ISSN No. 0976-5697

Volume 3, No. 3, May-June 2012

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Syslog a Promising Solution to Log Management

P. K. Sahoo*
Professor, Department of Computer Science and Engineering, Visvesvaraya College of Engineering and Technology, Ibrahimpatnam, Hyderabad-501510, India
s_pks@yahoo.com

Dr. R. K. Chottray
Professor, Department of Computer Science and Engineering, National Institute of Technology, Rourkela, Odisha- 769008, India
rkc_ray@rediffmail.com

Dr. Gunamani Jena
Professor and Head, Department of Computer Science and Engineering, BVCEC (JNTUK), A. P. -533210, India
drgjena@ieee.org

Dr. S. Pattnaiak
Professor, P. G .Department of Information & Communication Technology, Fakir Mohan University, Vyasa Vihar, Balasore, Odisha-756019, India
spattnaik40@yahoo.co.in

Abstract: Log data are very useful in the changing scenario as it contains information related to types of events/attacks occurring within an organizations network. Log data are also very useful to track the history of an intruder's activity in day-to-day work and providing evidence to investigate malicious activity. Hence log files, which are most significant for cyber security investigation, should be stored in a secured place so that intruders will not be able to alter or erase log files. In order to protect the log data from breaches of their confidentiality and integrity log management is required in almost all enterprises. Windows event log has too many limitations, which becomes the biggest challenge in the process of log management. One of the limitations of windows event log is that, it is incapable of handling of messages from network devices such as routers and switches. Also there are no native window tools available to facilitate the centralization of logging process from different log sources in an organization where as Syslog offers very efficient solution to centralize the logging function. The proposed solution strongly recommends using syslog for the log management process. The proposed architectural model is very efficient to capture log data from anywhere in an organizations networks. The solution proposed here greatly simplifies the process of log storage and analysis by centralizing the logging process from all the devices present in the network and also provide a secured storage for the log data. The proposed model also makes it possible for Windows event log to be compatible with the logging function of other operating system.

Keywords: Syslog, Audit logs, Cyber security, Windows Event logs, Log management.

I. INTRODUCTION

Computer security logs are very useful, as security device log that trace possible attacks from the attackers and records day-to-day activity of the system users. A log is an evidence of, what events occurring in an organization and networks? In most of companies or organizations, logs play an important role in information security [1]. Logs are one of the most fundamental resources to any security professional. It is widely recognized by the government and industry that it is both beneficial and desirable to share logs for the purpose of security research [2]. Today log traces are widely used to identify and prevent violations of corporate information systems [3]. It is important to maintain Internet security system during and after the occurrences to collect evidence and forensics essences by various devices, such as hard disks, system logs, firewall, IDS log, processes as well as Internet connections [4]. Logs are composed of log entries; each entry contains information related to a specific event that has occurred within a system or network.

Originally, logs were used primarily for troubleshooting problems, but logs now serve many functions within most organizations, such as optimizing system and network performance, recording the actions of users and providing data useful for investigating malicious activity. Logs have evolved to contain information related to many different types of events occurring within networks and systems. Common examples of these computer security logs are audit logs that contain descriptions of notable events such as crashes of system programs, system resource exhaustion, failed login attempts, etc. and security device logs that records possible attacks. Computer security logs offer an endless well of valuable information about systems, networks, and applications. Through logs, audit records, and alerts information systems often give signs that something is broken or will be broken soon.

They can also reveal larger weaknesses that might affect regulatory compliance and even corporate governance. Many of these events are critical for post-mortem analysis after a break-in. At the very highest level, logs are a vehicle of accountability. Audit logs which are being considered as one of the most important parts of modern computer systems, provides information about the current and past states of systems [5]. Event logging and event logs play an important role in modern IT systems. Today, many applications, operating systems, network devices, and other system components are able to log their events to a local or remote log server. For this reason, event logs are an excellent source for determining the health status of the system. An audit log is the simplest, yet also one of the most effective forms of tracking temporal information. The idea is that any time something significant happens we write some record indicating, what happened and when it happened [6]. Log-files are important sources of forensic information because they usually connect a certain event to a particular point in time [7]. Logs from firewalls, intrusion detection systems and proxy server logs should be monitored periodically to protect from infections [8]. The log management refers to the process for generating, transmitting, storing, analyzing and disposing of computer

security log data. Log management is essential to ensure that the computer security records are stored in sufficient detail for an appropriate period of time [9]. Hence log management is very essential for any organization, as it is a helping hand to combat cyber security by protecting the log files from the attackers, who are trying to alter/erase the log files in order to wipe out evidence of his trespass out of those files.

