

El Día a Día del Administrador de Sistemas

LA MÁQUINA LECHERA 2.0

El uso de SQL para obtener los datos del registro del sistema de una base de datos se conoce universalmente, pero es una solución bastante enrevesada. phpLogCon, con su interfaz web, brinda a los administradores una opción más sencilla. **POR CHARLY KÜHNAST**

En el número del mes pasado hablé de Rsyslog, un sustituto de los servicios de syslog [1]. En vez de hacer referencia a los ficheros de registro estándar en `/var/log`, Rsyslog funciona con una o varias bases de datos en las que registra los resultados locales o los datos suministrados por los servidores remotos. Siempre utilizo una base de datos, Maillog, para el correo y una segunda base de datos, syslog, para el resto de los mensajes.

Un par de scripts extraen las estadísticas del rendimiento del fitro antispam de Maillog DB.

Consultas Rápidas

Todo esto funciona perfectamente, pero no es de utilidad si se tiene que consultar alguna información de la base de datos rápidamente, como por ejemplo, si alguien pierde un correo.

O quizás sólo desee conocer qué filtro antispam está bloqueando la mayoría de

los correos de mi dirección. (A propósito, es una copia de seguridad MX, que los spammers parecen preferir como regla general). En estos casos utilizo phpLogCon [2], una interfaz web para realizar consultas rápidas. Si está sentado delante de la máquina de alguien y sólo tiene acceso al navegador web, el programa le suministrará un acceso fácil a la mayoría de las consultas populares de la base de datos.

PhpLogCon proporciona una instalación web simple, y está preparada para funcionar con múltiples ficheros de registro y con múltiples autorizaciones de usuarios.

Interfaz Web

La interfaz web podría estar más ordenada, pero al menos no se encuentra totalmente sobrecargada (Figura 2).

Se puede establecer el número de entradas por página entre 5 y 2000, y ordenar los resultados de forma ascendente y descendente por fecha, utilidad, urgencia y por nombre de equipo.

Además, phpLogCon resaltaré las ocurrencias de un término específico en el conjunto de los resultados.

Limitando la Búsqueda

Como tengo que procesar ficheros de registro bastante grandes, resulta particularmente útil la selección del período de tiempo en el que desee realizar la búsqueda. Por ejemplo, si ya sé que el error sucedió en algún momento entre las 14:00 y las 16:00, no tendría sentido escudriñar la base de datos de registro entera. Puedo establecer la ventana de búsqueda en *Manual event date selection*.

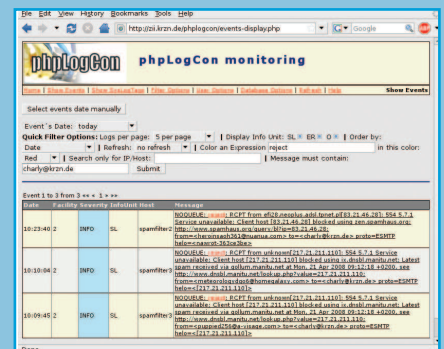


Figura 1: phpLogCon arroja la toalla cuando se enfrenta a consultas complejas, teniendo que volverme a la línea de comandos.

Opciones de Filtrado

Además podemos encontrar opciones de filtrado (*Filter options*), las cuales permiten establecer un nivel de urgencia (que oscila entre 0 para Emergencia y 7 para Debug). El autor de phpLogCon también ofrece de forma amable actualizaciones automáticas y un FAQ legible.

Lo que desafortunadamente no ofrece la interfaz web phpLogCon son consultas con múltiples cadenas de búsquedas conectadas con AND y OR. Por ahora habrá que volver a la línea de comandos para poder realizar consultas de esta clase (véase la Figura 1), aunque hay que destacar que la versión 2.0 está en desarrollo.

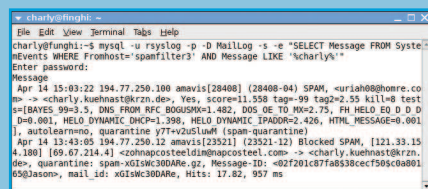


Figura 2: La interfaz web de phpLogCon puede que no ganara ningún concurso de belleza, pero le proporciona a los administradores resultados de búsqueda de manera rápida.

SYSADMIN
 Indicación de Nombres68
 Soportando servidores virtuales con Server Name Indication.

RECURSOS

- [1] El día a día del administrador de sistemas: "Rsyslog" por Charly Kühnast, N° 42 Linux Magazine edición en castellano.
- [2] phpLogCon: <http://www.phplogcon.org>