##### Logstash

官网：<https://www.elastic.co/cn/logstash>

文档：<https://www.elastic.co/guide/en/logstash/current/index.html>

论坛：<https://discuss.elastic.co/c/elastic-stack/logstash/14>

下载：<https://www.elastic.co/cn/downloads/logstash>

Logstash welcomes data of all shapes and sizes.

###### 安装

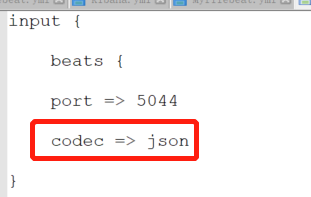
安装参考：<https://blog.csdn.net/Smookey/article/details/84202584>

官网GetStarted: <https://www.elastic.co/guide/en/logstash/current/getting-started-with-logstash.html>

测试安装成功：logstash -e "input { stdin { } } output { stdout {} }"

###### Conf文件

filebeat无下列设置则看不到效果。



###### 启动config文件命令

logstash -f xxx.conf -- config.reload.automatic

###### 各个场景使用

<https://www.cnblogs.com/qingqing74647464/p/9378385.html>

###### http input

<https://www.elastic.co/guide/en/logstash/current/plugins-inputs-http.html>

<https://kitwaicloud.github.io/elk/logstash.html>

<https://stackoverflow.com/questions/37434739/how-to-use-logstash-plugin-logstash-input-http>

