



Kibana Lens

Jerry 朱杰 Elastic架构师

主题

- Elastic 产品概览
- Lens
 - 背景
 - Lens 目标
 - Lens 关键概念
- Demo
- 未来展望
- Q&A

Elastic 产品概览

解决方案

企业搜索

App + Web + Workplace

全观察

日志 + 指标 + APM

安全防护

SIEM + Endpoint

Elastic
云服务

Elastic大数据平台

数据
展示



Kibana

存储索引
计算分析



Elasticsearch

数据
摄取



Logstash



Beats

+



机器学习

数据关联分析

规则告警

多集群监控

报表

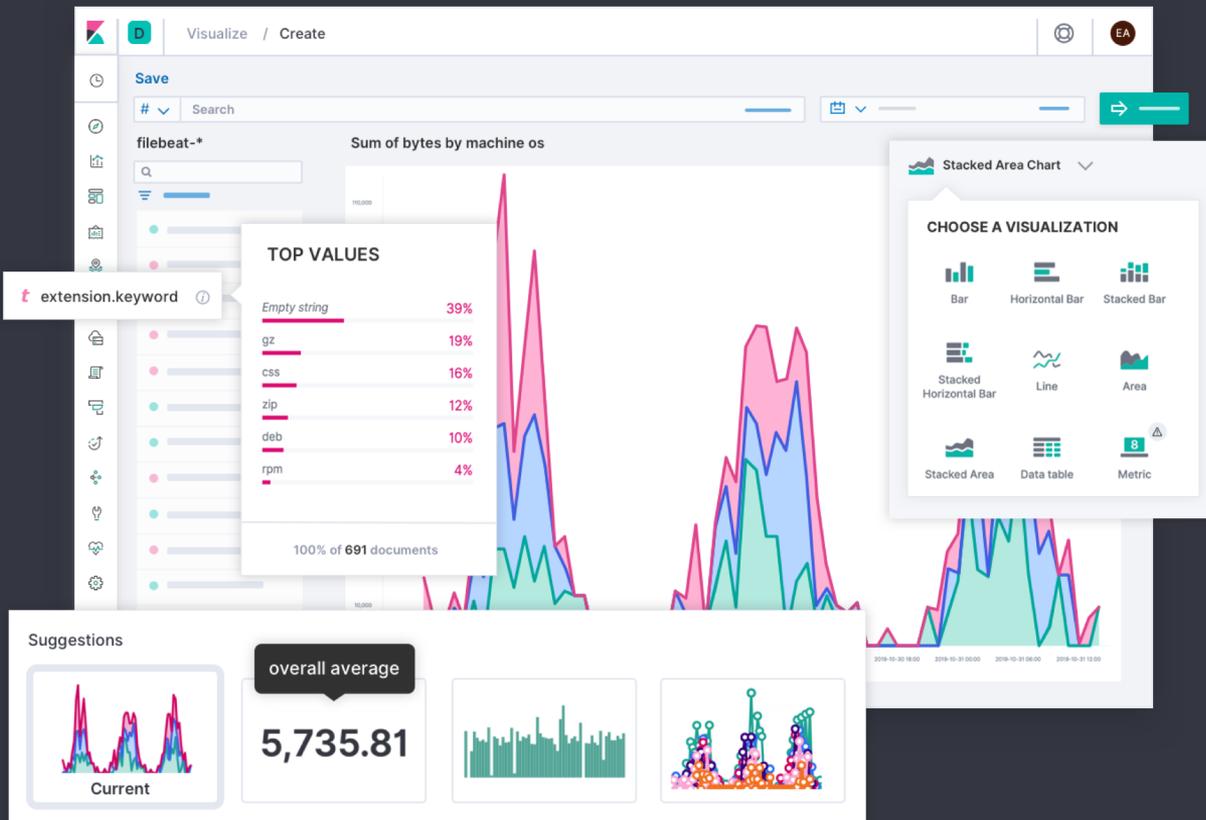
高级安全



Elastic
企业云

Kibana Lens

在Kibana中简单而直观地可视化分析数据



多年以前Kibana 用户

用例

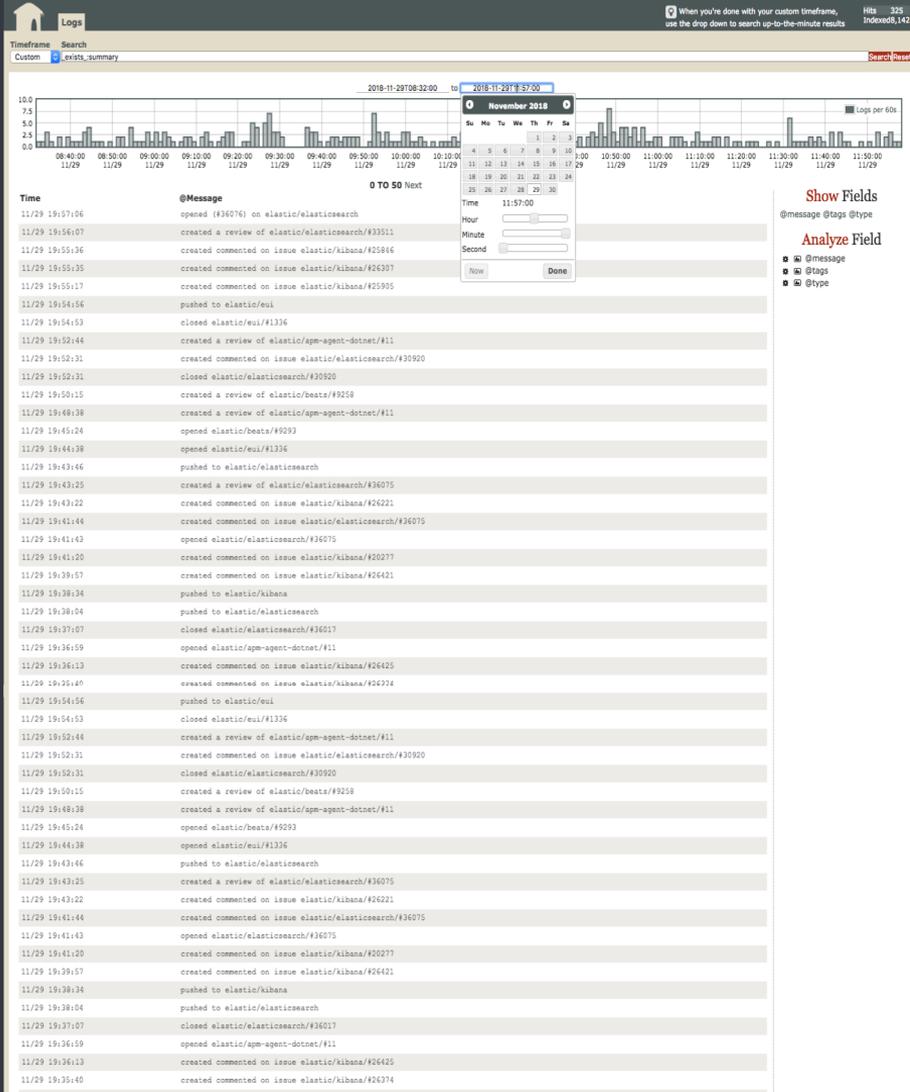
- 主要用来分析日志和运维分析

