

BAB V PENUTUP

5.1 Kesimpulan

Dari hasil penelitian yang dilakukan oleh penulis dapat diambil kesimpulan sebagai berikut:

1. Dari hasil penelitian ini didapatkan bahwa untuk mempermudah Administrator membaca log Asterisk, ELK Stack merupakan pilihan yang tepat. Karena ELK Stack bukan hanya sebuah platform open source, tetapi dari segi performa lebih cepat dan mudah digunakan untuk membaca log.
2. Dibandingkan dengan Platform ELK Stack, platform Splunk membutuhkan waktu yang lebih lama dalam proses membaca log.
3. Untuk melakukan proses pencarian log, pada platform ELK Stack menggunakan Query DSL (Domain Specific Language) yang lengkap berdasarkan JSON untuk mendefinisikan query.
4. Sedangkan platform Splunk dalam melakukan pencarian log menggunakan Raw Event Search yaitu pencarian yang hanya mengambil kejadian dari data yang di indeks, dan biasanya digunakan saat akan menganalisis suatu masalah.
5. Proses pencarian log juga tergantung dari jumlah CPU yang digunakan, besar size log, dan banyak baris log yang dicari pada saat proses pencarian log.

5.2 Saran

Sebagai penutup pada penelitian ini, penulis berharap dari hasil penelitian ini dapat memberikan manfaat bagi pembaca dan penulis sendiri. Pada penelitian ini penulis menyadari bahwa terdapat banyak kekurangan, oleh karena itu penulis memberikan saran kepada pembaca atau pada penelitian selanjutnya tidak hanya meneliti pada performa waktu ELK Stack & Splunk juga dapat mencoba tools monitorin yang lainnya. Dan juga dapat melakukan monitoring pada sistem lainnya selain Asterisk.