操作审计

操作指南

产品文档

腾讯云

文档目录

操作指南
查看操作记录事件详情

最近更新时间：2024-02-28 17:27:24

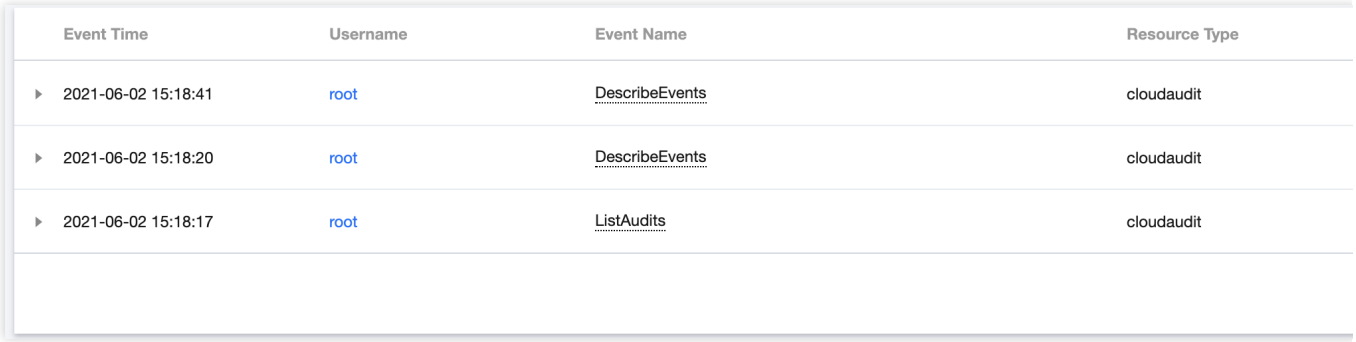
操作场景

本文介绍了如何通过操作审计控制台查看操作记录的事件详情，及事件详情包含的字段说明。

操作步骤

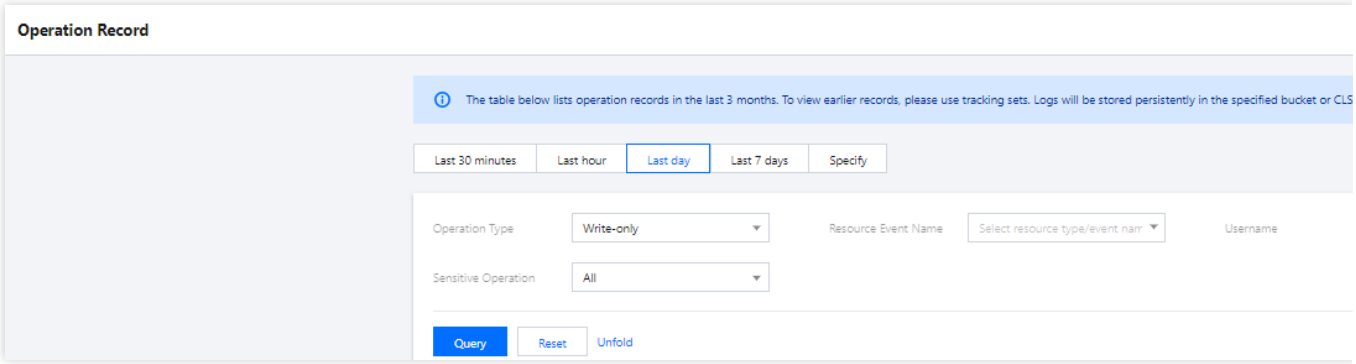
查看操作记录

1. 登录操作审计控制台，选择左侧导航栏中的 **操作记录** 。
2. 在“操作记录”列表页面，可查看事件操作记录。如下图所示：



Event Time	Username	Event Name	Resource Type
2021-06-02 15:18:41	root	DescribeEvents	cloudaudit
2021-06-02 15:18:20	root	DescribeEvents	cloudaudit
2021-06-02 15:18:17	root	ListAudits	cloudaudit

其中，操作者指事件操作人，分为以下几种类型：
主账号操作：用户名显示为 root。
子用户操作：用户名显示子用户名称，如果子用户已被删除，则显示子用户 ID。
角色操作：用户名显示角色名称，如果角色已被删除，则显示角色 ID。
您可单击**操作者**，前往**用户列表**页面查看该用户更多信息。
3. 操作审计支持多种筛选条件，包括按时间、事件、用户名称、操作读写类型、敏感操作、资源标签、资源名称、密钥 ID、请求 ID 及 API 错误码。您可选择**展开更多搜索**，参考以下说明按需设置。如下图所示：



