# 引言

<https://www.elastic.co/cn/elastic-stack>

# 1 定义

E elasticsearch

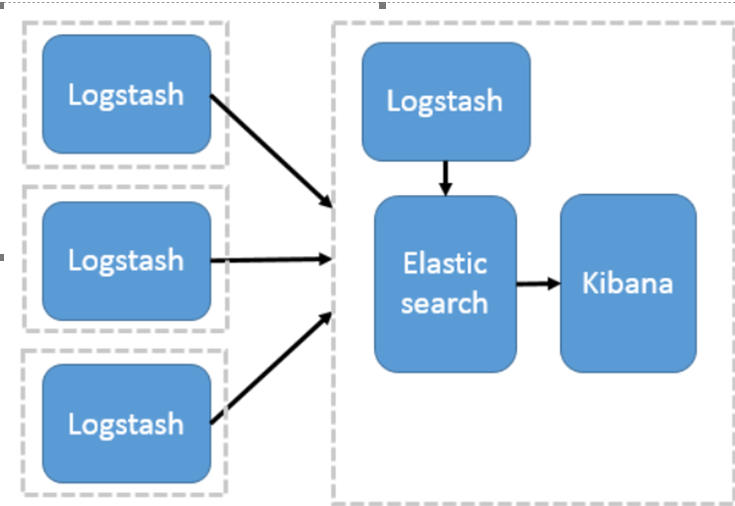
L logstash

K kibana

# 2 logstash

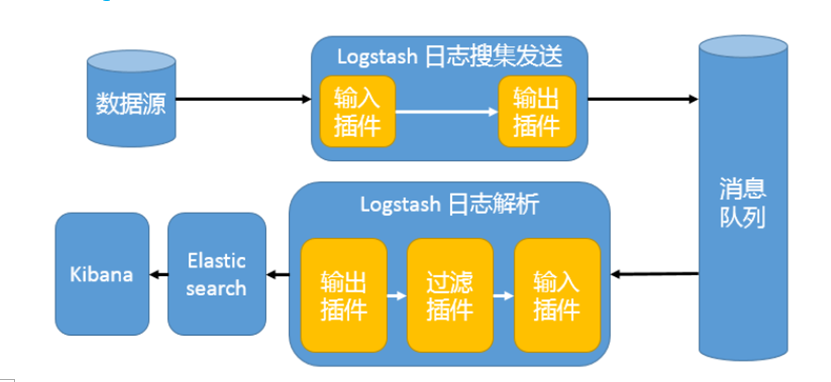
## 2.1 图解

一个详细结束的网址：<https://cloud.tencent.com/developer/article/1429335>



**缺点：每一个服务器上都需要部署笨重的logstash服务**

## 2.2 升级版



## 2.3 配置详解

**注意：真实配置的时候，请将全部注释去掉！这里是便于理解加上去的。**

可以在logstash目录下的任何文件夹下，创建一个配置文件，内容如下所示：

input {

file {

#这个是日志文件的来源路径

path => "E:/workspace/git/logstash-master/logs/house-info\*"

#这个是输出日志来源为文件，个人觉得没啥用

sincedb\_path => "E:/logstash-7.9.1/sincedb\_house"

codec => multiline {

pattern => "^%{TIMESTAMP\_ISO8601}"

negate => true

what => "previous"

