CloudAudit

Operation Guide

Product Documentation

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

Operation Guide
Viewing Event Details in Operation Record

Last updated : 2022-05-13 10:20:36

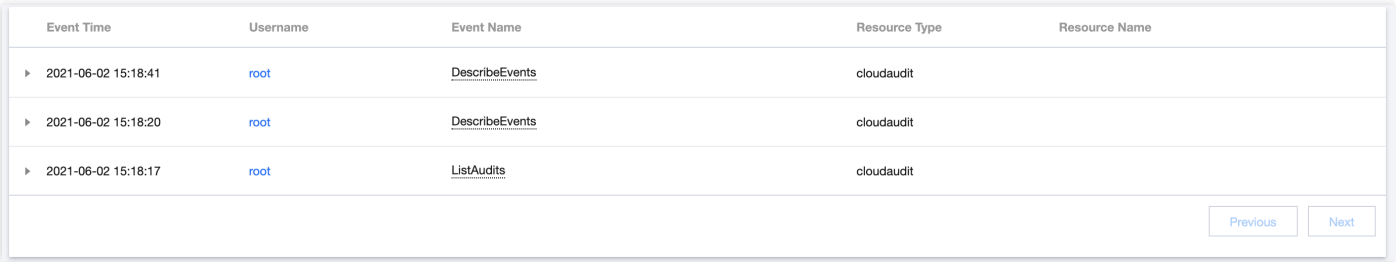
Overview

This document describes how to view the event details in operation records and the field descriptions involved in event details in the CloudAudit console.

Directions

Viewing operation record

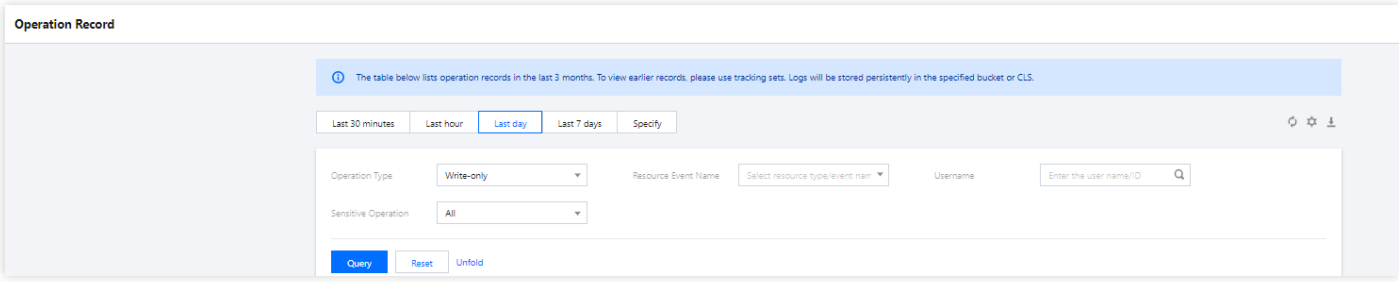
1. Log in to the CloudAudit console and select **Operation Record** on the left sidebar.
2. On the operation record list page, you can view the operation records of an event in the operation record list as shown below:



The username indicates the event operator. It is divided into three types based on the following operation types:

- **Operation by a root account**: "root" is displayed as the username.
- **Operation by a sub-user**: The sub-user name is displayed as the username. If the sub-user has been deleted, the sub-user ID will be displayed as the username.
- **Operation by a role**: The role name is displayed as the username. If the role has been deleted, the role ID will be displayed as the username.
  You can go to the user details page by clicking the username to view more user information.

3. CloudAudit supports many filters, including time, event, username, operation read/write type, sensitive operation, resource name, key ID, request ID, and API error code. You can click **Unfold** and refer to the following to configure filters as needed:



Filter descriptions:

- **Time Range**: You can filter logs within a 30-day range in the past 90 days.
- **Operation Type**: You can filter by all, read, or write.
- **Resource Event Name**: You can filter desired logs by API name in the API documentation of each product, such as CVM - RunInstances (for instance creation). Up to ten events can be queried at a time.

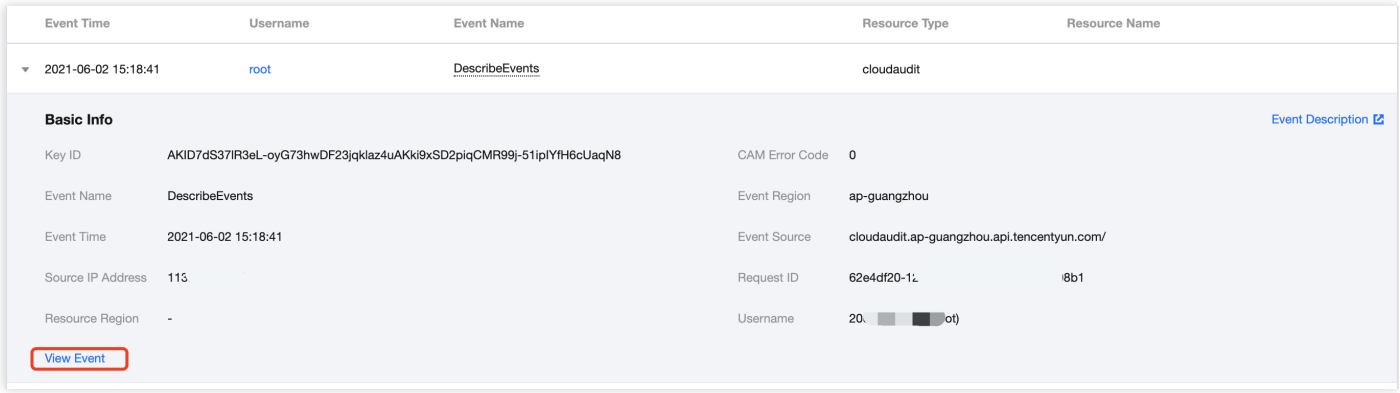
> Note
> If you can't find a product event name that you want to query in the list, submit a ticket for assistance.

