Elasticsearch（ES）是一个基于Lucene构建的开源、分布式、RESTful接口的全文搜索引擎。Elasticsearch还是一个分布式文档数据库，其中每个字段均可被索引，而且每个字段的数据均可被搜索，ES能够横向扩展至数以百计的服务器存储以及处理PB级的数据。可以在极短的时间内存储、搜索和分析大量的数据。通常作为具有复杂搜索场景情况下的核心发动机。

1.索引（Index）

Elasticsearch索引是一组具有共同特征的文档集合。每个索引(index)包含多个类型(type)，这些类型依次包含多个文档(document)，每个文档包含多个字段(Fields)。在Elasticsearch中索引由多个JSON文档组成。在Elasticsearch集群中可以有多个索引。
在ELK中，当logstash的JSON文档被发送给Elasticsearch时，它们被发送为默认的索引模式“logstash-%{+YYYY.mm.dd}”。它按日划分索引，以便在需要时可以方便地搜索和删除索引。这个模式可以在日志存储的输出插件中改变。

2.文档(document)

Elasticsearch文档是一个存储在索引中的JSON文档。每个文档都有一个类型和对应的ID，这是惟一的。如：

```
{
 "_index" : "packtpub",
 "_type" : "elk",
 "_id" : "1",
 "_version" : 1,
 "found" : true,
 "_source":{
 book_name : "learning elk"
 }
}
```

3.字段(Field)

文档内的一个基本单位,键值对形式(book_name : "learning elk")

4.类型(Type)

类型用于在索引中提供一个逻辑分区。它基本上表示一类类似类型的文档。一个索引可以有多个类型，我们可以根据上下文来解除它们。

5.映射(Mapping)

映射用于映射文档的每个field及其对应的数据类型，例如字符串、整数、浮点数、双精度数、日期等等。在索引创建过程中，elasticsearch会自动创建一个针对fields的映射，并且根据特定的需求类型，可以很容易地查询或修改这些映射。

6.分片(Shard)

分片是实际的物理实体用于存储每个索引的数据。每个索引都可以有大量的主和复制分片。分片分布在集群中的所有节点中，可以在节点故障或新节点添加时从一个节点移动到另一个节点。

7.主分片(Primary shard)与备份分片(replica shard)

备份分片通常驻留在一个不同的节点上，而不是主碎片，在故障转移和负载平衡的情况下，可以满足多个请求。

8.集群(Cluster)

集群是存储索引数据的节点集合。elasticsearch提供了水平的可伸缩性用以存储集群中的数据。每个集群都由一个集群名称来表示，不同的节点指明集群名称连接在一起。集群名称在elasticsearch.yml中的clustersearch.name的属性设置，它默认为“elasticsearch”：

9.节点(Node)

节点是一个单独运行的elasticsearch实例，它属于一个集群。默认情况下，elasticsearch中的每个节点都加入名为“elasticsearch”的集群。每个节点都可以在elasticsearch中使用自己的elasticsearch.yml，它们可以对内存和资源分配有不同的设置。

分成3类：

数据节点(Data Node)

数据节点索引文档并对索引文档执行搜索。建议添加更多的数据节点，以提高性能或扩展集群。通过在elasticsearch中设置这些属性，可以使节点成为一个数据节点。
elasticsearch.yml配置

```
node.master = false
node.data=true
```

管理节点(Master Node)

主节点负责集群的管理。对于大型集群，建议有三个专用的主节点(一个主节点和两个备份节点)，它们只作为主节点，不存储索引或执行搜索。在elasticsearch.yml配置声明节点为主节点:

```
node.master = true
node.data=false
```

路由节点亦称负载均衡节点(Routing Node or load balancer node)
这些节点不扮演主或数据节点的角色，但只需执行负载平衡，或为搜索请求路由，或将文档编入适当的节点。这对于高容量搜索或索引操作非常有用。

```
node.master = false
node.data=false
```

Elasticsearch有几个核心概念，先理解这些概念将有助于掌握Elasticsearch。

近实时(Near Realtime / NRT)

Elasticsearch是一个近实时的搜索平台，从生成文档索引到文档成为可搜索，有一个轻微的延迟(通常是一秒钟)。

集群(Cluster)

集群是一个或多个节点(服务器)的集合。集群中的节点一起存储数据，对外提供搜索功能。集群由一个唯一的名称标识，该名称默认是“elasticsearch”。集群名称很重要，节点都是通过集群名称加入集群。

集群不要重名，取名一般要有明确意义，否则会引起混乱。例如，开发、测试和生产集群的名称可以使用logging-dev、logging-test和logging-prod。

集群节点数不受限制，可以只有一个节点。

节点(Node)

节点是一个服务器，属于某个集群。节点存储数据，参与集群的索引和搜索功能。与集群一样，节点也是通过名称来标识的。默认情况下，启动时会分配给节点一个UUID（全局惟一标识符）作为名称。如有需要，可以给节点取名，通常取名时应考虑能方便识别和管理。

默认情况下，节点加入名为elasticsearch的集群，通过设置节点的集群名，可加入指定集群。

索引(Index)

