EKSPLORASI SPLUNK UNTUK MEMBANGUN DASHBOARD DAN ALERT BERDASARKAN DATA SYSLOG (STUDI KASUS: DATA CENTER PT. TELEKOMUNIKASI INDONESIA)

TUGAS AKHIR

Disusun sebagai salah satu syarat untuk kelulusan Program Strata 1, Program Studi Teknik Informatika, Universitas Pasundan Bandung

oleh:

Rizal Putra Ramadhan
nrp. 12.304.0463

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS PASUNDAN BANDUNG
AGUSTUS 2015
DAFTAR ISI

ABSTRAK .........................................................................................................................i
ABSTRACT ..........................................................................................................................ii
KATA PENGANTAR ............................................................................................................iii
DAFTAR ISI ..........................................................................................................................iv
DAFTAR TABEL .....................................................................................................................vi
DAFTAR GAMBAR ...............................................................................................................vii

BAB 1 PENDAHULUAN

1.1 Latar Belakang ..............................................................................................................1-1
1.2 Perumusan Masalah .....................................................................................................1-2
1.3 Batasan Masalah ..........................................................................................................1-2
1.4 Tujuan Tugas Akhir .....................................................................................................1-2
1.5 Metode Pelaksanaan Tugas Akhir ..............................................................................1-2
1.6 Sistematika Penulisan Tugas Akhir ...........................................................................1-3

BAB 2 LANDASAN TEORI

2.1 Data .............................................................................................................................2-1
   2.1.1 Data Mesin .............................................................................................................2-1
2.2 Syslog ..........................................................................................................................2-3
   2.2.1 Kode Fasilitas ......................................................................................................2-4
   2.2.2 Severity ...............................................................................................................2-5
   2.2.3 Protokol Jaringan ...............................................................................................2-6
2.3 Splunk ..........................................................................................................................2-6
   2.3.1 History Splunk .....................................................................................................2-7
   2.3.2 Produk Splunk .....................................................................................................2-7
   2.3.3 Lisensi ...............................................................................................................2-8
   2.3.4 Pengguna Splunk ...............................................................................................2-8
2.4 Pusat Data ....................................................................................................................2-8
   2.4.1 Perancangan Pusat Data Yang Ideal ................................................................2-8
   2.4.2 Service Utama Pada Data Center ...................................................................2-9
   2.4.3 Tier pada Pusat Data ........................................................................................2-11
   2.4.4 Next Generation Data Center .........................................................................2-12
2.5 Dashboard ....................................................................................................................2-14
   2.5.1 Manfaat Dashboard .........................................................................................2-14

BAB 3 EKSPLORASI SPLUNK

3.1 Kerangka Tugas Akhir ...............................................................................................3-1
3.2 Splunk ..........................................................................................................................3-4
3.2.1 Splunk Enterprise .......................................................... 3-4
3.2.2 Fitur Splunk Enterprise .................................................. 3-4
3.2.3 Komponen Splunk Enterprise ........................................... 3-6
3.2.4 Pengguna Splunk .......................................................... 3-8
3.2.5 Fungsi Utama Splunk ...................................................... 3-9
3.3 Jenis Data Splunk yang Bisa Dibaca .................................... 3-10
3.3.1 Data Input ................................................................. 3-10
3.3.2 Data Source ................................................................. 3-10
3.3.3 Indeks Data Splunk ....................................................... 3-12
3.4 Dashboard .................................................................. 3-13
3.4.1 Fitur Dashboard ............................................................. 3-14
3.4.2 Fungsi Search Pada Dashboard ..................................... 3-15
3.5 Alert ..................................................................... 3-16
3.5.1 Skenario Alert ............................................................. 3-17

BAB 4 STUDI KASUS
4.1 Tinjauan Umum ............................................................... 4-1
4.2 Sistem Yang Sedang Berjalan ............................................. 4-1
4.3 Kebutuhan Pengembangan Sistem .................................... 4-2
4.3.1 Model Topology ............................................................. 4-2
4.3.2 Kebutuhan Hardware ...................................................... 4-2
4.3.3 Kebutuhan Software ...................................................... 4-4
4.4 Instalasi Splunk ............................................................... 4-5
4.4.1 System Requirement ....................................................... 4-5
4.4.2 Lisensi Splunk ............................................................... 4-7
4.4.3 Memulai Instalasi Splunk ............................................. 4-7
4.5 Koneksi Data Syslog ......................................................... 4-11
4.5.1 Koneksi Data Log BRAS ............................................. 4-12
4.6 Membuat Dashboard ....................................................... 4-13
4.7 Membuat Alert ............................................................... 4-15

BAB 5 KESIMPULAN DAN SARAN
5.1 Kesimpulan ................................................................. 5-1
5.2 Saran ............................................................... 5-1

