链滴

ELK（一）：elk5.5+redis+logback

作者：zengxiaoyun

原文链接：https://ld246.com/article/1503473687098

来源网站：链滴

一、环境准备

1. vim /etc/security/limits.conf

```
* soft nofile 65536
* hard nofile 65536
* soft nproc 2048
* hard nproc 4096
```

2. vim /etc/security/limits.d/20-nproc.conf

```
* soft nproc 4096
```

3. vim /etc/sysctl.conf

```
vm.max_map_count=655360
fs.file-max=655360
```

保存之后执行 sysctl -p 生效

4. vim /etc/profile

```
ulimit -n 65536
```

保存之后执行 source /etc/profile 生效

5. jdk1.8安装（过程略，必须1.8+）

6. elk5.5.1安装包下载

```
wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-5.5.1.tar.gz
wget https://artifacts.elastic.co/downloads/kibana/kibana-5.5.1-linux-x86_64.tar.gz
wget https://artifacts.elastic.co/downloads/logstash/logstash-5.5.1.tar.gz
```

==xxxxxxxxxxxxxxxxxxxx 以上完成之后，reboot重启机器 xxxxxxxxxxxxxxxxxxxx==

二、机器规划

#1台redis和logstash

- 192.168.254.210

#3台elasticsearch

- 192.168.254.208 es-node-1 master
- 192.168.254.209 es-node-2
- 192.168.254.213 es-node-3

#1台kibana

- 192.168.254.213

三、elasticsearch安装

1. 安装/配置/启动

```
#建立目录
mkdir -p /opt/app/es
mkdir -p /opt/data/es
mkdir -p /opt/logs/es

#解压
tar -zxvf elasticsearch-5.5.1.tar.gz
mv elasticsearch-5.5.1/* /opt/app/es/

#建立用户并授权(es不能用root运行)
useradd es
chown -R es:es /opt/app/es
chown -R es:es /opt/data/es
chown -R es:es /opt/logs/es

#修改配置文件
su - es
cd /opt/app/es/config

vim elasticsearch.yml
#------------------------------------
cluster.name: es-cluster      #集群名称，必须相同
node.name: es-node-1          #节点名称，必须唯一
node.master: true             #可作为主节点
node.data: true               #存储数据
path.data: /opt/data/es       #数据目录
path.logs: /opt/logs/es       #日志目录
network.host: 192.168.254.208 #绑定IP
http.port: 9201               #绑定端口
http.cors.enabled: true       #允许跨域访问，head使用
http.cors.allow-origin: "*"   #允许跨域访问，head使用
discovery.zen.ping.unicast.hosts: ["192.168.254.209", "192.168.254.213"] #其他2个节点IP
discovery.zen.minimum_master_nodes: 2 #最少需X个节点正常整个集群才正常

vim jvm.options
#------------------------------------
-Xms4g  #内存调整为机器的内存的一半
-Xmx4g


#启动es
../bin/elasticseach -d
```

2. 验证安装结果

```
curl -XGET http://192.168.254.208:9200/_cluster/health?pretty
#返回结果
{
  "cluster_name" : "es-cluster",
  "status" : "green",
  "timed_out" : false,
  "number_of_nodes" : 3,
  "number_of_data_nodes" : 3,
  "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
}
#检查集群健康状态
curl 'http://192.168.254.208:9200/_cat/health?v'
#检查集群的节点
curl 'http://192.168.254.208:9200/_cat/nodes?v'
#显示所有的index
curl 'http://192.168.254.208:9200/_cat/indices?v'
```

四、kibana安装

1. 解压安装

```
tar -zxvf kibana-5.5.1-linux-x86_64.tar.gz
mv kibana-5.5.1-linux-x86_64 /opt/app/
cd /opt/app/
mv kibana-5.5.1-linux-x86_64 kibana
```

2. 配置启动

```
vim config/kibana.yml
#------------------------------------
server.port: 5601
server.host: "192.168.254.213"
elasticsearch.url: "http://192.168.254.208:9200"

#启动
su - es
nohup /opt/app/kibana/bin/kibana serve -l /opt/logs/kibana/kibana.log >/dev/null 2>&1 &
```

3. 验证安装

浏览器打开：http://192.168.254.213

五、redis安装

```
tar -zxvf redis-3.2.10.tar.gz
cd redis-3.2.10
make
make install PREFIX=/opt/app/redis
cp /opt/install/redis-3.2.10/redis.conf /opt/app/redis/
cd /opt/app/redis
mv redis.conf common.conf

vim redis.conf
#-------------------------------------
#引入通用配置
include /opt/app/redis/common.conf
#绑定IP
bind 0.0.0.0
#后台运行
daemonize yes
#日志文件
logfile "/opt/logs/redis/redis.log"
#存储目录
dir /opt/data/redis/
#关闭rdb
save ""
#rdb文件名
dbfilename dump.rdb
#关闭aof
appendonly no
#aof文件名
appendfilename "appendonly.aof"
#最大内存12G，内存的3/4
maxmemory 12582912
#过期策略
maxmemory-policy volatile-lru
#取样数
maxmemory-samples 5

#启动
mkdir -p /opt/logs/redis
mkdir -p /opt/data/redis
/opt/app/redis/bin/redis-server /opt/app/redis/redis.conf
```

