ANALISA DAN PERANCANGAN SISTEM MONITORING PERANGKAT JARINGAN KOMPUTER BERBASIS SYSLOG MENGGUNAKAN ELASTIC STACK DAN NOTIFIKASI TELEGRAM (STUDI KASUS PT. XYZ)

TUGAS AKHIR

DWI ZULFIKAR FUADI
41518110045

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2022

ANALISA DAN PERANCANGAN SISTEM MONITORING PERANGKAT JARINGAN KOMPUTER BERBASIS SYSLOG MENGGUNAKAN ELASTIC STACK DAN NOTIFIKASI TELEGRAM (STUDI KASUS PT. XYZ)

Tugas Akhir

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:
DWI ZUFIKAR FUADI
41518110045

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2022

LEMBAR PERNYATAAN ORISINALITAS

Yang bertanda tangan dibawah ini:

NIM	:	41518110045
Nama	:	Dwi Zulfikar Fuadi
Judul Tugas Akhir	:	Analisa dan Perancangan Sistem Monitoring Perangkat Jaringan Komputer Berbasis Syslog Menggunakan Elastic Stack dan Notifikasi Telegram

Menyatakan bahwa Laporan Tugas Akhir saya adalah hasil karya sendiri dan bukan plagiat. Apabila ternyata ditemukan di dalam laporan Tugas Akhir saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Jakarta, 4 Juli 2022

Dwi Zulfikar Fuadi

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR

Sebagai mahasiswa Universitas Mercu Buana, saya yang bertanda tangan di bawah ini :

Nama Mahasiswa	:	Dwi Zulfikar Fuadi
NIM	:	41518110045
Judul Tugas Akhir	:	Analisa dan Perancangan Sistem Monitoring Perangkat Jaringan Komputer Berbasis Syslog Menggunakan Elastic Stack dan Notifikasi Telegram

Dengan ini memberikan izin dan menyetujui untuk memberikan kepada Universitas Mercu Buana **Hak Bebas Royalti Non Eksklusif** (*Non-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul di atas beserta perangkat yang ada (jika diperlukan).

Dengan Hak Bebas Royalti/Non Eksklusif ini Universitas Mercu Buana berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat dan mempublikasikan tugas akhir saya.

Selain itu, demi pengembangan ilmu pengetahuan di lingkungan Universitas Mercu Buana, saya memberikan izin kepada Peneliti di Lab Riset Fakultas Ilmu Komputer, Universitas Mercu Buana untuk menggunakan dan mengembangkan hasil riset yang ada dalam tugas akhir untuk kepentingan riset dan publikasi selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 4 Juli 2022

Dwi Zulfikar Fuadi

SURAT PERNYATAAN LUARAN TUGAS AKHIR

Sebagai mahasiswa Universitas Mercu Buana, saya yang bertanda tangan di bawah ini :

Nama Mahasiswa	:	Dwi Zulfikar Fuadi
NIM	:	41518110045
Judul Tugas Akhir	:	Analisa dan Perancangan Sistem Monitoring Perangkat Jaringan Komputer Berbasis Syslog Menggunakan Elastic Stack dan Notifikasi Telegram

Menyatakan bahwa :

1. Luaran Tugas Akhir saya adalah sebagai berikut :

No	Luaran	Jenis		Status	
1	Publikasi Ilmiah	Jurnal Nasional Tidak Terakreditasi		Diajukan	✓
		Jurnal Nasional Terakreditasi	✓		
		Jurnal International Tidak Bereputasi		Diterima	
		Jurnal International Bereputasi			
	Disubmit/dipublikasikan di :	Nama Jurnal	: Al Qalam		
		ISSN	: 1907-4174 (Print) | 2621-0681 (Online)		
		Link Jurnal	: https://jurnal.stiq-amuntai.ac.id/index.php/al-qalam/index		
		Link File Jurnal Jika Sudah di Publish	: -		

2. Bersedia untuk menyelesaikan seluruh proses publikasi artikel mulai dari submit, revisi artikel sampai dengan dinyatakan dapat diterbitkan pada jurnal yang dituju.
3. Diminta untuk melampirkan scan KTP dan Surat Pernyataan (Lihat Lampiran Dokumen HKI), untuk kepentingan pendaftaran HKI apabila diperlukan

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 4 Juli 2022

Dwi Zulfikar Fuadi

LEMBAR PERSETUJUAN

Nama Mahasiswa	:	Dwi Zulfikar Fuadi
NIM	:	41518110045
Judul Tugas Akhir	:	Analisa dan Perancangan Sistem Monitoring Perangkat Jaringan Komputer Berbasis Syslog Menggunakan Elastic Stack dan Notifikasi Telegram

Tugas Akhir ini telah diperiksa dan disetujui

Jakarta, 4 Juli 2022

Menyetujui,

(Afiyati, SSi., MT)
Dosen Pembimbing

LEMBAR PERSETUJUAN PENGUJI

8/8/22, 9:22 PM TEMPLATE LEMBAR PERSETUJUAN PENGUJI - 41518110045 - DWI ZULFIKAR FUADI_001.png

LEMBAR PERSETUJUAN PENGUJI

NIM	:	41518110045
Nama	:	Dwi Zulfikar Fuadi
Judul Tugas Akhir	:	Analisa dan Perancangan Sistem Monitoring Perangkat Jaringan Komputer Berbasis Syslog Menggunakan Elastic Stack dan Notifikasi Telegram

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 05 Agustus 2022

(Wawan Gunawan, S.Kom., M.T.)

