**ELK日志监控分析平台搭建**

目录

[简介 1](#_Toc3023258)

[一、部署ElasticSearch 2](#_Toc3023259)

[1.安装 2](#_Toc3023260)

[2.启动 2](#_Toc3023261)

[二、部署kibana 3](#_Toc3023262)

[1.安装 3](#_Toc3023263)

[2.启动 3](#_Toc3023264)

[三、部署logstash 4](#_Toc3023265)

[1.安装 4](#_Toc3023266)

[2.启动 4](#_Toc3023267)

[四、部署filebeat 5](#_Toc3023268)

[1.安装 5](#_Toc3023269)

[2.启动 6](#_Toc3023270)

[五、kibana UI界面简介 6](#_Toc3023271)

[1.访问kibana界面 6](#_Toc3023272)

# 简介

ELK是一套完整的日志解决方案，由ElasticSearch、Logstash、 Kibana  
这三款开源软件组成。

* EastiSearch是基于Lucene开发的分布式存储检引擎，用来存储各类日志;
* Logstash对日志进行收集、分析，并将其存储供以后使用:
* Kibana 是基于Node.js开发的展示工具，为Logstah和ElasticSearch提供用于日志展示的Web界面，还用于帮助汇总、分析和搜索重要日志数据。
* 在所有需要收集日志的服务上部署Logstash（可以使用轻量级的filebeat进行收集）,作为署Logstash agent用于监控并过滤所收集的日志，将过滤后的内容整合在一起，最终全部交给EastiSearch检索引擎；
* 用EastiSearch进行自定义检索;
* 再通过Kibana通过结合自定义检索内容生成图表，进行日志数据展示

