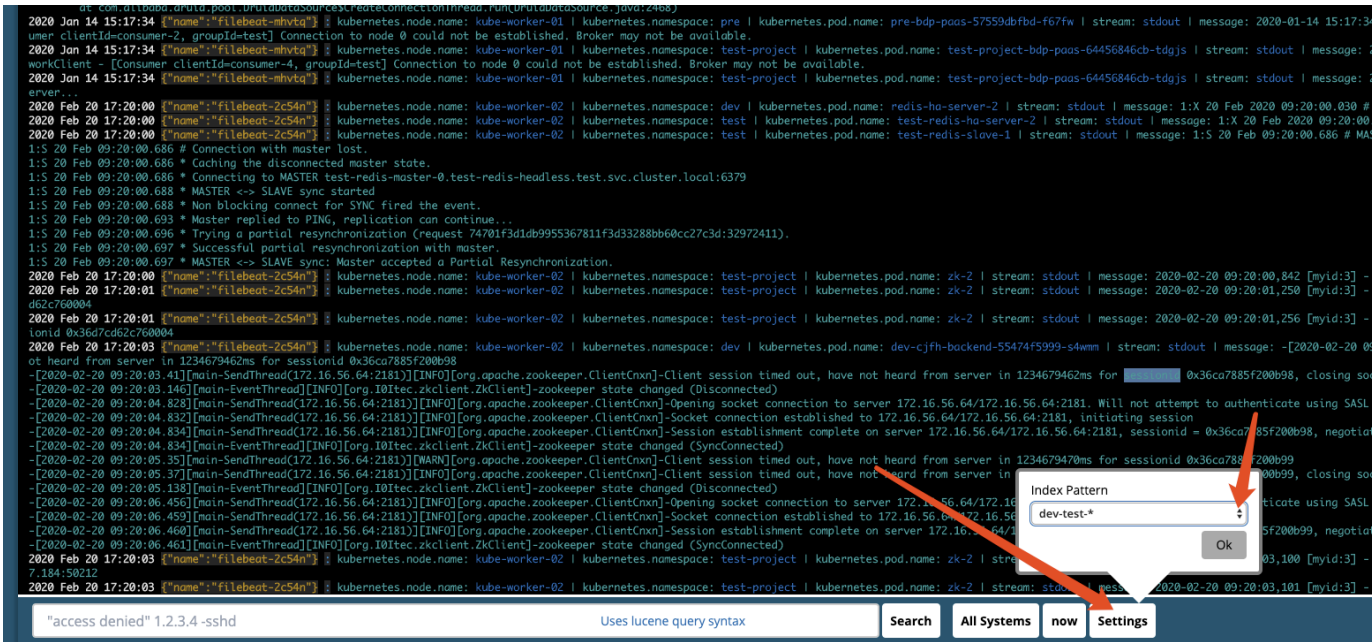


2.2 选择索引

点击下方Settings，选择要查看的索引名称，然后点击OK，如图：

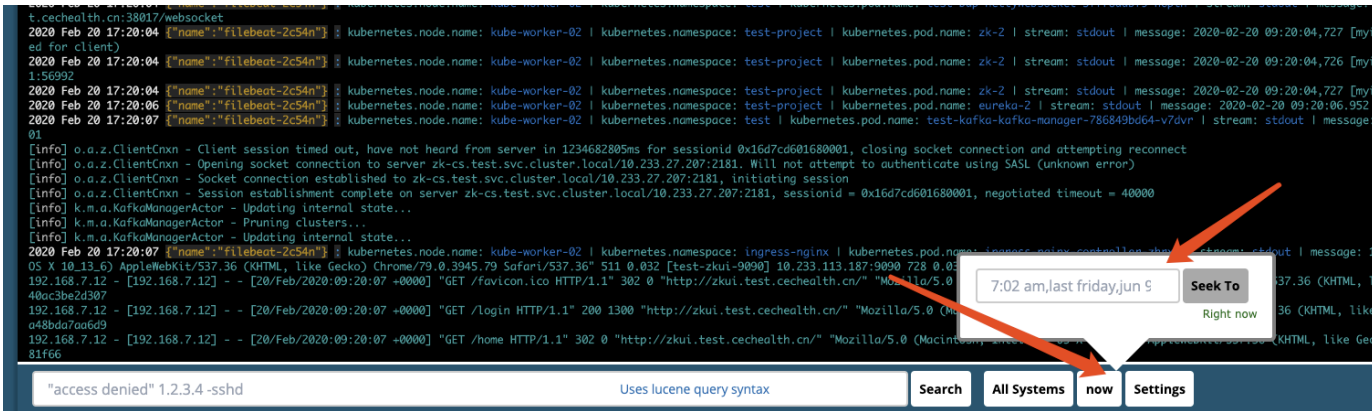


Index名称说明：

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

```
2020 Jan 15 10:15:53 ["name":"filebeat-v8jfq"] kubernetes.node.name: kube-worker-04 | kubernetes.namespace: dev | kubernetes.pod.name: dev-mdc-backend-bb8899f665-nagpc | stream: stdout | me
peerName: peer0.ccc.dams.com, url: grpc://192.168.16.65:7051] Channel cc connect time exceeded for peer eventing service peer0.ccc.dams.com, timed out at 5000 ms.
2020 Jan 15 10:15:54 ["name":"filebeat-v8jfq"] kubernetes.node.name: kube-worker-04 | kubernetes.namespace: dev | kubernetes.pod.name: dev-mdc-backend-bb8899f665-nagpc | stream: stdout | me
peerName: peer0.la3.dams.com, url: grpc://192.168.16.66:7051] Channel ca connect time exceeded for peer eventing service peer0.la3.dams.com, timed out at 5000 ms.
2020 Jan 15 10:15:54 ["name":"filebeat-nhvta"] kubernetes.node.name: kube-worker-01 | kubernetes.namespace: dev | kubernetes.pod.name: dev-dms-backend-bb8c6579-n7lqf | stream: stdout | me
nnel: cc, peerName: peer0.gov.dams.com, url: grpc://192.168.16.68:7051] Channel cc connect time exceeded for peer eventing service peer0.gov.dams.com, timed out at 5000 ms.
2020 Jan 15 10:15:56 ["name":"filebeat-nhvta"] kubernetes.node.name: kube-worker-01 | kubernetes.namespace: dev | kubernetes.pod.name: dev-scorpia-backend-5468f68b84-k8k27 | stream: stdout | me
channel: cc, peerName: peer0.ccc.dams.com, url: grpc://192.168.16.65:7051] Channel cc connect time exceeded for peer eventing service peer0.ccc.dams.com, timed out at 5000 ms.
2020 Jan 15 10:15:56 ["name":"filebeat-4j8zj"] kubernetes.node.name: kube-worker-03 | kubernetes.namespace: dev | kubernetes.pod.name: dev-bdp-nettywebsocket-95b6d7bc7-98v5n | stream: stdout | me
health.cn:48017/websocket
2020 Jan 15 10:15:56 ["name":"filebeat-4j8zj"] kubernetes.node.name: kube-worker-03 | kubernetes.namespace: dev | kubernetes.pod.name: dev-bdp-nettywebsocket-95b6d7bc7-98v5n | stream: stdout | me
health.cn:48017/websocket
2020 Jan 15 10:15:57 ["name":"filebeat-nhvta"] kubernetes.node.name: kube-worker-01 | kubernetes.namespace: dev | kubernetes.pod.name: dev-scorpia-backend-5468f68b84-k8k27 | stream: stdout | me
channel: cc, peerName: peer0.ccc.dams.com, url: grpc://192.168.16.65:7051] Channel ca connect time exceeded for peer eventing service peer0.ccc.dams.com, timed out at 5000 ms.
2020 Jan 15 10:15:57 ["name":"filebeat-nhvta"] kubernetes.node.name: kube-worker-04 | kubernetes.namespace: dev | kubernetes.pod.name: dev-dms-backend-bb8c6579-n7lqf | stream: stdout | me
