

Assignment No. 4: Write a program for Log Capturing and Event Correlation

Name of Student:

Class: B.E.

Division: A / B/C

Roll No:

Date of Submission:

Marks Obtained: / 10

Signature of subject teacher:

Prerequisite:

- Latest version of Squid should be used.(version 2.5 or greater)
- A web server for testing purpose which can be used instead of Internet.
- Squid Version greater than 2.6 is required for Transparent squid proxy configuration in this lab.
-

Learning Objectives:

- To understand how Log Records are generated for Further Analysis.

New Concepts:

- Squid and Sarg

Theory

4.1. Introduction:

- During the period of development of internet, users are allowed for unlimited access to the resources due to less number of users. So there were less issues related to accessing speed over internet.
- With the increase in internet usage, many issues raised related to accessing speed, effective bandwidth utilization etc. One method of overcoming these issues is, maintaining a copy of webpage visited by a user in the cache so that the other user who visits the same webpage will access the same website within a short period of time. This method not only increases the accessing speed but also helps in utilizing the bandwidth effectively.
- The above said functionality can be achieved by maintaining a proxy server through which all the users in the organization or a group access the internet. The most widely used proxy server in Linux is Squid Proxy, which is free software released General Public License.

- Squid provides proxy and cache services for **Hyper Text Transfer Protocol (HTTP)**,

File Transfer Protocol (FTP), and various other protocols.

To configure a system as a proxy server, one should have a sufficient amount of memory for maintaining the cache which in turn increases the performance.

- In case if the internet connection is not available, setup one host as a web server in place of internet and assign the IP address to the proxy server network interface in the network, used by web server instead of public IP address assigned to that interface.

4.2. Steps to Configure Squid Proxy:

4.2.1. Installation of Squid Package

A Squid proxy server is generally installed on a separate server than the Web server with the original files. Squid works by tracking object use over the network. Squid will initially act as an intermediary, simply passing the client's request on to the server and saving a copy of the requested object. If the same client or multiple clients request the same object before it expires from Squid's **cache**, Squid can then immediately serve it, accelerating the download and saving bandwidth.

```
sudo apt update
sudo apt -y install squid
```

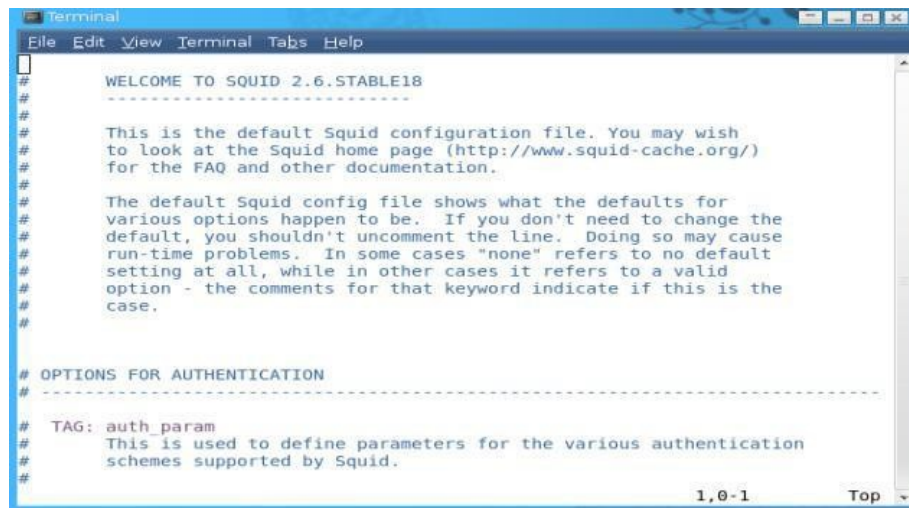
4.2.2. Accessing the Proxy Server configuration file

To configure squid proxy server we need to edit the `sudo gedit /etc/squid/squid.conf`

file and the default location of squid.conf file varies from distribution to distribution and from version to version. We can edit the configuration file using vi editor through command prompt.

```
sudo gedit /etc/squid/squid.conf
```