角色

- 最早被开发者和工程师采用

技能

- 熟悉 Elasticsearch 主要都是技术背景



现在Kibana用户

用例

商业分析，地理，安全分析，指标，日志，其它更多

角色

• 从开发者到商业分析的都有

技能

• 多样化的



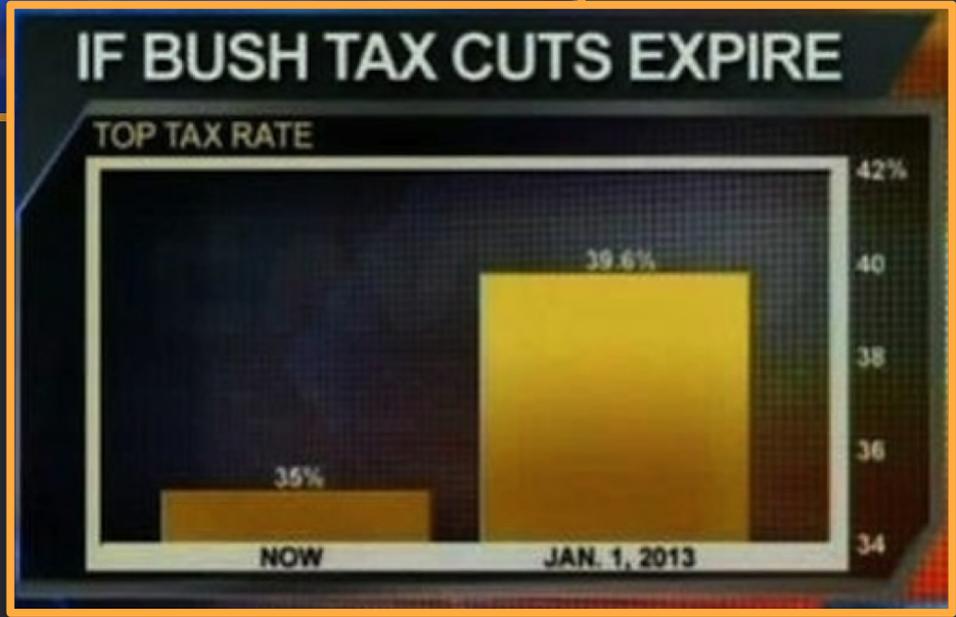
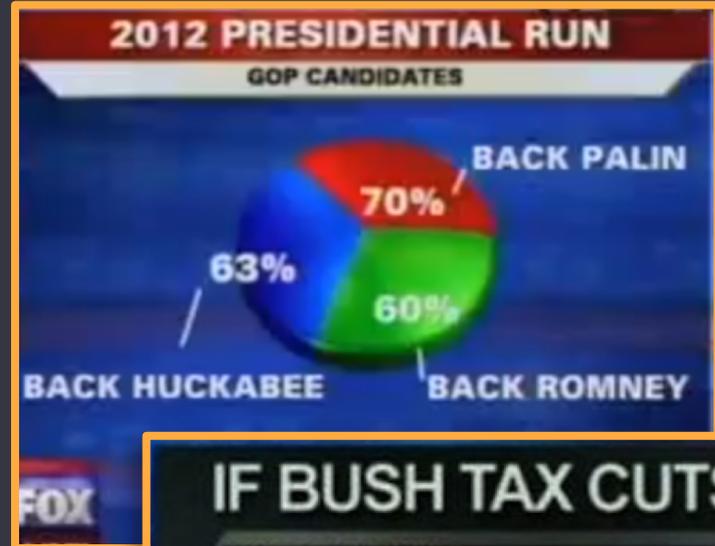
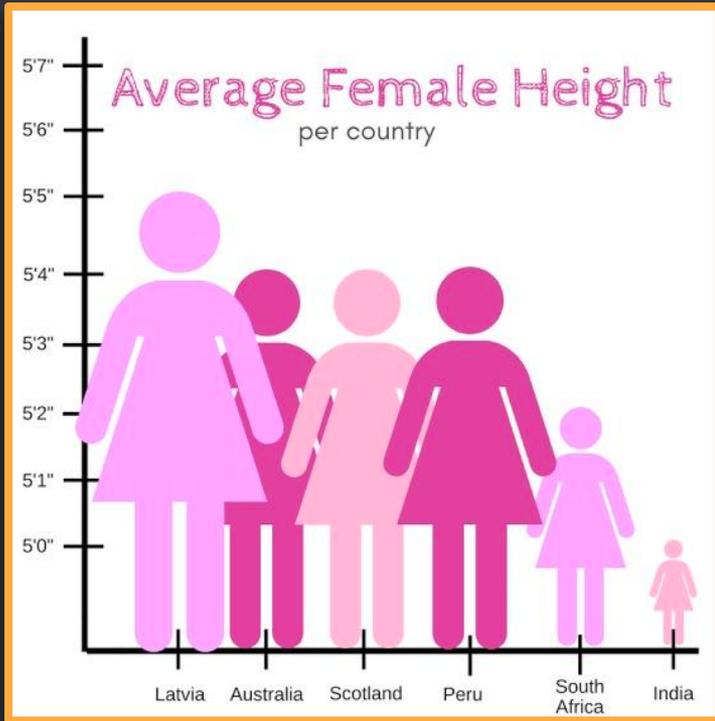
数据可视化的挑战

