

# Elastic Stack在证券行业 业务系统监控中的应用

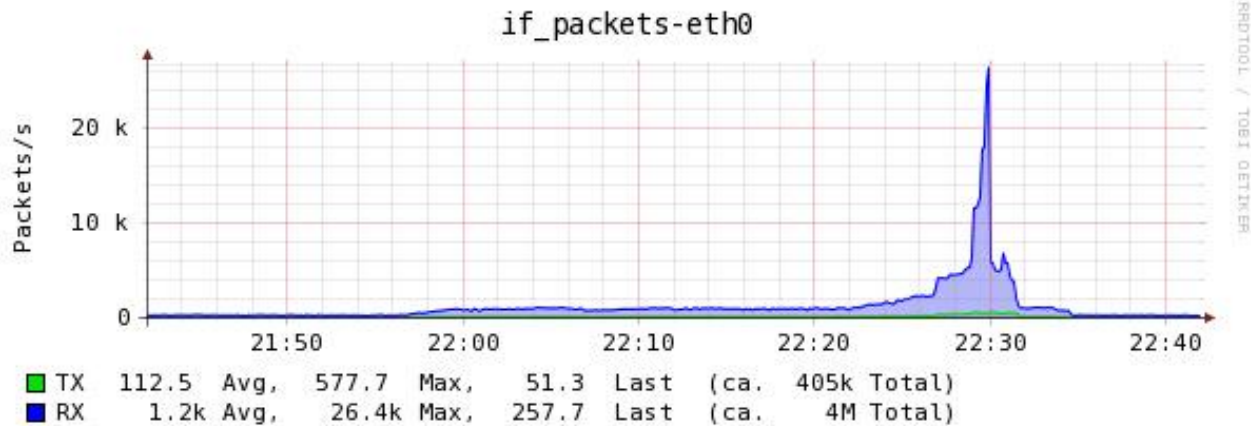
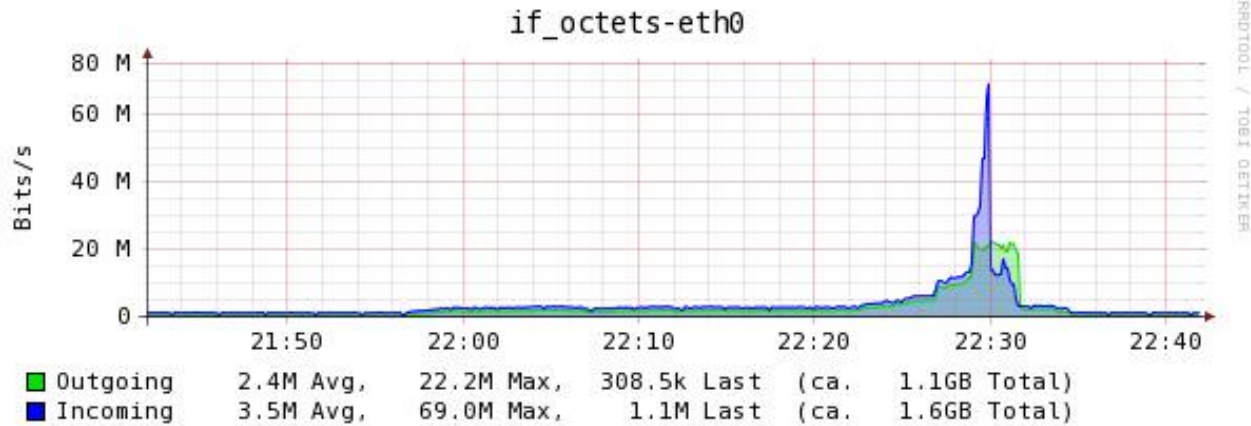
中国中投证券信息技术部 尉晋洪

- 运维遇到的问题
- 券商系统简介及ELK具体部署方案
- 应用一：排查问题
- 应用二：业务监控

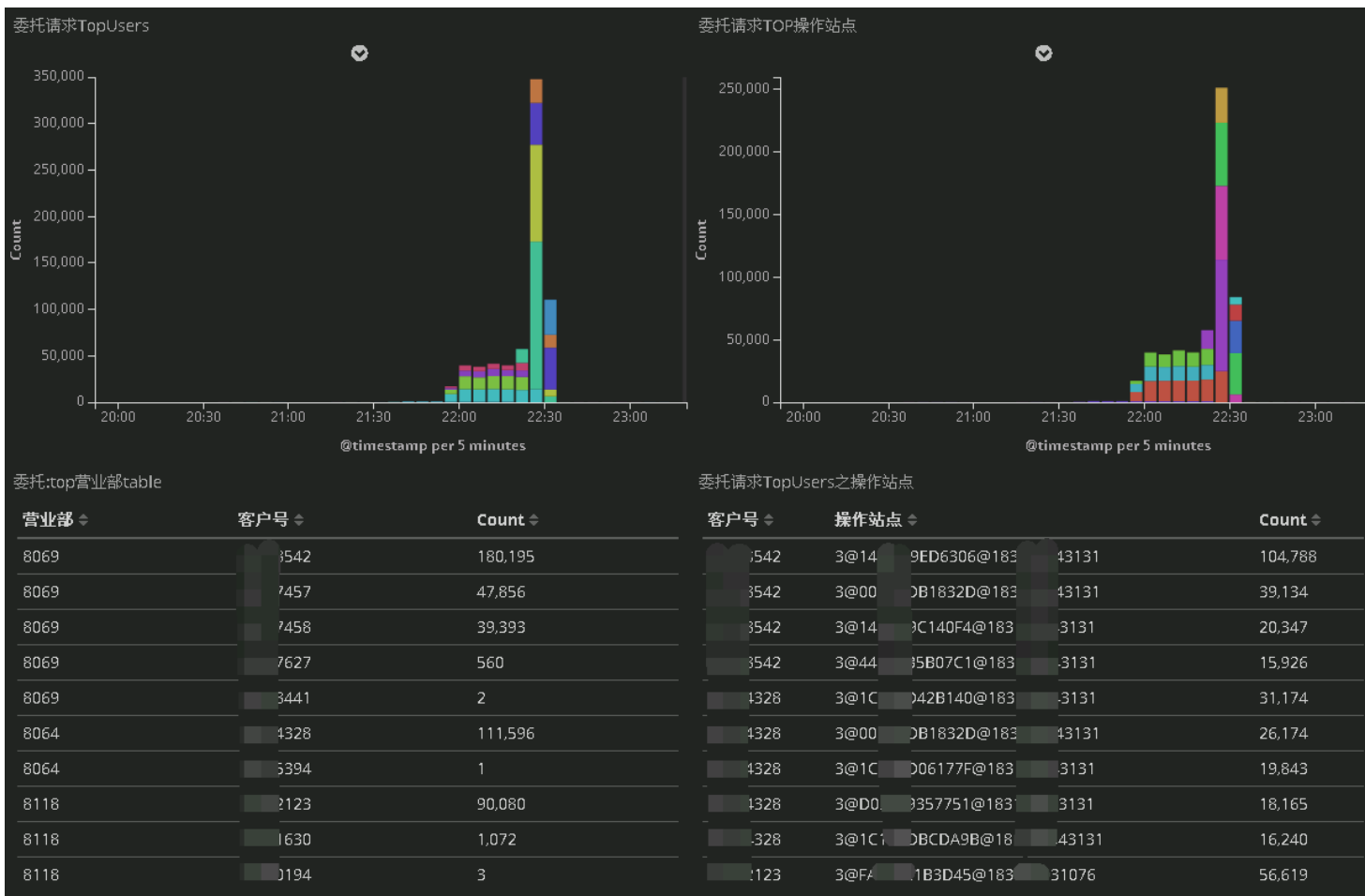
# 如何回答以下问题.....

- 功能号调用Top 10 ?
- 大耗时功能号Top 10 ?
- 客户登录、委托的平均耗时是多少 ?
- 最近半小时错误信息Top 10 ?
- 营业部客户委托Top 10 ?
- 网上交易站点地域分布是否合理 ?
- 系统有突发峰值，具体是什么引起 ?

