



Shockware Gaming S.A. | Crédito de Síntesi 2014

SARG

Generando reportes del dominio Shockware Gaming S.A. periódicamente...



Squid Analysis Report Generator

Shockware Gaming S.A. Reportes SQUID

FILE/PERIOD	CREATION DATE	USERS	BYTES	AVERAGE
2014May25-2014May25-shockware-gaming.com	dom 25 may 2014 18:07:11 CEST	1	3.31K	3.31K
2014May24-2014May25	dom 25 may 2014 17:49:18 CEST	5	597.78K	119.55K

Generated by sarg-2.3.2 Nov-23-2011 on may/25/2014 18:07

SARG es una herramienta de analisis de logs de Squid, tiene soporte para generar reportes en diferentes idiomas, mediante los reportes de uso web usted podra obtener la siguiente información:

- Top Ten de sitios más visitados
- Reportes diarios, semanales y mensuales
- Gráficas semanales y mensuales del consumo por usuario/host
- Detalles de todos los sitios a los que entro un usuario/host
- Descargas

Sarg será configurado para generar reportes web de los accesos a Internet de forma periodica, además de poder ejecutarlo manualmente para generar reportes de fechas, usuarios o dominios en especifico.

Reporte Manual

Estos reportes son aquellos creados por el administrador del sistema y ejecutados manualmente, pueden ser personalizados en base a diferentes criterios, son almacenados en el directorio /var/www/squid-reports/Manual, cada reporte bajo su propio directorio.

Reporte Diario

Estos reportes son generados automáticamente por un trabajo de CRON diario a las 6:25 am y genera un reporte del día anterior, son almacenados en el

directorio /var/www/squid-reports/Diario, cada reporte bajo su propio directorio.

Reporte Semanal

Estos reportes son generados automáticamente por un trabajo de CRON cada semana a las 6:47 am y genera un reporte del día anterior, son almacenados en el directorio /var/www/squid-reports/Semanal, cada reporte bajo su propio directorio.

Reporte Mensual

Estos reportes son generados automáticamente por un trabajo de CRON cada mes a las 6:52 am y genera un reporte del día anterior. Estos reportes son almacenados en el directorio /var/www/squid-reports/Mensual, cada reporte bajo su propio directorio.

Siga en la siguiente sección para instalar sarg...

Instalación y configuración SARG

1. apt-get update & apt-get dist-upgrade.
2. Apt-get install sarg.
3. Gedit /etc/sarg/sarg.conf: "Modificar" →
 - **language Spanish**
 - **access_log /var/log/squid3/access.log**
 - **output_dir /var/www/sarg**
 - **title "Shockware Gaming S.A. Reportes Squid"**
 - **show_sarg_info yes**
 - **show_sarg_logo yes**
4. Reiniciar squid **service squid3 restart**.
5. Ejecutar **sarg**.
6. Entonces abrimos un navegador y ponemos localhost/sarg.
7. Tendremos esto:



Squid Analysis Report Generator

Shockware Gaming S.A. Reportes SQUID

FILE/PERIOD	CREATION DATE	USERS	BYTES	AVERAGE
2014May25-2014May25-shockware-gaming.com	dom 25 may 2014 18:07:11 CEST	1	3.31K	3.31K
2014May24-2014May25	dom 25 may 2014 17:49:18 CEST	5	597.78K	119.55K

Generated by sarg-2.3.2 Nov-23-2011 on may/25/2014 18:07

- Es un poco soso lo de localhost/sarg asi que le añadiremos HTTPS y un SUBDOMINIO llamado **shocksarg.shockware-gaming.com**:

1. Creamos una entrada en el BIND9 llamada shocksarg.*:

```

@      IN      SOA      shockware-gaming.com. root.shockware-gaming.co
                        2          ; Serial
                        604800     ; Refresh
                        86400      ; Retry
                        2419200     ; Expire
                        604800 )    ; Negative Cache TTL
;
@      IN      NS       shockware-gaming.com.
@      IN      A        192.168.19.233
www    IN      CNAME    shockware-gaming.com.
shockgamer  IN      A        192.168.19.233
shockcloud  IN      A        192.168.19.233
shockopkm   IN      A        192.168.19.233
shockmail   IN      A        192.168.19.233
shocksarg   IN      A        192.168.19.233

```

2. En el inverso también.
3. Entonces reiniciamos bind9.
4. En apache2/sites*/default creamos este contenido:

```
*default ✕

NameVirtualHost shocksarg.shockware-gaming.com:80
<VirtualHost shocksarg.shockware-gaming.com:80>
    ServerName shocksarg.shockware-gaming.com
    DocumentRoot /var/www/sarg
    ErrorLog /var/log/apache2/error.log
    CustomLog /var/log/apache2/error.log combined
    RewriteEngine on
    RewriteCond %{SERVER_PORT} !^443$
    RewriteRule ^/(.*) https://%{HTTP_HOST}/$1 [NC,R,L]
</VirtualHost>

NameVirtualHost shocksarg.shockware-gaming.com:443
<VirtualHost shocksarg.shockware-gaming.com:443>
    ServerName shocksarg.shockware-gaming.com
    DocumentRoot /var/www/sarg

    SSLEngine On
    SSLCertificateFile /etc/ssl/certs/shock2.pem
    ErrorLog /var/log/apache2/error.log
    CustomLog /var/log/apache2/error.log combined
    <Directory "/var/www/sarg">
        Options Indexes FollowSymlinks MultiViews
        AllowOverride None
        Order allow,deny
        Allow from all
        SSLRequireSSL
    </Directory>
</VirtualHost>
```

