

# 阿里云 操作审计

API参考

文档版本：20181105

# 法律声明

---

阿里云提醒您在使用或阅读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。	 <b>禁止：</b> 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。	 <b>警告：</b> 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。	 <b>说明：</b> 您也可以通过按 <b>Ctrl + A</b> 选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
<b>粗体</b>	表示按键、菜单、页面名称等UI元素。	单击 <b>确定</b> 。
<code>courier</code> 字体	命令。	执行 <code>cd /d C:/windows</code> 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	<code>bae log list --instanceid Instance_ID</code>
[ ]或者[a b]	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
{ }或者{a b}	表示必选项，至多选择一个。	<code>swich {stand   slave}</code>

# 目录

---

法律声明.....	I
通用约定.....	I
<b>1 调用方式.....</b>	<b>1</b>
1.1 调用方式.....	1
<b>2 实例相关接口.....</b>	<b>2</b>
2.1 CreateTrail.....	2
2.2 DescribeTrails.....	5
2.3 GetTrailStatus.....	7
2.4 StartLogging.....	8
2.5 StopLogging.....	9
2.6 UpdateTrail.....	10
2.7 DeleteTrail.....	13
<b>3 查询相关接口.....</b>	<b>15</b>
3.1 LookupEvents.....	15
3.2 DescribeRegions.....	18

# 1 调用方式

---

## 1.1 调用方式

对 API 接口调用是通过向 API 的服务端地址发送 HTTP 或 HTTPS GET 请求来实现的。根据请求的处理情况，系统会返回处理结果。

具体实现方式如下：

1. [请求结构](#)
2. [公共参数](#)
3. [返回结果](#)
4. [签名机制](#)

## 2 实例相关接口

### 2.1 CreateTrail

创建跟踪，您可以根据需要选择合适的投递目标，创建的跟踪可以投递到日志服务或者 OSS bucket，优先推荐投递到日志服务中。

请求参数

名称	类型	是否必须	描述
Action	String	是	操作接口名 CreateTrail。
RegionId	String	是	实例所属的地域 ID。 查看最新的阿里云地域列表，请参考： <a href="#">DescribeRegions</a> 。
Name	String	是	创建的跟踪名称。同一个账户内跟踪名称不可重复。
OssBucketName	String	是	跟踪写入的 OSS bucket。创建跟踪时必须保证该 bucket 已经存在。
RoleName	String	是	用户允许 ActionTrail 服务扮演的 RAM 角色名称。
OssKeyPrefix	String	否	写入的 OSS bucket 文件名的前缀，可为空。
SlsProjectArn	String	否	日志服务项目的阿里云唯一标识符 ( Aliyun Resource Name, ARN )。详情请参考： <a href="#">相关术语</a> 。
SlsWriteRoleArn	String	否	日志服务角色的阿里云唯一标识符 ( Aliyun Resource Name,

名称	类型	是否必须	描述
			ARN )。详情请参考： <a href="#">相关术语</a> 。

## 返回参数

公共返回参数，详见[公共参数](#)。

名称	类型	描述
Name	String	跟踪名称。
HomeRegion	String	跟踪的 home region。
OssBucketName	String	用户指定的 OSS bucket。
OssKeyPrefix	String	用户指定的 OSS 文件名的前缀。
RoleName	String	用户指定的角色名称。
SlsProjectArn	String	日志服务项目的阿里云唯一标识符 ( Aliyun Resource Name, ARN )。详情请参考： <a href="#">相关术语</a> 。
SlsProjectArn	String	日志服务角色的阿里云唯一标识符 ( Aliyun Resource Name, ARN )。详情请参考： <a href="#">相关术语</a> 。

## 需要的权限

### Action

actiontrail:CreateTrail

### Resource

acs:actiontrail:\${region}:\${AccountId}:\*

## 错误码

错误代码	描述	HTTP 状态码
InvalidBucketNameException	非法的 bucket 名称。	400
InvalidPrefixException	非法的前缀。	400

