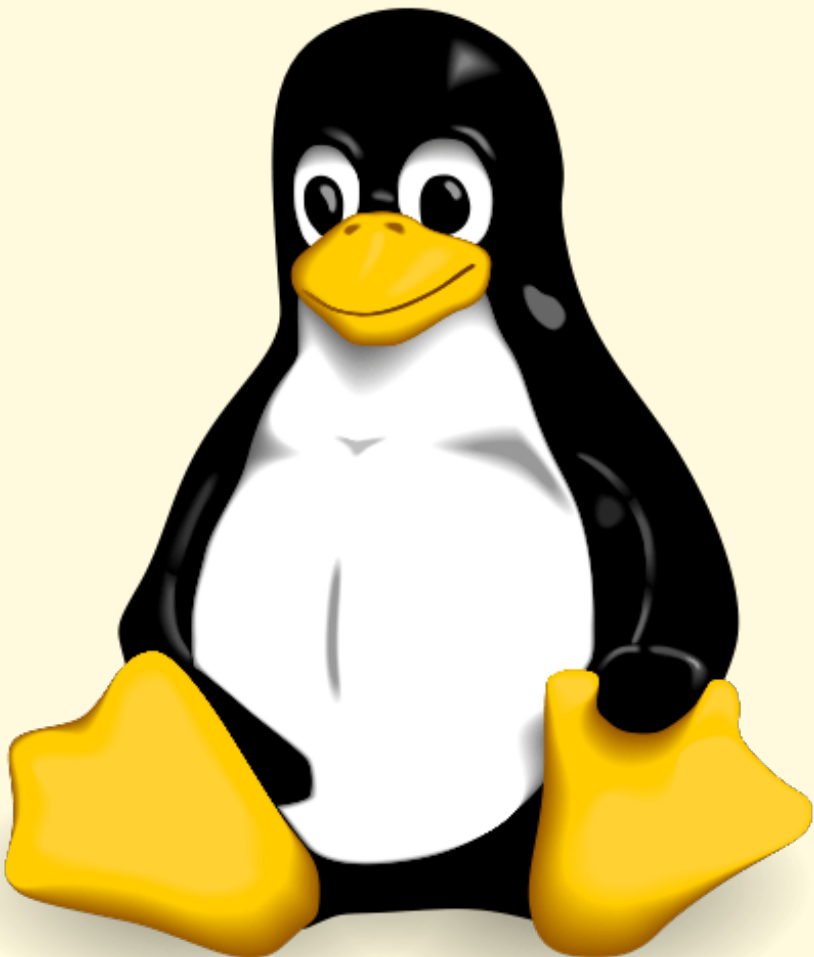


LINUX: MONITORIZACIÓN DEL SISTEMA



Juan Carlos Navidad García
Sistemas Operativos en Red

MONITORIZACION DE EVENTOS

1. Monitorización de eventos:

a. Función principal:

Monitorizar y controlar en qué situación se encuentra el sistema. Ya que gran parte de los sistemas son críticos, es decir, deben estar funcionando 365 días al año las 24 horas del día.

b. Objetivos:

- Aprovechar al máximo los recursos hardware del equipo.
- Prevención y notificación mediante alarmas de posibles problemas que puedan impedir el correcto funcionamiento del equipo.

c. Métodos usados.

El método más básico y en el que se basan los demás, es el sistema logs del SO Linux. Este es un mecanismo mediante el cual registran los mensajes generados por los programas, aplicaciones y procesos que se están ejecutando en el sistema.

2. Instala el entorno grafico GNOME: recuerda cambiar a root

a. Reconfigura dpkg: `dpkg --configure -a`

```
jnav@jnav-server:~$ sudo dpkg --configure -a
[sudo] password for jnav:
jnav@jnav-server:~$
```

b. Resolver dependencias: `apt -f install`

```
jnav@jnav-server:~$ sudo apt -f install
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 17 no actualizados.
jnav@jnav-server:~$ _
```

c. Actualizar paquetes: apt dist-upgrade

```
jnav@jnav-server:~$ sudo apt dist-upgrade
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Calculando la actualización... Hecho
Se actualizarán los siguientes paquetes:
  cloud-init dnsmasq-base libnetplan0 linux-base netplan.io nplan python3-software-properties
  rsync snapd software-properties-common ubuntu-advantage-tools ufw vim vim-common vim-runtime
  vim-tiny xxd
17 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
5 standard security updates
Se necesita descargar 31,9 MB de archivos.
Se utilizarán 143 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Des:1 http://es.archive.ubuntu.com/ubuntu bionic-updates/main amd64 linux-base all 4.5ubuntu1.7 [17,9 kB]
Des:2 http://es.archive.ubuntu.com/ubuntu bionic-updates/main amd64 libnetplan0 amd64 0.99-0ubuntu3~18.04.5 [22,6 kB]
Des:3 http://es.archive.ubuntu.com/ubuntu bionic-updates/main amd64 netplan.io amd64 0.99-0ubuntu3~18.04.5 [71,1 kB]
Des:4 http://es.archive.ubuntu.com/ubuntu bionic-updates/main amd64 nplan all 0.99-0ubuntu3~18.04.5 [1.800 B]
5% [Trabajando]
```

d. Instalar paquete del entorno grafico: apt install --reinstall ubuntu-desktop

```
jnav@jnav2:~$ sudo apt install --reinstall ubuntu-desktop
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  fonts-liberation2 fonts-opensymbol gir1.2-gst-plugins-base-1.0
  gir1.2-gstreamer-1.0 gir1.2-gudev-1.0 gir1.2-udisks-2.0
  grilo-plugins-0.3-base gstreamer1.0-gtk3 libboost-date-time1.65.1
  libboost-filesystem1.65.1 libboost-iostreams1.65.1 libboost-locale1.65.1
  libcdr-0.1-1 libclucene-contribs1v5 libclucene-core1v5 libcmis-0.5-5v5
  libcolamd2 libdazzle-1.0-0 libe-book-0.1-1 libdataserverui-1.2-2 libeot0
  libepubgen-0.1-1 libetonyek-0.1-1 libevent-2.1-6 libexiv2-14
  libfreerdp-client2-2 libfreerdp2-2 libgc1c2 libgee-0.8-2 libgexiv2-2
  libgom-1.0-0 libgpgmepp6 libgpod-common libgpod4 liblangtag-common
  liblangtag1 liblirc-client0 liblua5.3-0 libmediaart-2.0-0 libmspub-0.1-1
  libodfgen-0.1-1 libqqwing2v5 libraw16 libvenge-0.0-0 libsgutils2-2
  libssh-4 libsuitesparseconfig5 libvncclient1 libwinpr2-2 libxapian30
  libxmlsec1 libxmlsec1-nss lp-solve media-player-info python3-mako
  python3-markupsafe syslinux syslinux-common syslinux-legacy
  usb-creator-common
Utilice «sudo apt autoremove» para eliminarlos.
Paquetes recomendados:
```

e. Limpiar el sistema de bibliotecas inútiles de los paquetes descargados

i. Apt autoremove

```
jnav@jnav-server:~$ sudo apt autoremove
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
jnav@jnav-server:~$ _
```

ii. Apt clean

```
jnav@jnav-server:~$ sudo apt clean
jnav@jnav-server:~$
```

f. Reinicia: init 6 o reboot

```
jnav@jnav-server:~$ reboot
```

```
[ OK ] Stopped target Sound Card.
[ OK ] Stopped Ubuntu Advantage Timer for running repeated
[ OK ] Stopped Ubuntu Advantage Timer for running repeated jobs.
[ OK ] Closed Load/Save RF Kill Switch Status /dev/rfkill Watch.
[ OK ] Stopped target Cloud-init target.
[ OK ] Stopped Discard unused blocks once a week.
[ OK ] Stopped LVM2 PV scan on device 8:3...
[ OK ] Stopped Daily apt upgrade and clean activities.
[ OK ] Stopped target Host and Network Name Lookups.
[ OK ] Stopped Authorization Manager...
[ OK ] Stopped Execute cloud user/final scripts.
[ OK ] Stopped Session 1 of user jnav.
[ OK ] Stopped Apply the settings specified in cloud-config.
[ OK ] Stopped target Cloud-config availability.
[ OK ] Stopped User Manager for UID 1000...
[ OK ] Stopped Message of the Day.
[ OK ] Stopped Daily apt download activities.
[ OK ] Stopped target System Time Synchronized.
[ OK ] Stopped Daily Cleanup of Temporary Directories.
[ OK ] Stopped target Graphical Interface.
[ OK ] Stopped Accounts Service...
[ OK ] Stopped target Multi-User System.
[ OK ] Stopped LSB: Record successful boot for GRUB...
[ OK ] Stopped LSB: web-based administration interface for Unix systems...
[ OK ] Stopped Deferred execution scheduler...
[ OK ] Stopped BIND Domain Name Server...
[ OK ] Stopped OpenBSD Secure Shell server...
[ OK ] Stopped System Logging Service...
[ OK ] Stopped Dispatcher daemon for systemd-networkd...
[ OK ] Stopped LXDM - container startup/shutdown...
[ OK ] Stopped D-Bus System Message Bus...
[ OK ] Stopped FUSE filesystem for LXC...
[ OK ] Stopped target Login Prompts.
[ OK ] Stopped Getty on tty1...
[ OK ] Stopped Wait until snapd is fully seeded.
[ OK ] Stopped Regular background program processing daemon...
[ OK ] Stopped LSB: automatic crash report generation...
```

