ELK

ELK是Elasticsearch,Logstash和Kibana，这三款软件都是elastic公司的产品，ELK能够我们开发和运维人员带些什么呢，下面将做些笔记。

1. 介绍ELK

架构图如下



从上面的架构图中可以看到logstash是和应用部署在同一个服务器上的，然后把数据传输给kafka消息队列, 再传给logstash到存储到Elastisearch中，接着利用Kibana来展示日志数据和数据交互(查询，搜索，监控，生成图表)。

* 1. Elasticsearch

ElasticSearch是一个基于Lucene的搜索服务器。它提供了一个分布式多用户能力的全文搜索引擎，基于RESTful web接口。Elasticsearch是用Java开发的，并作为Apache许可条款下的开放源码发布，是当前流行的企业级搜索引擎。设计用于云计算中，能够达到实时搜索，稳定，可靠，快速，安装使用方便。

我们建立一个网站或应用程序，并要添加搜索功能，但是想要完成搜索工作的创建是非常困难的。我们希望搜索解决方案要运行速度快，我们希望能有一个零配置和一个完全免费的搜索模式，我们希望能够简单地使用JSON通过HTTP来索引数据，我们希望我们的搜索服务器始终可用，我们希望能够从一台开始并扩展到数百台，我们要实时搜索，我们要简单的多租户，我们希望建立一个云的解决方案。因此我们利用Elasticsearch来解决所有这些问题及可能出现的更多其它问题。

* 1. Logstash

Logstash 是开源的服务器端数据处理管道，能够同时从多个来源采集数据，转换数据，然后将数据发送到存储库中。

数据往往以各种各样的形式或分散或集中地存在于很多系统中，Logstash 支持各种输入选择 ，可以在同一时间从众多常用来源捕捉事件。能够以连续的流式传输方式从日志、指标、Web 应用、数据存储以及各种 AWS 服务采集数据。

数据从源传输到存储库的过程中，Logstash 过滤器能够解析各个事件，识别已命名的字段以构建结构，并将它们转换成通用格式，以便更轻松、更快速地分析。

尽管 Elasticsearch 是我们的首选输出方向，能够为我们的搜索和分析带来很大的帮助。

Logstash 提供很多输出选择，您可以将数据发送到您要指定的地方。

* 1. Kibana

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，并且以各种图表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。

1. 使用目的

通上面的部分功能介绍，它们可以做什么在具体项目。

2.1、日志统一管理

项目的使用Redis，PostgreSQL,Mysql等数据库，那么这些数据库日志怎么管理呢？Jboss应用服务器的日志又如何管理呢？项目应用程序是核心，那么日志又如何管理呢？

这些日志都是在各自的主目录下面，应用有问题，可能就到看什么挂了如果到各个目录下面看日志。如图用户ELK,架构图如下。

通过logstash把Jboss,Redis,Mysql等日志采集到Elasticsearch统一管理，方便了操作和管理。

2.2日志的操作

在上面的架构上面，在加上Kibana。如下图所示。

从上面的图中，通过logstash把日志采集存储到Elasticsearch中，最后在通过Kibana来操作日志或数据

通过kibana来的可是可视化操作数据，对数据的查询，并且Elasticsearch检索速度很快。在统一的地方管理操作，检索的效率也比较高的情况。

2.3生成报表和监控

上面的操作的更重要的是运行和维护方面来做的，但要深层次的挖掘用户的数据，发现用户行为习惯或是对应用的深度优化。还是要从这些数据统计分析

数据统计的这是工作最常见的事，在kibana中我们可以根据数据生成我们想要的图表，如下图



数据分析，通过机器学习对我们数据在挖机分析。