ALIBABA CLOUD

Alibaba Cloud

操作审计

操作审计公共云合集

文档版本：20210127

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、多账号跟踪和平台事件跟踪的差异

操作审计支持单账号跟踪、多账号跟踪和平台事件跟踪，您可以根据所需进行选择。

单账号跟踪、多账号跟踪和平台事件跟踪的差异如下表所示。

差异项	单账号跟踪	多账号跟踪	平台事件跟踪
场景	个人用户需要投递操作事件到日志服务SLS或对象存储OSS时，可以创建单账号跟踪。 通过创建多个单账号跟踪，可以实现以下需求： • 不同角色审计不同范围的操作事件。 • 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。	企业用户（开通了资源目录的企业）需要将资源目录内的所有成员账号的操作事件投递到日志服务SLS或对象存储OSS时，可以创建多账号跟踪。	个人用户需要将阿里云运维团队针对用户服务的维护操作所产生的事件投递到日志服务SLS时，可以创建平台事件跟踪。
开通方式	阿里云账号登录即可使用，免开通。	当企业开通了资源目录并在资源目录中创建了组织结构后，企业管理账号可以在操作审计中创建多账号跟踪。	提交工单或向销售经理申请白名单。
支持的云服务	支持操作审计的云服务	支持操作审计的云服务	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。
创建跟踪的账号	阿里云账号	企业管理账号	阿里云账号
投递的事件	个人用户通过阿里云控制台、OpenAPI、开发者工具访问和管控云上服务所产生的事件。	企业用户通过阿里云控制台、OpenAPI、开发者工具访问和管控云上服务所产生的事件。	阿里云运维团队针对用户服务的维护操作所产生的事件。
投递事件的范围	当前账号的操作事件	所有成员账号的操作事件	当前账号的平台操作事件
投递事件的存储空间	• 日志服务SLS • 对象存储OSS	• 日志服务SLS • 对象存储OSS	日志服务SLS

差异项	单账号跟踪	多账号跟踪	平台事件跟踪

事件查询方式	• 操作审计控制台
	• LookupEvents 接口
	• 对象存储控制台
	• 日志服务控制台
		• 企业管理账号：
		  ◦ 操作审计控制台
		  ◦ LookupEvents 接口
		• 成员账号：
		  ◦ 对象存储控制台
		  ◦ 日志服务控制台
			• 操作审计控制台
			• 日志服务控制台

创建的最大跟踪数目	每个地域5个	每个地域1个	所有地域共享1个
OSS Bucket存储路径	oss://<bucket>/<日志文件前缀>/AliyunLogs/Actiontrail/regionid/<年>/<月>/<日>/<日志文件>	oss://<bucket>/<日志文件前缀>/AliyunLogs/Actiontrail/rd_id/accountid/regionid/yyyy/mm/dd/日志文件	不涉及
SLS Logstore默认名称	actiontrail_单账号跟踪名称	actiontrail_多账号跟踪名称	innertrail_平台事件跟踪名称

2.管理权限

2.1. 操作审计服务关联角色

本文为您介绍操作审计服务关联角色（AliyunServiceRoleForActionTrail）的应用场景、权限策略、创建及删除操作。

应用场景

操作审计服务关联角色（AliyunServiceRoleForActionTrail）的应用场景如下：

- 访问日志服务SLS（Log Service）

  当您创建跟踪并设置了SLS Project地址用于接收操作日志时，操作审计需要向您指定的SLS Project创建Logstore并写入操作日志，需要通过服务关联角色获取写入SLS Logstore的权限。

- 访问对象存储OSS（Object Storage Service）

  当您创建跟踪并设置了OSS Bucket地址用于接收操作日志时，操作审计需要向您指定的OSS Bucket写入日志文件，需要通过服务关联角色获取写入OSS Bucket的权限。

