DBAplus

金融行业运维实践沙龙-上海站

# 平安集团 旁路运营监察系统

CTO办公室 王权

# 旁路监控系统介绍

# 2017年

王权

2017年6月

# 目前运维监控的困境

1. 运维与开发分属不同部门，监控方面的需求运维很重视，但开发无暇顾及；
2. 系统与系统、组件与组件耦合关系梳理不清楚，不知道你不知道时常发生；
3. 随着监控指标增多，监控平台延迟越来越大；
4. 缺少预警功能；
5. 较难做到端到端的监控；
6. 虚拟机、容器越来越多，agent负载越来越大，且效果不好；
7. 基础层面监控较难关联到业务层面的监控；
8. 运维就是纯技术，但是老板希望看到实时报表，或者大促时候的实时交易数据；
9. 传统监控与安全关系不大。

# 现状

- ✓ 埋点，例如：Metrics+influxdb+grafana
- ✓ Agent，例如：Zabbix
- ✓ 现有日志，例如：Syslog、ELK
- ✓ 数据库采集

# 比较

旁路监控系统与现有监控系统在异常发现及告警时效方面和业务（交易）监控范围方面等互补。旁路监控系统通过网络监听方式，构成第一道为提高运营稳定性的快速预警线。

| 对比项 | 非旁路 | 旁路 |
| --- | --- | --- |
| 实施周期 | 较长 | 较短 |
| 服务路径发现 | 较难 | 较易 |
| 实时性 | 依赖日志采样频率（最小一分钟间隔） | 准实时（秒级延迟） |
| 单笔交易追踪 | 尚未实现（较难） | 已实现（标准功能） |
| 部署 | 需要远程登录每一台主机部署日志采集客户端 | 不需要接触主机 |
| 生产系统性能影响 | 日志采集客户端会使用一部分主机资源（cpu，内存，网络带宽） | 不占用任何生产环节资源 |
| 安全 | 需要访问主机，有一定安全隐患 | 不需访问生产环境 |
| 现有系统日志质量及采样颗粒度 | 完全依赖 | 完全不依赖 |
| 主机状况监控(cpu, mem等) | 有 | 无(不接触主机) |
| 应用排障 | 直接使用收集的日志 | 另行获取日志 |

