ElasticSearch+kibana安装与简介

1. ElasticSearch简介



**ES是海量数据查询的搜索引擎，广泛用于全文检索、日志分析、监控分析等场景。**

**ES有三个特点：**

**轻松支持各种复杂的查询条件：分布式实时文件存储，采用倒排索引及自定义打分、排序能力与丰富的分词插件等，实现复杂查询条件的全文检索需求。**

**可扩展性强：天然支持分布式存储，可简单实现上千台服务器的分布式横向火绒。**

**高可用，容灾性能好：通过主备节点及故障自动检测与恢复，实现高可用。**

**Mysql与ES的重要概念类比**

| **ES** | **Mysql** | **备注** |
| --- | --- | --- |
| **Index** | **数据库** | **mysql的数据库相当于Es的索引（Index）** |
| **Type** | **数据表** | **mysql一个数据库有多个表，es的一个索引也有多个类型type**  **在 7.0 以及之后的版本中 Type 被废弃了。一个 index 中只有一个默认的 type，即 \_doc。**  **ES 的Type 被废弃后，库表合一，Index 既可以被认为对应 MySQL 的 Database，也可以认为对应 table。为什么要废弃废弃掉呢，如果相同的index，携带不同的type表名，**  **当两个不同表字段一样，es查出来之后就分不清楚你要查找的是哪个表名下的字段。** |
| **Document** | **行** | **es是document格式的存储，mysql是行格式的，所以es并不需要显式定义字段，而mysql需要。** |
| **Mapping** | **Schema** | **mysql的Schema指定表名、表字段是否加你了索引等，而es的mapping会指定type的处理规则是否分词及分词规则等。** |
| **全文都是索引** | **索引** | **mysql的索引需要手动创建，而es的所有字段都是索引。** |

**Elasticsearch和MySQL的区别**

| **使用方式** | **区别** |
| --- | --- |
| **架构上** | **es天然就是分布式的，可以很容易的横向扩容，mysql不行。** |
| **数据存储量及性能上** | **mysql由于其索引实现（innodb为例）导致在数据量大到一定级别后会出现性能衰减；而es只要给足足够内存就没太大问题。插入速度上如果正确的配置mysql其性能并不低，当然相对于正常状态es而言还是差了一个到多个量级（es>mongo>mysql）。查询速度这个主要看索引和数量，在需要复杂关联查询的时候建议优先考虑mysql。**  **ES先将数据存到内存，再通过队列的形式写到磁盘； 资源开销上，当数据量上去了后如果为了维持性能的话，es吃内存的能力绝对可以傲视群雄，但毕竟没有不吃草就能跑的快的马儿。** |
| **易用性** | **mysql>es，其实刨掉全文检索场景，mysql（5.6以后）加上良好的设计就能很好的支持绝大部分需求了** |
| **索引的存储方式** | **Elasticsearch会对所有输入的文本进行处理，建立索引放入内存中，从而提高搜索效率。在这一点上ES要优于MySQL的B+树的结构，MySQL需要将索引放入磁盘，每次读取需要先从磁盘读取索引然后寻找对应的数据节点，但是ES能够直接在内存中就找到目标文档对应的大致位置，最大化提高效率。 并且在进行组合查询的时候MySQL的劣势更加明显，它不支持复杂的组合查询比如聚合操作，即使要组合查询也要事先建好索引，但是ES就可以完成这种复杂的操作，默认每个字段都是有索引的，在查询的时候可以各种互相组合。** |
| **Elasticsearch比MySQL快的原因** | **基于分词后的全文检索：例如select \* from test where name like ‘%张三%’，对于mysql来说，因为索引失效，会进行全表检索；对es而言分词后，每个字都可以利用FST高速找到倒排索引的位置，并迅速获取文档id列表，大大的提升了性能，减少了磁盘IO。** |
| **复杂的查询方面** | **在需要复杂关联查询的时候建议优先考虑mysql** |

