# Cmbc集中监控平台介绍

## 一．NMS平台简介

集中监控平台是民生科技应用系统的重要监控工具，负责对it基础设施(包括：操作系统，数据库，中间件，进程服务，应用日志，网络探测等)的运行情况就行实时监控。通过对监控数据的搜集与统计，为事件处理，容量分析，交易趋势等提供服务。

集中监控平台(三期)是对现有**集中监控平台(NMS)**的一个重构，在迁移现有平台主要功能和配置的前提下，涉及开发了新功能以满足行内的监控需求。且在用户体验，数据容量，和吃力性能上有明显的提升

集中监控平台(三期NMS)的系统整体技术设计采用主流的大数据开源处理框架设计，为民生提供在业内较为先进的基于大数据环境的一体化集中监控，数据再挖掘，数据分析，业务影响分析，数据治理与共享的信息化监控运维整体解决方案

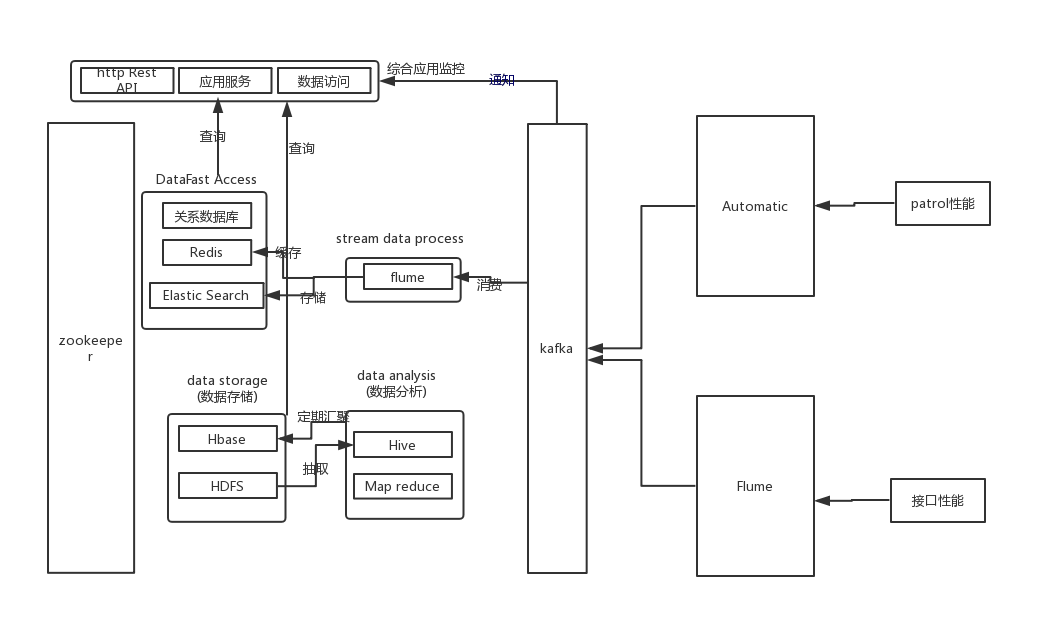
集中监控平台(nms)面向的用户主要为：信息科技部运维，开发，测试人员，分行科技人员等