SISTEMA DE LOG (LINUX)**1. ¿En qué se basan los log de Linux?**

El demonio rsyslogd es el que gestiona los logs del sistema, usando las indicaciones especificadas en su archivo de configuración /etc/rsyslog.conf, en el que se indica que se registra y donde envían estos logs.

2. ¿Qué información nos muestra los logs?

Los Logs, que nos muestran el comportamiento de nuestros sistemas o programas, para así poder detectar cualquier problema.

3. Ordena de mayor a menor prioridad los niveles de mensajes.

(De menos a más prioridad): debug, info, notice, warning, warn, err, crit, alert, emerg y panic.

4. Indica algunos tipos de mensajes

Auth, authpriv, cron, Daemon, kern, lpr, mail, mark, news, security, syslog, user, uuco y local0–local7.

5. ¿Cuál es el demonio que gestiona los logs del sistema? ¿y el archivo de configuración?

El demonio que gestiona los logs del sistema es rsyslogd.

Su archivo de configuración está en /etc/Rsyslog.conf

6. ¿Dónde se guardan los logs? ¿Es posible que algunos programas almacenen sus propios logs?

Los logs se guardan en archivos ubicados en el directorio `/var/log`.

Cuando los programas necesitan guardar sus propios logs, estos crean un directorio propio dentro de `/var/log` (`/var/log/<programa>`).

7. Especifica algunos directorios de logs:

- a. **Referentes a el sistema:** `/var/log/syslog`
- b. **Los del núcleo:** `/var/log/kern.log`
- c. **De autenticación:** `/var/log/auth.log`
- d. **De instalación de paquetes:** `/var/log/dpkg.log`

8. ¿De qué se encarga logrotate y cuál es su fichero de configuración?

Logrotate es una utilidad de sistema que administra la compresión y rotación de archivos de logs en sistemas Linux.

9. Ejercicios del libro: 3.15–3-17

10. ¿Qué realiza el comando journalctl?

Te permite visualizar los logs del sistema

11. Define:**a. PID:**

Es el identificador de un proceso

b. UID:

Es el identificador de un usuario

c. GID:

Es el identificador de un grupo

12. ¿Cuál es el UID del root?

El UID del root es el 0, igual que el GID del grupo root.

13. Ejercicio 3.18

No tengo equipo en el aula, todo lo hago con el portátil y los datos solicitados ya los he proporcionado en las actividades anteriores.

CONOCIENDO EL HARDWARE DE NUESTRO EQUIPO: HARDINFO**1. Función de hardinfo**

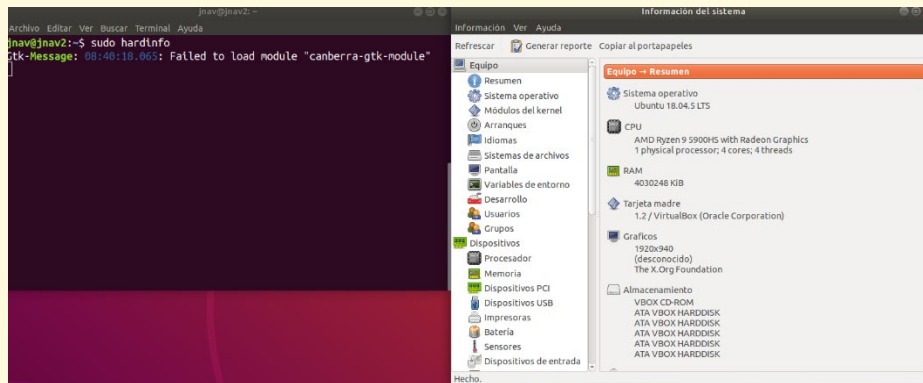
Verifica la información del hardware de un equipo.

2. Instalar hardinfo

Se utiliza el comando **sudo apt-get install hardinfo**

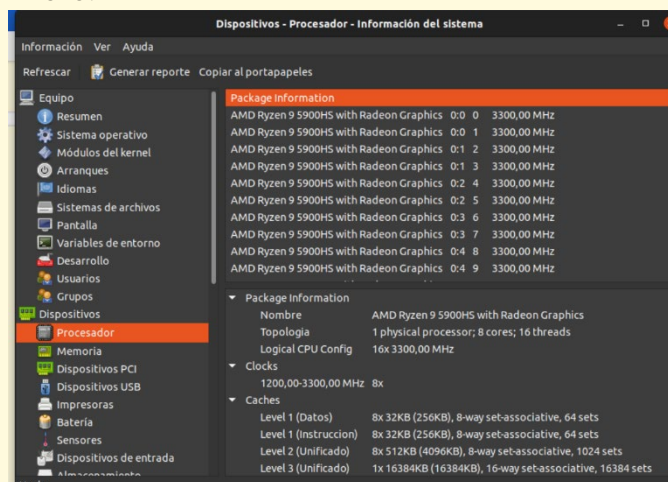
```
jnav@jnav2:~$ sudo apt-get install hardinfo
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
```

3. Abrir la app desde terminal

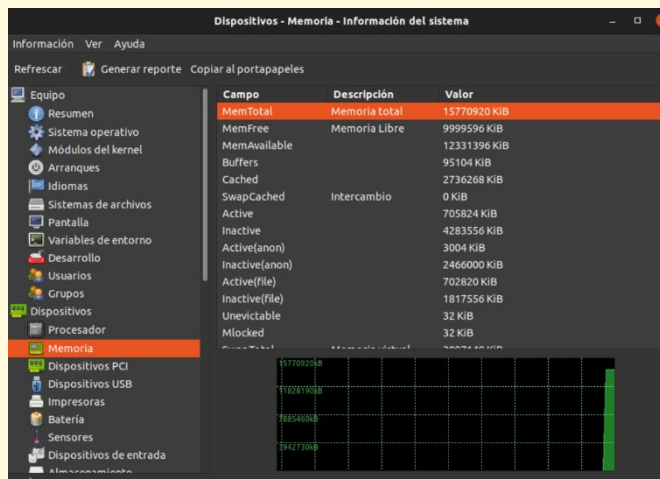


4. Analiza las principales características de tu equipo:

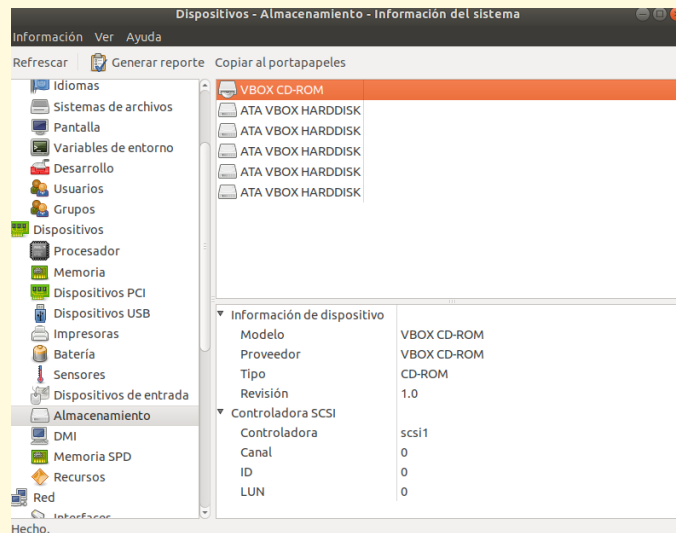
a. Micro:



