KubeCon | CloudNativeCon

North America 2017

Full Stack Visibility with Elastic

Logs, Metrics and Traces

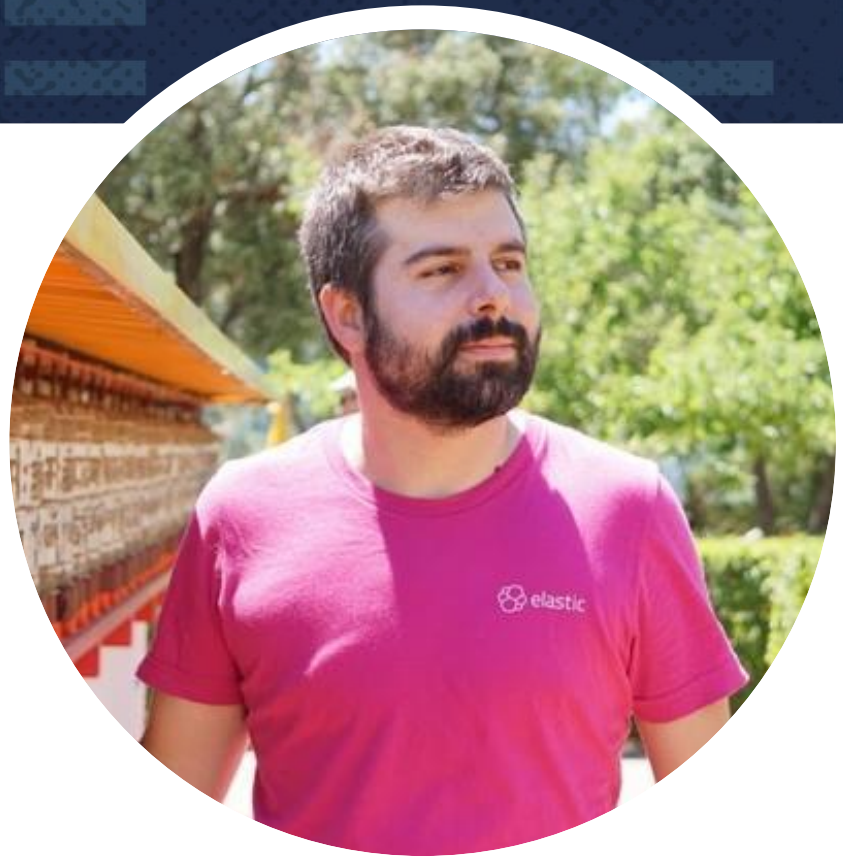
Carlos Pérez-Aradros, Software Engineer, Elastic

