KKU Engineering Journal

https://www.tci-thaijo.org/index.php/kkuenj/index

The software architecture of network management system based on elastics search technology

Natthakorn Chuaychoo, Thitaporn Rimdusit and Chanankorn Jandaeng*

Ubiquitous Networked Embedded System Laboratory (UbiNES), School of Informatics, Walailak University, Nakorn Sri Thamnarat, 80160, Thailand.

Received April 2016
Accepted June 2016

Abstract

The network monitoring system needs all data sources in order to monitors network service and system, resource capacity plan, statistics and accounting, fault management and performance; such as throughput, latency and round trip time. SNMP, audit log and network traffic are required for data analysis together. This paper present software architecture for network monitoring system that consists of data collection, data analysis and data visualization. The software architecture is implemented in web based application to evaluate this architecture.

Keywords: Network monitoring system, Elastic search

1. Introduction

Monitoring a network is importance to network management. A major function of network monitoring is an early identification of trend and pattern, in both network traffic and device. The network monitoring system (NMS) [1] monitors network service and system, resource capacity plan, statistics and accounting, fault management and performance; such as throughput, latency and round trip time. Furthermore, the network monitoring system supports the network under service level agreement (SLA) and network policy.

Walailak University is large organization that consist of 9,000 users, produce an enormous traffic data. Thus, NMS is vitally required for network administration. The system is expected to provide a realtime monitor network, notify the network status: alert via email and Short Message Service (SMS), quota usage of all user, daily, weekly and monthly report, and root cost for director.

There are varieties of network monitoring system: commercial, shareware, and freeware application. However, no system implemented all requirements in freeware and shareware version. Even thought, there are available in commercial version but all raw data are encrypted, which effects network administrator an inability to extend or implement some specific requirement. In addition, each application monitors and analyses the data from any data source such as audit log, traffic, or SNMP data, separately. Moreover, network monitoring needs data from total network in order to improve the accuracy of problem solving. The examples of network monitoring are shown in Table 1.

The table 1 shows that network monitoring system function consists of fault management, configuration management, performance management, accounting management, and security management. Data source comes from SNMP, audit log, and/or network traffic. Selected information are stored in databases such as MySQL and MongoDB. And most of NMS are web based application and notified via web.

This paper proposes the network monitoring system that supports 5 functions, NMS process and analyse data from SNMP, audit log and network traffic. All events are recorded and indexed by elastic search technology. The software architecture are shown and described in this paper. Its user interface are implemented in web based and mobile web application.

2. Materials and methods

2.1 Software architecture

The software architecture consist of three modules: data logger, data analysis and data visualization. The data logger collects all information from network devices and save in data base with Elastic Search technology. Whereas data visualization acts as user interface that retrieve data from Elastic Search database directly. Moreover user can access network data via web based and mobile web based application in term of analyzed data. The system architecture is show in Figure 1.

2.1.1 Data logger

The data logger collects raw data from network devices that be composed of three data sources: SNMP, audit log and packet traffic. The managed network devices are any

*Corresponding author. Tel.: +66 7567 2209
Email address: cjundang@gmail.com

doi: 10.14456/kkuenj.2016.146

Table1 Examples of Network Monitoring System

Application	*Functions*					*Data Source*			*Database*	*Platform*
	F	*C*	*P*	*A*	*S*	*SNMP*	*Audit Log*	*Traffic*		
Cati [2]	x		x			x		x	MySQL	Web
MRTG [3]	x		x			x		x	MySQL	Web
graylog [4]	x		x				x		MongoDB	Web
Nagios [5]	x		x					x	MySQL	Web
Capsa [6]	x		x					x	MySQL	Web

