

Búsqueda en ficheros log con tail, grep y compañía

INMERSIÓN

Si nuestro hardware o software están de huelga, o fallan el sistema gráfico o la conexión a Internet, a menudo puede ser de gran ayuda comprobar los ficheros log. Este mes examinaremos herramientas de la línea de comandos que pueden ayudarnos a rastrear en las profundidades de estos ficheros críticos.

POR HEIKE JURZIK

Mensajes del kernel, inicios de sesión de usuarios o desconexiones, procesos de red y muchos otros eventos son registrados meticulosamente por un sistema Linux. El sistema de registro del sistema Linux se conoce con el nombre de *syslogs* (o *syslog-ng*, Syslog New Generation” en SUSE Linux); el logger del sistema es un demonio que se inicia en el momento de arranque del sistema. Todos los ficheros log se almacenan en la carpeta */var/log/* y en sus subdirectorios (Figura 1).

A Vista de Pájaro

Con un par de excepciones, la mayoría de estos ficheros están protegidos de los entrometidos y sólo pueden leerse por el administrador del sistema. Para verlos podemos usar el administrador de ficheros de KDE, Konqueror, por ejemplo, en modo administración de sistemas. Para hacerlo pulsamos Alt + F2, y aparecerá un starter, escribimos *kdesu konqueror* e introducimos a continuación la contraseña root después del prompt.

Como los ficheros log son sólo texto, podremos ver el contenido con cualquier editor de texto. Evidentemente, hacerlo de

este modo resulta bastante tedioso, y encontrar la información que necesitamos puede llevarnos un buen rato.

Las secciones que siguen describen métodos alternativos empleados en la línea de comandos y nos dan algunos trucos para la resolución del problema anterior.

Bien Clasificado

Uno de los ficheros log más importantes, y el primer lugar en el que mirar si algo va mal, es */var/log/messages*. En este fichero la mayoría de las distribuciones escriben mensajes sobre conexiones de red, arranque y parada de servicios, carga de drivers hardware al kernel, autenticación de usuarios y más.

Por otro lado, la mayoría de los sistemas escriben información sobre el sistema de impresión en la carpeta */var/log/cups*. Los ficheros log de esta carpeta pueden contener mensajes de error, acceso a dispositivos configurados, etc. Si la pantalla se queda en blanco, falla el ratón, o la aceleración 3D no está correctamente soportada, necesitaremos comprobar el fichero */var/log/Xorg.O.log*. Los foros y las listas de correo serán útiles si podemos ofrecer referencias

a las secciones adecuadas de cada fichero log.

¿Acceso Permitido?

Si alguien intenta escalar sus privilegios a nivel de administrador introduciendo *su* en una ventana terminal o arrancando una herramienta de configuración de una distribución específica, la información del intento se escribirá en */var/log/messages* (o */var/log/auth* en algunos sistemas).

Además de la fecha y hora, la entrada nos dice qué usuario inició el comando y si tuvo éxito. Mientras SUSE Linux sólo nos da detalles de los éxitos o fallos del intento, Mandriva Linux también nos dice el programa con el cual se intentó conseguir privilegios root. El Listado 1 muestra algunos mensajes importantes de los sistemas SUSE y Mandriva Linux respectivamente.

Si nuestro ordenador tiene asignada una dirección IP a través de un servidor DHCP, resulta muy fácil identificar la actividad del cliente DHCP. Líneas como las que siguen

```
Mar 27 18:18:45 localhost 2
dhclient: DHCPREQUEST on eth0 2
to 255.255.255 port 67 2
```



Figura 1: Los ficheros log están localizados en "/var/log/".