nnel: cc, peerName: peer0.gov.dams.com, url: grpc://192.168.16.68:7051] Channel ca connect time exceeded for peer eventing service peer0.gov.dams.com, timed out at 5000 ms.
2020 Jan 15 10:15:58 ["name":"filebeat-4j8zj"] kubernetes.node.name: kube-worker-04 | kubernetes.namespace: dev | kubernetes.pod.name: dev-mdc-backend-bb8899f665-nagpc | stream: stdout | me
peerName: peer0.ic3.dams.com, url: grpc://192.168.16.67:7051] Channel cc connect time exceeded for peer eventing service peer0.ic3.dams.com, timed out at 5000 ms.
2020 Jan 15 10:15:58 ["name":"filebeat-4j8zj"] kubernetes.node.name: kube-worker-03 | kubernetes.namespace: dev | kubernetes.pod.name: dev-bdp-nettywebsocket-95b6d7bc7-98v5n | stream: stdout | me
health.cn:48017/websocket
2020 Jan 15 10:15:59 ["name":"filebeat-v8jfq"] kubernetes.node.name: kube-worker-04 | kubernetes.namespace: dev | kubernetes.pod.name: dev-mdc-backend-bb8899f665-nagpc | stream: stdout | me
peerName: peer0.ccc.dams.com, url: grpc://192.168.16.65:7051] Channel ca connect time exceeded for peer eventing service peer0.ccc.dams.com, timed out at 5000 ms.
2020 Jan 15 10:15:59 ["name":"filebeat-4j8zj"] kubernetes.node.name: kube-worker-03 | kubernetes.namespace: dev | kubernetes.pod.name: dev-bdp-nettywebsocket-95b6d7bc7-98v5n | stream: stdout | me
health.cn:48017/websocket
2020 Jan 15 10:16:01 ["name":"filebeat-4j8zj"] kubernetes.node.name: kube-worker-03 | kubernetes.namespace: dev | kubernetes.pod.name: dev-bdp-nettywebsocket-95b6d7bc7-98v5n | stream: stdout | me
health.cn:48017/websocket
2020 Jan 15 10:16:02 ["name":"filebeat-4j8zj"] kubernetes.node.name: kube-worker-03 | kubernetes.namespace: dev | kubernetes.pod.name: dev-bdp-nettywebsocket-95b6d7bc7-98v5n | stream: stdout | me
health.cn:48017/websocket
2020 Jan 15 10:16:03 ["name":"filebeat-v8jfq"] kubernetes.node.name: kube-worker-04 | kubernetes.namespace: dev | kubernetes.pod.name: dev-mdc-backend-bb8899f665-nagpc | stream: stdout | me
peerName: peer0.ccc.dams.com, url: grpc://192.168.16.65:7051] Channel cc connect time exceeded for peer eventing service peer0.ccc.dams.com, timed out at 5000 ms.
2020 Jan 15 10:16:03 ["name":"filebeat-nhvta"] kubernetes.node.name: kube-worker-04 | kubernetes.namespace: dev | kubernetes.pod.name: dev-mdc-backend-bb8899f665-nagpc | stream: stdout | me
ent{id: 481130, channel: cc, peerName: peer0.ccc.dams.com, url: grpc://192.168.16.65:7051}, attempts 120301. UNAVAILABLE: Channel shutdownNow invoked
2020 Feb 20 17:20:00 ["name":"filebeat-2c54n"] kubernetes.node.name: kube-worker-02 | kubernetes.namespace: dev | kubernetes.pod.name: redis-ha-server-2 | stream: stdout | message: 1:X 20 Fe
2020 Feb 20 17:20:03 ["name":"filebeat-2c54n"] kubernetes.node.name: kube-worker-02 | kubernetes.namespace: dev | kubernetes.pod.name: dev-cjfh-backend-55474f5999-54wm | stream: stdout | me
