IT运维分析与日志搜索分析引擎案例分析

日志易CEO 陈军

提纲

- IT 运维分析（IT Operation Analytics）
- 不同数据源及解决方案对比
- 日志处理技术的演进
- 日志搜索分析引擎详解
- 日志搜索分析引擎案例

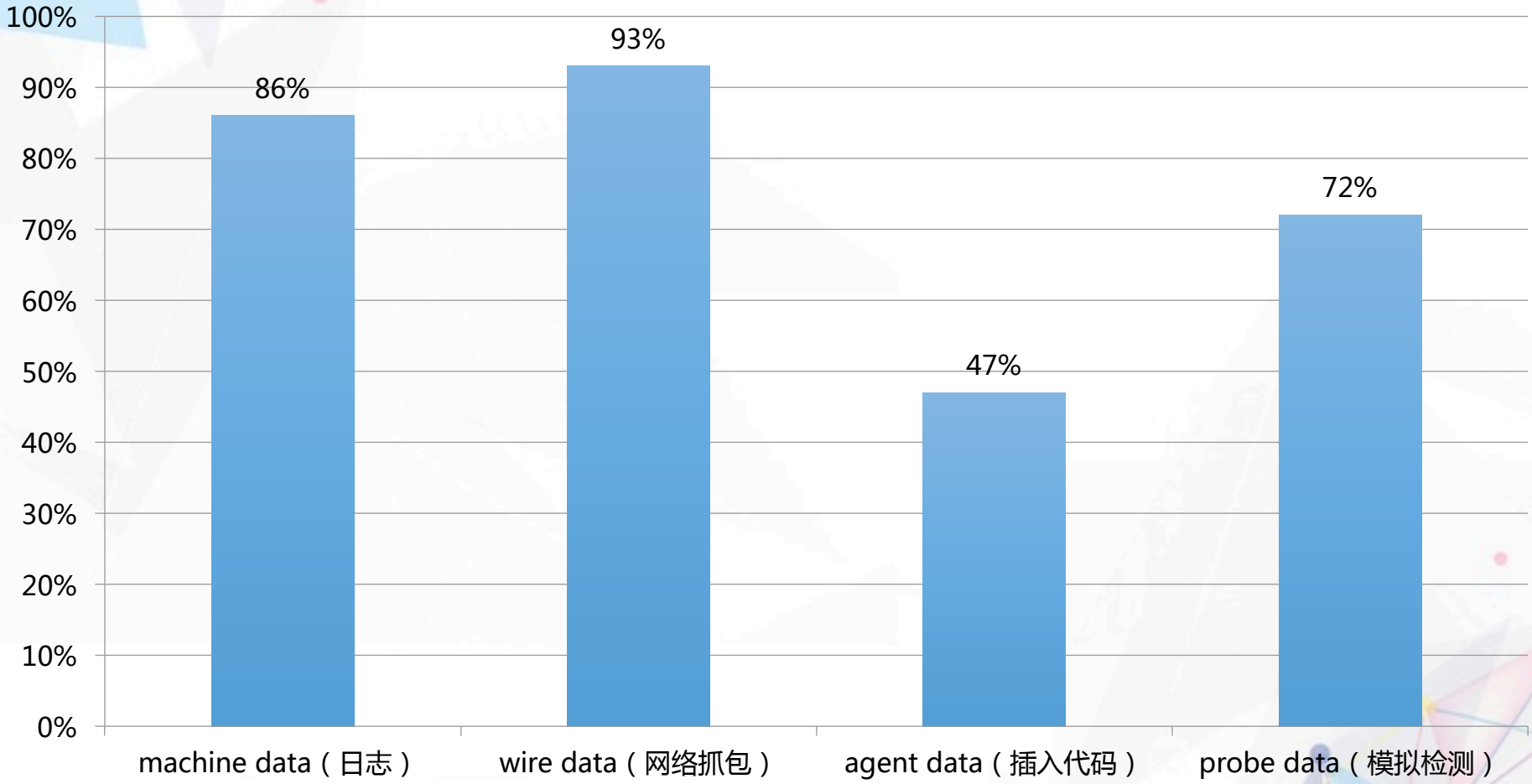
IT 运维分析

- 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
  - 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%

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/Ruby/Python/PHP 字节码里插入代码，统计函数调用、堆栈使用
- 探针数据（Probe Data）
  - 布点拨测
  - 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/解决方案比较

