ABSTRACT

PT Paragon Technology and Innovation develops various applications that are used to enhance both internal and external business needs. These applications are managed internally by PT Paragon Technology and Innovation using the company's internal servers. Continuous monitoring is required to ensure that all applications are running smoothly. Therefore, management and analysis of application logs, known as log management, are necessary as logs store all activities of the applications, including information about the application's operations and any issues that occur. Log management activities can be aided by log monitoring tools such as ELK Stack and Graylog.The objective of this final project is to compare these two tools based on several factors such as architecture, performance, and flexibility. This will help identify the strengths of each platform and determine which one is more suitable for PT Paragon's needs. Both tools will be installed on an Amazon Elastic Compute Cloud (EC2) virtual machine, which will perform various log management stages such as log collection, log transformation, log storage, and log analysis. ELK Stack requires more resources than Graylog, resulting in better response time compared to Graylog. ELK Stack also offers better visualization capabilities with its Kibana dashboard and a more comprehensive library due to a larger community. On the other hand, Graylog is simpler, making the configuration process easier and efficient with the assistance of two NoSQL databases, Elasticsearch and MongoDB. Graylog also provides user-friendly alert features and can be connected to other devices for sending notifications without relying on third-party devices.its configuration process easier. Graylog also provides user-friendly alert features.

Key Words: ELK Stack, Graylog, Log Monitoring, Log Management, Server