# BAB 3
# PELAKSANAAN KERJA MAGANG

## 3.1 Kedudukan dan Koordinasi

Pelaksanaan kerja magang pada PT Global Innovation Technology sebagai *Technical Consultant* pada departemen *operation* di bawah pimpinan *Chief Operating Officer* dan *VP Operation*. Pengembangan dan pemeliharaan *platform* Splunk dilakukan bersama Bapak Rizki sebagai *VP Operation* dan Bapak Wahyu sebagai *Project Manager*, dan Bapak Akmal sebagai Senior *Technical Consultant*. Proses pelaksanaan, dipantau langsung dan dilakukan evaluasi oleh Bapak Aditya Pratama yang merupakan *Chief Executive Officer* dari PT Global Innovation Technology.

Seluruh koordinasi dilakukan melalui *website* internal dari PT Global Innovation Technology yang dihasilkan dari *meeting* besar departemen *operation* untuk menentukan *goals* selanjutnya. Juga, kebutuhan *support*, penambahan fitur, dan pemeliharaan yang diinginkan klien dari PT Bursa Efek Indonesia semua dilakukan melalui *Google Meet*, *Gmail* dan *WhatsApp*.

## 3.2 Tugas yang Dilakukan

Tugas yang diberikan selama melaksanakan program kerja magang yaitu pengembangan dan pemeliharaan *platform* Splunk dari PT Bursa Efek Indonesia. Pengembangan dan pemeliharaan disebut sebagai kegiatan *mock*. Kegiatan *mock* dilakukan pada hari Jumat dan Sabtu di gedung Cyber-1. Penjabaran kegiatan *mock* adalah sebagai berikut.

1. Skenario Implementasi

   Skenario Implementasi adalah proses menambah atau mengubah fitur baru pada platform Splunk. Ini dapat mencakup penambahan dashboard, visualisasi data, integrasi dengan sistem lain, dan pembuatan laporan khusus. Tim akan berkumpul setiap Jumat pukul 17.00 WIB untuk melakukan skenario Implementasi ini. Saat ini dialokasikan secara khusus untuk mempelajari kebutuhan baru, membuat solusi, dan menerapkannya ke platform Splunk. Proses ini memastikan bahwa platform Splunk terus berubah sesuai dengan perubahan.

2. *Fallback*

   *Fallback* adalah proses pemulihan atau pengembalian ke kondisi sebelumnya jika terjadi kegagalan atau masalah pada skenario implementasi yang baru dilakukan. Ini merupakan langkah yang penting untuk memastikan bahwa platform Splunk tetap stabil dan berfungsi setelah terjadinya perubahan. *Fallback* dilakukan setiap hari Sabtu pukul 09.00 WIB. Waktu ini dipilih agar jika terjadi masalah pada skenario implementasi yang dilakukan pada hari Jumat, tim memiliki cukup waktu untuk menanganinya sebelum pengguna aktif menggunakannya.

3. *Pre-live*

   *Pre-Live* adalah tahap persiapan sebelum perubahan atau fitur baru diperkenalkan ke dalam lingkungan produksi atau digunakan oleh pengguna akhir secara aktif. Ini adalah tahap penting yang memungkinkan tim untuk melakukan uji coba akhir, memvalidasi bahwa semua fitur dan perubahan berfungsi, dan memastikan bahwa tidak ada masalah yang mungkin terjadi saat fitur tersebut aktif digunakan oleh pengguna. Tahap ini dilakukan setelah tiga kali kegiatan *mock*, jika semua telah terbukti sesuai pada saat *Proof of Concept*. Dengan demikian, *pre-live* adalah langkah terakhir sebelum fitur atau perubahan benar-benar diluncurkan secara resmi.

## 3.3 Uraian Pelaksanaan Magang

Pelaksanaan kerja magang dilakukan dari bulan Januari 2024 hingga Juni 2024 seperti pada Tabel 3.1.

Tabel 3.1. Pekerjaan yang dilakukan tiap minggu selama pelaksanaan kerja magang

| Minggu Ke - | Pekerjaan yang dilakukan |
|---|---|
| 1 | Perkenalan, *briefing*, dan penentuan tim proyek |
| 2 | Mempelajari sistem dari Splunk dan mendapatkan sertifikasi resmi dari Splunk |
| 3 | Mengerjakan *courses* dari Splunk dan mendapatkan sertifikasi resmi dari Splunk |
| 4 | Eksperimen untuk membuat tampilan *dashboard* dari Splunk dan menerapkan yang sudah dipelajari |
| 5 | Pelatihan intensif dari Splunk *Expert* terkait Splunk *Core* dan Splunk *Enterprise Security* |
| 6 | Pelatihan intensif dari Splunk *Expert* dan mempelajari dokumen proyek perusahaan yang terdahulu |
| 7 | Pelatihan intensif dari Splunk *Expert* dan mempelajari dokumen proyek perusahaan yang terdahulu |
| 8 | Instalasi *Virtual Machine* untuk setup Splunk di *environment* kantor |
| 9 | Mempelajari cara *ingest data* ke dalam *platform* Splunk dan Pelatihan Splunk bersama Splunk *Expert* |
| 10 | Instalasi *Active Directory* ke dalam Splunk *Cloud Platform* di *environment* kantor dan *briefing* untuk melakukan penugasan kegiatan *mock* di PT Bursa Efek Indonesia |
| 11, 12, 13 | Melakukan kegiatan *mock* untuk melakukan implementasi fitur dan *fallback* Skenario Implementasi dari PT Bursa Efek Indonesia |
| 14 | Membuat *dashboard* untuk *client* dan eksplorasi *WhatsApp API* |
| 15, 16, 17, 18 | Implementasi WhatsApp API untuk membuat *Chatbot* dengan integrasi ke OpenAI API |
| 19 | Eksplorasi terkait Splunk dan produk lainnya yang berkaitan dengan *tools monitoring* |
| 20, 21, 22 | Eksplorasi terkait Elastic Stack dan implementasi ke *server* kantor untuk *Proof Of Concept* kepada pihak manajemen dan *sales* |

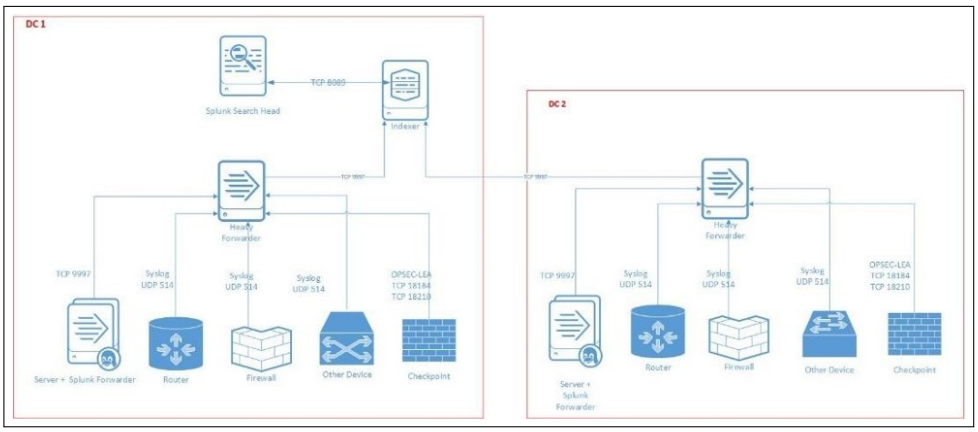
### 3.3.1 Mempelajari dokumen dan tools yang digunakan

Pelaksanaan magang diawali dengan pembelajaran dokumen dan *tools* yang digunakan dalam pengembangan dan pemeliharaan sistem pada PT Bursa Efek Indonesia. Dokumen yang dipelajari mencakup berbagai aspek mulai dari *history* yang pernah dilakukan sampai dengan *system architecture*. Proses pembelajaran didampingi oleh pembimbing lapangan dan senior *technical consultant* terkait cara pemakaian dan konfigurasi. *Tools* yang dipelajari berasal dari *environment* kantor dan disediakan menyerupai *tools* yang dipakai oleh klien. Berikut merupakan dokumen dan *tools* yang dipakai.

**A. Dokumen**

- Splunk *System Architecture* di PT Bursa Efek Indonesia

  Splunk *System Architecture* di PT Bursa Efek Indonesia memiliki dua *Data Center* yang terpisah dinamakan DC1 dan DC2. Setiap *Data Center* memiliki kegunaannya masing-masing untuk menjalankan *service* dari aplikasi yang dibangun oleh klien.




Gambar 3.1. Splunk *System Architecture* di PT Bursa Efek Indonesia

Di dalam DC1 pada Gambar 3.2 terdapat tiga *IP Address* yang memiliki fitur Splunk dan 30 *hostname* dan *30 IP Address* yang berbeda, setiap *IP Address* memiliki tugasnya masing-masing. Dari tiga puluh *hostname* dan tiga puluh *IP Address* tersebut terdapat empat aplikasi yang menjadi fokus utama dari *service* yang *existing* yaitu JATS/INET, Remote Trading, Server Smarts, dan Datafeed.

| Hostname | IP | JATS/INET |
|---|---|---|
| XPMDCTRDSEQMA | 10. | done |
| XPMDCTRDSEQBU | 10. | done |
| XPMDCTRDSEQRS | 10. | done |
| XPMDCTRDDBEMA | 10. | done |
| XPMDCTRDSVR01 | 10. | done |
| XPMDCTRDSVR02 | 10. | done |
| XPMDCTRDSVR03 | 10. | done |
| XPMDCTRDSVR04 | 10. | done |
| XPMDCTRDSVR05 | 10. | done |
| XPMDCTRDSVR06 | 10. | done |
| XPMDCTRDSVR07 | 10. | done |
| XPMDCTRDSVR08 | 10. | done |
| XPMDCTRDSVR09 | 10. | done |
| XPMDCTRDSVR10 | 10. | done |
| XPMDCTRDSVR11 | 10. | done |
| Hostname | | Remote Trading |
| XPMDOREMFIX01 | 10.1 | done |
| XPMDOREMFIX02 | 10.1 | done |
| XPMDOREMFIX03 | 10.1 | done |
| XPMDOREMQUO01 | 10.1 | done |
| XPMDOREMQUO02 | 10.1 | done |
| Hostname | | Server Smarts |
| XPMDCSUVOSK01 | 10. | done |
| XPMDCSUVOSK02 | 10. | done |
| XPCBDSUVAPL01 | 10.1 | done |
| XPCBDSUVAPL02 | 10.1 | done |
| Hostname | | Datafeed |
| XPMDCDFDDCO01 | 10.1 | done |
| XPMDCDFDDCO02 | 10.1 | done |
| XPMDCDFDDD101 | 10.1 | done |
| XPMDCDFDDD102 | 10.1 | done |
| XPMDCDFDDD103 | 10.1 | done |

Gambar 3.2. *List server* pada DC1

Berikut merupakan Splunk *System Architecture* di dalam DC1 yang ditampilkan pada Gambar 3.1.

