日志收集系统

2018-11-23

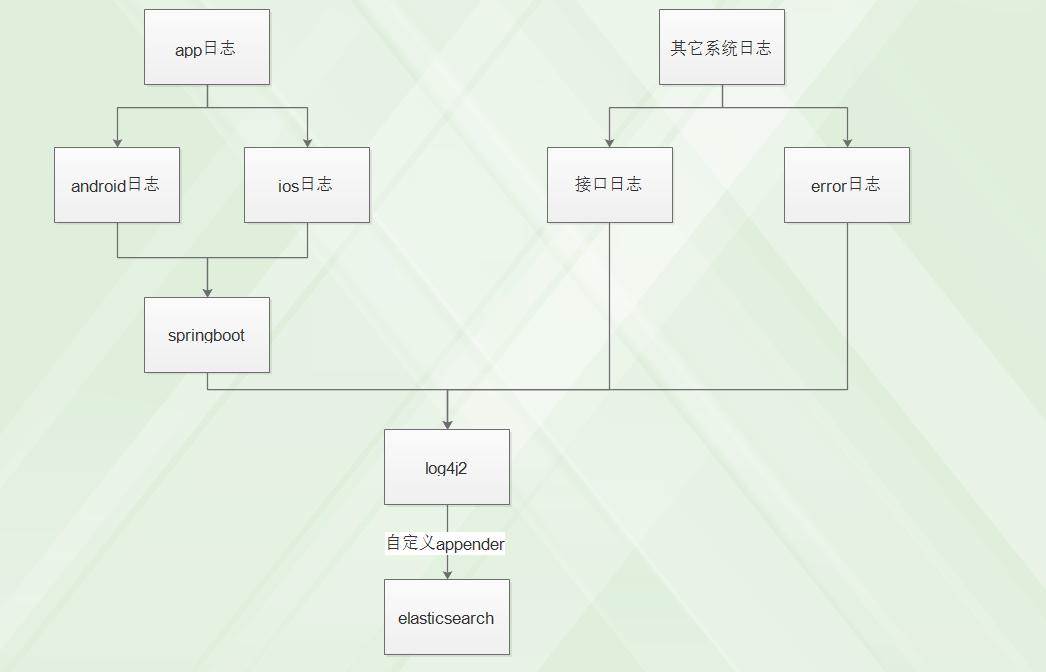
# 一、需求：

为了更好实现系统得调优，提升系统得性能，需要对app和其它各个系统的日志进行收集，然后对日志进行分析，需要搭建日志收集系统

# 二、实现思路：

1. App将日志传入后台，利用springboot对日志数据进行清洗
2. 将清洗完成的数据放入到放入到log4j2中
3. 利用loj4j2的自定义插件配置，将日志发送到elasticsearch

# 三、框架结构



Elasticsearch简介：

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](https://baike.baidu.com/item/%E4%BA%91%E8%AE%A1%E7%AE%97/9969353)中，能够达到实时搜索，稳定，可靠，快速，安装使用方便

# 四、所用到技术版本

|  |  |
| --- | --- |
| 技术名称 | 版本号 |
| Jdk | 1.8.x |
| springboot | 2.0.4.RELEASE |
| Log4j2 | 2.0.4.RELEASE |
| elasticsearch | 1.7.3 |

# 五、架构搭建：

1、搭建java环境（略）

2、搭建es集群

上传elasticsearch,然后解压



修改配置文件（config/elasticsearch.yml）

cluster.name: test-es

node.name: node05(随便起)

network.host: 192.168.73.15

http.port: 9200

在末尾添加防脑裂

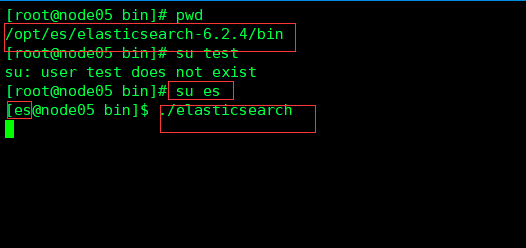
discovery.zen.ping.multicast.enabled: false

discovery.zen.ping.unicast.hosts: ["192.168.73.16","192.168.73.1", "192.168.73.14"]

discovery.zen.ping\_timeout: 120s

client.transport.ping\_timeout: 60s

切换到bin目录下，用非root用户启动es

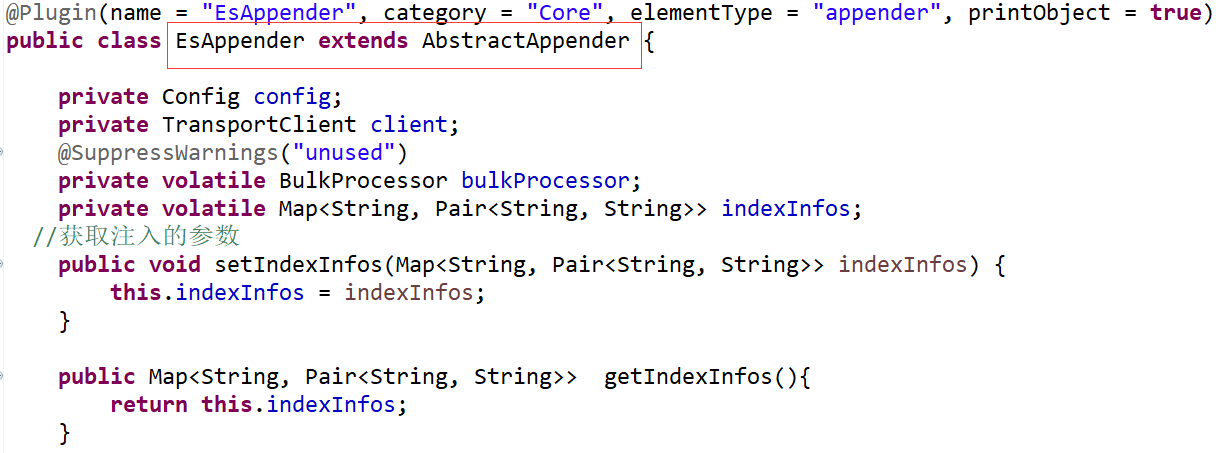


# 六、接口开发:

1.app日志接口开发

Springboot环境搭建（略）

创建类，继承AbstractAppender，重写方法



在append中实现自定义的业务



使用：

然后在其他项目的log4j2.Xml中引用



这样就用log4j2将日志，以自己想要的形式写入到了elasticsearch中

1．其它系统日志格式：

系统id^Aip^A调用时间^A响应时间^A请求参数^A响应内容

将这些信息拼接成json格式传过来调用接口