ELK Logtrail插件使用说明

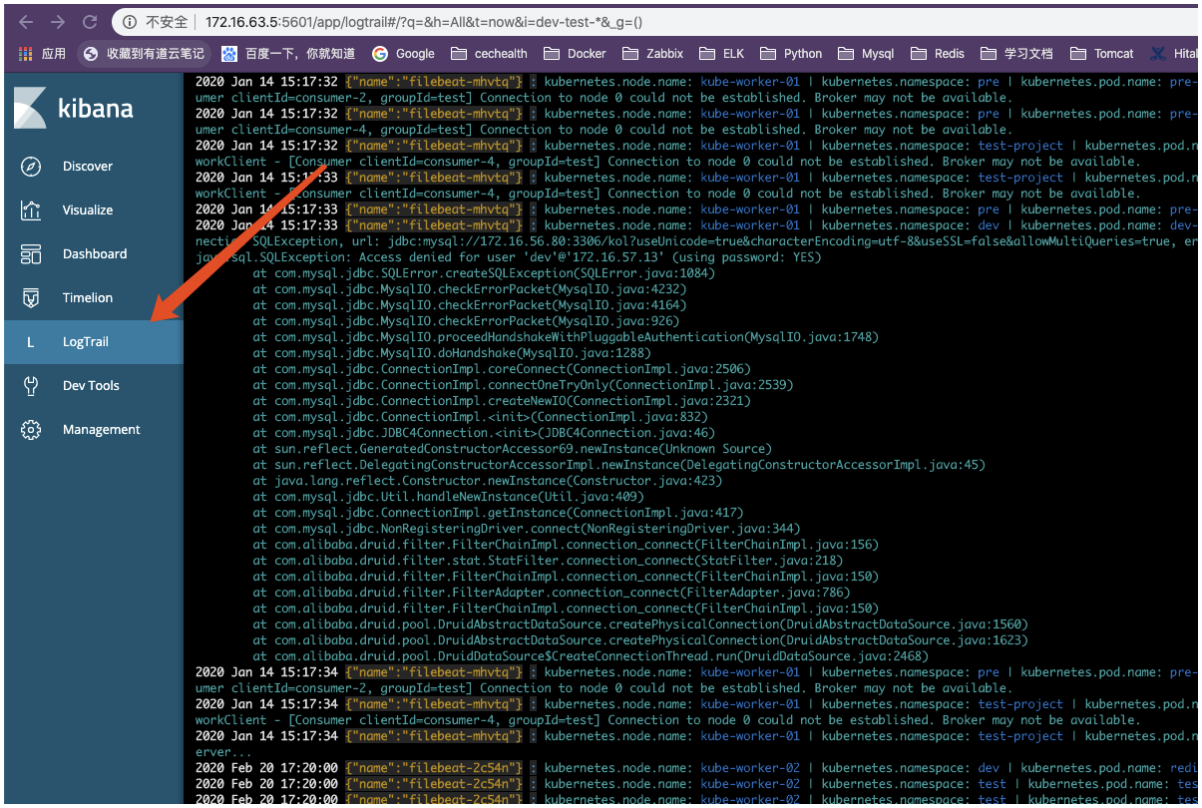
1、目的

为了方便开发人员更直观快捷的查看业务日志，特安装logtrail插件，针对每个index配置相关规则。特编写此文档，介绍如何使用该插件进行查看相关日志。

2、使用说明

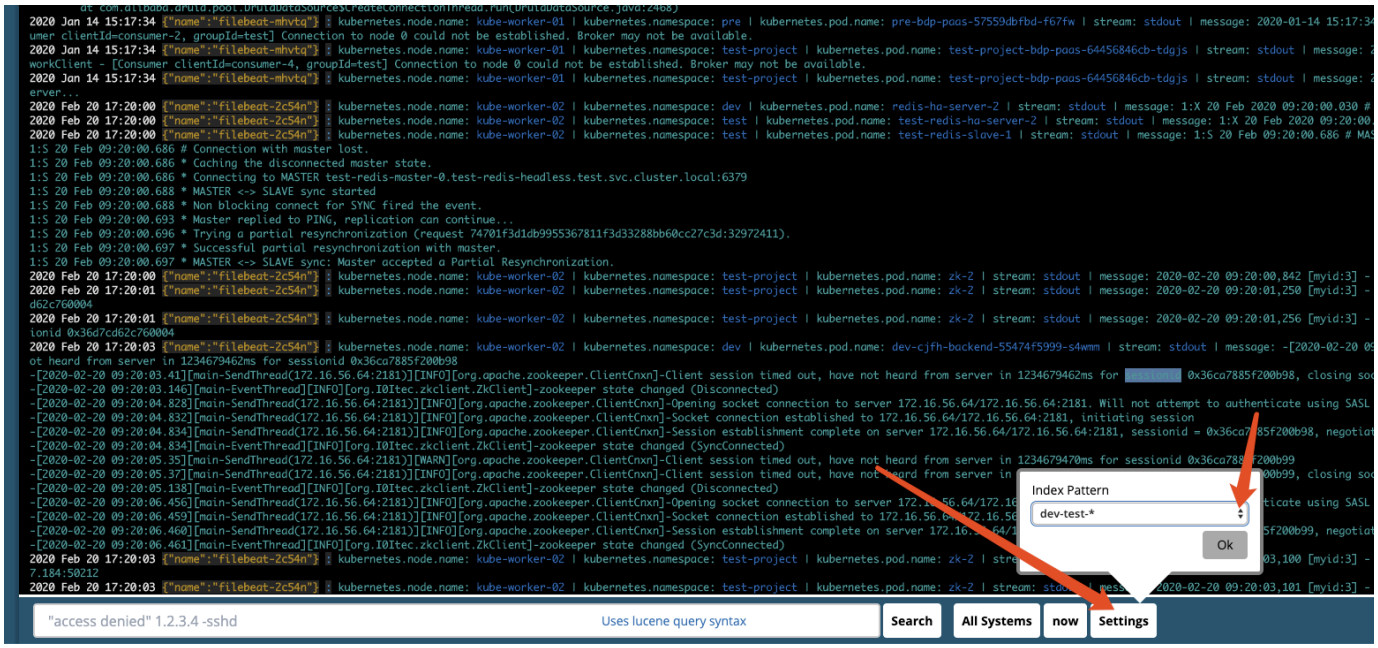
2.1 地址

http://172.16.63.5:5601/



2.2 选择索引

点击下方Settings，选择要查看的索引名称，然后点击OK，如图：



