Cloud Trace Service

Getting Started

Issue	01
Date	2023-11-24

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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 Overview

Scenarios

If you log in to Cloud Trace Service (CTS) for the first time, click **Enable CTS** on the **Tracker List** page. A management tracker named **system** will be automatically created. Then you can create data trackers on this page. Th management tracker identifies and associates with all cloud services your tenant account is using, and records all operations of your tenant account. Data trackers record details of the tenant's operations on data in OBS buckets.

You can only query operation records of the last seven days on the CTS console. To store operation records for more than seven days, you must configure an OBS bucket to transfer records to it. Otherwise, you cannot query the operation records generated seven days ago.

Associated Services

- OBS: used to store trace files.

  NOTE

  You must select a standard OBS bucket because CTS needs to frequently access the OBS bucket that stores traces.

- Data Encryption Workshop (DEW): Provides keys that can be used to encrypt trace files.
- LTS: stores logs.
- SMN: Sends email or SMS message notifications to users when key operations are performed.

Enabling CTS for the First Time

Step 1 Log in to the management console.

Step 2 If you log in to Huawei Cloud as an administrator, go to **Step 3**. If you log in to Huawei Cloud as an IAM user, first contact your CTS administrator (account owner or a user in the **admin** user group) to obtain the **CTS FullAccess** permissions.

For details, see **Assigning Permissions to an IAM User**.

Step 3 Click  in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.

Step 4 Choose **Tracker List** in the navigation pane on the left and click **Enable CTS** in the upper right corner. A management tracker named **system** will be automatically created. The management tracker records management traces, which are operations on all cloud resources, such as creation, login, and deletion.

Step 5 Create trackers (data trackers only). Data trackers record details of the tenant's operations on data in OBS buckets.

Step 6 Choose **Tracker List** in the navigation pane on the left to view operation records of the last seven days.

----End

2 Querying Real-Time Traces

Scenarios

After you enable CTS and the management tracker is created, CTS starts recording operations on cloud resources. After a data tracker is created, the system starts recording operations on data in OBS buckets. CTS stores operation records generated in the last seven days.

This section describes how to query and export operation records of the last seven days on the CTS console.

- **Viewing Real-Time Traces in the Trace List of the New Edition**
- **Viewing Real-Time Traces in the Trace List of the Old Edition**

Constraints

- Traces of a single account can be viewed on the CTS console. Multi-account traces can be viewed only on the **Trace List** page of each account, or in the OBS bucket or the **CTS/system** log stream configured for the management tracker with the organization function enabled.
- You can only query operation records of the last seven days on the CTS console. To store operation records for more than seven days, you must configure an OBS bucket to transfer records to it. Otherwise, you cannot query the operation records generated seven days ago.
- After performing operations on the cloud, you can query management traces on the CTS console 1 minute later and query data traces on the CTS console 5 minutes later.

Viewing Real-Time Traces in the Trace List of the New Edition

1. Log in to the management console.
2. Click  in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. On the **Trace List** page, use advanced search to query traces. You can combine one or more filters.

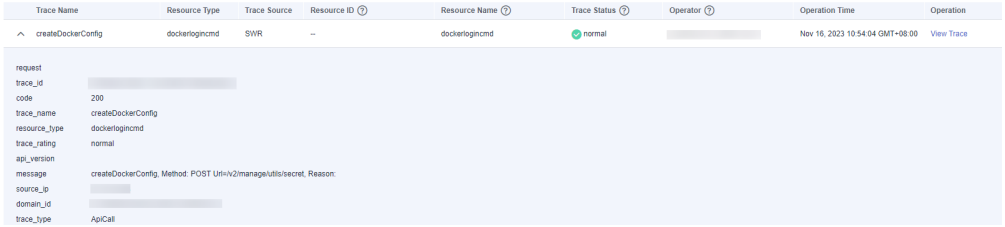
- **Trace Name**: Enter a trace name.
- **Trace ID**: Enter a trace ID.
- **Resource Name**: Enter a resource name. If the cloud resource involved in the trace does not have a resource name or the corresponding API operation does not involve the resource name parameter, leave this field empty.
- **Resource ID**: Enter a resource ID. Leave this field empty if the resource has no resource ID or if resource creation failed.
- **Trace Source**: Select a cloud service name from the drop-down list.
- **Resource Type**: Select a resource type from the drop-down list.
- **Operator**: Select one or more operators from the drop-down list.
- **Trace Status**: Select **normal**, **warning**, or **incident**.
  - **normal**: The operation succeeded.
  - **warning**: The operation failed.
  - **incident**: The operation caused a fault that is more serious than the operation failure, for example, causing other faults.
- Time range: Select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range.

