ELK统一日志管理平台操作手册1.0.0

--2019.07.31

目录

[一、 日志标准化：](#_Toc32254_WPSOffice_Level1) [1](#_Toc32254_WPSOffice_Level1)

[1. 标准日志](#_Toc24823_WPSOffice_Level2) [1](#_Toc24823_WPSOffice_Level2)

[2. 标准解析](#_Toc10291_WPSOffice_Level2) [2](#_Toc10291_WPSOffice_Level2)

[3. 解析结果](#_Toc739_WPSOffice_Level2) [2](#_Toc739_WPSOffice_Level2)

[4. ELK框架配置](#_Toc21722_WPSOffice_Level2) [3](#_Toc21722_WPSOffice_Level2)

[二、kibana使用案例：](#_Toc24823_WPSOffice_Level1) [3](#_Toc24823_WPSOffice_Level1)

[1. 索引管理](#_Toc8015_WPSOffice_Level2) [3](#_Toc8015_WPSOffice_Level2)

[2. 创建新的索引](#_Toc2959_WPSOffice_Level2) [3](#_Toc2959_WPSOffice_Level2)

[3. 删除不用的索引](#_Toc32229_WPSOffice_Level2) [4](#_Toc32229_WPSOffice_Level2)

[4. 管理es数据](#_Toc29648_WPSOffice_Level2) [4](#_Toc29648_WPSOffice_Level2)

[5. 真正的功能-日志查询](#_Toc5309_WPSOffice_Level2) [5](#_Toc5309_WPSOffice_Level2)

[6. 查询案例](#_Toc11677_WPSOffice_Level2) [6](#_Toc11677_WPSOffice_Level2)

[7. 查询案例](#_Toc9459_WPSOffice_Level2) [7](#_Toc9459_WPSOffice_Level2)

[8. 保存本次查询逻辑为模板](#_Toc6717_WPSOffice_Level2) [13](#_Toc6717_WPSOffice_Level2)

[9. 打开历史保存模板，快速查询](#_Toc1259_WPSOffice_Level2) [14](#_Toc1259_WPSOffice_Level2)

[10. 视图展示](#_Toc4079_WPSOffice_Level2) [14](#_Toc4079_WPSOffice_Level2)

[案例1：日志监控：](#_Toc24823_WPSOffice_Level3) [14](#_Toc24823_WPSOffice_Level3)

[案例2：时间段和级别监控](#_Toc10291_WPSOffice_Level3) [15](#_Toc10291_WPSOffice_Level3)

[案例3：标签监控（无用，只为测试功能）：](#_Toc739_WPSOffice_Level3) [15](#_Toc739_WPSOffice_Level3)

[案例4：用户画像：地域热力图等功能：](#_Toc21722_WPSOffice_Level3) [15](#_Toc21722_WPSOffice_Level3)

[11. 显示自定义可视化-添加仪表画板](#_Toc19879_WPSOffice_Level2) [15](#_Toc19879_WPSOffice_Level2)

[案例1：日志监控](#_Toc8015_WPSOffice_Level3) [15](#_Toc8015_WPSOffice_Level3)

[12. 对服务器性能进行监控](#_Toc30823_WPSOffice_Level2) [16](#_Toc30823_WPSOffice_Level2)

## 日志标准化：

#### 标准日志

2019-07-30T02:57:51,102 ERROR tag\_weight-lirui-su.bpiu.dmp.usertag.api.monitor Attempting to install template {:manage\_template=>{"template"=>"logstash-\*", "version"=>50001, "settin

**时间** **日志级别 任务名称**-**归属人**-**全类名** **报错详细信息**

#### 标准解析

logstash--filter插件

|  |
| --- |
| filter {  grok {  match => { "message" => "%{YEAR:year}-%{MONTHNUM:month}-%{MONTHDAY:day}.%{HOUR:hour}:%{MINUTE:minute}:%{SECOND:second},(?<mil>[0-9]\*) %{LOGLEVEL:level} (?<modulejobid>[a-z0-9A-Z/\_]+)-(?<owner>[a-z0-9A-Z/\_]+)-(?<fullname>[a-zA-Z0-9/.]\*) (?<detail>.\*)"}  }  } |

#### 解析结果

|  |
| --- |
| {  "owner" => "lirui",  "year" => "2019",  "level" => "ERROR",  "message" => "2019-07-30T02:57:51,102 ERROR tag\_weight-lirui-su.bpiu.dmp.usertag.api.monitor Attempting to install template {:manage\_template=>{\"template\"=>\"logstash-\*\", \"version\"=>50001, \"settin",  "modulejobid" => "tag\_weight",  "minute" => "57",  "second" => "51",  "mil" => "102",  "@timestamp" => 2019-07-31T03:02:53.594Z,  "month" => "07",  "hour" => "02",  "@version" => "1",  "host" => "ip-10-1-12-10.cn-north-1.compute.internal",  "fullname" => "su.bpiu.dmp.usertag.api.monitor",  "detail" => "Attempting to install template {:manage\_template=>{\"template\"=>\"logstash-\*\", \"version\"=>50001, \"settin",  "day" => "30"  } |