监控主机端口被请求的http请求，会添加host及header信息。

需要postman或者浏览器辅助测试。

目前在本机测试只有8080端口可以正常让logstash运行。

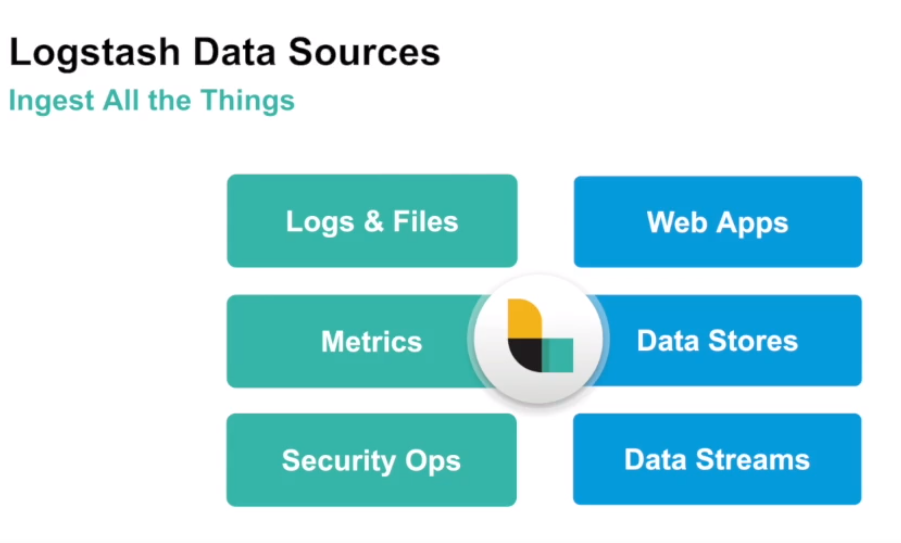
###### http\_poller input

会每隔1分钟去设定的url拿数据；

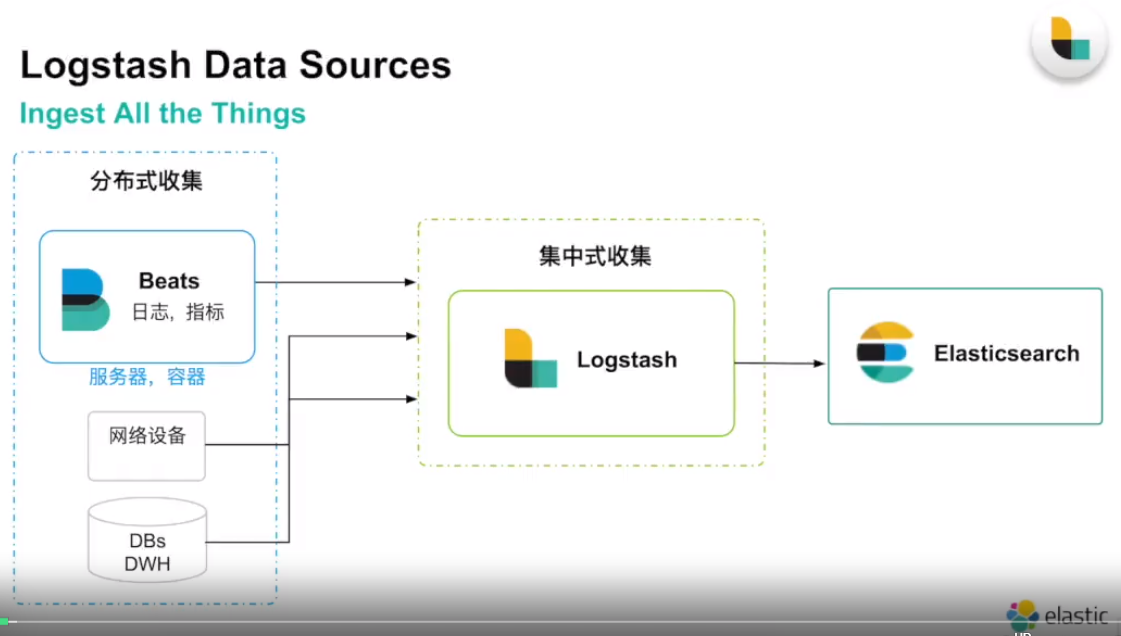
怀疑schedule设置轮询时间。

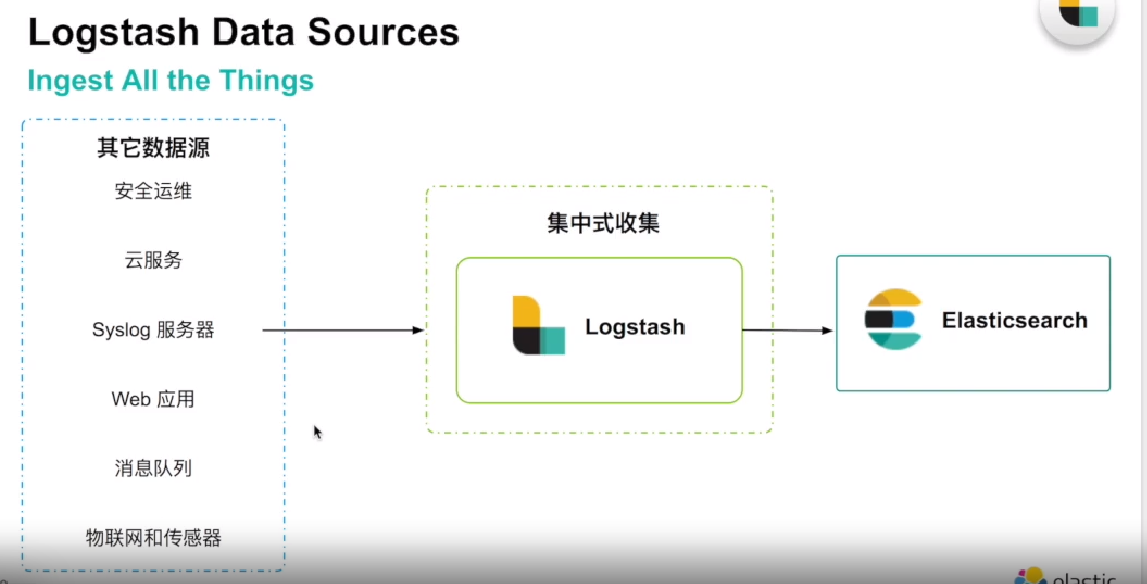
