

El Día a Día del Administrador de Sistemas: Sarg

LAS HERRAMIENTAS DE PEDRO

Un servidor proxy ocupado es algo que ningún administrador debería permitir. El analizador de los ficheros de registro del Squid, denominado Sarg por su autor, le ayuda a mantener su servidor Squid actualizado.

POR CHARLY KÜHNAST

Lo pasé bien navegando en sitios como Sourceforge o Freshmeat buscando paquetes de software interesantes. Desde luego, los paquetes con nombres sugerentes me llaman más la atención. No pude evitar fijarme en la herramienta del desarrollador de software brasileño, Pedro Orso. Estoy seguro que Pedro no era consciente de las connotaciones de su Generador de Informes de Análisis de Squid (Squid Analysis Report Generator, Sarg) para los usuarios alemanes de Linux. (Sarg en alemán significa ataúd). Pero esto no me desanimó en lo más mínimo, y menos mal, porque Sarg es exactamente la clase de herramienta que me gusta: eficiente y rápida. Realiza de manera muy eficiente la tarea para la que fue ideado: crear informes basados en los ficheros de registro de Squid.

SYSADMIN

El Taller del Administrador: NTP.....66

El Network Time Protocol (NTP) proporciona la hora exacta a través de la red.

Programación Segura..... 69

Asegure su servidor aprendiendo a pensar como un atacante.

El Taller del Administrador: NTP.....66

El Network Time Protocol (NTP) proporciona la hora exacta a través de la red.

Programación Segura..... 69

Asegure su servidor aprendiendo a pensar como un atacante.

El código fuente de Sarg y los paquetes binarios para varias distribuciones Linux, *BSD, MacOS e incluso OS/2 están disponibles en [1]. Sarg toma los ficheros de registro de Squid y utiliza los datos para generar un resumen estadístico muy útil, como el mostrado en la Figura 1. Pero al contrario que la utilidad Calamaris de Squid, Sarg genera una estadística específica de usuario.

Puede pasar los parámetros más importantes para Sarg en la línea de comandos; el fichero de configuración *sarg.conf*, (Sarg trae un ejemplo), le proporciona más opciones, como modificar el diseño de la salida. Obviamente Pedro piensa en lo que la mayoría de los usuarios esperan de la herramienta Sarg y ha proporcionado los ajustes por defecto necesarios. Esto significa que para generar un informe, simplemente se especifica el archivo de origen, es decir, el fichero *access.log* de Squid y el directorio objetivo donde le gustaría que Sarg pusiera los resultados.

```
sarg -l ➤
/var/log/squid/access.log ➤
-o /www/sarg/
```

Sarg y DNS

Para mayor conveniencia, Sarg tiene la opción de la línea de comandos *-n* que permite al DNS resolver las direcciones. Esto está bien para un Squid pequeño que cuente sólo con unos cuantos usuarios, pero si tiene una gran caché que procesa miles de millones de respuestas al día, no es conveniente dejar que Sarg lleve a cabo la resolución

de nombres, ya que el análisis le llevará todo el día. Aparte de esto, la mayoría de los administradores de DNS no estarían demasiado contentos con el estrés involuntario al que serían sometidos sus servidores.

Otra característica útil es el poder restringir el análisis a un período de tiempo específico, para ello utilice la opción *-d TT/MM/YYYY-TT/MM/YYYY*. El tiempo ha sido siempre un problema para Squid, que lo almacena en segundos a partir de la era en su archivo *access.log*, con una resolución de una milésima de segundo. Aunque puede evitarse que Squid haga esto indicándole que utilice el formato del fichero de registros común, si bien se perderá alguna información en el proceso. Sarg puede ser de gran ayuda aquí. Introduciendo:

```
sarg -convert ➤
/var/log/squid/access.log
```

se mostrará el fichero de registro en STDOUT y lo proporciona en un formato legible con fecha.

Un valor como *1126705707.537* se transforma en *09/14/2005 14:48:27*. La pérdida del milisegundo no es en absoluto preocupante.

Gracias por la aplicación, Pedro, hacía tiempo que no me divertía tanto, pero debería replantearse las siglas en beneficio de todos aquellos hackers alemanes de Linux. ■

RECURSOS

[1] Sarg: <http://sarg.sourceforge.net/sarg.php>