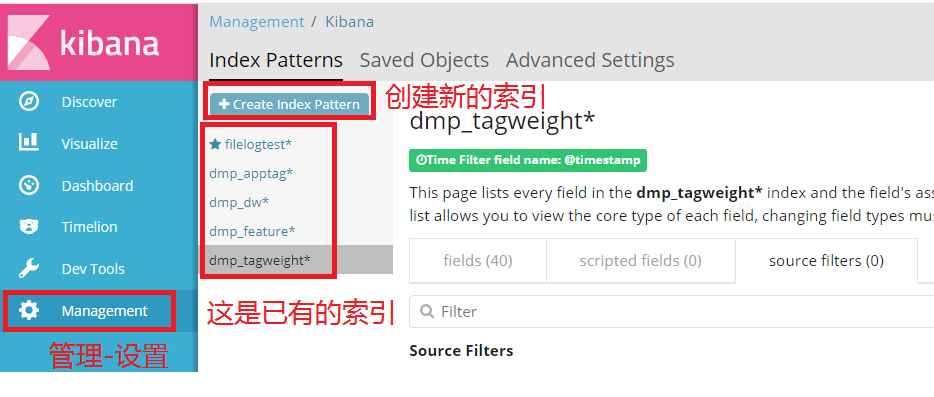
#### ELK框架配置

输入端----过滤修改----输出端----映射----查询过滤----保存模板----可视化（可选）

## 二、kibana使用案例：

#### 索引管理

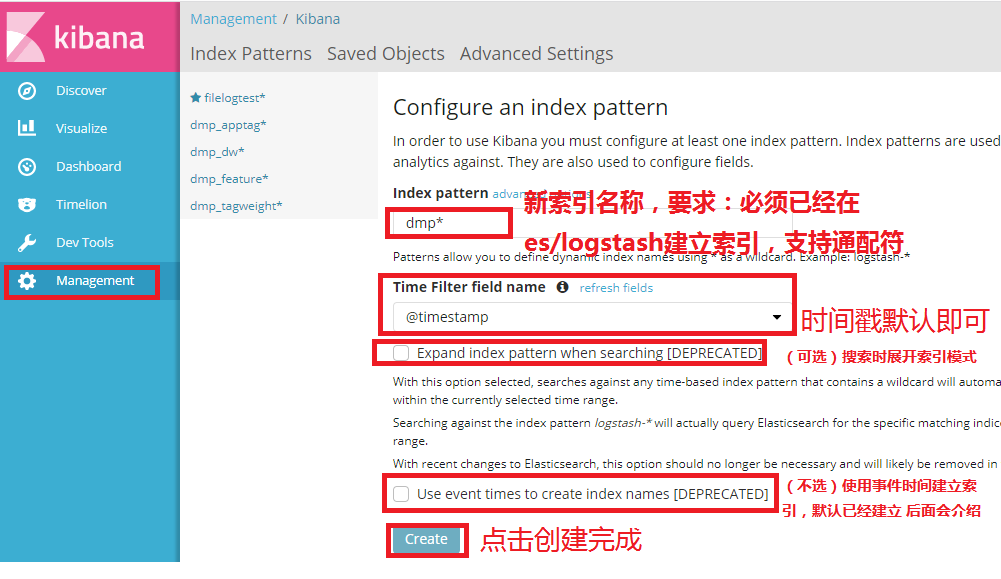
即支持索引的index（类似于mysql的数据库）。



#### 创建新的索引

点击上图中创建新的索引。

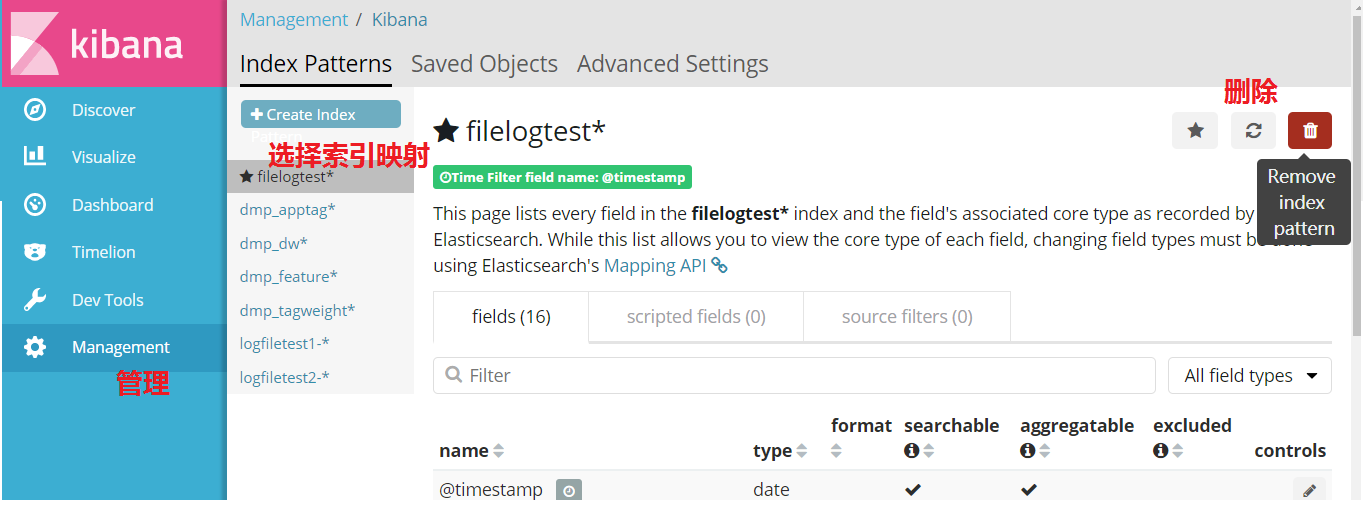
提醒：数据到了es，必须在kibana建立索引映射，才可查询，过滤等操作。



#### 删除不用的索引

管理kibana的es-index映射（此处并不是删除es的的index）

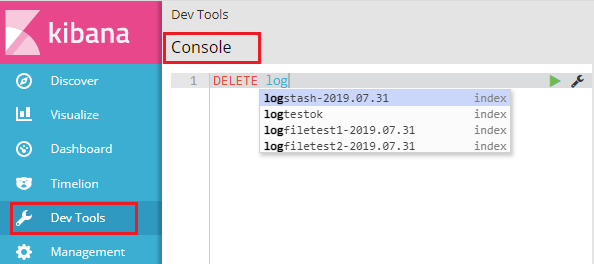
再次添加kibana的es-index映射，查询功能仍然可用。



#### 管理es数据

index，type,

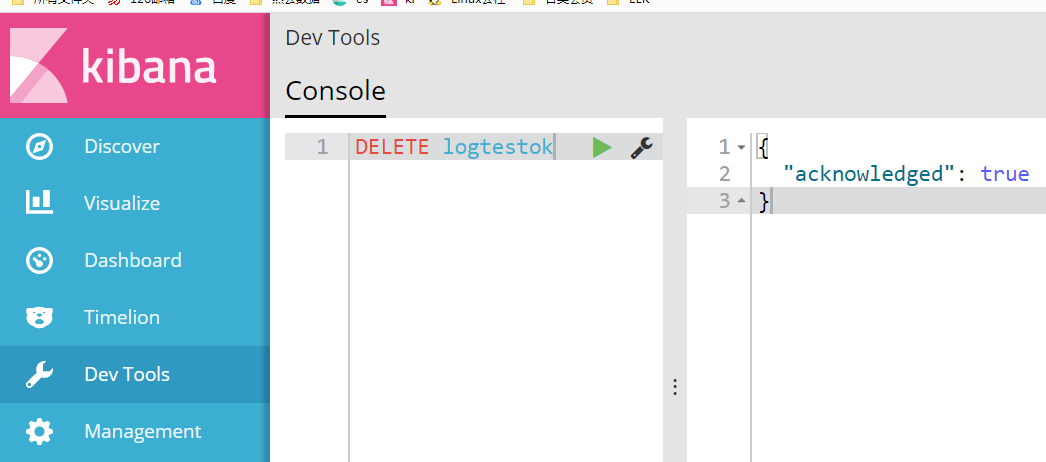
管理es数据，由logtestok这条index信息可知：此处针对是es数据管理，而不是kibana建立的索引，而kibana建立的索引，可以使用Managment界面管理。