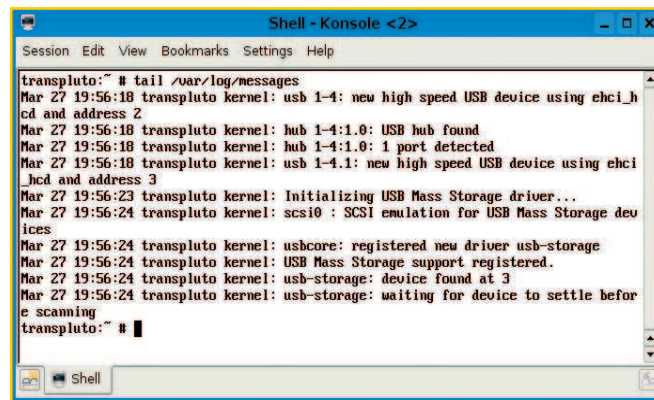


Figura 2: "/var/log/messages" nos presenta eventos tales como la conexión o desconexión de medios (un stick USB en este caso).

```
Mar 27 18:18:45 localhost dhclient: DHCPACK from 192.168.2.15
Mar 27 18:18:46 localhost dhclient: bound to 192.168.2.237
- - renewal in 235 seconds.
```

muestran cómo nuestro ordenador pide direcciones IP y detalles sobre su período de validez.

Si usamos conexión a Internet directa vía módem, ISDN, o DSL, /var/log/messages también nos dirá si nuestra conexión está funcionando, porque el programa por red telefónica pppd (módem y DSL) o ipppd (ISDN) escribe su mensaje de estado aquí. Por ejemplo:

```
Mar 25 22:14:19 asteroid pppd[1432]: local IP address 195.14.222.177
```

¿Toda la Verdad?

Si nos preocupa un evento reciente, es lógico comprobar las últimas líneas de un

fichero log. En vez de abrir el fichero completo en nuestro editor de texto y expandirlo hasta el final, podemos usar el paginador tail en la línea de comandos.

Abrimos una línea de comandos, por ejemplo, escribiendo konsole en la ventana de inicio rápido que hicimos aparecer pulsando Alt + F2, y nos convertimos en root escribiendo su e introduciendo la contraseña del administrador. Ahora llamamos a tail, pasándole el nombre del fichero log, para mostrar las 10 líneas últimas del fichero (Figura 2). Si necesitamos más de 10 líneas, podemos configurar la opción -n para especificar un número diferente:

```
tail -n 20 /var/log/messages
```

Si vemos un mensaje de error como

```
Mar 27 15:43:21 transpluto kernel: usb.c: USB device 10 (vend/prodx82d/0x200) is not claimed by any active driver.
```

```
Mar 27 15:43:25 transpluto /etc/hotplug/usb.agent: ... no modules for USB product 82d/200/100
```

podemos inferir que el dispositivo no ha sido detectado y no será soportado.

El programa tail incluye otra práctica funcionalidad: Podemos configurar la opción -f para cambiar a modo acceso seguimiento, donde tail actualizará la presentación del fichero siempre que cambie su contenido.

Si deseamos vigilar /var/log/messages, escribimos:

```
tail -f /var/log/messages
```

A partir de este momento podemos monitorizar las actividades de entrada. Pulsando Ctrl + C abandonamos la visualización.

"tail" y "grep"

Finalmente, para filtrar las salidas de tail en busca de palabras clave, podemos usarlo en combinación con otra herramienta de la línea de comandos y descubrir mensajes críticos mucho más rápidamente. La herramienta grep busca coincidencias en cadenas.

Si deseamos buscar en las últimas 100 líneas del fichero log /var/log/messages las letras "USB" o "usb", podemos hacerlo con un simple comando:

```
tail -n 100 /var/log/messages | grep -i usb
```

Este comando dirige la salida ("|") desde tail al comando grep. El parámetro -i (de ignorar) desactiva la discriminación entre mayúsculas y minúsculas (por ejemplo, no distingue entre "usb" y "USB" o incluso "usB").

Listado 1: Privilegios Root Denegados

```
01 # Intento frustrado del usuario suse93 de obtener privilegios de root
02 # en SUSE Linux System
03 Mar 27 14:30:51 transpluto su: FAILED SU (to root) suse93 on /dev/pts/6
04
05 # Arranque de centro de control Mandriva con subsiguiente entrada
06 # incorrecta de la contraseña de root
07 Mar 27 18:11:41 local host drakconf.real[4395]: ### Program is starting ###
08 Mar 27 18:11:41 localhost su(pam_unix)[4404]: authentication failure: logname= uid=500 euid=0 tty= ruser=mandriva2006 rhost= user=root
```