

# Cloud Trace Service

## User Guide

**Issue** 01  
**Date** 2025-01-17



**Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2025. 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**



HUAWEI 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

---

<b>1 Overview</b>	<b>1</b>
<b>2 Querying Traces</b>	<b>3</b>
2.1 Querying Real-Time Traces	3
2.2 Querying Transferred Traces	6
<b>3 Management Trackers</b>	<b>10</b>
3.1 Creating a Tracker	10
3.2 Configuring a Tracker	10
3.3 Disabling or Enabling a Tracker	15
3.4 Deleting a Tracker	16
<b>4 Data Trackers</b>	<b>18</b>
4.1 Creating a Tracker	18
4.2 Configuring a Tracker	21
4.3 Disabling or Enabling a Tracker	24
4.4 Deleting a Tracker	25
<b>5 Organization Trackers</b>	<b>27</b>
5.1 Overview	27
5.2 Setting CTS as a Trusted Service	28
5.3 Configuring an Organization Tracker	29
<b>6 Creating a Key Event Notification</b>	<b>34</b>
<b>7 Application Examples</b>	<b>39</b>
7.1 Security Auditing	39
7.2 Fault Locating	41
7.3 Resource Tracking	43
<b>8 Trace References</b>	<b>45</b>
8.1 Trace Structure	45
8.2 Example Traces	50
<b>9 Cross-Tenant Transfer Authorization</b>	<b>54</b>
<b>10 Verifying Trace File Integrity</b>	<b>59</b>
10.1 Enabling Verification of Trace File Integrity	59
10.2 Digest Files	60

---

10.3 Verifying Trace File Integrity.....	63
<b>11 Auditing.....</b>	<b>69</b>
<b>12 Permissions Management.....</b>	<b>70</b>
<b>13 Quota Management.....</b>	<b>72</b>
<b>14 Supported Services and Operations.....</b>	<b>73</b>

# 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. The 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 Traces

---

## 2.1 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.
  - **Enterprise Project ID:** Enter an enterprise project ID.
  - **Access Key:** Enter an access key ID, including temporary access credentials and permanent access keys.
  - **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 press Enter 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.

Trace Name	Resource Type	Trace Source	Resource ID	Resource Name	Trace Status	Operator	Operation Time	Operation
createDockerConfig	dockerlogincmd	SWR	-	dockerlogincmd	normal		Nov 16, 2023 10:54:04 GMT+08:00	<a href="#">View Trace</a>

request

trace\_id

code 200

trace\_name createDockerConfig

resource\_type dockerlogincmd

trace\_rating normal

api\_version

message createDockerConfig, Method: POST URI=/v2/managerultrasecret, Reason:

source\_ip

domain\_id


trace\_type ApiCall

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

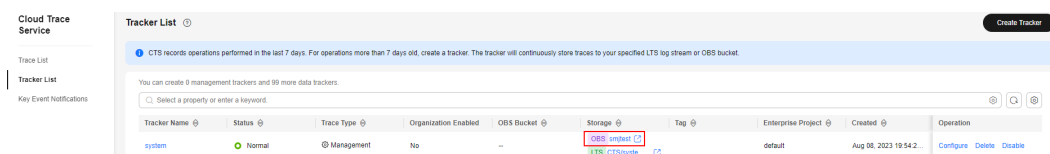


## Querying Traces Transferred to OBS

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.
4. Click a bucket in the **OBS Bucket** column.

**Figure 2-1** 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-DayT Hour-Minute-SecondZ\_Random characters.json.gz*

Example: *File prefix\_CloudTrace\_region-project\_2016-05-30T16-20-56Z\_21d36ced8c8af71e.json.gz*

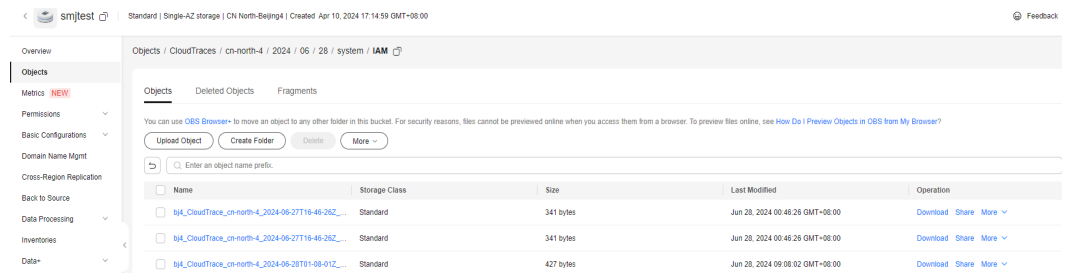
### NOTE

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 2-2 Viewing trace file content



- Decompress the downloaded package to obtain a JSON file with the same name as the package, as shown in Figure 2-3. Open the JSON file using a text file editor to view traces.

Figure 2-3 JSON file

```


1 [{"time": 1491482332020,
2  "user": {
3    "id": "59c402916547e0d470b56c41dfc939",
4    "name": "*****",
5    "domain": {
6      "name": "*****",
7      "id": "0027bc42d1ab46a69482a72cbfc039e02"
8    }
9  },
10 "request": {
11   "bucket_name": "obj-s70z",
12   "file_prefix_name": "-RAD",
13   "status": "disabled"
14 },
15 "response": {
16   "bucket_name": "obj-s70z",
17   "file_prefix_name": "-RAD",
18   "status": "disabled",
19   "tracker_name": "system"
20 },
21 "service_type": "CTS",
22 "resource_type": "tracker",
23 "resource_name": "system",
24 "source_ip": "*****",
25 "trace_name": "updateTracker",
26 "trace_type": "ConsoleAction",
27 "api_version": "1.0",
28 "request_time": 151141032895,
29 "trace_id": "75194f09-1a0c-11e7-80c0-3ab12929a6df",
30 "trace_status": "normal"
31 },
32 [{"time": 1491482332020,
33  "user": {
34    "id": "59c402916547e0d470b56c41dfc939",
35    "name": "*****",
36    "domain": {
37      "name": "*****",
38      "id": "0027bc42d1ab46a69482a72cbfc039e02"
39    }
40 },
41 "request": {
42   "bucket_name": "obj-s70z",
43   "file_prefix_name": "-RAD",
44   "status": "disabled"
45 },
46 "response": {
47   "bucket_name": "obj-s70z",
48   "file_prefix_name": "-RAD",
49   "status": "disabled",
50   "tracker_name": "system"
51 },
52 "service_type": "CTS",
53 "resource_type": "tracker",
54 "resource_name": "system",
55 "source_ip": "*****",
56 "trace_name": "updateTracker",
57 "trace_type": "ConsoleAction",
58 "api_version": "1.0",
59 "request_time": 151141032921,
60 "trace_id": "76831b09-1a0c-11e7-99cf-1109e2f246d0f",
61 "trace_status": "normal"
62 }]]

```

## 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**.

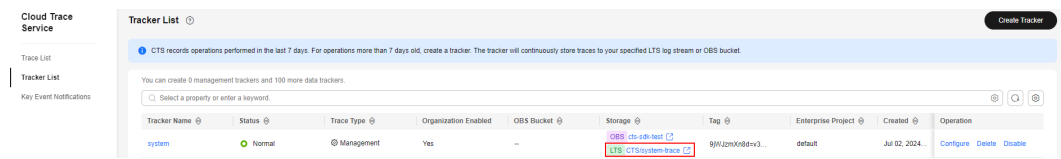
**Step 1** Log in to the management console.

**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.


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

**Figure 2-4** Selecting an LTS log stream



**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 5,000 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

# 3 Management Trackers

---

CTS provides two types of trackers: a management tracker and multiple data trackers. The management tracker records management traces, which are operations on all cloud resources, such as creation, login, and deletion. Data trackers record data traces, which are operations performed by tenants on data in OBS buckets, such as upload and download.

This section describes how to use the management tracker.

## 3.1 Creating a Tracker

If you log in to CTS for the first time, click **Enable CTS** on the **Tracker List** page. A management tracker named **system** will be automatically created. The management tracker identifies and associates with all cloud services your tenant account is using, and records all operations of your tenant account.

### NOTE

- CTS records operations performed in the last seven days. To store traces for a longer time, configure a tracker. The tracker will store traces to your specified LTS log streams or OBS buckets.
- Each account can have only one management tracker. The stored historical traces are retained even after the management tracker is deleted. When you enable CTS again, the management tracker is restored.

## 3.2 Configuring a Tracker

### Scenario

You can configure the created management tracker to transfer traces recorded in CTS to OBS or LTS for long-term storage.

You can select whether to send recorded traces to an OBS bucket. You can also transfer the traces of multiple accounts to the same OBS bucket for centralized management.

**NOTE**

There are three storage classes of OBS buckets, Standard, Infrequent Access, and Archive. You must use Standard OBS buckets for trace transfer because CTS needs to frequently access the OBS buckets.

After the tracker configuration is complete, CTS will immediately start recording operations under the new settings.

This section describes how to configure the management tracker.

## Constraints

For global services, you must configure trackers on the CTS console in the central region (CN-Hong Kong). This configuration enables the function of transferring traces to OBS or LTS. The preceding function will not take effect if you perform the configuration on the CTS console in any region outside the central region.


For details about Huawei Cloud global services, see [Constraints](#).


## Prerequisites

You have enabled CTS.

## Configuring a Management Tracker

**Step 1** Log in to the management console.

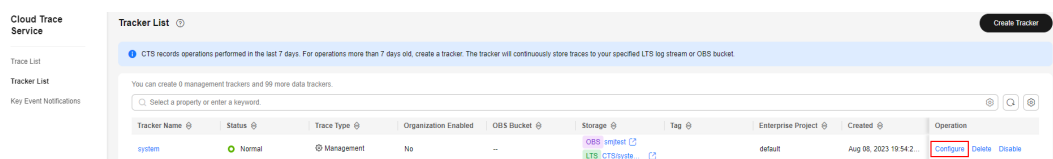
**Step 2** Click  in the upper left corner to select the desired region and project.

**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.

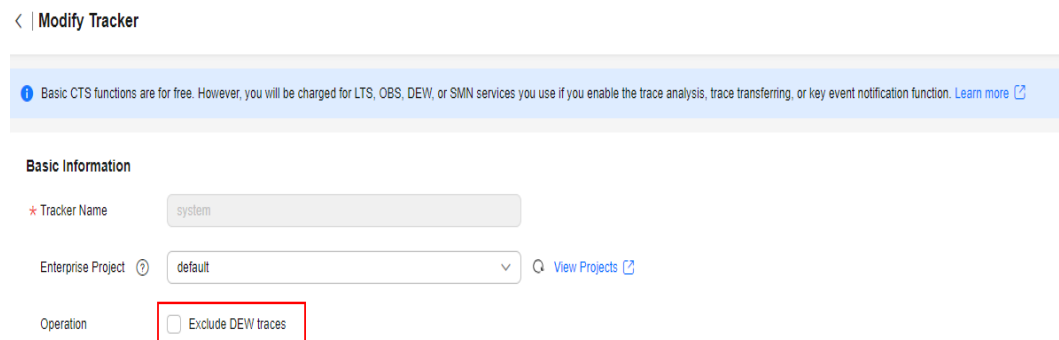
**Step 5** Click **Configure** in the **Operation** column in the row of the management tracker.

