Centos 7.7安装RabbitMQ3.8和ELK\_7.6

# 一. 安装所需软件列表

|  |
| --- |
| #将压缩包文件上传到CentOS的/opt目录下  erlang-22.3.2-1.el6.x86\_64.rpm  rabbitmq-server-3.8.3-1.el7.noarch.rpm  socat-1.7.3.2-2.el7.x86\_64.rpm  jdk-8u251-linux-x64.tar.gz  elasticsearch-7.6.2-x86\_64.rpm  kibana-7.6.2-x86\_64.rpm  logstash-7.6.2.rpm |

# 二. 安装RabbitMQ

## 2.1安装erlang

|  |
| --- |
| rpm -ivh erlang-22.3.2-1.el6.x86\_64.rpm  安装结果  warning: erlang-22.3.2-1.el6.x86\_64.rpm: Header V4 RSA/SHA1 Signature, key ID 6026dfca: NOKEY  Preparing... ################################# [100%]  Updating / installing...  1:erlang-22.3.2-1.el6 ################################# [100%] |

## 2.2安装socat

|  |
| --- |
| rpm -ivh socat-1.7.3.2-2.el7.x86\_64.rpm  安装结果  Preparing... ################################# [100%]  Updating / installing...  1:socat-1.7.3.2-2.el7 ################################# [100%] |

## 2.3安装RabbitMQ

|  |
| --- |
| rpm -ivh rabbitmq-server-3.8.3-1.el7.noarch.rpm  安装结果  warning: rabbitmq-server-3.8.3-1.el7.noarch.rpm: Header V4 RSA/SHA256 Signature, key ID 6026dfca: NOKEY  Preparing... ################################# [100%]  Updating / installing...  1:rabbitmq-server-3.8.3-1.el7 ################################# [100%] |

## 2.4防火墙放行RabbitMQ端口

|  |
| --- |
| # 放行端口  firewall-cmd --zone=public --add-port=15672/tcp --permanent  # 更新规则  firewall-cmd --reload  # 验证  firewall-cmd --query-port=15672/tcp  说明：  –zone 作用域  –add-port=15672/tcp 添加端口，格式为：端口/通讯协议  –permanent #永久生效，没有此参数重启后失效 |

## 2.5启动RabbitMQ

|  |
| --- |
| # 放行端口  firewall-cmd --zone=public --add-port=15672/tcp --permanent  # 更新规则  firewall-cmd --reload  # 验证  firewall-cmd --query-port=15672/tcp  说明：  –zone 作用域  –add-port=15672/tcp 添加端口，格式为：端口/通讯协议  –permanent #永久生效，没有此参数重启后失效 |

### 2.5.1 启动

|  |
| --- |
| systemctl start rabbitmq-server |

### 2.5.2 配置rabbitmq管理账户

|  |
| --- |
| rabbitmqctl add\_user springcloud admin  结果如下：  Adding user "springcloud" ... |

### 2.5.3 执行命令 rabbitmqctl set\_user\_tags springcloudadministrator，设置springcloud为管理员权限

|  |
| --- |
| rabbitmqctl set\_user\_tags springcloud administrator  结果如下：  Setting tags for user "springcloud" to [administrator] ... |

### 2.5.4 执行命令 rabbitmq-plugins enable rabbitmq\_management，打开rabbitmq web管理

|  |
| --- |
| rabbitmq-plugins enable rabbitmq\_management  结果如下：  Enabling plugins on node rabbit@localhost:  rabbitmq\_management  The following plugins have been configured:  rabbitmq\_management  rabbitmq\_management\_agent  rabbitmq\_web\_dispatch  Applying plugin configuration to rabbit@localhost...  The following plugins have been enabled:  rabbitmq\_management  rabbitmq\_management\_agent  rabbitmq\_web\_dispatch  started 3 plugins. |

### 2.5.5 Chrome浏览器登陆管理端http://192.168.0.21:15672/，输入用户名和密码：

|  |
| --- |
|  |

|  |
| --- |
|  |

# 三、 安装JDK

## 3.1 解压

|  |
| --- |
| tar -zxvf jdk-8u251-linux-x64.tar.gz -C /usr/local  # 该软链接用于配置JAVA\_HOME  ln -s /usr/local/jdk1.8.0\_251/ /usr/local/jdk  # Logstash默认配置文件去 /usr/bin、/bin、/sbin、/usr/sbin，所以需要建立该软连接，若通过yum安装JDK则无需配置  ln -s /usr/local/jdk1.8.0\_251/bin/\* /bin |

