ALIBABA CLOUD

阿里云

操作审计

平台操作审计

文档版本：20201203

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.平台操作审计概览 05
2.开通平台操作审计 07
3.创建跟踪 08
4.更新跟踪 09
5.删除跟踪 10
6.关闭跟踪状态 11
7.日志字段详情 12

1.平台操作审计概览

操作审计（ActionTrail）联合日志服务推出平台操作审计（Inner-ActionTrail）功能，提供平台操作事件的实时采集、分析、加工、消费等一站式服务，满足您平台操作审计相关的分析与审计需求。本文介绍平台操作审计相关的资产详情、费用说明及使用限制等。

> **说明** 目前，平台操作审计功能支持采集对象存储OSS、云服务器ECS、云数据库RDS、容器服务Kubernetes版ACK、容器镜像服务ACR和E-MapReduce的平台操作事件。

应用场景

- 追踪平台操作事件，查看资产变化原因。
- 近实时查看平台操作事件，进行审计与评估。
- 将平台操作事件存储到自建的数据与计算中心。

功能特性

- 等保合规：存储六个月及以上的平台操作事件，满足等保合规要求。
- 配置简单：轻松配置，实时采集平台操作事件。
- 实时分析：依托日志服务，提供近实时日志分析能力、开箱即用的报表中心，让您对平台操作事件的细节了如指掌。
- 实时告警：支持基于特定指标定制近实时的监测与告警，确保关键业务异常时可及时响应。
- 生态体系：支持对接其他生态系统（例如流计算、云存储、可视化），进一步挖掘数据价值。

资产说明

- 自定义Project和Logstore
  - 该Logstore默认开启索引，并配置部分字段的索引。
  - 该Logstore默认永久存储操作事件，您也可以修改存储时间。具体操作，请参见管理Logstore。

  > **说明** 请勿删除平台操作审计相关的日志服务Project和Logstore，否则无法将操作事件投递到日志服务。

- 专属仪表盘

  默认生成名为 `innertrail_跟踪名称_audit_center_cn` 和 `innertrail_跟踪名称_audit_center_en` 的仪表盘，展示云资源操作的实时动态，包括PV、UV、来源服务数、事件来源分布、PV/UV趋势等内容。

  > **说明** 专属仪表盘可能随时进行升级与更新，建议您不要修改专属仪表盘。您可以自定义创建仪表盘用于查询结果展示。具体操作，请参见创建仪表盘。

费用说明

- 目前，操作审计不针对平台操作审计收取额外费用。
- 操作审计将平台操作事件投递到日志服务后，日志服务根据存储空间、读取流量、请求数量、数据加工和数据投递等进行计费。更多信息，请参见计费概述。

使用限制

- 您需要通过提交工单或向销售经理申请白名单，获取平台操作审计（Inner-ActionTrail）的使用权限。
- 日志服务需处于可用状态（无欠费）。
- 只支持创建1个跟踪。
- 所有平台操作事件只能投递到1个Logstore中。
- 专属Logstore不支持写入其他数据，但在统计、告警、消费等功能上无特殊限制。

2.开通平台操作审计

本文介绍如何开通平台操作审计（Inner-ActionTrail）。

前提条件

- 通过提交工单或向销售经理申请白名单，获取平台操作审计功能（Inner-ActionTrail）的使用权限。
- 授权操作审计使用AliyunActionTrailDefaultRole角色投递操作事件到日志服务SLS中。

  单击云资源访问授权，根据提示完成授权。

  > 说明
  > - 该操作仅在首次配置时需要，且需要由阿里云账号进行授权。
  > - 如果您使用了RAM用户，该RAM用户需具备相关权限。更多信息，请参见RAM用户授权。

