

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

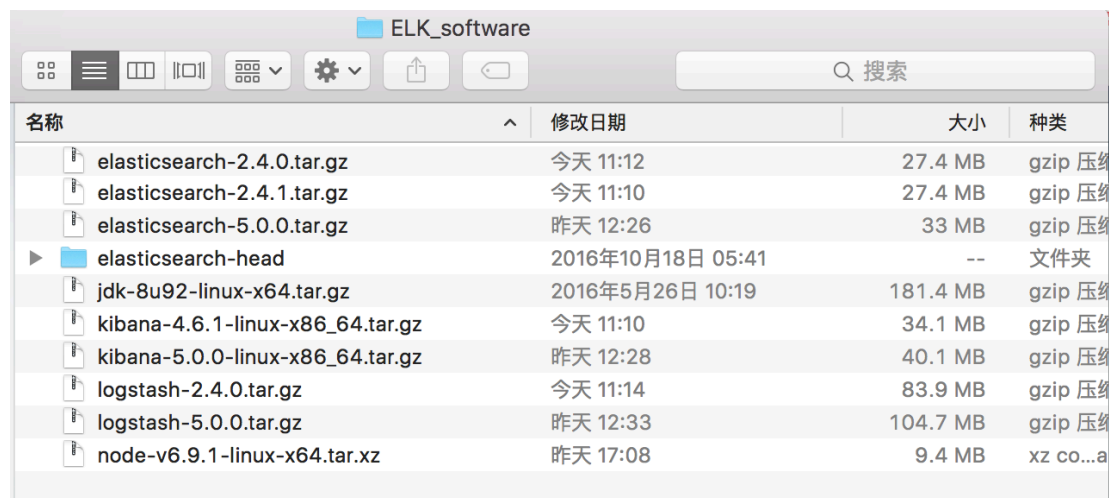
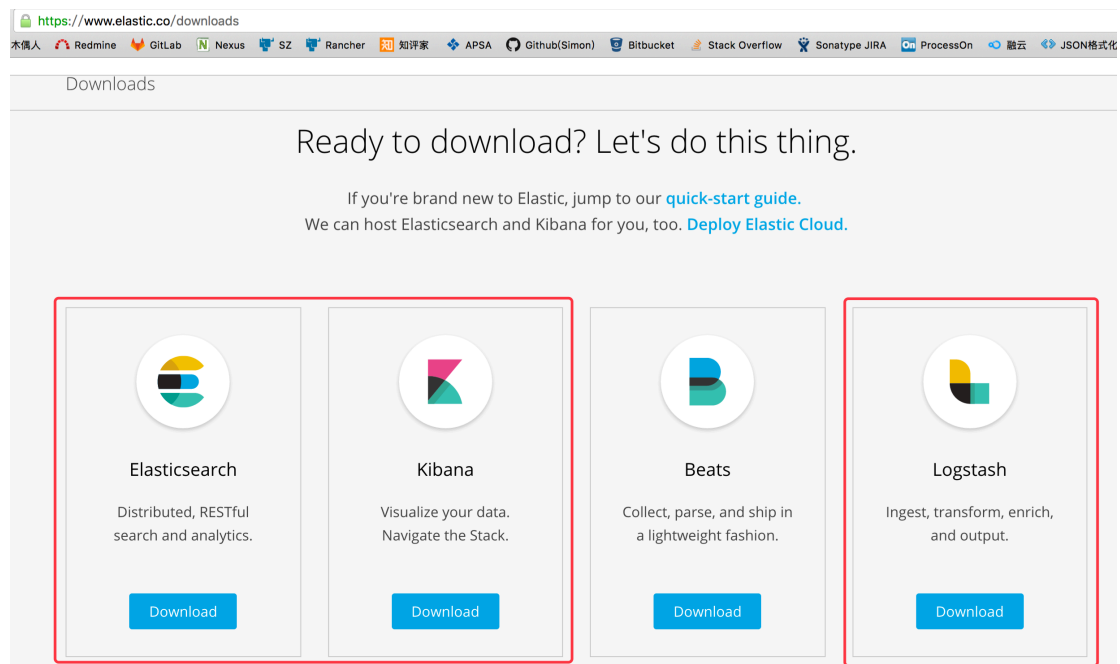
一 .	环境准备	- 3 -
1.1	服务器及配置.....	- 3 -
1.2	软件准备	- 4 -
二 .	安装 Elasticsearch 2.4.0 集群	- 5 -
2.1	系统设置	- 5 -
2.1.1	安装 JDK.....	- 5 -
2.1.2	创建用户及组.....	- 5 -
2.1.3	修改/etc/security/limits.conf	- 5 -
2.1.4	修改/etc/security/limits.d/90-nproc.conf	- 5 -
2.1.5	修改/etc/sysctl.conf.....	- 6 -
2.1.6	修改/etc/hosts	- 6 -
2.2	安装 Elasticsearch	- 6 -
2.2.1	解压安装包	- 6 -
2.2.2	修改权限	- 7 -
2.2.3	修改 elasticsearch.yml	- 7 -
2.3	安装 Elasticsearch 插件.....	- 7 -
2.4	安装 Elasticsearch 其它节点	- 7 -
2.5	启动 Elasticsearch	- 8 -
三 .	安装 LogStash 2.4.0	- 10 -
3.1	系统设置	- 10 -
3.1.1	安装 JDK.....	- 10 -
3.2	安装 LogStash	- 10 -
3.2.1	解压安装	- 10 -
3.2.2	创建 LogStash 配置文件.....	- 10 -
3.3	启动 LogStash	- 11 -
四 .	安装 Kibana 4.6.1.....	- 11 -
4.1	安装 Kibana	- 11 -
4.1.1	解压安装	- 11 -
4.2	配置 Kibana	- 12 -
4.3	启动 Kibana	- 12 -
4.4	设置 Kibana	- 12 -
五 .	应用程序接入	- 13 -
5.1	创建 JAVA 程序	- 13 -
5.2	配置 log4j.properties	- 14 -
5.3	运行程序	- 14 -
5.4	ElasticSearch 查看日志.....	- 15 -

