# 简介

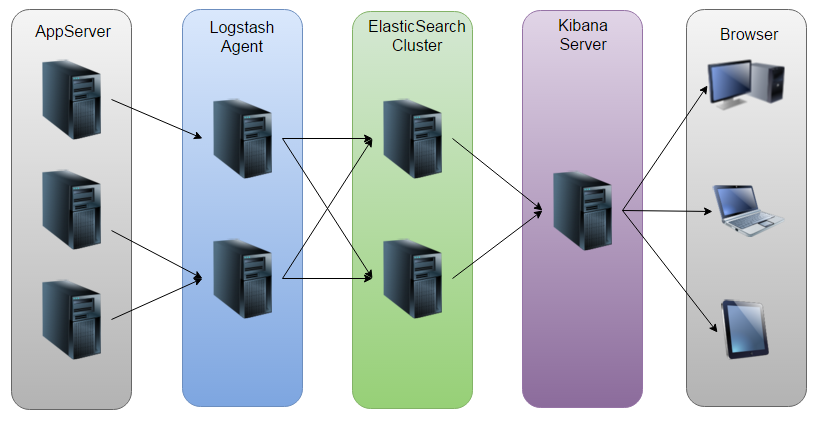
http://blog.chinaunix.net/uid-26168435-id-5759443.html

ELK由ElasticSearch、Logstash和Kiabana三个开源工具组成。

* Elasticsearch是个开源分布式搜索引擎，它的特点有：分布式，零配置，自动发现，索引自动分片，索引副本机制，restful风格接口，多数据源，自动搜索负载等。
* Logstash是一个完全开源的工具，他可以对你的日志进行收集、过滤，并将其存储供以后使用（如，搜索）。
* Kibana 也是一个开源和免费的工具，它可以为 Logstash 和 ElasticSearch 提供的日志分析友好的 Web 界面，可以帮助您汇总、分析和搜索重要数据日志。
* Logstash: logstash server端用来搜集日志；
* Elasticsearch: 存储各类日志；
* Kibana: web化接口用作查寻和可视化日志；

ELK工作流程

在需要收集日志的所有服务上部署logstash，作为logstash agent（logstash shipper）用于监控并过滤收集日志，将过滤后的内容发送到Redis，然后logstash indexer将日志收集在一起交给全文搜索服务ElasticSearch，可以用ElasticSearch进行自定义搜索通过Kibana 来结合自定义搜索进行页面展示。

* ELK工作的原理图：
* 
* 如图：Logstash收集AppServer产生的Log，并存放到ElasticSearch集群中，而Kibana则从ES集群中查询数据生成图表，再返回给Browser。

# 安装

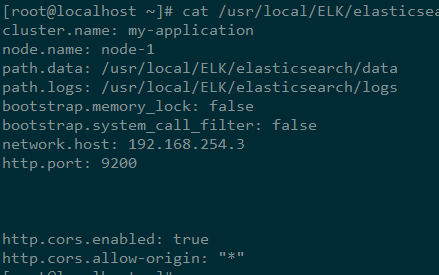
## elasticsearch

解压



配置vim elasticsearch.yml

sed -n '/^#/!p' /usr/local/ELK/elasticsearch/config/elasticsearch.yml



cluster.name: my-application # 设置ES集群的集群名称

node.name: node-1 #本台机器在集群中的名称

path.data: /usr/local/ELK/elasticsearch/data #设置ES存储data

path.logs: /usr/local/ELK/elasticsearch/logs #设置ES存储logs

network.host: 192.168.254.3 #访问地址

http.port: 9200 #访问端口

#以下两项设置es5.x版本的head插件可以访问es

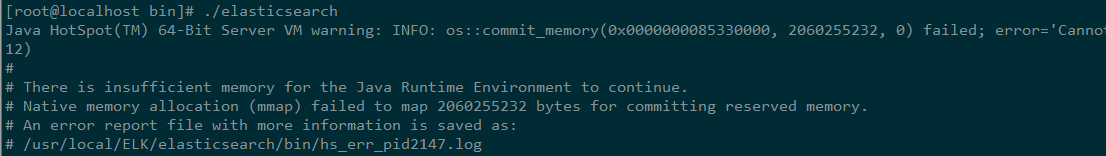
http.cors.enabled: true #开启跨域访问支持，默认为false