- 机器数据（日志）
  - 旁路
  - 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）
  - 旁路
  - 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）
  - 侵入式
  - 代码级精细监控
  - 对C/C++无效
  - 带来安全、稳定、性能问题
- 探针数据（布点拨测）
  - 旁路
  - 端到端监控
  - 只是模拟，不是真实用户度量（Real User Measurement，RUM）

ITOA 解决方案厂商（1）

- 机器数据（日志）
  - Splunk
  - ELK
  - 日志易
- 通信数据（网络抓包）
  - Netscout
  - 科来
  - 天旦
- 代理数据（嵌入代码）
  - New Relic
  - AppDynamics
  - DynaTrace (Compuware)
  - 云智慧
  - OneAPM

ITOA 解决方案厂商（2）

- 探针数据（布点拨测）
  - Gomez (Compuware)
  - Keynote
  - 听云（基调）
  - 博睿
- 大公司综合性产品
  - IBM
  - HP
  - Computer Associate
  - BMC
  - Riverbed

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
  - 深度解析LinkedIn大数据平台（http://www.csdn.net/article/2014-07-23/2820811/1）
  - “The Log: What every software engineer should know about real-time data's unifying abstraction”，Jay Kreps, LinkedIn engineer

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

日志的应用场景

- 运维监控
  - 可用性监控
  - 应用性能监控 (APM)
- 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)
- 用户及业务统计分析

过去：没有集中管理日志

- 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（grep/awk/regexp）
- 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
  - 没有事中监控、分析

过去：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

Timestamp	Hostname	Message
15/Apr/2015:00:27:19 +0800	180.150.189.243	“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

近年：大数据处理框架

- 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
  - 毫秒级延时
- Spark Streaming
  - 秒级延时
- Hadoop/Storm/SparkStreaming都只是一个开发框架，不是拿来即用的产品
- NoSQL
  - Mongodb
  - Redis
  - Druid
  - 不支持全文检索

现在

- 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

日志管理系统的进化

1 日志1.0：数据库

- 固定的schema无法适应任意日志格式
- 无法处理大数据量

2 日志2.0：Hadoop 或 NoSQL

- 需要开发成本
- 批处理，实时性差
- 不支持全文检索

3 日志3.0：实时搜索引擎

- 实时
- 灵活
- 全文检索

常用日志处理解决方案

- ELK
  - Elasticsearch/Logstash/Kibana
  - 基础功能开源免费
  - 告警、权限、管理模块收费
- Splunk
- 日志易

在线与离线日志处理结合

- 在线处理实时性好，但资源消耗大
- 离线处理资源消耗小，但实时性差
- 日志从消息系统出来，一路进在线系统，一路进离线系统
- 在线系统的索引文件备份到离线系统，检索时再从备份系统恢复

如果对几年的日志做统计分析

- 把定时生成的统计分析数据写入新的索引文件
- 长期的统计分析基于二次生成的索引文件，而不是原始数据

机器学习在日志分析的应用

- 异常自动检测
- 预测、容量规划

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
  - 入库速度慢
  - 占用硬盘空间大
  - 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
  - 检索速度慢
  - 入库速度快
  - 占用硬盘空间小
  - 灵活，检索时根据需要抽取字段

