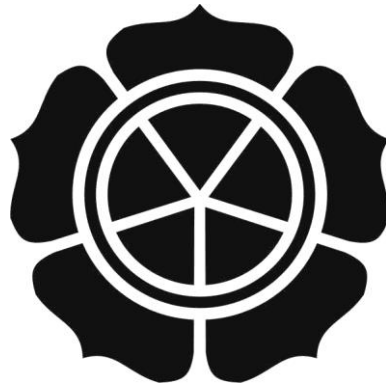


**SENTRALISASI MANAJEMEN LOG MENGGUNAKAN ELK UNTUK  
MONITORING SYSLOG BERBASIS OPEN SOURCE PADA  
UBUNTU SERVER 14.04**

**SKRIPSI**



disusun oleh

**Ricki Firmansyah**

**12.11.6324**

**JURUSAN TEKNIK INFORMATIKA  
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER  
AMIKOM YOGYAKARTA  
YOGYAKARTA  
2016**

**SENTRALISASI MANAJEMEN LOG MENGGUNAKAN ELK UNTUK  
MONITORING SYSLOG BERBASIS OPEN SOURCE PADA  
UBUNTU SERVER 14.04**

**SKRIPSI**

Untuk memenuhi sebagian persyaratan  
mencapai derajat sarjana S1  
pada jurusan teknik informatika



disusun oleh

**Ricki Firmansyah**

**12.11.6324**

**JURUSAN TEKNIK INFORMATIKA  
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER  
AMIKOM YOGYAKARTA  
YOGYAKARTA  
2016**

**PERSETUJUAN**

**SKRIPSI**

**SENTRALISASI MANAJEMEN LOG MENGGUNAKAN ELK UNTUK  
MONITORING SYSLOG BERBASIS OPEN SOURCE PADA  
UBUNTU SERVER 14.04**

yang dipersiapkan dan disusun oleh

**Ricki Firmansyah**

**12.11.6324**

telah disetujui oleh Dosen Pembimbing Skripsi  
pada tanggal 4 Februari 2016

**Dosen Pembimbing,**

  
**HERI SISMORO, M.Kom**

**NIK. 190302057**

**PENGESAHAN**

**SKRIPSI**

**SENTRALISASI MANAJEMEN LOG MENGGUNAKAN ELK UNTUK  
MONITORING SYSLOG BERBASIS OPEN SOURCE PADA  
UBUNTU SERVER 14.04**

Yang disusun oleh

**Ricki Firmansyah**

**12.11.6324**

telah dipertahankan di depan Dewan Penguji  
pada tanggal 21 Januari 2016

**Susunan Dewan Penguji**

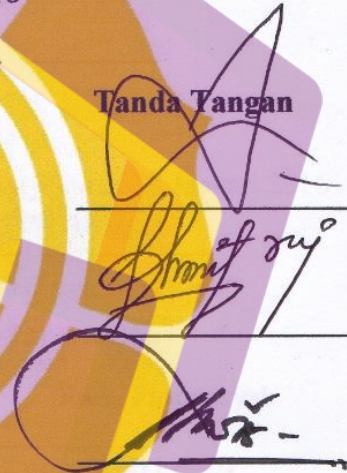
**Nama Penguji**

**Armadyah Amborowati, S.Kom, M. Eng**  
**NIK. 190302063**

**Dhani Ariatmanto, M.Kom**  
**NIK. 190302197**

**Heri Sismoro, M.Kom**  
**NIK. 190302057**

**Tanda Tangan**



Skripsi ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Sarjana Komputer  
Tanggal 4 Februari 2016

**KETUA STMIK AMIKOM YOGYAKARTA**



**Prof. Dr. M. Suyanto, M.M.**

**NIK. 190302001**



## PERNYATAAN KEASLIAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 28 Januari 2016



Ricki Firmansyah

12.11.6324

## MOTTO

\*Berangkat dengan penuh keyakinan,  
berjalan dengan penuh keikhlasan,  
istiqomah dalam menghadapi cobaan.\*

\*Hari ini harus lebih baik daripada hari kemarin, hari esok harus lebih baik  
daripada hari ini.\*

