Design Log Management System of Computer Network Devices Infrastructures Based on ELK Stack

Adian F. Rochim
Department of Computer Engineering
Diponegoro University
Semarang 50275, Indonesia
adian@ce.undip.ac.id

Mukhlish A. Aziz
Department of Computer Engineering
Diponegoro University
Semarang 50275, Indonesia
aamukhlish@student.undip.ac.id

Adnan Fauzi
Department of Computer Engineering
Diponegoro University
Semarang 50275, Indonesia
adnan@live.undip.ac.id

***Abstract*—Device monitoring is an important thing to manage networks. Information-related network state or condition can be gathered through the device monitoring for administrators to take decisions regarding occurred events. Logs can be useful information to monitor network devices. Network administrator of Diponegoro University needs a centralized the logs, so that can receive, manage, and analyze logs. This research identifies functional requirements of the log management system. DSR Method was used to design topology and software of the log management system. The next step is implementation of the topology, software, and application. The last step is testing the system and log management application. The results show that collecting centralized logs and processing these logs into information in the form of dashboards using ELK Stack application successfully implemented. The dashboard resulted by ELK Stack Application will be implemented on the web application using PHP programming language and Code Igniter framework. The test results show that system can receive logs and group the log according to the device location and the severity level of the log.**

Keywords *— Monitoring; log; ELK Stack; PHP; Codeigniter; Dashboard*

I. INTRODUCTION

Information technology advancement nowadays provides new services for humane activities. This various of technology makes an easy way for human to implement information dissemination [1]. The ease of information dissemination today cannot be separated from the role of network administrators to manage network resources properly.

Computer networks are sets of interconnections between two or more autonomous computers that are connected by wired or wireless transmission media [2][3]. Network administrators are responsible for designing, configuring network devices, and maintaining traffic stability. Network devices, as objects managed by administrators, often experience problems. Each problem has a variety of causes, could be due to administrator faults, lack of documentation, or device exploitation by unauthorized parties. Each problem becomes an event from a network device that recorded in the system log (syslog).

Syslog is a way for network devices to send event messages to a logging server, usually known as a Syslog server. Understanding syslog is the most effective way to "hear" server messages to users [4]. The next problem is, on large computer networks, there are many devices and will make it difficult for network administrators to detect the source and cause of the problems on these network devices. So the centralize log was needed to ship the log of network devices, which is making a reporting system that is easily analyzed by network administrators. The system is called syslog management.

Our research used much software to develop the syslog management, i.e., ELK Stack or a combination of open source applications Elasticsearch, Logstash and Kibana to collect and visualize logs. Elasticsearch was used to store all logs originated from network devices; Logstash is an open-source software for collecting and parsing logs then save them at Elasticsearch. Kibana is a web interface that is useful for displaying logs in a graphical or other visualizations form [5].

In this research, author intends to implement a computer network devices syslog management and visualization system based on ELK Stack to integrate logs from network devices used by ICT Diponegoro University and visualize data from each of these devices to facilitate network administrators to analyze and take action based on problems occurred in network devices.

S. Alspaugh et al., in 2014, describe the implementation of Log Management System (LMS) using Splunk application [6]. Splunk is a commercial application specifically designed for centralized log management. The results of their research are log management using the query and workflow from Splunk to filter, reformat, and summarize the logs.

Anastopoulos, et.al., in 2017 described implementation strategy of log management in a WAN network environment. The results of this study are, several stages of designing the log management systems in WAN networks. Those are sorting requirements, asset inventory, checking network topology, selecting logs to be used, choosing infrastructure architecture, creating logs, log collection, time synchronization, log processing, oversaw scalability, and performance measurement [7].

This paper is divided into four section. The first section describes the background and purpose of log management system (LMS) implementation. Second section describes the research methodology used throughout in this paper. Next section describes result and discussion of LMS implementation. Finally, this paper is closed by conclusion.

II. RESEARCH METHODOLOGY

Design Science Research (DSR) methodology, are used to design the implementation of the LMS. DSR methodology process consist of system definition, system specifications, system configuration, evaluation, and results.

The first step is system definition. This step defines the system that will be created, including the definition of the system, identification of system requirements, the purpose and benefits of the system, how it works and the topology used.

The next step is system specifications. The process of requirement specification will be described in the initial system design by determining the specification of the requirements that match the system definition.

