

# Proyecto Segundo Corte

## Entorno híbrido con QEMU y Docker

Melanie Aponte  
Universidad Santo Tomás

29 de Abril

## Índice

<b>1. Instalación de Máquinas Virtuales (QEMU)</b>	<b>2</b>
1.1. Sistemas operativos instalados . . . . .	2
1.2. Instalación de Arch Linux en Máquina Virtual con Entorno Gráfico KDE Plasma	2
1.2.1. Creación de la máquina virtual . . . . .	2
1.2.2. Particionado y formateo del disco . . . . .	2
1.2.3. Instalación del sistema base . . . . .	2
1.2.4. Configuraciones iniciales . . . . .	3
1.2.5. Instalación del entorno gráfico KDE Plasma . . . . .	4
1.2.6. Arranque en entorno gráfico . . . . .	4
1.3. Configuración de red . . . . .	5
1.4. Herramientas instaladas y pruebas . . . . .	5
<b>2. Instalación de Contenedores Docker</b>	<b>11</b>
2.1. Contenedores usados . . . . .	11
2.2. Subred personalizada . . . . .	11
2.3. Herramientas instaladas . . . . .	12
<b>3. Contenedor Central Fedora</b>	<b>14</b>
3.1. Creación de imagen personalizada . . . . .	14
3.2. Ejecución en red compartida . . . . .	14
3.3. Verificación de conectividad . . . . .	14
<b>4. Análisis de Red y Procesos (Inicio)</b>	<b>18</b>
4.1. Escaneo de puertos . . . . .	18
4.2. Comparación de servicios y uso de recursos . . . . .	18
<b>5. Integración y uso de herramientas como Grafana, Prometheus y Zabbix.</b>	<b>21</b>
5.1. Imagenes de resultados . . . . .	21

# 1 Instalación de Máquinas Virtuales (QEMU)

## 1.1 Sistemas operativos instalados

- Rocky Linux
- Manjaro Linux
- Arch Linux

## 1.2 Instalación de Arch Linux en Máquina Virtual con Entorno Gráfico KDE Plasma

### 1.2.1. Creación de la máquina virtual

- Se creó una nueva máquina virtual en Virt-Manager:
  - Firmware: **UEFI (OVMF)**.
  - Chipset: **Q35**.
  - Disco duro de 20 GB en formato **qcow2**.
  - Memoria RAM de 2 GB o más, y 2 CPU.
  - Fuente de arranque: ISO de Arch Linux oficial.
- Se verificó el arranque en modo UEFI mediante:

```
ls /sys/firmware/efi/efivars
```

### 1.2.2. Particionado y formateo del disco

- Creación de particiones con **cfdisk** en esquema GPT:
  - 512 MiB EFI System Partition.
  - 2 GiB Swap Partition.
  - Resto para Linux filesystem (raíz).
- Formateo y activación:

```
mkfs.fat -F32 /dev/vda1
mkswap /dev/vda2
swapon /dev/vda2
mkfs.ext4 /dev/vda3
```

### 1.2.3. Instalación del sistema base

- Montaje de particiones:

```
mount /dev/vda3 /mnt
mkdir /mnt/boot
mkdir /mnt/boot/efi
mount /dev/vda1 /mnt/boot/efi
```

- Instalación de paquetes esenciales:

```
pacstrap /mnt base linux linux-firmware nano networkmanager grub efibootmgr
```

- Generación del archivo fstab:

```
genfstab -U /mnt >> /mnt/etc/fstab
```

- Cambio de raíz al nuevo sistema:

```
arch-chroot /mnt
```

#### 1.2.4. Configuraciones iniciales

- Zona horaria:

```
ln -sf /usr/share/zoneinfo/America/Bogota /etc/localtime
hwclock --systohc
```

- Locales:

```
nano /etc/locale.gen
# Descomentar en_US.UTF-8 UTF-8 y es_CO.UTF-8 UTF-8
locale-gen
echo "LANG=en_US.UTF-8" > /etc/locale.conf
```

- Hostname:

```
echo "archvm" > /etc/hostname
nano /etc/hosts
# Agregar:
127.0.0.1      localhost
::1            localhost
127.0.1.1      archvm.localdomain archvm
```

- Instalación y configuración de GRUB:

```
grub-install --target=x86_64-efi --efi-directory=/boot/efi --bootloader-id=Arch
grub-mkconfig -o /boot/grub/grub.cfg
```

- Activación de NetworkManager:

```
systemctl enable NetworkManager
```

### 1.2.5. Instalación del entorno gráfico KDE Plasma

- Instalación de servidor gráfico y drivers:

```
pacman -S xorg-server xorg-apps xf86-video-qxl
```

- Instalación de KDE Plasma y sus aplicaciones:

```
pacman -S plasma kde-applications
```

- Instalación y habilitación de SDDM (gestor de sesión gráfica):

```
pacman -S sddm  
systemctl enable sddm
```

- Instalación adicional para soporte de sesión:

```
pacman -S xorg-xinit plasma-meta
```

### 1.2.6. Arranque en entorno gráfico

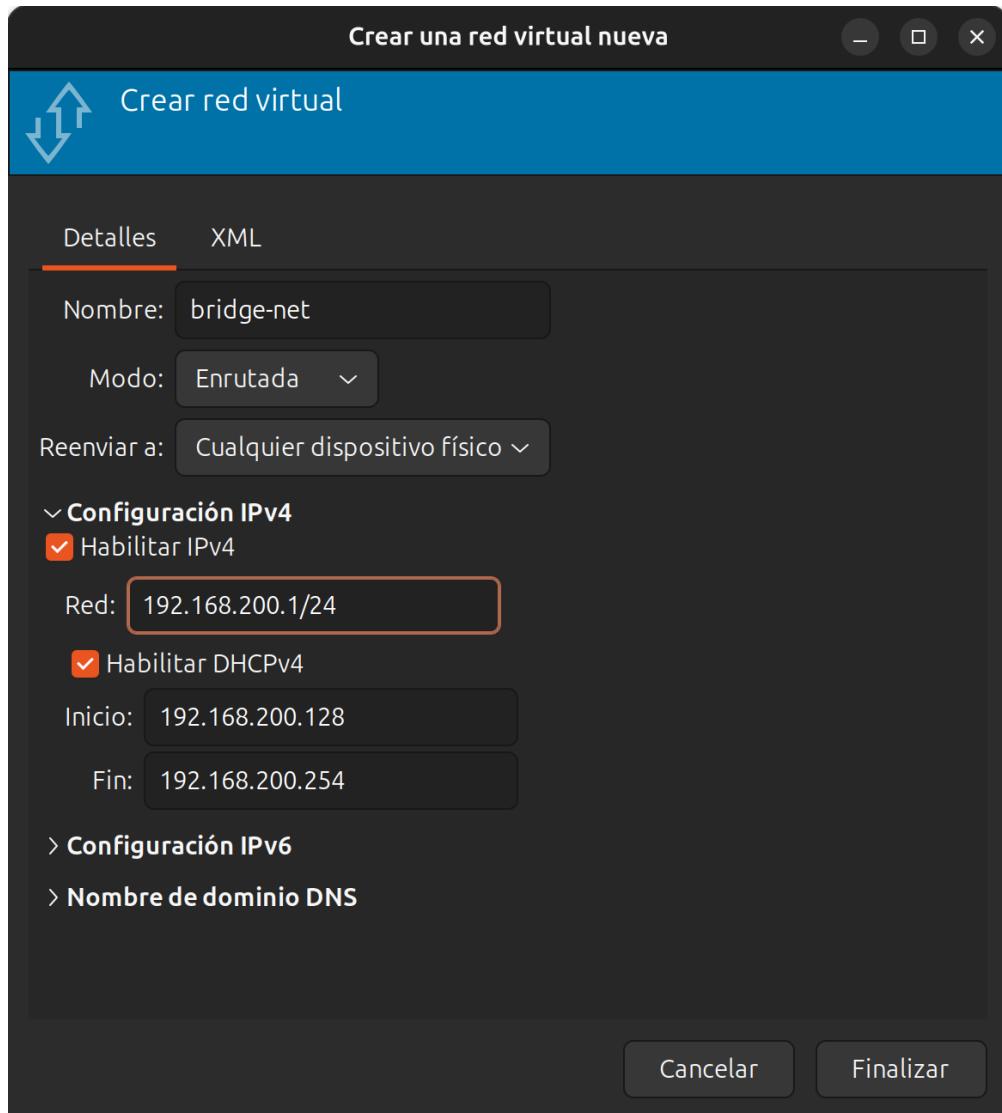
- Tras reiniciar el sistema:

```
reboot
```

Se selecciona la sesión **Plasma (X11)** en SDDM para iniciar correctamente el entorno de escritorio KDE Plasma.

