

Cloud Trace Service

Getting Started

Date **2022-09-30**

Contents

1 Enabling CTS.....	1
2 Querying Real-Time Traces.....	3
3 Querying Archived Traces.....	5
4 Configuring Key Event Notifications.....	7

1 Enabling CTS

Scenarios

You need to enable Cloud Trace Service (CTS) before using it to record operations on resources. After being enabled, CTS automatically creates a management tracker named **system** and records all operations of your tenant account in the tracker. CTS displays traces generated in the last seven days. To store traces for a long time, you can transfer them to Object Storage Service (OBS). Ensure that you have enabled OBS and have full permissions for the OBS bucket you are going to use.

This section describes how to enable CTS.

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.
- Simple Message Notification (SMN): Sends email or SMS message notifications to users when key operations are performed.

Procedure

Step 1 Log in to the management console.

Step 2 If you have logged in as an account administrator, go to **Step 3** directly. If you have logged in as an IAM user, first contact your administrator (account owner, a user in the admin user group, or a user who has been granted the **Security Administrator** permissions) to obtain the following permissions:

- Security Administrator
- CTS FullAccess

For details, see [Assigning Permissions to an IAM User](#).


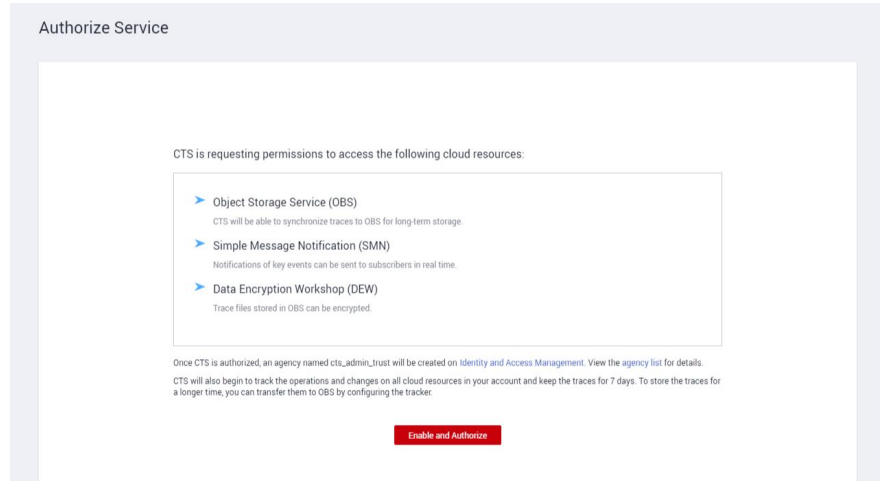
Step 3 Click  in the upper left corner and choose **Management & Deployment > Cloud Trace Service**. The CTS authorization page is displayed.

Figure 1-1 Enabling CTS



Step 4 Click **Enable and Authorize**.

 **NOTE**

After you enable CTS, two trackers are automatically created to record management traces, which are operations (such as creation, login, and deletion) performed on all cloud resources.

- In the current region, a tracker is created to record management traces of all project-level services deployed in this region.
- In the EU-Dublin region, a tracker is created to record management traces of all global services, such as IAM.

When using CTS, you only need the required permissions for relevant operations, but do not need the **Security Administrator** permissions.

----End



2 Querying Real-Time Traces

Scenarios

After CTS is enabled, the tracker starts recording operations on cloud resources and data in OBS buckets. CTS stores operation records for the last seven days.

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

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and choose **Management & Deployment > Cloud Trace Service**. The CTS console is displayed.
3. In the navigation pane on the left, choose **Trace List**.
4. Specify the search criteria as needed.
 - Search time range: In the upper right corner, choose **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range.
 - **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 **Data** for **Trace Type**, you can only filter traces by tracker.
 - **Operator**: Select one or more operators from the drop-down list.
 - **Trace Status**: Select **All trace statuses**, **Normal**, **Warning**, or **Incident**.
5. Click **Query**.
6. Click **Export** on the right to export all traces in the query result as a CSV file. The file can contain up to 5000 records.
7. Click  on the left of a trace to expand its details.

Trace Name	Resource Type	Trace Source	Resource ID	Resource Name	Trace Status	Operator	Operation Time	Operation
login	user	IAM			normal		Dec 24, 2021 14:16:15 GMT+08:00	View Trace

code	302
source_id	
trace_type	ConsoleAction
event_type	global
project_id	
trace_id	
trace_name	login
resource_type	user
trace_status	normal
service_type	IAM
resource_id	
tracker_name	system
time	Dec 24, 2021 14:16:15 GMT+08:00
resource_name	
resource_time	Dec 24, 2021 14:16:15 GMT+08:00
user	

