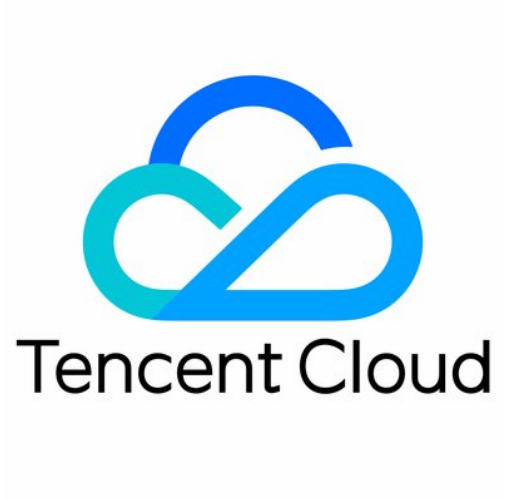
CloudAudit

Operation Guide

Product Documentation



Contents

Operation Guide
Viewing Event Details in Operation Record

Last updated：2024-01-24 17:35:28

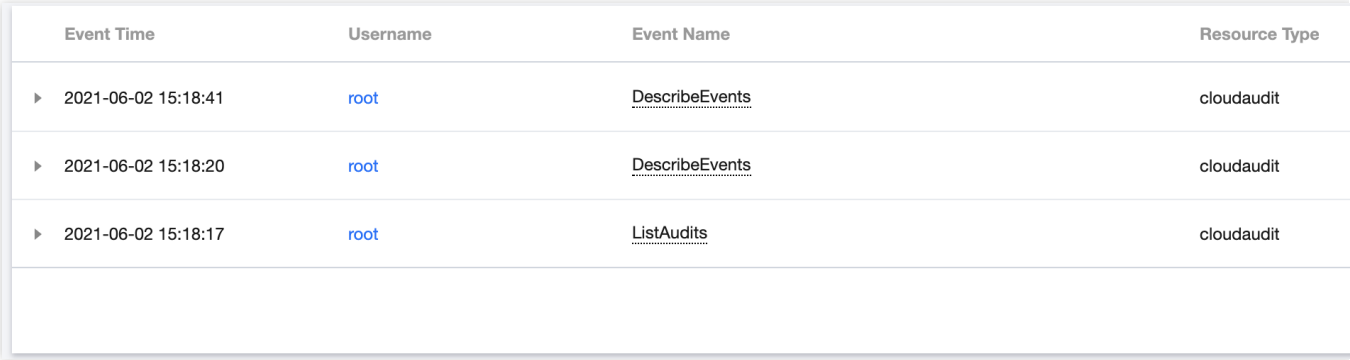
Overview

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

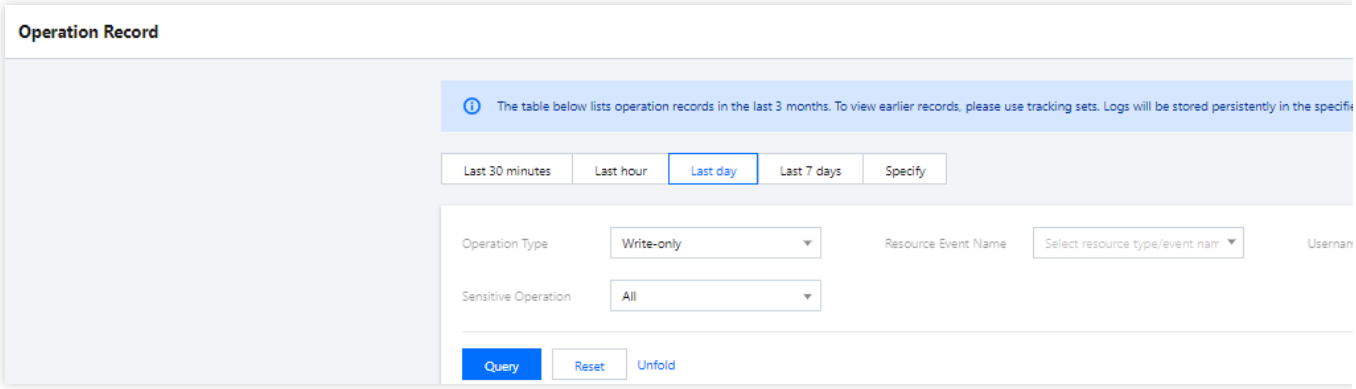
Directions

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.



The operator indicates the event operator. It is divided into three types based on the following operation types:
Operation by a root account: The name “root” is displayed as the operator.
Operation by a sub-user: The sub-user name is displayed as the operator. If the sub-user has been deleted, the sub-user ID will be displayed instead.
Operation by a role: The role name is displayed as the operator. If the role has been deleted, the role ID will be displayed as the operator.
You can click an operator to go to the **User List** page in the CAM console to view the detailed user information.
3. CloudAudit supports many filters, including time, event, username, operation read/write type, sensitive operation, resource tag, resource name, key ID, request ID, and API error code. You can click **Unfold** and 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-only**, or **Write-only**.

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 Tag: You can filter logs by resource tag. For more information on tags, see Tag Overview.

Resource Name: You search by resource ID, such as `ins-fi8oxxxx` .

Key ID: You can search by key ID, such as `AKIDZ0GSXSG2nT5c6Xxxxxxxxxxxxxxxx` .

