Jurnal Informatika Terpadu

https://journal.nurulfikri.ac.id/index.php/JIT
ISSN ONLINE : 2460-8998

PENERAPAN *LOG ANALYZER LOG* UNTUK MENGETAHUI LALU LINTAS JARINGAN BERBASIS *ELASTICSEARCH, LOGSTASH,* DAN KIBANA

Muhammad Jafier Rama Putra[1] , Henry Saptono[2]

[1, 2]Teknik Informatika, Sekolah Tinggi Teknologi Terpadu Nurul Fikri
Jakarta Selatan, DKI Jakarta, Indonesia 12640
jafier7@gmail.com , henry@nurulfikri.ac.id

Abstract

Recent advances in information technology have changed the way people view the development of existing applications or networks. New information technology intends to help people divert time and energy to other jobs in their daily lives. What is needed for information technology is management, maintenance, and monitoring. Management, maintenance, and monitoring of information technology or computer networks and the services expected to run as expected by individuals, organizations, or institutions to assist and support work processes within the organization. This research intends to implement a log analyzer and network traffic data based on ELK Stack (Elasticsearch Logstash Kibana), which can send logs, collect logs and visualize logs from the server. The implementation of the log analyzer and network traffic data in this study uses Ubuntu 18.04 Server and Ubuntu 18.04 as a client. The results of testing the implementation of the log analyzer and network traffic data that have been carried out with a success rate of 100% show that all log tests that occur on the server can be sent in real-time to the central server of the ELK Stack.

Keywords*: Log, Information Technology, Monitoring, Network, ELK Stack*

Abstrak

Kemajuan dalam bidang teknologi informasi terkini telah mengubah cara pandang masyarakat mengenai pengembangan aplikasi atau jaringan yang ada sekarang. Sebuah teknologi informasi baru yang dimaksudkan untuk membantu manusia dalam hidup kesehariannya sehingga waktu dan tenaga dapat dialihkan pada pekerjaan lainnya. Hal yang diperlukan untuk teknologi informasi adalah pengelolaan, pemeliharaan, dan pemantauan. Pengelolaan, pemeliharaan, dan pemantauan teknologi informasi atau jaringan komputer dan layanan yang ada di dalamnya diharapkan dapat berjalan sebagaimana yang diharapkan oleh individu, organisasi atau institusi untuk membantu dan menunjang proses kerja dalam organisasi tersebut. Dalam penelitian ini bermaksud untuk melakukan implementasi *analyzer log* dan data lalu lintas jaringan berbasis ELK Stack (*Elasticsearch Logstash Kibana*) yang dapat melakukan pengiriman log, mengumpulkan log dan memvisualisasi log dari *server*. Implementasi *analyzer log* dan data lalu lintas jaringan dalam penelitian kali ini menggunakan Ubuntu 18.04 Server, dan Ubuntu 18.04 sebagai *client*. Dari hasil pengujian implementasi *analyzer log* dan data lalu lintas jaringan yang telah dilakukan dengan tingkat keberhasilan 100% menunjukan bahwa semua pengujian log terjadi pada *server* dapat dikirimkan secara *realtime* ke server utama ELK Stack.

Kata Kunci : Log, Teknologi Informasi, Pemantauan, Jaringan, ELK Stack

1. PENDAHULUAN

Pemanfaatan teknologi informasi merupakan sarana penunjang atau pendorong bagi masyarakat dalam mencapai tujuannya. Pemanfaatan teknologi yang efektif dapat meningkatkan kinerja. Kinerja berhubungan dengan pencapaian serangkaian tugas-tugas yang dilaksanakan oleh individu-individu di dalam organisasi. Sehingga semakin tinggi kinerja individu semakin meningkat pula efektifitas, produktivitas dan kualitas pelayanan individu tersebut. Hal yang diperlukan untuk teknologi informasi adalah pengelolaan, pemeliharaan, dan pemantauan dengan cara yang lebih efektif dan efisien.

Hal yang dibutuhkan keberlangsungan jaringan komputer untuk keandalan, keamanan, dan ketepatan layanan yang ada didalamnya. Untuk memastikan keandalan, keamanan, dan ketepatan maka dibutuhkan suatu proses analisis tersebut.

2. LANDASAN TEORI

2.1 Log

Diterima 15 Agustus 2021, Direvisi 13 Desember 2021, Diterima untuk publikasi 8 Maret 2022

Log adalah catatan tentang peristiwa yang terjadi dalam sistem organisasi dan jaringan. Log terdiri dari entri log; setiap entri berisi informasi yang berkaitan dengan peristiwa tertentu yang terjadi dalam sistem atau jaringan.

