日志指标与可视化分析

Jerry Zhu
Elastic 架构师

Elastic是 ELK背后的公司

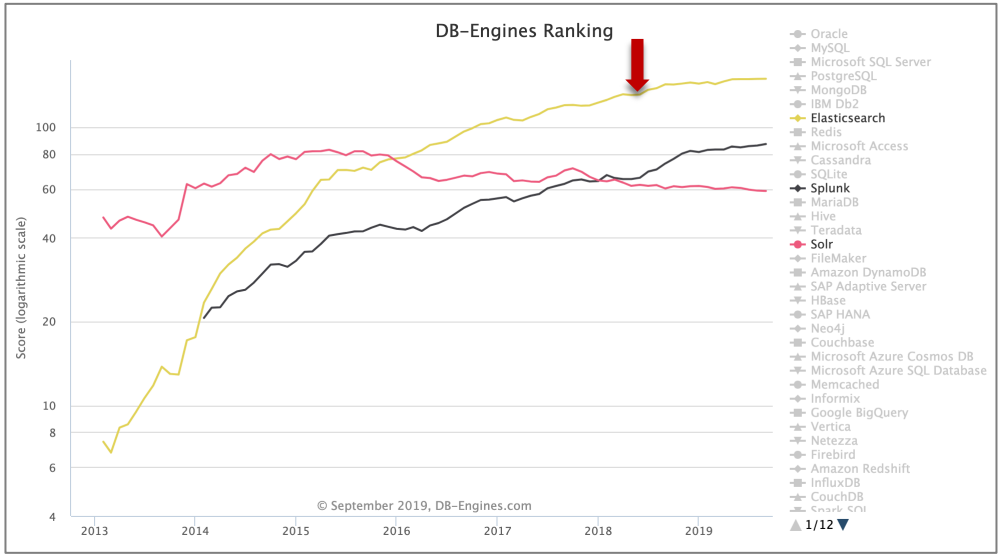
- **10万+** 全球社区参与者
  1万+ 中国社区参与者
- **3.5亿+** 下载 (持续增长中)
- **1680+** 员工
- **8800+** 付费订阅客户
- **NYSE: ESTC**

elastic

Elasticsearch 非常受欢迎

DB-Engines Ranking 2019 Sep

Rank Sep 2019	Rank Aug 2019	Rank Sep 2018	DBMS	Database Model	Score Sep 2019	Score Aug 2019	Score Sep 2018
1.	1.	1.	Oracle	Relational, Multi-model	1346.66	+7.18	+37.54
2.	2.	2.	MySQL	Relational, Multi-model	1279.07	+25.39	+98.60
3.	3.	3.	Microsoft SQL Server	Relational, Multi-model	1085.06	-8.12	+33.78
4.	4.	4.	PostgreSQL	Relational, Multi-model	482.25	+0.91	+75.82
5.	5.	5.	MongoDB	Document	410.06	+5.50	+51.27
6.	6.	6.	IBM Db2	Relational, Multi-model	171.56	-1.39	-9.50
7.	7.	7.	Elasticsearch	Search engine, Multi-model	149.27	+0.19	+6.67
8.	8.	8.	Redis	Key-value, Multi-model	141.90	-2.18	+0.96
9.	9.	9.	Microsoft Access	Relational	132.71	-2.63	-0.69
10.	10.	10.	Cassandra	Wide column	123.40	-1.81	+3.85
11.	11.	11.	SQLite	Relational	123.36	+0.65	+7.91
12.	12.	↑ 13.	Splunk	Search engine	87.01	+1.12	+12.98
13.	13.	↑ 14.	MariaDB	Relational, Multi-model	86.07	+1.11	+15.43
14.	14.	↑ 16.	Hive	Relational	83.10	+1.30	+23.46
15.	15.	↓ 12.	Teradata	Relational, Multi-model	76.97	+0.32	-0.42
16.	16.	↓ 15.	Solr	Search engine	58.97	-0.16	-1.24
17.	17.	↑ 19.	FileMaker	Relational	58.15	+0.13	+2.84
18.	18.	↑ 20.	Amazon DynamoDB	Multi-model	57.82	+1.25	+4.47
19.	↑ 20.	↓ 18.	SAP Adaptive Server	Relational	56.10	+0.24	-1.94
20.	↓ 19.	↓ 17.	HBase	Wide column	55.72	-0.82	-2.75
21.	21.	21.	SAP HANA	Relational, Multi-model	55.39	-0.04	+2.66