操作步骤

1. 登录操作审计控制台。
2. 在左侧导航栏，选择**平台操作审计 > 跟踪列表**，查看平台操作审计（Inner-ActionTrail）相关介绍。

   > 说明
   > - 只有开通了平台操作审计（Inner-ActionTrail）使用权限，才能查看**平台操作审计**。
   > - 平台操作审计（Inner-ActionTrail）开通后，默认生成一个名为 `innertrail_跟踪名称` 的专属Logstore。

后续步骤

您可以创建跟踪，将操作事件投递到日志服务SLS，存储和分析操作事件。更多信息，请参见云产品日志通用操作。

3.创建跟踪

通过创建平台操作审计（Inner-ActionTrail）的跟踪，操作审计会将平台操作事件投递到您指定的日志服务Logstore中，以便您分析平台操作事件。

前提条件

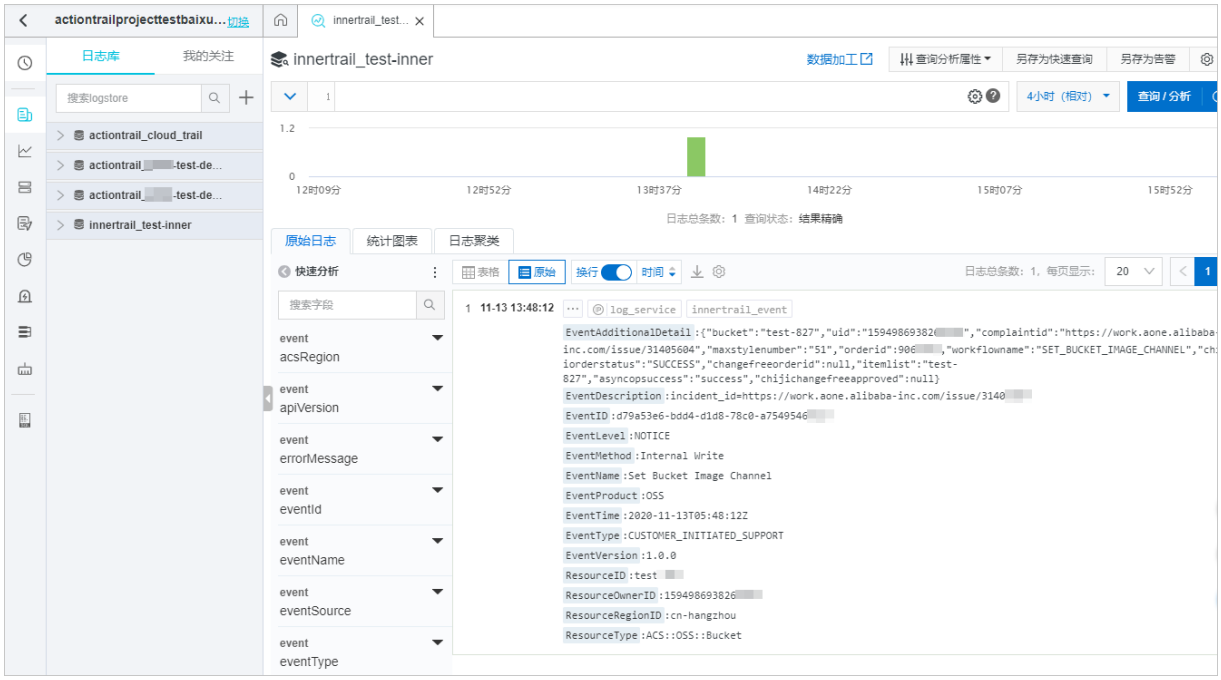
请确保您已开通平台操作审计（Inner-ActionTrail）。具体操作，请参见开通平台操作审计。

操作步骤

1. 登录操作审计控制台。
2. 在左侧导航栏，选择**平台操作审计 > 创建跟踪**。
3. 在**跟踪基本属性**页面，设置**跟踪名称**，单击**下一步**。
4. 在**审计事件投递**页面，勾选**将事件投递到日志服务SLS**，选择日志项目，单击**下一步**。
   - **创建新的日志项目**：选择**日志库所属地域**，设置**日志项目名称**。
   - **选择已有的日志项目**：选择**日志库所属地域**和**日志项目名称**。
5. 在**预览并创建**页面，确认跟踪信息，单击**提交**。