**Figure 3-1** Configuring the tracker



**Step 6** Configure the basic information of the tracker, and click **Next**.

**Figure 3-2** Excluding KMS traces



Parameter	Description
Tracker Name	The default value is <b>system</b> and cannot be changed.
Enterprise Project	Select an enterprise project. <b>NOTE</b> Enterprise projects allow you to manage cloud resources and users by project. For details about how to enable the enterprise project function, see <a href="#">Creating an Enterprise Project</a> .
Exclude KMS traces	Deselected by default. After this option is selected, the tracker will not transfer the data about user operations on Data Encryption Workshop (DEW). <b>NOTE</b> For details about DEW audit operations, see <a href="#">Operations supported by CTS</a> .

**Step 7** On the **Configure Transfer** page, configure the transfer parameters of the tracker. You can query operation records of the last seven days on the CTS console. To store and query operation records beyond seven days, transfer them to OBS or LTS. For details, see [Table 3-1](#) and [Table 3-2](#).

**Table 3-1** Parameters for configuring the transfer to OBS

Parameter	Description
Transfer to OBS	Select an existing OBS bucket or create one on this page and set <b>File Prefix</b> if <b>Transfer to OBS</b> is enabled. When <b>Transfer to OBS</b> is disabled, no operation is required.
Create a cloud service agency.	(Mandatory) If you select this check box, CTS automatically creates a cloud service agency when you create a tracker. The agency authorizes you to use OBS.



Parameter	Description
OBS Bucket Account	<p>CTS allows you to transfer traces to OBS buckets of other users for unified management.</p> <ul style="list-style-type: none"> <li>If you select <b>Logged-in user</b>, you do not need to grant the transfer permission.</li> <li>If you select <b>Other users</b>, ensure that the user to which the OBS bucket belongs has granted the transfer permission to your current user. Otherwise, the transfer fails. For details about how to grant the transfer permission, see <a href="#">Cross-Tenant Transfer Authorization</a>.</li> </ul>
OBS Bucket	<p><b>New:</b> An OBS bucket will be created automatically with the name you enter.</p> <p><b>Existing:</b> Select an existing OBS bucket.</p>
Select Bucket	<p>If you select <b>New</b> for <b>OBS Bucket</b>, enter an OBS bucket name. The OBS bucket name cannot be empty. It can contain 3 to 63 characters, including only lowercase letters, digits, hyphens (-), and periods (.). It cannot contain two consecutive periods (for example, my..bucket). A period (.) and a hyphen (-) cannot be adjacent to each other (for example, my-.bucket and my.-bucket). Do not use an IP address as a bucket name.</p> <p>If you select <b>Existing</b> for <b>OBS Bucket</b>, select an existing OBS bucket.</p>
Retention Period	For the management tracker, the retention period configured on the OBS console is used by default and cannot be changed.
File Prefix	A file prefix is used to mark transferred trace files. The prefix you set will be automatically added to the beginning of the file names, facilitating file filtering. Enter 0 to 64 characters. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.
Compression	<p>The usage of object storage space can be reduced.</p> <ul style="list-style-type: none"> <li><b>Do not compress:</b> Transfer files in the *.json format.</li> <li><b>gzip:</b> Transfer files in *.json.gz format.</li> </ul>
Sort by Cloud Service	<ul style="list-style-type: none"> <li>When this function is enabled, the cloud service name is added to the transfer file path, and multiple small files are generated in OBS. Example: <code>/CloudTrace/cn-north-7/2022/11/8/doctest/Cloud service/_XXX.json.gz</code></li> <li>When this function is disabled, the cloud service name will not be added to the transfer file path. Example: <code>/CloudTrace/cn-north-7/2022/11/8/doctest/_XXX.json.gz</code></li> </ul>
Transfer Path	Log transfer path is automatically set by the system.
Verify Trace File	When this function is enabled, integrity verification will be performed to check whether trace files in OBS buckets have been tampered with. For details about file integrity verification, see <a href="#">Verifying Trace File Integrity</a> .

Parameter	Description
Encrypt Trace File	<p>When <b>OBS Bucket Account</b> is set to <b>Logged-in user</b>, you can configure an encryption key for the traces.</p> <p>When <b>Encrypt Trace File</b> is enabled, CTS obtains the key IDs of the current login user from DEW. You can select a key from the drop-down list.</p> <p><b>NOTE</b> Use the keys in DEW to fully or partially encrypt objects in an OBS bucket. For details, see <a href="#">Encrypting Data in OBS</a>.</p>

**Table 3-2** Parameters for configuring the transfer to LTS


Parameter	Description
Transfer to LTS	When <b>Transfer to LTS</b> is enabled, traces are transferred to the log stream.
Log Group	When <b>Transfer to LTS</b> is enabled, the default log group name <b>CTS</b> is set. When <b>Transfer to LTS</b> is disabled, no operation is required.

**Step 8** Click **Next > Configure** to complete the configuration of the tracker.

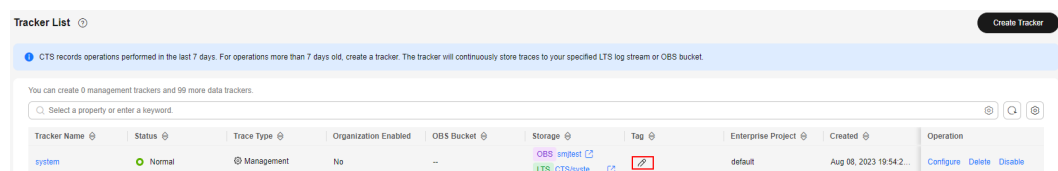
You can then view the tracker details on the **Tracker List** page.

**NOTE**

Traces recorded by CTS are delivered periodically to the OBS bucket for storage. If you configure an OBS bucket for a tracker, traces generated during the current cycle (usually several minutes) will be delivered to the configured OBS bucket. For example, if the current cycle is from 12:00:00 to 12:05:00 and you configure an OBS bucket for a tracker at 12:02:00, traces received from 12:00:00 to 12:02:00 will also be delivered to the configured OBS bucket for storage at 12:05:00.

**Step 9** (Optional) On the **Tracker List** page, click  in the **Tag** column to add tags to the tracker.

**Figure 3-3** Adding a tag



Tags are key-value pairs, which are used to identify, classify, and search for trackers. Tracker tags are used to filter and manage trackers only. A maximum of 20 tags can be added to a tracker.

If your organization has configured tag policies for CTS, add tags to trackers based on the policies. For details about tag policies, see [Overview of a Tag Policy](#). For details about tag management, see [Overview of a Tag](#).

**Table 3-3** Tag parameters

Parameter	Description	Example
Tag key	<p>A tag key of a tracker must be unique. You can customize a key or select the key of an existing tag created in Tag Management Service (TMS).</p> <p>A tag key:</p> <ul style="list-style-type: none"> <li>• Can contain 1 to 128 characters.</li> <li>• Can contain letters, digits, spaces, and special characters <code>._:=-@</code>, but cannot start or end with a space or start with <code>_sys_</code>.</li> </ul>	Key_0001
Tag value	<p>A tag value can be repetitive or left blank.</p> <p>A tag value:</p> <ul style="list-style-type: none"> <li>• Can contain 0 to 255 characters.</li> <li>• Can contain letters, digits, spaces, and special characters <code>._:/=-@</code></li> </ul>	Value_0001

----End

## 3.3 Disabling or Enabling a Tracker

### Scenario

You can enable or disable a tracker on the CTS console. Disabling a tracker does not affect existing operation records.


This section describes how to enable or disable a tracker.


### Prerequisites

You have enabled CTS.

### Procedure

**Step 1** Log in to the management console.

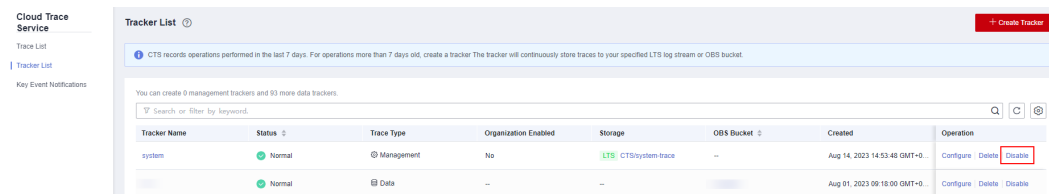
**Step 2** Click  in the upper left corner to select the desired region and project.

**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 left navigation pane.

**Step 5** Click **Disable** in the **Operation** column in the row of the management tracker.

**Figure 3-4** Disabling a tracker



**Step 6** Click **OK**.

----End

After the tracker is disabled, the **Disable** button changes to **Enable**. To enable the management tracker again, click **Enable** and then click **OK**. The tracker will start recording operations again.

## 3.4 Deleting a Tracker

### Scenario


You can delete the management tracker on the CTS console. Deleting it does not affect the existing operation records. This section describes how to delete the management tracker on the console.


### Prerequisites

You have enabled CTS.

### Procedure

**Step 1** Log in to the management console.

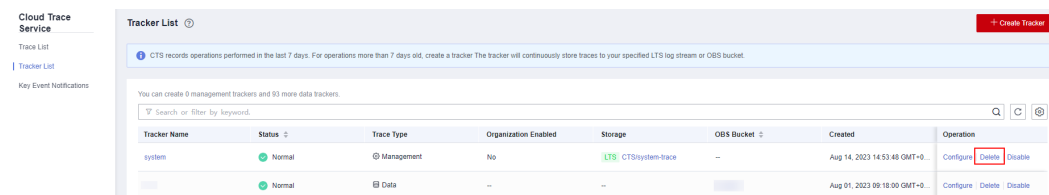
**Step 2** Click  in the upper left corner to select the desired region and project.

**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 left navigation pane.

**Step 5** Click **Delete** in the **Operation** column of the management tracker.

**Figure 3-5** Deleting a tracker



**Step 6** Click **OK**.

 **NOTE**

After the management tracker is deleted, CTS still retains historical traces. You can enable CTS again to restore the management tracker.

**----End**

# 4 Data Trackers

---

CTS provides two types of trackers: a management tracker and multiple data trackers. The management tracker records management traces, which are operations on all cloud resources, such as creation, login, and deletion. Data trackers record data traces, which are operations performed by tenants on data in OBS buckets, such as upload and download.

This section describes how to use a data tracker.

## 4.1 Creating a Tracker

### Scenario

You can create data trackers to log operations on data. Data trackers record data traces, that is, logs of tenant operations (such as upload and download) on data in OBS buckets.

When you enable CTS, a management tracker is created automatically. Only one management tracker can be created. The trackers you created are all data trackers.

#### NOTE

- CTS records operations performed in the last seven days. To store traces for a longer time, configure a tracker. The tracker will store traces to your specified LTS log streams or OBS buckets.

### Prerequisites

You have enabled CTS. For details, see [Overview](#).

### Creating a Data Tracker

1. Log in to the management console.
2. In the service list, choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Tracker List** in the left navigation pane. In the upper right corner of the displayed page, click **Create Tracker**.

4. Set basic information. Enter a tracker name. Click **Next**.

 **NOTE**

- Tracker name contains only letters, digits, hyphens (-), and underscores (\_), and must start with a letter or digit.
  - Tracker name cannot be empty and contains a maximum of 32 characters.
  - The name of the data tracker cannot be system or system-trace.
5. Select a trace. Set parameters and click **Next**.