- 访问消息服务MNS（Message Notification Service）

  当您创建跟踪并设置了OSS Bucket地址用于接收操作日志时，您可以设置当投递发生时向您的MNS主题推送消息。操作审计需向对应默认的MNS主题写入消息事件，需要通过服务关联角色获取通过MNS推送消息的权限。

- 访问资源管理（Resource Management）

  当您通过创建多账号跟踪将整个资源目录所有成员账号的操作日志收集到统一的存储空间时，操作审计需要获取您的资源目录结构和成员账号列表，需要通过服务关联角色获取查看资源目录和成员账号的权限。

关于服务关联角色的更多信息，请参见服务关联角色。

权限说明

角色名称：AliyunServiceRoleForActionTrail。

权限策略：AliyunServiceRolePolicyForActionTrail。

权限说明：操作审计默认使用此角色来访问您的OSS、SLS、MNS、RD等其他云产品资源。

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "oss:ListObjects",
        "oss:PutObject",
        "oss:GetBucketLocation"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
```

```
    {
      "Action": [
        "log:PostLogStoreLogs",
        "log:CreateLogstore",
        "log:GetLogstore"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "mns:PublishMessage"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "resourcemanager:GetResourceDirectory",
        "resourcemanager:ListAccounts",
        "resourcemanager:GetResourceDirectoryAccount"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": "ram:DeleteServiceLinkedRole",
      "Resource": "*",
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "ram:ServiceName": "actiontrail.aliyuncs.com"
        }
      }
    }
  ]
}
```

创建服务关联角色

系统会在以下场景中自动创建服务关联角色（AliyunServiceRoleForActionTrail）：

- 当您调用CreateTrail接口创建跟踪时，如果之前没有创建过服务关联角色，会自动进行创建。
- 当您在操作审计控制台创建跟踪时，如果之前没有创建过服务关联角色，会自动进行创建。

删除服务关联角色

删除服务关联角色前，您需要在操作审计控制台删除所有的跟踪，详情请参见删除单账号跟踪和删除多账号跟踪。

您可以在RAM控制台删除服务关联角色，详情请参见删除RAM角色。

2.2. 对RAM用户进行授权

您可以授权RAM用户访问和管理操作审计，如查询历史事件、管理跟踪等。

前提条件

- 请确保您已创建RAM用户，详情请参见创建RAM用户。
- 请确保您已创建操作审计服务关联角色（AliyunServiceRoleForActionTrail），详情请参见创建服务关联角色。

操作步骤

1. 登录RAM控制台。
2. 在左侧导航栏，单击**人员管理 > 用户**。
3. 在**用户登录名称/显示名称**列表下，找到目标RAM用户。
4. 单击**添加权限**，被授权主体会自动填入。
5. 在**添加权限**页面，选择权限策略。
   - **系统策略**：从**权限策略名称**列表，选择需要的权限。权限详情如下表所示。

权限策略名称	说明
AliyunActionTrailReadOnlyAccess	查看操作审计
AliyunActionTrailFullAccess	管理操作审计
AliyunOSSReadOnlyAccess	查看对象存储
AliyunLogReadOnlyAccess	查询日志服务

   - **自定义策略**：您需要先创建自定义策略，然后从**权限策略名称**列表，选择需要的权限。

     创建自定义策略的详情，请参见创建自定义策略。

     自定义策略代码示例如下：

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "actiontrail:*",
        "oss:GetService",
        "log:ListProject"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}
```

代码中的权限说明如下表所示。

Action	说明
oss:GetService	获取OSS Bucket列表的权限
log:ListProject	获取SLS Project列表的权限
actiontrail:*	操作审计所有操作的权限