错误代码	描述	HTTP 状态码
InvalidTrailNameException	非法的跟踪名称。	400
TrailAlreadyExistsException	该区域已存在指定的跟踪名称。	400
InsufficientBucketPolicyException	没有权限访问指定的 OSS bucket。	403
MaximumNumberOfTrailsExceededException	超过了在该区域允许创建跟踪的数量。	403
BucketDoesNotExistException	bucket 不存在。	404

## 示例

### 请求示例

```
http://actiontrail.cn-hangzhou.aliyuncs.com/?
Action=CreateTrail
&RegionId=cn-hangzhou
&Name=trail-test
OssBucketName=yuanchuang
&RoleName=aliyunactiontraildefaultrole
&OssKeyPrefix=
&<公共请求参数>
```

### 返回示例

#### JSON示例

```
{
  "Name": "trail-test",
  "OssBucketName": "yuanchuang",
  "OssKeyPrefix": "",
  "RoleName": "aliyunactiontraildefaultrole",
  "SlsProjectArn": "acs:log:cn-shanghai::project/**",
  "SlsWriteRoleArn": "acs:ram::**:*:role/aliyunactiontraildefaultrole"
```

}

## 2.2 DescribeTrails

查询当前区域跟踪的设置信息。

请求参数

名称	类型	是否必须	描述
Action	String	是	操作接口名，系统规定参数，取值： <code>DescribeTrails</code> 。
RegionId	String	是	实例所属的地域 ID。查看最新的阿里云地域列表，请参考： <a href="#">DescribeRegions</a> 。
NameList	String	否	需要查询的跟踪名称列表，以逗号分隔。
IncludeShadowTrails	String	否	是否显示影子跟踪。取值为true或false，默认为否。

返回参数

返回参数TrailList中包含的字段见下表。

名称	类型	描述
Name	String	跟踪名称。
OssBucketName	String	OSS bucket 名称。
OssBucketLocation	String	OSS bucket 所在的区域。
OssKeyPrefix	String	OSS bucket 名称前缀。
RoleName	String	ActionTrail 的角色名称。
SlsProjectArn	String	日志服务项目的阿里云唯一标识符 ( Aliyun Resource Name, ARN )。详情请参考： <a href="#">相关术语</a> 。
SlsWriteRoleArn	String	日志服务角色的阿里云唯一标识符 ( Aliyun Resource Name,

名称	类型	描述
		ARN )。详情请参考： <a href="#">相关术语</a> 。

## 需要的权限

### Action

```
actiontrail:DescribeTrails
```

### Resource

```
acs:actiontrail:${region}:${AccountId}:*
```

## 错误码

无。

## 示例

### 请求示例

```
http://actiontrail.cn-hangzhou.aliyuncs.com/?
Action=DescribeTrails
&RegionId=cn-hangzhou
&NameList=abc%2cdef
&<公共请求参数>
```

### 返回示例

#### JSON示例

```
{
  "TrailList": [
    {
      "Name": "default",
      "OssBucketName": "secloud",
      "OssBucketLocation": "cn-hangzhou",
      "OssKeyPrefix": "trail1",
      "RoleName": "aliyunactiontraildefaultrole",
      "SlsProjectArn": "acs:log:cn-shanghai::project/**",
      "SlsWriteRoleArn": "acs:ram::***:role/aliyunactiontraildef
aultrole"
    }
  ]
}
```

```
}
```

## 2.3 GetTrailStatus

查询跟踪的工作状态。

请求参数

名称	类型	是否必须	描述
Action	String	是	操作接口名，系统规定参数，取值： <code>GetTrailStatus</code> 。
RegionId	String	是	实例所属的地域 ID。查看最新的阿里云地域列表，请参考： <a href="#">DescribeRegions</a> 。
Name	String	是	跟踪名称，同一账户内名称不可重复。

返回参数

公共返回参数，详见[公共参数](#)。

名称	类型	描述
IsLogging	Boolean	服务是否打开。
LatestDeliveryError	String	最后一次行为追踪异常的日志信息。
LatestDeliveryTime	String	最后一次成功记录行为的时间。
StartLoggingTime	String	用户上一次开启该跟踪的时间。
StopLoggingTime	String	用户上一次停止该跟踪的时间。

需要的权限

### Action

`actiontrail:GetTrailStatus`

**Resource**

```
acs:actiontrail:${region}:${AccountId}:*
```

## 错误码

错误代码	描述	HTTP 状态码
InvalidTrailNameException	指定的跟踪名称不存在。	400
TrailNotFoundException	找不到指定的跟踪。	404

## 示例

## 请求示例

```
http://actiontrail.cn-hangzhou.aliyuncs.com/?
Action=GetTrailStatus
&RegionId=cn-hangzhou
&Name=trail-test
&<公共请求参数>
```

## 返回示例

## JSON示例

```
{
  "IsLogging": true,
  "StartLoggingTime": "Wed Dec 02 15:41:06 CST 2015"
}
```

**2.4 StartLogging**

启用跟踪。

## 请求参数

名称	类型	是否必须	描述
Action	String	是	操作接口名，系统规定参数，取值：StartLogging。
RegionId	String	是	实例所属的地域 ID。查看最新的阿里云地域列表，请参考： <a href="#">DescribeRegions</a> 。
Name	String	是	要启用的跟踪的名称。

## 返回参数

无。

## 需要的权限

### Action

```
actiontrail:StartLogging
```

### Resource

```
acs:actiontrail:${region}:${AccountId}:*
```

## 错误码

错误代码	描述	HTTP 状态码
InvalidBucketNameException	非法的bucket名称。	400
TrailNotFoundException	要启用的跟踪不存在。	404

## 示例

### 请求示例

```
http://actiontrail.cn-hangzhou.aliyuncs.com/?
Action=StartLogging
&RegionId=cn-hangzhou
&Name=trail-test
&<公共请求参数>
```

## 2.5 StopLogging

禁用跟踪。

### 请求参数

名称	类型	是否必须	描述
Action	String	是	操作接口名，系统规定参数，取值：StopLogging。
RegionId	String	是	实例所属的地域 ID。查看最新的阿里云地域列表，请参考： <a href="#">DescribeRegions</a> 。

名称	类型	是否必须	描述
Name	String	是	要禁用的跟踪名。

#### 返回参数

无。

#### 错误码

错误代码	描述	HTTP 状态码
InvalidBucketNameException	非法的 bucket 名称。	400
TrailNotFoundException	要禁用的跟踪不存在。	404

#### 需要的权限

##### Action

actiontrail:StopLogging

##### Resource

acs:actiontrail:\${region}:\${AccountId}:\*

#### 示例

##### 请求示例

```
http://actiontrail.cn-hangzhou.aliyuncs.com/?
Action=StopLogging
&RegionId=cn-hangzhou
&Name=trail-test
&<公共请求参数>
```

## 2.6 UpdateTrail

更新跟踪可以写入日志服务logstore或者 OSS bucket，该操作必须调用跟踪的 Home Region 的 API 服务器。

#### 请求参数

名称	类型	是否必须	描述
Action	String	是	操作接口名，系统规定参数，取值：UpdateTrail。

名称	类型	是否必须	描述
RegionId	String	是	实例所属的地域 ID。 查看最新的阿里云地域列表，请参考： <a href="#">DescribeRegions</a> 。
Name	String	是	要更新的跟踪的名字。
OssBucketName	String	否	写入的 OSS bucket 名称。该 bucket 必须已经存在。
RoleName	String	否	用户允许 ActionTrail 服务扮演的 RAM 角色名称。
OssKeyPrefix	String	否	写入的 OSS bucket 文件名的前缀，可为空。
SlsProjectArn	String	否	日志服务项目的阿里云唯一标识符 ( Aliyun Resource Name, ARN )。详情请参考： <a href="#">相关术语</a> 。
SlsWriteRoleArn	String	否	日志服务角色的阿里云唯一标识符 ( Aliyun Resource Name, ARN )。详情请参考： <a href="#">相关术语</a> 。

