ElasticSearch-2.x+LogStash-2.x+Kibana-4.x

集群环境搭建

技术文档

（版本：V1.0.0）

|  |  |  |  |
| --- | --- | --- | --- |
| 版本 | 日期 | 说明 | 作者 |
| V1.0.0 | 2016/11/7 | 创建 | Simon Hoo |
|  |  |  |  |

目 录

一． 环境准备 - 4 -

1.1 服务器及配置 - 4 -

1.2 软件准备 - 5 -

二． 安装ElasticSearch 2.4.0集群 - 6 -

2.1 系统设置 - 6 -

2.1.1 安装JDK - 6 -

2.1.2 创建用户及组 - 6 -

2.1.3 修改/etc/security/limits.conf - 6 -

2.1.4 修改/etc/security/limits.d/90-nproc.conf - 6 -

2.1.5 修改/etc/sysctl.conf - 7 -

2.1.6 修改/etc/hosts - 7 -

2.2 安装ElasticSearch - 7 -

2.2.1 解压安装包 - 7 -

2.2.2 修改权限 - 8 -

2.2.3 修改elasticsearch.yml - 8 -

2.3 安装ElasticSearch插件 - 8 -

2.4 安装ElasticSearch其它节点 - 8 -

2.5 启动ElasticSearch - 9 -

三． 安装LogStash 2.4.0 - 11 -

3.1 系统设置 - 11 -

3.1.1 安装JDK - 11 -

3.2 安装LogStash - 11 -

3.2.1 解压安装 - 11 -

3.2.2 创建LogStash配置文件 - 11 -

3.3 启动LogStash - 12 -

四． 安装Kibana 4.6.1 - 12 -

4.1 安装Kibana - 12 -

4.1.1 解压安装 - 12 -

4.2 配置Kibana - 13 -

4.3 启动Kibana - 13 -

4.4 设置Kibana - 13 -

五． 应用程序接入 - 14 -

5.1 创建JAVA程序 - 14 -

5.2 配置log4j.properties - 15 -

5.3 运行程序 - 15 -

