BAB IV
ANALISIS DAN PERANCANGAN

Pada bab ini, akan membahas mengenai perancangan sistem meliputi analisis kebutuhan *software*, perancangan arsitektur ELK Stack, perancangan visualisasi, perancangan pengujian dan skenario pengujian.

4.1 Analisis Sistem

Analisis kebutuhan perangkat yang dibutuhkan dalam penelitian diperlukan identifikasi terlebih dahulu. Berdasarkan skema sistem yang telah dibuat, dapat ditentukan perangkat apa saja yang dibutuhkan dalam penelitian. Pada tahap ini spesifikasi *hardware* dan *software* yang digunakan akan diidentifikasi.

4.1.2 Analisis Kebutuhan *Hardware*

Analisis kebutuhan *hardware* merupakan tahapan awal pada penelitian ini yang berguna untuk mengetahui spesifikasi *hardware* yang optimal untuk implementasi. Setiap infrastruktur IT memiliki kebutuhan perangkat keras yang berbeda-beda dan ELK Stack membutuhkan sumber perangkat keras yang cukup besar untuk instalasi di komputer lokal. Selain itu, kinerja ELK akan bergantung pada besarnya data log aktivitas dalam sistem yang akan diolah. Hal ini terbukti pada saat penulis mencoba untuk instalasi sistem ELK pada komputer lokal terjadi *crash* yang diakibatkan dari spesifikasi komputer penulis yang pada saat itu tidak memadai untuk mengeksekusi sistem ELK.

Penulis akan merancang ELK pada sistem terpisah dari web server yang menyimpan akses log sistem Elena, apabila sistem ELK tidak dipisah dengan sistem Elena maka kemungkinan akan membebani server web sistem Elena. Website resmi ELK Stack sendiri secara resmi merekomendasikan instalasi ELK dilakukan pada server fisik daripada VM (*Virtual Machine*) karena apabila dijalankan pada *hardware* yang sama dengan web server sistem, maka akan memberatkan sistem dan berisiko kehilangan data dalam lingkungan virtualisasi.

Selain itu, ELK Stack merekomendasikan agar mesin host nantinya menyediakan antara 128 GB dan 256 GB memori dan juga minimal *hardware* sebagai berikut :

a. Processor : 2 cores
b. RAM : 8 GB
c. Hardisk : 200GB

Dalam penelitian ini, penulis menggunakan laptop pribadi yang telah di *upgrade* dengan spesifikasi sebagai berikut:

a. Processor : Intel(R) Core(TM) i5-2520M CPU @2.50GHz
b. RAM : 12 GB
c. Hardisk : 200GB

4.1.3 Analisis Kebutuhan *Software*

Analisis kebutuhan *software* merupakan tahapan awal pada penelitian ini yang berguna untuk mengetahui *software* apa saja yang akan digunakan untuk implementasi. Dalam penelitian ini penulis menggunakan *software* yang dibutuhkan berdasarkan studi literatur yang berkaitan dengan penerapan atau implementasi sistem ELK Stack untuk memproses data log web server sebuah sistem. Berikut beberapa *software* yang lebih spesifik dan akan penulis gunakan :

Tabel 4.1 Analisis Kebutuhan Softtware

No.	Perangkat Lunak	Versi	Deskripsi
1.	Elasticsearch	8.11.1	Sebuah mesin pencari dan analisis untuk semua jenis data
2.	Logstash	8.11.1	Alat mengumpulkan dan mengolah data skala besar dengan *plugin input* dan *output* sebelum dikirim ke elasticsearch
3.	Kibana	8.11.1	Alat visualisasi dan manajemen data yang sudah diindexs di elasticsearch
4.	Open JDK	1.8.0	Alat yang digunakan untuk menjalankan aplikasi berbasis java (elasticsearch)