# 需求

✓数量：集团下面全部30+家专业公司，如银行、证券、信托、陆金所、汽车之家等等；

✓流量：互联网C端入口流量　N*100Tb/s；

✓数据量：N*100TB/天；

✓指标：x十万个；

✓告警延迟：10秒内；

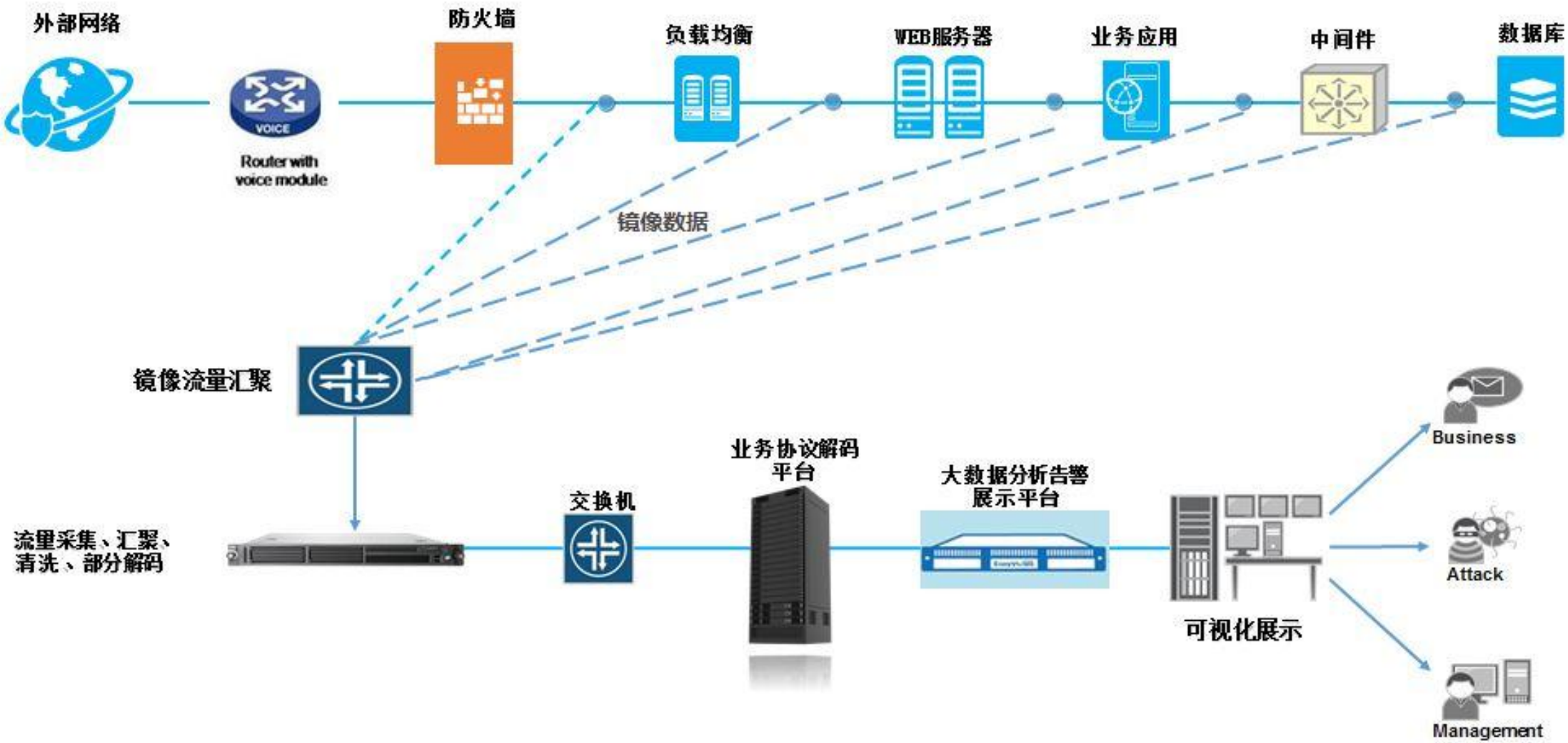
✓展示延迟：30秒内；

✓预警提前：1周；

✓颗粒度：每一个业务，每一个维度，每一个产品，例如陆金所基金3000+支基金，监控每一支交易趋势；

✓深圳监察室，集中展示与告警。

# 旁路方案


外部网络
防火墙
负载均衡
WEB服务器
业务应用
中间件
数据库
VOICE
Router with
voice module
镜像数据
镜像流量汇聚
流量采集、汇聚、
清洗、部分解码
交换机
业务协议解码
平台
大数据分析告警
展示平台
可视化展示
Business
Attack
Management