A. The Various sources of Log Data:

a. ***Security Software*** Most of the organizations use several types of network-based and host-based security software to detect malicious activity, protect systems and data. Accordingly, security software's are a major source of computer security log data.

b. ***Operating Systems*** Operating systems for servers, workstations, printers and networking devices (e.g., routers, switches) usually log a variety of information related to security.

c. ***Applications*** Most of the organizations depend on a variety of commercial off-the-shelf (COTS) applications, such as e-mail servers, Web servers, browsers, file servers and database servers. Many organizations also use various COTS or government off-the-shelf (GOTS) business applications such as supply chain management, financial management, procurement systems, enterprise resource planning, and customer relationship management. All these applications produce a variety of log data.

II. NEED FOR LOG MANAGEMENT

Log management refers to the process of generating, storing and analysis of the log data. As logs contain records of system and network security, they need to be protected from breaches of their confidentiality and integrity. For example, logs might intentionally or inadvertently capture sensitive information such as users' passwords and the content of e-mails. This raises security and privacy concerns involving both the individuals that review the logs and others that might be able to access the logs through authorized or unauthorized means. Logs that are secured improperly in storage or in transit might also be susceptible to intentional and unintentional alteration and destruction. This could cause a variety of impacts, including allowing malicious activities to go unnoticed and manipulating evidence to conceal the identity of a malicious party. Log management helps us to ensure that computer security records are stored in sufficient detail for an appropriate period of time. Routine log reviews and analysis are beneficial for identifying security incidents, policy violations, fraudulent activity and operational problems. Log data are also useful for performing auditing and forensic analysis, supporting the organization's internal investigations.

III. THE CHALLENGES IN LOG MANAGEMENT

There are so many challenges in the process of log management; one of these is balancing a limited amount of log management resources with an ever-increasing supply of log data. A single source may use many different formats for its log message content, so an analysis program would need to be familiar with each format and be able to extract the meaning of the data within the fields of each format. This problem becomes much more challenging when log messages are generated by many sources. It might not be feasible to understand the meaning of all messages, so analysis might be limited to keyword and pattern searches. The section below discusses some of the most common types of challenges in log management process.

A. Many Log Sources:

Logs are located on many hosts throughout the organization, necessitating log management to be performed throughout the organization. Also, a single log source can generate multiple logs—for example, an application storing authentication attempts in one log and network activity in another log.

B. Inconsistent Log Content:

Each log source records certain pieces of information in its log entries, such as host IP addresses and usernames. For efficiency, log sources often record only the pieces of information that they consider most important. This can make it difficult to link events recorded by different log sources because they may not have any common values recorded (e.g., source 1 records the source IP address but not the username, and source 2 records the username but not the source IP address). Each type of log source may also represent values differently; these differences may be slight, such as one date being in MMDDYYYY format and another being in MM-DD-YYYY format.

C. Inconsistent Timestamps:

Each host that generates logs typically references its internal clock when setting a timestamp for each log entry. If a host's clock is inaccurate, the timestamps in its logs will also be inaccurate. This can make analysis of logs more difficult, particularly when logs from multiple hosts are being analyzed.

IV. PROBLEMS IN LOG MANAGEMENT

Windows operating systems (Windows NT, 2000, XP) and applications produce audit data that are written to the windows event log in a binary format. The window event log is incapable of handling messages from network devices such as routers and firewalls and also not compatible with other operating system logging functions. The window event viewer application supports only basic functionality and is inadequate for monitoring audit log files for medium to large size network and also there are no native window tools available to facilitate the centralization of logging process. There is as well a lack of unanimously accepted logging process for all the log sources. Another limitation of windows event log is because of its distributed in nature and there are no native windows tools available to facilitate the centralization of logging process. Each event log resides locally in the host system and centralization of log files is not possible, which makes log management most difficult.