一 . 环境准备

1.1 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

1.2 软件准备



注：JDK 自行在 ORACLE 官网下载。

二 . 安装 Elasticsearch 2.4.0 集群

2.1 系统设置

2.1.1 安装 JDK

```
[root@elk1] mkdir -p /usr/local/java
[root@elk1] tar -xzf 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 nfile 65536
es soft nfile 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
```

2.2 安装 ElasticSearch

2.2.1 解压安装包

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

```
[root@elk1 software]# tar -xzf 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
```

2.3 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
```

2.4 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/conf/elasticsearch.yml
```

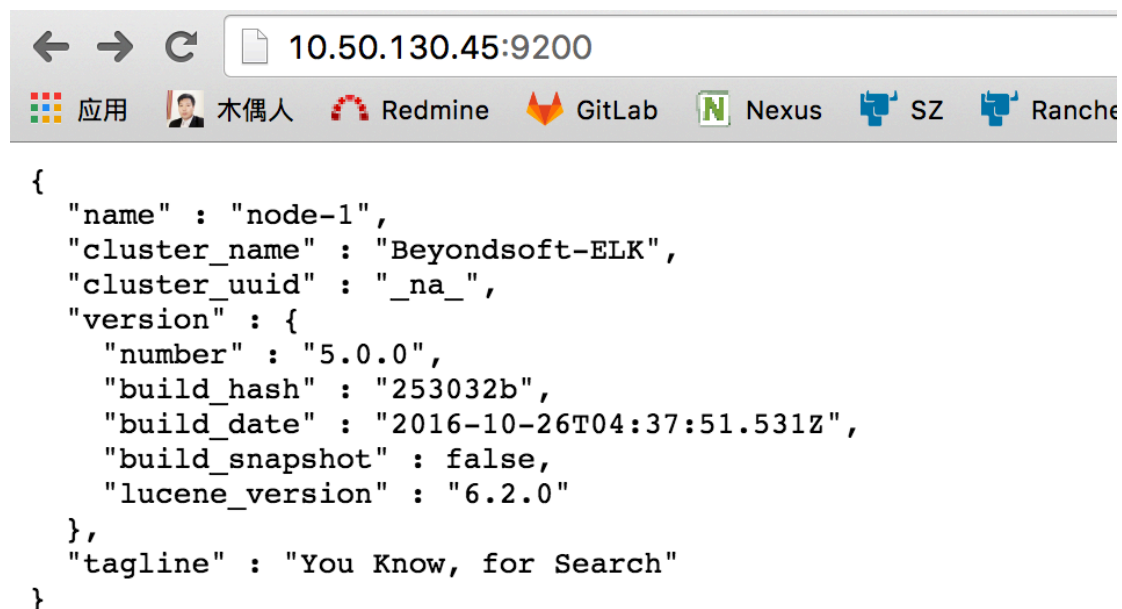
```
cluster.name: Beyondsoft-ELK
node.name: node-2
node.attr.rack: r1
bootstrap.memory_lock: false
network.host: 10.50.130.46
http.port: 9200
discovery.zen.ping.unicast.hosts: ["elk1.beyondsoft-dev.com", "elk2.beyondsoft-dev.com"]
discovery.zen.minimum_master_nodes: 2
```

