

Trucos: Logrotate

# ROTANDO LOS REGISTROS

Cada sistema Linux produce gran cantidad de datos en los registros.

Para impedir que el disco duro se llene existe una aplicación que ayuda a rotar los ficheros de registros y se deshace de los datos obsoletos. **POR MARC ANDRÉ SELIG**

Tienes que ser un tipo de persona muy especial si disfrutas analizando los ficheros de registros. Pero debe admitirse que los ficheros de registros de `/var/log` proporcionan a los administradores el tipo de información que necesitan para descubrir el origen de los errores misteriosos del sistema. También proporcionan información si los servicios en el sistema están funcionando.

Si tiene cualquier problema instalando un servicio o ejecutando un script, los registros pueden indicarle lo que va mal. Los administradores paranoicos (y deberían serlo todos) comprueban sus sistemas en busca de accesos no autorizados y bloquean cualquier traza que encuentran.

Los registros de información también pueden usarse para controlar el comportamiento del equipo. Por ejemplo, un servidor SMTP podría ver una dirección IP como autorizada para enviar correo si el

fichero de registro tiene una entrada de login correcta para el buzón. O un cortafuegos podría desplegar un filtro de paquetes para bloquear automáticamente una dirección IP siguiendo un ataque obvio.

Si no se leen los ficheros de registros, aún se les puede echar un vistazo. Éstos consumen más y más espacio en el disco duro o en la partición `/var`. El consumo gradual de espacio de disco, tarde o temprano hará que el equipo caiga.

El manejo de los ficheros de registro (evaluación, archivado, eliminación) es una tarea administrativa tradicional. Pero ahora que Linux ha empezado a conquistar los escritorios, es absurdo esperar que los usuarios manejen la administración de los archivos de registro. Hace años que se presentaron algunas herramientas totalmente automatizadas para ayudar con la tarea de manejar los ficheros de registros.

## ¡No Borre, Rote!

Un sistema Linux no borra los ficheros de registros, los rota. Primero renombra un fichero como `XXX.log` a `XXX.log.0` (o algo parecido). Este paso es importante, ya que el programa de limpieza automático no tiene forma de conocer si el proceso está actualmente accediendo al fichero de registro. Si un proceso tiene abierto el fichero de registro, posee un manejador de ficheros exactamente para ese fichero, y escribirá al archivo independientemente de si otro proceso lo ha renombrado o lo ha suprimido.

Tras renombrar el fichero, el protocolo de limpieza necesita volver a crear los ficheros de registros nuevos (en blanco) e indicarle al proceso correspondiente que el

fichero de registro se ha cambiado. El proceso de escritura necesita cerrar cualquier fichero de registro que se esté usando y reabrir estos ficheros, así se reciben las versiones actualizadas (en blanco) que pueden actualizarlos.

Cuando la herramienta de gestión del fichero de registro central necesita encontrar qué procesos escribir en qué ficheros de registro. El hecho de que muchos servicios utilicen `syslog` hace que esto sea más fácil de manejar, pero aún hay paquetes (como Apache) que insisten en utilizar sus propios ficheros de registro por rendimiento u otras razones.

## Configuración Modular

Para establecer este mecanismo en un sistema Linux libremente configurable y extensible, muchos desarrolladores utilizan el paquete Logrotate. Éste utiliza una configuración modular como muchos otros

### Listado 1: Fichero Ejemplo de logrotate.conf

```
01 weekly
02 rotate 4
03 create
04 compress
05 delaycompress
06
07 /var/log/wtmp {
08 missingok
09 monthly
10 create 0664 root utmp
11 rotate 1
12 }
13
14 include /etc/logrotate.d
```

### Listado 2: /etc/logrotate.d/apache2

```
01 /var/log/apache2/*.log {
02 missingok
03 rotate 52
04 notifempty
05 create 640 root adm
06 sharedscripts
07 postrotate
08 if [ -f /var/run/apache2.pid
09 ]; then
10 /etc/init.d/apache2 restart
11 >/dev/null
12 fi
13 }
14 }
```

paquetes centralizados. Las variables del núcleo se establecen mediante un fichero de configuración central. El fichero realiza una anotación de la frecuencia en la que Logrotate debe rotar el fichero de registro, qué tamaño deben tener los registros antiguos, si se comprimen estos ficheros y así continuamente. El fichero de configuración central se llama `/etc/logrotate.conf`.

Además, cada paquete software puede añadir una entrada al fichero de configuración de Logrotate durante la instalación. Por supuesto, no se debería escribir en el fichero de configuración central. Esto podría conducir a inconsistencias; en vez de esto, Logrotate utiliza un directorio de configuración denominado `/etc/logrotate.d`.

Los paquetes pueden almacenar sus propios mini ficheros de configuración Logrotate bajo su nombre de paquete. Estos ficheros indican lo que hay hacer con el fichero de registro rotado. La entrada de configuración para un servidor proxy puede ser, por ejemplo, `/etc/logrotate.d/squid`.

## Un Ejemplo

El Listado 1 proporciona un ejemplo de un `/etc/logrotate.conf` mínimo. Basándose en esta configuración, Logrotate rotaría los ficheros de registros semanalmente y proporcionaría un total de cuatro versiones previas. Tras cada rotación, la herramienta creará un nuevo fichero de registro y comprimirá las versiones previas semanales.

