章节三 Logstash零基础入门到采集日志实战

11、Logstash基本介绍和使用场景

简介：讲解什么是logstash，里面的基本工作流程input,filter,output等说明

什么是logstash (文档地址 https://www.elastic.co/guide/en/logstash/current/index.html)

开源的日志收集引擎，具备实时传输的能力

读取不同的数据源，并进行过滤，开发者自定义规范输出到目的地

日志来源多（如系统日志，应用日志，服务器日志等）

流程讲解

logstash通过管道pipeline进行传输，必选的两个组件是输入input和输出output，还有个可选过滤器filter

logstash将数据流中等每一条数据称之为一个event,即读取每一行数据的行为叫做事件

#输入

input {

...

}

# 过滤器

filter {

...

}

# 输出

output {

...

}