## 监控目标指标

# 主机可用性

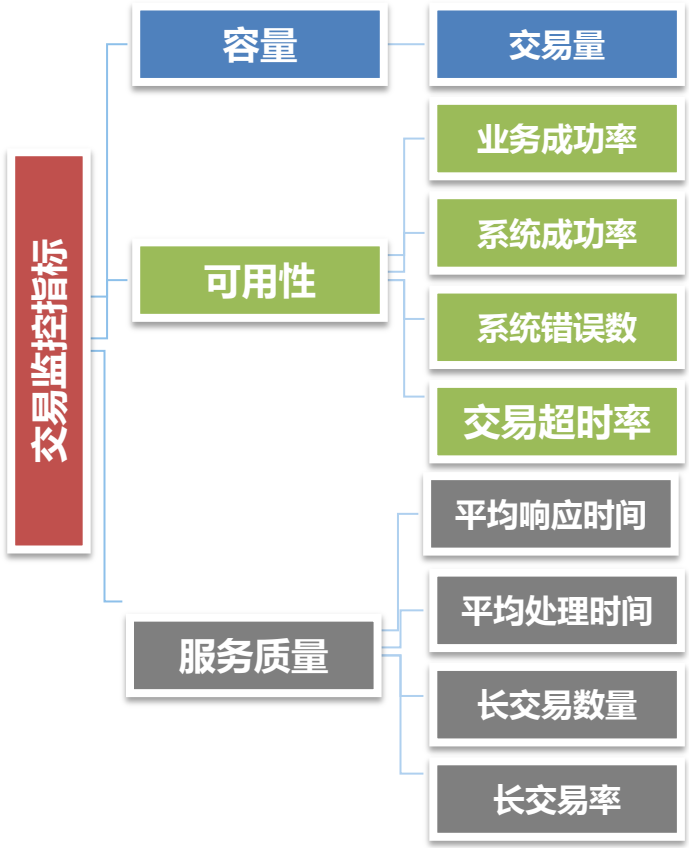
# 交易可用性

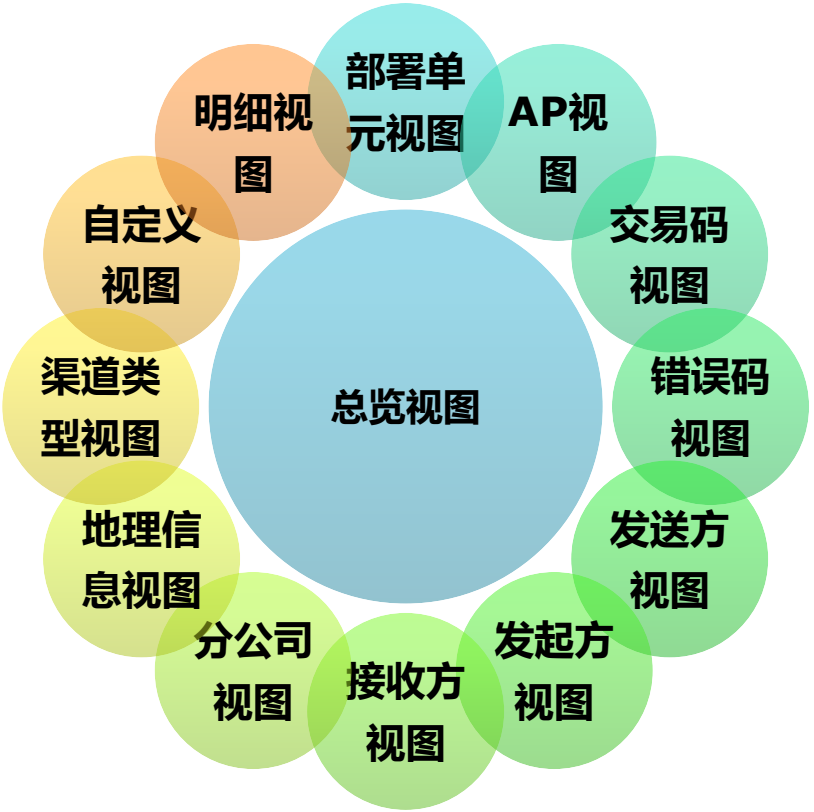
# 数据库可用性

# 网络可用性

# 应用可用性

# 安全可用性



## 流量采集

- ✓ 商业的有tap例如gigamon；
- ✓ 开源的为Pf_ring，High-speed packet capture, filtering and analysis.
- ✓ 实现数据采集和解析一体化，同时完成流量采集，数据包解析和清洗。
- ✓ 使用旁路模式进行部署。通过镜像流量来捕获数据，不影响现有应用系统和网络，为纯软件解决方案，直接部署在通用服务器上即可实现实时采集和解析数据。
- ✓ 大吞吐量和高可用，最高可支持每秒40Gb数据的采集。
- ✓ 安全可靠。旁路接收口位于防火墙之后，仅用于数据采集，不配置IP，不会被外部攻击。
- ✓ 提供强大的分析清洗能力，访问及交易请求处理能力可达20000笔/s。

