ELK集群搭建手册

1. 环境准备

三台Linux服务器，ip地址分别为：

192.168.25.30

192.168.25.31

192.168.25.32

角色划分：

3台机器全部安装jdk1.8，因为elasticsearch是java开发的

3台全部安装elasticsearch (后续都简称为es)

192.168.25.30作为主节点

192.168.25.31以及192.168.25.32作为数据节点

主节点上需要安装kibana

在192.168.77.130上安装 logstash

ELK版本信息：

Elasticsearch-6.4.2

logstash-6.4.2

kibana-6.4.2

filebeat-6.4.2

配置三台机器的hosts文件内容如下：

$ vim /etc/hosts

192.168.25.30 data-node-0

192.168.25.31 data-node-1

192.168.25.32 data-node-2

然后三台机器都得关闭防火墙或清空防火墙规则。

1. 安装java环境

|  |
| --- |
| 安装包版本：jdk-8u25-linux-x64.tar.gz  #tar -zxvf jdk-8u25-linux-x64.tar.gz  #cd jdk1.8.0\_25/  #mkdir –p /app/jdk  #cp -r ../jdk1.8.0\_25 /app/jdk  #vim /etc/profile  在最后插入如下几行：  export JAVA\_HOME=/app/jdk/jdk1.8.0\_25  export PATH=$JAVA\_HOME/bin:$JAVA\_HOME/jre/bin:$PATH:$HOME/bin  export CLASSPATH=.:$JAVA\_HOME/lib/dt.jar:$JAVA\_HOME/jre/lib/tools.jar  检查安装情况：  # source /etc/profile  # java –version  java version "1.8.0\_25"  Java(TM) SE Runtime Environment (build 1.8.0\_25-b17)  Java HotSpot(TM) 64-Bit Server VM (build 25.25-b02, mixed mode)  #javac  Usage: javac <options> <source files>  where possible options include:  -g Generate all debugging info  -g:none Generate no debugging info  -g:{lines,vars,source} Generate only some debugging info  -nowarn Generate no warnings  -verbose Output messages about what the compiler is doing  -deprecation Output source locations where deprecated APIs are used  -classpath <path> Specify where to find user class files and annotation processors  -cp <path> Specify where to find user class files and annotation processors  -sourcepath <path> Specify where to find input source files  -bootclasspath <path> Override location of bootstrap class files  -extdirs <dirs> Override location of installed extensions  -endorseddirs <dirs> Override location of endorsed standards path  -proc:{none,only} Control whether annotation processing and/or compilation is done.  -processor <class1>[,<class2>,<class3>...] Names of the annotation processors to run; bypasses default discovery process  -processorpath <path> Specify where to find annotation processors  -parameters Generate metadata for reflection on method parameters  -d <directory> Specify where to place generated class files  -s <directory> Specify where to place generated source files  -h <directory> Specify where to place generated native header files  -implicit:{none,class} Specify whether or not to generate class files for implicitly referenced files  -encoding <encoding> Specify character encoding used by source files  -source <release> Provide source compatibility with specified release  -target <release> Generate class files for specific VM version  -profile <profile> Check that API used is available in the specified profile  -version Version information  -help Print a synopsis of standard options  -Akey[=value] Options to pass to annotation processors  -X Print a synopsis of nonstandard options  -J<flag> Pass <flag> directly to the runtime system  -Werror Terminate compilation if warnings occur  @<filename> Read options and filenames from file |