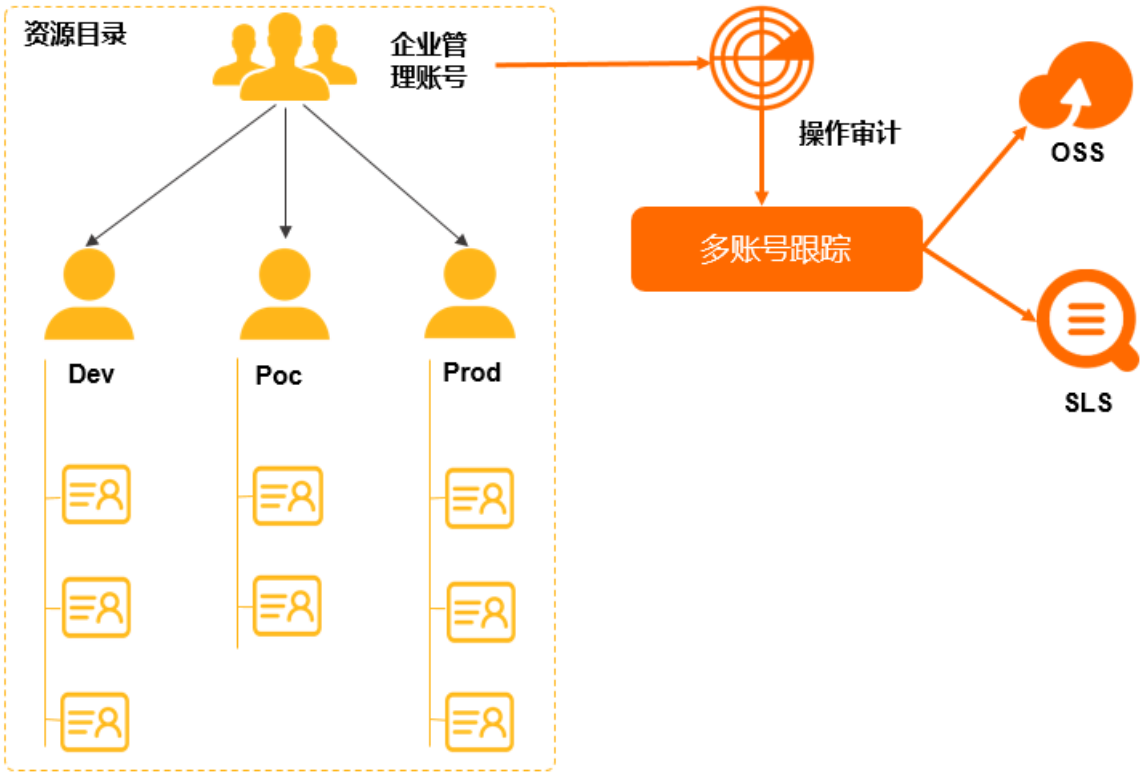
6. 单击**确定**。
7. 单击**完成**。

3.管理多账号跟踪

3.1. 多账号跟踪概览

当企业开通了资源目录后，企业管理账号可以在操作审计中创建多账号跟踪。多账号跟踪将把资源目录内的所有成员账号的操作事件投递到对象存储OSS或日志服务SLS。

多账号跟踪与资源目录的协作原理如下图所示。



基本概念

名词	说明
企业管理账号	企业管理账号是资源目录的超级管理员，也是开通资源目录的初始账号，对其创建的资源目录和成员账号拥有完全控制权限。只有通过企业实名认证的阿里云账号才能开通资源目录，每个资源目录有且只有一个企业管理账号。
成员账号	在资源目录内，成员账号作为资源容器，是一种资源分组单位。成员账号通常用于指代一个项目或应用，每个成员账号中的资源相对其他成员账号中的资源是物理隔离的。 成员账号被企业管理账号邀请进入资源目录，或由企业管理账号在资源目录内直接创建。
多账号跟踪	通过企业管理账号在操作审计控制台创建的跟踪，并且**将跟踪应用到所有成员账号**选择为**是**。多账号跟踪会把所有成员账号的操作事件投递到多账号跟踪设置的OSS Bucket或SLS Logstore中。