DAFTAR PUSTAKA .............................................................. 6-1
DAFATAR TABEL

Tabel 2.1 Tipe Data Mesin [SPL14B] .................................................................................. 2-2
Tabel 2.2 Kode Fasilitas ....................................................................................................... 2-4
Tabel 2.3 Tingkat Severity .................................................................................................... 2-5
Tabel 2.4 Aspek-aspek Pusat Data ....................................................................................... 2-9
Tabel 2.5 Tier pada Pusat Data ............................................................................................ 2-11
Tabel 3.1 Kerangka Tugas Akhir ......................................................................................... 3-1
Tabel 3.2 Field Splunk .......................................................................................................... 2-13
Tabel 4.1 Kinerja Model Single Server ................................................................................ 4-1
Tabel 4.2 Unix Operating System ......................................................................................... 4-5
Tabel 4.3 Hardware Requirement Indexer ............................................................................ 4-5
Tabel 4.4 Hardware Requirement Collector (forwarder) ....................................................... 4-6
Tabel 4.5 Disk Partition Server Indexer ................................................................................ 4-6
Tabel 4.6 Disk Partition Server Collector (forwarder) .......................................................... 4-6
DAFTAR GAMBAR

Gambar 2.1 Data Mesin [SPL14A] .................................................................................2-2
Gambar 2.2 Servis Utama Data Center .................................................................2-9
Gambar 2.3 Data Berupa Angka ..............................................................................2-14
Gambar 2.4 Dashboard Interaktif ...........................................................................2-14
Gambar 3.1 Skema Splunk .......................................................................................3-3
Gambar 3.2 Indexing Splunk [ZIO15]......................................................................3-4
Gambar 3.3 Pivot [SPL14D] .......................................................................................3-5
Gambar 3.4 Panel Dashboard [ASM13] .................................................................3-6
Gambar 3.5 Apps Splunk .........................................................................................3-6
Gambar 3.6 Forwarder dan Reciever Splunk [ZIO15] ...........................................3-7
Gambar 3.7 Indexer Splunk [DAT13] .......................................................................3-7
Gambar 3.8 Search head dan Search Peer Splunk [SPL14E] ...............................3-8
Gambar 3.9 Data Source File dan Direktori ............................................................3-11
Gambar 3.10 Data Source UDP .............................................................................3-11
Gambar 3.11 Data Source Script ..........................................................................3-12
Gambar 3.12 Karakteristik Indeks Splunk ............................................................3-12
Gambar 3.13 Dashboard ..........................................................................................3-13
Gambar 3.14 Fitur Dashboard ................................................................................3-14
Gambar 3.15 Search Dashboard .............................................................................3-16
Gambar 4.1 Model Single Server ...........................................................................4-1
Gambar 4.2 Model Multiple Server .......................................................................4-2
Gambar 4.3 Server Indexer .....................................................................................4-3
Gambar 4.4 Server Collector (forwarder) ..............................................................4-3
Gambar 4.5 UTP Cat6 ............................................................................................4-3
Gambar 4.6 Switch .................................................................................................4-4
Gambar 4.7 Download Splunk ...............................................................................4-7
Gambar 4.8 Instalasi Splunk Sebagai Indexer .......................................................4-8
Gambar 4.9 Web Splunk ........................................................................................4-9
Gambar 4.10 Antarmuka Splunk ..........................................................................4-9
Gambar 4.11 Instalasi Splunk Sebagai Forwarder ..............................................4-9
Gambar 4.12 Status Splunk Forwarder .................................................................4-10
Gambar 4.13 Splunk Stop dan Start .......................................................................4-10
Gambar 4.14 Splunk Restart ..................................................................................4-11
Gambar 4.15 Ping Splunk ke BRAS .......................................................................4-11

vii
Gambar 4.16  Ping BRAS ke Splunk .................................................................4-11
Gambar 4.17  Konfigurasi BRAS .................................................................4-12
Gambar 4.18  Log pada BRAS .................................................................4-12
Gambar 4.19  Cek Log pada Forwarder ..................................................4-13
Gambar 4.20  Cek Log pada Search Head ..............................................4-13
Gambar 4.21  Query Search .................................................................4-14
Gambar 4.22  Konfigurasi Panel Dashboard ...........................................4-14
Gambar 4.23  Tampilan Dashboard BRAS ..................................................4-15
Gambar 4.24  Konfigurasi Email Splunk ..................................................4-15
Gambar 4.25  Query Search .................................................................4-16
Gambar 4.26  Konfigurasi Alert ...............................................................4-16
Gambar 4.27  Konfigurasi Email ...............................................................4-17
Gambar 4.28  Notifikasi Email ...............................................................4-17