http.cors.allow-origin: "\*" #跨域访问允许的域名地址，使用正则表达式

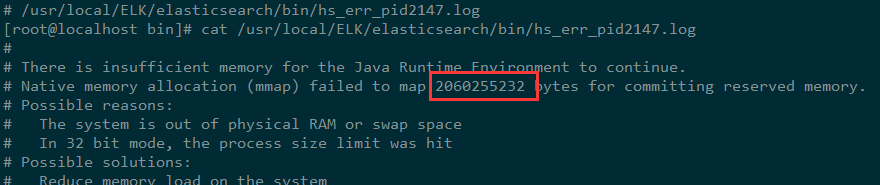
启动

进入bin目录，./elasticsearch启动

启动时报错



查看日志，显示需要2G的内存。

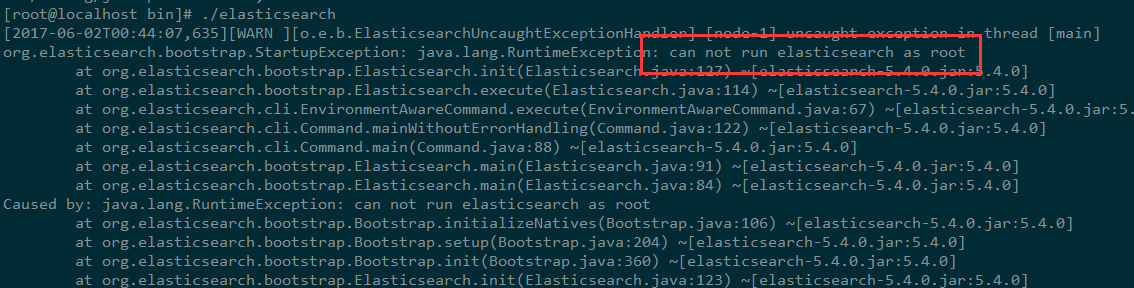


解决：因为elasticsearch5.0默认分配jvm空间大小为2g，修改jvm空间分配即可

config/jvm.options



再启动再报错

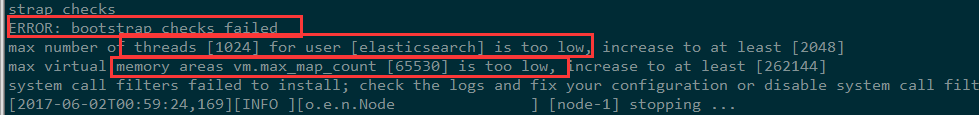


意思说不能用root直接启动elasticsearch。 ela2.0之后不能用root启动了。新建账号即可

useradd elasticsearch -s /bin/bash

chown -R elasticsearch.elasticsearch /usr/local/ELK/elasticsearch

su elasticsearch ./elasticsearch



解决方法

vi /etc/security/limits.conf

添加如下内容:

\* soft nofile 65536

\* hard nofile 131072

\* soft nproc 2048

\* hard nproc 4096

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

修改如下内容：

\* soft nproc 1024

#修改为

\* soft nproc 2048

vi /etc/sysctl.conf

添加下面配置：

vm.max\_map\_count=655360

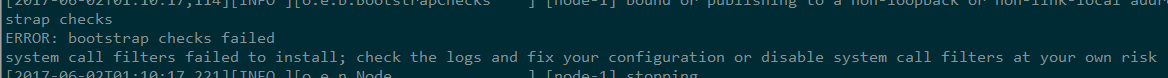
并执行命令：

sysctl -p

再次启动再次报错：

ERROR: bootstrap checks failed

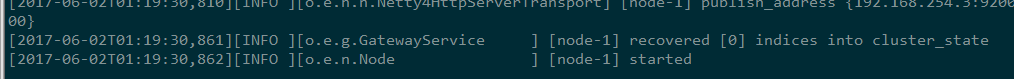
system call filters failed to install; check the logs and fix your configuration or disable system call filters at your own risk



