Elastic Stack在证券行业业务系统监控中的应用

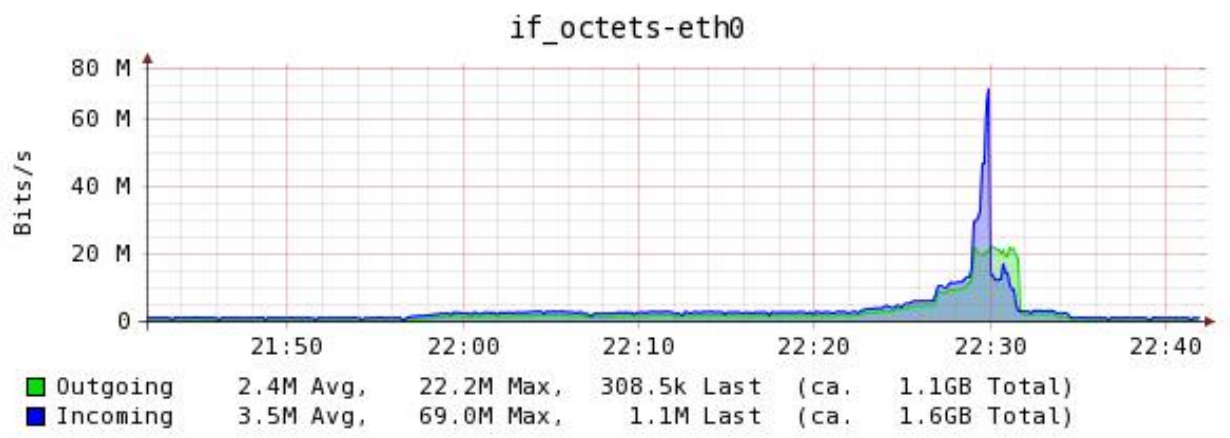
中国中投证券信息技术部 尉晋洪

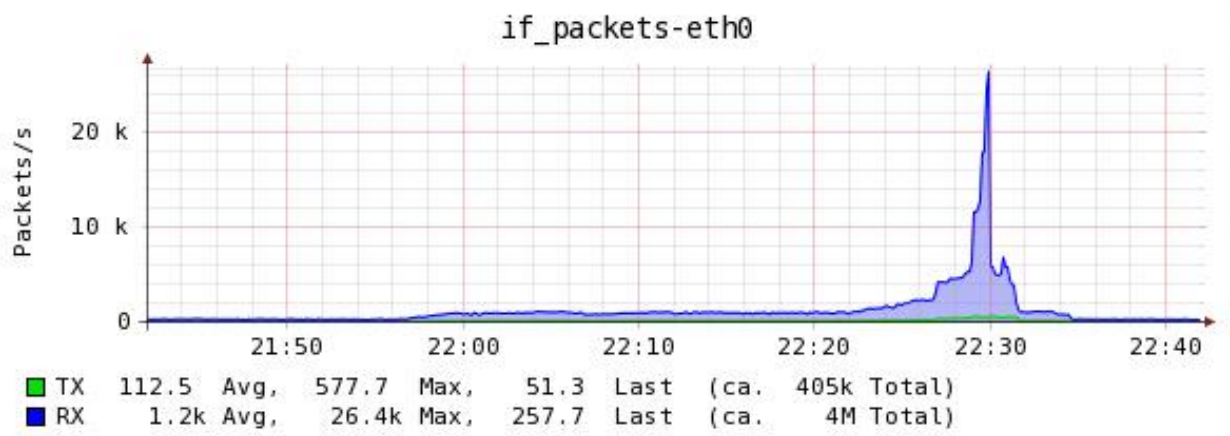
- 运维遇到的问题
- 券商系统简介及ELK具体部署方案
- 应用一：排查问题
- 应用二：业务监控

如何回答以下问题.....

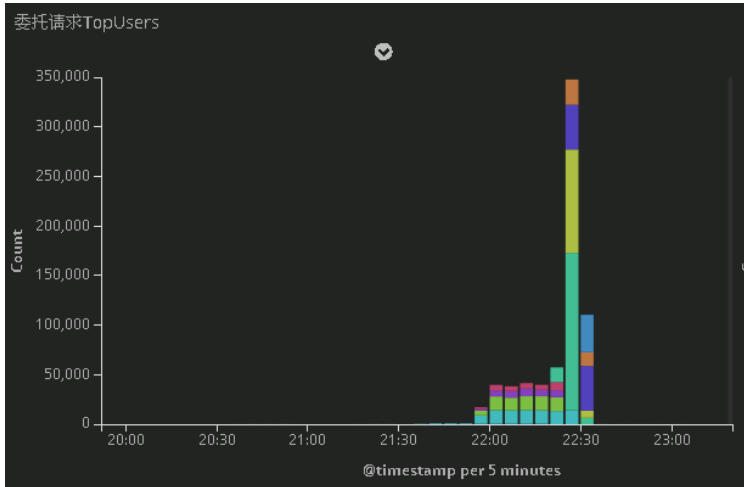
- 功能号调用Top 10 ？
- 大耗时功能号Top 10？
- 客户登录、委托的平均耗时是多少？
- 最近半小时错误信息Top 10？
- 营业部客户委托Top 10？
- 网上交易站点地域分布是否合理？
- 系统有突发峰值，具体是什么引起？

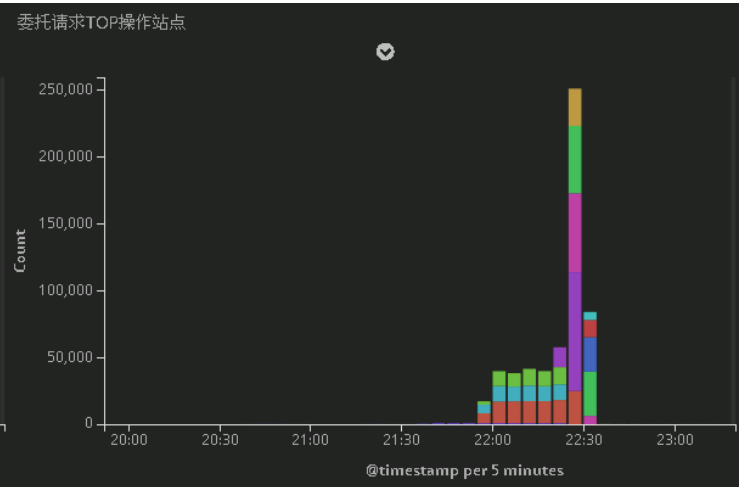
发生了什么？


if_octets-eth0
Bits/s
80 M
60 M
40 M
20 M
0
21:50
22:00
22:10
22:20
22:30
22:40
Outgoing 2.4M Avg, 22.2M Max, 308.5k Last (ca. 1.1GB Total)
Incoming 3.5M Avg, 69.0M Max, 1.1M Last (ca. 1.6GB Total)
RRDTOOL / TOBI OETIKER


if_packets-eth0
Packets/s
20 k
10 k
0
21:50
22:00
22:10
22:20
22:30
22:40
TX 112.5 Avg, 577.7 Max, 51.3 Last (ca. 405k Total)
RX 1.2k Avg, 26.4k Max, 257.7 Last (ca. 4M Total)
RRDTOOL / TOBI OETIKER

直观展示





委托:top营业部table

营业部	客户号	Count
8069	3542	180,195
8069	7457	47,856
8069	7458	39,393
8069	7627	560
8069	3441	2
8064	4328	111,596
8064	5394	1
8118	2123	90,080
8118	1630	1,072
8118	0194	3

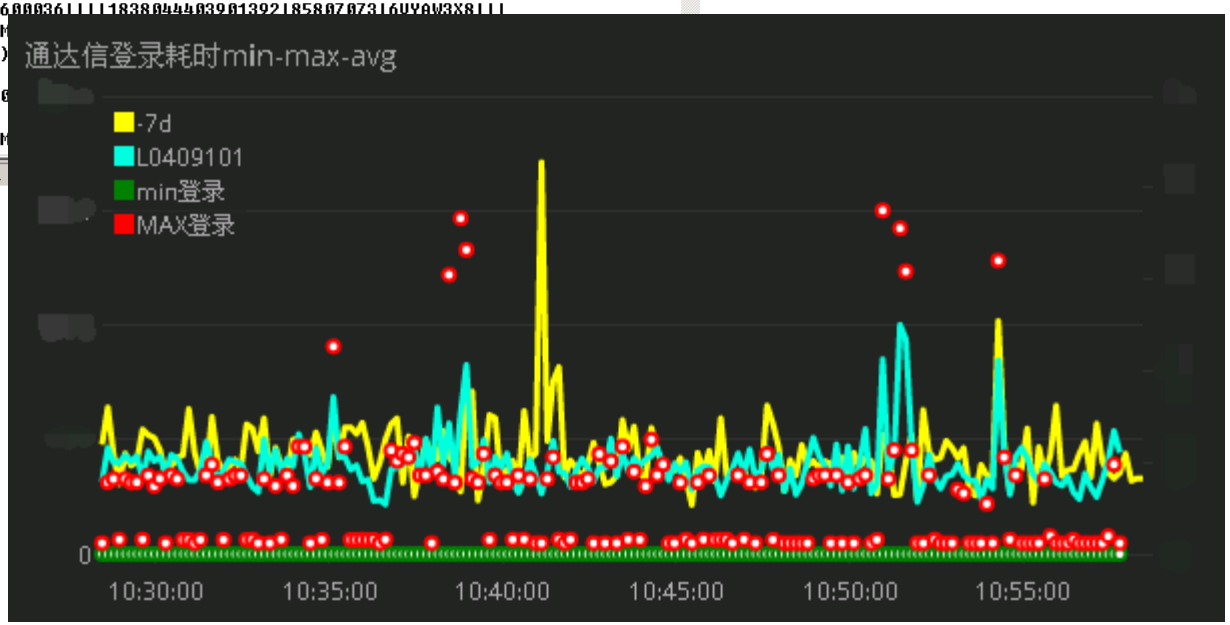
委托请求TopUsers之操作站点

客户号	操作站点	Count
5542	3@14 9ED6306@183 43131	104,788
3542	3@00 DB1832D@183 43131	39,134
3542	3@14 C140F4@183 3131	20,347
3542	3@44 5B07C1@183 3131	15,926
4328	3@1C 42B140@183 3131	31,174
4328	3@00 DB1832D@183 43131	26,174
4328	3@1C D06177F@183 3131	19,843
4328	3@D0 9357751@183 3131	18,165
328	3@1C DBCDA9B@18 43131	16,240
2123	3@FA 1B3D45@183 31076	56,619

