

卓越运维三连击
日志 指标 APM

杰瑞朱 = Jerry (朱杰)
Elastic 架构师



Elastic是 ELK背后的公司

- **10万+** 全球社区参与者
  1万+ 中国社区参与者
- **3.5亿+** 下载 (持续增长中)
- **1680+** 员工
- **8800+** 付费订阅客户
- **NYSE: ESTC**



elastic

Elastic 产品生态



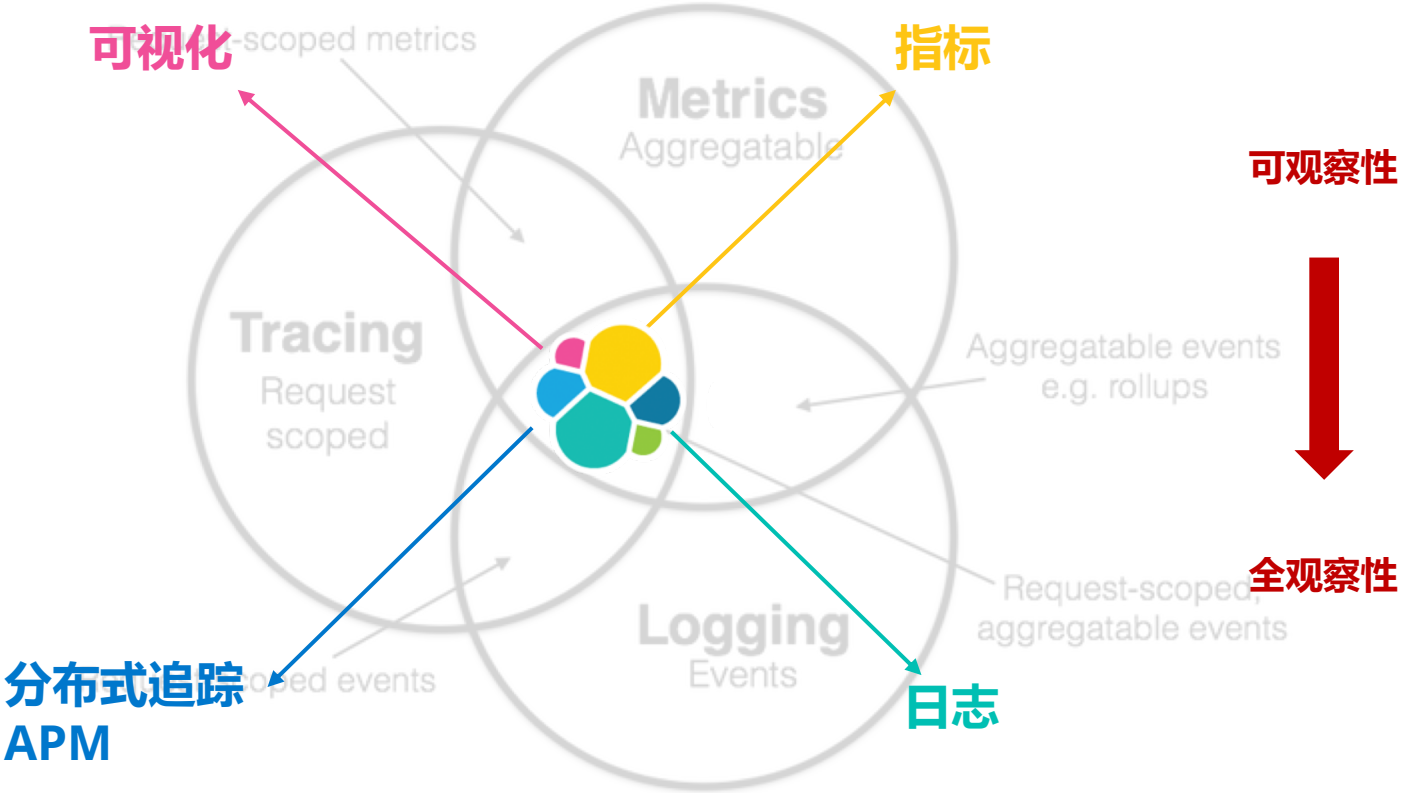
elastic



日志 + 指标 + APM融入同一个技术栈

Why?

日志仅仅是起点 – 终点是全方位的可观察性



elastic


Talk is cheap.
Show me the code.
Linus Torvalds
quotefancy

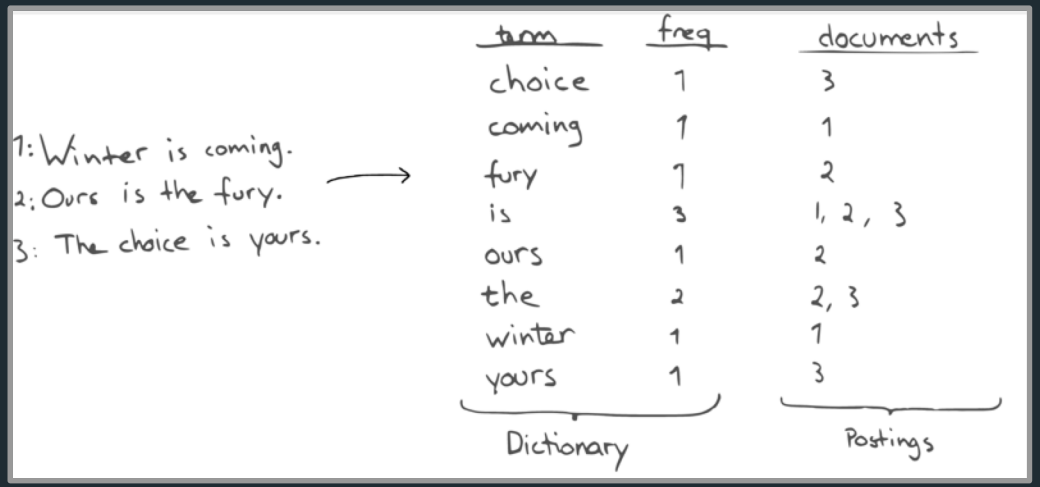
Lucene & Elasticsearch
付出的努力

elastic

在 Elasticsearch 初期

它主要为应用提供搜索功能

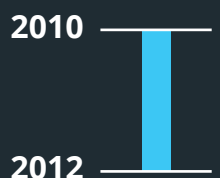
2010 —— **搜索引擎**
Inverted index primary data structure, and is great for search



Elasticsearch 进化到分析支持

基于Lucene 的 "doc values"构建的列存储

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



搜索引擎
Inverted index primary data structure, and is great for search

列存储
Structured data storage, resulting in compact storage and faster analytics

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

聚合框架

不仅仅是聚合功能

```
{
    "_index": "helioweb",
    "_type": "voyager1",
    "_id": "1977-257",
    "_score": 1,
    "_source": {
        "seLon": 353.8,
        "objectName": "voyager1",
        "seLat": 0.2,
        "year": 1977,
        "date": "1977-09-14T10:28:25.178Z",
        "radAU": 1.02,
        "dayOfYear": 257
    }
}
```

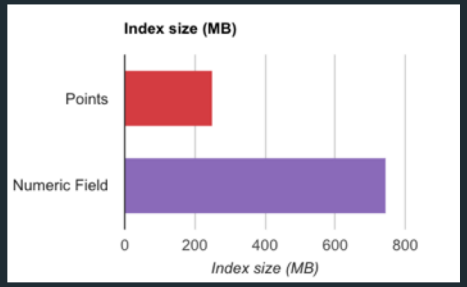


https://www.elastic.co/blog/out-of-this-world-aggregations

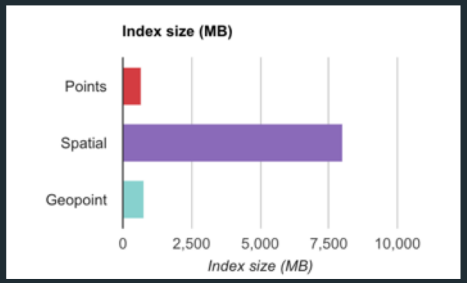
Elasticsearch 存储效率增强

BKD Trees & Sparse Fields

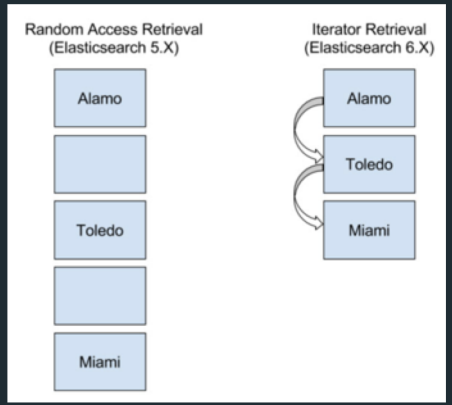
1-维数据



2-维数据



稀疏数据



2010 — **搜索引擎**
Inverted index primary data structure, and is great for search

2012 — **列存储**
Structured data storage, resulting in compact storage and faster analytics

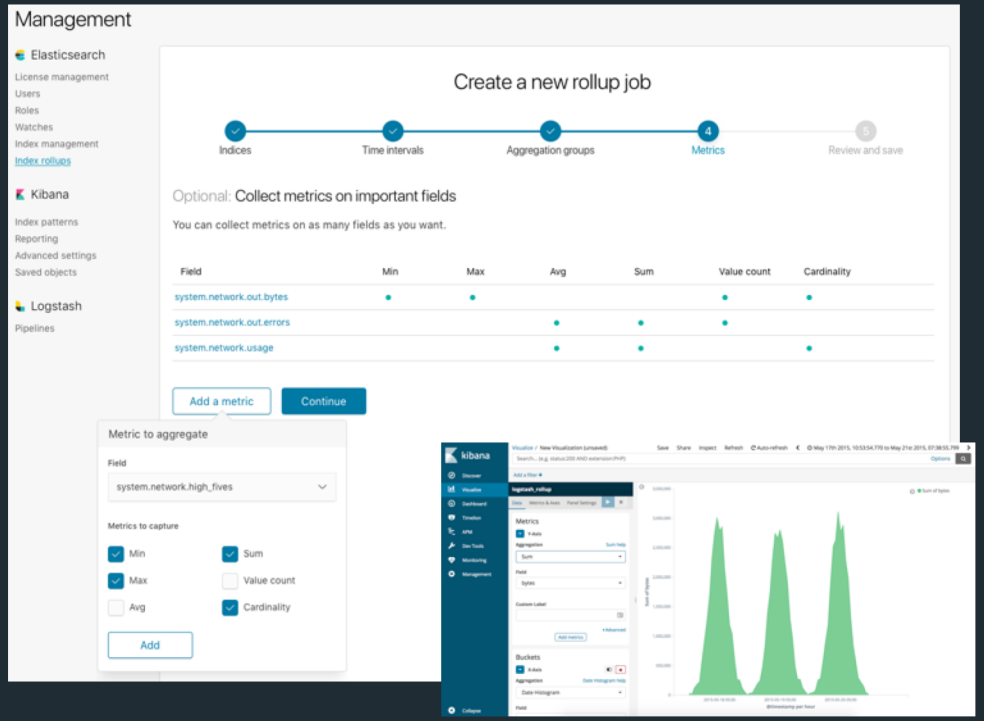
2014 — **聚合框架**
Analytics features to slice and dice data along various dimensions

2016 — **BKD树和稀疏数据**
Data structures optimized for numbers. Faster analytics, lower storage footprint

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

Rollup支持长期保留

在Elasticsearch 6.3中加入



2010 — **搜索引擎**
Inverted index primary data structure, and is great for search

2012 — **列存储**
Structured data storage, resulting in compact storage and faster analytics