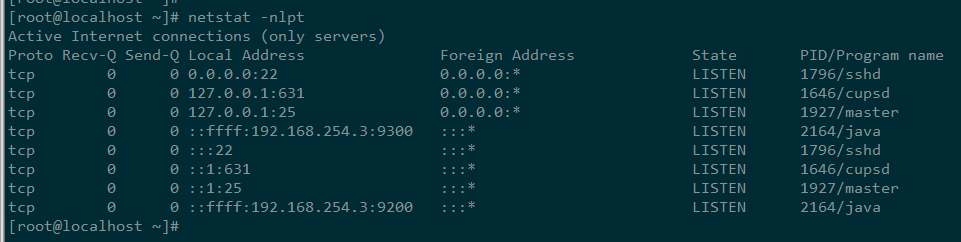
原因：因为Centos6不支持SecComp，而ES5.2.1默认bootstrap.system\_call\_filter为true进行检测，所以导致检测失败，失败后直接导致ES不能启动。

解决：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

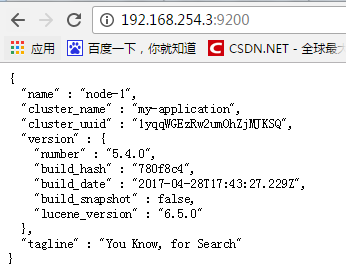
重启服务器再次启动成功



端口也在了



网页也打开了



## head插件（可以不装，不装忽略这一步骤）

Elasticsearch可以安装很多插件，接下来我们安装一个head插件，用于查看集群相关信息。

http://www.cnblogs.com/rethink-east/p/6547171.html

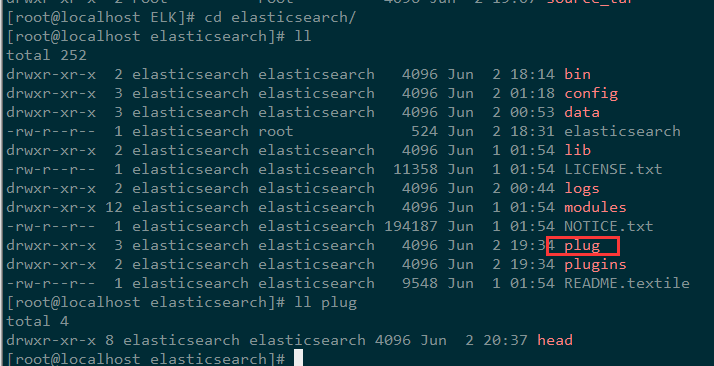
1.下载nodejs

wget [https://nodejs.org/dist/v4.6.1/node-v4.6.1-linux-x64.tar.gz](https://nodejs.org/dist/v4.6.1/node-v4.6.1-linux-x64.tar.gz%EF%BC%88linux%E5%91%BD%E4%BB%A4%E7%9B%B4%E6%8E%A5%E4%B8%8B%E8%BD%BD%EF%BC%89)

2.解压后添加环境变量

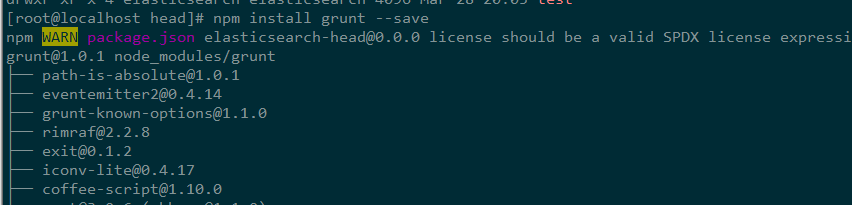
export PATH=/usr/local/node-v4.6.1-linux-x64/bin:$PATH

3.在elasticsearch中新建plug目录，然后下载elasticsearch-head-master.zip解压到elasticsearch/plug目录中，并重命名为head



