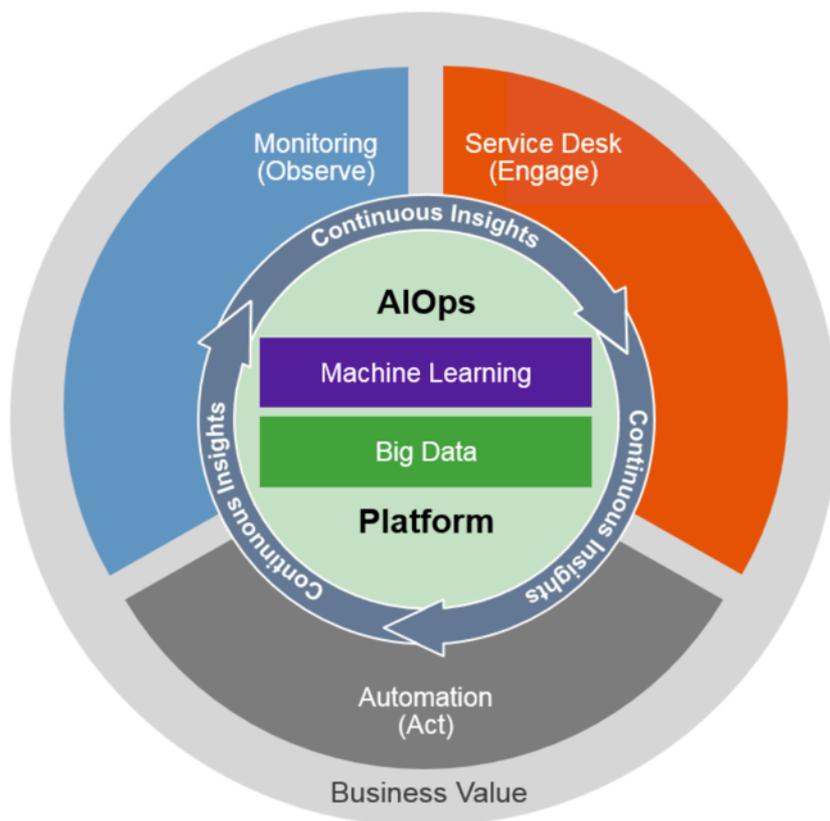


- ▶ IT 运维分析 (ITOA , IT Operation Analytics)
- ▶ 智能运维 (AIOps , Algorithmic IT Operations)
- ▶ 日志的应用场景
- ▶ 日志搜索分析引擎
- ▶ 日志易的一些用例

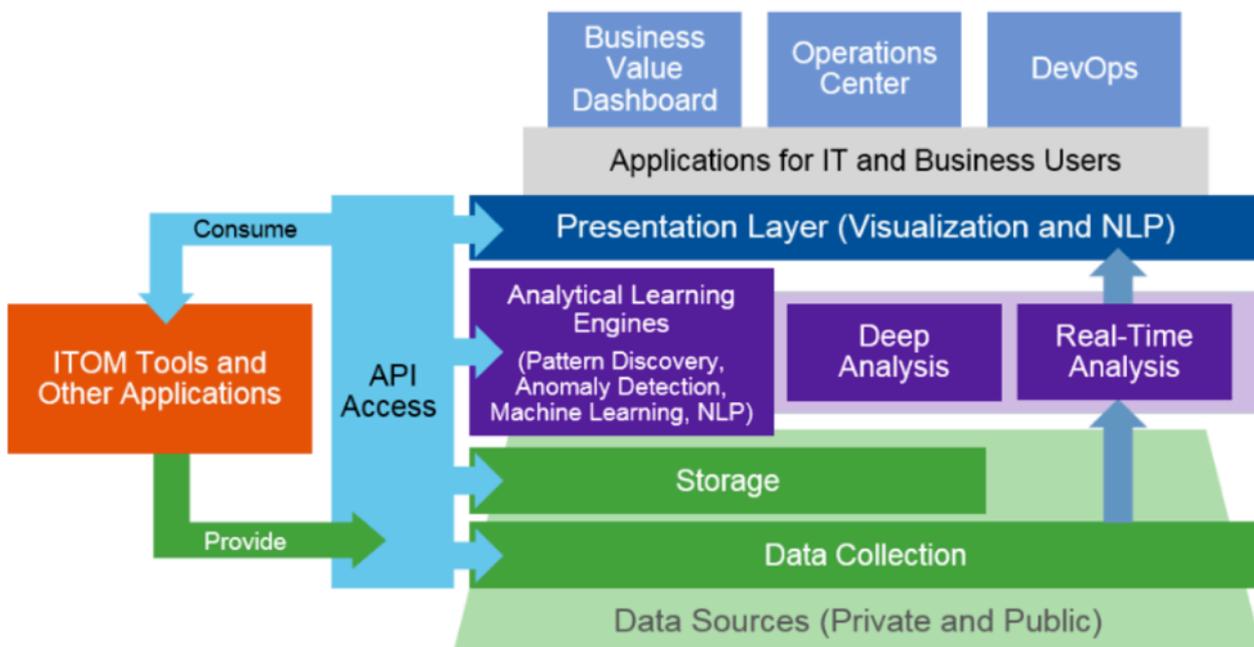
- ✦ 从 IT Operation Management (ITOM) 到 IT Operation Analytics (ITOA)
- ✦ 大数据技术应用于IT运维，通过数据分析提升IT运维效率
 - 可用性监控
 - 应用性能监控
 - 故障根源分析与预警
 - 容量规划
 - 安全审计
- ✦ Gartner估计，到2017年15%的大企业会积极使用ITOA；而在2014年这一数字只有5%

