

安装 elasticsearch

版本: v1.0

www.atguigu.com

1 安装包下载

Elasticsearch 官网: <https://www.elastic.co/products/elasticsearch>

<https://www.elastic.co/downloads/past-releases/elasticsearch-5-6-4>

本课程选择的版本是 elasticsearch-5.6.4



下载好后放到/opt/目录下

2 安装 elasticsearch

拷贝 elasticsearch-5.6.4.rpm 到/opt 目录下

```
[root@jack opt]# rpm -ivh elasticsearch-5.6.4.rpm
warning: elasticsearch-5.6.4.rpm: Header V4 RSA/SHA512 Signature, key ID d88e42b4: NOKEY
Preparing... ##### [100%]
Creating elasticsearch group... OK
Creating elasticsearch user... OK
   1:elasticsearch ##### [100%]
### NOT starting on installation, please execute the following statements to configure elasti
sudo chkconfig --add elasticsearch
### You can start elasticsearch service by executing
sudo service elasticsearch start
```

2.1 注册并启动服务

```
[root@jack opt]# cd /etc/init.d
[root@jack init.d]# ll
总用量 408
-rwxr-xr-x. 1 root root 1288 5月 12 2016 abrt-ccpp
-rwxr-xr-x. 1 root root 1628 5月 12 2016 abrtcd
-rwxr-xr-x. 1 root root 1642 5月 12 2016 abrt-oops
-rwxr-xr-x. 1 root root 1818 2月 17 2016 acpid
-rwxr-xr-x. 1 root root 2062 2月 20 2015 atd
-rwxr-xr-x. 1 root root 3580 5月 11 2016 auditd
-r-xr-xr-x. 1 root root 1343 5月 11 2016 blk-availability
-rwxr-xr-x. 1 root root 710 11月 11 2010 bluetooth
-rwxr-xr-x. 1 root root 11864 7月 24 2015 cpuspeed
-rwxr-xr-x. 1 root root 2826 11月 10 2015 crond
-rwxr-xr-x. 1 root root 3034 5月 11 2016 cups
-rwxr-xr-x. 1 root root 1734 5月 11 2016 dnsmasq
-rwxr-xr-x. 1 root root 5113 11月 1 02:57 elasticsearch
-rwxr-xr-x. 1 root root 1186 11月 5 00:19 fdfs_storaged
-rwxr-xr-x. 1 root root 1186 11月 5 00:19 fdfs_trackerd
-rwxr-xr-x. 1 root root 3245 7月 9 2013 firstboot
-rw-r--r--. 1 root root 25419 4月 12 2016 functions
-rwxr-xr-x. 1 root root 1801 10月 15 2014 haldaemon
-rwxr-xr-x. 1 root root 5985 4月 12 2016 halt
-rwxr-xr-x. 1 root root 2001 5月 12 2016 htcacheclean
```

CentOS6.8 通过 `chkconfig --list` 可以查看

```
[root@jack init.d]# chkconfig --add elasticsearch
[root@jack init.d]# chkconfig --list
NetworkManager 0:关闭 1:关闭 2:启用 3:启用 4:启用 5:启用 6:关闭
abrt-ccpp 0:关闭 1:关闭 2:关闭 3:启用 4:关闭 5:启用 6:关闭
abrt-d 0:关闭 1:关闭 2:关闭 3:启用 4:关闭 5:启用 6:关闭
acpid 0:关闭 1:关闭 2:启用 3:启用 4:启用 5:启用 6:关闭
atd 0:关闭 1:关闭 2:关闭 3:启用 4:启用 5:启用 6:关闭
auditd 0:关闭 1:关闭 2:启用 3:启用 4:启用 5:启用 6:关闭
blk-availability 0:关闭 1:启用 2:启用 3:启用 4:启用 5:启用 6:关闭
bluetooth 0:关闭 1:关闭 2:关闭 3:启用 4:启用 5:启用 6:关闭
cpuspeed 0:关闭 1:启用 2:启用 3:启用 4:启用 5:启用 6:关闭
crond 0:关闭 1:关闭 2:启用 3:启用 4:启用 5:启用 6:关闭
cups 0:关闭 1:关闭 2:启用 3:启用 4:启用 5:启用 6:关闭
dnsmasq 0:关闭 1:关闭 2:关闭 3:关闭 4:关闭 5:关闭 6:关闭
elasticsearch 0:关闭 1:关闭 2:启用 3:启用 4:启用 5:启用 6:关闭
firstboot 0:关闭 1:关闭 2:关闭 3:关闭 4:关闭 5:关闭 6:关闭
haldaemon 0:关闭 1:关闭 2:关闭 3:启用 4:启用 5:启用 6:关闭
htcacheclean 0:关闭 1:关闭 2:关闭 3:关闭 4:关闭 5:关闭 6:关闭
httpd 0:关闭 1:关闭 2:关闭 3:关闭 4:关闭 5:关闭 6:关闭
ip6tables 0:关闭 1:关闭 2:启用 3:启用 4:启用 5:启用 6:关闭
iptables 0:关闭 1:关闭 2:启用 3:启用 4:启用 5:关闭 6:关闭
```

