ABSTRACT

The development of digital technology requires a capable Information Technology infrastructure, including the adoption of microservice architecture and containerization that encourages the use of Kubernetes as a container orchestrator. Kubernetes makes it easier to manage and deploy complex applications, but also increases the complexity of managing logs from various containers. These logs include application activity, system performance, and debugging messages that are important for understanding application performance, detecting problems, and meeting security needs. This study focuses on distributed log management in a Kubernetes environment using Fluentd and Elasticsearch. Fluentd acts as an efficient log collection agent, while Elasticsearch provides fast log storage, indexing, and analysis. The combination of the two is expected to improve the efficiency, availability, and security of complex cloud infrastructure. The research method includes the implementation of two main scenarios, namely manual log collection using the kubectl logs command on one pod and 20 pods to get performance, and distributed log collection using Fluentd integrated with Elasticsearch in a Kubernetes cluster. The evaluation was carried out based on log search time, log collection efficiency, and ease of analysis using visualization from Kibana. The results of the study show that log collection using Fluentd and Elasticsearch is significantly more efficient than the manual method.

Keywords: *Containerization, Elasticsearch, Fluentd, IT infrastructure, Kubernetes, log management, microservices.*