



Elastic Stack Monitor your Services

Aravind Putrevu

Developer | Evangelist

@aravindputrevu | aravindputrevu.in



Agenda

- 1 Why Monitoring?
- 2 Why Elastic Stack?
- 3 Beats : Lightweight data shipper framework
- 4 Monitor All things with Beats
- 5 Demo

Agenda

1 Why Monitoring?

2 Why Elastic Stack?

3 Beats : Lightweight data shipper framework

4 Monitor All things with Beats

5 Demo

Agenda

- 1 Why Monitoring?
- 2 Why Elastic Stack?
- 3 Beats : Lightweight data shipper framework
- 4 Monitor All things with Beats
- 5 Demo

Agenda

- 1 Why Monitoring?
- 2 Why Elastic Stack?
- 3 Beats : Lightweight data shipper framework
- 4 Monitor All things with Beats
- 5 Demo

Agenda

1 Why Monitoring?

2 Why Elastic Stack?

3 Beats : Lightweight data shipper framework

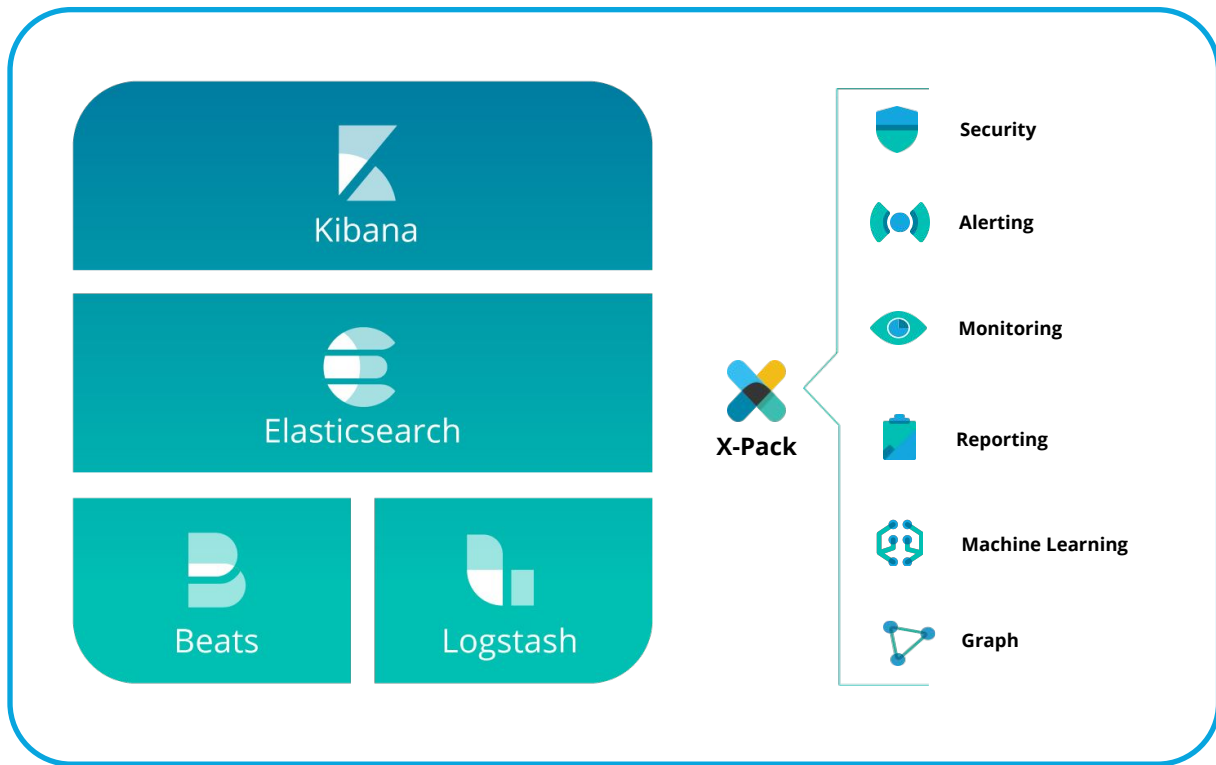
4 Monitor All things with Beats

5 Demo



Elastic Stack

No enterprise edition
All new versions with 6.3



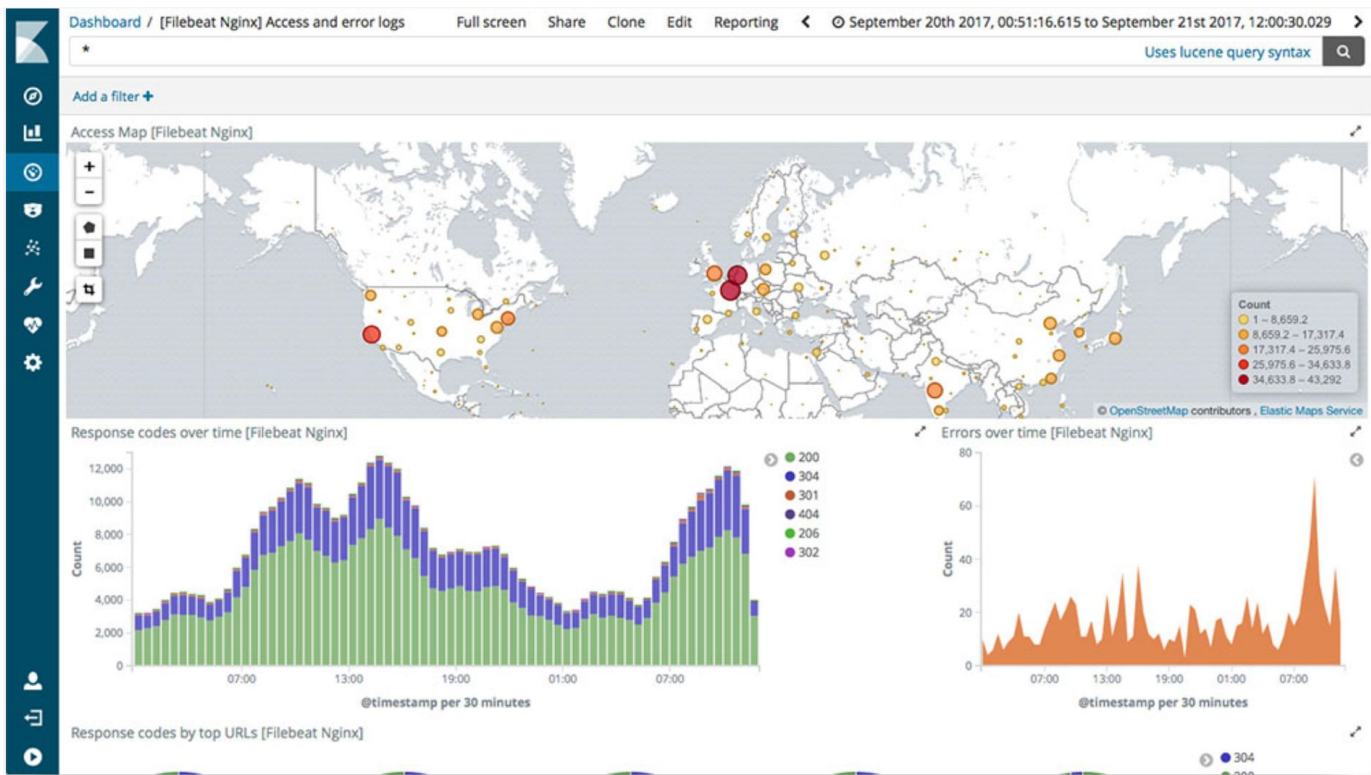
Why Monitoring?

