

SARG SQUID ANALYSIS REPORT GENERATOR



Squid Analysis Report Generator

Squid User Access Reports

FILE/PERIOD	CREATION DATE	USERS	BYTES	AVERAGE
2012Apr27-2012Apr27	Fri Apr 27 13:48:45 2012	12	416.65M	34.72M
2012Apr26-2012Apr26	Fri Apr 27 13:49:05 2012	12	689.73M	57.47M
2012Apr25-2012Apr25	Wed Apr 25 12:59:01 2012	1	3.77K	3.77K
2012Apr24-2012Apr24	Tue Apr 24 18:59:02 2012	1	3.77K	3.77K
2012Apr23-2012Apr23	Tue Apr 24 06:25:25 2012	2	24.17M	12.08M

APA ITU SARG SQUID ANALYSIS REPORT GENERATOR?

SARG adalah tools open source untuk menganalisis file log squid atau proxy dan menghasilkan laporan yang indah dalam format HTML dengan informasi tentang pengguna, alamat IP, situs diakses atas, total penggunaan bandwidth, waktu berlalu, download, akses ditolak website, laporan harian, laporan mingguan dan laporan bulanan.

SARG adalah alat yang sangat berguna untuk melihat berapa banyak bandwidth internet yang digunakan oleh mesin individu pada jaringan dan situs apa saja yang diakses oleh user melalui jaringan.

CARA INSTALL SARG DI UBUNTU

- Install sarg dan apache, dengan perintah sebagai berikut :

```
apt-get install sarg apache2
```

- Backup sarg.conf sebelum dilakukan perubahan, dengan perintah sebagai berikut :

```
cp /etc/sarg/sarg.conf /etc/sarg/sarg.conf.old
```

- Edit sarg.conf, dengan perintah sebagai berikut :

```
nano /etc/sarg/sarg.conf
```

```
//sesuaikan dengan sistem sobat
//yang perlu diperhatikan warna merah

language English

#access_log /var/log/squid3/access.log (ini untuk squid 3)
access_log /var/log/squid/access.log

title "OPINIKOE Squid User Access Reports"

font_face Tahoma,Verdana,Arial

header_color darkblue

header_bgcolor blanchedalmond

font_size 9px

background_color white

text_color #000000

text_bgcolor lavender

title_color green

temporary_dir /tmp

output_dir /var/www/squid-report

resolve_ip

user_ip no

topuser_sort_field BYTES reverse

user_sort_field BYTES reverse

exclude_users /etc/sarg/exclude_users

exclude_hosts /etc/sarg/exclude_hosts

date_format u

lastlog 0

remove_temp_files yes

index yes

index_tree file

overwrite_report yes

records_without_userid ip
```

```

use_comma yes

mail_utility mailx

topsites_num 100

topsites_sort_order CONNECT D

index_sort_order D

exclude_codes /etc/sarg/exclude_codes

max_elapsed 28800000

report_type topusers topsites sites_users users_sites date_time denied
auth_failures site_user_time_date downloads

usertab /etc/sarg/usertab

long_url no

date_time_by bytes

charset Latin1

show_successful_message no

show_read_statistics no

topuser_fields NUM DATE_TIME USERID CONNECT BYTES %BYTES IN-CACHE-OUT
USED_TIME MILLISEC %TIME TOTAL AVERAGE

user_report_fields CONNECT BYTES %BYTES IN-CACHE-OUT USED_TIME MILLISEC
%TIME TOTAL AVERAGE

topuser_num 0

download_suffix
"zip,arj,bzip,gz,ace,doc,iso,adt,bin,cab,com,dot,drv$,lha,lzh,mdb,mso,p
pt,rtf,src,shs,sys,exe,dll,mp3,avi,mpg,mpeg,pdf,tar,rar,docx,pptx,xlsx,
chm,flv,mp4,mkv,bz2,deb"

```

- Buat direktori squid-report pada root apache, dengan perintah berikut :

```

cd /var/www

mkdir squid-report

chmod 775 squid-report

```

- Jalankan perintah generate report sarg secara manual, dengan perintah berikut :

```

sarg -x

```

atau

```
sarg-reports today
```

- Agar log squid dibaca otomatis oleh sarg buatlah crontab, dengan perintah berikut :

```
crontab -e
```

```
//isikan kode ini
```

```
* /5 * * * * /usr/sbin/sarg-reports today > /dev/null 2>&1
```

```
00 00 * * * /usr/sbin/sarg-reports daily > /dev/null 2>&1
```

```
00 00 * * * /usr/sbin/sarg-reports weekly > /dev/null 2>&1
```

```
00 00 * * * /usr/sbin/sarg-reports monthly > /dev/null 2>&1
```

Untuk melihat hasil report sarg, ketikkan **http://ip-server-sarg/squid-report** pada browser, hasilnya akan tampil seperti gambar dibawah ini :

📄 192.168.11.3/squid-report/



Access Reports on proxy

[Daily](#)

[Weekly](#)

[Monthly](#)

📄 192.168.11.3/squid-report/Daily/



Squid Analysis Report Generator

Squid User Access Reports

FILE/PERIOD	CREATION DATE	USERS	BYTES	AVERAGE
2016Jan11-2016Jan11	Mon Jan 11 13:35:03 2016	53	1.53G	29.02M

Generated by sarg-2.3.6 Arp-21-2013 on Jan/11/2016 13:35



Squid Analysis Report Generator

Squid User Access Reports

Period: 2016 Jan 11

Sort: bytes, reverse

Top users

Top sites

Sites & Users

Downloads

Denied accesses

NUM		USERID	CONNECT	BYTES	%BYTES	IN-CACHE-OUT	ELAPSED TIME	MILLISEC	%TIME
1		172.100.1.197	2.25K	384.87M	25.02%	0.64% 99.36%	05:25:40	19,540,805	14.87%
2		172.100.1.99	1.65K	348.25M	22.64%	0.27% 99.73%	15:37:51	56,271,759	42.83%
3		172.100.1.121	1.92K	72.76M	4.73%	30.71% 69.29%	00:17:32	1,052,211	0.80%
4		172.100.1.158	440	71.68M	4.66%	2.12% 97.88%	00:06:00	360,809	0.27%
5		172.100.1.122	2.26K	66.35M	4.31%	56.70% 43.30%	00:13:18	798,615	0.61%
6		172.100.1.86	6.10K	64.20M	4.17%	36.74% 63.26%	00:29:09	1,749,507	1.33%
7		172.100.1.77	2.44K	61.49M	4.00%	72.18% 27.82%	00:11:58	718,371	0.55%
8		172.100.1.68	7.33K	56.89M	3.70%	63.67% 36.33%	00:08:52	532,776	0.41%
9		172.100.1.160	1.70K	49.63M	3.23%	72.60% 27.40%	00:34:23	2,063,831	1.57%
10		172.100.1.71	1.16K	39.33M	2.56%	36.40% 63.60%	00:06:10	370,314	0.28%
11		172.100.1.96	1.25K	32.71M	2.13%	5.80% 94.20%	00:05:38	338,488	0.26%
12		172.100.1.176	6.01K	30.74M	2.00%	12.56% 87.44%	00:42:15	2,535,389	1.93%
13		172.100.1.168	737	27.15M	1.77%	96.78% 3.22%	00:02:18	138,528	0.11%

Demikian tutorial SARG Squid Analysis Report Generator ini, semoga bermamfaat bagi kita semua.

Source :

<https://opinikoe.com/sarg-squid-analysis-report-generator/>