ALIBABA CLOUD

阿里云

日志服务

告警

文档版本：20210525

阿里云

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
危险	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。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会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，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	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。	单击**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。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	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。	`switch {active|stand}`

目录

1.简介

日志服务支持为查询或分析结果设置告警。设置告警后，日志服务定期检查查询或分析结果，当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。

使用限制

日志服务告警相关限制说明如下表所示。

限制项	说明
组合查询	组合查询个数为1~3个。
字符串	如果日志字段长度超过1024个字符，只截取前1024个字符用于计算。
条件表达式	条件表达式限制说明如下： • 条件表达式长度为1~128个字符。 • 条件表达式只判断每次查询中的前100条查询结果。 • 条件表达式计算次数不超过1000次。
查询区间	每条查询语句的查询时间跨度不能超过24小时。
告警语音通知	告警语音未拨通时，不会重复拨打，将以短信方式发送一次通知。 无论告警语音是否拨通均按一次计费。未拨通的提示短信，不会额外产生短信费用。

告警中的查询语句

告警配置中的语句，可以为查询语句或查询分析语句。两者区别如下：

- 查询语句：返回查询条件命中的日志数据。更多信息，请参见查询简介。

  例如，查询最近15分钟内包含error的日志，查询语句为error，一共有154条查询结果。每条日志都是Key-Value组合，您可以对某个Key对应的Value设置告警规则。

  > **说明** 当查询结果超过100条时，告警规则只判断前100条，只要前100条中任意一条日志符合告警规则，就会触发告警。

- 查询分析语句：对查询条件命中的日志进行计算，返回计算结果。更多信息，请参见分析简介。

  例如，统计所有日志中状态码为ok的日志比例，查询分析语句为`* | select sum(case when status='ok' then 1 else 0 end) *1.0/count(1) as ratio`。设置触发条件为`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。

费用标准

日志服务告警通知升级后，取消短信、语音和邮件每天99条通知的限制。其中，短信和语音通知将变更为按调用次数收费，邮件通知免费。日志服务计划于2020年12月7日完成升级，正式开始对当日及之后的短信、语音告警账单收费，并取消短信、语音和邮件的每天99条的限制。更多信息，请参见计量项和计费项。

说明

- 告警语音未拨通时，不会重复拨打，将以短信方式发送一次通知。
- 无论告警语音是否拨通均按一次计费。未拨通的提示短信，不会额外产生短信费用。

2.设置告警

日志服务支持在查询分析页面或仪表盘页面设置告警，并在满足告警条件时发送告警信息。本文介绍如何在日志服务控制台上设置告警。

前提条件

- 已采集到日志数据。
- 已配置索引。

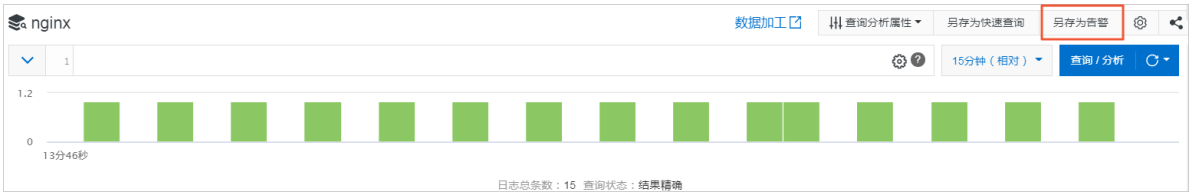
背景信息

基于统计图表设置告警。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。

> **说明** 如果仪表盘中的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。详情请参见修改告警配置。