Then the content of the configuration file can be viewed as shown below in the figure.



```

# WELCOME TO SQUID 2.6.STABLE18
#
# This is the default Squid configuration file. You may wish
# to look at the Squid home page (http://www.squid-cache.org/)
# for the FAQ and other documentation.
#
# The default Squid config file shows what the defaults for
# various options happen to be. If you don't need to change the
# default, you shouldn't uncomment the line. Doing so may cause
# run-time problems. In some cases "none" refers to no default
# setting at all, while in other cases it refers to a valid
# option - the comments for that keyword indicate if this is the
# case.
#
# OPTIONS FOR AUTHENTICATION
#
# TAG: auth_param
# This is used to define parameters for the various authentication
# schemes supported by Squid.
#
1,0-1 Top

```

Editing the squid configuration file

```
sudo gedit /etc/squid/squid.conf
```

Search the TAG: auth_param and paste the following acl

```

auth_param basic program /usr/lib/squid/basic_ncsa_auth /etc/squid/passwd
auth_param basic children 5
auth_param basic realm Squid Basic Authentication
auth_param basic credentialsttl 2 hours
acl auth_users proxy_auth REQUIRED
http_access allow auth_users

```

#search localnet and paste line in last

```

acl localnet src 192.168.60.70
>sudo service squid3 restart

```

Specifying the interface and port number on which the proxy server should listen.

By default, the proxy server will listen on all the available network interfaces on the system for requests. For Example, if one interface card is assigned a public ip from which it is connected to internet and the other interface card is assigned an ip address which belongs to your local area network. Then in order to make you proxy server to listen for requests from your Local Area Network through a particular port, then change the variable http_port 3128 in the squid configuration file to desired ip address and port number in the format shown below.

`http_port <ip address belonging to LAN>:<port number>`

Example: For example, if your proxy server has an ip address 192.168.60.70 which belongs to the local area network 192.168.60.0/24 and you want the server to listen for requests from your LAN through a particular port say 3456, then you can change the variable `http_port` as shown.

`http_port 192.168.60.70:3456`

Assigning Access Controls

By default, no user machine is allowed to connect to the proxy server except the localhost. To allow the local machines access your proxy server, locate the `acl` section in the squid configuration file starting with `acl` and at the end of the last `acl` line specify your access

control. For example to allow local area network 192.168.60.0/24 machines to access your proxy server, specify the `acl` as

`acl mylan src 192.168.60.0/255.255.255.0`

In the above example, `mylan` specifies the name of my access control. We can specify any name other than `mylan` for access control. `src` specifies the source network.

Allow or Deny based on Access Control.

After specifying the access control for your local LAN, we need to provide allow permission for the specified LAN using `http_access` variable in the squid configuration file as shown in the example below.

Example: To allow the above specified access control (i.e `acl mylan src 192.168.60.0/255.255.255.0`), we need to specify the `http_access` variable as

Copyright © 2009, Centre for Development of Advanced Computing,
Hyderabad `http_access allow mylan`

Here `mylan` specifies the access control used. Suppose if we want to allow all the networks except the 192.168.60.0/24 network to access the proxy then we can specify the `http_access` variable as

`http_access deny !mylan`

In the above line, `!mylan` specifies except `mylan` network.

Note:

The above specified `http_access` variable should be specified before the line

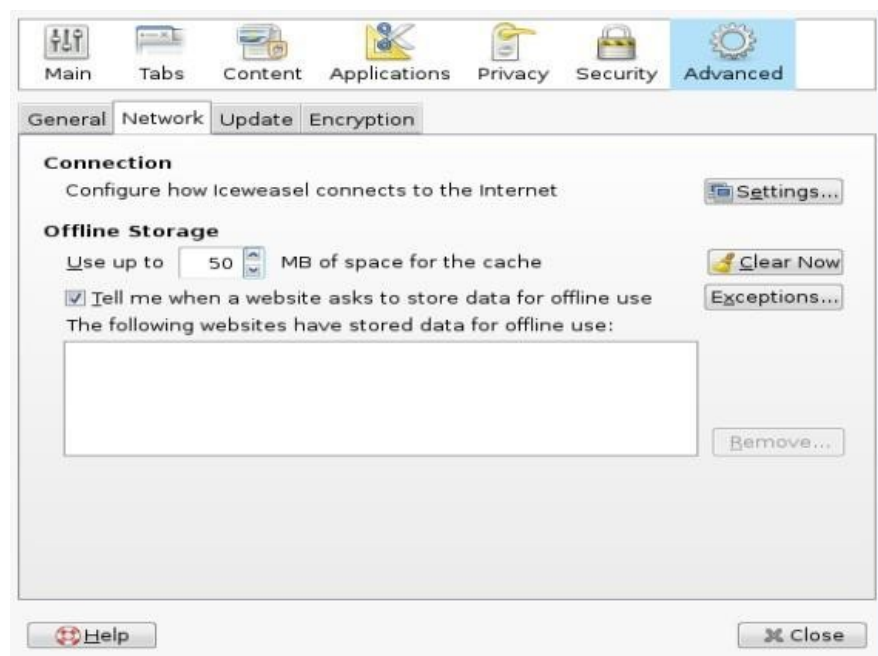
http_access deny all in the configuration file.

