

CloudAudit

Getting Started

Product Documentation



Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

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.

Getting Started

Last updated : 2024-01-24 17:35:28

You can get started with CloudAudit easily in the Tencent Cloud console, where you can view operation records, create and delete a tracking set, edit its storage location, and disable its logging feature.

Signup and Login

[Sign up](#) for a Tencent Cloud account if you don't have one yet, and then complete identity verification as instructed in [Identity Verification Guide](#).

If you have already signed up for a Tencent Cloud account and completed identity verification, you can directly log in to the [Tencent Cloud console](#) and click **Products > Management and Audit > CloudAudit** to enter the CloudAudit page.

Viewing Operation Records

List

1. Log in to the [CloudAudit console](#).
2. Click **Event history** in the left sidebar to enter the event history page.
3. On the event history page, you can view related operation records by username, operation type, resource event name, resource name, resource ID, API error code, key IP, and corresponding operation event time. The queried operation records will be displayed in a list. By default, only partial data is displayed as shown below:

Last 30 minutes Last hour Last day Last 7 days Specify				
Operation Type <input type="text"/>		Resource Event Name <input type="text" value="Select resource type/event nam"/>		Username
Query Reset Unfold				
Event Time	Operator	Event Name	Resource Type	Resource
+ 2021-11-12 11:40:06	root	<input type="text"/>	<input type="text"/>	<input type="text"/>

Details

In the operation record list, you can click



on the left of an operation to get its details, including event time, username, event name, access key, event ID, source IP address, resource region, CAM error code, event region, event source, and request ID. You can also click **View Event** to view the details of the event as shown below:

Event time		User name	Event name	
▼ 2020-07-22 15:07:29		100011212224	ConsoleLogin	
access key			CAM Error Code	0
Event ID	68	1a7d691	Event Region	ap-guangzhou
Event name	ConsoleLogin		Event source	ac
Event time			Request ID	15
Source IP address			User name	
Resource Region	gz			
View event				

Using Tracking Set

1. Create a tracking set

- Log in to the [CloudAudit console](#) and select **Tracking Set** > **Create** on the left sidebar to enter the tracking set creation page.
- On the **Tracking Set** page, click **Create** as shown below:

1. During public trial, only one tracking set can be created.

2. If your tracking set is normal, it records the operation logs under your account and stores them to the bucket configured for it. If your tracking set is disabled, operation log

3. Fees for storing the tracking logs you recorded into COS are charged based on the standard COS billing.[View COS billing details.](#)

Create

Name	All regions	COS Bucket	Log File Prefix
No tracking sets			

Note:

You can create up to 5 tracking sets.

3. Enter the tracking set name, storage location, and other relevant information on the page and click **Creation completed** as shown below:

create Audit

Basic info

Audit name * ✓
Only uppercase and lowercase letters, numbers, and combinations of _ are supported, 3-128 characters.

Audit all regions Yes

Management event

Management event * ☒ All ☐ Read only ☐ Write only

Storage location

Create a new COS bucket ☒ Yes ☐ No

COS bucket * ✓
Only combinations of lowercase letters, numbers, and the underscore "-" are supported, and cannot exceed 40 characters, and don't support the beginning with _.

Add advanced settings ▾

Log File Prefix ✓
Only combinations of letters and numbers, 3-40 characters are supported.

Send CMQ notifications * ☐ Yes ☒ No


Use KMS to encrypt logging file * ☐ Yes ☒ No
KMS is not supported in the current region

4. Disable/Enable the tracking set's logging feature

5. After you successfully create a tracking set, it is **Enabled** by default as shown below:

Name	All regions	COS Bucket
test	Yes	cloud

6. Click the name of the tracking set in the **Name** column or **Edit** on the right on the tracking set row to enter the tracking set details page as shown below:

 **test**

Basic info

Audit name *	test
Audit all regions	Yes

Management event

Management event *	All
--------------------	-----

Storage location

COS bucket	Region: ap-shanghai	Name: cloud
Log File Prefix	audit	
Send CMQ notifications	No	

Delete Audit

7. Click



on the right of **Enable Logging** in the top-right corner of the page to **disable or enable** the tracking set's logging feature (which is enabled in the screenshot).

8. Edit the storage location

Click **Edit** in the **Shipping Location** section on the tracking set details page. You can choose to ship to a COS bucket or CLS. After editing, click **Save** as shown below:

test

Basic info

Audit name *

test

Audit all regions

Yes

Management event

Management event *

All

Storage location

Create a new COS bucket

☐ Yes ☒ No

COS bucket *

shanghai

cloud

Only combinations of lowercase letters, numbers, and the underscore "-" are supported, and cannot exceed 40 characters, and don't support the beginning or end of the t

Add advanced settings ▾

Log File Prefix

audit

Only combinations of letters and numbers, 3-40 characters are supported.

Send CMQ notifications *

☐ Yes ☒ No

Use KMS to encrypt logging file *

☐ Yes ☒ No

KMS is not supported in the current region

Save

Cancel

9. Delete the tracking set

Click **Delete** on the right on a tracking set row on the **Tracking Set** page or click **Delete Tracking Set** on the tracking set details page.