ELK日志采集分析系统

# 参考资料

https://www.rabbitmq.com

<https://www.cnblogs.com/kevingrace/p/5919021.html>

elasticsearch优化<https://www.jianshu.com/p/e59a3cce5840>

安装elasticsearch <https://www.jianshu.com/p/688c0fbe7f39>

# 软件版本

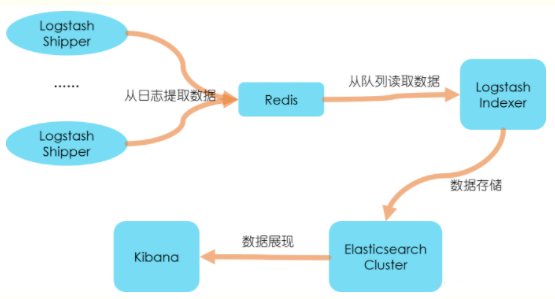
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 软件名称 |  | 版本号 | 软件形式 |  |  |  |
| Elasticsearch |  | 5.6.9 | Tar |  |  |  |
| Logstash |  | 6.6.0 | Tar |  |  |  |
| Kibana |  | 5.6.9 | Tar |  |  |  |
| Elasticsearch-header |  | 无 | elasticsearch-head.zip |  |  |  |
| JDK |  | 1.8+ |  |  |  |  |

# 系统架构模型

## Elk整体思路

1）在每台生成日志文件的机器上，部署Logstash，作为Shipper的角色，负责从日志文件中提取数据，但是不做任何处理，直接将数据输出到Redis队列(list)中；  
2）需要一台机器部署Logstash，作为Indexer的角色，负责从Redis中取出数据，对数据进行格式化和相关处理后，输出到Elasticsearch中存储；  
3）部署Elasticsearch集群，当然取决于你的数据量了，数据量小的话可以使用单台服务，如果做集群的话，最好是有3个以上节点，同时还需要部署相关的监控插件，如es-head；  
4）部署Kibana服务，提供Web的 全文搜索等服务。

## 架构模型



其中里边的redis ，我们或许用 rabbitMQ来代替。理由简单做redis集群非常复杂，rabbitmq有,当然，如果系统并发数不高，机器少，也可将 redis的中转部分去掉，即：将logstash的搜集结果直接录入到ES。如下面的部署是不包含redis中转环节的。

# 软件部署

## 测试环境

|  |  |  |  |
| --- | --- | --- | --- |
| 172.16.176.210 | ES  Es-head | /usr/local/es/elasticsearch-5.6.9 |  |
| 172.16.14.105 | ES  KIBANNA  LOGSTASH | /usr/local/src/es  /usr/local/src/ kibana  /usr/local/src/logstash | 9200 9300  5601  9600 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## 部署elasticsearch

### 修改操作系统

#### 锁定内存

vim /etc/security/limits.conf

添加如下内容:

\* soft memlock unlimited

\* hard memlock unlimited

备注：\* 代表Linux所有用户名称

保存、退出、重新登录才可生效

临时取消限制

ulimit -l unlimited

#### 为新建的elasticsearch用户配置内存

执行命令：

sysctl -w vm.max\_map\_count=262144

查看结果：

sysctl -a|grep vm.max\_map\_count

显示：

vm.max\_map\_count = 262144

上述方法修改之后，如果重启虚拟机将失效，所以：

解决办法：

在 /etc/sysctl.conf文件最后添加一行

vm.max\_map\_count=262144

即可永久修改

### 新建elasticsearch的用户组

.新建用户和组，并为用户赋予解压elasticsearch后产生的文件夹权限

adduser elasticsearch

passwd elasticsearch ，然后会让你输入密码

chown -R 你的用户名 文件夹名

### 获取安装包

下载并解压es tar包即可。最好是5.6.9版本，因为 spring全家桶用的是这个版本的

### 修改配置文件

主要有两个配置文件

#### elasticsearch.yml

bootstrap.system\_call\_filter: false

http.cors.enabled: true #head插件发现节点

http.cors.allow-origin: "\*" #head插件发现节点

http.cors.allow-headers: Authorization,X-Requested-With,Content-Length,Content-Type

action.auto\_create\_index: .security,.security-6,.monitoring\*,.watches,.triggered\_watches,.watcher-history\*,app-a-\*,app-b-\*,.ml\*

cluster.name: my-application-1

node.name: node-taishiji-shemiserver10x

bootstrap.memory\_lock: false#关闭使用交换分区

network.host: 0.0.0.0#表示任意ip可以访问

discovery.zen.ping.unicast.hosts: ["dongshengtaishiji1","shemeserver105"]