Carlos Pérez-Aradros

Software Engineer

carlos@elastic.co

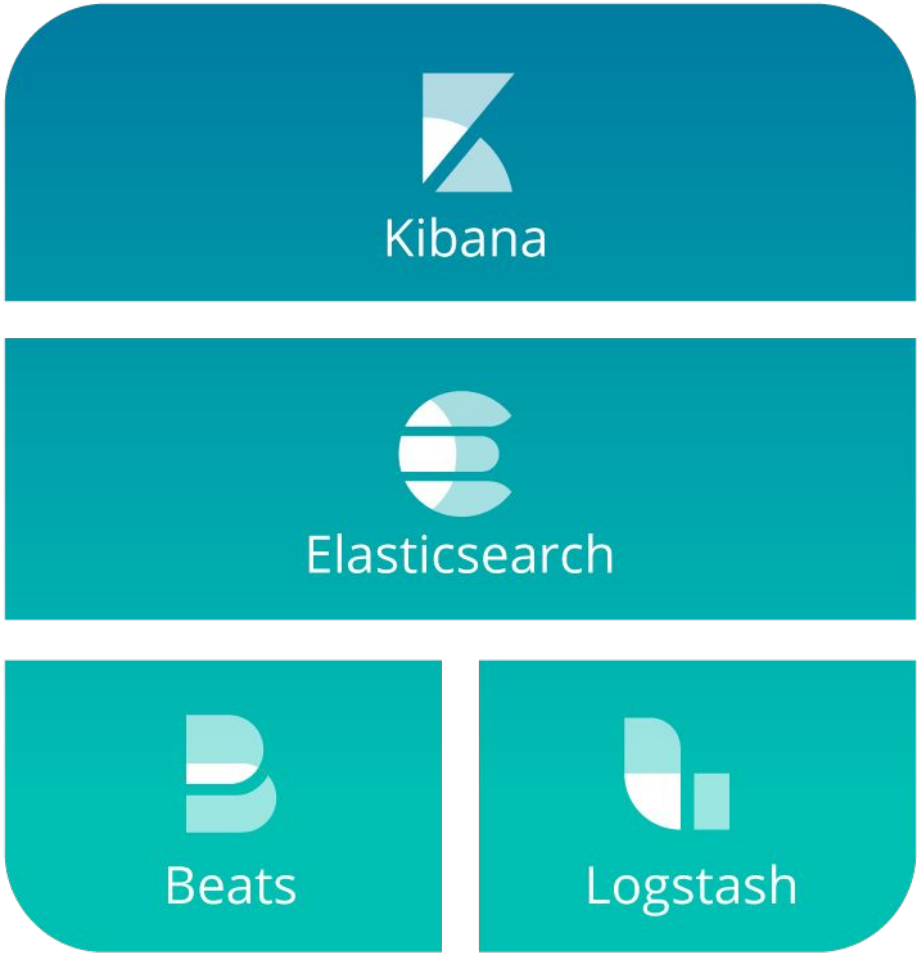
@exekias



elastic

Elastic Stack

100% open source
No enterprise edition
All new versions with 6.0

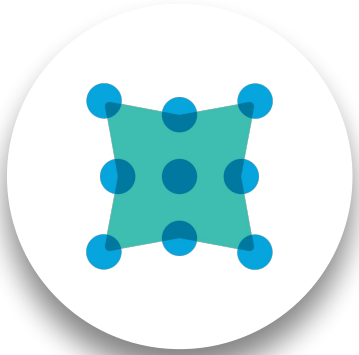


elastic


elastic

Beats is a family of lightweight shippers that collect and ship all kinds of operational data to Elasticsearch

The Beats family



Packetbeat

Network data

Metricbeat

Metrics

Winlogbeat

Windows Event Logs

Auditbeat

Audit data

Filebeat

Log files

Heartbeat

Uptime monitoring

+40 community Beats

elastic

Logs

Filebeat

Tails and ships logs

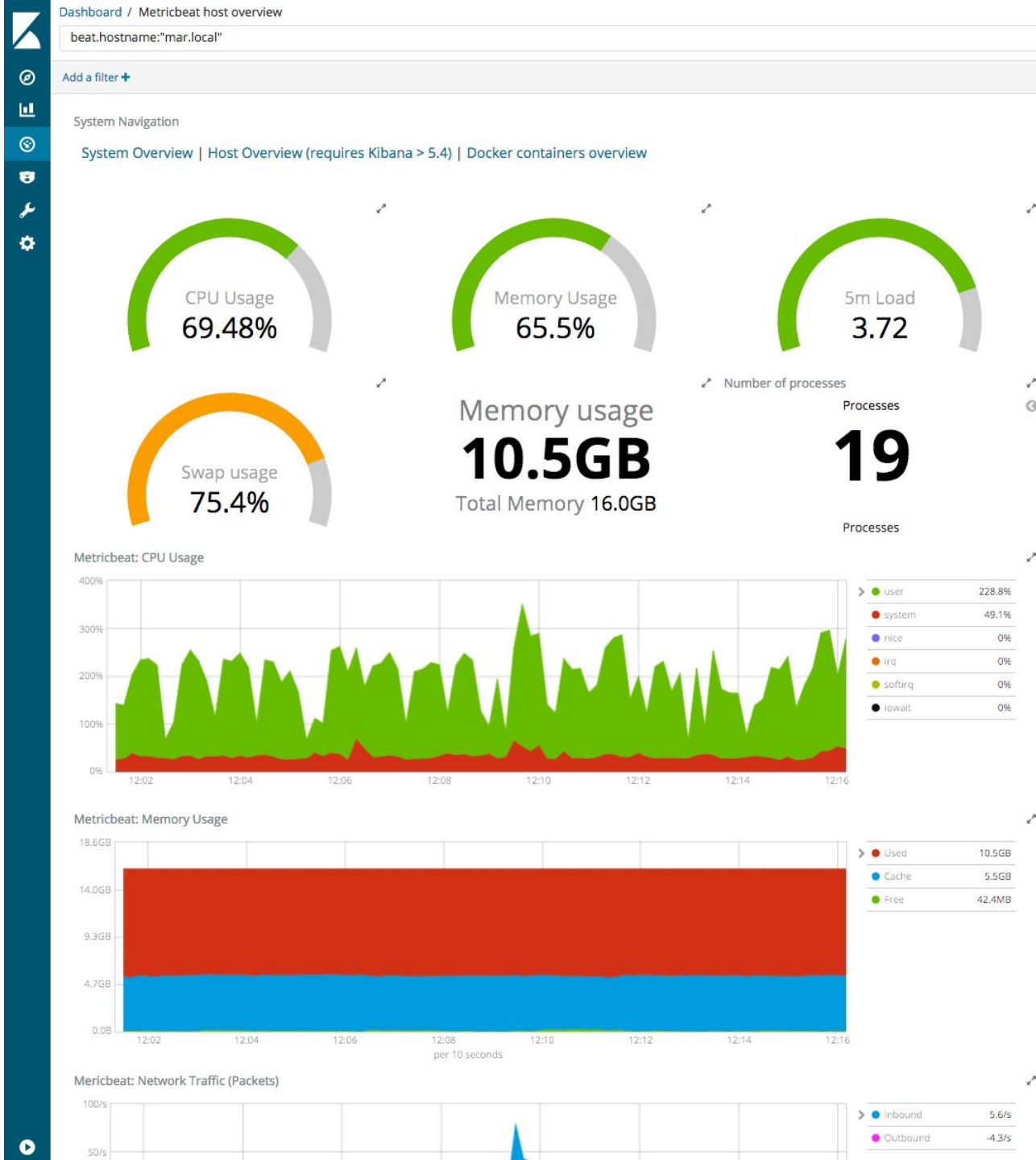
- Correctly handles log rotation
- Back-pressure sensitive
- “at least once” guarantee
- Structured logging
- Multiline
- Conditional filtering

Metrics & Events

Metricbeat

Ship metrics from OS & services

- Polls the API of services to collect metrics
- Efficiently stores metrics in Elasticsearch
- Application metrics via JMX/Jolokia, Prometheus, Dropwizard, Graphite



