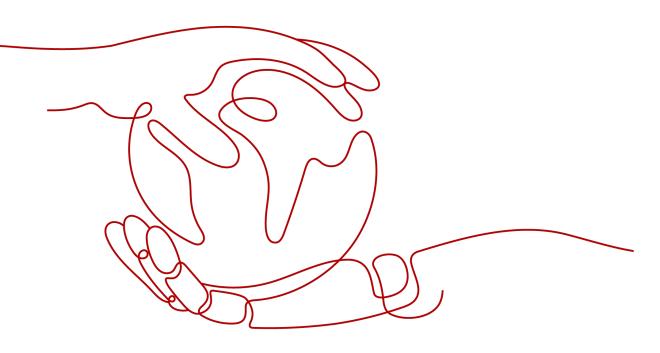
Cloud Trace Service

FAQs

 Issue
 01

 Date
 2023-11-15





Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2023. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions

NUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road Qianzhong Avenue Gui'an New District Gui Zhou 550029 People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

| 1 Must I Use an IAM User (Sub Account) to Configure Transfer on CTS and Perform Operations on an OBS Bucket? |
|--|
| 2 How Will CTS Be Affected If My Account Is in Arrears? |
| 3 What Are the Recommended Users of CTS? |
| 4 What Will Happen If I Have Enabled Trace Transfer But Have Not Configured an Appropriate Policy for an OBS Bucket? |
| 5 Does CTS Support Integrity Verification of Trace Files? |
| 6 Why Are There Some Null Fields on the View Trace Page? |
| 7 Why Is an Operation Recorded Twice in the Trace List?7 |
| 8 What Services Are Supported by Key Event Notifications? |
| 9 How Can I Store Trace Files for a Long Time?9 |
| 10 Why Are user and source_ip Null for Some Traces with trace_type as SystemAction? |
| 11 How Can I Find Out Who Created a Specific ECS?11 |
| 12 How Can I Find Out the Login IP Address of an IAM User? |
| 13 Why Are Two deleteMetadata Traces Generated When I Buy an ECS in Pay-per- Use or Yearly/Monthly? |
| 14 What Can I Do If I Cannot Query Traces? |
| 15 Can I Disable CTS? |
| 16 How Do I Configure the Storage Duration of CTS Audit Logs to 180 Days? 16 |
| 17 What Should I Do If I Cannot Enable CTS as an IAM User?21 |
| 18 How Do I Enable Alarm Notifications for EVS? |

1 Must I Use an IAM User (Sub Account) to Configure Transfer on CTS and Perform Operations on an OBS Bucket?

No. You only need to ensure that you have the permissions for OBS buckets.

2 How Will CTS Be Affected If My Account Is in Arrears?

If your account is in arrears, CTS can still receive operation records from supported services, but the records can only be retained for 7 days. In most cases, records can be merged into trace files and transferred to OBS buckets for long term storage. Trace file storage in OBS buckets generates fees and this function cannot work when your account is in arrears.

In addition, the only action you can perform on trackers is to delete them.

3 What Are the Recommended Users of CTS?

It is highly recommended that cloud users should enable CTS.

- CTS is core to information security audit. It is an essential part of security risk control for information systems in enterprises and public sectors, and is also necessary for compliance with many industry standards and audit specifications.
- CTS helps accelerate troubleshooting and reduces workforce costs when exceptions occur on cloud resources. With CTS, you can track all operations involved when a fault happens, which helps narrow the possibilities.

4 What Will Happen If I Have Enabled Trace Transfer But Have Not Configured an Appropriate Policy for an OBS Bucket?

CTS delivers trace files based on the OBS bucket policy. If the policy is configured incorrectly, trace files cannot be delivered.

If an OBS bucket has been deleted or encounters an exception, an error message will be displayed on the management console. In this case, **create an OBS bucket** or **reconfigure access control of the OBS bucket**.