The third step is system configuration. At this step, the specifications of predetermined requirements will be designed according to the network topology / design and applied as a series of systems or units of systems that enable the system to run. Data source was gained from Diponegoro University campus infrastructure i.e. router, switches a by simple network management protocol (SNMP). Data collection started from April 29th to July 9th, 2019.

The fourth step is evaluation and the final step is result. Research is considered successful if the system has fulfilled the objectives of the study.

A. Functional Requirements

Functional requirements of the log management system are the system can collect log activities from remote network devices using syslog. The system can group logs based on the severity level of the log. Severity levels represent the urgency level of a log message. Severity level 0 (Emergency) contains messages with the highest urgency and level 6 severity (Informational) contain messages with the lowest urgency [8]. The last functional requirement is the system can visualize logs into information that is easily understood by network administrators.

B. Hardware Requirements

Hardware is used as a system support so the system can run. The system is implemented in a virtual machine. The virtual machine used has the specifications in Table 1.

TABLE 1. VIRTUAL MACHINE SPECIFICATION

Component	Server
Processor	Intel(R) Xeon(R) Silver 4114 CPU @ 2.20GHz
Motherboard	Intel 440BX
RAM	4 GB
HDD	60 GB
NIC	1 Fast Ethernet

1 Cisco WS-C4510R + E Switch Unit in ICT as the main device that connects all network devices at Diponegoro University. Cisco 2921 routers and Cisco WS-C2960X-24TD-L switches as distribution network devices for monitoring in each faculty and unit at Diponegoro University. One Toshiba R30 laptop to configure the system and create the application.

C. Software Requirements

The log management system requires software to build servers and other supporting components. Log management server use Ubuntu 18.04 LTS as the operating system. The application for collecting logs uses Logstash then be saved to Elasticsearch and visualized using Kibana [9].

Monitoring application created using PHP programming language with a CodeIgniter framework. CodeIgniter is a framework that uses the M-V-C (Model-View-Controller) concept that allows separation between application-logic and presentation layers [10]. Nginx is used as a web server to serve applications to be able to access using web browser. Nginx is a high-performance reverse proxy web server designed to use only a few system resources [11]. Nginx uses the event-based connection handling mechanism feature. A feature that is able to minimize threads to process requests from clients, which resulting smaller memory usage [12].

Server configuration is done remotely using Putty application. Google Chrome application as a web browser that runs on the Windows 10 x64 operating system and used to test the running of the application.

D. Topology Design

The topology design of the log management system consists of various entities involved in system development. The entity is connected using a star topology with a switch as the center. This topology allows the log management server to receive data from network devices. Figure 1 shows the physical topology of the log management system.

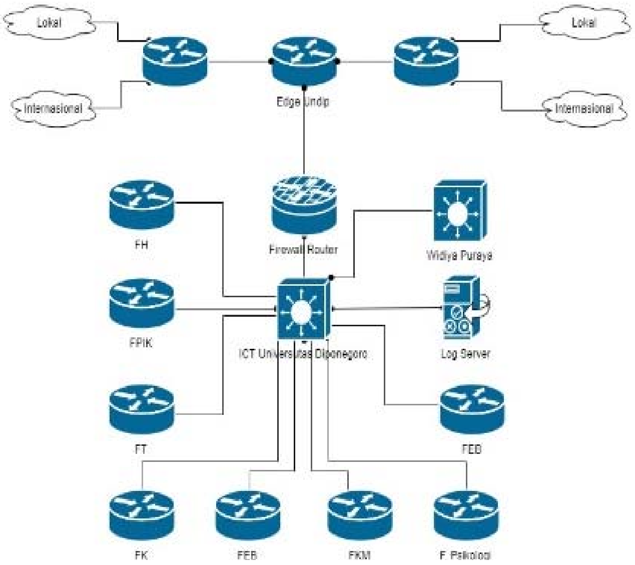


Figure 1. Design and Network Topology System

Each device has its own functions as a manager, agent, and user who uses the log management system application.

E. System Design

System design provides a per block overview or part of a monitoring system. Figure 2 shows the server system design.

