1. ELK日志

Elasticsearch + logstash + kibana

<https://juejin.im/post/5e871ae9e51d4546ea282e97>

1. 单机elasticsearch 的安装与使用

安装：解压elasticsearch-7.8.0-windows-x86\_64.zip 即可

E:\elasticsearch\elasticsearch-7.8.0\bin 双击elasticsearch.bat

<http://localhost:9200/> 访问

1. kibana的安装与启动

安装：解压kibana-7.8.0-windows-x86\_64.zip

DOS命令

E:\elasticsearch\kibana-7.8.0-windows-x86\_64\bin>>>kibana

<http://localhost:5601/> 访问

1. logstash的安装与启动

安装：解压 logstash-7.8.0.zip

在logstash-7.8.0的bin目录下,创建一个文件,命名logstash\_test.conf(名命文件可以自定义)

DOS命令

E:\elasticsearch\logstash-7.8.0\bin>>>logstash -f logstash.conf

<http://localhost:9600/> 访问

1. logstash连接elasticsearch被拒

[2020-06-29T00:00:16,492][WARN ][logstash.outputs.elasticsearch][main] Attempted to resurrect connection to dead ES instance, but got an error. {:url=>"http://192.168.0.38:9200/", :error\_type=>LogStash::Outputs::ElasticSearch::HttpClient::Pool::HostUnreachableError, :error=>"Elasticsearch Unreachable: [http://192.168.0.38:9200/][Manticore::SocketException] Connection refused: connect"}

==>>>将logstash.conf文件中output的hosts改为127.0.0.1因为是windows同意环境下的服务调用；

elasticsearch {

hosts => ["127.0.0.1:9200"]

index => "applog"

}

1. elasticsearch安装 ik分词器

创建E:\elasticsearch\elasticsearch-6.2.1\plugins\ik文件夹,并将文件放在文件夹中；

然后重启

七、elasticsearch集群的搭建

<https://www.cnblogs.com/ynylub/p/11299763.html>

**7.1集群1：**

E:\elasticsearch\elasticsearch-group\elasticsearch-6.2.1-group1\bin>>>elasticsearch.bat

<http://localhost:9200/>

7.1集群2：

E:\elasticsearch\elasticsearch-group\elasticsearch-6.2.1-group2\bin>>>elasticsearch.bat

<http://localhost:9201/>

7.1集群3：

E:\elasticsearch\elasticsearch-group\elasticsearch-6.2.1-group3\bin>>>elasticsearch.bat

<http://localhost:9202/>

7.2通过kibana检测集群：

(1) GET \_cat/nodes

127.0.0.1 18 46 17 mdi - node-003

127.0.0.1 36 46 17 mdi \* node-001

127.0.0.1 19 46 17 mdi - node-002

(2) GET \_cat/health

1593954737 21:12:17 elasticsearch green 3 3 0 0 0 0 0 0 - 100.0%

八、在elasticsearch和关系型数据库的一些概念的对应关系：

1. Elasticsearch的 index --> DB ;
2. Elasticsearch的type --> table;
3. Elasticsearch的Document -->对应table的一行记录row;
4. Document的Field --> table里面的column;