elastic

Elastic 产品生态

elastic

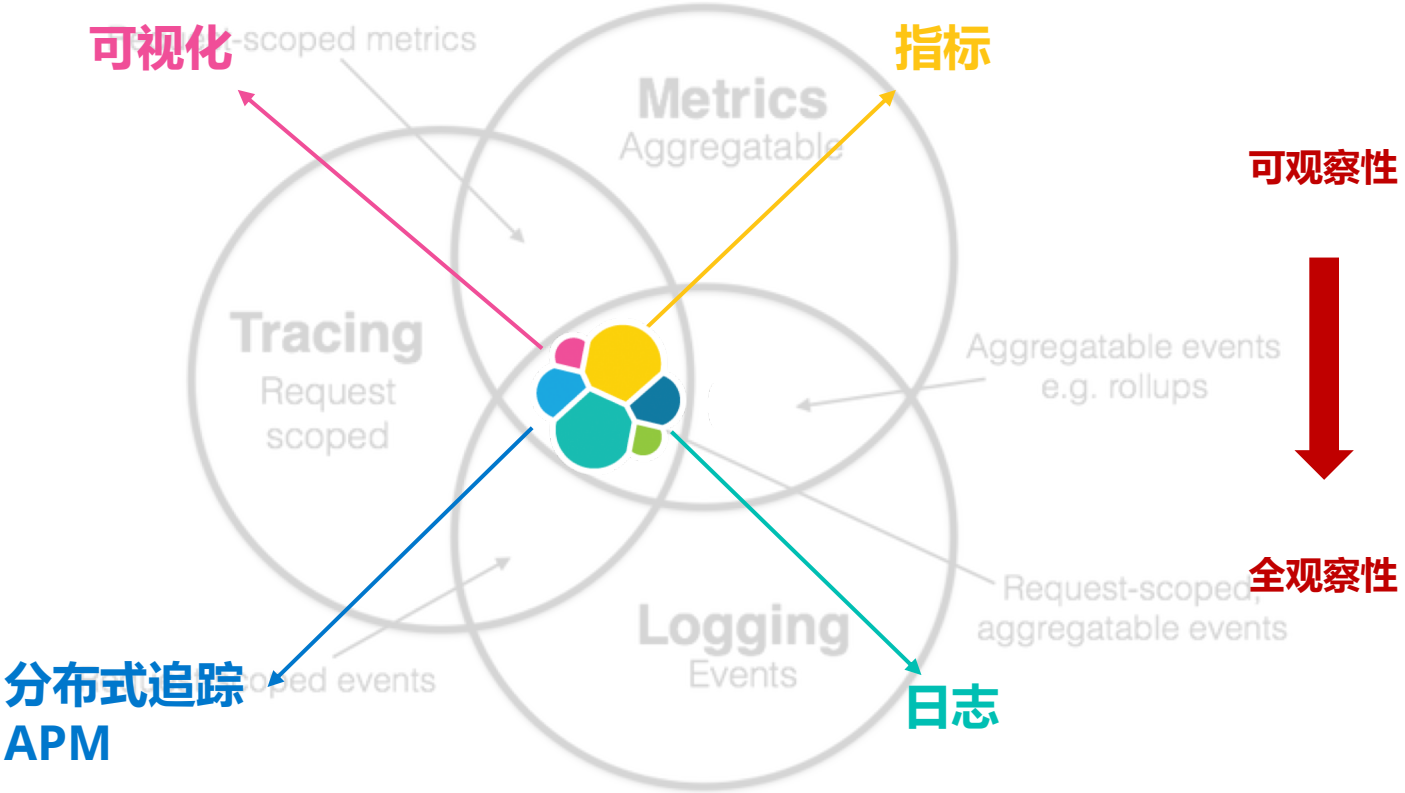
日志 指标 APM
IT全方位可观察性

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

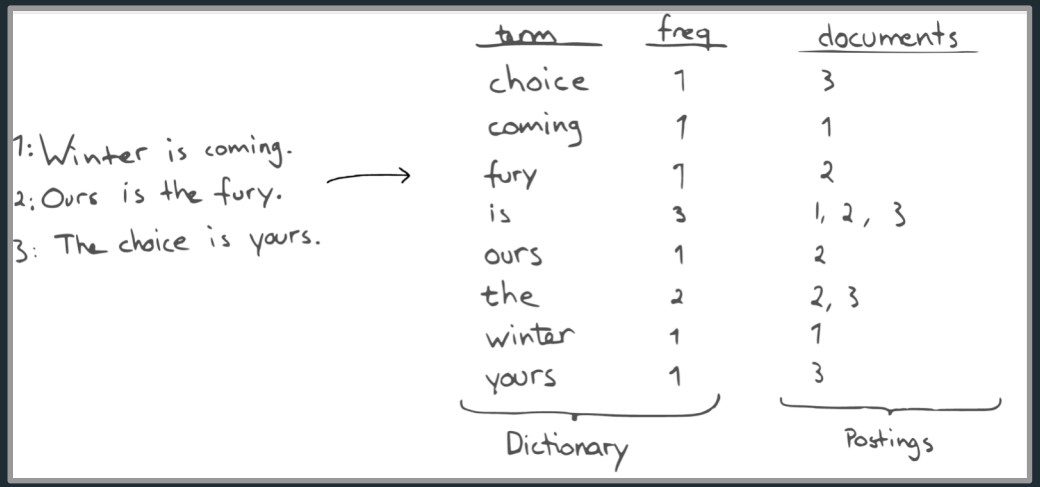
Lucene & Elasticsearch
付出的努力

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

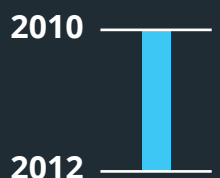
SEARCH



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

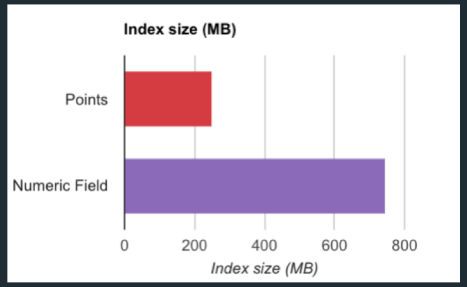
```
{
    "_index": "helioweb",
    "_type": "voyager1",
    "_id": "1977-257",
    "_score": 1,
    "_source": {
        "seLon": 353.8,
        "objectName": "voyager1",
        "seLat": 0.2,
        "year": 1977,
        "date": "1977-09-14T10:28:25.178Z",
        "radAU": 1.02,
        "dayOfYear":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

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

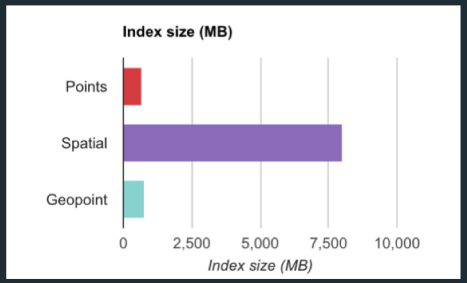
Elasticsearch 存储效率增强

BKD Trees & Sparse Fields

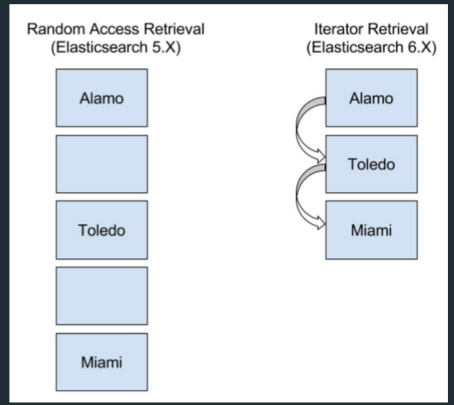
1-维数据



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

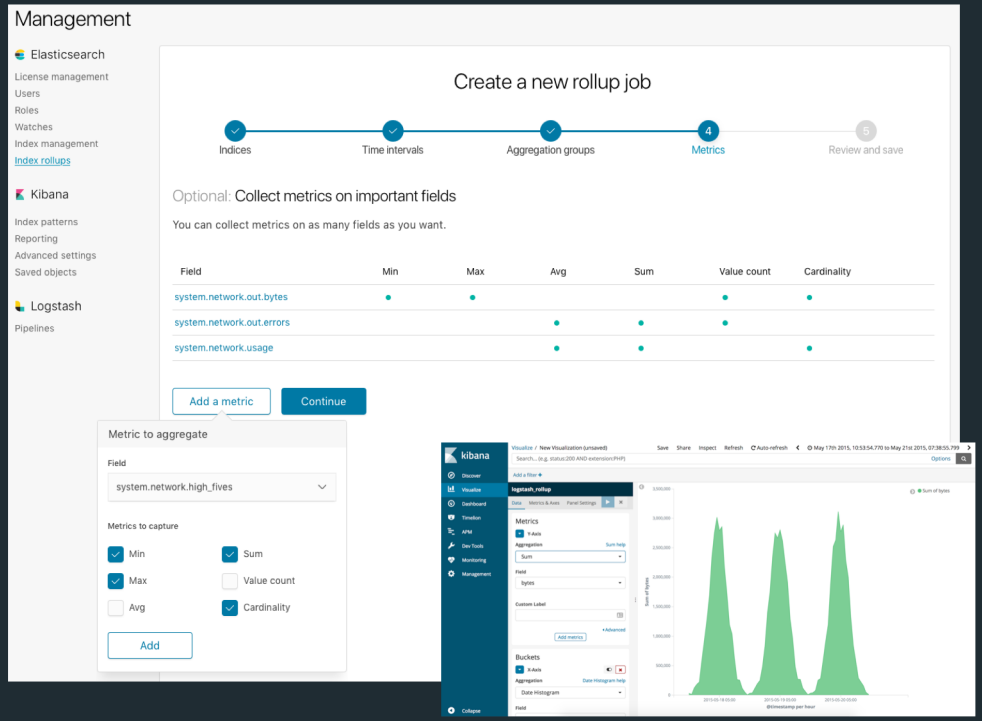
2014 — **聚合框架**
Analytics features to slice and dice data along various dimensions