- 1 Splunk *Search Head*

  Fungsi dari satu *IP Address* yang berperan sebagai Splunk *Search Head* adalah sebagai wadah untuk menerima permintaan pencarian dari *user* dan mengirimkannya ke dalam indeks yang sesuai untuk dieksekusi. Setiap *query* yang diminta akan dikirimkan ke dalam *indexer*, lalu ketika sudah sesuai maka akan ditampilkan hasil dari *query* yang diminta.

- 1 *Indexer*

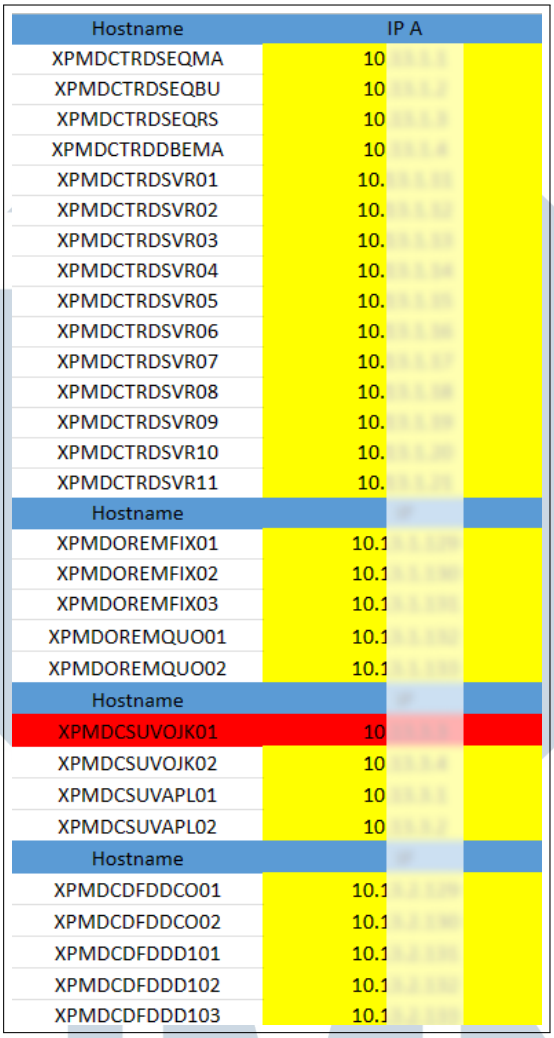
  Fungsi dari satu *IP Address* yang berperan sebagai Splunk *Indexer* adalah sebagai penyimpan data. *Indexer* bertanggung jawab untuk menerima, memproses, dan menyimpan *raw* data yang dikirimkan dari berbagai *devices* yang sudah dihubungkan. *Indexer* juga berfungsi

sebagai pengelompokan data berdasarkan *sourcetype*-nya, dan sebagai replika data agar ketika terjadi kegagalan di suatu *hardware* ataupun jaringan, data tetap tersedia dan dapat ditampilkan.

- 1 Heavy *Forwarder*

  Fungsi dari satu *IP Address* yang berperan sebagai Splunk *Heavy Forwarder* adalah sebagai pengumpul dan *routing* data. *Heavy Forwarder* bertanggung jawab untuk mengumpulkan data dari berbagai sumber, termasuk *log file*, *database*, perangkat jaringan, dan aplikasi yang terhubung dari *devices* klien. *Heavy Forwarder* melakukan pemrosesan awal terhadap data yang dikumpulkannya sebelum dikirim ke *Indexer*. Dalam Gambar 3.1 dapat dilihat bahwa seluruh *devices* yang ada pada DC1 dari *server*, *Router*, *Firewall*, dan lain-lain, disambungkan satu arah ke dalam *Heavy Forwarder* terlebih dahulu agar alur dalam *routing data* dapat berjalan dengan efisien dan optimal.

Di dalam DC2 pada Gambar 3.3 hanya terdapat satu *IP Address* yang memiliki fitur Splunk dan tiga puluh *hostnames* dan 30 *IP Address* yang berbeda. Tiga puluh *IP Address* memiliki tugasnya masing-masing di dalam proses kerja bisnis dari PT Bursa Efek Indonesia.



| Hostname | IP A |
|---|---|
| XPMDCTRDSEQMA | 10 |
| XPMDCTRDSEQBU | 10 |
| XPMDCTRDSEQRS | 10 |
| XPMDCTRDDBEMA | 10 |
| XPMDCTRDSVR01 | 10. |
| XPMDCTRDSVR02 | 10. |
| XPMDCTRDSVR03 | 10. |
| XPMDCTRDSVR04 | 10. |
| XPMDCTRDSVR05 | 10. |
| XPMDCTRDSVR06 | 10. |
| XPMDCTRDSVR07 | 10. |
| XPMDCTRDSVR08 | 10. |
| XPMDCTRDSVR09 | 10. |
| XPMDCTRDSVR10 | 10. |
| XPMDCTRDSVR11 | 10. |
| Hostname | |
| XPMDOREMFIX01 | 10.1 |
| XPMDOREMFIX02 | 10.1 |
| XPMDOREMFIX03 | 10.1 |
| XPMDOREMQUO01 | 10.1 |
| XPMDOREMQUO02 | 10.1 |
| Hostname | |
| XPMDCSUVOJK01 | 10 |
| XPMDCSUVOJK02 | 10 |
| XPMDCSUVAPL01 | 10 |
| XPMDCSUVAPL02 | 10 |
| Hostname | |
| XPMDCDFDDCO01 | 10.1 |
| XPMDCDFDDCO02 | 10.1 |
| XPMDCDFDDD101 | 10.1 |
| XPMDCDFDDD102 | 10.1 |
| XPMDCDFDDD103 | 10.1 |

Gambar 3.3. *List server* pada DC2

Berikut merupakan Splunk *System Architecture* di dalam DC2 yang ditampilkan pada Gambar 3.1.

- 1 *Heavy Forwarder*

  Fungsi dari satu *IP Address* yang berperan sebagai Splunk *Heavy Forwarder* adalah sebagai pengumpul dan *routing* data. *Heavy Forwarder* bertanggung jawab untuk mengumpulkan data dari berbagai sumber, termasuk *log file*, *database*, perangkat jaringan, dan aplikasi yang terhubung dari *devices* klien. *Heavy Forwarder* melakukan pemrosesan awal terhadap data yang dikumpulkannya sebelum dikirim ke *Indexer*. Dalam Gambar 3.1 dapat dilihat bahwa seluruh *devices* yang ada pada DC2 dari *server*, *Router*, *Firewall*, dan lain-lain,

disambungkan satu arah ke dalam *Heavy Forwarder* terlebih dahulu agar alur dalam *routing data* dapat berjalan dengan efisien dan optimal.

Namun, *Heavy Forwarder* yang ada pada DC2 disambungkan ke *Indexer* pada DC1 agar ketika *IP Address* dari Splunk *Search Head* diakses, data yang ada pada DC2 dapat ditampilkan juga karena ditampung pada *Indexer* yang ada di DC1.

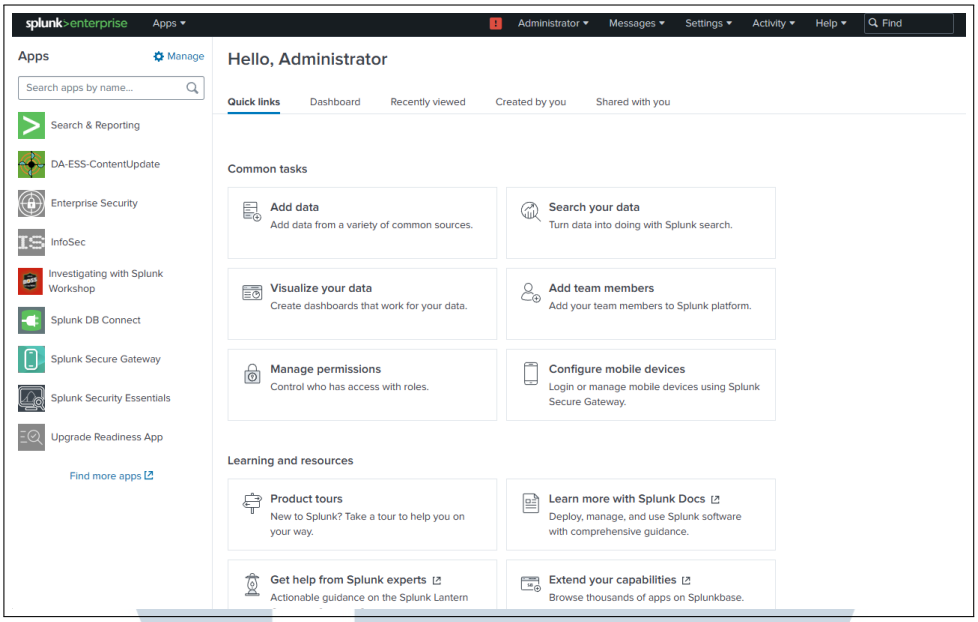
## B. *Tools*

- Splunk Enterprise

Splunk Enterprise berguna sebagai platform analitik data yang digunakan untuk mengumpulkan, mencari, memvisualisasikan, dan menganalisis data dari berbagai sumber dalam skala besar. Berikut merupakan fitur-fitur yang dipakai dalam proses *training* untuk persiapan ke proyek PT Bursa Efek Indonesia.


Gambar 3.4. Logo Splunk

Di halaman pertama Splunk *Enterprise* pada Gambar 3.5, yang juga dikenal sebagai Splunk *Home*, terdapat berbagai aplikasi yang digunakan untuk mengelola dan menganalisis data perusahaan. Aplikasi-aplikasi ini memberikan akses cepat ke fitur-fitur kunci yang dibutuhkan oleh pengguna untuk memulai proses pencarian, analisis, dan visualisasi data. Berikut merupakan detail dari Splunk *Home*.




Gambar 3.5. Splunk *Home Page*

1. *Search and Reporting*

   *Search and Reporting* merupakan titik awal yang paling umum digunakan oleh pengguna Splunk. Ini menyediakan antarmuka pencarian yang kuat dan intuitif yang memungkinkan pengguna untuk mencari, menyaring, dan menganalisis data dari berbagai sumber. Pengguna dapat menggunakan bahasa pencarian Splunk untuk menemukan informasi yang relevan, membuat laporan, dan membuat visualisasi secara grafik.