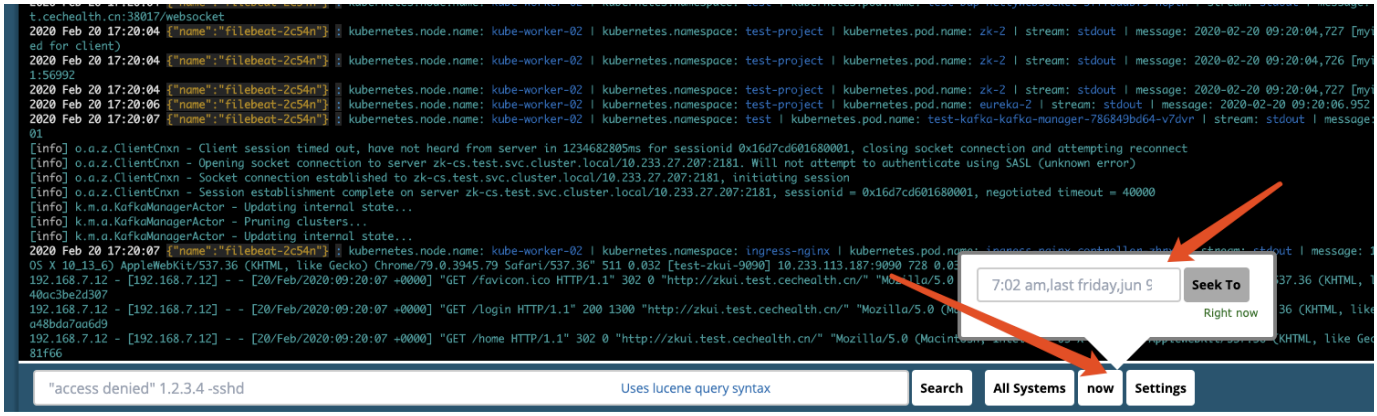
Index名称说明：

索引名	日志说明
dev-test-*	开发、测试、预生产环境K8S应用日志
k8s-prod-*	生产环境K8S应用日志

mysql-slow-log-*	生产环境数据库慢查询日志

2.3 选择时间

点击下方now按钮，填写时间，如查看当前时间，可输入 now；如查看上午11:00，可输入11:00 am；如查看上周五，可输入last friday，以此类推。然后点击Seek To即可。如图：