# 一、**部署ElasticSearch**

## 1.安装

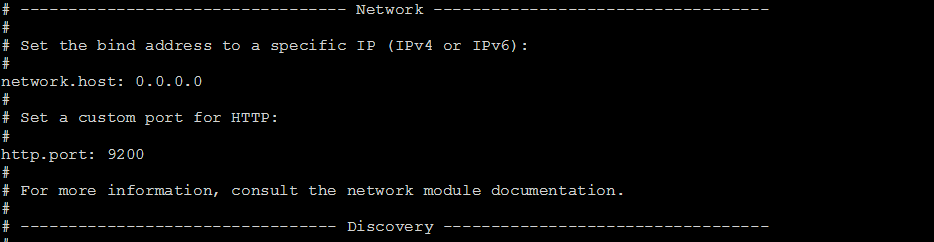
* 安装JDK
* 解压Elasticsearch安装包



* 修改elasticsearch.yml

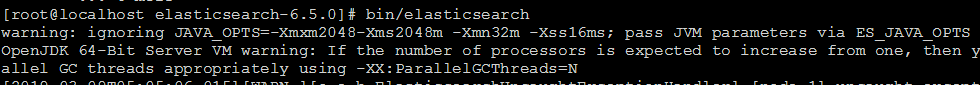
Network.host:设置为elasticsearch部署的主机ip

http.port: 9200

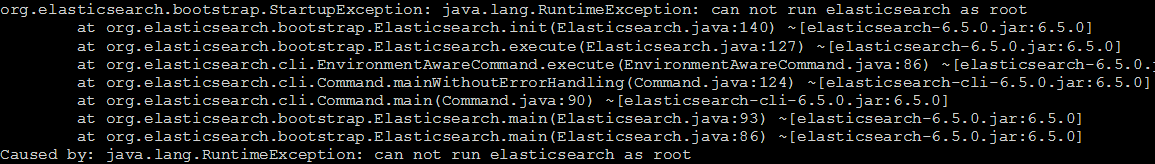


## 2.启动

进入elasticsearch的解压目录，”bin/elasticsearch”启动：



注：如果有一下错误，切换为非root用户启动



# 二、部署kibana

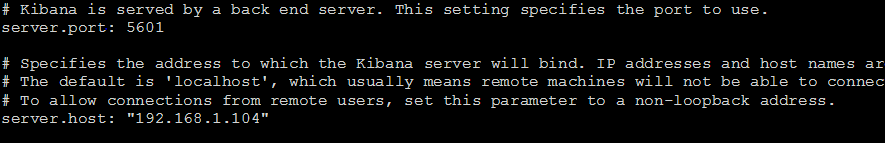
## 1.安装

* 解压kibana安装包
* 修改kibana.yml

server.host:设置为kibana部署的主机ip

server.port: 9200

其他根据需求修改



## 2.启动

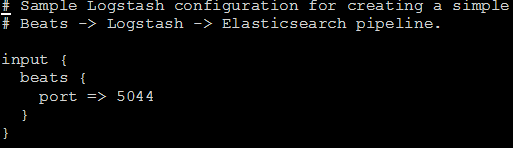
进入kibana的解压目录，命令”bin/kibana”启动

# 三、部署logstash

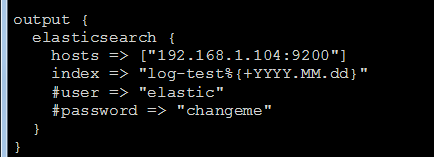
## 1.安装

* 解压logstash安装包
* bin目录下创建logstash启动的.conf配置文件，文件名自取，如：logstash-start.conf

配置input为filebeat收集日志，端口为5044：

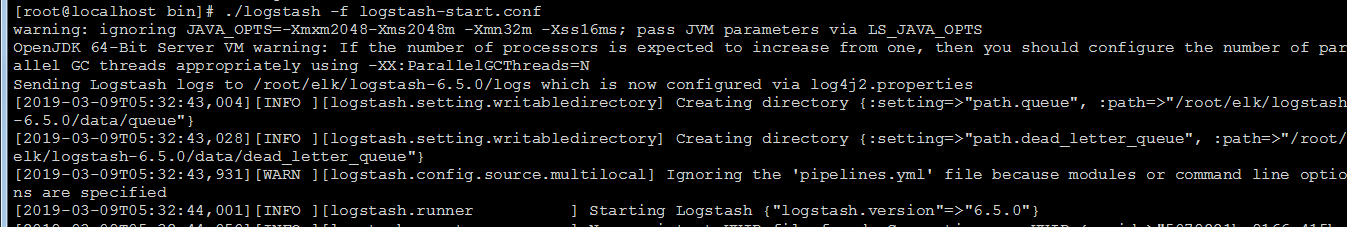


配置output：elasticsear的地址和索引



## 2.启动

进入logstash的bin目录，命令 启./logstash -f logstash-start.conf动



# 四、部署filebeat

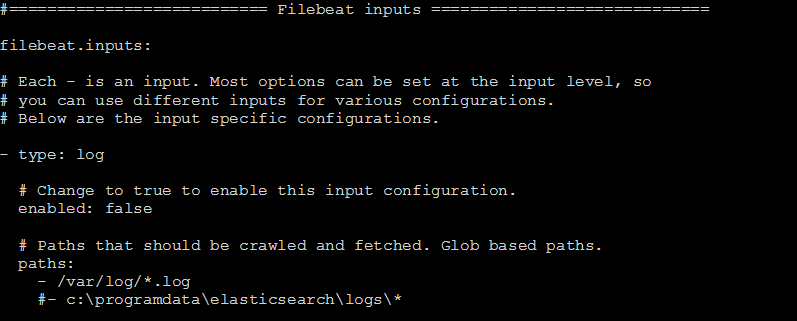
说明：在需要收集日志的客户端安装filebeat,filebeat再将日志传输至logstash

## 1.安装

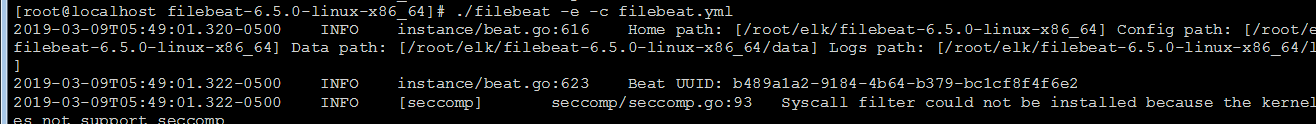
* 解压filebeat安装包
* 配置filebeat

配置inputs:

Paths:采集日志的路径，可以配置多个



## 2.启动

进入filebea解压目录，命令 ./filebeat -e -c filebeat.yml启动

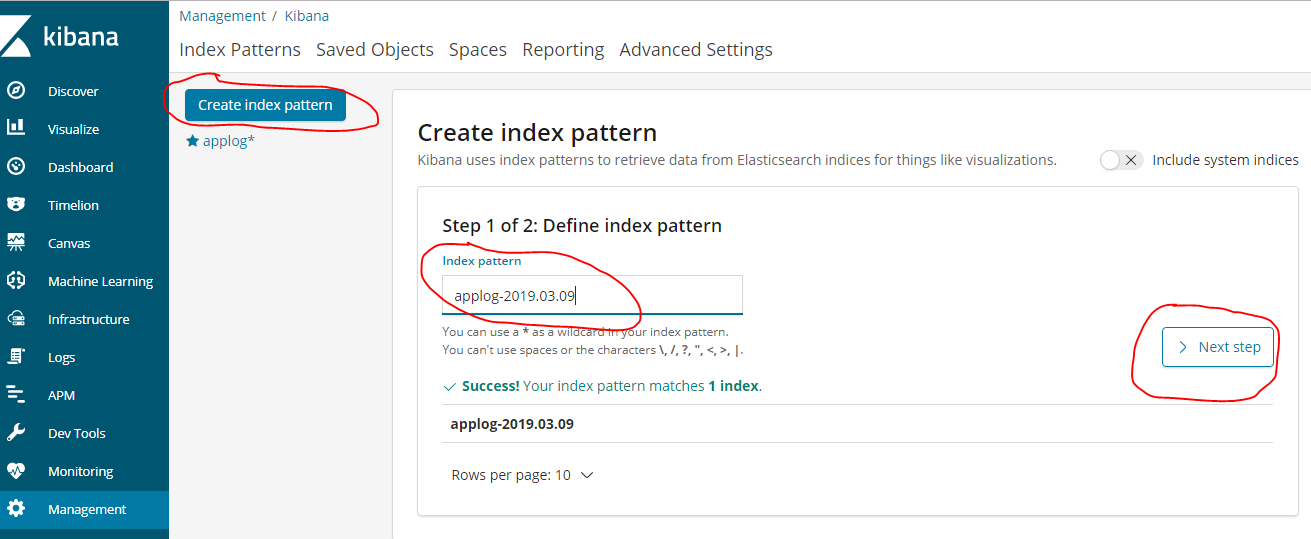
# 五、kibana UI界面简介

## 1.访问kibana界面

浏览器：ip:5601