安装java成功

1. 安装Elasticsearch

|  |
| --- |
| 安装ES：  下载安装包elasticsearch-6.4.2.rpm  <https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-6.4.2.rpm>  #wget –O /app/elasticsearch-6.4.2.rpm <https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-6.4.2.rpm>  #cd /app  #rpm -ivh elasticsearch-6.4.2.rpm  warning: elasticsearch-6.4.2.rpm: Header V4 RSA/SHA512 Signature, key ID d88e42b4: NOKEY  Preparing... ################################# [100%]  Creating elasticsearch group... OK  Creating elasticsearch user... OK  Updating / installing...  1:elasticsearch-0:6.4.2-1 ################################# [100%]  ### NOT starting on installation, please execute the following statements to configure elasticsearch service to start automatically using systemd  sudo systemctl daemon-reload  sudo systemctl enable elasticsearch.service  ### You can start elasticsearch service by executing  sudo systemctl start elasticsearch.service  Created elasticsearch keystore in /etc/elasticsearch  配置ES：  elasticsearch配置文件在/etc/elasticsearch/下和/etc/sysconfig/elasticsearch这个文件，其中elasticsearch.yml 文件用于配置集群节点等相关信息的，elasticsearch 文件则是配置服务本身相关的配置，例如某个配置文件的路径以及java的一些路径配置什么的。  # cd /etc/elasticsearch/  # ll  total 28  -rw-rw---- 1 root elasticsearch 207 Nov 5 11:48 elasticsearch.keystore  -rw-rw---- 1 root elasticsearch 2869 Sep 26 21:39 elasticsearch.yml  -rw-rw---- 1 root elasticsearch 3009 Sep 26 21:39 jvm.options  -rw-rw---- 1 root elasticsearch 6380 Sep 26 21:39 log4j2.properties  -rw-rw---- 1 root elasticsearch 473 Sep 26 21:39 role\_mapping.yml  -rw-rw---- 1 root elasticsearch 197 Sep 26 21:39 roles.yml  -rw-rw---- 1 root elasticsearch 0 Sep 26 21:39 users  -rw-rw---- 1 root elasticsearch 0 Sep 26 21:39 users\_roles  # ll /etc/sysconfig/elasticsearch  -rw-rw---- 1 root elasticsearch 1613 Sep 26 21:39 /etc/sysconfig/elasticsearch  在每个节点上创建数据data和logs目录：  #mkdir -p /app/elk/elasticsearch/data  #mkdir -p /app/elk/elasticsearch/logs  #chown -R elasticsearch /app/elk/elasticsearch/  开始配置集群节点，在主节点 192.168.25.30 上编辑配置文件：  # vim /etc/elasticsearch/elasticsearch.yml  添加或修改以下内容（没有的增加，存在的修改）：  path.data: /app/elk/elasticsearch/data  path.logs: /app/elk/elasticsearch/logs  cluster.name: elk-test # 集群中的名称  node.name: data-node-0 # 该节点名称  node.master: true # 意思是该节点是否可选举为主节点  node.data: true # 表示这不是数据节点  network.host: 0.0.0.0 # 监听全部ip，在实际环境中应为一个安全的ip  http.port: 9200 # es服务的端口号  discovery.zen.ping.unicast.hosts: ["192.168.25.30", "192.168.25.31", "192.168.25.32"] # 配置自动发现  然后在从节点192.168.25.31、32上编辑配置文件，添加或修改如下内容：  path.data: /app/elk/elasticsearch/data  path.logs: /app/elk/elasticsearch/logs  cluster.name: elk-test # 集群中的名称  node.name: data-node-? # 该节点名称，与前面配置hosts保持一致  node.master: true # 意思是该节点是否可选举为主节点  node.data: true # 表示这不是数据节点  network.host: 0.0.0.0 # 监听全部ip，在实际环境中应为一个安全的ip  http.port: 9200 # es服务的端口号  discovery.zen.ping.unicast.hosts: ["192.168.25.30", "192.168.25.31", "192.168.25.32"] # 配置自动发现  修改 /etc/sysconfig/elasticsearch中的java路径  # vim /etc/sysconfig/elasticsearch  JAVA\_HOME=/app/jdk/jdk1.8.0\_25  完成以上的配置之后，到主节点上，启动es服务, 主节点启动完成之后，再启动其他节点的es服务:  # systemctl start elasticsearch.service  # systemctl status elasticsearch.service  ● elasticsearch.service - Elasticsearch  Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; disabled; vendor preset: disabled)  Active: active (running) since Mon 2018-11-05 14:30:56 CST; 2s ago  Docs: http://www.elastic.co  Main PID: 522372 (java)  CGroup: /system.slice/elasticsearch.service  ├─522372 /app/jdk/jdk1.8.0\_25/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupancyFraction=75 -XX:+UseCMSInitiatingOccupancyOnly -XX:+AlwaysPreTouch -Xss1m -...  └─522574 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86\_64/bin/controller  Nov 05 14:30:56 cnsz22pl1030 systemd[1]: Started Elasticsearch.  Nov 05 14:30:56 cnsz22pl1030 systemd[1]: Starting Elasticsearch...  安装成功  检查安装好的集群健康状态：  # curl '192.168.25.30:9200/\_cluster/health?pretty'  {  "cluster\_name" : "master-node",  "status" : "green",  "timed\_out" : false,  "number\_of\_nodes" : 3,  "number\_of\_data\_nodes" : 2,  "active\_primary\_shards" : 0,  "active\_shards" : 0,  "relocating\_shards" : 0,  "initializing\_shards" : 0,  "unassigned\_shards" : 0,  "delayed\_unassigned\_shards" : 0,  "number\_of\_pending\_tasks" : 0,  "number\_of\_in\_flight\_fetch" : 0,  "task\_max\_waiting\_in\_queue\_millis" : 0,  "active\_shards\_percent\_as\_number" : 100.0  }  查看集群的详细信息：  # curl '192.168.25.30:9200/\_cluster/state?pretty' |

