ELK总结

ELK分别代表：

–E: Elasticsearch负责日志检索和储存(非关系型数据库,java开发的, 重要级:1)

–L: Logstash负责日志的收集和分析、处理(重要级:2)

–K: Kibana负责日志的可视化(把数据做成网页,重要级:3)

工作流程:

Web日志、通过filebeat发送数据--->Logstash格式化数据----->E(elastic...)储存数据<------>Kibana从E读取数据、把数据做成页面

Filebeat把日志发给logstash,

logstash通过配置文件的input插件接收数据,在通过filter过滤插件,把数据处理成

Filebeat

直接安装

配置文件: