阿里云
日志服务

告警

文档版本：20190806

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的”现状“、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含”阿里云”、Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告:** 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明:** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
粗体	表示按键、菜单、页面名称等UI元素。	单击 确定。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
*## *	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig` *[-all|-t]*
{}或者{a|b}	表示必选项，至多选择一个。	`swich` *{stand | slave}*

目录

法律声明.....I
通用约定.....I
1 简介..... 1
2 设置告警任务..... 3
2.1 设置告警.....3
2.2 子账号设置告警.....11
2.3 通知方式.....13
3 修改与查看告警.....25
3.1 修改告警规则.....25
3.2 查看告警记录.....29
3.3 管理告警配置.....31
3.4 升级旧版告警.....34
4 参考信息.....36
4.1 告警条件表达式语法.....36
4.2 告警日志字段.....40
5 最佳实践.....43
5.1 告警设置.....43
6 FAQ..... 53
6.1 告警配置案例.....53

1 简介

日志服务支持根据仪表盘中的查询图表设置告警，实现实时的服务状态监控。

日志服务的告警功能基于仪表盘中的查询图表实现。在日志服务控制台查询页面或仪表盘页面设置告警规则，并指定告警规则的配置、检查条件和通知方式。设置告警后，日志服务定期对仪表盘的查询结果进行检查，检查结果满足预设条件时发送告警通知，实现实时的服务状态监控。

说明:

日志服务于近期升级了告警功能，控制台保留旧版的告警配置，但建议您尽快将旧版告警规则手动升级到新版本。详细步骤请参考升级旧版告警。

使用限制

限制项	说明
组合查询	组合查询的个数为1~3个。
字符串	字符串长度如果超过1024个字符，只会截取前1024个字符用于计算。
条件表达式	· 条件表达式长度为1~128个字符。 · 每个查询只会取查询结果的前100条用于计算条件表达式。 · 条件表达式计算次数不超过1000次，如使用组合查询，则组合计算的次数最多只会计算1000次。
短信数量	同一个手机号码每天接收的短信不超过50条。
语音通知数量	同一个手机号码每天接收的语音电话通知不超过50个。
邮件数量	同一个邮箱每天接收的邮件不超过100条。
查询区间	每个查询语句的查询区间时间跨度不能超过24小时。

告警中的查询语句

告警基于仪表盘中的分析图表，而分析图表实质上是一条查询分析语句的可视化查询结果。其中，查询语句可以是查询语句或查询分析语句。

· 查询语句：直接返回查询条件命中的日志数据。
· 查询分析语句：对查询条件命中的日志进行统计，返回统计结果。

- 查询语句

例如，查询最近 15 分钟内包含 error 的数据，条件为 error，一共有 154 条。每条内容都是 Key、Value 组合，您可以对某个 Key 下的 Value 设置告警条件。

> **说明:**
> 对于查询结果一次超过 100 条的情况，告警规则只判断前100条，只有前100条中任意一条符合条件，才会触发告警。

图 1-1: 查询语句

- 查询分析语句

例如查询所有日志中状态码为ok的日志比例，查询语句如下（查询语法请参考查询语法）：

```
* | select sum(case when status='ok' then 1 else 0 end) *1.0/count(1) as ratio
```

因此，可以设置告警检查条件为`ratio < 0.9`，表示当状态码为ok的日志小于总日志数的90%时进行告警。

图 1-2: 查询分析语句

2 设置告警任务

2.1 设置告警

在查询页面或仪表盘页面设置告警，日志服务会定时执行检查，并在满足告警条件时发送告警信息。

前提条件

- 已采集到日志数据。
- 已开启并配置索引。

背景信息

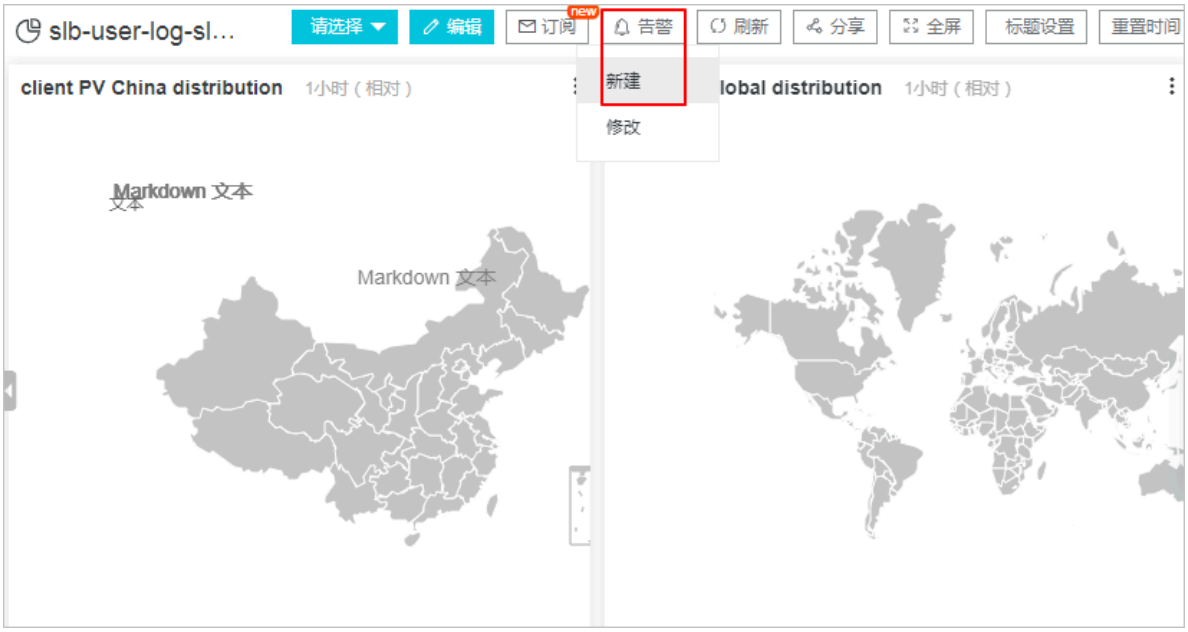
告警基于查询分析图表设置，您可以在查看图表时，将图表保存在仪表盘中，同时另存为告警，也可以在仪表盘页面中对已有的图表设置告警。

- 创建图表并设置告警

  将当前的查询分析语句保存在仪表盘中，并为查询分析语句设置告警。在查询页面设置告警时，您需要指定图表保存到的仪表盘名称和图表名称。

- 在仪表盘中对已有图表设置告警

  为仪表盘中的一个或多个图表设置告警。为多个图表设置告警时，可以设置组合触发条件。



本文档以在仪表盘中对已有图表设置告警为例。

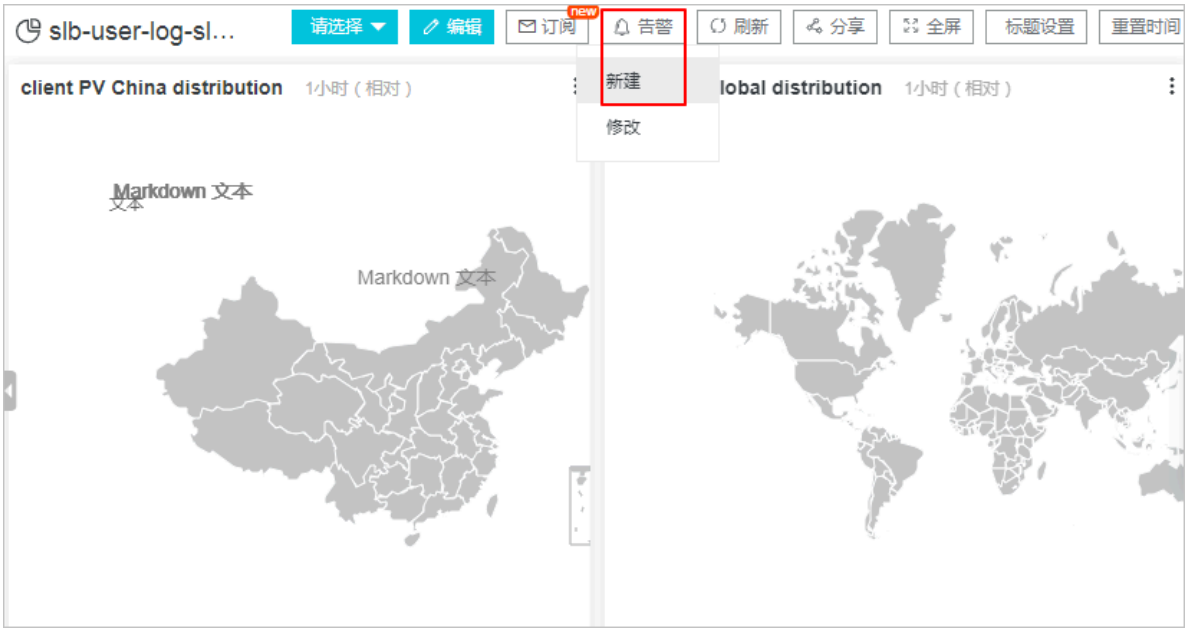
> 说明:
> 如果仪表盘中的分析图表绑定了告警规则，更新图表的查询分析语句后，需要手动更新告警规则，将告警规则中绑定的查询分析语句修改为更新后的语句。详细说明请参考更新告警规则。