#定义3秒输出更新的日志内容一次

auto\_flush\_interval => 3

}

}

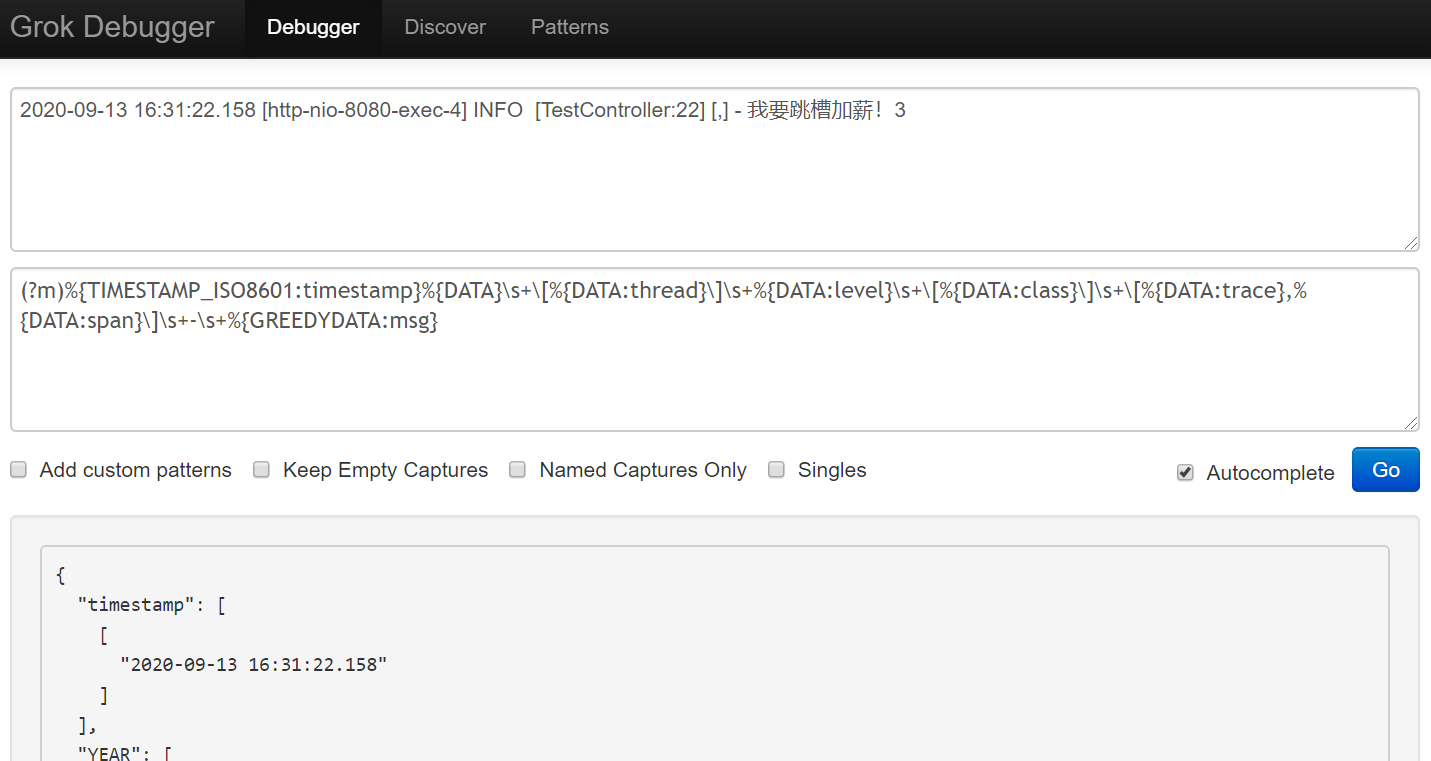
}

filter {

grok {

#定义日志输出格式，网址：<http://grokdebug.herokuapp.com/>

例如：



不懂配置规则，可以查看网址: <http://grokdebug.herokuapp.com/>

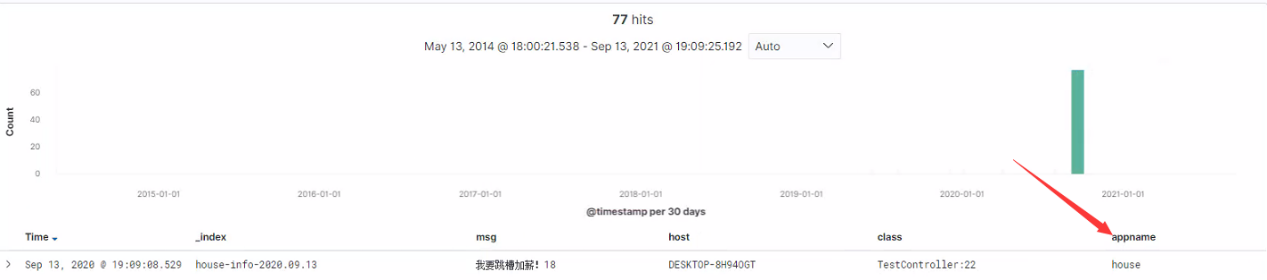
match => {

"message" => "(?m)%{TIMESTAMP\_ISO8601:timestamp}%{DATA}\s+\[%{DATA:thread}\]\s+%{DATA:level}\s+\[%{DATA:class}\]\s+\[%{DATA:trace},%{DATA:span}\]\s+-\s+%{GREEDYDATA:msg}"