Pet vs Cattle



Why Monitoring?

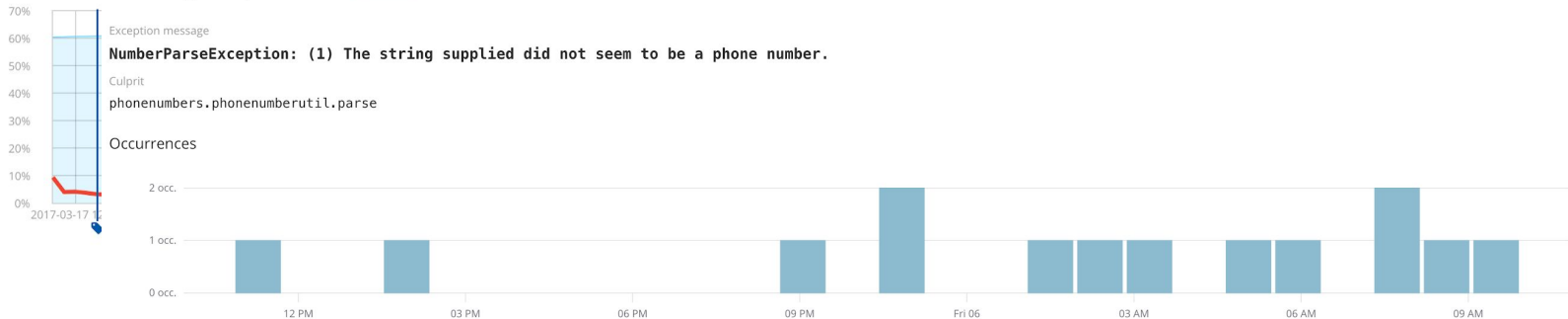
Find out what's happening?



Why Monitoring?

Resolving Errors and bottlenecks

Operational Anal Error group f96f1 Unhandled



CPU Usage 33.15%
System Memory Util 50.16%

Error occurrence

[View 14 occurrences in Discover](#)

Timestamp	an hour ago (July 6th 2018, 09:46:26.475)	URL	http://cyclops:8000/checkout/addresses/
Request method	POST	Handled	false
		User ID	113

[Exception stacktrace](#) [Request](#) [System](#) [Service](#) [Process](#) [User](#) [Tags](#) [Custom](#)

12 library frames

cyclops/shuup/forms/forms.py in clean at line 43

```
41.         raise forms.ValidationError(_('Telephone number must be specified'))
42.     if cleaned_data.get("country"):
43.         phone = phonenumbers.parse(cleaned_data.get("phone"), cleaned_data.get("country"))
44.         if phonenumbers.is_possible_number(phone):
45.             cleaned_data["phone"] = phonenumbers.format_number(phone, phonenumbers.PhoneNumberFormat.INTERNATIONAL)
```

Local variables

Why Elastic?

