elastic | 中国开发者大会

Logging, Metrics, and APM: The Operations Trifecta

Monica Sarbu

Elastic, Beats Creator and Team Lead of Ingest



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

elastic

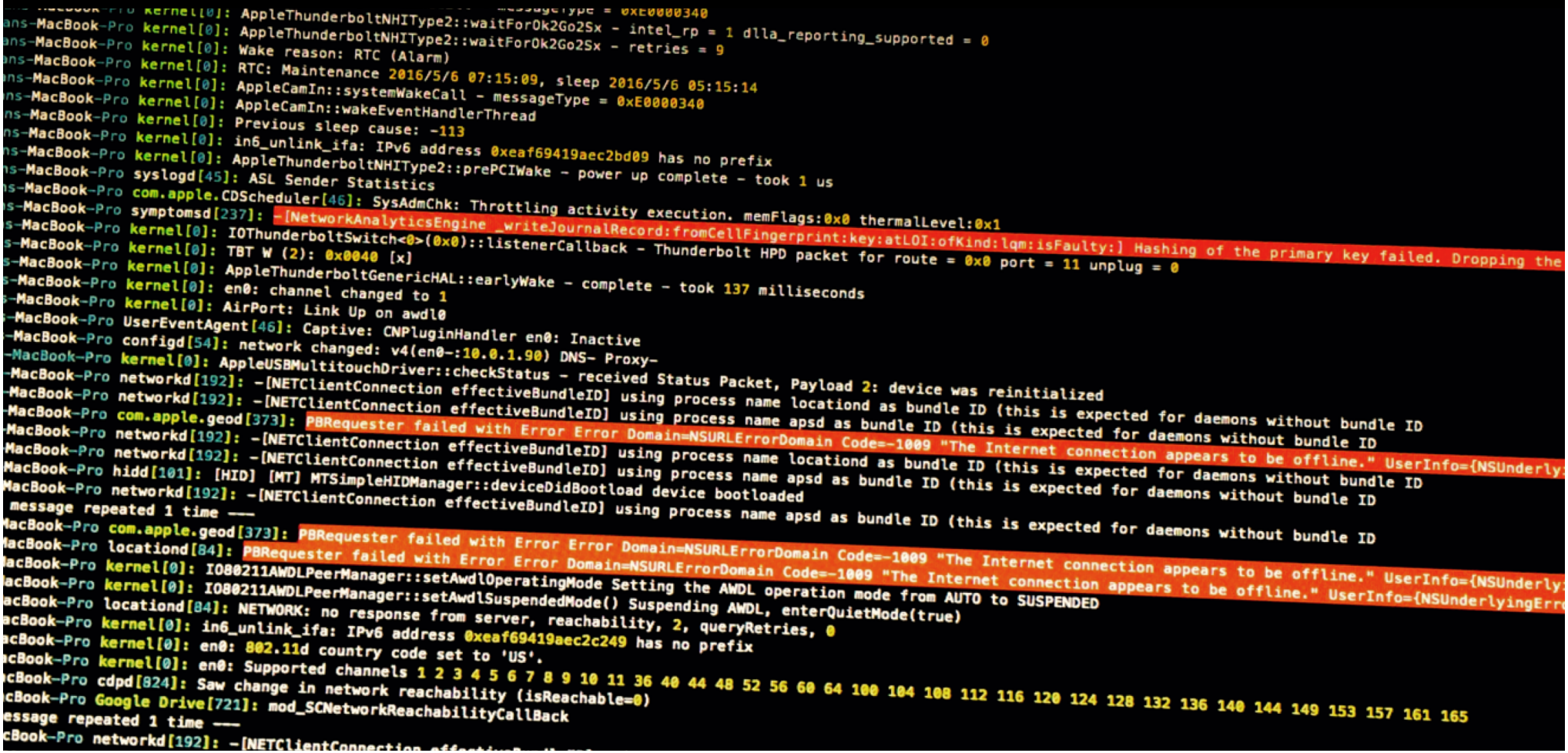
你好



Monica Sarbu
Beats creator and Team lead of Ingest,
Elastic

elastic

You know us for searching logs...



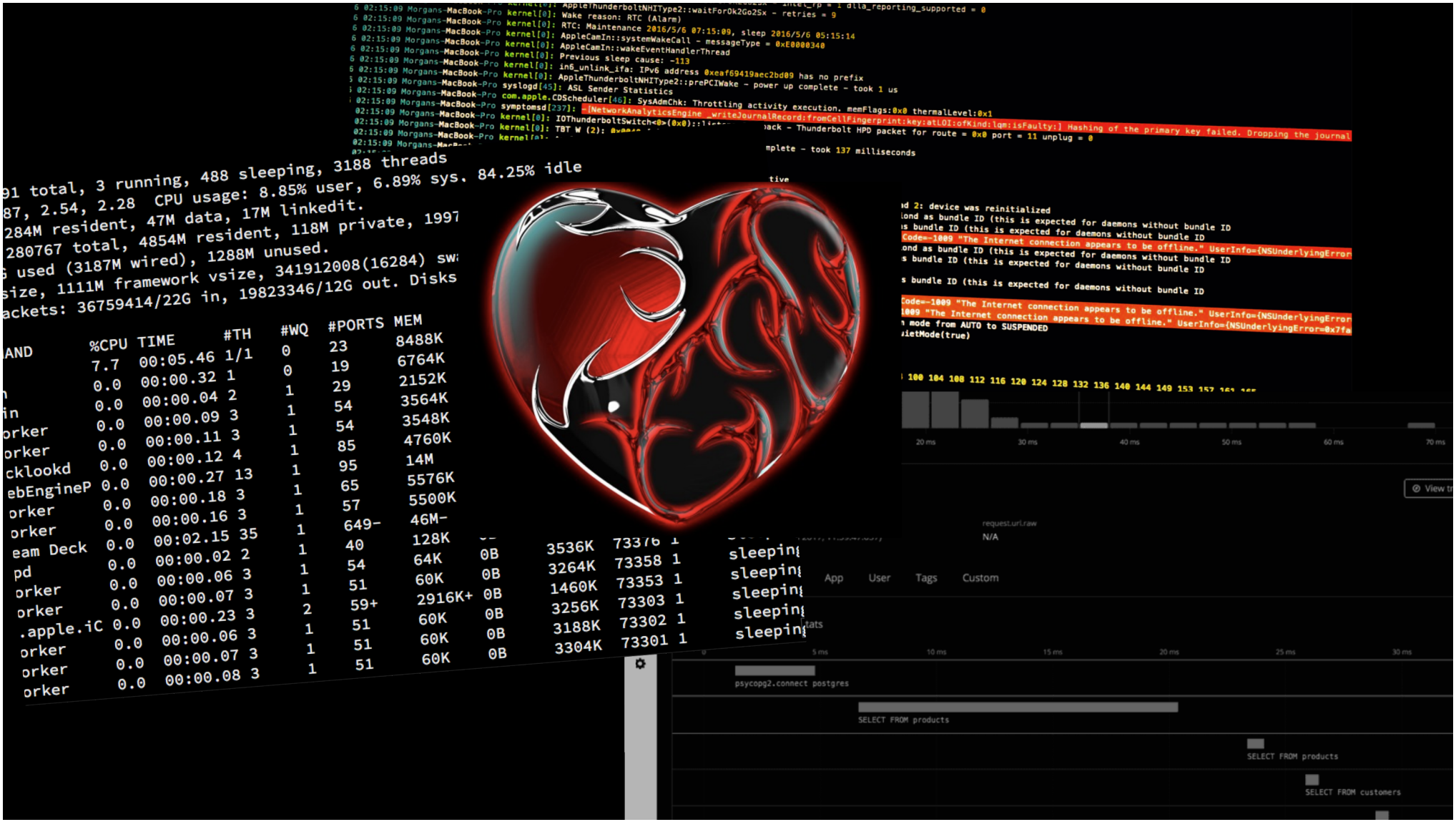
You heard we are good at metrics...

```
Load Avg: 2.87, 2.54, 2.28  CPU usage: 8.85% user, 6.89% sys, 84.25% idle
SharedLibs: 284M resident, 47M data, 17M linkedit.
MemRegions: 280767 total, 4854M resident, 118M private, 1997M shared.
PhysMem: 15G used (3187M wired), 1288M unused.
VM: 6150G vsize, 1111M framework vsize, 341912008(16284) swapins, 348809712(0) swapouts.
Networks: packets: 36759414/22G in, 19823346/12G out. Disks: 87127310/2211G read, 32948289/2457G written.

PID    COMMAND      %CPU TIME     #TH   #WQ  #PORTS MEM    PURG   CMPRS  PGRP  PPID  STATE
73698  top          7.7  00:05.46 1/1   0    23     8488K  0B     0B     73698 73428 running
73428  bash         0.0  00:00.32 1     0    19     6764K  0B     0B     73428 73427 sleeping
73427  login        0.0  00:00.04 2     1    29     2152K  0B     0B     73427 1291  sleeping
73426  mdworker     0.0  00:00.09 3     1    54     3564K  0B     0B     73426 1     sleeping
73425  mdworker     0.0  00:00.11 3     1    54     3548K  0B     0B     73425 1     sleeping
73413  quicklookd   0.0  00:00.12 4     1    85     4760K  32K    0B     73413 1     sleeping
73412  QtWebEngineP 0.0  00:00.27 13    1    95     14M    0B     0B     73408 73408 sleeping
73411  mdworker     0.0  00:00.18 3     1    65     5576K  0B     0B     73411 1     sleeping
73410  mdworker     0.0  00:00.16 3     1    57     5500K  0B     0B     73410 1     sleeping
73408  Stream Deck  0.0  00:02.15 35    1    649-   46M-   1476K  5292K  73408 1     sleeping
73403  helpd        0.0  00:00.02 2     1    40     128K   0B     1104K  73403 1     sleeping
73376  mdworker     0.0  00:00.06 3     1    54     64K    0B     3536K  73376 1     sleeping
73358  mdworker     0.0  00:00.07 3     1    51     60K    0B     3264K  73358 1     sleeping
73353  com.apple.iC 0.0  00:00.23 3     2    59+    2916K+ 0B     1460K  73353 1     sleeping
73303  mdworker     0.0  00:00.06 3     1    51     60K    0B     3256K  73303 1     sleeping
73302  mdworker     0.0  00:00.07 3     1    51     60K    0B     3188K  73302 1     sleeping
73301  mdworker     0.0  00:00.08 3     1    51     60K    0B     3304K  73301 1     sleeping
```

You learned that we added APM

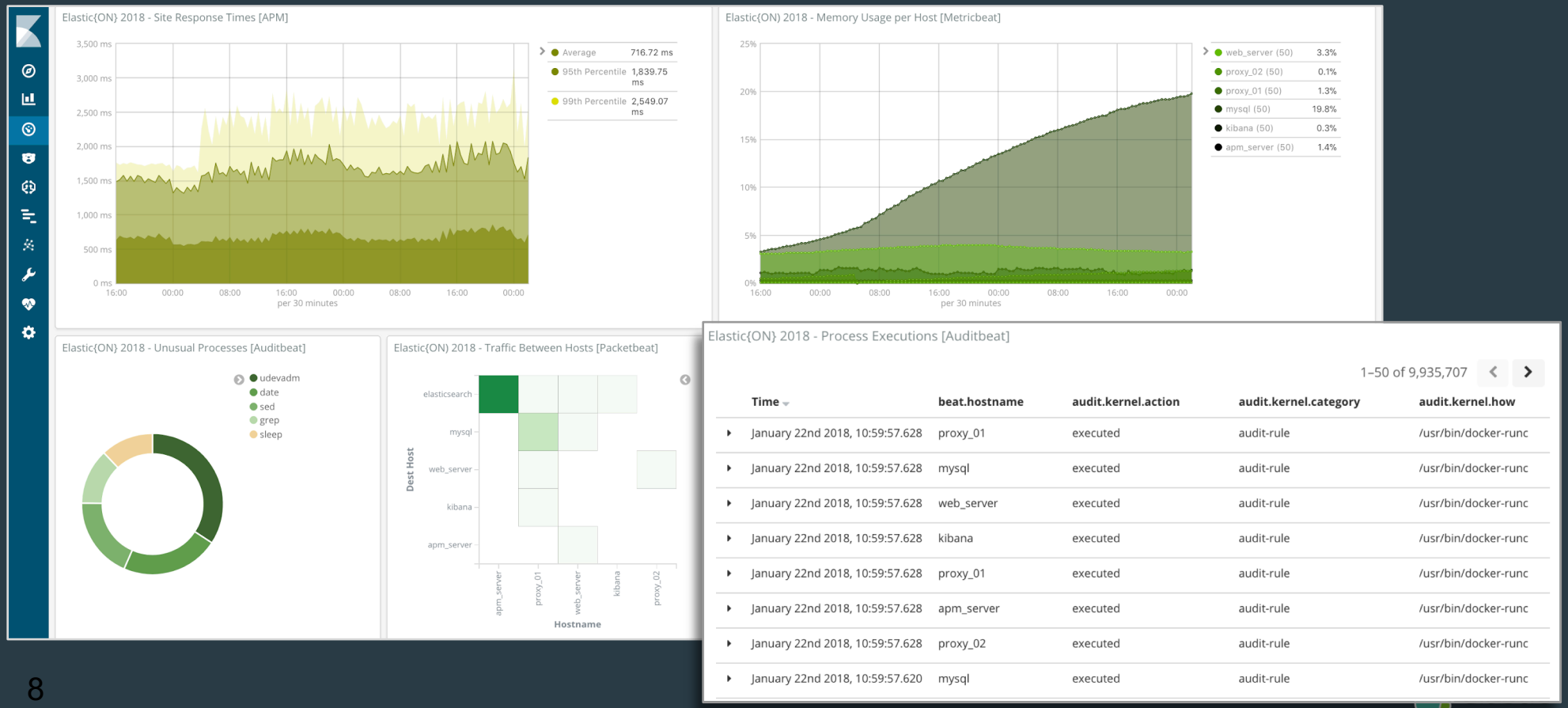



91 total, 3 running, 488 sleeping, 3188 threads
87, 2.54, 2.28 CPU usage: 8.85% user, 6.89% sys, 84.25% idle
284M resident, 47M data, 17M linkedit.
280767 total, 4854M resident, 118M private, 1997
used (3187M wired), 1288M unused.
size, 1111M framework vsize, 341912008(16284) swa
ackets: 36759414/22G in, 19823346/12G out. Disks
AND %CPU TIME #TH #WQ #PORTS MEM
7.7 00:05.46 1/1 0 23 8488K
0.0 00:00.32 1 0 19 6764K
0.0 00:00.04 2 1 29 2152K
in 0.0 00:00.09 3 1 54 3564K
orker 0.0 00:00.11 3 1 54 3548K
orker 0.0 00:00.12 4 1 85 4760K
cklookd 0.0 00:00.27 13 1 95 14M
ebEngineP 0.0 00:00.18 3 1 65 5576K
orker 0.0 00:00.16 3 1 57 5500K
orker 0.0 00:02.15 35 1 649- 46M-
eam Deck 0.0 00:00.02 2 1 40 128K
pd 0.0 00:00.06 3 1 54 64K 0B 3536K 73376 1 sleepin
orker 0.0 00:00.07 3 1 51 60K 0B 3264K 73358 1 sleepin
orker 0.0 00:00.23 3 2 59+ 2916K+ 0B 1460K 73353 1 sleepin
.apple.iC 0.0 00:00.06 3 1 51 60K 0B 3256K 73303 1 sleepin
orker 0.0 00:00.07 3 1 51 60K 0B 3188K 73302 1 sleepin
orker 0.0 00:00.08 3 1 51 60K 0B 3304K 73301 1 sleepin
6 02:15:09 Morgans-MacBook-Pro kernel[0]: Wake reason: RTC (Alarm)
6 02:15:09 Morgans-MacBook-Pro kernel[0]: RTC: Maintenance 2016/5/6 07:15:09, sleep 2016/5/6 05:15:14
6 02:15:09 Morgans-MacBook-Pro kernel[0]: AppleCamIn::systemWakeCall - messageType = 0xE0000340
6 02:15:09 Morgans-MacBook-Pro kernel[0]: AppleCamIn::wakeEventHandlerThread
6 02:15:09 Morgans-MacBook-Pro kernel[0]: Previous sleep cause: -113
6 02:15:09 Morgans-MacBook-Pro kernel[0]: in6_unlink_ifa: IPv6 address 0xeaf69419aec2bd09 has no prefix
02:15:09 Morgans-MacBook-Pro syslogd[45]: ASL Sender Statistics
02:15:09 Morgans-MacBook-Pro com.apple.CDScheduler[46]: SysAdmChk: Throttling activity execution. memFlags:0x0 thermalLevel:0x1
02:15:09 Morgans-MacBook-Pro symptomsd[237]: -[NetworkAnalyticsEngine _writeJournalRecord:fromCellFingerprint:key:atLOI:ofKind:lqm:isFaulty:] Hashing of the primary key failed. Dropping the journal
02:15:09 Morgans-MacBook-Pro kernel[0]: IOThunderboltSwitch<0>(0x0)::
ack - Thunderbolt HPD packet for route = 0x0 port = 11 unplug = 0
mplete - took 137 milliseconds
tive
id 2: device was reinitialized
iond as bundle ID (this is expected for daemons without bundle ID
is bundle ID (this is expected for daemons without bundle ID
Code=-1009 "The Internet connection appears to be offline." UserInfo={NSUnderlyingError
ond as bundle ID (this is expected for daemons without bundle ID
s bundle ID (this is expected for daemons without bundle ID
s bundle ID (this is expected for daemons without bundle ID
Code=-1009 "The Internet connection appears to be offline." UserInfo={NSUnderlyingError
1009 "The Internet connection appears to be offline." UserInfo={NSUnderlyingError=0x7f
n mode from AUTO to SUSPENDED
zietMode(true)
100 104 108 112 116 120 124 128 132 136 140 144 149 153
20 ms
30 ms
40 ms
50 ms
60 ms
70 ms
View tr
request.url.raw
N/A
App
User
Tags
Custom
tats
0
5 ms
10 ms
15 ms
20 ms
25 ms
30 ms
psycopg2.connect postgres
SELECT FROM products
SELECT FROM products
SELECT FROM customers

