[**ELK测试笔记：filebeat与logsmash写入redis**](http://blog.csdn.net/jianblog/article/details/54578094)

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

2017-01-16 22:41 2128人阅读 [评论](http://blog.csdn.net/jianblog/article/details/54578094#comments)(0) [收藏](javascript:void(0);) [举报](http://blog.csdn.net/jianblog/article/details/54578094#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/54578094)

**测试场景**

监控nginx日志并读取缓存到redis，后端logstash读取。其中nginx日志已经按照json格式进行输出。以下测试分别使用filebeat和logstash对相同输入(stdin)情况下，是否能正确得到json相应字段。

**filebeat采集**

## 采用stdin进行测试

- input\_type: stdin

#-------------- Redis output --------------

output.redis:

hosts: ["192.168.100.34"]

port: 6379

key: "shopweb"

* 1
* 2
* 3
* 4
* 5
* 6
* 7
* 8

**logstash采集**

input {

stdin {

codec => "json"

type => "nginx"

}

}

output {

redis {

host => "192.168.100.34"

data\_type => "list"

key => "shopweb"

}

}

* 1
* 2
* 3
* 4
* 5
* 6
* 7
* 8
* 9
* 10
* 11
* 12
* 13
* 14

**比较**

分别在采集端输入相同json字符串，然后命令行连接redis读取结果

#输入：

{"host":"192.168.100.32", "method":"GET", "status":300}

使用filebeat以json输入到redis，命令行读取：

"{\"@timestamp\":\"2017-01-16T14:00:04.261Z\",\"beat\":{\"hostname\":\"elk.dev\",\"name\":\"elk.dev\",\"version\":\"5.1.1\"},\"input\_type\":\"stdin\",\"message\":\"{\\\"host\\\":\\\"192.168.100.32\\\", \\\"method\\\":\\\"GET\\\", \\\"status\\\":300}\",\"offset\":0,\"source\":\"\",\"type\":\"log\"}"

使用logstash 以json输入到redis, 命令行读取的内容：

"{\"@timestamp\":\"2017-01-16T13:55:30.651Z\",\"method\":\"GET\",\"host\":\"192.168.100.32\",\"@version\":\"1\",\"type\":\"nginx\",\"status\":300,\"tags\":[]}"

* 1
* 2
* 3
* 4
* 5
* 6
* 7
* 8

**后端logstash读取redis**

input {

redis {

host => "192.168.100.34"

port => 6379

key => "shopweb"

type => "nginx"

data\_type => "list"

}

}

output {

stdout {

codec => rubydebug

}

}

* 1
* 2
* 3
* 4
* 5
* 6
* 7
* 8
* 9
* 10
* 11
* 12
* 13
* 14

后端读取结论： 只有在前端以logstash解析存入redis的结果才能读取还原原始字段， 而filebeat写入时嵌套了hash导致不能直接解析。 目前仍未完全掌握原因及采用filebeat方式是否有解决途径[初稿2017-01-16]。

**20170117补充**

filebeat解析日志保存到redis后，使用logstash再次读取后，原有所有信息保存在message字段中，为正确提取原始的字段信息，需要对message再次解码。这里需要使用fliter:json   
filter {   
json {   
source => “message”   
remove\_field => [“beat”, “message”]   
}   
}   
解析后删除原有message字段和filebeat自动增加的beat字段。