elastic | 中国开发者大会

Getting Logs and Metric from Kubernetes with Beats

Nicolas Ruflin
Elastic



战略级赞助商 HUAWEI | 钻石级赞助商 普翔 | 白金级赞助商 华夏博格 神州数码 Digital China | 金牌级赞助商 iDataAPI

合作伙伴 开源中国 oschina.net 掘金 谱时 IT大咖说 otpub Broadview 百格活动 bagevent.com MAXHUB

Getting Logs and Metric from Kubernetes with Beats

Nicolas Ruflin
Software Engineer at Elastic
@ruflin



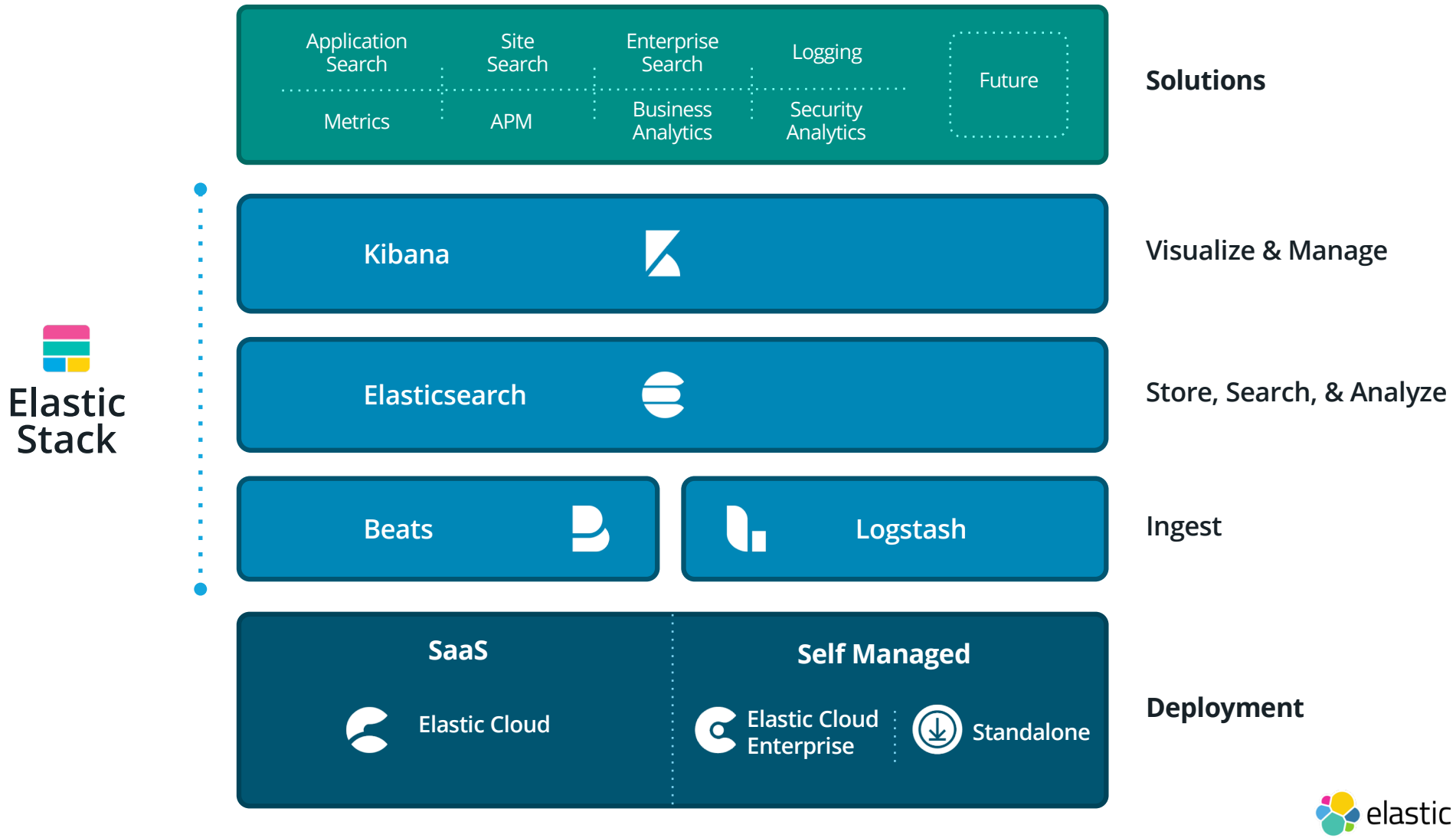
Nicolas Ruflin

Software Engineer at Elastic


ruflin@elastic.co


@ruflin

elastic


Elastic Stack
Application Search
Site Search
Enterprise Search
Logging
Metrics
APM
Business Analytics
Security Analytics
Future
Solutions
Kibana
Visualize & Manage
Elasticsearch
Store, Search, & Analyze
Beats
Logstash
Ingest
SaaS
Elastic Cloud
Self Managed
Elastic Cloud Enterprise
Standalone
Deployment
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