V. SYSLOG IS A DE-FACTO STANDARD

Syslog provides a simple framework for log entry generation, storage and transfer. Many log sources either use syslog as their native logging format or offer features that allow their logging formats can be converted to syslog

format. In syslog based logging infrastructure each log generator uses the same high-level format for its logs and the same basic mechanism for transferring its log entries to a syslog server running on another host. Syslog uses message priorities to determine which messages should be handled more quickly , such as forwarding higher-priority messages more quickly than lower-priority ones. However the priority does not affect which actions to be performed on each message. Syslog can be configured to handle log entries differently based on each message's facility and severity.

For example, it could forward severity 0 to kernel messages to a centralized server for further review and simply record all severity 7 messages without forwarding them. Syslog is intended to be very simple and each syslog message has only three parts. The first part specifies the facility and severity as numerical values. The second part of the message contains a timestamp and the hostname or IP address of the source of the log. The third part is the actual log message content. No standard fields are defined within the message content; it is intended to be human-readable and not easily machine-parse able. This provides very high flexibility for log generators, which can place whatever information they deemed to be important within the content field but it makes automated analysis of the log data very challenging. Some organizations design their syslog infrastructure so that similar types of messages are grouped together or assigned similar codes, which can make log analysis automation easier to perform. The Syslog protocol and message format are defined in RFC3164 and RFC 3195 which defines reliable delivery of syslog over TCP [10, 11]. The syslog file contains data that are useful to diagnosing system problems and security events.

VI. PROPOSED SOLUTION

The architectural model proposed below in figure 1 used to centralize the storage and interpretation of the logs of an organization's system or networks and to protect the logs from the attacker. Centralization of the interpretation of the logs, serves to protect critical audit data from attackers by removing it immediately from the host, on which it is generated. The first tier of this architecture contains the hosts that generate the log data. The Syslog Server receives the log files from the individual log generating hosts such as routers, Switches, and local servers. This research paper implements the Winsyslog as the central Syslog Server. The central server then writes the log data into the database as per the rules specified in the Winsyslog configuration. The Syslog Server receives Syslog messages, processes them via the rule base and stores them in a database. Then the log files are stored separately on a data base server (Central Storage) for a period of time. Each host generating logs uses the same standard log format and forwards its log files to the Centralized storage. All UNIX-Based operating system have implementation of the Syslog protocol, which facilitates the centralized remote collection of Log messages from network devices and workstations whereas Windows can be configured to implement Syslog protocol.