Saving the changes and exit the gedit Editor

After making appropriate changes to your configuration file exit the vi editor window by pressing Esc followed by :wq!. Here wq specifies save changes and exit the configuration file.

4.3 Testing the Squid configuration

To test the squid configuration, open a browser in any one of the pc in local area network or on the proxy server and specify the proxy settings as the ipaddress of the proxy server and port on which it is listening for requests. For example, in firefox web browser if we want to set the proxy settings in the browser window goto **Edit --> Preferences** and window similar to shown below will be displayed.



Now select Advanced tab, and under advanced tab click on Network tab and click on Settings option under Connection field. Then a window similar to the shown below will be displayed.



4.4 SARG – Squid Analysis Report Generator and Internet Bandwidth Monitoring Tool

SARG is an open source tool that allows you to analyze the squid log files and generates beautiful reports in HTML format with information's about users, IP addresses, top accessed sites, total bandwidth usage, elapsed time, downloads, access denied websites, daily reports, weekly reports and monthly reports.

The SARG is very handy tool to view how much internet bandwidth is utilized by individual machines on the network and can watch on which websites the network's users are accessing.

Installing Sarg from Source

The 'sarg' package by default not included in **RedHat** based distributions, so we need to manually compile and install it from source tar ball. For this, we need some additional pre- requisites packages to be installed on the system before compiling it from source.

\$ sudo apt-get install sarg

Configuring Sarg

Now it's time to edit some parameters in SARG main configuration file. The file contains lots of options to edit, but we will only edit required parameters like:

Access logs

path

Output

directory

Date

Format

Overwrite report for the same date.

Open sarg.conf file with your choice of editor and make changes as shown below.

```
# vi /usr/local/etc/sarg.conf    [On RedHat based systems]
```

Now Uncomment and add the original path to your squid access log file. # sarg.conf

```
# TAG: access_log file
```

```
#   Where is the access.log file
```

```
#   sarg
```

```
-l file
```

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

Next, add the correct Output directory path to save the generate squid reports in that directory. Please note, under Debian based distributions the Apache web root directory is '/var/www'. So, please be careful while adding correct web root paths under your Linux distributions.

```
# TAG: output_dir
```

```
#   The reports will be saved in that
```

```
directory # sarg -o dir
```

```
output_dir /var/www/html/squid-reports
```

Set the correct date format for reports. For example, 'date_format e' will

display reports in 'dd/mm/yy' format.

```
# TAG: date_format
```

```
#      Date format in reports: e (European=dd/mm/yy), u
```

```
(American=mm/dd/yy), w (Weekly=yy.ww)
```

```
#
```

```
date_format e
```

Next, uncomment and set Overwrite report to

```
'Yes'. # TAG: overwrite_report yes|no
```

```
# yes - if report date already exist then will be overwritten.
```

```
# no - if report date already exist then will be renamed to filename.n,
```

```
filename.n+1 #
```

```
overwrite_report yes
```

That's it! Save and close the file.

Step 3: Generating Sarg Report

Once, you've done with the configuration part, it's time to generate the squid log report using the following command.

```
# sarg -x      [On RedHat based systems]
```

Assessing Sarg Report

The generated reports placed under '/var/www/html/squid-reports/' or '/var/www/squid-reports/' which can be accessed from the web browser using the address.