2. *Dashboard*

   *Dashboard* memungkinkan pengguna untuk membuat dan mengatur *dashboard custom* yang berisi visualisasi data yang penting. *Dashboard* ini dapat menampilkan metrik kinerja, tren, dan statistik kunci dari data yang dilakukan *indexing* oleh Splunk.

3. *Alerts*

   *Alerts* memungkinkan pengguna untuk membuat aturan peringatan yang otomatis memberi tahu ketika kondisi tertentu terpenuhi dalam data. Ini membantu perusahaan dalam mendeteksi dan menanggapi peristiwa penting secara *real-time*, seperti ancaman keamanan atau masalah operasional.

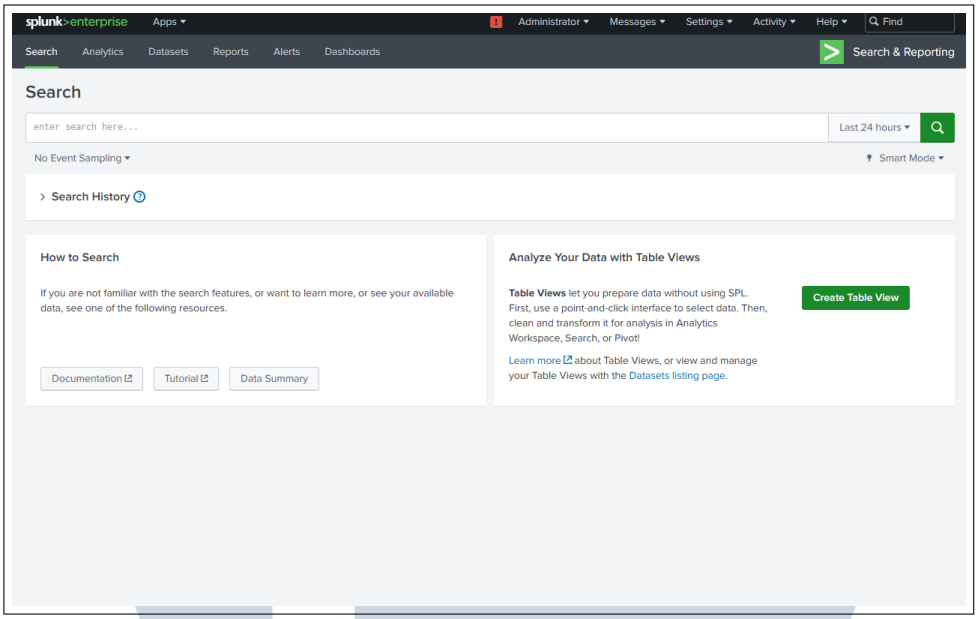
4. *Settings*

menyediakan akses ke berbagai pengaturan konfigurasi dan manajemen sistem Splunk. Ini mencakup manajemen pengguna, manajemen izin, konfigurasi *index*, integrasi dengan sistem eksternal, dan lain-lain.

5. *Apps*

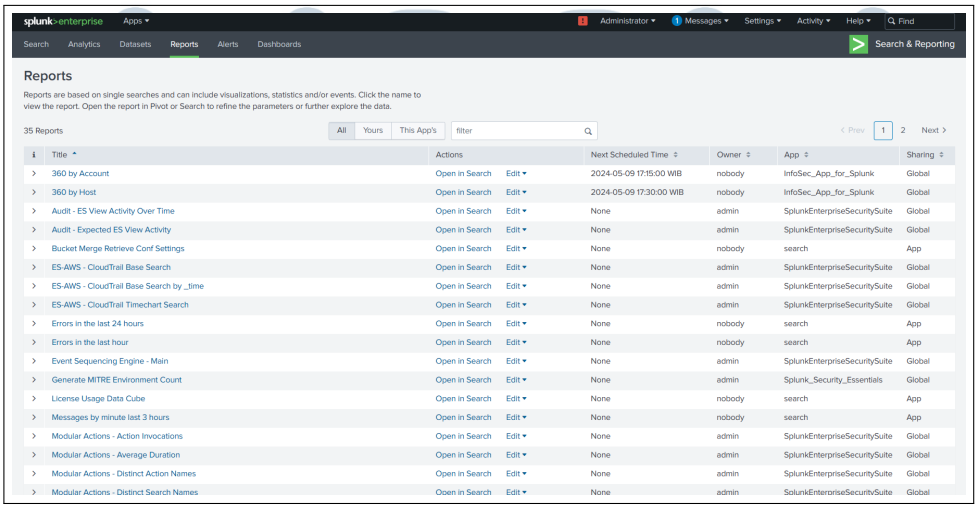
   *Apps* memungkinkan pengguna untuk mengelola aplikasi tambahan yang ditambahkan ke lingkungan Splunk. Ini bisa berupa aplikasi resmi dari Splunk, aplikasi pihak ketiga yang dikembangkan oleh vendor atau komunitas, atau aplikasi *custom* yang dibuat secara internal. Aplikasi ini dapat menyediakan fungsionalitas tambahan, integrasi dengan teknologi lain, atau solusi khusus untuk kasus penggunaan tertentu.

Splunk *Search and Reporting* pada Gambar 3.6 adalah salah satu fitur utama yang digunakan untuk mencari, menyaring, dan menganalisis berbagai data yang diperoleh dari berbagai sumber dalam lingkungan *monitoring*. Pada Gambar 3.6 menampilkan antarmuka Splunk yang menampilkan *search bar* yang memungkinkan pengguna untuk melakukan *query* data berdasarkan *time frame* yang diinginkan. Pengguna dapat dengan cepat menyesuaikan rentang waktu untuk mencari data historis atau data *real-time*, memungkinkan pengguna untuk secara efektif memonitor peristiwa saat terjadi atau menganalisis tren sepanjang waktu. Selain itu, fitur *search history* juga disertakan dalam tampilan antarmuka ini, memungkinkan pengguna untuk melihat daftar *query* yang sudah pernah dilakukan sebelumnya. Ini membantu pengguna untuk mengakses kembali *query-query* yang sering digunakan atau merujuk kembali pada analisis sebelumnya. Dengan demikian, pengguna dapat menghemat waktu dan usaha dalam mencari kembali *query* yang relevan atau meneruskan analisis sebelumnya.




Gambar 3.6. Splunk *Search and Reporting*

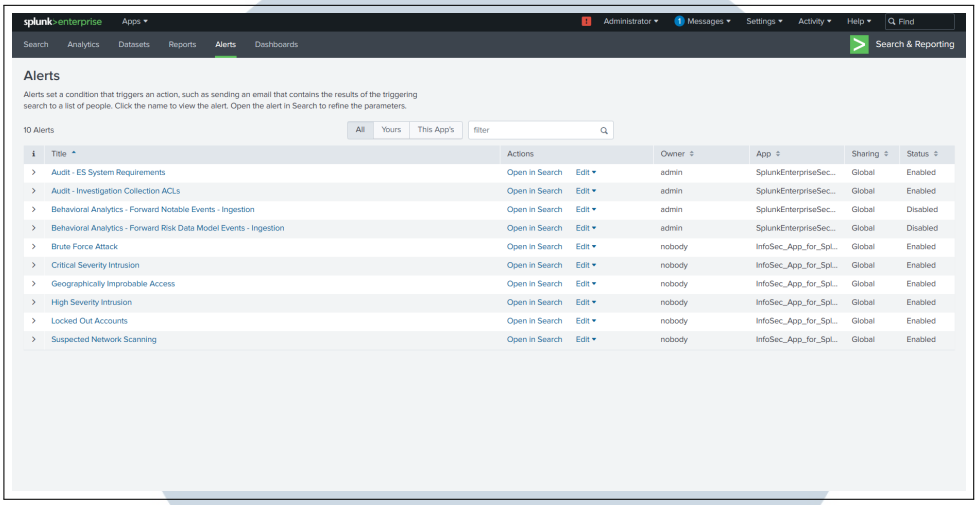
Splunk *Reports* pada Gambar 3.7 adalah wadah untuk menyimpan, menganalisis, ataupun memantau *query* yang sudah disimpan oleh *user* dari Splunk *Search and Reporting* menggunakan *"Save as Report"*. Fitur ini digunakan untuk memudahkan dalam menampilkan data yang repetitif, sehingga *query* tidak dilakukan secara berulang.




Gambar 3.7. Splunk *Reports*

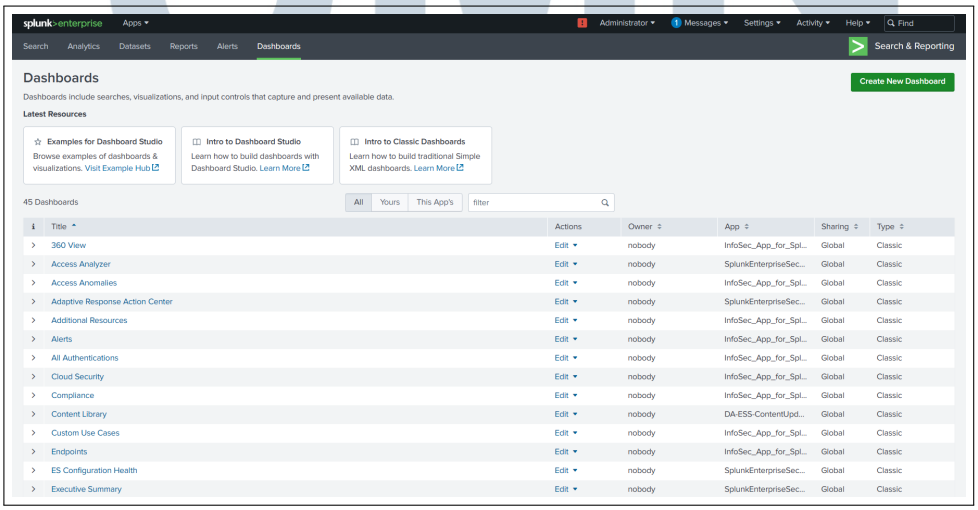
Pada Gambar 3.8 merupakan tampilan dari Splunk *Alerts*. Di dalam suatu perusahaan fitur ini berfungsi untuk melakukan tindakan preventif sesuai kasus atau kondisi yang diinginkan. Biasanya pada suatu perusahaan

*Alerts* mengirim pesan notifikasi jika suatu kinerja sistem, aplikasi, atau infrastruktur suatu perusahaan terjadi peningkatan beban kerja, penurunan kerja, atau mencapai batas kapasitas tertentu.



