



---

## INSTITUTO TECNOLÓGICO DE MORELIA

Ingeniería en Sistemas Computacionales

Seguridad en la nube

### Manual Práctica 1

ALUMNO:

**Rogelio Cristian Punzo Castro**

PROFESOR:

**Roque Trujillo Ramos**

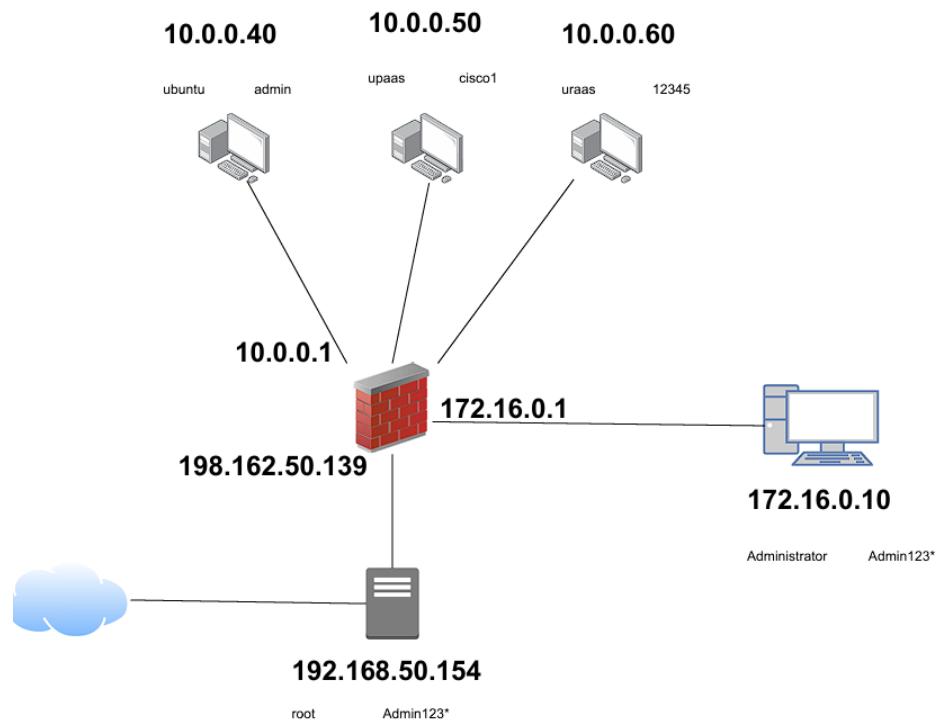
MORELIA, MICHOACÁN

**(Octubre 2024)**

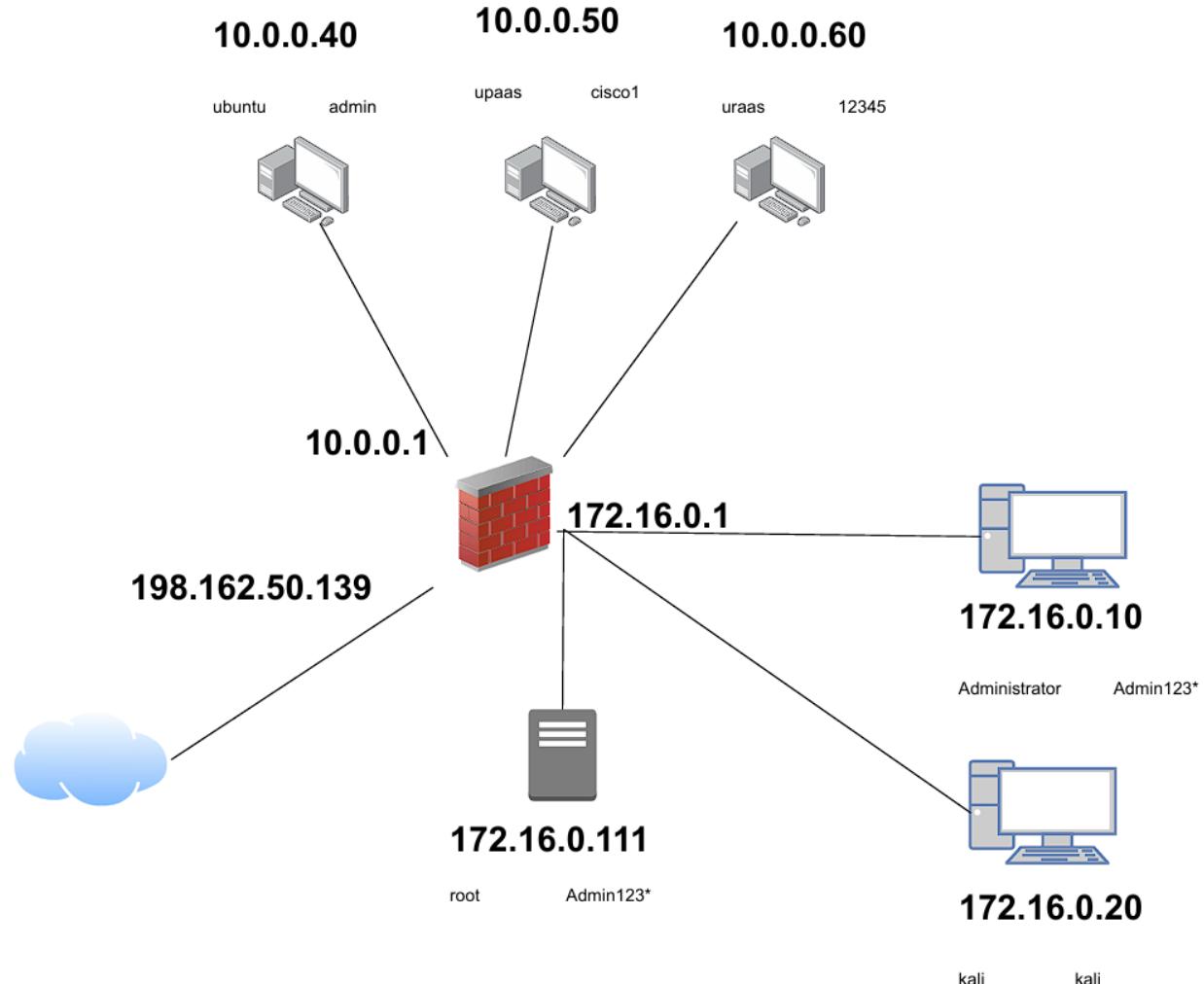
## Índice

Diseño de red .....	2
Diseño 2 .....	3
Instalación de ESXi 6.7.0 .....	4
Instalación de vSphere Client .....	19
Instalación de pfSense .....	25
Instalación de máquinas virtuales .....	41
Creación de discos para las máquinas virtuales.....	41
Máquinas virtuales en VMware ESXi .....	47
Clonación de Máquinas virtuales .....	53
Usuarios y permisos en ESXi .....	57
Usuarios en Ubuntu .....	62
Red.....	65
Firewall ESXi .....	65
Firewall pfSense .....	68
IP Ubuntu (IaaS).....	74
Firewall maquina virtuales .....	76
Port Groups (VLANs) .....	79
Virtual Switches .....	86
VMkernel NICs .....	90
Configurar VLAN en máquina virtual.....	95
Aplicación web .....	97
Servicios .....	104
SSH ESXi .....	104
SSH Ubuntu.....	107
Apache en Ubuntu (PaaS): .....	114
Base de datos .....	115
MySQL .....	115
PHP.....	118
Referencias .....	119

## Diseño de red

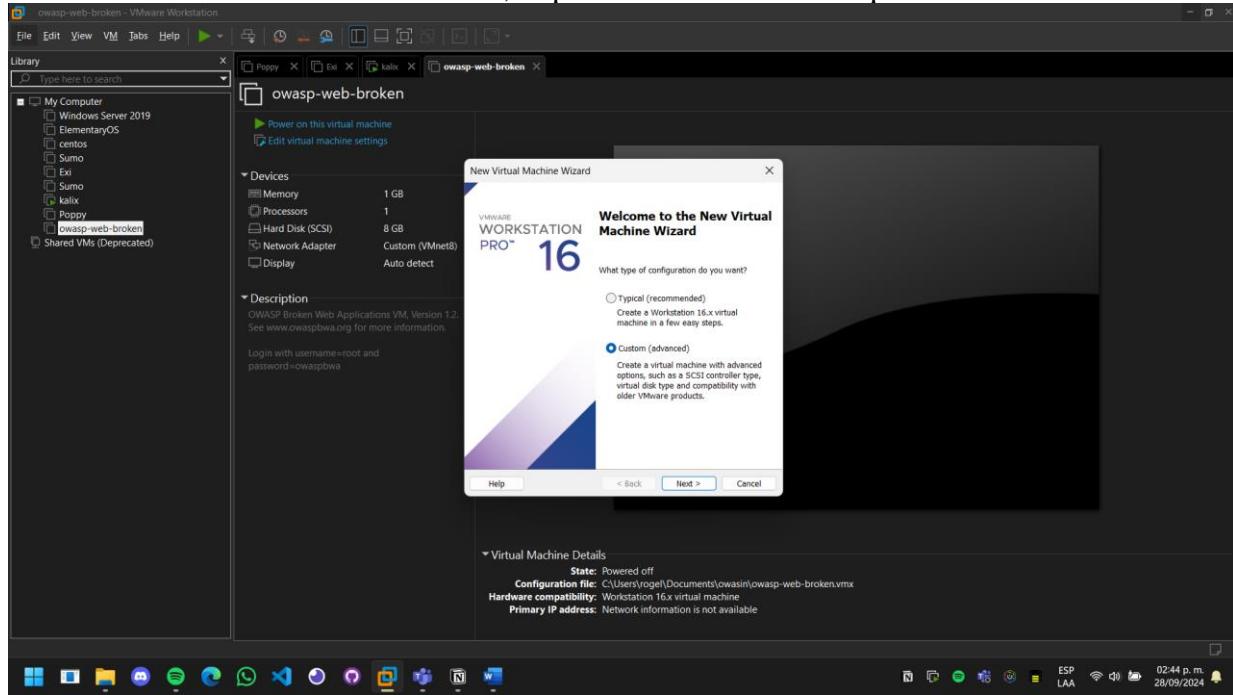


## Diseño 2

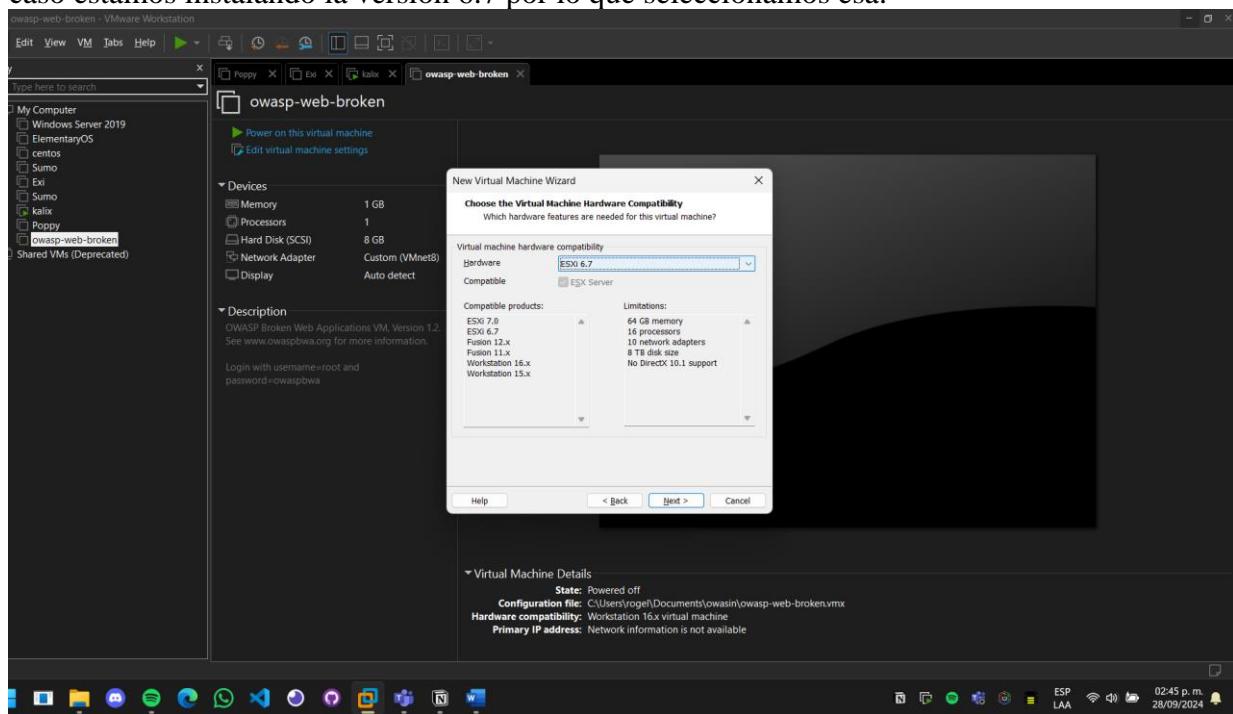


## Instalación de ESXi 6.7.0

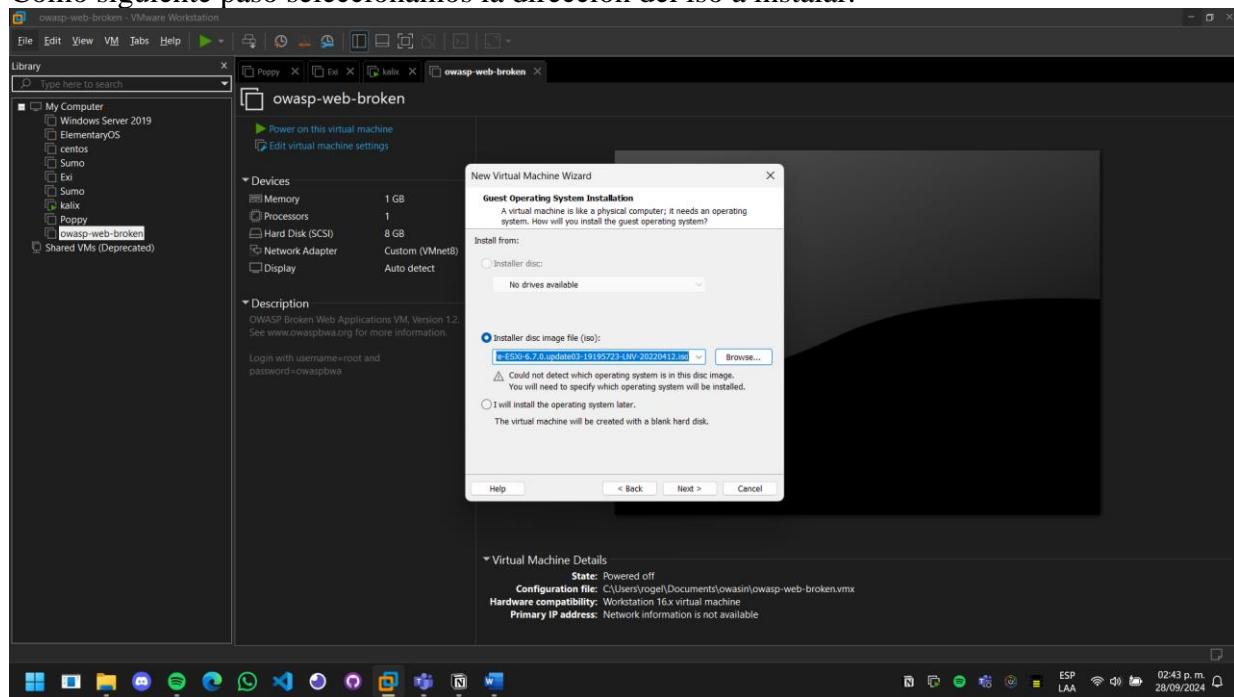
Para iniciar con la instalación de ESXi, lo primero es crear una máquina virtual



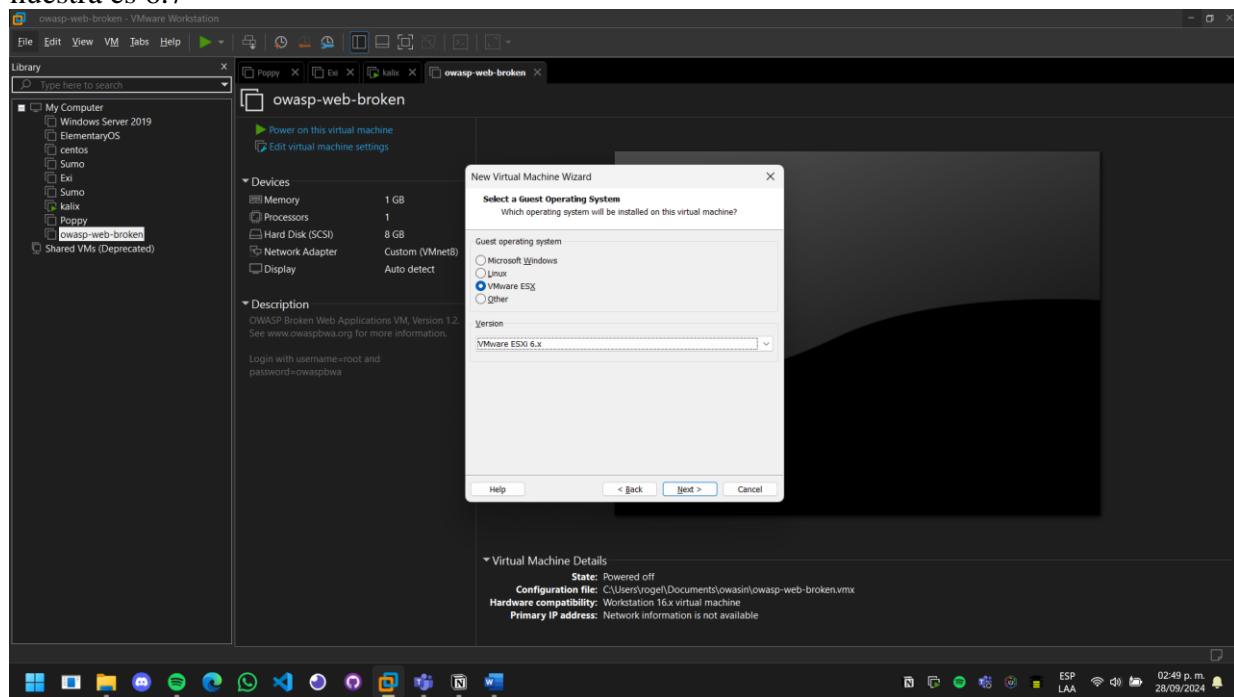
A continuación, seleccionamos a que tipo de hardware queremos que sea compatible, en este caso estamos instalando la versión 6.7 por lo que seleccionamos esa.



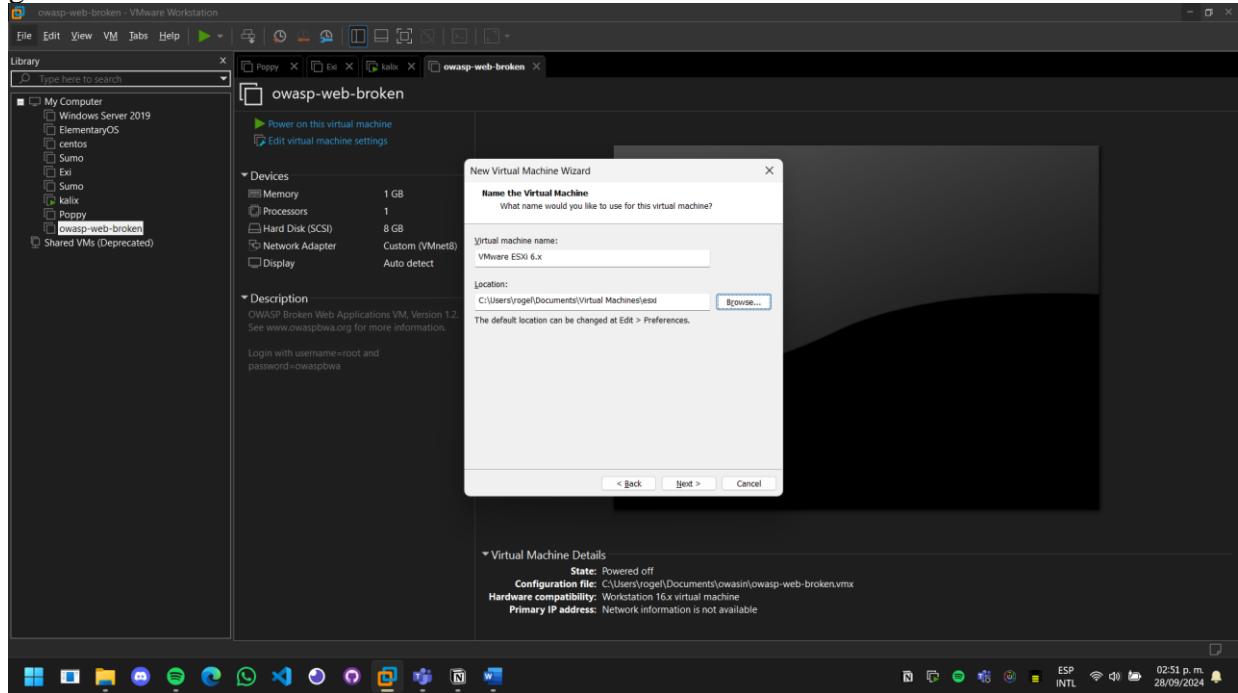
Como siguiente paso seleccionamos la dirección del iso a instalar.



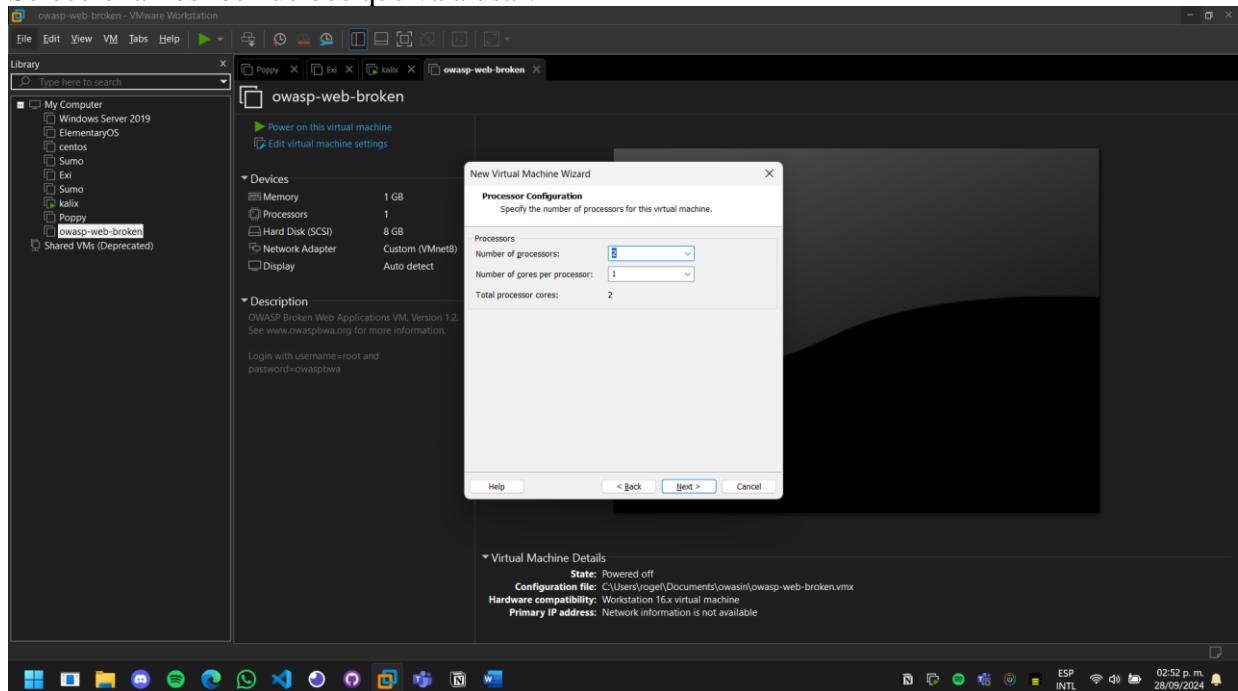
Seleccionamos el tipo de sistema operativo el cual es “VMware ESX” y la versión 6.x ya que la nuestra es 6.7



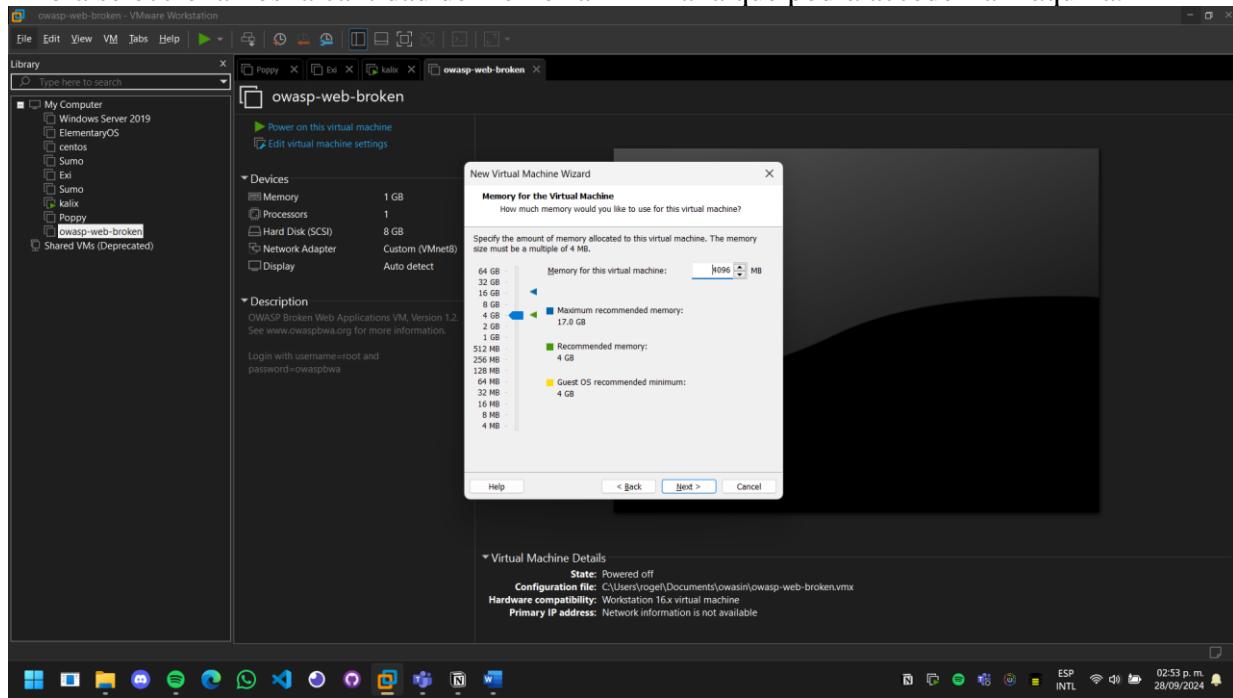
Ahora colocamos el nombre de la máquina virtual y el directorio en donde queremos que se guarde



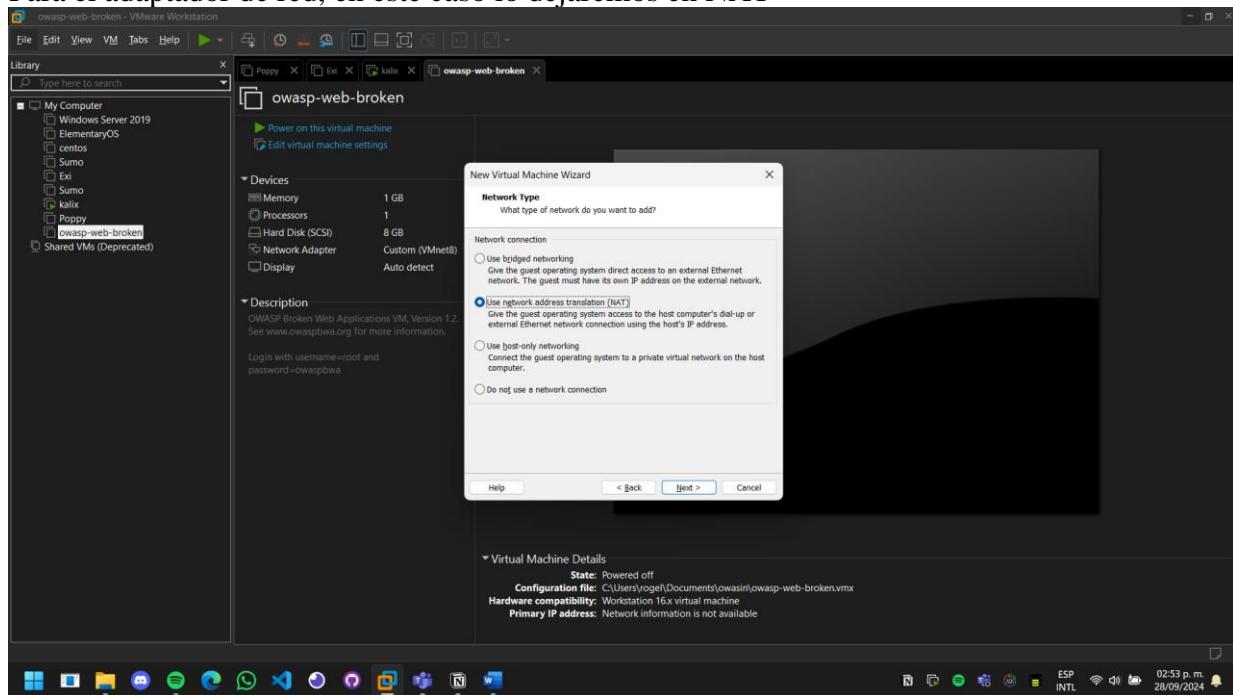
Seleccionamos los núcleos que va a usar.



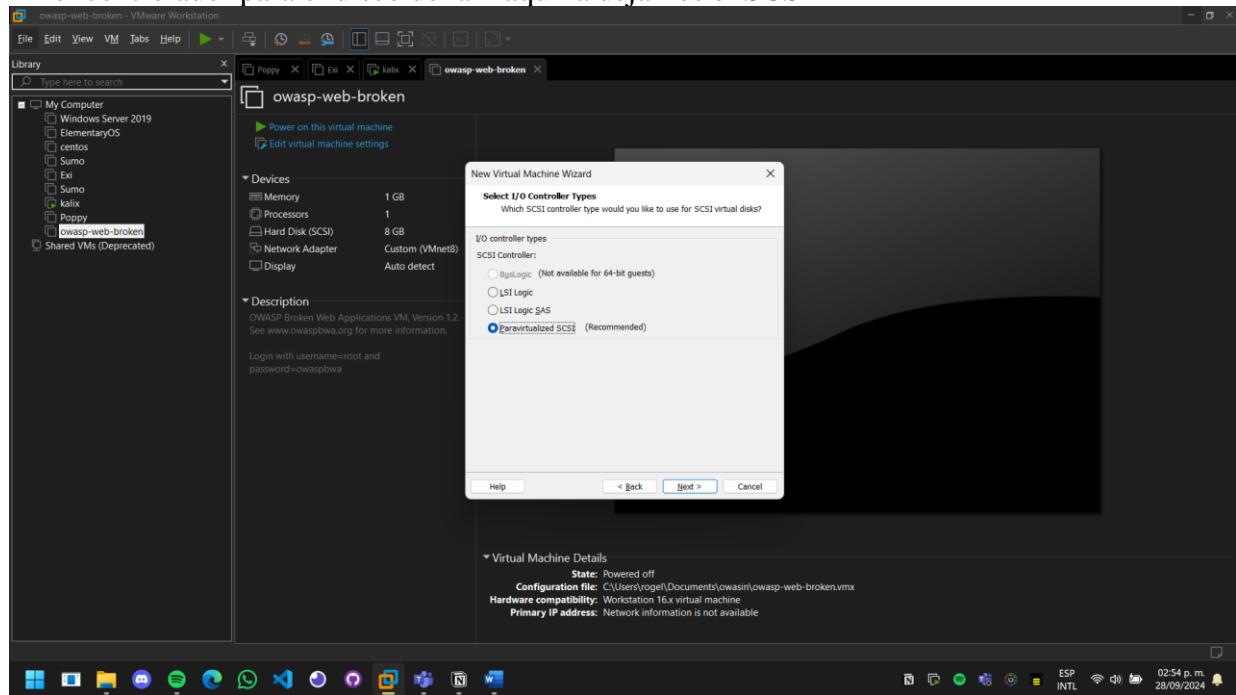
Ahora seleccionamos la cantidad de memoria RAM a la que podrá acceder la máquina.



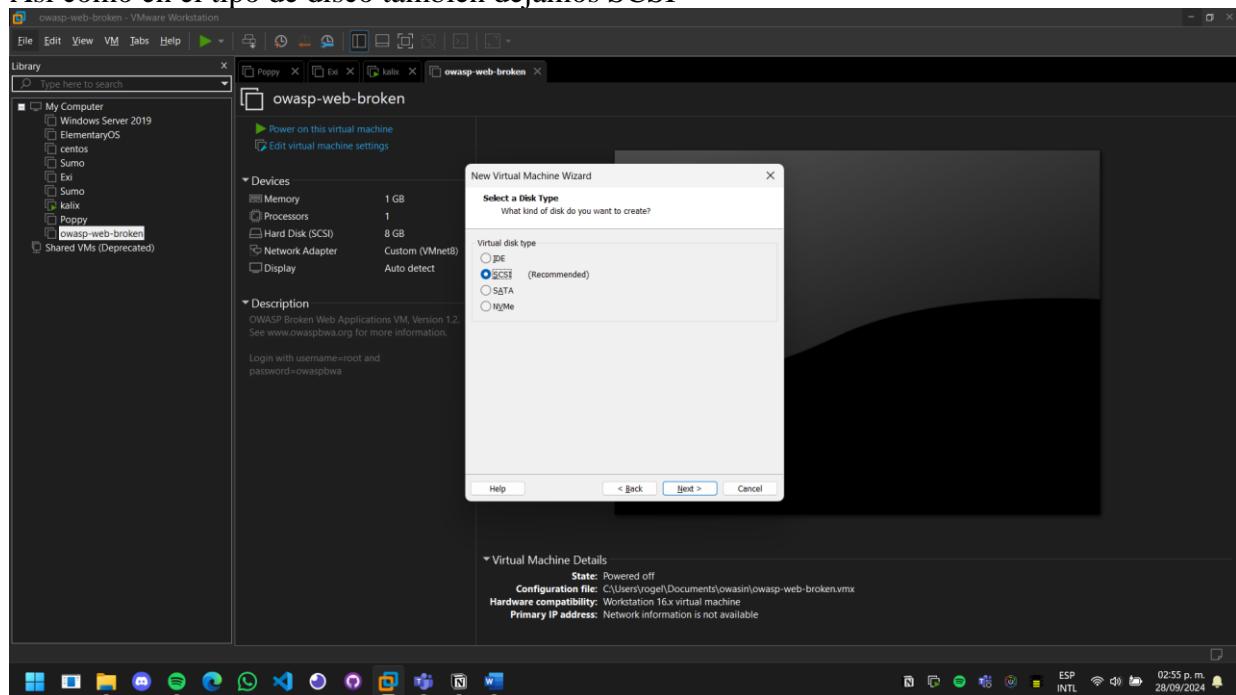
Para el adaptador de red, en este caso lo dejaremos en NAT



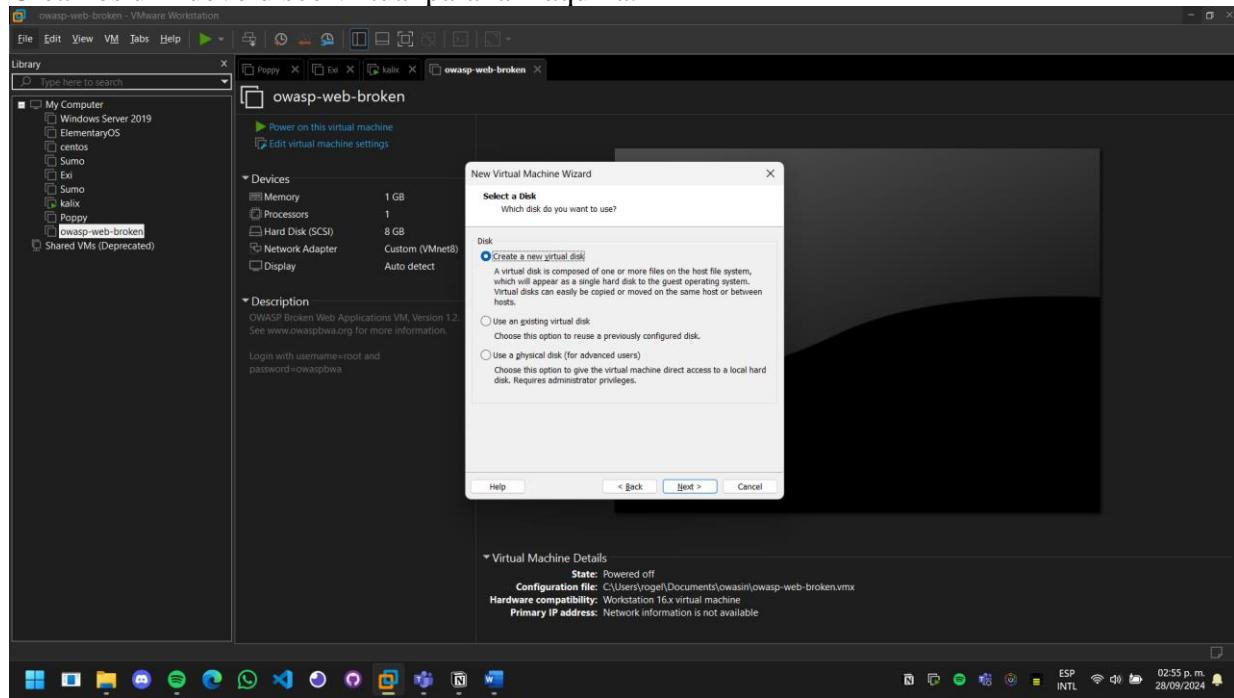
En el controlador para el disco de la maquina dejamos el SCSI



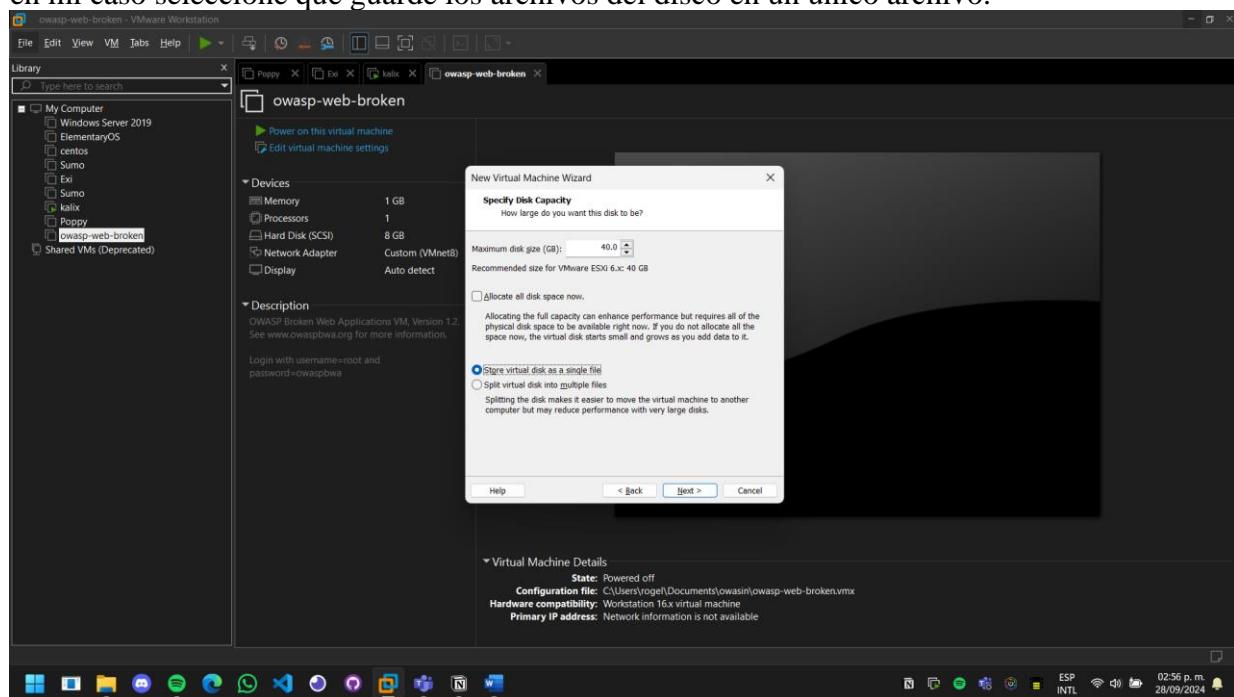
Así como en el tipo de disco también dejamos SCSI



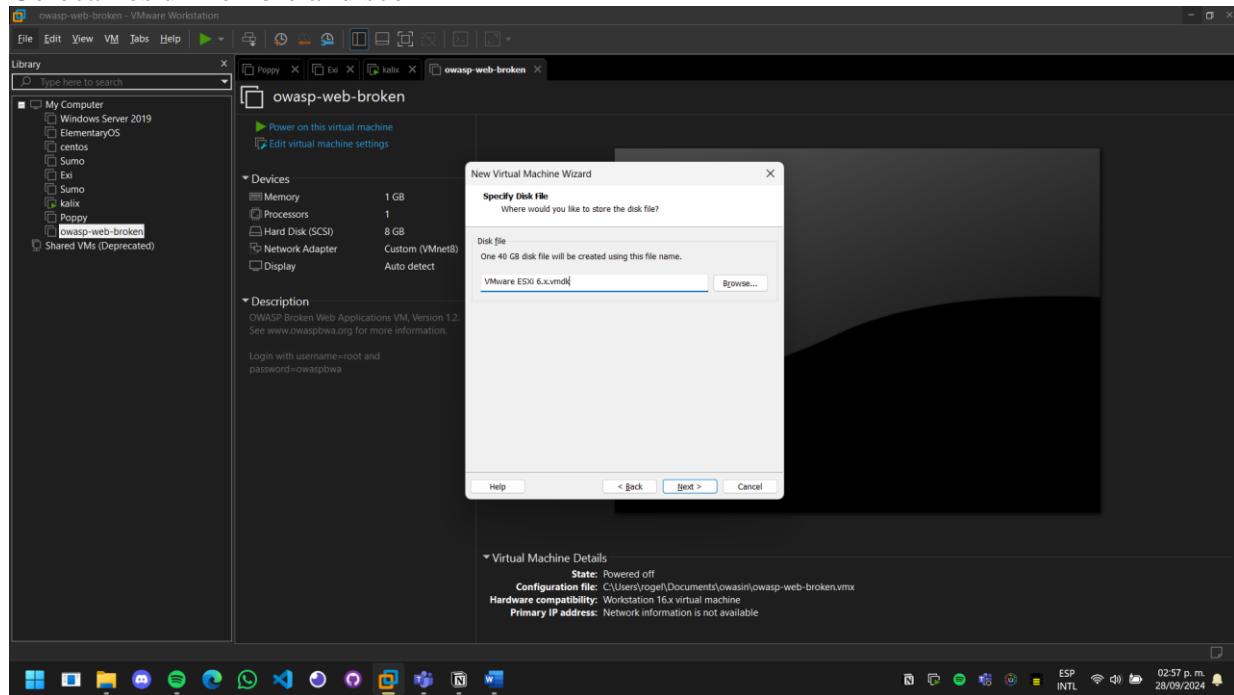
Creamos un nuevo disco virtual para la máquina.



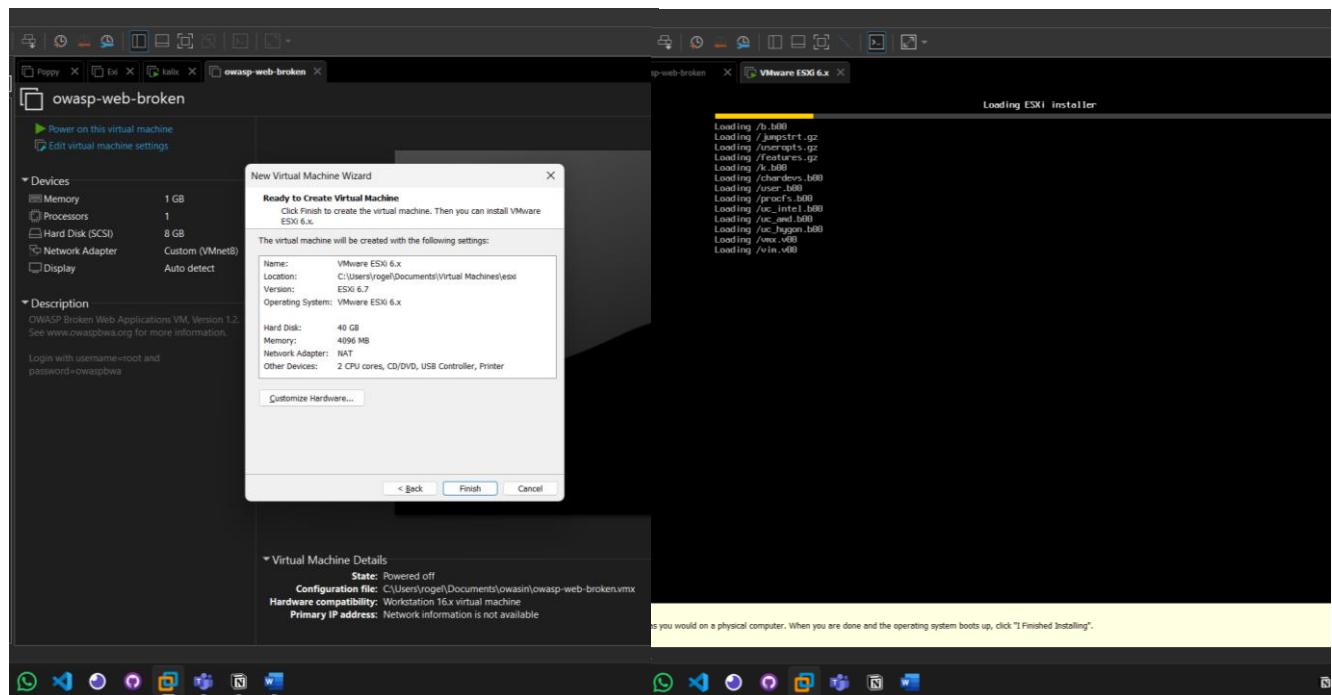
Asignamos la cantidad de espacio que puede llegar a tener el disco, aquí deje 40 gb, y también en mi caso seleccione que guarde los archivos del disco en un único archivo.



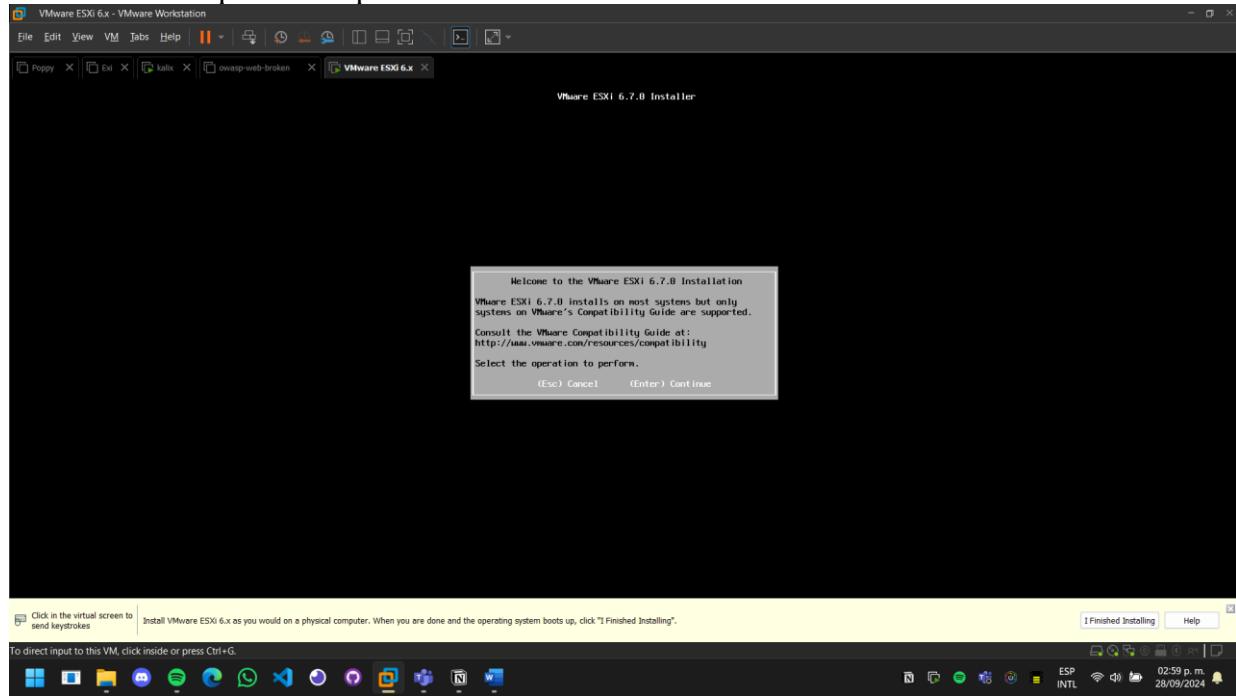
## Colocamos un nombre al disco



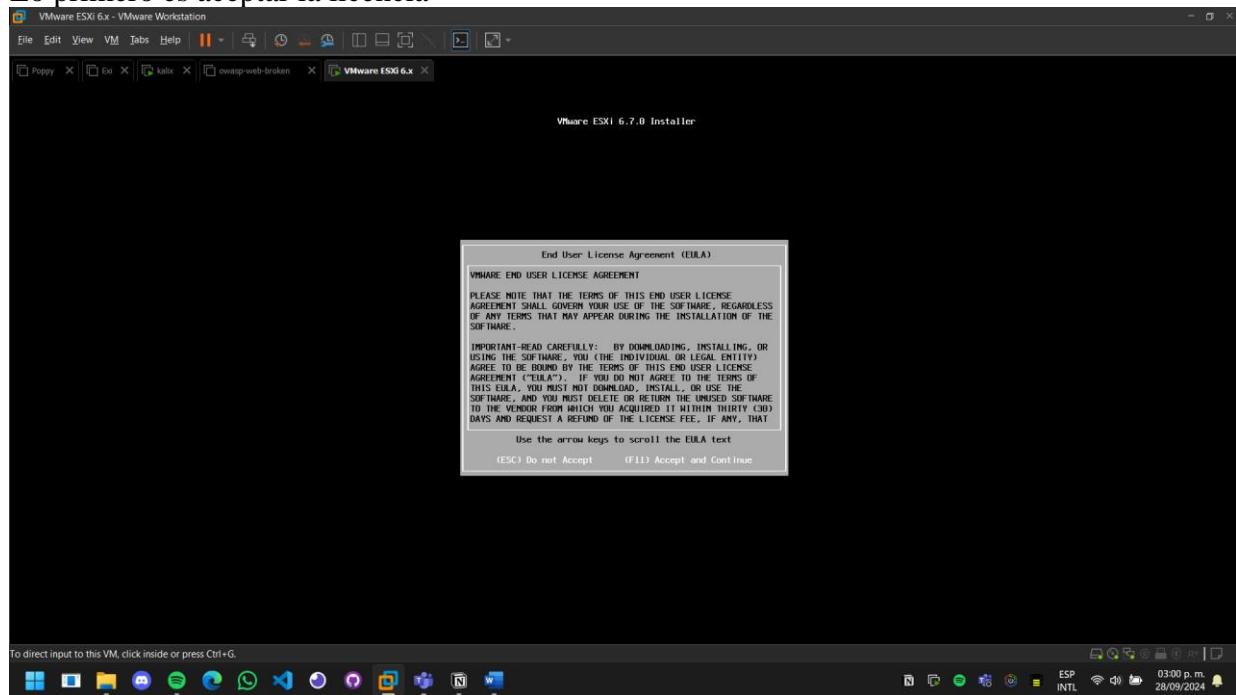
Finalizamos la configuración e iniciamos la máquina virtual.