Packetbeat

Monitor services by sniffing packets

- “Distributed Wireshark”
- Parses protocols (HTTP, DNS...)
- Correlate the messages into transactions
- TLS handshake parsing

Heartbeat

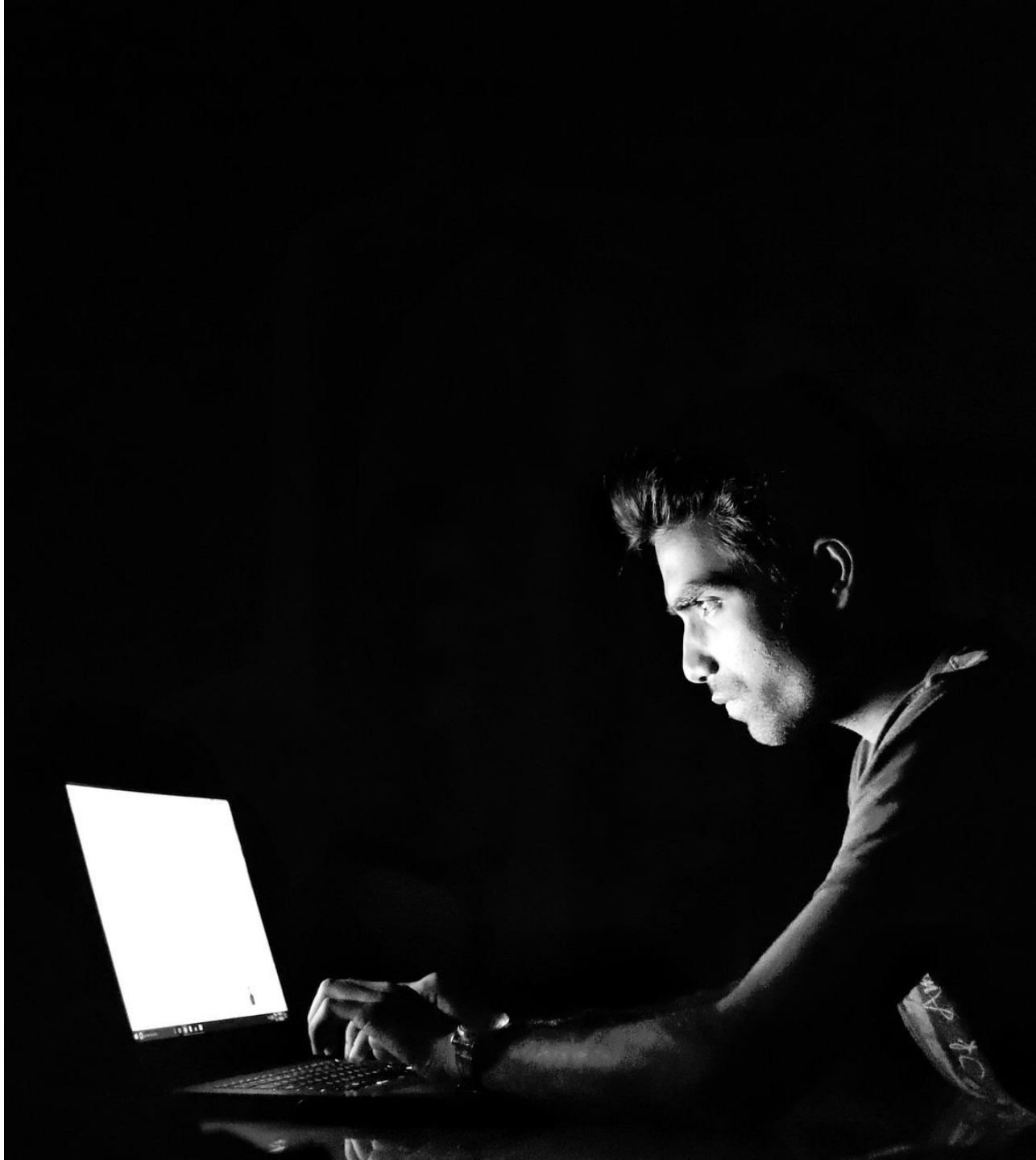
Ping remote services for availability

- Uptime monitoring
- HTTP, TCP and ICMP (ping)
- IPv4 & IPv6
- Cron-like scheduling
  - */5 * * * * * *
  - @every 5s

Auditbeat

Audit users & processes activity

- Listen events from Linux Audit Framework
- Group messages into a single event
- Sidecar auditd or standalone
- File Integrity Monitoring

