# 课程介绍

课程名称：

日志监控告警系统

基于的日志进行监控，监控需要一定规则，对触发监控规则的日志信息进行告警，告警的方式，是短信和邮件。

log4j---->error,info,debug 应用程序的日志 error级别 TimeOutException 角标越界IndexXXXException ......Error

com.alibaba.jstorm.daemon.worker.WorkerData]-[INFO] Current worker taskList:[1, 2, 3, 4, 5, 6, 7]

String.contains.(" taskList ")-------------->当订单量触发一千万时，告警通知，让大家庆祝下。

OrdertotalNum：1000万

课程目标：

1. 掌握Storm编程的应用场景及编程模型
2. 掌握Storm开发生态圈各知识点
3. 掌握短信和邮件告警功能

课程大纲：

1. 背景知识
2. 需求分析
3. 功能分析
4. 架构设计
5. 代码开发

# 课程内容

## 1、背景知识

一款优秀的软件需要具备的特点

* 软件的实用性

所谓有的放矢，软件的诞生是为了解决特定的问题，比如现在流行的MVC 框架，早期的没有MVC 开发的时候，耦合度很大，后期维护更新成本高，难度大，这样MVC 框架就孕育而生；比如陌陌这种社交软件，是为了解决陌生人之间交流的问题；比如通信软件是为了解决人们远程沟通的问题；比如OA系统为了解决公司协同流程、项目管理、知识管理等问题……所以一款优秀的软件必须能够解决一个领域内的问题。

* 软件的稳定性

软件的实用性问题解决之后，急需要解决的问题就是软件的稳定性。一般线上系统都会承载企业的某项业务，系统的稳定性直接影响了业务是否能够正常运营。很多创业公司在前期只注重业务的发展，不太在意系统的稳定性，一旦用户量上升之后，就会出现很多性能的问题。这种情况就好比，你找了一个妹子，并准备深入交往后结婚，却发现这个妹子总是有很多异性朋友在联系……

* 代码的规范性

铁打的营盘流水的兵，一款优秀的软件不仅仅是功能的实现。**整体架构、功能模块、代码注释、扩展性等问题也需要考虑**，毕竟在一个软件的生命周期过程中，参与的人实在是太多了，主创人员也可能随时流失。所以代码的规范性就难能可贵了。

* 升级保持向前兼容性

如果一个软件平常使用挺好的，但是升级却越来越费劲，或者升级后稳定性大打折扣，也难以称得上一个好的软件。

* 基本的使用手册

文档、文档、文档、一个简单有效的使用手册，才是程序的王道，知其然才能知其所以然。能让用户一目了然，功能、架构、设计思路、代码等等。

## 2、需求分析

随着公司业务发展，支撑公司业务的各种系统越来越多，为了保证公司的业务正常发展，急需要对这些线上系统的运行进行监控，做到问题的及时发现和处理，最大程度减少对业务的影响。

目前系统分类有：

1. 有基于Tomcat的web应用
2. 有独立的Java Application应用
3. 有运行在linux上的脚本程序
4. 有大规模的集群框架（zookeeper、Hadoop、Storm、Spark ……）
5. 有操作系统的运行日志

主要功能需求分为：

监控系统日志中的内容，按照一定规则进行过滤

发现问题之后通过短信和邮件进行告警

## 3、功能分析

* 数据输入

使用flume客户端获取个系统的数据；

用户通过页面输入系统名称、负责人触发规则等信息

* 数据存储

使用flume采集数据并存放在kafka集群中

* 数据计算

使用storm编写程序对日志进行过滤，将满足过滤规则的信息，通过邮件短信告警并保存到数据库中

* 数据展示

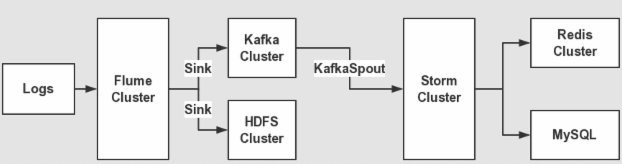
管理页面可以查看触发规则的信息，系统负责人，联系方式，触发信息明细等

## 4、原型设计

产品经理设计产品原形

## 5、架构设计

### 5.1、整体架构设计



主要架构为应用+flume+kafka+storm+mysql+Java web。数据流程如下：

1. 应用程序使用log4j产生日志
2. 部署flume客户端监控应用程序产生的日志信息，并发送到kafka集群中
3. storm spout拉去kafka的数据进行消费，逐条过滤每条日志的进行规则判断，对符合规则的日志进行邮件告警。
4. 最后将告警的信息保存到mysql数据库中，用来进行管理。