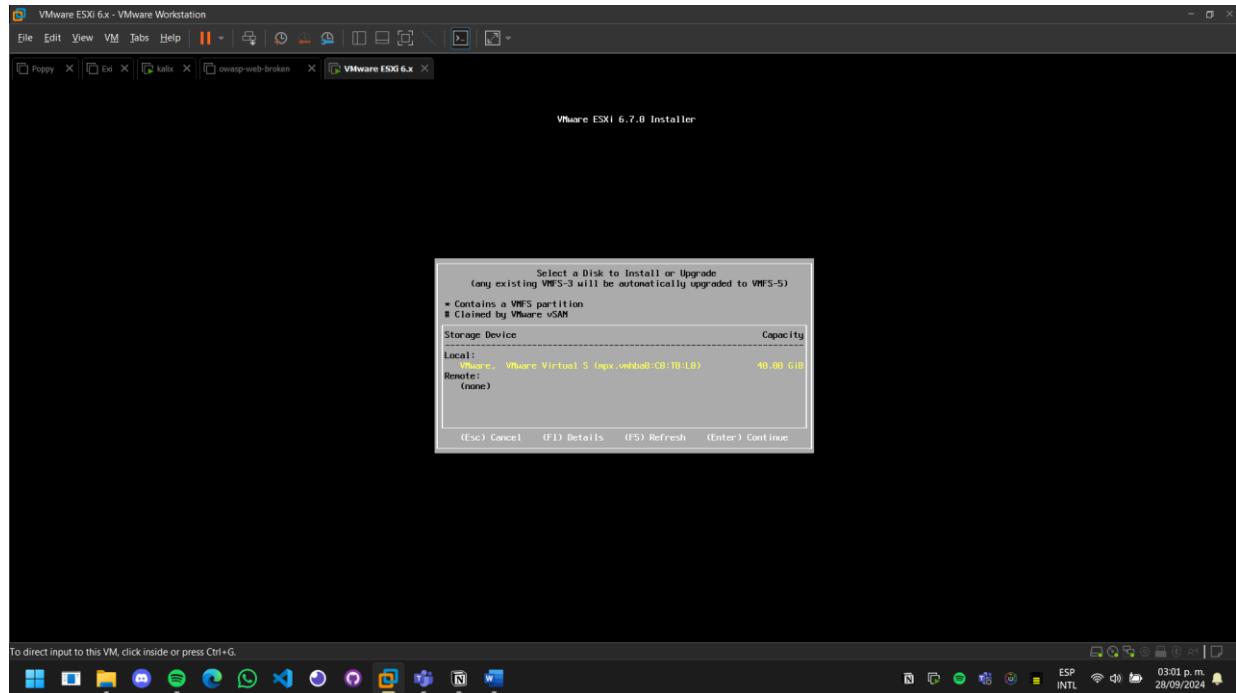
Al iniciar la maquina nos aparecerá el asistente de instalación.



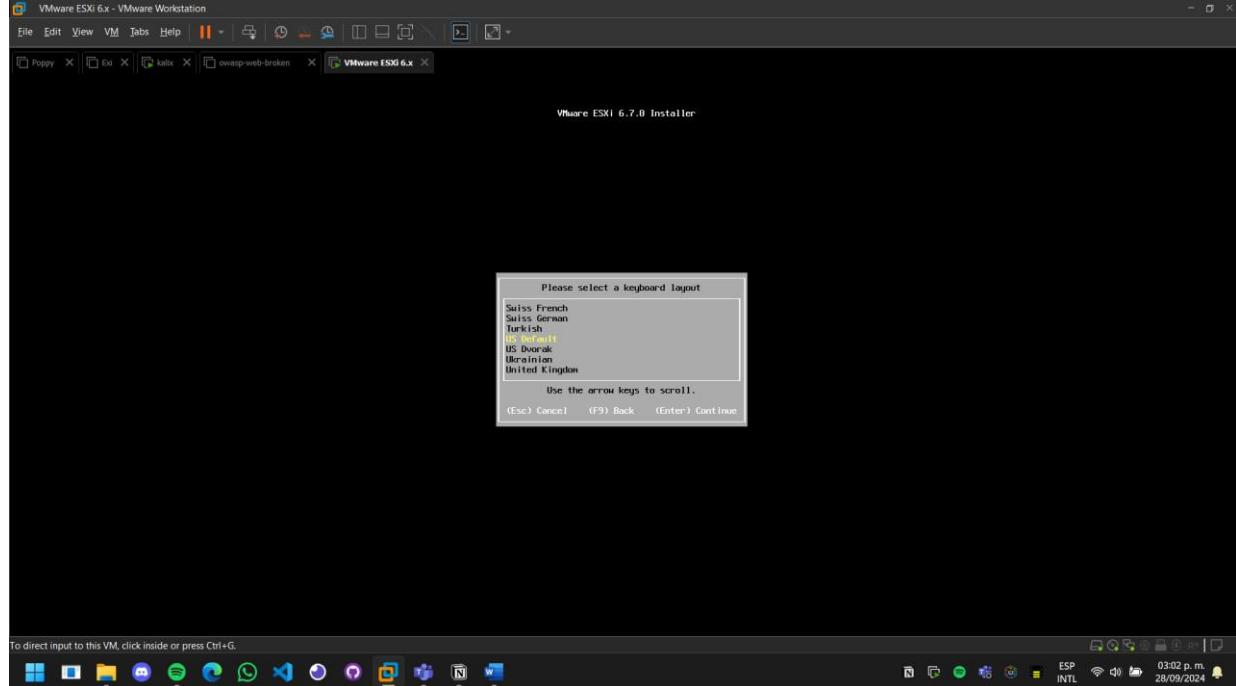
Lo primero es aceptar la licencia



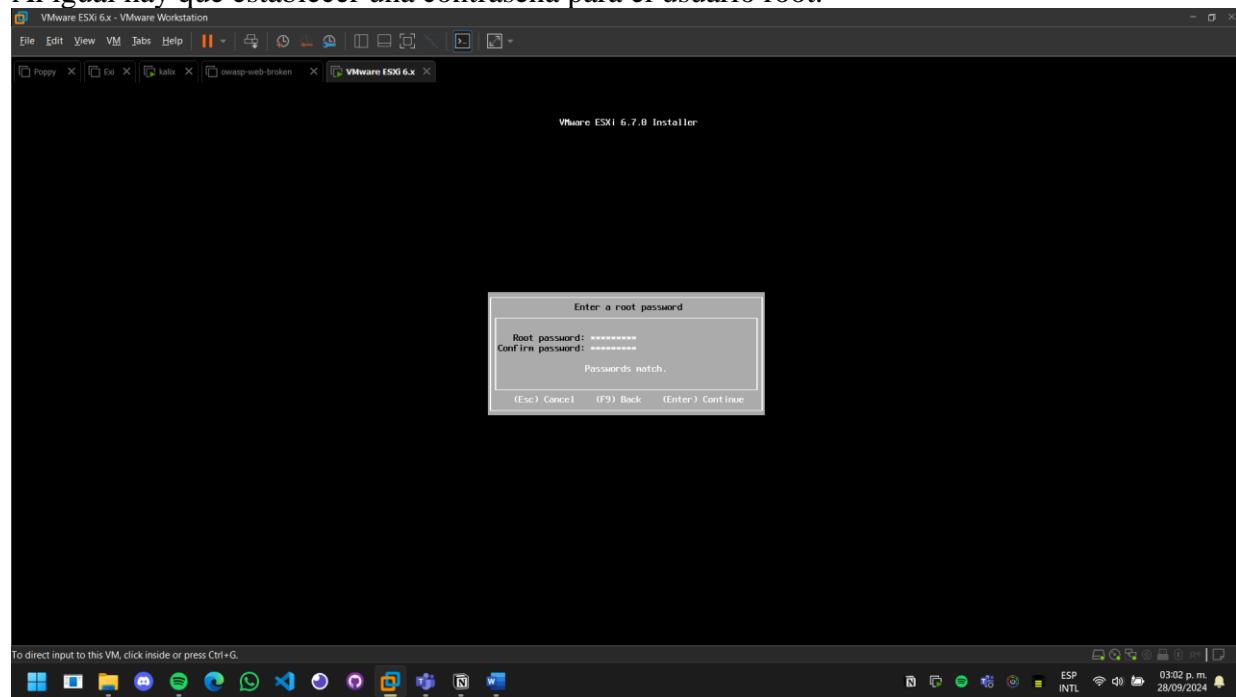
A continuación, nos pide seleccionar el disco en donde se instalará, y seleccionamos el disco creado anteriormente



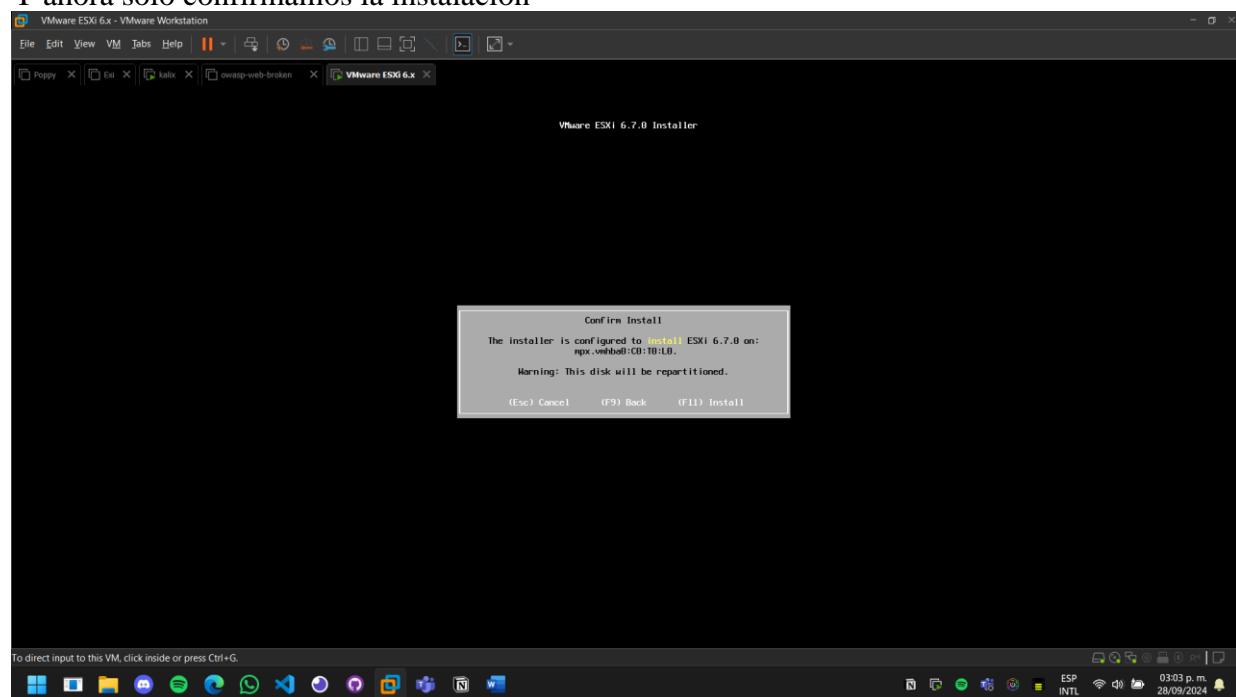
También tenemos que seleccionar el idioma de nuestro teclado.

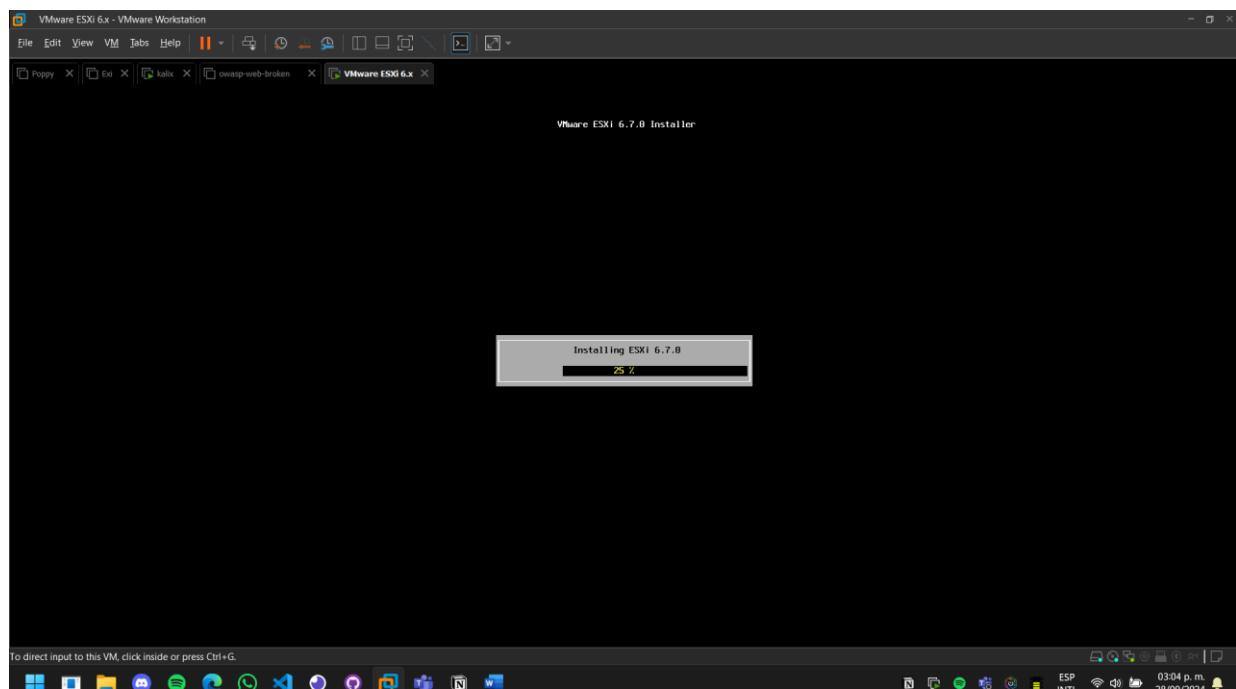


Al igual hay que establecer una contraseña para el usuario root.

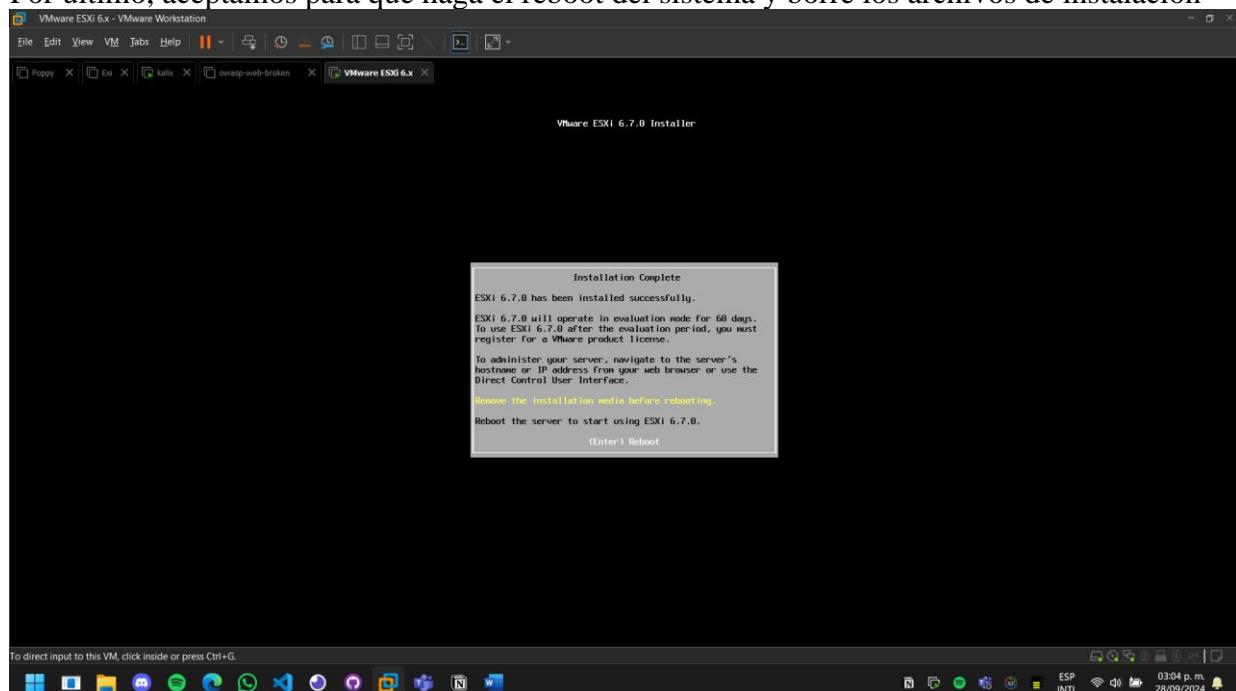


Y ahora solo confirmamos la instalación

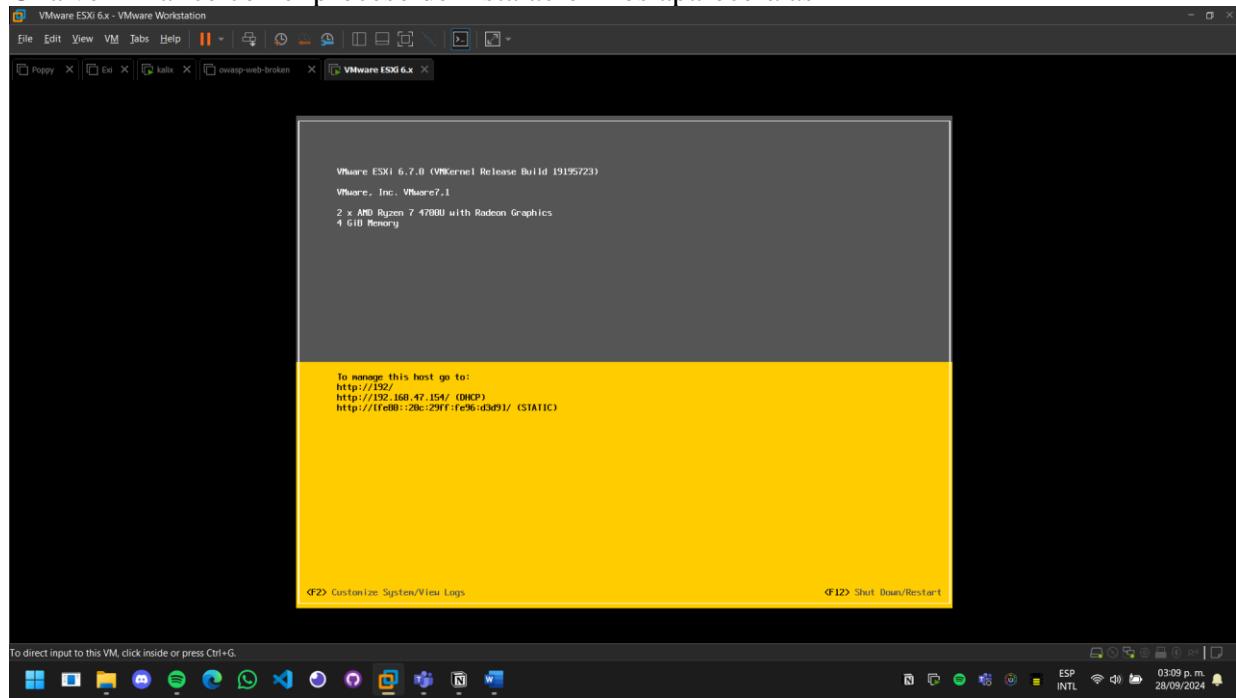




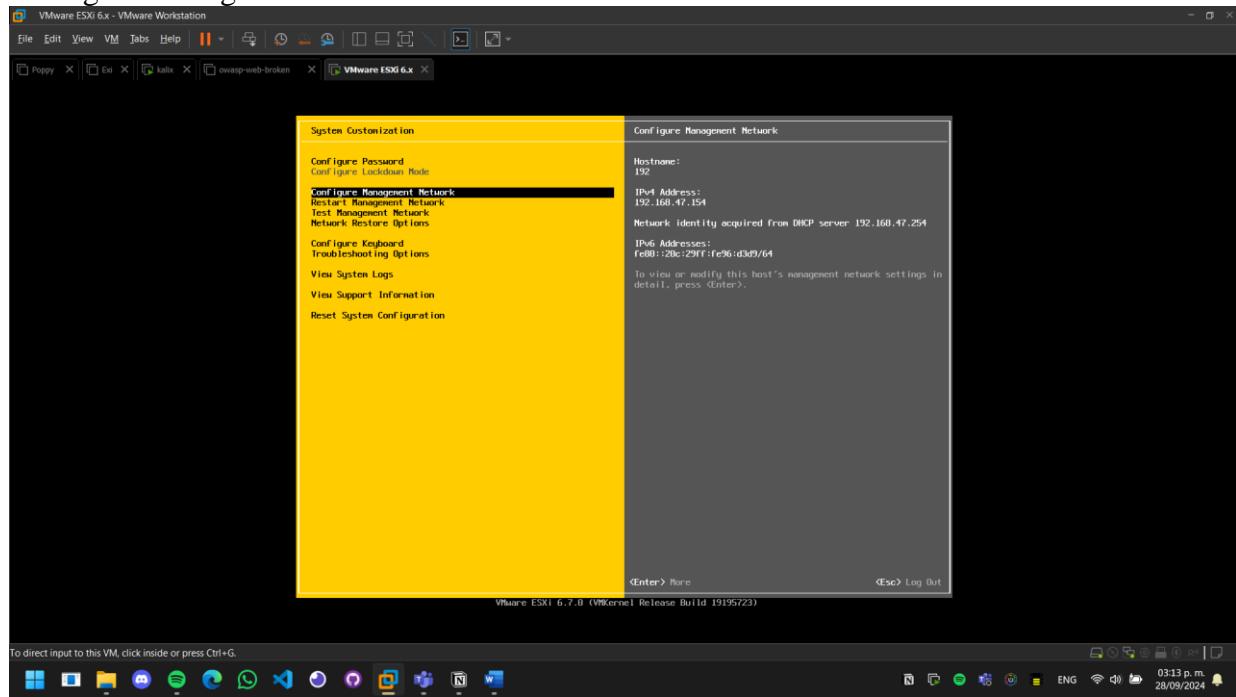
Por último, aceptamos para que haga el reboot del sistema y borre los archivos de instalación



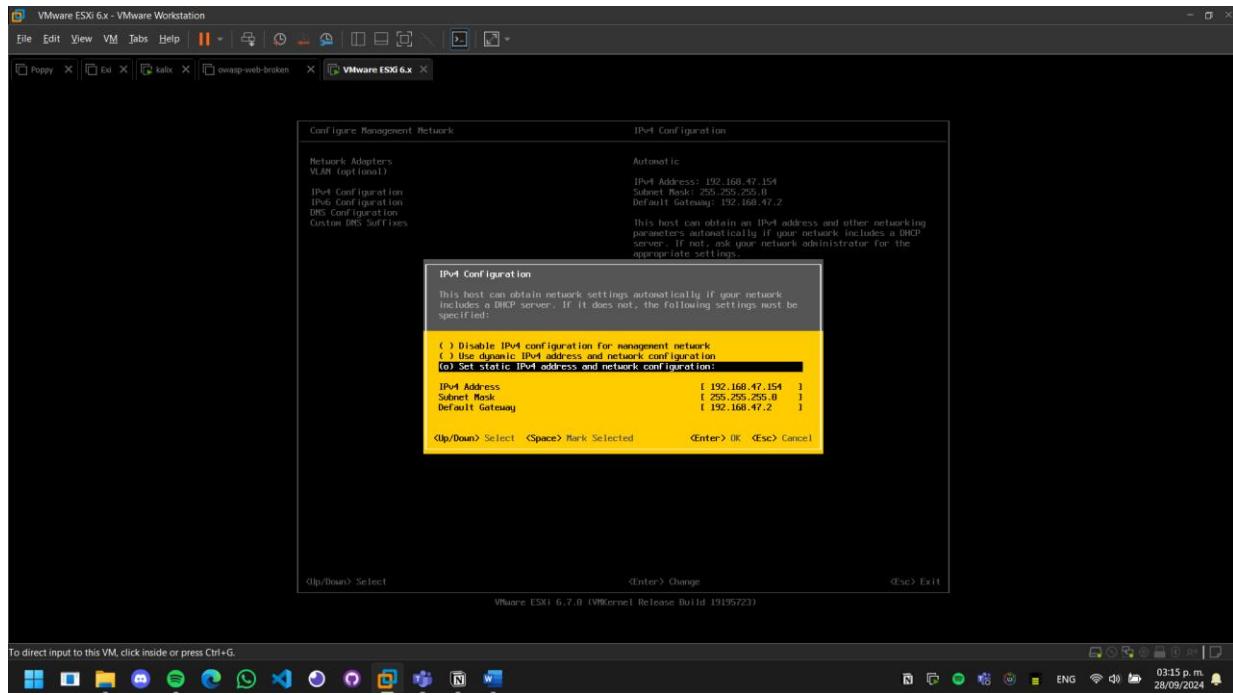
Una vez finalice con el proceso de instalación nos aparecerá así



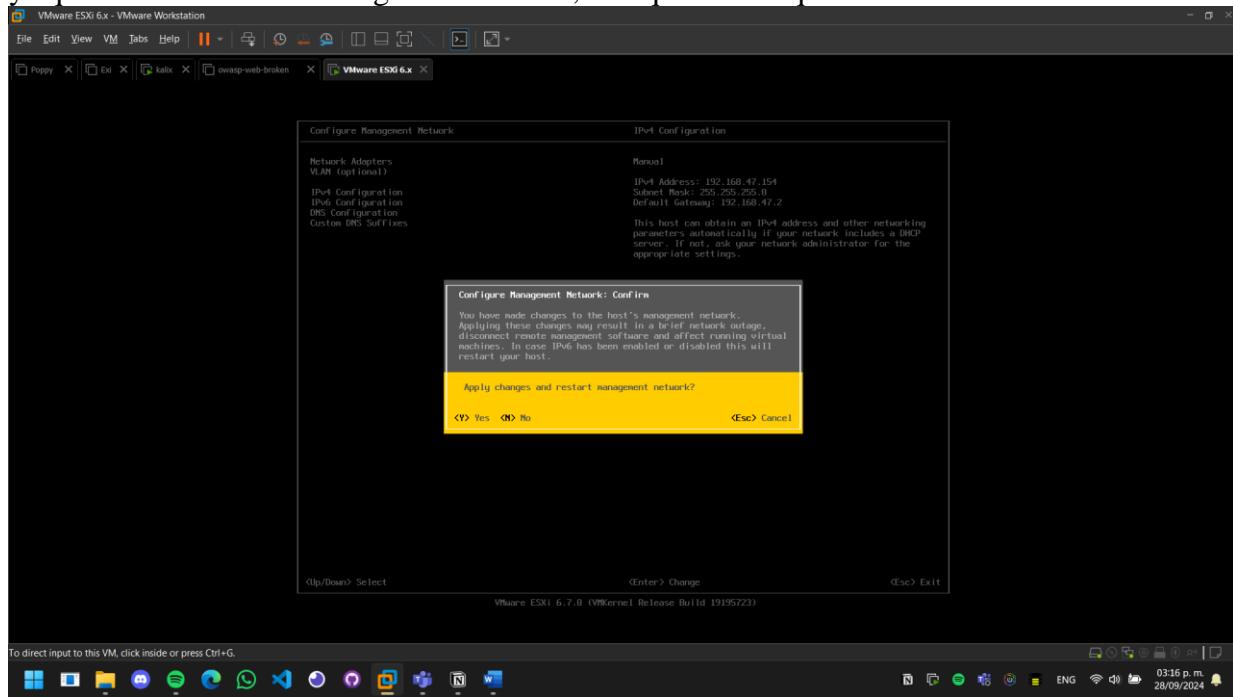
Hasta este punto la maquina ya estaría en funcionamiento, pero vamos a ajustar un detalle, y ese es la dirección ip, ya que actualmente está configurada para que la tome del dhcp, por lo que vamos a darle una dirección estática, para ello oprimimos F2 y nos vamos al apartado de Configure Management Network



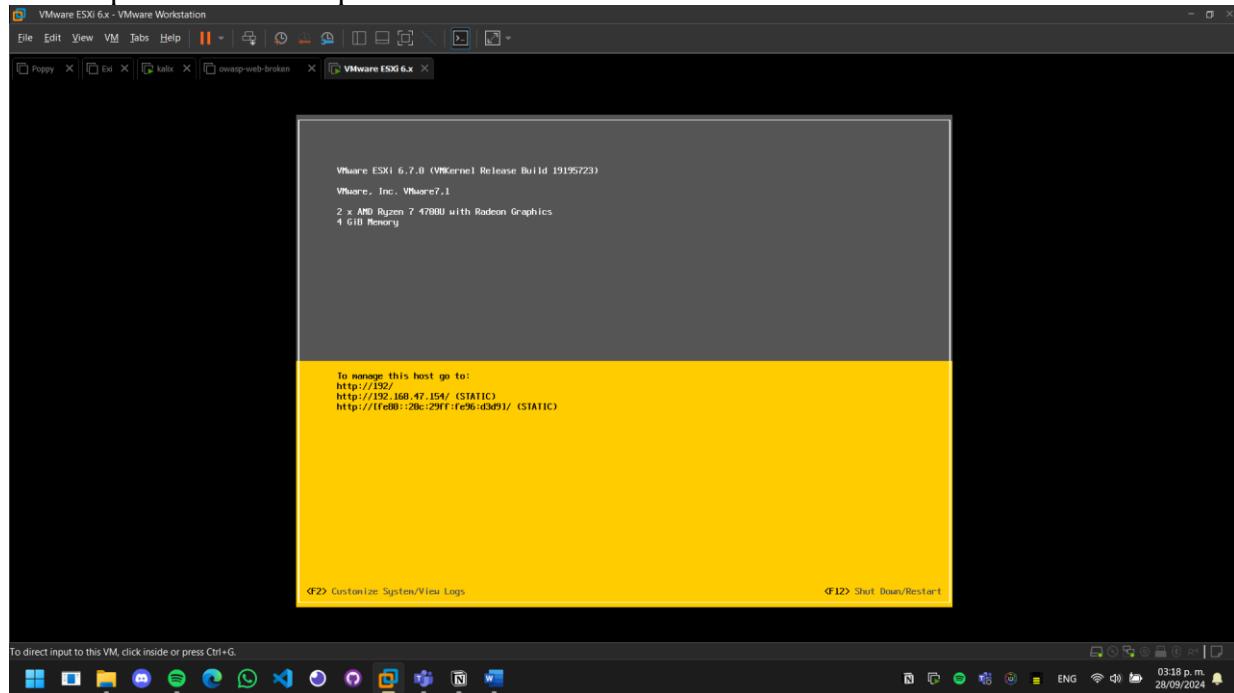
Una vez ahí nos dirigimos a las opciones de IPv4 Configuration, y ahí seleccionamos la opción de “Set static IPv4 address and network configuration:” con la barra espaciadora y luego damos enter.



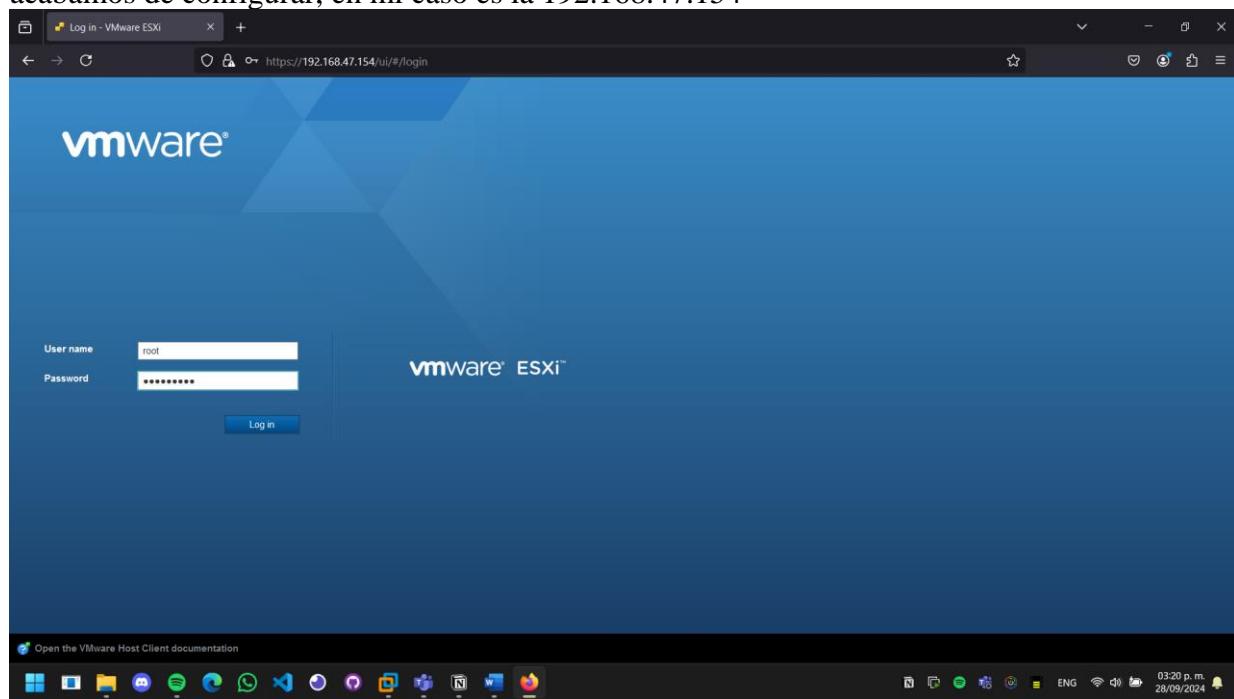
Ahora ya solo volvemos al inicio con ESC, y ya solo nos pide si deseamos aplicar los cambios ya que modificamos la configuración de red, a lo que damos que si



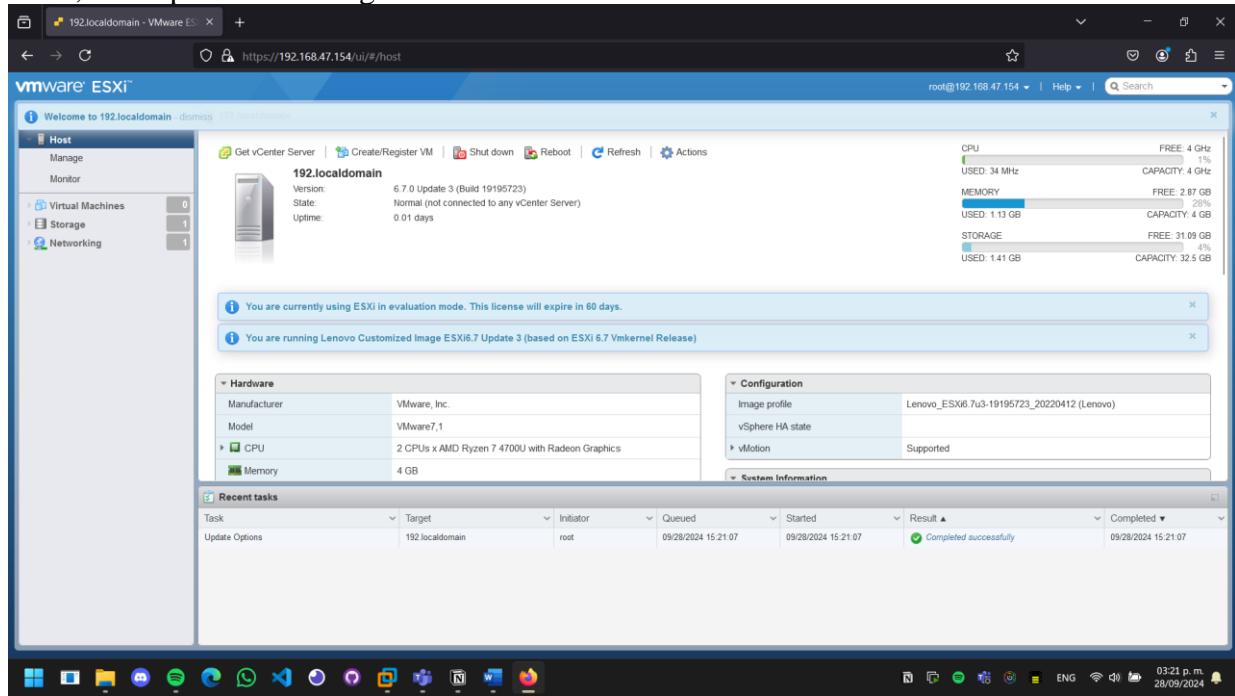
Y listo, ahora nuestra IP será estática, lo cual significa que no corremos el riesgo de que cambie cuando prendamos la máquina.



Para comprobar que la maquina funciona correctamente ingresamos a la dirección que acabamos de configurar, en mi caso es la 192.168.47.154

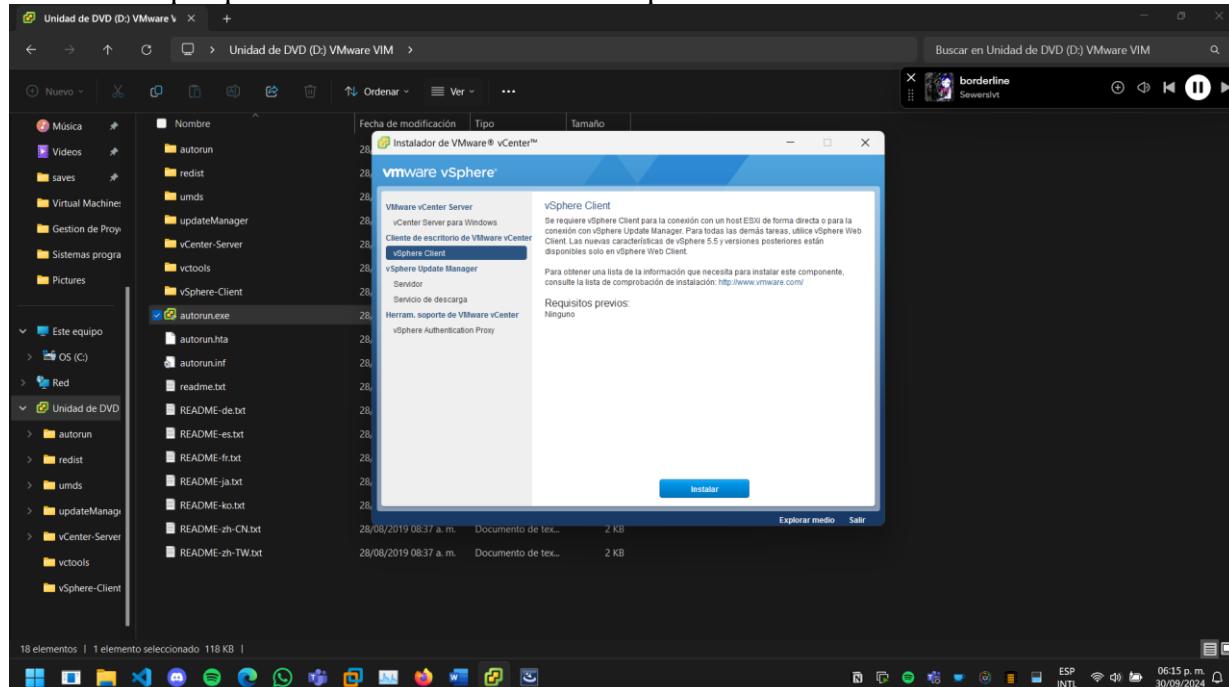


Listo, ahora podemos configurar nuestro servidor ESXi

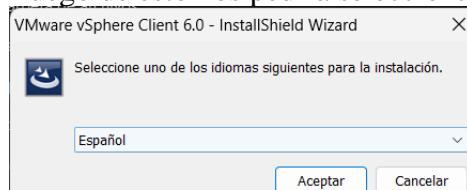


## Instalación de vSphere Client

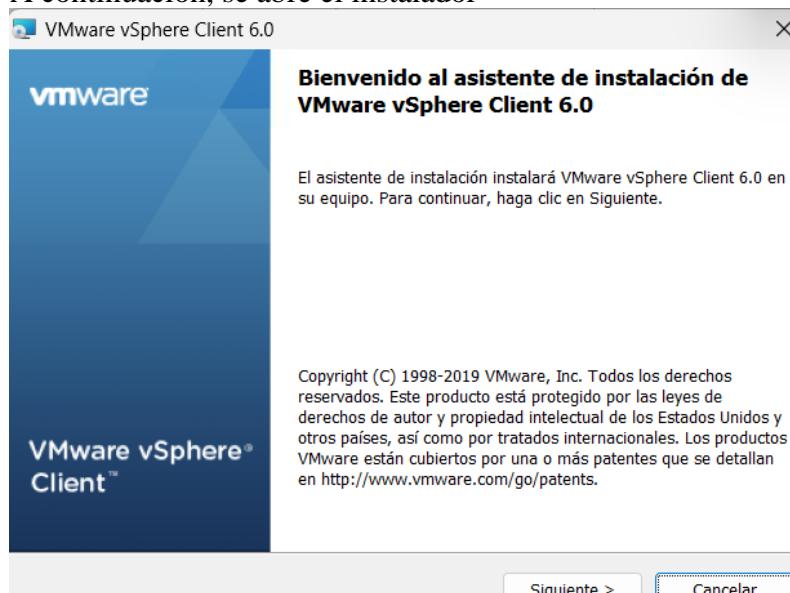
Lo primero es abrir el ejecutable, en donde nos saldrá la siguiente ventana, aquí podemos seleccionar que queremos instalar el cliente de vSphere.



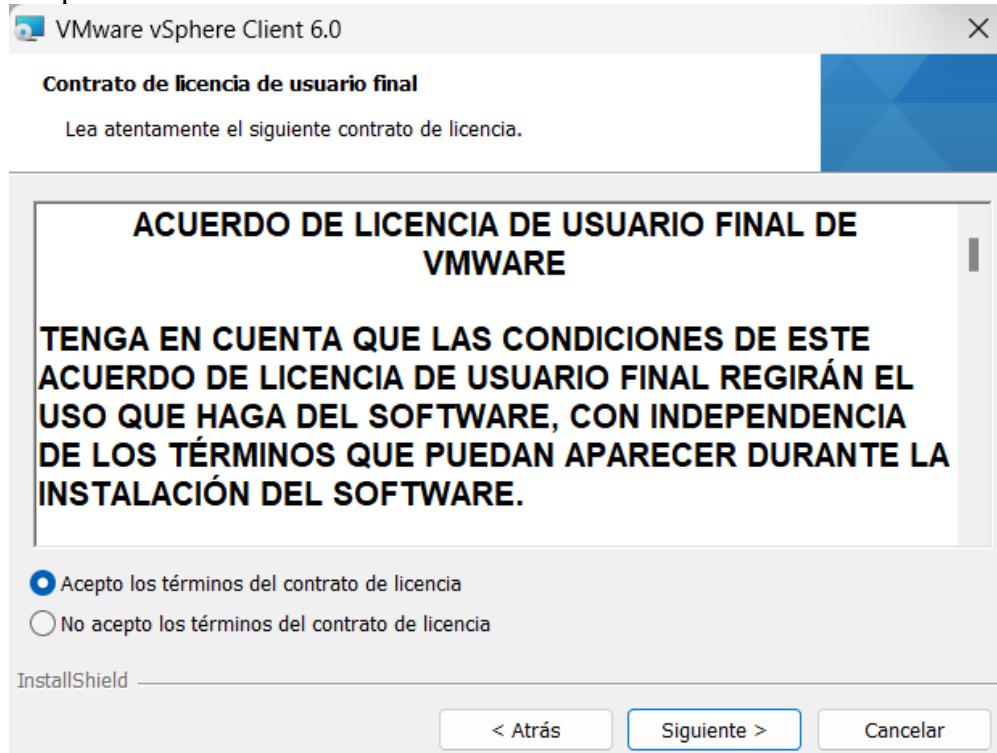
Luego de esto nos pedirá seleccionar el idioma.



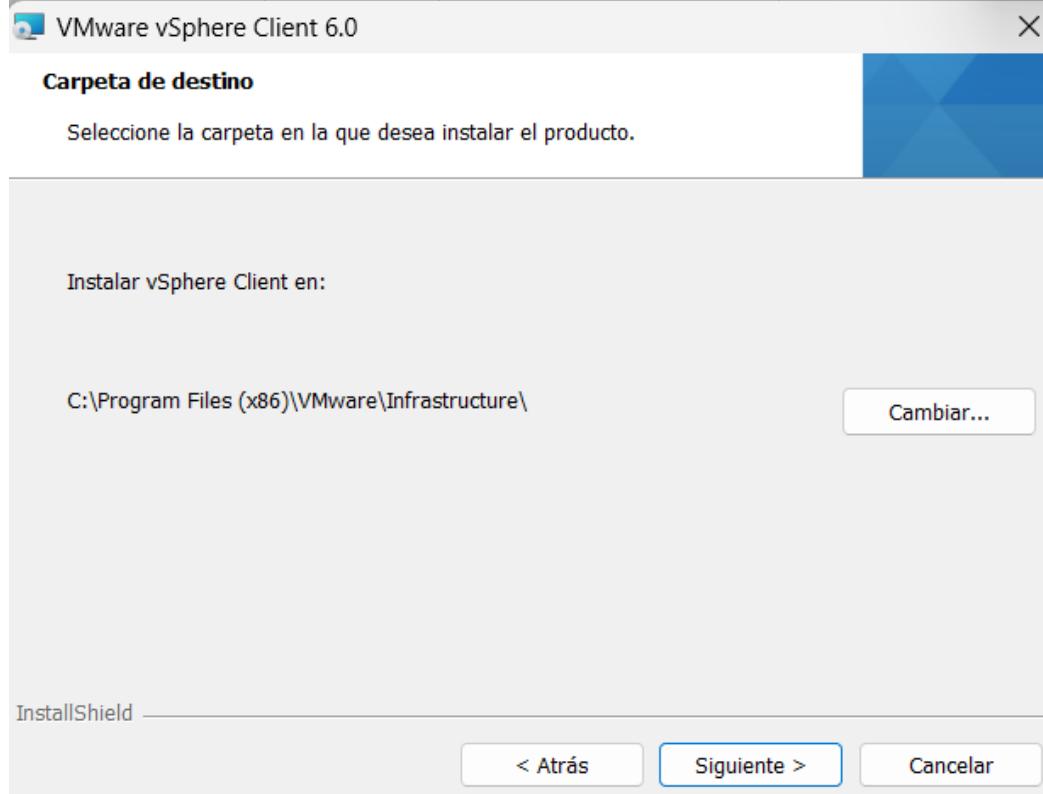
A continuación, se abre el instalador



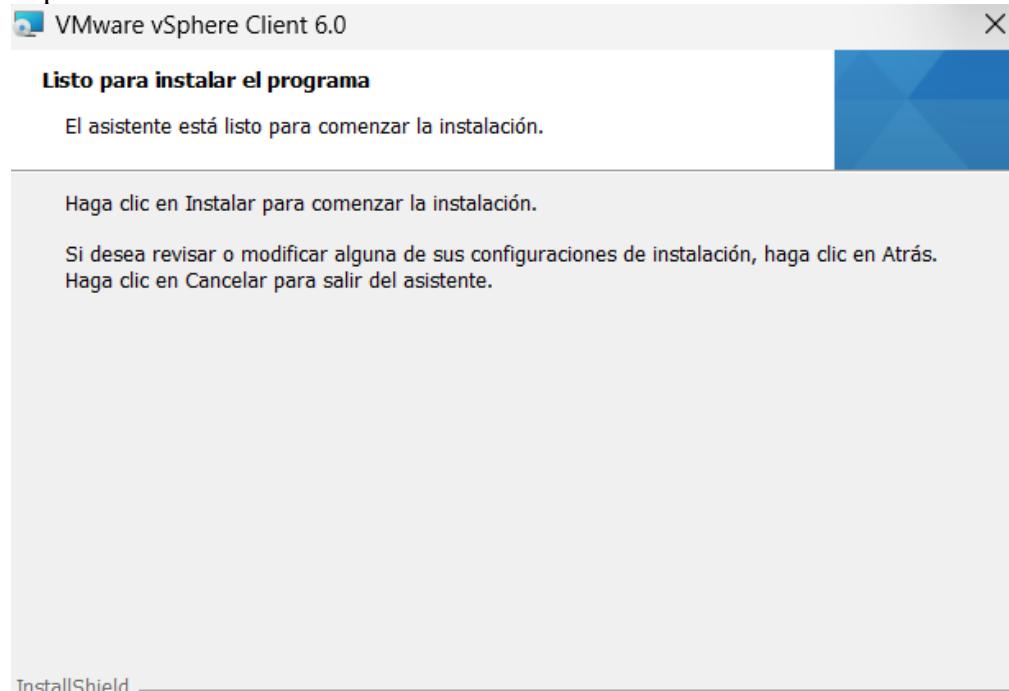
Aceptamos la licencia de usuario.