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

View Trace ✕

```
{
  "trace_id": "df201462-8373-11e9-a4db-c3ac3c023b88",
  "code": "302",
  "trace_name": "logout",
  "resource_type": "user",
  "trace_rating": "normal",
  "source_ip": "-",
  "service_type": "IAM",
  "trace_type": "SystemAction",
  "event_type": "system",
  "resource_id": "f3f18b9215014f0d9ded3045af020811",
  "tracker_name": "system",
  "time": "May 31, 2019 15:15:29 GMT+08:00",
  "resource_name": "██████████",
  "record_time": "May 31, 2019 15:15:29 GMT+08:00",
  "user": {
    "name": "██████████",
    "id": "f3f18b9215014f0d9ded3045af020811",
    "domain": {
      "name": "██████████",
      "id": "2306579dc99f4c8690b14b68e734fcd9"
    }
  }
}
```

For details about key fields in the trace structure, see section "Trace Structure" in the *Cloud Trace Service User Guide* and section "Example Traces" in the *Cloud Trace Service User Guide*.

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.

This section describes how to obtain historical operation records from trace files downloaded from the OBS bucket.

Prerequisites

You have configured a tracker. For details, see section "Configuring a Tracker" in the *Cloud Trace Service User Guide*.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and choose **Management & Deployment > 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.
5. Select the target trace by choosing in sequence an OBS bucket, the **CloudTraces** directory, a region, a year, a month, a day, a tracker name, and a service directory. Download the trace file to the default path by clicking Download in the Operation column. To download the trace file to a customized path, click **More > Download As**.
 - 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-DayT Hour-Minute-SecondZ_Random characters.json.gz

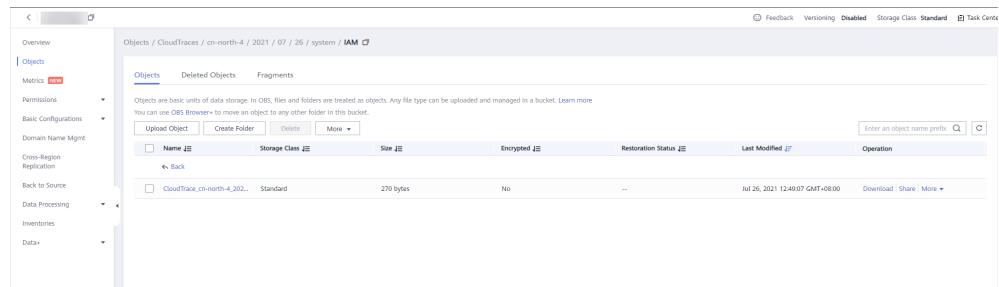
An example is ***File Prefix_CloudTrace_region_2016-05-30T16-20-56Z_21d36ced8c8af71e.js on.gz***.

 **NOTE**

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

For details about key fields in the CTS trace structure, see section "Trace Structure" in the *Cloud Trace Service User Guide* and section "Example Traces" in the *Cloud Trace Service User Guide*.

Figure 3-1 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.

4 Configuring Key Event Notifications

Scenarios


You can create key event notifications on CTS so that Simple Message Notification (SMN) sends you notifications of key events. This function is triggered by CTS, and notifications are sent by SMN. 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.
- Currently, you can create up to 100 key event notifications on CTS and specify key operations, users, and topics for each notification. Complete key event notifications and typical key event notifications can be sent to specified users and notification topics.
- If CTS and Cloud Eye use the same message topic, they will send messages to the same targets, but the message contents will be different.
- 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.
- You can select up to 1000 key operations of 100 cloud services for each notification.
- More configurations and more powerful functions are provided for key event notifications.

Creating a Key Event Notification


1. Log in to the management console.
2. Click  in the upper left corner and choose **Management & Deployment > 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.
 - **Operation Type:** Select **All**, **Typical**, 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.
Select the operations that will trigger notifications. Up to 1000 operations of 100 services can be added for each notification. For details, see section "Supported Services and Operations" in the *Cloud Trace Service User Guide*.
 - **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.
 - If you select **Yes** for **Send Notification**, you can select an existing topic or click **Topic** to create one on the SMN console.

- If you do not want to send notifications, no further action is required.
9. Click **OK**.


View Key Event Notification

1. Log in to the management console.
2. Click  in the upper left corner and choose **Management & Deployment > 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 **View** in the **Operation** column. The **View Key Event Notifications** page is displayed.


Enable Key Event Notification

1. Log in to the management console.
2. Click  in the upper left corner and choose **Management & Deployment > 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 **Start** in the **Operation** column. The **Enabling Key Event Notifications** page is displayed.
5. Click **Yes** to enable the key event notification function.

Modifying a Key Event Notification

1. Log in to the management console.
2. Click  in the upper left corner and choose **Management & Deployment > 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 **More > Modify** in the **Operation** column. The **Key Event Notifications** page is displayed.
5. Then, click **OK**.

Deleting a Key Event Notification

1. Log in to the management console.
2. Click  in the upper left corner and choose **Management & Deployment > 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. Choose **More > Delete** in the **Operation** column. The **Delete Key Event Notifications** page is displayed.
5. Click **Yes** to delete the key event notification function.