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

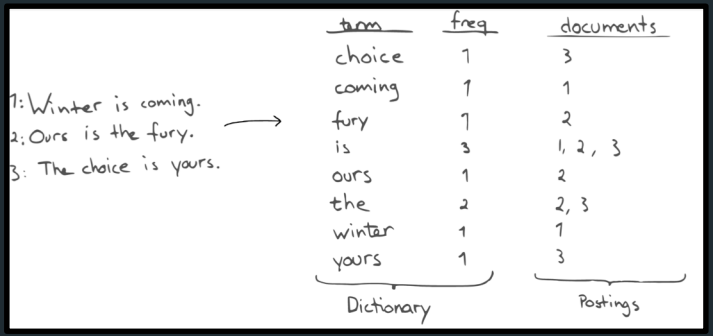
2016 — **BKD数据和稀疏数据**
Data structures optimized for numbers. Faster analytics, lower storage footprint

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

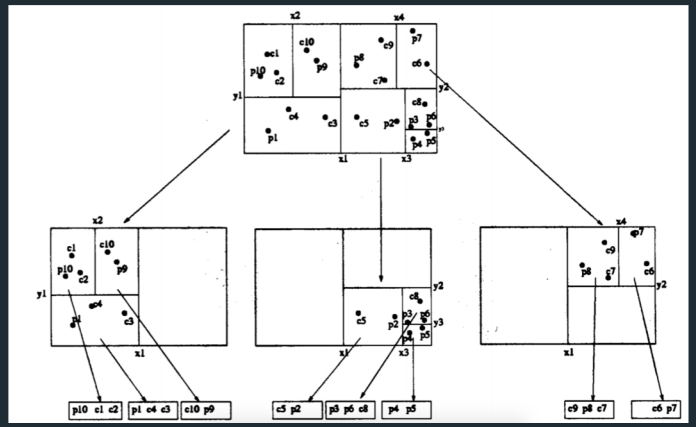
倒排序支持的全文搜索



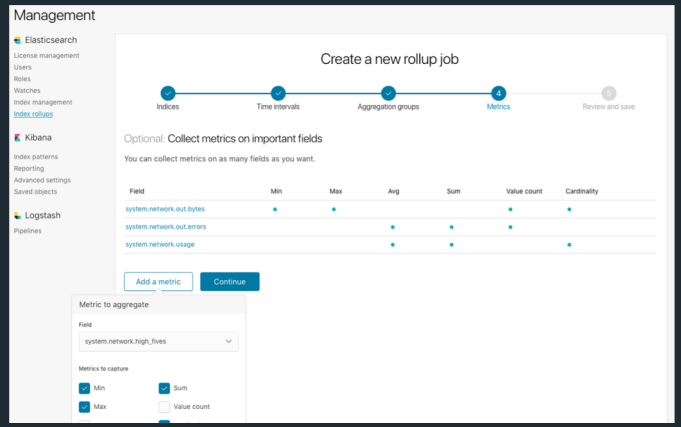
列存储支持的结构化数据

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

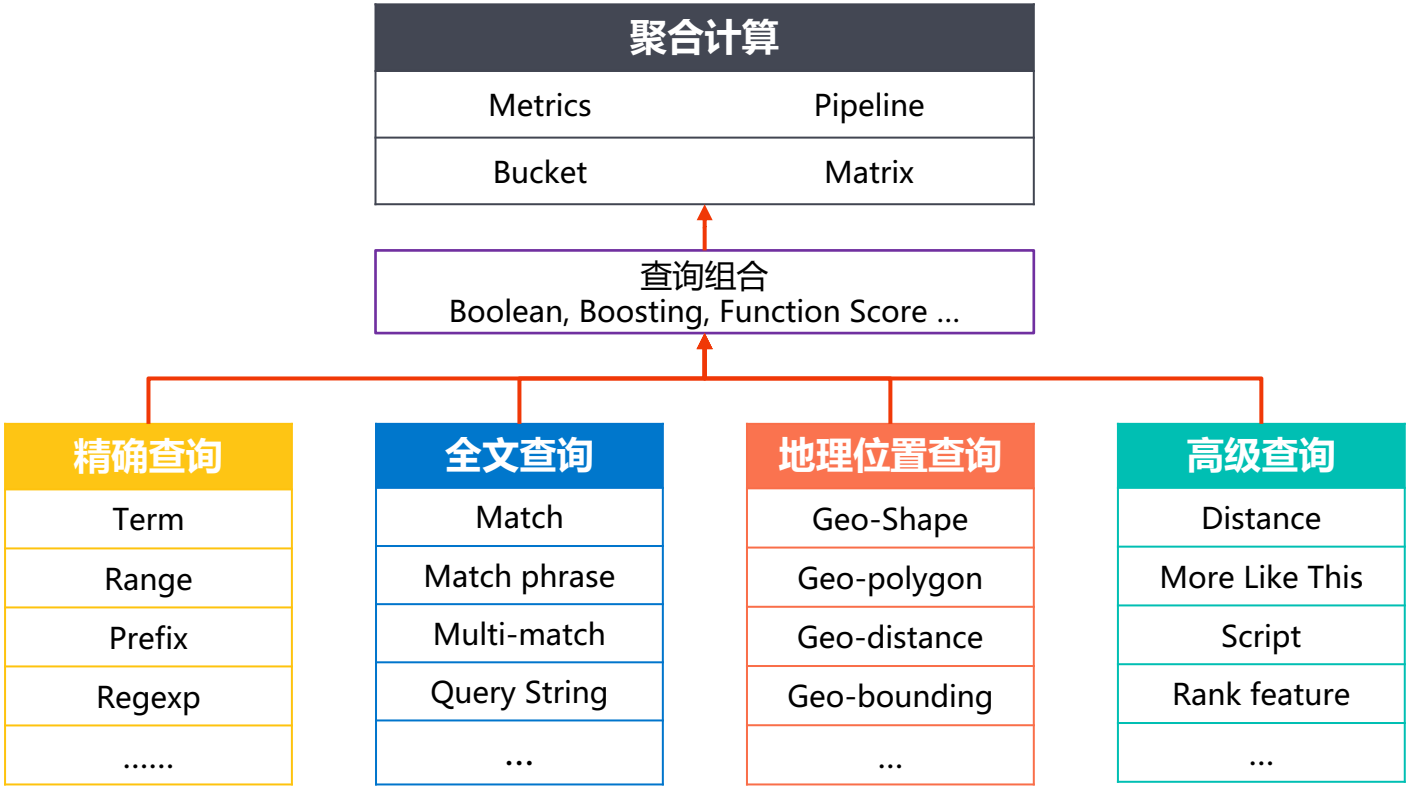
BKD数支持的数值型运算



Rollup 节省存储空间



查询能力变得空前强大



2019

Data Frames

未来…

Beats Logstash
付出的努力

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

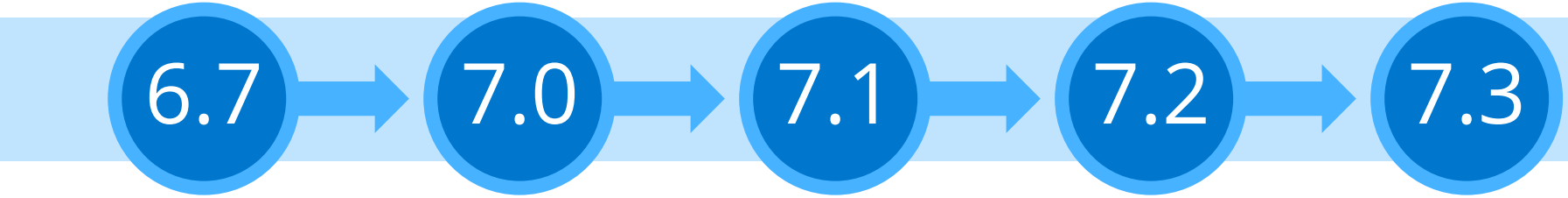
elastic

开放生态 第三方重磅工具

elastic

Kibana
付出的努力

产品快速迭代



以前的
Elastic Stack

一流的引擎！
三流的界面！

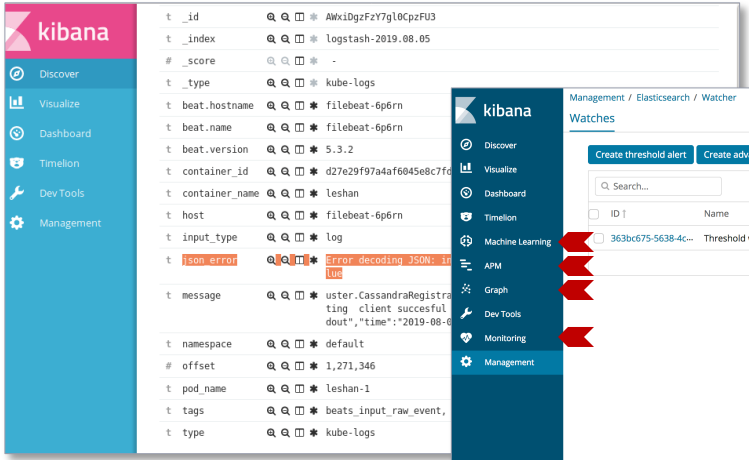
现在的
Elastic Stack

一流的引擎！
一流的界面！

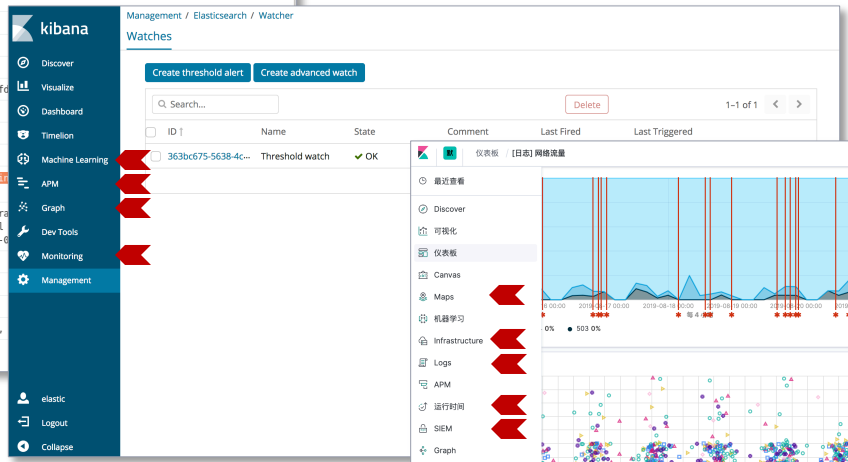
elastic

快速改进

Kibana 5.5



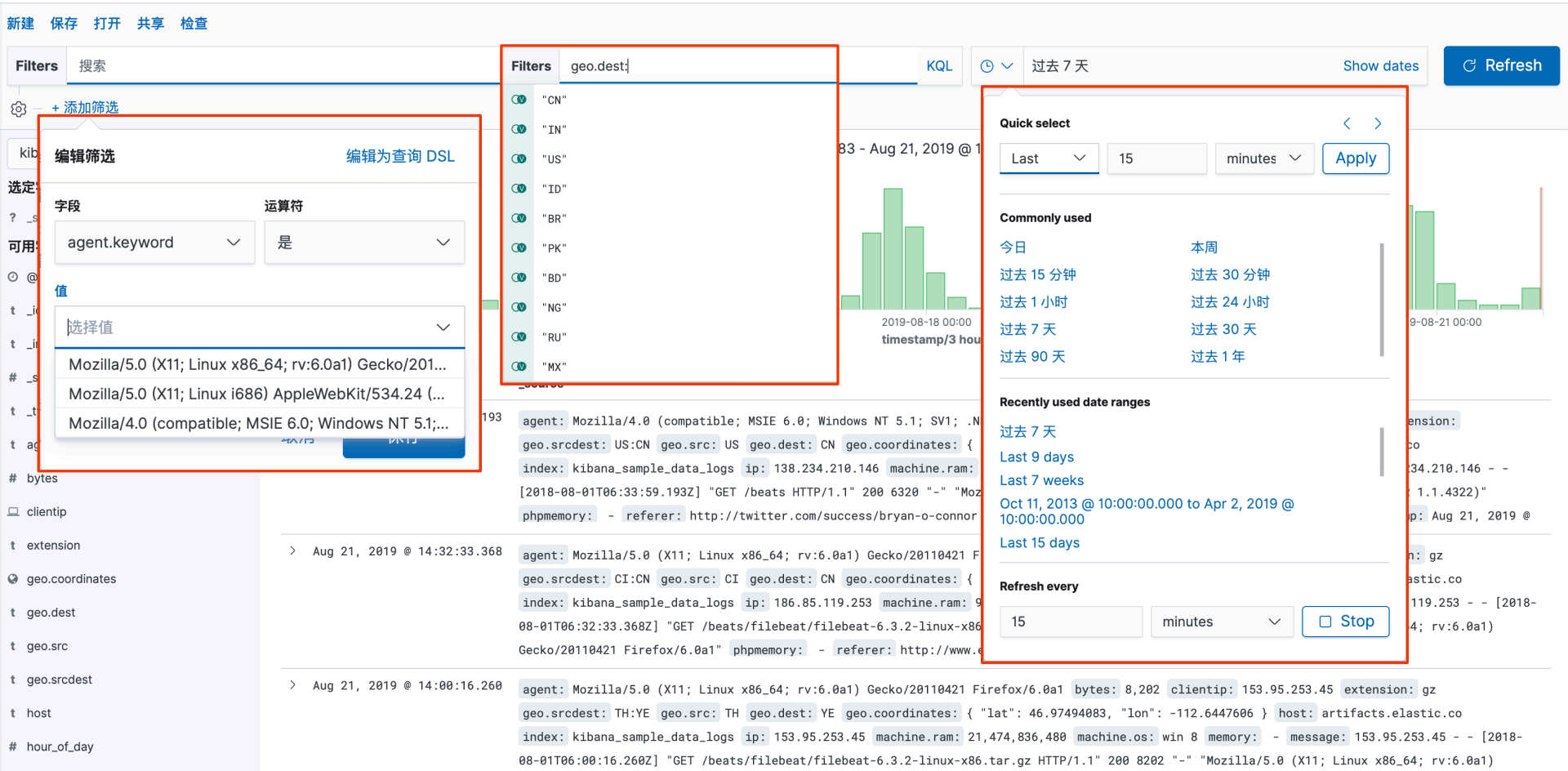
Kibana 6.5



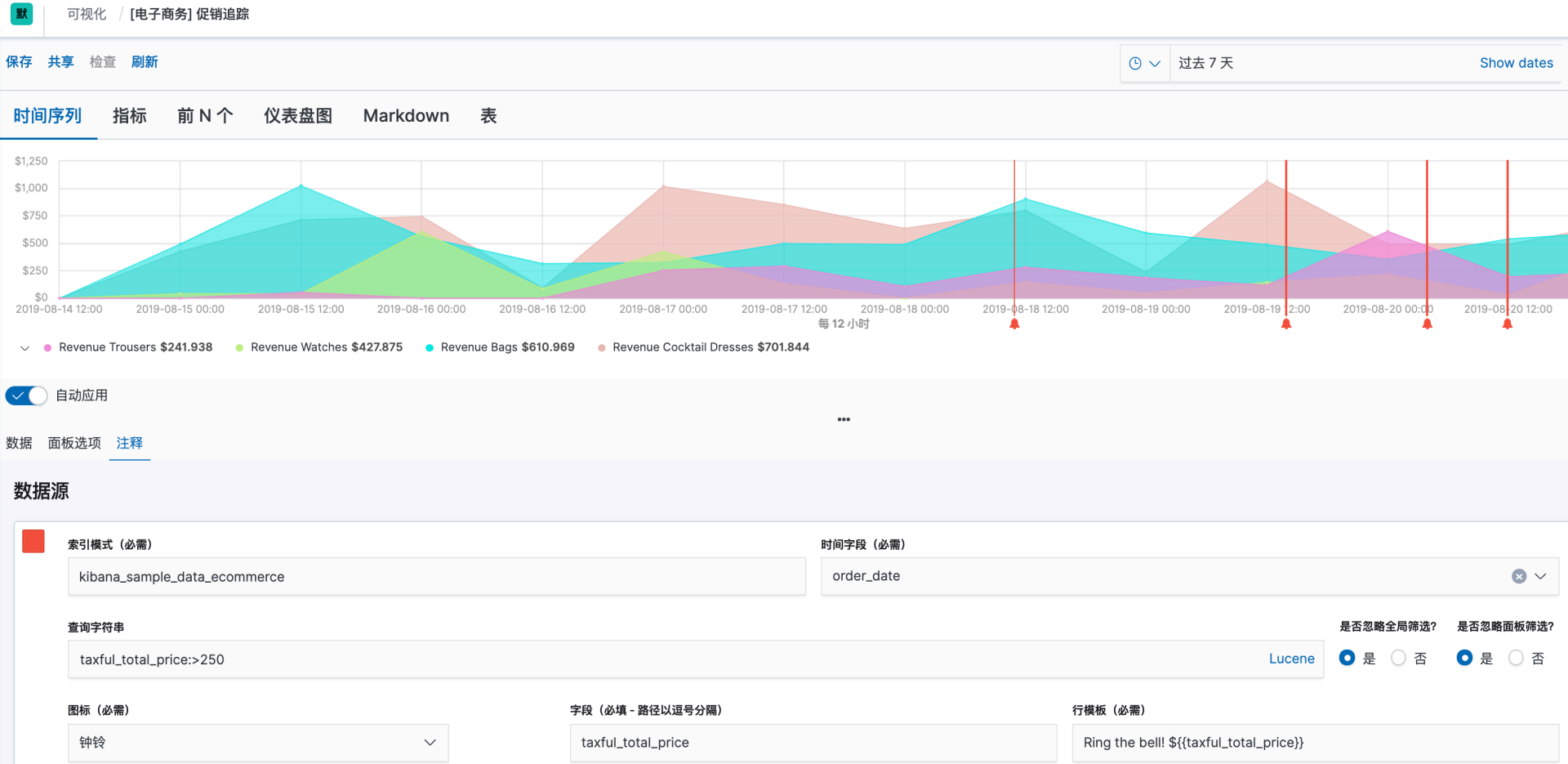
Kibana 7.3

elastic

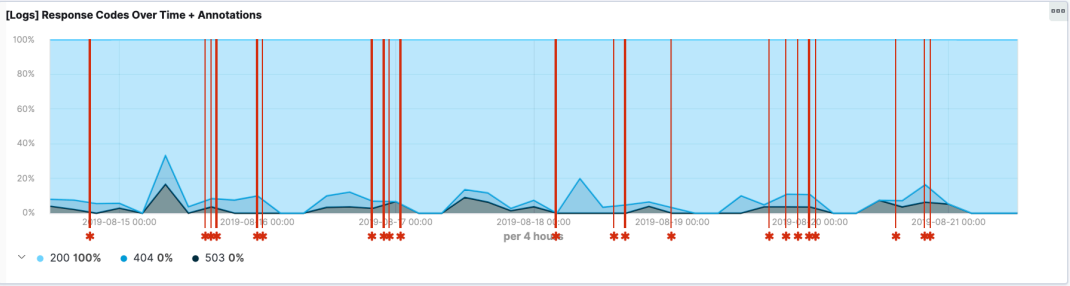
数据展现 – 日志分析

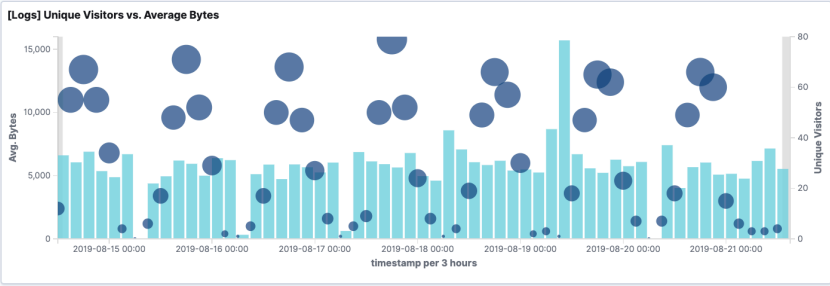

新建 保存 打开 共享 检查
Filters 搜索
+ 添加筛选
编辑筛选
编辑为查询 DSL
字段
运算符