如何从日志得到图表

```
68  0|||||||||||||||||
69  15:59:06.126 功能请求 IP:172.18.9.8 MAC:70F395155ADB 线程:00000BD0 通道ID:1 事务ID:14
    请求:(0-140)获取帐号状态标志(*) 营业部:(8070)深圳深南中路证券营业部
70  18798721|************|85807073|||7||36||||1838044403901392|85807073|6VYAW3X8|||
71  15:59:06.141 成功处理 IP:172.18.9.8 MAC:70F395155ADB 线程:00000BD0 通道ID:1 事务ID:14
    请求:(0-140)获取帐号状态标志(*) 营业部:(8070)深圳深南中路证券营业部 耗时A:15 耗时B:0 排队:0
72  0||1|||
73  1|||||||||||||||||
74  15:59:09.813 功能请求 IP:172.18.9.8 MAC:70F395155ADB 线程:00000CB4 通道ID:1 事务ID:15
    请求:(0-1114)股份查询(*) 营业部:(8070)深圳深南中路证券营业部
75  18798721|************|85807073|0|0123492912|7|P|||||||1838044403901392|85807073|6VYAW3X8|||
76  15:59:09.844 成功处理 IP:172.18.9.8 MAC:70F395155ADB 线程:00000CB4 通道ID:1 事务ID:15
    请求:(0-1114)股份查询(*) 营业部:(8070)深圳深南中路证券营业部 耗时A:31 耗时B:0 排队:0
77  0||2|||
78  000001|平安银行|300600|300600|0.000|9.500|0.00|2840670.00|2840670.00|0.00|0|0|0|300600|0.00|0.000|
    2840670.00|0123492912|0|0|85807073|18798721|深圳A股|002600||||
79  600000|浦发银行|88666600|88666600|1.000|16.710|88666600.00|850653173744.00|850564507144.00|959284.
    00|0|0|0|88666600|88666600.00|1.000|850564507144.00|A666522139|1|1|85807073|18798721|上海A股|21865
    ||||
80  15:59:11.407 功能请求 IP:172.18.9.8 MAC:70F395155ADB 线程:00000D84 通道ID:1 事务ID:16
    请求:(0-102)查询行情(*) 营业部:(8070)深圳深南中路证券营业部
81  18798721|************|85807073|||7||600036||||1838044403901392|85807073|6VYAW3X8|||
82  15:59:11.422 成功处理 IP:172.18.9.8 M
    请求:(0-102)查询行情(*) 营业部:(8070)
83  0||1|||
84  600036|招商银行|0.00|0.00|0.00|0.00|0
    0|0|0|0|1|100|0.01|0.01|1|0|255||
85  15:59:11.438 功能请求 IP:172.18.9.8 M
```

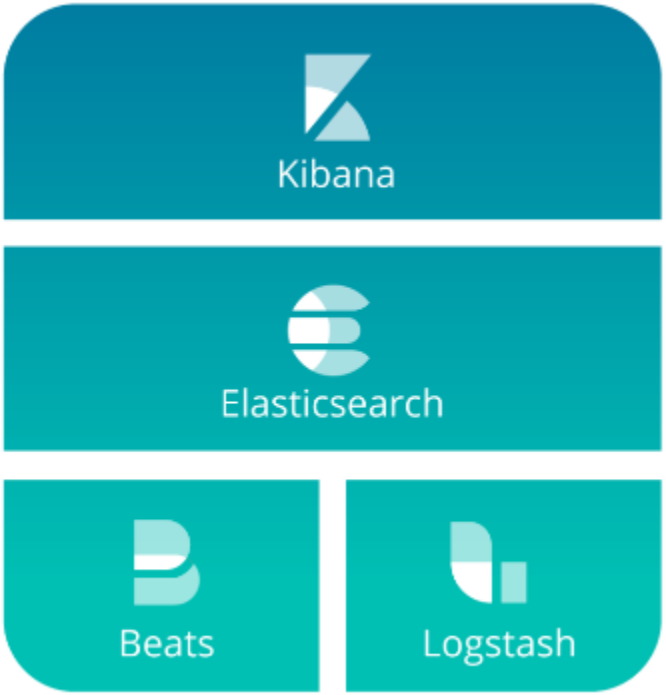
Normal text file | length : 43,231 | lines : 351 | Ln