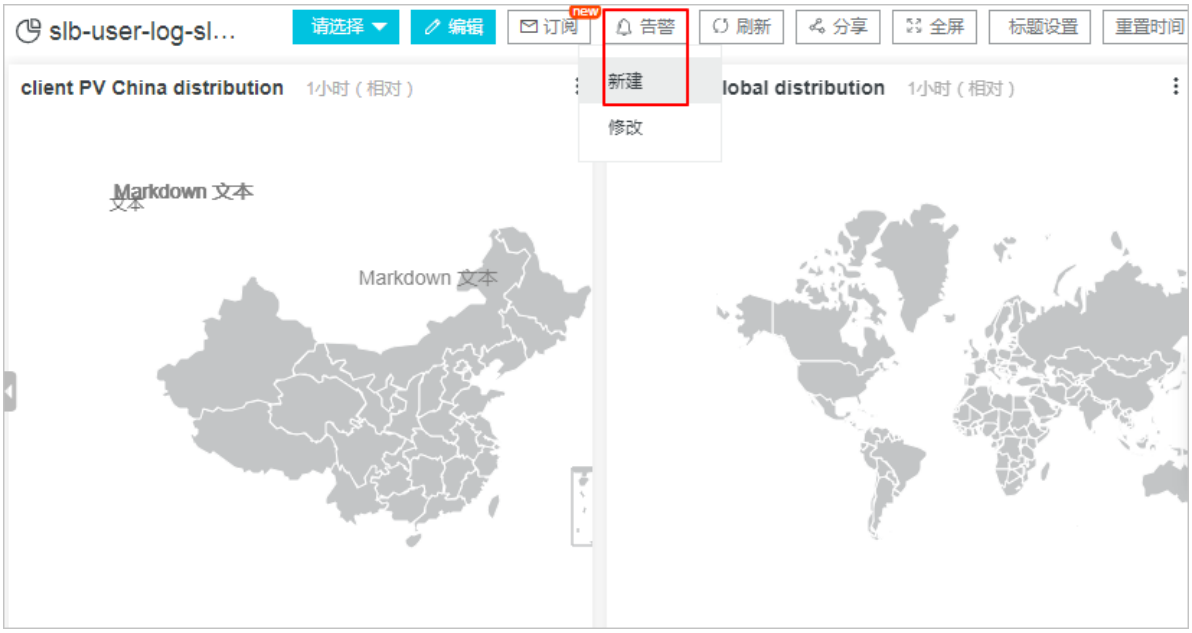
- 创建图表并设置告警

  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。



- 在仪表盘页面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。



常见告警配置案例请参见告警配置案例。

操作步骤

本文以在仪表盘页面对已有图表设置告警为例。

1. 登录日志服务控制台。
2. 单击目标Project。
3. 在左侧导航栏中，单击，进入仪表盘列表。
4. 单击目标仪表盘。
5. 在页面右上角，单击**告警 > 新建**。
6. 在**告警配置**页签中，设置告警规则并单击**下一步**。告警配置参数如下所示。

参数	说明
告警名称	告警名称，长度为1~64个字符。
关联图表	设置告警中关联的图表。 支持添加多个图表，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。 单击查询语句后面的，可修改查询语句。 设置关联图表时，**查询区间**为日志服务每次执行查询时，读取数据的时间范围，支持相对时间与整点时间。例如，执行查询的时间点为14:30:06： ○ 设置**查询区间**为15分钟（相对），则实际查询区间为14:15:06-14:30:06。 ○ 设置**查询区间**为15分钟（整点时间），则实际查询区间为14:15:00-14:30:00。
频率	日志服务每次执行告警检查的时间。 **说明** 目前日志服务只检查查询结果中的前100条日志。
触发条件	判断是否触发告警的条件表达式，满足该条件时产生告警。例如，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，详情请参见如何查看图表编号。
触发通知阈值	累计触发次数达到该值时，根据通知间隔发送告警。不满足触发条件时不计入统计。 默认值为1，即满足一次触发条件就检查通知间隔。 通过配置通知阈值可以实现多次触发，一次通知。例如，**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。

参数	说明
通知间隔	两次告警通知之间的时间间隔。 如果某次查询符合触发条件，累计的触发次数达到**触发通知阈值**，且距离上次发送通知的时间已满足**通知间隔**，则发送通知。例如，通知间隔为5分钟，则5分钟内最多收到一次通知。 **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。

7. 在**通知**页签中，设置通知方式，并单击**提交**。通知方式包括短信、语音、邮件、WebHook-钉钉机器人、WebHook-自定义和通知中心。您可以执行多次添加，添加多种通知方式，你也可以单击**导入已有通知方式**，通知方式介绍与操作步骤请参见通知方式。

