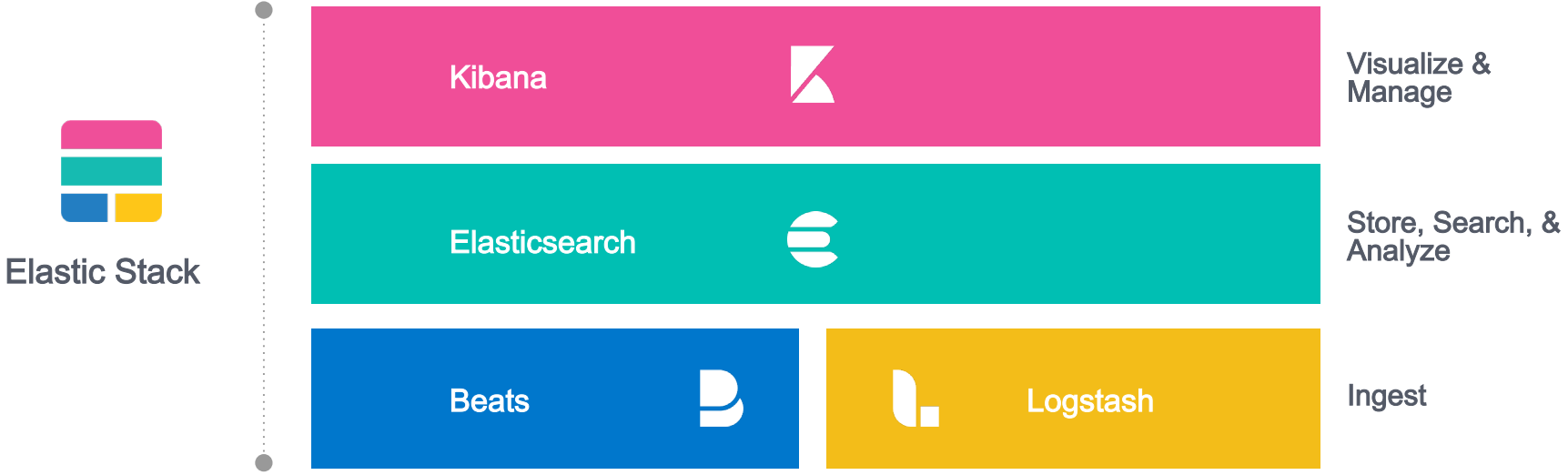
Three Pillars of Observability in Kubernetes with Elastic Stack