5 Does CTS Support Integrity Verification of Trace Files?

Yes. The following fields must be included in trace files: **time**, **service_type**, **resource_type**, **trace_name**, **trace_rating**, and **trace_type**. Other fields can be added by the services from which traces are collected.

6 Why Are There Some Null Fields on the View Trace Page?

Fields **source_ip**, **code**, **request**, **response**, and **message** can be null. These fields are not mandatory for CTS.

- **source_ip**: If the value of **trace_type** is **SystemAction**, the operation was triggered by the system. In this case, **source_ip** is null.
- **request**, **response**, and **code**: These three fields indicate the request content, request result, and HTTP return code of an operation. In some cases, these fields are null or have no service meaning. Therefore, they are left blank based on actual situations.
- **message**: This is a reserved field. Information of other cloud services will be added to this field when necessary. It is normal that the field is null.

Why Is an Operation Recorded Twice in the Trace List?

For an asynchronously invoked trace, such as **deleteDesktop** trace of Workspace, two records with the same trace name, resource type, and resource name will be generated. The two records may seem to be the same. However, they are generated at different times and document different details.

- The first record documents the request initiated by a user.
- The second record documents the response to the request and the operation result, and is usually several minutes later than the first record.

The two records together give a full view of the operation.

8 What Services Are Supported by Key Event Notifications?

CTS sends notifications of all key operations on services including ECS, EVS, VPC, DEW, native OpenStack, and IAM. These operations include creation, deletion, login, and native OpenStack API calls.

9 How Can I Store Trace Files for a Long Time?

CTS only retains traces for seven days. To store traces for a long time, configure your tracker to transfer traces to OBS buckets. For details, see section "Configuring a Tracker" in the *Cloud Trace Service User Guide*.

10 Why Are user and source_ip Null for Some Traces with trace_type as SystemAction?

The **trace_type** field indicates the request source. This field can be **ConsoleAction**, **ApiCall**, and **SystemAction**.

SystemAction indicates operations that are not triggered by users, such as alarms, elastic scaling, regular backup, or secondary invocations by systems to complete a user's request. In this case, **user** and **source_ip** are both null.

11 How Can I Find Out Who Created a Specific ECS?

Solution

To identify the user who created a specific ECS, you can view traces recorded by CTS.

Prerequisites

- You have enabled CTS.
- You have obtained the resource ID of the ECS.

Procedure

Log in to the CTS console, choose **Trace List**, and select **ECS** for **Trace Source**. In the displayed traces, look for the **createServer** trace with the obtained resource ID, and expand the trace details.

The **user** field shows details of the IAM user who created the ECS. The format is **{"name":** "*Account name*", "**id":** "*Account ID*", "**domain**"**{"name":** "*IAM user name*", "**id":** "*IAM user ID*"**}}**. If the ECS was created by an account, the IAM user name and the account name are the same.

12 How Can I Find Out the Login IP Address of an IAM User?

Background

If you want to check if there are security risks in your account by examining the login IP addresses and login time of IAM users, you can view traces recorded by CTS.

Prerequisites

You have enabled CTS.

Procedure

- **Step 1** Log in to the CTS console, select **IAM** for **Trace Source**, select a time range, and click **Query**.
- **Step 2** Click **View Trace** in the **Operation** column of a trace to view its details. **source_ip** indicates the login IP address, and **record_time** indicates the login time.

----End

13 Why Are Two deleteMetadata Traces Generated When I Buy an ECS in Pay-per-Use or Yearly/Monthly?

During ECS creation, metadata is used to store temporary information. When the creation is finished, the information is automatically deleted. Thus, two traces named **deleteMetadata** are generated.

14 What Can I Do If I Cannot Query Traces?

Background

Traces cannot be queried on the CTS console.

Procedure

- **Step 1** Check whether you have configured a proper query time range.
- **Step 2** Check whether you have configured filters correctly.
- **Step 3** For services that do not differentiate regions, such as IAM, you need to enable CTS and create a tracker named **system** in the central region (CN North-Beijing4) so that traces can be reported in other regions. To enable IAM to send SMS messages and emails, you also need to configure notification rules in the central region.
- **Step 4** If you still cannot query traces after the preceding steps, submit a service ticket for technical support.

