Guía desarrollo de Prácticas

ISE

Práctica 3: Monitoring & Profiling

Lección 1: Monitorización del Sistema Operativo

Prof. David Palomar Sáez (dpalomar@ugr.es)

Índice

Objetivo

Adquirir conocimientos prácticos sobre las herramientas y fuentes de información para monitorizar el funcionamiento del servidor. Aplicación práctica a la gestión de Raid.

Monitorización del Kernel con dmesg

dmesg es una herramienta para consultar los mensajes del kernel almacenados en el buffer circular del mismo nombre. Su empleo típico es la consulta del arranque del SO y la depuración de problemas con componentes del kernel como los módulos que actúan como gestores (drivers) de dispositivos físicos.

El alumno debe saber identificar la información generadas por el kernel al conectar un dispositivo USB.

```
dmesg -Hw
```

Referencias:

- Guía sobre el uso de dmesg. https://www.howtogeek.com/449335/how-to-use-the-dmesg-command-on-linux/
- Página de manual de dmesg: http://man7.org/linux/man-pages/man1/dmesg.1.html

Logs de Servicios y Aplicaciones

El directorio /var almacena la información generada como consecuencia del uso del servidor. Esta información varía (var) a lo largo de la vida del sistema.

El directorio /var/log contiene los logs del sistema (seguridad, timers, servicios, ...) comunicados a través de syslog o systemd y los gestionados por los propios servicios (como los vistos en la P2 para Apache Httpd o Mysql).

El alumno debe ser capaz de realizar consultas básiscas de seguridad, identificar los ficheros con la última información de logs y consultar su contenidos. Los comandos a emplear son:

- `who`
- `last`
- `logrotate`
- `grep`

Referencias:

- Filesystem Hierarchy Standard: http://www.pathname.com/fhs/pub/fhs-2.3.html
- Página de Manual de Logrotate: http://man7.org/linux/man-pages/man8/logrotate.8.html
- Página de manual de Who: http://man7.org/linux/man-pages/man1/who.1.html
- Página de Manual de Last: http://man7.org/linux/man-pages/man1/last.1.html
- Descripcion y configuracion de syslog: https://www.linuxjournal.com/article/5476

- Descripcion y configugración de systemd: https://wiki.archlinux.org/index.php/Systemd

Directorio /proc

El directorio `/proc` es un sistema de ficheros virtual (no persistido), empleado por el Kernel de Linux para facilitar la consulta del estado del sistema y la configuración de algunos elementos. Como hemos visto en anteriores prácticas, la interfaz de Sistema de Ficheros permite organizar la información jerárquicamente y proporciona una API de acceso ampliamente difundida, lo que la convierte en una interfaz idónea para muchos componentes de Linux.

El alumno debe ser capaz de consultar la información de proc sobre:

- Procesos en Ejecución
- Uso de Memoria Principal y Virtual
- Características, uso y carga media de la CPU
- Estado del Raid
- Monitorizar el contenido de esta información con el comando `watch`

El subdirectorio `/proc/sys` contiene parámetros del kernel que pueden ser modificados en tiempo de ejecución por el administrador del sistema. Por ejemplo:

```
echo 'ise' > /proc/sys/kernel/hostname
sysctl -w kernetl.hostname=ise2
```

Para hacer permanentes los cambios tras el reinicio, se puede emplear `sysctl` y su archivo de configuración.

El alumno debe ser capaz de modificar de forma permanente un parámetro del kernel de su elección. Sabiendo describir la naturaleza y efecto del cambio.

Referencias:

- Página de manual de watch: http://man7.org/linux/man-pages/man1/watch.1.html
- Documentacion Sysctl: https://wiki.archlinux.org/index.php/sysctl
- Tutorial sobre /proc de RedHat: https://web.mit.edu/rhel-doc/5/RHEL-5-manual/Deployment_Guide-en-US/ch-proc.html
- Sistema de ficheros /proc: https://www.tldp.org/LDP/Linux-Filesystem-Hierarchy/html/proc.html

Tareas programadas con Cron

Crond es el servicio standard en Linux para programar la ejecución de tareas (cron jobs). En algunas distribuciones, como CentOS, está siendo reemplazado por los Timers de Systemd con mayor versatilidad en la definición de los tiempos de ejecución. No obstante, cron sigue siendo la herramienta más empleada y su formato de configuración un referente empleado por multitud de sistemas.

El alumno debe ser capaz de localizar y modificar la configuración de crond para tareas del sistema y tareas personales.

Referencias:

- Documentación de Ubutu sobre Cron: https://help.ubuntu.com/community/CronHowto
- Página de manual de Crontab: http://man7.org/linux/man-pages/man5/crontab.5.html
- Página de manual de Cron: http://man7.org/linux/man-pages/man8/cron.8.html
- Timers de Systemd: https://wiki.archlinux.org/index.php/Systemd/Timers
- OnLine Cron expresions: https://crontab.guru

Monitorización del Estado del Raid

Empleando lo aprendido sobre cron, en el apartado anterior, y la administración de Raid en la práctica 1, el alumno debe ser capaz de configurar un monitor del estado de un dispositivo Raid1.

Para ello, debe realizar las siguientes tareas:

- Configurar un Raid1 como el empleado en la Práctica 1.
- Programar un script capaz de detectar que el Raid se encuentra degradado. Para ello, consultará la información proporcionada por `/proc/mdstat` o el comando `mdstat` y generar un mensaje de estilo "Raid1 KO" y "Raid1 OK"en caso de error.
- Programar la ejecución periódica del script con cron.
- Enviar el resultado del checkeo del Raid1 empleando syslog. Para ello, puede emplear el comando logger.

Para poner de manifiesto el correcto funcionamiento de la monitorización, el alumno debe ser capaz de marcar un disco del raid como fallido, así como añadir un nuevo dispositivo al raid1, empleando la herramienta `mdadm`.

Referencias:

- Marcar como fallido y recuperar un raid: https://bencane.com/2011/07/06/mdadm-manually-fail-a-drive/
- Página de manual de logger: http://man7.org/linux/man-pages/man1/logger.1.html
- Chequeando el estado del Raid: https://raid.wiki.kernel.org/index.php/Detecting,_querying_and_testing
- Monitorización automática del Raid: https://raid.wiki.kernel.org/index.php/Monitoring_your_system