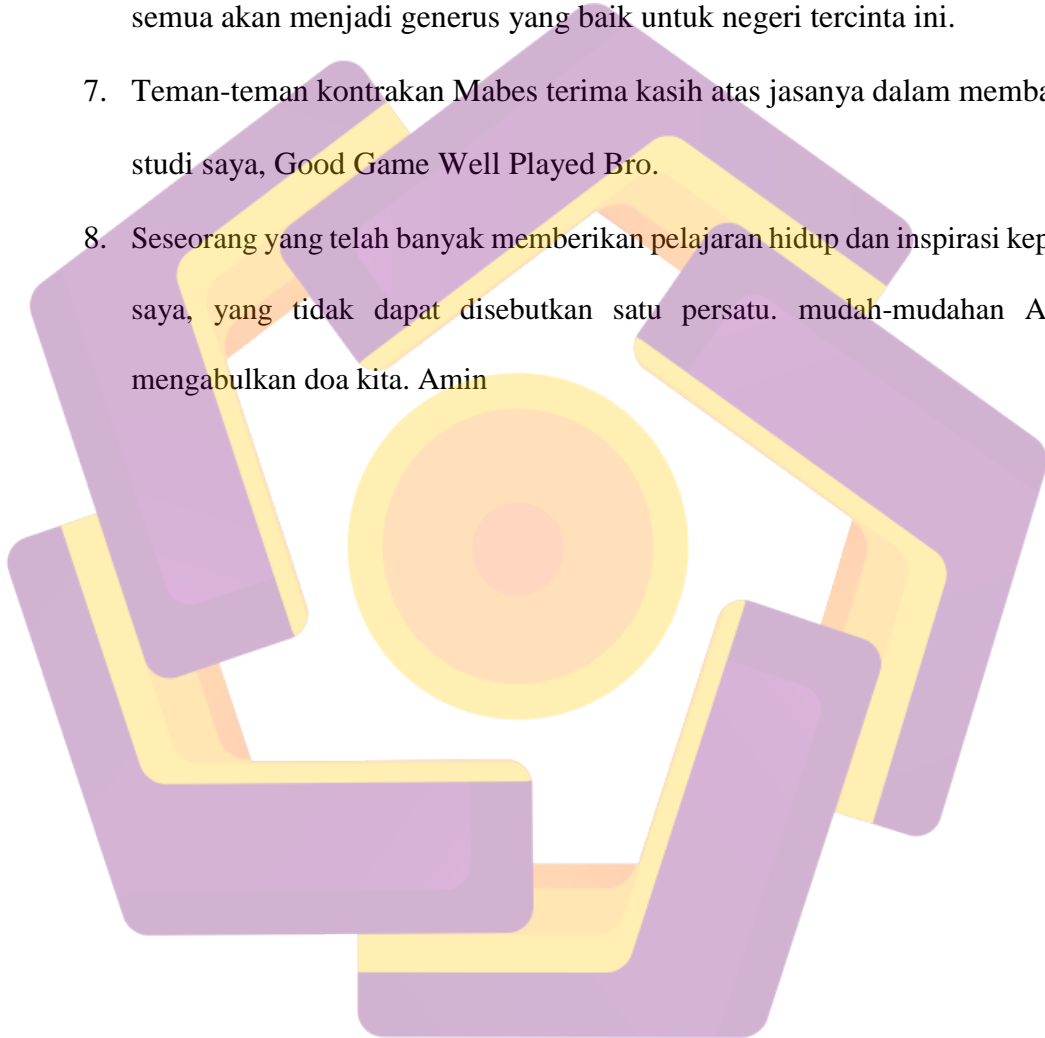
\*Ingat hanya pada allah apapun dan di manapun kita berada kepada dia-lah tempat  
meminta dan memohon\*

## PERSEMBAHAN

Alhamdulillah Puji Syukur ini penulis panjatkan, akhirnya skripsi ini dapat terselesaikan dengan baik. Karya ini merupakan wujud dari kegigihan dalam ikhtiar untuk sebuah makna kesempurnaan dengan tanpa berharap melampaui kemaha sempurna sang maha sempurna. Selaku penulis mempersembahkan skripsi ini kepada:

1. Allah SWT atas ridho-Nya skripsi ini dapat terselesaikan dengan baik, Sujud syukur aku panjatkan kepada-Mu dan jadikanlah hamba-Mu yang pandai bersyukur dan selalu dalam lindungan-Mu.
2. Shalawat serta salam senantiasa tercurah kepada Nabi Muhammad SAW. Sebagai sang pencerah yang menyempurnakan akhlak manusia menjadi manusia yang lebih cerdas.
3. Alhamdulillah Jazza Khummullohukhoirro untuk yang tercinta yaitu kedua orangtuaku Moh.Ganefi, A.pi dan Muniati, S.Pd. Yang selalu memanjatkan doa kepada putra nya dalam setiap sujudnya, memberi semangat serta penyemangat disaat keadaan yang memaksa untuk berhenti berjuang. Perjuangan ini sepenuhnya untuk kalian.
4. Alhamdulillah Jazza Khummullohukhoirro Kakak ku Reza Andika Firdause, Devi intan Permata dan adik ku Putri Adelia Zdafira yang menjadi penyemangat untuk menjadikan ku sosok yang paling baik dan berharga dalam hidup ini.

5. Untuk mu Dwi Vita Ratna Purwardini, teman hatiku, terima kasih untuk semangat dan doa yang kamu berikan, jangan pernah bosan ataupun ragu dirimulah yang terbaik untuk ku.
6. Teman-teman seperjuangan S1 TI 09 terima kasih kawan, insyaAlloh kita semua akan menjadi generus yang baik untuk negeri tercinta ini.
7. Teman-teman kontrakan Mabes terima kasih atas jasanya dalam membantu studi saya, Good Game Well Played Bro.
8. Seseorang yang telah banyak memberikan pelajaran hidup dan inspirasi kepada saya, yang tidak dapat disebutkan satu persatu. mudah-mudahan Alloh mengabulkan doa kita. Amin





## KATA PENGANTAR

Bismillahirrohmannirrokhim, Puji syukur penulis ucapkan hanya kepada Allah SWT yang telah melimpahkan karunia-Nya sehingga penulis dapat menyelesaikan laporan tugas akhir skripsi ini dengan judul “SENTRALISASI MANAJEMEN LOG MENGGUNAKAN ELK UNTUK MONITORING SYSLOG BERBASIS OPEN SOURCE PADA UBUNTU SERVER 14.04”.

Penulis mengucapkan terima kasih kepada semua pihak atas bantuan dan bimbingan dalam pembuatan tugas akhir skripsi ini, sehingga penulis dapat menyelesaikan laporan tugas akhir skripsi ini tepat waktu. Dengan kerendahan hati, pada kesempatan ini penulis mengucapkan rasa terima kasih yang sebesar-besarnya kepada :

1. Bapak Prof. Dr. M. Suyanto, MM, selaku Ketua STMIK “AMIKOM” Yogyakarta.
2. Bapak Heri Sismoro, M.Kom., selaku Dosen Pembimbing yang telah membantu dalam pembuatan skripsi ini.
3. Segenap Staf Pengajar di STMIK “AMIKOM” Yogyakarta yang telah memberikan ilmu dan pemahaman tentang dunia informatika.
4. Kedua orang tua, serta semua keluarga yang selalu memberikan dukungan dan semangat dalam menjalani kuliah.
5. Teman - teman yang telah ikut andil dan banyak membantu dalam penyelesaian skripsi ini.

