# ELK是什么？

ELK= Elasticsearch + Logstash + Kibana

1、elasticsearch：后台分布式存储以及全文检索
2、logstash: 日志加工、“搬运工”
3、kibana：数据可视化展示。

ELK架构为数据分布式存储、可视化查询和日志解析创建了一个功能强大的管理链。 三者相互配合，取长补短，共同完成分布式大数据处理工作。

# ES特点和优势

1）分布式实时文件存储，可将每一个字段存入索引，使其可以被检索到。

2）实时分析的分布式搜索引擎。
分布式：索引分拆成多个分片，每个分片可有零个或多个副本。集群中的每个数据节点都可承载一个或多个分片，并且协调和处理各种操作；
负载再平衡和路由在大多数情况下自动完成。

3）可以扩展到上百台服务器，处理PB级别的结构化或非结构化数据。也可以运行在单台PC上（已测试）
4）支持插件机制，分词插件、同步插件、Hadoop插件、可视化插件等。

# ES Restful API GET、POST、PUT、DELETE、HEAD含义：

1）GET：获取请求对象的当前状态。
2）POST：改变对象的当前状态。
3）PUT：创建一个对象。
4）DELETE：销毁对象。
5）HEAD：请求获取对象的基础信息。
Mysql与Elasticsearch核心概念对比示意图

TERMINOLOGY

| MySQL | Elastic Search |
| --- | --- |
| Database | Index |
| Table | Type |
| Row | Document |
| Column | Field |
| Schema | Mapping |
| Index | Everything is indexed |
| SQL | Query DSL |
| SELECT * FROM table … | GET http://… |
| UPDATE table SET … | PUT http://… |

# Elasticsearch是什么?

elasticsearch用来存储日志

# Logstash是什么？

Logstash 是一个开源的数据收集引擎，它具有备实时数据传输能力。它可以统一过滤来自不同源的数据，并按照开发者的制定的规范输出到目的地。

顾名思义，Logstash 收集数据对象就是日志文件。由于日志文件来源多（如：系统日志、服务器 日志等），且内容杂乱，不便于人类进行观察。因此，我们可以使用 Logstash 对日志文件进行收集和统一过滤，变成可读性高的内容，方便开发者或运维人员观察，从而有效的分析系统/项目运行的性能，做好监控和预警的准备工作等。

# Kibana是什么？

Kibana是专门用来为ElasticSearch设计开发的，可以提供数据查询，数据可视化等功能。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