



与「十」俱进,码出未来

2018源创会年终盛典

主办方  开源中国
oschina.net



基于 Elastic Stack 的 Logging、Metrics 和 APM 分析

曾勇

Dec 2018

Logs

Metrics

```

Pages: 0.00, 0.00, 0.00:
sses: 16 sleeping, 1 on CPU
ent: 0.0% used, 0.0% nice,
29M net, 6028M wired, 8336K

```

COMMAND	PRI	NICE	SIZE	RES	STATE	TIME	CPU	MEM	IO	NAME
at	13	0	17M	1800K	CPU	0:00	0.00%	0.00%	0.00%	at
at	06	0	0K	2912K	atath	0:00	0.00%	0.00%	0.00%	at
at	85	0	22M	6128K	power	0:00	0.00%	0.00%	0.00%	at
at	05	0	40M	3012K	kqueue	0:00	0.00%	0.00%	0.00%	at
atfix	85	0	48M	3856K	kqueue	0:00	0.00%	0.00%	0.00%	atfix
atfix	05	0	40M	3020K	kqueue	0:00	0.00%	0.00%	0.00%	atfix
at	85	0	54M	3736K	mail	0:00	0.00%	0.00%	0.00%	at
at	05	0	20M	1076K	kqueue	0:00	0.00%	0.00%	0.00%	at
at	85	0	13M	1740K	mail	0:00	0.00%	0.00%	0.00%	at
at	85	0	13M	1352K	ttynw	0:00	0.00%	0.00%	0.00%	at
at	85	0	13M	1352K	ttynw	0:00	0.00%	0.00%	0.00%	at
at	85	0	13M	1352K	ttynw	0:00	0.00%	0.00%	0.00%	at
at	85	0	11M	1320K	named.p	0:00	0.00%	0.00%	0.00%	at
at	85	0	13M	1316K	wait	0:00	0.00%	0.00%	0.00%	at
at	05	0	15M	1104K	kqueue	0:00	0.00%	0.00%	0.00%	at
at	85	0	11M	1072K	select	0:00	0.00%	0.00%	0.00%	at
at	05	0	10M	1020K	kqueue	0:00	0.00%	0.00%	0.00%	at



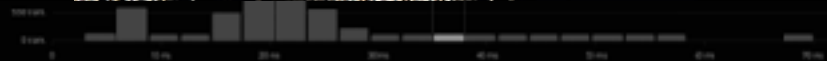
21:04:51

[illegible]

10 64 100 104 108 112 116 120 124 128 132 136 140 144 148 152 156 160

It is possible to [this is expected for demons without handle to


longestInterval_block: unexpected switch value
toIdentify: articleType: dominant: 1



Transaction samples

© 2004 Blackwell Publishing Ltd *Journal of Internal Medicine* 255: 101–108

psychology, communication, sociology

ADM  www.adm.com **SEARCH FOR PRODUCTS**

AI M AI M is a registered trademark of the American Institute of Mathematics.

APM

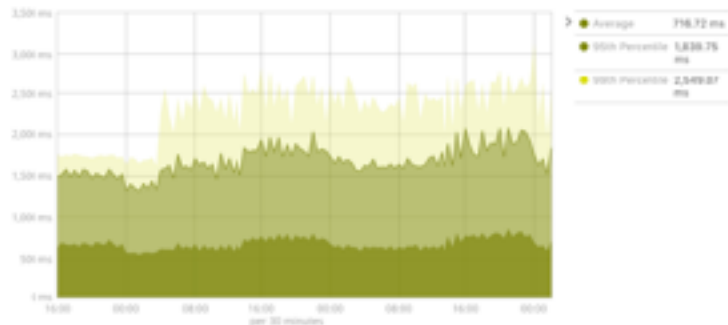
Logs、Metrics、APM 都在 Elastic Stack 的好处

统一的报表

相同的 UI 界面, KPI 摘要或是根因分析



Elastic[ON] 2018 - Site Response Times [APM]



Elastic[ON] 2018 - Memory Usage per Host [Metricbeat]



Elastic[ON] 2018 - Unusual Processes [Auditbeat]



Elastic[ON] 2018 - Traffic Between Hosts [Packetbeat]



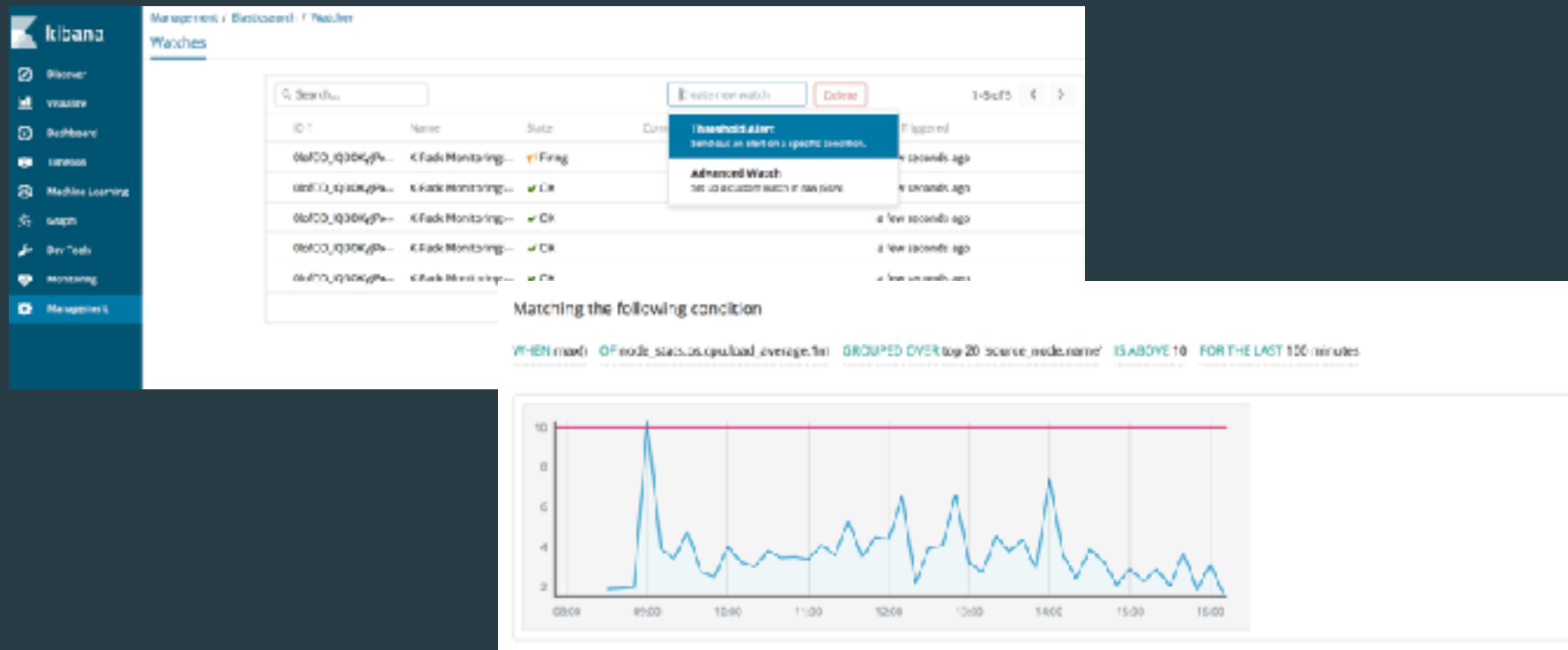
Elastic[ON] 2018 - Process Executions [Auditbeat]

1-50 of 9,935,707

Time	host.hostname	audit.kernel.action	audit.kernel.category	audit.kernel.new
January 22nd 2018, 10:59:57.628	proxy_01	executed	cat /etc/passwd	/usr/bin/cat
January 22nd 2018, 10:59:57.628	mysql	executed	cat /etc/passwd	/usr/bin/cat
January 22nd 2018, 10:59:57.628	web_server	executed	cat /etc/passwd	/usr/bin/cat
January 22nd 2018, 10:59:57.628	kibana	executed	cat /etc/passwd	/usr/bin/cat
January 22nd 2018, 10:59:57.628	proxy_01	executed	cat /etc/passwd	/usr/bin/cat
January 22nd 2018, 10:59:57.628	apm_server	executed	cat /etc/passwd	/usr/bin/cat
January 22nd 2018, 10:59:57.628	proxy_02	executed	cat /etc/passwd	/usr/bin/cat
January 22nd 2018, 10:59:57.628	mysql	executed	cat /etc/passwd	/usr/bin/cat

