International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 02 Issue: 03 | June-2015 www.irjet.net p-ISSN: 2395-0072

IMPORTANCE OF CENTRALIZED LOG SERVER AND LOG ANALYZER SOFTWARE FOR AN ORGANIZATION

R.Anusooya[1], J.Rajan[2], S.A.V.SatyaMurty[3]

1. Scientific Officer-E, Computer Division, Indira Gandhi Centre for Atomic Research, Tamilnadu, India
2. Scientific Officer-F, Computer Division, Indira Gandhi Centre for Atomic Research, Tamilnadu, India
3.Outstanding Scientist, Computer Division, Indira Gandhi Centre for Atomic Research, Tamilnadu, India

---

Abstract - ***Most of the enterprise organizations in the last few years have designed their network infra structure to higher levels of accountability and information security standards. Information Security Regulatory bodies have implemented a substantial number of regulations which forced the organizations to focus on their information security standards. One of the major guidelines provided by the regulatory bodies is to focus on collection, retention and review of logs from their application servers and network servers like e-mail server, firewall server, web server, proxy server, etc., Log data of such organizational servers are their richest information asset for assessing security posture, tracking sophisticated threats, and meeting audit requirements. Because of their evidentiary value, logs must be managed as a legal record; they must be complete, accurate and verifiable[1]. Analysis of these log files are very difficult to do without the support of an external utility designed for analyzing such data. There are many log analysis programs available in the market for analyzing these log files but an indigenous program is needed for an organization to analyze its own server log data format. This paper highlights on the importance of Central log server and also the effectiveness of log analyzer software for analyzing the huge volume of log data fetched from all the network servers and appliances. It briefly discusses the indigenous log analyzer software developed for our organization.***

Key words : Central Log Server, Log Server, Log analyzer, Rsyslog, syslog

1. INTRODUCTION:

The servers on the Internet and Intranet produce diverse and huge volume of logs. Obtaining relevant information from these logs daily will be a challenging task for the system / network administrator. For Example, e-mail server / web server is an essential communication tool for many industries, government and academic organizations. These servers play a vital role in exchanging messages, data files, images and voice messages over Internet. Since these kinds of servers will be contacted by many servers from the Internet, careful deployment planning according to the organization's security policy is needed. This ensures that these servers have been installed, configured and implemented in a secure manner. Logs of these servers are the richest source of information in an enterprise organization and it should be kept safe. Due to its evidentiary value, logs must be managed as a legal record; they must be complete, accurate and verifiable.[1] Logs of servers will vary according to the organization's security policy and posture. So an in-house developed log analyzer program will be an effective solution for an organization to analyze its own servers log data format. This paper discusses the importance of Central log server and how the huge volume of log data of an organization is converted into a meaningful Meta data and analyzed using scripts and programs.

2. CENTRAL LOG SERVER

A centralized log server stores the real-time and archived logs of various network services, hosts and appliances that are used in the network and these logs are referred to for troubleshooting, resource monitoring and security analysis. The network servers, hosts and network appliances keep their own logs and configured to simultaneously send all local logs to a secured remote log server. Storing the logs only on the host where the message has been generated is problematic for several security reasons.

To overcome these issues, a central log server with proper security measures is needed. With good planning and rigorous implementation of secure configurations and operational procedures, organizations can operate successful central logging system while protecting their networks and information resources. Network devices and operating systems generate text messages of various events that happen to them like – login information, file creation, server daemon statistics, user login, established connections between remote hosts and intranet servers, network activities, etc. These text messages are called log messages, these messages can be used to detect security incidents, operational problems, policy violations, and are useful in auditing and forensics situations.

The figure (Fig – 1) illustrates that each and every network device in an organizational network setup sends the log messages to the central log server and the system

administrator monitors the alerts and events generated by all logs of the server by sitting in a centralized location.

