Gdevops

全球敏捷运维峰会

敏捷运维与日志数据分析

演讲人：唐文俊

议题

- 敏捷运维—数据驱动
- 进阶—运维分析（IT Operation Analytics）
- 日志数据—企业IT数据宝藏
- 分析流派与模式
- 分析引擎与SPL（搜索处理语言）
- 日志分析案例功能解析

敏捷运维—数据驱动

- **运维当前的状态**

✦ 15年6月CNNIC报告：手机网民5.94亿，手机支付网民2.76亿，半年增26.9%

✦ 开源社区促进技术栈高速迭代，传统ITIL需要转型DevOps式的快速响应部队

✦ 越来越可怕的漏洞和攻击行为：Bash的shellshock, OpenSSL的heartbleed,Glibc漏洞等

✦ 分布式和微服务的潮流让业务模块更加离散

✦ BAT服务器数量100万级

敏捷运维—数据驱动

- **数据驱动**

✦监控软件大多是埋点或采样式的。

✦采样意味着监控的评定是一种模糊估算，是去除了细节的大趋势上的判断。

✦在通过监控做到了总体稳定的初级目标以后，有必要通过全量数据分析的方式，对细节做更明确、更高效的诊断和优化。

✦随着技术的发展，大数据的兴起，靠数据来驱动运维，也成为可能。

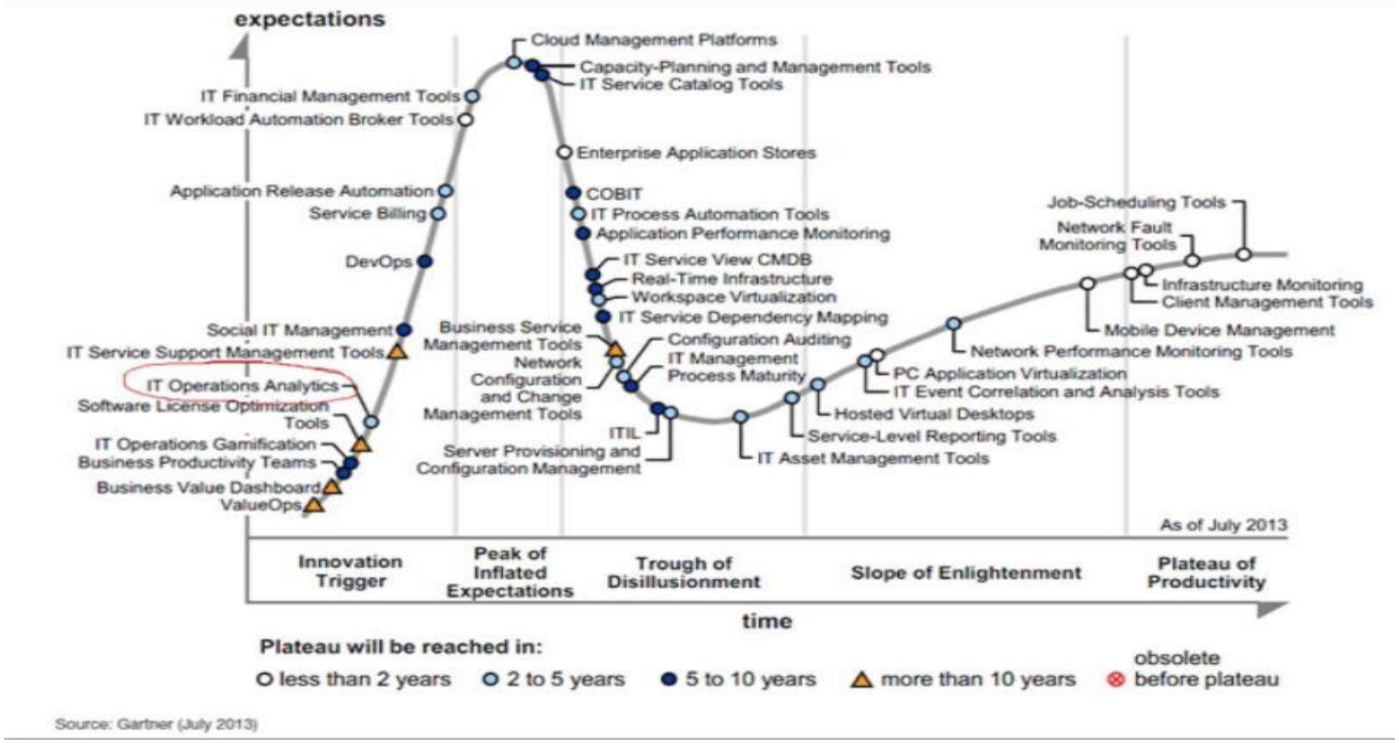
敏捷运维—数据驱动

✦ITOA(IT运营分析，IT Operations Analytics）将IT配置、变换和运行历程中孕育产生的海量数据转化为清楚地、可付诸实施的解决要领，客户通过使用ITOA产品生成的报表可以大大地缩短妨碍修复时间，减少变乱和宕机次数，实现无端障的应用颁布和系统升级。

进阶—运维分析

（IT Operation Analytics）

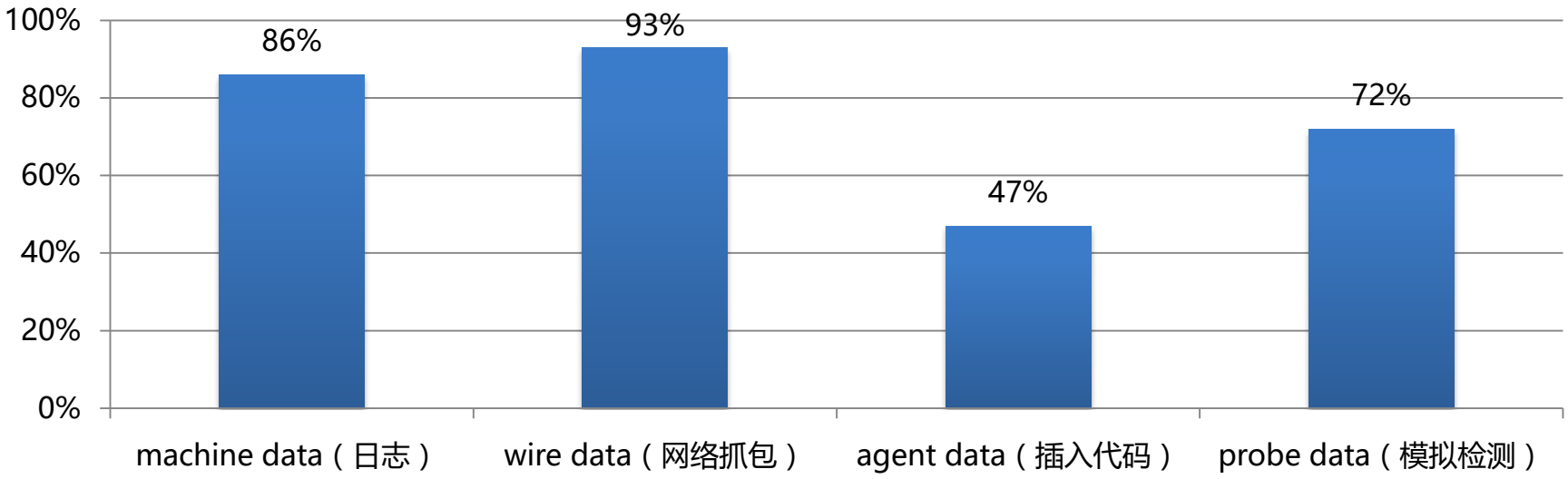
Gartner对ITOA发展的展望



✦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%

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



日志数据—企业IT数据宝藏

- 来自最终用户端的数据（客户端crash、启动速度、下载速度、首屏时间、DNS时间）
- 来自设备资源的数据（交换机，防火墙，数据库，以及不同业务的带宽、CPU、内存、IO）
- 来自服务资源的数据（响应时间、成功率、异常状态码、缓存命中率、qps）
- 来自业务接口的数据（接口响应时间、超时和失败率、调用链）

