



DAFTAR ISI

DAFTAR TABEL	ix
DAFTAR GAMBAR	ix
PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Tujuan	2
1.3 Manfaat	2
1.4 Ruang Lingkup	2
METODE KERJA	3
2.1 Lokasi dan Waktu PKL	3
2.2 Metode Bidang Kajian	3
2.2.1 Analisis	3
2.2.2 Pembuatan Topologi	4
2.2.3 Konfigurasi Server	4
2.2.4 Konfigurasi Client	4
2.2.5 Pengujian	4
KEADAAN UMUM	4
3.1 Sejarah	4
3.2 Struktur Organisasi	5
3.3 Fungsi dan Tujuan	6
3.4 Visi dan Misi	6
IMPLEMENTASI LOG EVENT MANAGEMENT SERVER MENGGUNAKAN ASTICSEARCH LOGSTASH KIBANA (ELK STACK)	7
4.1 Analisis Masalah	7
4.2 Pembuatan Topologi	7
4.3 Konfigurasi Server	9
4.3.1 Konfigurasi Server Pusat ELK-Stack	9
4.4 Konfigurasi Client	18
4.4.1 Konfigurasi Server Client Centos	18
4.4.2 Visualisasi dan Dashboard	24
4.4.3 Export File Dengan CSV	29
4.5 Pengujian	32
4.5.1 Pengujian Kegagalan Login	32
4.5.2 Pengujian Keberhasilan Login	34
4.5.3 Pengujian Kesalahan Login Dengan Username	35
4.5.4 Pengujian Ketepatan Waktu	36
4.5.5 Pengujian Penghapusan Log	37
4.5.6 Pengujian Penyerangan Brute Force Tanpa Fail2ban	38
4.5.7 Pengujian Penyerangan Brute Force Menggunakan Fail2ban	39
SIMPULAN DAN SARAN	42
5.1 Simpulan	42

© Hak cipta milik IPB (Institut Pertanian Bogor)



Sekolah Vokasi
College of Vocational Studies

Bogor Agricultural University

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:

a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.

b. Pengutipan tidak merugikan kepentingan yang wajar IPB.

2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin IPB.



5.2	Saran	42
DAFTAR PUSTAKA		43

DAFTAR TABEL

1	Hardware dan Software	7
2	Tabel Visualisasi Pada Kibana	24
3	Hasil dari Pengujian	41

DAFTAR GAMBAR

1	Tahapan Metode Kajian	3
2	Struktur Organisasi Direktorat Informasi Kepabeanaan dan Cukai	6
3	<i>Topologi Elk Stack</i>	8
4	Menonaktifkan Fitur <i>SELinux</i>	9
5	Melakukan <i>Stop</i> dan <i>Disable Firewall</i>	10
6	Melakukan Instalasi <i>Java 8</i>	10
7	Instalasi <i>ELK Stack</i>	11
8	Konfigurasi <i>Elasticsearch</i>	11
9	Konfigurasi <i>Elasticsearch.service</i>	12
10	Konfigurasi <i>Elasticsearch Memory</i>	12
11	Konfigurasi <i>Elasticsearch Reload Systemd</i>	12
12	Konfigurasi <i>Kibana</i>	12
13	Konfigurasi <i>Enable Start Kibana</i>	13
14	Konfigurasi <i>Nginx</i>	13
15	Konfigurasi Direktori <i>Nginx</i> Membuat Penyimpanan Baru <i>Kibana.conf</i>	13
16	Konfigurasi <i>Basic Authentication</i>	14
17	Konfigurasi Untuk Memulai <i>Nginx</i>	14
18	Konfigurasi <i>filebeat-input.conf</i>	14
19	Konfigurasi <i>output.conf</i>	15
20	Konfigurasi <i>remove-grokparse.conf</i>	15
21	Konfigurasi <i>removebeatscodec.conf</i>	16
22	Konfigurasi <i>ssh-filter.conf</i>	17
23	Konfigurasi <i>Openssl.cnf</i>	17
24	Konfigurasi Sertifikat <i>SSL</i>	18
25	Konfigurasi <i>Boot</i> dan <i>Start Service Logstash</i>	18
26	Konfigurasi <i>Logstash-Forwarder.crt</i>	18
27	Konfigurasi Firewall Client	19
28	Konfigurasi <i>SELinux Client</i>	19



Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar IPB.