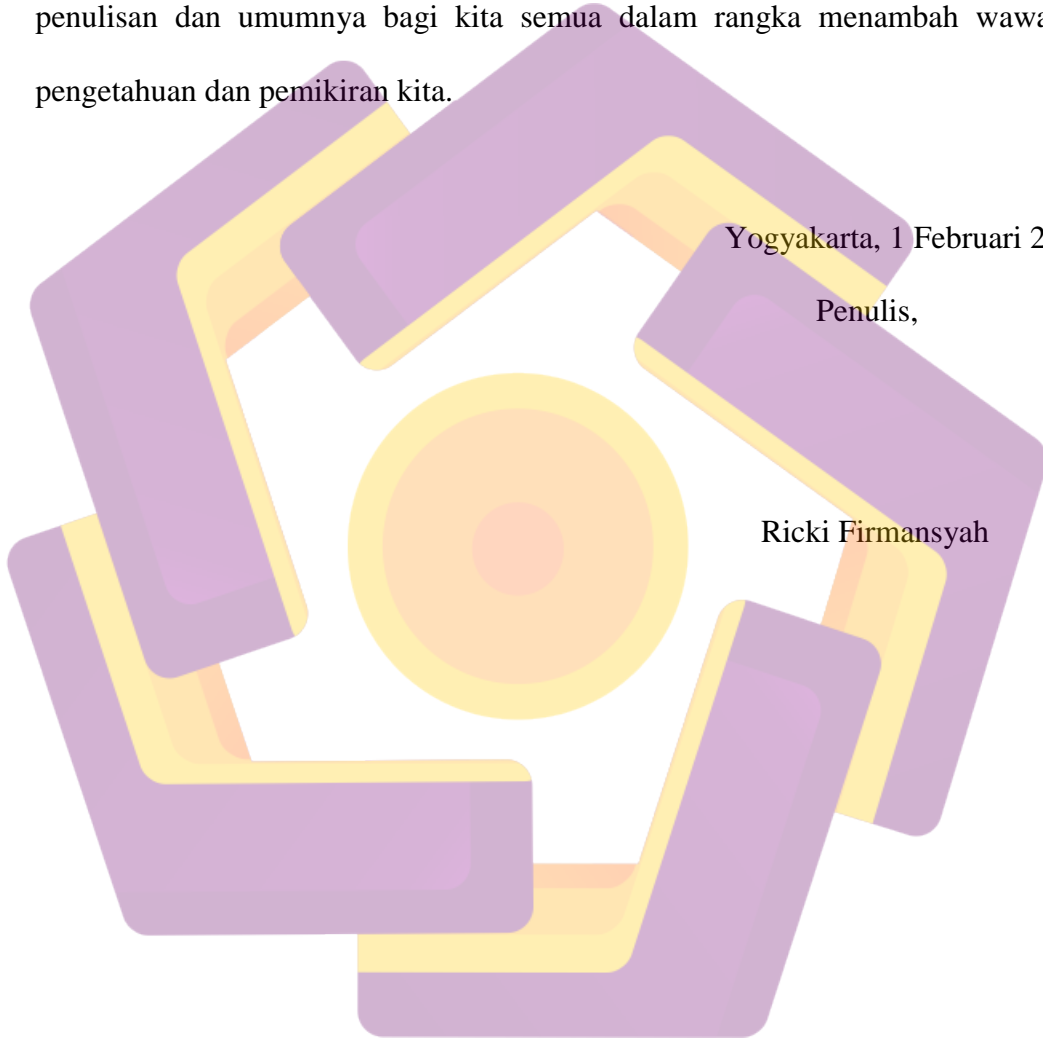
Disadari bahwa dalam penyusunan laporan skripsi ini masih jauh dari sempurna. Oleh karena itu kritik maupun saran yang bersifat membantu atau membangun sangat diharapkan.

Akhir kata, semoga penyusunan skripsi ini ada manfaatnya, khususnya bagi penulisan dan umumnya bagi kita semua dalam rangka menambah wawasan pengetahuan dan pemikiran kita.

Yogyakarta, 1 Februari 2016

Penulis,

Ricki Firmansyah



## DAFTAR ISI

JUDUL .....	i
PERSETUJUAN .....	ii
PENGESAHAN .....	iii
PERNYATAAN KEASLIAN.....	iv
MOTTO .....	v
PERSEMBAHAN .....	vi
KATA PENGANTAR .....	vii
DAFTAR ISI.....	ix
DAFTAR TABEL.....	xii
DAFTAR GAMBAR .....	xiv
INTISARI.....	xvi
<i>ABSTRACT</i> .....	xvi
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah .....	2
1.3 Batasan Masalah.....	2
1.4 Maksud dan Tujuan Penelitian .....	3
1.5 Metode Penelitian.....	3
1.5.1 Metode Pengumpulan Data .....	4
1.5.2 Metode Pengembangan Sistem .....	4
1.5.3 Metode Testing.....	4
1.6 Sistematika Penulisan.....	5
BAB II LANDASAN TEORI .....	7
2.1 Tinjauan Pustaka .....	7
2.2 Konsep Dasar Log Data .....	8
2.2.1 Pengertian Log Data.....	8
2.2.2 Definisi Log.....	9
2.3 Server.....	10
2.3.1 Sistem Server Monitoring .....	11

