# ELK Logtrail插件使用说明



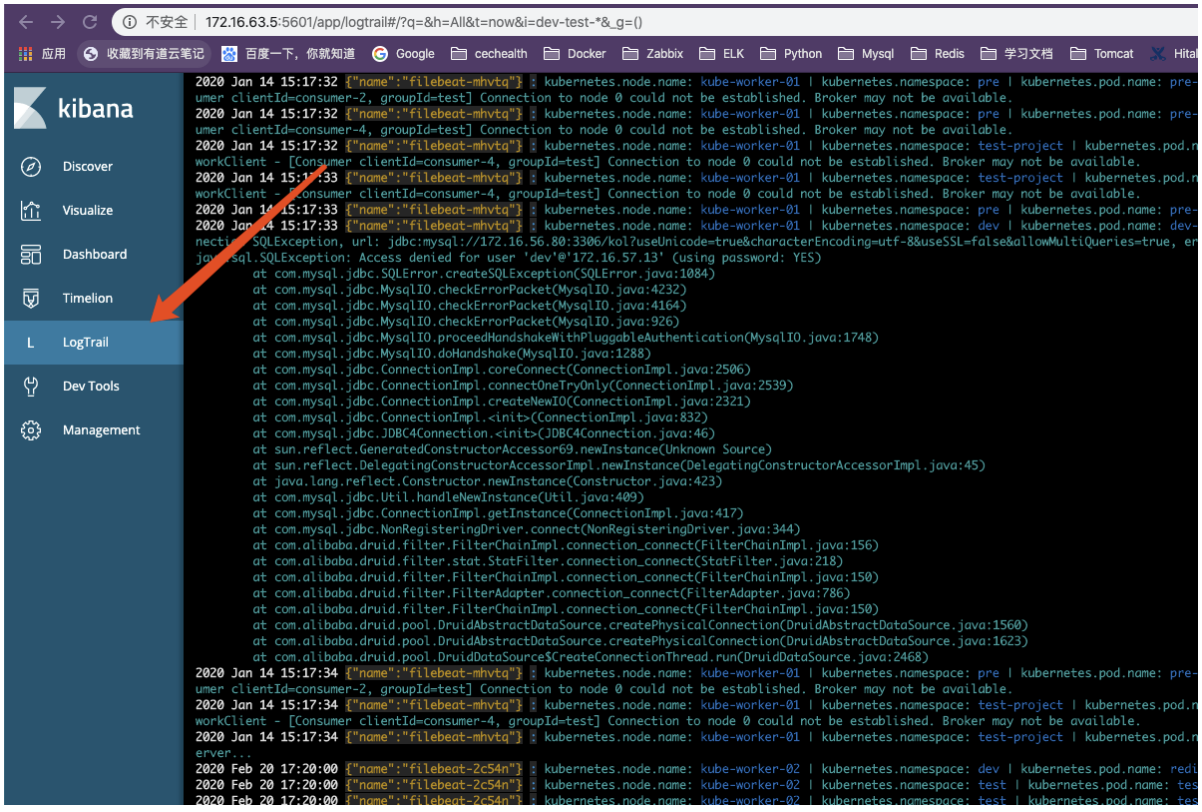
## 1、目的

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

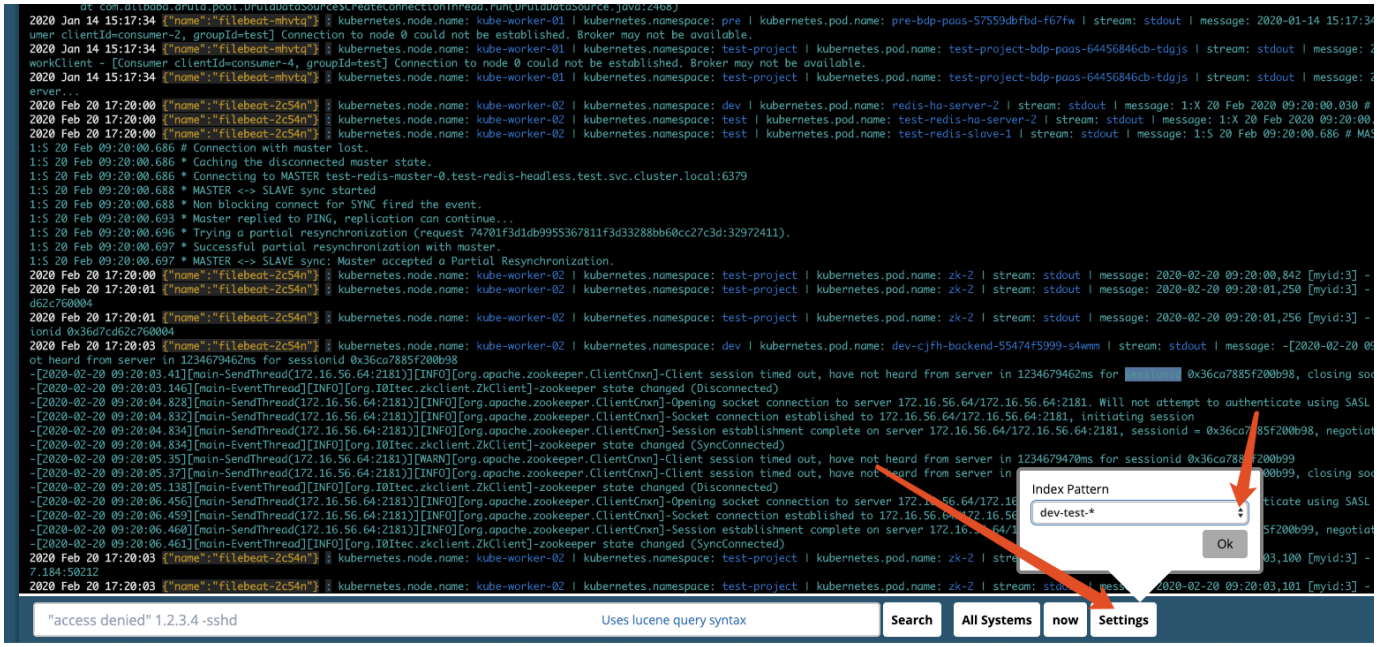
### 2.1 地址

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：