Eric Westberg
Solutions Architect, Elastic

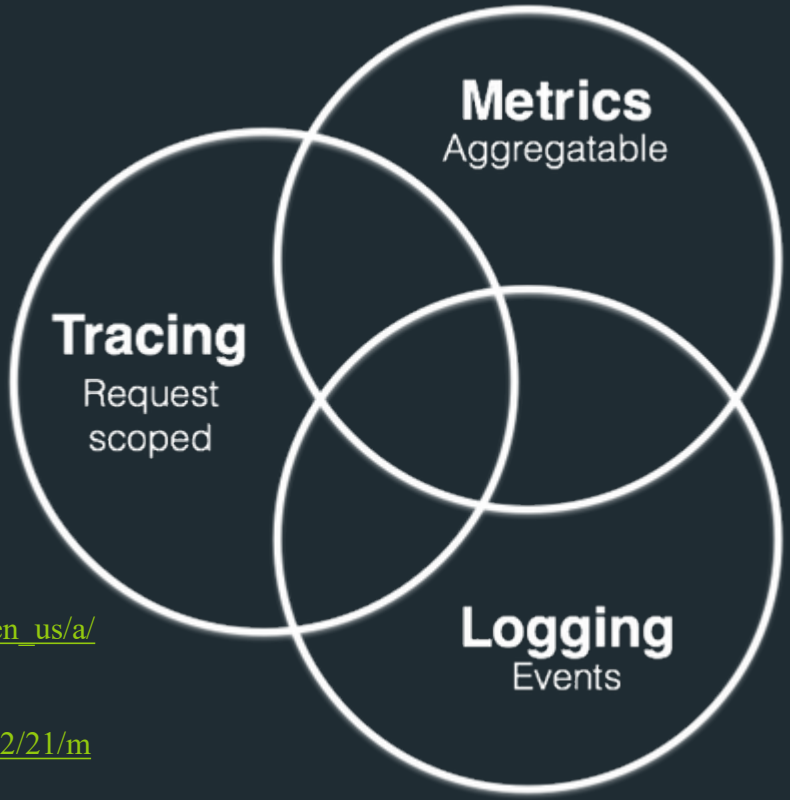
Elastic **Stack**



Kubernetes is Taking Over the Enterprise

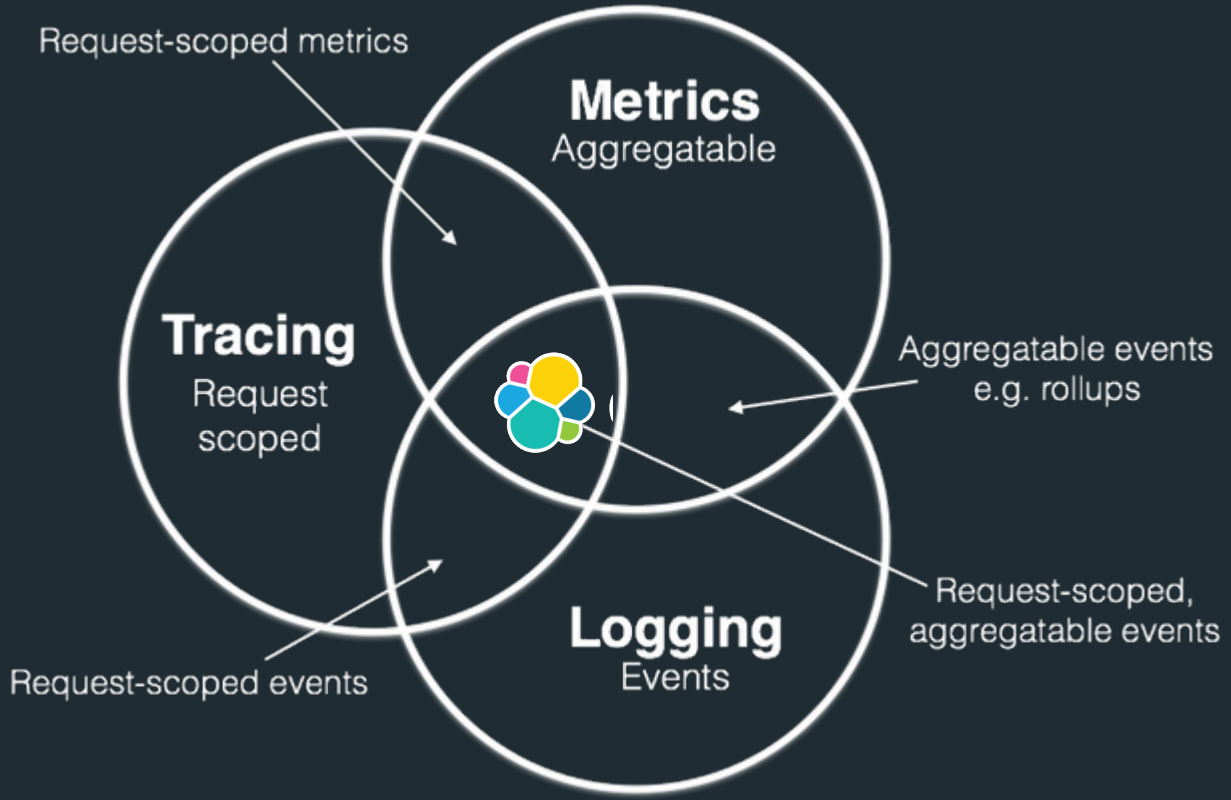
- Custom on-prem & cloud deployments
- Public cloud fully-managed deployments
  - Google Kubernetes Engine (GKE)
  - Amazon Elastic Container Service for Kubernetes (EKS)
  - Azure Kubernetes Service (AKE)
- Pivotal Container Service (PKS)
- Red Hat OpenShift

It Comes Down to The Three Pillars of Observability



Twitter:
https://blog.twitter.com/engineering/en_us/a/2013/observability-at-twitter.html
Peter Bourgon
https://peter.bourgon.org/blog/2017/02/21/metrics-tracing-and-logging.html

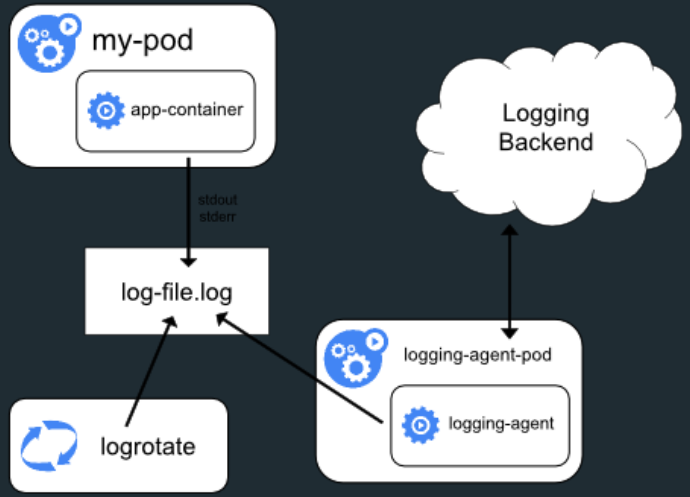
Elastic at the Center Stage



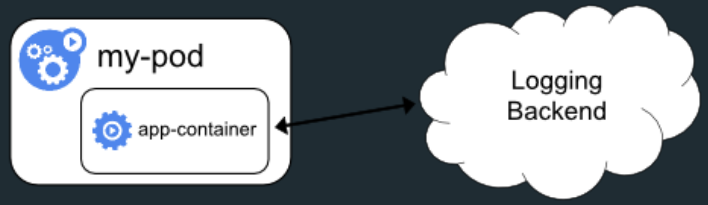
Logging

- Cluster level logging
- Services logging (eg. nginx, mysql)
- Custom application logging

