ELK 环境部署测试

注：Logstash Elasticsearch Kibana 的下载地址统一为 https://www.elastic.co/downloads/

问题排查可以登录 **https://discuss.elastic.co/c** 论坛查找相关信息

一． 安装 Logstash

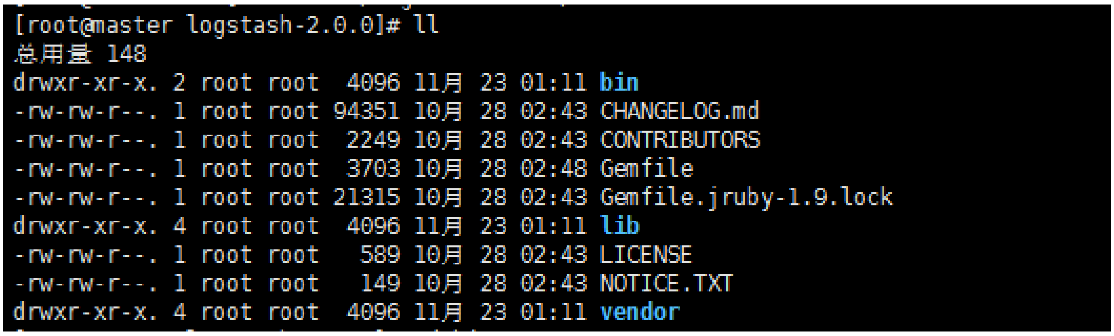
1.安装 Logstash

下载解压，从上面统一网址找到 Logstash 下载解压即可，也可以通过 wget 命令获得：

wget https://download.elastic.co/logstash/logstash/logstash-2.0.0.tar.gz

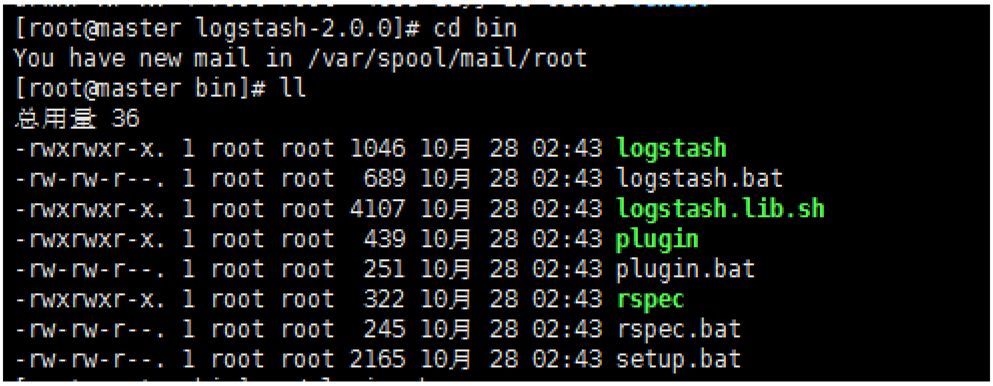
2.安装插件

解压后进去看到如下目录：



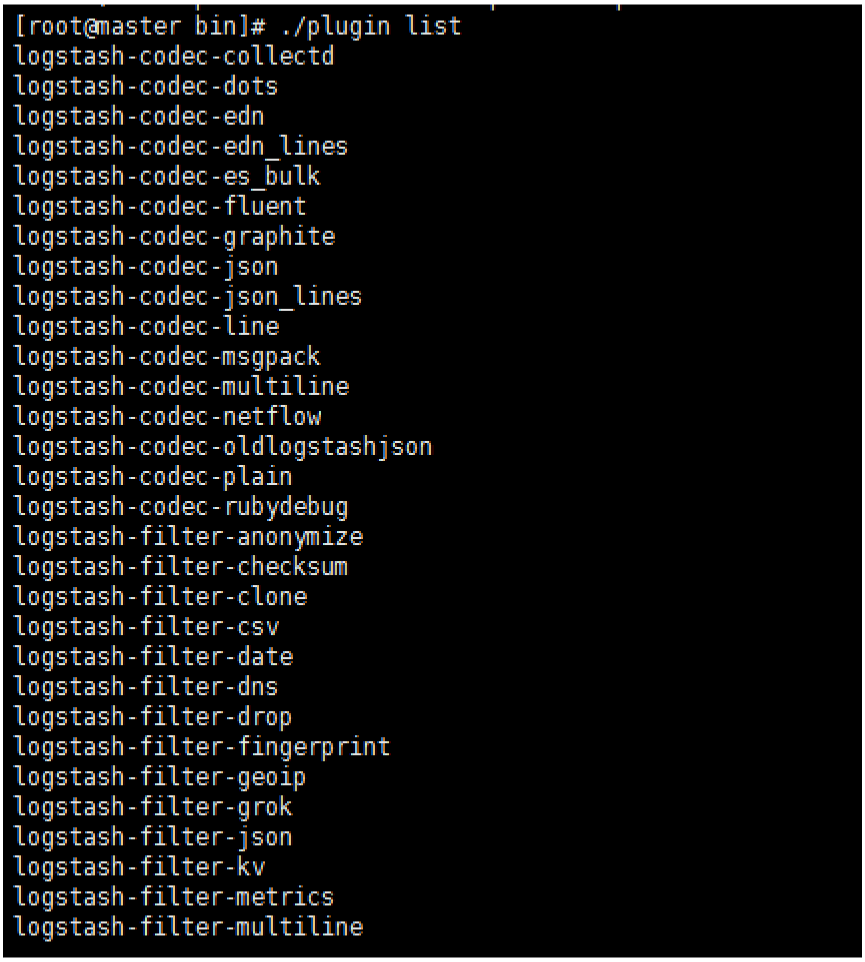
```
[root@master logstash-2.0.0]# ll
总用量 148
drwxr-xr-x. 2 root root  4096 11月  23 01:11 bin
-rw-rw-r--. 1 root root 94351 10月  28 02:43 CHANGELOG.md
-rw-rw-r--. 1 root root  2249 10月  28 02:43 CONTRIBUTORS
-rw-rw-r--. 1 root root  3703 10月  28 02:48 Gemfile
-rw-rw-r--. 1 root root 21315 10月  28 02:43 Gemfile.jruby-1.9.lock
drwxr-xr-x. 4 root root  4096 11月  23 01:11 lib
-rw-rw-r--. 1 root root   589 10月  28 02:43 LICENSE
-rw-rw-r--. 1 root root   149 10月  28 02:43 NOTICE.TXT
drwxr-xr-x. 4 root root  4096 11月  23 01:11 vendor
```