常见告警配置案例请参考告警配置案例。

操作步骤

1. 登录日志服务控制台，单击Project名称。
2. 在左侧导航栏中单击仪表盘图标。
3. 单击指定仪表盘名称。

4. 在页面右上角单击告警 > 新建。



5. 设置告警规则并单击 下一步。

告警配置信息如下：

规则	说明
告警名称	告警的名称。名称长度为1~64个字符。
关联图表	设置告警中关联的图表。 单击添加，选择图表名称并设置查询区间。查询区间为服务端每次执行查询时，读取的数据时间范围，支持相对时间与绝对时间。例如，执行时间点为14:30:06，设置查询区间为15分钟（相对），则查询区间为 14:15:06- 14:30:06；设置查询区间为15分钟（绝对），则查询区间为：14:15:00- 14:30:00。 需要添加多个图表时，只需多次添加并设置即可。图表名称前的编号为该图表在告警中的编号，您可以在触发条件中通过编号指定关联的图表。
频率	服务端每次执行告警检查的时间。 说明: 目前服务端每次告警规则检查只会采样处理时间区间开始的前100条数据。

规则	说明
触发条件	判断告警是否触发的条件表达式，满足该条件时会根据执行间隔和通知间隔发送告警通知。 例如，您可以设置为`pv%100 > 0 && uv > 0`。 说明: 触发条件中，通过`$编号`区分不同的关联图表，例如`$0`表示编号为0的图表。 如何查看图表编号?
高级选项	
触发通知阈值	累计触发次数达到该阈值时根据通知间隔发送告警。不满足触发条件时不计入统计。 默认触发通知阈值为1，即满足一次触发条件即可检查通知间隔。 通过配置触发通知阈值可以实现多次触发、一次通知。例如，配置触发通知阈值为100，则累计触发次数达到100次时检查通知间隔。如果同时满足触发通知阈值和通知间隔，则发送通知。发送通知之后，累计次数会清零。如果因网络异常等原因执行检查失败，不计入累计次数。

规则	说明
通知间隔	两次告警通知之间的时间间隔。 如果某次执行满足了触发条件，而且累计的触发次数已经达到触发通知阈值，且距离上次发送通知已经达到了通知间隔，则发送通知。如设置通知间隔为5分钟，则5分钟内至多收到一次通知。默认无间隔。 说明: 通过配置触发通知阈值和通知间隔可以实现告警抑制的功能，防止收到过多的告警信息。


创建告警
告警配置
通知
* 告警名称
每分钟写入不能低于平均数0.5倍
16/64
* 关联图表
0
图表名称
写入日志条数
查询语句
* | SELECT date_format(t, '%H:%i:%s') as time, count FROM(SELECT date_trunc('minute', __time__) as t, COUNT(1) as count FROM log GROUP BY t ORDER BY t LIMIT 1000)
查询区间
15分钟（相对）
1
图表名称
写入总行数
查询语句
* | SELECT COUNT(*) as total
查询区间
15分钟（相对）
2
添加
* 执行间隔
15
分钟
* 触发条件
$0.count < $1.total/15.0/2.0
28/128
支持加(+)减(-)乘(*)除(/)取模(%)运算和>,>=,<,<=,==,!=,=~,!~比较运算。不同查询结果的字段使用${编号}.fieldName的方式区分，如$0.fieldName>100。帮助文档
高级选项 >
下一步
取消

6. 设置通知方式。

通知方式可以设置一种或多种，包括短信、邮件、钉钉、WebHook和通知中心。

通知方式的详细说明及示例请参考通知方式。

通知方式	说明
短信	短信形式发送告警通知，需要指定手机号码和发送内容。 多个手机号码之间通过逗号（，）分隔。发送内容为短信通知的内容，支持使用模板变量，长度为1~100个字符。
邮件	邮件形式发送告警通知，需要指定邮箱地址为收件人，并指定发送内容。 多个邮箱地址之间通过逗号（，）分隔。发送内容为邮件通知的内容，支持使用模板变量，长度为1~500个字符。
钉钉机器人	钉钉机器人消息形式发送告警通知，当触发告警时，告警通知会以钉钉机器人消息的形式发送到钉钉群中。需要指定请求地址和发送内容。 发送内容为钉钉机器人消息的内容，支持使用模板变量，长度为1~500个字符。 如何设置钉钉机器人、获取请求地址，请查看通知方式。 说明: 每个机器人每分钟最多发送20条。
WebHook自定义	当触发告警时，告警通知会以指定形式发送到自定义WebHook地址中。需要指定请求地址、请求方法和发送内容。 请求方法可以设置为GET、PUT、POST、DELETE、和OPTIONS。发送内容为通知的内容，支持使用模板变量，长度为1~500个字符。

通知方式	说明
通知中心	通过阿里云通知中心中预设的通知方式向联系人发送告警通知。需要指定发送内容。发送内容为通知消息的内容，支持使用模板变量，长度为1~500个字符。 添加通知中心告警方式，需要在通知中心中设置联系人及通知方式。

7. 单击提交。

预期结果

创建完成告警规则后，您可以查看告警配置或查看告警记录。

2.2 子账号设置告警

可以通过授权，为子账号开通告警相关功能。

背景信息

请根据实际需求为子账号授权。

- 为子账号授予日志服务的全部操作权限：授予全部管理权限`AliyunLogFullAccess`。详细步骤请参考授权RAM 用户。
- 仅为子账号授予创建及修改告警的权限，不授予其他日志服务管理权限：创建自定义权限策略，并为子账号授予该自定义权限策略。详细步骤请参考本文档。

操作步骤

1. 登录 RAM 控制台。
2. 在左侧导航选择权限管理 > 权限策略管理。
3. 在权限策略管理页面单击新建权限策略。
4. 输入策略名称和备注。
5. 勾选脚本配置的配置模式。
6. 请替换参数后，输入以下策略内容。

说明:

请将`<Project名称>`替换为您的日志服务Project名称。

```
{
  "Version": "1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "log:CreateLogStore",
        "log:CreateIndex",
        "log:UpdateIndex"
      ],
      "Resource": "acs:log:*:*:project/<Project名称>/logstore/
internal-alert-history"
    },
    {
      "Effect": "Allow",
      "Action": [
        "log:CreateDashboard",
        "log:CreateChart",
        "log:UpdateDashboard"
      ],
      "Resource": "acs:log:*:*:project/<Project名称>/dashboard/*"
    },
    {
      "Effect": "Allow",
      "Action": [
```

```
        "log:*"
      ],
      "Resource": "acs:log:*:*:project/<Project名称>/job/*"
    }
  ]
}
```

7. 单击确定。
8. 在左侧导航栏中选择人员管理 > 用户。
9. 找到需要授权的子账号并单击对应的授权。
10. 添加上文中创建的自定义权限策略，并单击确定。

2.3 通知方式

日志服务的告警功能支持设置一种或多种通知方式，包括短信、语音、邮件、钉钉、WebHook和通知中心。

通知方式：

- 短信
- 语音
- 邮件
- WebHook-钉钉机器人
- WebHook-自定义
- 通知中心

发送内容：发送内容说明

短信

告警的通知方式可设置为短信，当触发告警时，日志服务会向预设的手机号码发送短信通知。

配置步骤

1. 在日志服务控制台设置告警。通知类型设置为短信。

2. 手机号码中填写接收告警通知的短信号码，通知内容中填写短信内容。

   多个手机号码之间通过逗号（，）分隔。发送内容为短信通知的内容，支持使用模板变量，长度为1~100个字符。

3. 单击提交。

语音

告警的通知方式可设置为语音电话，当触发告警时，日志服务会向预设的手机号码发送电话提醒，语音内容中包括Project名称、告警名称和已配置的发送内容。如果某次告警电话未接通，将以短信方式发送一次提醒。