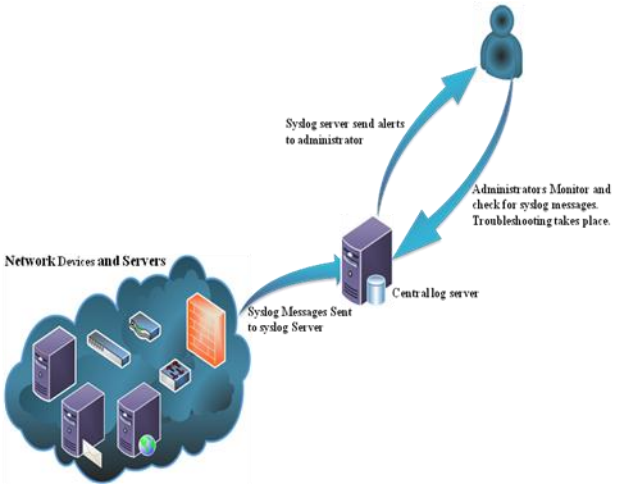

Fig – 1: Typical Central syslog server setup

The log messages use the legacy syslog / rsyslog protocol, which is supported by most of the UNIX distributions and appliances. Recent Linux distributions come with the "rsyslog" service. The "rsyslog" service replaces the "syslog/syslog-ng" services of earlier linux distributions. The "rsyslog" service has been implemented and is available on virtually in every UNIX-like operating system, and has become the de-facto standard of remote logging.

System administrators look at the syslogs as a critical source to troubleshoot performance problems on syslog supported systems & devices across the network. The need for a complete sys-log monitoring solution is often underestimated; leading to long hours spent sifting through tons of syslogs to troubleshoot a single problem. Efficient event log syslog analysis reduces system downtime, increases network performance, and helps tighten security policies in most of the organizations.

The following sections will briefly discuss on the importance of central log server, benefits of "rsyslog" service as it has more features when to the earlier "syslog / syslog-ng" service and the log analyzer software.

2.1 Aim of central log server

The aim of central logging system is to collect the log messages from different network hosts like switches, routers, firewall server, proxy server, e-mail server, web server etc., into a single, central log server. The main benefits of this server are listed below:

i. Since the logs of all network hosts, appliances are available at centralized location; an administrator need not login individually to each of the network hosts to check the logs.
ii. A centralized log server helps nullify any system overhead while running tools on logs, since the logs on the central log server are essentially offline to the hosts, applications etc.
iii. Each networked hosts does not need to provision disk space for logs that would accumulate over time, instead only the last few days/weeks can be retained on the client host and the server may be configured to keep logs for a much farther time span for the individual hosts, appliances, etc.
iv. If the client host, appliance etc., goes offline for some reason, the logs are still there to find out what happened.
v. Monitoring logs for security incidents are proactive and the cheapest line of defense towards an information security breach and is one of the first step towards IT security.

The following section details how to setup a central log server using a Linux host for the central log server.

2.2 Rsyslog configuration

System administrator monitors and responds immediately to the critical events or an alert that takes place in a network setup by implementing a suitable troubleshooting mechanism. This troubleshooting mechanism can be default software available with the operating system or an in-house developed software solution. Rsyslog service is one such mechanism to consolidate all logs from multiple sources into a single location. Typically, most central syslog servers have the following components that make this possible.

a. ***Rsyslog service:*** Log server needs to receive messages sent over the network. A listener process gathers rsyslog data sent over reliable TCP transport. This rsyslog service can also be used as a client as well as for a relay server forwarding syslog messages from a client to another server. Configurations are stores under /etc/rsyslog.d/ directory.
b. ***Database:*** Large networks can generate a huge amount of Syslog data. Good Syslog servers will use a database to store syslog data for quick retrieval.
c. ***Management and filtering software:*** Because of the potential for large amounts of data, it can be cumbersome to find specific log entries when needed. The solution is to use a syslog server that both automates part of the work, and makes it easy to filter and view important log messages.

