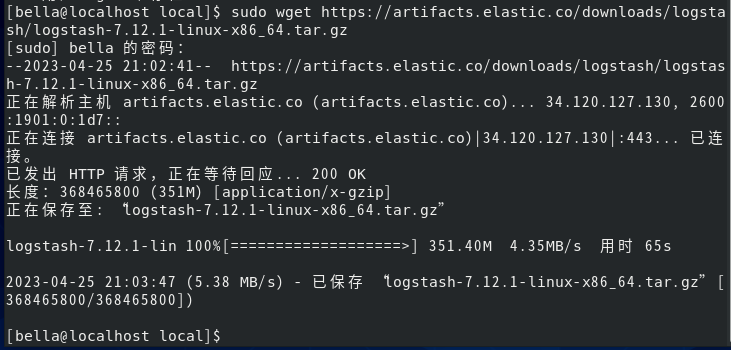
日志审计与分析

实验七

**实验目的：安装配置elk平台组件logstash**

配置logstash：



解压缩：

cd /usr/local/

tar -zxvf logstash-7.12.1-linux-x86\_64.tar.gz

mv logstash-7.12.1 logstash

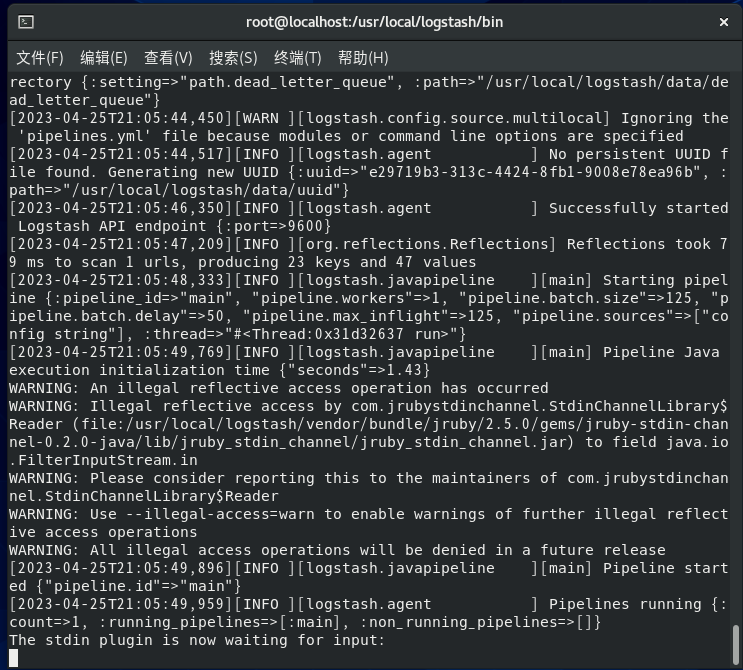
文本

描述已自动生成

测试logstash运行状态：

cd /usr/local/logstash/bin

./logstash -e 'input { stdin { } } output { stdout {} }'



命令说明：

-e 执行操作

input 标准输入

{ input } 插件

output 标准输出

{ stdout } 插件

等待logstash初始化完成

启动完成后，在命令输入任何内容，logstash会给出反馈

文本

描述已自动生成

建立配置logstash配置文件：

cd /usr/local/logstash/config

vim elk.conf

写入如内容：

input {

file {

path => "/var/log/messages"

type => "system"

start\_position => "beginning"

}

file {

path => "/var/log/secure"

type => "secure"

start\_position => "beginning"

}

}

# hosts字段ip修改为elasticsearch服务器ip地址

output {

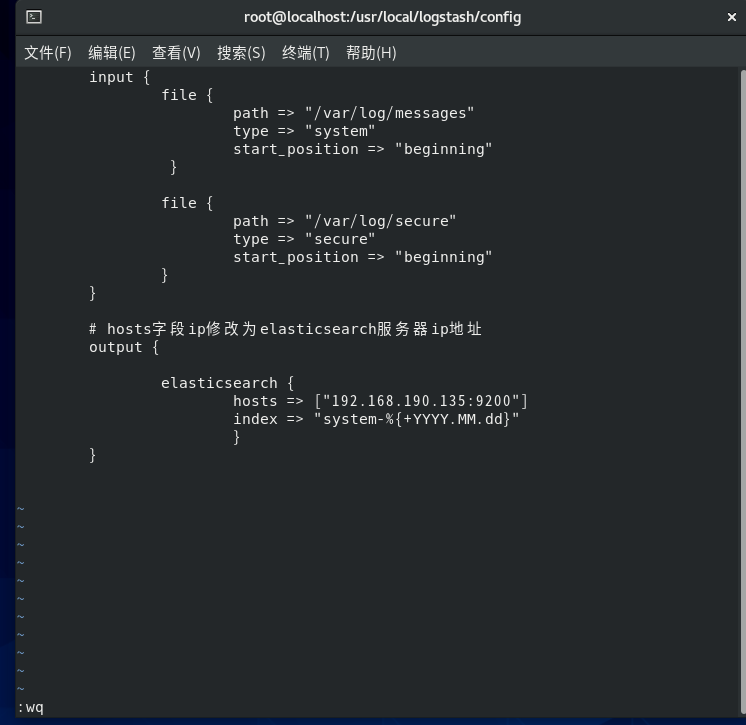
elasticsearch {

hosts => ["192.168.4.140:9200"]

index => "system-%{+YYYY.MM.dd}"

}

}



启动logstash：

logstash -f /usr/local/logstash/config/elk.conf &