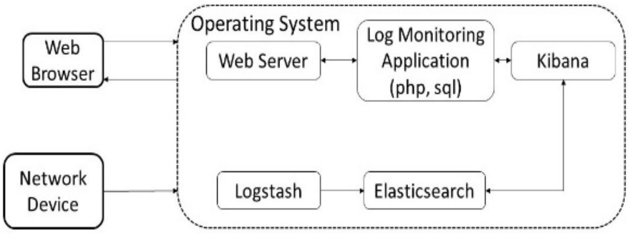


Figure 2. Block Diagram of Server System Design

F. Work Process Design

Syslog protocol was used as an information collector. Logstash as one of the syslog applications to collect logs of all agents that send logs to the log management server. Log shipping can use TCP or UDP networks. In this study, author used UDP networks on port number 8514.

Log collection is automatic so there is no need for data requests on the agent. The log from the agent will be sent to the server so the log can be processed by Logstash and stored at Elasticsearch. The server was configured to select traffic to be passed by UDP or TCP, the severity level, facility, mnemonic facility, and messages from each log sent by the agent. The agent is given configuration about the form of a network that will be used UDP or TCP, and the IP address of the log management server as the log shipping destination.

G. Log Management Flow Process

The flow chart diagram explains the process of information gathering using Syslog. Information collected will be stored in the database and the information is used to monitor the log according to the source and the value of the severity it has. The work process of the log management system is shown in Figure 3.

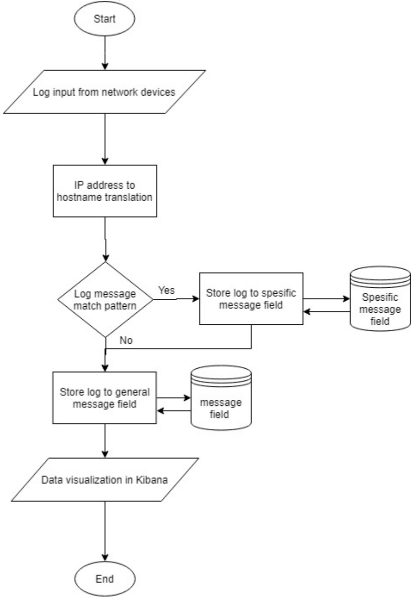

Start
Log input from network devices
IP address to hostname translation
Log message match pattern
Yes
Store log to spesific message field
Spesific message field
No
Store log to general message field
message field
Data visualization in Kibana
End

Figure 3. Flow chart of Log Management System

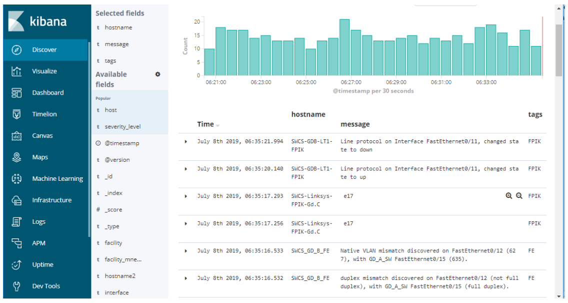
III. RESULT AND DISCUSSION

System evaluation is done to check the performance of the system being implemented. The main purpose of system evaluation is to ensure that the components of the system are functioning as needed.

A. Syslog Evaluation

The LMS server must be able to collect and manage network device logs. Communication protocol using syslog. The collection and management are process of collecting logs from agent devices that run syslog to the Elasticsearch application and identifying logs that contain special messages and grouping these logs according to the severity level.

Testing is done by observing the Discover page on Kibana as an interface for users. If a log that sent is detected, it will show as the data entered on the Discover page. Figure 4 shows the results of testing log entrance.