1. 安装kibana

|  |
| --- |
| Kibana只需要在主节点192.168.25.30上安装即可，由于kibana是使用node.js开发的，所以进程名称为node。  下载RPM安装包：kibana-6.4.2-x86\_64.rpm  下载地址：<https://artifacts.elastic.co/downloads/kibana/kibana-6.4.2-x86_64.rpm>  如果主机可以上外网，也可以执行以下命令：  #wget –O /app/ kibana-6.4.2-x86\_64.rpm <https://artifacts.elastic.co/downloads/kibana/kibana-6.4.2-x86_64.rpm>  # cd /app  # rpm -ivh kibana-6.4.2-x86\_64.rpm  warning: kibana-6.4.2-x86\_64.rpm: Header V4 RSA/SHA512 Signature, key ID d88e42b4: NOKEY  Preparing... ################################# [100%]  Updating / installing...  1:kibana-6.4.2-1 ################################# [100%]  配置kibana  # vim /etc/kibana/kibana.yml  添加或修改如下项：  server.port: 5601 # 配置kibana的端口  server.host: 192.168.25.30 # 配置监听ip  elasticsearch.url: "http://192.168.25.30:9200" # 配置es服务器的ip，如果是集群则配置该集群中主节点的ip  logging.dest: /var/log/kibana.log # 配置kibana的日志文件路径，不然默认是messages里记录日志  由于我们配置了日志路径，所以需要创建日志文件：  # touch /var/log/kibana.log  # chmod 777 /var/log/kibana.log  启动kibana服务，并检查进程和监听端口：  **# systemctl start kibana**  **# systemctl status kibana**  ● kibana.service - Kibana  Loaded: loaded (/etc/systemd/system/kibana.service; disabled; vendor preset: disabled)  Active: active (running) since Mon 2018-11-05 15:09:00 CST; 4s ago  Main PID: 146989 (node)  CGroup: /system.slice/kibana.service  └─146989 /usr/share/kibana/bin/../node/bin/node --no-warnings /usr/share/kibana/bin/../src/cli -c /etc/kibana/kibana.yml  Nov 05 15:09:00 cnsz22pl1030 systemd[1]: Started Kibana.  Nov 05 15:09:00 cnsz22pl1030 systemd[1]: Starting Kibana...  **# ps aux |grep kibana**  kibana 146989 47.0 0.0 1349520 269736 ? Ssl 15:09 0:29 /usr/share/kibana/bin/../node/bin/node --no-warnings /usr/share/kibana/bin/../src/cli -c /etc/kibana/kibana.yml  root 150923 0.0 0.0 112644 952 pts/1 R+ 15:10 0:00 grep --color=auto kibana  **#netstat -lntp |grep 5601**  tcp 0 0 127.0.0.1:5601 0.0.0.0:\* LISTEN 146989/node |