2.2 Analisis Log

Analisis log adalah proses mengubah data log mentah menjadi informasi untuk memecahkan masalah [8]. Sistem digital menghasilkan banyak jenis log files, yang memberikan informasi penting tentang sistem ini. Beberapa jenis file log, seperti pemantauan jaringan log, interaksi layanan web, atau penggunaan web log dieksploitasi secara luas [7].

2.3 Lalu Lintas Jaringan

Suatu jaringan dapat dikatakan *traffic*-nya padat atau tinggi, apabila banyak host yang melakukan koneksi ke *server* di dalam jaringan tersebut. Fungsi pengawasan terhadap unjuk kerja jaringan dan pengambilan tindakan untuk mengendalikan aliran trafik agar diperoleh kapasitas jaringan dengan pengoperasian yang maksimum. Manajemen lalu lintas jaringan adalah sebuah pekerjaan untuk memelihara seluruh sumber jaringan dalam keadaan baik.

2.4 *Domain Name System* (DNS)

Domain Name System (DNS) adalah *distribute database system* yang digunakan untuk pencarian nama komputer (*name resolution*) di jaringan yang mengunakan TCP/IP (*Transmission Control Protocol/Internet Protocol*) [1]. TCP/IP (*Transmission Control Protocol/Internet Protocol)* adalah sekumpulan protocol yang terdapat di dalam jaringan computer yang digunakan untuk berkomunikasi atau bertukar data antar komputer. DNS biasanya digunakan sebuah Layanan Nama Domain untuk menyelesaikan permintaan untuk nama-nama website menjadi alamat IP untuk tujuan menemukan layanan komputer serta perangkat di seluruh dunia.

2.5 *Dynamic Host Configuration Protocol* (DHCP)

DHCP (*Dynamic Host Configuration Protocol*) adalah protokol yang berbasis arsitektur *client/server* yang dipakai untuk memudahkan pengalokasian alamat IP dalam satu jaringan [2]. Kemudahannya dalam pemberian alamat IP kepada komputer *client* atau perangkat jaringan (walau dalam jumlah yang banyak) secara otomatis.

2.6 *Web Server*

Web server adalah sebuah *software* yang memberikan layanan berbasis data dan berfungsi menerima permintaan dari HTTP atau HTTPS pada *client* yang dikenal dan biasanya kita kenal dengan nama *web browser* (Mozilla Firefox, Google Chrome) dan untuk mengirimkan kembali yang hasilnya dalam bentuk beberapa halaman web dan pada umumnya akan berbentuk dokumen HTML [3]. Dalam Penggunaanya, biasanya sudah jadi satu paket dengan PHP dan MySQL diantaranya XAMPP dan *Appserv* [9].

2.7 *Elasticsearch*

Elasticsearch adalah mesin pencari *open-source* yang dibangun di atas Apache Lucene™, fulltext perpustakaan mesin pencari. Lucene bisa dibilang yang paling maju, kinerja tinggi, perpustakaan mesin pencari berfisalkan lengkap yang ada saat ini—baik sumber terbuka maupun berpemilik [4].

2.8 *Logstash*

Logstash adalah *software* gratis dan *open source* (berlisensi Apache 2.0) dan dikembangkan oleh American pengembang, Jordan Sissel dan tim dari Elastic. Mudah diatur, berkinerja, terukur dan mudah diperluas. *Logstash* memiliki berbagai macam mekanisme input: ia dapat mengambil input dari TCP/UDP, file, *Syslog*, Microsoft Windows *EventLogs*, STDIN, dan berbagai jenis sumber lain [5].

2.9 Kibana

Kibana adalah alat yang merupakan bagian dari tumpukan ELK, yang terdiri dari *Elasticsearch*, *Logstash*, dan Kibana. Itu dibangun dan dikembangkan oleh Elastic. Kibana adalah *platform* visualisasi yang dibangun di atas Elasticsearch dan memanfaatkan fungsionalitas *Elasticsearch* [6].

3. METODE PENELITIAN

3.1 Studi Literatur

Pada tahapan awal ini dilakukan dengan mencari, mengumpulkan, serta membaca artikel di *website* dan beberapa skripsi penelitian lainnya yang berhubungan dengan implementasi *analyzer log* dan lalu lintas jaringan berbasis ELK (*Elasticsearch*, Logstash, Kibana) Stack. Hasil dari studi literatur yaitu menerapkan ELK stack untuk memudahkan proses analisis data dan bagaimana penelitian harus dilakukan dan bahan apa saja yang diperlukan untuk tujuan penelitian ini agar dapat tercapai.