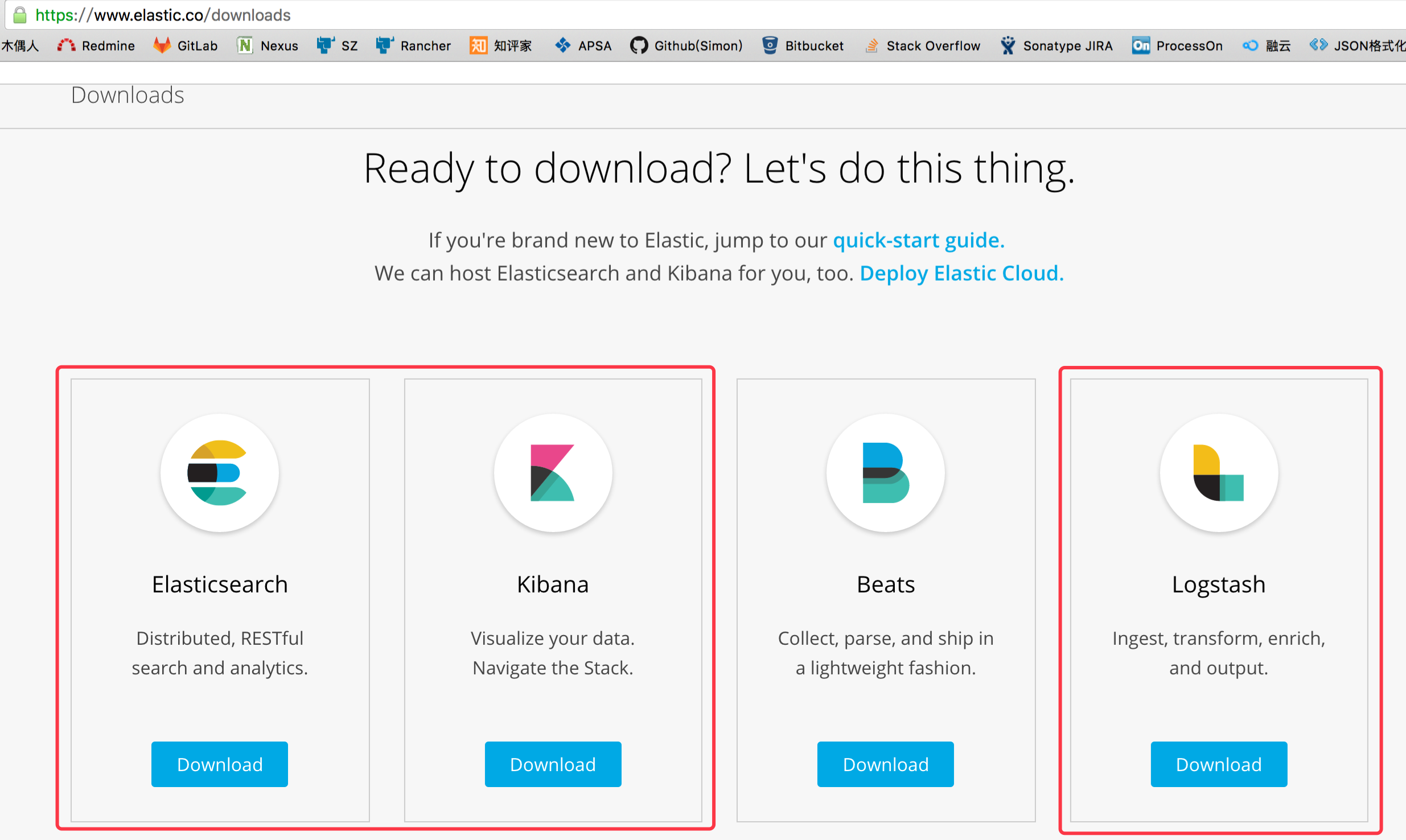
5.4 ElasticSearch 查看日志 - 16 -

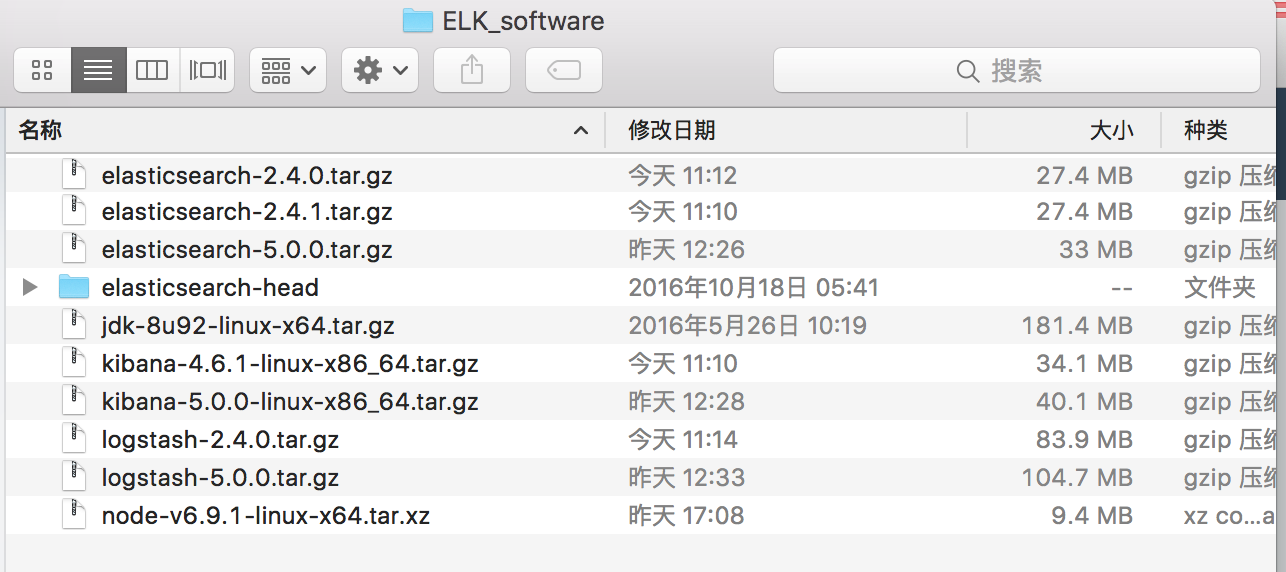
## 环境准备

### 服务器及配置

|  |  |  |  |
| --- | --- | --- | --- |
| 服务器 | IP地址 | 安装软件 | 备注 |
| ElasticSearch Server  Node1 | 10.50.130.45 | ElasticSearch 2.4.0  JDK 1.8 | CentOS 6.8 64位  CPU: 2x2CPUs  RAM: 8GB  Disk: 50GB |
| ElasticSearch Server  Node2 | 10.50.130.46 | ElasticSearch 2.4.0  JDK 1.8 | CentOS 6.8 64位  CPU: 2x2CPUs  RAM: 8GB  Disk: 50GB |
| LogStash Server  Node1 | 10.50.130.47 | LogStash 2.4.0  JDK 1.8 | CentOS 6.8 64位  CPU: 2x2CPUs  RAM: 8GB  Disk: 50GB |
| LogStash Server  Node2 | 10.50.130.48 | LogStash 2.4.0  JDK 1.8 | CentOS 6.8 64位  CPU: 2x2CPUs  RAM: 8GB  Disk: 50GB |
| Kibana Server | 10.50.130.49 | Kibana 4.6.1 | CentOS 6.8 64位  CPU: 2x2CPUs  RAM: 8GB  Disk: 50GB |
|  |  |  |  |

### 软件准备





注：JDK自行在ORACLE官网下载。

## 安装ElasticSearch 2.4.0集群

### 系统设置

#### 2.1.1 安装JDK

[root@elk1] mkdir –p /usr/local/java

[root@elk1] tar –xzvf jdk-8u92-linux-x64.tar.gz –C /usr/local/java

设置JAVA\_HOME:

[root@elk1] vi /etc/profile

export JAVA\_HOME=/usr/local/java/jdk1.8.0\_92

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

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

[root@elk1] source /etc/profile

[root@elk1] java -version

#### 2.1.2 创建用户及组

[root@elk1] useradd es

[root@elk1] passwd es

#### 2.1.3 修改/etc/security/limits.conf

[root@elk1] vi /etc/security/limits.conf

添加：

es hard nofile 65536

es soft nofile 65536

#### 2.1.4 修改/etc/security/limits.d/90-nproc.conf

[root@elk1] vi /etc/security/limits.d/90-nproc.conf

将

\* soft nproc 1024

改为

\* soft nproc 2048

#### 2.1.5 修改/etc/sysctl.conf

[root@elk1] vi /etc/sysctl.conf

添加：

vm.max\_map\_count=655360

#### 2.1.6 修改/etc/hosts

[root@elk1] vi /etc/hosts

添加：

10.50.130.45 elk1.beyondsoft-dev.com

10.50.130.46 elk2.beyondsoft-dev.com

[root@elk1] reboot

### 安装ElasticSearch

#### 2.2.1 解压安装包

[root@elk1 software] mkdir –p /usr/local/elasticsearch

[root@elk1 software]# tar -xzvf elasticsearch-2.4.0.tar.gz -C /usr/local/elasticsearch/

设置ES\_HOME:

[root@elk1] vi /etc/profile

export ES\_HOME=/usr/local/elasticsearch/elasticsearch-2.4.0

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

[root@elk1] source /etc/profile

#### 2.2.2 修改权限

[root@elk1 ~]# chown -R es.es /usr/local/elasticsearch/

#### 2.2.3 修改elasticsearch.yml

[root@elk1 ~]# vi $ES\_HOME/config/elasticsearch.yml

cluster.name: Beyondsoft-ELK

node.name: node-1

node.attr.rack: r1

bootstrap.memory\_lock: false

network.host: 10.50.130.45

http.port: 9200

discovery.zen.ping.unicast.hosts: ["elk1.beyondsoft-dev.com", "elk2.beyondsoft-dev.com"]

discovery.zen.minimum\_master\_nodes: 2

### 安装ElasticSearch插件

[root@elk1 ~]# su es

[es@elk1 ~]# cd $ES\_HOME/bin

安装head插件

[es@elk1 bin]# ./plugin install mobz/elasticsearch-head

安装kopf插件

[es@elk1 bin]# ./plugin install lmenezes/elasticsearch-kopf

[es@elk1 bin]# cd ..

[es@elk1 elasticsearch-2.4.0]# ls plugins

### 安装ElasticSearch其它节点

其它同2.2.1~2.2.3，修改elasticsearch.xml如下：

[root@elk2 ~]# vi $ES\_HOME/confi/elasticsearch.yml

cluster.name: Beyondsoft-ELK

node.name: node-2

node.attr.rack: r1

bootstrap.memory\_lock: false

network.host: 10.50.130.46

http.port: 9200

discovery.zen.ping.unicast.hosts: ["elk1.beyondsoft-dev.com", "elk2.beyondsoft-dev.com"]