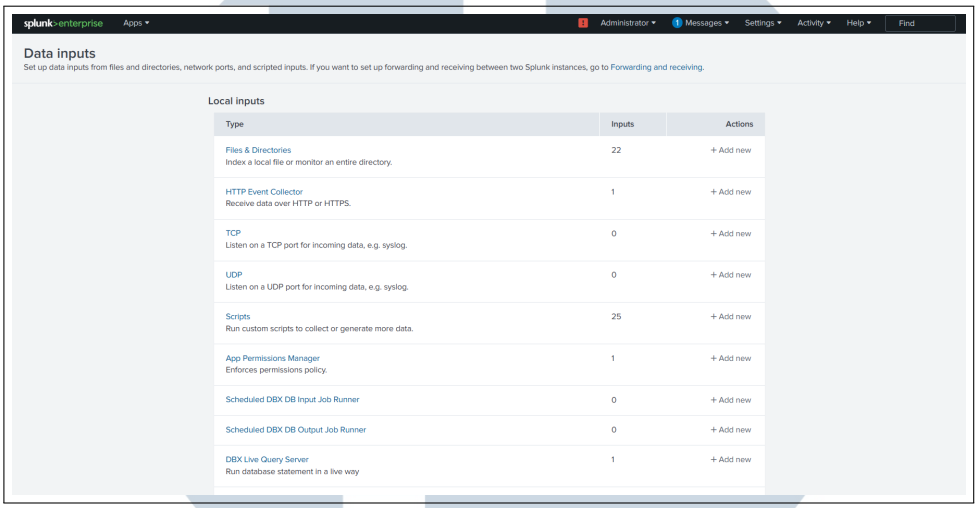

Gambar 3.8. Splunk *Alerts*

Pada Gambar 3.9 merupakan tampilan dari Splunk *Dashboards*. Fitur ini merupakan halaman yang mengumpulkan semua *dashboard* yang telah dibuat oleh *user*. *Dashboard* dibuat secara manual oleh *user* berdasarkan kegunaannya masing-masing dari *query* yang dibuat oleh *user*. Data akan ditampilkan secara visual yang memungkinkan *user* untuk mempresentasikan data dengan cara yang mudah dimengerti dan mudah diakses. Kegunaan dari Splunk *Dashboards* dalam suatu perusahaan mencakup berbagai aspek operasional, analitis, dan pengambilan keputusan.



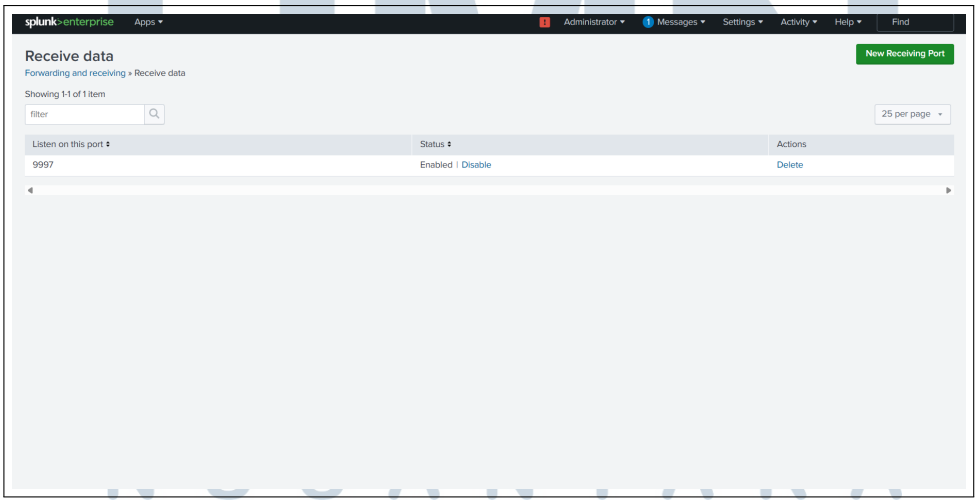

Gambar 3.9. Splunk *Dashboards*

Splunk *Data Inputs* pada Gambar 3.10 adalah halaman untuk *user* melihat kuantitas dari data yang sudah di-*ingest*. Splunk *Data Inputs* menghitung dan mengkategorisasi berdasarkan *sourcetype* ataupun *protocol* dari suatu data diambil.




Gambar 3.10. Splunk *Data Inputs*

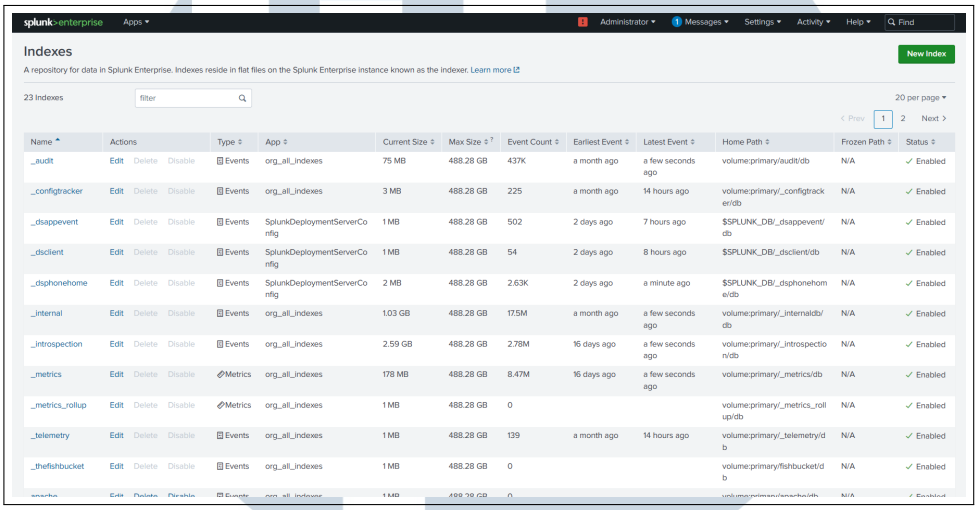
Splunk *Receive Data* pada Gambar 3.11 merupakan halaman untuk mengaktifkan ataupun menonaktifkan *Port* 9997. *Port* 9997 adalah *port default* yang ditetapkan oleh Splunk agar *server* dapat menerima data. Ditetapkan juga oleh Splunk, ketika *port* 9997 terbuka maka *server* tersebut berperan sebagai *Indexer*.




Gambar 3.11. Splunk *Receive Data*

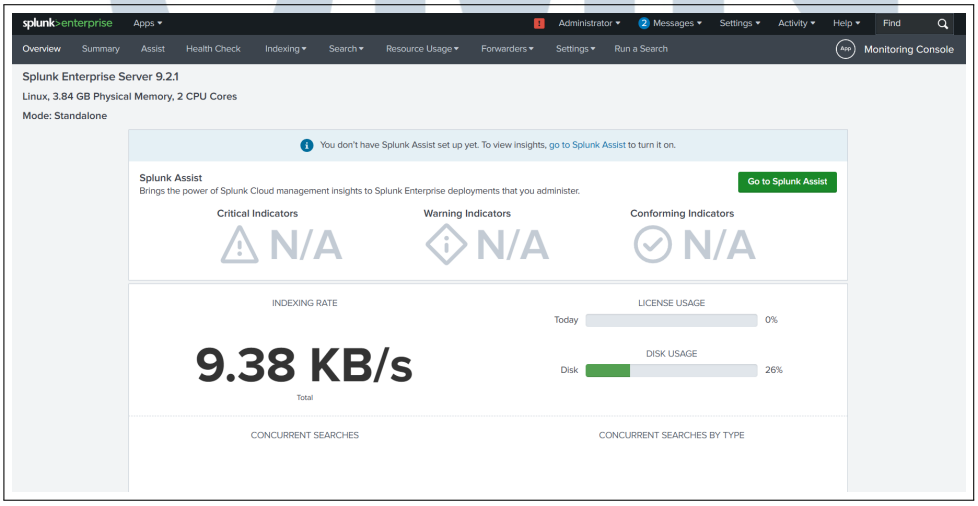
Splunk *Indexes* pada Gambar 3.12 adalah struktur penyimpanan yang digunakan oleh Splunk untuk menyimpan dan melakukan *indexing* data

yang dikumpulkan dari berbagai sumber. Setiap *index* berisi data yang dianalisis dan diolah untuk kemudian digunakan dalam pencarian, analisis, dan visualisasi. Biasanya ketika suatu *Indexer* ingin menerima data maka *user* akan membuat *index* baru sesuai dengan kategori dari sumber data yang diambil.



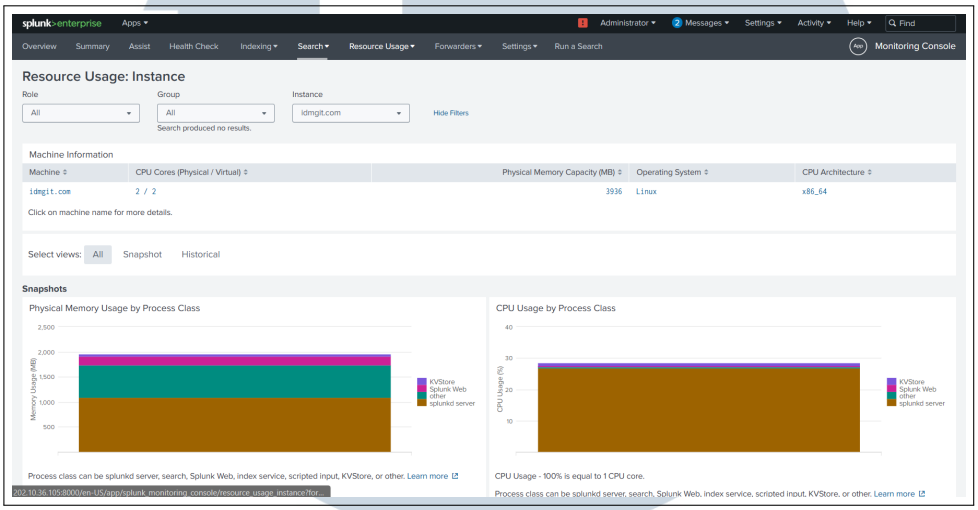

Gambar 3.12. Splunk *Indexes*

Splunk *Monitoring Console* pada Gambar 3.13 adalah *platform* untuk memantau, menganalisis, dan mengelola kesehatan serta kinerja *environment* dari *devices* yang dilakukan *monitoring*. Biasanya, Splunk *Monitoring Console* digunakan untuk memantau kesehatan sistem, melihat metrik dari *device* terkait, visualisasi kesehatan, manajemen kapasitas, dan manajemen konfigurasi.




Gambar 3.13. Splunk *Monitoring Console*

Splunk *Monitoring Resource Usage* pada Gambar 3.14 adalah fitur lanjutan dari Splunk *Monitoring Console*. Fitur berfungsi untuk membantu memahami atau memvisualisasikan *devices* yang terkait dengan Splunk. Biasanya, dalam suatu perusahaan Splunk *Monitoring Resource Usage* digunakan untuk melihat sumber daya agar bisa memantau optimasi kinerja, perencanaan kapasitas, deteksi masalah kinerja, dan pengelolaan biaya.