### 1.3 Configuración de red

- Modo Bridge
- Subred: 192.168.200.0/24
- Rango DHCP: 192.168.200.128 – 192.168.200.254



### 1.4 Herramientas instaladas y pruebas

- Análisis de servicios: glances, bpytop, systemctl/journalctl

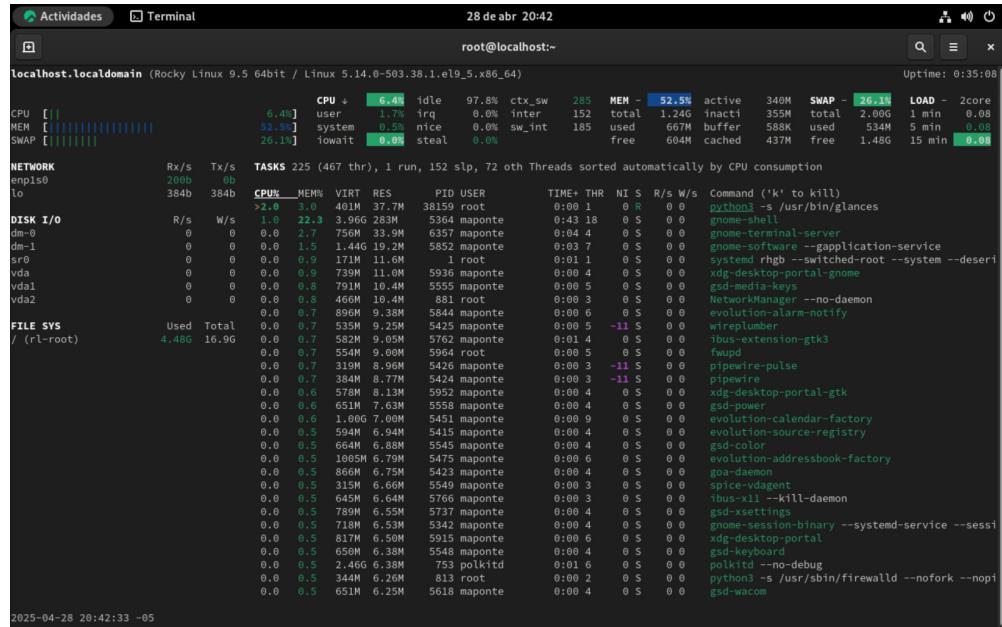


Figura 1: Glances

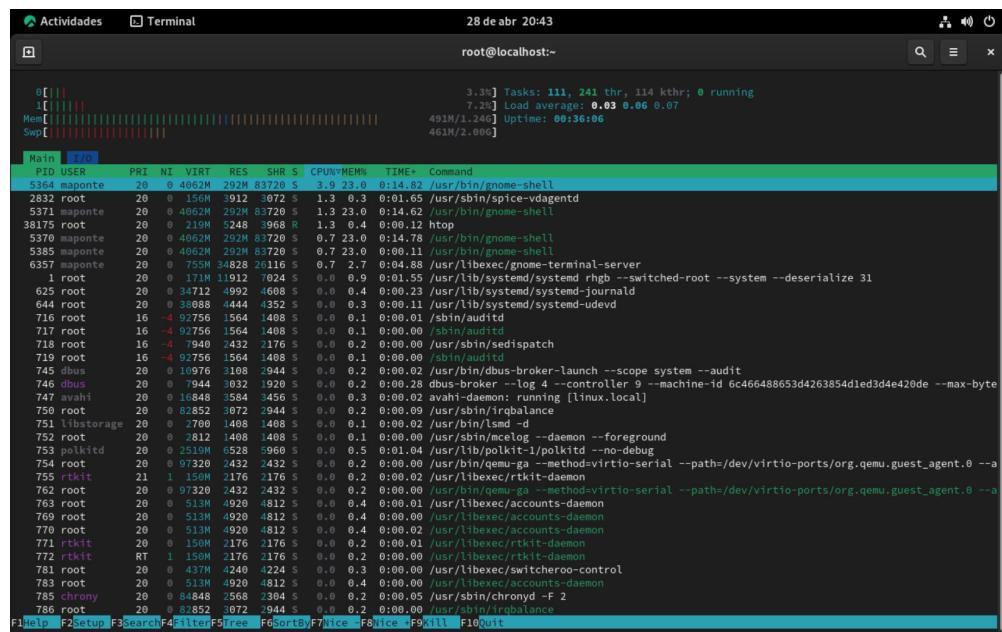


Figura 2: htop

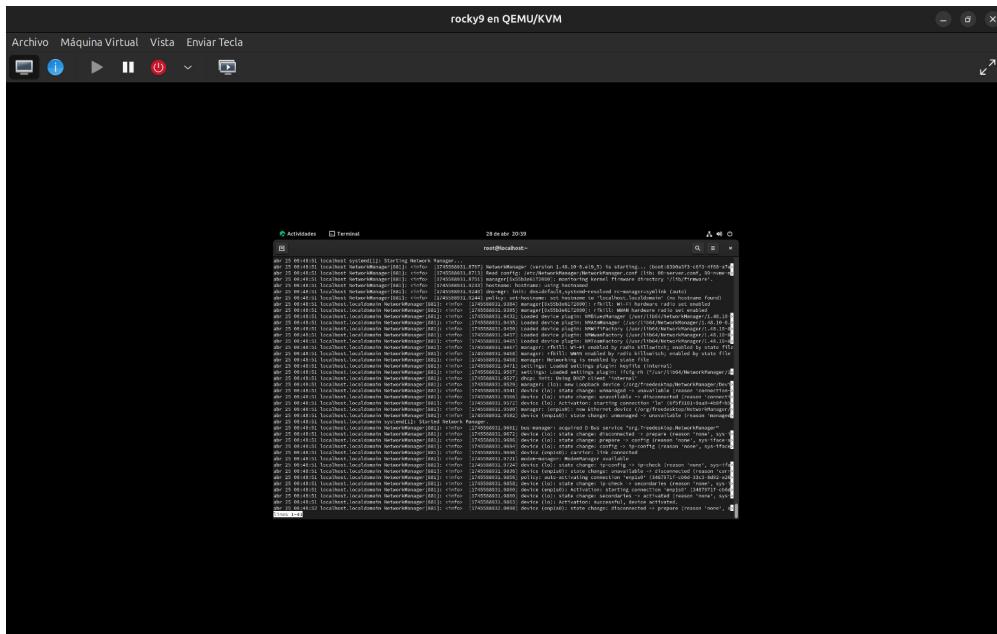


Figura 3: Journalctl

- Análisis de red: wireshark, iftop, nethogs

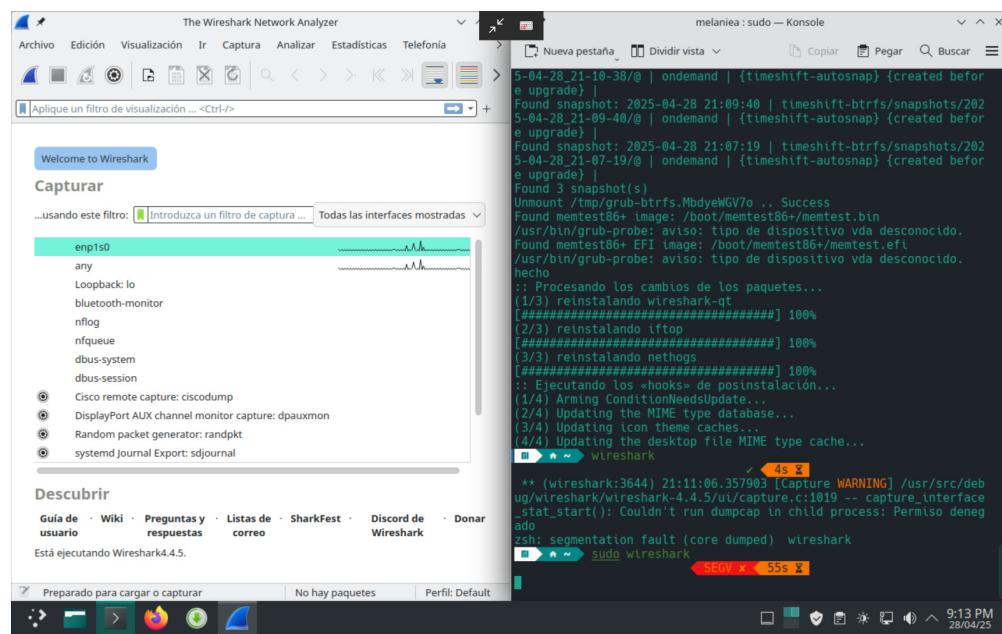


Figura 4: wireshark

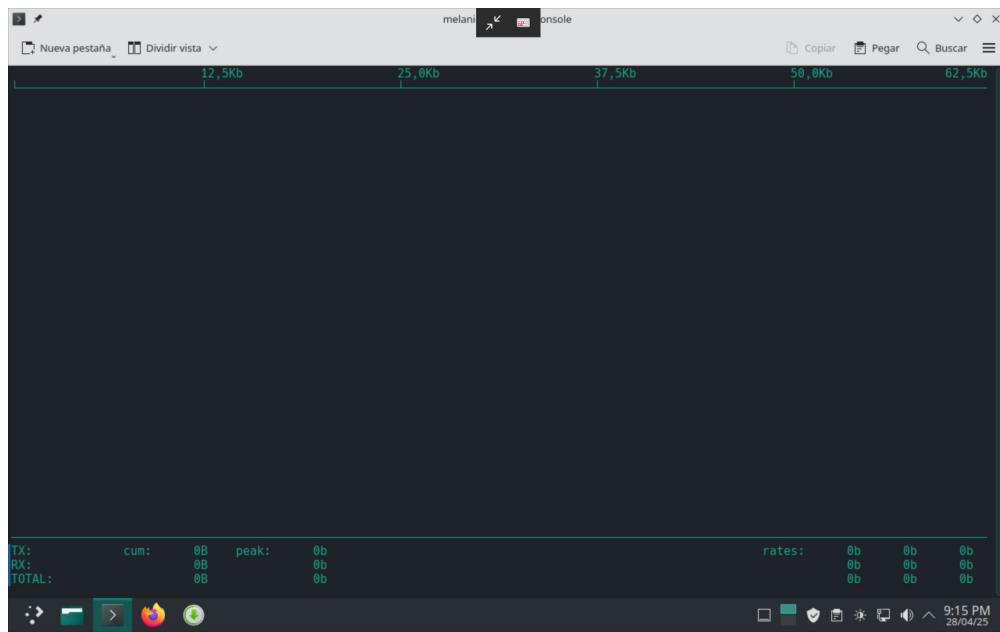


Figura 5: iftop

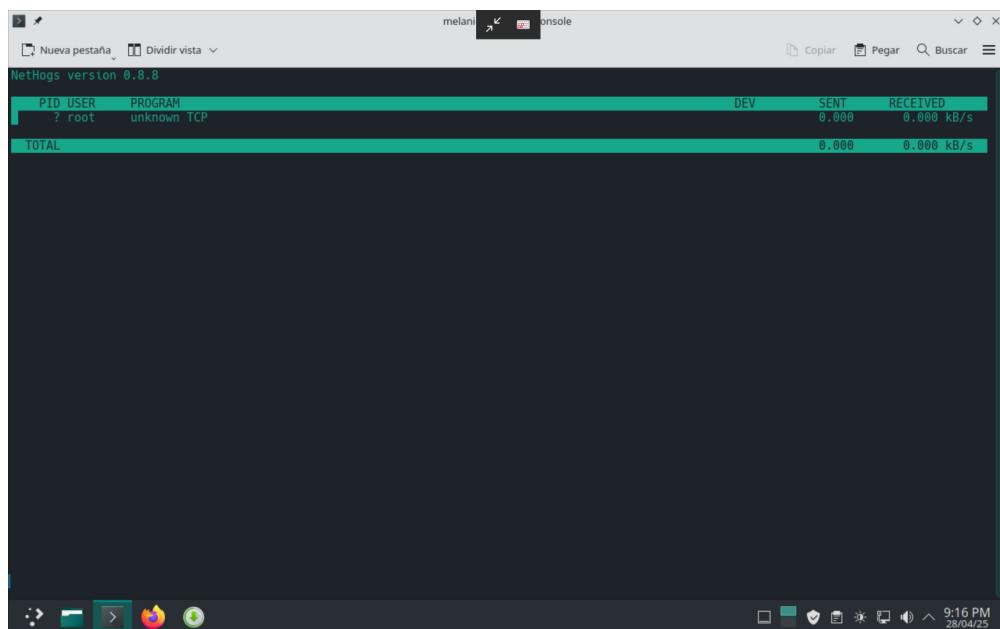