**Table 4-1** Parameters for selecting a trace

Parameter	Description
Data Trace Source	Container for storing data traces. Currently, OBS buckets are used.
OBS Bucket	Select an OBS bucket from the drop-down list.
Operation	<ul style="list-style-type: none"> <li>• Select the operations to record.</li> <li>• Options: <b>Read</b> and <b>Write</b>. Select at least one of them.</li> </ul>

6. Configure a transfer. Set parameters and click **Next**. You can query operation records of the last seven days on the CTS console. To store and query operation records beyond seven days, transfer them to OBS or LTS. For details, see [Table 4-2](#) and [Table 4-3](#).

**Table 4-2** Parameters for configuring the transfer to OBS

Parameter	Description
Transfer to OBS	If you select <b>Yes</b> , select an existing OBS bucket or create one on the <b>Configure Tracker</b> page and set <b>File Prefix</b> . When <b>Transfer to OBS</b> is disabled, no operation is required.
Create a cloud service agency.	(Mandatory) If you select this check box, CTS automatically creates a cloud service agency when you create a tracker. The agency authorizes you to use OBS.
OBS Bucket	<b>New:</b> An OBS bucket will be created automatically with the name you enter. <b>Existing:</b> Select an existing OBS bucket.
Select Bucket	When you select <b>New</b> , enter an OBS bucket name. The OBS bucket name cannot be empty. It can contain 3 to 63 characters, including only lowercase letters, digits, hyphens (-), and periods (.). It cannot contain two consecutive periods (for example, my..bucket). A period (.) and a hyphen (-) cannot be adjacent to each other (for example, my-.bucket and my.-bucket). Do not use an IP address as a bucket name.  When you select <b>Existing</b> , select an existing OBS bucket.

Parameter	Description
Retention Period	<p>The duration for storing traces in the OBS bucket. This configuration will apply to the selected bucket and all files in it. Different compliance standards require different trace retention periods. You are advised to set the retention period to at least 180 days.</p> <ul style="list-style-type: none"> <li>For a data tracker, you can set the duration to 30 days, 60 days, 90 days, 180 days, 3 years, or the same as that of OBS.</li> </ul>
File Prefix	<p>A file prefix is used to mark transferred trace files. The prefix you set will be automatically added to the beginning of the file names, facilitating file filtering. Enter 0 to 64 characters. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.</p>
Compression	<p>The space object storage can be reduced.</p> <ul style="list-style-type: none"> <li><b>No</b>: Transfer files in the *.json format.</li> <li><b>gzip</b>: Transfer files in *.json.gz format.</li> </ul>
Sort by Cloud Service	<ul style="list-style-type: none"> <li>When this function is enabled, the cloud service name is added to the transfer file path, and multiple small files are generated in OBS. Example: <b>/CloutTrace/cn-north-7/2022/11/8/doctest/Cloud service/_XXX.json.gz</b></li> <li>When this function is disabled, the cloud service name will not be added to the transfer file path. Example: <b>/CloutTrace/cn-north-7/2022/11/8/doctest/_XXX.json.gz</b></li> </ul>
Log Transfer Path	<p>Log transfer path is automatically set by the system.</p>
Verify Trace File	<p>When this function is enabled, integrity verification will be performed to check whether trace files in OBS buckets have been tampered with. For details about file integrity verification, see <a href="#">Verifying Trace File Integrity</a>.</p>

**Table 4-3** Parameters for configuring the transfer to LTS

Parameter	Description
Transfer to LTS	<p>When <b>Transfer to LTS</b> is enabled, traces are transferred to the log stream.</p>
Log group name	<p>When <b>Transfer to LTS</b> is enabled, the default log group name <b>CTS</b> is set. When <b>Transfer to LTS</b> is disabled, no operation is required.</p>

- Preview the tracker information and click **Create**.



8. Click **OK**.

## 4.2 Configuring a Tracker

### Scenario

You can configure key event notifications of trackers on the CTS console no matter whether the trackers are enabled or not. For enabled trackers, you can also configure **Transfer to OBS** or **Transfer to LTS** for trace transfer.

- You can select an existing OBS bucket for trace transfer. CTS will automatically attach a required policy to the OBS bucket.
- If you modify the trace file prefix of a tracker, the OBS bucket policy will not be affected.

#### NOTE

There are three storage classes of OBS buckets: Standard, Infrequent Access, and Archive. You must use Standard OBS buckets for trace transfer because CTS needs to frequently access the OBS buckets.

The configuration will take effect immediately after it is complete.

This section describes how to configure a data tracker.

### Constraints



For global services, you must configure trackers on the CTS console in the central region (CN-Hong Kong). This configuration enables the function of transferring traces to OBS or LTS. The preceding function will not take effect if you perform the configuration on the CTS console in any region outside the central region.

For details about Huawei Cloud global services, see [Constraints](#).

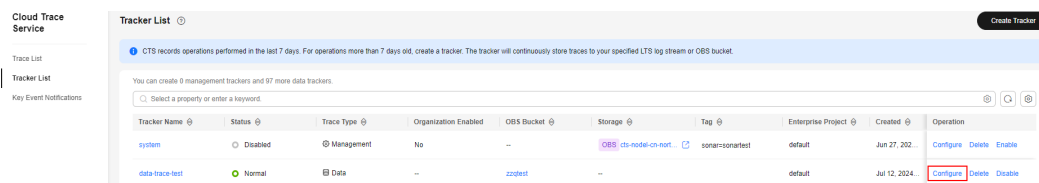
### Prerequisites

You have enabled CTS and created a data tracker.

### Configuring a Data Tracker

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner to select the desired region and project.
- 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.
- Step 5** Click **Configure** in the **Operation** column in the row of the target data tracker.

**Figure 4-1** Configuring a tracker



**Step 6** On the **Configure Transfer** page, modify the transfer parameters of the tracker. When you configure a data tracker, the OBS bucket name of the data trace source is set as **OBS Bucket** by default and cannot be modified. You can query operation records of the last seven days on the CTS console. To store and query operation records beyond seven days, transfer them to OBS or LTS. For details, see [Table 4-4](#) and [Table 4-5](#).

**Table 4-4** Parameters for configuring the transfer to OBS

Parameter	Description
Transfer to OBS	If you select <b>Yes</b> , select an existing OBS bucket or create one on the <b>Configure Tracker</b> page and set <b>File Prefix</b> . When <b>Transfer to OBS</b> is disabled, no operation is required.
Create a cloud service agency.	(Mandatory) If you select this check box, CTS automatically creates a cloud service agency when you create a tracker. The agency authorizes you to use OBS.
OBS Bucket	<b>New:</b> An OBS bucket will be created automatically with the name you enter. <b>Existing:</b> Select an existing OBS bucket.
Select Bucket	When you select <b>New</b> , enter an OBS bucket name. The OBS bucket name cannot be empty. It can contain 3 to 63 characters, including only lowercase letters, digits, hyphens (-), and periods (.). It cannot contain two consecutive periods (for example, my..bucket). A period (.) and a hyphen (-) cannot be adjacent to each other (for example, my-.bucket and my.-bucket). Do not use an IP address as a bucket name. When you select <b>Existing</b> , select an existing OBS bucket.
Retention Period	The duration for storing traces in the OBS bucket. This configuration will apply to the selected bucket and all files in it. Different compliance standards require different trace retention periods. You are advised to set the retention period to at least 180 days. <ul style="list-style-type: none"> <li>For a data tracker, you can set the duration to 30 days, 60 days, 90 days, 180 days, 3 years, or the same as that of OBS.</li> </ul>

Parameter	Description
File Prefix	A file prefix is used to mark transferred trace files. The prefix you set will be automatically added to the beginning of the file names, facilitating file filtering. Enter 0 to 64 characters. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.
Compression	The space object storage can be reduced. <ul style="list-style-type: none"> <li>• <b>No</b>: Transfer files in the *.json format.</li> <li>• <b>gzip</b>: Transfer files in *.json.gz format.</li> </ul>
Sort by Cloud Service	<ul style="list-style-type: none"> <li>• When this function is enabled, the cloud service name is added to the transfer file path, and multiple small files are generated in OBS. Example: <b>/CloudTrace/cn-north-7/2022/11/8/doctest/Cloud service/_XXX.json.gz</b></li> <li>• When this function is disabled, the cloud service name will not be added to the transfer file path. Example: <b>/CloudTrace/cn-north-7/2022/11/8/doctest/_XXX.json.gz</b></li> </ul>
Log Transfer Path	Log transfer path is automatically set by the system.
Verify Trace File	When this function is enabled, integrity verification will be performed to check whether trace files in OBS buckets have been tampered with. For details about file integrity verification, see <a href="#">Verifying Trace File Integrity</a> .

**Table 4-5** Parameters for configuring the transfer to LTS


Parameter	Description
Transfer to LTS	When <b>Transfer to LTS</b> is enabled, traces are transferred to the log stream.
Log group name	When <b>Transfer to LTS</b> is enabled, the default log group name <b>CTS</b> is set. When <b>Transfer to LTS</b> is disabled, no operation is required.

**Step 7** Click **Next > Configure** to complete the configuration of the data tracker.

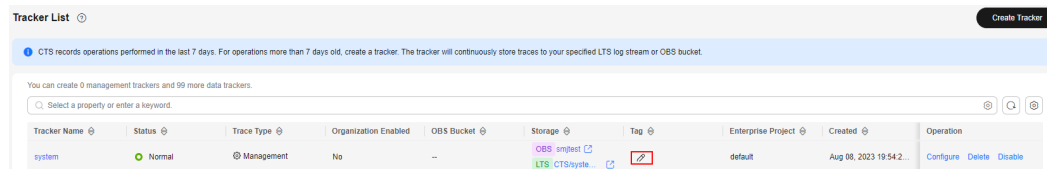
You can then view the tracker details on the **Tracker List** page.

 **NOTE**

Traces recorded by CTS are delivered periodically to the OBS bucket for storage. If you configure an OBS bucket for a tracker, traces generated during the current cycle (usually several minutes) will be delivered to the configured OBS bucket. For example, if the current cycle is from 12:00:00 to 12:05:00 and you configure an OBS bucket for a tracker at 12:02:00, traces received from 12:00:00 to 12:02:00 will also be delivered to the configured OBS bucket for storage at 12:05:00.

**Step 8** (Optional) On the **Tracker List** page, click  in the **Tag** column to add tags to the tracker.

**Figure 4-2** Adding a tag



Tags are key-value pairs, which are used to identify, classify, and search for trackers. Tracker tags are used to filter and manage trackers only. A maximum of 20 tags can be added to a tracker.

If your organization has configured tag policies for CTS, add tags to trackers based on the policies. For details about tag policies, see [Overview of a Tag Policy](#). For details about tag management, see [Overview of a Tag](#).

**Table 4-6** Tag parameters

Parameter	Description	Example
Tag key	<p>A tag key of a tracker must be unique. You can customize a key or select the key of an existing tag created in Tag Management Service (TMS).</p> <p>A tag key:</p> <ul style="list-style-type: none"> <li>• Can contain 1 to 128 characters.</li> <li>• Can contain letters, digits, spaces, and special characters <code>._:=-@</code>, but cannot start or end with a space or start with <code>_sys_</code>.</li> </ul>	Key_0001
Tag value	<p>A tag value can be repetitive or left blank.</p> <p>A tag value:</p> <ul style="list-style-type: none"> <li>• Can contain 0 to 255 characters.</li> <li>• Can contain letters, digits, spaces, and special characters <code>._:/=-@</code></li> </ul>	Value_0001

----End

## 4.3 Disabling or Enabling a Tracker

### Scenario

You can disable a tracker on the CTS console. After a tracker is disabled, it will stop recording operations, but you can still view operation records that have been collected.