名词	说明
单账号跟踪	通过阿里云账号在操作审计控制台创建的跟踪，可用于跟踪和记录当前账号的操作事件。

多账号跟踪和单账号跟踪的区别

跟踪类型	创建账号	投递操作事件范围	操作事件查询方式	创建的最大跟踪数目
单账号跟踪	阿里云账号	当前账号的操作事件	• 操作审计控制台 • `LookupEvents` 接口 • 对象存储控制台 • 日志服务控制台	每个地域5个

多账号跟踪	企业管理账号	所有成员账号的操作事件	• 企业管理账号：
			  ◦ 操作审计控制台
			  ◦ `LookupEvents` 接口
			• 成员账号：
			  ◦ 对象存储控制台
			  ◦ 日志服务控制台
				每个地域1个

资源目录中成员账号的变化

当资源目录中成员账号变更时，操作审计将做如下处理：

- 当新成员账号被邀请进入资源目录，或企业管理账号在指定资源目录中创建新的成员账号时，新成员账号能够在跟踪列表查看多账号跟踪，其操作事件将被自动投递到指定的OSS Bucket或SLS Logstore。
- 当成员账号被从资源目录移除时，该成员账号将无法查看多账号跟踪，并停止将操作事件投递到指定的OSS Bucket或SLS Logstore，但已经投递的操作事件不会自动删除。
- 当成员账号归属的资源目录发生变更时，不会影响操作事件的投递。

3.2. 创建多账号跟踪

本文为您介绍如何通过操作审计控制台创建多账号跟踪。多账号跟踪将把资源目录内所有成员账号的操作事件投递到多账号跟踪中设置的OSS Bucket或SLS Logstore中。

前提条件

您已经开通资源目录，详情请参见开通资源目录。

操作步骤

1. 通过企业管理账号登录操作审计控制台。
2. 在顶部导航栏选择您想创建多账号跟踪的地域。

   > **说明** 该地域将成为多账号跟踪的Home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。行业合规标准建议记录全量操作事件，因此建议选择此选项。 ○ **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。 ○ **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**。

参数	说明
将跟踪应用到所有成员账号	跟踪的应用范围。 ○ **是**：该跟踪为多账号跟踪，将收集企业管理账号和所有成员账号的操作事件，投递到统一的存储空间。多账号跟踪在所有地域均可查看。为避免遗漏事件，建议您选择此选项。 ○ **否**：该跟踪将成为单账号跟踪，仅投递当前账号的操作事件。跟踪仅在可以本账号所在地域查看。 **说明** ○ 此选项一旦选定不可更改。如果创建多账号跟踪后您需要修改**将跟踪应用到所有成员账号**选项，则需要删除多账号跟踪后重新创建。 ○ 创建多账号跟踪后，**跟踪列表**页面中的**创建来源**列将显示**将跟踪应用到所有成员账号**的选择情况。 ■ 若选择**是**，**创建来源**列显示**企业主账号**。 ■ 若选择**否**，**创建来源**列显示**本账号**。

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，是多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。

参数	描述
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

创建多账号跟踪后，操作日志会以JSON格式保存在OSS Bucket或SLS Logstore中。您可以通过企业管理账号在对象存储OSS或日志服务SLS中查看已投递的操作日志。

说明 企业管理账号仅能在对象存储OSS或日志服务SLS中看到资源目录中成员账号的操作事件，不能通过操作审计控制台的**详细事件查询**或 `LookupEvents` 接口查询成员账号的操作事件。