CentOS7.x 可以通过 `systemctl list-unit-files|grep elasticsearch`

```
[root@localhost init.d]# systemctl list-unit-files |grep elasticsearch
elasticsearch.service disabled
[root@localhost init.d]#
```

启动之前为 `elasticsearch` 配置 `jdk`

`vim /etc/sysconfig/elasticsearch` 中修改 `JAVA_HOME` 路径的路径

```
# Elasticsearch home directory
#ES_HOME=/usr/share/elasticsearch

# Elasticsearch Java path
JAVA_HOME=/opt/jdk1.8.0_152

# Elasticsearch configuration directory
#CONF_DIR=/etc/elasticsearch

# Elasticsearch data directory
#DATA_DIR=/var/lib/elasticsearch

# Elasticsearch log directory
```

启动 `elasticsearch`

```
root@localhost init.d]# service elasticsearch start
Starting elasticsearch (via systemctl): [ 确定 ]
root@localhost init.d]# ps -ef |grep java
```

查看进程

```
[root@jack ~]# ps -ef |grep elastic
495      7684      1  2 21:32 ?        00:00:42 /opt/jdk1.8.0_152/bin/java -Xms2g -Xmx2g -XX:+UseConcMarkSweepGC -
XX:CMSInitiatingOccupancyFraction=75 -XX:+UseCMSInitiatingOccupancyOnly -XX:+AlwaysPreTouch -server -Xss1m -Djava.aw
t.headless=true -Dfile.encoding=UTF-8 -Djna.nosys=true -Djdk.io.permissionsUseCanonicalPath=true -Dio.netty.noUnsafe
=true -Dio.netty.noKeySetOptimization=true -Dio.netty.recycler.maxCapacityPerThread=0 -Dlog4j.shutdownHookEnabled=fa
lse -Dlog4j2.disable.jmx=true -Dlog4j.skipJansi=true -XX:+HeapDumpOnOutOfMemoryError -Des.path.home=/usr/share/elast
icsearch -cp /usr/share/elasticsearch/lib/* org.elasticsearch.bootstrap.Elasticsearch -p /var/run/elasticsearch/elas
ticsearch.pid -d -Edefault.path.logs=/var/log/elasticsearch -Edefault.path.data=/var/lib/elasticsearch -Edefault.pat
h.conf=/etc/elasticsearch
root      7757      6807      0  21:38 pts/0    00:00:00 vim /etc/elasticsearch/elasticsearch.yml
```

核心文件

/etc/elasticsearch/elasticsearch.yml

数据文件路径

/var/lib/elasticsearch/

日志文件路径

/var/log/elasticsearch/elasticsearch.log

2.2 修改配置文件

```
vim /etc/elasticsearch/elasticsearch.yml
```

修改 yml 配置的注意事项:

每行必须顶格, 不能有空格

": "后面必须有一个空格

集群名称, 同一集群名称必须相同

```
#
# Use a descriptive name for your cluster:
#
cluster.name: my-es
#
# ----- Node -----
```

单个节点名称

```
# ----- Node -----
#
# Use a descriptive name for the node:
#
node.name: node-1
#
# Add custom attributes to the node
```

网络部分 改为当前的 ip 地址 ，端口号保持默认 9200 就行

```
#
# Set the bind address to a specific IP (IPv4 or IPv6):
#
network.host: 192.168.67.163
#http.host: 192.168.67.163
#transport.host: 192.168.67.147
# Set a custom port for HTTP:
#
```