###### 简介



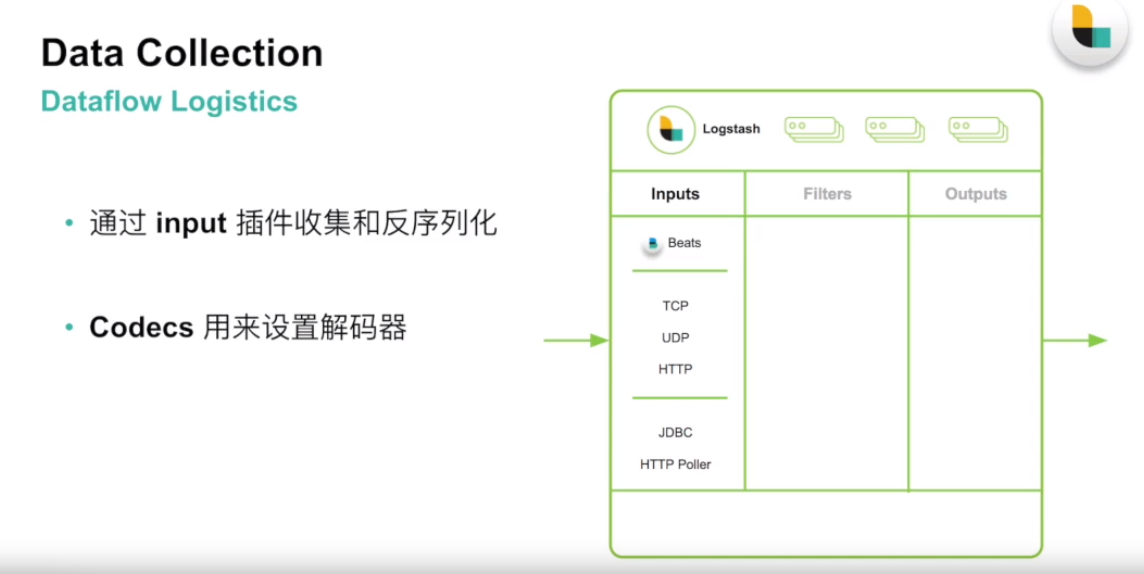


###### 收集数据的架构

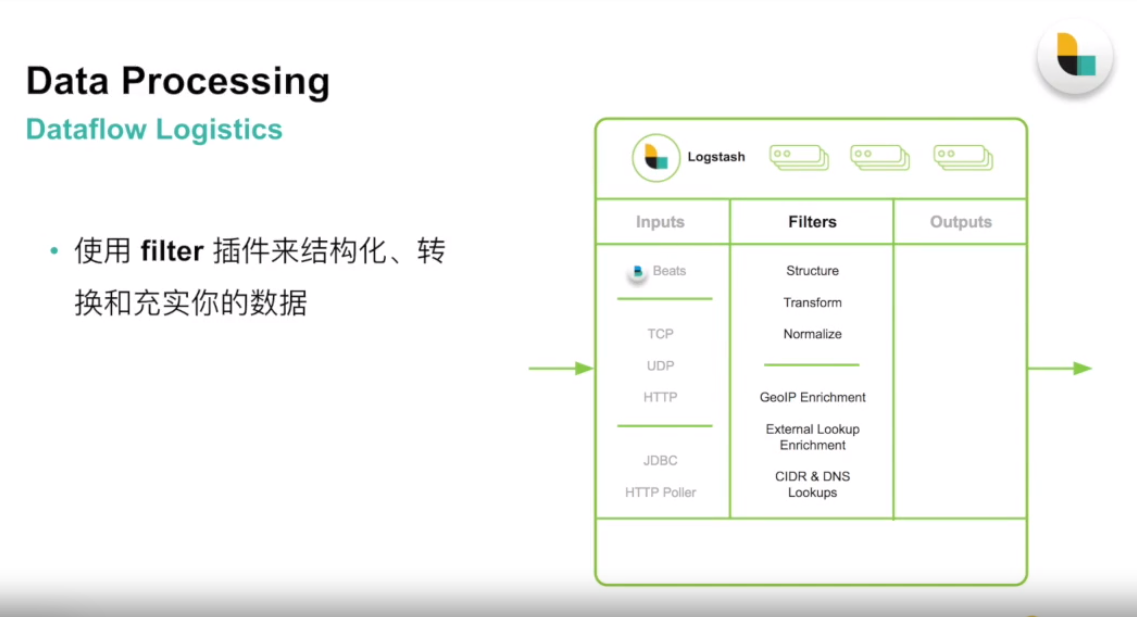




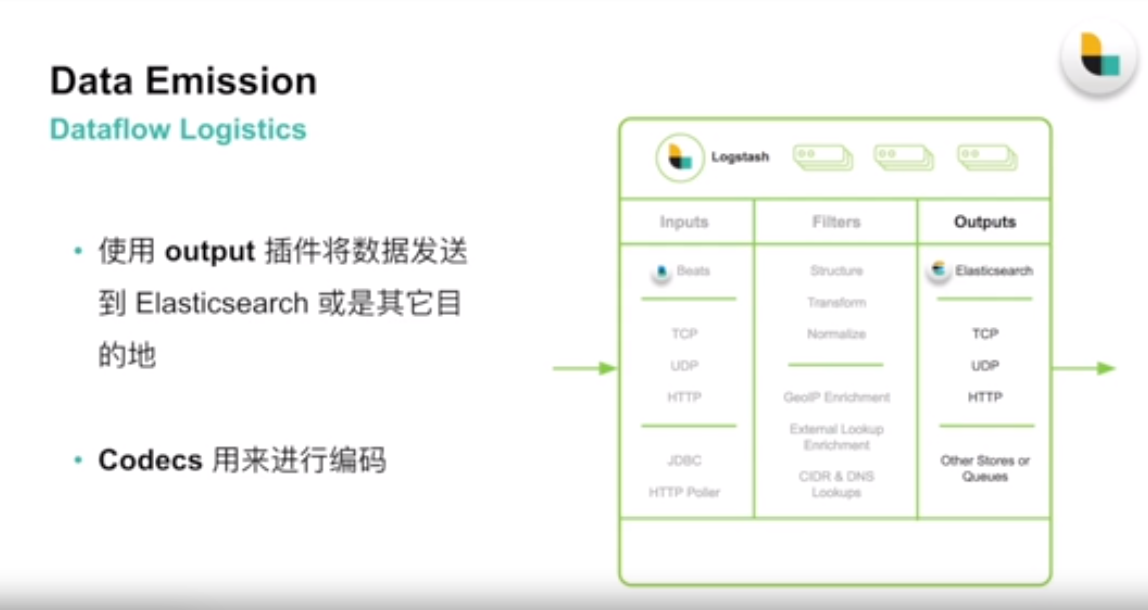
###### 输入插件



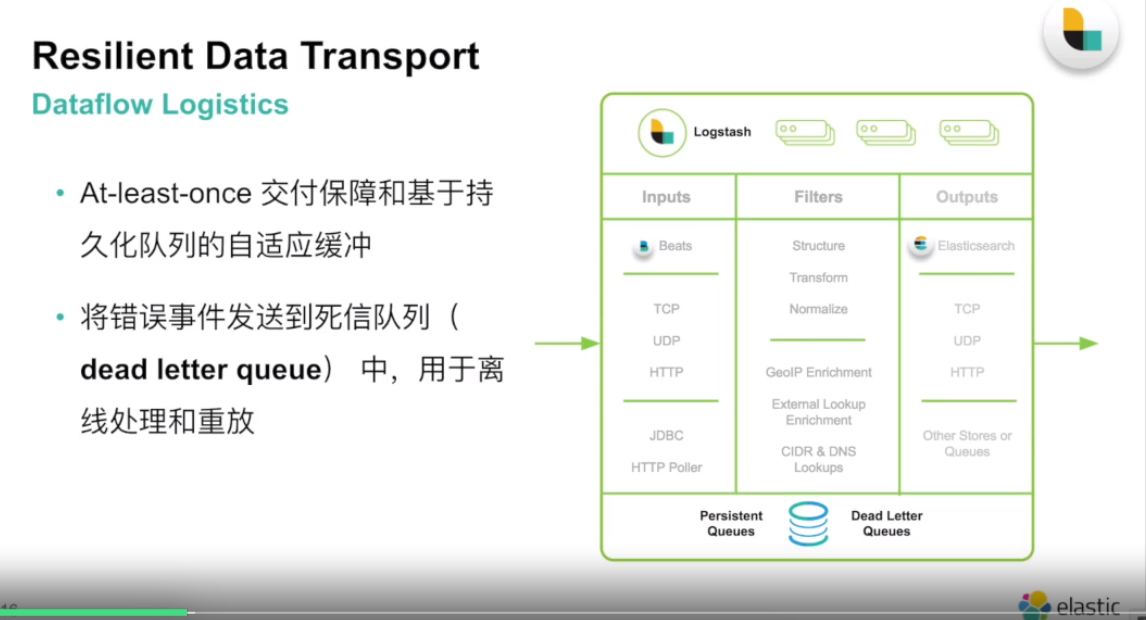
###### Filter(数据处理方法)



