**ELK-搭建实时日志ELK分析系统**

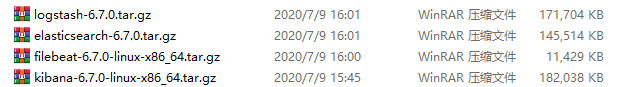
ELK是elasticsearch,logstash,kibana三个开源工具的简称，一般用于搭建日志分析系统。

* 1. elasticsearch是核心，是一个分布式搜索引擎，查询速度快，提供数据的存储和检索。
  2. logstash负责数据的收集和处理，目前多使用一个更加轻量级的工具filebeat进行收集数据。
  3. kibana用于可视化展示elasticsearch中的数据，并提供一些操作。

# 环境准备

前往华为镜像站下载工具

我们下载最新的 6.7.0 版本： -kibana自6.6.0之后支持中文



## 安装jdk环境

要求jdk版本为1.8+

查看jdk版本命令

java -version

显示结果为

java version "1.8.0\_171"  
Java(TM) SE Runtime Environment (build 1.8.0\_171-b11)  
Java HotSpot(TM) 64-Bit Server VM (build 25.171-b11, mixed mode)

## 安装elasticsearch及相应配置

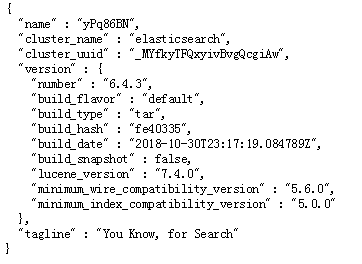
* 1. 解压文件

tar -zxvf elasticsearch-6.7.0.tar.gz

* 1. 修改config目录下elasticsearch.yml：  
     network.host: 0.0.0.0（以便在外网中访问）
  2. 启动elasticsearch，在bin目录下启动  
     前台启动命令  
     sh elasticsearch  
     后台启动命令  
     sh elasticsearch -d

常见错误及注意事项：

* 1. 需要用非root账号启动。
  2. 默认占用9200端口和9300端口，如已被占用，修改elasticsearch.yml  
     transport.tcp.port: 9301  
     http.port: 9201
  3. 启动报错[max file descriptors [4096] for elasticsearch process likely too low, increase to at least [65536]]  
     修改/etc/security/limits.conf，增加以下配置  
     \* soft nofile 65536  
     \* hard nofile 65536
  4. 启动报错max virtual memory areas vm.max\_map\_count [65530] is too low, increase to at least [262144]  
     修改/etc/sysctl.conf，增加  
     vm.max\_map\_count = 655360  
     修改完成之后重新登录
  5. 启动成功后在浏览器访问:你的ip:9200，显示以下页面则表示启动成功：



* 1. 可安装head插件，不过6.x版本安装head插件比较麻烦，可以安装chrome插件[elasticsearch-head](https://app.yinxiang.com/OutboundRedirect.action?dest=https://links.jianshu.com/go?to=https%3A%2F%2Fwww.gugeapps.com%2Fwebstore%2Fdetail%2Felasticsearch-head%2Fffmkiejjmecolpfloofpjologoblkegm%23download),比较方便

## 安装filebeat及相应配置

filebeat安装在日志文件存放的服务器上，读取本机指定的日志文件发送到logstash。

* 1. 解压文件  
     tar -zxvf kibana-6.7.0-linux-x86\_64.tar.gz
  2. 编辑filebeat.yml对应位置的配置

|  |
| --- |
| #=========================== Filebeat inputs =============================  filebeat.inputs:  # Each - is an input. Most options can be set at the input level, so # you can use different inputs for various configurations. # Below are the input specific configurations.  - type: log  # Change to true to enable this input configuration.  enabled: false  # Paths that should be crawled and fetched. Glob based paths.  paths:  #你的日志目录  - c:\programdata\elasticsearch\logs\\* |

编辑输出部分，注释默认的输出到elasticsearch，改为输出到logstash

|  |
| --- |
| #================================ Outputs =====================================  # Configure what output to use when sending the data collected by the beat.  #-------------------------- Elasticsearch output ------------------------------ #output.elasticsearch:  # Array of hosts to connect to.  # hosts: ["localhost:9201"]  # Optional protocol and basic auth credentials.  #protocol: "https"  #username: "elastic"  #password: "changeme"  #----------------------------- Logstash output -------------------------------- output.logstash:  # The Logstash hosts  hosts: ["localhost:5044"]  # Optional SSL. By default is off.  # List of root certificates for HTTPS server verifications  #ssl.certificate\_authorities: ["/etc/pki/root/ca.pem"]  # Certificate for SSL client authentication  #ssl.certificate: "/etc/pki/client/cert.pem"  # Client Certificate Key  #ssl.key: "/etc/pki/client/cert.key" |

