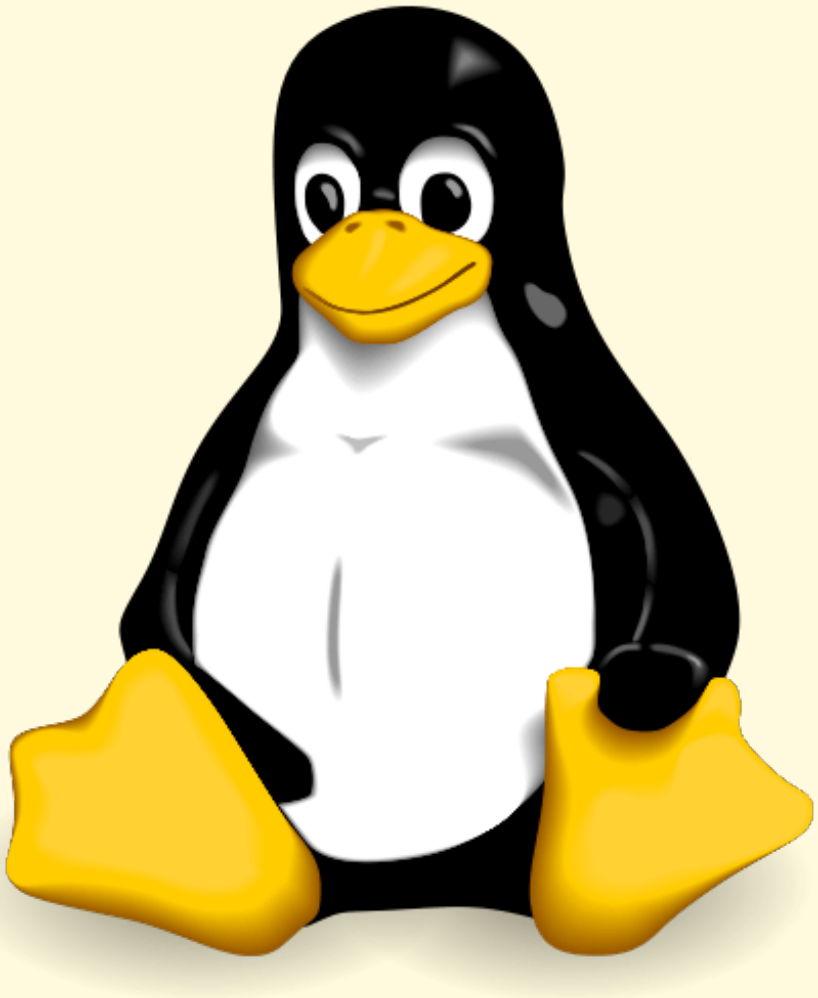
LINUX: MONITORIZACIÓN DEL SISTEMA



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**

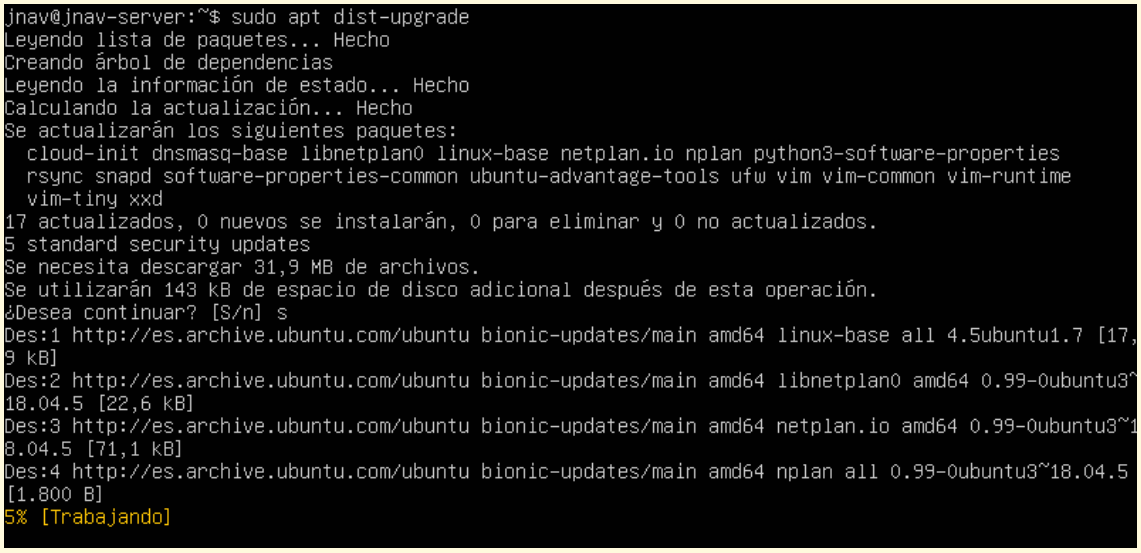
   a. Reconfigura dpkg: dpkg --configure -a

```
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. Acutalizar paquetes: apt dist-upgrade



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

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.