SECURITY
ANALYTICS

LOG
ANALYTICS

METRICS
ANALYTICS

BUSINESS
ANALYTICS

SEARCH

APM



Protect your
data



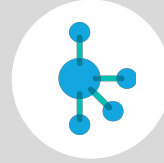
Be alerted on
changes



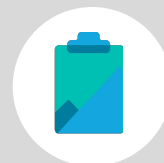
Detect anomalies



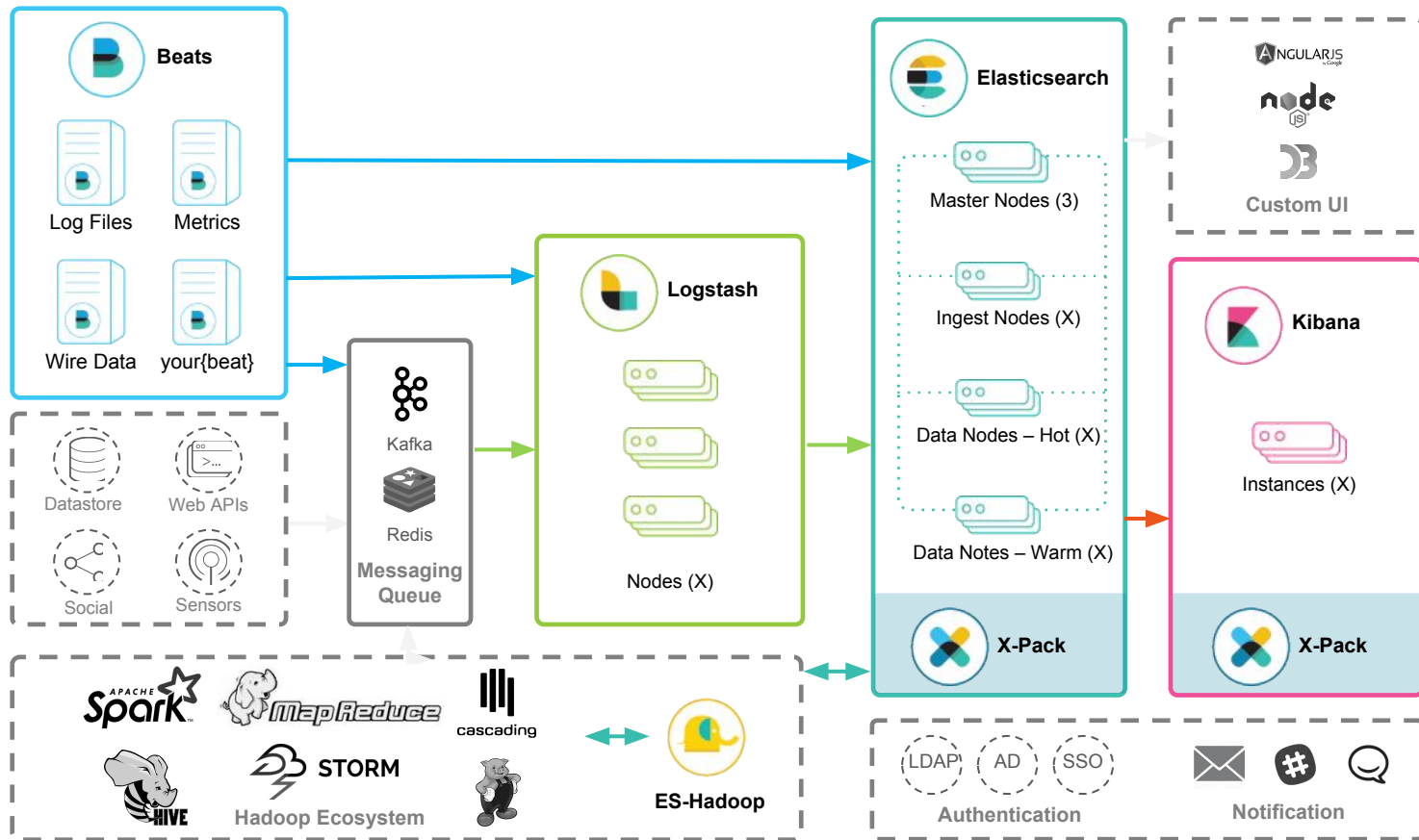
Monitor your
Elastic Stack

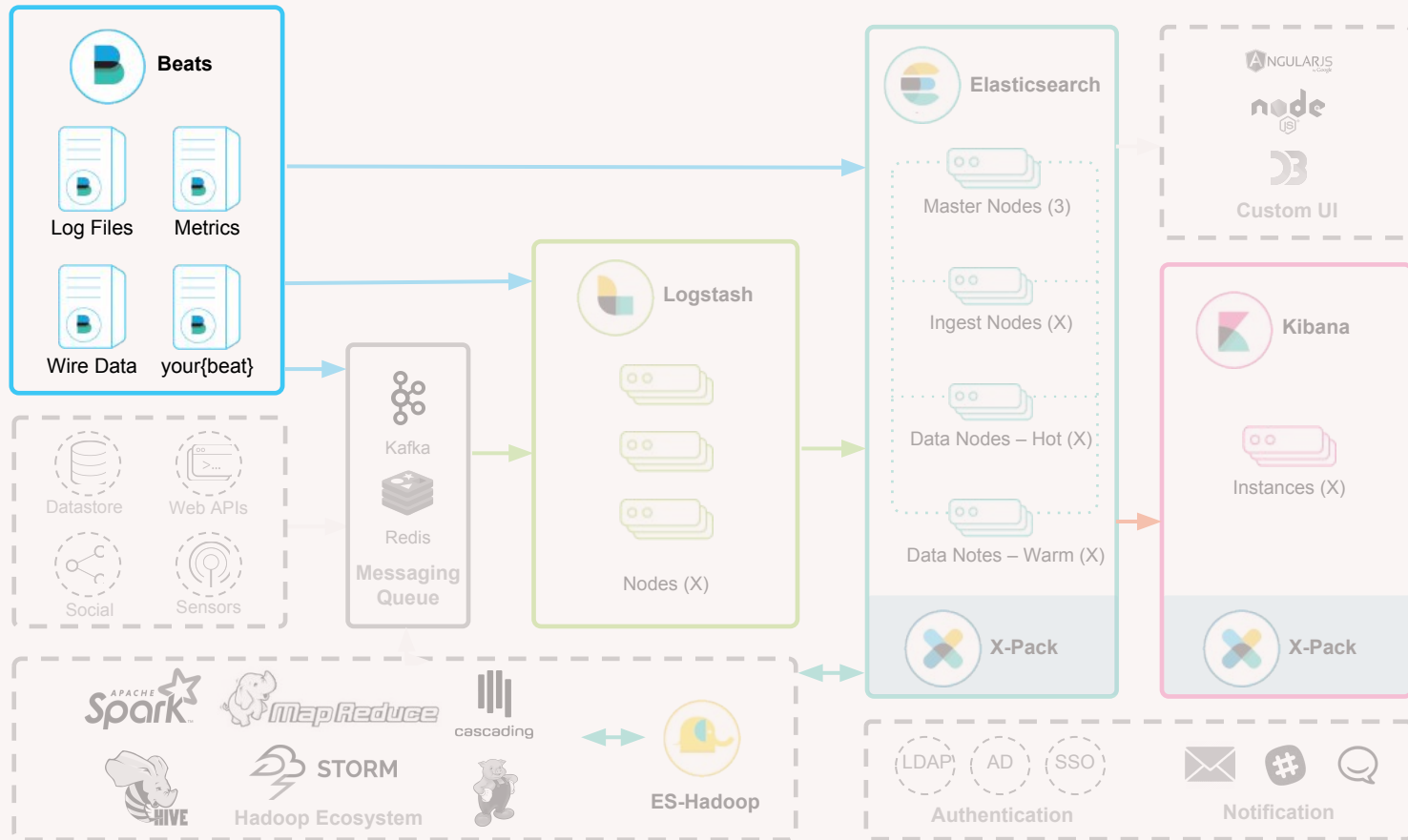


Find links in
your data



Share your
insights

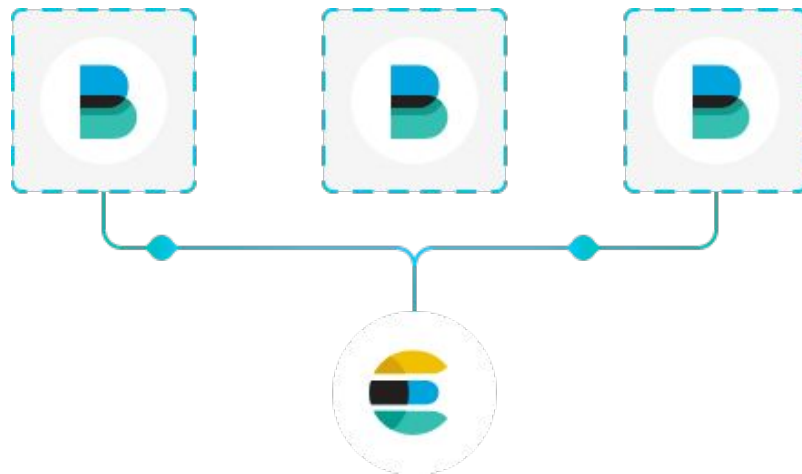






Beats

Lightweight data shippers



Ship data from the source	Ship and centralize in Elasticsearch	Ship to Logstash for transformation and parsing
Ship to Elastic Cloud	Libbeat: API framework to build custom beats	30+ community Beats