> 说明:
> 发送内容建议使用中文。

配置步骤

1. 在日志服务控制台设置告警。通知类型设置为语音。

2. 手机号码中填写接收告警通知的短信号码，通知内容中填写短信内容。

   多个手机号码之间通过逗号（，）分隔。发送内容为短信通知的内容，支持使用模板变量，长度为1~100个字符。

3. 单击提交。

邮件

告警的通知方式可设置为邮件，当触发告警时，日志服务会向指定邮箱地址发送邮件通知。

配置步骤

1. 在日志服务控制台设置告警。通知类型设置为邮件。
2. 收件人中填写接收告警通知的邮箱地址，主题中填写邮件主题。

   邮件主题字数必须在128以内，例如主题内容为日志服务告警。
3. 通知内容中填写邮件内容。

   多个邮箱地址之间通过逗号（,）分隔。发送内容为邮件通知的内容，支持使用模板变量，长度为1~500个字符。

4. 单击提交。

WebHook-钉钉机器人

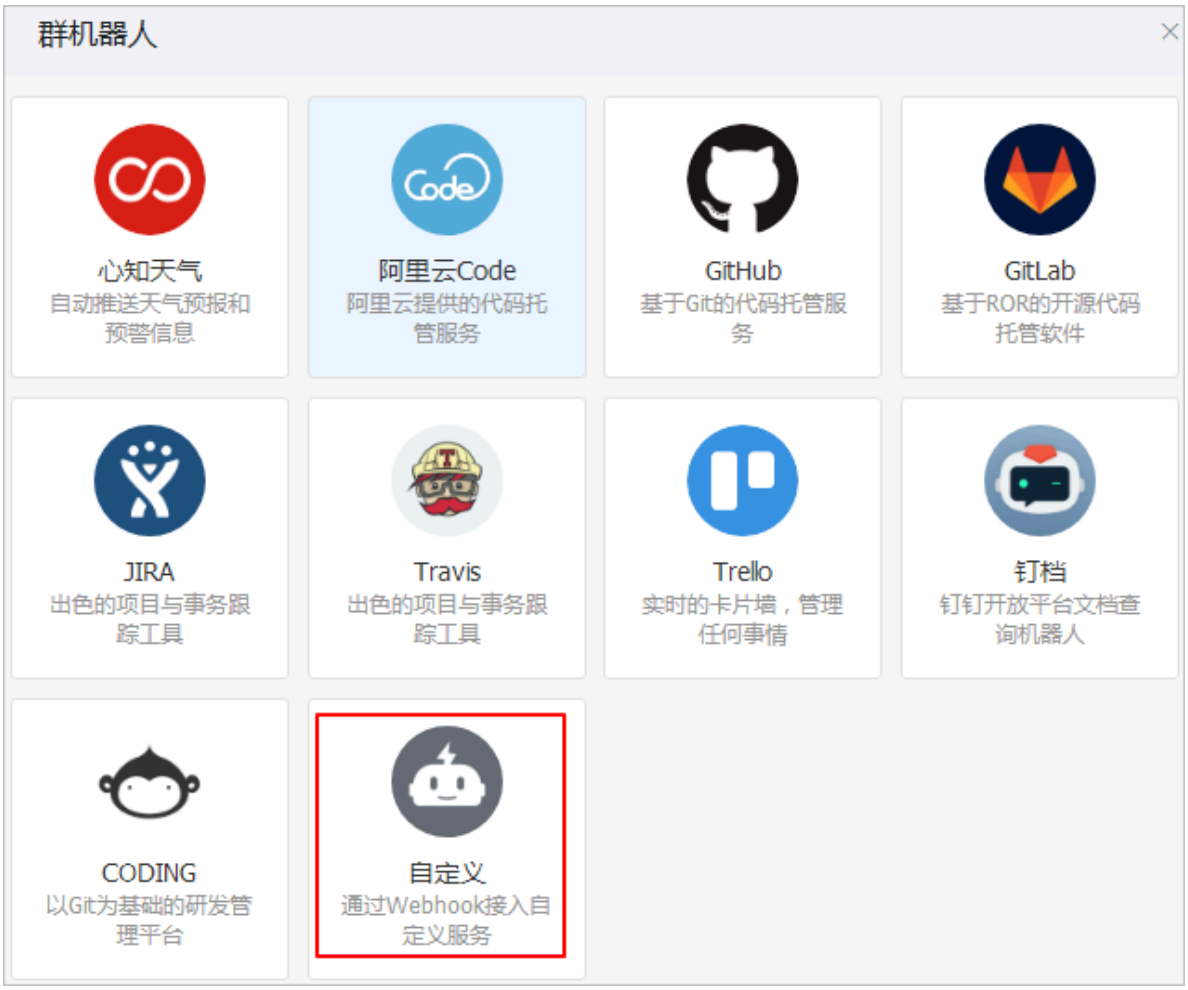
告警的通知方式可设置为钉钉，当触发告警时，告警通知会以钉钉机器人消息的形式发送到钉钉群中，还可以在提醒消息中设置被@的人。

> **说明:**
> 每个机器人每分钟最多发送20条告警通知。

配置步骤

1. 打开钉钉客户端，进入钉钉群。
2. 单击右上角群设置图标，并单击群机器人。
3. 选择自定义（通过WebHook接入自定义服务），并单击添加。

图 2-1: 钉钉机器人



4. 输入机器人名字，并单击完成。

5. 单击复制，复制WebHook链接。

6. 在日志服务控制台设置告警，且通知类型设置为钉钉。
7. 请求地址中，粘贴步骤5中复制的地址，并填写被@人列表。

   被@人列表中填写被@的人的手机号码，多个手机号用逗号（,）分隔。

8. 填写发送内容。

   页面已默认配置发送内容，您也可以在此基础上配置个性化的发送内容。

   如果有需要@的人，必须在发送内容中增加@手机号。

   图 2-2: 发送内容

WebHook-自定义

告警的通知方式可设置为WebHook，当触发告警时，告警通知会以指定方式发送到自定义WebHook地址中。

> **说明:**
> 告警通知方式为WebHook-自定义时，超时时间为5秒。如果发出请求后5秒内没有返回，则视作发送失败。

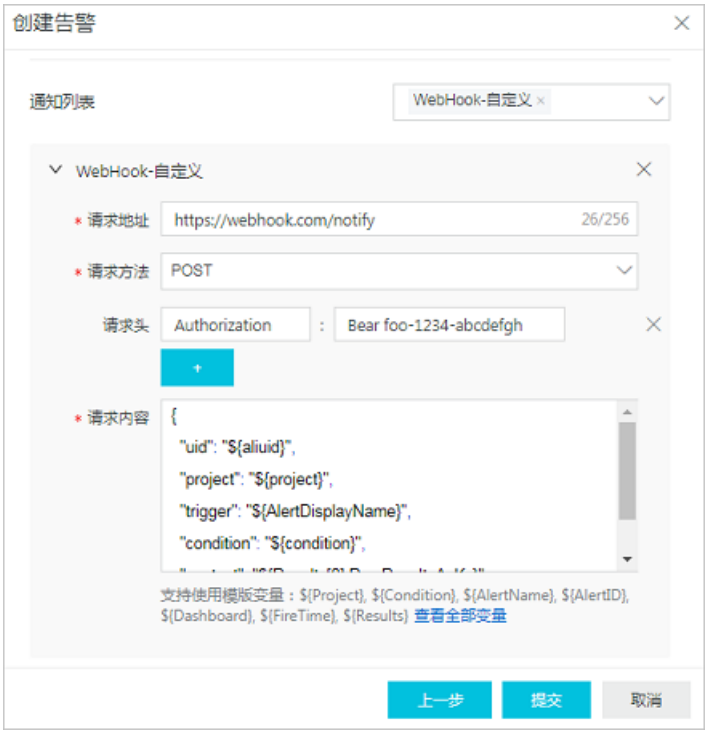
配置步骤

1. 在日志服务控制台设置告警。通知类型设置为WebHook。
2. 请求地址中填写自定义的WebHook地址，并指定请求方法。

3. （可选）单击添加请求头可以追加请求头（Header）信息。

   默认包含Header`Content-Type: application/json;charset=utf-8`，您也可以追加Header。

4. 填写通知内容。



   发生告警后会以指定方式将告警内容发到自定义WebHook地址。

5. 单击提交。

通知中心（推荐）

阿里云消息中心中可设置日志服务告警的联系人，当触发告警时，告警通知会以消息中心中预设的通知方式发送告警通知。

配置步骤

1. 设置告警，其中，通知方式设置为通知中心。

2. 在阿里云消息中心，单击消息接收管理 > 基本接收管理。

3. 在消息类型 > 日志服务（LOG）告警对应的消息接收人一列单击修改。

图 2-3: 修改消息接收人

4. 在修改消息接收人窗口选择消息接收人。

如您需要新增一位消息接收人，可以直接单击+新增消息接收人，并配置该人员用于接收告警信息的邮箱、手机号码和职位信息。仅账号负责人可以为消息接收人配置手机号码。

说明:

- 系统将自动发送验证信息到所填手机号和邮箱，通过验证后方可接收消息。
- 最少需要设置1位消息接收人。
- 通知方式默认为邮件 + 短信，且不可更改。
- 每个 手机号或邮箱 一天最多发送50次告警通知。

发送内容

配置通知方式时，必须设置发送内容，即通知的内容，通知内容中支持通过${fieldName}的方式引用一些告警触发时的模板变量。日志服务发送告警时，会将发送内容中的模板变量替换为真实值，如${Project}替换为告警规则所属的Project名称。

说明:

引用变量时变量名称必须完全匹配，对于不存在的变量或者不合法的引用会渲染为空字符串。如果引用的值为对象类型，则会转换为JSON字符串展示。

以下是目前支持的所有可用变量及引用方式。

变量	说明	举例	引用举例
Aliuid	Project所属的用户AliUid。	1234567890	用户${Aliuid}的告警规则已经触发。
Project	告警规则所属Project。	my-project	项目 ${Project}中的告警触发。
AlertID	执行的唯一ID。	0fdd88063a611aa114938f9371daeeb6-1671a52eb23	告警执行ID是 ${AlertID}。
AlertName	告警规则名称，Project内唯一。	alert-1542111415-153472	告警规则 ${AlertName} 已经触发。
AlertDisplayName	告警规则显示名称。	我的告警规则	告警名称 ${AlertDisplayName} 已经触发。
Condition	触发告警时的条件表达式。其中，以触发告警的值替换设置的变量，并使用括号中括号包裹。	[5] > 1	告警条件表达式为 ${Condition}。
RawCondition	原始的条件表达式，即condition中不替换变量的原始表达式。	count > 1	原始条件表达式为 ${RawCondition}。
Dashboard	告警关联的仪表盘名称。	mydashboard	告警关联的仪表盘 ${Dashboard}。
DashboardUrl	告警关联的仪表盘地址。	https://sls.console.aliyun.com/next/project/myproject/dashboard/mydashboard	告警关联的仪表盘地址${DashboardUrl}。

变量	说明	举例	引用举例
FireTime	触发时间。	2018-01-02 15:04:05	告警触发时间 ${FireTime}。
FullResultUrl	告警触发历史记录的查询地址URL。	https://sls.console.aliyun.com/next/project/my-project/logsearch/internal-alert-history?endTime=1544083998&queryString=AlertID%3A9155ea1ec10167985519fccede4d5fc7-1678293caad&queryTimeType=99&startTime=1544083968	单击查看详情： ${FullResultUrl}
Results	查询参数和结果，数组类型。内部字段解释请参考告警日志字段。	[{ "EndTime": 1542507580, "FireResult": { "__time__": "1542453580", "count": "0" }, "LogStore": "test-logstore", "Query": "* | SELECT COUNT(*) as count", "RawResultCount": 1, "RawResults": [{ "__time__": "1542453580", "count": "0" }], "StartTime": 1542453580 }]	第一个查询的开始时间为${Results[0].StartTime}；结束时间为${Results[0].EndTime}；count的值为${Results[0].FireResult.count}。 说明： 其中，0为图表/查询分析语句的编号。 如何查看图表编号?

3 修改与查看告警

3.1 修改告警规则

创建告警后，您可以修改告警图表后更新告警规则；基于查询语句的告警，可以直接在告警中修改查询语句。

注意事项

- 只有为查询语句设置的告警规则支持修改查询语句，且只能修改为查询语句，不支持修改为查询分析语句（查询语句|分析语句）。

  例如，为查询语句`request_method: GET`绑定告警规则后，可以将查询语句修改为`error`，但不能修改为`error| select count(1) as c`。
- 修改旧版告警规则，请参考升级旧版告警。
- 新版告警规则可以在告警配置页面中单击修改，或者在配置了告警的仪表盘页面右上角单击告警 > 修改。

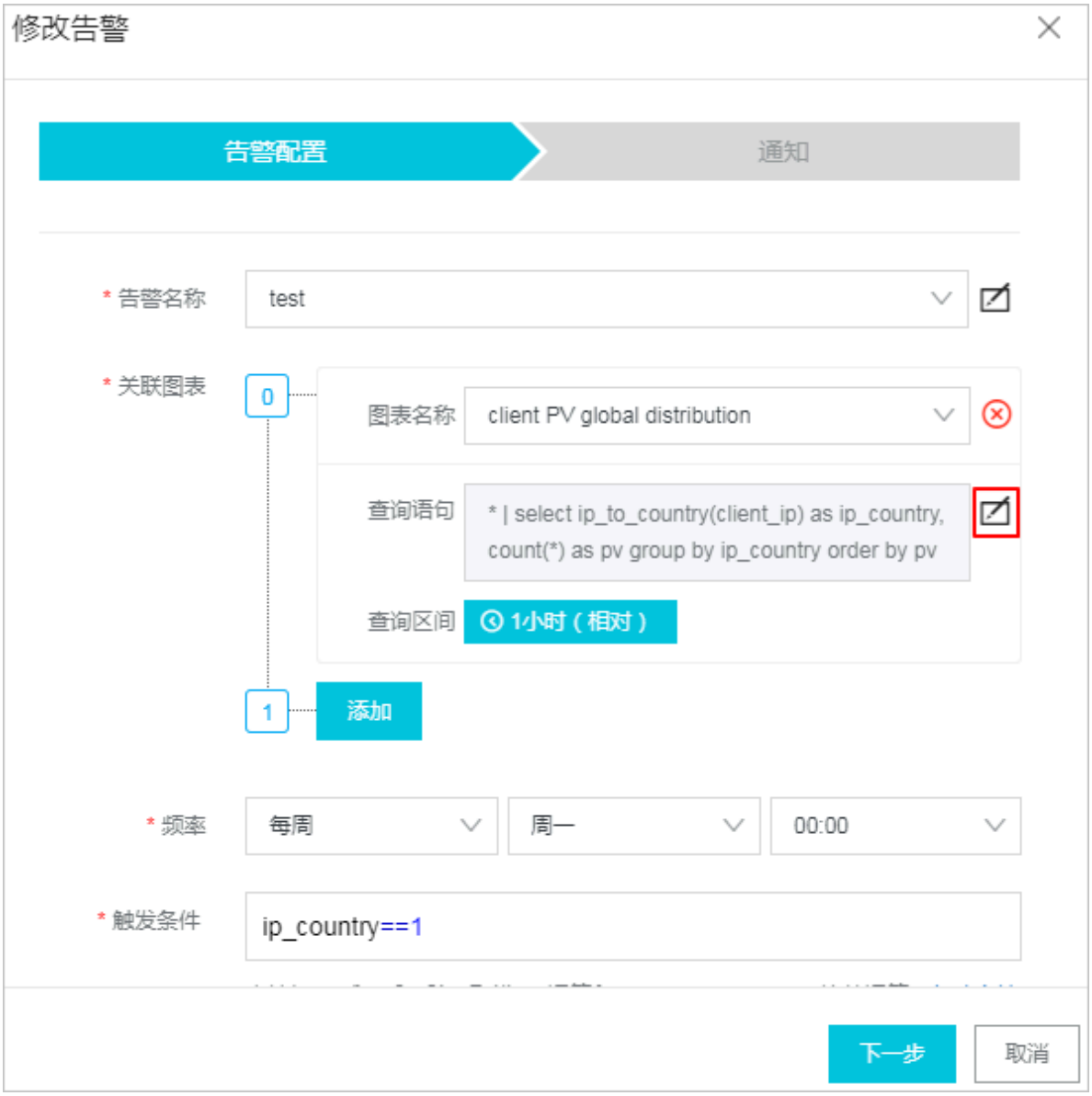
修改告警绑定的查询语句

在日志服务查询页面执行的查询语句如果被绑定了告警规则，绑定后可以修改查询语句。

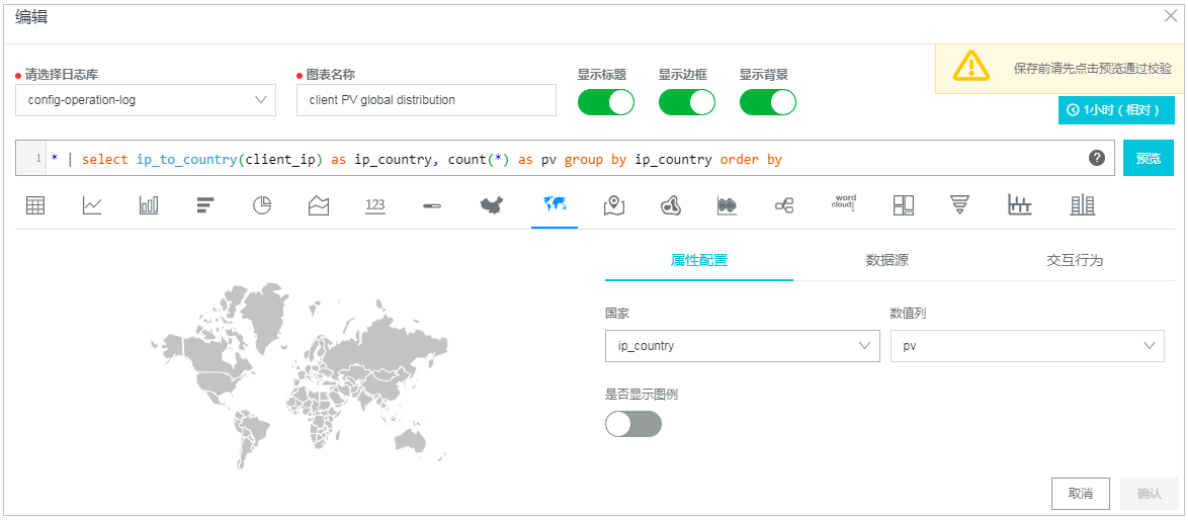
1. 登录日志服务控制台，单击Project名称。
2. 单击左侧导航栏的仪表盘图标。
3. 在仪表盘列表中单击指定仪表盘名称。
4. 在页面右上角单击告警 > 修改。