行为日志

网络日志

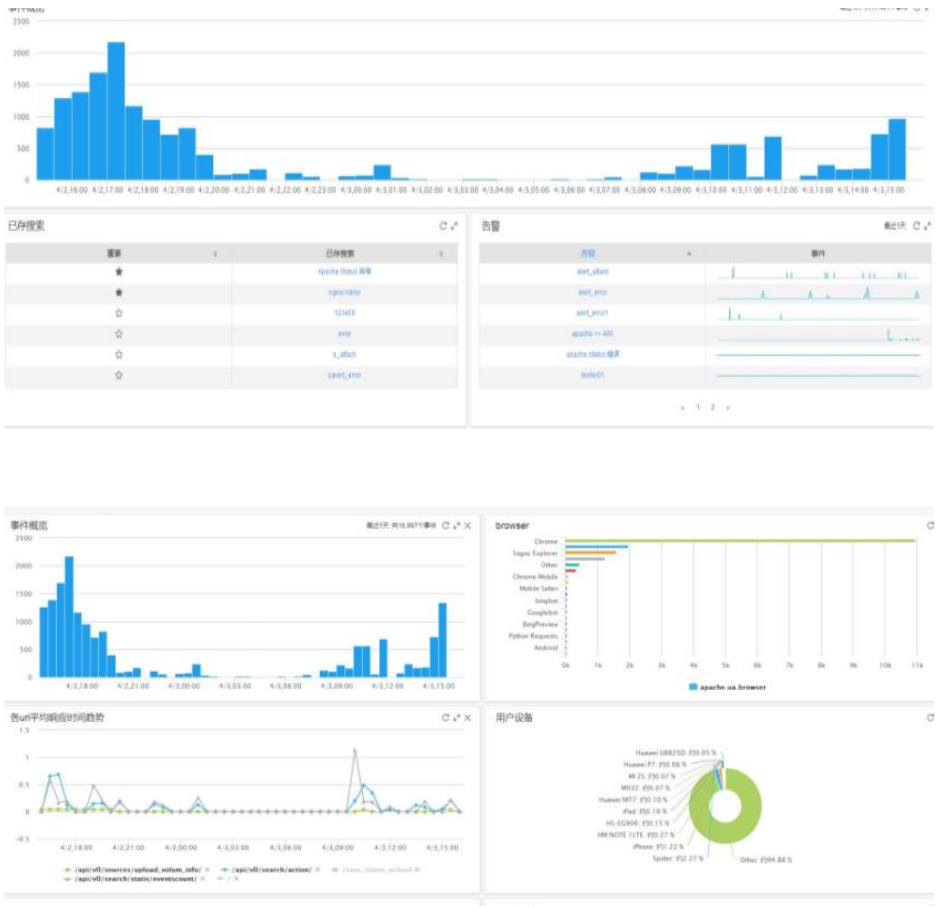
交易日志

应用及系统日志

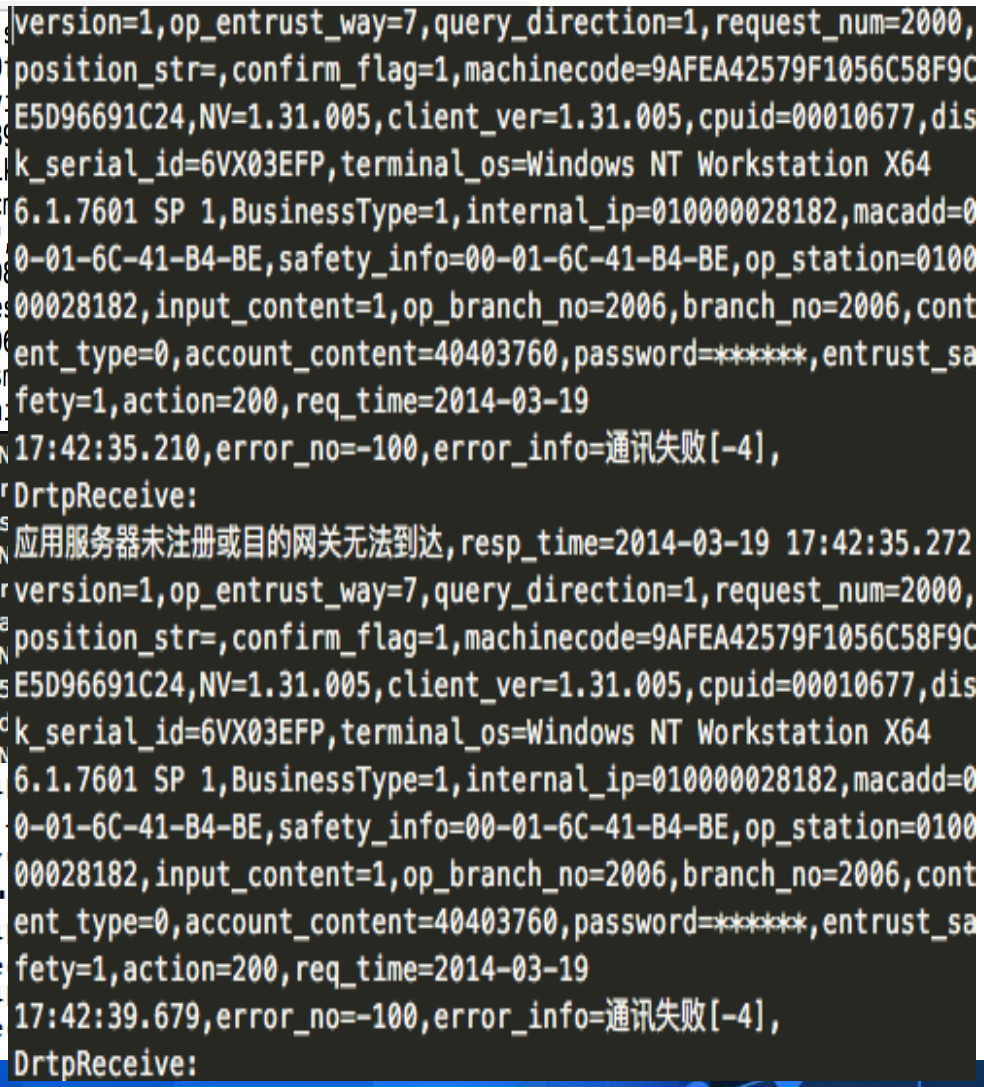
IT系统（服务器、网络设备）每天都产生大量的日志，包含了各种设备、系统、应用、用户信息

