

SARG.GenerandoReportesde Squid.

Original: Hugo Cisneros. hugo en devim punto com punto br

Traducción Castellano: Alberto Permuy alberto punto permuy en gmail punto com

Sarg(Squid Analysis Report Generator) es una muy buena herramienta desarrollada por un brasileño llamado Pedro Orso, que permite saber dónde han estado navegando los usuarios en Internet, a través del análisis del fichero de log "access.log" del famoso **proxy Squid**. El poder de esta herramienta es increíble, pudiendo saber qué usuarios accedieron a qué sitios, a qué horas, cuantos bytes han sido descargados, relación de sitios denegados, errores de autenticación...entre otros. La flexibilidad que puede obtener con Sarg es muy alta, principalmente para las empresas que quieren tener un control de accesos y ancho de banda de acceso a Internet.

Vamos a instalar y a configurar SARG para que genere los reportes diarios de los accesos del Squid. Para ello necesitamos Squid ya configurado y funcionando (no se explicará en este manual), que genere los logs de acceso en el fichero access.log. Si usted no sabe qué fichero es que almacena los logs de Squid, compruebe la siguiente línea en su fichero squid.conf, si no existe, añada a este fichero:

cache_access_log /var/log/squid/access.log

Generalmente el fichero de configuración de Squid está en "/etc/squid/squid.conf". La línea mencionada en el apartado anterior especifica que el fichero de log deberá estar en "/var/log/squid/access.log". Si ha tenido que añadir esta línea a su fichero de configuración de Squid, reinicie Squid con "reload" para que los cambios sean efectivos.

Ahora vamos a lo que interesa. Necesita descargar SARG de:

<http://sarg.sourceforge.net/sarg.php>

En este tutorial, he pasteado el código de la versión 2.1.1 (en el original de Hugo era el 1.2.2). Podrá comprobar que existen cantidad de paquetes precompilados para distribuciones tales como Debian GNU/Linux, OpenSuSE, Fedora, y, si utiliza alguna de estas distribuciones, podrá descargarla con su gestor de paquetes. Compilemos el programa:

tar zxvfp sarg-2.1.1.tar.gz

cd sarg-2.1.1

./configure --enable-sysconfdir

make

make install

Ahora que el programa ha sido compilado he instalado, necesitamos configurarlo para que llegue a funcionar. Hemos seleccionado en la compilación el directorio "/etc/sarg" para almacenar los ficheros de configuración. Nos situamos en dicho directorio.

pwd

/etc/sarg

ls

exclude_codes languages/ sarg.conf

NOTA: Pueden variar los ficheros en función de la versión que haya compilado.

Observe los ficheros que se crean. Como nuestra instalación va a ser un poco más compleja, tendremos que crear algún fichero más, y organizar los ya existentes:

```
# mv sarg.conf default.conf
# touch exclude.hosts
# touch exclude.strings
# touch exclude.users
# ls
default.conf  exclude.hosts  exclude.users
exclude_codes exclude.strings languages/
```

Breve explicación de los ficheros que hemos creado.

- `exclude.host`. Aquí, cada línea tendrá un dominio/URL que NO será mostrado en el informe. Es útil cuando para insertar direcciones, por ejemplo, direcciones de descargas de la Intranet que pasan por el Squid, pero que no consumen ancho de banda de Internet.
- `exclude.strings`. Si alguna línea del fichero de log contiene alguna cadena de este fichero (una cadena por línea), esta línea del log, será ignorada por el informe. Con esto podrá filtrar lo que desee en el informe.
- `exclude.users`. Los usuarios que figuren en este fichero no estarán incluidos en el reporte.

Ahora vamos a crear un fichero de configuración para SARG. Como se dijo anteriormente, este fichero de configuración será para un reporte diario. Colocaremos esta configuración en el fichero `"/etc/sarg/sarg.dia.conf"`. A continuación se muestra un fichero de configuración comentado, para su posterior análisis

```
# Idioma utilizado, he colocado el inglés aquí, pero estará todo en portugués
#
language English
# Fichero log de Squid.
#
access_log /var/log/squid/access.log
# Título de la página HTML
title "Reporte Diario del Proxy"
#
# --- Visual ---
#
# Aquí tenemos algunas variables que puede cambiar
# para cambiar el aspecto de los informes
font_face Arial
header_color darkblue
header_bgcolor blanchedalmond
header_font_size -1
background_color white
```

```
text_color black
text_bgcolor beige
title_color green
# --- Fin parte Visual
#
#
# Directorio Temporal
temporary_dir /tmp
#
#
# Directorio dónde se generarán los reportes
# Generalmente deben estar dentro del raiz de su webserver
output_dir /var/www/html/squid-report/dia
#
#
# Qué criterio de orden para la sección TOPUSER : USER/CONNECT/BYTES/TIME
# Con esto se organizará el reporte de la seccion TOPUSER
topuser_sort_field BYTES reverse
#
#
# Criterio de orden para la seccion USER: SITE/CONNECT/BYTES/TIME
# Con esto se organizará la sección de usuarios de mismo modos que el item anterior
user_sort_field BYTES reverse
#
#
# Fichero de los usuario que NO aparecerán en el reporte
exclude_users /etc/sarg/exclude.users
#
#
# Fichero que contiene los hosts que NO aparecerán en el reporte
exclude_hosts /etc/sarg/exclude.hosts
#
#
# Formato de fecha (e=dd/mm/yy, u=mm/dd/yy, w=yy/ww)
date_format e

# Limite de logs hasta que los antiguos sean eliminados. Cuando existan mas
# de N reporte, el más antiguo es automáticamente eliminado.
# Así(lastlg 0) indicamos que no se debe eliminar nunca.
lastlog 0
```