* 1. 使用root账号启动filebeat  
     ./filebeat -e -c filebeat.yml -d "publish"  
     后台启动方式: nohup ./filebeat -e -c filebeat.yml > filebeat.log &
  2. 启动之后显示如下:

|  |
| --- |
| 2018-11-20T09:08:07.318+0800 INFO [monitoring] log/log.go:141 Non-zero metrics in the last 30s {"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ticks":240,"time":{"ms":13}},"total":{"ticks":1220,"time":{"ms":30},"value":1220},"user":{"ticks":980,"time":{"ms":17}}},"info":{"ephemeral\_id":"f3fa0a1c-0bdc-40e7-9666-abeb3e308b75","uptime":{"ms":60017}},"memstats":{"gc\_next":58381296,"memory\_alloc":33685752,"memory\_total":313273096}},"filebeat":{"harvester":{"open\_files":15,"running":15}},"libbeat":{"config":{"module":{"running":0}},"pipeline":{"clients":1,"events":{"active":0}}},"registrar":{"states":{"current":15}},"system":{"load":{"1":0.1,"15":0.13,"5":0.18,"norm":{"1":0.025,"15":0.0325,"5":0.045}}}}}} 2018-11-20T09:08:37.318+0800 INFO [monitoring] log/log.go:141 Non-zero metrics in the last 30s {"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ticks":260,"time":{"ms":21}},"total":{"ticks":1240,"time":{"ms":26},"value":1240},"user":{"ticks":980,"time":{"ms":5}}},"info":{"ephemeral\_id":"f3fa0a1c-0bdc-40e7-9666-abeb3e308b75","uptime":{"ms":90017}},"memstats":{"gc\_next":58381296,"memory\_alloc":33998256,"memory\_total":313585600}},"filebeat":{"harvester":{"open\_files":15,"running":15}},"libbeat":{"config":{"module":{"running":0}},"pipeline":{"clients":1,"events":{"active":0}}},"registrar":{"states":{"current":15}},"system":{"load":{"1":0.06,"15":0.13,"5":0.17,"norm":{"1":0.015,"15":0.0325,"5":0.0425}}}}}} 2018-11-20T09:09:07.318+0800 INFO [monitoring] log/log.go:141 Non-zero metrics in the last 30s {"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ticks":270,"time":{"ms":13}},"total":{"ticks":1270,"time":{"ms":29},"value":1270},"user":{"ticks":1000,"time":{"ms":16}}},"info":{"ephemeral\_id":"f3fa0a1c-0bdc-40e7-9666-abeb3e308b75","uptime":{"ms":120017}},"memstats":{"gc\_next":58381296,"memory\_alloc":34325192,"memory\_total":313912536}},"filebeat":{"harvester":{"open\_files":15,"running":15}},"libbeat":{"config":{"module":{"running":0}},"pipeline":{"clients":1,"events":{"active":0}}},"registrar":{"states":{"current":15}},"system":{"load":{"1":0.04,"15":0.13,"5":0.15,"norm":{"1":0.01,"15":0.0325,"5":0.0375}}}}}} 2018-11-20T09:09:37.318+0800 INFO [monitoring] log/log.go:141 Non-zero metrics in the last 30s {"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ticks":290,"time":{"ms":15}},"total":{"ticks":1310,"time":{"ms":40},"value":1310},"user":{"ticks":1020,"time":{"ms":25}}},"info":{"ephemeral\_id":"f3fa0a1c-0bdc-40e7-9666-abeb3e308b75","uptime":{"ms":150017}},"memstats":{"gc\_next":12905552,"memory\_alloc":6551512,"memory\_total":314231136,"rss":258048}},"filebeat":{"harvester":{"open\_files":15,"running":15}},"libbeat":{"config":{"module":{"running":0}},"pipeline":{"clients":1,"events":{"active":0}}},"registrar":{"states":{"current":15}},"system":{"load":{"1":0.1,"15":0.13,"5":0.15,"norm":{"1":0.025,"15":0.0325,"5":0.0375}}}}}} |

* 1. 这个时候我发现日志并没有通过filebeat采集到并发送到logstash  
     在input和output下新增enabled: true，解决问题

|  |
| --- |
| # Paths that should be crawled and fetched. Glob based paths.  enabled: true  paths:  - /home/appadmin/elk/logs/\*  #- c:\programdata\elasticsearch\logs\\* 12345  #----------------------------- Logstash output -------------------------------- output.logstash:  # The Logstash hosts  hosts: ["localhost:5044"]  enabled: true |

## 安装logstash及相应配置

logstash主要由input,filter,output几大部分，可以根据实际场景进行配置，此次我们设置input从filebeat处采集数据，输出到elasticsearch。

* 1. 解压文件  
     tar -zxvf logstash-6.7.0.tar.gz
  2. 新建一个配置文件  
     vi start.conf  
     配置如下：

|  |
| --- |
| # 配置输入为 beats input {  beats {  port => "5044"  } } # 数据过滤 filter {  grok {  match => { "message" => "%{COMBINEDAPACHELOG}" }  } } # 输出到本机的 ES output {  elasticsearch {  hosts => [ "localhost:9200" ]  } } |

* 1. 验证配置文件格式是否正确  
     logstash -f start.conf -t  
     显示: Configuration OK 则证明正确。
  2. 启动logstash  
     bin/logstash -f start.conf --config.reload.automatic  
     成功监听5044端口

|  |
| --- |
| [2018-11-19T16:28:48,946][INFO ][logstash.inputs.beats ] Beats inputs: Starting input listener {:address=>"0.0.0.0:5044"} [2018-11-19T16:28:48,953][INFO ][org.logstash.beats.Server] Starting server on port: 5044 [2018-11-19T16:28:48,959][INFO ][logstash.pipeline ] Pipeline started successfully {:pipeline\_id=>"main", :thread=>"#<Thread:0x16b0a9f7 sleep>"} [2018-11-19T16:28:48,973][INFO ][logstash.agent ] Pipelines running {:count=>1, :running\_pipelines=>[:main], :non\_running\_pipelines=>[]} |

