ELK+filebeat 安装问题总结

ELK日志收集

官方文档 https://www.elastic.co/guide/index.html

中文帮助 https://www.gitbook.com/book/chenryn/elk-stack-guide-cn/details

网友博客写的配置帮助，如果版本不一样，不要参考。最好看官网的帮助文档

一，版本问题

5.0后的版本都统一了，但Elasticsearch5.0的head插件不太好装，很多插件还没有跟上来

推荐：

1、 Elasticsearch-2.3.2
2、 Kibana-4.5.0-linux-x64
3、 Logstash-2.3.2
4、 filebeat-5.0.0

elasticsearch

二，ES集群的Elasticsearch.yml配置顶格写，不要有空格。ES的数量要基数台（3台以上）

bin/elasticsearch －d   -- 后台运行

file-es.conf

#不能上网，插件离线安装

```
bin/plugin install  file:///home/ql/elasticsearch-head-master.zip
```

三，Logstash

后台运行：   nohup bin/logstash －f kafka-es.conf >/dev/null 2>1& &

file-es.conf:

```
input {
       file {
               path => “/opt/apache-tomcat-7.0.68/logs/localhost_access_log.2016-04-10.txt”
               start_position => “beginning”
       }
}
filter {
   grok {
               patterns_dir => “/opt/elk/logstash-patterns”
               match => {
                       “message” => “%{ACCESSLOG}”
               }
   }
}
output {
       elasticsearch {
           hosts => [“192.168.1.107”,“192.168.1.108”,“192.168.1.109”]
               index => “tomcat-%{yyyy/MM/dd}”
       }
}
```

filebeat-es.conf:

```
input {
   beats {
       port => 5044
   }
}
```

```
filter {
     grok {
         match => ["message", "%{COMMONAPACHELOG}%
{GREEDYDATA:additional_fields}"]
     }
}
output {
   elasticsearch {
       hosts => "10.154.238.233:9200"
       workers => 4
   }
}
```

kafka-es.conf:

```
input{
       kafka{
               type => "level-one"
               auto_offset_reset => "smallest"
               codec => plain{
                       charset => "GB2312"
               }
               group_id => "elas"
               topic_id => "accesslog"
               zk_connect
=>"192.168.1.200:2181,10.192.168.1201:2181,192.168.1.202:2181"
       }
}
filter{
       mutate{
               split => { "message" => "       "}
               add_field => {
                       "c1" => "%{message[3]}"
                       "c2" => "%{message[4]}"
               }
               remove_field => [ "message" ]
       }
}
```

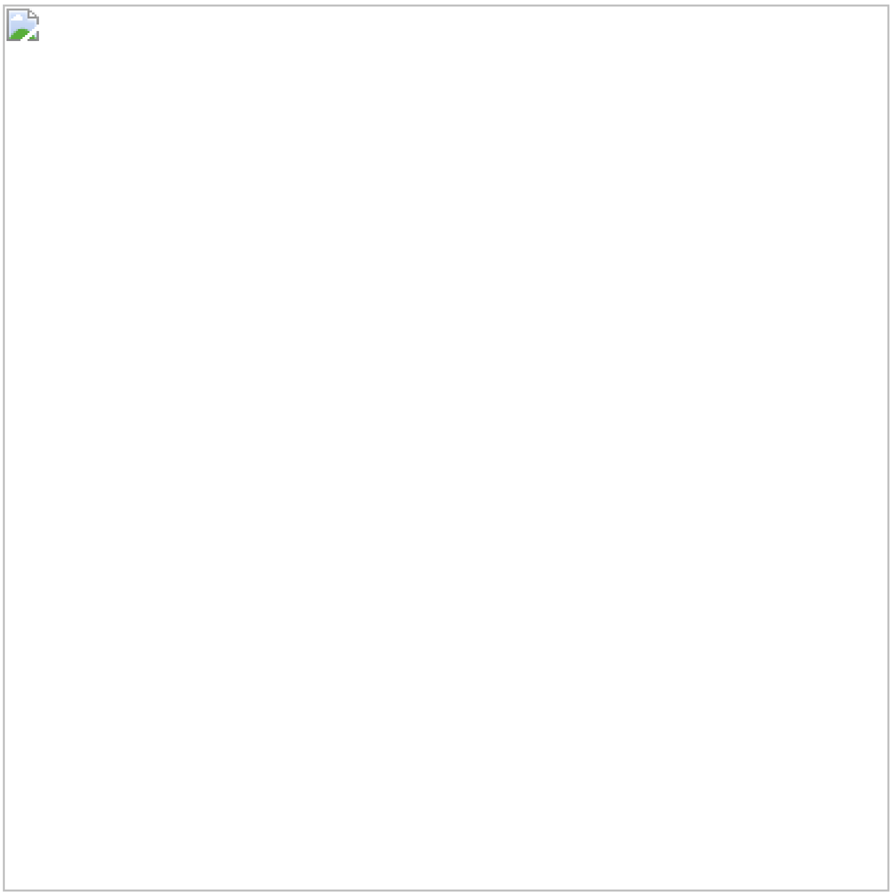
filebeat-kafka.conf:

```
input {
   beats {
       port => 5044
   }
}
filter {
     grok {
         match => ["message", "%{COMMONAPACHELOG}%{GREEDYDATA:additional_fields}"]
     }
}
output {
   kafka {
   topic_id =>"accesslog"
   codec => plain{
       format => "%{message}"
       charset => "UTF-8"
   }
       bootstrap_servers => "10.253.105.182:9092,10.253.105.167:9092,10.253.105.176:9092"
```

```
    }
}
```

