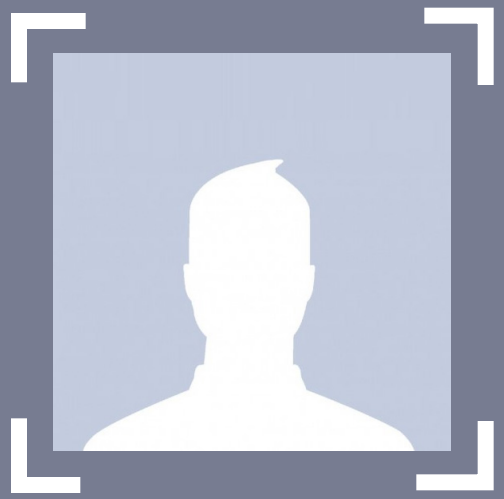
ELK在实时流量分析中的应用

Clearclouds-global.com
杨润达
Tech.lead



Tech.lead

杨润达

runda.yang@clearclouds-global.com

ELK在实时流量分析中的应用

Overview

1. 概　　述
2. 流量分析平台的比较
3. 为什么使用ES
4. 提高ES的导入速度
5. 网络数据分析
6. 网络流量的可视化
7. Kibana 插件开发
8. 功能演示
9. Questions & Answers

Thank you for being here today

流量分析的方式

overview

Netflow/Sflow

采样、精度不够
