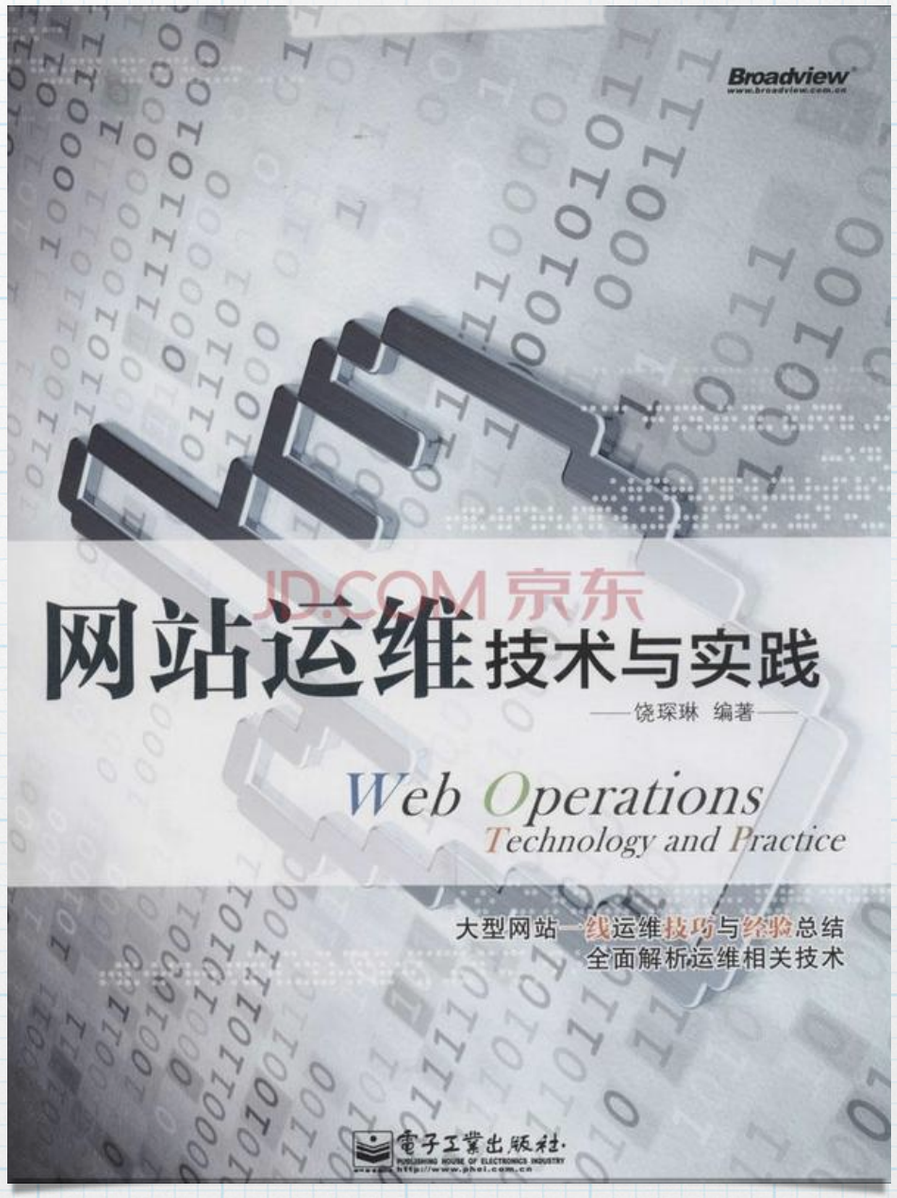
{{More}} Kibana

@argv

Who am I

* Perl Monger
* Author of《网站运维技术与实践》
* SRE Architect @sina.com
* weibo: @ARGV
* github: https://github.com/chenryn
* blog: http://chenlinux.com



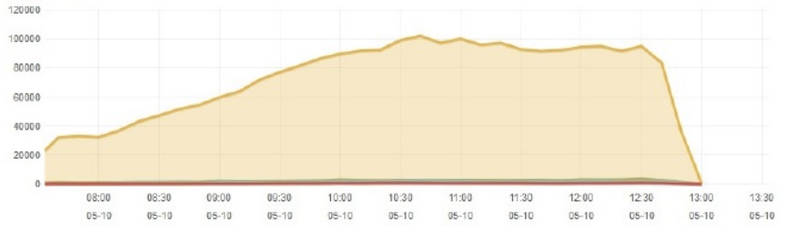
ELK and I

* Using ELK from 2012
* <Logstash> at slideshare.net had 18232 views
* 3.3 & 4.2 chapters in my Book
* 2 ebook at gitbook.io:
    * [logstash best practice](https://www.gitbook.io/book/chenryn/logstash-best-practice)
    * [kibana Chinese Guide](https://www.gitbook.io/book/chenryn/kibana-guide-cn)
* kibana fork: <https://github.com/chenryn/kibana>

Kibana Intro

* angular.js(framework) + jquery.flot(visualize) + elastic.js(search)
* time-based comparisons
* make sense of your data
* empower more team members
* flexible interface, easy to share
* powerful search syntax
* easy set up

运营商数据点趋势



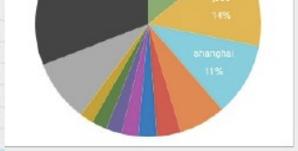
运营商平均响应时间

779 ms

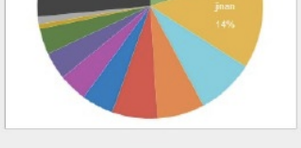
运营商	平均时间
*	779 ms
电信	811 ms
联通	751 ms
教育网	666 ms
移动	832 ms

城市平均响应时间(MS)