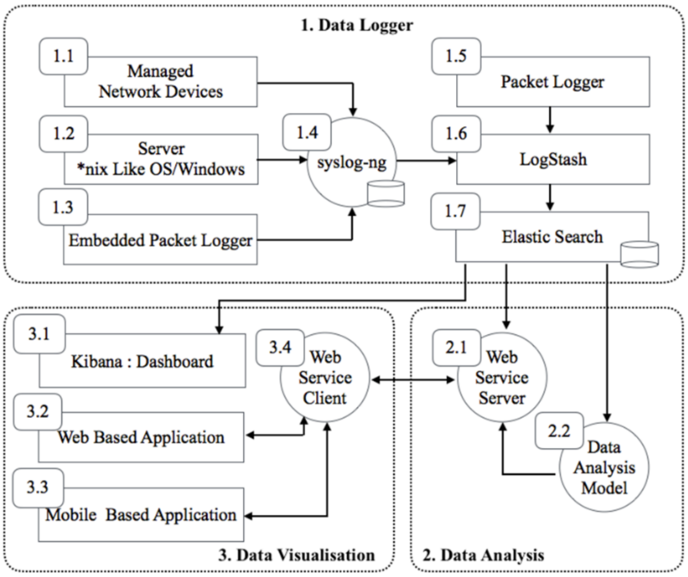

Figure 1 Software Architecture of Network Monitoring

network equipment that embedded network monitoring agent. SNMP is the traditional protocol that be founded in variety of commercial devices. Moreover some servers is installed and enabled SNMP agent in order to monitor their server. SNMP manager is implemented in module 1.1 of Figure 1. It query data from managed devices via SNMP-GET message, transform data from SNMP-DATA message to messages as JSON format and forward to central log server. The central log server is installed syslog-ng service.

All network devices such as firewall, core switch, distribution switch including WiFi access point that support syslog feature are enabled remote logging function. Then all log message are sent to central log via syslog-ng service as show in module 1.2 of Figure 1. In addition, each server platform support syslog-ng service. The syslog-ng is installed and configured in Unix Like-OS such as Linux and FreeBSD. For Microsoft Window Server, syslog service is enabled in version 2010 and later. On other hand, Microsoft Window Server that older than 2010 version sent log message via nxlog service. The nxlog service forwards message log via syslog-ng protocol.

Some network segment is implemented behind unmanaged devices. All traffic or network information are not monitored by administrator/network monitoring system. Example there are button neck problem occurs in some network segment and bring to users cannot access any network service. The packet sniffer is not implemented in rack container because of limitation of physical location. The embedded packet logger [7] (module 1.3 in Figure 1) is plugged into network devices as a packet logger and report statistical data in periodic time to syslog-ng service. The network administrator can collect network data with lightweight additional traffic.

For core switch, network administrator need some network traffic to monitor, account, evaluate network performance, or make network management plan. Network monitoring mode is enabled in core switch and forward to packet logger server. The raw traffic is translated to readable format and sent to syslog-ng.

The LogStash in module 1.6 is the main process is to collect data as messages from network devices and forward to Elastic Search services. All messages in log file are non-structor text that hard to process in next module. All messaged are pre-processed with Grok function of LogStash that result in log message are represented in JSON message.

In order to monitor itself, TopBeat is installed in NMS. This service monitors and collects performance of NSM like results from top command in Unix. All packets which forwarded via NMS is monitor with PacketBeats. The PacketBeat relies on libpcap library. Thus result of PacketBeat like other packet logger services such as tcpdump.

All messages from LogStash are represented in JSON format. All keys (filed) are indexed by Elastic Search. Thus

Elastic Search Service is the data broker and only one channel that other module can access. Data analysis and Data virtualization access data via REST web service.

2.1.2 Data analysis

The statistics method is selected for this module. Director of Computer Center and Network Administration needs daily, weekly, monthly and yearly report. These reports are top 10 users, protocol, destination, bandwidth usage and utilization etc.

Moreover, network administration needs user behavior tracking. Example, some course that registered was withdrawn by malicious user. Events were recorded in audit log but there were separated in to many logger server such as radius server, registration server and WiFi server. Network Administrator traced all events with command line. There are no any tools to support this function. This network monitoring system implements the function to link all behavior of user that distributed in each server into the central log server and analyze in the same time period.

Each function be implemented as web service causes extensibility of data analysis. Elastics Search database implements the indexing of column that bring to easily search and fast query via RESTful web service. Some functions are not implemented in this system in the first time. However, the extensibility is open for all network administrator to add new function or module via web service.