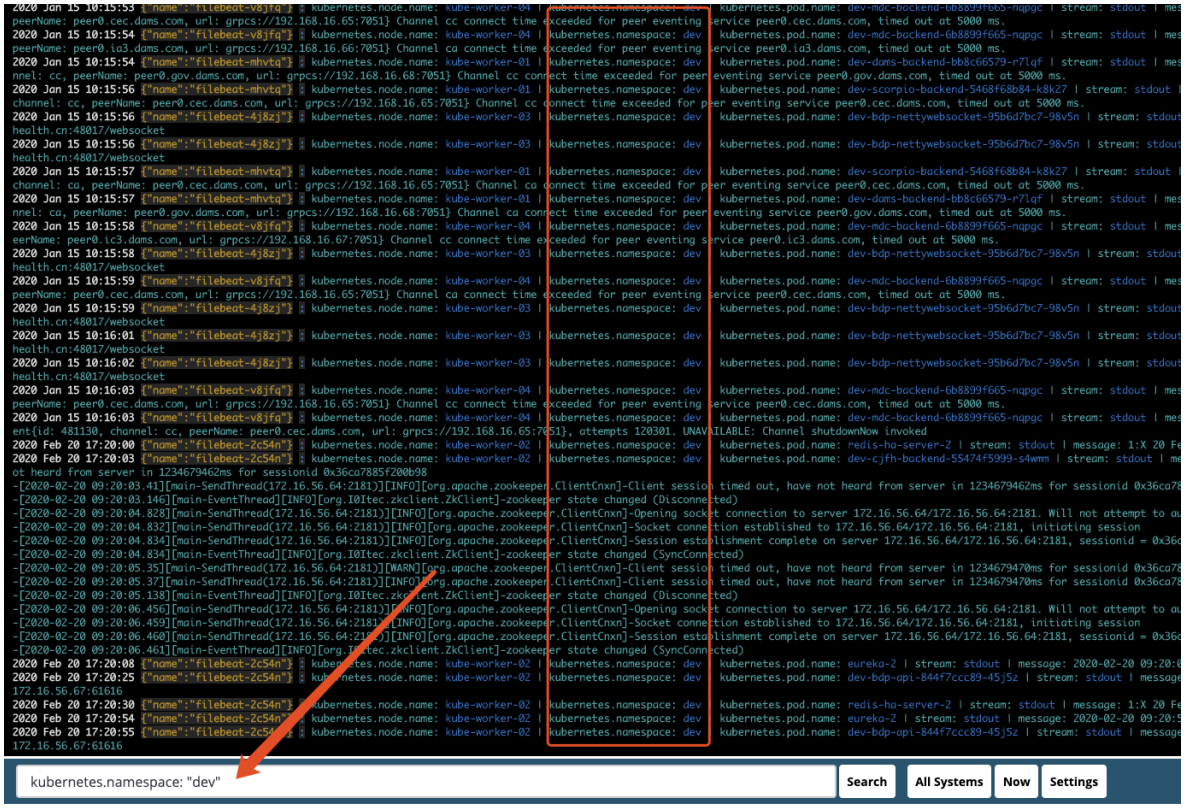


2.4 输入字段查询

在下方输入框，输入要查询的内容（Uses lucene query syntax），点击Search

k8s命名空间	对应环境
dev	开发环境
test	测试环境
pre	预生产环境
prod	生产环境

a. 如需要查看k8s命名空间为dev 的相关日志，可在输入框输入：kubernetes.namespace:dev，然后点击Search，即可进行查询，也可以直接双击屏幕中对应字段，也会自动显示在输入框中，并进行搜索