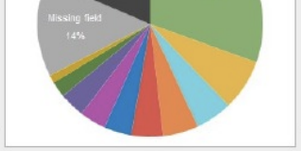
电信超时城市分布



联通超时城市分布

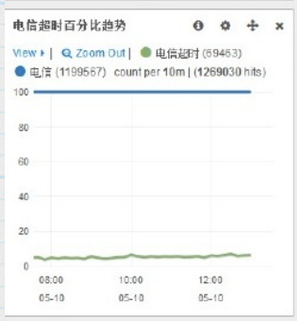


教育网超时城市分布

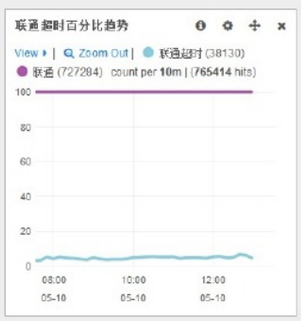


移动超时城市分布

电信超时百分比趋势



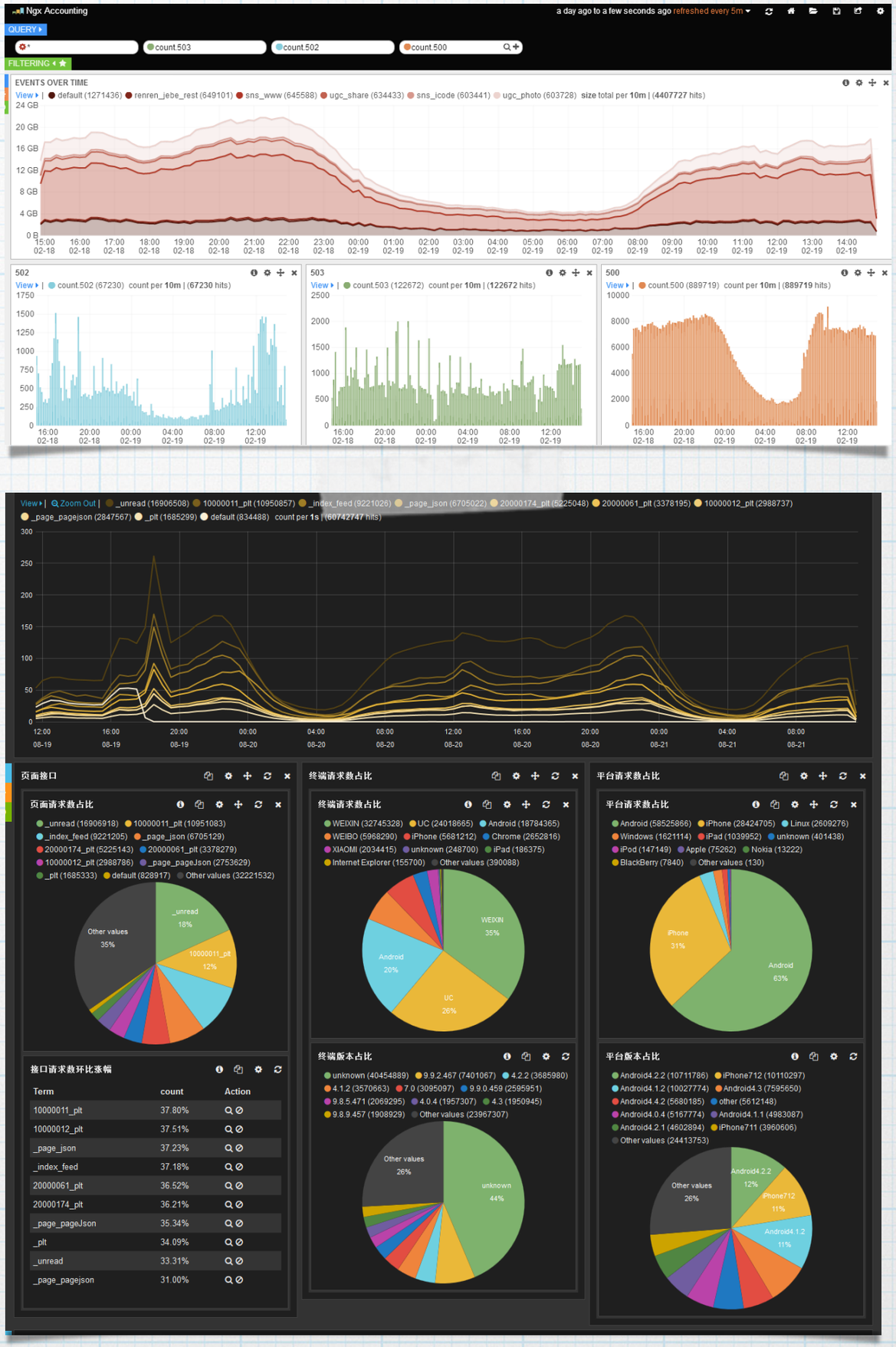
联通超时百分比趋势



教育网超时百分比趋势

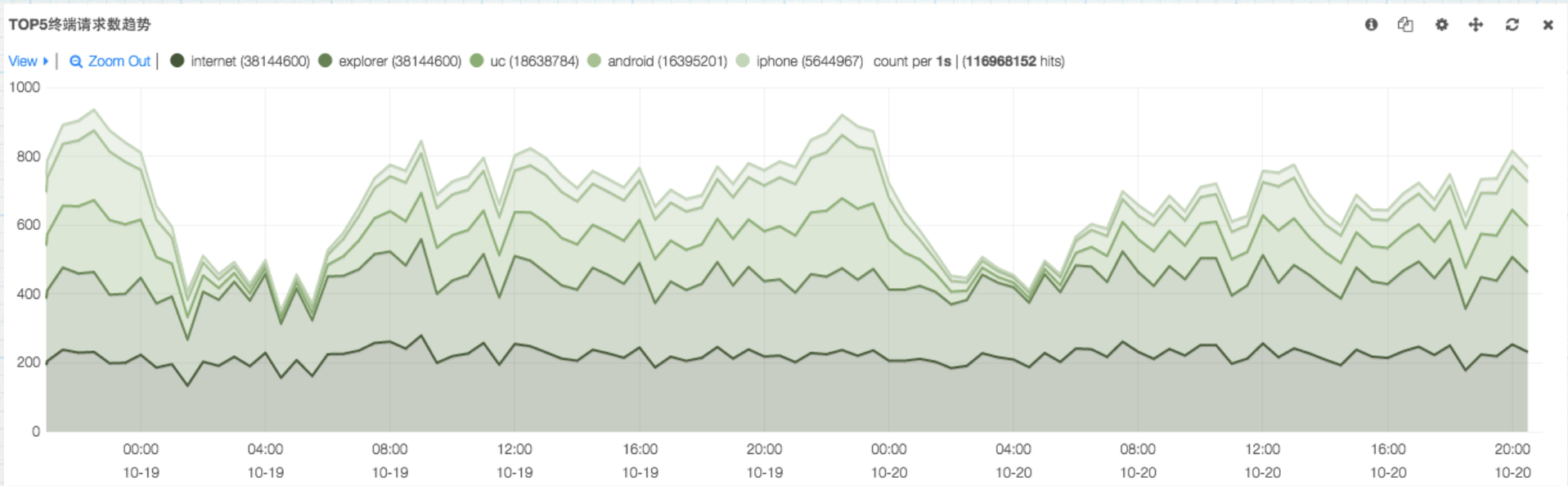
移动超时百分比趋势

访问分布



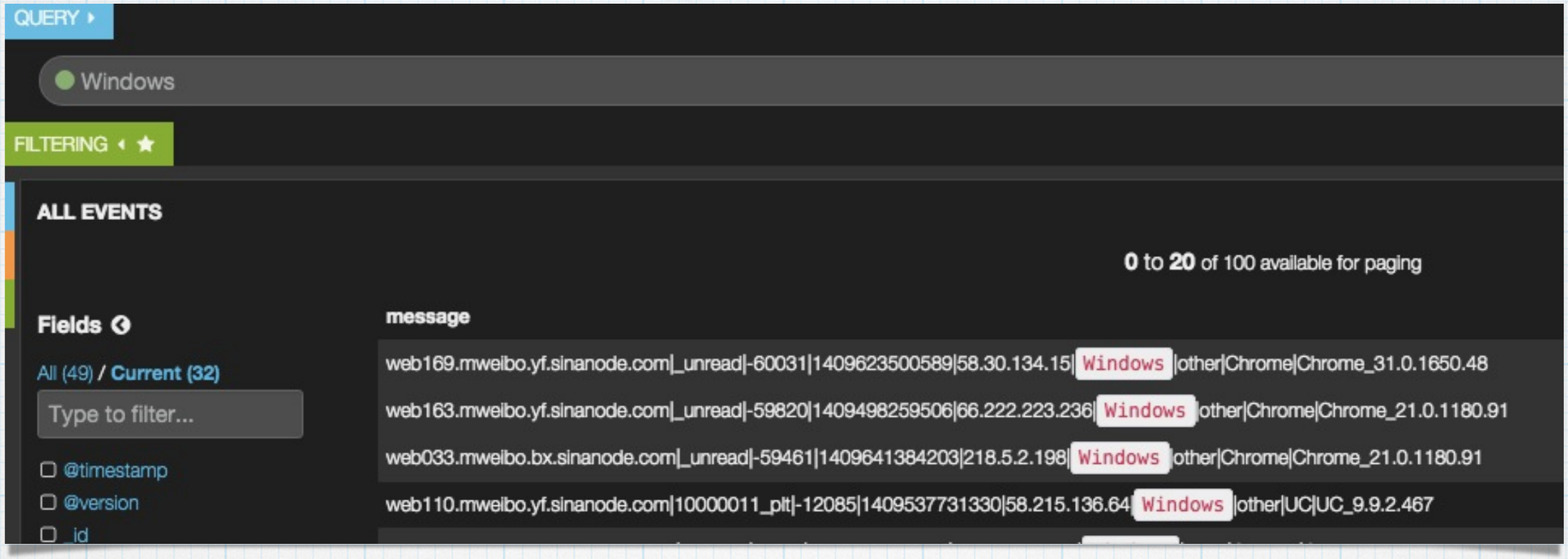
Kibana layout

* dashboard
* row != line
* panel
  * timepicker/query/filtering
  * charts/table/text...