Benefits of having
Logs + Metrics + APM
in one system

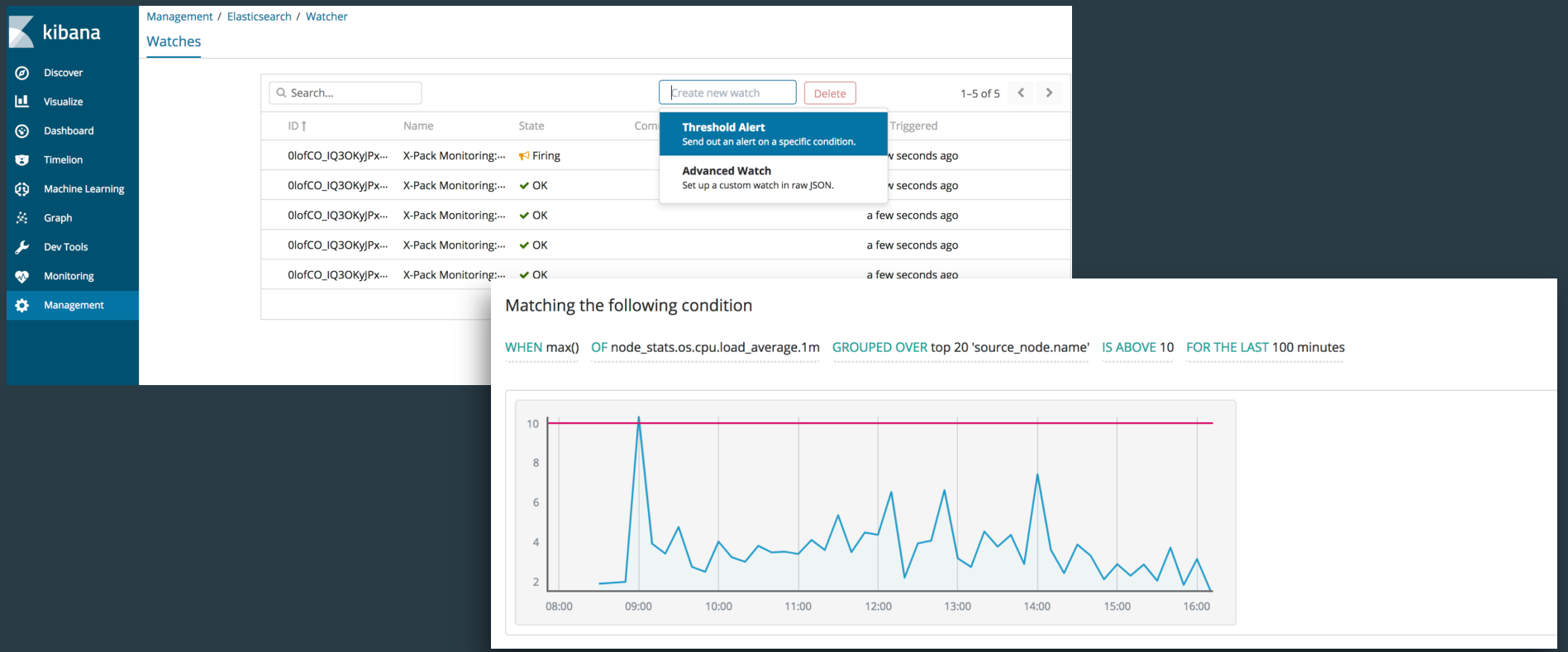
Unified Dashboard

Same UI for KPI summaries and root-cause analysis



Unified Alerting

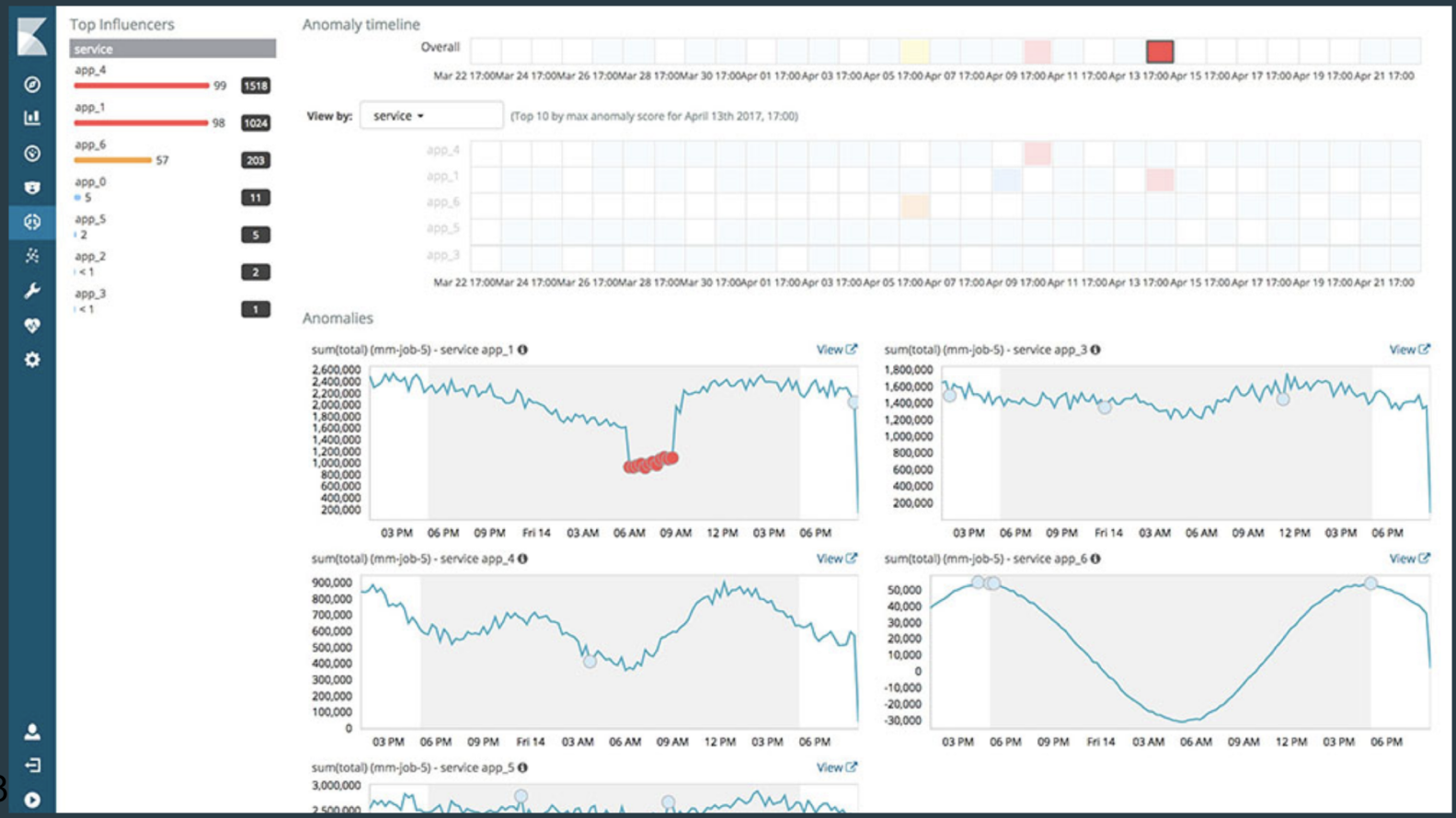
Trigger off any operational data to provide unified SLA monitoring



elastic

Unified Machine Learning

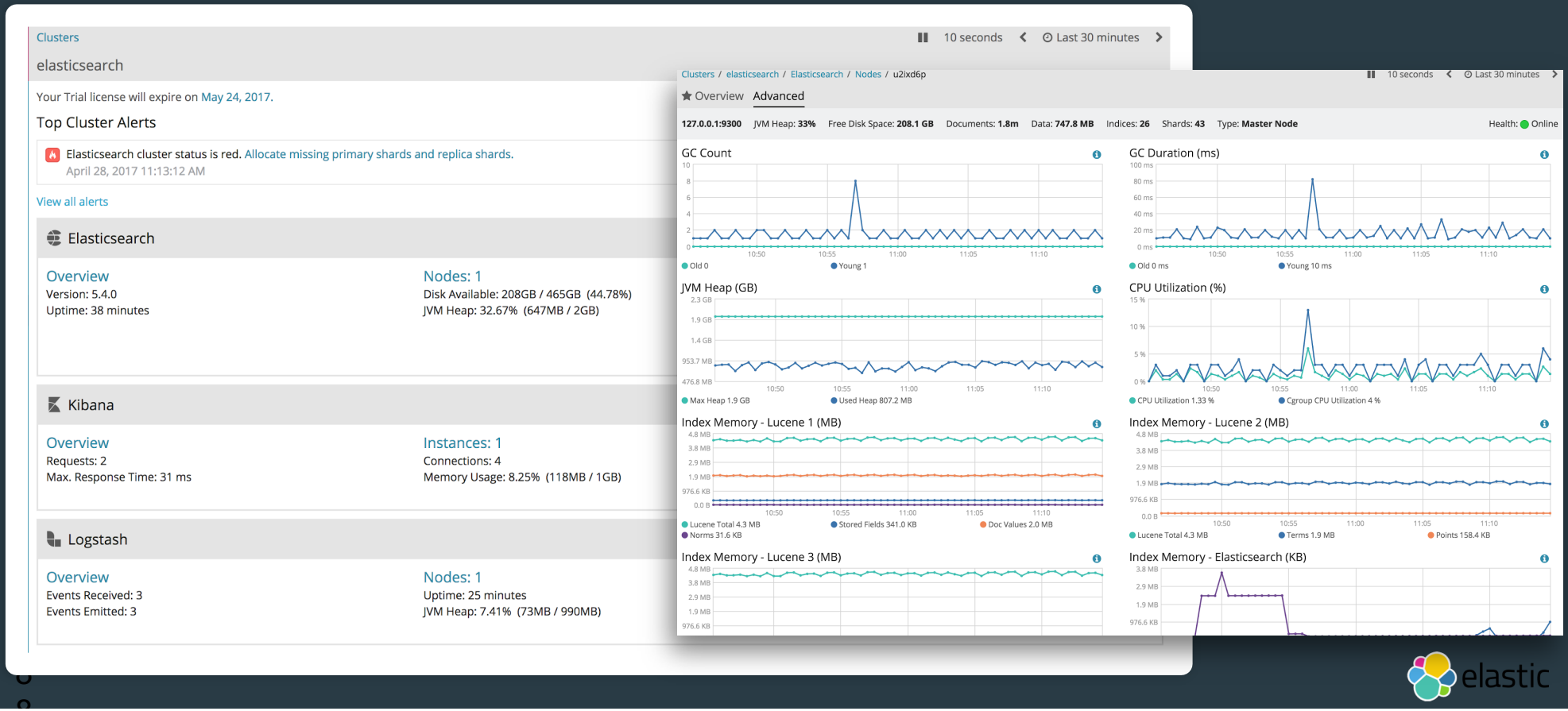
Correlate multiple data sources for more intelligent anomaly detection



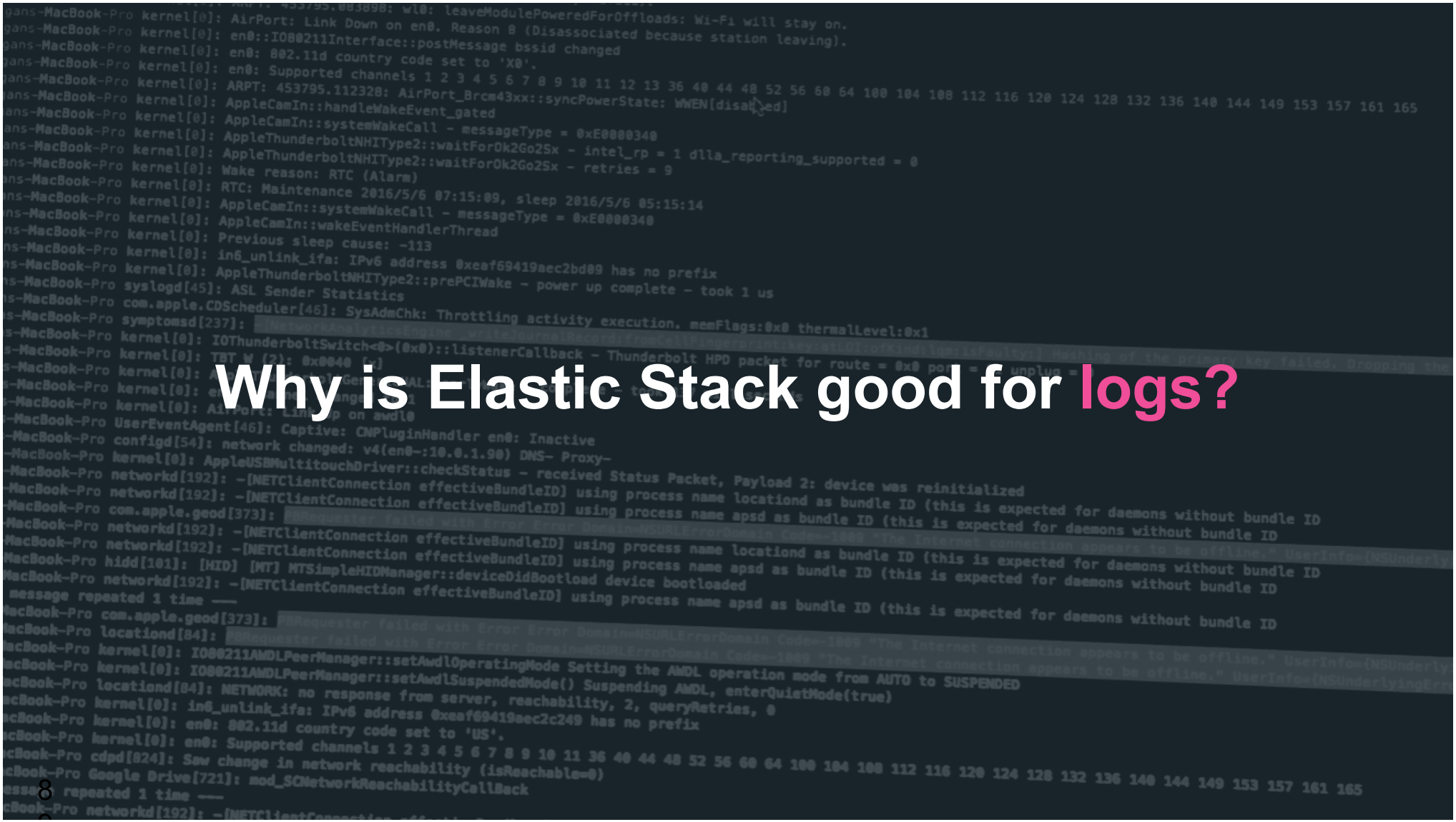
elastic

Operational Gains

Single technology for operational data saves on administrative costs



elastic


Why is Elastic Stack good for logs?

Get logs from system



Filebeat

- Ships your logs
- Get logs from:
  - Local system
  - Over TCP/UDP
  - Over syslog

Journalbeat coming soon

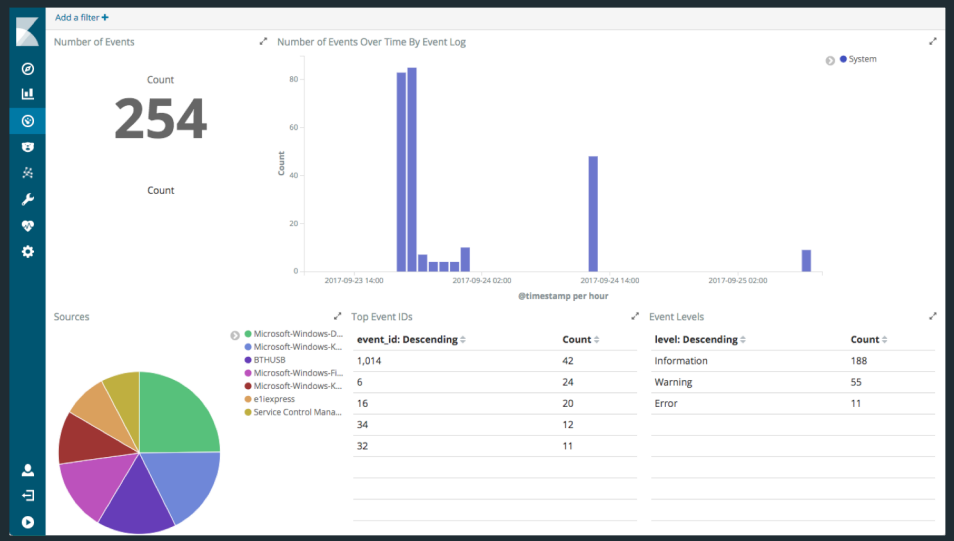
- Ships your Journald logs
- To be released as experimental in 6.5
- Plan to become a Filebeat input

Get logs from system

WINLOGBEAT

Winlogbeat

- Ships your **Windows Event Logs**
- You can get information like logons, logon failures, when a USB device is attached or new software installed.