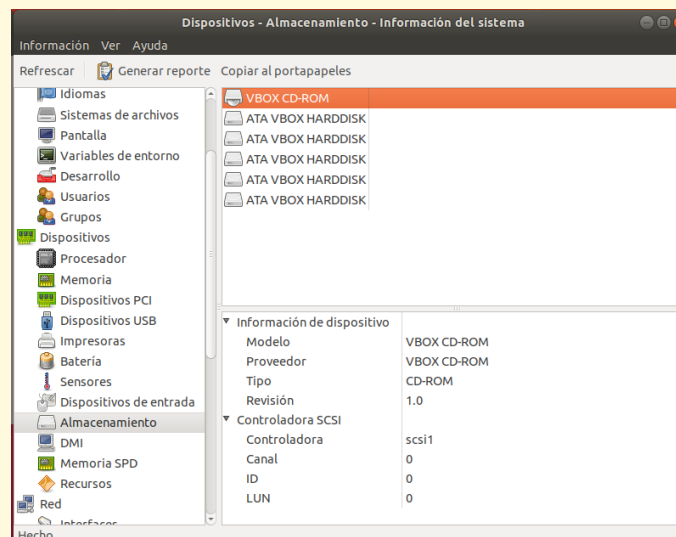
b. Memoria:



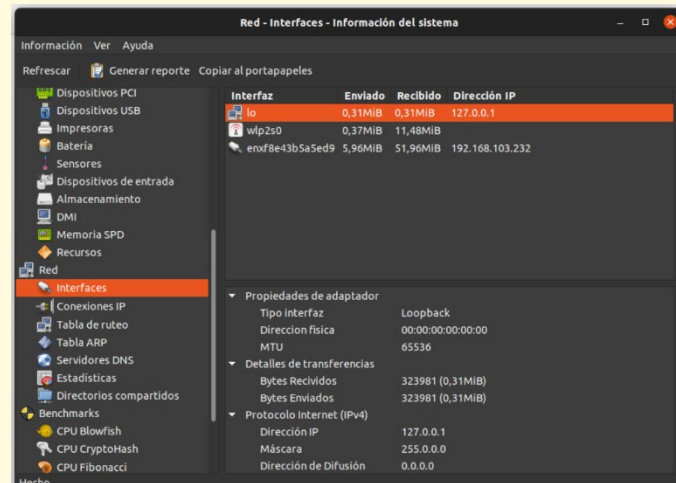
c. Storage:



d. Particiones:



e. Red:



CONOCIENDO EL HARDWARE DE NUESTRO EQUIPO: COMANDOS

1. Indica los archivos donde se guarda la información de:

- Micro:** /proc/cpuinfo
- Memoria:** /proc/meminfo
- DD:** /dev/<<nombre del disco>> (suele ser sda, sdb, sdc y las particiones sda1, sda2, sdb1, etc)
- Net:** lspci, este comando contiene todo el hardware conectado a la entrada PCI.

2. Utilizando el comando grep busca información del micro de:

- Fabricante (vendedor_id)

```
jnav@ROG-Zephyrus:~$ grep "vendor_id" /proc/cpuinfo
vendor_id       : AuthenticAMD
vendor_id       : AuthenticAMD
vendor_id       : AuthenticAMD
vendor_id       : AuthenticAMD
vendor_id       : AuthenticAMD
vendor_id       : AuthenticAMD
vendor_id       : AuthenticAMD
vendor_id       : AuthenticAMD
vendor_id       : AuthenticAMD
vendor_id       : AuthenticAMD
vendor_id       : AuthenticAMD
vendor_id       : AuthenticAMD
vendor_id       : AuthenticAMD
vendor_id       : AuthenticAMD
vendor_id       : AuthenticAMD
jnav@ROG-Zephyrus:~$
```

- Modelo (model name)

```
jnav@ROG-Zephyrus:~$ grep "model name" /proc/cpuinfo
model name      : AMD Ryzen 9 5900HS with Radeon Graphics
model name      : AMD Ryzen 9 5900HS with Radeon Graphics
model name      : AMD Ryzen 9 5900HS with Radeon Graphics
model name      : AMD Ryzen 9 5900HS with Radeon Graphics
model name      : AMD Ryzen 9 5900HS with Radeon Graphics
model name      : AMD Ryzen 9 5900HS with Radeon Graphics
model name      : AMD Ryzen 9 5900HS with Radeon Graphics
model name      : AMD Ryzen 9 5900HS with Radeon Graphics
model name      : AMD Ryzen 9 5900HS with Radeon Graphics
model name      : AMD Ryzen 9 5900HS with Radeon Graphics
model name      : AMD Ryzen 9 5900HS with Radeon Graphics
model name      : AMD Ryzen 9 5900HS with Radeon Graphics
model name      : AMD Ryzen 9 5900HS with Radeon Graphics
model name      : AMD Ryzen 9 5900HS with Radeon Graphics
model name      : AMD Ryzen 9 5900HS with Radeon Graphics
jnav@ROG-Zephyrus:~$
```

- Núcleos

```
jnav@ROG-Zephyrus:~$ grep "cpu cores" /proc/cpuinfo
cpu cores      : 8
cpu cores      : 8
cpu cores      : 8
cpu cores      : 8
cpu cores      : 8
cpu cores      : 8
cpu cores      : 8
cpu cores      : 8
cpu cores      : 8
cpu cores      : 8
cpu cores      : 8
cpu cores      : 8
cpu cores      : 8
cpu cores      : 8
cpu cores      : 8
cpu cores      : 8
jnav@ROG-Zephyrus:~$
```

3. Usa el comando LSCPU para desplegar información detallada sobre la arquitectura del micro

```
jnav@ROG-Zephyrus:~$ sudo lscpu
Arquitectura: x86_64
modo(s) de operación de las CPUs: 32-bit, 64-bit
Orden de los bytes: Little Endian
Address sizes: 48 bits physical, 48 bits virtual
CPU(s): 16
Lista de la(s) CPU(s) en línea: 0-15
Hilo(s) de procesamiento por núcleo: 2
Núcleo(s) por «socket»: 8
«Socket(s)»: 1
Modo(s) NUMA: 1
ID de fabricante: AuthenticAMD
Familia de CPU: 25
Modelo: 80
Nombre del modelo: AMD Ryzen 9 5900HS with Radeon Graphics
Revisión: 0
Frequency boost: enabled
CPU MHz: 1200.000
CPU MHz máx.: 3300.0000
CPU MHz mín.: 1200.0000
BogoMIPS: 6587.55
Virtualización: AMD-V
Cache L1d: 256 KiB
Cache L1i: 256 KiB
Cache L2: 4 MiB
Cache L3: 16 MiB
CPU(s) del nodo NUMA 0: 0-15
Vulnerability Itlb multihit: Not affected
Vulnerability L1tf: Not affected
Vulnerability Mds: Not affected
Vulnerability Meltdown: Not affected
Vulnerability Spec store bypass: Mitigation; Speculative Store Bypass disabled via prctl and seccomp
Vulnerability Spectre v1: Mitigation; usercopy/swapgs barriers and __user pointer sanitization
Vulnerability Spectre v2: Mitigation; Full AMD retpoline, IBPB conditional, IBRS_FW, STIBP always-on, RSB filling
Vulnerability Srbds: Not affected
Vulnerability Tsx async abort: Not affected
Indicadores: fpu vme de pse tsc msr pae mce cx8 apic sep mt
rr pge mca cmov pat pse36 clflush mmx fxsr sse
sse2 ht syscall nx mmxext fxsr_opt pdpe1gb rd
tscp lm constant_tsc rep_good nopl nonstop_tsc
cpuid extd_apicid aperfmperf not_rdt_mixed po
```

