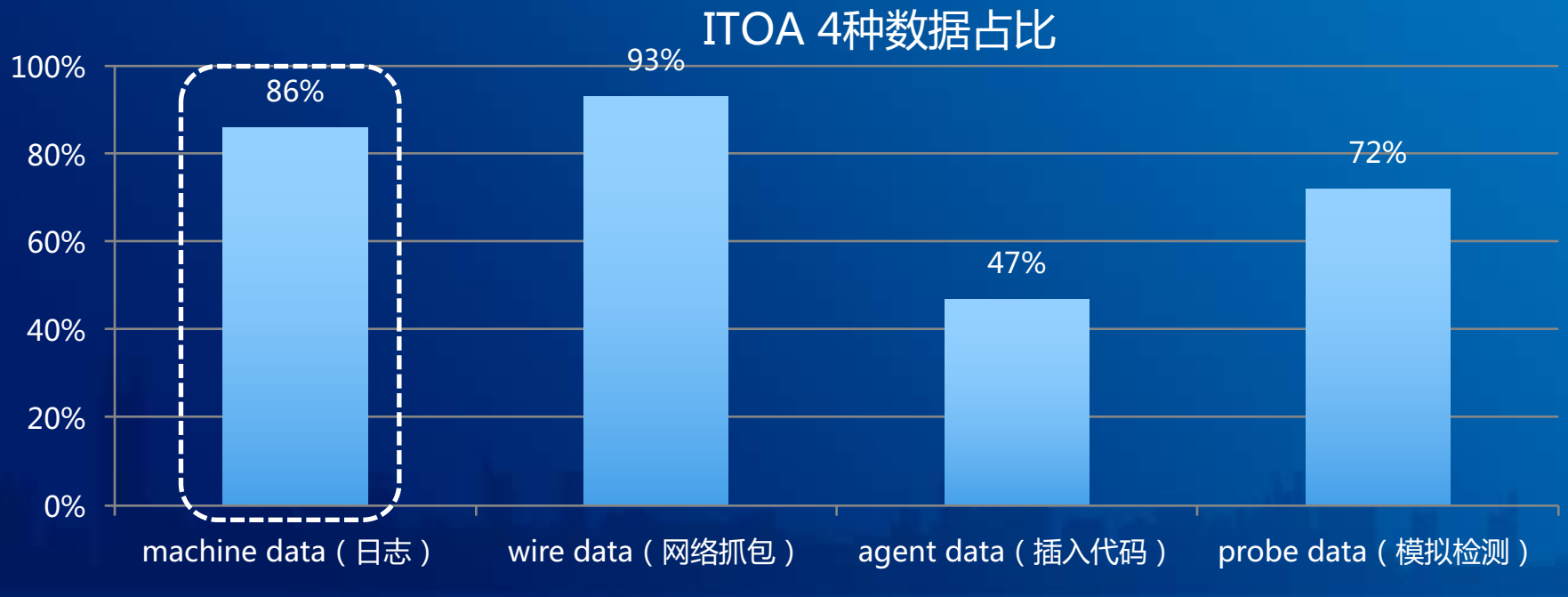
运维世界大会·深圳站

海量日志搜索分析技术及行业应用案例

日志易 黄俊毅

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
- 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 四种数据来源的比较

运维世界 Ops World

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）

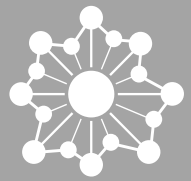
日志，我们重要的数据资产

clientIP　timestamp　method　uri

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; r:37.0) Gecko/20100101 Firefox/37.0” “10.10.33.174” 0.005

status　length　reference　span

安全审计



运维监控

回溯取证

业务分析

过去

存储日志性能方面

- 无法适应每天TB级海量日志
- 数据库的schema无法适应千变万化的日志格式
- 无法提供海量日志全文检索和字段统计功能

运维方面

- 需要登陆每一台服务器，使用脚本命令或程序查看，操作繁琐，容易出错
- 数据是孤立分散的，无法进行关联，无法提取出其中的共性
- 只能做简单搜索和统计，无法满足分析要求
- 没有实时监控和报警，如程序出错日志

安全方面

- 黑客入侵后往往会删除 / 修改日志，抹除入侵痕迹，导致无法通过日志分析攻击行为
- 海量的ids / waf报警，根本无法辨别是否是误报

近年

运维世界 Ops World

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 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

