

Elasticsearch 集群部署

=====安装 java 环境=====

yum -y list java*

sudo yum -y install java-1.8.0-openjdk*

验证是否安装成功

```
[root@localhost ~]# java -version
openjdk version "1.8.0_181"
OpenJDK Runtime Environment (build 1.8.0_181-b13)
OpenJDK 64-Bit Server VM (build 25.181-b13, mixed mode)
[root@localhost ~]#
```

=====修改文件=====

su root

vi /etc/security/limits.conf

文件末尾添加如下信息

End of file

```
*          hard    nofile          65536
*          soft    nofile          65536
*          hard    nproc           65536
*          soft    nproc           65536
```

```
# End of file
*          hard    nofile          65536
*          soft    nofile          65536
*          soft    nproc           65536
*          hard    nproc           65536
-- INSERT --
```

vi /etc/sysctl.conf

备注：行末加上 **vm.max_map_count = 655360** ， esc +: wq 保存退出

并执行命令：

sysctl -p

出现如下信息

```
[root@localhost ~]# sysctl -p
vm.max_map_count = 655360
[root@localhost ~]#
```

=====下载 elasticsearch=====

wget <https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-6.4.1.tar.gz>

```
[root@localhost ~]#
[root@localhost ~]# wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-6.4.1.tar.gz
--2018-09-25 04:44:42-- https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-6.4.1.tar.gz
Resolving artifacts.elastic.co (artifacts.elastic.co)... 107.21.237.95, 107.21.127.184, 107.21.202.15, ...
Connecting to artifacts.elastic.co (artifacts.elastic.co)[107.21.237.95]:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 97924081 (93M) [application/x-gzip]
Saving to: 'elasticsearch-6.4.1.tar.gz'
```

解压

```
sudo tar -zxvf elasticsearch-6.4.1.tar.gz
```

将解压出来的文件夹移动到 /usr/local/ 目录下

```
cp elasticsearch-6.4.1 /usr/local/ -rf
```

进入 elasticsearch

```
cd /usr/local/elasticsearch-6.4.1/
```

为 elasticsearch 新建用户

```
useradd elastic
```

```
passwd elastic
```

```
[root@localhost elasticsearch-6.4.1]# useradd elastic
[root@localhost elasticsearch-6.4.1]# passwd elastic
Changing password for user elastic.
New password:
Retype new password:
```

把 elasticsearch-6.4.1 的整个文件夹赋给用户 elastic

```
sudo chown -R elastic:elastic /usr/local/elasticsearch-6.4.1/
```

```
[root@localhost elasticsearch-6.4.1]# sudo chown -R elastic:elastic /usr/local/elasticsearch-6.4.1/
[root@localhost elasticsearch-6.4.1]#
```

切换到 elastic

```
su elastic
```

修改 elasticsearch 配置文件 elasticsearch.yml

```
[root@localhost config]# pwd
/usr/local/elasticsearch-6.4.1/config
[root@localhost config]# vi elasticsearch.yml
```

```
cd /usr/local/elasticsearch-6.4.1/config
```

```
vi elasticsearch.yml
```

主要修改如下配置（单点）

=====配置文件修改开始=====

```
cluster.name: idsbg-cluster
```

```
network.host: 0.0.0.0
```

```
http.port: 9200
```

=====配置文件修改结束=====

测试

```
[elastic@localhost elasticsearch-6.4.1]$ pwd
/usr/local/elasticsearch-6.4.1
```