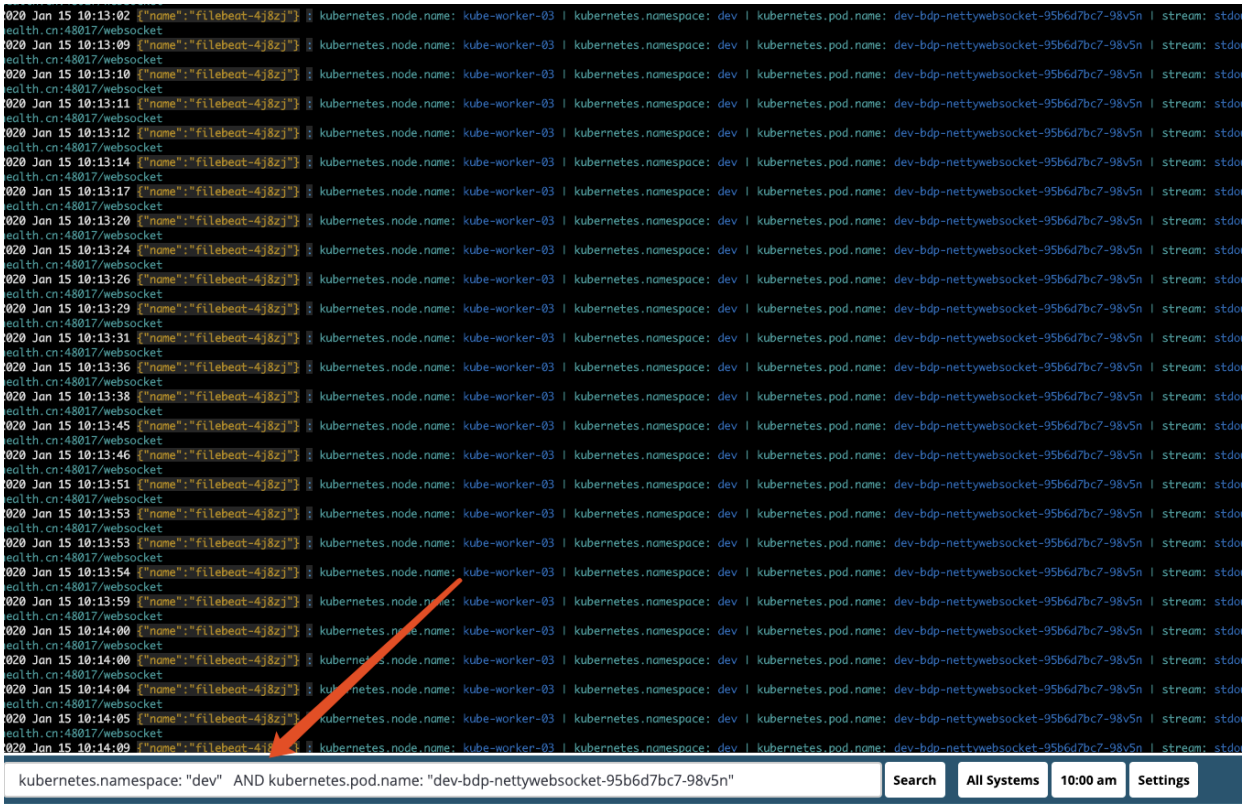
b. 如需要查看namespace为dev对应为开发环境，应用为bdp-nettywebsocket 的pod日志，可输入：

```
kubernetes.namespace: "dev" AND kubernetes.pod.name:
dev-bdp-nettywebsocket*  //pod
```

同理需要查看测试环境的应用bdp-nettywebsocket 的pod日志，可输入：

```
kubernetes.namespace: "test" AND kubernetes.pod.name:
test-bdp-nettywebsocket*
```

【备注】注意必须使用大写。如果不使用AND，而是and，可能会被单做关键词进行搜索！



c. 如果不知道完整pod.name 的情况下可进行模糊查询，如需要查看namespace为dev，应用为dev-bdp-api的日志，可输入：

```
kubernetes.namespace: "dev" AND kubernetes.pod.name: dev-bdp-api*
```

【备注】：使用通配符的情况，切记不要用引号引起需要模糊查询的字段，否则会查询不到

2.5 查询语法

其他查询语法遵循Lucene查询语法，可参考《Uses lucene query syntax》，下面简单说明一些查询语法。

Kibana使用的查询语法是Lucene的查询语法，这里在使用Kibana的同事一定要注意，不然，在进行搜索的时候，你会抓狂的。
下面了解下Lucene的查询语法，了解了Lucene的查询语法也就知道了改如何使用Kibana的使用方式
Lucene查询语法以可读的方式书写，然后使用JavaCC进行词法转换，转换成机器可识别的查询。