用户不熟悉他们的数据

用户难以将问题转换为一个可视化

如何有效的可视化数据

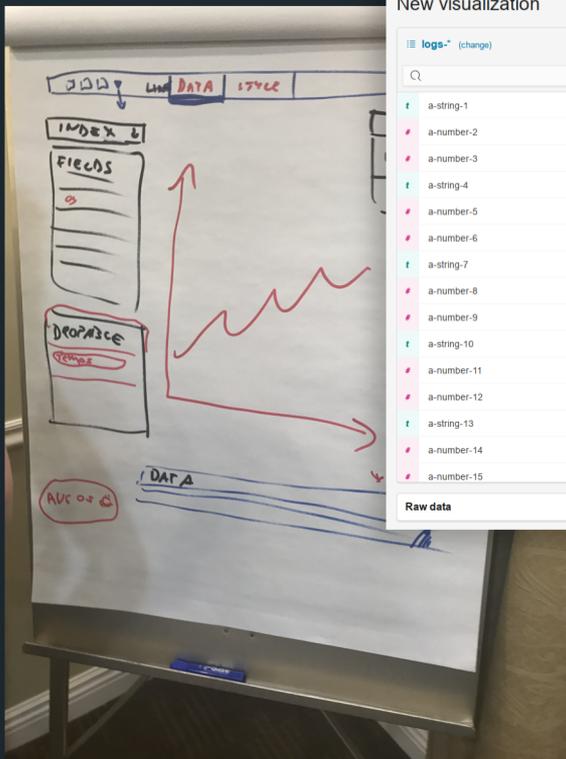
领域专业知识 vs 数据分析知识



我们如何帮助人们利用他们的数据？

简单直观的方法来可视化数据

- 不需要具备可视化分析背景
- 帮助用户找到他们需要的字段
- 帮助用户有效地可视化他们的数据
- 使用简单而功能强大
- 从架构上支持未来的可视化分析场景
- 标准的可复用的数据浏览-允许修改数据，图表和指标
- 利用 Elasticsearch独有的优势: 快速, 可扩展, 强大的聚合和搜索



Visualize / Editor

New visualization

logs-* (change)

Basic chart (change)

Y AXIS

- Count
- MAX of machine.ram

X AXIS

- HISTOGRAM of bytes

Raw data

- a-string-1
- a-number-2
- a-number-3
- a-string-4
- a-number-5
- a-number-6
- a-string-7
- a-number-8
- a-number-9
- a-string-10
- a-number-11
- a-number-12
- a-string-13
- a-number-14
- a-number-15

Visualize Create

logs-* (change)

Filters >

12/14/2017 03:30:00.00 → 12/14/2017 03:30:00.00

Sum of bytes over time

Configuration

Y-axis

- Sum of bytes

X-axis

- Date histogram of @timestamp

Suggestions

Top 5 values

12.7k documents (90%)

win 7 23%

win 8 22%

win xp 22%

ios 22%

osx 11%

Keep dragging fields to the stage or configuration panel to combine data sets.