elastic

Filebeat

Tails and ships logs

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



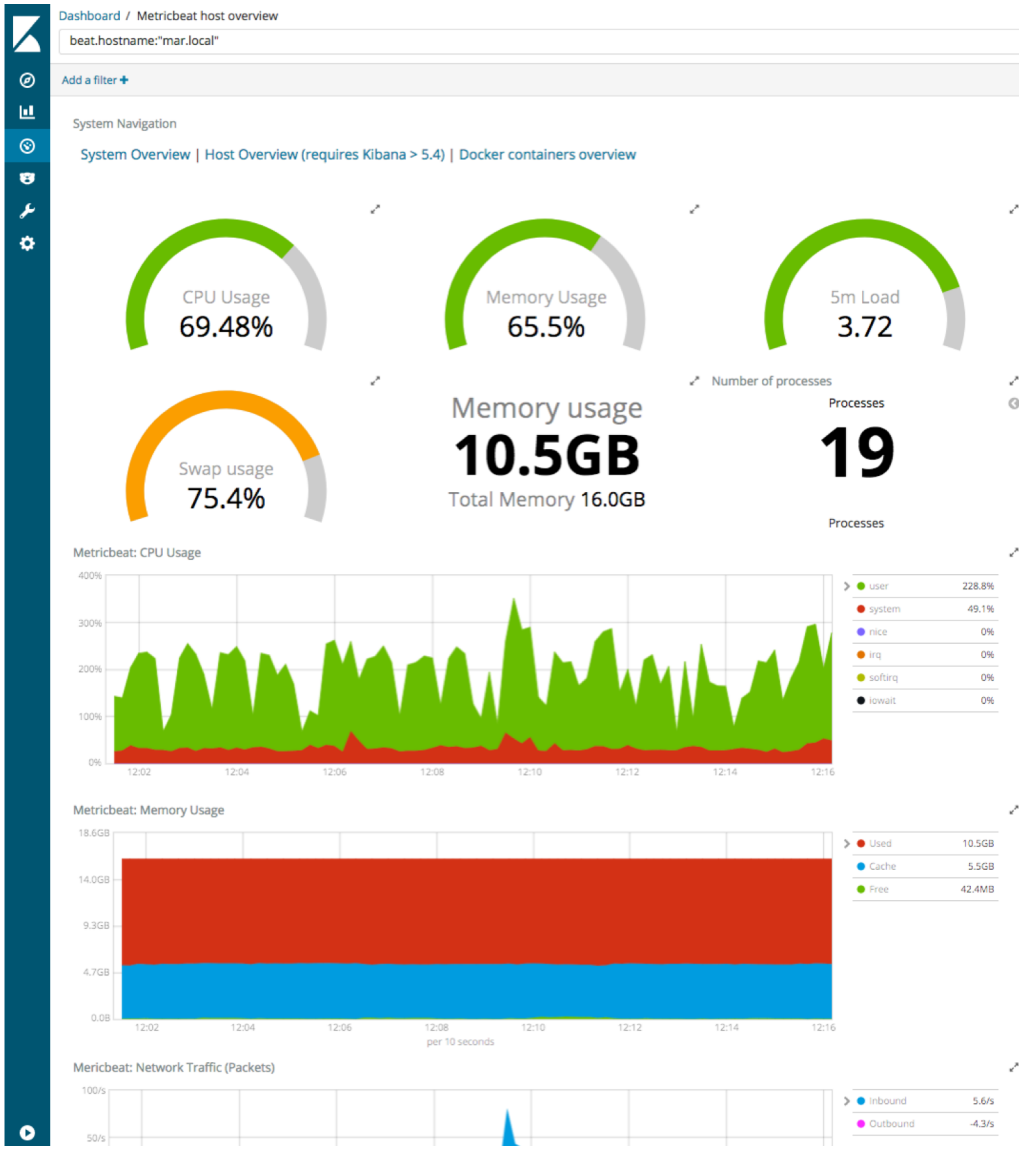
Metrics & Events

elastic

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

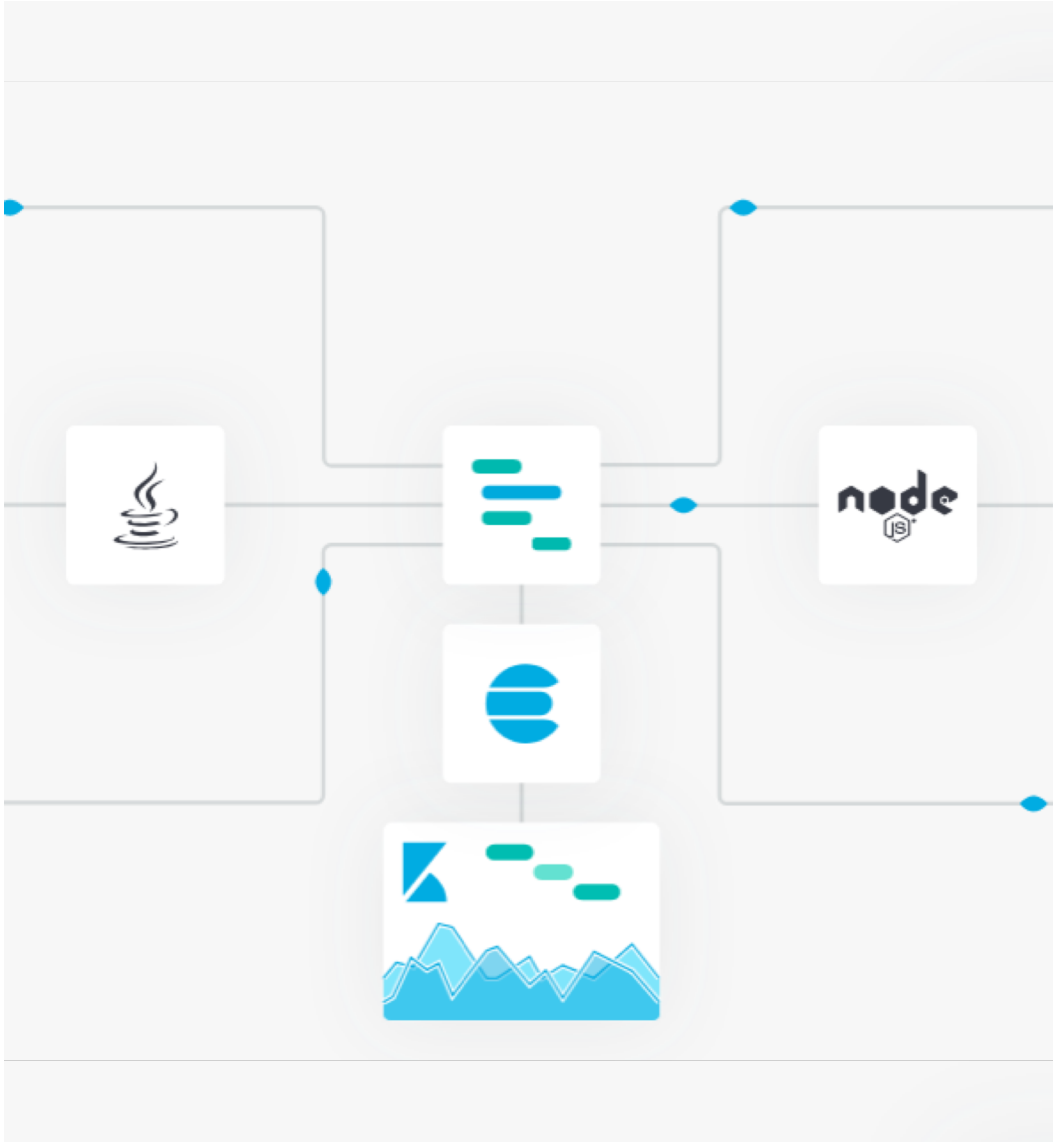


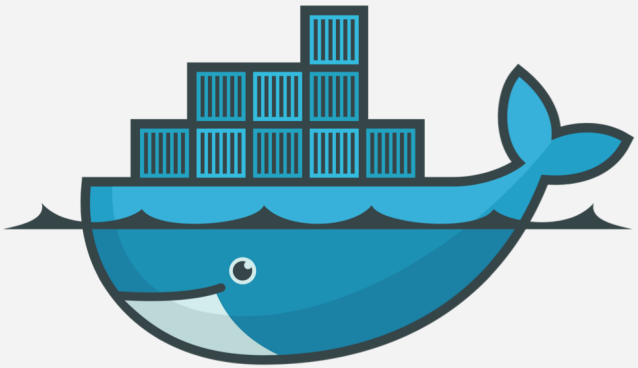
Traces

elastic

Elastic APM

- apm-server based on libbeat
  - collects traces from agents
  - benefits from metadata processors
- Node.js, Python, Rails, JS, Java, Go agents...
- RUM





docker



kubernetes

elastic


With containers architecture everything is a moving target
We need specific tools to track things down