The main configuration file is the rsyslog.conf file under the /etc/ directory. "rsyslog" has the following sections a) Configuration directives which are global, b) Templates that format the message to be logged, c) Output modules that write the message to their specified destination and d) Rules that define the action to be taken on a match. *"rsyslogd"* has been configured to accept remote messages from different client machines. To configure the log server, the client must be listed in /etc/rsyslog.conf, and the logging facility must be specified,

+client1.example.com
. /var/log/client1.log
Once added, all *facility* messages will be logged to the file, /var/log/client1.log. The log file should be created with the following command,
touch /var/log/client1.log

The following figure (Fig – 2) shows the sample rsyslog configuration file with comments.

```
root@localhost /]# more /etc/rsyslog.conf
# ************************************************************
$IncludeConfig /etc/rsyslog.d/*.conf # Include all config files in /etc/rsyslog.d

#################
#    MODULES    #
#################
module(load="imuxsock") # provides support for local system logging (e.g. via logger command)
module(load="imklog") # provides kernel logging support (previously done by rklogd)
module(load="imudp") # needs to be done just once
input(type="imudp" port="514")
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

#################
#      RULES    #
#################
*.info;mail.none;authpriv.none;cron.none      /var/log/messages
authpriv.*                                    /var/log/secure
mail.*                                        /var/log/maillog
cron.*                                        /var/log/cron
*.emerg                                       :omusrmsg:*
uucp,news.crit                                /var/log/spooler
local7.*                                      /var/log/boot.log

######################
#    Directives      #
######################
# Set the default permissions for all log files.

$FileOwner root
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755

####################
#    Templates     #
####################

$template TmplAuth, "/var/log/rsyslog_custom/%HOSTNAME%/%PROGRAMNAME%.log"
$template TmplMsg, "/var/log/rsyslog_custom/%HOSTNAME%/%PROGRAMNAME%.log" authpriv.* ?TmplAuth
*.info,mail.none,authpriv.none,cron.none ?TmplMsg
[root@localhost /]#
```

Fig – 2: Configuration file - rsyslog

The rsyslogd daemon should be restarted and verified:
service rsyslogd restart
ps –ef |grep rsyslog
If a PID is returned, the server has been restarted successfully, and client configuration may begin. If the server has not restarted, consult the */var/log/messages* log for any output. Now the servers configured with rsyslog service will be able to generate alerts, notifications and alarms in response to select messages. Now the administrators will know as soon as a problem occurs and can take faster action.

2.3 Features of "rsyslog"

2.3.1 Security

"rsyslog" supports TCP based network transport for messages from log sources and has the ability to support encrypting log traffic between client and server with TLS (SSL). With this capability any organization may place their log server and clients in remote geographies and use the public Internet for transferring log data[12].

2.3.2 Log rotation

Rotating the remote message logs on the server will save precious disk space. Without rotating the log disk space will just continue to grow eventually filling up drives. Log rotation not only saves the disk space it will make searching for log files easier than opening up a large log file that was not set into log rotate[12]. Log file can be compressed in gzip file format and can be rotated after a specified number of weeks or months.

2.3.3 Log message routing

Log messages collected from different network hosts with time-stamps should be routed for further analysis. The following figure (Fig – 3) shows the routing of log messages with rsyslog service collected from different sources and filtered according to the application and importance of the log data.

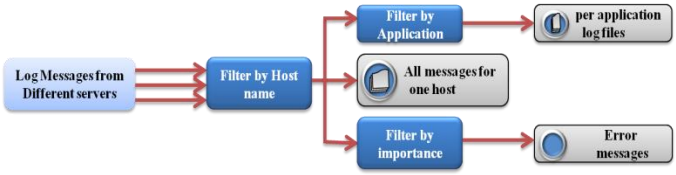

Fig – 3: Routing of Log messages using rsyslog

3. ROLE OF NTP SERVER IN THE ORGANIZATIONAL NETWORK SETUP

System log contains log messages with the following information, i.e. the log message, the network application/node/device/appliance and the time-stamp. The time-stamp of an event is one of the most important pieces of information in the logs. Administrator's, quite frequently need to refer to time-stamp's in order to correlate events that have occurred in the network. An NTP server helps maintain the system date-time in all the hosts in a network and is the one important service that must be available to all hosts in a network while creating a centralized log solution for an Organization[12].