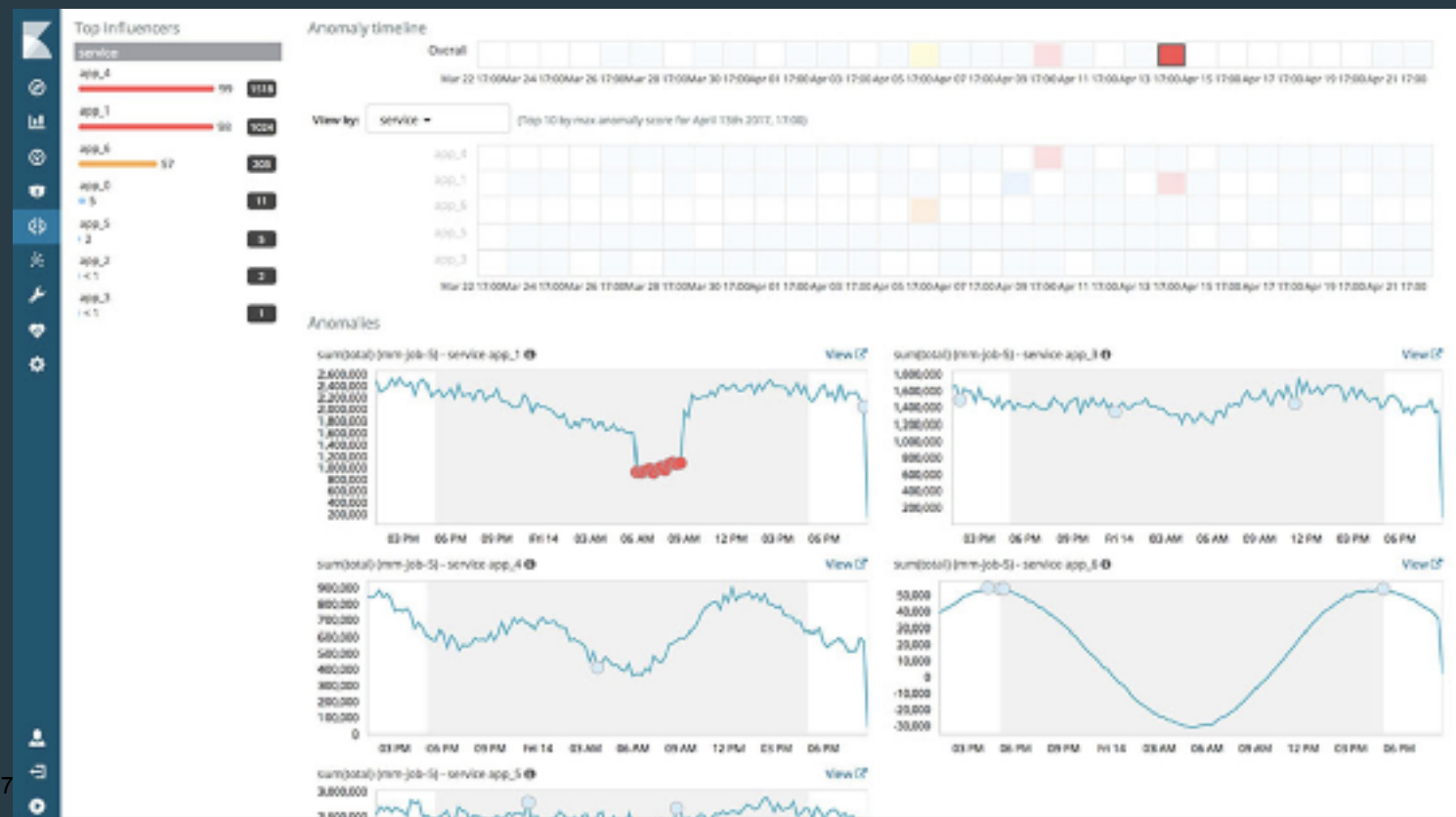
统一的告警

从任何数据的触发统一的告警



统一的机器学习

关联多个数据源，实现更智能的异常检测



实施成本

一站式技术解决方案节省运营成本



Metrics vs Logs

日志是事件在时间上的顺序记录

64.242.88.10 - - [07/Mar/2017:16:10:02 -0800] "GET /mailman/listinfo/hsdivision HTTP/1.1" 200 6291

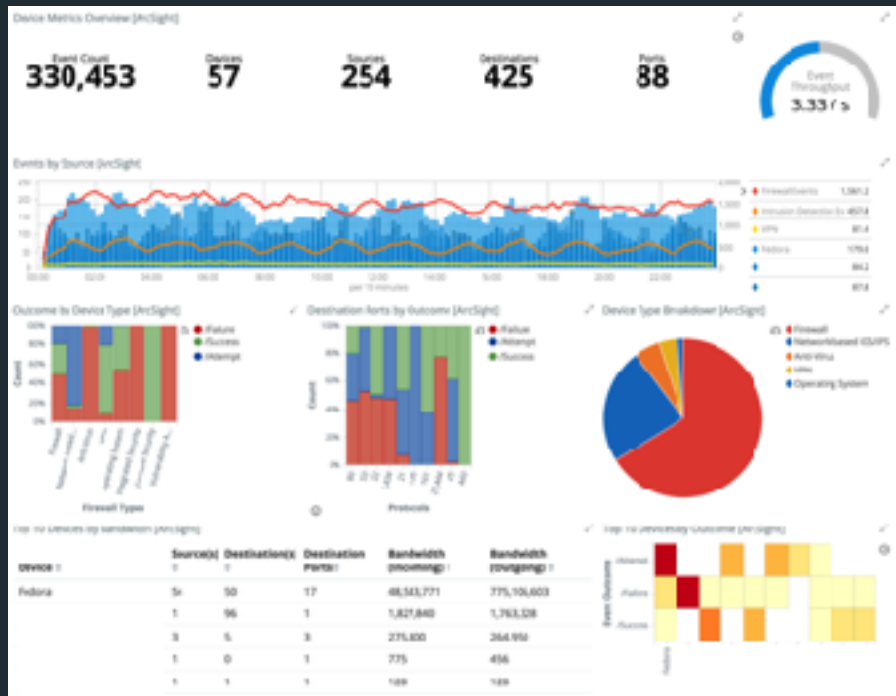
64.242.88.10 - - [07/Mar/2017:16:11:58 -0800] "POST /twiki/bin/view/TWiki/WikiSyntax HTTP/1.1" 404 7352

64.242.88.10 - - [07/Mar/2017:16:20:55 -0800] "GET /twiki/bin/view/Main/DCCAndPostFix HTTP/1.1" 200 5253

每个事件，输出当前正在发生的事情。

预置常用模块，开箱即用

- 常用数据类型，开箱即用
- 从数据到报表，一键直达
- 全自动的日志解析和处理
- 内置报表、告警规则和机器学习任务



Logging 模块

AUDITBEAT



FILEBEAT



WINLOGBEAT



Infrastructure

System

- Linux / MacOS
- Windows Events

Containers

- Docker
- Kubernetes

Applications

Databases

- MySQL
- PostgreSQL

Web servers

- Apache
- Nginx

Queues

- Kafka
- Redis

Audit data

- Filesystem
- System calls

Log 文件导入

自动的日志结构识别

kibana

Discover Visualize Dashboard Tools Monitoring Management

Machine Learning / File Data Visualizer (Experimental)

Job Management Anomaly Explorer Single Metric Viewer **Data Visualizer** Settings

File contents

First 300 lines

```
1 93.188.71.5 - - [17/May/2017:08:05:32 +0000] "GET /downloads/product_1 HTTP/1.1" 304 0 "-" "Debian APT-HTTP/1.3 (6.4.16-exim2ubuntu9.21)"
2 93.188.71.5 - - [17/May/2017:08:05:33 +0000] "GET /downloads/product_1 HTTP/1.1" 304 0 "-" "Debian APT-HTTP/1.3 (6.4.16-exim2ubuntu9.21)"
3 86.51.13.131 - - [17/May/2017:08:05:34 +0000] "GET /downloads/product_1 HTTP/1.1" 304 0 "-" "Debian APT-HTTP/1.3 (6.4.16-exim2ubuntu9.21)"
4 137.154.17.5 - - [17/May/2017:08:05:34 +0000] "GET /downloads/product_1 HTTP/1.1" 206 450 "-" "Debian APT-HTTP/1.3 (6.4.16-exim2ubuntu9.21)"
5 137.154.17.5 - - [17/May/2017:08:05:35 +0000] "GET /downloads/product_1 HTTP/1.1" 206 450 "-" "Debian APT-HTTP/1.3 (6.4.16-exim2ubuntu9.21)"
6 93.188.71.5 - - [17/May/2017:08:05:37 +0000] "GET /downloads/product_1 HTTP/1.1" 304 0 "-" "Debian APT-HTTP/1.3 (6.4.16-exim2ubuntu9.21)"
7 137.154.17.5 - - [17/May/2017:08:05:38 +0000] "GET /downloads/product_1 HTTP/1.1" 404 127 "-" "Debian APT-HTTP/1.3 (6.4.16-exim2ubuntu9.21)"
8 137.154.17.5 - - [17/May/2017:08:05:40 +0000] "GET /downloads/product_1 HTTP/1.1" 404 132 "-" "Debian APT-HTTP/1.3 (6.4.16-exim2ubuntu9.21)"
9 86.51.13.131 - - [17/May/2017:08:05:41 +0000] "GET /downloads/product_1 HTTP/1.1" 304 0 "-" "Debian APT-HTTP/1.3 (6.4.16-exim2ubuntu9.21)"
10 93.188.71.5 - - [17/May/2017:08:05:47 +0000] "GET /downloads/product_1 HTTP/1.1" 304 0 "-" "Debian APT-HTTP/1.3 (6.4.16-exim2ubuntu9.21)"
11 137.154.17.5 - - [17/May/2017:08:05:48 +0000] "GET /downloads/product_1 HTTP/1.1" 206 1216 "-" "-"
12 188.132.90.301 - - [17/May/2017:08:05:49 +0000] "GET /downloads/product_1 HTTP/1.1" 304 0 "-" "Debian APT-HTTP/1.3 (6.4.16-exim2ubuntu9.21)"
```

Summary

Number of lines analyzed: 995

Format: `remote_addr - - [timestamp] "method url http_version" status size "-" user_agent"`

Grok pattern: `%{COMBINEDAPACHELOG}`

Time field: `@timestamp`

Time format: `dd/MMM/YYYY:HH:mm:ss Z`

[Override settings](#)