Luego seleccionamos la ruta donde queremos que se instale.

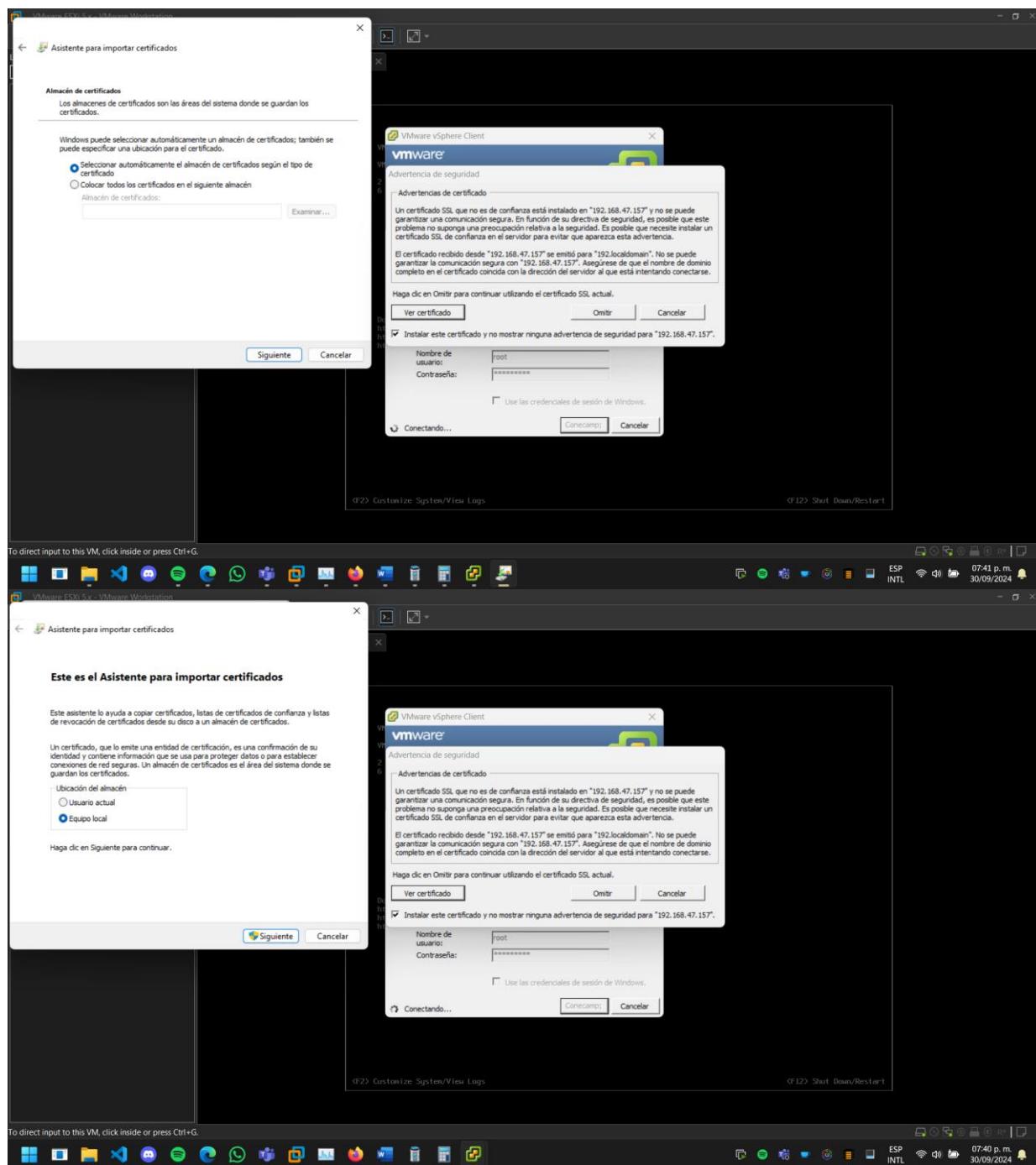


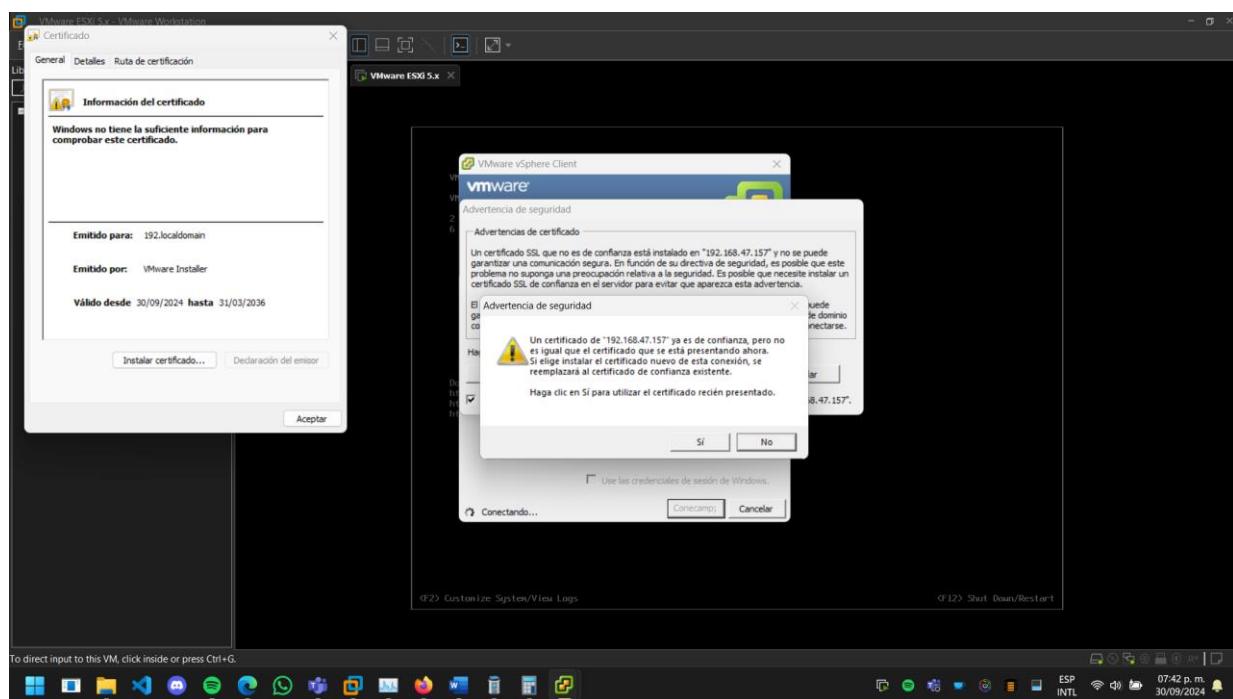
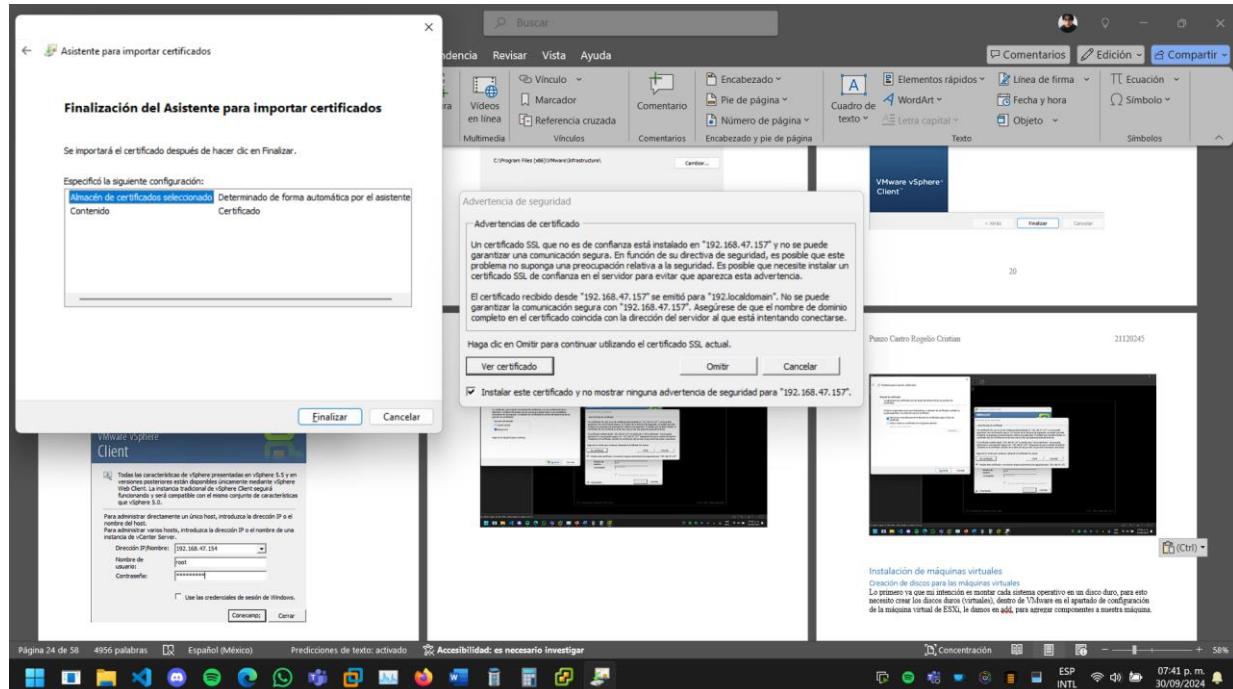
Y procedemos con la instalación.



Ahora procedemos a buscar y ejecutar el cliente, donde lo primero que nos pide es la dirección de la maquina ESXi, así como sus credenciales para iniciar sesión.

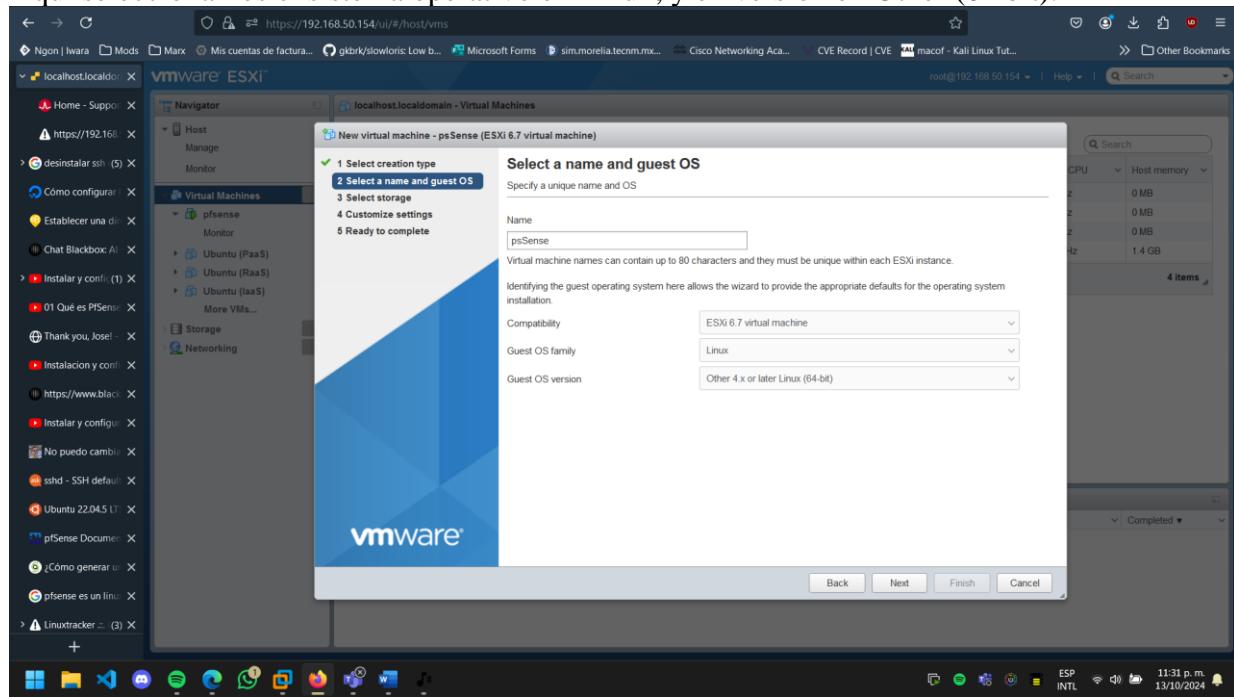




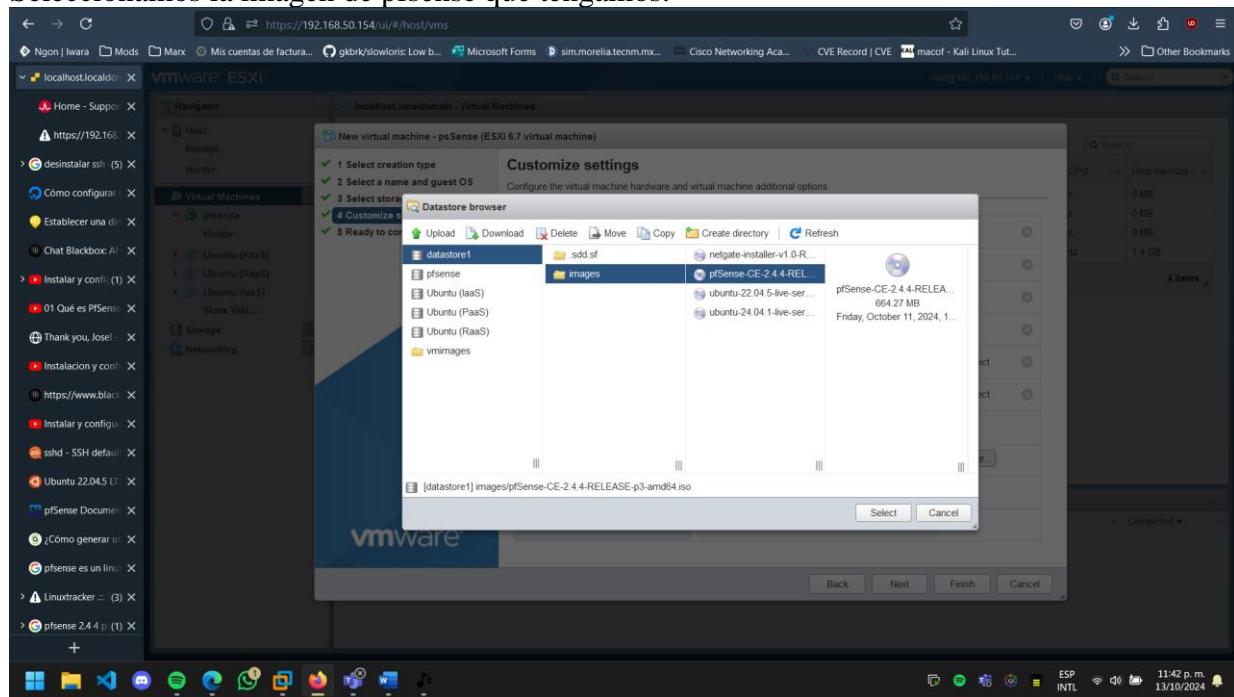


## Instalación de pfSense

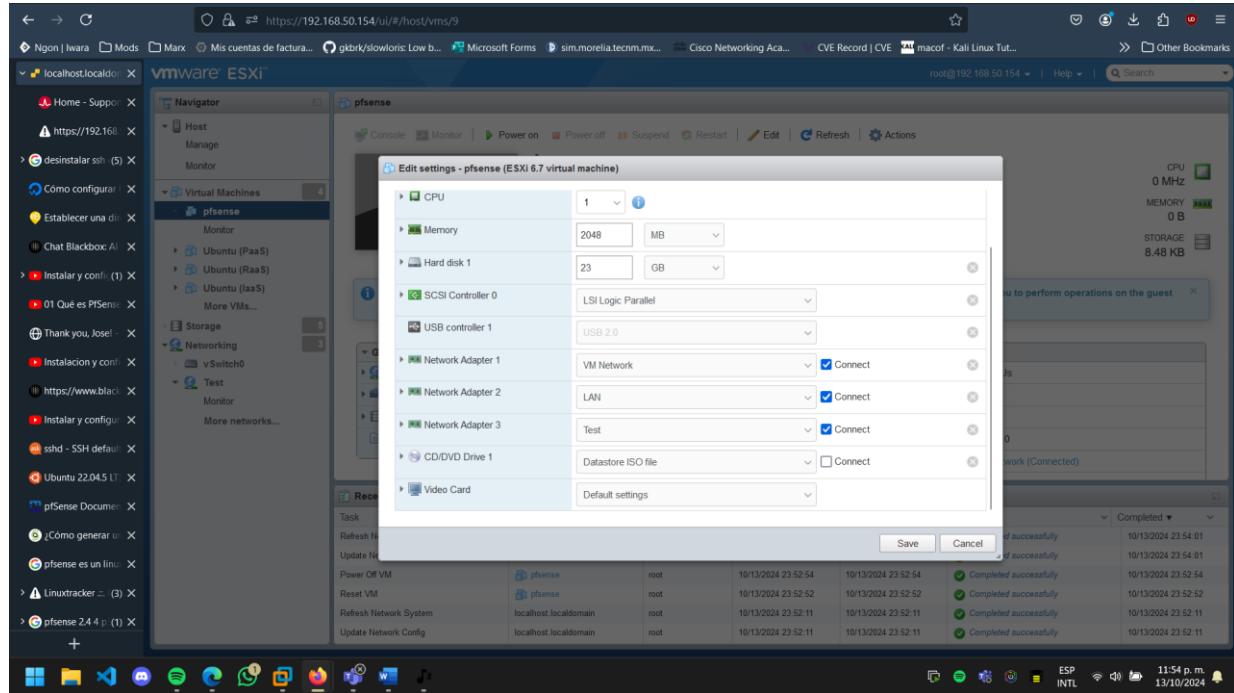
Lo primero es crear una máquina virtual dentro de nuestra maquina ESXi.  
Aquí seleccionamos el sistema operativo en Linux, y en versión en Other (64 bit).



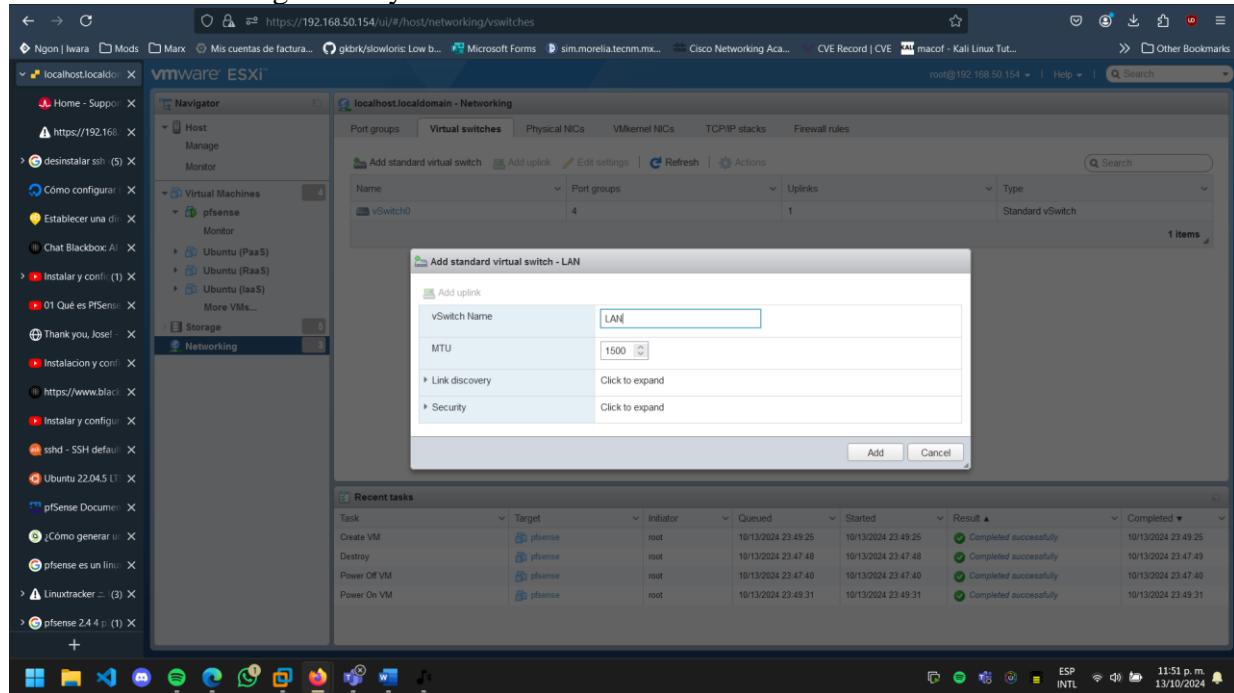
Seleccionamos la imagen de pfSense que tengamos.



También hay que agregar dos tarjetas de red, las necesitaremos para la configuración más adelante.



Ahora en Networking vamos y creamos un nuevo vSwitch



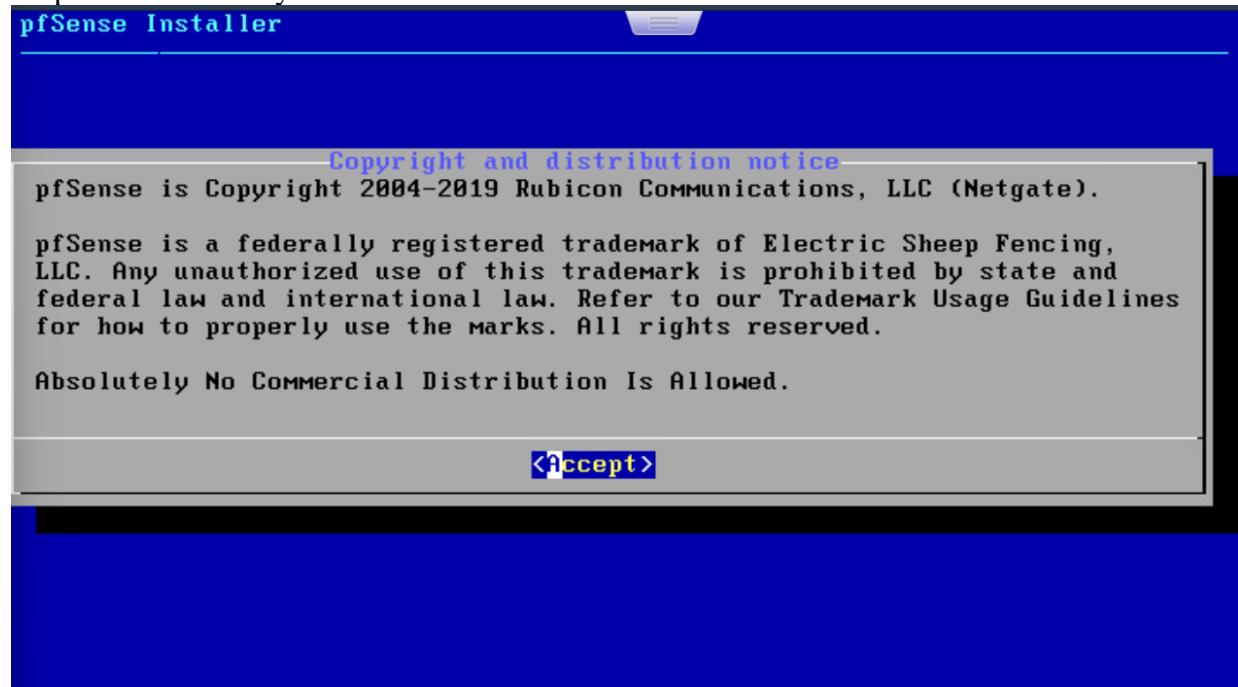
Ahora agregamos un nuevo port group que va a tener el vSwitch que creamos

The screenshot shows the VMware ESXi interface with the URL <https://192.168.50.154/ui/#/host/networking/portgroups>. The left sidebar has sections for Home, Support, Host, Virtual Machines, Storage, Networking, and Test. The Networking section is selected. In the main pane, the 'Port groups' tab is active, showing a table with three entries: VM Network, Production, and Test. A modal dialog titled 'Add port group - LAN' is open, prompting for Name (LAN), VLAN ID (0), and Virtual switch (LAN). Below the table is a 'Recent tasks' list with several completed items. The bottom right corner shows the system status bar with the date 13/10/2024 and time 11:53 p.m.

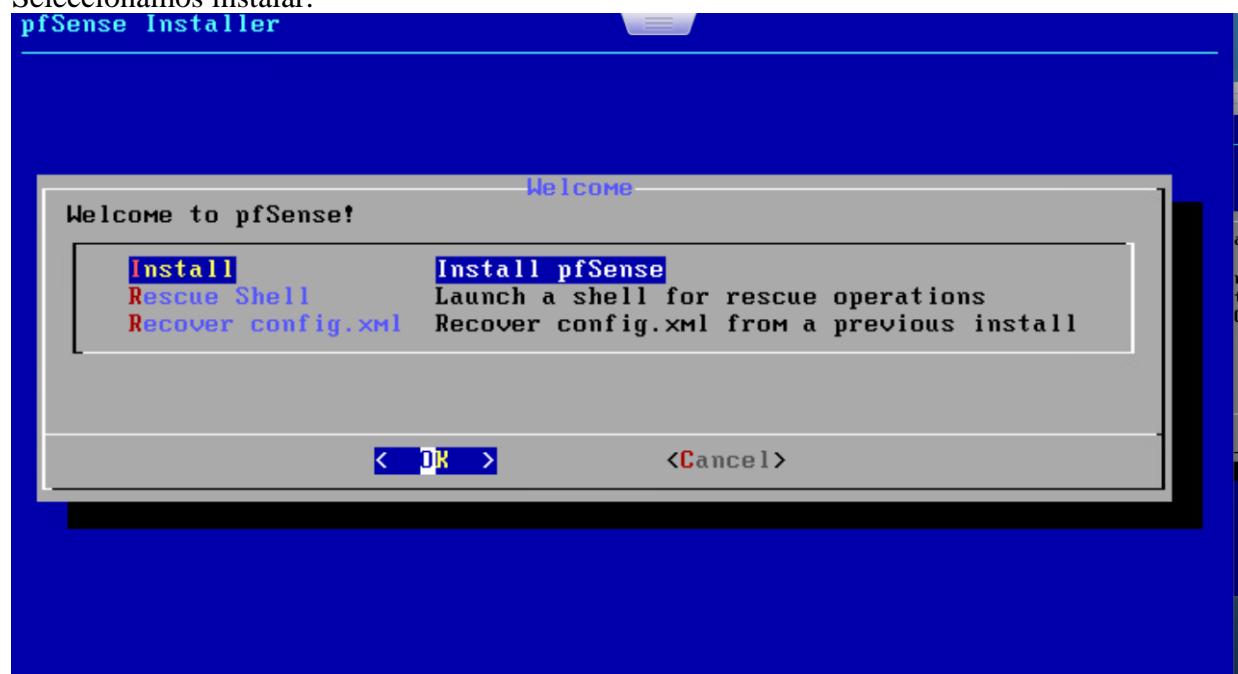
También ponemos la tarjeta de la máquina de pfSense en ese grupo

The screenshot shows the VM settings interface for a VM named 'pfSense'. On the left, there are tabs for General, Processor, Memory, Storage, and Network. The Network tab is selected, showing four network adapters: Network Adapter 1 (VM Network, connected), Network Adapter 2 (LAN, connected), Network Adapter 3 (Producción, connected), and CD/DVD Drive 1 (VM Network, not connected). The 'Video Card' tab is also visible at the bottom.

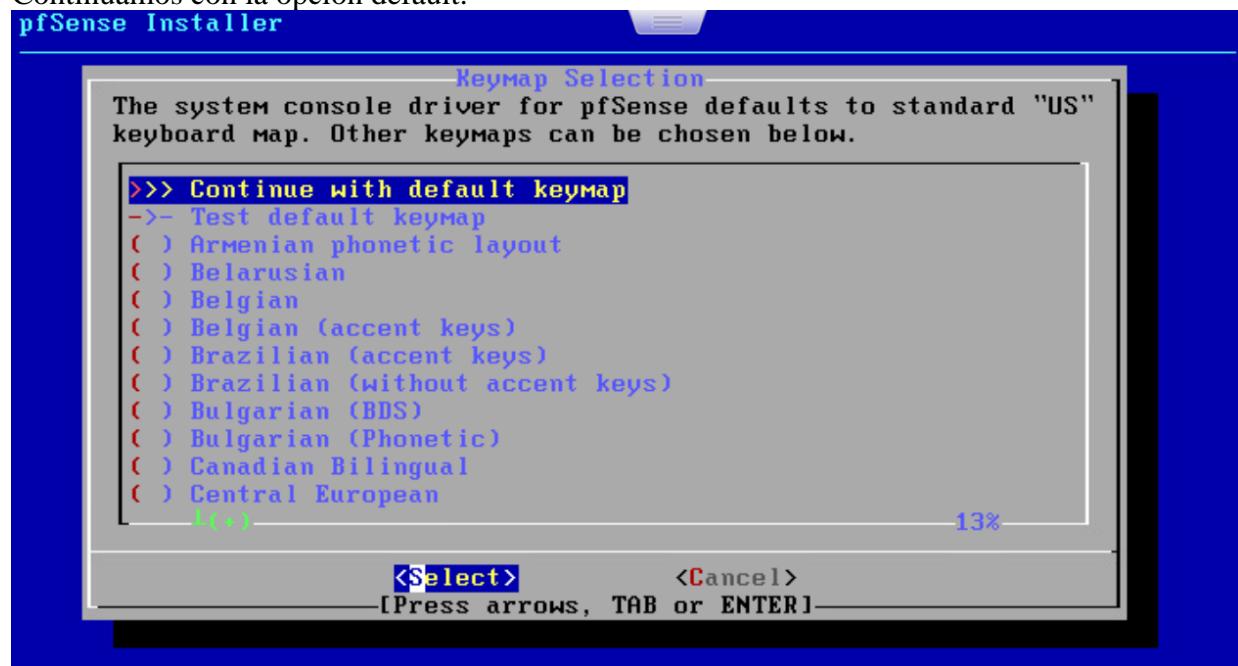
Ahora procedemos a iniciar la máquina virtual, la instalación es bastante sencilla, primero aceptamos términos y condiciones.



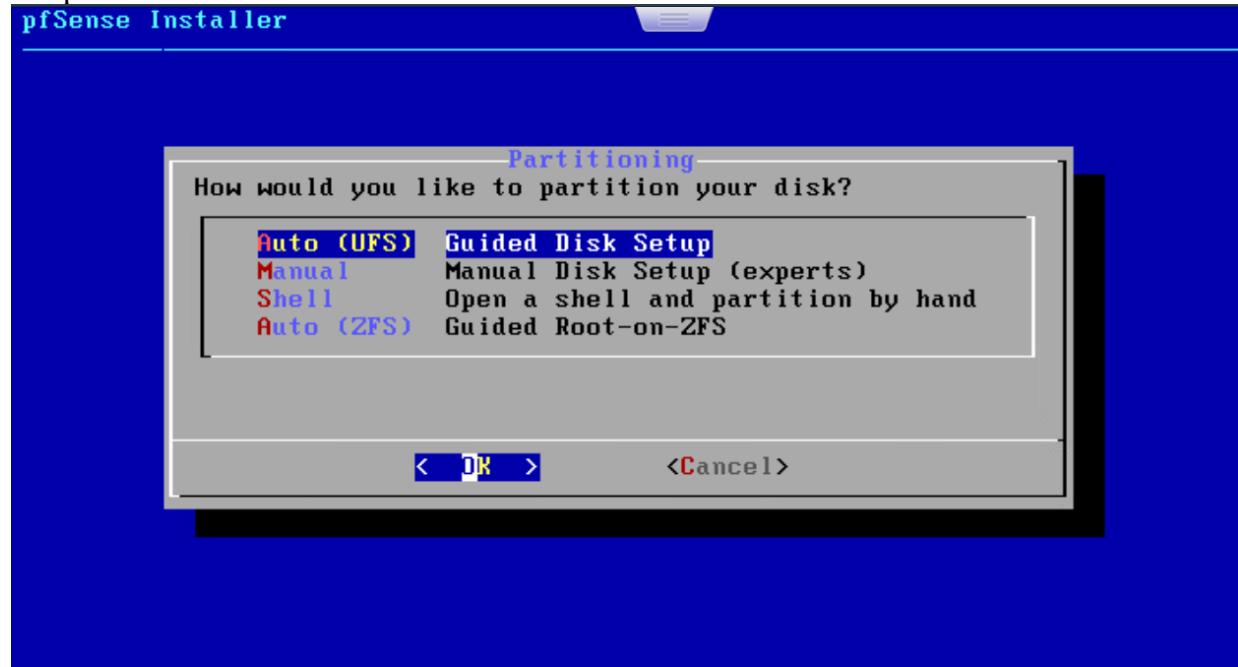
Seleccionamos instalar.



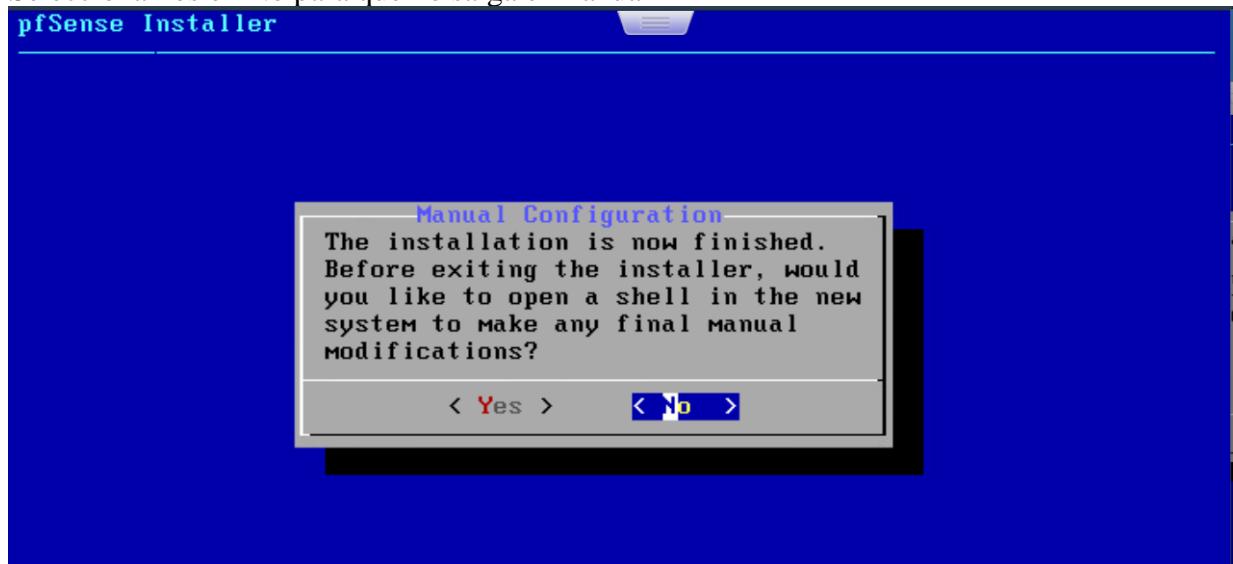
Continuamos con la opción default.



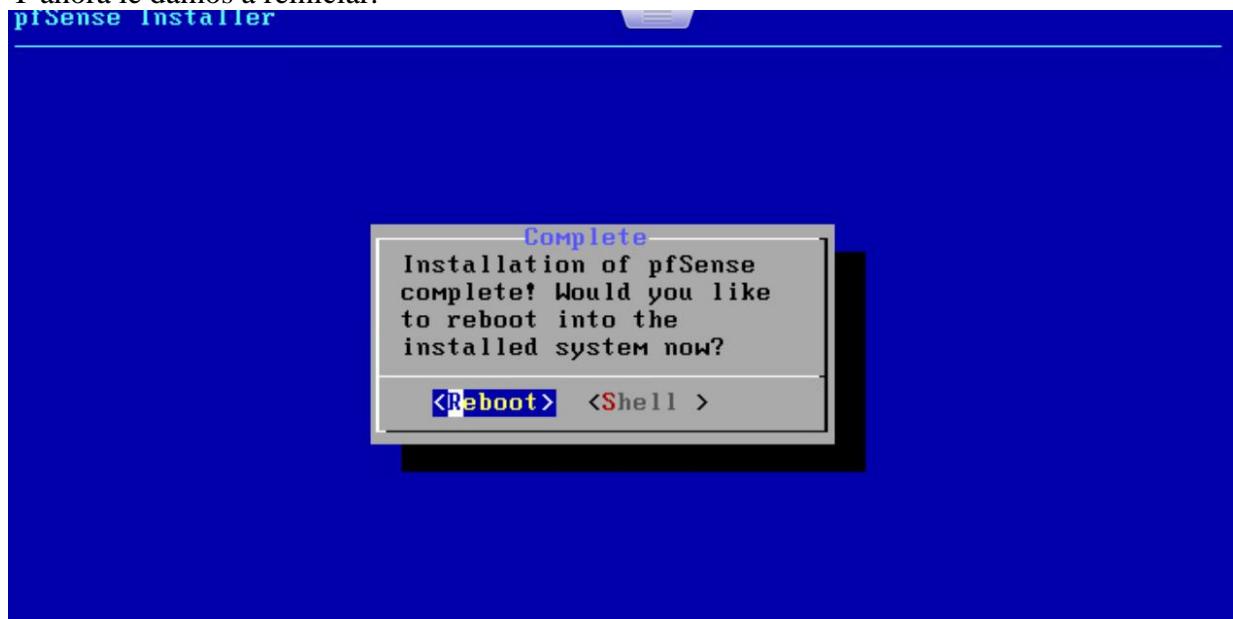
Aceptamos el modo automático.



Seleccionamos en No para que no salga el manual



Y ahora le damos a reiniciar.



Ahora vamos con las configuraciones iniciales desde la consola:

Para iniciar seleccionamos 1, para asignar las interfaces, lo primero que nos pregunta es si queremos asignar vlans, ahorita escribimos “n” para decir que no.

```

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

```

Enter an option: 1

Valid interfaces are:

```

em0      00:0c:29:57:dd:cc  (up) Intel(R) PRO/1000 Legacy Network Connection 1.
em1      00:0c:29:57:dd:d6  (up) Intel(R) PRO/1000 Legacy Network Connection 1.
em2      00:0c:29:57:dd:e0  (down) Intel(R) PRO/1000 Legacy Network Connection 1.

```

Do VLANs need to be set up first?

If VLANs will not be used, or only for optional interfaces, it is typical to say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y\!n]? ■

Ahora nos pide:

- Seleccionar la interfaz para la WAN seleccionamos “em0”

```

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

```

```

Enter the WAN interface name or 'a' for auto-detection
(em0 em1 em2 or a): em0

```

- Seleccionar la interfaz para la LAN seleccionamos “em2”

```

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 em2 a or nothing if finished): em1

```

- Seleccionar la interfaz “em2” para la DMZ

```

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em2 - static)
3 - OPT1 (em1)

```

- Por último, nos pregunta si queremos proceder y damos “y”

```
Do you want to proceed [y/n]? y

Writing configuration...done.
One moment while the settings are reloading... done!
VMware Virtual Machine - Netgate Device ID: fb45a4b9a8c73e467099
```

- Y ya nos mostrara las ip de la WAN y LAN.

```
*** Welcome to pfSense 2.4.4-RELEASE-p3 (amd64) on pfSense ***
WAN (wan)      -> em0          -> v4/DHCP4: 192.168.50.139/24
LAN (lan)      -> em1          -> v4: 192.168.1.1/24
```

- Ahora pasamos a asignar las ips a las interfaces, primero comenzamos con la red LAN y le asignamos la red 172.16.0.1 con mascara de 24 bits

```
Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em2 - static)
3 - OPT1 (em1)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 172.16.0.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0 = 16
     255.0.0.0 = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24
```

- A continuación, damos enter para indicar que, si es una red LAN, volvemos a dar enter cuando pida ipv6, y en la parte de HTTP damos un “y”.

```
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) █
```

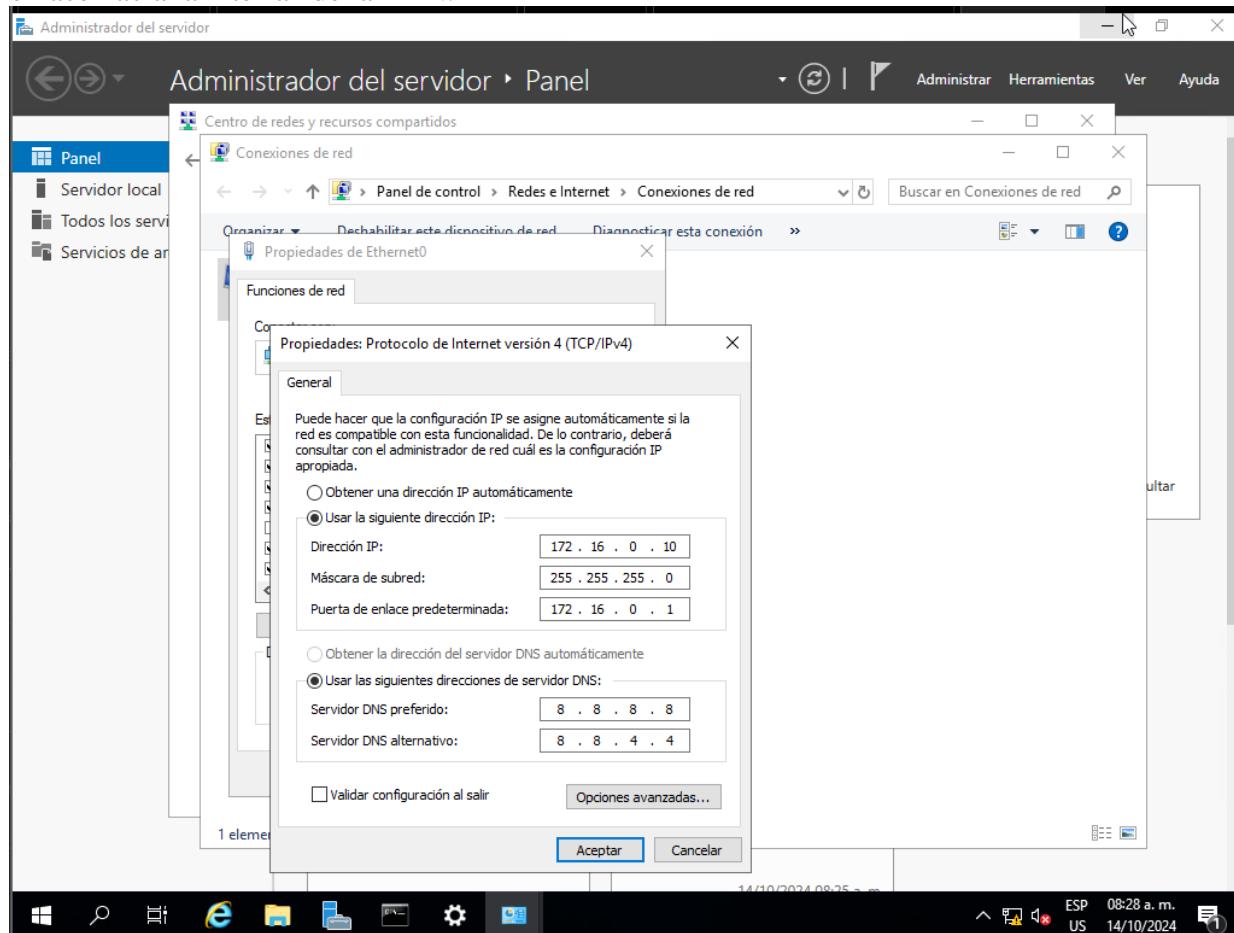
Y ahora nos da la ip a la cual podemos conectarnos para tener acceso a pfSense.

```
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y

Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...
Restarting webConfigurator...

The IPv4 LAN address has been set to 172.16.0.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
http://172.16.0.1/
```

Ahora dentro de la máquina Windows que usaremos para conectarme a esa red, tenemos que asignarle una ip que esté dentro del rango. En este caso pondré la 172.16.0.10, con puerta de enlace hacia la interfaz de la LAN.



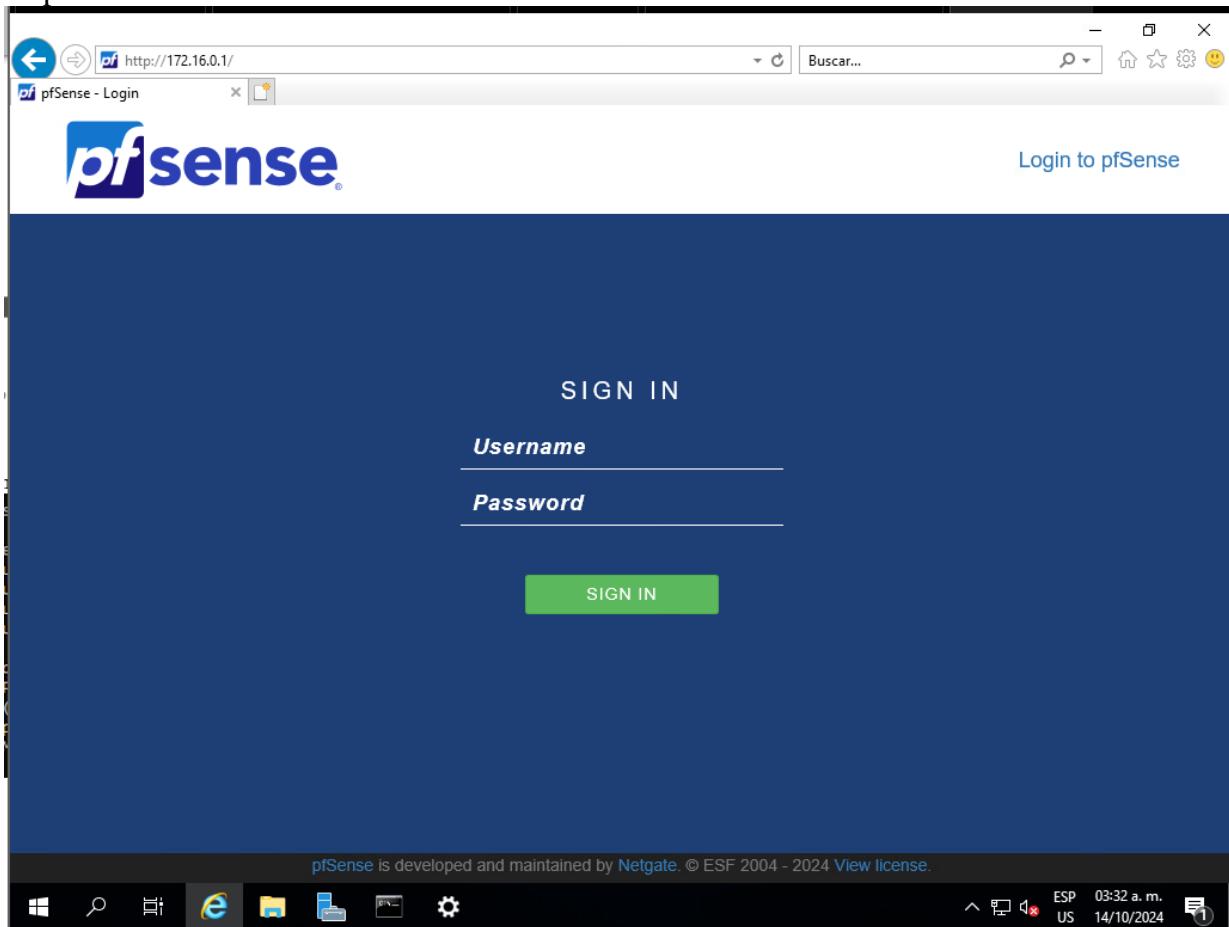
Y como vemos ya existe comunicación con nuestro Gateway

```
C:\Users\Administrador>ping 172.16.0.1

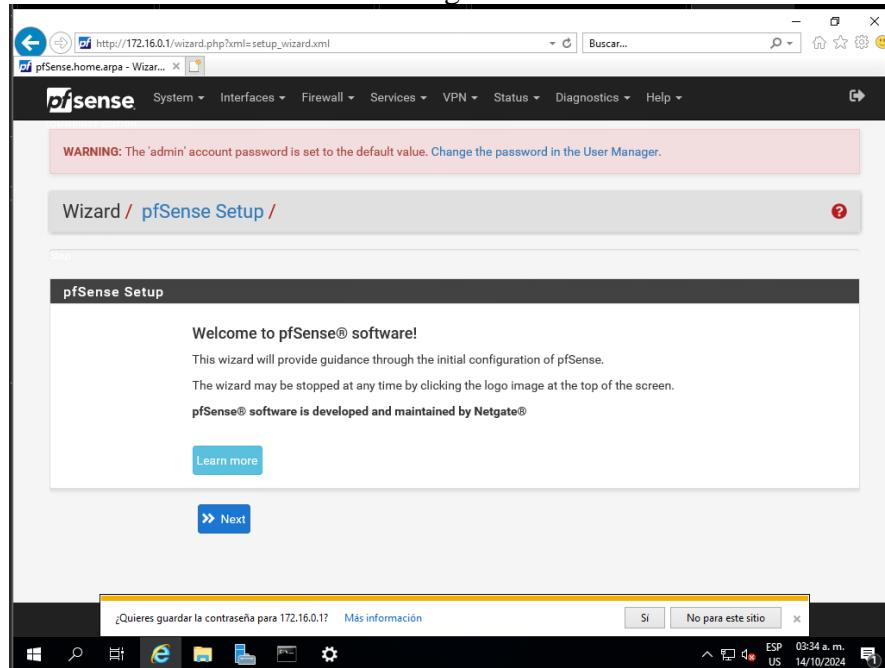
Haciendo ping a 172.16.0.1 con 32 bytes de datos:
Respuesta desde 172.16.0.1: bytes=32 tiempo<1ms TTL=64
Respuesta desde 172.16.0.1: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.0.1: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.0.1: bytes=32 tiempo<1ms TTL=64

Estadísticas de ping para 172.16.0.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
                (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 2ms, Media = 0ms
```

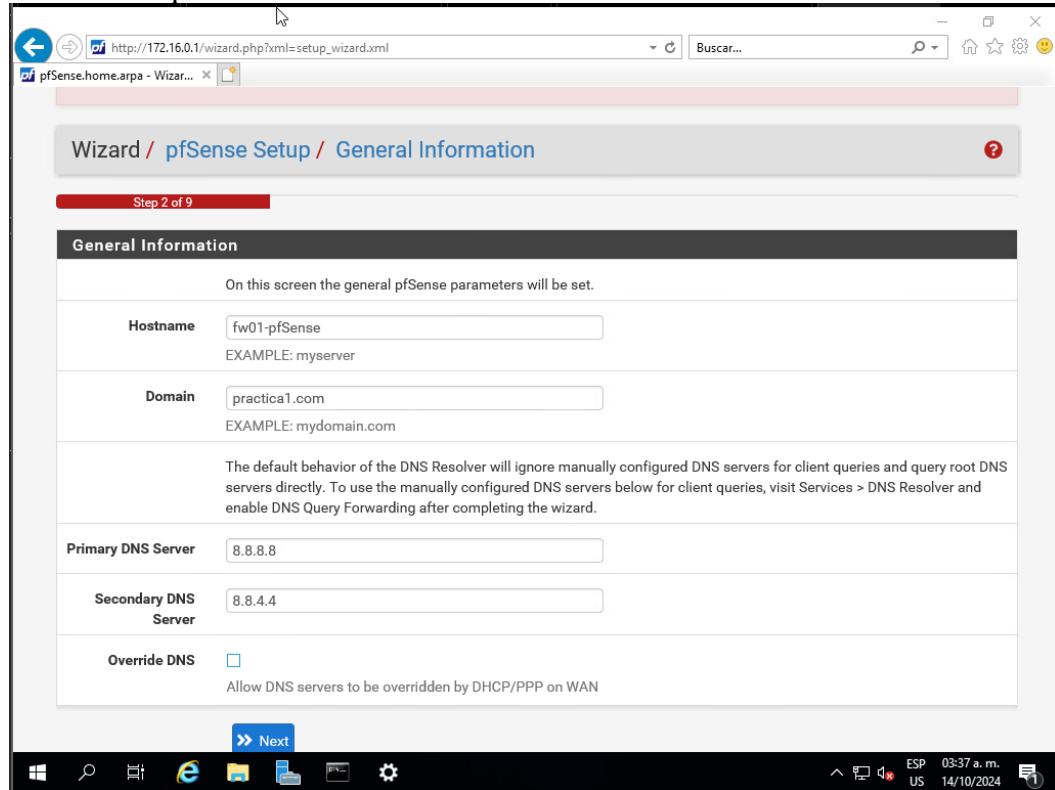
Ahora si al ingresar a esa dirección a través del navegador, podemos entrar a la interfaz gráfica de pfSense.



