## Elasticsearch

|  |  |
| --- | --- |
| **服务器 / IP** | **端口** |
| **192.168.243.6** | 9084 |

|  |  |
| --- | --- |
| **安装**ES**版本** | elasticsearch-5.2.2 |
| **安装节点** | 单节点 |
| **安装路径** | /data/elk/elasticsearch |
| **安装过程** | **1）解压es安装包**  tar -zxvf elasticsearch-5.2.2.tar.gz  mv elasticsearch-5.2.2 /data/elk/  mv elasticsearch-5.2.2 elasticsearch  **2）修改es的配置文件**  vim /data/elk/elasticsearch/config/elasticsearch.yml  ==修改内容如下==  http.port: 9084 |
| **启动命令** | nohup /data/elk/elasticsearch/bin/elasticsearch & |
| **WEB-UI界面** | **\** |

## Kibana

|  |  |
| --- | --- |
| **服务器 / IP** | **端口** |
| **192.168.243.6** | 9085 |

|  |  |
| --- | --- |
| **安装**Kibana**版本** | kibana-5.2.2-linux-x86\_64.tar.gz |
| **安装节点** | 只需要安装在一台即可，我们选择192.168.243.6服务器安装kibana应用 |
| **安装路径** | /data/elk/kibana |
| **安装过程** | **1）解压kibana压缩包**  tar -zxvf kibana-5.2.2-linux-x86\_64.tar.gz.tar.gz  mv kibana-5.2.2-linux-x86\_64 /data/elk/  mv kibana-5.2.2-linux-x86\_64 kibana  **2）修改kibana的配置文件**  cd /data/elk/kibana/config  vi kibana.yml  ==修改内容如下==  server.port: 9085  server.host: "192.168.243.6"  elasticsearch.url: "http://127.0.0.1:9084" |
| **启动命令** | **1）启动kibana程序**  nohup /data/elk/kibana/bin/kibana &  **2）通过webUI验证kibana程序是否启动成功**  http://192.168.243.6:9085 |
| **WEB-UI界面** | http://192.168.243.6:9085 |

## Logstash

|  |  |  |
| --- | --- | --- |
| **服务器 / IP** | **启动端口** | **监听端口** |
| **192.168.243.6** | 9086 | 9087 |

|  |  |
| --- | --- |
| **安装Logstash版本** | Logstash-5.2.2-linux-x86\_64.tar.gz |
| **安装节点** | 只需要安装在一台即可，我们选择192.168.243.6服务器安装Logstash应用 |
| **安装路径** | /data/elk/logstash |
| **安装过程** | **1）解压**logstash**压缩包**  tar -zxvf logstash-5.2.2-linux-x86\_64.tar.gz.tar.gz  mv logstash-5.2.2-linux-x86\_64 /data/elk/  mv logstash-5.2.2-linux-x86\_64 logstash  **2）修改**logstash**的配置文件**  cd /data/elk/logstash/config  vim logstash.yml  ==修改内容如下==  http.port: 9086-9086   1. **创建日志收集配置文件**   cd /data/elk/logstash/config  vim logstash-bluemoon.conf  ==添加内容如下==  input {  log4j {  mode => "server"  host => "0.0.0.0"  port => 9087  }  }  output {  elasticsearch {  hosts => "127.0.0.1:9084"  index => "logstash-bluemoon"  }  stdout { }  } |
| **启动命令** | 1. **启动logstash程序**   cd /data/elk/logstash/  nohup ./bin/logstash -f config/logstash-bluemoon.conf & |
| **WEB-UI界面** | **\** |

## Log4j

修改项目中的log4j.porperties，添加内容：

# Logstash appender  
log4j.appender.logstash=org.apache.log4j.net.SocketAppender   
log4j.appender.logstash.RemoteHost=192.168.243.6  
log4j.appender.logstash.port=9087  
log4j.appender.logstash.Threshold=INFO  
log4j.appender.logstash.ReconnectionDelay=10000  
log4j.appender.logstash.LocationInfo=true

log4j.rootLogger修改为：

log4j.rootLogger=info,error,warn,stdout,logstash