常见问题

如何查看图表编号？

在**关联图表**中显示各个图表及查询语句的编号。其中第一个图表及查询语句编号为0，第二个图表及查询语句编号为1，第三个图表及查询语句编号为2。

执行结果

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。

3.通知方式

日志服务支持设置一种或多种告警通知方式，包括短信、语音、邮件、钉钉、WebHook-钉钉机器人、WebHook-自定义和通知中心。本文介绍各种通知方式的配置步骤。

通知中心（推荐）

设置告警通知方式为通知中心，则触发告警后，日志服务会通过通知中心向指定人员发送告警通知。

1. 在阿里云消息中心，配置消息接收人。
   i. 登录阿里云消息中心。
   ii. 选择**消息接收管理 > 基本接收管理**，单击**日志服务（LOG）告警**右侧的**修改**。

   iii. 在**修改消息接收人**窗口选择消息接收人，单击**保存**。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码和邮箱，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。

2. 在日志服务控制台上配置通知方式。
   i. 在设置告警时，在**通知列表**中选中**通知中心**，并单击**添加**。
   ii. 配置发送内容。发送内容的长度为1~500个字符。支持自定义，并且支持使用模板变量。更多信息，请参见模板变量。
   iii. 单击**提交**。此处以配置一种通知方式为例，如果您要添加多种通知方式，可以执行多次添加操作后，再单击**提交**。

短信

设置告警通知方式为短信，则触发告警后，日志服务会向指定的手机号码发送短信通知。

> **说明** 使用短信告警通知时，发送通知的号码是随机的，无法提供固定号码。

1. 在设置告警时，在**通知列表**中选中**短信**，并单击**添加**。

2. 配置如下参数。

参数	说明
手机号码	填写接收告警通知的手机号码，多个手机号码之间通过逗号（,）分隔。
发送内容	填写告警短信内容，长度为1~100个字符。支持使用模板变量。更多信息，请参见模板变量。

3. 单击**提交**。此处以配置一种通知方式为例，如果您要添加多种通知方式，可以执行多次添加操作后，再单击**提交**。

语音

设置告警通知方式为语音，则触发告警后，日志服务会向指定的手机号码发送电话通知。语音内容中包括Project名称、告警名称和已配置的发送内容。

> **说明**
> - 如果某次告警电话未接通，将以短信方式发送一次通知。
> - 日志服务使用如下号码进行语音告警通知，您可将如下号码添加到手机白名单中，以免告警电话被拦截。
>
>   02388560936、02031241964、02031341953、02386133954、02386133948、051068094476、051068094459、051068094479、051068094489、051068094436、051068094429、051068094426、057126886446、057126886464、057126886644、057126886767、057126886776

1. 在设置告警时，在**通知列表**中选中**语音**，并单击**添加**。
2. 配置如下参数。

参数	说明
手机号码	填写接收告警通知的手机号码，多个手机号码之间通过逗号（,）分隔。
发送内容	填写告警语音内容，长度为1~100个字符。支持使用模板变量。更多信息，请参见模板变量。 **说明** 建议使用中文。

3. 单击**提交**。此处以配置一种通知方式为例，如果您要添加多种通知方式，可以执行多次添加操作后，再单击**提交**。

邮件

设置告警通知方式为邮件，则触发告警后，日志服务会向指定的邮箱地址发送邮件通知。

> **说明** 日志服务使用monitor@monitor.aliyun.com邮件地址发送邮件告警通知，您可将该邮件地址添加到邮箱白名单中，以免告警邮件被拦截。

1. 在设置告警时，在**通知列表**中选中**邮件**，并单击**添加**。

2. 配置如下参数。

参数	说明
收件人	填写接收告警通知的邮箱地址，多个邮箱地址之间通过逗号（,）分隔。
主题	告警主题，长度为1~100个字符。支持自定义，并且支持使用模板变量。更多信息，请参见模板变量。
发送内容	填写告警邮件通知的内容，长度为1~500个字符，支持使用模板变量。更多信息，请参见模板变量。

3. 单击**提交**。此处以配置一种通知方式为例，如果您要添加多种通知方式，可以执行多次添加操作后，再单击**提交**。

WebHook-钉钉机器人

设置告警通知方式为WebHook-钉钉机器人，则触发告警后，日志服务会通过钉钉机器人向指定的钉钉群发送告警通知，还支持提醒指定人员。

> **说明** 每个机器人每分钟最多发送20条告警通知。

1. 配置钉钉机器人。
   i. 打开钉钉客户端，进入钉钉群。
   ii. 单击右上角**群设置**图标，并单击**智能群助手 > 添加机器人**。
   iii. 在**群机器人**对话框中，单击**添加机器人**区域中的**+**。
   iv. 选择**自定义（通过WebHook接入自定义服务）**，并单击**添加**。
   v. 在**添加机器人**对话框中，输入**机器人名字**，配置**安全设置**，勾选**我已阅读并同意《自定义机器人服务及免责条款》**并单击**完成**。

      > **说明** 建议**安全设置**选择为**自定义关键字**，最多可以设置10个关键字，消息中至少包含其中1个关键字才可以发送成功，建议其中一个关键字设置为**告警**。更多关于安全设置请参见钉钉开放平台。

   vi. 单击**复制**，复制WebHook链接。
2. 在日志服务控制台上配置通知方式。
   i. 在设置告警时，在**通知列表**中选中**WebHook-钉钉机器人**，并单击**添加**。

ii. 配置如下参数。

参数	说明
请求地址	输入步骤1中复制的WebHook链接。
标题	告警主题，支持自定义，并且支持使用模板变量。更多信息，请参见模板变量。长度为1~100个字符。
提醒接收者	可选值为不提醒、所有人、指定成员。选择**指定成员**时，**被@人列表**中需填写指定人员的手机号码，多个手机号用逗号（,）分隔。
发送内容	已默认配置发送内容，长度为1~500个字符。支持自定义，并且支持使用模板变量。更多信息，请参见模板变量。 **说明** 如果需要提醒指定人员，必须在**发送内容**中增加 `@指定人员的手机号码` 。

iii. 单击**提交**。此处以配置一种通知方式为例，如果您要添加多种通知方式，可以执行多次添加操作后，再单击**提交**。

WebHook-自定义

设置告警通知方式为WebHook-自定义，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 此方式对应的超时时间为5秒，如果发出请求后5秒内没有返回，则表示发送失败。

1. 在设置告警时，在**通知列表**中选中**WebHook-自定义**，并单击**添加**。
2. 配置如下参数。

参数	说明
请求地址	自定义的WebHook地址，必须为外网域名。
请求方法	支持GET、POST、DELETE、PUT、OPTIONS等请求方法，默认请求头为Content-Type: application/json;charset=utf-8。 单击**添加请求头**，可追加请求头（Header）信息。
发送内容	已默认配置发送内容，长度为1~500个字符。支持自定义，并且支持使用模板变量。更多信息，请参见模板变量。

3. 单击**提交**。此处以配置一种通知方式为例，如果您要添加多种通知方式，可以执行多次添加操作后，再单击**提交**。

4.授权RAM用户告警操作权限

使用阿里云主账号给RAM用户授权，可实现通过RAM用户进行告警操作。本文档介绍如何创建阿里云RAM用户并授予其告警操作权限。

背景信息

您可以通过如下两种方式给RAM用户授予日志服务告警操作权限。

- 极简授权：授予RAM用户日志服务的全部操作权限（AliyunLogFullAccess）。更多信息，请参见创建RAM用户及授权。
- 自定义权限策略：仅授予RAM用户创建、修改告警的权限。本文以此方式为例进行授权操作。

操作步骤

1. 登录RAM 控制台。
2. 创建权限策略。
   i. 在左侧导航栏中，选择**权限管理 > 权限策略管理**。
   ii. 单击**创建权限策略**。
   iii. 在**新建自定义权限策略**页面中，配置如下参数，并单击**确定**。

参数	说明
策略名称	配置策略名称。
配置模式	选择**脚本配置**。

参数	说明

策略内容	将配置框中的原有脚本替换为如下内容。
	其中，请根据实际情况替换*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/*"
	}
	]
	}

3. 创建RAM用户。如何创建RAM用户，请参见创建RAM用户。如果已有可用的RAM用户，请跳过此步骤。
4. 为RAM用户授权。
   i. 在左侧导航栏中，选择**人员管理 > 用户**。

ii. 找到目标RAM用户，单击**添加权限**。

iii. 单击**自定义策略**，选中步骤2中创建的策略，单击**确定**。

iv. 单击**完成**。

5.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。

背景信息

- 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创建一个名为**internal-alert-history**的Logstore。当前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该Logstore中，日志字段内容请参见告警日志字段。