LEMBAR PERSETUJUAN PENGUJI

NIM	:	41518110045
Nama	:	Dwi Zulfikar Fuadi
Judul Tugas Akhir	:	Analisa dan Perancangan Sistem Monitoring Perangkat Jaringan Komputer Berbasis Syslog Menggunakan Elastic Stack dan Notifikasi Telegram

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 04 Agustus 2022

(Sabar Rudiarto, M.Kom)

LEMBAR PERSETUJUAN PENGUJI

NIM	:	41518110045
Nama	:	Dwi Zulfikar Fuadi
Judul Tugas Akhir	:	Analisa dan Perancangan Sistem Monitoring Perangkat Jaringan Komputer Berbasis Syslog Menggunakan Elastic Stack dan Notifikasi Telegram

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 05 Agustus 2022

(Puji Rahayu, Dr, MT)

LEMBAR PENGESAHAN

NIM	:	Dwi Zulfikar Fuadi
Nama	:	41518110045
Judul Tugas Akhir	:	Analisa dan Perancangan Sistem Monitoring Perangkat Jaringan Komputer Berbasis Syslog Menggunakan Elastic Stack dan Notifikasi Telegram

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 27 Juli 2022

Menyetujui,

(Afiyati, SSi., MT)
Dosen Pembimbing

Mengetahui,	
(Wawan Gunawan, S.Kom, MT)	(Ir. Emil R. Kaburuan, Ph.D., IPM.)
Koord. Tugas Akhir Teknik Informatika	Ka. Prodi Teknik Informatika

KATA PENGANTAR

Dengan memanjatkan puji syukur kehadirat Allah SWT yang telah melimpahkan rahmat dan karunia-Nya kepada penulis sehingga penulis dapat menyelesaikan penulisan laporan tugas akhir ini dengan judul "Analisa dan Perancangan Sistem Monitoring Perangkat Jaringan Komputer Berbasis Syslog Menggunakan Elastic Stack dan Notifikasi Telegram".

Pada kesempatan yang baik ini, izinkanlah penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada semua pihak yang telah memberikan bantuan dan dorongan semangat kepada penulis dalam menyelesaikan penulisan laporan tugas akhir ini, terutama kepada:

1. Emil R. Kaburuan, Ph.D selaku Ka. Prodi Teknik Informatika yang telah memberikan pengarahan selama masa perkuliahan.
2. Afiyati, S.Si, MT selaku Dosen Pembimbing tugas akhir yang telah memberikan arahan terkait materi dan penulisan laporan tugas akhir kepada penulis.
3. Orang tua dan rekan - rekan perkuliahan yang telah memberikan dukungan serta doa selama proses penyusunan laporan tugas akhir.

Penulis menyadari bahwa laporan tugas akhir ini masih banyak kekurangan baik bentuk, isi, maupun teknik penyajiannya. Oleh sebab itu, kritikan yang bersifat membangun dari berbagai pihak penulis terima dengan tangan terbuka dan sangat diharapkan. Semoga kehadiran jurnal tugas akhir ini dapat bermanfaat serta menjadi sumber inspirasi.

Jakarta, 1 Juli 2022

Dwi Zulfikar Fuadi

DAFTAR ISI

NASKAH JURNAL

Analisa dan Perancangan Sistem Monitoring Perangkat Jaringan Komputer Berbasis *Syslog* Menggunakan *Elastic Stack* dan Notifikasi Telegram (Studi Kasus PT.XYZ)

Dwi Zulfikar Fuadi *[1]

Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana,
Jakarta Barat, Indonesia 11650

e-mail: *[1] 41518110045@student.mercubuana.ac.id

Abstrak

Perkembangan teknologi informasi menuntut penggunaan perangkat yang semakin banyak, mulai dari Server, Switch, Router, Firewall dan perangkat jaringan lainnya. Masalah yang muncul adalah banyaknya perangkat dalam jaringan skala besar dapat mempersulit Administrator untuk mengidentifikasi sumber dan akar penyebabnya. Lebih banyak perangkat jaringan akan membutuhkan lebih banyak biaya perawatan, terutama jika seorang Administrator perlu mencari log pesan untuk semua perangkat jaringan. Setiap masalah menjadi event pada perangkat jaringan, yang semuanya ada di dalam log sistem (syslog). Syslog adalah standar logging yang digunakan aplikasi untuk mengirim informasi ke server fokus, Melalui penelitian ini, akan dilakukan analisa serta perancangan sistem monitoring secara terpusat berbasis syslog. Metode yang akan digunakan dalam penelitian ini adalah Design Science and Research (DSR), peneliti akan menggunakan Elastic Stack (ELK) dan notifikasi telegram. Elastic Stack atau gabungan dari aplikasi opensource Elasticsearch, Logstash dan Kibana yaitu tool yang digunakan untuk membantu mengumpulkan log sistem, menyimpan, dan memvisualisasikan log tersebut. Notifikasi telegram digunakan untuk memberikan informasi kepada Administrator, sehingga dapat mengetahui informasi perangkat secara realtime.