ut heard from server in 1234679462ms for sessionid 0x36ca78
[2020-02-20 09:20:03.411][main-SendThread(172.16.56.64:2181)][INFO][org.apache.zookeeper.ClientCnxn]-Client session timed out, have not heard from server in 1234679462ms for sessionid 0x36ca78
[2020-02-20 09:20:03.146][main-EventThread][INFO][org.10ttec.zkclient.ZkClient]-zookeeper state changed (Disconnected)
[2020-02-20 09:20:04.828][main-SendThread(172.16.56.64:2181)][INFO][org.apache.zookeeper.ClientCnxn]-Opening socket connection to server 172.16.56.64/172.16.56.64:2181. Will not attempt to au
[2020-02-20 09:20:04.832][main-SendThread(172.16.56.64:2181)][INFO][org.apache.zookeeper.ClientCnxn]-Socket connection established to 172.16.56.64/172.16.56.64:2181, initiating session
[2020-02-20 09:20:04.834][main-EventThread][INFO][org.10ttec.zkclient.ZkClient]-zookeeper state changed (SyncConnected)
[2020-02-20 09:20:05.381][main-SendThread(172.16.56.64:2181)][WARN][org.apache.zookeeper.ClientCnxn]-Client session timed out, have not heard from server in 1234679470ms for sessionid 0x36ca78
[2020-02-20 09:20:05.371][main-SendThread(172.16.56.64:2181)][INFO][org.apache.zookeeper.ClientCnxn]-Client session timed out, have not heard from server in 1234679470ms for sessionid 0x36ca78
[2020-02-20 09:20:05.138][main-EventThread][INFO][org.10ttec.zkclient.ZkClient]-zookeeper state changed (Disconnected)
[2020-02-20 09:20:06.459][main-SendThread(172.16.56.64:2181)][INFO][org.apache.zookeeper.ClientCnxn]-Opening socket connection to server 172.16.56.64/172.16.56.64:2181. Will not attempt to au
[2020-02-20 09:20:06.459][main-SendThread(172.16.56.64:2181)][INFO][org.apache.zookeeper.ClientCnxn]-Socket connection established to 172.16.56.64/172.16.56.64:2181, initiating session
[2020-02-20 09:20:06.461][main-EventThread][INFO][org.10ttec.zkclient.ZkClient]-zookeeper state changed (SyncConnected)
2020 Feb 20 17:20:08 ["name":"filebeat-2c54n"] kubernetes.node.name: kube-worker-02 | kubernetes.namespace: dev | kubernetes.pod.name: eureka-2 | stream: stdout | message: 2020-02-20 09:20:0
172.16.56.67:61616
2020 Feb 20 17:20:30 ["name":"filebeat-2c54n"] kubernetes.node.name: kube-worker-02 | kubernetes.namespace: dev | kubernetes.pod.name: redis-ha-server-2 | stream: stdout | message: 1:X 20 Fe
2020 Feb 20 17:20:54 ["name":"filebeat-2c54n"] kubernetes.node.name: kube-worker-02 | kubernetes.namespace: dev | kubernetes.pod.name: eureka-2 | stream: stdout | message: 2020-02-20 09:20:5
2020 Feb 20 17:20:55 ["name":"filebeat-2c54n"] kubernetes.node.name: kube-worker-02 | kubernetes.namespace: dev | kubernetes.pod.name: dev-bdp-api-8447fcc89-45j5z | stream: stdout | message
172.16.56.67:61616
```