## 3.2 配置环境

|  |
| --- |
| vi /etc/profile  #最后面添加以下配置文件  export JAVA\_HOME=/usr/local/jdk  export JRE\_HOME=$JAVA\_HOME/jre  export PATH=$PATH:$JAVA\_HOME/bin |

## 3.3 验证结果

|  |
| --- |
| source /etc/profile  java -version  #检查结果：  java version "1.8.0\_251"  Java(TM) SE Runtime Environment (build 1.8.0\_251-b08)  Java HotSpot(TM) 64-Bit Server VM (build 25.251-b08, mixed mode) |

# 四、 部署elasticsearch

## 4.1 rpm安装

|  |
| --- |
| cd /opt  rpm -ivh elasticsearch-7.6.2-x86\_64.rpm |

## 4.2 修改elasticsearch配置文件

### 4.2.1 vi /etc/elasticsearch/elasticsearch.yml

|  |
| --- |
| cd /etc/elasticsearch/  [root@localhost elasticsearch]# vi elasticsearch.yml  添加如下内容（也可以关闭并修改对应设置的注释）  node.name: node-1  path.data: /var/lib/elasticsearch  path.logs: /var/log/elasticsearch  network.host: 0.0.0.0  http.port: 9200  cluster.initial\_master\_nodes: ["node-1"]  http.cors.enabled: true  http.cors.allow-origin: "\*"  xpack.security.enabled: true  xpack.security.transport.ssl.enabled: true |

### 4.2.2 vi /etc/sysconfig/elasticsearch

|  |
| --- |
| JAVA\_HOME=/usr/local/jdk |

## 4.3 启动elasticsearch

|  |
| --- |
| systemctl start elasticsearch |

## 4.4 检查启动情况

### 4.4.1 查看启动状态

|  |
| --- |
| systemctl status elasticsearch    内容如下：  ● elasticsearch.service - Elasticsearch  Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; disabled; vendor preset: disabled)  Active: active (running) since Wed 2020-04-22 11:44:00 CST; 24s ago  Docs: http://www.elastic.co  Main PID: 17442 (java)  CGroup: /system.slice/elasticsearch.service  ├─17442 /usr/local/jdk/bin/java -Des.networkaddress.cache.ttl=60 -Des.networkaddress.cache.negative.ttl=10 -XX:+AlwaysPreTouch -Xss1m -Djava.awt.headless=true -Df...  └─17519 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86\_64/bin/controller  Apr 22 11:43:47 localhost.localdomain systemd[1]: Starting Elasticsearch...  Apr 22 11:43:47 localhost.localdomain elasticsearch[17442]: future versions of Elasticsearch will require Java 11; your Java version from [/usr/local/jdk1.8.0\_251/j...quirement  Apr 22 11:44:00 localhost.localdomain systemd[1]: Started Elasticsearch.  Hint: Some lines were ellipsized, use -l to show in full. |

### 4.4.2 查看启动日志

|  |
| --- |
| cd /var/log/elasticsearch/  tail -f elasticsearch.log  内容如下：  [2020-04-22T12:58:25,611][INFO ][o.e.h.AbstractHttpServerTransport] [node-1] publish\_address {192.168.0.21:9200}, bound\_addresses {[::]:9200}  [2020-04-22T12:58:25,612][INFO ][o.e.n.Node ] [node-1] started  [2020-04-22T12:58:25,777][INFO ][o.e.l.LicenseService ] [node-1] license [ae42aa65-0097-48dc-b18b-5a43a86dbe7f] mode [basic] - valid  [2020-04-22T12:58:25,777][INFO ][o.e.x.s.s.SecurityStatusChangeListener] [node-1] Active license is now [BASIC]; Security is enabled  [2020-04-22T12:58:25,787][INFO ][o.e.g.GatewayService ] [node-1] recovered [0] indices into cluster\_state |

### 4.4.3 防火墙放行Elastic Search 9200端口

|  |
| --- |
| # 放行端口  firewall-cmd --zone=public --add-port=9200/tcp --permanent  # 更新规则  firewall-cmd --reload  # 验证  firewall-cmd --query-port=9200/tcp  说明：  –zone 作用域  –add-port=9200/tcp 添加端口，格式为：端口/通讯协议  –permanent #永久生效，没有此参数重启后失效 |