4. ROLE OF CENTRAL LOG SERVER FOR AN ENTERPRISE ORGANIZATION

The most critical servers of an organization under constant attack from spammers and hackers are e-mail server / web server / application server. Even if they're not successful at stealing data or compromising the network, spammers can cripple bandwidth, while hacks such as relay theft can interfere with effective communications and cause network instability. So organizations should have an efficient central log server to monitor all the network activities and should follow some of the following best practices to keep their network servers secure.

a. *Dynamic network traffic inspection using Intrusion Prevention system to block malicious network requests.*
b. *Keep virus and spam off the network before it can cause trouble. Implementing effective filtering, proactive monitoring, reputation filtering, Black listing domains, etc.,*

c. *DMZ Zone should be isolated and no direct connection to access the LAN by writing a rule in the firewall.*
d. *Restrictive mail relay parameters to avoid relay thefts.*
e. *Limit the number of connections allowed to your Web / SMTP server to prevent DOS attacks.*
f. *Application servers are patched periodically to avoid the exploitation of vulnerabilities in them.*
g. *Taking backup of Web server data / Mail boxes / Application data on a regular basis.*
h. *Regular monitoring of Router / Firewall / Proxy server logs.*
i. *Correct position of servers in an organization network.*
j. *Information security auditing of servers like firewall (rules), NIPS rules, proxy settings, web server, SMTP server, etc., on a regular basis are some of the best practices organization should follow to avoid security breach.*

The following figure (Fig – 4) shows the typical network setup of an enterprise organization.

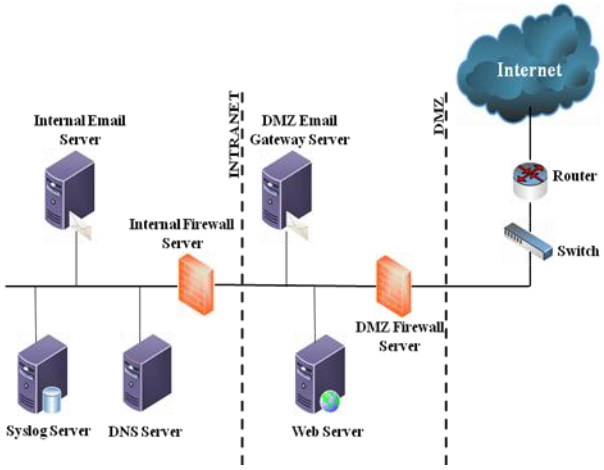

Fig – 4: Typical Network setup in an Organization

This kind of multi-stage approach for keeping network servers secure requires installation and configuration of different servers like Firewall, Network Intrusion Prevention system, Application level Firewall, SMTP server at various levels of an organization's network setup. These servers will be configured with anti-spam, anti-virus, anti-spyware, anti-malware software and also with authentication and encryption features. Web servers / web application servers need be protected against sql injection, cross site scripting attacks, etc., Services supported by the web server / e-mail server / application server should be well-defined according to the organization's security policy.

5. LOG ANALYZER SOFTWARE

As mentioned in the above section, a defense-in-depth approach is needed for the smooth functioning of systems. All these servers configured with proper security features in addition to software configurations complicate the event analysis and log management. So an in-house developed, indigenous event analyzer and management solution will help to solve these kinds of issues and it will be easy for the system administrator to trace back any kind of events that had happened in those servers with this software solution. The log analyzer software analyzes how the huge volume of log data is distinguished, disseminated and presented after demystification. The indigenously developed log analyzer program helps to analyze the log Meta data viz; utilization of the organizational service, security incident handling, domain wise statistics, network data peak hour usage, individual's e-mail / web usage statistics, Internet and Intranet applications usage statistics, periodical network statistics, etc.,

The following sections will explain the log data analysis software, its architecture and management.