进入 bin 目录看到：



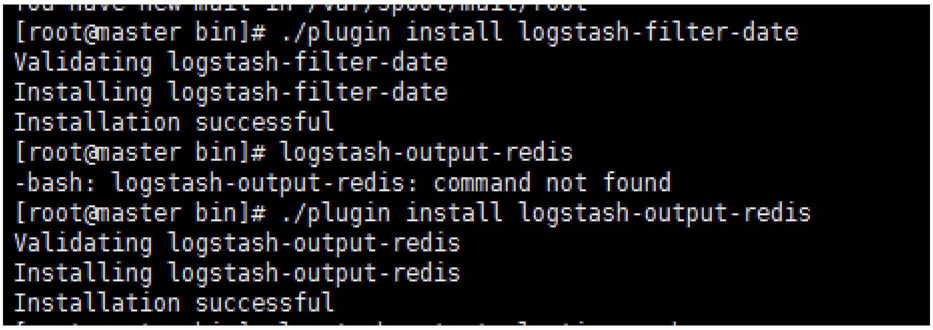
```
[root@master logstash-2.0.0]# cd bin
You have new mail in /var/spool/mail/root
[root@master bin]# ll
总用量 36
-rwxrwxr-x. 1 root root 1046 10月  28 02:43 logstash
-rw-rw-r--. 1 root root  689 10月  28 02:43 logstash.bat
-rwxrwxr-x. 1 root root 4107 10月  28 02:43 logstash.lib.sh
-rwxrwxr-x. 1 root root  439 10月  28 02:43 plugin
-rw-rw-r--. 1 root root  251 10月  28 02:43 plugin.bat
-rwxrwxr-x. 1 root root  322 10月  28 02:43 rspec
-rw-rw-r--. 1 root root  245 10月  28 02:43 rspec.bat
-rw-rw-r--. 1 root root 2165 10月  28 02:43 setup.bat
```

执行./plugin list 可以看到目前能安装的插件



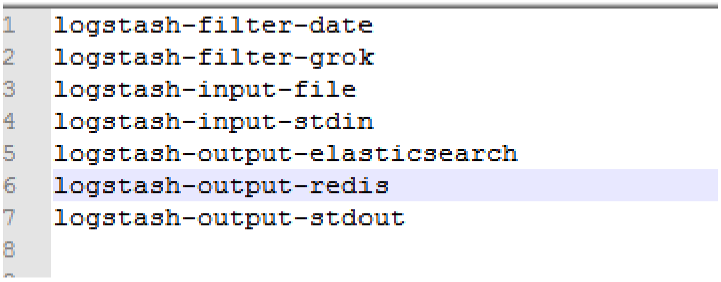
```
[root@master bin]# ./plugin list
logstash-codec-collectd
logstash-codec-dots
logstash-codec-edn
logstash-codec-edn_lines
logstash-codec-es_bulk
logstash-codec-fluent
logstash-codec-graphite
logstash-codec-json
logstash-codec-json_lines
logstash-codec-line
logstash-codec-msgpack
logstash-codec-multiline
logstash-codec-netflow
logstash-codec-oldlogstashjson
logstash-codec-plain
logstash-codec-rubydebug
logstash-filter-anonymize
logstash-filter-checksum
logstash-filter-clone
logstash-filter-csv
logstash-filter-date
logstash-filter-dns
logstash-filter-drop
logstash-filter-fingerprint
logstash-filter-geoip
logstash-filter-grok
logstash-filter-json
logstash-filter-kv
logstash-filter-metrics
logstash-filter-multiline
```

通过./plugin install 插件名来安装插件



```
You have new mail in /var/spool/mail/root
[root@master bin]# ./plugin install logstash-filter-date
Validating logstash-filter-date
Installing logstash-filter-date
Installation successful
[root@master bin]# logstash-output-redis
-bash: logstash-output-redis: command not found
[root@master bin]# ./plugin install logstash-output-redis
Validating logstash-output-redis
Installing logstash-output-redis
Installation successful
```

一些常用的一定要安装的例如：



```
logstash-filter-date
logstash-filter-grok
logstash-input-file
logstash-input-stdin
logstash-output-elasticsearch
logstash-output-redis
logstash-output-stdout
```