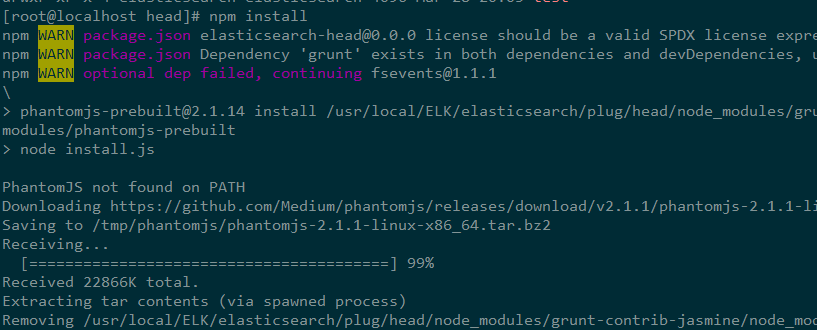
4.cd到elasticsearch/plug/head插件目录查看目录下有无node\_modules/grunt目录：

没有：执行命令创建：npm install grunt –-save



5. 安装head插件：

npm install

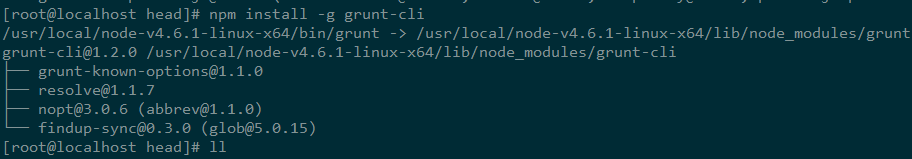


6. 安装grunt：

#grunt是一个方便的构建工具，可以进行打包压缩、测试、执行等等的工作，5.x里的head插件就是通过grunt启动的；

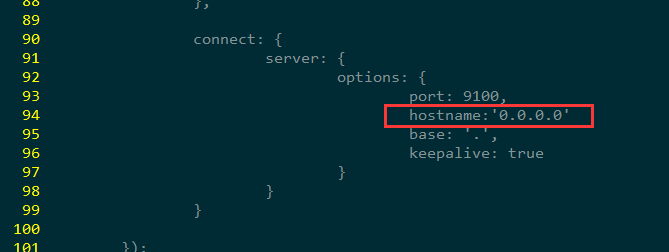
#”-g”参数代表全局安装，一般安装到nodejs的”lib/node\_modules”目录下；不带参数”-g”，则是本地安装，一般安装到运行npm命令时所在的目录，这里就需要安装到head插件目录；

npm install -g grunt-cli



7. 编辑Gruntfile.js

文件93行添加hostname:’0.0.0.0’ 确保能被访问。



8. **检查head根目录下是否存在base文件夹**

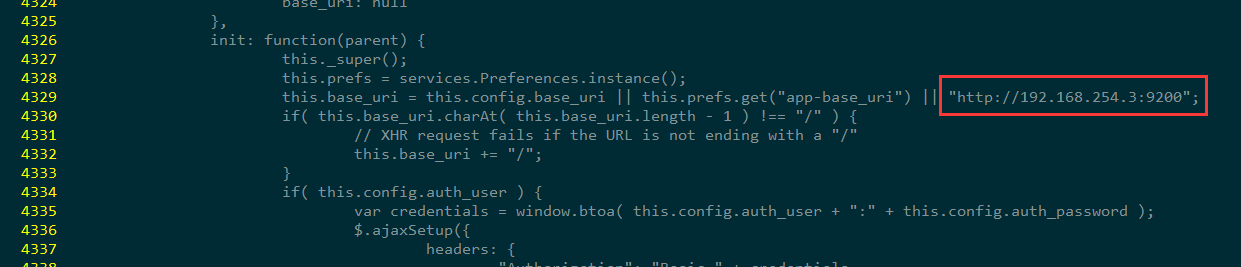
**没有：将 \_site下的base文件夹及其内容复制到head根目录下**



9.配置app.js

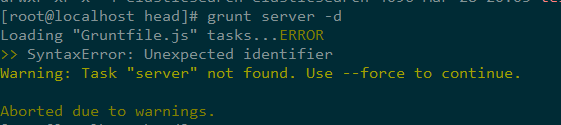
cp app.js app.js.bak && vi app.js

#在4328行将原"http://localhost:9200"修改为"http://192.168.254.3:9200"，否则head插件不能获取节点状态信息。