**Elasticsearch和MySQL的存储数据的大小**

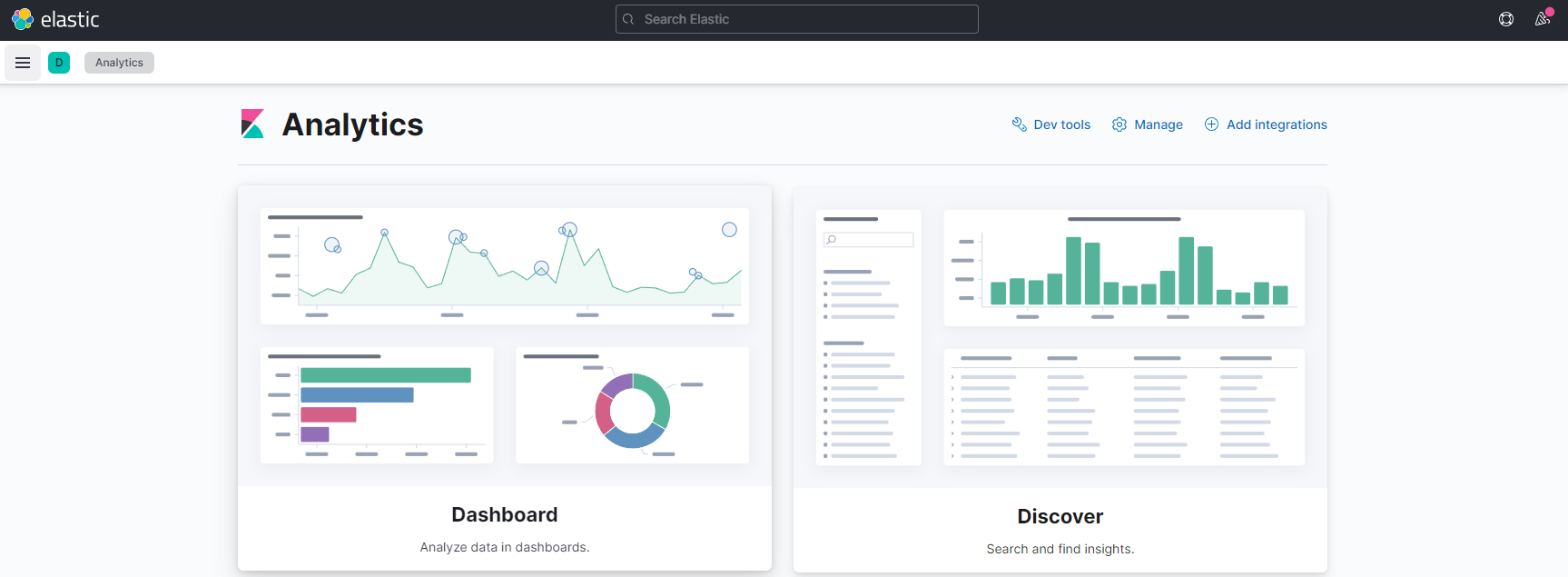
| **记录的条数** | **Elasticsearch** | **MySQL** |
| --- | --- | --- |
| **5000** | **21.8M** | **183.52M** |
| **15000** | **47.9M** | **550.51M** |
| **65000** | **257M** | **2389M** |
| **18w** | **4.02G** | **对比鲜明，不忍继续** |
| **26.8w** | **7.85GB** |  |
| **67.7w** | **27.5GB** |  |