4. Ejecuta lshw y verifica que salida muestra

Muestra la información de todo el hardware del equipo

```
jnav@jnav2: ~
Archivo Editar Ver Buscar Terminal Ayuda
jnav@jnav2:~$ lshw
Aviso: debería ejecutar este programa como superusuario.
jnav2
  descripción: Computer
  anchura: 64 bits
  capacidades: smp vsyscall32
*-core
  descripción: Motherboard
  id físico: 0
*-memory
  descripción: Memoria de sistema
  id físico: 0
  tamaño: 3935MiB
*-cpu
  producto: AMD Ryzen 9 5900HS with Radeon Graphics
  fabricante: Advanced Micro Devices [AMD]
  id físico: 1
  información del bus: cpu@0
  anchura: 64 bits
  capacidades: fpu fpu_exception wp vme de pse tsc msr pae mce cx8 apic
sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ht syscall nx mmxext f
xsr_opt rdtscp x86-64 constant_tsc rep_good nopl nonstop_tsc cpuid extd_apicid t
sc_known_freq pni pclmulqdq ssse3 cx16 sse4_1 sse4_2 x2apic movbe popcnt aes xsa
ve avx rdrand hypervisor lahf_lm cmp_legacy cr8_legacy abm sse4a misalignsse 3dn
```

5. Verifica si tu ordenador es de 32 o 64 bits usando la herramienta lshw. La opción **-C** es para indicar el hardware del que queremos la información CPU, RAM...

```
jnav@jnav2: ~
Archivo Editar Ver Buscar Terminal Ayuda
jnav@jnav2:~$ sudo lshw -class cpu
*-cpu
  producto: AMD Ryzen 9 5900HS with Radeon Graphics
  fabricante: Advanced Micro Devices [AMD]
  id físico: 2
  información del bus: cpu@0
  anchura: 64 bits
```

6. Que hace CPUID. Instálalo y Verifica su salida

CPUID es una herramienta que te permite comprobar las especificaciones técnicas de tu procesador núcleo a núcleo:

```
jnav@ROG-Zephyrus:~$ sudo apt-get install cpuid
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes NUEVOS:
cpuid
```

```
memory management enhancements support = true
capacity bitmask length = 0xc (12)
number of classes of service = 0xf (15)
0x00000021 0x00: eax=0x00000004 ebx=0x00000000 ecx=0x00000000 edx=0x00000000
0x00000022 0x00: eax=0x00000000 ebx=0x00000000 ecx=0x00000000 edx=0x00000000
0x00000023 0x00: eax=0x00000000 ebx=0x00000000 ecx=0x00000000 edx=0x00000000
(instruction supported synth):
  CMOVDB = true
  conditional move/compare = true
  PREFETCH/PREFETCHW = true
  (multi-processing synth) = multi-core (c=16)
  (multi-processing method) = AMD
  (APIC widths synth): CORE_width=3 SMT_width=1
  (APIC synth): PKG_ID=0 CORE_ID=1 SMT_ID=1
  (uarch synth) = AMD Zen 3, 7nm
  (synth) = AMD (unknown model) [Zen 3], 7nm
CPU 4:
  vendor_id = "AuthenticAMD"
  version information (1/eax):
    processor type = primary processor (0)
    family = 0xf (15)
    model = 0x0 (0)
    stepping id = 0x0 (0)
    extended family = 0xa (10)
    extended model = 0x5 (5)
    (family synth) = 0x19 (25)
    (model synth) = 0x5b (91)
    (single synth) = AMD (unknown model) [Zen 3], 7nm
miscellaneous (1/ebx):
  process local APIC physical ID = 0x4 (4)
  maximum lds for CPUs in pkg = 0x10 (16)
  CLFLUSH line size = 0x8 (8)
  brand index = 0x0 (0)
brand id = 0x00 (0); unknown
feature information (1/edx):
  x87 FPU on chip = true
  VME: virtual-8086 mode enhancement = true
  DE: debugging extensions = true
  PSE: page size extensions = true
  TSC: time stamp counter = true
  RDNSR: and MONSR support = true
  PAE: physical address extensions = true
  MCE: machine check exception = true
  CPUXCHGDB inst. = true
```

7. Que hace nproc. Ejecútalo

Te dice los núcleos que tiene tu procesador.

```
jnav@jnav2:~$ sudo nproc
4
jnav@jnav2:~$
```

8. Utilizando el comando grep busca información de la memoria de:

a. Toda la información

```
jnav@ROG-Zephyrus:~$ sudo cat /proc/meminfo
MemTotal: 15770920 kB
MemFree: 9665952 kB
MemAvailable: 12110048 kB
Buffers: 99080 kB
Cached: 2873036 kB
SwapCached: 0 kB
Active: 783612 kB
Inactive: 4425724 kB
Active(anon): 2928 kB
Inactive(anon): 2574692 kB
Active(file): 780684 kB
Inactive(file): 1851032 kB
Unevictable: 32 kB
Mlocked: 32 kB
SwapTotal: 2097148 kB
SwapFree: 2097148 kB
Dirty: 720 kB
Writeback: 0 kB
AnonPages: 2237524 kB
Mapped: 1047708 kB
Shmem: 340312 kB
KReclaimable: 120396 kB
Slab: 241724 kB
SReclaimable: 120396 kB
SUnreclaim: 121328 kB
KernelStack: 20272 kB
PageTables: 36624 kB
WFS_Unstable: 0 kB
Bounce: 0 kB
WritebackTmp: 0 kB
CommitLimit: 9982608 kB
Committed_AS: 9694164 kB
VmallocTotal: 34359738367 kB
VmallocUsed: 49016 kB
VmallocChunk: 0 kB
Percpu: 18112 kB
HardwareCorrupted: 0 kB
AnonHugePages: 0 kB
ShmemHugePages: 0 kB
ShmemPmdMapped: 0 kB
FileHugePages: 0 kB
FilePmdMapped: 0 kB
HugePages_Total: 0
```

b. Tamaño de la memoria física

```
jnav@ROG-Zephyrus:~$ egrep "MemTotal" /proc/meminfo
MemTotal: 15770920 kB
jnav@ROG-Zephyrus:~$
```

c. Tamaño de la memoria virtual

```
jnav@ROG-Zephyrus:~$ egrep "SwapTotal" /proc/meminfo
SwapTotal: 2097148 kB
jnav@ROG-Zephyrus:~$
```

9. Utiliza el comando fdisk para conocer las particiones del disco. Identifícalas

Con el comando **fdisk -l** conseguimos lo siguiente:

```
Dispositivo      Comienzo      Final      Sectores  Tamaño  Tipo
/dev/nvme0n1p1    2048          206847     204800    100M    Sistema EFI
/dev/nvme0n1p2    206848        239615     32768     16M     Reservado para Microsoft
/dev/nvme0n1p3    239616        1896740863 1896501248 904,3G  Datos básicos de Microsoft
/dev/nvme0n1p4    1999142912    2000406527 1263616    617M    Entorno de recuperación de W
/dev/nvme0n1p5    1896740864    1999142911 102402048  48,8G   Sistema de ficheros de Linux

Las entradas de la tabla de particiones no están en el orden del disco.
```

10. Muestra el tipo de conexión de las tarjetas de red

```
jnav@ROG-Zephyrus:~$ lspci | grep "Network"
02:00.0 Network controller: MEDIATEK Corp. Device 7961
jnav@ROG-Zephyrus:~$
```

