

# 操作审计 快速入门



腾讯云

**【 版权声明 】**

©2013–2025 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

**【 商标声明 】**

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

**【 服务声明 】**

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。

您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

**【 联系我们 】**

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或95716。

# 快速入门

最近更新时间：2024-09-18 10:15:01

您可以通过腾讯云控制台快速了解操作审计服务。通过控制台，您可以查看操作记录，创建一个跟踪集并编辑其存储位置，还可以对已创建的跟踪集进行删除操作，以及关闭跟踪集记录日志。

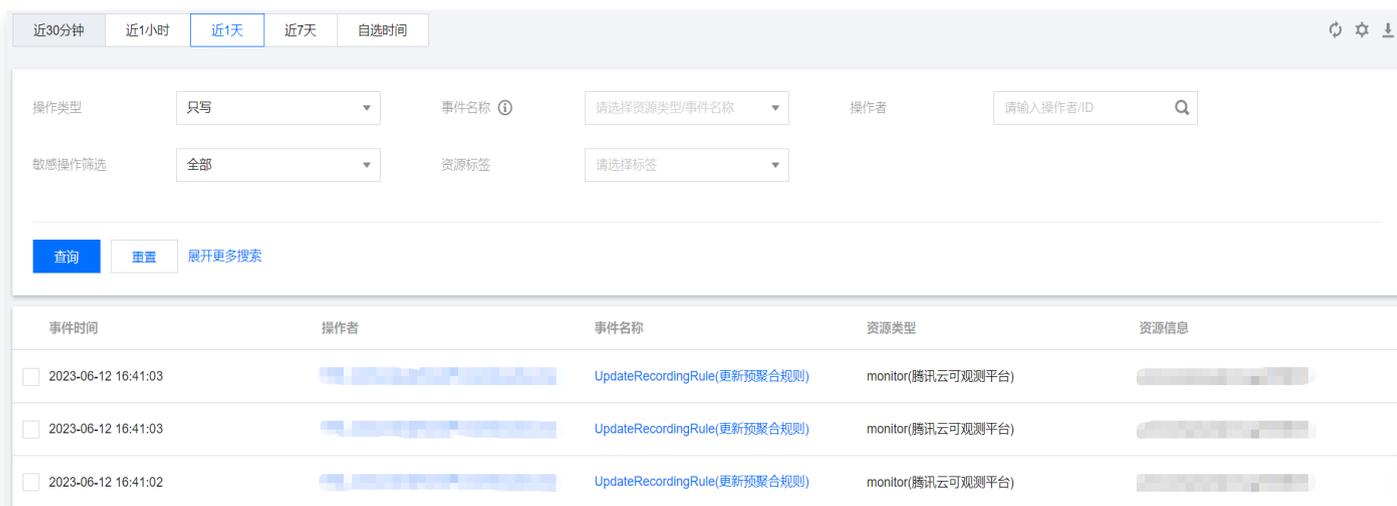
## 注册与登录

- 如果您还未完成腾讯云账户的注册，请先 [注册](#)，注册完成后您需要进行实名认证，具体操作可参考 [实名认证指引](#)。
- 如果您已注册腾讯云账户，并进行了实名认证，可直接登录 [腾讯云](#)，选择云产品 > 管理与审计 > 操作审计，进入操作审计页面。

## 查看操作记录

### 列表

- 登录 [操作审计控制台](#)。
- 在左侧导航中，单击[操作记录](#)，进入操作记录页面。
- 在操作记录页面中，默认情况下只展示部分数据。您可以输入操作者、操作类型、事件名称、资源类型、请求 ID、API 错误码、密钥 IP 及对应操作事件时间（您可单击  按需选择需要展示的字段），单击[查询](#)，即可获取相关的操作记录信息。



The screenshot shows the Tencent Cloud Audit Console interface. At the top, there are time range filters: 近30分钟, 近1小时, 近1天 (selected), 近7天, and 自选时间. Below these are search filters for 操作类型 (只写), 敏感操作筛选 (全部), 事件名称 (请选择资源类型/事件名称), 资源标签 (请选择标签), and 操作者 (请输入操作者/ID). A 查询 button is present. Below the filters is a table with columns: 事件时间, 操作者, 事件名称, 资源类型, and 资源信息. The table contains three rows of records.

事件时间	操作者	事件名称	资源类型	资源信息
<input type="checkbox"/> 2023-06-12 16:41:03	[Redacted]	UpdateRecordingRule(更新预聚合规则)	monitor(腾讯云可观测平台)	[Redacted]
<input type="checkbox"/> 2023-06-12 16:41:03	[Redacted]	UpdateRecordingRule(更新预聚合规则)	monitor(腾讯云可观测平台)	[Redacted]
<input type="checkbox"/> 2023-06-12 16:41:02	[Redacted]	UpdateRecordingRule(更新预聚合规则)	monitor(腾讯云可观测平台)	[Redacted]

