



Elastic Solutions

Tatjana Frank
Solutions Architect, CEMEA



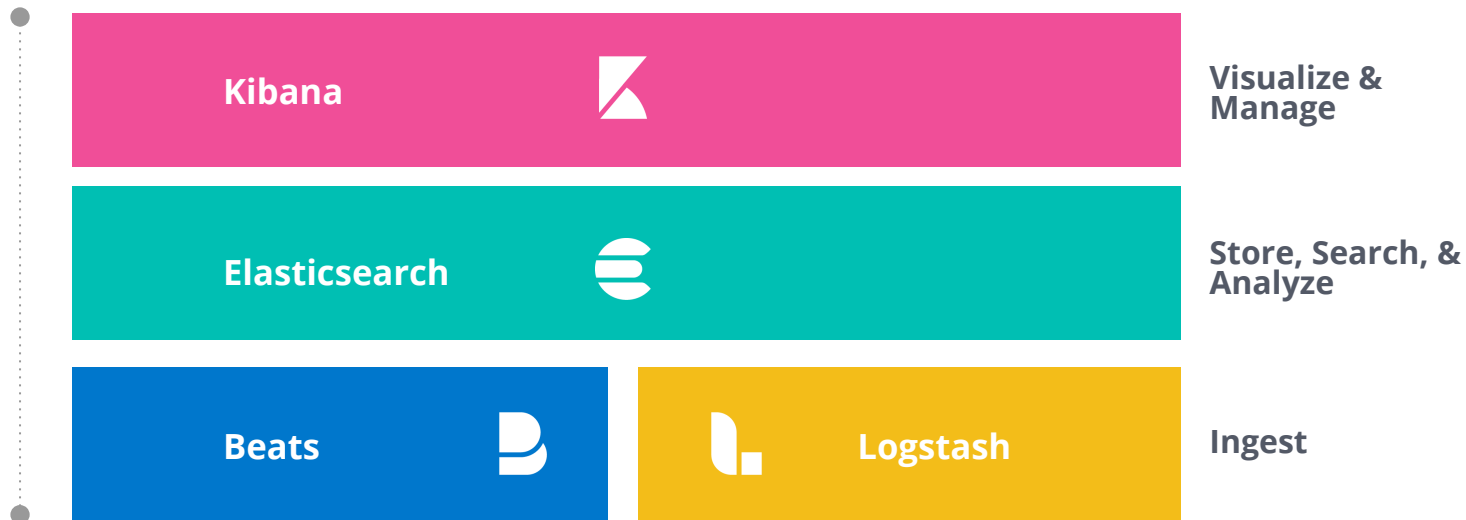
Become our local **Community Organizer!**

We are looking for someone to help our local Elastic user group thrive.

Email us at meetups@elastic.co, if you're interested.