增加设备压力

数据包

粒度最细、分析全面
数据量太大

元数据

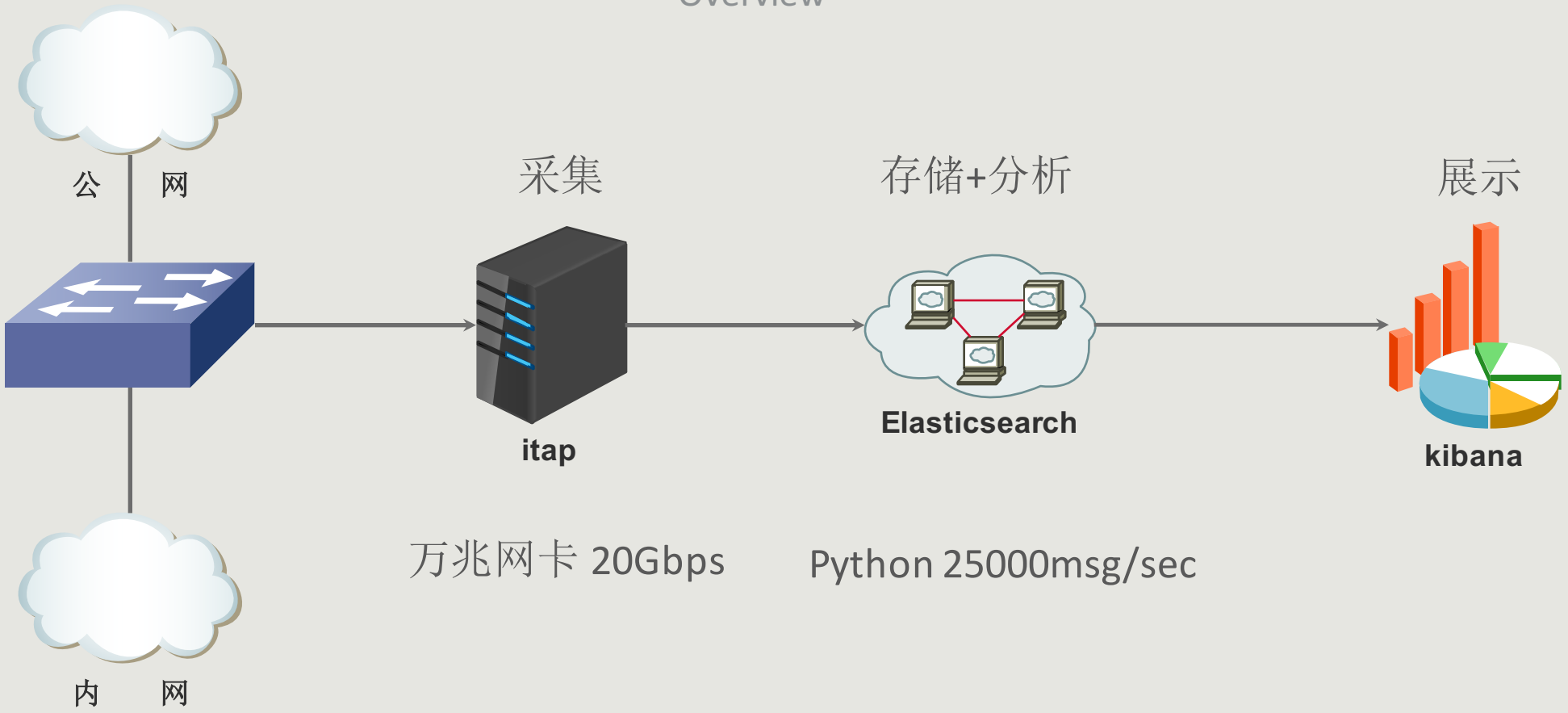
根据需求选择数据
全流量

为什么使用Elasticsearch

overview

概　述

Overview

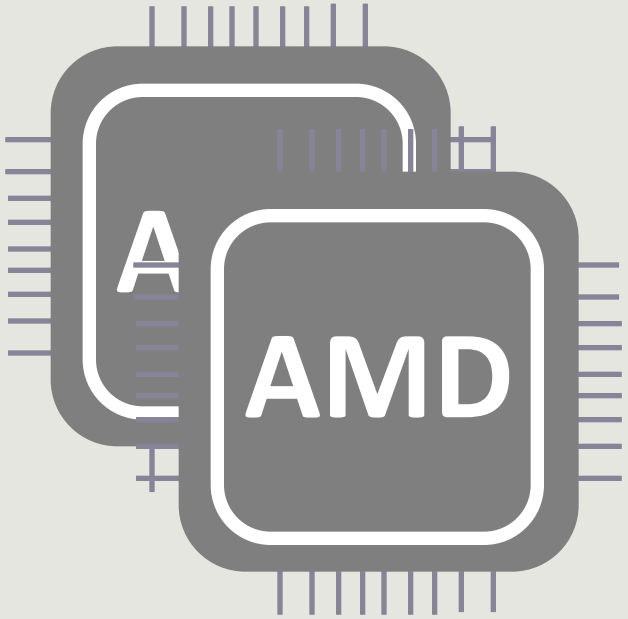


万兆网卡 20Gbps　　Python 25000msg/sec

提高数据导入的速度

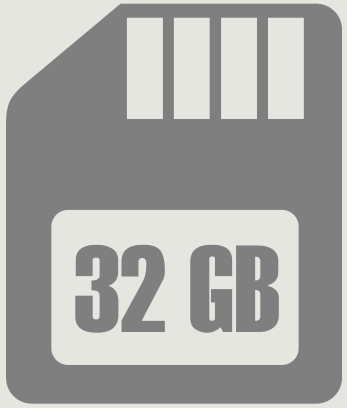
使用高性能的json库
例如python的ujson

机器配置

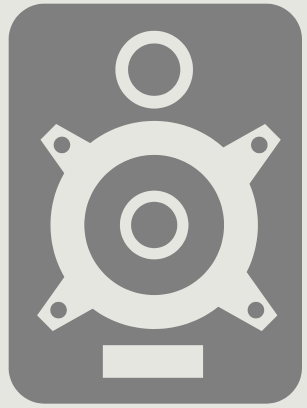


2 x AMD Opteron(tm) Processor 6172