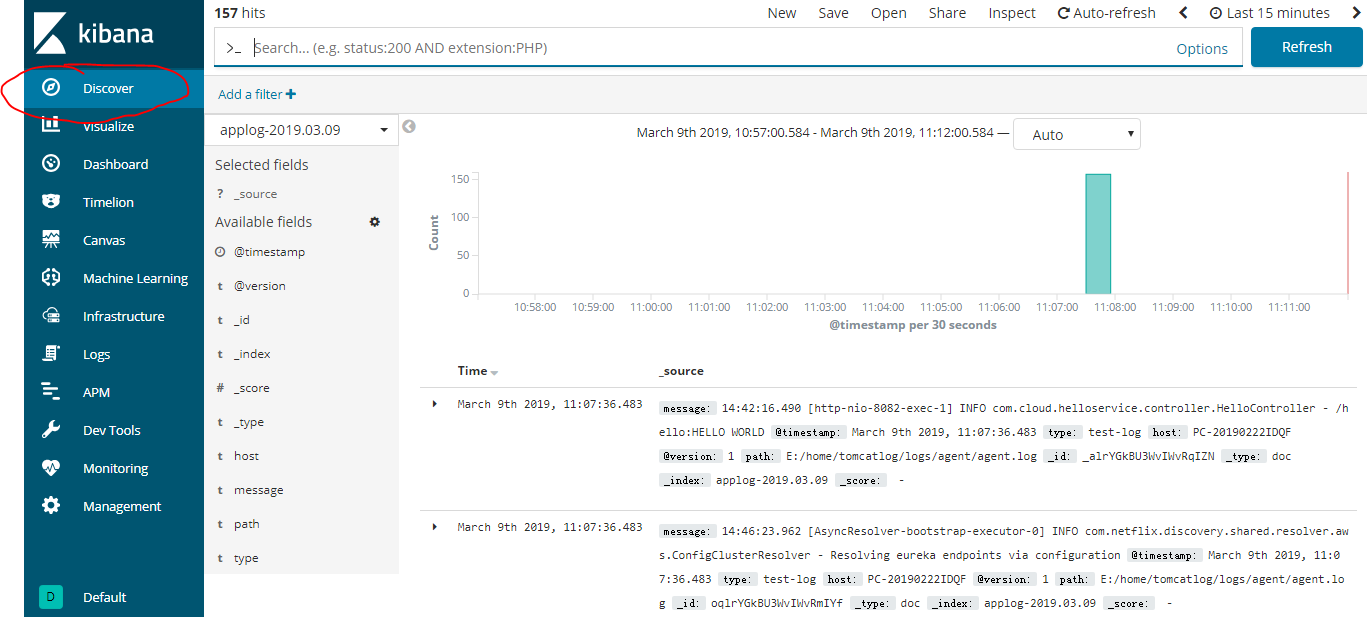
2.创建索引

Management -> Creat index pattern



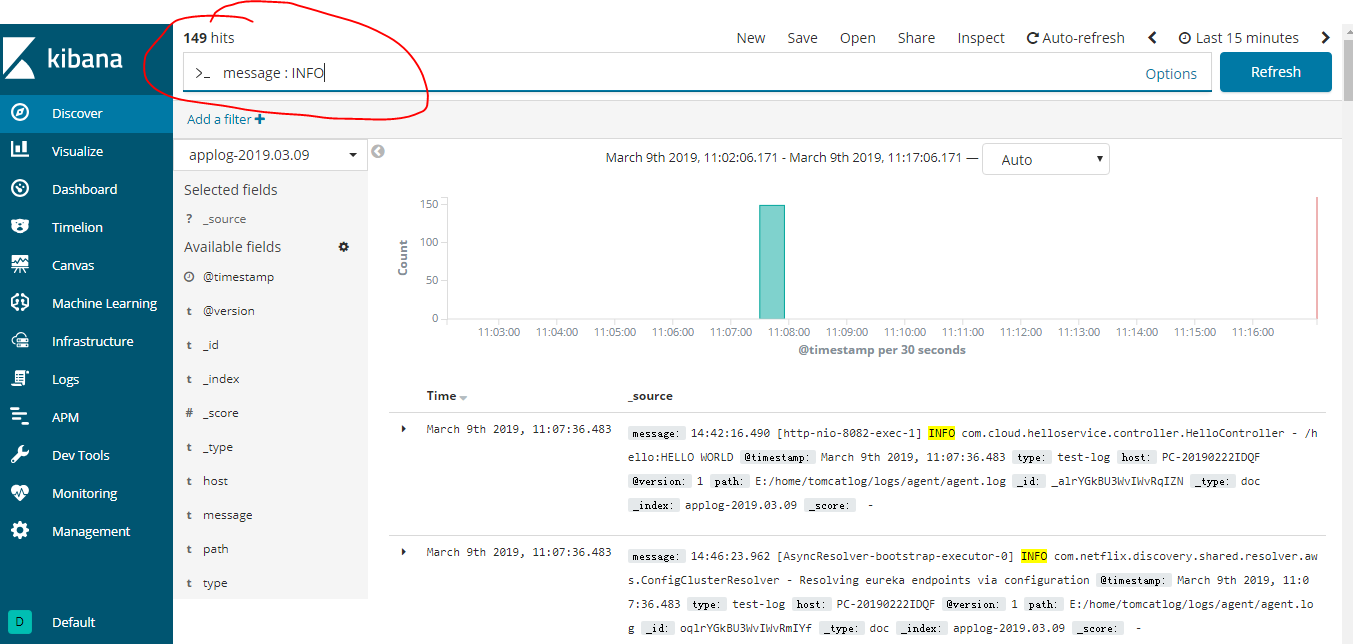
3.查看日志

进入Discovery 选择创建的索引查看日志：



