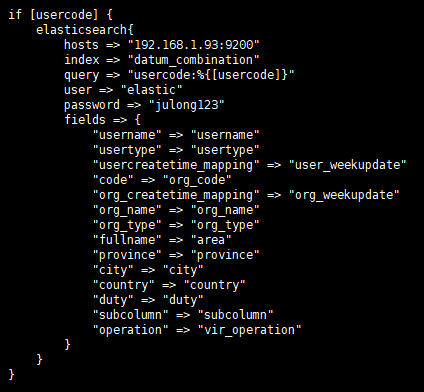
ELK部分功能总结

一、实时日志中用户ID和组织ID与数据库中注册用户相匹配

用插件logstash-jdbc-input，与mysql数据库同步，注意在上传数据库中两个表的内容时，数据不能冲突，否则传不上去。

利用usercode和数据库中的信息进行匹配：



query前：数据库，后：日志

field前：数据库，后：合并后

1. 对实时日志的处理：logstash中filter文件配置

（1）传入的每一条数据储存在”message”字段中

（2）插件：

2-1. grok：主要用于正则匹配

filter{

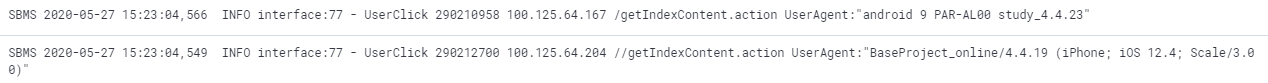
grok{

Match => {“字段名” => “(?<字段名>匹配规则)”}

}

}

如对以下信息的匹配：



代码：

1590564107(1)

2-2. gusb插件

mutate中gusb可用于替换

1590564330(1)

表示将link字段中的//换成/

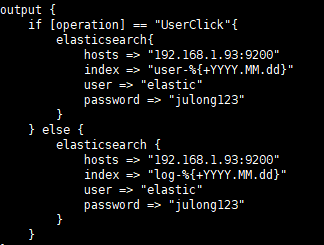
2-3. translate插件

翻译过滤器根据哈希或文件中指定的替换值替换字段内容。目前支持这些文件类型:YAML、JSON和CSV。



表示获取useragent\_from\_中的字段的值，并根据字典中的值将其转化，即，android、iphone转化为手机端，其余的内容转化为PC端，存储在useragent\_from字段中。

1. 在kibana中输出为多个索引



三、Kibana的使用

1. 开发者工具：
   1. 若出现索引长时间上传不上去或索引模式不能删除的情况，可在开发工具里执行

PUT \_settings

{

"index": {

"blocks": {

"read\_only\_allow\_delete": "false"

}

}

}

注意：此语句慎用，会将索引模式给删去。

* 1. Grok Debugger可以在线调试filter对日志内容的正则化匹配

1. 管理：

2-1. 汇总/打包作业，可以根据需求按时间进行汇总，并将某些字段进行聚合从而节省调用时长。

2-2. 已保留对象

当已经创建好可视化图表时，若不小心删去索引或索引模式，可以通过索引模式的id重新指向可视化图表。具体如下：

1. 重建索引模式，查询其id。

在开发者工具里执行：

GET /.kibana/\_search

{

"query" :{

"match" :{

"index-pattern.title": "user\*"

}

}

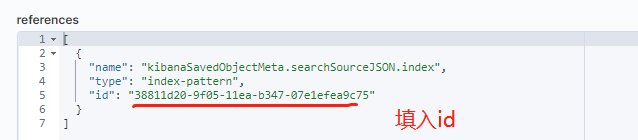
}

其中index-pattern.title为所建索引模式的名字。



划线部分即为id.

1. 在已保留对象中选择调用该索引模式的可视化图表，操作->检查，在id中填入刚刚查找的id。



至此，可视化图表又可使用。

此外，也可将可视化图表导出。

四、图表导出

仪表盘->检查->csv下载

五、更改logstash中filter的配置后重新上传相同索引，可能出现新添加的字段无法可视化（字段前是？表示该字段类型不可知），这时可将该索引刷新后方可使用。