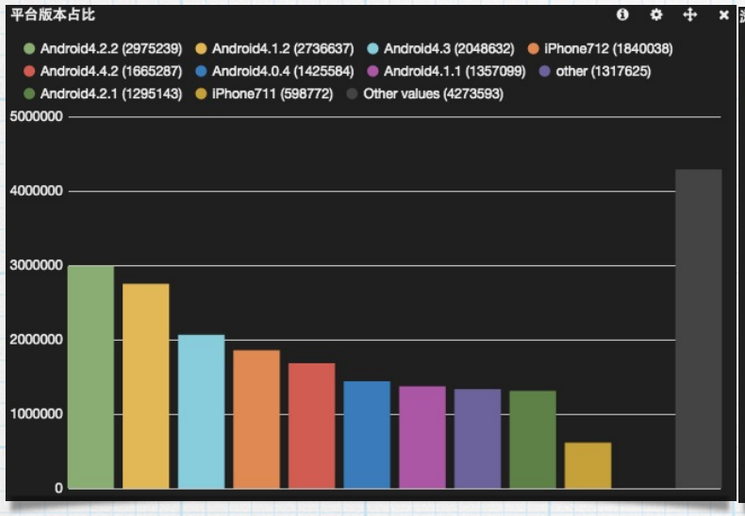
histogram

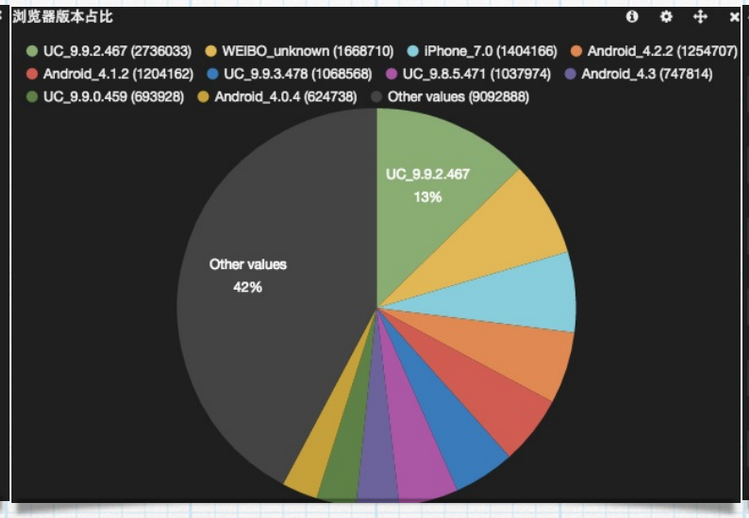
@timestamp based
count/mean/total
bar/lines/stack/percent
selected queries

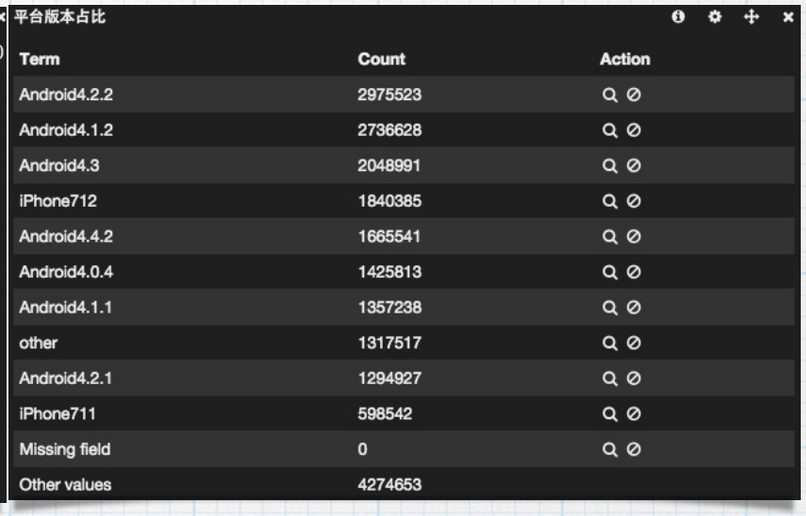


table

paging
fields.list
highlight
sortable
micro analysis







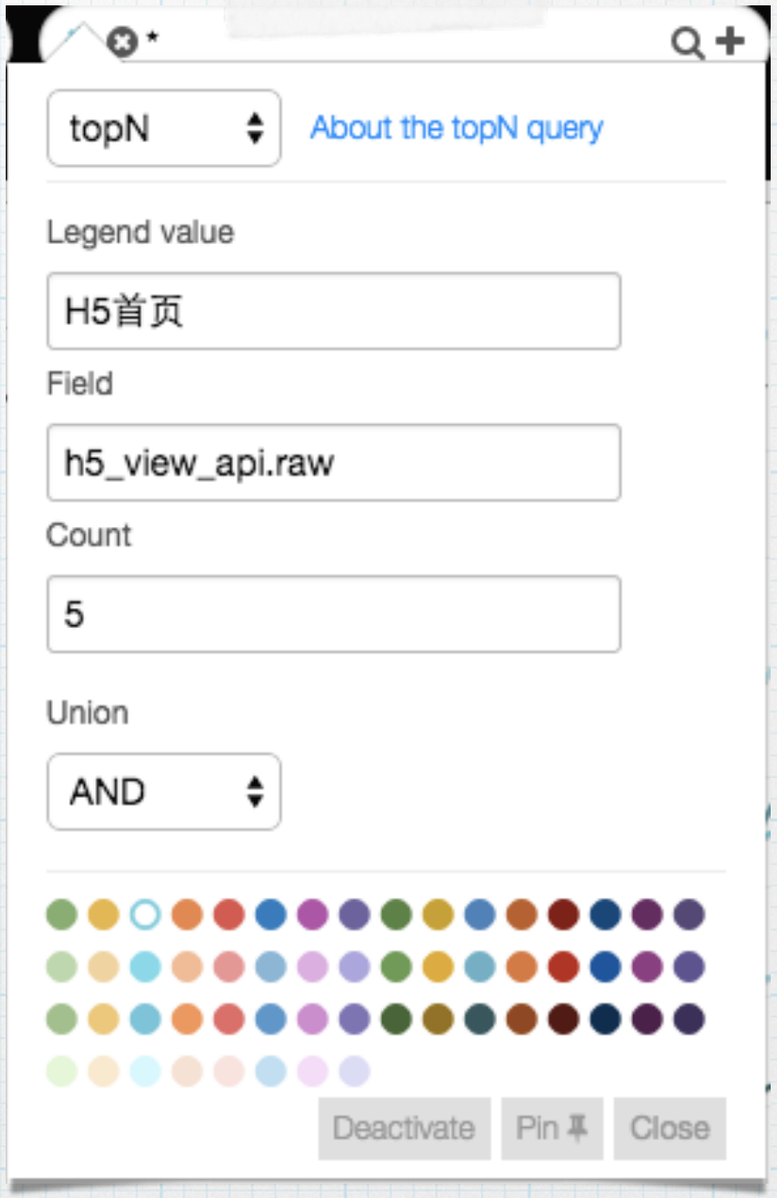
Term	Count	Action
Android4.2.2	2975523	
Android4.1.2	2736628	
Android4.3	2048991	
iPhone712	1840385	
Android4.4.2	1665541	
Android4.0.4	1425813	
Android4.1.1	1357238	
other	1317517	
Android4.2.1	1294927	
iPhone711	598542	
Missing field	0	
Other values	4274653	

terms

bar/pie/table
missing/other
donut/legend/lable

TopN query

* query termfacets before panel rendering
* multi-facet with filtering each term



Dynamic Kibana

* logstash.json
  * http://yourserver/index.html#/dashboard/file/logstash.json?query=status:200&from=7d
* logstash.js
  * http://yourserver/index.html#/dashboard/script/logstash.js?query=status:403,status:404&from=7d

Game Over?

No, We need more!