六、logstash安装

1. 安装&测试

```
#解压安装
tar -zxvf logstash-5.5.1.tar.gz
mv logstash-5.5.1 /opt/app/
cd /opt/app/
mv logstash-5.5.1 logstash
```

```
#配置
cd logstash/config/
vim logstash.yml
#-------------------------------------
path.logs: /opt/logs/logstash
path.data: /opt/data/logstash

#在config目录下建立测试配置
cd config
vi my-test.conf
#-------------------------------------
input { stdin { } }
output {
  elasticsearch {
    hosts => ["192.168.254.208:9200"]
  }
  stdout {
    codec => rubydebug
  }
}
#启动
../bin/logstash -f my-test.conf --debug
#启动后输入任意字符串，在kibana中查看（第一次需在kibana页面中建立索引）
http://192.168.254.213:5601
```

2. logstash + redis模式配置

```
#配置
vim my-redis.conf
#-------------------------------------
input {
  redis {
    data_type => "list"
    key => "logstash"
    host => "192.168.254.210"
    port => 6379
    threads => 5
    codec => "json"
  }
}
filter {
}
output {
  elasticsearch {
    hosts => ["192.168.254.208:9200", "192.168.254.209:9200", "192.168.254.213:9200"]
    index => "logstash-%{type}-%{+YYYY.MM.dd}"
    document_type => "%{type}"
    #workers => 4
    flush_size => 5000
    idle_flush_time => 2
    #template_overwrite => true
  }
  stdout {
  }
```

```
}


#启动（后台方式）
nohup /opt/app/logstash/bin/logstash -f /opt/app/logstash/config/my-redis.conf >/dev/null
>&1 &
#单机启动多个实例
nohup /opt/app/logstash/bin/logstash --node.name logstash1 --path.data /opt/data/logstas
1 --path.logs /opt/logs/logstash1 --path.config /opt/app/logstash/config/my-redis.conf >/de
/null 2>&1 &
nohup /opt/app/logstash/bin/logstash --node.name logstash3 --path.data /opt/data/logstas
2 --path.logs /opt/logs/logstash2 --path.config /opt/app/logstash/config/my-redis.conf >/de
/null 2>&1 &
nohup /opt/app/logstash/bin/logstash --node.name logstash3 --path.data /opt/data/logstas
3 --path.logs /opt/logs/logstash3 --path.config /opt/app/logstash/config/my-redis.conf >/de
/null 2>&1 &
```

七、集成logback -> redis模式

1. maven引入jar

```
<dependency>
    <groupId>com.cwbase</groupId>
    <artifactId>logback-redis-appender</artifactId>
    <version>1.1.3</version>
    <exclusions>
        <exclusion>
            <groupId>redis.clients</groupId>
            artifactId>jedis</artifactId>
        </exclusion>
    </exclusions>
</dependency>
```

2. 修改logback.xml

```
<appender name="STASH-REDIS" class="com.cwbase.logback.RedisAppender">
    <!-- 项目节点（这里取节点名称，唯一） -->
    <source>info-provider-1</source>
    <!-- 类型（这里取大项目名称，以便为每个大项目建立索引文件） -->
    <type>info</type>
    <!-- 标记（这里取dev/ci/test/prod环境标识） -->
    <tags>dev</tags>
    <!-- redis地址 -->
    <host>192.168.254.210</host>
    <!-- redis端口 -->
    <port>6379</port>
    <!-- redis键 -->
    <key>logstash</key>
    <mdc>true</mdc>
    <location>true</location>
    <callerStackIndex>0</callerStackIndex>
</appender>
```

```
<appender name="ASYNC" class="ch.qos.logback.classic.AsyncAppender">
    <!-- 不丢失日志.默认的,如果队列的80%已满,则会丢弃TRACT、DEBUG、INFO级别的日志 -->
    <discardingThreshold >0</discardingThreshold>
    <!-- 更改默认的队列的深度,该值会影响性能.默认值为256 -->
    <queueSize>512</queueSize>
    <appender-ref ref="STASH-REDIS" />
</appender>
<root level="DEBUG">
    <appender-ref ref="ASYNC" />
</root>
```

3. 启动项目查看日志是否收集到elk