         Stopping LVM2 PV scan on device 8:3...
[  OK  ] Stopped Daily apt upgrade and clean activities.
[  OK  ] Stopped target Host and Network Name Lookups.
         Stopping Authorization Manager...
[  OK  ] Stopped Execute cloud user/final scripts.
         Stopping Session 1 of user jnav.
[  OK  ] Stopped Apply the settings specified in cloud-config.
[  OK  ] Stopped target Cloud-config availability.
         Stopping 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.
         Stopping Accounts Service...
[  OK  ] Stopped target Multi-User System.
         Stopping LSB: Record successful boot for GRUB...
         Stopping LSB: web-based administration interface for Unix systems...
         Stopping Deferred execution scheduler...
         Stopping BIND Domain Name Server...
         Stopping OpenBSD Secure Shell server...
         Stopping System Logging Service...
         Stopping Dispatcher daemon for systemd-networkd...
         Stopping LXD - container startup/shutdown...
         Stopping D-Bus System Message Bus...
         Stopping FUSE filesystem for LXC...
[  OK  ] Stopped target Login Prompts.
         Stopping Getty on tty1...
[  OK  ] Stopped Wait until snapd is fully seeded.
         Stopping Regular background program processing daemon...
         Stopping 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 gestión 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 autentificación:** /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

CONOCIENDO EL HARDWARE DE NUESTRO EQUIPO: HARDINFO

1. **Función de hardinfo**

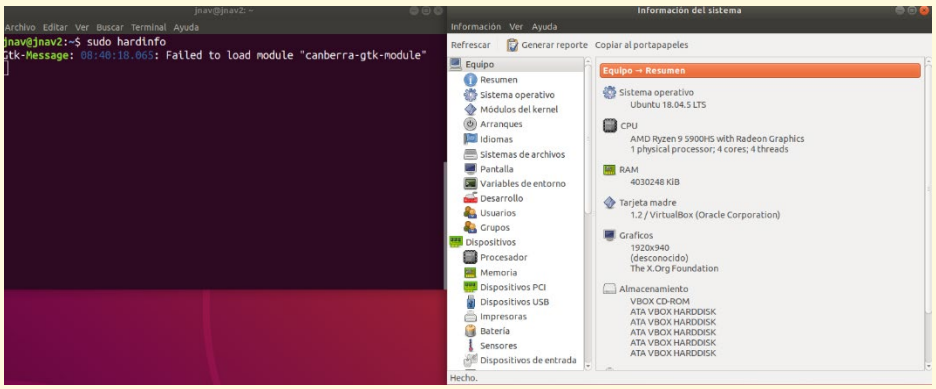
   Verifica la información del hardware de un equipo.

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: AMD Ryzen 9 5900HS; 8 Núcleos; 16 Hilos.
    b. Memoria: 16GB 3200 Mhz
    c. Storage:
    d. Particiones:
    e. Red:

CONOCIENDO EL HARDWARE DE NUESTRO EQUIPO: COMANDOS

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

    a. **Micro:** /proc/cpuinfo

    b. **Memoria:** /proc/meminfo

    c. **DD:** /dev/<<nombre del disco>> (suele ser sda, sdb, sdc y las particiones sda1, sda2, sdb1, etc)

    d. **Net:** lspci, este comando contiene todo el hardware conectado a la entrada PCI.