现在

运维世界 Ops World

Fast big data

非结构化

能处理所有机器数据，能适应各种日志格式，而无需对原有日志进行改造

大

每天处理 TB 级的日志量，数十TB的日志只需几秒就能搜索出结果

实时大数据

无缝横向扩展
丰富对外接口

快

日志从产生到搜索分析出结果只有几秒的延时

灵活

Google for IT，可搜索、分析任何日志

日志管理系统演进

运维世界 Ops World

01

日志1.0 数据库

- 固定的schema无法适任意日志格式
- 无法处理大数据量

02

日志2.0 Hadoop / Nosql

- 需要开发成本
- 批处理，实时性差
- 不支持全文检索

03

日志3.0 实时搜索分析

- 实时
- 灵活
- 全文检索

04

NG 日志

- 机器学习
- 人工智能

日志管理核心技术

运维世界 Ops World

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

日志管理核心技术

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

用一条SPL语法解决复杂的聚合逻辑，以缴费业务关联分析为例：

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

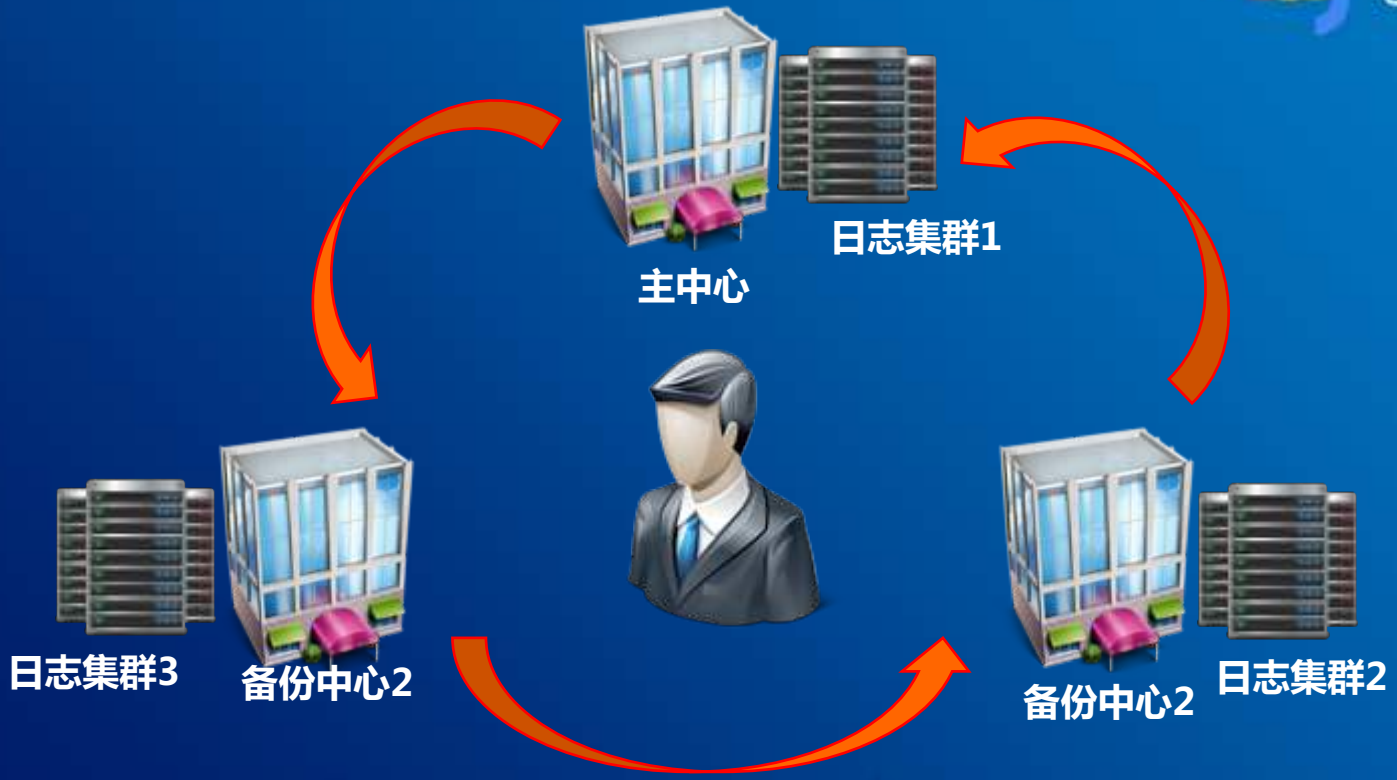
2.通过menuid进行分组聚合

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

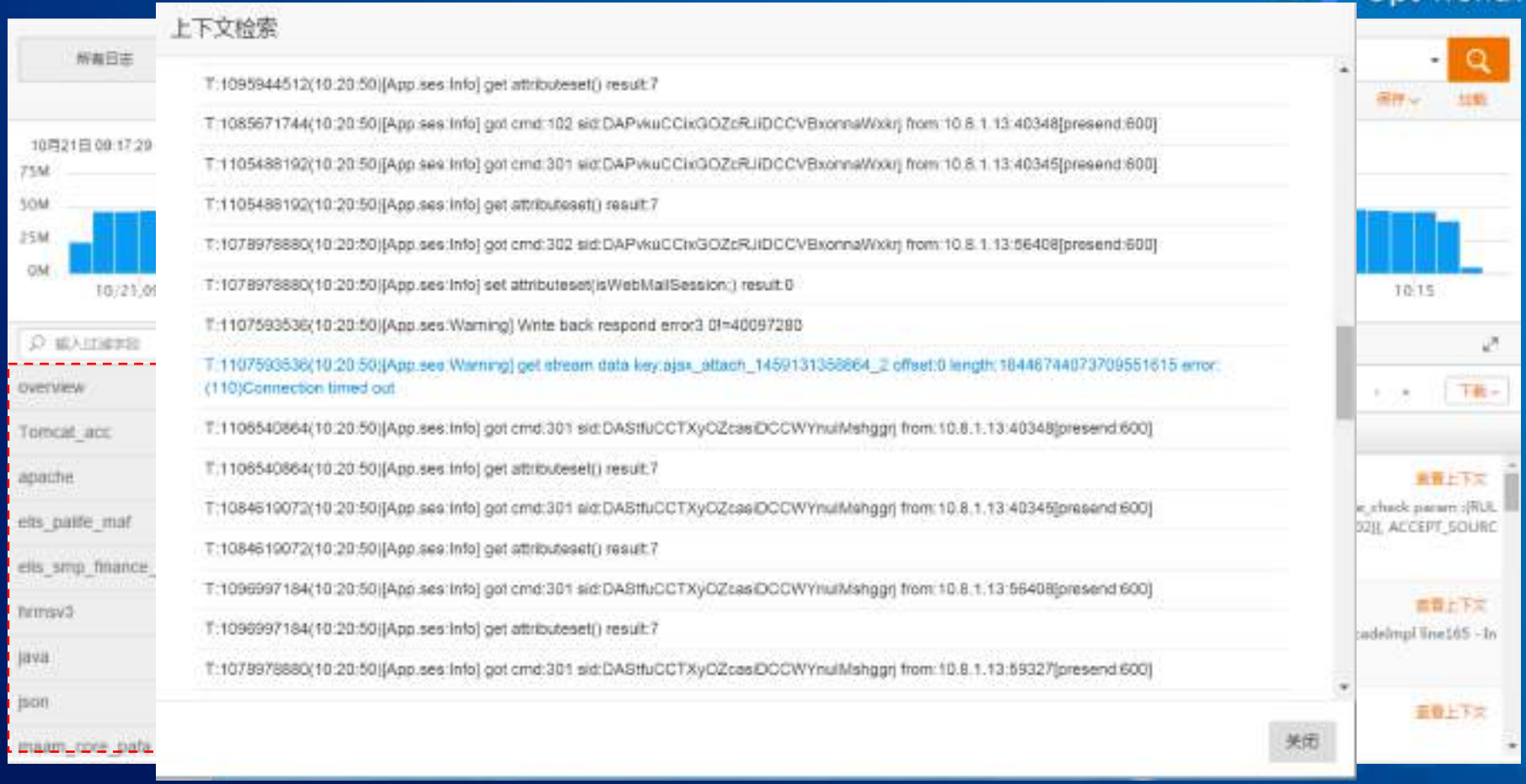
5.将“提交”动作作为步骤结束