常见错误及注意事项：

* 1. 报错Expected one of #, input, filter, output at line 1, column 1 (byte 1) after  
     原因是配置文件第一行有空白，需要把文件更改为UTF-8无BOM形式，使用notepad++进行修改，修改完成后将文件移动到bin目录下。
  2. 此外还报了一个异常，最后先启动filebeat再启动logstash解决，建议先启动filebeat。

## 安装kibana及相应配置

* 1. 解压文件  
     tar -zxvf kibana-6.7.0-linux-x86\_64.tar.gz
  2. 修改conf/kibana.yml使外网可以访问  
     server.host: "0.0.0.0"

后台启动kibana:

|  |
| --- |
| nohup ./bin/kibana & |

* 1. 浏览器访问:ip:5601

到现在一个elk就搭建完成了。

进一步设置参考[ELK-搭建实时日志ELK分析系统（2）-配置日志合并，@timestamp，根据不同beats来源建立不同索引](https://app.yinxiang.com/OutboundRedirect.action?dest=https://www.jianshu.com/p/bdbc41ee9fa0)

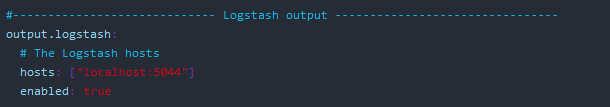
# 多服务多实例配置

此次服务采集192.168.198.171及192.168.198.235两台服务器上的日志，采集日志只需要在服务器上安装filebeat，filebeat采集日志后会发送到logstash中

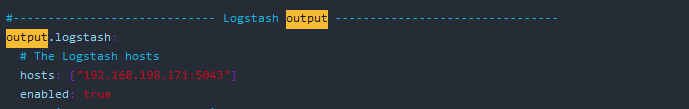
## 171：logstash配置



## 171：filebeats配置

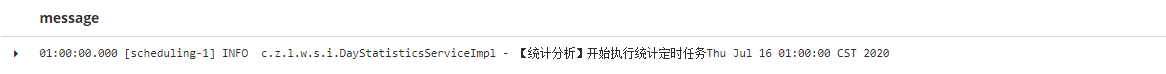


## 235：filebeats配置



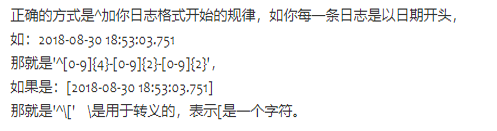
## 235：多行日志合并配置

小红帽日志开头为时间



使用正则匹配日志格式。以定义格式开头，如果不为定义格式则追加至上一行。





## 235：服务器标识配置

IMG_257

## filebeat多行读取

filebeat正则（根据时间判断一条日志，开头不是时间的都往上一行数据累积）：

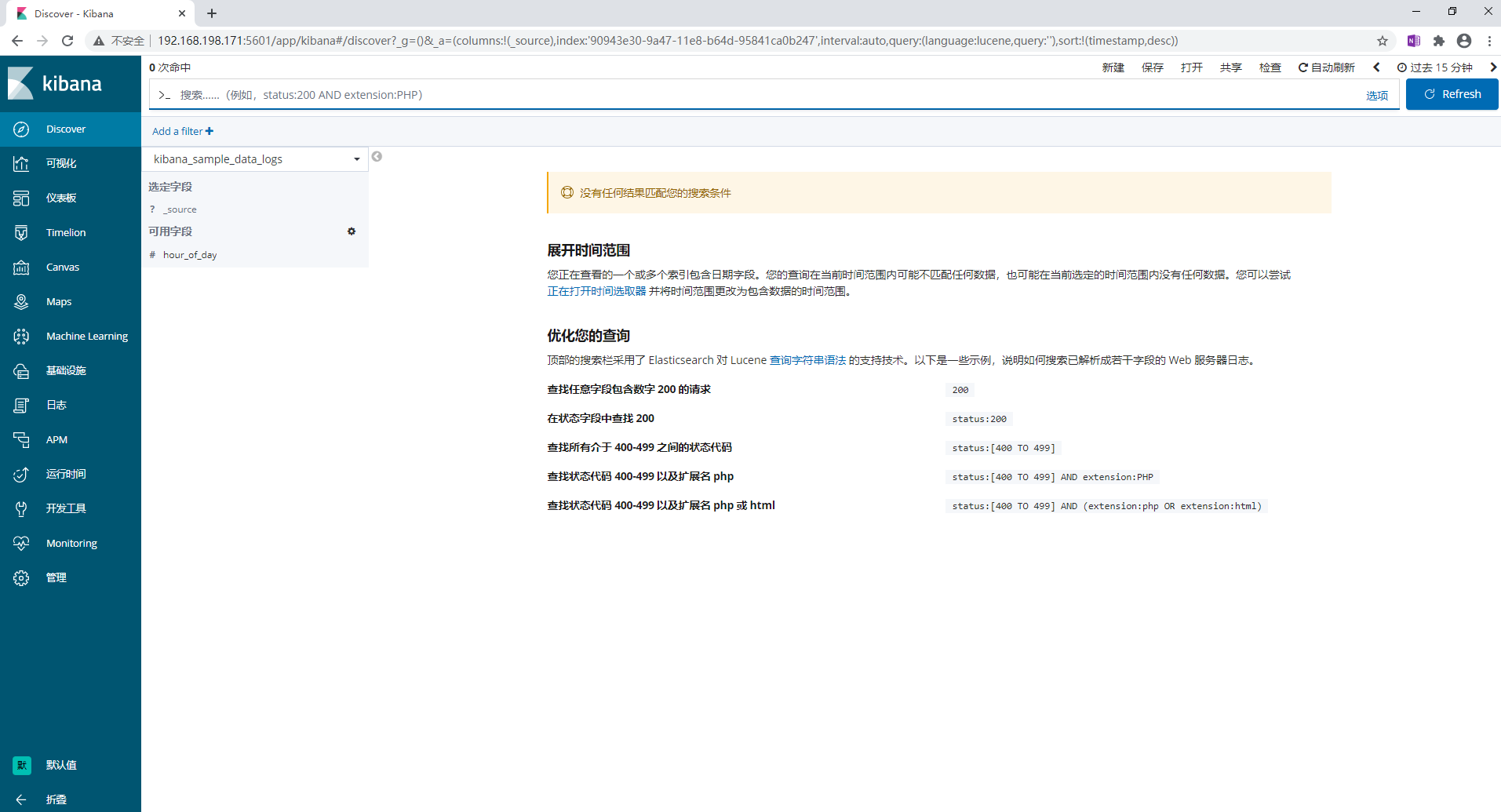
multiline.pattern: '^\[[0-2][0-9]:[0-6][0-9]:[0-6][0-9].[0-9]{3}'