索引是具有某种特征的文档集合，相当于一本书的目录。例如，可以为客户数据建立索引，为订单数据建立另一个索引。索引由名称标识(必须全部为小写)，可以使用该名称，对索引中的文档进行建立索引、搜索、更新和删除等操作。

一个集群中，索引数量不受限制。

文档(Document)

文档是可以建立索引的基本信息单元，相当于书的具体章节。例如，可以为单个客户创建一个文档，为单个订单创建另一个文档。文档用JSON (JavaScript对象表示法)表示。在索引中，理论上可以存储任意数量的文档。

分片与副本(Shards & Replicas)

索引可能存储大量数据，数据量可能超过单个节点的硬件限制。例如，一个索引包含10亿个文档，将占用1TB的磁盘空间，单个节点的磁盘放不下。

Elasticsearch提供了索引分片功能。创建索引时，可以定义所需的分片数量。每个分片本身都是一个功能齐全，独立的“索引”，可以托管在集群中的任何节点上。

分片之所以重要，主要有2个原因:

- 允许水平切分内容，以便内容可以存储到普通的服务器中

- 允许跨分片操作（如查询时，查询多个分片），提高性能/吞吐量

分片如何部署、如何跨片搜索完全由Elasticsearch管理，对外是透明的。

网络环境随时可能出现故障，如果某个分片/节点由于某种原因离线或消失，那么使用故障转移机制是非常有用的，强烈建议使用这种机制。为此，Elasticsearch允许为分片创建副本。

副本之所以重要，主要有2个原因:

- 在分片/节点失败时提供高可用性。因此，原分片与副本不应放在同一个节点上。
- 扩展吞吐量，因为可以在所有副本上并行执行搜索。

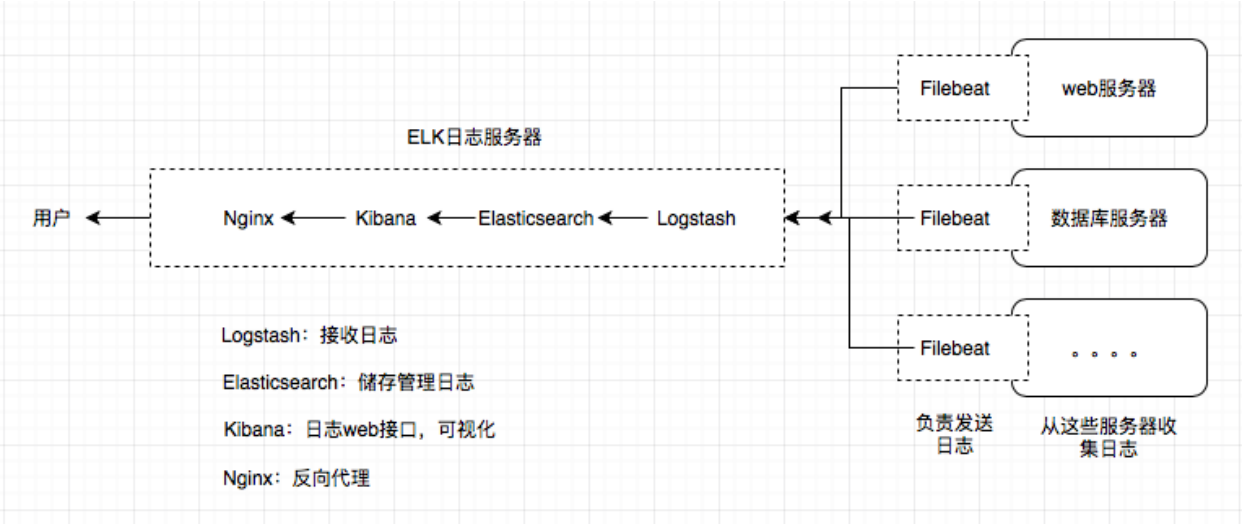
总而言之，索引可以分片，索引分片可以创建副本。复制后，每个索引将具有主分片与副本分片。

创建索引时，可以为每个索引定义分片和副本的数量。之后，还可以随时动态更改副本数量。您可以使用_shrink和_split api更改现有索引的分片数量，但动态修改副本数量相当麻烦，最好还是预先计划好分片数量。

默认情况下，Elasticsearch中的每个索引分配一个主分片和一个副本。如果集群中有两个节点，就可以将索引主分片部署在一个节点，副本分片放在另一个节点，提高可用性。

每个Elasticsearch分片都是一个Lucene索引。Lucene索引中的文档数量有限制，在LUCENE-5843中，极限是2,147,483,519(= 整数的最大值 – 128)个文档。可以使用_cat/shardsAPI监视分片大小。

日志平台的结构示意图


ELK日志服务器
用户
Nginx
Kibana
Elasticsearch
Logstash
Filebeat
web服务器
Filebeat
数据库服务器
Filebeat
. . . .
Logstash：接收日志
Elasticsearch：储存管理日志
Kibana：日志web接口，可视化
Nginx：反向代理
负责发送日志
从这些服务器收集日志

日志平台的结构示意图


日志收集
(Nxlog)
日志收集
(Nxlog)
日志收集
(Nxlog)
汇总和分析
（Logstash）
搜索和存储
(ElasticSearch)
Web界面
（Kibana）
反向代理
（Nginx）