筛选条件说明如下：

时间范围：您可以筛选最近90天中，30天范围内的日志。

操作类型：支持按全部、只读、只写过滤。

资源事件名称：您可以通过各产品的接口文档中的接口名称，搜索过滤您希望查询到的日志。例如 CVM - RunInstances（创建实例）。最多支持同时查询10个事件。

说明

若您未在列表中查找到所需查询产品的事件名称，则请通过 提交工单 进行反馈，我们将尽快排查处理。

用户名称：可通过搜索用户主账号、子账号 ID 或角色 ID 筛选日志。

敏感操作筛选：支持筛选全部敏感及非敏感操作。敏感操作是可能涉及云资源重要操作的事件，由平台定义。若您需将某些操作也纳入敏感操作，则请通过 提交工单 进行反馈，我们将尽快处理。

资源标签：支持按照标签筛选。如需了解标签更多信息，请参见 标签。

资源名称：支持输入资源 ID 搜索。例如 `ins-fi8oxxxx` 。

密钥 ID：支持输入密钥 ID 搜索。例如 `AKIDZ0GSXSG2nT5c6Xxxxxxxxxxxxxxxx` 。

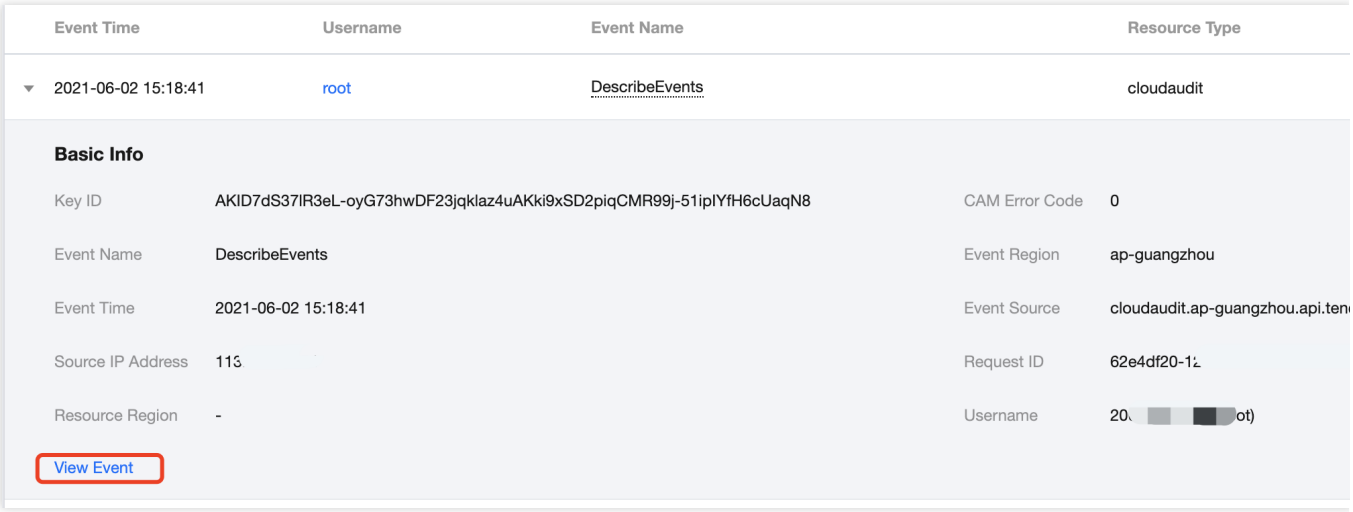
请求 ID：支持输入请求 ID 搜索。例如 `a7da0568-7580-4798-88c8-xxxxxxxxxx` 。

API 错误码：支持输入 API 错误码搜索。请参考各产品 API 文档中的错误码，进行对比后按需搜索。

4. 单击**查询**，即可获取对应操作记录信息。

查看事件详情

1. 若您需查看某一事件的详细信息，可单击列表中的信息，或单击信息前的 `+` ，并在展开的模块中，单击**查看事件**。如下图所示：



说明

您可通过 “CAM 错误码”字段判断事件是否执行成功。若 CAM 错误码为空，则事件执行成功。若 CAM 错误码不为空，则事件执行失败，具体错误原因请查看事件详情中的 `errorCode` 及 `errorMessage` 字段。

