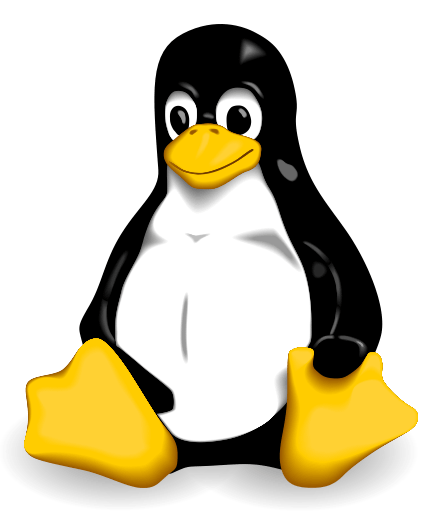
**Juan Carlos Navidad García**

**Sistemas Operativos en Red**



**LINUX: MONITORIZACIÓN DEL SISTEMA**

**MONITORIZACION DE EVENTOS**

1. **Monitorización de eventos:**
   1. **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.

* 1. **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.
  1. **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.

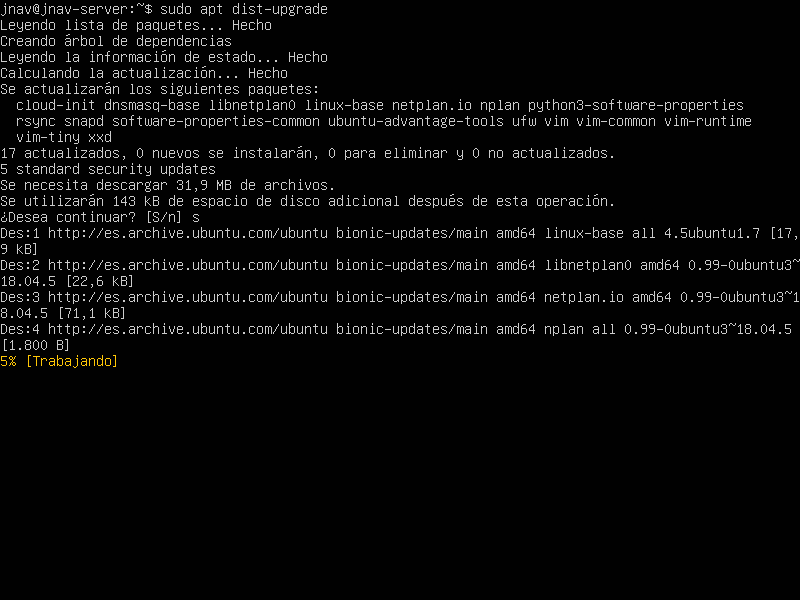
1. **Instala el entorno grafico GNOME: recuerda cambiar a root**
   1. Reconfigura dpkg: dpkg --configure -a



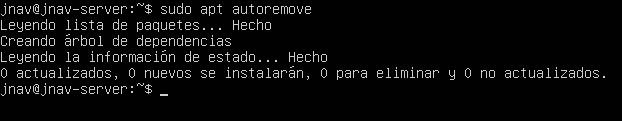
* 1. Resolver dependencias: apt -f install



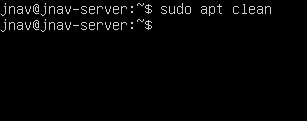
* 1. Acutalizar paquetes: apt dist-upgrade



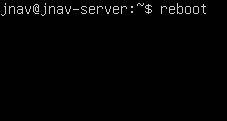
* 1. Instalar paquete del entorno grafico: apt install -reinstall ubuntu-desktop
  2. Limpiar el sistema de bibliotecas inútiles de los paquetes descargados
     1. Apt autoremove