3.2 Pengujian dan Evaluasi

Pada tahapan ini akan dilakukan pengujian terhadap proses untuk memudahkan proses analisis data log dan data lalu lintas jaringan yang akan kita analisis dengan menggunakan ELK (*Elasticsearch*, *Logstash*, Kibana) Stack. serta mengetahui seberapa efektifitas dari manfaat log analisis dan lalu lintas jaringan. Setelah menguji dan melakukan evaluasi dari beberapa faktor, maka peneliti akan menganalisis hasil yang di dapat dari pengujian yang telah dilakukan. Pengujian ini dilakukan untuk

memberikan jawaban dari rumusan masalah, apa benar efektif atau tidaknya sistem analisis ini bekerja sebenarnya.

3.3 Rancangan Penelitian

3.3.1 Metode Pengumpulan Data

Metode pengumpulan data yang dilakukan oleh peneliti yaitu dengan metode deskriptif, metode ini akan mempelajari aspek-aspek apa yang akan di tinjau untuk mengetahui analisis implementasi *analyzer log* dan lalu lintas dalam suatu jaringan.

3.3.2 Studi Pusaka

Metode pengumpulan data dilakukan dari suatu jaringan yang akan di analisis dan diimplementasikannya berdasarkan rumusan masalah yang ada.

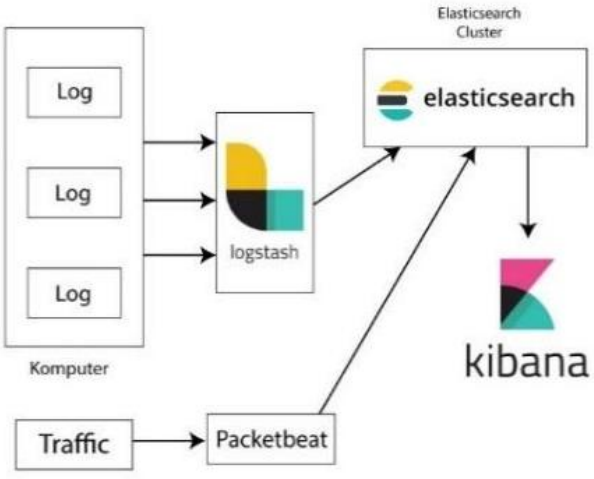
4. ANALISIS DAN PENELITIAN

4.1 Analisis Sistem

Analisis Sistem adalah menganalisa sistem yang sedang ingin di bangun yang bertujuan untuk mengetahui kebutuhan sistem dalam menganalisanya, sehingga memudahkan peneliti pada tahapan selanjutnya yaitu perancangan sistem.

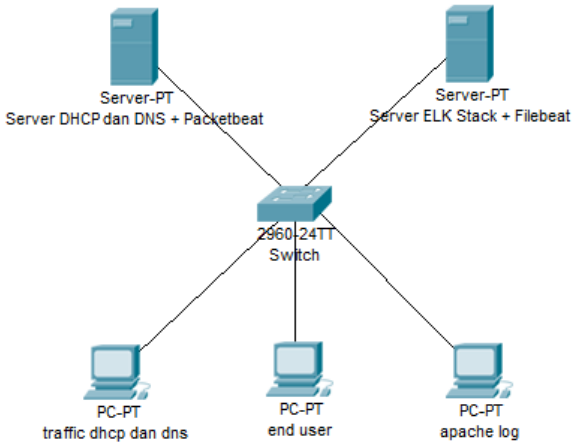
4.2 Perancangan Sistem

Perancangan sistem secara umum dilakukan dengan maksud untuk memberikan gambaran umum tentang sistem yang baru atau sistem yang akan diusulkan. Dalam penelitian ini, peneliti melakukan perancangan arsitektur sistem yang terdiri dari masing-masing menggunakan sistem operasi Linux Ubuntu Server 18.04 dan Ubuntu Desktop 18.04.



Gambar 1. Perancangan Sistem *Logic*

Perancangan sistem ini merupakan gambaran keseluruhan dari proses analisis secara fisik yang akan dijalankan. Dalam perancangan ini, digambarkan suatu sistem dengan tampilan yang *real* dalam mengimplementasikannya.



Gambar 2. Perancangan Sistem Fisik

5. HASIL DAN PEMBAHASAN

5.1 Pengujian

Pengujian ini peneliti akan memaparkan pengujian yang peneliti lakukan setelah pengimplementasian ELK Stack. Peneliti melakukan pengujian efektivitas dan Pengujian *Analyzer Log* dan Lalu lintas Jaringan berbasis ELK Stack.