日志应用场景 - 统一日志平台



多个IDC日志易集群之间用同一个帐号登录即可查询多个 IDC的数据

日志应用场景 - 统一日志平台



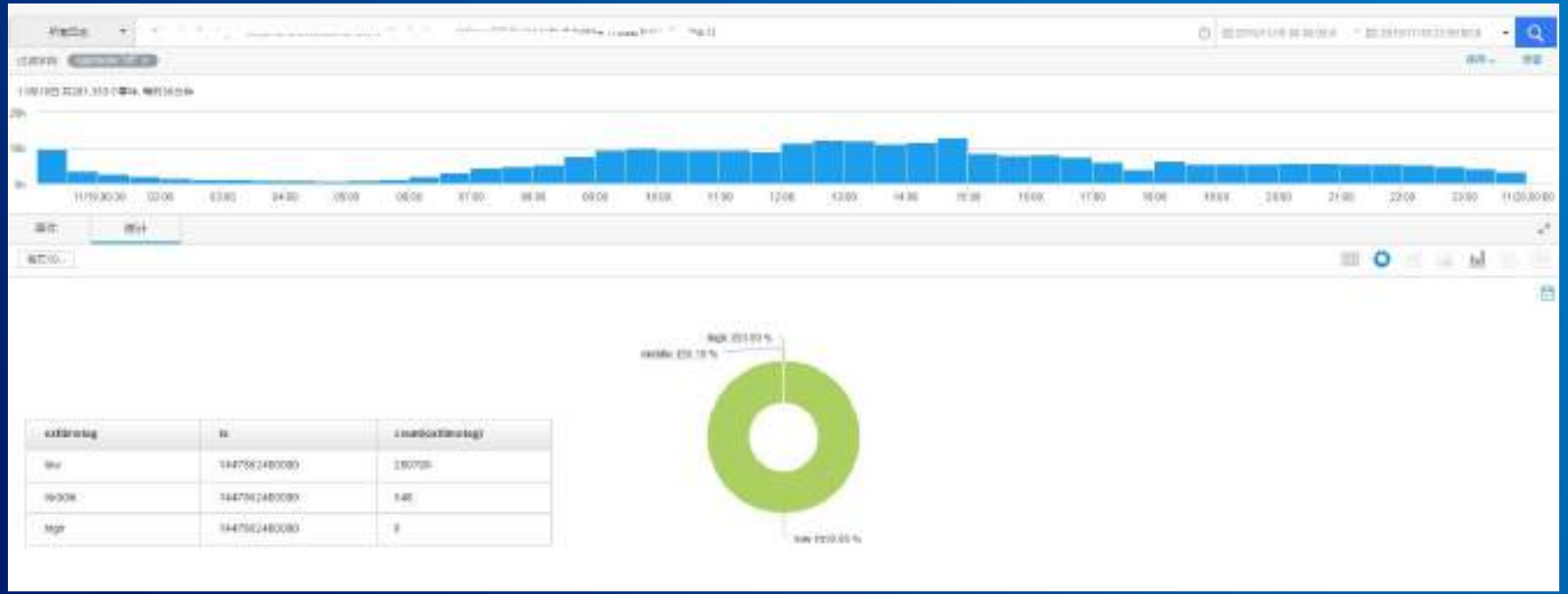
日志应用场景 - 业务运维分析

运维世界 Ops World

实时监控每一笔交易，对异常和错误实时告警

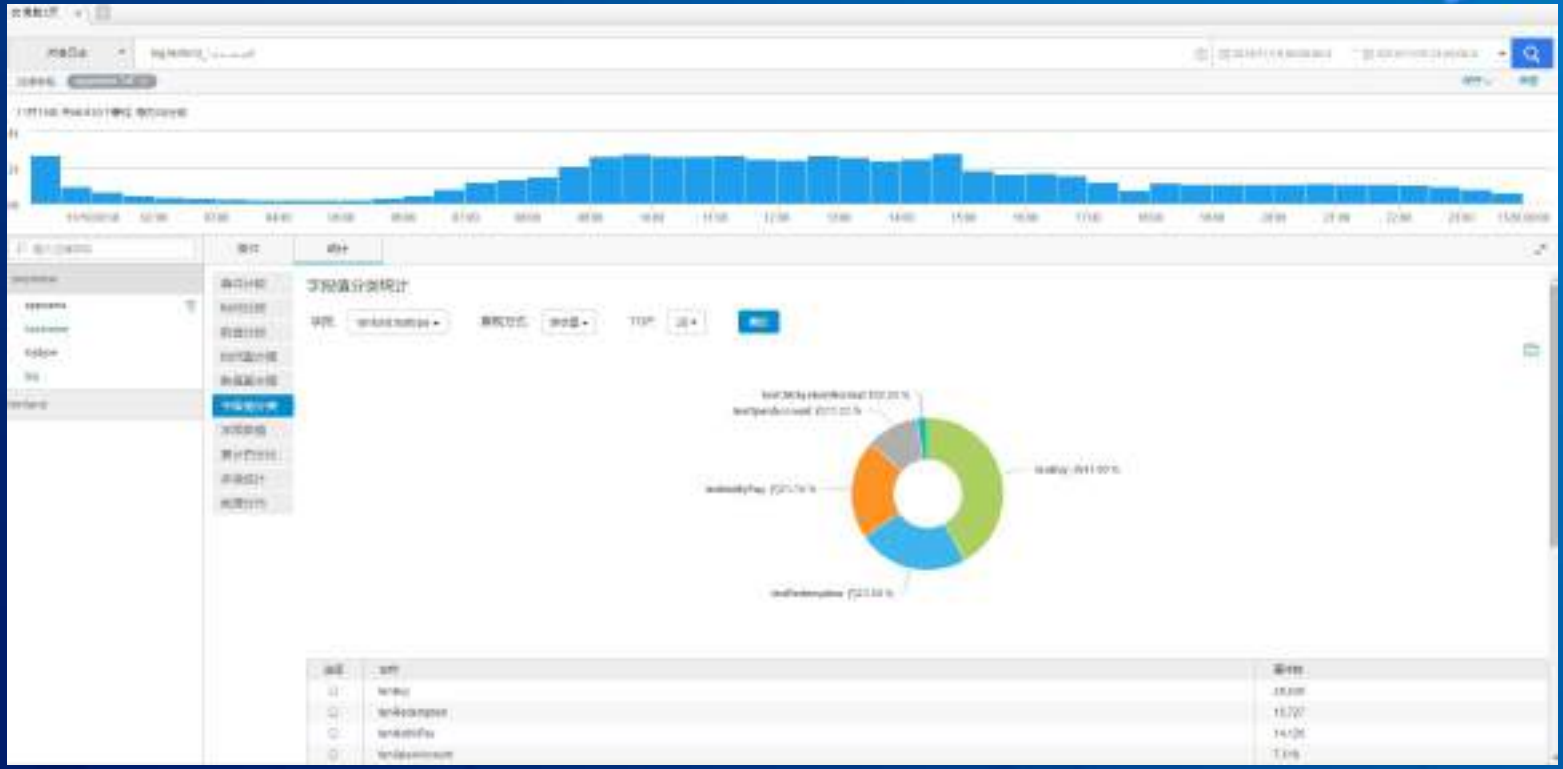
- 交易是否正常
- 交易耗时
- 交易的服务器资源消耗
- 接口、服务调用实时统计
- 交易量统计、分析

日志应用场景 - 业务运维分析



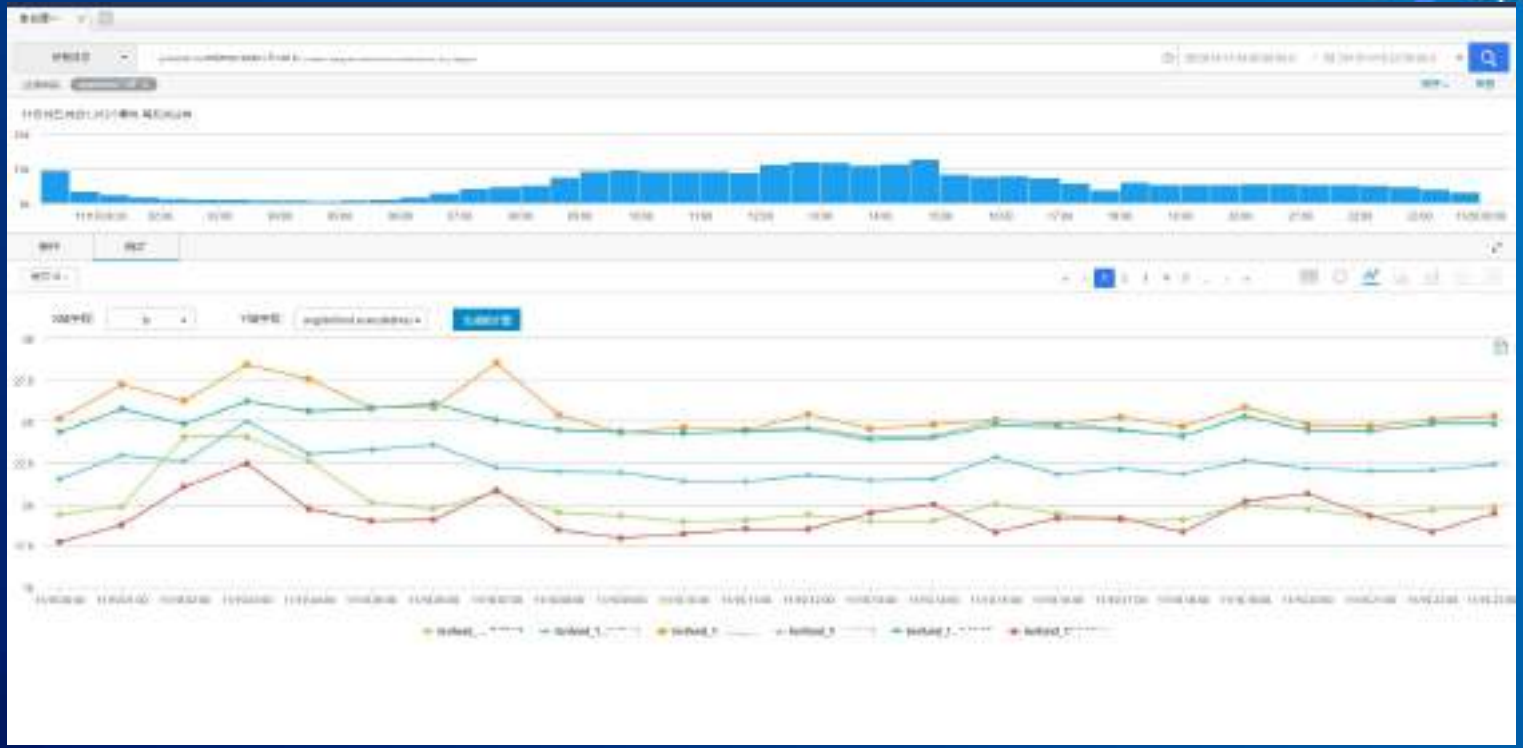
快速统计任意时间段，0-50ms操作时长的业务数量（low），50-500ms的业务数量（middle），以及500ms以上的业务数量（high）