# 发生了什么？



# 直观展示





# ELK提供全套解决方案



## Elastic Stack

100% open source  
No enterprise edition



Kibana



Elasticsearch

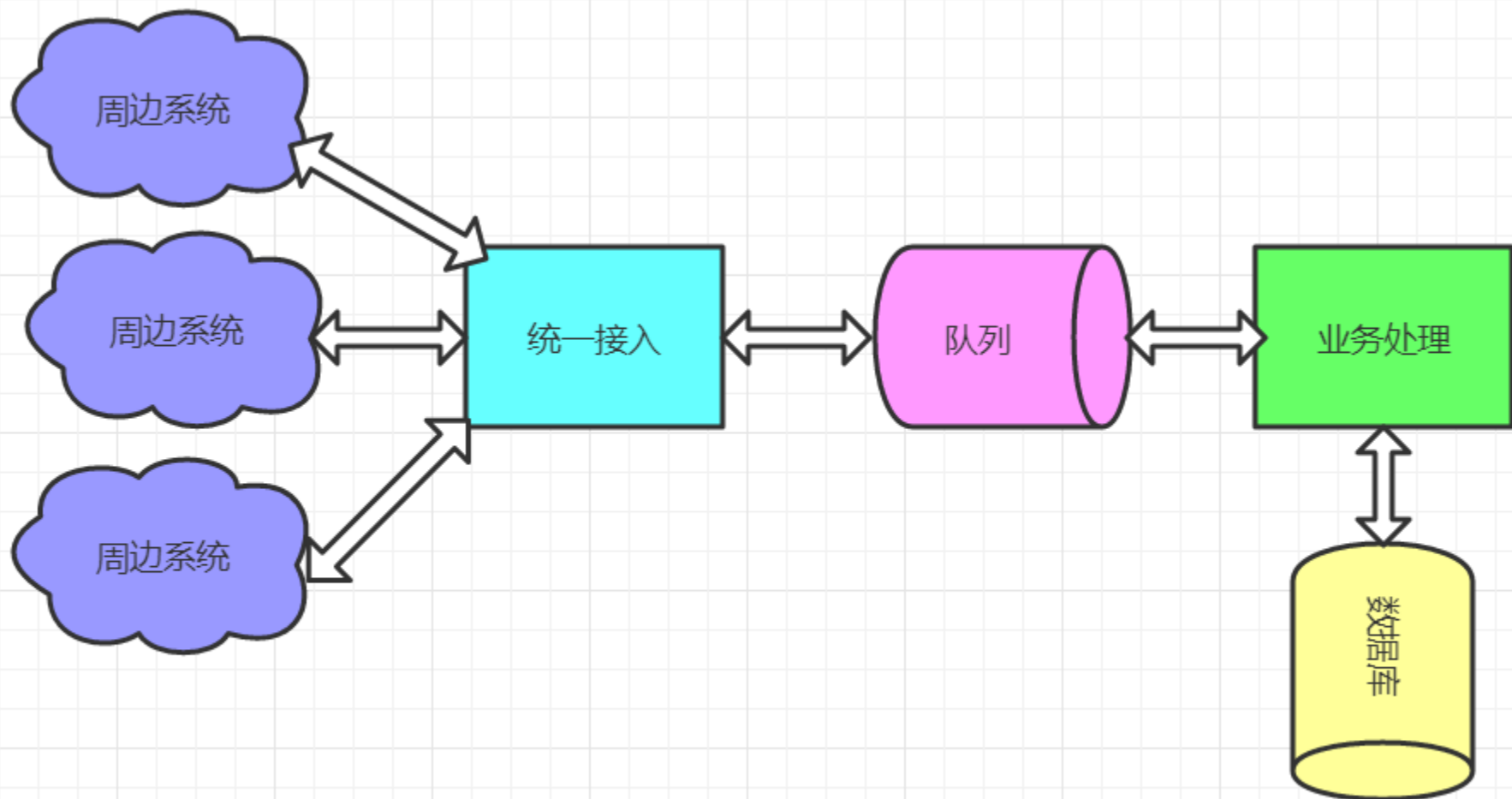


Beats



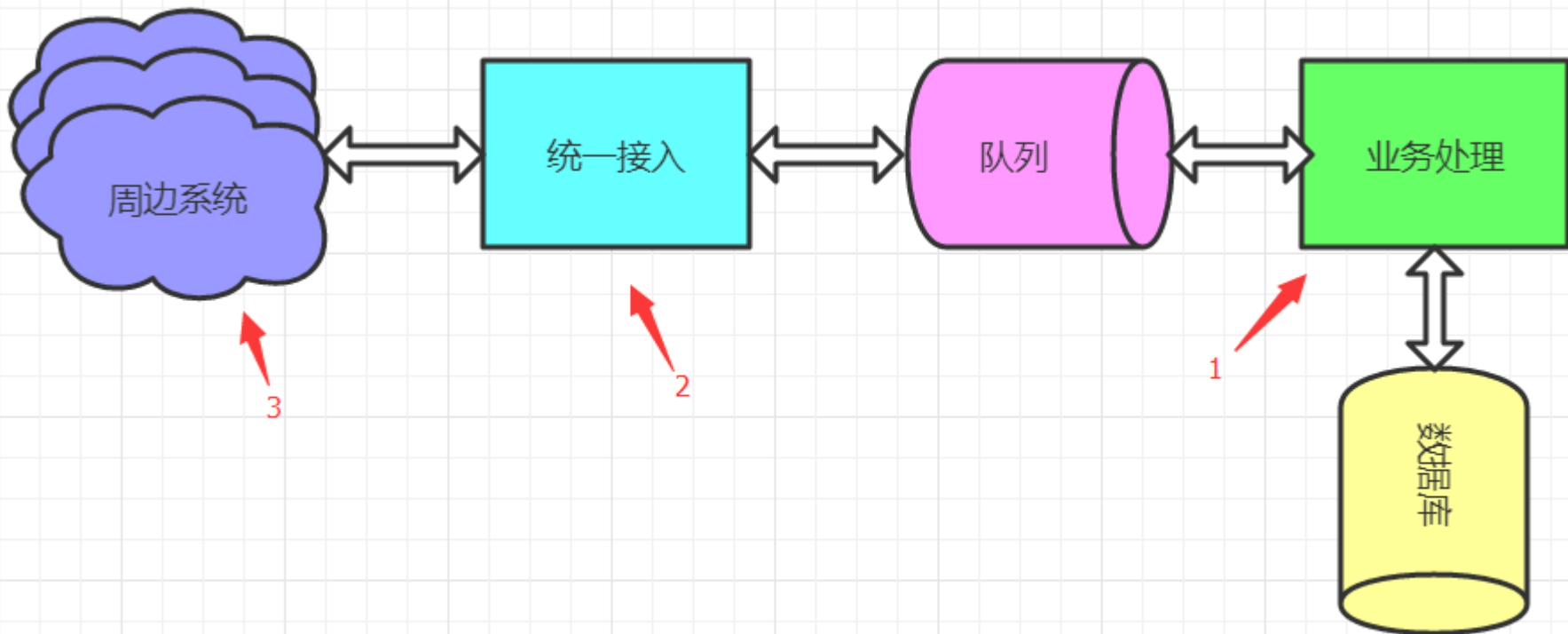
Logstash

# 业务系统架构简图





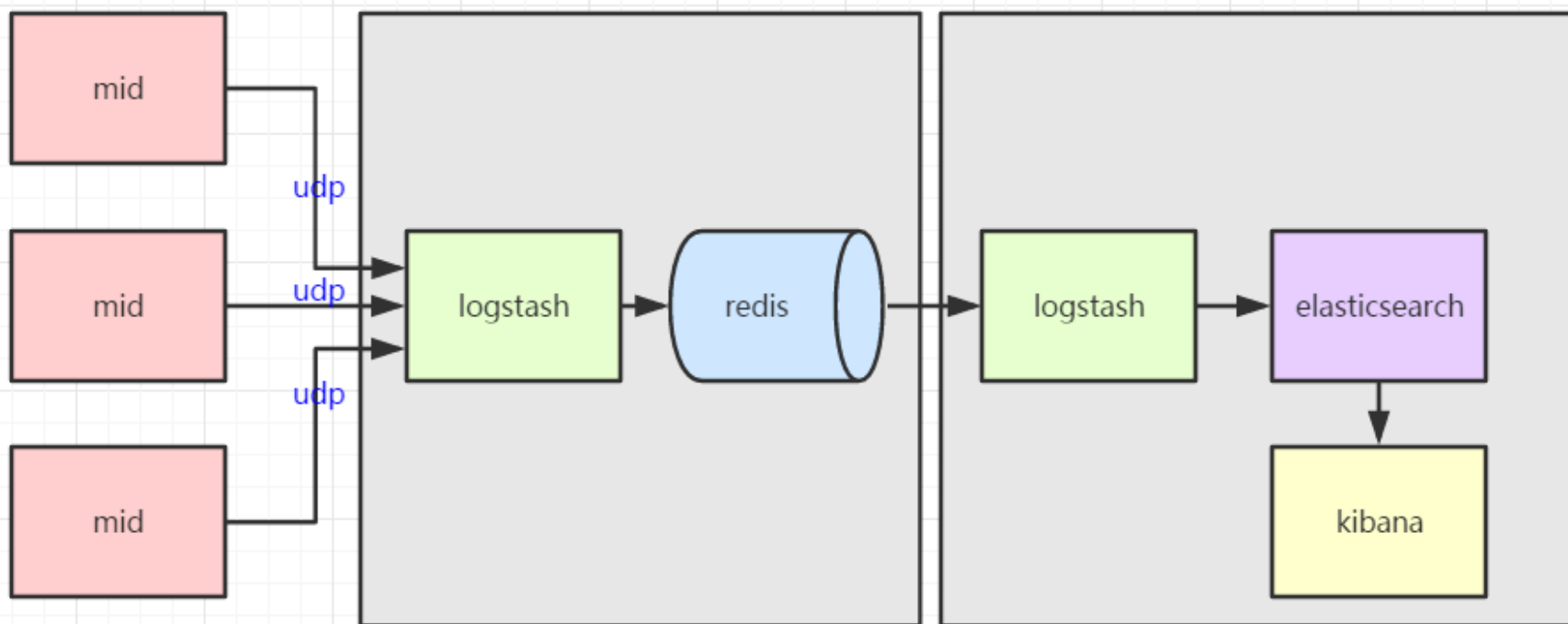
# 三大类业务系统日志



# 统一接入系统的日志

- 2016.09之前，出于性能的考虑，生产环境的统一接入系统不记录日志
- 2016.09月在排除一个生产问题时，利用开发商新版本支持的log4cplus库，向往发udp syslog，系统开销小，不影响生产
- udp 要求接收端处理速度足够快，否则丢包

# 统一接入系统日志数据流向



# Logstash input udp接收日志

- input {
- udp {
- port => "5140"
- type => tdxmid
- codec => plain { charset => "GBK" }
- queue\_size => 15000
- }
- .....
- }

# cat /etc/sysctl.conf

- # logstash udp input
- net.core.rmem\_default = 70000000
- net.core.rmem\_max = 70000000
- net.core.netdev\_max\_backlog = 1000
  
- # redis
- vm.overcommit\_memory = 1
- net.core.somaxconn = 65535

# 操作系统udp丢包监控

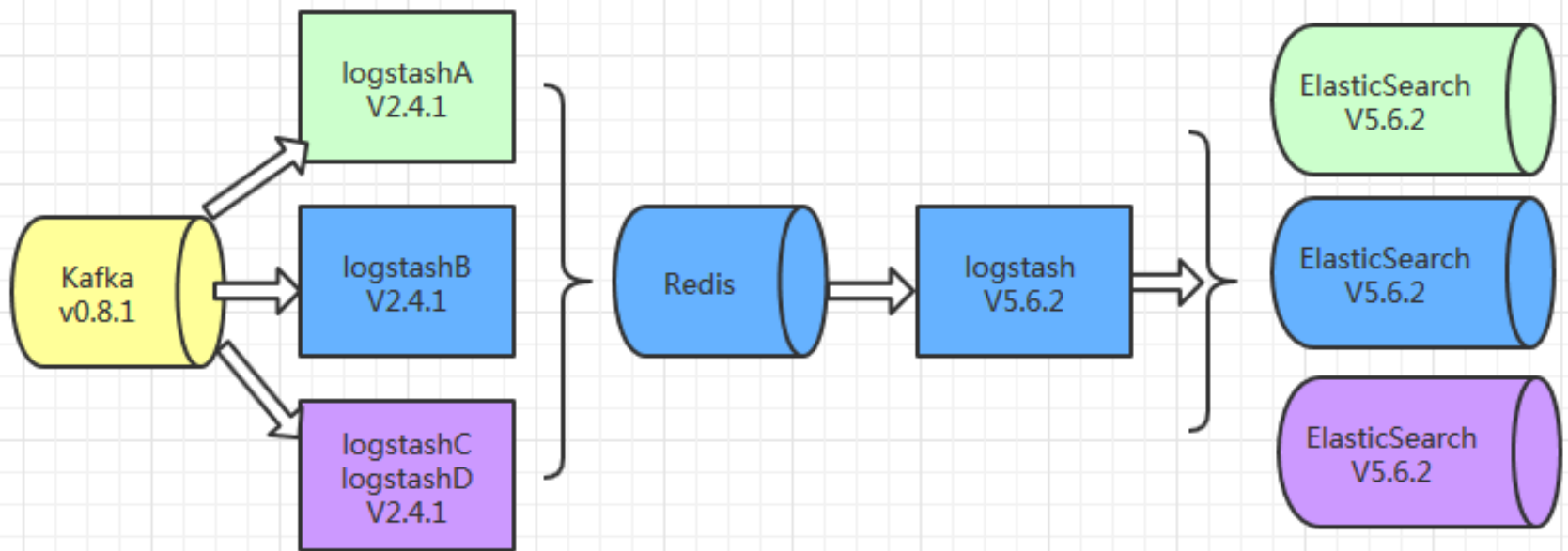
- watch “netstat -us|grep packet”

```
Every 2.0s: netstat -us|grep packet
1650643502 packets received
26987 packets to unknown port received.
0 packet receive errors
268064223 packets sent
```

- 接收端这里看到是0，说明没有丢包，处理速度够

# 业务处理系统的日志

- 从公司已有的Kafka中采集
- 功能号最全的日志，但日志信息有限
- Kafka v0.8.1，故采用logstash v2.4.1和logstash v5.6混编模式，redis做中介





# Logstash v2.4.1

## 3机4实例8线程对应8 Kafka分区

- `bin/logstash -f lsbpkafka.conf -w 4 -b 300`

```
input
{
  kafka {
    zk_connect => "10.10.10.10:2181,10.10.10.11:2181,10.10.10.12:2181"
    topic_id => "jzjy"
    type => "jzjybp"
    group_id => "logstash"