Search All Systems Now Settings

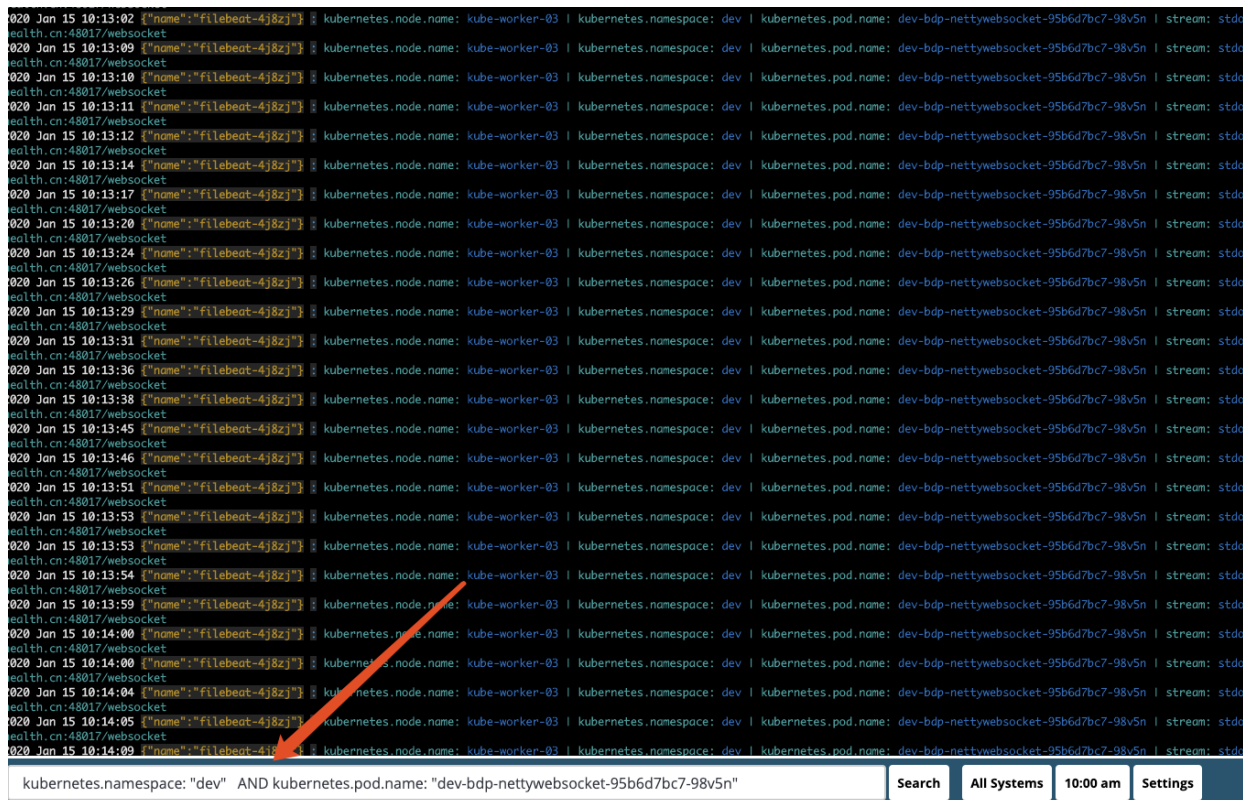
b. 如需要查看namespace为dev对应为开发环境，应用为bdp-nettywebsocket 的pod日志，可输入：

```
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。

```
?:  
*:  
  
?tere  
therewhere  
test*  
testtesttester
```

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