日志应用场景 - 业务运维分析



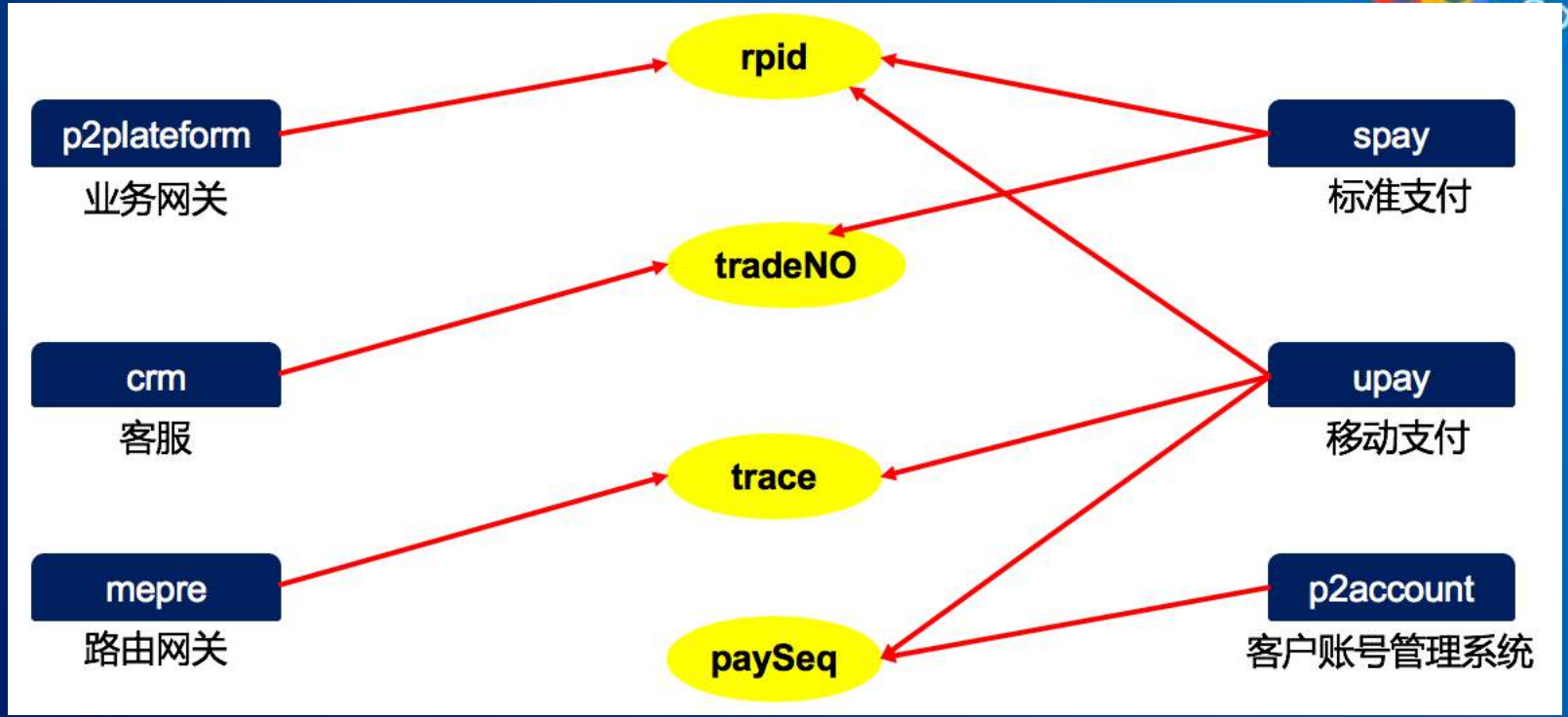
快速统计任意时间段，每台服务器各业务类型的业务数量占比

日志应用场景 - 业务运维分析



快速统计各台服务器每天各时段操作时长趋势，可以看出服务器操作时长变化趋势非常相似，业务耗时长的操作集中在某1，2台机器

日志应用场景 - 业务关联分析



不同的交易，应用系统之间的逻辑流程各不一样，而且出现错误日志的模块，很可能不是真正发生异常的模块，但应用系统之间有明确的日志关键字进行关联，通过日志关联以及时间排序，能快速定位出每笔交易的业务流程以及最早的故障源

日志应用场景 - 业务关联分析

运维世界 Ops World

p2plateform日志

0801-153205-064[SER_29569_WPF153204e561dd3]INFO Ser: 【P2P标的余额查询】业务网关返回的P2P标的余额查询结果为：Swap[result=0,e=null]{msgNum=0, merId=7001079, rpid=WPF153204e561dd3, reqDate=20160801, transNum=0, balance=00000000000000, accDate=20160801, retCode=0000, Memo=null, reqTime=153205, retMsg=null, funCode=0602, brc=01, bidId=7001079A0005990, avlBal=00000000000000}