- ✦ AIOp (Algorithmic IT Operation)
- ✦ 把机器学习、人工智能应用在运维领域



智能运维架构

- ✦ 数据采集：日志、事件、性能指标
- ✦ 数据存储：非结构化数据存储
- ✦ 数据分析：深度分析、实时分析
- ✦ 数据展现：可视化、自然语言



IT运维的进化



• ITIL

• 大数据技术

• 机器学习
• 人工智能

故障处理的进化



- 数小时、数天
- 人工判断异常

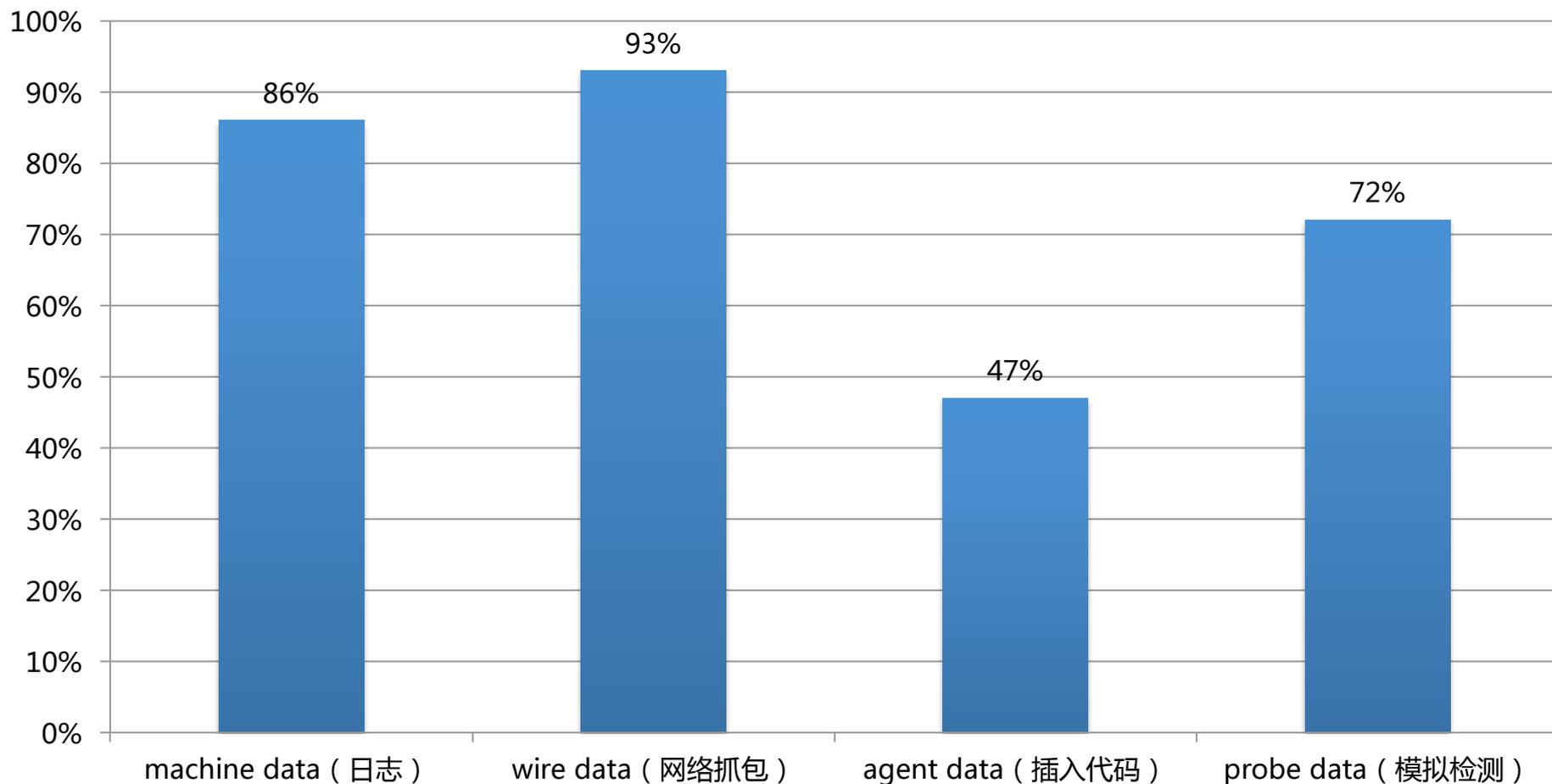
- 秒级延时
- 异常自动检测

- 预测故障
- 容量规划

ITOA 的四种数据来源

- ✦ 机器数据 (Machine Data)
 - 日志
- ✦ 通信数据 (Wire Data)
 - 网络抓包 , 流量分析
- ✦ 代理数据 (Agent Data)
 - 在 .NET/Java 字节码里插入代码 , 统计函数调用、堆栈使用
- ✦ 探针数据 (Probe Data)
 - 在各地模拟ICMP ping、HTTP GET请求 , 对系统进行检测

ITOA 四种数据来源使用占比



ITOA 四种数据来源的比较

- ✦ 机器数据（日志）
 - 日志无所不在
 - 但不同应用输出的日志内容的完整性、可用性不同
- ✦ 通信数据（网络抓包）
 - 网络流量信息全面
 - 但一些事件未必触发网络流量
- ✦ 代理数据（嵌入代码）
 - 代码级精细监控
 - 但侵入性，会带来安全、稳定、性能问题
- ✦ 探针数据（模拟用户请求）
 - 端到端监控
 - 但不是真实用户度量（Real User Measurement）

日志，我们重要的数据资产



用户日志



业务日志



交易日志



应用及系统日志

IT系统（服务器、网络设备）每天都产生大量的日志，包含了各种设备、系统、应用、用户信息

日志：时间序列机器数据

- ✦ 带时间戳的机器数据
- ✦ IT 系统信息
 - 服务器
 - 网络设备
 - 操作系统
 - 应用软件
- ✦ 用户信息
 - 用户行为
- ✦ 业务信息
- ✦ 日志反映的是事实数据
 - “The Log: What every software engineer should know about real-time data's unifying abstraction” , Jay Kreps, LinkedIn engineer
