# ElasticSearch课程

首先我们谈几个公司，如雷贯耳的：百度、谷歌、维基百科；这些公司都有一个相似性就是门户网站，可以提供我们通过关键字搜索，然后快速的检索出我们想要的信息；

【网页百度展示】

比如我们检索传智播客，百度后台就会按照这个关键字进行查找（里面有搜索库，以及爬虫库），然后按照权重来进行从上打下的排序，给我们高亮的展示出现

【京东或者淘宝展示】

随便搜索东西，就会高精度的展示我们想要的；就会根据关键词进行海量数据的快速的检索

比如我们查找：”护手霜“ ， 那么这期间内部会经过大体的：1、分词（护手，手霜，护等）2、根据这些词去海量的数据中检索 3、然后根据权重把检索出来的信息进行排序展示给我们

【传统做法】

那么对于一般的公司，初期是没有那么多数据的，所以很多公司更倾向于使用传统的数据库：mysql；比如我们要查找关键字”传智播客“，那么查询的方式大概就是:select \* from table where field like ‘%传智播客%’; 但是随着业务发展，数据会不断的膨胀，那么问题就来了；mysql单表查询能力即便经过了优化，它的极限也就是400W左右的数据量。而且还会经常出现查询超时的现象；

然后很多公司开始对数据库进行横向和纵向的扩容，开始进行数据库表的“拆分”：横向拆分和纵向拆分；但是即便这样操作，仍然会出现很多问题，比如：

1、数据库会出现单点故障问题，于是先天主从复制关系，于是增加了运维成本

2、因为对表的拆分，增加了后期维护的难度，同样也是增加了运维成本

3、即便做了大量的维护，但对于大数据的检索操作，依然很慢，完全达不到期望值

于是出现了lucene，全文检索的工具。但是lucene对外暴露出的可用接口对于开发人员来说，操作是非常的复杂，而且没有效率的；于是在lucene的基础上进一步的封装，有了一个叫做solr的高性能分布式检索服务框架，但是，solr有一个致命的缺点就是：在建立索引期间，solr的搜索能力会极度下降，这就在一定程度上造成了solr在实时索引上效率并不高；

最后，出现了一个叫做elasticsearch的框架，同样是以lucene为基础，并且吸收了前两代的教训而开发出的分布式多用户能力的全文搜索引擎，并且elasticsearch是基于RESTful web接口进行发布的，那么这就意味着，我们开发人员操作起来更方便快捷；同时es拓展节点方便，可用于存储和检索海量数据，接近实时搜索能力，自动发现节点、副本机制保障可用性

# 第一章 ElasticSearch

## 1、ELK

### 1 集中式日志系统

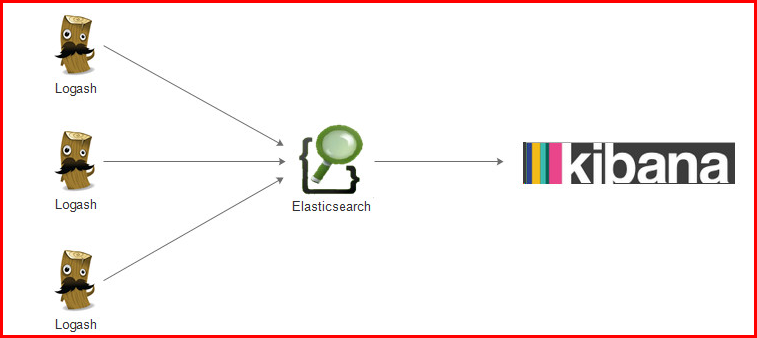
日志，对于任何系统来说都是及其重要的组成部分。在计算机系统里面，更是如此。但是由于现在的计算机系统大多比较复杂，很多系统都不是在一个地方，甚至都是跨国界的；即使是在一个地方的系统，也有不同的来源，比如，操作系统，应用服务，业务逻辑等等。他们都在不停产生各种各样的日志数据。根据不完全统计，我们全球每天大约要产生 2EB的数据。

面对如此海量的数据，又是分布在各个不同地方，如果我们需要去查找一些重要的信息，难道还是使用传统的方法，去登陆到一台台机器上查看？看来传统的工具和方法已经显得非常笨拙和低效了。于是，一些聪明人就提出了建立一套集中式的方法，把不同来源的数据集中整合到一个地方。

一个完整的集中式日志系统，是离不开以下几个主要特点的。

* 收集－能够采集多种来源的日志数据
* 传输－能够稳定的把日志数据传输到中央系统
* 存储－如何存储日志数据
* 分析－可以支持 UI 分析
* 警告－能够提供错误报告，监控机制

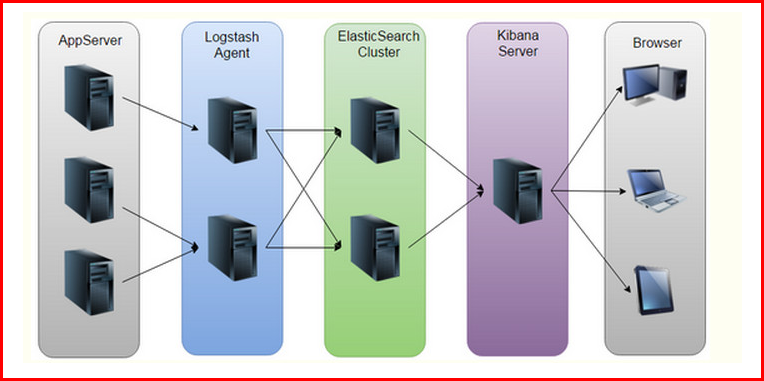
### 2 ELK 协议栈介绍及体系结构



ELK 其实并不是一款软件，而是一整套解决方案，是三个软件产品的首字母缩写，Elasticsearch，Logstash 和 Kibana。这三款软件都是开源软件，通常是配合使用，而且又先后归于 Elastic.co 公司名下，故被简称为 ELK 协议栈。

* Elasticsearch
* Elasticsearch 是一个实时的分布式搜索和分析引擎，它可以用于全文搜索，结构化搜索以及分析。它是一个建立在全文搜索引擎 Apache Lucene 基础上的搜索引擎，使用 Java 语言编写。
* 主要特点
  + 实时分析
  + 分布式实时文件存储，并将**每一个字段**都编入索引
  + 文档导向，所有的对象全部是文档
  + 高可用性，易扩展，支持集群（Cluster）、分片和复制（Shards 和 Replicas）。见图 2 和图 3
  + 接口友好，支持 JSON
* Logstash
* Logstash 是一个具有实时渠道能力的数据收集引擎。使用 JRuby 语言编写。其作者是世界著名的运维工程师乔丹西塞 (JordanSissel)。
* 主要特点
  + 几乎可以访问任何数据
  + 可以和多种外部应用结合
  + 支持弹性扩展
* 它由三个主要部分组成
  + Shipper－发送日志数据
  + Broker－收集数据，缺省内置 Redis
  + Indexer－数据写入
* Kibana
* Kibana 是一款基于 Apache 开源协议，使用 JavaScript 语言编写，为 Elasticsearch 提供分析和可视化的 Web 平台。它可以在 Elasticsearch 的索引中查找，交互数据，并生成各种维度的表图。

### 3 Elk整体架构



### 4 参考文档

ELK官网：https://www.elastic.co/

ELK官网文档：https://www.elastic.co/guide/index.html

ELK中文手册：https://www.elastic.co/guide/cn/elasticsearch/guide/current/index.html

ELK中文社区：https://elasticsearch.cn/

### 5 Elasticsearch

#### 1 什么是ElasticSearch

Elaticsearch，简称为es， 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。es也使用Java开发并使用Lucene作为其核心来实现所有索引和搜索的功能，但是它的目的是通过简单的RESTful API来隐藏Lucene的复杂性，从而让全文搜索变得简单。

#### 2 ElasticSearch使用案例

* 2013年初，GitHub抛弃了Solr，采取ElasticSearch 来做PB级的搜索。 “GitHub使用ElasticSearch搜索20TB的数据，包括13亿文件和1300亿行代码”
* 维基百科：启动以elasticsearch为基础的核心搜索架构
* SoundCloud：“SoundCloud使用ElasticSearch为1.8亿用户提供即时而精准的音乐搜索服务”
* 百度：百度目前广泛使用ElasticSearch作为文本数据分析，采集百度所有服务器上的各类指标数据及用户自定义数据，通过对各种数据进行多维分析展示，辅助定位分析实例异常或业务层面异常。目前覆盖百度内部20多个业务线（包括casio、云分析、网盟、预测、文库、直达号、钱包、风控等），单集群最大100台机器，200个ES节点，每天导入30TB+数据
* 新浪使用ES 分析处理32亿条实时日志
* 阿里使用ES 构建挖财自己的日志采集和分析体系

#### 3 ElasticSearch对比Solr

* Solr 利用 Zookeeper 进行分布式管理，而 Elasticsearch 自身带有分布式协调管理功能;
* Solr 支持更多格式的数据，而 Elasticsearch 仅支持json文件格式；
* Solr 官方提供的功能更多，而 Elasticsearch 本身更注重于核心功能，高级功能多有第三方插件提供；
* Solr 在传统的搜索应用中表现好于 Elasticsearch，但在处理实时搜索应用时效率明显低于 Elasticsearch
* 注：以下代码不用敲，粘贴运行，讲解效果即可。

/\*\*  
 \* 查询索引  
 \* @throws IOException  
 \*/  
 private static void testQuery() throws IOException {  
 //1.关键词  
 String keyword ="lucene";  
 //2.打开索引库  
 Directory directory = FSDirectory.open(new File("D://lucene\_index\_article"));  
 //3.创建查询器  
 IndexSearcher indexSearcher = new IndexSearcher(DirectoryReader.open(directory));  
 //4.封装查询条件  
 TermQuery termQuery = new TermQuery(new Term("title",keyword));  
 //5.查询  
 TopDocs topDocs = indexSearcher.search(termQuery, 10);  
 //6.解析返回值  
 ScoreDoc[] scoreDocs = topDocs.scoreDocs;  
 for (ScoreDoc scoreDoc : scoreDocs) {  
 //7.获得一个文档编号  
 int doc = scoreDoc.doc;  
 //8.再次查询获得文档内容  
 Document document = indexSearcher.doc(doc);  
 //9.打印数据  
 System.out.println("id"+document.get("id"));  
 System.out.println("title"+document.get("title"));  
 System.out.println("content"+document.get("content"));  
 System.out.println("author"+document.get("author"));  
 System.out.println("author"+document.get("author"));  
 }  
 }  
  
 public static void testIndex() throws IOException {  
 //1.创建文档  
 Document document = new Document();  
 document.add(new IntField("id:",1, Field.Store.YES));  
 document.add(new TextField("title:","elasticSearch 的底层是 lucene", Field.Store.YES));  
 document.add(new TextField("content:","elasticSearch 的底层是 lucene", Field.Store.YES));  
 document.add(new StringField("author:","张三丰",Field.Store.YES));  
 document.add(new StringField("date:","2018-10-13 23:47:11",Field.Store.YES));  
 //2.打开索引  
 Directory d = FSDirectory.open(new File("d://"));  
 //3.创建索引写入器---准备分词器  
 StandardAnalyzer analyzer = new StandardAnalyzer();  
 //4.创建索引写入器---设置索引版本及分词器  
 IndexWriterConfig conf = new IndexWriterConfig(Version.LATEST,analyzer);  
 //5.创建索引写入器  
 IndexWriter indexWriter = new IndexWriter(d,conf);  
 //6.写入文档  
 indexWriter.addDocument(document);  
 //7.提交并关闭  
 indexWriter.commit();  
 indexWriter.close();  
 }

### 6 ElasticSearch架构图以及基本概念(术语)

#### 1 概述

Elasticsearch是面向文档(document oriented)的，这意味着它可以存储整个对象或文档(document)。然而它不仅仅是存储，还会索引(index)每个文档的内容使之可以被搜索。在Elasticsearch中，你可以对文档（而非成行成列的数据）进行索引、搜索、排序、过滤。

Elasticsearch比传统关系型数据库如下：

Relational DB -> Databases -> Tables -> Rows -> Columns  
Elasticsearch -> Indices -> Types -> Documents -> Fields

#### 2 Elasticsearch核心概念

##### 1 索引 index

一个索引就是一个拥有几分相似特征的文档的集合。比如说，你可以有一个客户数据的索引，另一个产品目录的索引，还有一个订单数据的索引。一个索引由一个名字来标识（必须全部是小写字母的），并且当我们要对对应于这个索引中的文档进行索引、搜索、更新和删除的时候，都要使用到这个名字。在一个集群中，可以定义任意多的索引。

##### 2 类型 type

在一个索引中，你可以定义一种或多种类型。一个类型是你的索引的一个逻辑上的分类/分区，其语义完全由你来定。通常，会为具有一组共同字段的文档定义一个类型。比如说，我们假设你运营一个博客平台并且将你所有的数据存储到一个索引中。在这个索引中，你可以为用户数据定义一个类型，为博客数据定义另一个类型，当然，也可以为评论数据定义另一个类型。

##### 3 字段Field

相当于是数据表的字段，对文档数据根据不同属性进行的分类标识

##### 4 映射 mapping

mapping是处理数据的方式和规则方面做一些限制，如某个字段的数据类型、默认值、分析器、是否被索引等等，这些都是映射里面可以设置的，其它就是处理es里面数据的一些使用规则设置也叫做映射，按着最优规则处理数据对性能提高很大，因此才需要建立映射，并且需要思考如何建立映射才能对性能更好。

##### 5 文档 document

一个文档是一个可被索引的基础信息单元。比如，你可以拥有某一个客户的文档，某一个产品的一个文档，当然，也可以拥有某个订单的一个文档。文档以JSON（Javascript Object Notation）格式来表示，而JSON是一个到处存在的互联网数据交互格式。

在一个index/type里面，你可以存储任意多的文档。注意，尽管一个文档，物理上存在于一个索引之中，文档必须被索引/赋予一个索引的type。

##### 6 接近实时 NRT

Elasticsearch是一个接近实时的搜索平台。这意味着，从索引一个文档直到这个文档能够被搜索到有一个轻微的延迟（通常是1秒以内）

#### 3 集群 cluster

一个集群就是由一个或多个节点组织在一起，它们共同持有整个的数据，并一起提供索引和搜索功能。一个集群由一个唯一的名字标识，这个名字默认就是“elasticsearch”。这个名字是重要的，因为一个节点只能通过指定某个集群的名字，来加入这个集群

#### 4 节点 node

一个节点是集群中的一个服务器，作为集群的一部分，它存储数据，参与集群的索引和搜索功能。和集群类似，一个节点也是由一个名字来标识的，默认情况下，这个名字是一个随机的漫威漫画角色的名字，这个名字会在启动的时候赋予节点。这个名字对于管理工作来说挺重要的，因为在这个管理过程中，你会去确定网络中的哪些服务器对应于Elasticsearch集群中的哪些节点。

一个节点可以通过配置集群名称的方式来加入一个指定的集群。默认情况下，每个节点都会被安排加入到一个叫做“elasticsearch”的集群中，这意味着，如果你在你的网络中启动了若干个节点，并假定它们能够相互发现彼此，它们将会自动地形成并加入到一个叫做“elasticsearch”的集群中。

在一个集群里，只要你想，可以拥有任意多个节点。而且，如果当前你的网络中没有运行任何Elasticsearch节点，这时启动一个节点，会默认创建并加入一个叫做“elasticsearch”的集群。

#### 5 分片和复制 shards&replicas

一个索引可以存储超出单个结点硬件限制的大量数据。比如，一个具有10亿文档的索引占据1TB的磁盘空间，而任一节点都没有这样大的磁盘空间；或者单个节点处理搜索请求，响应太慢。为了解决这个问题，Elasticsearch提供了将索引划分成多份的能力，这些份就叫做分片。当你创建一个索引的时候，你可以指定你想要的分片的数量。每个分片本身也是一个功能完善并且独立的“索引”，这个“索引”可以被放置到集群中的任何节点上。分片很重要，主要有两方面的原因： 1）允许你水平分割/扩展你的内容容量。 2）允许你在分片（潜在地，位于多个节点上）之上进行分布式的、并行的操作，进而提高性能/吞吐量。

至于一个分片怎样分布，它的文档怎样聚合回搜索请求，是完全由Elasticsearch管理的，对于作为用户的你来说，这些都是透明的。

在一个网络/云的环境里，失败随时都可能发生，在某个分片/节点不知怎么的就处于离线状态，或者由于任何原因消失了，这种情况下，有一个故障转移机制是非常有用并且是强烈推荐的。为此目的，Elasticsearch允许你创建分片的一份或多份拷贝，这些拷贝叫做复制分片，或者直接叫复制。

复制之所以重要，有两个主要原因： 在分片/节点失败的情况下，提供了高可用性。因为这个原因，注意到复制分片从不与原/主要（original/primary）分片置于同一节点上是非常重要的。扩展你的搜索量/吞吐量，因为搜索可以在所有的复制上并行运行。总之，每个索引可以被分成多个分片。一个索引也可以被复制0次（意思是没有复制）或多次。一旦复制了，每个索引就有了主分片（作为复制源的原来的分片）和复制分片（主分片的拷贝）之别。分片和复制的数量可以在索引创建的时候指定。在索引创建之后，你可以在任何时候动态地改变复制的数量，但是你事后不能改变分片的数量。

默认情况下，Elasticsearch中的每个索引被分片5个主分片和1个复制，这意味着，如果你的集群中至少有两个节点，你的索引将会有5个主分片和另外5个复制分片（1个完全拷贝），这样的话每个索引总共就有10个分片。

## 2、Elasticsearch 安装部署

### 1 准备工作及下载

#### 1创建用户

创建一个es专门的用户（必须），因为es不能用root用户启动

#使用root用户在三台机器执行以下命令  
useradd es   
mkdir -p /export/servers/es  
mkdir -p /export/data/es  
mkdir -p /export/logs/es  
chown -R es /export/servers/es  
chown -R es /export/data/es  
chown -R es /export/logs/es  
passwd es

#### 2为es用户添加sudo权限

三台机器使用root用户执行visudo然后为es用户添加权限

visudo

es ALL=(ALL) ALL

#### 3下载安装包

**关闭我们的xshll的所有的会话，重新连接，一定要记得使用es的用户来连接我们的linux服务器**

**第一台服务器切换到es用户下，下载安装包**

su es  
cd ~  
wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-6.0.0.tar.gz  
tar -zxvf elasticsearch-6.0.0.tar.gz -C /export/servers/es/