Y se nos abre el asistente de configuración



Aquí nos pide información del host, lo importante son los DNS, podemos establecer unos manuales o que los tome de la WAN al marcar la última casilla.



En esta parte seleccionamos nuestra zona horaria.

The screenshot shows the pfSense setup wizard at step 3 of 9, titled "Time Server Information". A red warning box at the top says: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below it, the form fields are shown:

- Time server hostname:** 2.pfsense.pool.ntp.org (with a note: "Enter the hostname (FQDN) of the time server.")
- Timezone:** America/Mexico\_City

A blue "Next" button is at the bottom right.

Lo que sigue es la configuración de la interfaz WAN, lo dejamos en DHCP.

The screenshot shows the "Configure WAN Interface" screen. A note says: "On this screen the Wide Area Network information will be configured." A dropdown menu labeled "SelectedType" has "DHCP" selected.

Y en la parte inferior de esa ventana tendremos la opción para bloquear las redes privadas que entren por la WAN.

The screenshot shows the "RFC1918 Networks" configuration screen. Under "Private Networks", there is a checked checkbox labeled "Block RFC1918 Private Networks from entering via WAN". A note explains: "When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too."

Esta otra casilla es para bloquear cualquier dispositivo que su ip no pertenezca o no este asignada por la IANA, después damos en siguiente.

The screenshot shows the "Block bogon networks" configuration screen. Under "Block bogon networks", there is a checked checkbox labeled "Block non-Internet routed networks from entering via WAN". A note explains: "When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received."

Ahora nos muestra la configuración de la interfaz (lo que ya había configurado por la línea de comandos)

**Configure LAN Interface**

On this screen the Local Area Network information will be configured.

LAN IP Address	<input type="text" value="172.16.0.1"/> <span style="font-size: small;">X</span>
Type dhcp if this interface uses DHCP to obtain its IP address.	
Subnet Mask	<input type="text" value="24"/>

**>> Next**

Ya por último ingresamos una nueva contraseña para iniciar sesión, ahora ya solo le damos en recargar página.

**Reload configuration**

Click 'Reload' to reload pfSense with new changes.

**>> Reload**

Y ya nos dice que está todo configurando

**Congratulations! pfSense is now configured.**

We recommend that you check to see if there are any software updates available. Keeping your software up to date is one of the most important things you can do to maintain the security of your network.

**Check for updates**

**Remember, we're here to help.**

**Click here** to learn about Netgate 24/7/365 support services.

### User survey

Please help all the people involved in improving and expanding pfSense software by taking a moment to answer this short survey (all answers are anonymous)

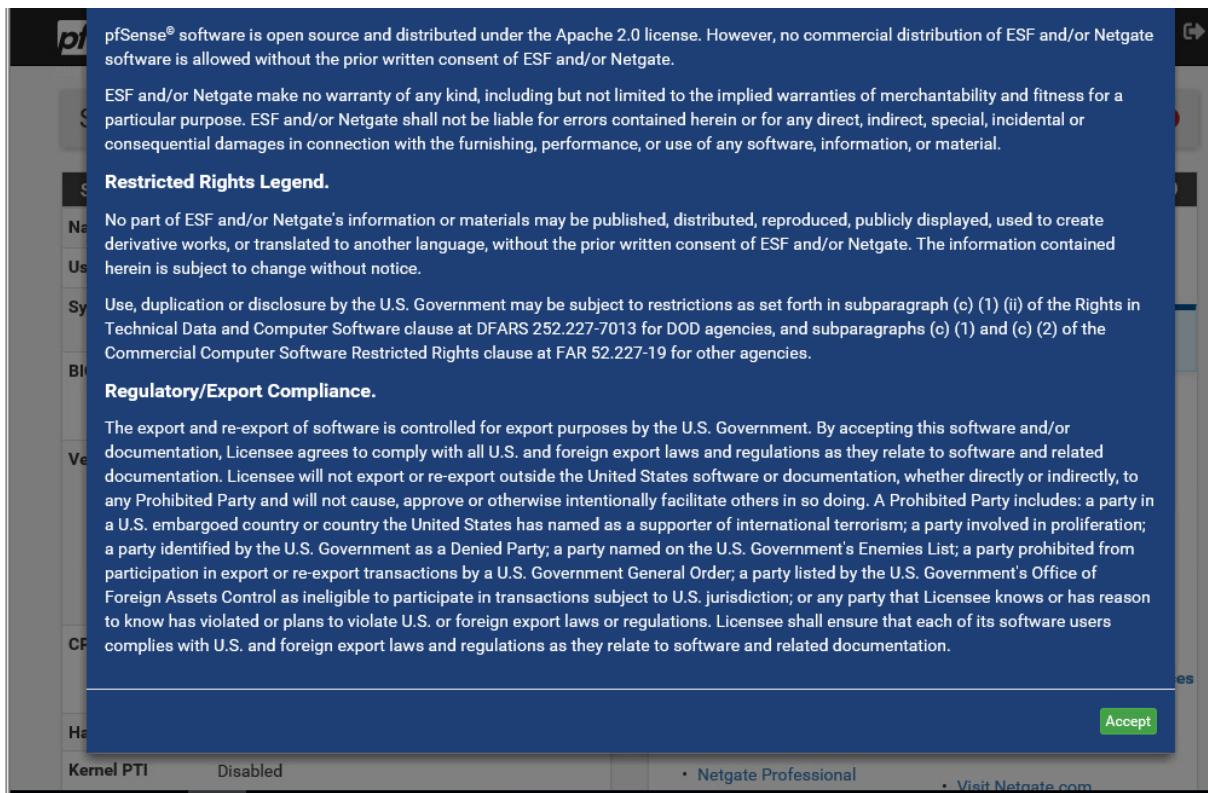
**Anonymous User Survey**

### Useful resources.

- Learn more about Netgate's product line, services, and pfSense software from our [website](#)
- To learn about Netgate appliances and other offers, [visit our store](#)
- Become part of the pfSense community. Visit our [forum](#)
- Subscribe to our [newsletter](#) for ongoing product information, software announcements and special offers.

**Finish**

Ya solo nos pide aceptar



Y ya nos aparecería el dashboard en donde sale nuestras interfaces que están conectadas.

CPU Type	AMD Ryzen 7 4700U with Radeon Graphics AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
<b>Hardware crypto</b>	
Kernel PTI	Disabled
MDS Mitigation	Inactive
Uptime	00 Hour 30 Minutes 57 Seconds
Current date/time	Mon Oct 14 3:55:42 CDT 2024
DNS server(s)	• 127.0.0.1 • 8.8.8.8 • 8.8.4.4
Last config change	Mon Oct 14 3:52:11 CDT 2024
State table size	0% (7/95000) <a href="#">Show states</a>
MBUF Usage	0% (2416/1000000)

If you decide to purchase a Netgate Global TAC Support subscription, you **MUST** have your **Netgate Device ID (NDI)** from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC supports [here](#).

Interfaces		
	WAN	1000baseT <full-duplex> 192.168.50.139
	LAN	1000baseT <full-duplex> 172.16.0.1

Para activar la interface DMZ vamos al apartado Interfaces>OPT1.

The screenshot shows the pfSense web interface at <http://172.16.0.1/>. The top navigation bar has tabs for System, Interfaces (which is highlighted in red), Firewall, Services, VPN, Status, Diagnostics, and Help. Below the navigation is a sidebar with 'Status / Dashboard' and 'System Information' sections. The main content area is titled 'Assignments' and shows three interface cards: WAN, LAN, and OPT1. The OPT1 card has edit and delete icons. To the right of the interface cards is a 'Netgate Services And Support' section with a '+ ?' button. At the bottom right of the page are 'Contract type' and 'Community Support' buttons.

Y nos muestra la configuración de esa interface, lo primero es seleccionar la casilla de enable para activarla, en descripción pones DMZ para cambiarle el nombre de OPT1, también seleccionamos el tipo de configuración IPv4 como Static IPv4

The screenshot shows the 'General Configuration' screen for the OPT1 interface. It includes fields for 'Enable' (checked), 'Description' (set to 'DMZ'), and 'IPv4 Configuration Type' (set to 'Static IPv4').

Lo siguiente es escribir la ip que tendrá la interfaz, así como su mascara de red, en este caso será 10.0.0.1 con mascara de 24 bits.

The screenshot shows the 'Static IPv4 Configuration' screen. It has fields for 'IPv4 Address' (10.0.0.1), 'IPv4 Upstream gateway' (None), and a green button '+ Add a new gateway'. Below the form is a note: 'If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Gateways can be managed by [clicking here](#)'.

En este caso no bloquearemos las redes privadas ya que usaremos en si una red privada, pero si marcamos para bloquear redes bogon.

**Reserved Networks**

<b>Block private networks and loopback addresses</b>	<input type="checkbox"/>	Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.
<b>Block bogon networks</b>	<input checked="" type="checkbox"/>	Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

**Save**

Damos clic en “Apply changes” para cargar los cambios.

**Interfaces / DMZ (em1)**

The DMZ configuration has been changed.  
The changes must be applied to take effect.  
Don't forget to adjust the DHCP Server range if needed after applying.

**Apply Changes**

Y después nos confirma los cambios.

The changes have been applied successfully.

Así ya nos aparecen las tres interfaces activas.

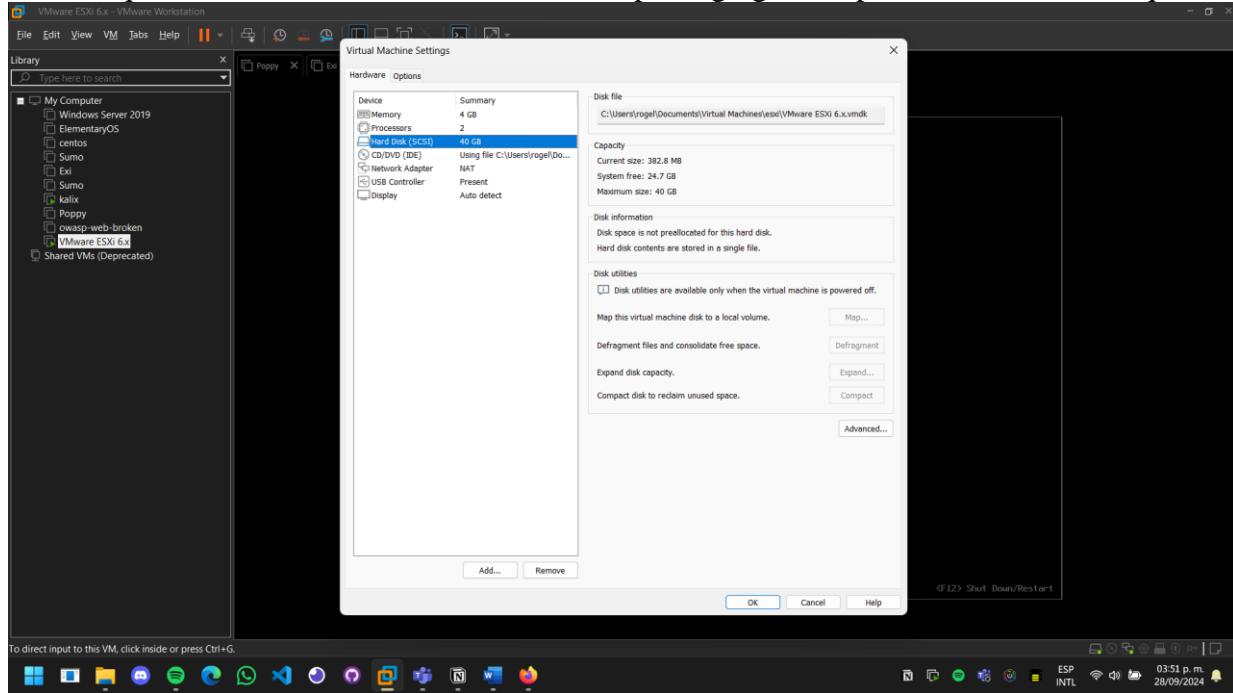
**Interfaces**

	WAN	1000baseT <full-duplex>	192.168.50.139
	LAN	1000baseT <full-duplex>	172.16.0.1
	DMZ	1000baseT <full-duplex>	10.0.0.1

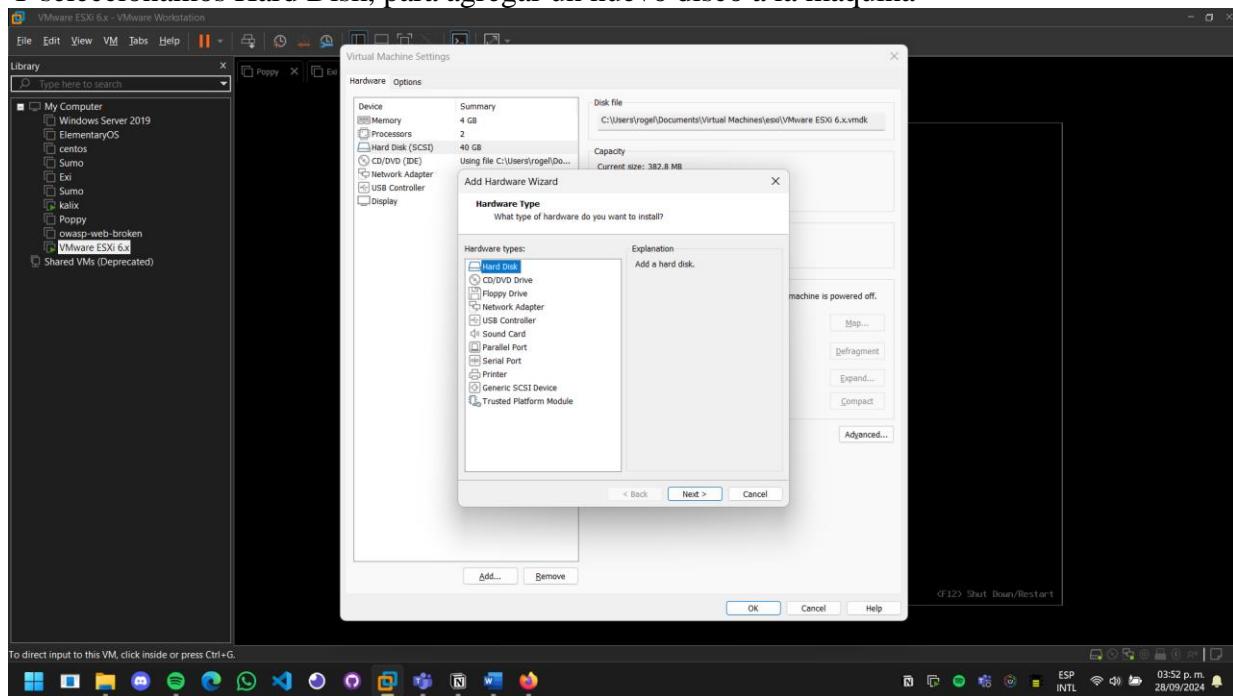
## Instalación de máquinas virtuales

### Creación de discos para las máquinas virtuales

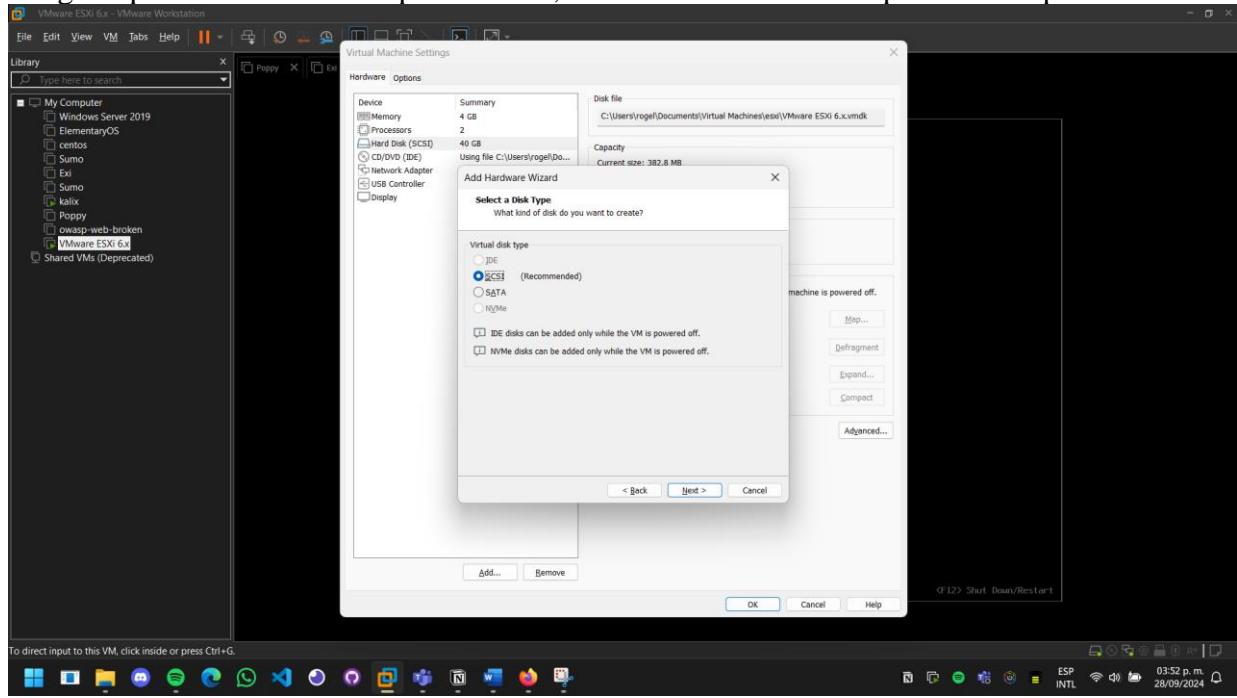
Lo primero ya que mi intención es montar cada sistema operativo en un disco duro, para esto necesito crear los discos duros (virtuales), dentro de VMware en el apartado de configuración de la máquina virtual de ESXi, le damos en add, para agregar componentes a nuestra máquina.



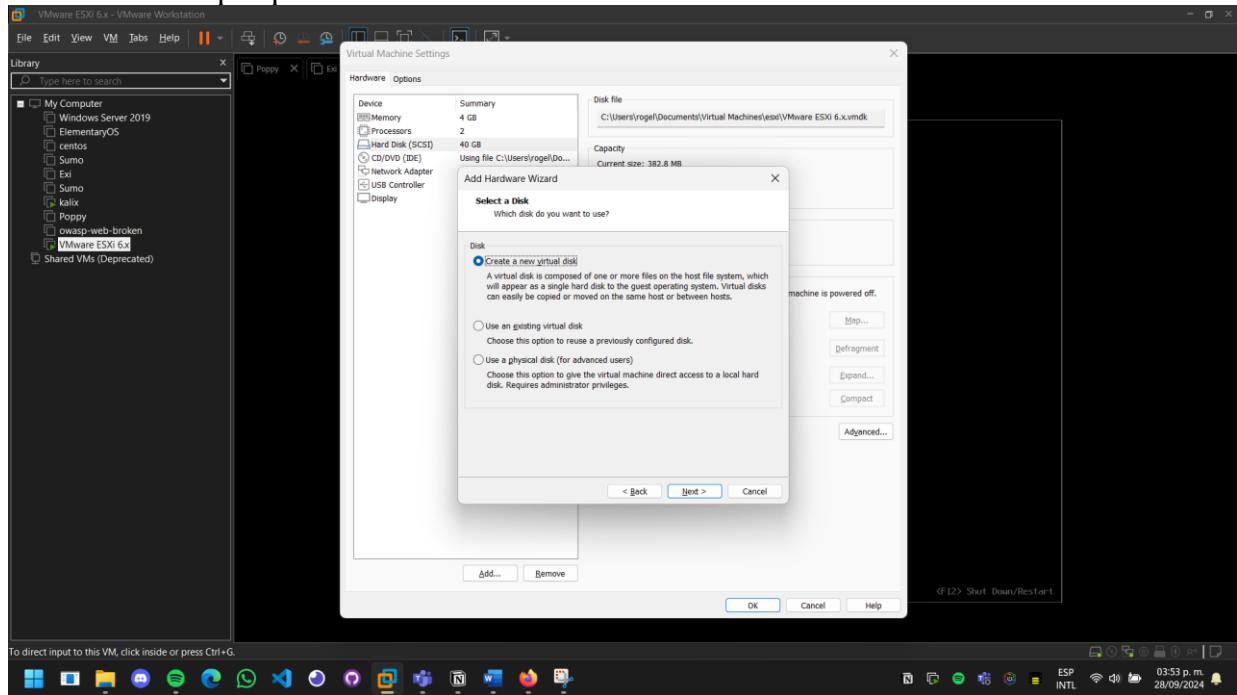
Y seleccionamos Hard Disk, para agregar un nuevo disco a la maquina



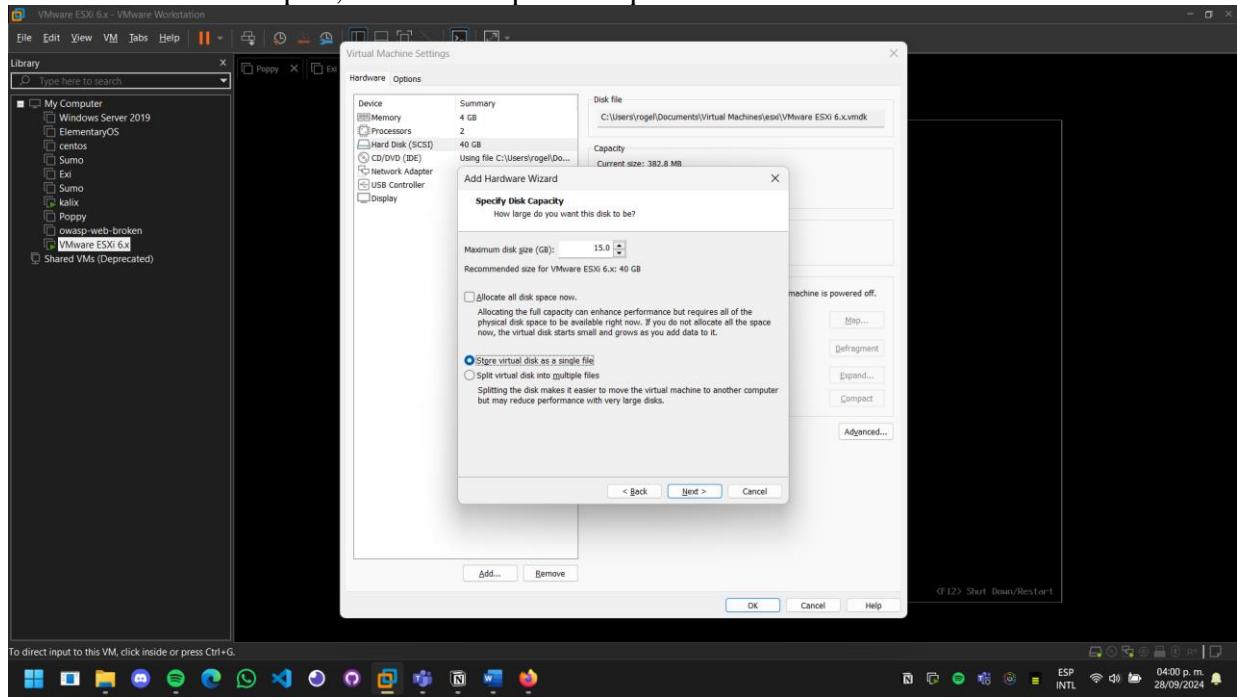
Al igual que el disco de la máquina virtual, también seleccionamos que sea del tipo SCSI



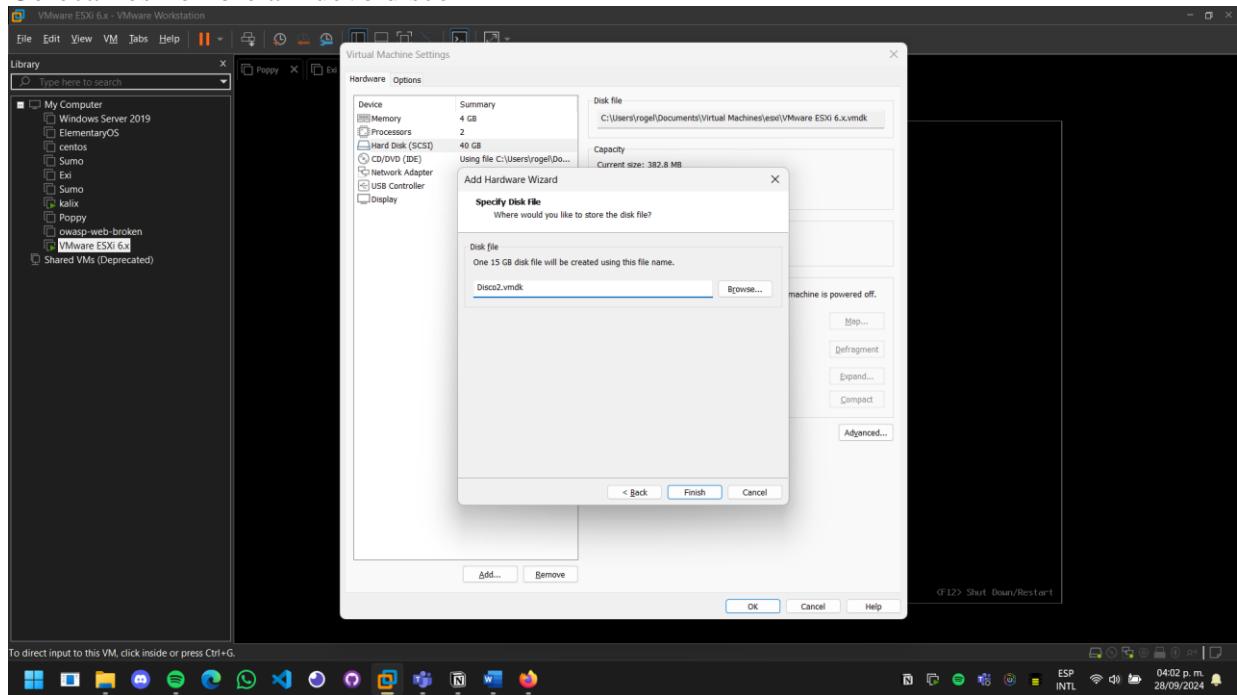
Seleccionamos que queremos crear un nuevo disco virtual



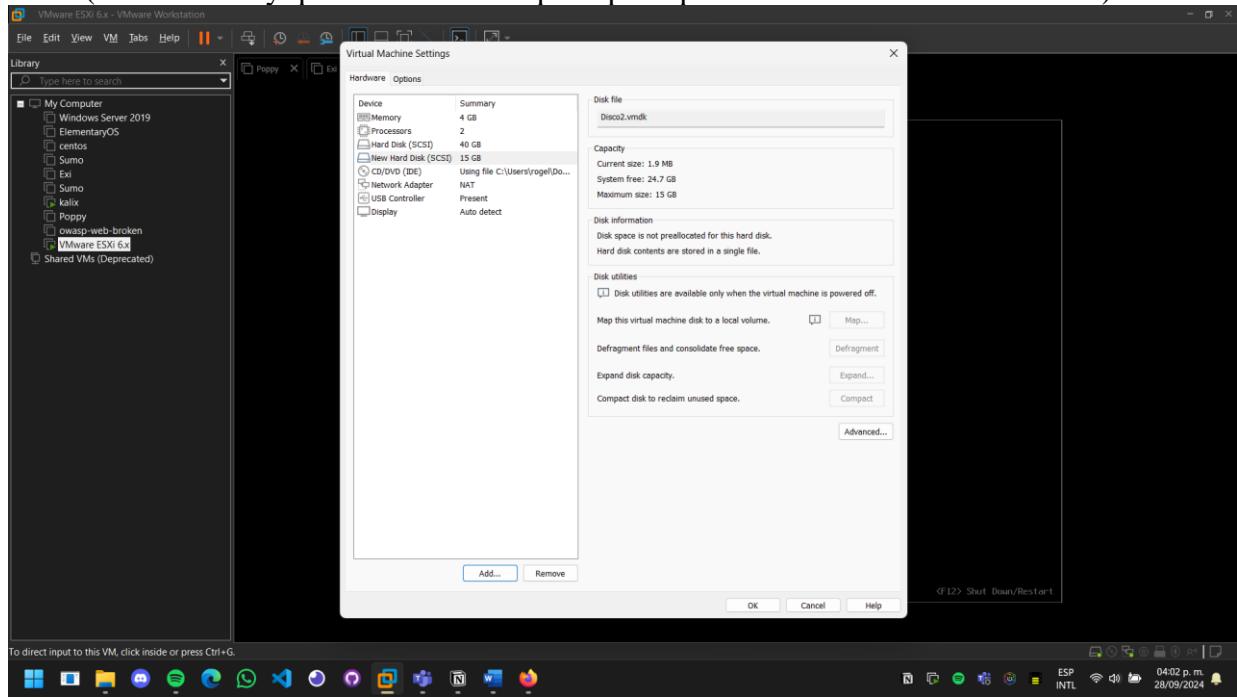
Ahora seleccionamos la cantidad de espacio para el disco nuevo y si queremos que se genere un único archivo o múltiples, en este caso prefiero que sea solo un único archivo.



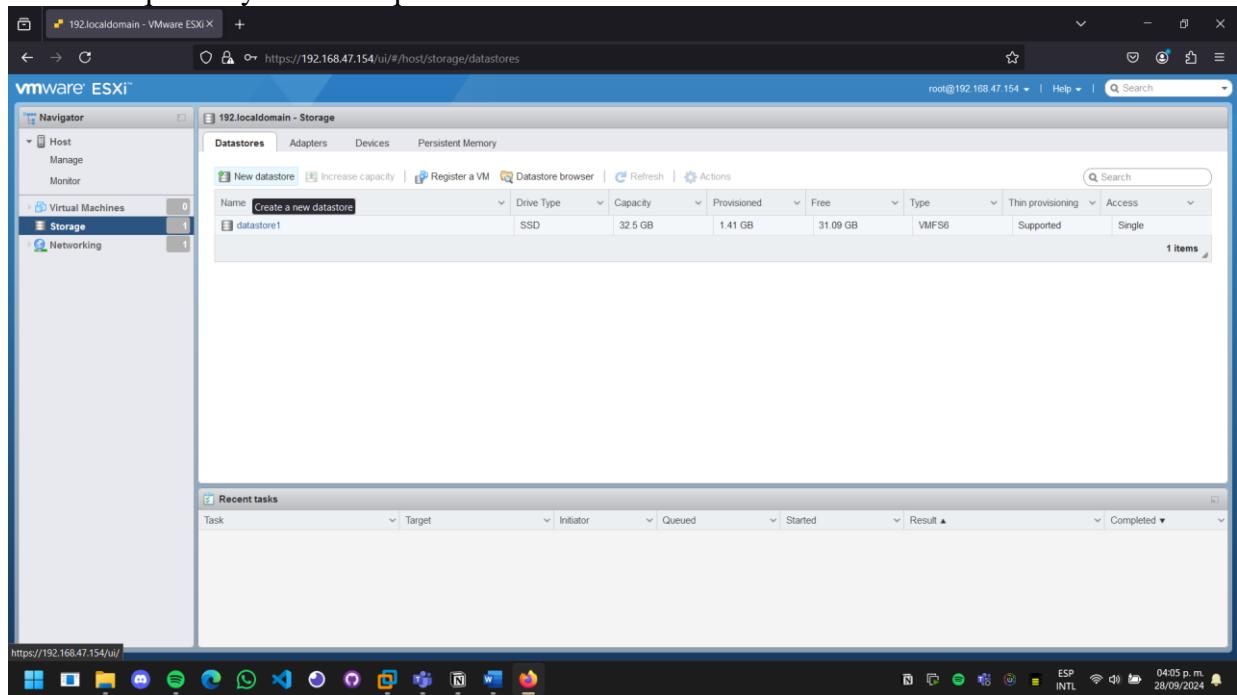
Colocamos nombre al nuevo disco



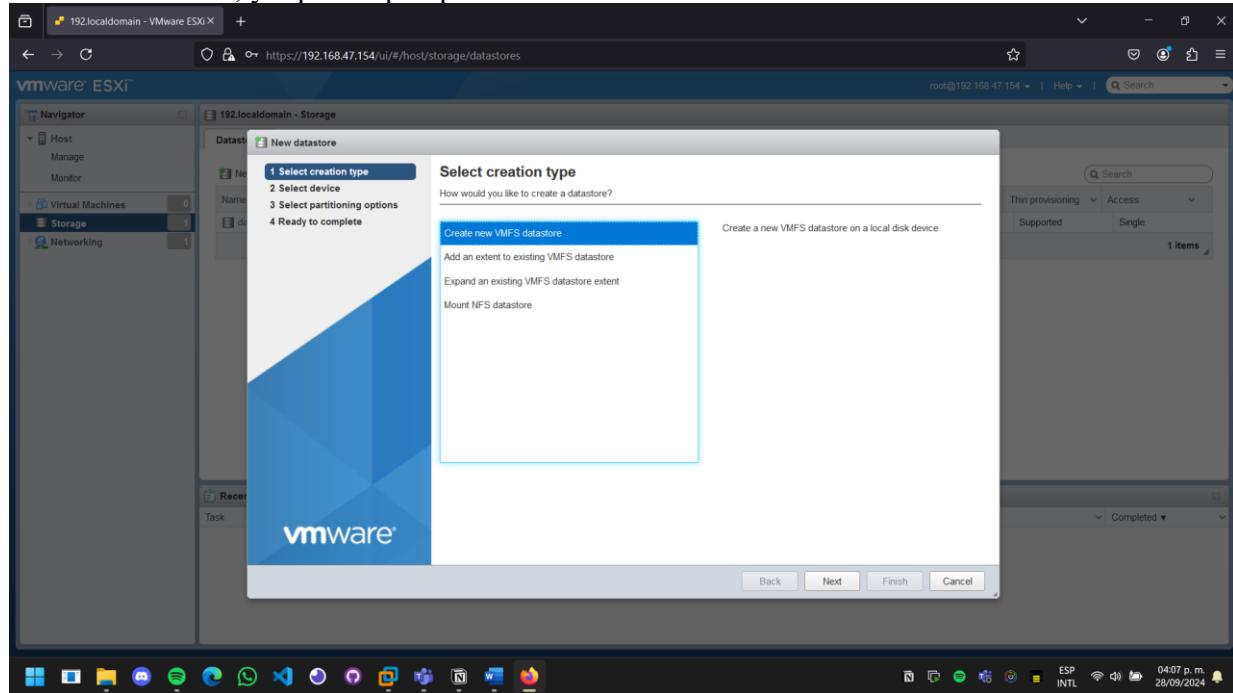
De esta forma nos aparecerá como si físicamente la máquina virtual tuviera conectado otro disco (ahora solo hay que reiniciar la máquina para que detecte el nuevo disco creado)



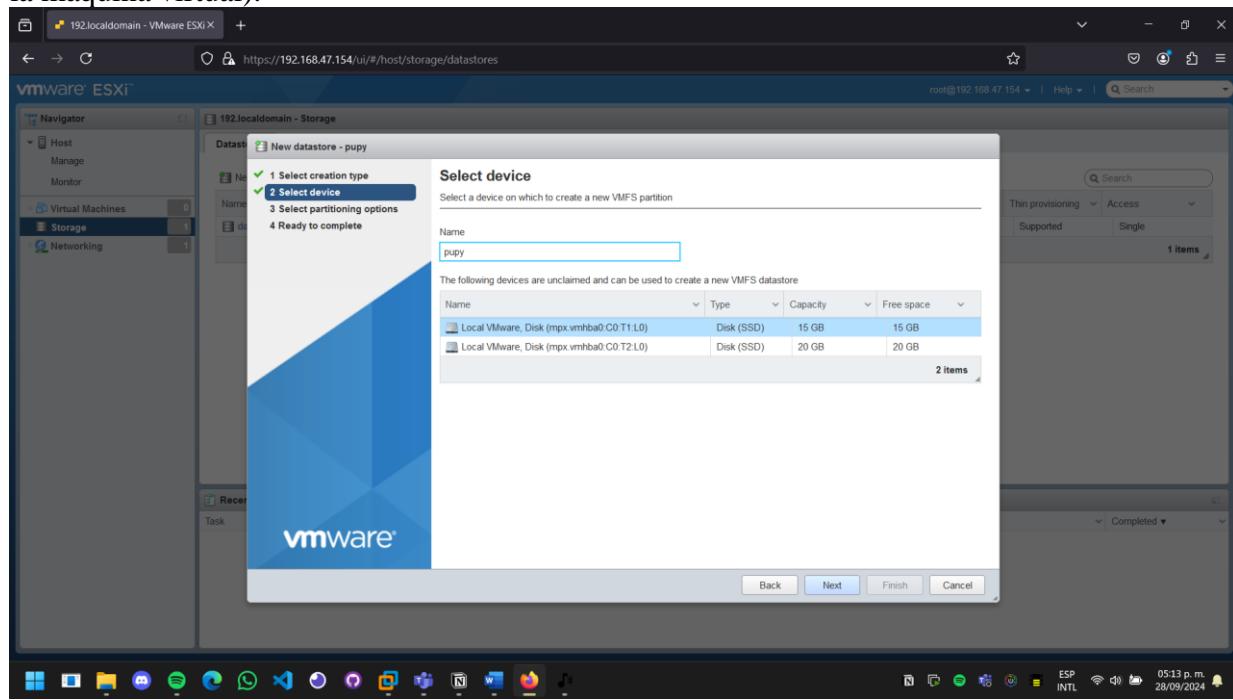
Ahora dentro del gestor de ESXi (el cual podemos acceder a través de la dirección que nos muestra nuestra máquina virtual con las credenciales del root), vamos al apartado de Storage en la barra izquierda y una vez aquí dentro le damos a “New datastore”



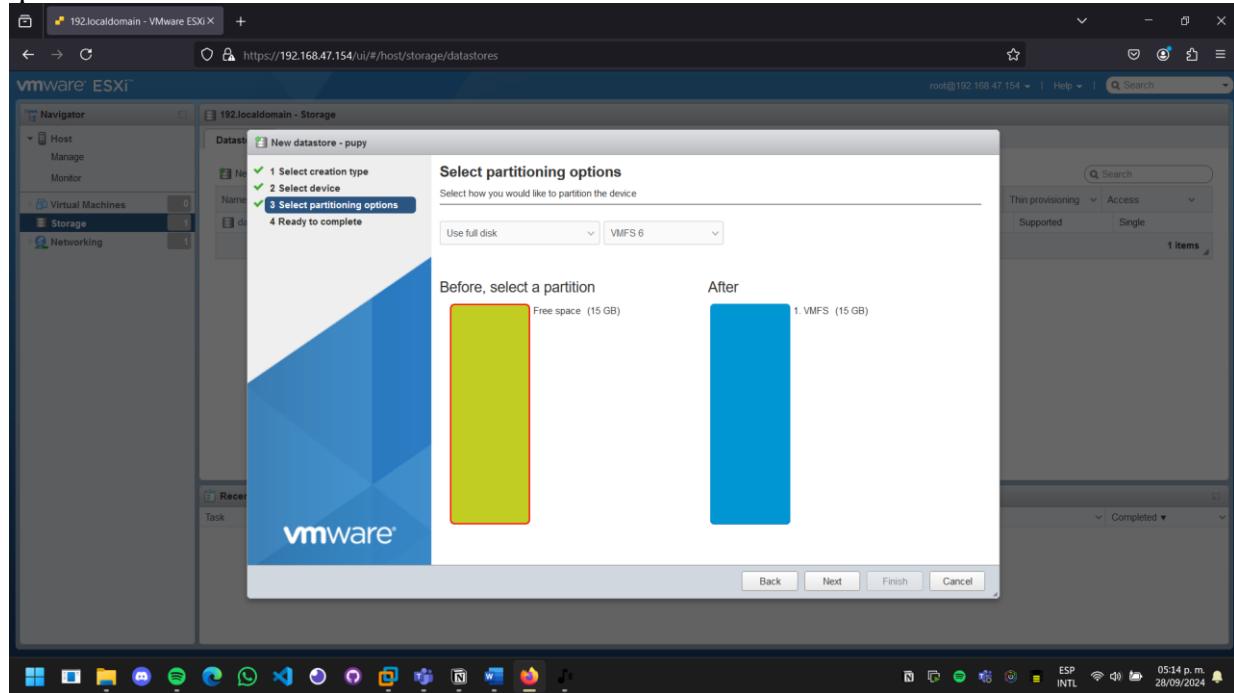
Ahora nos aparecerán las opciones para el datastore, en este caso seleccionamos “Create new VMFS datastore”, ya que lo que queremos es crear un datastore nuevo.



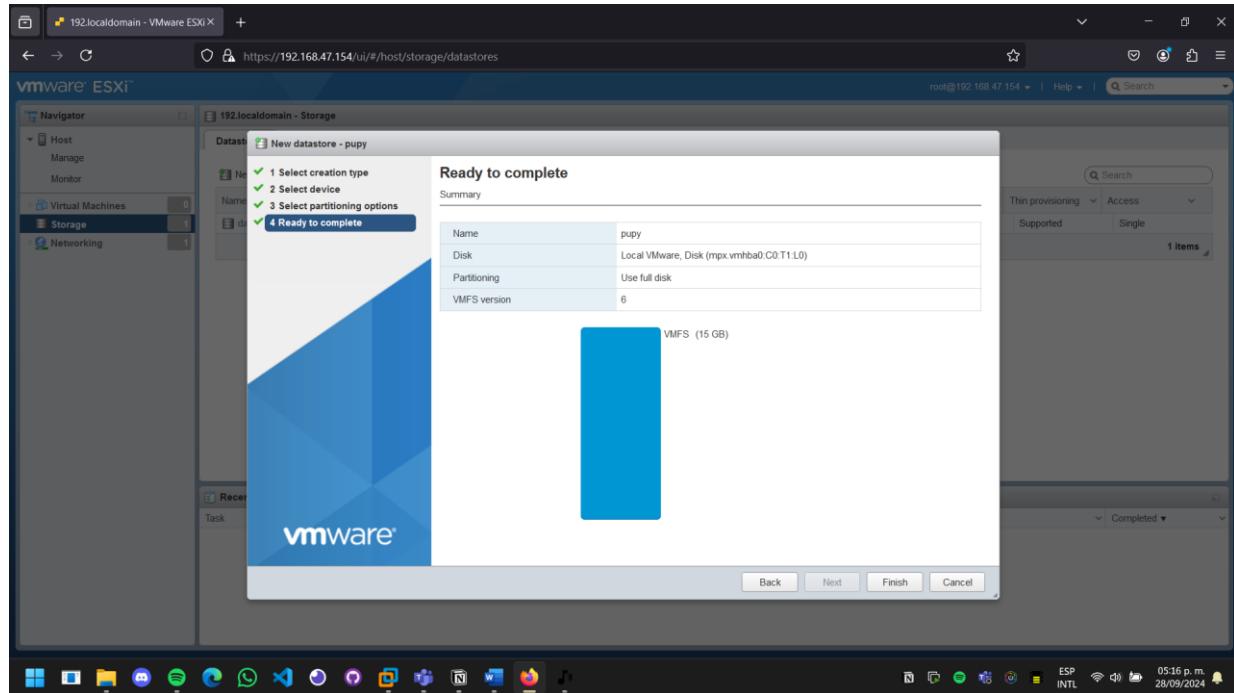
Elegimos un nombre para el disco y seleccionamos el disco (en caso de tener varios discos en la máquina virtual).



En las opciones de partición, seleccionamos que ocupe todo el disco y usamos la VMFS6 ya que nuestro ESXi es versión 6.



Para finalizar solo verificamos la información.



Ahora ya solo añadimos los discos que necesitemos y con todo esto hecho tendremos listos los almacenamientos para los sistemas operativos que vamos a montar,

Name	Drive Type	Capacity	Provisioned	Free	Type	Thin provisioning	Access
datastore1	SSD	32.5 GB	1.41 GB	31.09 GB	VMFS6	Supported	Single
pupy	SSD	14.75 GB	1.41 GB	13.34 GB	VMFS6	Supported	Single
user	SSD	19.75 GB	1.41 GB	18.34 GB	VMFS6	Supported	Single

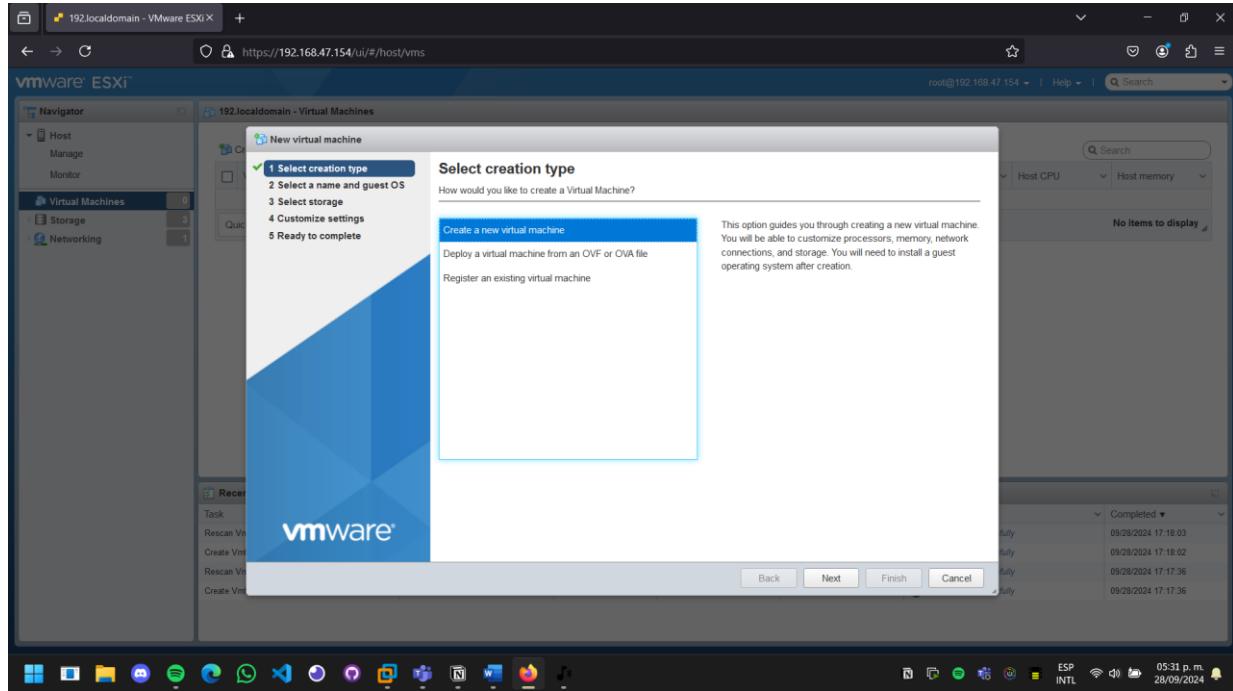
Task	Target	Initiator	Queued	Started	Result	Completed
Rescan Vmfs	192.localdomain	root	09/28/2024 17:18:02	09/28/2024 17:18:02	Completed successfully	09/28/2024 17:18:03
Create Vmfs Datastore	192.localdomain	root	09/28/2024 17:18:02	09/28/2024 17:18:02	Completed successfully	09/28/2024 17:18:02
Rescan Vmfs	192.localdomain	root	09/28/2024 17:17:36	09/28/2024 17:17:36	Completed successfully	09/28/2024 17:17:36
Create Vmfs Datastore	192.localdomain	root	09/28/2024 17:17:36	09/28/2024 17:17:36	Completed successfully	09/28/2024 17:17:36

## Máquinas virtuales en VMware ESXi

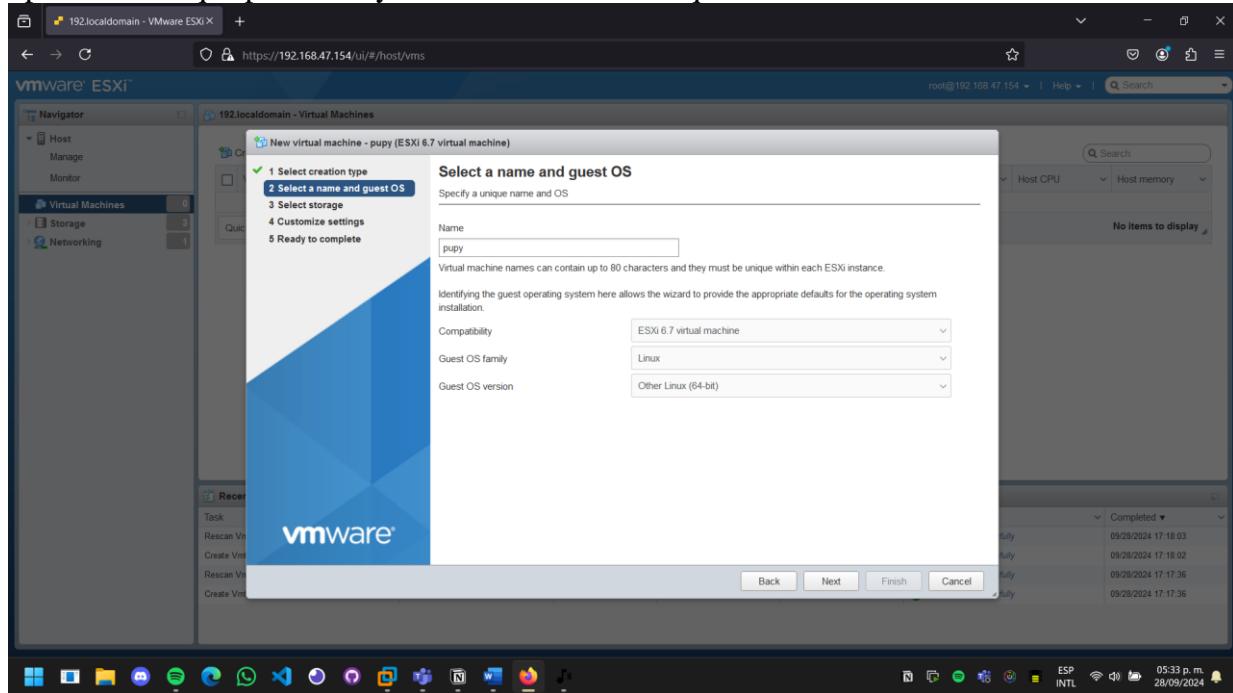
Para la creación de máquinas virtuales en nuestro servidor ESXi, lo primero es, dentro del apartado de “Virtual Machines” que aparece en la parte izquierda del gestor, nos dirigimos ahí y le damos en “Create / Register VM”.