HERRAMIENTAS DE MONITORIZACION: COMANDOS

1. Comando para monitorización de la CPU: ejecútalo

El comando para monitorizar la cpu es top:

```

Areas: 369 total, 1 ejecutar, 368 hibernar, 0 detener, 0 zombie
%cpu(s): 2,3 us, 1,2 sy, 0,0 ni, 96,4 id, 0,0 wa, 0,0 hi, 0,1 si, 0,0 st
MB Mem : 15401,3 total, 9353,9 libre, 3020,4 usado, 3026,9 búfer/cache
MB Intercambio: 2048,0 total, 2048,0 libre, 0,0 usado, 11765,9 dispon Me

PID USUARIO PR NI VIRT RES SHR S %CPU %MEM HORA+ ORDEN
1995 jnav 20 0 6179192 371324 168600 S 19,5 2,4 3:43.32 gnome-shell
6806 jnav 20 0 4346800 244476 142496 S 11,6 1,6 2:23.28 spotify
7147 jnav 20 0 11,7g 554076 264440 S 10,9 3,5 3:58.65 GeckoMain
8078 jnav 20 0 3246184 732244 298428 S 10,6 4,6 4:11.87 Web Content
1284 jnav 9 -11 2686812 27376 21672 S 9,9 0,2 1:46.08 pulseaudio
8220 jnav 20 0 585524 67032 48984 S 4,3 0,4 0:25.00 gnome-term+
7079 jnav 20 0 30,5g 289348 101312 S 3,0 1,8 1:03.30 spotify
10099 root 20 0 0 0 0 I 1,7 0,0 0:01.25 kworker/u3+
11114 jnav 20 0 21956 4480 3496 R 0,3 0,0 0:00.13 top
1 root 20 0 166148 12436 7708 S 0,0 0,1 0:01.11 systemd
2 root 20 0 0 0 0 S 0,0 0,0 0:00.01 kthreadd
3 root 0 -20 0 0 0 I 0,0 0,0 0:00.00 rcu_gp
4 root 0 -20 0 0 0 I 0,0 0,0 0:00.00 rcu_par_gp
6 root 0 -20 0 0 0 I 0,0 0,0 0:00.00 kworker/0:0+
7 root 20 0 0 0 0 I 0,0 0,0 0:00.19 kworker/0:0+
9 root 0 -20 0 0 0 I 0,0 0,0 0:00.00 mm_percpu_+
10 root 20 0 0 0 0 S 0,0 0,0 0:00.00 rcu_tasks_+
11 root 20 0 0 0 0 S 0,0 0,0 0:00.00 rcu_tasks_+
12 root 20 0 0 0 0 S 0,0 0,0 0:00.10 ksoftirqd/0
13 root 20 0 0 0 0 I 0,0 0,0 0:02.44 rcu_sched
14 root rt 0 0 0 0 S 0,0 0,0 0:00.01 migration/0
15 root -51 0 0 0 0 S 0,0 0,0 0:00.00 idle_injec+
16 root 20 0 0 0 0 S 0,0 0,0 0:00.00 cpuhp/0
17 root 20 0 0 0 0 S 0,0 0,0 0:00.00 cpuhp/1
18 root -51 0 0 0 0 S 0,0 0,0 0:00.00 idle_injec+
19 root rt 0 0 0 0 S 0,0 0,0 0:00.20 migration/1
20 root 20 0 0 0 0 S 0,0 0,0 0:00.04 ksoftirqd/1
22 root 0 -20 0 0 0 I 0,0 0,0 0:00.00 kworker/1:0+
23 root 20 0 0 0 0 S 0,0 0,0 0:00.00 cpuhp/2
24 root -51 0 0 0 0 S 0,0 0,0 0:00.00 idle_injec+
25 root rt 0 0 0 0 S 0,0 0,0 0:00.21 migration/2
26 root 20 0 0 0 0 S 0,0 0,0 0:00.03 ksoftirqd/2
28 root 0 -20 0 0 0 I 0,0 0,0 0:00.00 kworker/2:0+
29 root 20 0 0 0 0 S 0,0 0,0 0:00.00 cpuhp/3
30 root -51 0 0 0 0 S 0,0 0,0 0:00.00 idle_injec+
31 root rt 0 0 0 0 S 0,0 0,0 0:00.21 migration/3
jnav@ROG-Zephyrus:~$

```

- Utiliza `top -u usuario` para monitorizar los procesos de un usuario concreto

El comando sería `top -u <<usuario>>`

```

top - 09:27:01 up 24 min, 1 user, load average: 0,83, 0,69, 0,63
Areas: 372 total, 2 ejecutar, 370 hibernar, 0 detener, 0 zombie
%cpu(s): 1,0 us, 1,4 sy, 0,0 ni, 96,6 id, 0,0 wa, 0,0 hi, 0,0 si, 0,0 st
MB Mem : 15401,3 total, 9211,5 libre, 3085,4 usado, 3104,4 búfer/cache
MB Intercambio: 2048,0 total, 2048,0 libre, 0,0 usado, 11663,0 dispon Me

PID USUARIO PR NI VIRT RES SHR S %CPU %MEM HORA+ ORDEN
1995 jnav 20 0 6174632 371260 168532 S 17,6 2,4 4:06.09 gnome-shell
7147 jnav 20 0 11,7g 650010 306084 S 17,6 4,1 4:44.05 GeckoMain
8078 jnav 20 0 3234312 735276 284636 R 11,8 4,7 4:24.98 Web Content
6937 jnav 20 0 323440 11788 7240 S 5,9 0,1 0:07.07 libus-daemon
7079 jnav 20 0 30,5g 275104 101312 S 5,9 1,7 1:03.74 spotify
11174 jnav 20 0 21956 4504 3516 R 5,9 0,0 0:00.02 top
1203 jnav 20 0 16100 9880 7504 S 0,0 0,1 0:00.42 systemd
1208 jnav 20 0 168812 3692 4 5 0,0 0,0 0:00.00 (sd-pan)
1280 jnav 9 -11 47812 6100 5856 S 0,0 0,0 0:00.03 pipewire
1282 jnav 9 -11 31660 6096 5856 S 0,0 0,0 0:00.04 pipewire-m+
1284 jnav 9 -11 2686812 27376 21672 S 0,0 0,2 1:55.70 pulseaudio
1290 jnav 20 0 397832 8800 6864 S 0,0 0,1 0:00.14 gnome-keyr+
1309 jnav 20 0 10540 6776 4020 S 0,0 0 0:01.14 dbus-daemon
1337 jnav 20 0 249328 8376 7356 S 0,0 0,1 0:00.08 gvfsd
1349 jnav 20 0 379020 6304 5712 S 0,0 0,0 0:00.00 gvfsd-fuse
1441 jnav 39 19 608072 27656 19220 S 0,0 0,2 0:01:52 tracker-nl+
1482 jnav 20 0 324604 9912 8140 S 0,0 0,1 0:00.14 gvfs-udisk+
1497 jnav 20 0 245280 6212 5504 S 0,0 0,0 0:00.05 gvfs-mtp-v+
1508 jnav 20 0 322472 7732 6944 S 0,0 0,0 0:00.11 gvfs-afc-v+
1519 jnav 20 0 246140 7080 6320 S 0,0 0,0 0:00.05 gvfs-goa-v+
1528 jnav 20 0 563972 60864 37784 S 0,0 0,4 0:00.56 goa-daemon
1579 jnav 20 0 324376 9228 8164 S 0,0 0,1 0:00.09 goa-identit+
1799 jnav 20 0 171076 6136 5640 S 0,0 0,0 0:00.00 gdm-wayland+
1804 jnav 20 0 230140 15220 13536 S 0,0 0,1 0:00.02 gnome-sess+
1885 jnav 20 0 100248 5040 4632 S 0,0 0,0 0:00.00 gnome-sess+
1905 jnav 20 0 526136 17424 14684 S 0,0 0,1 0:00.09 gnome-sess+
1992 jnav 20 0 309312 7280 6764 S 0,0 0,0 0:00.01 qt-spl-bus+
2016 jnav 20 0 8232 4436 3980 S 0,0 0,0 0:00.02 dbus-daemon
2521 jnav 20 0 246232 6472 5716 S 0,0 0,0 0:00.05 gvfs-gphoto+
2884 jnav 20 0 244064 5404 4988 S 0,0 0,0 0:00.00 xdg-permit+
2904 jnav 20 0 794456 20560 17376 S 0,0 0,1 0:00.09 gnome-shel+
2947 jnav 20 0 476976 34872 26464 S 0,0 0,2 0:00.15 evolution+
3001 jnav 20 0 156844 5912 5252 S 0,0 0,0 0:00.01 dconf-serv+
3011 jnav 20 0 171776 6700 6096 S 0,0 0,0 0:00.05 gvfsd-net+
3032 jnav 20 0 1609540 35504 29904 S 0,0 0,2 0:00.19 evolution+
3083 jnav 20 0 679276 29448 25572 S 0,0 0,2 0:00.06 evolution+

```

3. ¿Qué utilidad tiene el comando sensors? Instálalo y analiza la salida

El comando sensors te especifica las temperaturas y los voltajes de los componentes.

```

jnav@ROG-Zephyrus:~$ sudo sensors
asus-lisa-0000
Adapter: ISA adapter
cpu_fan:          0 RPM

BAT0-acpi-0
Adapter: ACPI interface
ln0:              15.83 V

amdgpu-pci-0400
Adapter: PCI adapter
vddgfx:           718.00 mV
vddnb:            649.00 mV
edge:             +37.0°C
power1:           0.00 W

nvme-pci-0300
Adapter: PCI adapter
Composite:        +29.9°C (low = -0.1°C, high = +82.8°C)
                  (crit = +84.8°C)
Sensor 1:         +29.9°C (low = -273.1°C, high = +65261.8°C)
Sensor 2:         +35.9°C (low = -273.1°C, high = +65261.8°C)

acpitz-acpi-0
Adapter: ACPI interface
temp1:            +40.0°C (crit = +120.0°C)

jnav@ROG-Zephyrus:~$

```

4. Funcionamiento de la memoria virtual

La memoria virtual (también conocida como archivo de paginación) es básicamente un bloque de espacio en su disco duro o unidad de estado sólido asignado por el SO para que actúe como RAM cuando su RAM física no tenga suficiente capacidad para programas en ejecución.