Table 4.1 Analisis Kebutuhan Software

No.	Perangkat Lunak	Versi	Deskripsi
1.	Elasticsearch	8.11.1	Sebuah mesin pencari dan analisis untuk semua jenis data
2.	Logstash	8.11.1	Alat mengumpulkan dan mengolah data skala besar dengan *plugin input* dan *output* sebelum dikirim ke elasticsearch
3.	Kibana	8.11.1	Alat visualisasi dan manajemen data yang sudah diindexs di elasticsearch
4.	Open JDK	1.8.0	Alat yang digunakan untuk menjalankan aplikasi berbasis java (elasticsearch)
5.	Apache Web Server	2.4.29	Web server untuk mendapatkan halaman *website* yang di *request* oleh komputer *client*
6.	Web Browser Chrome	109.0.5414.119	Menampilkan dashboard kibana berbasis website
7.	Rsync	3.3.3	Utilitas yang berguna untuk melakukan sinkronisasi file dan direktori antar sistem atau server
8.	Cronjob	2.2.0	Menjadwalkan tugas secara otomatis
9.	SSHpass	1.06	Mengotomasi input password pada SSH
10.	*Shell Script*	1.00	Berisi kumpulan baris tugas dalam *script* untuk otomatis

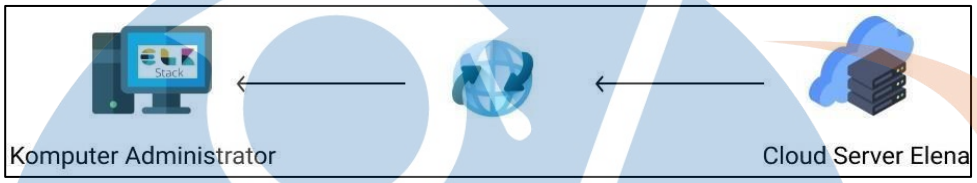
Beberapa *software* tersebut dipilih berdasarkan hasil rekomendasi dari jurnal terkait dan semua *software* di bawah dapat diunduh dari internet dan tidak berbayar. *Software* yang akan dibutuhkan adalah elasticsearch, logstash, kibana, open jdk, apache web server, SSHpass, *Rsync*, *Shell Script*, cronjob dan *browser*.

4.2 Perancangan Sistem

Perancangan sistem yang akan dibuat memerlukan identifikasi tentang rancangan arsitektur sistem ELK, arsitektur sistem fisik dan arsitektur sistem logik dari sistem yang akan dibangun.

4.2.1 Perancangan Arsitektur Sistem

Pada perancangan arsitektur sistem ini akan menjelaskan bagaimana rancangan dari visualisasi data akses log web Elena menggunakan ELK Stack.



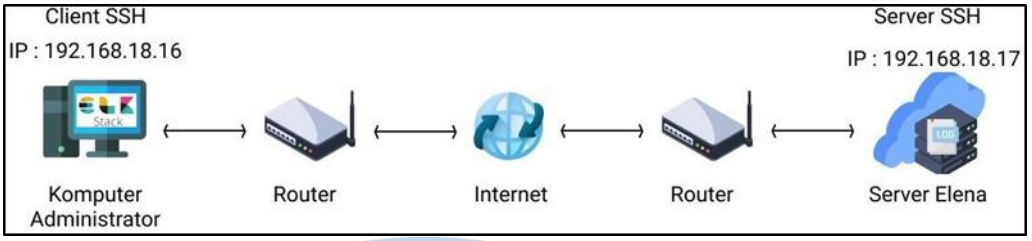
Gambar 4.2 Rancangan Arsitektur SIstem (Sumber:www.flaticon.com)

Dalam penelitian ini, penulis akan melakukan perancangan arsitektur sistem dimana komputer yang sudah di install ELK dan terhubung jaringan internet akan memproses data akses log web server sistem Elena yang terdapat pada *cloud server*. Data akses log yang akan diunduh otomatis menggunakan pola unduhan per *batch* yang artinya log yang sudah dihasilkan oleh server elena akan diunduh dan disinkronisasikan ke komputer lokal. Sistem ELK akan dipasang di komputer terpisah dengan komputer yang menyimpan akses log sistem Elena agar tidak memberatkan server sistem Elena.