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

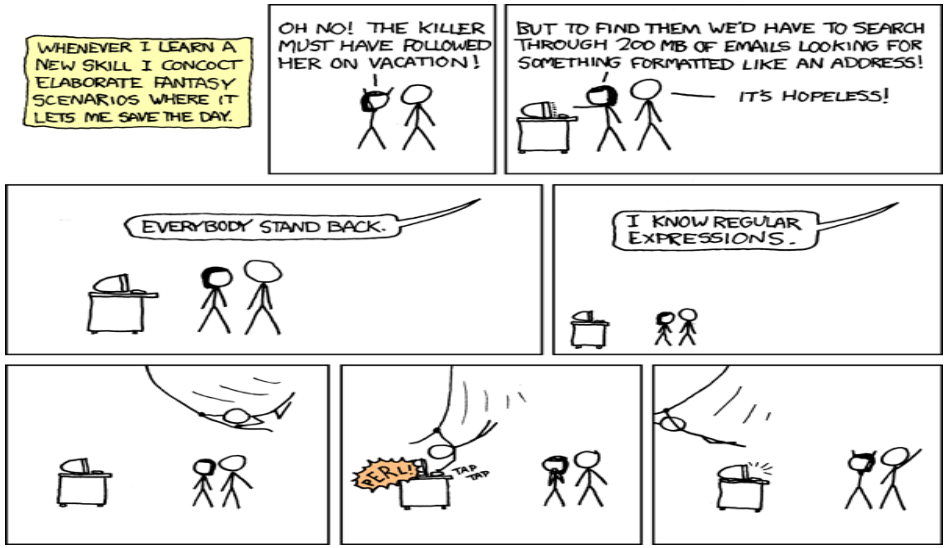


一些不知道是什么日志的日志



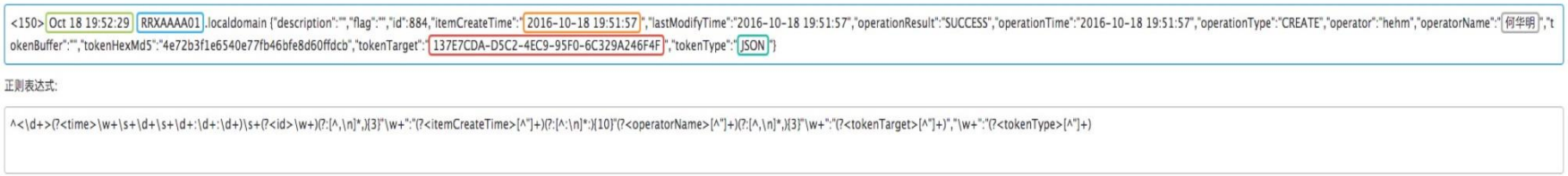
日志文件的解析转换-难点

- 日志处理系统的构建人员，并不知道日志长什么样子。
- 日志处理系统的用户，不应该投入过多精力在这个数据归一化的过程中

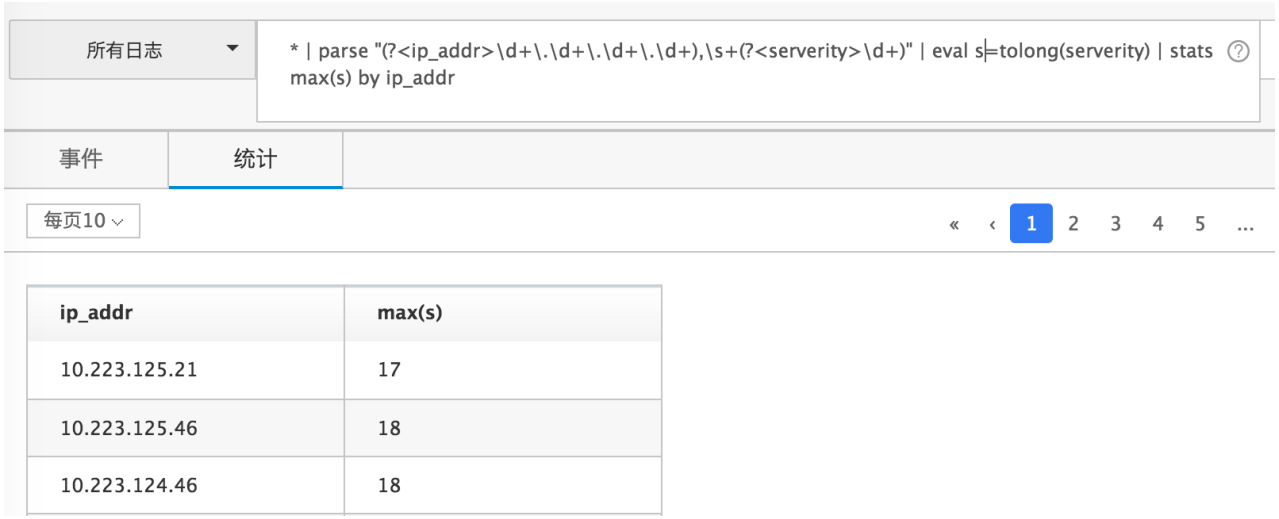


日志文件的解析转换-难点

- 需要有工具解决数据解析的学习难度



- 需要有方法可以按需处理之前没解析的数据



ip_addr	max(s)
10.223.125.21	17
10.223.125.46	18
10.223.124.46	18

日志数据处理的演进

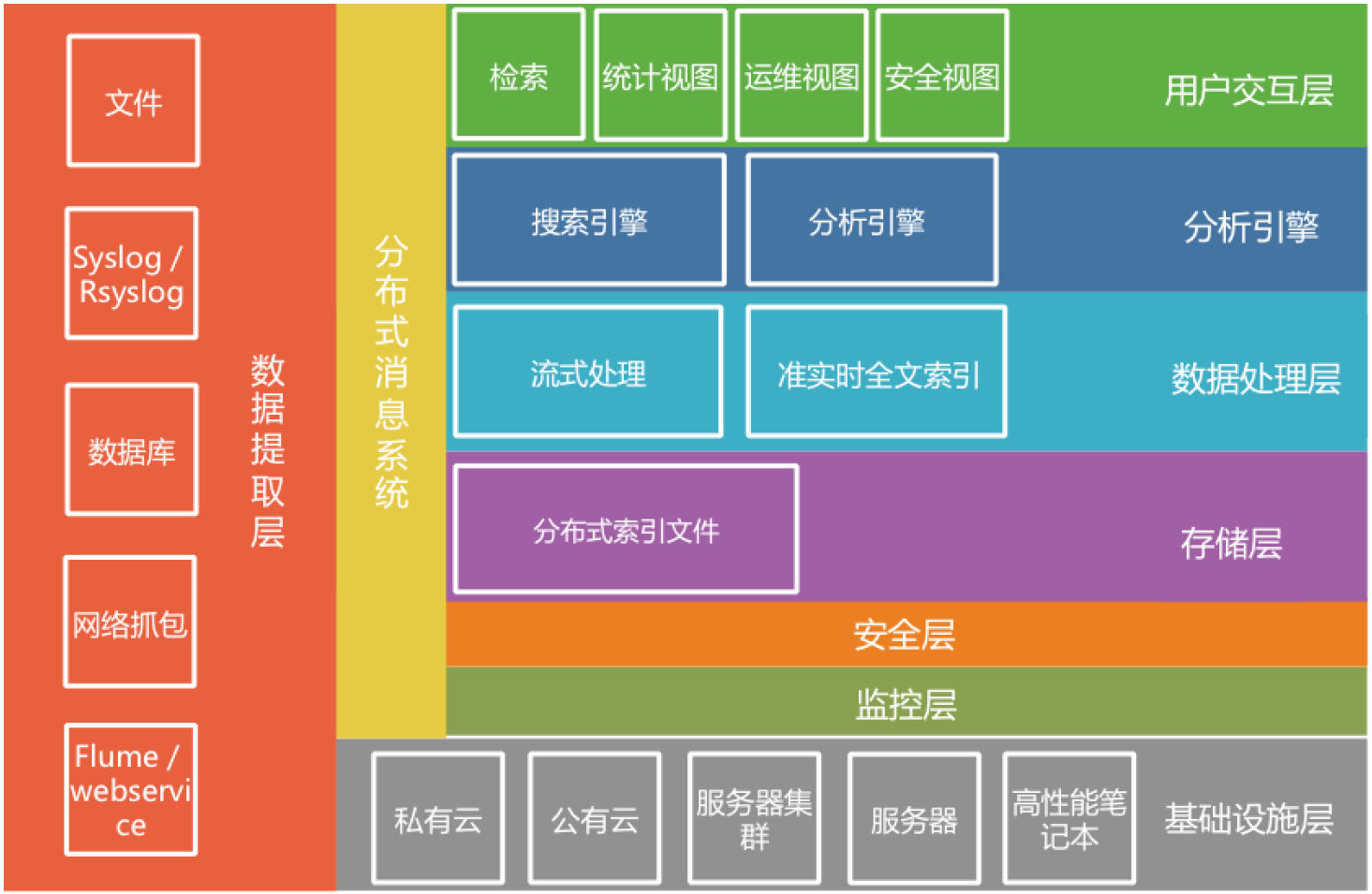
- 0.1 -- 单机grep/awk。
- 1.0 -- 存储在MySQL里，适合数百台网络设备、主机的syslog收集，每台每秒10条左右的频率。
- 2.0 -- 存储在Hadoop里，适合数百TB以上，MapReduce任务运行按小时计的长期计算任务。
- 3.0 -- 存储在实时搜索引擎里，适合无固定规则的毫秒至秒级别的查询统计任务。

- 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

分析流派与模式


文件
Syslog / Rsyslog
数据库
网络抓包
Flume / webservice
数据提取层
分布式消息系统
检索
统计视图
运维视图
安全视图
用户交互层
搜索引擎
分析引擎
分析引擎
流式处理
准实时全文索引
数据处理层
分布式索引文件
存储层
安全层
监控层
私有云
公有云
服务器集群
服务器
高性能笔记本
基础设施层

分析流派与模式

- 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

分析流派与模式

日志查询和可视化

- 日志集中管理，分为收集、存储、查询、可视化几方面。目前互联网发展的速度，日志中心普遍采用分布式集群存储日志。

- 对应的可视化方案有：
  - Graylog2：上个版本基于mongodb，现在基于ES
  - Kibana：基于ES
  - Hue：基于Hadoop

日志传输方案

- Flume：Java，apache基金会，Hadoop生态圈首选
- Scribe：C++，Facebook开源，已废弃
- Rsyslog：C，RedHat默认自带
- Fluentd：Ruby， treasuredata开源，messagepack作者
- Logstash：JRuby，Elastic开源，fpm作者
- Heka：Golang，mozilla开源，模仿Logstash，已停更

分析流派与模式

Schema on Write vs. Schema on Read

- 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
- 同时支持 Schema on Write 和 Schema on Read
  - 日志易的实现机制
  - 由用户选择需要的策略

日志分析案例功能解析

- 搜索
- 告警
- 统计
  - 事务关联
- 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、可扩展分布式架构
  - 索引性能：100万 EPS (Event Per Second)，20TB/天
  - 检索性能：60秒内检索1000亿条日志

