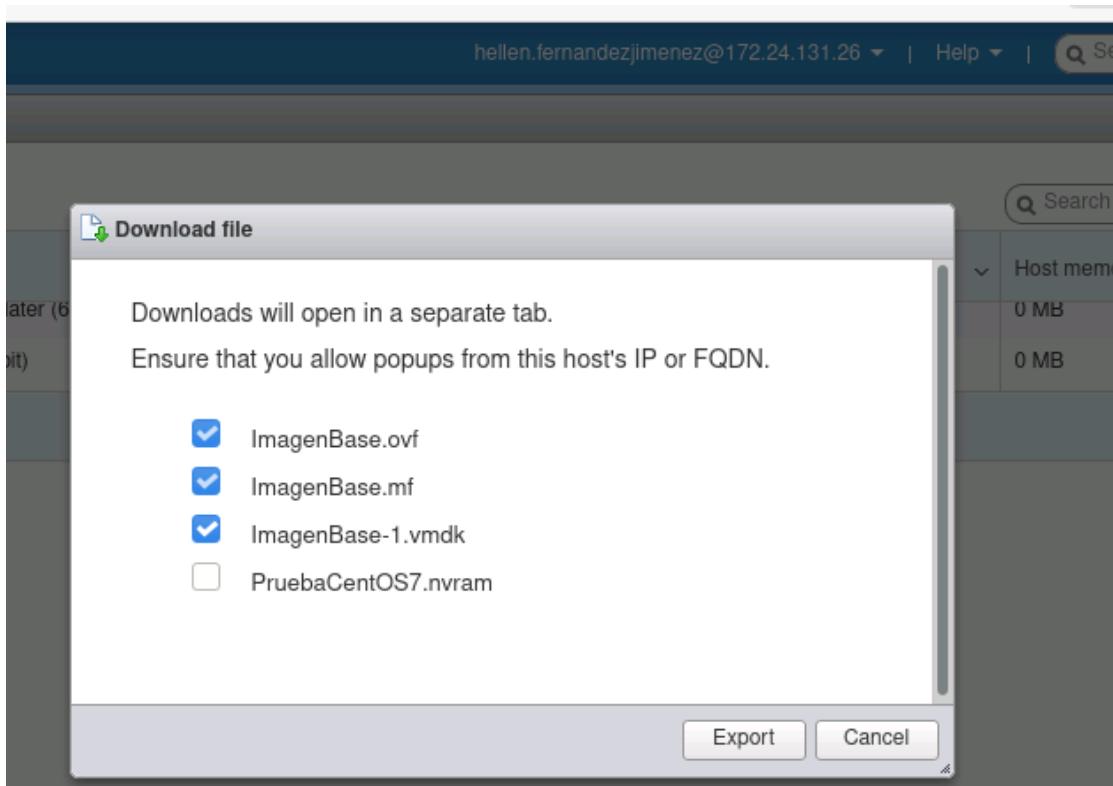
Para poder obtener la imagen con las configuraciones ya realizadas a esta máquina virtual se va a exportar esta máquina. Para esto:

1. Apague la máquina virtual que contiene la imagen base:

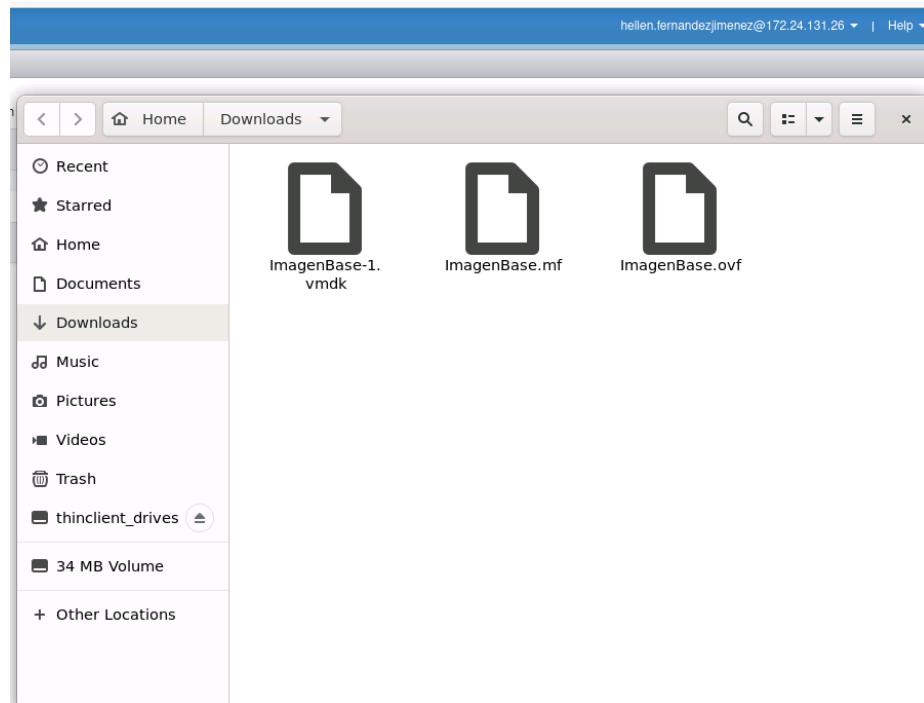
2. Seleccione la opción Export :



3. Seleccione Export nuevamente:



Ya están descargados en downloads los archivos:

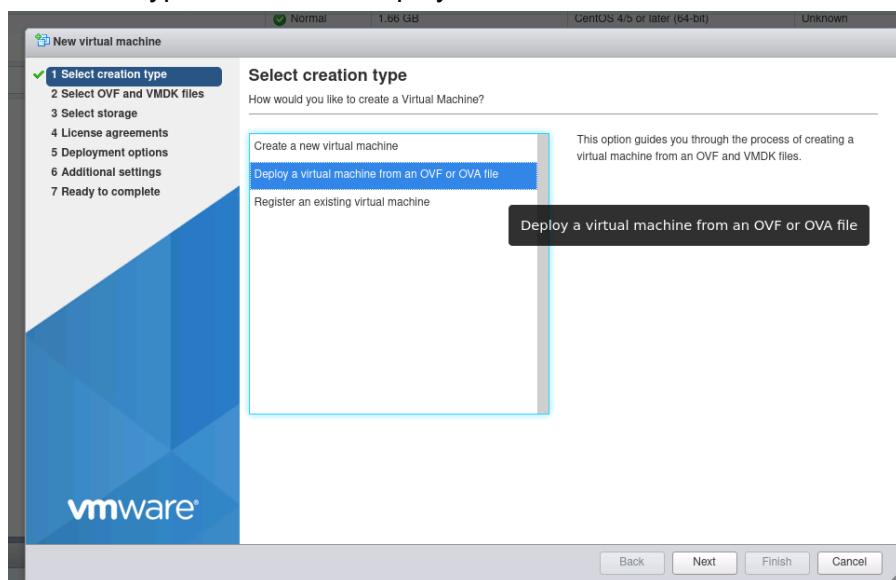


8. Cree los servidores de acuerdo a la imagen base

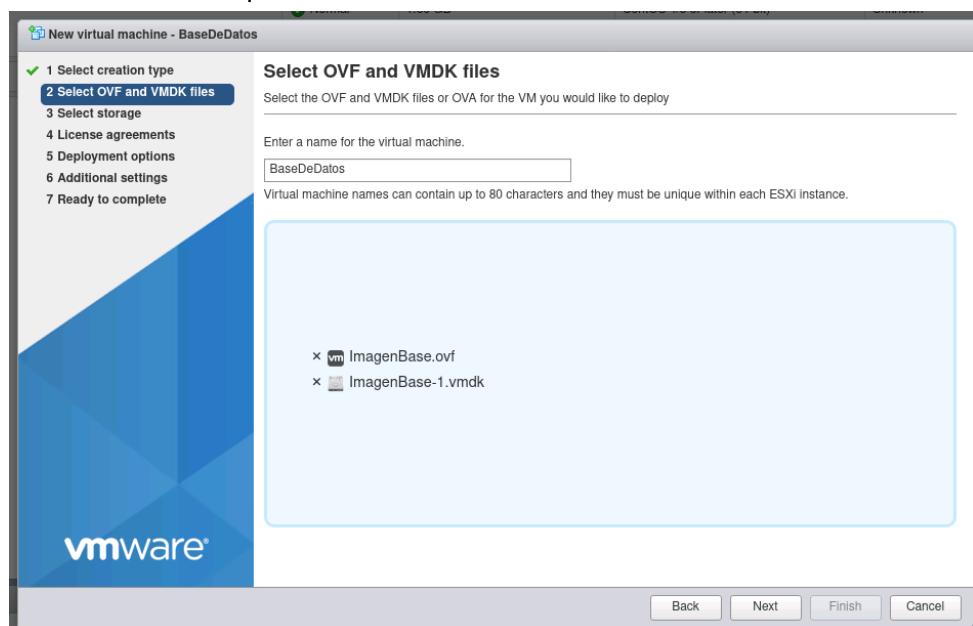
1. Seleccione la opción Create/ Register VM

A screenshot of a web-based interface titled "vm-131-026.unac.ucr.ac.cr - Virtual Machines". At the top, there are navigation links: Create / Register VM, Console, Power on, Power off, Suspend, Refresh, and Actions. Below this is a table listing existing virtual machines. The first row shows "VirtualBox" with a status of "Normal", used space of "1.66 GB", guest OS as "CentOS 4/5 or later (64-bit)", host name as "Unknown", host CPU as "0 MHz", and host memory as "0 MB". The second row shows "ImagenBase" with similar details. A "Create or register a virtual machine" button is prominently displayed in the center of the table. The status bar at the bottom right shows the user's name "hellen.fernandezjimenez@172.24.131.26" and a "Search" field.

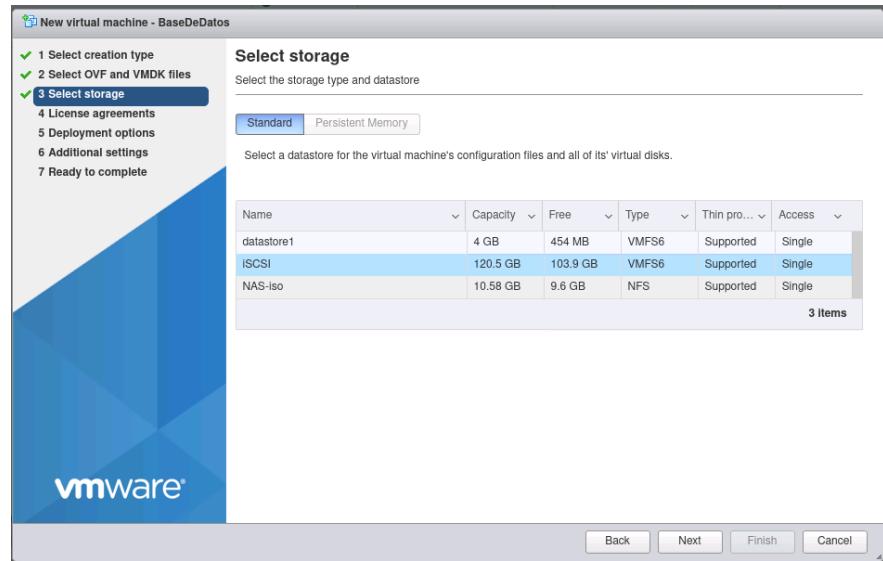
2. En select creation type, seleccione Deploy a virtual machine from an OVF or OVA file.



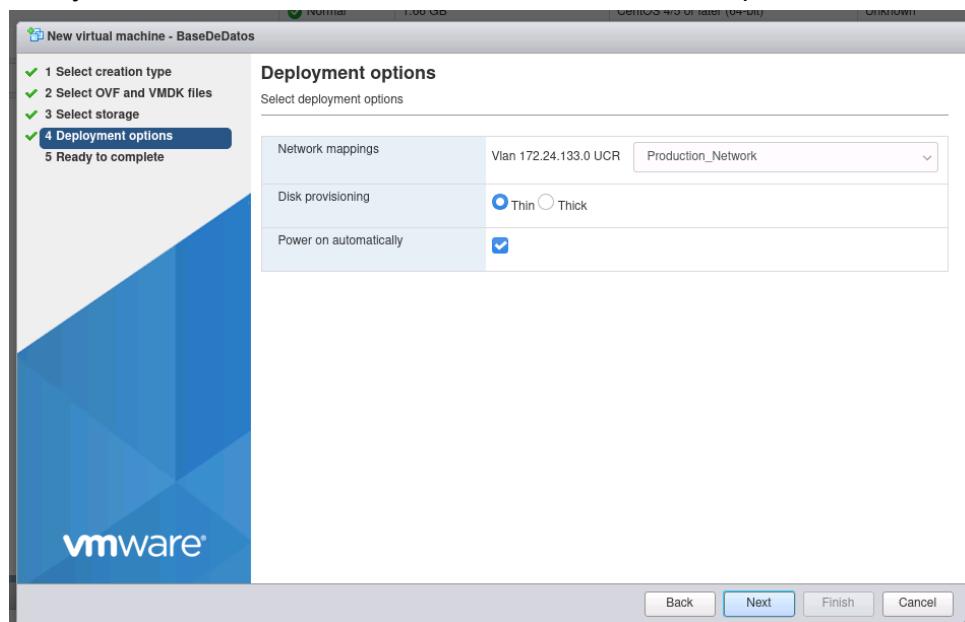
3. En Select OVF and VMDK files, seleccionar el nombre de la máquina virtual del servicio que se va a realizar en esta máquina virtual.