Task	Target	Initiator	Queued	Started	Result	Completed
Rescan Vmfs	192.localdomain	root	09/28/2024 17:18:02	09/28/2024 17:18:02	Completed successfully	09/28/2024 17:18:03
Create Vmfs Datastore	192.localdomain	root	09/28/2024 17:18:02	09/28/2024 17:18:02	Completed successfully	09/28/2024 17:18:02
Rescan Vmfs	192.localdomain	root	09/28/2024 17:17:36	09/28/2024 17:17:36	Completed successfully	09/28/2024 17:17:36
Create Vmfs Datastore	192.localdomain	root	09/28/2024 17:17:36	09/28/2024 17:17:36	Completed successfully	09/28/2024 17:17:36

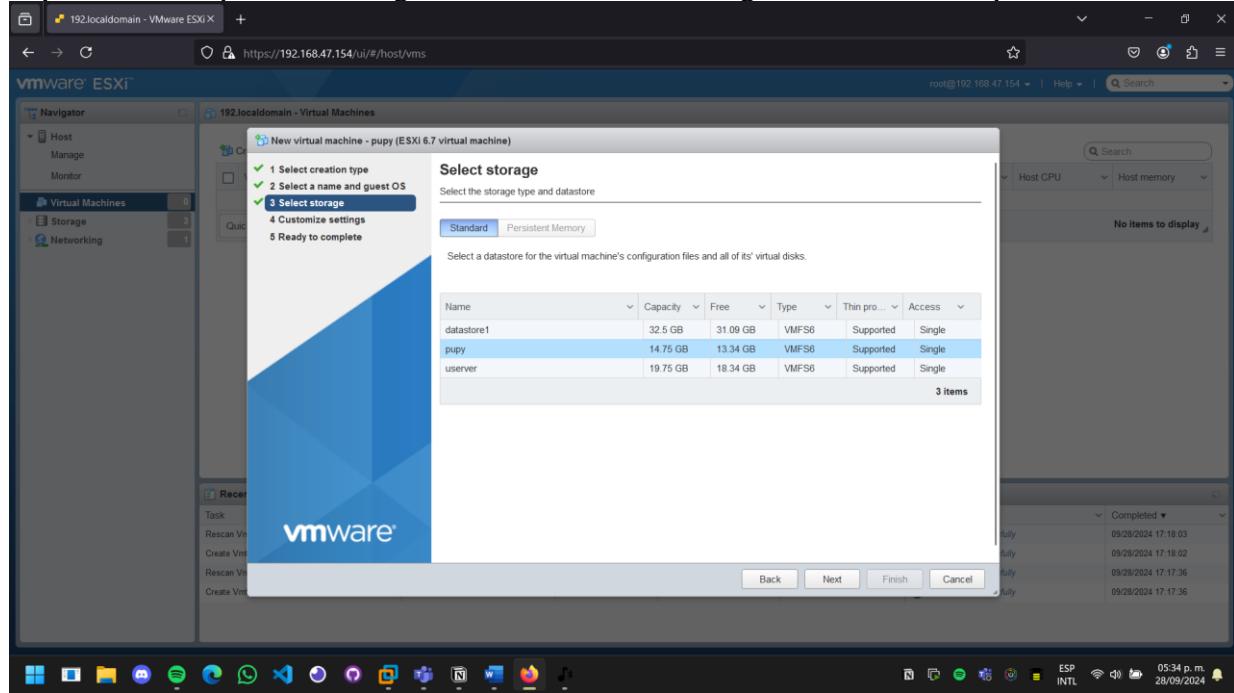
Ahora seleccionamos la primera opción, ya que contamos con el iso de la máquina que vamos a crear.



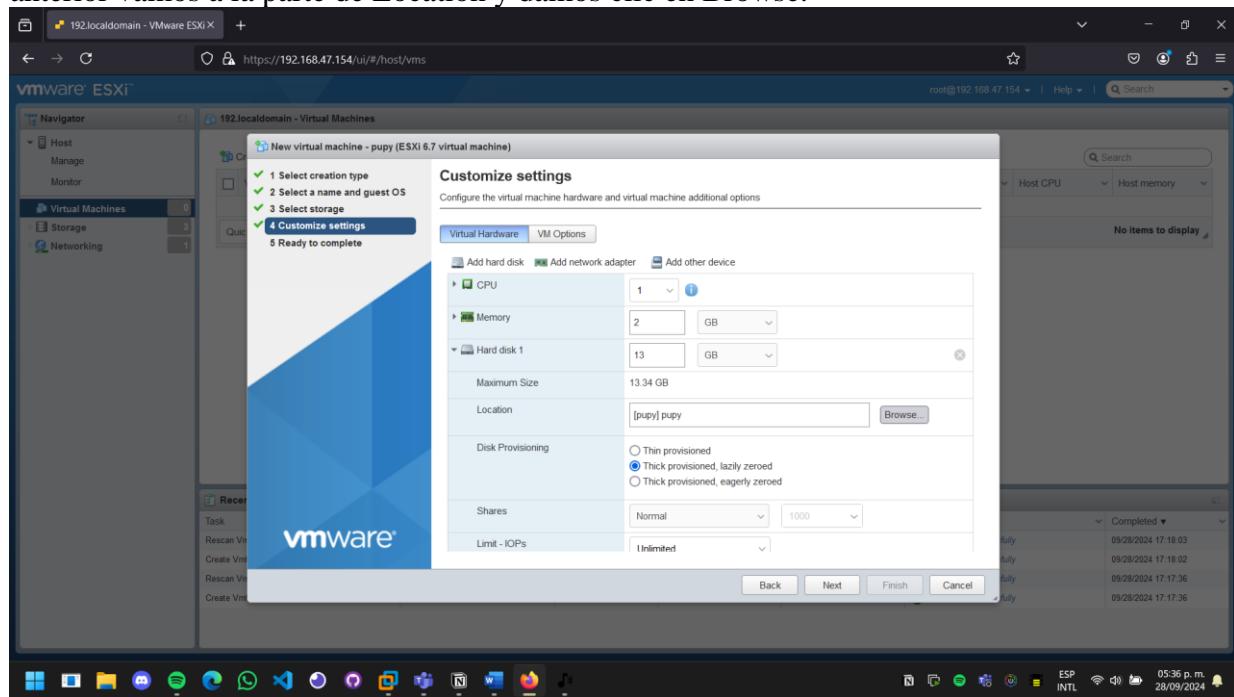
Ahora colocamos el nombre de la máquina, así como su compatibilidad, la familia de sistema operativo a la que pertenece y la versión del sistema que vamos a instalar.



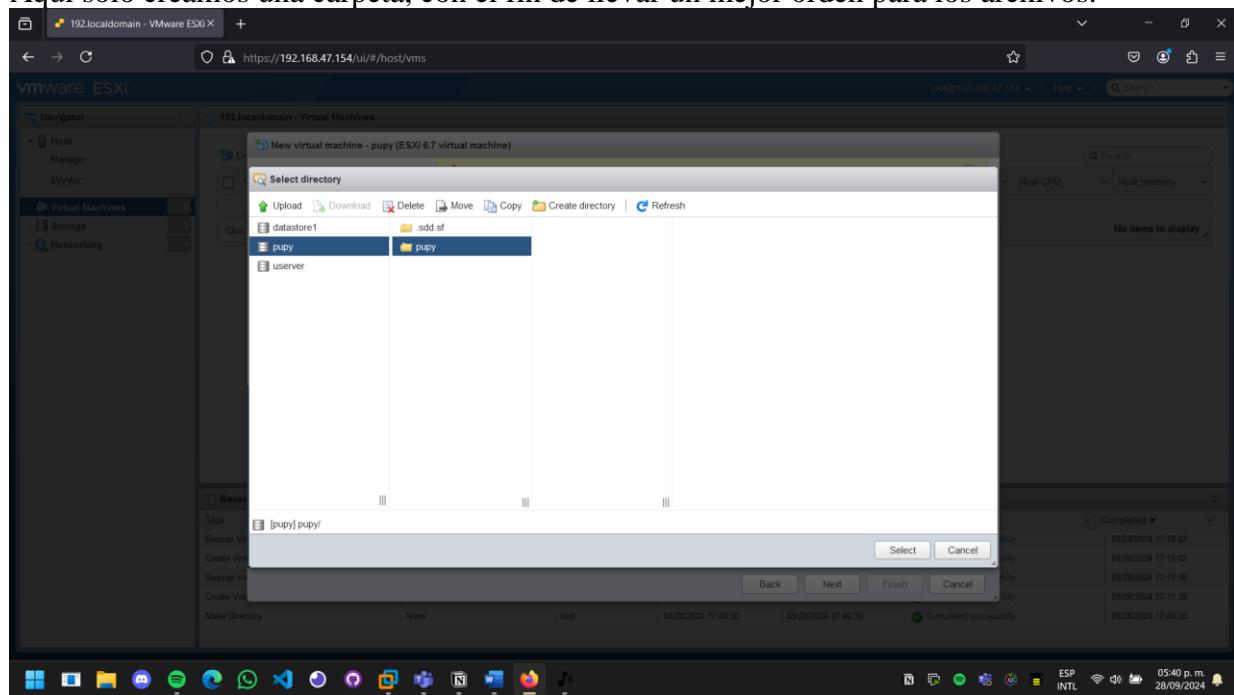
Aquí nos da la opción de escoger el disco duro en donde guardaremos la máquina virtual.



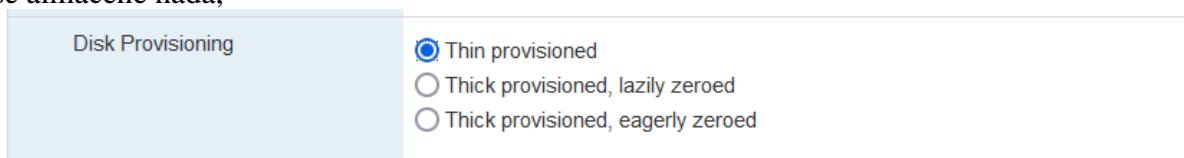
A continuación, nos aparecerá las opciones para los núcleos del CPU, cantidad de memoria RAM, cantidad de espacio para el disco, controlador de disco, etc. Luego de seleccionar lo anterior vamos a la parte de Location y damos clic en Browse.



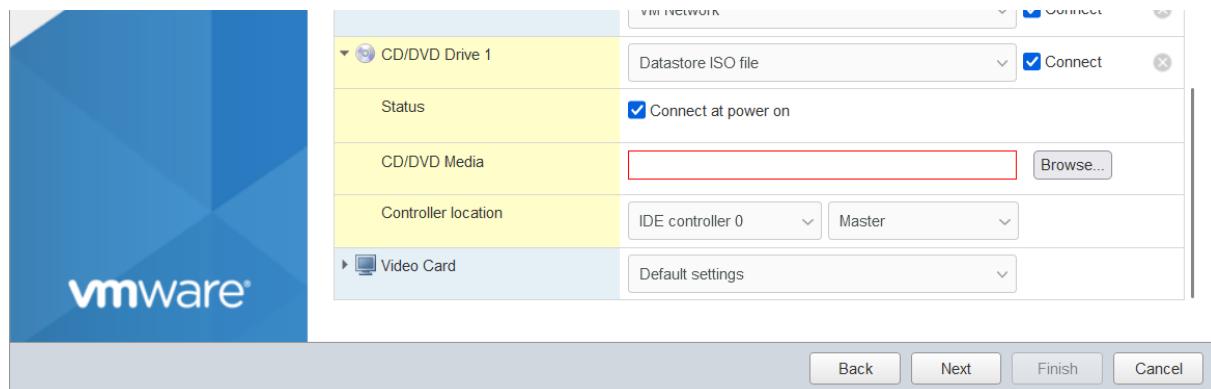
Aquí solo creamos una carpeta, con el fin de llevar un mejor orden para los archivos.



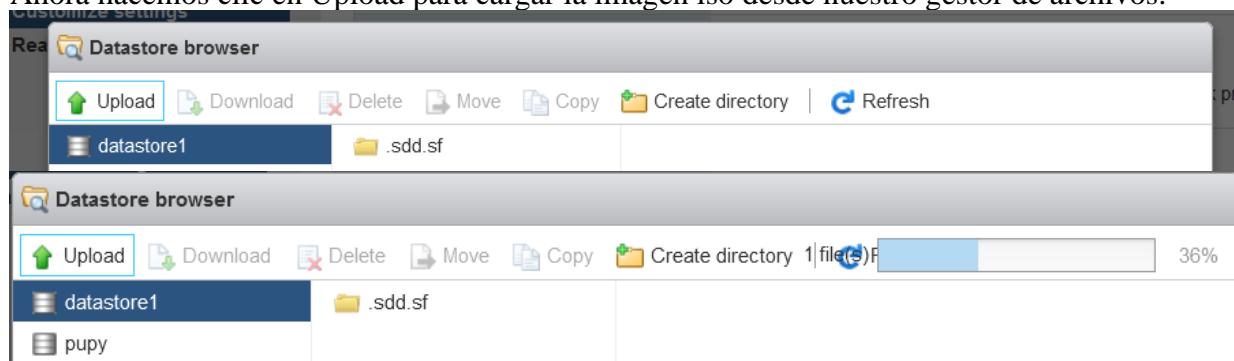
Importante, seleccionar el modo “Thin provisioned”, para que se vaya ocupando a medida que se necesite el espacio en disco, ya que de otra forma se tomara el espacio del disco, aunque no se almacene nada,



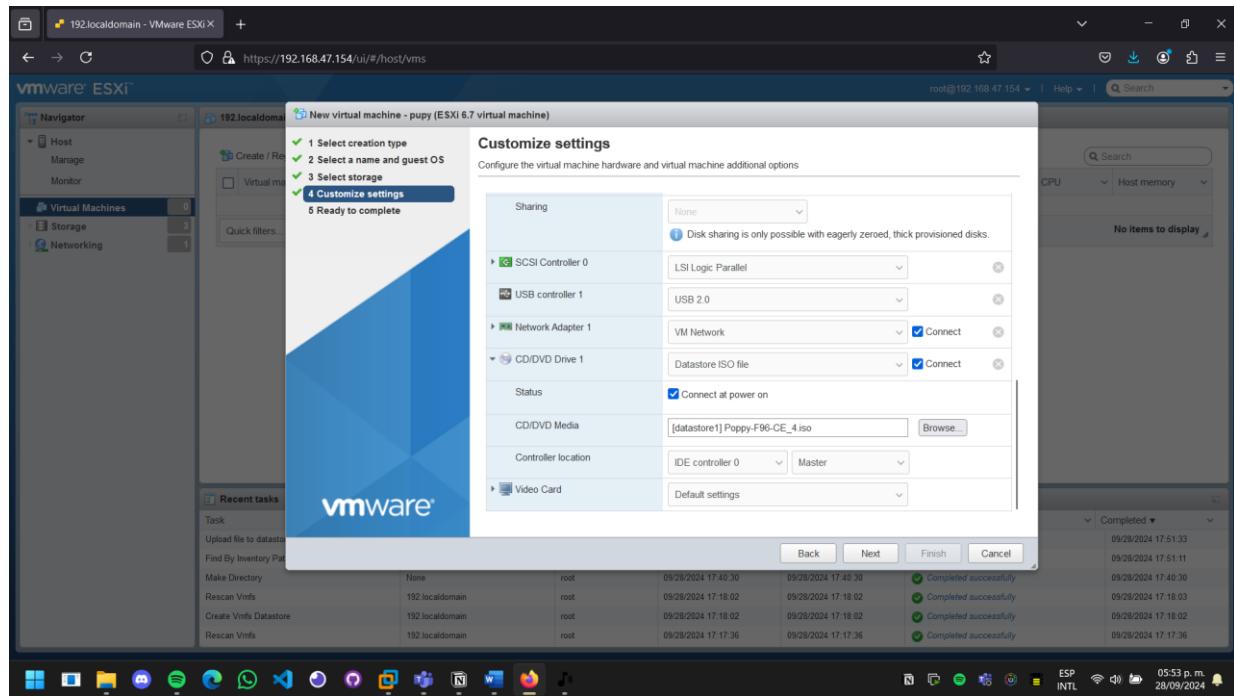
Ahora en el apartado de “CD/DVD Drive 1”, aquí cambiamos a la opción de “Datastore ISO File”, para poder cargar el iso de nuestro sistema operativo para esta nueva máquina virtual.



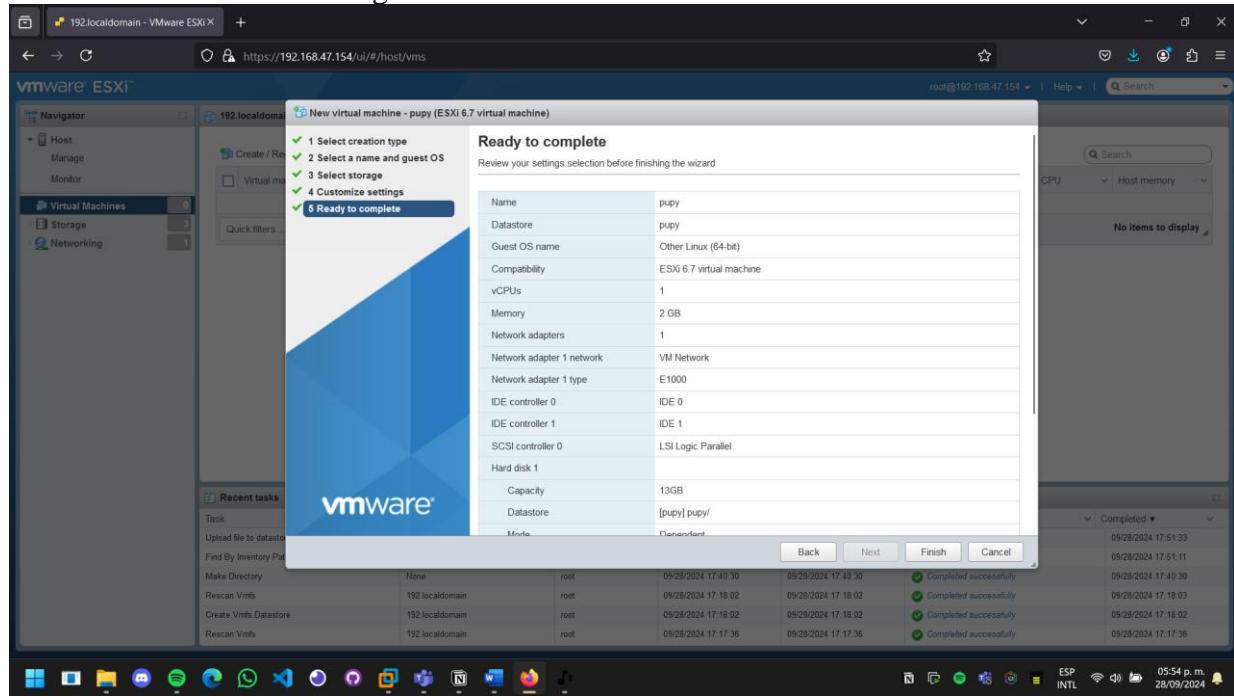
Ahora hacemos clic en Upload para cargar la imagen iso desde nuestro gestor de archivos.



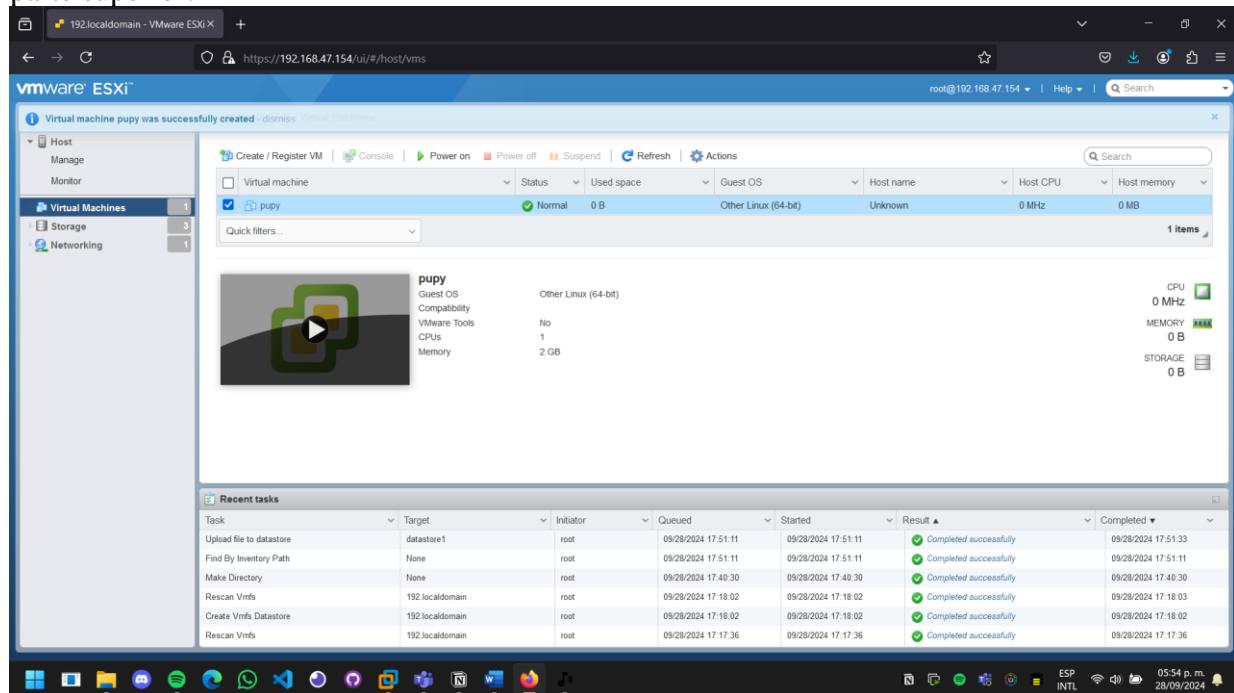
Una vez haya terminado de cargar le damos en Select (tiene que estar seleccionada).



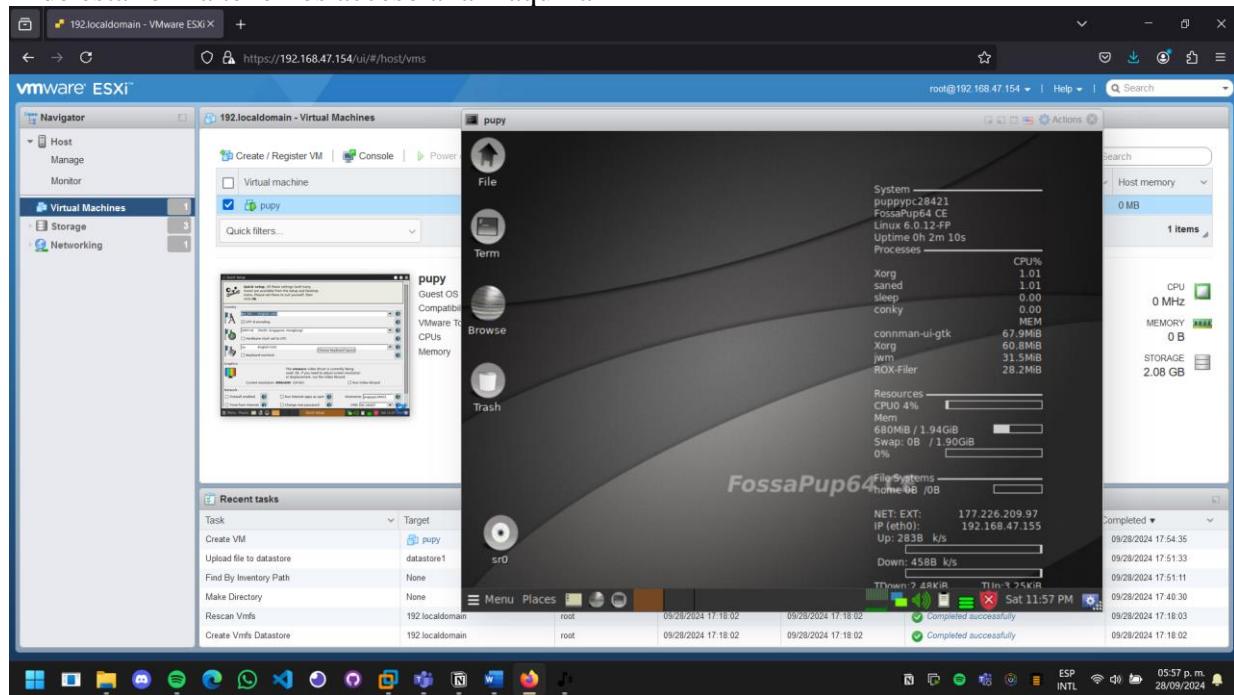
Ya solo verificamos la configuración antes de finalizar.



Listo, ya tendríamos lista la máquina para iniciarla con el botón de “Power on” que está en la parte superior.



Y de esta forma tenemos acceso a la maquina



## Clonación de Máquinas virtuales

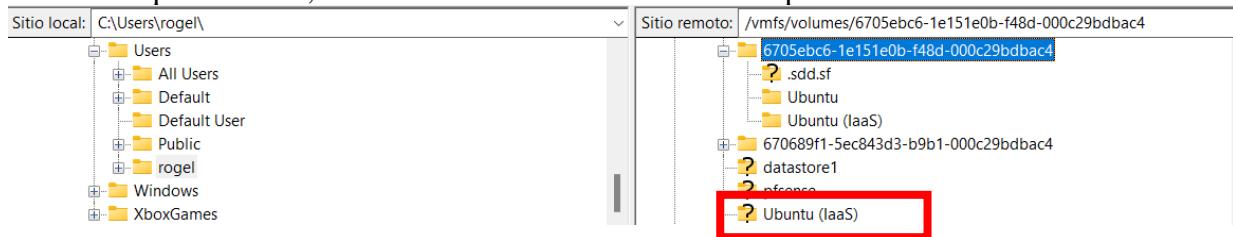
1. Lo primero es establecer una sesión SSH, yo lo hare desde FileZilla.

Nombre de archivo	Tamaño ...	Tipo de archivo	Última modif...
..			
.android		Carpeta de arc...	27/07/2024 09...
.arduinoIDE		Carpeta de arc...	31/05/2024 12...
.cache		Carpeta de arc...	11/05/2024 02...
.codetogether		Carpeta de arc...	27/06/2024 01...
.dia		Carpeta de arc...	21/02/2024 09...
.m2		Carpeta de arc...	17/03/2024 01...
.mputils		Carpeta de arc...	01/07/2024 02...
.ms-ad		Carpeta de arc...	04/02/2024 05...
.nbi		Carpeta de arc...	17/03/2024 01...
.openjfx		Carpeta de arc...	25/07/2024 04...

18 archivos y 52 directorios. Tamaño total: 30,078,457 bytes

Servidor/Archivo local	Direc...	Archivo remoto	Tamaño	Priori...	Estado
------------------------	----------	----------------	--------	-----------	--------

- Ahora ubicamos la carpeta con el nombre del disco en el que tenemos instalada la máquina virtual, al darle clic nos indica cual es la carpeta.



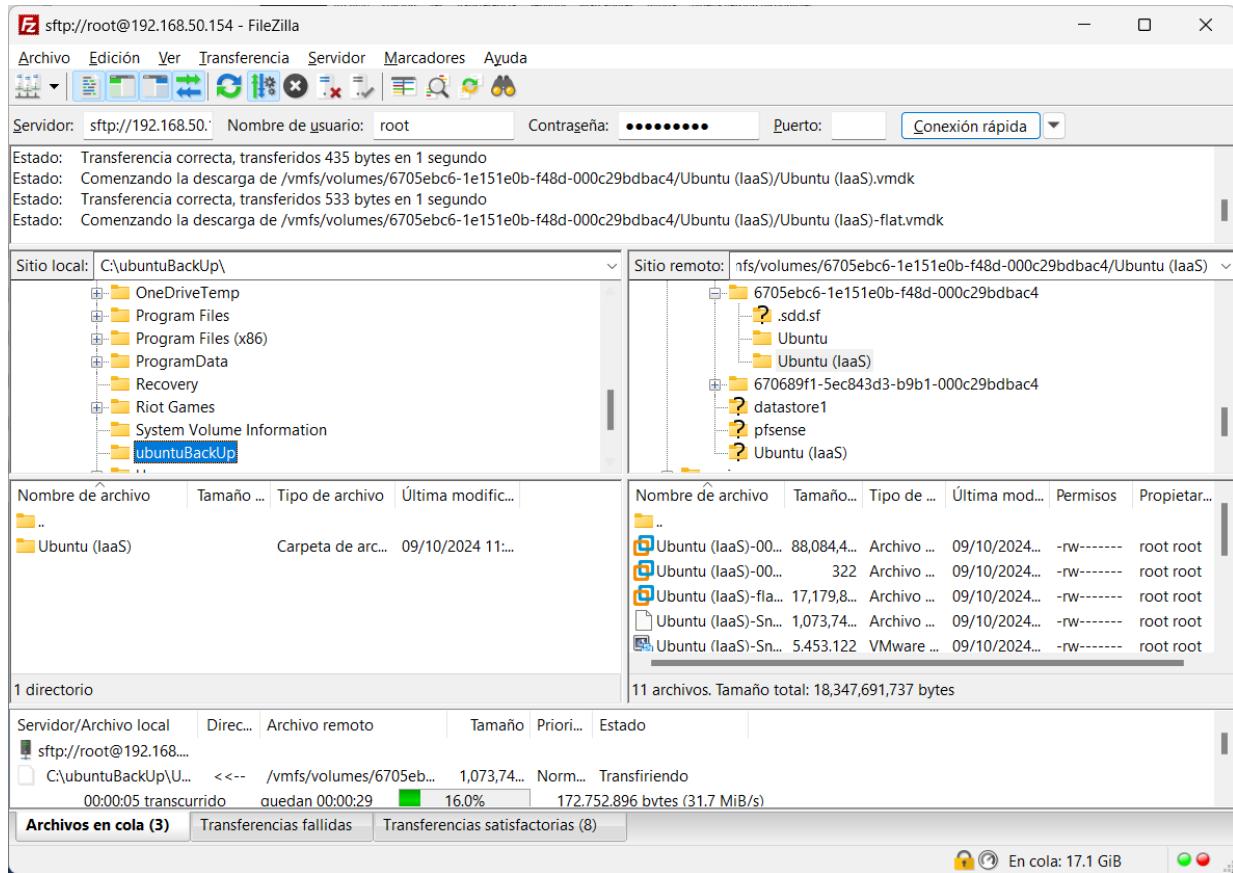
- Y aquí se encuentra la carpeta que nos interesa (con el nombre de la máquina virtual que queremos clonar).

Nombre de archivo	Tamaño...	Tipo de ...	Última mod...	Permisos	Propietar...
..					
Ubuntu (IaaS)-00...	88,084,4...	Archivo ...	09/10/2024...	-rw-----	root root
Ubuntu (IaaS)-00...	322	Archivo ...	09/10/2024...	-rw-----	root root
Ubuntu (IaaS)-fla...	17,179,8...	Archivo ...	09/10/2024...	-rw-----	root root
Ubuntu (IaaS)-Sn...	1,073,74...	Archivo ...	09/10/2024...	-rw-----	root root
Ubuntu (IaaS)-Sn...	5.453.122	VMware ...	09/10/2024...	-rw-----	root root

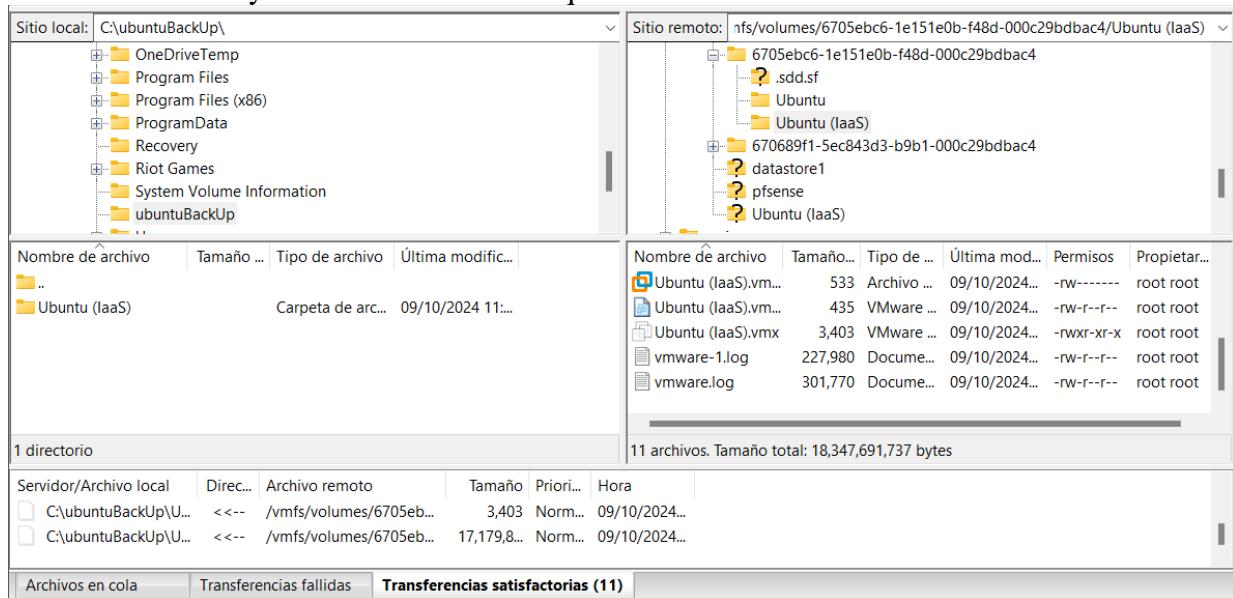
- Se recomienda que el equipo a clonar este apagado (ya que cuando esta encendida genera archivos temporales).



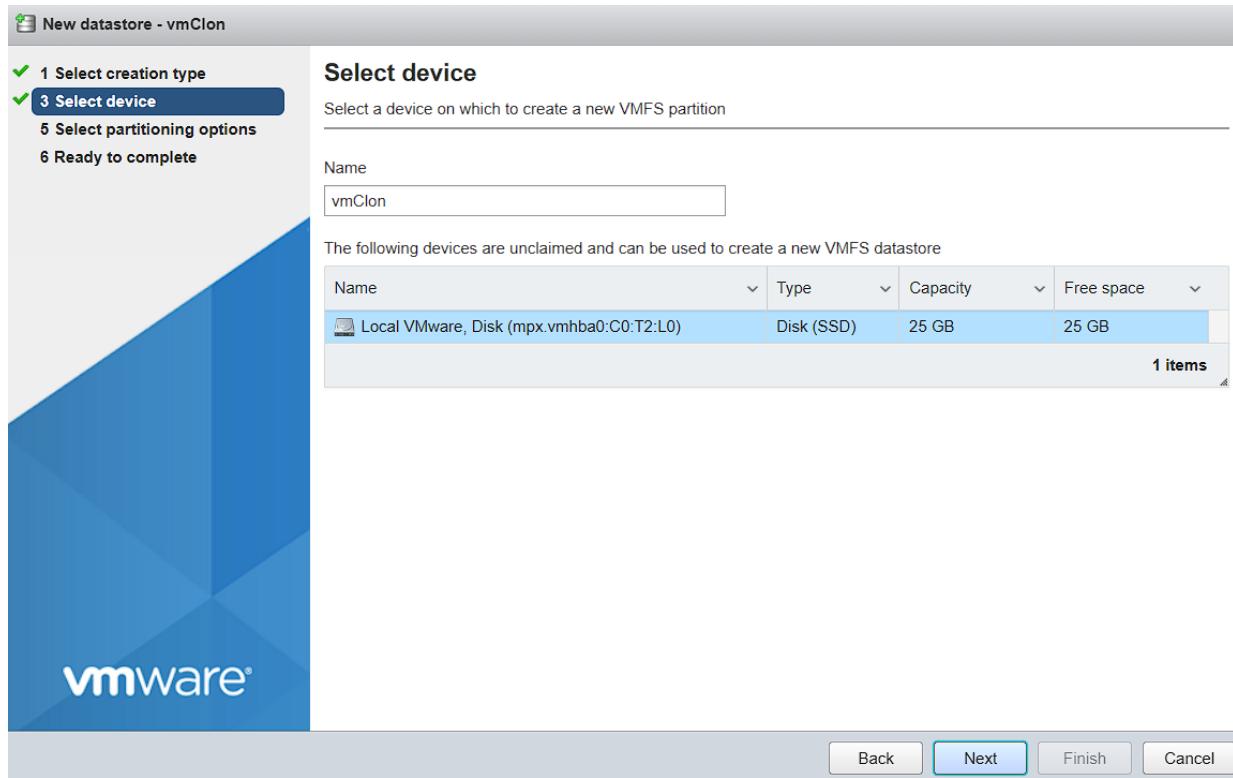
2. Ahora movemos la carpeta de la maquina a un directorio en nuestro disco local.



- Una vez haya terminado checamos que la transferencia se satisfactoria.



3. Creamos un nuevo disco para la maquina clonada.



4. Ahora creamos una nueva máquina virtual.



- Una vez creada la nueva máquina virtual nos iremos al directorio donde se encuentran los discos de la máquina origen (VMOrigen) y copiamos sus discos duros (ficheros .vmdk) al directorio de la nueva máquina virtual que hemos creado (VMClonada).

## Usuarios y permisos en ESXi

Para agregar un nuevo usuario vamos al apartado del host, en Manage > Security & users

User Name	Description
root	Administrator

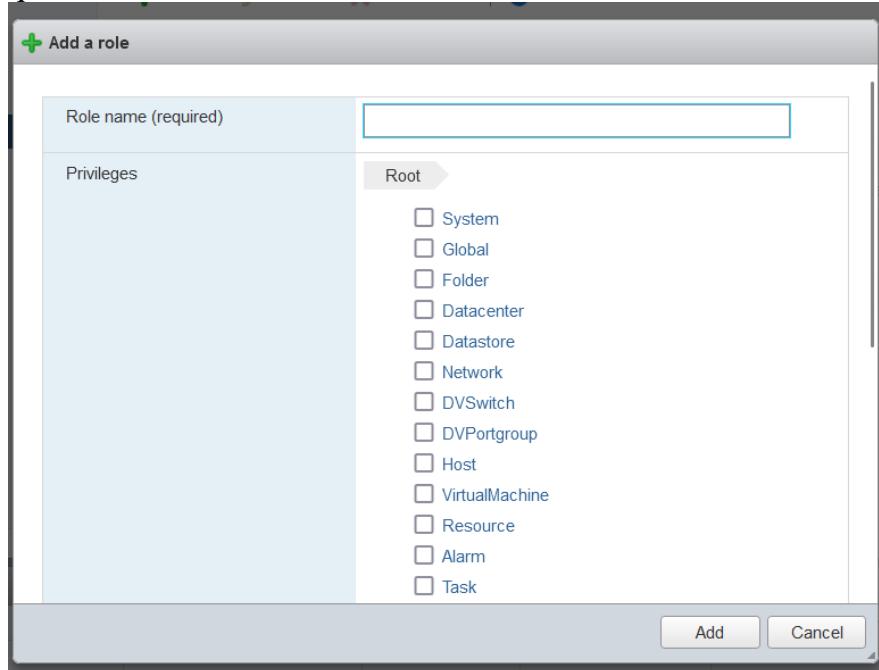
Luego en añadir usuario

User name (required)	iaas
Description	Usuario de ubuntu iaas
Password (required)	*****
Confirm password (required)	*****

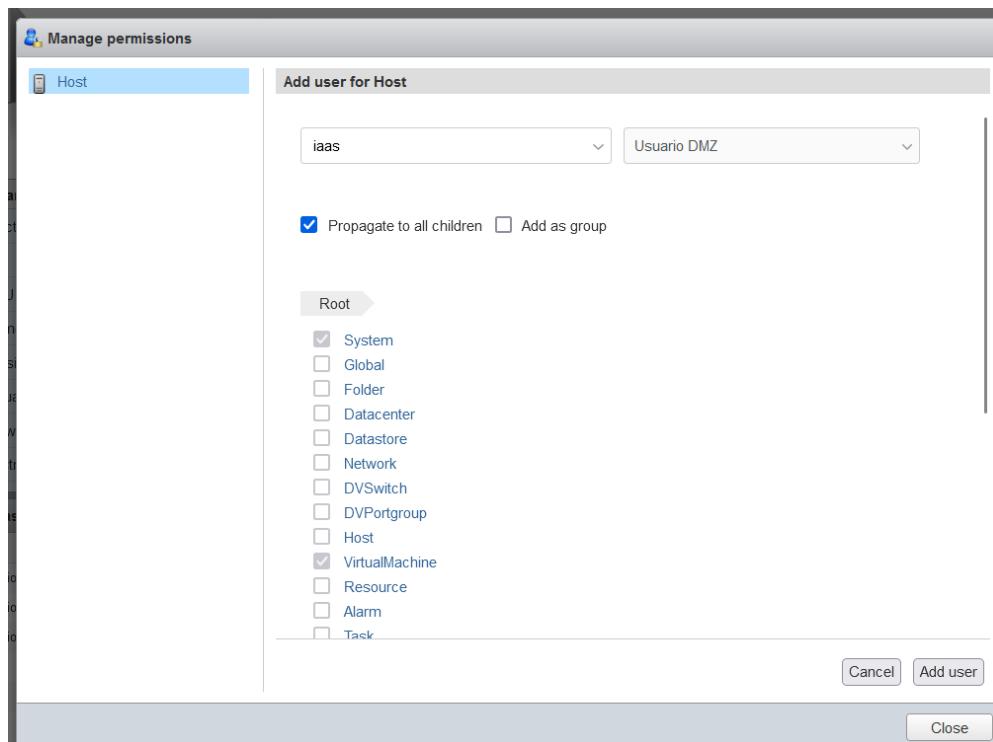
Y así agregamos los usuarios que necesitemos

User Name	Description
root	Administrator
iaas	Usuario de ubuntu iaas
paas	Usuario Ubuntu raas
saas	Usuario de ubuntu saas
uLAN	Usuario de LAN
SysAdmin	Administrador de infrestuctura

Para definir un rol solo hay que escribir el nombre del rol y seleccionar los privilegios que le queremos dar.



Una vez hecho lo anterior vamos a Host > Actions > Permissions, aquí podemos seleccionar el usuario y asignarle roles.



Y así es como podemos tener usuarios con roles asignados en ESXi

The screenshot shows the 'Manage permissions' interface for a Host. The main title is 'Assign users and roles for Host'. Below it are buttons for 'Add user', 'Remove user', and 'Assign role'. A table lists six users and their assigned roles:

User	Role
dcui	Administrator
iaas	Usuario DMZ
root	Administrator
SysAdmin	SysAdmin
uLAN	Usuario LAN
vpxuser	Administrator

At the bottom right of the table, it says '6 items'.

Para asignar el usuario solo ciertas máquinas virtuales, primero vamos a la maquina virtual que nos interese, vamos a Actions > Permissions

The screenshot shows the vSphere Web Client interface for a VM named 'Ubuntu (IaaS)'. The left sidebar shows the navigation tree with 'Virtual Machines' selected. The main pane displays the VM's configuration, including its guest OS as 'Ubuntu Linux (64-bit)', compatibility as 'ESXi 6.7 virtual machine', and resource allocation (1 CPU, 1 GB memory). The 'Actions' menu is open, and the 'Permissions' option is highlighted. The 'Recent tasks' panel at the bottom shows several completed tasks related to the VM.

Luego en Add User

The screenshot shows a 'Manage permissions' interface for 'Ubuntu (IaaS)'. On the left, there's a sidebar with a tree view showing 'Ubuntu (IaaS)' expanded. The main area is titled 'Assign users and roles for Ubuntu (IaaS)'. It contains a table with two columns: 'User' and 'Role'. Below the table, a message says 'No users'. At the bottom right, it says 'No items to display'.

Aquí podemos seleccionar nuestro usuario y rol.

The screenshot shows a 'Manage permissions' interface for 'Ubuntu (IaaS)'. On the left, there's a sidebar with a tree view showing 'Ubuntu (IaaS)' expanded. The main area is titled 'Add user for Ubuntu (IaaS)'. It has two dropdown menus: 'User' set to 'iaas' and 'Role' set to 'Usuario DMZ'. Below these are two checkboxes: 'Propagate to all children' (checked) and 'Add as group' (unchecked). A tree view under 'Root' shows several options, with 'System' and 'VirtualMachine' checked. At the bottom, there are 'Cancel', 'Add user', and 'Close' buttons.

De esta forma logramos tener un usuario para que acceda a esta maquina

The screenshot shows a web-based management interface titled 'Manage permissions'. On the left, there's a sidebar with a 'Ubuntu (IaaS)' entry. The main area is titled 'Assign users and roles for Ubuntu (IaaS)'. It includes buttons for 'Add user', 'Remove user', and 'Assign role'. A table lists a single user assignment: 'iaas' under 'User' and 'Usuario DMZ' under 'Role'. At the bottom right of the table, there's a link '1 items'.

User	Role
iaas	Usuario DMZ

Ahora iniciamos sesión en el cliente web de esxi de nuevo:

Y listo estamos dentro como el usuario que creamos y con los privilegios que le hemos dado.

## Usuarios en Ubuntu

### Paso 1: Crear el Usuario

1. Abre la terminal y ejecuta el siguiente comando para crear un nuevo usuario (reemplaza nombre\_usuario por el nombre deseado):

```
sudo adduser nombre_usuario
```

- Nos pedirá que ingreses una contraseña para el usuario y algunos detalles adicionales (que puedes dejar en blanco si no son necesarios).

```
upaas@upaas:~$ sudo adduser developer
[sudo] password for upaas:
Adding user `developer' ...
Adding new group `developer' (1001) ...
Adding new user `developer' (1001) with group `developer' ...
Creating home directory `/home/developer' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for developer
Enter the new value, or press ENTER for the default
      Full Name []: dEvEl0pEr rAmIrEz
      Room Number []: 11
      Work Phone []: 4400000000
      Home Phone []:
      Other []:
Is the information correct? [Y/n] Y
upaas@upaas:~$
```

2. Crea la carpeta a la que deseas restringir el acceso del usuario:

```
sudo mkdir /ruta/a/la/carpeta
```

- En este caso le voy a crear su carpeta en la carpeta de apache

```
upaas@upaas:/var/www/html$ sudo mkdir dev
upaas@upaas:/var/www/html$ ll
total 28
drwxr-xr-x 3 root root 4096 oct 15 17:06 .
drwxr-xr-x 3 root root 4096 oct 10 17:48 ..
drwxr-xr-x 2 root root 4096 oct 15 17:06 dev/
-rw-r--r-- 1 root root 10657 oct 15 16:56 index.html
-rw-r--r-- 1 root root    20 oct 10 18:25 info.php
```

3. Cambia el propietario de la carpeta al usuario creado:

```
sudo chown nombre_usuario:nombre_usuario /ruta/a/la/carpeta
```

```
upaas@upaas:/var/www/html$ sudo chown developer:developer /dev/
upaas@upaas:/var/www/html$ _
```

4. Configura los permisos de la carpeta para que el usuario pueda leer, escribir y ejecutar en ella:

```
sudo chmod 755 /var/www/html/carpeta_usuario
```

```
upaas@upaas:/var/www/html$ sudo chmod 755 /dev/
```

5. que el usuario solo tenga acceso a esta carpeta y no a otras partes del sistema, puedes usar chroot para crear un entorno limitado, o simplemente puedes ajustar el acceso a través de sftp.