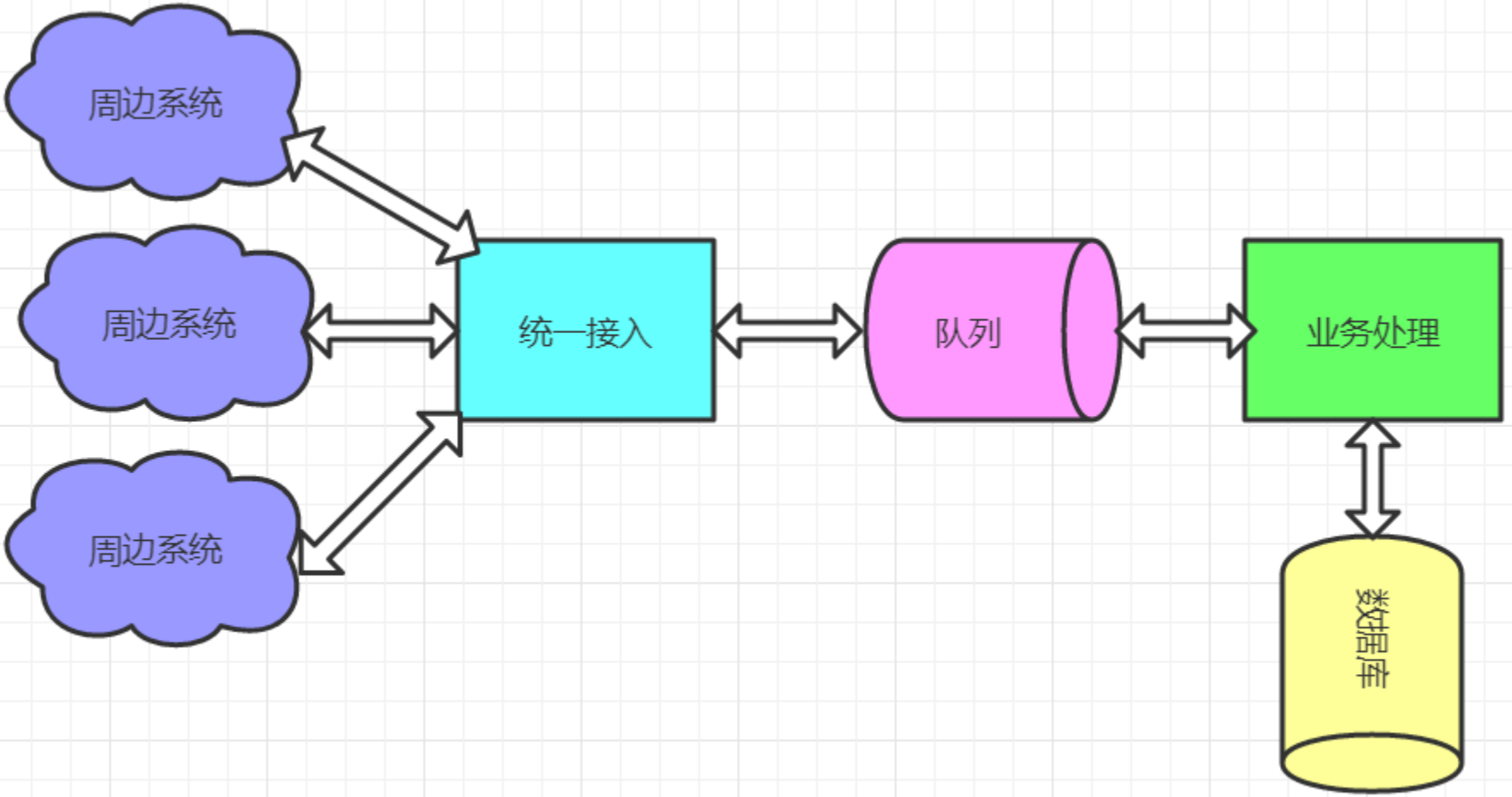
ELK提供全套解决方案

Elastic Stack

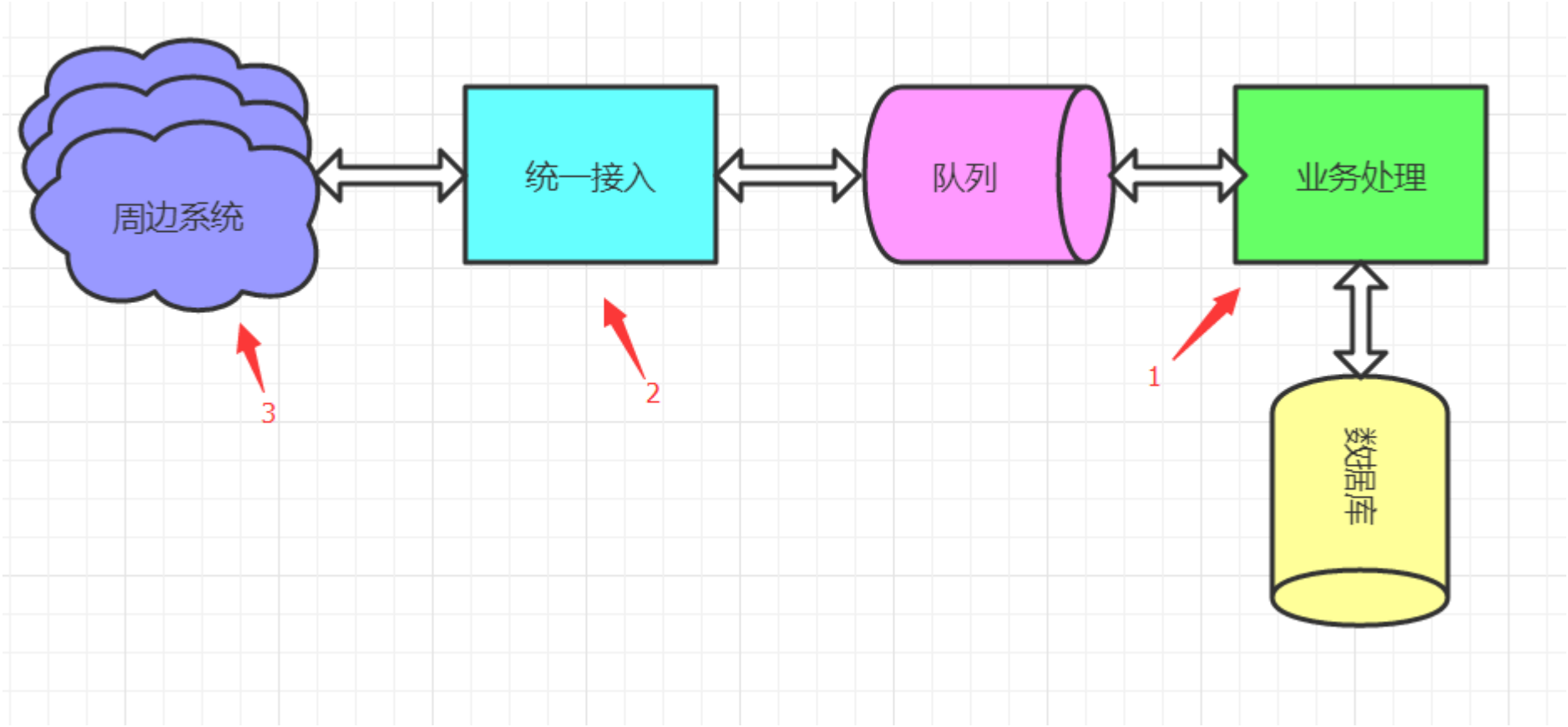
100% open source
No enterprise edition



业务系统架构简图



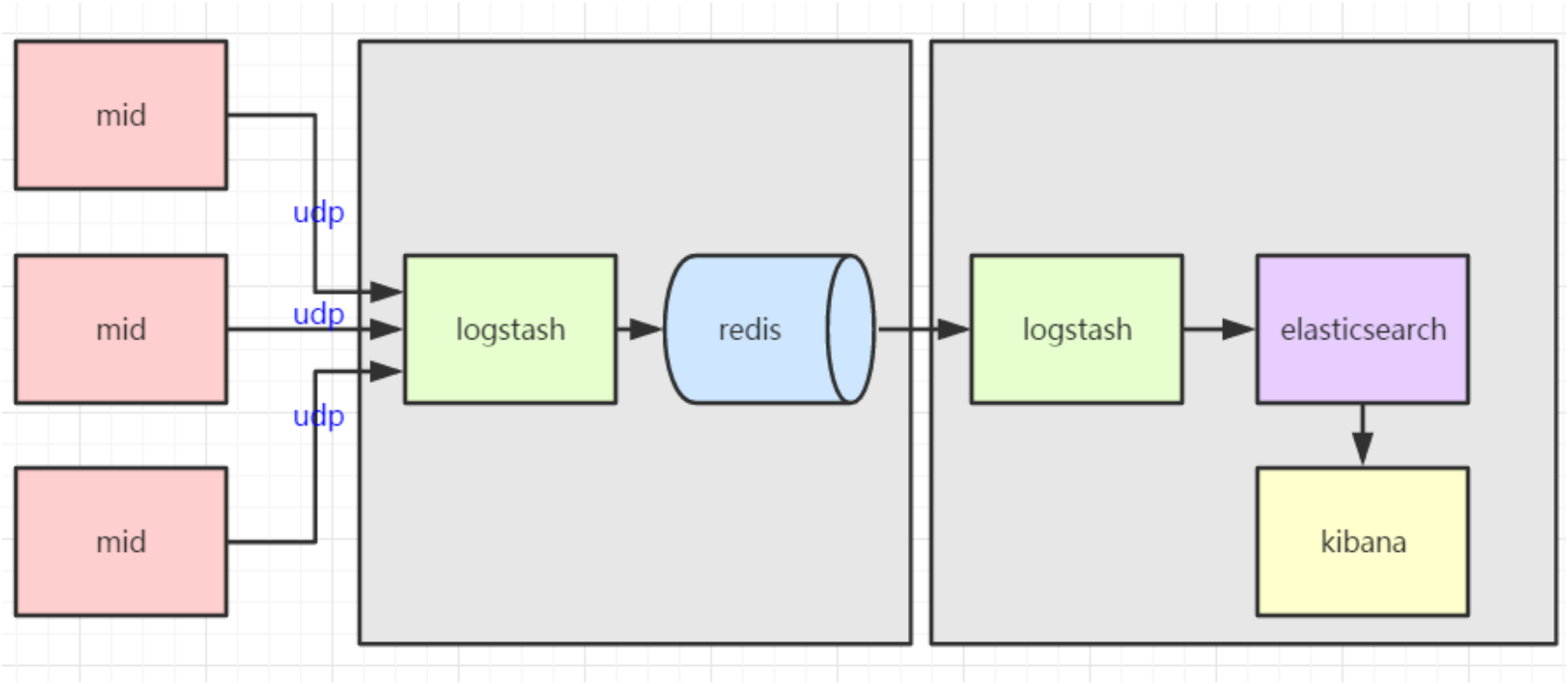
三大类业务系统日志



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
- }
- ……
- }

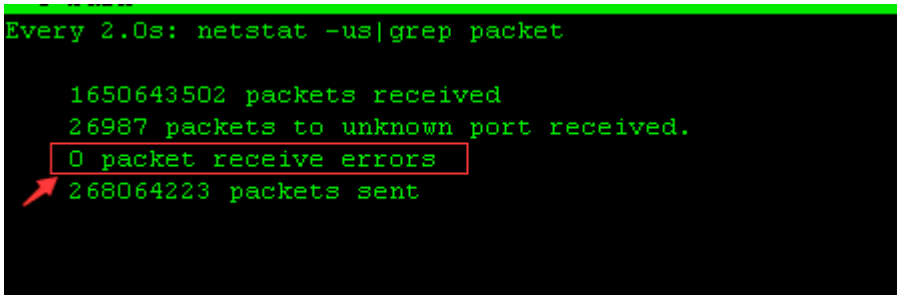
cat /etc/sysctl.conf

- # 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

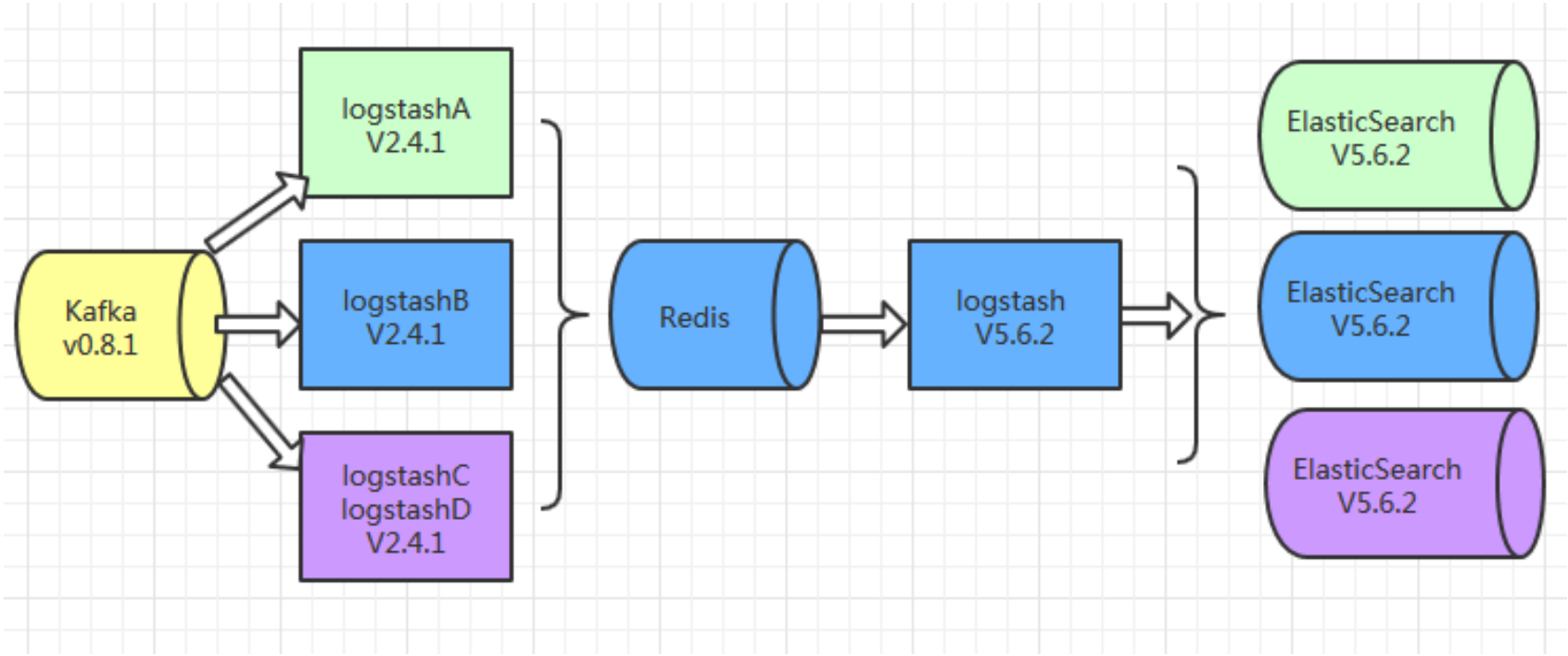
- watch “netstat -us|grep packet”



- 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


logstashA
V2.4.1
Kafka
v0.8.1
logstashB
V2.4.1
logstashC
logstashD
V2.4.1
Redis
logstash
V5.6.2
ElasticSearch
V5.6.2
ElasticSearch
V5.6.2
ElasticSearch
V5.6.2

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 => "[redacted]"
    topic_id => "jzjy"
    type => "jzjybp"
    group_id => "logstash"
    consumer_id => "O1220A"
    consumer_threads => 2
    # auto_offset_reset => "smallest"
    # reset_beginning => true
    codec => json
```

```
output {
  if [type] == "jzjybp" {
    redis {
      host => "i[redacted]: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 [redacted] --group logstash

