预警规则配置

一：配置界面 介绍

规则名称：该规则的名字。

项目：规则应用在 哪个项目上，此处名称和 输入日志中的 projectName字段内容相匹配。

数据来源：默认是Kafka的topic，如果以“http://”开头，则每隔2秒，进行一次http 接口调用，以获取数据。

过滤条件：过滤表达式，对输入的日志进行过滤，该表达式 后面详细介绍。

触发条件：触发表达式，对过滤后的日志 在指定的时间窗口内进行聚合运算，满足触发条件，发送预警信息，后面有详细介绍。

分组字段：对数据进行分组，默认不分组；类似SQL中的groupBy。

执行时间：定义该规则每天的运行时段。默认值：“0：24” 表示 全天运行。

按月重复：可选，定义规则每月几号执行。

按周重复：可选，定义每周几执行该规则。默认：”0，1，2，3，4，5，6“ 表示每天都执行。

时间窗口：配合“触发条件”进行使用，默认：1分钟，表示 只对过去一分钟内的数据进行计算。

间隔时间：当发生预警时，为了防止
同样的预警信息，多次发送通知，此处设置间隔时间。默认：30分钟，表示同样的预警信息，30分钟内只发送一次。

通知人员：此处选择预警信息的接收人，如果 下拉框中没有需要的人员，手动从后台数据库中增加新人。

通知方式：选择以何种方式通知接收人。

是否启用：是否启用该规则，默认：启用。

预警模板：信息的发送模板，可以使用 ${} 来植入参数。默认值：${_projectName}服务在${timestamp}发生${_name}告警，分组信息:${_group}

二：过滤条件表达式

（1）逻辑操作符：与运算&&， 或运算 ||，非运算：！

（2）关系运算：大于>，小于<，大于等于>=，小于等于<=，等于=，不等于!=，包含#，不包含!#，存在@，不存在!@，正则表达式~。

例子：(responseTime < 200 && responseTime >= 50) && logLevel != "error" && type="测试日志" && @ host && message ~ "^\S+\w+\d$" 表示，responseTime 在50到200只间，并且 logLevel不为error，并且 存在host字段，并且 type 的值为“测试日志”，并且 message 符合 指定的 正则表达式。

（3）四则运算：加+,减-,乘*,除/

例子：use_quota/total_quota*100>80, 表示：use_quota 除 total_quota 即 使用率 大于80% 的情况。

（4）其他符号 括号’()’，空白符 \t\n\r，转意字符 "\"；括号主要用来改变优先级，转意 字符，用来转换字符串中 出现 运算符的情况。

三：触发条件表达式

除了 拥有 “过滤条件表达式”的全部功能外，额外增加了 如下内置函数。

count()：计数器

sum(XXX)：对特定的字段XXX进行累加计算，注意：XXX字段的值必须是数字，否则 无效。

max(XXX)：对特定的字段XXX进行最大值计算，注意：XXX字段的值必须是数字，否则 无效。

min(XXX)：对特定的字段XXX进行最小值计算，注意：XXX字段的值必须是数字，否则 无效。

avg(XXX)：对特定的字段XXX进行平均值计算，注意：XXX字段的值必须是数字，否则 无效。