CYSEC

Solution Architecture - Monitoring of ARCA Trusted OS in a Hybrid Cloud-Edge World

ARCA Trusted OS

CYSEC

1. Introduction

Collecting logs from distributed systems is challenging due to multiple sources, varied log formats, high data volumes, etc... Despite these difficulties, centralized logging is essential for troubleshooting, monitoring performance, ensuring security, and gaining operational insights. It allows teams to trace issues across nodes, optimize resource usage, detect security breaches, and make informed decisions for scaling and improving the system's reliability.

Leveraging Kubernetes already helps that concern by recording and centralizing the majority of the application logs in a single place although it is not optimized for it because its primary design focus is orchestrating containerized workloads. Without mentioning the fact that it can't collect the logs from the host machines by default.

To overcome these limitations, there exists multiple software solutions that ingest data from different sources, optionally reformat the logs and finally export it to a visualizer. By coupling an effective log collector with an user-friendly observability platform, complex distributed systems can be monitored easily. It can offer benefits such as:

- An **unified observability**: multiple source, single dashboard
- A **better visualization**: to display logs in various formats (time-series, heat-maps, etc...)
- The **correlation between logs and other metrics**: e.g. by seeing a high CPU usage at the same times as error messages
- A **real time monitoring**: enabling proactive response to incidents

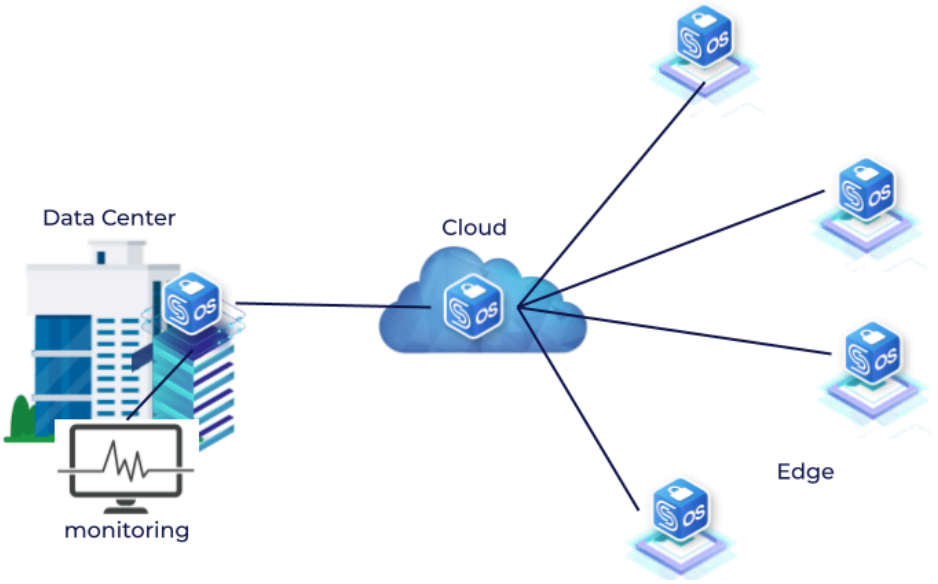

Figure 1. Centralized log monitoring of distributed cloud and edge nodes

2. Solution

In this solution architecture, we demonstrate how to ensure an unified and scalable log management system suitable for both cloud and edge deployments of ARCA Trusted OS with Fluent Bit. Fluent Bit is one of the most used log collection solutions. It is a standalone, lightweight software designed for ingesting logs from numerous sources, exporting them to multiple destinations, and processing, filtering, and formatting logs efficiently.

Deployment Architecture

The proposed log collection system is fully compatible with the two primary deployment modes of ARCA Trusted OS enabling seamless log management across both cloud-based and edge-based ARCA Trusted OS systems:

- As a Kubernetes Cluster Node: Fluent Bit is deployed as a Kubernetes DaemonSet, ensuring that each host in the cluster runs a copy of the log collection pod. Each pod collects logs from the host machine on which it resides, creating a comprehensive log collection mechanism within the Kubernetes environment.
- As a Standalone Node (Edge Deployment): ARCA Trusted OS nodes running outside the Kubernetes cluster will utilize Fluent Bit as a containerized application, deployed via Docker or Podman.