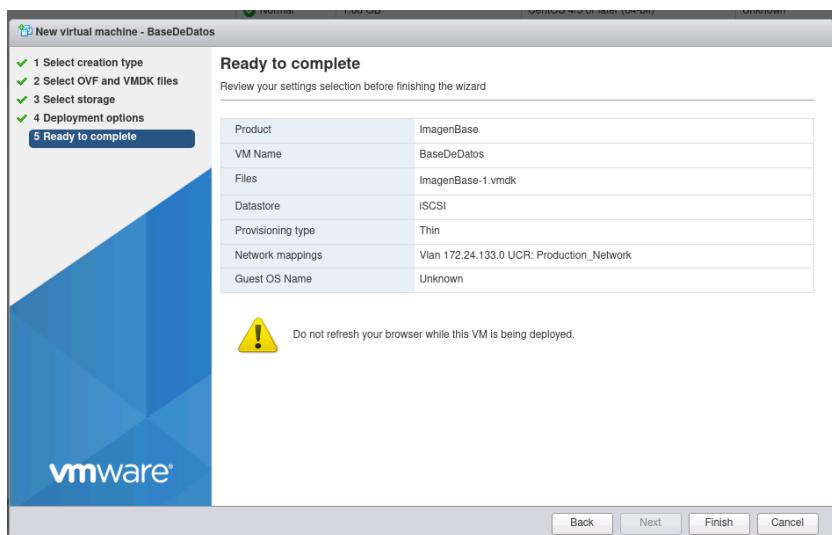
4. En la parte de select storage, se selecciona iSCSI que es correspondiente al almacenaje SAN para las máquinas virtuales:



- En la sección de deployment options, seleccionar la vlan que se desea que sea utilizada para esta máquina, dejar las otras opciones por defecto y seleccione next. En este caso, inicialmente como parte de las pruebas y como parte del proceso de aprendizaje, coloque las máquinas en la VLAN cuyas direcciones tuvieran acceso a internet, para poder descargar respectivamente los paquetes correspondientes a estos servicios, esto posteriormente fue modificado. Elija modo Thin, de esta forma sólo se reservará el espacio necesario.



- Posteriormente, se da click en finalizar.



Este proceso se repite para cada uno de los servicios, hasta que quede de la siguiente forma:

Virtual machine	Status	Used space	Guest OS	Host name	Host CPU	Host memory
centos7	Normal	1.66 GB	CentOS 4/5 or later (64-bit)	Unknown	0 MHz	0 MB
ImagenBase	Normal	13.98 GB	CentOS 7 (64-bit)	Unknown	12 MHz	435 MB
BaseDeDatos	Normal	4.14 GB	CentOS 7 (64-bit)	Unknown	12 MHz	439 MB
ServidorApache	Normal	4.14 GB	CentOS 7 (64-bit)	Unknown	14 MHz	442 MB

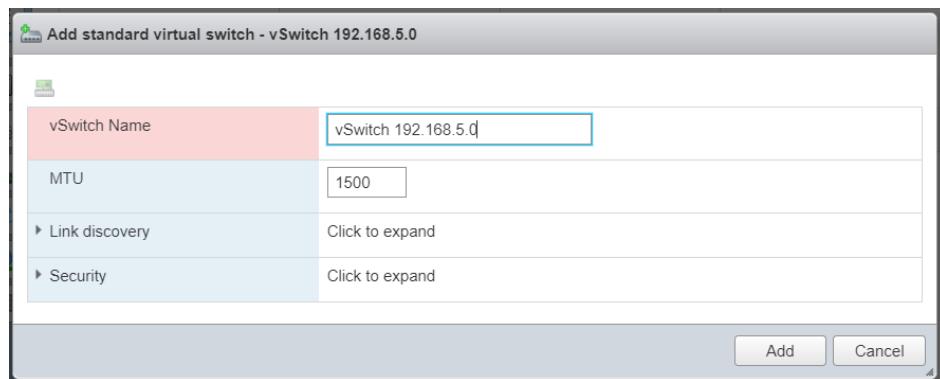
4. Cree red privada

Para este trabajo, es necesario que la base de datos y el servidor web se comuniquen a través de una red privada. Para alcanzar este objetivo, es necesario configurar un nuevo virtual switch que permita estas condiciones. Mediante los siguientes pasos.

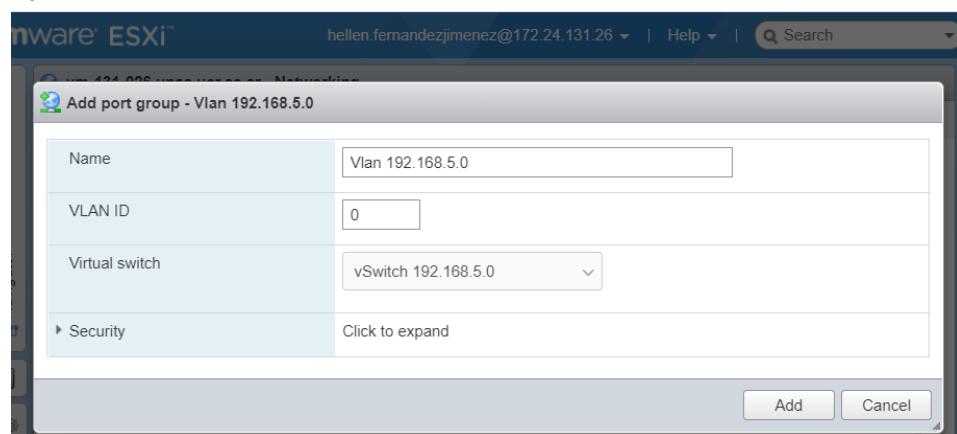
- Diríjase a la parte de networking, seleccione virtual switches y posteriormente haga click en add el el icono de Add a new standard virtual switch.

Name	Uplinks	Type
vSwitch0	1	Standard vSwitch
vSwitch1	1	Standard vSwitch
vSwitch2	2	Standard vSwitch
vSwitch3	1	Standard vSwitch
vSwitch4	0	Standard vSwitch

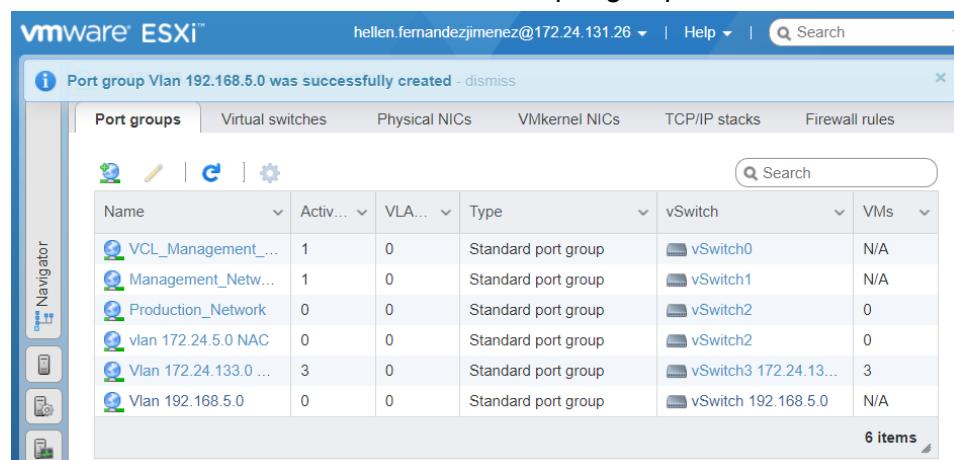
2. Escriba el nombre del switch y deje la configuración por defecto de las otras opciones:



3. En la parte de Port groups, seleccione el icono de Add port group, seleccione el nombre del port group, y seleccione el switch que fue recientemente creado, hacer click en Add:



4. Si se crea correctamente, deberá salir en la lista de portgroups:



Name	Activ...	VLA...	Type	vSwitch	VMs
VCL_Management_...	1	0	Standard port group	vSwitch0	N/A
Management_Netw...	1	0	Standard port group	vSwitch1	N/A
Production_Network	0	0	Standard port group	vSwitch2	0
vlan 172.24.5.0 NAC	0	0	Standard port group	vSwitch2	0
Vlan 172.24.133.0 ...	3	0	Standard port group	vSwitch3 172.24.13...	3
Vlan 192.168.5.0	0	0	Standard port group	vSwitch 192.168.5.0	N/A

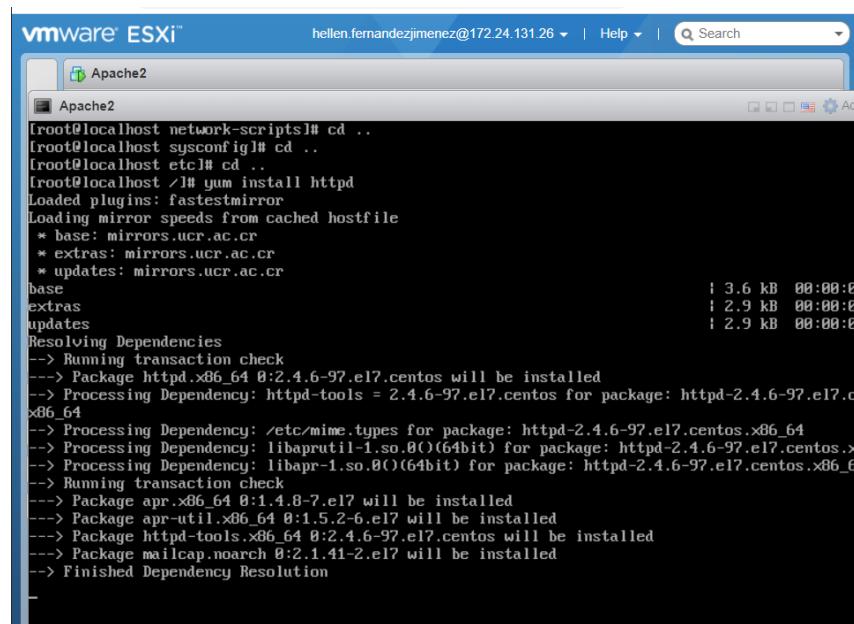
5. Implementación de servicios

1. Instale apache

Apache es el servidor http que va a ser utilizado en este caso para que soporte WordPress.
Para instalarlo siga los siguientes pasos:

1. Instale apache con el comando:

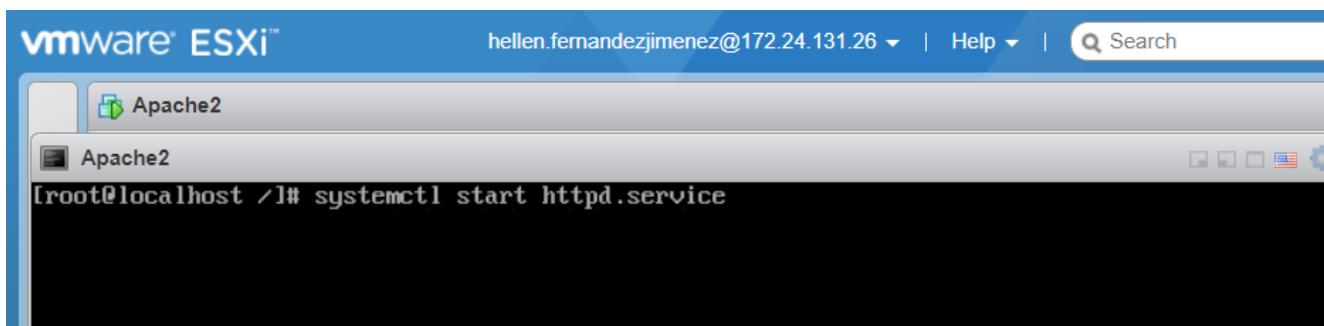
```
yum install httpd -y
```



```
[root@localhost network-scripts]# cd ..
[root@localhost sysconfig]# cd ..
[root@localhost etc]# cd ..
[root@localhost /]# yum install httpd
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirrors.ucr.ac.cr
 * extras: mirrors.ucr.ac.cr
 * updates: mirrors.ucr.ac.cr
base                                         | 3.6 kB  00:00:0
extras                                        | 2.9 kB  00:00:0
updates                                       | 2.9 kB  00:00:0
Resolving Dependencies
--> Running transaction check
--> Package httpd.x86_64 0:2.4.6-97.el7.centos will be installed
--> Processing Dependency: httpd-tools = 2.4.6-97.el7.centos for package: httpd-2.4.6-97.el7.c
x86_64
--> Processing Dependency: /etc/mime.types for package: httpd-2.4.6-97.el7.centos.x86_64
--> Processing Dependency: libaprutil-1.so.0()(64bit) for package: httpd-2.4.6-97.el7.centos.x
--> Processing Dependency: libapr-1.so.0()(64bit) for package: httpd-2.4.6-97.el7.centos.x86_6
--> Running transaction check
--> Package apr.x86_64 0:1.4.8-7.el7 will be installed
--> Package apr-util.x86_64 0:1.5.2-6.el7 will be installed
--> Package httpd-tools.x86_64 0:2.4.6-97.el7.centos will be installed
--> Package mailcap.noarch 0:2.1.41-2.el7 will be installed
--> Finished Dependency Resolution
```

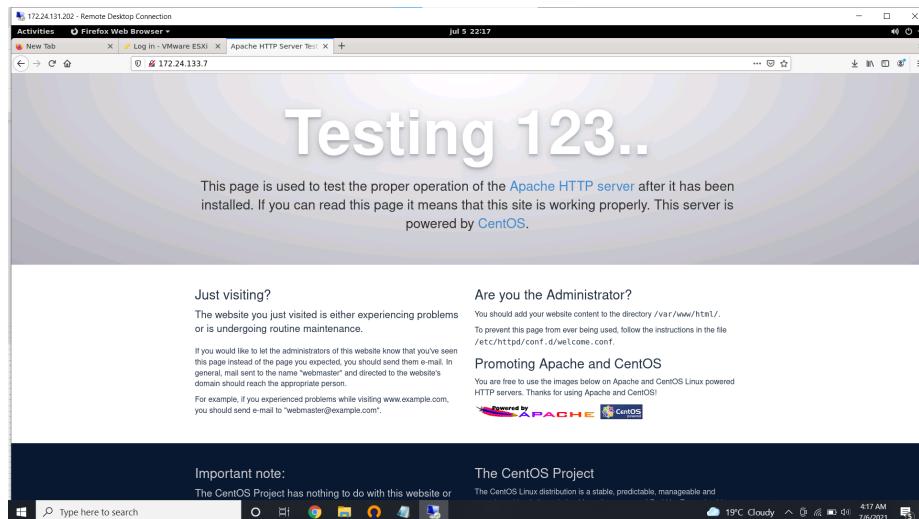
2. Inicie el servicio con el comando:

```
systemctl start httpd.service
```



```
[root@localhost /]# systemctl start httpd.service
```

- Se verifica que funcione desde una máquina reservada en VCL escribiendo desde el navegador la dirección ip del apache que tiene salida a internet según el direccionamiento planteado: 172.24.133.7