2.5.1 词语查询，语法如下

```
"here","there""here,there"
```

2.5.2 字段查询，语法如下

```
tag:there tag:"there are"
```

搜索语句是需要加上双引号，否则

```
tag:there are
```

就意味着，搜索tag为there，或者包含are关键字的文档

2.5.3 修饰符查询，通过增加修饰，从而扩大查询的范围。

```
?:
*:0


?tere
therewhere
test*
testteststester
```

2.5.4 模糊词查询，就是在词语后面加上符号~。语法如下

```
he~
herhei
~[0-1]10.5
he~0.8
```

2.5.5 邻近词查询，语法如下

```
"here there"~10
"here","there"

"here wowo wowo there""here,wowow,wowow,there"
```

2.5.6
范围查询，可以指定最大值和最小值，会自动查找在这之间的文档。如果是单词，则会按照字典顺序搜索。

```
{}
[]


grade8060

grade:{60,80]
nameAC
name:{A,C}
```

2.5.7 词语相关度查询

```
^
jarkarta
jakarta apache

jakarta^4 apache
```

2.5.8 布尔操作符

```
AND
AND&&
ANDand
ab
a AND b

a && b
OR
OR||
ab
a OR b

a || b
NOT
NOT!
ab
a NOT b

a && !b
kibanatest
NOT test
+
tom
+tom
AND
-
tom
-tom
NOT


abc
a AND (b OR c)
ab
title:(+a +"b")
```

2.5.9 转义字符

```
Lucene
+ - && || ! ( ) { } [ ] ^ " ~ * ? : \
 (1+1):2 \
\(1\+1\)\:2
```

2.5.10 参考文档

cnblogs.com/xing901022/p/4974977.html

segmentfault.com/a/1190000002972420

3.Logtrail安装配置

1. 下载跟kibana对应版本的logtrail插件，已下载并上传至(172.16.56.143:/opt/cechealth/files/7/x86_64/logtrail-6.7.1-0.1.31.zip)

2. 将logtrail-6.7.1-0.1.31.zip解压至kibana服务器的/usr/share/kibana/plugins/ 目录下即可

```
[root@es-5 plugins]# pwd
/usr/share/kibana/plugins
[root@es-5 plugins]# ll
总用量 0
drwxr-xr-x 5 root root 111 4月   1 17:19 logtrail
[root@es-5 plugins]# ll logtrail/
总用量 24
-rw-r--r--  1 root root   523 1月   7 16:22 index.js
-rw-r--r--  1 root root 10745 1月  14 11:19 logtrail.json
drwxr-xr-x 30 root root  4096 1月   7 16:22 node_modules
-rw-r--r--  1 root root   750 1月   7 16:22 package.json
drwxr-xr-x  5 root root    78 1月   7 16:22 public
drwxr-xr-x  3 root root    20 1月   7 16:22 server
[root@es-5 plugins]#
```

3. 修改logtrail.json

- 可以通过编辑位于./plugins/logtrail目录中的logtrail.json文件中的下列字段来配置 Logtrail。
- default_index- 存储syslog事件的Elasticsearch索引(默认： 在使用logstash-*以外的索引 NAME 时，确保在logstash-*索引中创建了相应的. raw 字段。
- default_time_range_in_days- 使用查找按钮指定时间时搜索的默认时间范围(以天为单位)。 例如：30表示logtrail将只在最近 30天中搜索，除非使用 Seek button指定时间。 值 0表示logtrail将在默认情况下在所有可用日志中搜索。
- display_timezone- 在 事件查看器 中显示时间戳的时区。 比如America/Los_Angeles默认值local将使用浏览器的时区。Seek To弹出式菜单中指定的时间将始终使用浏览器时区。
- display_timestamp_format- 在 事件查看器 中显示时间戳的格式。 有关有效值的列表，请参考这里的。
- fields- 编辑这里参数以将事件字段映射到logtrail字段中
    - timestamp- 映射到由logstash插入的@timestamp 字段。 这将用于内部查询。 Logtrail建议 @timestamp 以格式存储在中。
    - hostname- 接收事件的主机名。 也被主机名筛选器使用。 Hostname字段的类型应为关键字。 更多信息签出主机名字段需要为关键字类型。
    - program- 生成这里事件的程序。
    - message- 实际事件消息。 这里字段将被搜索使用。
- 如果事件字段名称为 @timestamp, 主机，进程，则映射应为

```
"mapping" : {
 "timestamp" : "@timestamp",
 "hostname" : "host",
 "program": "process",
 "message": "message" }
```