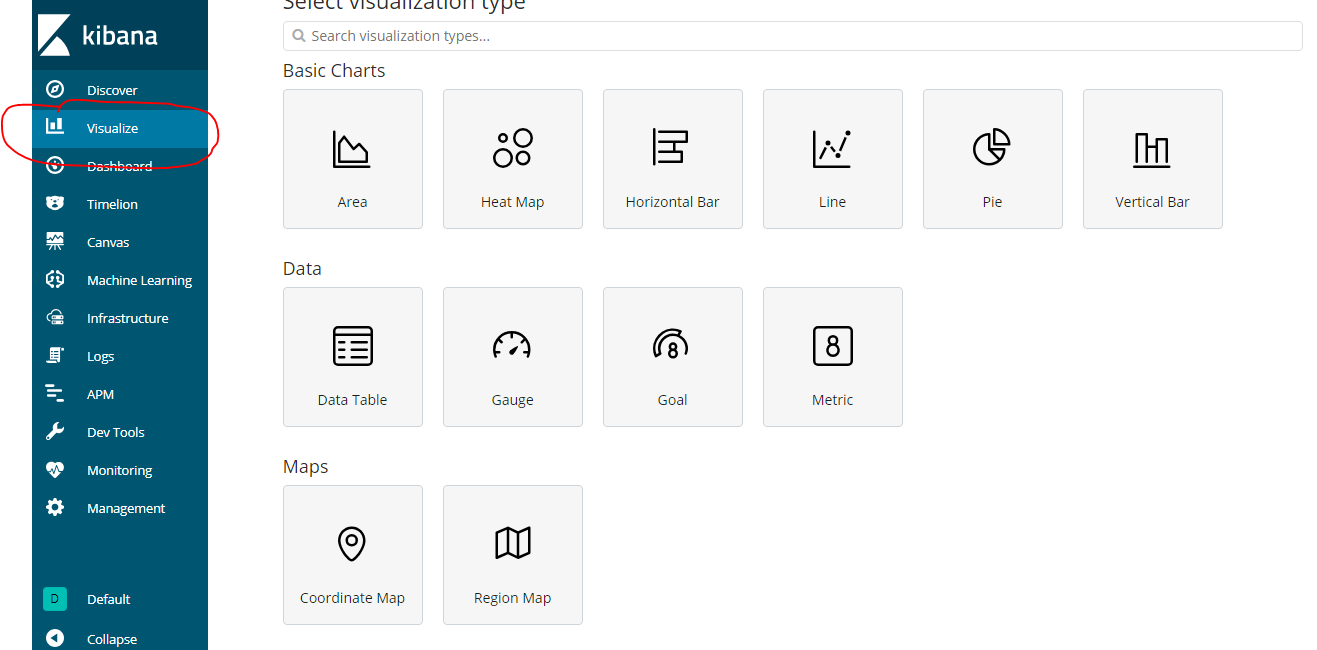
4.搜索日志

搜索栏输入搜索条件进行查询：



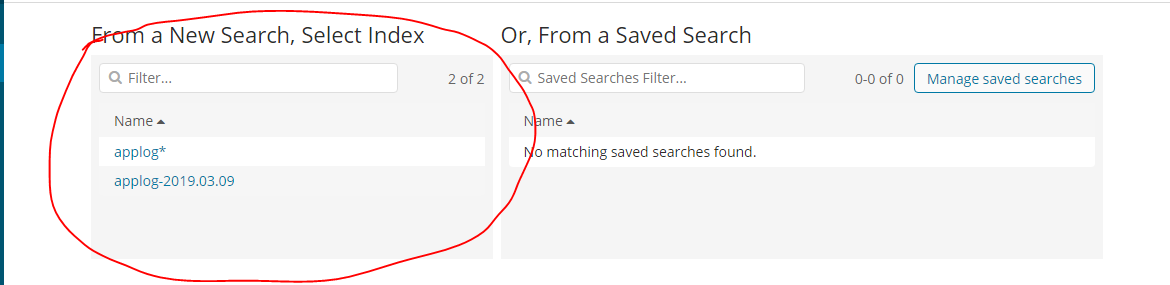
5.生成日志的分析图表

在Visualize栏点击创建需要的图表：



如生成饼状图Pie:

选择日志索引



选择字段和属性：