12 cores per CPU



32GB



SATA 1TB

多进程优化方法

5个字段

100万条真实TCP数据

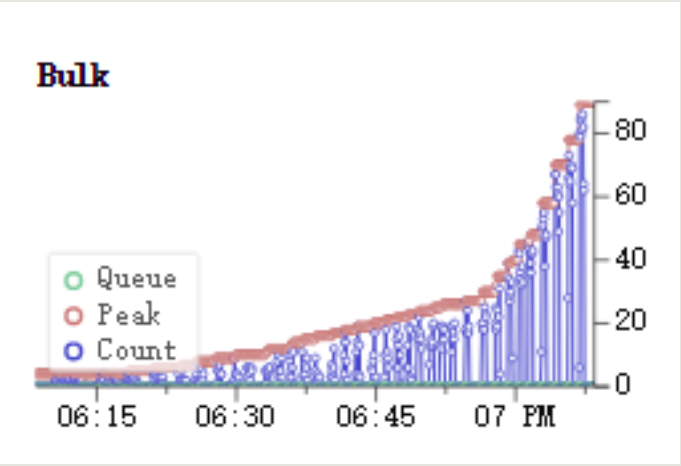
+1500~2000msg/s

+1500~2000msg/s

+1500~2000msg/s

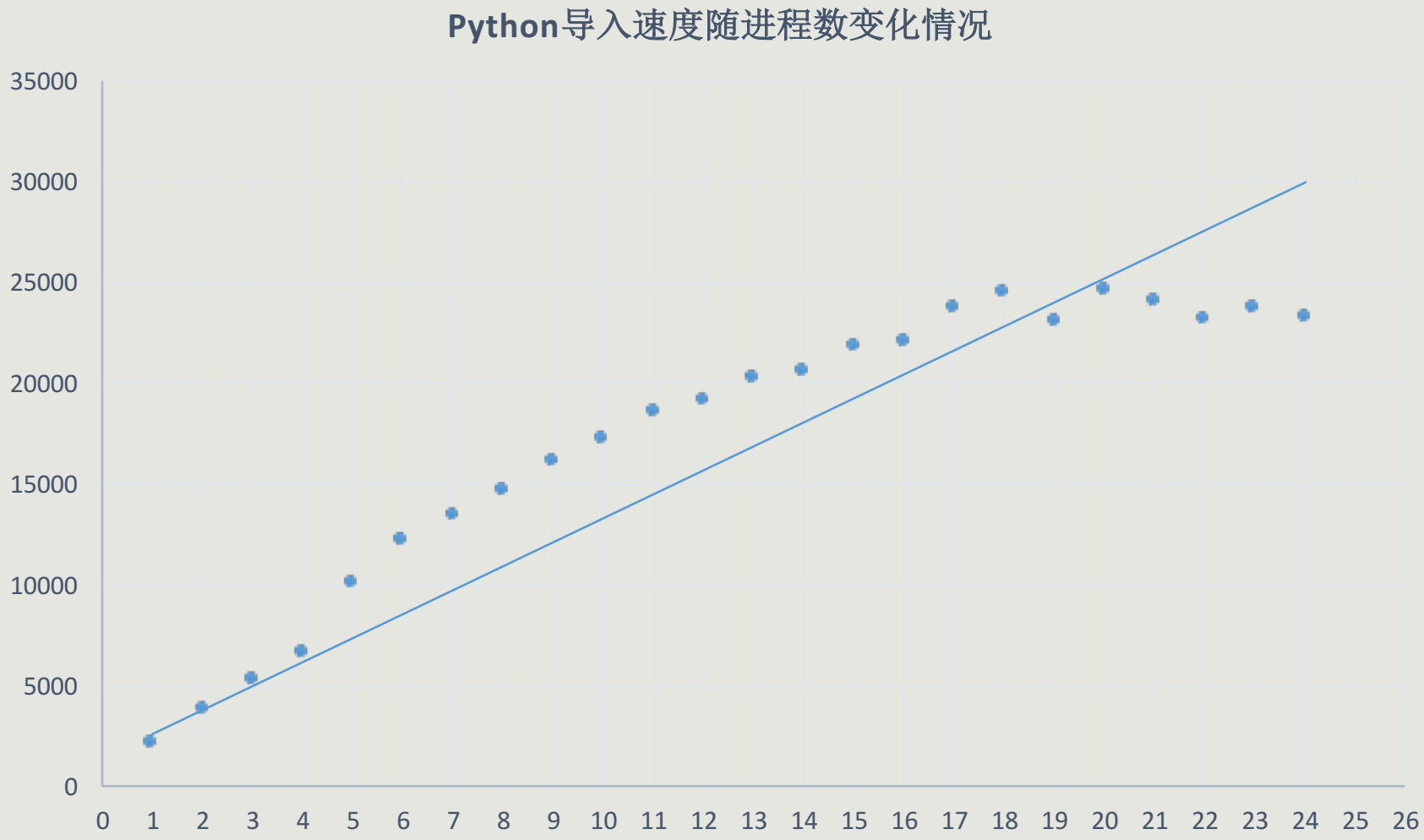
+1500~2000msg/s

多进程并行导入

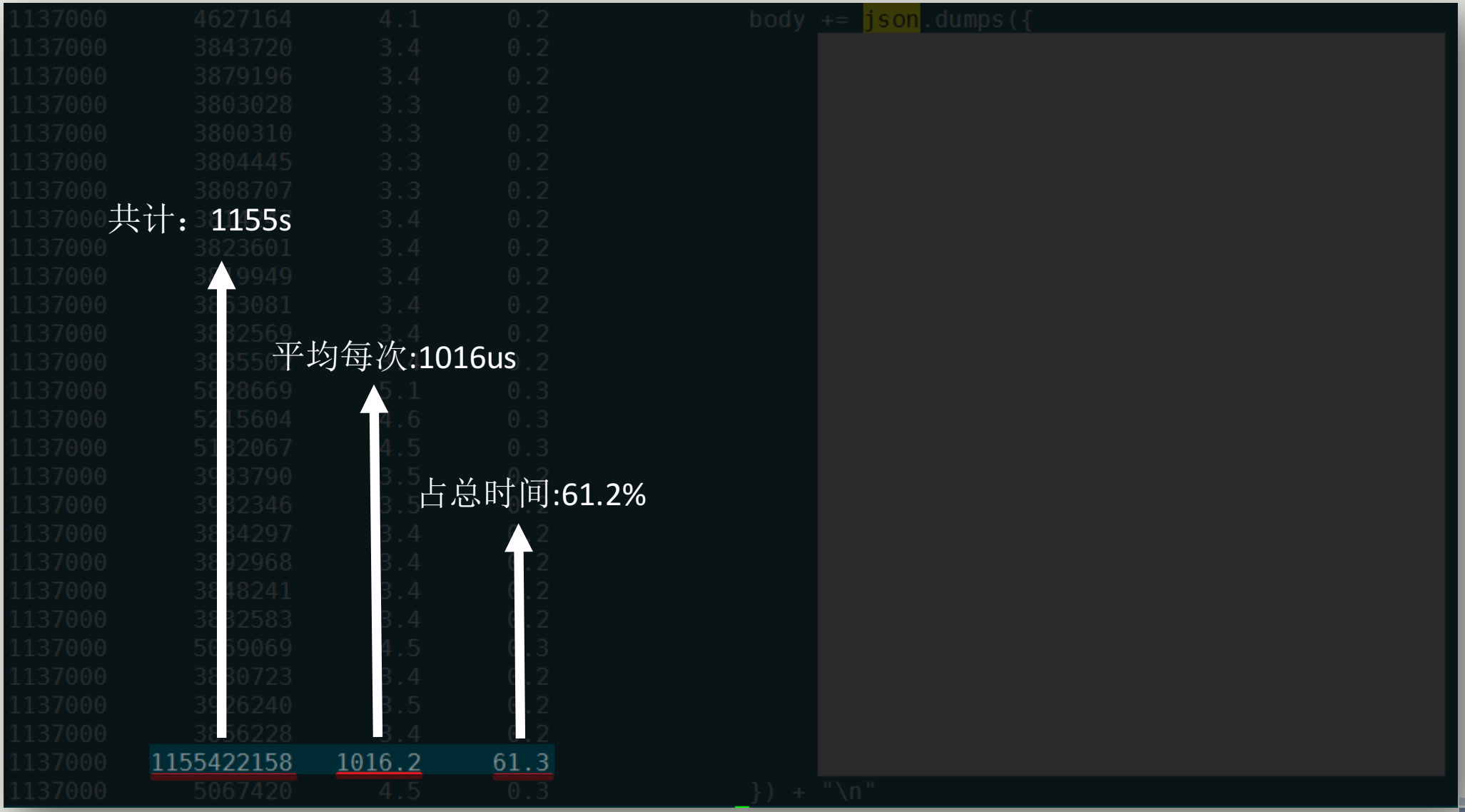


开启bulk线程池

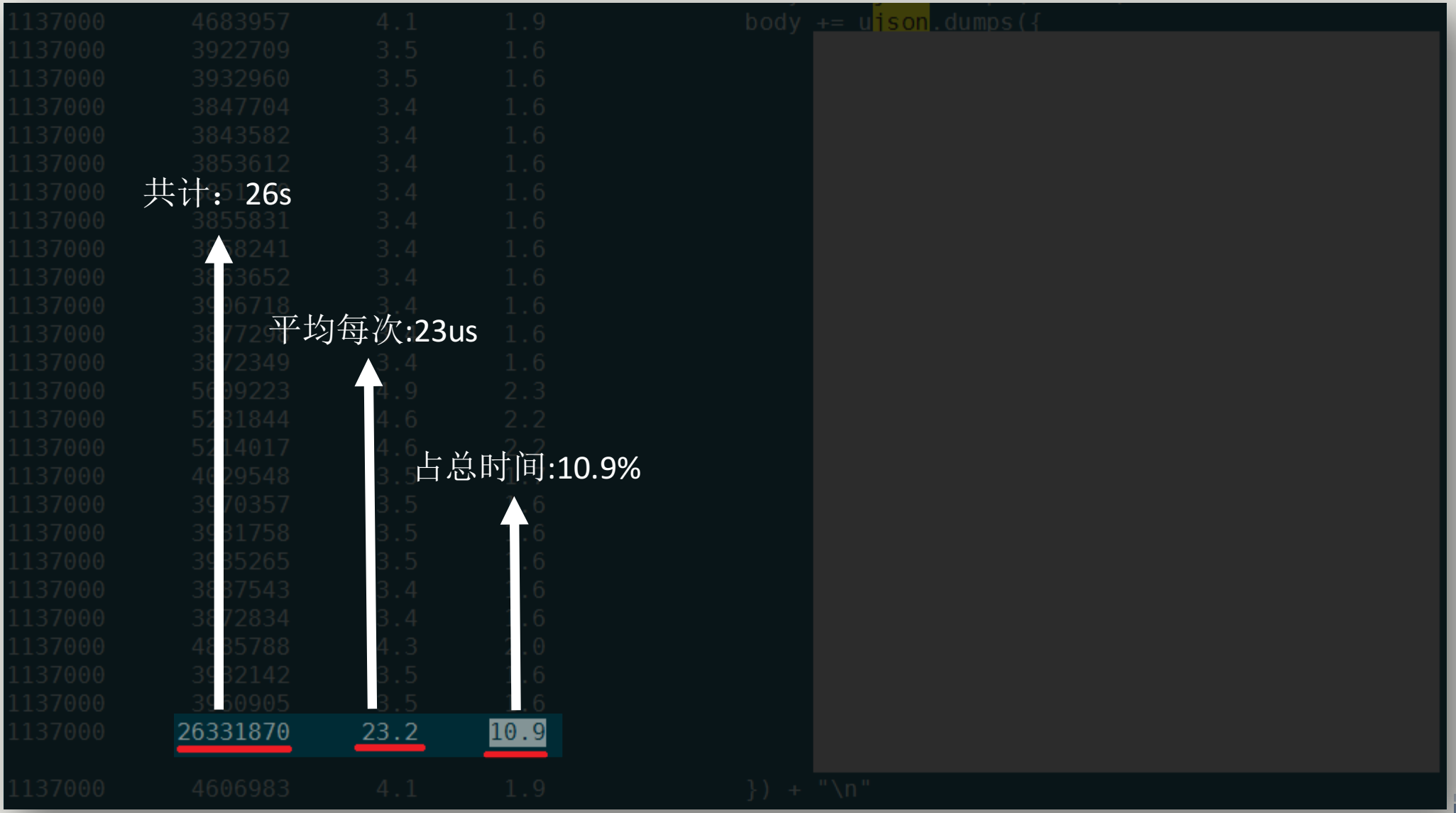
优化结果


Python导入速度随进程数变化情况
35000