- 默认情况下，事件视图中显示的每一行都是格式：display_timestamp hostname program:message
- message_format- 用于添加附加字段以显示日志事件。 有关详细信息，请参阅添加附加字段。
- color_mapping- 基于字段值的颜色代码消息。 有关详细信息，请参阅颜色代码。
- logtrail.json中的任何更改都需要重新启动 Kibana
- Logtrail可以从Elasticsearch而不是 文件系统 读取logtrail.json配置。 这将在跨多个安装共享相同配置时很有用。 有关更多信息，请参考来自服务器的配置 Logtrail。

- 参考logtrail-config-examplesrepo 示例配置
- 从 Windows。Java。python。PHP。Perl。ruby。Android。Docker。.NET 中的&事件可以使用syslog协议进行传送。
- 有关更多配置选项，请参阅Papertrail配置帮助()。
- bash/fluentd还可以用于将事件传送到 ES，而字段可以使用logtrail.json中的fields参数进行映射

目前的logtrail.json配置：

```
{
  "version" : 2,
  "index_patterns" : [
    {
      "es": {
        "default_index": "dev-test-*",
        "allow_url_parameter": false
      },
      "tail_interval_in_seconds": 10,
      "es_index_time_offset_in_seconds": 0,
      "display_timezone": "local",
      "display_timestamp_format": "YYYY MMM DD HH:mm:ss",
      "max_buckets": 500,
      "default_time_range_in_days" : 7,
      "max_hosts": 100,
      "max_events_to_keep_in_viewer": 5000,
      "default_search": "",
      "fields" : {
        "mapping" : {
            "timestamp" : "@timestamp",
            "hostname" : "host",
            "program": "process",
            "message": "message"
        },
        "message_format": "kubernetes.node.name: {{{kubernetes.node.name}}}
| kubernetes.namespace: {{{kubernetes.namespace}}} | kubernetes.pod.name:
{{{kubernetes.pod.name}}} | stream: {{{stream}}} | message: {{{message}}}",
        "keyword_suffix" : "keyword"
      },
      "color_mapping" : {
         "field" : "stream",
  "mapping": {
                "stderr": "#FF0000",
                "WARN": "#FFEF96",
                "DEBUG": "#B5E7A0",
                "TRACE": "#CFE0E8",
                "stdout": "#339999"
            }
      }
    },{
      "es": {
        "default_index": "firewall-*",
        "allow_url_parameter": false
      },
      "tail_interval_in_seconds": 10,
      "es_index_time_offset_in_seconds": 0,
```

```
    "display_timezone": "local",
    "display_timestamp_format": "YYYY MMM DD HH:mm:ss",
    "max_buckets": 500,
    "default_time_range_in_days" : 7,
    "max_hosts": 100,
    "max_events_to_keep_in_viewer": 5000,
    "default_search": "",
    "fields" : {
      "mapping" : {
          "timestamp" : "@timestamp",
          "hostname" : "host",
          "program": "process",
          "message": "message"
      },
      "message_format": "| message: {{{message}}}",
      "keyword_suffix" : "keyword"
    },
    "color_mapping" : {
"mapping": {
              "ERROR": "#FF0000",
              "WARN": "#FFEF96",
              "DEBUG": "#B5E7A0",
              "TRACE": "#CFE0E8",
              "INFO": "#339999"
          }
    }
  },{
    "es": {
      "default_index": "history-log-*",
      "allow_url_parameter": false
    },
    "tail_interval_in_seconds": 10,
    "es_index_time_offset_in_seconds": 0,
    "display_timezone": "local",
    "display_timestamp_format": "YYYY MMM DD HH:mm:ss",
    "max_buckets": 500,
    "default_time_range_in_days" : 7,
    "max_hosts": 100,
    "max_events_to_keep_in_viewer": 5000,
    "default_search": "",
    "fields" : {
      "mapping" : {
          "timestamp" : "@timestamp",
          "hostname" : "host",
          "program": "process",
          "message": "message"
      },
      "message_format": "| message: {{{message}}}",
      "keyword_suffix" : "keyword"
    },
    "color_mapping" : {
"mapping": {
              "ERROR": "#FF0000",
```

```
                "WARN": "#FFEF96",
                "DEBUG": "#B5E7A0",
                "TRACE": "#CFE0E8",
                "INFO": "#339999"
            }
      }
    },{
      "es": {
        "default_index": "ips-*",
        "allow_url_parameter": false
      },
      "tail_interval_in_seconds": 10,