分析引擎与SPL（搜索处理语言）

<root><fee_type>1</fee_type><input_charset>UTF-8</input_charset><out_trade_no>123456</out_trade_no><partner>123456</partner><retcode>0</retcode><retmsg>成功</retmsg><service_version>1.0</service_version><sign>123456</sign><sign_key_index>1</sign_key_index><sign_type>01</sign_type><sp_trans_id>123456</sp_trans_id><sp_user>123456</sp_user><time_end>123456</time_end><total_fee>123456</total_fee><transaction_id>123456</transaction_id></root>

所有日志

```
appname:jz AND  jz.MSG:* | eval trans=case(((jz.MSG=="实时清算完成")||(jz.MSG=="支付清算完成")||(jz.MSG=="赎回清算完成")),"赎回",((jz.MSG=="基金收益查询完成")||(jz.MSG=="余额查询完成")||(jz.MSG=="账户资料修改处理完成")),"查询",jz.MSG=="账户清算完成","开户",jz.MSG=="申购确认完成","申购",default,jz.MSG) |bucket timestamp span
```

2016/05/17 15:46:00.822 ~ 2016/05/17 16:09:59.137

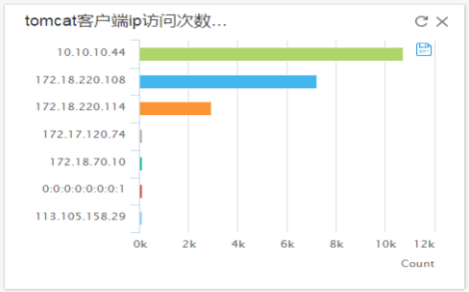
保存 告警

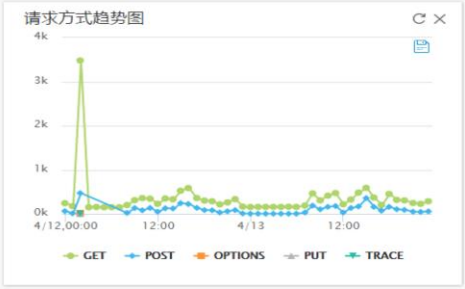
事件 统计

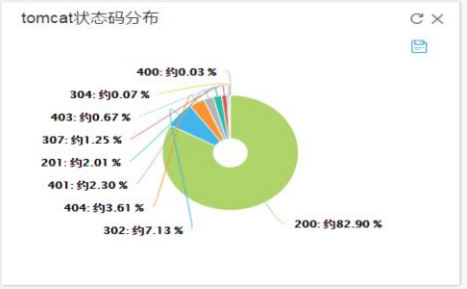
每页10 « ‹ 1 2 3 4 5 ... › »

保存为报表元素 保存定时任务

ts	trans	avg_
1463471160000	赎回	13.825283306581033
1463471160000	开户	16.84788038698329
1463471160000	查询	85.72281971580819
1463471160000	申购	11.970003671071952
1463471220000	赎回	13.869641751437403
1463471220000	开户	16.83785082872928
1463471220000	查询	84.8681521981701
1463471220000	申购	12.075921001173255
1463471280000	赎回	13.68320806771309





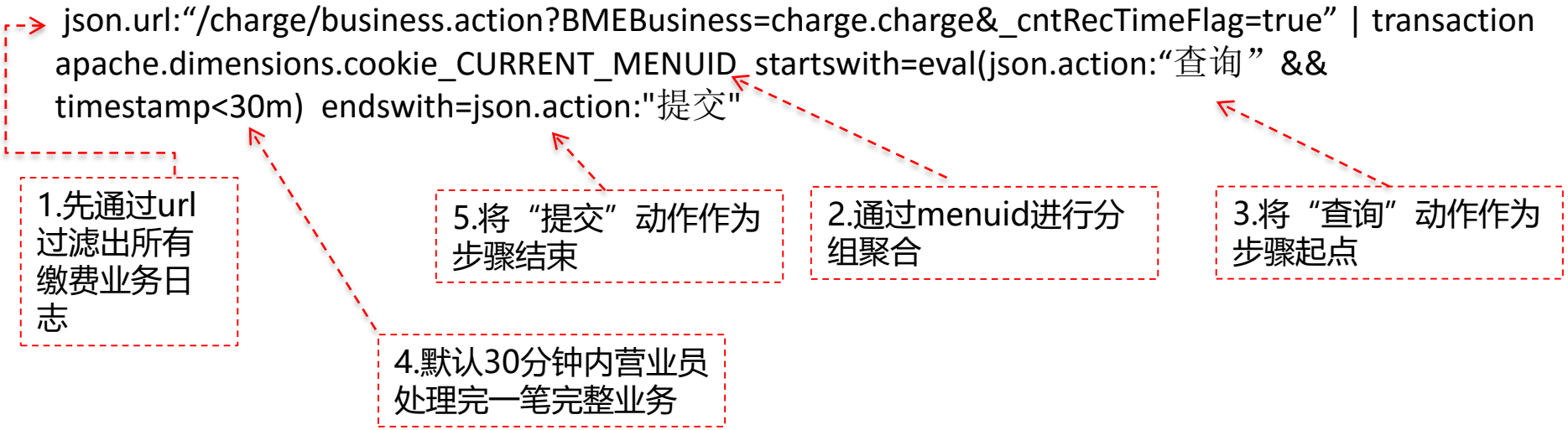


分析引擎与SPL（搜索处理语言）

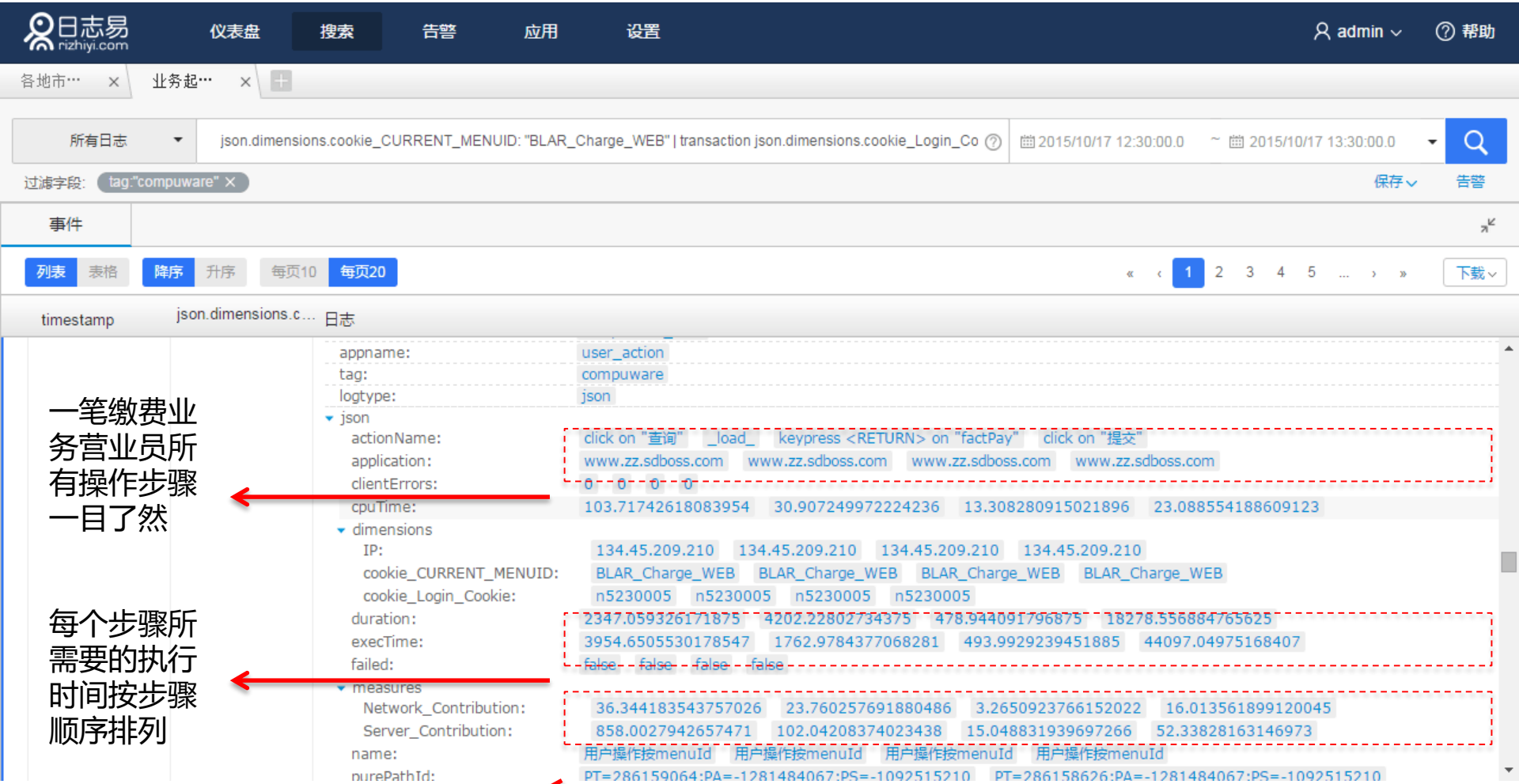
- 可编程的日志实时搜索分析平台
- 搜索处理语言（Search Processing Language, SPL）
  - SPL命令用管道符（“|”）串接成脚本程序
  - 在搜索框里写 SPL 脚本，完成复杂的查询、分析
- 可接入各种来源的数据
  - 日志文件
  - 数据库
  - 二进制日志