5. 找到需要修改的查询语句，单击其右侧的  。

只有为查询语句设置的告警规则支持修改查询语句，且只能修改为查询语句，不支持修改为查询分析语句（查询语句|分析语句）。



6. 输入新的查询语句，并单击其右侧的预览按钮，通过校验后单击确认。



7. 根据需求确认是否修改频率和触发条件，并单击下一步。

8. 配置通知方式，并单击提交。

修改告警关联图表

创建告警规则后，可以随时修改告警规则。

1. 登录日志服务控制台，单击Project名称。

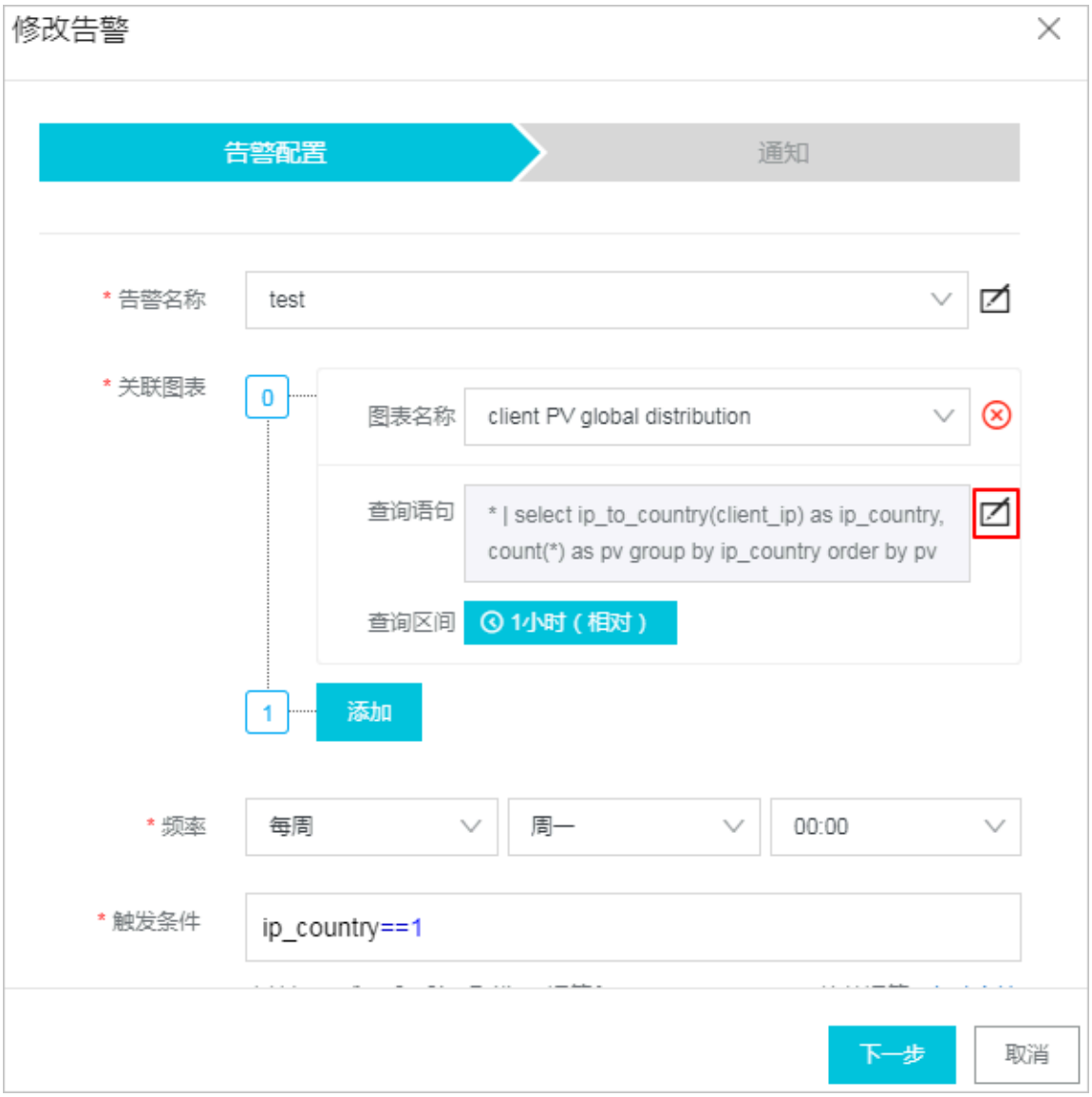
2. 修改告警关联图表。

   a. 单击左侧导航栏的仪表盘图标。

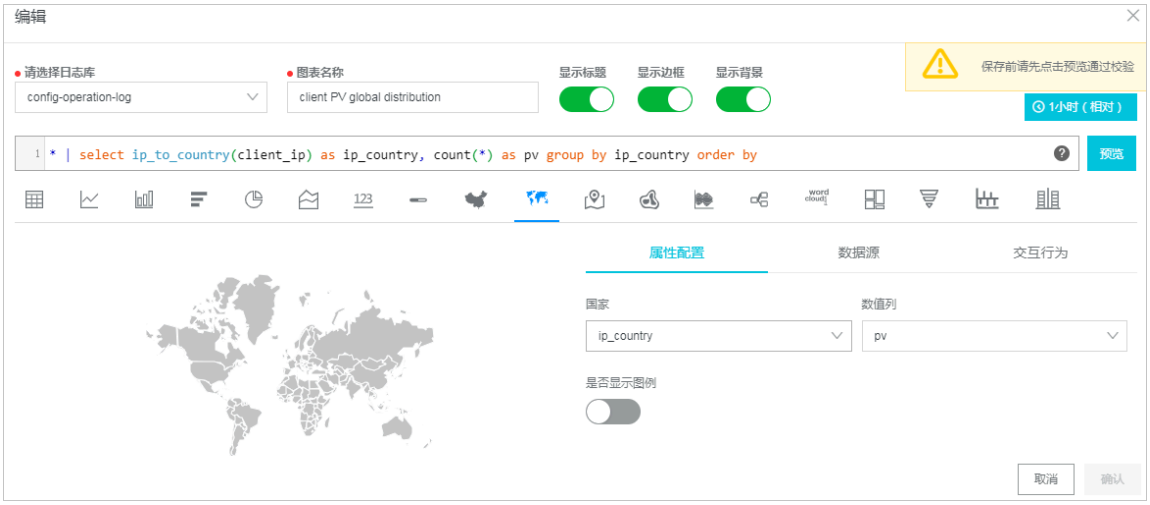
   b. 在仪表盘列表中单击指定仪表盘名称。

   c. 在仪表盘页面右上角单击告警 > 修改。

   d. 找到需要修改告警的关联图表，在查询语句右侧单击 。



   e. 输入新的查询语句，并单击其右侧的预览按钮，通过校验后单击确认。



f. 确认频率和触发条件，并单击下一步。

g. 重新设置告警配置及通知方式。告警配置及通知的详细说明请参考设置告警和通知方式。

h. 单击确定，修改生效。

3.2 查看告警记录

日志服务以告警日志方式提供告警历史记录信息，并自动创建仪表盘以可视化展示所有告警规则的执行与通知情况。

- 在Logstore中查看告警日志

  创建告警规则时，日志服务自动为告警所属的Project创建一个Logstore internal-alert-history。Project内所有告警规则的每一次执行无论是否触发告警，都会产生一条日志并写入到这个Logstore中，日志字段内容请参考告警日志字段 。

