ES：是一个开源的高扩展的分布式全文检索引擎。它可以近乎实时的存储、检索数据，本身扩展性很好，可以扩展到上百台服务器，处理PB级别的数据。也可以使用lucene作为你核心来实现所有索引和搜索的工功能，但它的目的是通过简单的RESTfulAPI来隐藏Lucene的复杂性，从而让全文搜索变得简单。

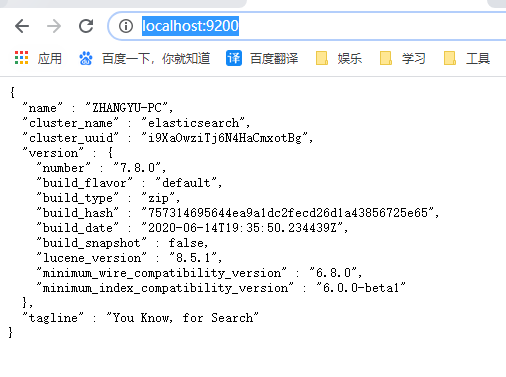
ELK: 是指elasticsearch、Logstash(中央数据流引擎，收集数据后通过过滤输出到不同的目的地[文件、redis\es])、Kibana(将es数据友好展示，提供实时分析功能)。

1. 在config中elasticsearch.yml 中，最后添加下面的代码，允许跨域访问。

http.cors.enabled: true

http.cors.allow-origin: "\*"

1. 在bin中双击 elasticsearch.bat启动elasticsearch，浏览器输入 <http://localhost:9200/> ，显示下图，表示成功



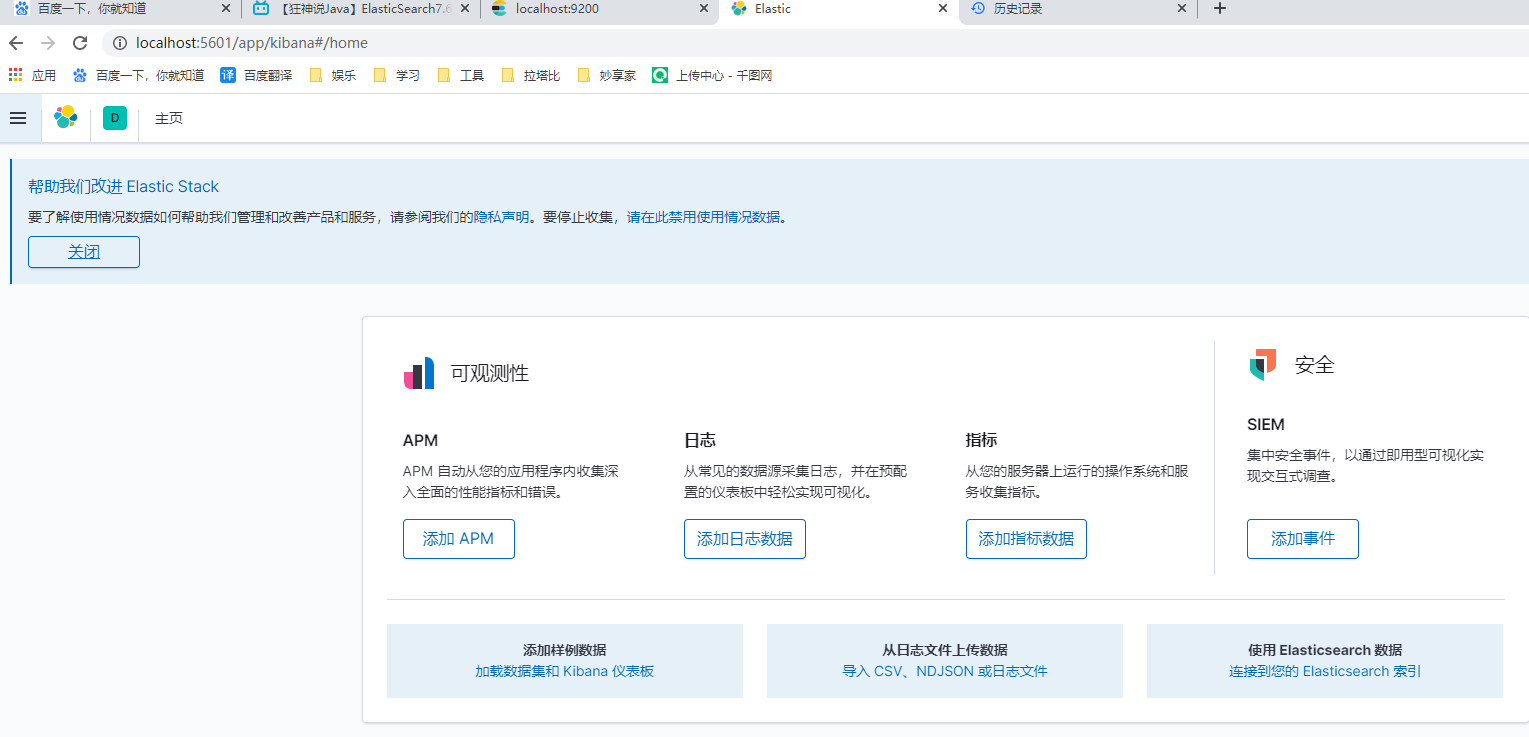
1. (过时)运行elasticsearch-head-master(es管理界面)，需要先安装node.js ,然后安装grunt

