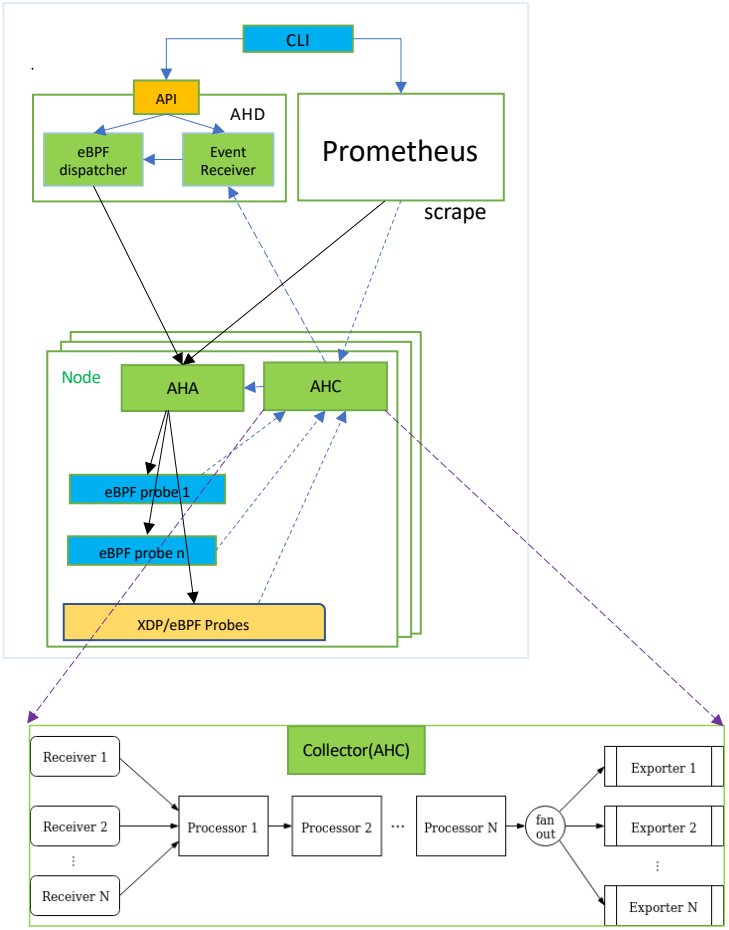
Aeolus: eBPF based monitoring framework for Container networks

Wei Yue
Cloud Lab
Futurewei Technologies
V0.1
12/2022

Aeolus work with k8s and Prometheus

Wei Yue wyue@futurewei.com



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 Receiver that receive the data
  - a series of optional Processor that get the data from receivers and process it
  - a set of Exporter which get the data from processors and send it further outside the Collector.

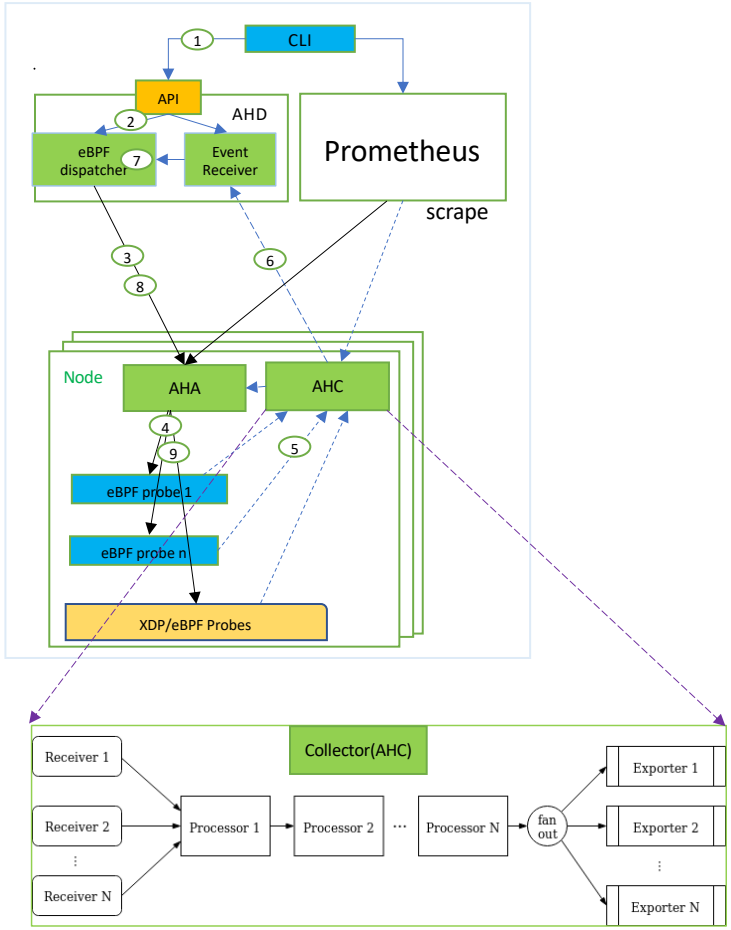
By default, one exporter(e.g. P Remote Writer Exporter) is needed to push event data to AHD's event receiver; another exporter can be configured for Prometheus;

- **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.