Efektifitas diukur dengan cara sebagai berikut :

> Efektifitas Pengujian = (Output/Input) * 100%
>
> Rerata Efektifitas = (Total Efektifitas / Jumlah pengujian)
>
> Tingkat efektifitas ~= Rerata Efektifitas

A. Ujian Pengiriman Data Log (*Logstash - Elasticsearch*)

Pada tahap pengujian ini dilakukan pengujian untuk memeriksa apakah data log tersimpan dari logstash ke *Elasticsearch* dan akan mengirim 10 log dalam kurun waktu tertentu. Selama waktu yang di tujukan akan terlihat berapa jumlah log yang di hasilkan dan apa log akan tersimpan di *Elasticsearch*. Jadi mengirim log dari /var/log/syslog.

B. Ujian menggunakan *Shell Script* (*syslog*)

Pengujian ini menggunakan *Shell Script* untuk membantu me-*generate* isi log yang akan input ke *Elasticsearch* sesuai isi dan jumlah log-nya. *Shell Script* adalah kumpulan beberapa *command* yang ditulis pada teks file yang nantinya akan di-*execute* oleh *shell*.

Tabel 1. Pengujian Data *Log (syslog)*

Pengujian ke	Jumlah Log Input	Waktu Awal	Selisih Waktu (rata-rata) detik	Waktu Akhir	Jumlah Log yang diterima (Output)	Efektivitas
1	10	06:33:27	1	06:33:28	10	100%
2	20	06:39:10	2	06:39:12	20	100%
3	30	06:44:00	4	06:44:04	30	100%
4	40	06:48:42	6	06:48:48	40	100%
5	50	07:08:31	7	07:08:38	50	100%
6	60	07:12:36	8	07:12:44	60	100%
7	70	07:20:51	8	07:20:59	70	100%
8	80	07:23:26	8	07:23:44	80	100%
9	90	07:28:21	9	07:28:30	90	100%
10	100	07:32:11	9	07:32:20	100	100%
			Rata-rata			100%

Rerata Efektifitas =

(100% + 100% + 100% + 100% + 100% + 100% + 100% + 100% + 100% + 100%)/10 = 100%)

Tabel 2. Pengujian *Traffic Log (packetbeat)*

Pengujian ke	IP Pengirim	Port	IP Tujuan	Waktu Awal	Selisih Waktu (rata-rata) detik	Traffic	Waktu Akhir
1	192.168.1.1	9200	192.168.1.6	08:30:31	20	08:30:31	TCP
2	192.168.1.6	5601	192.168.1.3	08:42:25	-	08:42:25	TCP
3	192.168.1.6	53	192.168.1.1	08:45:40	10	08:45:50	UDP
4	192.168.1.6	5044	192.168.1.3	08:51:07	3	08:51:10	TCP

Data pengujian dapat dikatakan memiliki tingkat efektifitas **100%.**

5.2 Pengujian Log Apache menggunakan Apache Benchmarks

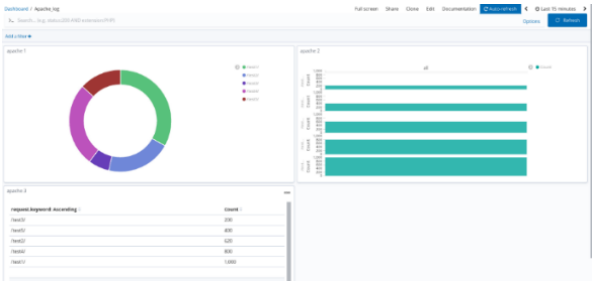
Pengujian ini menggunakan Apache Benchmark untuk mengukur kapabilitas Apache untuk melayani *request* dari *client* yang akan inputkan ke *Elasticsearch* sesuai isi dan jumlah lognya. Apache Benchmark adalah *tool* untuk mengukur kapabilitas Apache untuk melayani *request* dari *client* yang nantinya akan tertulis di Logstash dan tersimpan di *Elasticsearch*. Log tersebut akan terlihat di Kibana.