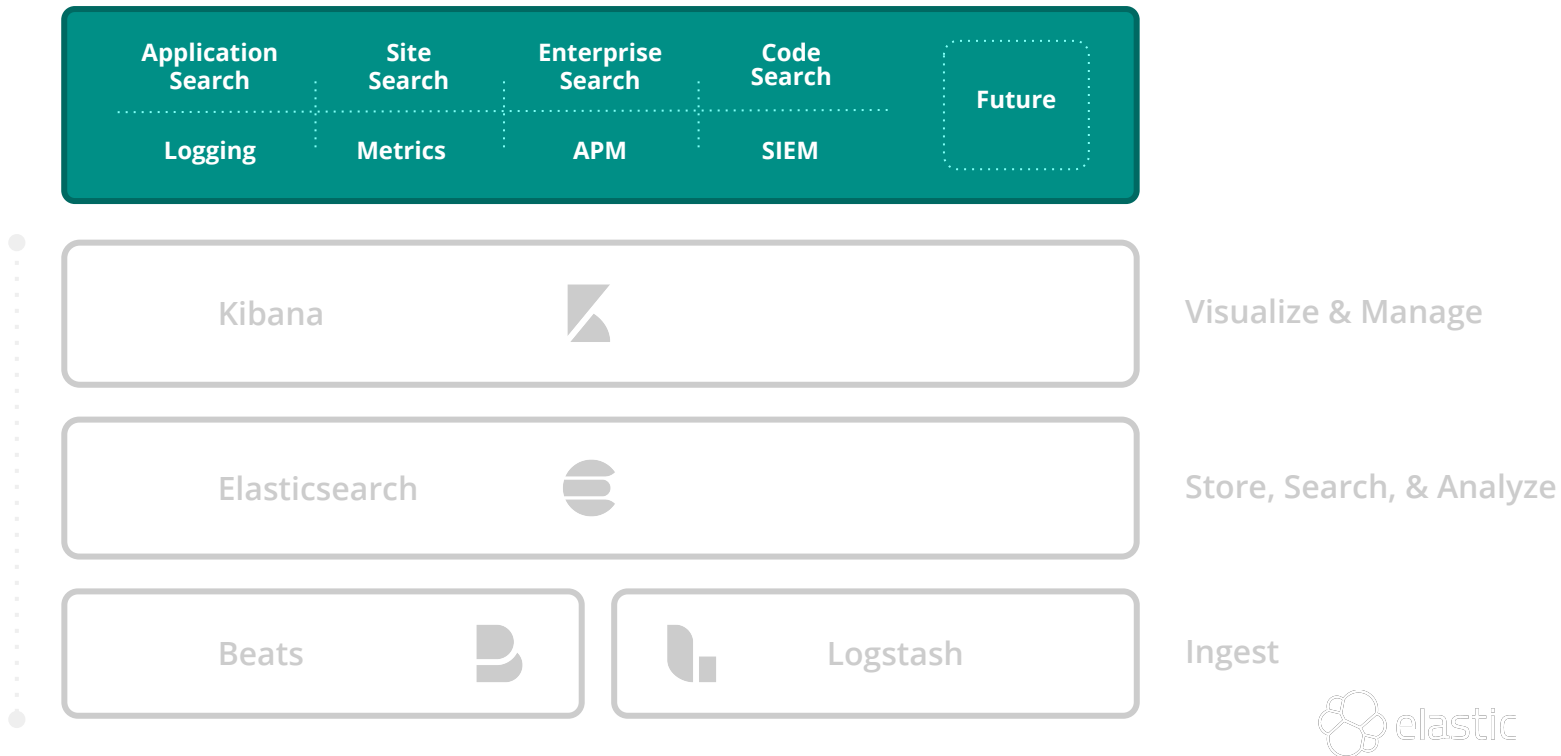
Learn more:
<https://ela.st/organize>

Elastic **Stack**



Solutions are built on top of Elastic Stack


Elastic Stack



However You Want to Run Elastic

The best software & support

Fully orchestrated

Elastic hosted

Self-managed

Download distributions
and install it on your
preferred infrastructure

Deploy anywhere.

Elastic Cloud Enterprise & Elastic Cloud on Kubernetes

Orchestration tailormade
for Elastic Stack. Centrally
manage multiple stacks.

Deploy anywhere.