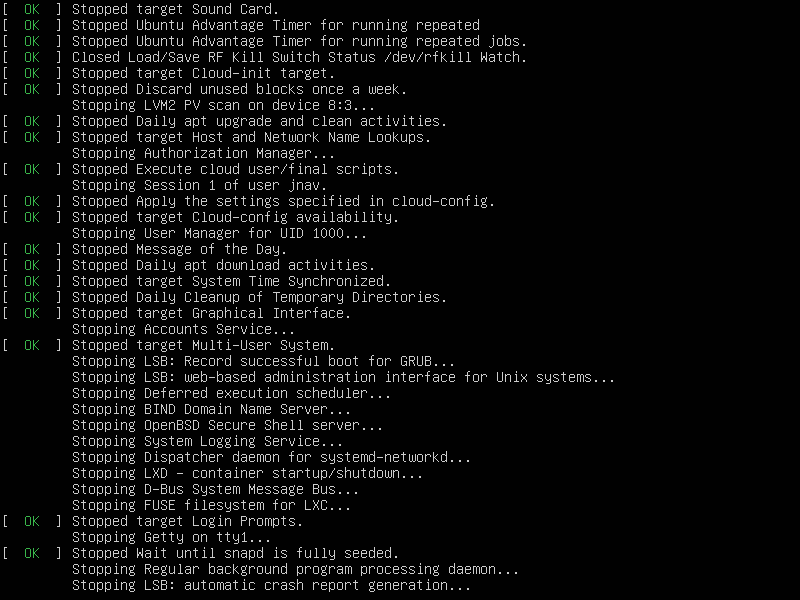


* + 1. Apt clean



* 1. Reinicia: init 6 o reboot





**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.

1. **¿Qué información nos muestra los logs?**

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

1. **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.

1. **Indica algunos tipos de mensajes**

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

1. **¿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

1. **¿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>).

1. **Especifica algunos directorios de logs:**
   1. **Referentes a el sistema:** /var/log/syslog
   2. **Los del núcleo:** /var/log/kern.log
   3. **De autentificación:** /var/log/auth.log
   4. **De instalación de paquetes:** /var/log/dpkg.log
2. **¿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.

1. Ejercicios del libro: 3.15-3-17
2. ¿Qué realiza el comando journalctl?
3. Define:
   1. PID
   2. UID
   3. GID
4. ¿Cuál es el UID del root
5. Ejercicio 3.18

**CONOCIENDO EL HARDWARE DE NUESTRO EQUIPO: HARDINFO**

1. Función de hardinfo
2. Instalar hardinfo
3. Abrir la app desde terminal
4. Analiza las principales características de tu equipo:
   1. Micro
   2. Memoria
   3. Storage
   4. Particiones
   5. Red

**CONOCIENDO EL HARDWARE DE NUESTRO EQUIPO: COMANDOS**

1. Indica los archivos donde se guarda la información de:
   1. Micro
   2. Memoria
   3. DD
   4. Net
2. Utilizando el comando grep busca información del micro de:
   1. Toda la información
   2. Fabricante (vendedor\_id)
   3. Modelo (model name)
   4. Nucleos
3. Usa el comando LSCPU para desplegar información detallada sobre la arquitectura del micro
4. Ejecuta lshw y verifica que salida muestra

https://esgeeks.com/lshw-ver-informacion-hardware-linux/

1. 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…
2. Usa el comando LSCPU para desplegar información detallada sobre la arquitectura del micro
3. Que hace CPUID. Instálalo y Verifica su salida
4. Que hace nproc. Ejecútalo
5. Utilizando el comando grep busca información de la memoria de:
   1. Toda la información
   2. Tamaño d la memoria física
   3. Tamaño de la memoria virtual
6. Utiliza el comando fdisk para conocer las particiones del disco. Identifícalas
7. 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.
   1. Que hace el parámetro -h
   2. Ejecútalo e interpreta la información explicando cada parámetro lo que significa
6. Comando para mostrar la ocupación del sistema:
   1. 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/>

1. Accede desde el navegador:
   1. Cambia a español

http://somebooks.es/poner-webmin-en-espanol/

* 1. Obtén información de El hardware
  2. 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/

* 1. Establece un ip estatica

<http://somebooks.es/establecer-una-direccion-ip-estatica-en-ubuntu-con-webmin/>

* 1. Actualización: verificar si hay actualizaciones y actualizar

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

* 1. 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/

* 1. 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?
   1. Su estado
   2. Si esta activo
   3. Si está habilitado
   4. 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
   1. Lista los servicios del sistema
   2. Explica el proceso para Editar el servicio cron