Undo Redo Share Save

Kibana Lens 研发历程

数据驱动

从数据开始

找到合适的字段:

- 寻找名字
- 按类型过滤
- 预览字段的值
- 字段统计

filebeat-*

Search field names

Filter by type

0

event.severity

event.start

fileset.name.keyword

host.architecture.keyword

host.containerized.keyword

host.hostname.keyword

host.id.keyword

host.name.keyword

host.os.codename.keyword

host.os.family.keyword

host.os.kernel.keyword

host.os.name.keyword

host.os.platform.keyword

host.os.version.keyword

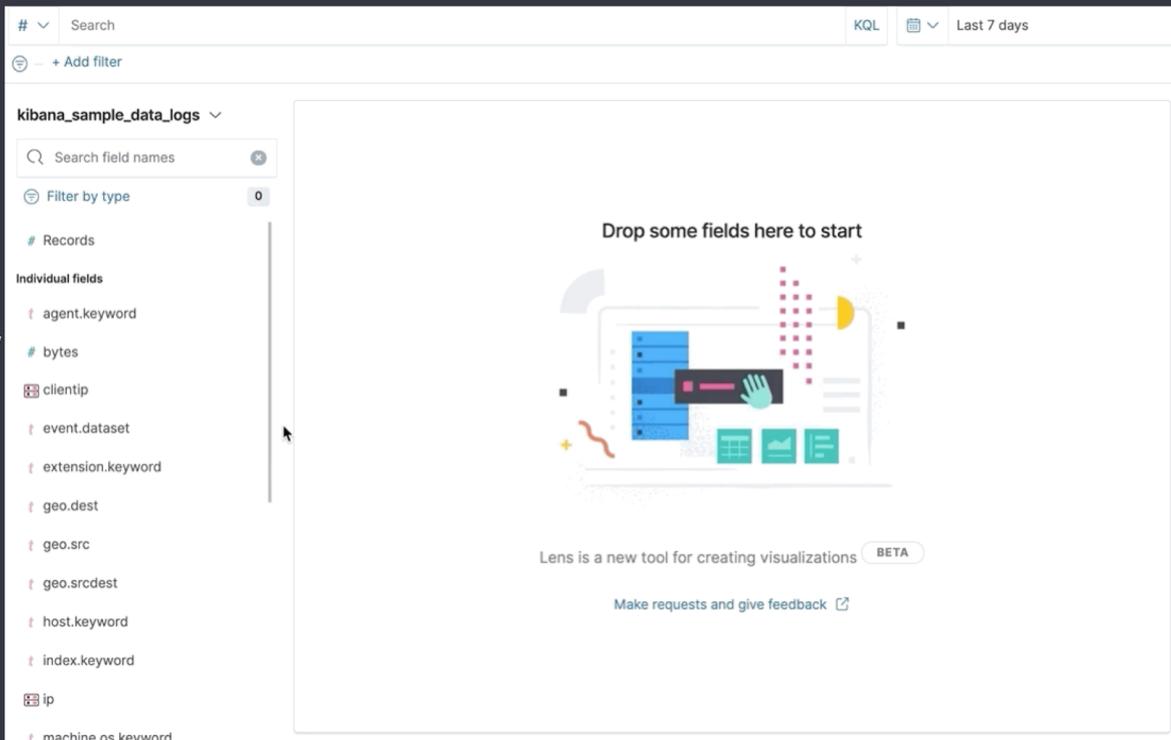
TOP VALUES

notice	17%
http	16%
auth	16%
ssl	14%
eve	13%
dns	12%
connection	12%

100% of 179 documents

即时预览

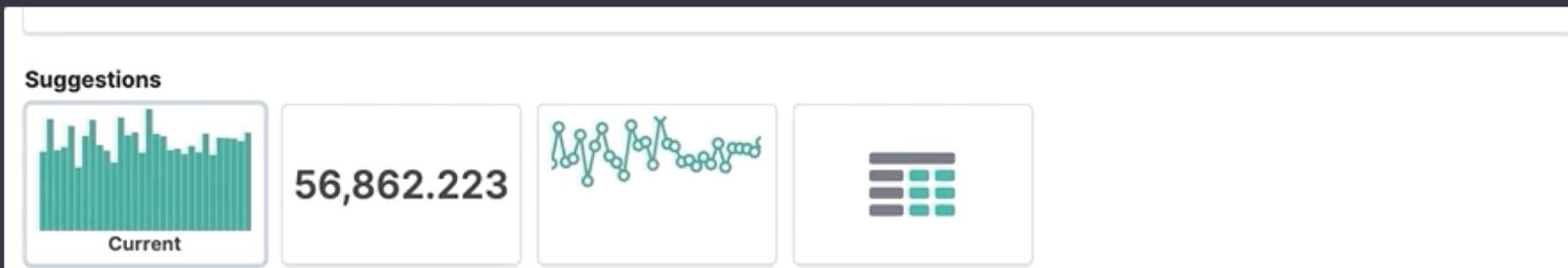
- 选择第一个字段就可以预览图表
- 隐藏复杂性: 更少的配置, 智能化选择图表