Kata kunci : Syslog, Elastic Stack, Telegram

1. **PENDAHULUAN**

Di masa sekarang ini, perkembangan teknologi informasi dapat memunculkan berbagai layanan baru yang berguna bagi pekerjaan manusia. Kemudahan dalam mengakses internet juga menjadikan point penting dalam penyebaran informasi. Berdasarkan survey lembaga Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) tentang penetrasi pengguna internet di Indonesia tahun 2019-2020 jumlah pengguna internet di Indonesia sekitar 196.700.000, naik 8.9% atau 25.500.000 juta pengguna dari tahun 2018[1]. Kemudahan komunikasi yang dialami saat ini tidak terlepas dari peranan Administrator jaringan dalam mengelola sumber daya jaringan dengan tepat. Administrator jaringan bertanggung jawab atas desain dan konfigurasi perangkat jaringan dan untuk menjaga stabilitas lalu lintas perangkat jaringan, tidak jarang objek yang dikelola Administrator mengalami masalah. Setiap masalah dapat memiliki penyebab yang berbeda, hal ini dapat terjadi karena kesalahan Administrator, kesalahan perangkat atau penggunaan perangkat yang tidak sah. Setiap masalah menjadi event pada perangkat jaringan, yang semuanya ada di dalam log sistem (syslog)[2].

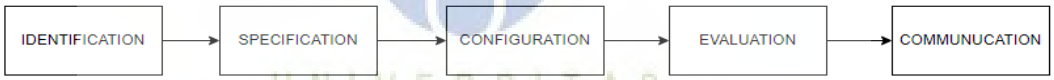
Syslog adalah standar logging yang digunakan aplikasi untuk mengirim informasi ke server fokus[3], dalam hal ini adalah perangkat Switch. Masalah yang muncul berikutnya adalah banyaknya perangkat dalam jaringan skala besar dapat mempersulit Administrator untuk mengidentifikasi sumber dan akar penyebabnya. Oleh karena itu diperlukan sistem monitoring yang dapat memusatkan transmisi log dari semua perangkat jaringan dan memiliki sistem pelaporan yang mudah dianalisis oleh Administrator jaringan. Elastic Stack atau gabungan dari aplikasi Elasticsearch, Logstash dan Kibana adalah tool yang berguna untuk mengumpulkan log dan memvisualisasikan log tersebut[4].

Melalui penelitian ini, peneliti bermaksud mengimplementasikan sistem monitoring berbasis syslog mengunakan Elastic Stack yang dibuat untuk mengumpulan semua informasi log dari perangkat jaringan yang digunakan dan notifikasi telegram untuk memudahkan administrator jaringan memperoleh informasi tentang masalah pada perangkat jaringan yang dikelola.

Peneliti memaparkan analisa dan perancangan sistem monitoring di lingkungan jaringan sub unit PT XYZ. Sub unit tersebut bertugas menyediakan layanan aplikasi yang dimiliki PT.XYZ dengan perangkat yang tersebar di berbagai wilayah Indonesia. Hasil dari penelitian ini, perancangan sistem monitoring di jaringan kantor meliputi beberapa tahapan yaitu mengurutkan kebutuhan, memeriksa perangkat jaringan aktif, pengumpulan log, pemrosesan log dan analisa log yang akan digunakan untuk notifikasi telegram.

2. METODE PENELITIAN

Dalam penelitian ini, pengumpulan data dilakukan dengan menggunakan metode observasi, yaitu mengumpulkan data langsung dari lapangan. Penelitian ini menggunakan pendekatan metode perancangan jaringan *Design Science Research (DSR),* tahapan-tahapan dalam metodologi DSR adalah definisi sistem, spesifikasi sistem, konfigurasi sistem, evaluasi, dan hasil. Seperti pada gambar 2.1



Gambar 2.1 Tahapan metodologi penelitian DSR

a. Identification

Di tahap pertama, peneliti melakukan identifikasi masalah serta latar belakang. Peneliti mengidentifikasi permasalahan spesifik yang ingin dipecahkan dan nilai pentingnya solusi dari permasalah tersebut. Sistem monitoring merupakan point penting dalam jaringan, maka di setiap jaringan dilakukan sebuah cara untuk memantau perangkat jaringan yang dimilikinya, sehingga ketika terjadi masalah dapat ditangani dengan segera, serta juga untuk faktor keamanan pihak pihak yang tidak bertanggung jawab[5]. Dalam monitoring perangkat jaringan ada dua metode yang biasanya digunakan, yaitu metode syslog dan SNMP. Pada penelitian ini peneliti fokus kepada metode syslog karena untuk memonitoring aktivitas

perangkat metode syslog adalah yang lebih baik[6]. Syslog merupakan sebuah informasi atau jejak aktivitas perangkat jaringan yang dapat disimpan sementara (buffered) atau dikirimkan ke sebuah perangkat jaringan lainnya secara terpusat . Melalui metode tersebut, peneliti akan mengumpulkan semua informasi perangkat jaringan, menyimpannya di dalam server dan memvisualisasikan, serta membuat sebuah notifikasi telegram.

b. Specification

Proses spesifikasi sistem akan menggambarkan awal dari perancangan sistem dengan mendefinisikan spesifikasi kebutuhan yang sesuai dengan tahap pertama.

1) Desain Sistem

Desain sistem menggambarkan bagian bagian dari sistem monitoring, berikut ini adalah desain sistem ELK Server pada gambar 2.2 :

Gambar 2.2 Design sistem monitoring

2) Analisis Kebutuhan Fungsional

Kebutuhan fungsional sistem adalah bahwa sistem dapat mengumpulkan log aktivitas dari perangkat jaringan menggunakan syslog. Sistem dapat mengelompokkan log berdasarkan tingkat keparahan pada log. Pesan Syslog digunakan untuk melaporkan tingkat darurat dan peringatan terkait dengan masalah perangkat lunak atau perangkat keras[7]. Sebagai ilustrasi, sistem restart akan dikirim melalui tingkat notification. Sistem reload akan dikirim melalui tingkat informational. Jika perintah debug dikeluarkan, itu disampaikan melalui

tingkat Debug (debugging) berisi pesan yang paling tidak mendesak[8], seperti dideskripsikan pada tabel 2.1.