6. LOG DATA ANALYSIS SOFTWARE ARCHITECTURE

Log data analysis is an important need of IT departments in all organizations. These logs need to be collected, analyzed, archived, searched and reports generated for the purpose of IT security audit and compliance of various regulatory acts. The log management can make serious demands on an organization's technological infrastructure, many commercial hardware and software vendors have attempted to meet the challenges of log management by implementing common approaches. One of the most common approaches is often built upon in-house developed software created for e-mail and computer systems. Such in-house software should deal with terabytes of message data in logs alone, this pressurizes system administrators and the risk management team to decide what to keep and how to manage the deluge of data with *completeness, accuracy and verifiability*[1].

a. *Completeness* in the context of logs means that activity is captured without gaps in time and collectively that logs throughout an organization are mainlined in the aggregate.
b. *Accuracy* means that the time, date and content of the log are the same as when it was created. Electronic copies are considered to be *best evidence* only if they accurately reflect the original.
c. *Verifiability* - If logs are to earn the labels of *complete* and *accurate* they must be verified as such. Some techniques such as hashing, documenting each step of the log management process and storing the data in multiple separate locations are used for the verification of logs.

If ensuring logs are complete, accurate and verifiable then the first step is to manage logs and the next step is to figure out how to turn all the data into an information

resource. It is essential to be able to extract information from the terabytes of enterprise log data for continuous log data analysis and its management.

7. IN-HOUSE DEVELOPED LOG DATA ANALYSIS SOFTWARE ARCHITECTURE

As we have seen in the above sections that the commercial and freeware software solutions available in the market for log analysis and management will not be an effective solution, it becomes mandatory for each system administrator to develop indigenously developed software compiled with their security policies for storing and analyzing the log data. This log analysis software should be web-based, real-time, log monitoring and compliance management solution for Security Information and Event Management (SIEM) that improves internal network security and helps to comply with the latest IT audit requirements.

In most of the enterprise organizations, all the servers are installed and configured with anti-virus, anti-spam and anti-spyware software, hence it would be difficult to trace out the occurrence of a particular event in the huge volume of log file. So the analysis software should consist of a central syslog server, log rotation scripts, data filtration and categorization programs, command line or web utilities to perform queries against the data and generate reports. The Figure (Fig – 5) shows the architecture of typical log data analysis and management software. It is consists of 3 layers as described in the following table (Table -1),

Table – 1: Layers of Log Analyzer Software

S.No.	Layers	Description
1.	Layer1	Log data fetching from servers and rotation using script program
2.	Layer2	Meta data analysis, categorization and storage of log data in Database
3.	Layer3	Querying and Report generation

In layer one, the script program fetches the log data, rotates it and store the raw log data in a file. This file is further analyzed and checked for consistency. In layer two, one more script program will categorize the data according to the organization policy and splits the data using the unique identifier of log and sends it to the database. In layer three, web utility programs are used for querying and generating the customized reports.

Log meta data analysis provides a dedicated section for log data search, where the e-mail maillog, server / router /switches messages, web access / secure log data stored in database are searched and network anomalies or events like mis-configurations, viruses, unauthorized access, applications errors, etc., are detected.