The Beats family



Packetbeat

Network data



Metricbeat

Metrics



Winlogbeat

Windows Event Logs



Auditbeat

Audit data



Filebeat

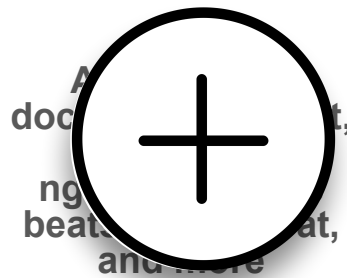
Log files



Heartbeat

Uptime monitoring

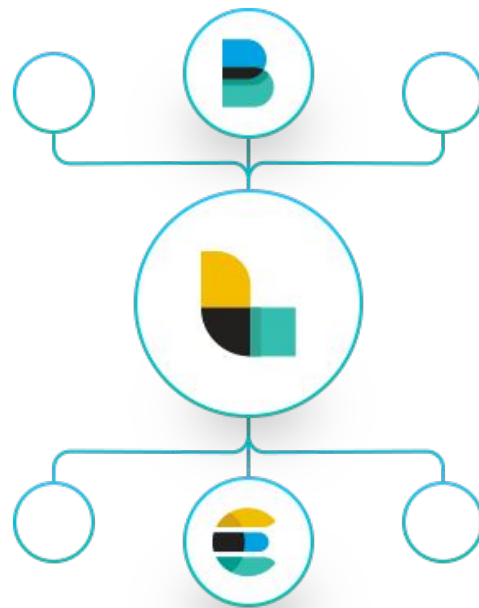
+40
community
Beats



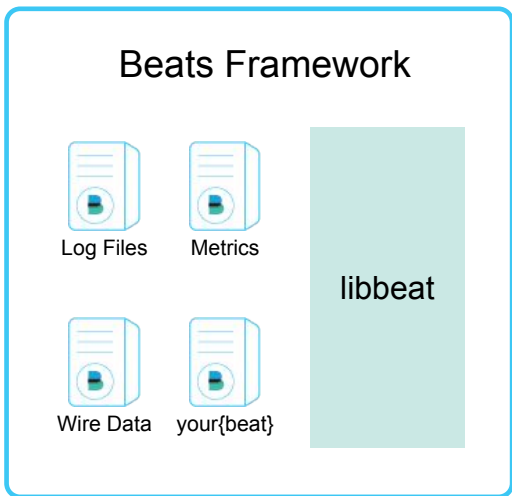
{your}beat

Logstash vs Beats

- Beats are lightweight data shippers that you install as agents on your servers
- Logstash has a larger footprint, but provides a broad array of input, filter, and output plugins for collecting, enriching, and transforming data from a variety of sources.

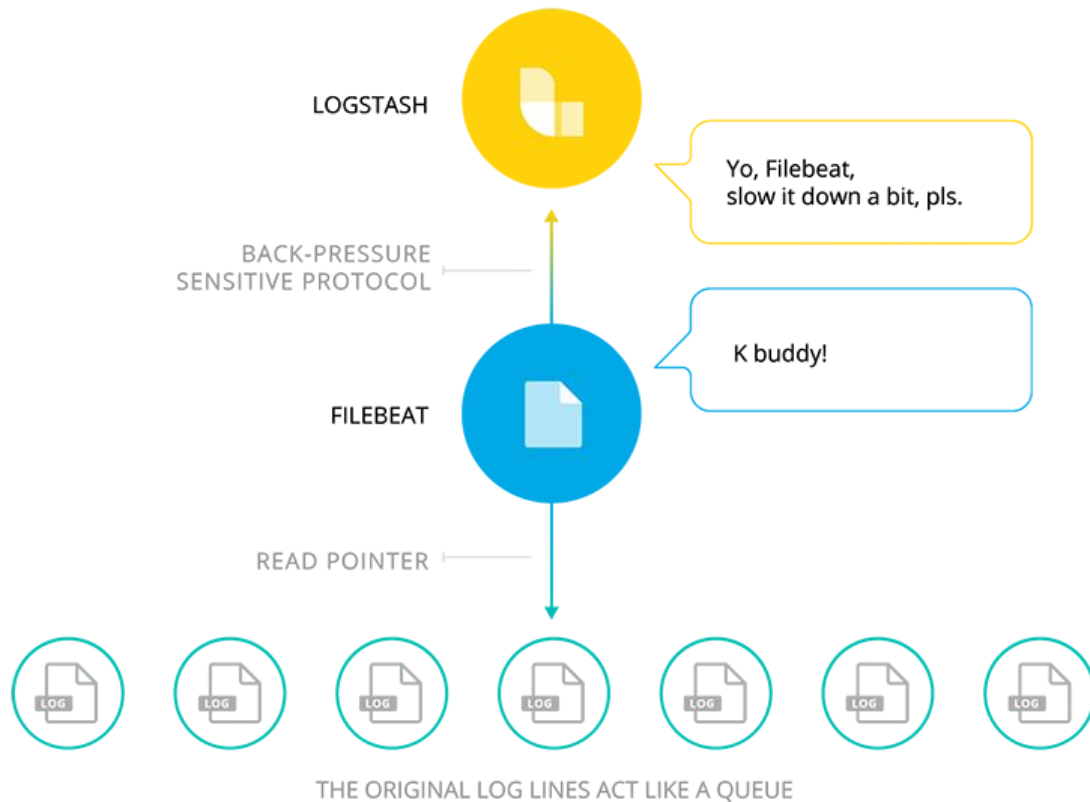


How beats work?



- Small application
- Install as agent on your servers
- Written in Golang
- No runtime dependencies
- Single purpose

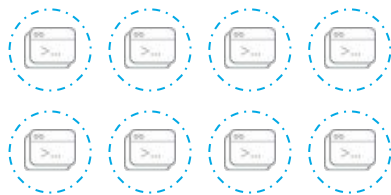
How beats work?



Classic Deployments



VM 1



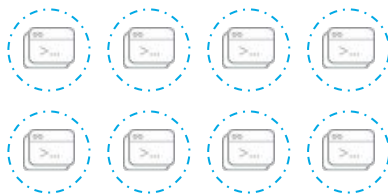
Filebeat



Metricbeat



VM 2



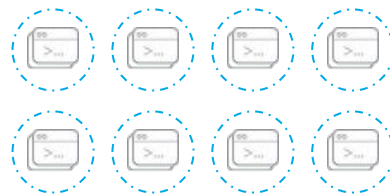
Filebeat



Metricbeat



VM n

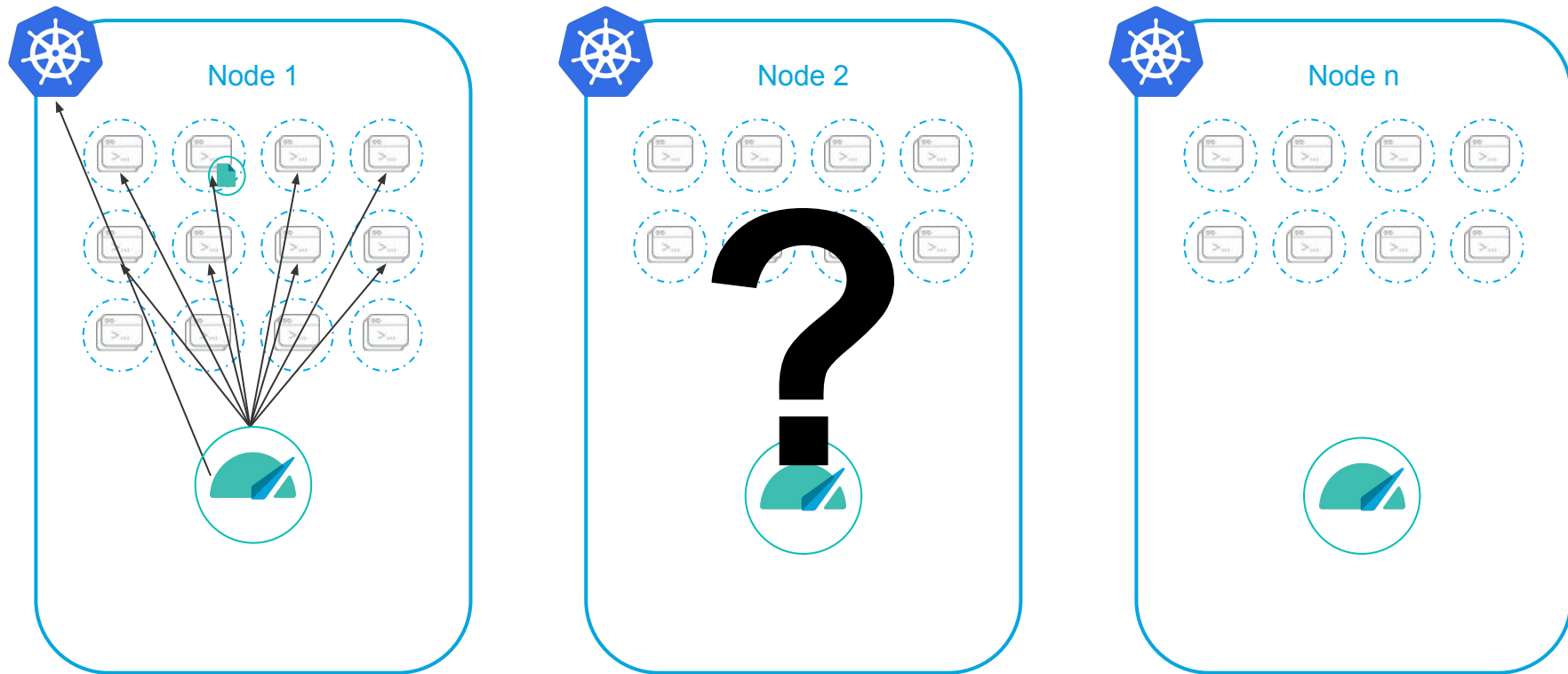


Filebeat

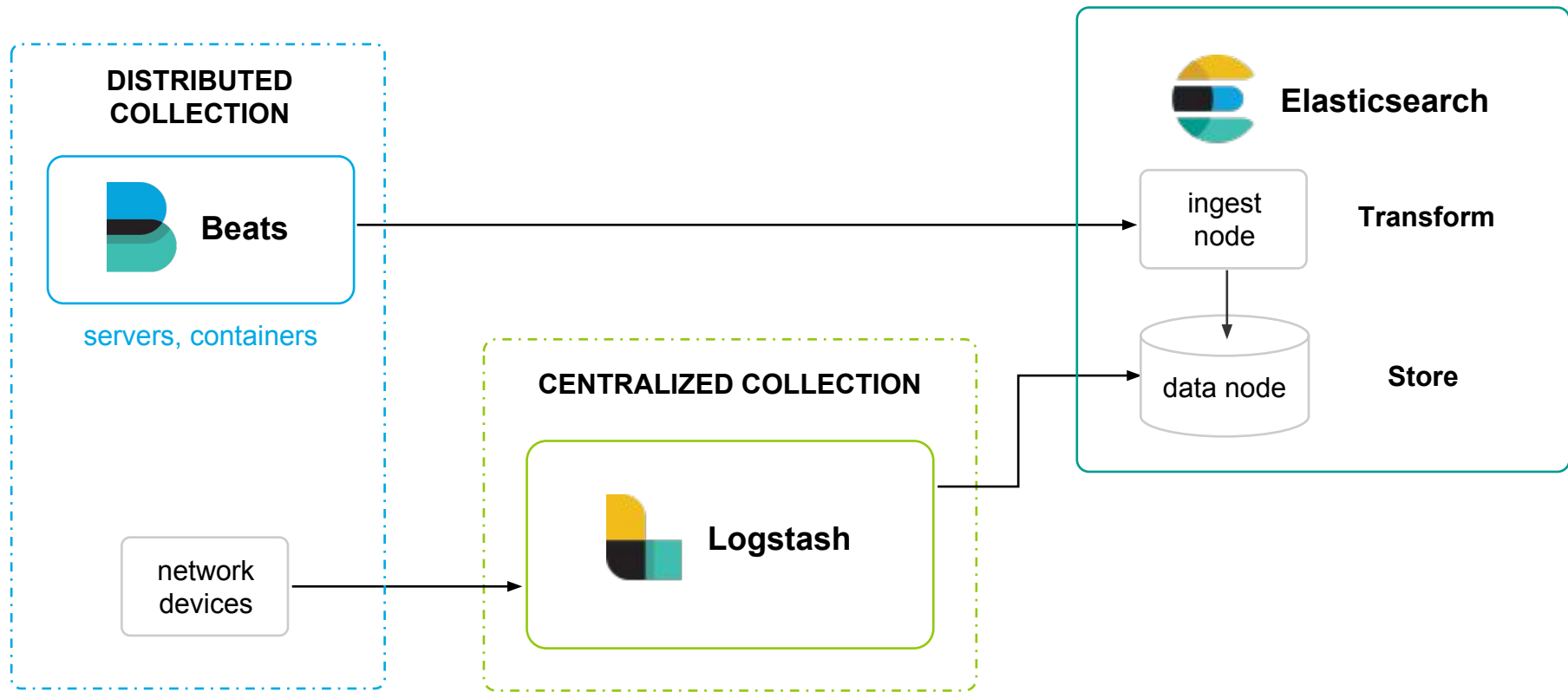


Metricbeat

Kubernetes deployment



Elastic evolving ingest story



Immediate insights with modules

- Turnkey experience for specific data types
- Data to dashboard in just one step
- Automated parsing and enrichment
- Default dashboards, alerts, ML jobs

Available with



Logging

Metrics

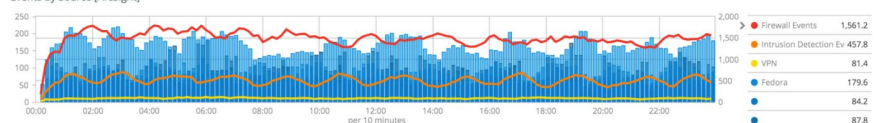
Security

Device Metrics Overview [ArcSight]

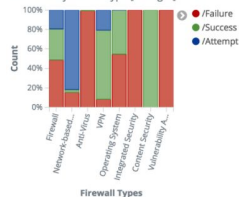
Event Count **330,453** Devices **57** Sources **254** Destinations **425** Ports **88**



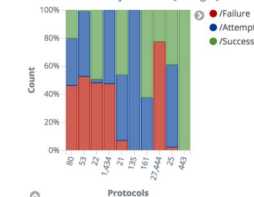
Events by Source [ArcSight]



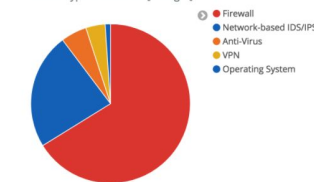
Outcome by Device Type [ArcSight]



Destination Ports by Outcome [ArcSight]



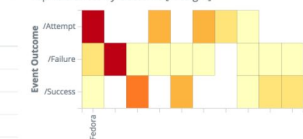
Device Type Breakdown [ArcSight]



Top 10 Devices by Bandwidth [ArcSight]

Device	Source(s)	Destination(s)	Destination Ports	Bandwidth (Incoming)	Bandwidth (Outgoing)
Fedora	54	50	17	48,543,771	775,106,603
	1	96	1	1,827,840	1,763,328
	3	5	3	275,800	264,950
	1	0	1	775	456
	1	1	1	128	128

Top 10 Devices by Outcome [ArcSight]



Logging modules

AUDITBEAT

FILEBEAT

WINLOGBEAT



Infrastructure

System

- Linux / MacOS
- Windows Events

Containers

- Docker
- Kubernetes

Applications

Databases

- MySQL
- PostgreSQL

Queues

- Kafka
- Redis

Web servers

- Apache
- Nginx

Audit data

- Filesystem
- System calls

Metrics modules

METRICBEAT PACKETBEAT LOGSTASH



Infrastructure

System

- Linux
- MacOS
- Windows
- Perfmon

Containers

- Docker
- Kubernetes

Virtualization

- vSphere

Cloud

- AWS
- Azure
- DigitalOcean
- GCP

Network

- Netflow
- Packets
- TLS Envelope

Storage

- Ceph

Metrics modules

HEARTBEAT



METRICBEAT



PACKETBEAT



LOGSTASH



Applications

Datastores

- MySQL
- PostgreSQL
- MongoDB
- Couchbase
- Aerospike
- Graphite

Queues

- Kafka
- Redis
- RabbitMQ

Caches

- Memcached

Uptime

- Heartbeat

Custom apps

- JMX/Jolokia
- PHP-FPM
- Golang

Web servers

- Apache
- Nginx

Other

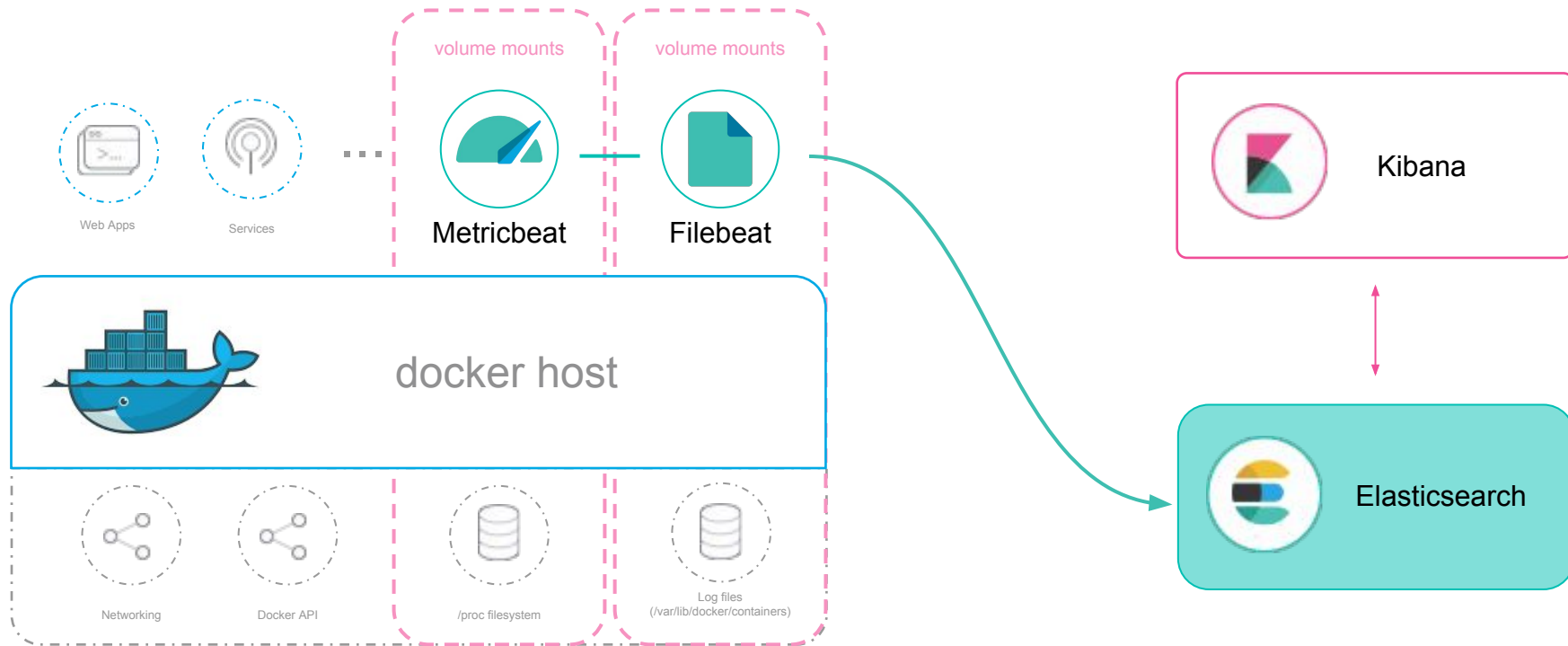
- HAProxy
- Zookeeper

With containers architecture, everything is a moving target

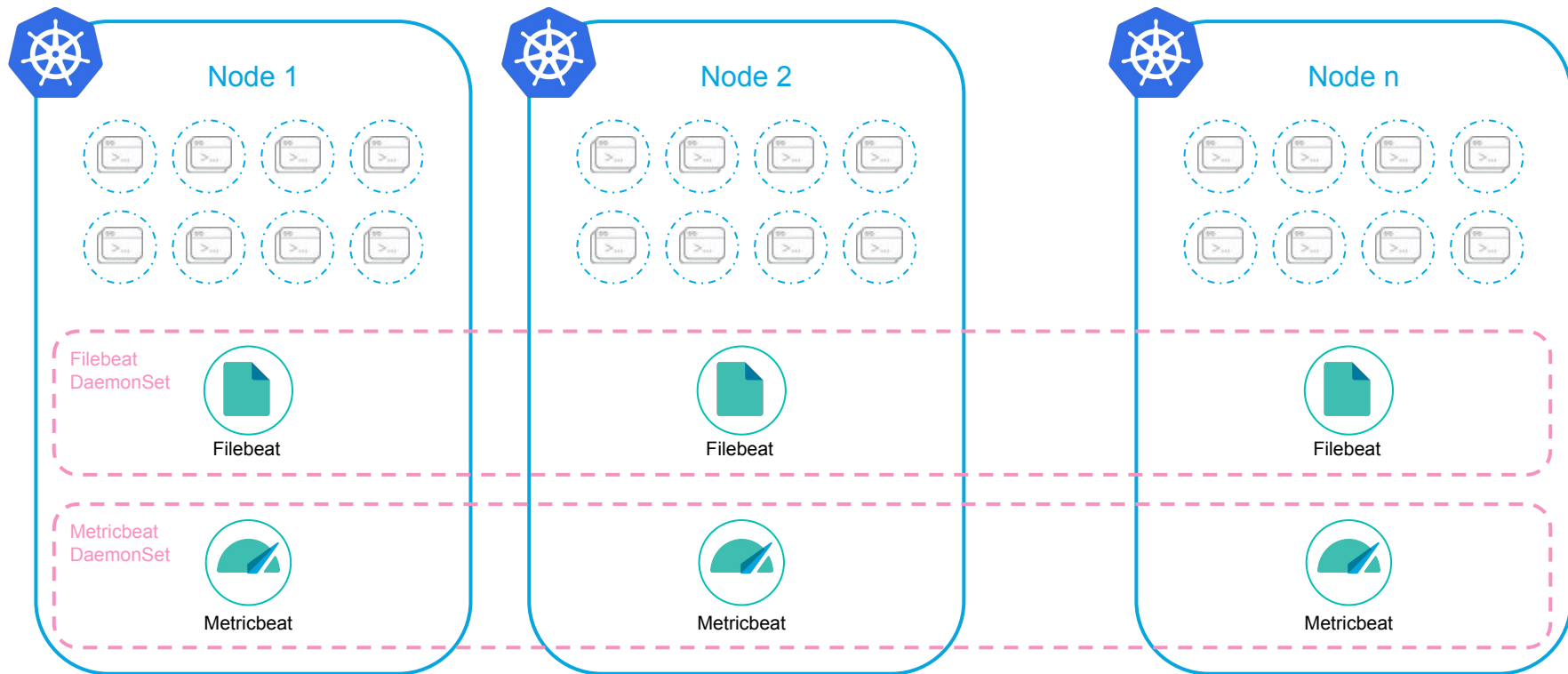
We need specific tools to track things down