5. On the **Trace List** page, you can also export and refresh the trace list, and customize the list display settings.
   - Enter any keyword in the search box and click to filter desired traces.
   - Click **Export** to export all traces in the query result as an .xlsx file. The file can contain up to 5000 records.
   - Click to view the latest information about traces.
   - Click to customize the information to be displayed in the trace list. If **Auto wrapping** is enabled ( ), excess text will move down to the next line; otherwise, the text will be truncated. By default, this function is disabled.
6. For details about key fields in the trace structure, see **Trace Structure** and **Example Traces**.
7. (Optional) On the **Trace List** page of the new edition, click **Go to Old Edition** in the upper right corner to switch to the **Trace List** page of the old edition.

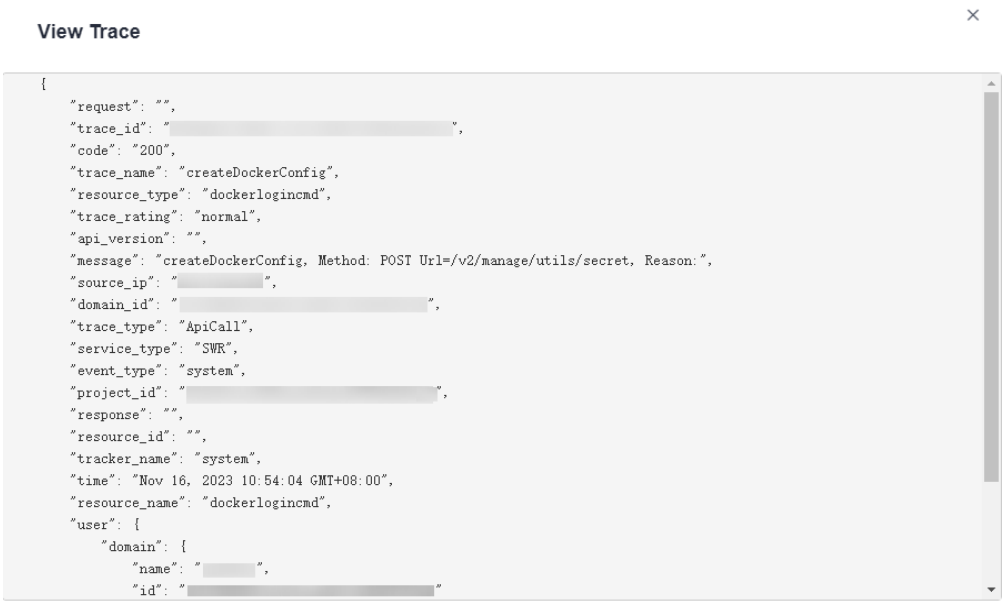
Viewing Real-Time Traces in the Trace List of the Old Edition

1. Log in to the management console.
2. Click in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. Each time you log in to the CTS console, the new edition is displayed by default. Click **Go to Old Edition** in the upper right corner to switch to the trace list of the old edition.

5. Set filters to search for your desired traces. The following filters are available:
   - **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**: Select a filter from the drop-down list.
     - If you select **Resource ID** for **Search By**, specify a resource ID.
     - If you select **Trace name** for **Search By**, specify a trace name.
     - If you select **Resource name** for **Search By**, specify a resource name.
   - **Operator**: Select a user.
   - **Trace Status**: Select **All trace statuses**, **Normal**, **Warning**, or **Incident**.
   - Time range: You can query traces generated during any time range in the last seven days.
   - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5000 records.
6. Click **Query**.
7. On the **Trace List** page, you can also export and refresh the trace list.
   - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5000 records.
   - Click to view the latest information about traces.
8. Click on the left of a trace to expand its details.



9. Click **View Trace** in the **Operation** column. The trace details are displayed.



10. For details about key fields in the trace structure, see **Trace Structure** and **Example Traces**.

11. (Optional) On the **Trace List** page of the old edition, click **New Edition** in the upper right corner to switch to the **Trace List** page of the new edition.

3 Querying Archived Traces

Scenarios

CTS periodically sends trace files to OBS buckets. A trace file is a collection of traces. CTS generates trace files based on services and transfer cycle, and adjusts the number of traces contained in each trace file as needed. CTS can also save audit logs to LTS log streams.

This section describes how to view historical operation records in trace files downloaded from OBS buckets and in LTS log streams.