El Listado 1 especifica el fichero de registro de Logrotate a manejar, `/var/log/wtmp`. La aplicación tan sólo crea este fichero una vez al mes, manejando los permisos para el fichero de `root` y el grupo `utmp`. La palabra reservada `rotate 1` en la línea 11 le indica a Logrotate que guarde tan sólo la versión anterior.

`logrotate.conf` no especifica como manejar los otros ficheros; en cambio estos se manejan por trocitos de configuración del `/etc/logrotate.d`, que tienen la directiva habilitada en la línea 14. Ignora cualquier fichero creado mediante editores, ficheros de versiones de sistemas de control, trozos dejados por gestores de paquetes (por ejemplo, `*.rpmsave` o `*.dpkg-old`) y ficheros con extensión `.disabled`.

## Tratamiento Especial para Apache

Los ficheros `/etc/logrotate.d` incluyen el fichero `apache2`, con un ejemplo para Apache (Listado 2) que contiene opciones especiales para rotar los registros de Apache. Este listado comienza con la ruta a

los ficheros de registro. Apache viene configurado para guardar los ficheros de registro bajo `/var/log/apache2`.

La configuración por defecto del Listado 1, se aplica a todos los ficheros en `/var/log/apache2`; primero: Logrotate rota los ficheros semanalmente, comprime los ficheros de la semana y crea un fichero nuevo por cada fichero que rota. La línea 5 del Listado 2 asigna privilegios de acceso específicos a los registros nuevos y vacíos para impedir que los usuarios normales los visualicen.

Una suposición que hace el ejemplo es que los registros del servidor web son más importantes para las operaciones del sistema y para la facturación. Se necesita que el sistema mantenga los registros de un año completo, creando 52 generaciones, a una tasa de una generación por semana. Si Apache falla al ejecutarse por alguna razón desconocida, lo que conduciría a un registro perdido, el programa no lo rotará como se estipula con la palabra reservada `notifempty`.

El Listado 2 también contiene instrucciones sobre cómo hacer que Apache conozca el momento en el que se van a rotar los ficheros. El mensaje se envía después de cada evento, como se indica con la palabra reservada `postrotate` (la palabra reservada para un mensaje anterior a la rotación es `prerotate`). Dicha palabra va seguida de unas cuantas líneas del script, que se cierra con la palabra reservada `endscript`. Las líneas de la 8 a la 10 dicen: si Apache se está ejecutando (es decir, si el fichero PID existe) la correspondencia en el script Init se encargará de relanzarlo.

La palabra reservada `sharedscript` de la línea 6 le indica a Logrotate que llame a este script de información una única vez, incluso cuando se rotan múltiples ficheros de registro. Ejecuta una rotación una vez que se ha completado para todos los ficheros de registro.

## Sofisticado

La configuración en los Listados 1 y 3 proporciona ejemplos de cómo configurar los servicios estándar en las distribuciones más comunes de Linux. Pero `logrotate` dispone de más trucos: el Listado 3 configura un filtro de paquetes, por ejemplo. Esta configuración supone que los registros del filtro de paquetes se almacenarán en `ipfilter-bulk.log`. Los ficheros podrían ser enormes en un servidor típico y su tamaño impediría una evaluación manual. Un script (que no se muestra aquí por razones de espacio) analizará el fichero en busca de informa-

ción relevante y crítica, escribiéndola en el fichero `ipfilter-high.log`.

El Listado 3 tiene que tratar estos dos ficheros de forma bastante diferente. Rota `ipfilter-bulk.log` si el fichero llega a un tamaño de 20 Mbytes, pero normalmente no más de una vez al día. Logrotate comprime los ficheros de registros antiguos usando `bzip2`. El siguiente paso es notificar al servicio de los cambios del fichero; para ello se usa la directiva `postrotate` en el script Init apropiado, como en el ejemplo anterior de Apache.

`ipfilter-high.log` requiere un tipo de tratamiento diferente. Como podría contener información crítica en el tiempo, `logrotate` rota este fichero una vez cada día y, además, envía un correo al administrador. Le proporciona bastantes avisos y tiempo suficiente para hacerse cargo de los registros. `logrotate` normalmente atiende a los ficheros de registros más antiguos, pero la directiva `mailfirst` le indica que envíe el fichero actual tan pronto como termine la rotación.

Los datos críticos simplemente no se descartan tras unas cuantas semanas, sino que se mantienen por razones forenses, en nuestro caso, 730 días, o dos años. Para impedir que los ficheros de registros antiguos se acumulen en el directorio `/var/log`, `logrotate` los mueve a un directorio separado en `/var/log/ipfilter-old.d`. ■

### Listado 3: Dos Registros Distintos en un Filtrado de Paquetes

```
01 /var/log/ipfilter-bulk.log {
02 size 20M
03 rotate 10
04 compress
05 compresscmd bzip2
06 compressext bz2
07 postrotate
08 /etc/init.d/syslogd reload
   >/dev/null
09 endscript
10 }
11
12 /var/log/ipfilter-high.log {
13 daily
14 rotate 730
15 olddir /var/log/ipfilter-old.d
16 nocompress
17 mail
   <I>ich<I>@<I>meine.domain.de<I
   >
18 mailfirst
19 }
```