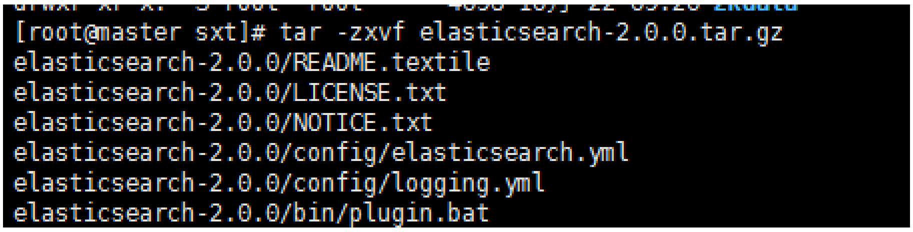
有时候会下载不下来，需要多尝试几次，有时候尝试十几次才行

配置 conf 文件，启动的时候 bin/logstash –f conf 文件路径，注意这里的 input 的文件必须是权限足够的 ，因为 Elasticsearch 需要普通用户才能启动，所以

二. 安装 Elasticsearch

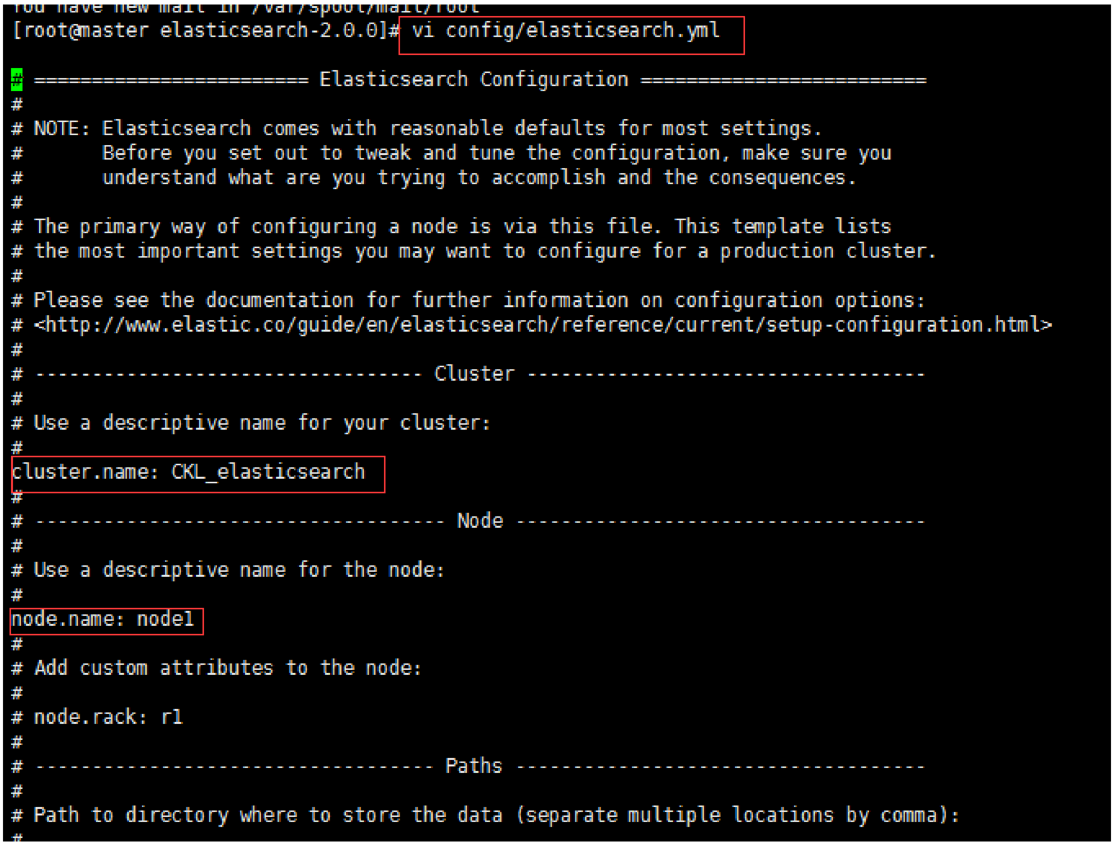
1.安装 Elasticsearch 集群

下载 elasticsearch-2.0.0.tar.gz，执行 tar -zxvf elasticsearch-2.0.0.tar.gz 解压



```
[root@master sxt]# tar -zxvf elasticsearch-2.0.0.tar.gz
elasticsearch-2.0.0/README.textile
elasticsearch-2.0.0/LICENSE.txt
elasticsearch-2.0.0/NOTICE.txt
elasticsearch-2.0.0/config/elasticsearch.yml
elasticsearch-2.0.0/config/logging.yml
elasticsearch-2.0.0/bin/plugin.bat
```