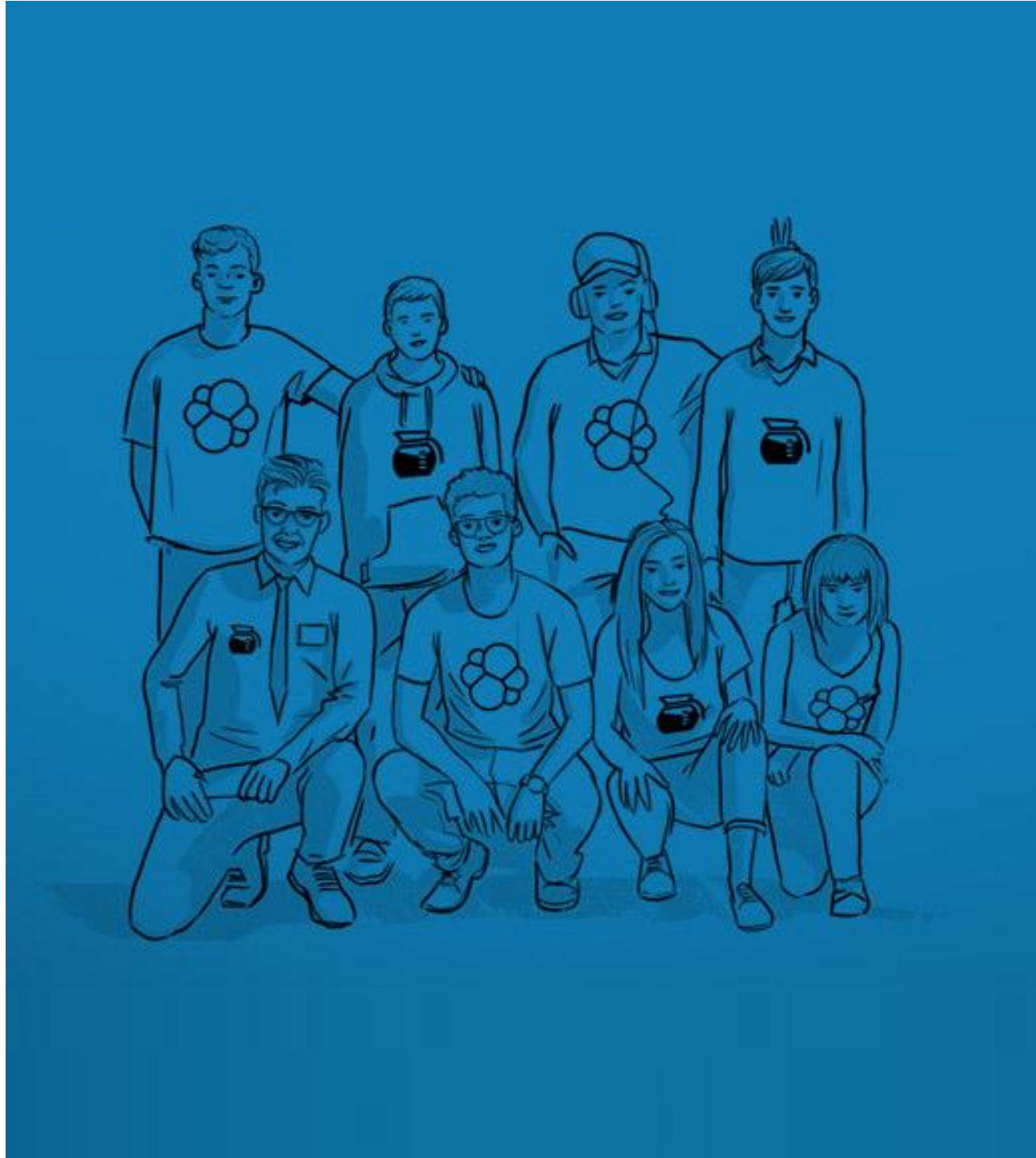


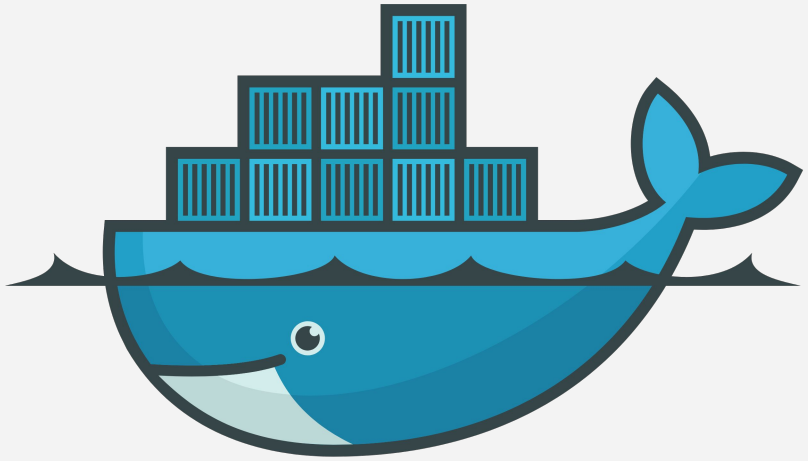
Traces

Elastic APM

Previously Opbeat, 6.0.0 in alpha

- apm-server based on libbeat
  - collects traces from agents
  - benefits from metadata processors
- Node.js & Python agents, more coming…