2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin IPB.



Konfigurasi <i>SSL Client Centos</i>	20
Konfigurasi Membuat Direktori Dan Menyimpan <i>SSL</i>	20
Proses Importelastic Key Dan Download <i>Filebeat</i>	20
Konfigurasi <i>Filebeat</i> Baris 21 dan 26	20
Konfigurasi <i>Filebeat</i> Baris 83 dan 85	21
Konfigurasi <i>Output.Logstash</i>	21
Konfigurasi <i>Boot dan Start Service Filebeat</i>	22
<i>Install Fail2ban</i>	22
Konfigurasi <i>Start Fail2ban</i>	22
Konfigurasi <i>Fail2ban jail.conf</i>	22
Konfigurasi Pengaturan <i>Banned</i> dan Percobaan Masuk	23
Restart <i>Fail2ban</i>	24
Konfigurasi <i>Sshd.local</i>	24
Klik Tombol Plus pada <i>Visualize</i>	25
<i>Visualize Kibana</i>	25
Tags <i>Ssh</i> Gagal <i>Login</i>	26
Tags <i>Ssh</i> Gagal <i>Login User</i>	26
Tags <i>Ssh</i> Gagal <i>Login Password</i>	27
Tags <i>Ssh</i> Sukses <i>Login</i>	27
Presentase <i>SSH</i> Sukses <i>Log</i>	28
Tags Presentase <i>Ssh</i> Gagal	28
<i>Dashboard LEMS Kibana</i>	29
Memasukkan <i>Tags</i> Ke <i>Dashboard</i>	29
Save Data Di <i>Kibana</i>	29
Laporan <i>CSV</i> Pada <i>Kibana</i>	30
Download file <i>Csv</i>	30
Hasil <i>Download Csv</i>	31
Kegagalan <i>Login SSH Client 1</i>	32
Kegagalan <i>Login SSH Client 2</i>	32
Kegagalan <i>Login SSH Client 3</i>	32
Kegagalan <i>Login SSH Client 4</i>	33
Kegagalan <i>Login SSH Client 5</i>	33
Tampilan <i>Dashboard Kibana SSH</i> Gagal <i>Login</i>	33
Sukses <i>Login</i> Pada <i>Client 1</i>	34
Sukses <i>Login</i> Pada <i>Client 2</i>	34
Sukses <i>Login</i> Pada <i>Client 3</i>	34
Sukses <i>Login</i> Pada <i>Client 4</i>	34
Sukses <i>Login</i> Pada <i>Client 5</i>	34
<i>Dashboard Kibana Ssh</i> Sukses <i>Login</i>	34
Kesalahan <i>Login Username</i> <i>Sangga</i>	35
Kesalahan <i>Login Username</i> <i>Pripambudi</i>	35

© Hak cipta milik IPB (Institut Pertanian Bogor)

Bogor Agricultural University



Sekolah Vokasi
College of Vocational Studies

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:

a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.

b. Pengutipan tidak merugikan kepentingan yang wajar IPB.

2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin IPB.



70	Kesalahan <i>Login Username</i> Teknik	35
71	Kesalahan <i>Login Username</i> IPB	35
72	Kesalahan <i>Login Username</i> Komputer	35
73	<i>Dashboard</i> Kesalahan <i>Login User</i>	36
74	Pengujian Kesalahan <i>Login</i> Dan Waktu Kejadian	36
75	Hasil Waktu Kejadian Pada <i>Server-ELK</i>	36
76	Percobaan Peghapusan <i>Log</i> Pada Client 1	37
77	Hasil Visualisasi Setelah <i>Log</i> Dihapus	37
78	Menghapus <i>Log</i> ssh sukses <i>login</i> pada Kibana	38
79	<i>Tags</i> telah terhapus di Kibana	38
80	<i>Dashboard</i> Pada <i>Log</i> Kibana	38
81	Percobaan Penyerangan <i>Brute Force</i>	39
82	Hasil Penyerangan yang Dilakukan	39
83	Penyerangan brute-force Dengan Fail2ban	40
84	<i>Fail2band Status</i>	40
85	Hasil <i>Fail2band</i> di <i>Kibana</i>	40

© Hak cipta milik IPB (Institut Pertanian Bogor)



Sekolah Vokasi
College of Vocational Studies

Bogor Agricultural University

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:

a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.

b. Pengutipan tidak merugikan kepentingan yang wajar IPB.