Kubernetes Logging

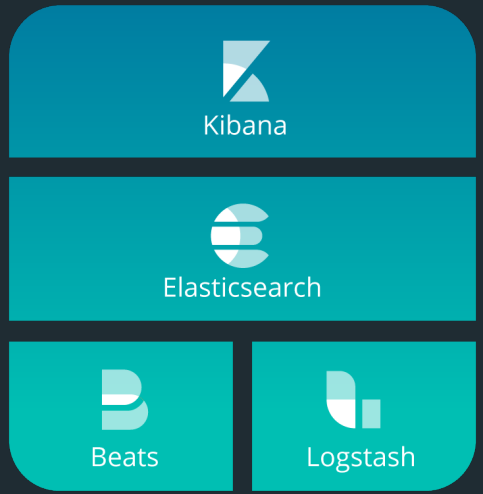


- Need for a logging solution
  - Kubernetes does **not** have a native solution
  - `kubectl logs` is too hard for large clusters
- Cluster-level logging
  - Logs have separate storage and lifecycle independent of nodes, pods and containers
  - Kubernetes provides no native storage solution for log data
- Application-level logging
  - Complicated
  - Packaged applications (eg. nginx)
  - Custom applications

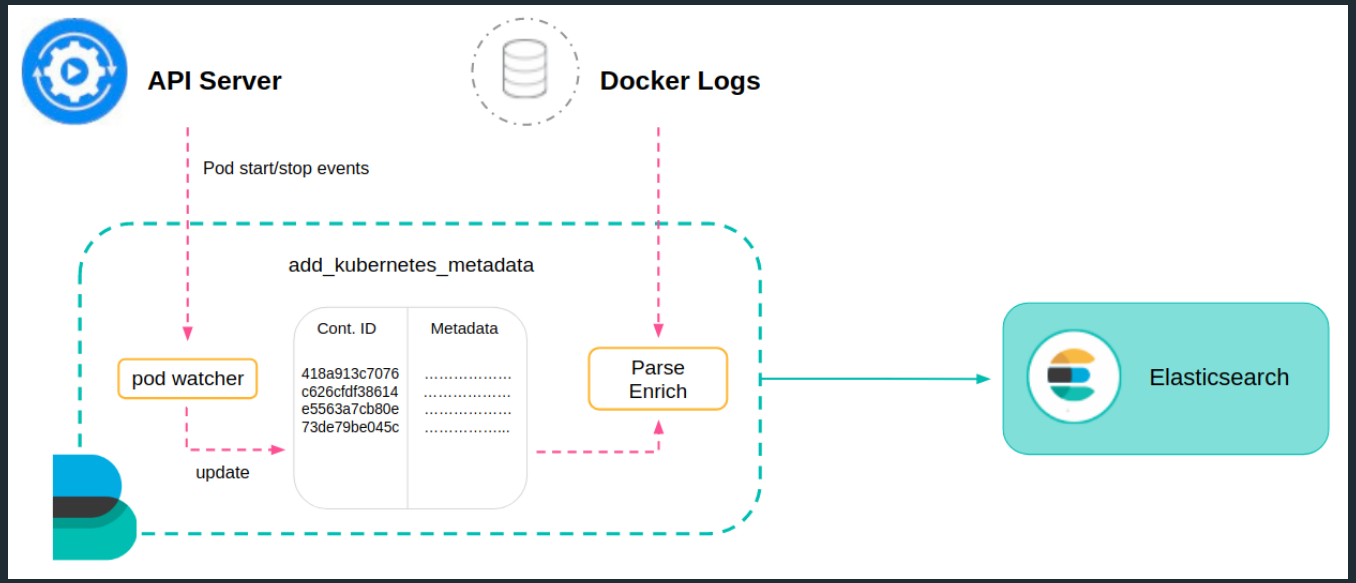


Two Packaged Solutions

- Fluentd DaemonSet
  - Log collection, parsing and distribution
- Fluentd + Stackdriver for GCP
- Fluentd + Elasticsearch