Docker deployment



Kubernetes deployment



Docker logs input

Retrieve logs from Docker containers

```
filebeat.prospectors:  
- type: docker  
  containers.ids:  
    - '*'
```

Parse and ship `/var/lib/docker/containers/*/*.log`:

```
{"log":"INFO elasticsearch/client.go:145 Elasticsearch  
url:http://elasticsearch:9200\r\n","stream":"stdout","t  
ime":"2018-02-11T23:29:19.236692181Z"}
```

Metadata processors

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

add_cloud_metadata

- cloud.region
- cloud.instance_id
- cloud.machine_type
- 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

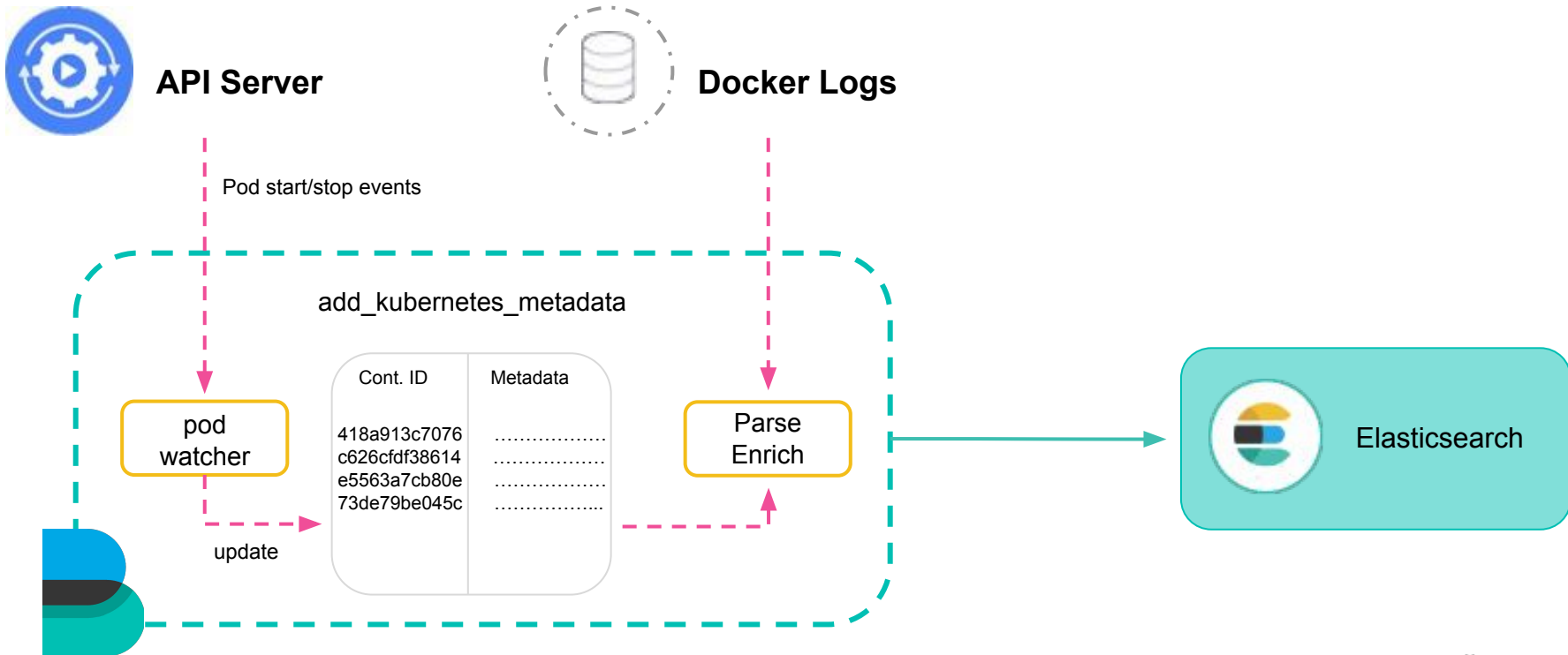
Metadata processors

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": "1234567",
      "provider": "digitalocean",
      "region": "blr1"
    }
  }
}
```

Metadata processors

`add_kubernetes_metadata` internals



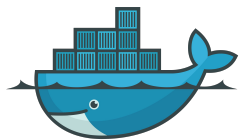
Autodiscover

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

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

config template

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

3. var expansion

4. launch module

```
- module: etcd
  hosts: "10.4.15.9:237" metricsets:
["leader", "self", "store"]
9"
```

DEMO

What Next?

How Elastic Stack can help you?



APM

Real User Monitoring (RUM)



APM

Application-level monitoring



Beats

Server-level monitoring



Beats



Logstash

Logging

- 100% Open Source
- Readymade UI in Kibana
- Language Agents



Flask

django



Resources

- <https://www.elastic.co/learn>
- <https://www.elastic.co/blog/category/engineering>
- <https://discuss.elastic.co/>
- <https://fb.com/groups/ElasticIndiaUserGroup>
- <https://elastic.co/community>

Fin!



discuss.elastic.co | aravind@elastic.co | [@aravindputrevu](https://twitter.com/aravindputrevu)