Get logs from containers

FILEBEAT



Docker

- **add_docker_metadata** processor annotates each event with container ID, name, image, labels
- **Docker input** (experimental) in Filebeat

Kubernetes

- **add_kubernetes_metadata** processor annotates each event with pod name, namespace, labels

Get logs from cloud

FILEBEAT WINLOGBEAT





Filebeat / Winlogbeat

- **add_cloud_metadata** processor to annotate logs with region, instance type, availability zone

Supported cloud providers

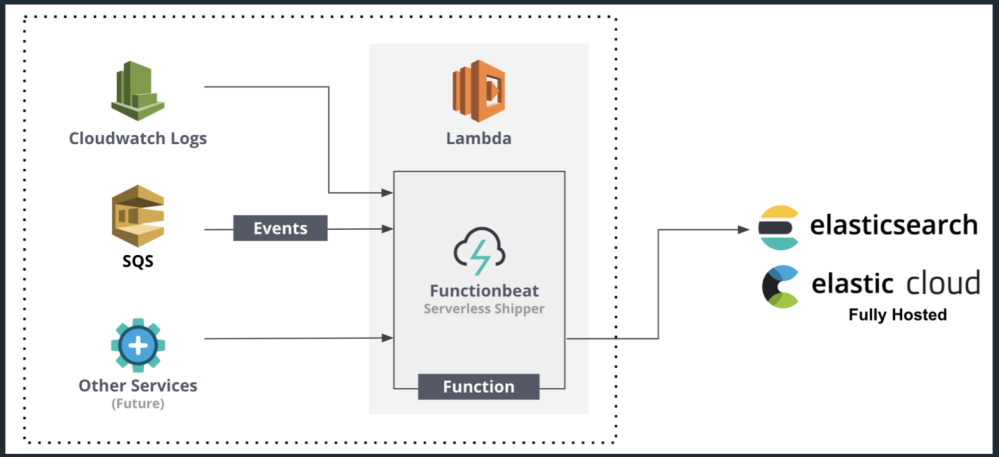
- Amazon Elastic Cloud
- Digital Ocean
- Google Compute Engine,
- Alibaba Cloud
- Azure Virtual Machine
- Tencent Cloud
- Openstack Nova

Get logs from cloud

FUNCTIONBEAT

Functionbeat coming soon

- **Agentless shipper**
- Automation to start Functionbeat in AWS from a single CLI command
- Example: Install in AWS Lambda functions to collect logs from CloudWatch and send it to Elasticsearch

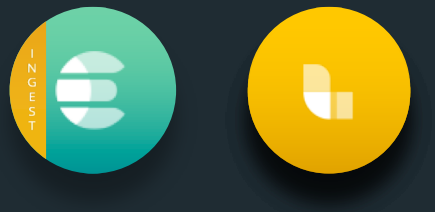


Filebeat ships Raw Logs

```
message: “55.3.244.1 GET /index.html 15824 0.043”
```

elastic

Parse the logs




```
message: “55.3.244.1 GET /index.html 15824 0.043”
```

+

```
%{IP:client} %{WORD:method} %{URIPATHPARAM:request}
%{NUMBER:bytes} %{NUMBER:duration}
```

elastic

Parsed logs




```
message: “55.3.244.1 GET /index.html 15824 0.043”
```

+

```
%{IP:client} %{WORD:method} %{URIPATHPARAM:request}
%{NUMBER:bytes} %{NUMBER:duration}
```

=

```
message: “55.3.244.1 GET /index.html 15824 0.043”
  client: “55.3.244.1”,
  method: “GET”,
  request: “/index.html”
  bytes: 15824,
  duration: 0.043
  …
```

elastic

Filebeat Modules

Services

Databases
- MySQL
- PostgreSQL

Queues
- Kafka
- Redis

Web servers
- Apache
- Nginx

Others
- IIS
- Traefik
- Auditd
- Icinga

Elastic Stack
- Kibana
- Logstash
- Elasticsearch

elastic

Load Filebeat module

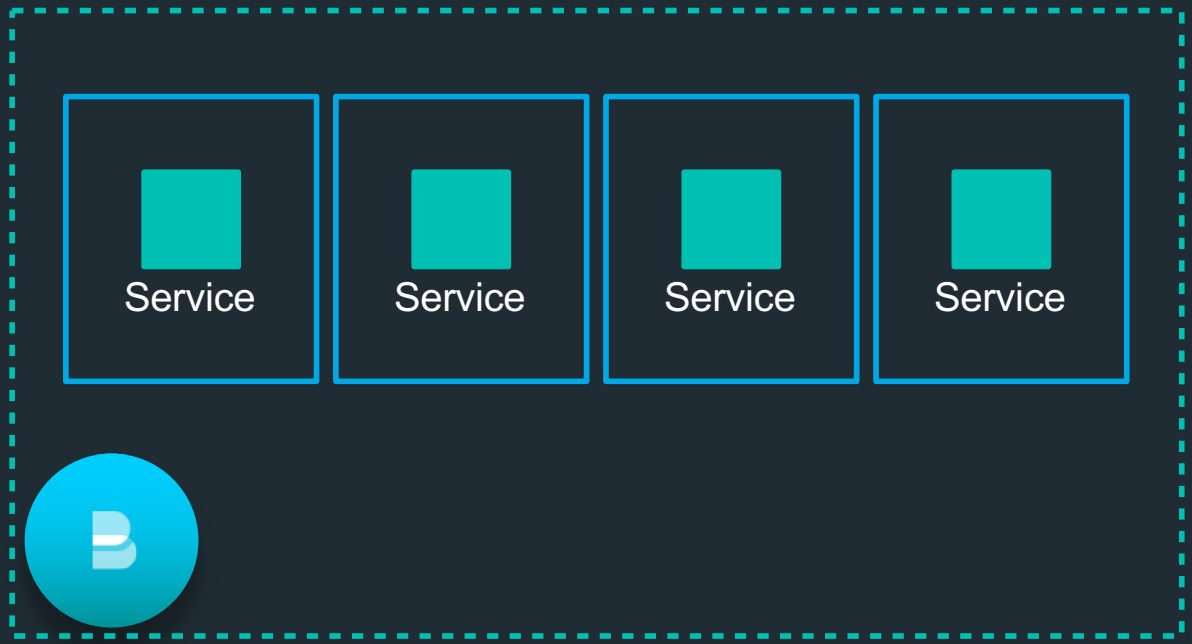
```
$ filebeat modules enable nginx
$ vim modules.d/nginx.yml
$ filebeat setup
$ filebeat -e
```

elastic

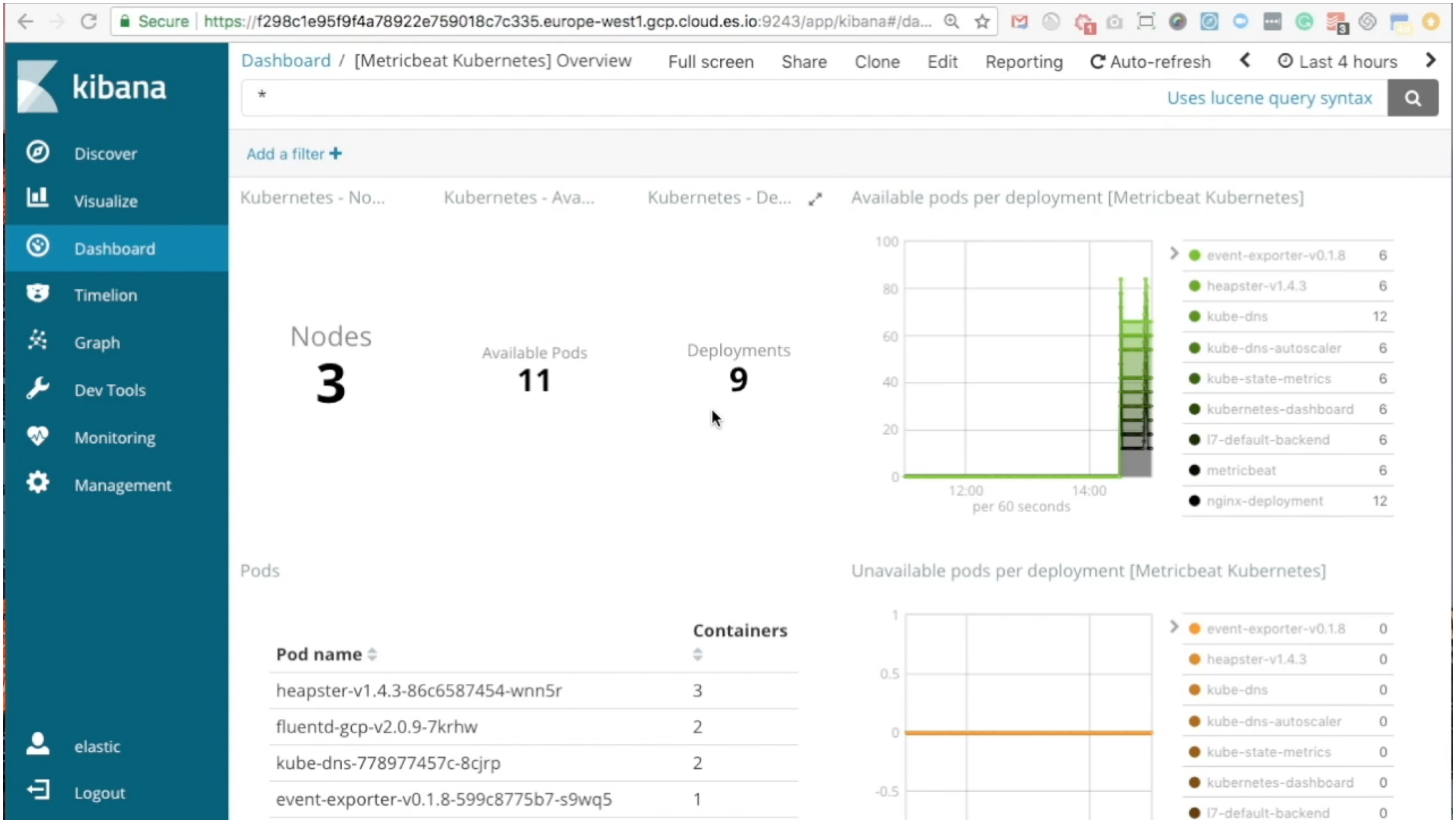
Autodiscovery

Supported providers

- Docker
- Kubernetes
- Jolokia



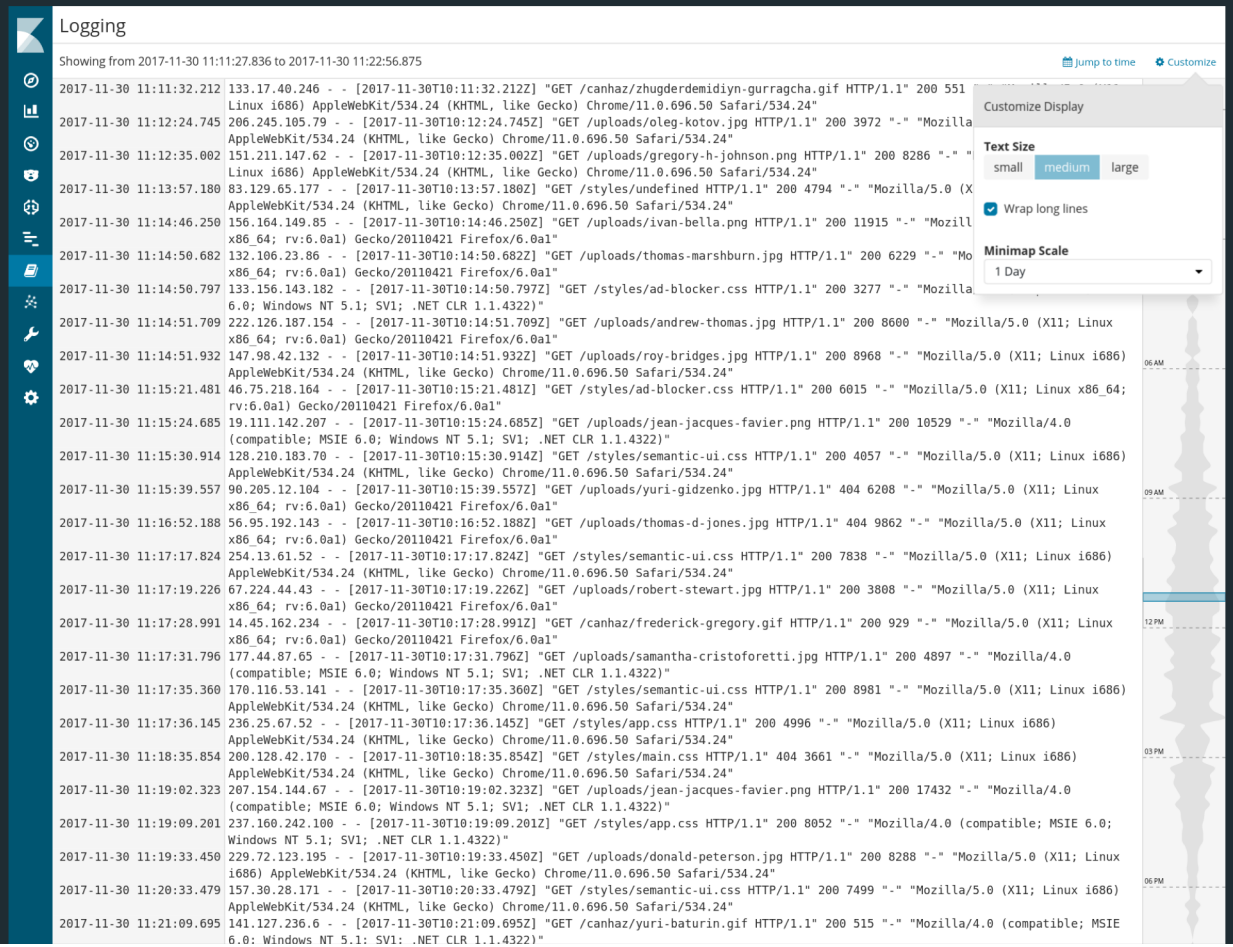
elastic


Secure | https://f298c1e95f9f4a78922e759018c7c335.europe-west1.gcp.cloud.es.io:9243/app/kibana#/da...
kibana
Discover
Visualize
Dashboard
Timelion
Graph
Dev Tools
Monitoring
Management
elastic
Logout
Dashboard / [Metricbeat Kubernetes] Overview
Full screen
Share
Clone
Edit
Reporting
Auto-refresh
Last 4 hours
*
Uses lucene query syntax
Add a filter +
Kubernetes - No...
Kubernetes - Ava...
Kubernetes - De...
Nodes
3
Available Pods
11
Deployments
9
Available pods per deployment [Metricbeat Kubernetes]
100
80
60
40
20
0
12:00
14:00
per 60 seconds
event-exporter-v0.1.8 6
heapster-v1.4.3 6
kube-dns 12
kube-dns-autoscaler 6
kube-state-metrics 6
kubernetes-dashboard 6
l7-default-backend 6
metricbeat 6
nginx-deployment 12
Pods
Pod name
Containers
heapster-v1.4.3-86c6587454-wnn5r 3
fluentd-gcp-v2.0.9-7krhw 2
kube-dns-778977457c-8cjrp 2
event-exporter-v0.1.8-599c8775b7-s9wq5 1
Unavailable pods per deployment [Metricbeat Kubernetes]
1
0.5
0
-0.5
event-exporter-v0.1.8 0
heapster-v1.4.3 0
kube-dns 0
kube-dns-autoscaler 0
kube-state-metrics 0
kubernetes-dashboard 0
l7-default-backend 0

Introduce Logs viewer

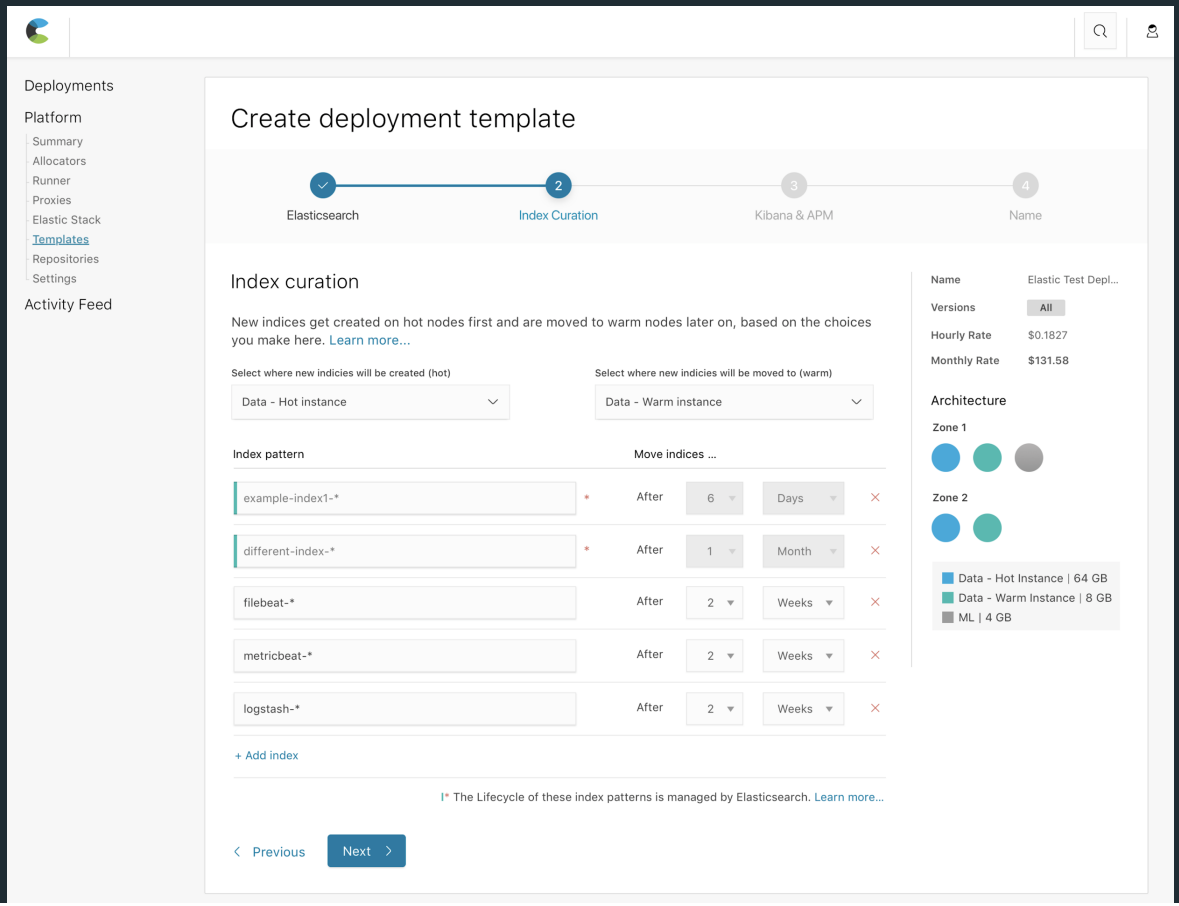
Coming in 6.5

- ✓ Infinite scrolling
- ✓ Search
- ✓ Highlight
- ✓ Timeline navigation
- ✓ Live streaming



Streamlined integration with Elastic Cloud

- Ship to your cluster using **cloud.id**
- One click **hot-warm** deployments





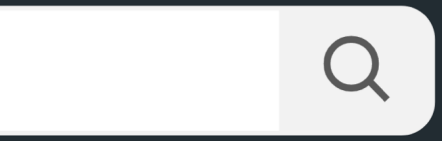
Why is Elastic Stack good for metrics?

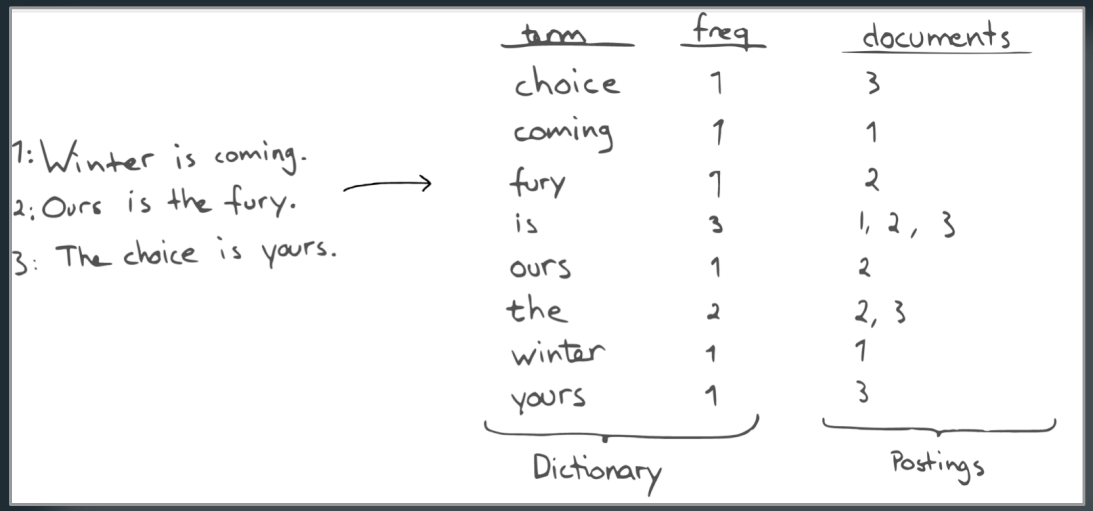
Evolution of Elasticsearch into a Metrics Store

Elasticsearch beginnings

Circa 2010

- Elasticsearch primarily used for **application search**
- **Inverted index,** at the heart of the full-text search that makes the search very fast





elastic

Elasticsearch evolving to support analytics

~ 2010 to 2014

- Elasticsearch 1.0 evolves to support a **columnar store** (built on top of Lucene **"doc values**") that allows filtering, analytics and aggregations
- Structured string and **numerical data** can be stored

usernid	first	middle	last	city	state
john123	John	James	Smith	Alamo	California
jrice	Jill	Amy	Rice		
mt123	Jeff		Twain	Toledo	Ohio
sadams	Sue		Adams		
adoe	Amy		Doe	Miami	Florida

https://www.elastic.co/blog/elasticsearch-as-a-column-store

elastic

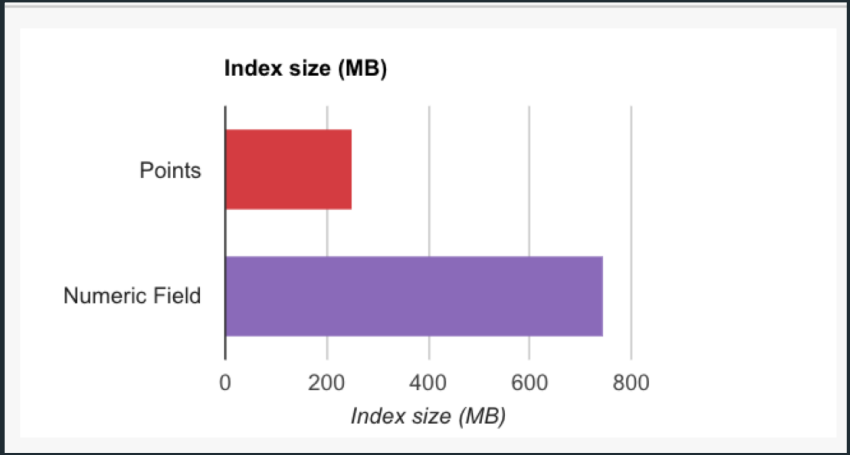
Elasticsearch storage efficiencies

2016

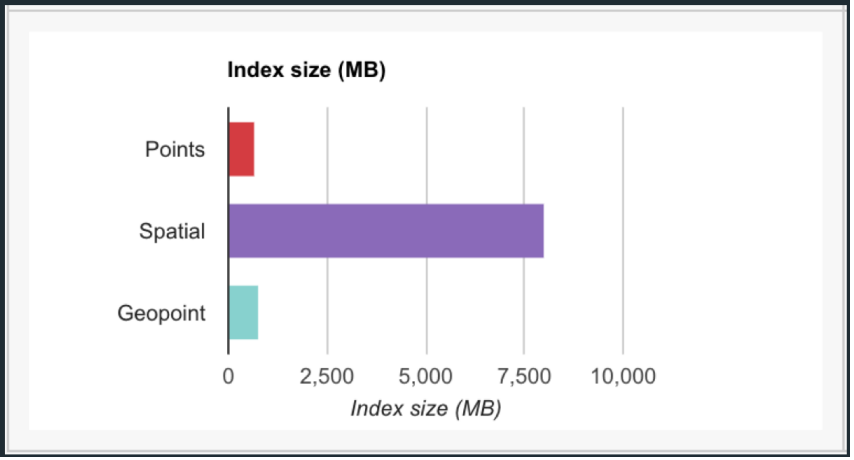
- Elasticsearch 5.0 adds more data structures for efficient storing and querying numbers (**BKD Trees**)
- These structures become the default storage for numerical and geospatial data in Elasticsearch

https://www.elastic.co/blog/searching-numb3rs-in-5.0

1-Dimension



2-Dimensions

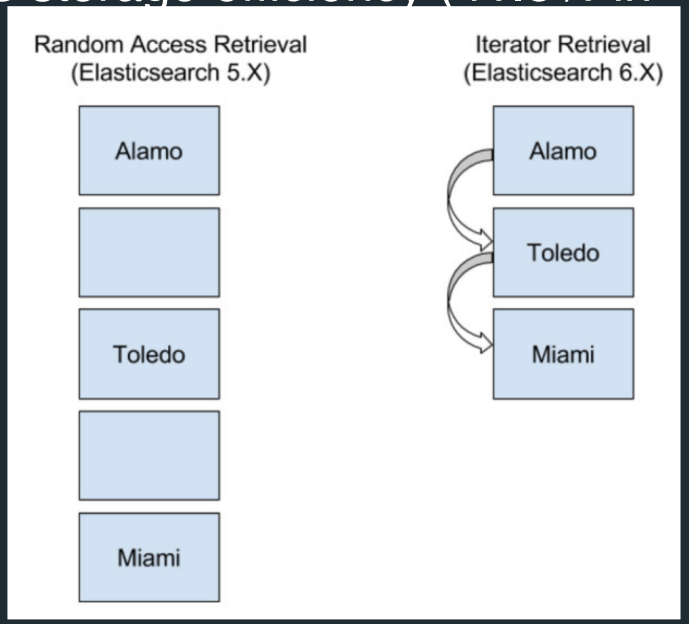


Elasticsearch storage efficiencies

2017

- Elasticsearch 6.0 improves Lucene **sparse values** storage efficiency (41.5% in Metricbeat index size)

usernid	first	middle	last	city	state
john123	John	James	Smith	Alamo	California
jrice	Jill	Amy	Rice		
mt123	Jeff		Twain	Toledo	Ohio
sadams	Sue		Adams		
adoe	Amy		Doe	Miami	Florida

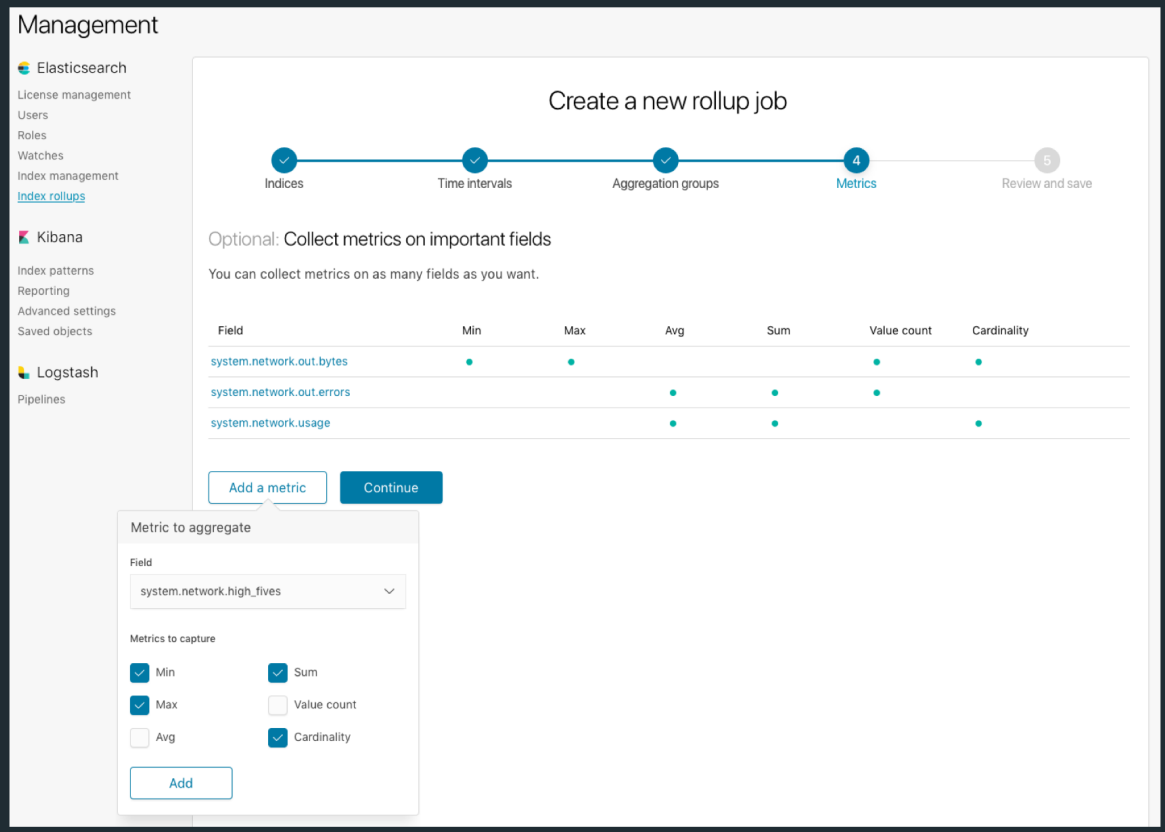


https://www.elastic.co/blog/minimize-index-storage-size-elasticsearch-6-0

elastic

Rollup support for long-term retentions

Added in Elasticsearch 6.3

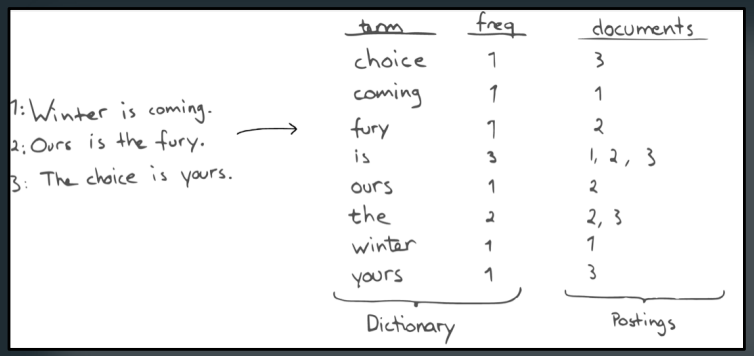


https://www.elastic.co/blog/data-rollups-in-elasticsearch-you-know-for-saving-space

elastic

Elasticsearch for search and numerical analytics

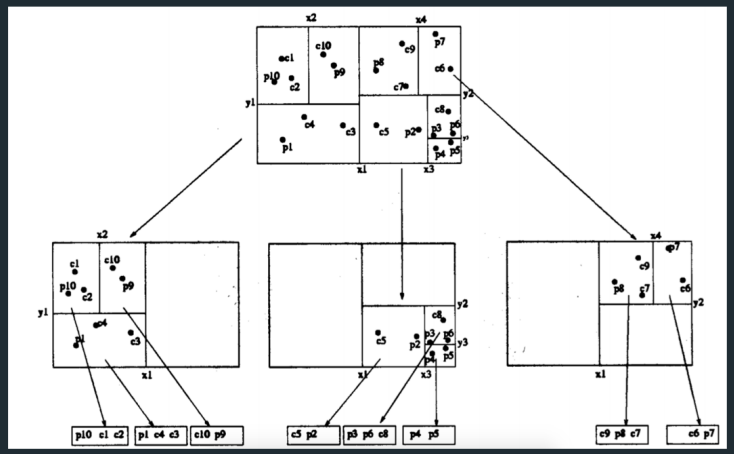
Inverted Index for full-text search



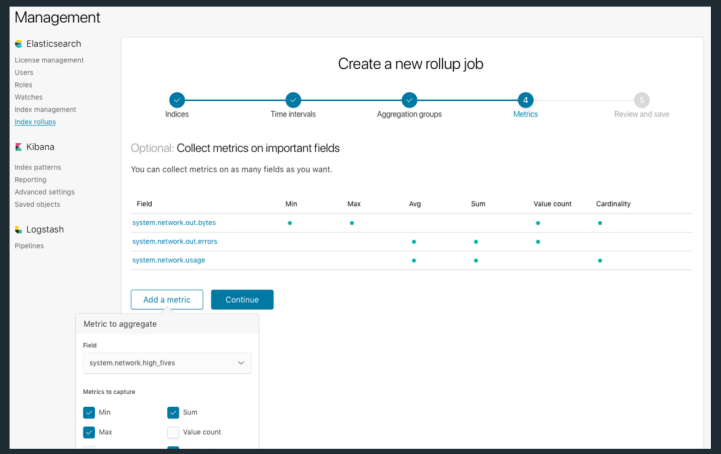
Columnar store for structured data

usernid	first	middle	last	city	state
john123	John	James	Smith	Alamo	California
jrice	Jill	Amy	Rice		
mt123	Jeff		Twain	Toledo	Ohio
sadams	Sue		Adams		
adoe	Amy		Doe	Miami	Florida

BKD Trees for numerical operations



Rollups

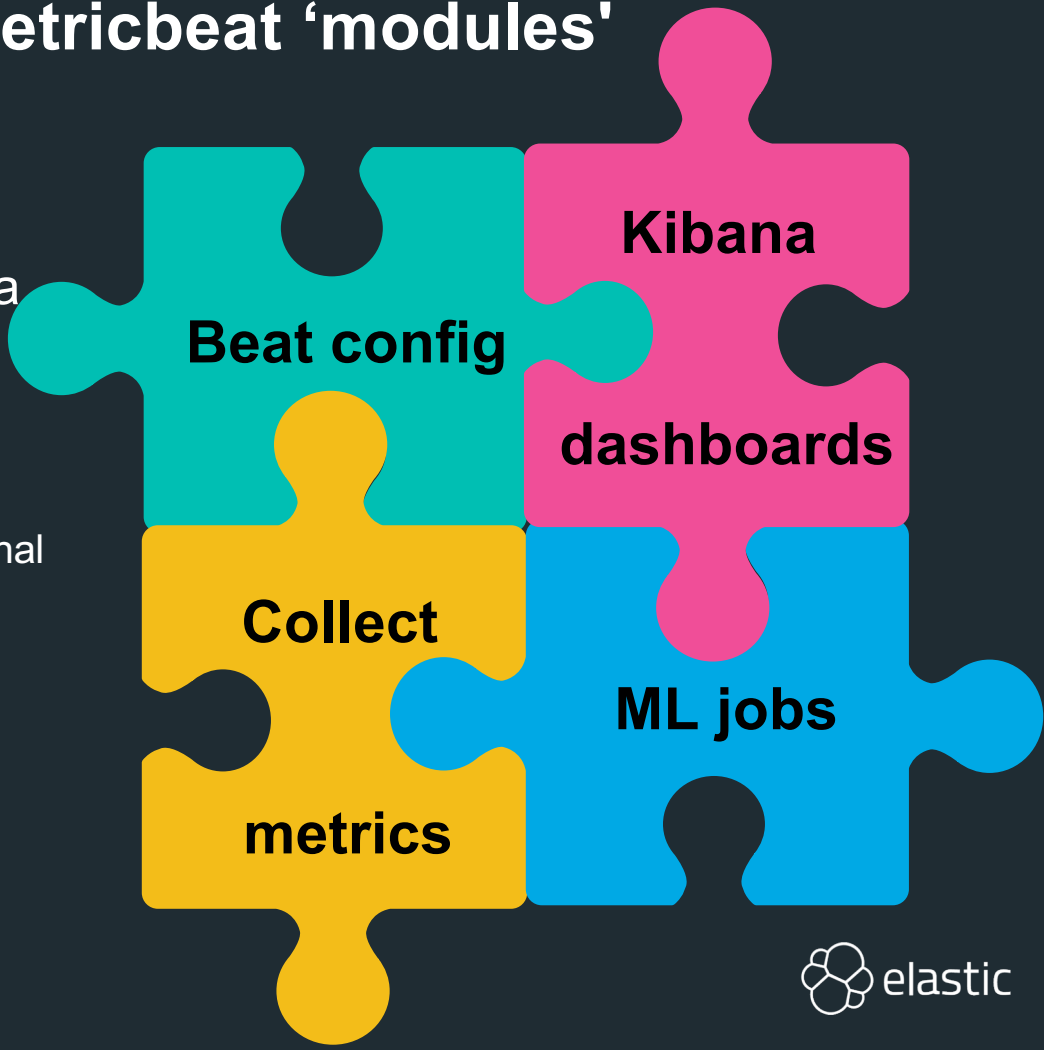


elastic

Evolution of the rest of Elastic Stack into a Metrics Solution

Turn-key monitoring with Metricbeat ‘modules'

- Turn-key experience for specific data types
- A Metricbeat module:
  - Collects periodically metrics from external systems
  - Comes with Kibana dashboards
  - Comes with ML jobs



elastic

Metricbeat Modules

METRICBEAT



Infrastructure

System

- Linux
- MacOS
- Windows
- Perfmon

Containers

- Docker
- Kubernetes

Virtualization

- vSphere

Storage

- Ceph

elastic

Metricbeat Modules

METRICBEAT



Services

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

Queues
- Kafka
- Redis
- RabbitMQ

Caches
- Memcached

Custom apps
- JMX/Jolokia
- PHP-FPM
- Golang

Web servers
- Apache
- Nginx

Elastic Stack
- Kibana
- Logstash
- Elasticsearch

Other
- HAProxy
- Zookeeper

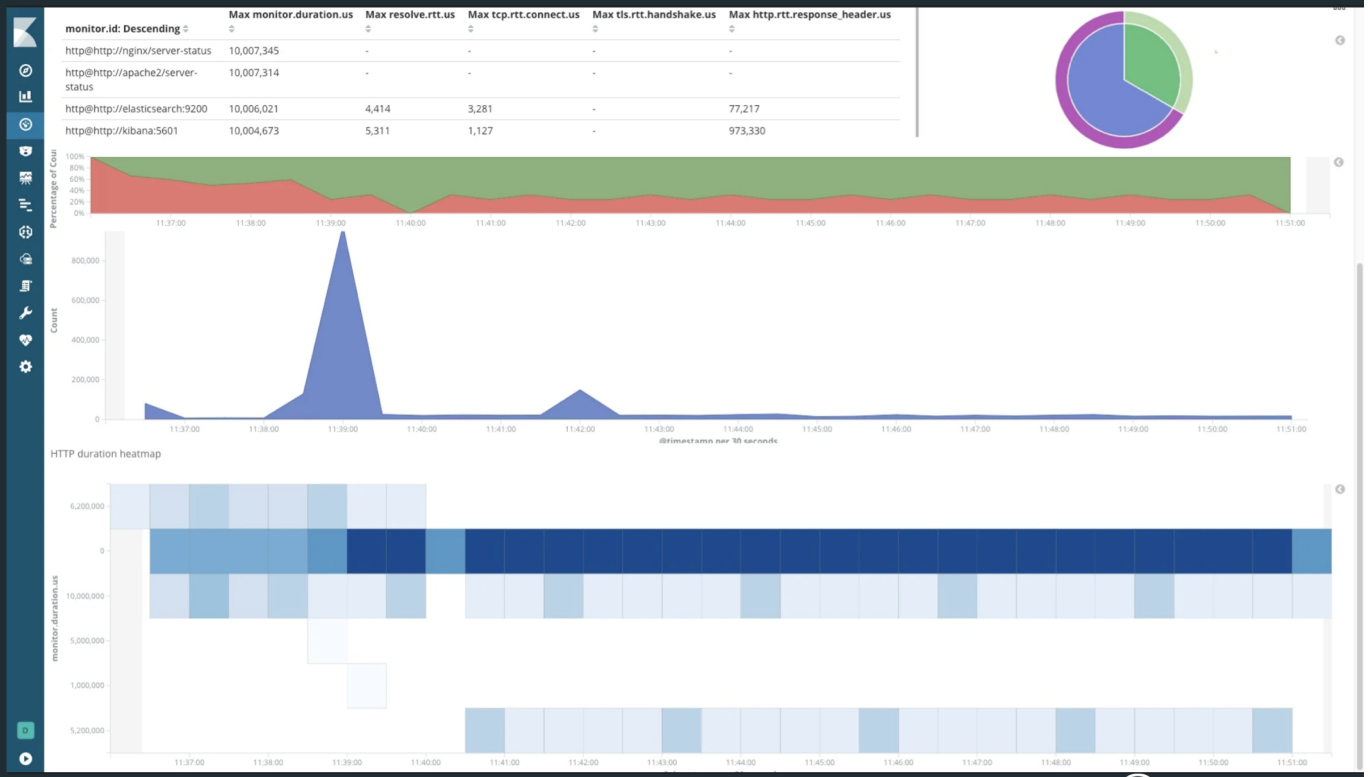
elastic

Uptime monitoring

HEARTBEAT

Ping all the things via

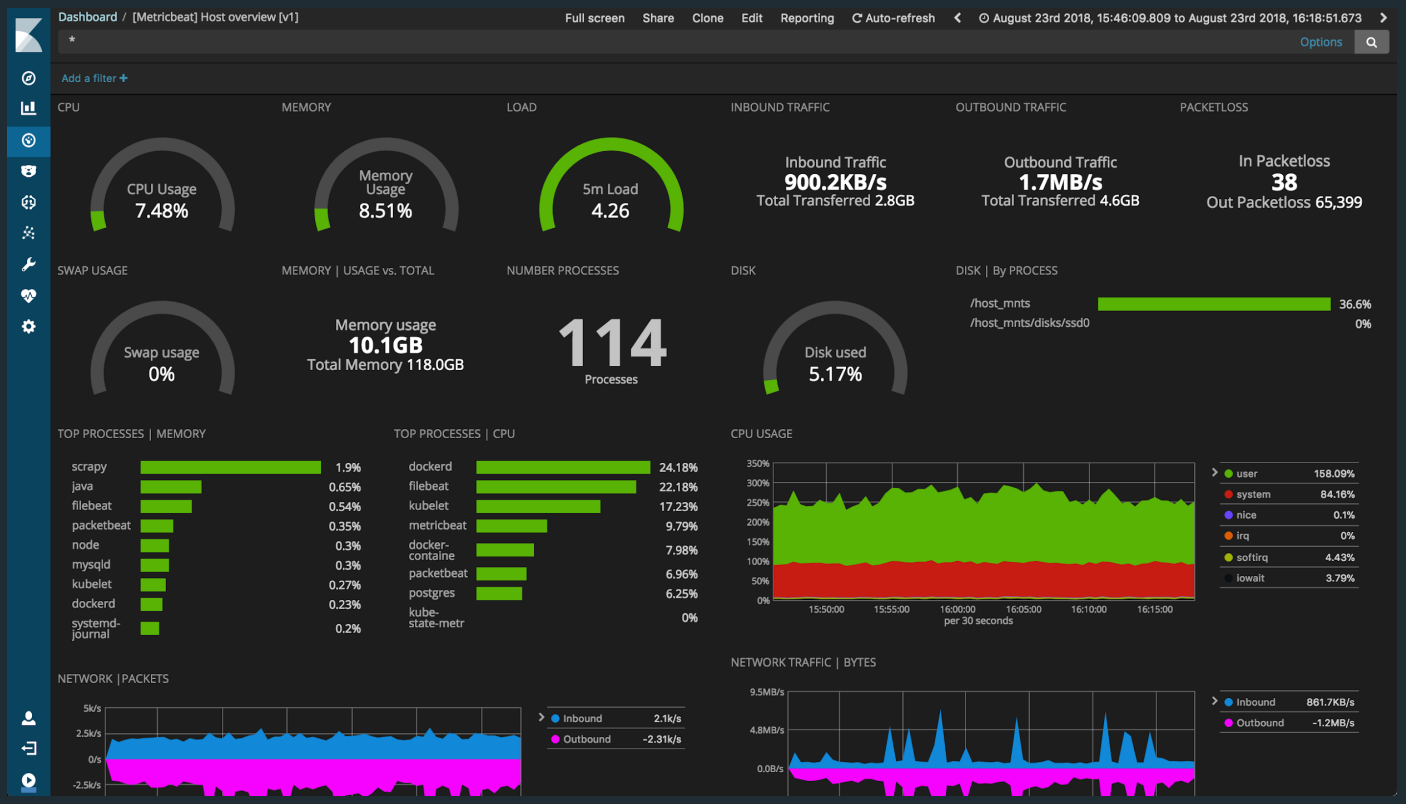
- ✓ ICMP
- ✓ TCP
- ✓ HTTP



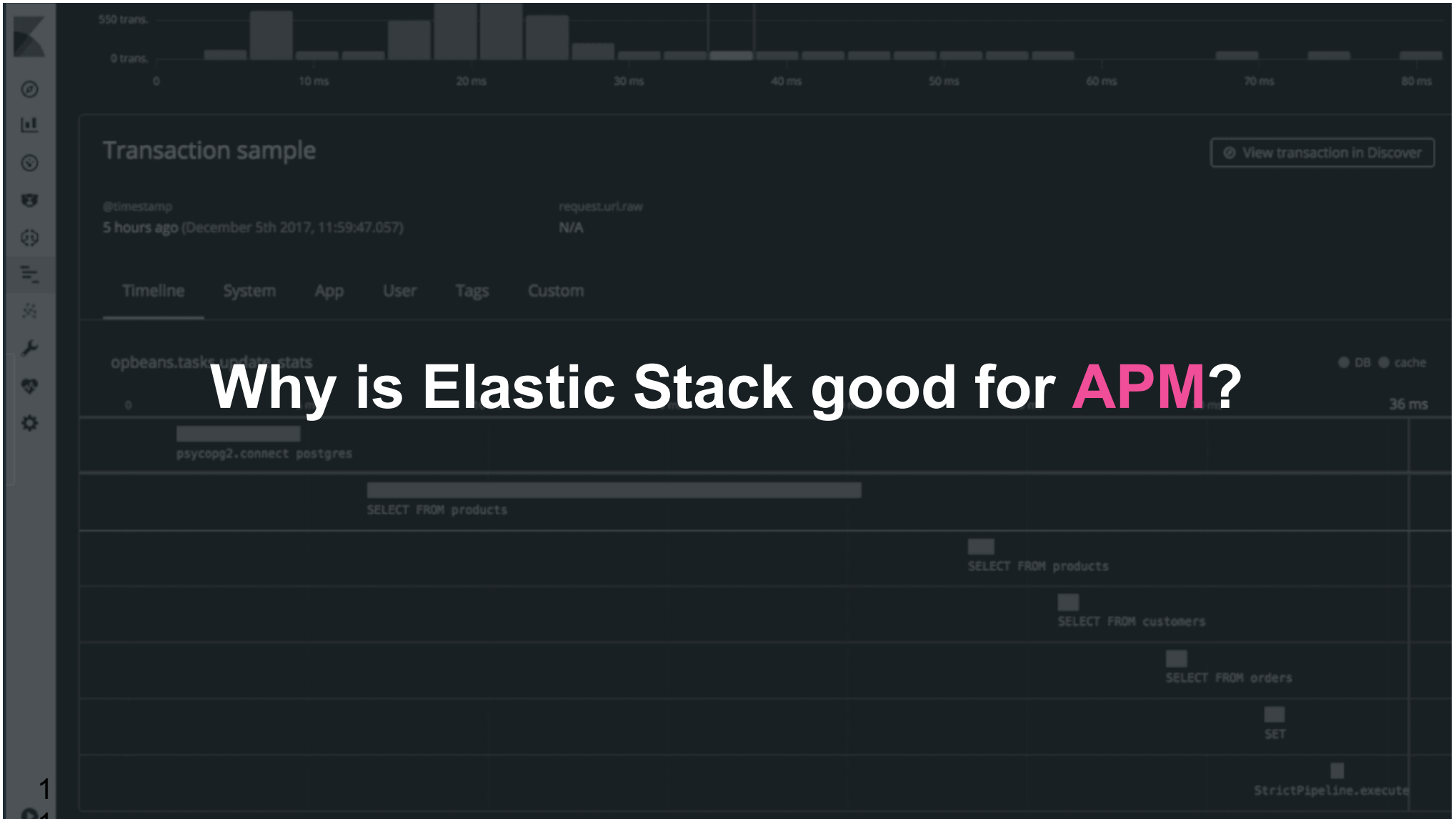
elastic

Visualizing time series data

Time Series Visual Builder



elastic

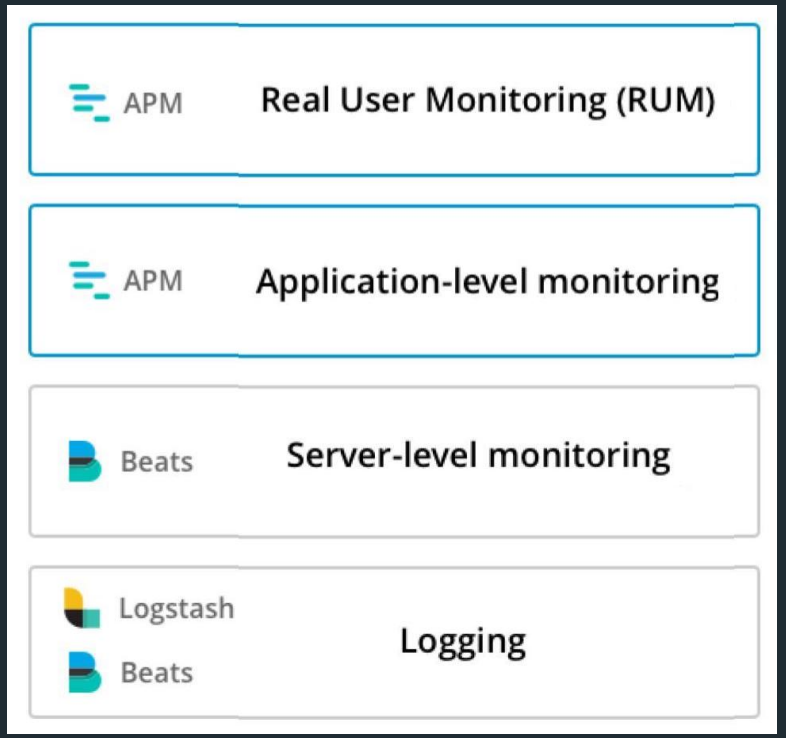


Why is Elastic Stack good for APM?