agent.keyword
是
值
选择值
Mozilla/5.0 (X11; Linux x86_64; rv:6.0a1) Gecko/201...
Mozilla/5.0 (X11; Linux i686) AppleWebKit/534.24 (...
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;...
Filters geo.dest:
KQL
"CN"
"IN"
"US"
"ID"
"BR"
"PK"
"BD"
"NG"
"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

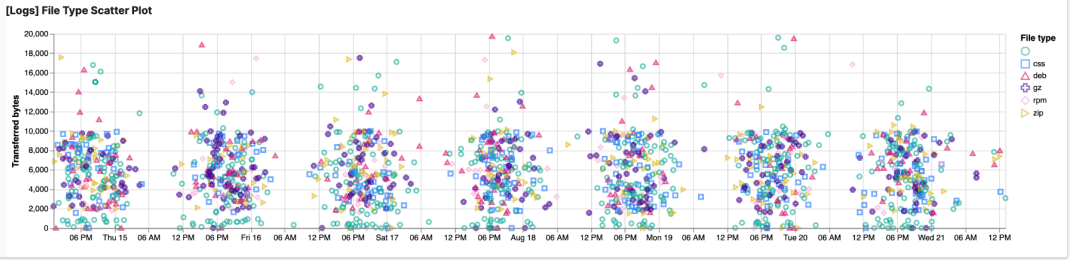
数据展现 - 时序数据分析器



数据展现 – 丰富的图表

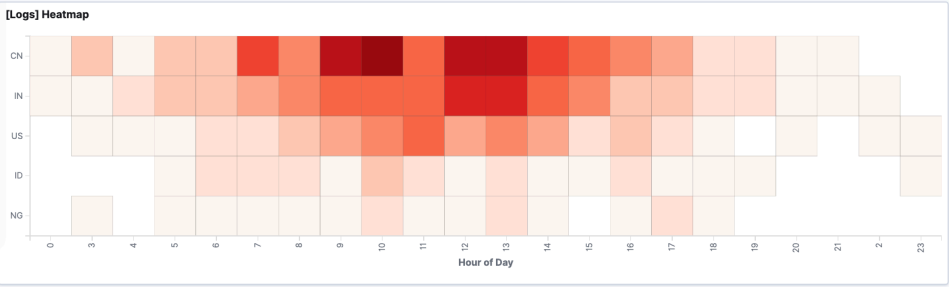


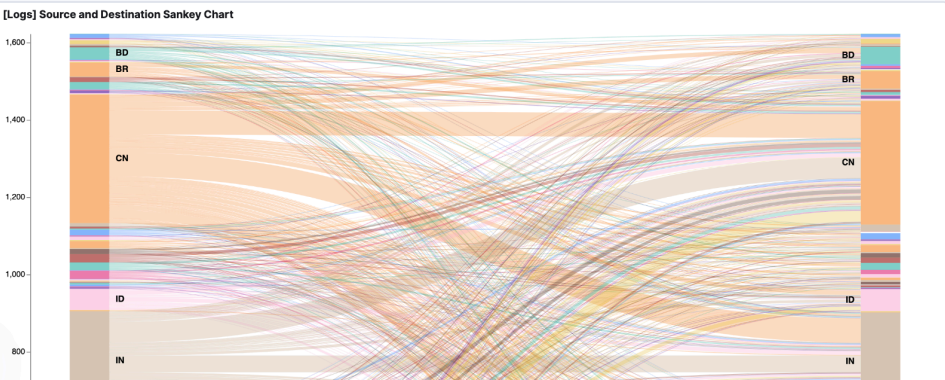


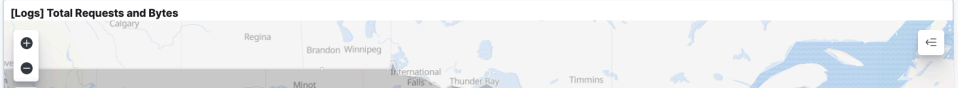


[Logs] Host, Visits and Bytes Table

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

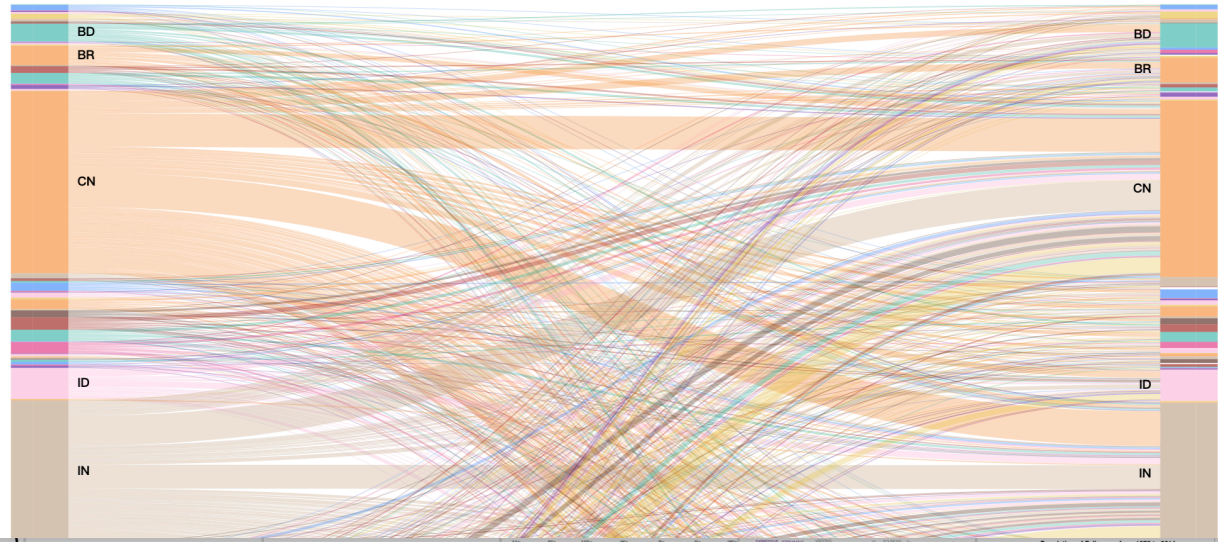


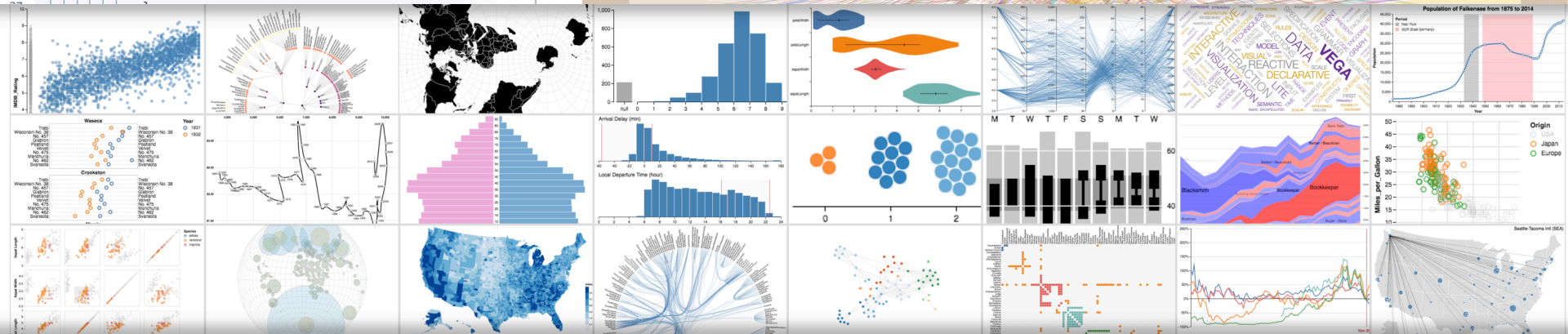




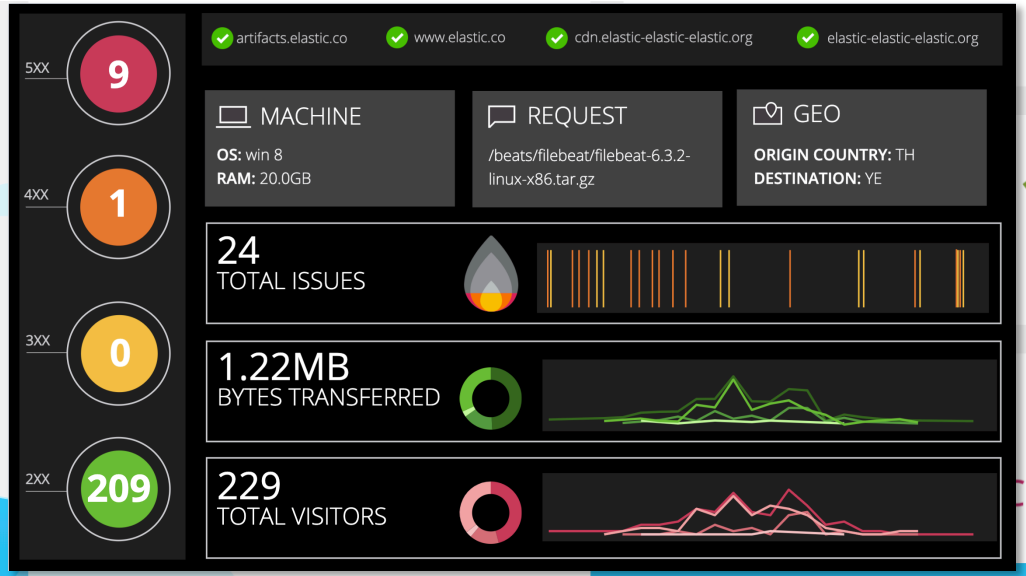
数据展现 – 丰富的开放生态，支持开源Vega图表组件

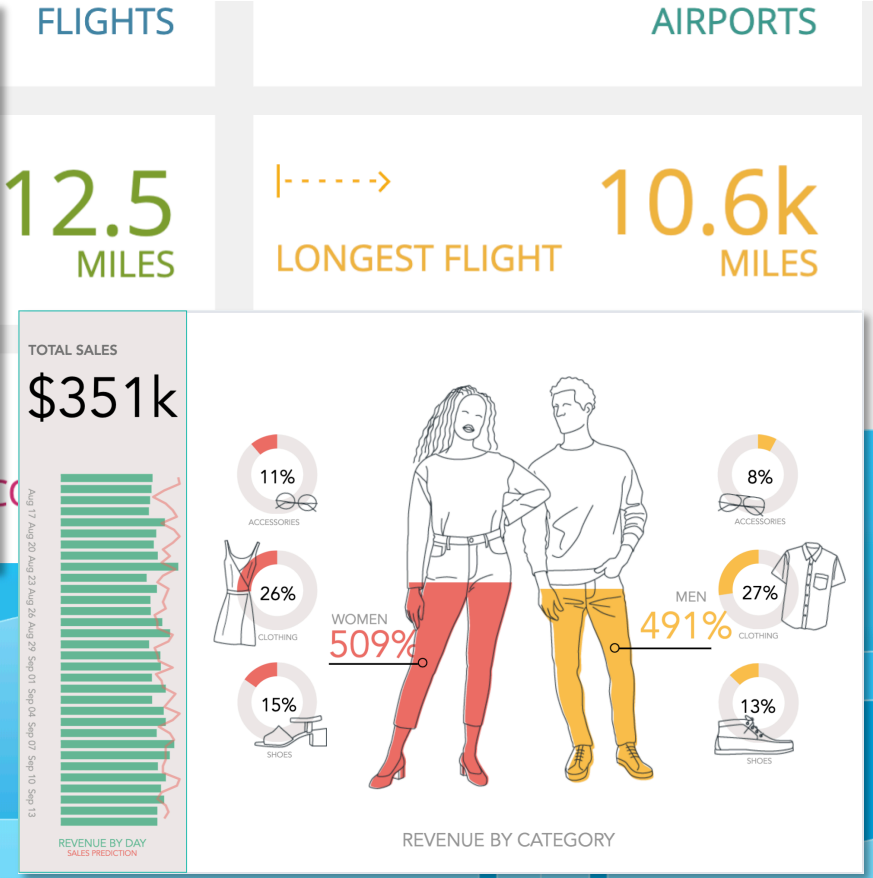
```
{
  $schema: https://vega.github.io/schema/vega/v3.0.json
  data: [
  {
    // query ES based on the currently selected time range and
       filter string
    name: rawData
    url: {
      %context%: true
      %timefield%: timestamp
      index: kibana_sample_data_logs
      body: {
        size: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