- Habilite la opción de que apache inicie cuando se reinicie la máquina:

```
sudo systemctl enable httpd.service
```

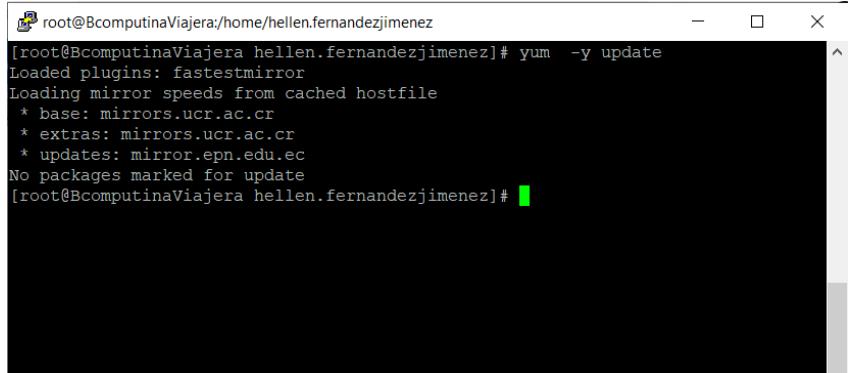
The screenshot shows a terminal window titled 'Apache2' on a VMware ESXi host. The user is running the command 'sudo systemctl enable httpd.service'. The output shows that a symlink was created from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system/httpd.service. The terminal window has a blue header bar with the VMware logo and the user's session information: 'hellen.fernandezjimenez@172.24.131.26'.

```
[root@localhost ~]# systemctl enable httpd.service
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system/httpd.service.
[root@localhost ~]#
```

2. Instale MariaDB

- Asegúrese de estar ejecutando un servidor CentOS 7 actualizado con el comando:

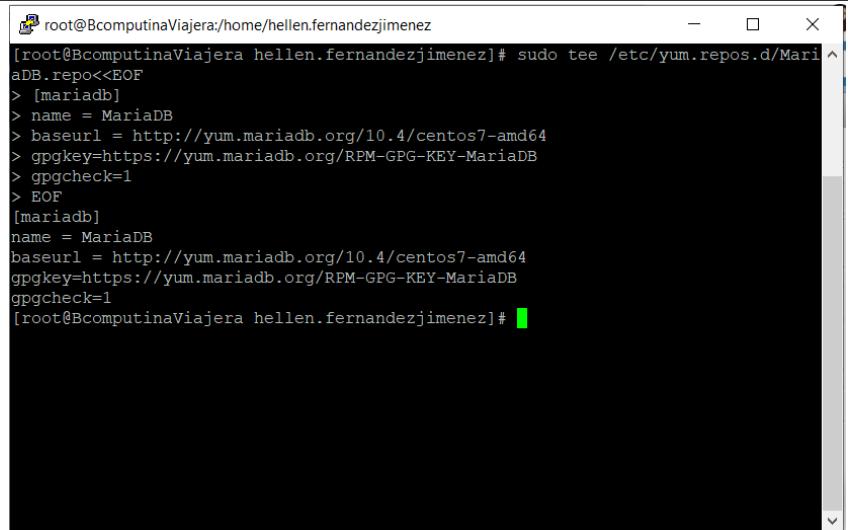
```
sudo yum -y update
```



```
[root@BcomputinaViajera ~]# yum -y update
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirrors.ucr.ac.cr
 * extras: mirrors.ucr.ac.cr
 * updates: mirror.epn.edu.ec
No packages marked for update
[root@BcomputinaViajera ~]#
```

2. Modifique la versión de yum para que se pueda instalar la versión 10.4:

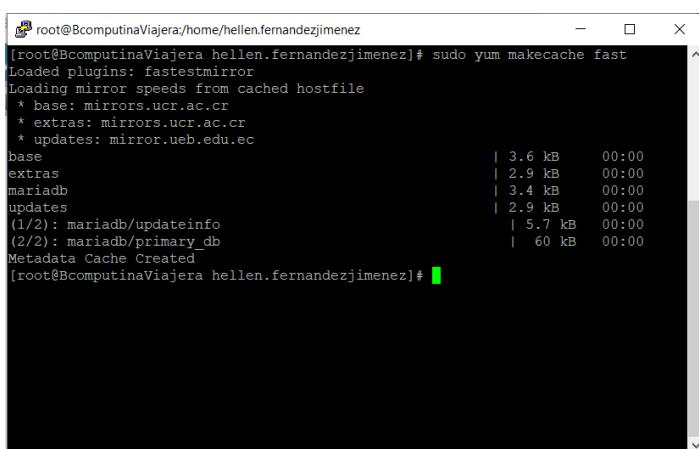
```
sudo tee /etc/yum.repos.d/MariaDB.repo<<EOF
[mariadb]
name = MariaDB
baseurl = http://yum.mariadb.org/10.4/centos7-amd64
gpgkey=https://yum.mariadb.org/RPM-GPG-KEY-MariaDB
gpgcheck=1
EOF
```



```
[root@BcomputinaViajera ~]# sudo tee /etc/yum.repos.d/Mariadb.repo<<EOF
> [mariadb]
> name = MariaDB
> baseurl = http://yum.mariadb.org/10.4/centos7-amd64
> gpgkey=https://yum.mariadb.org/RPM-GPG-KEY-MariaDB
> gpgcheck=1
> EOF
> [mariadb]
> name = MariaDB
> baseurl = http://yum.mariadb.org/10.4/centos7-amd64
> gpgkey=https://yum.mariadb.org/RPM-GPG-KEY-MariaDB
> gpgcheck=1
[root@BcomputinaViajera ~]#
```

3. Actualice cache index:

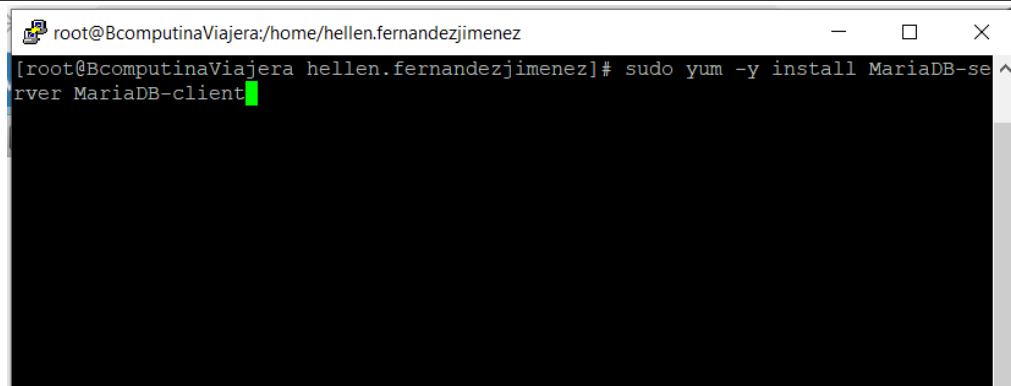
```
sudo yum makecache fast
```



```
[root@BcomputinaViajera ~]# sudo yum makecache fast
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirrors.ucr.ac.cr
 * extras: mirrors.ucr.ac.cr
 * updates: mirror.epn.edu.ec
base                                         | 3.6 kB     00:00
extras                                        | 2.9 kB     00:00
mariadb                                       | 3.4 kB     00:00
updates                                        | 2.9 kB     00:00
(1/2): mariadb/updateinfo                   | 5.7 kB     00:00
(2/2): mariadb/primary_db                    | 60 kB      00:00
Metadata Cache Created
[root@BcomputinaViajera ~]#
```

4. Instale MariaDB 10.4 usando el administrador de paquetes yum:

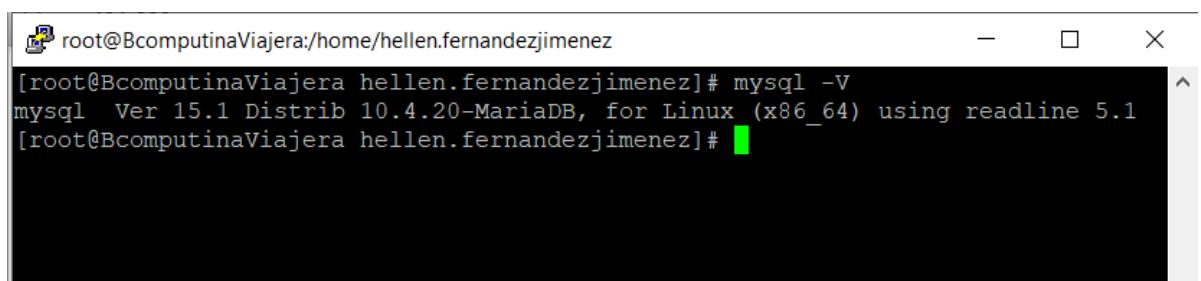
```
sudo yum -y install MariaDB-server MariaDB-client
```



A terminal window titled 'root@BcomputinaViajera:/home/hellen.fernandezjimenez'. The command 'sudo yum -y install MariaDB-server MariaDB-client' is entered at the prompt. The window has standard Linux terminal icons at the top.

5. Revise la versión de mariadb que está instalada, debería ser la 10.4:

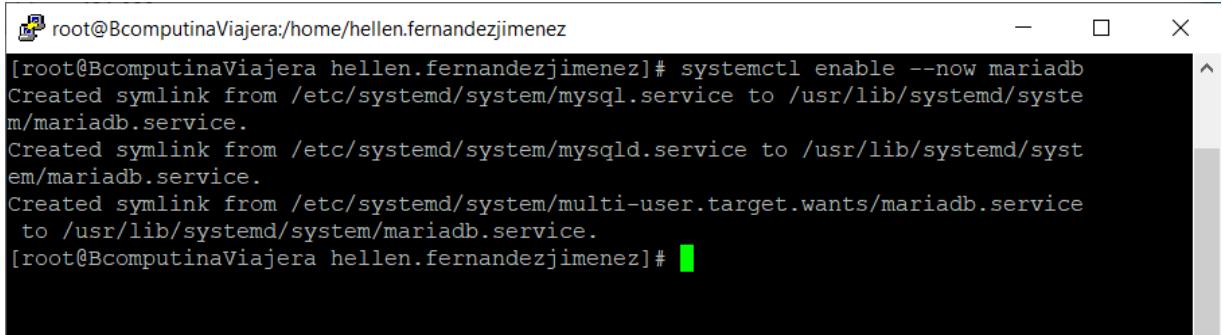
```
mysql -V
```



A terminal window titled 'root@BcomputinaViajera:/home/hellen.fernandezjimenez'. The command 'mysql -V' is entered at the prompt. The output shows 'mysql Ver 15.1 Distrib 10.4.20-MariaDB, for Linux (x86_64) using readline 5.1'. The window has standard Linux terminal icons at the top.

6. Inicie y habilite el servicio MariaDB

```
sudo systemctl enable --now mariadb
```

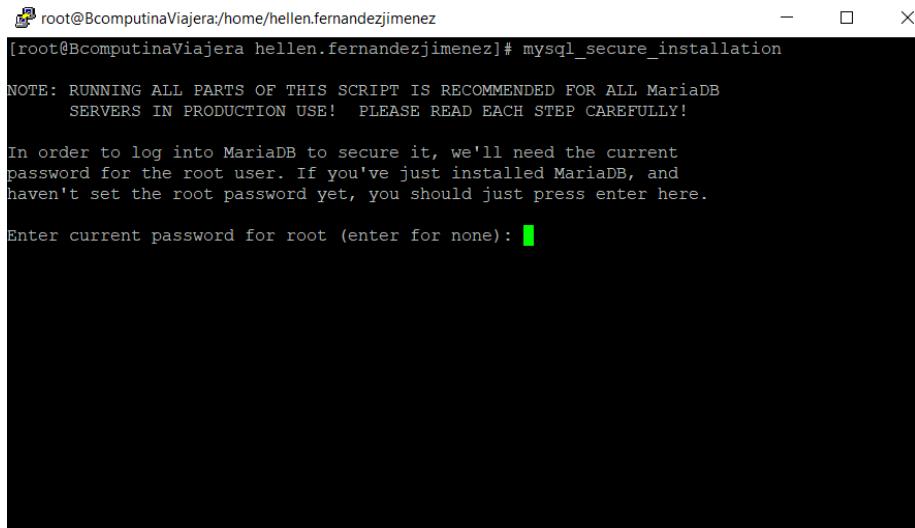


A terminal window titled 'root@BcomputinaViajera:/home/hellen.fernandezjimenez'. The command 'systemctl enable --now mariadb' is entered at the prompt. The output shows the creation of symlinks from /etc/systemd/system/mysql.service to /usr/lib/systemd/system/mariadb.service, and from /etc/systemd/system/mysqld.service to /usr/lib/systemd/system/mariadb.service. It also creates a symlink from /etc/systemd/system/multi-user.target.wants/mariadb.service to /usr/lib/systemd/system/mariadb.service. The window has standard Linux terminal icons at the top.