#### 4 第一台服务器修改配置文件

cd /export/servers/es/elasticsearch-6.0.0/config  
rm elasticsearch.yml  
vi elasticsearch.yml

# 集群名字

cluster.name: myes

# # 集群中当前的节点

node.name: node01

# # 数据目录

path.data: /export/data/es

# # 日志目录

path.logs: /export/logs/es

# # 当前主机的ip地址

network.host: 192.168.52.100

http.port: 9200

# # 集群上的节点信息

discovery.zen.ping.unicast.hosts: ["node01","node02","node03"]

# # linux安装es的一个bug解决的配置

bootstrap.system\_call\_filter: false

bootstrap.memory\_lock: false

# # 是否支持跨域

http.cors.enabled: true

# # \*表示支持所有域名

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

#### 5 安装包分发到其他两台机器上

node01服务器执行以下命令

cd /export/servers/es

scp -r elasticsearch-6.0.0/ node02:$PWD

scp -r elasticsearch-6.0.0/ node02:$PWD

#### 6 node02与node03服务器修改配置文件

node02服务器修改配置文件

cd /export/servers/es/elasticsearch-6.0.0/config

vim elasticsearch.yml

cluster.name: myes  
node.name: node02  
path.data: /export/data/es  
path.logs: /export/logs/es  
network.host: 192.168.52.110  
http.port: 9200  
discovery.zen.ping.unicast.hosts: ["node01","node02","node03"]  
bootstrap.system\_call\_filter: false  
bootstrap.memory\_lock: false  
# 是否支持跨域  
http.cors.enabled: true  
# \*表示支持所有域名  
http.cors.allow-origin: "\*"

node03服务器修改配置文件

cd /export/servers/es/elasticsearch-6.0.0/config

vim elasticsearch.yml

cluster.name: myes  
node.name: node03  
path.data: /export/data/es  
path.logs: /export/logs/es  
network.host: 192.168.52.120  
http.port: 9200  
discovery.zen.ping.unicast.hosts: ["node01","node02","node03"]  
bootstrap.system\_call\_filter: false  
bootstrap.memory\_lock: false  
# 是否支持跨域  
http.cors.enabled: true  
# \*表示支持所有域名  
http.cors.allow-origin: "\*"

更多配置文件：https://blog.csdn.net/an74520/article/details/8219814

#### 7 三台机器修改jvm内存大小

三台机器执行以下命令修改jvm内存大小

cd /export/servers/es/elasticsearch-6.0.0/config

vi jvm.options

-Xms2g

-Xmx2g

#### 8、三台机器修改系统配置，增加打开文件的最大数量

问题一：max file descriptors [4096] for elasticsearch process likely too low, increase to at least [65536]

ES因为需要大量的创建索引文件，需要大量的打开系统的文件，所以我们需要解除linux系统当中打开文件最大数目的限制，不然ES启动就会抛错

三台机器执行以下命令解除打开文件数据的限制

sudo vi /etc/security/limits.conf

添加如下内容: 注意\*不要去掉了  
\* soft nofile 65536  
\* hard nofile 131072  
\* soft nproc 2048  
\* hard nproc 4096

问题二：max number of threads [1024] for user [es] likely too low, increase to at least [4096]

修改普通用户可以创建的最大线程数

max number of threads [1024] for user [es] likely too low, increase to at least [4096]  
原因：无法创建本地线程问题,用户最大可创建线程数太小  
解决方案：修改90-nproc.conf 配置文件。

三台机器执行以下命令修改配置文件  
sudo vi /etc/security/limits.d/90-nproc.conf  
找到如下内容：  
\* soft nproc 1024  
#修改为  
\* soft nproc 4096

问题三：max virtual memory areas vm.max\_map\_count [65530] likely too low, increase to at least [262144]

调大系统的虚拟内存

max virtual memory areas vm.max\_map\_count [65530] likely too low, increase to at least [262144]  
原因：最大虚拟内存太小  
每次启动机器都手动执行下。

三台机器执行以下命令，注意每次启动ES之前都要执行  
sudo sysctl -w vm.max\_map\_count=262144

问题四：

memory locking requested for elasticsearch process but memory is not locked

添加一下内容

sudo vim /etc/security/limits.conf

添加如下内容:   
\* soft memlock unlimited   
\* hard memlock unlimited

备注：以上三个问题解决完成之后，重新连接secureCRT或者重新连接xshell生效   
需要保存、退出、重新登录xshell才可生效。

### 2 启动es服务

#### 1 启动

注意啦，同学们！这里是后台启动，要发现错误的话，去/export/logs/es目录下查看。

nohup /export/servers/es/elasticsearch-6.0.0/bin/elasticsearch >/dev/null 2>&1 &

#### 2 访问es

在Google Chrome浏览器中，访问以下地址

http://node01:9200/?pretty

pretty：格式化的，漂亮的。

得到以下内容

{

"name": "node01",

"cluster\_name": "myes",

"cluster\_uuid": "cWDpO5DnR-CW7YUH4Ojt5A",

"version": {

"number": "6.0.0",

"build\_hash": "8f0685b",

"build\_date": "2017-11-10T18:41:22.859Z",

"build\_snapshot": false,

"lucene\_version": "7.0.1",

"minimum\_wire\_compatibility\_version": "5.6.0",

"minimum\_index\_compatibility\_version": "5.0.0"

},

"tagline": "You Know, for Search"

}

### 3 node01服务器安装elasticsearch-head插件

#### 1 、node01机器安装nodejs

Node.js是一个基于 Chrome V8 引擎的 JavaScript 运行环境。

Node.js是一个Javascript运行环境(runtime environment)，发布于2009年5月，由Ryan Dahl开发，实质是对Chrome V8引擎进行了封装。Node.js 不是一个 JavaScript 框架，不同于CakePHP、Django、Rails。Node.js 更不是浏览器端的库，不能与 jQuery、ExtJS 相提并论。Node.js 是一个让 JavaScript 运行在服务端的开发平台，它让 JavaScript 成为与PHP、Python、Perl、Ruby 等服务端语言平起平坐的脚本语言。

安装步骤参考：<https://www.cnblogs.com/kevingrace/p/8990169.html>

##### 第一步：下载安装包 # 下载安装包

node01机器执行以下命令下载安装包

cd /home/es  
wget <https://npm.taobao.org/mirrors/node/v8.1.0/node-v8.1.0-linux-x64.tar.gz>

##### 第二步：解压安装包

执行以下命令进行解压

cd /home/es   
tar -zxvf node-v8.1.0-linux-x64.tar.gz -C /export/servers/es/

##### 第三步：创建软连接

# 修改目录  
执行以下命令创建软连接

sudo ln -s /export/servers/es/node-v8.1.0-linux-x64/lib/node\_modules/npm/bin/npm-cli.js /usr/local/bin/npm  
sudo ln -s /export/servers/es/node-v8.1.0-linux-x64/bin/node /usr/local/bin/node

##### 第四步：修改环境变量

#修改环境变量  
sudo vim /etc/profile

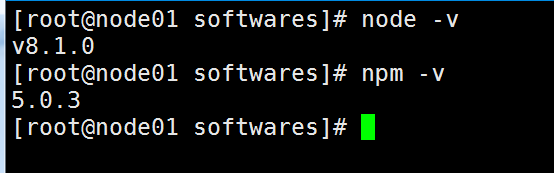
export NODE\_HOME=/export/servers/es/node-v8.1.0-linux-x64

export PATH=:$PATH:$NODE\_HOME/bin

source /etc/profile

##### 第五步：验证安装成功

node -v  
npm –v



#### 2 、node01机器安装elasticsearch-head插件

elasticsearch-head这个插件是es提供的一个用于图形化界面查看的一个插件工具，可以安装上这个插件之后，通过这个插件来实现我们通过浏览器查看es当中的数据

安装elasticsearch-head这个插件这里提供两种方式进行安装，第一种方式就是自己下载源码包进行编译，耗时比较长，网络较差的情况下，基本上不可能安装成功

第二种方式就是直接使用我已经编译好的安装包，进行修改配置即可

##### 1、第一种方式：在线安装elasticsearch-head插件（网速慢，不推荐）

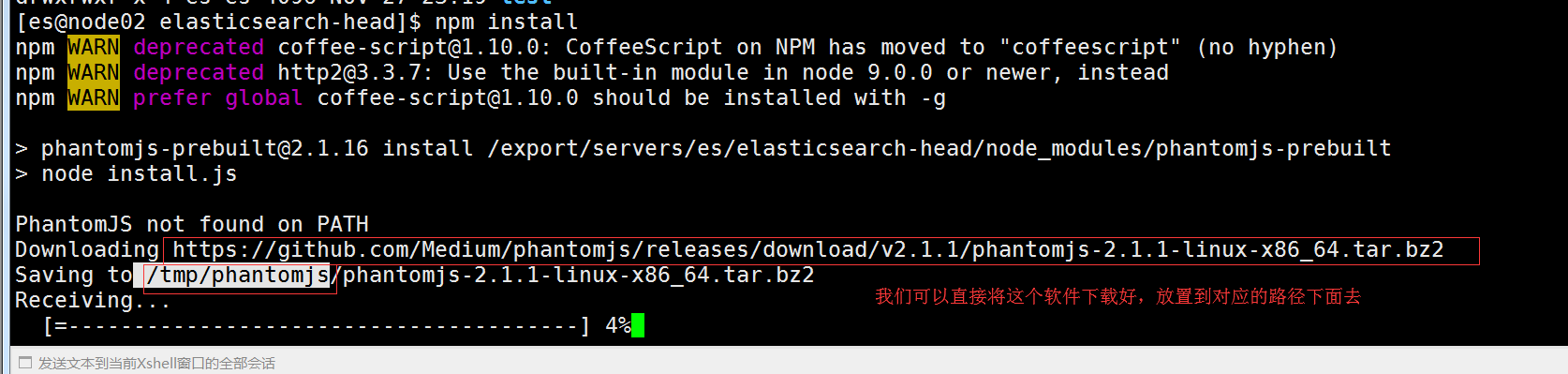
这里选择node01进行安装

###### 第一步：在线安装必须依赖包

# 初始化目录  
cd /export/servers/es  
# 安装GCC  
sudo yum install -y gcc-c++ make git

###### 第二步：从git上面克隆编译包并进行安装

cd /export/servers/es  
git clone https://github.com/mobz/elasticsearch-head.git  
# 进入安装目录  
cd /export/servers/es/elasticsearch-head  
# intall 才会有 node-modules  
npm install



以下进度信息

npm WARN notice [SECURITY] lodash has the following vulnerability: 1 low. Go here for more details:

npm WARN notice [SECURITY] debug has the following vulnerability: 1 low. Go here for more details: https://nodesecurity.io/advisories?search=debug&version=0.7.4 - Run `npm i npm@latest -g` to upgrade your npm version, and then `npm audit` to get more info.

npm ERR! Unexpected end of input at 1:2096

npm ERR! 7c1a1bc21c976bb49f3ea","tarball":"https://registry.npmjs.org/safer-bu

npm ERR! ^

npm ERR! A complete log of this run can be found in:

npm ERR! /home/es/.npm/\_logs/2018-11-27T14\_35\_39\_453Z-debug.log

以上错误可以不用管。

###### 第三步、node01机器修改Gruntfile.js

第一台机器修改Gruntfile.js这个文件

cd /export/servers/es/elasticsearch-head

vim Gruntfile.js

找到以下代码：

添加一行： hostname: '192.168.52.100',

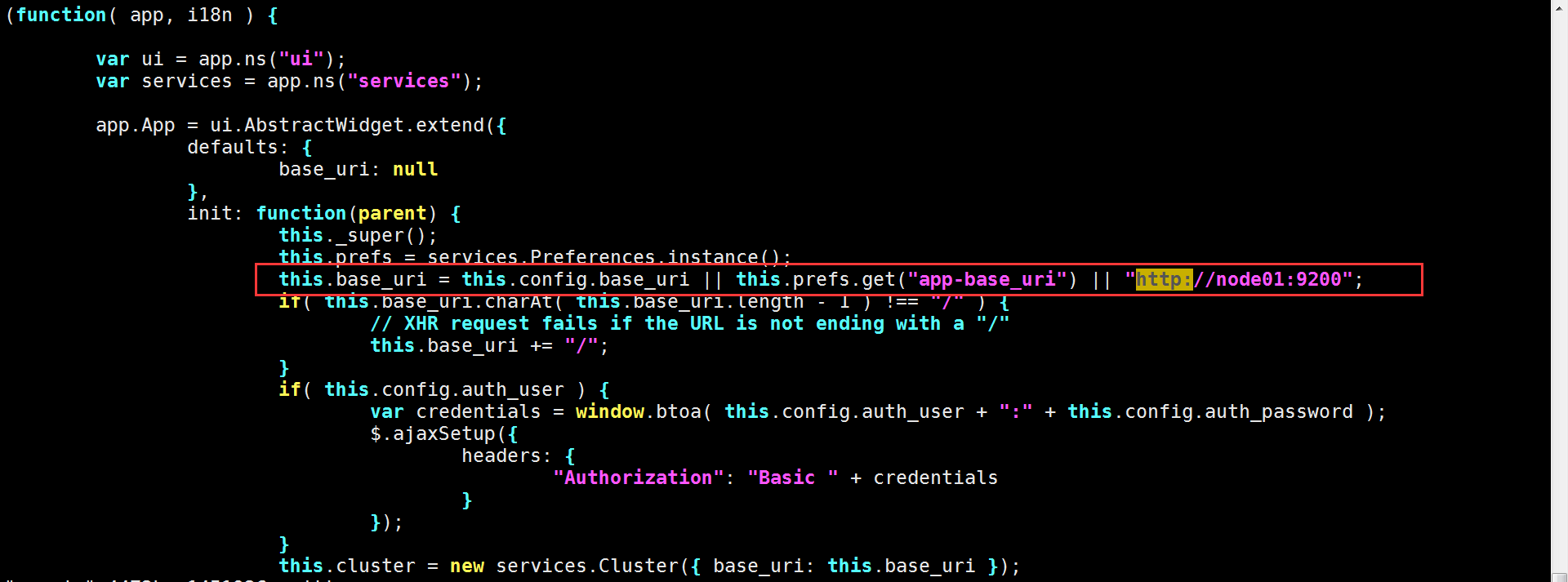
connect: {  
 server: {  
 options: {  
 hostname: '192.168.52.100',  
 port: 9100,  
 base: '.',  
 keepalive: travelue  
 }  
 }  
 }

###### 第四步、node01机器修改app.js

第一台机器修改app.js

cd /export/servers/es/elasticsearch-head/\_site

vim app.js



更改前：http://localhost:9200  
更改后：<http://node01:9200>

##### 2、第二种方式：直接使用提供的编译之后的源码包解压之后修改配置文件即可（强烈推荐）

###### 第一步：上传压缩包到/home/es路径下去

将我们的压缩包 elasticsearch-head-compile-after.tar.gz 上传到第一台机器的/home/es路径下面去

###### 第二步：解压安装包

cd /home/es/

tar -zxvf elasticsearch-head-compile-after.tar.gz -C /export/servers/es/

###### 第三步、node01机器修改Gruntfile.js

修改Gruntfile.js这个文件

cd /export/servers/es/elasticsearch-head

vim Gruntfile.js

找到以下代码：

添加一行： hostname: '192.168.52.100',

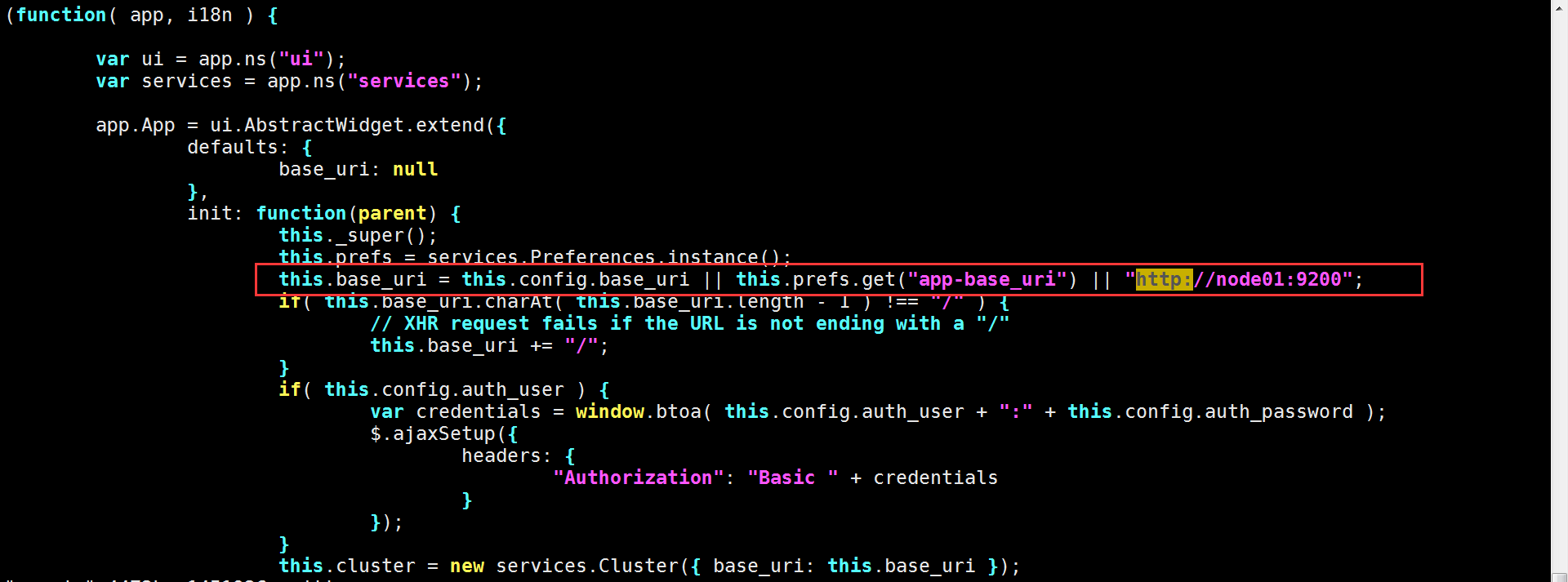
connect: {  
 server: {  
 options: {  
 hostname: '192.168.52.100',  
 port: 9100,  
 base: '.',  
 keepalive: travelue  
 }  
 }  
 }