  > **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。

- 在仪表盘中查看告警记录

  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创建一个名为**internal-alert-analysis**的仪表盘，用于展示告警记录。该仪表盘记录了当前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

1. 登录日志服务控制台。
2. 单击目标Project。
3. 在**日志存储 > 日志库**页签中，单击**internal-alert-history**Logstore右侧的图标 > **查询分析**。
4. 根据需求查询告警日志信息。

在仪表盘中查看告警记录

1. 登录日志服务控制台。
2. 单击目标Project。
3. 在左侧导航栏中，单击图标，进入仪表盘列表。
4. 单击**告警历史统计**仪表盘。
5. 查看详细的告警历史统计信息。**告警历史统计**仪表盘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。


告警历史统计
请选择
订阅
刷新
分享
全屏
标题设置
重置时间
告警次数 今天（相对）
0 次
环比昨日
执行成功率 今天（相对）
执行成功率
100%
执行成功时通知率 今天（...
执行成功时通知率
0%
告警规则执行次数Top10 今天（相对）
mgqdd
100.00%
通知成功次数 今天（相对）
0 次
环比昨日
告警历史 今天（相对）
ID
告警名称
显示名称
执行时间
触发条件
仪表盘
通知发送状态
执行结果
alert-1564134857-894296
mgqdd
2019-07-26 18:09:23
request_method==1
dashboard-1564134857-996966
NotNotified
Success
错误信息
解释
如何解决
检查条件表达式是

6.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，并执行修改、删除等操作。

背景信息

在告警概览页面，您可以执行关闭与启用告警、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。
2. 在**Project列表**区域，单击目标Project。
3. 在左侧导航栏中，单击 图标。
4. 单击目标告警，进入告警概览页面。
5. 查看告警配置信息。 在**告警概览**页面中，展示所属仪表盘名称、创建时间、上次更新、检查频率、启用状态、通知状态等信息。

修改告警配置

1. 在**告警概览**页面中，单击**修改配置**。您也可以在左侧导航栏中，单击 图标，再单击目标仪表盘，然后单击**告警 > 修改**，进入**修改告警**页面，进行修改。
2. 修改告警关联图表。 在**图表名称**中选择目标图表。
3. 修改查询语句。
   i. 在**关联图表**中，找到需要修改的查询语句，单击
   图标。

   > **说明** 如果告警规则绑定的为查询语句，则只支持修改为查询语句。如果告警规则绑定的为查询分析语句（查询语句|分析语句），则只支持修改为查询分析语句。例如，为查询语句request_method: GET设置告警规则后，可以将查询语句修改为error，但不能修改为error| select count(1) as c。

   ii. 输入新的查询语句，单击**预览**。
   iii. 通过校验后单击**确定**。
4. 修改频率、触发条件、触发通知阈值和触发条件，并单击**下一步**。参数说明请参见设置告警。
5. 修改通知方式，并单击**提交**。通知方式详情请参见通知方式。

关闭与启用告警

日志服务支持在创建告警后，随时关闭或启用告警。

> **说明** 关闭告警后，日志服务不再执行告警检查、发送通知等操作。

在**告警概览**页面，单击**启用状态**后的**开启**或**关闭**，可开启或关闭告警。

关闭与恢复告警通知

告警的开启状态为**已开启**时，支持关闭告警通知。

> **说明** 在关闭告警通知期间，日志服务仍会定期执行告警检查，即使满足告警条件也不会发送告警通知。

1. 在**告警概览**页面，单击**通知状态**后的**设置**。
2. 设置关闭时长，并单击**确定**。关闭告警通知后，可在**通知状态**中查看告警通知的恢复时间。单击**通知状态**后的**设置**，可在自动恢复告警通知前，手动恢复告警通知。