- Edita el archivo de configuración de sshd:

```
sudo nano /etc/ssh/sshd_config
```

- Agrega las siguientes líneas al final del archivo para limitar el acceso:

```
Match User nombre_usuario
  ChrootDirectory /var/www/html/carpeta_usuario
  ForceCommand internal-sftp
  AllowTcpForwarding no
```

```
# Example of overriding settings on a per-user basis
#Match User anoncvs
#    X11Forwarding no
#    AllowTcpForwarding no
#    PermitTTY no
#    ForceCommand cvs server

Match User developer
    ChrootDirectory /var/www/html/dev
    ForceCommand internal-sftp
    AllowTcpForwarding no
```

- Asegúrate de que el ChrootDirectory sea propiedad de root:

```
sudo chown root:root /var/www/html
```

- Reinicia el servicio SSH:

```
sudo systemctl restart ssh
```

## Red

### Firewall ESXi

Primero abrimos una sesión de SSH a nuestra maquina ESXi, en mi caso usare el programa PuTTy para hacer la conexión.

```
192.168.47.154 - PuTTY
login as: root
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
vSphere Security documentation for more information.
[root@192:~] 
```

Ahora necesitamos saber las estadísticas del firewall en el host con el siguiente comando

```
[root@192:~] esxcli network firewall get
Default Action: DROP
Enabled: true
Loaded: true
```

Como vemos el firewall esta activo y cargado. Ahora el siguiente comando es para ver las configuraciones del firewall.

```
[root@192:~] esxcli network firewall ruleset list
Name           Enabled
-----
sshServer      true
sshClient      false
nfsClient      false
nfs41Client    false
dhcp          true
dns            true
snmp          true
ntpClient      false
CIMHttpServer  true
CIMHttpsServer true
CIMSLP         true
iSCSI          false
vpxHeartbeats true
updateManager   true
faultTolerance true
webAccess      true
vMotion        true
vSphereClient  true
activeDirectoryAll false
NFC            true
HBR            true
ftpClient      false
httpClient     false
gdbserver      false
DVFilter       false
DHCPv6         true
DVSSync        true
syslog         false
WOL            true
vSPC           false
remoteSerialPort false
rdt            false
cmmds          false
rabbitmqproxy  true
ipfam          false
vvold          false
iofiltervp     true
esxupdate      false
vit            false
vsanEncryption false
pvrdma         false
vic-engine     false
vsanhealth-unicasttest false
```

El siguiente comando es para ver los detalles específicos de un ruleset.

```
[root@192:~] esxcli network firewall ruleset list --ruleset-id=iSCSI  
Name      Enabled  
-----  
iSCSI     false
```

Si queremos activar el tráfico, es con el siguiente comando.

```
[root@192:~] esxcli network firewall ruleset set --enabled=true --ruleset-id=iSCSI
```

Y como vemos se ha activado correctamente.

```
[root@192:~] esxcli network firewall ruleset list --ruleset-id=iSCSI  
Name      Enabled  
-----  
iSCSI     true
```

Para ver la lista de direcciones permitidas

```
[root@192:~] esxcli network firewall ruleset allowedip list --ruleset-id=iSCSI  
Ruleset  Allowed IP Addresses  
-----  
iSCSI    All
```

Este comando bloquea todo el tráfico iSCSI, independientemente de la dirección IP de origen. Es como cerrar por completo la puerta al tráfico iSCSI.

```
[root@192:~] esxcli network firewall ruleset set --allowed-all=false --ruleset-id=iSCSI
```

Este comando abre un agujero en el firewall para permitir el tráfico iSCSI proveniente de la red 10.0.1.2/24. Es como abrir una pequeña puerta en el muro que solo permite el paso a las personas de esa red específica.

```
[root@192:~] esxcli network firewall ruleset allowedip add --ip-address=10.0.1.2/24 --ruleset-id=iSCSI
```

Y como vemos ahora la ip 10.0.1.2 está permitida

```
[root@192:~] esxcli network firewall ruleset allowedip list --ruleset-id=iSCSI  
Ruleset  Allowed IP Addresses  
-----  
iSCSI    10.0.1.2/24
```

Este último comando es por si queremos desactivar de nuevo el tráfico

```
[root@192:~] esxcli network firewall ruleset set --enabled=false --ruleset-id=iSCSI
```

Después de que hayamos hecho los cambios necesarios al firewall, es necesario recargar el firewall para que se guarden los cambios, con el siguiente comando.

```
[root@192:~] esxcli network firewall refresh
```

## Firewall pfSense

Como primer paso es ingresar a la dirección de la interfaz gráfica de pfsense, en este caso es la 172.16.0.1, la cual accedo desde una maquina Windows que se encuentra en el mismo segmento.

Una vez dentro, vamos al apartado de Firewall>Rules.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<span style="color: red;">X</span>	0/5 KiB	*	RFC 1918 networks	*	*	*	*	*	Block private networks	<span style="color: blue;">⚙️</span>
<span style="color: red;">X</span>	0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*	Block bogon networks	<span style="color: blue;">⚙️</span>

Como vemos tenemos dos reglas creadas por defecto, la primera bloquea paquetes de cualquier protocolo que venga de cualquier red privada, la segunda bloquea paquetes que vengan de redes no asignadas por la IANA.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<span style="color: green;">✓</span>	1/496 KiB	*	*	*	LAN Address	80	*	*	Anti-Lockout Rule	<span style="color: blue;">⚙️</span>
<span style="color: green;">✓</span>	0/8.17 MiB	IPv4 *	LAN net	*	*	*	*	none	Default allow LAN to any rule	<span style="color: blue;">-trash</span> <span style="color: blue;">edit</span> <span style="color: blue;">copy</span> <span style="color: blue;">delete</span>
<span style="color: green;">✓</span>	0/0 B	IPv6 *	LAN net	*	*	*	*	none	Default allow LAN IPv6 to any rule	<span style="color: blue;">-trash</span> <span style="color: blue;">edit</span> <span style="color: blue;">copy</span> <span style="color: blue;">delete</span>

En el apartado de LAN, la primera regla que está ahí lo que hace nos da el acceso al firewall (ósea la interfaz gráfica que estamos usando). La siguiente recibe tráfico de la red LAN (172.16.0.0/24) y hacia cualquier destino, la tercera es lo mismo, pero para ipv6.

En la DMZ solo esta la regla de si se recibe trafico de redes no registradas por la IANA se van a bloquear.

Rules (Drag to Change Order)											Actions
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<span style="color: red;">X</span>	0 / 0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	

Debido a que pfSense bloquea todo, se necesita de reglas que permitan la conexión, en este caso en la DMZ no hay reglas que permitan, por eso es por lo que no tiene conexión.

Para agregar una nueva regla damos clic en Add



En la acción nos da tres opciones, Pass (permite tráfico), Block (bloquea el tráfico) y Reject (bloquea el tráfico y manda un mensaje de que bloqueo). El disable lo dejamos desactivado para que no esté desactivada la regla, en interfaz dejamos DMZ, en protocolo permitimos todo.

**Edit Firewall Rule**

Action	<input type="button" value="Block"/>
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.	
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	<input type="button" value="DMZ"/>
Choose the interface from which packets must come to match this rule.	
Address Family	<input type="button" value="IPv4"/>
Select the Internet Protocol version this rule applies to.	
Protocol	<input type="button" value="Any"/>
Choose which IP protocol this rule should match.	

Ahora seleccionamos el origen y destino, en origen marcamos el network e ingresamos la red del DMZ, y en el destino marcamos LAN net, para que tome el segmento de la LAN.

<b>Source</b>
<b>Source</b> <input type="checkbox"/> Invert match <input type="button" value="Network"/> <input type="text" value="10.0.0.0"/> / <input type="button" value="24"/>
<b>Destination</b>
<b>Destination</b> <input type="checkbox"/> Invert match <input type="button" value="LAN net"/> <input type="button" value="Destination Address"/>

Y ya solo colocamos una descripción.

Extra Options	
<b>Log</b>	<input type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the <a href="#">Status: System Logs: Settings</a> page).
<b>Description</b>	<input type="text" value="Bloquear trafico DMZ a LAN"/> <input type="button" value="X"/>
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.	
<b>Advanced Options</b>	<input type="button" value="Display Advanced"/>

## Ahora para permitir internet

Edit Firewall Rule	
<b>Action</b>	<input type="button" value="Pass"/> <input type="button" value="▼"/>
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.	
<b>Disabled</b>	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
<b>Interface</b>	<input type="button" value="DMZ"/> <input type="button" value="▼"/>
Choose the interface from which packets must come to match this rule.	
<b>Address Family</b>	<input type="button" value="IPv4"/> <input type="button" value="▼"/>
Select the Internet Protocol version this rule applies to.	
<b>Protocol</b>	<input type="button" value="Any"/> <input type="button" value="▼"/>
Choose which IP protocol this rule should match.	
Source	
<b>Source</b>	<input type="checkbox"/> Invert match <input type="button" value="DMZ net"/> <input type="button" value="▼"/> <input type="button" value="Source Address"/> / <input type="button" value="▼"/>
Destination	
<b>Destination</b>	<input type="checkbox"/> Invert match <input type="button" value="any"/> <input type="button" value="▼"/> <input type="button" value="Destination Address"/> / <input type="button" value="▼"/>
Extra Options	
<b>Log</b>	<input type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the <a href="#">Status: System Logs: Settings</a> page).
<b>Description</b>	<input type="text" value="Permitir DMZ a internet"/> <input type="button" value="X"/>
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.	
<b>Advanced Options</b>	<input type="button" value="Display Advanced"/>

De esta forma podemos crear reglas para el firewall en pfsense.

Especificación de cada punto al agregar una regla al firewall:

## 1. Action (Acción)

Este apartado determina qué debe hacer el firewall con los paquetes que coincidan con los criterios de la regla.

- **Pass:** Permite el tráfico que coincide con la regla.
- **Block:** Bloquea el tráfico. El paquete es descartado sin notificar al remitente.
- **Reject:** Bloquea el tráfico, pero notifica al remitente que la conexión ha sido rechazada (aplicable solo para TCP y UDP).

## 2. Disabled (Deshabilitado)

- **Check:** Si esta opción está marcada, la regla estará deshabilitada y no se aplicará. Es útil para desactivar temporalmente una regla sin eliminarla.

## 3. Interface (Interfaz)

Determina en qué interfaz de red se aplicará la regla.

- **DMZ:** La regla será aplicada a la interfaz de la red DMZ.
- **LAN:** Se aplica a la red local.
- **WAN:** Se aplica a la interfaz de red pública (internet).
- **OPT1, OPT2, etc.:** Se refiere a interfaces opcionales configuradas en tu pfSense.

## 4. Address Family (Familia de direcciones)

Especifica el tipo de dirección IP a la que se aplica la regla.

- **IPv4:** Aplica solo a direcciones IPv4.
- **IPv6:** Aplica solo a direcciones IPv6.
- **IPv4+IPv6:** Aplica a ambas versiones de IP.

## 5. Protocol (Protocolo)

Especifica qué protocolo debe coincidir para que la regla se aplique.

- **TCP:** Solo aplica a tráfico TCP (Transmission Control Protocol).
- **UDP:** Solo aplica a tráfico UDP (User Datagram Protocol).
- **ICMP:** Aplica a tráfico ICMP (usado para comandos como "ping").
- **TCP/UDP:** Aplica tanto a TCP como a UDP.
- **Any:** La regla se aplica a cualquier protocolo.

## 6. Source (Origen)

Este apartado define de dónde viene el tráfico que será afectado por la regla.

- **Source (IP):** Puedes especificar una dirección IP o una red (ejemplo: 10.0.0.0/24) desde donde proviene el tráfico.
- **Invert match:** Si está marcado, la regla se aplicará a todo **excepto** al rango o IP seleccionada.

Al hacer clic en "Display Advanced", puedes configurar más opciones, como:

- **Source Port Range:** Generalmente no se utiliza, ya que los puertos de origen suelen ser aleatorios, pero puedes especificarlo si tienes una necesidad específica.

## 7. Destination (Destino)

Define el destino del tráfico que será afectado por la regla.

- **Destination (IP):** Puedes especificar la dirección IP o rango de red al que va dirigido el tráfico (ejemplo: 10.0.0.50 o any para cualquier destino).
- **Invert match:** Si está marcado, la regla se aplicará a todo **excepto** al rango o IP seleccionada.

Al hacer clic en "Display Advanced", puedes configurar más opciones, como:

- **Destination Port Range:** Especifica el rango de puertos de destino. Por ejemplo, el puerto 80 para HTTP o el puerto 22 para SSH.

#### 8. Log (Registro)

- **Check:** Marca esta opción si deseas registrar el tráfico que coincide con la regla. Es útil para depuración o auditoría.

#### 9. Description (Descripción)

Escribe una descripción para la regla. Esto es importante para que puedas identificar fácilmente el propósito de cada regla en el futuro.

#### 10. Schedule (Horario)

Puedes crear reglas que solo se apliquen durante ciertos períodos de tiempo.

- **None:** La regla estará activa todo el tiempo.
- **Schedule:** Puedes seleccionar un horario previamente definido para que la regla se aplique solo en esos momentos. Esto es útil, por ejemplo, si solo quieras permitir el acceso SSH en ciertas horas.

#### Ejemplo de configuración:

- **Action:** Pass
- **Interface:** DMZ
- **Address Family:** IPv4
- **Protocol:** TCP
- **Source:** 10.0.0.40
- **Source Port Range:** Any
- **Destination:** 10.0.0.50
- **Destination Port Range:** Custom (22) para SSH
- **Log:** Activado si quieras registrar este tráfico
- **Description:** Permitir SSH de 10.0.0.40 a 10.0.0.50

#### Importancia del orden de las reglas:

- **pfSense** evalúa las reglas de arriba hacia abajo\*\*, deteniéndose en la primera regla que coincida. Si tienes reglas que permiten y otras que bloquean tráfico, asegúrate de que las reglas que permiten tráfico específico estén **antes** de las reglas que bloquean el tráfico general.

The screenshot shows a web browser window displaying the pfSense firewall rules configuration. The URL in the address bar is [http://172.16.0.1/firewall\\_rules.php?if=opt1](http://172.16.0.1/firewall_rules.php?if=opt1). The tab title is "fw01-pfSense.practica1.co...". The interface has tabs for Floating, WAN, LAN, and DMZ, with DMZ selected. The main area is titled "Rules (Drag to Change Order)" and contains a table of rules:

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✗	0 / 0 B	*	Reserved Not assigned by IANA	*	*	*	*	*	*	Block bogon networks	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Preview</a> <a href="#">Details</a>
✓	0 / 0 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none		Permitir trafico HTTP	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Preview</a> <a href="#">Details</a>
✓	0 / 0 B	IPv4 TCP	*	*	*	443 (HTTPS)	*	none		Permitir trafico HTTPS	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Preview</a> <a href="#">Details</a>
✓	0 / 0 B	IPv4 TCP	*	*	*	3306	*	none		Permitir trafico MySQL	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Preview</a> <a href="#">Details</a>
✓	0 / 0 B	IPv4 TCP	10.0.0.40	*	10.0.0.50	1101	*	none		Permitir conexion ssh 40 a 50	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Preview</a> <a href="#">Details</a>
✗	0 / 0 B	IPv4 ICMP	10.0.0.40	*	10.0.0.50	*	*	none		Bloquear ICMP de 40 a 50	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Preview</a> <a href="#">Details</a>
✗	0 / 0 B	IPv4 ICMP	10.0.0.40	*	10.0.0.60	*	*	none		Bloquear ICMP de 40 a 60	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Preview</a> <a href="#">Details</a>
✗	0 / 0 B	IPv4 ICMP	10.0.0.50	*	10.0.0.40	*	*	none		Bloquear ICMP de 50 a 40	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Preview</a> <a href="#">Details</a>
✗	0 / 0 B	IPv4 ICMP	10.0.0.50	*	10.0.0.60	*	*	none		Bloquear ICMP de 50 a 60	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Preview</a> <a href="#">Details</a>
✗	0 / 0 B	IPv4 ICMP	10.0.0.60	*	10.0.0.40	*	*	none		Bloquear ICMP de 60 a 40	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Preview</a> <a href="#">Details</a>
✗	0 / 0 B	IPv4 ICMP	10.0.0.60	*	10.0.0.50	*	*	none		Bloquear ICMP de 60 a 50	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Preview</a> <a href="#">Details</a>
✓	0 / 0 B	IPv4 TCP	10.0.0.40	*	10.0.0.60	1101	*	none		Permitir conexion ssh 40 a 60	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Preview</a> <a href="#">Details</a>
✓	0 / 0 B	IPv4 TCP	10.0.0.50	*	10.0.0.40	1101	*	none		Permitir conexion ssh 50 a 40	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Preview</a> <a href="#">Details</a>
✓	0 / 0 B	IPv4 TCP	10.0.0.50	*	10.0.0.60	1101	*	none		Permitir conexion ssh 50 a 60	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Preview</a> <a href="#">Details</a>
✓	0 / 0 B	IPv4 TCP	10.0.0.60	*	10.0.0.40	1101	*	none		Permitir conexion ssh 60 a 40	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Preview</a> <a href="#">Details</a>
✓	0 / 0 B	IPv4 TCP	10.0.0.60	*	10.0.0.50	1101	*	none		Permitir conexion ssh 60 a 50	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Preview</a> <a href="#">Details</a>
✓	2/121 Kib	IPv4 *	DMZ net	*	*	*	*	none		Permitir DMZ a internet	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Preview</a> <a href="#">Details</a>
✗	0 / 0 B	IPv4 *	10.0.0.40	*	10.0.0.50	*	*	none		Bloquear trafico de 40 a 50	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Preview</a> <a href="#">Details</a>
✗	0 / 0 B	IPv4 *	10.0.0.40	*	10.0.0.60	*	*	none		Bloquear trafico de 40 a 60	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Preview</a> <a href="#">Details</a>
✗	0 / 0 B	IPv4 *	10.0.0.50	*	10.0.0.40	*	*	none		Bloquear trafico de 50 a 40	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Preview</a> <a href="#">Details</a>
✗	0 / 0 B	IPv4 *	10.0.0.50	*	10.0.0.60	*	*	none		Bloquear trafico de 50 a 60	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Preview</a> <a href="#">Details</a>

The browser taskbar at the bottom shows the Windows Start button, a search icon, a file icon, a settings icon, and the date/time (14/10/2024, 09:56 a.m., US). The system tray icons include a network connection, battery, and volume.

## IP Ubuntu (IaaS)

### ¿Por qué configurar una IP estática?

A diferencia de una IP dinámica, que se asigna automáticamente por un servidor DHCP, una IP estática permanece fija, lo que es útil para:

- **Servidores:** Los servidores necesitan una dirección IP estable para que otros dispositivos puedan conectar a ellos de forma confiable.
- **Dispositivos de red:** Routers, firewalls y otros dispositivos de red a menudo se configuran con IP estáticas para facilitar su administración.

### Pasos para configurar una IP estática en Ubuntu Server 24.04:

Ubuntu Server 24.04 utiliza Netplan para configurar las redes. Esto hace que el proceso sea bastante sencillo.

#### 1. Identificar la interfaz de redsa:

```
ip a
```

- Identifica la interfaz que deseas configurar (por ejemplo, enp0s3).

```
root@ubuntu:/home/ubuntu# 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 noprefixroute
        valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:69:04:a8 brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    inet 192.168.50.40/24 brd 192.168.50.255 scope global ens160
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe69:4a8/64 scope link
        valid_lft forever preferred_lft forever
root@ubuntu:/home/ubuntu#
```

#### 2. Editar el archivo de configuración de Netplan:

- El nombre del archivo de configuración suele ser algo como 00-installer-config.yaml o 50-cloud-init.yaml. Para encontrar la ubicación exacta ejecutando:

```
sudo netplan --list
```

```
root@ubuntu:/home/ubuntu# netplan --list
You need to specify a command
usage: /usr/sbin/netplan [-h] [--debug] ...

Network configuration in YAML

options:
  -h, --help  show this help message and exit
  --debug    Enable debug messages

Available commands:

  help      Show this help message
  apply     Apply current netplan config to running system
  generate  Generate backend specific configuration files from /etc/netplan/*.yaml
  get       Get a setting by specifying a nested key like "ethernets.eth0.addresses", or "all"
  info      Show available features
  ip        Retrieve IP information from the system
  set       Add new setting by specifying a dotted key=value pair like ethernets.eth0.dhcp4=true
  rebind   Rebind SR-IOV virtual functions of given physical functions to their driver
  status    Query networking state of the running system
  try      Try to apply a new netplan config to running system, with automatic rollback
root@ubuntu:/home/ubuntu# _
```

- Luego se edita el archivo con un editor de texto como nano o vim:

```
sudo nano /etc/netplan/50-cloud-init.yaml
```

### 3. Configurar la IP estática:

- Dentro del archivo, busca la sección correspondiente a la interfaz que deseas configurar.
- Agrega o modifica las siguientes líneas para establecer la IP estática, máscara de subred y puerta de enlace:

```
network:
  version: 2
  ethernets:
    enp0s3:
      addresses: [192.168.50.40/24]
      routes:
        - to: default
          via: 192.168.50.1
      nameservers:
        addresses: [8.8.8.8, 8.8.4.4]
```

```
# This file is generated from information provided by the datasource. Changes
# to it will not persist across an instance reboot. To disable cloud-init's
# network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
  version: 2
  ethernets:
    ens160:
      dhcp4: no
      addresses:
        - 192.168.50.40/24
      routes:
        - to: default
          via: 192.168.50.2
      nameservers:
        addresses: [8.8.8.8, 8.8.4.4]
```

#### 4. Aplicar los cambios:

- Guarda el archivo y aplica los cambios:

```
sudo netplan apply
```

```
oot@ubuntu:/home/ubuntu# netplan apply
oot@ubuntu:/home/ubuntu# _
```

#### 5. Verificar la configuración:

- Una vez aplicado los cambios, puedes verificar la configuración ejecutando:

```
root@ubuntu:/home/ubuntu# 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 noprefixroute
        valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:69:04:a8 brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    inet 192.168.50.40/24 brd 192.168.50.255 scope global ens160
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe69:4a8/64 scope link
        valid_lft forever preferred_lft forever
```

### Firewall maquina virtuales

Lo primero antes de comenzar con la configuración del Firewall del equipo Ubuntu, es borrar las reglas del firewall (en caso de que el sistema tuviera alguna).

```
root@ubuntu:/home/ubuntu# iptables -F
root@ubuntu:/home/ubuntu# iptables -t nat -F
root@ubuntu:/home/ubuntu# ^~_
```

Ahora reiniciamos los contadores de todos los paquetes.

```
root@ubuntu:/home/ubuntu# iptables -Z
root@ubuntu:/home/ubuntu# iptables -t nat -Z
root@ubuntu:/home/ubuntu#
```

Para configurar un firewall, existen dos políticas, la primera consiste en aceptar todo y denegar en lo particular, mientras que la segunda consiste en denegar todo y aceptar en lo particular. Para este firewall vamos a denegar todo y luego a permitir el tráfico correcto, para ello crearemos el archivo **mifirewall.sh**, el cual será el script que ejecutaremos para cargar las reglas al firewall, de otra forma tendríamos que ingresar línea por línea en la terminal.

Entonces lo primero es crear el archivo del script.

```
root@ubuntu:/home/ubuntu/firewall# cat > mifirewall.sh
^C
root@ubuntu:/home/ubuntu/firewall# ll
total 8
drwxr-xr-x 2 root  root  4096 Sep 29 02:24 .
drwxr-x--- 5 ubuntu ubuntu 4096 Sep 29 02:23 ..
-rw-r--r-- 1 root  root     0 Sep 29 02:24 mifirewall.sh
root@ubuntu:/home/ubuntu/firewall# _
```

Ahora agregamos las reglas para que denegar el tráfico.

```
GNU nano 7.2                                     mifirewall.sh *
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
```

Importante darle permisos con chmod 777 al archivo mifirewall.sh para que lo podamos ejecutar.

```
root@ubuntu:/home/ubuntu/firewall# chmod 777 mifirewall.sh
root@ubuntu:/home/ubuntu/firewall#
```

Para ejecutar el script y cargar las reglas al firewall solo es con:

```
root@ubuntu:/home/ubuntu/firewall# ./mifirewall.sh
```

Y ahora para ver el listado de las reglas del firewall:

```
root@ubuntu:/home/ubuntu/firewall# iptables -L -nv --line-numbers
Chain INPUT (policy DROP 13 packets, 936 bytes)
num  pkts bytes target     prot opt in     out      source          destination
Chain FORWARD (policy DROP 0 packets, 0 bytes)
num  pkts bytes target     prot opt in     out      source          destination
Chain OUTPUT (policy DROP 8 packets, 596 bytes)
num  pkts bytes target     prot opt in     out      source          destination
root@ubuntu:/home/ubuntu/firewall# _
```

Ahora agregamos al archivo del script algunas reglas, entre ellas están para permitir los pings, consulta y respuesta del dns, y en este caso también agregamos la del loopback ya que nuestro sistema la utiliza.

```
GNU nano 7.2                                         mifirewall.sh
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

#Permitir ping
iptables -A OUTPUT -o ens160 -p icmp -j ACCEPT
iptables -A INPUT -i ens160 -p icmp -j ACCEPT

#Consultas y respuestas del DNS
iptables -A OUTPUT -o ens160 -p udp --dport 53 -j ACCEPT
iptables -A INPUT -i ens160 -p udp --sport 53 -j ACCEPT

iptables -A OUTPUT -o ens160 -p tcp --dport 53 -j ACCEPT
iptables -A INPUT -i ens160 -p tcp --sport 53 -j ACCEPT

#Habilitar la interfaz del loopback en system-resolve
iptables -I INPUT 1 -i lo -j ACCEPT
iptables -I OUTPUT 1 -o lo -j ACCEPT
```

Para permitir el tráfico http

```
#Trafico HTTP
iptables -A OUTPUT -o ens160 -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -i ens160 -p tcp --sport 80 -j ACCEPT
```

Para permitir el tráfico https

```
#Trafico HTTPS
iptables -A OUTPUT -o ens160 -p tcp --dport 443 -j ACCEPT
iptables -A INPUT -i ens160 -p tcp --sport 443 -j ACCEPT
```

Quedando de la siguiente forma:

```
root@ubuntu:/home/ubuntu/firewall# iptables -L -nv --line-numbers
Chain INPUT (policy DROP 1 packets, 72 bytes)
num  pkts bytes target  prot opt in     out    source          destination
1    6   517 ACCEPT   0     --  lo    *      0.0.0.0/0        0.0.0.0/0
2    4   336 ACCEPT   1     --  ens160 *      0.0.0.0/0        0.0.0.0/0
3    3   300 ACCEPT   17    --  ens160 *      0.0.0.0/0        0.0.0.0/0
4    0   0   ACCEPT   6     --  ens160 *      0.0.0.0/0        0.0.0.0/0
                                         udp spt:53
                                         tcp spt:53

Chain FORWARD (policy DROP 0 packets, 0 bytes)
num  pkts bytes target  prot opt in     out    source          destination

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
num  pkts bytes target  prot opt in     out    source          destination
1    6   517 ACCEPT   0     --  *      lo   0.0.0.0/0        0.0.0.0/0
2    4   336 ACCEPT   1     --  *      ens160 0.0.0.0/0       0.0.0.0/0
3    3   217 ACCEPT   17    --  *      ens160 0.0.0.0/0       0.0.0.0/0
4    0   0   ACCEPT   6     --  *      ens160 0.0.0.0/0       0.0.0.0/0
                                         udp dpt:53
                                         tcp dpt:53
root@ubuntu:/home/ubuntu/firewall# _
```

Para saber si nuestro equipo utiliza system-resolve

```
root@ubuntu:/home/ubuntu/firewall# cat /etc/resolv.conf
# This is /run/systemd/resolve/stub-resolv.conf managed by man:systemd-resolved(8).
# Do not edit.
#
# This file might be symlinked as /etc/resolv.conf. If you're looking at
# /etc/resolv.conf and seeing this text, you have followed the symlink.
#
# This is a dynamic resolv.conf file for connecting local clients to the
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
#
# Run "resolvectl status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs should typically not access this file directly, but only
# through the symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a
# different way, replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 127.0.0.53
options edns0 trust-ad
search localdomain
```

## Port Groups (VLANs)

Un port group en VMware ESXi es como un conjunto de puertos virtuales que comparten una configuración de red común. Imagina un switch físico en tu red: cada puerto de ese switch puede tener una configuración diferente (VLAN, QoS, etc.). En ESXi, un port group es como uno de esos puertos, pero en el mundo virtual.

### ¿Para qué sirven los Port Groups?

- Organización: Agrupan puertos virtuales con características similares, facilitando la gestión de la red virtual.
- Configuración: Permiten aplicar una configuración de red específica a un grupo de máquinas virtuales, como la VLAN, la política de QoS o las reglas de seguridad.
- Aislamiento: Puedes crear port groups separados para diferentes tipos de tráfico (por ejemplo, producción y pruebas) para aumentar la seguridad.

- Flexibilidad: Facilitan la creación de redes virtuales complejas y la adaptación de la infraestructura a las necesidades cambiantes.

### Tipos de Port Groups en ESXi

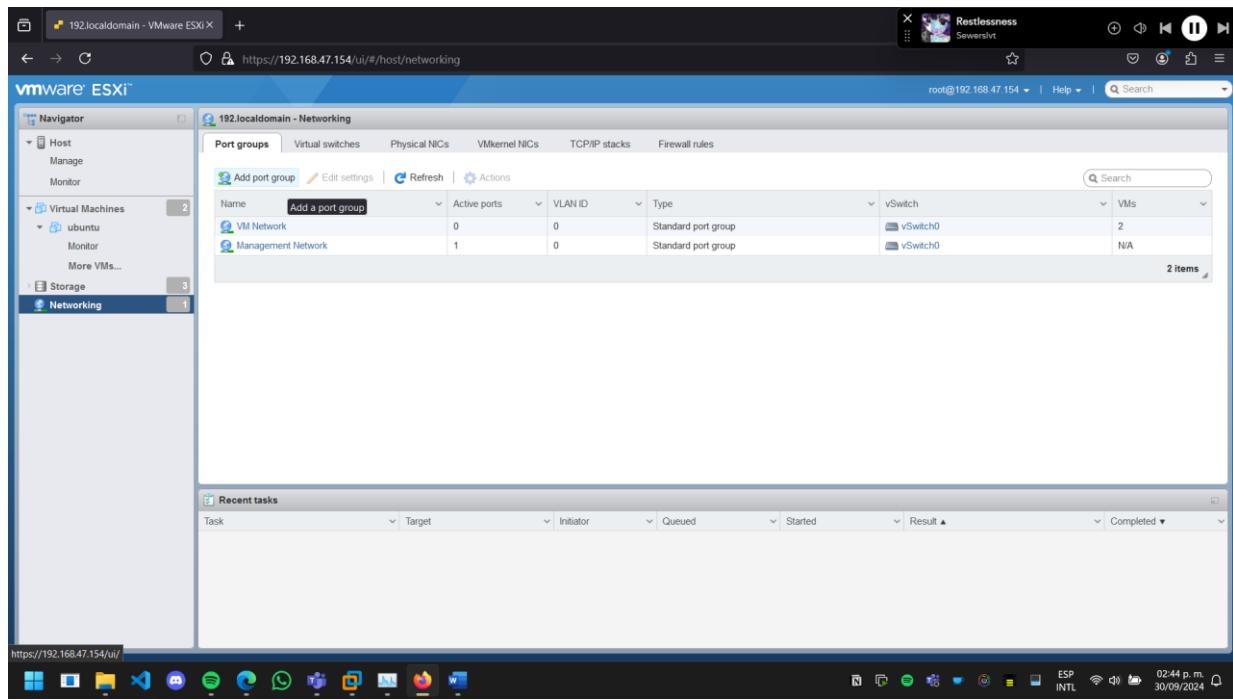
Existen dos tipos principales de port groups:

- VMkernel Port Groups: Se utilizan para conectar servicios de ESXi al conmutador virtual, como vMotion, vSAN, administración de iSCSI, etc.
- Virtual Machine Port Groups: Se utilizan para conectar las máquinas virtuales a la red virtual.

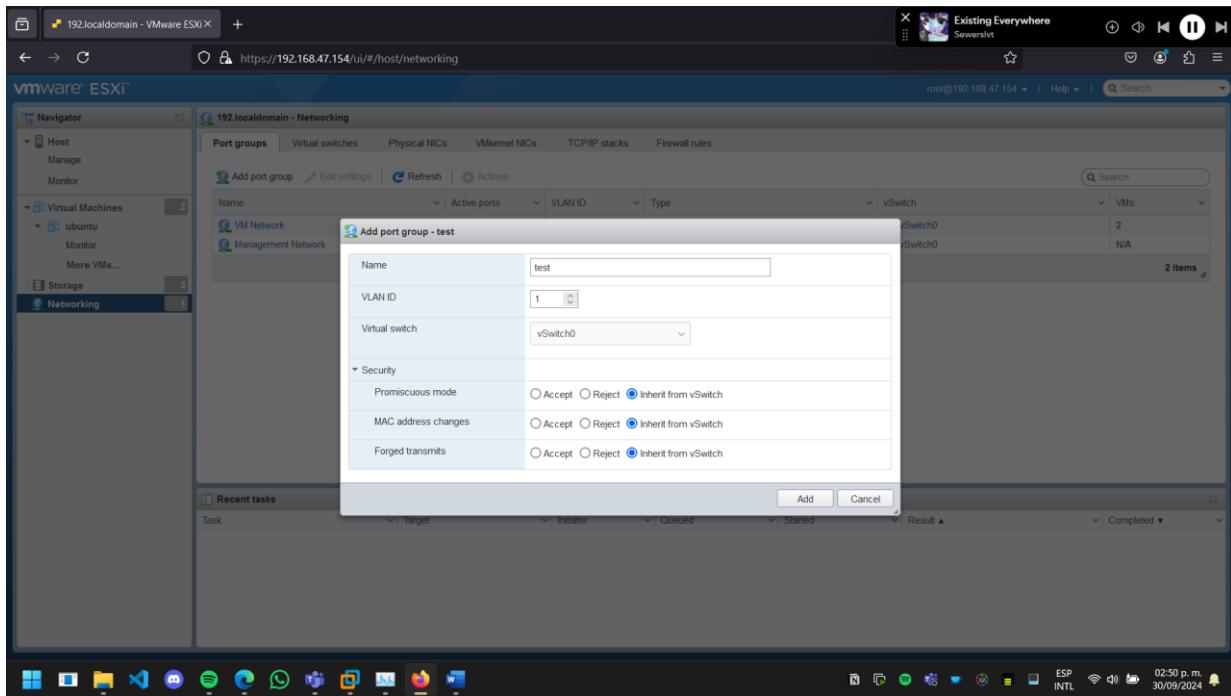
### ¿Cómo funcionan los Port Groups?

Cuando creas una máquina virtual, le asignas un adaptador de red virtual que se conecta a un port group específico. Todos los adaptadores de red virtuales conectados a un mismo port group heredarán la configuración de ese port group.

Para añadir un nuevo port group tenemos que ir al apartado de Networking, y en la pestaña de “Port Groups” le damos en “Add port group”.



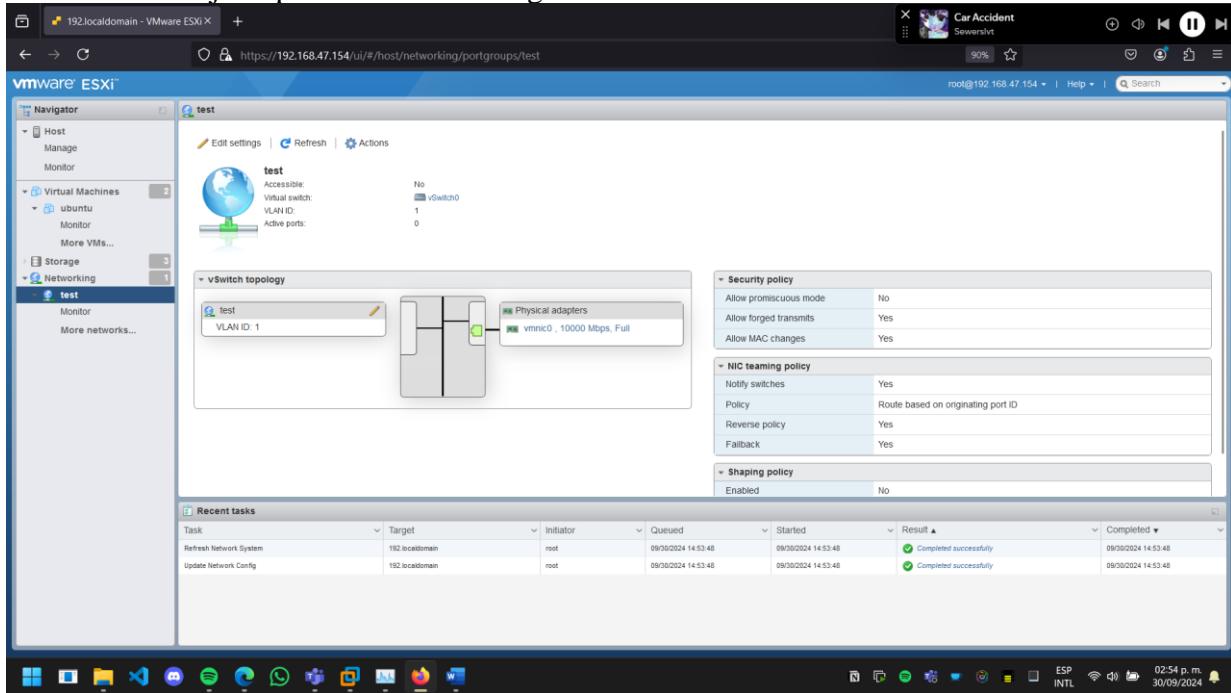
Nos aparecerá una ventana en la cual podemos asignar nombre, id de la vlan, seleccionar el vswitch que usará, así como algunas opciones de seguridad para diferentes situaciones.



Las tres opciones de seguridad que nos da:

- **Promiscuous mode:** Este modo permite a una interfaz de red capturar todo el tráfico de la red, incluso si no está dirigido a esa interfaz.
- **MAC address changes:** Controla si se permiten cambios en las direcciones MAC de las interfaces de red conectadas al port group.
- **Forged transmits:** Se refiere a los paquetes de red que parecen provenir de una dirección MAC diferente a la real.

De momento dejare que hereden la configuración del vswitch.



Una vez tengamos el grupo creado, podemos editar sus configuraciones de acuerdo con lo que necesitemos, por ejemplo, una configuración interesante es:

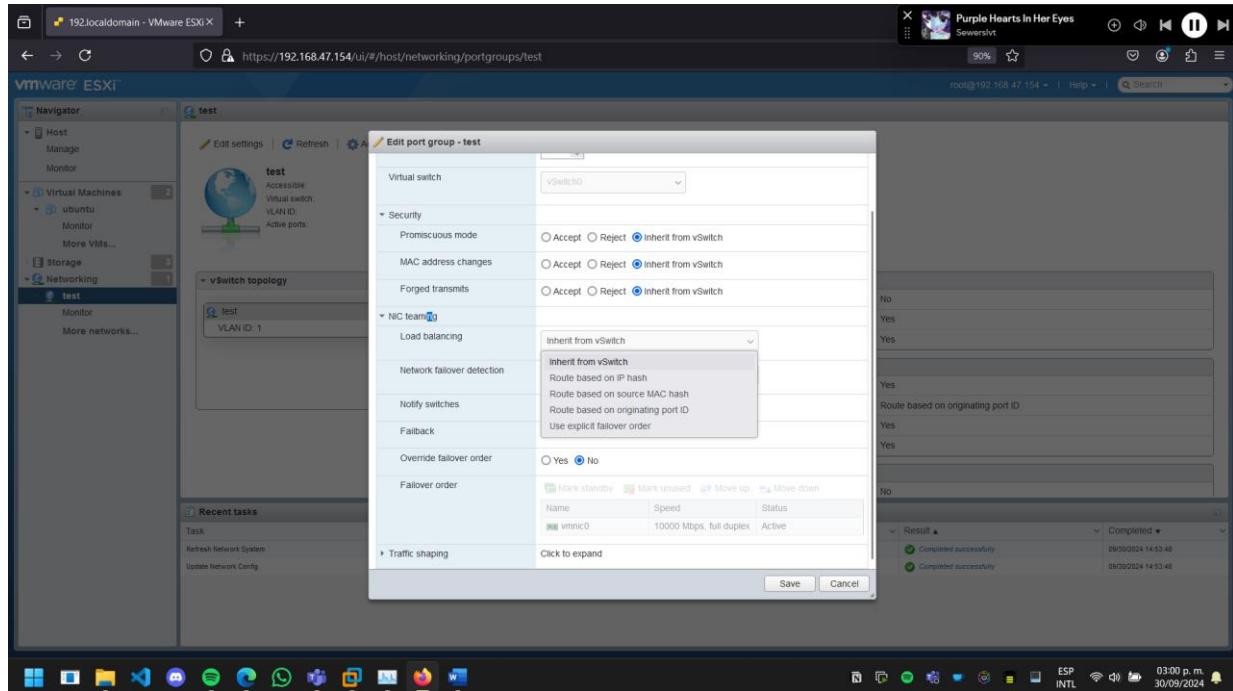
**NIC Teaming** (o agrupamiento de NIC) es una tecnología que permite agrupar múltiples tarjetas de red físicas en una sola interfaz lógica. Esto ofrece una serie de beneficios, como el aumento del ancho de banda, la redundancia y la tolerancia a fallos. Una de las configuraciones más importantes dentro de NIC Teaming es el método de **balanceo de carga**.

### ¿Qué es el Balanceo de Carga en NIC Teaming?

El balanceo de carga determina cómo se distribuye el tráfico de red entre las diferentes interfaces físicas que conforman el equipo. Es decir, define la forma en que los paquetes de datos son enviados y recibidos a través de las distintas NIC.

### Opciones de Balanceo de Carga Comunes

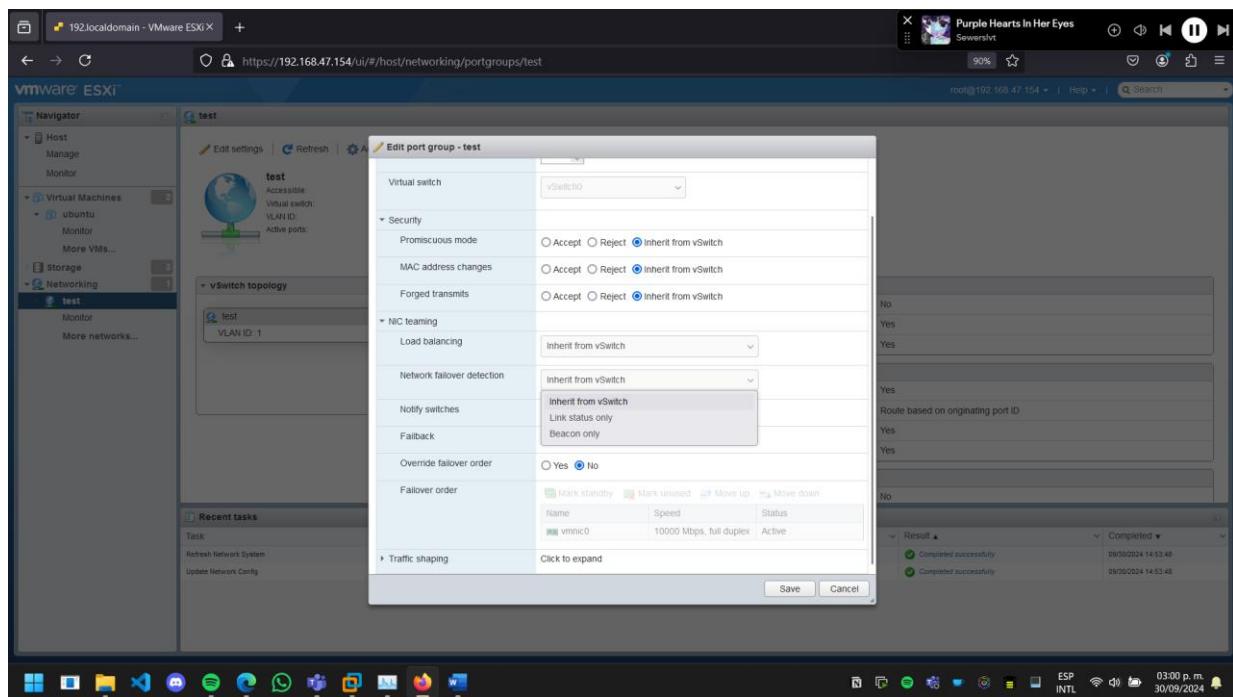
- **Route based on IP hash:** El tráfico se distribuye entre las interfaces físicas en función de un hash calculado a partir de la dirección IP de destino. Esta es una opción común y suele proporcionar un buen equilibrio de carga en la mayoría de los casos.
- **Route based on source MAC hash:** Similar al anterior, pero el hash se calcula a partir de la dirección MAC de origen del paquete.
- **Route based on originating port ID:** El tráfico se distribuye en función de un identificador de puerto de origen. Esta opción puede ser útil en entornos donde se requiere un control más granular sobre el flujo de tráfico.
- **Use explicit failover order:** En esta opción, se define un orden específico para las interfaces físicas. Si una interfaz falla, el tráfico se redirigirá a la siguiente interfaz en la lista.



La opción "**Network failover detection**" (detección de fallos de red) en la configuración de NIC Teaming define el método que se utiliza para determinar cuándo una interfaz de red física ha fallado y es necesario comutar a otra interfaz. Esto es fundamental para garantizar la alta disponibilidad y la tolerancia a fallos en un entorno de red.

#### Opciones de la detección de fallos de red

- **Inherit from vSwitch:** Hereda la configuración de detección de fallos del conmutador virtual. Esto significa que la detección de fallos se realizará de acuerdo con las reglas establecidas en el conmutador virtual. Esta opción es útil cuando se desea mantener una configuración coherente en todo el entorno virtual.
- **Link status only:** La detección de fallos se basa únicamente en el estado del enlace físico. Si el enlace se cae, se considera que ha ocurrido un fallo. Es una opción simple y eficaz para detectar fallos físicos en la interfaz de red.
- **Beacon only:** Se utilizan paquetes especiales (beacons) para verificar la conectividad de la interfaz. Si no se reciben los beacons, se considera que ha ocurrido un fallo. Esta opción es más adecuada para entornos donde se requiere una detección de fallos más precisa y rápida, ya que los beacons permiten detectar problemas antes de que se produzcan fallos en el enlace físico.



Notify switches	<input type="radio"/> Yes <input type="radio"/> No <input checked="" type="radio"/> Inherit from vSwitch						
Fallback	<input type="radio"/> Yes <input type="radio"/> No <input checked="" type="radio"/> Inherit from vSwitch						
Override failover order	<input type="radio"/> Yes <input checked="" type="radio"/> No						
Failover order	<div style="display: flex; justify-content: space-between;"> <span> Mark standby</span> <span> Mark unused</span> <span> Move up</span> <span> Move down</span> </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Name</th> <th>Speed</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td> vmnic0</td> <td>10000 Mbps, full duplex</td> <td>Active</td> </tr> </tbody> </table>	Name	Speed	Status	vmnic0	10000 Mbps, full duplex	Active
Name	Speed	Status					
vmnic0	10000 Mbps, full duplex	Active					

### Notify switches (Notificar switches)

Esta opción determina si se informa al switch físico cuando ocurre un cambio en el estado de las interfaces virtuales agrupadas. Al seleccionar "Yes" (Sí), el switch físico será notificado de eventos como la falla de una interfaz o un cambio en el balanceo de carga. Esto permite al switch actualizar su tabla de direcciones MAC y realizar ajustes necesarios.

#### Beneficios de notificar a los switches:

- **Actualización de la tabla MAC:** El switch mantiene una tabla de direcciones MAC de los dispositivos conectados. Al ser notificado de cambios, puede actualizar esta tabla de manera oportuna.
- **Optimización del enrutamiento:** El switch puede ajustar sus rutas de enrutamiento en función de los cambios en la topología de la red.
- **Mejoramiento de la estabilidad:** La notificación de cambios ayuda a prevenir problemas de bucle y otras anomalías en la red.

### Fallback (Commutación por recuperación)

Esta opción define el comportamiento del sistema cuando una interfaz física que previamente había fallado vuelve a estar disponible. Si se selecciona "Yes" (Sí), el sistema intentará restaurar el tráfico a la interfaz original una vez que se haya recuperado.

#### Consideraciones sobre la conmutación por recuperación:

- **Estabilidad:** La conmutación por recuperación puede introducir inestabilidad en la red si no se realiza de manera cuidadosa.
- **Rendimiento:** La conmutación por recuperación puede afectar el rendimiento de la aplicación si se produce con frecuencia.

### Override failover order (Anular orden de conmutación por error)

Esta opción permite modificar el orden predefinido de conmutación por error. Por defecto, el sistema conmuta a la siguiente interfaz disponible en la lista. Al seleccionar "Yes" (Sí), puedes personalizar este orden para satisfacer tus necesidades específicas.

#### Uso de la anulación del orden de conmutación por error:

- **Priorización de interfaces:** Puedes colocar las interfaces más críticas en la parte superior de la lista para garantizar que el tráfico se redirija a ellas en caso de falla.
- **Aislamiento de tráfico:** Puedes separar el tráfico de diferentes aplicaciones en diferentes interfaces y definir un orden de conmutación por error específico para cada tipo de tráfico.

### **Failover order (Orden de conmutación por error)**

Esta sección te permite definir el orden específico en el que las interfaces físicas se utilizarán en caso de falla. Puedes marcar una interfaz como "standby" (en espera) o "unused" (no utilizada), y ajustar su posición en la lista.

#### **Configuración del orden de conmutación por error:**

- **Mark standby:** Marca una interfaz como en espera. Esta interfaz se utilizará solo si todas las demás interfaces han fallado.
- **Mark unused:** Marca una interfaz como no utilizada. Esta interfaz no se utilizará para el tráfico de red.
- **Move up/Move down:** Te permite ajustar la posición de una interfaz en la lista.

Traffic shaping	
Status	<input type="radio"/> Enabled <input type="radio"/> Disabled <input checked="" type="radio"/> Inherit from vSwitch
Average bandwidth	100000 <input type="button"/> kb/s
Peak bandwidth	100000 <input type="button"/> kb/s
Burst size	102400 <input type="button"/> KB
Note	Traffic shaping policy is applied to the traffic of each virtual network adapter attached to the virtual switch.

El "**Traffic Shaping**" o "**Modelado de Tráfico**" es una técnica de gestión de redes que permite controlar el flujo de datos a través de una interfaz de red. En términos simples, es como poner un límite de velocidad a la cantidad de datos que pueden pasar por una carretera en un momento dado.