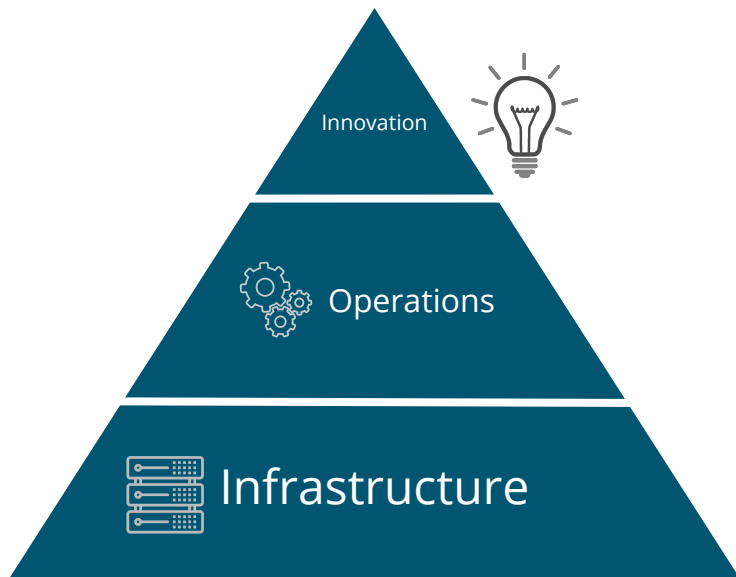
Elasticsearch Service

The official fully managed
Elasticsearch & Kibana
solution.

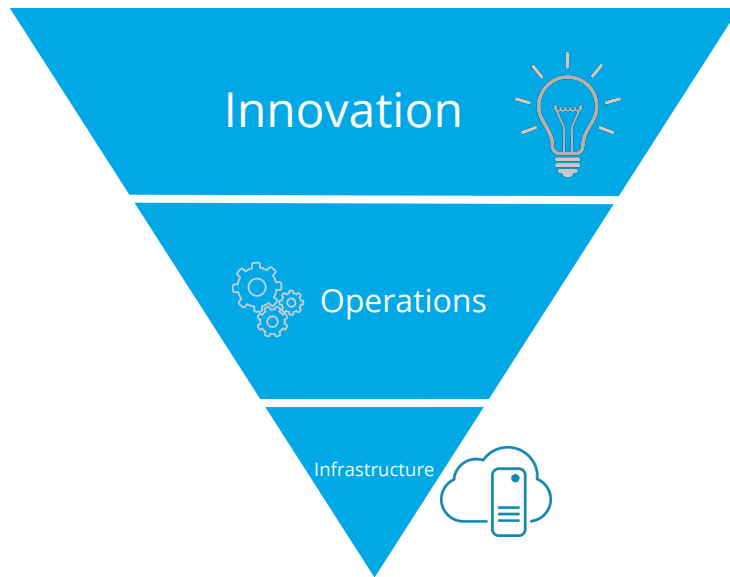
Available on AWS, GCP,
and Azure.

Improve Your Time to Innovation with Elastic Cloud

Where do you want to spend your time?