discovery.zen.minimum\_master\_nodes: 2

### 启动ElasticSearch

[root@elk1 ~]#su es

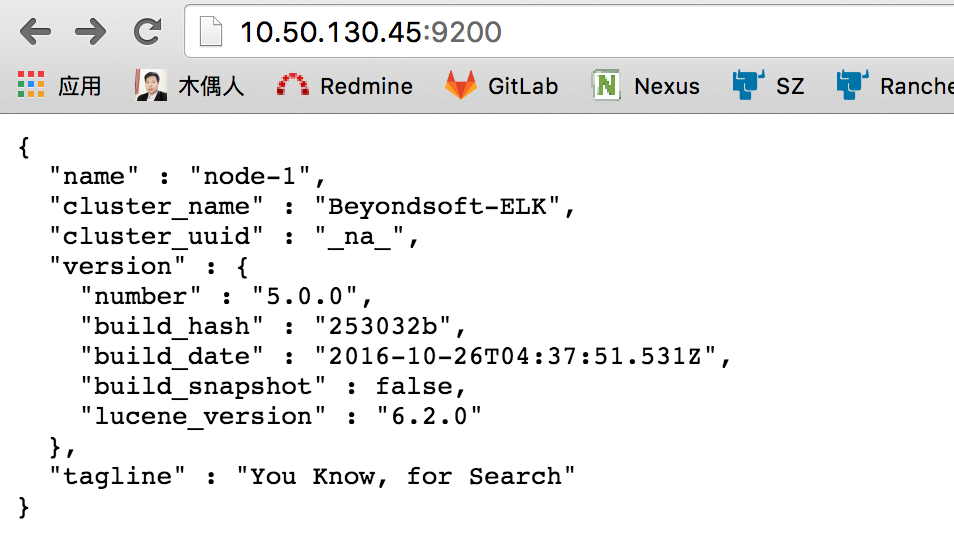
[es@elk1 ~]$ cd $ES\_HOME/bin

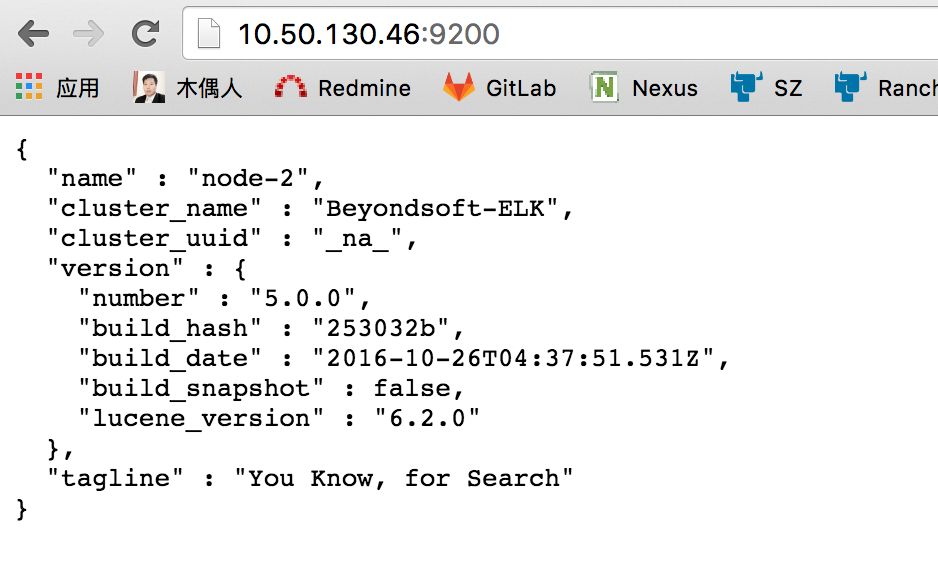
[es@elk1 bin]$ ./elasticsearch &

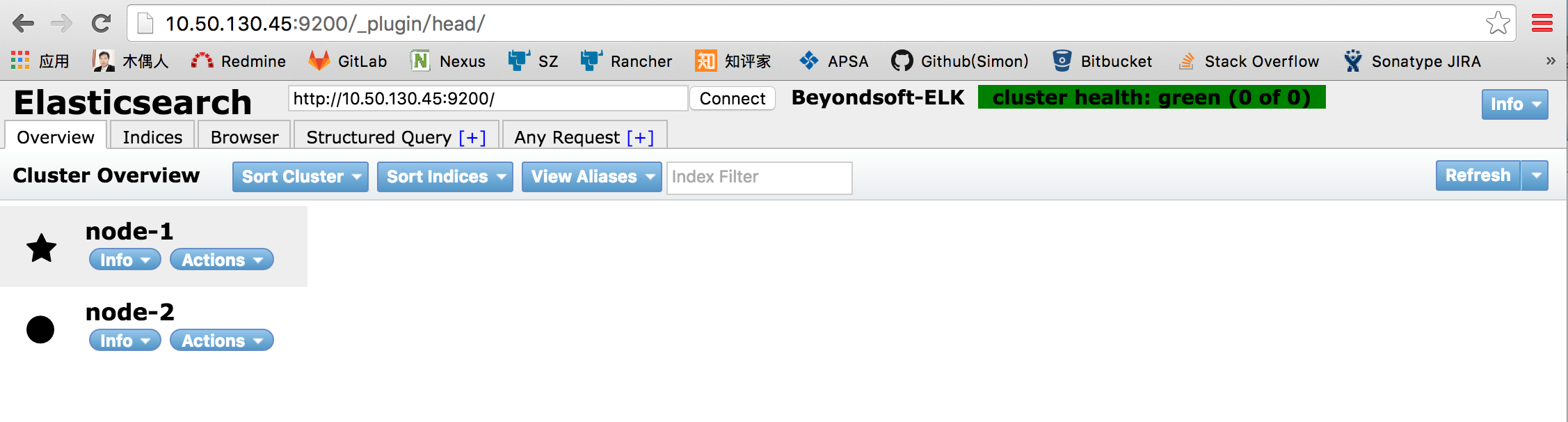
查看日志

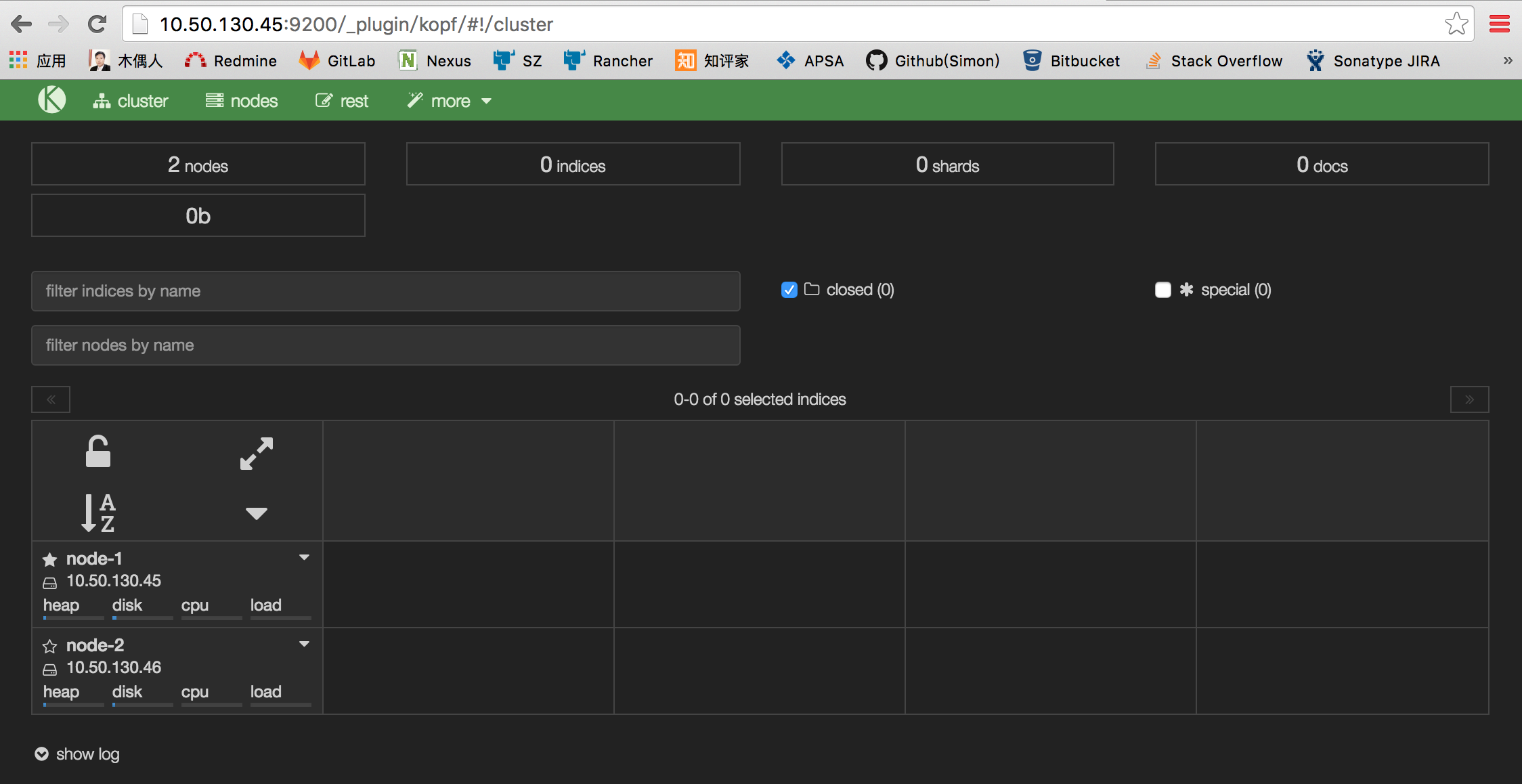
[es@elk1 ~]$ cd $ES\_HOME/logs

[es@elk1 logs]$ tail -f Beyondsoft-ELK.log









## 

## 安装LogStash 2.4.0

### 系统设置

#### 3.1.1 安装JDK

[root@logstash1 ~] mkdir –p /usr/local/java

[root@logstash1 ~] cd /root/software

[root@logstash1 software] tar –xzvf jdk-8u92-linux-x64.tar.gz –C /usr/local/java

设置JAVA\_HOME:

[root@ logstash1 ~] vi /etc/profile

export JAVA\_HOME=/usr/local/java/jdk1.8.0\_92

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

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

[root@ logstash1 ~] source /etc/profile

[root@ logstash1 ~] java -version

### 安装LogStash

#### 3.2.1 解压安装

[root@logstash1 ~] mkdir –p /usr/local/logstash

[root@logstash1 ~] cd /root/software

[root@logstash1 software] tar –xzvf logstash-2.4.0.tar.gz –C /usr/local/logstash

#### 3.2.2 创建LogStash配置文件

这里以LOG4J为例：

[root@logstash1 ~] vi /usr/local/logstash/logstash-2.4.0/config/log4j\_to\_es.conf

input {

log4j {

mode => "server"

host => "10.50.130.47"

port => 4567

}

}

filter {

}

output {

elasticsearch {

action => "index"

hosts => "10.50.130.45:9200"

index => "applog"

}

}

### 启动LogStash

[root@logstash1 ~] cd /usr/local/logstash/logstash-2.4.0

[root@logstash1 logstash-2.4.0]./bin/logstash agent –f config/log4j\_to\_es.conf &

## 安装Kibana 4.6.1

### 安装Kibana

#### 4.1.1 解压安装

[root@kibana ~] mkdir –p /usr/local/kibana

[root@ kibana ~] cd /root/software

[root@ kibana software] tar –xzvf kibana-4.6.1-linux-x86\_64.tar.gz –C /usr/local/kibana

