日志审计与分析

实验五

实验目的：1、了解Linux软件安装配置过程

2、安装配置elasticsearch环境

实验步骤：按照文档中的流程，完成实验操作并截图

**elk平台介绍**

**e代表elasticsearch：**

**开源分布式搜索引擎**

**l代表logstash：**

**开源日志收集、过滤、并存储日志，logstash server用来收集日志。**

**k代表kibana：**

**为日志分析提供web界面，汇总、分析、搜索重要数据日志，对日志实现可视化操作。**

**---------------------------------------------------------------**

**工作流程：**

**在需要收集日志的主机上安装logstash，将收集到的内容发送到redis，将日志交给elasticsearch进行全文搜索服务，通过kibana来结合自定义搜索进行页面展示。**

**---------------------------------------------------------------**

**下载java jdk：**

**jdk-16.0.1\_linux-x64\_bin.tar.gz**

**下载地址：https://www.oracle.com/java/**

**下载elasticsearch：**

**elasticsearch-7.12.0-linux-x86\_64.tar.gz**

**下载地址：https://www.elastic.co/cn/downloads/elasticsearch**

**下载elasticsearch-head-master**

**elasticsearch-head-master.zip**

**下载地址：https://github.com/mobz/elasticsearch-head/tree/master**

**----------------------------------------------------------------**

**上传java jdk、elasticsearch、elasticsearch-head-master上传到linux：**

**1、通过mobaxterm终端上传**

**2、通过secureCRT，使用linux内置命令rz命令上传（rz命令需要centos安装lrzsz软件）**

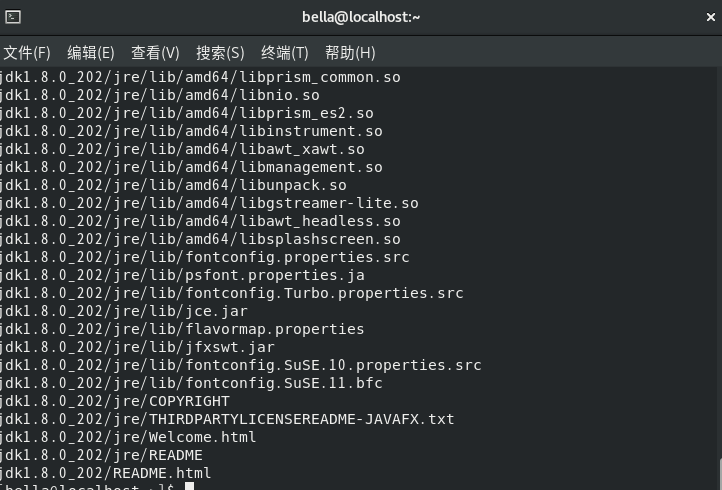
**---------------------------------------------------------------**