2014 — **聚合框架**
Analytics features to slice and dice data along various dimensions

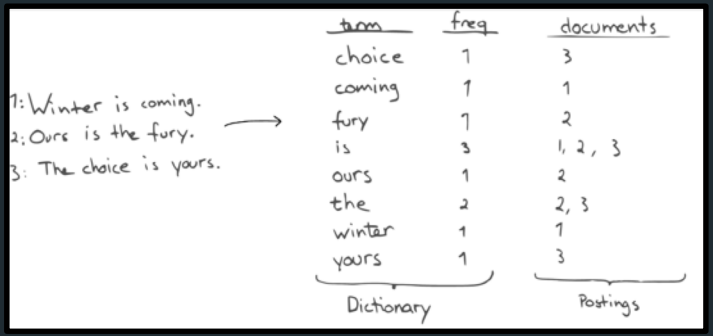
2016 — **BKD数据和稀疏数据**
Data structures optimized for numbers. Faster analytics, lower storage footprint

2018 — **Rollups**
Roll up or aggregate older data into bigger time buckets and save on disk space

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

Elasticsearch 用于搜索和数值分析

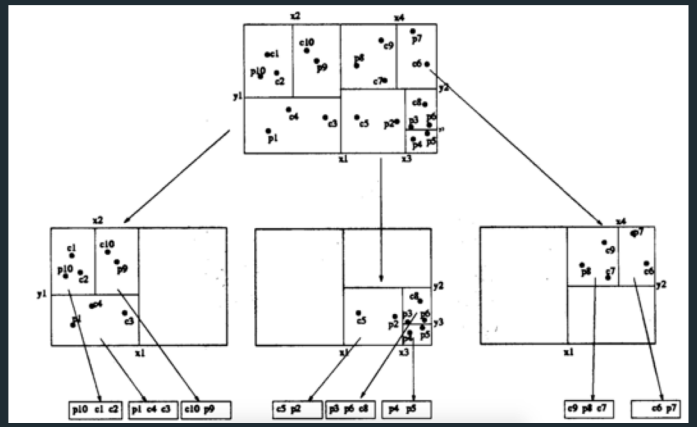
倒排序支持的全文搜索



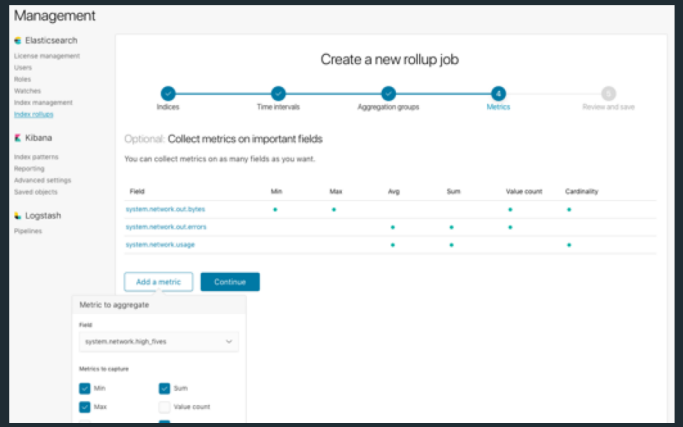
列存储支持的结构化数据

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

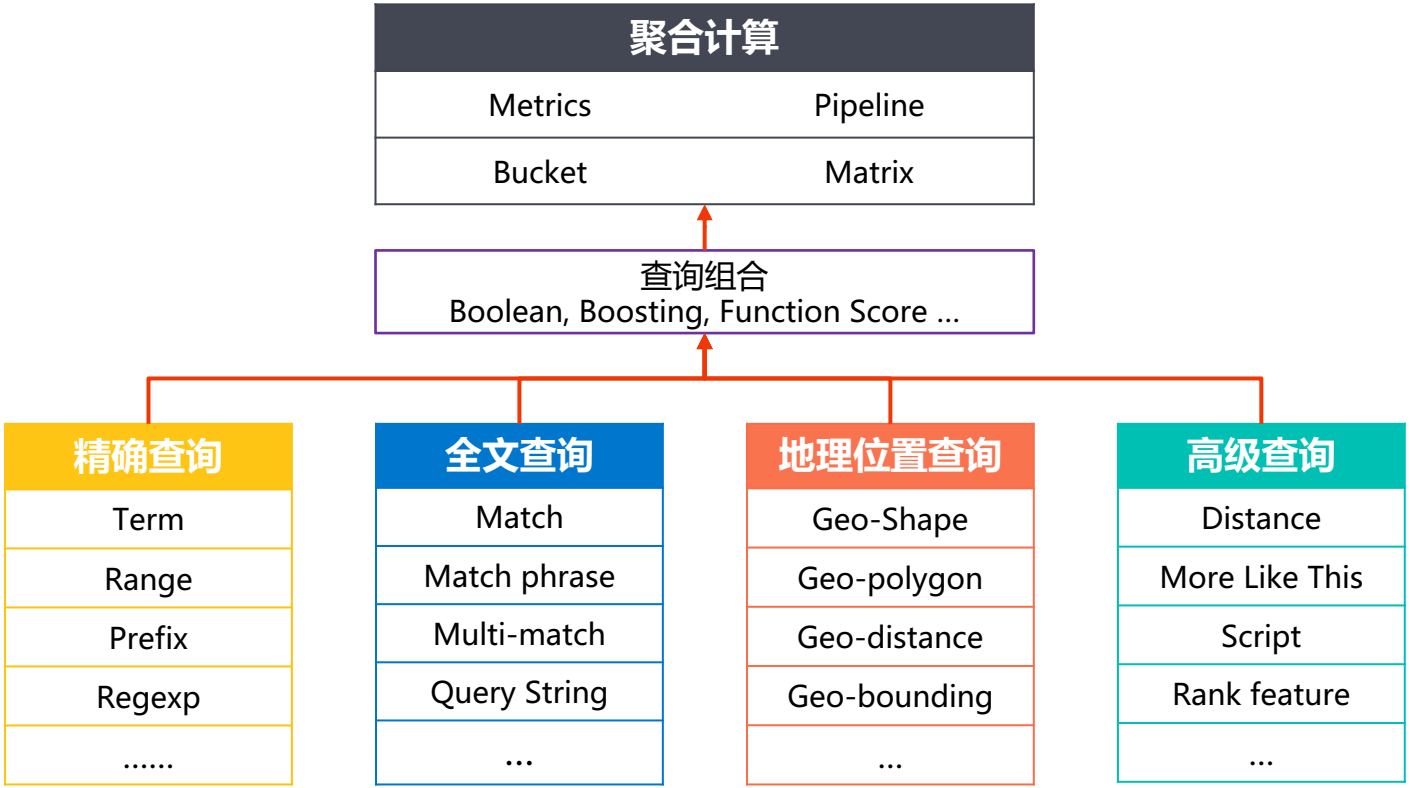
BKD数支持的数值型运算



Rollup 节省存储空间



查询能力变得空前强大



elastic

2019

Data Frames

未来…

Beats Logstash
付出的努力

elastic

日志、指标采集 Beats生态

libbeat



插件

FILEBEAT
日志文件



插件

METRICBEAT
指标数据



PACKETBEAT
网络数据



FUNCTIONBEAT
云服务器监控



WINLOGBEAT
Window日志



HEARTBEAT
服务可用性监控



AUDITBEAT
Linux审核框架事件

httpbeat

apachebeat

nginxbeat

pingbeat

execbeat

dockerbeat

elasticbeat

70+
社区制造

elastic

日志、指标采集 Logstash生态



Logstash

200+ 插件

azure event hub	cloudwatch	couchdb	elasticsearch	exec
file	websocket	tcp	upd	graphite
http	http poller	imap	irc	java generator
java stdin	jdbc	jms	jmx	kafka
log4j	xmpp	redis	rss	s3
snmp	sqlite	stdin	syslog	github