multiline.negate: true

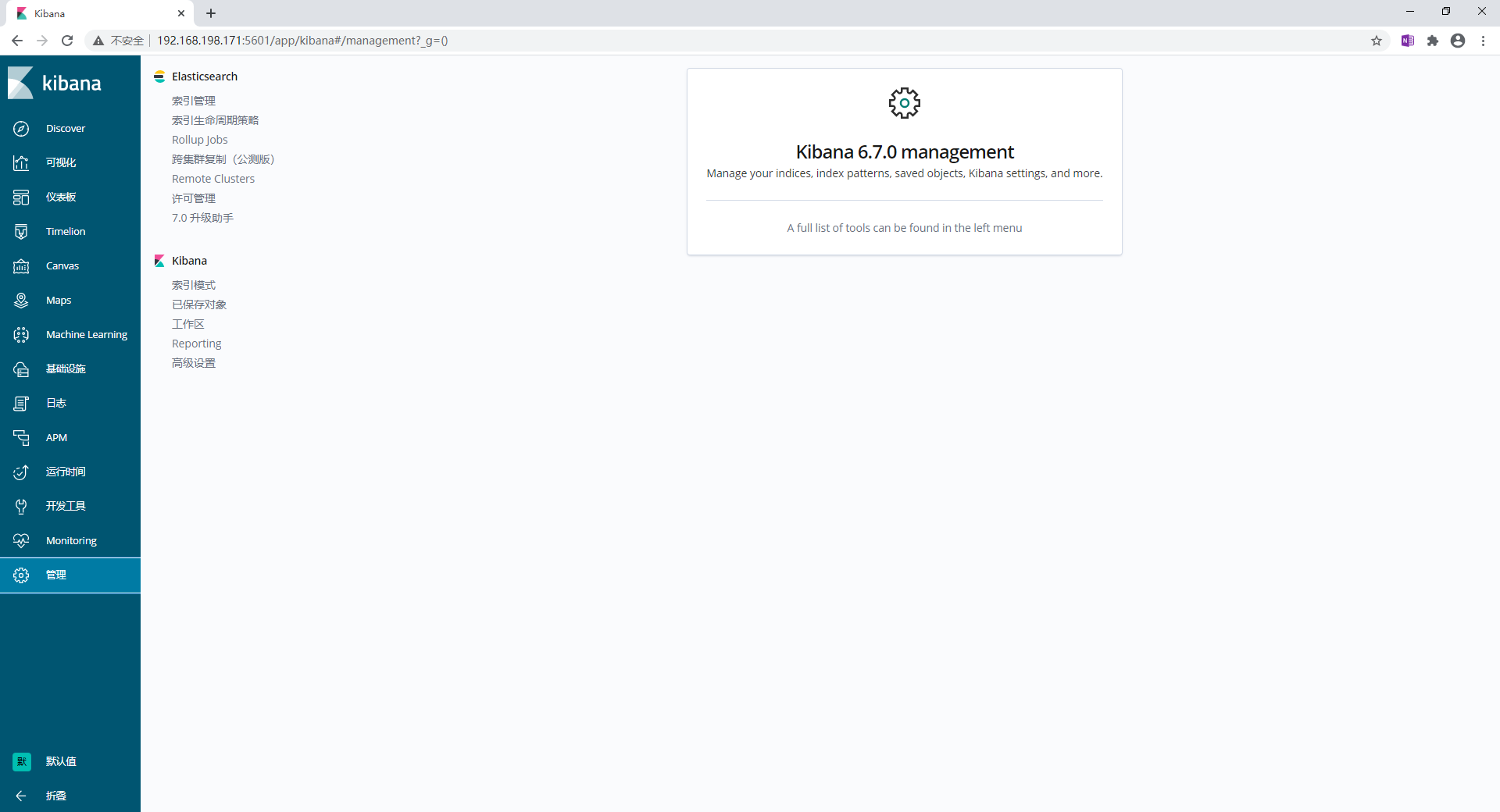
multiline.match: after