5. Comando para mostrar la ocupación de la memoria física y virtual.

a. Que hace el parámetro -h

Te da los detalles de uso de la memoria física y virtual

b. Ejecútalo e interpreta la información explicando cada parámetro lo que significa

```

jnav@ROG-Zephyrus:~$ free -h
              total        used         free      shared  buff/cache   available
Memoria:    15Gi         3,1Gi         8,9Gi        307Mi        3,0Gi        11Gi
Swap:        2,0Gi          0B         2,0Gi
jnav@ROG-Zephyrus:~$

```

6. Instala el paquete IPTraf-ng para monitorizar los paquetes de red


```
jnav@ROG-Zephyrus:~$ sudo apt-get install iptraf-ng
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  iptraf-ng
```

7. Descarga algo de internet para poder monitorizar la red antes y después de la descarga

```
jnav@ROG-Zephyrus:~$ sudo apt-get install nmap
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  liblinear4 lua-lpeg nmap-common
```

HERRAMIENTAS DE MONITORIZACION :ENTORNO GRÁFICO: WEBMIN

1. Para que sirve la herramienta webmin

Webmin es una interfaz web que le permite administrar archivos de configuración y volver a cargar programas sin necesidad de usar SSH.

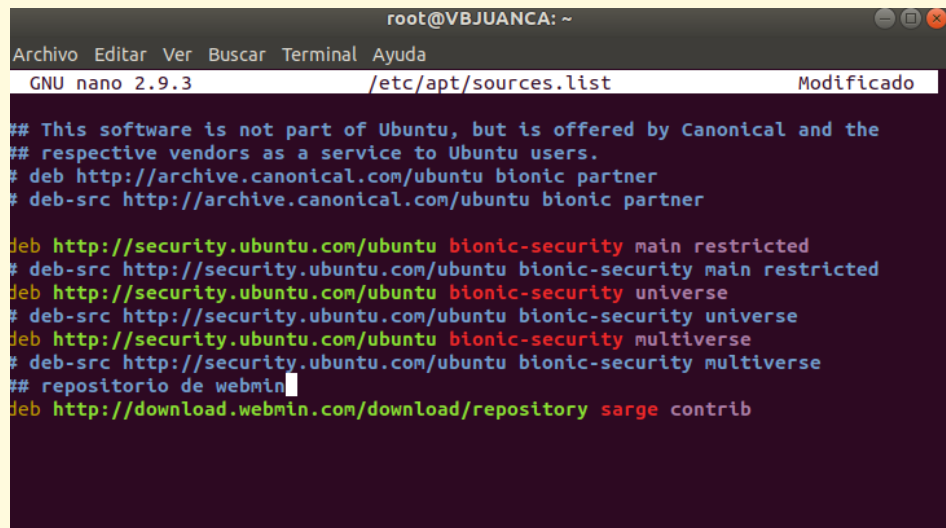
2. ¿Es posible monitorizar los servicios y apps con webmin?

Con Webmin se puede cambiar la configuración de los paquetes comunes sobre la marcha, incluidos los servidores web y las bases de datos, así como administrar usuarios, grupos, paquetes de software y servicios sin necesidad de utilizar comandos en una terminal.

3. Instala webmin

Primero añadimos el repositorio de paquetes de Webmin

```
deb http://download.webmin.com/download/repository sarge contrib
```



```

root@VBJUANCA: ~
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.9.3 /etc/apt/sources.list Modificado

## This software is not part of Ubuntu, but is offered by Canonical and the
## respective vendors as a service to Ubuntu users.
# deb http://archive.canonical.com/ubuntu bionic partner
# deb-src http://archive.canonical.com/ubuntu bionic partner

deb http://security.ubuntu.com/ubuntu bionic-security main restricted
# deb-src http://security.ubuntu.com/ubuntu bionic-security main restricted
deb http://security.ubuntu.com/ubuntu bionic-security universe
# deb-src http://security.ubuntu.com/ubuntu bionic-security universe
deb http://security.ubuntu.com/ubuntu bionic-security multiverse
# deb-src http://security.ubuntu.com/ubuntu bionic-security multiverse
## repositorio de webmin
deb http://download.webmin.com/download/repository sarge contrib

```

A continuación, agrego la clave PGP de Webmin para que el sistema confíe en el nuevo repositorio:

```
wget http://www.webmin.com/jcameron-key.asc
```

```
sudo apt-key add jcameron-key.asc
```



```

root@VBJUANCA:~# wget http://www.webmin.com/jcameron-key.asc
--2021-10-16 12:47:38-- http://www.webmin.com/jcameron-key.asc
Resolviendo www.webmin.com (www.webmin.com)... 216.105.38.11
Conectando con www.webmin.com (www.webmin.com)[216.105.38.11]:80... conectado.
Petición HTTP enviada, esperando respuesta... 301 Moved Permanently
Ubicación: https://www.webmin.com/jcameron-key.asc [siguiente]
--2021-10-16 12:47:40-- https://www.webmin.com/jcameron-key.asc
Conectando con www.webmin.com (www.webmin.com)[216.105.38.11]:443... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 1320 (1,3K) [text/plain]
Guardando como: "jcameron-key.asc"

jcameron-key.asc 100%[=====] 1,29K --.-KB/s en 0s
2021-10-16 12:47:41 (603 MB/s) - "jcameron-key.asc" guardado [1320/1320]

root@VBJUANCA:~# sudo apt-key add jcameron-key.asc
OK
root@VBJUANCA:~#

```

Luego, actualizo la lista de paquetes para que incluya el repositorio Webmin:

sudo apt update

```
root@VBJUANCA:~# sudo apt update
Obj:1 http://es.archive.ubuntu.com/ubuntu bionic InRelease
Obj:2 http://es.archive.ubuntu.com/ubuntu bionic-updates InRelease
Obj:3 http://security.ubuntu.com/ubuntu bionic-security InRelease
Obj:4 http://es.archive.ubuntu.com/ubuntu bionic-backports InRelease
Ign:5 http://download.webmin.com/download/repository sarge InRelease
Des:6 http://download.webmin.com/download/repository sarge Release [16,9 kB]
Des:7 http://download.webmin.com/download/repository sarge Release.gpg [173 B]
Des:8 http://download.webmin.com/download/repository sarge/contrib amd64 Packages [1.387 B]
Des:9 http://download.webmin.com/download/repository sarge/contrib i386 Packages [1.387 B]
Descargados 19,8 kB en 2s (9.481 B/s)
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se pueden actualizar 308 paquetes. Ejecute «apt list --upgradable» para verlos.
root@VBJUANCA:~#
```

Finalmente instalo Webmin:

Sudo apt install webmin

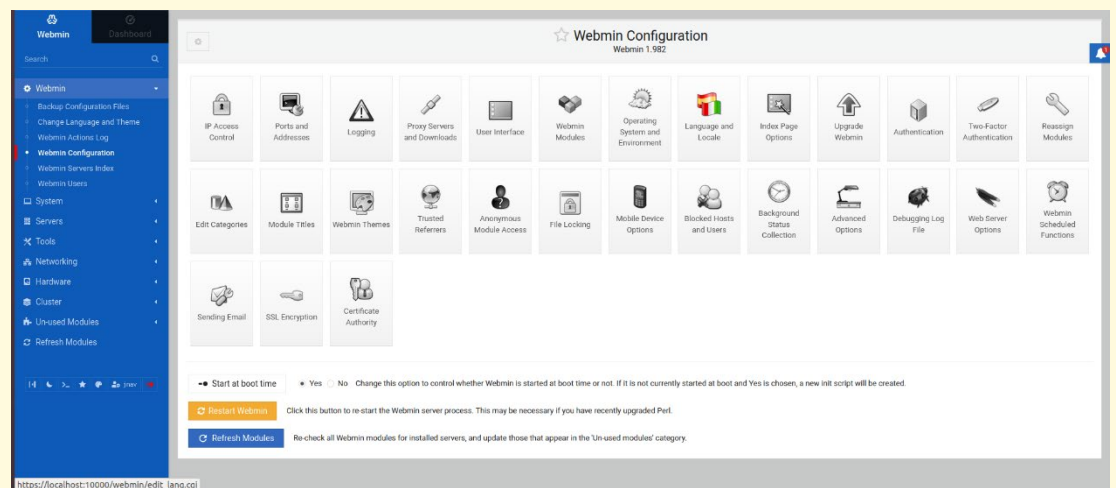
```
root@VBJUANCA: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
root@VBJUANCA:~# sudo apt install webmin  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias  
Leyendo la información de estado... Hecho  
Los paquetes indicados a continuación se instalaron de forma automática y ya no  
son necesarios.  
  fonts-liberation2 fonts-opensymbol gir1.2-gst-plugins-base-1.0  
  gir1.2-gstreamer-1.0 gir1.2-gudev-1.0 gir1.2-udisks-2.0  
  grilo-plugins-0.3-base gstreamer1.0-gtk3 libboost-date-time1.65.1  
  libboost-filesystem1.65.1 libboost-iostreams1.65.1 libboost-locale1.65.1  
  libcdr-0.1-1 libclucene-contribs1v5 libclucene-core1v5 libcmis-0.5-5v5  
  libcolamd2 libdazzle-1.0-0 libe-book-0.1-1 libdataserverui-1.2-2 libeot0  
  libepubgen-0.1-1 libetonyek-0.1-1 libevent-2.1-6 libexiv2-14  
  libfreerdp-client2-2 libfreerdp2-2 libgc1c2 libgee-0.8-2 libgexiv2-2  
  libgom-1.0-0 libgpgmepp6 libgpod-common libgpod4 liblangtag-common  
  liblangtag1 liblirc-client0 liblua5.3-0 libmediaart-2.0-0 libmspub-0.1-1  
  libodfgen-0.1-1 libqqwing2v5 libraw16 librevenge-0.0-0 libsgutils2-2  
  libssh-4 libsuitesparseconfig5 libvncclient1 libwinpr2-2 libxapian30  
  libxmlsec1 libxmlsec1-nss lp-solve media-player-info python3-mako  
  python3-markupsafe syslinux syslinux-common syslinux-legacy  
  usb-creator-common  
Utilice «sudo apt autoremove» para eliminarlos.  
Se instalarán los siguientes paquetes adicionales:  
  libauthen-pam-perl
```

4. Accede desde el navegador:

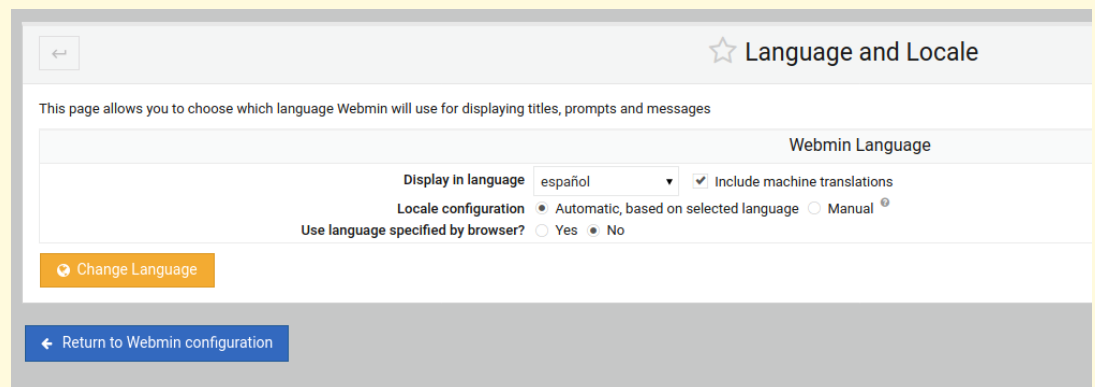
a. Cambia a español

Nos vamos al panel izquierdo y pulsamos en Webmin, posteriormente en Webmin Configuration.

Se nos abrirá la siguiente ventana y clicaremos sobre Language and Locale.

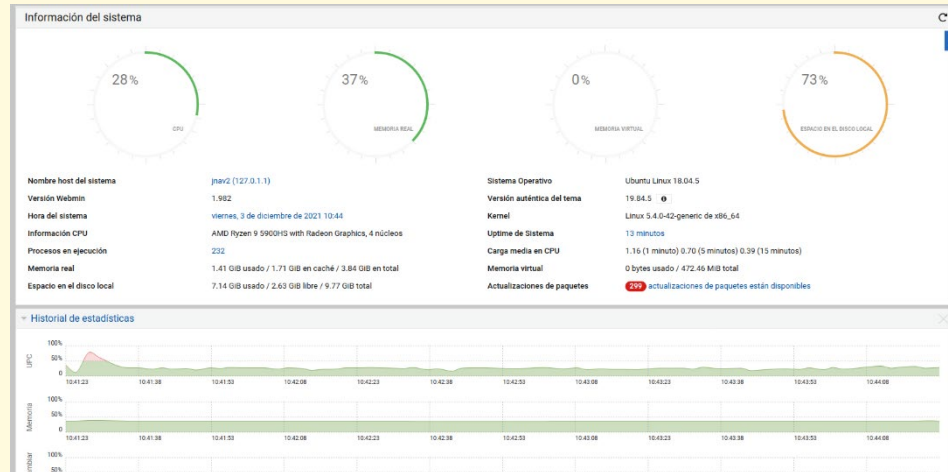


Cambiamos el idioma al español:



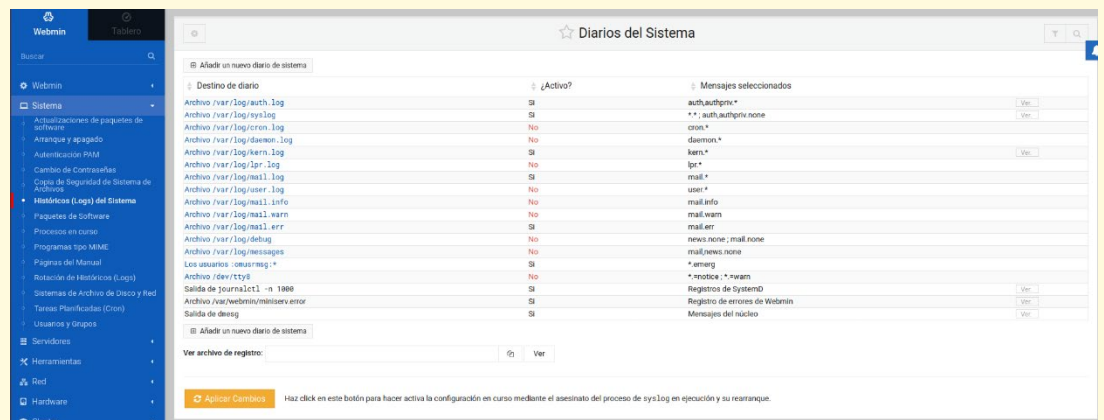
b. Obtén información del hardware:

La información del hardware aparece en la página principal de Webmin:



c. Consulta el fichero de log general. Consulta el fichero log donde se guarda la información del kernel del sistema

Simplemente nos vamos al apartado sistema del panel izquierdo y clicamos en Históricos (Logs) del sistema



d. Establece un ip estática

En el apartado de red del panel izquierdo, le damos a configuración de red.