2.4	Linux .....	12
2.4.1	Sejarah Ubuntu .....	13
2.4.2	Ubuntu Server.....	14
2.5	Syslog .....	15
2.6	Log Data Sources .....	19
2.6.1	<i>Operating System Logs</i> .....	19
2.6.2	<i>Network Daemon Logs</i> .....	20
2.6.3	<i>Application Logs</i> .....	21
2.6.4	<i>Network Infrastructure Logs</i> .....	22
2.7	Perangkat Lunak Yang Digunakan.....	22
2.7.1	Pengertian ELK (Elasticsearch, Logstash, Kibana) .....	22
2.7.2	Logstash.....	22
2.7.3	Elasticsearch.....	23
2.7.4	Kibana .....	24
2.7.5	Nginx .....	24
2.7.6	Logstash Agent (Logstash Forwarder) .....	25
2.7.7	Curator.....	25
2.7.8	VPS (Virtual Private Server).....	26
2.7.9	Putty.....	27
<b>BAB III ANALISIS DAN PERANCANGAN SISTEM</b> .....		28
3.1	Tinjauan Umum.....	28
3.2	Analisis Kelemahan Sistem.....	30
3.2.1	Kelemahan Sistem Log yang Digunakan .....	30
3.2.2	Tindak Penanganan Masalah.....	32
3.2.3	Rancangan <i>Log Management</i> .....	32
3.3	Analisis Sistem.....	32
3.3.1	Identifikasi Sistem .....	32
3.3.2	Pemahaman Kerja Sistem.....	33
3.4	Analisa Kebutuhan Sistem .....	34
3.4.1	Kebutuhan Sistem Fungsional.....	34
3.4.2	Kebutuhan Sistem Non-Fungsional.....	35

3.4.2.1	Kebutuhan Perangkat Keras ( <i>Hardware</i> ) .....	35
3.4.2.2	Kebutuhan Perangkat Lunak ( <i>Software</i> ) .....	36
3.5	Analisis Perancangan Sistem.....	36
3.5.1	Perancangan Arsitektur <i>Log Management</i> .....	37
3.5.2	Perancangan Hubungan Modul Sistem .....	38
3.5.2.1	Penjelasan Komponen Modul .....	38
3.5.3	Flowchart Sistem.....	40
3.5.3.1	Penjelasan Flowchart.....	41
3.6	Rancangan Antar Muka ( <i>Interface</i> ).....	41
<b>BAB IV IMPLEMENTASI DAN PEMBAHASAN .....</b>		<b>43</b>
4.1	Implementasi Sistem .....	43
4.1.1	Persiapan Sistem.....	43
4.1.1.1	Menambah Repository .....	43
4.1.1.2	Instalasi Oracle Java .....	44
4.1.1.3	Instalasi Elasticsearch.....	45
4.1.1.4	Instalasi Logstash .....	47
4.1.1.5	Instalasi Nginx.....	49
4.1.1.6	Instalasi Logstash Agent (Logstash-Forwarder) .....	49
4.1.1.7	Instalasi dan Konfigurasi Kibana .....	50
4.1.2	Konfigurasi Elasticsearch.....	54
4.1.3	Konfigurasi Logstash .....	55
4.1.4	Konfigurasi Nginx sebagai <i>Reverse Proxy</i> .....	59
4.1.5	Konfigurasi SSL Certificates.....	61
4.1.6	Konfigurasi Logstash Agent (Logstash-Forwarder).....	63
4.1.7	Instal dan Konfigurasi Plugin Curator.....	65
4.1.8	Menggunakan Kibana.....	68
4.2	Pengujian Sistem .....	69
4.2.1	Pengujian Sistem dengan Akses Root .....	70
4.2.1.1	Skenario Pengujian.....	70
4.2.1.2	Proses Pengujian.....	70
4.2.1.3	Evaluasi .....	72