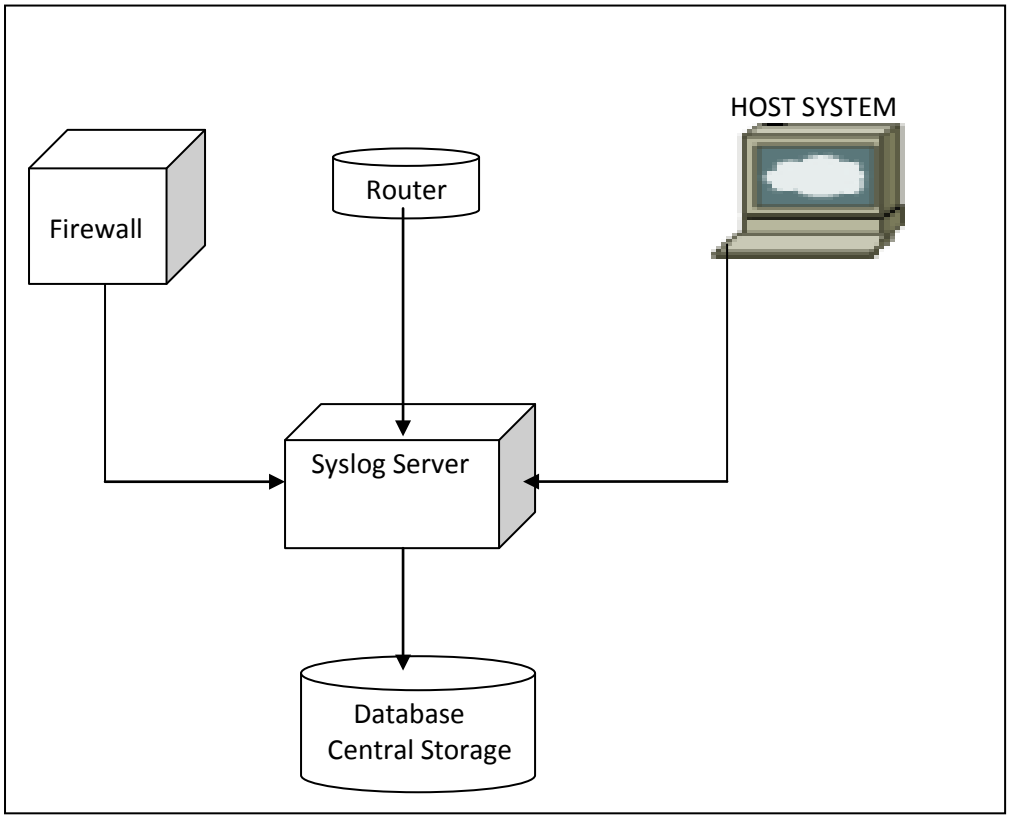

Figure: 1 shows the Architectural diagram of the proposed work

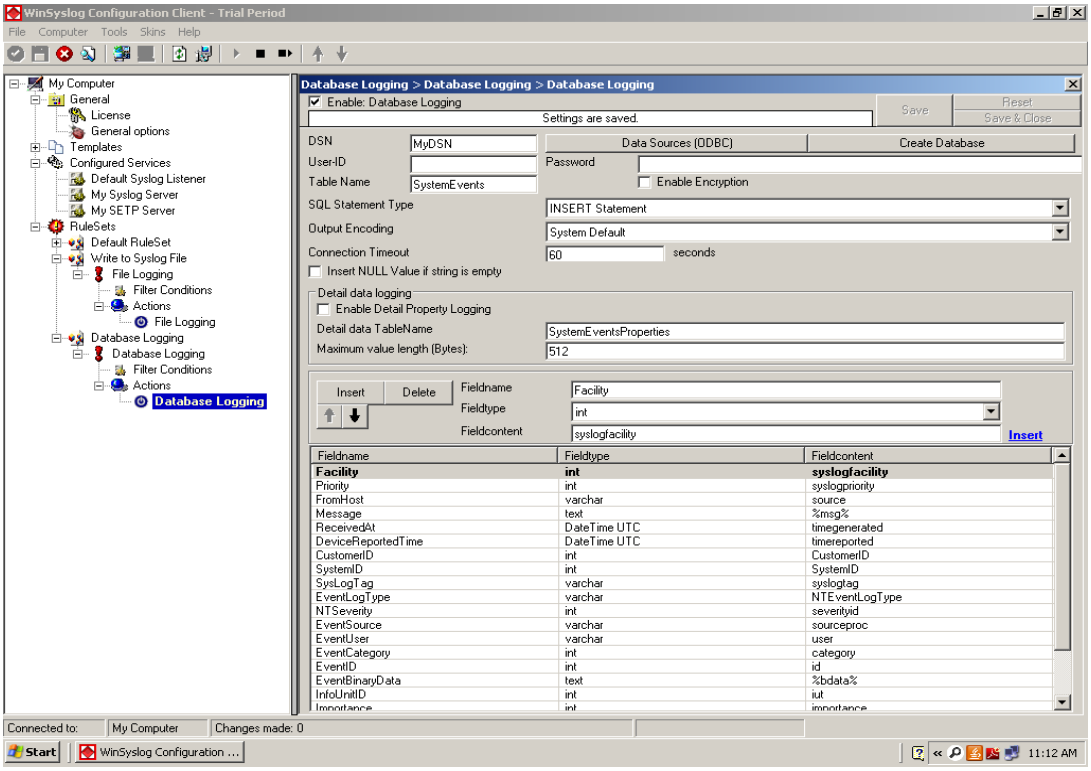

Figure 2: shows the Winsyslog configuration for the database logging rule set.