## Prerequisites

You have created a data tracker on the CTS console.

## Procedure



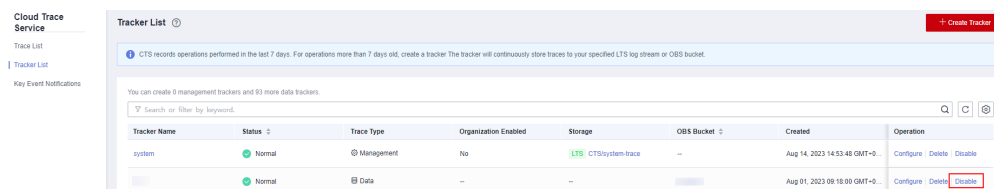
1. Log in to the management console.
2. Click  in the upper left corner to select the desired region and project.
3. Click  in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.
4. Choose **Tracker List** in the left navigation pane.
5. Click **Disable** in the **Operation** column in the row of the target data tracker.

Figure 4-3 Disabling a tracker



6. Click **OK**.

After the tracker is disabled, the **Disable** button changes to **Enable**. To enable the tracker, click **Enable** and then click **OK**. The tracker will start recording operations again.

## 4.4 Deleting a Tracker

### Scenario

Deleting a data tracker on the CTS console is available, and does not affect the existing operation records. This section describes how to delete a data tracker on the management console.

### Prerequisites

A data tracker has been created.

### Deleting a Data Tracker



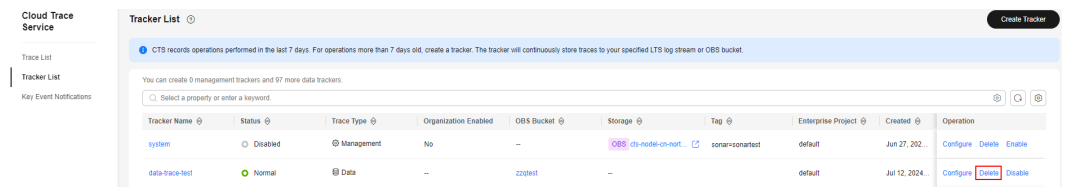
1. Log in to the management console.
2. Click  in the upper left corner to select the desired region and project.
3. Click  in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.
4. Choose **Tracker List** in the navigation pane.
5. Click **Delete** in the **Operation** column of the target configuration item.

Figure 4-4 Deleting a tracker



6. Click **Yes**.

# 5 Organization Trackers

---

## 5.1 Overview

The Organizations service helps you govern multiple accounts within your organization. It enables you to consolidate multiple Huawei Cloud accounts into an organization that you create and centrally manage these accounts. You can use Organizations to apply access policies to different accounts in your organization. This helps you better meet the security and compliance requirements of your business.

CTS supports multi-account management of Organizations.

1. Use an organization administrator account to [set CTS as a trusted service](#) on the Organizations console and specify a delegated administrator account.
2. You can use the delegated administrator account to [configure an organization tracker](#) in CTS. Then the delegated administrator account can implement cloud audit capabilities, such as security audit.

### Constraints

1. Only one organization tracker can be enabled for an organization.
2. Currently, the organization function is supported only by management trackers and not supported by data trackers.
3. Before removing a delegated administrator, disable the organization tracker and then remove the delegated administrator on the Organization console.
4. Traces of a single account can be viewed on the **Trace List** page of the CTS console. For traces of multiple accounts, you can view only the traces of your own account on the CTS console. To view traces of all accounts in the organization, go to the OBS bucket or the **CTS/system-trace** log stream configured for the organization tracker.
5. Organization trackers rely on certain Organizations APIs to implement the multi-account management capability of Organizations. Users without the enterprise project management function enabled can use this capability as long as they have the CTS permissions. However, users with enterprise project management function enabled must also be granted certain IAM permissions to use this capability.

## Helpful Links

[What Is Organizations?](#)

[Enabling or Disabling a Trusted Service](#)

[Specifying, Viewing, or Removing a Delegated Administrator](#)

## 5.2 Setting CTS as a Trusted Service

Use an organization administrator account to set CTS as a trusted service on the Organizations console and specify a delegated administrator account.

### NOTE


Currently, the trusted service function for CTS is available in ME-Riyadh, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, CN South-Guangzhou, CN Southwest-Guiyang1, CN-Hong Kong, AP-Bangkok, AP-Singapore, AP-Jakarta, AF-Johannesburg, TR-Istanbul, LA-Mexico City1, LA-Mexico City2, LA-Sao Paulo1, and LA-Santiago regions.


## Prerequisites

1. You are using an organization administrator account.
2. You have planned a delegated administrator account for security operations and audit trace management.

## Procedure

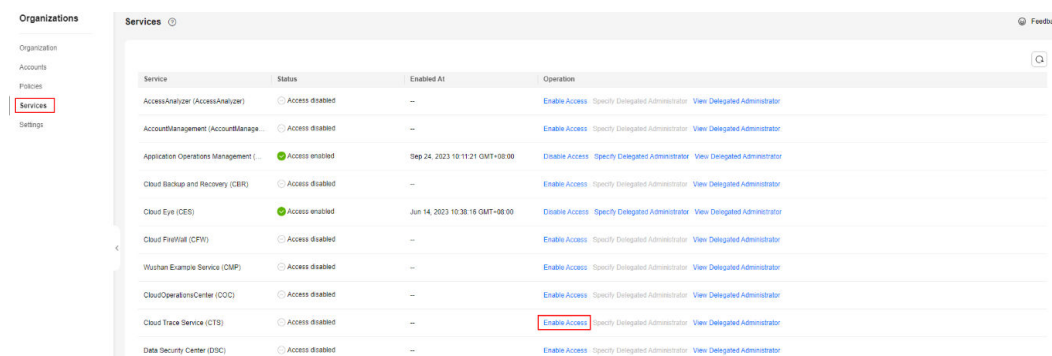
**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner to select the desired region and project.

**Step 3** Click  in the upper left corner and choose **Management & Governance > Organizations**.

**Step 4** In the navigation pane, choose **Services**. On the displayed page, locate CTS and click **Enable Access** to set CTS as a trusted service.

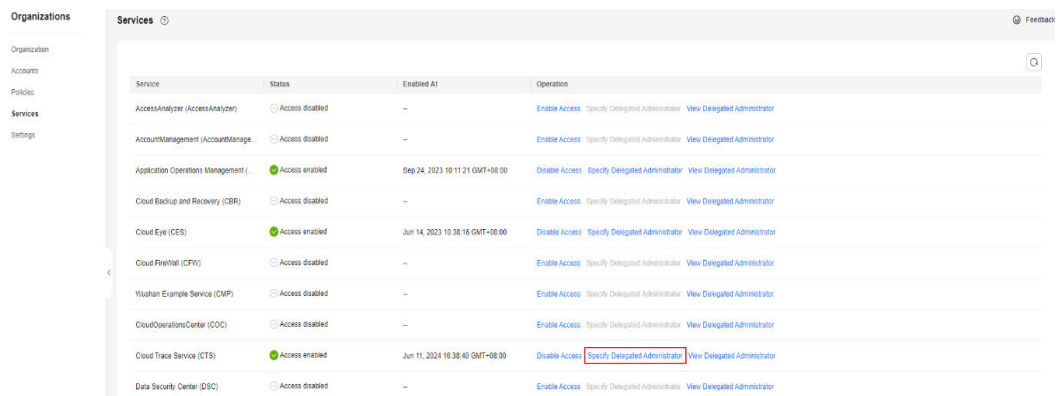
**Figure 5-1** Setting CTS as a trusted service



**Step 5** Click **Specify Delegated Administrator** on the right of CTS to set a delegated administrator for CTS.



**Figure 5-2** Specifying a delegated administrator



----End

## Removing the Delegated Administrator Permission

- Step 1** Log in to the Organizations console.
- Step 2** In the navigation pane, choose **Services**. On the displayed page, locate CTS.
- Step 3** Click **View Delegated Administrator** on the right of CTS.
- Step 4** Select the delegated administrator account to be removed and click **Remove**. In the displayed dialog box, click **OK** to cancel the delegated administrator permission of the account.

----End



## 5.3 Configuring an Organization Tracker

An organization tracker is a management tracker with organization function enabled. To configure it, use a delegated or organization administrator account to log in to CTS and enable **Apply to Organization** for the management tracker.

### Prerequisites

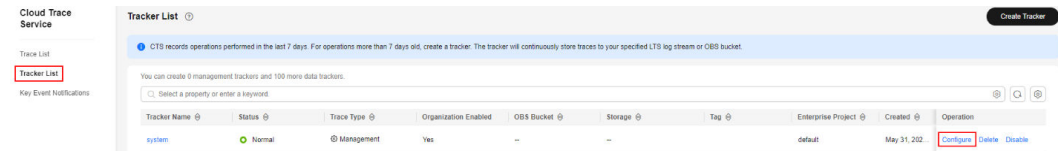
1. You are using a delegated or organization administrator account.
2. You have used an organization administrator account to set CTS as a trusted service in Organizations.
3. You have planned an OBS bucket for the delegated administrator to store audit traces.

### Configuring an Organization Tracker

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner to select the desired region and project.
- Step 3** Click  in the upper left corner and choose **Management & Governance > Cloud Trace Service**.

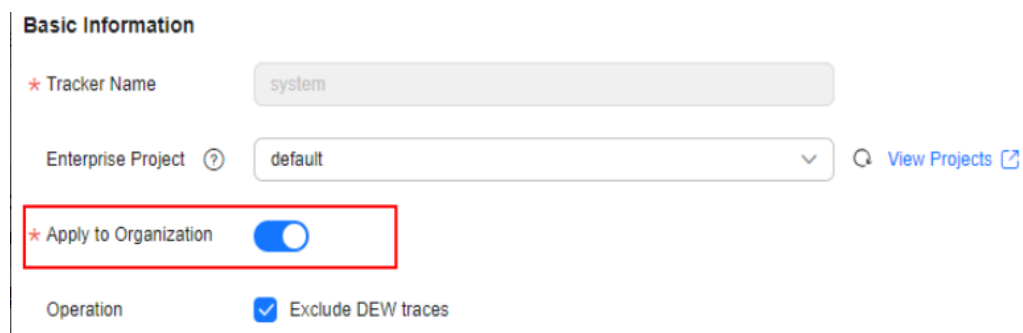
**Step 4** In the navigation pane, choose **Tracker List**. Click **Configure** on the right of the management tracker. If no management tracker is displayed, **enable CTS** first.

**Figure 5-3** Management tracker



**Step 5** On the **Basic Information** page, enable **Apply to Organization** and click **Next**.

**Figure 5-4** Applying to my organization



**Step 6** On the **Configure Transfer** page, enable **Transfer to OBS** and **Transfer to LTS**. You can query operation records of the last seven days on the CTS console. To store and query operation records beyond seven days, transfer them to OBS or LTS. For details, see **Table 5-1** and **Table 5-2**. Set **OBS Bucket Account** to **Logged-in user**, select **Existing** for **OBS Bucket**, and select the OBS bucket planned by the administrator. Click **Next > Configure**.

**Table 5-1** Parameters for configuring the transfer to OBS

Parameter	Description
Transfer to OBS	Select an existing OBS bucket or create one on this page and set <b>File Prefix</b> if <b>Transfer to OBS</b> is enabled. When <b>Transfer to OBS</b> is disabled, no operation is required.
Create a cloud service agency.	(Mandatory) If you select this check box, CTS automatically creates a cloud service agency when you create a tracker. The agency authorizes you to use OBS.