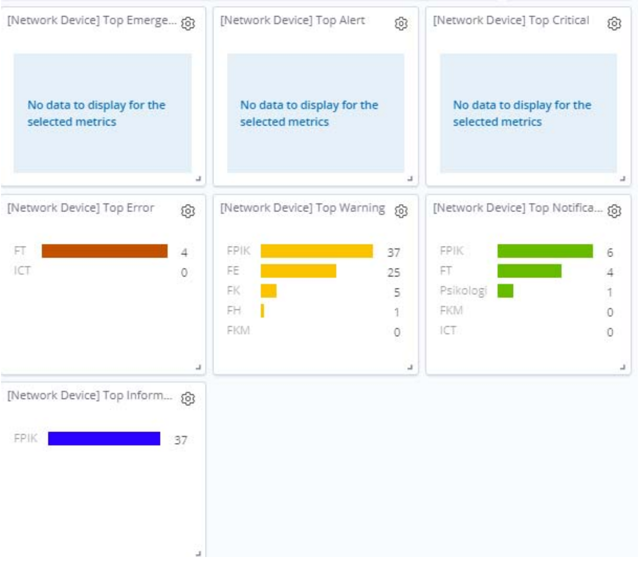
```
                            hostname                                                          tags
  Time                      message
▸ July 8th 2019, 06:35:21.994  SWCS-GDB-LT1-  Line protocol on Interface FastEthernet0/11, changed sta  FPIK
                            FPIK           te to down
▸ July 8th 2019, 06:35:20.140  SWCS-GDB-LT1-  Line protocol on Interface FastEthernet0/11, changed sta  FPIK
                            FPIK           te to up
▸ July 8th 2019, 06:35:17.293  SWCS-Linksys-   e17                                                    FPIK
                            FPIK-Gd.C
▸ July 8th 2019, 06:35:17.256  SWCS-Linksys-   e17                                                    FPIK
                            FPIK-Gd.C
▸ July 8th 2019, 06:35:16.533  SWCS_GD_B_FE   Native VLAN mismatch discovered on FastEthernet0/12 (62   FE
                                           7), with GD_A_SW FastEthernet0/15 (635).
▸ July 8th 2019, 06:35:16.532  SWCS_GD_B_FE   duplex mismatch discovered on FastEthernet0/12 (not full  FE
                                           duplex), with GD_A_SW FastEthernet0/15 (full duplex).
```

Figure 4. Visualization of Log Received from the Devices

Figure 4 shows the log of network devices successfully received by the server and can represent identification of parts of the message from the log received. The IP address of the device that sent the log can be translated into a hostname and successfully tagged unit based on the hostname. Special messages can be visualized using special fields to store the message as shown in the Available Fields section in Figure 4.

B. Log Severity Evaluation

Based on the functional requirements of the log management system, it is necessary to group logs based on the severity level of the log. Log grouping uses the severity_level field in Elasticsearch which is useful as a log separation filter parameter. Figure 5 shows the logs that has been grouped by the the severity levels of the logs.


[Network Device] Top Emerge...
[Network Device] Top Alert
[Network Device] Top Critical
[Network Device] Top Error
FT
ICT
4
0
[Network Device] Top Warning
FPIK
FE
FK
FH
FKM
37
25
5
1
0
[Network Device] Top Notifica...
FPIK
FT
Psikologi
FKM
ICT
6
4
1
0
0
[Network Device] Top Inform...
FPIK
37

No data to display for the selected metrics

No data to display for the selected metrics

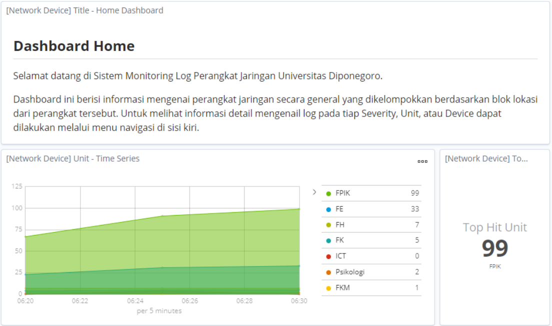
No data to display for the selected metrics

Figure 5. Log grouping based on severity level

Based on Figure 5 grouping logs on each unit tag based on the severity level of each unit including the top severity per unit.

C. Home Dashboard Evaluation

The Home Dashboard displays general information about network devices that are grouped based on the location of the device placement unit. The Home Dashboard consists of Time Series Units, Top Hit Units, Severity Gauge, and Top Severity Visualization. Figure 6 shows the information contained on the Home dashboard.



Dashboard Home

Selamat datang di Sistem Monitoring Log Perangkat Jaringan Universitas Diponegoro.

Dashboard ini berisi informasi mengenai perangkat jaringan secara general yang dikelompokkan berdasarkan blok lokasi dari perangkat tersebut. Untuk melihat informasi detail mengenail log pada tiap Severity, Unit, atau Device dapat dilakukan melalui menu navigasi di sisi kiri.

