TESIS^APPROVAL STATUS FORM

JUDUL: CENTRALIZED LOG FOR SYSLOG SERVER

SESI PENGAJIAN: 2005/2006

Saya NORAZLINI BINTI JAMALUDIN
(HURUF BESAR)

mengaku membenarkan tesis (PSM/Sarjana/Doktor Falsafah) ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dengan syarat-syarat kegunaan seperti berikut:

1. Tesis adalah hakmilik Kolej Universiti Teknikal Kebangsaan Malaysia.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. ** Sila tandakan (/)

_____ SULIT (Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)

_____ TERHAD (Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)

_____ TIDAK TERHAD

(TANDATANGAN PENULIS)

Alamat tetap : 32, Felda Gunung Bongsu,
09700 Kulim, Kedah

Tarikh : 21 NOVEMBER 2006

(TANDATANGAN PENYELIA)

Pn.Wahidah Binti Md. Shah
Nama Penyelia

Tarikh : 21 NOVEMBER 2006

CATATAN: ** Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.
^ Tesis dimaksudkan sebagai Laporan Projek Sarjana Muda (PSM)

CENTRALIZED LOG FOR SYSLOG SERVER

NORAZLINI BINTI JAMALUDIN

This report is submitted in partial fulfillment of the requirement for the Bachelor of Computer Science (Computer Network)

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
KOLEJ UNIVERSITI TEKNIKAL KEBANGSAAN MALAYSIA
2006

DECLARATION

I hereby declare that this project report entitled

CENTRALIZED LOG FOR SYSLOG SERVER

is written by me and is my own effort and that no part has been plagiarized without citations.

STUDENT : _____ Date : _____
(NORAZLINI BINTI JAMALUDIN)

SUPERVISOR : _____ Date : _____
(PUAN WAHIDAH BINTI MD. SHAH)

DEDICATION

To my beloved Parent

Whose boundles love and support replenishes and enriches my soul

ACKNOWLEDGEMENT

I would like to this opportunity to personally express my deepest appreciation and gratitude. The completion of this project would be impossible without the help of these people. It gives me a great pleasure in completing this project.

First and foremost, I would like to gratitude my sincere appreciation to my Supervisor, Mrs. Wahidah Binti Md Shah for her concerns, time, advice, guidance and supervision throughout the progress of the project. Her invaluable and suggestion is much appreciated.

Last but not least, I would like to acknowledge to my family, friends for their support and trust.

ABSTRACT

The title of this thesis is "Centralized log For Syslog Server (CLSS)". The main purpose of CLSS system is easy for administrator to solve the problem about client. This system is easy for administrator to know about all log names at this system. The log names for this system are application, system and security. This system involves administrator and many clients. Only system administrator can view all client log record. This system is easy for administrator to read all log record for client. This system is easy for administrator to view all log events in all client. System administrator can set filter followed date, event source and category. Administrator can view all information about example of source that have in this system. As for a conclusion, hope this project will help to improve the knowledge of the network system. Finally, hope this system will give a benefit to all people.

ABSTRAK

Tesis yang bertajuk "Centralized Log for Syslog Server (CLSS)" ini adalah bertujuan untuk memudahkan pelayan mengenal pasti masalah yang berkaitan dengan yang dihadapi oleh pelayan. Sistem ini memudahkan pelayan mengatahui segala nama log yang terdapat di dalam sistem ini. Antaranya ialah aplikasi, sistem dan sekuriti. Sistem ini melibatkan pelayan sistem dan banyak pelayan. Hanya pelayan sistem sahaja yang boleh melihat segala rekod log yang terdapat di dalam setiap pelayan. Pelayan sistem juga dapat mengetahui jumlah rekod log yang terdapat di dalam setiap pelayan. Sistem ini juga dapat mengatahui jenis peristiwa yang terdapat setiap pelayan. Pelayan sistem juga boleh set penjaring mengikut tarikh, sumber peristiwa dan kategori. Pelayan sistem juga melihat segala maklumat lengkap mengenai contoh sumber yang terdapat di dalam sistem ini. Kesimpulannya, diharapkan projek ini dapat membantu dalam meningkatkan lagi pengetahuan mengenai sistem rangkaian. Disamping itu juga adalah diharapkan agar cadangan kajian ini dapat memberi manfaat kepada semua pihak.