Security Name	Security Level	Explanation
Emergency	Level 0	System Unsuable
Alert	Level 1	Immediate Action Needed
Critical	Level 2	Critical Condition
Error	Level 3	Error Condition
Warning	Level 4	Warning Condition
Notification	Level 5	Normal,Significant Condition
Informational	Level 6	Informational Message
Debugging	Level 7	Debugging Message

Table 2.1 Table Security level pada syslog

Kebutuhan fungsional lainnya adalah bahwa sistem dapat melihat log sebagai informasi yang mudah dipahami oleh Administrator jaringan. Dan yang terakhir adalah log dapat dikirimkan melalui pesan telegram untuk diterima oleh akun telegram Administrator.

3) Analisis Kebutuhan Perangkat Keras

Pada penelitian ini digunakan sebuah Microtower PC sebagai server pengoperasian sistem. Sistem diimplementasikan pada mesin virtual menggunakan aplikasi Virtual Box. Dengan spesifikasi seperti pada tabel 2.2 berikut ini.

Nama	Deskripsi
CPU	AMD Phenom II X2 550 Processor
Core	1
RAM	8GB
Hardisk	100GB
Network Adapter	1

Table 2.2 Spesifikasi Server Monitoring

1 Unit Switch Cisco WS-C2960S-24PS-L sebagai perangkat utama yang menghubungkan semua perangkat pada jaringan komputer. dan 3 buah switch cisco model WS-C2960X-24TS-L yang digunakan untuk dilakukan monitoring. Switch tersebut menghubungkan perangkat perangkat PC kabel serta server server ke jaringan komputer. satu buah Laptop Acer Aspire 5 yang digunakan untuk melakukan konfigurasi dan pembuatan aplikasi.

4) Kebutuhan perangkat Lunak

Sistem monitoring membutuhkan perangkat lunak untuk membuat server dan komponen pendukung lainnya. Server monitoring menggunakan sistem operasi Ubuntu 22.04.4 LTS. Aplikasi mengumpulkan log menggunakan Logstash dan kemudian menyimpannya di Elasticsearch dan visualisasi menggunakan Kibana.

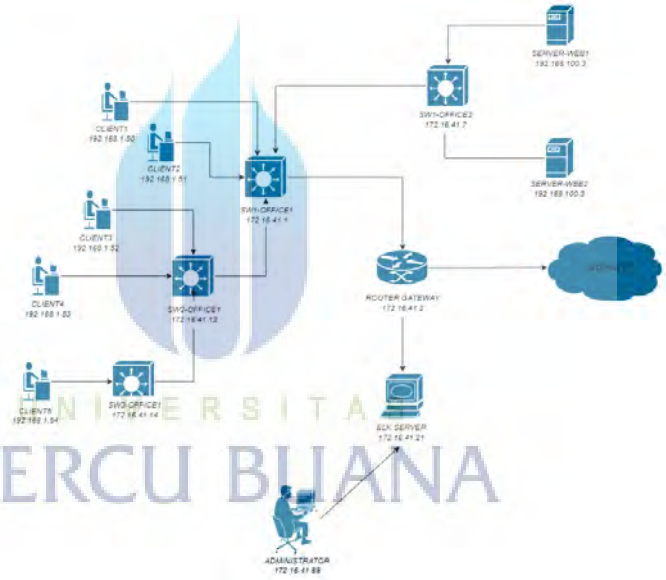
Konfigurasi pada server dilakukan secara remote menggunakan aplikasi Putty. Aplikasi Google Chrome sebagai web browser yang berjalan pada sistem operasi Windows 11 x64 digunakan untuk melakukan percobaan dan pengujian berjalannya aplikasi serta aplikasi telegram yang digunakan untuk pengujian notifikasi.

c. Configuration

Konfigurasi sistem. spesifikasi kebutuhan yang telah ditentukan akan dirancang sesuai topologi jaringan dan diimplementasikan sebagai sebuah sistem atau sub sistem yang bertujuan untuk menjalankan sistem dan cara kerja sistem.

1) Topologi jaringan

Desain topologi terdiri dari berbagai perangkat yang terlibat dalam pembangunan sistem. Perangkat tersebut dihubungkan menggunakan topologi star dan menggunakan Teknik cascade, yaitu dengan satu switch sebagai pusat. Seperti pada gambar 2.2 dibawah ini :



Gambar 2.2 Design jaringan sistem monitoring

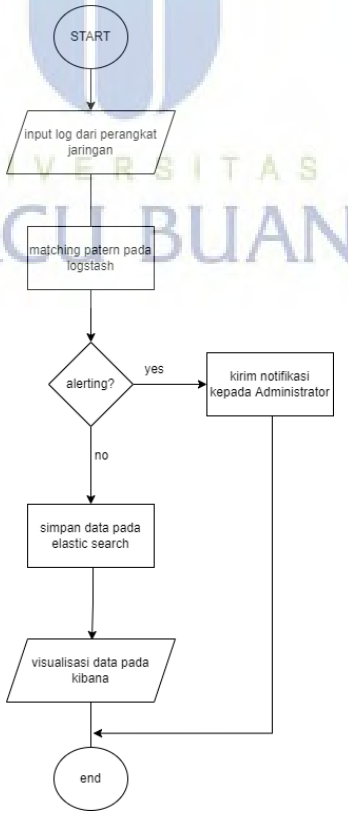
Setiap perangkat memiliki fungsi masing-masing, untuk faktor keamanan penyebaran ip dibedakan berdasarkan fungsinya, Dikonfigurasi menggunakan VLAN, berikut adalah penjabarannya pada tabel 2.3 :

