Aeolus: eBPF based monitoring framework for Container network

Wei Yue
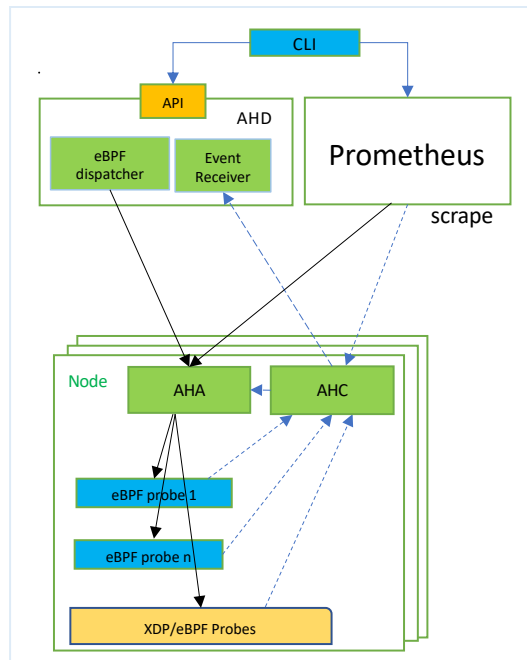
Cloud Lab

Futurewei Technologies

V0.1

12/2022

Aeolus works with K8s and Prometheus

AHD: Aeolus Health Dictator;
AHA: Aeolus Health Agent;
AHC: Aeolus Health Collector

Aeolus includes three major components:

- **AHC** is literally an *open telemetry collector*. The collector can be configured to have one or more pipelines. Each pipeline includes:
    - a set of Receivers that receive the data
    - a series of optional Processors that get the data from receivers and process it
    - a set of Exporters which get the data from processors and send it further outside the Collector.

  By default, one exporter(e.g. P Remote Writer Exporter) is needed to push event data to AHD's event receiver; another exporter can be configured for Prometheus;

- **AHA** is deployed on needed node as daemon-set, it receives instruction from AHD and/or optionally from Prometheus and injects eBPF snippet to specific hooks;

- **AHD** is responsible for receiving triggered event data from AHC and provide mechanism to dynamically generate eBPF snippet based on the response and deploy to AHA. It is a critical and intelligent part for push based live anomaly detection and reaction which is not possible in pull-based Prometheus framework.

wyue@futurewei.com

Actor

policy CR

Kata-agent

eBPF map

eBPF map

Guest OS

eBPF programs

eBPF programs

containerd

dolphin-agent

dolphin-nri

Aeolus-Agent

Pod

Pod

containerd/ dockershim

dolphin-agent

Aeolus-agent

eBPF programs

eBPF map

eBPF map

eBPF programs

CCE Auto Scaler

P Server

eBPF event stream collector

OpenTelemetry/ Metrics/Logs

Event Remote Writer

P Exporter