    consumer_id => "01220A"
    consumer_threads => 2
    # auto_offset_reset => "smallest"
    # reset_beginning => true
    codec => json
  }
}
```

```
output {
  if [type] == "jzjybp" {
    redis {
      host => "10.10.10.10:7379"
      db => 0
      data_type => "list"
      key => "logstash"
      batch => true
      batch_events => 500
      workers => 4
    }
  }
}
```

# 监控Kafka Lag, redis队列深度

```
Every 10.0s: bin/kafka-run-class.sh kafka.tools.ConsumerOffsetChecker --zkconnect 192.168.1.100:2181 --group logstash
```

Group	Topic	Pid	Offset	logSize	Lag	Owner
logstash	jzjy	0	7739185736	7739185813	77	logstash_01220A-0
logstash	jzjy	1	7858821802	7858821905	103	logstash_01220A-1
logstash	jzjy	2	6610951965	6610952065	100	logstash_16003B-0
logstash	jzjy	3	6586928896	6586928977	81	logstash_16003B-1
logstash	jzjy	4	6656794422	6656794422	0	logstash_16004C-0
logstash	jzjy	5	6629045170	6629045263	93	logstash_16004C-1
logstash	jzjy	6	1747020913	1747021007	94	logstash_16004D-0
logstash	jzjy	7	1738956306	1738956418	112	logstash_16004D-1
logstash	rzrq	0	1796944878	1796944975	97	logstash_2r01220A-0
logstash	rzrq	1	1792342322	1792342485	163	logstash_2r01220A-1
logstash	rzrq	2	1198765010	1198765167	157	logstash_2r16003B-0
logstash	rzrq	3	1184973848	1184973983	135	logstash_2r16003B-1
logstash	rzrq	4	1198335597	1198335767	170	logstash_2r16004C-0
logstash	rzrq	5	1189790133	1189790226	93	logstash_2r16004C-1

```
watch redis-cli -p 7379 -n 0 LLEN logstash  
watch redis-cli -p 7379 -n 1 LLEN logstash
```

