elastic | 中国开发者大会

基于Kibana的二次开发扩展

牧茗
Alibaba

阿里安全
ALIBABA SECURITY

ALIBABA SECURITY

基于Kibana的二次开发

--牧茗

分享目的

通过对我们在kibana上的使用场景、部分二次开发扩展、和一些扩展技术的介绍，希望以此给听众带来一些启发。

大纲

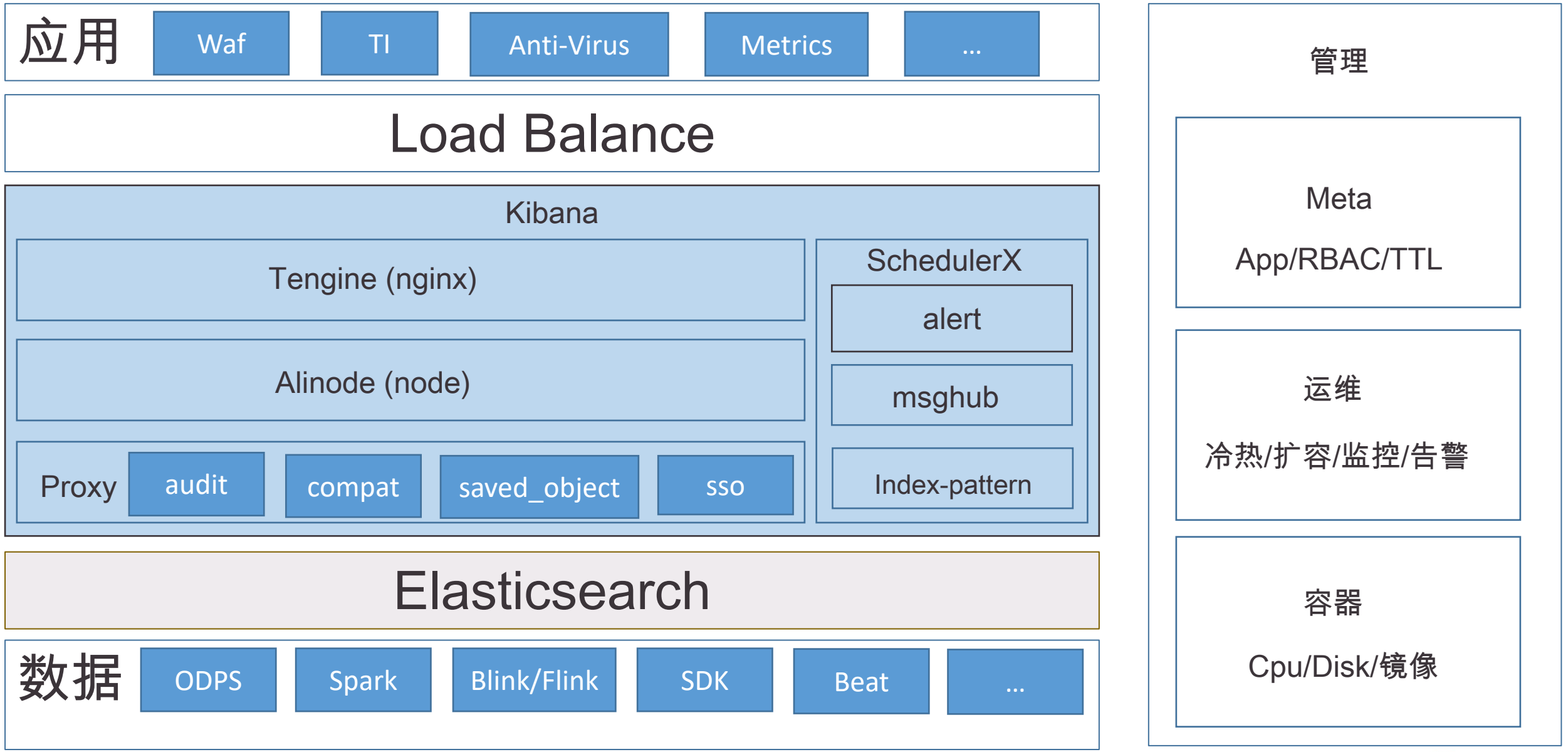
简介
二次开发
示例
开源
总结

01 简介

场景

数据类型	安全类日志数据
数据特点	格式复杂，体量庞大
业务种类	waf、anti-virus、TI
用户类型	运营小二、安全专家、技术人员
体验诉求	快速，交互友好