3. Configure MariaDB

1. Ahora que MariaDB 10.4 está instalado en CentOS 7, asegúrelo ejecutando:

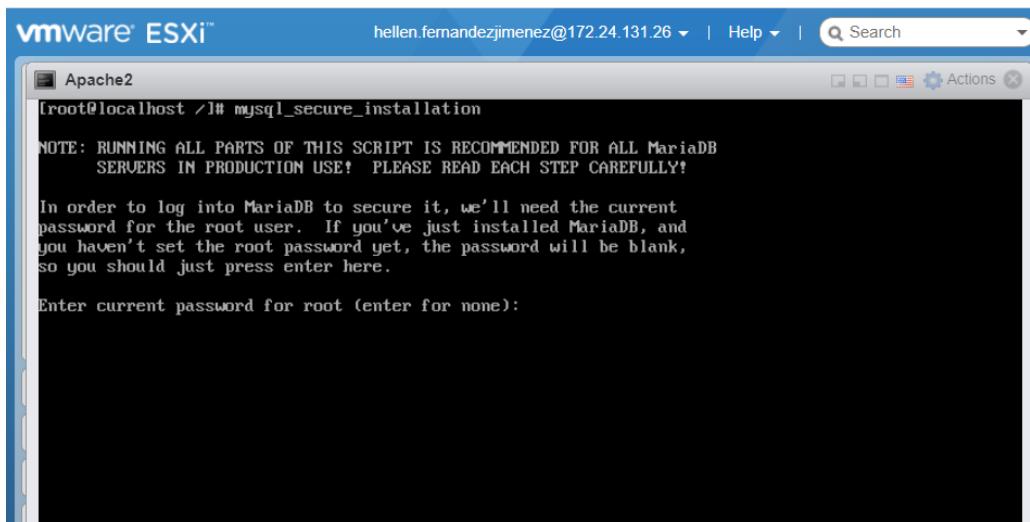
```
# mysql_secure_installation
```



```
[root@BcomputinaViajera ~]# mysql_secure_installation
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!
In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
haven't set the root password yet, you should just press enter here.

Enter current password for root (enter for none):
```

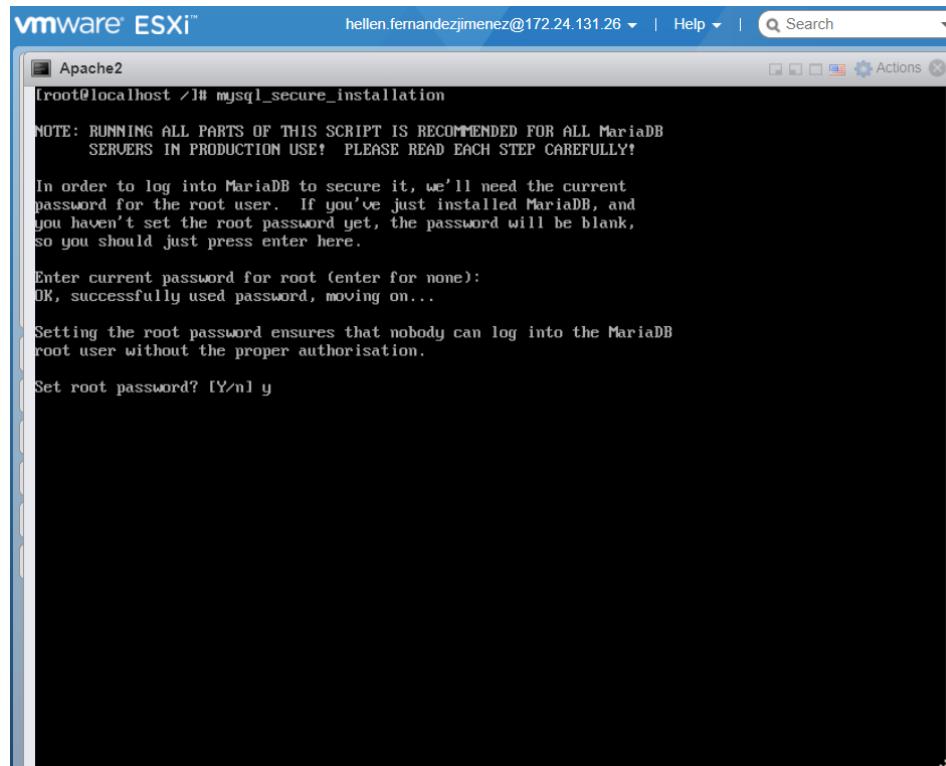
2. Digite enter porque en este momento no hay contraseña para root:



```
hellen.fernandezjimenez@172.24.131.26 | Help | Search
Apache2
[root@localhost ~]# mysql_secure_installation
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!
In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none):
```

3. Cuando pregunte si desea establecer una contraseña para root digite "y" y enter:

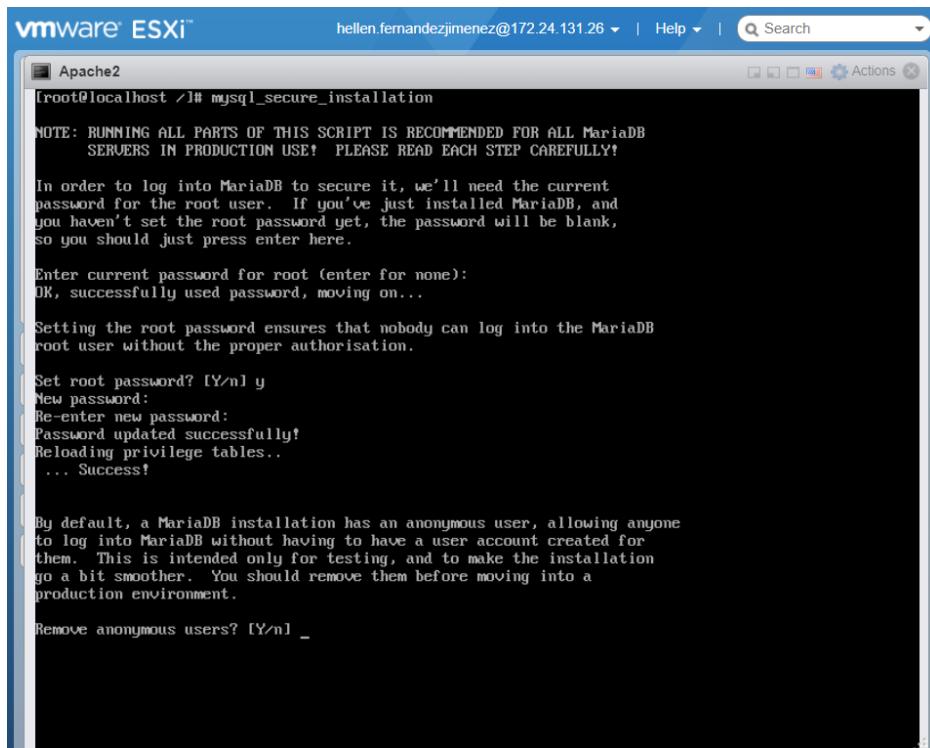


```
hellen.fernandezjimenez@172.24.131.26 | Help | Search
Apache2
[root@localhost ~]# mysql_secure_installation
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!
In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...
Setting the root password ensures that nobody can log into the MariaDB
root user without the proper authorisation.

Set root password? [Y/n] y
```

4. Escriba la contraseña para root mariaDB:
1UcHiT44



```
root@localhost ~# mysql_secure_installation
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

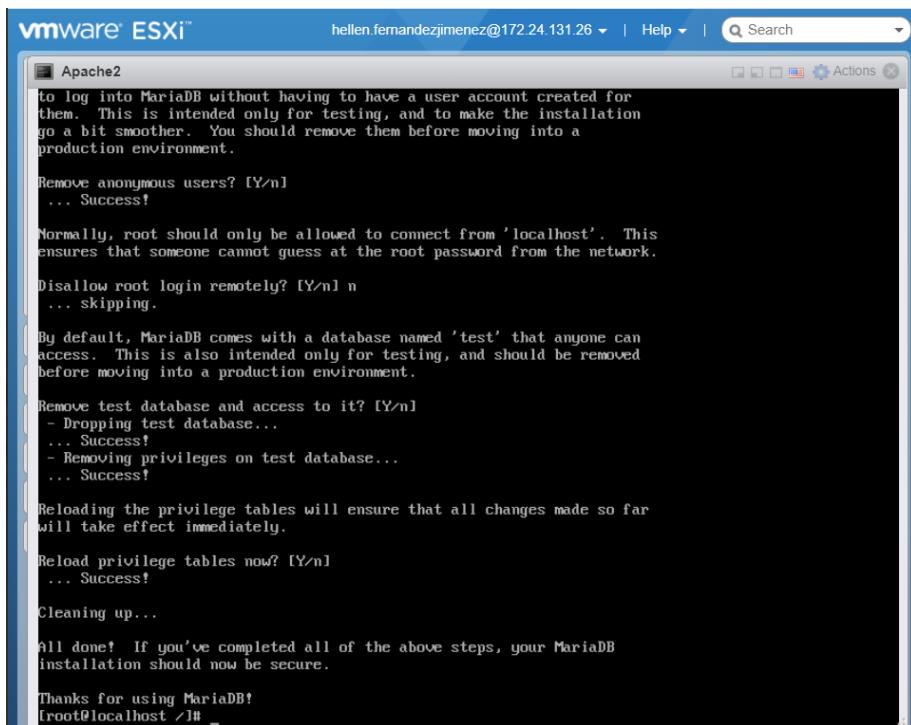
Setting the root password ensures that nobody can log into the MariaDB
root user without the proper authorisation.

Set root password? [Y/n] y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
... Success!

By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them. This is intended only for testing, and to make the installation
go a bit smoother. You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] _
```

5. Presione la tecla enter hasta que salga del programa, esto acepta las opciones que ahí se presentan:



```
to log into MariaDB without having to have a user account created for
them. This is intended only for testing, and to make the installation
go a bit smoother. You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n]
... Success!

Normally, root should only be allowed to connect from 'localhost'. This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n]
... skipping.

By default, MariaDB comes with a database named 'test' that anyone can
access. This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n]
- Dropping test database...
... Success!
- Removing privileges on test database...
... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n]
... Success!

Cleaning up...

All done! If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
[root@localhost ~]# _
```

6. Ingrese a mysql:

```
# mysql -u root -p
```

Digite la contraseña: 1UcHiT44

```
[root@BcomputinaViajera:~/home/hellen.fernandezjimenez]
[root@BcomputinaViajera hellen.fernandezjimenez]# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 15
Server version: 10.4.20-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> 
```

7. Cree la base de datos para wordpress:

```
CREATE DATABASE BaseViajera;
```

```
[root@BcomputinaViajera:~/home/hellen.fernandezjimenez]
[root@BcomputinaViajera hellen.fernandezjimenez]# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 9
Server version: 5.5.68-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> CREATE DATABASE BaseViajera;
Query OK, 1 row affected (0.01 sec)

MariaDB [(none)]> 
```

8. Cree un usuario para la base de datos con la dirección privada otorgada al servidor web, ya que este será el cliente que va a consultar a esta base de datos, esto se realiza de la siguiente manera:

```
CREATE USER compuUsuaria@192.168.5.4 IDENTIFIED BY 'm4.GgUi3';
CREATE USER compuUsuaria@192.168.5.5 IDENTIFIED BY 'm4.GgUi3';
```

```
CREATE USER compuUsuaria@192.168.5.3 IDENTIFIED BY 'm4.GgUi3';
```

```

root@BcomputinaViajera:/home/hellen.fernandezjimenez# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 9
Server version: 5.5.68-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> CREATE DATABASE BaseViajera;
Query OK, 1 row affected (0.01 sec)

MariaDB [(none)]> CREATE USER compuUsuaria@192.168.5.3 IDENTIFIED BY 'm4.GgUi3';
Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]>

```

9. Asígnele todos los privilegios al usuario recientemente creado sobre la base de datos creada para el sitio de Wordpress:

```

GRANT ALL PRIVILEGES ON BaseViajera.* TO compuUsuaria@192.168.5.4 IDENTIFIED BY
'm4.GgUi3';
GRANT ALL PRIVILEGES ON BaseViajera.* TO compuUsuaria@192.168.5.5 IDENTIFIED BY
'm4.GgUi3';
GRANT ALL PRIVILEGES ON BaseViajera.* TO compuUsuaria@192.168.5.3 IDENTIFIED BY
'm4.GgUi3';

```

```

root@BcomputinaViajera:/home/hellen.fernandezjimenez# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 9
Server version: 5.5.68-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> CREATE DATABASE BaseViajera;
Query OK, 1 row affected (0.01 sec)

MariaDB [(none)]> CREATE USER compuUsuaria@192.168.5.3 IDENTIFIED BY 'm4.GgUi3';
Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON BaseViajera.* TO compuUsuaria@192.168.5.3 IDENTIFIED BY 'm
4.GgUi3';
Query OK, 0 rows affected (0.01 sec)

MariaDB [(none)]>

```

FLUSH PRIVILEGES;

```

root@BcomputinaViajera:/home/hellen.fernandezjimenez# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 9
Server version: 5.5.68-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> CREATE DATABASE BaseViajera;
Query OK, 1 row affected (0.01 sec)

MariaDB [(none)]> CREATE USER compuUsuaria@192.168.5.3 IDENTIFIED BY 'm4.GgUi3';
Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON BaseViajera.* TO compuUsuaria@192.168.5.3 IDENTIFIED BY 'm
4.GgUi3';
Query OK, 0 rows affected (0.01 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]>

```

10. Digite exit para salir:

```
exit
```

```
[root@BcomputinaViajera /home/hellen.fernandezjimenez]# Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 9
Server version: 5.5.68-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> CREATE DATABASE BaseViajera;
Query OK, 1 row affected (0.01 sec)

MariaDB [(none)]> CREATE USER compuUsuaria@192.168.5.3 IDENTIFIED BY 'm4.GgUi3';
Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON BaseViajera.* TO compuUsuaria@192.168.5.3 IDENTIFIED BY 'm4.GgUi3';
Query OK, 0 rows affected (0.01 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]> exit
Bye
[root@BcomputinaViajera hellen.fernandezjimenez]#
```

11. Ahora, desde el servidor de apache, que en este caso es el servidor cliente, pruebe la conexión remota hacia la base de datos con el comando:

```
mysql -u compuUsuaria -h 192.168.5.7 -p
```

```
# mysql -u compuUsuaria -h 192.168.5.2 -p
```

Introduzca la contraseña establecida anteriormente para ese usuario.