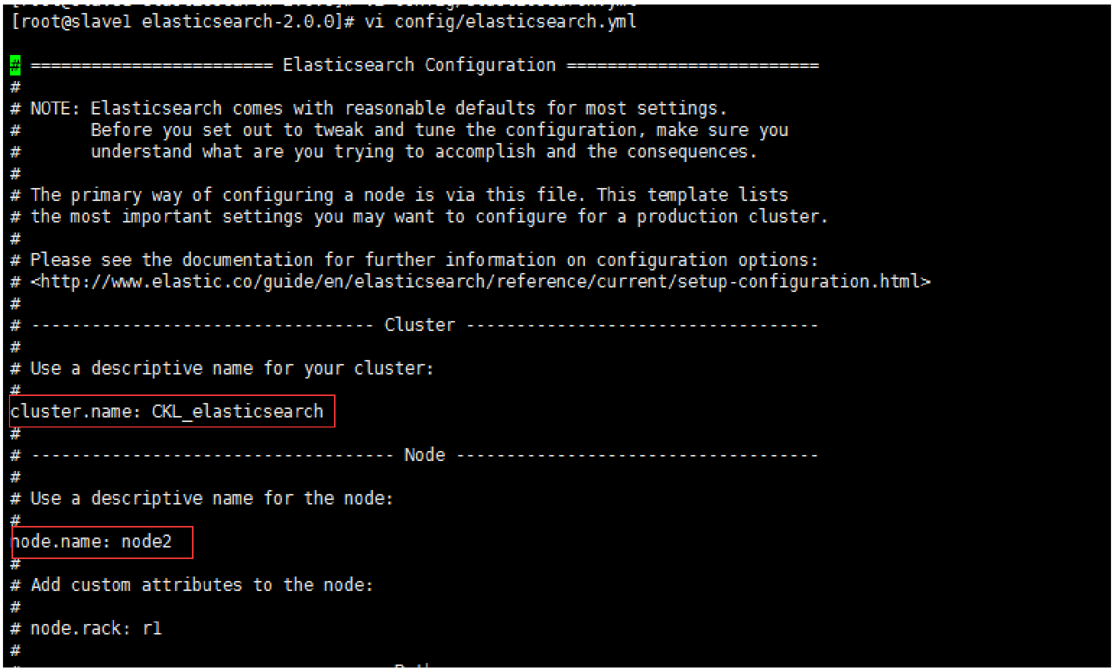
修改配置文件 config/elasticsearch.yml



```
You have new mail in /var/spool/mail/root
[root@master elasticsearch-2.0.0]# vi config/elasticsearch.yml

# ======================== 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 see the documentation for further information on configuration options:
# <http://www.elastic.co/guide/en/elasticsearch/reference/current/setup-configuration.html>
#
# ---------------------------------- Cluster -----------------------------------
#
# Use a descriptive name for your cluster:
#
cluster.name: CKL_elasticsearch
#
# ------------------------------------ Node ------------------------------------
#
# Use a descriptive name for the node:
#
node.name: node1
#
# Add custom attributes to the node:
#
# node.rack: r1
#
# ----------------------------------- Paths ------------------------------------
#
# Path to directory where to store the data (separate multiple locations by comma):
#
```

如果要配置集群需要两个节点上的 elasticsearch 配置的 cluster.name 相同，都启动可以自动组成集群，这里如果不改 cluster.name 则默认是 cluster.name=elasticsearch，nodename 随意取但是集群内的各节点不能相同

本人这里另外一台机器配置如图：



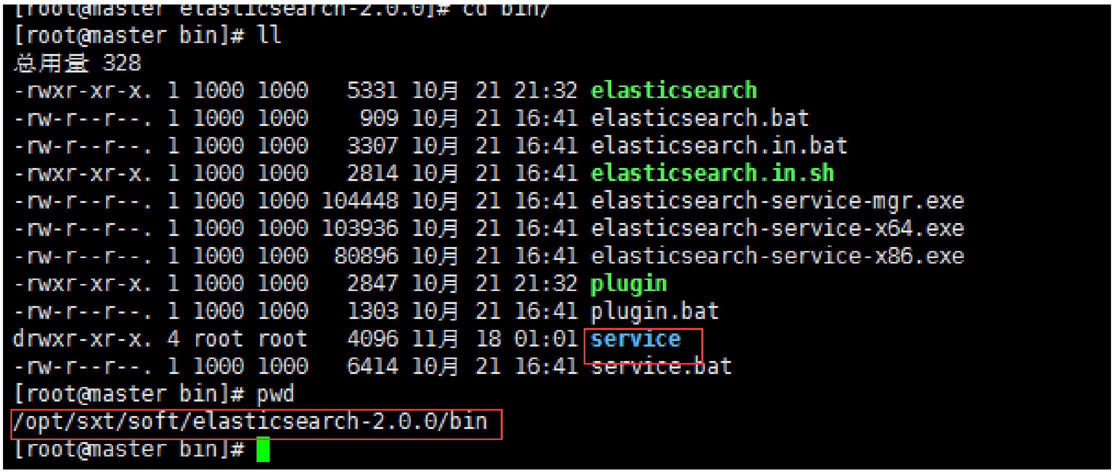
```
[root@slave1 elasticsearch-2.0.0]# vi config/elasticsearch.yml

# ======================== 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 see the documentation for further information on configuration options:
# <http://www.elastic.co/guide/en/elasticsearch/reference/current/setup-configuration.html>
#
# ---------------------------------- Cluster -----------------------------------
#
# Use a descriptive name for your cluster:
#
cluster.name: CKL_elasticsearch
#
# ------------------------------------ Node ------------------------------------
#
# Use a descriptive name for the node:
#
node.name: node2
#
# Add custom attributes to the node:
#
# node.rack: r1
#
```

最后同时启动可以组成集群

2.安装 elasticsearch-servicewrapper 插件

（1）下载 elasticsearch-servicewrapper

git clone https://github.com/elasticsearch/elasticsearch-servicewrapper，然后将目录下的 service 目录拷贝至 ES_HOME/bin 目录下。



```
[root@master elasticsearch-2.0.0]# cd bin/
[root@master bin]# ll
总用量 328
-rwxr-xr-x. 1 1000 1000   5331 10月 21 21:32 elasticsearch
-rw-r--r--. 1 1000 1000    909 10月 21 16:41 elasticsearch.bat
-rw-r--r--. 1 1000 1000   3307 10月 21 16:41 elasticsearch.in.bat
-rwxr-xr-x. 1 1000 1000   2814 10月 21 16:41 elasticsearch.in.sh
-rw-r--r--. 1 1000 1000 104448 10月 21 16:41 elasticsearch-service-mgr.exe
-rw-r--r--. 1 1000 1000 103936 10月 21 16:41 elasticsearch-service-x64.exe
-rw-r--r--. 1 1000 1000  80896 10月 21 16:41 elasticsearch-service-x86.exe
-rwxr-xr-x. 1 1000 1000   2847 10月 21 21:32 plugin
-rw-r--r--. 1 1000 1000   1303 10月 21 16:41 plugin.bat
drwxr-xr-x. 4 root root   4096 11月 18 01:01 service
-rw-r--r--. 1 1000 1000   6414 10月 21 16:41 service.bat
[root@master bin]# pwd
/opt/sxt/soft/elasticsearch-2.0.0/bin
[root@master bin]# 
```