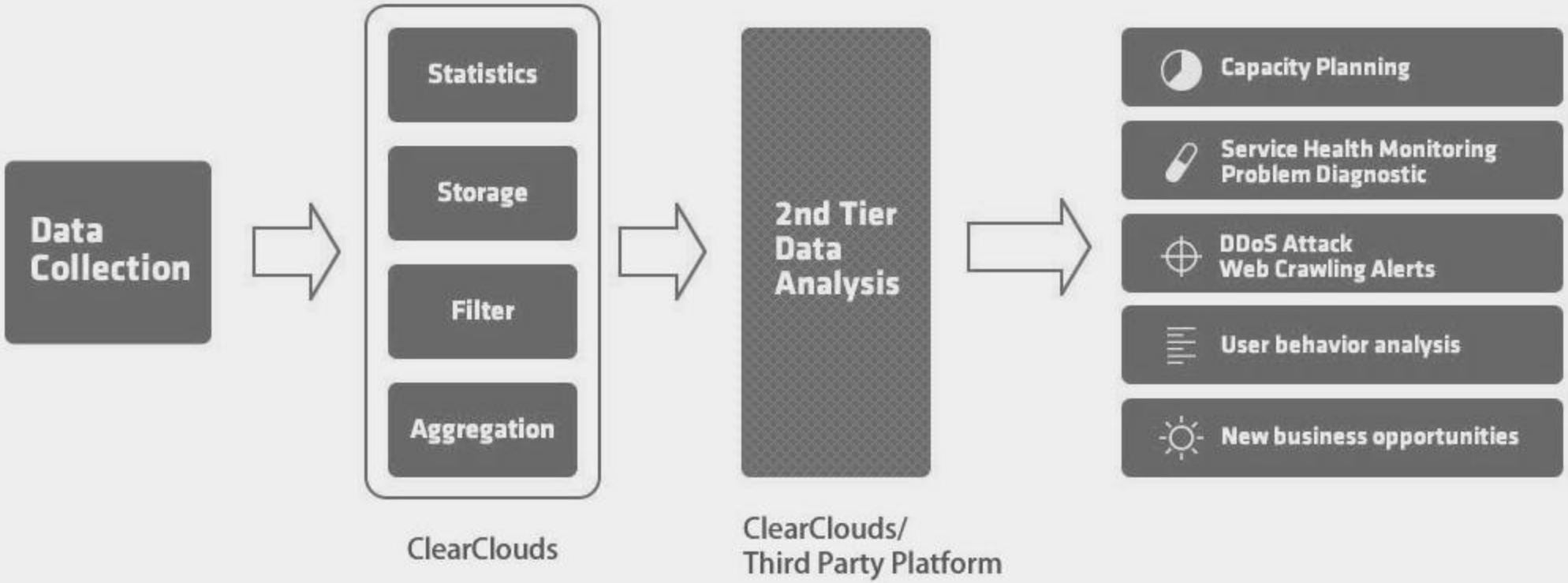
# 流量采集-TAP

✓ iTAP：


✓ Gigamon

# 流量采集-iTAP

With high speed, high bandwidth （20Gbps） traffic flow capture and analysis, ClearClouds can provide unprecedented insight into the traffic flow and intelligence at both application level (http) and TCP/IP level. This intelligence can be consumed by data centers and cloud operational team, system integrators, or solution providers (partners) to do various applications.