Parameter	Description
OBS Bucket Account	<p>CTS allows you to transfer traces to OBS buckets of other users for unified management.</p> <ul style="list-style-type: none"> <li>If you select <b>Logged-in user</b>, you do not need to grant the transfer permission.</li> <li>If you select <b>Other users</b>, ensure that the user to which the OBS bucket belongs has granted the transfer permission to your current user. Otherwise, the transfer fails. For details about how to grant the transfer permission, see <a href="#">Cross-Tenant Transfer Authorization</a>.</li> </ul>
OBS Bucket	<p><b>New:</b> An OBS bucket will be created automatically with the name you enter.</p> <p><b>Existing:</b> Select an existing OBS bucket.</p>
Select Bucket	<p>If you select <b>New</b> for <b>OBS Bucket</b>, enter an OBS bucket name. The OBS bucket name cannot be empty. It can contain 3 to 63 characters, including only lowercase letters, digits, hyphens (-), and periods (.). It cannot contain two consecutive periods (for example, my..bucket). A period (.) and a hyphen (-) cannot be adjacent to each other (for example, my-.bucket and my-.bucket). Do not use an IP address as a bucket name.</p> <p>If you select <b>Existing</b> for <b>OBS Bucket</b>, select an existing OBS bucket.</p>
Retention Period	For the management tracker, the retention period configured on the OBS console is used by default and cannot be changed.
File Prefix	A file prefix is used to mark transferred trace files. The prefix you set will be automatically added to the beginning of the file names, facilitating file filtering. Enter 0 to 64 characters. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.
Compression	<p>The usage of object storage space can be reduced.</p> <ul style="list-style-type: none"> <li><b>Do not compress:</b> Transfer files in the *.json format.</li> <li><b>gzip:</b> Transfer files in *.json.gz format.</li> </ul>
Sort by Cloud Service	<ul style="list-style-type: none"> <li>When this function is enabled, the cloud service name is added to the transfer file path, and multiple small files are generated in OBS. Example: <code>/CloudTrace/cn-north-7/2022/11/8/doctest/Cloud service/_XXX.json.gz</code></li> <li>When this function is disabled, the cloud service name will not be added to the transfer file path. Example: <code>/CloudTrace/cn-north-7/2022/11/8/doctest/_XXX.json.gz</code></li> </ul>
Transfer Path	Log transfer path is automatically set by the system.
Verify Trace File	When this function is enabled, integrity verification will be performed to check whether trace files in OBS buckets have been tampered with. For details about file integrity verification, see <a href="#">Verifying Trace File Integrity</a> .

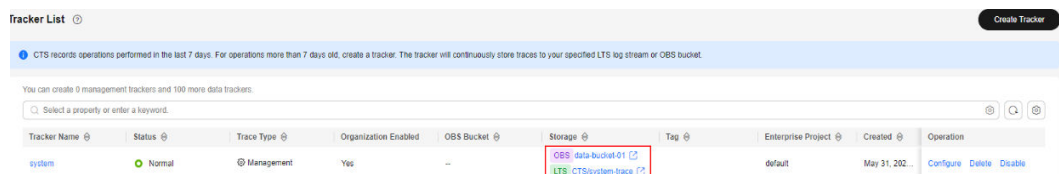
Parameter	Description
Encrypt Trace File	<p>When <b>OBS Bucket Account</b> is set to <b>Logged-in user</b>, you can configure an encryption key for the traces.</p> <p>When <b>Encrypt Trace File</b> is enabled, CTS obtains the key IDs of the current login user from DEW. You can select a key from the drop-down list.</p> <p><b>NOTE</b> Use the keys in DEW to fully or partially encrypt objects in an OBS bucket. For details, see <a href="#">Encrypting Data in OBS</a>.</p>

**Table 5-2** Parameters for configuring the transfer to LTS

Parameter	Description
Transfer to LTS	When <b>Transfer to LTS</b> is enabled, traces are transferred to the log stream.
Log Group	When <b>Transfer to LTS</b> is enabled, the default log group name <b>CTS</b> is set. When <b>Transfer to LTS</b> is disabled, no operation is required.

**Step 7** After the configuration is complete, administrators can view information about OBS buckets and LTS log groups on the **Tracker List** page.

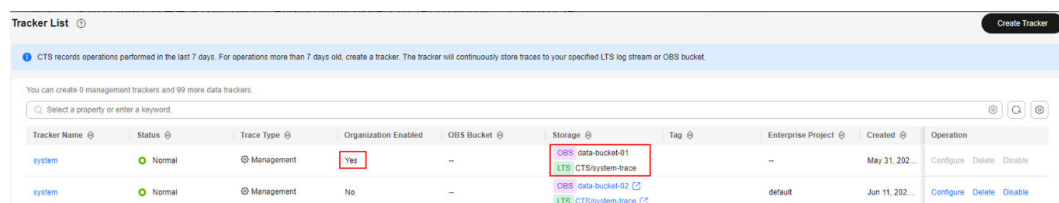
**Figure 5-5** Viewing trackers as an administrator



**Step 8** Log in to CTS using an organization member account and go to the **Tracker List** page. The value in the **Organization Enabled** column of the target tracker is **Yes**.

The system tracker of the administrator account is displayed in the first row, and the system tracker of the current account is displayed in the second row. Audit logs of the organization member account can be transferred to the OBS buckets and LTS log groups of both the administrator account and the current account.

**Figure 5-6** Viewing a tracker as an organization member



----End

# 6 Creating a Key Event Notification

---

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.

## Usage Description

- For global services, you must configure key event notifications on the CTS console in the central region (CN-Hong Kong). This configuration enables the function of sending key event notifications. The preceding function will not take effect if you perform the configuration on the CTS console in any region outside the central region. For details about Huawei Cloud global services, see [Constraints](#).
- 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 1,000 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).

**Table 6-1** Advanced filtering parameters

Parameter	Description
api_version	Version of the API called in a trace. Enumerated values: <ul style="list-style-type: none"> <li>• v1</li> <li>• v3</li> </ul>
code	HTTP status code returned by an API.
trace_rating	Trace status. Enumerated values: <ul style="list-style-type: none"> <li>• normal</li> <li>• warning</li> <li>• incident</li> </ul>
trace_type	Trace type. The value can be <b>system</b> (management traces) or <b>data</b> (data traces). Enumerated values: <ul style="list-style-type: none"> <li>• system</li> <li>• data</li> </ul>
resource_id	ID of a cloud service resource on which operations are performed. Example: <b>5a0215bed7a14de38193a*****facef</b>
resource_name	Resource name recorded in a trace.

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 up to 50 users across up to 10 user groups. During each selection, you can choose multiple users within a single group, but not multiple groups at once. To add more groups, click **Add** for each one.

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 6-2](#).

**Table 6-2** Related operations

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

Operation	Description
Configuring basic settings	Click  in the upper right corner to set table text wrapping, fixed operation column position, and custom columns.

----End

# 7 Application Examples

## 7.1 Security Auditing

### Scenario

You can query operation records matching specified conditions and check whether operations have been performed by authorized users for security analysis.


### Prerequisites


You have enabled CTS and trackers are running properly.

### Procedure (for New Console)

The following takes the records of EVS disk creation and deletion in the last two weeks as an example.

**Step 1** Log in to the management console as a CTS administrator.

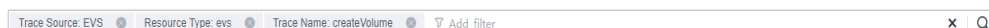
**Step 2** Click  in the upper left corner to select the desired region and project.

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

**Step 4** Choose **Trace List** in the left navigation pane.

**Step 5** Set the time range to **Last 1 week** and set filters as follows:

- For creation operations: Select **EVS** for **Trace Source**, **evs** for **Resource Type**, and **createVolume** for **Trace Name**. View the filtering result.



- For deletion operations: Select **EVS** for **Trace Source**, **evs** for **Resource Type**, and **deleteVolume** for **Trace Name**. View the filtering result.



 NOTE

- By default, all EVS creation or deletion operations performed in the last hour are queried. You can also set the time range to query all EVS creation or deletion operations performed in the last seven days at most.
- For all cloud services and operations that can be audited by CTS, see [Supported Services and Operations](#).

To obtain the operation records of the last week, query them in the OBS bucket. Choose **Tracker List** in the left navigation pane. In the displayed tracker list, click the OBS bucket name in the row of the management tracker.

 NOTE



To store operation records for more than seven days, you must configure the management tracker to transfer them to an OBS bucket. Otherwise, you cannot query the operation records generated seven days ago.

- Step 6** Download traces older than seven days or all traces by following the instructions in [Querying Transferred Traces](#).
- Step 7** In the trace files, search traces using keywords **createVolume** or **deleteVolume**.
- Step 8** Check the traces obtained in steps [Step 5](#) and [Step 7](#) to see whether there are any unauthorized operations or operations that do not conform to security rules.

----End

## Procedure (for Old Console)

The following takes the records of EVS disk creation and deletion in the last two weeks as an example.

1. Log in to the management console as a CTS administrator.
2. Click  in the upper left corner to select the desired region and project.
3. Click  in the upper left corner and choose **Management & Governance > Cloud Trace Service**. The CTS console is displayed.
4. Choose **Trace List** in the left navigation pane.
5. Set the time range to **Last 1 week**, set filters in sequence, and click **Query**.

 NOTE

Select **Management** for **Trace Type**, **evs** for **Trace Source**, **evs** for **Resource Type**, **Trace name** for **Search By**, select **createVolume** or **deleteVolume**, and click **Query**. By default, all EVS disk creation or deletion operations performed in the last hour are queried. You can also set the time range to query all EVS creation or deletion operations performed in the last seven days at most.

6. To obtain the operation records of the last week, query them in the OBS bucket. Choose **Tracker List** in the navigation pane on the left.

 NOTE

To store operation records for more than seven days, you must configure the management tracker to transfer them to an OBS bucket. Otherwise, you cannot query the operation records generated seven days ago.

7. Download traces older than seven days or all traces by following the instructions in [Querying Transferred Traces](#).

- In the trace files, search traces using keywords **createVolume** or **deleteVolume**.
- Check the traces obtained from steps 5 and 8 to see whether there are any unauthorized operations or operations that do not conform to security rules.

## 7.2 Fault Locating

### Scenario

If a resource or an action encounters an exception, you can query operation records of the resource or action in a specified time period and view the requests and responses to facilitate fault locating.


### Prerequisites


You have enabled CTS and trackers are running properly. For details about how to enable CTS, see [Overview](#).

### Procedure (for New Console)

The following shows how to locate an ECS fault which occurred in a morning.

**Step 1** Log in to the management console as a CTS administrator.

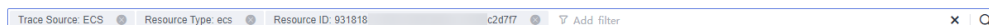
**Step 2** Click  in the upper left corner to select the desired region and project.

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

**Step 4** Choose **Trace List** in the left navigation pane.

**Step 5** Set the time range to 06:00 to 12:00 of a certain day and set the filters as follows:

Select **ECS** for **Trace Source** and **ecs** for **Resource Type**, and enter *{ID of the faulty VM}* for **Resource ID**. You can also directly enter *{ID of the faulty VM}* to view the filtering result.





**Step 6** Check the returned traces, especially the request type and response of each trace. Pay attention to traces whose status is **warning** or **incident**, and traces whose response indicates a failure.

----End

The following shows how to locate a fault after an ECS server failed to be created.