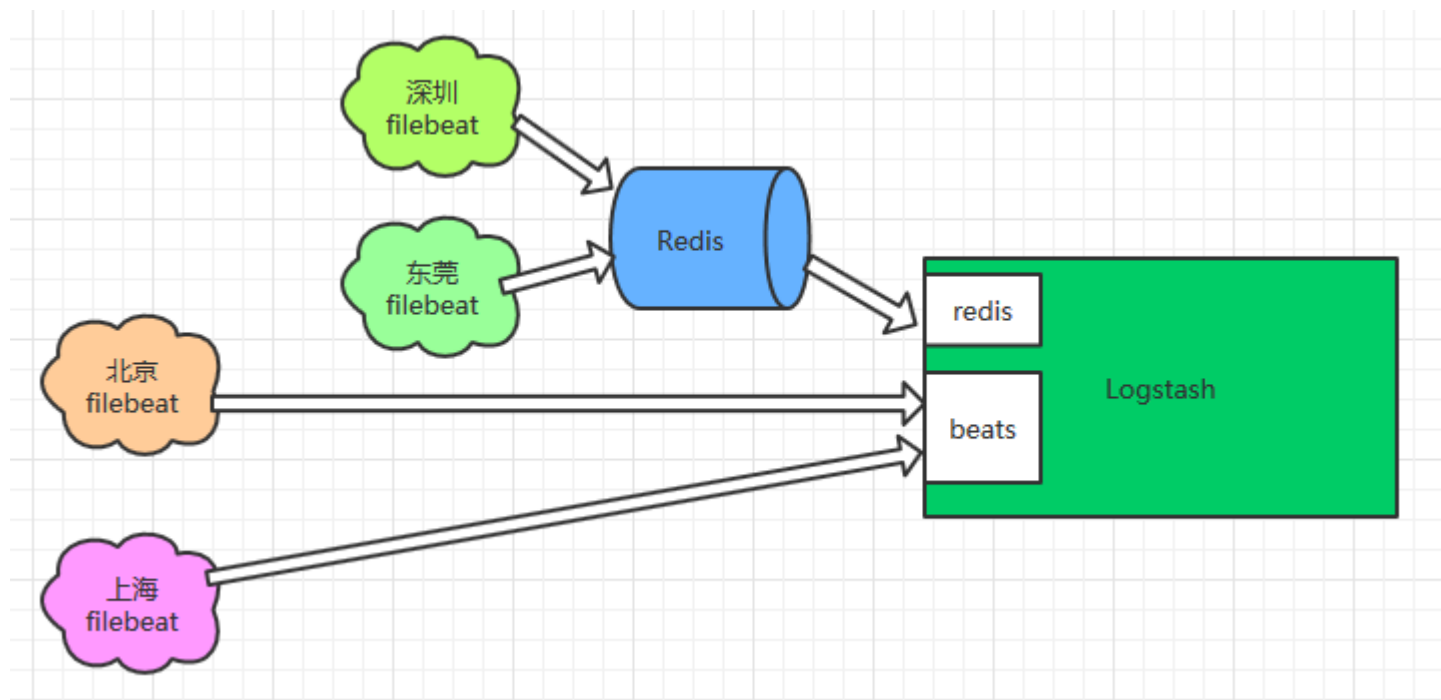
# Redis中介，不同业务入不同的库

## Logstash v5.6读取后写入ES

```
# read from redis data wrote by logstash 2.4.1
input {
  redis {
    host => "127.0.0.1"
    port => 7379
    db => 0
    data_type => "list"
    key => "logstash"
    threads => 6
  }
  redis {
    host => "127.0.0.1"
    port => 7379
    db => 1
    data_type => "list"
    key => "logstash"
    threads => 4
  }
}
```

# 周边系统日志

- 目前只分析了通达信网上交易
- **filebeat**做采集和基本过滤、多行合并
- 一台虚拟机 **Logstash ES Kibana**
- 根据站点采用不同策略，避免开太多端口
- 本地站点接**redis**
- 外地站点接**beats**（公网 / 压缩 / IP白名单）
- 各地站点的耗时最接近客户真实感受



# 目前集群规模


- 最大一套网上交易接入日志，两台虚拟机
- 最大一套手机交易接入日志，两台虚拟机
- 全部融资融券接入日志，一台虚拟机
- 通达信交易周边系统日志，一台虚拟机
- 全业务处理系统日志，三台