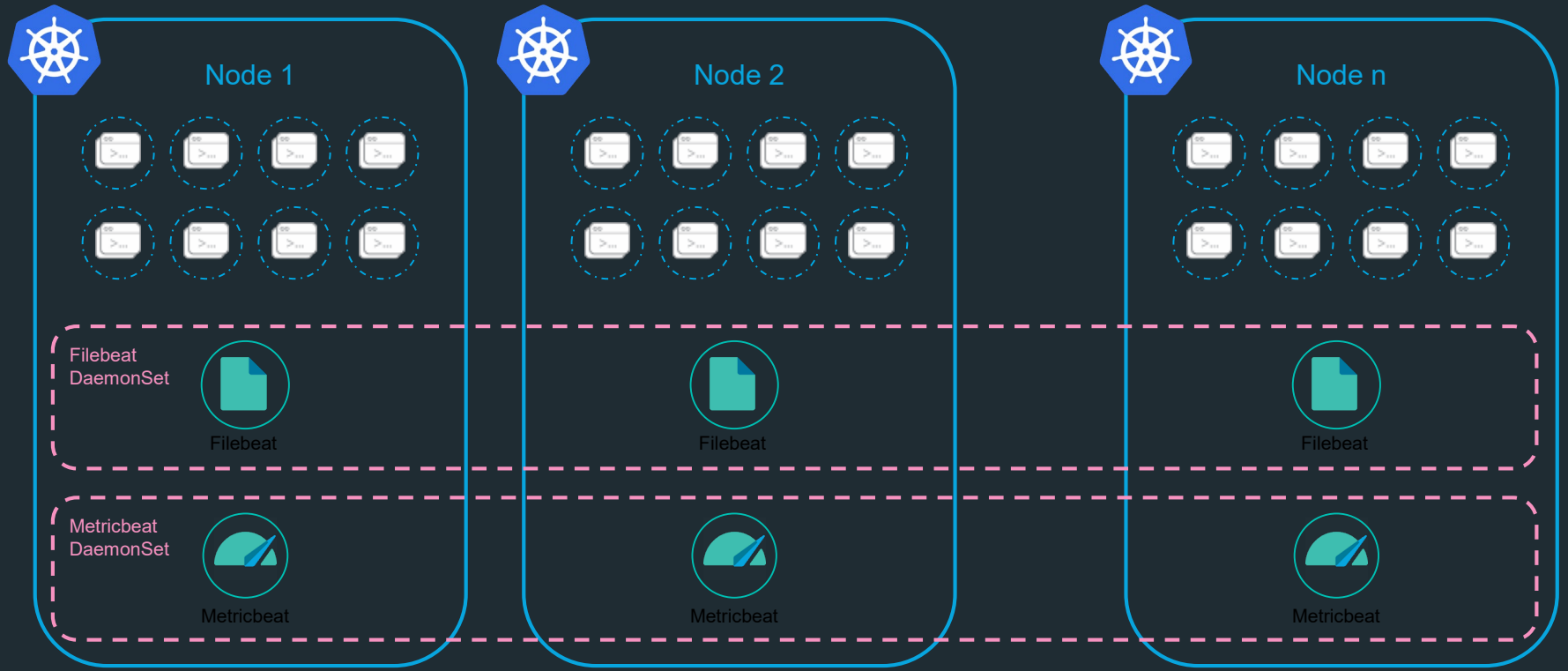


Better Log Collection with Filebeat




```
kubectl create -f filebeat-kubernetes.yaml
```

Kubernetes deployment



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

Filebeat Auto-Discovery

```
filebeat.autodiscover:
  providers:
    - type: kubernetes
      templates:
        - condition:
            contains:
              kubernetes.container.image: "nginx"
          config:
            - module: nginx
              access: # For nginx access log
                prospector:
                  type: docker
                  containers.ids:
                    - "${data.kubernetes.container.id}"
```

- A module contains
  - Log file path
  - Ingest pipeline
  - Fields definitions
  - Sample dashboards

Filebeat Modules

Simplify collection, parsing and visualization of common log formats

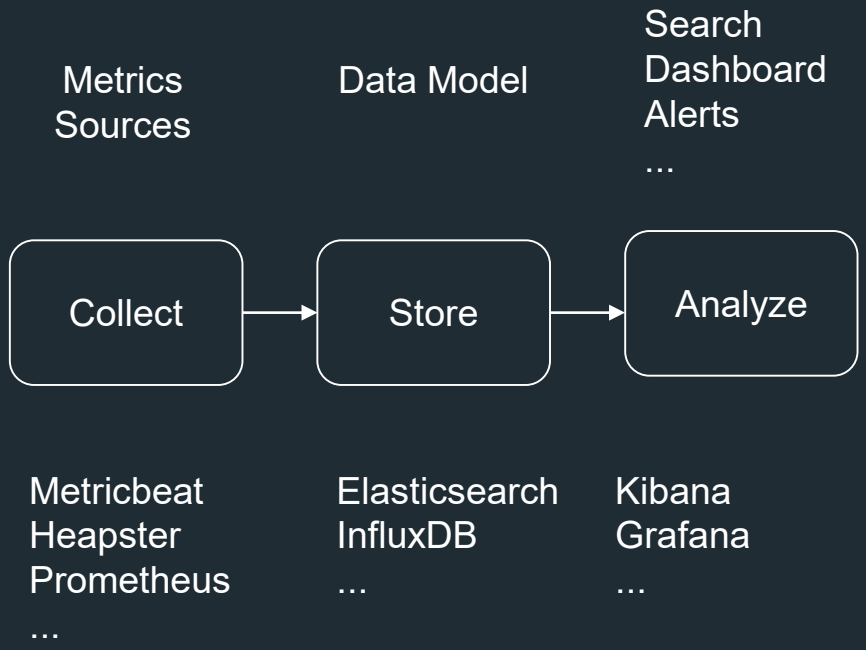
- *Apache2 module*
- *Auditd module*
- *Icinga module*
- *IIS module*
- *Kafka module*
- *Logstash module*
- *MongoDB module*
- *MySQL module*
- *Nginx module*
- *Osquery module*
- *PostgreSQL module*
- *Redis module*
- *System module*
- *Traefik module*

