# logstash方案总决定

1.多个file分开采集，对于三大类（系统，安全，应用）分开采集

2.去重

3.~~去重方案研究（1，2）还没决定~~

~~（补1:目前倾向于方案二）~~

4.grok字段：时间戳，日志源，pid，日志等级（可选，数据库没有参数时默认为null），日志内容

5.logstash用配置文件中的output插件进行对MySQL数据库的连接

6.决定用去重方案二

——————————————————————————————————