



SARG Linux Server by Mr.Jodoi

บทความนี้เหมาะสำหรับผู้ที่ต้องการติดตั้งตัวเก็บ log การเข้า website User

Sarg ( Squid Analysis Report Generator ) เป็นเครื่องมือในการเก็บ log เข้า website User ที่ใช้งานผ่าน Proxy Server (Squid ) Server OS Linux นั้นจะต้องทำการติดตั้งตัว Squid Apache ก่อนนะครับ โดยผมใช้ Linux CentOS 5.2

เริ่มต้นเลยนะครับ ก่อนอื่นต้องทำการติดตั้งตัวโปรแกรม sarg ผมเลือกใช้วิธี rpm เนื่องจากสะดวกและง่ายดี โดยต้องไปหา file sarg-XXX.rpm internet มาให้ได้ก่อน

<http://dag.wieers.com/rpm/packages/sarg/>

เลือกให้ตรงกับ linux ของเราน่าครับ แล้วทำการ download ไปไว้ใน Server ให้ได้ วิธีนี้ดังนี้

```
[root@jodoi-server2 ~]# wget
http://dag.wieers.com/rpm/packages/sarg/sarg-2.2.3.1-1.el5.rf.i386.rpm
```

หลังจากนั้นก็ทำการติดตั้ง ด้วย command rpm

```
[root@jodoi-server2 html]# rpm -ivh sarg-2.2.3.1-1.el5.rf.i386.rpm
warning: sarg-2.2.3.1-1.el5.rf.i386.rpm: Header V3 DSA signature: NOKEY,
key ID 6b8d79e6
Preparing...
#####
[100%]
1:sarg #####
[100%]
```

หลังจากติดตั้งเรียบร้อยแล้วก็ทำการตรวจสอบหรือแก้ไข file config sarg.conf

```
[root@jodoi-server2 html]# vi /etc/sarg/sarg.conf
```

จุดที่ควรตรวจสอบหรือแก้ไข แนะนำ 2

access\_log /var/log/squid/access.log ( file log squid proxy ต้องตรง )

output\_dir /var/www/html/squid-reports ( ตำแหน่งที่เก็บ report log )

ขั้นตอนต่อไปเป็นการสั่งให้ sarg ทำงานหรือสร้าง report โดยการพิมพ์ command sarg

```
[root@jodoi-server2 ~]# sarg  
SARG: Records in file: 1658, reading: 100.00%
```

ต่อไปเป็นการดู report browser โดยต้องพิมพ์ดังนี้ครับ <http://Ip-Linux-Server/squid-reports/>

เช่น <http://192.168.1.220/squid-reports/> เป็นต้น

FILE/PERIOD	CREATION DATE	USERS	BYTES	AVERAGE
2008Oct20-2008Oct20	Tue Oct 21 08:40:39 ICT 2008	1	7.89M	7.89M
2008Oct20-2008Oct20.2	Mon Oct 20 15:15:51 ICT 2008	3	10.89M	3.63M
2008Oct20-2008Oct20.1	Mon Oct 20 15:05:27 ICT 2008	1	1.96M	1.96M

Generated by sarg-2.2.3.1 Jan-02-2007 on Oct/21/2008 08:40

cron job นิดหน่อยครับ เพื่อให้ได้ report ที่แบ่งเป็นวันๆ

```
[root@jodoi ~]# crontab -e  
  
30 20 * * * /usr/bin/sarg >/dev/null 2>&1  
35 20 * * * rm -f /var/log/squid/access.log  
38 20 * * * /etc/init.d/squid restart
```

จะได้ผลดังนี้

FILE/PERIOD	CREATION DATE	USERS	BYTES	AVERAGE
2008Oct20-2008Oct20	Mon Oct 20 20:30:01 ICT 2008	3	2.01M	670.06K
2008Oct19-2008Oct19	Sun Oct 19 20:30:01 ICT 2008	3	449.36K	149.78K
2008Oct18-2008Oct18	Sat Oct 18 20:30:01 ICT 2008	2	133.62K	66.81K
2008Oct17-2008Oct17	Fri Oct 17 20:30:01 ICT 2008	5	2.68M	537.53K
2008Oct16-2008Oct16	Thu Oct 16 20:30:01 ICT 2008	4	647.11K	161.77K
2008Oct15-2008Oct15	Wed Oct 15 20:30:02 ICT 2008	4	530.05K	132.51K
2008Oct14-2008Oct14	Tue Oct 14 20:30:01 ICT 2008	1	295.67K	295.67K
2008Oct13-2008Oct13	Mon Oct 13 20:30:02 ICT 2008	2	2.99M	1.49M
2008Oct12-2008Oct12	Sun Oct 12 20:30:02 ICT 2008	3	12.68M	4.22M
2008Oct11-2008Oct11	Sat Oct 11 20:30:02 ICT 2008	2	239.94K	119.97K
2008Oct10-2008Oct10	Fri Oct 10 20:30:01 ICT 2008	2	452.86K	226.43K

หวังว่าคงเป็นประโยชน์บ้างนะครับ

### แหล่งข้อมูลอ้างอิง

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

<http://dag.wieers.com/rpm/packages/sarg/>

บริษัท โจดอย ไอทีเอนด์เซอร์วิส จำกัด

เลขที่ 300/1 อาคารแกรนด์ ดานา ทาวเวอร์ ซ.ลาดพร้าว 20 แขวงลาดยาว เขตจตุจักร กรุงเทพฯ 10900

โทร.0-2938-6583 ,0-2938-6239 แฟกซ์ 0-2938-6239

Hotline : 081-499-1807, 081-916-5773 , 089005-3124

[www.jodoi.com](http://www.jodoi.com)