ABSTRACT

One of the technologies widely used by companies to run applications effectively and safely is containers. Through containers, each application only needs to have the dependencies needed by the program without any unnecessary dependencies. Container runtime is a core component in containers to be able to bridge the processes in the container and the host server. One of the problems that arise behind the widespread use of containers is cyber attacks such as Denial of Service (DOS) attacks that can cause the server to become paralyzed. The urgency of preparing a container runtime that is resilient to DOS attacks is increasingly needed. This study aims to provide a comprehensive analysis of the performance between the commonly used runC container runtime, with container runtimes that have a high security isolation architecture such as gVisor and Kata Containers. The performance of runC, Kata Containers and gVisor is based on host CPU, host memory usage, container CPU, container memory usage, web throughput, and web response time. The test results in this study show that runC has the best results on host CPU, host memory, container CPU, web throughput, and web response time. Meanwhile, Kata Container has the best results in memory container consumption and also Kata Container becomes the runtime container after runC that has the best results in every metric.

Keywords: *container runtime, runc, gvisor, kata containers, denial of services*