#### jvm.options

默认值

### 启动及测试

#### 启动

使用 elasticsearch用户，进入bin下

./elasticsearch –d

#### 测试

curl 'http://localhost:9200/?pretty'

<http://172.16.176.210:9200/rbac/user/18111218125600001>

### 部署gui插件（elasticsearch head插件）

#### 参考文档

可以完全按照这个安装

<https://www.jianshu.com/p/c20c2793bff5>

#### 安装部署

如果打不开上面链接，可以按照下面的安装：部署完elasticsearch集群后，下面开始部署head插件，head插件只需要在一个节点安装

##### 首先安装环境

su root #在root角色下

curl -sL https://rpm.nodesource.com/setup\_8.x | bash -

sudo yum install gcc-c++ make

curl -sL https://dl.yarnpkg.com/rpm/yarn.repo | sudo tee /etc/yum.repos.d/yarn.repo

yum -y install yarn nodejs git

npm install -g grunt-cli

cd /home/elastic #在elasticsearch的同级目录下

#clone head插件

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

##### 修改配置文件

###### Gruntfile.js

vi /usr/local/es/elasticsearch-head/Gruntfile.js

#只修改下面这一段： hostname: ‘\*’

connect: {

server: {

options: {

port: 9100,

hostname: '\*', #添加hostname这一行

base: '.',

keepalive: true

}

}

}

###### app.js

cd /home/elastic/elasticsearch-head/\_site

vim app.js

#修改下面这一段，就是修改ip:port，

#如果使用的是通过公网ip来访问，此处就写公网ip,否则就写局域网ip，port是elasticsearch配置文件的http.port

this.base\_uri = this.config.base\_uri || this.prefs.get("app-base\_uri") || "http://ip:port";

##### 安装install grunt

npm install grunt --save-dev

npm install

##### 启动

在解压后的elasticxxxx-head下执行如下命令：

nohup grunt server &

##### 访问

##### <http://ip:9100>

## 部署logstash

下载tar包 <https://www.elastic.co/downloads/logstash>

### 注意事项

解压tar包后，如果安装不是使用root权限，需要为解压后的目录配置权限。

chown –R 用户名 目录

### 安装

解压即可。

#### 配置文件

在config下新建tongdao1.conf

# Sample Logstash configuration for creating a simple

# Beats -> Logstash -> Elasticsearch pipeline.

input {

file {

type => "example\_nginx\_access\_1"

path => ["/var/log/applog/\*","/var/log/nginx/example.access.log"]

start\_position => "beginning"

sincedb\_path => "/dev/null"

stat\_interval => 2

discover\_interval => 15

}

}

output {

elasticsearch {

hosts => ["http://172.16.14.105:9200"]

index => "example\_nginx\_access\_1-%{+YYYY.MM.dd}"

#user => "elastic"

#password => "changeme"

}

}

注意：如果是output到es，如上，则需要修改 elasticsearch服务中config下的配置文件elasticsearch.yml，将 action.auto\_create\_index 注释掉。

#### 启动

需要在bin下执行此命令。

nohup ./logstash -f /data/logstash/logstash-6.6.0/config/tongdao1.conf --config.reload.automatic --path.data=/data/logstash/datastore &

daemon模式启动，头尾加上 nohup & 如下：

nohup logstash -f /usr/local/src/logstash/logstash-6.6.0/config/tongdao1.conf --config.reload.automatic --path.data=/usr/local/src/logstash/datastore &