执行结果

操作审计会自动创建一个名为 `innertrail_跟踪名称` 的Logstore，以及平台操作事件的索引和图表。



> **说明** 平台操作事件字段含义，请参见日志字段详情。

4.更新跟踪

本文为您介绍如何更新平台操作审计（Inner-ActionTrail）的跟踪。

操作步骤

1. 登录操作审计控制台。
2. 在左侧导航栏，选择**平台操作审计 > 跟踪列表**。
3. 找到需要更新的跟踪，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**跟踪名称**，单击**下一步**。
6. 在**审计事件投递**页面，勾选**将事件投递到日志服务SLS**，更新日志项目，单击**下一步**。
   - **创建新的日志项目**：选择**日志库所属地域**，设置**日志项目名称**。
   - **选择已有的日志项目**：选择**日志库所属地域**和**日志项目名称**。
7. 在**预览并创建**页面，确认更新后的跟踪信息，单击**提交**。

5.删除跟踪

本文为您介绍如何删除平台操作审计（Inner-ActionTrail）的跟踪。

操作步骤

1. 登录操作审计控制台。
2. 在左侧导航栏，选择**平台操作审计 > 跟踪列表**。
3. 找到需要删除的跟踪，单击右侧操作列中的**删除**。
4. 在弹出的**删除跟踪**对话框，单击**确认**。

> **说明** 已经投递到SLS Logstore中的平台操作事件将不会被删除。

6.关闭跟踪状态

本文介绍如何关闭单账号平台操作审计（Inner-ActionTrail）的跟踪状态。关闭后，操作审计将停止将平台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**平台操作审计 > 跟踪列表**。
3. 找到需要关闭的跟踪，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. 在弹出的**关闭跟踪**对话框，单击**确定**。
6. 在**手机验证**对话框，单击**点击获取**。阿里云会向您绑定的手机发送一个校验码。
7. 输入**校验码**，单击**确认**。

7.日志字段详情

本文为您介绍Inner-ActionTrail日志字段详情。

字段名称	字段说明
EventID	事件ID，事件的唯一标识。
EventVersion	事件定义的版本，固定为1.0.0。
EventProduct	被操作的产品名称，例如OSS。
EventName	云产品使用的API所对应的事件名称。例如Set Bucket Quota Limit。
EventDescription	操作原因，包括工单ID、内部运维/变更单ID、安全扫描操作ID等。
EventType	操作类型，包括： • CUSTOMER_INITIATED_SUPPORT 阿里云内部人员针对用户授权的技术支持操作，例如基于工单问题处理等操作日志。 • ALIYUN_INITIATED_SERVICE 阿里云内部人员或系统基于运维需求所发起的操作，如因集群硬件过保发起的跨集群Bucket迁移。 • ALIYUN_INITIATED_PENALTY 阿里云内部人员或系统基于法律法规要求对用户公开数据进行处置的操作日志。
EventMethod	操作形态，包括正常的读写操作、使用内部接口的读写操作或者其他操作（例如备份恢复）等。
ResourceType	事件归属的资源类型，例如Acs::Oss::Bucket。
ResourceID	资源ID，例如OSS Bucket ID。
ResourceRegionID	发生事件的资源归属的地域ID。
ResourceOwnerID	资源归属的阿里云账号ID。
EventAdditionalDetail	事件的补充，备注详情。
EventTime	操作行为发生的时间（UTC格式），例如2019-09-18T05:23:37Z。
EventLevel	操作对应的客户告知程度，包括： • NOTICE：在日志中记录。 • WARNING：在日志中记录并主动告警客户。