docker

kubernetes

elastic

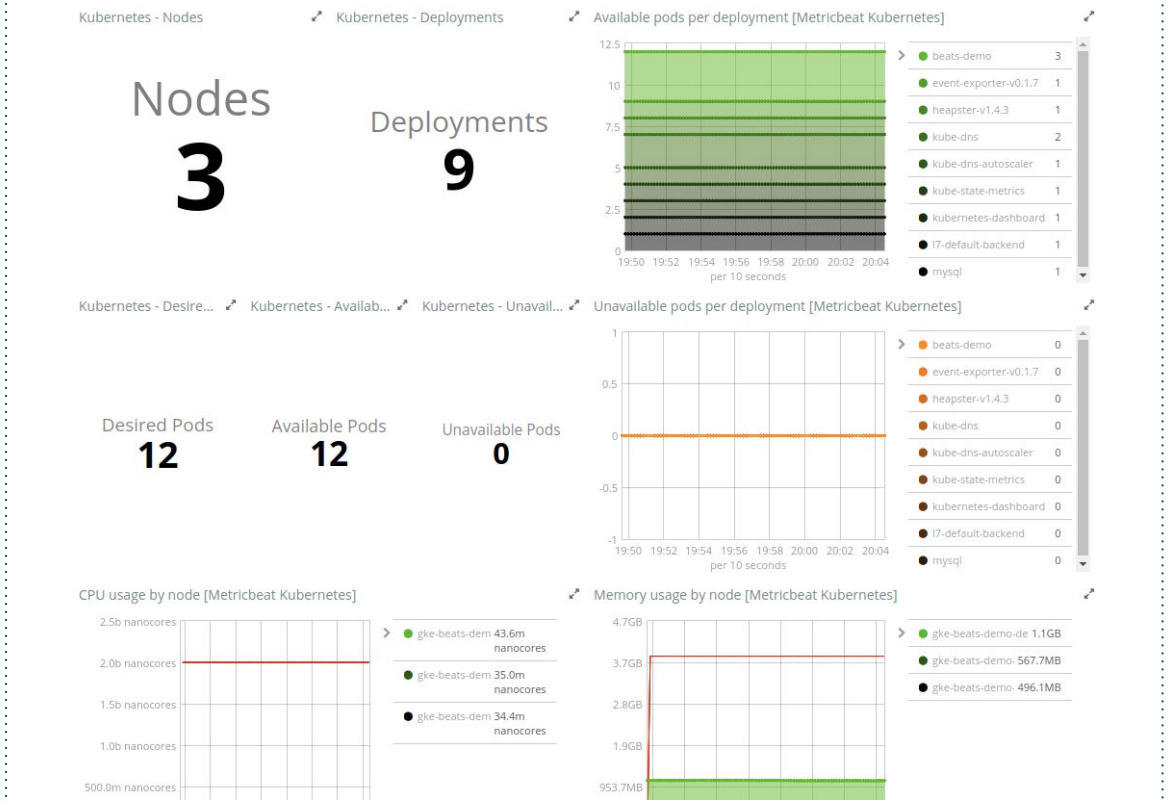
> ***With containers architecture everything is a moving target***

We need specific tools to track things down

elastic

Metricbeat modules

Monitor Docker & Kubernetes



elastic

Metadata processors

Enrich events with useful metadata to correlate logs, metrics & traces

add_cloud_metadata

- cloud.availability_zone
- cloud.region
- cloud.instance_id
- cloud.machine_type
- cloud.project_id
- cloud.provider

add_docker_metadata

- docker.container.id
- docker.container.image
- docker.container.name
- docker.container.labels

add_kubernetes_metadata

- kubernetes.pod.name
- kubernetes.namespace
- kubernetes.labels
- kubernetes.annotations
- kubernetes.container.name
- kubernetes.container.image