辛苦琛琳！

我们看到这数据分析平台十分强大，所呈现的准实时曲线图和统计饼图也非常直观漂亮，
不过有些占比数据可能和实际情况还有些出入，相信通过合理分类筛选能够得到更有帮助的数据图表

就目前来看，有一部分我们现阶段需要统计的数据尚未统计到，为了让统计数据更具有指导意义，有
帮我们统计或调整：

待调整点①
目前统计百分比的饼图维度估计是按照各平台或浏览器的“请求数的和”的一个占比，如下4个饼图
<image004.jpg>
需要调整为：统计百分比的饼图**维度需要按照各平台或浏览器的“H5首页的PV”的一个占比**

待调整点②
由于近阶段需要关注页面加载时长区间占比，所以需要**新增一个H5首页的加载时长区间占比**，如下
<image008.png>
同时，**时长区间最好是可调的，该饼图左侧并列一个饼图为改版前的H5首页的平均加载时长占比**

待调整点③
顶部的准实时曲线图的纵坐标目前是接口请求数，
<image012.jpg>

需要调整为：**H5首页加载平均时长准实时曲线，也就是纵坐标是H5首页加载平均时长，单位为毫秒**
琛琳帮忙看下这三个待调整点是否好支持到，如果有疑问可随时和我沟通，我的座机短号为3317，
非常感谢！

查看更多

各位好，下图这个图表，我们希望将 平台/浏览器 分开统计，并且点击进入二级的图表时，能看到平
分成。不知道能不能实现。。。

Range panel

* No range panel in kibana3
  * well, it's in kibana4 now~
  * DIY beginning

* ~~find~~search range facets in ES doc. ✓
* find pie charts code in Kibana. ✓
* copy terms/, paste to range/. ✓
* change request in module.js. ✓
* change ng-model in editor.html. ✓
* it work. ✓

module.js

* scope.ejs.RangeFacet()
* rangefacet.addRange()
* rangefacet.field()
* request.facet()
* scope.ejs.doSearch()
* results.then()

```
// Ranges mode
if($scope.panel.tmode === 'ranges') {
  rangefacet = $scope.ejs.RangeFacet('ranges');
  // AddRange
  _.each($scope.panel.values, function(v) {
    rangefacet.addRange(v.from, v.to);
  });
  request = request
    .facet(rangefacet
    .field($scope.field)
    .facetFilter($scope.ejs.QueryFilter(
      $scope.ejs.FilteredQuery(
        boolQuery,
        filterSrv.getBoolFilter(filterSrv.ids())
      )))).size(0);
}

// Populate the inspector panel
$scope.inspector = request.toJSON();

results = $scope.ejs.doSearch(dashboard.indices, request);
// Populate scope when we have results
results.then(function(results) {
  $scope.panelMeta.loading = false;
  if($scope.panel.tmode === 'ranges') {
    $scope.hits = results.hits.total;
  }

  $scope.results = results;
```

editor.html

<tr ng-repeat="value in panel.values">

<td><input ng-model="value.from"></td>

<td><input ng-model="value.to"></td>

</tr>

```
<table class="table table-condensed table-striped">
  <thead>
    <tr>
      <th>From</th>
      <th>To</th>
      <th ng-show="panel.values.length > 1">Delete</th>
    </tr>
  </thead>
  <tbody>
    <tr ng-repeat="value in panel.values">
      <td>
        <div class="editor-option">
          <input class="input-small" type="number" ng-model="value.from
        </div>
      </td>
      <td>
        <div class="editor-option">
          <input class="input-small" type="number" ng-model="value.to"
        </div>
      </td>
      <td ng-show="panel.values.length > 1">
        <i ng-click="panel.values = _.without(panel.values, value);set_

      </td>
    </tr>
  </tbody>
</table>
```

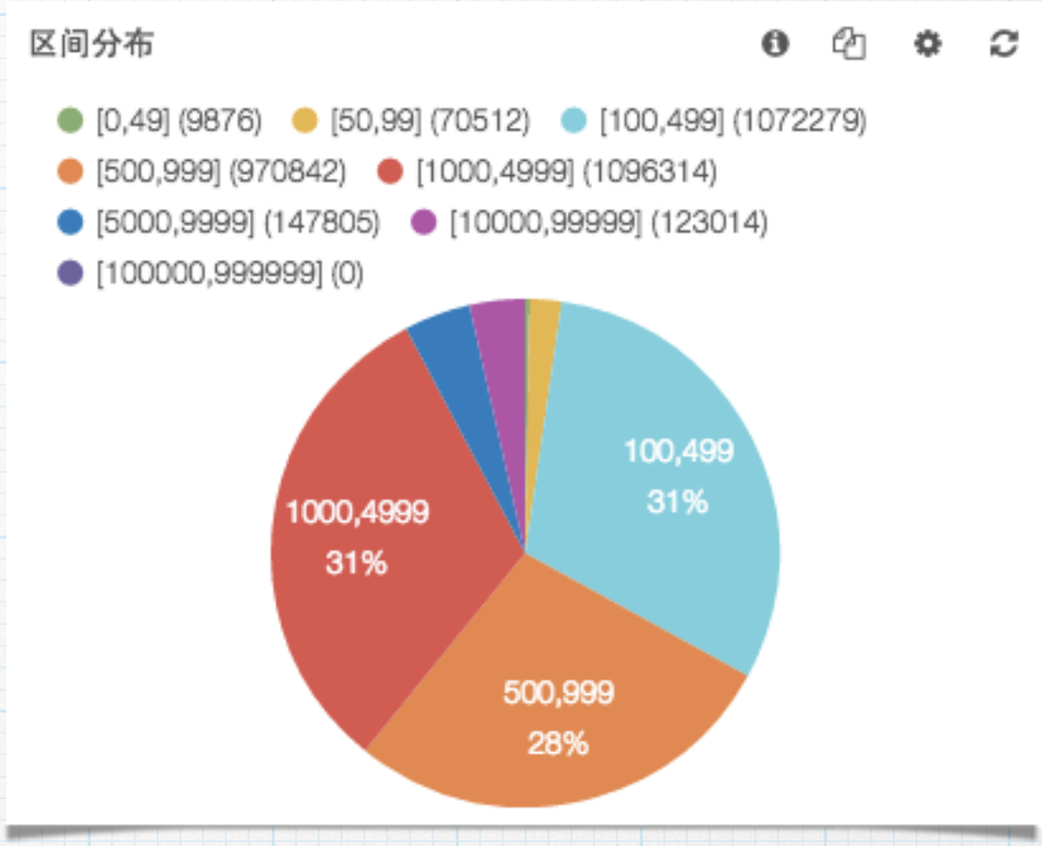
Parameters

Ranges mode: ranges

Field: h5_view_loadt

From	To	Delete
0	49	✖
50	99	✖
100	499	✖
500	999	✖
1000	4999	✖
5000	9999	✖
10000	99999	✖
100000	999999	✖

Add value



Range Panel DIY Result

More DIY panels

* percentile panel
* selectable bettermap providers
* queries generate helper
* histogram thereshold notification
* china map panel
* term_stats map panel
* statisticstrend panel
* multifieldhistogram panel
* valuehistogram panel
* force panel