 - 深度解析LinkedIn大数据平台 (<http://www.csdn.net/article/2014-07-23/2820811/1>)

一条 Apache Access 日志

- 180.150.189.243 - - [15/Apr/2015:00:27:19 +0800] "POST /report HTTP/1.1"
200 21 "https://rizhiyi.com/search/" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:
37.0) Gecko/20100101 Firefox/37.0" "10.10.33.174" 0.005 0.001

- 字段：

- Client IP: 180.150.189.243
- Timestamp: 15/Apr/2015:00:27:19 +0800
- Method: POST
- URI: /report
- Version: HTTP/1.1
- Status: 200
- Bytes: 21
- Referrer: <https://rizhiyi.com/search/>
- User Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:37.0) Gecko/20100101 Firefox/
37.0
- X-Forward: 10.10.33.174
- Request_time: 0.005
- Upstream_request_time:0.001

- ✦ 运维监控
 - 可用性监控
 - 应用性能监控 (APM)
 - 故障根源分析与预警
 - 容量规划
- ✦ 安全审计
 - 安全信息事件管理 (SIEM)
 - 合规审计
 - 发现高级持续威胁 (APT)
- ✦ 用户分析
- ✦ 业务分析

- ✦ 日志没有集中处理
 - 登陆每一台服务器，使用脚本命令或程序查看
- ✦ 日志被删除
 - 磁盘满了删日志
 - 黑客删除日志，抹除入侵痕迹
- ✦ 日志只做事后追查
 - 没有实时监控、分析
- ✦ 使用数据库存储日志
 - 无法适应TB级海量日志
 - 数据库的schema无法适应千变万化的日志格式
 - 无法提供全文检索

✦ Hadoop

- 批处理，不够及时
- 查询慢
- 数据离线挖掘，无法做 OLAP (On Line Analytic Processing)