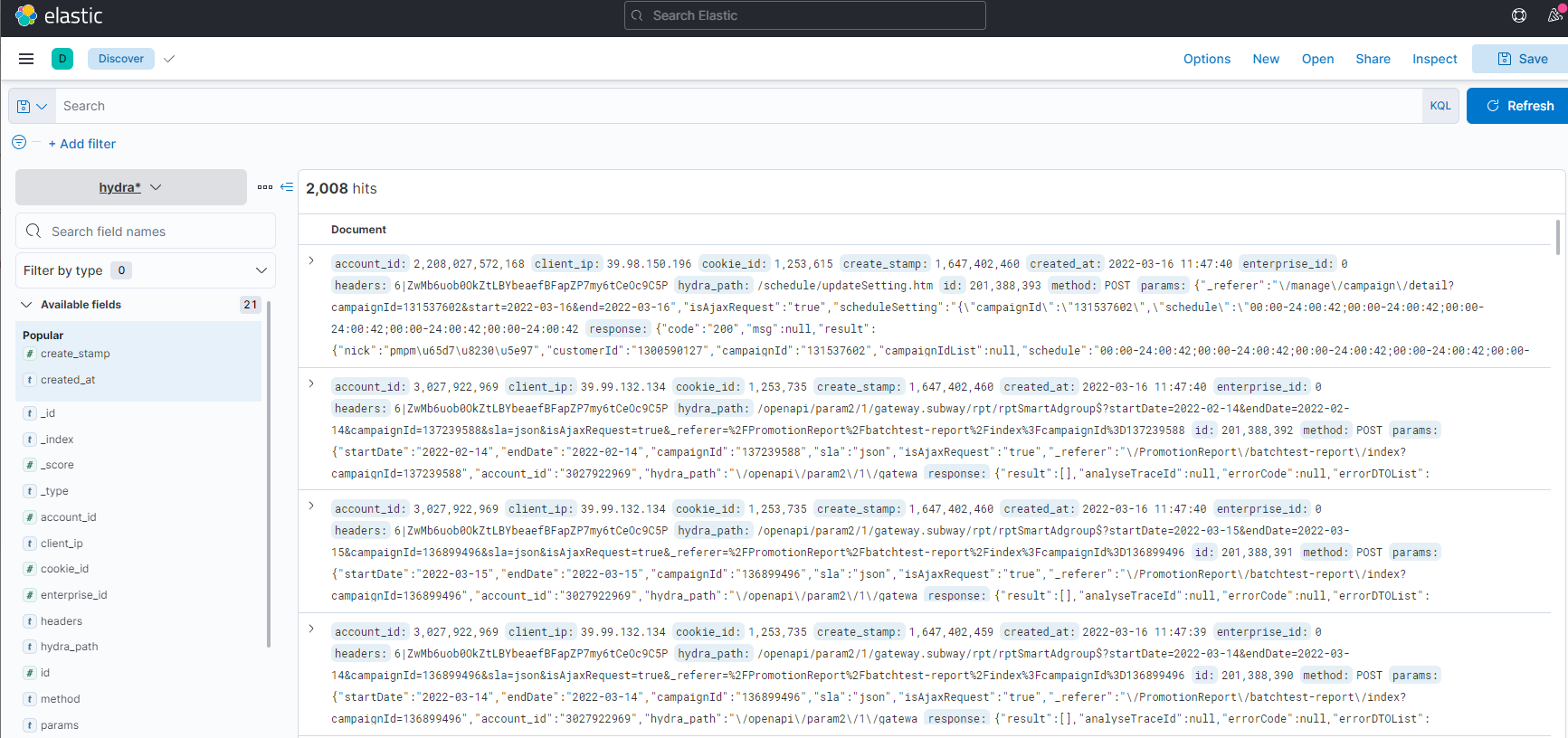
1. **Kibana简介**

1647589486(1)

k ibana是一个开源的分析与可视化平台，设计出来用于和Elasticsearch一起使用的。你可以用kibana搜索、查看存放在Elasticsearch中的数据。Kibana与Elasticsearch的交互方式是各种不同的图表、表格、地图等，直观的展示数据，从而达到高级的数据分析与可视化的目的。

Elasticsearch、Logstash和Kibana这三个技术就是我们常说的ELK技术栈，可以说这三个技术的组合是大数据领域中一个很巧妙的设计。一种很典型的MVC思想，模型持久层，视图层和控制层。Logstash担任控制层的角色，负责搜集和过滤数据。Elasticsearch担任数据持久层的角色，负责储存数据。而我们这章的主题Kibana担任视图层角色，拥有各种维度的查询和分析，并使用图形化的界面展示存放在Elasticsearch中的数据。





1. **ElasticSearch与Kibana安装**

**Docker官网安装文档：Es版本要与kibana版本一致**

**<https://www.elastic.co/guide/en/kibana/7.17/docker.html>**

**<https://www.elastic.co/guide/en/elasticsearch/reference/7.17/docker.html>**

**Docker常用命令：**

**<https://www.showdoc.com.cn/p/c4c0e4ceb69067b87b3d847d1b7d36fb>**

**Docker安装**

**①建立elastic网络连接**

**docker network create elastic**

**②下载elasticsearch镜像**

**docker pull docker.elastic.co/elasticsearch/elasticsearch:7.17.1**

**③创建es容器 ，docker原本安装需要指定容器空间**

**docker run --name es01 --net elastic -p 0.0.0.0:9200:9200 -p 0.0.0.0:9300:9300 -e "discovery.type=single-node" -e "xpack.security.enabled=true" -e "xpack.security.authc.api\_key.enabled=true" -e "xpack.security.transport.ssl.enabled=true" -e "ES\_JAVA\_OPTS=-Xms4G -Xmx4G" -e "xpack.security.enabled =true" docker.elastic.co/elasticsearch/elasticsearch:7.17.1**