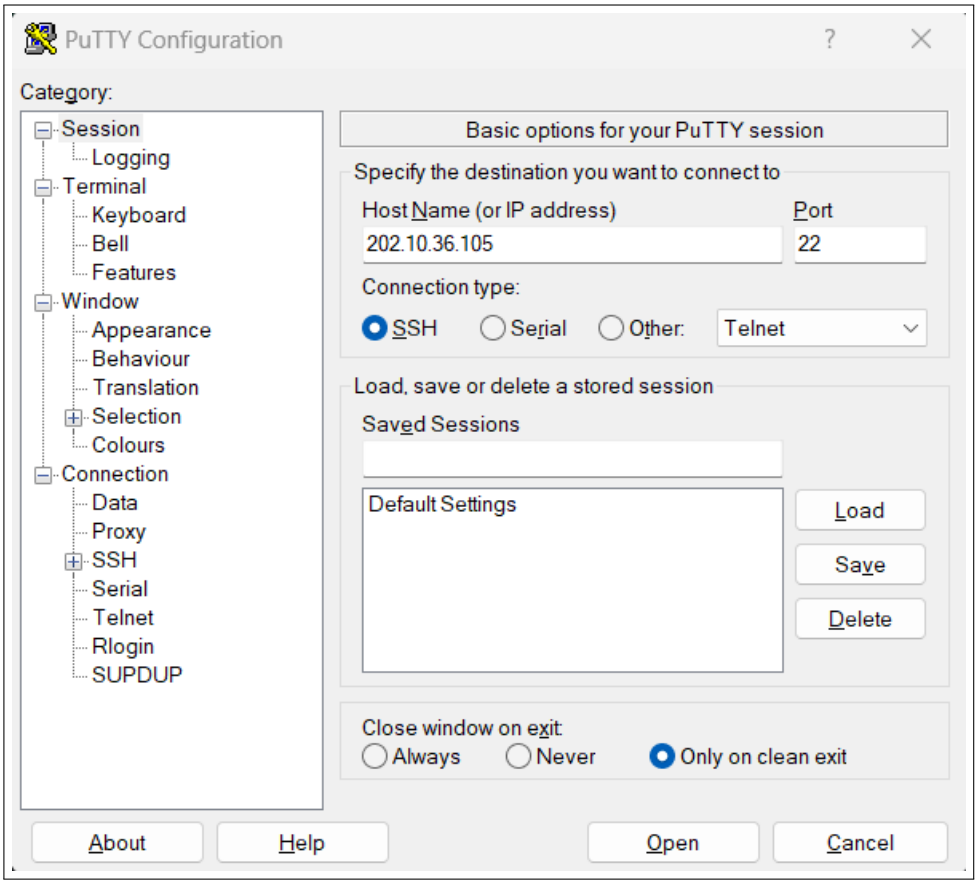

Gambar 3.14. Splunk *Monitoring Resource Usage*

- PuTTY

  PuTTY adalah aplikasi *open-source* untuk klien SSH, Telnet, dan Rlogin. Di dalam PT Bursa Efek Indonesia, semua akses dari *server* fisik *(on-premise)* menggunakan klien SSH langsung ke *IP Address*. Berikut merupakan langkah-langkah konfigurasi yang dipakai untuk *connect* ke dalam SSH menggunakan *environment* kantor.

  1. Konfigurasi awal PuTTY

     Untuk dapat terhubung ke *Hostname* atau Alamat IP yang diinginkan, pertama-tama Anda perlu mengisi alamat dan *port* yang sesuai. Langkah ini sangat penting karena Hostname atau Alamat IP berfungsi sebagai penanda unik yang memungkinkan perangkat atau aplikasi untuk menemukan dan berkomunikasi dengan tujuan yang diinginkan di jaringan. Selain itu, *port* juga harus diisi dengan benar karena *port* ini merupakan titik akhir komunikasi di perangkat tujuan yang digunakan untuk mengidentifikasi jenis layanan atau aplikasi yang akan diakses.



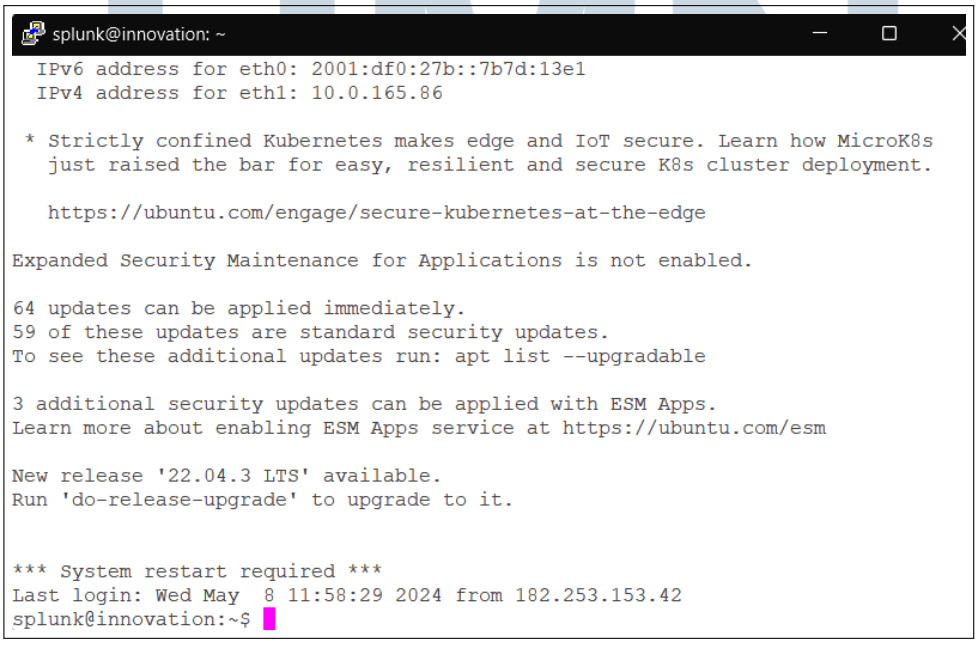

Gambar 3.15. PuTTY *Configurations*

2. PuTTY *login* SSH dengan *credential* dari *server*

   Setelah berhasil melakukan koneksi ke *Hostname* atau Alamat IP yang diinginkan dengan memasukkan alamat dan *port* yang sesuai, langkah berikutnya adalah user akan disajikan dengan *prompt* seperti pada Gambar 3.16 untuk mengisi kredensial pengguna dari *server* tersebut. Kredensial ini terdiri dari *username* dan *password* yang harus diisi dengan benar untuk memastikan bahwa *user* memiliki izin yang diperlukan untuk mengakses layanan atau sumber daya di *server*.


Gambar 3.16. Putty SSH *login*

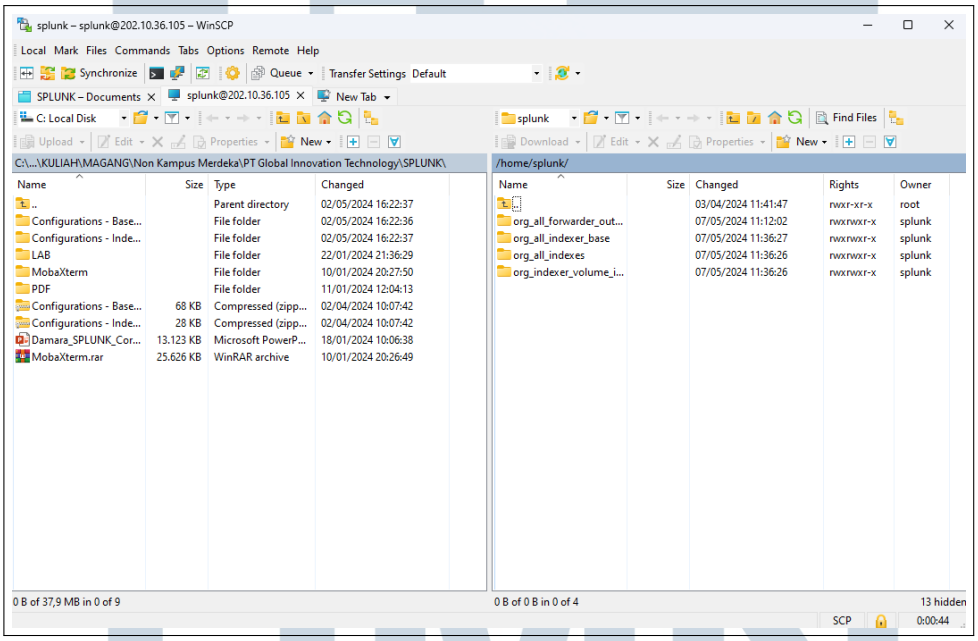
Ketika kredensial pengguna yang dimasukkan sudah sesuai dan cocok dengan akun yang terdaftar di server, maka sistem akan memberikan akses dan menampilkan antarmuka seperti yang ditunjukkan pada Gambar 3.17. Proses ini melibatkan verifikasi username dan password yang telah dimasukkan oleh pengguna, di mana sistem memeriksa kecocokan dengan data yang tersimpan di basis data autentikasi server.




Gambar 3.17. PuTTY saat sudah berhasil *connect* SSH

- WinSCP

  WinSCP *(Windows Secure Copy)* adalah sebuah aplikasi *open-source* yang digunakan untuk mentransfer file secara aman antara komputer lokal dan *server* jarak jauh. Di dalam Gambar 3.18 merupakan tampilan dari WinSCP saat sudah *connect* dan siap untuk mentransfer *file*. Aplikasi ini memungkinkan pengguna untuk memindahkan *file* menggunakan protokol SSH, SFTP, atau SCP. Tampilan dari WinSCP mirip dengan Windows Explorer, membuatnya mudah digunakan oleh orang yang terbiasa dengan sistem operasi Windows.




Gambar 3.18. Tampilan WinSCP

Tampilan dari WinSCP terdiri dari dua kolom utama, kolom di sebelah kiri merupakan isi dari *directory* di komputer lokal, dan kolom di sebelah kanan mewakili merupakan isi dari *directory* pada *server* target. *User* dapat dengan mudah menyeret dan melepaskan *file* yang ada pada kolom untuk memindahkan *file* dari komputer lokal ke *server* atau sebaliknya. Dengan adanya aplikasi ini, memudahkan kolaborasi dalam mengelola *file* dalam *environment* yang sudah ditetapkan.