更多
社区制造

elastic

开放生态 第三方重磅工具









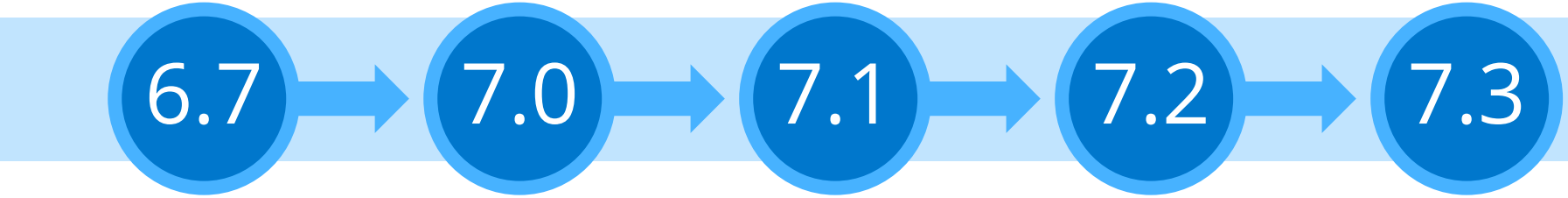




Kibana
付出的努力

elastic

产品快速迭代



elastic

以前的
Elastic Stack

一流的引擎！
三流的界面！

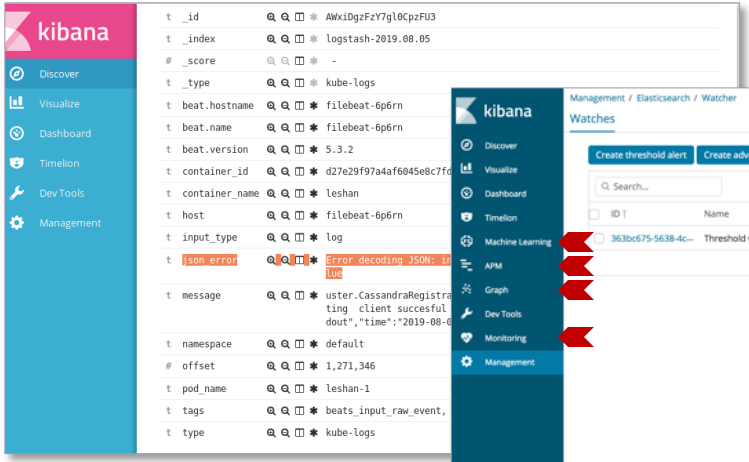
现在的
Elastic Stack

一流的引擎！
一流的界面！

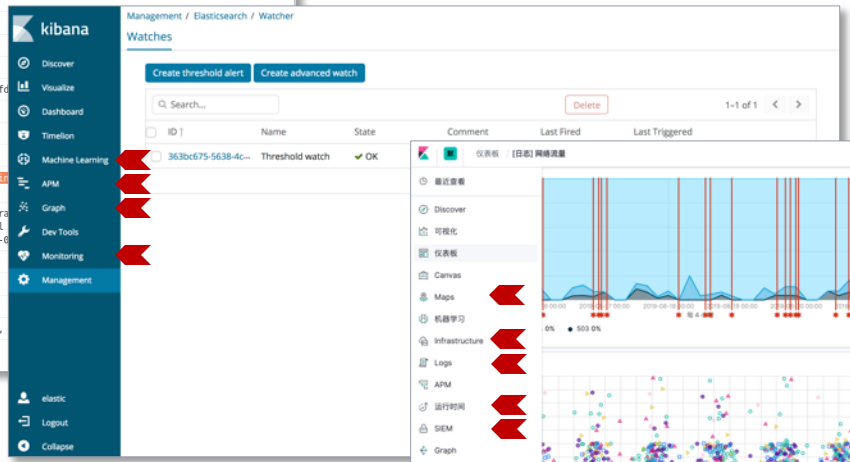
elastic

快速改进

Kibana 5.5



Kibana 6.5

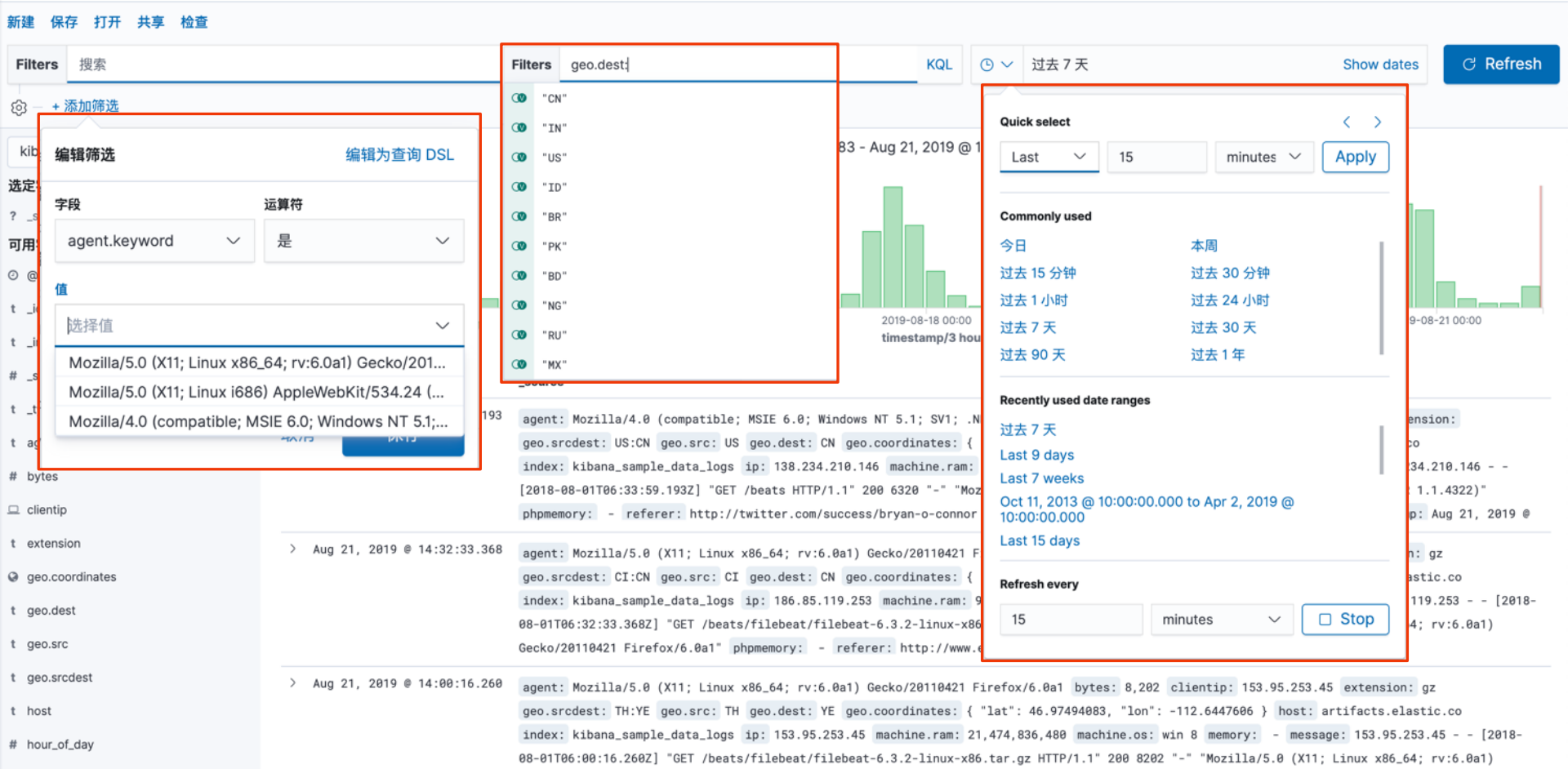


Kibana 7.3

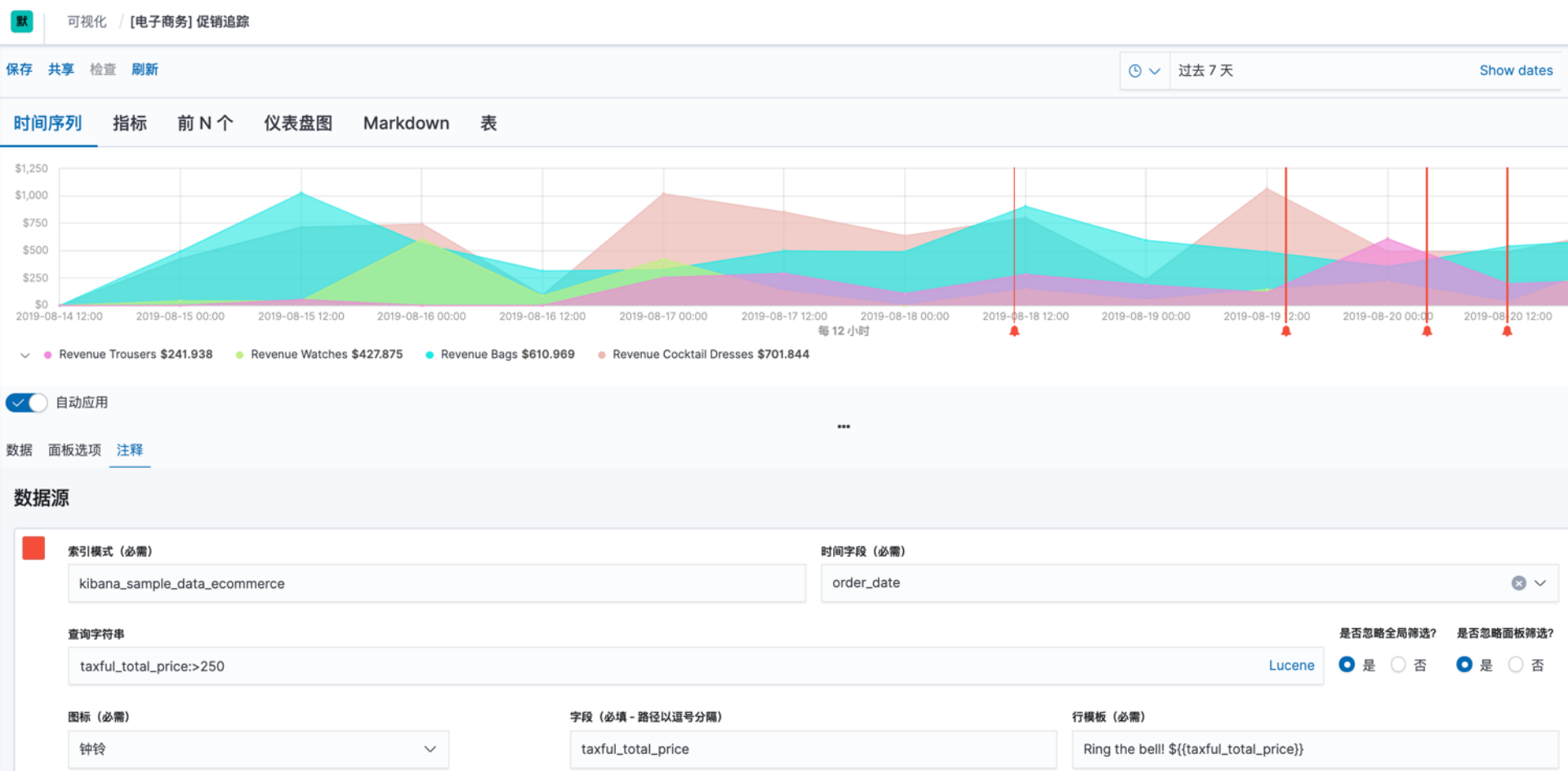


elastic

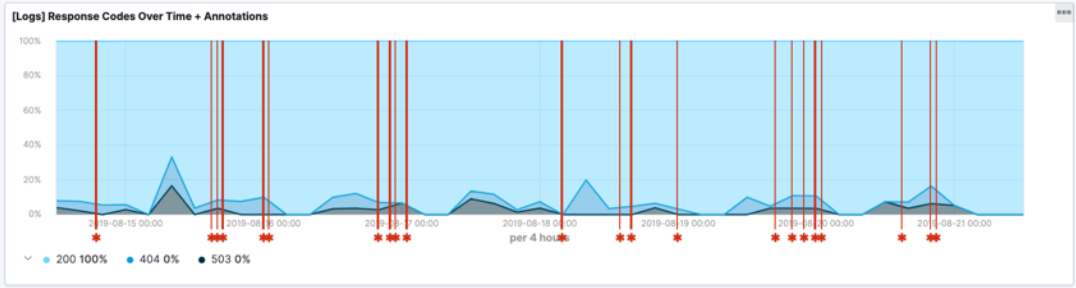
数据展现 – 日志分析

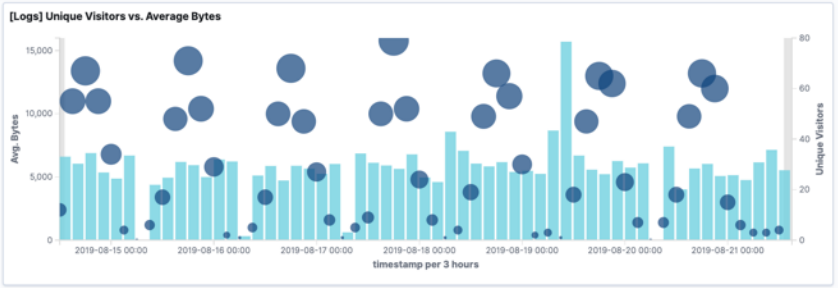

新建 保存 打开 共享 检查
Filters 搜索
+ 添加筛选
编辑筛选
编辑为查询 DSL
字段
运算符
agent.keyword
是
值
选择值
Mozilla/5.0 (X11; Linux x86_64; rv:6.0a1) Gecko/201...
Mozilla/5.0 (X11; Linux i686) AppleWebKit/534.24 (...
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;...
Filters geo.dest:
KQL
"CN"
"IN"
"US"
"ID"
"BR"
"PK"
"BD"
"NG"
"RU"
"MX"
过去 7 天
Show dates
Refresh
Quick select
Last
15
minutes
Apply
Commonly used
今日
本周
过去 15 分钟
过去 30 分钟
过去 1 小时
过去 24 小时
过去 7 天
过去 30 天
过去 90 天
过去 1 年
Recently used date ranges
过去 7 天
Last 9 days
Last 7 weeks
Oct 11, 2013 @ 10:00:00.000 to Apr 2, 2019 @ 10:00:00.000
Last 15 days
Refresh every
15
minutes
Stop
2019-08-18 00:00
timestamp/3 hou
bytes
clientip
extension
geo.coordinates
geo.dest
geo.src
geo.srcdest
host
hour_of_day
Aug 21, 2019 @ 14:32:33.368
Aug 21, 2019 @ 14:00:16.260