----End

15 Can I Disable CTS?

If you do need to disable CTS, you can do it in the following two ways:

- Delete or disable existing trackers. (The **system** tracker created by CTS can only be disabled and cannot be deleted.) No traces will be generated.
- Delete the CTS agency from the IAM agency list. CTS will become unavailable.

16 How Do I Configure the Storage Duration of CTS Audit Logs to 180 Days?

Background

Audit logs may need to be stored for 180 days for query and backtracking purposes. You can perform the following steps to configure the storage duration of audit logs and query and analyze audit logs:

Procedure

• Configuring a transfer

After being enabled, CTS automatically creates a management tracker named **system** and records all operations of your tenant account in the tracker. Configure the tracker for CTS to transfer logs to Log Tank Service (LTS). After the configuration is complete, LTS creates a log group and a log stream automatically and stores CTS audit logs in the log stream for 30 days by default. To store them for 180 days, change the log retention duration setting of the log stream to 180 days on LTS.

- a. Log in to the management console.
 - If you log in to the console using a Huawei Cloud account, go to 3.
 - If you log in to the console as an IAM user, contact the administrator (Huawei Cloud account or a user in the user group **admin**) to grant the following permissions to the IAM user. For details, see .
 - CTS FullAccess
- b. Click \bigcirc in the upper left corner to select the desired region and project.
- c. Click in the upper left corner and choose Management & Governance > Cloud Trace Service.
- d. Click **Configure** in the **Operation** column of the **system** tracker to configure the tracker to transfer audit logs to LTS.

Figure 16-1 Configuring a tracker

 Titteder Name 1
 Status 1
 Titter Type 1
 Oppertudints Existed
 Status 2
 Status 2
 Operation
 Operation

 typem
 ® homat
 ® Managerett
 No
 USE CENtypen=3A
 April 102.25 Selfer Configse Deads
 Configse Deads

e. Enable **Transfer to LTS**. The system automatically creates a log group **CTS** and a log stream **system-trace** on LTS.

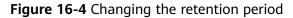
Figure 16-2 Transfer to LTS

| Basic Information — | —— 2 Configure Transfer —— | — (3) Preview and Finish |
|---------------------|----------------------------|--------------------------|
| * Transfer to OBS | | |
| * Transfer to LTS | | |
| * Log Group | CTS | |

- f. Go to the LTS console, change the storage duration of LTS log streams to 180 days, and configure the structuring rule to CTS.
 - i. Click in the upper left corner and choose **Management & Governance** > **Log Tank Service** to access the LTS console.
 - ii. On the **Log Management** page, click the modifying button in the **Operation** column of the **system-trace** log stream created in **e**. On the displayed page, enable **Log Retention Duration** and change the duration to 180 days.

Figure 16-3 Modifying the log stream

| Log Tank Service | | | • Warning 0 | Oct 12, 2023 11:08:03.544 GMT+08:00 |
|--|---|--|---|-------------------------------------|
| Dashboards Bata Alarms | Log Applications | | Enter a ke | word. Q |
| Log Ingestion Host Management Log Transfer | ELB Log Center ELB layer-7 access log analysis | APIG Log Center APIG access log analysis | VPC Flow Log Center VPC log analysis | |
| Log Jobs Beta | Log Groups Q. Log Stream Name/ID: system-trace 0 | Click here to choose a filler condition | | × C d |
| | Log Group Name | Remark | Log Streams Tags | Operation |
| | ∧ CTS | | 5 | Modity Delete Details |
| | Create Log Stream Q Log Stream | n Name/ID: system-trace 3 Click here to choose a tiller co | andilion | X All Enterprise Pr * |
| | Log Stream Name Ro | emark Enterprise P Tags | Metric Filters Billing | Operation |
| | system-trace | | | 32 🗘 🕆 🕁 🖘 |