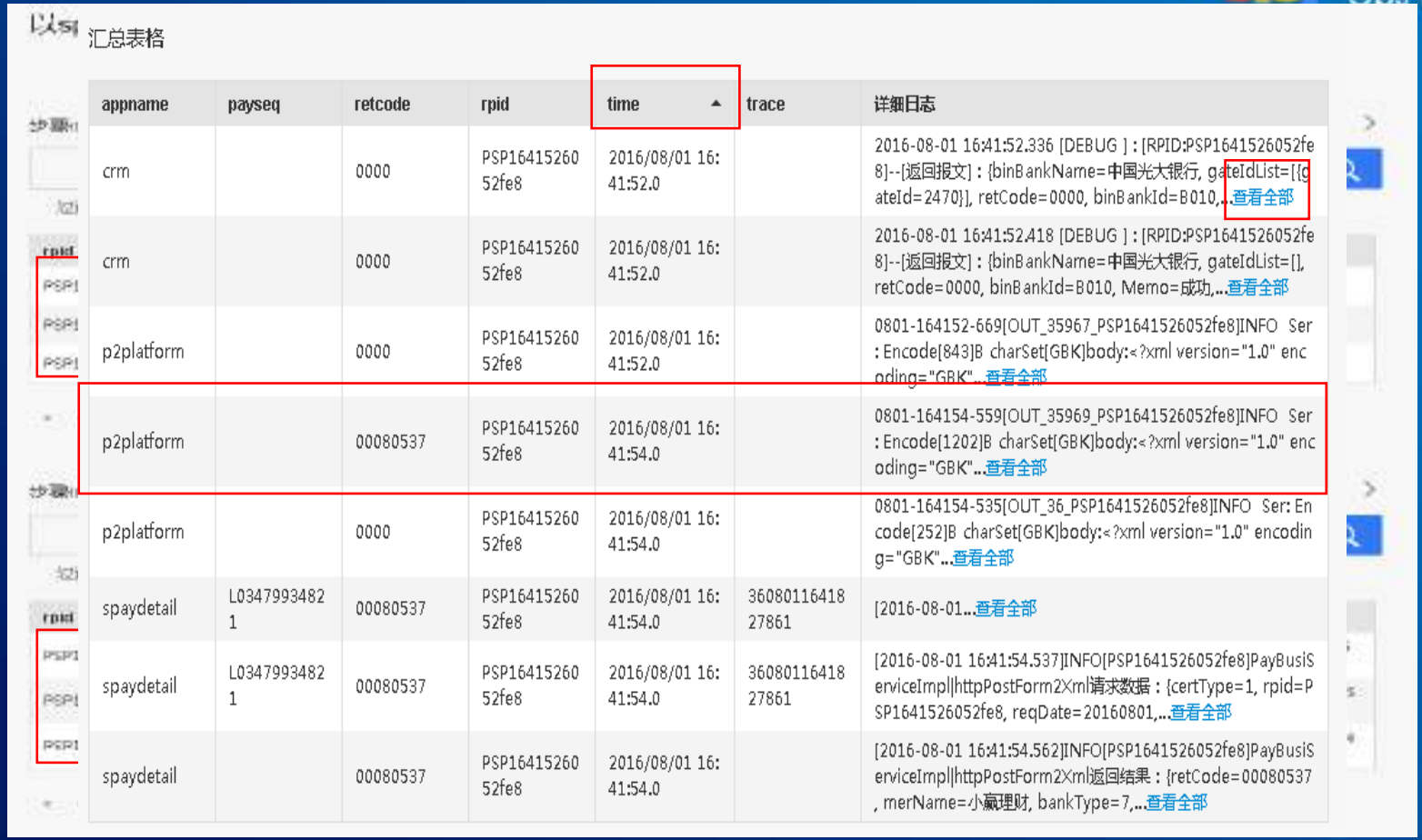
spay日志

[2016-08-01 15:19:58.950]INFO[9800-20160801-17453288]PayBusiServiceImpl|httpPostForm2Xml 返回结果：{orderState=4, tradeNo=1608011519586161, trace=1608011519584381, orderDate=20160801, merId=9800, transferSettleDate=20160801, purpose=司机提现, rpid=WPF153204e561dd3, comAmtType=-99, reqDate=20160801, resFormat=HTML, origAmt=12865, retCode=0000, transferDate=20160801, reqTime=151958, funCode=BE311001, retMsg=查询成功, comAmt=0, orderId=17453288, accessType=U}

CRM日志

0801-153204-822[OUT_35969_PSP153204ad5a11d]INFO Ser: Encode[252]B charSet[GBK]body:<?xml version="1.0" encoding="GBK" ?><xmlMobile> <retCode>0000</retCode> <Memo>操作成功</Memo> <retMsg>操作成功</retMsg> <tpValue>,9426,9430,9832,9996,7000998,</tpValue> <tradeno >1608011519586161</tradeno> <accessType>P</accessType></xmlMobile>

日志应用场景 - 业务关联分析



汇总表格

appname	payseq	retcode	rpid	time	trace	详细日志
crm		0000	PSP1641526052fe8	2016/08/01 16:41:52.0		2016-08-01 16:41:52.336 [DEBUG] : [RPID:PSP1641526052fe8]--[返回报文] : {binBankName=中国光大银行, gateIdList=[{gateId=2470}], retCode=0000, binBankId=B010,...查看全部
crm		0000	PSP1641526052fe8	2016/08/01 16:41:52.0		2016-08-01 16:41:52.418 [DEBUG] : [RPID:PSP1641526052fe8]--[返回报文] : {binBankName=中国光大银行, gateIdList=[], retCode=0000, binBankId=B010, Memo=成功,...查看全部
p2platform		0000	PSP1641526052fe8	2016/08/01 16:41:52.0		0801-164152-669[OUT_35967_PSP1641526052fe8]INFO Ser : Encode[843]B charSet[GBK]body:<?xml version="1.0" encoding="GBK"...查看全部
p2platform		00080537	PSP1641526052fe8	2016/08/01 16:41:54.0		0801-164154-559[OUT_35969_PSP1641526052fe8]INFO Ser : Encode[1202]B charSet[GBK]body:<?xml version="1.0" encoding="GBK"...查看全部
p2platform		0000	PSP1641526052fe8	2016/08/01 16:41:54.0		0801-164154-535[OUT_36_PSP1641526052fe8]INFO Ser: Encode[252]B charSet[GBK]body:<?xml version="1.0" encoding="GBK"...查看全部
spaydetail	L03479934821	00080537	PSP1641526052fe8	2016/08/01 16:41:54.0	360801164182 7861	[2016-08-01...查看全部
spaydetail	L03479934821	00080537	PSP1641526052fe8	2016/08/01 16:41:54.0	360801164182 7861	[2016-08-01 16:41:54.537]INFO[PSP1641526052fe8]PayBusiServiceImpl|httpPostForm2Xml请求数据 : {certType=1, rpid=PSP1641526052fe8, reqDate=20160801,...查看全部
spaydetail		00080537	PSP1641526052fe8	2016/08/01 16:41:54.0		[2016-08-01 16:41:54.562]INFO[PSP1641526052fe8]PayBusiServiceImpl|httpPostForm2Xml返回结果 : {retCode=00080537, merName=小赢理财, bankType=7,...查看全部