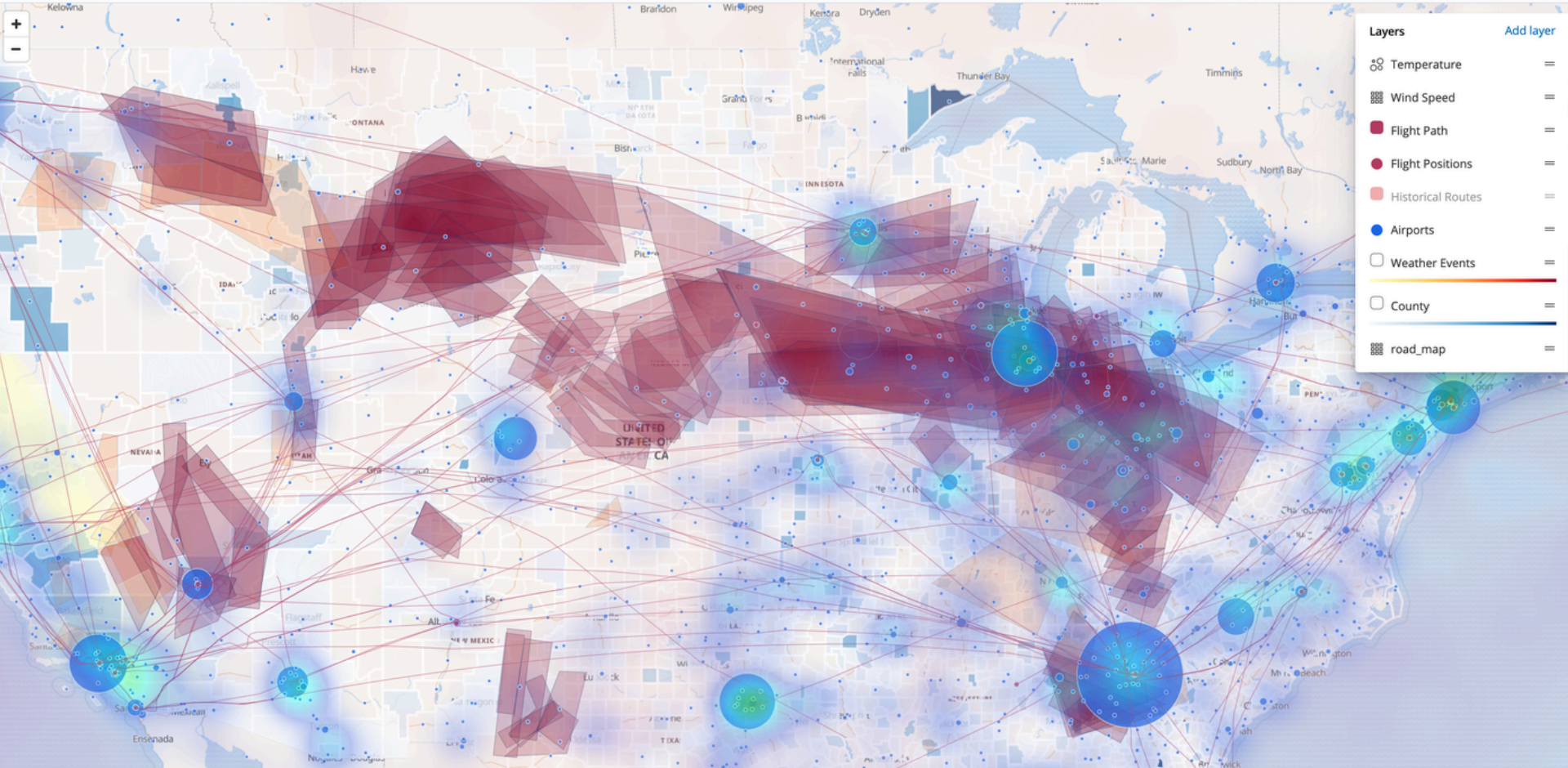


数据展现 – 像PPT一样的全动态大屏报表

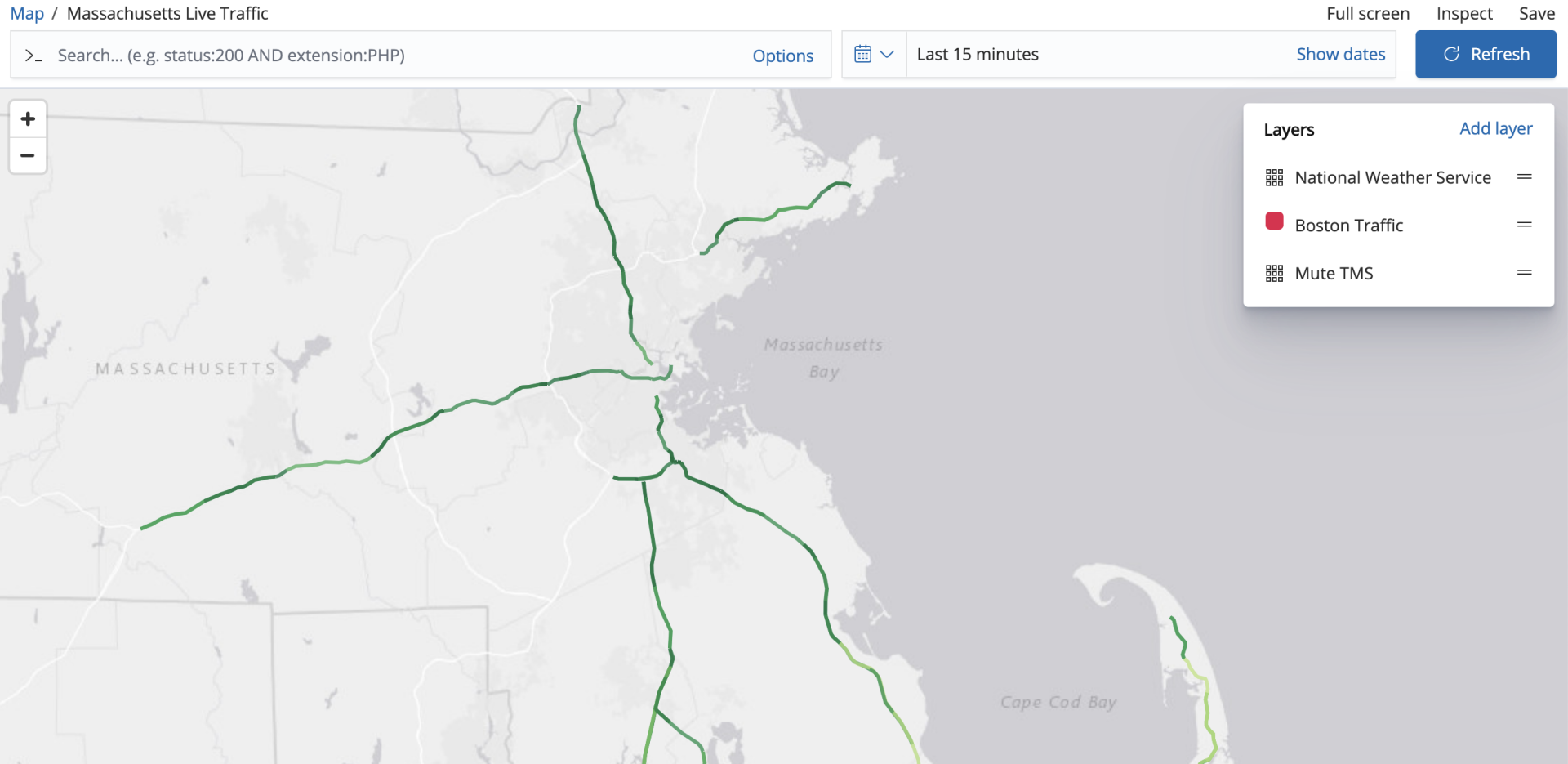




数据展现 – 在地图上分析数据



数据展现 – 地图上画路径也能做到

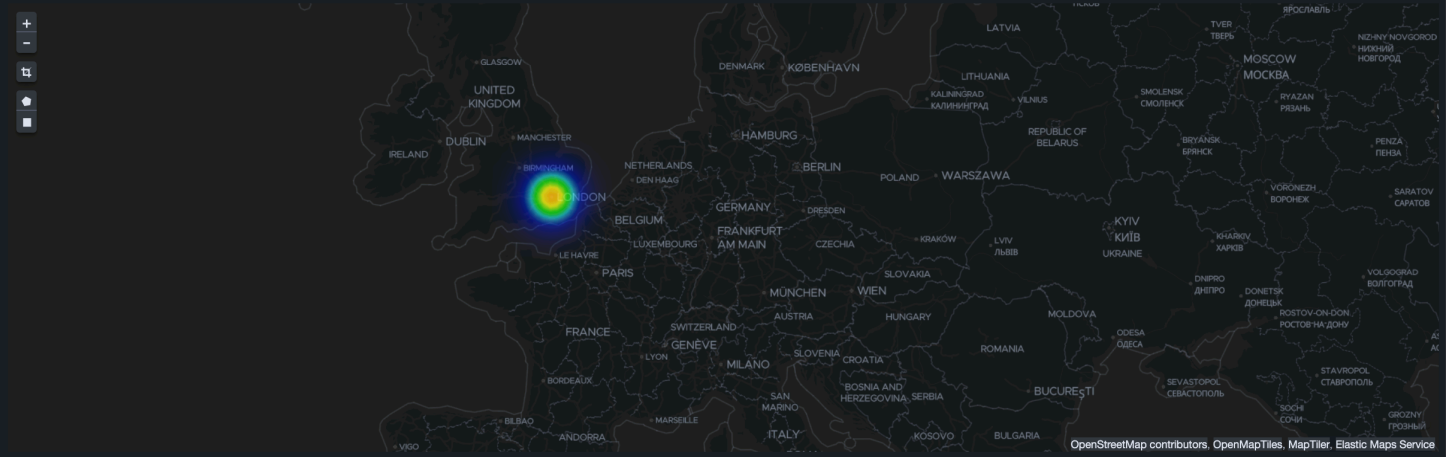


1,021	4	5	3	2
Total Attacks	Unique Rules Hit	Unique Sources	Source Attack Countries	Reporting Hosts

WAF - Chart of Top 10 Rules

- 911100
- 920180
- 949110
- 980130

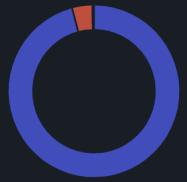
WAF - Attack Heat Map



WAF - Chart Of Severities

- 2
- 0
- 4

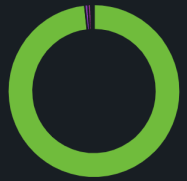
WAF - OS Pie Chart



- Other
- Mac OS X
- Linux

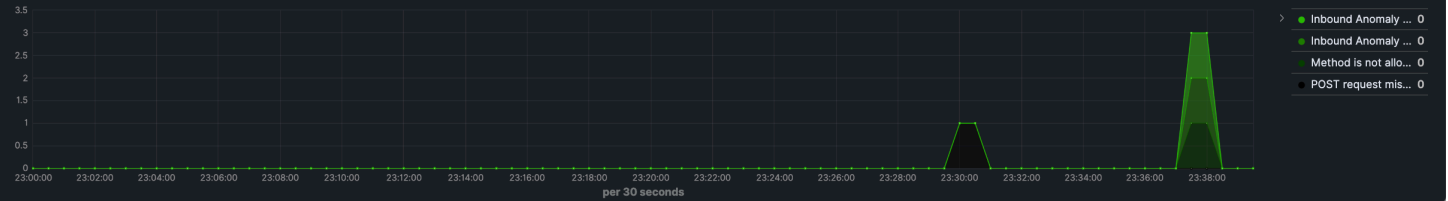
WAF - Events Over Time, By Severity

WAF - Top 5 Targeted URI's



- /login.php
- /api/case/AWiu25...
- /
- /api/case/AWiu25...
- /api/case/task/_st...

WAF - Messages Over Times



BCR Gates Open
(last 10 minutes)

97% (519) Accepted
3% (18) Rejected

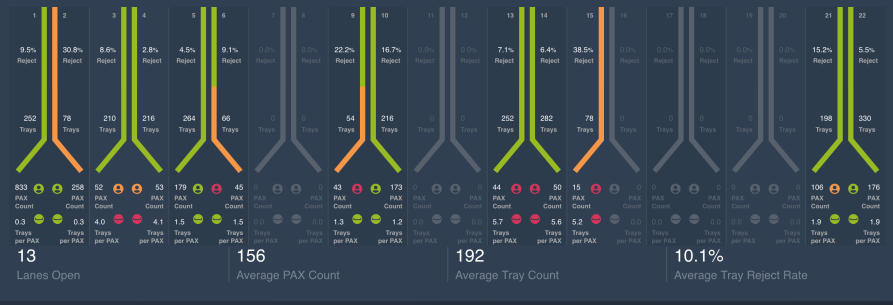
PAX Count
(last minute)

BCR Scans
(last hour)

IDL Occupancy
(last 5 minutes)

Projected Queue Time
(next minute)

Lane Usage
(projected hour)



13
Lanes Open

156
Average PAX Count

192
Average Tray Count

10.1%
Average Tray Reject Rate

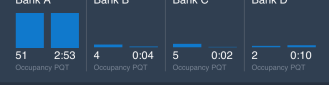
The information in this dashboard is sample data only

London Stansted Airport

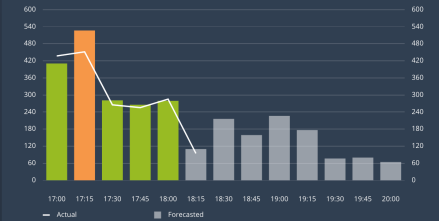
BCR Gates Open
(last hour)

BCR Scans
(last 2 hours)

Security Queue Zone Status
(current)



Passenger Count
(last hour)

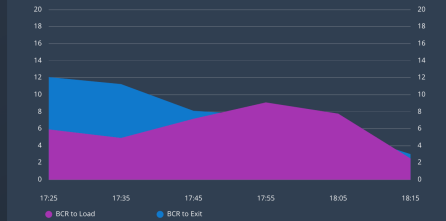


141
Actual

255
Forecast

-45%
Variance

Security Queue
(last hour)

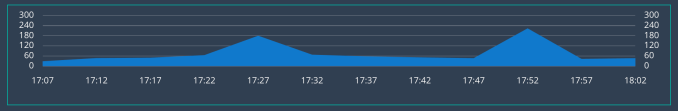


The information in this dashboard is sample data only

London Stansted Airport

IDL Occupancy
(last 5 minutes)

BCR Scans
(last hour)



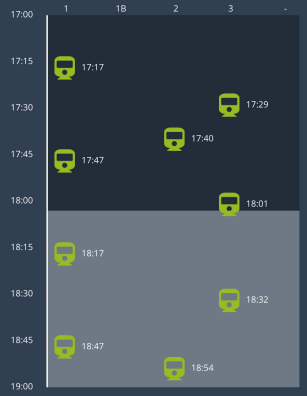
Departures
(next 3 hours)

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)