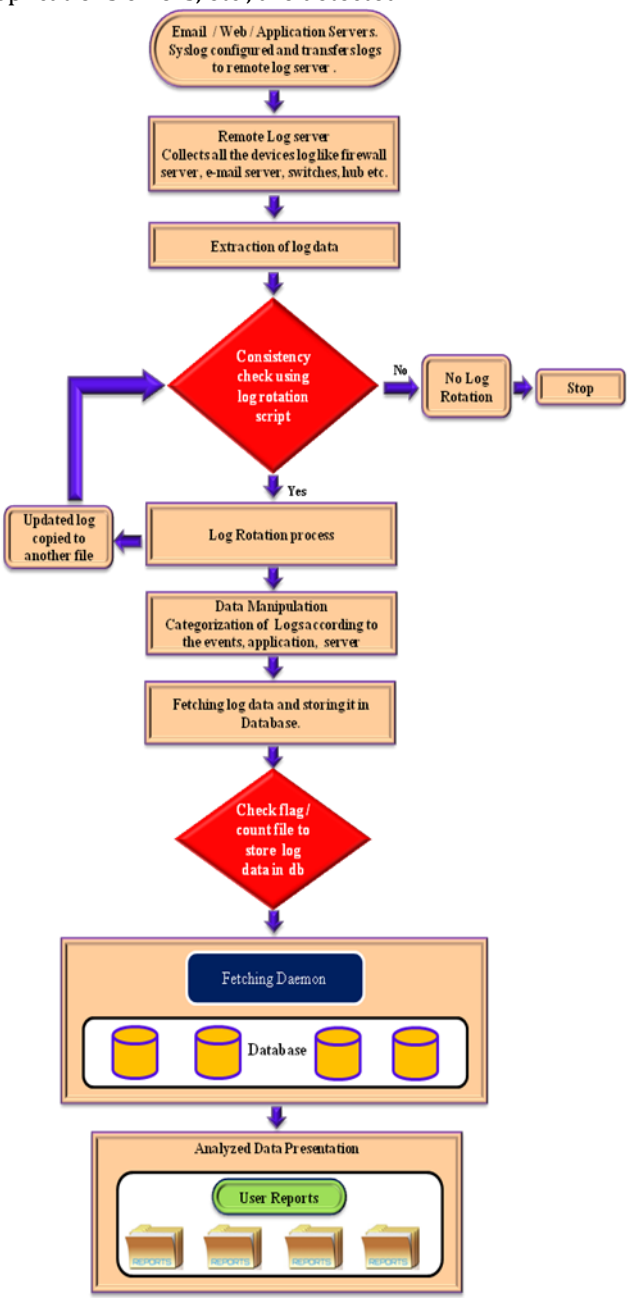

Fig-5: Log data analysis and management software architecture

8. REPORT GENERATION

The raw data collected from all the servers is converted into meaningful log data according to the organization's event management. This log data can be filtered based on various criteria and the reports can be scheduled as and when required. The log analysis software offers highly

flexible custom reports like Internet user activities, intranet e-mail statistics, internet e-mail statistics, spam / virus mail statistics, web access report, event severity, event category and alert trend, current and historical hourly and weekly reports etc.,

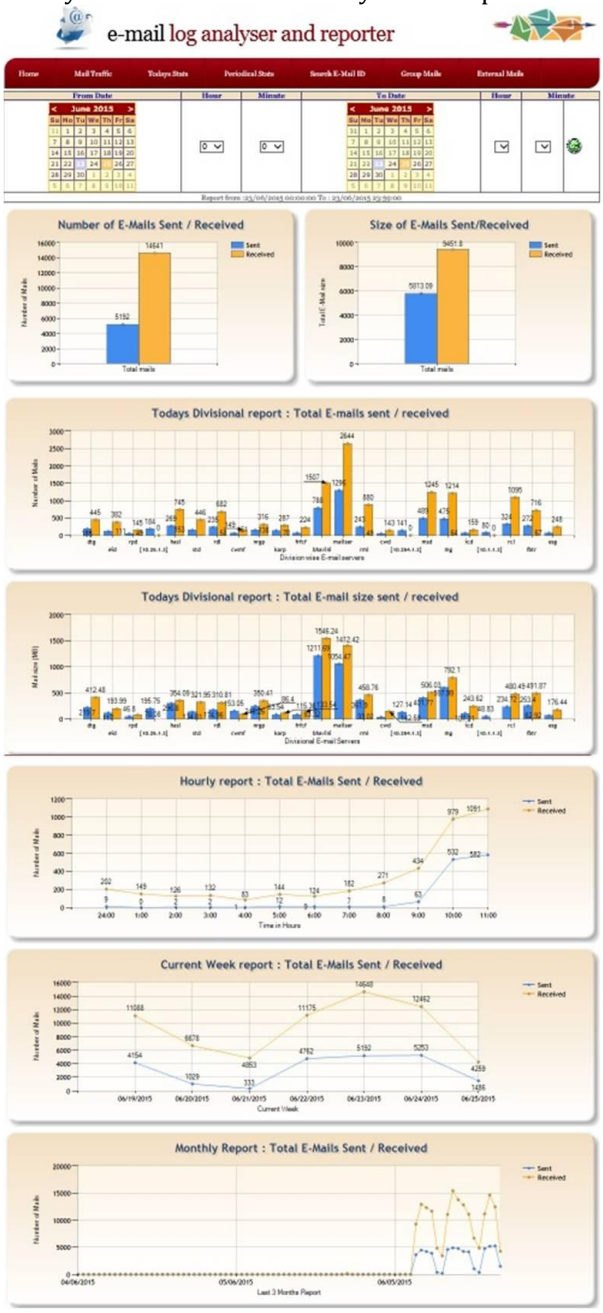

Fig – 6: Report generated using in-house developed e-mail log analysis software

Reports are displayed in both graph and table formats, reports can be configured for working and non-working hours, Reports can be filtered for individual severity and category. The figure (Fig-6) shows the report generated against the requirement of IT Manager / system administrator for e-mail server:

Same kind of reports can be generated for Web servers, proxy servers, firewall servers, etc., The raw data of all the servers thereby classified and demystified using the indigenous, in-house developed software solution. This helps the administrator to monitor all the internet / intranet user activities and generate reports by sitting in a centralized location.

9. CONCLUSION

Organizations need to monitor all the activities happening in their network and accesses to sensitive data, regardless of their security policy imposed. Sensitive data resides on core applications such as web applications / e-mail should be monitored primarily through the analysis of the logs. These data are highly complex and adherence to compliance mandates requires a robust log analysis solution that can accommodate the speed and complexity of these sources for immediate alerting as well as long-term reporting. Thus the efficient event log analysis or syslog analysis solves the data management problems, reduces system downtime, increases network performance, and helps tighten security policies of the enterprise.

REFERENCES

[1] *E-Mail auditing, logging and reporting,* White paper – Sendmail Inc, 2007
[2] *E-Mail Data-Mining: An Approach to construct an Organization position-wise structure while performing E-Mail Analysis*, Bhargav vadher, San Jose State University, 1-1-2010
[3] *National Institute of standards and technology*, ITL Bulletin, U.S. Department of Commerce, January, N2003
[4] *SANS Institute Info Sec Reading Room, Log Analyzer for Dummies*, December 10, 2007
[5] *Log message classification with syslog-ng*, www.balabit.com, *18, January, 2011*
[6] *Understanding Syslog: Servers, Messages & Security*, AaronLeskiw,http://www.Networkmanagement software.com, 2011
[7] *Kaspersky-Web-Mail-Server-Best-Practice-Guide*, Kaspersky Lab ZAO, 2012
[8] *SANS Information System Audit Logging Requirements* (2006)
[9] *NIST Information System Audit Logging Requirements* (2006)
[10] *Distributed syslog architectures with syslog-ng Premium Edition* (2008)
[11] *Archiving For Linux / Unix Systems & Syslog Supported Devices*
[12] *Central Log Server – Why and How,* Cyber Diligence, July-September, 2013
[13] haradchhetri.com/2014/03/01/install-and-

configure-rsyslog-on-rhel-6-centos-6/

BIOGRAPHIES

R.Anusooya received her B.E Degree from Madras University, T.N in 1997. She joined in Indira Gandhi Centre for Atomic Research (IGCAR) in 2001. She did her M.Tech in Sathyabama University in 2013. She is currently a Scientific Officer-E in Electronics, Instrumentation and Radiological Safety Group-IGCAR. She has 8 Journal Publications / Conference Papers and 10 Internal Design Reports.

J. Rajan did his B.E. (ECE) from Madras University (1992) & M.S (Software Systems) from BITS, Pilani (1999). He joined Computer Division, Indira Gandhi Centre for Atomic Research in 1999. He is presently functioning as the head of Networking Section (Computer Division) of Indira Gandhi Centre for Atomic Research. He is specialized in the areas of Computer Networks, Information Security and 3D Visualization.

S.A.V Satya Murty received his BTech Degree from Jawaharlal Nehru Technological University, A.P in 1977. Later, he joined one year orientation course in Nuclear Science & Engineering (21st Batch) at Bhaba Atomic Research Centre,Mumbai and then he joined in Indira Gandhi Centre for Atomic Research (IGCAR) in 1978. He is currently an Outstanding Scientist, Director of Electronics, Instrumentation and Radiological Safety Group-IGCAR. He has 110 Journal Publications / Conference Papers, 40 Internal Design Reports and edited two International Conference Proceedings.