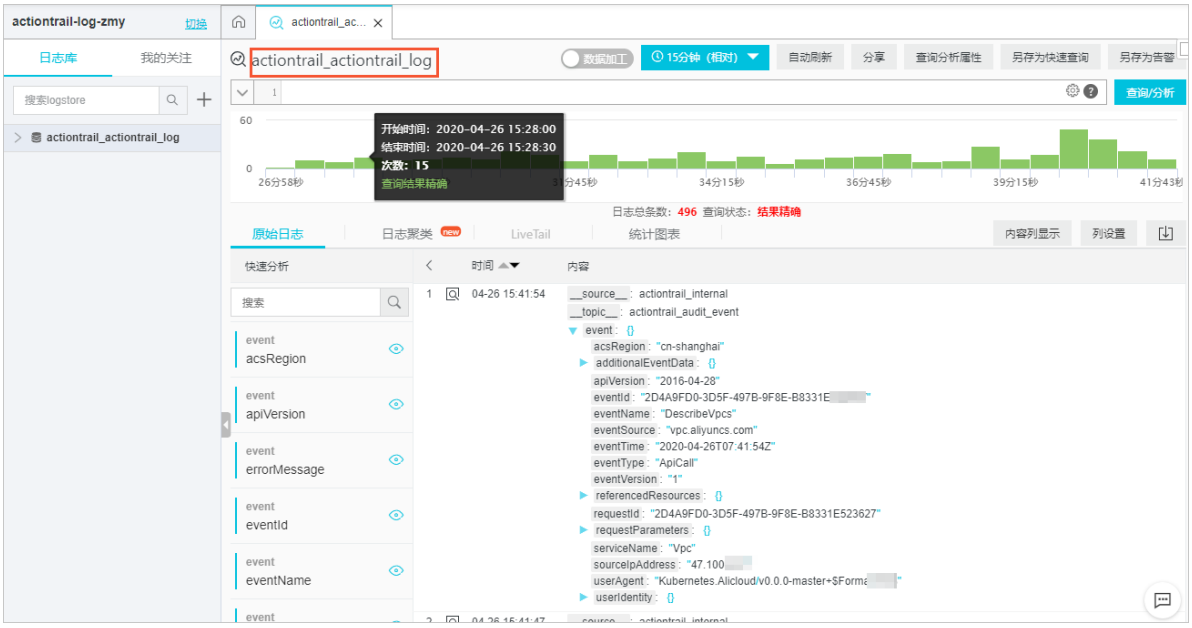
- 对象存储OSS：各成员账号中产生的全局事件，将与Home地域的操作事件放在一起。非全局事件存放在资源归属的地域目录下。您可以通过Elastic MapReduce服务或自行授权第三方日志分析服务来分析此操作事件。

  OSS存储路径格式：

  ```
  oss://<bucket>/<日志文件前缀>/AliyunLogs/Actiontrail/rd_id/accountid/regionid/yyyy/mm/dd/日志文件
  ```

- 日志服务SLS：操作审计会自动创建一个名为 `actiontrail_跟踪名称` 的Logstore以及日志的索引和图表。

  更多详细信息，请参见ActionTrail访问日志。



3.3. 更新多账号跟踪

本文为您介绍如何使用操作审计控制台更新多账号跟踪。

前提条件

您已经开通资源目录，详情请参见开通资源目录。

操作步骤

1. 通过企业管理账号登录操作审计控制台。

   > **说明** 成员账号仅能查看多账号跟踪，无权对多账号跟踪进行更新操作。

2. 在左侧导航栏，选择**操作审计 > 跟踪列表**。
3. 找到需要更新的多账号跟踪，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**。

   > **说明** **将跟踪应用到所有成员账号**选项无法进行更新。如果创建多账号跟踪后您需要更新此选项，则需要删除多账号跟踪后重新创建。

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**。
8. （可选）在弹出的对话框，单击**确认**。

> **说明** 当**将跟踪应用到所有成员账号**选项为是时，需要进行**确认**操作。此时资源目录中所有成员账号的参数设置都将被更新。

3.4. 删除多账号跟踪

本文为您介绍如何使用操作审计控制台删除多账号跟踪。删除后多账号跟踪后，将停止收集资源目录中成员账号的操作事件。

前提条件

您已经开通资源目录，详情请参见开通资源目录。

操作步骤

1. 通过企业管理账号登录操作审计控制台。

> **说明** 成员账号仅能查看多账号跟踪，无权对多账号跟踪进行删除操作。

2. 在顶部导航栏选择创建该多账号跟踪的地域。
3. 在左侧导航栏，选择**操作审计 > 跟踪列表**。
4. 找到需要删除的多账号跟踪，单击右侧操作列中的**删除**。
5. 在弹出的**删除**对话框，单击**确认**将此多账号跟踪从跟踪列表中删除。

