

Xerando relatorios do Squid co SARG.

Orixinal: hugo en devim punto com punto br

Traducción: Evaristo Deus : evaristo punto deus en gmail punto com

O SARG (Squid Analysis Report Generator) é unha ferramenta moi boa desenvolvida polo brasileiro Pedro Orso, que permítenos saber onde foron os usuarios en Internet , a través da análise do ficheiro de log “access.log” do famoso proxy squid. O poder desta ferramenta é incríbel, pódese informarnos dos sitios ós que os usuarios acceden, os usuarios que máis acceden, relatorio de lugares negados, falla de autenticación, entre outros. A xestión que obtense é moi boa, principalmente para as empresas que queren economizar o uso da internet. Imos a instalar e configurar o SARG para xerar relatorios diarios dos accesos do Squid. Para eso precisamos dun Squid xa configurado e funcionando (que non se explica neste manual), que xenere os logs de acceso no ficheiro access.log. Si descoñécese o ficheiro que almacena os logs no Squid, é necesario comprobar a existencia no ficheiro de configuración squid.conf da seguinte liña de código. Se non engadaa:
cache_acces_log /var/log/squid/access.log

Xeralmente o ficheiro de configuración do Squid está en “/etc/squid/squid.conf”. A liña de enriba especifica que o ficheiro de log deberá estar en “/var/log/squid/access.log”. Se é necesario adicionar esa liña no Squid, reinicieo (ou de un “reload” ó servizo) para que os cambios sexan efectivos.

Agora imos ó que interesa. É necesario baixar o SARG do enderezo:

- SARG - <http://web.onda.com.br/orso/>

Neste tutorial, peguei o código fonte da versión 2.1.1 (no texto orixinal de Hugo a versión é a 1.2.2). Pódese comprobar a existencia de paquetes precompilados para distribucións como Debian, GNU/Linux, OpenSuse, Fedora, e nestes casos pódense compilar e instalar co xestor de paquetes. Como temos o código fonte, compilemos o programa:

```
tar zxvfp sarg-2.1.1.tar.gz
```

```
cd sarg-2.1.1
```

```
./configure --enable-sysconffdir
```

```
make
```

```
make install.
```

Esta operación débese executar como root, aínda que soamente é necesario no “make install”, xa que instala o SARG en /usr/bin e no directorio de configuración “/etc/sarg”. Si desexamos coñecer máis opcións do comando configure teclearemos:

```
./configure --help
```

Agora que o programa foi compilado e instalado, é necesario configuralo para conquistar o seu funcionamento. Na configuración escollimos o directorio /etc/sarg para almacenar os ficheiros de configuración, polo que nos situamos nel.

```
pwd
```

```
/etc/sarg
```

```
ls
```

```
exclude_codes languages/sarg.conf
```

Nota: Poden variar os ficheiros en función da versión que compilamos.

Observaremos os ficheiros tipo creados. A nosa instalación vai ser un pouco máis complexa, e teremos que crear algúns arquivos máis e organizar o xa 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/
```

Unha breve explicación dos arquivos que creamos:

- `exclude.hosts` – Eiquí cada liña terá un dominio/URL que non será mostrado no relatorio. Nos é útil insertar, por exemplo, direccións de descargas da Intranet que pasan polo Squid, pero que non consumen ancho da banda de Internet.
- `exclude.strings` – Se algunha liña do arquivo log contén algunha das cadeas deste arquivo, será ignorada no relatorio. Con isto poderase filtrar calquera cousa no relatorio.
- `exclude.users` – Os usuarios que figuren neste arquivo non estarán incluídos no relatorio.

Agora imos a crear un arquivo de configuración para o SARG. Como díxose anteriormente, este arquivo de configuración será para un relatorio diario. Poñeremos esta configuración no arquivo “etc/sarg/sarg-dia.conf”. Deseguido fica un arquivo de configuración comentado, para a súa posterior análise:

Relatorio do Squid por día:

```
# Idioma utilizado, coloquei eiquí o inglés, pero estará todo en galego, verase despois
```