**Step 1** Log in to the management console as a CTS administrator.

**Step 2** Click  in the upper left corner to select the desired region and project.

**Step 3** Click  in the upper left corner and choose **Management & Governance > Cloud Trace Service**.

**Step 4** Choose **Trace List** in the left navigation pane.

**Step 5** Set filters as follows:

Select **ECS** for **Trace Source**, **ecs** for **Resource Type**, and **warning** for **Trace Status**. For failed ECS creation operations, view the trace named **createServer** in the filtering result.





**Step 6** Check the trace details and locate the fault based on the error code or error message.

----End

## Procedure (for Old Console)

The following shows how to locate an ECS fault which occurred in a morning.



1. Log in to the management console as a CTS administrator.
2. Click  in the upper left corner to select the desired region and project.
3. Click  in the upper left corner and choose **Management & Governance > Cloud Trace Service**. The CTS console is displayed.
4. Choose **Trace List** in the left navigation pane.
5. Set filters in sequence and click **Query**.

### NOTE

Select **Management** for **Trace Type**, **ECS** for **Trace Source**, **ecs** for **Resource Type**, **Resource ID** for **Search By**, and enter the ID of the faulty virtual machine (VM). In the upper right corner, select a time range from 06:00:00 to 12:00:00 on the day when the fault occurred. Then, click **Query** to view the result.

6. Check the returned traces, especially the request type and response of each trace. Pay attention to traces whose status is **warning** or **incident**, and traces whose response indicates a failure.

The following shows how to locate a fault after an ECS server failed to be created.

1. Log in to the management console as a CTS administrator.
2. Click  in the upper left corner to select the desired region and project.
3. Click  in the upper left corner and choose **Management & Governance > Cloud Trace Service**. The CTS console is displayed.
4. Choose **Trace List** in the left navigation pane.
5. Select **Management** for **Trace Type**, **ECS** for **Trace Source**, **ecs** for **Resource Type**, and **Warning** for **Trace Status**. In the returned traces, locate the trace named **createServer**.
6. Check the trace details and locate the fault based on the error code or error message.

## 7.3 Resource Tracking

### Scenario

You can view operation records of a cloud resource throughout its lifecycle.


### Prerequisites


You have enabled CTS and trackers are running properly. For details about how to enable CTS, see [Overview](#).

### Procedure (for New Console)

The following takes the records of all operations on an ECS server as an example.

**Step 1** Log in to the management console as a CTS administrator.

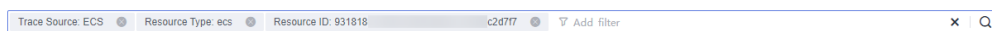
**Step 2** Click  in the upper left corner to select the desired region and project.

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

**Step 4** Choose **Trace List** in the left navigation pane.

**Step 5** Set filters as follows:

Select **ECS** for **Trace Source** and **ecs** for **Resource Type**, and enter *{ID of the faulty VM}* for **Resource ID**. You can also directly enter *{ID of the faulty VM}* to view the filtering result.



#### NOTE

By default, operations performed in the last hour are queried. You can also set the time range to view the matching traces in the last seven days at most.

To obtain the operation records of the last week, query them in the OBS bucket. Choose **Tracker List** in the left navigation pane. In the displayed tracker list, click the OBS bucket name in the row of the management tracker.

#### NOTE

To store operation records for more than seven days, you must configure the management tracker to transfer them to an OBS bucket. Otherwise, you cannot query the operation records generated seven days ago.



**Step 6** Download traces older than seven days or all traces by following the instructions in [Querying Transferred Traces](#).

**Step 7** Check all the traces obtained in [Step 5](#) and [Step 6](#).

----End

## Procedure (for Old Console)

The following takes the records of all operations on an ECS server as an example.

1. Log in to the management console as a CTS administrator.
2. Click  in the upper left corner to select the desired region and project.
3. Click  in the upper left corner and choose **Management & Governance > Cloud Trace Service**. The CTS console is displayed.
4. Choose **Trace List** in the left navigation pane.
5. Set filters in sequence and click **Query**.

### NOTE

Select **Management** for **Trace Type**, **ECS** for **Trace Source**, **ecs** for **Resource Type**, **Resource ID** for **Search By**, enter the ID of the faulty VM, and click **Query**. By default, the matching traces generated in the last hour are returned. You can also set the time range to view the matching traces in the last seven days at most.

6. Choose **Tracker List** in the navigation pane on the left.
7. Download traces older than seven days or all traces by following the instructions in [Querying Transferred Traces](#).
8. Check all the traces obtained in [5](#) and [7](#).



# 8 Trace References

## 8.1 Trace Structure

A trace consists of multiple key fields shown in [Table 8-1](#).

 **NOTE**

- This section describes the key trace fields displayed on the CTS console.
- When some fields are displayed on the CTS console, their formats are optimized for easy understanding.

**Table 8-1** Key trace fields

Field	Mandatory	Type	Description
time	Yes	Long	Timestamp when a trace was generated. The value is the local standard time, for example, <b>1660927593570</b> . This field is transmitted and stored in the form of a timestamp. It is the total number of milliseconds from 00:00:00, January 1, 1970 to the current time.
user	Yes	<b>UserInfo</b> object	Information of the user who performed the operation that triggered the trace.
request	No	Structure	Request of an operation on resources.
response	No	Structure	Response to a user request, that is, the returned information for an operation on resources.

Field	Mandatory	Type	Description
service_type	Yes	String	Type of a cloud service whose traces are to be queried. The value must be the acronym of a cloud service that has been connected with CTS. It is a word composed of uppercase letters.
event_type	Yes	String	Trace type.
project_id	Yes	String	ID of the project to which the trace belongs.
resource_type	Yes	String	Type of the resource on which the operation was performed.
resource_account_id	No	String	ID of the account to which the resource belongs. This parameter has a value only when resources are operated across tenants. For example, if tenant A operates resources of tenant B, the value is the account ID of account B.  Note: In the cross-tenant scenario, CTS copies an audit log so that both tenants can view the trace on the CTS console.
read_only	No	boolean	Whether a user request is read-only.
tracker_name	No	String	Name of the tracker that records the trace. <ul style="list-style-type: none"> <li>When <b>trace_type</b> is set to <b>system</b>, the default value <b>system</b> is used.</li> <li>When <b>trace_type</b> is set to <b>data</b>, the value is the name of the corresponding data tracker.</li> </ul>
operation_id	Yes	String	Operation ID of the trace.
resource_name	No	String	Name of a resource on which the recorded operation was performed.
resource_id	No	String	ID of a cloud resource on which the recorded operation was performed.

Field	Mandatory	Type	Description
source_ip	Yes	String	IP address of the tenant who performed the operation that triggered the trace. The value of this parameter is empty if the operation is triggered by the system.
domain_id	Yes	String	ID of the account that triggers the trace.
trace_name	Yes	String	Trace name.
trace_rating	Yes	String	Trace status. The value can be <b>normal</b> , <b>warning</b> , or <b>incident</b> . <ul style="list-style-type: none"> <li>• <b>normal</b>: The operation succeeded.</li> <li>• <b>warning</b>: The operation failed.</li> <li>• <b>incident</b>: The operation caused a serious consequence, for example, a node failure or service interruption.</li> </ul>
trace_type	Yes	String	Trace source. For management traces, the value can be <b>ApiCall</b> , <b>ConsoleAction</b> , or <b>SystemAction</b> . For data traces, the value can be <b>ObsSDK</b> or <b>ObsAPI</b> .
api_version	No	String	Version of the API called in a trace.
message	No	Structure	Remarks added by other cloud services to a trace.
record_time	Yes	Number	Timestamp when a trace was recorded by CTS.
trace_id	Yes	String	Trace ID. The value is the UUID generated by the system.
code	No	String	HTTP status code returned by the associated API.
request_id	No	String	Request ID.
location_info	No	String	Additional information required for fault locating after a request error.

Field	Mandatory	Type	Description
endpoint	No	String	Endpoint in the detail page URL of the cloud resource on which a recorded operation was performed.
resource_url	No	String	Detail page URL (excluding the endpoint) of the cloud resource on which a recorded operation was performed.
enterprise_project_id	Yes	String	ID of the enterprise project to which the resource belongs.
user_agent	No	String	ID of the request client agent.
content_length	No	Number	Length of the request message body.
total_time	No	Number	Request response time.

**Table 8-2** UserInfo

Field	Mandatory	Type	Description
type	Yes	String	Operator identity type.
principal_id	Yes	String	ID of the user who performs the operation. <ul style="list-style-type: none"> <li>For an IAM user, the format is &lt;user-id&gt;.</li> <li>For an IAM agency session identity, the format is &lt;agency-id&gt;:&lt;agency-session-name&gt;.</li> <li>For an IAM federated identity, the format is &lt;idp_id&gt;:&lt;user-session-name&gt;.</li> </ul>
principal_urn	Yes	String	URN of the operator. <ul style="list-style-type: none"> <li>For an IAM user, the format is iam::&lt;account-id&gt;:user:&lt;user-name&gt;.</li> <li>For an IAM agency session identity, the format is sts::&lt;account-id&gt;:assumed-agency:&lt;agency-name&gt;/&lt;agency-session-name&gt;.</li> <li>For an IAM federated identity, the format is sts::&lt;account-id&gt;:external-user:&lt;idp_id&gt;/&lt;user-session-name&gt;.</li> </ul>

Field	Mandatory	Type	Description
account_id	Yes	String	Account ID. To obtain it, hover over the username in the upper right corner of the console, select <b>My Credentials</b> from the drop-down menu, and locate the ID on the right of <b>Account ID</b> .
access_key_id	Yes	String	Access key ID.
id	Yes	String	User ID. To obtain it, hover over the username in the upper right corner of the console, select <b>My Credentials</b> from the drop-down menu, and locate the ID on the right of <b>IAM User ID</b> .
name	Yes	String	Username. To obtain it, hover over the username in the upper right corner of the console, select <b>My Credentials</b> from the drop-down menu, and locate the name on the right of <b>IAM User Name</b> .
domain	Yes	<b>BaseUser</b> object	Domain information of the user who performed the operation generating the trace.
user_name	Yes	String	Username. The meaning of <b>user_name</b> is the same as that of <b>name</b> .
principal_is_root_user	Yes	String	Whether the operator is a root user. <ul style="list-style-type: none"> <li>If the value is <b>true</b>, the operator is a root user.</li> <li>If the value is <b>false</b>, the operator is an IAM user of an entrusted session identity, a federated identity, or a non-root user.</li> </ul>
invoked_by	Yes	Array of strings	Name of the service that sends the request. The value is <b>["service.console"]</b> for console operations.
session_context	No	<b>SessionContext</b> object	Temporary security credential attribute.

**Table 8-3** BaseUser

Field	Mandatory	Type	Description
id	Yes	String	Account ID. To obtain it, hover over the username in the upper right corner of the console, select <b>My Credentials</b> from the drop-down menu, and locate the ID on the right of <b>Account ID</b> .
name	Yes	String	Account name. To obtain it, hover over the username in the upper right corner of the console, select <b>My Credentials</b> from the drop-down menu, and locate the name on the right of <b>Account Name</b> .

**Table 8-4** SessionContext

Field	Mandatory	Type	Description
attributes	No	<a href="#">Attributes</a> object	Temporary security credential attribute.

**Table 8-5** Attributes

Field	Mandatory	Type	Description
mfa_authenticated	No	String	Whether MFA identity authentication has been passed.
created_at	No	String	Time when a temporary security credential is issued.