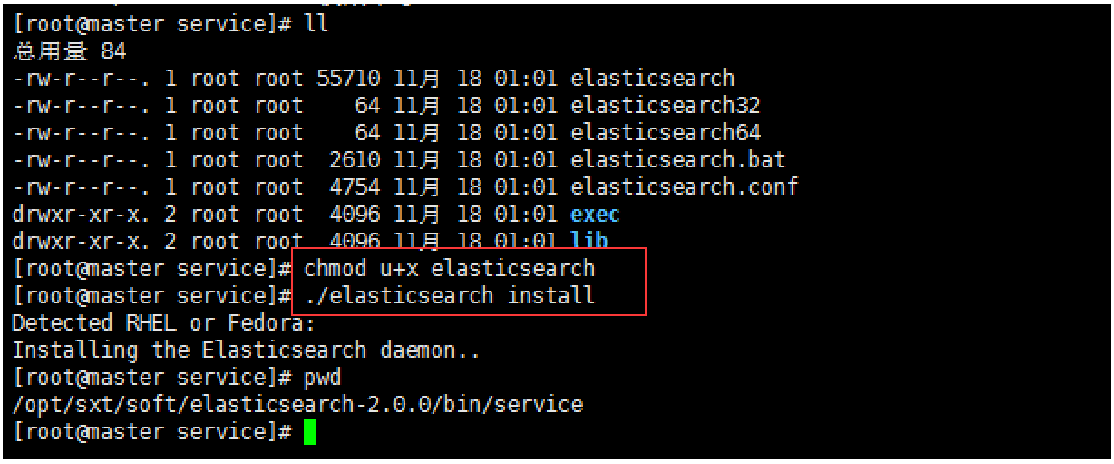
（2）简单配置 jvm 的内存

修改 ES_HOME/bin/service/elasticsearch.conf，set.default.ES_HEAP_SIZE=1024，该值根据机器的配置可自定义。

（3）安装启动服务

执行命令：ES_HOME/bin/service/elasticsearch install

这里需要添加一下执行权限

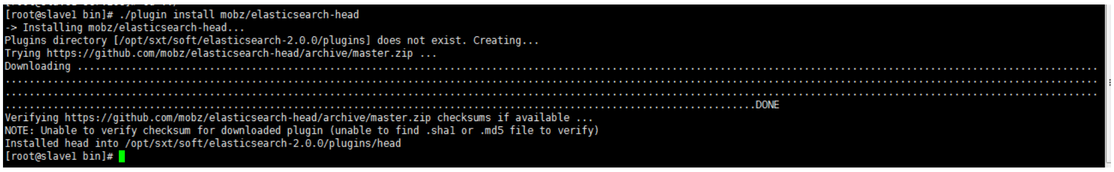


```
[root@master service]# ll
总用量 84
-rw-r--r--. 1 root root 55710 11月 18 01:01 elasticsearch
-rw-r--r--. 1 root root    64 11月 18 01:01 elasticsearch32
-rw-r--r--. 1 root root    64 11月 18 01:01 elasticsearch64
-rw-r--r--. 1 root root  2610 11月 18 01:01 elasticsearch.bat
-rw-r--r--. 1 root root  4754 11月 18 01:01 elasticsearch.conf
drwxr-xr-x. 2 root root  4096 11月 18 01:01 exec
drwxr-xr-x. 2 root root  4096 11月 18 01:01 lib
[root@master service]# chmod u+x elasticsearch
[root@master service]# ./elasticsearch install
Detected RHEL or Fedora:
Installing the Elasticsearch daemon..
[root@master service]# pwd
/opt/sxt/soft/elasticsearch-2.0.0/bin/service
[root@master service]# 
```

（4）启动/停止/重启服务

执行命令：ES_HOME/bin/service/elasticsearch start/stop/restart

在 bin 目录下执行./plugin install mobz/elasticsearch-head 来安装 head 插件



```
[root@slave1 bin]# ./plugin install mobz/elasticsearch-head
-> Installing mobz/elasticsearch-head...
Plugins directory [/opt/sxt/soft/elasticsearch-2.0.0/plugins] does not exist. Creating...
Trying https://github.com/mobz/elasticsearch-head/archive/master.zip ...
Downloading ..........................................................................................................
..........................................................................................................................
..........................................................................................................................
.........................................................................................DONE
Verifying https://github.com/mobz/elasticsearch-head/archive/master.zip checksums if available ...
NOTE: Unable to verify checksum for downloaded plugin (unable to find .sha1 or .md5 file to verify)
Installed head into /opt/sxt/soft/elasticsearch-2.0.0/plugins/head
[root@slave1 bin]# 
```