Figura 6: nethogs

- Gestión de archivos: **ncdu**, **baobab**, **tree**, **rsync**

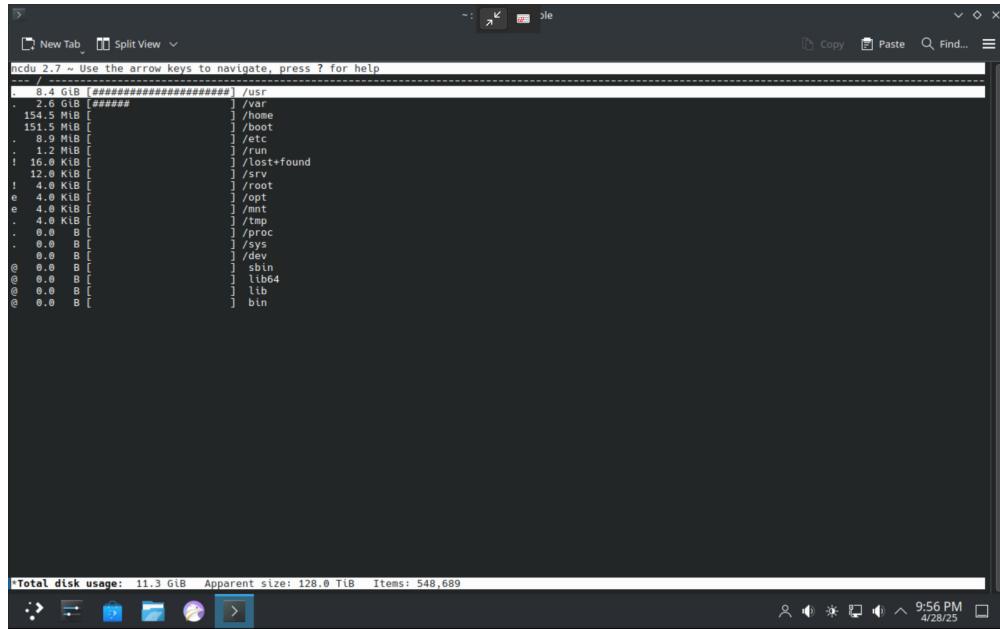


Figura 7: Ncdu

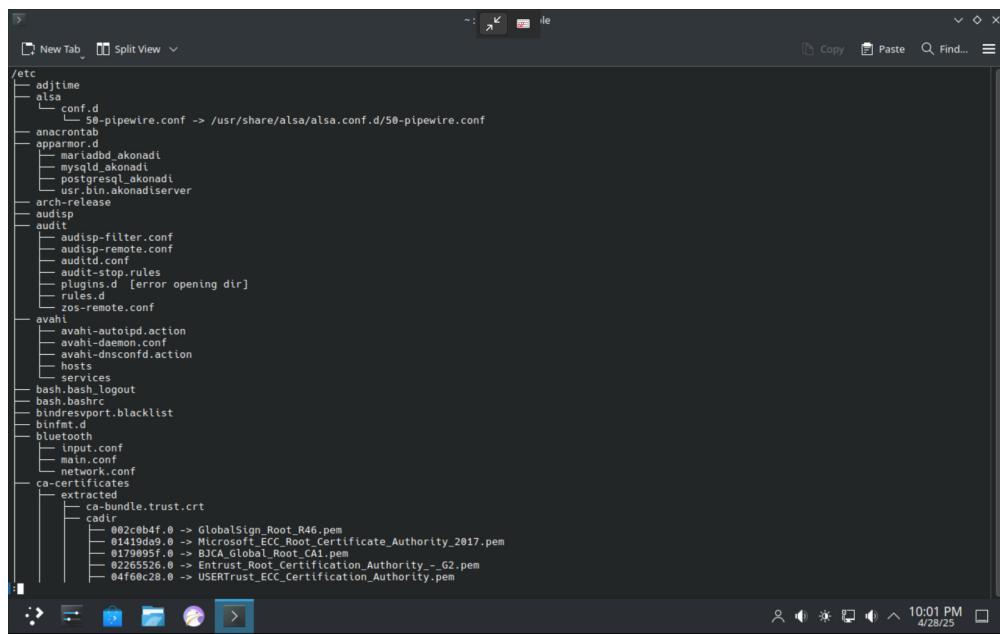


Figura 8: tree

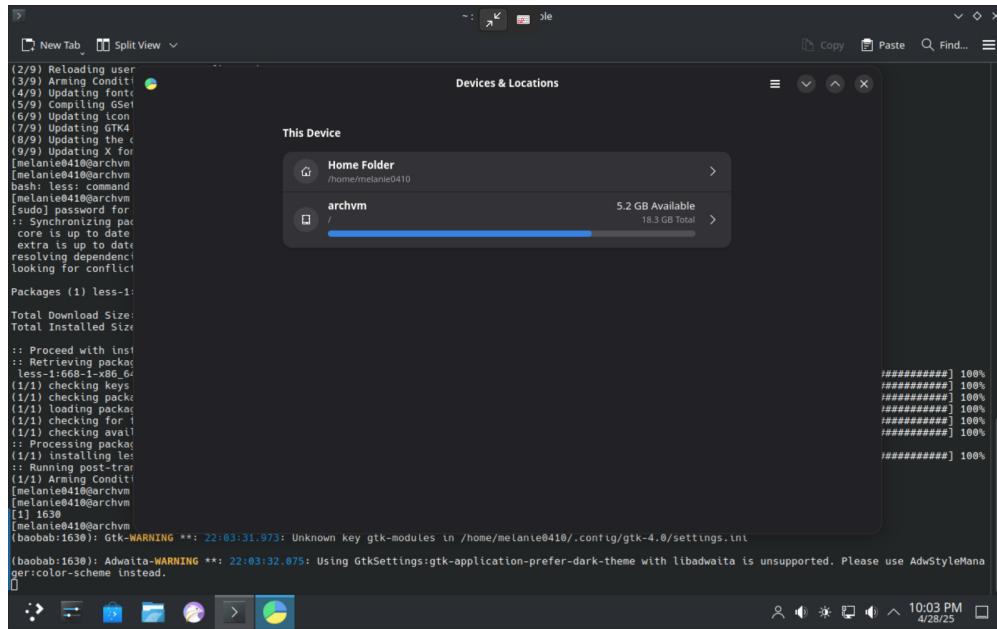


Figura 9: baobab

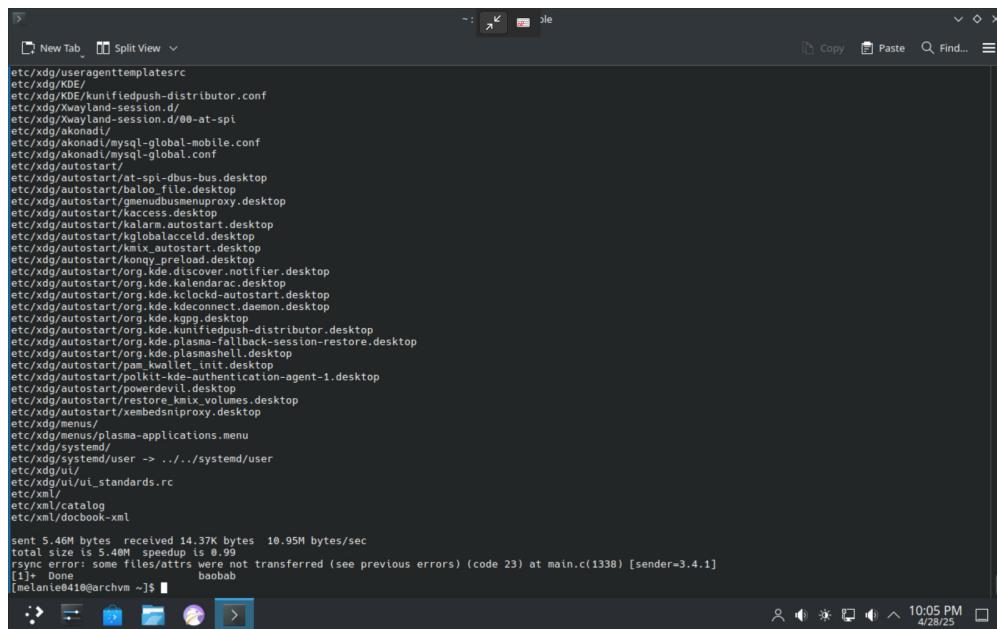


Figura 10: rsync

## 2 Instalación de Contenedores Docker

### 2.1 Contenedores usados

- Debian
- Alpine
- Arch (simulando Garuda)

```
d1223dadd942 archlinux           "bash"  
      garuda_container  
1a4580ca9c28  debian            "bash"  
      debian_container  
849d84523505  alpine             "sh"  
      alpine_container
```