把 bootstrap 自检程序关掉

```
# ----- Memory -----
#
# Lock the memory on startup:
#
bootstrap.memory_lock: false
bootstrap.system_call_filter: false
#
# Make sure that the heap size is set to about half the memory available
# on the system and that the owner of the process is allowed to use this
# limit.
```

自发现配置：新节点向集群报到的主机名


```
# ----- Discovery -----  
#  
# Pass an initial list of hosts to perform discovery when new node is started:  
# The default list of hosts is ["127.0.0.1", "[::1]"]  
#  
discovery.zen.ping.unicast.hosts: ["jack.atguigu"]  
#
```

2.3 修改 linux 配置

为什么要修改 linux 配置？

默认 elasticsearch 是单机访问模式，就是只能自己访问自己。

但是我们之后一定会设置成允许应用服务器通过网络方式访问。这时，elasticsearch 就会因为嫌弃单机版的低端默认配置而报错，甚至无法启动。

所以我们在这里就要把服务器的一些限制打开，能支持更多并发。

**问题1: max file descriptors [4096] for elasticsearch process likely too low,
increase to at least [65536] elasticsearch**

原因：系统允许 Elasticsearch 打开的最大文件数需要修改成 65536

解决：vi /etc/security/limits.conf

添加内容：

```
* soft nfile 65536  
* hard nfile 131072  
* soft nproc 2048  
* hard nproc 65536
```

注意：“*” 不要省略掉

**问题2: max number of threads [1024] for user [judy2] likely too low,
increase to at least [2048] (CentOS7.x 不用改)**

原因：允许最大进程数修该成 2048

解决：vi /etc/security/limits.d/90-nproc.conf

修改如下内容：

```
* soft nproc 1024
```

#修改为

```
* soft nproc 2048
```

问题3: max virtual memory areas vm.max_map_count [65530] likely too low, increase to at least [262144] (CentOS7.x 不用改)

原因：一个进程可以拥有的虚拟内存区域的数量。

解决：可零时提高 vm.max_map_count 的大小

命令：sysctl -w vm.max_map_count=262144

2.4 重启 linux

2.5 测试

```
[root@centos147 ~]# curl http://192.168.67.147:9200
{
  "name" : "atguigu",
  "cluster_name" : "my-application",
  "cluster_uuid" : "dLWGNLJsQ7efpvofNCQLIA",
  "version" : {
    "number" : "5.6.4",
    "build_hash" : "8bbedf5",
    "build_date" : "2017-10-31T18:55:38.105Z",
    "build_snapshot" : false,
    "lucene_version" : "6.6.1"
  },
}
```

```
"tagline" : "You Know, for Search"
}
```

或者直接浏览器访问 <http://192.168.67.147:9200>



```
{
  "name" : "atguigu",
  "cluster_name" : "my-application",
  "cluster_uuid" : "dLWGNLJsQ7efpvoFNCQLLA",
  "version" : {
    "number" : "5.6.4",
    "build_hash" : "8bbedf5",
    "build_date" : "2017-10-31T18:55:38.105Z",
    "build_snapshot" : false,
    "lucene_version" : "6.6.1"
  },
  "tagline" : "You Know, for Search"
}
```