架构


应用
Waf
TI
Anti-Virus
Metrics
...
Load Balance
Kibana
Tengine (nginx)
Alinode (node)
Proxy
audit
compat
saved_object
sso
SchedulerX
alert
msghub
Index-pattern
Elasticsearch
数据
ODPS
Spark
Blink/Flink
SDK
Beat
...
管理
Meta
App/RBAC/TTL
运维
冷热/扩容/监控/告警
容器
Cpu/Disk/镜像

统计

用户数	数百+
es节点	500+
索引	2000+
doc	数千亿+

02

二次开发

Why

用户需求推动
数据业务导向
kibana扩展能力强
社区活跃、生命力强

面临的问题

版本更新快
前端技术更新快
代码侵入后难以维护
业务后端es版本更新跟不上

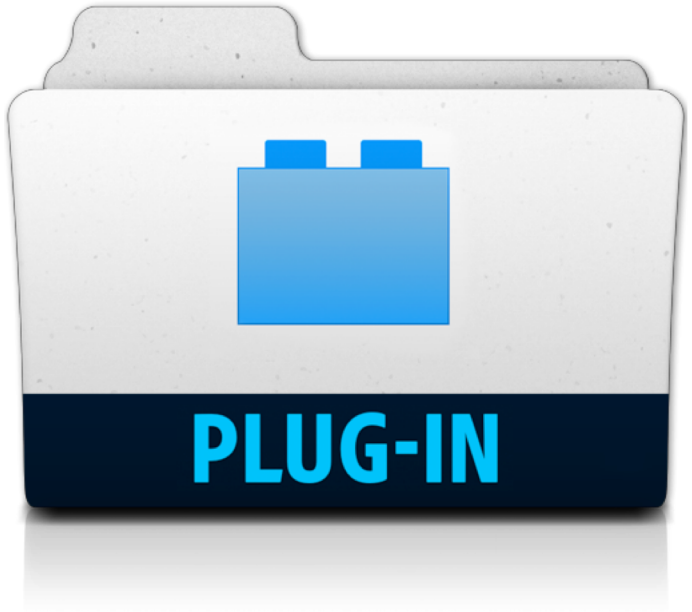
Kibana Release Notes

This section summarizes the changes in each release.

- *Kibana 6.4.2*
- *Kibana 6.4.1*
- *Kibana 6.4.0*
- *Kibana 6.3.2*
- *Kibana 6.3.1*
- *Kibana 6.3.0*
- *Kibana 6.2.4*
- *Kibana 6.2.3*
- *Kibana 6.2.2*
- *Kibana 6.2.1*
- *Kibana 6.2.0*
- *Kibana 6.1.4*
- *Kibana 6.1.3*
- *Kibana 6.1.2*
- *Kibana 6.1.1*
- *Kibana 6.1.0*
- *Kibana 6.0.1*
- *Kibana 6.0.0*