在 elasticsearch 根目录下执行以下命令(当前用户为 elastic)

```
./bin/elasticsearch
```

出现如下结果表明启动成功

```
master [master {3gkCTTP:3gkCTTPKRBK14NMOXS6Na0i:JLQM16EBSZUM2JUGEn8nGA}{192.168.98.133}{192.168.98.133:9300}{m.machine_memory{1021906944, xpack.inst
lled=true, ml.max_open_jobs=20, ml.enabled=true} committed version [1] source [zen-disco-elected-as-master ([0] nodes joined)[, ]]}]
[2018-09-25T05:26:37.919] [WARN] [o.e.x.s.a.s.m.NativeRoleMappingStore] [3gkCTTP] failed to clear cache for roles [[]]
[2018-09-25T05:26:37.961] [INFO] [o.e.x.s.t.n.SecurityNetty4HttpServerTransport] [3gkCTTP] publish_address {192.168.98.133:9200}, bound_addresses {[::]
:9200}
[2018-09-25T05:26:37.968] [INFO] [o.e.n.Node] [3gkCTTP] started
[2018-09-25T05:26:38.157] [INFO] [o.e.g.GatewayService] [3gkCTTP] recovered local indices into cluster state
[2018-09-25T05:26:38.505] [INFO] [o.e.c.m.MetadataIndexTemplateService] [3gkCTTP] adding template [.watches] for index patterns [.watches*]
[2018-09-25T05:26:38.564] [INFO] [o.e.c.m.MetadataIndexTemplateService] [3gkCTTP] adding template [.triggered_watches] for index patterns [.triggered_w
atches*]
[2018-09-25T05:26:38.836] [INFO] [o.e.c.m.MetadataIndexTemplateService] [3gkCTTP] adding template [.watcher-history-9] for index patterns [.watcher-hist
ory-9*]
[2018-09-25T05:26:38.943] [INFO] [o.e.c.m.MetadataIndexTemplateService] [3gkCTTP] adding template [.monitoring-logsstash] for index patterns [.monitoring
-logsstash-6-*]
[2018-09-25T05:26:39.058] [INFO] [o.e.c.m.MetadataIndexTemplateService] [3gkCTTP] adding template [.monitoring-es] for index patterns [.monitoring-es-6
-*]
[2018-09-25T05:26:39.146] [INFO] [o.e.c.m.MetadataIndexTemplateService] [3gkCTTP] adding template [.monitoring-beats] for index patterns [.monitoring-be
ats-6-*]
[2018-09-25T05:26:39.196] [INFO] [o.e.c.m.MetadataIndexTemplateService] [3gkCTTP] adding template [.monitoring-alerts] for index patterns [.monitoring-
alerts-6-*]
[2018-09-25T05:26:39.280] [INFO] [o.e.c.m.MetadataIndexTemplateService] [3gkCTTP] adding template [.monitoring-kibana] for index patterns [.monitoring-
kibana-6-*]
[2018-09-25T05:26:39.512] [INFO] [o.e.l.LicenseService] [3gkCTTP] license [063d875a-75bb-4a3c-ada6-c3bbe8a7c008] mode [basic] - valid
```

关闭当前 elasticsearch
Ctrl+C
关闭后台运行的 elasticsearch
losf -i:9200
Kill -9 <pid>

=====集群配置=====

假如有三台服务器

192.168.1.110

192.168.1.111

192.168.1.112

110 配置如下

cluster.name: idsbg-cluster

node.name:node-110

network.host: 0.0.0.0

http.port: 9200

discovery.zen.ping.unicast.hosts:["192.168.1.110","192.168.1.111","192.168.1.112"]

transport.tcp.port: 9300 #用于集群之间相互发现

111 配置如下

cluster.name: idsbg-cluster

node.name:node-111

network.host: 0.0.0.0

http.port: 9200

discovery.zen.ping.unicast.hosts:["192.168.1.110","192.168.1.111","192.168.1.112"]

transport.tcp.port: 9300 #用于集群之间相互发现

112 配置如下

cluster.name: idsbg-cluster

node.name:node-112

network.host: 0.0.0.0

http.port: 9200

discovery.zen.ping.unicast.hosts:["192.168.1.110","192.168.1.111","192.168.1.112"]

transport.tcp.port: 9300 #用于集群之间相互发现

保证 cluster.name 相同，node.name 不同

分别启动，即可完成集群搭建