搜索处理语言

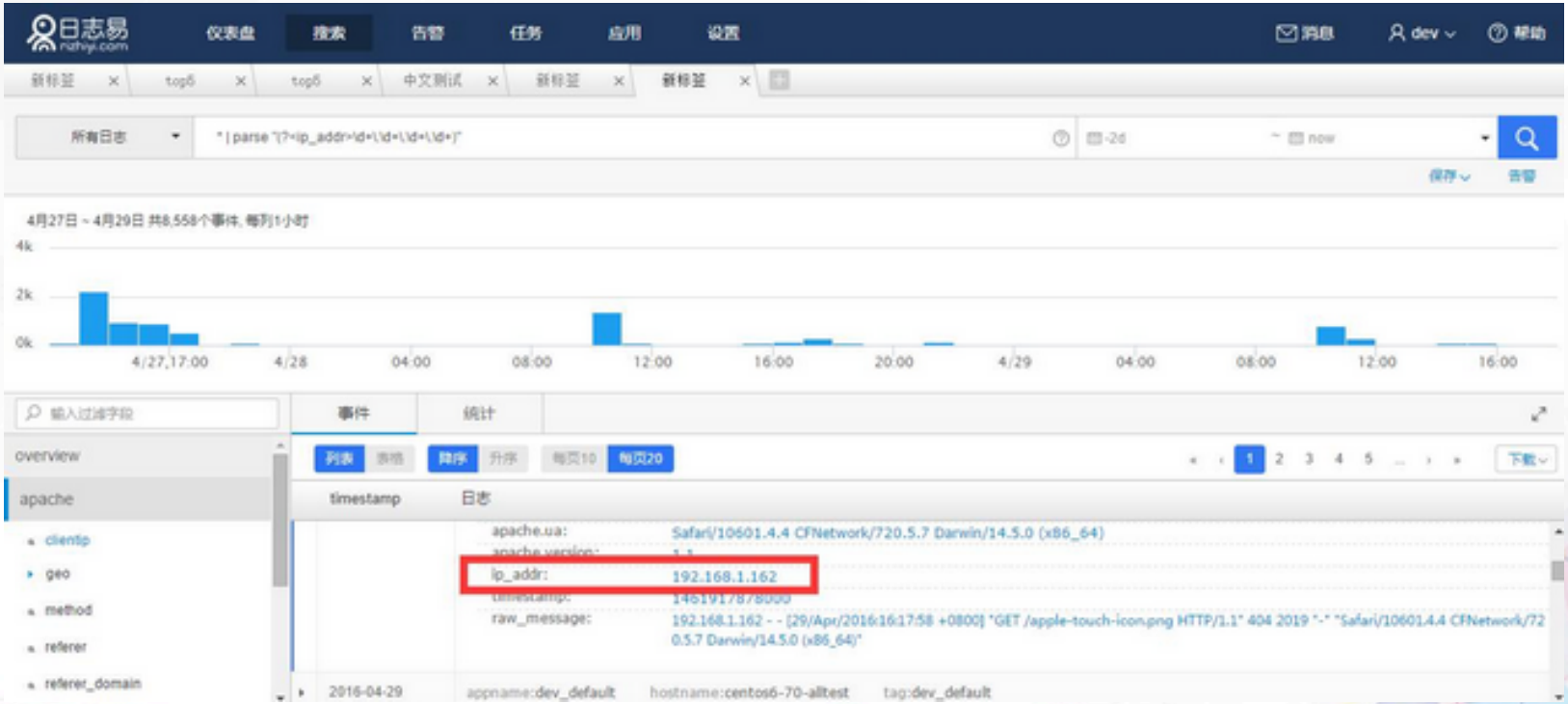
- SPL (Search Processing Language)
- 可编程的日志实时搜索分析平台
  - 灵活适应各种业务分析
  - 在搜索框里写 SPL 脚本，完成复杂的查询、分析
  - ”框计算“
- 用管道符（“|”）串接
  - 前命令的输出作为后命令的输入
- 用双方括号(“[[ ]]”）执行子命令
  - 子命令的结果作为父命令的输入

常见 SPL 命令

命令	描述
eval	对日志字段或统计结果进行计算表达式，并将表达式值放入新增字段中
bucket	将连续的值分别放入按区间分割的桶中，用于计算趋势以及数组分组变化
fields	保留结果中的字段
join	类似sql的连接，将主管道的结果和子管道的结果连接在一起
limit	返回前n个结果，常用于限制统计结果数量
movingavg	计算列值之间移动平均值
rollingstd	计算列值之间的标准差
rename	重命名字段名
stats	提供各种统计函数，并可以选择按字段分组统计
sort	安装指定的字段对结果进行排序
where	使用表达式对结果进行过滤
save	将搜索结果保存为外部csv文件
transaction	将结果分组形成交易日志组合
top	对字段进行数量和百分比统计

Schema on Read 案例

- 从日志的原文中抽取 ip_addr 字段
- * | parse “(?<ip_addr>\d+\.\d+\.\d+\.\d+)”



SPL 关联分析案例：transaction

json.url:“/charge/business.action?BMEBusiness=charge.charge&_cntRecTimeFlag=true” | transaction apache.dimensions.cookie_CURRENT_MENUID startswith=eval(json.action:“查询” && timestamp<30m) endswith=json.action:"提交"