Network	VLAN	Fungsi
172.16.41.0/24	6	Management Syslog
192.168.1.0/24	7	Client
192.168.100.0/24	8	Server

Table 2.2 mapping ip sistem monitoring

2) Aliran proses sistem monitoring

Aliran proses merupakan penjelasan dari langkah kerja sistem monitoring. Log dikirimkan perangkat jaringan akan dikumpulkan, disimpan dan diproses didalam ELK server. Informasi tersebut dapat digunakan Administrator jaringan untuk memantau jaringan miliknya, menggunakan dashboard dan menerima pesan notifikasi. Aliran proses sistem monitoring seperti pada gambar 2.3

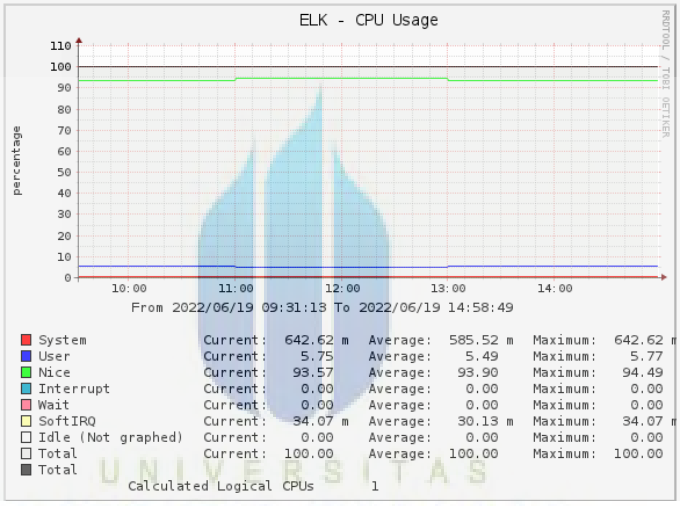


Gambar 2.3 Aliran proses sistem monitoring

d. Evaluation

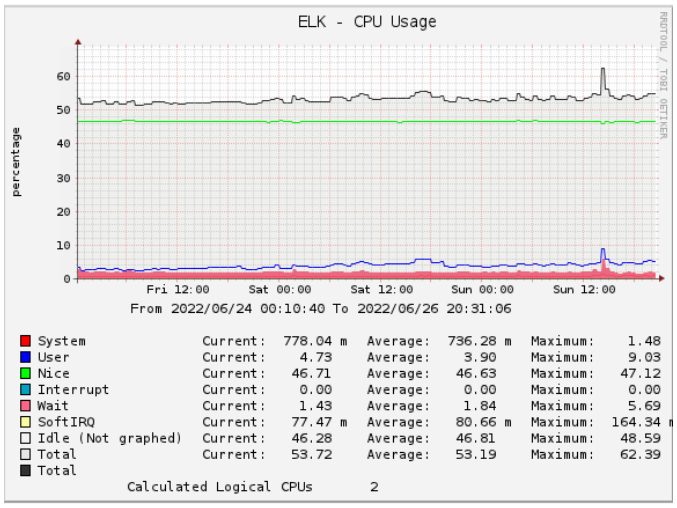
Tahap keempat adalah evaluasi. Pengujian dilakukan mulai tanggal 6 Mei 2022 sampai 19 Juni 2022 menghasilkan 1,527, 484 log yang berhasil terkumpul di server.

Perancangan sistem monitoring terdiri dari kemampuan hardware yang tinggi utuk dapat mengolah pesan dengan baik Pada gambar 2.5 dibawah ini, dapat dilihat bahwa performa server (CPU) cukup tinggi, sehingga server tidak bekerja dengan maksimal karena beban yang diberikan tidak sesuai dengan kapasitas server.



Gambar 2.5 Penggunaan CPU 1 core pada server ELK

Dengan demikian, peneliti melakukan penambahan komponen hardware pada server ELK, yaitu dengan menaikan jumlah core CPU pada server dari 1 core menjadi 2 core, setelah itu usage rata rata turun menjadi 50% dan server berjalan dengan lancar. seperti pada gambar 2.6 dibawah ini.



Gambar 2.6 Penggunaan CPU 2 core pada server ELK

e. Communication

Setelah diperoleh hasil evaluasi, selanjutnya Peneliti mengkomunikasikan Permasalahan, Salah satu bentuk komunikasi adalah Publikasi Ilmiah [9]. Penelitian akan berhasil jika sistem berjalan sesuai dengan tujuan utama penelitian

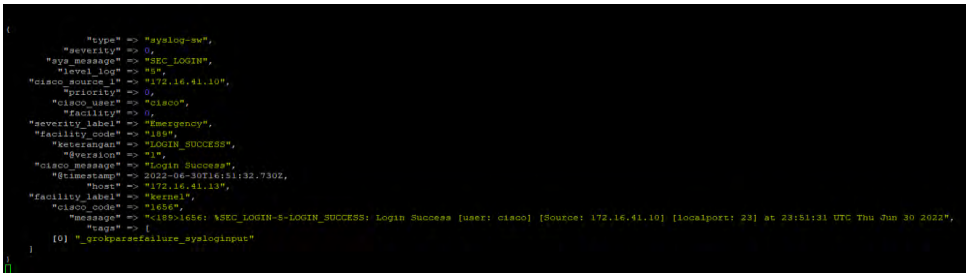
3. HASIL DAN PEMBAHASAN

Pengujian sitem terdapat dua bagian, yaitu pengujian dashboard visualisasi dan pengujian Bot notifikasi. Tujuan utama dari pengujian sistem adalah untuk memastikan bahwa komponen sistem bekerja seperti yang diinginkan.