# 应用之一： 排查问题

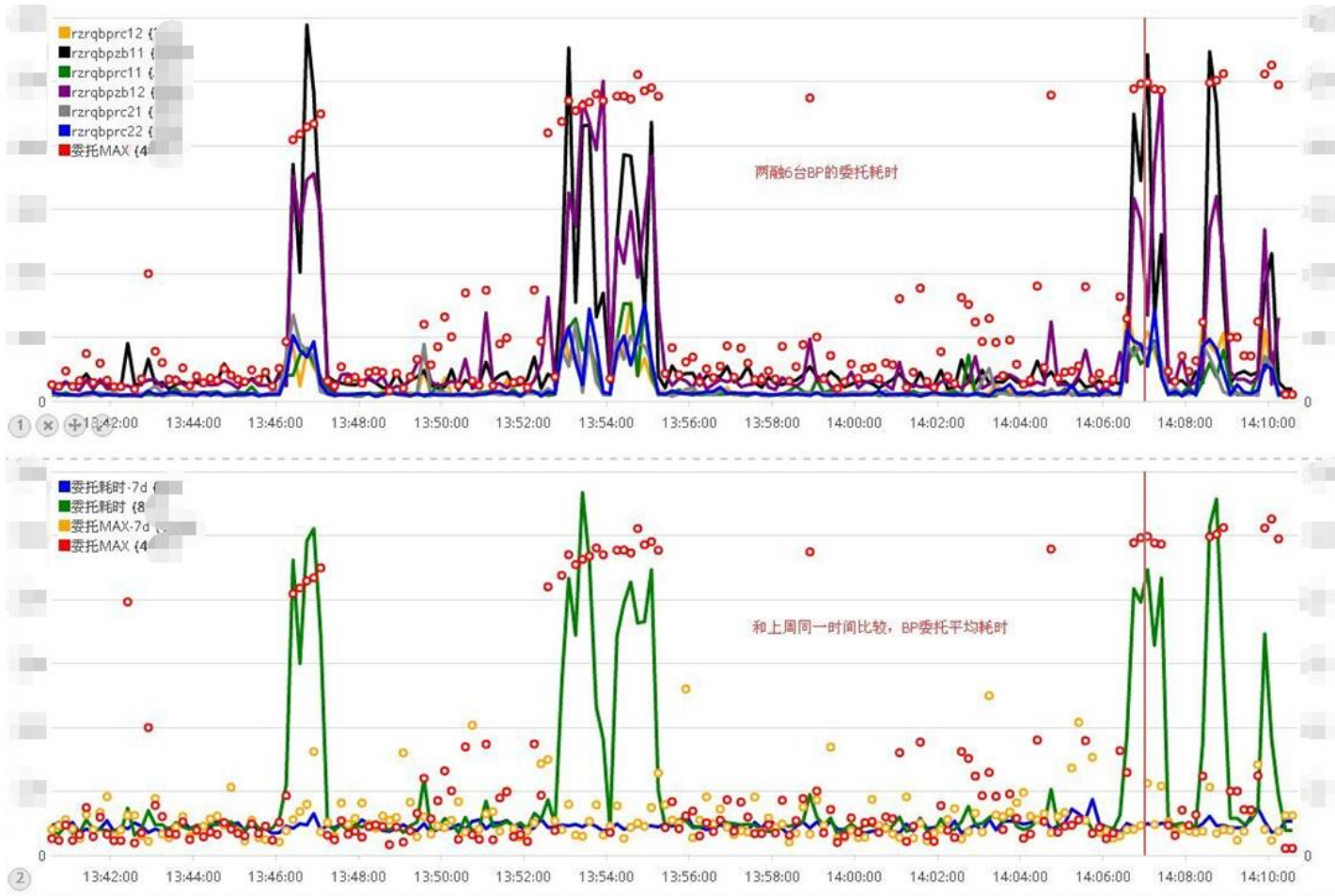




# 无用功能号调用

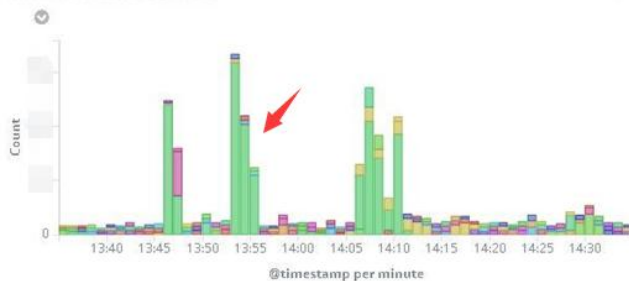
错误 	Count
应用接入网关正式版(-7415):RPC调用域中不存在指定路由	18,621
(313)密码有误	2,277
(100010)网关:业务提示:[市值配售新股申购禁止重复委托]	1,946
(107532)网关:用户[1000000000]在操作渠道[7]上需要强制使用高安全等级的认证方式!	1,242
(409)已成交或已撤单	640
系统暂不支持该功能!	395
(0)网络不稳定或后台服务忙,接收包头失败,请稍后重试!	289
(305)资产帐号不存在	270
(600241)网关:委托数量超过最大可申购数量[0]!	261
(413)资金可用数不足	190

