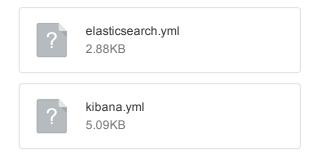
Linux 部署ELK搭建指南

/welive项目服务

10.0.0.73 james.fxy 2wsdFR\$# welive test 10.0.0.74 james.fxy 2wsdFR\$# welive prod /elasticsearch服务 10.0.0.13,10.0.0.15 James.fxy 3edfGT%\$

rpm文件的下载解压 这里主要是安装elk服务 RPM red-hat package manager rpm -ivh aa.rpm

这里是配置文件

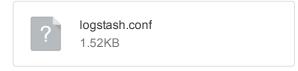


ELK elasticsearch logstash kibana 本身是一个日志分析引擎 而通过 ELK 这套解决方案,可以同时实现日志收集、日志搜索和日志分析的功能。 我们主要使用elasticsearch的全文检索

这里需要通过logstash将数据库的数据绑定导入elasticsearch (根据网上教程修改)

- 1.在/usr/share/logstash下建立config文件夹
 2.在文件夹下建立logstash.conf和logstash.yml文件
 logstash.conf是链接sqlserver数据库,进行数据的导入导出
 logstash.yml是liunx配置文件
- 具体配置如下 logstash.conf

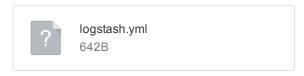
这里配置了多个索引对应的数据



单个索引的配置如下



logstash.yml配置如下



然后切换到logstash 下的bin目录下执行 sudo ./logstash 将数据导入elasticsearch

注:elasticsearch 和kibana 的配置文件放在 etc 文件目录下 logstash 的配置文件放在usr/share目录下

配置logstash.yml是启动logstash.log的

elasticsearch 配置它的elasticsearch.yml