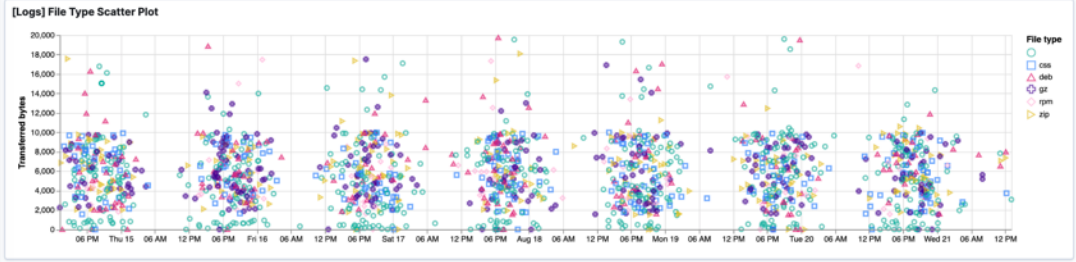
数据展现 - 时序数据分析器



数据展现 – 丰富的图表

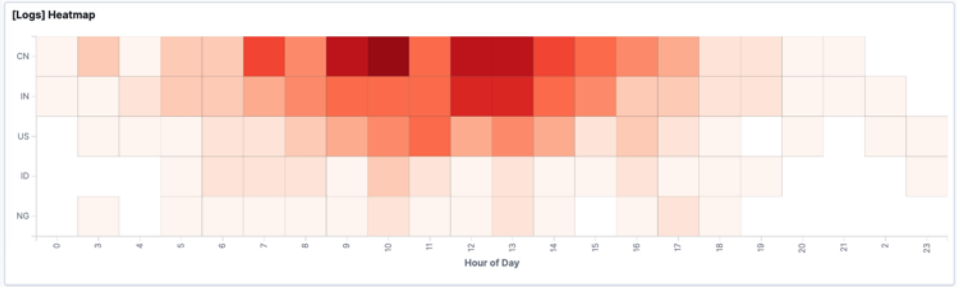


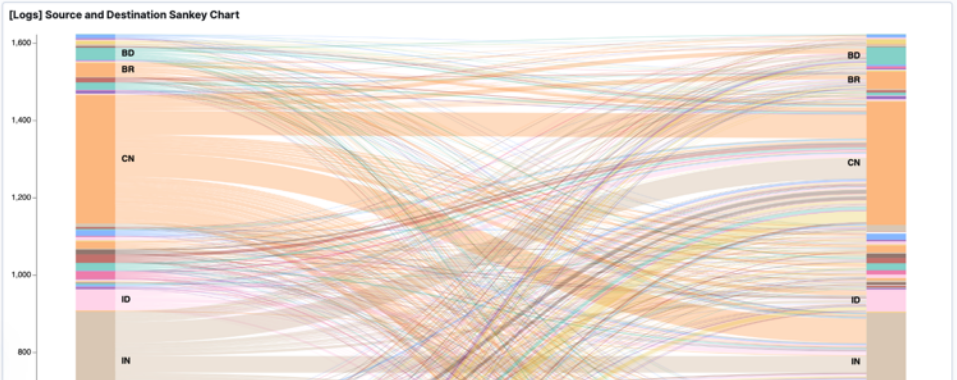


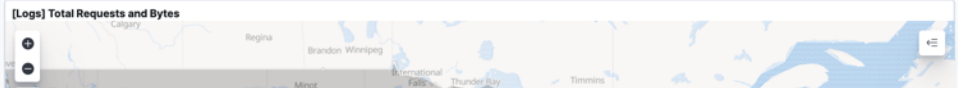


[Logs] Host, Visits and Bytes Table

Type	Bytes (Total)	Bytes (Last Hour)	Unique Visits (Total)	Unique Visits (Last Hour)
	0B	0B	0	0
gz	0B	0B	0	0
css	0B	3.634KB	0	1
zip	0B	7.195KB	0	1
deb	0B	7.793KB	0	1
rpm	0B	0B	0	0

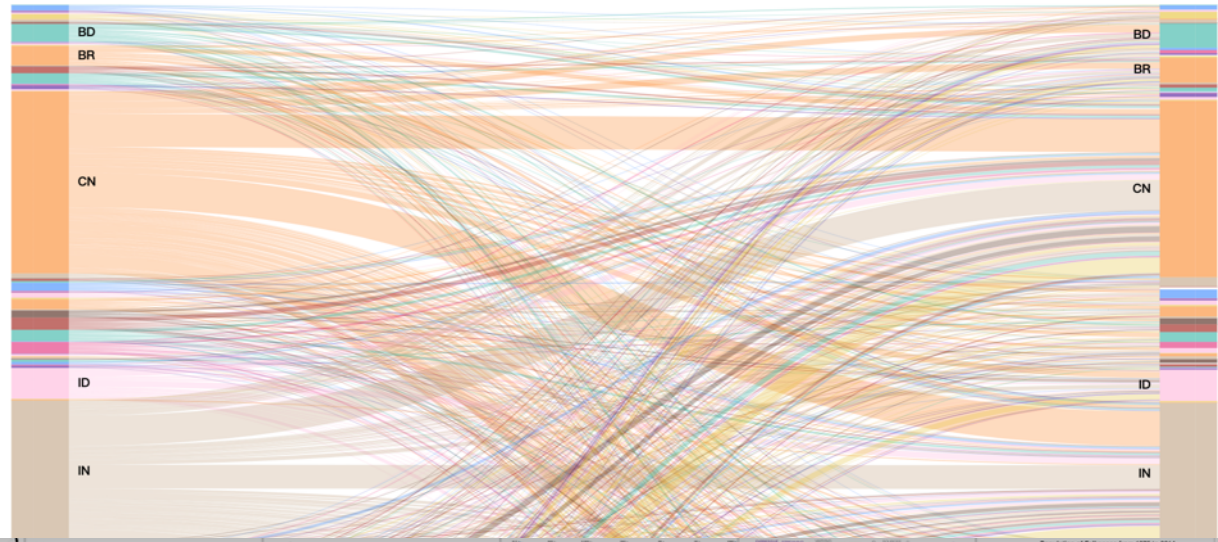


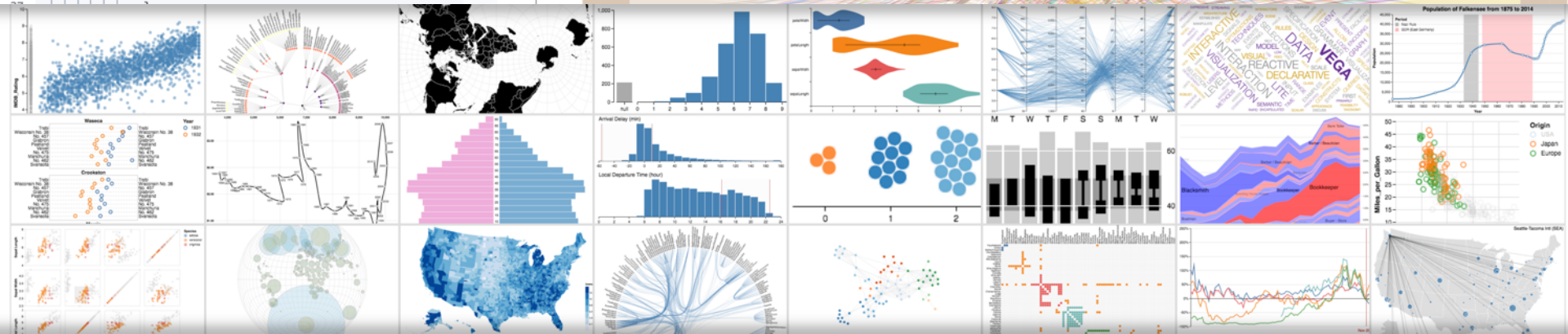




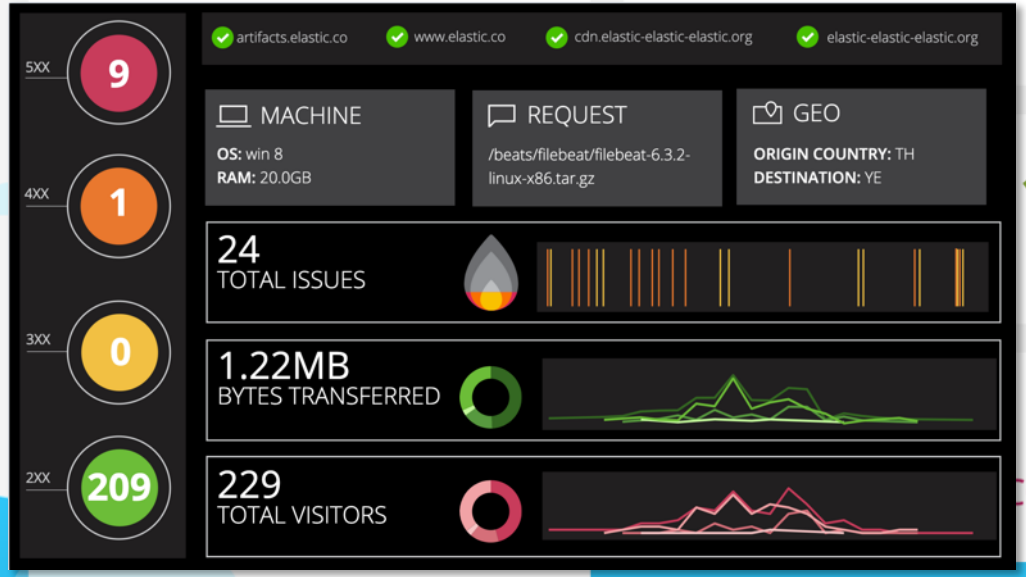
数据展现 – 丰富的开放生态，支持开源Vega图表组件

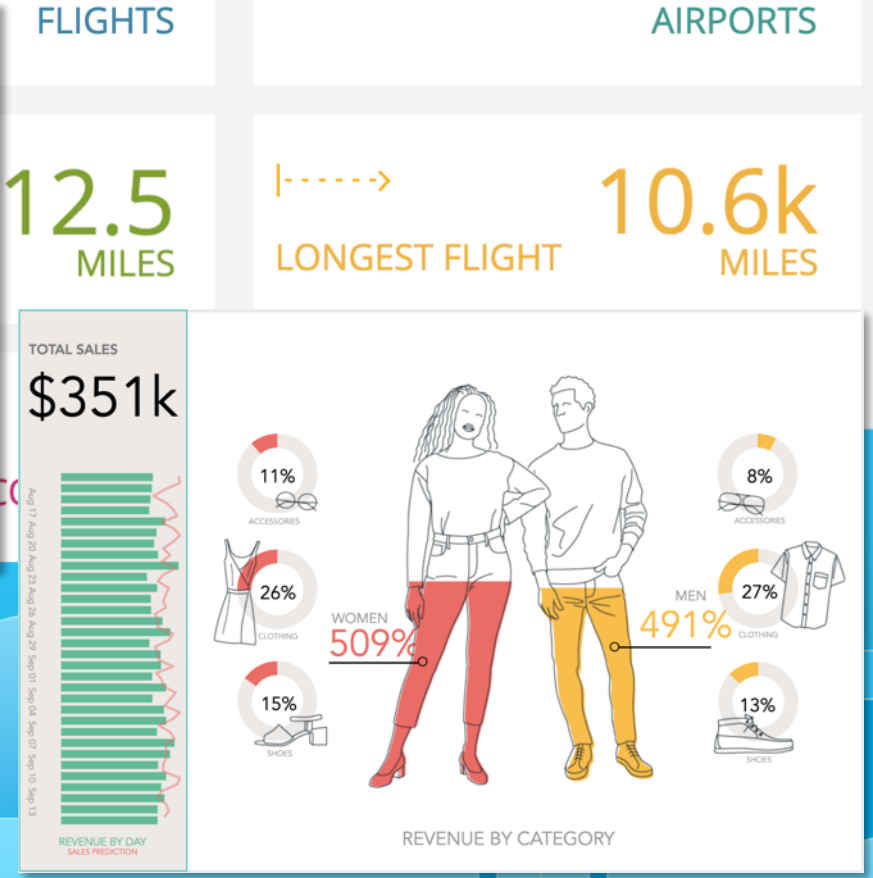
```
{
  $schema: https://vega.github.io/schema/vega/v3.0.json
  data: [
  {
    // query ES based on the currently selected time range and
       filter string
    name: rawData
    url: {
      %context%: true
      %timefield%: timestamp
      index: kibana_sample_data_logs
      body: {
        size: 0
        aggs: {
          table: {
            composite: {
              size: 10000
              sources: [
                {
                  stk1: {
                    terms: {field: "geo.src"}
                  }
                }
                {
                  stk2: {
                    terms: {field: "geo.dest"}
                  }
```

