Ficheros de información /var/log

Mensajes de información del sistema. Archivos LOG

- El sistema operativo deja información para el administrador a cerca de el núcleo, los servicios, las aplicaciones y lo que está ocurriendo en el sistema.
- Esta información es muy importante para detectar intentos no autorizados, como se comporta un manejador, seguridad, estadísticas, detección de problemas, etc.
- La información se envía en forma de mensajes a unos archivos conocidos como Archivos de Registro o Archivos Log.

Archivos LOG

- Los archivos de log son ficheros de texto plano y son escritos por el núcleo, por los servicios o por las aplicaciones.
- La mayoría de archivos de log están localizados en el directorio **/var/log**.
- Algunas aplicaciones como por ejemplo httpd y samba poseen un directorio propio en /var/log para sus archivos de log.
- Los archivos de log pueden visualizarse con el comando less o un editor de texto. RedHat tiene su propia herramienta gráfica. Visor de registros del sistema, o el comando redhat-logviewer.

Tipos de archivos de log

- log/messages – mensajes del sistema.
- log/secure - archivo de log para los mensajes de seguridad.
- log/cron - un archivo de log para las tareas cron.
- log/httpd – mensajes del servicio apache.
- log/samba – mensajes del servicio samba.
- log/maillog – mensajes del servicio de correo.
- log/spooler – mensajes de la cola de impresión.

Tipos de archivos de log

- log/boot.log y log/dmesg - información de inicio y apagado. Proporcionan información sobre errores en el hardware en el inicio. También sobre el proceso **isapnp** que configura los dispositivos plug and play.
- /var/run/utmp - lista los usuarios que están actualmente dentro del sistema.
- /var/log/wtmp - registra quienes estuvieron en el sistema y cuando.
- /var/log/lastlog - nos muestra, para cada usuario, cuando fue la última vez que entró en el sistema.
- /var/log/btmp - lista los intentos de ingreso fallidos.

log/messages

- Fichero principal para detectar problemas en el sistema.
- Fichero log donde escribe el núcleo.
- Para visualizar los mensajes del núcleo utilizamos el comando **grep**:

  grep kernel /var/log/messages

- Formato del fichero.

  fecha, hora, máquina, proceso que genera el mensaje, mensaje.

  sep 30 19:20:14 serdis kernel Floppy drive(s): fd0 is 1.44M

logrotate

- Para evitar que los archivos log crezcan indefinidamente con los mensajes, se hace que sean circulares, de forma que la información se mantiene un cierto tiempo (cuatro semanas). xxx, xxx.1, xxx.2, xxx.3, xxx.4.
- El paquete **logrotate** contiene una tarea de cron que hace circular automáticamente los archivos de log.
- Utiliza el archivo de configuración /etc/logrotate.conf y los archivos de configuración en el directorio /etc/logrotate.d

ksymoops

- Programa que dado un mensaje de error, lo analiza, crea un informe y lo almacena en un fichero.

  ksymoops <fichero entrada con el mensaje de error > fichero salida con el informe
- fichero de entrada es un fichero que contiene el mensaje de error extraído de log/messages.

- ksymoop en RedHat, viene en el paquete “Desarrollo del kernel”,
- Hay que compilarlo primero

  ```
  # cd /usr/src/linux/scripts/ksymoops
  # make
  ```
- ksymoops para generar el informe, utiliza el fichero **/boot/System.map** que contiene una tabla de símbolos con las direcciones estáticas, y empareja direcciones de memoria con la información de la tabla.

syslogd

- Existe un demonio llamado syslogd, que utiliza el fichero de configuración /etc/syslog.conf. que mantiene una lista de ficheros log.
- Los mensajes del núcleo los recoge klogd y se pasan a syslogd para que los escriba.