Group           Topic                          Pid Offset          logSize         Lag             Owner
SLF4J: Failed to load class "org.slf4j.impl.StaticLoggerBinder".
SLF4J: Defaulting to no-operation (NOP) logger implementation
SLF4J: See http://www.slf4j.org/codes.html#StaticLoggerBinder for further details.
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

elastic 中文社区

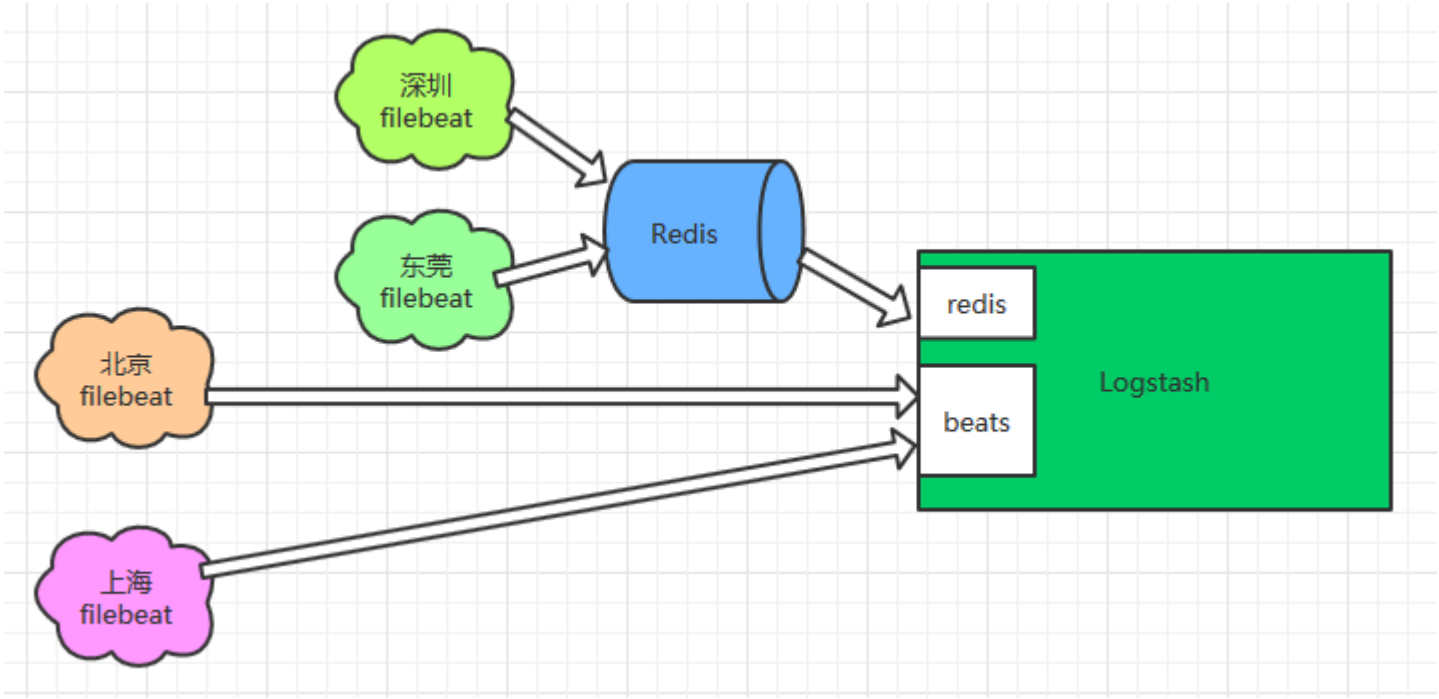
IT大咖说 知识共享平台

Logstash v5.6读取后写入ES

```
# read from redis data wroted 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


深圳
filebeat
东莞
filebeat
北京
filebeat
上海
filebeat
Redis
redis
beats
Logstash

目前集群规模

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

应用之一：排查问题

某客户端输入字段溢出bug

t	message	14:53:55.442 功能请求 IP:27.153.30 MAC:001E90 OF 线程:00000B5C 通道ID:782 事务ID:948172 请求: 股票委托(*) 营业部:(8055)晋江崇德路证券营业部 25520255|**********|22851045|0|0163532757|7|0|||002222 14 336|0||||||||||1||||||||||||||||||||20255 039|22 045|WD-W 480|||
t	mmbz	买
t	reqstr	(0-202)普通股票委托(*)
t	source	D:\tdx\tdxtc50\log\20170320.log
t	swid	948172
t	tags	beats_input_codec_plain_applied
t	tdid	782
t	type	tdxtc50
t	wtdm	002222
t	wtfs	0
#	wtje	-24,585,442,363.453
#	wtjg	16.9
t	wtother	||||||2025584 98039|2 45|WD-WC 2480|||
t	wtqd	7
#	wtsl	-1,454,759,936
t	xiancheng	00000B5C
t	yybid	8055
t	yybname	晋江崇德路证券营业部

2017-3-21 13:58:22

恩 是的

9:31:12

冷静燃烧 2017/3/21 9:31:12

有没可能 绕过检查

冷静燃烧 2017/3/21 9:31:20

比如闪电下单这种地方

13:55:35

2017/3/21 13:55:35