删除告警

在**告警概览**页面的右上角，单击**删除告警**。

> **注意** 删除告警后不可恢复，请谨慎操作。

7.参考信息

7.1. 模板变量

本文介绍告警所支持的模板变量以及引用方式。

引用原理

您在配置通知方式时，可在**发送内容**和**主题**中，通过*${fieldName}*方式引用模板变量。日志服务发送告警通知时，会将**发送内容**和**主题**中的模板变量替换为真实值。例如*${Project}*替换为告警规则所属的Project名称。

> **注意** 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。

可用变量及其引用

变量	说明	发送内容及告警主题配置示例	告警通知示例
Aliuid	Project所属的阿里云账号ID。	${Aliuid}用户的告警规则已触发。	1234567890用户的告警规则已触发。
Project	告警规则所属的Project。	${Project}项目中的告警规则已触发。	my-project项目中的告警规则已触发。
AlertID	告警ID。	告警ID是${AlertID}。	告警ID是0fdd88063a611aa114938f9371daeeb6-1671a52eb23。
AlertName	告警规则名称，Project内唯一。	${AlertName}告警规则已触发。	alert-1542111415-153472告警规则已触发。
AlertDisplayName	告警规则显示名称。	${AlertDisplayName}告警已触发。	网站监控告警已触发。
Condition	触发告警的条件表达式。告警通知中，变量将被替换为真实值，并使用中括号（[]）包裹。	告警条件表达式为${Condition}。	告警条件表达式为[5] > 1。
RawCondition	触发告警的原始条件表达式。	触发告警的原始条件表达式为${RawCondition}。	触发告警的原始条件表达式为count > 1。
Dashboard	告警所关联的仪表盘名称。	告警所关联的仪表盘为${Dashboard}。	告警所关联的仪表盘为mydashboard。

变量	说明	发送内容及告警主题配置示例	告警通知示例
DashboardUrl	告警所关联的仪表盘地址。	告警所关联的仪表盘地址为${DashboardUrl}。	告警所关联的仪表盘地址为https://sls.console.aliyun.com/next/project/myproject/dashboard/mydashboard。
FireTime	触发时间。	告警触发时间为${FireTime}。	告警触发时间为2021-01-02 15:04:05。
FullResultUrl	告警历史记录的查询地址URL。	单击${FullResultUrl}，查看告警详情。	单击https://sls.console.aliyun.com/next/project/my-project/logsearch/internal-alert-history?endTime=1544083998&queryString=AlertID%3A9155ea1ec10167985519fccede4d5fc7-1678293caad&queryTimeType=99&startTime=1544083968，查看告警详情。
	查询统计所涉及的参数及结果，数组类型。示例如下： **说明** Results中最多包含100条告警信息。		

变量	说明	发送内容及告警主题配置示例	告警通知示例

Results	[
	{
	"EndTime": "2021-05-21 18:33:12",
	"EndTimeTs": "1621593192",
	"FireResult": {
	"source": "",
	"time": "1621592292",
	"cnt": "2",
	"status": "403"
	},
	"FireResultAsKv": "[cnt:2,status:403]",
	"LogStore": "nginx-access-log",
	"Query": "status >= 400 | select status, count(*) as cnt group by status",
	"QueryUrl": "",
	"RawResultCount": 2,
	"RawResults": [
	{
	"__source__": "",
	"__time__": "1621592292",
	"cnt": "2",
	"status": "403"
	},
	{
	"__source__": "",
	"__time__": "1621592292",
	"cnt": "1",
	"status": "401"
	}
	],
	"RawResultsAsKv": "[cnt:2,status:403] \n\n[cnt:1,status:401]",
	"StartTime": "2021-05-21 18:18:12",
	"StartTimeTs": "1621592292",
	"Truncated": false
	}
	]
	
	更多信息，请参见告警日志字段。
		第一个查询统计的开始时间为${Results[0].StartTime}，结束时间为${Results[0].EndTime}。
		
		说明 其中0为图表编号。如何获取图表编号，请参见查看图表编号。
			第一个查询统计的开始时间为2021-05-21 18:18:12；结束时间为2021-05-21 18:33:12。