# 突发委托耗时增大

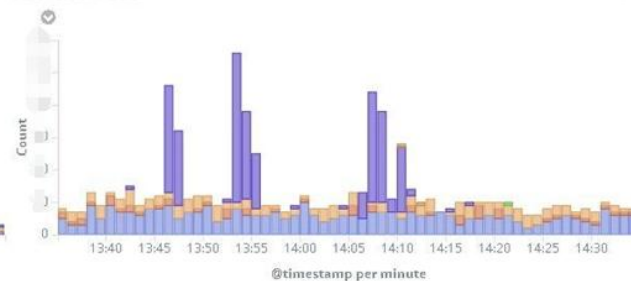


# 问题原因一目了然

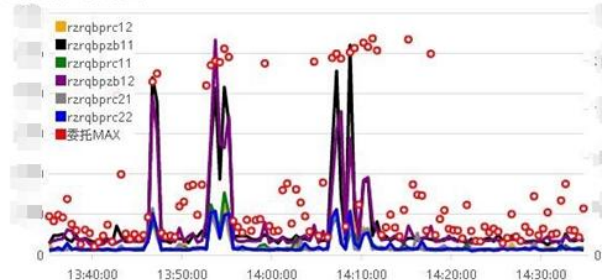
TOP操作站点-委托和撤单-两融



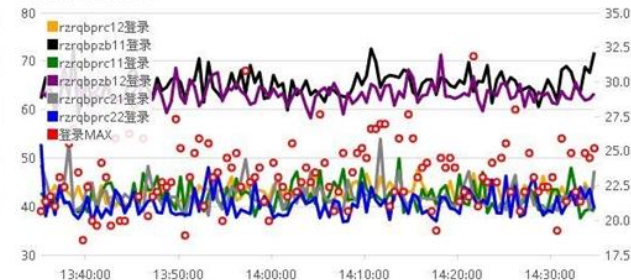
大耗时功能号-两融



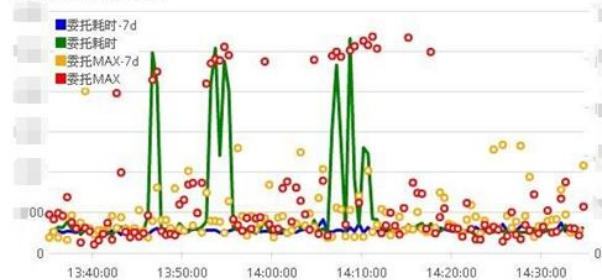
融资融券BP委托耗时



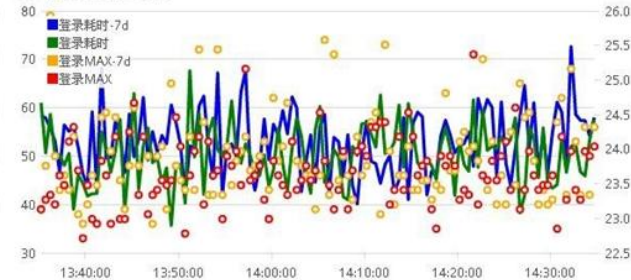
融资融券BP登录耗时



BP委托耗时比较图-两融



BP登录耗时比较图-两融

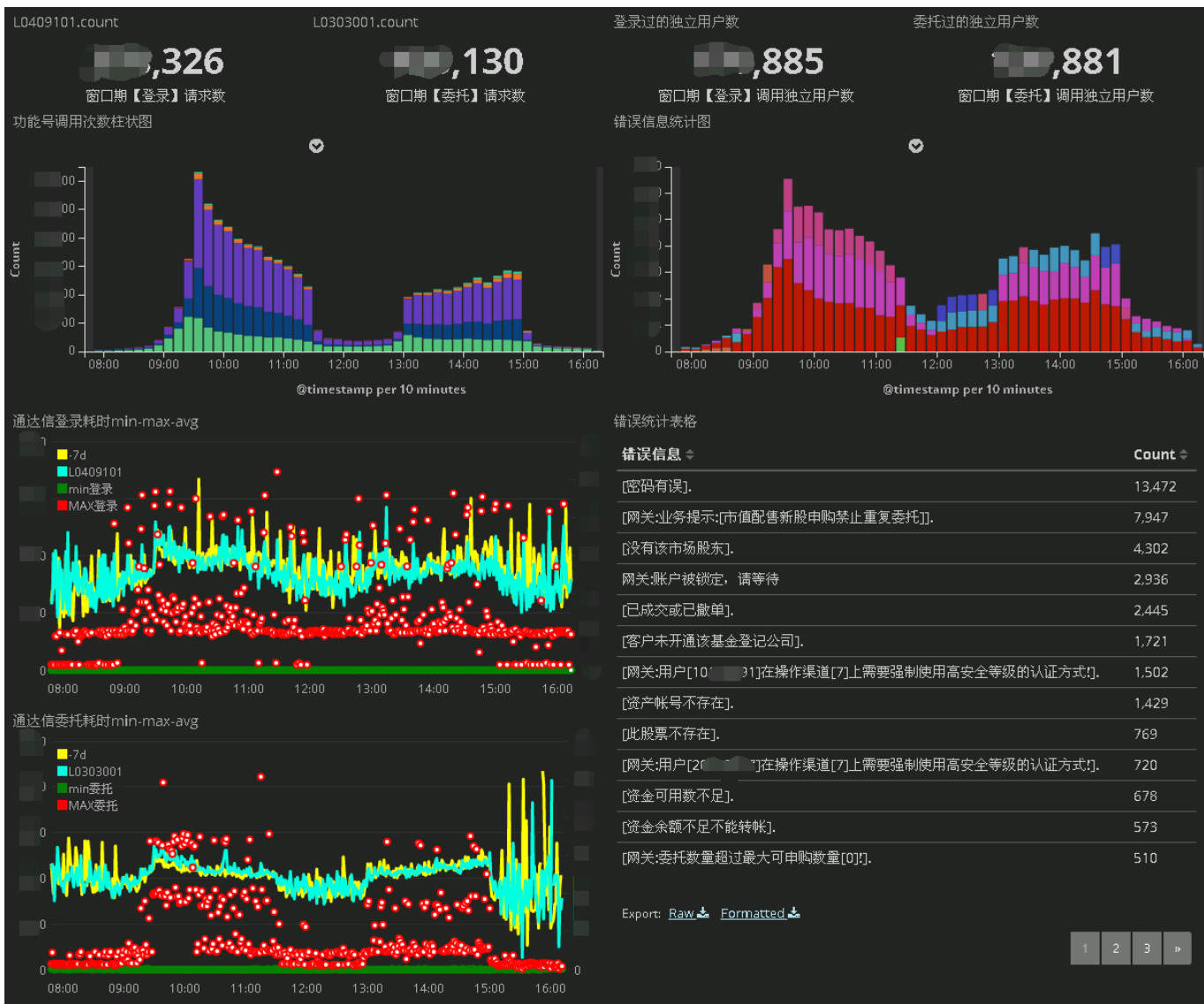


## 应用之二：业务监控

# 业务监控维度

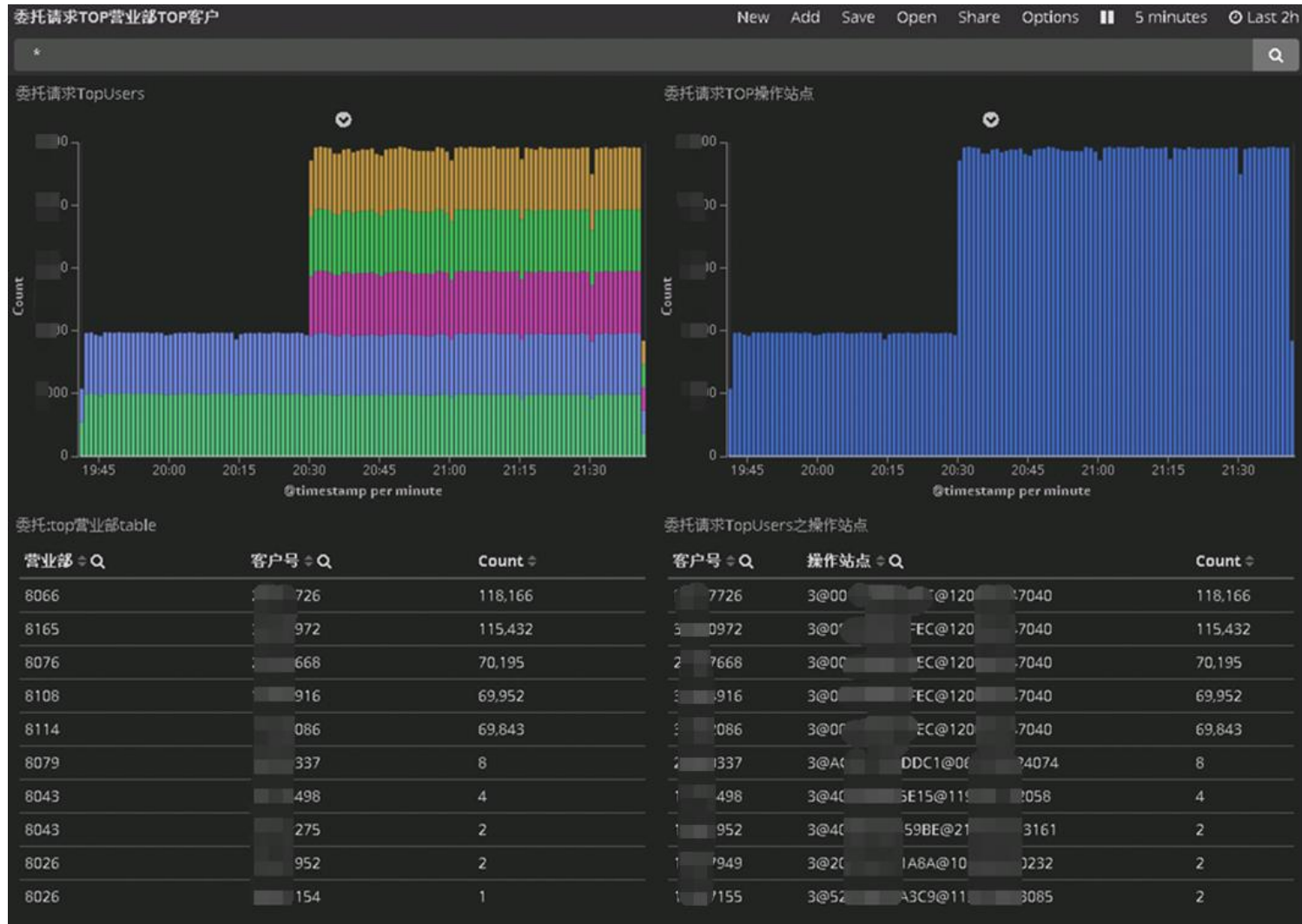
- ① 功能号
- ② 客户号
- ③ 错误信息
- ④ 响应时间
- ⑤ 客户IP地理信息
- ⑥ 其他，如客户端版本