Traditional IT



Elastic Cloud & Solutions

Solutions are a vertical slice through the Elastic Stack

Simple to get started

Turn-key features

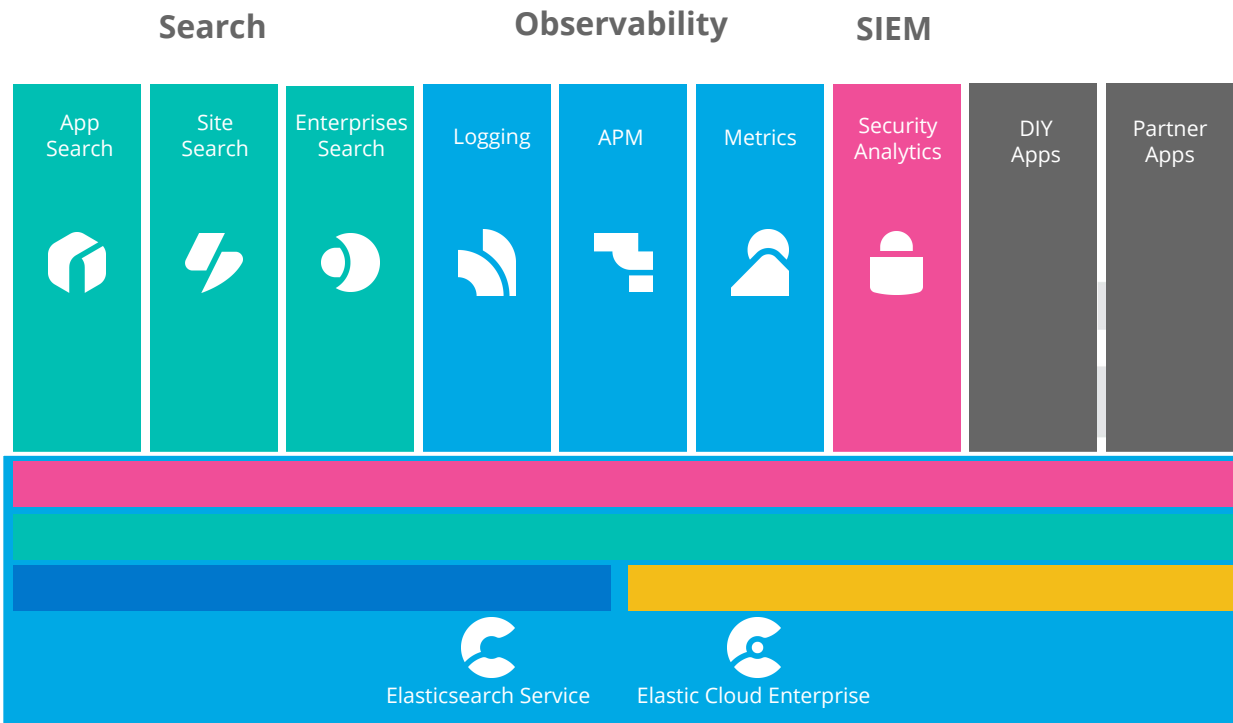
Lots of functionality out-of-the-box

“Off the shelf”