# 实际应用

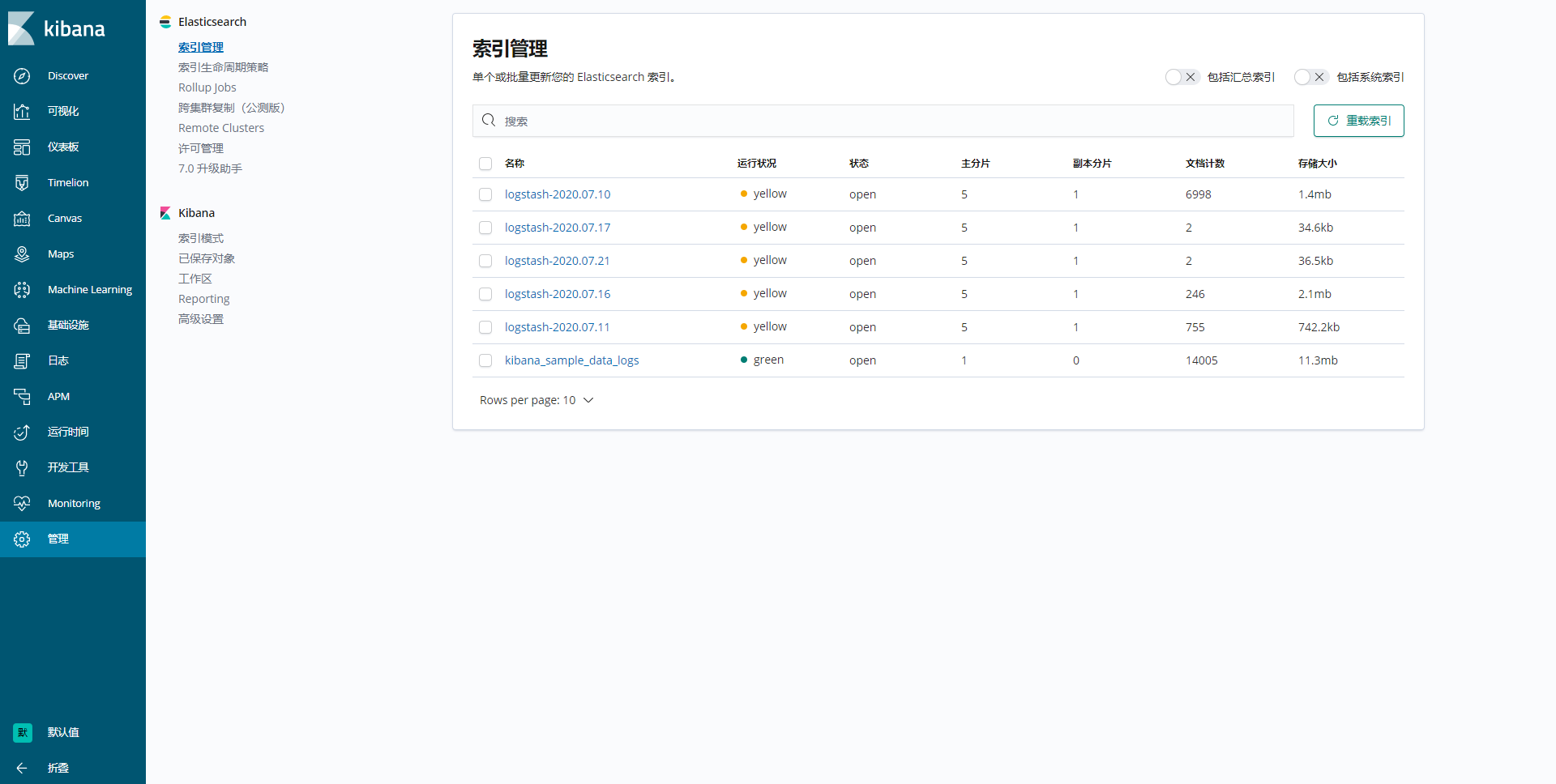
登陆<http://192.168.198.171:5601/>访问kibana界面