      "es_index_time_offset_in_seconds": 0,
      "display_timezone": "local",
      "display_timestamp_format": "YYYY MMM DD HH:mm:ss",
      "max_buckets": 500,
      "default_time_range_in_days" : 7,
      "max_hosts": 100,
      "max_events_to_keep_in_viewer": 5000,
      "default_search": "",
      "fields" : {
        "mapping" : {
            "timestamp" : "@timestamp",
            "hostname" : "host",
            "program": "process",
            "message": "message"
        },
        "message_format": "Severity: {{{Severity}}} | SrcIPAddr:
{{{SrcIPAddr}}} | SrcPort: {{{SrcPort}}} | DstIPAddr: {{{DstIPAddr}}}|
DstPort: {{{DstPort}}} |message: {{{message}}}",
        "keyword_suffix" : "keyword"
      },
      "color_mapping" : {
         "field" : "Severity",
  "mapping": {
                "CRITICAL": "#FF0000",
                "HIGH": "#FFEF96",
                "MEDIUM": "#B5E7A0",
                "LOW": "#CFE0E8"
            }
      }
    },{
      "es": {
        "default_index": "k8s-prod-*",
        "allow_url_parameter": false
      },
      "tail_interval_in_seconds": 10,
      "es_index_time_offset_in_seconds": 0,
      "display_timezone": "local",
      "display_timestamp_format": "YYYY MMM DD HH:mm:ss",
      "max_buckets": 500,
      "default_time_range_in_days" : 7,
      "max_hosts": 100,
```

```
      "max_events_to_keep_in_viewer": 5000,
      "default_search": "",
      "fields" : {
        "mapping" : {
            "timestamp" : "@timestamp",
            "hostname" : "host",
            "program": "process",
            "message": "message"
        },
        "message_format": "kubernetes.node.name: {{{kubernetes.node.name}}}
| kubernetes.namespace: {{{kubernetes.namespace}}} | kubernetes.pod.name:
{{{kubernetes.pod.name}}} | stream: {{{stream}}} | message: {{{message}}}",
        "keyword_suffix" : "keyword"
      },
      "color_mapping" : {
         "field" : "stream",
  "mapping": {
                "stderr": "#FF0000",
                "WARN": "#FFEF96",
                "DEBUG": "#B5E7A0",
                "TRACE": "#CFE0E8",
                "stdout": "#339999"
            }
      }
    },{
      "es": {
        "default_index": "mysql-slow-log-*",
        "allow_url_parameter": false
      },
      "tail_interval_in_seconds": 10,
      "es_index_time_offset_in_seconds": 0,
      "display_timezone": "local",
      "display_timestamp_format": "YYYY MMM DD HH:mm:ss",
      "max_buckets": 500,
      "default_time_range_in_days" : 7,
      "max_hosts": 100,
      "max_events_to_keep_in_viewer": 5000,
      "default_search": "",
      "fields" : {
        "mapping" : {
            "timestamp" : "@timestamp",
            "hostname" : "host",
            "program": "process",
            "message": "message"
        },
        "message_format": "mysql.slowlog.user: {{{mysql.slowlog.user}}} |
query_time: {{{mysql.slowlog.query_time.sec}}} | mysql.slowlog.query:
{{{mysql.slowlog.query}}} | message: {{{message}}}",
        "keyword_suffix" : "keyword"
      },
      "color_mapping" : {
  "mapping": {
                "ERROR": "#FF0000",
```

```
                "WARN": "#FFEF96",
                "DEBUG": "#B5E7A0",
                "TRACE": "#CFE0E8",
                "INFO": "#339999"
            }
      }
    },{
      "es": {
        "default_index": "openstack-cinder-log-*",
        "allow_url_parameter": false
      },
      "tail_interval_in_seconds": 10,
      "es_index_time_offset_in_seconds": 0,
      "display_timezone": "local",
      "display_timestamp_format": "YYYY MMM DD HH:mm:ss",
      "max_buckets": 500,
      "default_time_range_in_days" : 7,
      "max_hosts": 100,
      "max_events_to_keep_in_viewer": 5000,
      "default_search": "",
      "fields" : {
        "mapping" : {
            "timestamp" : "@timestamp",
