# centos7搭建EFK日志分析系统

#### 前言

EFK可能都不熟悉，实际上EFK是大名鼎鼎的日志系统ELK的一个变种

在没有分布式日志的时候，每次出问题了需要查询日志的时候，需要登录到Linux服务器，使用命令cat -n xxxx|grep xxxx 搜索出日志在哪一行，然后cat -n xxx|tail -n +n行|head -n 显示多少行，这样不仅效率低下，而且对于程序异常也不方便查询，日志少还好，一旦整合出来的日志达到几个G或者几十G的时候，仅仅是搜索都会搜索很长时间了，当然如果知道是哪天什么时候发生的问题当然也方便查询，但是实际上很多时候有问题的时候，是不知道到底什么时候出的问题，所以就必须要在聚合日志中去搜索（一般日志是按照天来分文件的，聚合日志就是把很多天的日志合并在一起，这样方便查询），而搭建EFK日志分析系统的目的就是将日志聚合起来，达到快速查看快速分析的目的，使用EFK不仅可以快速的聚合出每天的日志，还能将不同项目的日志聚合起来，对于微服务和分布式架构来说，查询日志尤为方便，而且因为日志保存在Elasticsearch中，所以查询速度非常之快

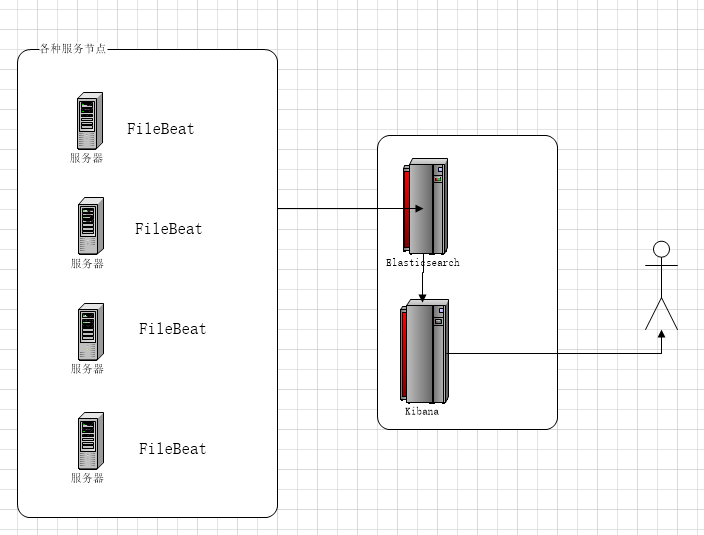
#### 认识EFK

EFK不是一个软件，而是一套解决方案，并且都是开源软件，之间互相配合使用，完美衔接，高效的满足了很多场合的应用，是目前主流的一种日志系统。EFK是三个开源软件的缩写，分别表示：Elasticsearch , FileBeat, Kibana , 其中ELasticsearch负责日志保存和搜索，FileBeat负责收集日志，Kibana 负责界面,当然EFK和大名鼎鼎的ELK只有一个区别，那就是EFK把ELK的Logstash替换成了FileBeat，因为Filebeat相对于Logstash来说有2个好处：  
1、侵入低，无需修改程序目前任何代码和配置  
2、相对于Logstash来说性能高，Logstash对于IO占用很大

当然FileBeat也并不是完全好过Logstash，毕竟Logstash对于日志的格式化这些相对FileBeat好很多，FileBeat只是将日志从日志文件中读取出来，当然如果你日志本身是有一定格式的，FileBeat也可以格式化，但是相对于Logstash来说，还是差一点

* 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。
* Filebeat隶属于Beats。目前Beats包含六种工具：  
  Packetbeat（搜集网络流量数据）  
  Metricbeat（搜集系统、进程和文件系统级别的 CPU 和内存使用情况等数据）  
  Filebeat（搜集文件数据）  
  Winlogbeat（搜集 Windows 事件日志数据）  
  Auditbeat（ 轻量型审计日志采集器）  
  Heartbeat（轻量级服务器健康采集器）
* Kibana 也是一个开源和免费的工具，它Kibana可以为 Logstash 、Beats、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。

**EFK架构图**



**安装Elasticsearch**

1. 首先安装jdk，下载好jdk后解压并配置环境变量

Shell > tar zxf jdk-8u101-linux-x64.tar.gz

Shell > vim /etc/profile //添加如下参数

export JAVA\_HOME=/usr/local/java/jdk1.8.0\_101

export CLASSPATH=.:$JAVA\_HOME/lib/dt.jar:$JAVA\_USR/lib/tools.jar

export PATH=$PATH:$JAVA\_HOME/bin

Shell > source /etc/profile //是配置生效

Shell > java -version //查看java版本

1. 下载Elasticsearch，本文以Elasticsearch6.3.0为例，当前Elasticsearch最新版本为Elasticsearch6.4.0，注意Elasticsearch、Kibana、FileBeat一定要使用相同的版本