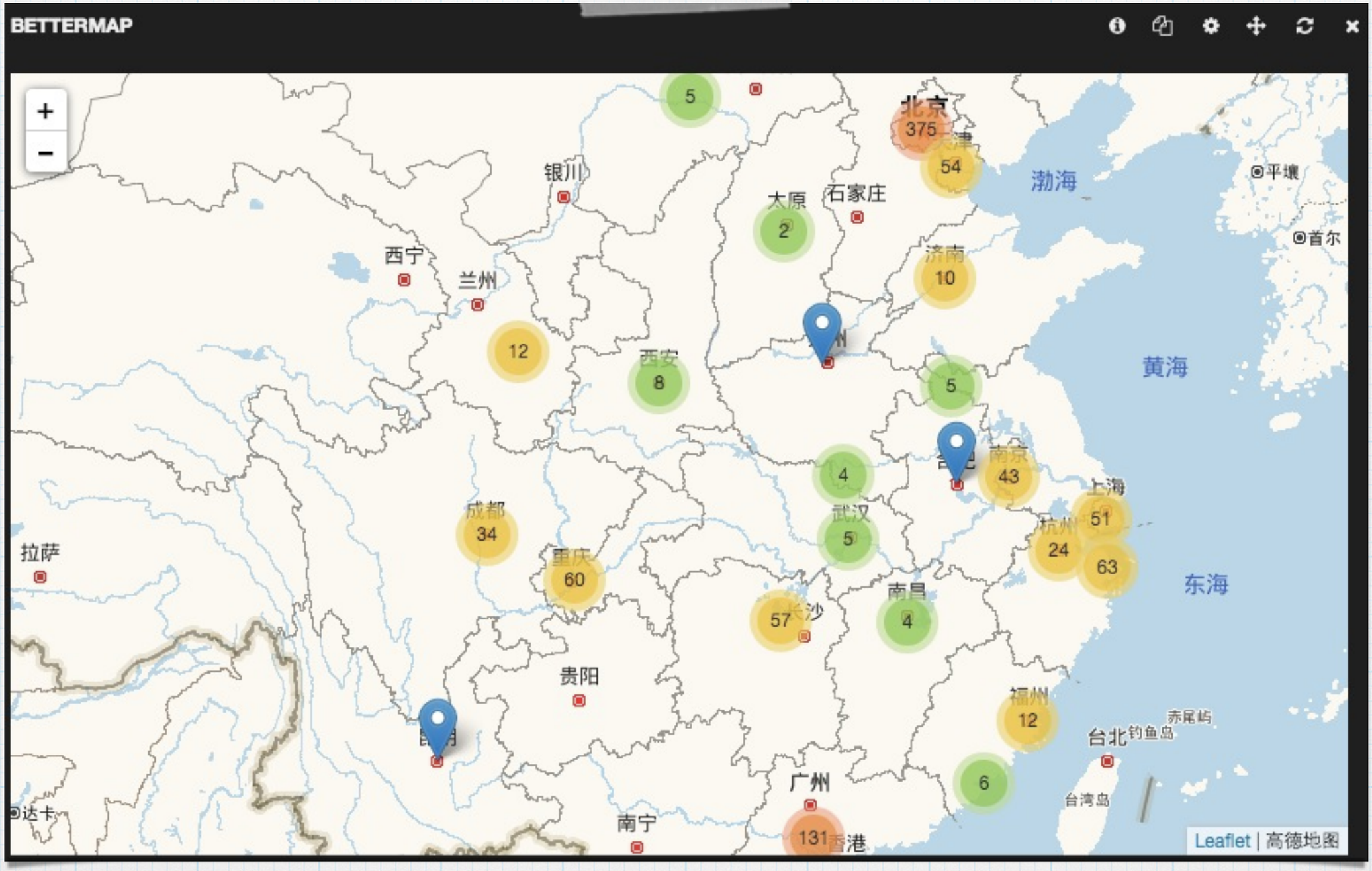
Percentile Panel

运营商响应时间区间

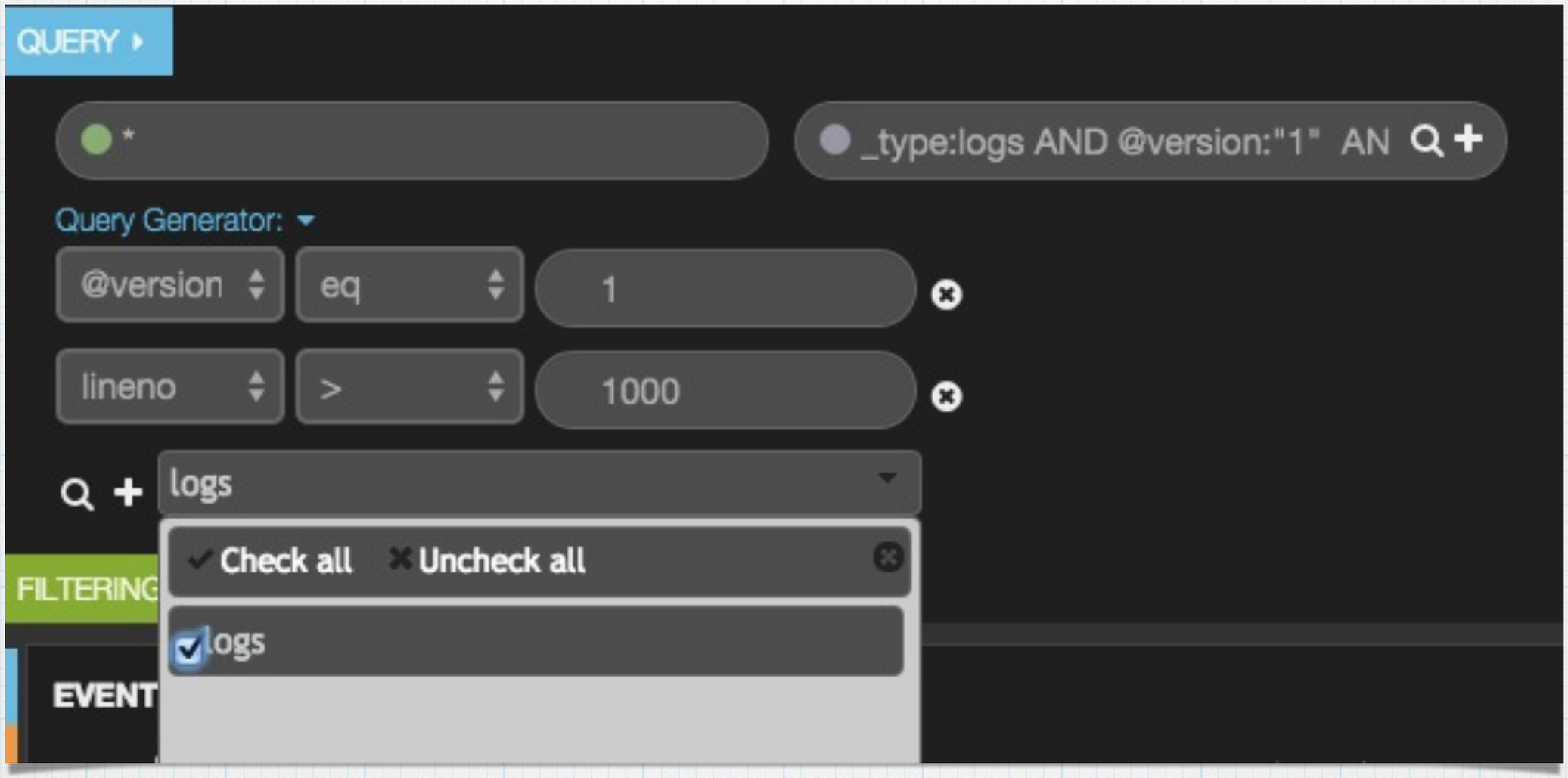
875 (85.0)

Query	85%	90%	95%	99%
电信	952	1,374	2,477	9,038
移动	931	1,349	2,505	8,738
*	875	1,284	2,383	8,935
联通	817	1,241	2,399	9,405
赛尔	704	1,006	1,872	7,085