# 某周边业务系统运行概览



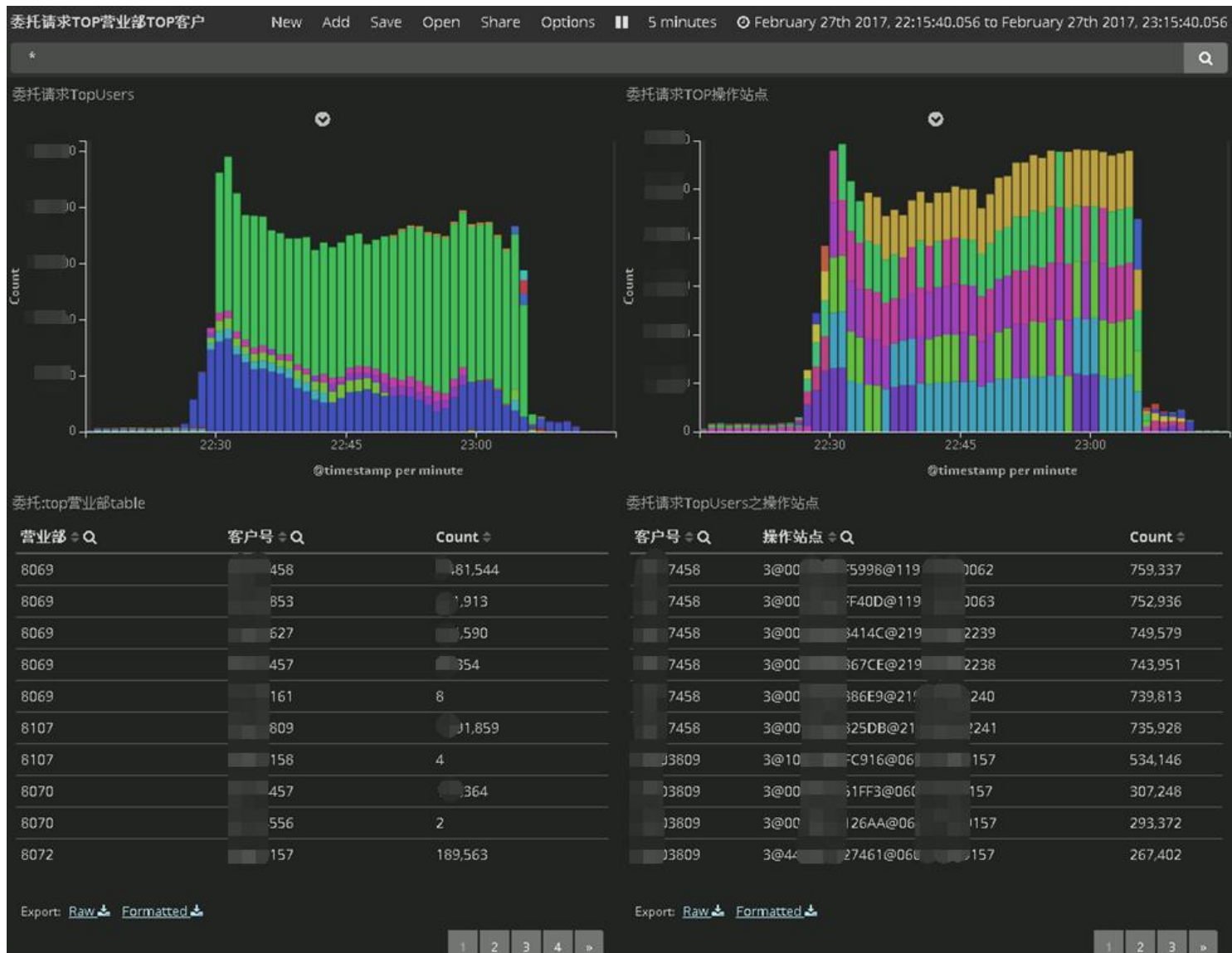


# 异常客户行为监控



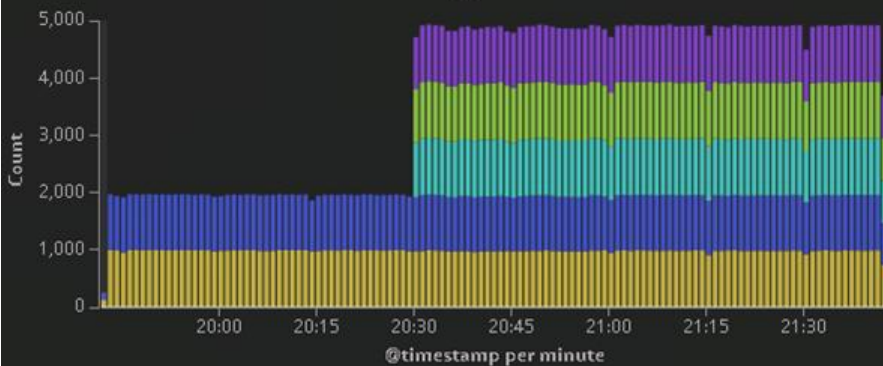


# 异常客户行为监控2

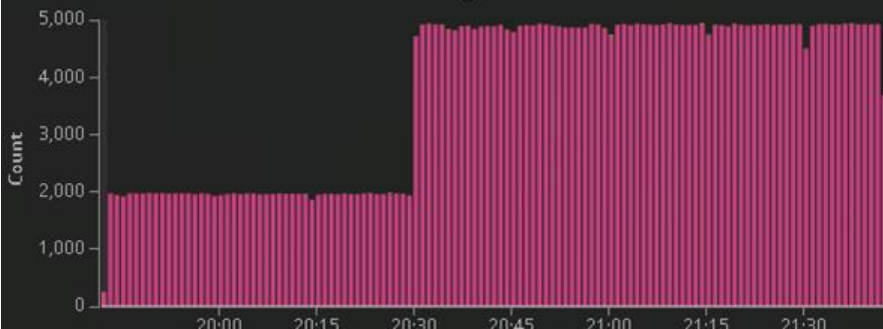


# 错误信息

委托请求TopUsers



错误信息统计图



错误统计表格

错误信息	Count
[不支持隔日委托].	447,606
[网关:业务提示:[该股票今日不支持申购]].	433
[密码有误].	297
[网关:业务提示:[此业务可执行时间段为08:30:00-16:05:00]].	69
[资产帐号不存在].	51
[股东代码不存在].	12
[网关:业务提示:[此业务可执行时间段为08:30:00-18:05:00]].	11
[客户未开通该基金登记公司].	8
[没有该市场股东].	6
[网关:业务提示:[无申购日期为20170125,缴款日期为20170203的新股或应缴款金额小于冻结金额]].	3
[网关:资产帐户[ ]34]不是[正常]状态].	3
[此股票不存在].	2
[用户代码不存在].	2

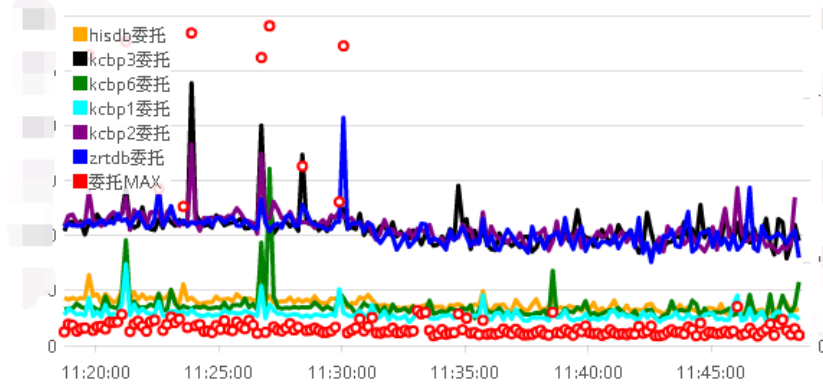
Export: [Raw](#) [Formatted](#)