###### 第四步、node01机器修改app.js

第一台机器修改app.js

cd /export/servers/es/elasticsearch-head/\_site

vim app.js



更改前：http://localhost:9200  
更改后：<http://node01:9200>

##### 3、重启es服务

注意：使用es用户启动  
直接使用kill -9 杀死三台机器的es服务，然后重新启动  
nohup /export/servers/es/elasticsearch-6.0.0/bin/elasticsearch >/dev/null 2>&1 &

##### 4、node01机器启动head服务

node01启动elasticsearch-head插件

cd /export/servers/es/elasticsearch-head/node\_modules/grunt/bin/

进程前台启动命令  
./grunt server

进程后台启动命令

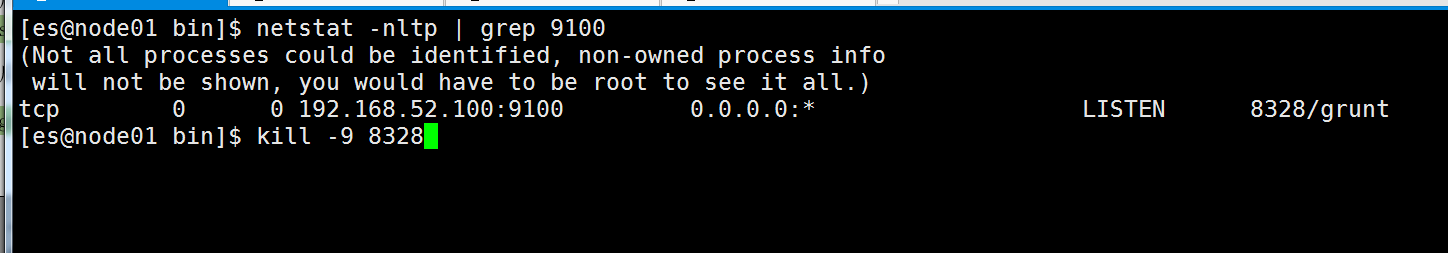
nohup ./grunt server >/dev/null 2>&1 &

Running "connect:server" (connect) task  
Waiting forever...  
Started connect web server on <http://192.168.52.100:9100>

杀死elasticsearch-head进程

netstat -nltp | grep 9100

kill -9 8328



##### 5、访问elasticsearch-head界面

打开Google Chrome访问   
<http://192.168.52.100:9100/>

### 4、node01服务器安装Kibana

kibana的基本介绍

Kibana是一个开源的分析和可视化平台，设计用于和Elasticsearch一起工作。

你用Kibana来搜索，查看，并和存储在Elasticsearch索引中的数据进行交互。

你可以轻松地执行高级数据分析，并且以各种图标、表格和地图的形式可视化数据。

Kibana使得理解大量数据变得很容易。它简单的、基于浏览器的界面使你能够快速创建和共享动态仪表板，实时显示Elasticsearch查询的变化。

接着使用我们的es用户来实现我们的kibana的安装部署

#### 下载资源

cd /home/es

在线下载

wget https://artifacts.elastic.co/downloads/kibana/kibana-6.0.0-linux-x86\_64.tar.gz

#### 2、解压文件

cd /home/es

tar -zxvf kibana-6.0.0-linux-x86\_64.tar.gz -C /export/servers/es/

#### 3、修改配置文件

cd /export/servers/es/kibana-6.0.0-linux-x86\_64/config  
vi kibana.yml

配置内容如下：

server.host: "node01"  
elasticsearch.url: "http://node01:9200"

#### 4、启动服务

cd /export/servers/es/kibana-6.0.0-linux-x86\_64  
nohup bin/kibana >/dev/null 2>&1 &

停止kibana服务进程

查看进程号

ps -ef | grep node

然后使用kill -9杀死进程即可

#### 5、访问

浏览器地址访问kibana服务

http://192.168.52.100:5601

## 3、 管理索引

curl是利用URL语法在命令行方式下工作的开源文件传输工具，使用curl可以简单实现常见的get/post请求。简单的认为是可以在命令行下面访问url的一个工具。在centos的默认库里面是有curl工具的，如果没有请yum安装即可。

curl

-X 指定http的请求方法 有HEAD GET POST PUT DELETE  
-d 指定要传输的数据  
-H 指定http请求头信息

### 3.1 使用 Xput创建索引

#### 3.1.1 创建索引

在我们的kibana的dev tools当中执行以下语句

curl -XPUT <http://node01:9200/blog01/?pretty>



#### 3.1.2 插入文档

前面的命令使用 PUT 动词将一个文档添加到 /article(文档类型)，并为该文档分配 ID 为1。URL 路径显示为index/doctype/ID（索引/文档类型/ID）。

curl -XPUT http://node01:9200/blog01/article/1?pretty -d '{"id": "1", "title": "What is lucene"}'

问题：Content-Type header [application/x-www-form-urlencoded] is not supported

解决：

curl -XPUT http://node01:9200/blog01/article/1?pretty -d '{"id": "1", "title": "What is lucene"}' -H "Content-Type: application/json"

原因：

此原因时由于ES增加了安全机制， 进行严格的内容类型检查，严格检查内容类型也可以作为防止跨站点请求伪造攻击的一层保护。 [官网解释](https://www.elastic.co/blog/strict-content-type-checking-for-elasticsearch-rest-requests)

http.content\_type.required

#### 3.1.3 查询文档

curl -XGET <http://node01:9200/blog01/article/1?pretty>

问题：Content-Type header [application/x-www-form-urlencoded] is not supported

解决：

curl -XPUT http://node01:9200/blog01/article/1?pretty -d '{"id": "1", "title": "What is lucene"}' -H "Content-Type: application/json"

curl -XGET <http://node01:9200/blog01/article/1?pretty> -H "Content-Type: application/json"

#### 3.1.4 更新文档

curl -XPUT http://node01:9200/blog01/article/1?pretty -d '{"id": "1", "title": " What is elasticsearch"}'

问题：Content-Type header [application/x-www-form-urlencoded] is not supported

解决：

curl -XPUT http://node01:9200/blog01/article/1?pretty -d '{"id": "1", "title": " What is elasticsearch"}' -H "Content-Type: application/json"

#### 3.1.5 搜索文档

curl -XGET "http://node01:9200/blog01/article/\_search?q=title:elasticsearch"

问题：Content-Type header [application/x-www-form-urlencoded] is not supported

解决：

curl -XGET "http://node01:9200/blog01/article/\_search?q=title:'elasticsearch'&pretty" -H "Content-Type: application/json"

#### 3.1.6 删除文档

curl -XDELETE "http://node01:9200/blog01/article/1?pretty"

#### 3.1.7 删除索引

curl -XDELETE <http://node01:9200/blog01?pretty>

### 3.3 返回值说明

#### 3.3.1 Hits

返回结果中最重要的部分是 hits ，它包含 total 字段来表示匹配到的文档总数，并且一个 hits 数组包含所查询结果的前十个文档。  
在 hits 数组中每个结果包含文档的 \_index 、 \_type 、 \_id ，加上 \_source 字段。这意味着我们可以直接从返回的搜索结果中使用整个文档。这不像其他的搜索引擎，仅仅返回文档的ID，需要你单独去获取文档。  
每个结果还有一个 \_score ，它衡量了文档与查询的匹配程度。默认情况下，首先返回最相关的文档结果，就是说，返回的文档是按照 \_score 降序排列的。在这个例子中，我们没有指定任何查询，故所有的文档具有相同的相关性，因此对所有的结果而言 1 是中性的 \_score 。  
max\_score 值是与查询所匹配文档的 \_score 的最大值。

#### 3.3.2 took

took 值告诉我们执行整个搜索请求耗费了多少毫秒

#### 3.3.3 Shard

\_shards 部分 告诉我们在查询中参与分片的总数，以及这些分片成功了多少个失败了多少个。正常情况下我们不希望分片失败，但是分片失败是可能发生的。  
如果我们遭遇到一种灾难级别的故障，在这个故障中丢失了相同分片的原始数据和副本，那么对这个分片将没有可用副本来对搜索请求作出响应。假若这样，Elasticsearch 将报告这个分片是失败的，但是会继续返回剩余分片的结果。

#### 3.3.4 timeout

timed\_out 值告诉我们查询是否超时。默认情况下，搜索请求不会超时。 如果低响应时间比完成结果更重要，你可以指定 timeout 为 10 或者 10ms（10毫秒），或者 1s（1秒）：  
GET /\_search?timeout=10ms  
在请求超时之前，Elasticsearch 将会返回已经成功从每个分片获取的结果。

### 3.4 花式查询

在kibana提供的界面上进行操作。

POST /school/student/\_bulk  
{ "index": { "\_id": 1 }}  
{ "name" : "liubei", "age" : 20 , "sex": "boy", "birth": "1996-01-02" , "about": "i like diaocan he girl" }  
{ "index": { "\_id": 2 }}  
{ "name" : "guanyu", "age" : 21 , "sex": "boy", "birth": "1995-01-02" , "about": "i like diaocan" }  
{ "index": { "\_id": 3 }}  
{ "name" : "zhangfei", "age" : 18 , "sex": "boy", "birth": "1998-01-02" , "about": "i like travel" }  
{ "index": { "\_id": 4 }}  
{ "name" : "diaocan", "age" : 20 , "sex": "girl", "birth": "1996-01-02" , "about": "i like travel and sport" }  
{ "index": { "\_id": 5 }}  
{ "name" : "panjinlian", "age" : 25 , "sex": "girl", "birth": "1991-01-02" , "about": "i like travel and wusong" }  
{ "index": { "\_id": 6 }}  
{ "name" : "caocao", "age" : 30 , "sex": "boy", "birth": "1988-01-02" , "about": "i like xiaoqiao" }  
{ "index": { "\_id": 7 }}  
{ "name" : "zhaoyun", "age" : 31 , "sex": "boy", "birth": "1997-01-02" , "about": "i like travel and music" }  
{ "index": { "\_id": 8 }}  
{ "name" : "xiaoqiao", "age" : 18 , "sex": "girl", "birth": "1998-01-02" , "about": "i like caocao" }  
{ "index": { "\_id": 9 }}  
{ "name" : "daqiao", "age" : 20 , "sex": "girl", "birth": "1996-01-02" , "about": "i like travel and history" }

#### 3.4.1、使用match\_all做查询

GET /school/student/\_search?pretty  
{  
 "query": {  
 "match\_all": {}  
 }  
}

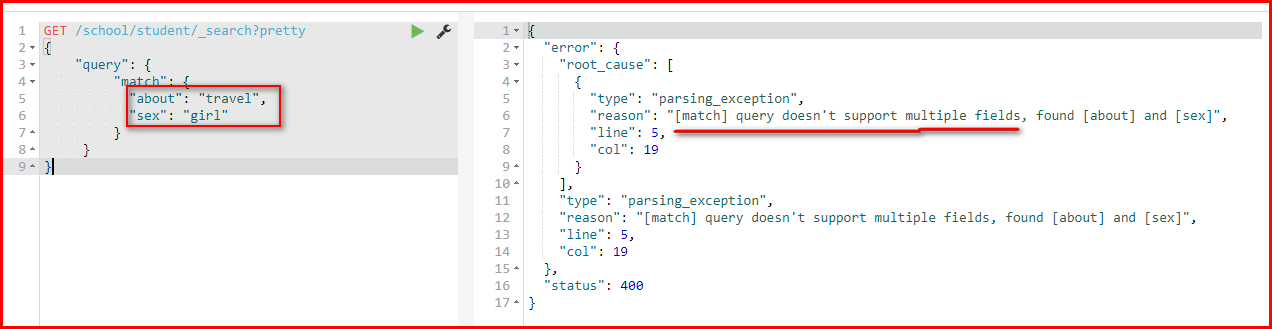
问题：通过match\_all匹配后，会把所有的数据检索出来，但是往往真正的业务需求并非要找全部的数据，而是检索出自己想要的；并且对于es集群来说，直接检索全部的数据，很容易造成GC现象。所以，我们要学会如何进行高效的检索数据

#### 3.4.2、通过关键字段进行查询

GET /school/student/\_search?pretty  
{  
 "query": {  
 "match": {"about": "travel"}  
 }  
}

如果此时想查询**喜欢旅游的，并且不能是男孩的**，怎么办？

【这种方式是错误的，因为一个match下，不能出现多个字段值[match] query doesn't support multiple fields】，需要使用复合查询



#### 3.4.3、bool的复合查询

当出现多个查询语句组合的时候，可以用bool来包含。bool合并聚包含：must，must\_not或者should， should表示or的意思

例子：查询非男性中喜欢旅行的人

GET /school/student/\_search?pretty  
{  
"query": {  
 "bool": {  
 "must": { "match": {"about": "travel"}},  
 "must\_not": {"match": {"sex": "boy"}}  
 }  
 }  
}

#### 3.4.4、bool的复合查询中的should

should表示可有可无的（如果should匹配到了就展示，否则就不展示）

例子：

查询喜欢旅行的，如果有男性的则显示，否则不显示

GET /school/student/\_search?pretty  
{  
"query": {  
 "bool": {  
 "must": { "match": {"about": "travel"}},  
 "should": {"match": {"sex": "boy"}}   
 }  
 }  
}

#### 3.4.5、term匹配

使用term进行精确匹配（比如数字，日期，布尔值或 not\_analyzed的字符串(未经分析的文本数据类型)）

语法

{ "term": { "age": 20 }}

{ "term": { "date": "2018-04-01" }}

{ "term": { "sex": “boy” }}

{ "term": { "about": "trivel" }}

例子：

查询喜欢旅行的

GET /school/student/\_search?pretty  
{  
"query": {  
 "bool": {  
 "must": { "term": {"about": "travel"}},  
 "should": {"term": {"sex": "boy"}}   
 }}  
}

#### 3.4.6、使用terms匹配多个值

GET /school/student/\_search?pretty  
{  
"query": {  
 "bool": {  
 "must": { "terms": {"about": ["travel","history"]}}   
 }  
 }  
}

term主要是用于精确的过滤比如说：”我爱你”

在match下面匹配可以为包含：我、爱、你、我爱等等的解析器

在term语法下面就精准匹配到：”我爱你”

#### 3.4.7、Range过滤

Range过滤允许我们按照指定的范围查找一些数据：操作范围：gt::大于，gte::大于等于,lt::小于，lte::小于等于

例子：

查找出大于20岁，小于等于25岁的学生

GET /school/student/\_search?pretty  
{  
"query": {  
 "range": {  
 "age": {"gt":20,"lte":25}  
 }  
 }  
}

#### 3.4.8、exists和 missing过滤

exists和missing过滤可以找到文档中是否包含某个字段或者是没有某个字段

例子：

查找字段中包含age的文档

GET /school/student/\_search?pretty  
{  
"query": {  
 "exists": {  
 "field": "age"   
 }  
 }  
}

#### 3.4.9、bool的多条件过滤

用bool也可以像之前match一样来过滤多行条件：

must :: 多个查询条件的完全匹配,相当于 and 。  
must\_not :: 多个查询条件的相反匹配，相当于 not 。  
should :: 至少有一个查询条件匹配, 相当于 or

例子：

过滤出about字段包含travel并且年龄大于20岁小于30岁的同学

GET /school/student/\_search?pretty  
{  
 "query": {  
 "bool": {  
 "must": [  
 {"term": {  
 "about": {  
 "value": "travel"  
 }  
 }},{"range": {  
 "age": {  
 "gte": 20,  
 "lte": 30  
 }  
 }}  
 ]  
 }  
 }  
}

#### 3.4.10、查询与过滤条件合并

通常复杂的查询语句，我们也要配合过滤语句来实现缓存，用filter语句就可以来实现

例子：

查询出喜欢旅行的，并且年龄是20岁的文档

GET /school/student/\_search?pretty  
{  
 "query": {  
 "bool": {  
 "must": {"match": {"about": "travel"}},   
 "filter": [{"term":{"age": 20}}]  
 }  
 }  
}

## 4、索引映射（mappings）管理

### 4.1 为什么要映射

elasticsearch中的文档等价于java中的对象，那么在java对象中有字段（比如string、int、long等），同理在elasticsearch索引中的具体字段也是有类型的。

PUT /document/article/1  
{  
 "title" : "elasticsearchshi是是什么",  
 "author" : "zhangsan",  
 "titleScore" : 60  
}

这种操作并没有指定字段类型，那么elasticsearch会自动根据数据类型的格式识别字段的类型；查看索引字段类型：GET /document/article/\_mapping。可以发现titleScore的类型是long。



然后在插入一条数据：

PUT /document/article/2  
{  
 "title" : "elasticsearchshi是是什么",  
 "author" : "zhangsan",  
 "titleScore" : 66.666  
}

查询数据：GET /document/article/2

**我们会发现es能存入，并没有报错（注意），这其实是一个问题**，因为如果后期elaticsearch对接java的时候，我们会写一个类对数据做封装，比如：

class Article{  
private String title;  
private String author;  
private String titleScore //《什么类型合适》？如果使用long类型，那么后面肯定会有数据格式转换的异常 doublelong  
}

**所以，我们如果能提前知道字段类型，那么最好使用mapping的映射管理，提前指定字段的类型，防止后续的程序问题；**

DELETE document  
PUT document  
{  
 "mappings": {  
 "article" : {  
 "properties":  
 {  
 "title" : {"type": "text"} ,   
 "author" : {"type": "text"} ,   
 "titleScore" : {"type": "double"}   
   
 }  
 }  
 }  
}  
get document/article/\_mapping

### 4.2 基本命令

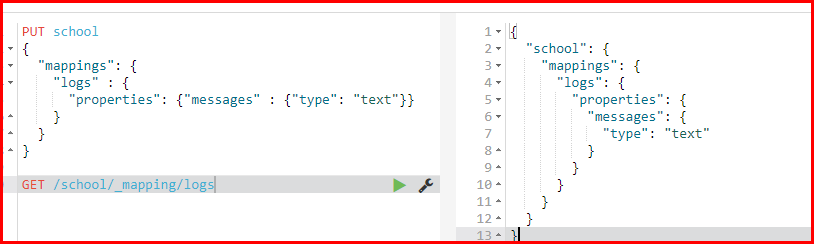
DELETE school

PUT school  
{  
 "mappings": {  
 "logs" : {  
 "properties": {"messages" : {"type": "text"}}  
 }  
 }