### 4.4.4 设置用户名和密码

|  |
| --- |
| cd /usr/share/elasticsearch/bin/  ./elasticsearch-setup-passwords interactive  future versions of Elasticsearch will require Java 11; your Java version from [/usr/local/jdk1.8.0\_251/jre] does not meet this requirement  Initiating the setup of passwords for reserved users elastic,apm\_system,kibana,logstash\_system,beats\_system,remote\_monitoring\_user.  You will be prompted to enter passwords as the process progresses.  Please confirm that you would like to continue [y/N]y  输入需要设置的密码，密码需要全部设置：  Enter password for [elastic]:  Reenter password for [elastic]:  Enter password for [elastic]:  Reenter password for [elastic]:  Enter password for [apm\_system]:  Reenter password for [apm\_system]:  Enter password for [kibana]:  Reenter password for [kibana]:  Enter password for [logstash\_system]:  Reenter password for [logstash\_system]:  Enter password for [beats\_system]:  Reenter password for [beats\_system]:  Enter password for [remote\_monitoring\_user]:  Reenter password for [remote\_monitoring\_user]:  Changed password for user [apm\_system]  Changed password for user [kibana]  Changed password for user [logstash\_system]  Changed password for user [beats\_system]  Changed password for user [remote\_monitoring\_user]  Changed password for user [elastic] |

### 4.4.5 登录测试打开浏览器访问：http://192.168.0.21:9200，IP和端口是虚拟的地址，返回如下地址表示访问成功；

|  |
| --- |
| cd /usr/share/elasticsearch/bin/  ./elasticsearch-setup-passwords interactive  future versions of Elasticsearch will require Java 11; your Java version from [/usr/local/jdk1.8.0\_251/jre] does not meet this requirement  Initiating the setup of passwords for reserved users elastic,apm\_system,kibana,logstash\_system,beats\_system,remote\_monitoring\_user.  You will be prompted to enter passwords as the process progresses.  Please confirm that you would like to continue [y/N]y  输入需要设置的密码，密码需要全部设置：  Enter password for [elastic]:  Reenter password for [elastic]:  Enter password for [elastic]:  Reenter password for [elastic]:  Enter password for [apm\_system]:  Reenter password for [apm\_system]:  Enter password for [kibana]:  Reenter password for [kibana]:  Enter password for [logstash\_system]:  Reenter password for [logstash\_system]:  Enter password for [beats\_system]:  Reenter password for [beats\_system]:  Enter password for [remote\_monitoring\_user]:  Reenter password for [remote\_monitoring\_user]:  Changed password for user [apm\_system]  Changed password for user [kibana]  Changed password for user [logstash\_system]  Changed password for user [beats\_system]  Changed password for user [remote\_monitoring\_user]  Changed password for user [elastic] |

### 4.4.6 Chrome浏览器安装Elastic Search Head 插件

(1) Elastic Search Head是监控Elastic Search状态的插件，打开电脑上Chrome浏览器的扩展程序页面

|  |
| --- |
|  |

(2) 将安装包中的“chrome-extention-elastic-search-head-0.1.5.crx”，拖动到Chrome扩展程序页面，选择“添加扩展程序，

|  |
| --- |
|  |

(3)安装成功后会在Chrome扩展程序栏看到 Elastic Search Head的图标""，点击图标，出现如下页面

|  |
| --- |
|  |

(4) 输入虚拟机IP和端口如http://192.168.0.21:9200，然后点击连接按钮，并输入用户名elastic，密码是步骤4.3所设置的密码，可以看到当前Elastic Searchd的状态：

|  |
| --- |
|  |

# 五、 部署kibana

## 5.1 rpm安装

|  |
| --- |
| cd /opt  rpm -ivh kibana-7.6.2-x86\_64.rpm  安装结果  warning: kibana-7.6.2-x86\_64.rpm: Header V4 RSA/SHA512 Signature, key ID d88e42b4: NOKEY  Preparing... ################################# [100%]  Updating / installing...  1:kibana-7.6.2-1 ################################# [100%] |

## 5.2 修改配置文件

|  |
| --- |
| [root@localhost bin]# vi /etc/kibana/kibana.yml  添加如下内容（也可以关闭并修改对应设置的注释），Elastic Search用户名和密码按步骤4.3设置  server.port: 5601  server.host: "0"  xpack.monitoring.ui.container.elasticsearch.enabled: true  # 设置Kibana界面为中文  i18n.locale: "zh-CN"  ## X-Pack security credentials  elasticsearch.username: elastic  elasticsearch.password: elk654123 |

## 5.3 防火墙放行Kibana 5601端口

|  |
| --- |
| # 放行端口  firewall-cmd --zone=public --add-port=5601/tcp --permanent  # 更新规则  firewall-cmd --reload  # 验证  firewall-cmd --query-port=5601/tcp  说明：  –zone 作用域  –add-port=9200/tcp 添加端口，格式为：端口/通讯协议  –permanent #永久生效，没有此参数重启后失效 |

## 5.4 启动kibana

|  |
| --- |
| systemctl start kibana |

## 5.5 访问测试(默认端口为5601)

在Chrome浏览器中输入http://192.168.0.21:5601/，输入步骤4.3设置的Elastic Search用户名和密码

|  |
| --- |
|  |

# 六、部署logstash

## 6.1 rpm安装

|  |
| --- |
| cd /opt  rpm -ivh logstash-7.6.2.rpm  安装结果  warning: logstash-7.6.2.rpm: Header V4 RSA/SHA512 Signature, key ID d88e42b4: NOKEY  Preparing... ################################# [100%]  Updating / installing...  1:logstash-1:7.6.2-1 ################################# [100%]  Using provided startup.options file: /etc/logstash/startup.options  /usr/share/logstash/vendor/bundle/jruby/2.5.0/gems/pleaserun-0.0.30/lib/pleaserun/platform/base.rb:112:  warning: constant ::Fixnum is deprecated  Successfully created system startup script for Logstash |

## 6.2 修改和配置文件

|  |
| --- |
| mkdir -p /usr/share/logstash/config  cp /etc/logstash/log4j2.properties /usr/share/logstash/config  [root@localhost logstash]# vi /etc/logstash/logstash.yml  添加如下内容（也可以关闭并修改对应设置的注释），  node.name: logstash  path.data: /var/lib/logstash  path.config: /etc/logstash/conf.d  path.logs: /var/log/logstash |

## 6.3 编写Logstash配置文件logstash.conf

### 6.3.1 将安装包中的"logstash.conf"复制到在/etc/logstash/conf.d目录下

|  |
| --- |
| cp /opt/logstash.conf /etc/logstash/conf.d/ |

### 6.3.2 测试配置文件编写，正式环境需要移除该文件：

(1) 新建测试用的test.conf，内容如下，请修改elasticsearch的hosts，user，password内容：

|  |
| --- |
| input {  stdin {  }  }  output {  elasticsearch {  hosts =>["192.168.0.21:9200"]  index => "test-%{+YYYY.MM.dd}"  user => elastic  password => "elk654123"  }  stdout {  codec => rubydebug  }  } |

(2) 启动命令为 ：

|  |
| --- |
| /usr/share/logstash/bin/logstash -f /etc/logstash/conf.d/test.conf |

(3) 启动后在控制台输入"hello, elk"和"hi, logstash"：

|  |
| --- |
| hello, elk  {  "message" => "hello, elk",  "host" => "localhost.localdomain",  "@timestamp" => 2020-04-22T07:04:15.274Z,  "@version" => "1"  }  hi, logstash  {  "message" => "hi, logstash",  "host" => "localhost.localdomain",  "@timestamp" => 2020-04-22T07:04:25.761Z,  "@version" => "1"  } |

(4) 打开Kibana界面，如<http://192.168.0.21:5601/>，点击侧边栏的“Dicover”按钮，可以看到测试数据：

|  |
| --- |
|  |

(5) 在Kibana中创建索引:

|  |
| --- |
|  |

(6) 完成后点击侧边栏Discover，可以看到对应的数据 :

|  |
| --- |
|  |

### 6.3.3 正式环境的logstash.conf,  修改对应input插件中RabbitMQ的host，user，password以及output插件中Elastic Search的hosts，user和passwod ：

|  |
| --- |
| input {  rabbitmq {  host => "your rabbitmq host"  port => 5672  user => "your rabbitmq username"  password => "your rabbitmq password"  queue => "logDirectQueue"  durable=> true  codec => json  }  }  filter {  json {  source => "message" # 指定json格式字段，也就是message字段  remove\_field => "message" # message已被解析为各个字段，不再需要，所以删掉  }  }  output {  elasticsearch {  hosts => "your elasticsearch hosts"  user => "your elasticsearch username"  password => "your elasticsearch username"  index => "sdms\_log-%{+YYYY-MM-dd}" # 自定义索引名称  }  stdout {}  } |

## 6.4 启动运行

|  |
| --- |
| systemctl start logstash |