30000
25000
20000
15000
10000
5000
0
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26

json优化前


body += json.dumps({
共计：1155s
平均每次:1016us
占总时间:61.2%
1155422158 1016.2 61.3

使用uJson



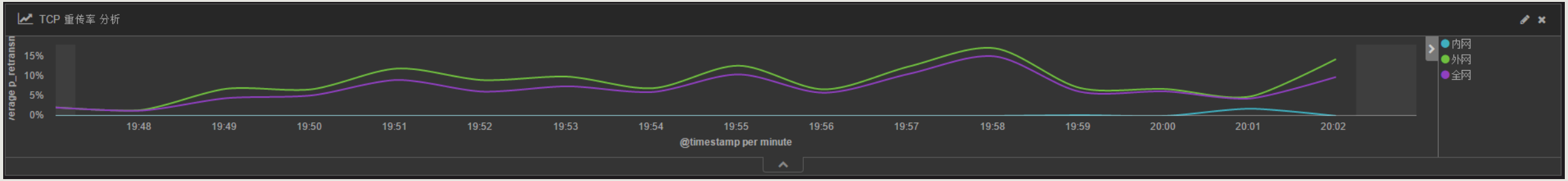
IP段聚合分析

内网

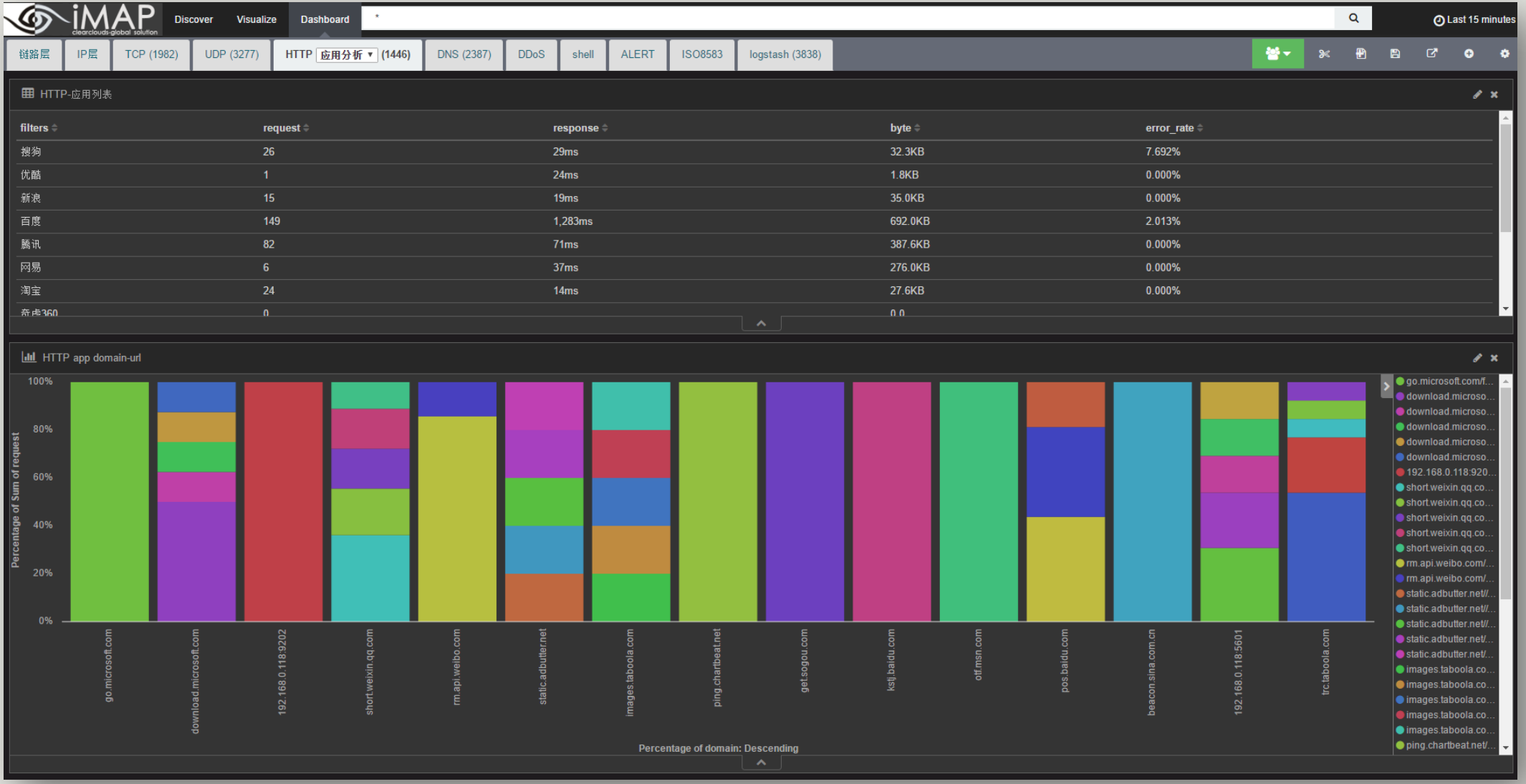
sip: [192.168.0.0 TO 192.168.1.255] AND
dip: [192.168.0.0 TO 192.168.1.255]

