安装Elasticsearch，配置Elasticsearch确保日志的存储和Elasticsearch的正常运行。安装Kibana，配置Kibana使Kibana与安装好的Elasticsearch相连，确保日志的可视化功能的正常运行。安装Packetbeat，对Packetbeat的日志收集部分进行详细配置，将Packetbeat监视的每个端口的采集处理填写完整，对Packetbeat的日志输出部分进行配置，完成Beat向Kafka的传输。完成Kafka的安装与配置以及根据Packetbeat采集的日志标签创建相关topic。安装Logstash，将Kafka的输入，根据日志标签的分类处理流程，向Elasticsearch输出写在Logstash的配置文件里。按照Elasticsearch、Kibana、Kafka、Logstash、Packetbeat的顺序运行软件，检查其中是否与连接错误，修改其中的连接错误确保传输没有任何问题。使用Go语言和开源框架libbeat开发出一个具有全盘扫描获取日志并对日志进行简单分析添加标签的Beat软件。将自制的Beat软件插入到目前的运行队列里，停止Packetbeat、Kafka、Logstash的运行。配置自制的Beat软件的日志输出部分，完成Beat向Kafka的传输。对Kafka进行配置根据自制的Beat软件可能会创建的日志标签创建出新的topic。对Logstash的配置文件进行修改，添加上自制的Beat软件可能会创建的日志标签的处理过程，启动Kafka、Logstash、Packetbeat、自制Beat。

完成日志消息队列的开源软件Kafka的安装与配置以及Kafka 相关topic的创建。对Logstash进行配置将按照Beat的类型和日志分类的标签分别写处理流程。配置Elasticsearch确保日志的存储和Elasticsearch的正常运行。配置Kibana确保日志的可视化功能的正常运行。

使用Go语言和开源框架libbeat开发出一个具有全盘扫描获取日志并对日志进行简单分析添加标签的Beat软件，将制作出来的Beat软件和开源软件Packetbeat进行配置，使两个Beat软件将日志传递到日志消息队列的开源软件Kafka。配置Kafka，使Kafka能够接收自制Beat和Packetbeat发送来的日志并且将日志发送到日志处理软件Logstash。配置Logstash，使Logstash按类型标签处理自制Beat和Packetbeat采集的日志，Logstash将处理好的日志传送给Elasticsearch进行存储和检索。