http://localhost/squid-

reports OR

<http://ip-address/squid-reports>

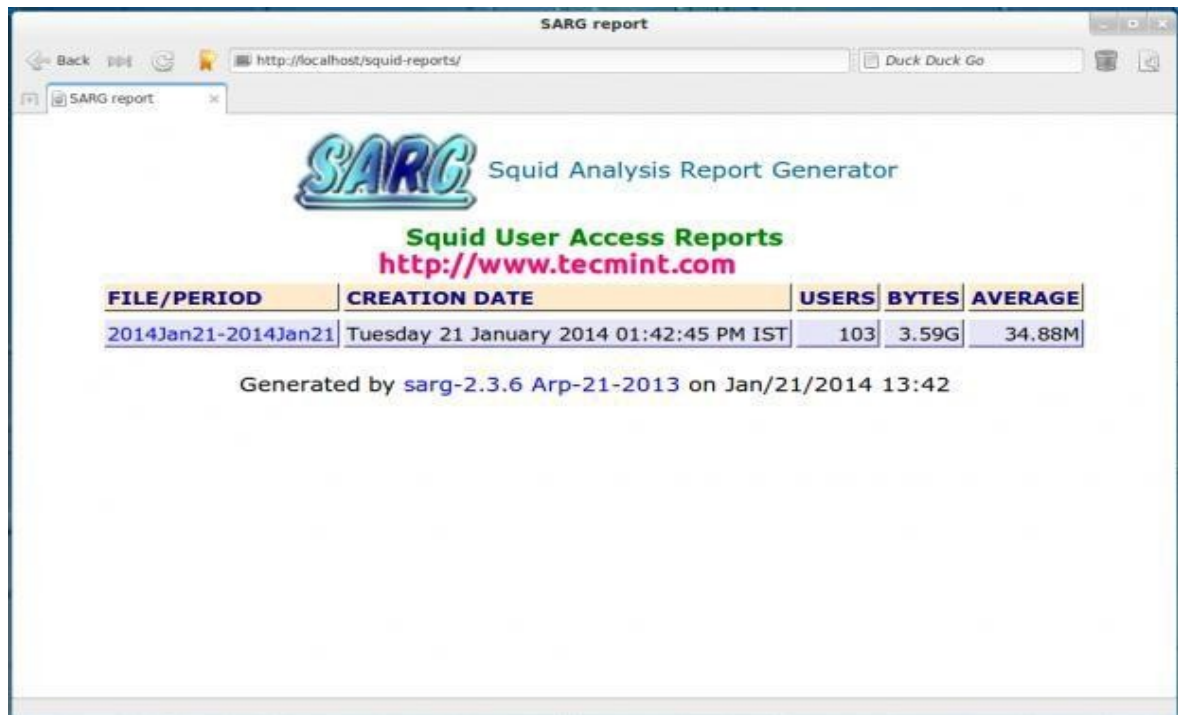


Fig.1 Sarg Main Window

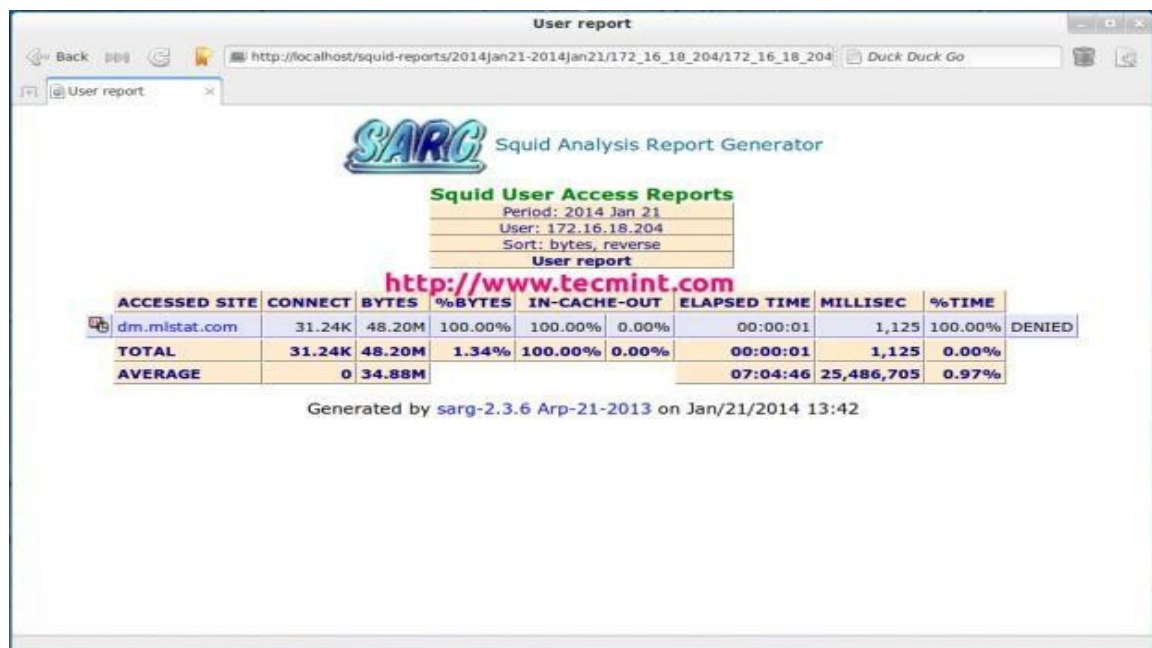


Fig2.User Report

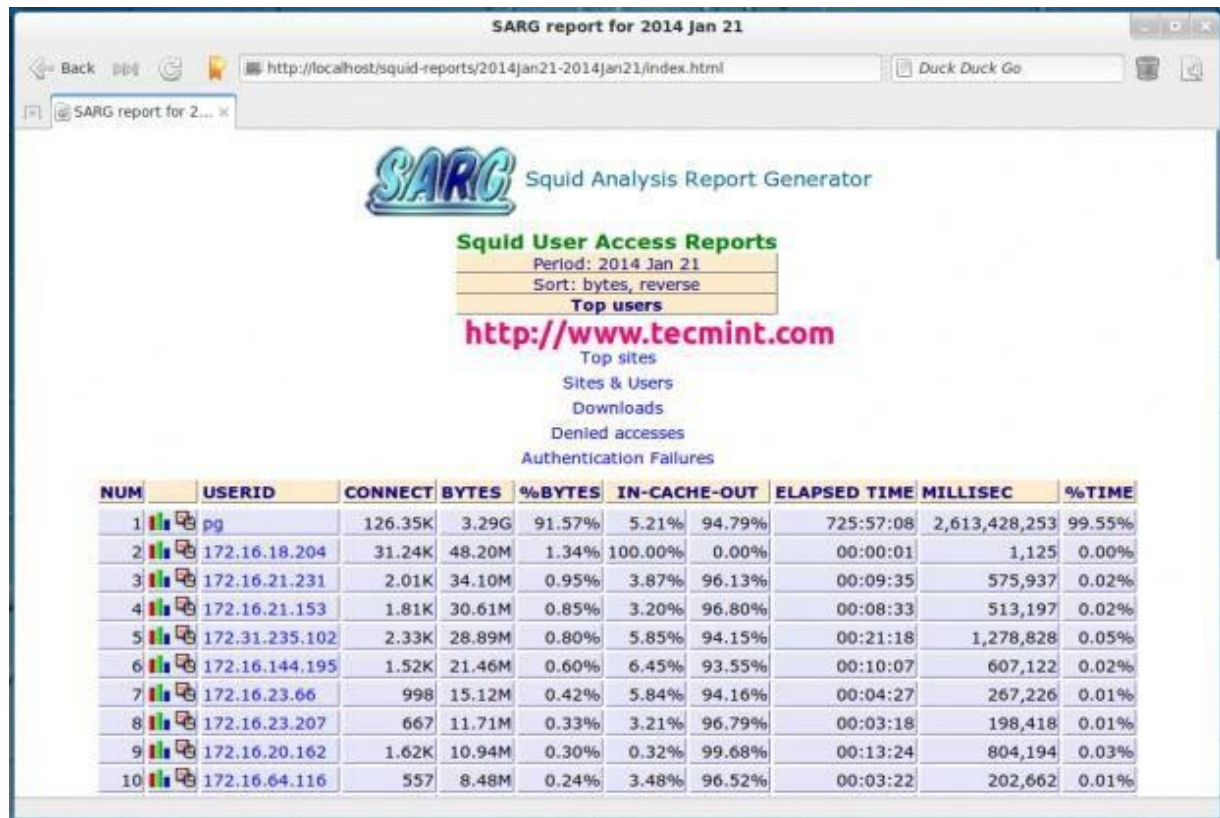


Fig 3. Specific Date



Fig 4. Top Accessed Sites

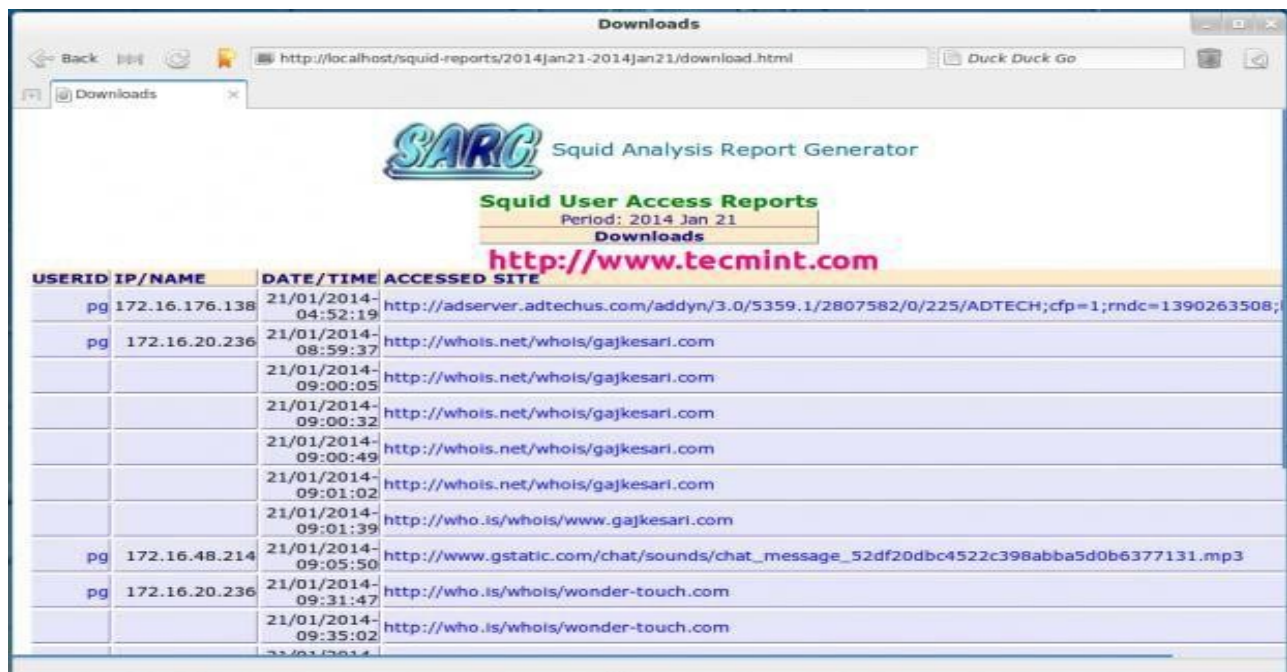


SARG Squid Analysis Report Generator

Squid User Access Reports
Period: 2014 Jan 21
Sites & Users
<http://www.tecmint.com>

NUM	ACCESSED SITE	USERS
1	01cefa72.f5b4ddd0	pg
2	0.gravatar.com	pg
3	0-p-04-frc3.channel.facebook.com:443	pg
4	0-p-06-ash2.channel.facebook.com:443	pg
5	0-p-06-frc1.channel.facebook.com:443	pg
6	0-p-07-ash2.channel.facebook.com:443	pg