            "hostname" : "host",
            "program": "process",
            "message": "message"
        },
        "message_format": "fields.name: {{{fields.name}}} | message:
{{{message}}}",
        "keyword_suffix" : "keyword"
      },
      "color_mapping" : {
  "mapping": {
                "ERROR": "#FF0000",
                "WARN": "#FFEF96",
                "DEBUG": "#B5E7A0",
                "TRACE": "#CFE0E8",
                "INFO": "#339999"
            }
      }
    },{
      "es": {
        "default_index": "openstack-cinder-scheduler-log-*",
        "allow_url_parameter": false
      },
      "tail_interval_in_seconds": 10,
      "es_index_time_offset_in_seconds": 0,
      "display_timezone": "local",
      "display_timestamp_format": "YYYY MMM DD HH:mm:ss",
      "max_buckets": 500,
      "default_time_range_in_days" : 7,
      "max_hosts": 100,
      "max_events_to_keep_in_viewer": 5000,
```

```
      "default_search": "",
      "fields" : {
        "mapping" : {
            "timestamp" : "@timestamp",
            "hostname" : "host",
            "program": "process",
            "message": "message"
        },
        "message_format": "fields.name: {{{fields.name}}} | message:
{{{message}}}",
        "keyword_suffix" : "keyword"
      },
      "color_mapping" : {
  "mapping": {
                "ERROR": "#FF0000",
                "WARN": "#FFEF96",
                "DEBUG": "#B5E7A0",
                "TRACE": "#CFE0E8",
                "INFO": "#339999"
            }
      }
    },{
      "es": {
        "default_index": "openstack-neutron-log-*",
        "allow_url_parameter": false
      },
      "tail_interval_in_seconds": 10,
      "es_index_time_offset_in_seconds": 0,
      "display_timezone": "local",
      "display_timestamp_format": "YYYY MMM DD HH:mm:ss",
      "max_buckets": 500,
      "default_time_range_in_days" : 7,
      "max_hosts": 100,
      "max_events_to_keep_in_viewer": 5000,
      "default_search": "",
      "fields" : {
        "mapping" : {
            "timestamp" : "@timestamp",
            "hostname" : "host",
            "program": "process",
            "message": "message"
        },
        "message_format": "fields.name: {{{fields.name}}} | message:
{{{message}}}",
        "keyword_suffix" : "keyword"
      },
      "color_mapping" : {
  "mapping": {
                "ERROR": "#FF0000",
                "WARN": "#FFEF96",
                "DEBUG": "#B5E7A0",
                "TRACE": "#CFE0E8",
                "INFO": "#339999"
```

```
            }
        }
    },{
        "es": {
          "default_index": "openstack-nova-compute-log-*",
          "allow_url_parameter": false
        },
        "tail_interval_in_seconds": 10,
        "es_index_time_offset_in_seconds": 0,
        "display_timezone": "local",
        "display_timestamp_format": "YYYY MMM DD HH:mm:ss",
        "max_buckets": 500,
        "default_time_range_in_days" : 7,
        "max_hosts": 100,
        "max_events_to_keep_in_viewer": 5000,
        "default_search": "",
        "fields" : {
          "mapping" : {
              "timestamp" : "@timestamp",
              "hostname" : "host",
              "program": "process",
              "message": "message"
          },
          "message_format": "fields.name: {{{fields.name}}} | message:
{{{message}}}",
          "keyword_suffix" : "keyword"
        },
        "color_mapping" : {
  "mapping": {
                "ERROR": "#FF0000",
                "WARN": "#FFEF96",
                "DEBUG": "#B5E7A0",
                "TRACE": "#CFE0E8",
                "INFO": "#339999"
            }
        }
```

```
        }
      ]
    }
```

```
"fields": {
// mapping的key是logtrail控制台显示的属性，mapping的value是对应kibana显示filebeat的属性
// 这个映射的意思就是，告诉logtrail我们要把kibana的哪些日志拿来展示
```