### 2.2 Subred personalizada

- Subred: 172.25.0.0/24
- Nombre: **red\_contenedores**

```
09b7ec109890  red_contenedores    bridge    local
```

### 2.3 Herramientas instaladas

- Análisis de hardware: `lshw`, `inxi`, `lsblk`, `udevadm`
- Gestión de logs: `lnav`, `goaccess`
- Visualización de datos: `netdata`, `ctop`, `lazydocker`

```

melanie-aponte@melanie-aponte-Vivobook-ASUSLaptop-X3400PA-K3400PA: ~
melanie-aponte@melanie-aponte-Vivobook-ASUSLaptop-X3400PA-K3400PA: ~
lsblk is already the newest version (02.19.git.2021.06.19.996aaad9c7-2+b1).
inxi is already the newest version (3.3.26-1).
udev is already the newest version (252.36-1-deb12u1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@e60fa3632224:/# lsblk
NAME      MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
loop0      7:0    0   73.9M  1 loop
loop1      7:1    0   4K  1 loop
loop2      7:2    0   73.9M  1 loop
loop3      7:3    0  258.3M  1 loop
loop4      7:4    0  242M  1 loop
loop5      7:5    0  10.7M  1 loop
loop6      7:6    0 505.1M  1 loop
loop7      7:7    0 11.1M  1 loop
loop8      7:8    0  516M  1 loop
loop9      7:9    0  91.7M  1 loop
loop10     7:10   0  10.8M  1 loop
loop11     7:11   0  10.8M  1 loop
loop12     7:12   0  44.4M  1 loop
loop13     7:13   0  44.4M  1 loop
loop14     7:14   0  500K  1 loop
loop15     7:15   0  568K  1 loop
sda       8:0    1   7.3G  0 disk
`-sda1     8:1    1   7.2G  0 part
`-sda2     8:2    1   32M  0 part
nvme0n1   259:0   0 476.9G  0 disk
`-nvme0n1p1 259:1   0 268M  0 part
`-nvme0n1p2 259:2   0 16M  0 part
`-nvme0n1p3 259:3   0 290.4G 0 part
`-nvme0n1p4 259:4   0   1G  0 part
`-nvme0n1p5 259:5   0  200M 0 part
`-nvme0n1p6 259:6   0  89.2G 0 part
          /etc/hosts
          /etc/hostname
          /etc/resolv.conf
root@e60fa3632224:/# 

```

Figura 11: Lsblk

```

melanie-aponte@melanie-aponte-Vivobook-ASUSLaptop-X3400PA-K3400PA: ~
melanie-aponte@melanie-aponte-Vivobook-ASUSLaptop-X3400PA-K3400PA: ~
lshw
product: AT Translated Set 2 keyboard
physical id: 6
logical name: input3
logical name: event3
logical name: input3::capslock
logical name: input3::numlock
logical name: input3::scrolllock
capabilities: i8042
*.input:4
product: ASUE120B:00 04F3:31C0 Mouse
physical id: 7
logical name: input6
logical name: event4
logical name: mouse0
capabilities: i2c
*.input:5
product: ASUE120B:00 04F3:31C0 Touchpad
physical id: 8
logical name: input7
logical name: event5
logical name: mouse1
capabilities: i2c
*.input:6
product: Asus WMI hotkeys
physical id: 9
logical name: input8
logical name: event6
capabilities: platform
*.input:7
product: Video Bus
physical id: a
logical name: input9
logical name: event7
capabilities: platform
root@e60fa3632224:/# 

```

Figura 12: Lshw

```
root@e60fa3632224:/# inxi
CPU: quad core 11th Gen Intel Core i5-11300H (-MT MCP-) speed/min/max: 951/400/4400 MHz
Kernel: 6.11.0-24-generic x86_64 Up: 1h 53m Mem: 6419.6/15685.2 MiB (40.9%)
Storage: 484.2 GiB (14.1% used) Procs: 4 Shell: Bash lnxxt: 3.3.26
root@e60fa3632224:/#
```

Figura 13: inxi

```
melanie-aponte@melanie-aponte-Vivobook-ASUSLaptop-X3400PA-K3400PA: ~
melanie-aponte@melanie-aponte-Vivobook-ASUSLaptop-X3400PA-K3400PA: ~
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
--- Netdata, X-Ray Vision for your infrastructure! ---
You are about to build and install netdata to your system.

The build process will use /tmp for
any temporary files. You can override this by setting $TMPDIR to a
writable directory where you can execute files.

It will be installed at these locations:

- the daemon      at /usr/sbin/netdata
- config files   in /etc/netdata
- web files      in /usr/share/netdata
- plugins        in /usr/libexec/netdata
- cache files    in /var/cache/netdata
- db files       in /var/lib/netdata
- log files      in /var/log/netdata
- pid file       at /var/run/netdata.pid
- logrotate file at /etc/logrotate.d/netdata

This installer allows you to change the installation path.
Press Control-C and run the same command with -help for help.

NOTE:
Anonymous usage stats will be collected and sent to Netdata.
To opt-out, pass --disable-telemetry option to the installer or export
the environment variable DISABLE_TELEMETRY to a non-zero or non-empty value
(e.g: export DISABLE_TELEMETRY=1).

--- Found CMake at /usr/bin/cmake. CMake version: cmake version 3.31.1 ---
--- Could not find Ninja, will use Make instead. ---
Press ENTER to build and install netdata to your system > [ ]
```

Figura 14: Netdata

```
LOG
nao@Pepper:~/Melanie
[2025-04-29T18:02:00.000 ~] access.log [~] access.log[2] ~] 127.0.0.1 ~
|127.0.0.1 - - [29/Apr/2025:18:02:00 +0000] "GET /dashboard HTTP/1.1" 200 5412
Press ENTER to focus on the breadcrumb bar
```

Files :: Text Filters :: Press TAB to edit  
L2 100% ?View Help  
Press e/E to move forward/backward through error messages

Figura 15: Lnav

```
wget openbase
root@4282606d6c60:/# cat << EOF > access.log
127.0.0.1 - - [29/Apr/2025:18:00:00 +0000] "GET /index.html HTTP/1.1" 200 2326
127.0.0.1 - - [29/Apr/2025:18:01:00 +0000] "POST /login HTTP/1.1" 302 123
127.0.0.1 - - [29/Apr/2025:18:02:00 +0000] "GET /dashboard HTTP/1.1" 200 5412
EOF
root@4282606d6c60:/# lnav access.log
root@4282606d6c60:/# ]
```

Figura 16: Inav

```
root@4282606d6c60:/# goaccess access.log --log-format=COMBINED --real-time-html
Cleaning up resources...
==3103== GoAccess - version 1.7 - Jan 4 2023 18:36:47
==3103== Config file: /etc/goaccess/goaccess.conf
==3103== https://goaccess.io - <hello@goaccess.io>
==3103== Released under the MIT License.
==3103==
==3103== FILE: access.log
==3103== Parsed 3 lines producing the following errors:
==3103== Token for '%b' specifier is NULL.
==3103== Token for '%b' specifier is NULL.
==3103== Token for '%b' specifier is NULL.
==3103==
==3103== Format Errors - Verify your log/date/time format
root@4282606d6c60:/# ]
```

Figura 17: Goaccess

### 3 Contenedor Central Fedora

#### 3.1 Creación de imagen personalizada

- Herramientas incluidas: `htop`, `net-tools`, `iputils`, `python3`, `git`, `nmap`, `traceroute`

daa5fb086acb fedora-central	"/bin/bash"
fedora_central	

#### 3.2 Ejecución en red compartida

```
docker run -dit --name fedora_central --network host fedora-central
```

#### 3.3 Verificación de conectividad

- Ping exitoso a VMs y contenedores
- Escaneo de red con `nmap`

Cada máquina virtual conectada a `bridge-net` recibió una dirección IP válida dentro del rango definido:

- Rocky Linux: 192.168.200.188

```
[maponte@localhost ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp1s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 52:54:00:27:b3:53 brd ff:ff:ff:ff:ff:ff
    inet 192.168.200.188/24 brd 192.168.200.255 scope global dynamic noprefixroute enp1s0
        valid_lft 3576sec preferred_lft 3576sec
    inet6 fe80::5e04:ff:fe27:b353/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[maponte@localhost ~]$
```

Figura 18: ip a para Rocky

- Arch Linux: 192.168.200.195

```
[melanie041@archvm ~]$ 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: enp1s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 52:54:00:bf:fd:14 brd ff:ff:ff:ff:ff:ff
    altname enx525400bfdf14
    inet 192.168.200.195/24 brd 192.168.200.255 scope global dynamic noprefixroute enp1s0
        valid_lft 3475sec preferred_lft 3475sec
    inet6 fe80::21ee:fbff:fe00:65de:995e/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[melanie041@archvm ~]$
```

Figura 19: ip a para Arch

- Manjaro Linux: 192.168.200.234

```
melaniea : zsh — Konsole
melaniea : ~
melaniea : ~ 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: enp1s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 52:54:00:8c:f5:76 brd ff:ff:ff:ff:ff:ff
    altnet enx5254008cf576
    inet 192.168.200.234/24 brd 192.168.200.255 scope global dynamic noprefixroute enp1s0
        valid_lft 3525sec preferred_lft 3525sec
    inet6 fe80::e6b7:5337:5830:b1f1/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Figura 20: ip a para Manjaro

- ip a: para verificar la IP del contenedor. Se observó que utiliza la red 192.168.200.0/24 a través de la interfaz virbr2.