外网

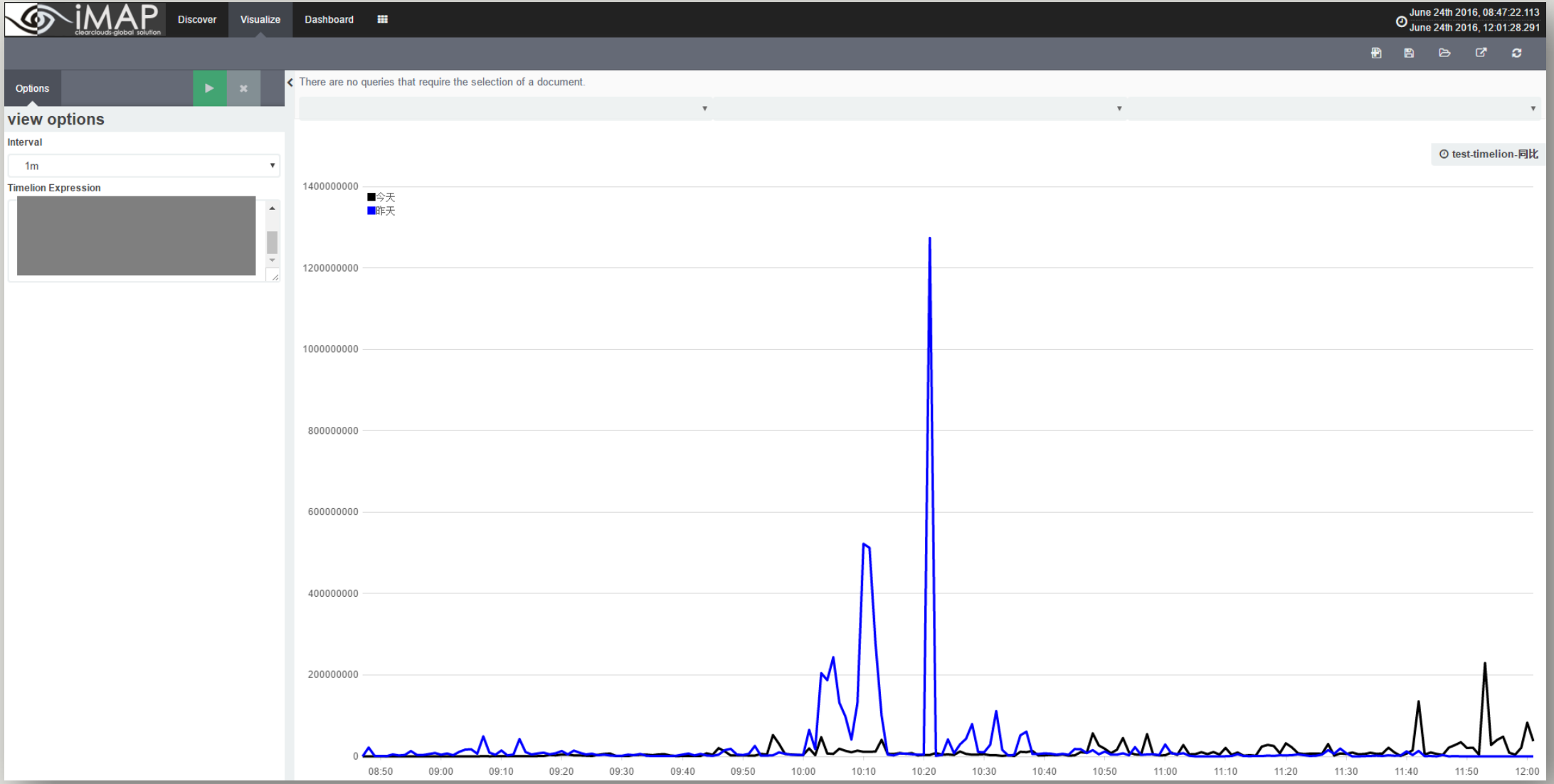
NOT (sip:[192.168.0.0 TO 192.168.0.255] AND
dip: [192.168.0.0 TO 192.168.1.255])



应用聚合分析


iMAP
Discover
Visualize
Dashboard
Last 15 minutes
链路层
IP层
TCP (1982)
UDP (3277)
HTTP 应用分析 (1446)
DNS (2387)
DDoS
shell
ALERT
ISO8583
logstash (3838)
HTTP-应用列表
filters
request
response
byte
error_rate
搜狗 26 29ms 32.3KB 7.692%
优酷 1 24ms 1.8KB 0.000%
新浪 15 19ms 35.0KB 0.000%
百度 149 1,283ms 692.0KB 2.013%
腾讯 82 71ms 387.6KB 0.000%
网易 6 37ms 276.0KB 0.000%
淘宝 24 14ms 27.6KB 0.000%
HTTP app domain-url
Percentage of Sum of request
100%
80%
60%
40%
20%
0%
go.microsoft.com
download.microsoft.com
192.168.0.118:9202
short.weixin.qq.com
rm.api.weibo.com
static.adbutter.net
images.taboola.com
ping.chartbeat.net
get.sogou.com
ksj.baidu.com
otf.msn.com
pos.baidu.com
beacon.sina.com.cn
192.168.0.118:5601
trc.taboola.com
Percentage of domain: Descending