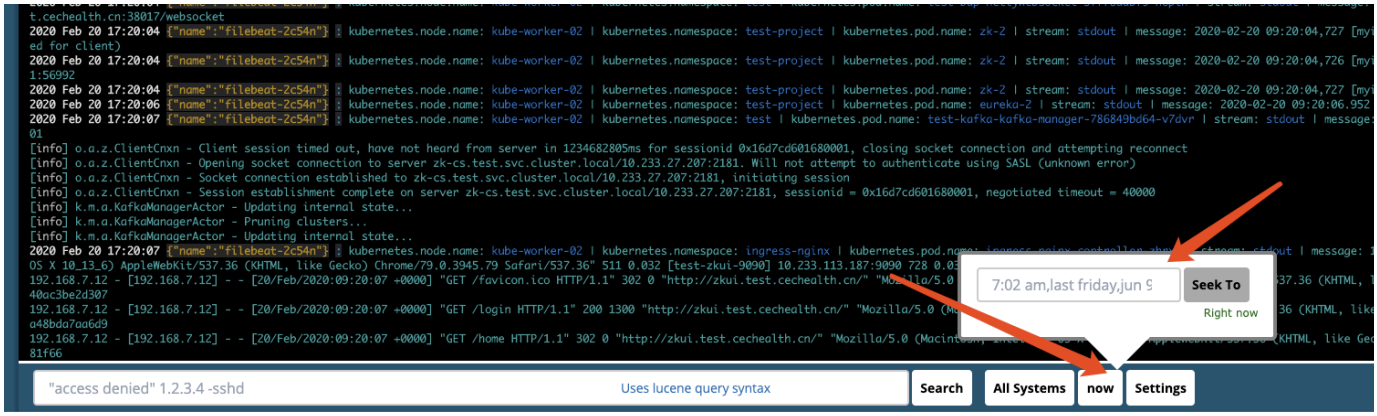



Index名称说明：

| 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：

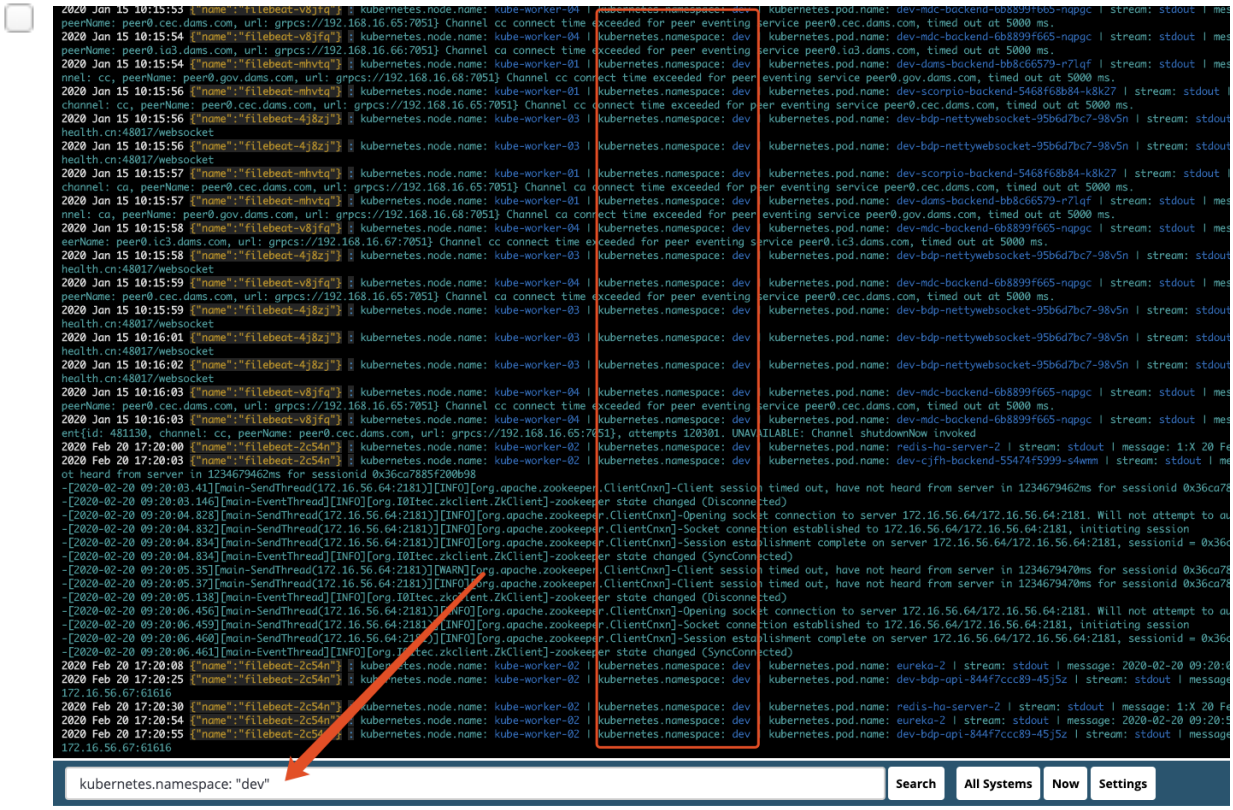