### 配置Kibana

[root@kibana ~] cd /usr/local/kibana/kibana-4.6.1

[root@kibana kibana-4.6.1] vi config/kibana.yml

修改内容：

server.port: 5601

server.host: “10.50.130.49”

elasticsearch.url: http://10.50.130.45:9200

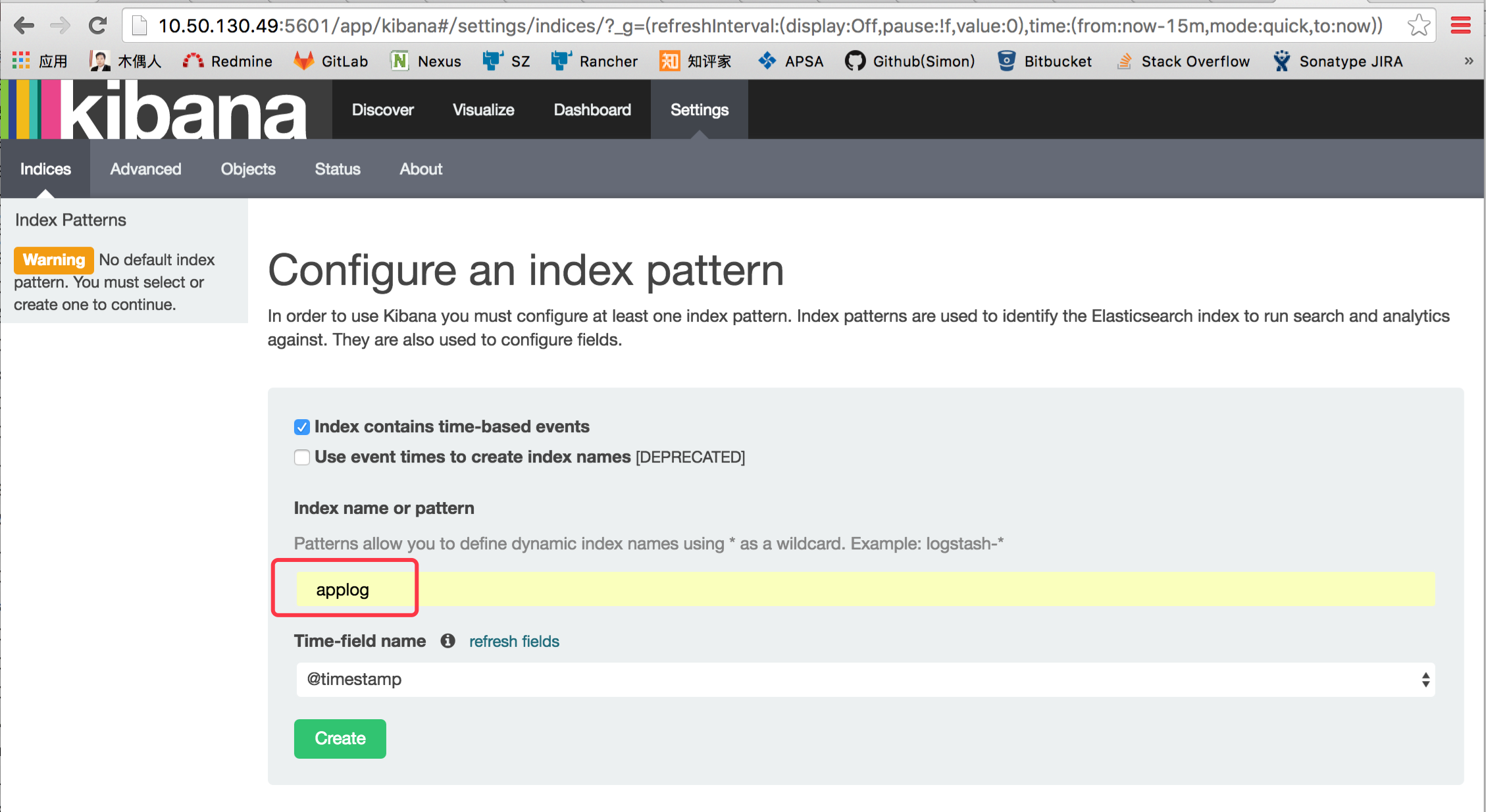
kibana.index: “.kibana”