Elastic APM

APM adds end-user experience and application-level monitoring to the stack

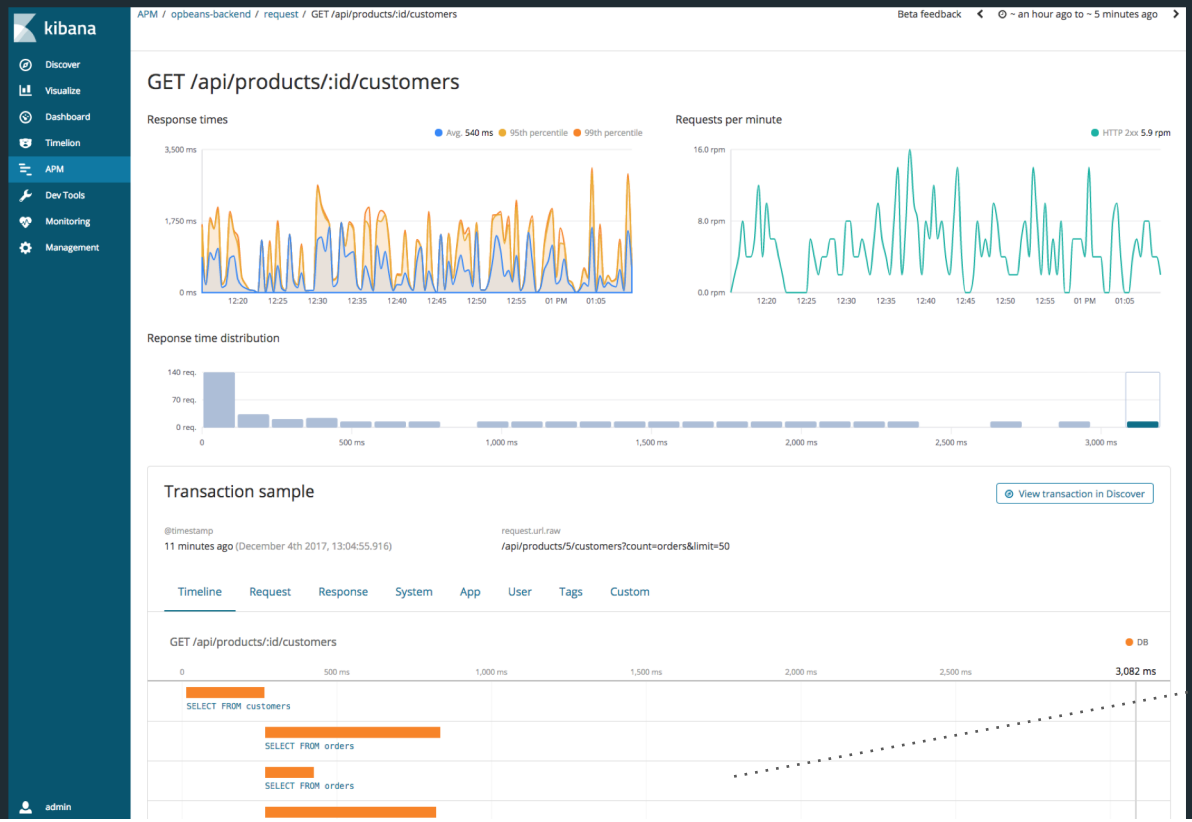
- Open-source alternative to traditional APM tools
- **APM agents** run with your application and instrument your code
- Language Support: Python, Node.js, Ruby, Java (Beta), Go (Beta), RUM (Real User Monitoring)

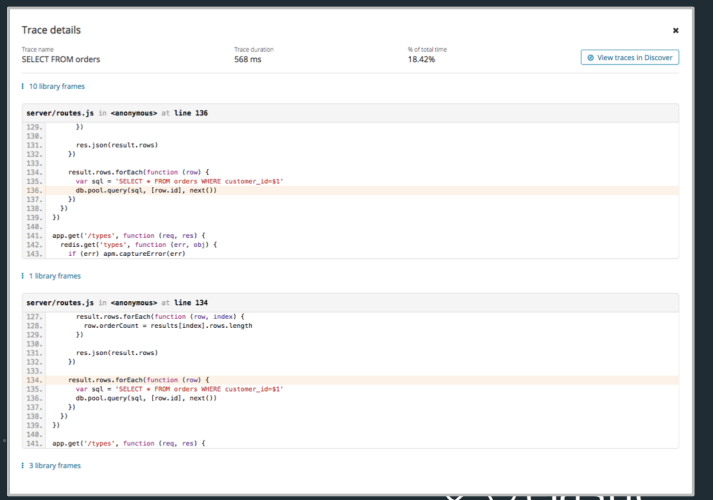


elastic

Dedicated APM UI

Great overview and drill-down with industry-standard visualizations

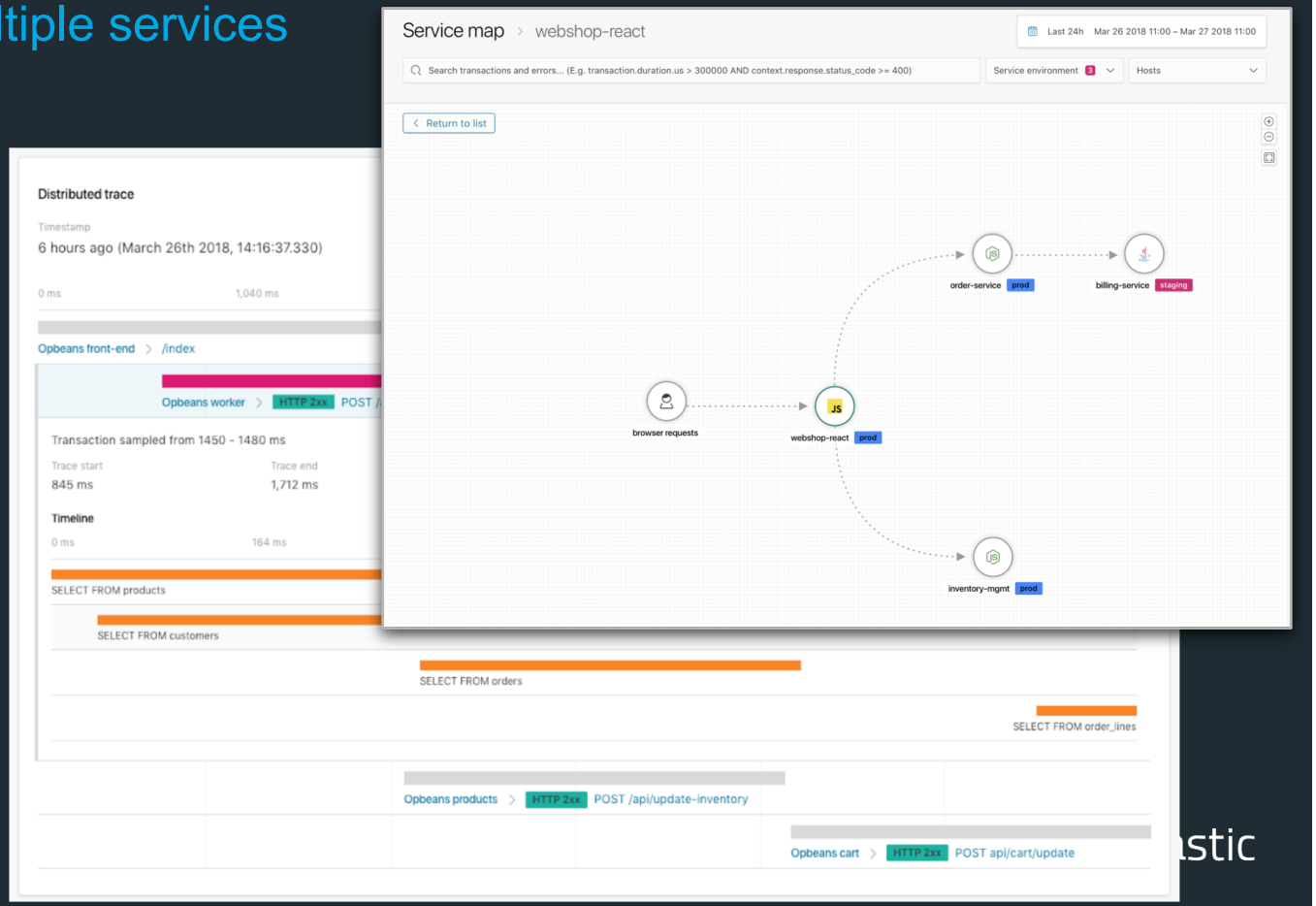




Roadmap: Distributed Tracing

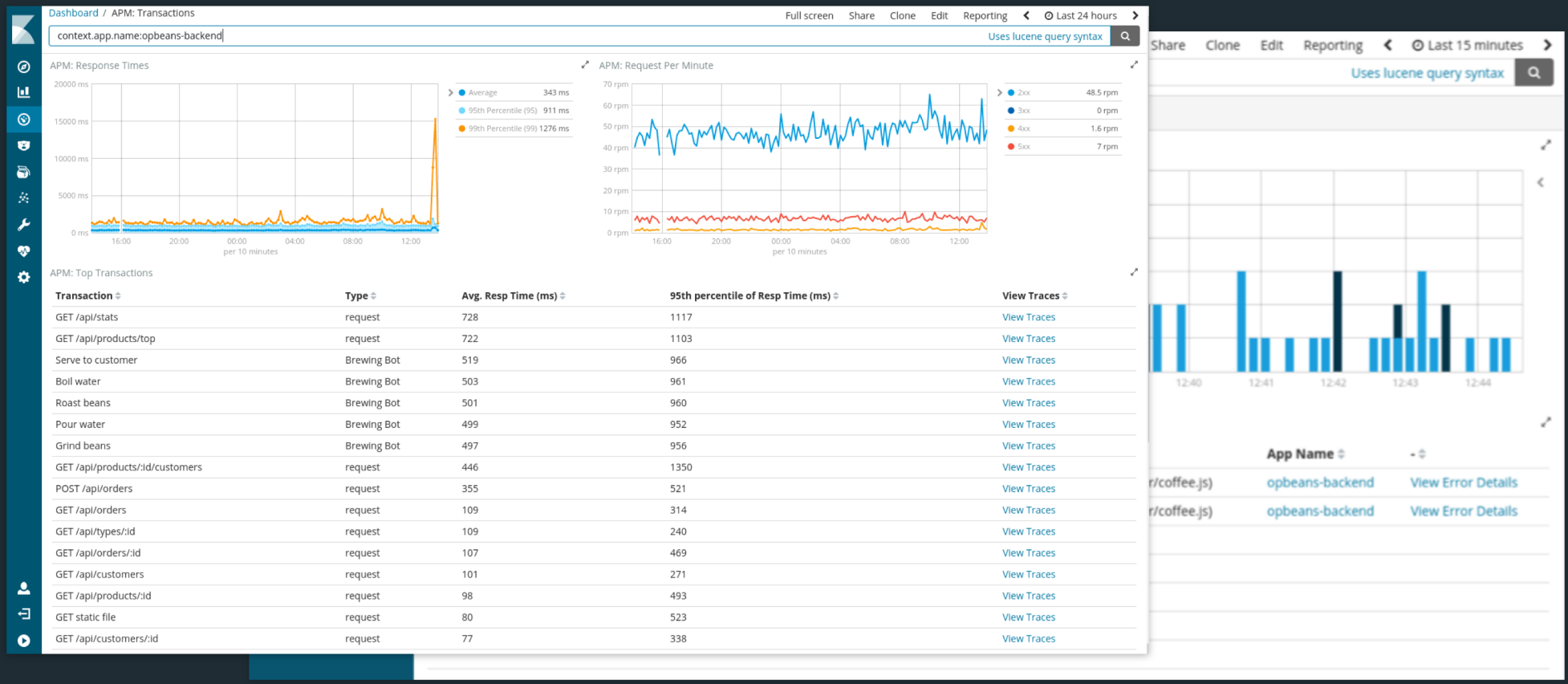
Trace and map across multiple services

- See the end-to-end view and navigate to individual transactions
- Based on the notion of a end-to-end **Trace ID** across services
- **OpenTracing** support



APM is just another index in Elasticsearch

Need another visualization? Build a dashboard, no need to wait for your vendor



Correlation between logs, metrics, and APM

Elastic Common Schema

Benefits

- Correlate data from different sources
- Ability to re-use analysis content
- Ability to re-use Elastic-provided content

Status

- Version 0.1 published: github.com/elastic/ecs
- Working with internal groups to validate
- Community feedback welcome!

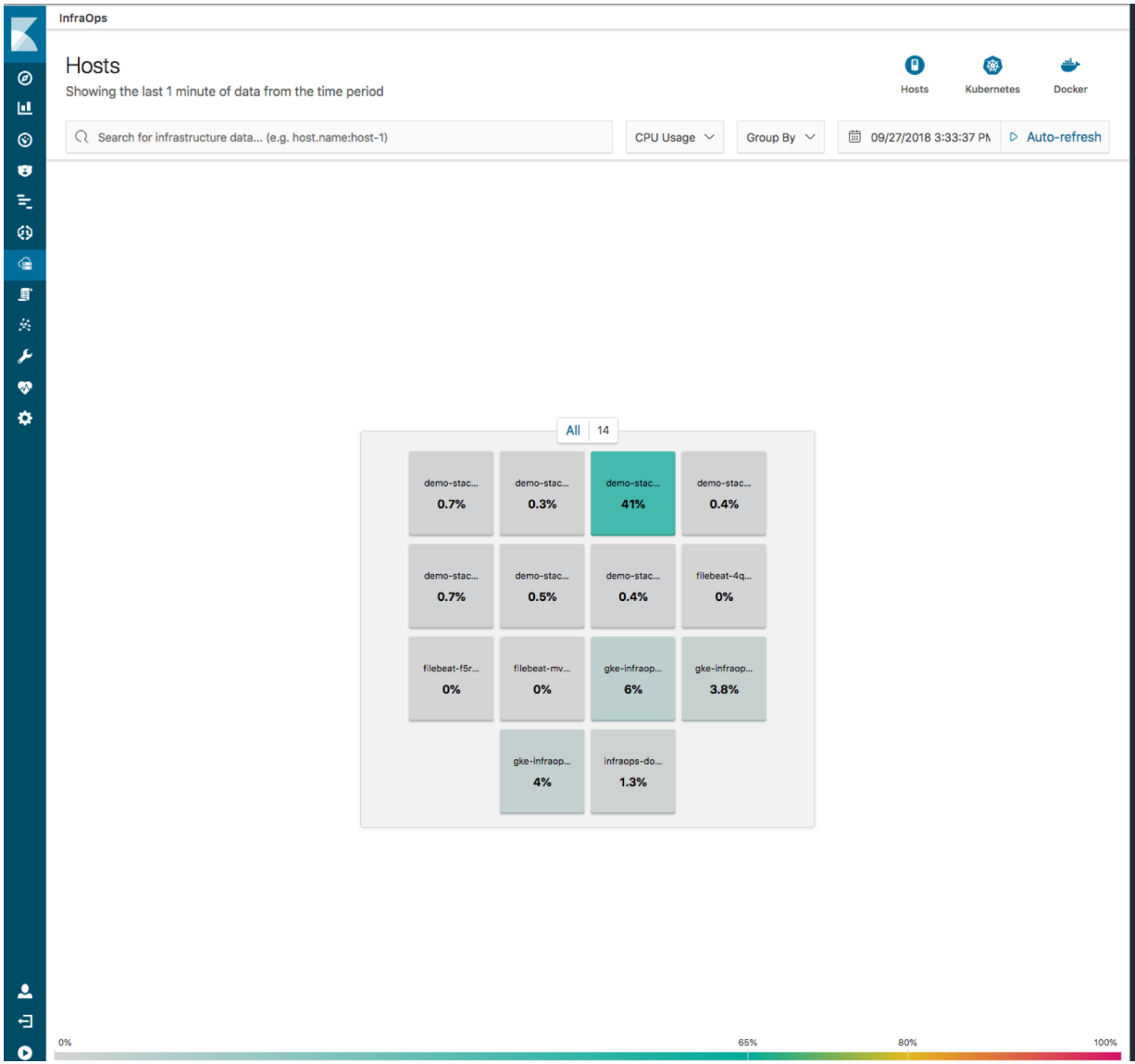
ECS Revision: 0.992 Group 1 Fields: 3 Group 2 Fields: 81

Group 1 (Must be populated)

@timestamp
ecs_version
message

Group 2 (Must be populated to the max extent practical where event message contains relevant fields.)