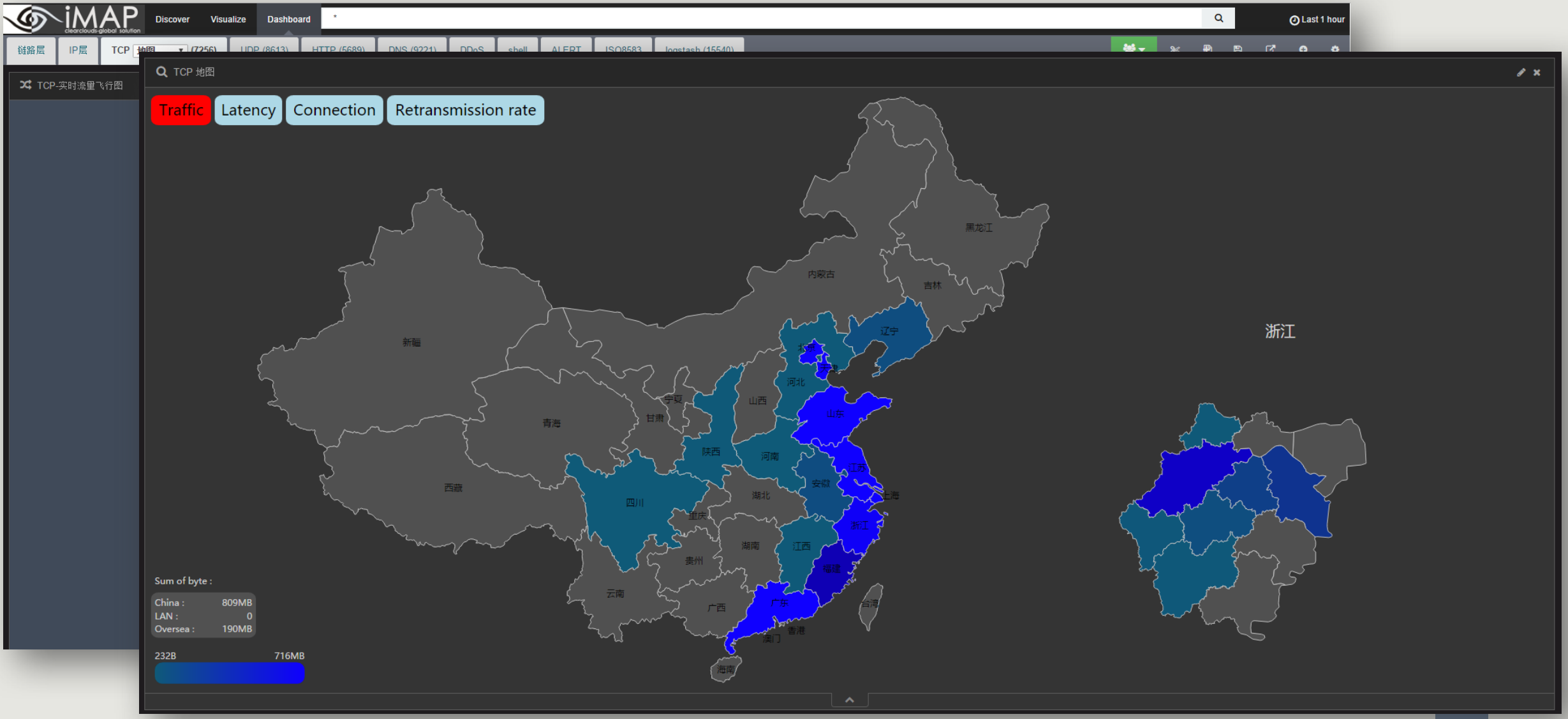
时间序列分析


iMAP
clearclouds-global solution
Discover
Visualize
Dashboard
June 24th 2016, 08:47:22.113
June 24th 2016, 12:01:28.291
Options
view options
Interval
1m
Timelion Expression
There are no queries that require the selection of a document.
test-timelion-同比
今天
昨天
1400000000
1200000000
1000000000
800000000
600000000
400000000
200000000
0
08:50
09:00
09:10
09:20
09:30
09:40
09:50
10:00
10:10
10:20
10:30
10:40
10:50
11:00
11:10
11:20
11:30
11:40
11:50
12:00

时间序列分析

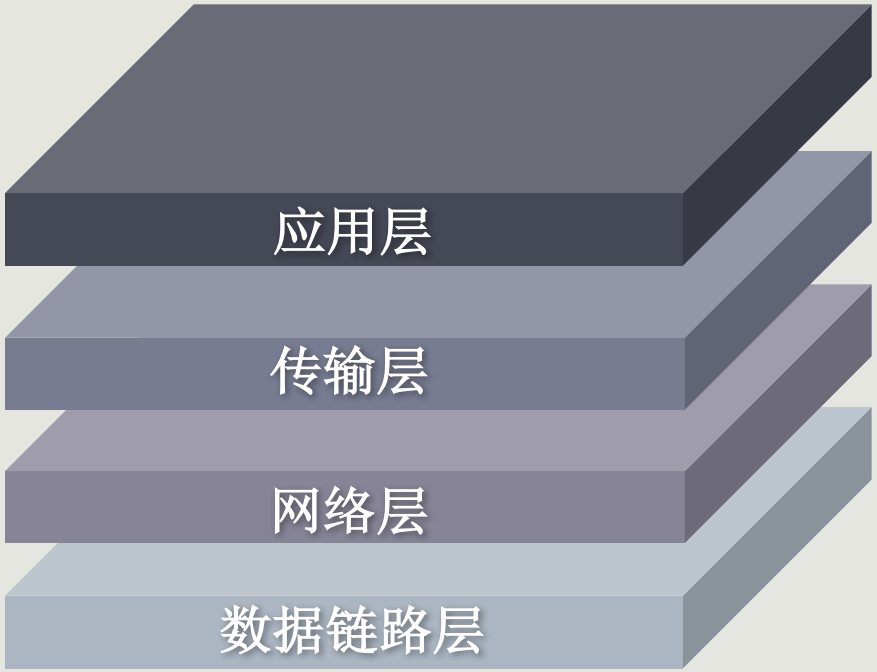

iMAP
clearclouds-global solution
Discover
Visualize
Dashboard
June 24th 2016, 10:27:57.049
June 24th 2016, 13:55:41.311
Options
There are no queries that require the selection of a document.
view options
Interval
1m
Timelion Expression
test-timelion-重传告警
异常
警告
正常
重传率
55
50
45
40
35
30
25
20
15
10
5
0
10:30
10:40
10:50
11:00
11:10
11:20
11:30
11:40
11:50
12:00
12:10
12:20
12:30
12:40
12:50
13:00
13:10
13:20
13:30
13:40
13:50

