[**ELK测试笔记-filebeat输出到logstash**](http://blog.csdn.net/jianblog/article/details/54580300)

标签： [ELK](http://www.csdn.net/tag/ELK)

2017-01-17 09:50 3486人阅读 [评论](http://blog.csdn.net/jianblog/article/details/54580300#comments)(1) [收藏](javascript:void(0);) [举报](http://blog.csdn.net/jianblog/article/details/54580300#report)

http://static.blog.csdn.net/images/category_icon.jpg分类：

Elastic*（11）* http://static.blog.csdn.net/images/arrow_triangle%20_down.jpg

版权声明：本文为博主原创文章，未经博主允许不得转载。

目录[(?)[+]](http://blog.csdn.net/jianblog/article/details/54580300)

**测试说明**

通过filebeat监控nginx日志（已配置为json格式）。之后直接输出到logstash。

**filebeat配置**

增加部分：   
output.logstash:   
# The Logstash hosts   
hosts: [“192.168.100.34:5044”]   
index: shopweb

**logstash配置**

input {

beat {

port => 5044

codec => json # 直接将filebeat保存在message中的json字串解析出来

}

}

filter {

mutate {

remove\_field => ["tags", "beat"]

#删除filebeat自动添加的字段

## 测试发现：如果换成drop { remove\_field =>

## 无输出

}

}

output {

stdout {

codec => rubydebug

}

}

运行输出结果

{

"request" => "POST /dybuat/invest/getBorrowListPage.do?status=1 HTTP/1.1",

"referer" => "http://shopweb.dev/dybuat/invest/index.html?status=1",

"agent" => "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.87 Safari/537.36",

"offset" => 167804,

"input\_type" => "log",

"source" => "/var/log/nginx/access.log",

"type" => "log",

"http\_host" => "shopweb.dev",

"url" => "/dybuat/invest/getBorrowListPage.do",

"tags" => [

[0] "beats\_input\_codec\_json\_applied"

],

"upstreamhost" => "192.168.100.121:8081",

"@timestamp" => 2017-01-17T01:35:26.799Z,

"size" => "13932",

"clientip" => "192.168.20.32",

"host" => "192.168.100.70",

"@version" => "1",

"responsetime" => "0.018",

"xff" => "-",

"fields" => {

"log\_source" => "shopweb"

},

"upstreamtime" => "0.018",

"status" => "200"

}