Metrics

- Metrics data sources
  - Popular solutions
    - Metricbeat

Kubernetes Monitoring

- What to monitor
  - Cluster monitoring
  - Pod monitoring
  - Application monitoring
- Metrics sources
  - cAdvisor & Heapster
  - Kube-state-metrics
  - Prometheus
  - APM
- Solutions
  - Heapster/InfluxDB/Grafana
  - Heapster/Elasticsearch
  - Prometheus/Grafana
  - APM - Datadog, Dynatrace
  - Metricbeat with Autodiscovery

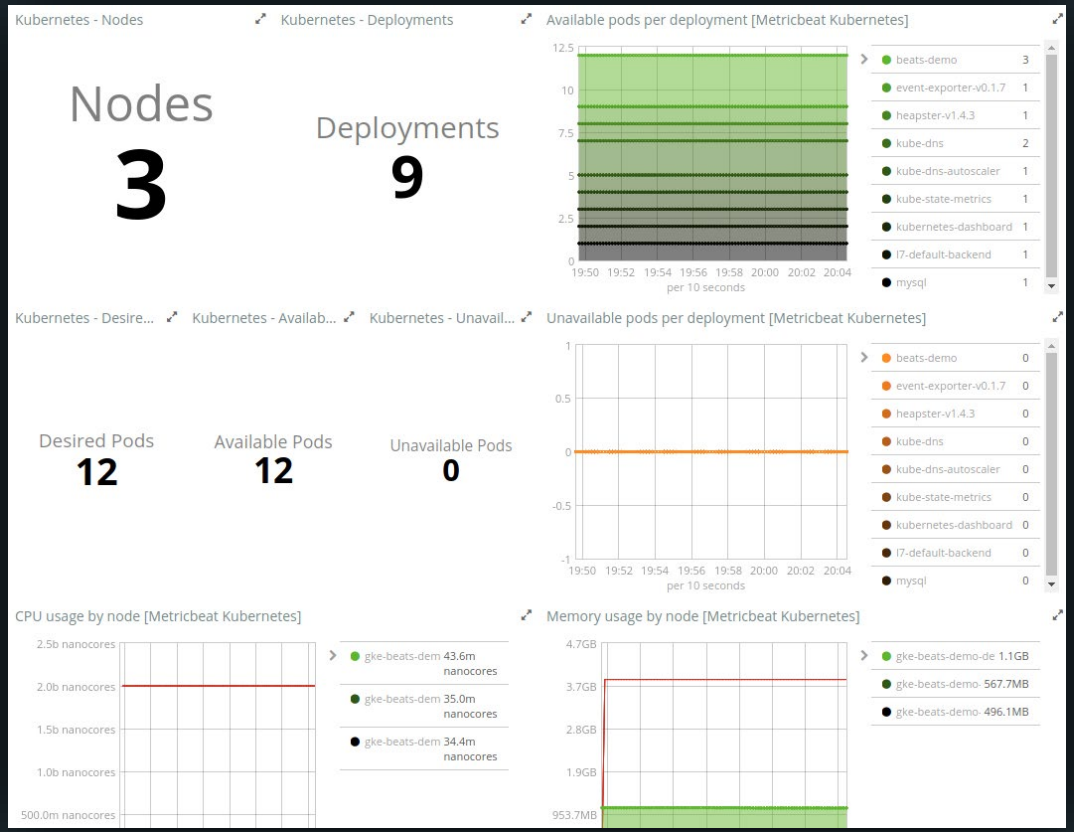


Comprehensive Metrics Collection Metricbeat

- Kubernetes module
- Monitors pods and services
  - Cluster, pod & container metrics
  - Application metrics through auto-discovery (eg. Nginx)
- Metrics sources - Cover them **ALL**
  - Kubelet (heapster, cAdvisor)
  - kube-state-metric
  - Kubernetes events
  - Prometheus module (*beta*)
- Curated Infra UI
  - Dedicated Kibana app