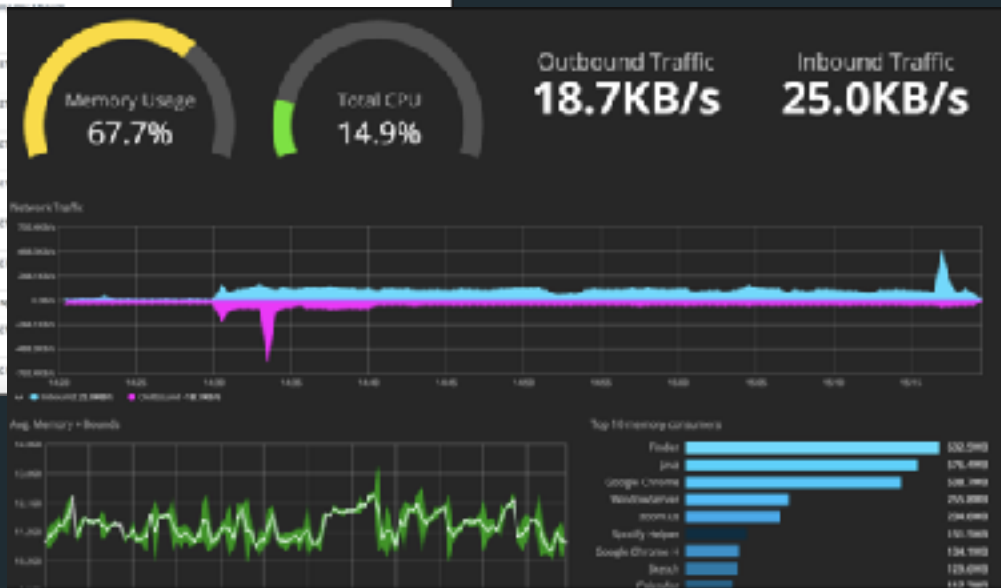
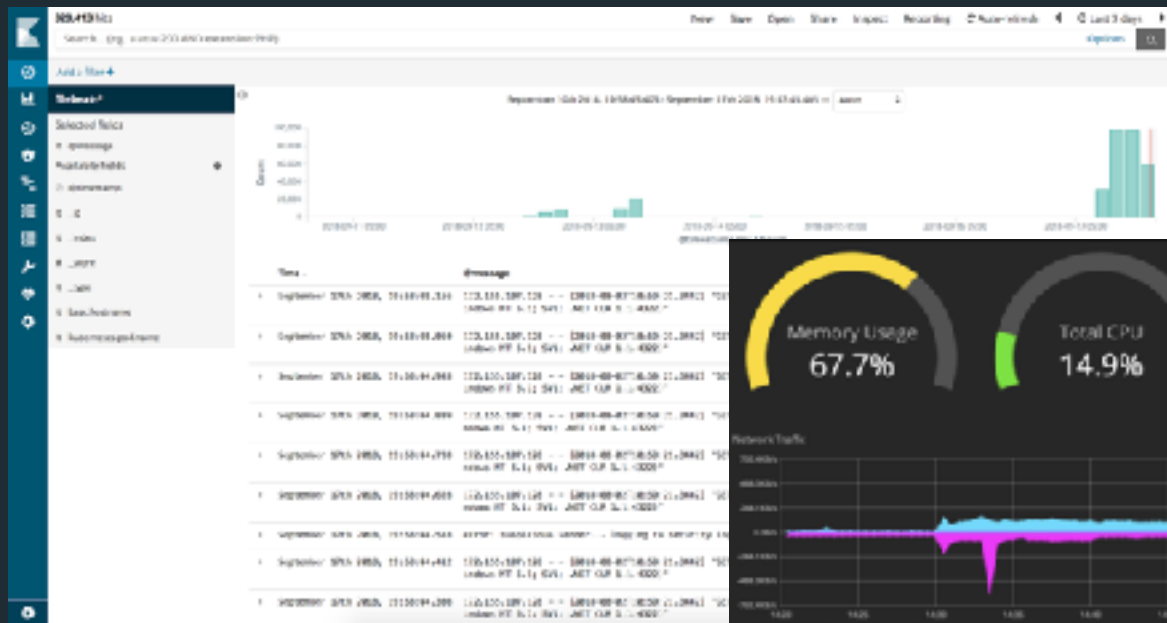
File stats

1 GB

[View index in Discover](#) [Create new ML job](#) [Open in Data Visualizer](#) [Index Management](#) [Index Pattern Management](#)

即时的日志搜索、可视化分析

Kibana Discover, Visualize, Dashboard



支持 Hot/Warm 架构部署

- 一键 **hot-warm** 部署
- 可大大优化数据存储

5 Optimize your deployment

I/O Optimized

Recommended

Use for search and general all-purpose workloads. Includes a balance of compute, memory, and storage.

Default specs

Compute Optimized

Run CPU-intensive workloads or run smaller workloads cost effectively when you need less memory and storage.

Default specs

Memory Optimized

Perform memory-intensive operations efficiently, including workloads with frequent aggregations.

Default specs

Hot-Warm Architecture

Use for time-series analytics and logging workloads that benefit from automatic index expiration.

Default specs

Create deployment template

1. Select cluster

2. Select topology

3. Select node type

4. Name

Index configuration

How indices get created and deleted, nodes fire, and are moved to warm nodes later on. Based on the choices you make here, [Google](#) [will](#) [auto](#) [scale](#) [up](#) [or](#) [down](#).

Event when node should be moved to hot

Event when new nodes will be moved to hot

Index pattern

example-index-1	After	5	Days	x
example-index-2	After	5	Days	x
example-index-3	After	5	Days	x
example-index-4	After	5	Days	x
example-index-5	After	5	Days	x

1. The lifecycle of 5 new nodes get auto managed up the cluster. It's a new...

```
load averages: 0.00, 0.00, 0.00; up 0+00:13:17 21:04
17 processes: 16 sleeping, 1 on CPU
CPU states: 0.0% user, 0.0% nice, 0.0% system, 0.0% interrupt, 100% idle
Memory: 29M Act, 6028K Wired, 8336K Exec, 14M File, 184M Free
Swap:
```

Elastic Stack for metrics

PID	USERNAME	PRI	NICE	SIZE	RES	STATE	TIME	WCPU	CPU	COMMAND
684	root	43	0	17M	1800K	CPU	0:00	0.00%	0.00%	top
0	root	96	0	0K	2912K	atath	0:00	0.00%	0.00%	[system]
303	root	85	0	22M	6128K	pause	0:00	0.00%	0.00%	ntpd
537	root	85	0	48M	3912K	kqueue	0:00	0.00%	0.00%	master
529	postfix	85	0	48M	3912K	kqueue	0:00	0.00%	0.00%	qmgr
525	postfix	85	0	48M	3820K	kqueue	0:00	0.00%	0.00%	pickup
570	root	85	0	59M	3736K	wait	0:00	0.00%	0.00%	login
198	root	85	0	23M	1876K	kqueue	0:00	0.00%	0.00%	syslogd
530	root	85	0	13M	1740K	wait	0:00	0.00%	0.00%	sh
532	root	85	0	13M	1352K	ttyraw	0:00	0.00%	0.00%	getty
519	root	85	0	13M	1352K	ttyraw	0:00	0.00%	0.00%	getty
568	root	85	0	13M	1352K	ttyraw	0:00	0.00%	0.00%	getty
484	root	85	0	11M	1320K	nanoslp	0:00	0.00%	0.00%	cron
1	root	85	0	13M	1316K	wait	0:00	0.00%	0.00%	init
539	root	85	0	15M	1104K	kqueue	0:00	0.00%	0.00%	inetd
150	root	85	0	11M	1072K	select	0:00	0.00%	0.00%	powerd
341	root	85	0	13M	1020K	kqueue	0:00	0.00%	0.00%	powerd

Metrics vs Logs

日志是事件在时间上的顺序记录

64.242.88.10 - - [07/Mar/2017:16:10:02 -0800] "GET /mailman/listinfo/hsdivision HTTP/1.1" 200 6291

64.242.88.10 - - [07/Mar/2017:16:11:58 -0800] "POST /twiki/bin/view/TWiki/WikiSyntax HTTP/1.1" 404 7352

64.242.88.10 - - [07/Mar/2017:16:20:55 -0800] "GET /twiki/bin/view/Main/DCCAndPostFix HTTP/1.1" 200 5253

每个事件，输出当前正在发生的事情。

Metrics 是一系列 KPI 的周期度量

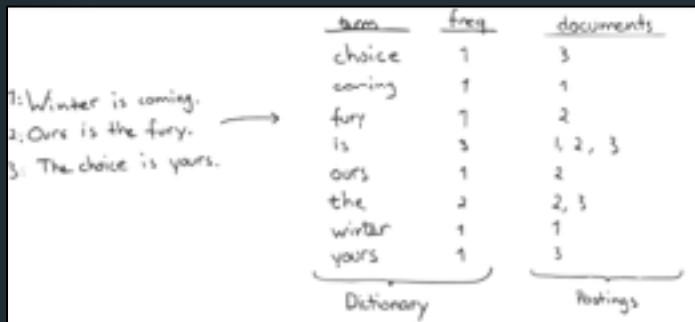
07/Mar/2017 16:10:00	all	2.58	0.00	0.70	1.12	0.05	95.55	server1	containerX	regionA
07/Mar/2017 16:20:00	all	2.56	0.00	0.69	1.05	0.04	95.66	server2	containerY	regionB
07/Mar/2017 16:30:00	all	2.64	0.00	0.65	1.15	0.05	95.50	server2	containerZ	regionC

每隔x分钟，测量CPU负载并将其打印出来，并用元数据进行注释。

Elasticsearch 在 Metrics 存储上的演进

Elasticsearch 搜索和数值型的分析

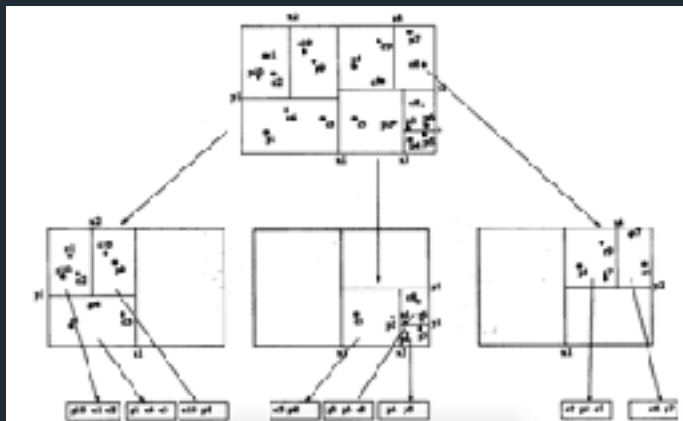
Inverted Index for full-text search



Columnar store for structured data

userid	first	middle	last	city	state
john123	John	Janes	Smith	Alamo	California
jrice	Bill	Any	Rice		
mt123	Jeff		Twain	Toledo	Ohio
adams	Sue		Adams		
adoc	Any		Doe	Miami	Florida

BKD Trees for numerical operations



Rollups



Elasticsearch 早期

2010 年

- Elasticsearch 主要用于 应用搜索
- Lucene 数据结构: 倒排索引

SEARCH



	<u>term</u>	<u>freq</u>	<u>documents</u>
	choice	1	3
	coming	1	1
	fury	1	2
	is	3	1, 2, 3
	ours	1	2
	the	2	2, 3
	winter	1	1
	yours	1	3
	Dictionary		Postings

1: Winter is coming.
2: Ours is the fury.
3: The choice is yours.