```
14: virbr2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 52:54:00:13:a5:0b brd ff:ff:ff:ff:ff:ff
    inet 192.168.200.1/24 brd 192.168.200.255 scope global virbr2
        valid_lft forever preferred_lft forever
```

- ping <ip-vm>: se realizó ping a cada máquina virtual:

- Rocky Linux: 192.168.200.188

```
[root@melanie-aponte-Vivobook-ASUSLaptop-X3400PA-K3400PA /]# ping 192.168.200.188
PING 192.168.200.188 (192.168.200.188) 56(84) bytes of data.
64 bytes from 192.168.200.188: icmp_seq=1 ttl=64 time=0.414 ms
64 bytes from 192.168.200.188: icmp_seq=2 ttl=64 time=0.442 ms
64 bytes from 192.168.200.188: icmp_seq=3 ttl=64 time=0.412 ms
64 bytes from 192.168.200.188: icmp_seq=4 ttl=64 time=0.357 ms
```

Figura 21: Ping a rocky desde el contenedor

- Arch Linux: 192.168.200.195

```
[root@melanie-aponte-Vivobook-ASUSLaptop-X3400PA-K3400PA /]# ping 192.168.200.195
PING 192.168.200.195 (192.168.200.195) 56(84) bytes of data.
64 bytes from 192.168.200.195: icmp_seq=1 ttl=64 time=0.368 ms
64 bytes from 192.168.200.195: icmp_seq=2 ttl=64 time=0.504 ms
64 bytes from 192.168.200.195: icmp_seq=3 ttl=64 time=0.471 ms
64 bytes from 192.168.200.195: icmp_seq=4 ttl=64 time=0.477 ms
64 bytes from 192.168.200.195: icmp_seq=5 ttl=64 time=0.403 ms
```

Figura 22: Ping a Arch desde el contenedor

- Manjaro Linux: 192.168.200.234

```
[root@melanie-aponte-Vivobook-ASUSLaptop-X3400PA-K3400PA /]# ping 192.168.200.234
PING 192.168.200.234 (192.168.200.234) 56(84) bytes of data.
64 bytes from 192.168.200.234: icmp_seq=1 ttl=64 time=0.449 ms
64 bytes from 192.168.200.234: icmp_seq=2 ttl=64 time=0.386 ms
64 bytes from 192.168.200.234: icmp_seq=3 ttl=64 time=0.408 ms
64 bytes from 192.168.200.234: icmp_seq=4 ttl=64 time=0.368 ms
^C
```

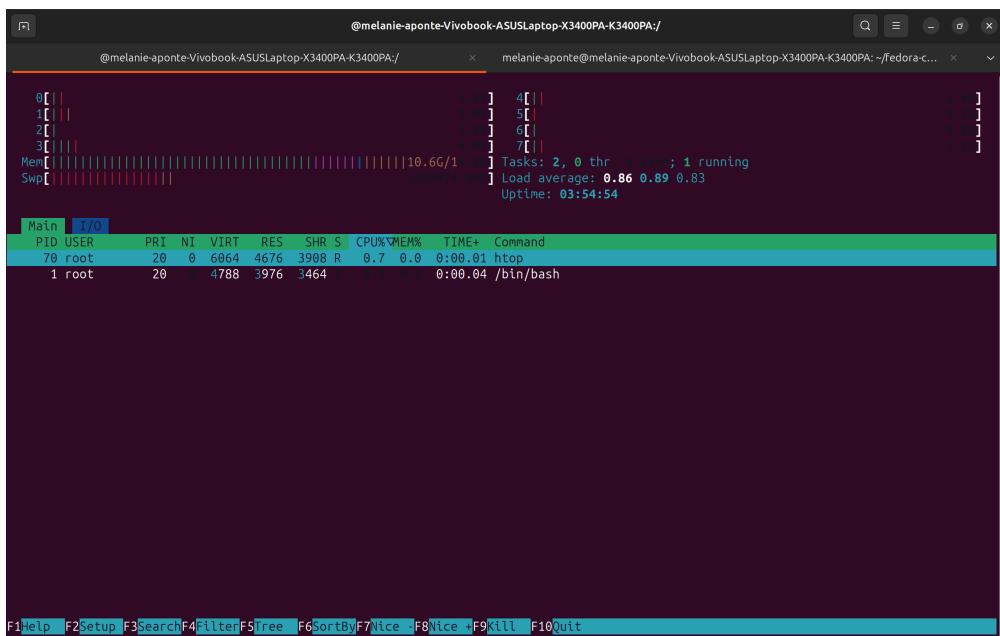
Figura 23: Ping a manjaro desde el contenedor

Todas respondieron exitosamente.

- **traceroute <ip-vm>**: para ver la ruta hacia las máquinas virtuales.

```
[root@melanie-aponte-Vivobook-ASUSLaptop-X3400PA-K3400PA /]# traceroute 192.168.200.195
traceroute to 192.168.200.195 (192.168.200.195), 30 hops max, 60 byte packets
 1  192.168.200.195 (192.168.200.195)  0.505 ms  0.467 ms  0.426 ms
[root@melanie-aponte-Vivobook-ASUSLaptop-X3400PA-K3400PA /]# traceroute 192.168.200.234
traceroute to 192.168.200.234 (192.168.200.234), 30 hops max, 60 byte packets
 1  192.168.200.234 (192.168.200.234)  0.596 ms  0.540 ms  0.516 ms
[root@melanie-aponte-Vivobook-ASUSLaptop-X3400PA-K3400PA /]# traceroute 192.168.200.188
traceroute to 192.168.200.188 (192.168.200.188), 30 hops max, 60 byte packets
 1  192.168.200.188 (192.168.200.188)  0.644 ms !X  0.588 ms !X  0.569 ms !X
[root@melanie-aponte-Vivobook-ASUSLaptop-X3400PA-K3400PA /]#
```

- **ps aux y htop**: para observar procesos en ejecución dentro del contenedor central.



Esto permitió comprobar que el contenedor central podía comunicarse con el resto del entorno virtualizado, cumpliendo el objetivo de ser el nodo central de análisis.

## 4 Análisis de Red y Procesos (Inicio)

### 4.1 Escaneo de puertos

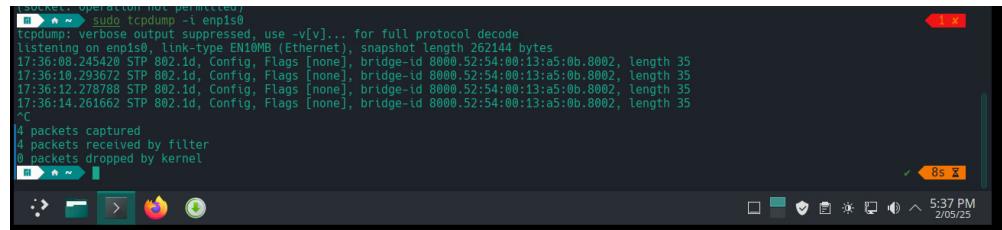
```
nmap -Pn 192.168.200.130
nmap -Pn 172.25.0.2
```

### 4.2 Comparación de servicios y uso de recursos

- ps aux, htop, netstat -tulpn, ip a, docker inspect

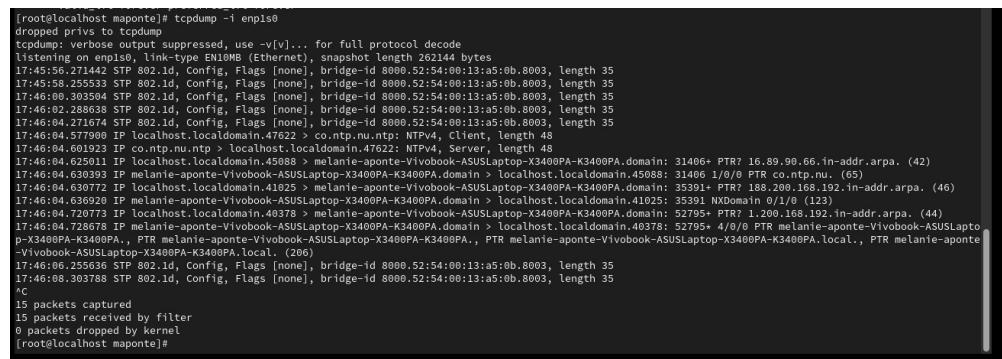
Entorno	Interfaz	¿Tcpcdump instalado?	¿Captura tráfico?
Rocky Linux (VM)	enp0s3	Sí (dnf)	Sí
Manjaro (VM)	enp0s3	Sí (pacman)	Sí
Arch Linux (VM)	enp0s3	Sí (pacman)	Sí
Debian (Contenedor)	eth0	Sí (apt)	Sí
Alpine (Contenedor)	eth0	Sí (apk)	Sí
Garuda/Arch (Contenedor)	eth0	Sí (pacman)	Sí

Cuadro 1: Comparativa del uso de tcpcdump en máquinas virtuales y contenedores



```
[root@localhost maponte]# sudo tcpdump -i enp0s3
tcpdump: verbose output suppressed, use -v[el]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
17:36:08.245420 STP 802.1d, Config, Flags [none], bridge-id 8000.52:54:00:13:a5:0b.8002, length 35
17:36:10.293672 STP 802.1d, Config, Flags [none], bridge-id 8000.52:54:00:13:a5:0b.8002, length 35
17:36:12.278788 STP 802.1d, Config, Flags [none], bridge-id 8000.52:54:00:13:a5:0b.8002, length 35
17:36:14.261662 STP 802.1d, Config, Flags [none], bridge-id 8000.52:54:00:13:a5:0b.8002, length 35
^C
4 packets captured
4 packets received by filter
0 packets dropped by kernel
[...]
```

Figura 24: Tcp manjaro



