



链滴

# ELK 环境搭建之 logstash

作者: [toalaska](#)

原文链接: <https://ld246.com/article/1557236547625>

来源网站: [链滴](#)

许可协议: [署名-相同方式共享 4.0 国际 \(CC BY-SA 4.0\)](#)

# 下载地址

<https://www.elastic.co/downloads/logstash>

# 运行

```
./bin/logstash -f logstash.conf
```

## 新增一个配置文件first-pipeline.conf

配置说明 从 filebeat中收集日志 然后输出到标准输出和 elasticcsearch

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

filter {
  # grok {
    # match => { "message" => "%{IP:client} %{WORD:method} %{URIPATHPARAM:request} %{NUMBER:bytes} %{NUMBER:duration}" }

    # }
  json {
    source => "message" #要解析的字段名
    target => "msg_json" #解析后的存储字段， 默认和message同级别
  }
}

output {
  stdout{
    codec => rubydebug
  }
  elasticsearch { }
```

```
    hosts => [ "localhost:9200" ]  
}  
}
```

## 检查并启动

```
./bin/logstash -f config/first-pipeline.conf --config.test_and_exit
```

## 自动加载配置

```
./bin/logstash -f config/first-pipeline.conf --config.reload.automatic
```

## grok 插件 适合系统日志

### 日志示例

```
55.3.244.1 GET /index.html 15824 0.043
```

```
#filter  
  
grok {  
  
  match => { "message" => "%{IP:client} %{WORD:method} %{URIPATHPARAM:request} %{NUMBER:bytes} %{NUMBER:duration}" }  
  
}
```

## json 插件

```
json {  
  
  source => "message" #要解析的字段名  
  
  target => "msg_json" #解析后的存储字段， 默认和message同级别  
  
}
```

## nginx的过滤器

```
grok {  
  
  match => { "message" => "%{IP:client} - - \[%{HTTPDATE:logdate}\] \"%{WORD:verb} %{URIPATHPARAM:request} HTTP/%{NUMBER:httpversion}\\" %{NUMBER:http_status_code} %{NUMBER:status_code} %{NUMBER:bytes}" }  
  
}
```

```
:bytes} \"%{NOTSPACE:ref}\\" \"%{DATA:user_agent}\" }
```

```
}
```

```
date {
```

```
match => ["logdate", "dd/MMM/yyyy:HH:mm:ss Z"]
```

```
target => "@timestamp"
```

```
}
```

```
kv {
```

```
source => "request"
```

```
field_split => "&?"
```

```
value_split => "="
```

```
}
```

```
urldecode {
```

```
all_fields => true
```

```
}
```

## start\_position

从哪个位置读取文件数据， 默认从尾部， 值为： end

如果要导入历史数据则设置成： beginning

```
input {
```

```
file {
```

```
path => [/opt/flights2.csv" ]
```

```
start_position => "beginning"
```

```
}
```

```
}
```