Elasticsearch 进化到对数据分析的支持

~ 2010 到 2014

- Elasticsearch 1.0 开始支持 列式存储 (基于 Lucene “doc values”)
- 结构化的文本和数值型数据能够更快的取出来并用于分析

userid	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

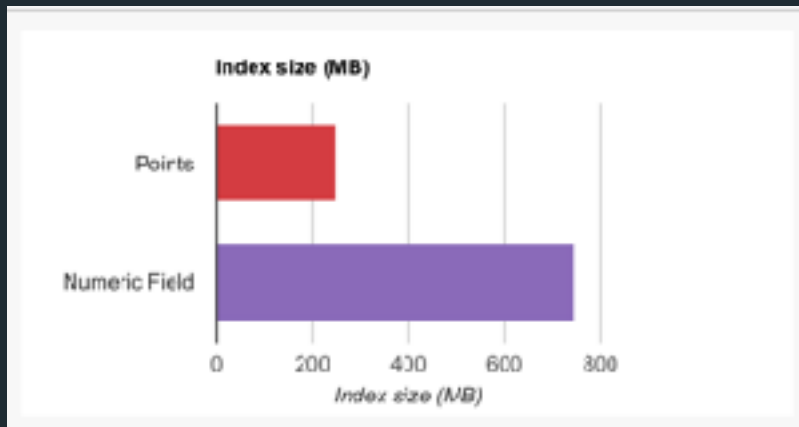
<https://www.elastic.co/blog/elasticsearch-as-a-column-store>

Elasticsearch 改善存储效率

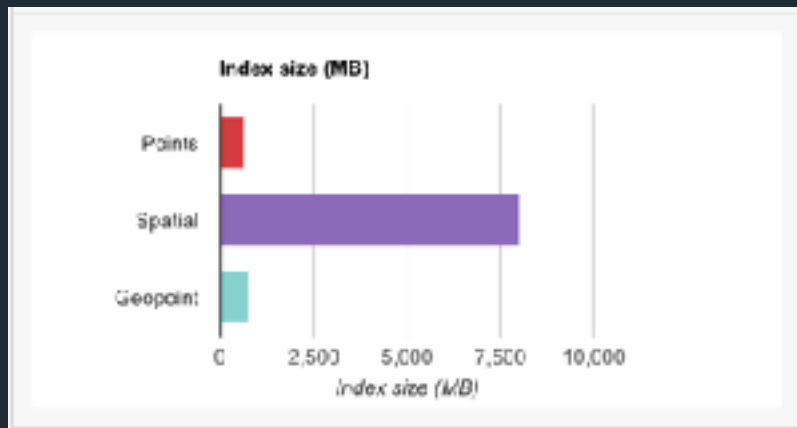
2016

- Elasticsearch 5.0 添加更多数据结构来高效存储数值型数据 (**BKD Trees**)
- 数值型数据以及地理位置数据默认都采用这种数据结构来进行存储

1-Dimension



2-Dimensions



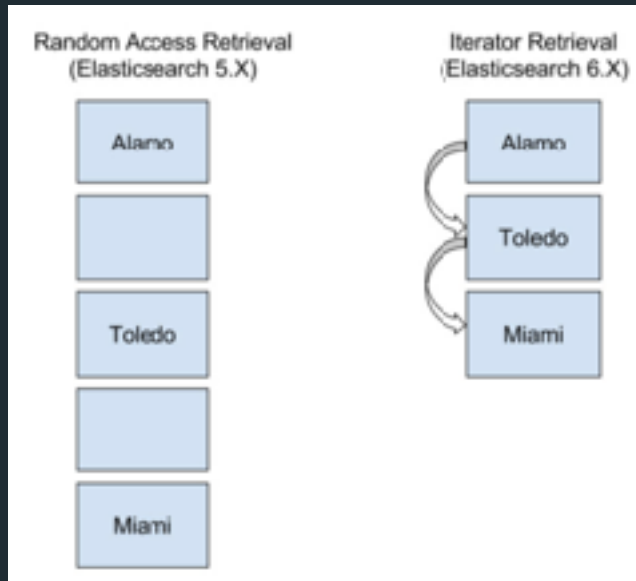
<https://www.elastic.co/blog/searching-numb3rs-in-5.0>

Elasticsearch 改善存储效率

2017

- Elasticsearch 6.0 改进 **sparse values** 的存储效率 (Metricbeat 节省 59.5% 的索引存储)

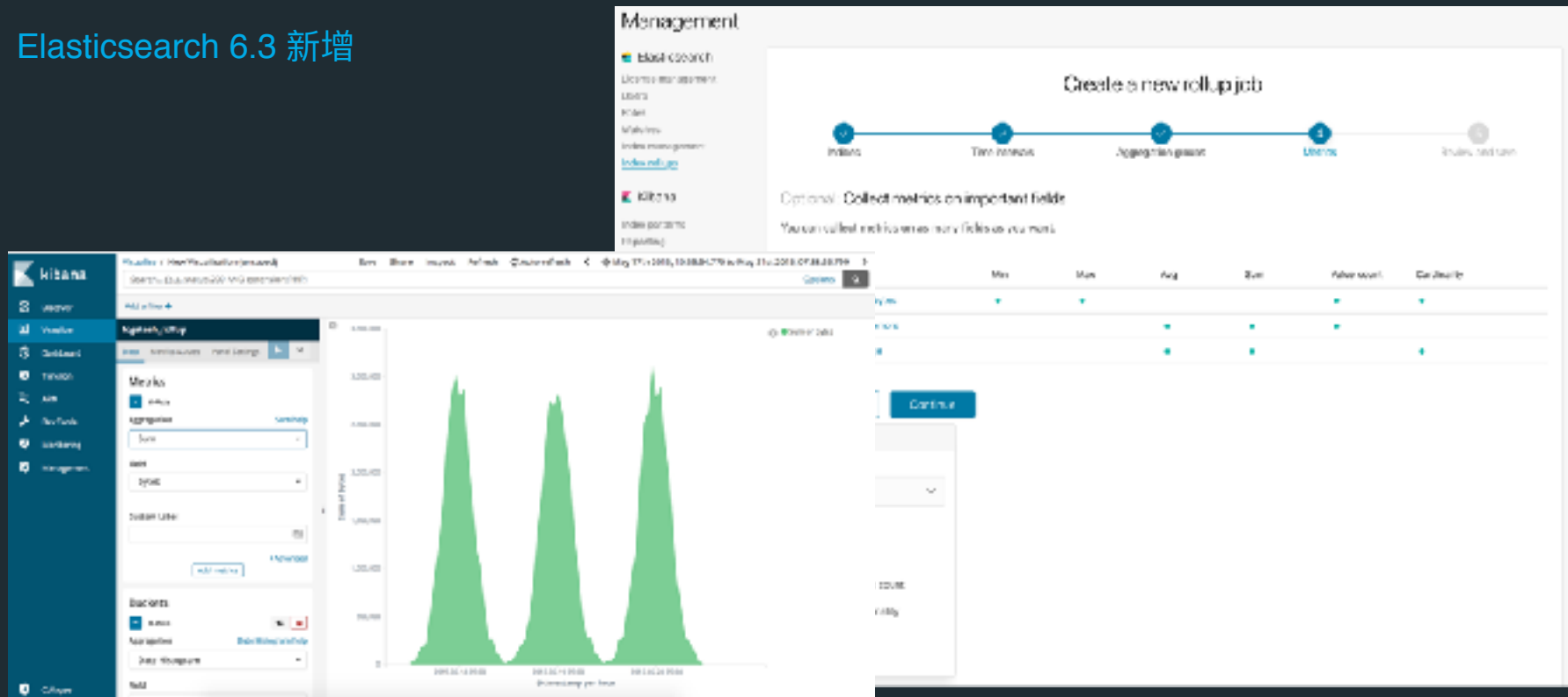
userid	first	middle	last	city	state
john123	John	James	Smith	Alamo	California
jrice	Jill	Amy	Rice		
mt123	Jeff		Twain	Toledo	Ohio
sadams	Sue		Adams		
adoe	Amy		Doe	Miami	Florida