Adding value by abstracting away work

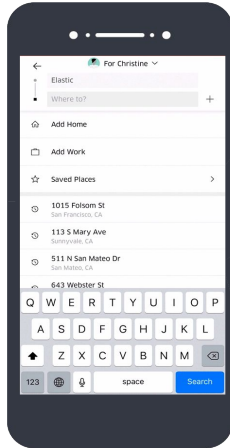


Elastic Helps Get You There Faster



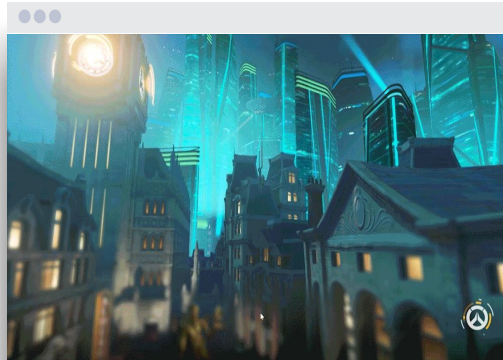
Search

Uber



Observe

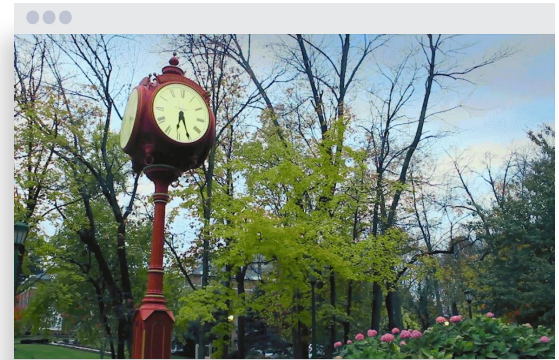
ACTIVISION
BLIZZARD



Protect



INDIANA UNIVERSITY





Logs



**Infrastructure
Metrics**

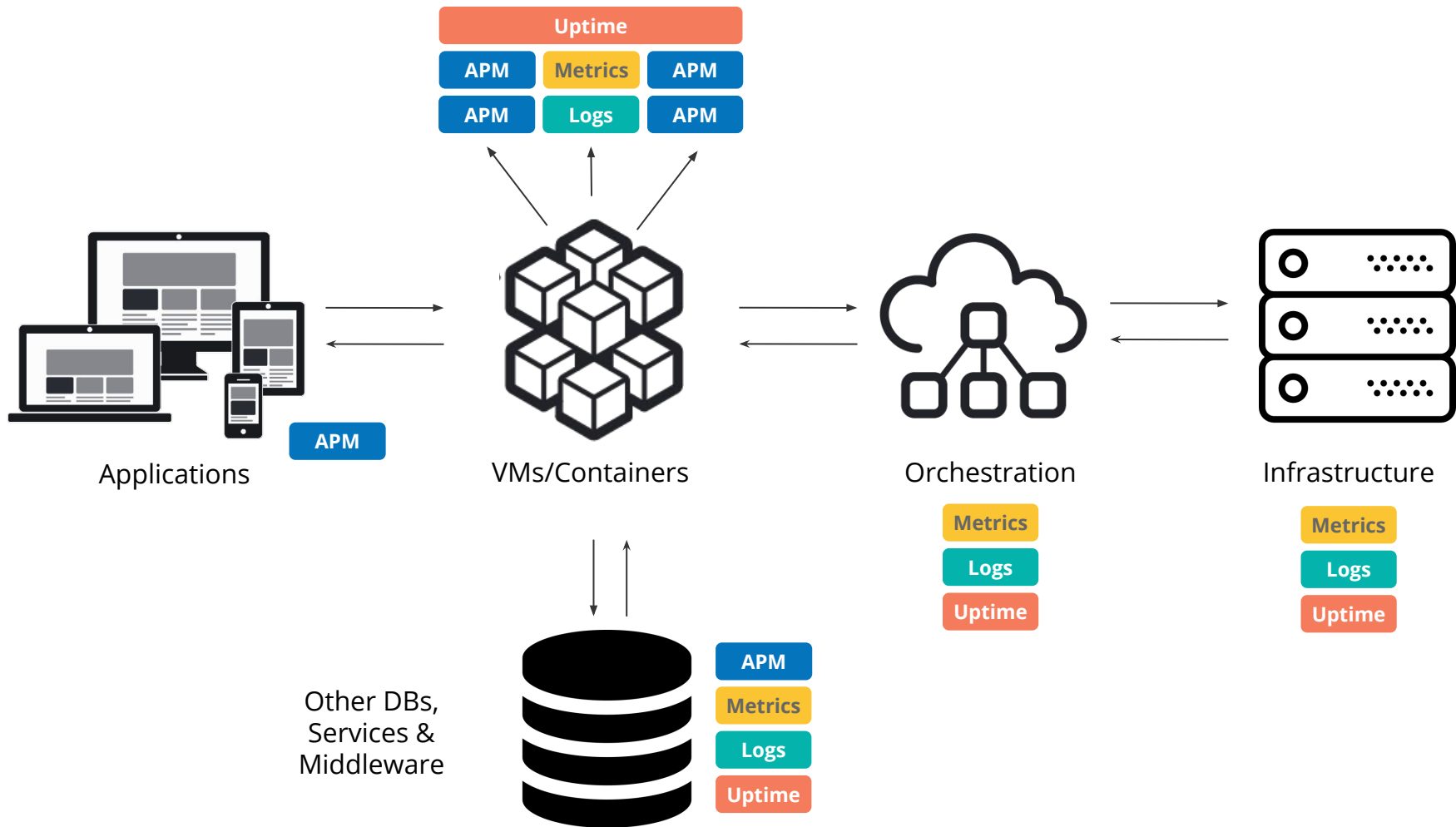


APM



Uptime

Observability



Operational Monitoring

Unify Logs + Metrics + APM

Ingest

Rich ecosystem of connectors

Extensible ingest pipelines

Developer friendly APIs

Exploration

Turnkey solution UIs

OOTB dashboards

Live presentations

Analytics

Anomaly detection

Trending & forecasting

Flexible alerting tools

The screenshot displays the 'Add Data to Kibana' interface. At the top, there's a navigation bar with 'Home', 'Logging', 'Metrics', 'Security analytics', and 'Sample data'. Below this, a grid of 16 data source tiles is shown, each with an icon, a title, and a brief description of what it collects. The tiles are arranged in four rows and four columns. The first row includes Aerospike metrics, Apache logs, Apache metrics, and APM. The second row includes Ceph metrics, Couchbase metrics, Docker metrics, and Dropwizard metrics. The third row includes Elasticsearch logs, Elasticsearch metrics, Etcd metrics, and Golang metrics. The fourth row includes HAProxy metrics, IIS logs, Kafka logs, Kafka metrics, Kibana metrics, Kubernetes metrics, Logstash logs, and Logstash metrics. A vertical sidebar on the left contains various icons for navigation and settings.