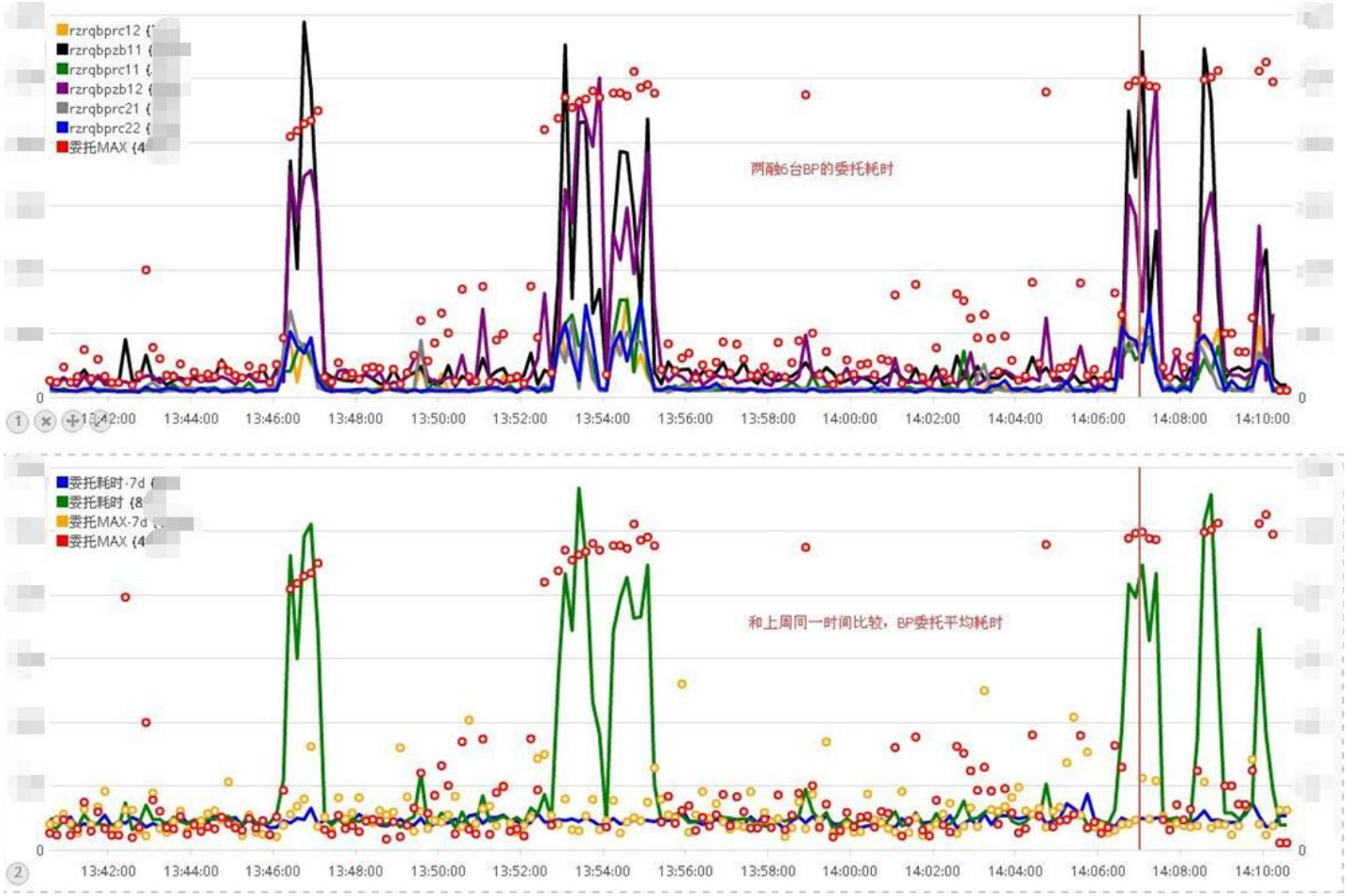
是的 有一个界面没限制 溢出了

t	message	14:53:55.473 调用失败 IP:27.153.30.168 MAC:001E90EFEEBF 线程:00000B5C 通道ID:782 事务ID:948172 请: 股票委托(*) 营业部:(8055)晋江崇德路证券营业部 耗时A:31 耗时B:0 排队:0 -1|(-121)网关:SQLNumResultCols E
t	msg	(-121)网关:SQLNumResultCols Error
#	pdtime	0
t	reqstr	(0-202)普通股票委托(*)
t	source	D:\tdx\tdxtc50\log\20170320.log
t	swid	948172

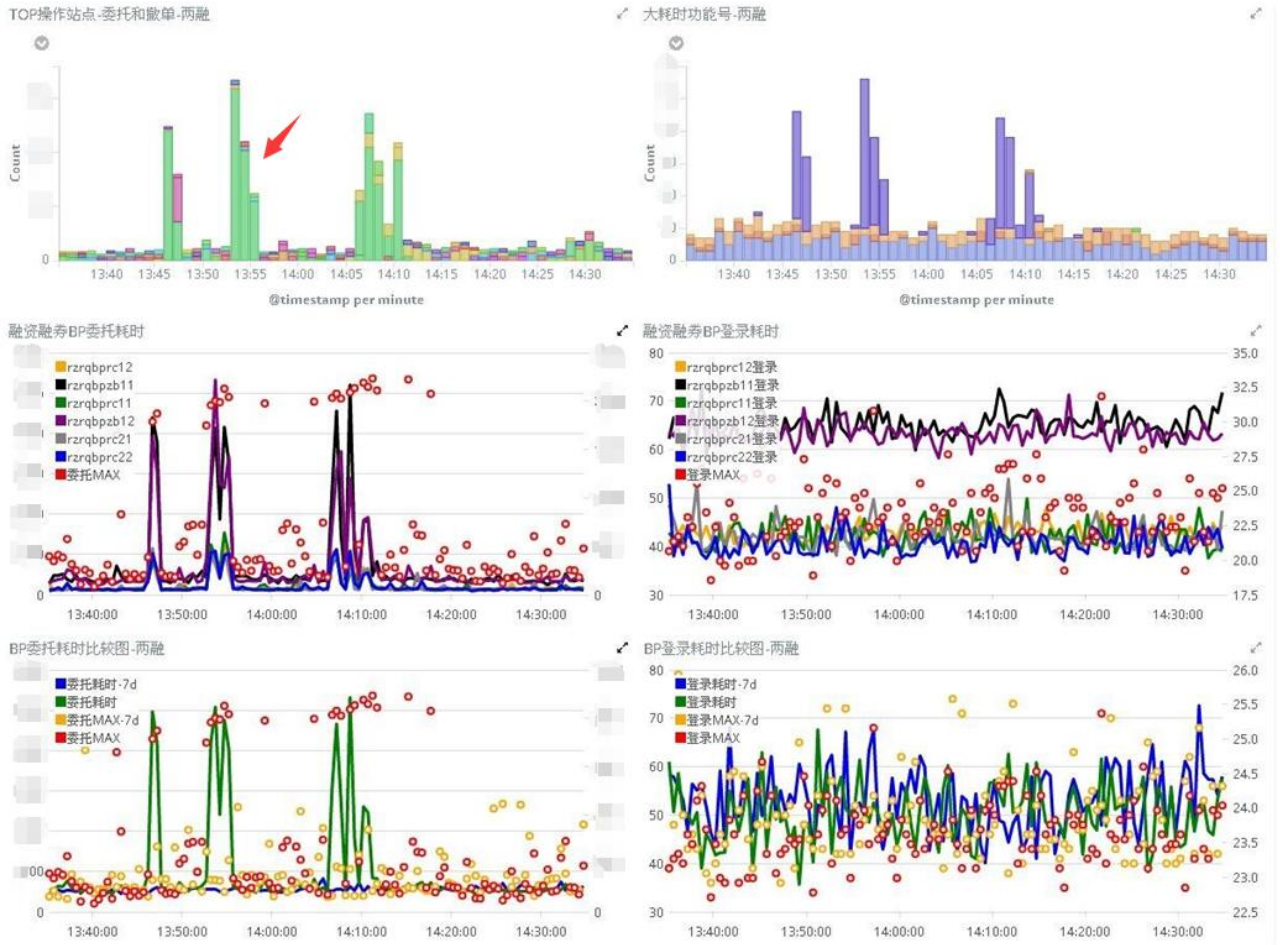
无用功能号调用

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[[redacted]]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


rzrqbprc12
rzrqbpzb11
rzrqbprc11
rzrqbpzb12
rzrqbprc21
rzrqbprc22
委托MAX
两融6台BP的委托耗时
13:42:00
13:44:00
13:46:00
13:48:00
13:50:00
13:52:00
13:54:00
13:56:00
13:58:00
14:00:00
14:02:00
14:04:00
14:06:00
14:08:00
14:10:00
委托耗时-7d
委托耗时
委托MAX-7d
委托MAX
和上周同一时间比较，BP委托平均耗时

问题原因一目了然

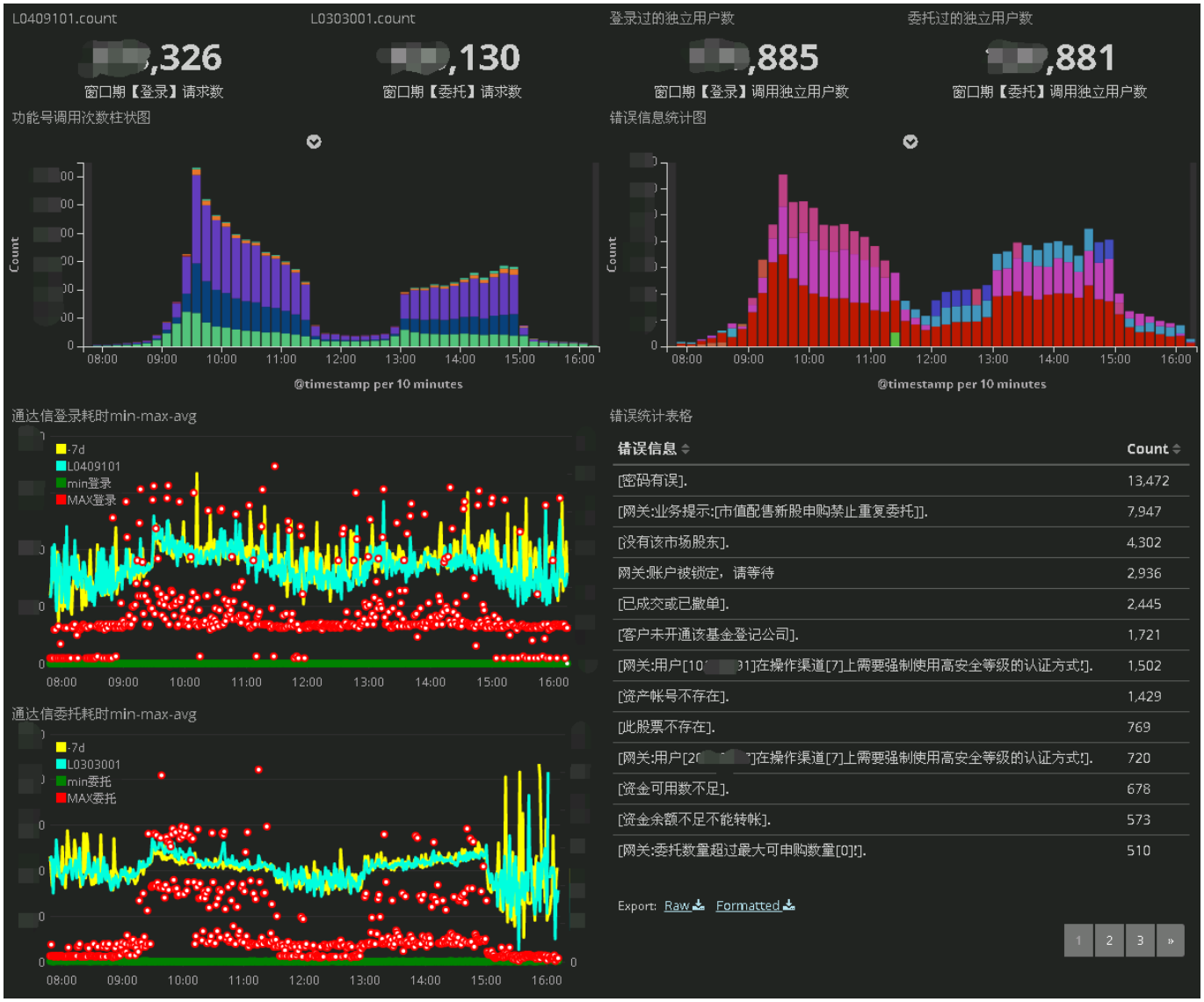

TOP操作站点-委托和撤单-两融
Count
@timestamp per minute
大耗时功能号-两融
Count
@timestamp per minute
融资融券BP委托耗时
rzrqbprc12
rzrqbpzb11
rzrqbprc11
rzrqbpzb12
rzrqbprc21
rzrqbprc22
委托MAX
融资融券BP登录耗时
rzrqbprc12登录
rzrqbpzb11登录
rzrqbprc11登录
rzrqbpzb12登录
rzrqbprc21登录
rzrqbprc22登录
登录MAX
BP委托耗时比较图-两融
委托耗时-7d
委托耗时
委托MAX-7d
委托MAX
BP登录耗时比较图-两融
登录耗时-7d
登录耗时
登录MAX-7d
登录MAX

应用之二：业务监控

业务监控维度

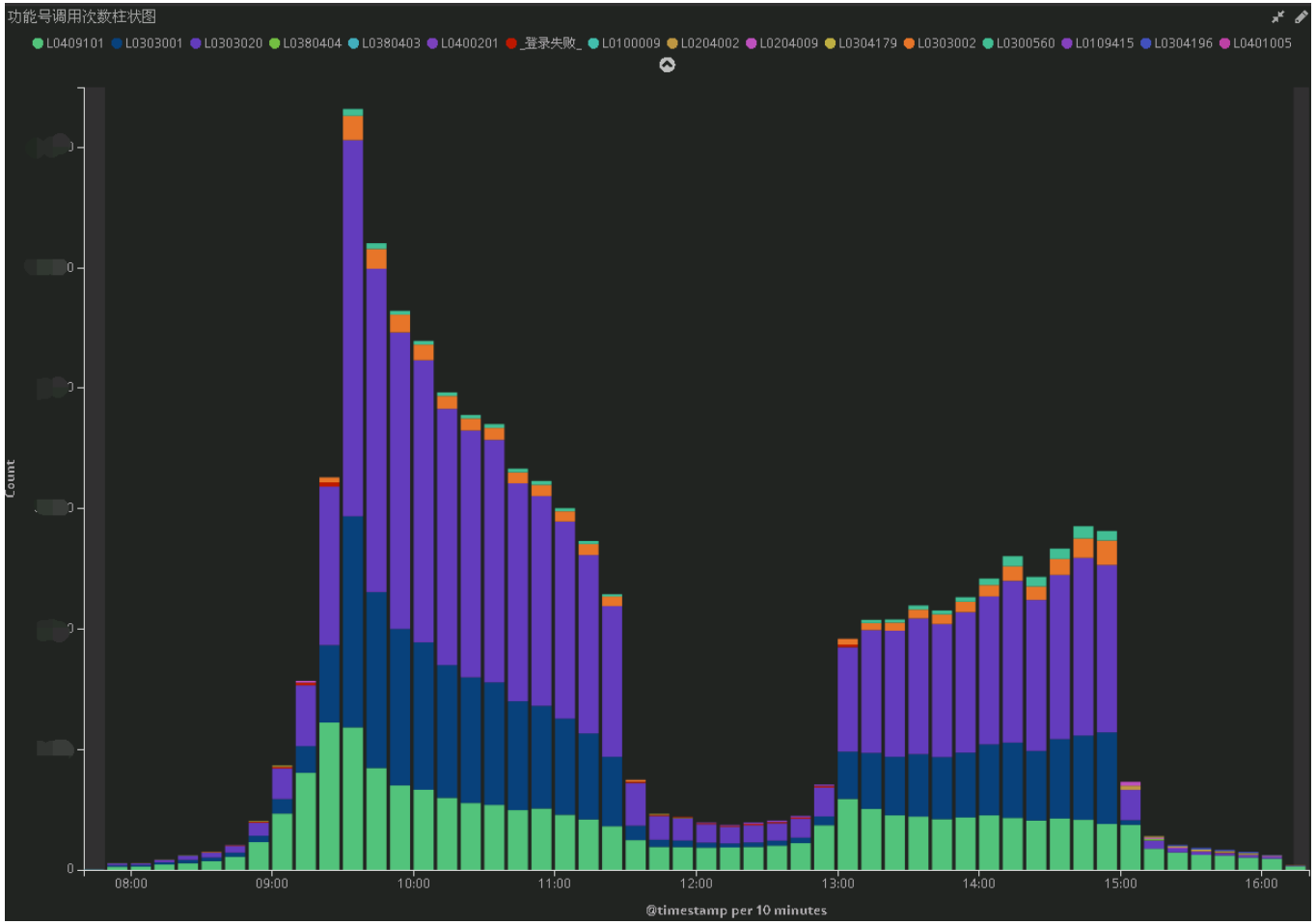
① 功能号
② 客户号
③ 错误信息
④ 响应时间
⑤ 客户IP地理信息
⑥ 其他，如客户端版本

某周边业务系统运行概览

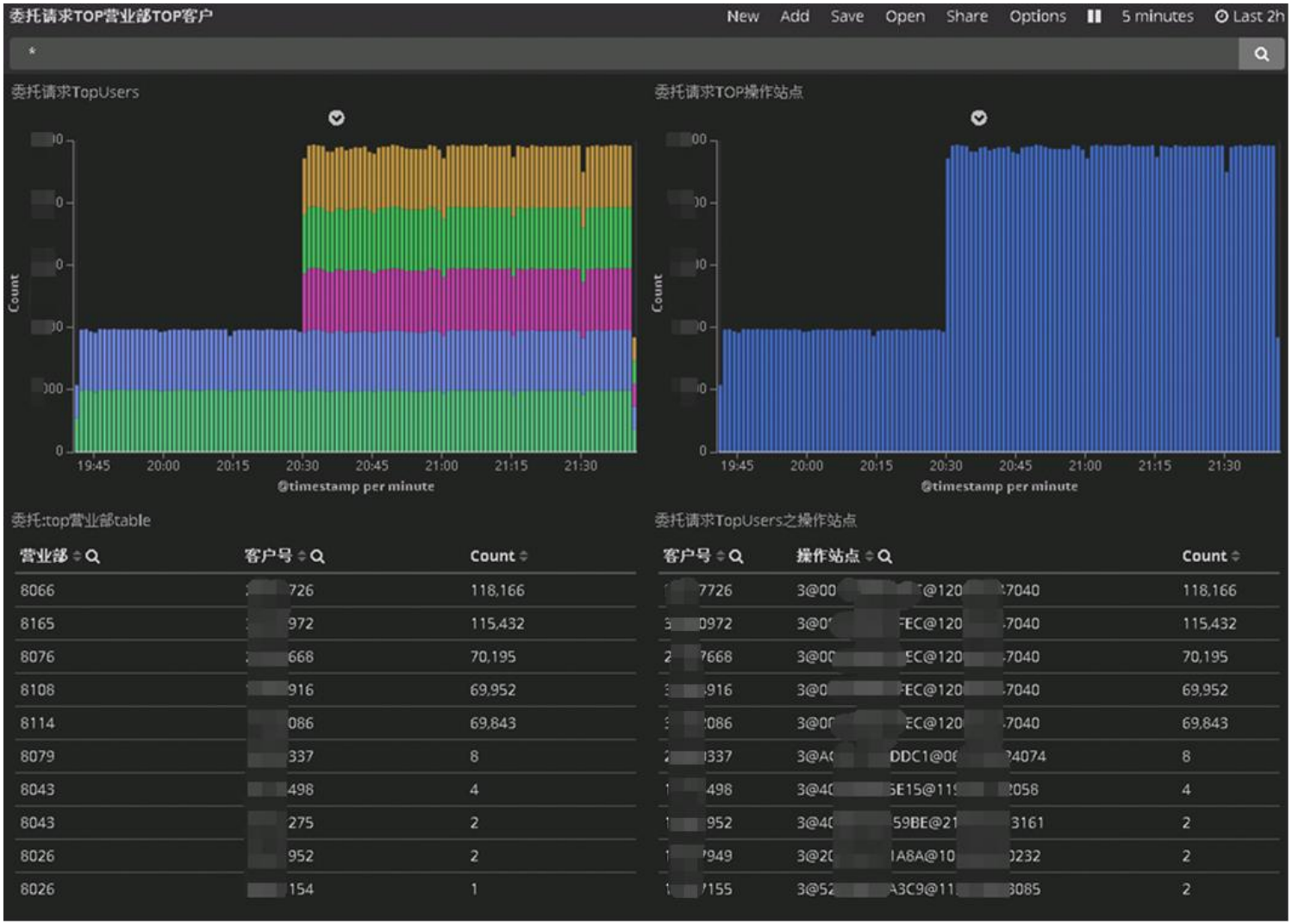


错误信息	Count
[密码有误].	13,472
[网关:业务提示:[市值配售新股申购禁止重复委托]].	7,947
[没有该市场股东].	4,302
网关:账户被锁定，请等待	2,936
[已成交或已撤单].	2,445