2.1.3 Data visualization

The network monitoring system is web based application. It support responsive web design that are shown in PC, Tablet and mobile. All requirement from network administrator are transformed to web service client as requestor and web service server as provider. Then the user interface is implemented with jQuery technology and Bootstrap that support asynchronous and responsive web design. Moreover, visualization in chart module such as bar chart, line chart, donut and table are implement with Kibana package.

3. Results

This software architecture is implemented and tested in laboratory. The testbed network are shown in Figure 2.

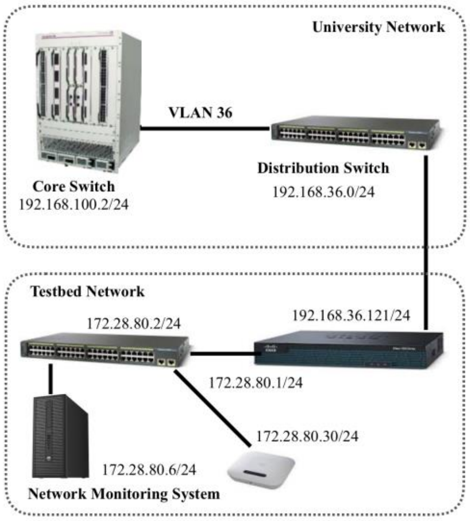

Figure 2 Testbed network

The Figure 2 show that there are two networks: university network and testbed network. This network monitoring system (NMS) monitors core switch and distribution switch that be managed switches. SNMP agent are embedded and enabled while syslog service is enabled. In addition, testbed network consists of CISCO network devices: router, switch and access point.

All modules is Figure 1 and web based application as user interface are implemented in NMS (172.28.80.6/24). The NMS server is Intel i5 processor, 16GB Main memory, 2TB Harddisk (7200 rpm) and 1 Fast Ethernet interface. The Examples of user interface are shown in Figure 3.

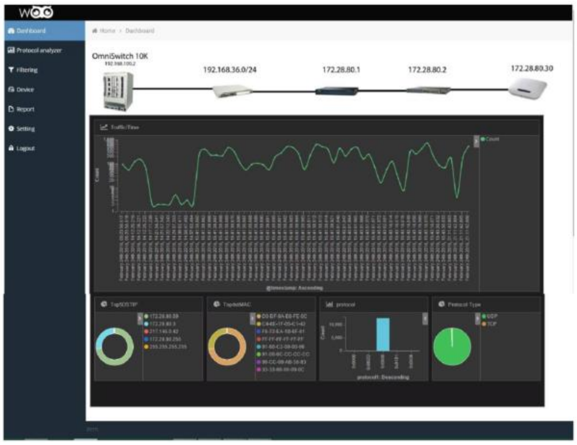

Figure 3 Dash board of network monitoring system

4. Discussion and conclusion

This is the first experimental test of network monitoring system based on Elastic Search. The software framework is implemented as web based application. This application show the statistic values of network traffic as summary value. The matching learning methodology such as data mining will be applied in data analysis for network prediction and user behavior analysis. More over it will bring to network security analysis from audit log of firewall and intrusion detection system.

5. Acknowledgement

This research is supported by Senior Project Supported Scholarship 2016 and Walailak University.

6. References

[1] Subramamian M, Timothy A, Gonsalves N, Rani U. Network Management: Principles and Practice. Dorling Kindersley, India: Peason Education Inc.; 2010.

[2] Cacti [Internet]. [cited 2016 January 15]. Available from: http://www.cacti.net/,

[3] MRTG [Internet]. [cited 2016 January 15]. Available from: http://oss.oetiker.ch/mrtg/doc/mrtg.en.html.

[4] Graylog. Open Source Log Management [Internet]. [cited 2016 January 15]. Available from: https://www.graylog.org.

[5] Nagios Open Source Project [Internet]. [cited 2016 January 15]. Available from: https://www.nagios.org/.

[6] Capsa [Internet]. [cited 2016 January 15]. Available from: www.colasoft.com/capsa/capsa/.

[7] Jandaeng C. Embedded Packet Logger for Network Monitoring System. 2015, The 2nd International Conference on Communication and Computer Engineering; 2015 Jun 9-11; Phuket, Thailand. Switzerland: Springer International Publishing; 2015. p. 1093-1102.