## 部署kibana

注意，kibana版本务必要和elasticsearch版本一致。

下载：<https://www.elastic.co/cn/downloads>

https://artifacts.elastic.co/downloads/kibana/kibana-5.6.9-linux-x86\_64.tar.gz

### 安装

#### 注意事项

解压tar包后，如果安装不是使用root权限，需要为解压后的目录配置权限。

chown –R 用户名 目录

#### 配置文件

server.port: 5601

elasticsearch.url: <http://elasticsearch的ip地址:9200>

server.host: "0.0.0.0" 允许任意的ip地址访问kibana服务

#### 启动和关闭

进入bin下 ： nohup ./kibana &

关闭服务：通过命令（netstat -natp|grep 5601）找到端口号对应的进程id ，杀掉 即可。

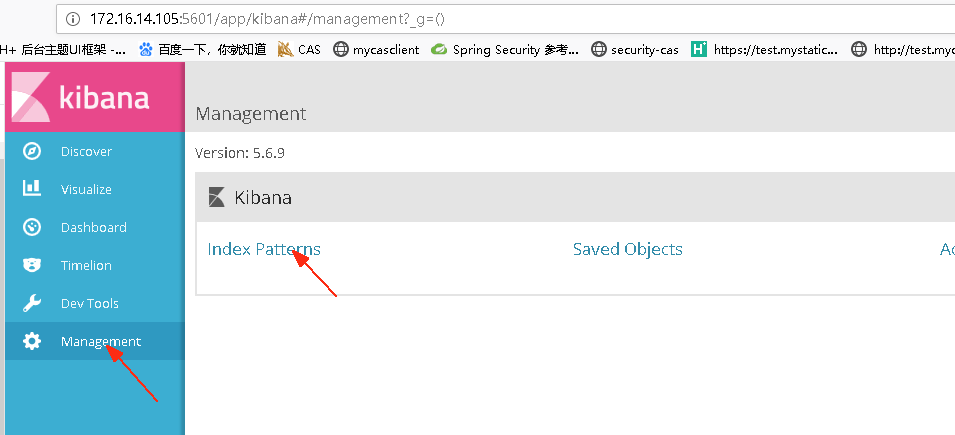
#### 测试

<http://172.16.14.105:5601>

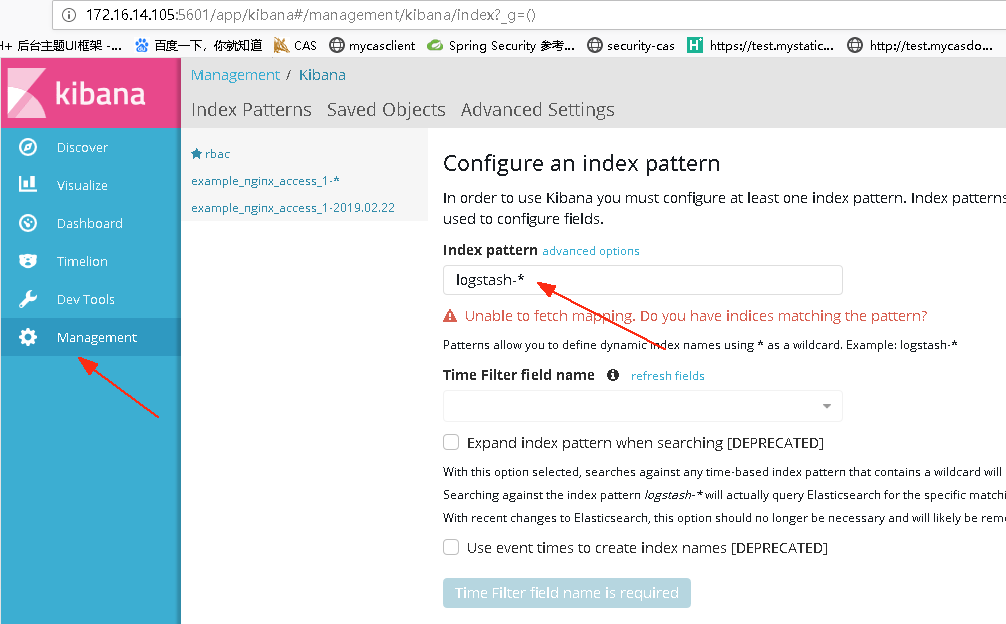
### 同ES结合使用

启动完kibana后，访问ip：5601即可看到界面。初次使用时，会让你配置一个默认的index，也就是你至少需要关联一个ES里的Index，可以使用pattern正则匹配。由于之前我们已经使用过ES了，里面是有index的，用es的head看看

#### 关联index



Index就是es中的index，es中index对应数据库的数据库实例，这里的输入项可以是正则表达式，可以对应多个index，这样，在kibana搜索的时候，也是从多个index里搜索了。



#### 全文搜索

1. 点击discover
2. 选择index
3. 点击time picker，选择要查找的时间范围
4. 然后再搜索栏输入要搜索的关键词，此搜索为全文搜索，但注意其分词策略，不是随意输入搜索内容都搜索到的。比如搜索ProtocolHandler可以搜索到，但去掉个r,就什么都搜不到了。