删除成功：

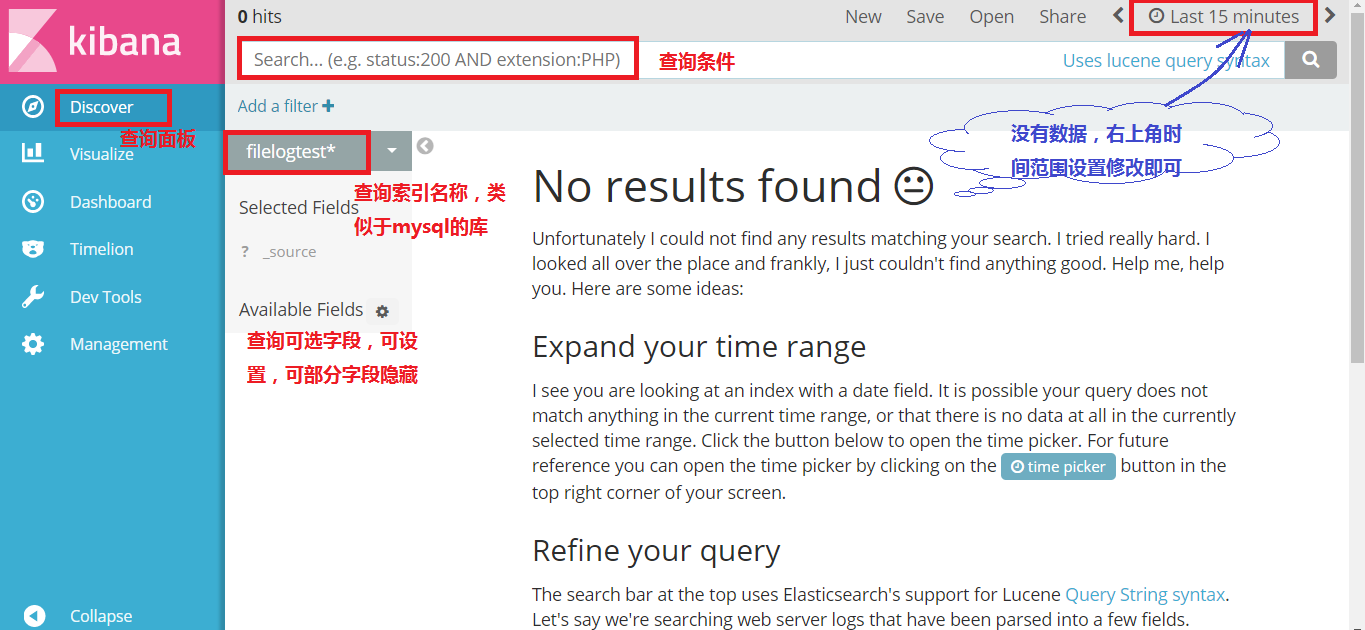
再次添加kibana的es-index映射，查询功能不可用，

且如果在此之间没有数据进来，则不能添加相关kibana的es-index映射。



#### 真正的功能-日志查询

主要是做索引以及多维度的查询过滤，可自定义模板保存等，功能非常强大。



#### 查询案例

（字段均支持通配符\*）：

查询

时间范围：**2019.07.30 —— 2019-07.31**

主机：**ip-10-1-12-10.cn-north-1.compute.internal**（直接写\*10-1-12-10\*通配即可）

工程**：dmp工程**

模块：**feature特征工程库**

任务：**hive定时任务style表**

日志级别：**INFO,WARN,ERROR...**

**各级别日志条数，**

**各级别日志占比，**

**并且过滤级别为ERROR的日志，**

**并查看报错信息**

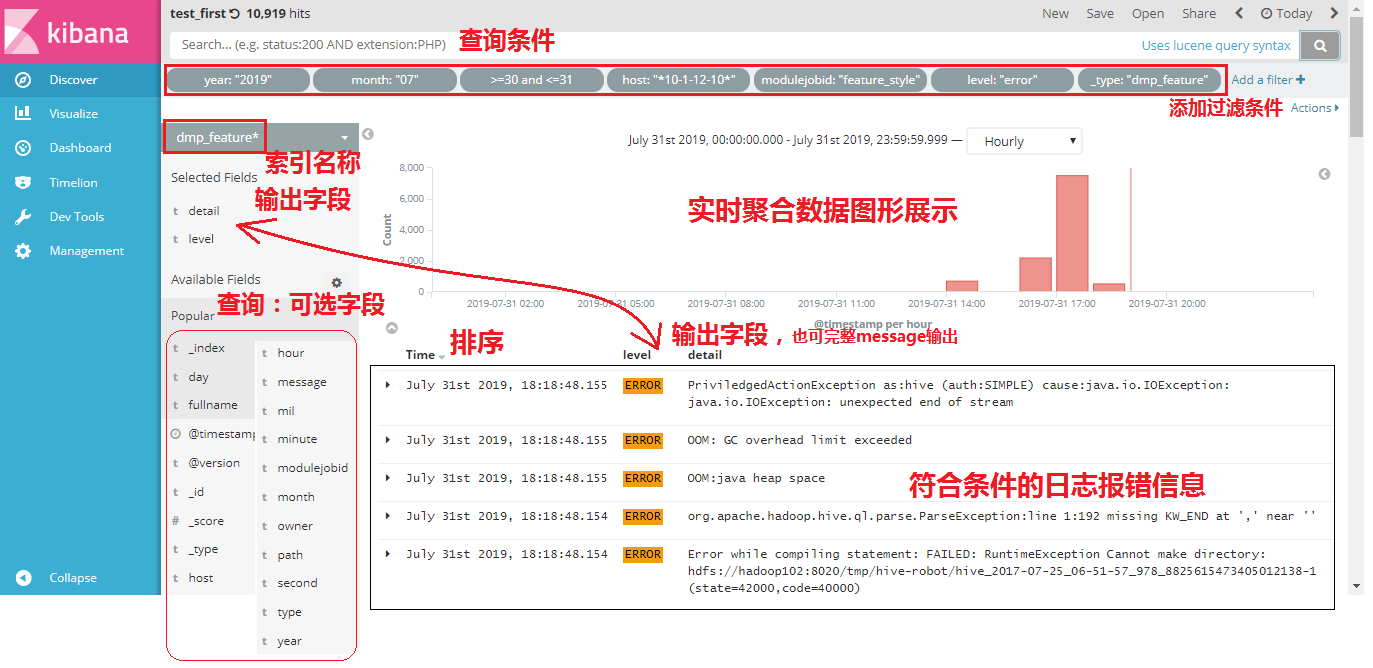
排序:**并按照最近时间排序**

结果过滤：**要求只取级别、全类名、报错信息。**

附属结果输出**：各个时间段内（**粒度自定义即可**）日志条数，报表（**支持下载.csv**）和图形。**

**---------------------------------------------------------------------------------------------------------------------------------**

