ALIBABA CLOUD

Alibaba Cloud

操作审计

管理单账号跟踪

文档版本：20201023

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.单账号跟踪概览

您可以通过操作审计控制台创建单账号跟踪。创建单账号跟踪可以持续将操作日志收集到OSS Bucket或SLS Logstore中，以便对操作日志进行分析。如果未创建跟踪，操作审计控制台仅能查看近90天的操作日志。

创建单账号跟踪后，操作事件会以JSON格式保存在OSS Bucket或SLS Logstore中，便于您对操作事件进行查询和分析。单账号跟踪原理如下图所示。

> **说明** 当您使用多个单账号跟踪时，建议您不要将多个单账号跟踪设置为同一个投递地址，这可能造成事件的重复投递和存储空间的浪费。

多个单账号跟踪可以解决以下问题：

- 创建多个单账号跟踪可以将不同的数据投递到不同的存储空间，并授予企业角色相应的权限，从而实现不同角色审计不同范围的操作事件。
- 创建多个单账号跟踪到不同的国家和地域，分别投递到当地的存储空间，可以合规管理多地域的审计数据。
- 为操作事件创建多个副本备份，以免数据的丢失。

操作审计支持多个单账号跟踪后，为避免全局事件的重复记录，会根据以下原则处理全局事件：

- 当您在线查看操作事件时，无论将控制台切换到哪个地域，都可以看到所有的全局事件。
- 当您创建单账号跟踪时将操作事件投递到OSS Bucket后，全局事件默认与Home地域的事件在同一个文件中。

2.创建单账号跟踪

本文为您介绍如何通过操作审计控制台创建单账号跟踪。创建单账号跟踪可以将操作事件投递到对象存储OSS或日志服务SLS，以便对操作事件进行分析。如果未创建跟踪，操作审计控制台仅能查看最近90天的操作事件。

操作步骤

1. 登录操作审计控制台。
2. 在顶部导航栏选择您想创建单账号跟踪的地域。

   > **说明** 该地域将成为单账号跟踪的Home地域，即创建跟踪的地域。

3. 在左侧导航栏，选择**操作审计 > 创建跟踪**。
4. 在**跟踪基本属性**页面，设置如下参数，单击**下一步**。

参数	说明
跟踪名称	跟踪的名称。您需要在阿里云账号中设置唯一的名称。
跟踪的地域	投递跟踪的地域。 ○ **全部地域**：操作审计会投递所有地域的操作事件。 ○ **部分地域**：选择**地域**，操作审计仅投递您选中地域的操作事件。 **说明** Home地域指创建跟踪的地域，跟踪的地域指将哪些地域的操作事件进行投递。如果您只需要投递部分地域的操作事件，建议您将Home地域和跟踪的地域选择为相同地域。
事件类型	阿里云操作事件的类型。 ○ **写事件**：增加、删除或修改云上资源的事件，例如：CreateInstance（创建一台包年包月或者按量付费的ECS实例）。如果您仅导出操作事件进行自定义分析，且只关注会影响云资源的事件，则选择**写事件**。 ○ **读事件**：本身没有在云上增加、删除或修改配置的操作意图，也不会对云上配置造成变更，仅读取云服务资源信息的事件，例如：DescribeInstances（查询一台或多台ECS实例的详细信息）。读事件一般事件量非常大，会占用较多存储空间，不推荐选择。 ○ **所有事件**：读事件和写事件。如果您需要投递阿里云账号下所有操作事件，则选择**所有事件**。

5. 在**审计事件投递**页面，选择投递方式，单击**下一步**。

   > **说明** 目前投递的操作事件范围，是单账号跟踪生效后产生的新事件，不包括原有的最近90天操作事件。后续我们会默认将最近90天的操作事件一次性投递给您，最大限度、最大范围满足您的需求。

   ○ 选择**将事件投递到日志服务SLS**时，设置如下参数。

参数	描述
日志库所属地域	日志项目所在地域。
日志项目名称	日志服务SLS中日志项目的名称。同一账号同一地域下，日志项目名称不能重复。 ■ 当您选中**创建新的日志项目**时，通过操作审计控制台新建日志项目，输入日志项目名称。 在日志服务SLS中新建日志项目的操作方法，请参见快速入门。 ■ 当您选中**选择已有的日志项目**时，在日志服务SLS中选择已有日志项目名称。