The above figure shows that Winsyslog configuration for the database logging rule set to send the data collected by the Syslog Server to the database.

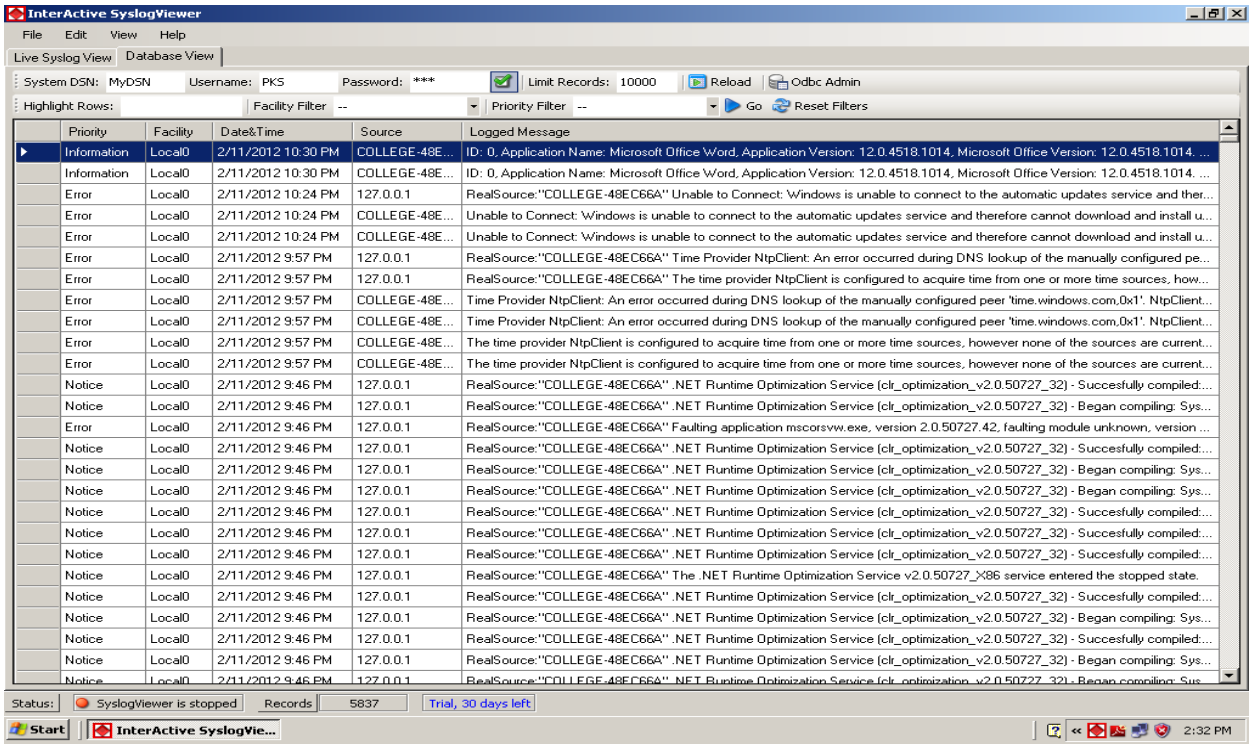

Fig 3: shows the interactive syslog viewer showing the syslog messages stored in the database.

This work have implemeted the Syslog Server to collect and store the log data for our institution campus network. The figure 3 shown above is the log data of our institution campus stored in the database.

A. Advantages of the Proposed Model:

a. Events which are collected from different log sources remain on the central storage for a period of time, even if the sending system fails or the logs on it are accidentally erased.

b. Access to all the events or logs can be provided through a single and central interface.

c. The central storage provides a secure and forensically sound storage for the log files, where it is far difficult for an attacker to alter or destroy log files.

d. Centralized logging using the Syslog protocol makes it possible to collect log files from almost all log generating devices present within the network, thus greatly simplify the process of log management.
e. Log data can be stored on the central storage in an encrypted form.