}

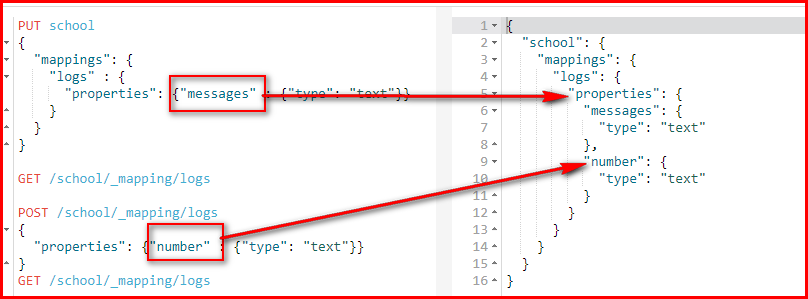
添加索引：school，文档类型类logs，索引字段为message ，字段的类型为text

GET /school/\_mapping/logs



继续添加字段

POST /school/\_mapping/logs  
{  
 "properties": {"number" : {"type": "text"}}  
}  
  
GET /school/\_mapping/logs

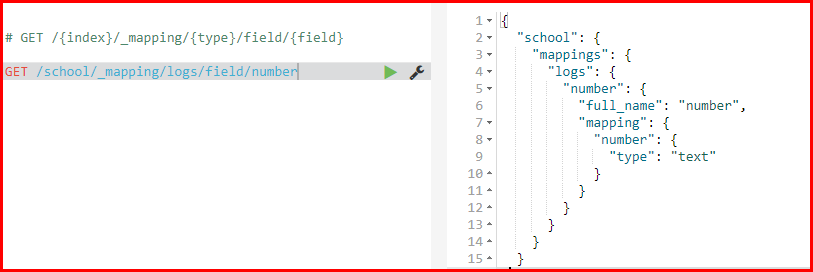


### 4.3 获取映射字段

语法：

GET /{index}/\_mapping/{type}/field/{field}

GET /school/\_mapping/logs/field/number



## 5、索引库配置管理（settings）

### 5.1 索引库配置

**所谓的settings就是用来修改索引分片和副本数的；**

比如有的重要索引，副本数很少甚至没有副本，那么我们可以通过setting来添加副本数

DELETE document  
PUT document  
{  
 "mappings": {  
 "article" : {  
 "properties":  
 {  
 "title" : {"type": "text"} ,   
 "author" : {"type": "text"} ,   
 "titleScore" : {"type": "double"}   
   
 }  
 }  
 }  
}  
GET /document/\_settings



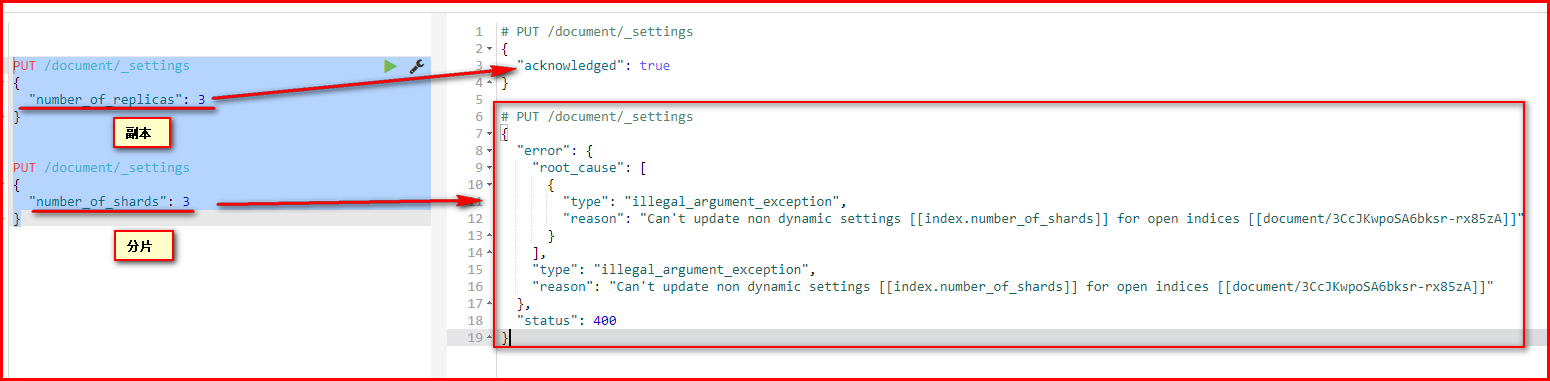
可以看到当前的副本数是1，那么为了提高容错性，我们可以把副本数改成2：

PUT /document/\_settings  
{  
 "number\_of\_replicas": 2  
}



**副本可以改，分片不能改**

PUT /document/\_settings  
{  
 "number\_of\_shards": 3  
}



### 5.2 零停机重新索引数据

实际生产，对于文档的操作，偶尔会遇到这种问题：

某一个字段的类型不符合后期的业务了，但是当前的索引已经创建了，我们知道es在字段的mapping建立后就不可再次修改mapping的值。

#### 5.2.1 新建索引库articles1，并添加数据

DELETE articles1  
PUT articles1  
{   
 "settings":{   
 "number\_of\_shards":3,   
 "number\_of\_replicas":1   
 },   
 "mappings":{   
 "article":{   
 "dynamic":"strict",   
 "properties":{   
 "id":{"type": "text", "store": true},   
 "title":{"type": "text","store": true},   
 "readCounts":{"type": "integer","store": true},   
 "times": {"type": "text", "index": false}  
 }   
 }   
 }   
}  
  
  
PUT articles1/article/1  
{  
 "id" : "1",  
 "title" : "世界1",  
 "readCounts" : 2 ,   
 "times" : "2018-05-01"  
}  
  
get articles1/article/1

#### 5.2.2 新建索引库articles2

DELETE articles2  
PUT articles2  
{   
 "settings":{   
 "number\_of\_shards":5,   
 "number\_of\_replicas":1   
 },   
 "mappings":{   
 "article":{   
 "dynamic":"strict",   
 "properties":{   
 "id":{"type": "text", "store": true},   
 "title":{"type": "text","store": true},   
 "readCounts":{"type": "integer","store": true},   
 "times": {"type": "date", "index": false}  
 }   
 }   
 }   
}   
  
  
GET articles2/article/1

#### 5.2.3 拷贝数据并验证

POST \_reindex  
{  
 "source": {  
 "index": "articles1"  
 },  
 "dest": {  
 "index": "articles2"  
 }  
}  
  
GET articles2/article/1

## 6、分页解决方案

### 6.1、导入数据

DELETE us  
POST /\_bulk  
{ "create": { "\_index": "us", "\_type": "tweet", "\_id": "1" }}  
{ "email" : "john@smith.com", "name" : "John Smith", "username" : "@john" }  
{ "create": { "\_index": "us", "\_type": "tweet", "\_id": "2" }}  
{ "email" : "mary@jones.com", "name" : "Mary Jones", "username" : "@mary" }  
{ "create": { "\_index": "us", "\_type": "tweet", "\_id": "3" }}  
{ "date" : "2014-09-13", "name" : "Mary Jones", "tweet" : "Elasticsearch means full text search has never been so easy", "user\_id" : 2 }  
{ "create": { "\_index": "us", "\_type": "tweet", "\_id": "4" }}  
{ "date" : "2014-09-14", "name" : "John Smith", "tweet" : "@mary it is not just text, it does everything", "user\_id" : 1 }  
{ "create": { "\_index": "us", "\_type": "tweet", "\_id": "5" }}  
{ "date" : "2014-09-15", "name" : "Mary Jones", "tweet" : "However did I manage before Elasticsearch?", "user\_id" : 2 }  
{ "create": { "\_index": "us", "\_type": "tweet", "\_id": "6" }}  
{ "date" : "2014-09-16", "name" : "John Smith", "tweet" : "The Elasticsearch API is really easy to use", "user\_id" : 1 }  
{ "create": { "\_index": "us", "\_type": "tweet", "\_id": "7" }}  
{ "date" : "2014-09-17", "name" : "Mary Jones", "tweet" : "The Query DSL is really powerful and flexible", "user\_id" : 2 }  
{ "create": { "\_index": "us", "\_type": "tweet", "\_id": "8" }}  
{ "date" : "2014-09-18", "name" : "John Smith", "user\_id" : 1 }  
{ "create": { "\_index": "us", "\_type": "tweet", "\_id": "9" }}  
{ "date" : "2014-09-19", "name" : "Mary Jones", "tweet" : "Geo-location aggregations are really cool", "user\_id" : 2 }  
{ "create": { "\_index": "us", "\_type": "tweet", "\_id": "10" }}  
{ "date" : "2014-09-20", "name" : "John Smith", "tweet" : "Elasticsearch surely is one of the hottest new NoSQL products", "user\_id" : 1 }  
{ "create": { "\_index": "us", "\_type": "tweet", "\_id": "11" }}  
{ "date" : "2014-09-21", "name" : "Mary Jones", "tweet" : "Elasticsearch is built for the cloud, easy to scale", "user\_id" : 2 }  
{ "create": { "\_index": "us", "\_type": "tweet", "\_id": "12" }}  
{ "date" : "2014-09-22", "name" : "John Smith", "tweet" : "Elasticsearch and I have left the honeymoon stage, and I still love her.", "user\_id" : 1 }  
{ "create": { "\_index": "us", "\_type": "tweet", "\_id": "13" }}  
{ "date" : "2014-09-23", "name" : "Mary Jones", "tweet" : "So yes, I am an Elasticsearch fanboy", "user\_id" : 2 }  
{ "create": { "\_index": "us", "\_type": "tweet", "\_id": "14" }}  
{ "date" : "2014-09-24", "name" : "John Smith", "tweet" : "How many more cheesy tweets do I have to write?", "user\_id" : 1 }

### 6.2、size+from浅分页

按照一般的查询流程来说，如果我想查询前10条数据：

* 1 客户端请求发给某个节点
* 2 节点转发给个个分片，查询每个分片上的前10条
* 3 结果返回给节点，整合数据，提取前10条
* 4 返回给请求客户端

**from定义了目标数据的偏移值，size定义当前返回的事件数目**

GET /us/\_search?pretty  
{  
 "from" : 0 , "size" : 5  
}  
  
GET /us/\_search?pretty  
{  
 "from" : 5 , "size" : 5  
}

这种浅分页只适合少量数据，因为随from增大，查询的时间就会越大，而且数据量越大，查询的效率指数下降

优点：from+size在数据量不大的情况下，效率比较高

缺点：在数据量非常大的情况下，from+size分页会把全部记录加载到内存中，这样做不但运行速递特别慢，而且容易让es出现内存不足而挂掉

### 6.3、scroll深分页

对于上面介绍的浅分页，当Elasticsearch响应请求时，它必须确定docs的顺序，排列响应结果。

如果请求的页数较少（假设每页20个docs）, Elasticsearch不会有什么问题，但是如果页数较大时，比如请求第20页，Elasticsearch不得不取出第1页到第20页的所有docs，再去除第1页到第19页的docs，得到第20页的docs。

解决的方式就是使用scroll，**scroll就是维护了当前索引段的一份快照信息--缓存**（这个快照信息是你执行这个scroll查询时的快照）。

可以把 scroll 分为初始化和遍历两步： 1、初始化时将所有符合搜索条件的搜索结果缓存起来，可以想象成快照； 2、遍历时，从这个快照里取数据；

初始化

GET us/\_search?scroll=3m  
{  
 "query": {"match\_all": {}},  
 "size": 3  
}  
  
初始化的时候就像是普通的search一样  
其中的scroll=3m代表当前查询的数据缓存3分钟  
Size：3 代表当前查询3条数据

遍历

在遍历时候，拿到上一次遍历中的*scroll*id，然后带scroll参数，重复上一次的遍历步骤，知道返回的数据为空，就表示遍历完成

GET /\_search/scroll  
{  
 "scroll" : "1m",  
 "scroll\_id" : "DnF1ZXJ5VGhlbkZldGNoBQAAAAAAAAPXFk0xN1BmSnlVUldhYThEdWVzZ19xbkEAAAAAAAAAIxZuQWVJU0VSZ1JzcVZtMGVYZ3RDaFlBAAAAAAAAA9oWTVZOdHJ2cXBSOU9wN3c1dk5vcWd4QQAAAAAAAAPYFk0xN1BmSnlVUldhYThEdWVzZ19xbkEAAAAAAAAAIhZuQWVJU0VSZ1JzcVZtMGVYZ3RDaFlB"  
}

【注意】：每次都要传参数scroll，刷新搜索结果的缓存时间，另外不需要指定index和type（**不要把缓存的时时间设置太长，占用内存**）

**对比**

浅分页，每次查询都会去索引库（本地文件夹）中查询pageNum\*page条数据，然后截取掉前面的数据，留下最后的数据。 这样的操作在每个分片上都会执行，最后会将多个分片的数据合并到一起，再次排序，截取需要的。

深分页，可以一次性将所有满足查询条件的数据，都放到内存中。分页的时候，在内存中查询。相对浅分页，就可以避免多次读取磁盘。

## 7 、三台机器安装IK分词器

### 7.1 安装

每台机器都要配置。配置完成之后，需要重启ES服务

将安装包上传到node01机器的/home/es路径下

cd /home/es

wget https://github.com/medcl/elasticsearch-analysis-ik/releases/download/v5.5.2/elasticsearch-analysis-ik-6.0.0.zip  
# 将ik分词器的插件，上传到/home/es目录下   
cd /home/es   
unzip elasticsearch-analysis-ik-6.0.0.zip -d /export/servers/es/elasticsearch-6.0.0/plugins/  
cd /export/servers/es/elasticsearch-6.0.0/plugins  
mv elasticsearch analysis-ik

将安装包分发到其他机器上

node01机器执行以下命令进行安装包的分发

cd /export/servers/es/elasticsearch-6.0.0/plugins

scp -r analysis-ik/ node02:$PWD

scp -r analysis-ik/ node03:$PWD

# 三台机器都配置完成  
# 配置完成之后，需要重启服务。

三台机器重启es服务

三台机器执行以下命令停止es服务

ps -ef|grep elasticsearch|grep bootstravelap |awk '{print $2}' |xargs kill -9

nohup /export/servers/es/elasticsearch-6.0.0/bin/elasticsearch >/dev/null 2>&1 &

### 7.2 配置

delete iktest  
PUT /iktest?pretty  
{  
 "settings" : {  
 "analysis" : {  
 "analyzer" : {  
 "ik" : {  
 "tokenizer" : "ik\_max\_word"  
 }  
 }  
 }  
 },  
 "mappings" : {  
 "article" : {  
 "dynamic" : true,  
 "properties" : {  
 "subject" : {  
 "type" : "text",  
 "analyzer" : "ik\_max\_word"  
 }  
 }  
 }  
 }  
}

说明：ik带有两个分词器:

* ik\_*max\_*word ：会将文本做最细粒度的拆分；尽可能多的拆分出词语
* 句子：我爱我的祖国
* 结果： 我|爱|我的|祖|国|祖国
* ik\_smart：会做最粗粒度的拆分；已被分出的词语将不会再次被其它词语占有
* 句子：我爱我的祖国
* 结果： 我|爱|我|的|祖国

### 7.3 查看分词效果

GET \_analyze?pretty  
 {  
 "analyzer": "ik\_max\_word",  
 "text": "希拉里是个妹子"  
 }

### 7.4 插入测试数据

POST /iktest/article/\_bulk?pretty  
{ "index" : { "\_id" : "1" } }  
{"subject" : "＂闺蜜＂崔顺实被韩检方传唤 韩总统府促彻查真相" }  
{ "index" : { "\_id" : "2" } }  
{"subject" : "韩举行＂护国训练＂ 青瓦台:决不许国家安全出问题" }  
{ "index" : { "\_id" : "3" } }  
{"subject" : "媒体称FBI已经取得搜查令 检视希拉里电邮" }  
{ "index" : { "\_id" : "4" } }  
{"subject" : "村上春树获安徒生奖 演讲中谈及欧洲排外问题" }  
{ "index" : { "\_id" : "5" } }  
{"subject" : "希拉里团队炮轰FBI 参院民主党领袖批其”违法”" }

查看分词器

对"希拉里和韩国"进行分词查询

ik*max*word分词后的效果：希|拉|里|希拉里|和|韩国

POST /iktest/article/\_search?pretty  
{  
 "query" : { "match" : { "subject" : "希拉里和韩国" }},  
 "highlight" : {  
 "pre\_tags" : ["<font color=red>"],  
 "post\_tags" : ["</font>"],  
 "fields" : {  
 "subject" : {}  
 }  
 }  
}

### 7.5 热词更新

查看分词效果

GET \_analyze?pretty

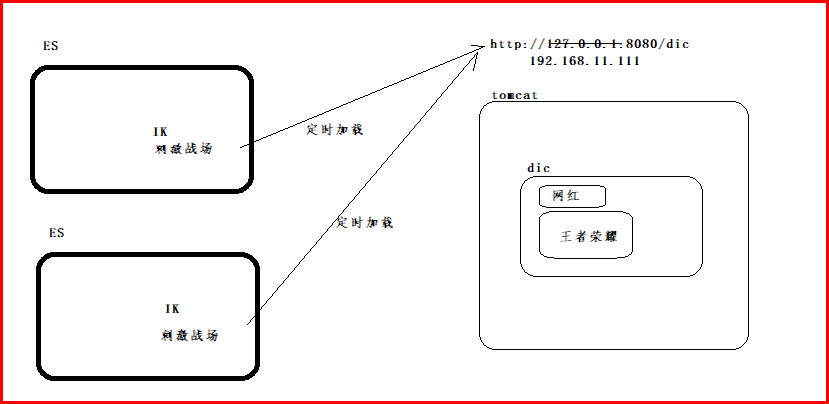
{

"analyzer": "ik\_max\_word",

"text": "传智播客在哪里"