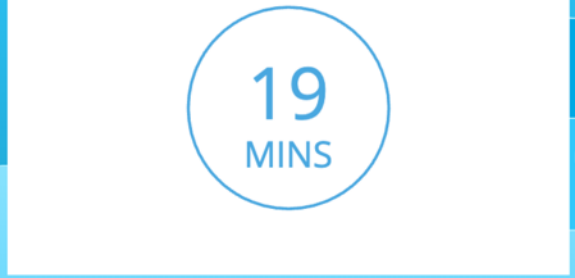




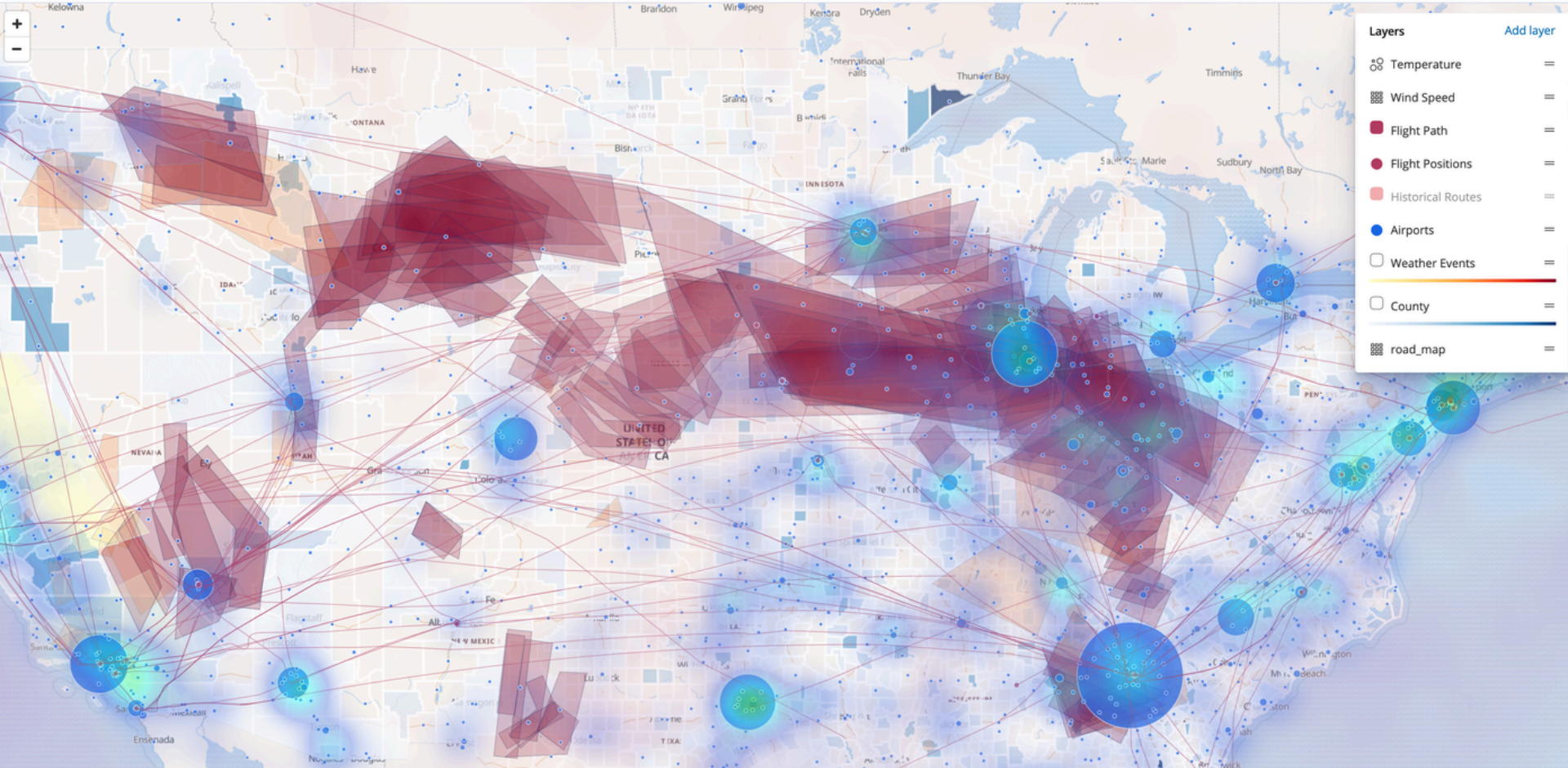
数据展现 – 像PPT一样的全动态大屏报表



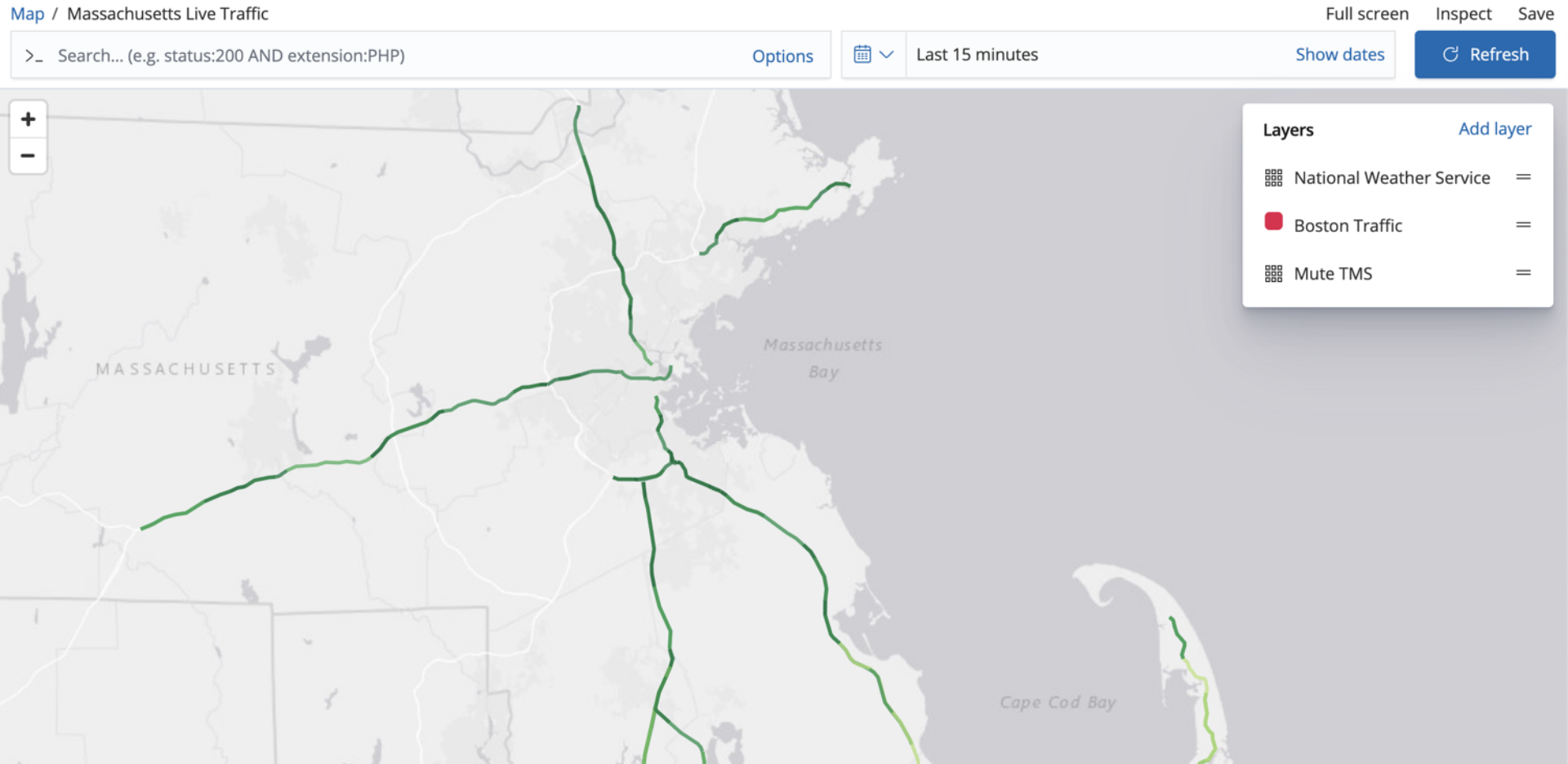




数据展现 – 在地图上分析数据



数据展现 – 地图上画路径也能做到



1,021	4	5	3	2
Total Attacks	Unique Rules Hit	Unique Sources	Source Attack Countries	Reporting Hosts