###### Output

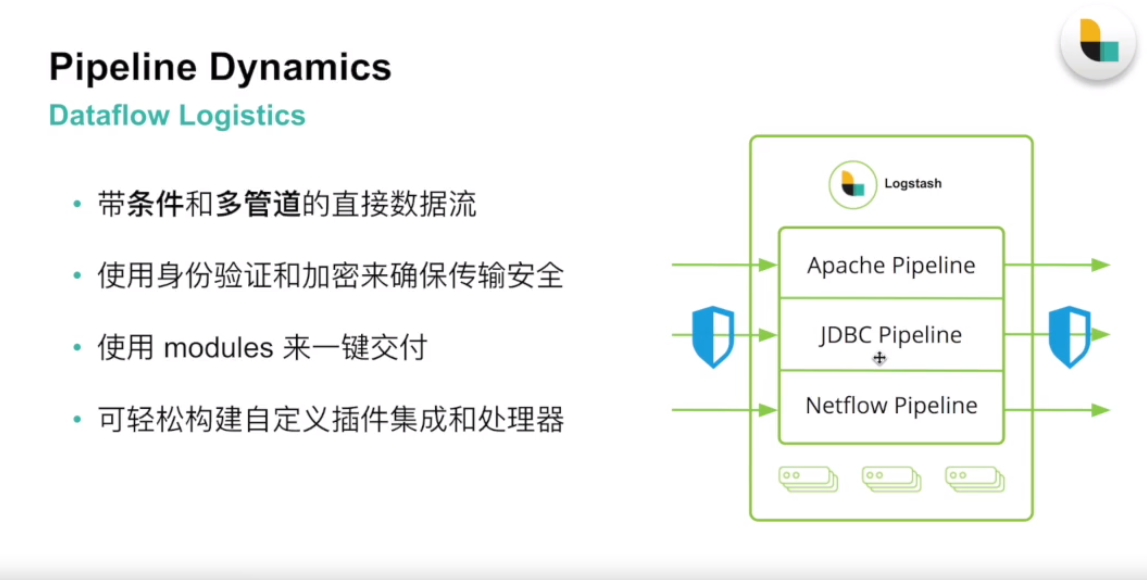


###### Resilient data transport



###### Pipeline Dynamics

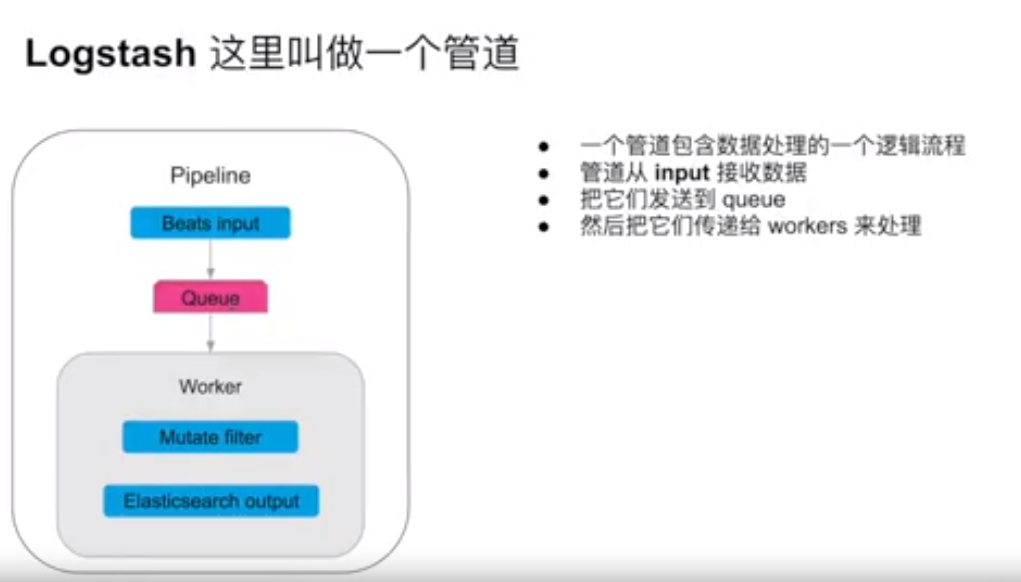
动态创建管道 动态加载

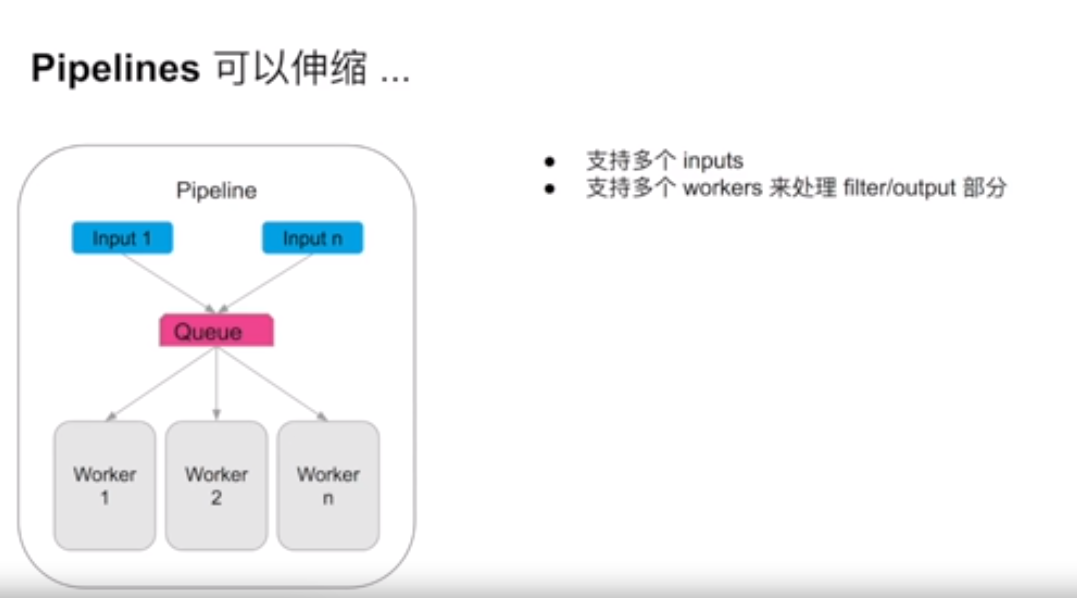


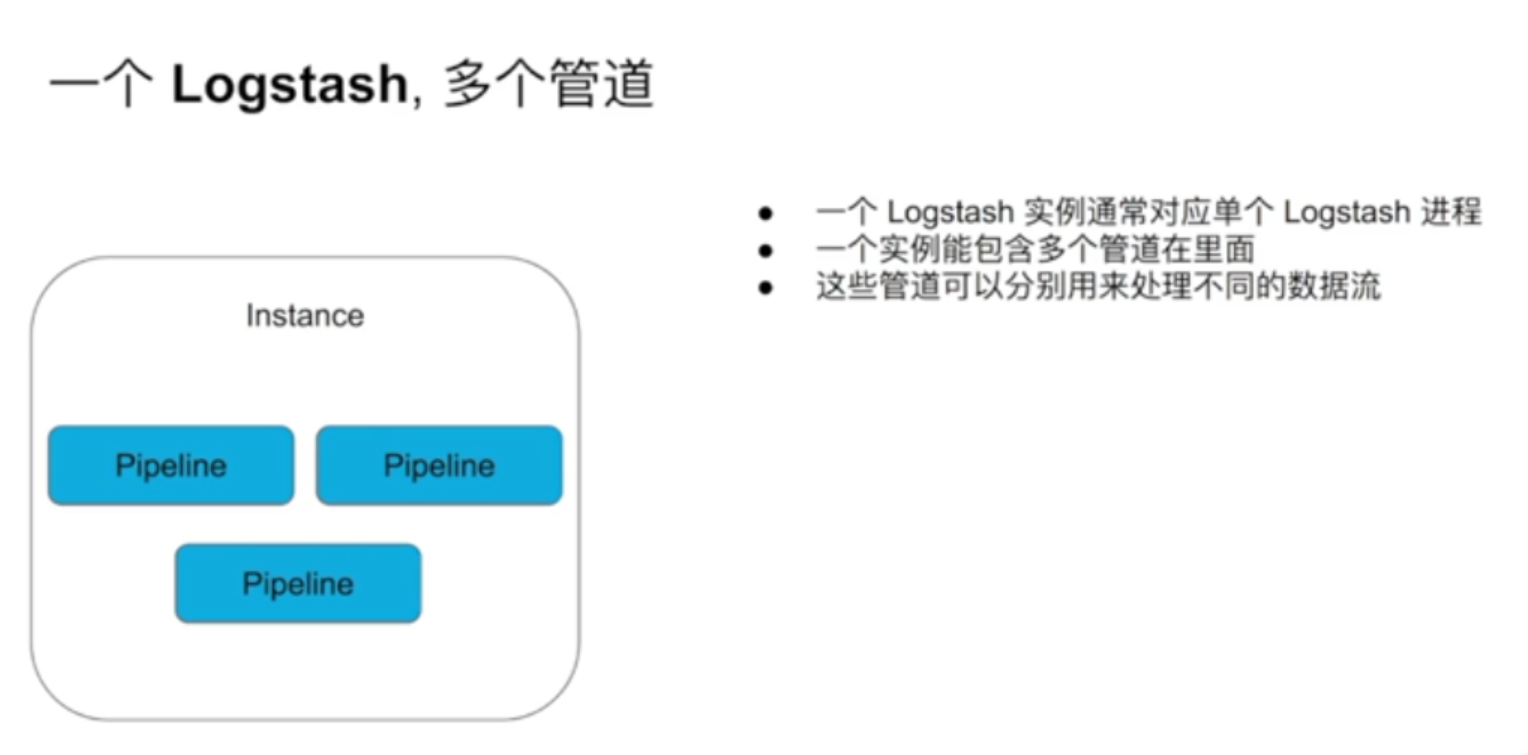
###### 一个事件



###### 执行模式

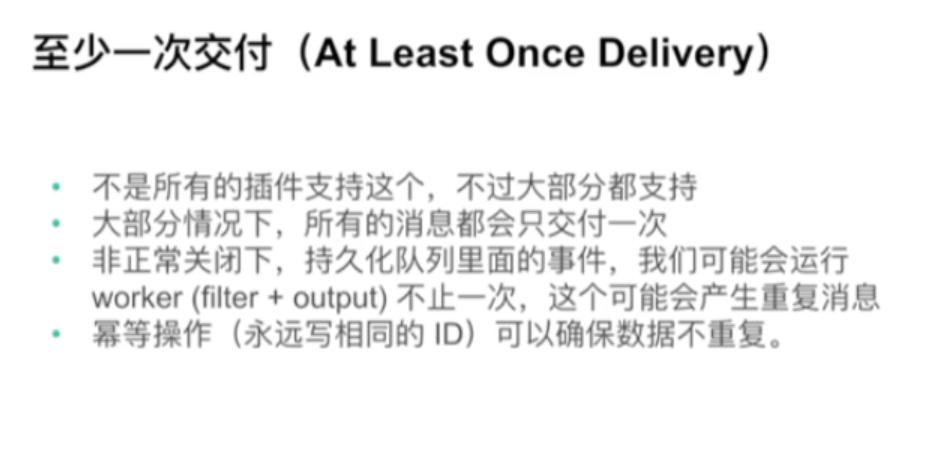