| | | | • Wa | Log Group Name | CTS | | |
|-----------------------------|---------------------------|---|---|--------------------------|-------------------------|--|----------------------------------|
| | | | | Log Stream Name | system-trace | | |
| .og Applications | | | | | The log stream name ca | annot be the same as the name or origi | inal name of another log stream. |
| | | | | Original Log Stream Name | system-trace | | |
| ELB Log Center | | APIG Log Center APIG access log analysis | VPC Flow Log Center VPC log analysis | Log Stream ID | e4789eab-458e-4c | 94-803a-62d7bfc4fd7b | |
| | | | | Enterprise Project Name | default | | |
| Log Groups | | | | Log Retention Duration | () () 180 | | |
| | | | | | | n duration to 1 to 365 days. Logs that e ransfer logs to OBS buckets. | exceed the duration are deleted. |
| Q Log Stream Name/ID: syste | m-trace Click here to cho | | | Hot/Cold Tiered Storage | | | |
| Log Group Name | | Remark | Log Streams Ta | | To enable this smart op | tion, data must be stored for over 30 da | iys. |
| ∧ CTS | | | 5 | Anonymous Write | | | |
| Create Log Stream Q | Log Stream Name/ID: sy: | stem-trace O Click here to choose a f | Ber condition | | | is to logs reported by Android, iOS, app mous write is allowed for the log stream generate dirty data. | |
| Log Stream Name | Remark | Enterprise P Tags | Metric Filters Billing | | | | |
| system-trace | | default | | Tag | Key | Value | Operation |
| | | | | | + Add Tags You ca | n add 20 more tags. (System tags not i | ncluded) Learn more |
| | | | | Remark | | | |
| | | | | | | | |
| | | | | | | | 0/1024 |

iii. Choose Log Ingestion and click CTS (Cloud Trace Service). On the displayed page, select CTS for Log Group and system-trace for Log Stream.

Figure 16-5 Selecting a log stream

| < Ingest Log | | | |
|----------------------|---|------------------------------|---|
| Select Log Stream —— | (2) Configure CTS | — (3) Configure Log Stream — | (4) Finish |
| (8) | Type CTS (Cloud Trace Service Is CTS audit logs. CTS logs record clo | | aces for security compliance analysis. Learn more |
| Log Group | СТS | • | C Create Log Group |
| Log Stream | system-trace | v | C Create Log Stream |

- iv. Click **Next: Configure Log Stream** to configure the CTS log structuring.
- v. Click **Submit** to complete the log ingestion configuration.
- vi. Click Log Streams. The log stream details page is displayed.