LIST OF TABLES

LIST OF FIGURE

LIST OF ABBREVIATIONS

UDP	-	User Datagram Protocol
SNMP	-	Simple Network Management Protocol
IP	-	Internet Protocol
TCP	-	Transmission Control Protocol
API	-	Application Programming Interface
SIP	-	Session Initiation Protocol
SQL	-	Structured Query Language
RAD	-	Rapid Application Development
IT	-	Information Technology
LAN	-	Local Area Network
JSP	-	Java Server Pages
PHP	-	Personal Home Page
XML	-	Extensible Markup Language
HTML	-	Hyper Text Markup Language
ASP	-	Active Server Pages
GPL	-	General Public License
DBMS	-	Database Management System
NIC	-	Network Interface Card
PSMI	-	Projek Sarajana Muda I
PSM II	-	Projek Sarjana Muda II
ODBC	-	Open Database Connectivity
SNMP	-	Simple Network Management Protocol
DNS	-	Domain Name Server
SMS	-	Short Message Service
CLSS	-	Centralized Log for Syslog Server
PRI	-	Public Radio International

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION

1.1 Project Background

Syslog was developed by Eric Allman as a part of the Sendmail project. In 1980, it was used and designed for Sendmail only. Syslog was not standardized until recently. A formal specification and standardization of message content and transport layer mechanisms is scheduler for 2005.

Syslog Server listens for incoming Syslog messages on UDP port 514 and decodes the messages for logging purposes. This system can filter IP Address ranges or classes, message content string or pattern matching, severity and facilities, time of day – day of week, trigger threshold and easy to any user defined rule. SysLog system is a new application is very functional providing real-time alerting, filtering and management of SysLog messages. It provides a centralized, securely stored log of all devices on network, whatever platform that run on. SysLog also incorporates a host of powerful features, including filtering based on message content, as well as customizable data mining and analysis capabilities.

System logs is very important for the continue health in the system. It provides a standard location to find errors, information, debug messages, and alerts. Syslog can be used for diagnosis in order to prevent problems, and a valuable resource for troubleshooting. Syslog system logger has flexibility, simplicity and

security. The Syslog protocol is a very simplistic protocol. The Syslog sender sends a small textual message (less than 1024 bytes) to the Syslog receiver.

1.2 Problem Statement

In LAN, current centralized log for syslog server system has a fully facilities for network administrator include with centralized all log, view all log and many features are provided. It so complicated to build up the application like that even thought it is not suitable with the project scope.

Problem of the currently centralized log for syslog server system:-

i. All syslog server software is trial software. After 30 days trial, user need update the software licensed. So it make difficult for user to use this software.
ii. Network administrator also cannot centralize what the application, system and security running by server and client. It so hard to isolate the server and client activities.
iii. Admin do not know what are the user log activities in the network.
iv. Without the systems, Administrator cannot show the computer status as error in the graphical.

1.3 Objective

The main objective of this project is to overcome the problem above and to show the detail network problem. The objectives of the project are:

- **To develop a new system for Centralized Log for Syslog Server.**

  Centralized Log for Syslog Server system has many tools to view all server information. That system has are databases, alarms, SNMP and agents. In this tools are easy to all users to view all information about centralized log.

- **To compare all Syslog server open source and try to solve a problem in open source and change a new system.**

  As a technology arising, trial software is a very difficult to our user because user need to update the open source licensed of software. So, a new system to support Syslog Server is needed.