Aeolus specific e2e workflow

Wei Yue wyue@futurewei.com



Preparation stage

1. Inject eBPF templates and relationship graph between eBPF templates to **AHD via CLI**;
2. **AHD** compiles predefined eBPF codes(templates + parameters) and generate eBPF snippets;
3. **AHD** dispatches eBPF snippets to **AHA**;
4. **AHA** deploys eBPF snippets to specific hooks;

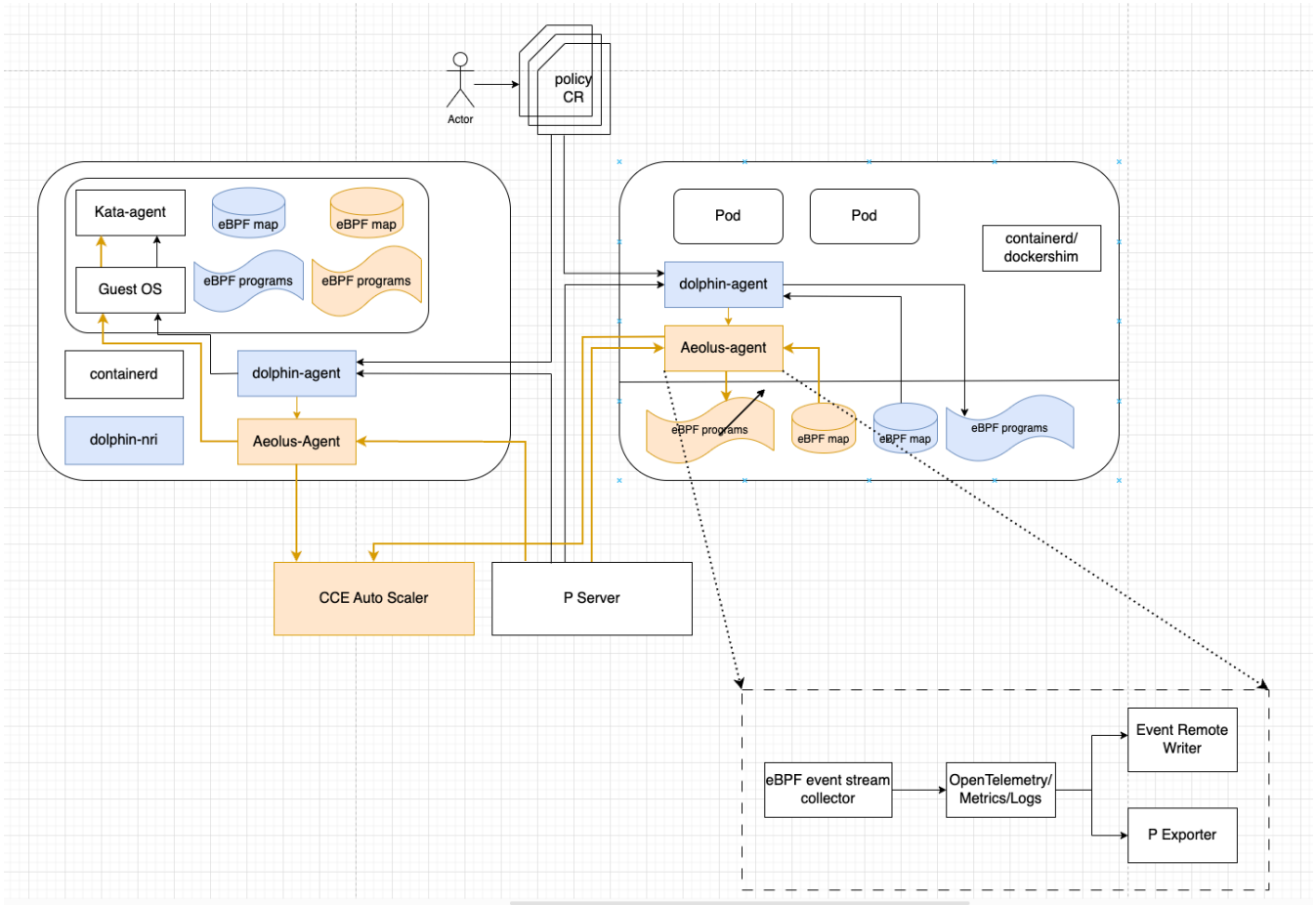
Collection stage

5. **AHC** collects desired event metrics from eBPF probes;
6. **AHC** pushes event metrics to ***Event Receiver*** in **AHD**, the metrics includes node and flow specific parameters which are needed for **AHD** to generate follow up eBPF snippets;

Reaction stage

7. **AHD *event receiver*** receives event metrics and searches eBPF template relationship graph to find specific eBPF templates and generate eBPF code with parameters included in event metrics; generated eBPF code are verified and compiled to eBPF snippets;
8. **AHD** dispatches eBPF snippets and deploy instructions to **AHA**;
9. **AHA** deploys and/or deletes eBPF snippets from specific hooks;

10. Back to collection stage.


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