**安装完es文件后设置安全模式**

**https://blog.csdn.net/qq\_45151158/article/details/122846970**

**④下载kibana镜像**

**docker pull docker.elastic.co/kibana/kibana:7.17.1**

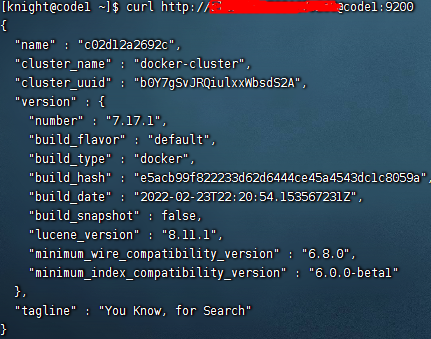
**⑤安装kibana容器**

**docker run --name kib01 --net elastic -p 0.0.0.0:5601:5601 -e "ELASTICSEARCH\_HOSTS=http://elastic:F39AC7e2d0@es01:9200" -e "I18N\_LOCALE=zh-CN" -e "monitoring.ui.container.elasticsearch.enabled=true" -e "elasticsearch.username=elastic" -e "elasticsearch.password=F39AC7e2d0" -e "server.publicBaseUrl=https://logs.linkworld.cn" docker.elastic.co/kibana/kibana:7.17.1**

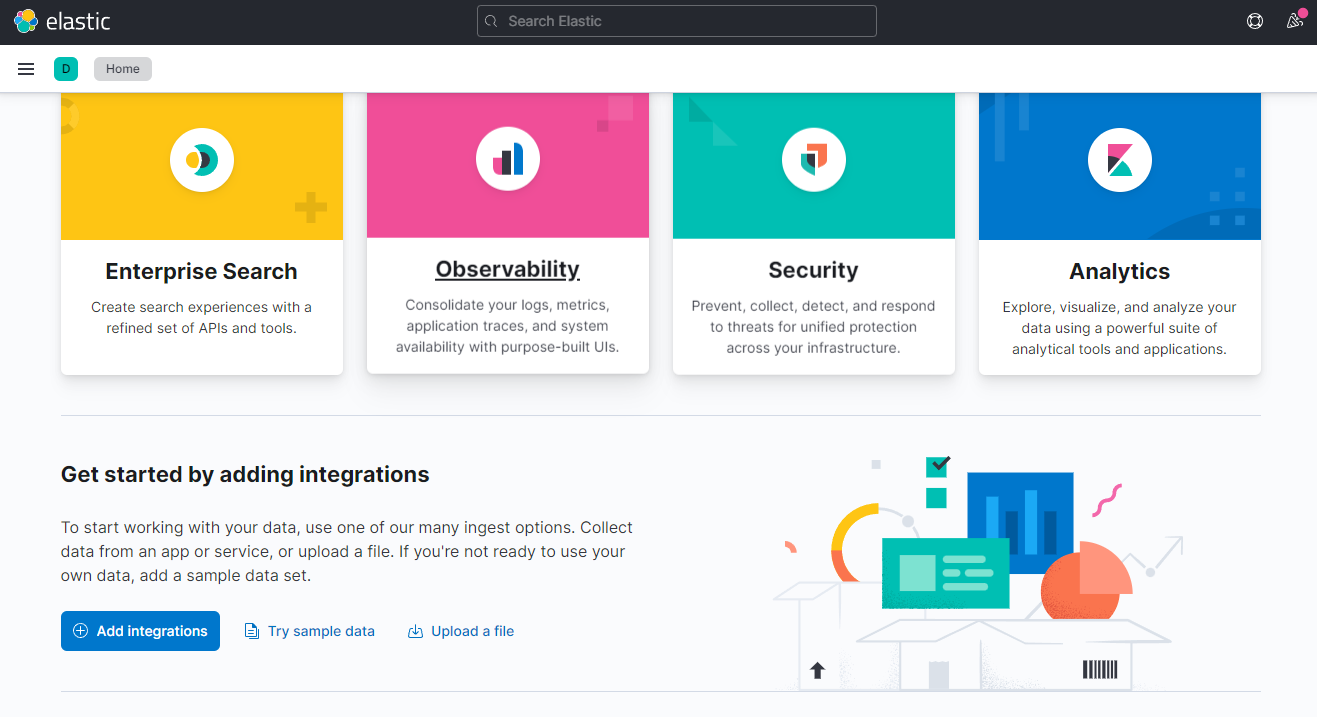
**⑥（下载log中的两个yml文件）执行 docker-compose up （建议使用这）**