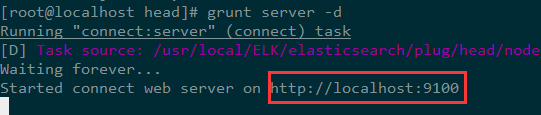


9. 启动grunt server：

运行grunt server -d启动head插件



原因是添加hostname:’0.0.0.0’ 后面没加逗号，加上即可，再次启动

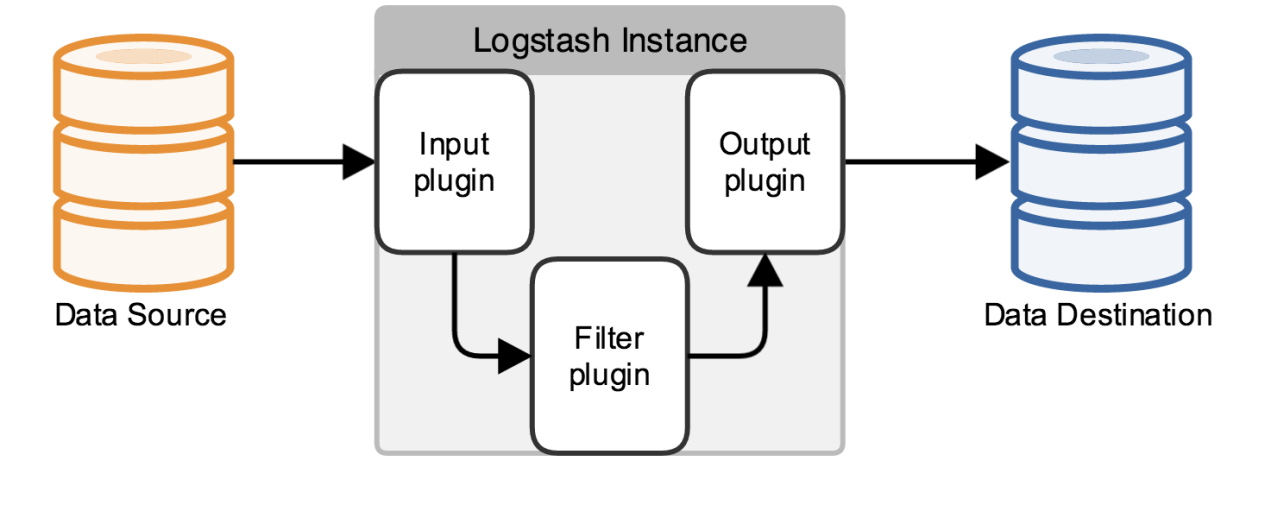


10．访问head插件：

<http://localhost:9100>



## Logstash



由于Logstash的运行依赖于Java环境， 而Logstash 1.5以上版本不低于java 1.8，因此推荐使用最新版本的Java。因为我们只需要Java的运行环境，所以可以只安装JRE，不过这里我依然使用JDK。

JDK JRE区别

JDK=JRE+开发工具集（例如javac编译工具等）  
JRE=JVM+java SE标准类库

Logstash是一个收集器，我们需要为它指定Input和Output（当然Input和Output可以为多个）。由于我们需要把Java代码中Log4j的日志输出到ElasticSearch中，因此这里的Input就是Log4j，而Output就是ElasticSearch。



### pipeline文件

pipeline名字和位置可以随意，这里我放在config目录下，取名为log4j-message.conf

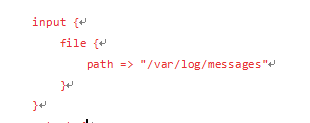
input {

    file {

        path => "/var/log/messages"

    }

}



output {

    elasticsearch {

        hosts => ["192.168.254.3:9200"] #把本机日志信息发往elasticsearch主机

        index => "messages-%{+YYYY.MM.dd}"