## 2.4 输入字段查询

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



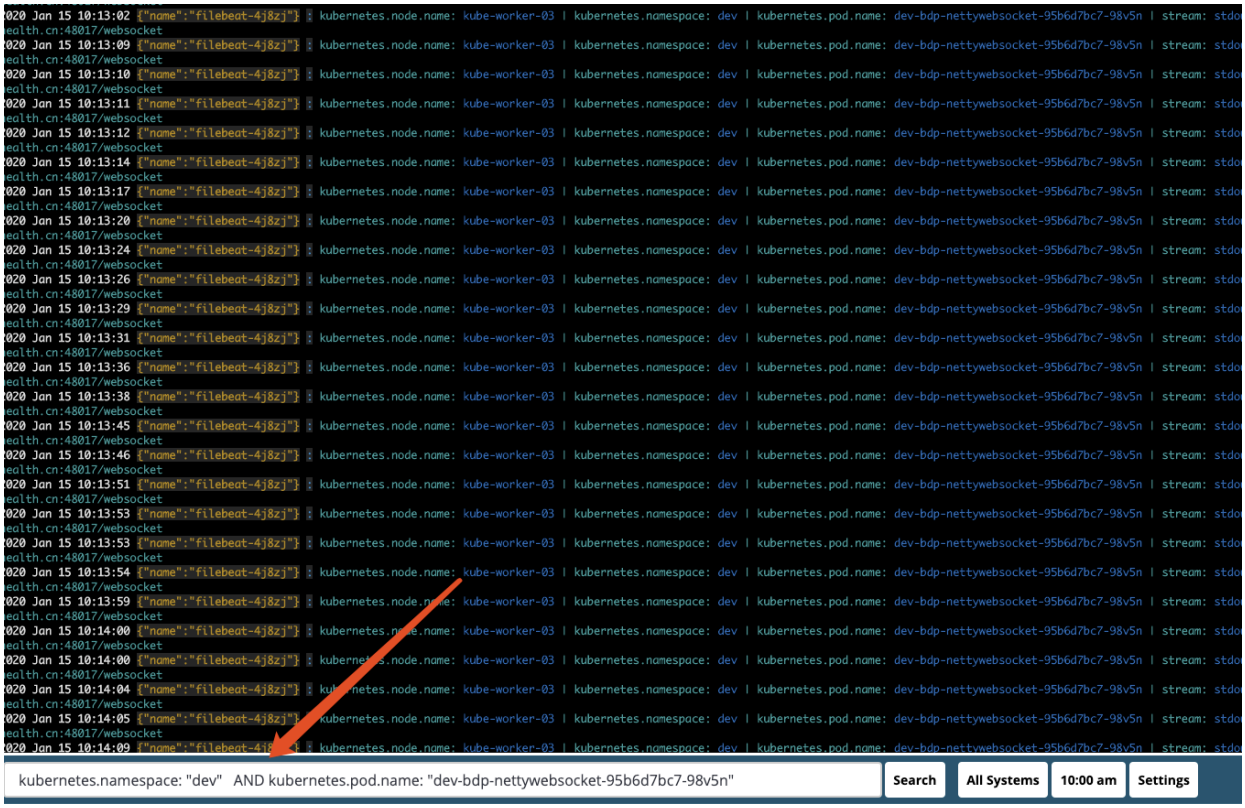

b. 如需要查看namespace为dev对应为开发环境，应用为bdp-nettywebsocket 的pod日志，可输入：

```
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