无侵入

一切皆plugin（server/ui）
独立app
装饰器
代理

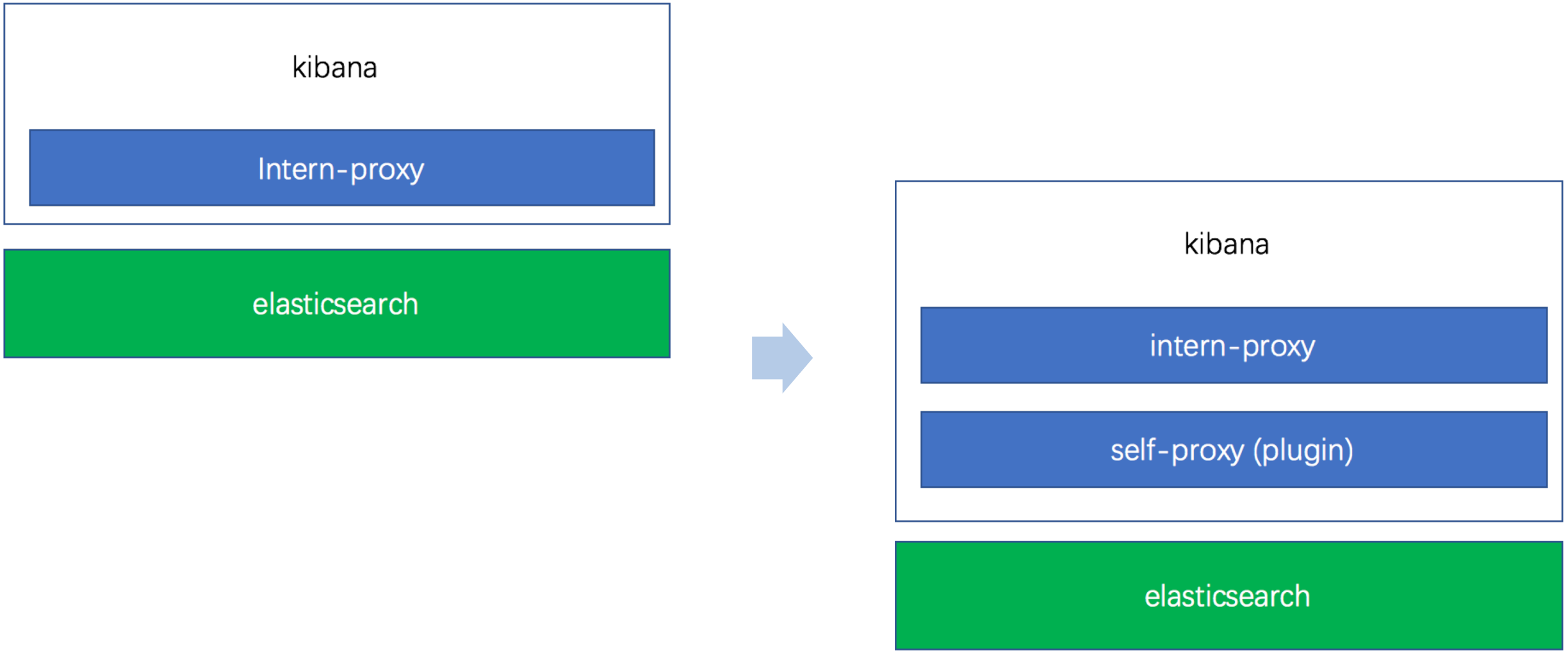


一切皆插件

独立app

独立菜单
独立页面
独立逻辑
甚至多种可选技术栈

代理


kibana
Intern-proxy
elasticsearch
kibana
intern-proxy
self-proxy (plugin)
elasticsearch

插件形式的代理：

优点：可复用kibana代码
可对es查询请求，查询结果进行更改定制
可以兼容es版本

缺点：只适用于kibana层

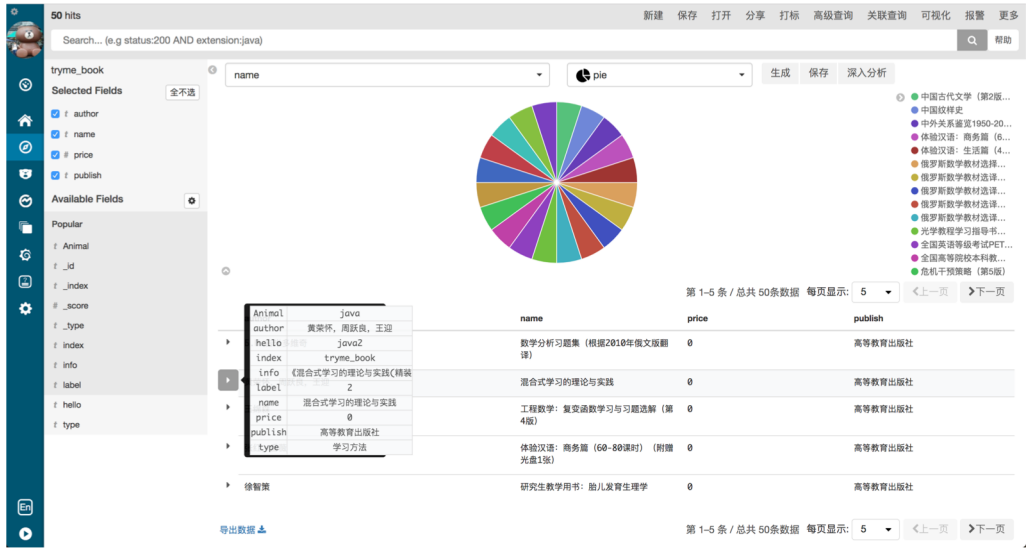
装饰器

angular装饰器:

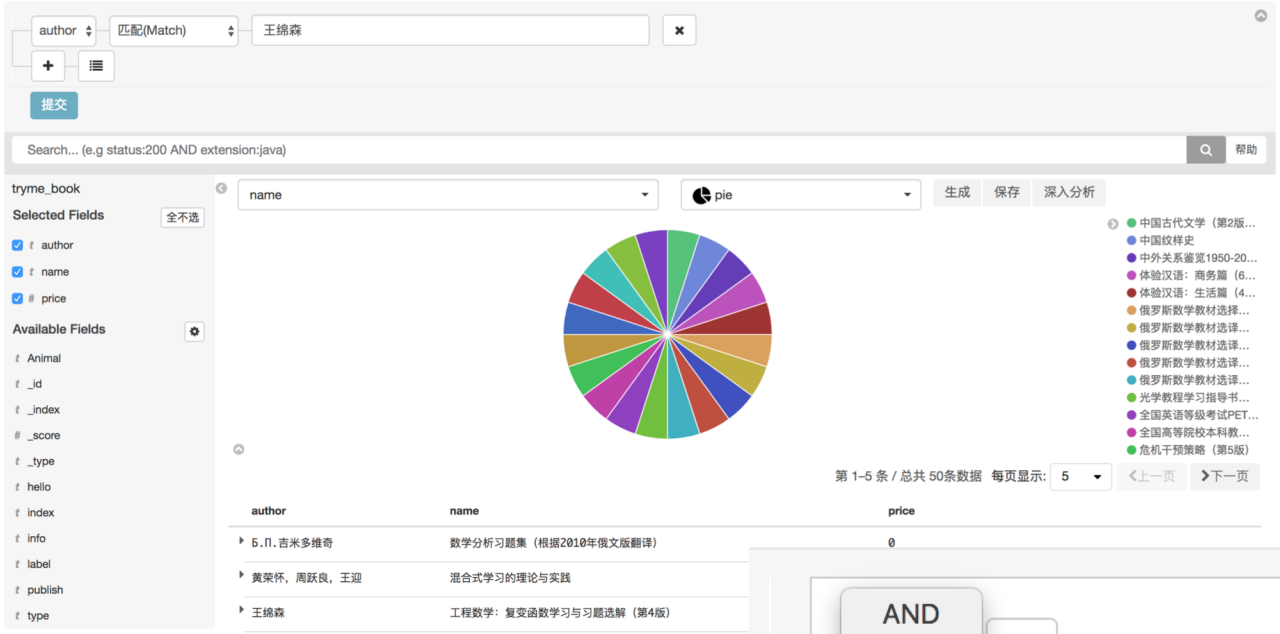
优点：无侵入更改html, javascript, css
缺点：可能会多写一些重复代码
kibana源码变动后装饰器部分的代码也需要相应变化

03

示例


50 hits
新建 保存 打开 分享 打标 高级查询 关联查询 可视化 报警 更多
Search... (e.g status:200 AND extension:java)
帮助
tryme_book
Selected Fields
全不选
author
name
price
publish
Available Fields
Popular
Animal
_id
_index
_score
_type
index
info
label
hello
type
name
pie
生成 保存 深入分析
第 1–5 条 / 总共 50条数据 每页显示: 5
上一页 下一页
Animal java
author 黄荣怀，周跃良，王迎
hello java2
index tryme_book
info 《混合式学习的理论与实践(精装
label 2
name 混合式学习的理论与实践
price 0
publish 高等教育出版社
type 学习方法
name price publish
数学分析习题集（根据2010年俄文版翻译） 0 高等教育出版社
混合式学习的理论与实践 0 高等教育出版社
工程数学：复变函数学习与习题选解（第4版） 0 高等教育出版社
体验汉语：商务篇（60-80课时）（附赠光盘1张） 0 高等教育出版社
徐智策
研究生教学用书：胎儿发育生理学 0 高等教育出版社
导出数据
第 1–5 条 / 总共 50条数据 每页显示: 5
上一页 下一页