## 返回参数

公共返回参数，详见[公共参数](#)。

名称	类型	描述
Name	String	跟踪名称。
HomeRegion	String	跟踪的 home region。
OssBucketName	String	OSS bucket 名称。
OssKeyPrefix	String	OSS bucket 文件名的前缀。
RoleName	String	角色名称。

名称	类型	描述
SlsProjectArn	String	日志服务项目的阿里云唯一标识符 ( Aliyun Resource Name, ARN )。详情请参考： <a href="#">相关术语</a> 。
SlsWriteRoleArn	String	日志服务角色的阿里云唯一标识符 ( Aliyun Resource Name, ARN )。详情请参考： <a href="#">相关术语</a> 。

### 需要的权限

#### Action

```
actiontrail:UpdateTrail
```

#### Resource

```
acs:actiontrail:${region}:${AccountId}:*
```

### 错误码

错误代码	描述	HTTP 状态码
InvalidBucketNameException	非法的 bucket 名称。	400
InvalidPrefixException	非法的前缀。	400
InvalidTrailNameException	非法的跟踪名称。	400
InsufficientBucketPolicyException	没有权限访问指定的 OSS bucket。	403
BucketDoesNotExistException	指定的 bucket 不存在。	404
TrailNotFoundException	指定的跟踪不存在。	404

### 示例

#### 请求示例

```
http://actiontrail.cn-hangzhou.aliyuncs.com/?
Action=UpdateTrail
&RegionId=cn-hangzhou
&Name=trail-test
&OssBucketName=yuanchuang
&RoleName=aliyunactiontraildefaultrole
&OssKeyPrefix=
```

&<公共请求参数>

返回示例

JSON示例

```
{
  "Name": "trail-test",
  "OssBucketName": "yuanchuang",
  "OssKeyPrefix": "",
  "RoleName": "aliyunactiontraildefaultrole",
  "SlsProjectArn": "acs:log:cn-shanghai::project/**",
  "SlsWriteRoleArn": "acs:ram::***:role/aliyunactiontraildefaultrole"
}
```

## 2.7 DeleteTrail

删除跟踪。

请求参数

名称	类型	是否必须	描述
Action	String	是	操作接口名，系统规定参数，取值：DeleteTrail。
RegionId	String	是	实例所属的地域 ID。查看最新的阿里云地域列表，请参考： <a href="#">DescribeRegions</a> 。
Name	String	是	要删除的跟踪的名称。

返回参数

无。

需要的权限

### Action

actiontrail:DeleteTrail

### Resource

acs:actiontrail:\${region}:\${AccountId}:\*

## 错误码

错误代码	描述	HTTP 状态码
InvalidTrailNameException	非法的跟踪名称。	400
TrailNotFoundException	指定的跟踪不存在。	404

## 示例

### 请求示例

```
http://actiontrail.cn-hangzhou.aliyuncs.com/?  
Action=DeleteTrail  
&RegionId=cn-hangzhou  
&Name=my-test  
&<公共请求参数>
```

## 3 查询相关接口

### 3.1 LookupEvents

检索事件。

请求参数

名称	类型	是否必须	描述
Action	String	是	操作接口名，系统规定参数，取值： <code>LookupEvents</code> 。
RegionId	String	是	实例所属的地域 ID。查看最新的阿里云地域列表，请参考： <a href="#">DescribeRegions</a> 。
Event	String	否	要检索的事件 ID。
Request	String	否	要检索的请求 ID。
EventType	String	否	要检索的事件类型，比如 <code>ApiCall</code> 。
ServiceName	String	否	要检索的云服务名，比如 <code>Ecs</code> 。
EventName	String	否	要检索的事件名，比如 <code>CreateInstance</code> 。
User	String	否	要检索的调用者名，RAM 账号。
ResourceType	String	否	要检索的资源类型，比如 <code>Database</code> 。
ResourceName	String	否	要检索的资源名，比如 RDS 的 <code>rdsxxxxxxx</code> 。
NextToken	String	否	用于请求下一页检索结果。请求参数必须保证和上次请求一致。