Event	Device	Host	Agent	Network	Source	Destination	Service	Resource
event.category	device.mac	host.mac	agent.id	network.protocol	source.mac	destination.mac	service.id	resource.type
event.type	device.timezone_offset	host.timezone_offset	agent.name	network.forwarded_ip	source.ip	destination.ip	service.name	resource.id
event.data_source_id	device.ip	host.ip	agent.version	network.inbound_bytes	source.hostname	destination.hostname	service.version	resource.file_name
event.module	device.network_interface	host.network_interface		network.inbound_packets	source.domain	destination.domain	service.type	resource.uri
event.organization_name	device.hostname	host.hostname		network.outbound_bytes	source.port	destination.subdomain	service.state	resource.url
event.organization_id	device.type	host.id		network.outbound_packets		destination.port	service.query	resource.path
event.id	device.vendor	host.type		network.total_bytes			service.response_code	resource.version
event.raw	device.product	host.sub_type		network.total_packets				resource.hash_value
event.hash	device.version	host.operating_system		network.direction				resource.hash_type
event.tags	device.serial_number	host.operating_system_version						
event.labels	device.action	host.provider						
event.duration	device.rule_set	host.availability_zone						
event.severity	device.event_id	host.region						
event.risk_score								

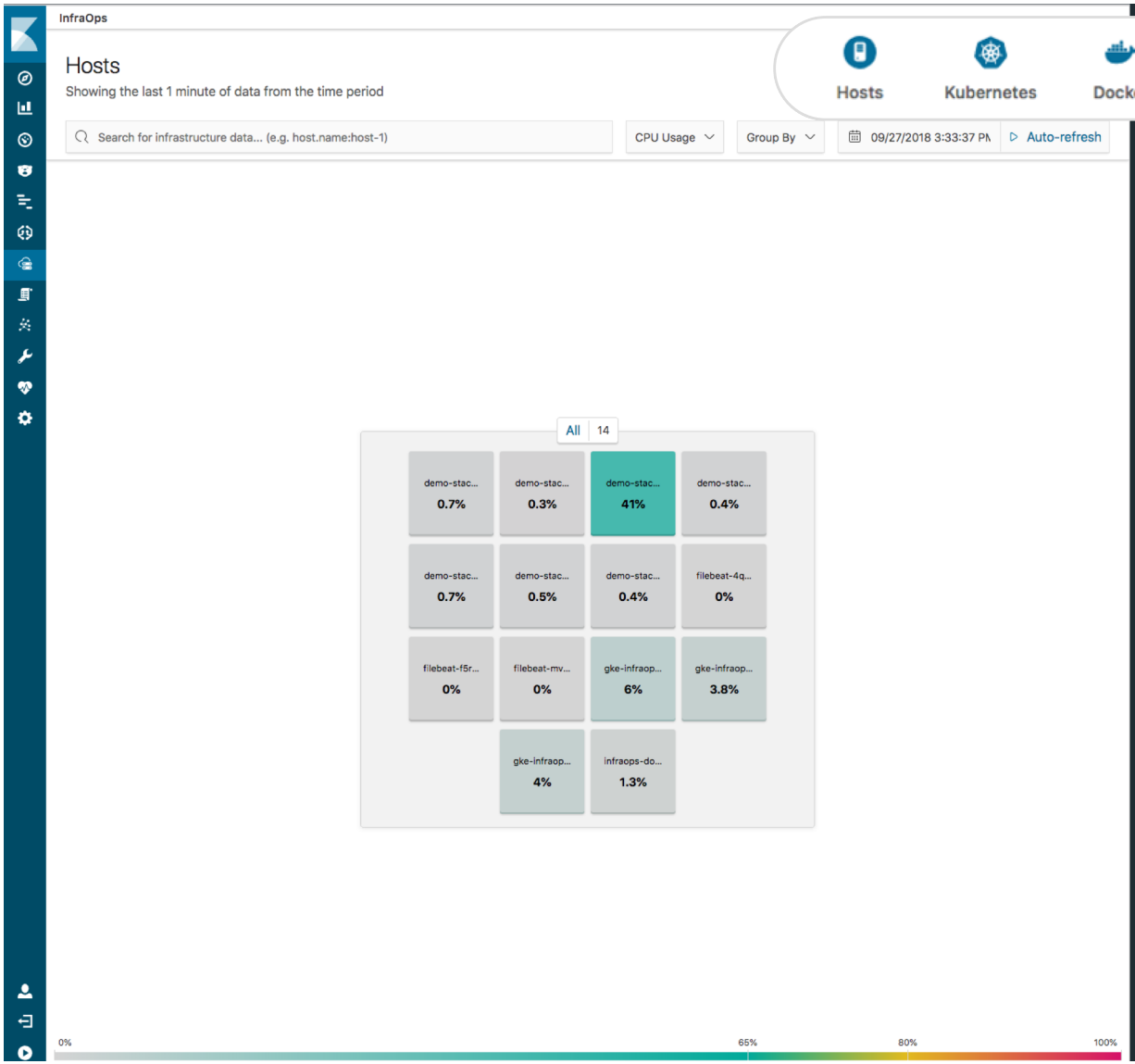


Coming in 6.5

Infrastructure UI

- Shows an overview of your **infrastructure**
- Correlates different types of operational data

elastic

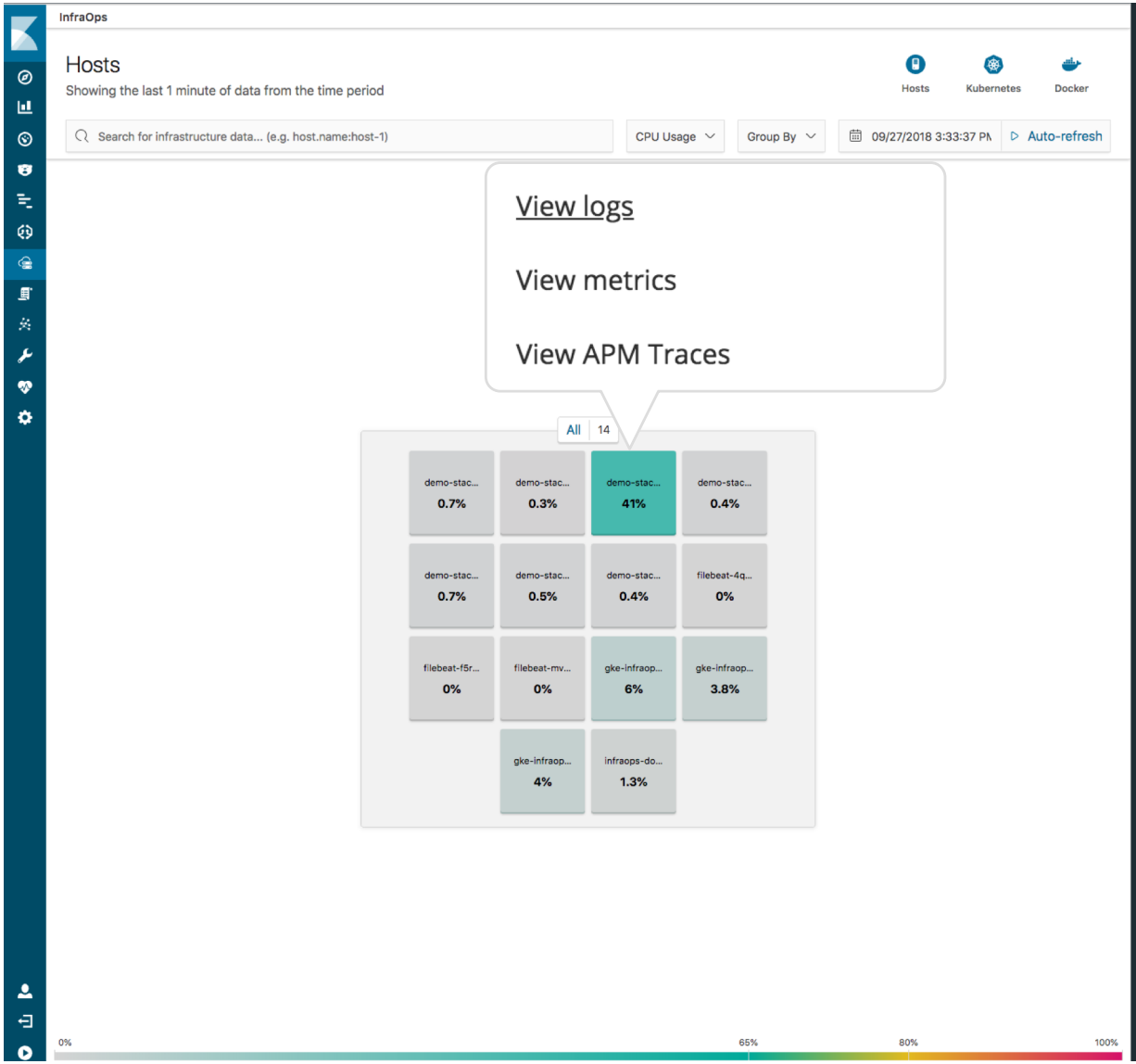


Coming in 6.5

Identity

- Your infrastructure is represented by the Waffle map
- Waffle map shows not only hosts, but also containers

elastic

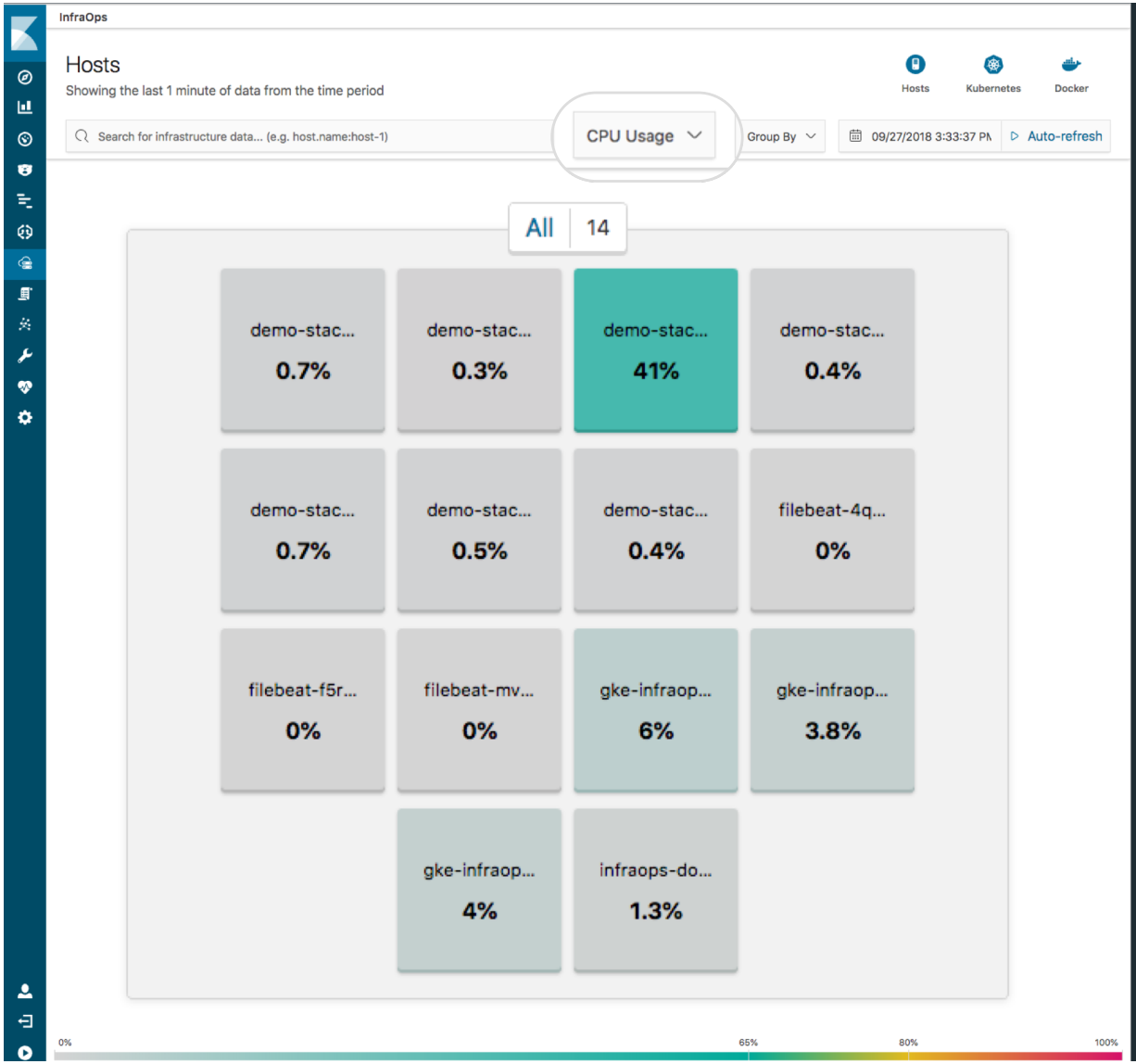


Coming in 6.5

Drill down

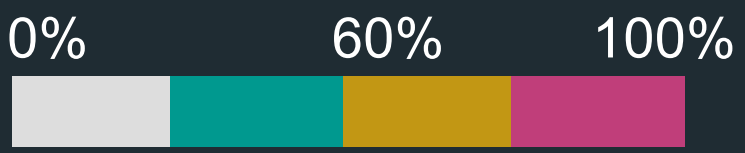
- Drill down to see logs in the Logs explorer, more metrics details or redirect to APM to see the traces

elastic



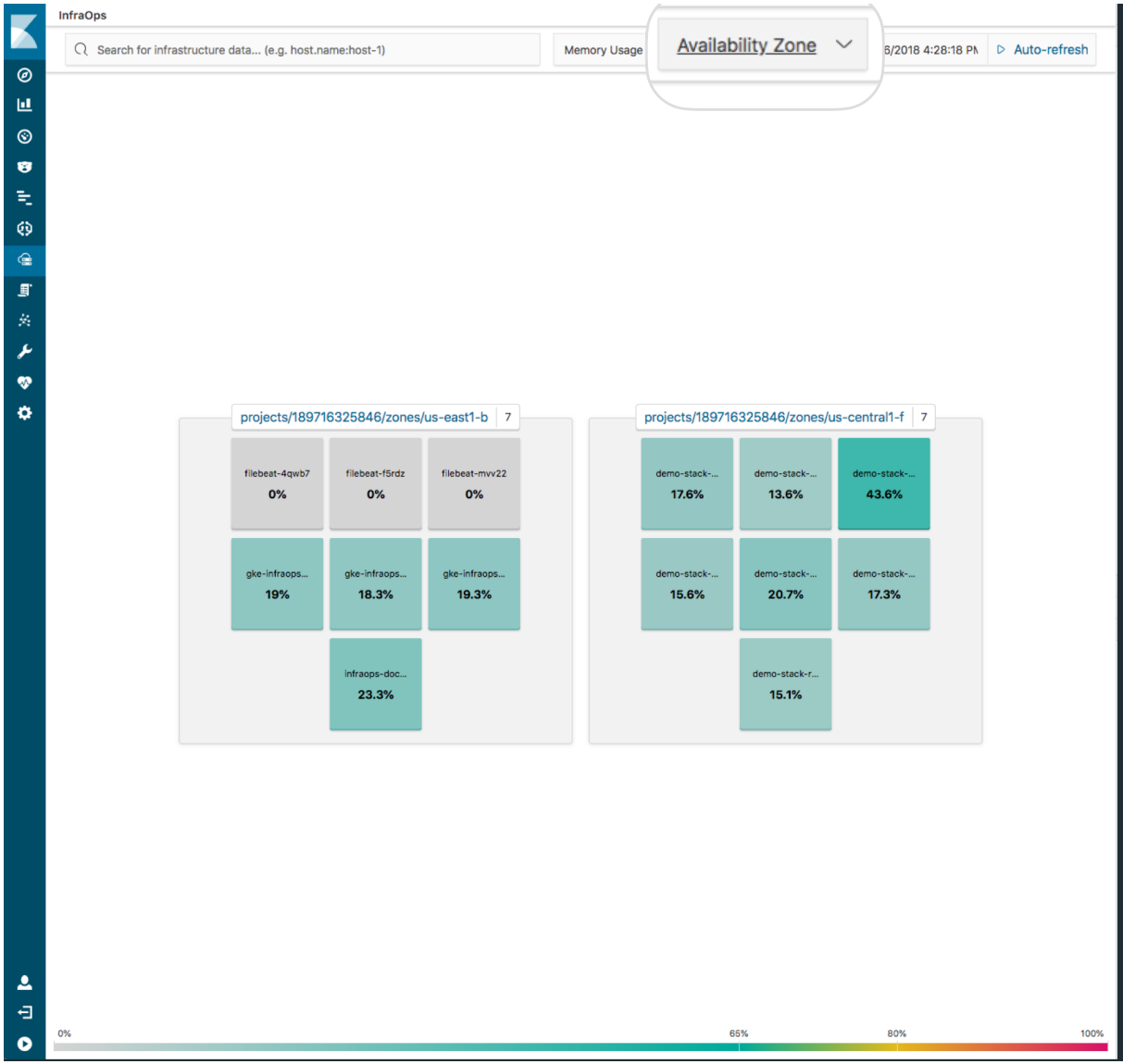
Coming in 6.5

Metric



- The color of each box depends on the associated metric (CPU Usage)