[客户未开通该基金登记公司].	1,721
[网关:用户[10 31]在操作渠道[7]上需要强制使用高安全等级的认证方式!].	1,502
[资产帐号不存在].	1,429
[此股票不存在].	769
[网关:用户[2]在操作渠道[7]上需要强制使用高安全等级的认证方式!].	720
[资金可用数不足].	678
[资金余额不足不能转帐].	573
[网关:委托数量超过最大可申购数量[0]!].	510

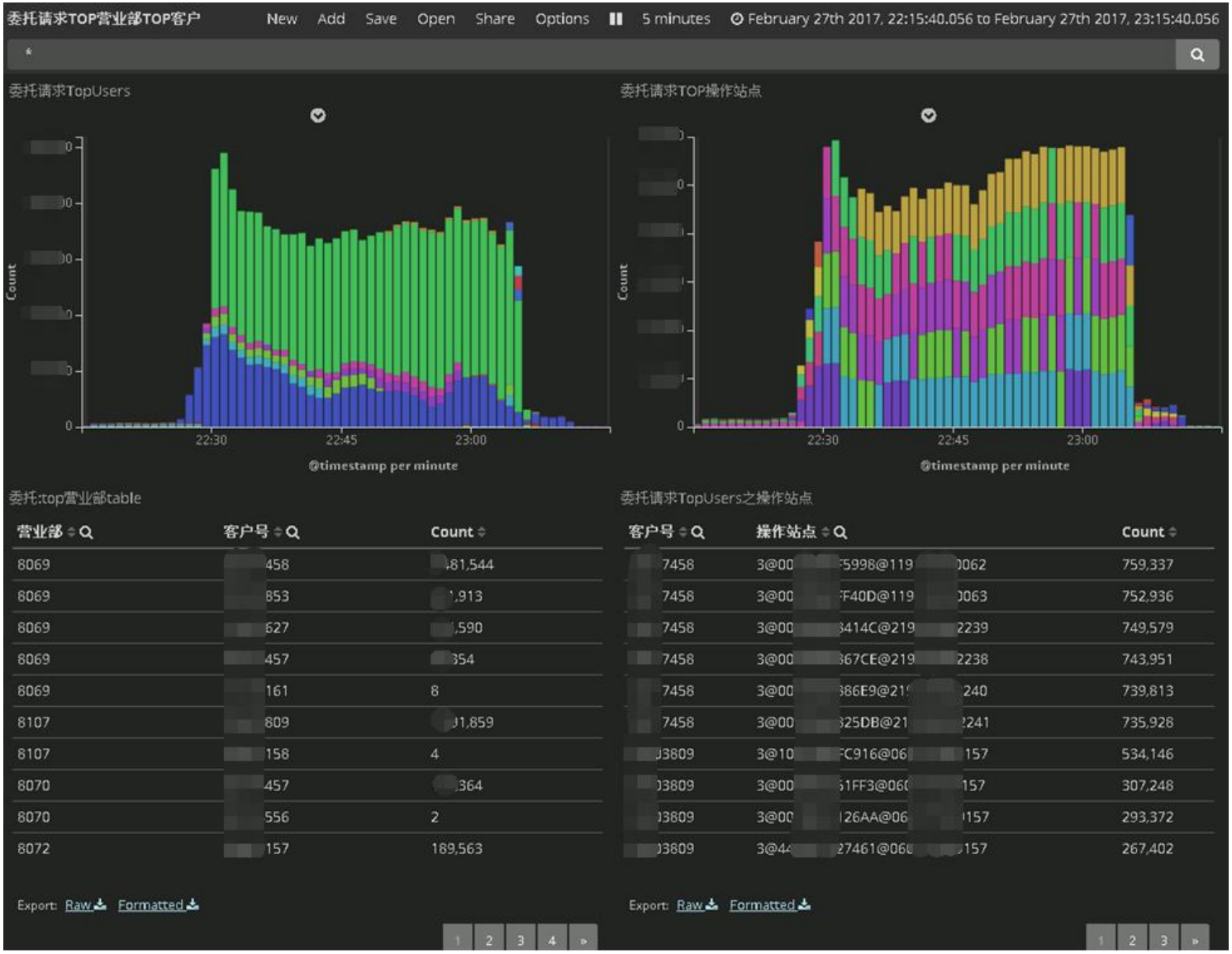
功能号调用


功能号调用次数柱状图
L0409101 L0303001 L0303020 L0380404 L0380403 L0400201 _登录失败_ L0100009 L0204002 L0204009 L0304179 L0303002 L0300560 L0109415 L0304196 L0401005
Count
0
08:00
09:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00
@timestamp per 10 minutes

异常客户行为监控

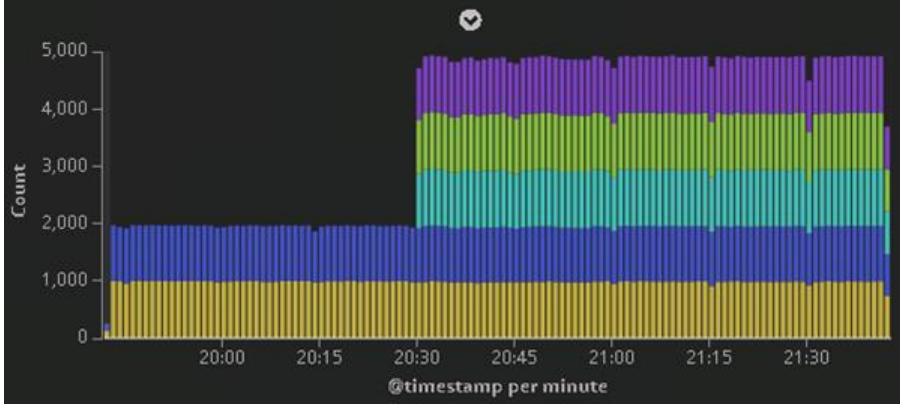

委托请求TOP营业部TOP客户
New
Add
Save
Open
Share
Options
5 minutes
Last 2h
委托请求TopUsers
Count
19:45
20:00
20:15
20:30
20:45
21:00
21:15
21:30
@timestamp per minute
委托请求TOP操作站点
Count
19:45
20:00
20:15
20:30
20:45
21:00
21:15
21:30
@timestamp per minute
委托:top营业部table
营业部
客户号
Count
8066 726 118,166
8165 972 115,432
8076 668 70,195
8108 916 69,952
8114 086 69,843
8079 337 8
8043 498 4
8043 275 2
8026 952 2
8026 154 1
委托请求TopUsers之操作站点
客户号
操作站点
Count
7726 3@00 @120 7040 118,166
0972 3@0 EC@120 7040 115,432
7668 3@00 EC@120 7040 70,195
916 3@0 EC@120 7040 69,952
086 3@0 EC@120 7040 69,843
337 3@A DDC1@0 4074 8
498 3@40 5E15@11 2058 4
952 3@40 59BE@21 3161 2
949 3@2 1A8A@10 0232 2
7155 3@52 A3C9@11 3085 2

异常客户行为监控2

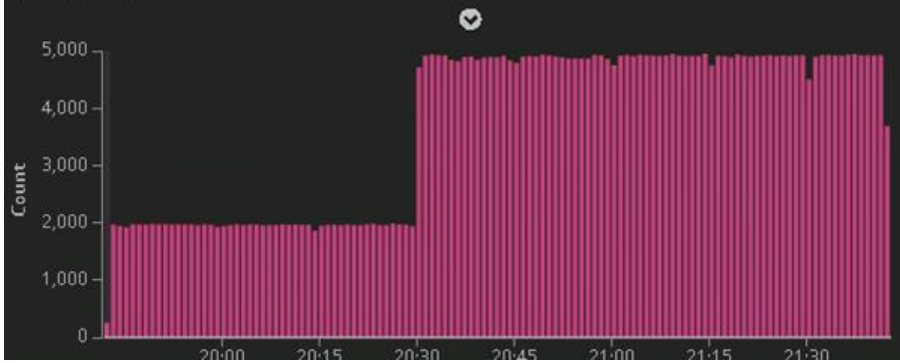

委托请求TOP营业部TOP客户
New
Add
Save
Open
Share
Options
5 minutes
February 27th 2017, 22:15:40.056 to February 27th 2017, 23:15:40.056
委托请求TopUsers
委托请求TOP操作站点
Count