# 响应时间

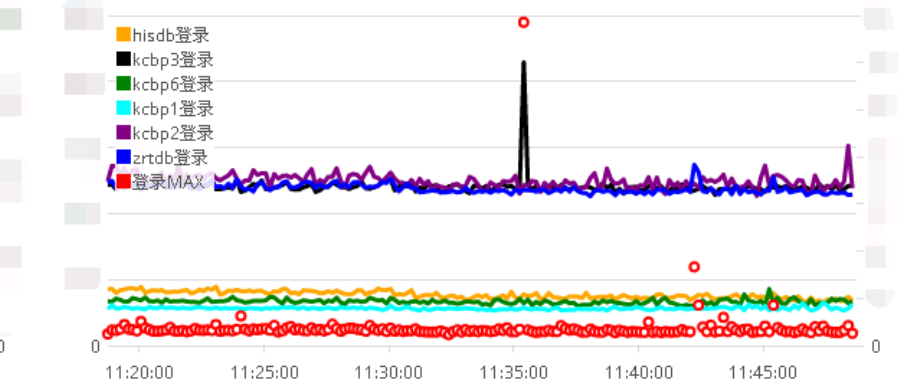


# 耗时

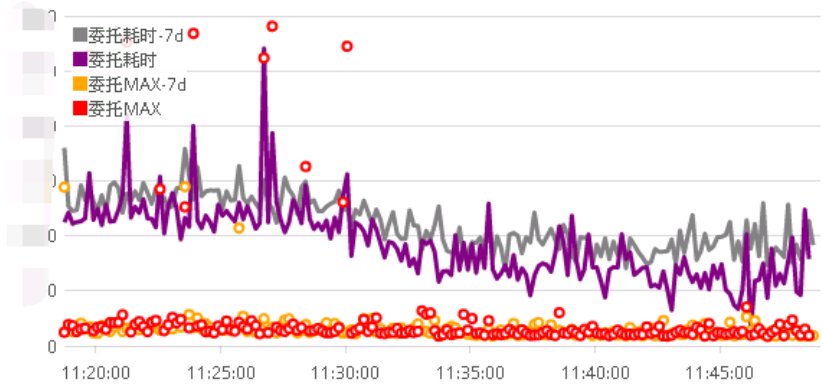
集中交易BP委托耗时



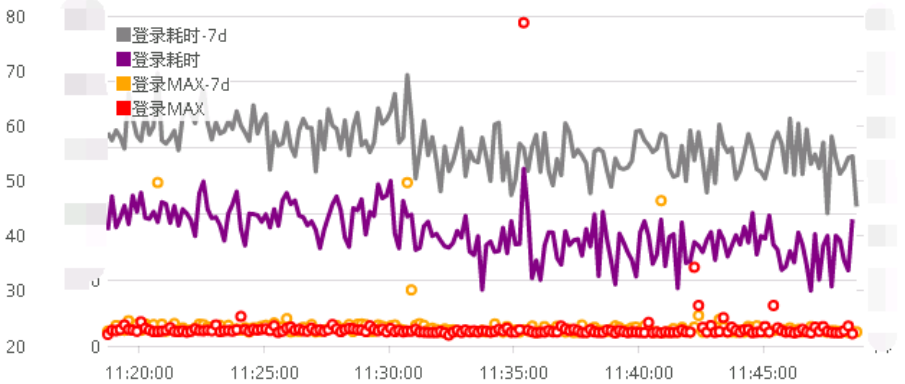
集中交易BP登录耗时



BP委托耗时比较图

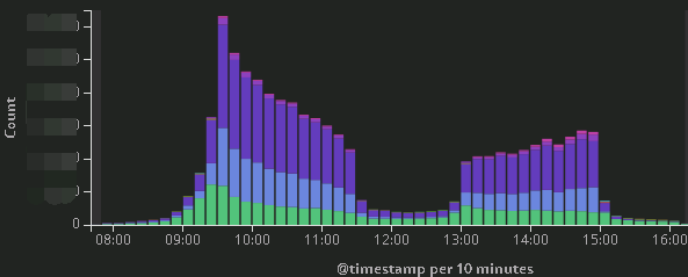


BP登录耗时比较图

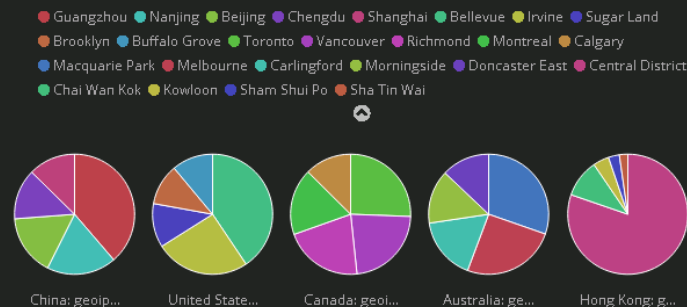


# 客户委托地理位置信息

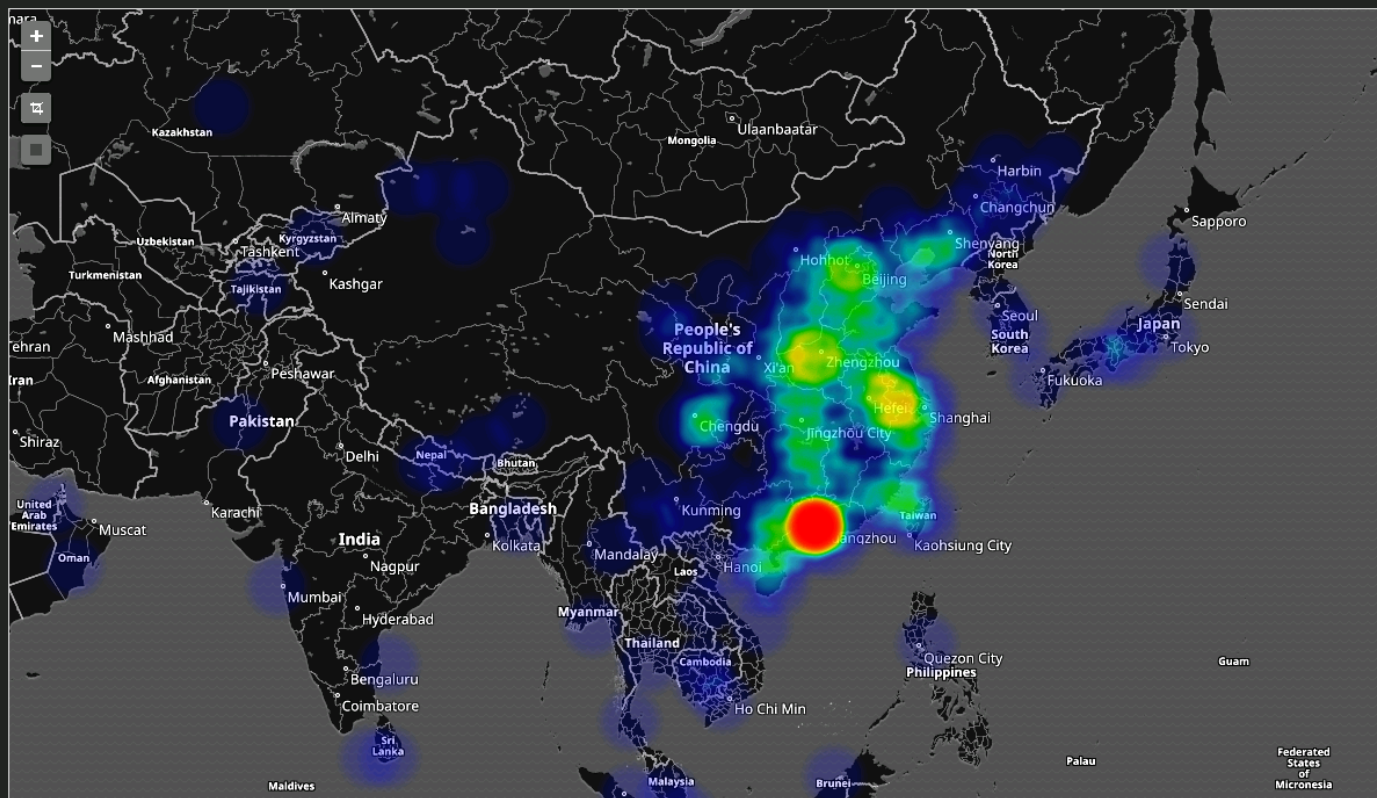
功能号调用次数柱状图



委托请求0303001地理分布饼图



地理位置之全部



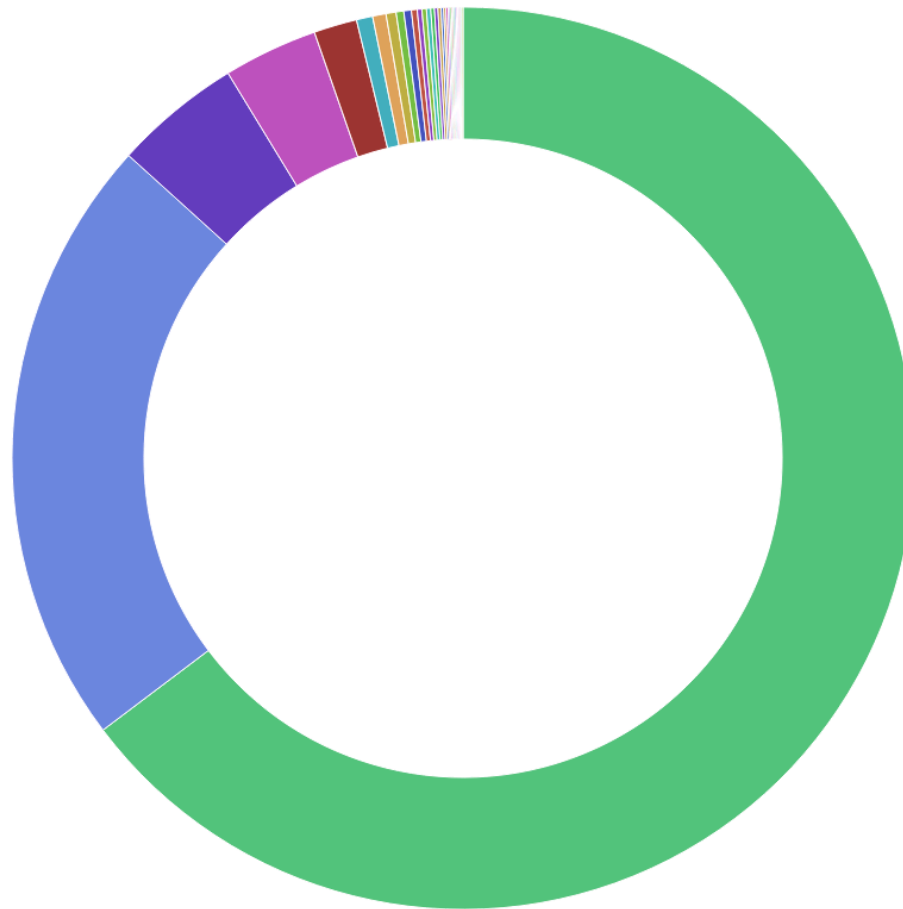
# 客户端版本统计

Visualize / 饼图-客户端版本

Save Share Refresh 1 minute Last 4 hours

Linked to Saved Search "查询-98-100登录请求"

Add a filter +



- 7.13
- 8.54
- 7.14
- 8.55
- 8.5
- 7.06
- 7.1
- 6.66
- 7.03
- 6.99
- 7.05
- 8.53
- 8.47
- 7.12
- 8.38
- 8.49
- 8.46
- 6.9
- 7.3
- 6.93
- 6.94
- 8.42
- 7.09
- 6.65
- 8.45
- 7.07
- 6.68
- 6.88
- 6
- 7.02

# 运维必备之神器

- ELK是日志监控的全套解决方案
- 学习从logstash入手，熟悉业务日志
- 参考资料：三斗的书，官网文档，官网blog
- yum安装升级，一路从5.0.0到目前的5.6.3
- ELK可以平行扩展，效率完全满足要求

# 谢谢



weijh

广东 深圳



扫一扫上面的二维码图案，加我微信