Below is a conceptual overview of the deployment architecture:

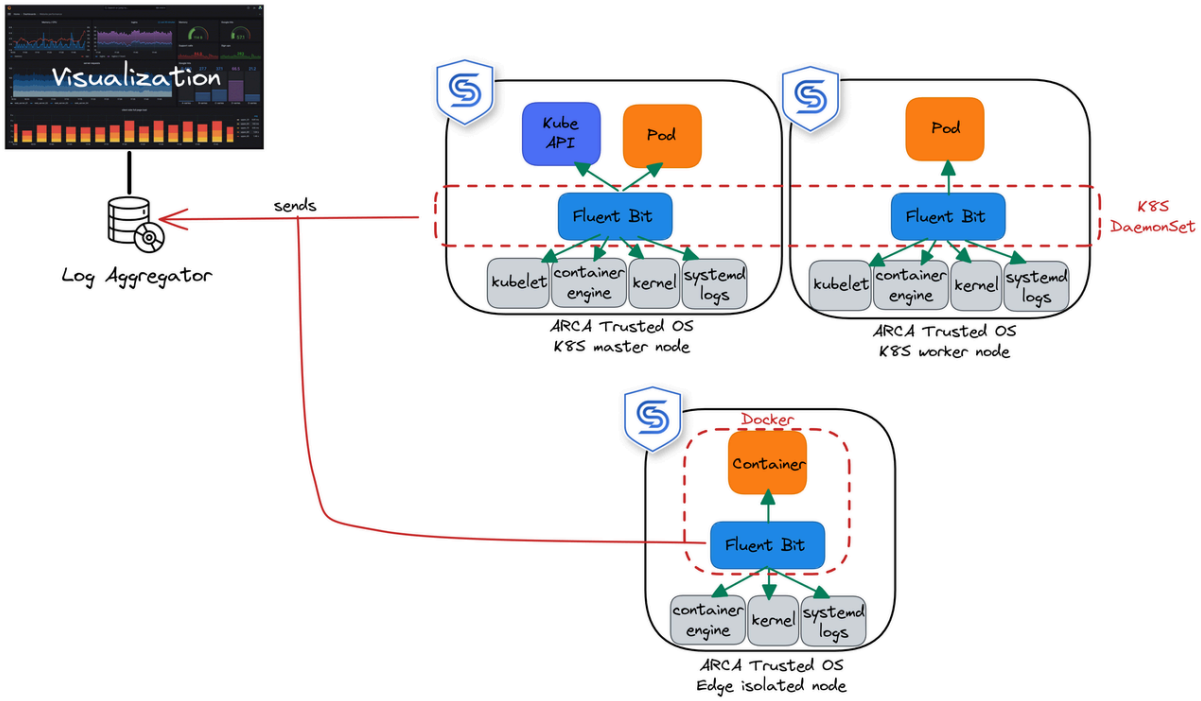

Figure 2. Fluent Bit deployment over Kubernetes and Docker

- Cloud Nodes: Kubernetes cluster nodes run Fluent Bit as a DaemonSet. Each pod collects host-level logs, including application outputs, kernel logs, and critical system services.
- Edge Nodes: Fluent Bit operates as a containerized application, performing the same log collection as for the cloud but from standalone nodes.

To establish a baseline for effective monitoring, we recommend the following log types:

- Neighbor Container Application Outputs:
  - For Kubernetes: Logs from other pods
  - For standalone Docker or Podman deployments: Logs from other containers
- Host Kernel Logs:
  - Captures low-level host system activities
- Critical system services:
  - Examples include **sshd** and **kubelet** for monitoring essential host services

Additional systemd services such as **docker** can be included as needed to enhance visibility further.

Log Aggregation and Visualization

Once logs are collected, they must be forwarded to a centralized log aggregator for visualization and analysis. There exists multiple solutions, either free or as a paid service. We recommend Datadog (SaaS Platform) as a production-ready, scalable platform offering robust log aggregation and visualization capabilities. Moreover, it has high availability and ability to detect cluster-wide failures independently.

On the other hand, Loki/Grafana (Self-Hosted Solution) is a cost-effective alternative for organizations preferring an in-house setup. Loki serves as the log aggregator, while Grafana provides advanced visualization dashboards.

Regardless of the chosen technology, the log aggregation workflow is as follows:

- Logs are transmitted (in plaintext or encrypted form) to the aggregator.
- The aggregator parses the logs, applying custom policies and labels.
- Logs are visualized in dashboards, providing actionable insights.

To support implementation, we have provided a detailed How-To Guide in our public documentation. This guide outlines the step-by-step process for combining Fluent Bit with Loki/Grafana to deploy a self-hosted log management solution effectively.