Pada perancangan ini penulis juga akan menggunakan metode otomatisasi dalam mengunduh data akses log sistem Elena dari server ke komputer lokal. Otomatisasi pengunduhan dengan cara melakukan sinkronisasi tanpa interaksi dengan pengguna dengan rentang waktu tertentu agar *file* log dikirimkan dan diproses ke sistem ELK untuk kemudian dapat divisualisasikan. Hasil visualisasi yang sudah dibuat berguna untuk analisis dan untuk mendapatkan informasi penting yang terdapat pada log.

4.2.2 Perancangan Arsitektur Sistem Fisik

Gambar dibawah ini adalah gambar perancangan arsitektur sistem fisik.



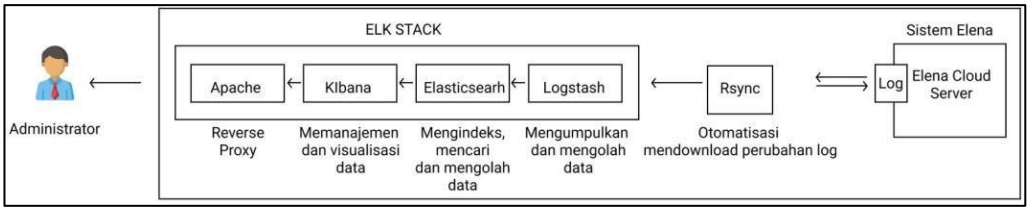
Gambar 4.3 Rancangan Arsitektur Sistem Fisik (Sumber:www.flaticon.com)

Pada gambar diatas berisi tentang perancangan arsitektur sistem fisik dan dijelaskan bahwa :

a. Komputer administrator (*client*) yang sudah terpasang ELK Stack dan terhubung dengan router yang terkoneksi internet akan berkomunikasi dengan server elena secara jarak jauh (*remote*).
b. Komputer *client* yang telah terhubung secara *remote* selanjutnya akan disinkronisasikan untuk otomatis mengunduh data akses log beserta perubahan yang terjadi pada data akses log web Elena yang berada di *cloud* server.
c. Setelah *file* akses log web Elena otomatis diunduh, kemudian log tersebut akan ditransmisikan ke *logstash* untuk disimpan ke elasticsearch.
d. Data akses log yang sudah tersimpan pada Elasticsearch selanjutnya akan divisualisasikan di kibana.

4.2.3 Perancangan Arsitektur Sistem Logik

Gambar dibawah ini adalah gambar perancangan arsitektur sistem logik:



Gambar 4.4 Rancangan Arsitektur Sistem Logik (Sumber : www.flaticon.com)

Pada gambar diatas berisi tentang perancangan arsitektur sistem fisik dan dijelaskan bahwa :

a. Pada penelitian ini sistem ELK Stack yang sudah terpasang dandikonfigurasi akan berkomunikasi dengan server elena secara jarak jauh menggunakan akses *SSH*.