VII. CONCLUSION

As log data are very critical in the modern information systems, they need to be stored securely. Audit log data provides information about the current and past states of a system are being considered as one of the most important component of the cyber security. Log management is necessitated to ensure that log files are stored securely for an appropriate period of time to enable further investigations. The proposed architectural model is very efficient by centralizing the storage of log data from the various log sources in an organizations network. The architecture proposed here can be used to collect and centralize messages for an entire network including windows, UNIX hosts, printer and routers etc. The use of Syslog makes log management very easy and efficient by providing a simple framework for log generation and storage. The distributed nature of windows event log is easily overcome in the proposed solution. This model can be easily extended to other networks also in the future.

VIII. REFERENCES

[1]. Ya-Ting Fan, Shiuh-Jeng Wang, "Intrusion Investigations with Data-Hiding for Computer Log-File Forensics", Proceedings of the IEEE 5th International Conference on Future Information Technology (FUTURETECH 2010), IEEE Press, May 2010, pp. 1-6, doi:10.1109/FUTURETECH.2010.5482741.

[2]. Slagell A., Yurcik W., "Sharing computer network logs for security and privacy: a motivation for new methodologies of anonymization", Proceedings of the IEEE 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks (SECCMW 2005), IEEE Press, September 2005, pp. 80-89, doi: 10.1109/SECCMW.2005.1588299.

[3]. Forte, D.V., Maruti, C.; Vetturi, M.R. and Zambelli, M. "SecSyslog: an approach to secure logging based on covert channels", Proceedings of the IEEE 1st International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE 2005), IEEE Press, November 2005, pp. 248-263,doi: 10.1109/SADFE.2005.21.

[4]. I-Long Lin, Hong-Cheng Yang, Guo-Long Gu and Lin, A.C., "A study of information and communication security forensic technology capability in Taiwan", Proceedings of the 37th Annual IEEE International Carnahan Conference on Security Technology (CCST 2003), IEEE Press, October 2003,pp. 386-393, doi: 10.1109/ CCST. 2003. 1297591.

[5]. Attila Altay Yavuz, Peng Ning, "BAF: An Efficient Publicly Verifiable Secure Audit Logging Scheme for Distributed Systems", Annual IEEE Computer Security Applications Conferences (ACSAC 2009), IEEE Press, Issue ii, 2009, pp. 219-228, doi**:** 10.1109/ACSAC.2009.28.

[6]. Mihir Bellare, Bennet S. Yee, "Forward Integrity for Secure Audit Logs", IEEE Transactions on Information and Systems Security (TISC 1997), November 23, 1997, **doi:** 10.1.1.28.7970.

[7]. Gunnar Peterson, Deborah A. Frincke, "logging in the Age of Web Services", CO Published by the IEEE Computer and reliability Societies, 1540-7993/09, June 2009, http://www.arctecgroup.net/pdf/82-85.pdf

[8]. "Current Malware Threats and Mitigation Strategies", US-CERT Informational Whitepaper, Multi-State Information Sharing and Analysis Center and United States Computer Emergency Readiness Team, May 16, 2005.

[9]. Erika McCallister, Tim Grance, Karen Scarfone," Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)", National Institute of Standards and Technology Special Publication 800-122(Draft), 58 pages, January 2009.

[10]. C. Lonvick, "The BSD syslog Protocol", Network Working Group, Cisco Systems, Request for Comments: 3164, August 2001.

[11]. D. new and M. Rose, "Reliable Delivery for syslog", Network Working Group, Dover Beach Consulting, Inc., Request for Comments: 3195, November 2001.

[12]. Kaveesh Dashora, Deepak Singh Tomar and J.L. Rana, "A Practical Approach for Evidence Gathering in Windows Environment", International Journal of Computer Applications (0975 – 8887), Volume 5– No.10, August 2010, pp. 21-27.