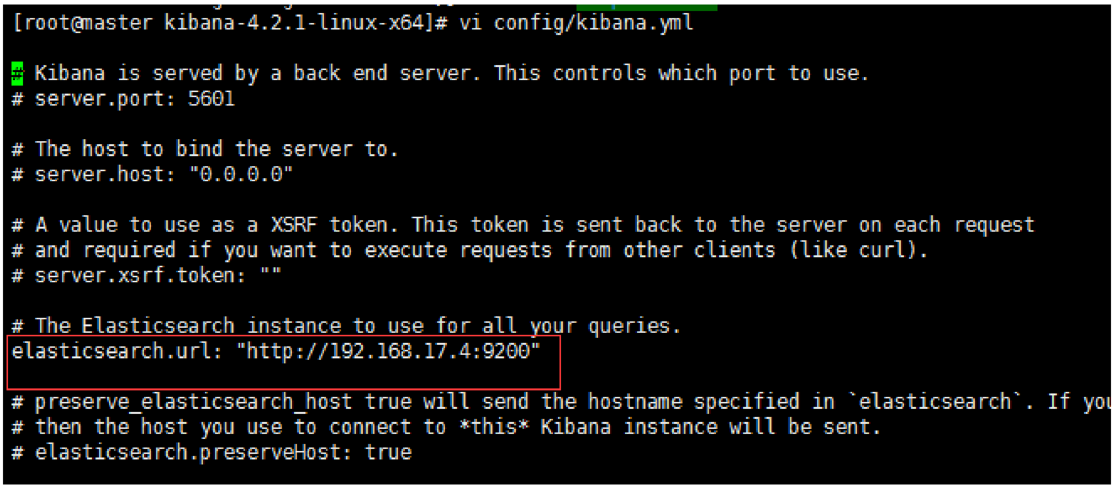
注意：因为 elasticsearch 有远程执行脚本的功能所以容易中木马病毒，所以不允许用 root 用户启动，root 用户是起不来的，赋权限，用一般的用户启动

要配置 network.host 和 network.publish_host 和 network.bind_host 才能别的机器或者网卡访问，否则只能是 127.0.0.1 或者 localhost 访问

注意配置 yml 结尾的配置文件都需要冒号后面加空格才行

三.　安装 Kibana

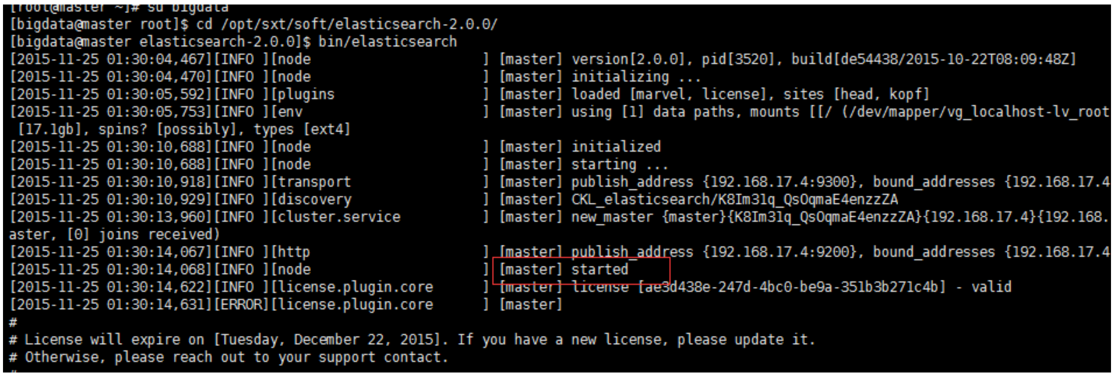
解压安装，修改配置文件 vi config/kibana.yml 的 elasticsearch.url 属性即可



```
[root@master kibana-4.2.1-linux-x64]# vi config/kibana.yml

# Kibana is served by a back end server. This controls which port to use.
# server.port: 5601

# The host to bind the server to.
# server.host: "0.0.0.0"

# A value to use as a XSRF token. This token is sent back to the server on each request
# and required if you want to execute requests from other clients (like curl).
# server.xsrf.token: ""

# The Elasticsearch instance to use for all your queries.
elasticsearch.url: "http://192.168.17.4:9200"

# preserve_elasticsearch_host true will send the hostname specified in `elasticsearch`. If you
# then the host you use to connect to *this* Kibana instance will be sent.
# elasticsearch.preserveHost: true
```