### 3.3.2 Pengembangan dan pemeliharaan platform Splunk

Pengembangan dan pemeliharaan *platform* Splunk dilakukan setiap hari Jumat dan Sabtu di Gedung Cyber-1. Rutinitas kegiatan akan selalu dipantau dan dilaksanakan sesuai dengan dokumen yang diberikan. *Technical Consultant* dari PT Global Innovation Technology diwajibkan untuk selalu memberikan keterangan dalam setiap perubahan yang dilakukan. Berikut merupakan tahapan dari pengembangan dan pemeliharaan *platform* Splunk pada PT Bursa Efek Indonesia

**A. Pengembangan**

Pelaksanaan pengembangan sistem *platform* Splunk diawali dengan koordinasi *meeting* yang dipimpin oleh pihak dari PT Bursa Efek Indonesia dan diikuti oleh *Project Manager* dan *Senior Technical Consultant*. Pada tahap awal ini, pertemuan tersebut bertujuan untuk merumuskan tujuan proyek secara menyeluruh, mengidentifikasi kebutuhan dan persyaratan teknis, serta menetapkan kerangka waktu dan *milestone* yang harus dicapai. Berikut merupakan penjabaran yang dilakukan saat pengembangan dan pemeliharaan sistem Splunk.

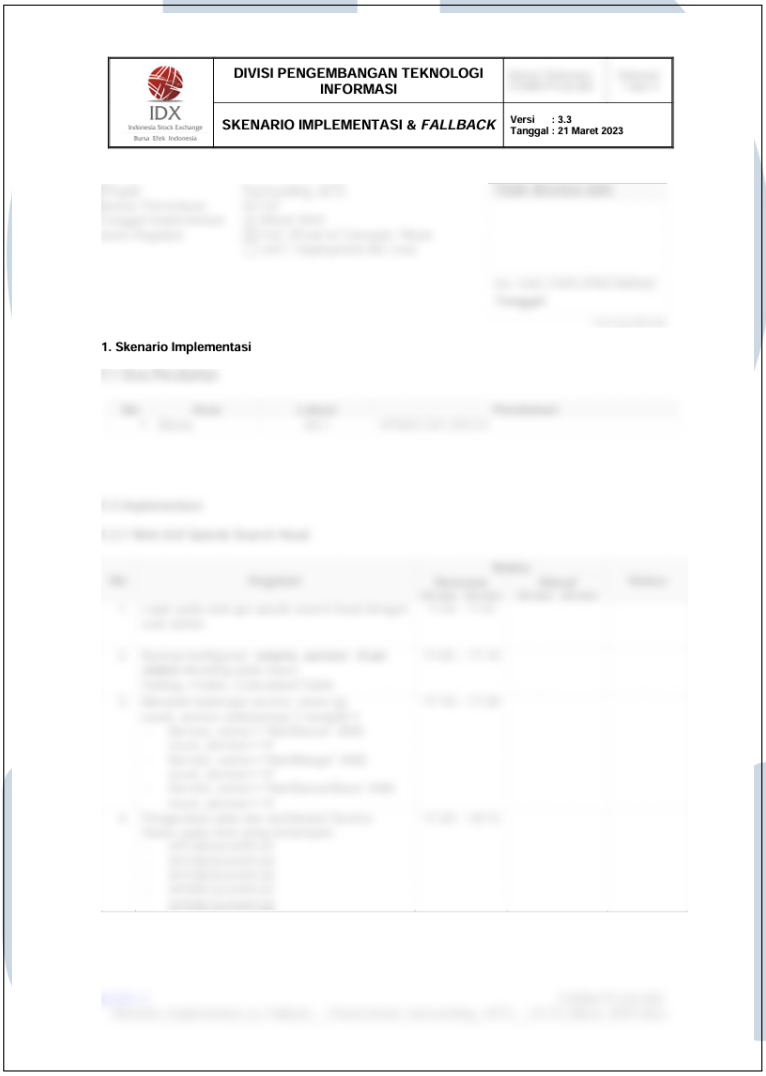
- Koordinasi dokumen SIF Aktual *Surrounding*

  Dokumen SIF Aktual *Surrounding* adalah sebuah dokumen yang digunakan dalam proyek pengembangan dan integrasi sistem untuk memastikan bahwa semua langkah yang diperlukan untuk implementasi dan *fallback* sistem telah direncanakan dan didokumentasikan secara terstruktur. SIF sendiri adalah singkatan dari *System Integration Framework*, yang merupakan kerangka kerja atau metodologi yang digunakan untuk mengelola dan mengkoordinasikan berbagai aspek dari integrasi sistem. Untuk menetapkan *milestones* kegiatan yang terkait dengan Skenario Implementasi dan *fallback*. Proses ini direncanakan secara rinci untuk memastikan setiap tahapan berjalan sesuai jadwal dan mencapai hasil yang diinginkan.

  1. Skenario Implementasi

     Skenario implementasi adalah serangkaian langkah dan prosedur yang direncanakan untuk mengintegrasikan fitur baru atau sistem ke dalam lingkungan operasional yang ada. Ini mencakup seluruh proses dari persiapan hingga evaluasi pasca-implementasi. Skenario

implementasi dibuat untuk memastikan bahwa setiap tahap integrasi berjalan dengan lancar, meminimalkan gangguan pada operasi sehari-hari, dan memastikan bahwa fitur baru berfungsi sebagaimana mestinya. Gambar 3.19 merupakan contoh dari dokumen skenario implementasi.




Gambar 3.19. Skenario Implementasi

2. *Fallback*

   *Fallback* adalah sebuah proses yang direncanakan dan dilaksanakan untuk mengembalikan sistem ke kondisi stabil sebelumnya jika implementasi fitur baru atau perubahan sistem mengalami kegagalan atau menimbulkan masalah yang signifikan. *Fallback* bertujuan untuk meminimalkan gangguan pada operasional bisnis dan memastikan bahwa sistem dapat terus berfungsi meskipun terjadi masalah selama

proses implementasi. Gambar 3.20 merupakan contoh dari dokumen *fallback*.


Gambar 3.20. Skenario *Fallback*

Setelah dokumen SIF ditinjau ulang dan disetujui oleh semua pihak yang berkepentingan, akan dilakukan pelaksanaan *Mock* onsite. Saat kegiatan *mock* ini melibatkan berbagai kegiatan dengan koordinasi menggunakan WhatsApp *Group* agar keseluruhan kegiatan berjalan dengan sesuai.

- Kegiatan *Mock*

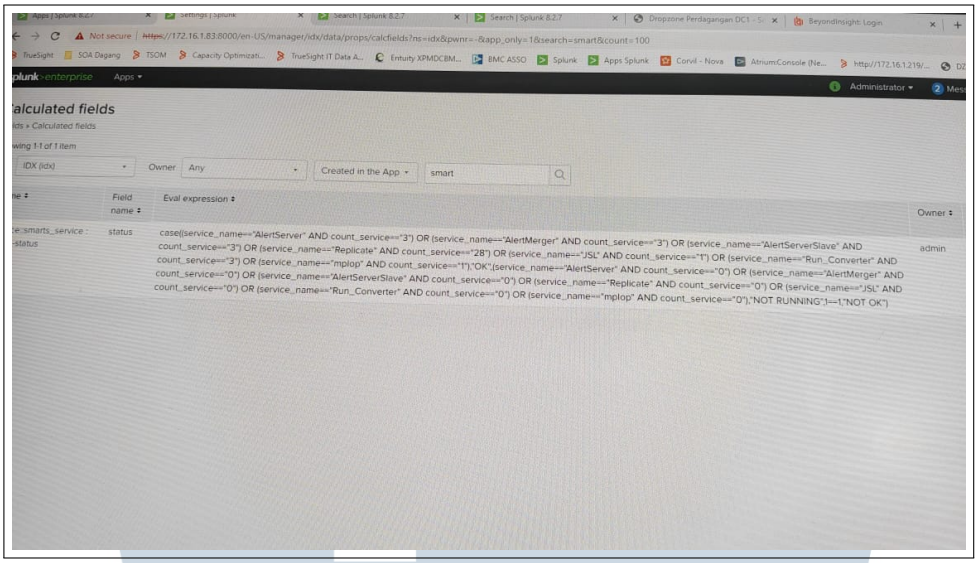
  Kegiatan *Mock* merupakan kegiatan simulasi atau keadaan yang dirancang untuk meniru suatu keadaan atau skenario tertentu, bertujuan untuk

membuktikan kesiapan dari *checkpoint* yang sudah dibuat pada dokumen SIF. *Mock* mencakup berbagai aktivitas yaitu pengubahan *query*, menunggu kegiatan *cycle*, dan pemantauan pada sistem yang diubah ketika suatu permasalahan terjadi.

Technical Consultant dari PT Global Innovation Technology melakukan *Mock* sesuai dengan jadwal yang ditetapkan pada perjanjian awal. Jadwal untuk pelaksanaan *maintenance* biasanya dilaksanakan pada hari Jumat dan Sabtu. Pemilihan hari ini bertujuan untuk meminimalkan gangguan pada operasional harian klien, karena PT Bursa Efek Indonesia melakukan operasional *trading* di hari Senin sampai Jum 'at. Berikut merupakan tahapan yang dilakukan saat *Mock*.

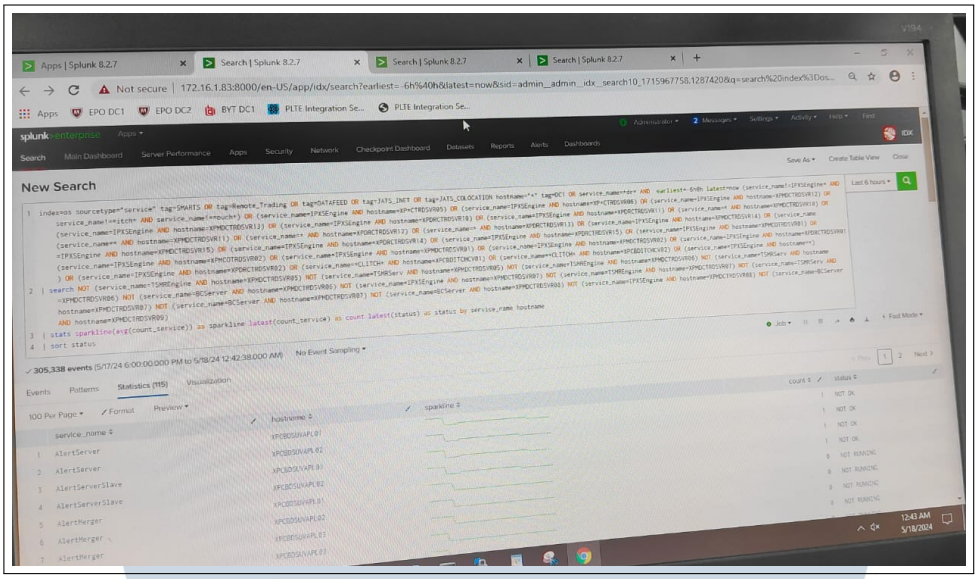
1. Mengubah *query* sesuai dokumen SIF Aktual *Surrounding*

   Pada pengubahan *query* akan dilakukan bersama dengan *Senior Technical Consultant*. Keseluruhan tugas yang akan dilakukan semuanya ada di dokumen SIF yang sudah dicontohkan pada Gambar 3.19 dan Gambar 3.20. Sesuai arahan dari dokumen SIF, *Technical Consultant* mengakses salah satu *dashboard* untuk melakukan penyesuaian yang sudah dikoordinasikan. Pada Gambar 3.21 diperlihatkan fitur *Calculated fields* dari Splunk, fitur ini berguna untuk membuat *field* baru tanpa harus mengubah data asli yang sudah dilakukan *indexing*. Terlihat ada kolom *Field name* yang berisikan *status* dan kolom *Eval expression* yang berisikan *query*. *Query* ini bertujuan untuk memvisualisasikan status dari *services* yang ada. Terdapat entitas yang bernama *"service_name"* yang bertujuan untuk memberi nama pada servisnya dan ada entitas yang bernama *"count_service"* yang bertujuan sebagai penanda atau *flag* pada *service* yang ada.