7	0-p-13-prn1.channel.facebook.com:443	pg
8	0.r5o3z5kego.wc.lognormal.net	pg
9	0.tqn.com	pg
10	10138630.log.optimizely.com	pg
11	101greatgoals.disqus.com	pg
12	124.124.40.62	pg
13	124.124.40.62:1935	pg
14	125-events.olark.com	pg
15	131788053.log.optimizely.com	pg
16	172.16.16.36:9090	172.16.144.195 172.16.21.144 172.16.21.153 172.16.21.2 172.16.21.231 172.16.21.79 172.16.22.158 172.16.23.143 172.16.23.207 172.16.23.66 172.16.64.116 172.31.235.102

Fig 5. Top Sites and Users



SARG Squid Analysis Report Generator

Squid User Access Reports
Period: 2014 Jan 21
Downloads
<http://www.tecmint.com>

USERID	IP/NAME	DATE/TIME	ACCESSED SITE
pg	172.16.176.138	21/01/2014-04:52:19	http://adserver.adtechus.com/addyn/3.0/5359.1/2807582/0/225/ADTECH;cfp=1;rndc=1390263508;
pg	172.16.20.236	21/01/2014-08:59:37	http://whois.net/whois/gajkesari.com
		21/01/2014-09:00:05	http://whois.net/whois/gajkesari.com
		21/01/2014-09:00:32	http://whois.net/whois/gajkesari.com
		21/01/2014-09:00:49	http://whois.net/whois/gajkesari.com
		21/01/2014-09:01:02	http://whois.net/whois/gajkesari.com
		21/01/2014-09:01:39	http://who.is/whois/www.gajkesari.com
pg	172.16.48.214	21/01/2014-09:05:50	http://www.gstatic.com/chat/sounds/chat_message_52df20dbc4522c398abba5d0b6377131.mp3
pg	172.16.20.236	21/01/2014-09:31:47	http://who.is/whois/wonder-touch.com
		21/01/2014-09:35:02	http://who.is/whois/wonder-touch.com