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

    a. Toda la información

    b. Fabricante (vendedor_id)

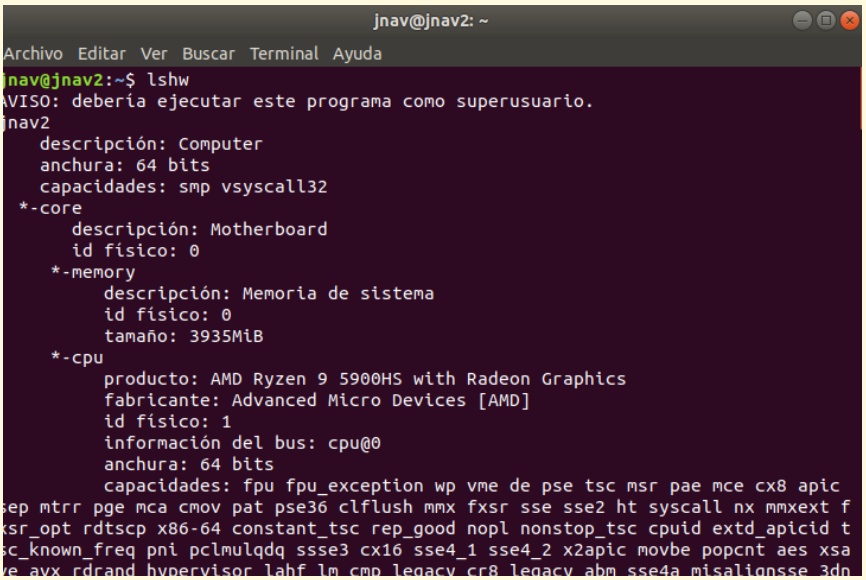
    c. Modelo (model name)

    d. Núcleos

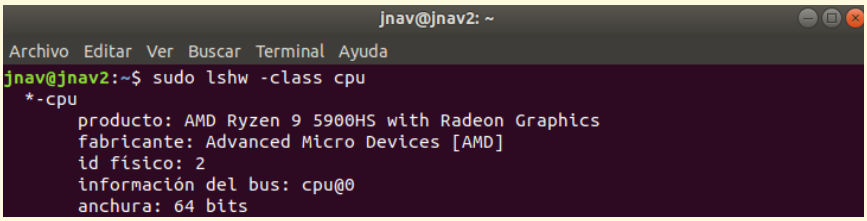
3. Usa el comando LSCPU para desplegar información detallada sobre la arquitectura del micro

4. **Ejecuta lshw y verifica que salida muestra**

   Muestra la información de todo el hardware del equipo



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…**



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

7. Que hace CPUID. Instálalo y Verifica su salida

8. **Que hace nproc. Ejecútalo**

   Te dice los núcleos que tiene tu procesador.

9. Utilizando el comando grep busca información de la memoria de:
   a. Toda la información
   b. Tamaño d la memoria física
   c. Tamaño de la memoria virtual

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

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

HERRAMIENTAS DE MONITORIZACION: COMANDOS

1. Comando para monitorización de la CPU: ejecútalo
2. Utiliza top -u usuario para monitorizar los procesos de un usuario concreto
3. ¿Qué utilidad tiene el comando sensors? Instalalo y analiza la salida
4. Funcionamiento de la memoria virtual
5. Comando para mostrar la ocupación de la memoria física y virtual.
    a. Que hace el parámetro -h
    b. Ejecútalo e interpreta la información explicando cada parámetro lo que significa
6. Comando para mostrar la ocupación del sistema:
    a. Ejecútalo e interpreta resultado
7. Instala el paquete IPTraf-ng para monitorizar los paquetes de red
8. Descarga algo de internet para poder monitorizar la red antes y después de la descara

HERRAMIENTAS DE MONITORIZACION :ENTORNO GRÁFICO: WEBMIN

1. Para que sirve la herramienta webmin
2. ¿Es posible monitorizar los servicios y apps con webmin?
3. Instala webmin
   http://somebooks.es/instala-webmin-y-administra-ubuntu-20-04-desde-el-navegador/

4. Accede desde el navegador:
    a. Cambia a español
       http://somebooks.es/poner-webmin-en-espanol/

b. Obtén información de El hardware
c. Consulta el fichero de log general. Consulta el fichero log donde se guarda la información del kernel del sistema http://somebooks.es/administrar-eventos-de-ubuntu-18-04-lts-con-webmin/

d. Establece un ip estatica http://somebooks.es/establecer-una-direccion-ip-estatica-en-ubuntu-con-webmin/

e. Actualización: verificar si hay actualizaciones y actualizar http://somebooks.es/establecer-una-direccion-ip-estatica-en-ubuntu-con-webmin/

f. Verifica que la zona horaria sea Europa/Madrid, spain mainland. En caso de no, actualizarla. Ademas Sincroniza el reloj de nuestro equipo con un NTP. http://somebooks.es/establecer-la-fecha-hora-y-zona-horaria-en-ubuntu-usando-webmin/

g. Cambiar el nombre del equipo. http://somebooks.es/proporcionar-un-nuevo-nombre-para-el-equipo-en-ubuntu-usando-webmin/

ADMINISTRAR SERVICIOS DE SYSTEMD CON SYSTEMCTL EN UBUNTU

http://somebooks.es/administrar-servicios-systemd-systemctl-ubuntu-parte-1/

http://somebooks.es/administrar-servicios-demonios-de-ubuntu-18-04-lts-con-webmin/

1. ¿Qué es systemd?
2. ¿Como controlamos los servicios administrados por systemd?
3. ¿Qué servicio se encarga de las configuraciones de red de ubuntu en modo texto (configuración de los adaptadores de red)?
4. ¿comprueba del servicio de red?
    a. Su estado
    b. Si esta activo
    c. Si está habilitado

    d. Si tiene un problema
5. Deshabilita/habilita el servicio de red
6. Para/Inicia el servicio de red
7. Reinicia el servicio de red
8. Mediante webmin
    a. Lista los servicios del sistema
    b. Explica el proceso para Editar el servicio cron