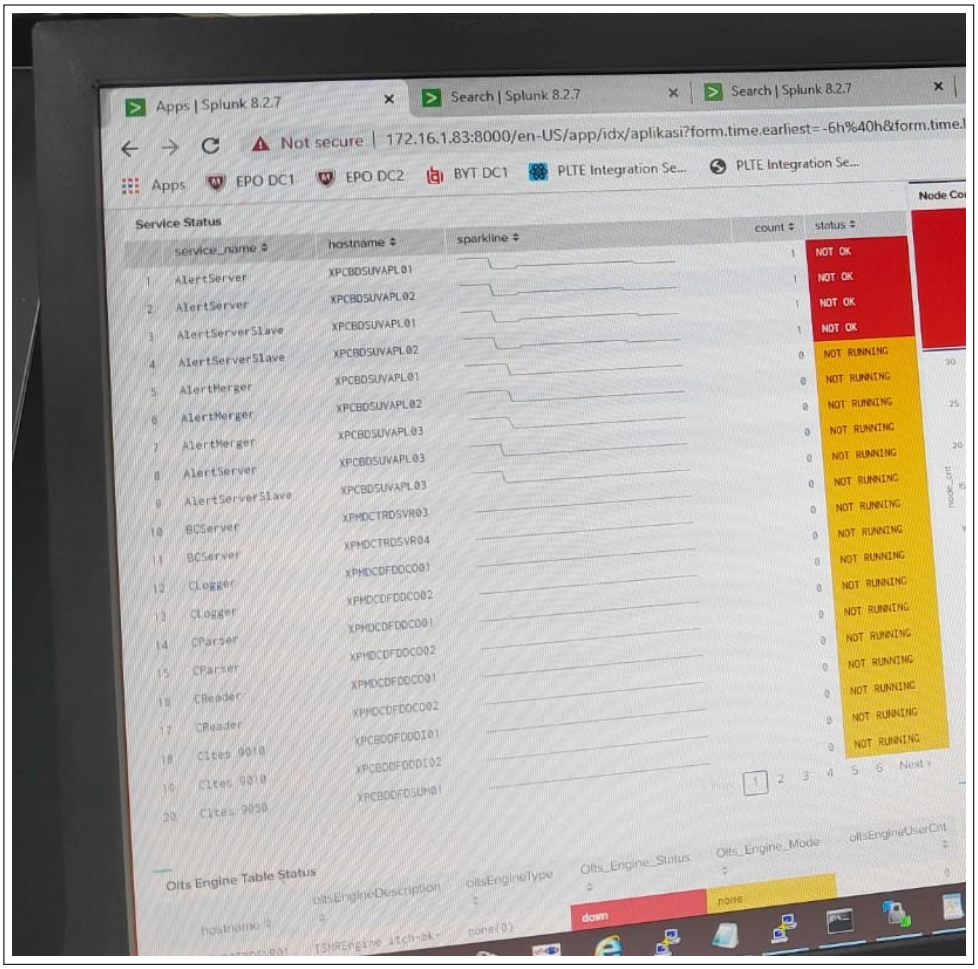

Gambar 3.21. Tampilan *Calculated fields* pada Splunk di PT Bursa Efek Indonesia

Pada Gambar 3.22 merupakan *query* dari *service* status yang sedang dirancang untuk memastikan apakah pengubahan di dalam fitur *calculated fields* pada Gambar 3.21 dapat dilihat perubahannya. *Query* tersebut memanggil *index* dari *operating system* dan memanggil servisnya dengan masing-masing *tag* dari aplikasi yang ada. Setelah itu terdapat *query search* yang berfungsi untuk memfilter beberapa *"service_name"* dan *"hostname"*. Terdapat *query stats* yang berfungsi untuk memvisualisasikan data menjadi *sparkline chart*. Dan terakhir, ada *query sort* untuk men-*sorting* berdasarkan status *"NOT OK"*, *"NOT RUNNING"*, dan *"RUNNING"*.




Gambar 3.22. Tampilan *query* dari *service* status pada Splunk di PT Bursa Efek Indonesia

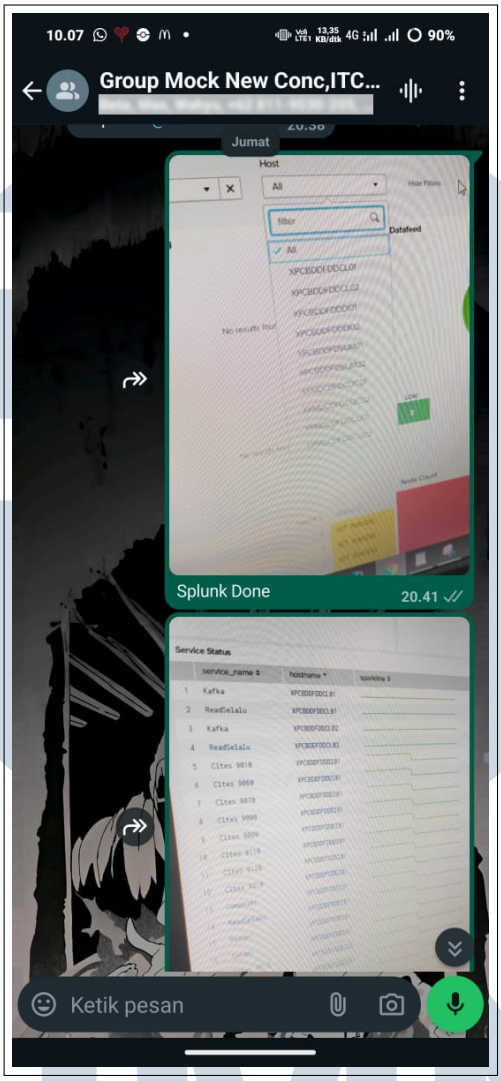
Pada Gambar 3.23 merupakan visualisasi dari *query service status* yang dipakai untuk mempermudah pemeliharaan dan analisa ketika suatu insiden terjadi pada *services* tertentu. Status dapat dilihat dengan warna yang berbeda hijau menandakan *"RUNNING"*, kuning menandakan *"NOT RUNNING"*, dan merah menandakan *"NOT OK"*.




Gambar 3.23. Tampilan *dashboard* dari *query service* status pada Splunk di PT Bursa Efek Indonesia

2. Melapor kegiatan kepada *Person in Charge* dari PT Bursa Efek Indonesia

   Setelah perubahan *query* dilakukan sesuai dengan arahan dalam dokumen SIF Aktual *Surrounding*, pada Gambar 3.24 dilakukan pelaporan hasil kepada tim IT PT Bursa Efek Indonesia melalui WhatsApp Group. Laporan ini mencakup *screenshot*-an dari perubahan yang dilakukan.




Gambar 3.24. Tampilan pelaporan ke WhatsApp Group

3. Pemantauan terhadap *query* yang diubah dan menunggu *cycle* berlangsung

   Pemantauan terhadap *query* yang diubah dilakukan dengan seksama untuk memastikan bahwa perubahan yang dilakukan pada *query* tidak menimbulkan masalah baru atau mengganggu operasional sistem. Bersamaan dengan pemantauan, diberlakukan penungguan *cycle*. *Cycle* di PT Bursa Efek Indonesia merupakan siklus operasional yang sudah ditetapkan oleh klien sesuai urutan penjadwalan. Saat kegiatan *mock* berlangsung, terdapat banyak *vendor* yang hadir untuk melakukan pemeliharaan pada sistem pengguna masing-masing. Hal ini dapat menyebabkan risiko bentrokan sistem jika tidak dikelola.

- Kegiatan *Pre-live*

  Setelah *mock* selesai sesuai dengan jadwal yang telah ditetapkan, yaitu pada minggu ketiga, maka dilanjutkan dengan kegiatan *pre-live*. Pada tahap *pre-live*, keseluruhan *checkpoint* dari *mock* sebelumnya akan dilakukan implementasi secara menyeluruh ke dalam sistem yang sesungguhnya. Tahap ini bertujuan untuk memastikan bahwa semua perubahan dan penyesuaian yang telah diuji coba dalam *mock* dapat berfungsi tanpa masalah ketika dilakukan implementasi di lingkungan produksi. Kegiatan *pre-live* ini juga melibatkan pemantauan intensif dan penyesuaian terakhir sebelum sistem benar-benar siap untuk digunakan oleh pengguna akhir dalam operasional sehari-hari. Dengan demikian, tahap *pre-live* sangat penting untuk memastikan kelancaran dan keberhasilan pelaksanaan proyek secara keseluruhan.

- *Babysitting*

  Pada tahap ini, *Technical Consultant* dari PT Global Innovation Technology akan terus memantau sistem untuk memastikan bahwa semua fungsi berjalan dan stabil. Kegiatan *babysitting* melibatkan pengawasan intensif terhadap sistem yang baru dilakukan implementasi untuk mengidentifikasi dan menangani segera setiap permasalahan atau anomali yang muncul. Dengan adanya *babysitting* dapat memberikan respons cepat terhadap isu-isu yang tidak terduga dan melakukan penyesuaian yang diperlukan guna memastikan bahwa operasional sistem tidak terganggu. Bertujuan untuk menjamin transisi yang mulus dari tahap *pre-live* ke operasional penuh, sehingga *user* dapat menggunakan tanpa ada kendala.