Search Processing Language 范例

- 中移动某省分公司
  - 分析营业厅业务办理日志
  - 聚合出每个营业员每项业务的详细操作步骤，对每个步骤操作时长进行告警、统计分析



Search Processing Language 范例



一笔缴费业务营业员所有操作步骤一目了然

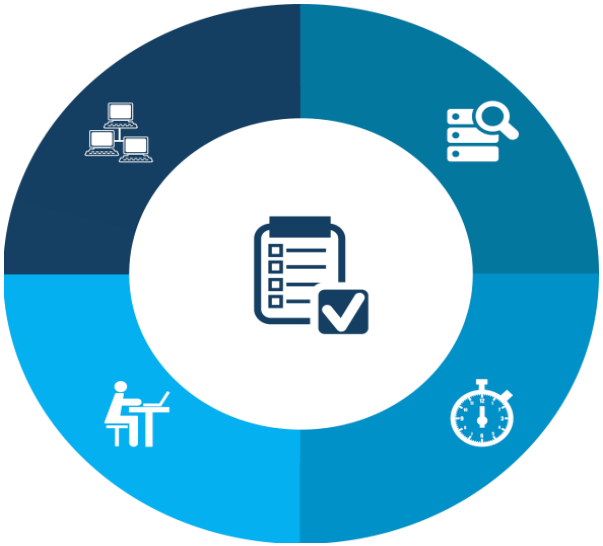
每个步骤所需要的执行时间按步骤顺序排列

网络处理时间，服务器处理时间按步骤顺序排列

分析优势

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



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

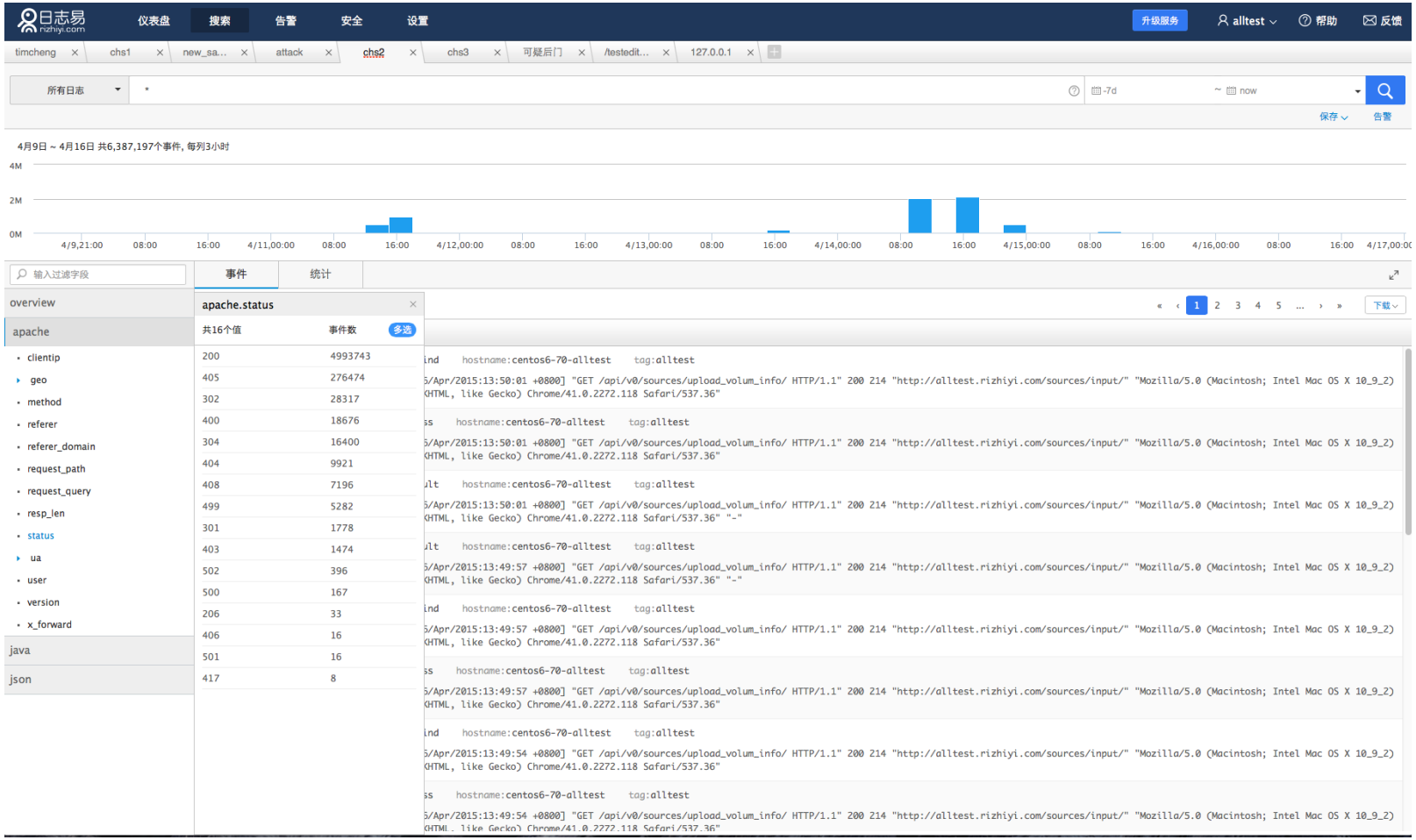
可视化统计

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

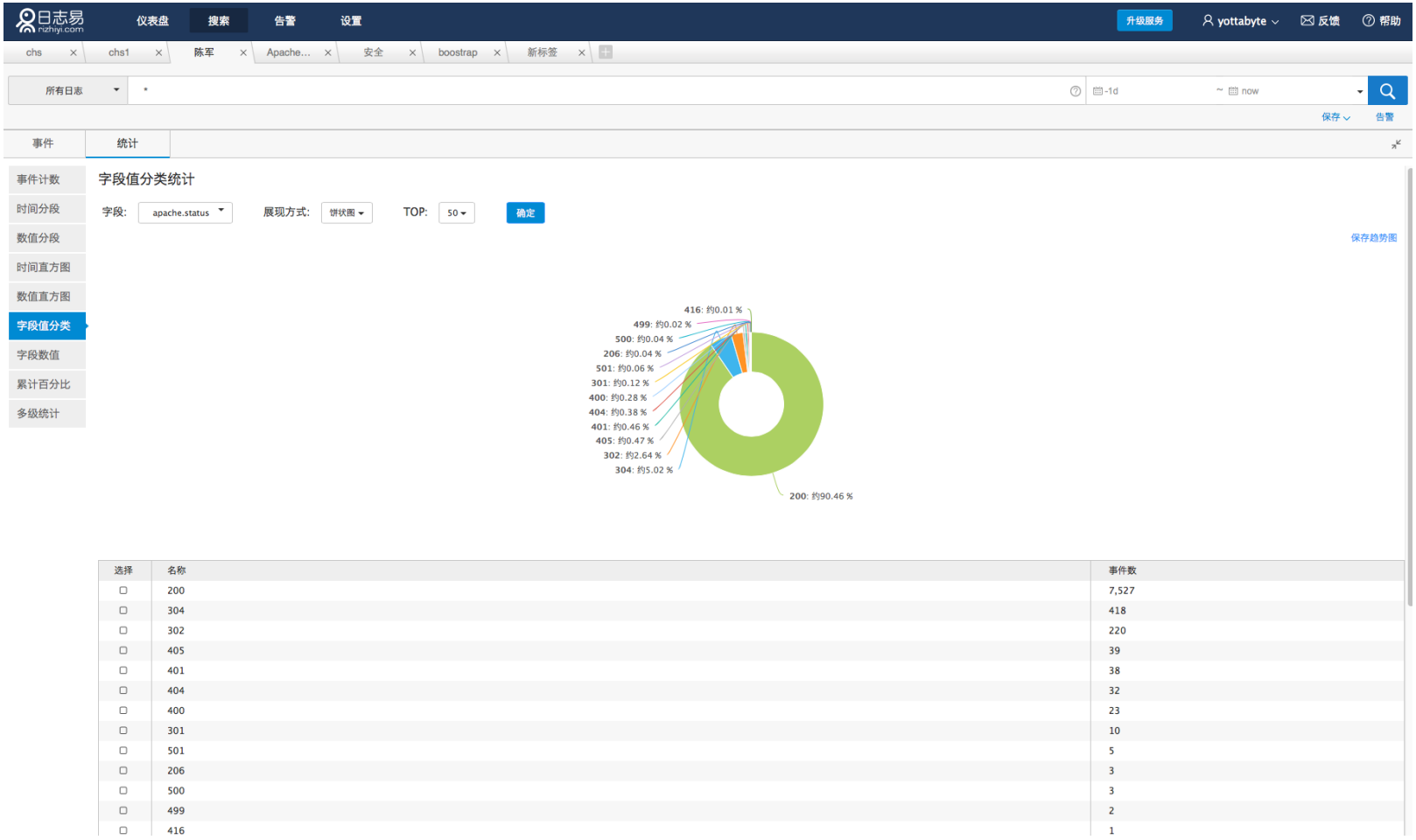
秒级回馈

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

字段抽取、统计

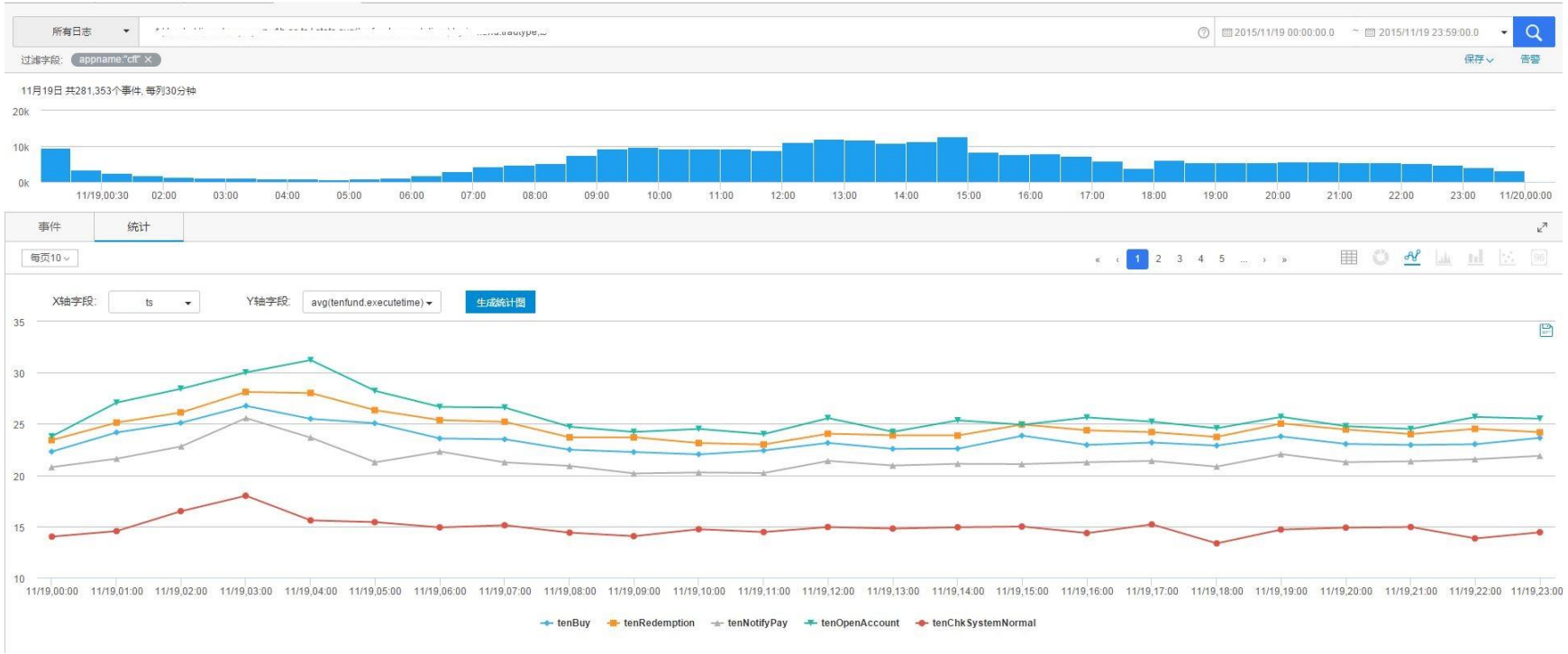

日志易
仪表盘
搜索
告警
安全
设置
升级服务
alltest
帮助
反馈
timcheng
chs1
new_sa...
attack
chs2
chs3
可疑后门
/testedit...