}

#### 7.5.1 node03配置Tomcat



使用es用户来进行配置tomcat，此处我们将tomcat装在node03机器上面即可

cd /home/es

tar -zxvf apache-tomcat-8.5.34.tar.gz -C /export/servers/es/

tomcat当中添加配置hot.dic

cd /export/servers/es/apache-tomcat-8.5.34/webapps/ROOT/

vi hot.dic

传智播客

# 启动tomcat

/export/servers/es/apache-tomcat-8.5.34/bin/startup.sh

浏览器访问

wget http://node03:8080/hot.dic

#### 7.5.2 三台机器修改配置文件

三台机器都要修改es的配置文件（使用es用户来进行修改即可）

第一台机器node01修改es的配置

cd /export/servers/es/elasticsearch-6.0.0/plugins/analysis-ik/config

vim IKAnalyzer.cfg.xml

<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">

<properties>

<comment>IK Analyzer 扩展配置</comment>

<!--用户可以在这里配置自己的扩展字典 -->

<entry key="ext\_dict"></entry>

<!--用户可以在这里配置自己的扩展停止词字典-->

<entry key="ext\_stopwords"></entry>

<!--用户可以在这里配置远程扩展字典 -->

<entry key="remote\_ext\_dict">http://node03:8080/hot.dic</entry>

<!--用户可以在这里配置远程扩展停止词字典-->

<!-- <entry key="remote\_ext\_stopwords">words\_location</entry> -->

</properties>

修改完成之后拷贝到node02与node03机器上面去

node01执行以下命令进行拷贝

cd /export/servers/es/elasticsearch-6.0.0/plugins/analysis-ik/config

sudo scp IKAnalyzer.cfg.xml node02:$PWD

sudo scp IKAnalyzer.cfg.xml node03:$PWD

#### 7.5.3 三台机器修改JDK权限

三台机器修改jdk的权限问题

第一台机器执行以下命令修改jdk的权限问题

#修改JDK安全设置  
cd /export/servers/jdk1.8.0\_141/jre/lib/security

sudo vim java.policy

添加以下四行配置

permission java.net.SocketPermission "192.168.52.120:8080","accept";  
 permission java.net.SocketPermission "192.168.52.120:8080","listen";  
 permission java.net.SocketPermission "192.168.52.120:8080","resolve";  
 permission java.net.SocketPermission "192.168.52.120:8080","connect";

修改完成之后拷贝到第二台和第三台机器

node01执行以下命令拷贝到第二台和第三台

cd /export/servers/jdk1.8.0\_141/jre/lib/security

sudo scp java.policy node02:$PWD

sudo scp java.policy node03:$PWD

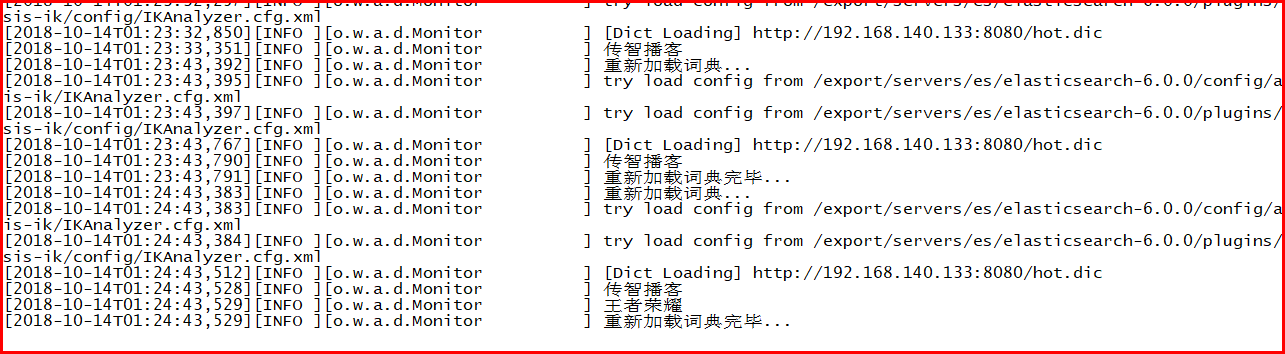
<http://mahilion.blog.163.com/blog/static/1830872952012101225243655/>

#### 7.5.4 三台机器重新启动es

三台机器重新启动es服务，三台机器先使用kill -9杀死es的服务，然后再执行以下命令进行重启

cd /export/servers/es/elasticsearch-6.0.0/

nohup bin/elasticsearch >/dev/null 2>&1 &



查看我们的分词过程

GET \_analyze?pretty

{

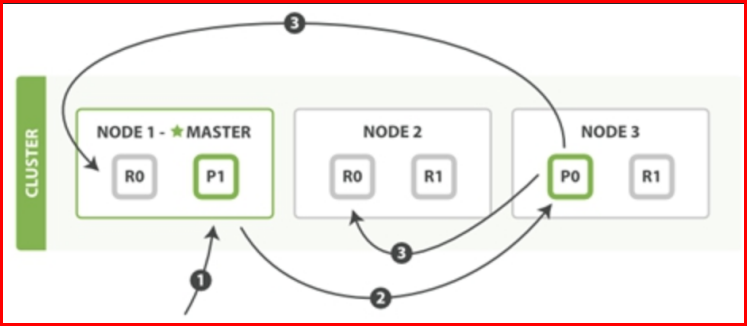
"analyzer": "ik\_max\_word",

"text": "传智播客在哪里"

}

## 8、分片交互过程

### 8.1 创建索引



首先：发送一个索引或者删除的请求给node1

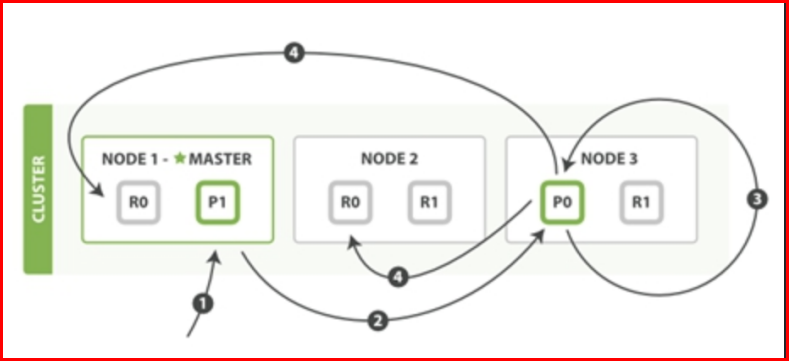
其次：node1介绍到请求之后，会根据请求中携带的参数“文档id”判断出该文档应该存储在具体哪一个shard中

**shard = hash(routing) % number*of*primary\_shards**

，比如shard0；其次就是node1通过元数据信息可以知道shard0在具体哪一个节点，于是node1会把请求转发给node3

最后：node3接收到请求之后会将请求并行的分发给shard0的所有replica shard之上，也就是存在于node 1和node 2中的replica shard；如果所有的replica shard都成功地执行了请求，那么将会向node 3回复一个成功确认，当node 3收到了所有replica shard的确认信息后，则最后向用户返回一个Success的消息。

### 8.2 删除索引



该过程可以分为四个阶段来描述：

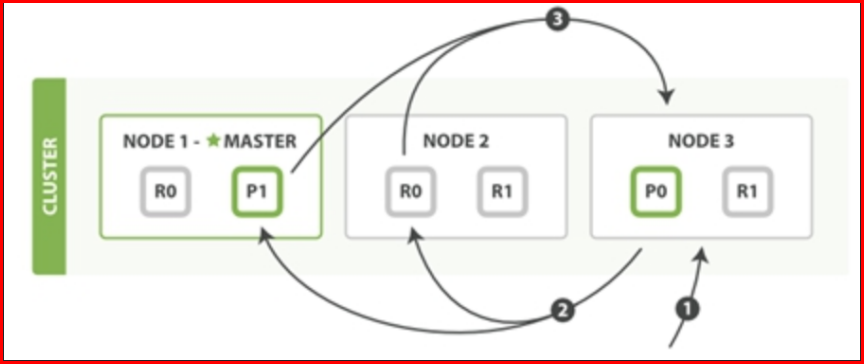
阶段1：客户端向node 1发送一个文档删除的请求。

阶段2：同样的node 1通过请求中文档的 \_id 值判断出该文档应该被存储在shard 0 这个分片中，并且node 1知道shard 0的primary shard位于node 3这个节点上。因此node 1会把这个请求转发到node 3。

阶段3：node 3接收到请求后，在主分片上面执行删除请求

阶段4：如果node 3成功地删除了文档，node 3将会请求并行地发给其余所有的replica shard所在node中。这些node也同样操作删除，执行后则向node 3确认成功，当node 3接收到所有的成功确认之后，再向客户端发送一个删除成功的信息。

### 8.3 查询索引



检索文档的时候，我们并不知道文档在集群中的哪个位置，所以一般情况下不得不去询问index中的每一个shard，然后将结果拼接成一个大的已排好序的汇总结果列表；

（1）：客户端发送一个检索请求给node3，此时node3会创建一个空的优先级队列并且配置好分页参数from与size。

（2）：node3将检所请求发送给index中的每一个shard（primary 和 replica），每一个在本地执行检索，并将结果添加到本地的优先级队列中；

（3）：**每个shard返回本地优先级序列中所记录的\_id与\***\*score值\*\*，并发送node3。Node3将这些值合并到自己的本地的优先级队列中，并做全局的排序（node 3将它们合并成一条汇总的结果），返回给客户端。

## 9、使用Java API访问集群

### 1 导入pom

<dependencies>  
 <dependency>  
 <groupId>org.elasticsearch.client</groupId>  
 <artifactId>transport</artifactId>  
 <version>6.0.0</version>  
 </dependency>  
 <dependency>  
 <groupId>org.apache.logging.log4j</groupId>  
 <artifactId>log4j-core</artifactId>  
 <version>2.9.1</version>  
 </dependency>  
 <dependency>  
 <groupId>org.junit.jupiter</groupId>  
 <artifactId>junit-jupiter-api</artifactId>  
 <version>5.3.0-M1</version>  
 <scope>test</scope>  
 </dependency>  
  
 <!-- https://mvnrepository.com/artifact/com.alibaba/fastjson -->  
 <dependency>  
 <groupId>com.alibaba</groupId>  
 <artifactId>fastjson</artifactId>  
 <version>1.2.47</version>  
 </dependency>  
</dependencies>  
<build>  
 <plugins>  
 <plugin>  
 <groupId>org.apache.maven.plugins</groupId>  
 <artifactId>maven-compiler-plugin</artifactId>  
 <configuration>  
 <source>1.8</source>  
 <target>1.8</target>  
 </configuration>  
 </plugin>  
 </plugins>  
</build>

### 2 创建索引 prepareIndex

#### 1、创建Client

**private** TransportClient **client**;  
@Before  
**public void** test1() **throws** UnknownHostException {  
 Settings settings = Settings.*builder*().put(**"cluster.name"**, **"myes"**).build();  
 **client** = **new** PreBuiltTransportClient(settings).addTransportAddress(**new** TransportAddress(InetAddress.*getByName*(**"node01"**),9300)).addTransportAddress(**new** TransportAddress(InetAddress.*getByName*(**"node02"**),9300));  
}

#### 2、自己拼装json创建索引保存到myindex1索引库下面的article当中去

*/\*\*  
 \* 插入json格式的索引数据  
 \*/*@Test  
**public void** createIndex(){  
 String json = **"{"** +  
 **"\"user\":\"kimchy\","** +  
 **"\"postDate\":\"2013-01-30\","** +  
 **"\"message\":\"travelying out Elasticsearch\""** +  
 **"}"**;  
 IndexResponse indexResponse = **client**.prepareIndex(**"myindex1"**, **"article"**, **"1"**).setSource(json, XContentType.***JSON***).get();  
 **client**.close();  
}

#### 3、使用map创建索引

@Test  
**public void** index2() **throws** Exception {  
 HashMap<String, String> jsonMap = **new** HashMap<String, String>();  
 jsonMap.put(**"name"**, **"zhangsan"**);  
 jsonMap.put(**"sex"**, **"1"**);  
 jsonMap.put(**"age"**, **"18"**);  
 jsonMap.put(**"address"**, **"bj"**);  
 IndexResponse indexResponse = **client**.prepareIndex(**"myindex1"**, **"article"**, **"2"**)  
 .setSource(jsonMap)  
 .get();  
 **client**.close();  
}

#### 4、XcontentBuilder实现创建索引

*/\*\*  
 \* 通过XContentBuilder来实现索引的创建  
 \** ***@throws*** *IOException  
 \*/*@Test  
**public void** index3() **throws** IOException {  
 IndexResponse indexResponse = **client**.prepareIndex(**"myindex1"**, **"article"**, **"3"**)  
 .setSource(**new** XContentFactory().*jsonBuilder*()  
 .startObject()  
 .field(**"name"**, **"lisi"**)  
 .field(**"age"**, **"18"**)  
 .field(**"sex"**, **"0"**)  
 .field(**"address"**, **"bj"**)  
 .endObject())  
 .get();  
 **client**.close();  
  
}

#### 5、将对象转换为json格式字符串进行创建索引

定义person对象

**public class** Person **implements** Serializable{  
 **private** Integer **id**;  
 **private** String **name** ;  
 **private** Integer **age**;  
 **private** Integer **sex**;  
 **private** String **address**;  
 **private** String **phone**;  
 **private** String **email**;  
 **private** String **say**;  
  
  
 **public** Person() {  
 }  
  
 **public** Person(Integer id, String name, Integer age, Integer sex, String address, String phone, String email,String say) {  
 **this**.**id** = id;  
 **this**.**name** = name;  
 **this**.**age** = age;  
 **this**.**sex** = sex;  
 **this**.**address** = address;  
 **this**.**phone** = phone;  
 **this**.**email** = email;  
 **this**.**say** = say;  
 }  
  
 **public** String getSay() {  
 **return say**;  
 }  
  
 **public void** setSay(String say) {  
 **this**.**say** = say;  
 }  
  
 **public** Integer getId() {  
 **return id**;  
 }  
  
 **public void** setId(Integer id) {  
 **this**.**id** = id;  
 }  
  
 **public** String getName() {  
 **return name**;  
 }  
  
 **public void** setName(String name) {  
 **this**.**name** = name;  
 }  
  
 **public** Integer getAge() {  
 **return age**;  
 }  
  
 **public void** setAge(Integer age) {  
 **this**.**age** = age;  
 }  
  
 **public** Integer getSex() {  
 **return sex**;  
 }  
  
 **public void** setSex(Integer sex) {  
 **this**.**sex** = sex;  
 }  
  
 **public** String getAddress() {  
 **return address**;  
 }  
  
 **public void** setAddress(String address) {  
 **this**.**address** = address;  
 }  
  
 **public** String getPhone() {  
 **return phone**;  
 }  
  
 **public void** setPhone(String phone) {  
 **this**.**phone** = phone;  
 }  
  
 **public** String getEmail() {  
 **return email**;  
 }  
  
 **public void** setEmail(String email) {  
 **this**.**email** = email;  
 }  
}

插入索引数据

*/\*\*  
 \* 将java对象转换为json格式字符串进行创建索引  
 \*/*@Test  
**public void** objToIndex(){  
 Person person = **new** Person();  
 person.setAge(18);  
 person.setId(20);  
 person.setName(**"张三丰"**);  
 person.setAddress(**"武当山"**);  
 person.setEmail(**"zhangsanfeng@163.com"**);  
 person.setPhone(**"18588888888"**);  
 person.setSex(1);  
 String json = JSONObject.*toJSONString*(person);  
 System.***out***.println(json);  
 **client**.prepareIndex(**"myindex1"**,**"article"**,**"32"**).setSource(json,XContentType.***JSON***).get();  
 **client**.close();  
}

#### 6、批量创建索引

*/\*\*  
 \* 批量创建索引  
 \** ***@throws*** *IOException  
 \*/*@Test  
**public void** index4() **throws** IOException {  
 BulkRequestBuilder bulk = **client**.prepareBulk();  
 bulk.add(**client**.prepareIndex(**"myindex1"**, **"article"**, **"4"**)  
 .setSource(**new** XContentFactory().*jsonBuilder*()  
 .startObject()  
 .field(**"name"**, **"wangwu"**)  
 .field(**"age"**, **"18"**)  
 .field(**"sex"**, **"0"**)  
 .field(**"address"**, **"bj"**)  
 .endObject()));  
 bulk.add(**client**.prepareIndex(**"myindex1"**, **"article"**, **"5"**)  
 .setSource(**new** XContentFactory().*jsonBuilder*()  
 .startObject()  
 .field(**"name"**, **"zhaoliu"**)  
 .field(**"age"**, **"18"**)  
 .field(**"sex"**, **"0"**)  
 .field(**"address"**, **"bj"**)  
 .endObject()));  
 BulkResponse bulkResponse = bulk.get();  
 System.***out***.println(bulkResponse);  
 **client**.close();  
}

### 3 查询索引

#### 1、初始化一批数据到索引库中准备查询

*/\*\*  
 \* 初始化一批数据到索引库当中去准备做查询使用  
 \* 注意这里初始化的时候，需要给我们的数据设置分词属性  
 \** ***@throws*** *Exception  
 \*/*@Test  
**public void** createIndexBatch() **throws** Exception {  
 Settings settings = Settings  
 .*builder*()  
 .put(**"cluster.name"**, **"myes"**) *//节点名称， 在es配置的时候设置  
 //自动发现我们其他的es的服务器* .put(**"client.transport.sniff"**, **"true"**)  
 .build();  
 *//创建客户端* TransportClient client = **new** PreBuiltTransportClient(settings)  
 .addTransportAddress(**new** TransportAddress(InetAddress.*getByName*(**"node01"**), 9300));*//以本机作为节点  
 //创建映射* XContentBuilder mapping = XContentFactory.*jsonBuilder*()  
 .startObject()  
 .startObject(**"properties"**)  
 *// .startObject("m\_id").field("type","keyword").endObject()* .startObject(**"id"**).field(**"type"**, **"integer"**).endObject()  
 .startObject(**"name"**).field(**"type"**, **"text"**).field(**"analyzer"**, **"ik\_max\_word"**).endObject()  
 .startObject(**"age"**).field(**"type"**, **"integer"**).endObject()  
 .startObject(**"sex"**).field(**"type"**, **"text"**).field(**"analyzer"**, **"ik\_max\_word"**).endObject()  
 .startObject(**"address"**).field(**"type"**, **"text"**).field(**"analyzer"**, **"ik\_max\_word"**).endObject()  
 .startObject(**"phone"**).field(**"type"**, **"text"**).endObject()  
 .startObject(**"email"**).field(**"type"**, **"text"**).endObject()  
 .startObject(**"say"**).field(**"type"**, **"text"**).field(**"analyzer"**, **"ik\_max\_word"**).endObject()  
 .endObject()  
 .endObject();  
 *//pois：索引名 cxyword：类型名（可以自己定义）* PutMappingRequest putmap = Requests.*putMappingRequest*(**"indexsearch"**).type(**"mysearch"**).source(mapping);  
 *//创建索引* client.admin().indices().prepareCreate(**"indexsearch"**).execute().actionGet();  
 *//为索引添加映射* client.admin().indices().putMapping(putmap).actionGet();  
  