## 8.2 Example Traces

This section provides two example traces and describes their key fields to help you better understand traces. You can read other traces in a similar way as shown below.

For details on the fields in a trace file, see [Trace Structure](#).

- [ECS Server Creation](#)
- [EVS Disk Creation](#)

## ECS Server Creation

```
{
  "trace_id": "cbdd4480-2e03-11ef-82de-cf140e2a70fb",
  "trace_name": "createServer",
  "resource_type": "ecs",
  "trace_rating": "normal",
  "api_version": "1.0",
  "source_ip": "124.71.93.243",
  "domain_id": "7e0d78c85***d0b9b7cba",
  "trace_type": "ConsoleAction",
  "service_type": "ECS",
  "event_type": "system",
  "project_id": "07066c6fc90025a02f6dc01e105b286e",
  "read_only": false,
  "tracker_name": "system",
  "operation_id": "ListSubscriptions",
  "resource_account_id": "7e0d78c85***d0b9b7cba",
  "time": 1718777931170,
  "resource_name": "ecs-test",
  "user": {
    "access_key_id": "HSTAZVL6WYS0J5MYE2GA",
    "account_id": "7e0d78c85***d0b9b7cba",
    "user_name": "IAMUserA",
    "domain": {
      "name": "IAMDomainB",
      "id": "7e0d78c85***d0b9b7cba"
    },
    "name": "IAMUserA",
    "principal_is_root_user": "true",
    "id": "f36972ced***d619f1214",
    "principal_urn": "iam::7e0d78c85***d0b9b7cba:user:IAMUserA",
    "type": "User",
    "principal_id": "f36972ced***d619f1214"
  },
  "record_time": 1718777931170,
  "request": "{\n  \"server\":{\n    \"adminPass\": \"*****\",\n    \"extendparam\":{\n      \"chargingMode\": \"0\",\n      \"regionID\": \"cn-north-4\",\n      \"count\": 1,\n      \"metadata\":{\n        \"op_svc_userid\": \"f36972ced***d619f1214\",\n        \"_support_agent_list\": \"hss.ces\",\n        \"availability_zone\": \"cn-north-4c\",\n        \"description\": \"\",\n        \"name\": \"ecs-test\",\n        \"imageRef\": \"7d940784-ac0a-425f-b3fa-8478f1a1df70\",\n        \"root_volume\":{\n          \"volumetype\": \"GPSSD\",\n          \"extendparam\":{\n            \"resourceSpecCode\": \"GPSSD\",\n            \"resourceType\": \"3\",\n            \"size\": 40,\n            \"metadata\": null,\n            \"hw.passthrough\": false,\n            \"cluster_type\": null,\n            \"cluster_id\": null,\n            \"iops\": null,\n            \"throughput\": null,\n            \"data_volumes\": [],\n            \"flavorRef\": \"sn3.small.1\",\n            \"personality\": [],\n            \"vpcid\": \"250ad46d-9c89-44ec-a97d-293da771b06b\",\n            \"security_groups\": [\n              {\n                \"id\": \"3bb87748-e387-42e5-ad7a-4331638f1321\",\n                \"nics\": [\n                  {\n                    \"subnet_id\": \"1a02d148-e7f9-4a3c-ba58-18099dfbf752\",\n                    \"nictype\": \"\",\n                    \"ip_address\": \"\",\n                    \"port_id\": null,\n                    \"binding:profile\": {\n                      \"disable_security_groups\": false,\n                      \"extra_dhcp_opts\": [],\n                      \"ipv6_bandwidth\": null,\n                      \"ipv6_enable\": false,\n                      \"driver_mode\": null,\n                      \"allowed_address_pairs\": null,\n                      \"efi_enable\": false,\n                      \"efi_protocol\": null,\n                      \"publicip\": {\n                        \"id\": null,\n                        \"eip\": {\n                          \"bandwidth\": {\n                            \"name\": \"ecs-test-bandwidth\",\n                            \"size\": 1,\n                            \"id\": null,\n                            \"sharetype\": \"PER\",\n                            \"productid\": \"\",\n                            \"chargemode\": \"traffic\",\n                            \"extendparam\": {\n                              \"chargingMode\": \"postPaid\",\n                              \"iptype\": \"5_bgp\",\n                              \"iproductid\": \"\",\n                              \"key_name\": \"KeyPair-ebbe\",\n                              \"isAutoRename\": false,\n                              \"server_tags\": [],\n                              \"batch_create_in_multi_az\": false,\n                              \"spod_enable\": false,\n                              \"user_data\": \"\"\n                            }\n                          }\n                        }\n                      }\n                    }\n                  }\n                }\n              }\n            ],\n            \"message\": \"success\",\n            \"response\": {\n              \"job_id\": \"ff8080828fe9028a01902f2542df1b10\",\n              \"job_type\": \"createSingleServer\",\n              \"begin_time\": \"2024-06-19T06:18:09.502Z\",\n              \"end_time\": \"2024-06-19T06:18:51.169Z\",\n              \"status\": \"SUCCESS\",\n              \"error_code\": null,\n              \"fail_reason\": null,\n              \"entities\": {\n                \"server_id\": \"7285ea5d-f15c-4d9c-9e4e-37d37023f2f4\"\n              }\n            },\n            \"resource_id\": \"7285ea5d-f15c-4d9c-9e4e-37d37023f2f4\",\n            \"request_id\": \"null\"\n          }\n        }\n      }\n    }\n  }
}
```

You can pay special attention to the following fields:

- **time** indicates the timestamp when a trace was generated. In this example, the value is **1718777931170**.
- **user** indicates the user who performed the operation. In this example, the user is **IAMUserA** (**name** field) under the account **IAMDomainB** (**domain** field).

- **request** indicates the request to create an ECS. It contains basic information about the ECS, such as its name (**ecs-test-bandwidth**) and VPC ID (**250ad46d-9c89-44ec-a97d-293da771b06b**).
- **response** indicates the response to the ECS creation request. It contains **status** (**SUCCESS** in this example), **error\_code** (**null** in this example), and **fail\_reason** (**null** in this example).

## EVS Disk Creation

```
{
  "trace_id": "c4ddaa0b-2e05-11ef-bdc6-e1851d8cb7fb",
  "trace_name": "deleteVolume",
  "resource_type": "evs",
  "trace_rating": "normal",
  "api_version": "1.0",
  "source_ip": "124.71.93.243",
  "domain_id": "7e0d78c85***d0b9b7cba",
  "trace_type": "ConsoleAction",
  "service_type": "EVS",
  "event_type": "system",
  "project_id": "07066c6fc90025a02f6dc01e105b286e",
  "read_only": false,
  "resource_id": "bc661a99-3088-4e86-899f-fb4f46c2bb71",
  "tracker_name": "system",
  "resource_account_id": "7e0d78c85***d0b9b7cba",
  "time": 1718778778419,
  "user": {
    "access_key_id": "HSTAA8960GPIROJGW19L",
    "account_id": "7e0d78c85***d0b9b7cba",
    "user_name": "IAMUserA",
    "domain": {
      "name": "IAMDomainB",
      "id": "7e0d78c85***d0b9b7cba"
    },
    "name": "IAMUserA",
    "principal_is_root_user": "true",
    "id": "f36972ced***d619f1214",
    "principal_urn": "iam::7e0d78c85***d0b9b7cba:user:IAMUserA",
    "type": "User",
    "principal_id": "f36972ced***d619f1214"
  },
  "record_time": 1718778778419,
  "request": "",
  "response": "{\"job_id\":\"defe9cf7b5ca4566860edbebb181e17a\",\"job_type\":\"deleteVolume\", \"begin_time\":\"2024-06-19T06:32:53.018Z\", \"end_time\":\"2024-06-19T06:32:58.411Z\", \"status\": \"SUCCESS\", \"error_code\": null, \"fail_reason\": null, \"entities\": {\"volume_type\": \"GPSSD\", \"volume_id\": \"bc661a99-3088-4e86-899f-fb4f46c2bb71\", \"size\": 10, \"name\": \"volume-d64d\"}}, \"resource_name\": \"volume-d64d\", \"request_id\": \"defe9cf7b5ca4566860edbebb181e17a\""}
}
```

You can pay special attention to the following fields:

- **time** indicates the timestamp when a trace was generated. In this example, the value is **1718778778419**.
- **user** indicates the user who performed the operation. In this example, the user is **IAMUserA** (**name** field) under the account **IAMDomainB** (**domain** field).
- **request**: optional. It is null in this example.
- **response** records the returned result of disk deletion.



- **trace\_rating** indicates the trace status. It can replace the **response** field to indicate the operation result. In this example, the value is **normal**, indicating that the operation was successful according to [Trace Structure](#).

# 9 Cross-Tenant Transfer Authorization

## Scenario



To centrally manage management traces, you can configure the management tracker to transfer the traces of multiple accounts to one OBS bucket. This topic describes how to configure cross-tenant transfer.

## Authorizing Cross-Tenant Transfer

1. Tenant B logs in to the management console.

### NOTE

- Tenant A is the account for which you want to configure cross-tenant transfer, and tenant B is the account where the OBS bucket resides.
- OBS does not support cross-region transfer. Currently, OBS buckets must be located in the same region of different tenants.

2. Click  in the upper left corner to select the desired region and project.
3. Click  in the upper left corner and choose **Storage > Object Storage Service**.
4. In the navigation pane, choose **Buckets**. In the bucket list, click the name of the desired bucket. The **Objects** page is displayed.
5. In the navigation pane, choose **Permissions > Bucket Policies**.
6. In the upper right corner of the page, select **JSON** and click **Edit**, and grant permissions to tenant A as follows. Set the italic parameters based on site requirements. Bucket policies are described in JSON format. For details, see [Bucket Policy Parameters](#).

Bucket policies have different authorization objects based on tenant A's login modes. The login modes include logging in as a common user, logging in as a federated tenant, switching as an agency, and logging in as an IAM Identity Center user.