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

Rollup 用于长期数据存储

Elasticsearch 6.3 新增



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

Elastic Stack 作为 Metrics 解决方案

Metrics 模块

HEARTBEAT



METRICBEAT



PACKETBEAT



Infrastructure

System

- Linux
- MacOS
- Windows
- Perfmon

Containers

- Docker
- Kubernetes

Virtualization

- vSphere

Cloud

- AWS
- GCP
- Azure
- DigitalOcean
- Alibaba

Network

- Netflow
- Packets
- TLS Envelope

Storage

- Ceph

Metrics 模块

HEARTBEAT

METRICBEAT

PACKETBEAT



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

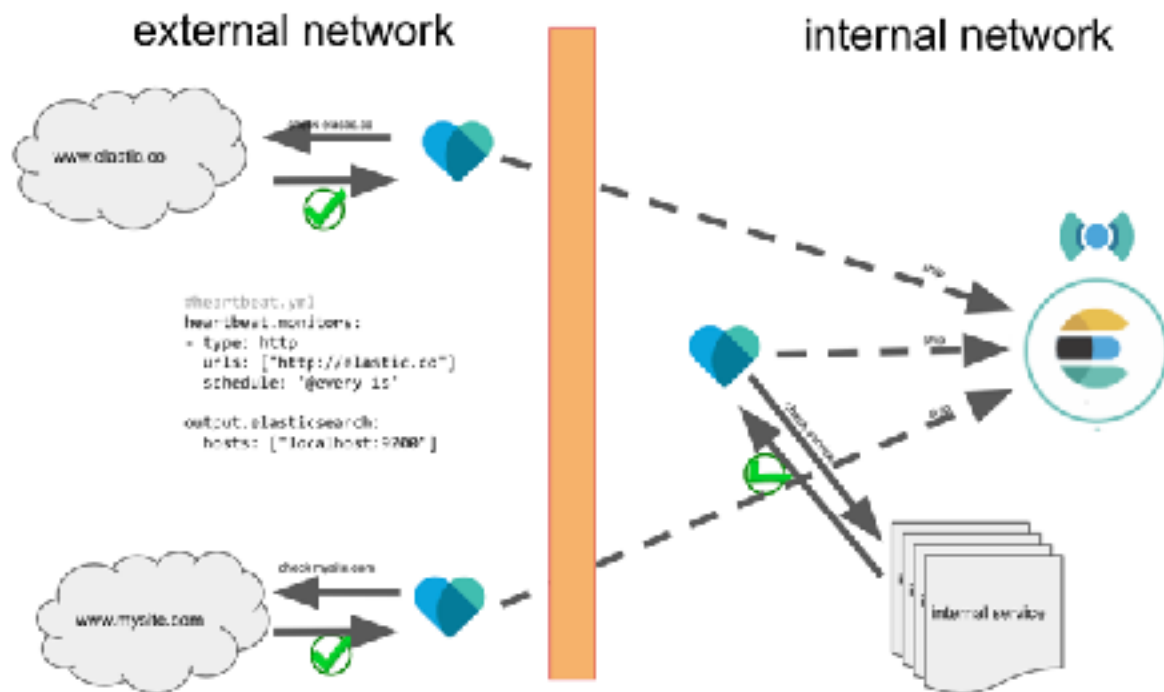
Other

- HAProxy
- Zookeeper

Heartbeat: 心跳监测

Deployment steps

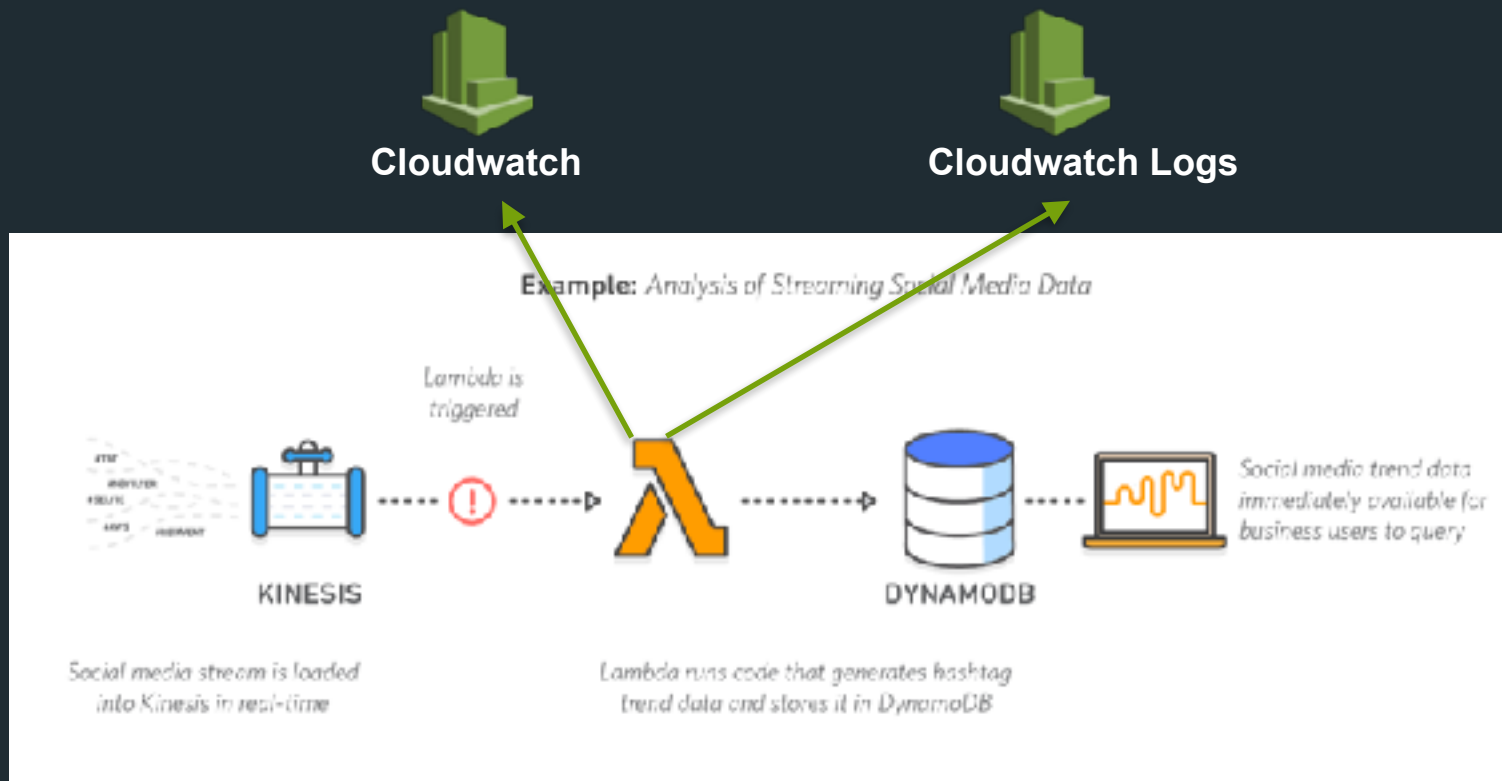
- 1 Deploy Heartbeat shippers
- 2 Configure & run each shipper
- 3 Load dashboard
- 4 Define watches



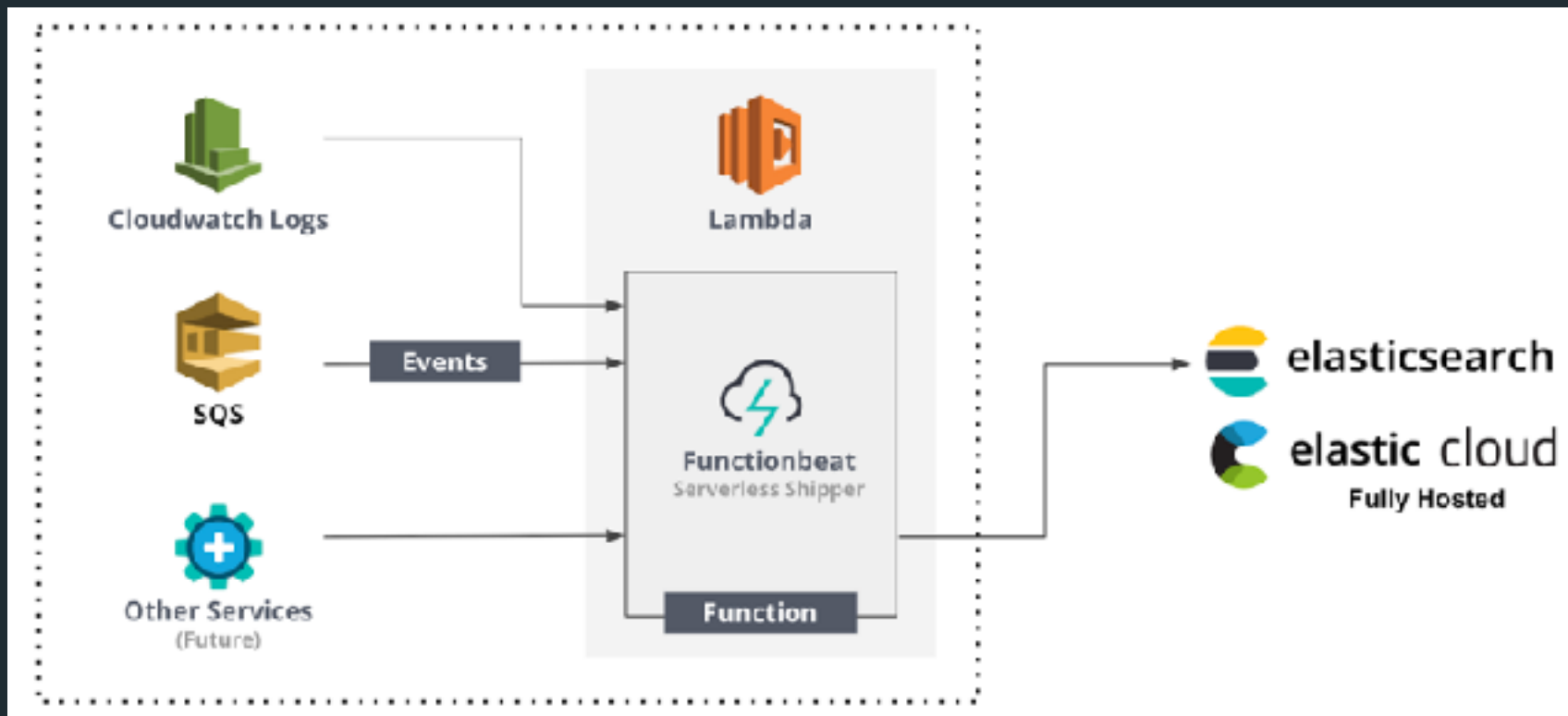
Heartbeat: 心跳监测



Functionbeat: Serverless 日志采集器



Functionbeat: Serverless 日志采集器



将 Logs, metrics, APM 关联起来

Elastic Common Schema

Benefits

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

Status

- Beta published: github.com/elastic/ecs
- Integrating into Elastic products in progress
- Community feedback welcome!

ECS Revision: 0.9.02 Group 1 Fields: 3 Group 2 Fields: 87

Group 1 (Must be populated)

@timestamp
_type
_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.subtype	resource.version
event.organization_id	device.type	host.id		network.outbound_packets		destination.port	service.query	resource.hash_value
event.id	device.vendor	host.type		network.totall_bytes			service.response_code	
event.new	device.product	host.sub_type		network.totall_packets				
event.hash	device.version	host.operating_system		network.direction				
event.tags	device.vendor_number	host.operating_system_version						
event.labels	device.action	host.provider						
event.duration	device.risk_score	host.provider						
event.severity	device.event_id	host.region						
event.risk_score								