2.5 启动 Elasticsearch

```
[root@elk1 ~]#su es
[es@elk1 ~]$ cd $ES_HOME/bin
[es@elk1 bin]$ ./elasticsearch &
```

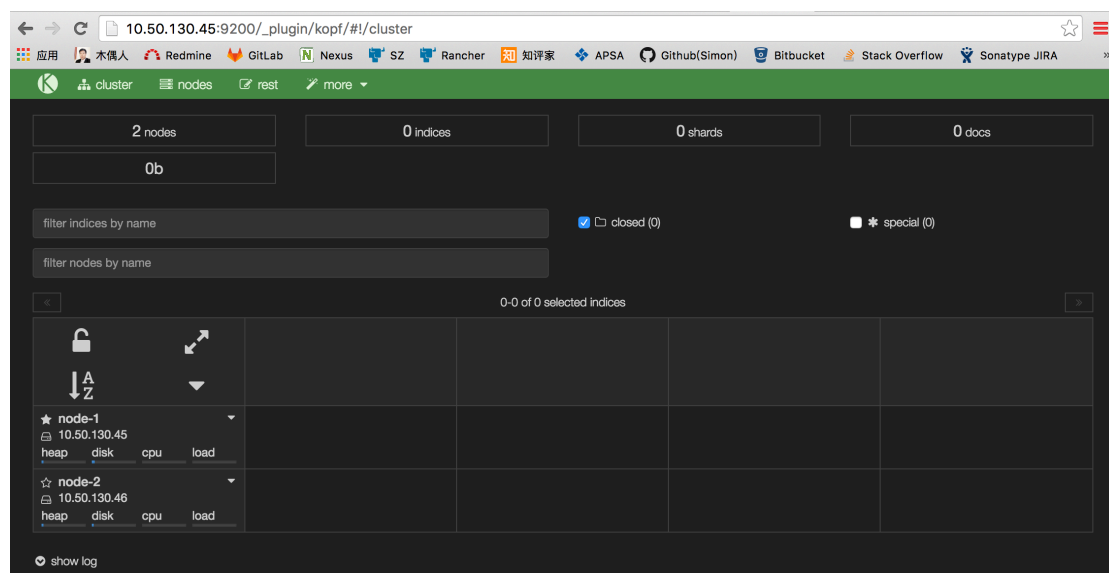
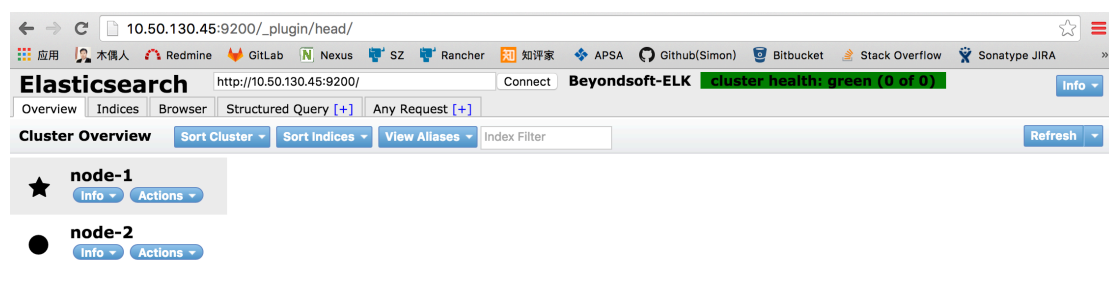
查看日志

```
[es@elk1 ~]$ cd $ES_HOME/logs
[es@elk1 logs]$ tail -f Beyondsoft-ELK.log
```




```
← → ↺ 10.50.130.46:9200
应用 木偶人 Redmine GitLab Nexus SZ Rancher

{
  "name" : "node-2",
  "cluster_name" : "Beyondsoft-ELK",
  "cluster_uuid" : "_na_",
  "version" : {
    "number" : "5.0.0",
    "build_hash" : "253032b",
    "build_date" : "2016-10-26T04:37:51.531Z",
    "build_snapshot" : false,
    "lucene_version" : "6.2.0"
  },
  "tagline" : "You Know, for Search"
}
```



