

Administración de Sistemas Operativos

Tema 6. Auditoría y monitorización

Contenidos

- Consultar la configuración del sistema
- Registros de actividad (*logs*)
- Registros de accesos al sistema
- Sistema de ficheros **/proc**
- Monitorizar la CPU y los procesos
- Monitorizar la memoria
- Monitorizar la E/S y los sistemas de ficheros

Auditoría y monitorización

- ¿Para qué?
 - Para saber el grado de utilización de los recursos: si hay algún recurso saturado, o un mal reparto, etc.
 - Para detectar comportamientos anómalos (ej. posibles intrusiones, fallos del hardware...)
 - Para observar el cumplimiento de las especificaciones y detectar posibles mejoras o evoluciones
- ¿Cómo?
 - Registros de actividad (*logs*)
 - Órdenes específicas
 - Sistema **/proc**

Algunos conceptos

- **Auditoría.** Examen del sistema para verificar que cumple con los requisitos establecidos.
- **Monitorización.** Observación en tiempo real del comportamiento del sistema.
- **Afinamiento (*system tuning*).** Ajuste de parámetros del sistema para mejorar algún aspecto del rendimiento.

Consultar la configuración del sistema

- Hardware
- Núcleo del SO
- Sistema operativo

Consultar configuración del hardware

free	uso de la memoria, swap, cachés...
lscpu	información sobre los procesadores
lsusb	lista de dispositivos USB
lspci	dispositivos conectados al bus PCI
ifconfig	dispositivos de red y su estado

Consultar configuración del núcleo (módulos cargables)

lsmod muestra los módulos instalados

modprobe añade o quita módulos

modinfo muestra información de los módulos

Consultar configuración del SO

- **hostname** nombre del equipo.
- **uname** versión del núcleo.
- **/etc/issue** fichero de texto con la versión del SO (en Linux, la distribución). Es lo que se visualiza antes de abrir sesión en la consola.

Registros de actividad (*logs*)

- Los servicios del SO suelen registrar en ficheros los eventos que les ocurren.
- Muchos registros están en **/var/log** y son ficheros de texto.
- Ejemplos:

/var/log/boot.log	mensajes del arranque del SO
/var/log/dmesg	mensajes del núcleo
/var/log/messages	mensajes de los servicios
/var/log/secure	incidentes de seguridad

Ejemplos de entradas de *logs*

/var/log/secure

```
Nov 13 09:02:25 labsopa sshd[18270]: Failed password for  
invalid user pepe from 212.129.27.164 port 51818 ssh2
```

/var/log/messages

```
Nov 13 09:29:35 labsopa dhcpcd: DHCPREQUEST for  
192.168.200.24 from fc:aa:14:1a:92:84 via eth1
```

/var/log/cron

```
Nov 13 11:41:01 labsopa CROND[20857]: (jomis) CMD  
(/usr/bin/date +)
```

Configuración de los registros

- Demonio **rsyslogd**, se configura editando el fichero **/etc/rsyslogd.conf**
- Páginas del *man*: rsyslog.conf, rsyslogd
- **logrotate**: para controlar el crecimiento de los registros, se pueden ir limpiando periódicamente. logrotate utiliza un *crontab* con ciclos diarios y semanales (se puede cambiar en **/etc/logrotate.conf**).

Registros de acceso al sistema

- Órdenes:
 - last** listado de últimos accesos al sistema
 - lastb** listado de últimos intentos fallidos de acceso
 - lastlog** lista de usuarios y su último acceso
 - ac** estadísticas del tiempo de conexión
- Ficheros de registro:
 - /var/log/wtmp** ¡ojo, este es binario!
 - /var/log/btmp** también es binario
 - /var/log/lastlog**

Sistema de ficheros **/proc**

- *Seudosistema* de ficheros: ofrece información del núcleo del SO bajo la apariencia de ficheros normales.
- Ej. **/proc/meminfo** nos da los datos de ocupación actual de la memoria como un fichero de texto.
- **man proc** nos da el catálogo completo de ficheros disponibles.

Ejemplos de ficheros **/proc**

fichero	contenido
/proc/cpuinfo	Número de procesadores y arquitectura
/proc/devices	Dispositivos reconocidos por el núcleo
/proc/filesystems	Sistemas de ficheros reconocidos por el núcleo
/proc/loadavg	Tiempo de marcha del sistema (<i>uptime</i>), número de usuarios conectados y carga media del sistema (1-5-15 minutos anteriores)
/proc/meminfo	Información de ocupación de la memoria RAM y mem. virtual
/proc/mounts	Sistemas de ficheros montados para el proceso actual
/proc/net/*	Varios ficheros con información sobre los servicios de red
/proc/stat	Estadísticas del núcleo: consumo de CPU, memoria, procesos...
/proc/sys/*	Acceso a variables del núcleo
/proc/version	Versión del núcleo y plataforma (lo usa uname)
/proc/vmstat	Estadísticas de la memoria virtual