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

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

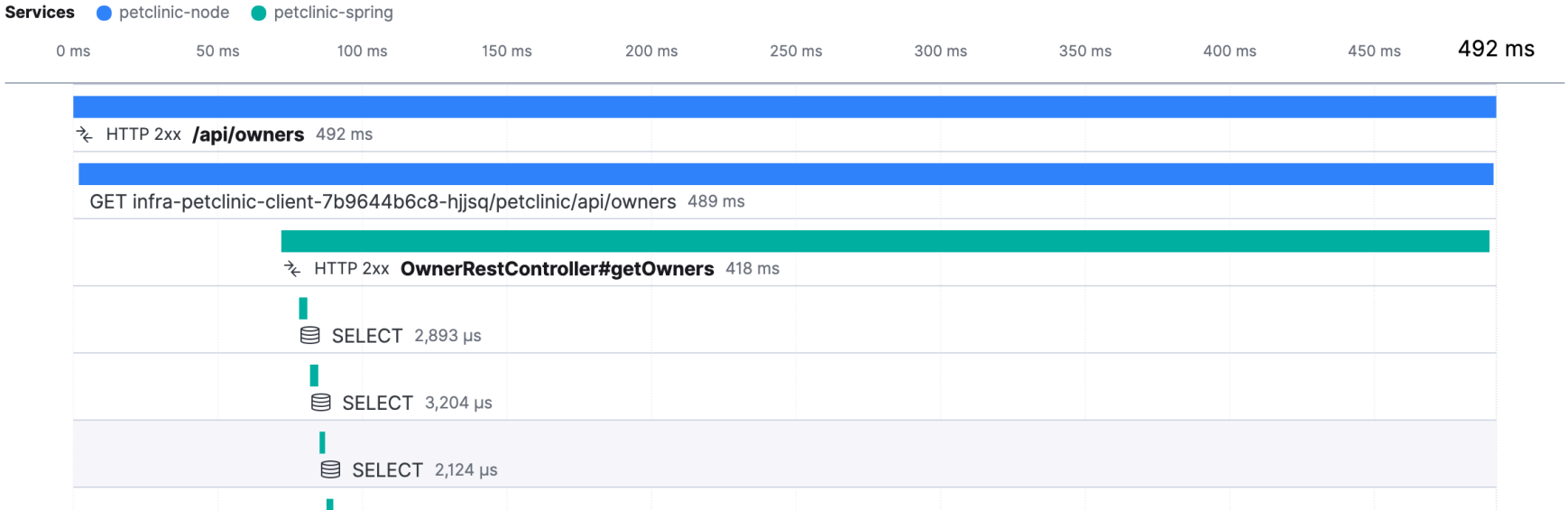
Actions | View full trace

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

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

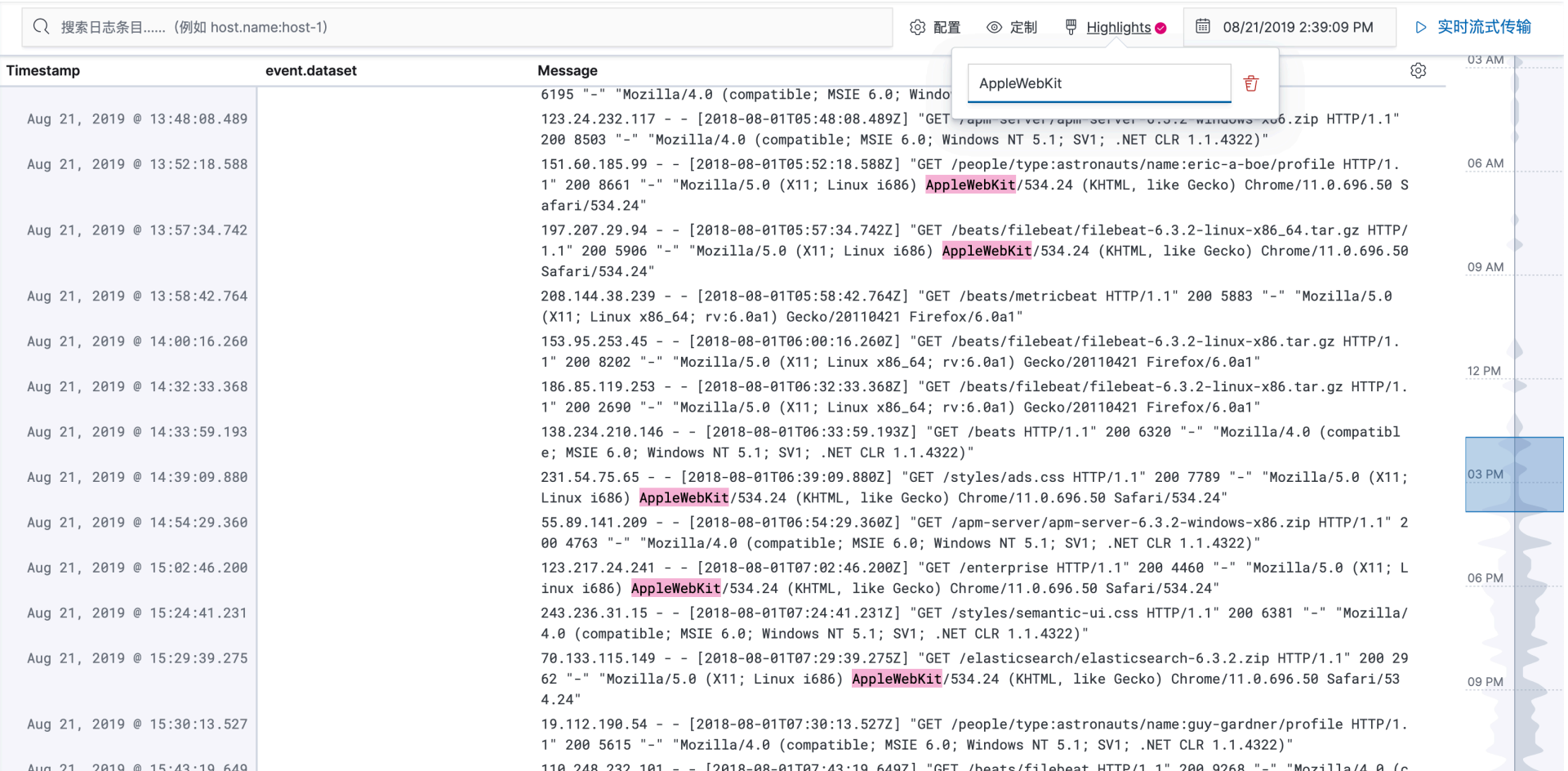
Duration	% of trace	Result	Errors	User ID
492 ms	N/A	HTTP 2xx	None	lwoollaston52