Tahap pertama melakukan proses konfigurasi menggunakan metode syslog dengan menentukan server ELK sebagai tempat untuk menerima informasi yang dikirim oleh Switch.

%SYS-6-LOGGINGHOST_STARTSTOP: Logging to host
port 5514 started – CLI initiated

Tahap selanjutnya melakukan identifikasi field pesan yang dikirimkan oleh switch agar informasi yang dikirim dapat diolah oleh server, berikut gambar 5.2 adalah hasil field yang sudah dilakukan identifikasi.

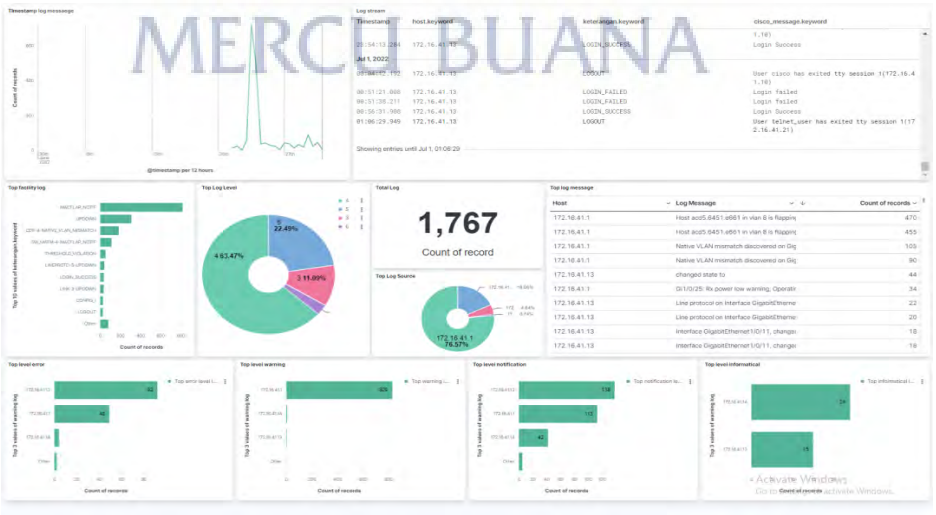


Gambar 5.2 hasil identifikasi pesan syslog pada Logstash

Pattern yang sudah dilakukan identifikasi pada tahap sebelumnya, dilakukan pengecekan pada tool elasticsearch, jika berhasil maka akan tersimpan dan data bisa ditampilkan seperti pada gambar 5.3 dibawah ini :

Gambar 5.3 tampilan pesan syslog pada Kibana

Untuk memudahkan dalam menganalisis dibuatkan sebuah visualisasi log seperti pada gambar 5.4



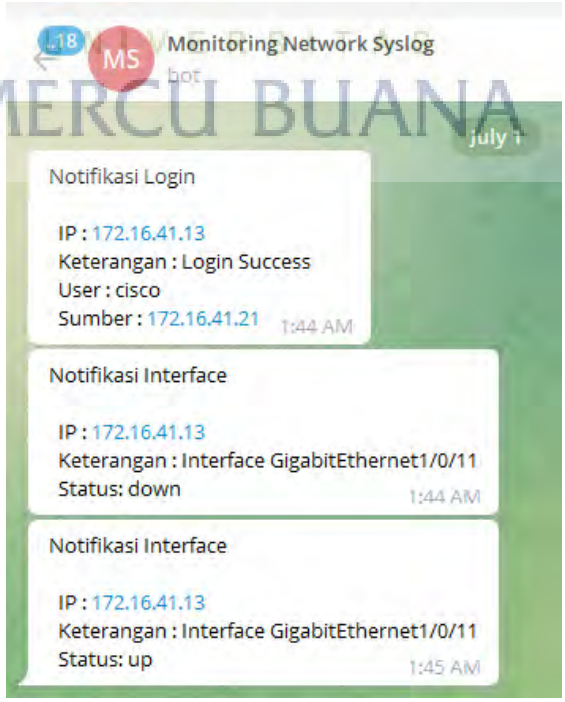
Gambar 5.4 Dashboard visualisasi sistem monitoring berbasis syslog

Selanjutnya adalah pengujian bot notifikasi, bot merupakan sebuah progam yang dirancang untuk melakukan sesuatu perintah secara automatis sesuai dengan

tujuan tertentu. Bot notifikasi dalam penelitian ini yaitu menggunakan aplikasi chat telegram. Telegram tidak hanya sebuah aplikasi chat pesan, berbagi foto ataupun video, tetapi juga dapat membuat sebuah bot dengan memanfaatkan API pada website resmi milik telegram secara gratis[10]. Dalam penelitian ini, penggunaan notifikasi diolah pada saat pesan log diterima oleh Logstash dan secara langsung akan dikirimkan pesan ke akun telegram Administrator seperti pada konfigurasi gambar 5.5, sehingga pesan notifikasi terkirim secara realtime seperti pada gambar 5.6.

```
if "Login" in [cisco_message] {
http {
        format => "json"
        http_method => "post"
        url => "https://api.telegram.org/bot22312/sendMessage"
        mapping => {
                "chat_id" => "1234556"
                "text" => " Notifikasi Login
                           IP : %{host}
                           Keterangan : %{cisco_message}
                           User : %{cisco_user}
                           Sumber : %{cisco_source_1}"
        }
}
```