- **Username**: You can filter logs by root account, sub-account ID, or role ID.
- **Operation Query**: You can filter all sensitive and non-sensitive operations. Sensitive operations are defined by the platform as events that may involve key operations on cloud resources. If you need to include certain operations as sensitive operations, submit a ticket for assistance.
- **Resource Name**: You can enter a resource ID for search, such as `ins-fi8oxxxx`.
- **Key ID**: You can enter a key ID for search, such as `AKIDZ0GSXSG2nT5c6Xxxxxxxxxxxxxxxx`.
- **Request ID**: You can enter a request ID for search, such as `a7da0568-7580-4798-88c8-xxxxxxxxxx`.
- **API Error Code**: You can enter an API error code as listed in the corresponding API documentation for search.

4. Click **Query** to get the filtered operation records.

Viewing event details

1. If you need to view the details of an event, you can click the information in the list. You can also click `+` before the information and click **View Event** in the expanded module as shown below:



> Note
> You can check whether the event was successfully executed through the "CAM Error Code" field. If this field is empty, the event was successfully executed; otherwise, it means the execution failed. For failure details, check the `errorCode` and `errorMessage` fields in the event details.

2. Then you can view the event details in the module on the right. For more information on field descriptions, see Appendix.

Appendix

The table below displays the field descriptions of the event details in an operation record.

Name	Type	Example	Description
userIdentity	dict	N/A	Identity information of the requester
actionType	String	Read	The read/write type of a request event
eventRegion	String	ap-guangzhou	Cluster region of a request event
eventVersion	int	2	Log version

errorCode	int	0	Error code that appears when there is an API request error
errorMessage	String	N/A	Error message that appears when there is an API request error
requestID	String	be59bbc7-e539-4b14-9d2c-eb7061e61***	Request ID. Each API request has a request ID.
apiVersion	String	3.0	API version
eventType	String	ConsoleCall	• ConsoleCall means the request is initiated by the Tencent Cloud console. • ApiCall means the request is initiated by the direct call of TencentCloud API.
eventTime	int	2022-04-01 11:30:36	Event occurrence time (local time at Tencent Cloud International)
sourceIPAddress	String	113.*.*.*	Source IP address
resourceType	String	cam	The requested Tencent Cloud service name
eventName	String	GetPolicy	The requested event name
eventSource	String	cam.ap-guangzhou.api.tencentyun.com	Request source
requestParameters	-	N/A	The requested parameter information
resourceName	String	policy/7934***	The requested resource name

The table below displays the requester's identity descriptions:

Name	Type	Example	Description
principalId	String	100015591***	Operator information: • Operation by a root account: The root account ID

			• Operation by a sub-user: The sub-user ID • Operation by a role: The role ID
accountId	String	100015591***	Root account ID
secretId	String	AKID4IrZ2GV***	Key ID
type	String	root	• root: Tencent Cloud root account • CAMuser: Tencent Cloud CAM account ID (or username) • AssumedRole: Tencent Cloud roleUser
userName	String	root	• root: Tencent Cloud root account • CAMuser: Tencent Cloud CAM account ID (or username) • AssumedRole: Tencent Cloud roleUser
roleName	String	SSA_QcsRole	Name of the current role, which needs to be determined together with `type`. If `type` is `AssumedRole` and `userName` is `roleUser`, then `roleName` is the name of the role.
sessionContext	String	N/A	Error code that appears when there is an API request error

Shipping Log with Tracking Set

Last updated : 2021-09-16 12:42:31

Overview

This document describes how to create a tracking set and ship logs in the CloudAudit console.

Directions

1. Log in to the CloudAudit console and select **Tracking Set** on the left sidebar.

2. On the **Tracking Set** page, click **Create** as shown below:

3. On the **Create Tracking Set** page, enter the following main information as shown below:

   - **Basic Info**: enter a custom tracking set name.
   - **Manage Event**: you can filter events by **event type** and **resource type** or further select **All events** or **Some events** for filtering and shipping.
   - **Shipping Location**:
     - Ship the event to CLS: you can directly create a new log topic or select an existing one for log shipping. For more information on how to use CLS, please see Getting Started in 5 Minutes.
     - Ship the event to a COS bucket: you can directly create a new bucket or select an existing one for log shipping. For more information on how to use buckets, please see Bucket Overview.

4. Click **Creation completed** to create the tracking set. After about 10 minutes, logs will be shipped normally.