WAF - Chart of Top 10 Rules



WAF - Chart Of Severities



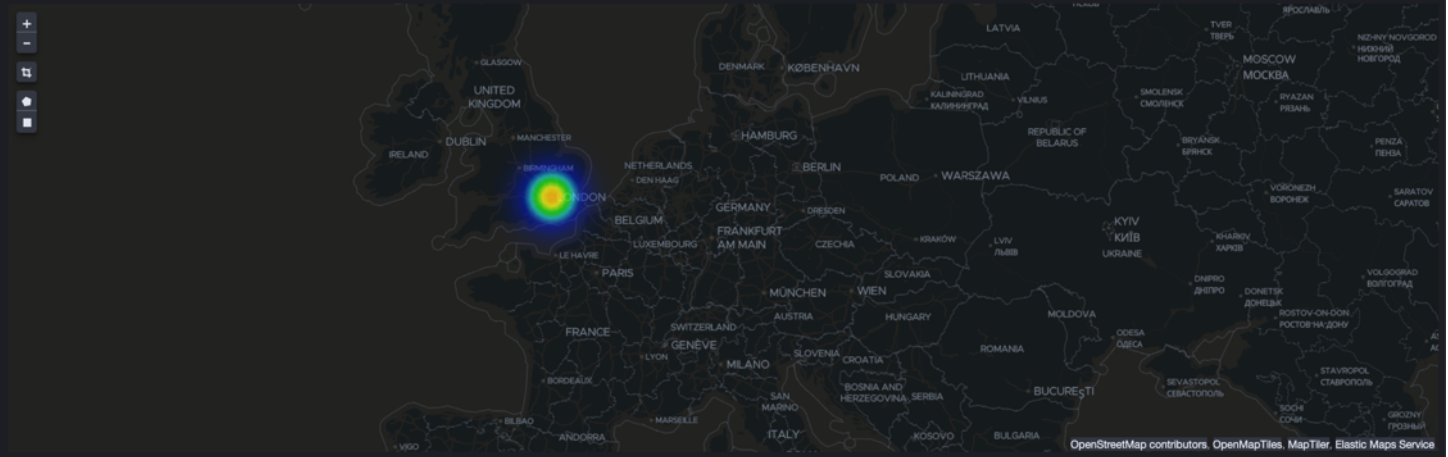
WAF - OS Pie Chart



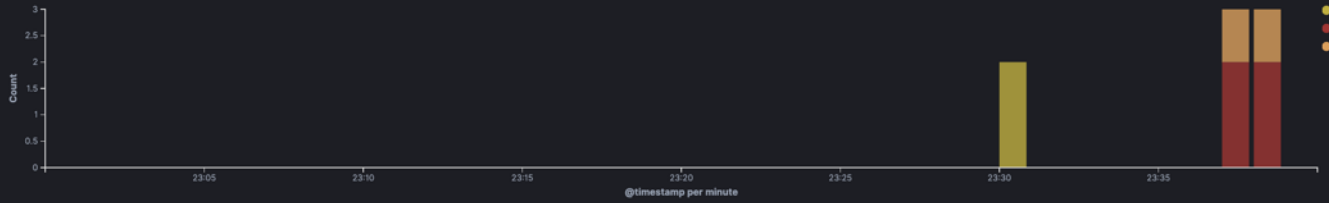
WAF - Top 5 Targeted URI's



WAF - Attack Heat Map

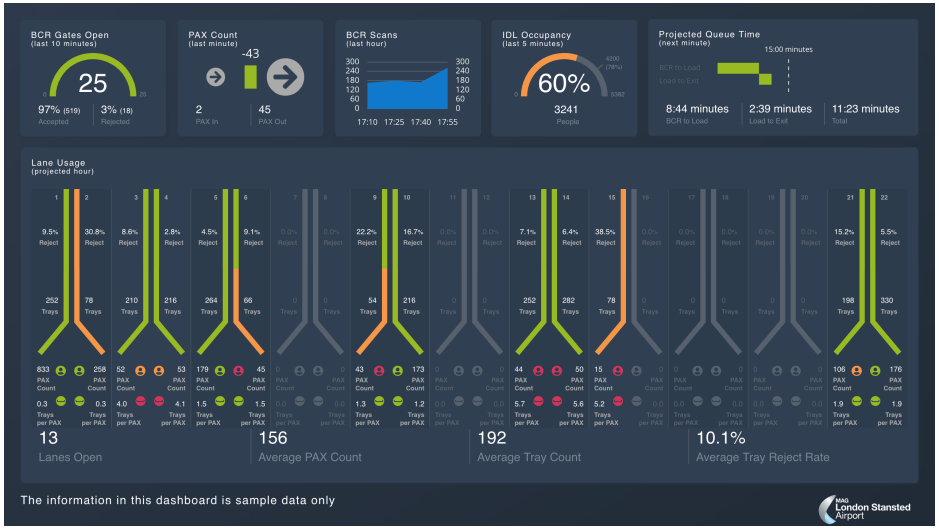


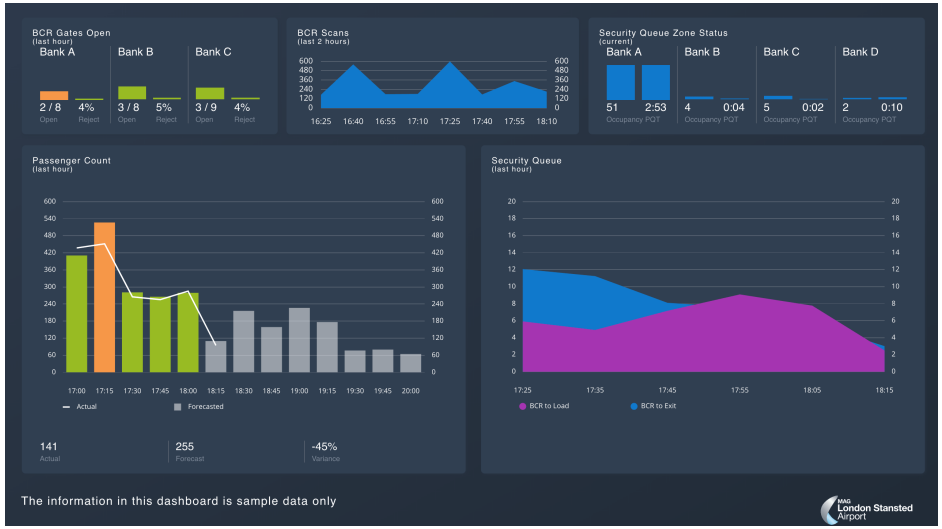
WAF - Events Over Time, By Severity

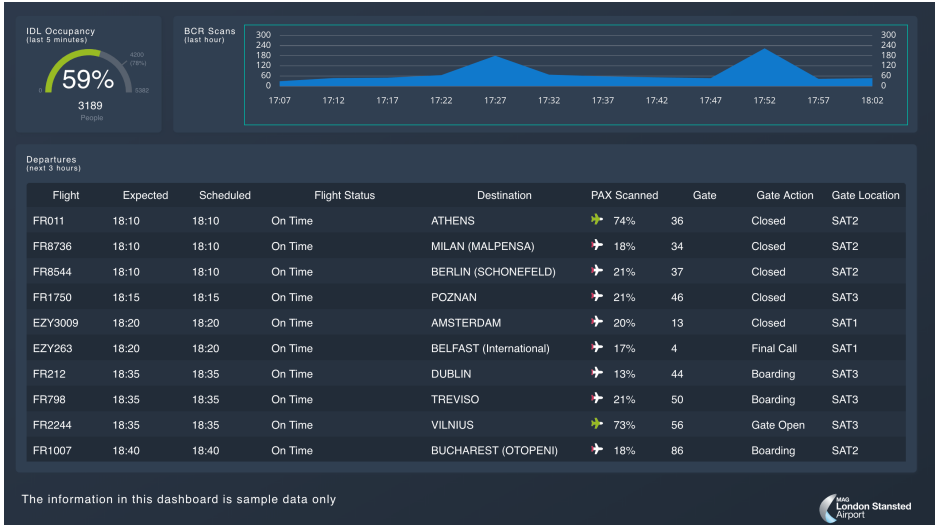


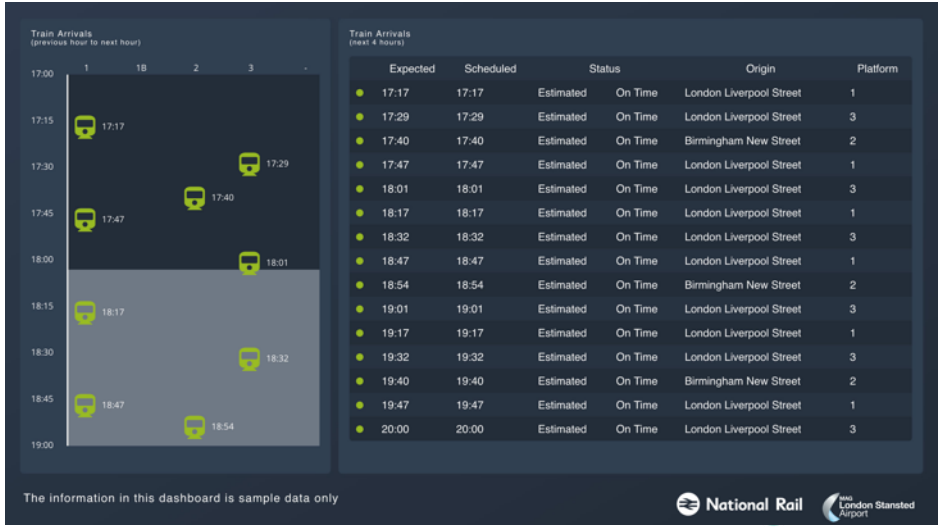
WAF - Messages Over Times




BCR Gates Open
(last 10 minutes)
25
97% (519)
Accepted
3% (18)
Rejected
PAX Count
(last minute)
-43
2
PAX In
45
PAX Out
BCR Scans
(last hour)
17:10 17:25 17:40 17:55
IDL Occupancy
(last 5 minutes)
60%
3241
People
Projected Queue Time
(next minute)
15:00 minutes
8:44 minutes
BCR to Load
2:39 minutes
Load to Exit
11:23 minutes
Total
Lane Usage
(projected hour)
13
Lanes Open
156
Average PAX Count
192
Average Tray Count
10.1%
Average Tray Reject Rate
The information in this dashboard is sample data only
London Stansted Airport


BCR Gates Open
(last hour)
Bank A
2 / 8
Open
4%
Reject
Bank B
3 / 8
Open
5%
Reject
Bank C
3 / 9
Open
4%
Reject
BCR Scans
(last 2 hours)
16:25 16:40 16:55 17:10 17:25 17:40 17:55 18:10
Security Queue Zone Status
(current)
Bank A
51
2:53
Occupancy PQT
Bank B
4
0:04
Occupancy PQT
Bank C
5
0:02
Occupancy PQT
Bank D
2
0:10
Occupancy PQT
Passenger Count
(last hour)
17:00 17:15 17:30 17:45 18:00 18:15 18:30 18:45 19:00 19:15 19:30 19:45 20:00
Actual
Forecasted
141
Actual
255
Forecast
-45%
Variance
Security Queue
(last hour)
17:25 17:35 17:45 17:55 18:05 18:15
BCR to Load
BCR to Exit
The information in this dashboard is sample data only
London Stansted Airport


IDL Occupancy
(last 5 minutes)
59%
3189
People
BCR Scans
(last hour)
17:07 17:12 17:17 17:22 17:27 17:32 17:37 17:42 17:47 17:52 17:57 18:02
Departures
(next 3 hours)
Flight Expected Scheduled Flight Status Destination PAX Scanned Gate Gate Action Gate Location
FR011 18:10 18:10 On Time ATHENS 74% 36 Closed SAT2
FR8736 18:10 18:10 On Time MILAN (MALPENSA) 18% 34 Closed SAT2
FR8544 18:10 18:10 On Time BERLIN (SCHONEFELD) 21% 37 Closed SAT2
FR1750 18:15 18:15 On Time POZNAN 21% 46 Closed SAT3
EZY3009 18:20 18:20 On Time AMSTERDAM 20% 13 Closed SAT1
EZY263 18:20 18:20 On Time BELFAST (International) 17% 4 Final Call SAT1
FR212 18:35 18:35 On Time DUBLIN 13% 44 Boarding SAT3
FR798 18:35 18:35 On Time TREVISO 21% 50 Boarding SAT3
FR2244 18:35 18:35 On Time VILNIUS 73% 56 Gate Open SAT3
FR1007 18:40 18:40 On Time BUCHAREST (OTOPENI) 18% 86 Boarding SAT2
The information in this dashboard is sample data only
London Stansted Airport