Timeline | Metadata

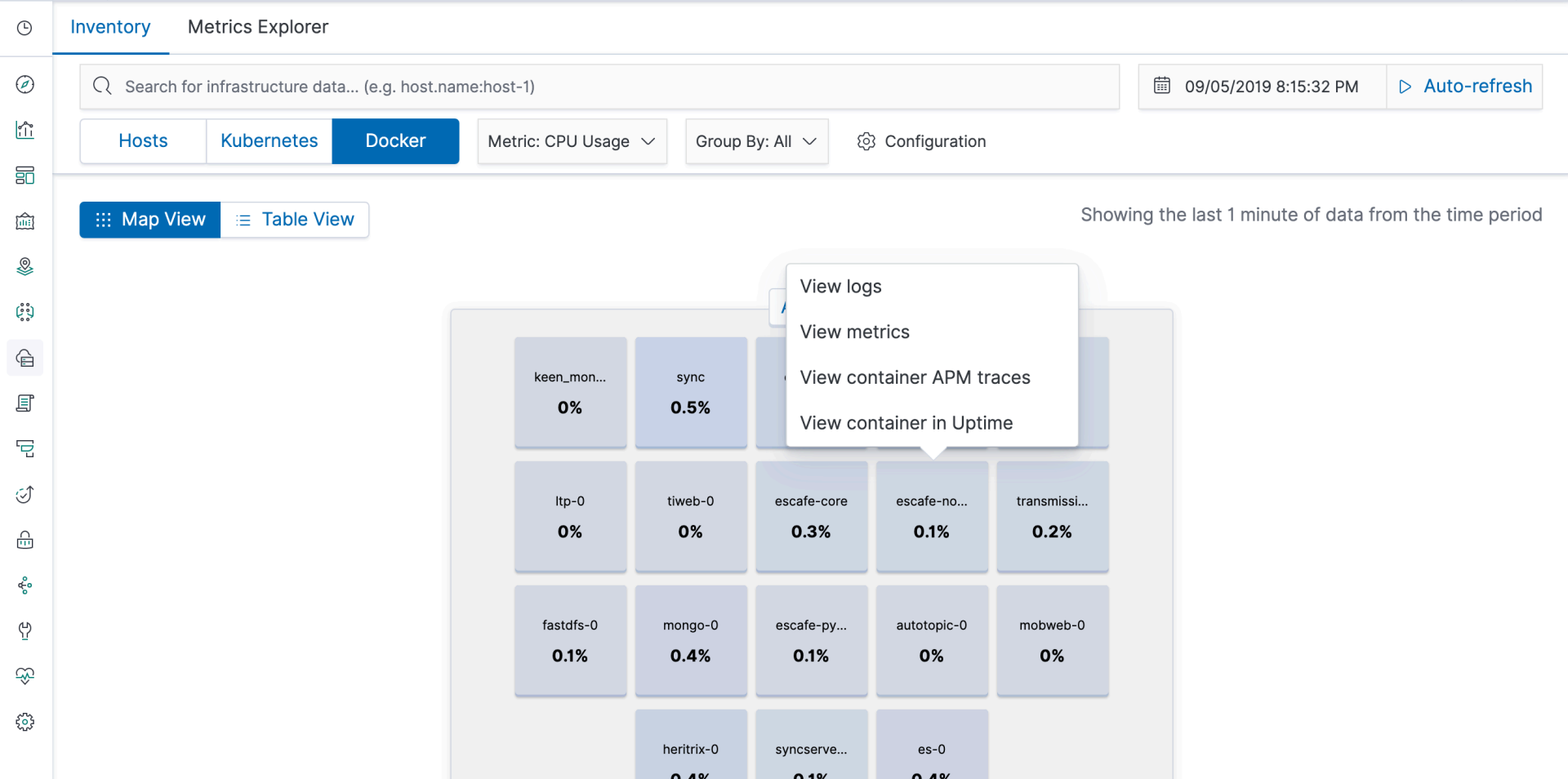


其它Kibana APP

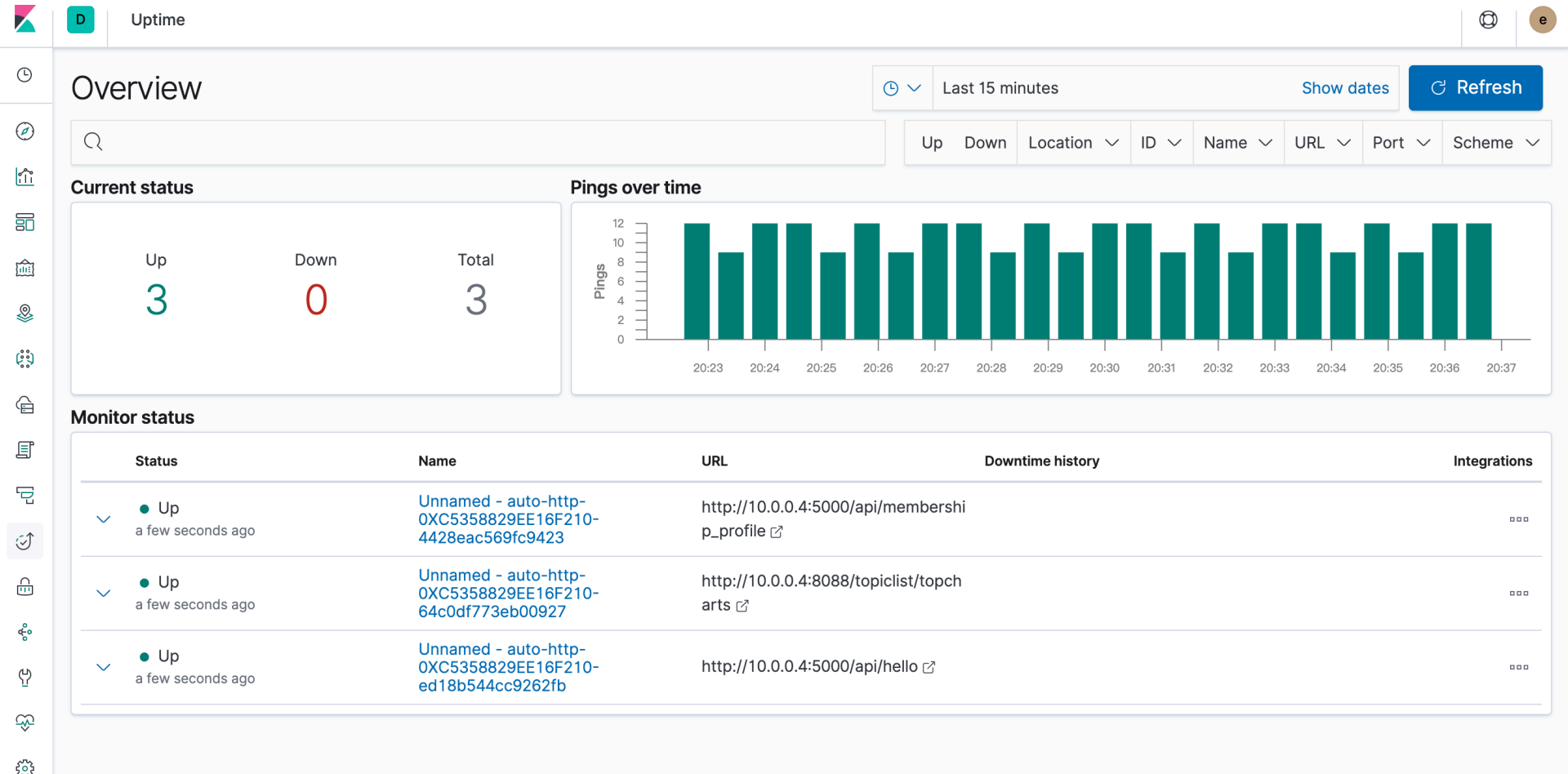
Logs 实时流式日志查看器



Infrastructure



Uptime


D
Uptime
e
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


Grafana


pentaho
Spark
Streaming


Apache Flink


fluentd


FLUME


Elastic


+ a b | e a u


HIVE


ZABBIX

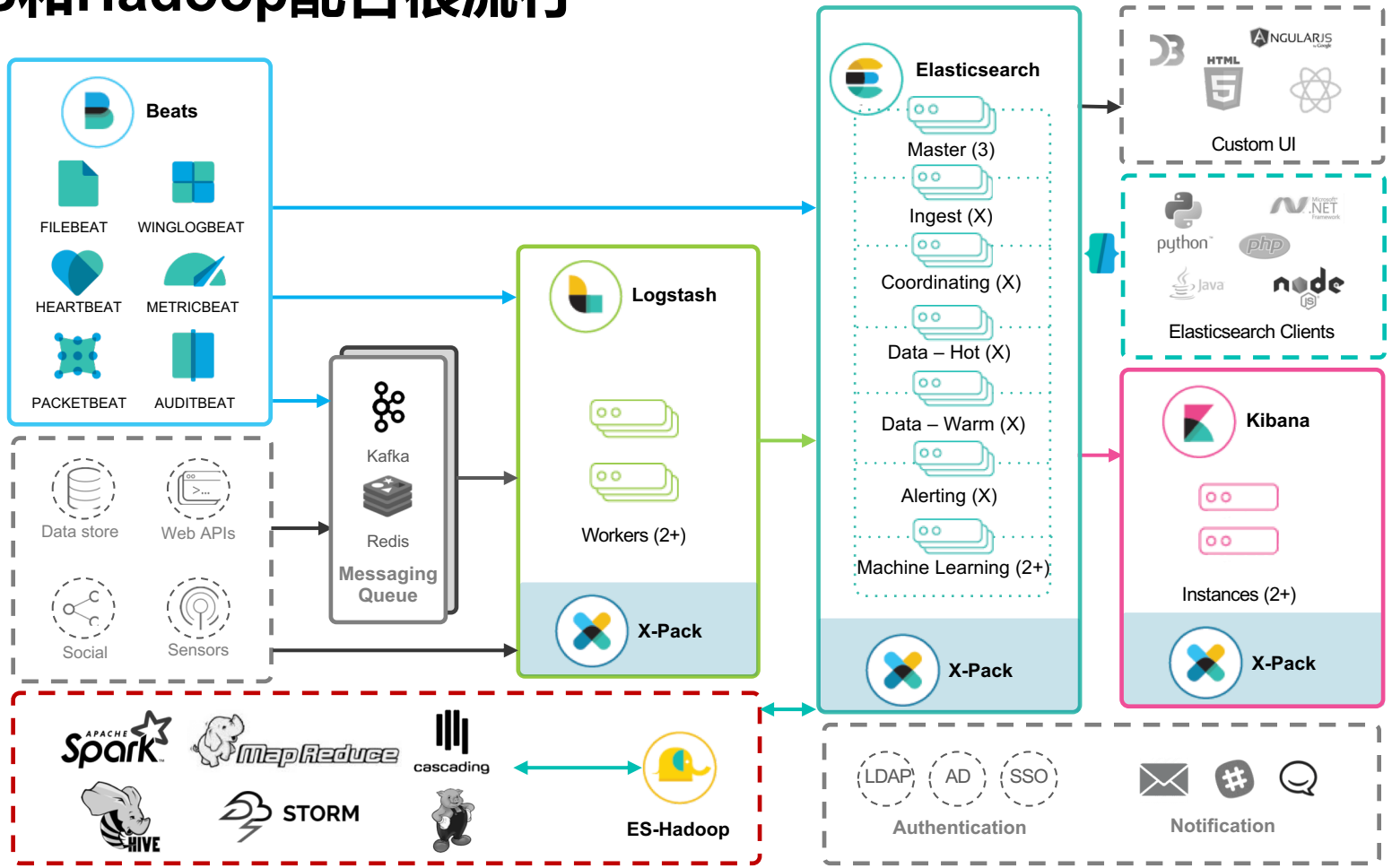

Prometheus


CISCO


paloalto
NETWORKS


hadoop

ES和Hadoop配合很流行

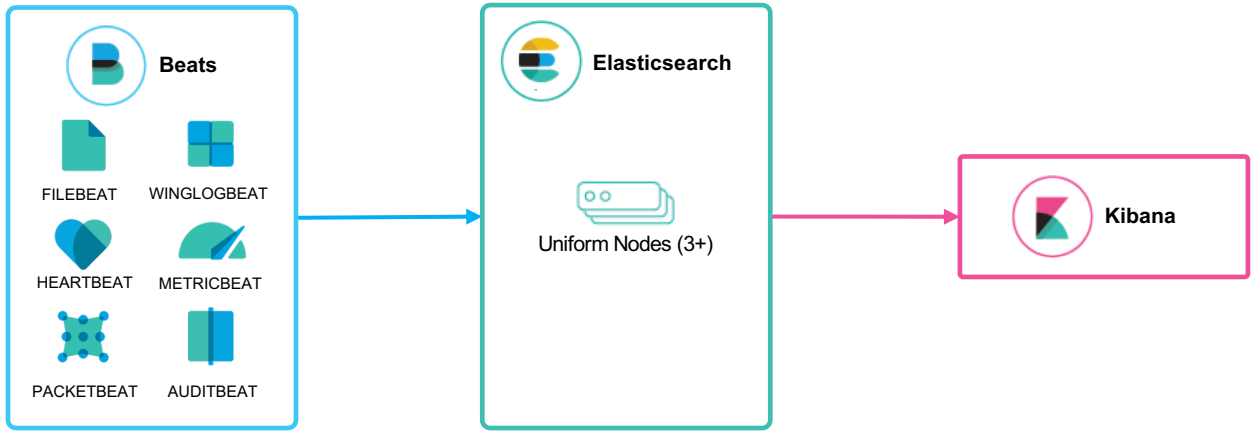


elastic

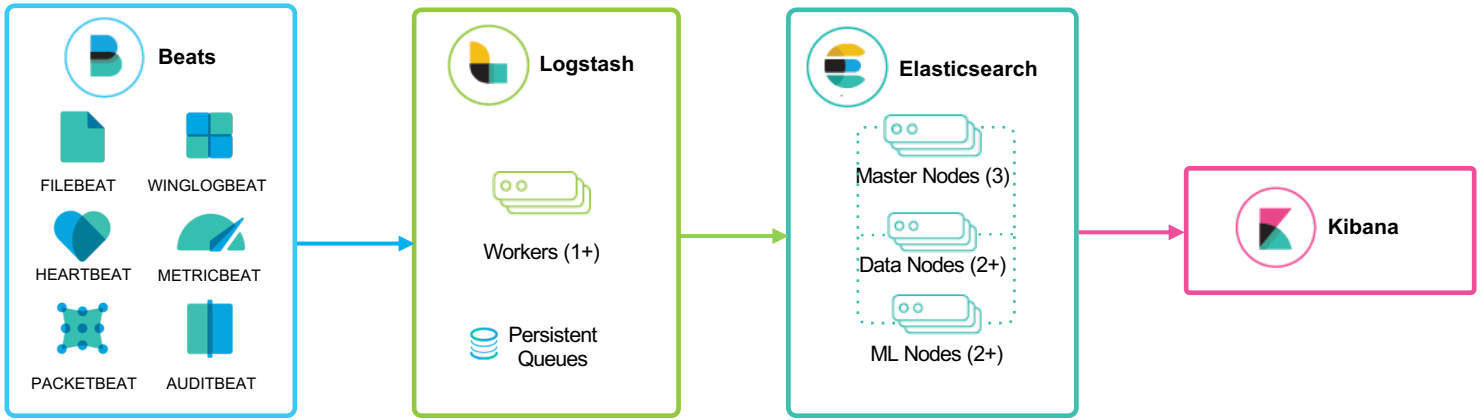
日志指标APM
整体架构

elastic

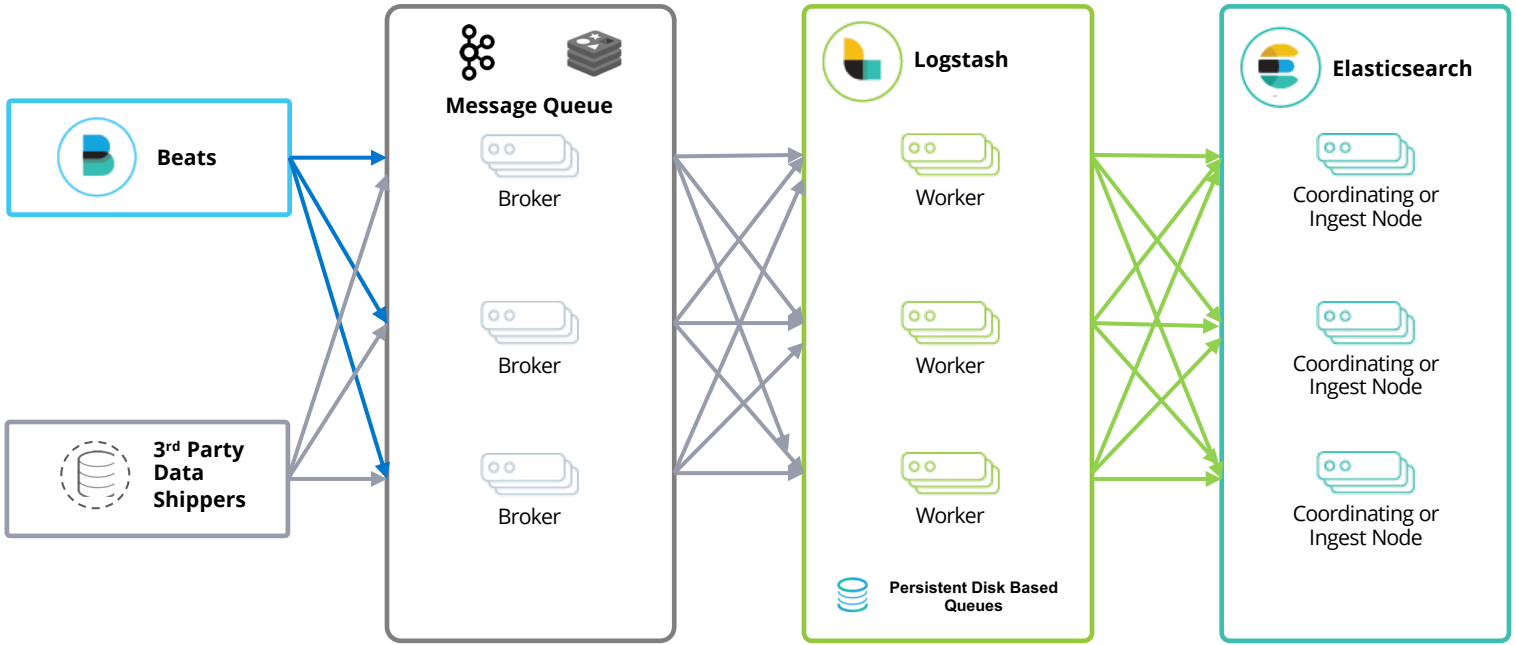
整体架构图



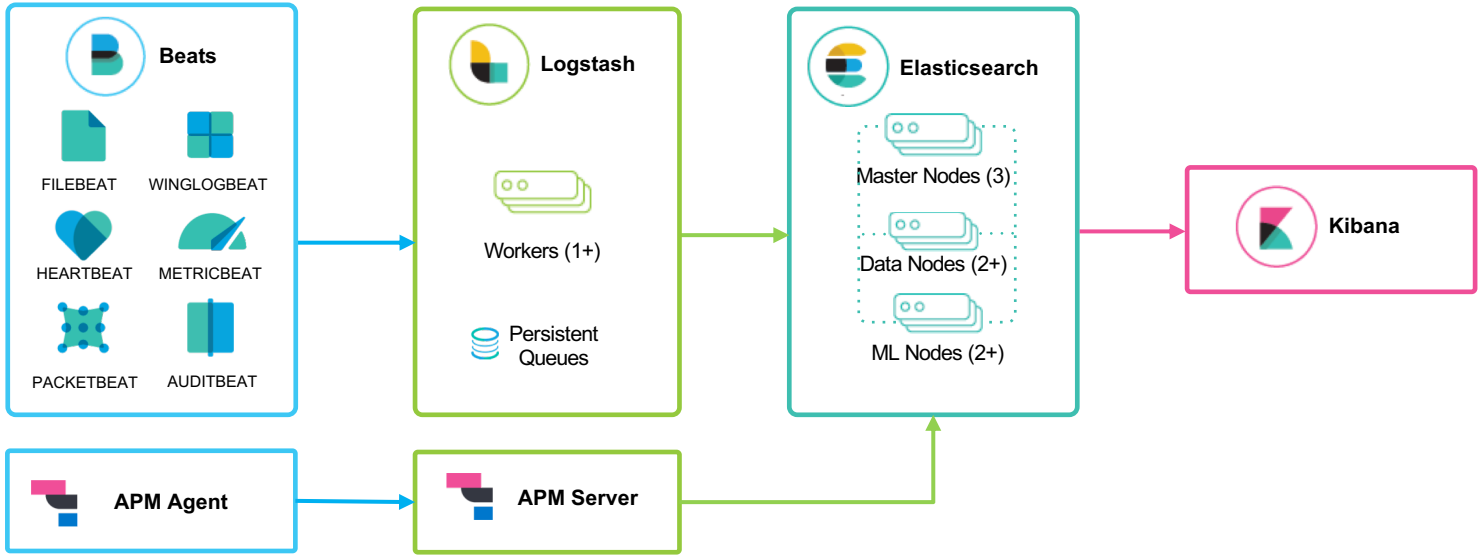
整体架构图



更复杂一些的架构图



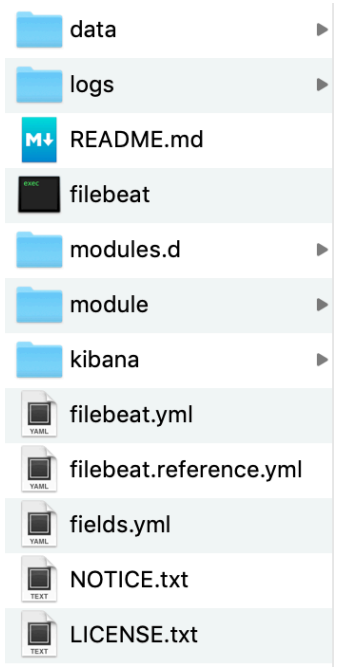
整体架构图



Filebeat使用详解

elastic

Filebeat详解



模块开关，配置

模块文件

Kibana Dashboard模板

Filebeat 配置文件

Filebeat module作用

对一些常用的日志格式做到开箱即用

- 缺省的配置
- Elasticsearch pipeline定义
- Kibana Dashboard配置

Filebeat命令行

```
./filebeat --help
```

```
Usage:
  filebeat [flags]
  filebeat [command]


Available Commands:
  enroll      Enroll in Kibana for Central Management
  export      Export current config or index template
  generate    Generate Filebeat modules, filesets and fields.yml
  help        Help about any command
  keystore    Manage secrets keystore
  modules     Manage configured modules
  run         Run filebeat
  setup       Setup index template, dashboards and ML jobs
  test        Test config
  version     Show current version info
```