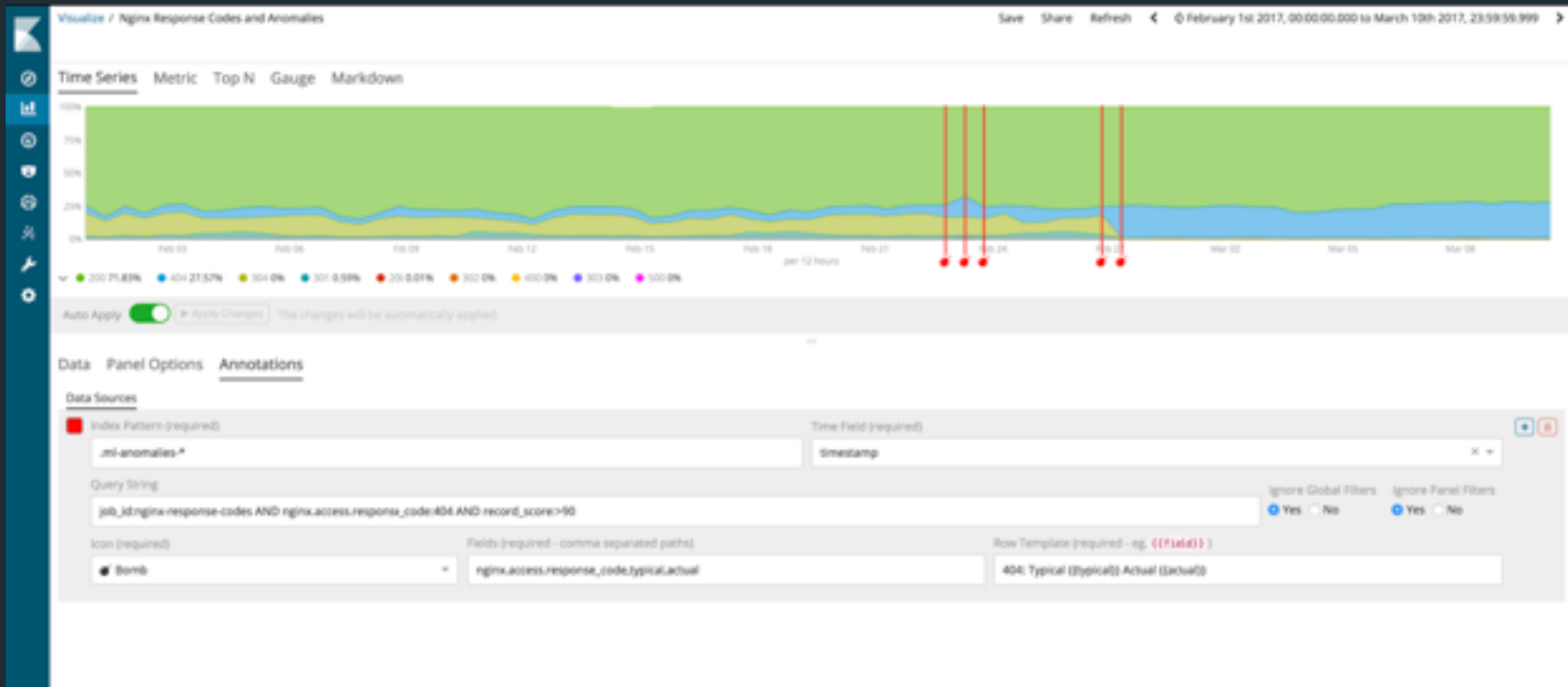
时序型数据的可视化

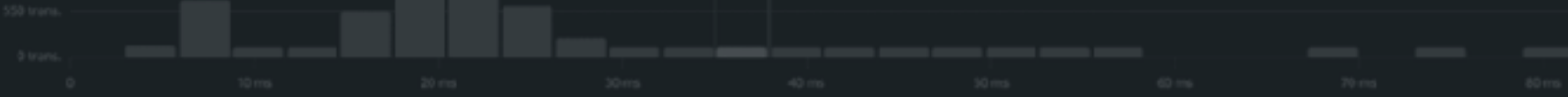
Time Series Visual Builder



时序型数据的可视化

Annotations





Transaction sample

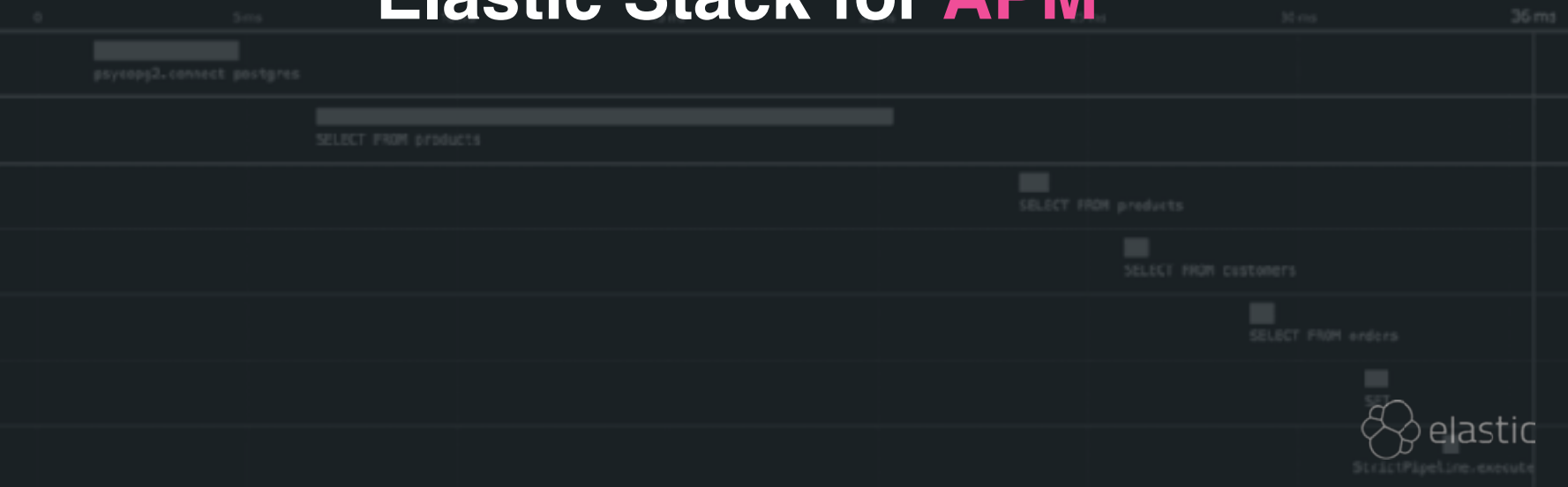
[View transaction in Discover](#)

@timestamp: 5 hours ago (December 5th 2017, 11:59:47.057)
request.url.raw: /N/A

Timeline System App User Tags Custom

opbeans.tasks.update_stats

DB cache



Elastic Stack for APM

什么是 APM?

Example

08:32:10 Request "/api/checkout"

08.32:11 Response "/api/checkout 500 ERROR"

什么是 APM?

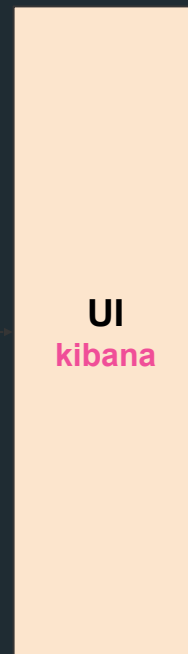
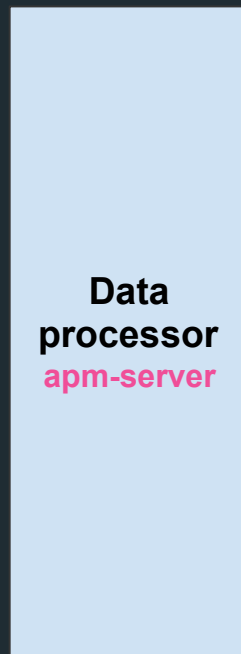
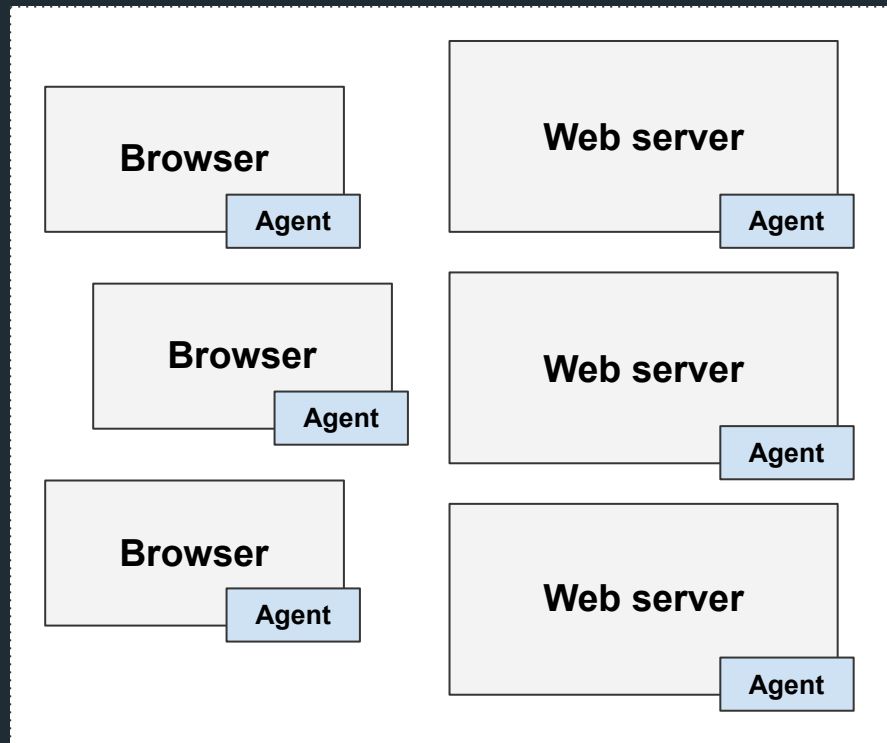
Example

08:32:10 Request "/api/products/top"

08.32:17 Response "/api/products/top 200 OK"

7 seconds - zZzzZZz

Elastic APM 如何工作?