  
 BulkRequestBuilder bulkRequestBuilder = client.prepareBulk();  
 Person lujunyi = **new** Person(2, **"玉麒麟卢俊义"**, 28, 1, **"水泊梁山"**, **"17666666666"**, **"lujunyi@itcast.com"**,**"hello world今天天气还不错"**);  
 Person wuyong = **new** Person(3, **"智多星吴用"**, 45, 1, **"水泊梁山"**, **"17666666666"**, **"wuyong@itcast.com"**,**"行走四方，抱打不平"**);  
 Person gongsunsheng = **new** Person(4, **"入云龙公孙胜"**, 30, 1, **"水泊梁山"**, **"17666666666"**, **"gongsunsheng@itcast.com"**,**"走一个"**);  
 Person guansheng = **new** Person(5, **"大刀关胜"**, 42, 1, **"水泊梁山"**, **"17666666666"**, **"wusong@itcast.com"**,**"我的大刀已经饥渴难耐"**);  
 Person linchong = **new** Person(6, **"豹子头林冲"**, 18, 1, **"水泊梁山"**, **"17666666666"**, **"linchong@itcast.com"**,**"梁山好汉"**);  
 Person qinming = **new** Person(7, **"霹雳火秦明"**, 28, 1, **"水泊梁山"**, **"17666666666"**, **"qinming@itcast.com"**,**"不太了解"**);  
 Person huyanzhuo = **new** Person(8, **"双鞭呼延灼"**, 25, 1, **"水泊梁山"**, **"17666666666"**, **"huyanzhuo@itcast.com"**,**"不是很熟悉"**);  
 Person huarong = **new** Person(9, **"小李广花荣"**, 50, 1, **"水泊梁山"**, **"17666666666"**, **"huarong@itcast.com"**,**"打酱油的"**);  
 Person chaijin = **new** Person(10, **"小旋风柴进"**, 32, 1, **"水泊梁山"**, **"17666666666"**, **"chaijin@itcast.com"**,**"吓唬人的"**);  
 Person zhisheng = **new** Person(13, **"花和尚鲁智深"**, 15, 1, **"水泊梁山"**, **"17666666666"**, **"luzhisheng@itcast.com"**,**"倒拔杨垂柳"**);  
 Person wusong = **new** Person(14, **"行者武松"**, 28, 1, **"水泊梁山"**, **"17666666666"**, **"wusong@itcast.com"**,**"二营长。。。。。。"**);  
  
 bulkRequestBuilder.add(client.prepareIndex(**"indexsearch"**, **"mysearch"**, **"1"**)  
 .setSource(JSONObject.*toJSONString*(lujunyi), XContentType.***JSON***)  
 );  
 bulkRequestBuilder.add(client.prepareIndex(**"indexsearch"**, **"mysearch"**, **"2"**)  
 .setSource(JSONObject.*toJSONString*(wuyong), XContentType.***JSON***)  
 );  
 bulkRequestBuilder.add(client.prepareIndex(**"indexsearch"**, **"mysearch"**, **"3"**)  
 .setSource(JSONObject.*toJSONString*(gongsunsheng), XContentType.***JSON***)  
 );  
 bulkRequestBuilder.add(client.prepareIndex(**"indexsearch"**, **"mysearch"**, **"4"**)  
 .setSource(JSONObject.*toJSONString*(guansheng), XContentType.***JSON***)  
 );  
 bulkRequestBuilder.add(client.prepareIndex(**"indexsearch"**, **"mysearch"**, **"5"**)  
 .setSource(JSONObject.*toJSONString*(linchong), XContentType.***JSON***)  
 );  
 bulkRequestBuilder.add(client.prepareIndex(**"indexsearch"**, **"mysearch"**, **"6"**)  
 .setSource(JSONObject.*toJSONString*(qinming), XContentType.***JSON***)  
 );  
 bulkRequestBuilder.add(client.prepareIndex(**"indexsearch"**, **"mysearch"**, **"7"**)  
 .setSource(JSONObject.*toJSONString*(huyanzhuo), XContentType.***JSON***)  
 );  
 bulkRequestBuilder.add(client.prepareIndex(**"indexsearch"**, **"mysearch"**, **"8"**)  
 .setSource(JSONObject.*toJSONString*(huarong), XContentType.***JSON***)  
 );  
 bulkRequestBuilder.add(client.prepareIndex(**"indexsearch"**, **"mysearch"**, **"9"**)  
 .setSource(JSONObject.*toJSONString*(chaijin), XContentType.***JSON***)  
 );  
 bulkRequestBuilder.add(client.prepareIndex(**"indexsearch"**, **"mysearch"**, **"10"**)  
 .setSource(JSONObject.*toJSONString*(zhisheng), XContentType.***JSON***)  
 );  
 bulkRequestBuilder.add(client.prepareIndex(**"indexsearch"**, **"mysearch"**, **"11"**)  
 .setSource(JSONObject.*toJSONString*(wusong), XContentType.***JSON***)  
 );  
  
 bulkRequestBuilder.get();  
 client.close();  
  
}

#### 2、通过数据id使用prepareGet来查询索引

通过id来进行查询索引

*/\*\*  
 \* 通过id来进行精确查询  
 \*/*@Test  
**public void** query1() {  
 GetResponse documentFields = **client**.prepareGet(**"indexsearch"**, **"mysearch"**, **"11"**).get();  
 String index = documentFields.getIndex();  
 String type = documentFields.getType();  
 String id = documentFields.getId();  
 System.***out***.println(index);  
 System.***out***.println(type);  
 System.***out***.println(id);  
 Map<String, Object> source = documentFields.getSource();  
 **for** (String s : source.keySet()) {  
 System.***out***.println(source.get(s));  
 }  
}

#### 3、查询索引库当中的所有数据

*/\*\*  
 \* 查询所有数据  
 \*/*@Test  
**public void** queryAll() {  
 SearchResponse searchResponse = **client** .prepareSearch(**"indexsearch"**)  
 .setTypes(**"mysearch"**)  
 .setQuery(**new** MatchAllQueryBuilder())  
 .get();  
 SearchHits searchHits = searchResponse.getHits();  
 SearchHit[] hits = searchHits.getHits();  
 **for** (SearchHit hit : hits) {  
 String sourceAsString = hit.getSourceAsString();  
 System.***out***.println(sourceAsString);  
 }  
 **client**.close();  
}

#### 4、RangeQuery范围值查询

查找索引库当中年龄为18到28的所有人

*/\*\*  
 \* 查找年龄18到28的人,包含18和28  
 \*/*@Test  
**public void** rangeQuery(){  
 SearchResponse searchResponse = **client**.prepareSearch(**"indexsearch"**)  
 .setTypes(**"mysearch"**)  
 .setQuery(**new** RangeQueryBuilder(**"age"**).gt(17).lt(29))  
 .get();  
 SearchHits hits = searchResponse.getHits();  
 SearchHit[] hits1 = hits.getHits();  
 **for** (SearchHit documentFields : hits1) {  
 System.***out***.println(documentFields.getSourceAsString());  
 }  
 **client**.close();  
}

#### 5、termQuery词条查询

*/\*\*  
 \* 词条查询  
 \*/*@Test  
**public void** termQuery(){  
 SearchResponse searchResponse = **client**.prepareSearch(**"indexsearch"**).setTypes(**"mysearch"**)  
 .setQuery(**new** TermQueryBuilder(**"say"**, **"熟悉"**))  
 .get();  
 SearchHits hits = searchResponse.getHits();  
 SearchHit[] hits1 = hits.getHits();  
 **for** (SearchHit documentFields : hits1) {  
 System.***out***.println(documentFields.getSourceAsString());  
 }  
}

#### 6、fuzzyQuery模糊查询

模糊查询可以自动帮我们纠正写错误的英文单词，最大纠正次数两次

*/\*\*  
 \* fuzzyQuery表示英文单词的最大可纠正次数，最大可以自动纠正两次  
 \*/*@Test  
**public void** fuzzyQuery(){  
 SearchResponse searchResponse = **client**.prepareSearch(**"indexsearch"**).setTypes(**"mysearch"**)  
 .setQuery(QueryBuilders.*fuzzyQuery*(**"say"**, **"helOL"**).fuzziness(Fuzziness.***TWO***))  
 .get();  
 SearchHits hits = searchResponse.getHits();  
 SearchHit[] hits1 = hits.getHits();  
 **for** (SearchHit documentFields : hits1) {  
 System.***out***.println(documentFields.getSourceAsString());  
 }  
 **client**.close();  
}

#### 7、wildCardQuery通配符查询

\*：匹配任意多个字符

？：仅匹配一个字符

*/\*\*  
 \* 模糊匹配查询有两种匹配符，分别是" \* " 以及 " ? "， 用" \* "来匹配任何字符，包括空字符串。用" ? "来匹配任意的单个字符  
 \*/*@Test  
**public void** wildCardQueryTest(){  
 SearchResponse searchResponse = **client**.prepareSearch(**"indexsearch"**).setTypes(**"mysearch"**)  
 .setQuery(QueryBuilders.*wildcardQuery*(**"say"**, **"hel\*"**))  
 .get();  
 SearchHits hits = searchResponse.getHits();  
 SearchHit[] hits1 = hits.getHits();  
 **for** (SearchHit documentFields : hits1) {  
 System.***out***.println(documentFields.getSourceAsString());  
 }  
 **client**.close();  
}

#### 8、boolQuery 多条件组合查询

使用boolQuery实现多条件组合查询

查询年龄是18到28范围内且性别是男性的，或者id范围在10到13范围内的

*/\*\*  
 \* 多条件组合查询 boolQuery  
 \* 查询年龄是18到28范围内且性别是男性的，或者id范围在10到13范围内的  
 \*  
 \*/*@Test  
**public void** boolQueryTest(){  
 RangeQueryBuilder age = QueryBuilders.*rangeQuery*(**"age"**).gt(17).lt(29);  
 TermQueryBuilder sex = QueryBuilders.*termQuery*(**"sex"**, **"1"**);  
 RangeQueryBuilder id = QueryBuilders.*rangeQuery*(**"id"**).gt(**"9"**).lt(**"15"**);  
  
 SearchResponse searchResponse = **client**.prepareSearch(**"indexsearch"**).setTypes(**"mysearch"**)  
 .setQuery(  
 QueryBuilders.*boolQuery*().should(id)  
 .should(QueryBuilders.*boolQuery*().must(sex).must(age)))  
 .get();  
 SearchHits hits = searchResponse.getHits();  
 SearchHit[] hits1 = hits.getHits();  
 **for** (SearchHit documentFields : hits1) {  
 System.***out***.println(documentFields.getSourceAsString());  
 }  
 **client**.close();  
}

#### 9、分页与高亮查询

##### 1、分页查询

*/\*分页查询  
 \*/*@Test  
**public void** getPageIndex(){  
 **int** pageSize = 5;  
 **int** pageNum = 2;  
 **int** startNum = (pageNum-1)\*5;  
 SearchResponse searchResponse = **client**.prepareSearch(**"indexsearch"**)  
 .setTypes(**"mysearch"**)  
 .setQuery(QueryBuilders.*matchAllQuery*())  
 .addSort(**"id"**,SortOrder.***ASC***)  
 .setFrom(startNum)  
 .setSize(pageSize)  
 .get();  
 SearchHits hits = searchResponse.getHits();  
 SearchHit[] hits1 = hits.getHits();  
 **for** (SearchHit documentFields : hits1) {  
 System.***out***.println(documentFields.getSourceAsString());  
 }  
 **client**.close();  
}

##### 2、高亮查询

在进行关键字搜索时，搜索出的内容中的关键字会显示不同的颜色，称之为高亮

百度搜索关键字"传智播客"



京东商城搜索"笔记本"



##### 3、高亮显示的html分析

通过开发者工具查看高亮数据的html代码实现：



ElasticSearch可以对查询出的内容中关键字部分进行标签和样式的设置，但是你需要告诉ElasticSearch使用什么标签对高亮关键字进行包裹

##### 4、高亮显示代码实现

*/\*\*  
 \* 高亮查询  
 \*/*@Test  
**public void** highLight(){  
 *//设置我们的查询高亮字段* SearchRequestBuilder searchRequestBuilder = **client**.prepareSearch(**"indexsearch"**)  
 .setTypes(**"mysearch"**)  
 .setQuery(QueryBuilders.*termQuery*(**"say"**, **"hello"**));  
  
 *//设置我们字段高亮的前缀与后缀* HighlightBuilder highlightBuilder = **new** HighlightBuilder();  
 highlightBuilder.field(**"say"**).preTags(**"<font style='color:red'>"**).postTags(**"</font>"**);  
  
 *//通过高亮来进行我们的数据查询* SearchResponse searchResponse = searchRequestBuilder.highlighter(highlightBuilder).get();  
 SearchHits hits = searchResponse.getHits();  
 System.***out***.println(**"查询出来一共"**+ hits.**totalHits**+**"条数据"**);  
 **for** (SearchHit hit : hits) {  
 *//打印没有高亮显示的数据* System.***out***.println(hit.getSourceAsString());  
 System.***out***.println(**"========================="**);  
 *//打印我们经过高亮显示之后的数据* Text[] says = hit.getHighlightFields().get(**"say"**).getFragments();  
 **for** (Text say : says) {  
 System.***out***.println(say);  
 }  
  
 */\* Map<String, HighlightField> highlightFields = hit.getHighlightFields();  
 System.out.println(highlightFields);\*/* }  
 **client**.close();  
}

### 4、更新索引

根据系统给数据生成的id来进行更新索引

*/\*\*  
 \* 更新索引  
 \* 根据数据id来进行更新索引  
 \*/*@Test  
**public void** updateIndex(){  
 Person guansheng = **new** Person(5, **"宋江"**, 88, 0, **"水泊梁山"**, **"17666666666"**, **"wusong@itcast.com"**,**"及时雨宋江"**);  
 **client**.prepareUpdate().setIndex(**"indexsearch"**).setType(**"mysearch"**).setId(**"5"**)  
 .setDoc(JSONObject.*toJSONString*(guansheng),XContentType.***JSON***)  
 .get();  
 **client**.close();  
}

### 5、删除索引

#### 1、按照id进行删除

*/\*\*  
 \* 按照id进行删除数据  
 \*/*@Test  
**public void** deleteById(){  
 DeleteResponse deleteResponse = **client**.prepareDelete(**"indexsearch"**, **"mysearch"**, **"14"**).get();  
 **client**.close();  
}

#### 2、按照查询条件来进行删除

*/\*  
按照条件进行删除  
 \*/*@Test  
**public void** deleteByQuery(){  
  
 BulkByScrollResponse bulkByScrollResponse = DeleteByQueryAction.***INSTANCE***.newRequestBuilder(**client**)  
 .filter(QueryBuilders.*rangeQuery*(**"id"**).gt(2).lt(4))  
 .source(**"indexsearch"**)  
 .get();  
 **long** deleted = bulkByScrollResponse.getDeleted();  
 System.***out***.println(deleted);  
  
}

#### 3、删除整个索引库

*/\*\*  
 \* 删除索引  
 \* 删除整个索引库  
 \*/*@Test  
**public void** deleteIndex(){  
 DeleteIndexResponse indexsearch = **client**.admin().indices().prepareDelete(**"indexsearch"**).execute().actionGet();  
 **client**.close();  
}

# 第二章 LogStash

## 1、LogStash介绍及安装

官网：

<https://www.elastic.co/guide/en/logstash/current/index.html>

### 1.1 介绍

logstash就是一个具备实时数据传输能力的管道，负责将数据信息从管道的输入端传输到管道的输出端；与此同时这根管道还可以让你根据自己的需求在中间加上滤网，Logstash提供里很多功能强大的滤网以满足你的各种应用场景。是一个input | filter | output 的数据流。

### 1.2 、node01机器安装LogStash

下载logstache并上传到第一台服务器的/home/es路径下，然后进行解压  
# 下载安装包---可以直接将已经下载好的安装包上传到/home/es路径下即可

cd /home/eswget https://artifacts.elastic.co/downloads/logstash/logstash-6.0.0.tar.gz# 解压tar -zxvf logstash-6.0.0.tar.gz -C /export/servers/es/

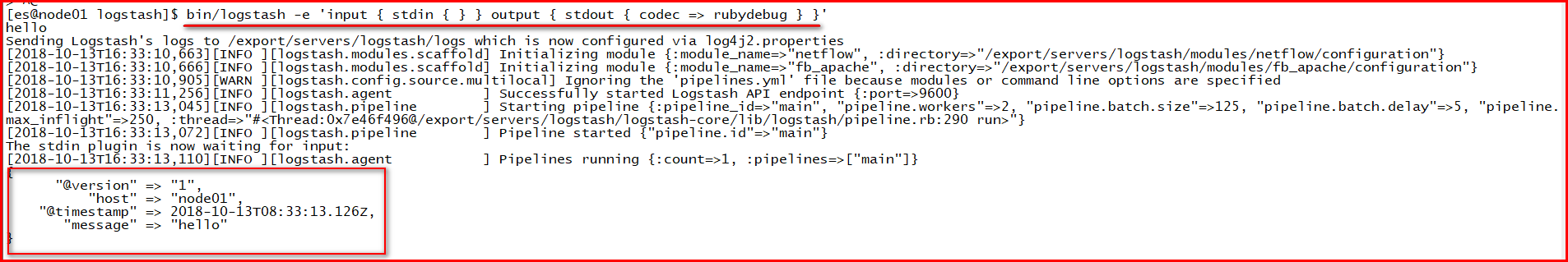
### 1.3 Input插件

#### 1.3.1 stdin标准输入和stdout标准输出

使用标准的输入与输出组件，实现将我们的数据从控制台输入，从控制台输出

cd /export/servers/es/logstash-6.0.0

bin/logstash -e 'input{stdin{}}output{stdout{codec=>rubydebug}}'