  > 说明:
  > 该Logstore不会产生任何费用，不支持删除和修改。日志保存时间为7天。

- 查看告警记录仪表盘

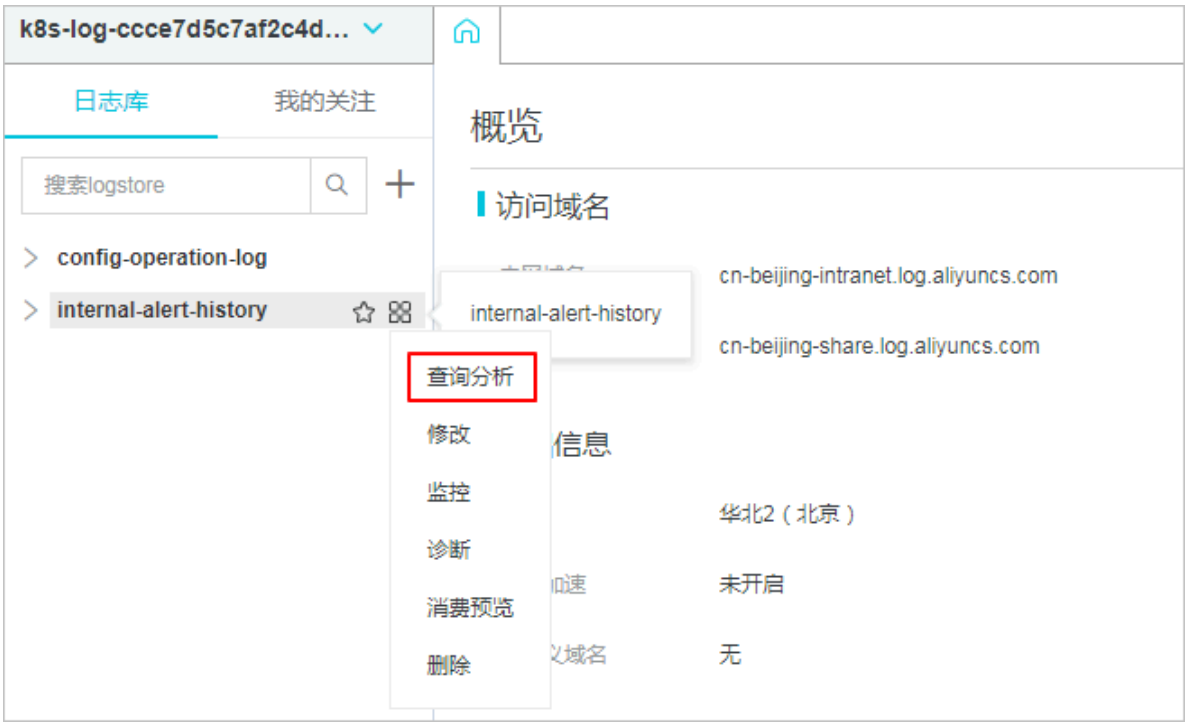
  创建告警规则之后，日志服务默认会在该告警规则所属的Project创建一个仪表盘internal-alert-analysis 用于展示告警记录。告警记录仪表盘中记录了当前Project中所有告警动作的信息，如告警次数、执行成功率、执行成功时通知率、告警规则执行次数Top10等信息。

  > 说明:
  > 不支持删除或修改该仪表盘。

在Logstore中查看告警日志

Logstore internal-alert-history中记录了当前Project中的所有告警规则的执行记录，您可以在查询界面预览、查询、分析告警记录信息。告警日志字段请参考告警日志字段。

1. 登录日志服务控制台，单击Project名称。
2. 单击internal-alert-history Logstore后的图标，选择查询分析。



3. 根据需求查询告警日志信息。

查看告警记录仪表盘

告警记录仪表盘中可以查看每次告警执行的状态、通知消息的发送状态等统计信息。

1. 在日志服务控制台单击Project名称。
2. 单击左侧导航栏的仪表盘图标。

3. 单击告警历史统计进入仪表盘。

告警历史统计仪表盘中详细展示了告警历史，包括报警是否被触发、触发状态的原因、错误信息及说明等信息。

3.3 管理告警配置

配置告警后，可以在告警概览页面查看告警规则详情与状态等信息。

除此之外，告警概览页面还支持关闭与启用告警、暂停与恢复告警、修改与删除告警、查看告警规则更新时间等操作。

查看告警配置信息

1. 登录日志服务控制台，单击Project名称。
2. 单击左侧导航栏的告警图标。
3. 在告警列表中单击指定告警规则名称。

   告警概览页面中展示了所属仪表盘名称、创建时间、上次更新时间、检查频率、启用状态、通知状态等信息。

关闭与启用告警

创建告警后可以随时关闭或启用告警。告警关闭后不会定期执行告警检查、发送通知。

1. 单击左侧导航栏的告警图标。
2. 在告警列表中单击指定告警规则名称。

   在告警概览页面中，单击启用状态后的开启或关闭按钮。

暂停与恢复告警通知

开启状态的告警可以设置暂停告警通知，在指定的时段内会定期执行告警检查，但即使满足预设条件也不会发送告警通知。

1. 单击左侧导航栏的告警图标。

2. 在告警列表中单击指定告警规则名称。

   在告警概览页面中，单击通知状态后的设置按钮。

3. 指定关闭通知的时长，并单击确认。

   暂停告警通知后，可以在通知状态列查看告警通知的恢复时间。单击通知状态后的设置按钮，可以在自动恢复告警通知之前，手动恢复告警通知。

> **说明:**
> 最多可以暂停告警通知30天。

删除告警

告警删除后不可恢复，请谨慎操作。

1. 单击左侧导航栏的告警图标。
2. 在告警列表中单击指定告警规则名称。
3. 在告警概览页面中，单击右上方的删除告警。

4. 在弹出对话框中单击确认。

3.4 升级旧版告警

新版告警兼容已经创建的旧版告警规则，如需修改告警规则，则需要补充相关属性并升级为新告警规则。

背景信息

日志服务于近期升级了告警功能，控制台保留旧版的告警配置，但建议您尽快将旧版告警规则手动升级到新版本。

如何区分新版告警规则和旧版告警规则：

- 旧版告警规则：升级前创建的告警规则，旧版告警配置不与任何仪表盘绑定。在告警配置列表中，所属仪表盘一列为空的，是旧版告警。
- 新版告警规则：升级后通过新版告警页面创建的告警规则。在告警配置列表中，新版告警的所属仪表盘一列显示为告警绑定的仪表盘名称，单击可以进入仪表盘页面。

操作步骤

1. 登录日志服务控制台，单击Project名称。
2. 在左侧导航栏中单击告警图标。
3. 在告警列表中单击需要升级的旧版告警。

   所属仪表盘一列为空的，是旧版告警。

4. 单击修改告警。

   日志服务为您保留原有的告警名称、查询语句和触发条件等信息，您只需选择设置图表名称和告警绑定的仪表盘即可。该查询语句会以图表形式保存在您指定的仪表盘中。

   告警配置的参数说明请查看设置告警。

5. 设置通知方式。

   默认保留旧版告警的通知方式和通知内容，也可以增加一种或多种通知方式。

6. 确认完毕后，单击提交。

   完成旧版告警配置的迁移后，用户就可以去关联的仪表盘中查看默认创建的图表，还可以在告警历史统计中查看到新的告警配置的告警情况。

4 参考信息

4.1 告警条件表达式语法

告警支持用户配置条件表达式，根据表达式的结果是否为真来判断是否满足告警条件。

在判断表达式是否为真时，用户配置的查询的执行结果将作为输入，日志字段作为变量，一旦条件为真则触发告警并返回。

限制说明

- 负数需要使用括号，如 x+(-100)<100。
- 数值类型都被当成64位浮点数，如果使用比较操作如等于可能存在误差。
- 变量只能包含字母和数字，且首字母必须是字母。
- 表达式长度最多支持128个字符。
- 组合求值时最多只会计算1000种组合，如果没有找到结果为真的组合，则视为false。
- 最多只支持三个查询。
- 当且仅当表达式的值为布尔值true的时候，才会触发告警。如 100+100，计算结果为200，不会触发告警。
- `true`、`false`、`$`和`.`是保留字，不能作为变量使用。

基础语法

告警条件表达式支持以下语法类型。

语法类型	说明	示例
基础运算符	支持加减乘除、取模运算符，即： +-*/%。	x*100+y>200 x%10>5

语法类型	说明	示例
比较运算符	支持大于（>）、大于等于（>=）、小于（<）、小于等于（<=）、等于（==）、不等于（!=）、正则匹配 （=~）、 正则不匹配（!~）8种比较运算符。 说明: · 斜杠需要转义。 · 正则表达式目前支持符合RE2规范的语法。	x >= 0 x < 100 x <= 100 x == 100 x == "foo" 正则匹配：x =~ "\\w+"
逻辑操作符	支持逻辑操作符：与（&&）、或（||）。	x >=0&&y <=100 x > 0 || y > 0
取反前缀操作	支持取反前缀操作（!）。	!(a < 1 && a > 100)
数值常量	支持数值常量，作为64位浮点数处理。	x > 100
字符串常量	支持字符串常量，形式为单引号引起来的字符串。如：'string'。	foo == 'string'
布尔常量	支持布尔常量：true和false。	(x > 100) == true
括号	支持使用括号改变计算的优先级。	x*(y+100)>100
contains函数	支持使用contains函数判断是否包含子串， 如contains(field, 'xxxx') 返回true则表示 field 包含 xxxx 这个子串。	contains(foo, 'hello')

多个结果集组合求值

· 语法

告警支持用户关联多个图表的查询，在使用多个查询结果进行计算时，变量需要加上特定前缀以区分从哪个结果集中获取对应的变量值，格式为$N.fieldname，其中N为查询的编号。目前支持用户最多配置三个查询，因此N的取值范围为[0,2]。如$0.foo表示第1个查询的foo字段。当仅有一个查询时，前缀可以省略。

说明:
如何查看查询的编号?