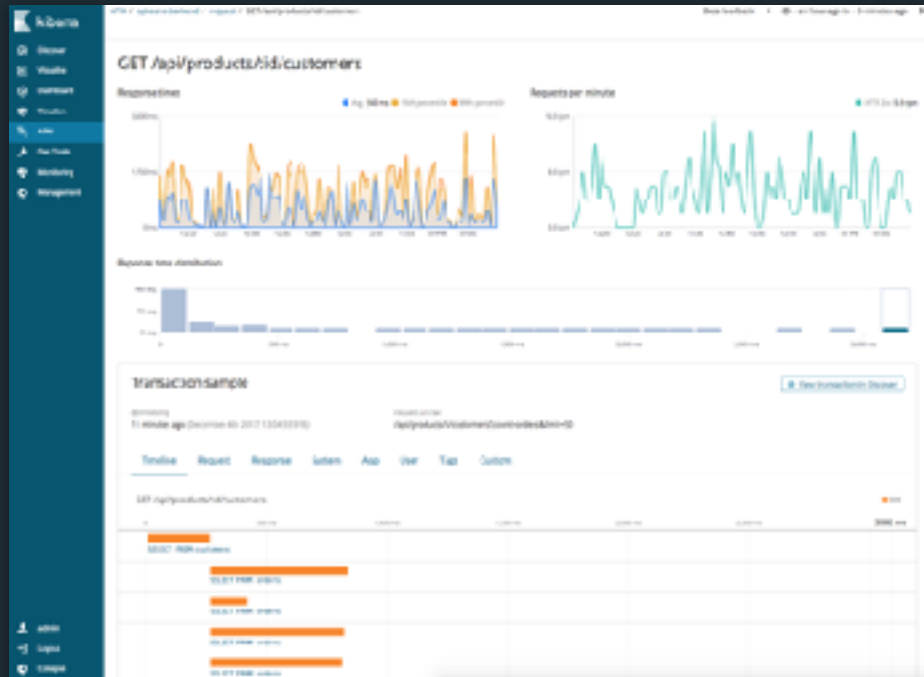
Elastic APM

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

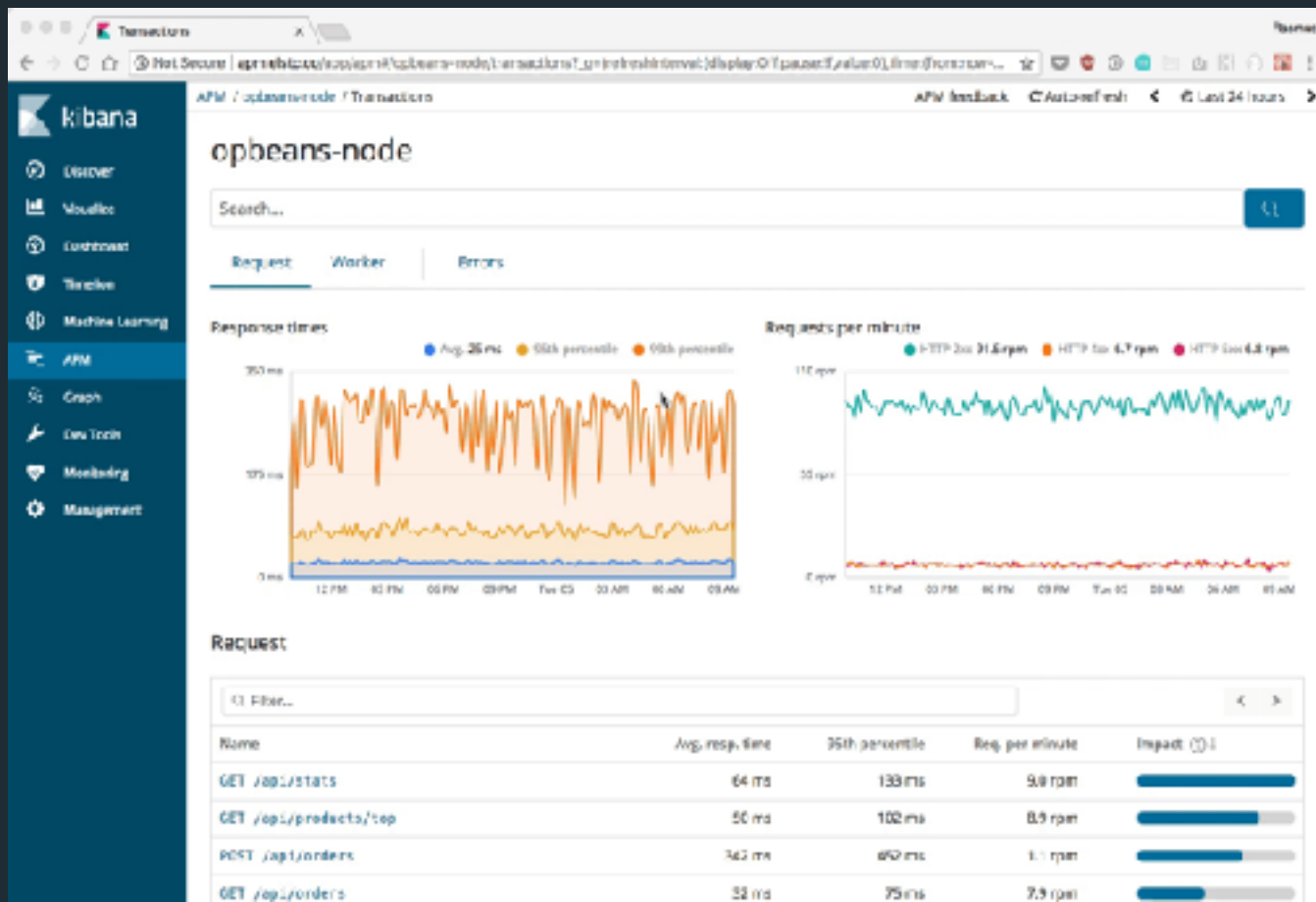
- Focuses on search experience on top of APM data
- 'Just another index' in Elastic Stack

Language support

- Python
- Node.js
- Ruby
- RUM
- Java
- Go
- .NET (in dev)



