ALIBABA CLOUD

Alibaba Cloud

操作审计

平台操作日志

文档版本：20200917

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.使用前须知

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

> **说明** 目前，平台操作日志功能支持采集对象存储OSS的平台操作日志、云服务器ECS的平台操作日志、云数据库RDS的平台操作日志、容器服务Kubernetes版ACK的平台操作日志和E-MapReduce的平台操作日志。

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默认永久保存日志，您也可以修改日志存储时间，详情请参见管理Logstore。

    > **说明** 请勿删除平台操作日志相关的日志服务Project和Logstore，否则将无法正常采集日志到日志服务。

- 专属仪表盘

  默认生成1个仪表盘。

  > **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，详情请参见创建仪表盘。

仪表盘	说明
innertrail_*跟踪名称*_audit_center_cn	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。

费用说明

- 目前，ActionTrail不针对平台操作日志功能收取额外费用。
- ActionTrail将平台操作日志投递到日志服务后，日志服务根据存储空间、读取流量、请求数量、数据加工、数据投递等进行收费，计费说明请参见日志服务产品定价。

使用限制

- 平台操作日志功能（Inner-ActionTrail）需要您提工单或联系您的销售经理获得使用权限。
- 阿里云日志服务产品需处于可用状态（无欠费）。
- 所有平台操作日志只能投递到1个Logstore中。
- 专属Logstore不支持写入其他数据，但在查询、统计、告警、消费等功能上无特殊限制。
- 不支持修改Logstore的数据存储时长。

功能优势

- 等保合规：存储六个月及以上的平台操作日志，助力产品符合等保合规要求。
- 配置简单：轻松配置即可实时采集平台操作日志。

- 实时分析：依托日志服务产品，提供近实时日志分析能力、开箱即用的报表中心，让您对平台操作日志的分布及细节了如指掌。
- 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。

应用场景

- 追踪平台操作日志，查看资产变化原因。
- 近实时查看平台操作日志，审计与评估。
- 输出日志到自建的数据与计算中心。

2.开通平台操作日志功能

本文介绍如何通过日志服务控制台采集平台操作日志。

前提条件

- 已提工单或联系您的销售经理获得平台操作日志功能（Inner-ActionTrail）使用权限。
- 已授权ActionTrail使用AliyunActionTrailDefaultRole角色投递日志到日志服务中。

  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，且需要由主账号进行授权。
  > - 如果您使用的是RAM用户，该RAM用户需具备相关权限，详情请参见RAM用户授权。
  > - 请勿取消授权或删除RAM角色，否则将导致日志无法正常推送到日志服务。

- 已创建Project和Logstore，详情请参见创建Project和Logstore。

操作步骤

1. 登录日志服务控制台。
2. 在**接入数据区域**，选择**平台操作日志（Inner-ActionTrail）**。

   您也可以登录操作审计控制台，在**平台操作审计 > 跟踪列表**页面中接入平台操作日志。

   > 说明
   > - 如果您是在操作审计控制台开通平台操作日志功能，则默认生成一个名为innertrail_跟踪名称的专属Logstore。
   > - 在日志服务控制台上开通平台操作日志功能后，不会同步到操作审计控制台。如果您已在日志服务控制台中开通，又在操作审计控制台中创建跟踪，则操作审计侧的操作会覆盖日志服务侧的操作。
   > - 如果您在日志服务控制台的**接入数据区域**找不到**平台操作日志（Inner-ActionTrail）**或在操作审计控制台中找不到**平台操作审计 > 跟踪列表**页面，请提工单或联系您的销售经理申请平台操作日志功能（Inner-ActionTrail）使用权限。

3. 在**选择日志空间**页签中，选择目标Project和Logstore，单击**下一步**。 您也可以单击**立即创建**，重新创建Project和Logstore，详情请参见步骤1：创建Project和Logstore。
4. 在**数据源配置**页签中，单击**下一步**。

说明

- 所有平台操作日志只能投递到1个Logstore中。
- 如果您需要关闭平台操作日志功能，可以在**数据源配置**页签中进行关闭。
- 如果您是在操作审计控制台上开通平台操作日志功能，请在操作审计控制台的**平台操作审计 > 跟踪列表**中删除跟踪，即可关闭日志投递。
- 关闭日志投递后，新产生的Inner-ActionTrail日志不再投递到Logstore中，已投递的日志在Logstore存储时间到期后自动删除。

5. 在**查询分析配置**页签中，单击**下一步**。日志服务默认为平台操作日志对应的Logstore开启并配置索引。

后续步骤

日志服务采集到平台操作日志后，您可以执行查询分析、下载、投递、加工日志，创建告警等操作，详情请参见云产品日志通用操作。

3.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。