## 平台架构设计

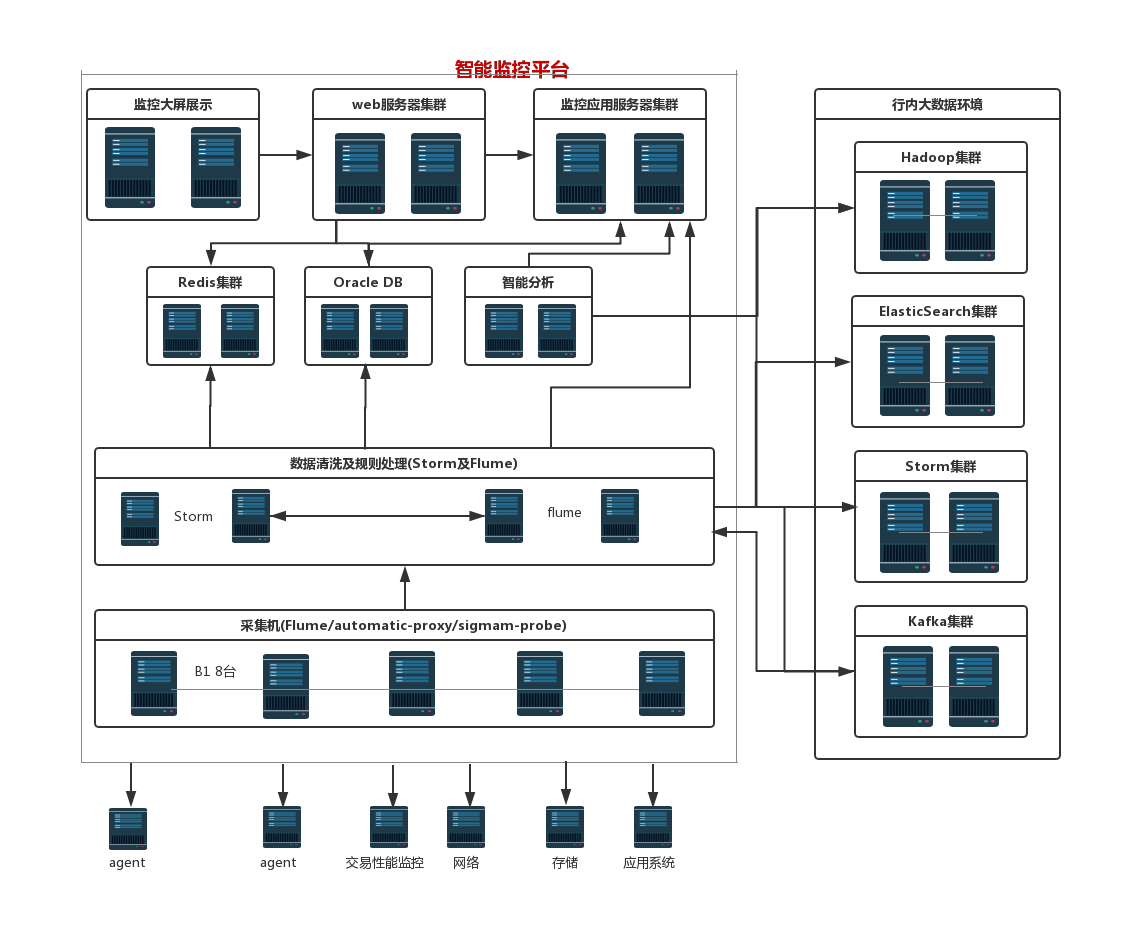
### 2-1 技术架构图--事件数据

### 技术架构(事件数据)

### 2-2 技术架构图--性能数据



### 2-3 物理架构图



### 2-4 架构介绍

#### 1-1 采集层

**Flume**:接受采集机agent发送的事件数据，并由采集机agent通过脚本将数据发送给flume， flume转发给Kafka，接受网络，存储，应用系统相关事件及性能数据。

**Automatic-proxy**：执行性能数据采集任务，并转发给Kafka

**Sigmam-probe**：接受非patrol产生的事件，主要为syslog，trap

#### 1-2 中间层

**Storm**:直接消费Kafka原始事件数据，事件处理：事件过滤，事件标准化，特殊规则(压制，升级，合并)处理等；事件通知(短信通知，邮件通知)

**Flume**:消费Kafka性能数据，将性能数据同时分发给Elastic Search 和 Hadoop

### **1-3 应用层**

**Web server:**前端展示，从redis及Oracle获取告警视图，应用视图配置数据

**App Server:**后端处理，分为视图类 和 运维管理类

**视图类：**基于elastic search 做查询分析，接受服务请求，根据不同请求做业务处理。包括 告警视图，应用视图

**运维管理类：**基于patrol配置管理，监控，巡检

## 基本概念

### (1)告警级别：

1. **主要告警**：需要立刻处理的告警；方式：打电话，短信/邮件
2. **次要告警**：需要及时关注的告警；只发邮件通知
3. **清除告警**：主/次要告警回复正常；发短信通知

### 告警阈值：

告警触发的临界值，当**监控指标**的取值在告警阈值的范围内时，会触发告警

在告警阈值设定时，会指定对应的告警级别

### (3)告警级别：

**当前告警：**为清除的告警

**历史告警：**已清除的告警

### 告警处理：六种方式

**确认：**如果用户负责某跳告警的后续分析和对应问题处理，可以对该告警进行确认操作，表示该告警已处理

**清除：**如果用户确认某条告警的问题已解决，不应该告警，或无须做任务和处理，可以对该告警进行清除操作，表示该告警已处理

**派发：**该功能一般为值班用户使用，当需要在ITOMS流程平台中生成对应事件工单派发给指定责任人时，进行派发操作，表示该告警已处理

**通知：**当需要把某条告警以短信或者邮件的方式发给指定责任人时，进行通知操作

**跟踪：**(只给值班用户使用???)目的是把需要后续重点关注跟跟踪解决的告警区分出来，便于后续跟踪

**响应：**(只给值班用户使用???)表示一条告警已有人知悉。当用户还不知道如何处理时，可点击响应，代表该告警已执行，会进一步处理；对告警进行 确认，清除，派发，通知，跟踪 操作都会触发响应。

### 服务器：“维护中/生产中”

维护中：服务器当前产生的告警会被暂时屏蔽，直到置回“生产中”，这些告警才会发送

生产中：服务器的监控正常运行，产生的告警会实时 发送出来。当主动性维护时，为避免触发监控的告警，应该置“维护中”，在操作完毕后，手工确认清除维护中产生的告警，再置回“生产中”