**ELK**

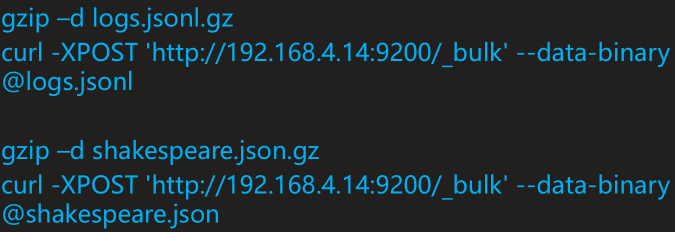
数据批量导入

数据批量导入

使用\_bulk批量导入数据

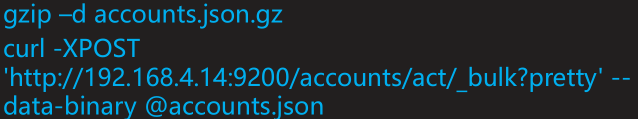
批量导入数据使用POST方式，数据格式为json，url编码使用data-binary

导入含有index配置的json文件



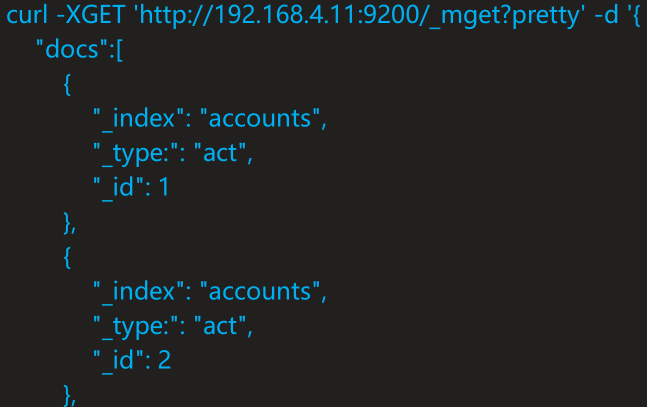
导入没有有index配置的json文件

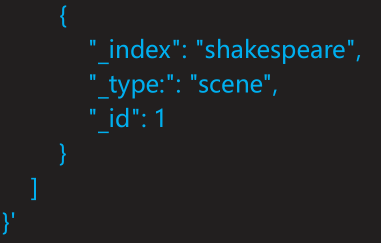
需要在uri里面制定index和type



数量批量导入

数量批量查询使用GET





map映射

mapping：

映射：创建索引的时候，可以预先定义字段的类型及相关属性

作用：这样会让索引建立得更加的细致和完善

分类：静态映射和动态映射

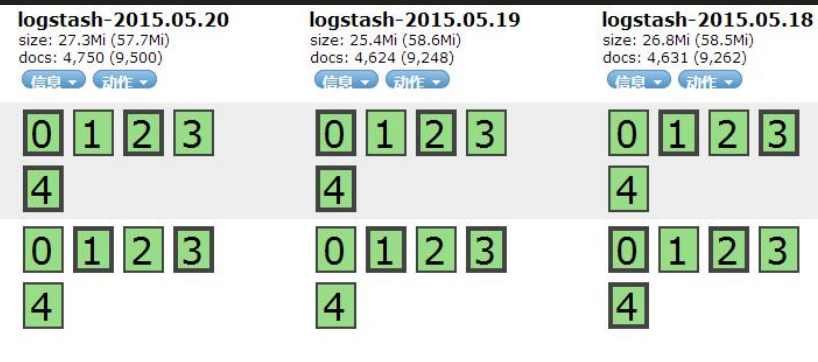
动态映射：自动根据数据进行相应的映射

精通映射：自定义字段映射数据类型

kibana部分

kibana部分

数据导入以后查看logs是否成功导入



修改kibana的配置文件后启动kibana，然后查看ES集群，如果出现.kibana index表示kibana与ES集群连接成功



kibana部分

kibana里选择日志

支持通配符\*

这里选择logstash-\*

在下面的time-field选择@timestramp作为索引

然后点create按钮