Escriba:

```
SHOW TABLES
```

En este punto debería salir la Tabla creada para la base de datos BaseViajera que fue la creada para Wordpress.

```
[root@computinaViajera hellen.fernandezjimenez]# mysql -u compuUsuaria -h 192.168.5.2 -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 10
Server version: 5.5.68-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show Tables
      -> ;
ERROR 1046 (3D000): No database selected
MariaDB [(none)]> show databases
      -> ;
+-----+
| Database |
+-----+
| information_schema |
| BaseViajera |
+-----+
2 rows in set (0.00 sec)

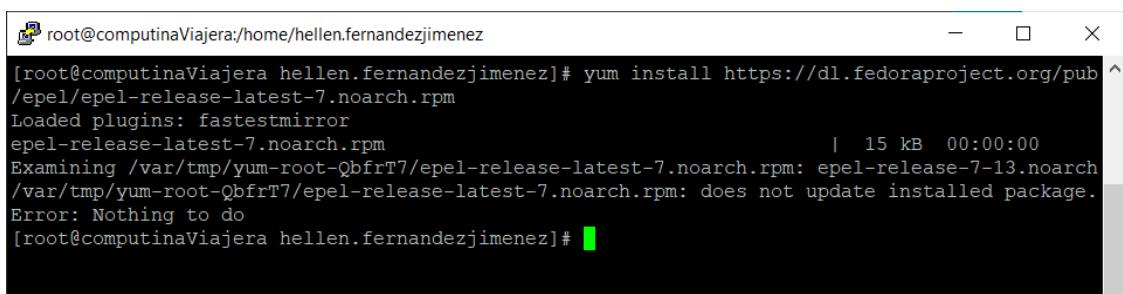
MariaDB [(none)]>
```

4. Instale PHP

PHP es un requisito que tiene Wordpress para poder funcionar. En este caso se debe instalar la versión 7.4 ya que Wordpress necesita como mínimo PHP 5.2, sin embargo no es lo recomendable. Actualmente se encuentra liberada la versión 8.0 sin embargo aún no es una versión estable presenta algunos problemas con Wordpress, así que la versión 7.4 es adecuada en este caso. Para realizar esto siga los siguientes pasos:

1. Obtenga la última liberación de php versión 7.

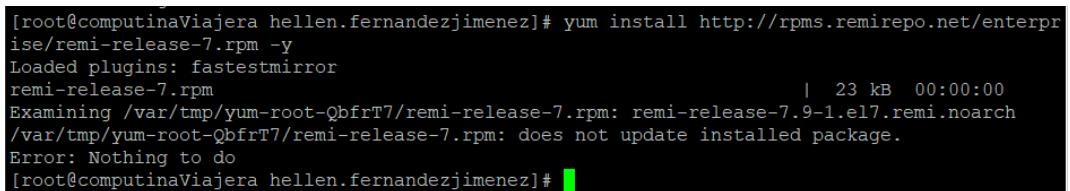
```
# yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm -y
```



```
[root@computinaViajera hellen.fernandezjimenez]# yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
Loaded plugins: fastestmirror
epel-release-latest-7.noarch.rpm | 15 kB 00:00:00
Examining /var/tmp/yum-root-QbfrT7/epel-release-latest-7.noarch.rpm: epel-release-7-13.noarch
/var/tmp/yum-root-QbfrT7/epel-release-latest-7.noarch.rpm: does not update installed package.
Error: Nothing to do
[root@computinaViajera hellen.fernandezjimenez]#
```

2. Instale el repositorio que cuenta con la versión 7 de PHP:

```
# yum install http://rpms.remirepo.net/enterprise/remi-release-7.rpm -y
```



```
[root@computinaViajera hellen.fernandezjimenez]# yum install http://rpms.remirepo.net/enterprise/remi-release-7.rpm -y
Loaded plugins: fastestmirror
remi-release-7.rpm | 23 kB 00:00:00
Examining /var/tmp/yum-root-QbfrT7/remi-release-7.rpm: remi-release-7.9-1.el7.remi.noarch
/var/tmp/yum-root-QbfrT7/remi-release-7.rpm: does not update installed package.
Error: Nothing to do
[root@computinaViajera hellen.fernandezjimenez]#
```

3. Instale el paquete yum-utils:

```
# yum install yum-utils
```

```
[root@computinaViajera hellen.fernandezjimenez]# yum install yum-utils
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
epel/x86_64/metalink
* base: mirrors.ucr.ac.cr
* epel: dl.fedoraproject.org
* extras: mirrors.ucr.ac.cr
* remi-php56: mirror.pit.terawhite.com
* remi-safe: mirror.pit.terawhite.com
* updates: mirror.epn.edu.ec
base
epel
extras
remi-php56
remi-safe
updates
(1/4): epel/x86_64/updateinfo
(2/4): remi-safe/primary_db
(3/4): epel/x86_64/primary_db
(4/4): updates/7/x86_64/primary_db
Package yum-utils-1.1.31-54.el7_8.noarch already installed and latest version
Nothing to do
[root@computinaViajera hellen.fernandezjimenez]#
```

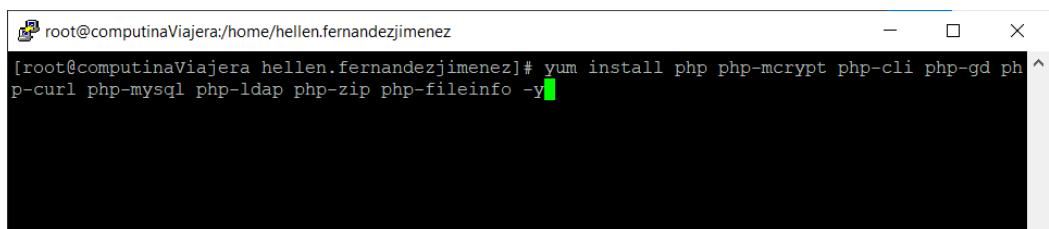
4. Habilite el repositorio remi-php74

```
# yum-config-manager --enable remi-php74
```

```
[root@computinaViajera hellen.fernandezjimenez]# yum-config-manager --enable remi-php74
Loaded plugins: fastestmirror
=====
[remi-php74]
async = True
bandwidth = 0
base_persistdir = /var/lib/yum/repos/x86_64/7
baseurl =
cache = 0
cachedir = /var/cache/yum/x86_64/7/remi-php74
check_config_file_age = True
compare_providers_priority = 80
cost = 1000
deltarpm_metadata_percentage = 100
deltarpm_percentage =
enabled = 1
enableingroups = True
exclude =
failovermethod = priority
ftp_disable_epsv = False
gpgadir = /var/lib/yum/repos/x86_64/7/remi-php74/gpgadir
gpgkey =
gpgcheck = True
ggmdir = /var/lib/yum/repos/x86_64/7/remi-php74/ggmdir
ggpkey = file:///etc/pki/rpm-gpg/RPM-GPG-KEY-remi
ndiradir = /var/cache/yum/x86_64/7/remi-php74/headers
http_caching = all
includepkgs =
ip_resolve =
keepalive = True
keepcache = False
mddownloadpolicy = sqlite
mdpolicy = group:small
```

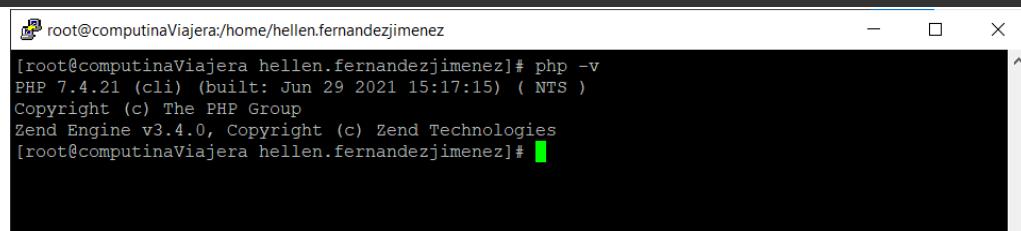
5. Instale los siguientes módulos de PHP necesarios para el correcto funcionamiento de WordPress:

```
# yum install php php-mcrypt php-cli php-gd php-curl php-mysql php-ldap php-zip
php-fileinfo -y
```



6. Verifique la versión de PHP instalada:

```
# php -v
```



```
[root@computinaViajera hellen.fernandezjimenez]# php -v
PHP 7.4.21 (cli) (built: Jun 29 2021 15:17:15) ( NTS )
Copyright (c) The PHP Group
Zend Engine v3.4.0, Copyright (c) Zend Technologies
[root@computinaViajera hellen.fernandezjimenez]#
```

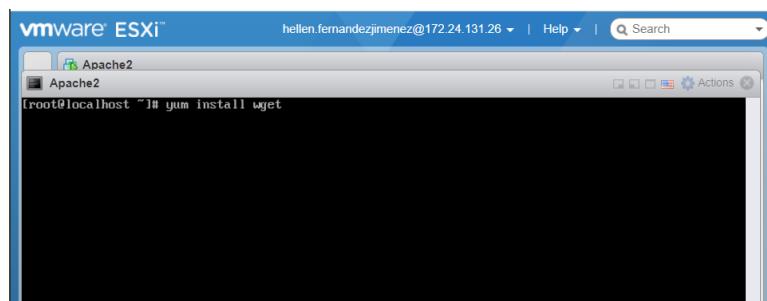
Como se puede observar, efectivamente se instaló una versión 7.4, lo que va a permitir una buena compatibilidad con Wordpress.

5. Instale Wordpress

Wordpress es una aplicación software para crear y gestionar sitios web. Este es el que va a ser utilizado en este caso en el servidor web. Para esto:

1. Instale wget:

```
# yum install wget -y
```

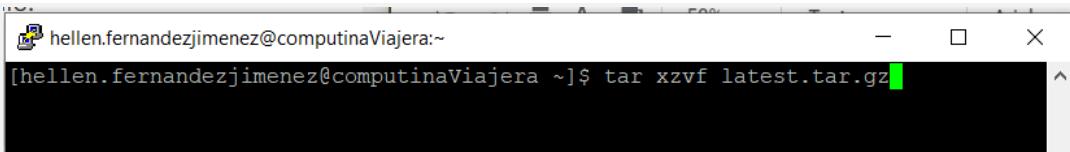


2. Para descargar Wordpress, escriba el siguiente comando:

```
cd ~
wget http://wordpress.org/latest.tar.gz
```

3. Descomprima la descarga de Wordpress que fue realizada anteriormente:

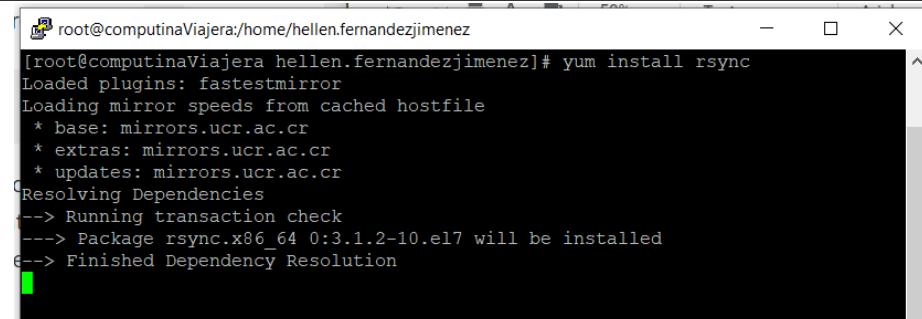
```
tar xzvf latest.tar.gz
```



```
[hellen.fernandezjimenez@computinaViajera:~]$ tar xzvf latest.tar.gz
```

4. Instale rsync:

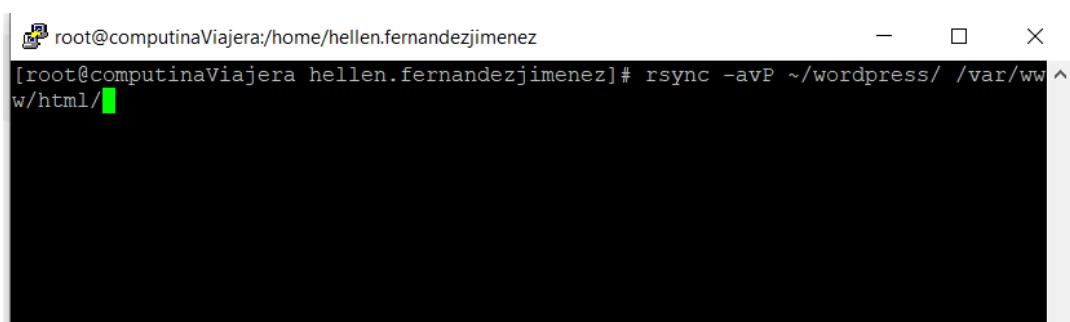
```
# yum install rsync -y
```



```
[root@computinaViajera:~]# yum install rsync
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirrors.ucr.ac.cr
 * extras: mirrors.ucr.ac.cr
 * updates: mirrors.ucr.ac.cr
Resolving Dependencies
--> Running transaction check
--> Package rsync.x86_64 0:3.1.2-10.el7 will be installed
--> Finished Dependency Resolution
```

5. Copie de forma segura todo el contenido del directorio que desempaquetó en la raíz del documento en /var/www/html/

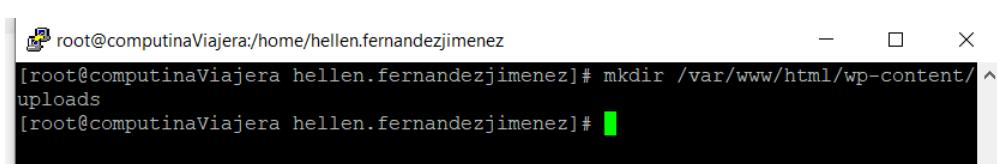
```
# rsync -avP ~/wordpress/ /var/www/html/
```



```
[root@computinaViajera:~]# rsync -avP ~/wordpress/ /var/www/html/
```

6. Realice una carpeta en la dirección de uploads del contenido de wordpress para que Wordpress almacene los archivos cargados de la siguiente forma:

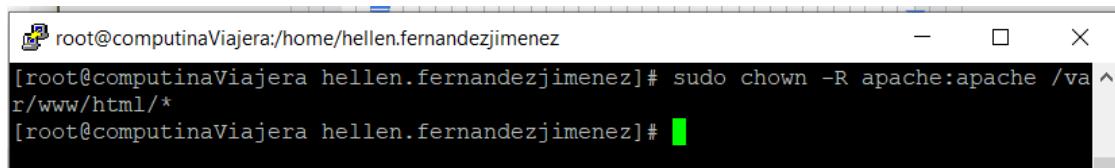
```
# mkdir /var/www/html/wp-content/uploads
```



```
[root@computinaViajera:~]# mkdir /var/www/html/wp-content/uploads
```

7. Asigne la propiedad y los permisos correctos a nuestros archivos y carpetas de WordPress.

```
# chown -R apache:apache /var/www/html/*
```



