# Logstash 收集其它日志

## 日志样例

1. 2016-02-25 15:37:01 [main] INFO com.aliyun.sls.test\_log4j - single line log
2. 2016-02-25 15:37:11 [main] ERROR com.aliyun.sls.test\_log4j - catch exception !
3. java.lang.ArithmeticException: / by zero
4. at com.aliyun.sls.test\_log4j.divide(test\_log4j.java:23) ~[bin/:?]
5. at com.aliyun.sls.test\_log4j.main(test\_log4j.java:13) [bin/:?]
6. 2016-02-25 15:38:02 [main] INFO com.aliyun.sls.test\_log4j - normal log

## 采集配置

1. input {
2. **file** {
3. **type** => "common\_log\_1"
4. path => ["C:/test/multiline/\*.log"]
5. start\_position => "beginning"
6. codec => **multiline** {
7. pattern => "^\d{4}-\d{2}-\d{2} \d{2}:\d{2}:\d{2}"
8. negate => **true**
9. auto\_flush\_interval => 3
10. what => previous
11. }
12. }
13. }
14. output {
15. **if** [**type**] == "common\_log\_1" {
16. logservice {
17. codec => "json"
18. endpoint => "\*\*\*"
19. **project** => "\*\*\*"
20. logstore => "\*\*\*"
21. topic => ""
22. **source** => ""
23. access\_key\_id => "\*\*\*"
24. access\_key\_secret => "\*\*\*"
25. max\_send\_retry => 10
26. }
27. }
28. }

***注意：***

* *配置文件格式必须以 UTF-8 无 BOM 格式编码，可以下载 notepad++ 修改文件编码格式。*
* path*填写文件路径时请使用 UNIX 模式的分隔符，如：*C:/test/multiline/\*.log*，否则无法支持模糊匹配。*
* type*字段需要统一修改并在该文件内保持一致，如果单台机器存在多个Logstash配置文件，需要保证各配置*type*字段唯一，否则会导致数据处理的错乱。*

相关插件：[file](https://www.elastic.co/guide/en/logstash/current/plugins-inputs-file.html)、[multiline](https://www.elastic.co/guide/en/logstash/2.3/plugins-codecs-multiline.html)（若日志文件是单行日志，可以去掉 codec => multiline 配置）。

## 重启Logstash生效

创建配置文件到 conf 目录，参考[配置Logstash](https://help.aliyun.com/document_detail/49021.html)重启Logstash生效。

重要配置：

input {

stdin {

codec => plain{ charset => "GBK" }

}

file {

path => "C:/logs/admin-impl/logstash.\*.log"

}

}

filter{

json {

source => "message"

}

date {

match => ["timestamp" , "yyyy-MM-dd HH:mm:ss Z"]

}

}

output {

elasticsearch { hosts => ["localhost:9200"] }

stdout { codec =>json }

}