✦ Storm/Spark

✦ Hadoop/Storm/Spark都只是一个开发框架，不是拿来即用的产品

✦ NoSQL

- 不支持全文检索

- ✦ 对日志实时搜索、分析
 - 日志实时搜索分析引擎
- ✦ 快
 - 日志从产生到搜索分析出结果只有几秒的延时
- ✦ 大
 - 每天处理 TB 级的日志量
- ✦ 灵活
 - Google for IT , 可搜索、分析任何日志
- ✦ Fast Big Data
 - 实时大数据

日志管理系统的进化



- 固定的schema无法适应任意日志格式
- 无法处理大数据量

- 需要开发成本
- 批处理，实时性差
- 不支持全文检索

- 实时
- 灵活
- 全文检索

- ✦ 可编程的日志实时搜索分析平台
- ✦ 搜索处理语言（ Search Processing Language, SPL）
 - SPL命令用管道符（ “|” ）或 “[[]]” 串接成脚本程序
 - 在搜索框里写 SPL 脚本，完成复杂的查询、分析，包括机器学习算法
- ✦ 可接入各种来源的数据
 - 日志文件
 - 数据库
 - 恒生电子交易系统二进制日志

✦ Schema on Write

- 索引时（入库前）抽取字段，对日志做结构化
- 检索速度快
- 但不够灵活，必须预先知道日志格式

✦ Schema on Read

- 检索时（入库后）抽取字段，对日志结构化
- 灵活，检索时根据需要抽取字段
- 但检索速度受影响

✦ 日志易同时支持 Schema on Write 和 Schema on Read

- 日志易实现机制
- 由用户选择需要的策略

- ✦ 搜索
 - 搜索日志里的任何字段
- ✦ 告警
 - 异常自动识别
- ✦ 统计分析
 - 事务关联
- ✦ 机器学习
 - 异常自动检测
 - 故障预警
 - 容量规划
- ✦ 配置解析规则，识别任何日志
 - 把日志从非结构化数据转换成结构化数据
- ✦ 开放API，对接第三方系统
- ✦ 高性能、可扩展的分布式架构
 - 索引性能：200万 EPS (Event Per Second)，40TB/天
 - 检索性能：60秒内检索1000亿条日志