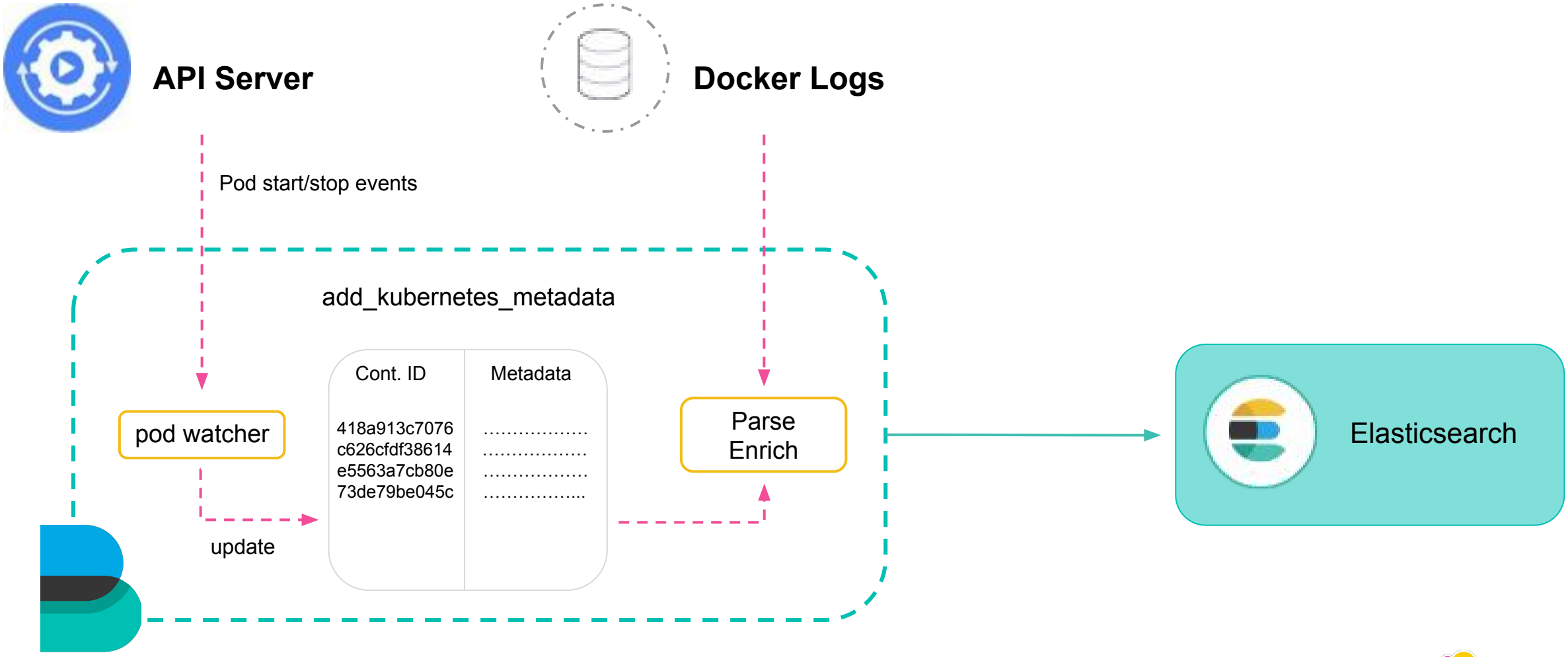
Metadata processors

Example


```
{
  "@timestamp": "2017-11-17T00:53:33.759Z",
  "message": "2017/11/07 00:53:32.804991 client.go:651: INFO Connected to Elasticsearch version 6.0.0",
  "kubernetes": {
    "pod": {
      "name": "filebeat-vqf85"
    },
    "container": {
      "name": "filebeat"
    },
    "namespace": "kube-system",
    "labels": {
      "k8s-app": "filebeat",
      "kubernetes.io/cluster-service": "true"
    }
  },
  "meta": {
    "cloud": {
      "instance_id": "6959555125944564951",
      "instance_name": "gke-demo-default-pool-6b42dcb3-z2x7",
      "machine_type": "projects/865493543029/machineTypes/n1-standard-1",
      "availability_zone": "projects/865493543029/zones/europe-west1-b",
      "project_id": "carlosperez-163008",
      "provider": "gce"
    }
  },
}
```

Metadata processors

add_kubernetes_metadata internals



elastic

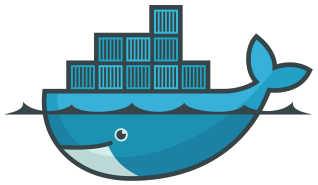
Autodiscover (new in 6.1)

Watch Docker events and react to changes

```
metricbeat.autodiscover:
  providers:
   - type: docker
     templates:
       - condition:
           contains.docker.container.image: etcd
         config:
          - module: etcd
            metricsets: ["leader", "self", "store"]
            hosts: "${data.host}:2379"
```

Autodiscover (new in 6.1)

Watch Docker events and react to changes



Events API
Container start/stop events

Beats

1. autodiscover event

```
{
  "host": "10.4.15.9",
  "port": 2379,
  "docker": {
    "container": {
      "id": "13a2...d716"
      "name": "etcd",
      "image": "quay.io/coreos/etcd:v3.0.0",
      "labels": {
        "io.kubernetes.pod.name": "etcd-4dk4c",
        "io.kubernetes.pod.namespace": "kube-system"
        ...
      }
    }
  }
}
```

2. match condition

3. var expansion

config template

```
- module: etcd
  metricsets: ["leader", "self", "store"]
  hosts: "${data.host}:2379"
```

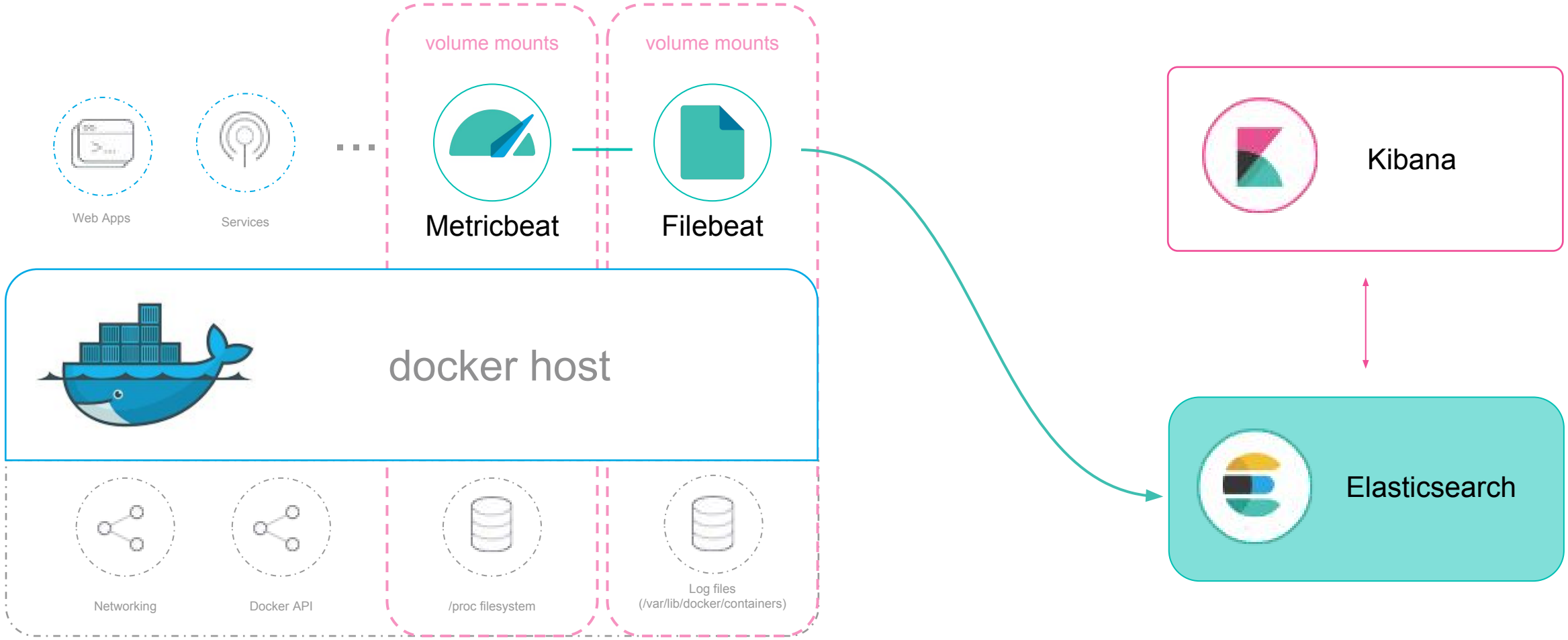
4. launch module

```
- module: etcd
  metricsets: ["leader", "self", "store"]
  hosts: "10.4.15.9:2379"
```