### 5.2、Flume设计

* Flume说明

Flume是一个分布式、可靠地、可用的服务，用来收集、聚合、传输日志数据。

它是一个基于流式数据的架构，简单而灵活。具有健壮性、容错机制、故障转移、恢复机制。

它提供一个简单的可扩展的数据模型，容许在线分析程序。

Flume 作为 cloudera 开发的实时日志收集系统，受到了业界的认可与广泛应用。

* Flume 设计摘要

使用 Flume EXEC执行一个linux命令来生成数据源。例如，可以用tail命令监控一个文件，那么，只要文件增加内容，EXEC就可以将增加的内容作为数据源发送出去。

使用 org.apache.flume.plugins.KafkaSink，将Flume EXEC产生的数据源发送到Kafka中。

### 5.3、Kafka设计

* Kafka说明

kafka是一个分布式消息队列：生产者、消费者的功能。

* Kakfa设计摘要

部署kafka集群，在集群中添加一个Topic：monitor\_realtime\_javaxy

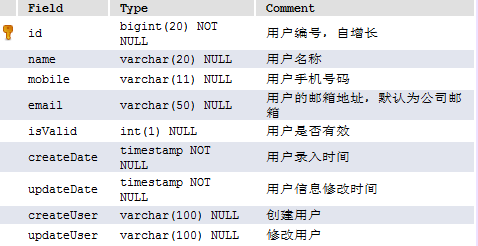
### 5.4、Storm设计

* KafkaSpout读取数据，需要配置Topic：monitor\_realtime\_javaxy
* FilterBolt判断规则
* NotifyBolt用来发送邮件或短信息
* Save2DB用来将告警信息写入mysql数据库