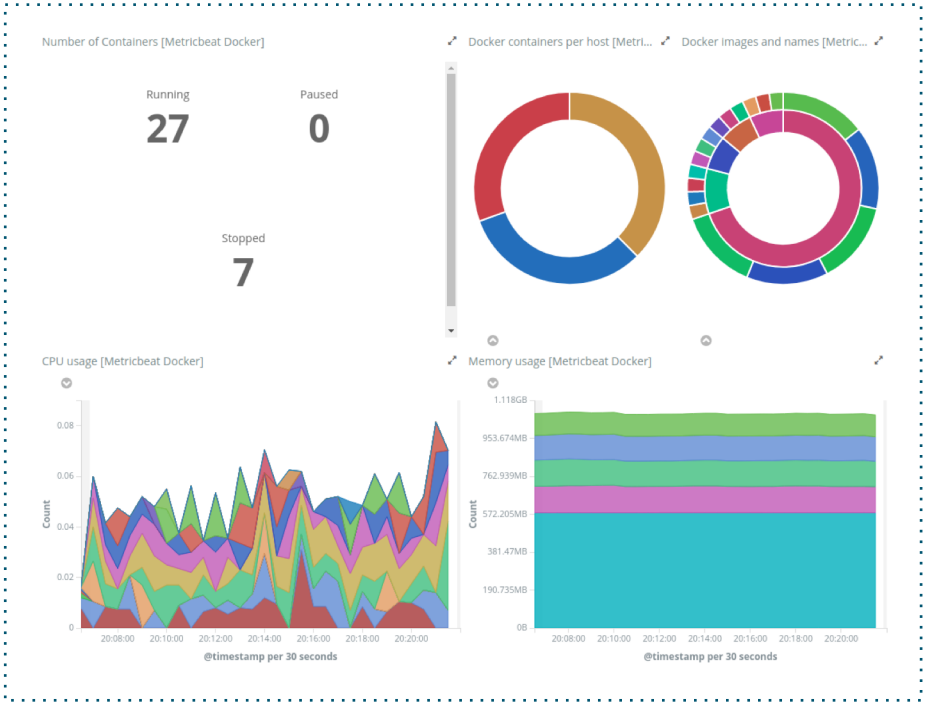
Beats containers toolbox

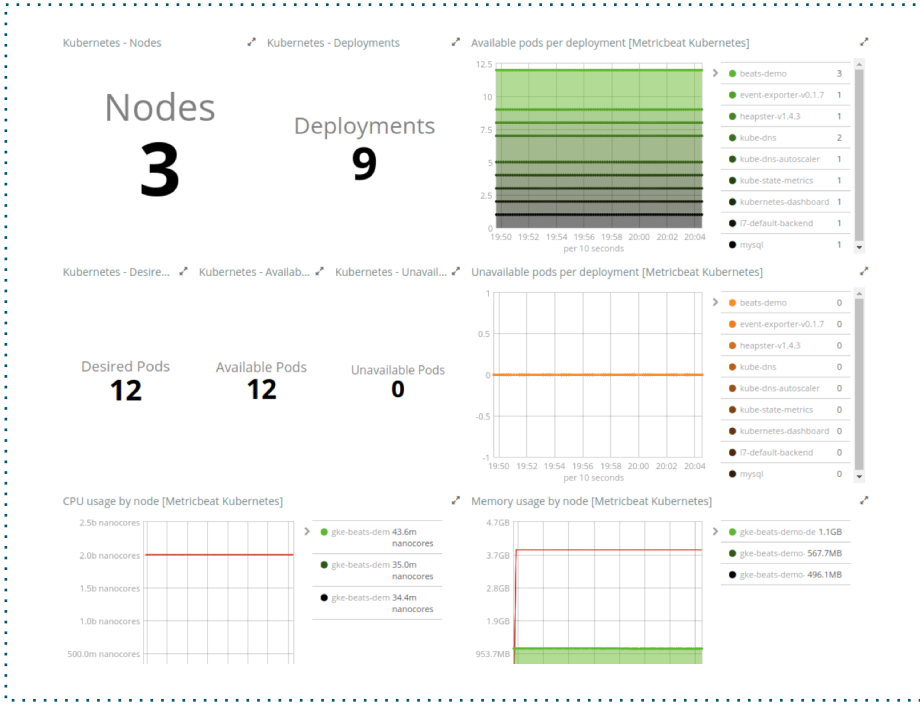
1. Modules: System, Docker and Kubernetes
2. Docker logs input
3. Metadata processors
4. Autodiscover