四，kibana

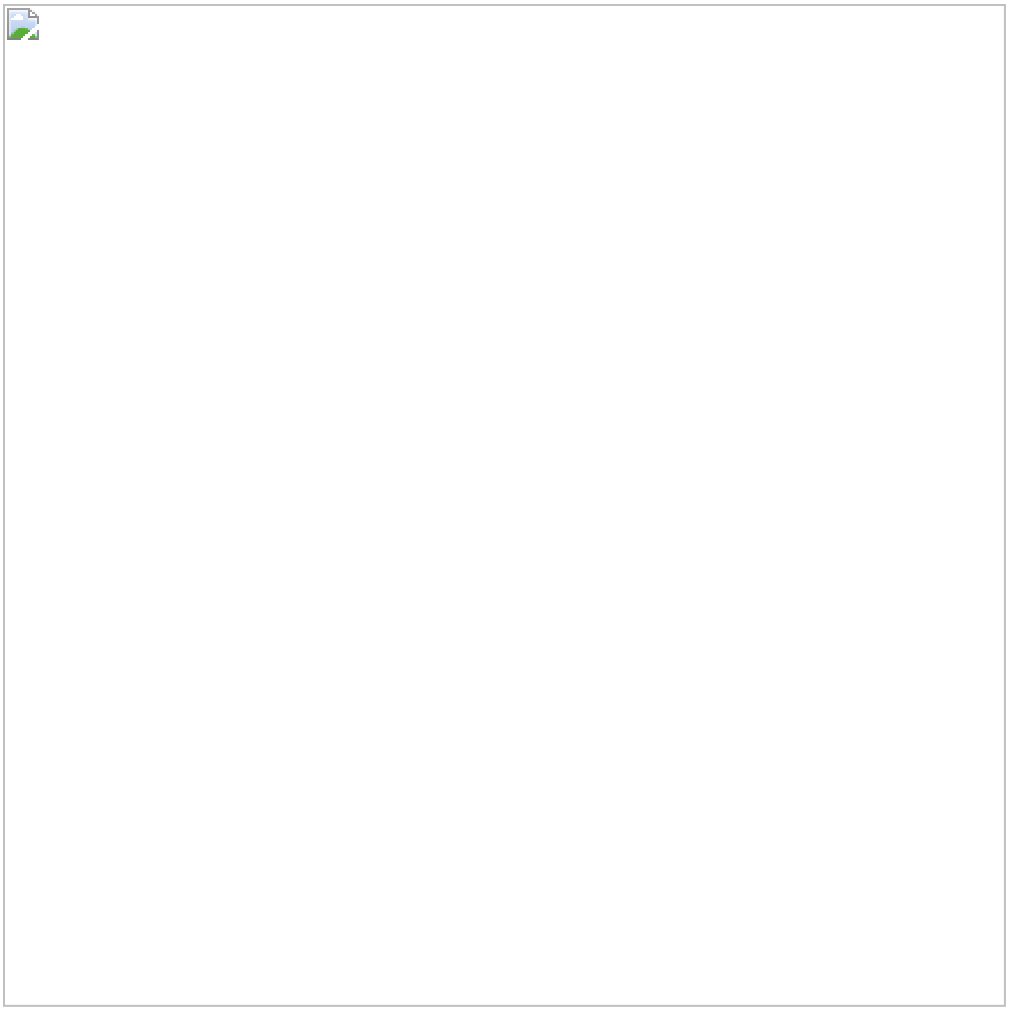
先settings 添加索引库



五，filebeat

更改日志目录

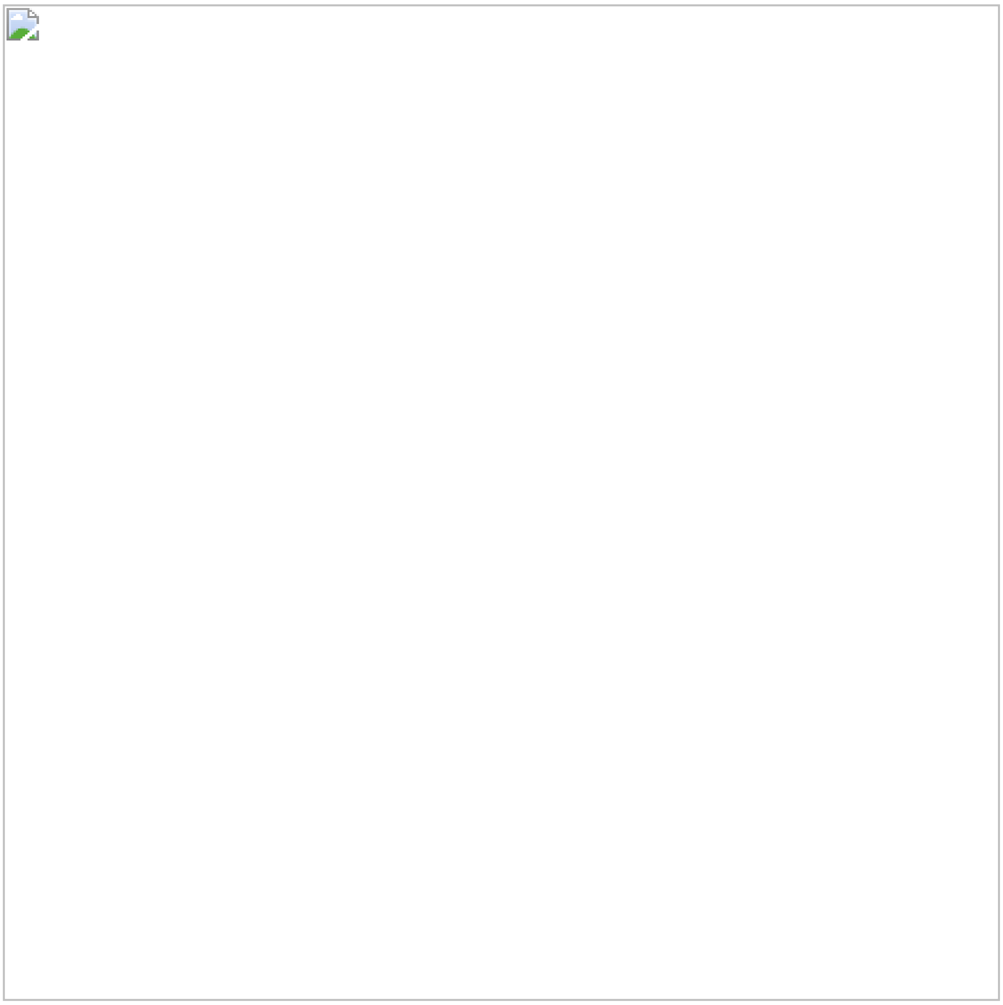
修改filebeat.yml



如果有多个日志目录，可以填写多行。

```
paths:
- /var/log/system.log # 指明读取文件的位置
- /var/log/wifi.log
```

注释elasticserrch,开放logstash,IP更改成192.168.1.88



```
#----------------------------- Logstash output --------------------------------
output.logstash:
hosts: ["192.168.1.88:5044"]
```