}

}

#下行可以理解为定义日志类型



mutate {

"add\_field" => {"appname" => "house"}

}

}

output {

#下面配置输出到elasticsearch的配置

elasticsearch {

hosts => ["localhost:9200"]

index => "house-info-%{+YYYY.MM.dd}"

}

stdout {codec => rubydebug}

}

## 2.4 启动

**注意：先启动elasticsearch**

进入logstash根目录下，我的2.3配置文件名称为houseConfig，放在根目录下，那就：

进入bin目录下，cmd执行： logstash.bat -f ../houseConfig

多配置文件启动：logstash.bat -f ../config/mineconfig

这里再config文件夹下继续创建了mineconfig文件夹，里面放了很多类似houseConfig的配置文件。

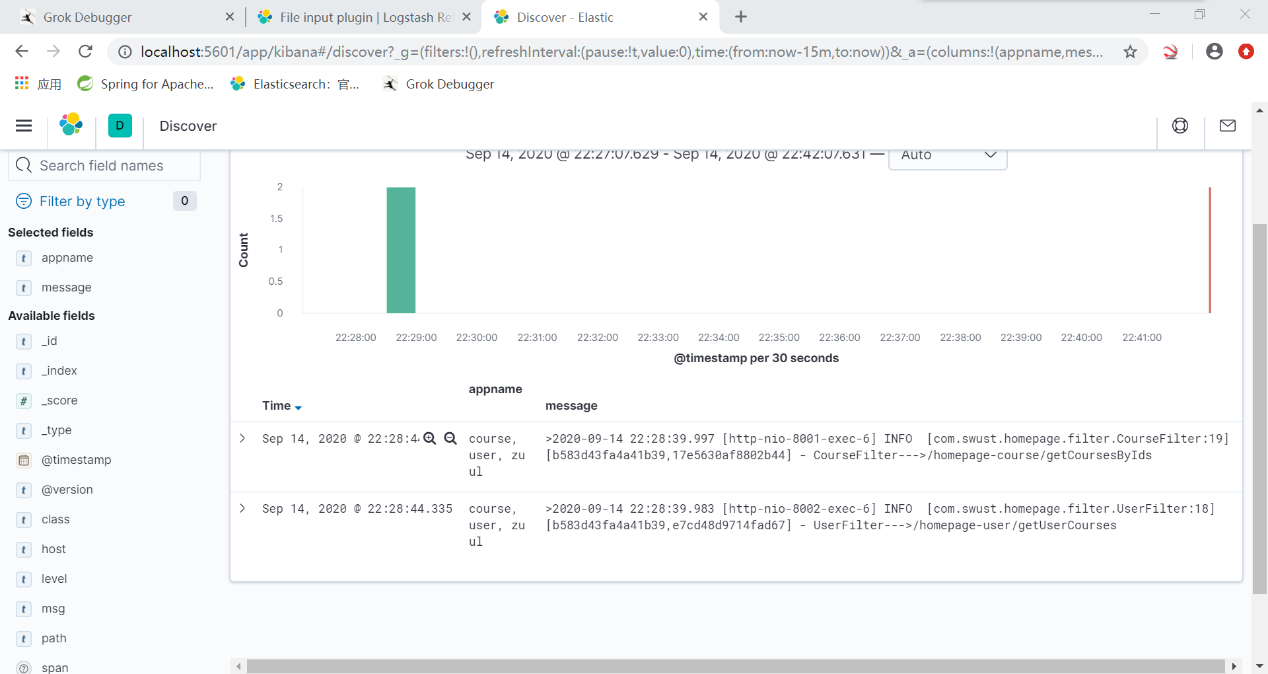
# 3 elasticsearch

进入elasticsearch所在的根目录，cmd进入bin文件夹，执行elasticsearch.bat即可。

相关极简用法参考网址：<http://www.ruanyifeng.com/blog/2017/08/elasticsearch.html>

# 4 kibana

进入kibana所在的根目录，cmd进入bin文件夹，执行kibana.bat即可。执行完毕最后一行会有登录网址的，打开网址就可看到页面了！



请求一个URL，路径上的所有信息都被显示出来了。上图过滤条件为：

trace:b583d43fa4a41b39，这里的trace就是这条sleuth信息