Prerequisites

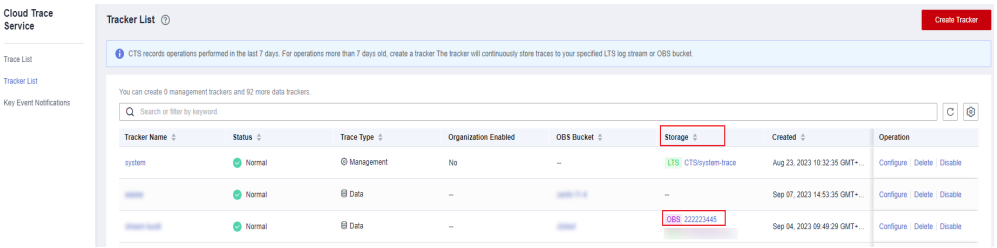
You have configured a tracker in CTS and enabled **Transfer to OBS** or **Transfer to LTS**. For details, see **Configuring a Tracker**.

Querying Traces Transferred to OBS

If you enable **Transfer to OBS** when configuring the tracker, traces will be periodically transferred to a specified OBS bucket as trace files for long-term storage.

1. Log in to the management console.
2. Click ☰ in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Tracker List** in the navigation pane on the left.
4. Click a bucket in the **OBS Bucket** column.

Figure 3-1 Selecting an OBS bucket



5. In the OBS bucket, locate the file storage path to view the desired trace, and click **Download** on the right to download the file to the default download path of the browser. If you need to save it to a custom path, click **More** > **Download As** on the right.
   - The trace file storage path is as follows:

     OBS bucket name > CloudTraces > Region > Year > Month > Day > Tracker name > Service directory

     An example is ***User-defined name > CloudTraces > region > 2016 > 5 > 19 > system > ECS***.
   - The trace file naming format is as follows:

     Trace file prefix_CloudTrace_Region/Region-project_Time when the trace file was uploaded to OBS: Year-Month-DayTHour-Minute-SecondZ_Random characters.json.gz

     An example is ***File Prefix*_CloudTrace_region-project_2016-05-30T16-20-56Z_21d36ced8c8af71e.json.gz**.

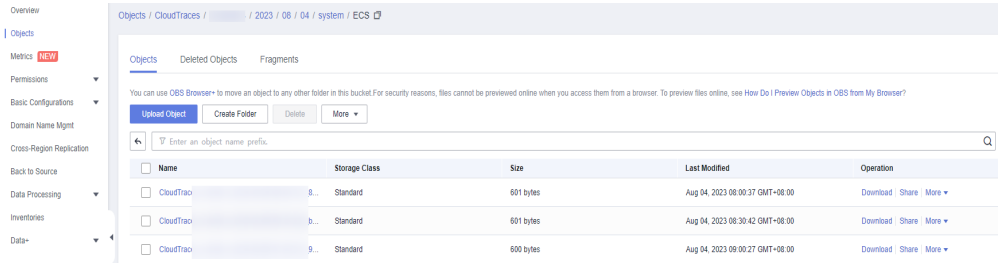
   NOTE

   The OBS bucket name and trace file prefix are user-defined, and other parameters are automatically generated.

   Downloading the file will incur request fees and traffic fees.

   For details about key fields in the CTS trace structure, see **Trace Structure** and **Example Traces**.

   Figure 3-2 Viewing trace file content



6. Decompress the downloaded package to obtain a JSON file with the same name as the package. Open the JSON file using a text file editor to view traces.

Querying Traces Transferred to LTS

If you enable **Transfer to LTS** when configuring a tracker, traces will be transferred to the **CTS/*{Tracker Name}*** log stream for long-term storage. *{Tracker Name}* indicates the name of the current tracker. For example, the log stream path of the management tracker is **CTS/system-trace**.

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.

Step 3 Choose **Tracker List** in the navigation pane on the left.

Step 4 Click an LTS log stream in the **Storage** column.

Step 5 On the **Log Stream** tab page in the **CTS** log group page, select the *{Tracker name}* log stream to view trace logs.

For details about key fields in the CTS trace structure, see **Trace Structure** and **Example Traces**.

Step 6 Click to download the log file to your local PC.

NOTE

Each time you can download up to 5000 log events. If the number of selected log events exceeds 5000, you cannot download them directly from LTS. Transfer them to OBS and then download them from OBS.

----End

4 Configuring Key Event Notifications

You can create key event notifications on CTS so that SMN sends you SMS, email, or HTTP/HTTPS notifications of key events. This function is triggered by CTS, and notifications are sent by SMN. SMN sends key event notifications to subscribers. Before setting notifications, you need to know how to create topics and add subscriptions on the SMN console.

Scenarios

You can use this function for:

- Real-time detection of high-risk operations (such as VM restart and security configuration changes), cost-sensitive operations (such as creating and deleting expensive resources), and service-sensitive operations (such as network configuration changes).
- Detection of operations such as login of users with admin-level permissions or operations performed by users who do not have the required permissions.
- Connection with your own audit system: You can synchronize all audit logs to your audit system in real time to analyze the API calling success rate, unauthorized operations, security, and costs.