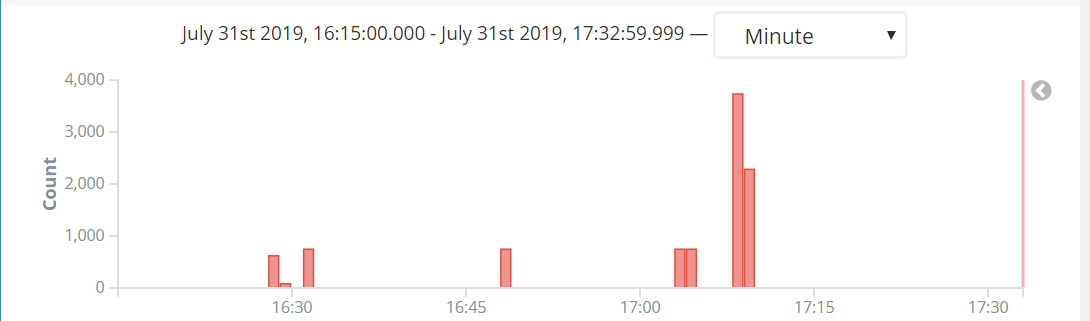
**日志查询结果输出：**



**报表输出：**



**图形输出：**



#### 查询案例

按照es的API查询（再回头对比，发现缺点明显：编程复杂，可读性差，学习成本高，无可视化界面，结果解析速度慢..）

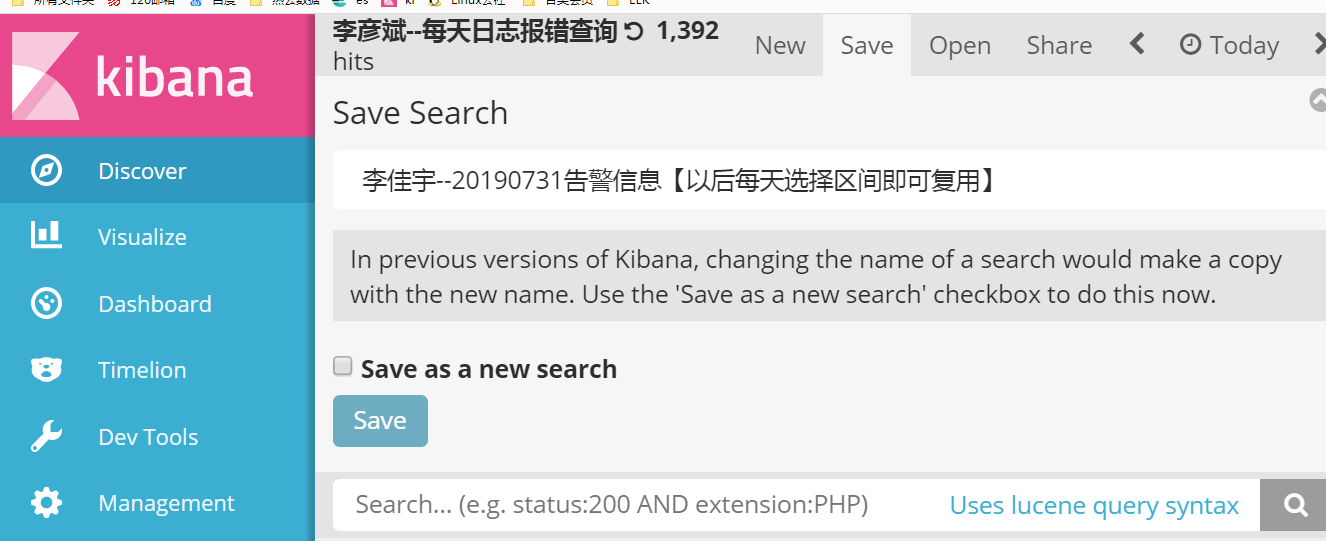
**Elasticsearch request body  如下：**

|  |
| --- |
| {  "version": true,  "size": 500,  "sort": [  {  "@timestamp": {  "order": "desc",  "unmapped\_type": "boolean"  }  }  ],  "query": {  "bool": {  "must": [  {  "match\_all": {}  },  {  "match\_phrase": {  "year": {  "query": "2019"  }  }  },  {  "match\_phrase": {  "month": {  "query": "07"  }  }  },  {  "$state": {  "store": "appState"  },  "exists": {  "field": "day"  }  },  {  "match\_phrase": {  "host": {  "query": "\*10-1-12-10\*"  }  }  },  {  "match\_phrase": {  "modulejobid": {  "query": "feature\_style"  }  }  },  {  "match\_phrase": {  "level": {  "query": "error"  }  }  },  {  "match\_phrase": {  "\_type": {  "query": "dmp\_feature"  }  }  },  {  "range": {  "@timestamp": {  "gte": 1564416000000,  "lte": 1564588799999,  "format": "epoch\_millis"  }  }  }  ],  "must\_not": []  }  },  "\_source": {  "excludes": []  },  "aggs": {  "2": {  "date\_histogram": {  "field": "@timestamp",  "interval": "10m",  "time\_zone": "Asia/Shanghai",  "min\_doc\_count": 1  }  }  },  "stored\_fields": [  "\*"  ],  "script\_fields": {},  "docvalue\_fields": [  "@timestamp"  ],  "highlight": {  "pre\_tags": [  "@kibana-highlighted-field@"  ],  "post\_tags": [  "@/kibana-highlighted-field@"  ],  "fields": {  "\*": {  "highlight\_query": {  "bool": {  "must": [  {  "match\_all": {}  },  {  "match\_phrase": {  "year": {  "query": "2019"  }  }  },  {  "match\_phrase": {  "month": {  "query": "07"  }  }  },  {  "$state": {  "store": "appState"  },  "exists": {  "field": "day"  }  },  {  "match\_phrase": {  "host": {  "query": "\*10-1-12-10\*"  }  }  },  {  "match\_phrase": {  "modulejobid": {  "query": "feature\_style"  }  }  },  {  "match\_phrase": {  "level": {  "query": "error"  }  }  },  {  "match\_phrase": {  "\_type": {  "query": "dmp\_feature"  }  }  },  {  "range": {  "@timestamp": {  "gte": 1564416000000,  "lte": 1564588799999,  "format": "epoch\_millis"  }  }  }  ],  "must\_not": []  }  }  }  },  "fragment\_size": 2147483647  }  } |