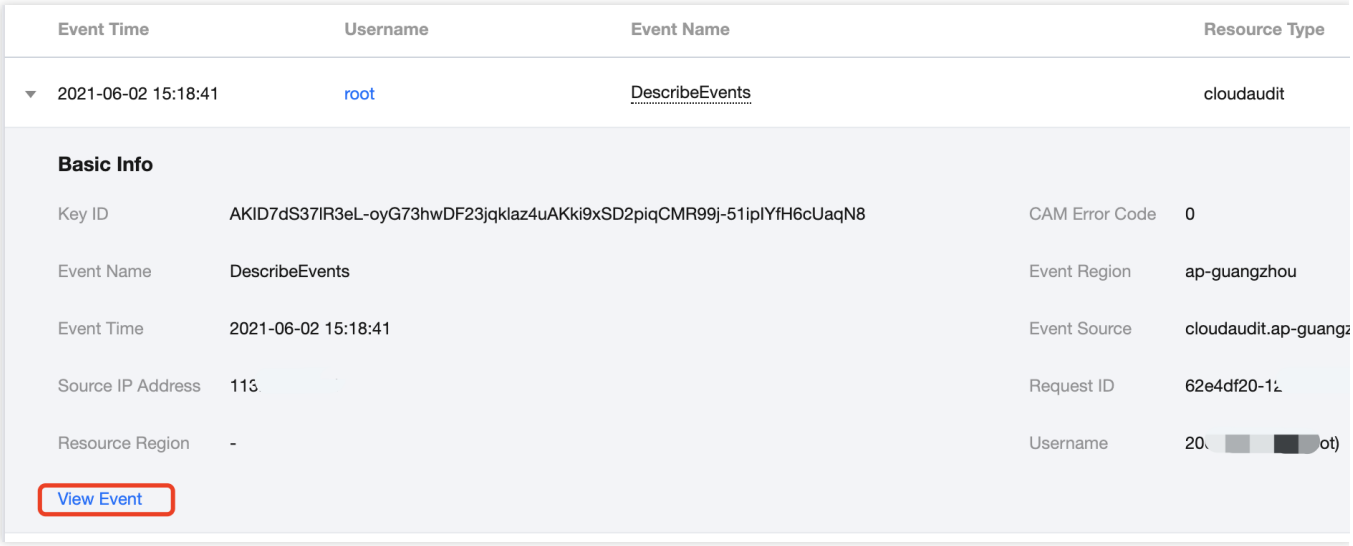
Request ID: You can search by request ID, such as `a7da0568-7580-4798-88c8-xxxxxxxxxx` .

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 the `+` icon before the information and click **View Event** in the expanded module.



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
eventRegion	String	ap-guangzhou	Cluster region of the requested Tencent Cloud service
eventVersion	int	2	Event version
errorCode	int	0	Error code returned when an error occurred while requesting the signature or authentication

errorMessage	String	N/A	Error message returned when an error occurred while requesting the signature or authentication
requestID	String	be59bbc7-e539-4b14-9d2c-eb7061e61***	Request ID, which is the ID of each API request
eventID	String	e2c8694c-12e6-4da9-a1e1-48bb703c0892	Event ID, which is the event GUID generated by CloudAudit
apiVersion	String	3.0	API version
eventType	String	ConsoleCall	Source type of the event request. Valid values: ConsoleCall: The request is initiated by the Tencent Cloud console. ApiCall: The request is initiated by the direct call of TencentCloud API. MiniProgramCall: The request is initiated by the Tencent Cloud Assistant mini program.
actionType	String	Read	Read/write type of the request event. Valid values: Write: Write

			Read: Read
apiErrorCode	int	0	Error code returned for an API request error
apiErrorMessage	String	N/A	Error message returned for an API request error
userAgent	String	SDK_GO_1.0.374	The client proxy that sends the API request
eventTime	int	2022-04-01 11:30:36	Event occurrence time
sensitiveAction	int	0	Whether the event is a sensitive operation. Valid values: 1: Sensitive operation 0: Non-sensitive operation
eventPlatform	int	0	Whether the event is a platform event. Valid values: 1: Platform event 0: Non-platform event
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	Input parameters of the request
requestElements	-	N/A	Response information of the request
resources	String	qcs:id/0:cos:ap-shanghai:uid/1252081001:prefix//1252081001/pdd-open-api/images/2018-07-02/6cff3fee97bbf0d2c930fb4ddd5658c4.jpeg	Resource information of the event, which is the value of the `qcs` segment in the six-segment resource description.
resourceName	String	policy/7934***	Resource name of the event
tags	String	{"key":"projectId","value":"0"}	Resource tag

The tabl

e b

elow displays the requester's identity descriptions.

Name	Type	Example	Description
principalId	String	100015591***	Operator account ID. Valid values: 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***	ID of the root account to which the operator belongs
secretId	String	AKID4IrZ2GV***	Key ID of the operator
type	String	root	Operator type. Valid values: root: Tencent Cloud CAM root account user: Tencent Cloud CAM account ID (or username) AssumedRole: Tencent Cloud role (roleUser)
userName	String	root	Operator name
sessionContext	String	N/A	Error code returned for an API request error
roleSessionName	String	EMR-Session	There are three types of role session name when

			the operator assumes a role: saml: IDP employees use Tencent Cloud user roles to initiate requests. WebIdentityUser: OIDC federated user roles initiate requests. TencentCloudService: Users authorizing Tencent Cloud Services to assume roles to initiate requests.

Shipping Log with Tracking Set

Last updated：2024-01-24 17:35:28

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.