Train Arrivals
(previous hour to next hour)
17:17
17:29
17:40
17:47
18:01
18:17
18:32
18:47
18:54
Train Arrivals
(next 4 hours)
Expected Scheduled Status Origin Platform
17:17 17:17 Estimated On Time London Liverpool Street 1
17:29 17:29 Estimated On Time London Liverpool Street 3
17:40 17:40 Estimated On Time Birmingham New Street 2
17:47 17:47 Estimated On Time London Liverpool Street 1
18:01 18:01 Estimated On Time London Liverpool Street 3
18:17 18:17 Estimated On Time London Liverpool Street 1
18:32 18:32 Estimated On Time London Liverpool Street 3
18:47 18:47 Estimated On Time London Liverpool Street 1
18:54 18:54 Estimated On Time Birmingham New Street 2
19:01 19:01 Estimated On Time London Liverpool Street 3
19:17 19:17 Estimated On Time London Liverpool Street 1
19:32 19:32 Estimated On Time London Liverpool Street 3
19:40 19:40 Estimated On Time Birmingham New Street 2
19:47 19:47 Estimated On Time London Liverpool Street 1
20:00 20:00 Estimated On Time London Liverpool Street 3
The information in this dashboard is sample data only
National Rail
London Stansted Airport

APM 从无到有

elastic

APM

统一 日志，指标，APM

Open Source

各种语言客户端

Java, .Net, Go, RUM, Node, Python, Ruby

Kibana UI

APM 工作流程耗时图
分布式的追踪

只是多了一种索引

和其它数据关联
借助于ES的功能



Transaction sample

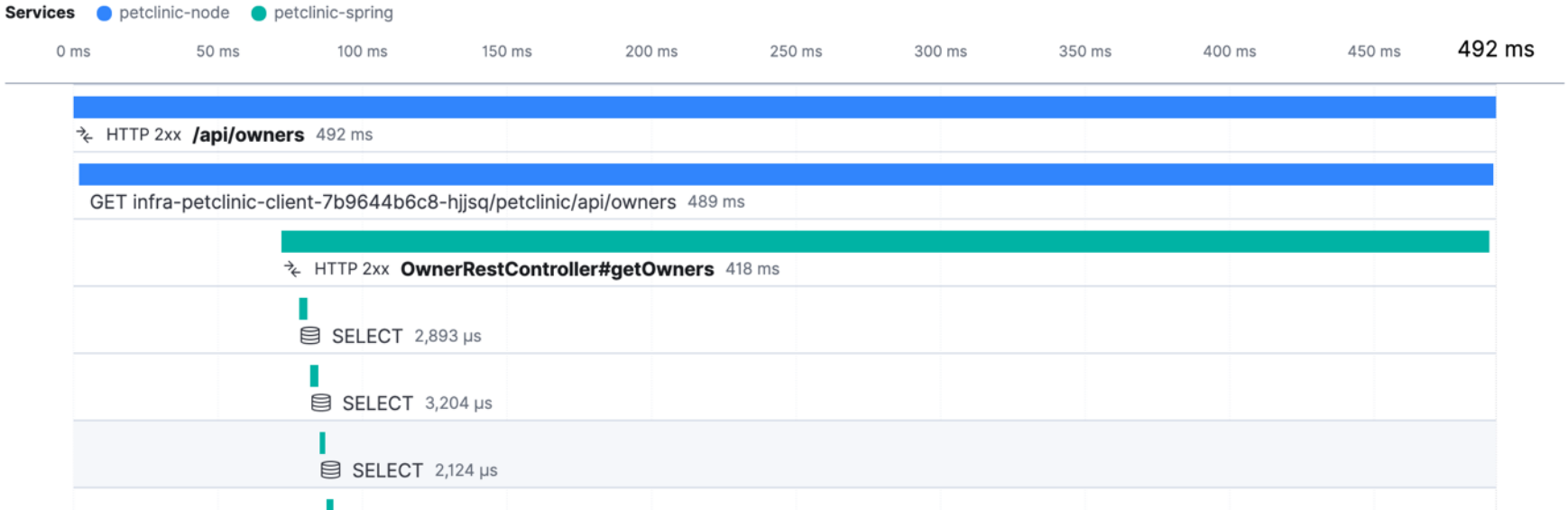
Actions | View full trace

Timestamp
9 months ago (November 27th 2018, 08:00:32.947)