22:30
22:45
23:00
@timestamp per minute
委托:top营业部table
营业部
客户号
Count
8069
8069
8069
8069
8069
8107
8107
8070
8070
8072
189,563
委托请求TopUsers之操作站点
客户号
操作站点
Count
759,337
752,936
749,579
743,951
739,813
735,928
534,146
307,248
293,372
267,402
Export: Raw
Formatted

错误信息

委托请求TopUsers



错误信息统计图



错误统计表格

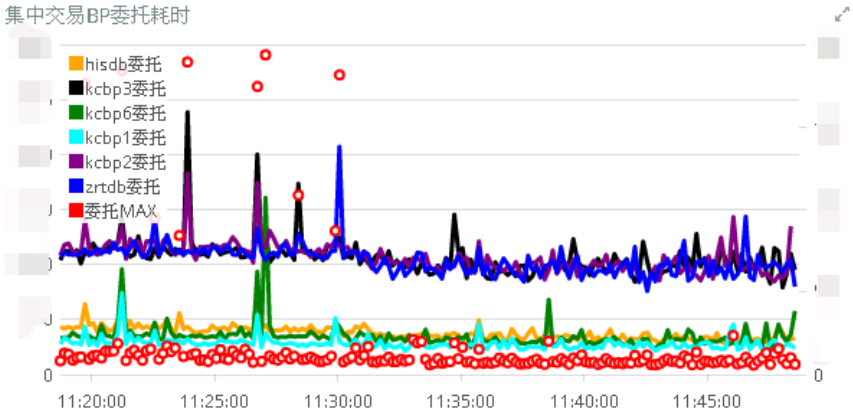
错误信息	Count
[不支持隔日委托].	447,606
[网关:业务提示:[该股票今日不支持申购]].	433
[密码有误].	297
[网关:业务提示:[此业务可执行时间段为08:30:00-16:05:00]].	69
[资产帐号不存在].	51
[股东代码不存在].	12
[网关:业务提示:[此业务可执行时间段为08:30:00-18:05:00]].	11
[客户未开通该基金登记公司].	8
[没有该市场股东].	6
[网关:业务提示:[无申购日期为20170125,缴款日期为20170203的新股或应缴款金额小于冻结金额!]].	3
[网关:资产帐户[34]不是[正常]状态].	3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

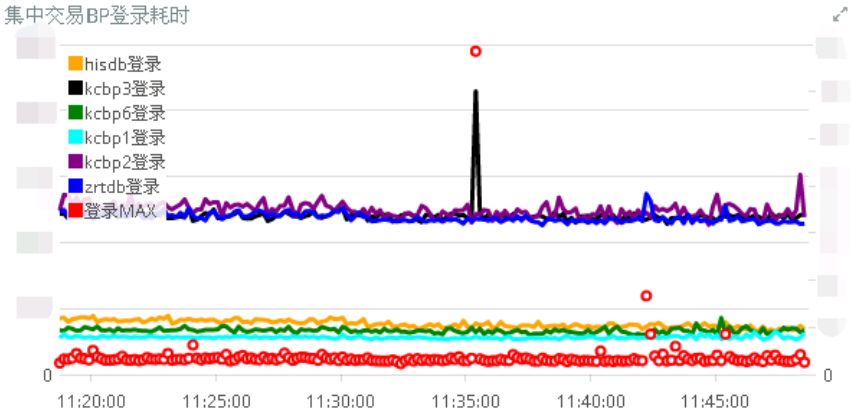
Export: Raw Formatted

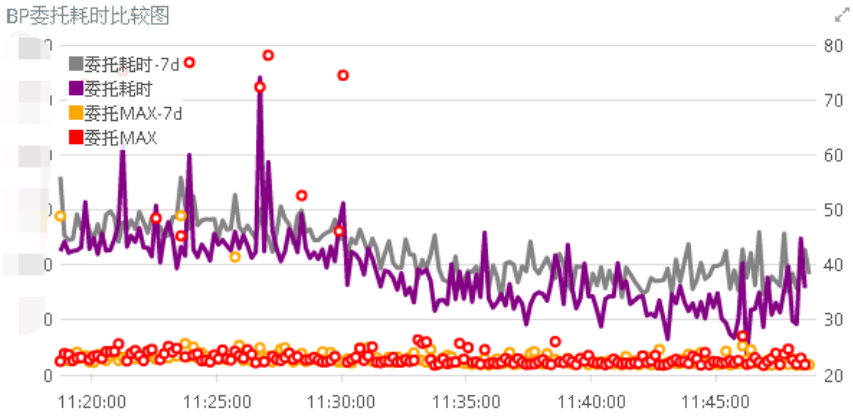
响应时间

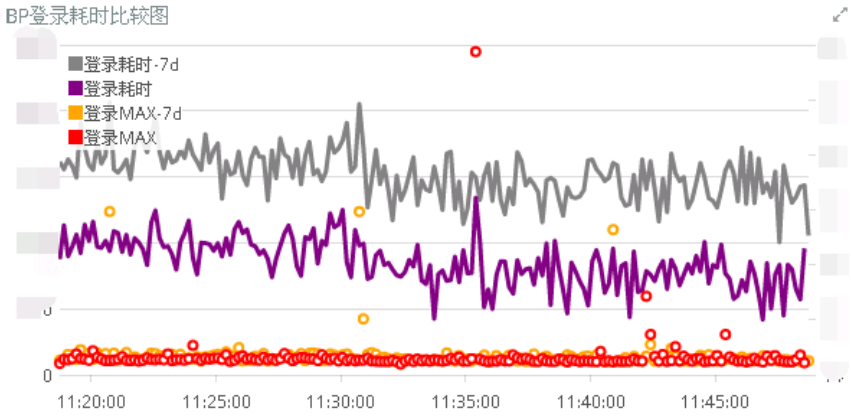

L0409101.count
,604
窗口期【登录】请求数
L0303001.count
,932
窗口期【委托】请求数
登录过的独立用户数
,115
窗口期【登录】调用独立用户户数
委托过的独立用户数
,001
窗口期【委托】调用独立用户户数
功能号调用次数柱状图
L0409101 L0303001 L0303002 _登录失败_ L0204002 L0204001 L0403001
Count
09:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00
@timestamp per 10 minutes
LbmtimeHeatmaps功能号耗时热力图
@timestamp per 10 minutes

耗时

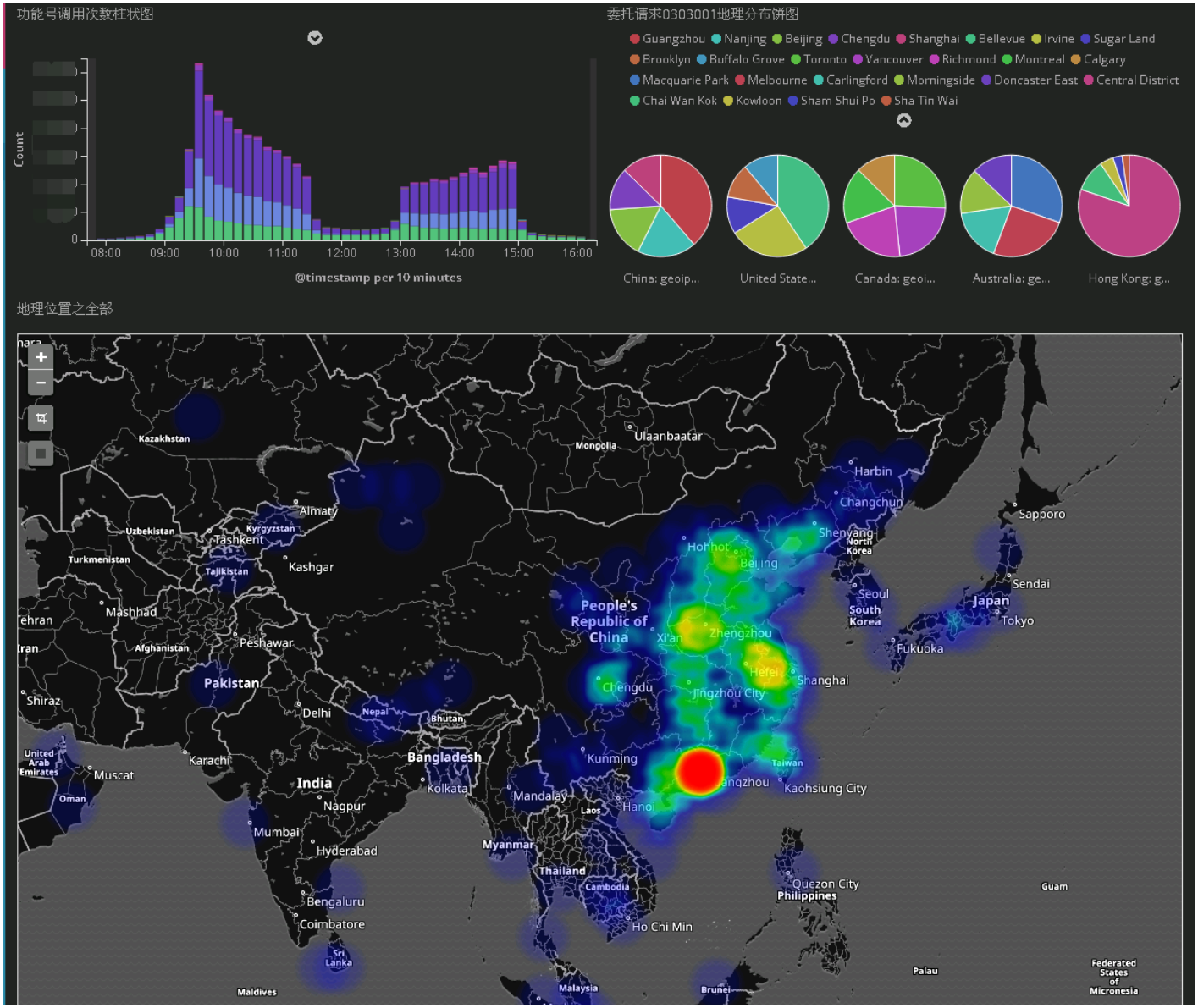

集中交易BP委托耗时
hisdb委托
kcbp3委托
kcbp6委托
kcbp1委托
kcbp2委托
zrtdb委托
委托MAX
11:20:00
11:25:00
11:30:00
11:35:00
11:40:00
11:45:00


集中交易BP登录耗时
hisdb登录
kcbp3登录
kcbp6登录
kcbp1登录
kcbp2登录
zrtdb登录
登录MAX
11:20:00
11:25:00
11:30:00
11:35:00