Shell > wget \

<https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-6.3.0.tar.gz>

2.1 解压安装包

Shell > tar -zxvf /usr/local/src/elasticsearch-6.3.0.tar.gz -C /usr/local/

2.2 编辑配置文件

Shell > vim /usr/local/elasticsearch-6.3.0/config/elasticsearch.yml

做以下修改：

path.data: /data/es-data

path.logs: /var/log/es-log

network.host:0.0.0.0

http.port: 9200

1. 修改系统参数

3.1设置内核参数

Shell > vim /etc/sysctl.conf 增加以下参数：

vm.max\_map\_count=655360

执行以下命令，确保配置生效：

Shell > sysctl –p

3.2设置资源参数

Shell > vim /etc/security/limits.conf

# 修改

soft nofile 65536

hard nofile 131072

soft nproc 65536

hard nproc 131072

3.3 设置用户资源参数：

Shell > vim /etc/security/limits.d/20-nproc.conf

# 设置elk用户参数

elk soft nproc 65536

1. 添加启动用户，设置权限

由于Elasticsearch不能使用root用户打开，所以需要专门创建一个用户来启动Elasticsearch

Shell > useradd elk

Shell > mkdir –p /data/es-data //创建数据目录

Shell > mkdir –p /var/log/es-log //创建日志目录

Shell > chown –R elk:elk /data/es-data

Shell > chown –R elk:elk /var/log/es-log

Shell > chown –R elk:elk /usr/local/elasticsearch-6.3.0

4.1 启动ES

使用elk用户启动elasticsearch 服务

切换至elk用户

Shell > su elk

Shell > cd /usr/local/elasticsearch-6.3.0

Shell > nohup /bin/elasticsearch &

关于ES内存设置，在es目录下/bin/elasticsearch 6.3.0版本是直接在es目录下的config/jvm.options 配置置即可，其他版本未知

**安装kibana**

1. 首先安装jdk，下载好jdk后解压并配置环境变量
2. 下载kibana

Shell > wget \

https://artifacts.elastic.co/downloads/kibana/kibana-6.3.0-linux-x86\_64.tar.gz

1. 解压kibana

Shell > tar zxvf /usr/local/src/kibana-6.3.0-linux-x86\_64.tar.gz –C /usr/local

3.1 修改配置文件

Shell > vim /usr/local/kibana-6.3.0-linux-x86\_64/config/kibana.yml

修改以下参数

server.port: 5601 #开启默认端口5601

server.host: “0.0.0.0’ #站点地址

elasticsearch.url:http://ip:9200 #指向elasticsearch服务的ip地址

kibana.index: “.kibana”

3.2 后台启动：

Shell > nohup /bin/kibana &

#/usr/local/src/kibana-6.3.0-linux-x86\_64/

#### **安装FileBeat**

Filebeat 是基于 logstash-forwarder 的源码改造而成，用 Golang 编写，无需依赖 Java 环境，效率高，占用内存和 CPU 比较少，非常适合作为 Agent 跑在服务器上。

Filebeat我们部署到每个java微服务机器上收集日志

在filebeat.yml配置文件中指定输出到ES中，然后通过kibana来看日志

1. 下载filebeat

Shell > wget \

https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-6.3.0-linux-x86\_64.tar.gz

1. 解压

Shell > tar zxf filebeat-6.3.0-linux-x86\_64.tar.gz

1. 进入到主目录，修改配置文件

Shell > cd /usr/local/src/filebeat-6.3.0-linux-x86\_64

Shell > vim filebeat.yml

修改如下配置：

==========Filebeat inputs===== 配置

enabled: false //false 改为 true

paths:

-/var/log/\*.log //收集日志的路径

multiline.pattern: ^\[ //取消#注释

multiline.negate: false //取消#注释，把false 改为 true

multiline.match: after //取消#注释

==========Elasticsearch output ====配置

setup.template.name: 索引名 默认是metricbeat

setup.template.pattern: 索引模式 默认模式是metricbeat-\*

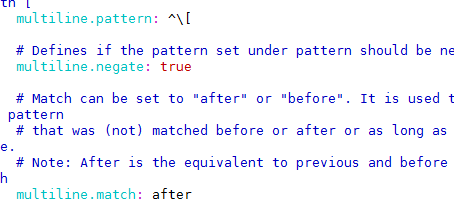
output.elasticsearch:

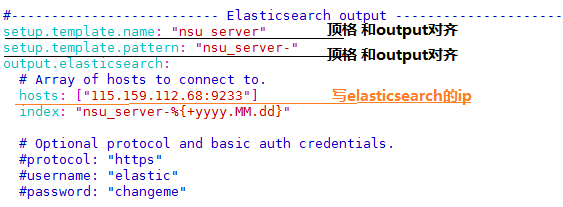
hosts: ["115.159.112.68:9233"] elasticsearch ip

index: "nsu\_server-%{+yyyy.MM.dd}"

配置文件图如下：







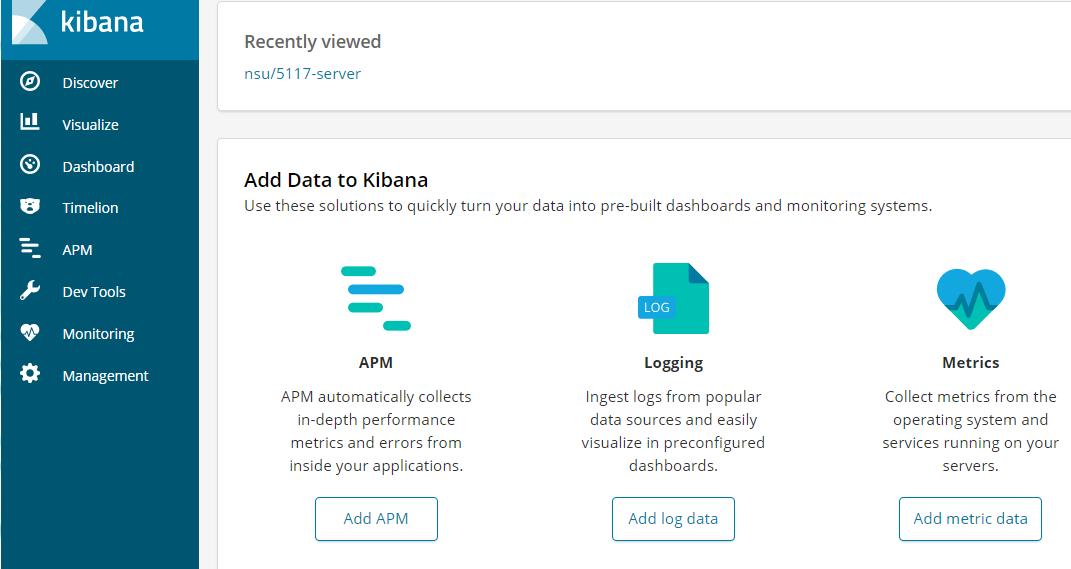
1. 启动filebeat

Shell > cd /usr/local/src/filebeat-6.3.0-linux-x86\_64

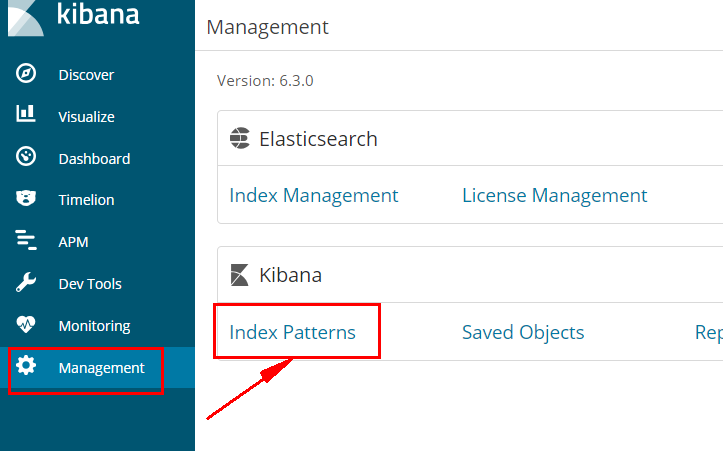
Shell > nohup ./filebeat &

**配置kibana**

1. 打开浏览器 http：//ip:5601，会出现如下页面：

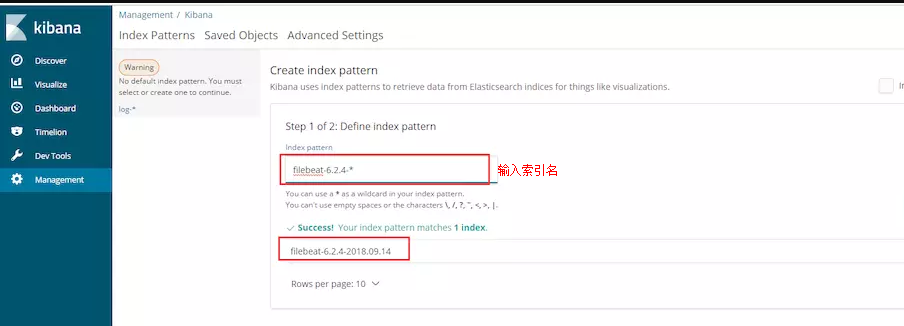


1. 点击Management进入配置

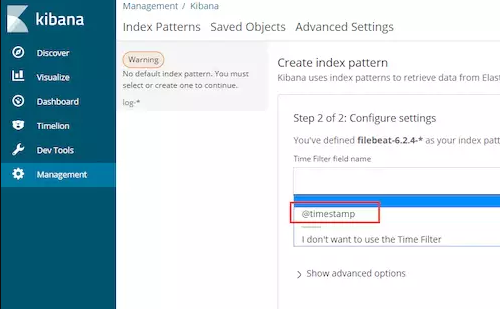


1. 点击进入Index Patterns

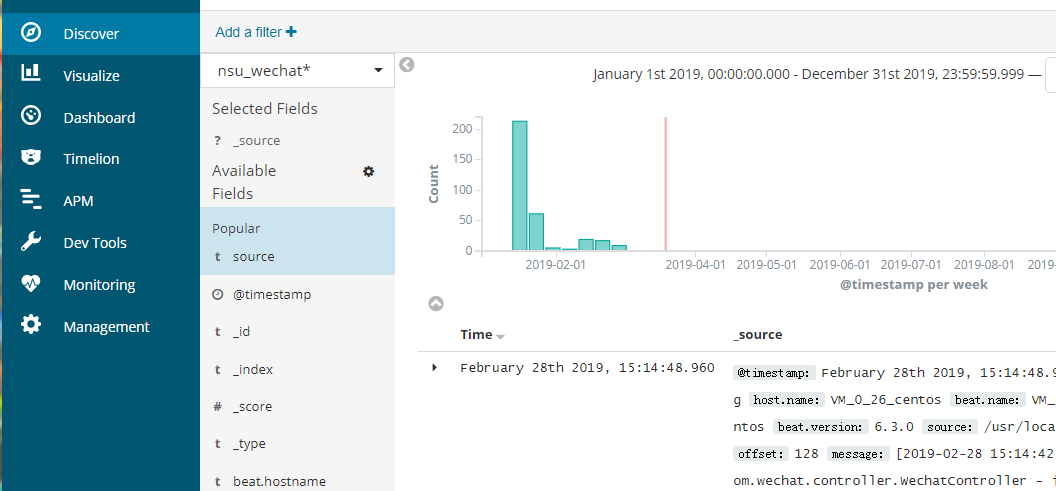
第二个红框出会显示出Elasticsearch中已有的索引，点击Next step进入下一步



1. 选择时间属性：@timestamp



1. 点击Create index pattern完成配置，配置完成后点击 Discover就能查看日志了，还能搜索，如下图



**相关文档说明链接：**

Filebeat6.0以后更改默认索引名时遇到的坑

官网说明很模糊

<https://www.elastic.co/guide/en/beats/metricbeat/current/configuration-template.html>

应该设置为：

<https://www.iyunw.cn/archives/filebeat-6-0-yi-hou-ban-ben-she-zhi-index-ming-zi/>

filebeat实践-内存占用-最大内存占用：

<https://yq.aliyun.com/articles/241161>

Filebeat6.0.x 版本多个index配置：

<https://elasticsearch.cn/question/3088>

ELK6.0已取消filebeat配置document\_type：

<http://blog.51cto.com/kexiaoke/2092029>

Filebeat占用Linux空间未释放的问题解决：

<http://www.360doc.com/content/17/1020/16/8507568_696677465.shtml>

filebeat指定常规设置：

<https://www.elastic.co/guide/en/beats/filebeat/current/configuration-general-options.html>

ES管理，监控和部署：

<https://www.elastic.co/guide/en/elasticsearch/guide/current/administration.html>

生产环境elasticsearch的配置建议：

<https://blog.csdn.net/thomas0yang/article/details/55518105>

Elasticsearch安装配置

<https://www.cnblogs.com/yypbingo/p/6839555.html>

<https://www.cnblogs.com/straycats/p/8053937.html>

ES基本操作：

<https://blog.csdn.net/weixin_35494719/article/details/70145540>

ES 内存大小设置：

https://www.elastic.co/guide/en/elasticsearch/guide/current/heap-sizing.html

Logstash详解：

<https://yq.aliyun.com/articles/152043?utm_content=m_27192>