{  
 "@version" => "1",  
 "host" => "node01",  
 "@timestamp" => 2018-10-13T08:33:13.126Z,  
 "message" => "hello"  
}

#### 1.3.2 监控日志文件变化

Logstash 使用一个名叫 *FileWatch* 的 Ruby Gem 库来监听文件变化。这个库支持 glob 展开文件路径，而且会记录一个叫 *.sincedb* 的数据库文件来跟踪被监听的日志文件的当前读取位置。所以，不要担心 logstash 会漏过你的数据。

##### 编写脚本

cd /export/servers/es/logstash-6.0.0/config

vim monitor\_file.conf

#输入一下信息

input{

file{

path => "/export/servers/es/datas/tomcat.log"

type => "log"

start\_position => "beginning"

}

}

output{

stdout{

codec=>rubydebug

}

}

##### 检查配置文件是否可用

cd /export/servers/es/logstash-6.0.0/

bin/logstash -f /export/servers/es/logstash-6.0.0/config/monitor\_file.conf -t

成功会出现一下信息：

Config Validation Result: OK. Exiting Logstash

##### 启动服务

cd /export/servers/es/logstash-6.0.0

bin/logstash -f /export/servers/es/logstash-6.0.0/config/monitor\_file.conf

##### 发送数据

新开xshell窗口通过以下命令发送数据

mkdir -p /export/servers/es/datas

echo "hello logstash" >> /export/servers/es/datas/tomcat.log

##### 其它参数说明

Path=>表示监控的文件路径  
Type=>给类型打标记，用来区分不同的文件类型。  
Start\_postion=>从哪里开始记录文件，默认是从结尾开始标记，要是你从头导入一个文件就把改成”beginning”.  
discover\_interval=>多久去监听path下是否有文件，默认是15s  
exclude=>排除什么文件  
close\_older=>一个已经监听中的文件，如果超过这个值的时间内没有更新内容，就关闭监听它的文件句柄。默认是3600秒，即一个小时。  
sincedb\_path=>监控库存放位置(默认的读取文件信息记录在哪个文件中)。默认在：/data/plugins/inputs/file。  
sincedb\_write\_interval=> logstash 每隔多久写一次 sincedb 文件，默认是 15 秒。  
stat\_interval=>logstash 每隔多久检查一次被监听文件状态（是否有更新），默认是 1 秒。

#### 1.3.3、jdbc插件

jdbc插件允许我们采集某张数据库表当中的数据到我们的logstashe当中来

##### 第一步：编写脚本

开发脚本配置文件

cd /export/servers/es/logstash-6.0.0/config

vim jdbc.conf

input {

jdbc {

jdbc\_driver\_library => "/home/es/mysql-connector-java-5.1.38.jar"

jdbc\_driver\_class => "com.mysql.jdbc.Driver"

jdbc\_connection\_string => "jdbc:mysql://192.168.31.82:3306/userdb"

jdbc\_user => "root"

jdbc\_password => "admin"

use\_column\_value => true

tracking\_column => "create\_time"

schedule => "\* \* \* \* \*"

statement => "SELECT \* from emp where create\_time > :sql\_last\_value ;"

}

}

output{

stdout{

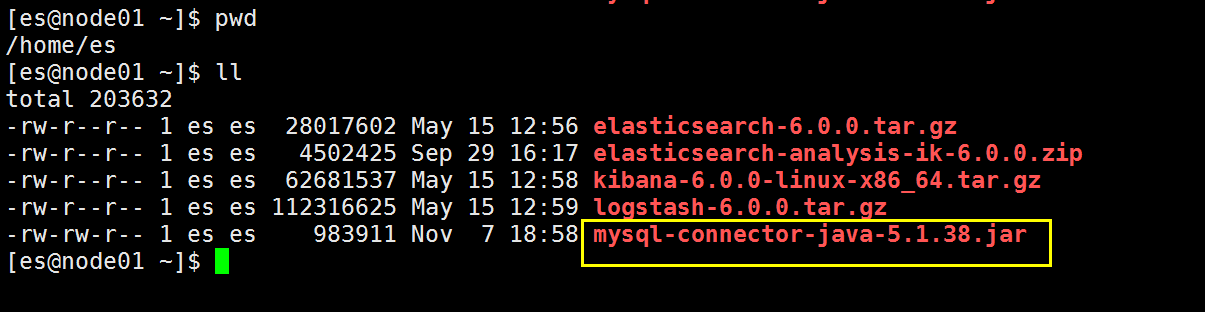
codec=>rubydebug

}

}

##### 第二步：上传mysql连接驱动包到指定路劲

将我们mysql的连接驱动包上传到我们指定的/home/es/路径下



##### 第三步：检查配置文件是否可用

cd /export/servers/es/logstash-6.0.0/

bin/logstash -f /export/servers/es/logstash-6.0.0/config/monitor\_tcp.conf -t

通过之后

Config Validation Result: OK. Exiting Logstash

##### 第四步：启动服务

通过以下命令启动logstash

cd /export/servers/es/logstash-6.0.0

bin/logstash -f /export/servers/es/logstash-6.0.0/config/jdbc.conf

##### 第五步：数据库当中添加数据

在我们的数据库当中手动随便插入数据，发现我们的logstash可以进行收集

#### 1.3.4 systlog插件

**syslog机制负责记录内核和应用程序产生的日志信息，管理员可以通过查看日志记录，来掌握系统状况**

默认系统已经安装了rsyslog.直接启动即可

##### 编写脚本

cd /export/servers/es/logstash-6.0.0/config

vim syslog.conf

input{  
 tcp{  
 port=> 6789  
 type=> syslog  
 }  
 udp{  
 port=> 6789  
 type=> syslog  
 }  
}  
  
filter{  
 if [type] == "syslog" {  
 grok {  
 match => { "message" => "%{SYSLOGTIMESTAMP:syslog\_timestamp} %{SYSLOGHOST:syslog\_hostname} %{DATA:syslog\_program}(?:\[%{POSINT:syslog\_pid}\])?: %{GREEDYDATA:syslog\_message}" }  
 add\_field => [ "received\_at", "%{@timestamp}" ]  
 add\_field => [ "received\_from", "%{host}" ]  
 }  
 date {  
 match => [ "syslog\_timestamp", "MMM d HH:mm:ss", "MMM dd HH:mm:ss" ]  
 }  
 }  
}  
  
output{  
 stdout{  
 codec=> rubydebug  
 }  
}

##### 检查配置文件是否可用

cd /export/servers/es/logstash-6.0.0

bin/logstash -f /export/servers/es/logstash-6.0.0/config/syslog.conf -t

##### 启动服务

执行以下命令启动logstash服务

cd /export/servers/es/logstash-6.0.0

bin/logstash -f /export/servers/es/logstash-6.0.0/config/syslog.conf

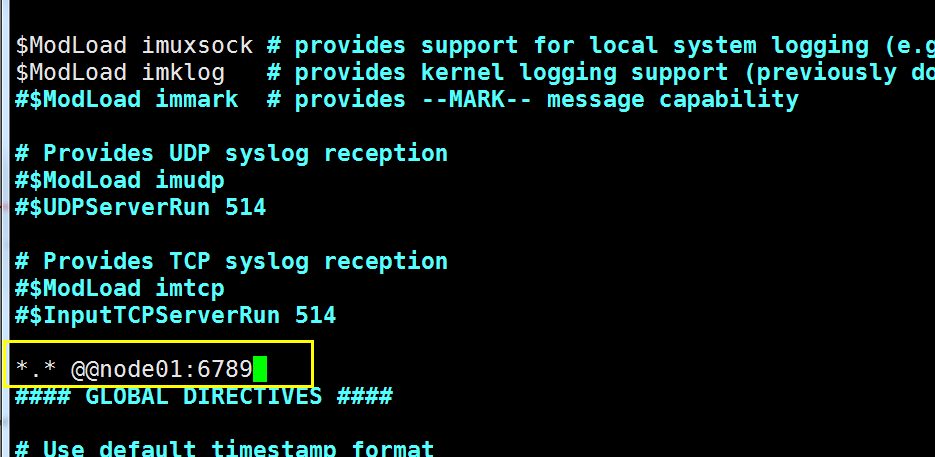
##### 发送数据

修改系统日志配置文件

sudo vim /etc/rsyslog.conf

添加一行以下配置

\*.\* @@node01:6789



# 重启系统日志服务

sudo /etc/init.d/rsyslog restart

##### 其它参数说明

在logstash中的grok是正则表达式，用来解析当前数据

原始数据其实是：

Dec 23 12:11:43 louis postfix/smtpd[31499]: connect from unknown[95.75.93.154]  
Jun 05 08:00:00 louis named[16000]: client 199.48.164.7#64817: query (cache) 'amsterdamboothuren.com/MX/IN' denied  
Jun 05 08:10:00 louis CRON[620]: (www-data) CMD (php /usr/share/cacti/site/poller.php >/dev/null 2>/var/log/cacti/poller-error.log)  
Jun 05 08:05:06 louis rsyslogd: [origin software="rsyslogd" swVersion="4.2.0" x-pid="2253" x-info="http://www.rsyslog.com"] rsyslogd was HUPed, type 'lightweight'.

### 1.4、filter插件

Logstash之所以强悍的主要原因是filter插件；通过过滤器的各种组合可以得到我们想要的结构化数据。

1、grok正则表达式

grok正则表达式是logstash非常重要的一个环节；可以通过grok非常方便的将数据拆分和索引

语法格式：

(?<name>pattern)

？<name>表示要取出里面的值，pattern就是正则表达式

#### 1、收集控制台输入数据，采集日期时间出来

##### 第一步：开发配置文件

cd /export/servers/es/logstash-6.0.0/config/

vim filter.conf

input {stdin{}} filter {

grok {

match => {

"message" => "(?<date>\d+\.\d+)\s+"

}

}

}

output {stdout{codec => rubydebug}}

##### 第二步：启动logstash服务

cd /export/servers/es/logstash-6.0.0/

bin/logstash -f /export/servers/es/logstash-6.0.0/config/filter.conf

##### 第三步：控制台输入文字

5.20 今天天气还不错



#### 2、使用grok收集nginx日志数据

nginx一般打印出来的日志格式如下

36.157.150.1 - - [05/Nov/2018:12:59:28 +0800] "GET /phpmyadmin\_8c1019c9c0de7a0f/js/get\_scripts.js.php?scripts%5B%5D=jquery/jquery-1.11.1.min.js&scripts%5B%5D=sprintf.js&scripts%5B%5D=ajax.js&scripts%5B%5D=keyhandler.js&scripts%5B%5D=jquery/jquery-ui-1.11.2.min.js&scripts%5B%5D=jquery/jquery.cookie.js&scripts%5B%5D=jquery/jquery.mousewheel.js&scripts%5B%5D=jquery/jquery.event.drag-2.2.js&scripts%5B%5D=jquery/jquery-ui-timepicker-addon.js&scripts%5B%5D=jquery/jquery.ba-hashchange-1.3.js HTTP/1.1" 200 139613 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36"

这种日志是非格式化的，通常，我们获取到日志后，还要使用mapreduce 或者spark 做一下清洗操作，

就是将非格式化日志编程格式化日志；

在清洗的时候，如果日志的数据量比较大，那么也是需要花费一定的时间的；

所以可以使用logstash 的grok 功能，将nginx 的非格式化数据采集成格式化数据：

##### 第一步：安装grok插件

###### 第一种方式安装：在线安装（墙裂不推荐）

在线安装grok插件

cd /export/servers/es/logstash-6.0.0/

vim Gemfile

#source 'https://rubygems.org' # 将这个镜像源注释掉

source <https://gems.ruby-china.com/> # 配置成中国的这个镜像源

准备在线安装

cd /export/servers/es/logstash-6.0.0/

bin/logstash-plugin install logstash-filter-grok

###### 第二种安装方式，直接使用我已经下载好的安装包进行本地安装（墙裂推荐使用）

上传我们的压缩包logstash-filter-grok-3.4.3.zip上传到/export/servers/es/logstash-6.0.0 这个路径下面

然后准备执行本地安装

cd /export/servers/es/logstash-6.0.0/

bin/logstash-plugin install <file:///export/servers/es/logstash-6.0.0/logstash-filter-grok-3.4.3.zip>

##### 第二步：开发logstash的配置文件

定义logstash的配置文件如下，我们从控制台输入nginx的日志数据，然后经过filter的过滤，将我们的日志文件转换成为标准的数据格式

cd /export/servers/es/logstash-6.0.0/config

vim monitor\_nginx.conf

input {stdin{}}

filter {

grok {

match => {

"message" => "%{IPORHOST:clientip} \- \- \[%{HTTPDATE:time\_local}\] \"(?:%{WORD:method} %{NOTSPACE:request}(?:HTTP/%{NUMBER:httpversion})?|%{DATA:rawrequest})\" %{NUMBER:status} %{NUMBER:body\_bytes\_sent} %{QS:http\_referer} %{QS:agent}"

}

}

}

output {stdout{codec => rubydebug}}

##### 第三步：启动logstash

执行以下命令启动logstash

cd /export/servers/es/logstash-6.0.0

bin/logstash -f /export/servers/es/logstash-6.0.0/config/monitor\_nginx.conf

##### 第四步：从控制台输入nginx日志文件数据

输入第一条数据

36.157.150.1 - - [05/Nov/2018:12:59:27 +0800] "GET /phpmyadmin\_8c1019c9c0de7a0f/js/messages.php?lang=zh\_CN&db=&collation\_connection=utf8\_unicode\_ci&token=6a44d72481633c90bffcfd42f11e25a1 HTTP/1.1" 200 8131 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36"

输入第二条数据

36.157.150.1 - - [05/Nov/2018:12:59:28 +0800] "GET /phpmyadmin\_8c1019c9c0de7a0f/js/get\_scripts.js.php?scripts%5B%5D=jquery/jquery-1.11.1.min.js&scripts%5B%5D=sprintf.js&scripts%5B%5D=ajax.js&scripts%5B%5D=keyhandler.js&scripts%5B%5D=jquery/jquery-ui-1.11.2.min.js&scripts%5B%5D=jquery/jquery.cookie.js&scripts%5B%5D=jquery/jquery.mousewheel.js&scripts%5B%5D=jquery/jquery.event.drag-2.2.js&scripts%5B%5D=jquery/jquery-ui-timepicker-addon.js&scripts%5B%5D=jquery/jquery.ba-hashchange-1.3.js HTTP/1.1" 200 139613 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36"

### 1.5、 Output插件

#### 1.5.1 标准输出到控制台

将我们收集的数据直接打印到控制台

output {  
 stdout {  
 codec => rubydebug  
 }  
}

bin/logstash -e 'input{stdin{}}output{stdout{codec=>rubydebug}}'

[es@node01 logstash]$ bin/logstash -e 'input{stdin{}}output{stdout{codec=>rubydebug}}'  
hello

#### 1.5.2 将采集数据保存到file文件中

logstash也可以将收集到的数据写入到文件当中去永久保存，接下来我们来看看logstash如何配置以实现将数据写入到文件当中

##### 第一步：开发logstash的配置文件

cd /export/servers/es/logstash-6.0.0/config

vim output\_file.conf

input {stdin{}}

output {

file {

path => "/export/servers/es/datas/%{+YYYY-MM-dd}-%{host}.txt"

codec => line {

format => "%{message}"

}

flush\_interval => 0

}

}

##### 第二步：检测配置文件并启动logstash服务

cd /export/servers/es/logstash-6.0.0

检测配置文件是否正确

bin/logstash -f config/output\_file.conf -t

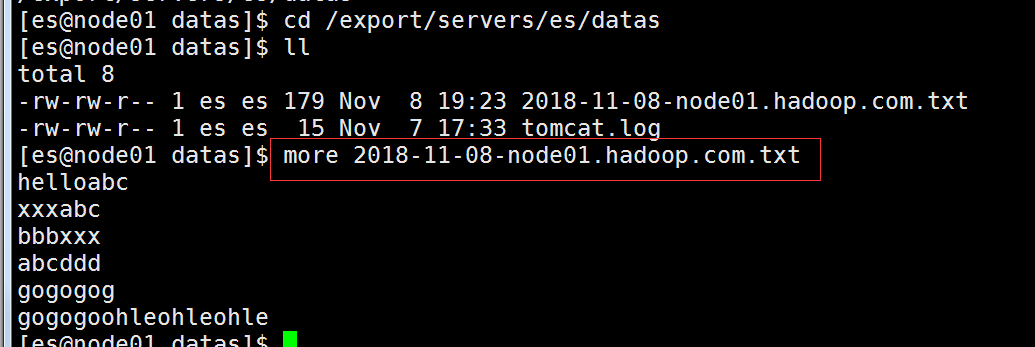
启动服务，然后从控制台输入一些数据

bin/logstash -f config/output\_file.conf

查看文件写入的内容

cd /export/servers/es/datas

more 2018-11-08-node01.hadoop.com.txt



#### 1.4.3 将采集数据保存到elasticsearch

##### 第一步：开发logstash的配置文件

cd /export/servers/es/logstash-6.0.0/config

vim output\_es.conf

input {stdin{}}  
output {  
 elasticsearch {  
 hosts => ["node01:9200"]  
 index => "logstash-%{+YYYY.MM.dd}"  
 }  
}

这个index是保存到elasticsearch上的索引名称，如何命名特别重要，因为我们很可能后续根据某些需求做查询，所以最好带时间，因为我们在中间加上type，就代表不同的业务，这样我们在查询当天数据的时候，就可以根据类型+时间做范围查询

##### 第二步：检测配置文件并启动logstash

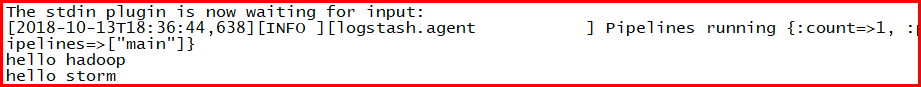
检测配置文件是否正确

cd /export/servers/es/logstash-6.0.0

bin/logstash -f config/output\_es.conf -t

启动logstash

bin/logstash -f config/output\_es.conf

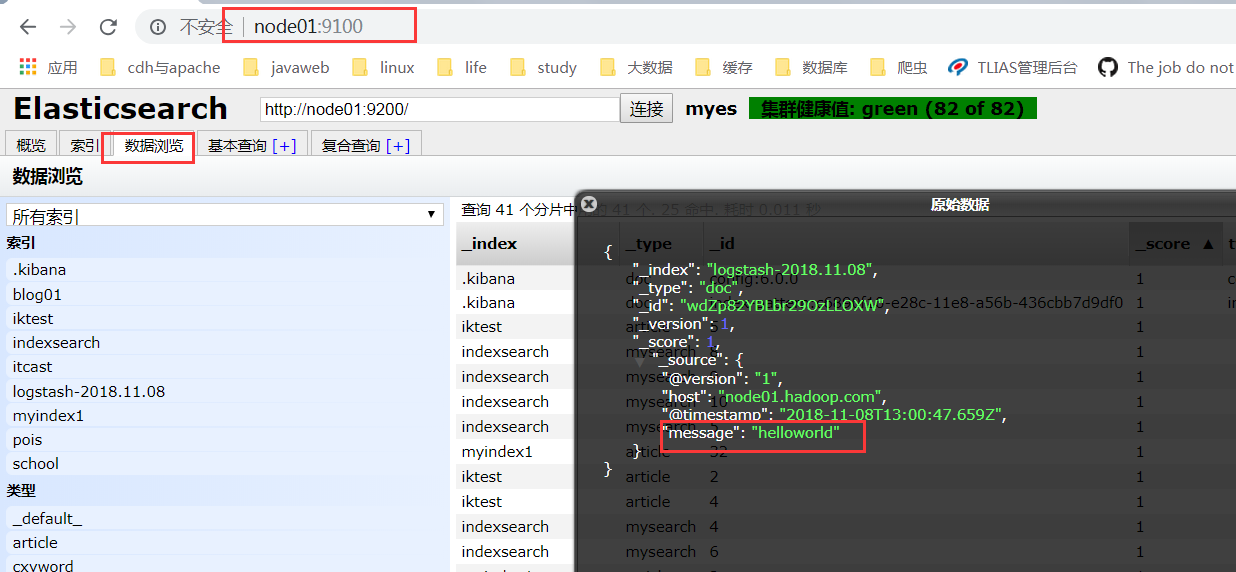


##### 第三步：es当中查看数据

访问

<http://node01:9100/>

查看es当中的数据



注意：

更多的input，filter，output组件参见以下链接

<https://www.elastic.co/guide/en/logstash/current/index.html>

# 第三章：kibana报表展示

官网对于kibana的基本简介

[*https://www.elastic.co/guide/cn/kibana/current/index.html*](https://www.elastic.co/guide/cn/kibana/current/index.html)

*kibana是一个强大的报表展示工具，可以通过kibana自定义我们的数据报表展示，实现我们的数据的各种图表查看*

*我们可以通过官网提供的数据集来实现我们的数据的报表展示*

## 第一步：下载数据集

下载账户数据集

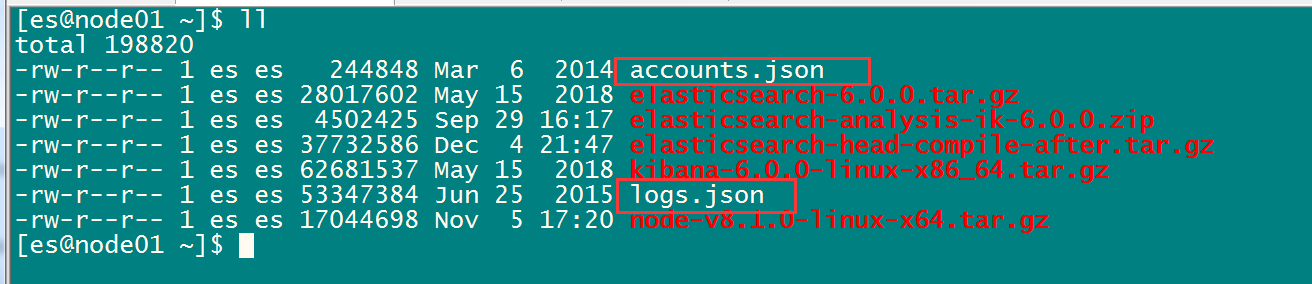
<https://download.elastic.co/demos/kibana/gettingstarted/accounts.zip>

下载日志数据集

<https://download.elastic.co/demos/kibana/gettingstarted/logs.jsonl.gz>

## 第二步：上传我们的数据集并解压

将我们以上下载的数据集全部上传到node01服务器的/home/es路径下



## 第三步：创建对应的索引库

创建我们的索引库，然后加载数据

### 第一个索引库：日志数据集数据索引库

创建第一个索引库，将我们第一个索引库日志数据也创建好

我们这里实际上按照日期，创建了三个索引库，都是用于加载我们的日志数据

PUT /logstash-2015.05.18

{

"mappings": {

"log": {

"properties": {

"geo": {

"properties": {

"coordinates": {

"type": "geo\_point"

}

}

}

}

}

}

}

PUT /logstash-2015.05.19

{

"mappings": {

"log": {

"properties": {

"geo": {

"properties": {

"coordinates": {

"type": "geo\_point"

}

}

}

}

}

}

}

PUT /logstash-2015.05.20

{

"mappings": {

"log": {

"properties": {

"geo": {

"properties": {

"coordinates": {

"type": "geo\_point"

}

}

}

}

}

}

}

## 第四步：加载示例数据到我们的索引库当中来

直接在node01的/home/es路径下执行以下命令来加载我们的示例数据到索引库当中来

node01机器上面执行以下命令

cd /home/es

curl -H 'Content-Type: application/x-ndjson' -XPOST 'node01:9200/bank/account/\_bulk?pretty' --data-binary @accounts.json

curl -H 'Content-Type: application/x-ndjson' -XPOST 'node01:9200/\_bulk?pretty' --data-binary @logs.json

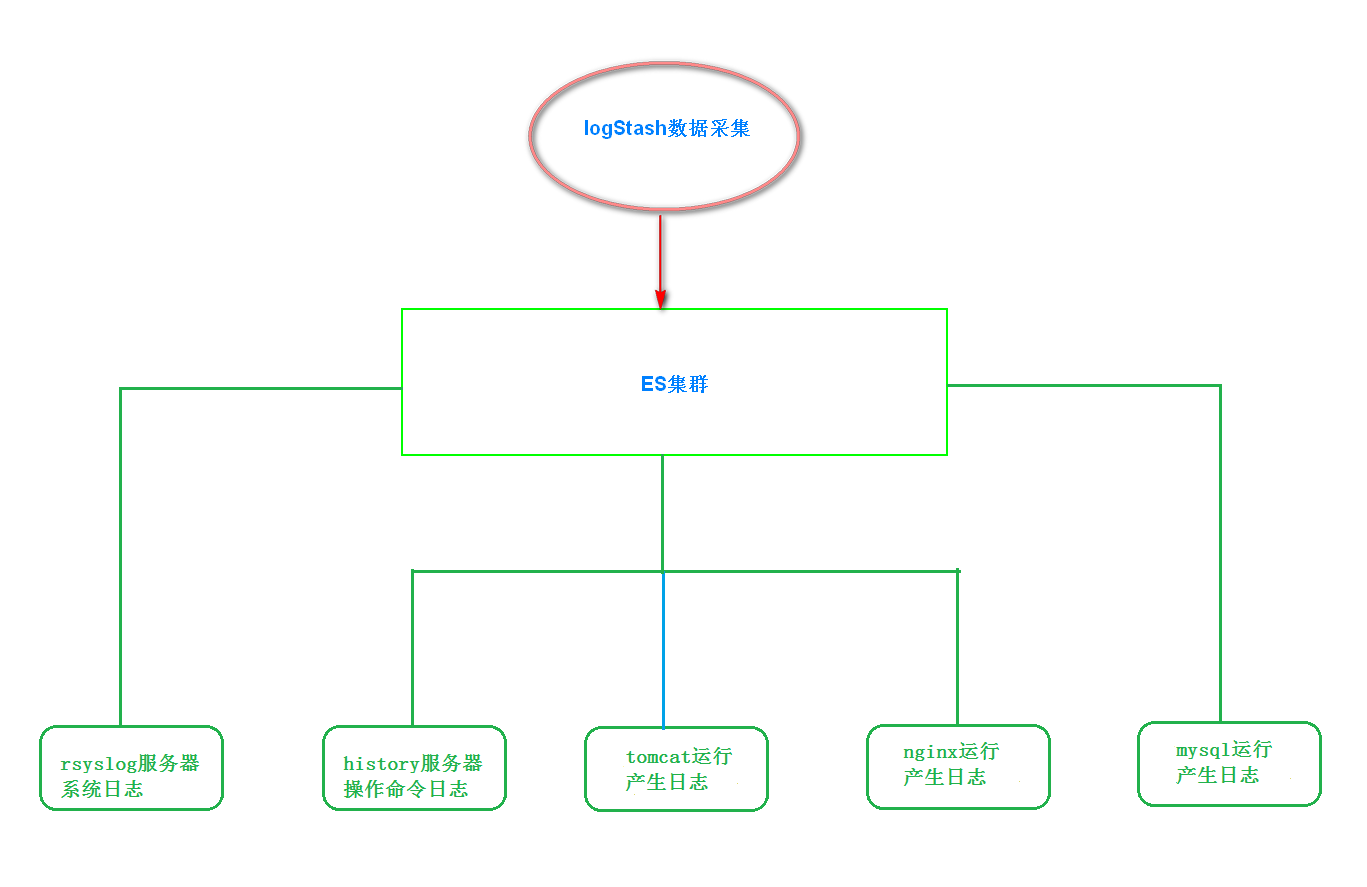
## 第五步：实现数据的报表展示

*使用饼图来展示银行数据，使用地图来实现日志数据展示*

# 第四章：logStash+ES综合案例

ELK Stack全量日志查询

在实际工作当中，我们经常会对服务器当中产生的各种日志比较感兴趣，因为产生的日志可以很好的说明我们的服务器的工作状态是否正常，日志的也可以供我们排查各种错误等。所以很多时候我们都会收集各种日志进行汇总，方便我们统一的查看，有了ELK技术栈之后，我们就可以很轻松方便的使用logstash来进行收集我们的日志数据，然后将数据存储到ES当中，然后通过kibana的可视化工具来查看我们的日志数据了



## 采集服务器运行产生的日志

### 1.1、rsyslog的基本介绍

每台linux服务器运行的时候，系统都会产生一些日志出来，我们可以收集这些日志以便于我们查看linux服务器运行的状况等

Rsyslog 是CentOS6.X 自带的一款系统日志工具：

具有以下多种特性

1.支持多线程

2.支持TCP,SSL,TLS,RELP 等协议

3.支持将日志写入MySQL, PGSQL, Oracle 等多种关系型数据中

4.拥有强大的过滤器，可实现过滤系统信息中的任意部分

*5.可以自定义日志输出格式*

接下来我们来看如何通过rsyslog来收集我们的系统日志

Rsyslog 配置文件介绍：

/etc/rsyslog.conf 文件：

|  |  |  |
| --- | --- | --- |
| \*.info;mail.none;authpriv.none;cron.none | /var/log/messages. | 各类型日志存放位置 |
| cron.\* | /var/log/cron | 具体日志存放的位置 |
| authpriv.\* | /var/log/secure | 认证授权认证 |
| mail.\* | -/var/log/maillog | 邮件日志 |
| cron.\* | /var/log/cron | 任务计划相关日志 |
| kern |  | 内核相关日志 |
| lpr |  | 打印 |
| mark(syslog) |  | rsyslog 服务内部的信  息,时间标识 |
| news |  | 新闻组 |
| user |  | 用户程序产生的相关信  息 |
| uucp |  | 协议 |
| local 0~7 |  | 用户自定义日志级别 |

日志级别：

rsyslog 共有7 种日志级别，数字代号从 0~7。具体的意义如下所示：

0 debug –有调式信息的，日志信息最多

1 info 一般信息的日志，最常用

2 notice –最具有重要性的普通条件的信息

3 warning –警告级别

4 err –错误级别，阻止某个功能或者模块不能正常工作的信息

5 crit –严重级别，阻止整个系统或者整个软件不能正常工作的信息

6 alert –需要立刻修改的信息

7 emerg –内核崩溃等严重信息

本项目中，将日志级别调整成3，并将日志信息发送至node01服务器的6789这个端口

### 1.2、修改rsyslog的配置文件

我们修改node01服务器的rsyslog的配置,

sudo vim /etc/rsyslog.conf

添加以下三行配置

local3.\* /var/log/boot.log

\*.warning /var/log/warning\_Log

\*.\* @@node01:6789



### 1.3、重启linux服务器的rsyslog服务

执行以下命令重启rsyslog服务

sudo /etc/init.d/rsyslog restart

### 1.4、开发logstash的配置文件，收集rsyslog日志

切换到logstash的配置文件目录下，开发logstash的配置文件

cd /export/servers/es/logstash-6.0.0/config

vim rsyslog.conf

input {

tcp {

port => "6789" #监控6789端口

type => "rsyslog" #日志类型是rsyslog

}

}

filter {

if [type] == "rsyslog" { # 做一次判断，只要从6789端口过来的rsyslog日志

grok { # 通过正则表达式，取出想要的字段

match => { "message" => "%{SYSLOGTIMESTAMP:syslog\_timestamp} %{SYSLOGHOST:syslog\_hostname} %{DATA:syslog\_program}(?:\[%{POSINT:syslog\_pid}\])?: %{GREEDYDATA:syslog\_message}" }

add\_field => [ "received\_at", "%{@timestamp}" ]

add\_field => [ "received\_from", "%{host}" ]

}

date {

match => [ "syslog\_timestamp", "MMM d HH:mm:ss", "MMM dd HH:mm:ss" ] #将系统的日志格式化成标准国际化时间

}

}

}

output{ #将日志打入elasticsearch

if [type] == "rsyslog"{

stdout{codec=>rubydebug}

elasticsearch {

action => "index"

hosts => "node01:9200"

index => "logstash-%{type}-%{+yyyy.MM.dd}"

}

}

}

### 1.5、启动logstash服务

cd /export/servers/es/logstash-6.0.0

bin/logstash -f config/rsyslog.conf

## 2、采集服务器用户操作所有历史日志

用户在命令行环境下的操作日志都会被系统记录下来；比如我们输入history命令，都会展示出每一个用户输入过的命令；

/etc/.bash\_history文件，这个日志格式我们可以定义成我们需要显示的内容，方便我们排查或者做入侵检查的时候；

自定义日志格式：

HISTFILESIZE=4000 #保存命令的记录总数

HISTSIZE=4000 #  history 命令输出的记录数

HISTTIMEFORMAT='%F %T' #输出时间格式

export HISTTIMEFORMAT. #自定义日志输出格式，也就是取出我们想要的字段，以json的形式

HISTTIMEFORMAT修改线上的相关格式

PROMPT\_COMMAND实时记录历史命令（一般用在存储history命令道文件中）

### 第一步：定义日志格式

修改/etc/bashrc配置文件，然后添加以下配置

sudo vim /etc/bashrc

HISTDIR='/var/log/command.log'

if [ ! -f $HISTDIR ];then

touch $HISTDIR

chmod 666 $HISTDIR

fi

export HISTTIMEFORMAT="{\"TIME\":\"%F%T\",\"HOSTNAME\":\"$HOSTNAME\",\"LI\":\"$(who am i 2>/dev/null| awk '{print $NF}'|sed -e's/[()]//g')\",\"LOGIN\_USER\":\"$(who am i|awk '{print$1}')\",\"CHECK\_USER\":\"${USER}\",\"CMD\":\""

export PROMPT\_COMMAND='history 1|tail -1|sed "s/^[ ]\+[0-9]\+ //"|sed "s/$/\"}/">>/var/log/command.log'

使配置修改立即生效

这个命令必须使用root用户来执行

export PROMPT\_COMMAND='history >> /var/log/command.log'

source /etc/bashrc

### 第二步：开发logstash的配置文件

继续开发我们logstash的配置文件

cd /export/servers/es/logstash-6.0.0/config

vim history.conf

input {

file {

path => ["/var/log/command.log"]

type => "command"

codec => "json"

}

}

output{

if [type] == "command"{

stdout{codec=>rubydebug}

elasticsearch {

hosts => "node01:9200"

index => "history-%{+yyyy.MM.dd}"

}

}

}

### 第三步：启动logstash

启动logstash：

cd /export/servers/es/logstash-6.0.0

bin/logstash -f config/history.conf

node01服务器任意目录执行任意命令，然后去9100页面，查看是否已经把history日志灌入elasticsearch

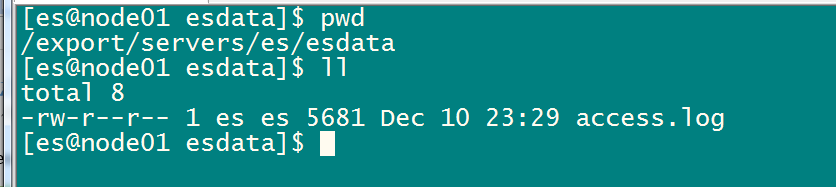
## 3、采集nginx日志到es当中

### 第一步：上传日志文件

node01机器创建文件夹，将我们的nginx的日志都上传到

/export/servers/es/esdatas

mkdir -p /export/servers/es/esdatas



### 第二步：开发logstash的配置文件

cd /export/servers/es/logstash-6.0.0/config

vim nginxlog.conf

input{

file {

path => "/export/servers/es/esdatas/access.log"

type => "access.log"

start\_position => "beginning"

}

}

filter {

grok {

match => {

"message" => "%{IPORHOST:clientip} \- \- \[%{HTTPDATE:time\_local}\] \"(?:%{WORD:method} %{NOTSPACE:request}(?:HTTP/%{NUMBER:httpversion})?|%{DATA:rawrequest})\" %{NUMBER:status} %{NUMBER:body\_bytes\_sent} %{QS:http\_referer}"

}

}

}

output {

stdout{codec=>rubydebug}

elasticsearch {

action => "index"

hosts =>"node01:9200"

index => "nginxes"

}

}

### 第三步：启动logstash并查看es当中的数据

cd /export/servers/es/logstash-6.0.0

bin/logstash -f /export/servers/es/logstash-6.0.0/config/nginxlog.conf