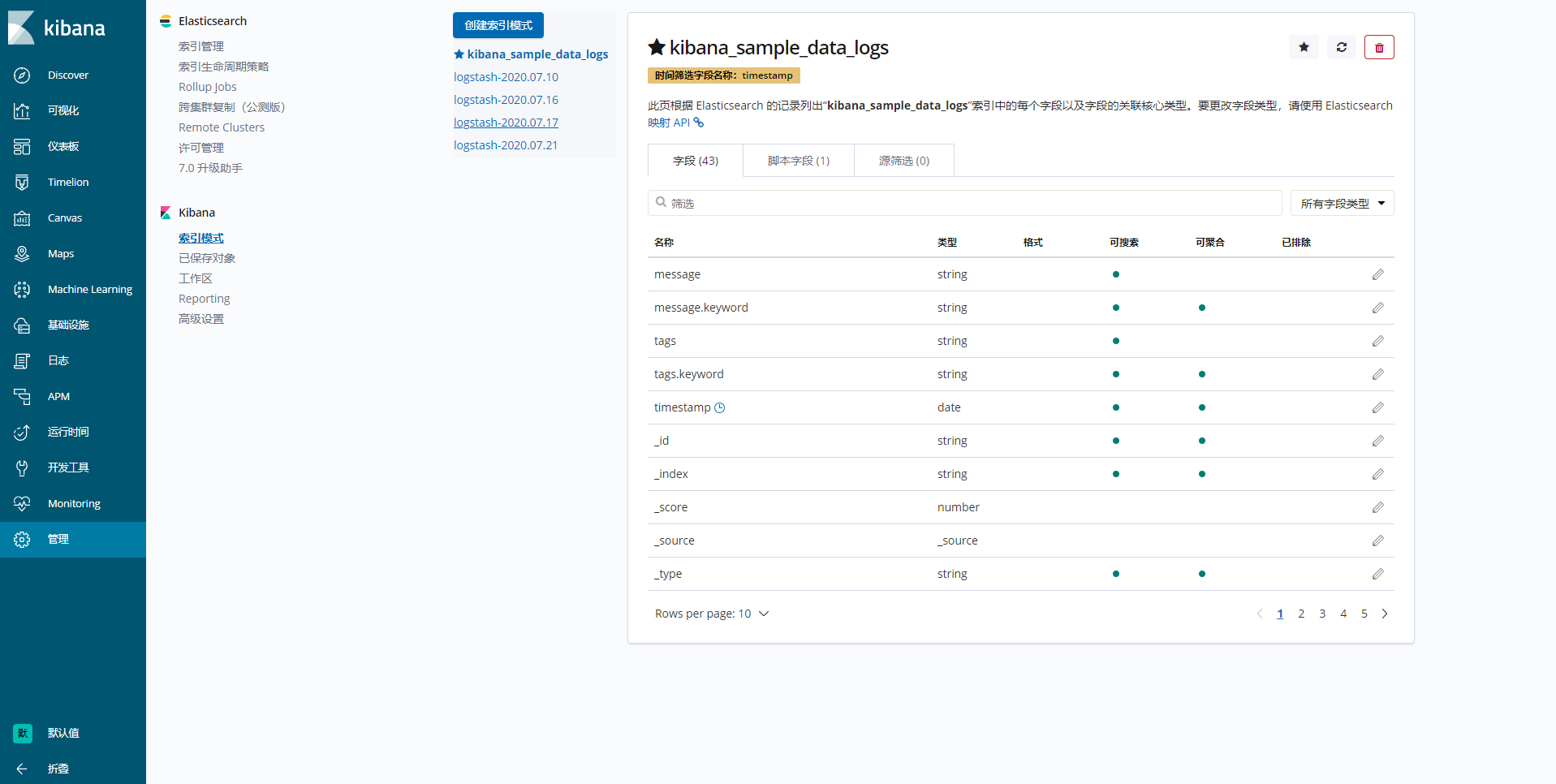
点击管理显示elasticsearch管理与kibana管理



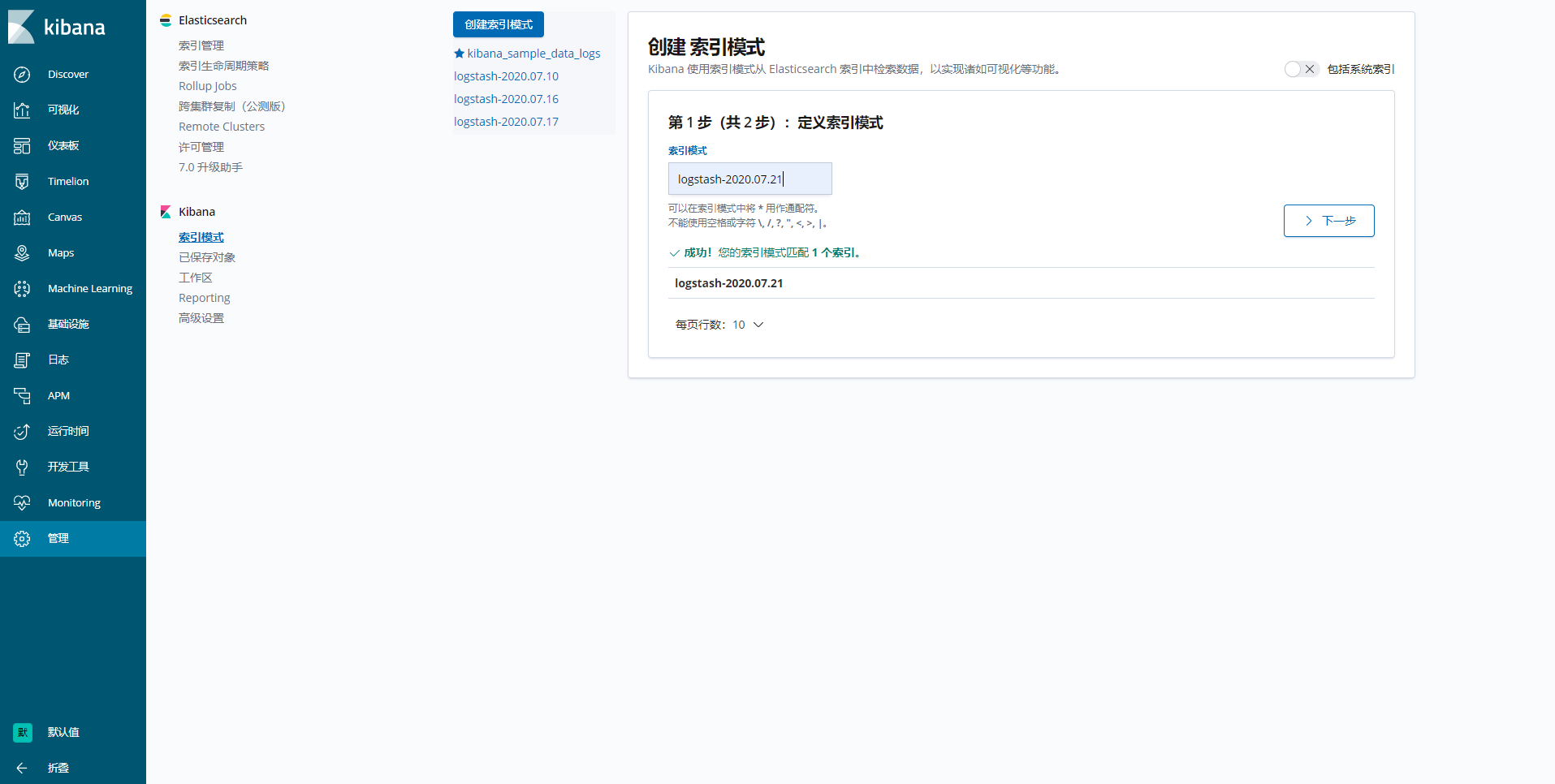
点击elasticsearch索引管理可以看到已经生成的日志索引

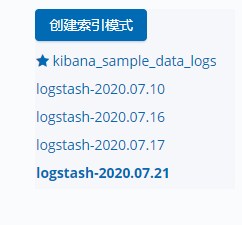