1.先通过url过滤出所有缴费业务日志

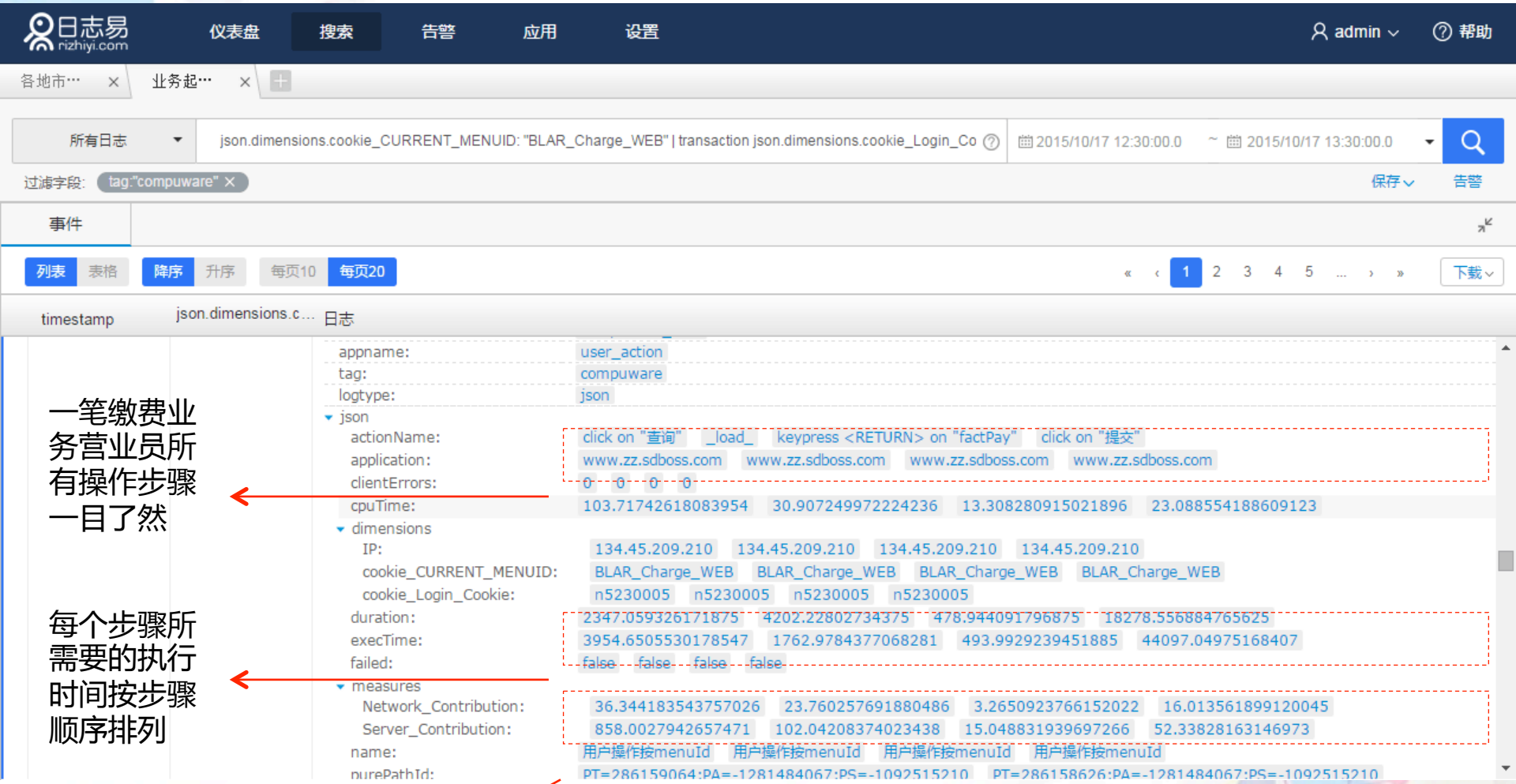
5.将“提交”动作作为步骤结束

2.通过menuid进行分组聚合

3.将“查询”动作作为步骤起点

4.默认30分钟内营业员处理完一笔完整业务

SPL 关联分析结果展示



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

SPL 关联分析案例：字典 Lookup

- 不同子系统的 ID 不同，如何关联？
- 通过字典把子系统1的 ID1 映射到子系统2的 ID2，从而把这两个不同ID的日志进行关联

SPL统计案例 - stats

logtype:apache | stats count(appname) as event_time,sum(apache.resp_len) as sum_len,max(apache.resp_len) as max_len,min(apache.resp_len) as min_len by apache.clientip | sort by sum_len | limit 5

apache.clientip	event_time	sum_len	max_len	min_len
119.145.41.230	123	1531881	1003110	0
218.81.139.51	39	302884	53353	53
113.66.199.117	36	21338	5211	46
119.129.209.5	173	17300	100	100
108.161.241.26	1	3222	3222	3222

logtype:apache | stats count(appname) as event_time,sum(apache.resp_len) as sum_len,max(apache.resp_len) as max_len,min(apache.resp_len) as min_len by apache.clientip|sort by sum_len | limit 5 | eval agv_len=if(event_time==0,0,sum_len/event_time)

apache.clientip	event_time	sum_len	max_len	min_len	agv_len
123.125.71.36	1	29816	29816	29816	29816
119.129.209.5	178	17800	100	100	0.5617977528089888
113.66.199.117	12	16617	4662	46	388.5
139.217.26.103	59	2183	37	37	0.6271186440677966
191.36.128.18	1	612	612	612	612