```
[root@localhost maponte]# tcpdump -i enp0s3
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v[el]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
17:45:56.271442 STP 802.1d, Config, Flags [none], bridge-id 8000.52:54:00:13:a5:0b.8003, length 35
17:45:58.255533 STP 802.1d, Config, Flags [none], bridge-id 8000.52:54:00:13:a5:0b.8003, length 35
17:46:00.303594 STP 802.1d, Config, Flags [none], bridge-id 8000.52:54:00:13:a5:0b.8003, length 35
17:46:02.288634 STP 802.1d, Config, Flags [none], bridge-id 8000.52:54:00:13:a5:0b.8003, length 35
17:46:04.271674 STP 802.1d, Config, Flags [none], bridge-id 8000.52:54:00:13:a5:0b.8003, length 35
17:46:04.601923 IP localhost.localdomain.45088 > localhost.localdomain.45088: [REDACTED] co.ntp.45088: NTP v4 Client, length 48
17:46:04.625011 IP localhost.localdomain.45088 > melanie-aponte-Vivobook-ASUSLaptop-X340PA-K3400PA.domain: 31406+ PTR? 16.89.98.66.in-addr.arpa. (42)
17:46:04.630393 IP melanie-aponte-Vivobook-ASUSLaptop-X340PA-K3400PA.domain > localhost.localdomain.45088: 31406 1/0/0 PTR co.ntp.ru. (65)
17:46:04.630772 IP localhost.localdomain.41025 > melanie-aponte-Vivobook-ASUSLaptop-X340PA-K3400PA.domain: 35391+ PTR? 188.208.168.192.in-addr.arpa. (46)
17:46:04.636920 IP melanie-aponte-Vivobook-ASUSLaptop-X340PA-K3400PA.domain > localhost.localdomain.41025: 35391 NXDomain 0/1/0 (123)
17:46:04.720773 IP localhost.localdomain.40378 > melanie-aponte-Vivobook-ASUSLaptop-X340PA-K3400PA.domain: 52795+ PTR? 1.200.168.192.in-addr.arpa. (44)
17:46:04.728678 IP melanie-aponte-Vivobook-ASUSLaptop-X340PA-K3400PA.domain > localhost.localdomain.40378: 52795+ 4/8/0 PTR melanie-aponte-Vivobook-ASUSLaptop-X340PA-K3400PA.local. (206)
17:46:06.255636 STP 802.1d, Config, Flags [none], bridge-id 8000.52:54:00:13:a5:0b.8003, length 35
17:46:08.303788 STP 802.1d, Config, Flags [none], bridge-id 8000.52:54:00:13:a5:0b.8003, length 35
^C
15 packets captured
15 packets received by filter
0 packets dropped by kernel
[root@localhost maponte]#
```

Figura 25: Tcp Rocky

```
[root@archvm melanie0410]# tcpdump -i ens0
tcpdump: ens0: No such device exists
(No such device exists)
[root@archvm melanie0410]# tcpdump -i enp1s0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp1s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
17:58:21.459888 STP 802.1d, Config, Flags [none], bridge-id 8000.52:54:00:13:a5:0b.8001, length 35
17:58:23.443898 STP 802.1d, Config, Flags [none], bridge-id 8000.52:54:00:13:a5:0b.8001, length 35
17:58:25.427955 STP 802.1d, Config, Flags [none], bridge-id 8000.52:54:00:13:a5:0b.8001, length 35
17:58:27.411950 STP 802.1d, Config, Flags [none], bridge-id 8000.52:54:00:13:a5:0b.8001, length 35
17:58:29.395913 STP 802.1d, Config, Flags [none], bridge-id 8000.52:54:00:13:a5:0b.8001, length 35
17:58:31.443998 STP 802.1d, Config, Flags [none], bridge-id 8000.52:54:00:13:a5:0b.8001, length 35
17:58:33.428094 STP 802.1d, Config, Flags [none], bridge-id 8000.52:54:00:13:a5:0b.8001, length 35
17:58:35.412191 STP 802.1d, Config, Flags [none], bridge-id 8000.52:54:00:13:a5:0b.8001, length 35
17:58:37.395997 STP 802.1d, Config, Flags [none], bridge-id 8000.52:54:00:13:a5:0b.8001, length 35
17:58:39.381187 STP 802.1d, Config, Flags [none], bridge-id 8000.52:54:00:13:a5:0b.8001, length 35
17:58:41.428078 STP 802.1d, Config, Flags [none], bridge-id 8000.52:54:00:13:a5:0b.8001, length 35
17:58:43.412988 STP 802.1d, Config, Flags [none], bridge-id 8000.52:54:00:13:a5:0b.8001, length 35
17:58:45.395985 STP 802.1d, Config, Flags [none], bridge-id 8000.52:54:00:13:a5:0b.8001, length 35
17:58:47.380104 STP 802.1d, Config, Flags [none], bridge-id 8000.52:54:00:13:a5:0b.8001, length 35
^C
14 packets captured
14 packets received by filter
0 packets dropped by kernel
[root@archvm melanie0410]#
```

Figura 26: Tcp Arch

```
[root@d1223dadd942 ~]# 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 proto kernel_l_o
                valid_lft forever preferred_lft forever
38: eth0@if39: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:19:00:04 brd ff:ff:ff:ff:ff:ff link-netnsid 0
        inet 172.25.0.4/24 brd 172.25.0.255 scope global eth0
            valid_lft forever preferred_lft forever
[root@d1223dadd942 ~]# tcpdump -i eth0@if39
tcpdump: eth0@if39: No such device exists
(No such device exists)
[root@d1223dadd942 ~]# tcpdump -i eth0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
23:03:02.099416 IP6 melanie-aponte-Vivobook-ASUSLaptop-X3400PA-K3400PA.mdns: 0 [2q] PTR (QM)? _ipp.s._tcp.local. PTR (QM)?
? _ipp._tcp.local. (45)
23:03:40.940594 IP6 melanie-aponte-Vivobook-ASUSLaptop-X3400PA-K3400PA.mdns: 0 [2q] PTR (QM)? _ipp.s._tcp.local. PTR (QM)?
? _ipp._tcp.local. (45)
```

Figura 27: Tcp garuda

```
[root@d1223dadd942 ~]# 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 proto kernel_l_o
                valid_lft forever preferred_lft forever
38: eth0@if39: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:19:00:04 brd ff:ff:ff:ff:ff:ff link-netnsid 0
        inet 172.25.0.4/24 brd 172.25.0.255 scope global eth0
            valid_lft forever preferred_lft forever
[root@d1223dadd942 ~]# tcpdump -i eth0@if39
tcpdump: eth0@if39: No such device exists
(No such device exists)
[root@d1223dadd942 ~]# tcpdump -i eth0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
23:03:02.099416 IP6 melanie-aponte-Vivobook-ASUSLaptop-X3400PA-K3400PA.mdns: 0 [2q] PTR (QM)? _ipp.s._tcp.local. PTR (QM)?
? _ipp._tcp.local. (45)
23:03:40.940594 IP6 melanie-aponte-Vivobook-ASUSLaptop-X3400PA-K3400PA.mdns: 0 [2q] PTR (QM)? _ipp.s._tcp.local. PTR (QM)?
? _ipp._tcp.local. (45)
```

Figura 28: Tcp Debian

```
[root@d1223dadd942 /]# 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 proto kernel_llo
        valid_lft forever preferred_lft forever
38: eth0@if39: <NOARP,BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:19:00:04 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.25.0.4/24 brd 172.25.0.255 scope global eth0
        valid_lft forever preferred_lft forever
[root@d1223dadd942 /]# tcpdump -i eth0
tcpdump: No such device exists
(No such device exists)
[root@d1223dadd942 /]# tcpdump -i eth0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
23:03:02.099416 IP6 melanie-aponte-Vivobook-ASUSLaptop-X3400PA-K3400PA.mdns > ff02::fb.mdns: 0 [2q] PTR (QM)? _ipp._tcp.local. PTR (QM)
? _ipp._tcp.local. (45)
23:03:40.940594 IP6 melanie-aponte-Vivobook-ASUSLaptop-X3400PA-K3400PA.mdns > ff02::fb.mdns: 0 [2q] PTR (QM)? _ipp._tcp.local. PTR (QM)
? _ipp._tcp.local. (45)
```

Figura 29: Tcp Alpine

```
[root@melanie-aponte-Vivobook-ASUSLaptop-X3400PA-K3400PA /]# tcpdump -i virbr2
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on virbr2, link-type EN10MB (Ethernet), snapshot length 262144 bytes
23:08:22.060721 IP 192.168.200.188.41770 > cronos.unad.edu.co.ntp: NTPv4, Client, length 48
23:08:22.067907 IP cronos.unad.edu.co.ntp > 192.168.200.188.41770: NTPv4, Server, length 48
23:08:24.642527 IP 192.168.200.188.47228 > 0.co.ntp.edgeuno.com.ntp: NTPv4, Client, length 48
23:08:24.646551 IP 0.co.ntp.edgeuno.com.ntp > 192.168.200.188.47228: NTPv4, Server, length 48
23:08:27.400368 ARP, Request who-has melanie-aponte-Vivobook-ASUSLaptop-X3400PA-K3400PA tell 192.168.200.188, length 28
23:08:27.400397 ARP, Reply melanie-aponte-Vivobook-ASUSLaptop-X3400PA-K3400PA is-at 52:54:00:13:a5:b6 (oul Unknown), length 28
23:08:29.741005 ARP, Request who-has 192.168.200.188 tell melanie-aponte-Vivobook-ASUSLaptop-X3400PA-K3400PA, length 28
23:08:29.741495 ARP, Reply 192.168.200.188 is-at 52:54:00:27:b3:53 (oul Unknown), length 28
23:08:19.773112 IP 192.168.200.195.59684 > dns.google.domain: 13202+ A? ping.archlinux.org. (36)
23:09:19.773195 IP 192.168.200.195.59684 > dns.google.domain: 27294+ AAAA? ping.archlinux.org. (36)
23:09:19.773208 IP 192.168.200.195.53337 > dns.google.domain: 10870+ A? ping.archlinux.org. (36)
23:09:19.773221 IP 192.168.200.195.53337 > dns.google.domain: 58187+ AAAA? ping.archlinux.org. (36)
23:09:19.796282 IP dns.google.domain > 192.168.200.195.53337: 10870 2/0/0 CNAME redirect.archlinux.org., A 95.216.195.133 (75)
23:09:19.796308 IP dns.google.domain > 192.168.200.195.53337: 58187 2/0/0 CNAME redirect.archlinux.org., AAAA 2a01:4f9:c010:2636::1 (87)
23:09:19.796407 IP dns.google.domain > 192.168.200.195.59684: 13202 2/0/0 CNAME redirect.archlinux.org., A 95.216.195.133 (75)
23:09:19.796528 IP dns.google.domain > 192.168.200.195.59684: 27294 2/0/0 CNAME redirect.archlinux.org., AAAA 2a01:4f9:c010:2636::1 (87)
23:09:19.797349 IP 192.168.200.195.46662 > redirect.archlinux.org.http: Flags [S.], seq 2685796498, win 64240, options [mss 1460,sackOK,T
S val 141657755 ecr 0,nop,wscale 7], length 0
23:09:19.985317 IP redirect.archlinux.org.http > 192.168.200.195.46662: Flags [S.], seq 935873799, ack 2685796499, win 65160, options [m
ss 1412,sackOK,T
S val 1842926514 ecr 141657755,nop,wscale 7], length 0
23:09:19.985713 IP 192.168.200.195.46662 > redirect.archlinux.org.http: Flags [.], ack 1, win 502, options [nop,nop,T
S val 141657943 ecr
1842926514], length 0
23:09:19.98609 IP 192.168.200.195.46662 > redirect.archlinux.org.http: Flags [P.], seq 1:89, ack 1, win 502, options [nop,nop,T
S val 14
1657944 ecr 1842926514], length 88: HTTP: GET /nm-check.txt HTTP/1.1
23:09:20.169299 IP redirect.archlinux.org.http > 192.168.200.195.46662: Flags [.], ack 89, win 508, options [nop,nop,T
S val 1842926734 e
cr 141657944], length 0
23:09:20.169570 IP redirect.archlinux.org.http > 192.168.200.195.46662: Flags [P.], seq 1:205, ack 89, win 508, options [nop,nop,T
S val 1842926734 ecr 141657944], length 204: HTTP: HTTP/1.1 200 OK
```

Figura 30: Tcp contendor central

## 5 Integración y uso de herramientas como Grafana, Prometheus y Zabbix.

### 5.1 Imagenes de resultados

CONTAINER ID	IMAGE NAMES	COMMAND
6145a530c568	zabbix/zabbix-server-pgsql zabbix-server	"/usr/bin/docker-entrypoint.sh"
a4f0870c85e1	grafana/grafana grafana	"/run.sh"
9632e8148954	zabbix/zabbix-web-nginx-mysql zabbix-web	"docker-entrypoint.sh"
5f30790366da	mysql:8.0 zabbix-db	"docker-entrypoint.sh"
edfc0b443117	prom/prometheus prometheus	"/bin/prometheus --config-directory=/etc/prometheus --storage-path=/var/lib/prometheus"
c8d570574da9	prom/node-exporter node-exporter	"/bin/node_exporter"
294ab1395521	zabbix/zabbix-agent:alpine-6.0-latest zabbix-agent	"/sbin/tini -- /usr/bin/zabbix-agent -c /etc/zabbix/zabbix-agent.conf"

- Estos contenedores se encuentran en una red llamada red monitorizacion