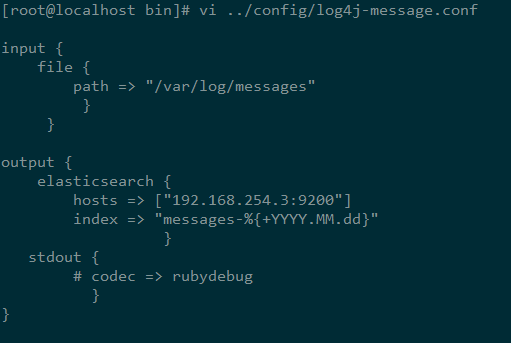
    }

    stdout {

# codec => rubydebug

    }

}



#pipeline实例文件以”input”，”output”，”filter”等区域组成，前两者为必选项；

Input就是收集哪个日志文件信息

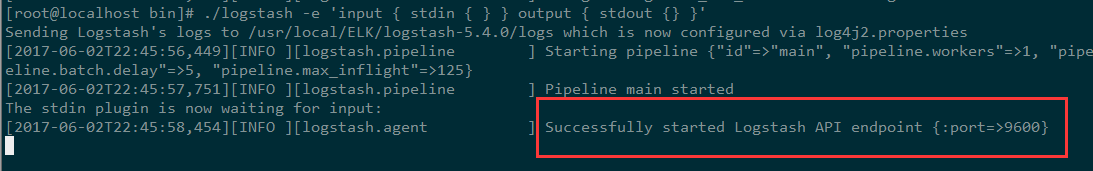
Output就是把收集的日志文件信息格式化输出

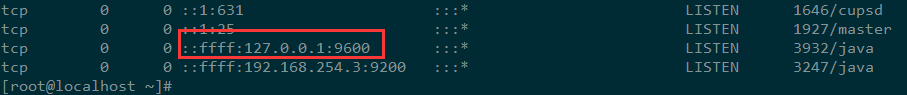
#codec => rubydebug会产生大量的debug文件至message（也可重定向到其他位置），此处注释掉；

#请注意权限，这里message常规权限是400，logstash无法读取，如果无法调用，在logstash的启动日志中会有相应的记录。

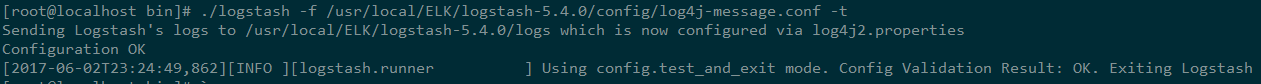
简单测试logstash是否安装成功

bin/logstash -e 'input { stdin { } } output { stdout {} }'