npm install –g grunt-cli

npm install

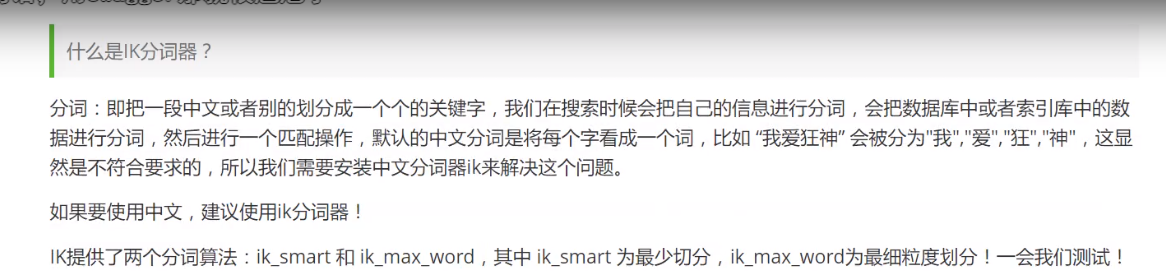
grunt server (启动管端界面, 浏览器输入 <http://localhost:9100/>)

1. 下载kibana，在config中的kibana.yml，最后一句添加 i18n.locale: "zh-CN"，界面汉化,浏览器输入<http://localhost:5601/app/kibana#/home>，打开首页

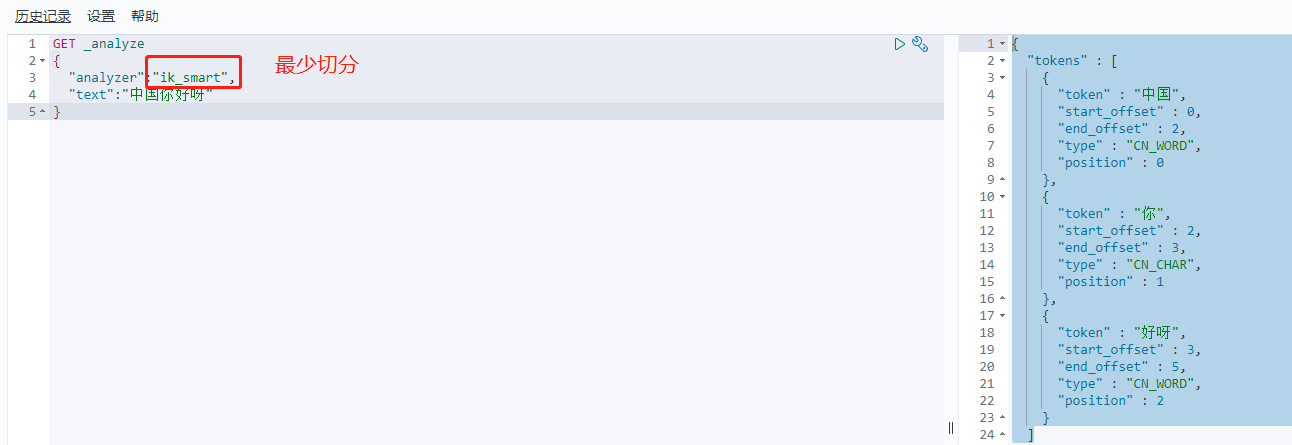


1. 下载分词器ik <https://github.com/medcl/elasticsearch-analysis-ik/releases>,然后在elasticsearch\elasticsearch-7.8.0\plugins 中新建ik文件夹，把代码解压到这里