Home

Add Data to Kibana

All Logging Metrics Security analytics Sample data

- Aerospike metrics**
Fetch internal metrics from the Aerospike server.
- Apache logs**
Collect and parse access and error logs created by the Apache HTTP server.
- Apache metrics**
Fetch internal metrics from the Apache 2 HTTP server.
- APM**
Collect in-depth performance metrics and errors from inside your applications.
- Ceph metrics**
Fetch internal metrics from the Ceph server.
- Couchbase metrics**
Fetch internal metrics from Couchbase.
- Docker metrics**
Fetch metrics about your Docker containers.
- Dropwizard metrics**
Fetch internal metrics from Dropwizard Java application.
- Elasticsearch logs**
Collect and parse logs created by Elasticsearch.
- Elasticsearch metrics**
Fetch internal metrics from Elasticsearch.
- Etcd metrics**
Fetch internal metrics from the Etcd server.
- Golang metrics**
Fetch internal metrics from a Golang app.
- HAProxy metrics**
Fetch internal metrics from the HAProxy server.
- IIS logs**
Collect and parse access and error logs created by the IIS HTTP server.
- Kafka logs**
Collect and parse logs created by Kafka.
- Kafka metrics**
Fetch internal metrics from the Kafka server.
- Kibana metrics**
Fetch internal metrics from Kibana.
- Kubernetes metrics**
Fetch metrics from your Kubernetes cluster.
- Logstash logs**
Collect and parse debug and slow logs created by Logstash.
- Logstash metrics**
Fetch internal metrics from Logstash.



Elastic Stack

Logging

Your logs, your way. Searchable at any scale, with speed.

Logs

container.image.name:"gcr.io/google-samples/gb-frontend@sha256:d44e7d7491a537f822e7fe86154

| Timestamp | event.dataset | Message |
|-----------------------------|---------------|-------------------------|
| Oct 10, 2019 @ 13:01:05.000 | apache.access | apons HTTP/1.1" 200 255 |
| Oct 10, 2019 @ 13:01:05.000 | apache.access | [apache][access] 10.12. |
| Oct 10, 2019 @ 13:01:06.000 | apache.access | [apache][access] 10.12. |
| Oct 10, 2019 @ 13:01:06.000 | apache.access | [apache][access] 10.12. |
| Oct 10, 2019 @ 13:01:07.000 | apache.access | [apache][access] 10.12. |
| Oct 10, 2019 @ 13:01:07.000 | apache.access | [apache][access] 10.12. |
| Oct 10, 2019 @ 13:01:08.000 | apache.access | [apache][access] 10.12. |
| Oct 10, 2019 @ 13:01:08.000 | apache.access | [apache][access] 10.12. |
| Oct 10, 2019 @ 13:01:09.000 | apache.access | [apache][access] 10.12. |
| Oct 10, 2019 @ 13:01:09.000 | apache.access | [apache][access] 10.12. |
| Oct 10, 2019 @ 13:01:10.000 | apache.access | [apache][access] 10.12. |
| Oct 10, 2019 @ 13:01:10.000 | apache.access | [apache][access] 10.12. |
| Oct 10, 2019 @ 13:01:11.000 | apache.access | [apache][access] 83.110 |
| Oct 10, 2019 @ 13:01:11.000 | apache.access | se HTTP/1.1" 200 255 |
| Oct 10, 2019 @ 13:01:11.000 | apache.access | [apache][access] 10.12. |
| Oct 10, 2019 @ 13:01:11.000 | apache.access | [apache][access] 10.12. |
| Oct 10, 2019 @ 13:01:12.000 | apache.access | [apache][access] 10.12. |
| Oct 10, 2019 @ 13:01:12.000 | apache.access | [apache][access] 10.12. |
| Oct 10, 2019 @ 13:01:13.000 | apache.access | [apache][access] 10.12. |

Log event document details

Field

Value

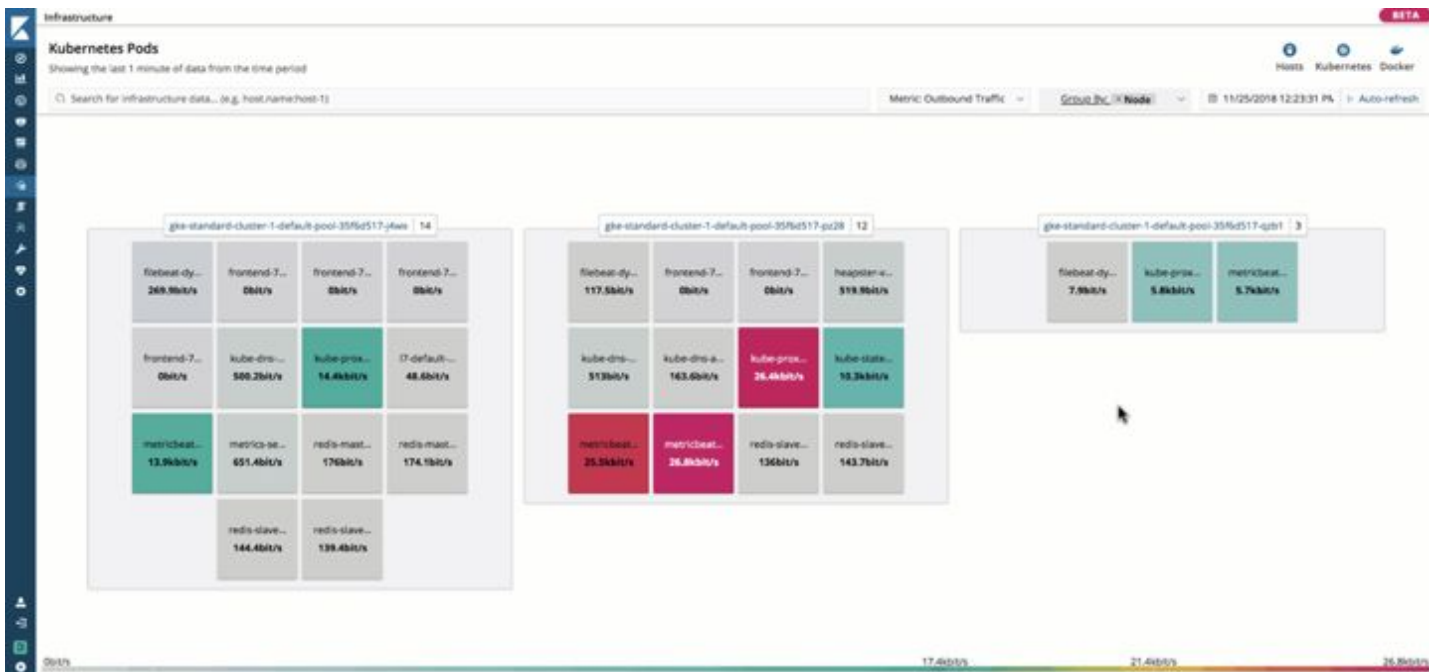
| | |
|-------------------------|--------------------------------------|
| @timestamp | 2019-10-10T17:01:10.000Z |
| _id | WLSetm0Bs6l2_dbQAiVr |
| _index | filebeat-7.2.0-2019.10.10-000307 |
| agent.ephemeral_id | 9f797298-5e27-4ed3-a0b0-d96d5f80bab8 |
| agent.hostname | filebeat-demo-green-868wc |
| agent.id | 5222143f-79cb-42a3-9950-2c8360d274c5 |
| agent.type | filebeat |
| agent.version | 7.2.0 |
| cloud.availability_zone | us-central1-a |
| cloud.instance.id | 8507180427070578873 |