智能的方式来可视化

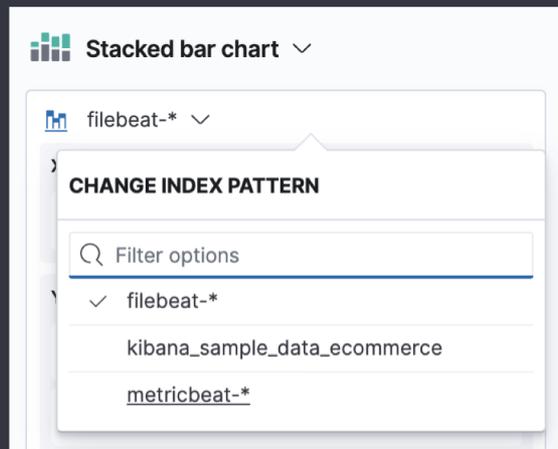
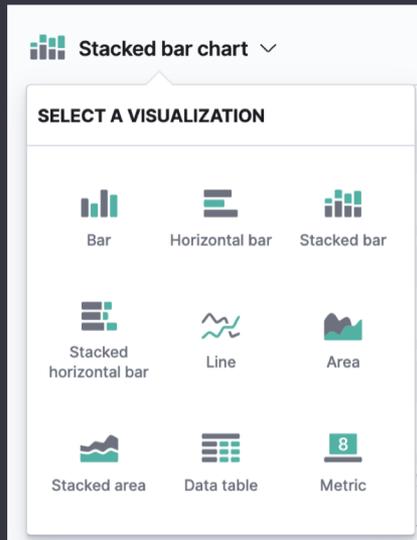
智能建议 Smart suggestions

- 基于选择的字段自动推荐聚合
- 基于数据建议图表的类型
- 数据建模
- 快捷方式 – 基于通用用例智能推荐缺省配置



标准和可复用

- 让用户用不同的方法来探索数据
- 可以改变index patterns和查询
- 用不同的图表类型查看数据
- 快速地在不同的字段间切换



DEMO

后续改进

扩展功能

- 新的图表
- 高级计算和函数
- 自定义公式
- 自定义图表
- 支持SQL

整合

- 更深入地整合进dashboard
- 和Canvas整合

更加智能

- 改进图表推荐
- 地图的推荐

底层改进

反馈

Visualize | Create

Save

Search

KQL Last 15 minutes

filebeat-*

Search field names

Filter by type

Records

Individual fields

- @timestamp
- agent.ephemeral_id.keyword
- agent.hostname.keyword
- agent.id.keyword
- agent.type.keyword
- agent.version.keyword
- cloud.availability_zone.keyword
- cloud.instance.id.keyword
- cloud.instance.name.keyword
- cloud.machine.type.keyword
- cloud.project.id.keyword
- cloud.provider.keyword
- destination.bytes
- destination.geo.city_name.keyword
- destination.geo.country_iso_code.keyword
- destination.geo.location.lat
- destination.geo.location.lon

Drop some fields here to start

Lens is a new tool for creating visualizations BETA

Make requests and give feedback

HELP v7.5.0

- Kibana documentation
- Ask Elastic
- Give feedback
- Open an issue in GitHub

Lens documentation

Provide feedback for the Lens application

Drop a field here

Break down by

Drop a field here

<https://www.elastic.co/kibana/feedback>

Lens 资源

[Lens webinar Dec 9th](#)

[Lens blog post](#)

[Lens video](#)

[Lens documentations](#)

[What is Lens webpage](#)