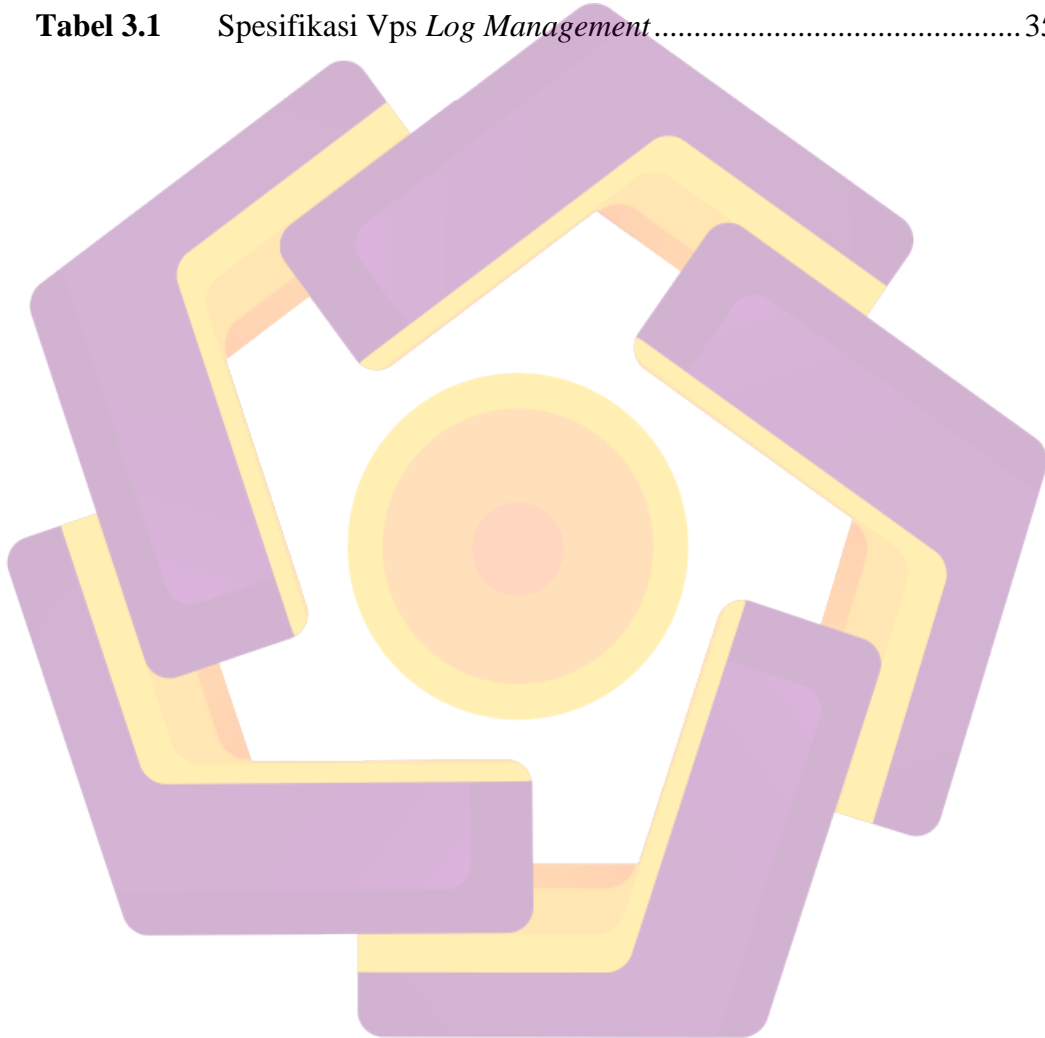
BAB V PENUTUP.....	74
5.1 Kesimpulan.....	74
5.2 Saran.....	74
DAFTAR PUSTAKA .....	75





## DAFTAR TABEL

<b>Tabel 2.1</b>	<i>Parameter Facility</i> .....	16
<b>Tabel 2.2</b>	<i>Parameter Severity</i> .....	18
<b>Tabel 3.1</b>	Spesifikasi Vps <i>Log Management</i> .....	35