2.6 如果启动未成功

如果启动未成功，请去查看相关日志

```
vim /var/log/elasticsearch/my-es.log
```

3 安装 kibana

拷贝 kibana-5.6.4-linux-x86_64.tar 到/opt 下

解压缩

进入 kibana 主目录的 config 目录下


```
drwxr-xr-x. 2 atguigu atguigu 76 3月 16 23:08 bin
drwxrwxr-x. 2 atguigu atguigu 24 3月 16 23:07 config
drwxrwxr-x. 2 atguigu atguigu 18 3月 16 22:57 data
-rw-rw-r--. 1 atguigu atguigu 562 11月 1 03:04 LICENSE.txt
drwxrwxr-x. 6 atguigu atguigu 108 11月 1 03:04 node
drwxrwxr-x. 618 atguigu atguigu 20480 11月 1 03:04 node_modules
-rw-rw-r--. 1 atguigu atguigu 798420 11月 1 03:04 NOTICE.txt
drwxrwxr-x. 3 atguigu atguigu 45 11月 1 03:04 optimize
-rw-rw-r--. 1 atguigu atguigu 721 11月 1 03:04 package.json
drwxrwxr-x. 2 atguigu atguigu 6 11月 1 03:04 plugins
-rw-rw-r--. 1 atguigu atguigu 4899 11月 1 03:04 README.txt
drwxr-xr-x. 13 atguigu atguigu 165 11月 1 03:04 src
drwxrwxr-x. 5 atguigu atguigu 52 11月 1 03:04 ui_framework
drwxr-xr-x. 2 atguigu atguigu 4096 11月 1 03:04 webpackShims
[root@jack kibana-5.6.4-linux-x86_64]# cd config
[root@jack config]#
```

vim kibana.yml

```
# Kibana is served by a back end server. This setting specifies the port to use.
#server.port: 5601

# Specifies the address to which the Kibana server will bind. IP addresses and hostnames
# are all valid. The default is 'localhost', which usually means remote machines.
# To allow connections from remote users, set this parameter to a non-loopback address.
server.host: "0.0.0.0"

# Enables you to specify a path to mount Kibana at if you are running behind a proxy.
# The default is '/'. This setting can't end in a slash.
#server.basePath: "/"

# The maximum payload size in bytes for incoming server requests.
#server.maxPayloadBytes: 1048576

# The Kibana server's name. This is used for display purposes.
#server.name: "your-hostname"

# The URL of the Elasticsearch instance to use for all your queries.
elasticsearch.url: "http://192.168.67.163:9200"

# When this setting's value is true Kibana uses the hostname specified in the
# `server.host` setting to generate absolute URLs. This is useful if you are using
# a hostname that is not an IP address.
```

启动

在 kibana 主目录 bin 目录下执行

nohup ./kibana &

然后 ctrl+c 退出

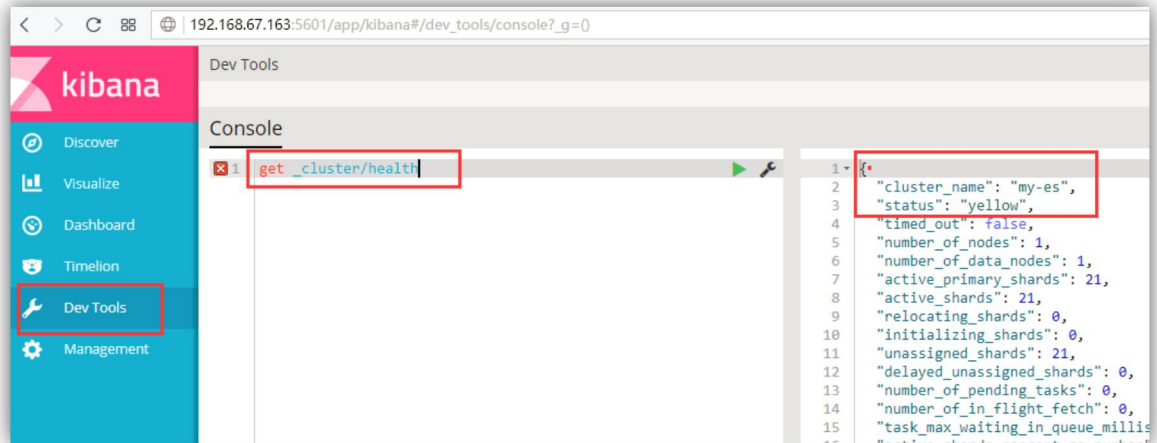
执行 ps -ef

```
root      1690      2    0 23:37 ?        00:00:00 [kworker/u256:1]
root      1757    1285    4 23:38 pts/0    00:00:10 ./../node/bin/node --no-warnings ./../src/cli
root      1768      2    0 23:39 ?        00:00:00 [kworker/5:1]
```

如上图,1757 号进程就是 kibana 的进程

用浏览器打开

<http://192.168.xx.xx:5601/>



点击左边菜单 DevTools

在 Console 中

执行 `get _cluster/health`

右边的结果中，status 为 yellow 或者 green。

表示 es 启动正常，并且与 kibana 连接正常。