*PD: En virtualhost *80 hemos añadido 3 parámetros para la redirección HTTPS permanente del virtualhost.*

5. Entonces a partir de aquí reiniciamos apache2.
6. A continuación verificamos en el servidor:



FILE/PERIOD	CREATION DATE	USERS	BYTES
2014May25-2014May25-shockware-gaming.com	dom 25 may 2014 18:07:11 CEST	1	3.31K
2014May24-2014May25	dom 25 may 2014 17:49:18 CEST	5	597.78K

Generated by sarg-2.3.2 Nov-23-2011 on may/25/2014 18:07

7. Verificamos que perfectamente se creó y ahora procederemos a crear reportes.

- Para generar un reporte de una fecha especifica, o rango de fechas en especifico use el parametro -d, por ejemplo:
 - `sarg -d 28/05/2014`
- Si desea generar un reporte usando un rango de fechas, use:
 - `sarg -d 27/05/2014-15/06/2014`
- Si desea generar un reporte para una hora en especifico use la opción -t para indicar la hora, por ejemplo:
 - `sarg -d 27/05/2014 -t 12`
- Para generar un reporte de un usuario en especifico use:
 - `sarg -d 27/05/2014 -u shockgadmin`
- Para generar un reporte de un dominio destino en especifico use:
 - `sarg -d 27/04/2010 -s shockware-gaming.com`
 - *En nuestro caso hemos generado un informe de hoy del dominio shockware-gaming.com FOTO_SUPERIOR.*

[FOTO_FINAL_REPORTES]

8. Generación automática de reportes periódicos con SARG.

9. Generar el archivo `/etc/cron.daily/sarg`

10. Dentro de ella:

```
# Eliminar reportes diarios con mas de 10 dias de antigüedad
echo "Rotacion diaria del dia `date +%d-%m-%Y`" >> /var/log/squid3/sarg-rotate.log
find /var/sarg/Diario -type d -mtime +10 -exec rm -rf {} \; >> /var/log/squid3/sarg-rotate.log 2>&1
#Crear carpeta DIARIO
```

```
rm -rf /var/www/squid-reports/Diario/index.html  
  
# Ejeutar sarg  
#!/bin/bash  
exec /usr/bin/sarg -s shockware-gaming.com
```

11. Darle permisos de ejecución al script.
12. Al estar en cron.daily se ejecutará diariamente el script hecho por el servicio cron.
13. Si queremos reportes semanales el mismo script pero en cron.weekly y cambiando un poco la configuración:

http://tuxjm.net/docs/Manual_de_Instalacion_de_Servidor_Proxy_Web_con_Ubuntu_Server_y_Squid/html-multiples/ch07s07.html

14. Nosotros optaremos por reportes diarios.

```
0 21 * * 1,3,4 /home/shockgadmin/.scripts/sarg.sh  
45 17 * * 2 /home/shockgadmin/.scripts/sarg.sh  
10 19 * * 5 /home/shockgadmin/.scripts/sarg.sh
```

Integración con PROXY SQUID transparente.

- Hemos planificado una directiva de empresa que solamente podrán revisar los reportes los **GERENTES E INFORMÁTICOS**. Mientras que anteriormente denegamos sólo al cliente4 acceso a las zonas administrativas, le añadiremos el SARG también. Como novedad a los otros trabajadores tampoco podrán revisar los reportes del SARG.

```
squid.conf ✕
# Páginas web administrativas internas de Shockware Gaming S.A.
acl shockadmin dstdomain "/etc/squid3/shockadmin"

# PRUEBAS PC4 DENEGACIÓN PÁGINAS Administrativas e Interinas

http_access allow cliente4 !shockadmin !repo
http_access deny cliente4

acl repo dstdomain shocksarg.shockware-gaming.com

# -----

# DENEGAR Y PERMITIR

http_access allow servidor2
http_access allow localhost
http_access allow cliente1
http_access allow cliente2
http_access allow red-empresa horario !repo
http_access deny red-empresa
http_access deny all

# PROXY SQUID NO FUNCIONA CON HTTPS
```

- Los trabajadores tienen un horario de Lunes a Viernes de 2PM a 10PM, éstos podrán acceder de las páginas administrativas de la empresa excepto cliente4.
- Como cosa especial permitimos todo a los administradores del sistema y a los jefes.
- Denegamos **shocksarg** en toda la LAN de Shockware Gaming S.A. excepto los administradores, jefes y los servidores.