日志易分析事件优势

完备的全量日志管理

日志分析的关键在于其完备性。日志易能够完整保存长周期、大容量的日志数据，为后期的分析提供了基础

可视化统计

分析人员通过几下鼠标点击，即可快速完成诸如计数、时间段、数值分布、百分比、多级汇总、地理分布等统计操作，并通过最适合的图表进行呈现



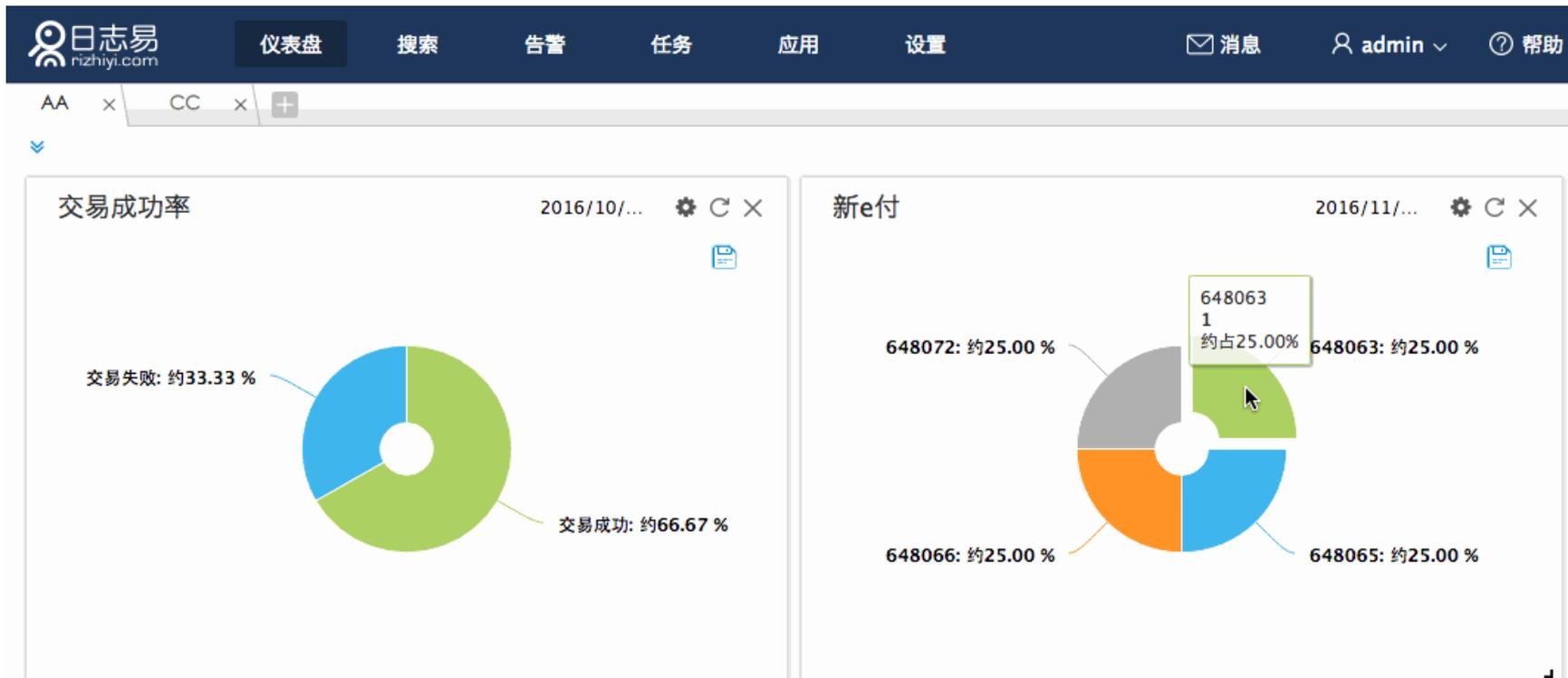
细粒度的数据分析

日志的格式、内容五花八门，对其分析的方式方法更是如此。日志易提供了灵活、高效的数据分析语句，能够帮助用户从容的进行细粒度的数据分析

秒级回馈

分析人员的任何一个想法、一个线索、一个疑点，都可以在几十甚至几秒的时间内得到验证，极大的提高了数据分析的效率

钻取分析（动画）



鼠标划选，自动生成正则表达式

划选辅助

在下面的日志样例上,用鼠标划选一段文字创建字段,字段命名捕获成功后就会高亮显示出来,重新点击高亮部分取消划选。

```
119.177.231.170 -- [09/Nov/2016:15:54:27.748 +0800] "GET /index/login/?gw_address=192.168.11.1&gw_port=2060&gw_id=0539f009979&mac=20:02:af:2f:9a:58&url=http%3A//andmbf.tj.jinshan.com/lb3d/%3Faction%3Dpush_msg_error%26channel%3D10000002%26cn%3D10000002%26install_channe%3D10000002%26version%3D212000%26imei%3D357070051130526%26mcc%3D460%26model%3DGT-I9300%26release%3D4.1.2%26sdk%3D16%26vga%3D720_1280%26dpi%3D320%26device%3Dm0chn%26cpu1%3Darmeabi-v7a%26cpu2%3Darmeabi%26uid%3D0%26cores%3D4%26did%3D97xncmaz9rodrf5ygyv7yyrhnsh8%26android_id%3Ddb500aebc574981%26app%3Dcheetah_fast%26errmsg%3Dcause%253Aorg.json.JSONException%253A%28value%28%253C%2521DOCTYPE%28%28Btype%28Bjava.lang.String%28cannot%28Bbe%28converted%28to%28BJSONObject%252C%28message%253Aparse%28the%28Bjson%28data%28of%28Bcomet%28Bnote%28failed%28err%3D-1%26nettype%3DWiFi) HTTP/1.1" 200 2341 "-" "Dalvik/1.6.0 (Linux; U; Android 4.1.2; GT-I9300 Build/JZ054K)" "-"
```

```
101.20.143.235 -- [09/Nov/2016:15:55:28.820 +0800] "GET /index/login/?gw_address=192.168.11.1&gw_port=2060&gw_id=0316YJ000364&mac=00:0c:e7:82:17:53&url=http%3A//192.168.0.1/" HTTP/1.1" 200 4605 "-" "Apache-HttpClient/UNAVAILABLE (java 1.4)" "-"
```

正则表达式:

```
^(?<clientip>[^\s]+)|^\[?<datetime>[^\]]+\]|^\[?<urlpath>[^\?]+\]|^\[?<urlargs>[^\s]+)
```