URL
http://infra-petclinic-client-7b9644b6c8-hjjsq/api/owners

Duration	% of trace	Result	Errors	User ID
492 ms	N/A	HTTP 2xx	None	lwoollaston52

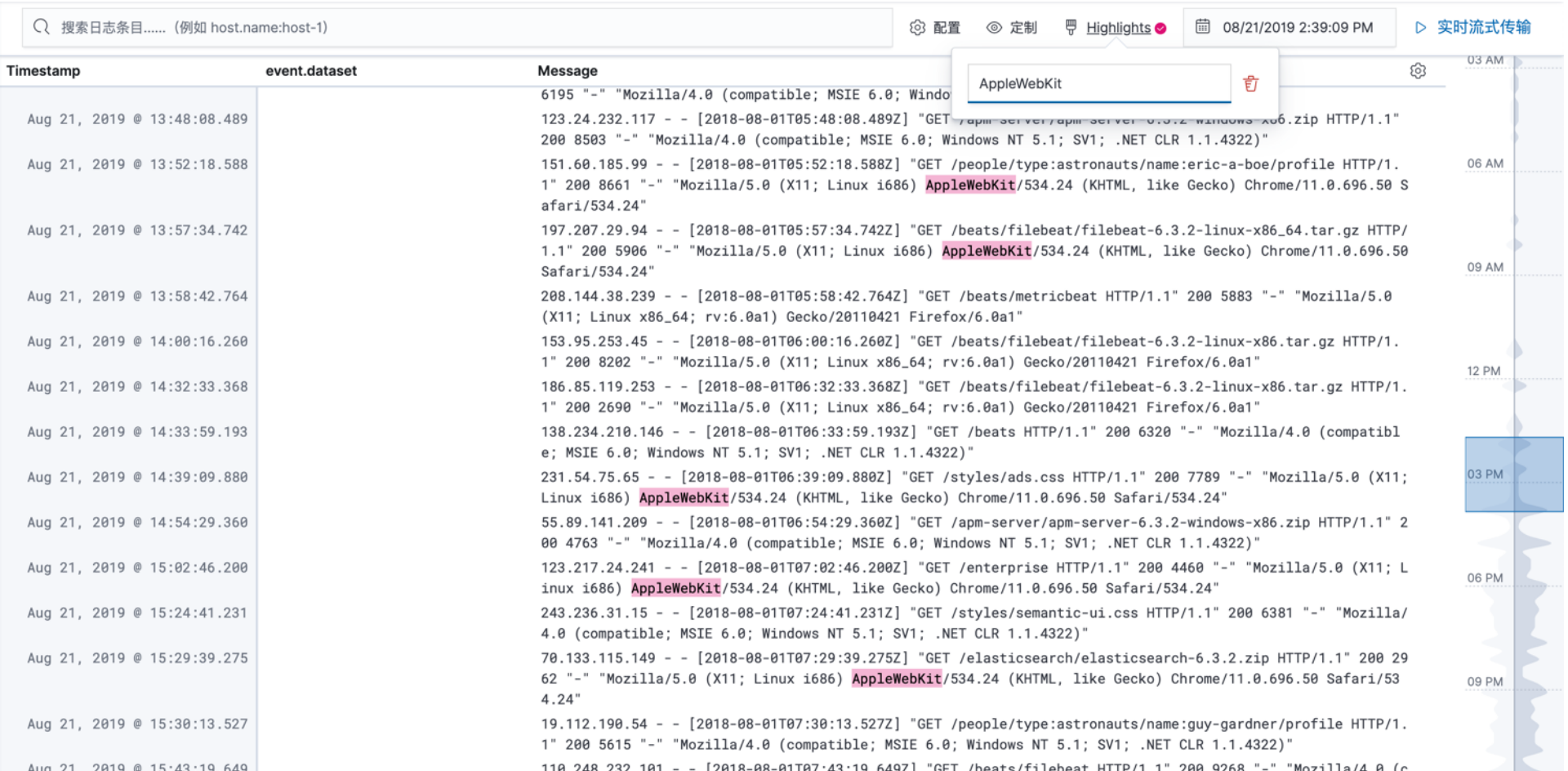
Timeline | Metadata



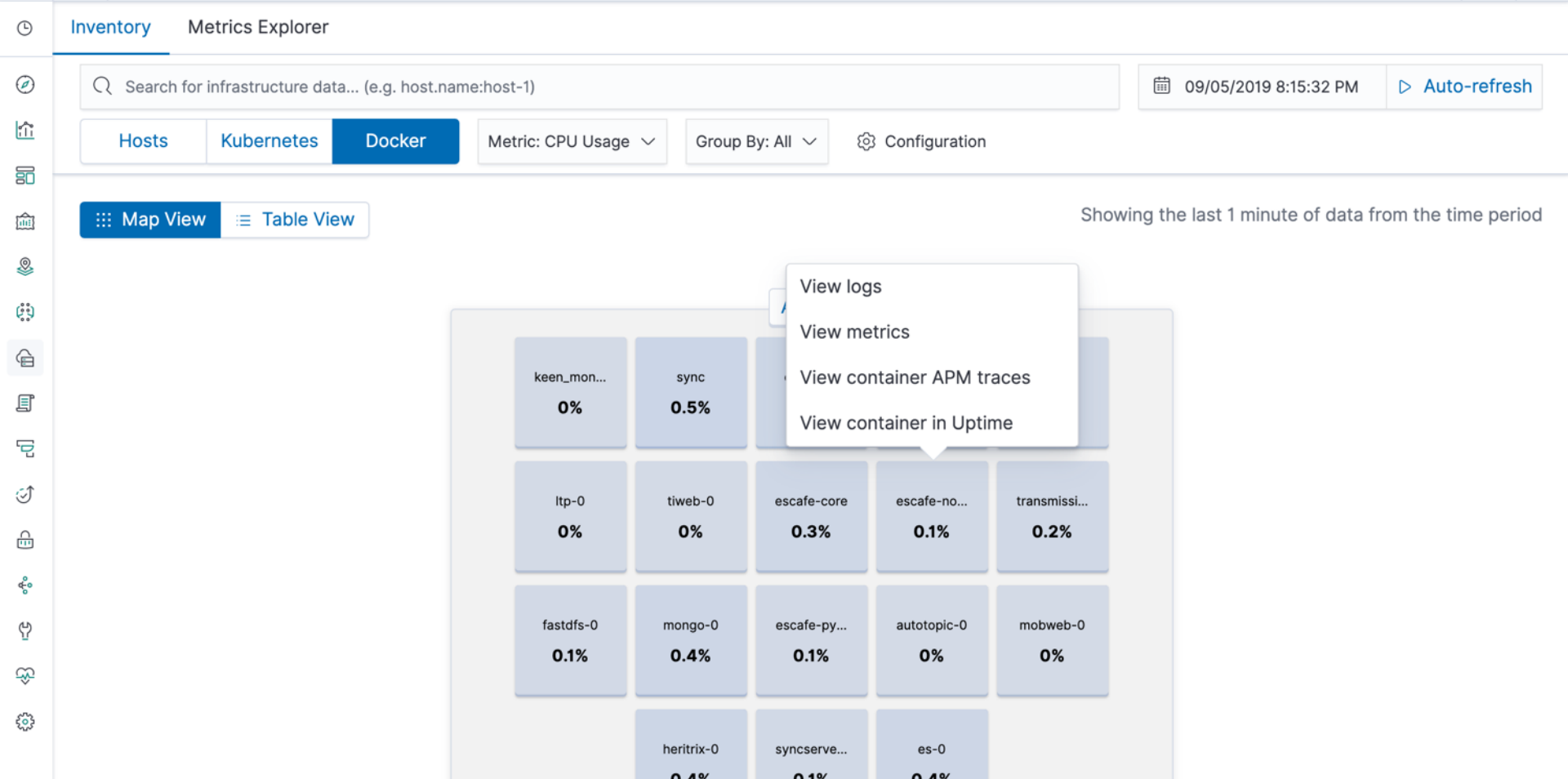
其它Kibana APP

elastic

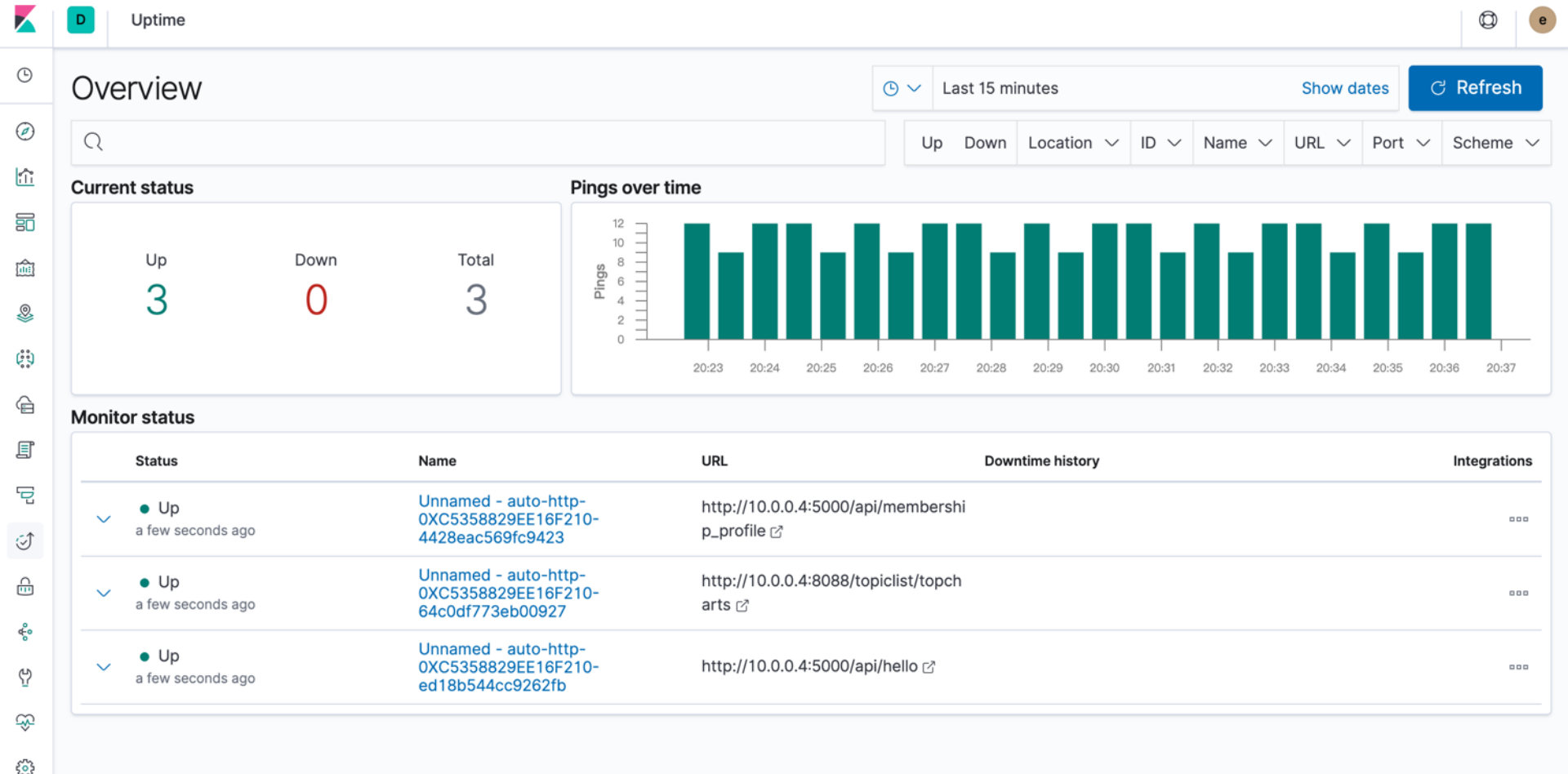
Logs 实时流式日志查看器



Infrastructure



Uptime

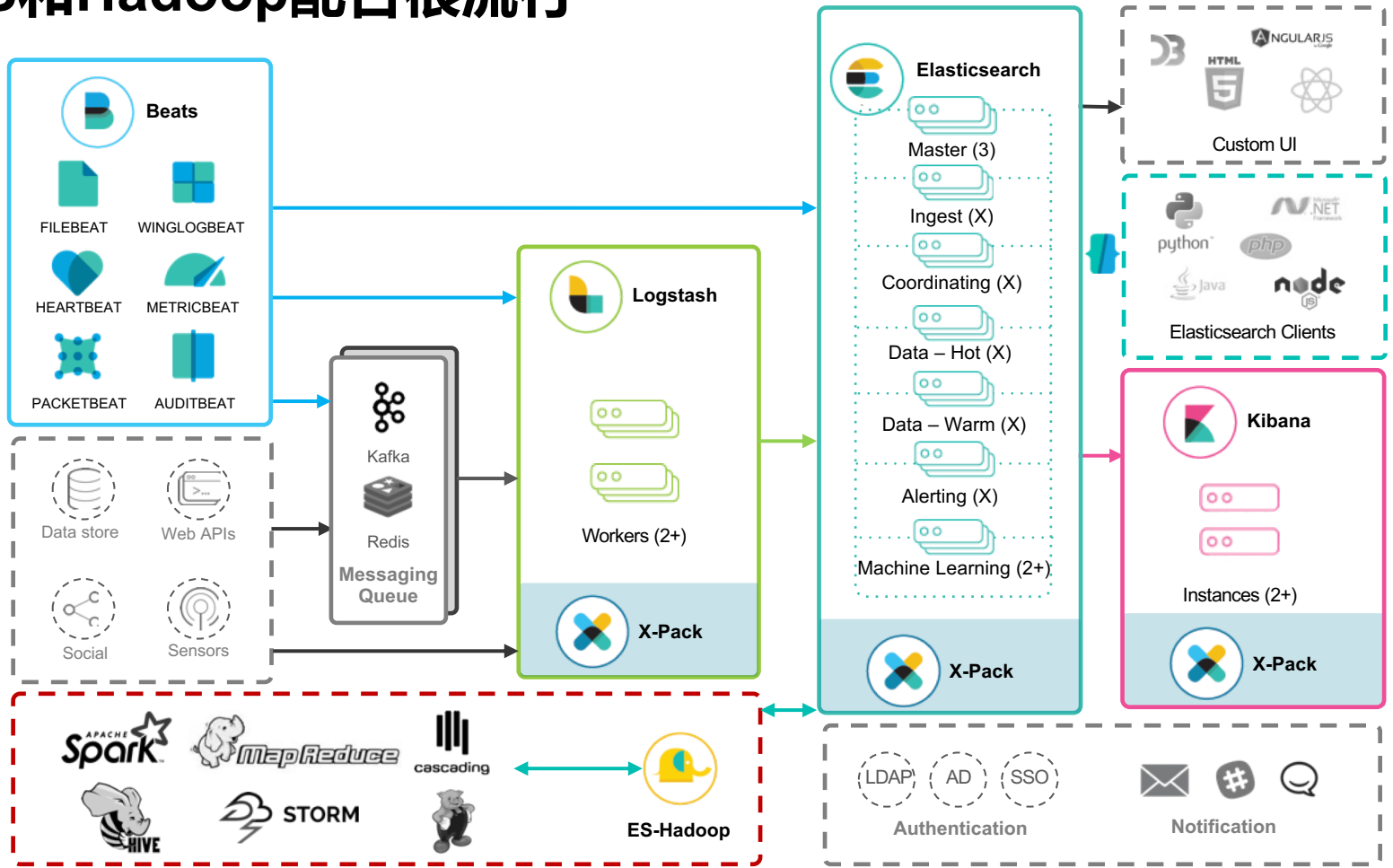

Uptime
Overview
Last 15 minutes
Show dates
Refresh
Up
Down
Location
ID
Name
URL
Port
Scheme
Current status
Up
3
Down
0
Total
3
Pings over time
Pings
12
10
8
6
4
2
0
20:23
20:24
20:25
20:26
20:27
20:28
20:29
20:30
20:31
20:32
20:33
20:34
20:35
20:36
20:37
Monitor status
Status
Name
URL
Downtime history
Integrations
Up
a few seconds ago
Unnamed - auto-http-0XC5358829EE16F210-4428eac569fc9423
http://10.0.0.4:5000/api/membership_profile
Up
a few seconds ago
Unnamed - auto-http-0XC5358829EE16F210-64c0df773eb00927
http://10.0.0.4:8088/topiclist/topcharts
Up
a few seconds ago
Unnamed - auto-http-0XC5358829EE16F210-ed18b544cc9262fb
http://10.0.0.4:5000/api/hello

Elastic Stack
需要 融入开放生态

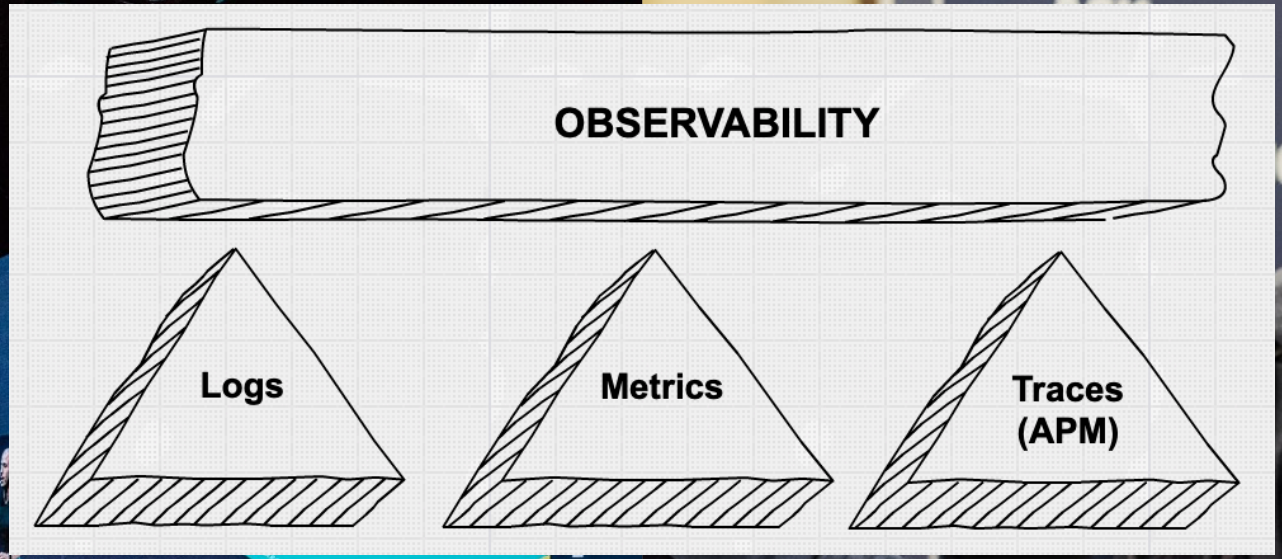
elastic


Grafana
pentaho
Spark Streaming
Apache Flink
fluentd
FLUME
Elastic
+ a b l e a u
ZABBIX
HIVE
Prometheus
CISCO
paloalto NETWORKS
hadoop

ES和Hadoop配合很流行



elastic



Elastic是一个快速行动的公司
快速实现目标，并将越来越好

elastic