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.
© Hak cipta milik IPB (Institut Pertanian Bogor)
Bogor Agricultural University

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 Kepabeanan 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 lainya yaitu server yang harus berjalan 24 jam penuh yang dapat menghasilkan *log service* dalam jumlah banyak. Manajemen *log* adalah proses yang digunakan untuk mengelola dan memfasilitasi pembuatan, transmisi, analisis, penyimpanan, pengarsipan, dan pembuangan 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*.

Sekolah Vokasi
College of Vocational Studies

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 teroganisasi 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