Fig 6. Top Downloads

Denied

http://localhost/squid-reports/2014Jan21-2014Jan21/denied.html

Duck Duck Go

SARG Squid Analysis Report Generator

Squid User Access Reports
Period: 2014 Jan 21
Denied

<http://www.tecmint.com>

USERID	IP/NAME	DATE/TIME	ACCESSED SITE
172.16.16.211	172.16.16.211	21/01/2014-12:05:04	aus3.mozilla.org:443
		21/01/2014-10:48:34	fhr.data.mozilla.com:443
		21/01/2014-11:04:30	fhr.data.mozilla.com:443
		21/01/2014-12:04:38	fhr.data.mozilla.com:443
		21/01/2014-12:11:25	services.addons.mozilla.org:443
		21/01/2014-12:11:25	versioncheck-bg.addons.mozilla.org:443
		21/01/2014-12:11:25	versioncheck-bg.addons.mozilla.org:443
		21/01/2014-12:11:25	versioncheck-bg.addons.mozilla.org:443
172.16.21.234	172.16.21.234	21/01/2014-04:22:22	http://si.informer.com
172.16.24.230	172.16.24.230	21/01/2014-07:31:41	http://www.msftncsl.com
172.16.26.1	172.16.26.1	21/01/2014-12:36:39	http://172.16.25.252
172.16.26.2	172.16.26.2	21/01/2014-12:30:10	http://sa.windows.com
		21/01/2014-12:30:10	http://sa.windows.com
		21/01/2014-12:30:13	http://sa.windows.com
		21/01/2014-12:31:36	http://sa.windows.com
		21/01/2014-12:31:58	http://sa.windows.com
172.16.26.3	172.16.26.3	21/01/2014-10:13:52	addons.mozilla.org:443
		21/01/2014-08:54:31	aus3.mozilla.org:443
		21/01/2014-08:48:35	http://archive.mid-dav.com

Fig 7. Denied Access

Authentication Failures

http://localhost/squid-reports/2014Jan21-2014Jan21/authfail.html

Duck Duck Go

SARG Squid Analysis Report Generator

Squid User Access Reports
Period: 2014 Jan 21
Authentication Failures

<http://www.tecmint.com>

USERID	IP/NAME	DATE/TIME	ACCESSED SITE
172.16.144.114	172.16.144.114	21/01/2014-12:21:26	accounts.google.com:443
		21/01/2014-12:21:26	accounts.google.com:443
		21/01/2014-12:21:26	accounts.google.com:443
		21/01/2014-12:21:26	accounts.google.com:443
		21/01/2014-12:21:26	accounts.google.com:443
		21/01/2014-12:21:27	accounts.google.com:443
		21/01/2014-12:21:27	accounts.google.com:443
		21/01/2014-12:21:28	accounts.google.com:443
		21/01/2014-12:21:30	accounts.google.com:443
		21/01/2014-12:21:30	accounts.google.com:443
		77 more authentication failures not shown here...	
172.16.144.130	172.16.144.130	21/01/2014-09:24:09	ent-shasta-rrs.symantec.com:443
		21/01/2014-09:34:46	ent-shasta-rrs.symantec.com:443
		21/01/2014-09:45:09	ent-shasta-rrs.symantec.com:443
		21/01/2014-09:05:01	http://172.16.16.70:8014
		21/01/2014-09:47:23	http://ad.goo.mx
		21/01/2014-09:04:59	http://defender:8014
		21/01/2014-09:05:01	http://defender:8014
		21/01/2014-09:05:00	http://defender.midcorp.mid-dav.com:8014

Fig 8. Authentication Failures

Conclusion:

By configuring this Network Administrator can easily analyze the Network Traffic and Bandwidth Utilization.

4.5 Assignment Questions:

1. Why to Configure Proxy Server?
2. What is SARG?
3. Which Parameter is there in SARG Report?
4. What do you mean by Log and Event Co-relation?