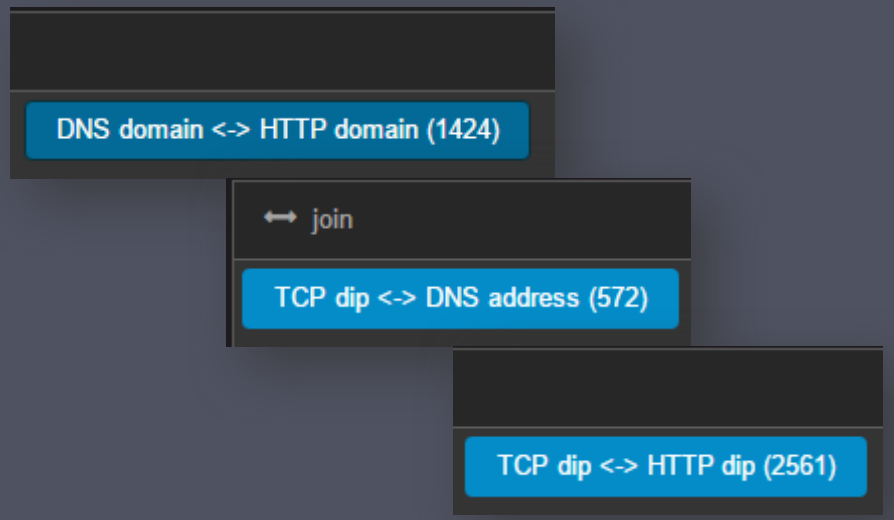
地理位置信息分析


iMAP
clearclouds-global solution
Discover
Visualize
Dashboard
Last 1 hour
链路层
IP层
TCP
TCP-实时流量飞行图
TCP 地图
Traffic
Latency
Connection
Retransmission rate
黑龙江
内蒙古
吉林
辽宁
新疆
北京
天津
河北
山西
宁夏
甘肃
青海
山东
陕西
河南
江苏
安徽
西藏
四川
湖北
上海
重庆
浙江
湖南
江西
贵州
福建
云南
广西
广东
台湾
香港
澳门
海南
浙江
Sum of byte :
China : 809MB
LAN : 0
Oversea : 190MB
232B
716MB