Observar procesos con **/proc**

- La carpeta **/proc/NNN** permite ver información detallada del proceso con PID=NNN.
- Algunos ficheros en **/proc/nnn**:

cmdline	Línea de órdenes que ejecuta el proceso (argv)
cwd	Directorio actual de trabajo
environ	Todas las variables <i>shell</i> del proceso
exe	Un enlace simbólico a la ruta del ejecutable
fd/*	Carpeta con una entrada por cada fichero abierto por este proceso
stat, status	Estado del proceso

Monitorización y afinamiento de CPU, memoria y E/S

Monitorizar CPU y procesos

- Órdenes básicas: **ps**, **pstree**
- **top** muestra una vista que se actualiza cada 5 segundos (configurable). Se puede cambiar la vista de forma interactiva.
- **time *orden*** nos devuelve el tiempo real invertido por *orden* y cuánta CPU consumió (tiempo en modo usuario y tiempo en modo sistema).
- **uptime** y **/proc/loadavg** nos dan la carga del sistema (nr. de procesos en colas de CPU).
- **vmstat** da info combinada de CPU y memoria.

time orden

Ejemplo:

```
[root@srv]# time find /home -size +1G
```

...

(salida normal de la orden)


...

```
real 3m13.512s
```



Tiempo real invertido

```
user 0m2.354s
```



Tiempo de CPU consumido
en modo usuario

```
sys 0m17.054s
```



Tiempo de CPU consumido
en modo núcleo

```
[root@srv]#
```

uptime

Ejemplo:

14:22:13 up 5 days, 6:04, 2 users, load average: 0.01, 0.18, 0.13

↑
Hora actual

↑
Tiempo que
lleva activo el
sistema

↑
Usuarios con
sesión abierta

↑
Carga promedio
último minuto

↑
Carga promedio
últimos 5
minutos

↑
Carga promedio
últimos 15
minutos

¿Cómo interpretar la información de **uptime** y **vmstat**?

- Las colas deberían tener de 0 a 3 procesos en espera... un valor superior significa que el sistema está sobrecargado.
- Sobrecarga si vemos que la CPU tiene menos de un 5% de tiempo desocupado, o más de un 35% de tiempo de sistema.

Afinamiento de procesos: **nice**, **at**

- Bajar la prioridad a los procesos muy intensivos en CPU o procesos por lotes:
nice -n *prioridad orden arg1 arg2...*
renice -n *nueva_prioridad -p pid*
 - Prioridad: -20 (máxima) ... +20 (mínima)
 - Ejemplo: `nice -n 15 find / -nouser >>/root/huerfanos &`
- Posponer la ejecución de un proceso “molesto” a horas de baja carga:
at para ejecutarlo en una fecha y hora dadas
batch para ejecutarlo cuando la carga del sistema esté por debajo de un nivel dado
 - Ejemplo: `at -f mi_script.sh 03:00 31.12.2016`
 - **atq** (ver la cola), **atrm** (borrar una tarea de la cola)

Monitorizar la memoria

- free** ocupación de la memoria del sistema
- vmstat** estado de uso de los principales recursos (memoria, CPU, E/S)
- top** vista interactiva y en tiempo real de los procesos y memoria, CPU y E/S

Afinamiento de la memoria

- Objetivo: aprovechar al máximo la RAM e impedir que la memoria virtual se sature o se haga mucho uso de ella.
- En Unix, la memoria virtual se almacena en particiones de tipo *swap*.
- Si los dispositivos *swap* están muy activos (>200-300 páginas por segundo), hay saturación en la memoria del sistema.
- Para crear o activar nuevas áreas de *swap*:
 mkswap crea una nueva área
 swapon/swapoff activa/desactiva un área

Monitorizar sistemas de ficheros

- df** consumo de espacio en un sistema de ficheros completo
- du** consumo de espacio para un directorio o un conjunto de ficheros
- ls** lista de los ficheros abiertos

Monitorizar la E/S

vmstat	también informa sobre la E/S
iostat	estado del subsistema de E/S
iostat	informa de la actividad de E/S
tune2fs	modifica atributos de un sistema de ficheros

Afinamiento de la E/S

- La E/S tiene más limitaciones de velocidad que la CPU y la memoria RAM:
 - Controladores de E/S
 - Los propios periféricos de E/S
- La E/S impacta en la velocidad de ejecución
 - Disco: al leer y escribir en ficheros; en el uso de memoria virtual (*swap*)
 - Red: mensajes, almacenamiento remoto...
- El parámetro clave es la **velocidad de transferencia**

Afinamiento de la E/S

- Monitorizar el área de intercambio, para asegurarse de que el uso de memoria virtual no perjudica al acceso al sistema de ficheros.
- Tamaño de colas de disco inferior a 3.
- Ajustar el tamaño de bloque de datos con el que formateamos nuestros discos:
 - Si nuestro perfil típico son procesos de larga duración y con poca E/S, es mejor formatear nuestros discos con tamaños grandes de bloques de datos (así se reduce el número de transferencias).
 - Si nuestro perfil típico son muchos procesos de corta duración, hay que compartir el ancho de banda de E/S entre todos ellos: tamaños de bloques pequeños.

Administración de Sistemas Operativos

Tema 6. Auditoría y monitorización