- **To make easier for administrator to monitor critical messages.**

  In this system, it is easy for server to monitor critical messages. It means that user can view all server information and try to solve that problem. In this Syglog Server system can view record in databases.

1.4 Scope

Centralized log for Syslog server is to make an administrators life easier by centralizing the logs from other servers on the network. Administrator can view all information about log, archival and compliance can be addressed easily from one repository. All logs in server can be monitored for critical (or warning or whatever) messages. If necessary a policy can be put in place to archive the logs for a set time period, possibly for compliance reasons.

In this system, five Syslog servers are important to view all log information, security and system. All servers have different record information to view. Time schedule is very important to all servers for pass all log to centralized log in any time.

Syslog server platform is a Microsoft Windows 2003 Server. In this system, three items are connected via log statements allowing for multiple message paths. Sources are the log information comes from, destinations are where it goes. Filters are used to filter messages on their path through the logging system.

1.5 Project Significance

Centralized log for Syslog Server (CLSS) eases the work of every network administrator. It is a real Syslog Server tool used to centralized, secure stored log of platform that run on. Syslog Server also incorporates a host of powerful features, including filtering based on message content, as well as customizable data mining and analysis capabilities.

This system are very important because it can filter IP Address ranges or classes, message content string or pattern matching, severity and facilities, time of day, trigger threshold and easy to admin defined rule. SysLog system is a new application is very functional providing real-time filtering, view log and management of SysLog messages.

The whole system can be viewed as a combined structure with important process. Centralized log application also presents the real-time alerting, filtering and management. This feature provides a more user friendly interface to centralized log and understands the situation of the Syslog server.

1.6 Expected Output

At the final project stage of this project, centralized log is a once of a Syslog server. Syslog server is a part of a network. An alarm is a very important to admin to compare messages with alarm definition, generate alarm if the message matches an alarm definition.

1.6.1 Filter Rules

Filter rules are sets of filters gathered in a filter list. Each rule in the list is sequentially processed from top to bottom. A rule contains conditions and actions.

Possible conditions are:

i) IP source and mask of the Syslog message sender. Syslog can filter a single host or hosts pertaining to an IP network or sub-network.

ii) The facility type of the Syslog message. 23 are defined by the RFC3164. The level of the message that helps to classify its severity.

iii) A first and second character string found anywhere or at a specified offset in the Syslog message body.