日志应用场景 - 安全分析

- 某驾校在2014年4月某天被黑客入侵导致网站无法登录，用户提供5GB的web日志文件，需要从日志文件中快速定位出攻击源ip

通过把服务器web日志导入到日志易系统，给日志打上标签“hacking”，标签和日志分组方便日志易系统同时处理不同的案件的日志，每个案件都有自己的标签和分组，方便不同的办案人查看不同的日志。这批将近5GB的日志总共有19,556,430条

01

日志应用场景 - 安全分析

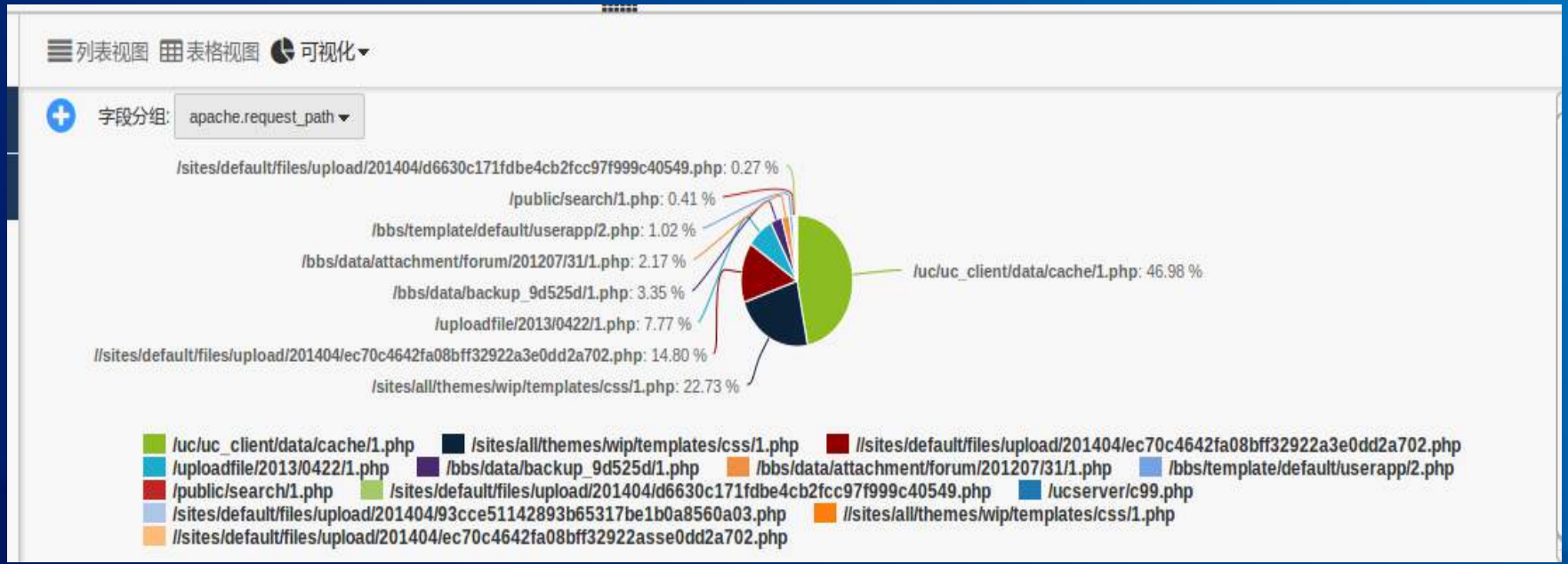
在服务器存在web后门的情况下，该后门程序格式通常为php文件，并且一般后门通过POST方式进行请求）。所以在搜索框搜索 “php AND apache.method:POST AND apache.status:200” ，得到以下结果，共3642条日志，可以清晰发现请求中存在异常文件

02

日志应用场景 - 安全分析

进行可视化统计视图（统计请求路径），可以发现搜索结果中（即步骤二筛选出来的3642条日志）请求数量最多的基本都是异常文件，可以统计这些异常文件的数量，快速确定了服务器内后门位置：
如//sites/default/files/upload/201404/ec70c4642fa08bff32922a3e0dd2a702.php
可以观察到该目录应为图片及其它文件上传目录，不应该存在可解析的php文件，所以判断为异常

