

es 集群以及 es-head 插件的安装

作者: [yj14114](#)

原文链接: <https://ld246.com/article/1512615366574>

来源网站: [链滴](#)

许可协议: [署名-相同方式共享 4.0 国际 \(CC BY-SA 4.0\)](#)

elasticserach安装

@(ELK日志系统)

一、首先安装supervisor

supervisor 是linux用于管理后台程序的守护进程、方便管理集群

二、安装es

- 下载最新版的es [官网地址](#)
- 准备好两台服务器(能够互相ping通)
 - 10.66.30.221
 - 10.66.2.90

es 配置文件示例

```
# ===== Elasticsearch Configuration =====  
=====  
#  
# NOTE: Elasticsearch comes with reasonable defaults for most settings.  
# Before you set out to tweak and tune the configuration, make sure you  
# understand what are you trying to accomplish and the consequences.  
#  
# The primary way of configuring a node is via this file. This template lists  
# the most important settings you may want to configure for a production cluster.  
#  
# Please consult the documentation for further information on configuration options:  
# https://www.elastic.co/guide/en/elasticsearch/reference/index.html  
#  
# ----- Cluster -----  
#  
# Use a descriptive name for your cluster:  
#  
cluster.name: es-cluster  
#  
# ----- Node -----  
#  
# Use a descriptive name for the node:  
#  
node.name: node-2  
#  
# Add custom attributes to the node:  
#  
#node.attr.rack: r1  
#  
# ----- Paths -----  
#  
# Path to directory where to store the data (separate multiple locations by comma):
```

```

#
path.data: /home/es/path/to/data
#
# Path to log files:
#
path.logs: /home/es/path/to/logs
bootstrap.memory_lock: true
#
# ----- Memory -----
#
# Lock the memory on startup:
#
#bootstrap.memory_lock: true
#
# 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.
#
# Elasticsearch performs poorly when the system is swapping the memory.
#
# ----- Network -----
#
network.host: 10.66.2.90
#
# Set a custom port for HTTP:
#
http.port: 9200
transport.tcp.port: 9300
transport.tcp.compress: true
discovery.zen.ping.unicast.hosts:
  - 10.6.2.90
  - 10.66.30.221
#
# For more information, consult the network module documentation.
#
# ----- 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: ["host1", "host2"]
#
# Prevent the "split brain" by configuring the majority of nodes (total number of master-elig
ble nodes / 2 + 1):
#
discovery.zen.minimum_master_nodes: 2
http.cors.enabled: true
http.cors.allow-origin: "*"
#
# For more information, consult the zen discovery module documentation.
#
# ----- Gateway -----
#
# Block initial recovery after a full cluster restart until N nodes are started:

```

```
#
#gateway.recover_after_nodes: 3
#
# For more information, consult the gateway module documentation.
#
# ----- Various -----
#
# Require explicit names when deleting indices:
#
#action.destructive_requires_name: true
```

es启动常见的错误

问题1:

```
$ ./elasticsearch
...
ERROR: bootstrap checks failed
max file descriptors [4096] for elasticsearch process likely too low, increase to at least [65536]
max virtual memory areas vm.max_map_count [65530] likely too low, increase to at least [262
44]
[2016-10-31T04:55:45,240][INFO ][o.e.n.Node                ] [vJDcSkt] stopping ...
[2016-10-31T04:55:45,249][INFO ][o.e.n.Node                ] [vJDcSkt] stopped
[2016-10-31T04:55:45,249][INFO ][o.e.n.Node                ] [vJDcSkt] closing ...
[2016-10-31T04:55:45,257][INFO ][o.e.n.Node                ] [vJDcSkt] closed
```

如图所示有两个错误

错误1的解决办法

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

修改/etc/security/limits.conf文件，添加或修改如下行：

退出当前账号，然后重新登录

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

错误2的解决办法

max virtual memory areas vm.max_map_count [65530] likely too low, increase to at least [26244]

切换到root用户修改配置sysctl.conf

vi /etc/sysctl.conf

添加下面配置：

vm.max_map_count=262144

并执行命令：

sysctl -p

然后，重新启动elasticsearch，即可启动成功。

问题2:

max number of threads [1024] for user [root] is too low, increase to at least [2048]

解决办法

切换到root用户，进入limits.d目录下修改配置文件。

vim /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:

ERROR: bootstrap checks failed
system call filters failed to install; check the logs and fix your configuration or disable system
all filters at your own risk

原因：

这是因为Centos6不支持SecComp，而ES5.2.0默认bootstrap.system_call_filter为true进行检测
所以导致检测失败，失败后直接导致ES不能启动。

解决：

在elasticsearch.yml中配置bootstrap.system_call_filter为false，注意要在Memory下面：

```
bootstrap.memory_lock: false  
bootstrap.system_call_filter: false
```

问题4: elasticsearch 索引问题

logstash传入es的序列必须全为小写，否则会报400的错误

解决：

直接在filebeat.yml中设置index

```
output.logstash:  
# The Logstash hosts  
hosts: ["10.66.140.37:5044"]  
worker: 1  
loadbalance: true  
index: "opennbk-filebeat"
```

####问题5： elasticsearch 使用supervisord启动时需要切换用户到非root启动问题

ES不能用root账户启动,否则会抛出异常 但是使用supervisord -c ../supervisor.conf启动的时候会出一下错误

解决:

这个时候我们可以把supervisor.conf文件中的program选项中的 user (谁来启动)注释,然后修改program选项中的command(启动命令) 为:su -c "ES启动脚本的目录" 非root用户.

问题6

ERROR: [1] bootstrap checks failed

[1]: memory locking requested for elasticsearch process but memory is not locked

修改/etc/security/limits.conf文件, 添加或修改如下行:

退出当前账号, 然后重新登录

```
* soft memlock unlimited
* soft memlock unlimited
```

三、supervisor配置es

```
[program: es_node2]
command=/home/es/elasticsearch-6.0.0/bin/elasticsearch
numprocs=1
user=es
autostart=true
autorestart=true
```

es 插件head安装

1.首先安装nodejs

2.全局安装grunt

```
npm install -g grunt-cli
```

3.克隆head工程

```
git clone https://github.com/mobz/elasticsearch-head
```

4.修改head目录下的Gruntfile.js文件

添加hostname

```
connect: {
  server: {
    options: {
      port: 9100,
      hostname: '*',
      base: '.',
```

```
        },
    },
    keepalive: true
}
```

修改head目录下的app.js文件。

vim/_site/app.js

```
app.App = ui.AbstractWidget.extend({
  defaults: {
    base_uri: null
  },
  init: function(parent) {
    this._super();
    this.prefs = services.Preferences.instance();
    this.base_uri = this.config.base_uri || this.prefs.get("app-base_uri") || "http://10
66.2.90:9200" || "http://10.66.30.221:9200";
    if( this.base_uri.charAt( this.base_uri.length - 1 ) !== "/" ) {
      // XHR request fails if the URL is not ending with a "/"
      this.base_uri += "/";
    }
    if( this.config.auth_user ) {
```

修改es目录下的elasticsearch.yml文件

```
http.cors.enabled: true
http.cors.allow-origin: "*"

```

grunt server 启动