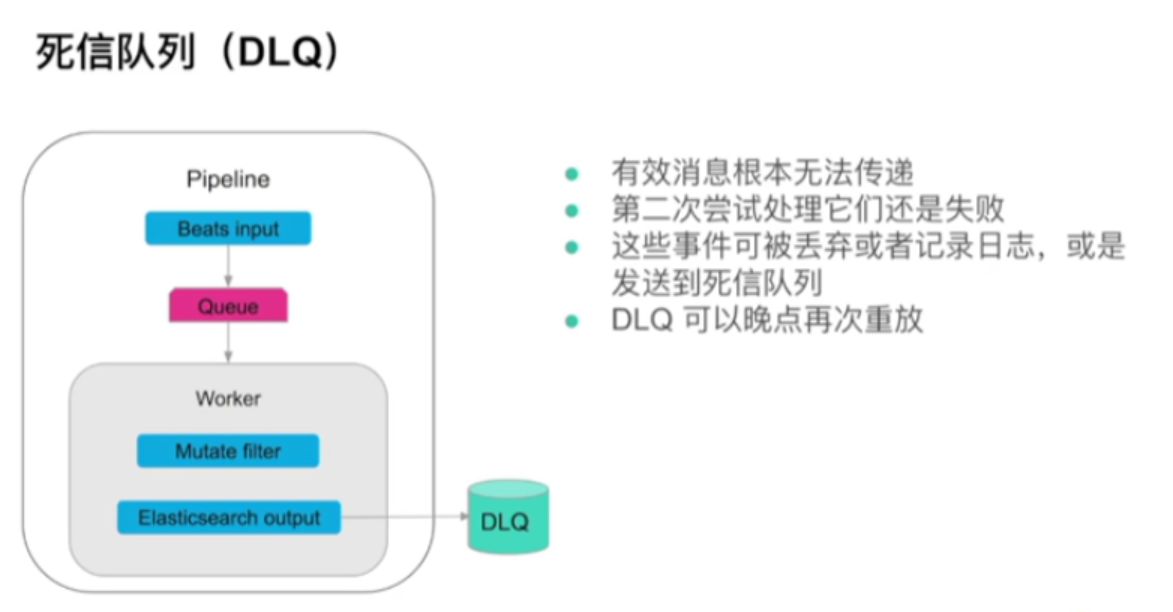


###### 队列和交付保障

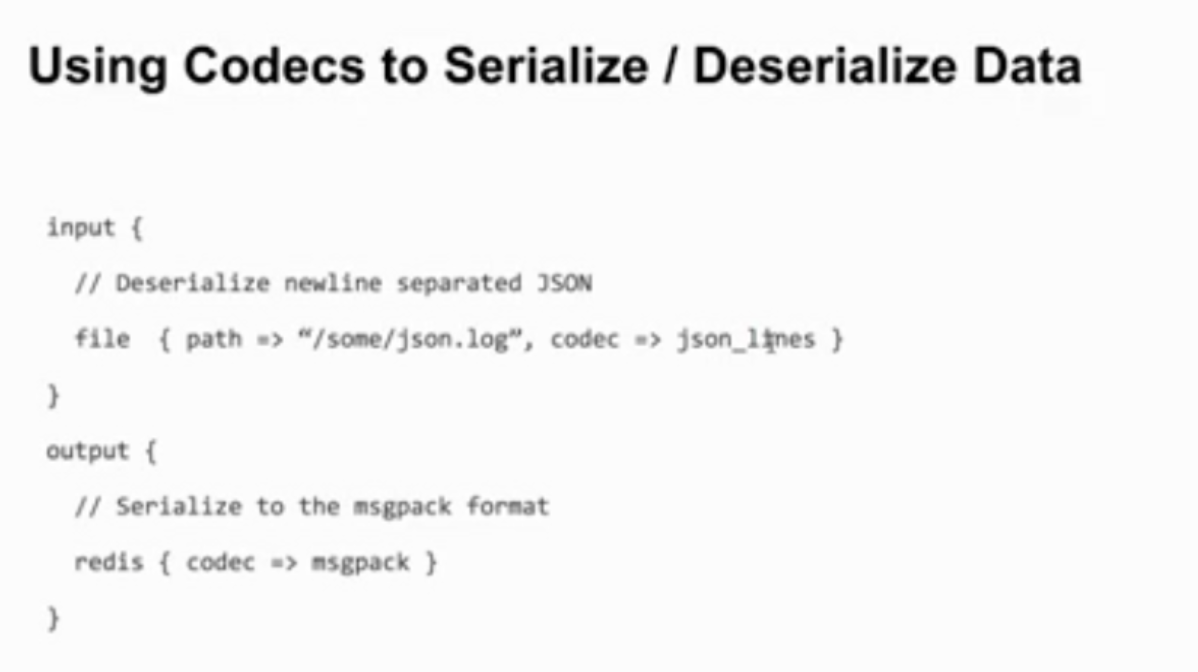


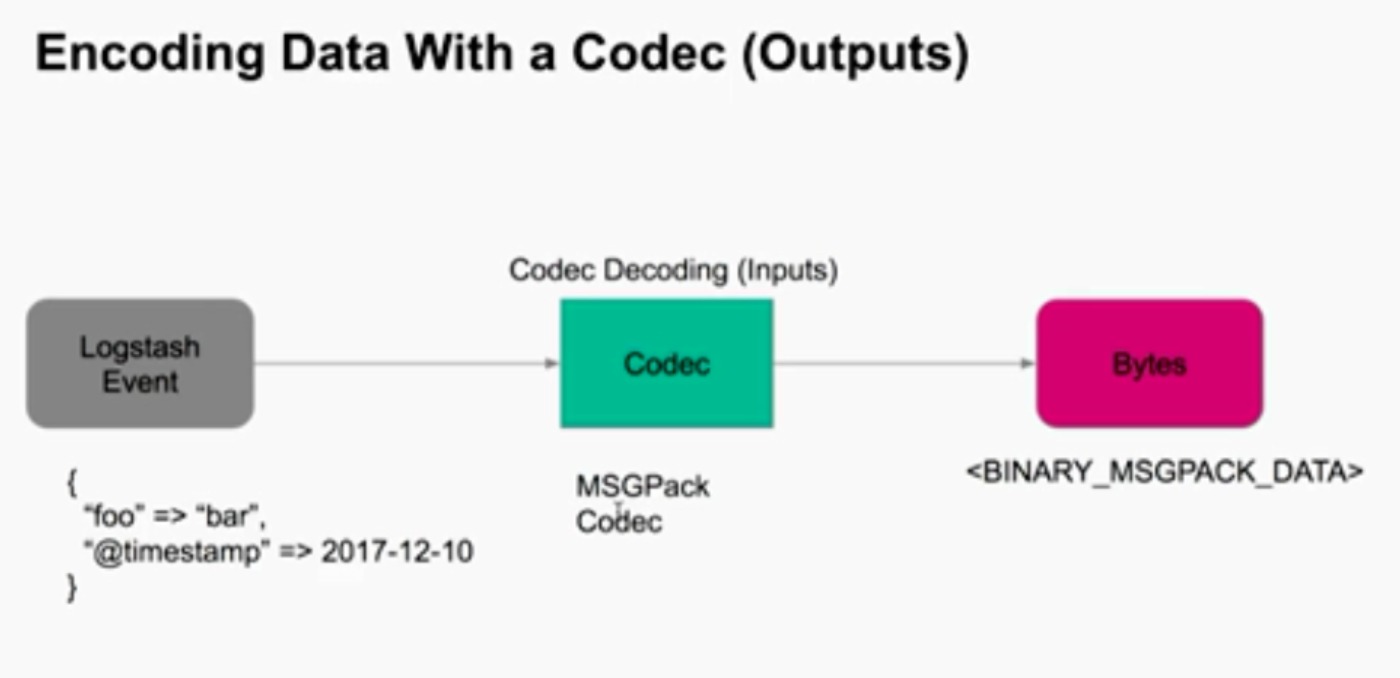


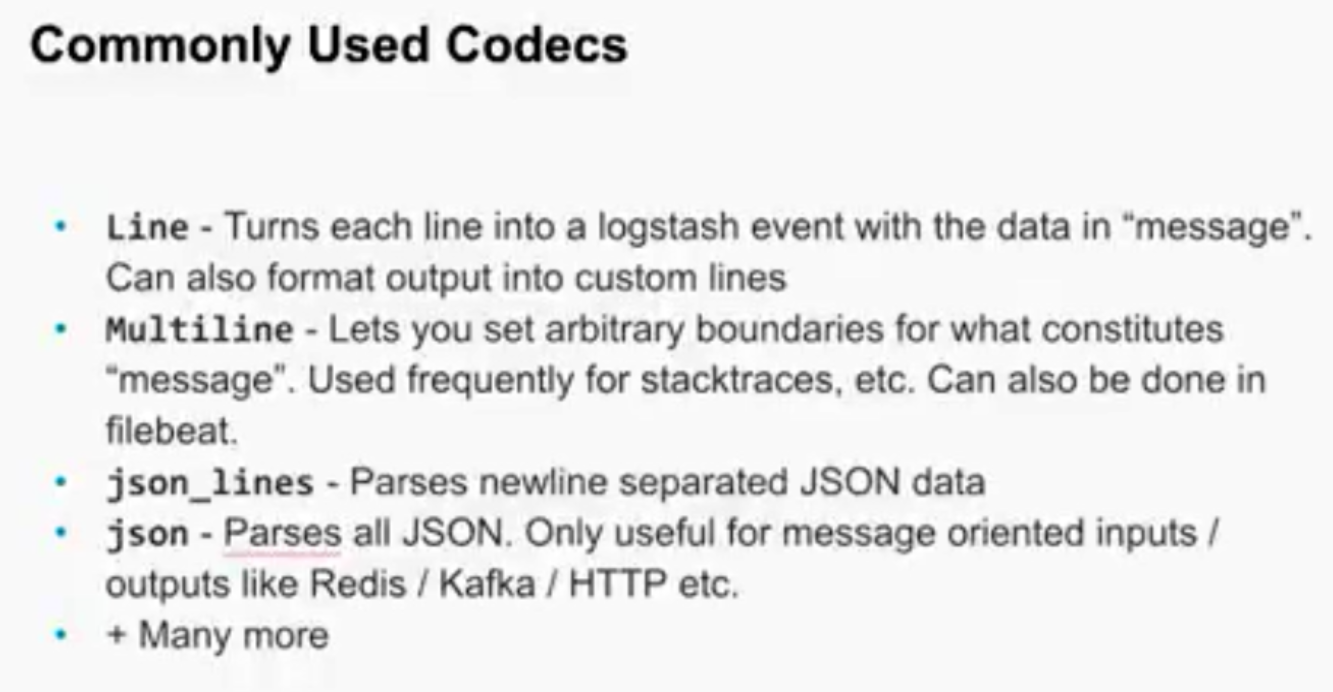
###### 死信队列



###### Codecs与序列化





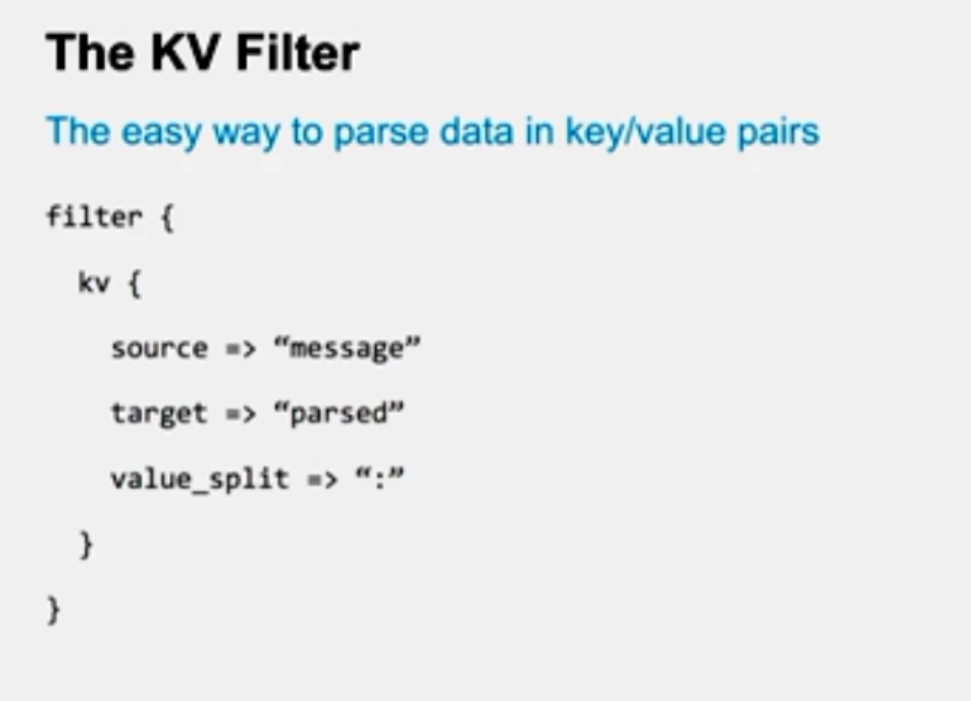


###### 解析/抽取

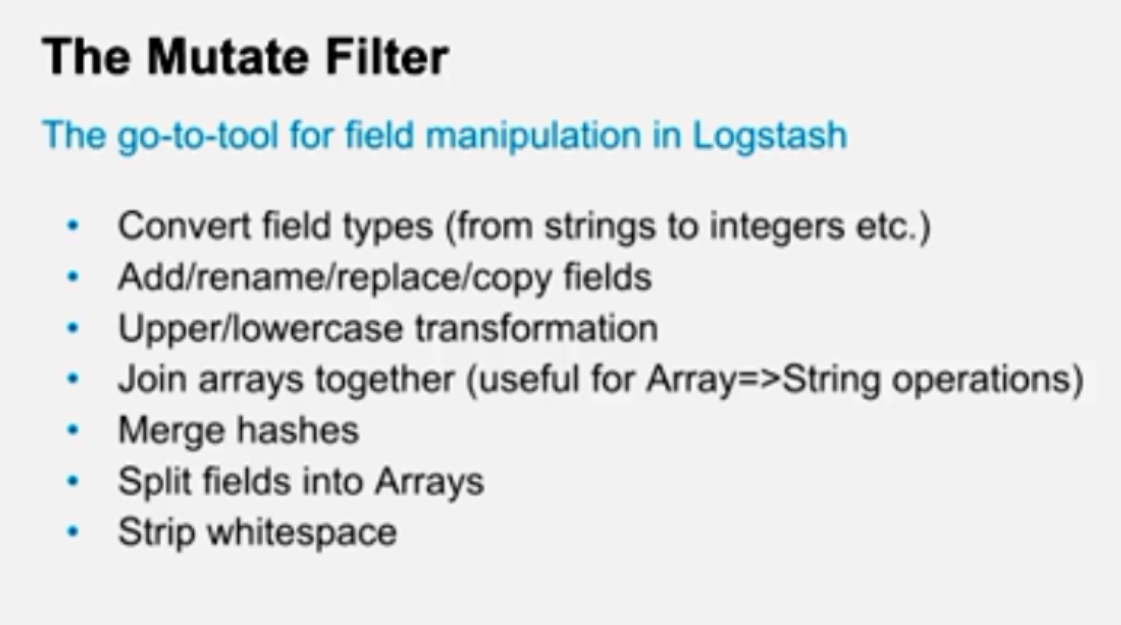