FPIK	99
FE	33
FH	7
FK	5
ICT	0
Psikologi	2
FKM	1

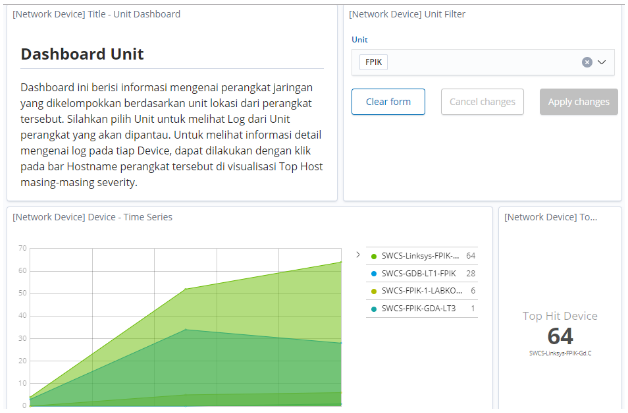
Top Hit Unit
99
FPIK

Figure 6. Home Dashboard View

Figure 6 shows the results of the Home dashboard testing which shows the system can receive logs from all network devices and process the log into information according to the type of visualization that has been configured. Through the Home dashboard information about the units that send the most logs, the type of severity that most reported and the time series of log shipping from each unit of network devices can be known.

D. Unit Dashboard Evaluation

Unit dashboards display information alike the Home dashboard, however the unit dashboard displays more specific information based on the unit location of the network device. The composition of the dashboard unit is the same as the Home dashboard. Figure 7 shows the results of the Unit Dashboard testing.



[Network Device] Title - Unit Dashboard

Dashboard Unit

Dashboard ini berisi informasi mengenai perangkat jaringan yang dikelompokkan berdasarkan unit lokasi dari perangkat tersebut. Silahkan pilih Unit untuk melihat Log dari Unit perangkat yang akan dipantau. Untuk melihat informasi detail mengenai log pada tiap Device, dapat dilakukan dengan klik pada bar Hostname perangkat tersebut di visualisasi Top Host masing-masing severity.

[Network Device] Unit Filter

Unit: FPIK

[Network Device] Device - Time Series

SWCS-Linksys-FPIK-...	64
SWCS-GDB-LT1-FPIK	28
SWCS-FPIK-1-LABKO...	6
SWCS-FPIK-GDA-LT3	1

[Network Device] To...

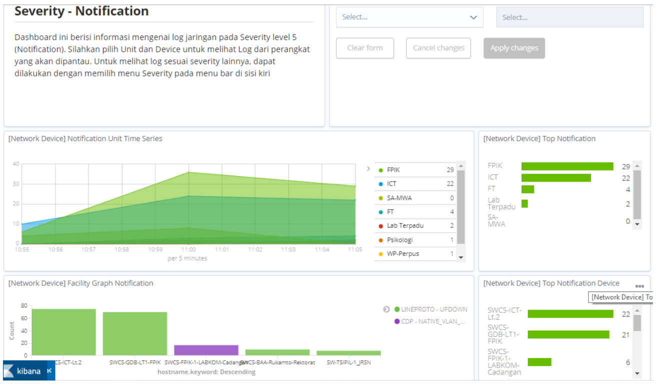
Top Hit Device 64 SWCS-Linksys-FPIK-Gd.C

Figure 7. Dashboard Evaluation

Figure 7 display the results of the unit dashboard testing show that the dashboard can display the log visualization of all network devices by grouping based on the location of the network device placement. Information on the devices in the units grouped based on the severity level.

E. Severity Dashboard Evaluation

The Severity Dashboard displays network device log information at a certain Severity level. Figure 8 shows the test results of the severity level 5 (Notification) dashboard.



Severity - Notification

Dashboard ini berisi informasi mengenai log jaringan pada Severity level 5 (Notification). Silahkan pilih Unit dan Device untuk melihat Log dari perangkat yang akan dipantau. Untuk melihat log sesuai severity lainnya, dapat dilakukan dengan memilih menu Severity pada menu bar di sisi kiri