Elastic Stack

Infrastructure Metrics

Unified Infrastructure Metrics, in One Place

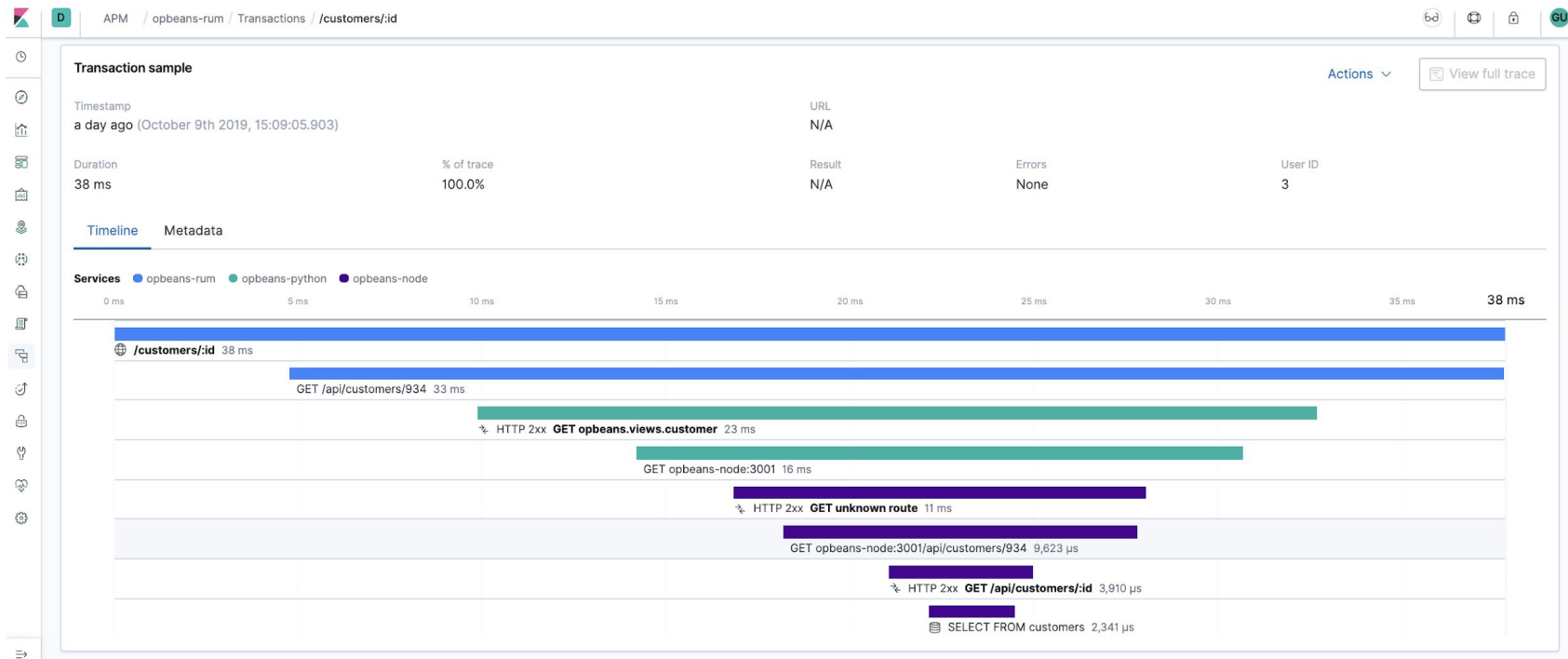




Elastic Stack

APM

Logs + Metrics + Distributed Tracing





Questions?

