日志审计与分析

实验六

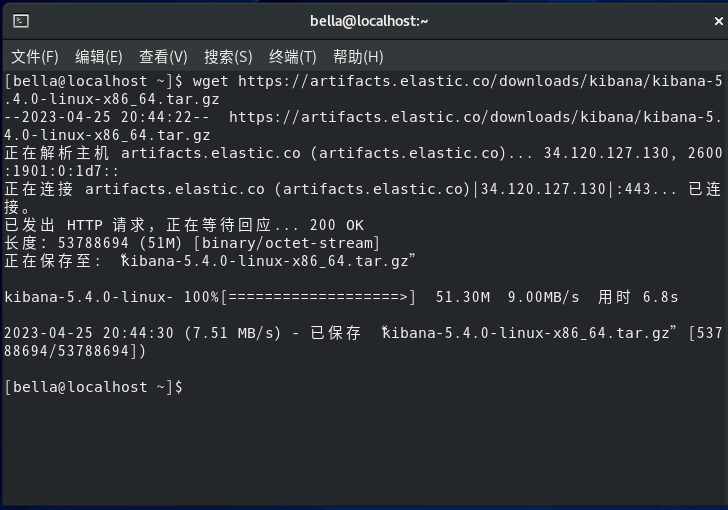
**实验目的：安装配置elk平台组件kibana**

安装kibana环境

官方安装手册:https://www.elastic.co/guide/en/kibana/current/install.html

1、下载kibana的tar.gz的软件包

# wget https://artifacts.elastic.co/downloads/kibana/kibana-5.4.0-linux-x86\_64.tar.gz



2、解压kibana的tar包

# tar -xzf kibana-5.4.0-linux-x86\_64.tar.gz



3、进入解压好的kibana

# mv kibana-5.4.0-linux-x86\_64 /usr/local

文本

描述已自动生成

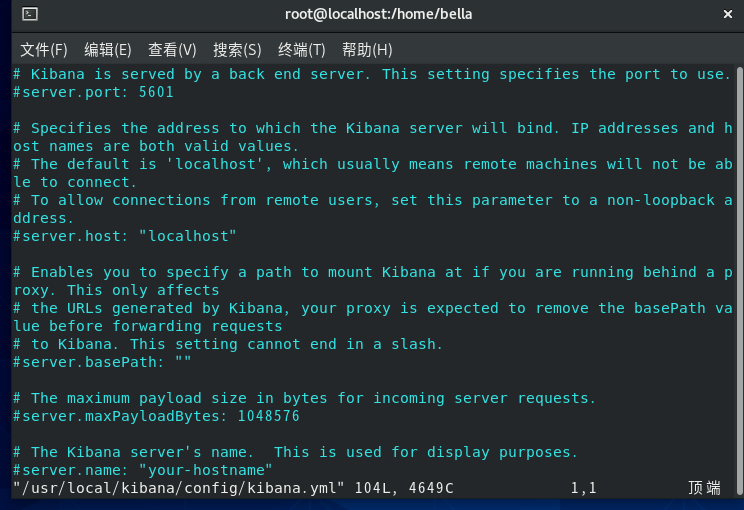
4、创建kibana的软连接

# ln -s /usr/local/kibana-5.4.0-linux-x86\_64/ /usr/local/kibana



5、编辑kibana的配置文件

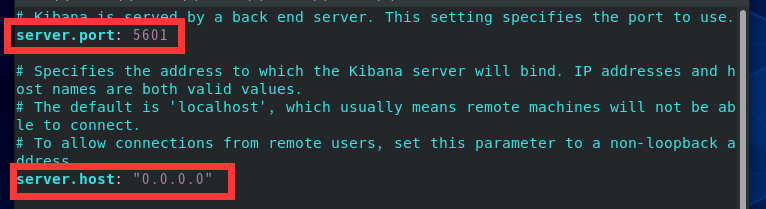
# vim /usr/local/kibana/config/kibana.yml



6、修改配置文件如下，开启以下的配置

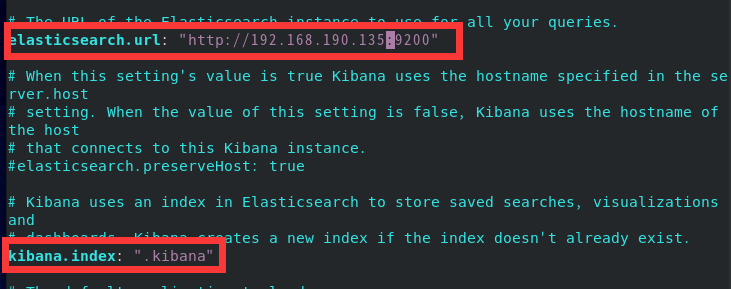
server.port: 5601

server.host: "0.0.0.0"



elasticsearch.url: "http://192.168.1.202:9200"

kibana.index: ".kibana"



7、启动kibana

# /usr/local/kibana/bin/kibana

netstat -antp |grep 5601

tcp 0 0 0.0.0.0:5601 0.0.0.0:\* LISTEN 17007/node

8、打开浏览器并设置对应的index

http://IP:5601

图形用户界面, 应用程序

描述已自动生成