变量	说明	发送内容及告警主题配置示例	告警通知示例

7.2. 告警条件表达式语法

日志服务根据告警条件表达式的执行结果来判断是否产生告警。

在判断告警条件表达式的执行结果时，您查询语句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。

限制说明

告警条件表达式相关限制说明如下所示：

- 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（例如等于）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。
- 表达式长度为1~128个字符。
- 组合求值时最多计算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true时，才会触发告警。例如100+100，计算结果为200，不会触发告警。
- true、false、美元符号（$）和英文句点（.）是保留词，不能作为变量使用。

基础语法

告警条件表达式支持如下语法类型。

语法类型	说明	示例
基础运算符	支持加减乘除、取模运算符，如下所示： +-*/%	• x * 100 + y > 200 • x % 10 > 5
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 • 反斜线（\）需要转义。 • 目前正则表达式支持符合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，格式为'字符串'，例如'string'。	foo == 'string'
布尔常量	支持布尔常量，true、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，例如contains(foo, 'hello')返回true则表示foo中包含hello子串。	contains(foo, 'hello')

多个结果组合求值

- 语法

  支持关联多个查询，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中获取对应的变量值，格式为$N.fieldname，其中N为查询编号，详情请参见如何查看查询编号。目前最多配置三个查询，则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。

- 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求值。例如您配置了三个查询，分别返回了x、y、z条结果，告警条件表达式为$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，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，目前计算次数上限为1000次。

运算方式

> **说明**
>
> - number为64位浮点数类型。
> - string常量需要使用单引号或英文双引号进行包裹，例如'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，例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，且运算结果为布尔值。		
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，且运算结果为布尔值。		
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。		

示例

- 示例1：如果1天（相对）内任务成功率低于90%且延时超过60秒则产生告警，告警表达式如下图所示。

- 示例2：如果15分钟内状态码500出现10次则产生告警，告警表达式如下图所示。

- 示例3：如果1小时内加工速率低于1000条则产生告警，告警表示式如下图所示。

7.3. 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。	0fdd88063a611aa114938f9371daeeb6-1671a52eb23
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

字段名称	说明	示例
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
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，字段说明请参见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
EndTimeTs	查询结束时间，Unix时间戳。注意，实际查询区间为 [StartTime, EndTime) 。	1542334900

字段名称	说明	示例

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格式化的原始查询结果。 **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]

8.最佳实践

8.1. 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，Alert Name，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
}
```

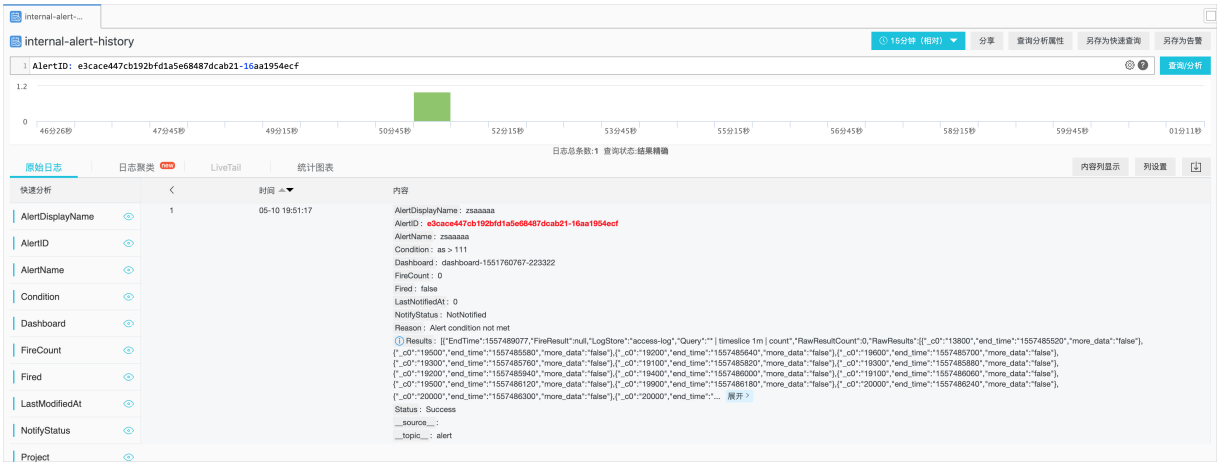

字段解释可以参考告警日志字段。Results中的字段时可以通过如下方式引用：

- 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。

9.FAQ

9.1. 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}`