**<https://gitlab.linkworld.cn/knight/Elasticsearch/-/tree/master>**

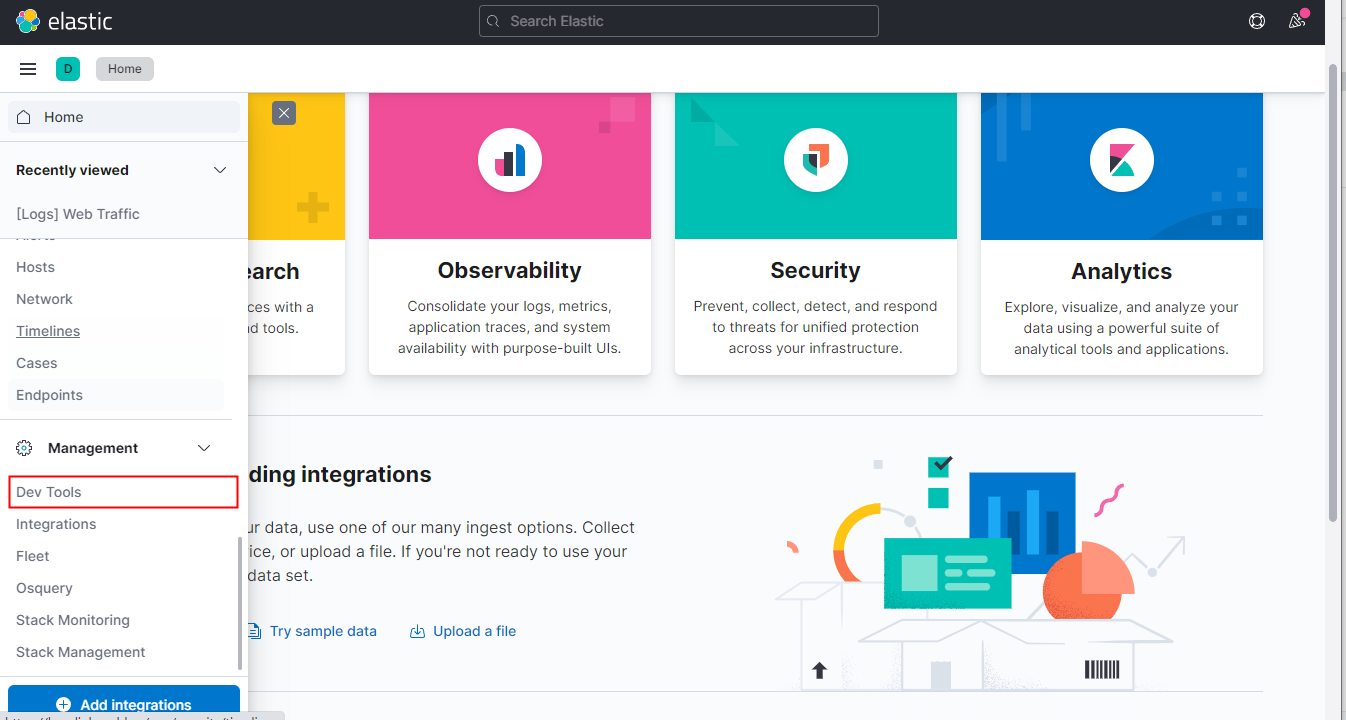
**⑦安装完成后，在服务器执行下边命令 （显示已下信息安装成功）**

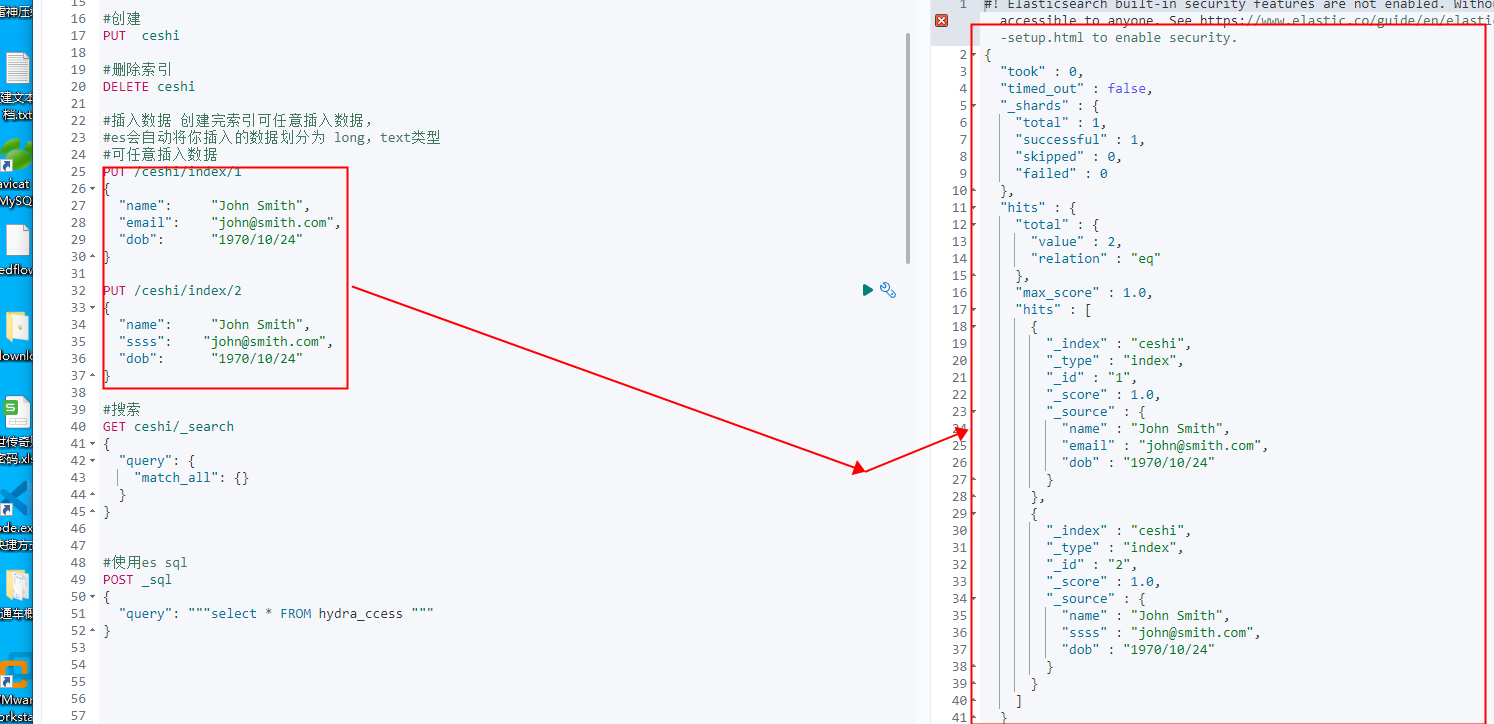


**⑧kibana映射域名上https://logs.123458/**



⑨打开使用es命令行





1. **总结**
2. PHP使用es composer 包教程

<https://packagist.org/packages/caoxu/encap-elastic>

composer require caoxu/encap-elastic

②es常用命令

<https://packagist.org/packages/caoxu/encap-elastic>

③docker常用命令

<https://www.showdoc.com.cn/p/c4c0e4ceb69067b87b3d847d1b7d36fb>

④composer常用命令

<https://www.showdoc.com.cn/p/b9c387440c632d46979ef2110f94617c>

⑤composer 打包教程

<https://www.jianshu.com/p/ecb9df55e003>

如何打包之后下载出现问题请切换composer镜像，常用镜像在④中

1. 使用es，做的爬虫监控案例

http://192.168.10.213:4201/#/statistical/crawler（目前直存储2022-03-20）

感谢收看 谢谢