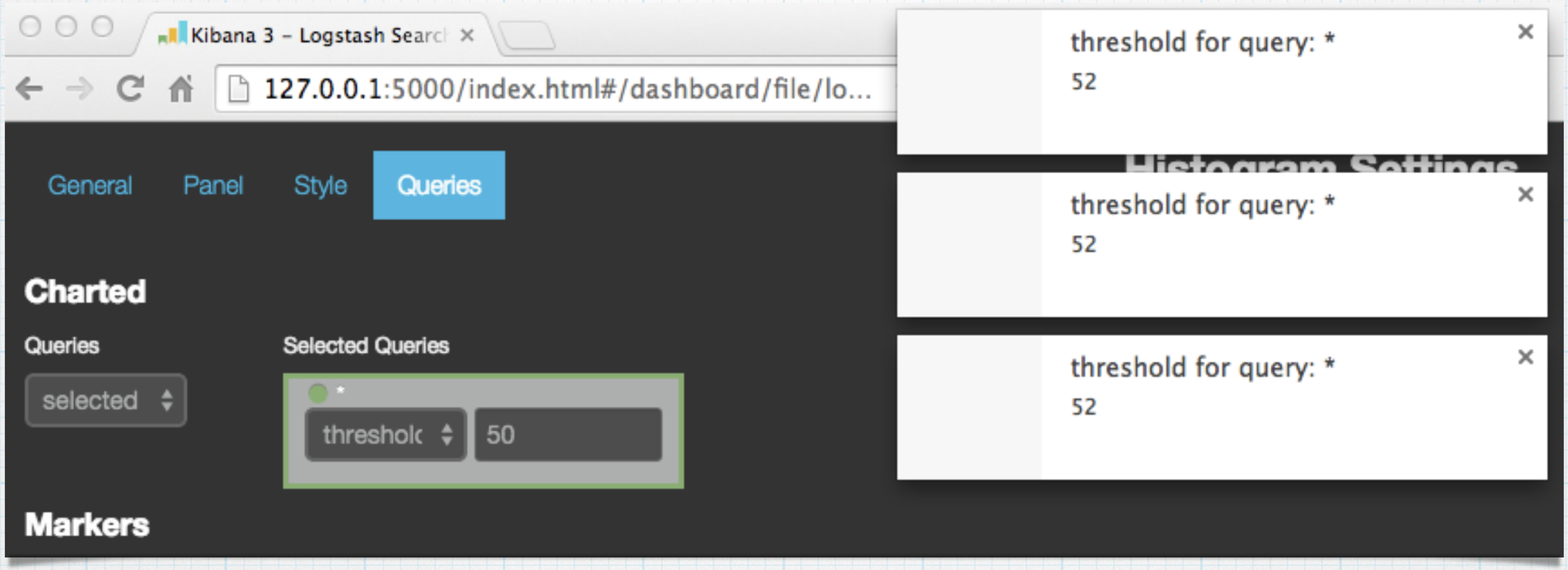
@AR
weibo.com/chenlin


BETTERMAP
北京
375
天津
54
渤海
平壤
首尔
石家庄
大原
2
银川
西宁
兰州
济南
10
5
12
西安
8
黄海
4
南京
43
上海
51
武汉
5
杭州
24
63
成都
34
重庆
60
南昌
4
东海
57
长沙
贵阳
福州
12
赤尾屿
钓鱼岛
台北
台湾岛
广州
6
拉萨
南宁
131
香港
Leaflet | 高德地图

Gaode(高德地图)

