阿里云
操作审计

最佳实践

文档版本：20190321

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}`*

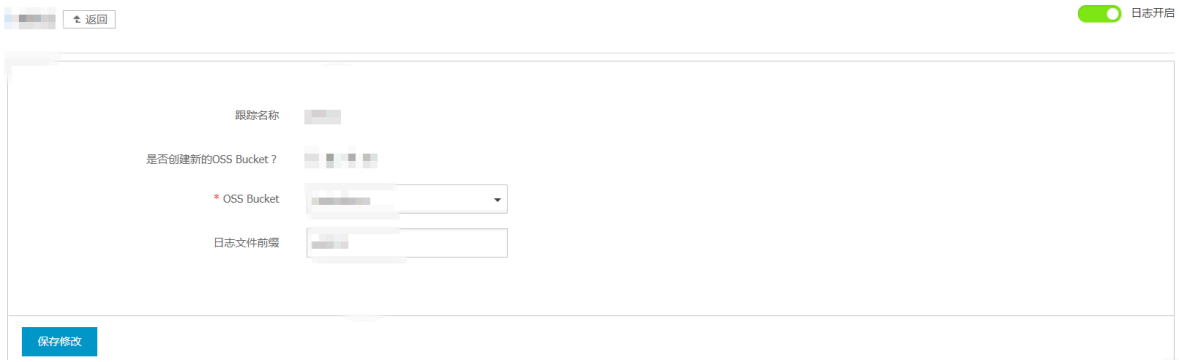
目录

1 如何关闭跟踪的日志记录

创建跟踪时，系统会自动启用日志记录。您可以通过 ActionTrail 控制台关闭跟踪的日志记录。

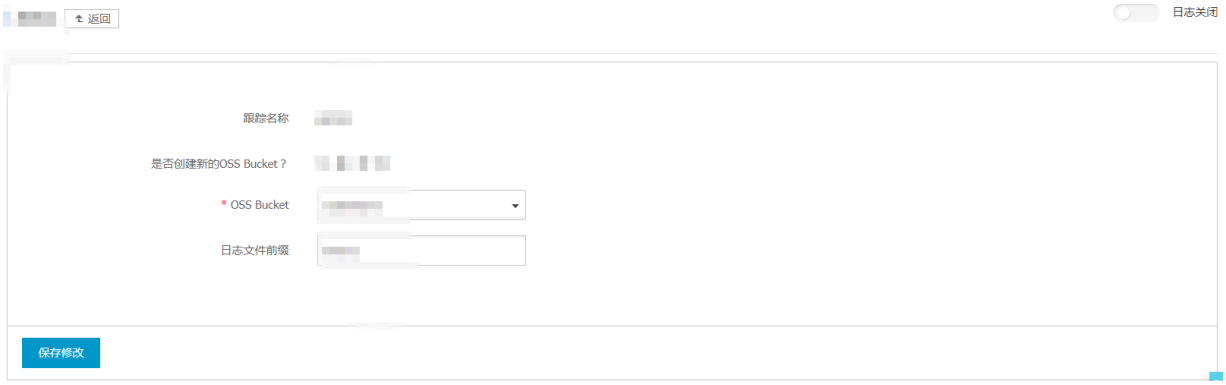
操作步骤

1. 登录*ActionTrail*控制台。
2. 在跟踪列表中，单击要配置的跟踪名称。
3. 在配置页面右上角，向左拖动日志开启滚轮按钮，然后单击保存修改按钮。



预期结果

要恢复该跟踪的日志记录，向右拖动日志关闭滚轮按钮。



2 通过 ActionTrail 监控 AccessKey 的使用

本文将介绍如何通过 ActionTrail 监控 AccessKey 的使用。通过历史事件可以查看近 30 天内 AccessKey 的使用情况。通过配置跟踪，将审计事件投递到日志服务，可以做到对 AccessKey 的监控报警。

查询历史事件

开通 ActionTrail 服务之后，即可查询最近 30 天的审计事件。

1. 登录 *ActionTrail*控制台。
2. 在左侧导航栏，单击历史事件查询。
3. 在过滤器下拉菜单选择 AccessKeyId。
4. 输入您的 AccessKeyId来检索事件。

> 说明:
> 在页面顶端切换区域，可以查询各个区域下 AccessKeyId使用的审计事件。

使用跟踪

通过将审计事件投递到日志服务，ActionTrail 还可以实现对 AccessKey 的监控和报警。

1. 在左侧导航栏，选择跟踪列表。
2. 单击创建跟踪。
3. 选择投递目标为将审计事件投递到日志服务。设置日志服务 Project 区域与日志服务 Project 名称。