在告警配置步骤中，关联图表一栏显示了各个图表/查询分析语句的编号。其中第一个图表/查询分析语句编号为0，第二个图表/查询分析语句编号为1，第三个图表/查询分析语句编号为2。

- 表达式求值

  在多个查询结果返回时，根据表达式的变量来判断需要使用哪些结果集求值。例如用户配置了三个查询，每个查询分别返回了x,y,z 条结果。而用户配置的表达式为$0.foo > 100 && $1.bar < 100，则说明判断表达式的值只需要使用前两个结果集，进行x*y次求值直到某次求值返回true，或者达到计算次数上限后直接返回false，目前上限为1000次。

运算方式

说明:

- number为64位浮点数类型。
- string常量需要以单引号或英文双引号包含起来，如'string'、“string”。
- 布尔值包括true和false。

运算符	运算方式		
	变量与变量运算	非string常量与变量运算	string常量与变量运算
四则运算（+-*/%）	左右值转number后运算。		不支持。
比较运算： 大于（>）、大于等于（>=）、小于（<）、小于等于（<=）、等于（==）、不等于（!=）	按照以下优先级决定运算顺序： 1. 左右值转number后按照数值序运算，如转换失败则执行下一优先级的运算。 2. 左右值按string类型字典序运算。	左右值转number后运算（数值序）。	左右值按string类型运算（字典序）。
正则是否匹配： 正则匹配（=~）、正则不匹配（!~）	左右值按string类型运算。	不支持。	左右值按string类型运算。
逻辑运算： 与（&&）、或（||）	不支持对查询结果字段直接应用该运算符，左右值必须分别为子运算式，且运算结果为bool类型。		
取反前缀（!）	不支持对查询结果字段直接应用该运算符，被取反的值必须为子运算式，且运算结果为bool类型。		
字符串查找（contains）	左右值转string类型运算。	不支持。	左右值按string类型运算。
括号()	决定运算结合顺序与优先级。		

4.2 告警日志字段

设置告警规则后，日志服务自动创建Logstore，以日志方式记录告警的执行与通知信息。本文档介绍告警日志的字段。

告警执行历史日志字段

字段名称	说明	示例
AlertDisplayName	告警规则显示名称。	告警规则测试
AlertID	每次执行的唯一ID。	0fdd88063a611aa11493 8f9371daeeb6-1671a52eb23
AlertName	每个Project内部唯一的告警规则名称。	alert-1542111415-153472
Condition	条件表达式。	$0.count > 1
Dashboard	告警规则关联的仪表盘	my-dashboard
FireCount	上次通知之后的累积触发次数。	1
Fired	是否触发告警，取值为true或者false。	true
LastNotifiedAt	上次通知时间，Unix时间戳。	1542164541
NotifyStatus	通知状态，可能的值为： · Success：成功。 · Failed：失败。 · NotNotified：未通知。 · PartialSuccess：部分成功。	Success

字段名称	说明	示例
Reason	失败或者未通知的原因。	result type is not bool

Results	查询参数和结果，数组类型，字段说明请参考Result字段说明。	[
		  {
		  "EndTime": 1542334900,
		  "FireResult": null,
		  "LogStore": "test-logstore",
		  "Query": "* | select count(1) as count",
		  "RawResultCount": 1,
		  "RawResults": [
		  {
		  "__time__": "1542334840",
		  "count": "0"
		  }
		  ],
		  "StartTime": 1542334840
		  }
		]

Status	执行结果，取值为Success或者Failed。	Success

Result字段说明

字段名称	说明	示例
Query	查询语句。	* | select count(1) as count
LogStore	查询的目标Logstore。	my-logstore
StartTime	查询开始时间。	2019-01-02 15:04:05
StartTimeTs	查询开始时间，Unix时间戳。	1542334840
EndTime	查询结束时间。	2019-01-02 15:19:05

字段名称	说明	示例
EndTimeTs	查询结束时间，Unix时间戳。注意，实际查询区间为[StartTime, EndTime)。	1542334900
RawResults	查询原始结果，数组类型，每个元素为一条日志。数组长度和日志内容大小有关，最多包含100条。	`[ { "__time__": "1542334840", "count": "0" } ]`
RawResultsAsKv	按照key-value格式化的触发告警的原始日志。 说明: 该字段只可以作为模版变量引用，不会保存到Logstore。	[foo:0]
RawResultCount	原始结果条数。	1
FireResult	触发告警的日志。如果告警未触发则为null。	`{ "__time__": "1542334840", "count": "0" }`
FireResultAsKv	按照key-value格式化的触发告警的日志。 说明: 该字段只可以作为模版变量引用，不会保存到Logstore。	[foo:0]

5 最佳实践

5.1 告警设置

日志服务支持根据仪表盘中的查询图表设置告警，实现实时的服务状态监控。

告警的查询区间和执行间隔

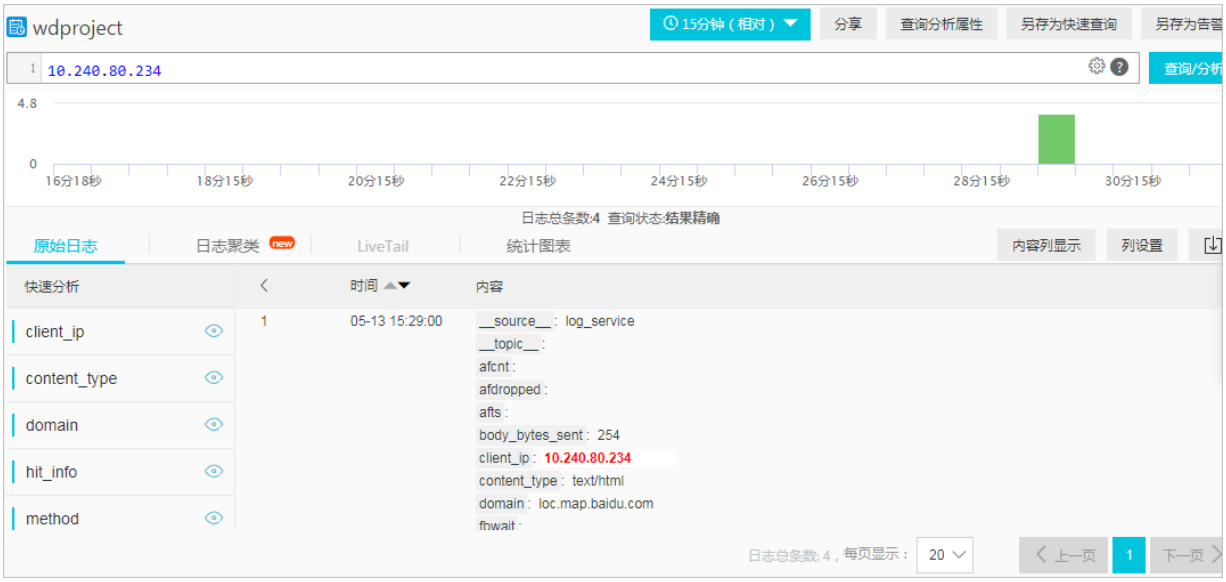
告警的实现原理是基于告警的查询范围，根据执行间隔定时执行配置的查询语句，并将查询结果作为告警条件的参数进行计算，如果计算结果为true，则告警触发。

不要将查询范围设置成和执行间隔一致的相对时间，如查询范围为相对1分钟，执行间隔为1分钟。原因如下（以执行间隔为1分钟为例）：

- 数据写入日志服务到能够被查询到中间存在延时，即便延时很低，也存在数据漏查的风险。如告警执行时间为12:03:30， 查询范围为相对一分钟则为[12:02:30，12:03:30)，对于12:03:29秒写入的日志，不能保证12:03:30这次时间点能够查询到。
  - 如果对告警的准确性要求高（不重复报警，不漏报），查询范围起止时间可以往前推移，如70秒前—10秒前。如告警执行时间为12:03:30，则查询范围为 [12:02:20, 12:03:20)，通过设置10秒的缓冲时间来避免因为索引速度导致的漏查。
  - 如果对实时性要求高（第一时间收到告警，能够容忍重复报警），查询范围开始时间可以往前推移，如 70秒—现在。如告警执行时间为12:03:30， 查询范围设置为相对70秒， [12:02:20, 12:03:30)。
- 对于写入包含同一分钟不同时间的日志时，由于日志服务的索引构建方式，可能会存在较晚的日志的索引落入较早的日志的时间点的可能。 如告警执行时间为12:03:30， 查询范围为相对一分钟则为[12:02:30，12:03:30)，如果在12:02:50秒写入多条日志，这些日志的时间有12:02:20，12:02:50等，那么这一批日志的索引可能会落入12:02:20 这个时间点，导致使用时间范围 [12:02:30，12:03:30) 查询不到。
  - 如果对告警的准确性要求高（不重复报警，不漏报），查询范围使用整点分钟，如整点1分钟，整点5分钟，整点1小时等，并且将执行间隔设置成一致的时间，如1分钟，5分钟，1小时等。
  - 如果对实时性要求高（第一时间收到告警，能够容忍重复报警），查询时间范围至少需要包含前一分钟。如告警执行时间为12:03:30， 查询范围可以设置为相对90秒，那么实际的查询范围为 12:02:00 - 12:03:30，同时设置执行间隔为1分钟。