Filebeat命令行举例

```
./filebeat modules list
```

```
./filebeat modules enable system
```

```
./filebeat modules disable system
```

elastic

Filebeat重要配置

```
filebeat.inputs:
- type: log

  # Change to true to enable this input configuration.
  enabled: false

  # Paths that should be crawled and fetched. Glob based paths.
  paths:
    - /var/log/*.log

  # Optional additional fields. These fields can be freely picked
  # to add additional information to the crawled log files for filtering
  #fields:
  #  level: debug
  #  review: 1
```

```
setup.kibana:

  # Kibana Host
  # Scheme and port can be left out and will be set to the default (http and 5601)
  host: "localhost:5601"

  # Kibana Space ID
  # ID of the Kibana Space into which the dashboards should be loaded. By default,
  # the Default Space will be used.
  #space.id:
```

elastic

Filebeat重要配置

```
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["localhost:9200"]

  # Optional protocol and basic auth credentials.
  #protocol: "https"
  #username: "elastic"
  #password: "changeme"
```

```
output.logstash:
  # The Logstash hosts
  #hosts: ["localhost:5044"]
```

Lab1 Filebeat Metricbeat使用

APM 使用详解

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, 等等.

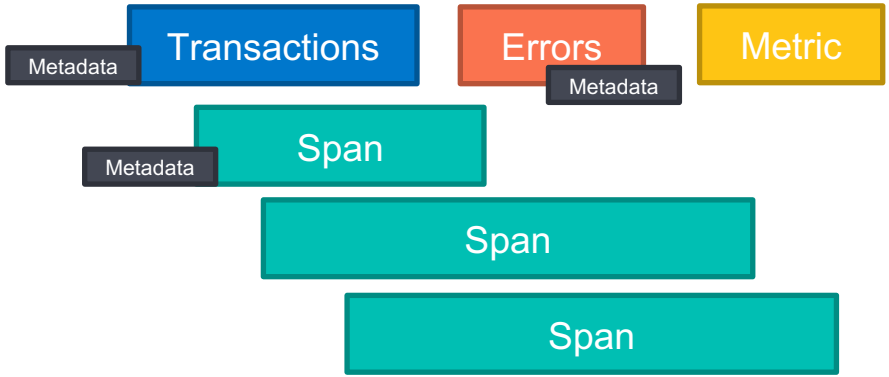
有专门UI

APM 工作流程耗时图
分布式的追踪

仅仅多了一些索引

和其它数据关联
借助于ES的功能

APM Date model



APM Agent 举例 java agent

加载 java apm agent的三种方式

方式一

```
java -javaagent:/path/to/elastic-apm-agent-<version>.jar
```

方式二

```
java -jar apm-agent-attach-standalone.jar --pid 42
```

方式三

```
import co.elastic.apm.attach.ElasticApmAttacher;
import org.springframework.boot.SpringApplication;

@SpringBootApplication
public class MyApplication {
   public static void main(String[] args) {
      ElasticApmAttacher.attach();
      SpringApplication.run(MyApplication.class, args);
   }
}
```

elastic

Java Agent Supported Technologies

web-frameworks	Servlet API, Spring Web MVC, Spring Boot, JAX-RS, JAX-WS
Application Servers Servlet Containers	Tomcat, Jboss EAP, Jetty, WebSphere, WebLogic, WildFly, …
Data Stores	JDBC, Elasticsearch, Hibernate Search
Networking frameworks	Apache HttpClient, Spring RestTemplate, OkHttp …
Asynchronous frameworks	ExecutorService
Messaging frameworks	JMS
Scheduling frameworks	Scheduling Annotation, Quzrtz
Logging frameworks	slf4j

不支持的可以通过API来创建 Transactions 和 Spans

Java Agent Metric

System Metric	JVM Metric
system.cpu.total.norm.pct	jvm.memory.heap.used
system.process.cpu.total.norm.pct	jvm.memory.heap.committed
system.memory.total	jvm.memory.heap.max
system.memory.actual.free	jvm.memory.non_heap.used
system.process.memory.size	jvm.memory.non_heap.committed
…	…

Java Agent 配置举例

```
service_name=escafe-core
application_packages=org.cafe.web.controller
server_urls=http://10.0.0.2:8200
trace_methods=com.cafe.web.controller.OrderReceiver#process
```

```
trace_methods 举例
org.example.* [1.4.0]Added in 1.4.0. Omitting the method is possible since 1.4.0
org.example.*#* (before 1.4.0, you need to specify a method matcher)
org.example.MyClass#myMethod
org.example.MyClass#myMethod()
org.example.MyClass#myMethod(java.lang.String)
org.example.MyClass#myMe*od(java.lang.String, int)
private org.example.MyClass#myMe*od(java.lang.String, *)
* org.example.MyClas*#myMe*od(*.String, int[])
public org.example.services.*Service#*
public @java.inject.ApplicationScoped org.example.*
public @java.inject.* org.example.*
public @@javax.enterprise.context.NormalScope org.example.*
```

elastic

APM Agent 举例 python agent

```
import elasticapm
from elasticapm.contrib.flask import ElasticAPM

app = Flask(__name__)

app.config['ELASTIC_APM'] = {
    'SERVICE_NAME': 'escafe-python',
    'SERVER_URL': config['elasticapm.url'],
    'INSTRUMENT': config['elasticapm.instrument']
}
apm = ElasticAPM(app)

@app.route("/api/hello")
def hello():
    do_calculation()
    return "Hello World!”

@elasticapm.capture_span()
def do_calculation():
    if avg_service_time != 0:
        delay = abs(gauss(avg_service_time, stdev_service_time))
        time.sleep(delay)
    return
```

elastic

Logstash 使用详解

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

Logstash 工作原理

file
syslog
redis
beats
…

grok
mutate
drop
clone
geoip

file
kafka
elasticsearch
stdout

Logstash配置文件基本结构

```
input {
  file {
    path => "/tmp/access_log"
    start_position => "beginning"
  }
}

filter {
  if [path] =~ "access" {
    mutate { replace => { "type" => "apache_access" } }
    grok {
      match => { "message" => "%{COMBINEDAPACHELOG}" }
    }
  }
  date {
    match => [ "timestamp" , "dd/MMM/yyyy:HH:mm:ss Z" ]
  }
}

output {
  elasticsearch {
    hosts => ["localhost:9200"]
  }
  stdout { codec => rubydebug }
}
```

Multiple Pipelines

pipelines.yml

```
- pipeline.id: my-pipeline_1
  path.config: "/etc/path/to/p1.config"
  pipeline.workers: 3

- pipeline.id: my-other-pipeline
  path.config: "/etc/different/path/p2.cfg"
  queue.type: persisted
```

grok基础

```
55.3.244.1 GET /index.html 15824 0.043
```

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

内置pattern定义 https://github.com/elastic/logstash/tree/v1.4.2/patterns

```
IP (?:%{IPV6}|%{IPV4})
WORD \b\w+\b
URIPATHPARAM %{URIPATH}(?:%{URIPARAM})?
NUMBER (?:%{BASE10NUM})
BASE10NUM (?<![0-9.+-])(?>[+-]?(?:(?:[0-9]+(?:\.[0-9]+)?)|(?:\.[0-9]+)))
```

```
grok {
   match => { "message" => ["%{SYSLOGTIMESTAMP:[system][syslog][timestamp]}
%{SYSLOGHOST:[system][syslog][hostname]}
%{DATA:[system][syslog][program]}(?:\[%{POSINT:[system][syslog][pid]}\])?:
%{GREEDYMULTILINE:[system][syslog][message]}"] }
   pattern_definitions => { "GREEDYMULTILINE" => "(.|\n)*" }
   patterns_dir => ["./patterns"]
}

# contents of ./patterns/postfix:
POSTFIX_QUEUEID [0-9A-F]{10,11}
```

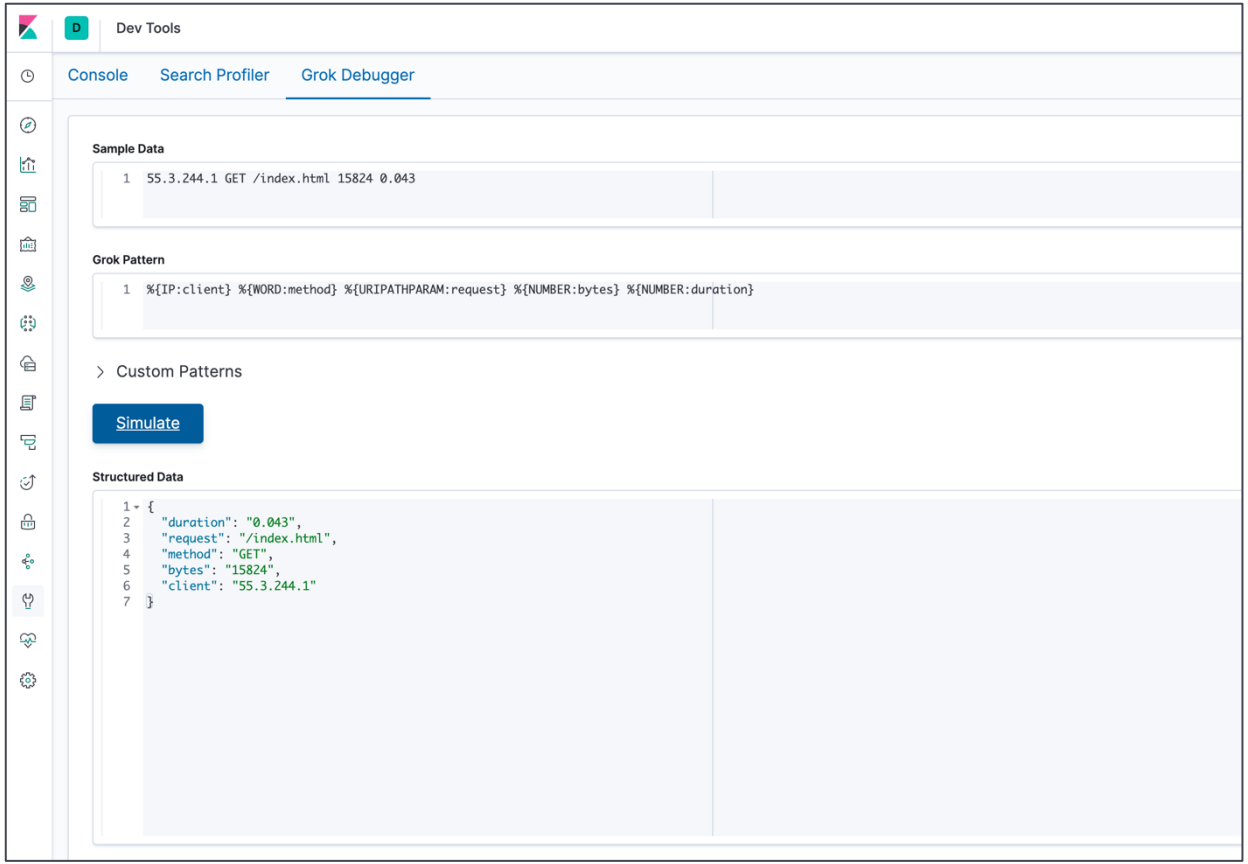
可以是数组

定义正则

正则文件

elastic

grok测试器



elastic

Lab2 Logstash使用

Kibana可视化分析

elastic

END