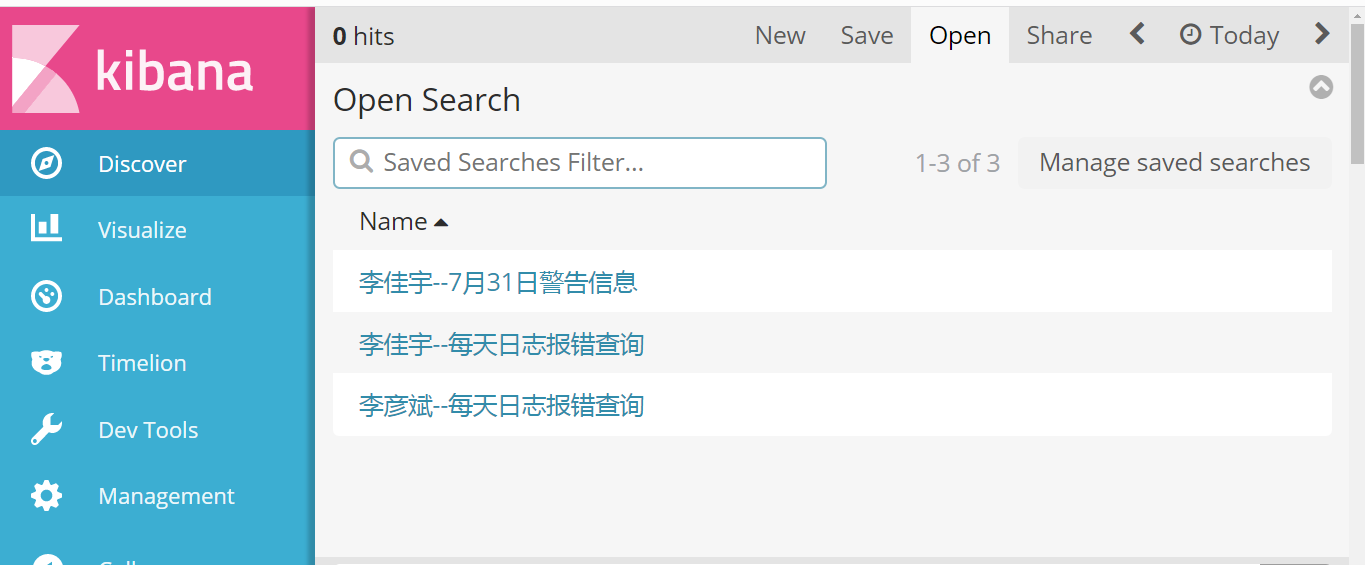
**Elasticsearch response body  如下：**

|  |
| --- |
| {  "took": 160,  "hits": {  "hits": [  {  "\_index": "dmp\_feature-2019.07.31",  "\_type": "dmp\_feature",  "\_id": "AWxHStNGMnKAQ0mk54n9",  "\_version": 1,  "\_score": null,  "\_source": {  "owner": "lijiayu",  "year": "2019",  "level": "ERROR",  "message": "2019-07-31T02:57:51,989 ERROR feature\_style-lijiayu-reyun.bpu.dmp.usertag.api.event Unable to revive connection: http://10.1.12.10:9200/dfhsj",  "type": "dmp\_feature",  "modulejobid": "feature\_style",  "minute": "57",  "second": "51",  "path": "/home/ec2-user/dmp/jiayu/elk/testlogs/lijiayu\_log/logfile2",  "mil": "989",  "@timestamp": "2019-07-31T09:09:41.812Z",  "month": "07",  "hour": "02",  "@version": "1",  "host": "ip-10-1-12-10.cn-north-1.compute.internal",  "fullname": "reyun.bpu.dmp.usertag.api.event",  "detail": "Unable to revive connection: http://10.1.12.10:9200/dfhsj",  "day": "31"  },  "fields": {  "@timestamp": [  1564564181812  ]  },  "highlight": {  "month": [  "@kibana-highlighted-field@07@/kibana-highlighted-field@"  ],  "year": [  "@kibana-highlighted-field@2019@/kibana-highlighted-field@"  ],  "level": [  "@kibana-highlighted-field@ERROR@/kibana-highlighted-field@"  ],  "host": [  "ip-@kibana-highlighted-field@10@/kibana-highlighted-field@-@kibana-highlighted-field@1@/kibana-highlighted-field@-@kibana-highlighted-field@12@/kibana-highlighted-field@-@kibana-highlighted-field@10@/kibana-highlighted-field@.cn-north-1.compute.internal"  ],  "modulejobid": [  "@kibana-highlighted-field@feature\_style@/kibana-highlighted-field@"  ]  },  **此处省略几万行....** |