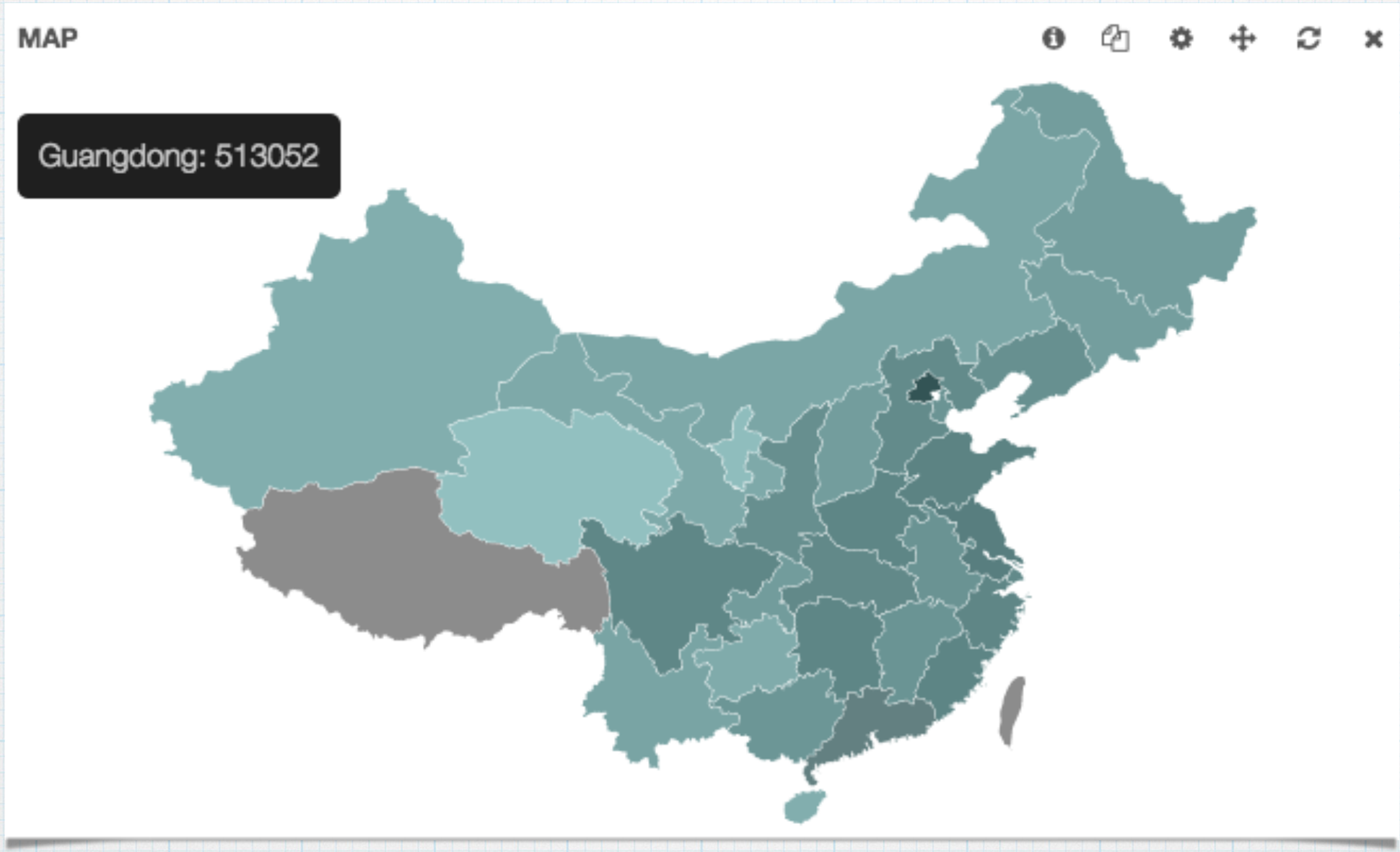


queries generate helper



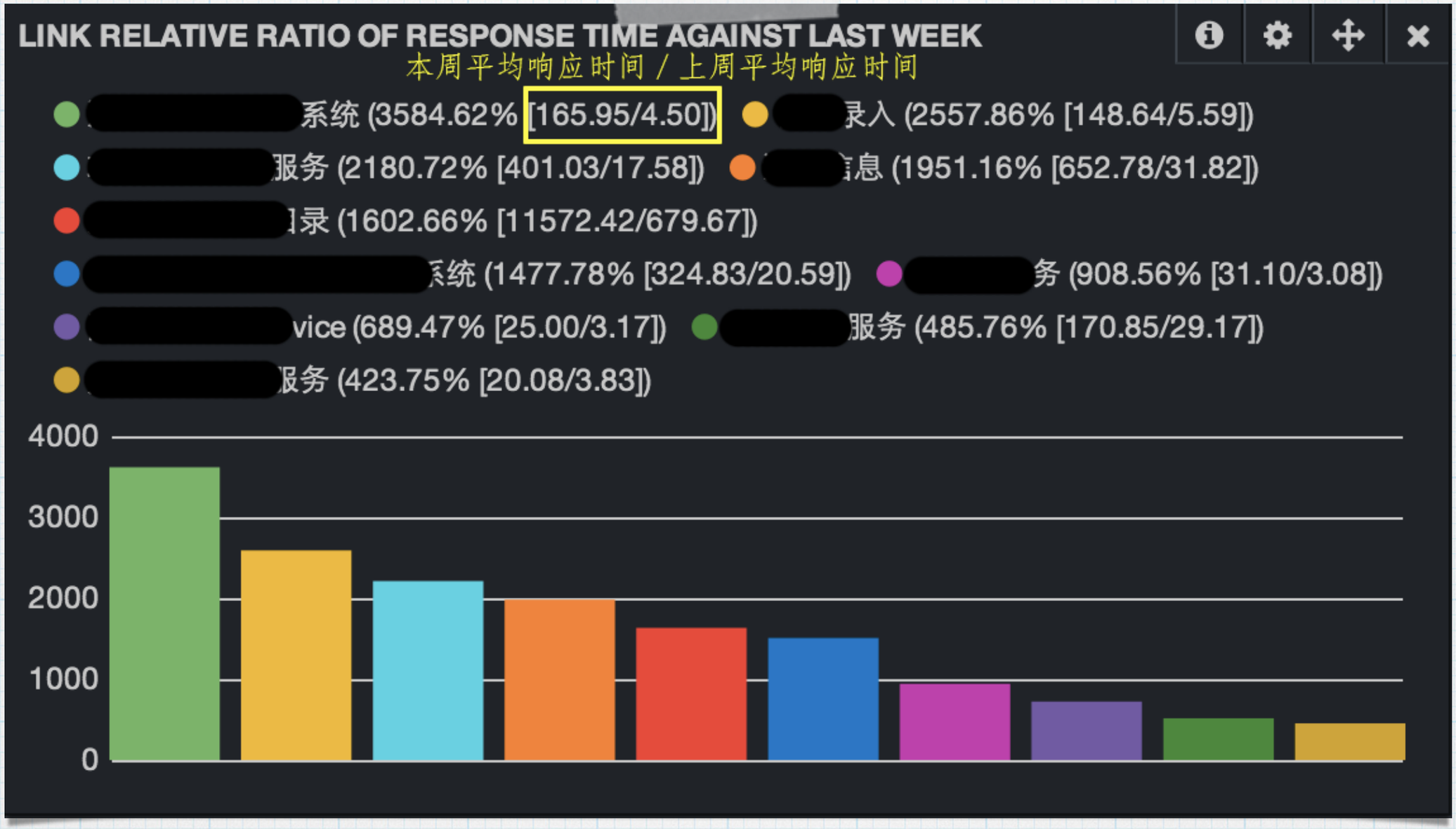
histogram threshold notification

threshold/anomaly detection
HTML5 notification API



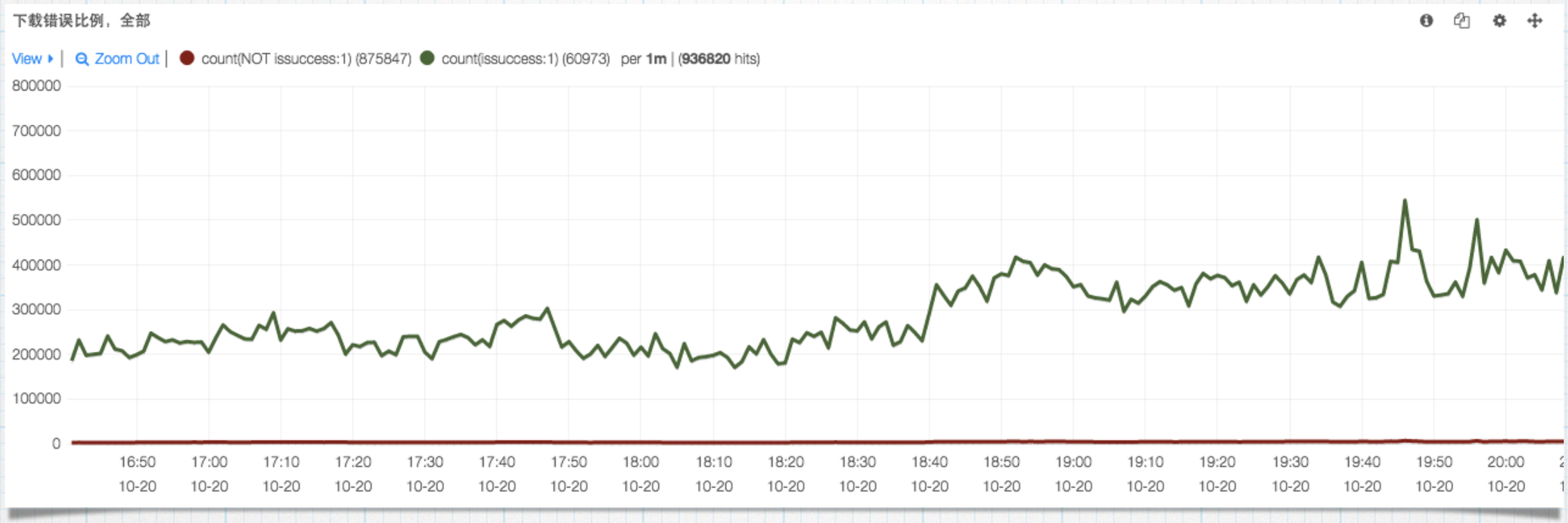
china map

term_stats map



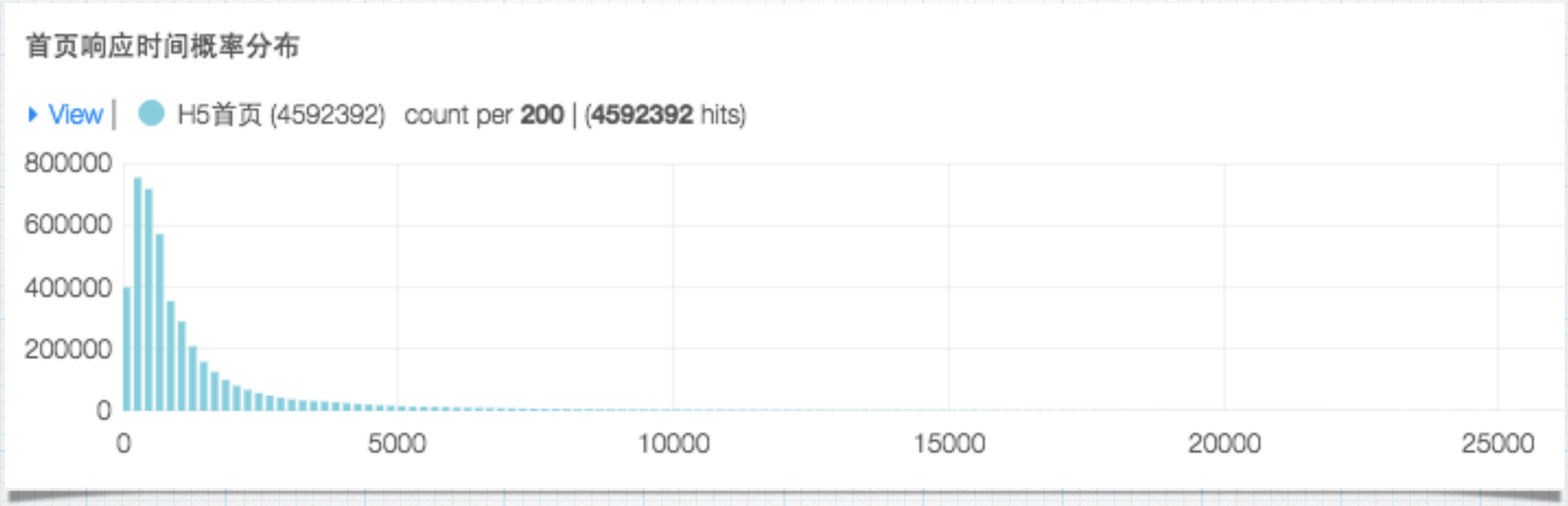
statisticstrend map

term_stats for trend map



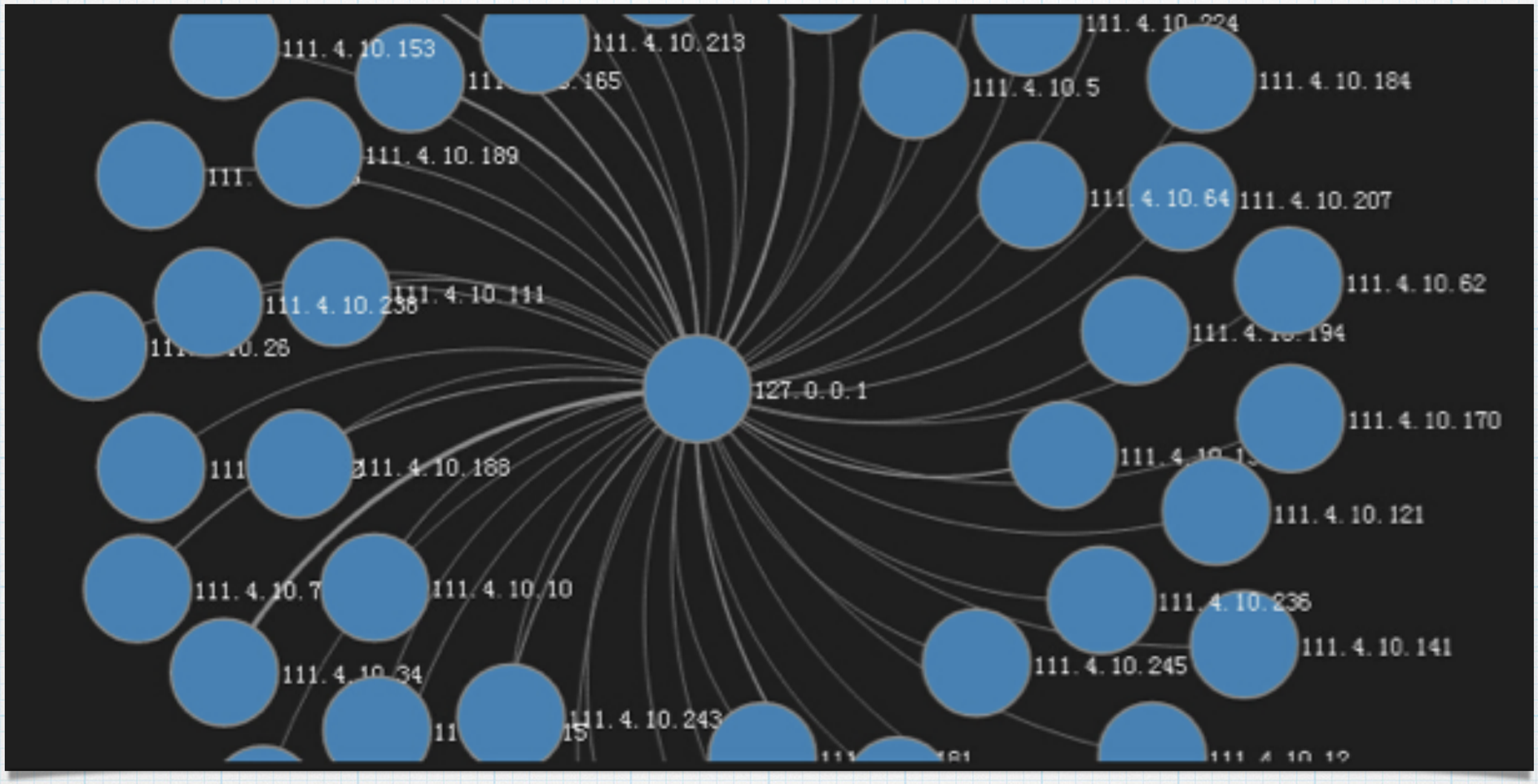
multifieldhistogram

different histogram setting for each query
for example: A : (B*1000)



valuehistogram

detect the probability distribution of responsetime



force

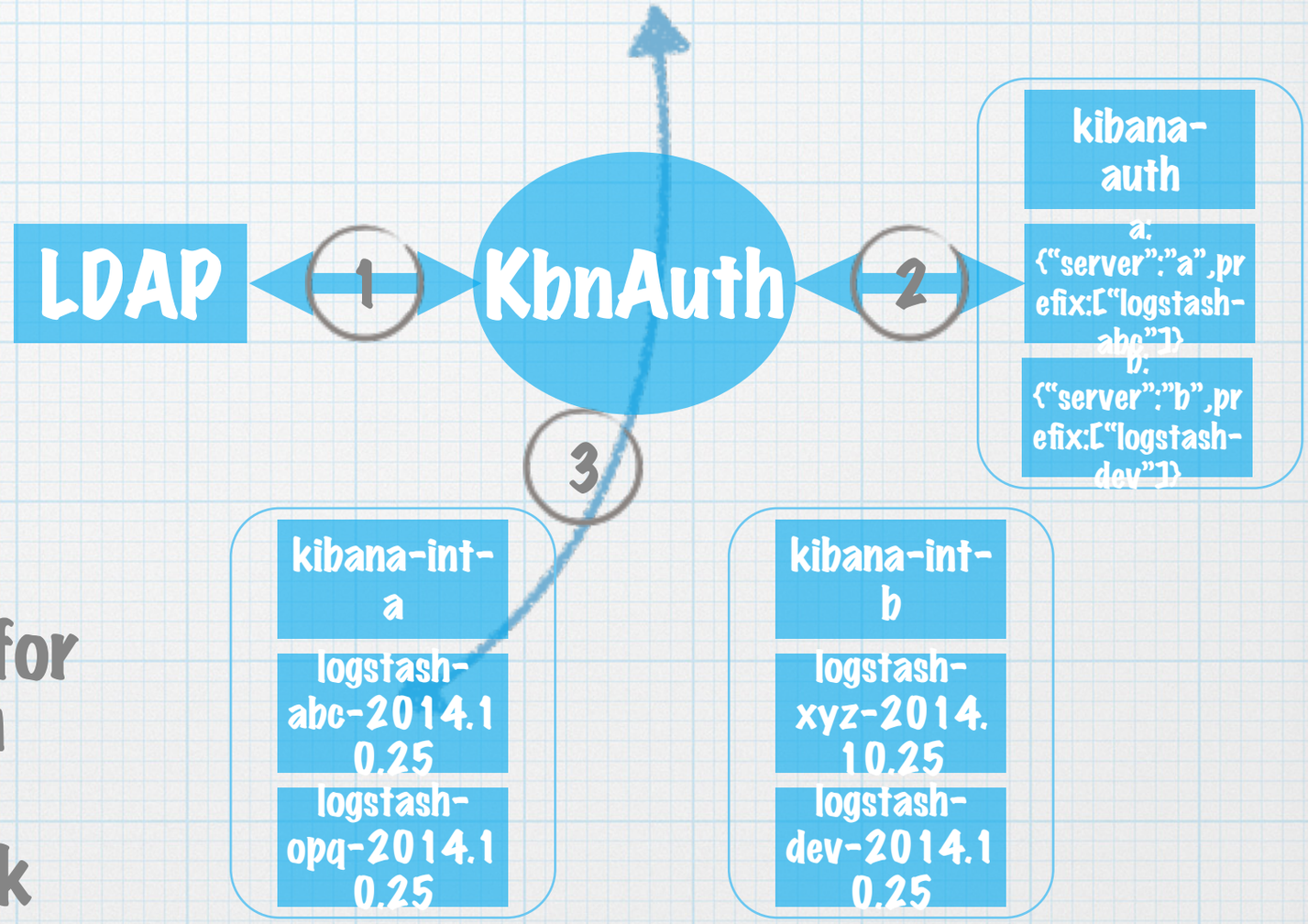
merge from packet beat

Kibana-Auth

* Exists solutions:
  * nginx + htpasswd(Kibana3 recommanded)
  * nodejs + CAS(Community recommanded)
  * sinatra(Kibana4 used)
* authentication VS authorization

my solution

* transparent proxy for ES
* fake `/_nodes` JSON
* `kibana-auth` index for cluster and indices authorization
* `kibana-int-$user` index for dashboards authorization
* Authen::Simple framework



kibana-auth

```
$ curl -XPOST http://127.0.0.1:9200/kibana-auth/indices/sri -
d '{
    "prefix":["logstash-sri","logstash-ops"],
    "server":"192.168.0.2:9200"
}'
```

* User “sri“ now can and **ONLY** can access `logstash-sri-yyyy.MM.dd` and `logstash-ops-yyyy.MM.dd` etc stored in `192.168.0.2:9200`