点击kibana索引管理可以看到已经纳入管理的索引以及管理界面

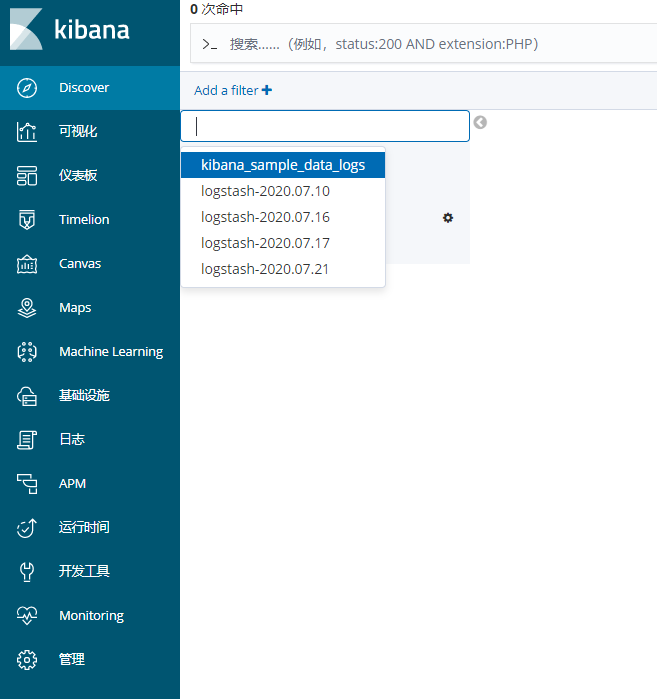


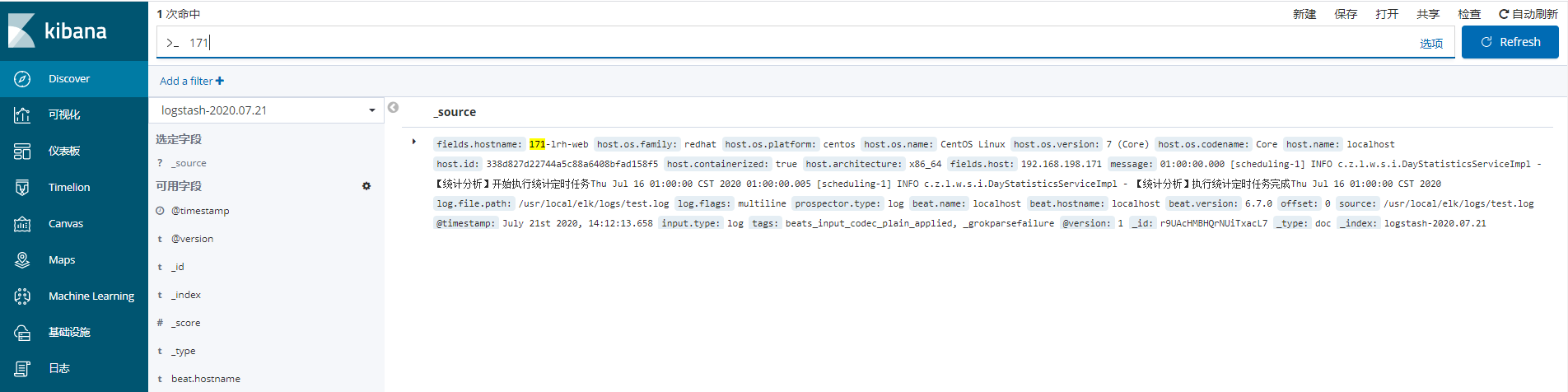
点击创建索引模式输入需要纳入kibana管理的索引显示匹配成功，下一步至创建，创建成功后可以看到管理界面已经出现刚加入的索引