> 说明:
> 此处设置的 Project 用于存储 ActionTrail 日志。您可以填写已选择的地域下的 Project 名称，也可以输入一个新的 Project 名称。

4. 打开是否开启日志记录开关。

5. 单击提交，结束配置。

成功新建跟踪任务后，ActionTrail 会将所有地域的审计事件都投递到指定的 Logstore 中。

配置日志服务

日志服务具有丰富的功能，包括数据分析、报表和报警等。下面举例说明如何设置报警。

1. 登录日志服务控制台。
2. 选择所需的项目，单击项目名称。
3. 在Logstore 列表页面，选择所需的日志库并单击查询。
4. 根据需求指定日志库（Logstore）、主题（Topic）和查询语句后，搜索指定日志。

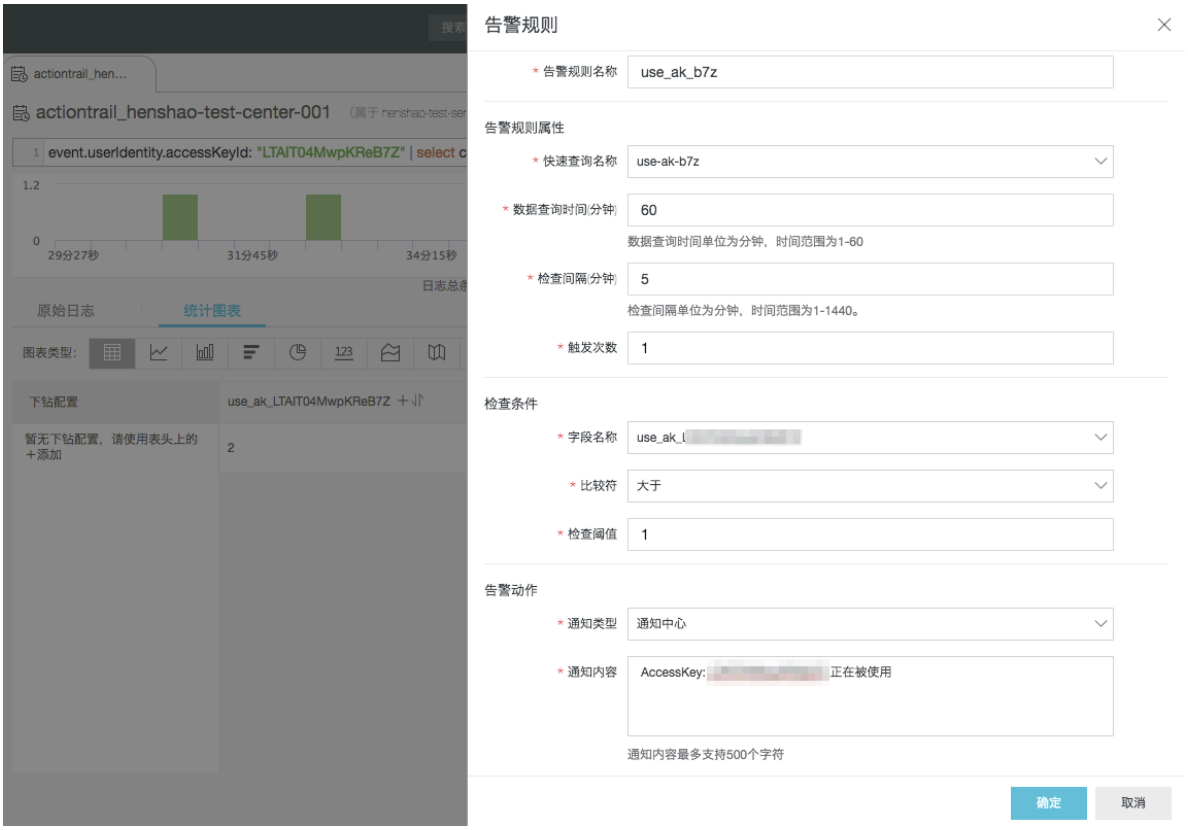
> 说明：
> 单击页面右上角的另存为快速查询，将查询参数保存为快速查询。
>
> 查询语句举例：

```
event.userIdentity.accessKeyId: "LTAI********eB7Z" | select count(1
) as use_ak_LTAI********eB7Z
```