Se nos abrirá la venta de configuración y clicaremos en interfaces de red:



Saldrán las interfaces de red que tenemos en nuestro equipo, pulsaremos sobre la que estemos utilizando:

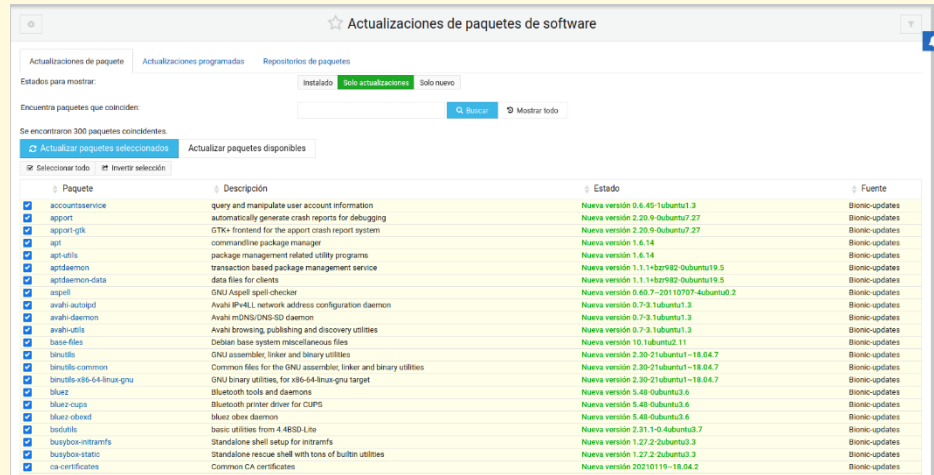


Al pulsar sobre la interfaz, se nos abrirá la pestaña de configuración de la interfaz, le cambiaremos la dirección IP:



e. Actualización:

Sobre el apartado sistema del panel izquierdo, nos vamos a actualización de paquetes y software y para actualizar le daremos a actualizar paquetes seleccionados:



- f. Verifica que la zona horaria sea Europa/Madrid, Spain mainland. En caso de no, actualizarla. Además, sincroniza el reloj de nuestro equipo con un NTP.

En el apartado Hardware del panel izquierdo, nos vamos a Hora del sistema.

Para comprobar la zona horaria, nos vamos al apartado cambiar zona horaria:



Para sincronizar la hora, nos iremos al apartado Hora del servidor de sincronización y le daremos a sincronizar y aplicar:

g. Cambiar el nombre del equipo.

En el apartado de red del panel izquierdo, le damos a configuración de red.

Hacemos clic en Nombre de máquina y cliente DNS

ADMINISTRAR SERVICIOS DE SYSTEMD CON SYSTEMCTL EN UBUNTU

1. ¿Qué es systemd?

Se trata de un mecanismo de inicio y administración de servicios del sistema operativo que interactúa con el núcleo.

2. ¿Como controlamos los servicios administrados por systemd?

Con el comando systemctl

3. ¿Qué servicio se encarga de las configuraciones de red de ubuntu en modo texto (configuración de los adaptadores de red)?

En Ubuntu 18 y 20.04 se encarga el servicio netstat, antiguamente era el networkd

4. ¿comprueba del servicio de red?

a. Su estado

```
jnav@jnav2:~$ systemctl status systemd-networkd.service
● systemd-networkd.service - Network Service
   Loaded: loaded (/lib/systemd/system/systemd-networkd.service; disabled; vendor preset: enabled)
   Active: inactive (dead)
     Docs: man:systemd-networkd.service(8)
lines 1-4/4 (END)
```

b. Si está activo

```
jnav@jnav2:~$ systemctl is-active systemd-networkd.service
inactive
```

c. Si está habilitado

```
jnav@jnav2:~$ systemctl is-enabled systemd-networkd.service
disabled
jnav@jnav2:~$
```

d. Si tiene un problema

```
jnav@jnav2:~$ systemctl is-failed systemd-networkd.service
inactive
jnav@jnav2:~$
```

5. Deshabilita/habilita el servicio de red

```
jnav@jnav2:~$ sudo systemctl enable systemd-networkd.service
jnav@jnav2:~$ sudo systemctl disable systemd-networkd.service
Removed /etc/systemd/system/sockets.target.wants/systemd-networkd.socket.
Removed /etc/systemd/system/multi-user.target.wants/systemd-networkd.service.
Removed /etc/systemd/system/network-online.target.wants/systemd-networkd-wait-online.service.
Removed /etc/systemd/system/dbus-org.freedesktop.network1.service.
jnav@jnav2:~$
```

6. Para/Inicia el servicio de red

```
jnav@jnav2:~$ systemctl start systemd-networkd.service
jnav@jnav2:~$ sudo systemctl stop systemd-networkd.service
```

7. Reinicia el servicio de red

```
jnav@jnav2:~$ sudo systemctl restart systemd-networkd.service
jnav@jnav2:~$
```

8. Mediante webmin

a. Lista los servicios del sistema

En el apartado izquierdo de Webmin clicamos sobre Procesos en curso y nos saldrán todos los servicios del sistema:

| PID | Usuario | Memoria | UCP | Buscar | Ejecutar |
|------|-----------------|---------|-----|--------|--|
| 1 | root | | | | /sbin/init splash |
| 360 | root | | | | /lib/systemd/systemd-journald |
| 379 | root | | | | /lib/systemd/systemd-udev |
| 440 | systemd-resolve | | | | /lib/systemd/systemd-resolved |
| 638 | root | | | | /lib/systemd/systemd-logind |
| 640 | messagebus | | | | /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-... |
| 698 | syslog | | | | /usr/sbin/rsyslogd -n |
| 699 | root | | | | /usr/sbin/cupsd |
| 700 | avahi | | | | avahi-daemon running [nuc2.local] |
| 709 | avahi | | | | avahi-daemon: croot helper |
| 701 | root | | | | /usr/sbin/NetworkManager --no-daemon |
| 2481 | root | | | | /usr/sbin/dhclient-d -q -f /usr/lib/NetworkManager/nm-dhcp-helper -pf /run/dhclient... |
| 704 | root | | | | /usr/sbin/irqbalance --foreground |
| 706 | root | | | | /usr/sbin/cron -f |
| 708 | root | | | | /usr/bin/wpa_supplicant -u -s -O /run/wpa_supplicant |
| 711 | root | | | | /usr/bin/python3 /usr/bin/networkd-dispatcher --run-startup-triggers |
| 717 | root | | | | /usr/lib/udev/rules.d/60.rules |
| 718 | root | | | | /usr/sbin/cupsd -l |
| 783 | lp | | | | /usr/lib/cups/notifier/dbus-dbus:// |
| 724 | root | | | | /usr/lib/AccountsService/accounts-daemon |
| 733 | root | | | | /usr/sbin/ModemManager --filter-policy=strict |
| 738 | root | | | | /usr/lib/cups/napd |
| 778 | root | | | | /usr/lib/policykit-1/policyd --no-debug |
| 779 | root | | | | /usr/bin/cups-browsed |
| 826 | bind | | | | /usr/sbin/named -f -u bind |
| 827 | root | | | | /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown --pa... |
| 920 | whoopsie | | | | /usr/bin/whoopsie -f |
| 927 | kernoops | | | | /usr/sbin/kernoops --test |
| 933 | kernoops | | | | /usr/sbin/kernoops |
| 1002 | root | | | | /usr/bin/madmind --monitor --scan |

b. Explica el proceso para Editar el servicio cron

Para editar el servicio Cron, buscaremos en la lista este servicio y pulsaremos sobre él para editarlo:

```

1 #!/bin/sh
2 # Start/stop the cron daemon.
3
4 # See BEGIN INIT INFO
5 # Provides: cron
6 # Required-Start: $network $syslog $time
7 # Required-Stop: $network $syslog $time
8 # Should-Start: $network $syslog $time $cron $time
9 # Should-Stop: $network $syslog $time $cron $time
10 # Default-Start: 2 3 4 5
11 # Default-Stop:
12 # Short-Description: Regular background program processing daemon.
13 # Description: cron is a standard UNIX program that runs user-specified
14 # programs at periodic intervals. cron uses a
15 # number of features to the basic UNIX cron, including better
16 # security and more powerful configuration options.
17 # See END INIT INFO
18
19 PATH=/bin:/usr/bin:/sbin:/usr/sbin
20 DESC="cron daemon"
21 NAME=cron
22 DAEMON=/usr/sbin/cron
23 PIDFILE=/var/run/cron.pid
24 SCRIPTNAME=/etc/init.d/"$NAME"
25
26 test -f $DAEMON || exit 0
27
28 /lib/lsb/init-functions
  
```