三 . 安装 LogStash 2.4.0

3.1 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
```

3.2 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"  
    }  
}
```

3.3 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 &
```

四 . 安装 Kibana 4.6.1

4.1 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 -xzf kibana-4.6.1-linux-x86_64.tar.gz -C  
/usr/local/kibana
```

4.2 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

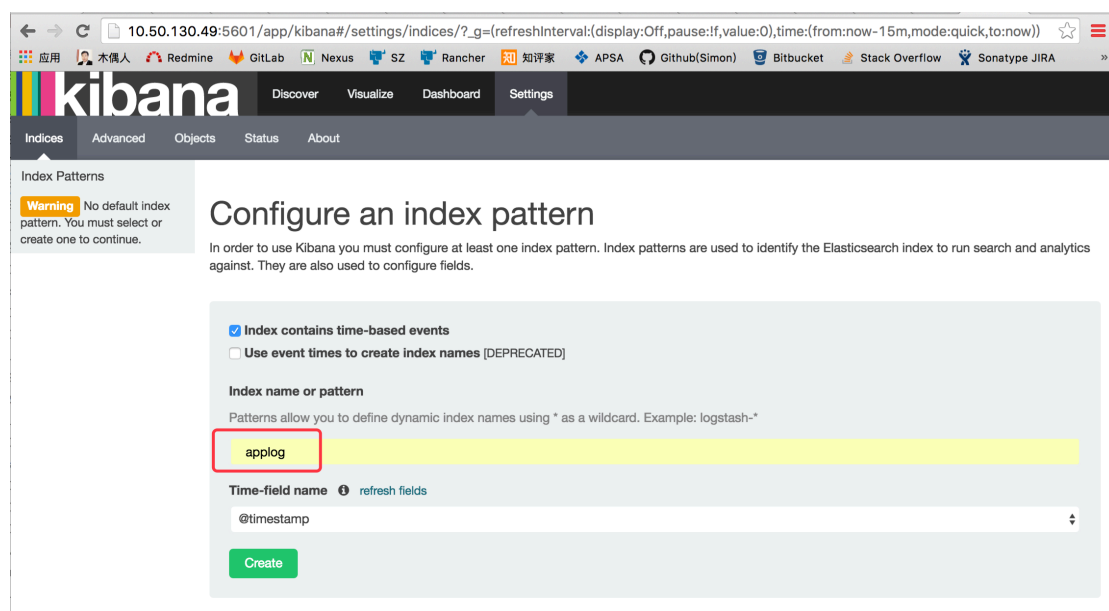
kibana.index: ".kibana"