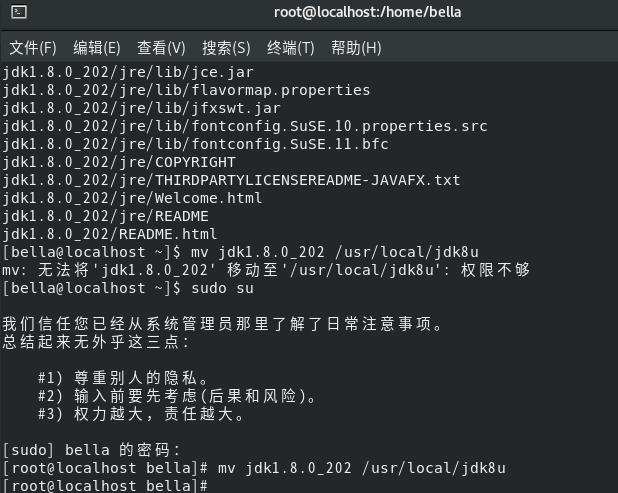
**配置java jdk：**

**解压缩：**

**tar -zxvf jdk-16.0.1\_linux-x64\_bin.tar.gz**

**mv jdk-16.0.1 /usr/local/jdk16**





**修改环境变量：**

**cd /etc**

**vim ~/.bash\_profile**

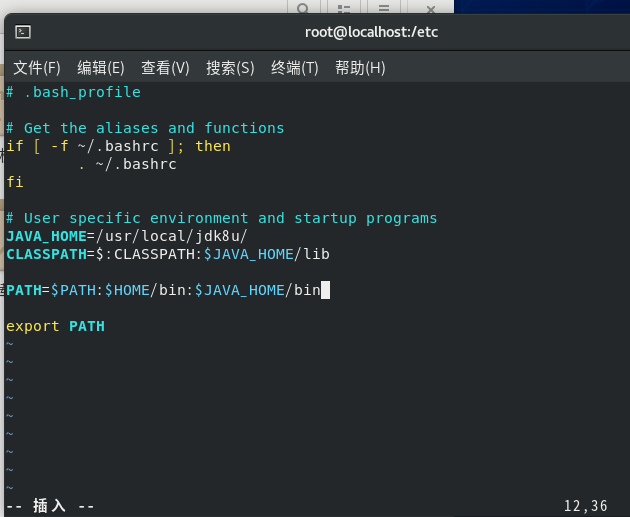
**添加如下内容：**

**JAVA\_HOME=/usr/local/jdk16/**

**CLASSPATH=$:CLASSPATH:$JAVA\_HOME/lib**

**修改PATH：**

**PATH=$PATH:$HOME/bin:$JAVA\_HOME/bin**



**使环境变量生效：**

**cd ~**

**source .bash\_profile**

一些文字和图案

描述已自动生成

**测试java环境配置：**

**java -version**

**反馈出如下内容表示配置完成：**

**[root@localhost ~]# java -version**

**java version "16.0.1" 2021-04-20**

**Java(TM) SE Runtime Environment (build 16.0.1+9-24)**

**Java HotSpot(TM) 64-Bit Server VM (build 16.0.1+9-24, mixed mode, sharing)**

图片包含 文本

描述已自动生成

**添加系统用户es：**

**useradd -r -M es**



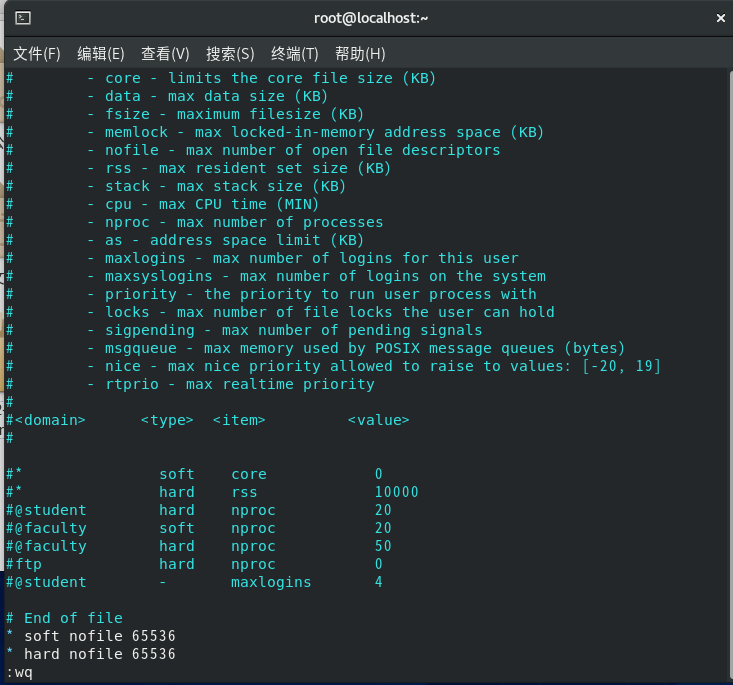
**配置系统参数：**

**vim /etc/security/limits.conf**

**添加以下内容：**

**\* soft nofile 65536**

**\* hard nofile 65536**



**vim /etc/sysctl.conf**

**添加以下内容：**

**vm.max\_map\_count=655360**

图形用户界面, 文本

描述已自动生成

**使sysctl.conf配置生效：**

**sysctl -p**



**配置elasticsearch：**

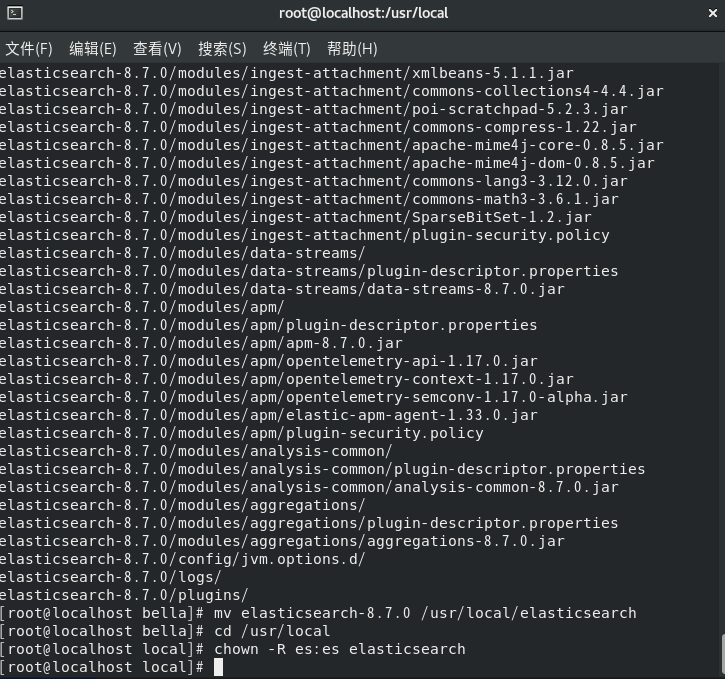
**解压缩：**

**tar -zxvf elasticsearch-7.12.0-linux-x86\_64.tar.gz**

**mv elasticsearch-7.12.0 /usr/local/elasticsearch**

**cd /usr/local/**

**chown -R es:es elasticsearch**



**测试elasticsearch配置：**

**su es**

**cd /usr/local/elasticsearch/bin/**

**./elasticsearch &**

文本

描述已自动生成