127.0.0.1
所有日志
*
-7d
now
保存
告警
4月9日 ~ 4月16日 共6,387,197个事件, 每列3小时
4M
2M
0M
4/9,21:00
08:00
16:00
4/11,00:00
4/12,00:00
4/13,00:00
4/14,00:00
4/15,00:00
4/16,00:00
4/17,00:00
输入过滤字段
事件
统计
overview
apache
clientip
geo
method
referer
referer_domain
request_path
request_query
resp_len
status
ua
user
version
x_forward
java
json
apache.status
共16个值
事件数
多选
200 4993743
405 276474
302 28317
400 18676
304 16400
404 9921
408 7196
499 5282
301 1778
403 1474
502 396
500 167
206 33
406 16
501 16
417 8
下载
hostname:centos6-70-alltest
tag:alltest

事件统计

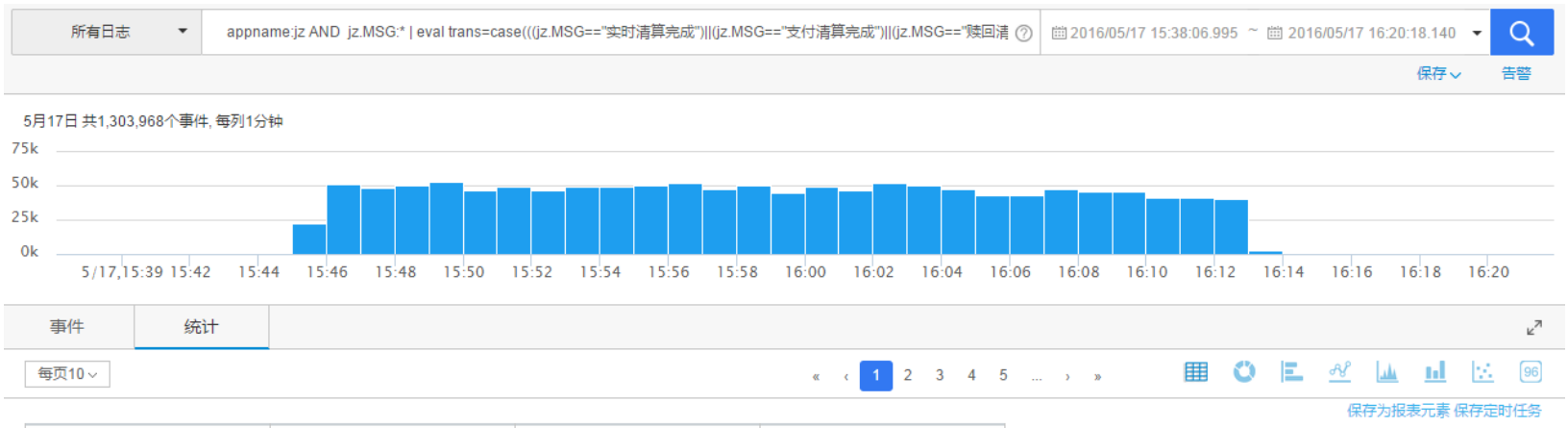


选择	名称	事件数
☐	200	7,527
☐	304	418
☐	302	220
☐	405	39
☐	401	38
☐	404	32
☐	400	23
☐	301	10
☐	501	5
☐	206	3
☐	500	3
☐	499	2
☐	416	1