2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin IPB.



1 PENDAHULUAN

1.1 Latar Belakang

Kementerian Keuangan (Kemenkeu) merupakan kementerian negara di lingkungan Pemerintah Indonesia yang membidangi urusan keuangan dan kekayaan negara, Kementerian Keuangan berkedudukan di bawah dan bertanggungjawab kepada Presiden. Kementerian Keuangan terdiri atas beberapa subbagian dan masing-masing tersebut memiliki tugas pokok yang berbeda-beda. Direktorat Informasi Kepabeanaan Dan Cukai (DIKC) mengendalikan segala pusat data dan sistem teknologi informasi mengenai DIKC. DIKC memegang peranan penting untuk menjaga stabilitas jaringan. DIKC sendiri memiliki kantor cabang sebanyak 136 yang terdapat di setiap provinsi di Indonesia yang di dalamnya memiliki server sebagai penyedia layanan. Server melayani seluruh client atau *workstation* yang terhubung ke jaringannya dan merupakan perangkat utama dalam sistem komunikasi jaringan berfungsi sebagai penyedia layanan dan memiliki *log* yang sangat banyak. Masalah yang sering dialami seorang administrator jaringan harus secara manual untuk melakukan pembacaan *log service*. *Log service* berfungsi untuk mencatat semua aktivitas yang berjalan pada sistem operasi dalam hal ini server dan harus berinteraksi langsung dengan server yang memakan waktu cukup lama. Masalah lainnya yaitu server yang harus berjalan 24 jam penuh yang dapat menghasilkan *log service* dalam jumlah banyak. Manajemen *log* adalah proses yang dilakukan untuk mengelola dan memfasilitasi pembuatan, transmisi, analisis, penyimpanan, pengalihan, dan penbuahan akhir volume besar data *log* yang dibuat dalam sistem informasi. *Log*, dalam konteks komputasi, adalah dokumentasi peristiwa yang dihasilkan secara otomatis dan bertanda waktu yang relevan dengan sistem tertentu. Hampir semua aplikasi dan sistem perangkat lunak menghasilkan *file log*.

Manajemen *log* yang efektif sangat penting untuk keamanan. Pemantauan, dokumentasi, dan analisis peristiwa sistem merupakan komponen penting. Perangkat lunak manajemen *log* mengotomatiskan banyak proses yang terlibat. *Event log manager* (ELM), misalnya, melacak perubahan dalam infrastruktur jaringan. Belum tersedianya *Log Event Management Server* yang sudah terintegrasi dengan *elasticsearch logstash kibana* di DIKC Kementerian Keuangan membuat data *log* pada server menjadi tidak terorganisasi dengan baik. Berdasarkan permasalahan diatas, maka perlu dibuatnya suatu *log event management server* yang mampu meringankan dan memudahkan dalam membaca sekaligus menganalisis *log service* pada server. Dalam hal ini *Elasticsearch Logstash Kibana* (ELK Stack) merupakan komponen yang tepat dalam membangun log event management yang dapat memberi informasi kepada sistem administrator mengenai tren, statistik, dan anomali yang terjadi.

ELK Stack dirancang untuk digunakan sebagai solusi terintegrasi Elasticsearch adalah sebuah platform berbasis opensource yang dibangun diatas Apache Lucene, distributable, dan merupakan mesin pencari dan pengindeksan. Proses pencarian pada elasticsearch dibatasi oleh alamat url dan kueri nya hanya berbeda dalam kondisi filter





Sekolah Vokasi
College of Vocational Studies

© Hak cipta milik IPB (Institut Pertanian Bogor)

Bogor Agricultural University



Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar IPB.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin IPB.