# 日志分析

## 第一阶段

（1）收集各种日志坐标并统计用途（7.3）

可直接使用命令（cat等）或工具采集的  
/var/log/messages 系统的主日志  
/var/log/mysqld.log mysql数据库日志  
/var/log/boot.log 记录系统启动时的服务启动情况  
/var/log/secure 记录与安全相关的事件，尤其是用户认证、登录尝试等  
/var/log/maillog 邮件服务（如 Postfix、Sendmail）的日志  
/var/log/cron 记录定时任务（crontab 和 systemd timer）的执行情况  
/var/log/nginx/access.log 记录所有客户端对 Nginx 的访问请求   
/var/log/nginx/error.log 记录 Nginx 自身的错误信息  
/var/log/firewalld 记录 firewalld 服务的运行状态和规则变更  
  
需要特殊命令采集的（如last）  
/var/log/wtmp 记录系统中所有用户的成功登录、注销以及系统启动/关机事件。  
/var/log/btmp 记录所有失败的登录尝试

（2）研究**Logstash（7.4-7.6）**

在主机上配置环境，下载好logstash了

正在研究配置文件（7.5：10.31）

放到/etc/logstash/conf.d/路径下，logstash会读取该路径下.conf结尾的文件

配置文件初步研究，卡在日志太多，读取日志时超过二十秒就开始乱码

使用“beginning”就会卡在二十秒后的乱码

使用“ending”读取日志速度太慢，且无法把握采集的日志是否包含所需日志

目前有进展，但未解决（7.3）思路：如果使用ending的话历史文件就用“tail”去采集

（3）研究MySQL和**Logstash的连接（7.3）**

**与配置文件中的output插件有关**

**需配置jdbc和数据库语句**