elastic

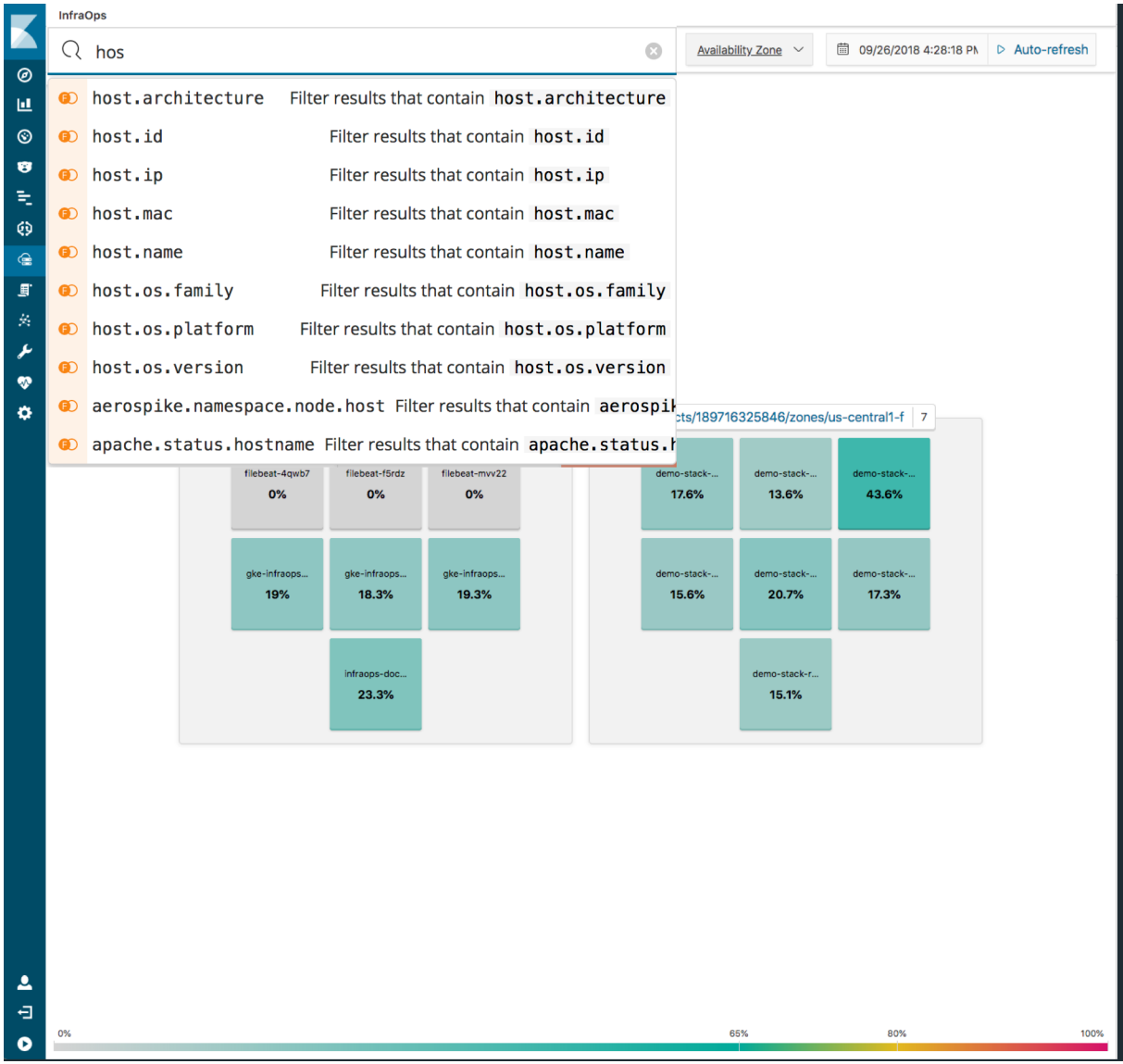


Coming in 6.5

Group by

- Group by your hosts or containers depending on your needs.
- For example group by:
  - Host
  - Availability zone
  - Machine Type
  - Namespace
  - Node

elastic

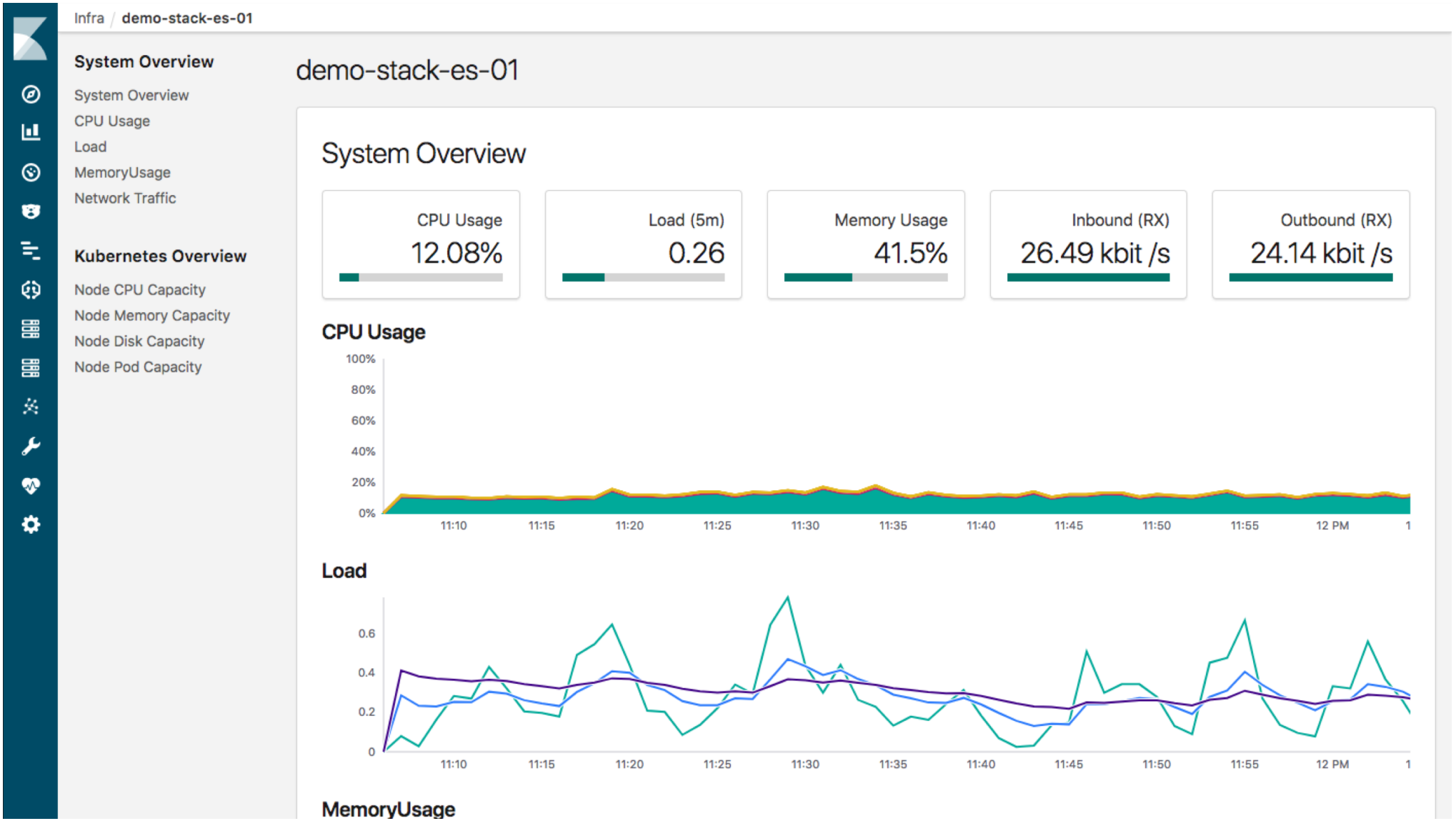


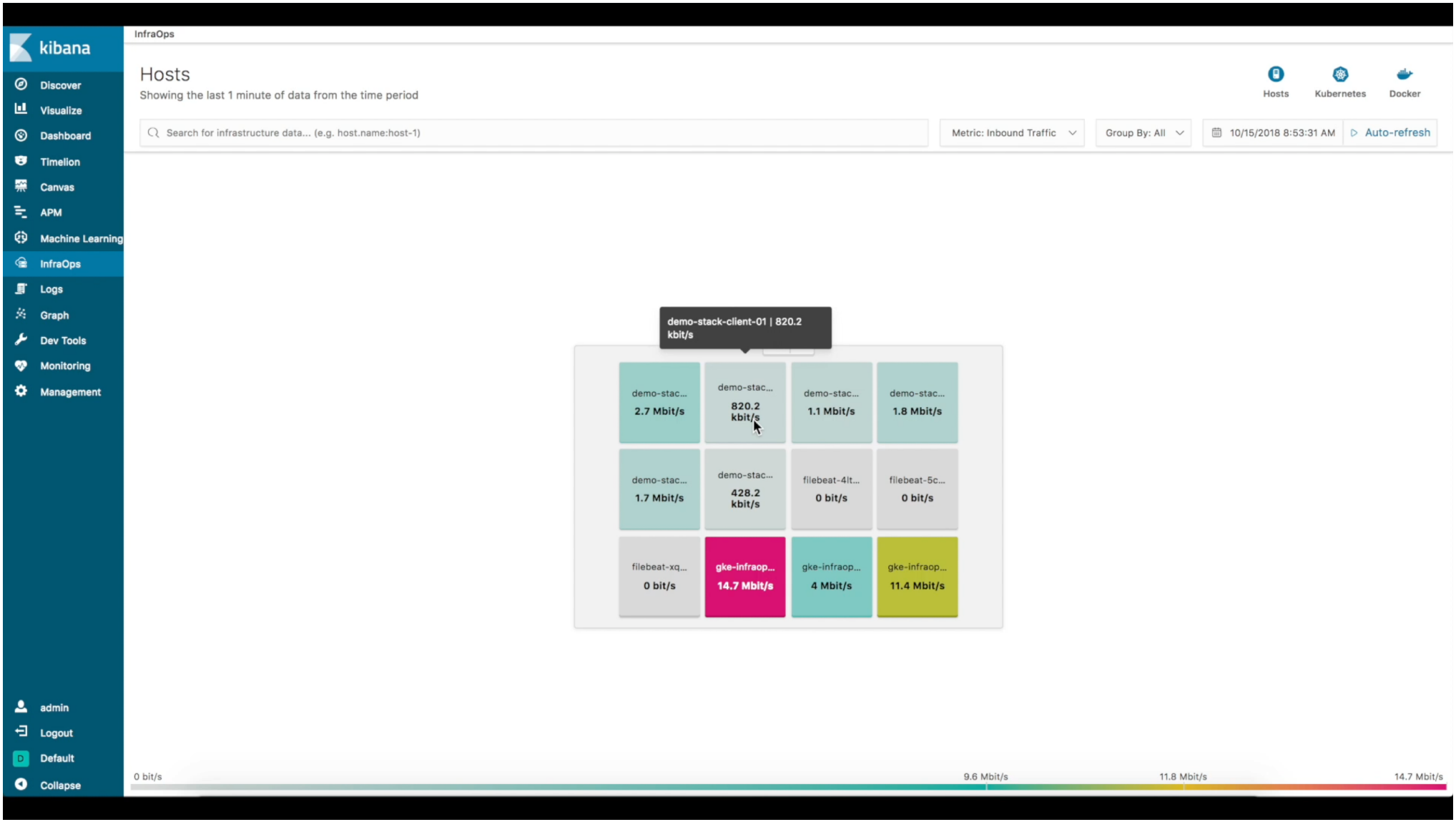
Coming in 6.5

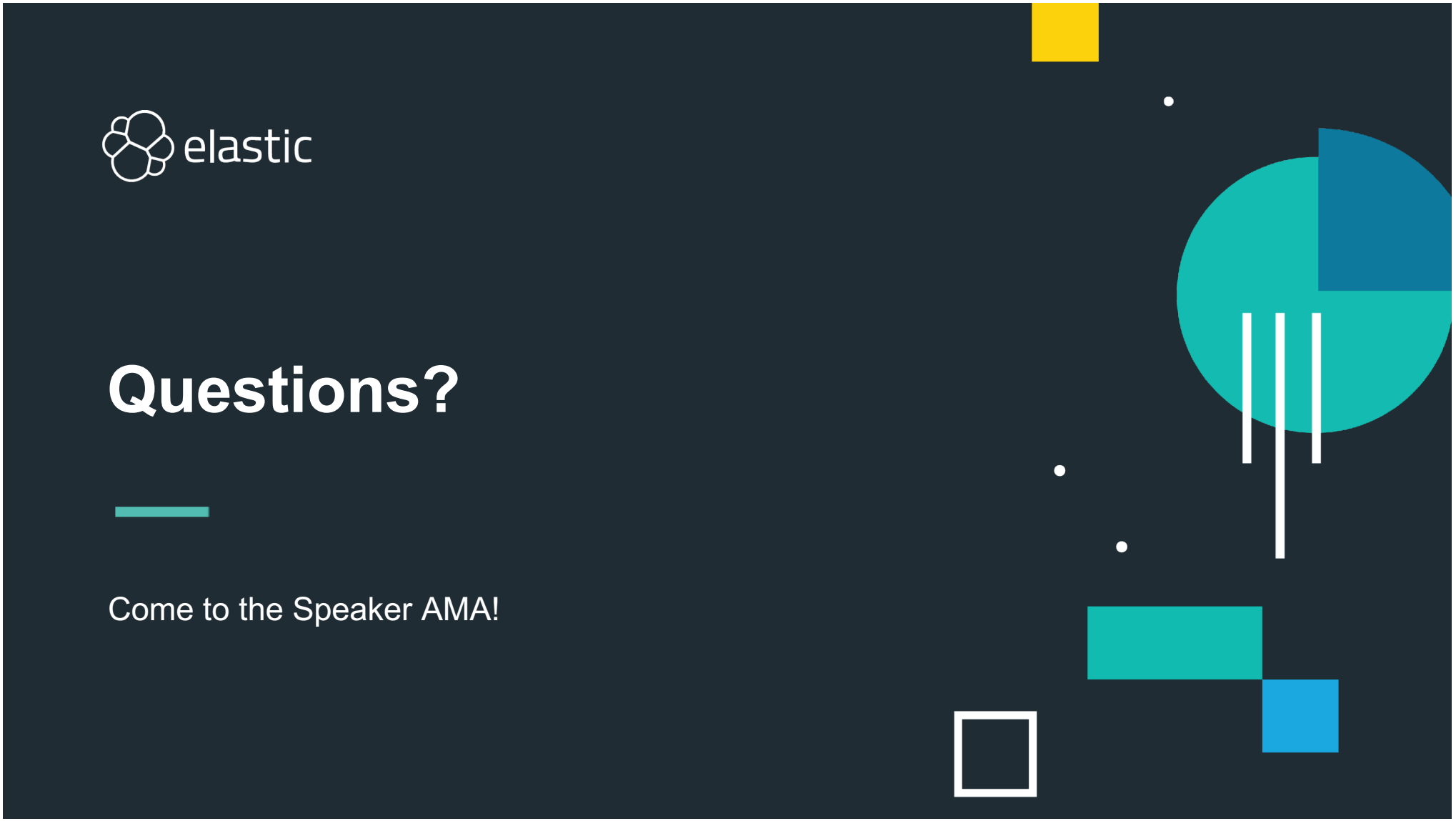
Search

Filter for the hosts, containers, pods that have a specific characteristic

elastic


Infra / demo-stack-es-01
System Overview
System Overview
CPU Usage
Load
MemoryUsage
Network Traffic
Kubernetes Overview
Node CPU Capacity
Node Memory Capacity
Node Disk Capacity
Node Pod Capacity
demo-stack-es-01
System Overview
CPU Usage
12.08%
Load (5m)
0.26
Memory Usage
41.5%
Inbound (RX)
26.49 kbit /s
Outbound (RX)
24.14 kbit /s
CPU Usage
100%
80%
60%
40%
20%
0%
11:10
11:15
11:20
11:25
11:30
11:35
11:40
11:45
11:50
11:55
12 PM
Load
0.6
0.4
0.2
0
11:10
11:15
11:20
11:25
11:30
11:35
11:40
11:45
11:50
11:55
12 PM
MemoryUsage


kibana
Discover
Visualize
Dashboard
Timelion
Canvas
APM
Machine Learning
InfraOps
Logs
Graph
Dev Tools
Monitoring
Management
admin
Logout
Default
Collapse
InfraOps
Hosts
Showing the last 1 minute of data from the time period
Hosts
Kubernetes
Docker
Search for infrastructure data... (e.g. host.name:host-1)
Metric: Inbound Traffic
Group By: All
10/15/2018 8:53:31 AM
Auto-refresh
demo-stack-client-01 | 820.2 kbit/s
demo-stac... 2.7 Mbit/s
demo-stac... 820.2 kbit/s
demo-stac... 1.1 Mbit/s
demo-stac... 1.8 Mbit/s
demo-stac... 1.7 Mbit/s
demo-stac... 428.2 kbit/s
filebeat-4lt... 0 bit/s
filebeat-5c... 0 bit/s
filebeat-xq... 0 bit/s
gke-infraop... 14.7 Mbit/s
gke-infraop... 4 Mbit/s
gke-infraop... 11.4 Mbit/s
0 bit/s
9.6 Mbit/s
11.8 Mbit/s
14.7 Mbit/s


elastic
Questions?
Come to the Speaker AMA!



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