System Log Isolation for Containers

Kun WANG, Song WU, Yanxiang CUI, Zhuo HUANG, Hao FAN, Hai JIN

Frontiers of Computer Science, DOI: 10.1007/s11704-024-2568-8

Problems & Ideas

- Problems of system isolation for containers:
  - Containers suffer from configuration conflict, operation conflict, namespace escape, information leakage, log loss, and log redundancy.
  - The root causes are that log configuration and storage are shared among containers, and containers have a global log view.
- Ideas: Our system provides each container with an individual system log that consists of private log configuration, storage, and view, instead of sharing system log among containers.

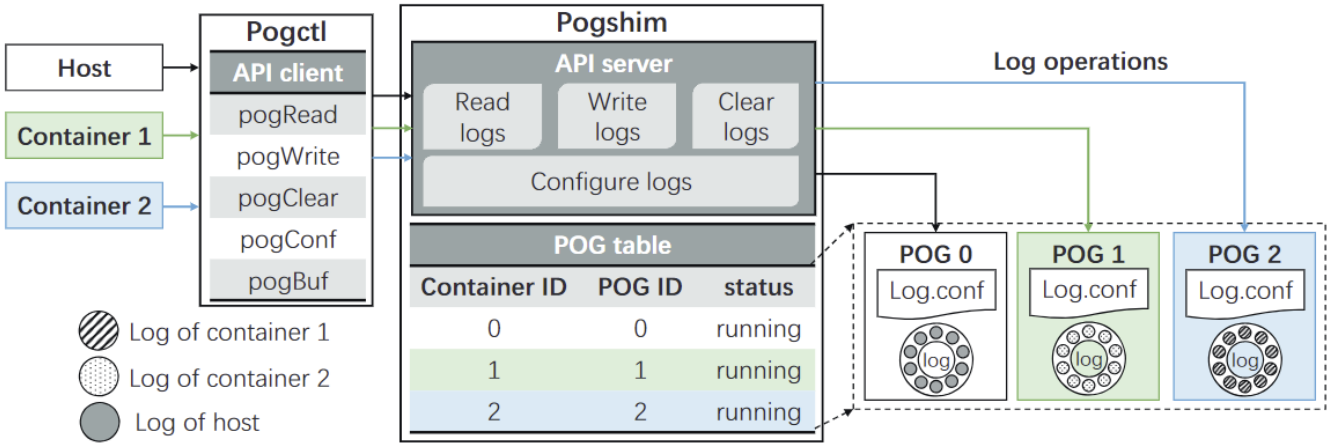

Figure 1 System architecture

We design two key components: pogctl and pogshim to manage the POGs;
Pogctl provides several APIs for containers to control and configure POGs precisely;
Pogshim realizes the management of POGs and identifies the belongers of POGs.

Main Contributions

- Contributions:
  - We make a detailed analysis of system log isolation problems in current container environment. We reveal the root causes and the possible impacts of such isolation problems;
  - We propose POGs to enhance system log isolation for containers. Our system provides each container with an individual POG that consists of private log configuration, storage, and view;
  - Experimental results demonstrate that POGs can effectively enhance system log isolation for containers with negligible performance overhead.

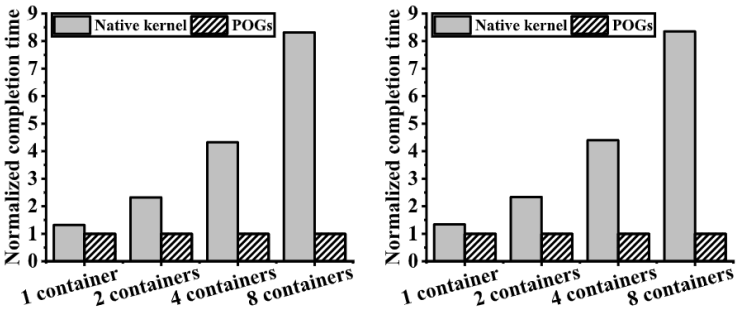

Figure 2 Isolation enhancement

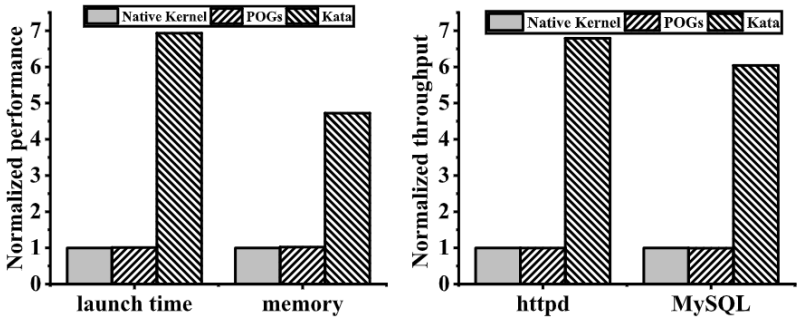

Figure 3 Performance overhead

System log isolation and performance overhead results yielded by our system versus original design. Left: The log analysis efficiency under various numbers of containers; Right: The performance overhead of POGs on launch time, memory footprint, and overall performance.