## DAFTAR GAMBAR

<b>Gambar 2.1</b>	Proses Dalam Sistem Monitoring .....	11
<b>Gambar 2.2</b>	Virtual Private server .....	26
<b>Gambar 3.1</b>	Grafik alasan mengumpulkan log .....	28
<b>Gambar 3.2</b>	Grafik 10 kasus untuk log data .....	29
<b>Gambar 3.3</b>	Uji Coba Akses syslog tanpa Log management .....	31
<b>Gambar 3.4</b>	Uji coba Auth.log tanpa Log management .....	31
<b>Gambar 3.5</b>	Grafik Kerja Sistem .....	34
<b>Gambar 3.6</b>	Rancangan Arsitektur yang Digunakan .....	37
<b>Gambar 3.7</b>	Hubungan Modul Sistem .....	38
<b>Gambar 3.8</b>	Flowchart <i>Log Management</i> .....	40
<b>Gambar 3.9</b>	Rancangan Antar Muka .....	41
<b>Gambar 4.1</b>	Menambahkan Repository .....	43
<b>Gambar 4.2</b>	Instalasi Oracle Java .....	44
<b>Gambar 4.3</b>	<i>License Agreement</i> Oracle Java .....	45
<b>Gambar 4.4</b>	Update Paket Elasticsearch .....	46
<b>Gambar 4.5</b>	Install Paket Elasticsearch .....	47
<b>Gambar 4.6</b>	Update Paket Logstash .....	48
<b>Gambar 4.7</b>	Instalasi Logstash .....	48
<b>Gambar 4.8</b>	Instalasi Nginx .....	49
<b>Gambar 4.9</b>	Instalasi Logstash-Forwarder .....	50
<b>Gambar 4.10</b>	Konfigurasi Kibana .....	51
<b>Gambar 4.11</b>	Membuat Directory Kibana .....	52
<b>Gambar 4.12</b>	Download <i>Init Script</i> Kibana .....	53
<b>Gambar 4.13</b>	Menjalakan Kibana sebagai Service .....	53
<b>Gambar 4.14</b>	Konfigurasi Elasticsearch .....	54
<b>Gambar 4.15</b>	Struktur Dasar Logstash .....	56
<b>Gambar 4.16</b>	Konfigurasi Logstash .....	58

<b>Gambar 4.17</b>	Menggunakan htpasswd.....	59
<b>Gambar 4.18</b>	Konfigurasi Nginx sebagai Reverse Proxy.....	60
<b>Gambar 4.19</b>	Konfigurasi OpenSSL.....	62
<b>Gambar 4.20</b>	Generate SSL Certificate .....	62
<b>Gambar 4.21</b>	Edit Logstash-forwarder.conf Server.....	63
<b>Gambar 4.22</b>	Edit Logstash-forwarder.conf File.....	64
<b>Gambar 4.23</b>	Uji Koneksi Logstash-forwarder .....	65
<b>Gambar 4.24</b>	Instal Python-pip.....	66
<b>Gambar 4.25</b>	Instal Curator .....	66
<b>Gambar 4.26</b>	Konfigurasi Crontab –e.....	67
<b>Gambar 4.27</b>	Sistem Autentikasi Kibana .....	68
<b>Gambar 4.28</b>	<i>Web Interface</i> Kibana .....	69
<b>Gambar 4.29</b>	Uji Coba Akses Root .....	71
<b>Gambar 4.30</b>	Uji Konektifitas Logstash Agent .....	71
<b>Gambar 4.31</b>	Sebelum Menggunakan Log Management .....	72
<b>Gambar 4.32</b>	Sesudah Menggunakan Log Management.....	73

## INTISARI

Segala kegiatan di sistem dapat dicatat dan diketahui oleh seorang administrator jaringan. Pencatatan ini digunakan untuk kebutuhan audit, yaitu memeriksa sistem jika dibutuhkan. Misalnya, jika terjadi kesalahan (*error*) maka administrator dapat lebih mudah mencari sumber kesalahan karena informasinya tercatat dengan rapi. Demikian pula jika terjadi penyalahgunaan fasilitas, maka dapat diketahui siapa yang melakukannya dan apa saja yang dilakukannya.

Pencatatan kegiatan dilakukan dengan menuliskan data-data ke dalam berkas catatan yang sering disebut dengan nama “logfile” atau berkas log. Proses pencatatan ini sendiri sering disebut dengan istilah *logging*. Bayangkan sebuah sistem yang memiliki banyak fungsi misalnya sebagai server database, server web, server email, dan seterusnya. Pencatatan yang berbeda-beda ini tentunya akan membingungkan administrator sehingga akhirnya muncul standar logging yang menggunakan fasilitas atau program *syslog*.

**Kata Kunci:** *Syslog, Log Management, Log, Logging, ELK Stack.*

## **ABSTRACT**

*All activities in the system can be recorded and acknowledged by a network administrator. This recording is used for auditing requirements, namely check the system if needed. For example, if an error occurred Then administrators can more easily find the source of error because the information is recorded neatly. Similarly, in case of misuse of the facility, it can be seen who did it and what it would do.*

*Recording the activities performed by writing data to a file note which is often called by the name "logfile" or the log file. The recording process itself is often referred to as logging. Imagine a system that has many functions for example as a database server, web server, email server, and so on. Different recording will certainly confuse the administrator so that eventually emerged that uses the standard logging facility or syslog program.*

**Keyword:** Syslog, Log Management, Log, Logging, ELK Stack.