确定 取消

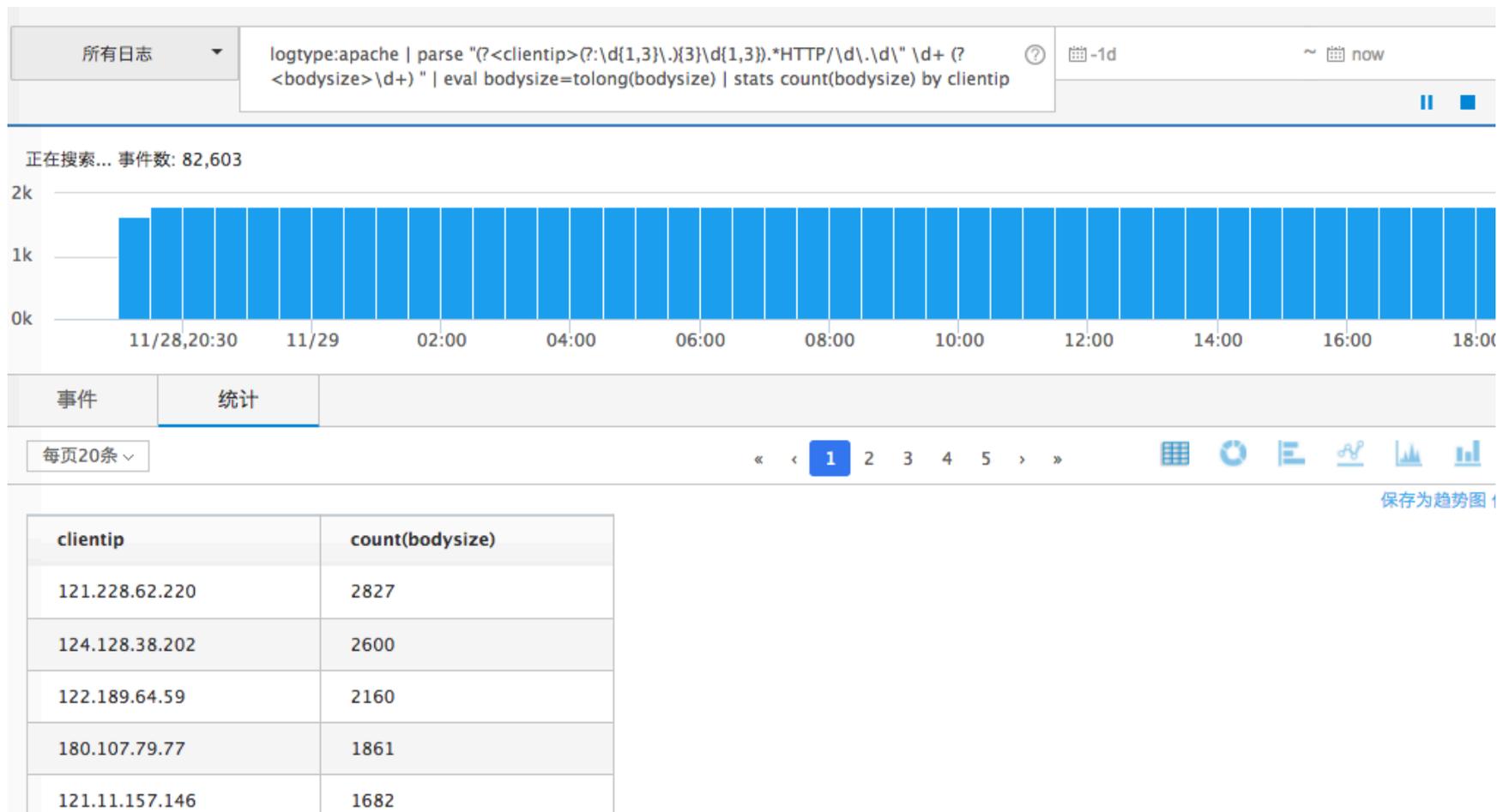
事件

使用检索日志验证 全部日志

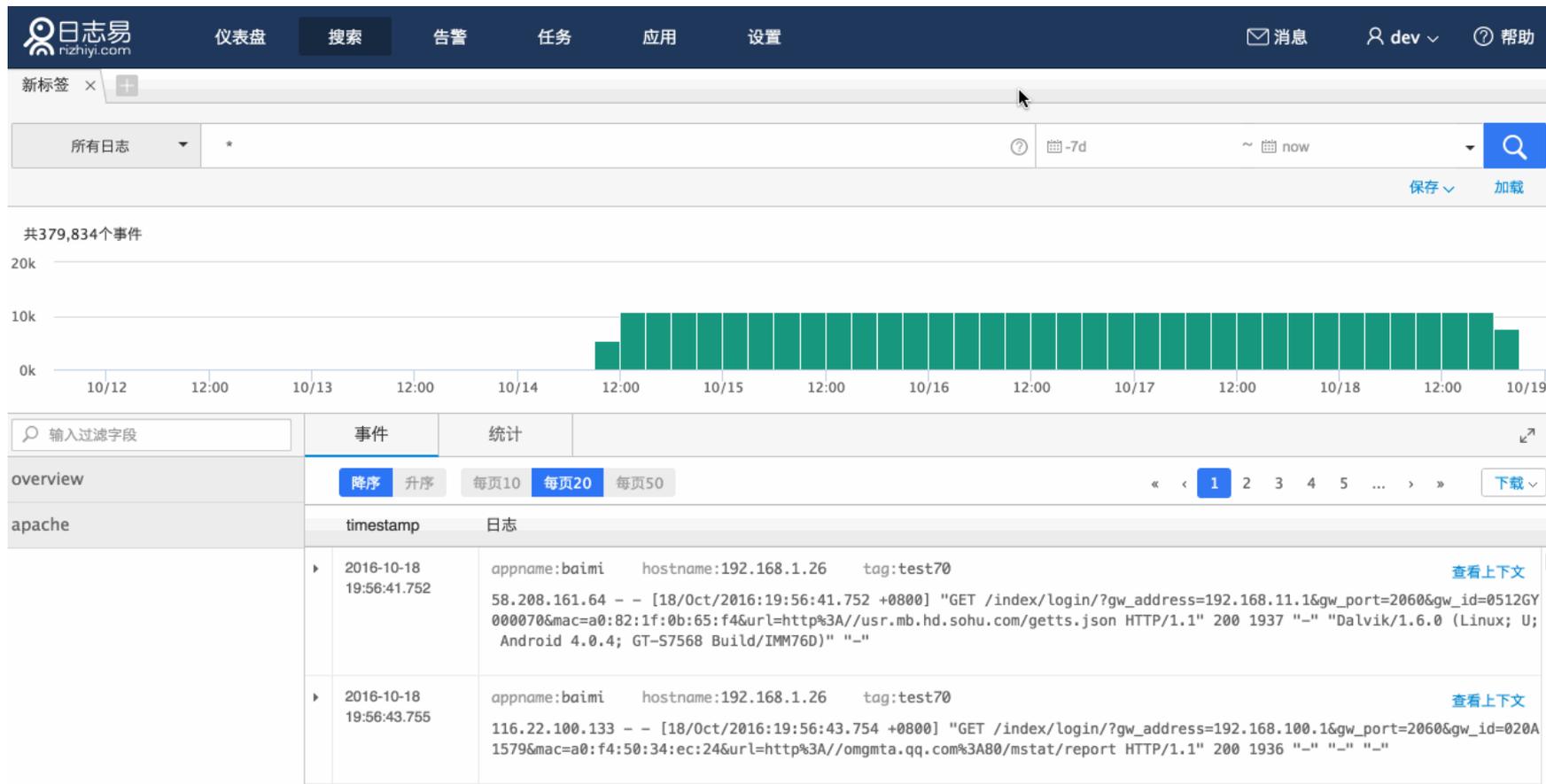
全部日志
解析成功
解析失败

状态	timestamp	raw_message	操作
✓	2016/11/09 15:55:28.821	101.20.143.235 -- [09/Nov/2016:15:55:28.820 +0800] "GET /index/login/?gw_address=192.168.11.1&gw_port=2060&gw_id=0316YJ000364&mac=00:0c:e7:82:17:53&url=http%3A//192.168.0.1/ HTTP/1.1" 200 4605 "-" "Apache-HttpClient/UNAVAILABLE (java 1.4)" "-"	添加日志样例
✓	2016/11/09 15:55:26.818	112.251.194.69 -- [09/Nov/2016:15:55:26.818 +0800] "GET /index/login/?gw_address=192.168.11.1&gw_port=2060&gw_id=0539is901329&mac=f8:a4:5f:fc:8c:be&url=http%3A//drm.cmgame.com/egsb/gshare/switches HTTP/1.1" 200 1942 "-" "-"	添加日志样例
✓	112.116.106.8 -- [09/Nov/2016:15:55:25.817 +0800] "GET /index/login/?gw_address=192.168.11.1&gw_port=2060&gw_id=07c5a2776&mac=d4-07-0b-4d-63&url=http%3A//file.market.vianon.com/thumbail/sonhu180/foundApp/71h3af8-a1hr-4		

检索阶段抽取字段 (Schema on Read)