Gamar 5.6 Alerting login pada Logstash menggunakan API telegram



Gambar 5.5 Pesan notifikasi login dan interface pada telegram Administrator

4. KESIMPULAN

Dari hasil penelitian perancangan sistem monitoring jaringan berbasis syslog dengan menggunakan ELK Stack ini, perangkat jaringan switch dapat mengirimkan informasi mengenai aktivitas yang ada pada log sistem pada server menggunakan protokol UDP. Pesan yang dikirimkan oleh perangkat switch ditentukan pada saat melakukan konfigurasi pada switch yaitu pada level logging. Semakin tinggi nilainya maka semakin banyak pesan yang akan dikirim, hal tersebut terjadi karena metode syslog membaca level debugging sehingga pesan log sistem pada level di bawahnya juga akan terkirim kedalam server.

Spesifikasi server yang digunakan untuk menerima log sistem sangat berpengaruh terhadap kehandalan dalam mengolah pesan. Hardware yang berpengaruh adalah CPU, CPU digunakan untuk pemrosesan multitasking atau beberapa proses berjalan secara bersamaan, pada penelitian ini proses yang berjalan paling banyak adalah Elasticsearch untuk menyimpan data dan analytics, Logstash untuk menerima log sistem, filtering pesan, dan proses visualisasi oleh Kibana. Dengan spesifikasi server menggunakan 2 core CPU mampu menghandle proses tersebut cukup baik dengan penggunaan rata-rata 50%. Semakin tinggi spesifikasi akan semakin bagus.

Telegram merupakan aplikasi pesan gratis yang tersedia pada perangkat mobile, PC ataupun berbasis WEB. Telegram tidak hanya dapat berbagi foto dan video, tetapi juga dapat membuat sebuah Bot yang dapat mengirimkan pesan otomatis serta dapat diintegrasikan dengan proses yang ada di dalam server. Sehingga Administrator dapat menerima pesan secara realtime dari ELK server. Pesan yang dikirimkan bisa ditentukan pada konfigurasi Logstash. Sehingga dapat memilih pesan mana yang akan dikirim ke telegram atau yang tidak dikirim.

ELK dapat digunakan untuk melakukan monitoring perangkat jaringan switch, dengan data bersumber dari log sistem. Salah satu komponen utamanya adalah Kibana, Kibana berfungsi untuk melakukan visualisasi terhadap pesan yang sudah tersimpan pada Elasticsearch. Visualisasi pada Kibana bisa digunakan sesuai dengan kebutuhan Administraor, terdapat berbagai tipe mulai dari pie cart, timestamp, bar chart sampai dengan streaming pesan log, dengan hal tersebut dapat

memudahkan Administrator dalam mengelola serta menganalisa masalah perangkat jaringan yang dimilikinya.

DAFTAR PUSTAKA

1. Aditya Wicaksono Irawan, Aan Yusufianto, Dwi Agustina & Reagan Dean. *Tentang Indonesia Survey Center*. https://apjii.or.id/survei2019 (2020).
2. Dan, L. *et al.* Implementasi Log Management Server Menggunakan Elk (Elastic Implementasi Log Management Server Menggunakan Elk (Elastic Search , Logstash Dan Kibana) Stack Pada Server Web Snort Di Pt . Xyz. *Jurnal Informatika Sunan Kalijaga* **4**, 1–8 (2020).
3. C. Roja & P. N. Jayanthi. *Syslog Daemon for Security Event Monitoring using UDP Protocol*. (2019).
4. Fauzi, A. Sistem Manajemen Dan Visualisasi Syslog Perangkat Jaringan Komputer Pada Ict Universitas Diponegoro Berbasis Elk Stack. *Jurnal Sistem Komputer* **10**, 42–46 (2020).
5. Raja, B., Ravindranath, K. & Jayanag, B. Monitoring and analysing anomaly activities in a network using packetbeat. *International Journal of Innovative Technology and Exploring Engineering* **8**, 45–49 (2019).
6. A. Leskiw. Understanding Syslog: Servers, Messages & Security. (2017).
7. Cisco. Configuring System Message Logging. **0**, 1–14 (2018).
8. Sudaryanto, S. & Nurhayati, D. Monitoring Interfaces Fastethernet on Cisco Catalyst 3750 to Ensure Use of The Security Computer Network In STTA Computing Laboratories. *Conference SENATIK STT Adisutjipto Yogyakarta* **5**, 215–222 (2019).
9. TONY D. SUSANTO, PH. D. Metode PENELITIAN SAINS-DESAIN (Design-Science Research). (2020).
10. Febriyanti, P. & Rusmin, S. Febriyanti Panjaitan PEMANFAATAN NOTIFIKASI TELEGRAM UNTUK MONITORING JARINGAN. *Jurnal SIMETRIS* **10**, 725–732 (2019).