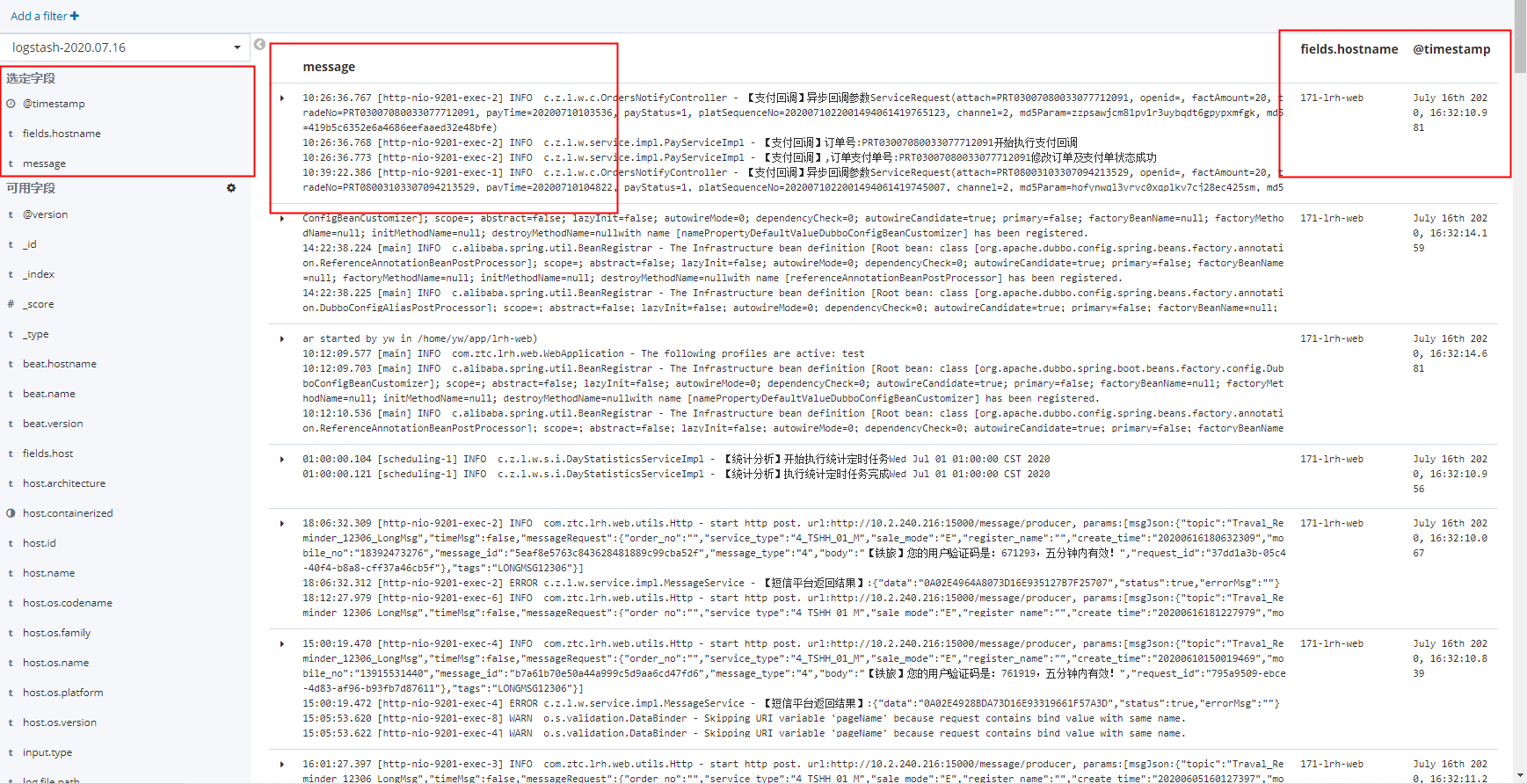


点击disvocer选择刚才加入的索引后既能搜索日志





可指定选定字段进行数据筛选



# 拓展

ELK配置进项目进行日志采集

在日志配置文件logback-spring.xml中加入



<appender

name="LOGSTASH" class="net.logstash.logback.appender.LogstashTcpSocketAppender">

//logstash ip和暴露的端口，logback就是通过这个地址把日志发送给logstash

<destination>39.108.135.163:5044</destination>

<encoder charset="UTF-8" class="net.logstash.logback.encoder.LogstashEncoder">

<customFields>{"appname":"${PROJECT\_NAME}"}</customFields>

</encoder>

</appender>

**通配ES索引**

kibana支持通配



添加后可根据过滤器筛选索引进行查找