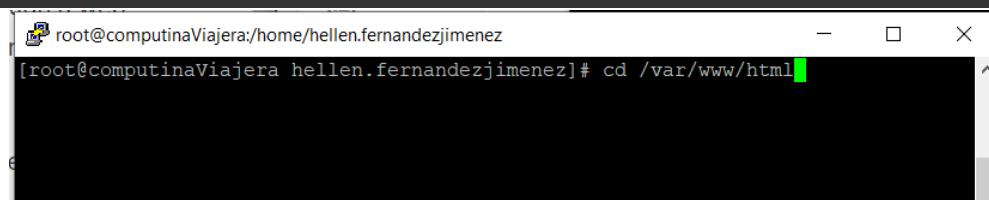
```
root@computinaViajera:/home/hellen.fernandezjimenez
[root@computinaViajera hellen.fernandezjimenez]# sudo chown -R apache:apache /var/www/html/*
[root@computinaViajera hellen.fernandezjimenez]#
```

7. Configure Wordpress

Para configurar Wordpress siga los siguientes pasos:

1. Muévase al directorio raíz de Apache donde instaló WordPress

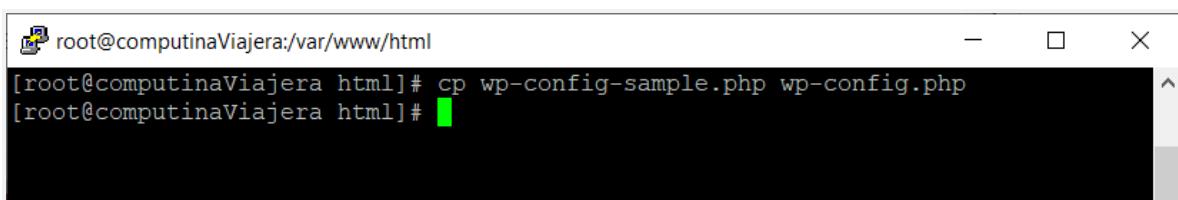
```
# cd /var/www/html
```



```
root@computinaViajera:/home/hellen.fernandezjimenez
[root@computinaViajera hellen.fernandezjimenez]# cd /var/www/html
```

2. El archivo de configuración principal en el que se basa WordPress se llama wp-config.php. De forma predeterminada, se incluye un archivo de configuración de muestra que coincide principalmente con la configuración que se necesita. Copielo a la ubicación predeterminada del archivo de configuración, para que WordPress pueda reconocer y usar el archivo:

```
# cp wp-config-sample.php wp-config.php
```



```
root@computinaViajera:/var/www/html
[root@computinaViajera html]# cp wp-config-sample.php wp-config.php
[root@computinaViajera html]#
```

3. Abra el archivo recién creado:

```
# nano wp-config.php
```



```
root@computinaViajera:/var/www/html
[root@computinaViajera html]# nano wp-config.php
```

4. Edítelo con el nombre de la base de datos, el usuario, la contraseña y la dirección ip del host correspondientes a las que fueron creadas en la base de datos remota de la siguiente forma:

```

root@computinaViajera:/var/www/html
GNU nano 2.3.1          File: wp-config.php          Modified ^

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'BaseViajera' );

/** MySQL database username */
define( 'DB_USER', 'compuUsuaria' );

/** MySQL database password */
define( 'DB_PASSWORD', 'm4.GgUi3' );

/** MySQL hostname */
define( 'DB_HOST', '192.168.5.2' );

/** Database Charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8' );

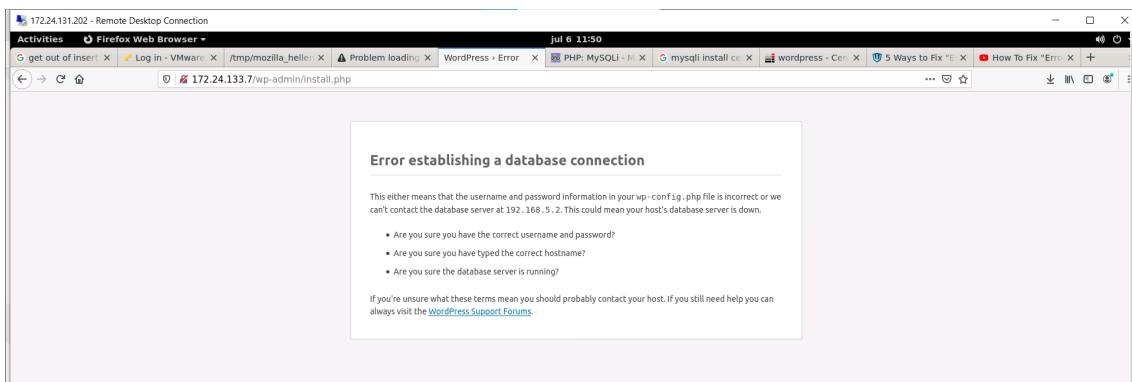
/** The Database Collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );

define('WP_ALLOW_REPAIR',true);

/**#@+
 * Authentication Unique Keys and Salts.
 *
 * Change these to different unique phrases!

```

- Revise la dirección ip correspondiente al servicio desde la máquina ubuntu que fue reservada:



- Este error probablemente se dio debido a la configuración actual de SELinux. Con el siguiente comando se puede comprobar que sí está habilitado SELinux:

```
# sestatus
```

```

root@computinaViajera:/var/www/html
[root@computinaViajera html]# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:              targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Max kernel policy version:      31
[root@computinaViajera html]#

```

- Para arreglar esto, escriba:

```
setsebool -P selinuxuser_mysql_connect_enabled 1
```

```
[root@computinaViajera html]# setsebool -P selinuxuser_mysql_connect_enabled 1
[root@computinaViajera html]#
```

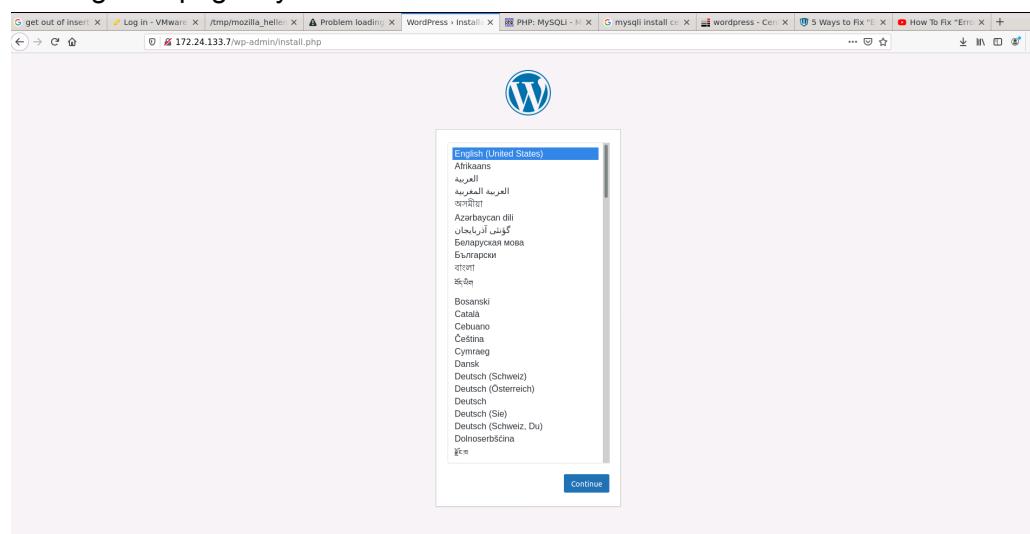
```
# setsebool -P httpd_can_network:connect_db on
```

```
[root@computinaViajera html]# setsebool -P httpd_can_network_connect_db on
[root@computinaViajera html]# setsebool -p httpd_can_network_connect_db on
setsebool: invalid option -- 'p'

Usage:  setsebool [ -NPV ] boolean value | booll=val1 bool2=val2...

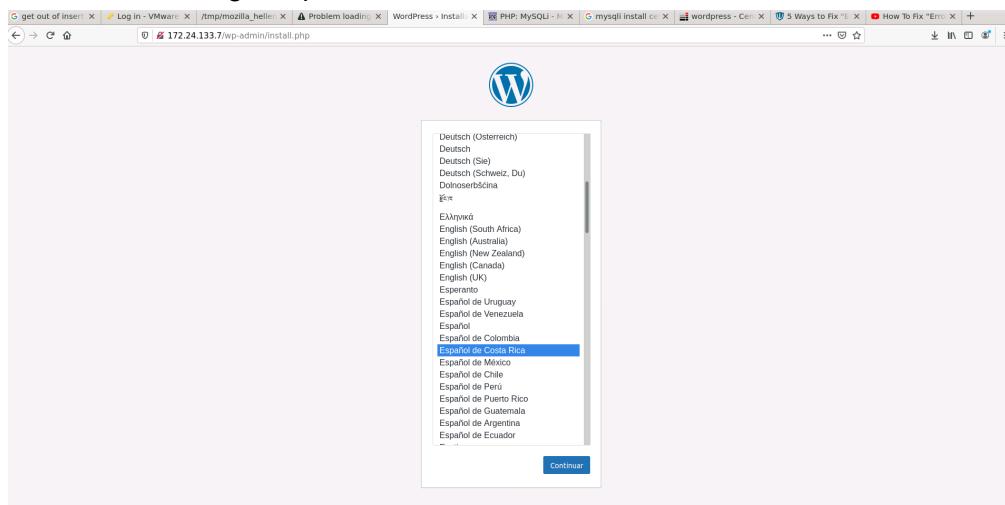
[root@computinaViajera html]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@computinaViajera html]#
```

8. Recargue la página y observe como efectivamente fue efectiva la conexión:

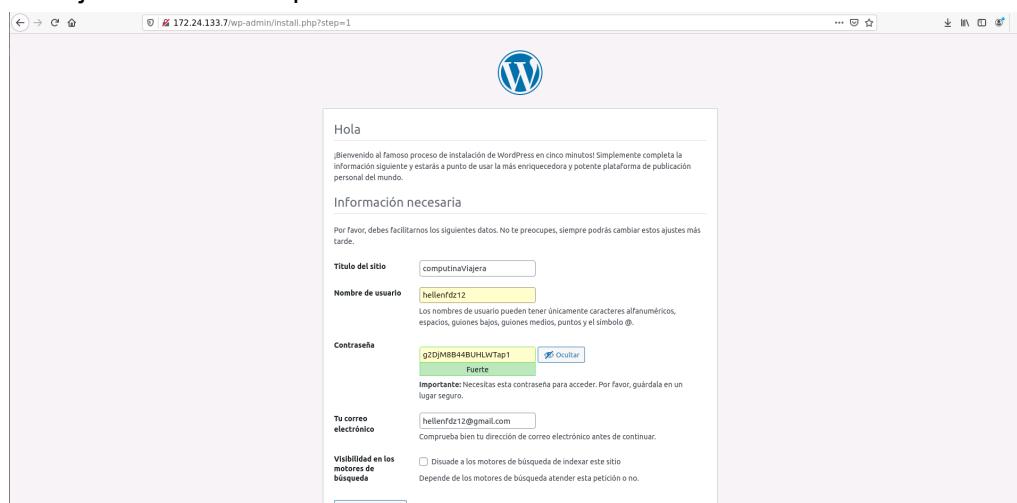


8. Gestione de Wordpress

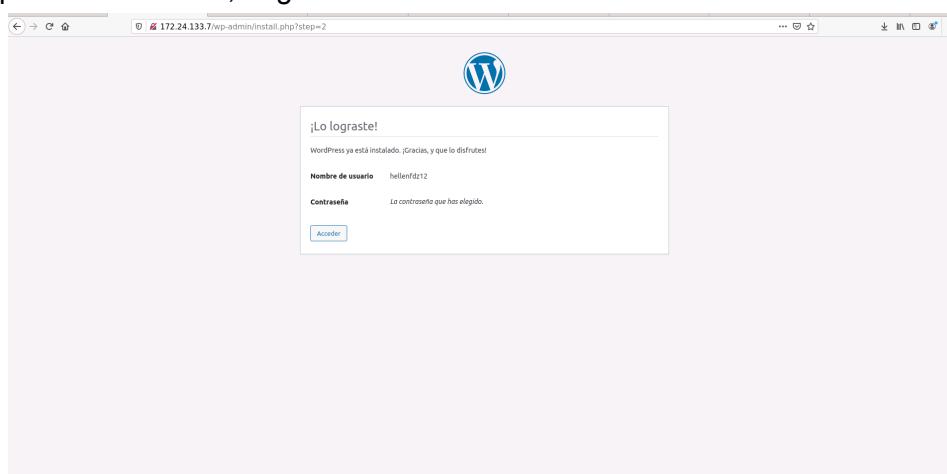
1. Seleccione el idioma que desee para Wordpress y de click en continuar:
En este caso, se va a elegir Español Costa Rica.