### 数据模型设计

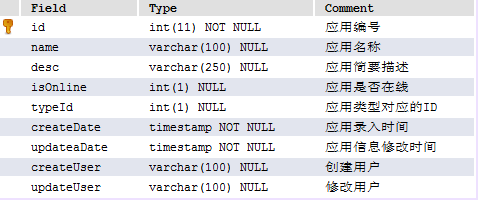
#### 5.5.1、用户表（负责人）

用来保存用户的信息，包括账号、手机号码、邮箱、是否有效等信息



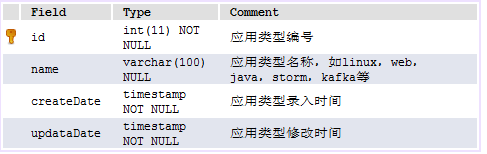
#### 5.5.2、应用表

用来保存应用的信息，包括应用名称、应用描述、应用是否在线等信息



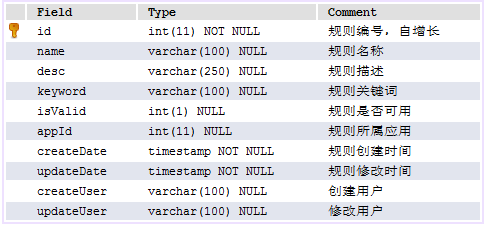
#### 5.5.3、应用类型表

用来保存应用的类型等信息



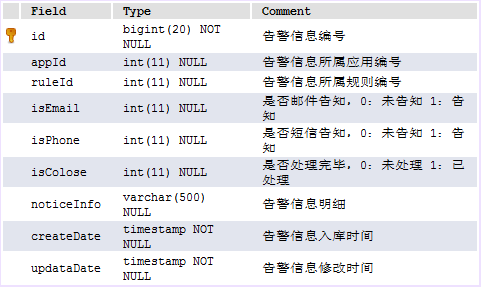
#### 5.5.4、规则表

用来保存规则的信息，包括规则名称，规则描述，规则关键词等信息



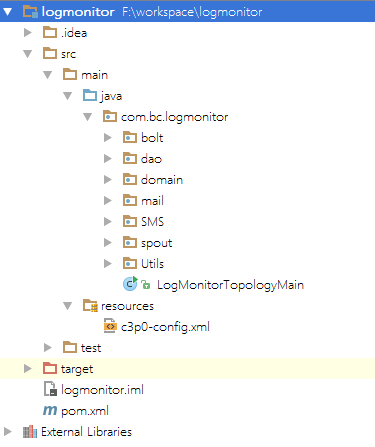
#### 5.5.5、规则记录表

用来保存触发规则后的记录，包括告警编号、是否短信告知、是否邮件告知、告警明细等信息。

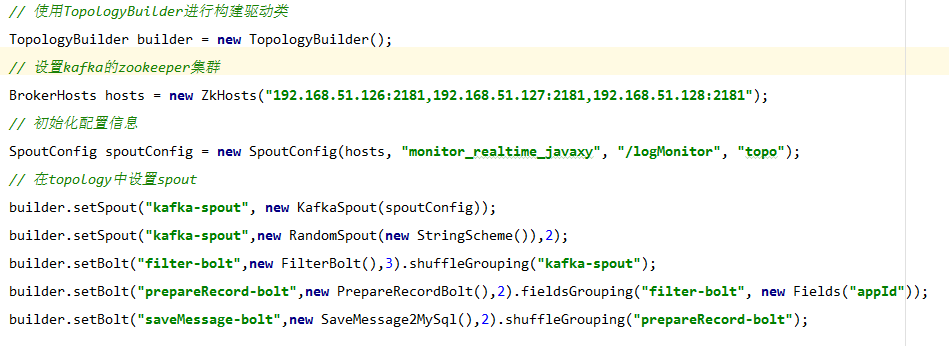


## 代码开发

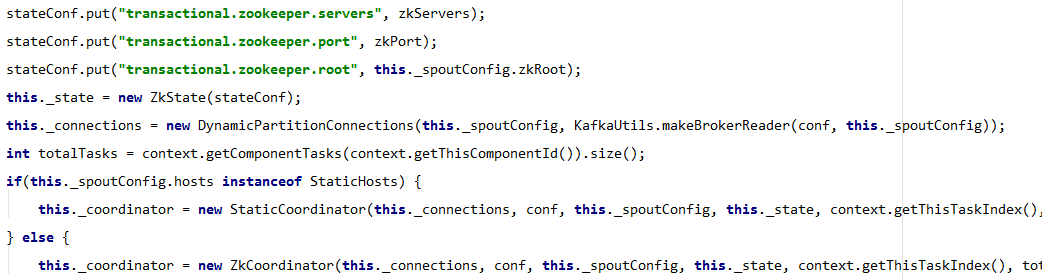
### 整体结构



### LogMonitorTopologyMain驱动类



### KafkaSpout获取数据源

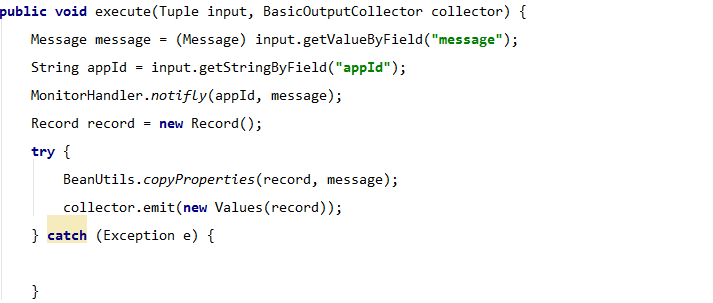


### 6.4、FilterBolt用来过滤日志信息

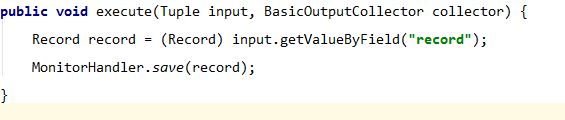
主要是过滤格式和校验appId是否合法。



### 6.5、PrepareRecordBolt发送邮件告警和短信告警



### SaveMessage2MySq保存到数据库



### 6.7、核心类 MonitorHandler  所有流程处理的核心代码

**见源码**

## 运行结果

### 7.1、短信发送

### 7.2、邮件发送