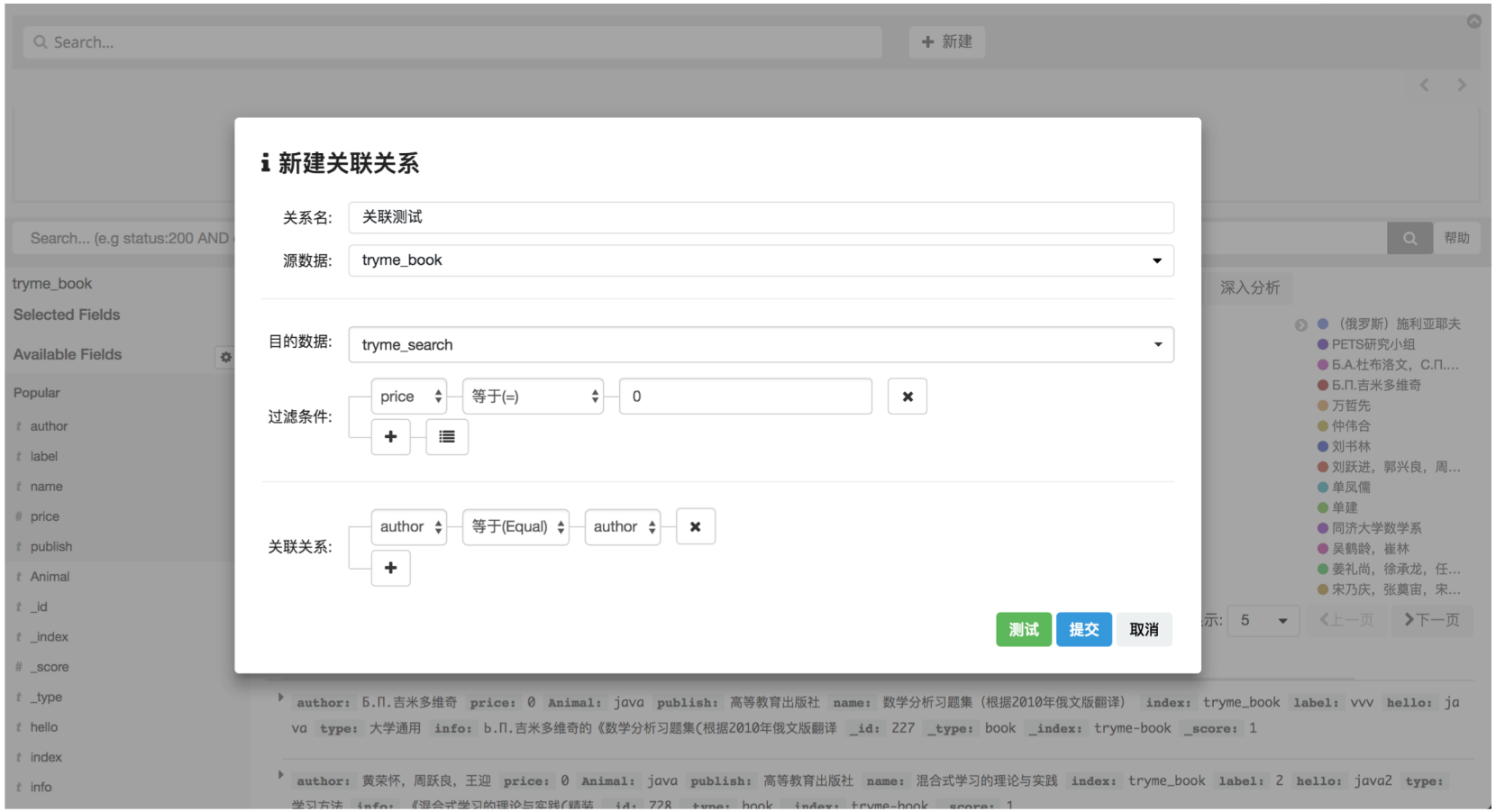
高级查询插件


author
匹配(Match)
王绵森
提交
Search... (e.g status:200 AND extension:java)
帮助
tryme_book
Selected Fields
全不选
t author
t name
price
Available Fields
t Animal
t _id
t _index
_score
t _type
t hello
t index
t info
t label
t publish
t type
name
pie
生成
保存
深入分析
中国古代文学（第2版...
中国纹样史
中外关系鉴览1950-20...
体验汉语：商务篇（6...
体验汉语：生活篇（4...
俄罗斯数学教材选择...
俄罗斯数学教材选译...
俄罗斯数学教材选译...
俄罗斯数学教材选译...
俄罗斯数学教材选译...
光学教程学习指导书...
全国英语等级考试PET...
全国高等院校本科教...
危机干预策略（第5版）
第 1–5 条 / 总共 50条数据 每页显示: 5
上一页
下一页
author
name
price
Б.П.吉米多维奇
数学分析习题集（根据2010年俄文版翻译）
0
黄荣怀，周跃良，王迎
混合式学习的理论与实践
王绵森
工程数学：复变函数数学习与习题选解（第4版）
张红，岳薇
体验汉语：商务篇（60-80课时）（附赠光盘1张）
徐智策
研究生教学用书：胎儿发育生理学