Figure 16-6 Log stream details

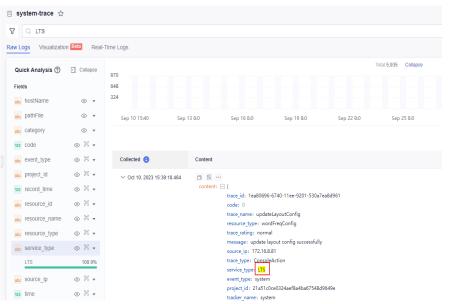
| < CTS - | | | | | | | | | | |
|-----------------------------------|------------------------|-------------------|-------------------------------------|--|----------------------|-------------------------------|----------|-----------|--------------|---------------|
| Log Stream Favorited Quick Search | < system-trace 0 | | | | | | | | | \rightarrow |
|), Enter a log stream name. | ⊜ system-trace ☆ | | | | | | Q 4 0 | 🗎 30 days | (From now) • | 0 . |
| Its-topic-6ax3 | Q. Enter a keyw | ord in the log. E | ract or fuzzy search by keyword. Ex | ample: "error", "er?or", "rro"", "er"r" | | | | | 0 5 | Search |
| Its-lopic-Bzo | Raw Logs Visualization | n Betal Real | Time Logs | | | | | | | |
| Its-topic-rivos | Quick Analysis 🗇 | Collapse | 176 | | Tota | 101,901 Collapse | | | | |
| stream-tuodi | Fields | | 17K | | | | | .11 | 111 | |
| system-trace | 🙀 hostP | ⊚ * | 6K | | | | | | | |
| | kostName | ۰ * | Sep 10 17:29 Sep 13 8:0 | Sep 16 8:0 Sep 19 8:0 | Sep 22 8/0 | Sep 25 80 Sep 28 80 | Oct 18.0 | Oct 4 8:0 | Oct 7 8.0 | Oct 10 8.0 |
| | 🐹 pathFile | * | | | | | Default | avouts | • = 4 | |
| | ategory | • • | | | | | | | | |
| | tode | © X • | Collected 💿 | Content | | | | | | |
| | event_type | ⊛ו ∞ו | ✓ Oct 10, 2023 17:29:20.131 | 0 9 11 (0 12 old content: ⊖ (| Jis 0 | | | | | |
| | vec project_id | © N • | | trace_id: 7d8a0a98-674f- | 11ee-bca6-d9a18e4i | le24f | | | | |
| | resource id | © X • | | code: 302 trace_name: login | | | | | | |
| | resource_o | © N + | | resource_type: user trace rating: normal | | | | | | |
| | resource_type | © N • | | message: ("login")("user_ | ype":"iam user","log | in_protect"("status")"off"()) | | | | |
| | service_type | © X • | | source_ip: 114.116.14.44 trace_type: ConsoleActio | | | | | | |
| | source_ip | © X + | | service_type: IAM event_type: global | | | | | | |
| | us time | • 8 • | | project_id: 21a51c0ce032 resource_id: 211cc148894 | | | | | | |
| | 😹 trace_id | ⊗≋• | | tracker_name: system | | | | | | |
| | | | | time: 1696930160131 | | | | | | |

• Log search and analysis

After you configure audit log transferring to LTS, you can search for and analyze audit logs on LTS.

- Method 1: Enter **LTS** in the search box to search for logs.

Figure 16-7 Searching for logs



 Method 2: In the Quick Analysis area, locate service_type and click LTS to quickly search for logs.

Figure 16-8 Searching for logs

| Ē | sy | vstem-trace 🏠 | | | | | | | | |
|---|---|-------------------|-------------------|-------------------------|---|-------------------------|--|----------------------|------------------------|----------|
| | 7 | Q Enter a keyw | ord in the log. E | xact or fuzzy search by | keyword. Exan | nple: "error", "er?or", | "ITO*", "er*r" | | | |
| R | aw Lo | ogs Visualization | n Beta Real- | Time Logs | | | | | | |
| | Quick Analysis ③ ① Collapse Total: 101,932 Collapse | | | | | | | | | |
| | Fiel | ds | | 11K | | | | | | |
| | abc | hostIP | ⊚ ▼ | 6K | | | | | | |
| | abc | hostName | • | Sep 10 17:32 | Sep 13 8:0 | Sep 16 8:0 | Sep 19 8:0 | Sep 22 8:0 | Sep 25 8:0 | Ser |
| | abc | pathFile | ⊚ ▼ | | | | | | | |
| | abc | category | • | | | | | | | |
| | 123 | code | ⊚ ≋ • | Collected 😌 | | Content | | | | |
| | abc | event_type | ⊚ 🕅 🔻 | ✓ Oct 10, 2023 17 | :32:11.487 | 0 6 … 0 | 🕑 🗟 old_ | lts 0 | | |
| | abc | project_id | ⊚ 🕅 🔻 | | | content: 🖃 { | d2 | aa afro od560622 | 947 | |
| | 123 | record_time | ⊚ 🕅 🔻 | | trace_id: e3adf5f6-674f-11ee-afc0-9d560b633847 code: 302 | | | | | |
| | abc | resource_id | ⊚ 🕅 🔻 | | | - | ame: login ce type: user | | | |
| | abc | resource_name | ⊚ 🕅 🔻 | | | trace_r | ating: normal | | | |
| | abc | resource_type | ⊚ ≋ • | | | | ge: {"login":{"user_t ip: 114.115.174.6 | /pe":"iam user","log | in_protect":{"status": | "off"}}} |
| | abc | service_type | ⊚ ≋ • | | | - | ype: ConsoleAction | | | |
| | | IAM | 86.01% | | | | type: IAM type: global | | | |
| | Г | LTS | 5.6% | | | | _id: 21a51c0ce0324 ce_id: 211cc148894 | | | |
| | L | AOM | 3.67% | | | | _name: system | 9401807 UE 10074280 | 11201 | |
| | | • | | | | time: | 1696930331487 | | | |