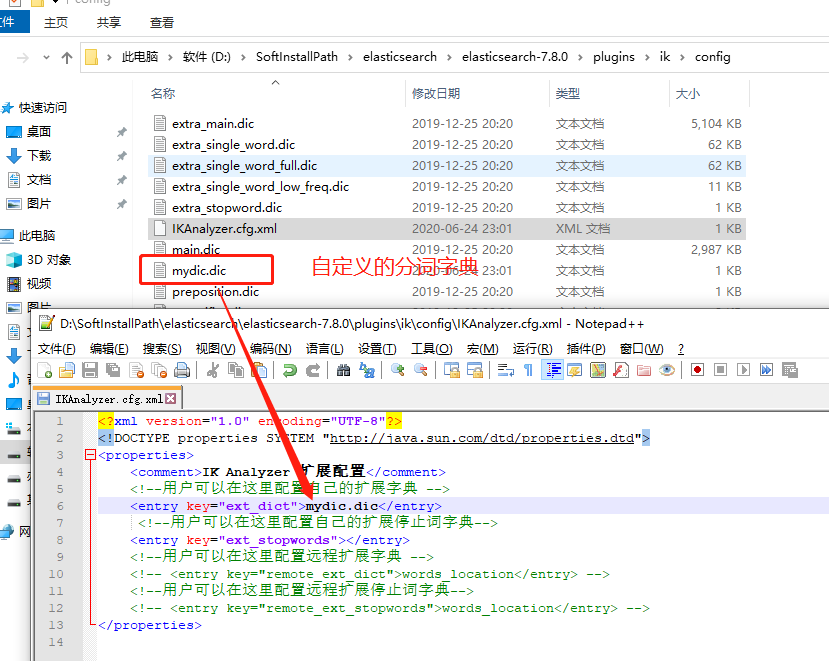
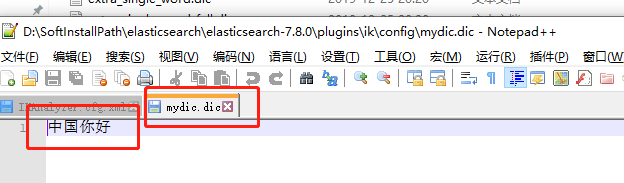
可以在elasticsearch 的bin的 cmd中，使用elasticsearch-plugin list查看是否安装成功

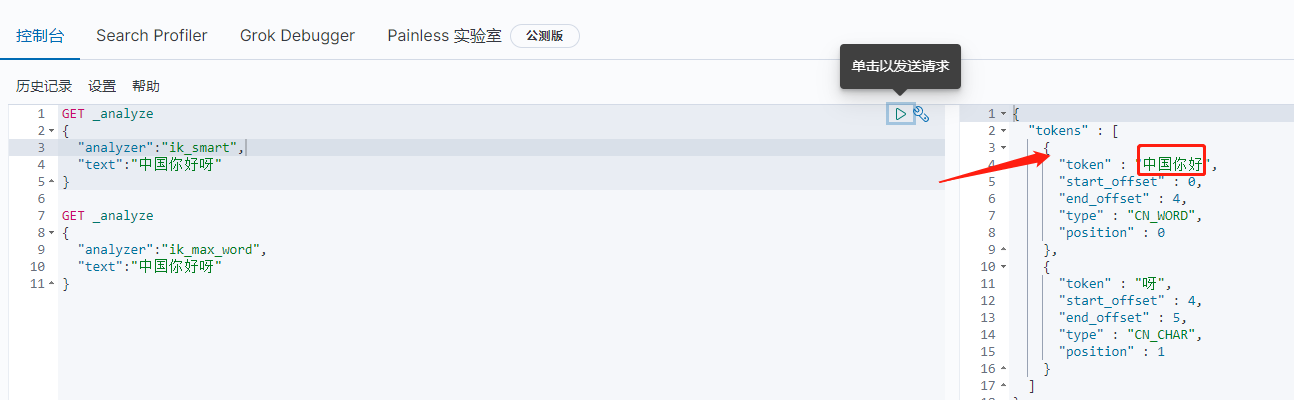


在kibana上查看分词结果(REST风格)：

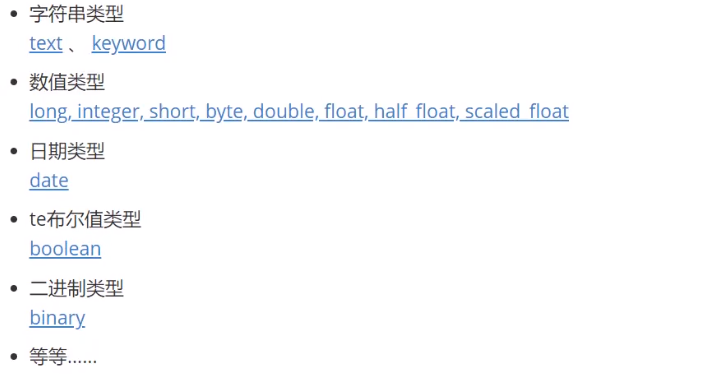


ik分词器上添加字典：elasticsearch\elasticsearch-7.8.0\plugins\ik\config中配置，添加自定义字典mydic.dic，然后在IKAnalyzer.cfg.xml中配置就行了