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

elastic

Metadata processors

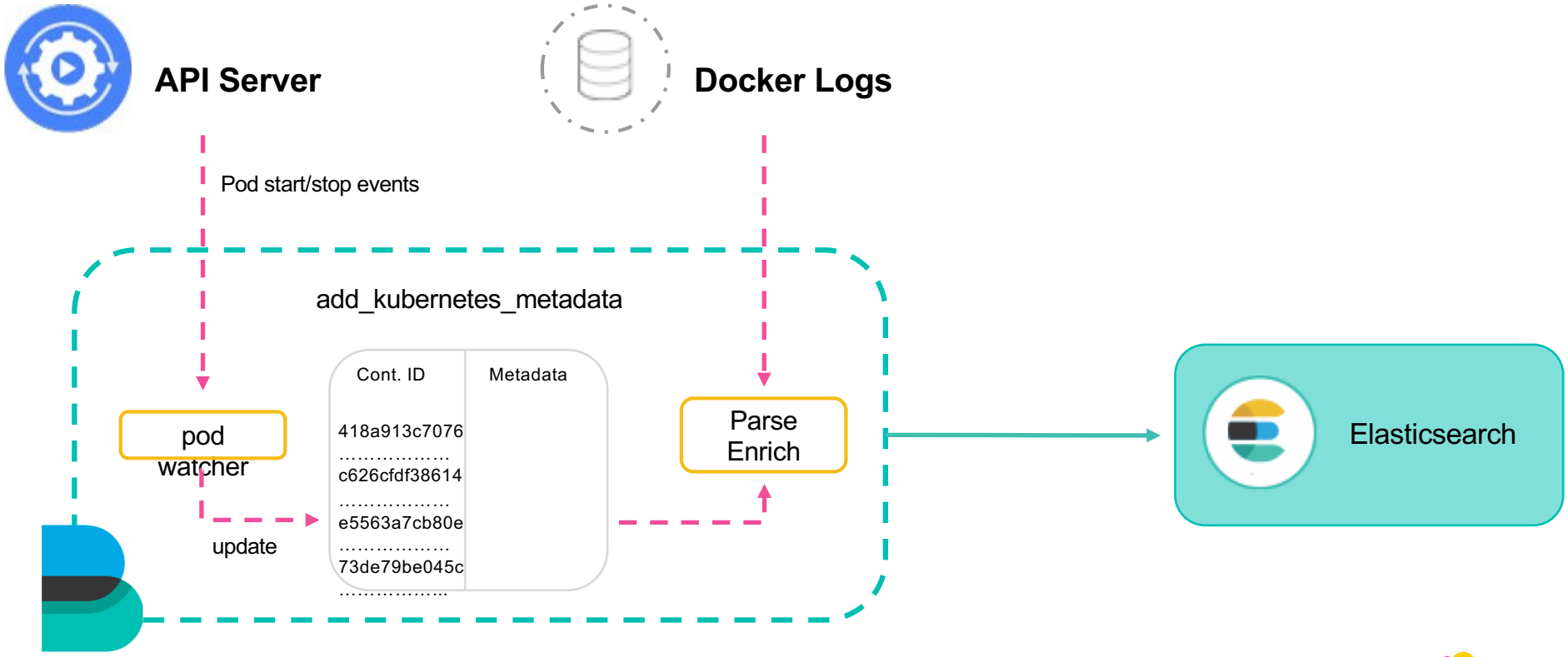
Example


```
{
  "@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"
    }
  },
}
```


elastic

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"
```


elastic

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

Autodiscover: Kubernetes (new in 6.2)

Watch Kubernetes events and react to changes

```
filebeat.autodiscover:
  providers:
    - type: kubernetes
      include_annotations: ["harvest"]
      templates:
        - condition:
            contains:
              kubernetes.annotations.harvest: true
          config:
            - type: docker
              containers.ids:
                - ${data.kubernetes.container.id}
```


elastic

Autodiscover: Hints based autodiscover (new in 6.3)

Invert control of monitoring settings

```
filebeat.autodiscover:
  providers:
    - type: kubernetes
      hints.enabled: true
```


elastic

Autodiscover: Hints based autodiscover (new in 6.3)

Invert control of monitoring settings

```
Labels / Annotations:
  co.elastic.logs/module: nginx
  co.elastic.logs/fileset.stdout: access
  co.elastic.logs/fileset.stderr: error

  co.elastic.metrics/module: nginx
  co.elastic.metrics/hosts: "${data.host}:8080"