> **注意** 已经投递到OSS Bucket或SLS Logstore中的操作事件将不会被删除。

3.5. 关闭多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多账号跟踪的跟踪状态。关闭后，操作审计会停止将资源目录中成员账号的操作事件投递到对象存储OSS或日志服务SLS。

前提条件

您已经开通资源目录，详情请参见开通资源目录。

操作步骤

1. 通过企业管理账号登录操作审计控制台。

> **说明** 成员账号仅能查看多账号跟踪，无权对多账号跟踪进行关闭跟踪状态操作。

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多账号跟踪，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**。

4.管理历史事件投递任务

4.1. 创建历史事件投递任务

当您需要分析最近90天的历史事件，或者因审计要求需要下载最近90天的历史事件时，您可以创建任历史事件投递任务，将历史事件投递到日志服务SLS。

前提条件

- 通过提交工单或向销售经理申请白名单，获取历史事件投递任务功能的使用权限。
- 请确保您已经在当前地域创建了跟踪。具体操作，请参见创建单账号跟踪。

使用限制

- 目前只支持为单账号跟踪投递历史事件。
- 目前只支持将历史事件投递到日志服务SLS。
- 一个阿里云账号同时只能存在一个正在运行的历史事件投递任务。

操作步骤

1. 登录操作审计控制台。
2. 在顶部导航栏选择您需要投递历史事件的地域。

   > **说明** 该地域必须与跟踪所在地域相同。

3. 在左侧导航栏，单击**历史事件投递任务**。
4. 在**历史事件投递任务**页面，单击**创建任务**。
5. 在**创建任务**页面，选择跟踪。

   > **说明** 选择跟踪后，系统将自动填入跟踪的地域、日志项目地域、日志项目名称和日志库信息。

6. 单击**确定**。创建任务后，您可以在**历史事件投递任务**页面查看关联跟踪、可补历史事件范围、投递状态、任务创建时间、任务完成时间等信息。

   > **说明**
   >
   > - 补投递的历史事件与关联跟踪的地域和事件类型保持一致。例如：您创建跟踪A时将跟踪的地域设置为华东1（杭州）、事件类型设置为写事件，历史事件投递任务将通过跟踪A向您指定的存储空间，补投递最近90天在华东1（杭州）地域的写事件。
   > - 补投递的历史事件时间范围的开始时间为当前时间往前90天，结束时间为关联跟踪生效后5分钟。例如：您创建历史事件投递任务时关联跟踪A已经创建了40天，历史事件投递任务将投递跟踪A创建时间往前50天的历史事件。

5.API参考

5.1. API概览

请根据使用场景选择对应的API。

场景	描述	API版本选择	API区别
跟踪管理	管理用户跟踪	2017-12-04	无
历史事件查询	查询最近90天历史事件	• 2020-07-06（推荐） • 2017-12-04	• 2020-07-06版本API查询延时低，支持90天范围内的事件查询，支持使用单个条件筛选事件。 • 2017-12-04版本API查询延时高，支持30天范围内的事件查询，支持8个条件组合筛选事件。