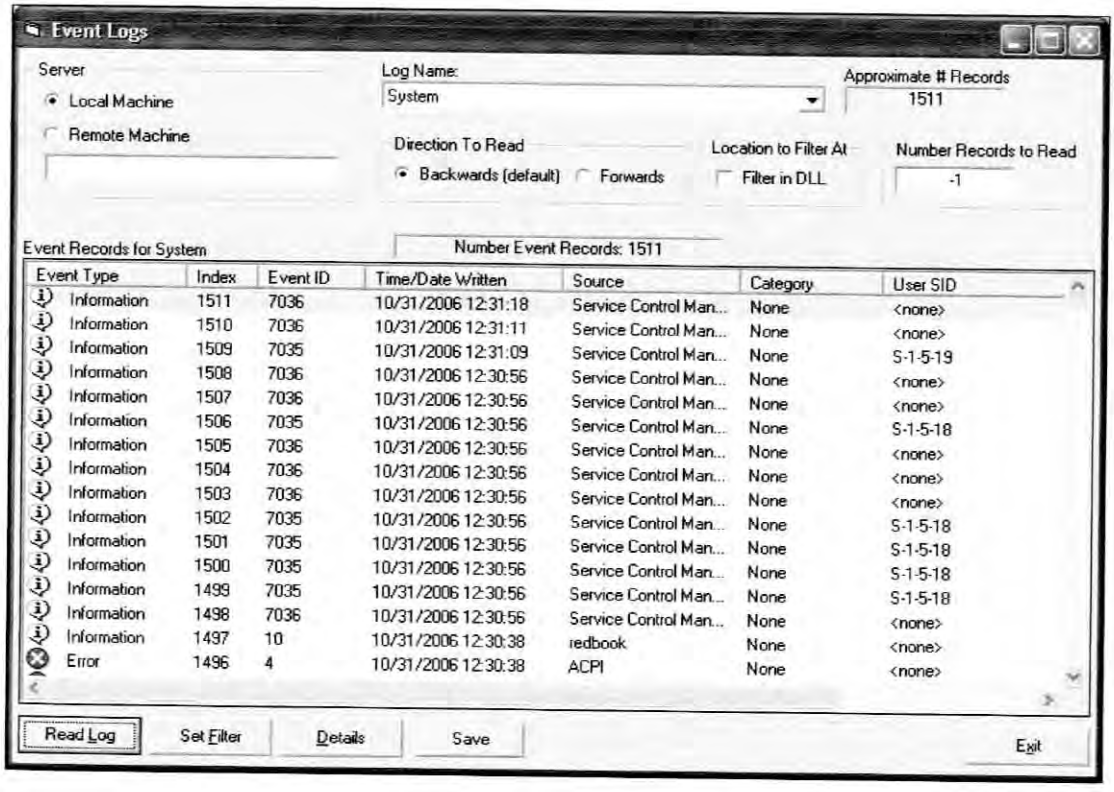

Figure 1.1: Filter Editor

1.6.2 Time Alert

Time alert is to send alerts to multiple people based on schedules for each individual. In this way, it can tell what people are responsible for various servers and

let it alert as appropriate based on server schedule of availability. To use team alert person and team entries must be setting to define who should be alerted and when.

1.6.3 Event Alarm

Event Alarm is to work with syslog messages in two different ways. Event Alarm can send notifications to a central syslog server (central syslog server can perform further actions or analysis). Event Alarm can also receive messages from other syslog devices through network, redirecting those messages into the Application log where Event Alarm is running.

1.7 Conclusion

This project has presented the approach to centralized log in a real-time system. Network topology information is obtained from network hardware specification, and centralized of server using User Datagram Protocol (UDP).

The next chapter will be carried out according to the literature researches that have been conducted. It also discuss about the chapter II.

CHAPTER II

LITERATURE REVIEW & PROJECT METHODOLOGY

2.1 Introduction

The literature review will help for research and fact finding. It also to identify the mission of project and provides consistency. This information is very important to determine a real time network and functional requirement for this project. Theories and concept that are related to the project development are also being studied here.

2.2 Fact and Finding

This section will discuss on the fact finding techniques that have been adopted to gather relevant information to be use in project development. The significance and contribution of conducting research on the related survey areas are also outlined.

2.2.1 Syslog Wikipedia

Syslog is a de facto standard for forwarding log messages in an IP network. The term "syslog" is often used for both the actual syslog protocol, as well as the application or library sending syslog messages. The syslog protocol is a very simplistic protocol: the syslog sender sends a small textual message (less than 1024 bytes) to the syslog receiver. The receiver is commonly called "syslogd", "syslog daemon" or "syslog server". Syslog messages can be sent via UDP and/or TCP. Often times the data is sent in cleartext, however, Stunnel can be used to provide for a layer of encryption through SSL/TLS.

Syslog is typically used for computer system management and security auditing. While it has a number of shortcomings, its big plus is that syslog is supported by a wide variety of devices and receivers. Because of this, syslog can be used to integrate log data from many different types of systems into a central repository.

2.2.2 Network Security Journal

2.2.2.1 System Analyzer is Network Administrator

According to an Earl Greer and Vincil Bishop (2005), said that the analyzer goes beyond packet-level details about network occurrences and correlates events that would otherwise be missed because they occur across network devices of disparate types and locations. Although the analyzer can give an impressive level of detail, provided that the details are reported to the syslog server, it does not replace the reporting functions of your firewall or intrusion-detection system.