## 详情

您在获取到相关的操作记录列表后，如果想更进一步了解单个操作记录，可以单击该操作记录左侧的 ，即可得到此操作记录的详情，包括事件时间、用户名、事件名称、访问密钥、事件 ID、源 IP 地址、资源区域、CAM 错误码、事件区域、事件源、请求 ID。同时，可以单击[查看事件](#)，进行了解事件的相关信息。如下图所示：

事件时间	用户名	事件名称	资源类型	资源名称	来源
2021-09-27 16:05:57	root	ConsoleLogin(登录)	account(账号中心)	account/ [redacted]	ConsoleCall

**基本信息** [事件说明](#)

密钥 ID - CAM 错误码 - 来源 ConsoleCall

事件名称 ConsoleLogin 事件区域 ap-guangzhou

事件时间 2021-09-27 16:05:57 事件源 account.tencentcloudapi.com

源 IP 地址 [redacted] (中国 广东省 深圳市 中国电信) 请求 ID [redacted]

资源区域 gz 用户名 [redacted] (root)

[查看事件](#)

## 使用跟踪集

### 1. 创建跟踪集

1.1 登录 [操作审计控制台](#)，选择左侧导航栏中的跟踪集 > 创建，进入跟踪集创建页面。

1.2 在跟踪集页面中，单击创建。如下图所示：



**注意：**  
最多支持创建5个跟踪集。

1.3 在创建跟踪集页面，按需填写跟踪集名称、存储位置等相关信息，单击完成新建即可。如下图所示：

←
创建跟踪集

**基础信息**

跟踪集名称 \*

仅支持大小写字母、数字、以及\_的组合，3-128个字符。

跟踪区域 所有区域

**管理事件**

管理事件类型 \*  只写  只读  全部

资源类型 \*

事件名称 \*  全部事件

**投递位置**

投递位置 将事件投递到

跟踪投递范围  集团账号下所有成员<sup>①</sup>

跟踪应用集团账号下所有成员，会将资源目录内所有成员的操作事件进行汇总投递至该集团账号。具体操作，请参见[功能介绍](#)。

补齐近三个月（90天）事件

选择补齐后，会将当前日志往前90天的操作事件汇总投递至跟踪集

取消
完成新建

## 2. 关闭或开启跟踪集记录日志

2.1 当您成功创建跟踪集后，跟踪集的状态显示默认为开启。如下图所示：

名称	跟踪区域	跟踪资源类型	COS 存储桶	CLS日志主题	日志文件前缀	日志记录状态	操作
doctest	所有区域	全部资源	-	日志分析	cloudaudit	开启	<a href="#">编辑</a> <a href="#">删除</a>

2.2 单击对应的跟踪集名称，或跟踪集所在行右侧的编辑，进入跟踪集详情页面。如下图所示：

← aasdsaf

---

### 基础信息

跟踪集名称 \* aasdsaf

跟踪区域 所有区域

创建时间 2023-06-08 15:44:53

---

### 管理事件

管理事件类型 \* 只写

资源类型 全部资源类型

事件名称 全部事件

---

### 投递位置

将事件投递到存储桶COS

COS 存储桶 (地域): 南京 (名称): sss

日志文件前缀 \* sd123

跟踪投递范围 集团账号下所有成员

补齐近三个月日志 ⓘ 是

2.3 单击页面右上角开启日志记录右侧的  (图示为开启状态)，即可关闭或开启跟踪集记录日志。

### 3. 修改投递存储位置

单击跟踪集详情页面投递位置中的编辑，可按需选择投递位置为投递存储桶（COS）或者投递到日志服务（CLS），编辑完成后单击保存即可。如下图所示：

**投递位置**

投递位置 将事件投递到

COS 存储桶  当前账号下的已有存储桶  当前账号下新建存储桶  其他操作审计管理员账号下已有存储桶

所属地域\*

日志文件前缀\*

仅支持字母和数字的组合，3-40个字符

跟踪投递范围  集团账号下所有成员 <sup>①</sup>

跟踪应用集团账号下所有成员，会将资源目录内所有成员的操作事件进行汇总投递至该集团账号。具体操作，请参见[功能介绍](#)。

补齐近三个月（90天）事件

选择补齐后，会将当前日志往前90天的操作事件汇总投递至跟踪集

#### 4. 集团账号跨账号投递

##### ① 说明：

当前账号为企业实名认证账号，且已 [创建集团账号组织](#) 时，可使用此功能。

单击跟踪集详情页面**投递位置**中的**编辑**，可以选择当前账号投递（默认）或者跨账号投递日志。

勾选**集团账号下所有成员**并保存后，即已开启跨账号投递功能，跟踪集会将集团账号下各成员的日志投递到您设置的投递位置中。如下图所示：

跟踪投递范围  集团账号下所有成员 <sup>①</sup>

跟踪应用集团账号下所有会员，会将资源目录内所有成员的操作事件进行汇总投递至该集团账号。具体操作，请参见[功能介绍](#)。

#### 5. 删除跟踪集

在跟踪集页面中，单击跟踪集所在行右侧的**删除**，或在跟踪集详情页面单击**删除跟踪集**即可。