[Network Device] Notification Unit Time Series

FPIK	29
ICT	22
SA-MWA	0
FT	4
Lab Terpadu	2
Psikologi	1
WP-Perpus	1

[Network Device] Top Notification

FPIK	29
ICT	22
FT	4
Lab Terpadu	2
SA-MWA	0

[Network Device] Facility Graph Notification

[Network Device] Top Notification Device

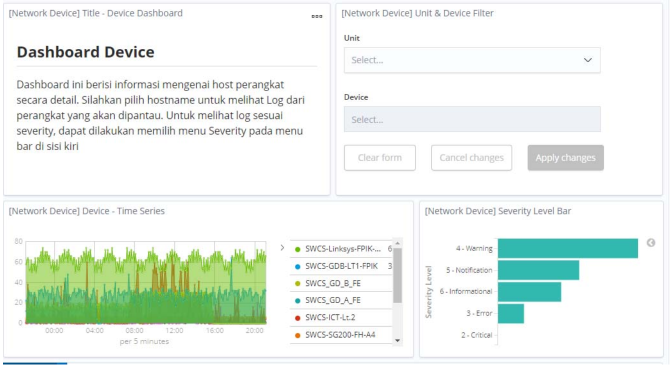
SWCS-ICT-Lt.2	22
SWCS-GDB-LT1-FPIK	21
SWCS-FPIK-1-LABKOM-Cadangan	6

Figure 8. Notification Dashboard view

Figure 8 display the results of the Notification dashboard testing which shows that the system can display the log severity level 5 (Notification) visualization on network devices. Through the dashboard information related the time series from the log with the severity notification can be displayed. There are several facilities that dominate the severity notification, those are LINK and LINEPROTO. From Figure 8, it is known that the unit sent the most log notification was FPIK. Through Notification dashboard visualization also information related to active and inactive interfaces, users accessing devices, devices that experience threshold violation, devices connected via OSPF protocol, devices that has been restarted, and devices that can be accessed via SSH can be known.

F. Device Dashboard Evaluation

Device dashboards display specific log information referring to a particular device. The visualization composition of the dashboard Device consists of visualization related to logs those are often sent by the device, including Link Time Series, Native VLAN Mismatch, MAC Address Flapping, and Duplex Mismatch. Figure 9 shows the results of the dashboard Device testing.



[Network Device] Title - Device Dashboard

Dashboard Device

Dashboard ini berisi informasi mengenai host perangkat secara detail. Silahkan pilih hostname untuk melihat Log dari perangkat yang akan dipantau. Untuk melihat log sesuai severity, dapat dilakukan memilih menu Severity pada menu bar di sisi kiri

[Network Device] Unit & Device Filter

Unit: Select...

Device: Select...

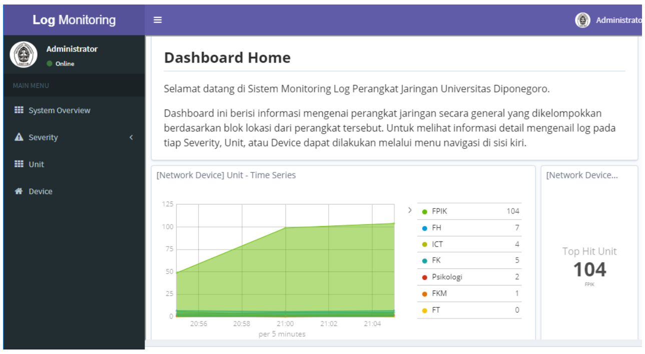
[Network Device] Device - Time Series

SWCS-Linksys-FPIK-...	6
SWCS-GDB-LT1-FPIK	3
SWCS_GD_B_FE	
SWCS_GD_A_FE	
SWCS-ICT-Lt.2	
SWCS-SG200-FH-A4	

[Network Device] Severity Level Bar

Figure 9. Device Dashboard Menu

Figure 9 display the results of the Device dashboard testing show that the dashboard able to display the visualization of network device logs. Through the dashboard, certain units and certain devices can be selected to be monitored, and there are log and log tables that are most often sent by the device to facilitate log analysis of a device.



Log Monitoring

Dashboard Home

Selamat datang di Sistem Monitoring Log Perangkat Jaringan Universitas Diponegoro.

Dashboard ini berisi informasi mengenai perangkat jaringan secara general yang dikelompokkan berdasarkan blok lokasi dari perangkat tersebut. Untuk melihat informasi detail mengenail log pada tiap Severity, Unit, atau Device dapat dilakukan melalui menu navigasi di sisi kiri.

[Network Device] Unit - Time Series

FPIK	104
FH	7
ICT	4
FK	5
Psikologi	2
FKM	1
FT	0

[Network Device...

Top Hit Unit 104 FPIK

Figure 10. Main Page of LMS.