11:40:00
11:45:00

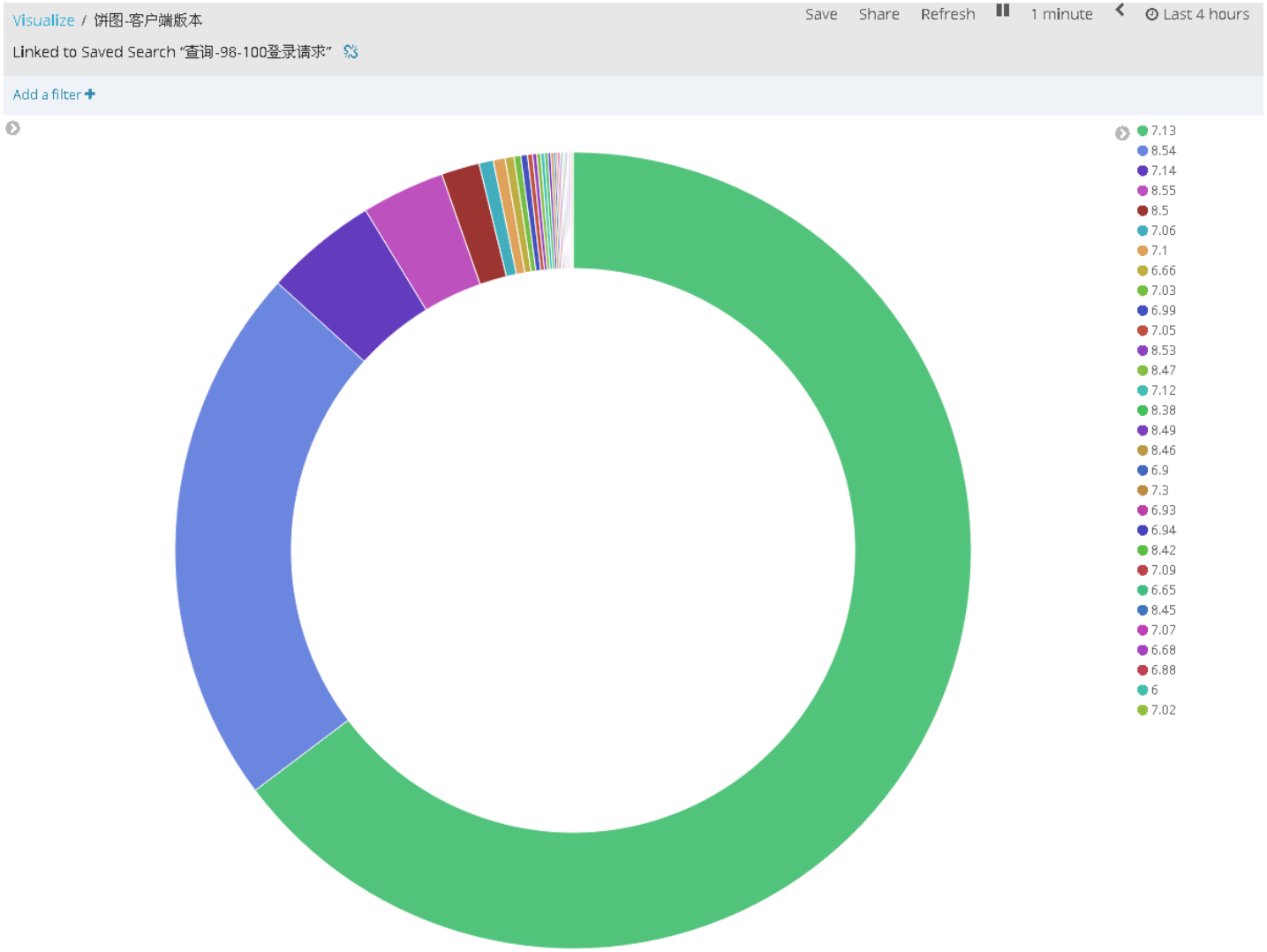

BP委托耗时比较图
委托耗时-7d
委托耗时
委托MAX-7d
委托MAX
80
70
60
50
40
30
20
11:20:00
11:25:00
11:30:00
11:35:00
11:40:00
11:45:00


BP登录耗时比较图
登录耗时-7d
登录耗时
登录MAX-7d
登录MAX
11:20:00
11:25:00
11:30:00
11:35:00
11:40:00
11:45:00

客户委托地理位置信息


功能号调用次数柱状图
Count
0
08:00
09:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00
@timestamp per 10 minutes
委托请求0303001地理分布饼图
Guangzhou
Nanjing
Beijing
Chengdu
Shanghai
Bellevue
Irvine
Sugar Land
Brooklyn
Buffalo Grove
Toronto
Vancouver
Richmond
Montreal
Calgary
Macquarie Park
Melbourne
Carlingford
Morningside
Doncaster East
Central District
Chai Wan Kok
Kowloon
Sham Shui Po
Sha Tin Wai
China: geoip...
United State...
Canada: geoi...
Australia: ge...
Hong Kong: g...
地理位置之全部
Kazakhstan
Mongolia
Ulaanbaatar
Harbin
Changchun
Sapporo
Almaty
Uzbekistan
Kyrgyzstan
Tashkent
Turkmenistan
Tajikistan
Kashgar
Hohhot
Shenyang
North Korea
Beijing
Sendai
Seoul
South Korea
Japan
Tokyo
Mashhad
People's Republic of China
Xi'an
Zhengzhou
Fukuoka
Afghanistan
Peshawar
Hefei
Shanghai
Pakistan
Chengdu
Jingzhou City
Shiraz
Delhi
Nepal
Bhutan
United Arab Emirates
Muscat
Karachi
Bangladesh
Kunming
Taiwan
India
Kaohsiung City
Oman
Kolkata
Mandalay
Laos
Hanoi
Nagpur
Mumbai
Myanmar
Hyderabad
Thailand
Cambodia
Quezon City
Philippines
Guam
Bengaluru
Coimbatore
Ho Chi Min
Sri Lanka
Palau
Federated States of Micronesia
Maldives
Malaysia
Brunei

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