El fichero de configuración en sí ya explica las configuraciones que se pueden alterar. Aún así, existen más opciones disponibles en el propio SARG. Puede verlas en el fichero de configuración que hemos dejado en **“/etc/sarg/default.conf”**.

En relación al idioma utilizado, he encontrado un error. Pero he encontrado una solución rápida para ello. Lo que sucede es que aún cambiando la variable language, SARG sigue generando los reportes en Inglés. Si le sucede esto, haga lo siguiente:

```
# cd /etc/sarg/languages  
# mv English English.old  
# ln -s Portuguese English
```

NOTA DEL TRADUCTOR: No he observado dicho error en Debian Sarge 3.1 r2 Kernel 2.6.8 con el paquete .deb sarg-2.0.5 ni con el paquete sarg-2.1.1.tar.gz

Lo que he hecho aquí es hacer un link simbólico del Inglés al Portugués, para que el programa pegue el contenido del archivo Portugués en el Inglés original. Nótese que se ha hecho un backup del fichero Inglés, recuerde: realice siempre backups”

Parece que tenemos el idioma configurado. Supongamos que hoy es día 05/02/2003 y que quiere generar un reporte con los usuarios que han pasado a través del proxy.

```
/usr/sbin/sarg -f /etc/sarg/sarg-dia.conf -d 05/02/2003-05/02/2003
```

Dependiendo de la cantidad de accesos a su proxy, y del tamaño del fichero de log, el proceso se puede demorar. Cuando termine esta operación, acceda al directorio que ha configurado en la línea:

```
output_dir /var/www/html/squid-report/dia
```

por medio de su navegador favorito. Ahora debemos configurar crontab para que se genere automáticamente el reporte todos los días a las 01:01 de la madrugada.

Nota: Varias distribuciones ya tienen un contrab diario configurado. Es decir, que todos los ficheros ejecutables que se encuentren dentro del directorio “/etc/cron.daily” serán ejecutados a determinada hora, generalmente a las 04:00 de la madrugada.

Si en su distribución ya existiese ese directorio, cree el fichero **“/etc/cron.daily/sarg-dia”**. En caso de no tenerlo, cree el fichero **“/usr/local/bin/sarg-dia”**, con el siguiente contenido en uno de esos dos archivos:

```
#!/bin/bash
```

```
HOY=$(date --date "1 day ago" +%d/%m/%Y)
```

```
/usr/sbin/sarg -f /etc/sarg/sarg-dia.conf -d $HOY-$HOY  
exit 0
```

Si en su caso he creado el fichero “/usr/local/bin/sarg-dai”, entonces tendrá que configurar el crontab para que se ejecute esta tarea a las 01:01 de la madrugada. Añadala siguiente línea al fichero “/etc/crontab”

```
01 1 * * * root /usr/local/bin/sarg-dia
```

Y no olvide dar permisos de ejecución al fichero:

```
# chmod +x /etc/cron.daily/sarg-dia
```

O también

```
chmod 700 /usr/local/bin/sarg-dia
```

NOTA DEL TRADUCTOR: He observado que en OpenSuSE 10.0 es necesario reiniciar el demonio cron para que guardelos cambios. En Debian no es necesario, pero recomiendo hacerlo: /etc/init.d/crontab restart

Aviso: Los reportes genera muchas páginas, e dependiendo del informe, puede llevar a ocupar un espacio considerable en el disco duro. Sea consciente de esto, Véase como prueba de esto que en el ejemplo propuesto de 03 de Febrero, el fichero access.log ocupaba 103 MB.

Nota del Traductor: Recomiendo encarecidamente utilizar una partición /var separada de la partición /.

Original: Hugo Cisneros. hugo en devim punto com punto br

Traducción Castellano: Alberto Permuy alberto punto permuy en gmail punto com