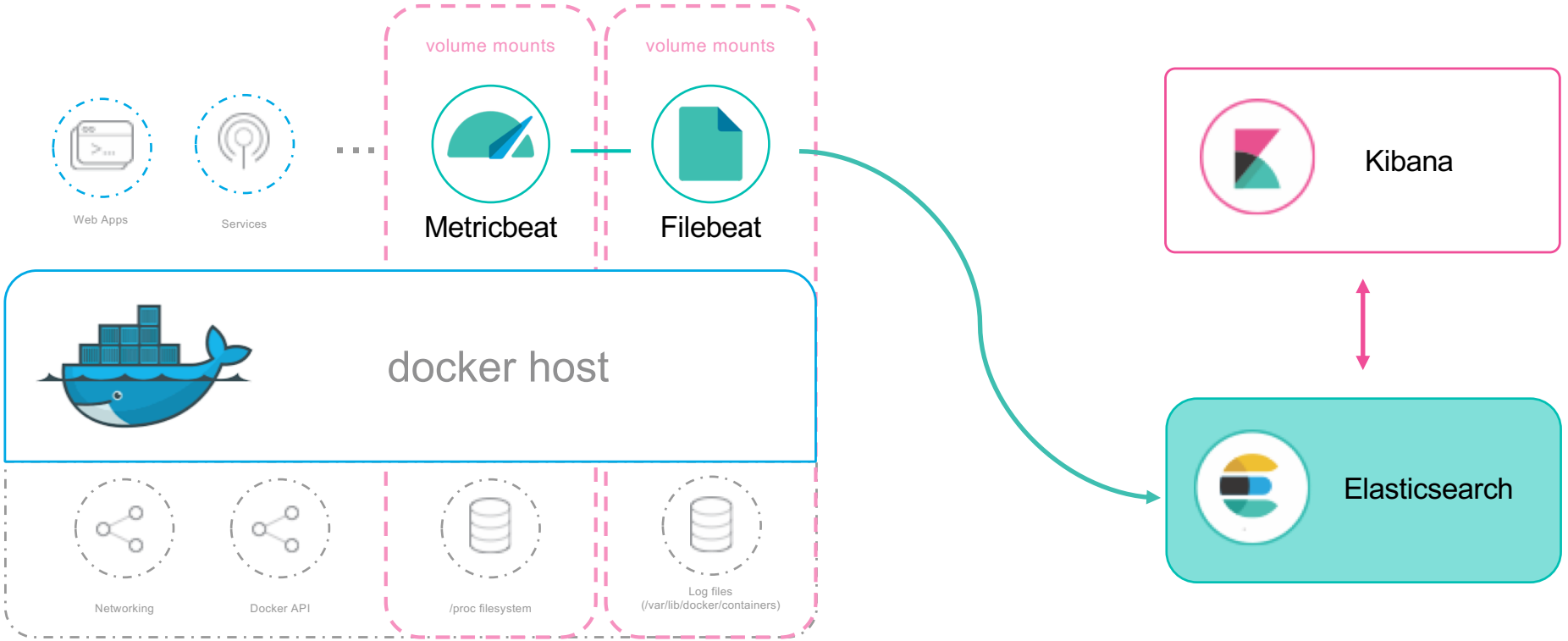
  co.elastic.logs/multiline.pattern: '^\['
  co.elastic.logs/multiline.negate: 'true'
  co.elastic.logs/multiline.match: after
```


elastic

Deployment Strategies

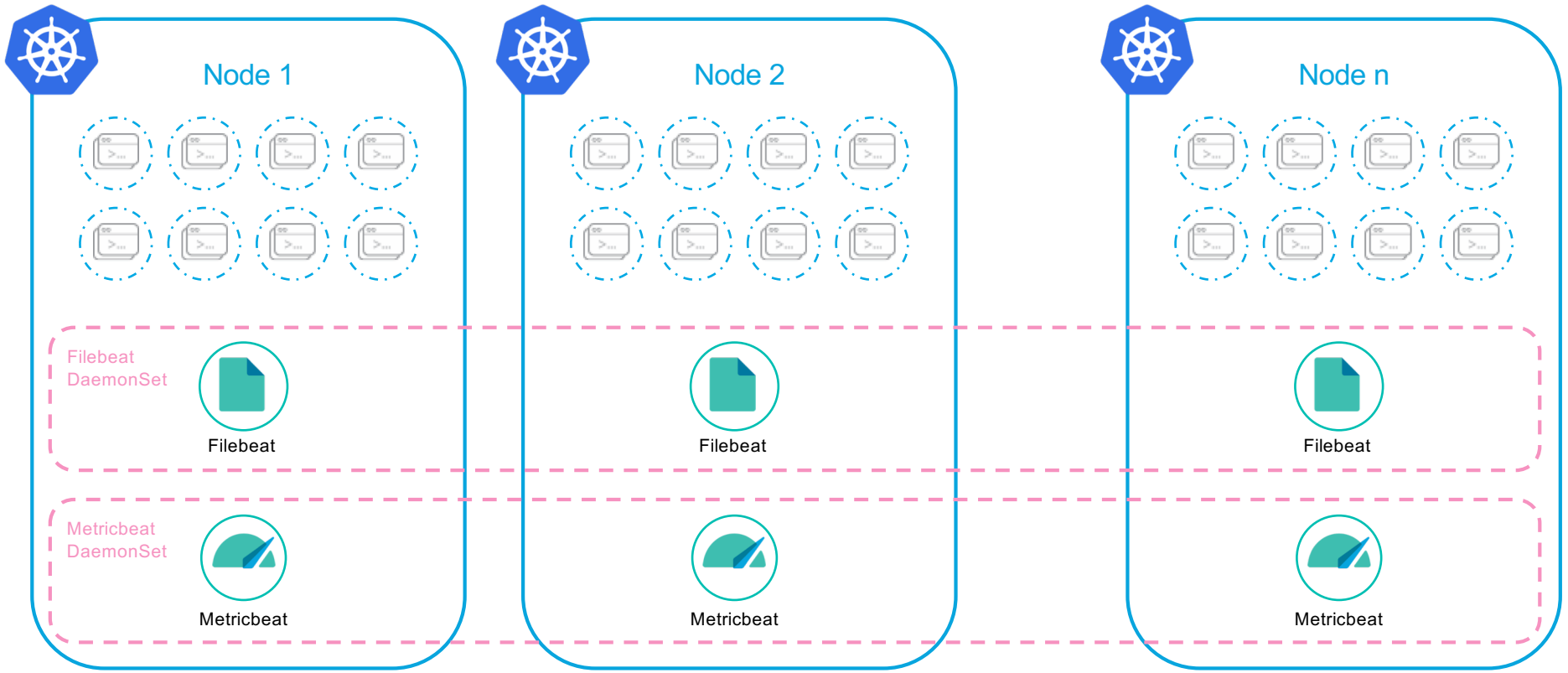


Docker deployment



elastic

Kubernetes deployment



elastic

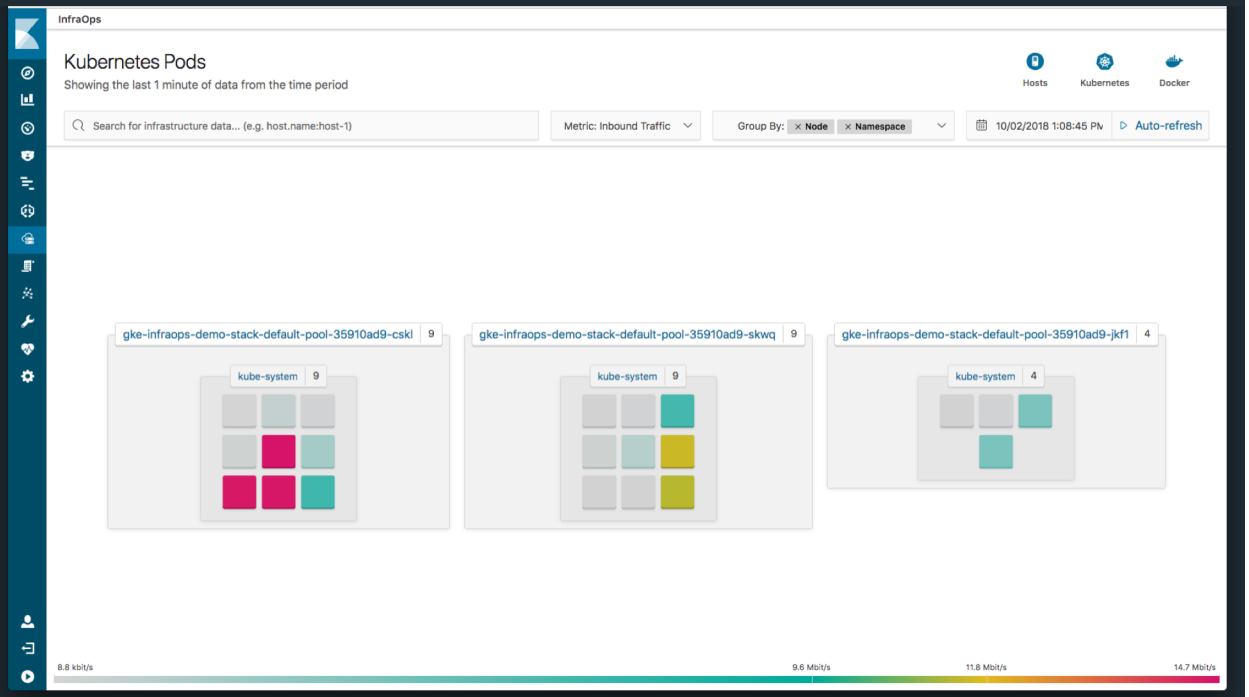
Infrastructure & Logs UI