#### 保存本次查询逻辑为模板

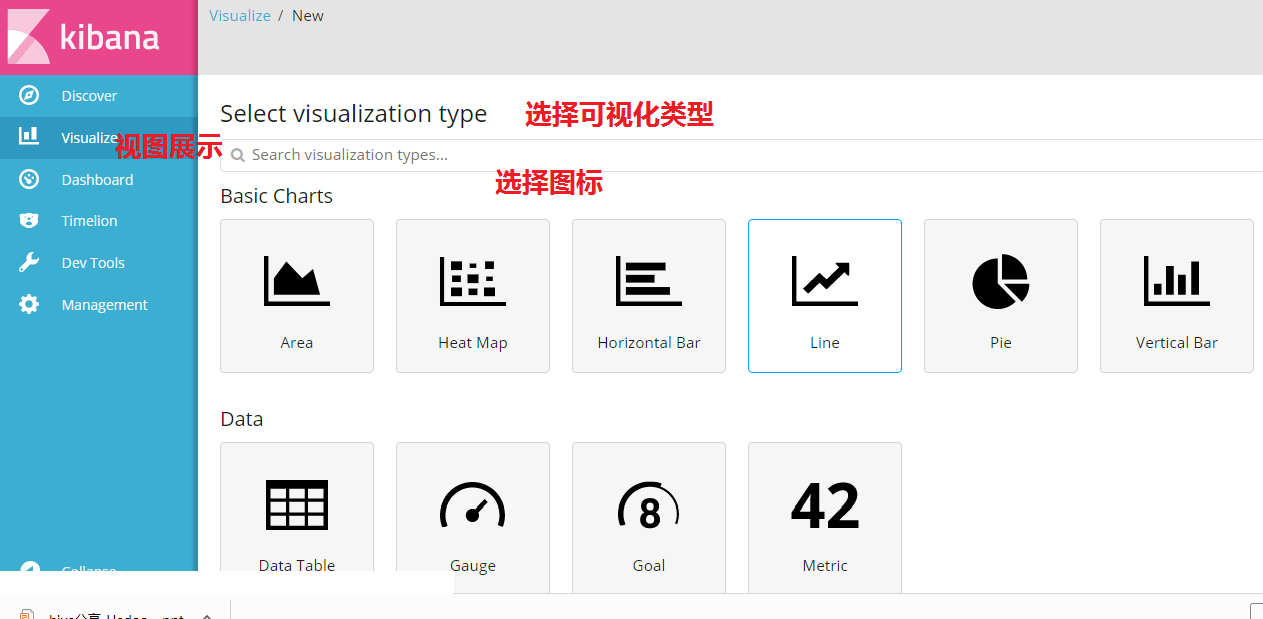


#### 打开历史保存模板，快速查询



#### 视图展示

可根据需求选择不同的可视化图标工具(很好用):