SPL 类数据库分析案例 - join（1）

场景：按照运营商isp，统计总数，status:400-499的数量及占比，status:500-599的数量及占比，请求长度大于1000的数量及占比，形成一张统计报表

（1）按照运营商isp，统计总数

logtype:"apache" | stats count(logtype) as count_all by apache.geo.isp | sort by count_all | limit 5

apache.geo.isp	count_all
中国电信	56021
中国联通	15860
未知	5832
microsoft-apnic-365-as microsoft global enterprise services ap,sg	2709
中国移动	1909

SPL 类数据库分析案例 - join（2）

场景：按照运营商isp，统计总数，status:400-499的数量及占比，status:500-599的数量及占比，请求长度大于1000的数量及占比，形成一张统计报表

（2）status:400-499的数量

logtype:"apache" AND apache.status:[400 TO 499] | stats count(logtype) as count_400 by apache.geo.isp

apache.geo.isp	count_400
中国电信	499
未知	90
中国联通	51
microsoft-corp-msn-as-block - microsoft corporation,us	17
hetzner-as hetzner online ag,de	12
中国移动	11
leaseweb-us - leaseweb usa, inc.,us	10
wii-kc - wholesale internet, inc.,us	8
yandex yandex llc,ru	7
advancedhosters-as advancedhosters limited,ua	6

SPL类数据库分析案例 - join（3）

场景：按照运营商isp，统计总数，status:400-499的数量及占比，status:500-599的数量及占比，请求长度大于1000的数量及占比，形成一张统计报表

（3）status:500-599的数量

logtype:"apache" AND apache.status:[500 TO 599] | stats count(logtype) as count_500 by apache.geo.isp

apache.geo.isp	count_500
中国电信	83
中国联通	46
未知	5
中国移动	3
长宽	1
阿里巴巴	1

SPL 类数据库分析案例 - join（4）

场景：按照运营商isp，统计总数，status:400-499的数量及占比，status:500-599的数量及占比，请求长度大于1000的数量及占比，形成一张统计报表

（4）请求长度大于1000的数量

logtype:“apache” AND apache.resp_len:>1000 | stats count(logtype) as len_1000 by apache.geo.isp

apache.geo.isp	len_1000
中国电信	14126
中国联通	5783
未知	1432
中国移动	1409
长宽	757
阿里巴巴	237
中国科技网	136
263网络	128
中国铁通	83
microsoft-corp-msn-as-block - microsoft corporation,us	71

SPL 类数据库分析案例 - join（5）

场景：按照运营商isp，统计总数，status:400-499的数量及占比，status:500-599的数量及占比，请求长度大于1000的数量及占比，形成一张统计报表

（5）join

```
logtype:"apache"|stats count(logtype) as count_all by apache.geo.isp|sort by count_all|limit 5|join type=left apache.geo.isp[[logtype:"apache" AND apache.status:[400 TO 499]|stats count(logtype) as count_400 by apache.geo.isp]]|join type=left apache.geo.isp [[logtype:"apache" AND apache.status:[500 TO 599]|stats count(logtype) as count_500 by apache.geo.isp]]|join type=left apache.geo.isp [[logtype:"apache" AND apache.resp_len:>1000|stats count(logtype) as len_1000 by apache.geo.isp]]
```

apache.geo.isp	count_all	count_400	count_500	len_1000
中国电信	55993	494	83	14098
中国联通	15862	51	46	5783
未知	5830	90	5	1432
microsoft-apnic-365-as microsoft global enterprise services ap,sg	2758	1		36
中国移动	1909	11	3	1409

SPL 类数据库分析案例 - join（6）

场景：按照运营商isp，统计总数，status:400-499的数量及占比，status:500-599的数量及占比，请求长度大于1000的数量及占比，形成一张统计报表