基于查询结果告警

如果针对某个查询，只要查询结果不为空就认为满足告警条件，可以设置告警条件为判断任意字段存在即告警。如搜索包含IP 10.240.80.234 的日志：



只要查询到包含 10.240.80.234 的日志就告警，则可以通过任意字段设置一个始终为true的告警条件。假设 client_ip 这个字段在每条日志都存在且不可能为空字符串，则只要 client_ip 这个字段不为空就触发告警：

基于分析结果告警

基于分析结果设置告警是最常见的场景，比如针对特定的字段聚合之后告警。以最常见的包含ERROR 关键字的日志条数达到阈值即触发告警为例，查询语句可以按照如下的方式设置：

```
ERROR | select count(1) as errorCount
```

告警条件则为 errorCount 大于某个阈值，如 errorCount > 0。

关联查询告警

当从仪表盘入口创建告警时，可以选择多个图表作为告警查询的输入。

- 对不同时间范围的查询结果进行组合告警。

  如 15分钟内的PV 大于100000 且一小时内的UV 小于1000时触发告警：

说明：

在选择多个图表时，查询区间相互独立。在触发条件中需要使用 ${编号}.{字段} 的方式引用查询结果中的字段。如：$0.pv > 100000 && $1.uv < 1000 。

- 基于部分图表告警，其他图表的查询结果作为辅助信息。

  基于日志级别为ERROR的日志条数告警，查询语句：

  ```
  level: ERROR | select count(1) as errorCount
  ```

  告警条件：

  ```
  errorCount > 10
  ```

  与此同时，也希望能够在告警通知中看到实际的日志级别为ERROR的日志，则可以再配置第2个查询：

  ```
  level: ERROR
  ```

  在告警通知中只需要设置：

  ```
  ${results[1].RawResultsAsKv}
  ```

  即可看到实际的日志级别为ERROR的日志。

告警抑制

当告警触发时，可能会在一段时间内多次收到通知。为了防止因为数据抖动导致的误报和重复告警，可以通过如下两种方式对告警进行抑制：

- 设置连续触发通知阈值。

  只有告警在连续多次检查中都满足告警条件才会触发告警。

  如告警执行间隔为1分钟，触发阈值为5，则表示在连续5次即5分钟内每次告警检查结果都满足告警条件才会发送通知。只要有一次没有满足触发条件，计数将会重置。

- 设置通知间隔。

  当告警设置的执行间隔较小时，防止频繁收到通知，可以设置两次通知之间的最小间隔。如告警执行间隔为1分钟，通知间隔为30分钟，即使30分钟内有告警触发，也不会收到任何通知。

关闭告警通知

收到告警通知之后，如果希望临时关闭通知。可以通过告警概览页面关闭通知，如下图所示：

选择关闭的时长，如30分钟：

则在30分钟内，不会再发送任何通知，即便告警触发。在30分钟之后，通知自动恢复。

钉钉群成员查看告警

钉钉群是最常见的告警通知渠道，在配置钉钉通知时，我们可以@钉钉群的成员处理告警。如下图所示：

说明:

需要在被@人列表和发送内容中同时指定对应成员的手机号。被@人列表是用于识别发送内容中的@是提醒还是普通的@字符。

使用模版变量丰富通知内容

在配置通知方式时，可以使用模版变量来丰富通知内容。邮件标题，钉钉标题，消息内容都支持使用模版变量。 每次告警执行的时候，都会生成一个告警的上下文，其中的每个变量都可以作为模版变量，完整的变量可以参考通知方式。

- **对于顶层的变量如Project，AlertName，Dashboard，可以直接使用${project} 这种方式引用，不区分大小写。**
- **对于每个查询的上下文，包含在Results 这个数组中，数组中的每个元素对应告警关联的一个图表（对于大多数场景，可能只有一个元素），包含的变量如下所示：**

```
{
  "EndTime": "2006-01-02 15:04:05",
```

```
  "EndTimeTs": 1542507580,
  "FireResult": {
    "__time__": "1542453580",
    "field": "value1",
    "count": "100"
  },
  "FireResultAsKv": "[field:value1,count:100]",
  "Truncated": false,
  "LogStore": "test-logstore",
  "Query": "* | SELECT field, count(1) group by field",
  "QueryUrl": "http://xxxx",
  "RawResultCount": 2,
  "RawResults": [
    {
      "__time__": "1542453580",
      "field": "value1",
      "count": "100"
    },
    {
      "__time__": "1542453580",
      "field": "value2",
      "count": "20"
    }
  ],
  "RawResultsAsKv": "[field:value1,count:100],[field:value2,count:20
]",
  "StartTime": "2006-01-02 15:04:05",
  "StartTimeTs": 1542453580
}
```

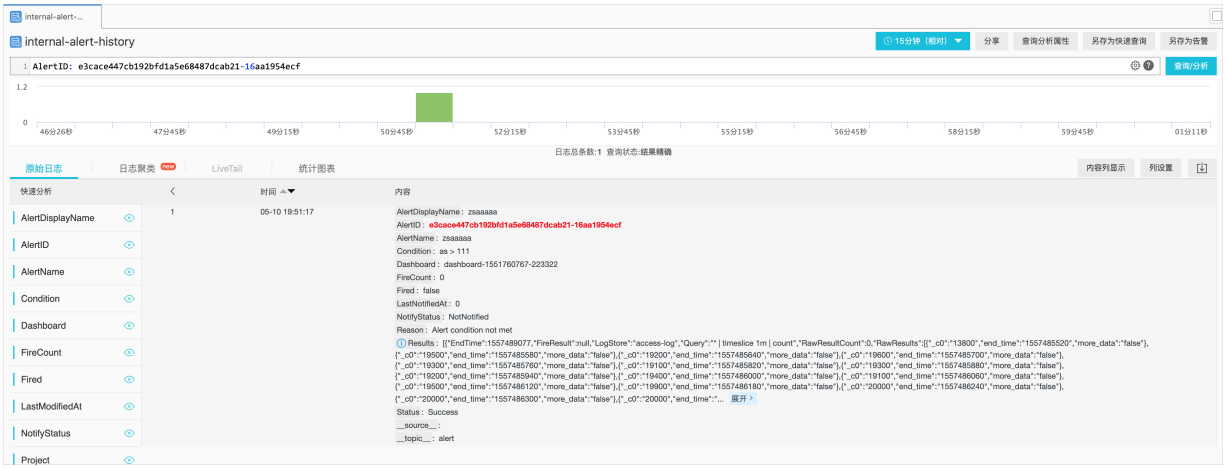

字段解释可以参考告警日志字段。Results中的字段时可以通过如下方式引用：

- 数组类型通过"${fieldName[{index}]}"方式引用， 下标从0开始。如 ${results[0]} 表示引用Results的第1个元素。
- 对象类型通过"${object.key}"引用，如 ${results[0].StartTimeTs}的结果为 1542453580。

> **说明：**
> 只有RawResults 和FireResult 内的字段为查询结果，区分大小写，其他字段均不区分大小写。

排查告警未触发原因

配置告警之后，可以通过查看告警记录查看告警统计。对于单次告警的上下文，可以直接在internal-alert-history这个Logstore中查看，如下图所示。



日志字段解释参考告警日志字段。

每次执行都会生成一个唯一的告警ID和一条对应的日志，日志中包含了告警执行的状态和查询的结果（如果查询结果超过2KB，会被截断），通过日志可以排查告警没有触发的原因。

6 FAQ

6.1 告警配置案例

本文档为您展示常见的告警配置案例。

在通知内容中添加错误日志的原始日志内容

需求：在过去5分钟内，错误日志5条以上即触发报警，通知内容中包含错误日志的原始日志内容。

方案：

- 关联的查询语句：
  - 编号0：`level: ERROR`
  - 编号1：`level: ERROR | select COUNT(*) as count`
- 触发条件：`$1.count > 5`
- 通知内容：`${results[0].rawresults}`


修改告警
告警配置
通知
* 告警名称
告警测试
* 关联图表
0
图表名称
告警测试
查询语句
level: ERROR
查询区间
15分钟（相对）
1
图表名称
错误日志条数
查询语句
level: ERROR | select COUNT(*) as count
查询区间
15分钟（相对）
2
添加
* 执行间隔
15
分钟
* 触发条件
$1.count > 5
支持加(+)减(-)乘(*)除(/)取模(%)运算和>,>=,<,<=,==,!=,=~,!~比较运算。帮助文