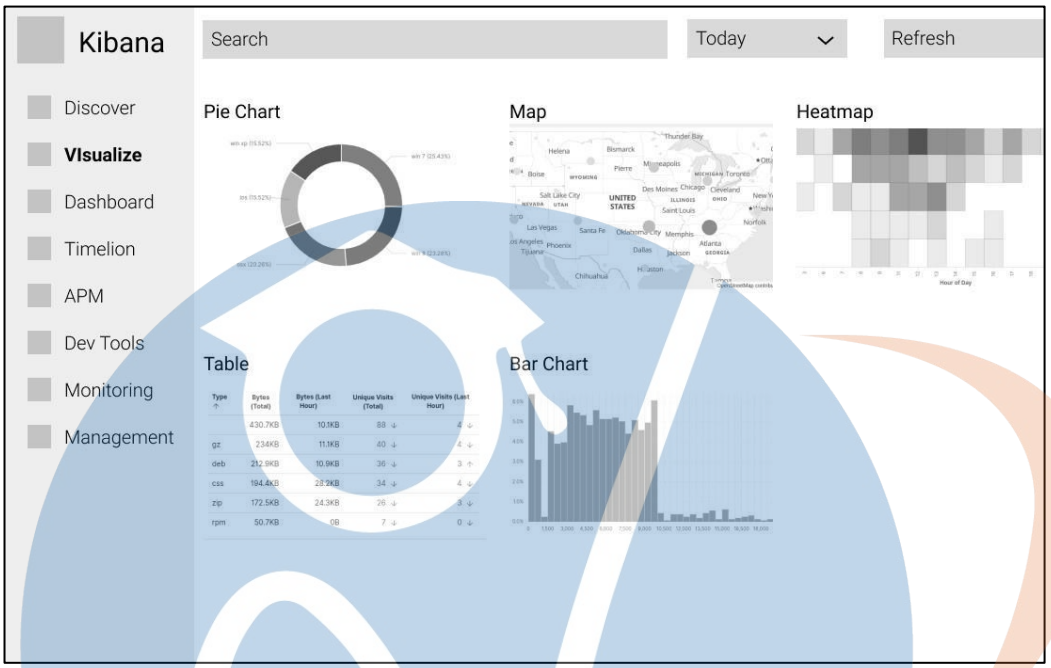
b. Setelah mendapatkan akses ke server sistem Elena, selanjutnya mengimplementasikan *rsync* berbasis *SSH* untuk mengunduh data dan sinkronisasi *file* akses log Elena beserta perubahan yang terjadi pada log secara otomatis bersama dengan autentikasi *password serve*r secara otomatis yakni menggunakan SSHpass.

c. Data akses log yang sudah diunduh selanjutnya di kirim dengan mengedit *file* konfigurasi *apache.conf* yang ada pada logstash untuk kemudian hasilnya akan dikirim ke elasticsearch untuk dilakukan pengindeksan data.

d. Setelah dilakukan pengindeksan data akses log, selanjutnya data akan di visualisasi di kibana dalam bentuk diagram/*chart* yang ditampilkan berbasis dashboard *website.*

4.3 Perancangan Visualisasi

Gambar dibawah ini adalah gambar perancangan visualisasi kibana:



Gambar 4.5 Rancangan Visualisasi (Sumber : www.elastic.co)

Perancangan visualisasi data akses log sistem Elena yaitu dengan memvisualisasikan data di dashboard kibana. Visualisasi yang ada pada dashboard tersebut nantinya akan menampilkan data akses log Elena dalam bentuk grafik/diagram yang berisi informasi statistik maupun informasi penting lainnya. Visualisasi di rancang dengan menggunakan sumber *field* data yang sudah terindeks di elasticsearch. Selain itu terdapat fitur aggregasi dan *filter* untuk megatur secara mandiri data yang akan di munculkan pada kibana.

Perancangan diagram visualisasi yang akan dibuat akan memuat datasebagai berikut :

Table 4.3 Rancangan Visualisasi

No.	Nama Visualisasi	Jenis Visualisasi	Informasi	Sumber
1.	*Visits*	*Goal*	Statistik data informasi total seluruh pengguna	- *clientp*
2.	*Unique Visitors*	*Gauge*	Statistik data informasi pengguna secara rinci	- *clientip*
3.	*Bytes Total*	*Table*	Statistik total *bytes* yang terekam per *request* di akses log	- *bytes* - *url*
4.	*Method Access*	*Pie Charts*	Statistik berdasarkan metode akses website	- *verb.keyword*
5.	*Response HTTP*	*Table*	Statistik data informasi *Response HTTP* pada sistem oleh pengguna	- *response.keyword*
6.	*Most Used Browser and OS*	*Pie Charts*	Statistik data informasi *web browser* dan sistem operasi yang banyak digunakan pengguna	- *agent.keyword*
7.	*Top 10 Ip Address*	*Bar Char*	Statistik data informasi sistem operasi yang banyak digunakan Pengguna	- *clientip*
8.	*Top 5 Url*	*Pie Charts*	Statistik data informasi *Url* yang paling banyak di kunjungi	- *referer,keyword*