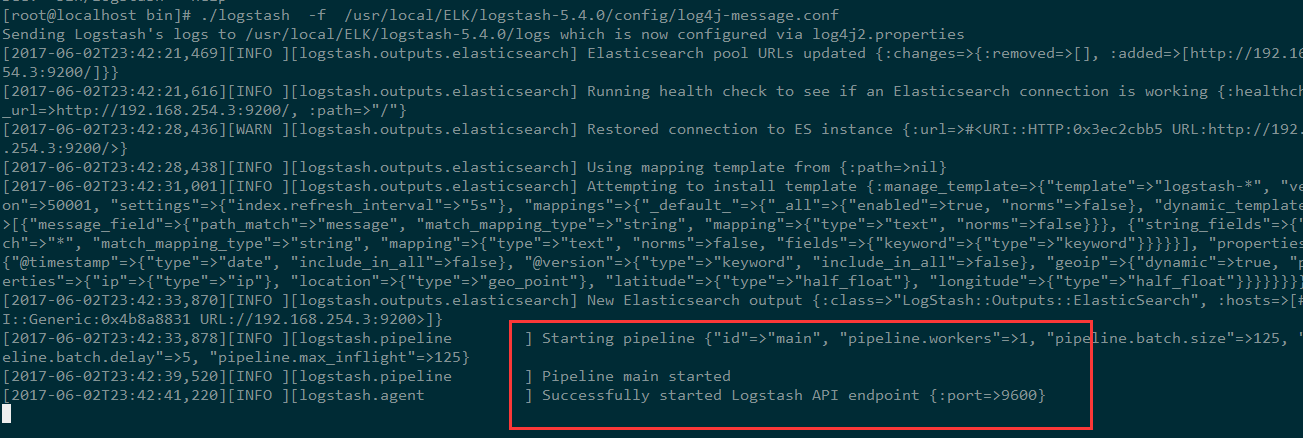




启动前检测配置文件

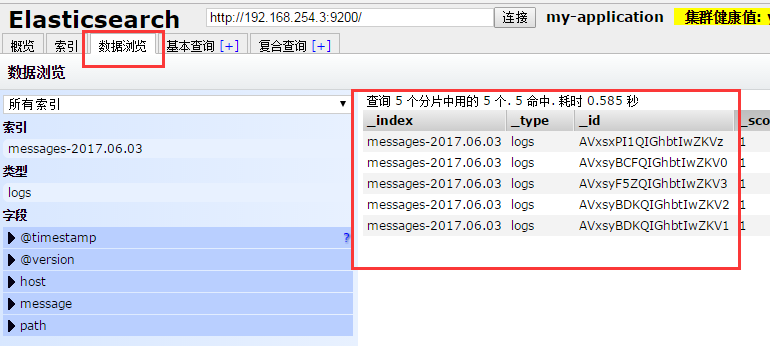
./logstash -f /usr/local/ELK/logstash-5.4.0/config/log4j-message.conf -t 

检测无问题，启动

./logstash -f /usr/local/ELK/logstash-5.4.0/config/log4j-message.conf 

登录<http://192.168.254.3:9100/>，一切ok

能看到收集到的日志了。



## Kibana

tar zxf kibana-5.4.0-linux-x86\_64.tar.gz

mv kibana-5.4.0-linux-x86\_64 kibana-5.4.0

vi config/kibana.yml

server.port: 5601

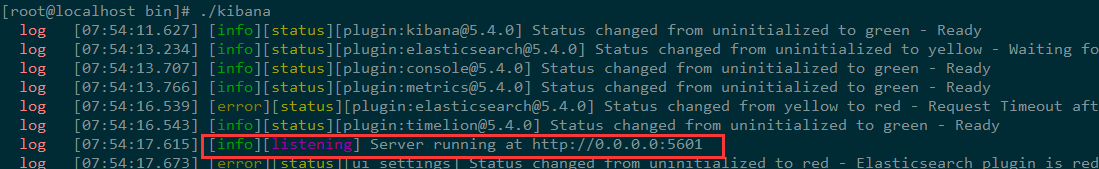
server.host: "0.0.0.0" #允许被访问的地址

elasticsearch.url: <http://192.168.254.3:9200> # elasticsearch服务器的地址

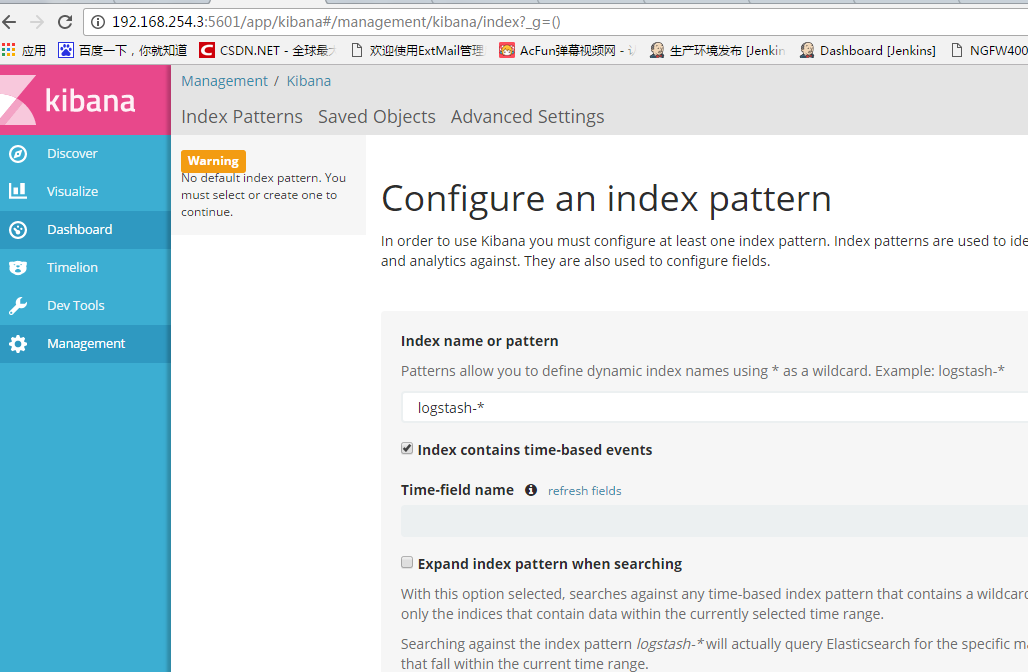
kibana.index: ".kibana"

