

# CloudAudit

## Getting Started

### Product Documentation



## Copyright Notice

©2013-2019 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 : 2021-11-09 11:53:28

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.

### 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	Resource type	Resource name
2020-07-22 15:07:29	100011212224	ConsoleLogin	account	account/100011212224
access key		CAM Error Code 0		
Event ID	68 [redacted] 1a7d691	Event Region	ap-guangzhou	
Event name	ConsoleLogin	Event source	ac [redacted] .om	
Event time	[redacted]	Request ID	15 [redacted] e172c6be0044bc1f3_v2	
Source IP address	[redacted]	User name	[redacted]	
Resource Region	gz			
<a href="#">View event</a>				

## Using Tracking Set

### 1. Create a tracking set

- i. Log in to the [CloudAudit console](#) and select **Tracking Set** > **Create** on the left sidebar to enter the tracking set creation page.
- ii. 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 logs are not stored to the appropriate bucket.  
 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	Status
No tracking sets				

#### Note

You can create up to 5 tracking sets.

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

## 2. Disable/Enable the tracking set's logging feature

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

Name	All regions	COS Bucket	Log File Prefix	Status
test	Yes	cloud	audit	Enable

ii. 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:

The screenshot displays the configuration page for an audit named 'test'. At the top right, there is a toggle switch for 'Turn on logging' which is currently turned on. The page is divided into three main sections: 'Basic info', 'Management event', and 'Storage location'. Each section has an 'Edit' link on the right side. At the bottom left, there is a 'Delete Audit' button.

Basic info	
Audit name *	test
Audit all regions	Yes


  

Management event		Edit
Management event *	All	

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

Delete Audit

iii. 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).

### 3. 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:

The screenshot displays the configuration page for a tracking set named "test". The page is divided into three main sections: "Basic info", "Management event", and "Storage location".

- Basic info:** "Audit name" is set to "test" and "Audit all regions" is set to "Yes".
- Management event:** "Management event" is set to "All". An "Edit" link is visible on the right.
- Storage location:** "Create a new COS bucket" is set to "No". "COS bucket" is set to "shanghai" and "cloud". A search icon is present next to the bucket name. Below this, there is a note: "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 underscore '-'". "Add advanced settings" is a dropdown menu. "Log File Prefix" is set to "audit". A note below states: "Only combinations of letters and numbers, 3-40 characters are supported." "Send CMQ notifications" is set to "No". "Use KMS to encrypt logging file" is set to "No", with a note: "KMS is not supported in the current region".

At the bottom of the form, there are "Save" and "Cancel" buttons.

#### 4. 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.