- 选择**将事件投递到对象存储OSS时，设置如下参数。**

参数	描述
存储桶名称	对象存储OSS中存储桶的名称。同一账号同一地域下，存储桶名称不能重复。 ■ 当您选中**创建新的存储桶**时，通过操作审计控制台新建存储桶，输入存储桶名称。 在对象存储OSS中新建存储桶的操作方法，请参见创建存储空间。 ■ 当您选中**选择已有的存储桶**时，在对象存储OSS中选择已有存储桶名称。
日志文件前缀	操作事件存放的日志文件前缀。
开启服务端加密	存储桶中的日志文件是否加密。当您选中**创建新的存储桶**时，需要设置该参数。 取值： ■ AES256 ■ KMS ■ 否 说明 关于OSS服务器加密功能，请参见服务器端加密。

6. **在预览并创建页面，确认跟踪信息，单击提交。**

执行结果

创建单账号跟踪后，操作事件会以JSON格式保存在OSS Bucket或SLS Logstore中，便于您对操作事件进行查询和分析。您可以在对象存储OSS或日志服务SLS中查看操作事件：

- 对象存储OSS：您可以通过Elastic MapReduce服务或自行授权第三方日志分析服务来分析此操作事件。

  OSS存储路径格式：

  ```
  oss://<bucket>/<日志文件前缀>/AliyunLogs/Actiontrail/<region>/<年>/<月>/<日>/<日志文件>
  ```

- 日志服务SLS：操作审计会自动创建一个名为 `actiontrail_单账号跟踪名称` 的Logstore，以及操作事件的索引和图表。

  更多详细信息，请参见ActionTrail访问日志。

3.更新单账号跟踪

本文为您介绍如何使用操作审计控制台更新单账号跟踪。

操作步骤

1. 登录操作审计控制台。
2. 在左侧导航栏，选择**操作审计 > 跟踪列表**。
3. 找到需要更新的单账号跟踪，单击跟踪名称。
4. 单击页面右上角**编辑**。
5. 在**跟踪基本属性**页面，更新**跟踪的地域**和**事件类型**，单击**下一步**。
6. 在**审计事件投递**页面，更新投递方式，单击**下一步**。
   - **将事件投递到日志服务SLS**
     - 选择**创建新的日志项目**，更新**日志库所属地域**和**日志项目名称**。
     - 选择**选择已有的日志项目**，更新**日志库所属地域**和**日志项目名称**。
   - **将事件投递到对象存储OSS**
     - 选择**创建新的存储桶**，更新**存储桶名称**、**日志文件前缀**和**开启服务端加密**。
     - 选择**选择已有的存储桶**，更新**存储桶名称**和**日志文件前缀**。
7. 在**预览并创建**页面，确认更新后的跟踪信息，单击**提交**。

4.删除单账号跟踪

本文为您介绍如何使用操作审计控制台删除单账号跟踪。如果要删除来自所有地域的日志文件的单账号跟踪，则必须选择最初创建此单账号跟踪的地域。

操作步骤

1. 登录操作审计控制台。
2. 在左侧导航栏，选择**操作审计 > 跟踪列表**。
3. 找到需要删除的单账号跟踪，单击右侧操作列中的**删除**。
4. 在弹出的**删除**对话框，单击**确认**将此单账号跟踪从跟踪列表中删除。

> 注意 已经投递到OSS Bucket或SLS Logstore中的日志文件将不会被删除。

5.关闭单账号跟踪的跟踪状态

本文介绍如何使用操作审计控制台关闭单账号跟踪的跟踪状态。关闭后，操作审计将停止将操作事件投递到指定的地址，但会保留已有参数配置。

操作步骤

1. 登录操作审计控制台。
2. 在左侧导航栏，选择**操作审计 > 跟踪列表**。
3. 找到需要关闭跟踪状态的单账号跟踪，单击跟踪名称。
4. 关闭**跟踪状态**开关。

   > **说明** 再次单击开关可以开启跟踪状态。

5. 在**关闭跟踪**对话框，单击**确定**。