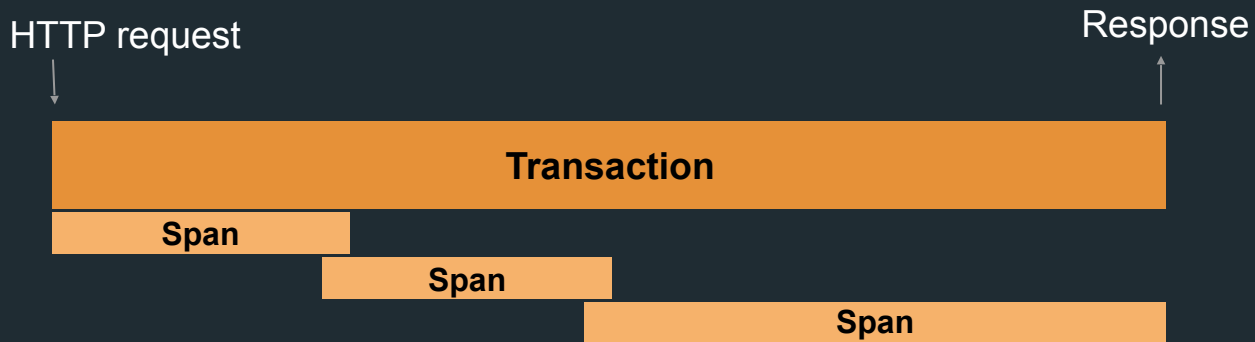
完善的 APM 分析 UI



Combine custom workflow with freedom of search

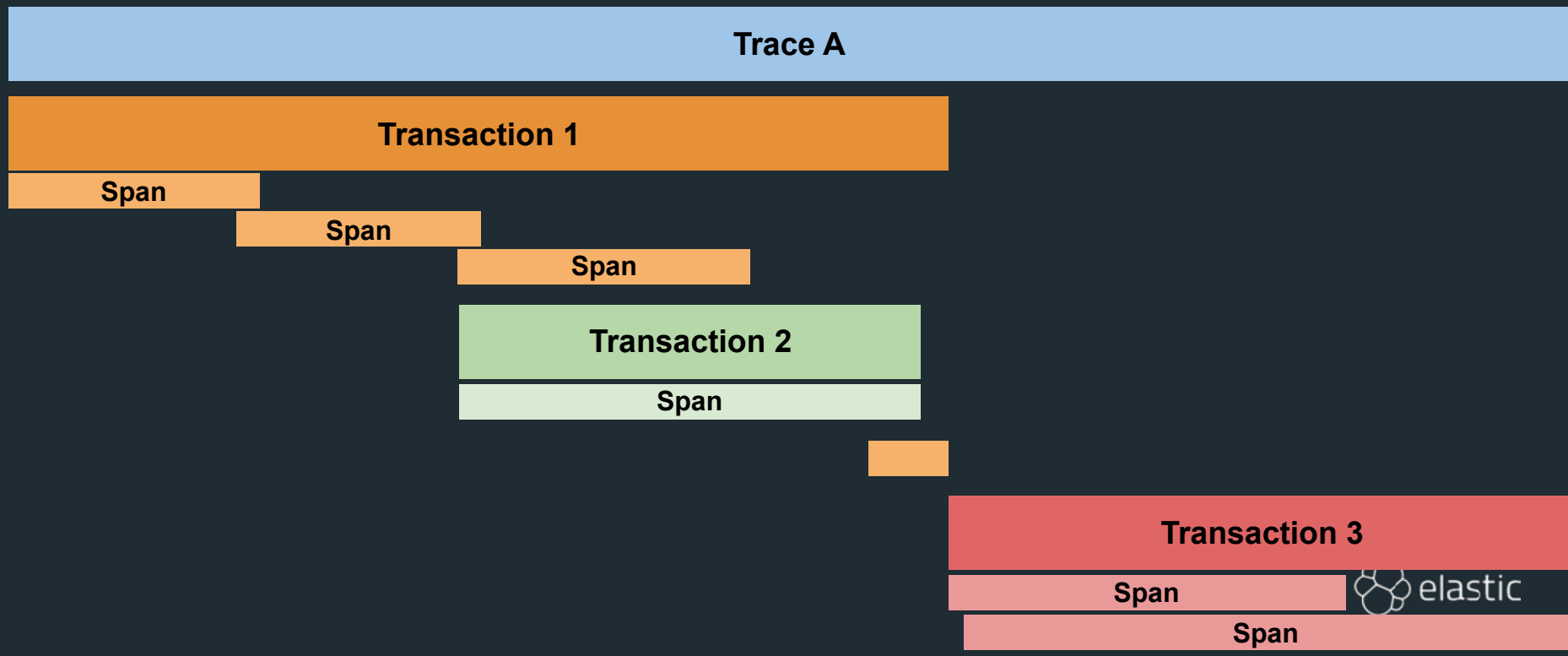
Distributed Tracing

Single transaction



Distributed Tracing

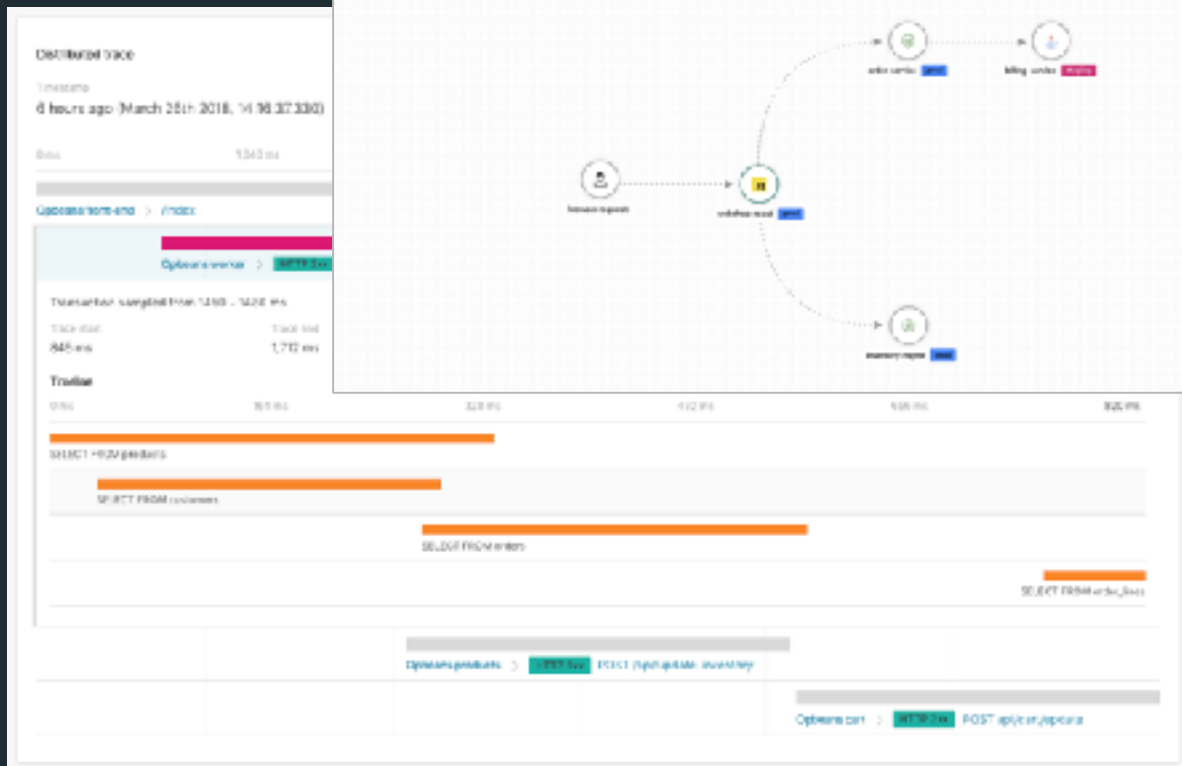
Distributed tracing example



Distributed Tracing

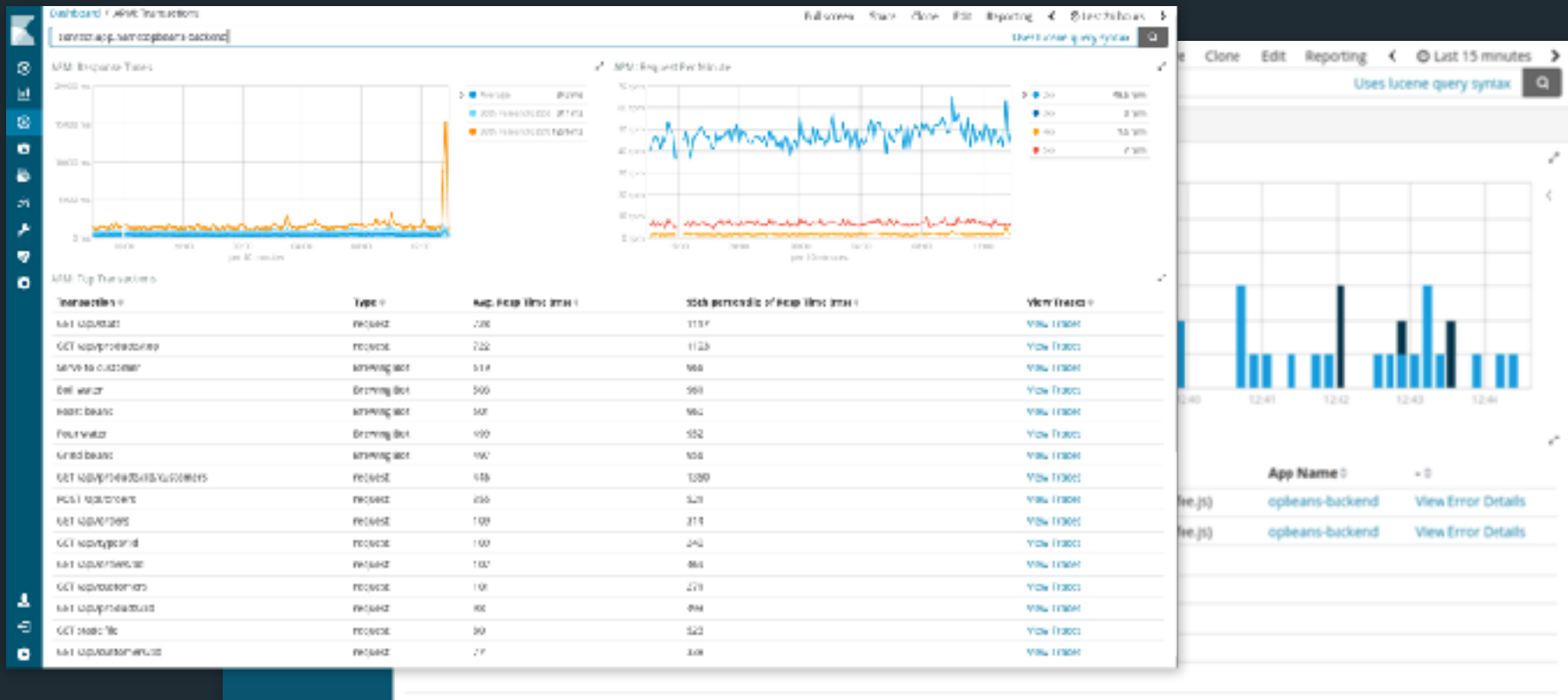
Trace and map across multiple services

- 查看端到端视图并导航到各个事务
- 基于 Trace ID 的分布式跨服追踪
- 兼容 OpenTracing API 和 W3C trace context 规范



APM is another index in Elasticsearch

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



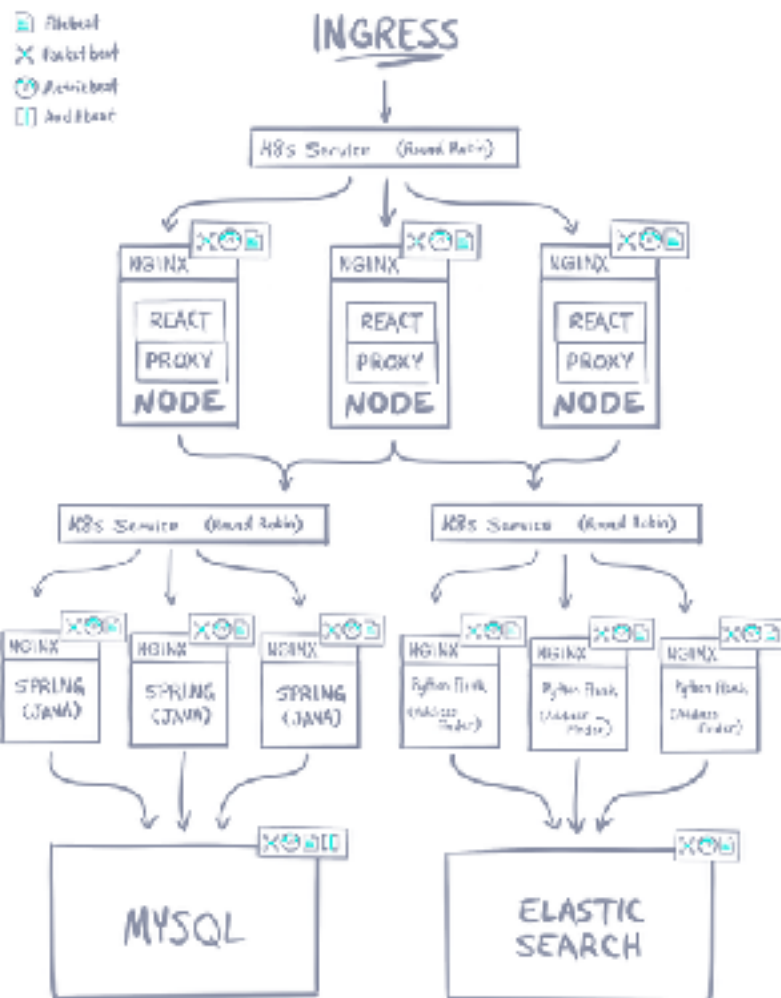
DEMO

Find Owners

Last name

51 Owners found

Name	Address	City	Telephone	Pets
George Franklin	8580, n 87 e, demotte, 56, indiana	demotte	8085551023	Dutchess, Grace, Guinness, Kaylee, Lady, Leo, Mikey, Sheila, Tiki, Tyler, Zoe
Betty Davis	412, s brooksville ave, brooksville, florida	brooksville	8085551749	Basil, Jersey, Luigi, Papa, Pumpkin
Eduardo Rodriguez	25, brookhaven drive, brookhaven, suffolk, new york	brookhaven	8085558763	Dodger, Dutch, Jewel, Niki, Oscar, Rosy
Harold Davis	850, rolling hills dr, bend, arizona	bend	8085553198	Fletcher, Iggy, Louis, Nico, Sandi, Velvet
Peter McTavish	1, brookhaven drive, brookhaven, suffolk, new york	brookhaven	8085552765	Alexis, Champ, George, Skylar
Jean Coleman	3251, cathedral canyon dr, cathedral city, california	cathedral city	8085552654	Cupcake, Joe, Lena, Max, Rose, Samantha
Jeff Black	408, park ave sw, bolivan, ohio	bolivan	8085555387	Daisy, Gwen, Kiara, Lucky, Tasha
Maris Escobito	109, west ridge mews, wood ridge, new jersey	wood ridge	8085557683	Mocha, Mulligan, Sammi
David Schroeder	3913, druid hills rd, druid hills, kentucky	druid hills	8085559435	Diesel, Dudley, Freddy, Jerry, Pugsley, Sage



怎样？

要不要下载试试？



The screenshot shows the Kibana web interface. On the left is a dark blue sidebar with the 'kibana' logo and a list of navigation items: Discover, Visualize, Dashboard, Timeline, APM, Infra, Dev Tools, Monitoring, and Management. The main content area is titled 'Home' and 'Add Data to Kibana'. It features a horizontal menu with 'All', 'Logging', 'Metrics', and 'Security Analytics'. Below this is a 3x4 grid of 12 cards, each representing a different data source. Each card has an icon, a title, and a brief description of what it does. The cards are: Apache logs, Apache metrics, APM, Docker metrics, Kibana metrics, MySQL logs, MySQL metrics, NetFlow, Nginx logs, Nginx metrics, Redis logs, and Redis metrics. The bottom left of the sidebar has a 'Collapse' button.

Questions?



更多 Demo: <http://demo.elastic.co>

官方网站: <http://elastic.co/cn>