Los ficheros de registro en GNU/Linux

Antonia Estero Botaro y Antonio García Domínguez

Seguridad y Competencias Profesionales
Curso 2009-2010
29 octubre 2009

Los ficheros de registro del sistema son unos de los más importantes que podemos tener en él ya que pueden ayudarnos a detectar problemas de seguridad. Estos ficheros registran la actividad de programas tales como *login*, *ftp*, etc. Normalmente estos mensajes se guardan en el fichero `/var/log/messages` en la mayor parte de los sistemas Linux. El fichero `/etc/syslog.conf` nos indica qué ficheros de registro se están utilizando.

A continuación se muestra un extracto de este fichero:

```
1 # /etc/syslog.conf − Configuration file for syslogd(8)
2
3 mail.∗                        −/var/log/mail
4 mail.info                     −/var/log/mail.info
5 mail.warning                  −/var/log/mail.warn
6 mail.err                       /var/log/mail.err
7 news.crit                     −/var/log/news/news.crit
8 news.err                      −/var/log/news/news.err
9 news.notice                   −/var/log/news/news.notice
```

Este tipo de mensajes es importante porque pueden dejar un rastro a través del cual se puede averiguar si alquien está intentando entrar de forma fraudulenta en el sistema, o incluso evidencias de lo que ha hecho una vez que ha entrado.

1. Rotación de los ficheros de auditoría

Estos ficheros requieren una atención regular puesto que pueden llegar a ser muy grandes, y la información antigua no es tan valiosa como la reciente. La orden *logrotate* ayuda a automatizar el proceso de compresión y archivado de los ficheros de auditoría para que éstos no se hagan excesivamente grandes. Los datos antiguos se pueden guardar en otro medio, como CD's, para que no ocupen espacio en el disco duro. El comportamiento de esta orden se puede controlar mediante su fichero de configuración `/etc/logrotate.conf` y mediante los ficheros individuales incluidos en `/etc/logrotate.d/`. Por ejemplo el

fichero `/etc/logrotate.d/xdm` controla la configuración de los ficheros de registro de *xdm*. A continuación se muestra este fichero:

```
/var/log/cups/*log {
  daily
  missingok
  rotate 7
  sharedscripts
  postrotate
    if [ -e /var/run/cups/cupsd.pid ]; then
      invoke-rc.d --quiet cups force-reload > /dev/null
      sleep 10
    fi
  endscript
  compress
  notifempty
  create 640 root lpadmin
}
```

Una posible configuración de *logrotate* puede ser la siguiente. Ejecutamos *logrotate* diariamente mediante su inclusión en `/etc/cron.daily`. Una vez por semana, *logrotate* copia con otro nombre los ficheros de registro actuales. Se guardan 4 semanas de mensajes, de forma que cuando se guarda un nuevo fichero de mensajes semanal, se borra el más antiguo. La configuración de *logrotate* permite guardar los ficheros comprimidos, enviarlos por correo electrónico a alguien, o rotarlos cuando alcanzan un cierto tamaño.

A continuación podemos ver un fichero `logrotate.conf`:

```
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
#compress

# packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own wtmp, or btmp -- we'll rotate them here
/var/log/wtmp {
```

```
19      missingok
20      monthly
21      create 0664 root utmp
22      rotate 1
23  }
24
25  /var/log/btmp {
26      missingok
27      monthly
28      create 0660 root utmp
29      rotate 1
30  }
31
32  # system-specific logs may be configured here
```

2. Revisión de los ficheros de registro

Los programas que se ejecutan en el sistema Linux están constantemente añadiendo información a sus correspondientes ficheros de registro. Esta es la razón por la que no es demasiado conveniente ver los ficheros completos, aunque sería posible. La forma más fácil de revisar un fichero de registro es buscando lo que nos interese mediante la orden *grep*. También puede ser adecuado ver los mensajes más recientes mediante la orden *tail*. Veamos algunos ejemplos:

```
$ grep "FAILED" /var/log/messages
```

Con esta línea buscamos las líneas de `/var/log/messages` donde aparece la palabra «*FAILED*».

```
$ tail -fn 20 /var/log/messages
```

Esta orden nos mostrará las últimas 20 líneas del fichero `/var/log/messages` y mediante la opción `-f` le indicamos que vaya mostrando las nuevas líneas a medida que éstas se van añadiendo al fichero.

Cuando se trabaja en un entorno gráfico, podemos utilizar el programa *xlogmaster* (incluido en el paquete xlogmaster), que permite ver varios recursos del sistema, incluyendo el fichero de registro. Al ejecutarlo muestra una ventana principal con varios botones que permite elegir la información del sistema que se quiere visualizar.

También existe un paquete denominado *logcheck* que comprueba cada hora los ficheros de registro para ver si existe una entrada sospechosa. Si la hay, éstas son enviadas por correro electrónico a **root** o a cualquier otra cuenta que se elija. Este paquete puede que no esté en muchas distribuciones de Linux pero se puede bajar de `rpmfind.net`. Cuando se instala este paquete, se coloca un fichero de trabajo en `/etc/cron.hourly` para que el programa se ejecute cada hora. El *script* se llama `/usr/bin/logcheck.sh`.