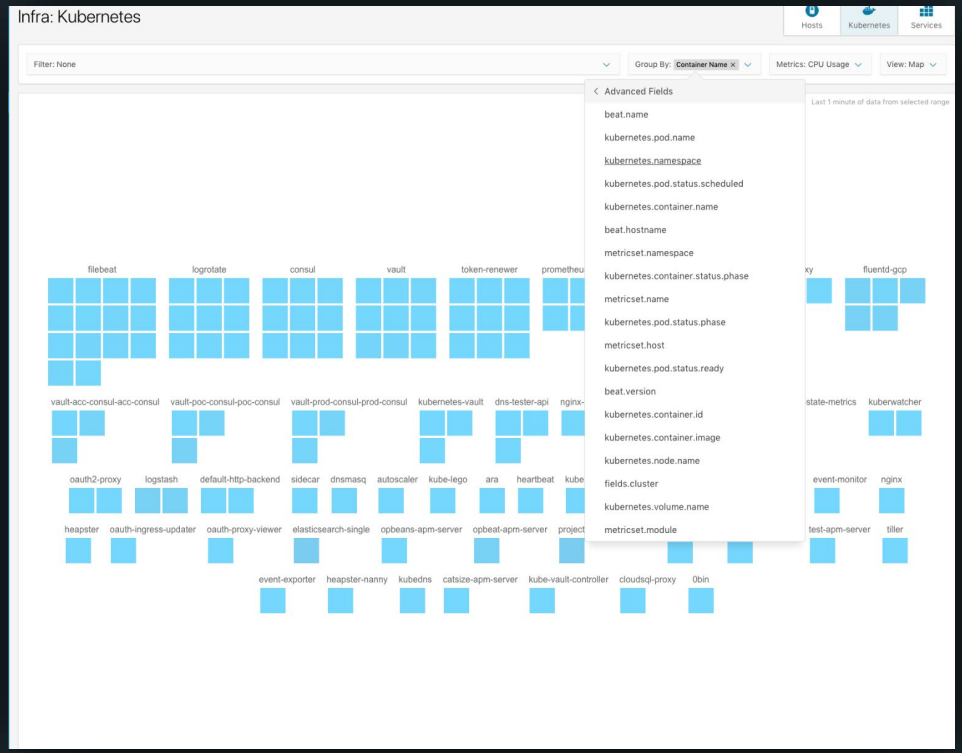
```
metricbeat.modules:
# Node metrics, from kubelet:
- module: kubernetes
  metricsets:
    - node
    - system
    - pod
    - container
    - volume
  period: 10s
  hosts: ["localhost:10255"]

# State metrics from kube-state-metrics service:
- module: kubernetes
  enabled: false
  metricsets:
    - state_node
    - state_deployment
    - state_replicaset
    - state_pod
    - state_container
  period: 10s
  hosts: ["kube-state-metrics:8080"]

# Kubernetes events
- module: kubernetes
  enabled: false
  metricsets:
    - event
```

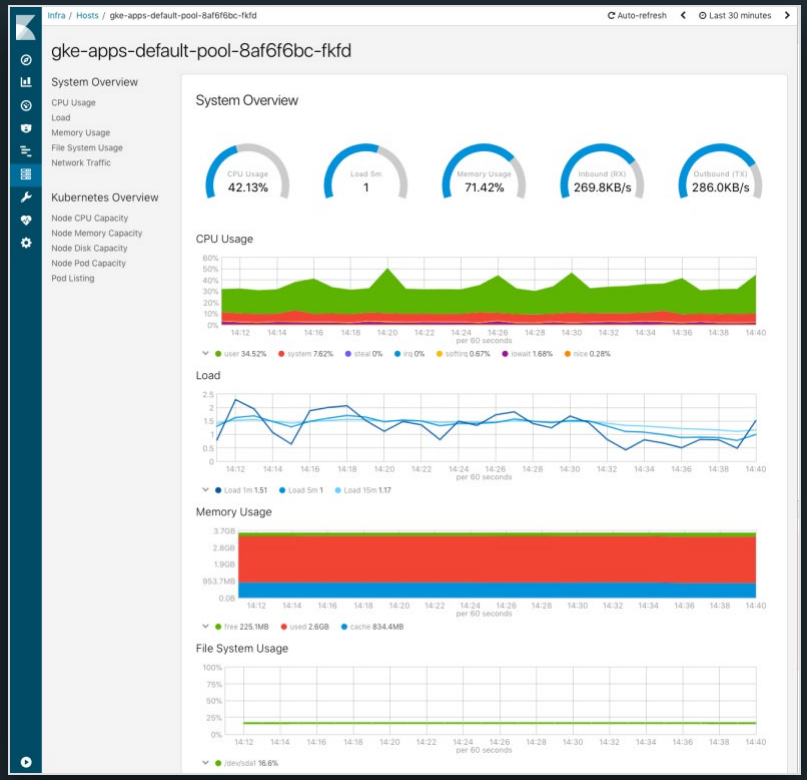
Out -of -the -box Dashboards



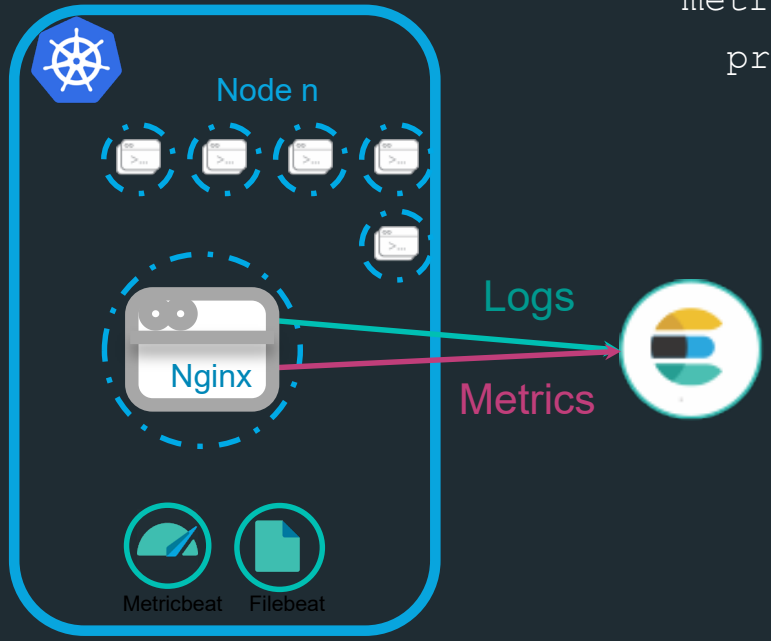
Curated UI for Kubernetes

Visualize the cluster and group by nodes or namespaces or pods





Monitor Services inside Containers with Auto-Discovery




```
metricbeat.autodiscover:
  providers:
    - type: kubernetes
      host: ${HOSTNAME}
      templates:
        - condition.contains:
            kubernetes.container.name: nginx
          config:
            - module: nginx
              period: 10s
              metricsets: ["stubstatus"]
              hosts: ["${data.host}:8080"]
```