- Method 3: Enter a SQL statement in **Visualization** to filter audit logs and calculate the total number of audit logs.

Figure 16-9 Querying logs using a SQL statement

| ⊟ system-trace ☆ | | | | | | | | | |
|------------------------------------|--|--|--|--|--|--|--|--|--|
| 1 SELECT count(*) where "service_t | 1 SELECT count(*) where "service_type"='LTS' | | | | | | | | |
| Raw Logs Visualization Beta | Real-Time Logs | | | | | | | | |
| +Ə Fields | Ø | | | | | | | | |
| Enter a field name. Q | | | | | | | | | |
| | First 100 log events by default ? | | | | | | | | |
| time | EXPR\$0 | | | | | | | | |
| code | 4,015.00 | | | | | | | | |
| T project_id | 8 | | | | | | | | |
| record_time | ±%u | | | | | | | | |
| T resource_id | 0 | | | | | | | | |

17 What Should I Do If I Cannot Enable CTS as an IAM User?

Background

If you fail to enable CTS as an IAM user, perform the following steps.

Procedure

Step 1 Check whether the IAM user has the permission.

If yes, go to Step 2.

If no, contact the CTS administrator (Huawei Cloud account or a user in user group **admin**) to grant the CTS FullAccess permission to the IAM user. For details, see **Assigning Permissions to an IAM User**.

Step 2 If the IAM user has the permission but cannot enable CTS, check whether CTS has been enabled in the central region. If not, enable CTS in the central region using the Huawei Cloud account.

----End

18 How Do I Enable Alarm Notifications for EVS?

Background

You can perform the following steps to enable alarm notifications for Elastic Volume Service (EVS) operations.

Procedure

Step 1 Log in to the CTS console, click **Key Event Notifications** on the left, and click **Create Key Event Notification** in the upper right corner.

| Cloud Trace Service | Key Event Notifications ③ | | | | 👳 Procedur | e for Using CTS Create Key Event Notification |
|----------------------------|---|------------|-----------------|------------------------------------|--|---|
| Trace List Tracker List | You can create 85 more notifications. Q Search or filter by keyword. | | | | | C |
| Key Event Notifications | Notification Name \$ | Status 💠 | Template Type 💠 | SMN Topic 💠 | Advanced Filter Conditions \Leftrightarrow | Operation |
| | xunjian_keyOperateInfo_IFv1e | Disabled | Custom | - | - | Enable Modity Delete |
| | keyOperate_KsZewtQmMD | Enabled | Custom | um:smn:cn-north-4.21a51c0ce0324aef | - | Disable Modify Delete |
| | keyOperate_info_jkem | O Disabled | All | - | - | Enable Modify Delete |

Step 2 In the **Operation** area, select **Custom** for **Operation Type**, and select **EVS**, **evs**, and the four key operations from the **Operation List** drop-down lists to enable alarm notifications for EVS operations.

| Key Event Notification | S Sack to Key Event Not | ification List | | | |
|---|---------------------------------------|-------------------------------|-------------|--|-----|
| Basic Information | keyOperate_info_6t9p | | | | |
| Operation SMN notifications will be se Operation Type | ent when specified operations are | e performed. | | | |
| Operation List | EVS You can add 100 services or 10 | evs 00 operations. Learn more | • | createVolume updateVolume createVolume | Add |
| | Service Type | Resource Type | Operation I | updateVolume extendVolume deleteVolume | |

----End