AND
OR
NOT
author
匹配(Match)
王绵森
price
等于(=)
0
提交

关联查询插件

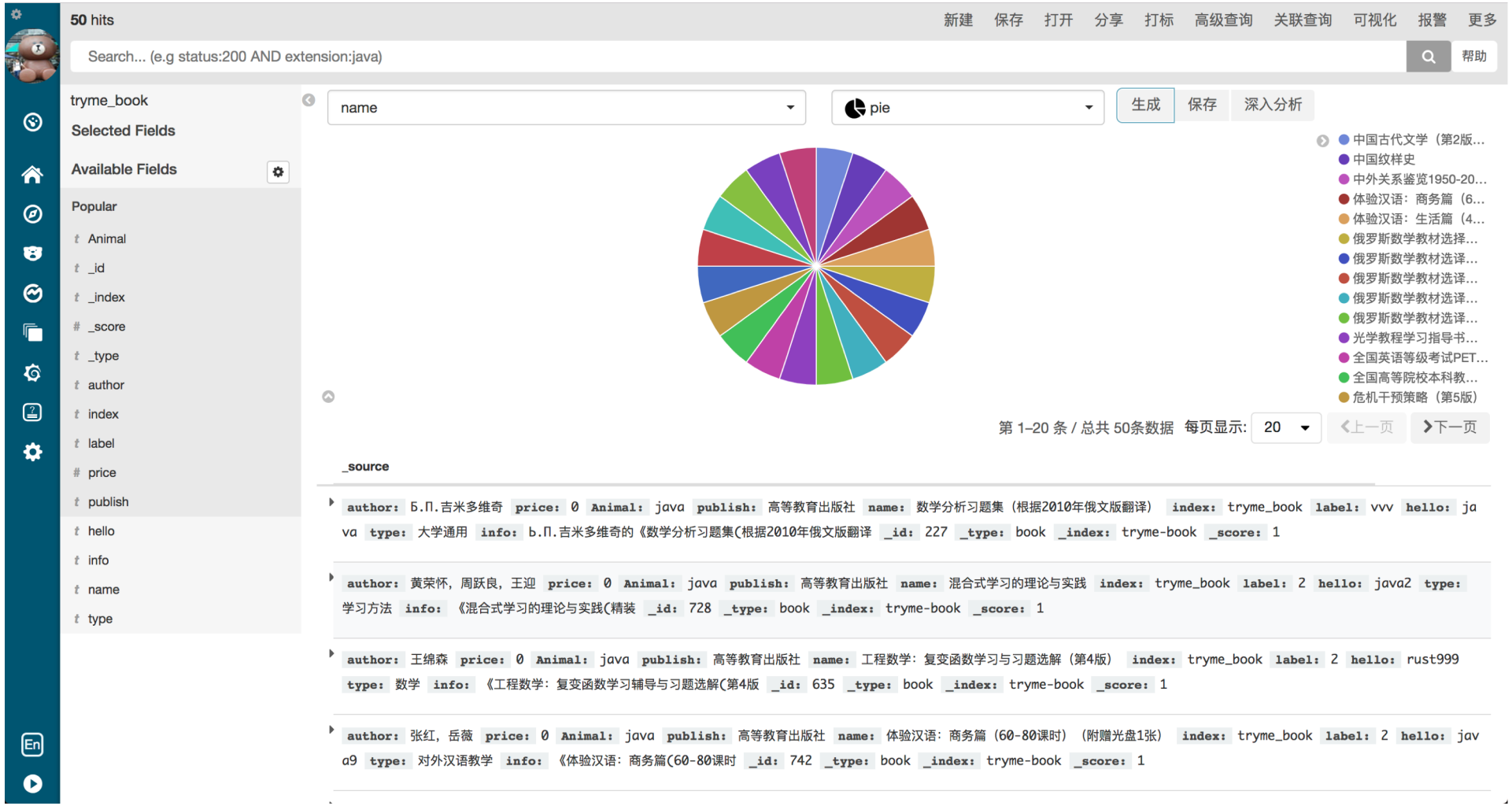
```
SELECT *
FROM tryme_search
WHERE name IN (
   SELECT name
   FROM tryme_book
   WHERE price > 0
   LIMIT 10000
)
```



原理：

Terms
（indices.query.bool.max_clause_count）
AppState
Rison

Discover聚合插件



04

开源

Plugins

05 总结

Kibana不仅仅是Elasticsearch的UI，更是一个具备良好扩展性的框架

THANKS && QA

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