Rerata Efektifitas = (100%+100%+100%+100%+100%)/5 = 100%

Data pengujian dapat dikatakan **efektif** atau dalam persentase memiliki tingkat efektifitas **100%.**

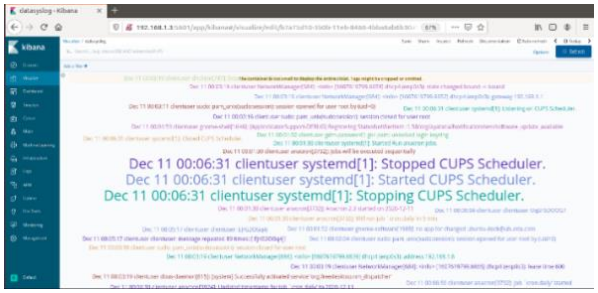
5.3 Hasil Visualisasi

- Hasil visualisasi Apache menggunakan tipe visual *Pie, Horizontal Bar, Data Table*



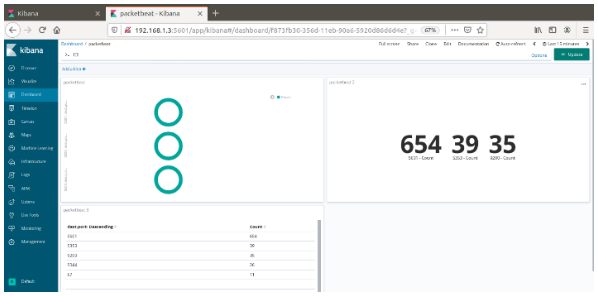
Gambar 3. Visualisasi Apache

- Hasil visualisasi *syslog* (*data log*) menggunakan tipe visual *Tag Cloud*



Gambar 4. Visualisasi *Syslog*

- Hasil visualisasi *Packetbeat* menggunakan tipe visual *Pie, Metrics, Data Table*



Gambar 5. Visualisasi *Packeybeat*

6. PENUTUP

6.1 Kesimpulan

Kesimpulan yang dapat diambil oleh peneliti dalam penelitian ini yaitu:

1. Rancangan yang dilakukan dalam implementasi ini sebagai proses untuk dapat mengelompokkan log secara tepat adalah menggunakan *Elasticsearch, Logstash* serta Kibana. Untuk rancangan sistem lalu lintas jaringan, menggunakan *Packetbeat* langsung ke *Elasticsearch* dan divisualisasikan dengan Kibana.
2. Log yang digunakan adalah log pada mesin linux dan dikirim di /var/log yang akan diproses melalui *Logstash*.
3. Efektivitas ELK Stack untuk (*syslog*) memiliki tingkat efektifitas 100%, sedangkan untuk Apache log yaitu memiliki efektifitas 100%. Kemudian untuk lalu lintas jaringan juga memiliki efektifitas 100%.

4. ELK Stack dapat menjadi solusi untuk implementasi sebuah *Log* yang membantu dalam memvisualisasikan hasil.

6.2 Saran

Beberapa saran yang dapat dilakukan untuk penelitian selanjutnya, yaitu:

1. Penelitian selanjutnya dapat diimplementasikan pada jaringan *real* atau tidak dalam lingkungan virtualisasi.
2. Penelitian ini memungkinkan dapat dikembangkan dengan jumlah data log dan menambah metode beragam dengan jumlah *node* (komputer).
3. Penelitian ini memungkinkan untuk diuji kembali dengan jumlah data lalu lintas jaringan yang lebih beragam dengan jumlah *node* (komputer) lebih banyak.

DAFTAR PUSTAKA

[1] D. Ardiantoro, "Pengantar DNS (*Domain Name System*)," 2003.

[2] M. R. Andargini, "Panduan Instalasi & *Setup* DHCP *Server*," 2008.

[3] C. Tarigan, *et al.*, "Sistem Pengawasan Kinerja Jaringan *Server Web* Apache dengan Log *Management System* ELK (*Elasticsearch, Logstash*, Kibana)," pp. 7–14, 2018.

[4] C. Gormley, Z. Tong, "*Elasticsearch: The Definitive Guide*," 2015.

[5] J. Turnbull, "*The Logstash Book*," 2014.

[6] Y. Gupta, "*Kibana Essentials*", 2015.

[7] H. Saneifar, *et al.*, "*Terminology Extraction from Log Files*," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, 2009.

[8] S. Alspaugh, *et al.*, "*Analyzing Log Analysis: An Empirical Study of User Log Mining*," LISA'14 Proc. 28th USENIX Conf. Large Install. Syst. Adm., pp. 53–68, 2014.

[9] A. Permatasari dan S. Suhendi, "Rancang Bangun Sistem Informasi Pengelolaan *Talent* Film berbasis Aplikasi Web", *J. Inform. Terpadu*, vol. 6, no. 1, hlm. 29-37, Mar 2020.

[10] D. O. Saputra dan H. Saptono, "Implementasi *Network Monitoring System* terintegrasi dengan Ticketing System menggunakan Nagios dan osTicket", *J. Inform. Terpadu*, vol. 5, no. 1, hlm. 06-17, Mar 2019