KERTAS KERJA

Ringkasan

Kertas kerja ini merupakan material kelengkapan artikel jurnal dengan dengan judul Analisa dan Perancangan Sistem Monitoring Perangkat Jaringan Komputer Berbasis Syslog Menggunakan Elastic Stack dan Notifikasi Telegram yang berisi semua material hasil penelitian Tugas Akhir yang tidak dimuat atau disertakan di artikel jurnal. Dalam kertas kerja ini akan dijelaskan mengenai literature review, dataset yang digunakan, serta langkah-langkah perancangan, tahapan implementasi dan hasil pengujian penelitian

Pendahuluan

Di masa sekarang ini, perkembangan teknologi informasi dapat memunculkan berbagai layanan baru yang berguna bagi pekerjaan manusia. Kemudahan dalam mengakses internet juga menjadikan point penting dalam penyebaran informasi. Berdasarkan survey lembaga Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) tentang penetrasi pengguna internet di Indonesia tahun 2019-2020 jumlah pengguna internet di Indonesia sekitar 196.700.000, naik 8,9% atau 25.500.000 juta pengguna dari tahun 2018. Kemudahan penyebaran informasi yang dialami saat ini tidak lepas dari peran Administrator jaringan dalam pengelolaan sumber daya jaringan yang tepat. Administrator jaringan bertanggung jawab atas desain dan konfigurasi perangkat jaringan dan untuk menjaga stabilitas lalu lintas perangkat jaringan, tidak jarang objek yang dikelola Administrator mengalami masalah. Setiap masalah dapat memiliki penyebab yang berbeda, hal ini dapat terjadi karena kesalahan Administrator, kesalahan perangkat atau penggunaan perangkat yang tidak sah. Setiap masalah menjadi event pada perangkat jaringan, yang semuanya ada di dalam log sistem (syslog).

Syslog adalah standar logging yang digunakan aplikasi untuk mengirim informasi ke server fokus, dalam hal ini adalah perangkat Switch. Masalah yang muncul berikutnya adalah, pada jaringan berskala besar terdapat banyak perangkat

hal itu akan menyulitkan Administrator jaringan untuk mendeteksi sumber dan penyebab kendal. Sehingga diperlukan suatu sistem monitoring yang dapat memusatkan pengiriman log dari seluruh perangkat jaringan serta memiliki sistem pelaporan yang mudah dianalisa oleh Administrator jaringan. Elastic Stack atau gabungan dari aplikasi opensource Elasticsearch, Logstash dan Kibana adalah tool yang berguna untuk mengumpulkan log dan juga menvisualisasi log tersebut.

Pada sebuah jurnal yang berjudul "*Automation of Log Analysis Using the Hunting ELK Stack*" ElK Stack atau Elastic Stack digunakan peneliti untuk mendeteksi serangan *Cyber*. Peneliti menggunakan tiga skenario yang diuji pada server X, dimana server tersebut sudah terintegrasi dengan server Elastic Stack. pertama adalah peneliti menyisipkan file *backdoor* di dalam jaringan, dan menjalankan *remote command* melalui powershell dengan hak akses admin. Skenario kedua peneliti menjalankan sebuah file *malware* didalam nya untuk mendapatkan informasi sistem seperti username dan password. Dan yang terakhir skenario ketiga adalah peneliti menggunakan sebuah tool hping3 yang digunakan untuk simulasi serangan DDOS. Hasilnya adalah setiap event message yang dianggap proses eksekusi mencurigakan, ketidaknormalan trafik jaringan, serta proses administrator command akan dikirimkan ke server Elastic Stack dan Kibana bisa digunakan untuk memvisualisasikan event tersebut.

Melalui penelitian ini, peneliti bermaksud mengimplementasikan sistem manajemen syslog perangkat jaringan komputer berbasis Elastic Stack yang dibuat untuk mengintegrasikan log dari perangkat jaringan yang digunakan dan notifikasi telegram guna memudahkan administrator jaringan untuk menganalisa dan mengambil tindakan dari masalah pada perangkat jaringan yang dikelola.

Peneliti memaparkan analisa dan perancangan system monitoring jaringan di lingkungan jaringan PT XYZ. Hasil dari penelitian ini adalah, terdapat beberapa tahapan perancangan sistem manajemen log di jaringan kantor, yaitu mengurutkan kebutuhan, inventaris aset, memeriksa topologi jaringan, sinkronisasi waktu , pembuatan log, pengumpulan log, pemrosesan log dan analisa log yang akan digunakan untuk notifikasi telegram.

Rumusan Masalah

Berdasarkan latar belakang di atas, rumusan dalam penelitian ini adalah sebagai berikut :

a. Bagaimana cara merancang sistem monitoring perangkat jaringan secara realtime?
b. Bagaimana metode syslog dapat digunakan untuk sistem monitoring?
c. Bagaimana menyajikan data syslog dengan baik untuk keperluan analisis ?

Tujuan dan Manfaat

Tujuan yang akan dicapai dalam penelitian ini, yaitu:

a. Merancang sistem monitoring jaringan secara realtime berbasis syslog.
b. Analisa serta merancang bot telegram untuk mengirimkan notifikasi ketika ada permasalahan perangkat jaringan.
c. Menampilkan visualisasi data syslog menggunakan Elastic Stack.

Manfaat yang akan dicapai dalam penelitian ini, yaitu:

a. Penelitian ini diharapkan dapat membantu dan mempermudah administrator dalam melakukan pemantauan, mempercepat penanganan troubleshooting serta untuk keamanan perangkat jaringan.
b. Penelitian ini diharapkan sebagai media referensi bagi peneliti selanjutnya yang nantinya menggunakan konsep dan dasar penelitian yang sama, yaitu mengenai membangun sistem monitoring jaringan komputer.

Batasan Masalah

Berdasarkan rumusan masalah diatas, maka batasan masalah dari penelitian ini adalah sebagai berikut :

a. Penelitian ini hanya meneliti sistem untuk monitoring aktivitas log pada perangkat jaringan Switch.
b. Penelitian ini hanya menjelaskan mengenai sistem perancangan monitoring jaringan berbasis syslog.
c. Penelitian ini hanya membuat sistem notifikasi bot telegram untuk monitoring login serta status interface perangkat.