（6）统计占比，eval

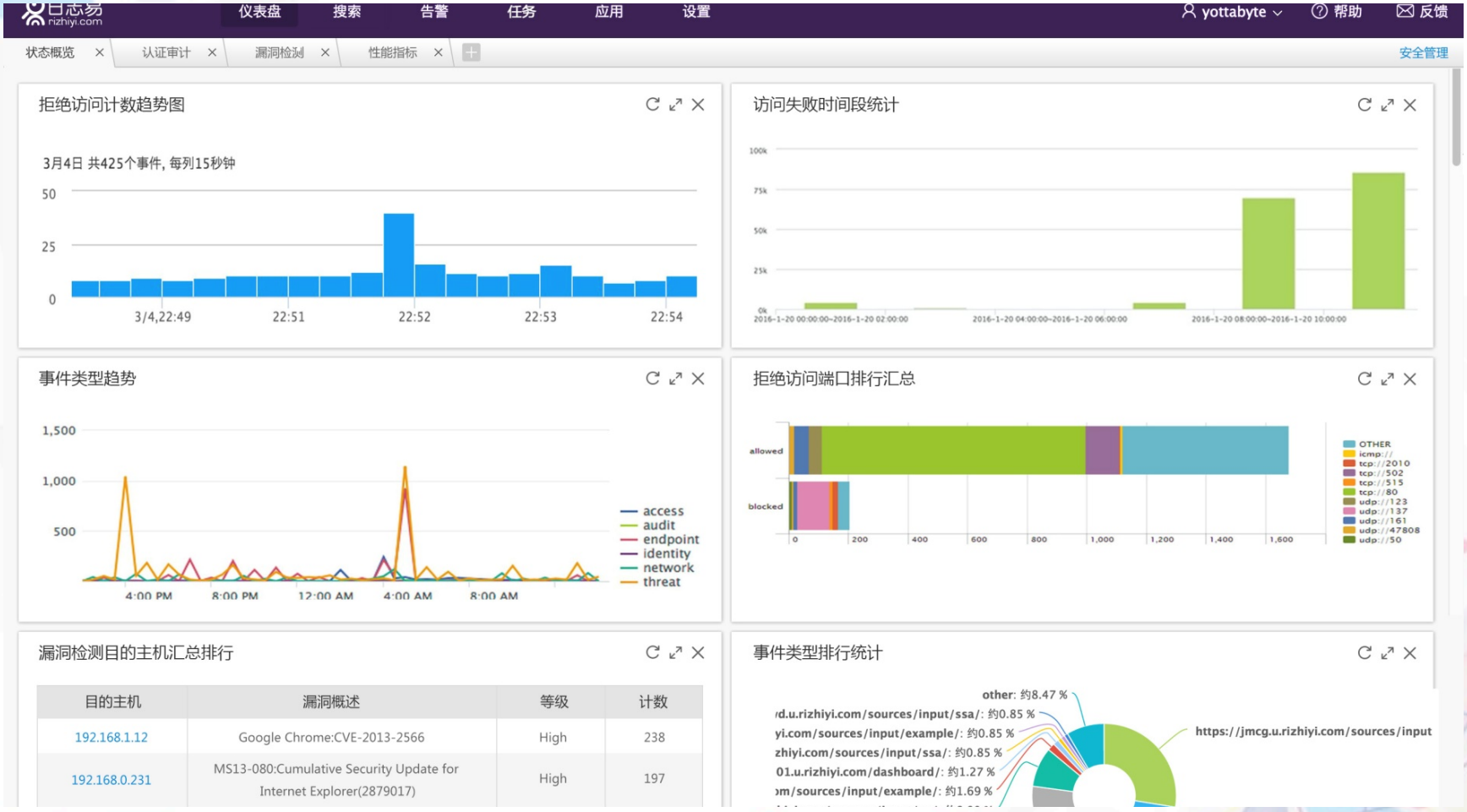
```
logtype:"apache"|stats count(logtype) as count_all by apache.geo.isp|sort by count_all|limit 5|join type=left apache.geo.isp[[logtype:"apache" AND apache.status:[400 TO 499]|stats count(logtype) as count_400 by apache.geo.isp]]|join type=left apache.geo.isp [[logtype:"apache" AND apache.status:[500 TO 599]|stats count(logtype) as count_500 by apache.geo.isp]]|join type=left apache.geo.isp [[logtype:"apache" AND apache.resp_len:>1000|stats count(logtype) as len_1000 by apache.geo.isp]]|eval rate_400=if(empty(count_400),0,count_400/count_all)|eval rate_500=if(empty(count_500),0,count_500/count_all)|eval rate_len_1000=if(empty(len_1000),0,len_1000/count_all)
```