G. Application Evaluation

Application evaluation explains the results and appearance of the application that has been created. The initial appearance of the application is a login page that serves to authenticate users who will access the server.

After authenticated, the user will be directed to the main page that contains the Home dashboard. The Home Dashboard displays general information from network devices. There are several navigation menus available in the application, those are System Overview, Severity, Units, and

Devices. Each menu will navigate to the dashboard page according to the menu selected. The main page view is shown in Figure 10.

IV. Conclusion

Cisco WS-C2960X-24TD-L Switch and Cisco 2921 Router acted as agents on network devices are able to send data to the server. The log management server is able to collect logs from devices on the network. Log collection from various devices using the UDP protocol on port number 8514 and the Logstash application has been successfully implemented. Logs that have been received are successfully grouped in the Elasticsearch field according to the message and severity level of the log. Similar information has been proven based on observations to have a different level of severity depending on the operating system version of the network device. The ratio of different device operating system is 4:1. Views on the Kibana dashboard can be shared and displayed on other web applications using iframe. Data collection started from 29th April to 8th July 2019 resulting 2.354.224 log collected, consist of 1.085.368 (46,1%) warning log, 569.892 (24,21%) notification log, 450.434 (19,133%) informational log, 248.266 (10,544%) error log, 262 (0.01292%) critical log, and 2 (0.000085%) alert log. LMS was evaluated by Diponegoro University's network administrator and resulting 75% users completely agree and 25% users agree that LMS provides complete information related to network device condition, 50% users completely agree, and 50% users agree that LMS is easy to operated, 75% completely agree and 25% agree that LMS provides analyzable information.

Suggestions for further research can be integrating log data with email, SMS, or messaging applications for notification to administrators. Further research can manage the log of application servers in the network infrastructures of Diponegoro University.

Acknowledgment

This research was financially supported by The Faculty of Engineering, Diponegoro University, Semarang, Indonesia through Strategic Research Grant 2019 number: 3161/3/ UNT7.3.3/PG/2019.

References

[1] K. Ratnaningsih and I. Suaryana, "Effects of information technology sophistication, management participation, and knowledge of accounting managers on the effectiveness of accounting information systems," J. Akunt. Univ. Udayana, vol. 6, no. 1, pp. 1–16, 2014.

[2] S. Wongkar et al., "Analysis of Internet Network Implementation by Combining LAN and WLAN Networks in Kawangkoan Village" vol. 4, no. 6, pp. 62–68, 2015.

[3] A. Leskiw, "Understanding Syslog: Servers, Messages & Security," 2017. [Online]. Available: https://www.networkmanagementsoftware.com/what-is-syslog/. [Accessed: 14-Mar-2019].

[4] C. Preneur, "ELK (ElasticSearch, Logstash, Kibana)," 2018. [Online]. Available: https://medium.com/elk-elasticsearch-logstash-kibaa-a48c12612b16. [Accessed: 15-Mar-2018].

[5] S. Alspaugh et al., "Analyzing Log Analysis: An Empirical Study of User Log Mining This paper is included in the Proceedings of the Analyzing Log Analysis: An Empirical Study of User Log Mining user surveys," 2014.

[6] V. Anastopoulos and S. Katsikas, "A structured methodology for deploying log management in WANs," J. Inf. Secur. Appl., vol. 34, pp. 120–132, 2017.

[7] S. Taftazanie, A. B. Prasetijo, and E. D. Widianto, "Web Based Network Device Monitoring Application Using SNMP Protocol and SMS Notification," J. Teknol. dan Sist. Komput., vol. 5, no. 2, p. 62, 2017.

[8] S. Chaajed, Learning ELK Stack. Birmingham: Packt Publishing Ltd., 2015.

[9] Q. J. A. Mara Destiningrum, "Web-Scheduled Doctor Scheduling Information System Using Codeigniter Framework (Case Study: Yukum Hospital Medical Center)," Teknoinfo, vol. 11, no. 2, pp. 6–13, 2017.

[10] M. Hourani, Q. Shambour, A. Al-Zubidy, and A. Al-Smadi, "Proposed Design and Implementation for RESTful Web Server," J. Softw., vol. 9, no. 5, pp. 1071–1080, 2014.

[11] R. Sharma, NGINX High Performance. Mumbai: Packt Publishing Ltd, 2015.