```
#
```

```
language English
```

```
# Arquivo log do Squid.
```

```
#
```

```
access_log /var/log/squid/access.log
```

```
# Título da páxina HTML
```

```
title “Relatorio Diario do Proxy”
```

```
#
```

```
# --- Visual ---
```

```
#
```

```
# Eiquí temos algunhas variables que pódense cambiar
```

```
# para mudar o aspecto dos relatorios
```

```
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 onde xeraranse os relatorios
# Xeralmente deben estar dentro do raíz da webserver
output_dir /var/www/html/squid-report/dia
#
#
# Qué criterio de orden para a sección TOPUSER : USER/CONNECT/BYTES/TIME
# Con esto organizarase o relatorio da sección TOPUSER
topuser_sort_field BYTES reverse
#
#
# Criterio de orde para a seccion USER: SITE/CONNECT/BYTES/TIME
# Con esto organizarase a sección de usuarios do mesmo xeito co item anterior
user_sort_field BYTES reverse
#
#
# Arquivo dos usuarios que NON aparecerán no relatorio
exclude_users /etc/sarg/exclude.users
#
#
# Arquivo que contén os hosts que NON aparecerán no relatorio
exclude_hosts /etc/sarg/exclude.hosts
#
#
# Formato da data (e=dd/mm/yy, u=mm/dd/yy, w=yy/ww)
date_format e
# Limite de logs ata que os antigos sexan eliminados. Cando existan máis
# de N relatorios, o máis antigo é eliminado automaticamente.
# Deste xeito (lastlg 0) indicamos que non se debe eliminar nunca.
lastlog 0
O arquivo de configuración xa explica as configuracións que podemos alterar. Tamén existen máis opcións
dispoñibles no propio SARG, e poden verse no arquivo tipo de configuración que deixamos como
"/etc/sarg/default.conf".

```

Sobre a lingua utilizada, atopei un erro. Pero ten unha solución rápida para o mesmo. O que acontece é que aínda mudando a variábel linguaxe, o SARG segue a xerar relatorios en inglés. De pasar isto temos que facer:

```

# cd /etc/sarg/languages
# mv English English.old
# ln -s Galician English
NOTA DO TRADUCTOR: Non observei dito erro na Debian Sarge 3.1 r2 Kernel 2.6.8 co paquete .deb sarg-2.0.5
nin co paquete sarg-2.1.1.tar.gz

```

O que fixen eiquí foi facer un vínculo simbólico do Inglés ó Galego, para que o programa pegue o contido do arquivo Galego e non o do Inglés orixinal. Nótase que tamén fíxose unha copia de respaldo do arquivo Inglés, lembrar que débense sempre facer copias de respaldo.

Parece que temos o idioma configurado. Supoñamos que hoxe é o día 05/02/2003 e queremos xerar un relatorio con os usuarios que pasaron a través do proxy.

```

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

```

Dependendo da cantidade de accesos ó proxy, e do tamaño do arquivo de log, o proceso pódese demorar.

Cando termine, accederemos ó directorio configurado como saída no servidor web, onde configurouse a liña de código, para ver o relatorio íntegramente no seu navegador favorito:

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

Agora configuraremos o crontab para xenerar automáticamente o relatorio todos os días ás 01:01 da madrugada.

Nota: Varias distribucións xa incorporan un crontab diario configurado. E dicir, todos os arquivos executábeis que atópanse dentro do directorio “/etc/cron.daily” executaranse a determinada hora, xeralmente ás 04:00 da madrugada.

Si na nosa distribución xa hai ese directorio, crearemos o arquivo “/etc/cron.daily/sarg-dia”. De non existir, crearemos o arquivo “/usr/local/bin/sarg-dia”, co seguinte contido nun deses dous arquivos:

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

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

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

```
exit 0
```

No caso de crear o arquivo “/usr/local/bin/sarg-dia”, entón teremos que configurar o crontab para que execute esta tarefa ás 01:01 da mañá. Engadiremos a seguinte liña no arquivo “/etc/crontab”:

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

E non esqueceremos dar os permisos de execución ó arquivo que criamos:

```
# chmod +x /usr/local/bin/sarg-dia
```

(ou)

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

Ou tamén:

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

NOTA DO TRADUCTOR: Observei que no OpenSuSE 10.0 é necesario reiniciar o demonio cron para que garde os cambios. En Debian non é necesario, pero recomendo facelo: /etc/init.d/crontab restart

Aviso: Os relatorios xeneran moitas páxinas, e dependendo da lista, pode levar a ocupar un espazo considerábel no disco duro. Seremos conscentes desto, véxase como proba que no exemplo proposto para o 3 de febreiro, o ficheiro access.log ocupaba 103 MB.

Nota do traductor: Recomendo encarecidamente utilizar a partición /var separa da partición /.

Orixinal: Hugo Cisneros. hugo_en_devim_punto_com_punto_br

Traducci3 Galego: Evaristo Deus : evaristo punto deus en gmail punto com