图表模板支持：

【基本图标类，偏向直观表格类图形，维度变化频次低，】

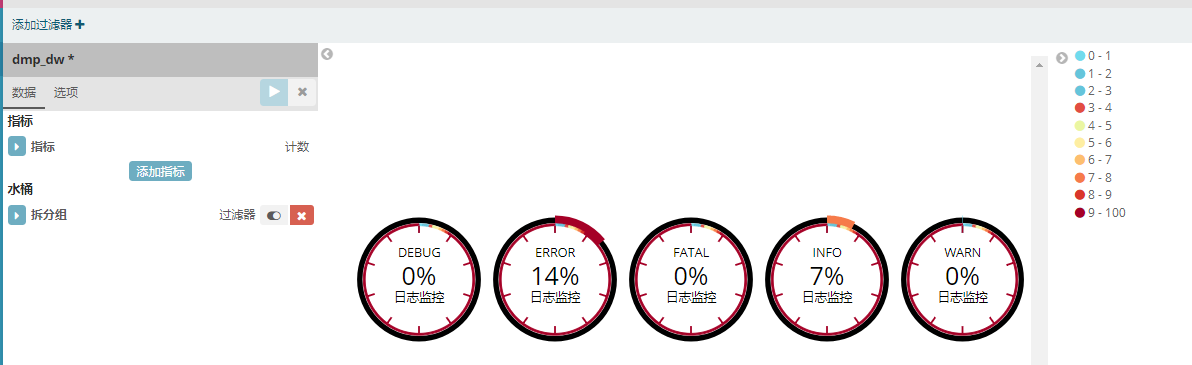
【数据展示类，形象的数据展示，管理类聚合数据选用】

【涉及到地图数据分布类,用户群体等，业务系统日志选用】

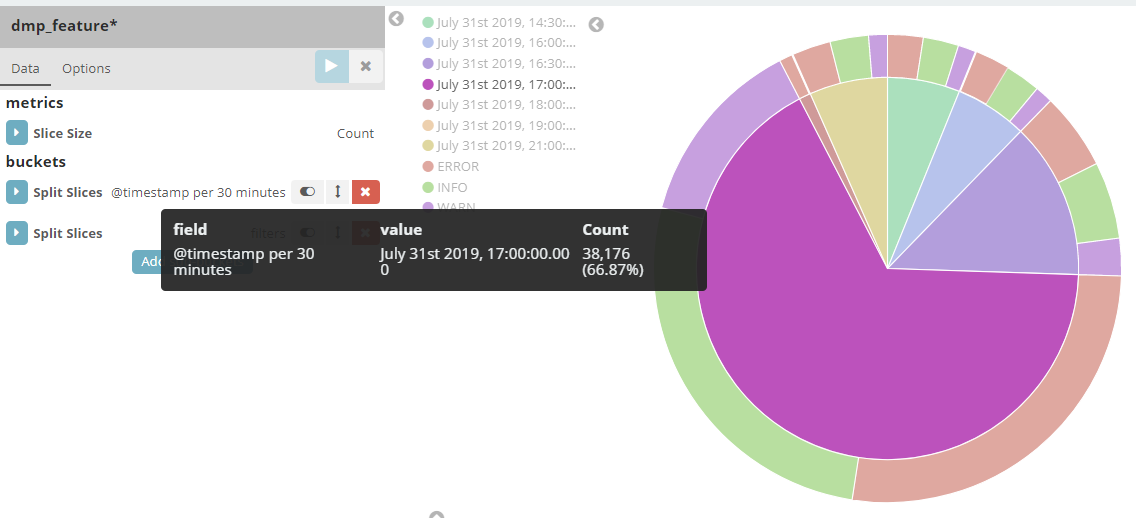
【时间序列】

【用户画像类，实例场景】

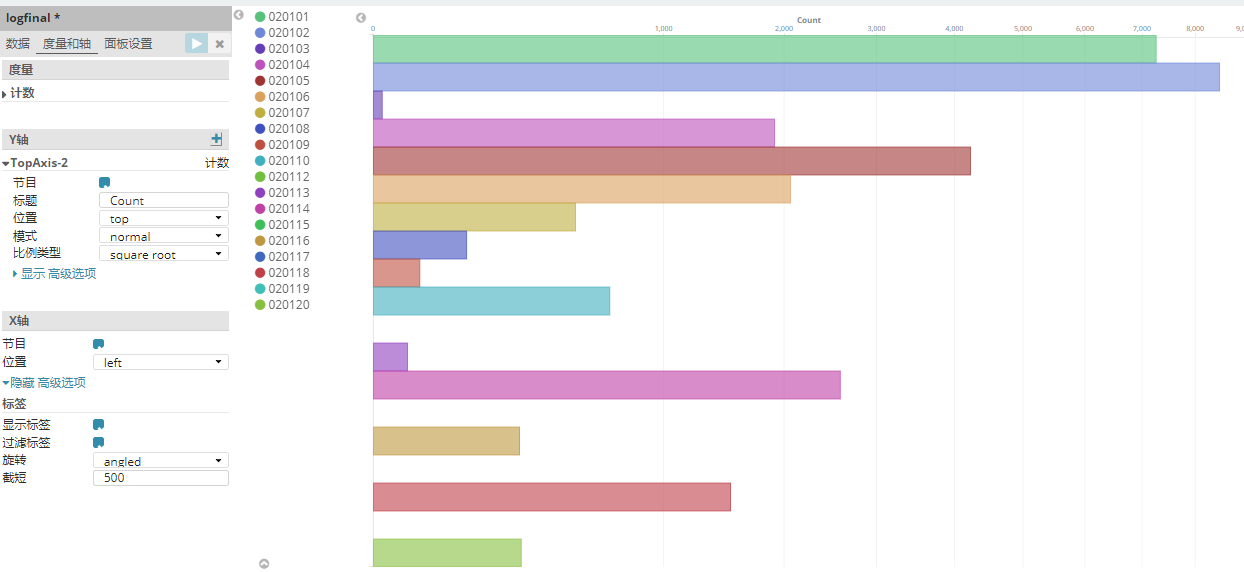