**启动完成后：**

**curl 127.0.0.1:9200**

**反馈如下内容，表示配置成功**

**{**

**"name" : "node01",**

**"cluster\_name" : "es-test",**

**"cluster\_uuid" : "i\_Yri9eASeeddbLlClFHzQ",**

**"version" : {**

**"number" : "7.12.0",**

**"build\_flavor" : "default",**

**"build\_type" : "tar",**

**"build\_hash" : "78722783c38caa25a70982b5b042074cde5d3b3a",**

**"build\_date" : "2021-03-18T06:17:15.410153305Z",**

**"build\_snapshot" : false,**

**"lucene\_version" : "8.8.0",**

**"minimum\_wire\_compatibility\_version" : "6.8.0",**

**"minimum\_index\_compatibility\_version" : "6.0.0-beta1"**

**},**

**"tagline" : "You Know, for Search"**

**}**

文本

描述已自动生成

**重启服务器：**

**reboot**

电子设备的屏幕

描述已自动生成

**创建elasticsearch服务控制文件：**

**vim /usr/lib/systemd/system/elasticsearch.service**

**写入如下内容：**

**[Unit]**

**Description=elasticsearch**

**[Service]**

**User=es**

**LimitNOFILE=100000**

**LimitNPROC=100000**

**ExecStart=/usr/local/elasticsearch/bin/elasticsearch**

**[Install]**

**WantedBy=multi-user.target**

图形用户界面, 文本

描述已自动生成



**修改elasticsearch配置文件elasticsearch.yml：**

**vim /usr/local/elasticsearch/config/elasticsearch.yml**

**添加如下内容：**

**cluster.name: es-test**

**node.name: node01**

**node.attr.rack: r1**

**network.host: 192.168.4.133 #修改为本机IP地址**

**http.port: 9200**

**cluster.initial\_master\_nodes: ["node01", "node02"]**

文本

描述已自动生成

**重启elasticsearch服务：**

**systemctl restart elasticsearch.service**



**测试服务器：**

**curl 192.168.4.133:9200**