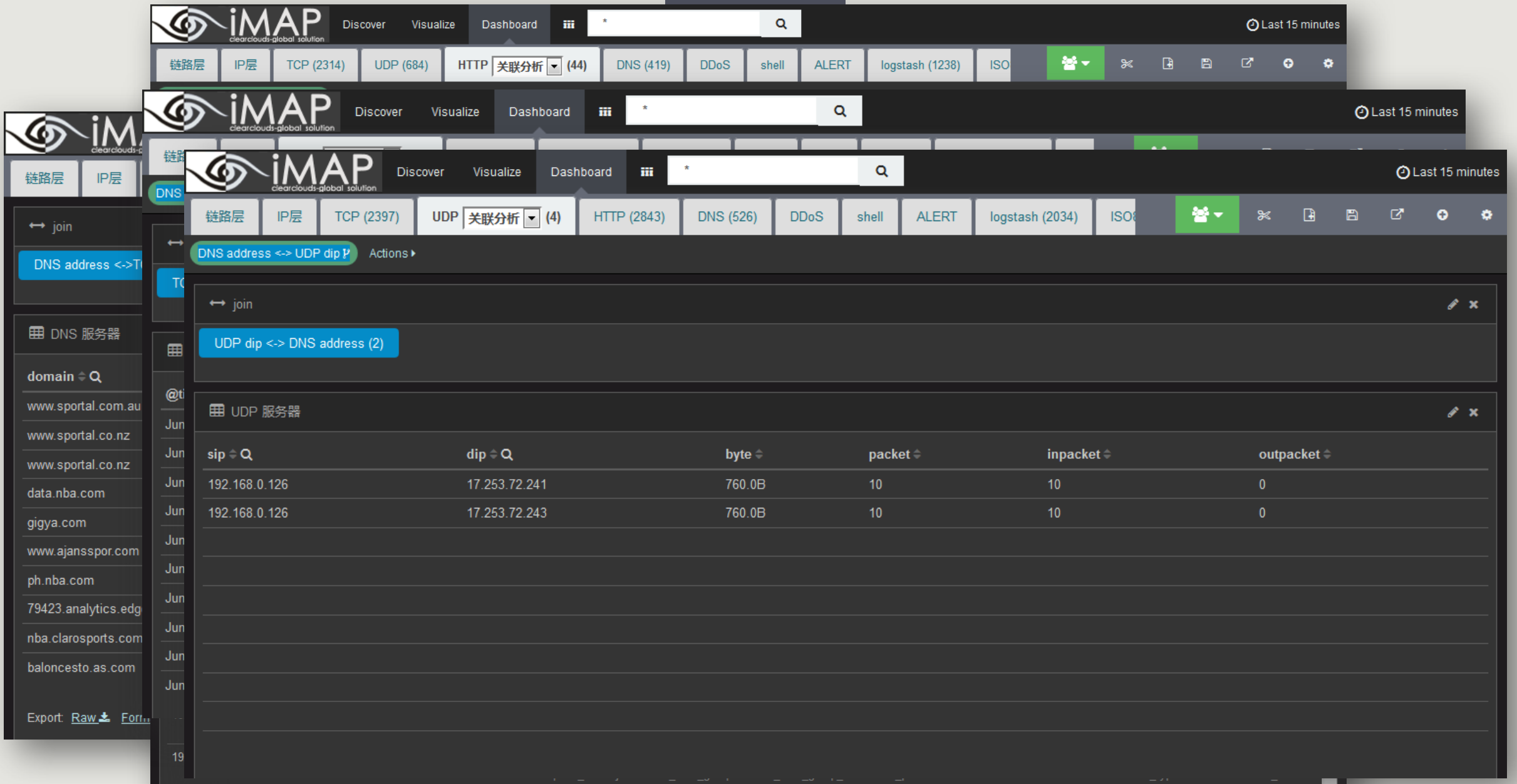
关联查询

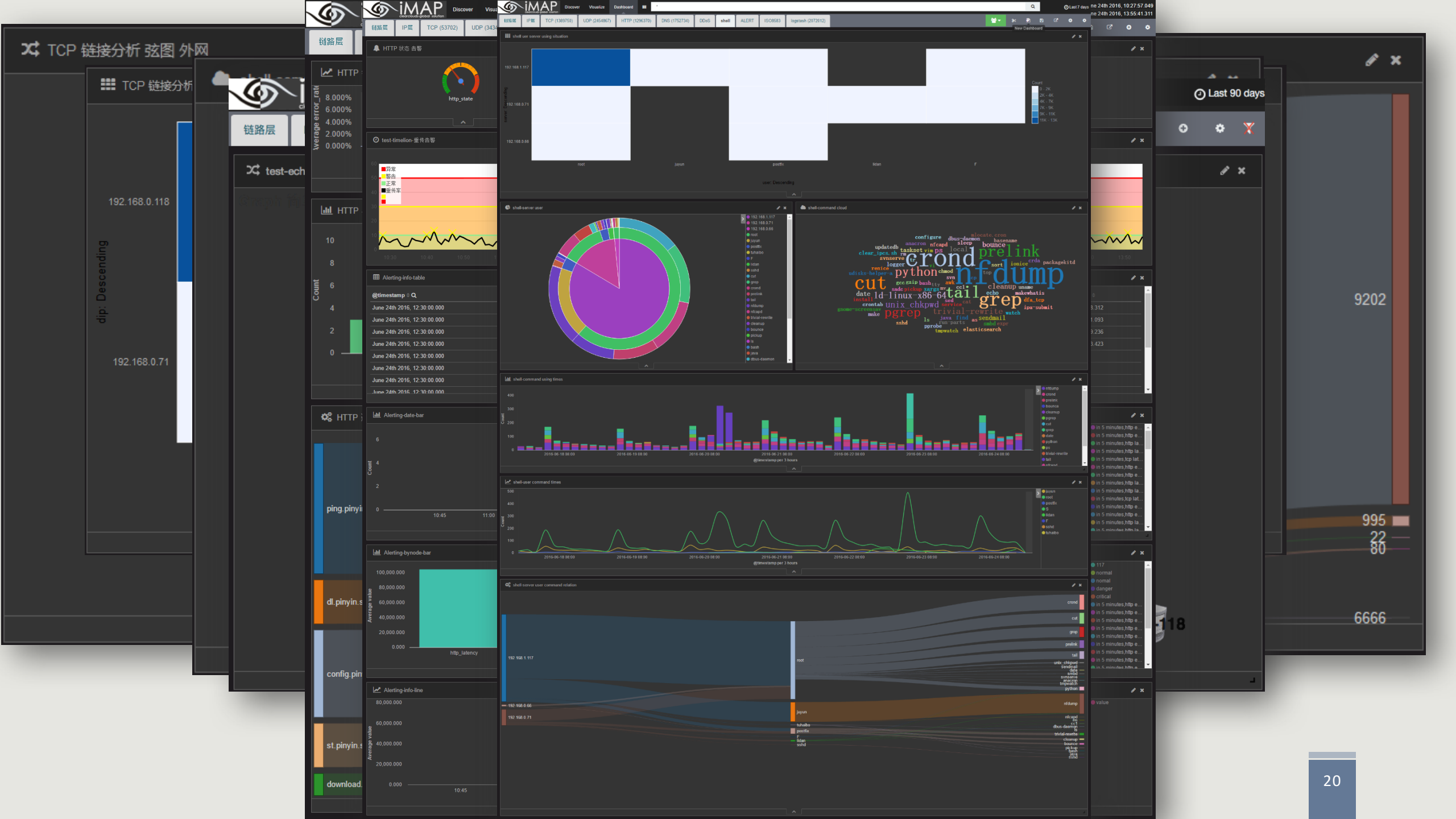
siren-join





将不同层次联系在一起


iMAP
clearclouds-global solution
Discover
Visualize
Dashboard
Last 15 minutes
链路层
IP层
TCP (2397)
UDP 关联分析 (4)
HTTP (2843)
DNS (526)
DDoS
shell
ALERT
logstash (2034)
DNS address <-> UDP dip
Actions
join
UDP dip <-> DNS address (2)
UDP 服务器
sip
dip
byte
packet
inpacket
outpacket
192.168.0.126 17.253.72.241 760.0B 10 10 0
192.168.0.126 17.253.72.243 760.0B 10 10 0
DNS 服务器
domain
www.sportal.com.au
www.sportal.co.nz
www.sportal.co.nz
data.nba.com
gigya.com
www.ajansspor.com
ph.nba.com
79423.analytics.edg
nba.clarosports.com
baloncesto.as.com
Export: Raw
192.168.0.123 180.149.153.11 rm.api.weibo.com GET rm.api.weibo.com/2/remind/push_count.json
192.168.0.123 180.149.153.11 rm.api.weibo.com GET rm.api.weibo.com/2/remind/push_count.json


TCP 链接分析 弦图 外网
TCP 链接分析
链路层
192.168.0.118
192.168.0.71
dip: Descending
HTTP 状态 告警
http_state
test-timelion-重传告警
异常
警告
正常
重传率
Alerting-info-table
@timestamp
June 24th 2016, 12:30:00.000
Alerting-date-bar
Alerting-bynode-bar
http_latency
Alerting-info-line
shell user server using situation
shell-server user
shell-command cloud
shell-command using times
shell-user command times
shell-server user command relation
Last 90 days
ping.pinyi
dl.pinyin.s
config.pin
st.pinyin.s
download
9202
995
22
80
6666

Q&A