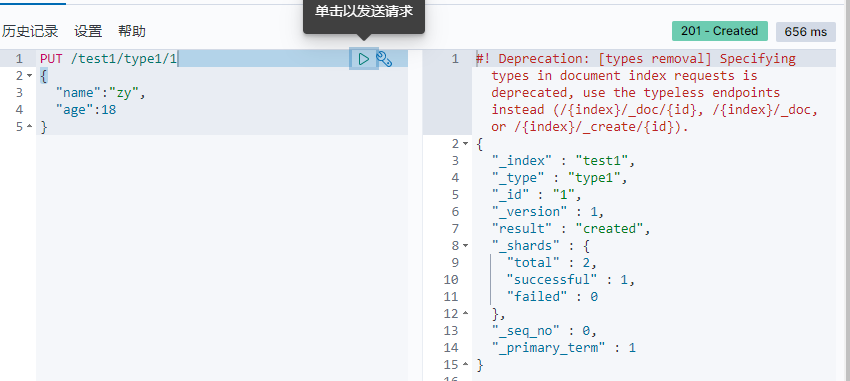
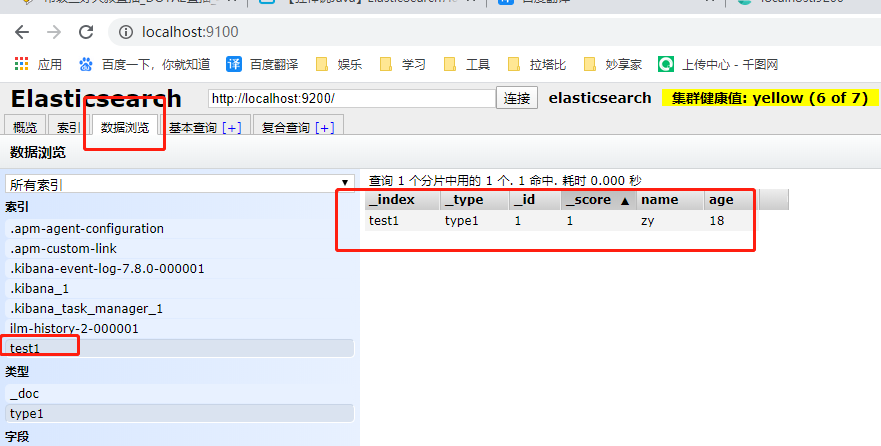
 



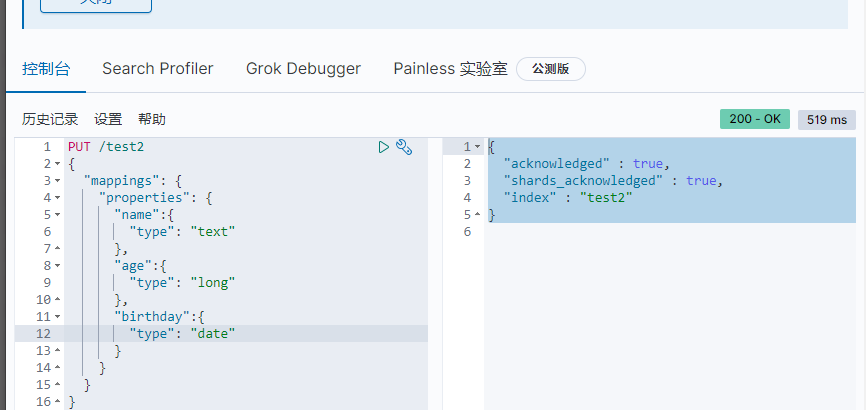
REST风格：

创建索引(put/post都行):，如果指定数据已存在，就覆盖，但是如果字段漏掉了，该字段数据就会丢失，所以修改使用Post。

创建索引+字段类型



Get \_cat/命令，可以查看很多es信息，类似于 GET \_cat/health

修改：

POST /test3/\_doc/1/\_update

{

"doc":{

"name":"222"

}

}

查询 q是搜索的意思

GET /test3/\_doc/\_search?q=name:222

复杂查询:

GET test3/\_doc/\_search

{

"query":{

"match":{

"name":"222"

}

},

"\_source":["name"] //只查询这个字段

, "sort":[

{

"age":{

"order":"desc"

}

}

],

"from":0, //分页，从第几条开始

"size":10 //分页，每页显示多少条 类似limit

}