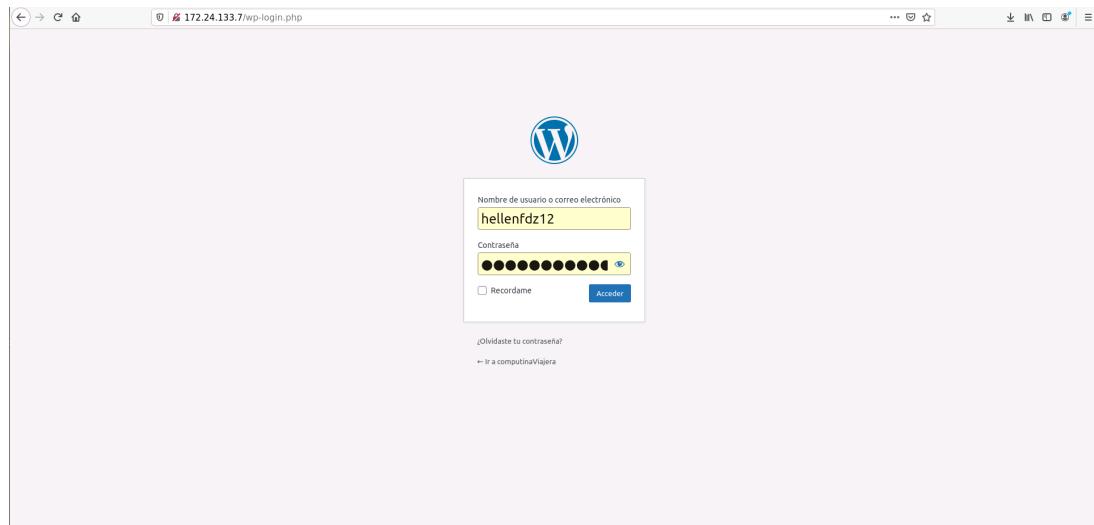
2. Se va a completar con los datos deseados para la creación de esta página y se selecciona el botón de abajo: Instalar Wordpress



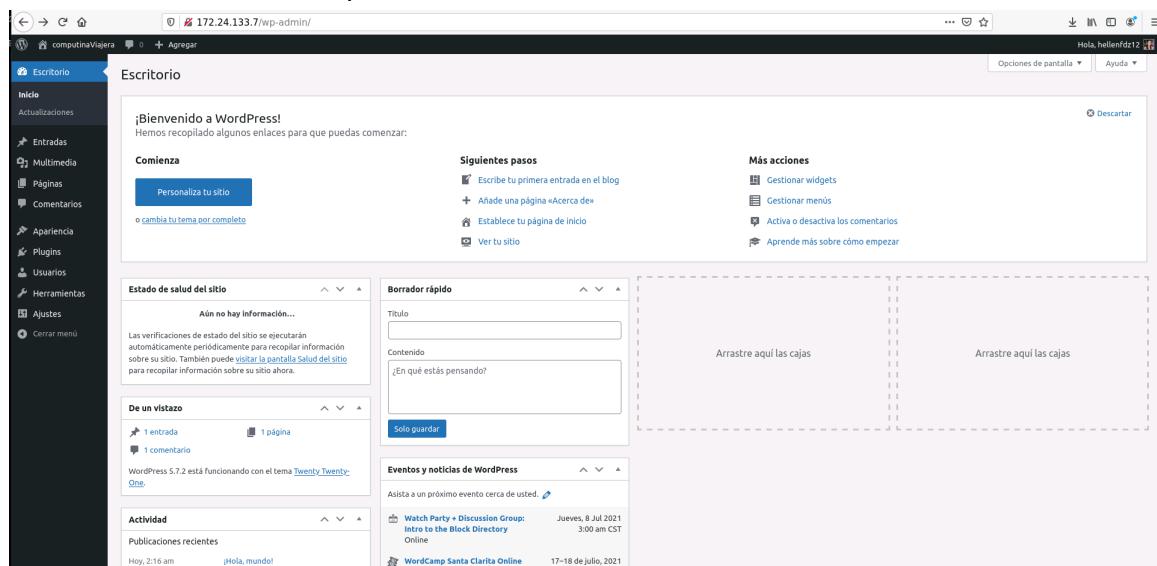
3. Una vez que esté instalado, haga click en acceder:



4. Escriba el nombre de usuario y contraseña previamente elegidas:



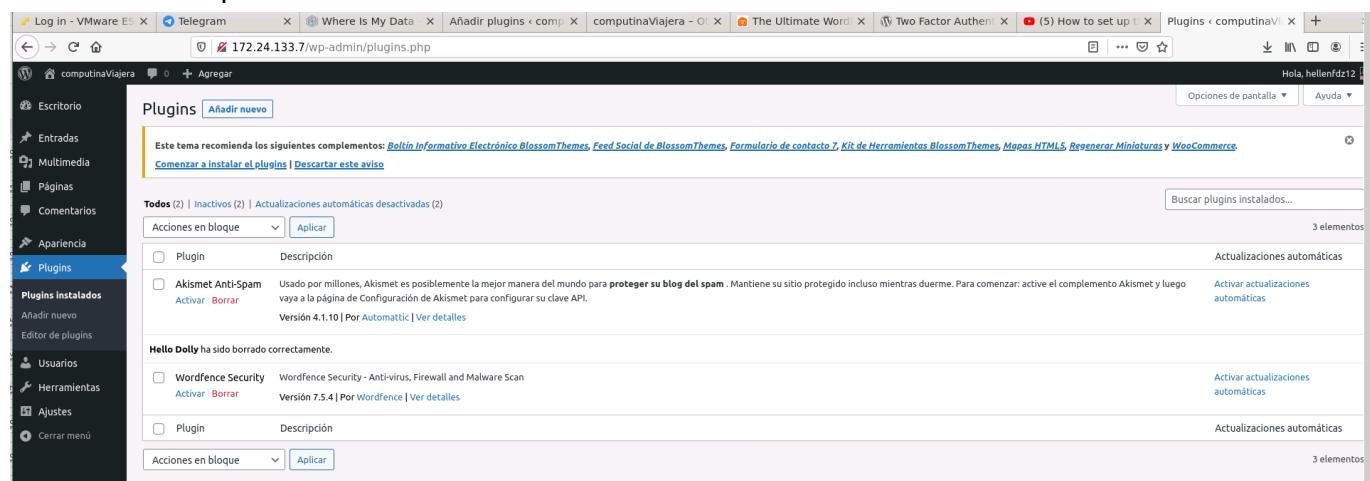
5. Al entrar, se observa esta pantalla:



Mejorar la seguridad de Wordpress

Para proteger el sitio que fue habilitado con una mayor seguridad, se va a habilitar un plugin llamado WordFence, que permite la autenticación de dos pasos, identifica tráfico malicioso, bloquea tráfico proveniente de fuentes catalogadas como parte de listas negras entre otros servicios que serán habilitados a continuación.

1. Busque e instale WordFence. Actívelo:



2. Incluir el correo electrónico en donde deberían llegar alertas:

The screenshot shows the WordPress admin interface at http://172.24.133.7/wp-admin/plugins.php?plugin_status=all&paged=1&s. The left sidebar is open, showing the 'Wordfence' section under 'Plugins'. A success message from Wordfence states: 'You have successfully installed Wordfence 7.5.4' and 'Please tell us where Wordfence should send you security alerts for your website:'. It includes fields for 'Admin Contact Info' (email: hellenfdz12@gmail.com) and 'Activate Premium'. A checkbox for accepting terms and conditions is checked, and a 'CONTINUE' button is visible.

3. En la parte de WordFence-> Firewall. Configure la cantidad de intentos fallidos de inicio de sesión máximos en 5, así como la cantidad de contraseñas fallidas en 5 así como el tiempo que pasará bloqueado el usuario si se supera esta cantidad de veces.

The screenshot shows the 'Advanced Firewall Options' page at http://172.24.133.7/wp-admin/admin.php?page=WordfenceWAF&subpage=waf_options. Under 'Brute Force Protection', the 'Enable brute force protection' switch is turned 'ON'. Configuration includes: 'Lock out after how many login failures' set to 5, 'Lock out after how many forgot password attempts' set to 5, 'Count failures over what time period' set to 4 hours, and 'Amount of time a user is locked out' set to 4 hours. Other options like 'Immediately lock out invalid usernames' and 'Immediately block the IP of users who try to sign in as these usernames' are also present.

4. Además, habilite las opciones adicionales para que queden de la siguiente forma y haga click en Save Changes:

The screenshot shows the 'Additional Options' section of the WordFence Firewall settings. Several checkboxes are checked: 'Prevent the use of passwords leaked in data breaches' (set to 'For admins only'), 'Enforce strong passwords' (with a note: 'Force admins and publishers to use strong passwords (recommended)'), 'Don't let WordPress reveal valid users in login errors', 'Prevent users registering 'admin' username if it doesn't exist', 'Prevent discovery of usernames through '?author=N' scans, the oEmbed API, the WordPress REST API, and WordPress XML Sitemaps', 'Disable WordPress application passwords', and 'Check password strength on profile update'. The 'Participate in the Real-Time Wordfence Security Network' option is also checked.

6. Gestión y restricción de accesos

iptables

iptables gestiona, mantiene e inspecciona las reglas de filtrado de paquetes IPv4 a través de tablas. Estas tablas clasifican y organizan las reglas de acuerdo al tipo de decisiones que se deben tomar sobre los paquetes.

<https://www.linuxito.com/seuridad/793-tutorial-basico-de-iptables-en-linux>

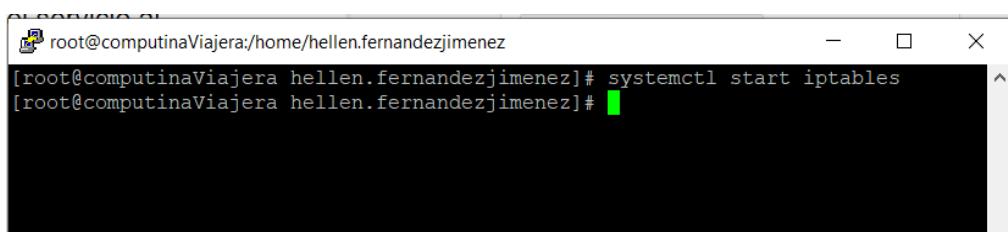
Hasta este momento, no han sido activados iptables, debido a que la estrategia usada en este caso era primero asegurarse de que funcionara el servicio ofrecido y sus debidas conexiones y posteriormente restringir accesos, de manera que se tenga certeza que si no funciona correctamente el servicio al momento de implementar iptables, esto se trate de configuración de estas reglas.

1. Active iptables

Realice los siguientes pasos tanto en el servidor como en la base de datos.

1. Active iptables mediante el comando:

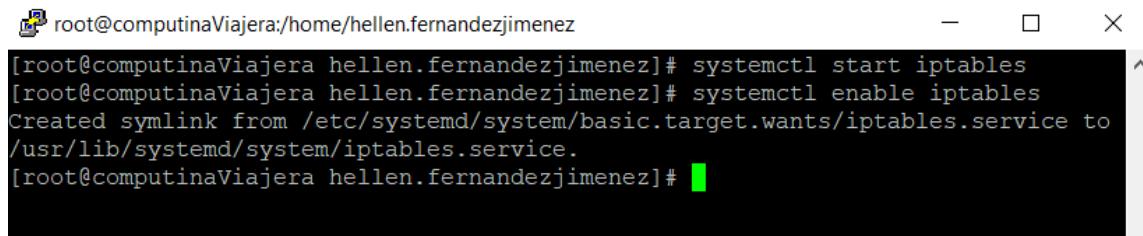
```
# systemctl start iptables
```



A terminal window titled 'root@computinaViajera: /home/hellen.fernandezjimenez'. The command '# systemctl start iptables' is entered and executed, followed by a prompt '[root@computinaViajera hellen.fernandezjimenez]#'. The terminal has a dark background with white text and standard Linux-style icons.

2. Habilite que el servicio se inicie automáticamente cuando el sistema bootea:

```
# systemctl enable iptables
```



A terminal window titled 'root@computinaViajera: /home/hellen.fernandezjimenez'. The commands '# systemctl start iptables' and '# systemctl enable iptables' are entered and executed. The output shows that a symlink was created from '/etc/systemd/system/basic.target.wants/iptables.service' to '/usr/lib/systemd/system/iptables.service'. The terminal has a dark background with white text and standard Linux-style icons.

3. Revise el estado de iptables:

```
# systemctl status iptables
```

```

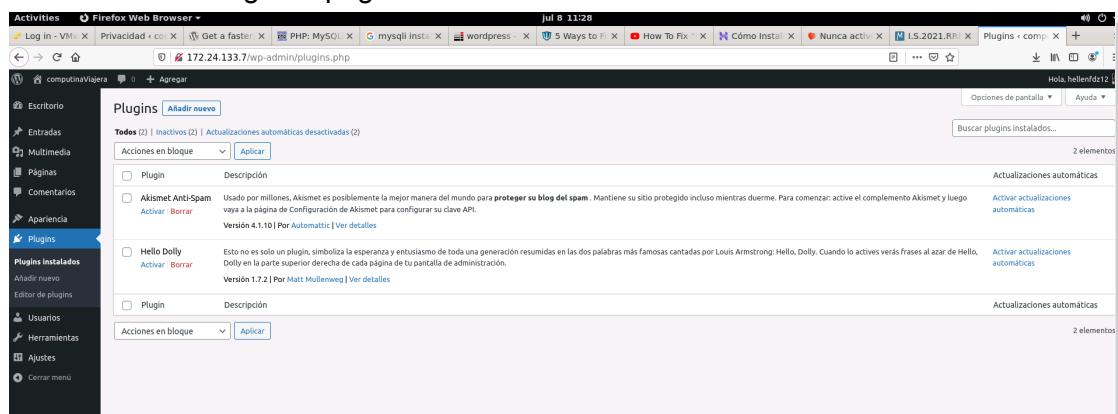
root@computinaViajera:/home/hellen.fernandezjmenez#
[root@computinaViajera hellen.fernandezjmenez]# systemctl status iptables
● iptables.service - IPv4 firewall with iptables
   Loaded: loaded (/usr/lib/systemd/system/iptables.service; enabled; vendor pre-
   set: disabled)
   Active: active (exited) since Thu 2021-07-08 13:21:36 EDT; 1min 20s ago
     Main PID: 2617 (code=exited, status=0/SUCCESS)

Jul 08 13:21:36 computinaViajera.com systemd[1]: Starting IPv4 firewall with...
Jul 08 13:21:36 computinaViajera.com iptables.init[2617]: iptables: Applying ...
Jul 08 13:21:36 computinaViajera.com systemd[1]: Started IPv4 firewall with ...
Hint: Some lines were ellipsized, use -l to show in full.
[root@computinaViajera hellen.fernandezjmenez]#

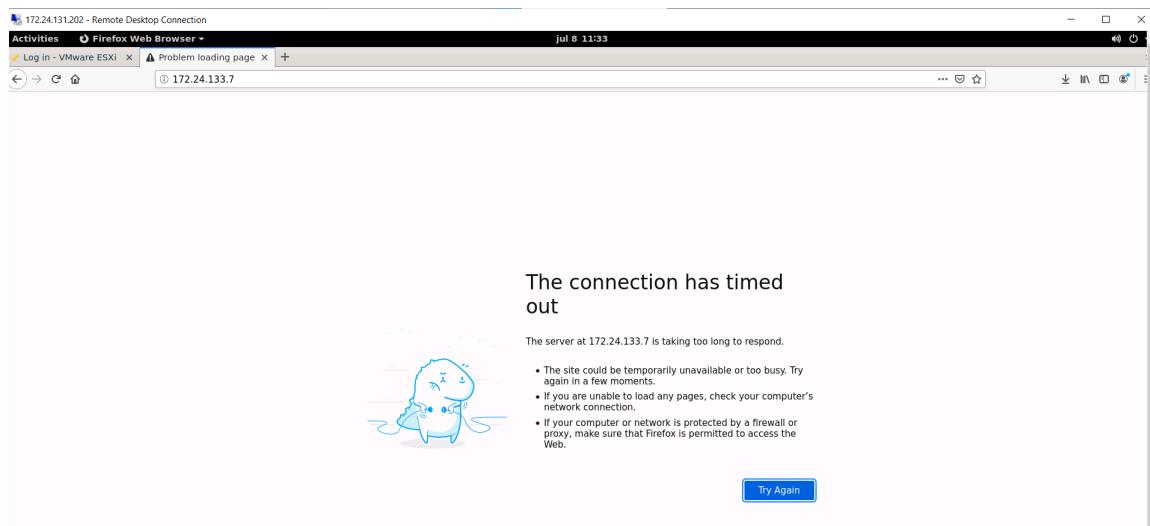
```

Como es de esperar, iptables por defecto rechaza todo tipo de conexión, permitiendo únicamente SSH inicialmente. Por este motivo es esperable que el servicio de wordpress no funcione correctamente.