Metricbeat Modules

Simplify collection and visualization of common metrics

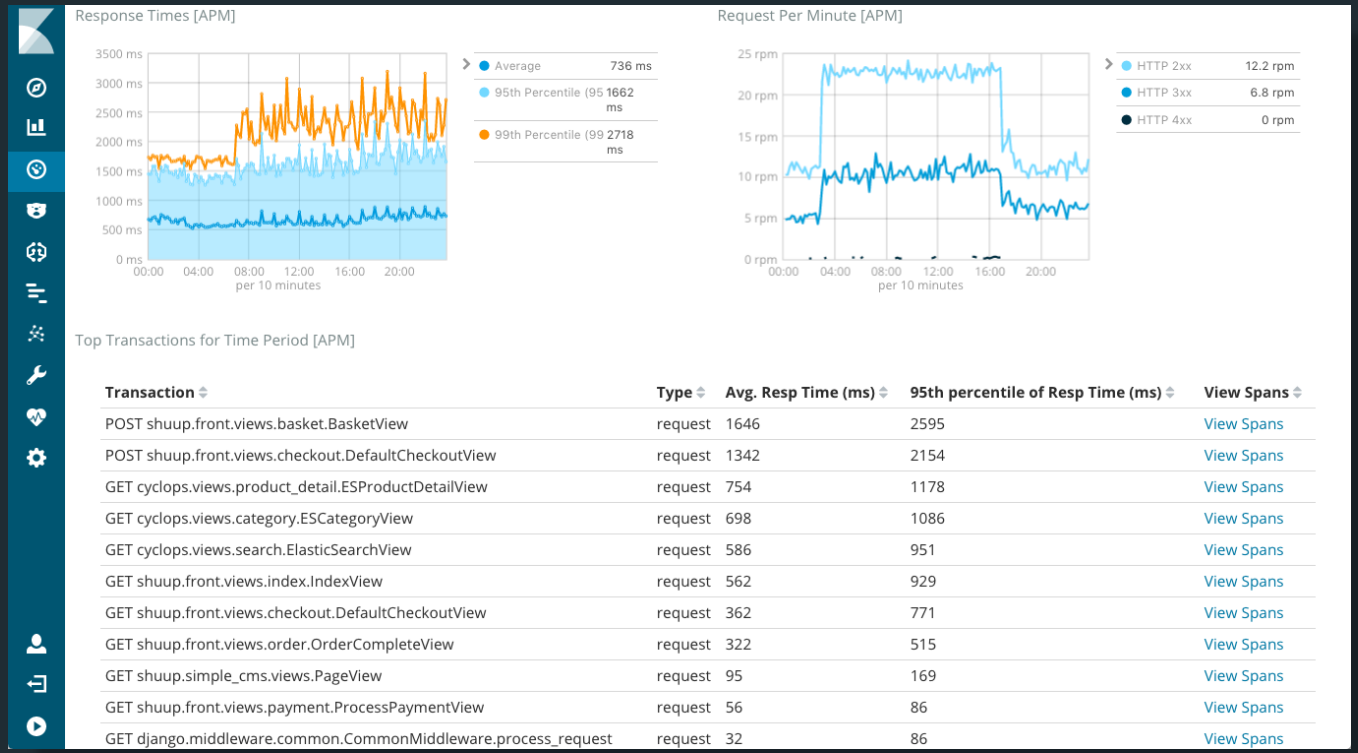
- Aerospike module
- Apache module
- Ceph module
- Couchbase module
- Docker module
- Dropwizard module
- Elasticsearch module
- Etcd module
- Golang module
- Graphite module
- HAProxy module
- HTTP module
- Jolokia module
- Kafka module
- Kibana module
- Kubernetes module
- kvm module
- Logstash module
- Memcached module
- MongoDB module
- Munin module
- MySQL module
- Nginx module
- PHP_FPM module
- PostgreSQL module
- Prometheus module
- RabbitMQ module
- Redis module
- System module
- uwsgi module
- vSphere module
- Windows module
- ZooKeeper module