会单独打开一个附件，来详细说明！

## 处理与展示—解码

✓全量解码，例如天旦；

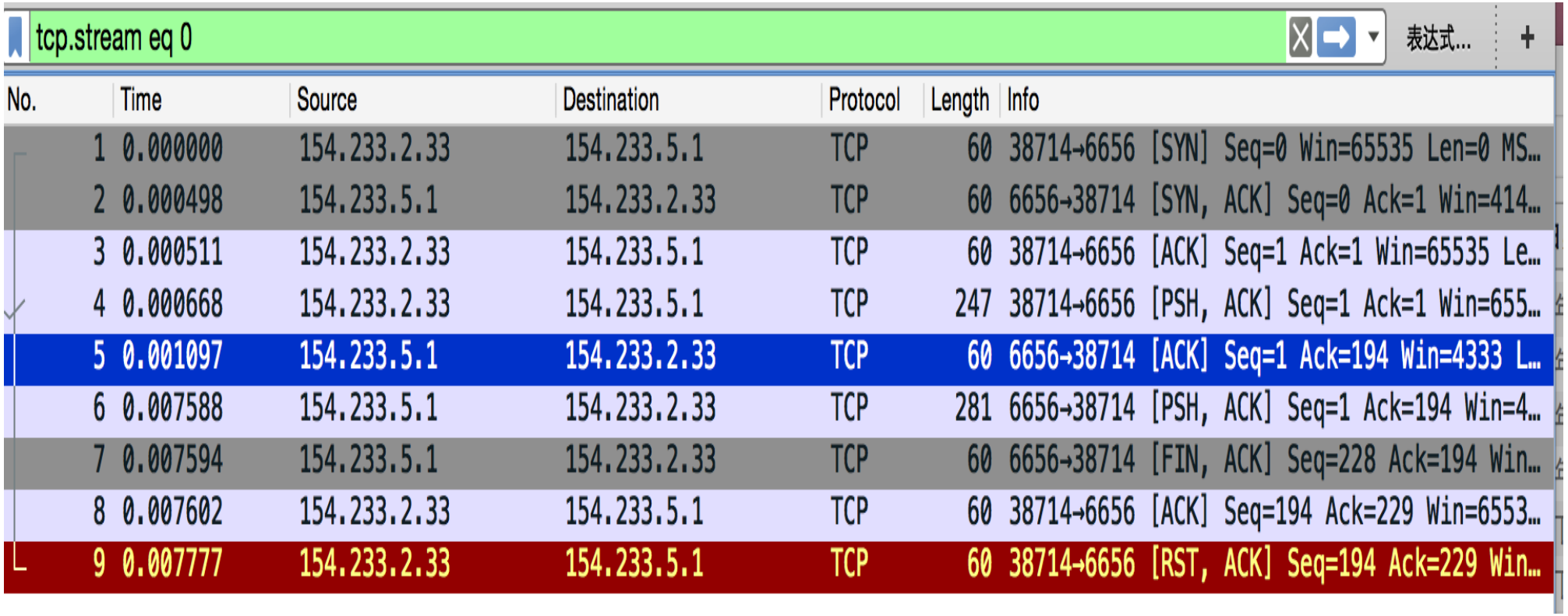
✓正则解码，例如华青；

✓iTAP解码。

会单独打开一个附件，来详细说明！

## 协议解码

- ✓ 拓扑发现
- ✓ 报文私有协议解析




| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000 | 154.233.2.33 | 154.233.5.1 | TCP | 60 | 38714→6656 [SYN] Seq=0 Win=65535 Len=0 MS… |
| 2 | 0.000498 | 154.233.5.1 | 154.233.2.33 | TCP | 60 | 6656→38714 [SYN, ACK] Seq=0 Ack=1 Win=414… |
| 3 | 0.000511 | 154.233.2.33 | 154.233.5.1 | TCP | 60 | 38714→6656 [ACK] Seq=1 Ack=1 Win=65535 Le… |
| 4 | 0.000668 | 154.233.2.33 | 154.233.5.1 | TCP | 247 | 38714→6656 [PSH, ACK] Seq=1 Ack=1 Win=655… |
| 5 | 0.001097 | 154.233.5.1 | 154.233.2.33 | TCP | 60 | 6656→38714 [ACK] Seq=1 Ack=194 Win=4333 L… |
| 6 | 0.007588 | 154.233.5.1 | 154.233.2.33 | TCP | 281 | 6656→38714 [PSH, ACK] Seq=1 Ack=194 Win=4… |
| 7 | 0.007594 | 154.233.5.1 | 154.233.2.33 | TCP | 60 | 6656→38714 [FIN, ACK] Seq=228 Ack=194 Win… |
| 8 | 0.007602 | 154.233.2.33 | 154.233.5.1 | TCP | 60 | 38714→6656 [ACK] Seq=194 Ack=229 Win=6553… |
| 9 | 0.007777 | 154.233.2.33 | 154.233.5.1 | TCP | 60 | 38714→6656 [RST, ACK] Seq=194 Ack=229 Win… |

## 数据分析

- ✓ Elasticsearch：
  - a) 至少1.7及以后，之前版本存在安全漏洞；
  - b) GC设置；
  - c) Index template设置；
  - d) 结合flume-collector或者kafka-批量压入方式，进行数据传输；