```
298e7c792904    red_monitorizacion          bridge      local
melanie-aponte@melanie-aponte-Vivobook-ASUSLaptop-X3400PA-K3400PA:~$
```

El docker-compose.yml es el siguiente:

```
version: '3'

services:

  prometheus:
    image: prom/prometheus
    container_name: prometheus
    ports:
      - "9091:9090"
    volumes:
      - ./prometheus.yml:/etc/prometheus/prometheus.yml
    networks:
      - red_monitorizacion

  grafana:
    image: grafana/grafana
    container_name: grafana
    ports:
      - "3001:3000"
    networks:
      - red_monitorizacion

  zabbix-server:
    image: zabbix/zabbix-server-pgsql
    container_name: zabbix-server
    environment:
      DB_SERVER_HOST: zabbix-db
    ports:
      - "10051:10051"
    networks:
      - red_monitorizacion

  zabbix-db:
    image: mysql:8.0
    environment:
      MYSQL_DATABASE: zabbix
      MYSQL_USER: zabbix
      MYSQL_PASSWORD: zabbix
      MYSQL_ROOT_PASSWORD: zabbix
    networks:
      - red_monitorizacion

  zabbix-web:
    image: zabbix/zabbix-web-nginx-mysql
    container_name: zabbix-web
    environment:
      DB_SERVER_HOST: zabbix-db
      DB_SERVER_PORT: 3306
      DB_SERVER_DBNAME: zabbix
      MYSQL_USER: zabbix
      MYSQL_PASSWORD: zabbix
      MYSQL_ROOT_PASSWORD: zabbix

    ports:
      - "8081:8080"
    networks:
      - red_monitorizacion

networks:
  red_monitorizacion:
```

El prometheus.yml es el siguiente:

```
global:
  scrape_interval: 15s

scrape_configs:
  - job_name: 'prometheus'
    static_configs:
      - targets: ['localhost:9090']

scrape_configs:
  - job_name: 'docker'
    static_configs:
      - targets: ['zabbix-agent:10050', 'node-exporter:9100']

  - job_name: 'qemu-vms'
    static_configs:
      - targets: ['192.168.200.188:9100', '192.168.200.195:9100', '192.168.200.234:9100']
```

Usando htop en grafana, zabbix y prometheus

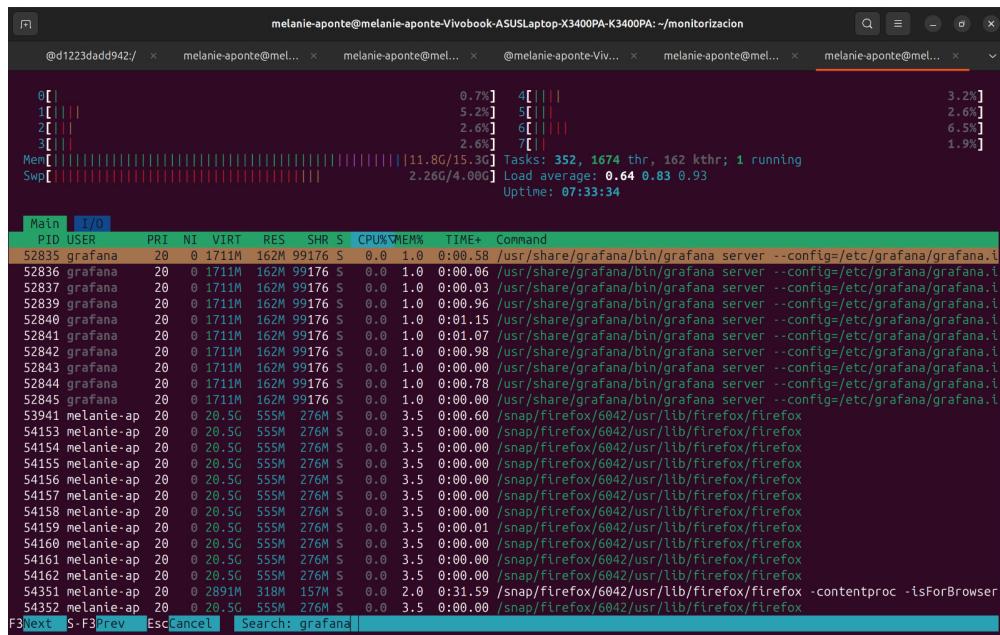


Figura 31: Htop grafana

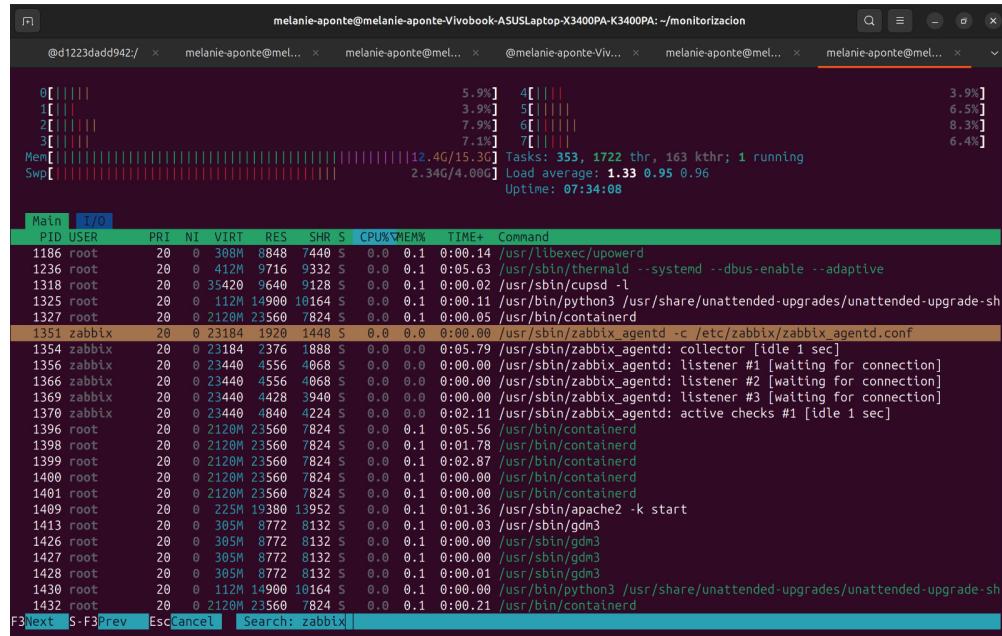


Figura 32: Htop zabbix

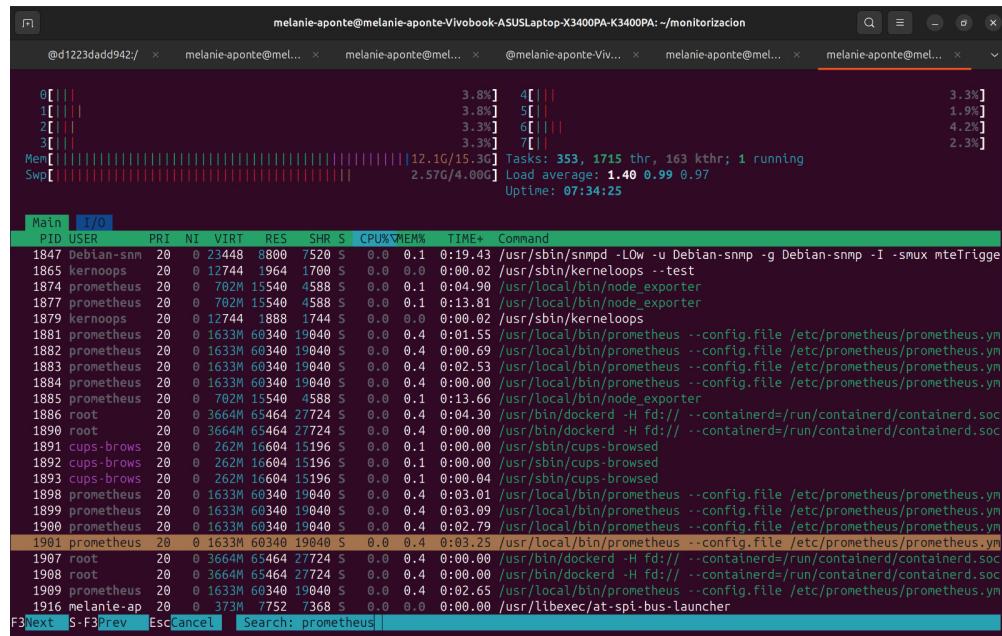
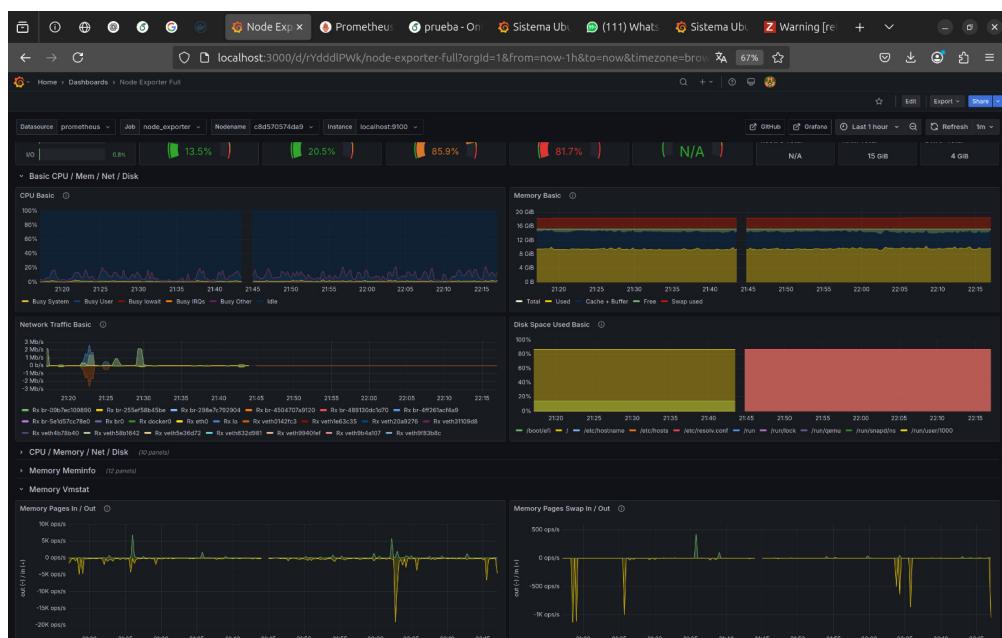
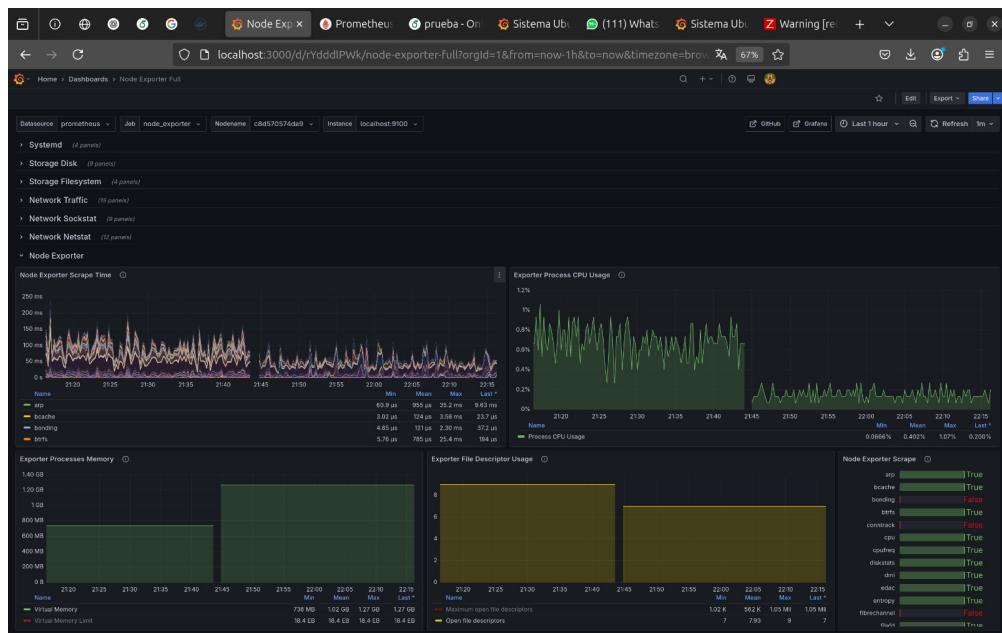


Figura 33: Htop prometheus

Para ver que los puertos están “escuchando”:

```
tcp6      0      0 ::1:3000          0:0:0:0:0:0:0:1  ESCUCHAR
tcp6      0      0 ::1:3001          0:0:0:0:0:0:0:1  ESCUCHAR
tcp6      0      0 ::1:80           0:0:0:0:0:0:0:1  ESCUCHAR
tcp6      0      0 ::1:9100         0:0:0:0:0:0:0:1  ESCUCHAR
tcp6      0      0 ::1:9090         0:0:0:0:0:0:0:1  ESCUCHAR
tcp6      0      0 ::1:9091         0:0:0:0:0:0:0:1  ESCUCHAR
tcp6      0      0 ::1:10050        0:0:0:0:0:0:0:1  ESCUCHAR
tcp6      0      0 ::1:10051        0:0:0:0:0:0:0:1  ESCUCHAR
tcp6      0      0 ::1:1631          0:0:0:0:0:0:0:1  ESCUCHAR
tcp6      0      0 ::1:8080          0:0:0:0:0:0:0:1  ESCUCHAR
```

A grafana se accede por el enlace: <http://localhost:3000>



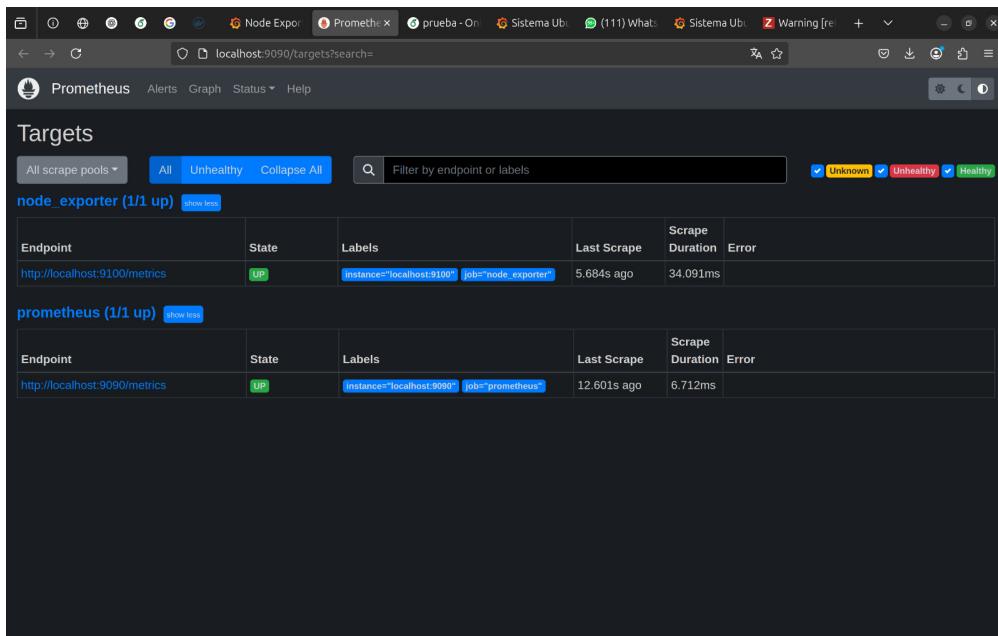


Figura 34: Prometheus

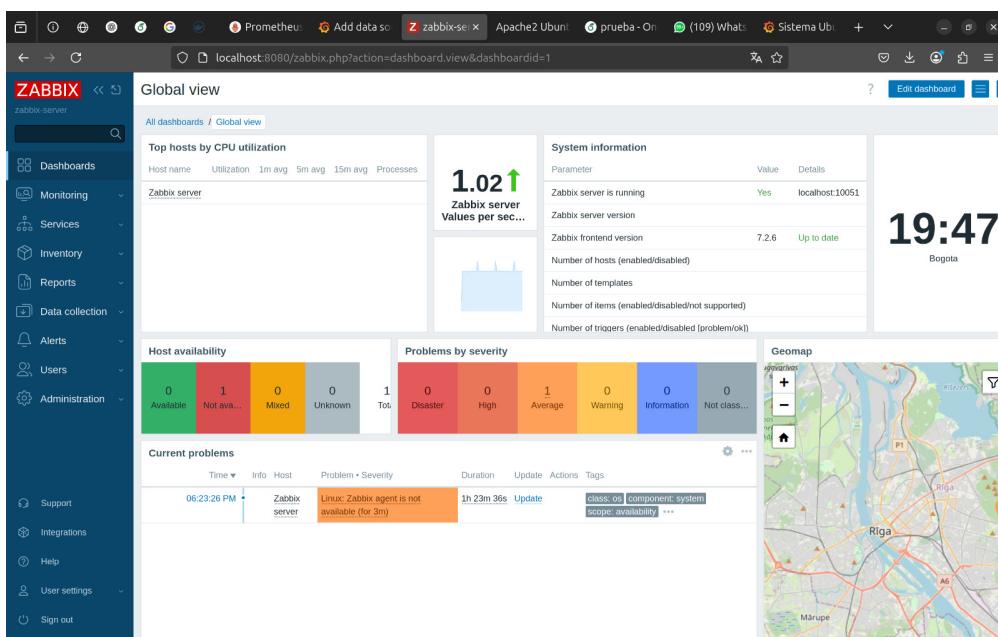


Figura 35: Zabbix