名称	类型	是否必须	描述
MaxResults	Integer	否	允许返回的最大结果数目。取值范围在 0 到 50 之间。
StartTime	String	否	<p>检索事件的开始时间戳。</p> <ul style="list-style-type: none"> <li>支持最多检索最近 7 天的事件。</li> <li>默认值是 7 天。</li> <li>日期格式按照ISO8601 标准表示，并使用 UTC 时间。格式为YYYY-MM-DDThh:mm:ssZ。例如，2014-05-26T12:00:00Z (北京时间 2014 年 5 月 27 日 00:00:00)。</li> </ul>
EndTime	String	否	<p>检索事件的结束时间戳。- 支持最多检索最近 7 天的事件。</p> <ul style="list-style-type: none"> <li>默认值是 7 天。</li> <li>日期格式按照ISO8601 标准表示，并使用 UTC 时间。格式为YYYY-MM-DDThh:mm:ssZ。例如，2014-05-26T12:00:00Z (北京时间 2014 年 5 月 27 日 00:00:00)。</li> </ul>

## 返回参数

公共返回参数，详见[公共参数](#)。

名称	类型	描述
Events	String	检索到的事件列表。
NextToken	String	返回下一页的检索结果。无更多结果则不返回此字段。 )
StartTime	String	检索到的事件的开始时间。
EndTime	String	检索到的事件的结束时间。

### 需要的权限

#### Action

actiontrail:LookupEvents

#### Resource

acs:actiontrail:\${region}:\${AccountId}:\*

### 错误码

错误代码	描述	HTTP 状态码
InvalidTimeRangeException	检索结束时间早于开始时间。	400
InvalidParameterValue	参数值错误。	400

### 示例

#### 请求示例

```
http://actiontrail.cn-hangzhou.aliyuncs.com/?
Action=LookupEvents
&RegionId=cn-hangzhou
&<公共请求参数>
```

#### 返回示例

##### JSON示例

```
{
  "EndTime": "2016-01-12T09:11:06Z",
  "Events": [],
  "StartTime": "2016-01-05T09:11:36Z"
```

}

## 3.2 DescribeRegions

查询您可以使用的阿里云地域。更多详情，请参阅 [地域与可用区](#)。

### 请求参数

名称	类型	是否必需	描述
Action	String	是	系统规定参数。取值： DescribeRegions
RegionId	String	是	实例所属的地域 ID。

### 返回参数

返回参数 Region 列表包含字段见下表：

名称	类型	描述
RegionId	String	地域 ID
LocalName	String	地域名称
RegionEndpoint	String	地域对应的接入地址 (Endpoint)

### 示例

#### 请求示例

```
https://ecs.cn-hangzhou.aliyuncs.com/?
Action=DescribeRegions
&RegionId=cn-hangzhou
&<公共请求参数>
```

#### 返回示例

#### XML格式

```
<DescribeRegionsResponse>
  <RequestId>38EC7366-F5A9-46B1-BDB1-0FDC2E296397</RequestId>
  <Regions>
    <Region>
      <RegionId>cn-shanghai</RegionId>
    </Region>
    <Region>
      <RegionId>cn-qingdao</RegionId>
    </Region>
  </Regions>
```

```
</DescribeRegionsResponse>
```

#### JSON 格式

```
{
  "RequestId": "38EC7366-F5A9-46B1-BDB1-0FDC2E296397",
  "Regions": {
    "Region": [
      {
        "RegionId": "cn-shanghai",
      },
      {
        "RegionId": "cn-qingdao",
      }
    ]
  }
}
```

#### 错误码

无。