elastic

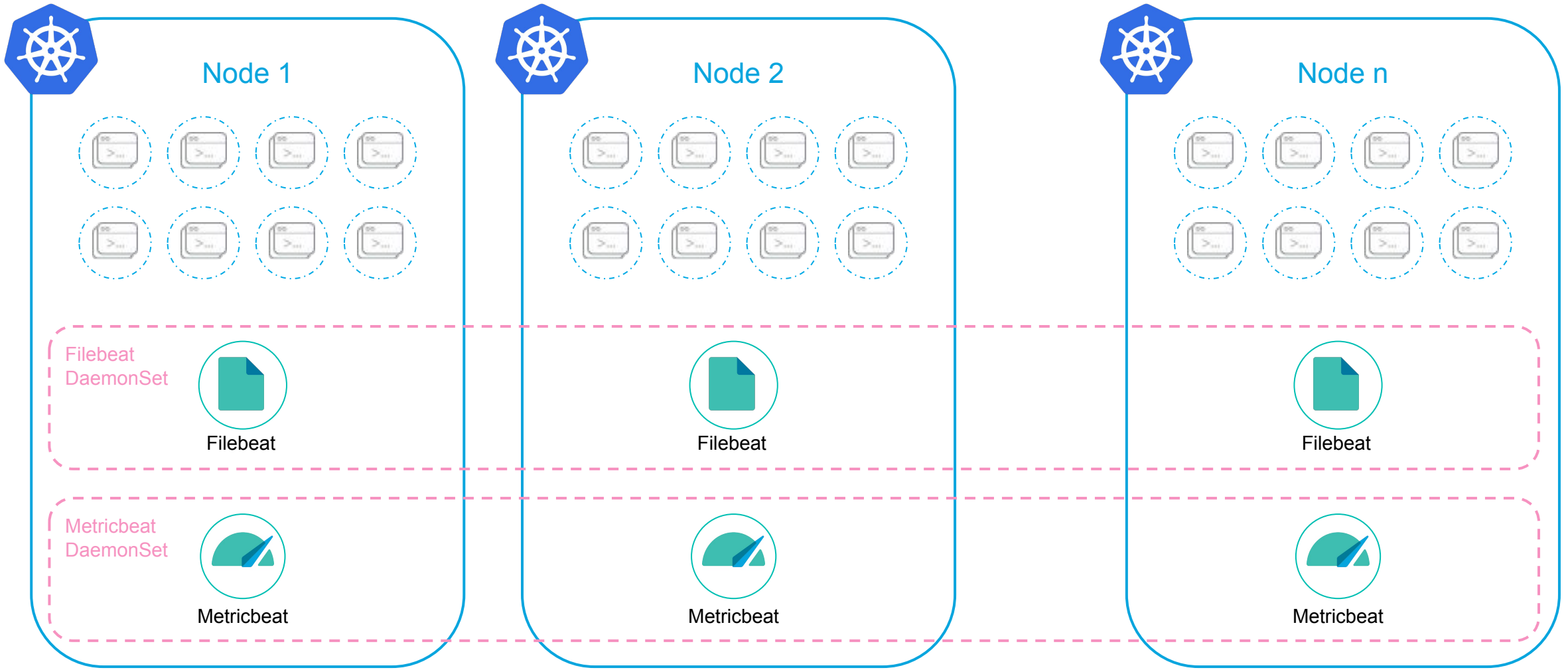
Deployment strategies

Docker deployment



elastic

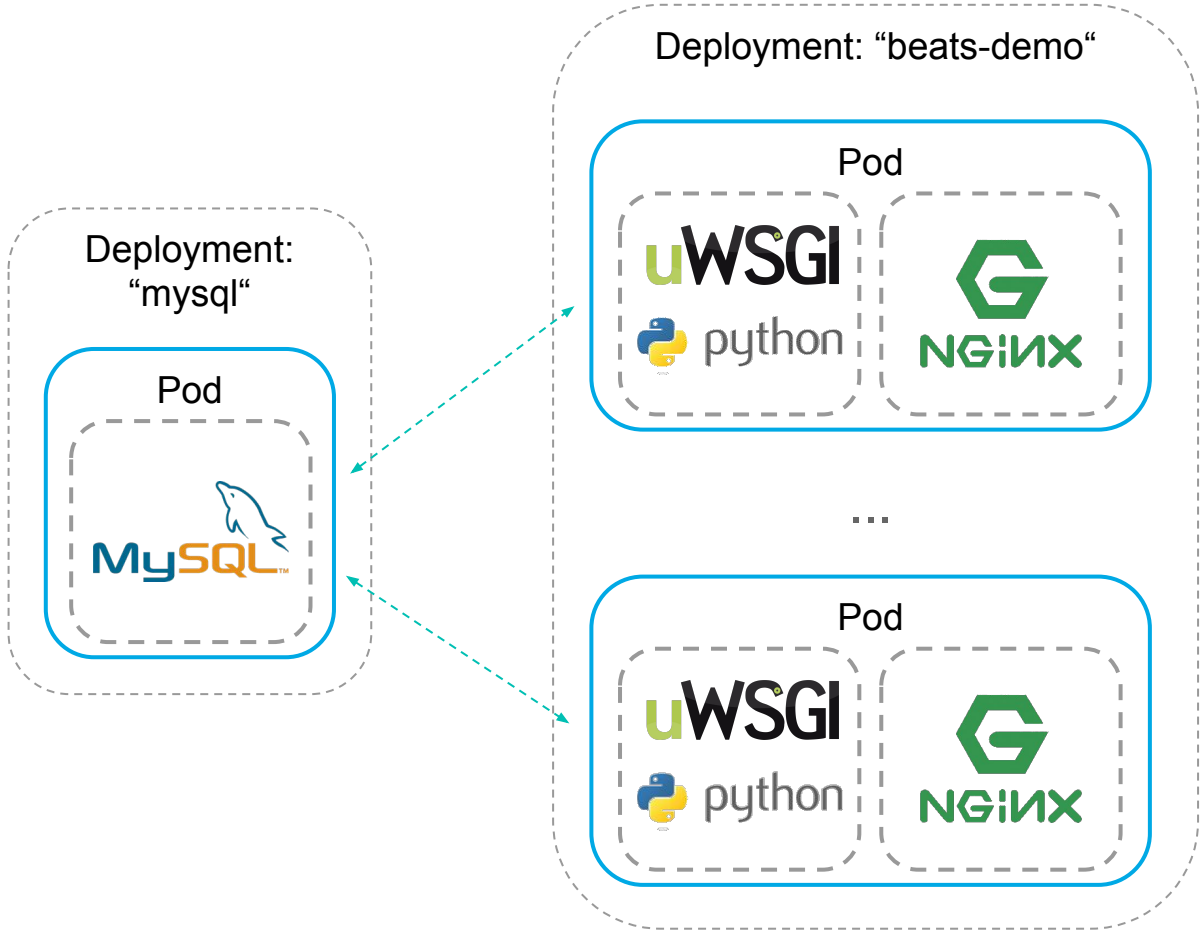
Kubernetes deployment

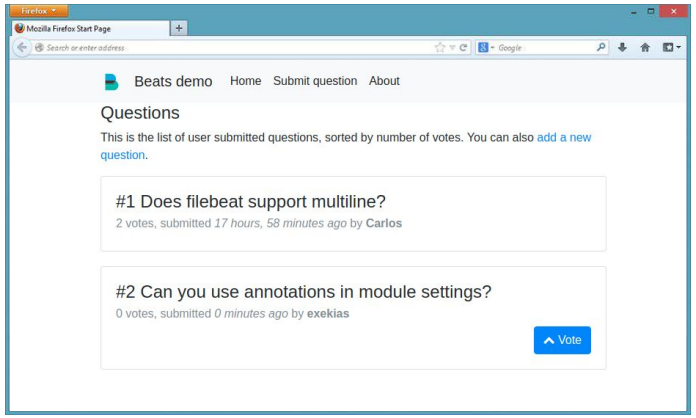


elastic

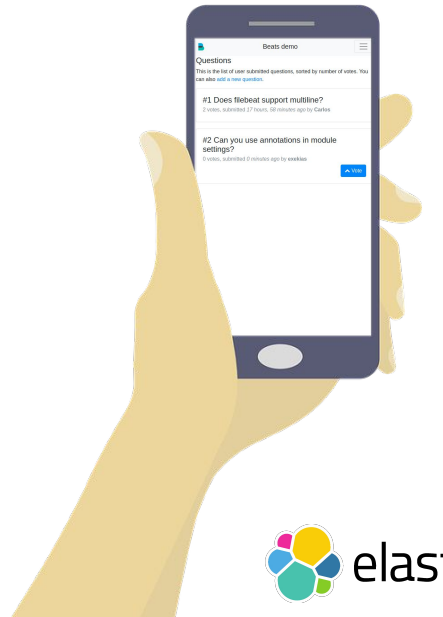
Demo time

Demo scenario:
https://github.com/exekias/beats-kubernetes-demo





- Logs
- Metrics
- Network analytics
- App Performance Metrics



elastic

Thank you!

Carlos Pérez-Aradros

Software Engineer

carlos@elastic.co

@exekias

PS: Stickers!

elastic