2. 可在右侧模块中查看事件详细信息，字段说明请参考 附录。

附录

操作记录中事件详情的字段说明如下表：

名称	类型	示例	描述
userIdentity	dict	不涉及	请求者的身份信息
eventRegion	String	ap-guangzhou	请求的云服务所在集群区域
eventVersion	int	2	事件版本
errorCode	int	0	请求签名或鉴权发生错误时的错误码
errorMessage	String	不涉及	请求签名或鉴权发生错误时的错误信息
requestID	String	be59bbc7-e539-4b14-9d2c-eb7061e61***	请求 ID，每个 API 请求都会有一个请求 ID
eventID	String	e2c8694c-12e6-4da9-a1e1-48bb703c0***	事件 ID，由操作审计生成的事件

			GUID
apiVersion	String	3.0	API 版本
eventType	String	ConsoleCall	事件请求的源头类型，取值： ConsoleCall：请求由腾讯云控制台发起 ApiCall：请求由直接调用云 API 发起 MiniProgramCall：请求由云助手小程序发起
actionType	String	Read	请求事件的读写类型，取值： Write：写类型 Read：读类型
apiErrorCode	int	0	API 请求发生错误时的错误码
apiErrorMessage	String	不涉及	API 请求发生错误时的错误信息
userAgent	String	SDK_GO_1.0.374	发送 API 请求的客户端代理
eventTime	int	2022-04-01 11:30:36	事件的发生时间
sensitiveAction	int	0	事件是否为敏感操作，取值： 1：敏感操作 0：非敏感操作

eventPlatform	int	0	事件是否为平台事件，取值： 1：平台事件 0：非平台事件
sourceIPAddress	String	113...*	源 IP 地址
resourceType	String	cam	请求的云服务名称
eventName	String	GetPolicy	请求的事件名称
eventSource	String	cam.ap-guangzhou.api.tencentyun.com	请求来源
requestParameters	-	不涉及	请求的入参信息
requestElements	-	不涉及	请求的回包信息
resources	String	qcs:id/0:cos:ap-shanghai:uid/1252081***:prefix//1252081***/pdd-open-api/images/2018-07-02/6cff3fee97bbf0d2c930fb4ddd5658c4.jpeg	事件的相关资源信息，是资源的 QCS
resourceName	String	policy/7934***	事件的相关资源名称
tags	String	{"key":"projectId","value":"0"}	资源标签

请求者身份信

息说明如下表：

名称	类型	示例	描述
principalId	String	100015591***	操作者账号 ID，取值： 主账号操作：为主账号 ID 子用户操作：为子用户 ID 角色操作：为角色 ID
accountId	String	100015591***	操作者所属主账号 ID
secretId	String	AKID4IrZ2GV***	操作者的密钥 ID

type	String	root	操作者类型，取值： root：腾讯云主账号 CAM user：腾讯云 CAM 账号 ID（或用户名称） AssumedRole：腾讯云角色 roleUser
userName	String	root	操作者昵称
sessionContext	String	不涉及	API 请求发生错误时的错误码
roleSessionName	String	EMR-Session	主体扮演角色时承担的角色会话名称，类型为： saml：IDP 员工使用腾讯云用户角色发起请求 WebIdentityUser：OIDC 联合用户角色发起请求 TencentCloudService：用户授权腾讯云服务扮演角色发起请求

使用跟踪集投递日志

最近更新时间：2024-02-28 17:27:24

操作场景

本文介绍了如何通过操作审计控制台创建跟踪集，并投递日志。

操作步骤

1. 登录操作审计控制台，选择左侧导航栏中的 **跟踪集** 。
2. 在**跟踪集**页面中，单击**创建**。
3. 在**创建跟踪集**页面中，根据以下主要信息进行填写。

基础信息：自定义填写跟踪集名称。

管理事件：可根据“事件类型”、“资源类型”进行筛选，还可进一步选择“全部事件”或“部分事件”来进行筛选投递。

投递位置：

将事件投递到日志服务CLS：可以直接创建新的日志主题并投递，也可选择投递到已有的日志主题。使用日志服务更多信息请参见 日志服务。

将事件投递到存储桶COS：可以直接创建存储桶并投递，也可投递到已有存储桶中。使用存储桶更多信息请参见 存储桶概览。

4. 单击**完成新建**即可创建跟踪集。约10分钟后， 开始正常投递日志。