通过spl语法，快速统计各类型业务每天各时段操作时长趋势



基金系统日志分析--操作频度趋势表



ts	trans	count_	time
1463471100000	赎回	16896	2016-05-17 15:45:00.000
1463471100000	开户	2571	2016-05-17 15:45:00.000
1463471100000	查询	1995	2016-05-17 15:45:00.000
1463471100000	申购	1250	2016-05-17 15:45:00.000
1463471160000	赎回	38122	2016-05-17 15:46:00.000
1463471160000	开户	5798	2016-05-17 15:46:00.000
1463471160000	查询	4580	2016-05-17 15:46:00.000
1463471160000	申购	2776	2016-05-17 15:46:00.000
1463471220000	赎回	36176	2016-05-17 15:47:00.000
1463471220000	开户	5430	2016-05-17 15:47:00.000

设备及业务运维告警

配置告警

编辑告警

*名称 switch mac地址漂移

描述 告警描述

*已存搜索 switchmac地址飘移

搜索命令 日志分组：所有日志
搜索内容：(mac AND ification) OR (mac AND move)
过滤条件：appname:"switch"

*告警类型 事件数告警

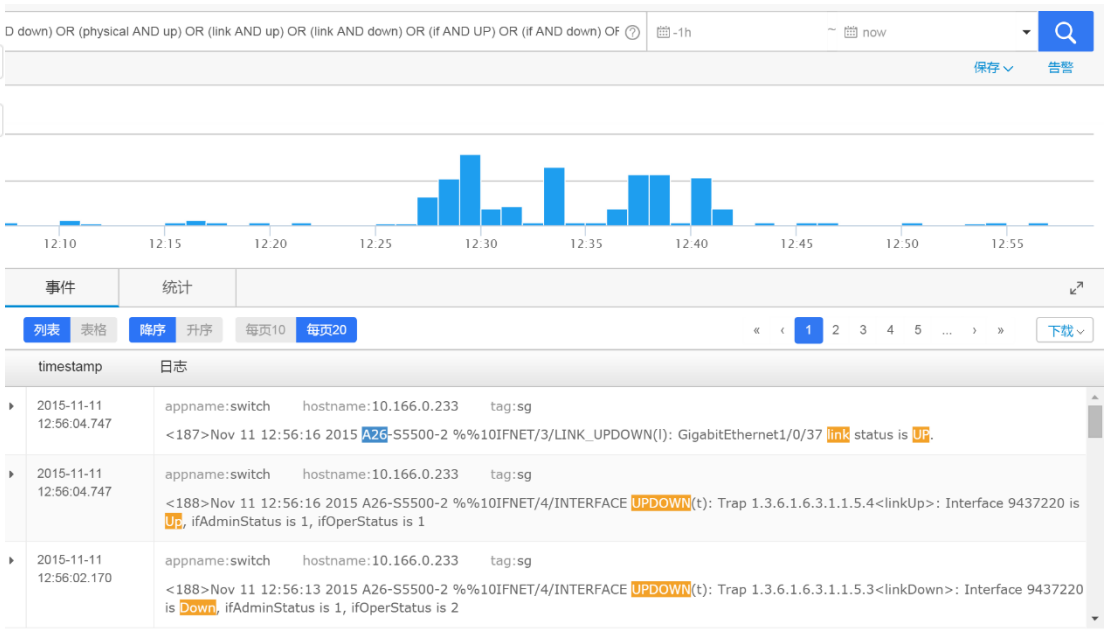
*触发条件 5 分钟 之内 计数 > 0

告警方式 发送邮件

*监测频率 3 分钟 *如果频率是秒级的，请设置大于10秒的频率！

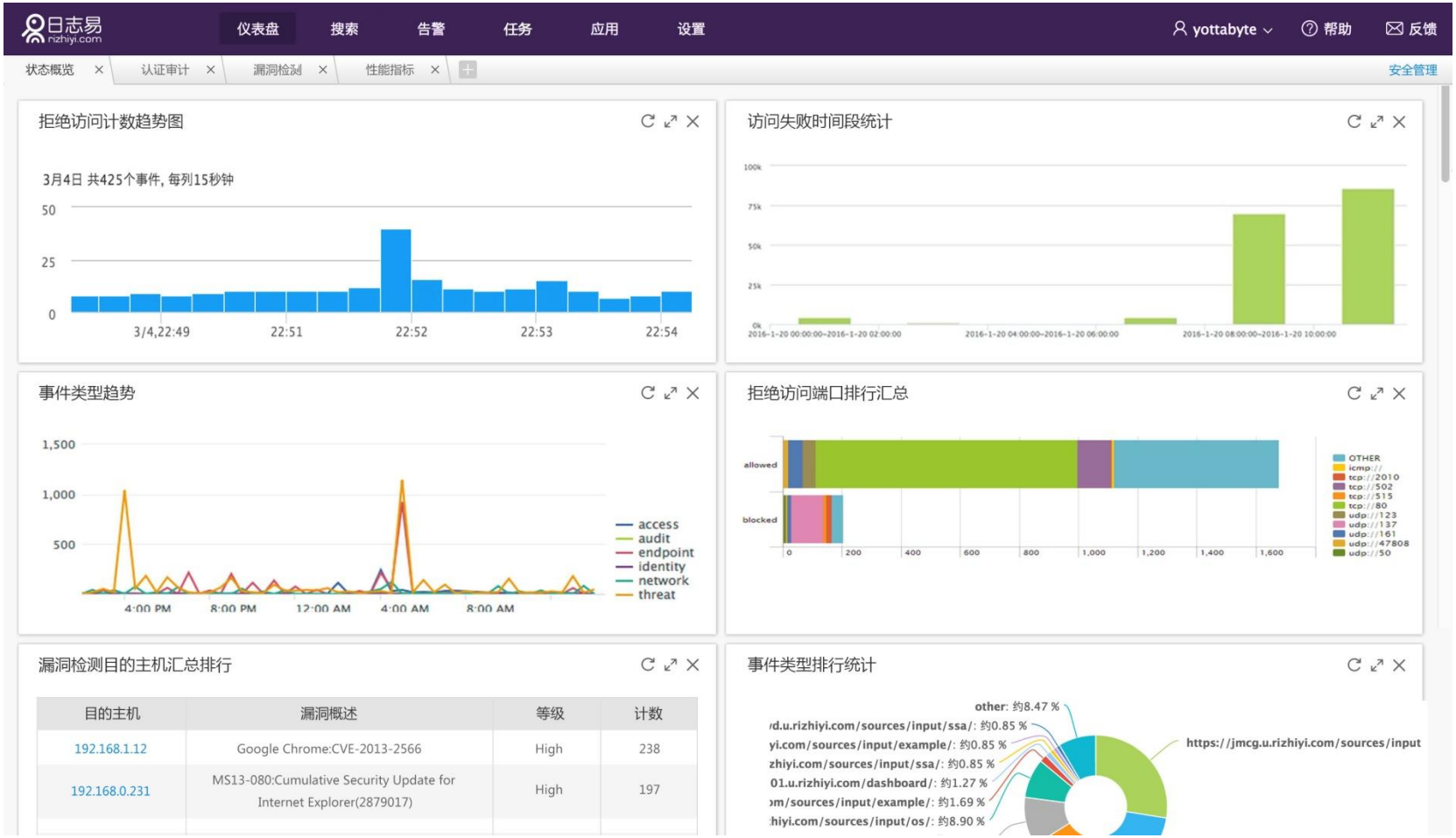
启用该告警

保存 保存 & 继续新建 取消

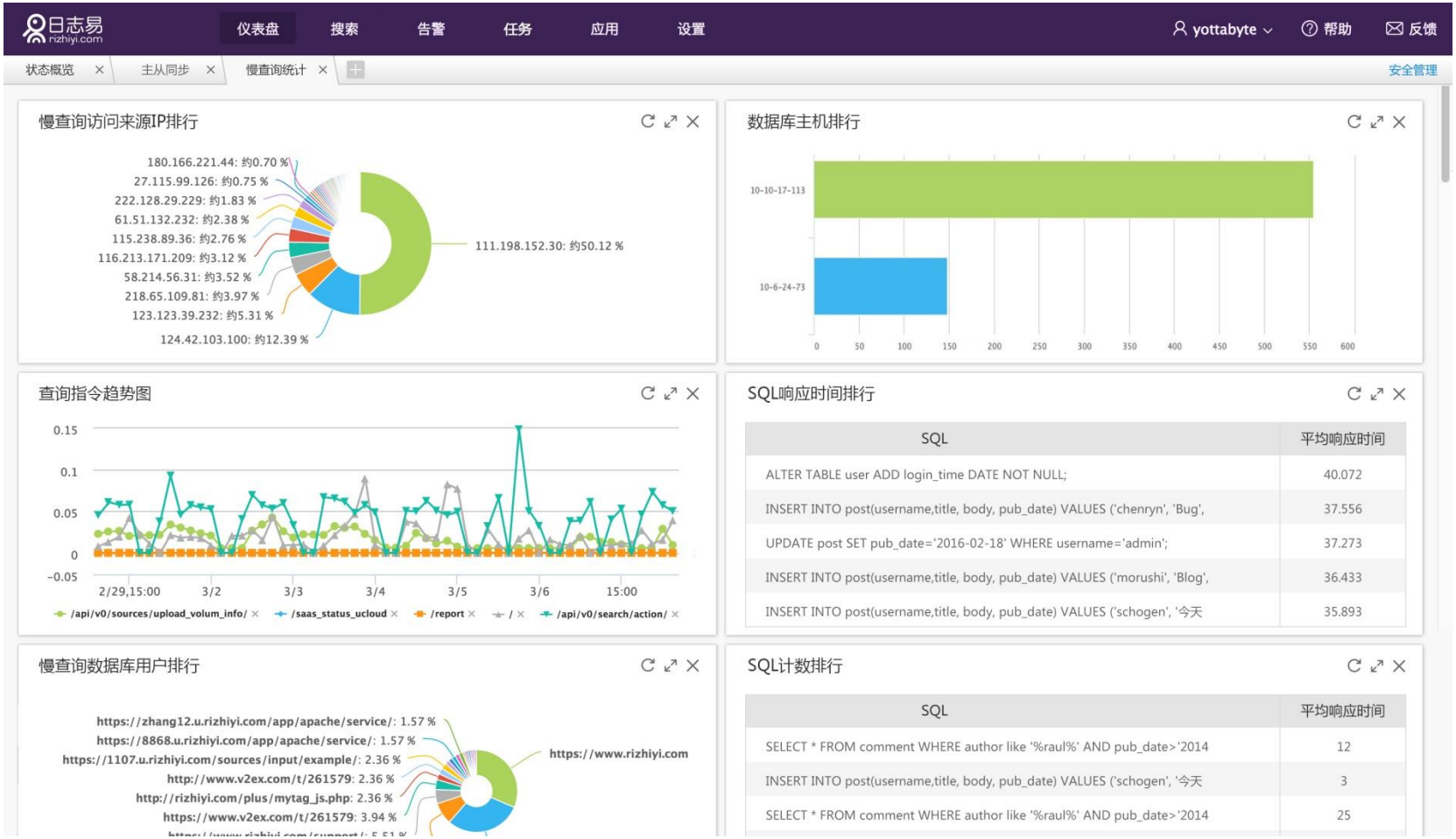


启用	名称	拥有者	频率	上次运行时间	24小时结果
☑	hljhg	admin	1分钟	2015-11-11 10:30:13	
☑	linux信息错误	admin	3分钟	2015-11-11 10:28:13	
☑	switch端口告警	admin	3分钟	2015-11-11 10:27:13	
☑	switchIP冲突告警	admin	3分钟	2015-11-11 10:30:13	
☑	switch vrrp故障	admin	3分钟	2015-11-11 10:30:13	
☑	switch 双机切换告警	admin	3分钟	2015-11-11 10:27:13	
☑	switch mac地址漂移	admin	3分钟	2015-11-11 10:27:13	

网络安全部门仪表盘


日志易 rizhiyi.com
仪表盘
搜索
告警
任务
应用
设置
yottabyte
帮助
反馈
状态概览
认证审计
漏洞检测
性能指标
安全管理
拒绝访问计数趋势图
3月4日 共425个事件, 每列15秒钟
50
25
0
3/4,22:49
22:51
22:52
22:53
22:54
访问失败时间段统计
100k
75k
50k
25k
0k
2016-1-20 00:00:00~2016-1-20 02:00:00
2016-1-20 04:00:00~2016-1-20 06:00:00
2016-1-20 08:00:00~2016-1-20 10:00:00
事件类型趋势
1,500
1,000
500
4:00 PM
8:00 PM
12:00 AM
4:00 AM
8:00 AM
access
audit
endpoint
identity
network
threat
拒绝访问端口排行汇总
allowed
blocked
0
200
400
600
800
1,000
1,200
1,400
1,600
OTHER
icmp://
tcp://2010
tcp://502
tcp://515
tcp://80
udp://123
udp://137
udp://161
udp://47808
udp://50
漏洞检测目的主机汇总排行
目的主机
漏洞概述
等级
计数
192.168.1.12
Google Chrome:CVE-2013-2566
High
238
192.168.0.231
MS13-080:Cumulative Security Update for Internet Explorer(2879017)
High
197
事件类型排行统计
other: 约8.47 %
d.u.rizhiyi.com/sources/input/ssa/: 约0.85 %
yi.com/sources/input/example/: 约0.85 %
zhiyi.com/sources/input/ssa/: 约0.85 %
01.u.rizhiyi.com/dashboard/: 约1.27 %
m/sources/input/example/: 约1.69 %
hiyi.com/sources/input/os/: 约8.90 %
https://jmcg.u.rizhiyi.com/sources/input

应用监控仪表盘


日志易 rizhiyi.com