elastic

Infrastructure Solution

Creates a curated experience for operators of infrastructure

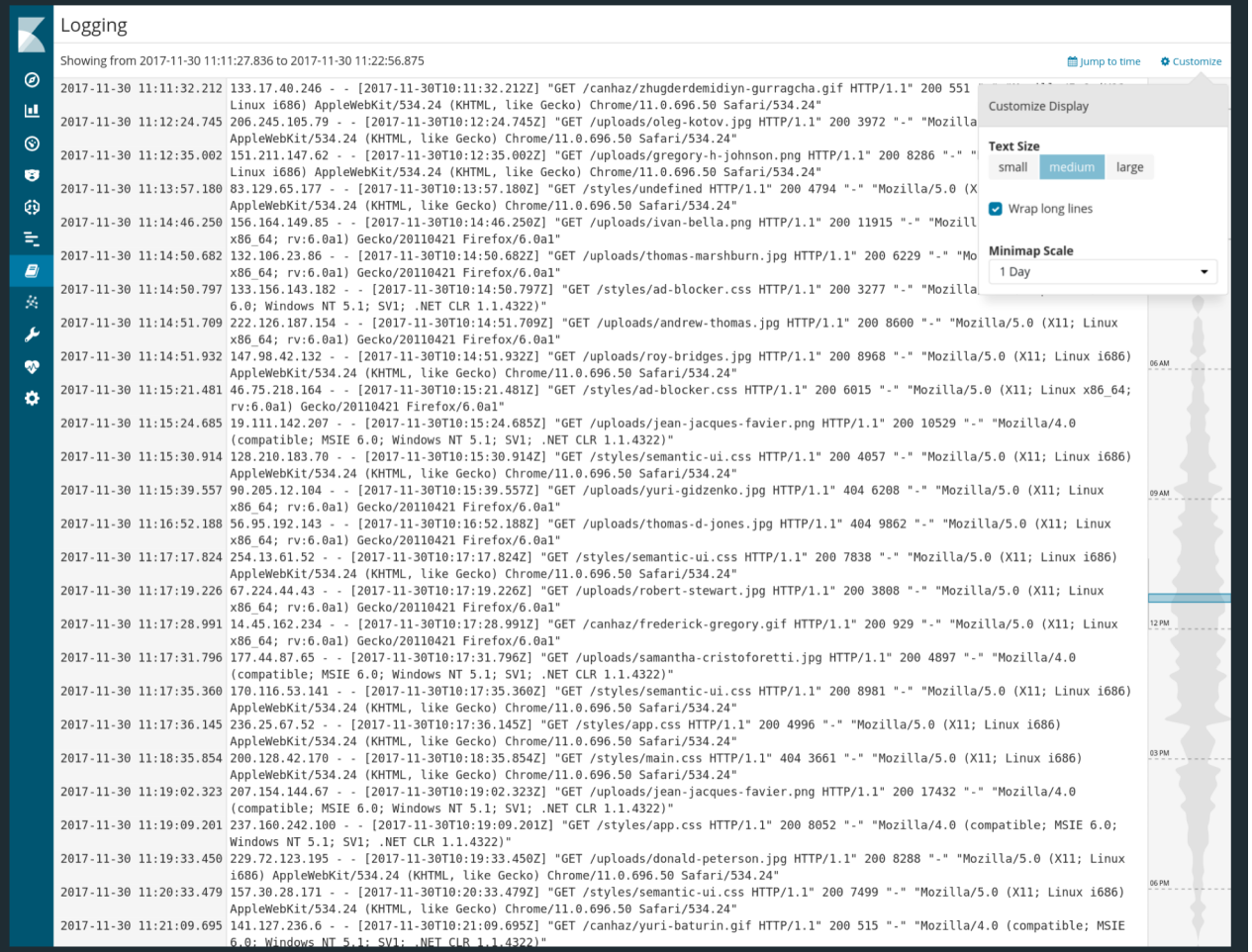
- Visual summaries that scale to 100K+ infrastructure elements
- Native support for container orchestration frameworks, e.g. Kubernetes/Docker
- Drill down to metrics, logs, APM views
- Adhoc and structured search



Logs Solution

Compact log viewer optimized for live log event troubleshooting

- Console-like display
- Customizable
- Live log tailing
- Historical logs infinite scroll
- Adhoc and structured search



Demo time



THANK YOU

Nicolas Ruflin

Sr. Software Engineer


ruflin@elastic.co


@ruflin

elastic



elastic
中文社区

专业、垂直、纯粹的 Elastic 开源技术交流社区
https://elasticsearch.cn/

elastic