启动

./kibana



访问这个地址 <http://192.168.254.3:5601/> 能打开网页表示ELK已经正常配置了



### 配置kibana

大体步骤：

      1.加载案例数据到你安装的Elasticsearch中

          2. 定义至少一个索引匹配模式

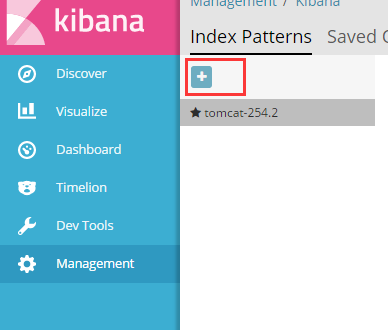
          3.使用Discover功能探索你的数据

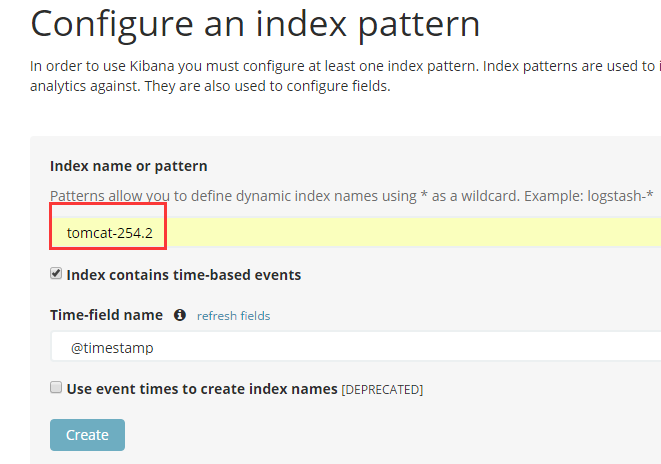
         4.建立一个visualization图形化地展示你的数据

       5.把许多visualization汇编组装成一个Dashboard

1. 加载数据

Management





为了后续使用Kibana，需要配置至少一个Index名字或者Pattern，它用于在分析时确定ES中的Index。这里我输入之前配置的Index名字Index就是之前logstash里配置的

，Kibana会自动加载该Index下doc的field，并自动选择合适的field用于图标中的时间字段。

1. 添加至少一个索引

这里的索引是在logstash里配置的

# 各个启动命令

su elasticsearch -c ./elasticsearch # elasticsearch/bin目录下启动

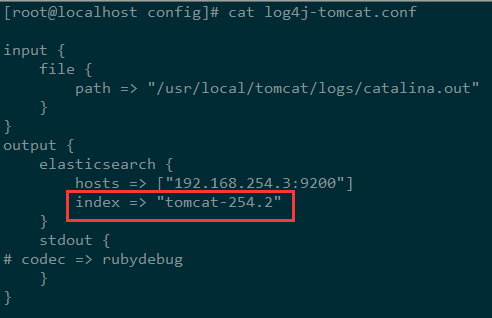
grunt server –d # /usr/local/ELK/elasticsearch/plug/head/node\_modules/grunt/bin目录下启动

./logstash -f /usr/local/ELK/logstash-5.4.0/config/log4j-message.conf # logstash目录下启动

./kibana #启动kibana

# 添加其他logstash服务器

在需要监控日志的服务器上安装logstash，然后添加配置：



启动logstash

登录<http://192.168.254.3:9100/>添加一个索引即可



删除索引：

curl -XDELETE 'http://192.168.254.3:9200/tomc\*' # tomc\*为需要删除的索引名