apache.geo.isp	count_all	count_400	count_500	len_1000	rate_400	rate_500	rate_len_1000
中国电信	55995	494	83	14098	0.00882221626930976	0.0014822752031431379	0.2517724796856862
中国联通	15859	51	46	5783	0.003215839586354751	0.002900561195535658	0.36465098682136327
未知	5830	90	5	1432	0.015437392795883362	0.0008576329331046312	0.24562607204116638
microsoft-apnic-365-as microsoft global enterprise services ap,sg	2774	1		36	0.0003604902667627974		0.012977649603460706
中国移动	1909	11	3	1409	0.005762179151388162	0.001571503404924044	0.7380827658459926

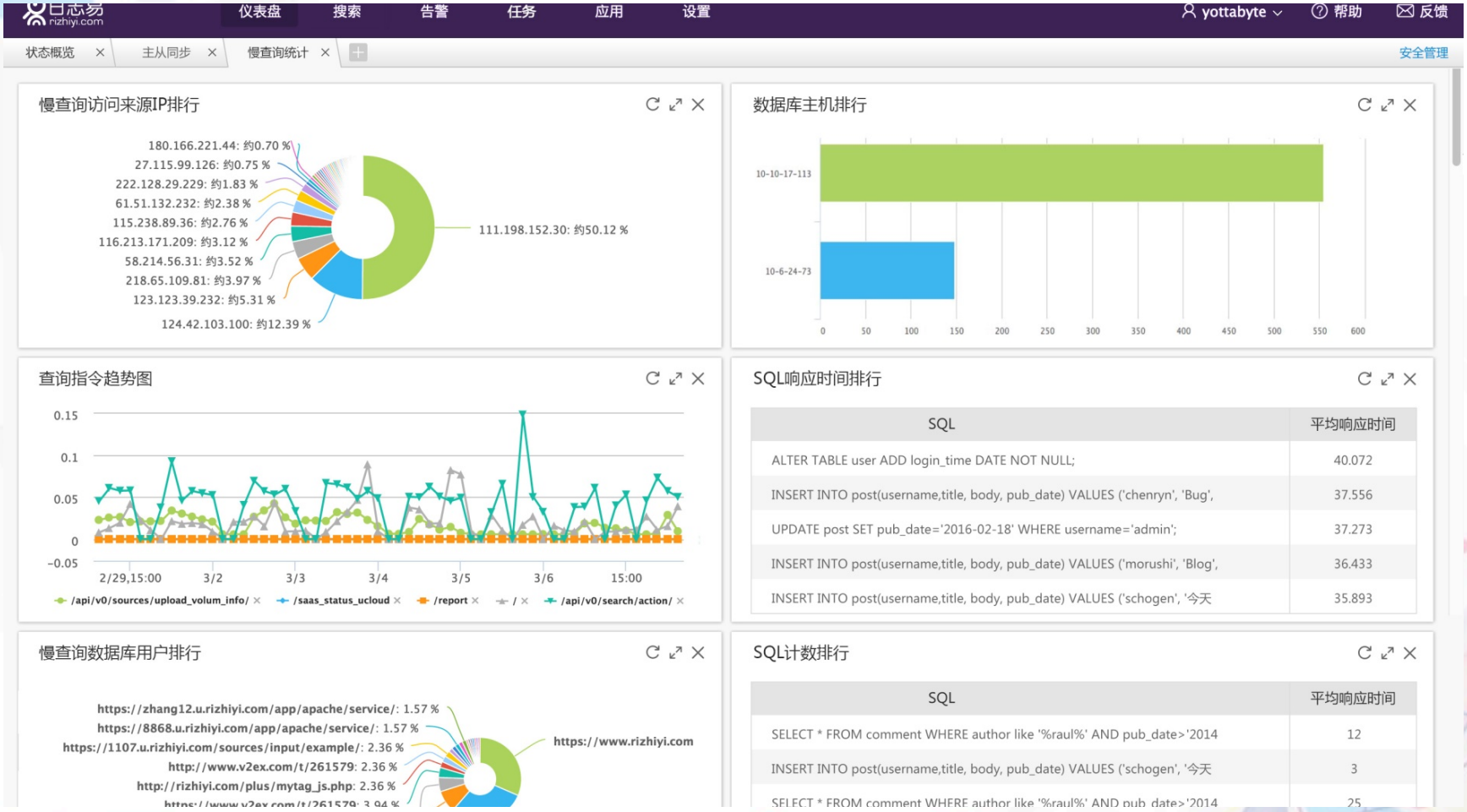
三个解决方案的比较

	Schema on Write	Schema on Read	SPL
Splunk	✔	✔	✔
日志易	✔	✔	✔
ELK	✔		

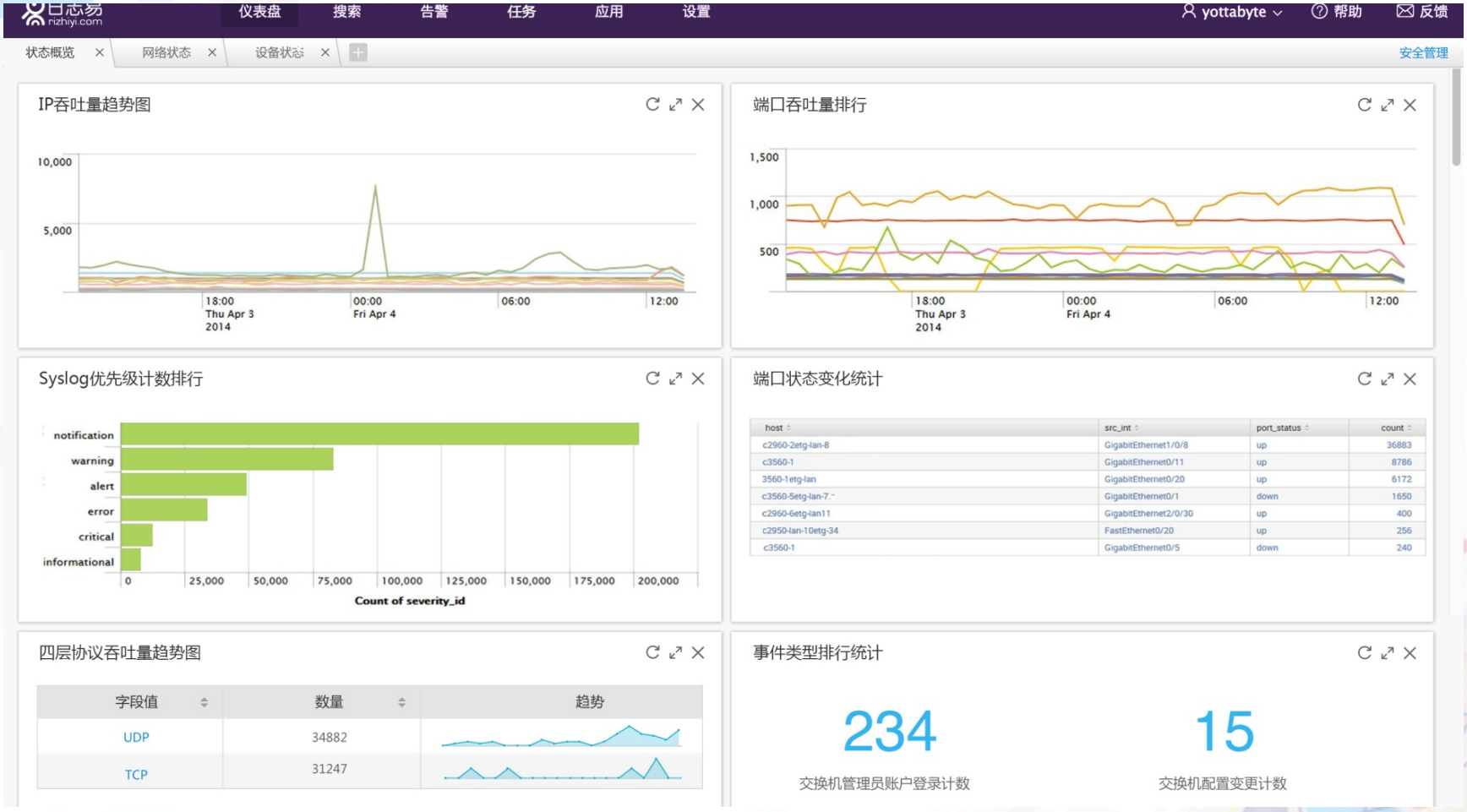
日志易-网络安全部门仪表盘



日志易-应用监控仪表盘



日志易-网络设备部门仪表盘



THANKS

SequeMedia 盛拓传媒 | IT168.com 专注导购16年 | ChinaUnix.net | ITPUB www.itpub.net