5. 基于快速查询创建报警，单击页面右上角的另存为告警。

> 说明：

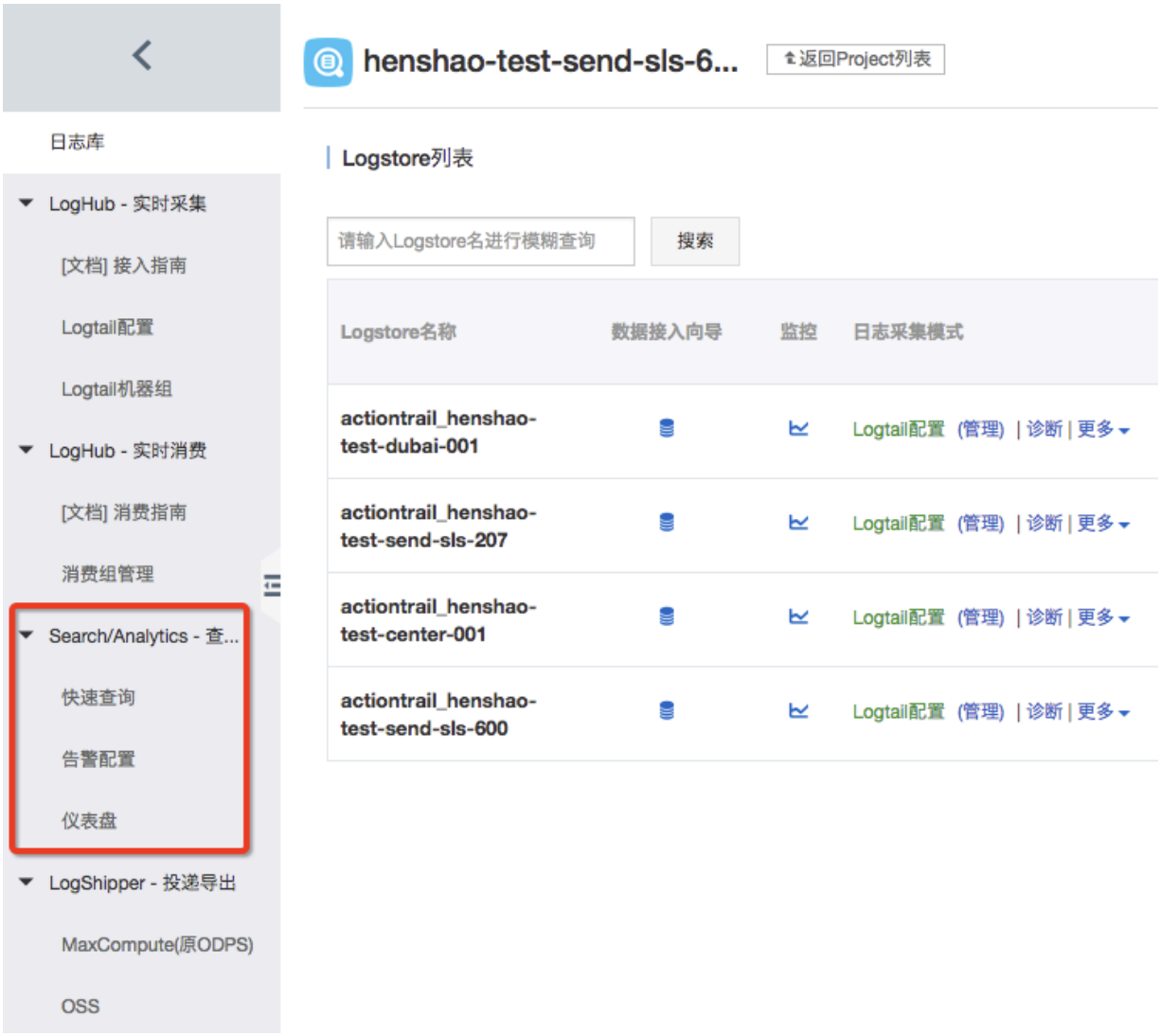
其中检查间隔设置为 5，即每隔 5 分钟检查最近 10 分钟的数据。如果`accessKeyId`（举例如下：LTAIT04MwpKRe****）在十分钟内被用过一次，那么就报警。



收到的报警内容举例如下：

《【阿里云】日志服务告警#账号 *71887**@qq.com*下项目*henshao-test-send-sls-600/*触发器*use_ak_b7z*生效*2 > 1*#内容*AccessKey: LTAI********eB7Z* 正在被使用#上下文*[use_ak_LTAI********eB7Z:2]*》

创建的快速查询和报警均可在项目界面进行查看和管理。



日志服务支持通知中心、短信、钉钉机器人和自定义 WebHook 等多种报警方式，您可以根据自身需求，选择合适的报警方式。详见通知方式。