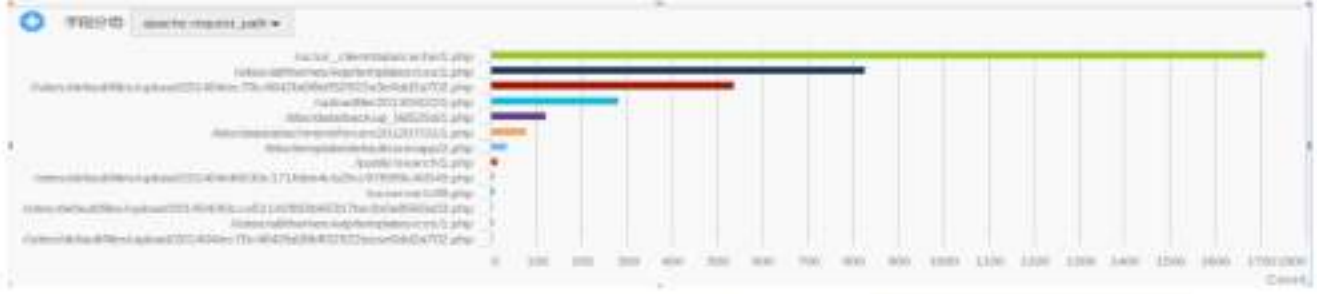
03



日志应用场景 - 安全分析

迅速统计出各异常路径的访问次数以及访问源ip

04



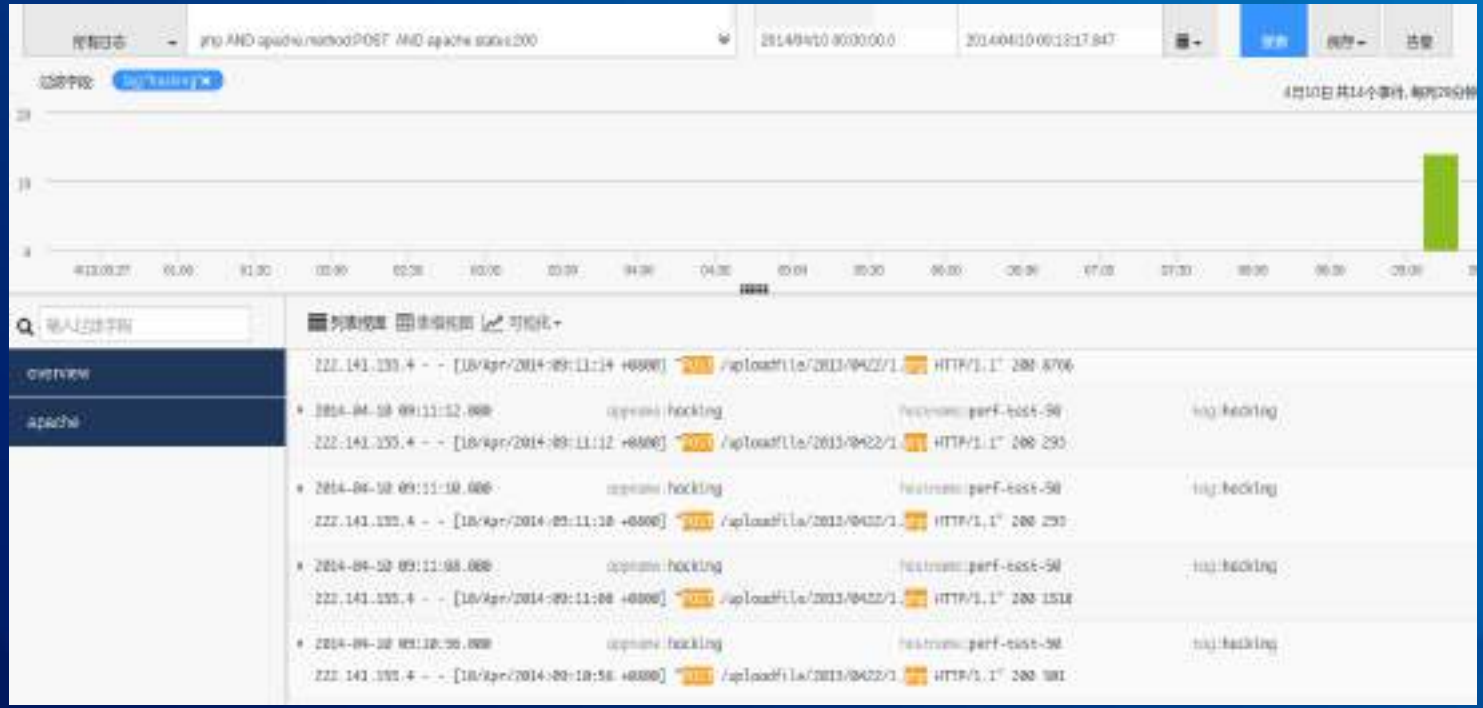
异常请求路径	请求次数
/uc/uc_client/data/cache/1.php	1711次
/sites/all/themes/wcp/templates/css/1.php	826次
/sites/default/files/upload/201404/	539次
/uploadfile/2013/0422/1.php	283次
/bbs/data/backup_%25%5/1.php	127次
/bbs/data/attachment/forum/201207/31/1.php	39次
/bbs/template/default/aserapp/2.php	37次
/public/search/1.php	15次
/sites/default/files/upload/201404/	10次
/uc/server/c90.php	9次
/sites/default/files/upload/	5次
/sites/all/themes/wcp/templates/css/1.php	3次
/sites/default/files/upload/201404/	1次

来源IP
222.141.155.4
203.160.131.104
119.4.252.36
119.4.252.209
119.4.252.123
182.16.27.66
61.53.40.82

日志应用场景 - 安全分析

通过日志查询，可以看到后门最初访问时间为2014年4月10日 9点10分，进一步缩小时间段，扩大搜索范围，以便查找该黑客攻击行为，定位该黑客攻击IP为222.141.155.4

05

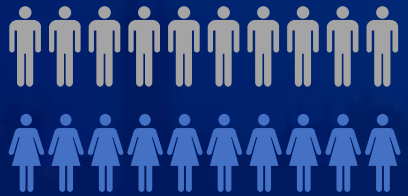


北京优特捷信息技术有限公司介绍

运维世界 Ops World

中国移动 China Mobile　国家电网公司 STATE GRID　小米开放平台　Letv乐视网　上汽通用汽车 SAIC-GM　有利网 YOOLI.COM

- 公司目前近70人，专注做好日志分析产品，一半以上为研发人员，基本上来自腾讯、高德、百度，名校硕士



真格基金1400万天使投资

红杉资本投资的6000万A轮融资

已为大型股份制银行，中移动，新疆农信，乐视，小米提供日志分析产品

基于运维日志的深度机器学习及智能运维产品即将推出

2014 **起步**

2015 **努力**

2016 **奋斗**

未来 **共创**

运维世界 Ops World

日志易，日志分析更容易

rizhiyi.com