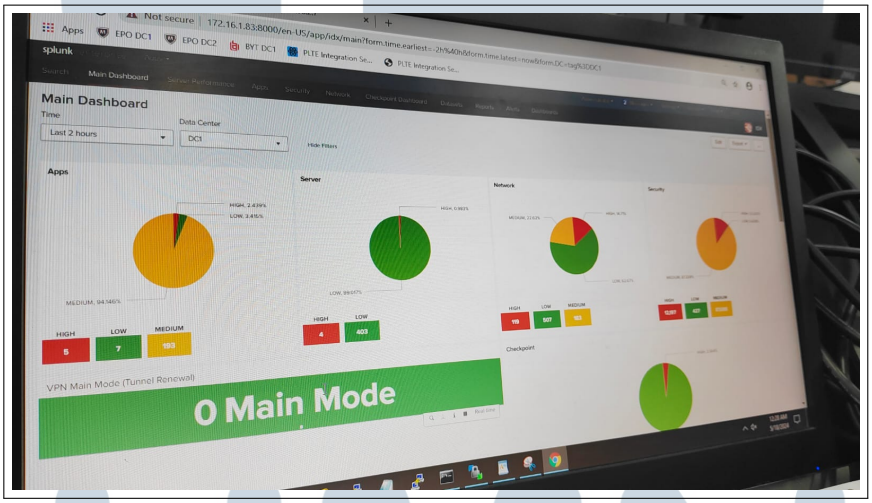
## B. Pemeliharaan

Pemeliharaan pada sistem *platform* Splunk dilakukan secara paralel dengan kegiatan Pengembangan. Sebelum dilakukan kegiatan *mock*, *Technical Consultant* dari PT Global Innovation Technology akan melihat keseluruhan *dashboard* yang ada pada PT Bursa Efek Indonesia. Untuk memastikan apakah ada suatu insiden yang terjadi. Berikut merupakan tampilan *dashboard* yang dipelihara.

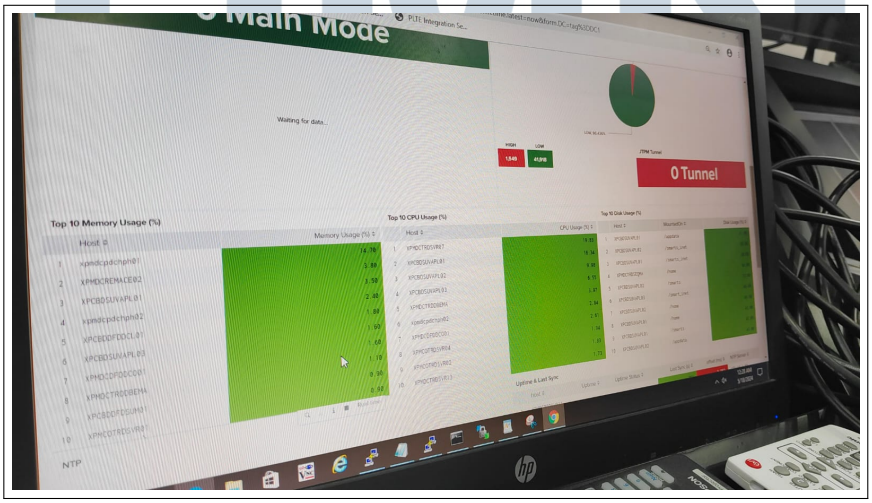
1. *Main Dashboard*

   Pada Gambar 3.25 merupakan tampilan *main dashboard* dari Splunk pada PT Bursa Efek Indonesia. Di bagian atas kiri terdapat *button time*

merepresentasikan *time range* pada suatu *services* atau aplikasi dan *data center* menunjukkan lokasi dari *data center* yang ingin di-*filter*. Setiap *services* atau aplikasi yang berjalan di-*monitoring*, dilakukan visualisasi dan ditandai dengan warna merah, hijau, dan kuning. Masing-masing warna memiliki kategorisasi yaitu high, low, dan medium untuk mempermudah pemeliharaan dan analisa. Dapat dilihat juga bahwa di *main dashboard* terdapat *Apps*, *Server*, *Network*, *Security*, *VPN Main Mode (Tunnel Renewal)*, *checkpoint*, kemudian pada Gambar 3.26 terdapat *Top 10 Memory Usage (%)*, *Top 10 CPU Usage (%)*, dan *Top 10 Disk Usage (%)* yang di-*monitor* dan divisualisasi untuk melakukan pencegahan ketika terjadi suatu insiden.



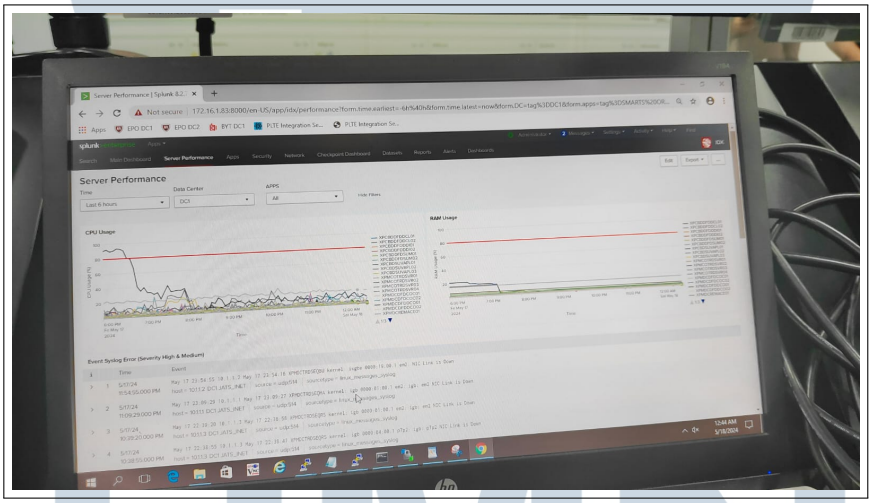

Gambar 3.25. Tampilan *Main Dashboard* dari Splunk pada PT Bursa Efek Indonesia




Gambar 3.26. Tampilan lanjutan *Main Dashboard* dari Splunk pada PT Bursa Efek Indonesia

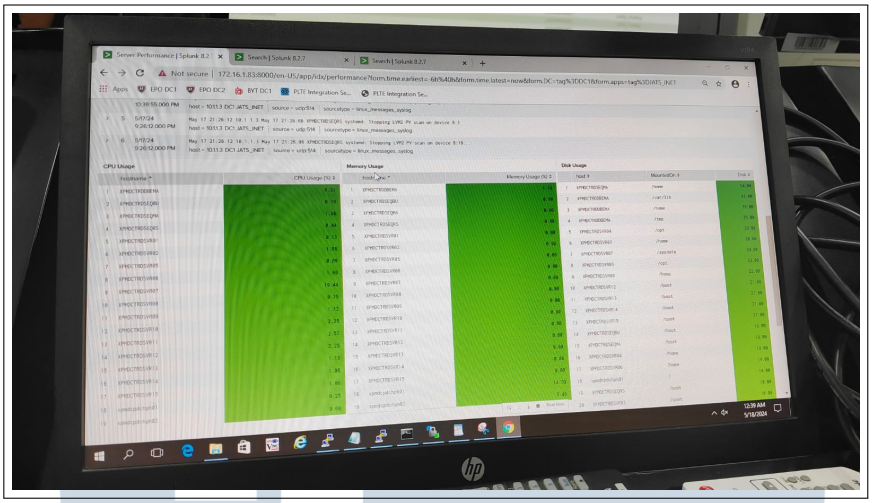
2. *Server Performance*

Pada Gambar 3.27 merupakan tampilan *server performance* dari PT Bursa Efek Indonesia. Di bagian atas kiri terdapat *button time, data center, dan apps*. *Button time* merepeperesentasikan *time range* dari *services* yang ada, *data center* menunjukkan lokasi dari *data center*, dan *apps* menunjukkan dari *apps* yang ingin di-*filter*. Selanjutnya, dapat dilihat visualisasi grafik dari *CPU Usage* pada masing-masing *apps* yang ada, dan grafik dari *RAM Usage* pada masing-masing *apps* yang ada berdasarkan KPI *(Key Performance Indicator)*. Dapat dilihat juga terdapat tabel untuk melihat *Event Syslog Error (Severity High & Medium )* yang berfungsi untuk melihat berbagai *event* dengan tingkat insiden dari *high* dan *medium*.




Gambar 3.27. Tampilan lanjutan *Server Performance* dari Splunk pada PT Bursa Efek Indonesia

Pada Gambar 3.28 merupakan tampilan lanjutan *server performance* dari PT Bursa Efek Indonesia. Pada Gambar ini diperlihatkan terdapat tiga tabel yaitu *CPU Usage*, *Memory Usage*, dan *Disk Usage*. Dapat dilihat juga *hostname* dan KPI berdasarkan penggunaan setiap CPU, *Memory*, ataupun, *disk* pada masing-masing *hostname*.



Gambar 3.28. Tampilan lanjutan *Server Performance* dari Splunk pada PT Bursa Efek Indonesia

## 3.4 Kendala dan Solusi yang Ditemukan

Selama proses kerja magang di PT Global Innovation Technology dalam pengembangan dan pemeliharaan sistem Splunk terdapat kendala yang dialami sebagai berikut.

- Diperlukan waktu untuk memahami fitur-fitur di dalam Splunk mulai dari istilah, bahasa *query (Splunk Processing Language)*, dan *ingest data*. Sehingga, membutuhkan waktu untuk memperdalam *platform* Splunk.
- Diperlukan waktu untuk memahami arsitektur IT dari Perusahaan PT Bursa Efek Indonesia, alur dari berbagai macam *server* dan aplikasi yang dikelola, tahapan-tahapan dalam membaca dokumen SIF. Sehingga perlu waktu untuk mempelajari proses bisnisnya.
- Dalam kegiatan implementasi terdapat beberapa kebingungan dalam melakukan *query* karena banyaknya *dashboard* visualisasi yang telah dibangun sebelumnya. Sehingga memerlukan waktu untuk beradaptasi dengan *dashboard* yang ada.

Pada setiap kendala yang disebutkan, berikut merupakan solusi yang dapat menanggulangi sebagai berikut.

- Mempelajari banyak hal yang berkaitan dengan *platform* Splunk dengan memanfaatkan fasilitas yang diberikan oleh perusahaan berupa *training*, materi, dan dokumentasi resmi dari *website* Splunk.

- Menelusuri dan mempelajari dokumentasi terkait PT Bursa Efek Indonesia. Memanfaatkan informasi yang diberikan oleh perusahaan berupa dokumen alur server dan aplikasi. Hal itu, sangat membantu dalam proses pembelajaran arsitektur dan studi kasus yang sedang ditangani.
- Menelusuri dan mempelajari *query dashboard* yang sudah dibangun sebelumnya dan meminta bimbingan dari *Senior Technical Consultant* yang menemani saat implementasi ke *client*.