kibana-int-ṣuser

* ./script/kbnauth migratint sri logstash accesslog php-error

* read logstash/accesslog/php-error dashboards' schema from your original kibana-int index, and write into `kibana-int-sri`

Authen::Simple

* Authen::Simple::ActiveDirectory
* Authen::Simple::CDBI
* Authen::Simple::DBI
* Authen::Simple::FTP
* Authen::Simple::HTTP
* Authen::Simple::Kerberos
* Authen::Simple::LDAP
* Authen::Simple::NIS
* Authen::Simple::PAM
* Authen::Simple::Passwd
* Authen::Simple::POP3
* Authen::Simple::RADIUS
* Authen::Simple::SMB
* Authen::Simple::SMTP
* Authen::Simple::SSH

Overview

```
{
  eshost    => 'http://127.0.0.1:9200',
  hypnotoad => { listen => [‘http://*:80'] },
  secret => 'kibana_auth_secret',
  authen => {
    LDAP => {
      host   => 'ad.company.com',
      binddn => 'proxyuser@company.com',
      bindpw => 'secret',
      basedn => 'cn=users,dc=company,dc=com',
      filter =>
'(&(objectClass=organizationalPerson)
(objectClass=user)(sAMAccountName=%s))'
    },
    Passwd => { path => ‘.htpasswd' }
  }
}
```

The Last But Not Latest

* give a star(23 star now)
* give a try(kibana4 still beta now)
* give a feedback

If a new user has a bad time, it's a bug in logstash.

Thank You!

ARGV

扫描上面的二维码，关注我吧