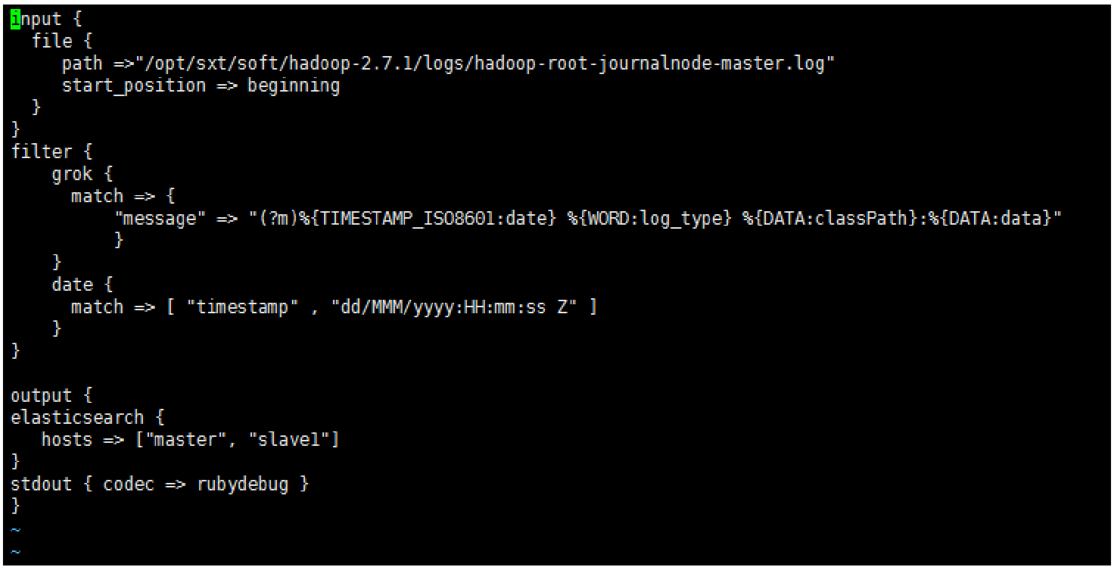
四. 测试

用非 root 用户启动 elasticsearch，



```
[root@master ~]# su bigdata
[bigdata@master root]$ cd /opt/sxt/soft/elasticsearch-2.0.0/
[bigdata@master elasticsearch-2.0.0]$ bin/elasticsearch
[2015-11-25 01:30:04,467][INFO ][node                     ] [master] version[2.0.0], pid[3520], build[de54438/2015-10-22T08:09:48Z]
[2015-11-25 01:30:04,470][INFO ][node                     ] [master] initializing ...
[2015-11-25 01:30:05,592][INFO ][plugins                  ] [master] loaded [marvel, license], sites [head, kopf]
[2015-11-25 01:30:05,753][INFO ][env                      ] [master] using [1] data paths, mounts [[/ (/dev/mapper/vg_localhost-lv_root
 [17.1gb], spins? [possibly], types [ext4]
[2015-11-25 01:30:10,688][INFO ][node                     ] [master] initialized
[2015-11-25 01:30:10,688][INFO ][node                     ] [master] starting ...
[2015-11-25 01:30:10,918][INFO ][transport                ] [master] publish_address {192.168.17.4:9300}, bound_addresses {192.168.17.4
[2015-11-25 01:30:10,929][INFO ][discovery                ] [master] CKL_elasticsearch/K8Im31q_QsOqmaE4enzzZA
[2015-11-25 01:30:13,960][INFO ][cluster.service          ] [master] new_master {master}{K8Im31q_QsOqmaE4enzzZA}{192.168.17.4}{192.168.
aster, [0] joins received)
[2015-11-25 01:30:14,067][INFO ][http                     ] [master] publish_address {192.168.17.4:9200}, bound_addresses {192.168.17.4
[2015-11-25 01:30:14,068][INFO ][node                     ] [master] started
[2015-11-25 01:30:14,622][INFO ][license.plugin.core      ] [master] license [ae3d438e-247d-4bc0-be9a-351b3b271c4b] - valid
[2015-11-25 01:30:14,631][ERROR][license.plugin.core      ] [master]
#
# License will expire on [Tuesday, December 22, 2015]. If you have a new license, please update it.
# Otherwise, please reach out to your support contact.
```

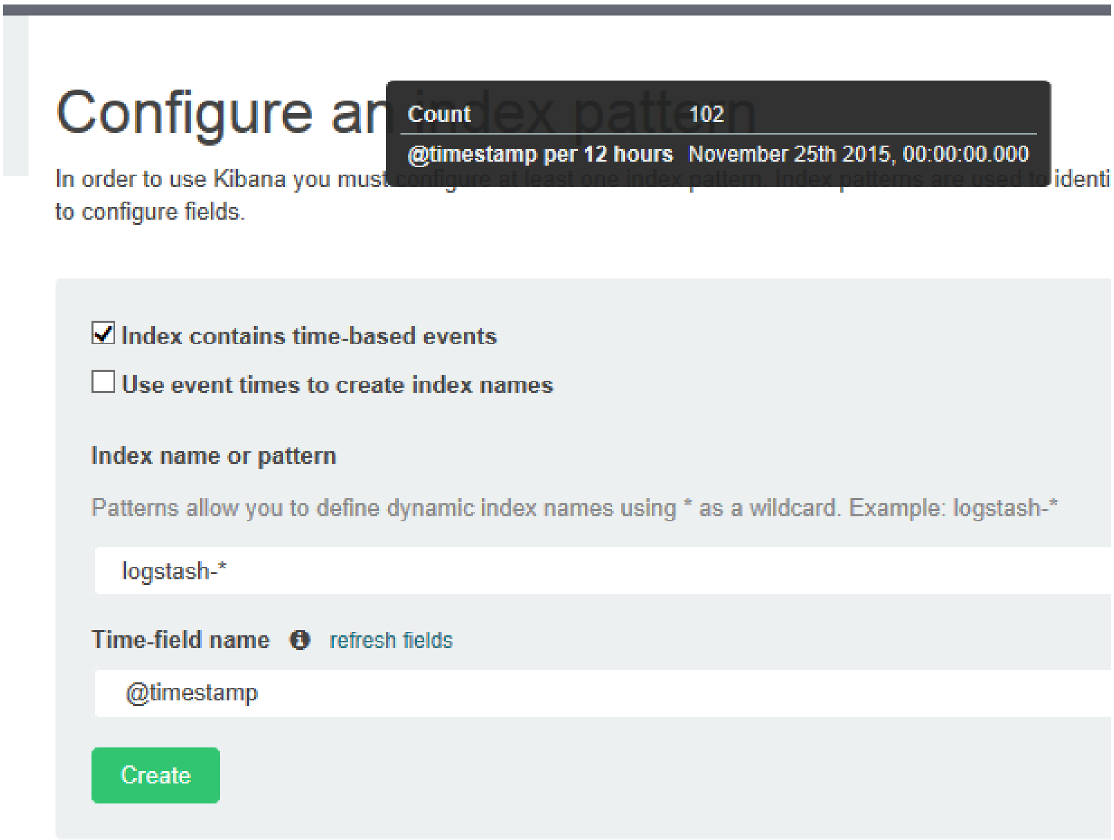
配置 logstash 的配置文件



```
input {
  file {
     path =>"/opt/sxt/soft/hadoop-2.7.1/logs/hadoop-root-journalnode-master.log"
     start_position => beginning
  }
}
filter {
    grok {
      match => {
          "message" => "(?m)%{TIMESTAMP_ISO8601:date} %{WORD:log_type} %{DATA:classPath}:%{DATA:data}"
          }
    }
    date {
      match => [ "timestamp" , "dd/MMM/yyyy:HH:mm:ss Z" ]
    }
}

output {
elasticsearch {
   hosts => ["master", "slave1"]
}
stdout { codec => rubydebug }
}
~
~
```