仪表盘
搜索
告警
任务
应用
设置
yottabyte
帮助
反馈
状态概览
主从同步
慢查询统计
安全管理
慢查询访问来源IP排行
180.166.221.44: 约0.70 %
27.115.99.126: 约0.75 %
222.128.29.229: 约1.83 %
61.51.132.232: 约2.38 %
115.238.89.36: 约2.76 %
116.213.171.209: 约3.12 %
58.214.56.31: 约3.52 %
218.65.109.81: 约3.97 %
123.123.39.232: 约5.31 %
124.42.103.100: 约12.39 %
111.198.152.30: 约50.12 %
数据库主机排行
10-10-17-113
10-6-24-73
0
50
100
150
200
250
300
350
400
450
500
550
600
查询指令趋势图
0.15
0.1
0.05
0
-0.05
2/29,15:00
3/2
3/3
3/4
3/5
3/6
15:00
/api/v0/sources/upload_volum_info/
/saas_status_ucloud
/report
/
/api/v0/search/action/
SQL响应时间排行
SQL
平均响应时间
ALTER TABLE user ADD login_time DATE NOT NULL;
40.072
INSERT INTO post(username,title, body, pub_date) VALUES ('chenryn', 'Bug',
37.556
UPDATE post SET pub_date='2016-02-18' WHERE username='admin';
37.273
INSERT INTO post(username,title, body, pub_date) VALUES ('morushi', 'Blog',
36.433
INSERT INTO post(username,title, body, pub_date) VALUES ('schogen', '今天
35.893
慢查询数据库用户排行
https://zhang12.u.rizhiyi.com/app/apache/service/: 1.57 %
https://8868.u.rizhiyi.com/app/apache/service/: 1.57 %
https://1107.u.rizhiyi.com/sources/input/example/: 2.36 %
http://www.v2ex.com/t/261579: 2.36 %
http://rizhiyi.com/plus/mytag_js.php: 2.36 %
https://www.v2ex.com/t/261579: 3.94 %
https://www.rizhiyi.com
SQL计数排行
SQL
平均响应时间
SELECT * FROM comment WHERE author like '%raul%' AND pub_date>'2014
12
INSERT INTO post(username,title, body, pub_date) VALUES ('schogen', '今天
3
SELECT * FROM comment WHERE author like '%raul%' AND pub_date>'2014
25

网络设备部门仪表盘


日志易
nizhiyi.com
仪表盘
搜索
告警
任务
应用
设置
yottabyte
帮助
反馈
状态概览
网络状态
设备状态
安全管理
IP吞吐量趋势图
10,000
5,000
18:00
Thu Apr 3
2014
00:00
Fri Apr 4
06:00
12:00
端口吞吐量排行
1,500
1,000
500
18:00
Thu Apr 3
2014
00:00
Fri Apr 4
06:00
12:00
Syslog优先级计数排行
notification
warning
alert
error
critical
informational
0
25,000
50,000
75,000
100,000
125,000
150,000
175,000
200,000
Count of severity_id
端口状态变化统计
host
src_int
port_status
count
c2960-2etg-lan-8
GigabitEthernet1/0/8
up
36883
c3560-1
GigabitEthernet0/11
up
8786
3560-1etg-lan
GigabitEthernet0/20
up
6172
c3560-5etg-lan-7
GigabitEthernet0/1
down
1650
c2960-6etg-lan11
GigabitEthernet2/0/30
up
400
c2950-lan-10etg-34
FastEthernet0/20
up
256
c3560-1
GigabitEthernet0/5
down
240
四层协议吞吐量趋势图
字段值
数量
趋势
UDP
34882
TCP
31247
事件类型排行统计
234
交换机管理员账户登录计数
15
交换机配置变更计数

Gdevops

全球敏捷运维峰会

THANK YOU！