Prerequisites

- SMN sends key event notifications to subscribers. Before setting notifications, you need to know how to create topics and add subscriptions on the SMN console.
- You can create up to 100 key event notifications on CTS:
  - Specify key operations, users, and topics to customize notifications.
  - Complete key event notifications can be sent to notification topics.
- If CTS and Cloud Eye use the same message topic, they can receive messages from the same terminal but with different content.
- You can configure one key event notification for operations initiated by a maximum of 50 users in 10 user groups. For each key event notification, you can add users from different user groups, but cannot select multiple user groups at once.

Creating a Key Event Notification

1. Log in to the management console.
2. Click  in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.
3. In the navigation pane on the left, choose **Key Event Notifications**.

   The **Key Event Notifications** page is displayed.
4. Click **Create Key Event Notification**. On the displayed page, specify required parameters.
5. Enter a key event notification name.

   Notification Name: Identifies key event notifications. This parameter is mandatory. The name can contain up to 64 characters. Only letters, digits, and underscores (_) are allowed.
6. Configure key operations.

   Select the operations that will trigger notifications. When a selected operation is performed, an SMN notification is sent immediately.

   - **Operation Type**: Select **All** or **Custom**.
     - **All**: This option is suitable if you have connected CTS to your own audit system. When **All** is chosen, you cannot deselect operations because all operations on all cloud services that have connected with CTS will trigger notifications. You are advised to use an SMN topic for which HTTPS is selected.
     - **Custom**: This option is suitable for enterprises that require detection of high-risk, cost-sensitive, service-sensitive, and unauthorized operations. You can connect CTS to your own audit system for log analysis.

       Customize the operations that will trigger notifications. Up to 1000 operations of 100 services can be added for each notification. For details, see **Supported Services and Operations**.
   - **Advanced Filter**: You can set an advanced filter to specify the operations that will trigger notifications. Operations can be filtered by fields **api_version**, **code**, **trace_rating**, **trace_type**, **resource_id**, and **resource_name**. Up to six filter conditions can be set. When you configure multiple conditions, specify whether an operation is considered a match when all conditions are met (AND) or any of the conditions are met (OR).
7. Configure users.

   SMN messages will be sent to subscribers when the specified users perform key operations.

   - If you select **All users**, SMN will notify subscribers of key operations initiated by all users.
   - If you select **Specified users**, SMN will notify subscribers of key operations initiated by your specified users. You can configure key event notifications on operations for up to 50 users in 10 user groups. For each notification, you can select multiple users in the same user group.
8. Configure an SMN topic.

- When **Yes** is selected for **Send Notification**:
  - **Create a cloud service agency.**: (Mandatory) If you select this check box, CTS automatically creates a cloud service agency when you create a key event notification. The agency authorizes you to use SMN.
  - **SMN Topic**: You can select an existing topic or click **SMN** to create one on the SMN console.
- If you do not want to send notifications, no further action is required.

9. Click **OK**.

Managing Key Event Notifications

After you create a key event notification, you can view its name, status, template, and SMN topic in the notification list and delete it as required.

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.

Step 3 Choose **Key Event Notifications** in the navigation pane on the left. On the displayed page, perform the following operations as required. For details, see **Table 4-1**.

Table 4-1 Related operations

Operation	Description
Viewing a key event notification	Click the notification name to view the operation list and user list details of the notification.
Enable/ Disable a key event notification	Click **Enable** or **Disable** in the **Operation** column. **NOTE** CTS can trigger key event notifications only after SMN is configured.
Modifying a key event notification	Click **Modify** in the **Operation** column to modify the configuration of the key event notification.
Deleting a key event notification	Click **Delete** in the **Operation** column.

Operation	Description
Searching for a notification	In the search box above the list, you can search for notifications by notification name, status, template type, or SMN topic.
Refreshing the key event notification list	Click  in the upper right corner.
Configuring basic settings	Click  in the upper right corner to set table text wrapping, fixed operation column position, and custom columns.

----End

5 Common Practices

After completing basic operations such as viewing traces and configuring trackers, you can implement common practices based on this section.

Table 5-1 Common practices

Practice	Description
Auditing and Analyzing Logins and Logouts with FunctionGraph	This practice describes how to use CTS to collect real-time records of operations on cloud resources. Obtain operation records of subscribed cloud resources with a CTS trigger, analyze and process the records using a custom function, and report alarms. Then, use Simple Message Notification (SMN) to push alarm messages to service personnel by SMS or email.