4. Verifique el estado de funcionamiento de wordpress desde la máquina ubuntu que reservó: Estado antes de recargar la página:



Estado después de recargar la página:



2. Configure iptables en Base de datos

En la base de datos tenemos dos direcciones en 2 diferentes redes: una privada y una pública. La dirección de red privada es únicamente para la comunicación con el servidor apache. La dirección pública es para realizar gestión a esta base de datos. Para configurar lo planteado anteriormente en iptables realice los siguientes pasos:

1. Acceda al servidor de base de datos. En este caso lo estoy haciendo desde ssh ya que me permite mayor flexibilidad en cuanto a copiar y pegar comandos. Pero también se puede realizar desde el esxi.
2. Diríjase a la carpeta sysconf y liste los archivos y carpetas presentes mediante los comandos:

```
# cd /etc/sysconfig  
# ls
```

3. Permita que exista comunicación de forma privada entre el servidor (192.168.5.3) y la base de datos que alimenta el Wordpress que está ubicado en el apache. El número de puerto del servicio de mariadb es 3306. Además, todos los paquetes que entran por defecto serán eliminados, lo mismo con la función de forward

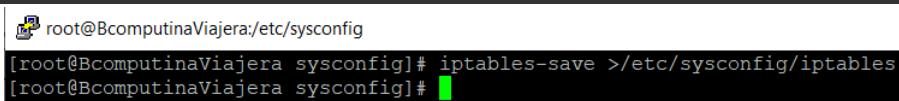
```
# iptables -P INPUT DROP  
# iptables -P FORWARD DROP  
# iptables -A INPUT -s 192.168.5.3 -p tcp --dport 3306 -j ACCEPT
```

4. Habilite SSH para la dirección ip que está destinada a gestión (172.24.133.5):

```
# iptables -A INPUT -s 172.24.131.0/24 -d 172.24.133.5/32 -p tcp -m state  
--state NEW -m tcp --dport 22 -j ACCEPT  
# iptables -A INPUT -s 172.17.0.0/16 -d 172.24.133.5/32 -p tcp -m state --state  
NEW -m tcp --dport 22 -j ACCEPT
```

5. Salve la configuración:

```
# iptables-save >/etc/sysconfig/iptables
```



```
[root@BcomputinaViajera:/etc/sysconfig]# iptables-save >/etc/sysconfig/iptables  
[root@BcomputinaViajera sysconfig]#
```

6. Observe si se aplicaron los cambios con el comando:

```
# iptables-save
```

```

root@BcomputinaViajera:/etc/sysconfig
[root@BcomputinaViajera sysconfig]# iptables-save
# Generated by iptables-save v1.4.21 on Sat Jul 17 04:47:42 2021
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [82:89896]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -s 192.168.5.3/32 -p tcp --dport 3306 -j ACCEPT
-A INPUT -s 172.24.131.0/24 -d 172.24.133.5/32 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -s 172.17.0.0/16 -d 172.24.133.5/32 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
# Completed on Sat Jul 17 04:47:42 2021
[root@BcomputinaViajera sysconfig]#

```

7. Verifique se se pueda realizar el servicio de SSH desde su computadora personal conectada a VPN:

```

hellen.fernandezjimenez@BcomputinaViajera:~
└─ login as: hellen.fernandezjimenez
└─ hellen.fernandezjimenez@172.24.133.5's password:
Last login: Sat Jul 17 04:33:53 2021 from 172.17.4.2
[hellen.fernandezjimenez@BcomputinaViajera ~]$

```

3. Configure iptables en servidor apache

1. Acceda a la máquina que aloja el servidor de apache. En este caso lo estoy haciendo desde ssh ya que me permite mayor flexibilidad en cuanto a copiar y pegar comandos. Pero también se puede realizar desde el esxi.
2. Diríjase a la carpeta sysconf y liste los archivos y carpetas presentes mediante los comandos:

```
# cd /etc/sysconfig
# ls
```

```

root@computinaViajera:/etc/sysconfig
[root@computinaViajera hellen.fernandezjimenez]# cd /etc/sysconfig
[root@computinaViajera sysconfig]# ls
anaconda      cpupower      grub          ip6tables      iptables-config   kernel      network-scripts   rsyslog      sshd
authconfig    crond        htcacheclen  ip6tables-config  iptables.rpmsave  man-db     rdisc          run-parts   wpa_supplicant
chronyd       ebtables-config httpd        iptables      irqbalance      network    rsyncd      selinux
[root@computinaViajera sysconfig]#

```

3. Permita que exista comunicación de forma privada entre el servidor de base de datos (192.168.5.2) hasta el propio servidor. El número de puerto del servicio de mariadb es 3306. Habilite la entrada de estos paquetes desde esa máquina.

```
# iptables -A INPUT -s 192.168.5.2/24 -p tcp --dport 3306 -j ACCEPT
```

4. Como es un servidor web. Permita que los puertos 80 correspondiente a http y 443 correspondiente a https estén ofreciendo sus servicios, además, por defecto establezca que los paquetes que entran serán descartados.

```
# iptables -P INPUT DROP
# iptables -P FORWARD DROP
# iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

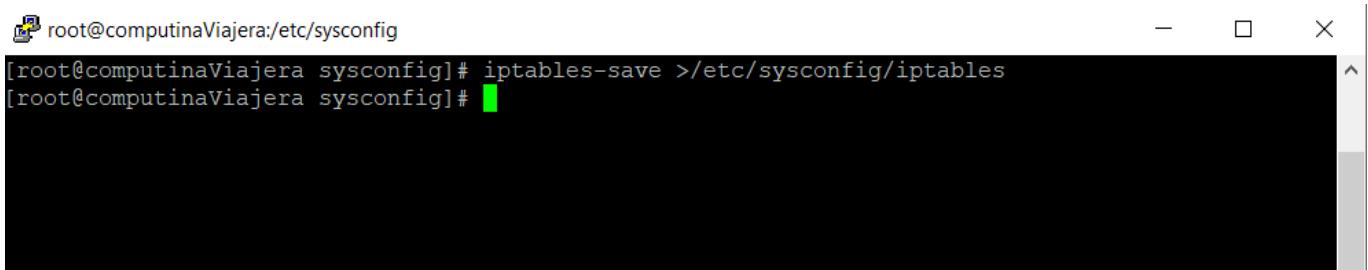
```
# iptables -A INPUT -p tcp --dport 443 -j ACCEPT  
# iptables -A INPUT -p tcp --dport 3306 -j ACCEPT
```

5. Permita que se realice ssh desde la máquina Ubuntu reservada desde VCL y desde su máquina personal que está conectada por OpenVPN. Como hay dos direcciones ip con conexión a la red universitaria y a internet, permita sólo aquellas conexiones SSH que tengan como destino la dirección ip 172.24.133.6 y como fuente la máquina VCL y si lo desea alguna otra máquina más para que tenga seguridad de poder tener acceso si es necesario. Mediante unas pruebas, determiné que se me estaban asignando direcciones IP de forma dinámica probablemente mediante un servidor de DHCP, pero en todas las ocasiones coincidían en que se me asignaban direcciones de la red 172.17.0.0 , por lo cual, esa fue la fuente que se indicó, de esta forma pude acceder desde putty en mi computadora personal con VPN. Para esto establecieron las siguientes reglas:

```
# iptables -A INPUT -s 172.24.131.0/24 -d 172.24.133.6/32 -p tcp -m state  
--state NEW -m tcp --dport 22 -j ACCEPT  
# iptables -A INPUT -s 172.17.0.0/16 -d 172.24.133.6/32 -p tcp -m state --state  
NEW -m tcp --dport 22 -j ACCEPT
```

6. Salve la configuración:

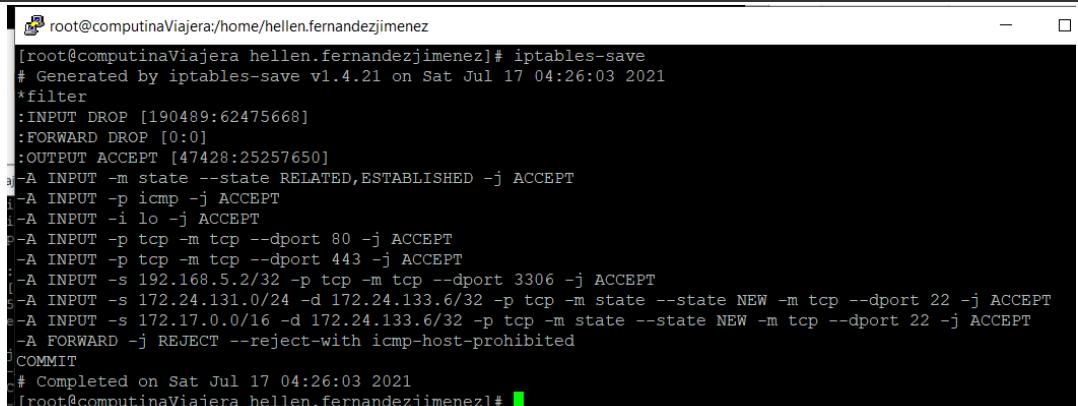
```
# iptables-save >/etc/sysconfig/iptables
```



```
[root@computinaViajera:/etc/sysconfig]# iptables-save >/etc/sysconfig/iptables  
[root@computinaViajera sysconfig]#
```

7. Observe si se aplicaron los cambios con el comando:

```
#iptables-save
```

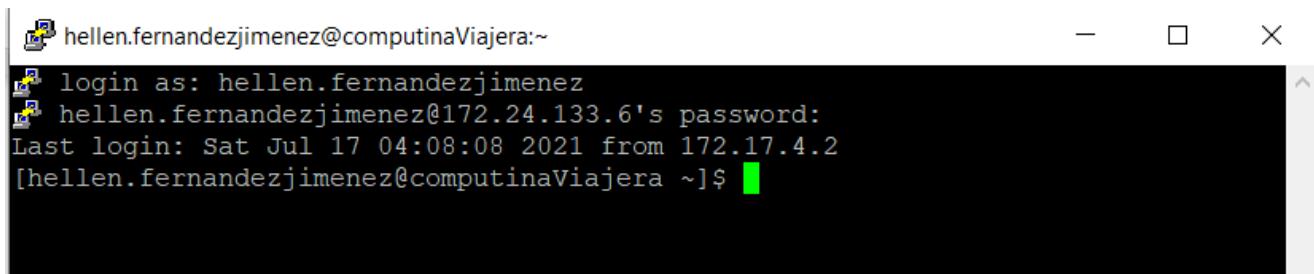


```
[root@computinaViajera:/home/hellen.fernandezjimenez]# iptables-save  
# Generated by iptables-save v1.4.21 on Sat Jul 17 04:26:03 2021  
*filter  
:INPUT DROP [190489:62475668]  
:FORWARD DROP [0:0]  
:OUTPUT ACCEPT [47428:25257650]  
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT  
-A INPUT -p icmp -j ACCEPT  
-A INPUT -i lo -j ACCEPT  
-A INPUT -p tcp -m tcp --dport 80 -j ACCEPT  
-A INPUT -p tcp -m tcp --dport 443 -j ACCEPT  
-A INPUT -s 192.168.5.2/32 -p tcp -m tcp --dport 3306 -j ACCEPT  
-A INPUT -s 172.24.131.0/24 -d 172.24.133.6/32 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT  
-A INPUT -s 172.17.0.0/16 -d 172.24.133.6/32 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT  
-A FORWARD -j REJECT --reject-with icmp-host-prohibited  
:COMMIT  
# Completed on Sat Jul 17 04:26:03 2021  
[root@computinaViajera hellen.fernandezjimenez]#
```

8. Escriba el comando iptables-restart para asegurarse de que efectivamente están funcionando aún después de que se haga rebooto en la máquina.

```
#service iptables-restart
```

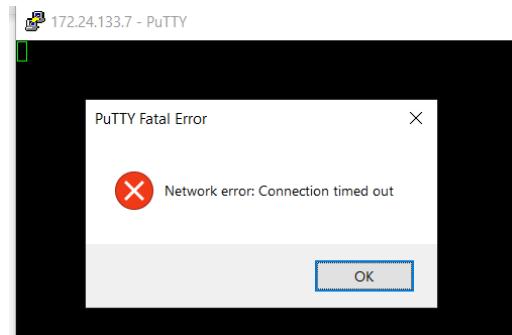
9. Intente acceder a la dirección 172.24.133.6 (la dirección ip destinada a gestión) por medio de SSH desde su computadora personal con VPN habilitada:



```
hellen.fernandezjimenez@computinaViajera:~  
login as: hellen.fernandezjimenez  
hellen.fernandezjimenez@172.24.133.6's password:  
Last login: Sat Jul 17 04:08:08 2021 from 172.17.4.2  
[hellen.fernandezjimenez@computinaViajera ~]$
```

Efectivamente está configurado el servicio para esta fuente.

10. Intente acceder a la dirección 172.24.133.7 (correspondiente) por medio de SSH desde su computadora personal con VPN habilitada:



No se puede acceder, lo cual es un comportamiento esperado para esta dirección ip.

Finalmente, verifique se que puede acceder al sitio web configurado:

