1、ELK是什么 ？

ELK是一种能够从任意数据源抽取数据，并实时对数据进行搜索、分析和可视化展现的数据分析框架

1、java 开发的开源的全文搜索引擎工具

2、基于lucence搜索引擎的

3、采用 restful - api 标准的

4、高可用、高扩展的分布式框架

5、实时数据分析的

2、为什么要用elk？

服务器众多，组件众多，日志众多
发现问题困难，技能要求高

业务场景：《实时日志分析展现》

日志主要包括系统日志、应用程序日志和安全日志。

系统运维和开发人员可以通过日志了解服务器软硬件信息、检查配置过程中的错误及错误发生的原因。经常分析日志可以了解服务器的负荷，性能安全性，从而及时采取措施纠正错误。

通常，日志被分散的储存不同的设备上。如果你管理数十上百台服务器，你还在使用依次登录每台机器的传统方法查阅日志。这样是不是感觉很繁琐和效率低下。

当务之急我们使用集中化的日志管理，例如：开源的 syslog ，将所有服务器上的日志收集汇总。

集中化管理日志后，日志的统计和检索又成为一件比较麻烦的事情，一般我们使用 grep 、awk和 wc 等 Linux 命令能实现检索和统计，但是对于要求更高的查询、排序和统计等要求和庞大的机器数量依然使用这样的方法难免有点力不从心。

开源实时日志分析 ELK 平台能够完美的解决我们上述的问题， ELK 由 ElasticSearch 、Logstash 和 Kiabana 三个开源工具组成。

3、体系架构

Elastic Stack体系架构

Beats：轻量级的数据传输组件，面向简单且目标明确的数据传输场景，可以将数据传给Logstash和Elasticsearch，需要在被采集端部署agent程序。Beats主要适用于日志文件、监控指标、网络封包、Windows事件日志、心跳等场景。

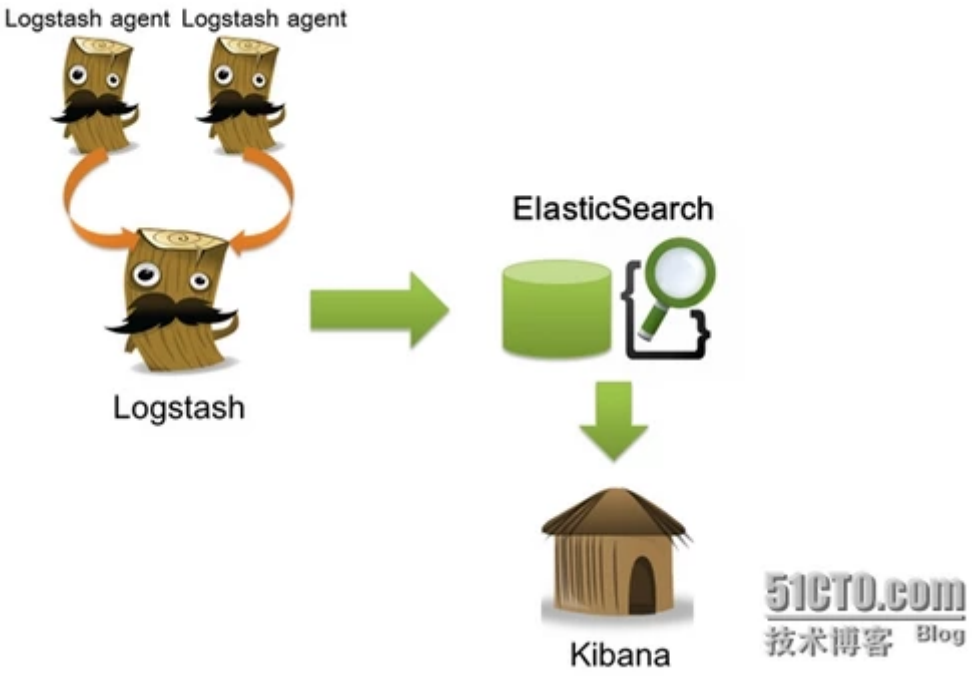
Logstash：一种动态的数据收集管道，通过丰富的插件可以方便的接驳任意数据源并输出到期望的系统中，与Elasticsearch具有强适配性。Logstash是服务侧的系统，不需要像Beats一样需要在被采集端部署agent程序。

Elasticsearch：一种分布式的，基于JSON的数据搜索分析引擎。Elasticsearch支持REST风格的API，具有可水平扩展、高可用、易维护等特点，是Elastic Stack的核心组件。

Kibana：Elastic Stack中的可视化组件，用户可以通过Kibana以多种形式查看索引在Elasticsearch中的数据，并使用Elastic Stack做数据搜索和分析。

X-Pack：提供一组加强Elastic Stack功能的扩展包，包括基于用户的安全管理、集群监控告警、数据报表导出、图探索。X-Pack需要分别在Elasticsearch节点和Kibana节点安装，部分功能可通过RestAPI管理和使用。X-Pack是付费的。

工作原理如下如所示：


Logstash agent
Logstash agent
Logstash
ElasticSearch
Kibana
51CTO.com
技术博客 Blog