启动 kibana

访问 http://192.168.17.4:5601/创建索引



Configure an index pattern

Count 102

@timestamp per 12 hours November 25th 2015, 00:00:00.000

In order to use Kibana you must configure at least one index pattern. Index patterns are used to identi
to configure fields.

☑ Index contains time-based events

□ Use event times to create index names

Index name or pattern

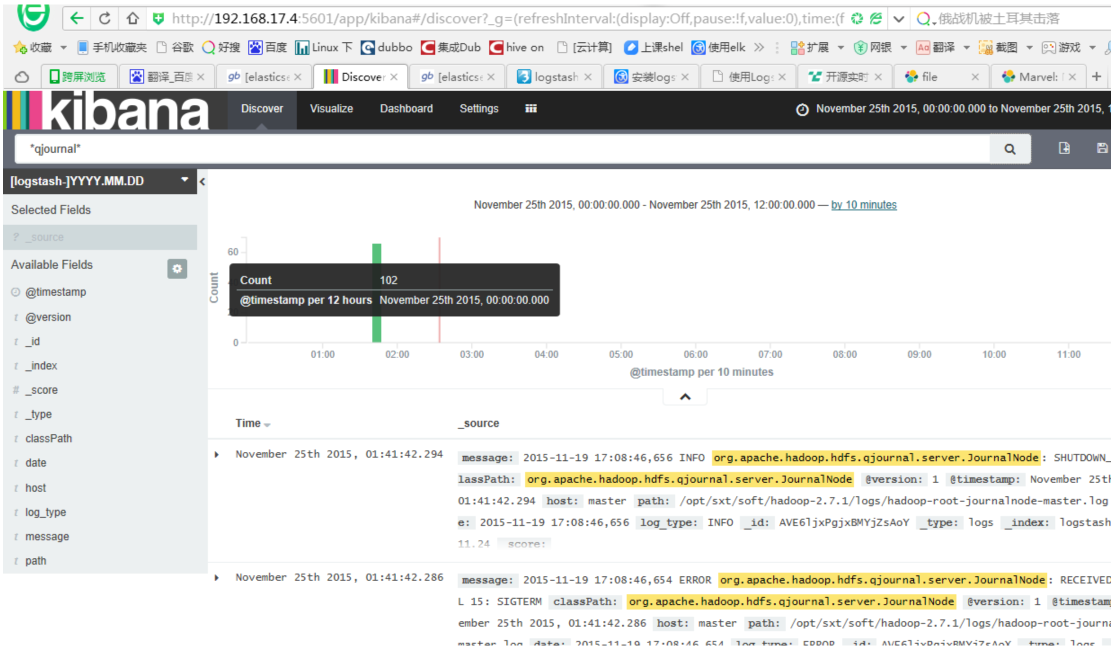
Patterns allow you to define dynamic index names using * as a wildcard. Example: logstash-*

logstash-*

Time-field name ℹ refresh fields

@timestamp

查询结果：



qjournal

[logstash-]YYYY.MM.DD

November 25th 2015, 00:00:00.000 - November 25th 2015, 12:00:00.000 — by 10 minutes

Count 102

@timestamp per 12 hours November 25th 2015, 00:00:00.000

```
Time                              _source
November 25th 2015, 01:41:42.294  message: 2015-11-19 17:08:46,656 INFO org.apache.hadoop.hdfs.qjournal.server.JournalNode: SHUTDOWN_
                                  lassPath: org.apache.hadoop.hdfs.qjournal.server.JournalNode @version: 1 @timestamp: November 25t
                                  01:41:42.294 host: master path: /opt/sxt/soft/hadoop-2.7.1/logs/hadoop-root-journalnode-master.log
                                  e: 2015-11-19 17:08:46,656 log_type: INFO _id: AVE6ljxPgjxBMYjZsAoY _type: logs _index: logstash
                                  11.24 _score:
November 25th 2015, 01:41:42.286  message: 2015-11-19 17:08:46,654 ERROR org.apache.hadoop.hdfs.qjournal.server.JournalNode: RECEIVED
                                  L 15: SIGTERM classPath: org.apache.hadoop.hdfs.qjournal.server.JournalNode @version: 1 @timestam
                                  ember 25th 2015, 01:41:42.286 host: master path: /opt/sxt/soft/hadoop-2.7.1/logs/hadoop-root-journa
                                  master.log date: 2015-11-19 17:08:46,654 log_type: ERROR _id: AVE6ljxPgjxBMYjZsAoX _type: logs
```