Tracing

- Elastic APM

First Major Open Source APM Solution

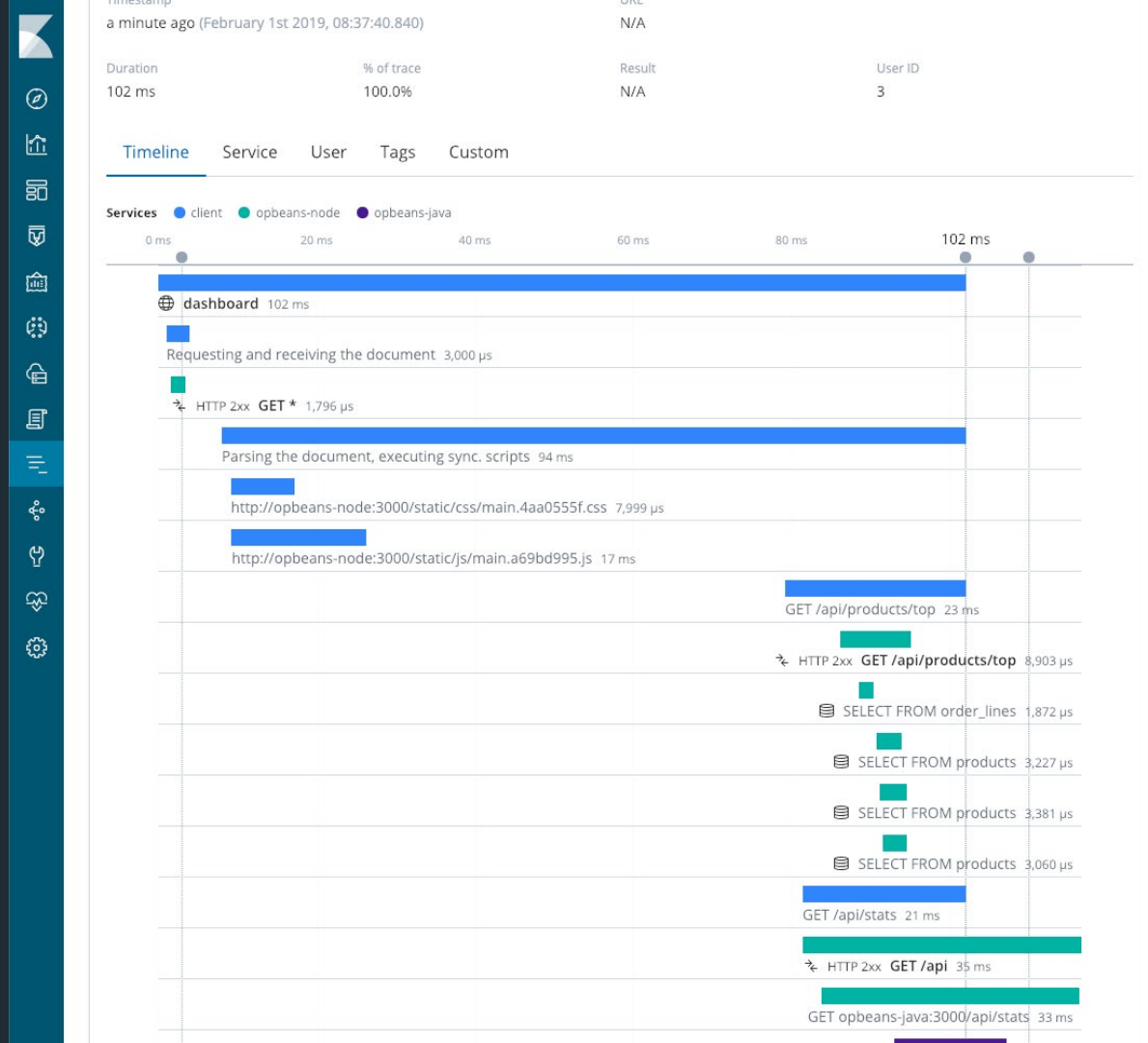
Agents, Server, Dashboards



Transaction	Type	Avg. Resp Time (ms)	95th percentile of Resp Time (ms)	View Spans
POST shuup.front.views.basket.BasketView	request	1646	2595	View Spans
POST shuup.front.views.checkout.DefaultCheckoutView	request	1342	2154	View Spans
GET cyclops.views.product_detail.ESProductDetailView	request	754	1178	View Spans
GET cyclops.views.category.ESCategoryView	request	698	1086	View Spans
GET cyclops.views.search.ElasticSearchView	request	586	951	View Spans
GET shuup.front.views.index.IndexView	request	562	929	View Spans
GET shuup.front.views.checkout.DefaultCheckoutView	request	362	771	View Spans
GET shuup.front.views.order.OrderCompleteView	request	322	515	View Spans
GET shuup.simple_cms.views.PageView	request	95	169	View Spans
GET shuup.front.views.payment.ProcessPaymentView	request	56	86	View Spans
GET django.middleware.common.CommonMiddleware.process_request	request	32	86	View Spans

APM Tracing - Transaction

- Distributed tracing
- Trace the entire transaction, across all instrumented services
- Includes calls to external services and databases



You can do MORE ...

- Enforce access policies with **Security**
- Be notified about changes & problems with **Alerting**
- Be smarter with **Machine Learning**
- ...

THANK YOU

Web : www.elastic.co
Products : https://www.elastic.co/products
Forums : https://discuss.elastic.co/
Community : https://www.elastic.co/community/meetups
Twitter : @elastic