Table 4.3 Rancangan Visualisasi

9	*Data Timeseries* (Perjam)	*Line Chart*	Statistik data informasi aktifitas pengguna pada periode waktu tertentu dan lebih rinci	- *timestamp* *elena*
10	*Traffic Log* (Perbulan)	*Line Chart*	Statistik data informasi jumlah total kunjungan perbulan	- *timestamp* *elena*

4.4 Perancangan Pengujian

Dalam penelitian ini, penulis akan melakukan perancangan pengujian visualisasi menggunakan *Black-Box testing* (pengujian fungsionalitas). Secara umum pengujian fungsional adalah pengujian yang dilakukan untuk mengetahui apakah sistem telah berfungsi efektif dan sesuai dengan rancangan yang telah dibuat. Singkatnya pengujian ini digunakan untuk mengetahui apakah proses *input* dan *output* sudah sesuai dan data log berhasil dikirim ke ELK. Pengujian ini dilakukan untuk menjawab rumusan masalah penulis.

Sistem ELK Stack yang telah dirancang, selanjutnya akan dilakukan pengujian apakah sistem bekerja efektif secara terus menerus dan handal. Pengujian ini untuk mengetahui apakah sistem tersebut berhasil menyalin akses log, menyimpan dan memvisualisasikan log. Berikut adalah tabel perancangan pengujian visualisasi sistem.

Table 4.4 Perancangan Pengujian

No.	Deskripsi Pengujian	Jumlah Batch File Akses Log	Banyak Percobaan
1.	Akses log Elena berhasil dikirim ke ELK stack	10 batch akses log	10x percobaan
2.	Akses log berhasil divisualisasikan ke ELK Stack	10 visualisasi diagram akses log	10x percobaan

Table 4.5 Perancangan Pengujian Indexing Akses Log di ELK

No.	Jumlah Log (input)	Jumlah Log (output)	Waktu Awal	Waktu Akhir	Hasil Uji	Persentase
1.	50.000 log	50.000 log	07.00.01	07.02.08	Berhasil menyalin	100 %
2.	50.000 log					
3.	50.000 log					
4.	50.000 log					
5.	50.000 log					
6.	50.000 log					
7.	50.000 log					
8.	50.000 log					
9.	50.000 log					
10.	24061 log					

Tabel 4.5 Perancangan Pengujian Visualisasi Akses Log di ELK

No.	Pengujian	Deskripsi	Jenis Visualisasi	Hasil Uji	Persentase
1.	*Visits*	Menampilkan visualisasi *Visits* padaKibana	*Goal*	Berhasil menampilkan	100 %
2.	*Unique Visitors*	Menampilkan visualisasi *Visitors* pada Kibana	*Gauge*		
3.	*Bytes Total*	Menampilkan visualisasi *Bytes Total* pada Kibana	*Table*		
4.	*Method Access*	Menampilkan visualisasi *Method Access* pada Kibana	*Pie Charts*		
5.	*Response HTTP*	Menampilkan visualisasi *Response HTTP* pada Kibana	*Table*		
6.	*Most Used Browser and OS*	Menampilkan visualisasi *Bytes Total* pada Kibana	*Pie Charts*		
7.	*Top 10 Ip Address*	Menampilkan visualisasi *Top 10 IpAddress* pada Kibana	*Bar Char*		
8.	*Top 5 Url*	Menampilkan visualisasi *Top 5 Url* pada Kibana	*Pie Charts*		

Table 4.5 Perancangan Pengujian Visualisasi Akses Log di ELK

9.	*Data Timeseries* (perjam)	Menampilkan visualisasi data *timeseries* perjam	*Line Chart*	Berhasil menampilkan	100 %
10.	*Traffic Log* (perbulan)	Menmpilkan visualisasi data jumlah *traffic* log perbulan	*Line Chart*	Berhasil menampilkan	100 %