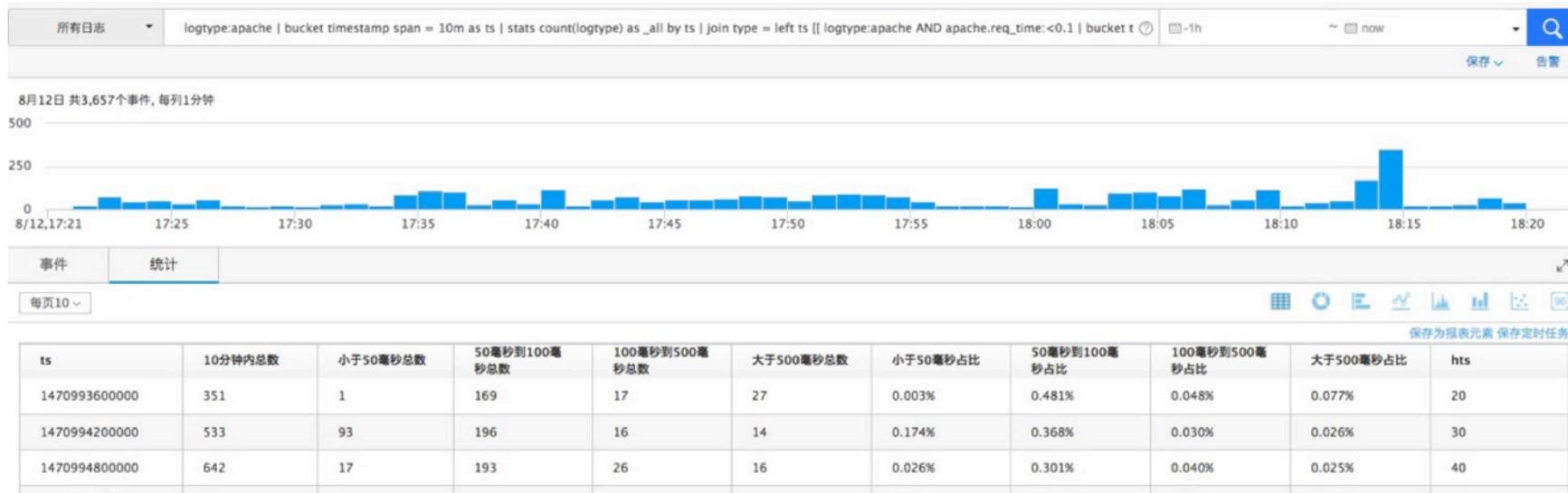
控制检索分析使用的资源 (动画)



使用SPL生成统计分析报表（1）

- logtype:apache | bucket timestamp span = 10m as ts | stats count(logtype) as _all by ts
- | join type = left ts [[logtype:apache AND apache.req_time:<0.1 | bucket timestamp span = 10m as ts | stats count(logtype) as c1 by ts]]
- | join type = left ts [[logtype:apache AND apache.req_time:[0.1 TO 0.2} | bucket timestamp span = 10m as ts | stats count(logtype) as c2 by ts]]
- | join type = left ts [[logtype:apache AND apache.req_time:[0.2 TO 0.3} | bucket timestamp span = 10m as ts | stats count(logtype) as c3 by ts]]
- | join type = left ts [[logtype:apache AND apache.req_time:>=0.3 | bucket timestamp span = 10m as ts | stats count(logtype) as c4 by ts]]
- | eval rate_c1=format("%.3f%%" ,if(empty(c1),0,c1/_all)) | eval rate_c2=format("%.3f% %" ,if(empty(c2),0,c2/_all))
- | eval rate_c3=format("%.3f%%" ,if(empty(c3),0,c3/_all)) | eval rate_c4=format("%.3f% %" ,if(empty(c4),0,c4/_all))
- | rename _all as "10分钟内总数" | rename c1 as "小于50毫秒总数" | rename c2 as "50毫秒 到100毫秒总数" | rename c3 as "100毫秒到500毫秒总数"
- | rename c4 as "大于500毫秒总数" | rename rate_c1 as "小于50毫秒占比" | rename rate_c2 as "50毫秒到100毫秒占比"
- | rename rate_c3 as "100毫秒到500毫秒占比" | rename rate_c4 as "大于500毫秒占比"
- | eval hts = formatdate(ts,"mm")

使用SPL生成统计分析报表 (2)



日志易，日志分析更容易

rizhiyi.com



微信公众号

124.83.222.115 - - [23/Apr/2015:16:28:43 +0800] "GET / HTTP/1.1" 200 53 "https://www.rizhiyi.com/docs/howto..." 537.36 (KHTML, like Gecko)

23/Apr/2015:16:27:20 +0800] "GET /saas_status_... W ebKtU537.36 (KHTML, like Gecko)

23/Apr/2015:16:27:19 +0800] "GET /saas_status_... docsiupload/risy...

23/Apr/2015:16:27:19 +0800] "GET /saas_status_... docsiupload/risy...