4.3 启动 Kibana

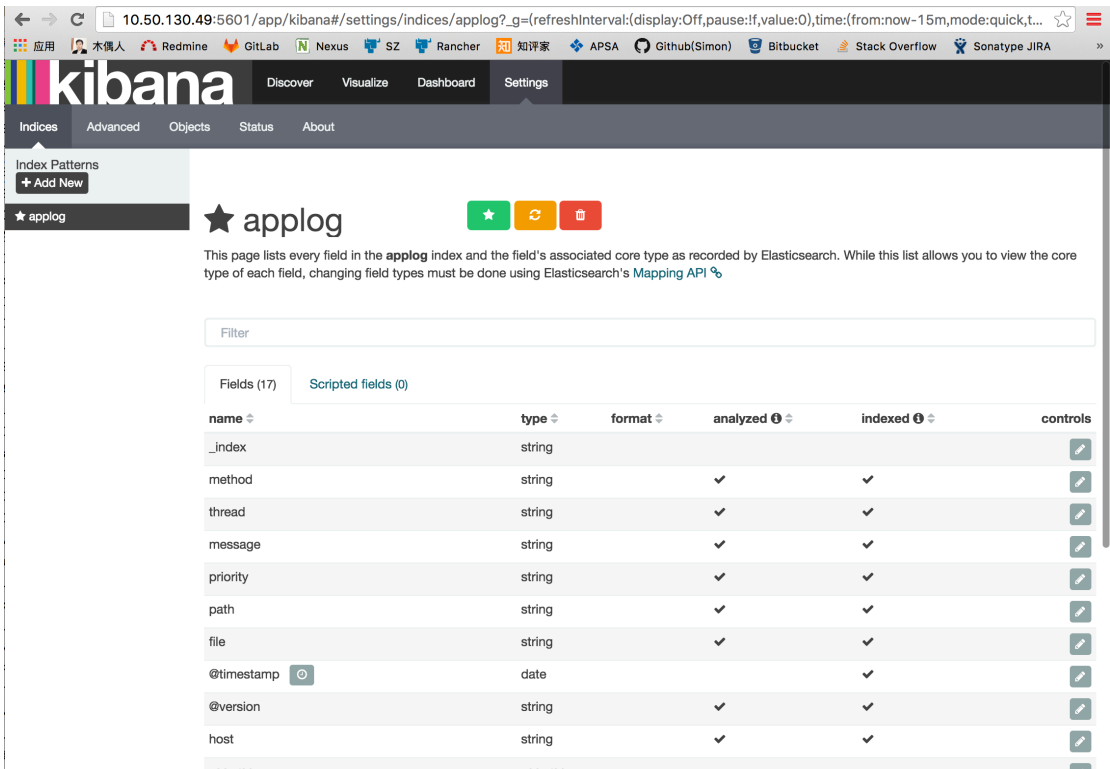
```
[root@kibana kibana-4.6.1] ./bin/kibana &
```

4.4 设置 Kibana

<http://10.50.130.49:5601>

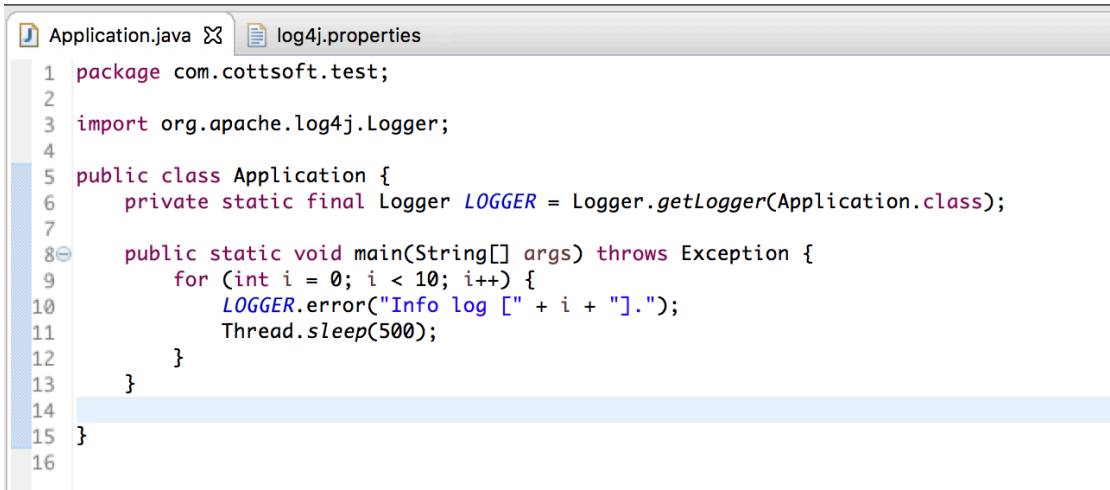


create:



五 . 应用程序接入

5.1 创建 JAVA 程序

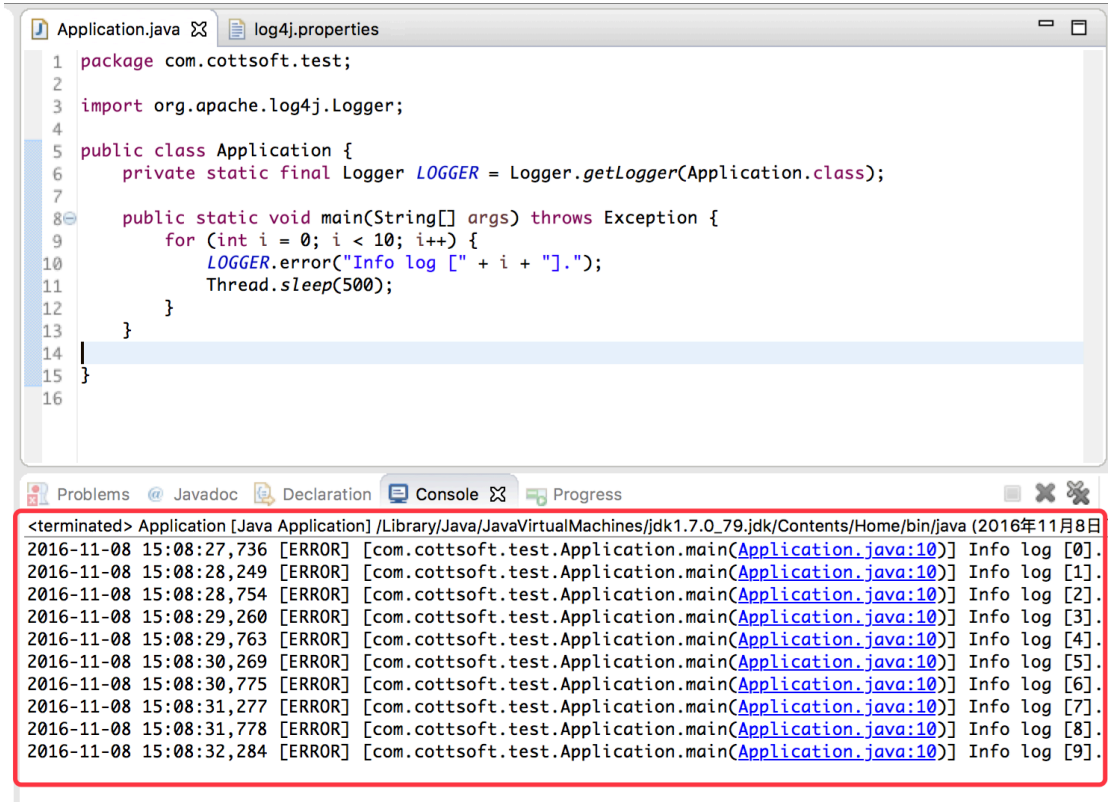


5.2 配置 log4j.properties

```
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
```

5.3 运行程序



The screenshot shows an IDE with two tabs: 'Application.java' and 'log4j.properties'. The 'Application.java' tab is active, displaying the following code:

```
1 package com.cottsoft.test;
2
3 import org.apache.log4j.Logger;
4
5 public class Application {
6     private static final Logger LOGGER = Logger.getLogger(Application.class);
7
8     public static void main(String[] args) throws Exception {
9         for (int i = 0; i < 10; i++) {
10             LOGGER.error("Info log [" + i + "].");
11             Thread.sleep(500);
12         }
13     }
14 }
15
16 }
```

The 'Console' tab is also active, showing the following log output:

```
<terminated> Application [Java Application] /Library/Java/JavaVirtualMachines/jdk1.7.0_79.jdk/Contents/Home/bin/java (2016年11月8日
2016-11-08 15:08:27,736 [ERROR] [com.cottsoft.test.Application.main(Application.java:10)] Info log [0].
2016-11-08 15:08:28,249 [ERROR] [com.cottsoft.test.Application.main(Application.java:10)] Info log [1].
2016-11-08 15:08:28,754 [ERROR] [com.cottsoft.test.Application.main(Application.java:10)] Info log [2].
2016-11-08 15:08:29,260 [ERROR] [com.cottsoft.test.Application.main(Application.java:10)] Info log [3].
2016-11-08 15:08:29,763 [ERROR] [com.cottsoft.test.Application.main(Application.java:10)] Info log [4].
2016-11-08 15:08:30,269 [ERROR] [com.cottsoft.test.Application.main(Application.java:10)] Info log [5].
2016-11-08 15:08:30,775 [ERROR] [com.cottsoft.test.Application.main(Application.java:10)] Info log [6].
2016-11-08 15:08:31,277 [ERROR] [com.cottsoft.test.Application.main(Application.java:10)] Info log [7].
2016-11-08 15:08:31,778 [ERROR] [com.cottsoft.test.Application.main(Application.java:10)] Info log [8].
2016-11-08 15:08:32,284 [ERROR] [com.cottsoft.test.Application.main(Application.java:10)] Info log [9].
```

5.4 Elasticsearch 查看日志