### 启动Kibana

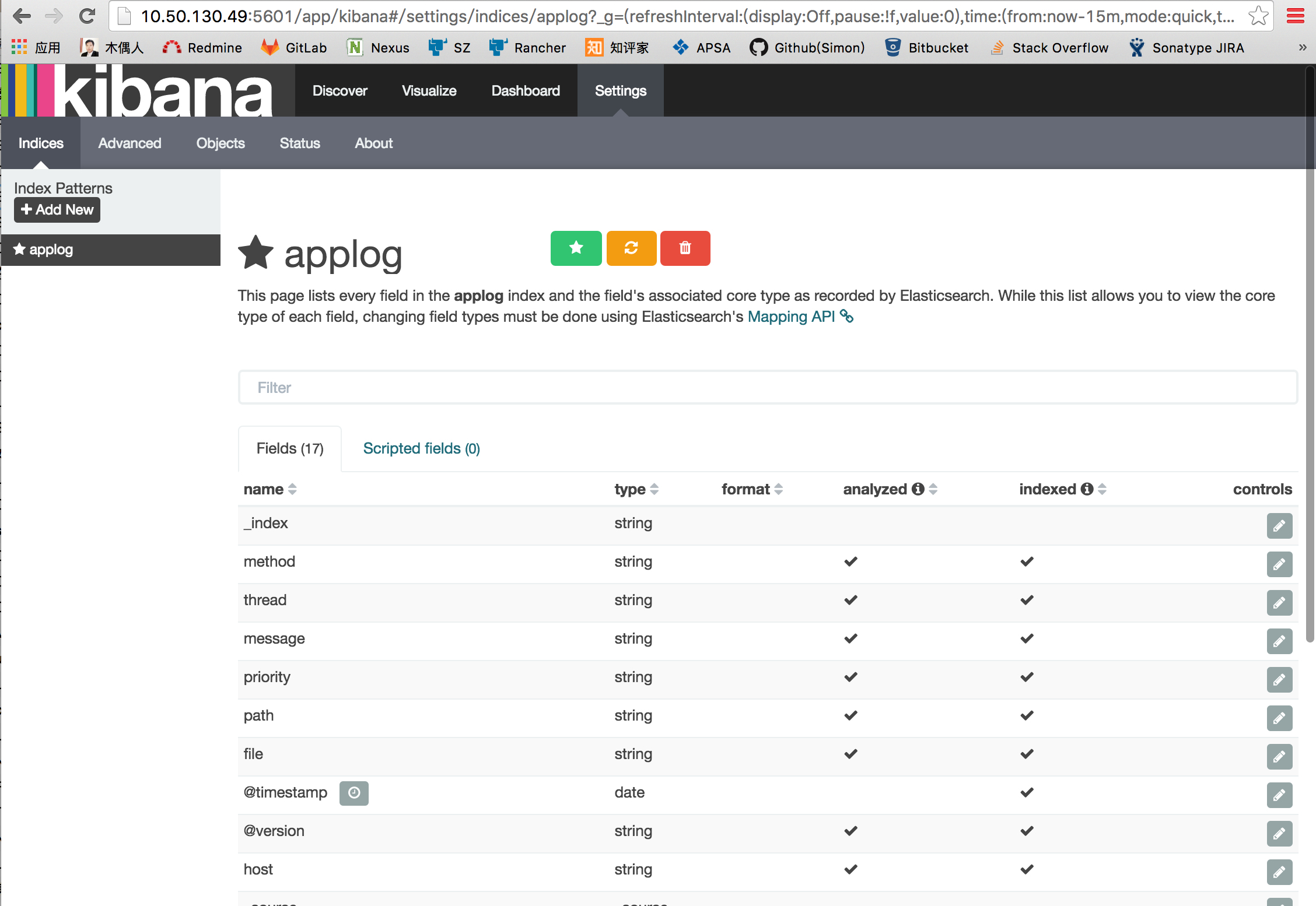
[root@kibana kibana-4.6.1] ./bin/kibana &

### 设置Kibana

<http://10.50.130.49:5601>

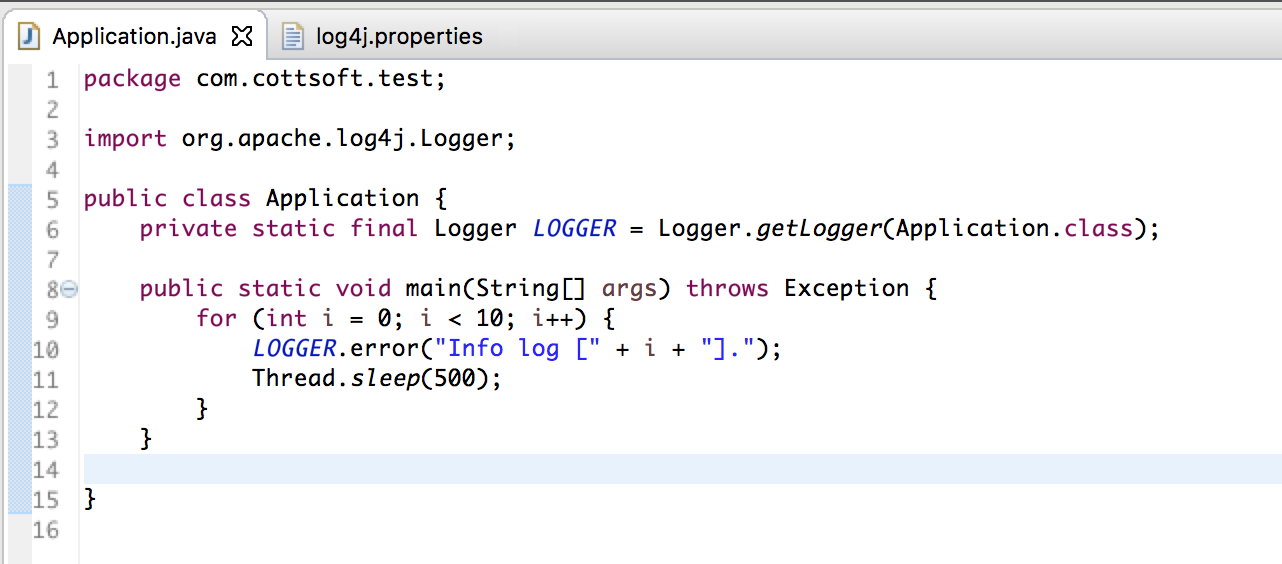


creare:



## 应用程序接入

### 创建JAVA程序



### 配置log4j.properties

log4j.rootLogger=INFO,console

# for package com.demo.elk, log would be sent to socket appender.

log4j.logger.com.cottsoft.test=DEBUG, socket

# appender socket

log4j.appender.socket=org.apache.log4j.net.SocketAppender

log4j.appender.socket.Port=4567

log4j.appender.socket.RemoteHost=10.50.130.47

log4j.appender.socket.layout=org.apache.log4j.PatternLayout

log4j.appender.socket.layout.ConversionPattern=%d [%-5p] [%l] %m%n

log4j.appender.socket.ReconnectionDelay=10000

# appender console

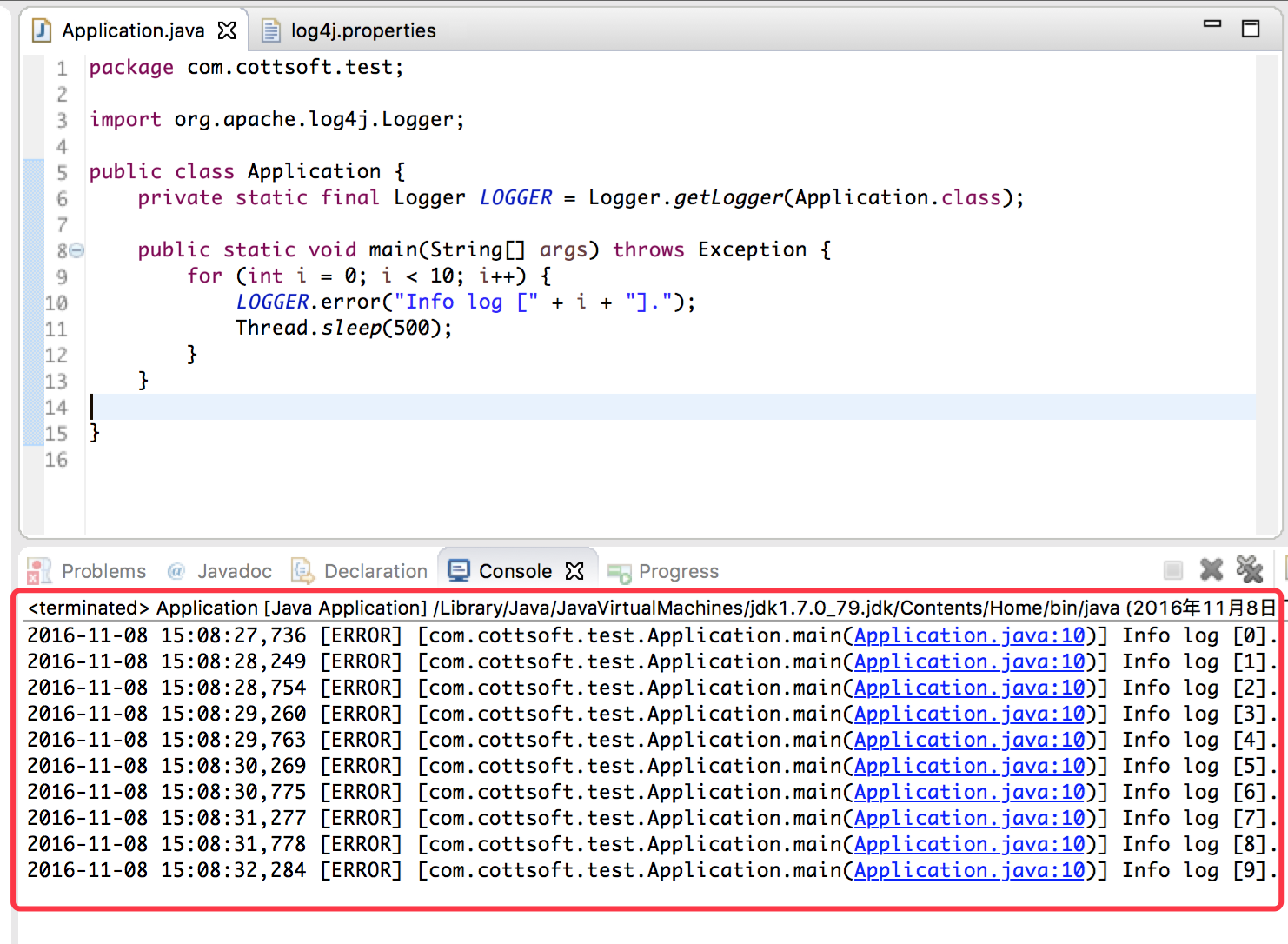
log4j.appender.console=org.apache.log4j.ConsoleAppender

log4j.appender.console.target=System.out

log4j.appender.console.layout=org.apache.log4j.PatternLayout

log4j.appender.console.layout.ConversionPattern=%d [%-5p] [%l] %m%n

### 运行程序



### ElasticSearch 查看日志