#### **¿Para qué sirve el Traffic Shaping?**

- **Controlar el ancho de banda:** Limita la cantidad de ancho de banda que una máquina virtual o aplicación puede utilizar, evitando que consuma todos los recursos disponibles y afectando el rendimiento de otras.
- **Evitar la congestión:** Previene la congestión de la red al limitar el tráfico durante los picos de actividad.
- **Mejorar la calidad de servicio (QoS):** Permite priorizar el tráfico de ciertas aplicaciones o usuarios, asegurando que servicios críticos como VoIP o videoconferencia tengan el ancho de banda necesario.

#### **Opciones de Configuración**

- **Status (Estado):** Activa la función de modelado de tráfico para el port group.
- **Average bandwidth (Ancho de banda promedio):** Define el ancho de banda promedio que se permitirá para el tráfico en el port group. Esto establece un límite general para el tráfico.
- **Peak bandwidth (Ancho de banda pico):** Define el ancho de banda máximo que se permitirá para ráfagas cortas de tráfico. Esto permite que haya picos ocasionales de tráfico, pero limita su duración.
- **Burst size (Tamaño de ráfaga):** Especifica la cantidad máxima de datos que se pueden enviar en una sola ráfaga, incluso si excede el ancho de banda promedio.

## Virtual Switches

Un **vSwitch** es un componente virtual que actúa como un commutador de red dentro de un entorno VMware ESXi. Sirve como el puente entre las máquinas virtuales y la red física.

Imagina un vSwitch como un pequeño switch físico dentro de tu servidor ESXi que conecta todas las máquinas virtuales que residen en él.

### Funciones principales de un vSwitch:

- **Conexión de máquinas virtuales:** Cada máquina virtual tiene al menos un adaptador de red virtual que se conecta a un port group de un vSwitch. Esto permite que las máquinas virtuales se comuniquen entre sí y con la red externa.
- **Enrutamiento:** Los vSwitches pueden realizar funciones de enrutamiento básico, lo que permite la comunicación entre diferentes redes virtuales.
- **QoS:** Los vSwitches permiten implementar políticas de Calidad de Servicio (QoS) para priorizar el tráfico de ciertas máquinas virtuales o aplicaciones.
- **Seguridad:** Los vSwitches ofrecen características de seguridad como VLANs, seguridad de puertos y listas de control de acceso (ACL) para proteger la red.
- **Alta disponibilidad:** Los vSwitches pueden configurarse para proporcionar alta disponibilidad a través de la agregación de enlaces y la conmutación por error.

### Tipos de vSwitches

Existen dos tipos principales de vSwitches en VMware ESXi:

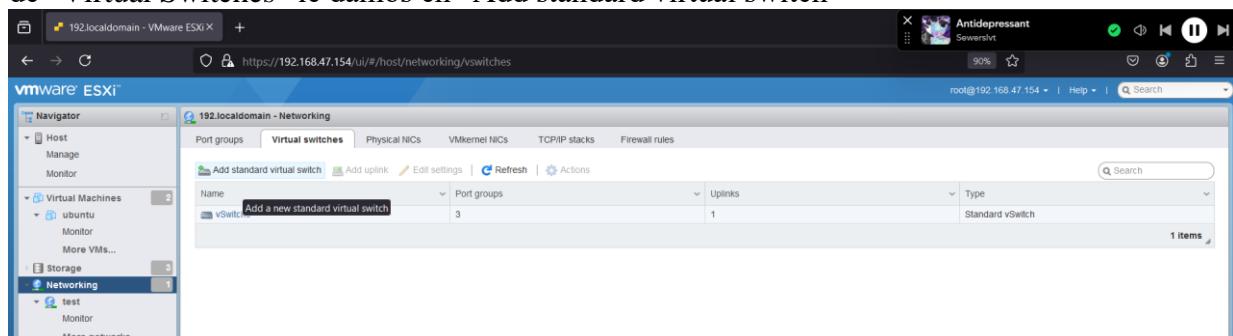
- **vSwitch estándar:** Es el tipo más básico de vSwitch y se utiliza para conectar máquinas virtuales a la red física.
- **vSwitch distribuido:** Ofrece características más avanzadas como la gestión centralizada de la configuración de la red, la alta disponibilidad y la capacidad de extenderse a múltiples hosts ESXi.

### Diferencias entre un port group y un vswitch

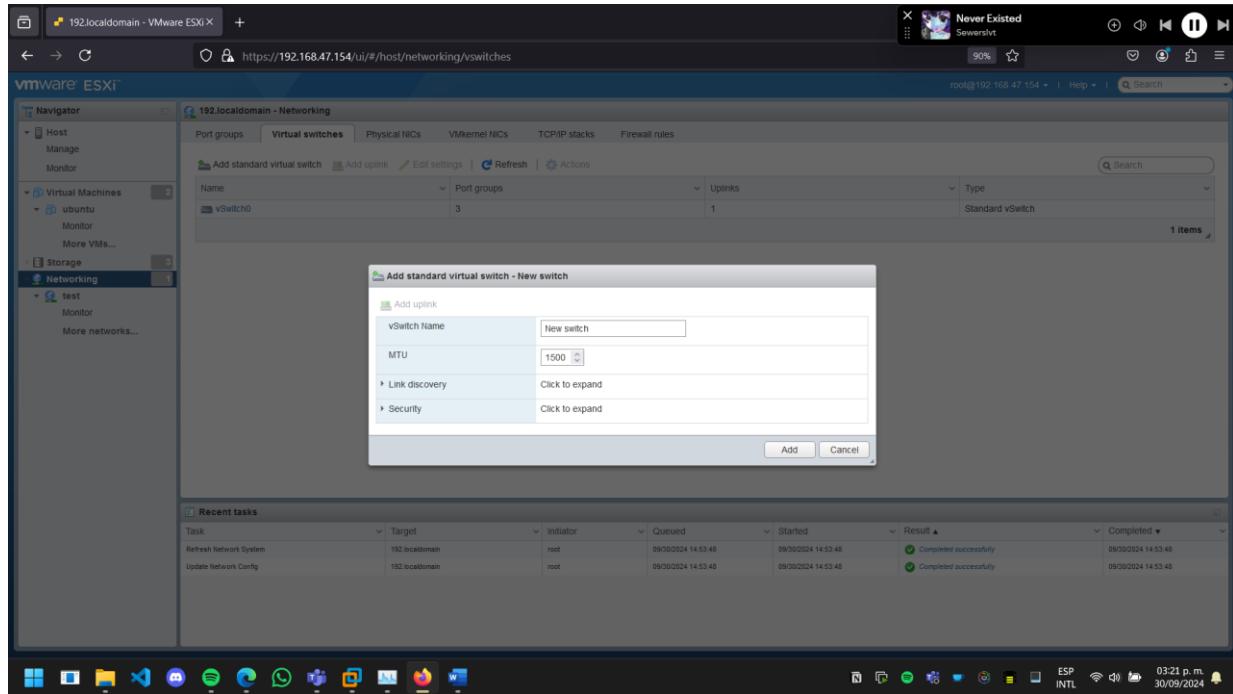
- **vSwitch:** Es el commutador virtual en sí, que proporciona la conectividad básica.
- **Port group:** Es un conjunto de puertos virtuales dentro de un vSwitch, que comparten una configuración de red común.

Imagina un vSwitch como un edificio y los port groups como las diferentes plantas de ese edificio. Cada planta tiene sus propias reglas y configuraciones, pero todas están conectadas al mismo edificio.

Para agregar un nuevo virtual switch tenemos que ir al apartado de Networking, y en la pestaña de “Virtual Switches” le damos en “Add standard virtual switch”



Y nos pedirá ingresar el nombre del nuevo vSwitch y el MTU.



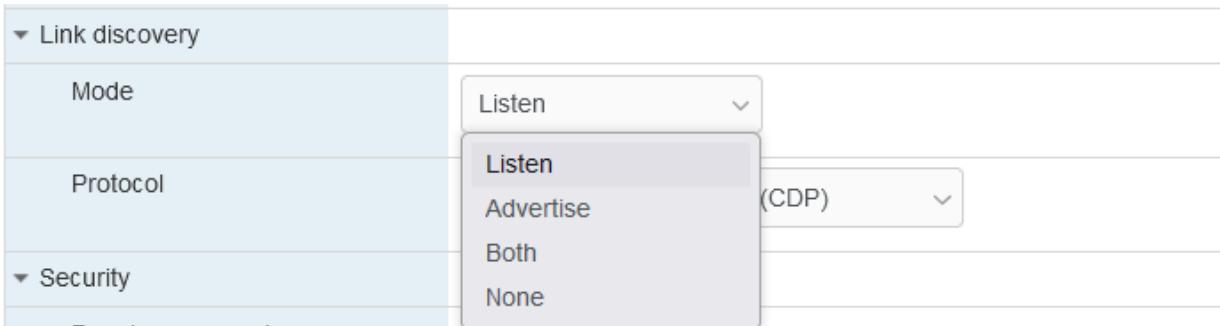
**MTU (Unidad de Transmisión Máximo):** La MTU define el tamaño máximo de un paquete de datos (en bytes) que puede transmitirse a través de una red sin que sea fragmentado.

#### Por qué es importante:

- **Evitar la fragmentación:** Un tamaño de MTU adecuado ayuda a evitar la fragmentación de paquetes, lo cual puede generar una sobrecarga en el procesador y reducir el rendimiento de la red.
- **Compatibilidad con redes:** Es crucial configurar la MTU de forma compatible con las redes a las que se conectarán las máquinas virtuales. Una MTU demasiado pequeña puede limitar el tamaño de los paquetes y afectar el rendimiento de aplicaciones que requieren un ancho de banda elevado.

#### Consideraciones al configurar la MTU:

- **MTU estándar:** El valor más común es 1500 bytes, que es el tamaño máximo de trama Ethernet estándar.
- **Redes jumbo frame:** Algunas redes admiten tramas de mayor tamaño (jumbo frames), lo que permite transmitir paquetes más grandes sin fragmentarlos. Sin embargo, todos los dispositivos en la ruta de comunicación deben admitir jumbo frames para que funcionen correctamente.
- **Impacto en el rendimiento:** Configurar una MTU demasiado grande puede causar problemas si los dispositivos intermedios no la admiten. Por otro lado, una MTU demasiado pequeña puede limitar el rendimiento de aplicaciones que requieren un ancho de banda elevado.
- ❖ En versiones posteriores de ESXi, también se incluye el apartado de **Uplink**, que es para ingresarle una tarjeta de red al switch.



**Mode:** Esta configuración determina cómo el vSwitch interactúa con otros dispositivos en la red para descubrir su presencia y establecer conexiones. Las opciones disponibles suelen ser:

- **Listen (Escuchar):** En este modo, el vSwitch solo escucha los paquetes de descubrimiento enviados por otros dispositivos. No inicia activamente el proceso de descubrimiento. Es decir, el vSwitch actúa como un receptor pasivo de información sobre otros dispositivos en la red.
- **Send (Enviar):** Aquí, el vSwitch tanto escucha como envía paquetes de descubrimiento. Esto significa que no solo detecta otros dispositivos, sino que también se anuncia a sí mismo a la red. Es el modo más común y permite una detección más completa de los dispositivos en la red.
- **Advertise (Anunciar):** Este modo es similar a "Send", pero con un enfoque más específico en anunciar su propia presencia. Es útil en escenarios donde se desea que otros dispositivos descubran el vSwitch de forma proactiva.
- 

#### Protocol (Protocolo):

- **Cisco Discovery Protocol (CDP):** Este es el protocolo de descubrimiento de enlaces propietario de Cisco. Se utiliza para descubrir dispositivos Cisco en la red y obtener información sobre ellos.

Security	
Promiscuous mode	<input type="radio"/> Accept <input checked="" type="radio"/> Reject
MAC address changes	<input type="radio"/> Accept <input checked="" type="radio"/> Reject
Forged transmits	<input type="radio"/> Accept <input checked="" type="radio"/> Reject

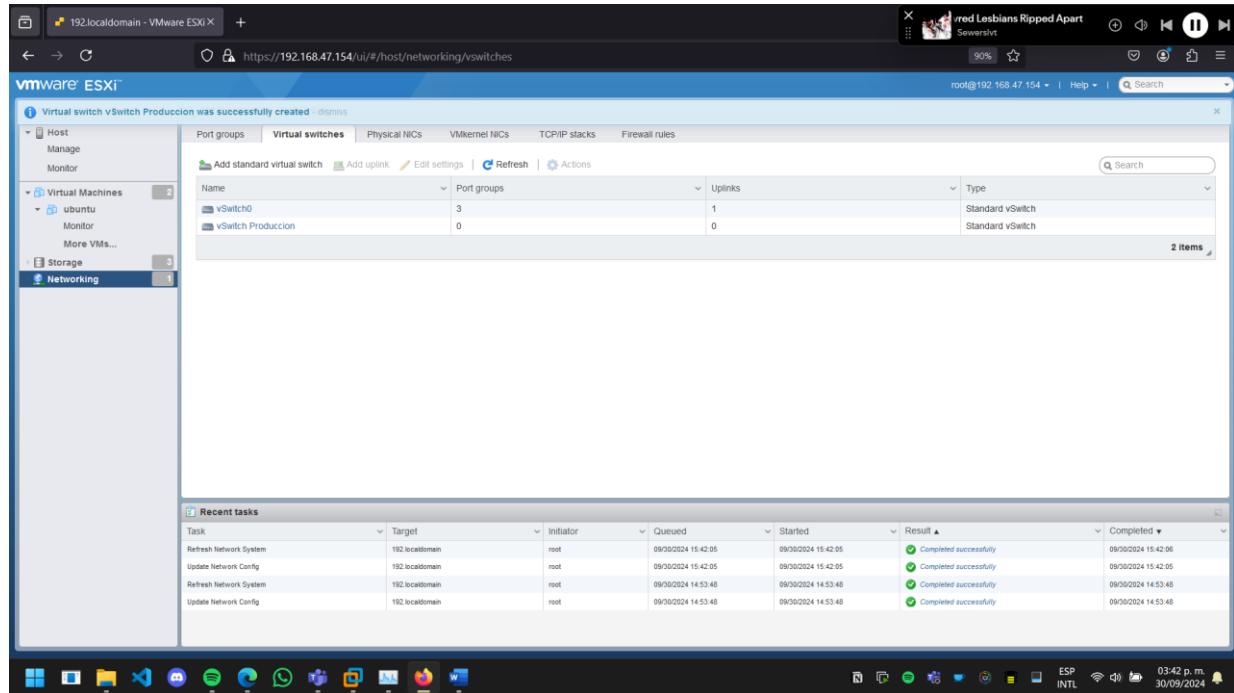
#### Security (Seguridad)

Esta sección se encarga de configurar las medidas de seguridad del vSwitch para protegerlo de posibles ataques.

- **Promiscuous mode (Modo promiscuo):**
  - **Accept (Aceptar):** Permite que el vSwitch reciba todas las tramas de red, incluso aquellas que no están destinadas a él. Esto puede ser útil para herramientas de monitoreo de red, pero también puede aumentar el riesgo de seguridad.

- **Reject (Rechazar):** El vSwitch solo recibirá las tramas que están destinadas a él, lo que mejora la seguridad.
- **MAC address changes (Cambios de dirección MAC):**
  - **Accept (Aceptar):** Permite que los dispositivos cambien su dirección MAC sin restricciones. Esto puede ser útil en entornos dinámicos, pero también puede facilitar ataques de spoofing de MAC.
  - **Reject (Rechazar):** Evita que los dispositivos cambien su dirección MAC, lo que dificulta los ataques de spoofing de MAC.
- **Forged transmits (Transmisiones falsificadas):**
  - **Accept (Aceptar):** Permite que se envíen tramas con direcciones MAC falsificadas. Esto puede ser útil en algunos entornos de laboratorio, pero también puede facilitar ataques.
  - **Reject (Rechazar):** Evita que se envíen tramas con direcciones MAC falsificadas, lo que mejora la seguridad.

De esta forma tendremos creado nuestro vSwitch.



Y al querer agregar otro port group a la red, ya nos aparece nuestro nuevo vswitch

Name	Active ports	VLAN ID	Type	vSwitch
test	0	1	Standard port group	vSwitch0
VM Network	0	0	Standard port group	vSwitch0
Management Network	1	0	Standard port group	vSwitch0
Produccion	0	2	Standard port group	vSwitch Produccion

## VMkernel NICs

Una **NIC de VMkernel** (Virtual Machine Kernel Network Interface) es una interfaz de red virtual que proporciona conectividad de red al **propio host ESXi**, a diferencia de las NICs virtuales que se asignan a las máquinas virtuales.

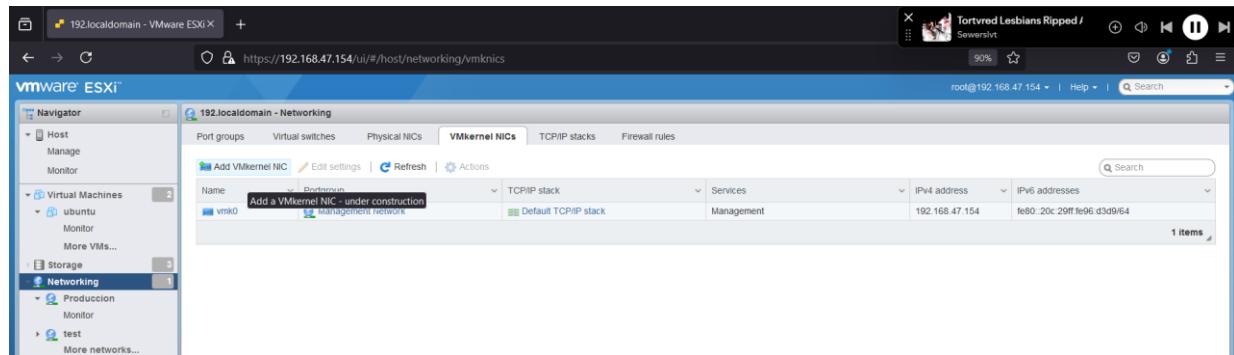
### Funciones principales de una NIC de VMkernel:

- Comunicación del host ESXi:** Se utiliza para la comunicación del host ESXi con otros sistemas, como servidores de vCenter, almacenamiento iSCSI o NFS, y otros hosts ESXi.
- Servicios de VMware:** Facilita el funcionamiento de servicios esenciales de VMware como:
  - vMotion:** Permite la migración en vivo de máquinas virtuales entre hosts.
  - Almacenamiento IP:** Proporciona acceso a almacenamiento basado en IP, como iSCSI y NFS.
  - Fault Tolerance:** Permite la alta disponibilidad al crear réplicas de máquinas virtuales.
  - vSAN:** Permite crear clústeres de almacenamiento distribuido.
  - Registro:** Facilita la recopilación y almacenamiento de registros del sistema.

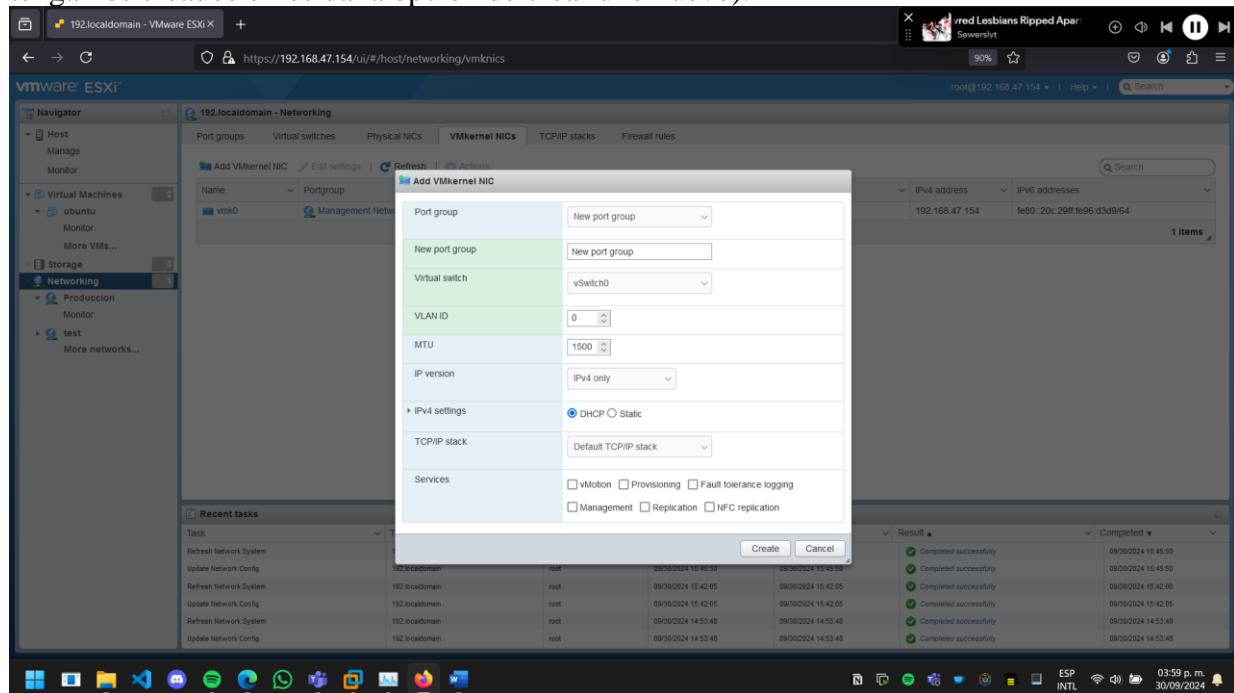
Name	Portgroup	TCP/IP stack	Services	IPv4 address	IPv6 addresses
vmk0	Management Network	Default TCP/IP stack	Management	192.168.47.154	fe80::20c:29ff:fe96:d3d9/64

Característica	NIC de VMkernel	NIC virtual
Propósito	Conectividad del host ESXi	Conectividad de las máquinas virtuales
Asignación	Al host ESXi	A las máquinas virtuales
Tráfico	Maneja tráfico de gestión y servicios de VMware	Maneja tráfico de las máquinas virtuales

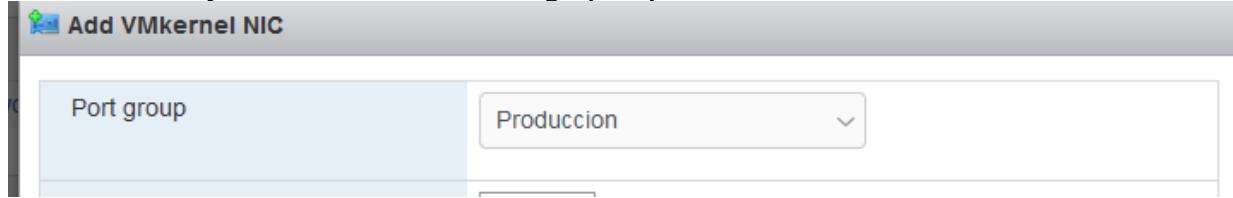
Para agregar un nuevo VMkernel tenemos que ir al apartado de Networking, y en la pestaña de “VMkernel NICs” le damos en “Add VMkenel NIC”



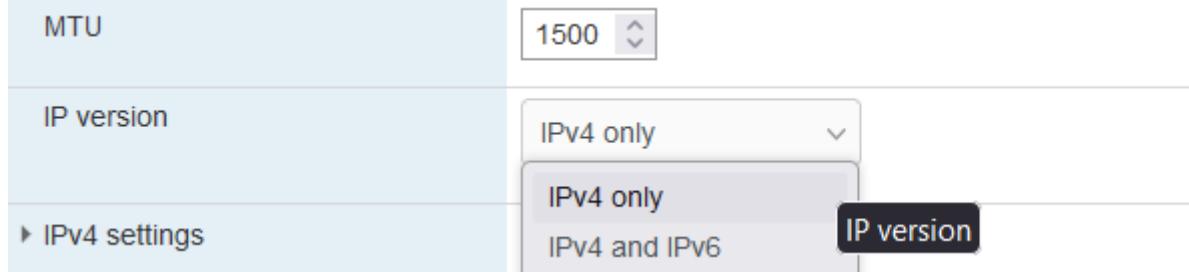
Nos aparece la venta, en donde nos pide seleccionar un port group (de acuerdo con los que tengamos creados o nos da la opción de crear uno nuevo).



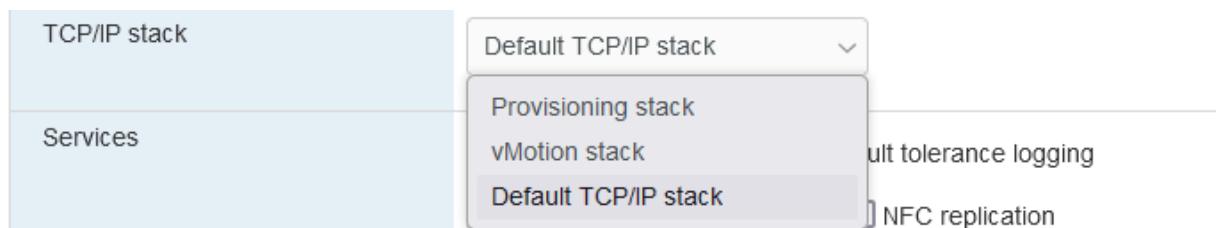
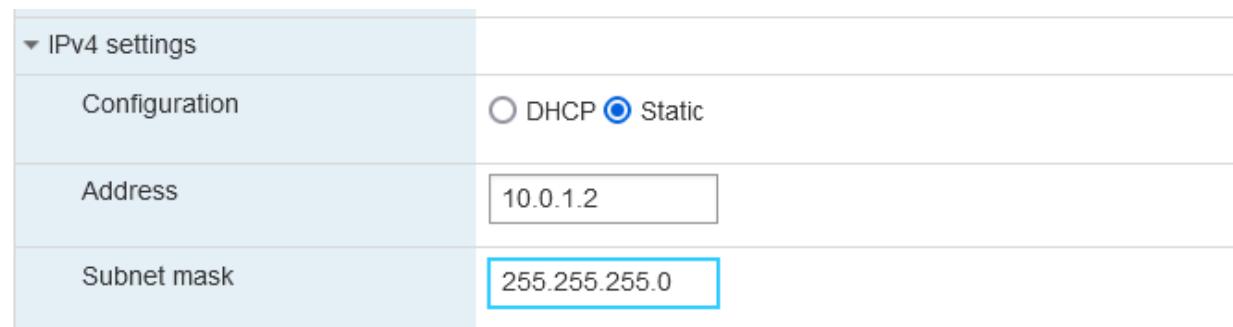
En este caso voy a seleccionar uno de los grupos que se tienen creados.



De igual forma nos deja seleccionar el MTU y si queremos usar ipv4 o ipv6.



También si queremos que sea estática o dinámica, en este caso le voy a asignar una estática.



Un **TCP/IP stack** (pila TCP/IP) es un conjunto de protocolos que permiten la comunicación entre dispositivos en una red. Es como un conjunto de reglas que definen cómo se envían y reciben los datos a través de Internet. En el contexto de una NIC de VMkernel, el TCP/IP stack especifica cómo se manejará el tráfico de red para ese adaptador.

#### Opciones del TCP/IP stack:

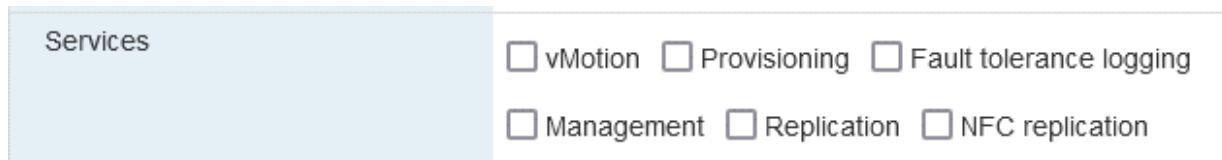
- **Default TCP/IP stack:** Esta es la opción más común y se utiliza para la mayoría de las NICs de VMkernel. Significa que la NIC utilizará la pila TCP/IP estándar del sistema operativo del host ESXi para manejar el tráfico de red. Esta pila es adecuada para la mayoría de los servicios de VMware, como vMotion, almacenamiento iSCSI y NFS.

- **Provisioning stack:** Esta pila se utiliza principalmente para servicios de aprovisionamiento, como la instalación de ESXi y la configuración inicial. Proporciona un conjunto de protocolos y servicios específicos para estas tareas.
- **vMotion stack:** Esta pila está optimizada para el tráfico de vMotion, que es el proceso de migrar máquinas virtuales en vivo entre hosts. Utiliza protocolos y configuraciones específicas para garantizar una migración rápida y sin interrupciones.

### ¿Cómo elegir la opción correcta?

La elección del TCP/IP stack dependerá del propósito de la NIC de VMkernel:

- **NIC de gestión:** Si la NIC se utilizará para la gestión del host ESXi, como la conexión a vCenter, se suele utilizar la pila **Default TCP/IP stack**.
- **NIC de vMotion:** Si la NIC se utilizará exclusivamente para el tráfico de vMotion, se recomienda utilizar la pila **vMotion stack**.
- **NIC de almacenamiento:** Para las NICs utilizadas para el acceso a almacenamiento iSCSI o NFS, la pila **Default TCP/IP stack** suele ser suficiente.



**Services:** Este apartado te permite especificar los **servicios de VMware** que utilizarán la NIC de VMkernel que estás creando. En otras palabras, defines qué funcionalidades de VMware se beneficiarán de la conectividad de red proporcionada por esa NIC.

### Opciones de los servicios

Las opciones que suelen aparecer en este apartado son las siguientes:

- **vMotion:** Este servicio permite migrar máquinas virtuales en vivo de un host a otro sin interrupción del servicio. Si marcas esta opción, la NIC se utilizará para el tráfico de migración de máquinas virtuales.
- **Provisioning:** Esta opción está relacionada con los servicios de aprovisionamiento, como la instalación inicial de ESXi o la configuración de nuevos hosts. La NIC se utilizará para el tráfico relacionado con estas tareas.
- **Fault Tolerance logging:** Este servicio proporciona alta disponibilidad al crear réplicas de máquinas virtuales. Si marcas esta opción, la NIC se utilizará para el tráfico de registro de las réplicas de Fault Tolerance.
- **Management:** Esta opción se utiliza para la comunicación de gestión del host ESXi, como la conexión a vCenter. Si marcas esta opción, la NIC se utilizará para el tráfico de gestión del host.
- **Replication:** Esta opción está relacionada con los servicios de replicación de datos, como vSAN. La NIC se utilizará para el tráfico de replicación de datos.
- **NFS replication:** Esta opción es específica para la replicación de datos basada en NFS (Network File System). Si marcas esta opción, la NIC se utilizará para el tráfico de replicación de datos NFS.

### Consideraciones:

- **Múltiples opciones:** Puedes marcar varias opciones para una misma NIC, lo que significa que la NIC se utilizará para múltiples servicios.

- Rendimiento:** La elección de los servicios puede afectar el rendimiento de la NIC. Por ejemplo, si una NIC se utiliza tanto para vMotion como para almacenamiento, es posible que el rendimiento de vMotion se vea afectado si el tráfico de almacenamiento es muy alto.
- Seguridad:** Es importante considerar las implicaciones de seguridad al seleccionar los servicios. Por ejemplo, si una NIC se utiliza para la gestión, es recomendable configurarla en una red aislada para protegerla de ataques.

De esta forma hemos logrado crear nuestra VMkernel NIC.

Name	Portgroup	TCP/IP stack	Services	IPv4 address	IPv6 addresses
vmk0	Management Network	Default TCP/IP stack	Management	192.168.47.154	fe80::20c:9ff:fe96:d3d9/64
vmk1	Producción	Default TCP/IP stack	Management, Replication, vMotion	10.0.1.2	fe80::250:56ff:fe61:e88b/64

2 items

Y ya nos aparecería en el apartado de nuestro vswitch

The screenshot shows the VMware ESXi host interface. In the left sidebar, under 'Networking', 'vSwitch Producción' is selected. The main pane displays the 'vSwitch Producción' configuration. A red box highlights the 'VMkernel ports (1)' section, which lists 'vmk1: 10.0.1.2'. The interface also shows 'Recent tasks' at the bottom, all completed successfully.

## Configurar VLAN en máquina virtual

Este paso es sencillo, lo primero es ir al apartado de “Virtual Machines”, e ingresamos dentro de la máquina que seleccionemos.

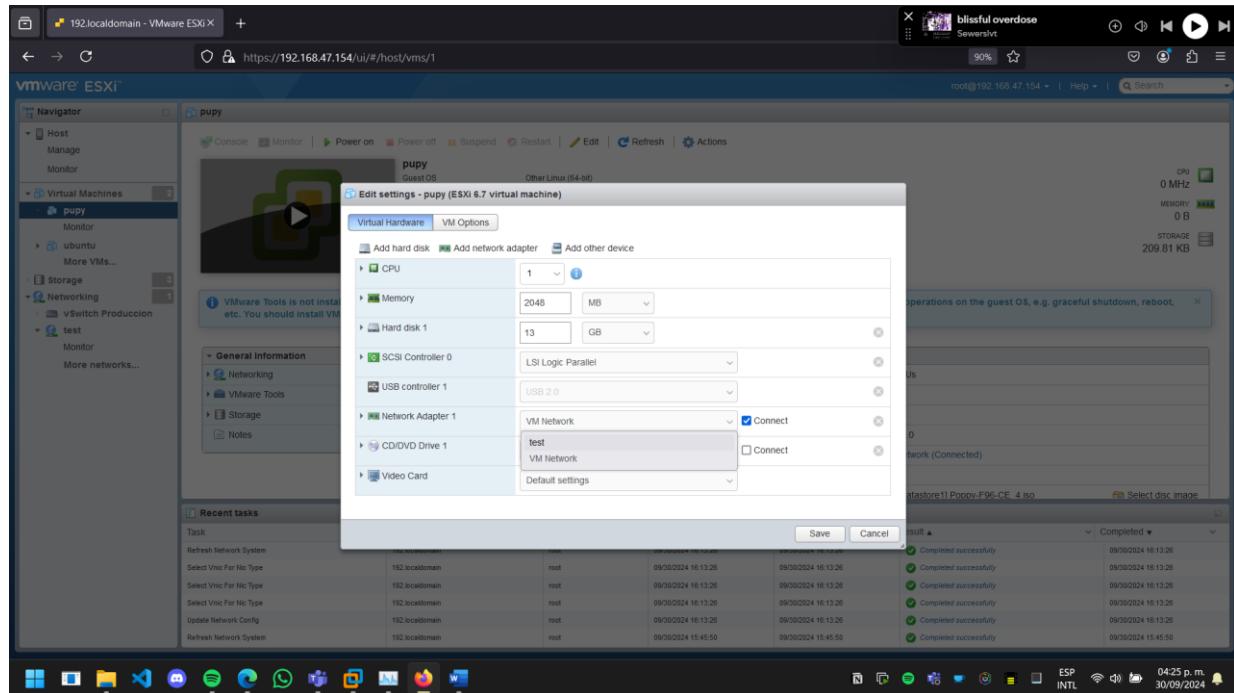
The screenshot shows the VMware ESXi web interface. On the left, the Navigator pane is open, showing categories like Host, Storage, Networking, and Virtual Machines. Under Virtual Machines, there are two entries: 'ubuntu' and 'pupy'. The 'pupy' entry is selected, and its details are shown in the main content area. Below the main content, a 'Recent tasks' table lists several completed system updates. At the bottom of the screen, a taskbar displays various icons and the system status.

Task	Target	Initiator	Queued	Started	Result	Completed
Refresh Network System	192.localdomain	root		09/03/2024 16:13:26	Completed successfully	09/03/2024 16:13:26
Select Vnic For Nic Type	192.localdomain	root		09/03/2024 16:13:26	Completed successfully	09/03/2024 16:13:26
Select Vnic For Nic Type	192.localdomain	root		09/03/2024 16:13:26	Completed successfully	09/03/2024 16:13:26
Select Vnic For Nic Type	192.localdomain	root		09/03/2024 16:13:26	Completed successfully	09/03/2024 16:13:26
Update Network Config	192.localdomain	root		09/03/2024 16:13:26	Completed successfully	09/03/2024 16:13:26
Refresh Network System	192.localdomain	root	09/03/2024 15:45:50	09/03/2024 15:45:50	Completed successfully	09/03/2024 15:45:50

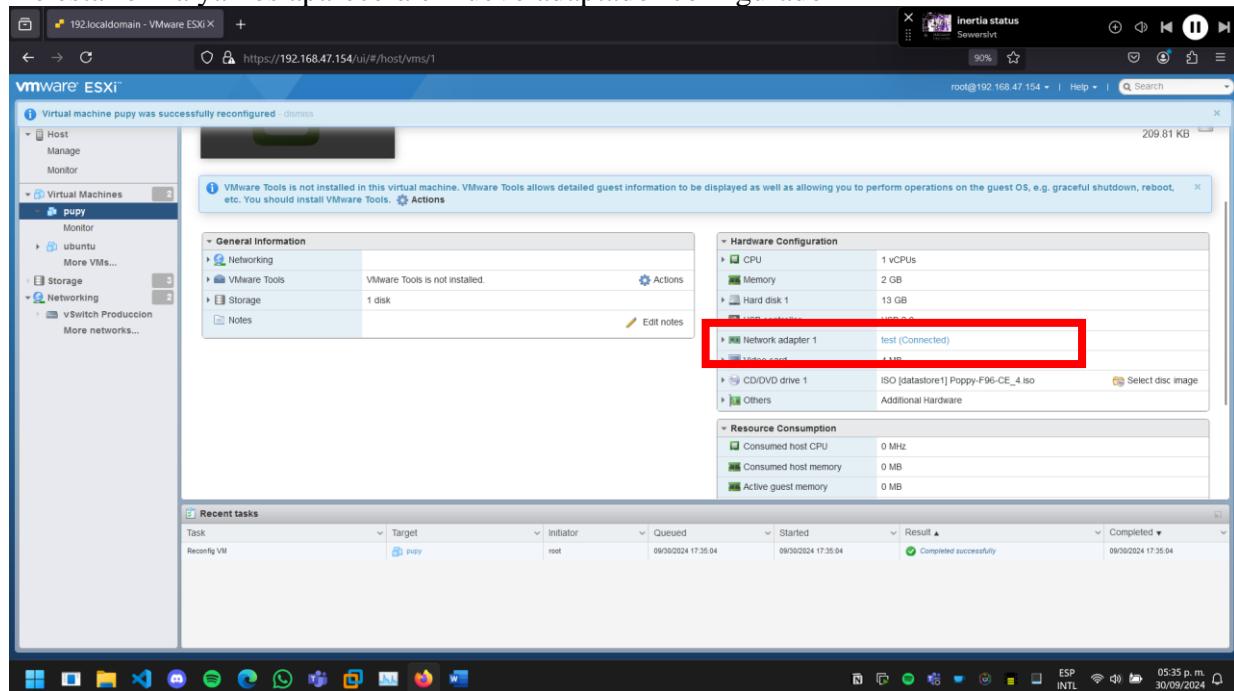
Una vez dentro ingresamos en “Edit”

The screenshot shows the 'Edit' screen for the 'pupy' virtual machine. The top navigation bar indicates the target is 'pupy'. The main content area shows the 'pupy' VM settings, including Guest OS (Other Linux), Compatibility (ESXi 6.7 virtual machine), CPU (1 vCPU), Memory (2 GB), and Storage (1 disk). A note states 'VMware Tools is not installed in this virtual machine. VMware Tools allows detailed guest information to be displayed as well as allowing you to perform operations on the guest OS, e.g. graceful shutdown, reboot, etc. You should install VMware Tools.' Below the settings, there are two tabs: 'General Information' and 'Hardware Configuration'. The 'General Information' tab shows Networking (VMware Tools not installed) and Storage (1 disk). The 'Hardware Configuration' tab lists CPU (1 vCPU), Memory (2 GB), Hard disk 1 (13 GB), USB controller (USB 2.0), Network adapter 1 (VM Network (Connected)), Video card (4 MB), and CD/DVD drive 1 (ISO file ISO1dastore11\_Popov-F96-CE\_4.iso). At the bottom, a 'Recent tasks' table shows completed system updates. The taskbar at the bottom of the screen is visible.

Aquí nos vamos a las opciones de adaptador de red y seleccionamos el adaptador que creamos anteriormente.



De esta forma ya nos aparecerá el nuevo adaptador configurado



## Aplicación web

### Wordpress

Primero necesitamos tener instalados apache, php y mysql, en la maquina en la que queramos tener el wordpress. Una vez tengas estos servicios, podemos comenzar con la creación de la base de datos que usara la página wordpress. Primero accedemos a la consola de mysql con:

```
sudo mysql -u root -p
```

Aquí creamos la base de datos que vamos a usar:

```
CREATE DATABASE wordpress;
CREATE USER 'wordpressuser'@'localhost' IDENTIFIED BY 'password';
GRANT ALL PRIVILEGES ON wordpress.* TO 'wordpressuser'@'localhost';
FLUSH PRIVILEGES;
EXIT;
```

```
uraas@uraas:~$ sudo mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 10
Server version: 8.0.39-0ubuntu0.22.04.1 (Ubuntu)

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

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

mysql> CREATE DATABASE wordpress;
Query OK, 1 row affected (0,01 sec)

mysql> CREATE USER 'wordpressuser'@'localhost' IDENTIFIED BY 'password';
Query OK, 0 rows affected (0,01 sec)

mysql> GRANT ALL PRIVILEGES ON wordpress.* TO 'wordpressuser'@'localhost';
Query OK, 0 rows affected (0,01 sec)

mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0,01 sec)

mysql> EXIT
Bye
```

Una vez hecho este paso, ahora si procedemos a la descarga de worpress, no sin antes movernos al directorio /tmp:

```
cd /tmp
```

Ahora descargamos el archivo:

```
wget https://wordpress.org/latest.tar.gz
```

```
uraas@uraas:/tmp$ wget https://wordpress.org/la
test.tar.gz
-- 2024-10-12 04:35:39 -- https://wordpress.org/
latest.tar.gz
Resolving wordpress.org (wordpress.org) ... 198.
143.164.252
Connecting to wordpress.org (wordpress.org)|198
.143.164.252|:443... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 24640061 (23M) [application/octet-stream]
Saving to: 'latest.tar.gz'
```

Procedemos a descomprimir el archivo en el directorio /tmp:

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

Y movemos los archivos de WordPress al directorio de Apache:

```
sudo mv wordpress /var/www/html/wordpress
```

También configuramos los permisos necesarios:

```
sudo chown -R www-data:www-data /var/www/html/wordpress
sudo chmod -R 755 /var/www/html/wordpress
```

```
uraas@uraas:/tmp$ sudo chown -R www-data:www-data
/var/www/html/wordpress
uraas@uraas:/tmp$ sudo chmod -R 755 /var/www/html/wordpress
restart apache2
```

Continuamos con la configuración de apache para wordpress, para ello creamos un archivo de configuración para el sitio de WordPress:

```
sudo nano /etc/apache2/sites-available/wordpress.conf
```

Que tendrá el siguiente contenido:

```
<VirtualHost *:80>
    ServerAdmin admin@example.com
    DocumentRoot /var/www/html/wordpress
    ServerName example.com
    ServerAlias www.example.com

    <Directory /var/www/html/wordpress/>
        AllowOverride All
    </Directory>

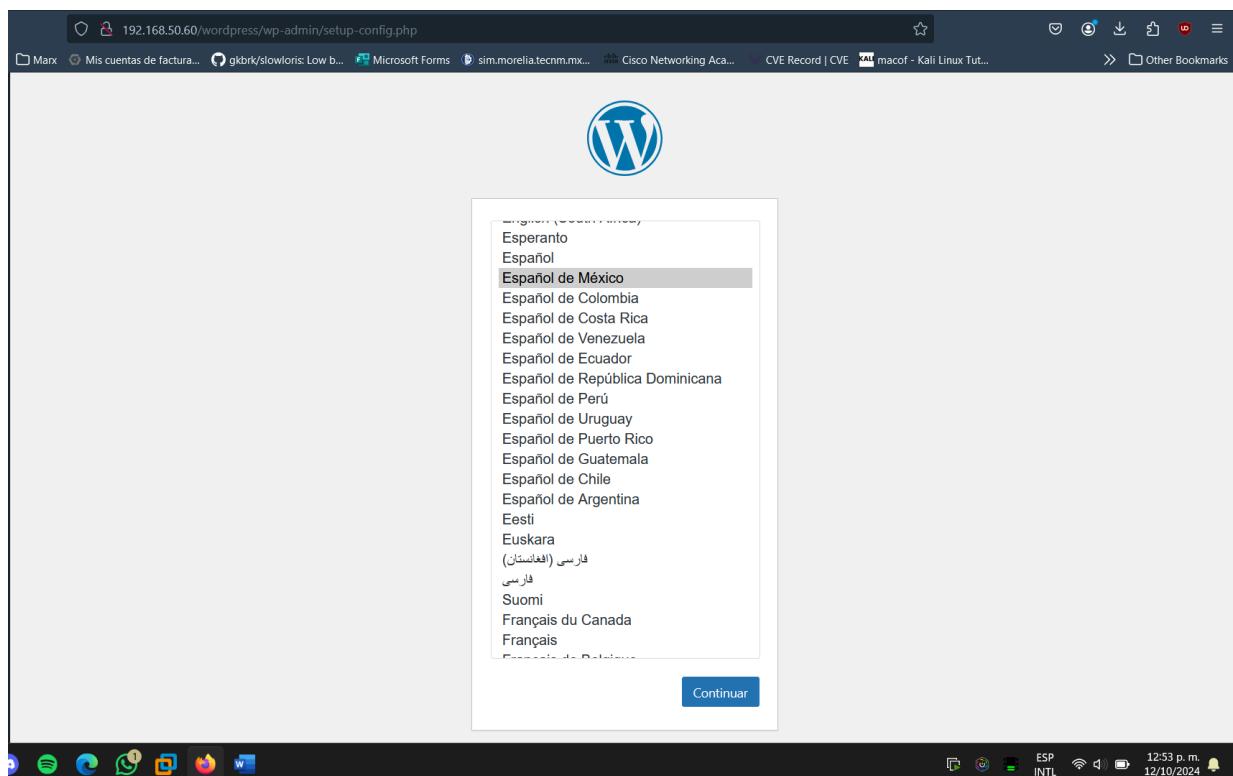
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Ahora habilitamos la configuración y el módulo rewrite:

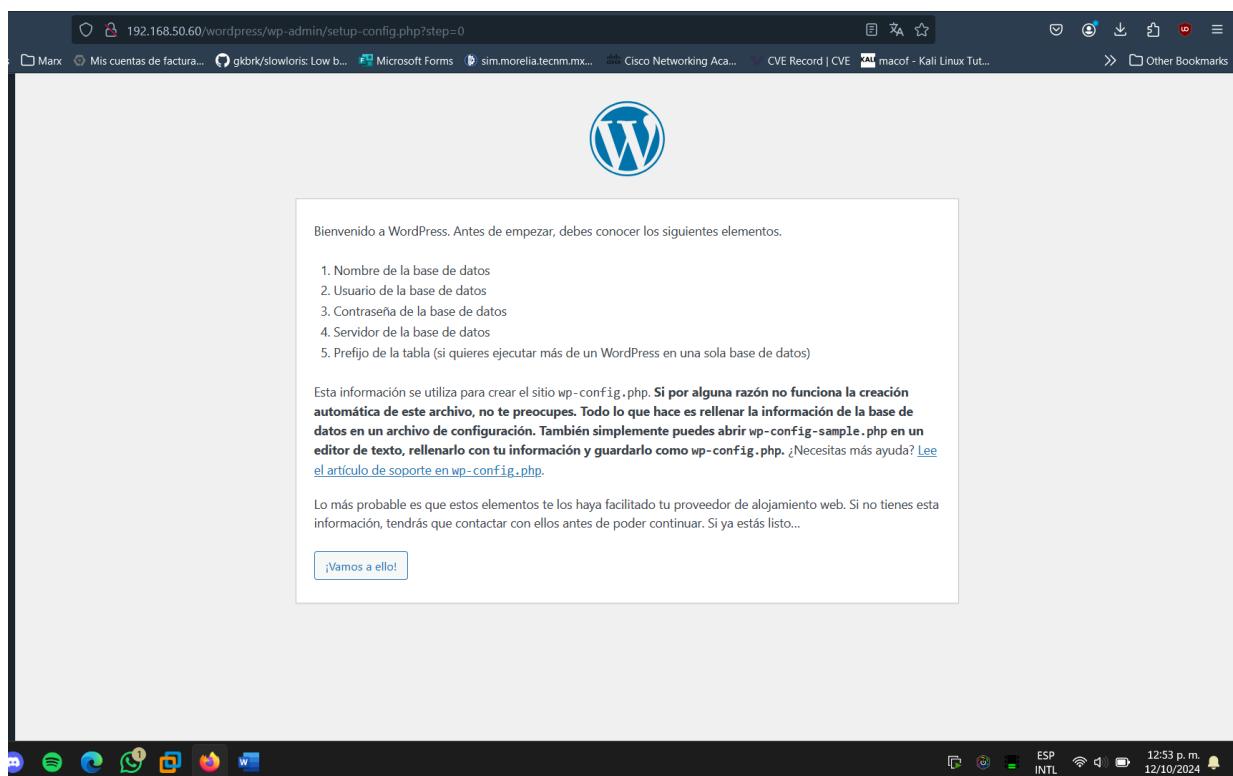
```
sudo a2ensite wordpress.conf
sudo a2enmod rewrite
sudo systemctl reload apache2
sudo systemctl restart apache2
```

