UNIVERSITI TEKNOLOGI MARA

THE DEVELOPMENT OF A STREAMING LOG ANALYSIS AND REPORTING TOOLS

MOHAMED FAZLI BIN MOHAMED ZINI

Thesis submitted in fulfillment of the requirements

for the degree of

Master of Science (Computer Networking)

Faculty of Information Technology and Quantitative Sciences

NOVEMBER 2008

Acknowledgement

A big gratefulness to Allah S.W.T for giving me the willingness, strength and knowledge.

Endless love for my parents, En. Mohamed Zini Saleh and Pn Sakinah Hashim, my wife, Hajariah Yacob, and my sons Adam and Arsyad. Thank you for all your love and endless support.

I would like to express my sincere gratitude to my supervisor En Farok bin Hj Azmat for his continuous support and guidance in completing this dissertation.

To all classmates CS778 batch 3, thanks for all the support, the knowledge that shared and experience that we have been through together. I am greatly indebted to all of you, lecturers and friends.

Wassalam.

Abstract

Log is one of the most important information in system and information technology industry. As from logs, administrators, management, engineers and customers could trace the performance of their system, health of their system and provide them lot of information and assist them to make decision. Some of the log that produce by system is in a raw format, and some of it are unreadable and cannot be understood. A tool is needed to translate analysis and report all of those logs. In this dissertation, a tool that specifically for streaming log produce by an appliance called NetCache, a streaming accelerator appliance, is study and developed. The whole architecture and design are proposed to support the live streaming architecture and also to support the tool itself.

This tool contains eight scripts and each script which was developed using Perl, has its own task in this tool. Systatstation.pl script and Smstats-station.pl script are purposed to do logs collecting from the appliance. Sum-sysstat-station.pl is a script that mainly to summarize and generating report for live streaming active session. Streamstat-daily-bkj.pl and Streamstat-monthv2-bkj.pl is a script to analyze all the raw logs of active connection and the analyzed logs will be processed by Chan-rank.pl-byday-bkj and Chan-rank.pl-bymonth-bkj accordingly. These scripts will generate required daily and monthly report. Stream_region_report.pl script will convert all the analyzed logs into database and will generate report to determine source IP of session based on country. Finally, combinations of these scripts become a tool that used to analyzing streaming logs and generating reports subsequently.

Table of Content