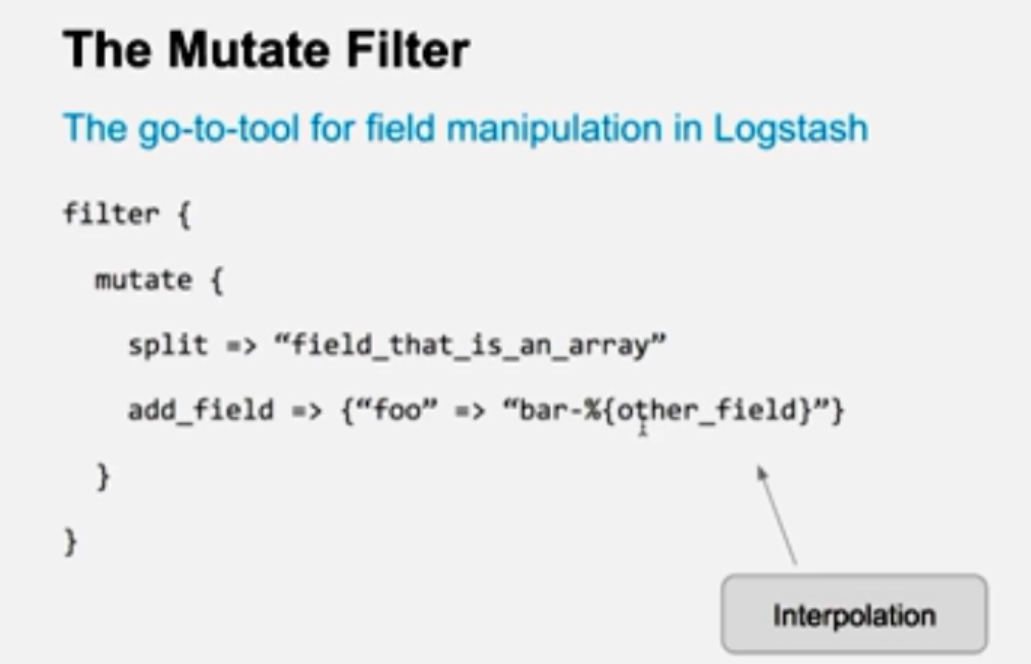


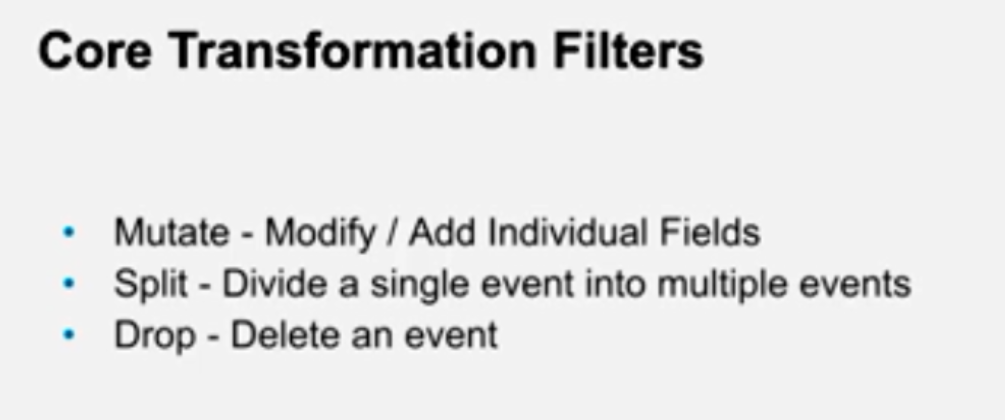


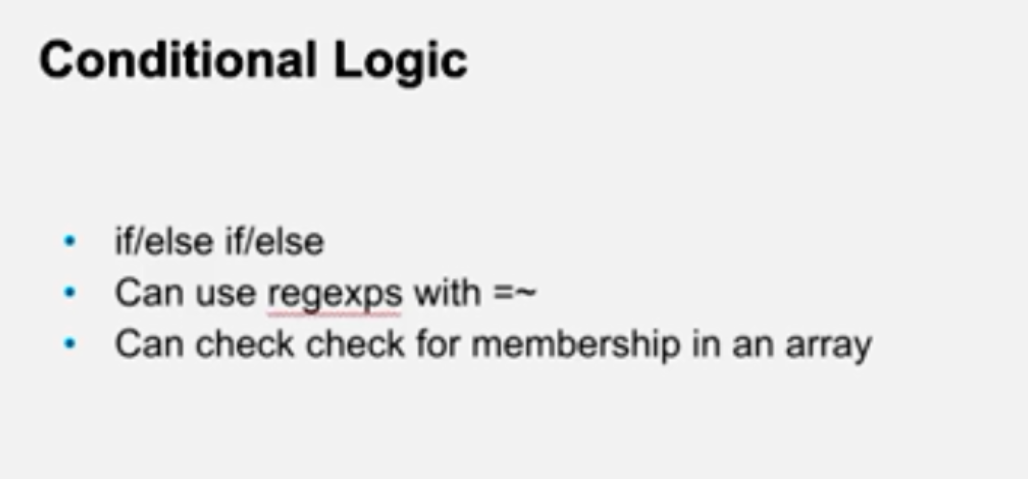


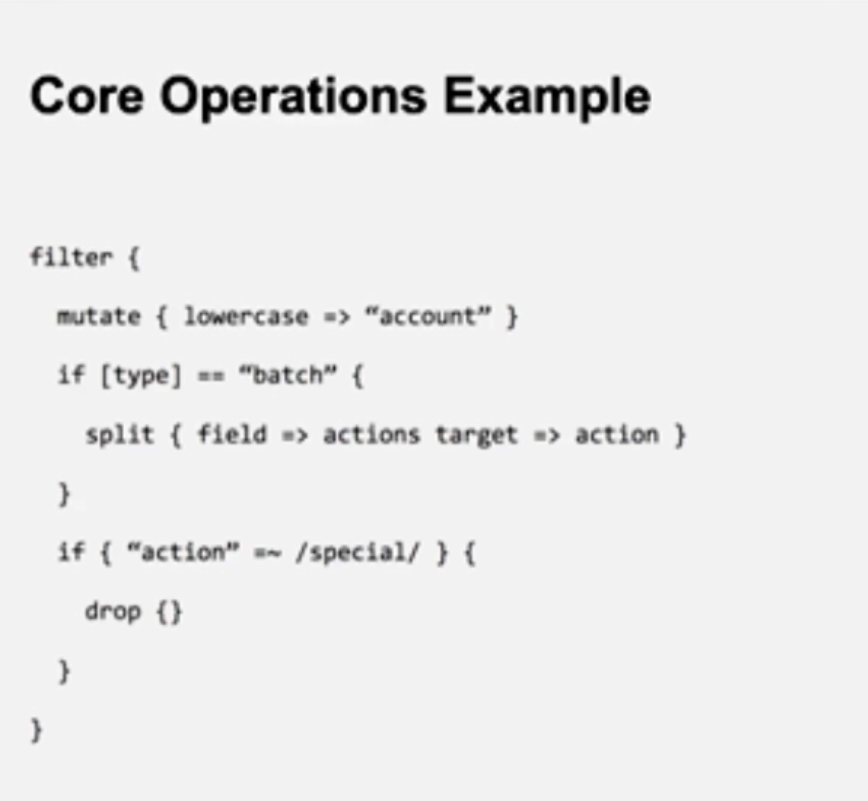
###### 核心操作



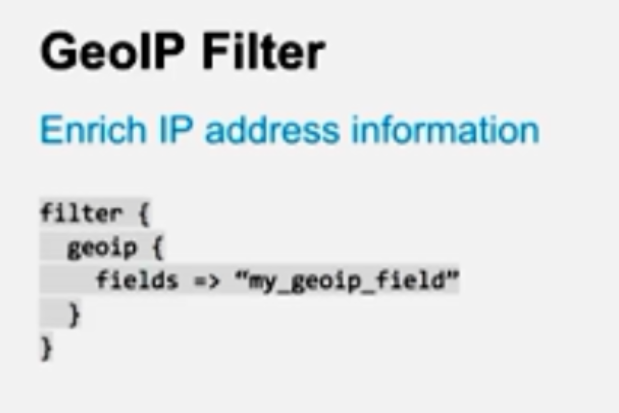








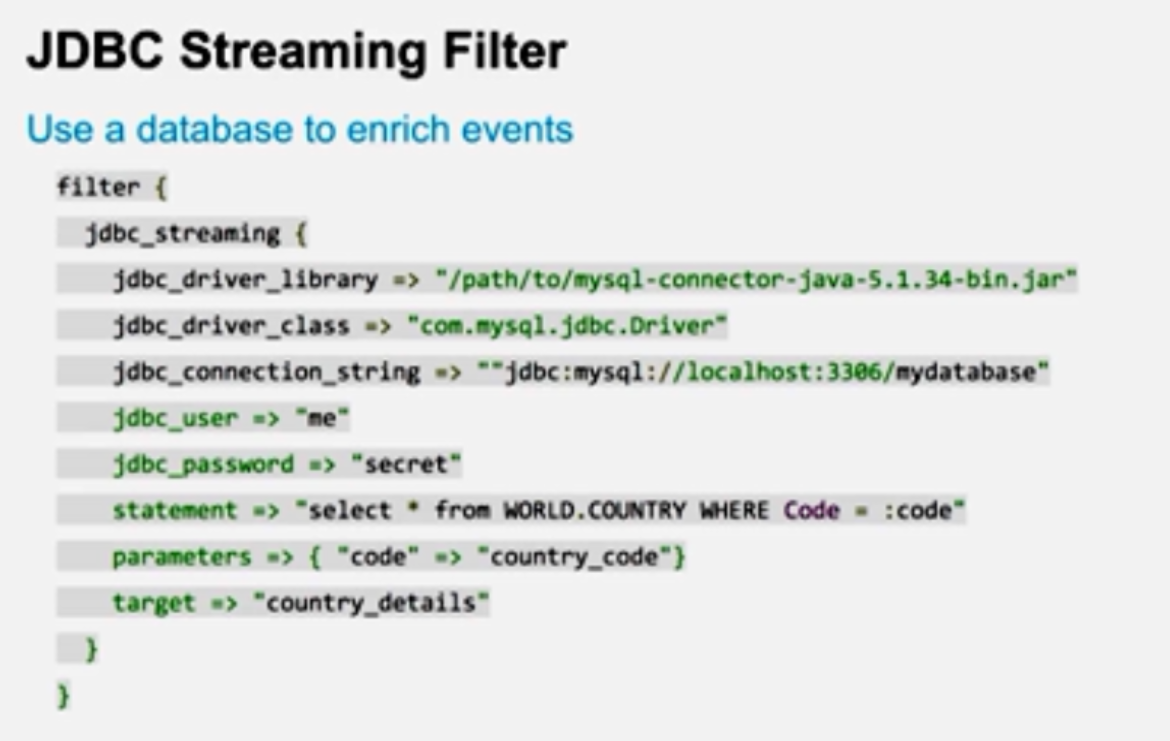
###### 查找

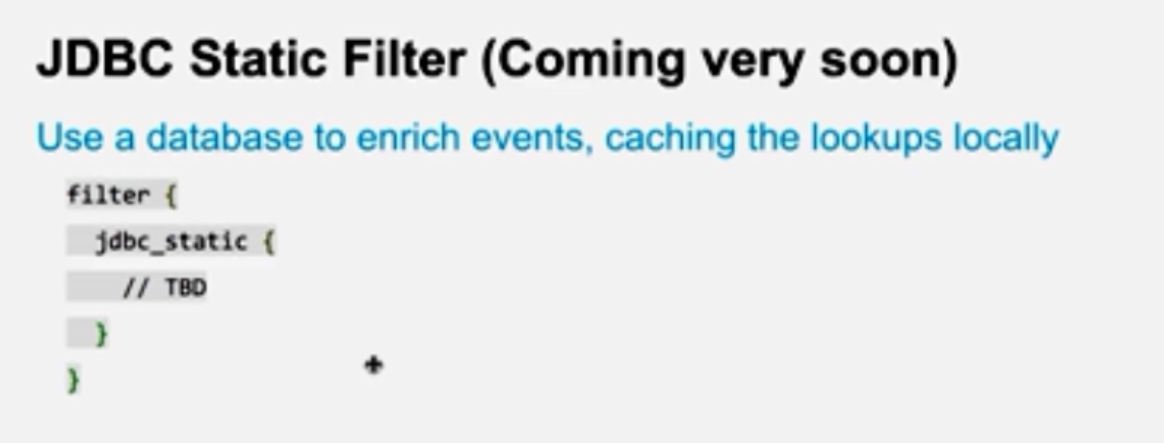












###### 监控管理



##### Elastic Search

文档：<https://www.elastic.co/cn/webinars/getting-started-elasticsearch?elektra=home&storm=sub1>

安装参考：<https://www.cnblogs.com/anech/p/Elasticsearch.html> 需要设置环境变量

测试： logstash -e "input { stdin { } } output { elasticsearch { hosts => localhost } }"

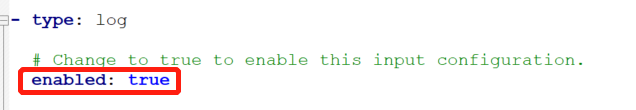
##### Filebeat

对于同一数据，logstash或者yml配置文件发生变化，停掉filebeat窗口，需要删data->registry文件，重新跑filebeat。

启动命令

filebeat -e -c xxx.yml

配置参数说明



必须设成true才生效。

其他参数说明：

<https://blog.csdn.net/weixin_41601114/article/details/105768172>

被采集的文件最后一行记录必须再回车才能被采集到。

##### Kibana

###### 删某个索引下的所有数据

POST logstash/\_delete\_by\_query

{

"query": {

"match\_all": {}

}

}