到此我们的kibana就安装完成了，很简单，接下来就是安装logstash，不然kibana是没法用的。

1. 安装logstash

|  |
| --- |
| 在192.168.25.31上安装logstash，注意目前logstash不支持JDK1.9：  下载RPM安装包logstash-6.4.2.rpm，下载地址如下：  <https://artifacts.elastic.co/downloads/logstash/logstash-6.4.2.rpm>  如果主机支持外网，可直接执行以下命令下载：  wget –O /app/ logstash-6.4.2.rpm <https://artifacts.elastic.co/downloads/logstash/logstash-6.4.2.rpm>  **# rpm -ivh logstash-6.4.2.rpm**  warning: logstash-6.4.2.rpm: Header V4 RSA/SHA512 Signature, key ID d88e42b4: NOKEY  Preparing... ################################# [100%]  Updating / installing...  1:logstash-1:6.4.2-1 ################################# [100%]  Using provided startup.options file: /etc/logstash/startup.options  Successfully created system startup script for Logstash  修改环境变量  # vim /etc/default/logstash  添加以下项：  JAVA\_HOME=/app/jdk/jdk1.8.0\_25  修改日志存储路径：  #mkdir -p /app/elk/logstash/data  #mkdir -p /app/elk/logstash/logs  #chown -R logstash /app/elk/logstash/  修改配置文件  **# vim /etc/logstash/logstash.yml**  将如下项的值修改为如下：  path.data: /app/elk/logstash/data  http.host: "192.168.25.31"  path.logs: /app/elk/logstash/logs  #  安装完之后，先不要启动服务，先配置logstash收集syslog日志：  #vim /etc/logstash/conf.d/syslog.conf  加入如下内容：  input { # 定义日志源  syslog {  type => "system-syslog" # 定义类型  port => 10514 # 定义监听端口  }  }  output { # 定义日志输出  elasticsearch {  hosts => ["192.168.25.30:9200","192.168.25.31:9200","192.168.25.32:9200"] # 定义es服务器的ip  index => "system-syslog-%{+YYYY.MM.dd}" # 定义索引  }  }  检测配置文件是否有错：  **# cd /usr/share/logstash/bin**  **# ./logstash --path.settings /etc/logstash/ -f /etc/logstash/conf.d/syslog.conf --config.test\_and\_exit**  Sending Logstash logs to /var/log/logstash which is now configured via log4j2.properties  [2018-11-05T16:20:07,997][WARN ][logstash.config.source.multilocal] Ignoring the 'pipelines.yml' file because modules or command line options are specified  Configuration OK  [2018-11-05T16:20:09,448][INFO ][logstash.runner ] Using config.test\_and\_exit mode. Config Validation Result: OK. Exiting Logstash  Configuration OK # 为ok则代表配置文件没有问题  命令说明：   * --path.settings 用于指定logstash的配置文件所在的目录 * -f 指定需要被检测的配置文件的路径 * --config.test\_and\_exit 指定检测完之后就退出，不然就会直接启动了   配置logstash服务器的ip以及配置的监听端口：  # vim /etc/rsyslog.conf  #### RULES ####  \*.\* @@192.168.25.31:10514  重启rsyslog，让配置生效：  # systemctl restart rsyslog  启动logstash并检查服务状态：  # systemctl start logstash  # systemctl status logstash |

1. 安装filebeats

|  |
| --- |
| 在192.168.25.32上安装filebeat。  下载RPM包filebeat-6.4.2-x86\_64.rpm，下载地址：  <https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-6.4.2-x86_64.rpm>  如果安装的主机可以直接上外网，也可以使用如下命令下载：  wget –O /app/filebeat-6.4.2-x86\_64.rpm <https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-6.4.2-x86_64.rpm>  下载完成执行命令安装  **#rpm -ivh filebeat-6.4.2-x86\_64.rpm**  warning: filebeat-6.4.2-x86\_64.rpm: Header V4 RSA/SHA512 Signature, key ID d88e42b4: NOKEY  Preparing... ################################# [100%]  Updating / installing...  1:filebeat-6.4.2-1 ################################# [100%]  安装完成后编辑配置文件：  # vim /etc/filebeat/filebeat.yml  filebeat.inputs:  - type: log  # Change to true to enable this input configuration.  enabled: true  paths:  - /var/log/\*.log  #================== Kibana=====================================  setup.kibana:  host: "192.168.25.30:5601"  #==================== Outputs =================================  # Configure what output to use when sending the data collected by the beat.  #-------------------------- Elasticsearch output ------------------------------  output.elasticsearch:  # Array of hosts to connect to.  hosts: ["192.168.25.30:9200","192.168.25.31:9200","192.168.25.32:9200"]  以下配置可选，根据实际需要配置  #----------------------------- Logstash output --------------------------------  #output.logstash:  # The Logstash hosts  #hosts: ["192.168.25.31:5044"]  启动服务：  #systemctl start filebeat.service  查看服务启动状态  #systemctl status filebeat.service  查看elasticsearch  **# curl '192.168.25.30:9200/\_cat/indices?v'**  health status index uuid pri rep docs.count docs.deleted store.size pri.store.size  green open system-syslogs-2018.11.06 9-WQSrX7Su2FeORk5XM5-w 5 1 614 0 924.1kb 406.5kb  green open filebeat-6.4.2-2018.11.06 gYOcxCK8THaJ57AWAUbK3Q 3 1 8039 0 2.7mb 1.3mb |