说明 2020-07-06版本API为最新版本，目前暂不支持跟踪相关接口，后续将逐渐支持。在进行历史事件查询时，推荐您使用2020-07-06版本API。

5.2. 附录

5.2.1. 通过VPC调用API

如果专有网络（VPC）内的ECS实例没有设置公网IP，则您无法通过公网调用API，但您可以通过VPC调用API。

接入地址

您可以使用下表所示的接入地址，通过VPC调用API。调用时只能操作同地域资源，不支持跨地域操作。

阿里云地域	地域ID	接入地址（Endpoint）
华东 1（杭州）	cn-hangzhou	actiontrail-vpc.cn-hangzhou.aliyuncs.com
华东 2（上海）	cn-shanghai	actiontrail-vpc.cn-shanghai.aliyuncs.com
华北 1（青岛）	cn-qingdao	actiontrail-vpc.cn-qingdao.aliyuncs.com
华北 2（北京）	cn-beijing	actiontrail-vpc.cn-beijing.aliyuncs.com
华北 3（张家口）	cn-zhangjiakou	actiontrail-vpc.cn-zhangjiakou.aliyuncs.com

阿里云地域	地域ID	接入地址（Endpoint）
华北 5（呼和浩特）	cn-huhehaote	actiontrail-vpc.cn-huhehaote.aliyuncs.com
华南 1（深圳）	cn-shenzhen	actiontrail-vpc.cn-shenzhen.aliyuncs.com
华南 2（河源）	cn-heyuan	actiontrail-vpc.cn-heyuan.aliyuncs.com
华南 3（广州）	cn-guangzhou	actiontrail-vpc.cn-guangzhou.aliyuncs.com
西南 1（成都）	cn-chengdu	actiontrail-vpc.cn-chengdu.aliyuncs.com
中国（香港）	cn-hongkong	actiontrail-vpc.cn-hongkong.aliyuncs.com
新加坡	ap-southeast-1	actiontrail-vpc.ap-southeast-1.aliyuncs.com
澳大利亚（悉尼）	ap-southeast-2	actiontrail-vpc.ap-southeast-2.aliyuncs.com
马来西亚（吉隆坡）	ap-southeast-3	actiontrail-vpc.ap-southeast-3.aliyuncs.com
印度尼西亚（雅加达）	ap-southeast-5	actiontrail-vpc.ap-southeast-5.aliyuncs.com
日本（东京）	ap-northeast-1	actiontrail-vpc.ap-northeast-1.aliyuncs.com
德国（法兰克福）	eu-central-1	actiontrail-vpc.eu-central-1.aliyuncs.com
英国（伦敦）	eu-west-1	actiontrail-vpc.eu-west-1.aliyuncs.com
美国（硅谷）	us-west-1	actiontrail-vpc.us-west-1.aliyuncs.com
美国（弗吉尼亚）	us-east-1	actiontrail-vpc.us-east-1.aliyuncs.com
印度（孟买）	ap-south-1	actiontrail-vpc.ap-south-1.aliyuncs.com
阿联酋（迪拜）	me-east-1	actiontrail-vpc.me-east-1.aliyuncs.com

方式一（推荐）：通过SDK调用API

Java SDK核心库在4.5.3版本以后，支持通过VPC调用API。Java代码示例如下：

```
DefaultProfile profile = DefaultProfile.getProfile("<RegionId>", "<AccessKeyId>", "<AccessKeySecret>");
IAcsClient client = new DefaultAcsClient(profile);
// 全局生效配置。其中，<product>为产品名称，操作审计取值为Actiontrail。
DefaultProfile.addEndpoint("<RegionId>", "<product>", "<Endpoint>");
// 只对当前请求生效配置。例如：调用DescribeRegions接口。
DescribeRegionsRequest regionsRequest = new DescribeRegionsRequest();
// 如设置下述productNetwork参数，则无需手动设置SysEndpoint。
regionsRequest.setSysEndpoint("<Endpoint>");
// 设置网络。productNetwork参数取值：vpc、 public。
// vpc为内网调用接入地址选项；public为公网调用API的选项，即默认选项。
regionsRequest.productNetwork = "vpc";
DescribeRegionsResponse regionsResponse = client.getAcsResponse(regionsRequest);
```

方式二：通过阿里云CLI调用API

以DescribeRegions接口为例，调用命令示例如下：

```
aliyun actiontrail DescribeRegions --endpoint actiontrail-vpc.cn-hangzhou.aliyuncs.com
```