**案例1：日志监控：**



**案例2：时间段和级别监控**



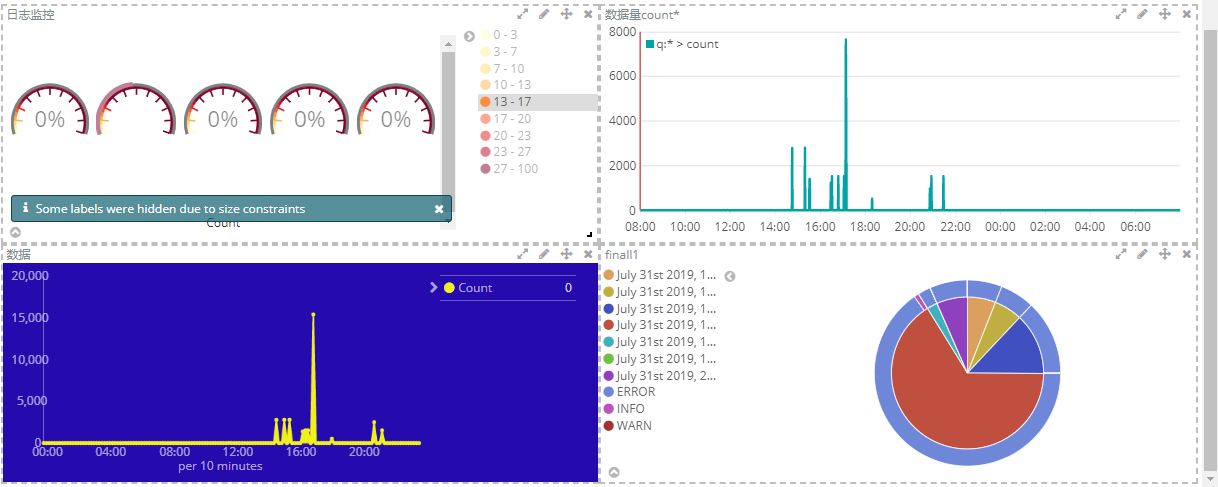
**案例3：标签监控（无用，只为测试功能）：**



#### **案例4：用户画像：地域热力图等功能：**

#### 显示自定义可视化-添加仪表画板

**案例1：日志监控**



#### 对服务器性能进行监控

Timelion结合Metricbeat（版本5.6.2）：(历史对比，移动平均线...)