- ✓ SPARK+HADOOP：
  - a) 延迟；
  - b) 分片；
  - c) 结合kafka进行数据传输，partition设置；

- ✓ 最小二乘法等趋势预测方法

# 数据展示

✓自定义视图；

✓权限控制显示，尤其单值显示；

✓色彩对比度大；

✓灵活配置界面；

✓刷新频率与方式；

✓显示点、线、图；

✓如何一个产品显示3000多个指标；

✓轮播形式

✓包线、图表

✓同比、环比

✓排期设置

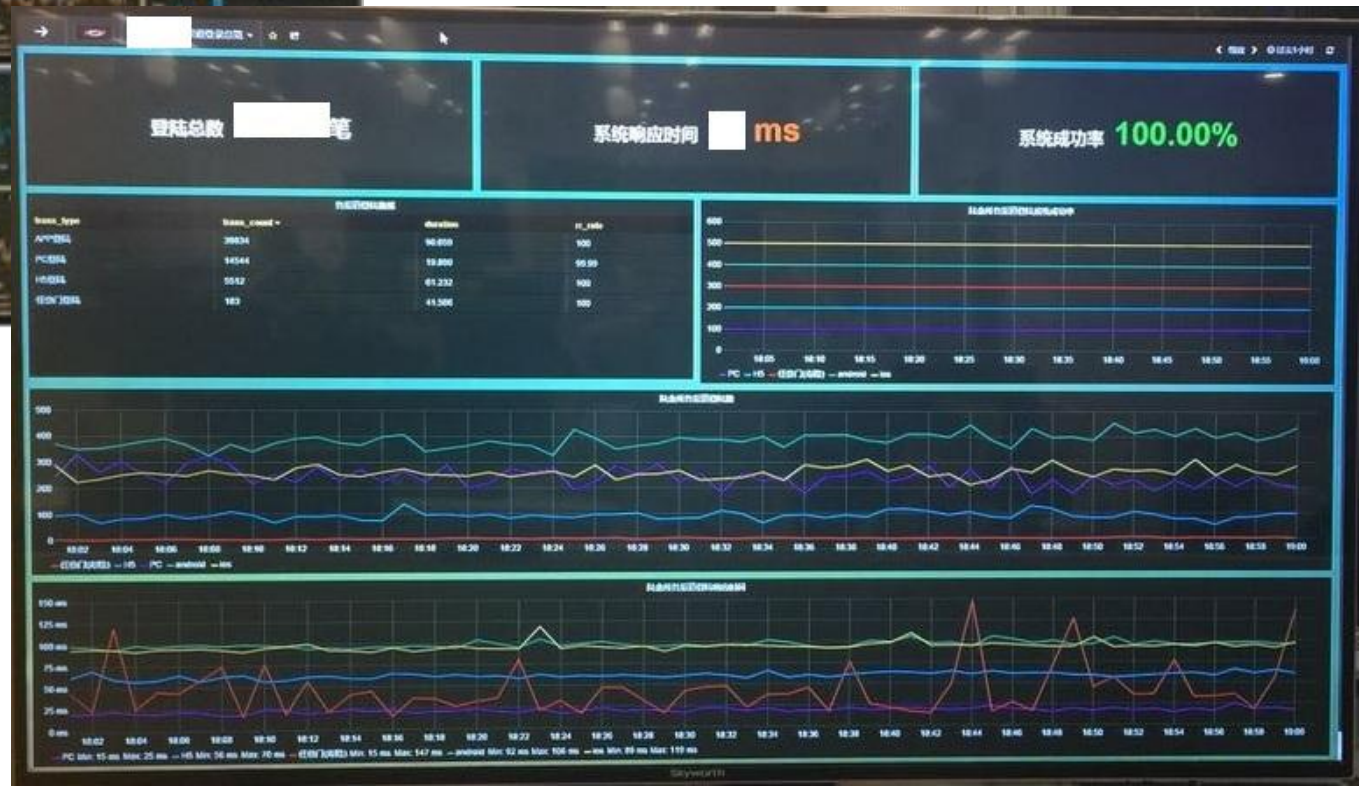
✓预警与告警

✓。。。。。

## 数据展示

- ✓ 数据分析平台特点
  - ➢ 支持EPL语言对事件进行复杂逻辑处理；
  - ➢ 灵活的数据处理：支持结构化、半结构化、非结构化等多种类型全文检索、分析和批处理；支持超高并发查询能力；
  - ➢ 支持监控大屏幕个性化配置功能，可根据不同监控、分析场景配置实现动态、实时的大屏幕监控视图。可提供业务地图、业务渠道、业务量同比环比变化、专业公司等不同维度业务指标的实时结果展示；
- ✓ 展示平台特点
  - ➢ 告警支持自定义过滤器（过滤器支持多条件的逻辑运算和搜索、数学计算）进行告警;
  - ➢ 支持对多个流的多个指标进行关联计算后的基线进行告警；
  - ➢ 仪表盘支持钻取，可以选取仪表盘某个时间点的监控指标，钻取到多维分析进行深入分析；

# 页面展示



# 分析与展示


DBAplus
www.dbaplus.cn
THANK YOU

限时优惠，扫码抢票


# APAC OTN TOUR 2017

The APAC OTN Tour 2017 will be running from November 20th until December 9th visiting 4 countries/7 Cities in the Asia Pacific Region. Bellow you can find more information regarding the events that are part of this year tour:

**Dates:**

- Wellington, NZ : November 20th
- Auckland, NZ : November 22nd
- Sydney, Australia: November 24th
- Melbourne, Australia: November 27th
- Perth, Australia: November 29th
- Shanghai, China: December 3rd
- Hyderabad, India: December 8 and 9

12月3日　D+ Day 欢迎来撩：
讲师、茶歇、场地、赞助，统统可以。

预计150人规模。
微信来撩：boypoo

限时优惠，扫码抢票


# APAC OTN TOUR 2017

The APAC OTN Tour 2017 will be running from November 20th until December 9th visiting 4 countries/7 Cities in the Asia Pacific Region. Bellow you can find more information regarding the events that are part of this year tour:

**Dates:**

- Wellington, NZ : November 20th
- Auckland, NZ : November 22nd
- Sydney, Australia: November 24th
- Melbourne, Australia: November 27th
- Perth, Australia: November 29th
- Shanghai, China: December 3rd
- Hyderabad, India: December 8 and 9

12月3日　D+ Day 欢迎来撩：
讲师、茶歇、场地、赞助，统统可以。

预计150人规模。
微信来撩：boypoo