```
uraas@uraas:~$ sudo a2ensite wordpress.conf
Enabling site wordpress.
To activate the new configuration, you need to run:
  systemctl reload apache2
uraas@uraas:~$ sudo a2enmod rewrite
Enabling module rewrite.
To activate the new configuration, you need to run:
  systemctl restart apache2
uraas@uraas:~$ sudo systemctl reload apache2
uraas@uraas:~$ sudo systemctl restart apache2
uraas@uraas:~$
```

Para continuar con la configuración ingresamos a la dirección <http://localhost/wordpress>



- Aquí solo seleccionamos el idioma de la pagina



Aquí ingresamos los datos para que realice la conexión con la base de datos:

A continuación tendrás que introducir los detalles de tu conexión con la base de datos. Si no estás seguro de ellos, contacta con tu proveedor de hosting.

**Nombre de la base de datos**  El nombre de la base de datos que quieras usar con WordPress.

**Nombre de usuario**  El nombre de usuario de tu base de datos.

**Contraseña**   La contraseña de tu base de datos.

**Servidor de la base de datos**  Si localhost no funciona, deberás poder obtener esta información de tu proveedor de hosting.

**Prefijo de tabla**  Si quieres ejecutar varias instalaciones de WordPress en una sola base de datos cambia esto.

Y ahora nos pide los datos, pero para la página:

¡Bienvenido al famoso proceso de instalación de WordPress en cinco minutos! Simplemente completa la información siguiente y estarás a punto de usar la más enriquecedora y potente plataforma de publicación personal del mundo.

### Información necesaria

Por favor, proporciona la siguiente información. No te preocupes, siempre podrás cambiar estos ajustes más tarde.

**Título del sitio**

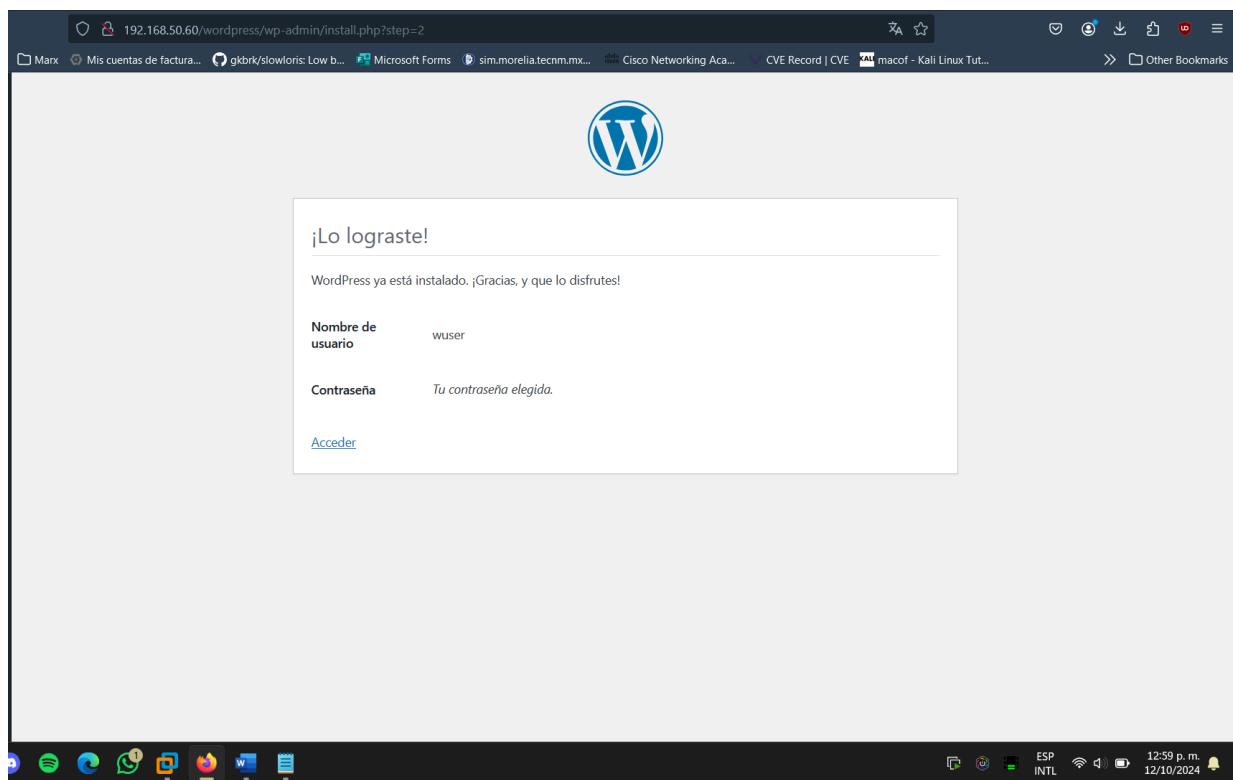
**Nombre de usuario**  Los nombres de usuario pueden tener únicamente caracteres alfanuméricos, espacios, guiones bajos, guiones medios, puntos y el símbolo @.

**Contraseña**     
 Fuerte

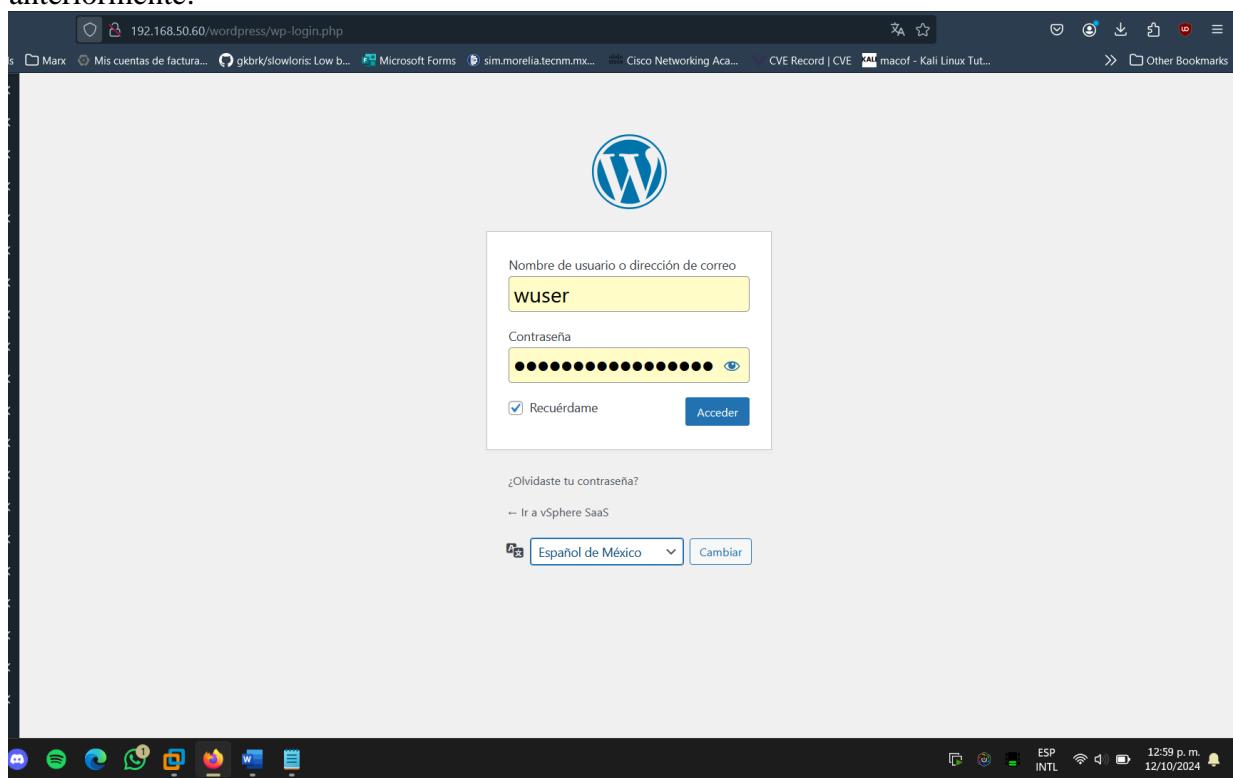
**Importante:** Necesitas esta contraseña para acceder. Por favor, guárdala en un lugar seguro.

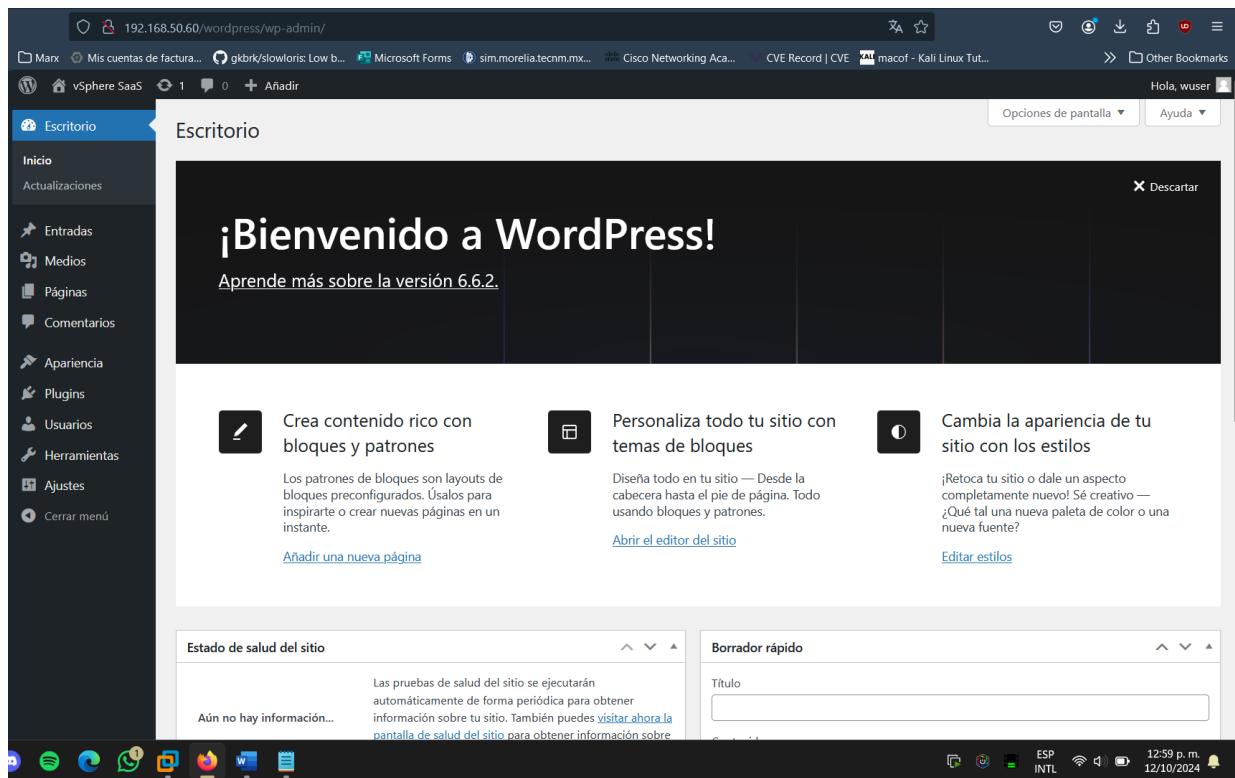
**Tu correo electrónico**  Comprueba bien tu dirección de correo electrónico antes de continuar.

**Visibilidad en los motores de búsqueda**  Disuade a los motores de búsqueda de indexar este sitio  
Depende de los motores de búsqueda atender esta petición o no.



Una vez concluido el proceso, ingresamos con el usuario y contraseña que creamos anteriormente:





Y ahora como vemos en la base datos ya está nuestra base de datos

```
mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| sys |
| wordpress |
+-----+
5 rows in set (0,01 sec)
```

También sus tablas creadas

```
mysql> show tables;
+-----+
| Tables_in_wordpress |
+-----+
| wp_commentmeta |
| wp_comments |
| wp_links |
| wp_options |
| wp_postmeta |
| wp_posts |
| wp_term_relationships |
| wp_term_taxonomy |
| wp_termmeta |
| wp_terms |
| wp_usermeta |
| wp_users |
+-----+
```

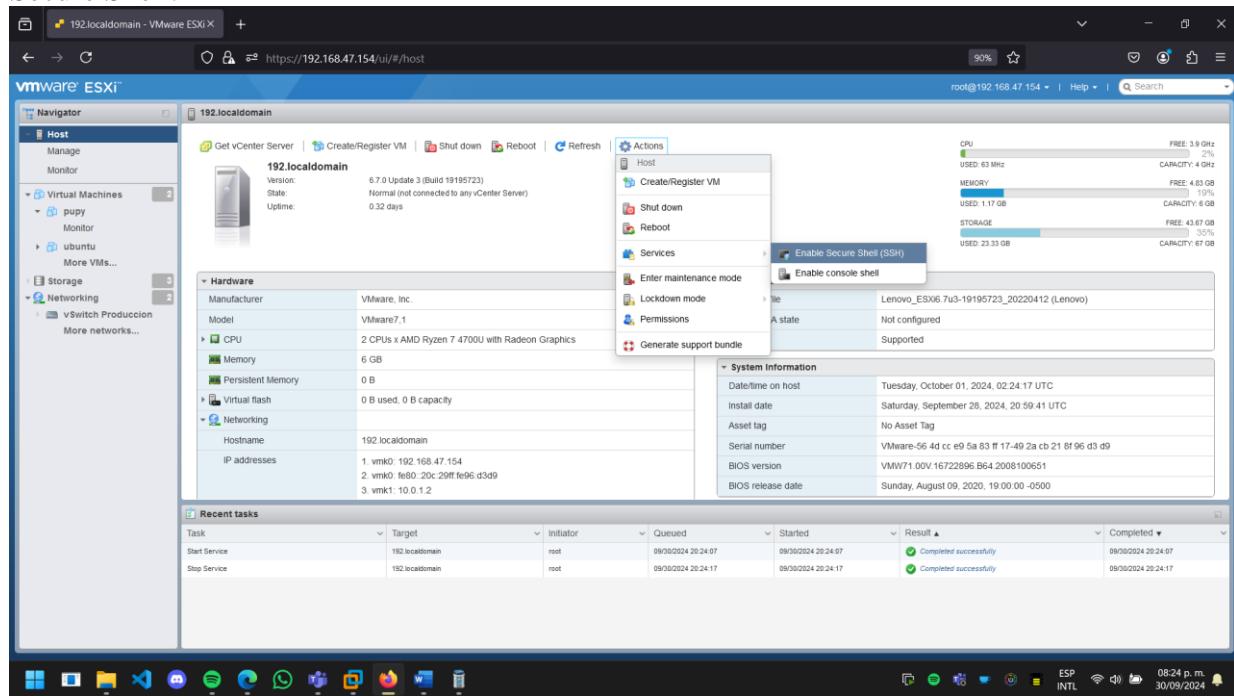
Y el usuario que acabamos de ingresar

```
mysql> select * from wp_users;
+----+-----+-----+-----+-----+-----+-----+
| ID | user_login | user_pass | user_registered | user_activation_key | user_status | display_name |
+----+-----+-----+-----+-----+-----+-----+
| 1 | wuser | $P$BDSSr6L7JfPZKjoPsQiTO.giL/4ukYd0 | 2024-10-12 18:58:57 | wuser | 0 | wuser |
+----+-----+-----+-----+-----+-----+-----+
1 row in set (0,00 sec)
```

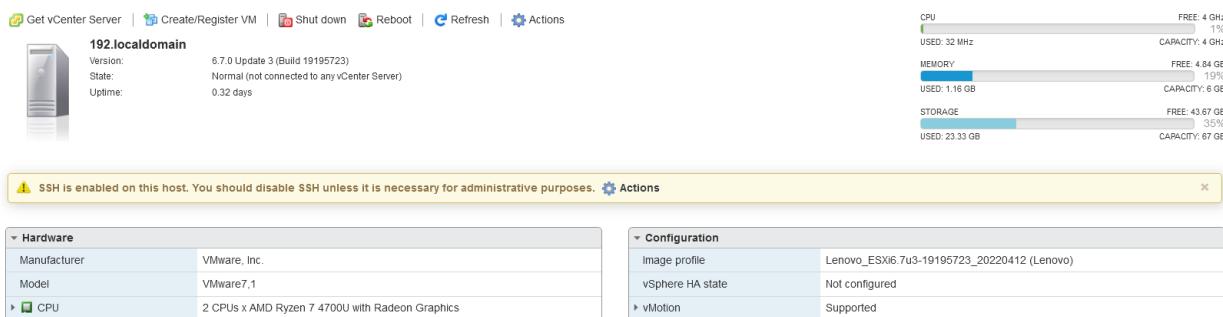
## Servicios

### SSH ESXi

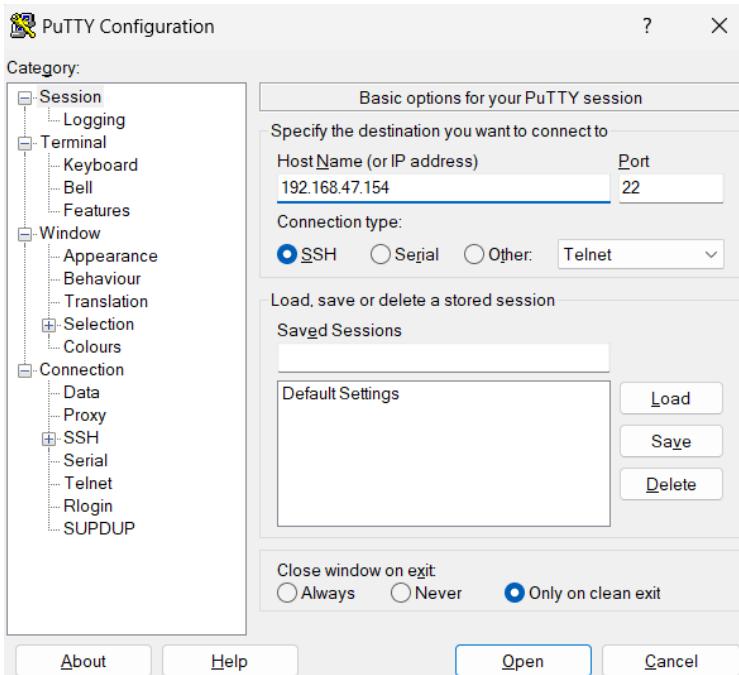
Para activar el SSH, primero debemos de dirigirnos a Host > Actions > Services > Enable Secure Shell.



Una vez lo activemos nos aparecerá el mensaje de que esta activado



Ahora para probarlo solo debemos de establecer la conexión, en mi caso usare el programa PuTTy para hacer la conexión.



Una vez establecida la conexión nos pide el usuario y contraseña.

```

login as: root
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
vSphere Security documentation for more information.
[root@192:~] 

```

- Otra forma de iniciar el servicio SSH es a través del administrador en el Web Client.

**localhost.localdomain - Manage**

Services

Name	Description	Status
crond	cron daemon	Stopped
sldp	sldp	Stopped
snmpd	SNMP Server	Stopped
TSM	ESXi Shell	Stopped
TSM-SSH	SSH	Stopped
vmsvslload	Svslod Server	Running

The service TSM-SSH was successfully started - dismiss

- Solo hay que buscar el servicio TSM-SSH y darle en Start

**sftp://root@192.168.50.154 - FileZilla**

Archivo Edición Ver Transferencia Servidor Marcadores Ayuda

Servidor: sftp://192.168.50.154 Nombre de usuario: root Contraseña: ..... Puerto: Conexión rápida

Estado: Connected to 192.168.50.154  
 Estado: Recuperando el listado del directorio...  
 Estado: Listing directory /  
 Estado: Directorio "/" listado correctamente

Sitio local:	Sitio remoto:
C:\Users\rogel\	/
..	
Users	altbootbank
All Users	bin
Default	bootbank
Default User	dev
Public	etc
rogel	lib
Windows	lib64
XboxGames	

Nombre de archivo	Tamaño ...	Tipo de archivo	Última modif...	Permisos	Propietar...
..					
.android	Carpetas de arc...	Carpetas de arc...	27/07/2024 09...		
.arduinoIDE	Carpetas de arc...	Carpetas de arc...	31/05/2024 12...		
.cache	Carpetas de arc...	Carpetas de arc...	11/05/2024 02...		
.codetogether	Carpetas de arc...	Carpetas de arc...	27/06/2024 01...		
.dia	Carpetas de arc...	Carpetas de arc...	21/02/2024 09...		
.m2	Carpetas de arc...	Carpetas de arc...	17/03/2024 01...		
.imutils	Carpetas de arc...	Carpetas de arc...	01/07/2024 02...		
.ms-ad	Carpetas de arc...	Carpetas de arc...	04/02/2024 05...		
.nbi	Carpetas de arc...	Carpetas de arc...	17/03/2024 01...		
.openjfx	Carpetas de arc...	Carpetas de arc...	25/07/2024 04...		
18 archivos y 52 directorios. Tamaño total: 30,078,457 bytes					
1 directorio seleccionado.					

Servidor/Archivo local Direc... Archivo remoto Tamaño Priori... Estado

## SSH Ubuntu

### 1. Abre una terminal:

- Puedes acceder a la terminal desde el menú de aplicaciones o presionando Ctrl+Alt+T.

### 2. Actualiza los paquetes:

```
sudo apt update && sudo apt upgrade
```

### 3. Instala el servidor SSH:

```
sudo apt install openssh-server
```

```
root@ubuntu:/home/ubuntu# apt install openssh-server
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  libwrap0 ncurses-term openssh-sftp-server ssh-import-id
Paquetes sugeridos:
  molly-guard monkeysphere ssh-askpass
Se instalarán los siguientes paquetes NUEVOS:
  libwrap0 ncurses-term openssh-server openssh-sftp-server ssh-import-id
0 actualizados, 5 nuevos se instalarán, 0 para eliminar y 4 no actualizados.
Se necesita descargar 879 kB de archivos.
Se utilizarán 6.857 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
```

### 4. Habilita e inicia el servicio SSH:

```
sudo systemctl enable ssh
sudo systemctl start ssh
```

```
root@ubuntu:/home/ubuntu# systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh
Created symlink /etc/systemd/system/sshd.service → /usr/lib/systemd/system/ssh.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /usr/lib/systemd/system/ssh.service.
root@ubuntu:/home/ubuntu# system start ssh
Command 'system' not found, did you mean:
  command 'systemd' from deb systemd (255.4-1ubuntu8.4)
  command 'system3' from deb simh (3.8.1-6.1)
Try: apt install <deb name>
root@ubuntu:/home/ubuntu# systemctl start ssh
root@ubuntu:/home/ubuntu# _
```

### 5. Comprobar status de SSH

```
systemctl status ssh
```

```
root@ubuntu:/home/ubuntu# systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
  Active: active (running) since Wed 2024-10-09 05:26:45 UTC; 15min ago
TriggeredBy: ● ssh.socket
    Docs: man:sshd(8)
           man:sshd_config(5)
  Process: 11099 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 11101 (sshd)
   Tasks: 1 (limit: 1068)
  Memory: 2.2M (peak: 3.1M)
    CPU: 70ms
   CGroup: /system.slice/ssh.service
           └─11101 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

oct 09 05:26:45 ubuntu systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
oct 09 05:26:45 ubuntu sshd[11101]: Server listening on :: port 22.
oct 09 05:26:45 ubuntu systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
oct 09 05:31:31 ubuntu sshd[11108]: Accepted password for ubuntu from 192.168.50.1 port 64102 ssh2
oct 09 05:31:31 ubuntu sshd[11108]: pam_unix(sshd:session): session opened for user ubuntu(uid=1000)>
```

## Crea un par de llaves RSA

1. Primero vamos a editar el archivo de configuración que se encuentra en:

```
sudo nano /etc/ssh/ssh_config
```

- Aquí agregamos la línea para especificar el puerto que usara el SSH, el cual por defecto es el 22, lo cambiamos al 1101.

```
# This is the ssh client system-wide configuration file. See
# ssh_config(5) for more information. This file provides defaults for
# users, and the values can be changed in per-user configuration files
# or on the command line.

# Configuration data is parsed as follows:
# 1. command line options
# 2. user-specific file
# 3. system-wide file
# Any configuration value is only changed the first time it is set.
# Thus, host-specific definitions should be at the beginning of the
# configuration file, and defaults at the end.

# Site-wide defaults for some commonly used options. For a comprehensive
# list of available options, their meanings and defaults, please see the
# ssh_config(5) man page.

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

Port 1101

Host *
# ForwardAgent no
# ForwardX11 no
# ForwardX11Trusted yes
# PasswordAuthentication yes
# HostbasedAuthentication no
# GSSAPIAuthentication no
# GSSAPIDelegateCredentials no
# GSSAPIKeyExchange no
# GSSAPITrustDNS no
# BatchMode no
# CheckHostIP no
# AddressFamily any
# ConnectTimeout 0
# StrictHostKeyChecking ask
Desactivar la introducción de la contraseña
# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication no
#PermitEmptyPasswords no
```

2. Ahora reiniciamos el servicio SSH para que los cambios se apliquen.

```
sudo service sshd restart
```

3. Generamos un par de claves públicas y privadas.

```
root@ubuntu:/home/ubuntu# cd /etc/ssh/
root@ubuntu:/etc/ssh# ssh-keygen
Generating public/private ed25519 key pair.
Enter file in which to save the key (/root/.ssh/id_ed25519):
/root/.ssh/id_ed25519 already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_ed25519
Your public key has been saved in /root/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:DKCf6Kv/P18r8QkC99kAKUjF23ULrV/ftZQW02tCISM root@ubuntu
The key's randomart image is:
+--[ED25519 256]--+
| .oo... . |
| . .oo. o E o . . |
| ..o.o + o o . .+ |
| .+o.+ . . . * . |
| .oo. +S . o + = |
| . . = ... o = |
| . . +.. o |
| ...o. |
| .oooooo... |
+---[SHA256]---+
root@ubuntu:/etc/ssh#
```

4. Transferir clave publica al servidor

- Primero comprobamos que podemos acceder al servidor por ssh con contraseña desde un cliente.

```
(kali㉿kali)-[~] 4096 Oct  7 01:50 Templates
$ ssh ubuntu@192.168.50.40 -p 1101 11:50 Videos
The authenticity of host '[192.168.50.40]:1101 ([192.168.50.40]:1101)' can't be established.
ED25519 key fingerprint is SHA256:Nti5+6+NdjXldu4ThHYLL8HDxLr76jj9EKoCtxsPbxA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.50.40]:1101' (ED25519) to the list of known hosts.
ubuntu@192.168.50.40's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-122-generic x86_64)

 * Documentation: https://help.ubuntu.com/22.04.5/pub
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

System information as of mié 09 oct 2024 12:49:49 UTC
System load: 0.0  ac11ZDI1NTE5AA Processes: 51KQFXD2pEULT0H202vh6wNm/xGE/HQK
Usage of /: 48.5% of 9.75GB  Users logged in: 1
Memory usage: 23%          IPv4 address for ens160: 192.168.50.40
Swap usage: 0%  .ssh/  BEGIN OPENSSH PRIVATE KEY
El mantenimiento de seguridad expandido para Applications está desactivado
Se pueden aplicar 11 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable
Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute «sudo pro status»

New release '24.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Wed Oct  9 12:35:43 2024
```

- Nos preguntará si queremos hacer la conexión, a lo que respondemos “yes”. Ya luego solo comprobamos que si se pudo conectar al servidor.

```
ubuntu@ubuntu:~$ whoami
ubuntu
```

- Generar llaves pública y privada para el cliente
  - Primero ingresamos a la carpeta /home/nombreusuario/.ssh

```
(kali㉿kali)-[~/ssh] 4096 Oct  7 01:50 Templates
$ llx-r-x 2 kali kali 4096 Oct  7 01:50 Videos
total 8
-rw-r-- 1 kali kali 2934 Oct  9 08:49 known_hosts
-rw-r-- 1 kali kali 2098 Oct  9 08:49 known_hosts.old
```

- Como vemos aún no se encuentra ninguna llave generada, los únicos dos archivos que están fueron creados al establecer la conexión.
- Ahora si podemos generar las llaves
  - Importante agregar -t rsa para que la clave sea compatible

```
(kali㉿kali)-[~/ssh]$ ssh-keygen -t rsa 4096 Oct  7 01:50 Downloads
$ ssh-keygen -t rsa 4096 Oct  7 01:50 Music
Generating public/private rsa key pair.
Enter file in which to save the key (/home/kali/.ssh/id_rsa):
Enter passphrase for "/home/kali/.ssh/id_rsa" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/kali/.ssh/id_rsa
Your public key has been saved in /home/kali/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:+Kg0laDoRXecwWENBnY+TAGfYhZt9PJwXL+Pr19AjWY kali@kali
The key's randomart image is:
+---[RSA 3072]---+
|total =*@= . |
|rw-. @+* .. kali kali 444 Oct  9 07:18 id_ed25519 |
|rw-..=% +1 k.Ei.. kali 91 Oct  9 07:18 id_ed25519.pub |
|rw...+.00* 1 k+.i kali 1956 Oct  9 01:48 known_hosts |
|rw...+ S.i kali kali 1120 Oct  9 01:48 known_hosts.old |
|... . o o. |
|... o . . . kali . . . ssh] |
+$ .o id_ed25519.pub |
|sh-ed25519 AAAo zaC1lZDI1NTESAAAAIFEToRsZ51kQFxD2pEULT0HNuvvh6wNm/xGE |
+---[SHA256]---+
(kali㉿kali)-[~/ssh]
```

- Y ya nos generó los archivos:

```
(kali㉿kali)-[~/ssh]
$ ll id_ed25519
total 16
-rw-r----- 1 kali kali 2590 Oct  9 08:56 id_rsa
-rw-r--r-- 1 kali kali 1563 Oct  9 08:56 id_rsa.pub
-rw-r----- 1 kali kali 2934 Oct  9 08:49 known_hosts
-rw-r----- 1 kali kali 2098 Oct  9 08:49 known_hosts.old
```

- El archivo que nos interesa es id\_rsa.pub, el cual copiamos su contenido en el portapapeles.

```
(kali㉿kali)-[~/ssh] cat id_rsa.pub
AAAAB3NzaC1yc2EAAAQABAAABgQChFZanE/z34/Pt2CsNK11Sx00x9qcb0V+dWrJ32mYYumWyNqXe6v00Sfl47MLgGs5xosUx6BxXvHdxEAdMJjKBRZFbq2Keznq/Faj9Zh9amux22rPJKPHHKyODsDsT15sUfuyzT79YnWfpfcnICsTTFAVvwlhT8IECiBqxqYk/VRdulEzG1LxCY+MEhfI69y6evZE3Tw41hCuJvgifVOqw7MrpXfw3xI56IAgM+Nlq6hK6hb1rG7cqhqUrA+1GgHBZA+8Jqa8fJ0bnMa++0= kali@kali
```

## 7. Autenticar usando llaves SSH

- Para esto tenemos que conectarnos en nuestro servidor y vamos a la ubicación de /home/nombreusuario/.ssh/

```
ubuntu@ubuntu:~$ cd /home/ubuntu/.ssh/
ubuntu@ubuntu:~/ssh$ ll
total 16
drwxr-x--- 2 ubuntu ubuntu 4096 oct  9 12:46 ./
drwxr-x--- 5 ubuntu ubuntu 4096 oct  9 12:50 ../
-rw-r----- 1 ubuntu ubuntu 560 oct  9 12:32 authorized_keys
-rw-r----- 1 ubuntu ubuntu 2602 oct  9 12:46 id_rsa
-rw-r--r-- 1 ubuntu ubuntu 567 oct  9 12:46 id_rsa.pub
ubuntu@ubuntu:~/ssh$ nano authorized_keys
```

- Luego procedemos a editar el archivo de authorized\_keys, pegando la key del cliente y guardando los cambios.

```
GNU nano 6.2
/home/ubuntu/.ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQChFZanE/z34/Pt2CsNK11Sx00x9qcb0V+dWrJ32mYYumWyNqXe6v00Sfl47MLgGs5xosUx6BxXvHd>
```

- Quedando de esta forma, luego procedemos a cerrar la sesión ssh.

```
ubuntu@ubuntu:~/ssh$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQChFZanE/z34/Pt2CsNK11Sx00x9qcb0V+dWrJ32mYYumWyNqXe6v00Sfl47MLgGs5xosUx6BxXvHd
EAdMjkBRZFbz2Kezng/Faj92h9amux22rPJkPHKKy0bsDsDt15sUfuyzT79YnWfpfcnICsTTFAVvwlhT8IECiBqxqYk/VRdulEzG1LxCY+MEhf169y6
evZE3Tw41hCuJvgifV0qwm7MrpXfw3xI56IAgM+Nlq6h6hb1rG7cqhUrA+16gHBZA+8Jqa8fJ0bnMa++0= kali@kali
ubuntu@ubuntu:~/ssh$ exit
oct  9 05:18 id_rsa.pub
logout
Connection to 192.168.50.40 closed.
```

- Listo ya podemos iniciar sesión desde nuestro cliente sin tener que ingresar la contraseña.

```
(kali㉿kali)-[~] ~$ ssh ubuntu@192.168.50.40 -p 1101 ago 27 14:21 vconsole.conf → default/keyboard
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-122-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: root https://landscape.canonical.com/getrc
 * Support: 4 root https://ubuntu.com/pro
System information as of mié 09 oct 2024 13:44:35 UTC
System load: 0.04 root      Processes:426 zsh_command203ot_found
Usage of /: 48.5% of 9.75GB   Users logged in:      1
Memory usage: 24%           IPv4 address for ens160: 192.168.50.40
Swap usage: 0%             

El mantenimiento de seguridad expandido para Applications está desactivado.

Se pueden aplicar 11 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable
Connection to 192.168.50.40 closed by remote host.

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute «sudo pro status»
New release '24.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Wed Oct  9 12:59:01 2024 from 192.168.50.131
```

- De esta forma generamos llaves para cada maquina y las agregamos en authorized\_keys

```
upaa$@upaa:~$ cat .ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAABgQCvZXV9qkRLKogzQYKACCJ86hfde9684uuRj4+tn0lnxp8q6H4Z8NFnWnqMhKLKPw6ptyO+SRH1x
6000hCDuekgMT7/Rb7ybNcwsaBAChg5K3S6T8Zauiygm1ZMvl0dwYyVahQse0kI0nGFiLcJFnxWwydIFksKf1KOYFAFUMxU4fVmDQuE6hHRB1jtUaihP
Bnv/cqZXBvNqOuqmrBmp0MjIHd8tpFj0aAt0yeshVR3HNRgSpmfK4/DEct0Mvg/Qtv3up4r6s35vLI/62909IVoEMtfGbur1k0p/9pPNMpcy74J89l
amGn1wV+u8wiUbdabRhnmqOTAvp0uB6LTfPiXrxXCRdWqopodn482ANFvcrFR57Sbb907Pdj4hRgWZJBpb3RA0tiiFif6u7ZnZpJ0ctRJOADEFPwf3y
cqYDnGcBiQko403upmDdJ2KCMBeS9hJG1z4a23GTcGM7PY0id4DAx09U4xSG+jhyCSF+sEwNaTzeMtujbAlNxvc= ubuntu@ubuntu
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAABgQD0Ms3rES1Rz4os88Rn0yonU0ya0cT7xLs0zj7JlIg/Ik5x+/KdijocTJOA8eU17gYzpX/GRcSezh0
l+ayq6Ap0EadPi4t/g36CH5JW0KYCOhYnGmE7df+Fv8A2LMD1yzYcqtwEqhpvAMOKUT09GzkeK3VqVw4oLRSQVnhGc86PcvgCUuzl0FwnGd/G9Epa282
aIKMU2UzDqMvk8BaieLtgao0VGQ433jPdLPSRmbng8JTZjHuMK85ktpsh9XwsVhy+v5EhmWR3N6ex3cei52KuntoKD7Zgx9guz9Pfr1IuHTWlZ0Fi
C8t+P5jE7cPS/Z564LoYMhijB9NUphMThuTDrprIiRy4Sg2sGIJG9MqISDwyuilyx8msX1xb6Tt6/lmGIi36cWNDOjjPPBDAvK3pEYfKQ+R4Pyd8iZeD
h4MKSSeIT6LTBpLbh6znj4htqtoNGHFs4qzsjp7+a5ckpMp5/JMxb037iLN8oZTxAuBCPXi4dNkXU7jsNLH+HeU= uraa$@uraas
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAABgQChFZanE/z34/Pt2CsNK11Sx009qcb0V+dWrJ32mYYumWyNqXe6v00Sfl47MLgGs5xosUx6BxVhDx
UYvNDja3C69upEwQRpft8h7YE3rRviikFQozEDXBLR2qe1RR6cTNCuIuqstL5rXJpIgFrTTBkgBEFZ90I9CYNMe2VlMs+QCb7u9kjSL6mdEai44k
IHmEAdMjJKBRZFbz22Kezqnf/Faj9Zh9amux22rPJPKPHHKy0DsDsT15sUfuyzT79YnWfpfcnICsTTFAVvwlhT8IECiBqxqYk/VRduIezG1LxCY+MEhfl6
9y6KQo+DeBLwbsR6A3bRnHgK9fxNCXimuCECM1CNCygeua0e1E0IsQzEncRXHQnN2J3e5WY7k7BF7LXNRhOU3IpwiLGxH/713UbbDsRJ6e3rPeeA9F6Y
464B6levZE3Tw41hCuJvgifV0qw7Mrpxfw3xI56IAgM+Nlq6hK6hb1rG7cqhUrA+1GgHBZA+8Jqa8fJ0bnMa++= kali@kali
upaa$@upaa:~$
```

## Apache en Ubuntu (PaaS):

- Para instala el servidor web Apache:

```
sudo apt install apache2
```

- Ahora pasamos a habilitar Apache:

```
sudo systemctl enable apache2
sudo systemctl start apache2
```

- Verificamos es estatus de Apache:

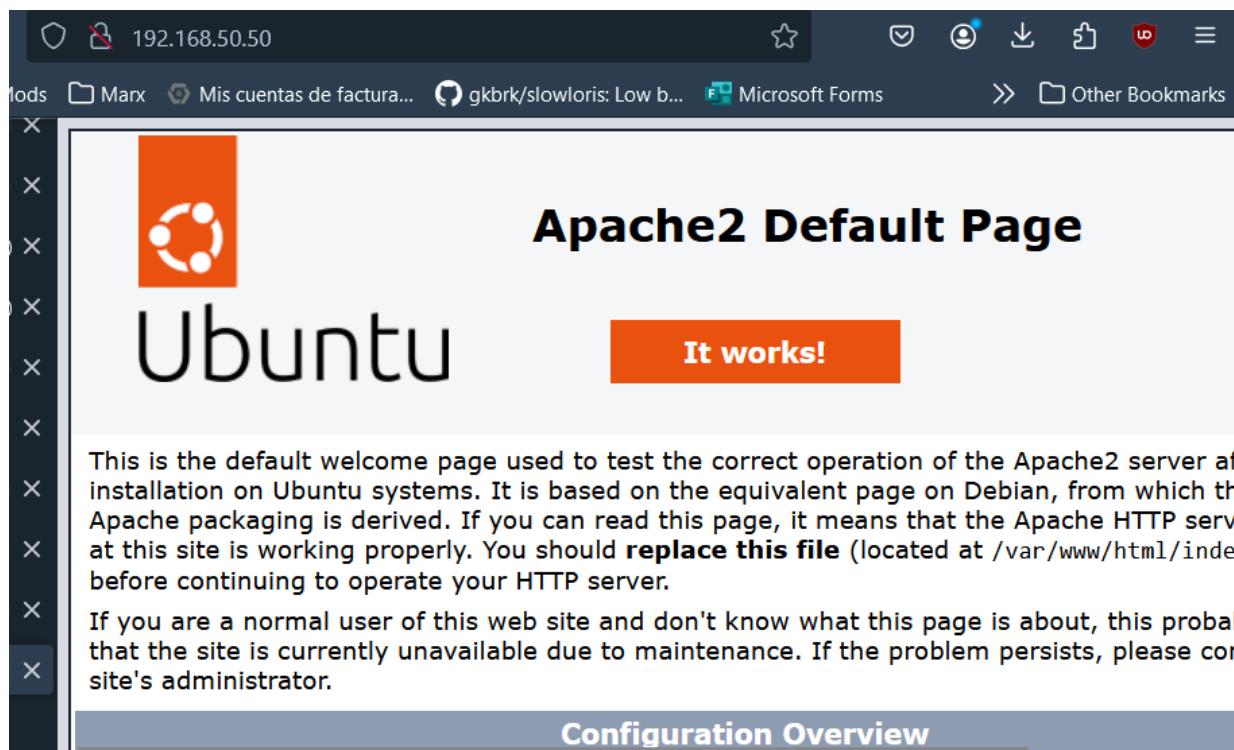
```
sudo systemctl status apache2
```

```
upaa$@upaa:~$ sudo systemctl status apache2
[sudo] password for upaa: You have an error in your SQL syntax; check the manual that corresponds to your
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2024-10-12 01:06:03 UTC; 48min ago
     Docs: https://httpd.apache.org/docs/2.4/
    Process: 742 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 846 (apache2) 0,01 sec)
      Tasks: 6 (limit: 1018)
     Memory: 21.5M
    CPU: 4.304ms You have an error in your SQL syntax; check the manual that corresponds to your
   CGroup: /system.slice/apache2.service
mysql> CREATE USER 'Sql1234*'@'localhost';
Query OK, 0 rows affected (0.00 sec)

mysql> GRANT ALL PRIVILEGES ON *.* TO 'Sql1234*'@'localhost';
Query OK, 0 rows affected (0.00 sec)

mysql> FLUSH PRIVILEGES;
oct 12 01:06:02 upaa systemd[1]: Starting The Apache HTTP Server ...
oct 12 01:06:03 upaa apachectl[813]: AH00558: apache2: Could not reliably determine the server's name [NameVirtualHost]
oct 12 01:06:03 upaa systemd[1]: Started The Apache HTTP Server.
lines 1-20/20 (END)
```

Ahora ingresamos a la dirección del equipo:



## Base de datos

### MySQL

1. Para instalar el servidor de base de datos MySQL.

```
sudo apt install mysql-server
```

2. Configura MySQL para mejorar la seguridad:

```
sudo mysql_secure_installation
```

Este comando nos da una serie de opciones para asegurar tu instalación de MySQL (como establecer una contraseña para el usuario root de MySQL).

3. Verificamos el estatus de mysql:

```
sudo systemctl status mysql
```

```
upaaS@upaaS:~$ sudo systemctl status mysql
● mysql.service - MySQL Community Server
   Loaded: loaded (/lib/systemd/system/mysql.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2024-10-12 01:06:08 UTC; 1h 0min ago
     Process: 754 ExecStartPre=/usr/share/mysql/mysql-systemd-start pre (code=exited, status=0/SUCCESS)
    Main PID: 971 (mysqld) main@localhost' IDENTIFIED BY 'Sql1234*'
      Status: "Server is operational"
        Tasks: 38 (limit: 1018)
     Memory: 414.4M
        CPU: 30.711s
       CGroup: /system.slice/mysql.service
           mysql> FLUSH LINES 971 /usr/sbin/mysqld
           Query OK, 0 rows affected (0.01 sec)
oct 12 01:06:02 upaaS systemd[1]: Starting MySQL Community Server ...
oct 12 01:06:08 upaaS systemd[1]: Started MySQL Community Server.
[lines 1-14/14 (END)]
```

4. Ahora procedemos a crear un usuario con una contraseña y darle acceso a una base de datos en MySQL, lo primero es ingresar en la consola de MySQL.

```
sudo mysql -u root -p
```

```
upaaS@upaaS:~$ sudo mysql -u root -p
[sudo] password for upaaS:emark of Oracle Corporation and/or its
Sorry, try again. names may be trademarks of their respective
[sudo] password for upaaS:
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \gurrent input statement.
Your MySQL connection id is 9
Server version: 8.0.39-0ubuntu0.22.04.1 (Ubuntu)
                               □
Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.
information_schema
paas
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

5. Procedemos a la creación de una base de datos:

```
CREATE DATABASE paas;
```

```
mysql> SHOW DATABASES;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| sys |
+-----+
4 rows in set (0,02 sec)

mysql> CREATE DATABASE paas;
Query OK, 1 row affected (0,02 sec)
```

```
mysql> SHOW DATABASES;
+-----+
| Database |
+-----+
| information_schema |
| paas |
| performance_schema |
+-----+
3 rows in set (0,01 sec)
```

5. Crea un nuevo usuario con una contraseña segura:

```
CREATE USER 'sql_admin' IDENTIFIED BY 'Sql1234*';
```

```
mysql> CREATE USER 'sql_admin'@'localhost' IDENTIFIED BY 'Sql1234*';
Query OK, 0 rows affected (0,01 sec)
```

6. Ahora, otorgamos todos los privilegios al nuevo usuario sobre la base de datos:

```
GRANT ALL PRIVILEGES ON paas.* TO 'sql_admin'@'localhost';
```

```
mysql> GRANT ALL PRIVILEGES ON paas.* TO 'sql_admin'@'localhost';
Query OK, 0 rows affected (0,00 sec)
```

Para asegurarnos de que MySQL reconozca los nuevos privilegios:

```
FLUSH PRIVILEGES;
```

Para salir de la consola de MySQL, simplemente se escribe:

```
EXIT;
```

7. Listo ahora solo iniciamos sesión con el usuario que hemos creado para comprobar que funcione:

```
mysql -u sql_admin -p
```

```
upaaS@upaaS:~$ mysql -u sql_admin -p
Enter password: Your password does not satisfy the current policy requirements
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 111 sec
Server version: 8.0.39-Ubuntu0.22.04.1 (Ubuntu)

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''sql_admin'' at line 1
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

## PHP

Ahora instalamos PHP junto con algunos módulos comunes:

```
sudo apt install php libapache2-mod-php php-mysql
```

Verificamos que la instalación de haya hecho correctamente:

```
php -v
```

```
uraas@uraas:~$ php -v
PHP 8.1.2-1ubuntu2.19 (cli) (built: Sep 30 2024 16:25:25) (NTS)
Copyright (c) The PHP Group
Zend Engine v4.1.2, Copyright (c) Zend Technologies
    with Zend OPcache v8.1.2-1ubuntu2.19, Copyright (c), by Zend Technologies
```

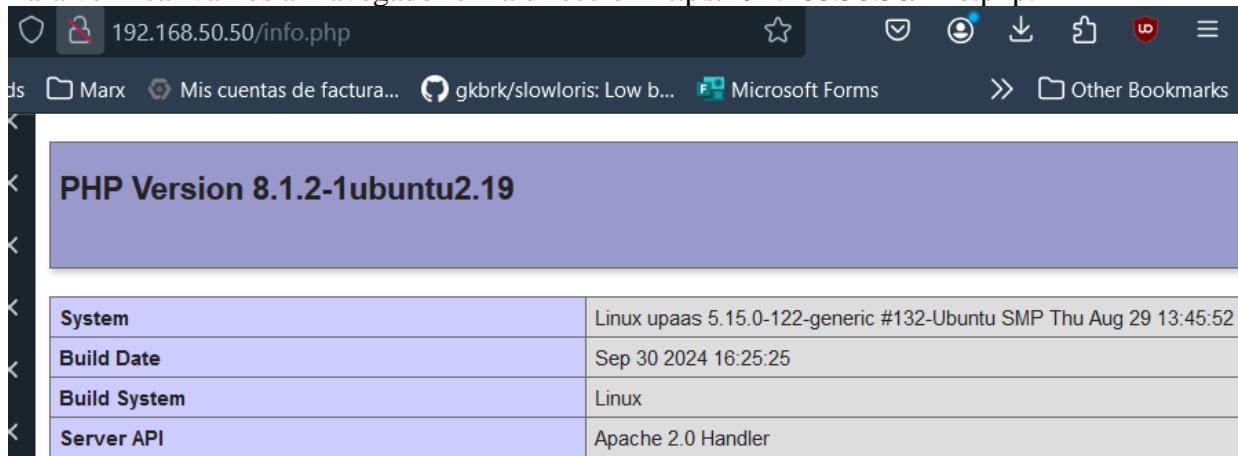
Después de instalar PHP, tenemos que reiniciar Apache para que cargue la configuración:

```
sudo systemctl restart apache2
```

Para probar PHP creamos un archivo de prueba en el directorio raíz de Apache para verificar que PHP esté funcionando correctamente:

```
echo "<?php phpinfo(); ?>" | sudo tee /var/www/html/info.php
```

Para verificar vamos al navegador en la dirección <http://192.168.50.50/info.php>.



## Referencias

1. Linux Console. (s.f.). Cómo establecer una dirección IP estática en Ubuntu Server 20.04.  
<https://es.linux-console.net/?p=12245>
2. DigitalOcean. (s.f.). Cómo configurar las llaves SSH en Ubuntu 18.04.  
<https://www.digitalocean.com/community/tutorials/como-configurar-las-llaves-ssh-en-ubuntu-18-04-es>
3. DigitalOcean. (s.f.). How to install LAMP stack on Ubuntu.  
<https://www.digitalocean.com/community/tutorials/how-to-install-lamp-stack-on-ubuntu>
4. SomeBooks. (s.f.). Establecer una dirección IP estática en Ubuntu Server 20.04.  
<https://somebooks.es/establecer-una-direccion-ip-estatica-en-ubuntu-server-20-04/>
5. CodeFX. (2021, marzo 11). How to configure static IP address on Ubuntu 20.04 [Video].  
YouTube. <https://www.youtube.com/watch?app=desktop&v=IYn6p97B4hI>
6. Alpha Academy. (2022, julio 15). Ubuntu SSH Server setup and configuration [Video].  
YouTube. <https://www.youtube.com/watch?v=dZIg8UOEV0Y>
7. Alfinete Tech. (2023, agosto 10). How to install and configure LAMP stack on Ubuntu [Video].  
YouTube. <https://www.youtube.com/watch?v=UEjxtk-tI2g&list=PLuMd8fg3qBxflEQOl0N2QK1YaUgD26Jvs&index=9>
8. Alfinete Tech. (2023, agosto 17). Enable UFW Firewall and configure ports on Ubuntu [Video].  
YouTube. <https://www.youtube.com/watch?v=djiAdi80zds&list=PLuMd8fg3qBxflEQOl0N2QK1YaUgD26Jvs&index=16>
9. Alfinete Tech. (2023, agosto 24). How to create a MySQL database on Ubuntu [Video].  
YouTube. <https://www.youtube.com/watch?v=LQE0SBOAPls&list=PLuMd8fg3qBxflEQOl0N2QK1YaUgD26Jvs&index=17>
10. Alfinete Tech. (2023, agosto 31). Configure PHP and Apache on Ubuntu [Video].  
YouTube. <https://www.youtube.com/watch?v=fPq1bq10g4M&list=PLuMd8fg3qBxflEQOl0N2QK1YaUgD26Jvs&index=18>
11. Alfinete Tech. (2023, septiembre 7). Enable SSL on Apache with Let's Encrypt [Video].  
YouTube. <https://www.youtube.com/watch?v=H2sW2xEVuA&list=PLuMd8fg3qBxflEQOl0N2QK1YaUgD26Jvs&index=19>

12. DigitalOcean. (2021, May 20). How to create a new user and grant permissions in MySQL. Retrieved from <https://www.digitalocean.com/community/tutorials/how-to-create-a-new-user-and-grant-permissions-in-mysql>.
13. Ubuntu Documentation. (n.d.). MySQL administration. Ubuntu Community Help Wiki. Retrieved from <https://help.ubuntu.com/community/MySQL>.
14. Oracle Corporation. (2022). MySQL 8.0 reference manual: Creating accounts. Retrieved from <https://dev.mysql.com/doc/refman/8.0/en/creating-accounts.html>.