- When tenant A logs in to the console as a common user to configure a CTS tracker:

```
{  
  "Statement": [{  
    "Sid": "xxxx",  
    "Effect": "Allow",
```

```

    "Principal": {
      "ID": [
        "domain/Domain ID of tenant A:agency/cts_admin_trust"
      ]
    },
    "Action": [
      "PutObject"
    ],
    "Resource": [
      "Example bucket name/*"
    ]
  }, {
    "Sid": "xxxx1",
    "Effect": "Allow",
    "Principal": {
      "ID": [
        "domain/Domain ID of tenant A:user/*"
      ]
    },
    "Action": [
      "HeadBucket",
      "ListBucket"
    ],
    "Resource": [
      "Example bucket name"
    ]
  }
]
}

```

- When tenant A logs in to the console as a federated tenant to configure a CTS tracker:

```

{
  "Statement": [{
    "Sid": "xxxx",
    "Effect": "Allow",
    "Principal": {
      "ID": [
        "domain/Domain ID of tenant A:agency/cts_admin_trust"
      ]
    },
    "Action": [
      "PutObject"
    ],
    "Resource": [
      "Example bucket name/*"
    ]
  }, {
    "Sid": "xxxx1",
    "Effect": "Allow",
    "Principal": {
      "Federated": [
        "domain/Domain ID of tenant A:identity-provider/Provider name"
      ]
    },
    "Action": [
      "HeadBucket",
      "ListBucket"
    ],
    "Resource": [
      "Example bucket name"
    ]
  }
]
}

```

- When a user switches to tenant A as an agency to configure the CTS tracker:

```

{
  "Statement": [{

```

```

        "Sid": "xxxx",
        "Effect": "Allow",
        "Principal": {
            "ID": [
                "domain/Domain ID of tenant A:agency/cts_admin_trust"
            ]
        },
        "Action": [
            "PutObject"
        ],
        "Resource": [
            "Example bucket name/*"
        ]
    }, {
        "Sid": "xxxx1",
        "Effect": "Allow",
        "Principal": {
            "ID": [
                "domain/Domain ID of tenant A:agency/Agency name"
            ]
        },
        "Action": [
            "HeadBucket",
            "ListBucket"
        ],
        "Resource": [
            "Example bucket name"
        ]
    }
}
]

```

- When tenant A logs in to the console as an IAM Identity Center user to configure a CTS tracker:

```

{
  "Statement": [{
    "Sid": "xxxx",
    "Effect": "Allow",
    "Principal": {
      "ID": [
        "domain/Domain ID of tenant A:agency/cts_admin_trust"
      ]
    },
    "Action": [
      "PutObject"
    ],
    "Resource": [
      "Example bucket name/*"
    ]
  }, {
    "Sid": "xxxx1",
    "Effect": "Allow",
    "Principal": {
      "ID": [
        "domain/Domain ID of tenant A:agency/Agency name"
      ]
    },
    "Action": [
      "HeadBucket",
      "ListBucket"
    ],
    "Resource": [
      "Example bucket name"
    ]
  }
]
}

```

**Table 9-1** Bucket policy parameters

Parameter	Description
Sid	ID of a statement. The value is a string that describes the statement.
Action	Actions which a statement applies to. This parameter specifies a set of all the operations supported by OBS. Its values are case insensitive. CTS requires only two actions: <b>PutObject</b> and <b>HeadBucket</b> .
Effect	Whether the permission in a statement is allowed or denied. The value is <b>Allow</b> or <b>Deny</b> .
Principal	Tenant A is authorized to use the bucket policy. You can obtain the domain ID on the <b>My Credential</b> page. Principal formats: <ul style="list-style-type: none"> <li>• <b>domain/Tenant A's account ID:agency/cts_admin_trust:</b> indicates that permissions are granted to the <b>cts_admin_trust</b> agency of tenant A, allowing CTS to transfer logs to OBS buckets using the agency. For details, see <a href="#">Bucket Policy Parameters</a>.</li> <li>• <b>domain/Account ID:user/*:</b> indicates that permissions are granted to all users of tenant A.</li> <li>• <b>domain/Account ID:identity-provider/provider-name:</b> indicates that permissions are granted to the specified identity provider of tenant A.</li> </ul>
Resource	A group of resources on which the statement takes effect. The wildcard (*) is supported, indicating all resources. <i>Example bucket name/*</i> and <i>Example bucket name</i> are required for cross-account transfer.

7. Click **Save**.
8. If the OBS bucket of tenant B is encrypted using a custom key, you need to authorize tenant A in Data Encryption Workshop (DEW). For details, see [Creating a Grant](#).

 **NOTE**

You are advised to use a custom key when configuring encryption for buckets of different tenants. Otherwise, the default OBS key of tenant A may be used. In this case, tenant B may fail to download transferred files.



Server-Side Encryption Disable **SSE-KMS** SSE-OBS  
Encryption keys managed by KMS are used to encrypt your objects.

Encryption Algorithm AES256 **SM4**  
Choose the algorithm you want to encrypt your data.

Encryption Key Type Default **Custom**  
You can use a custom key below to encrypt your objects.

Project

Custom KMS-3430  [Create KMS Key](#)

9. Tenant A logs in to the management console.
10. Click  in the upper left corner to select the desired region and project.
11. Click  in the upper left corner and choose **Management & Governance > Cloud Trace Service**. The CTS console is displayed.
12. Choose **Tracker List** in the navigation pane.
13. Locate a data tracker and click **Configure** in the **Operation** column.
14. Select **Yes** for **Transfer to OBS**. If **OBS Bucket Account** is set to **Other users**, you need to enter the name of the bucket used for transfer.
15. Click **OK** to complete the tracker configuration.

# 10 Verifying Trace File Integrity



---

## 10.1 Enabling Verification of Trace File Integrity

### Scenario

During a security investigation, operational records will not be able to serve as effective and authentic evidence if they are deleted or tampered with. You can enable the integrity verification on CTS to ensure the authenticity of trace files. The verification is performed only on management traces.

### Procedure

1. Log in to the management console.
2. Click  in the upper left corner to select the desired region and project.
3. Click  in the upper left corner and choose **Management & Governance > Cloud Trace Service**. The CTS console is displayed.
4. Choose **Tracker List** in the left navigation pane.

 **NOTE**

Click **Enable CTS** if you have not enabled CTS. For details about how to enable CTS, see [Overview](#).

5. Click **Configure** in the row of the management tracker **system**. On the displayed **Configure Tracker** page, click **Next**, and enable **Verify Trace File** in the **Configure Transfer** step.

 **NOTE**

CTS supports integrity verification of trace files only for the management tracker configured with OBS transfer.

## 10.2 Digest Files

### Overview

A digest file contains the names and hash values of the trace files transferred to an OBS bucket an hour ago as well as the digital signature of the previous digest file. The digital signature of this digest file is stored in metadata attributes of the digest file object. A digest file is stored in the following path:

*OBS bucket name* > **CloudTraces** > *Region* > *Year* > *Month* > *Day* > *tracker name* > **Digest** > *Service*

An example is *OBS bucket name* > **CloudTraces** > *Region* > **2016** > **5** > **19** > **system** > **Digest** > **ECS**.

### Digest File Name Format

The digest files are named as follows:

*Trace file prefix*\_**CloudTrace-Digest**\_*Region/Region-Project*\_*Time when the digest file was sent to OBS: Year-Month-DayT Hour-Minute-Second***Z.json.gz**

Example: *File Prefix*\_**CloudTrace-Digest**\_*region/region-project*\_**2016-05-30T16-20-56Z.json.gz**

### Digest File Structure

**Table 10-1** Key fields of a digest file

Field	Mandatory	Type	Description
project_id	Yes	String	Identifies the account to which a trace file covered in the digest file belongs.
digest_start_time	Yes	String	Specifies the start of the UTC time range covered by the digest file.
digest_end_time	Yes	String	Specifies the end of the UTC time range covered by the digest file.
digest_bucket	Yes	String	Specifies the name of the OBS bucket that the digest file has been sent to.
digest_object	Yes	String	Specifies where the digest file is stored in the OBS bucket.
digest_signature_algorithm	Yes	String	Specifies the algorithm used to sign the digest file.



Field	Mandatory	Type	Description
digest_end	Yes	Boolean	Specifies whether the digest file is an ending digest file.
previous_digest_bucket	No	String	Specifies the name of the OBS bucket that the previous digest file was sent to.
previous_digest_object	No	String	Specifies where the previous digest file is stored in the OBS bucket.
previous_digest_hash_value	No	String	Specifies the hexadecimal encoded hash value of the previous digest file.
previous_digest_hash_algorithm	No	String	Specifies the Hash algorithm used to hash the previous digest file.
previous_digest_signature	No	String	Specifies the digital signature of the previous digest file.
previous_digest_end	Yes	Boolean	Specifies whether the previous digest file is an ending digest file.
log_files	No	Array	Specifies the list of trace files covered in the digest file.
bucket	Yes	String	Specifies the name of the OBS bucket that the trace files have been sent to.
object	Yes	String	Specifies where the trace files are stored in the OBS bucket.
log_hash_value	Yes	String	Specifies the hexadecimal encoded hash value of the trace files.
log_hash_algorithm	Yes	String	Specifies the Hash algorithm used to hash the trace files.

## Example Digest File

A digest file contains the names and hash values of the trace files transferred to an OBS bucket an hour ago as well as the digital signature of the previous digest file. The digital signature of this digest file is stored in metadata attributes of the digest file object. A digest file is stored in the following path:

The following is an example digest file:

For details about the fields in the example, see [Table 10-1](#).

```
{
  "project_id": "3cfb09080bd944d0b4cdd72ef2685712",
  "digest_start_time": "2017-03-28T01-09-17Z",
  "digest_end_time": "2017-03-28T02-09-17Z",
```

```
"digest_bucket": "bucket",
"digest_object": "CloudTraces/ap-southeast-1/2017/3/28/Digest/EVS/mylog_CloudTrace-Digest_ap-
southeast-1/_2017-03-28T02-09-17Z.json.gz",
"digest_signature_algorithm": "SHA256withRSA",
"digest_end": false,
"previous_digest_bucket": "bucket",
"previous_digest_object": "CloudTraces/ap-southeast-1/2017/3/28/Digest/EVS/mylog_CloudTrace-Digest_ap-
southeast-1/_2017-03-28T01-09-17Z.json.gz",
"previous_digest_hash_value": "5e08875de01b894eda5d1399d7b049fe",
"previous_digest_hash_algorithm": "MD5",
"previous_digest_signature":
"7af7cbef4f3c78eab5048030d402810841400cf70eb22f93d4fedd13b13a8208a5dc04ce2f8bd0a4918f933ca3fc
b17595ae59386a2dc3e3046fa97688a9815a2d036fa10193534c0ebbecff67221e22ac9cf8b781cbae3a81eaccfc
0a2bd1a99081b1e4fe99b19caa771876ba7cce16d002feb4578cd89bc6f1faaca639ab48f3cb56007bcc5e248968
f4a17a95b8cd8bc7d8bbd7c63630da878cd4d471fc75c60bac5f730d94fefe8fdd2f2fa8accd62dbe100eab7773e79
15e91be4474291b9dacea63a8267390bcb4855b5825554ebb07d4a29ce077c364213c575c461d1e9fafa0c29fde
1c6de1d5630e015200821b2f3ae91e53cd8591433dd7c0b4c8bc",
"previous_digest_end": false,
"log_files": [{
  "bucket": "bucket",
  "object": "CloudTraces/ap-southeast-1/2017/3/28/ECS/mylog_CloudTrace_ap-southeast-1/
_2017-03-28T02-09-17Z_0faa86bc40071242.json.gz",
  "log_hash_value": "633a8256ae7996e21430c3a0e9897828",
  "log_hash_algorithm": "MD5"
}]
}
```

## Digest File Signature

The digital signature information of a digest file is in two metadata attributes of the digest file object. Each digest file has the following two metadata items:

- meta-signature

Hexadecimal encoded value of the digest file signature. Example:

```
7af7cbef4f3c78eab5048030d402810841400cf70eb22f93d4fedd13b13a8208a5dc04ce2f8bd0a4918f933c
a3fcb17595ae59386a2dc3e3046fa97688a9815a2d036fa10193534c0ebbecff67221e22ac9cf8b781cbae3
a81eaccfc0a2bd1a99081b1e4fe99b19caa771876ba7cce16d002feb4578cd89bc6f1faaca639ab48f3cb560
07bcc5e248968f4a17a95b8cd8bc7d8bbd7c63630da878cd4d471fc75c60bac5f730d94fefe8fdd2f2fa8accd
62dbe100eab7773e7915e91be4474291b9dacea63a8267390bcb4855b5825554ebb07d4a29ce077c3642
13c575c461d1e9fafa0c29fde1c6de1d5630e015200821b2f3ae91e53cd8591433dd7c0b4c8bc
```

- meta-signature-algorithm

Algorithm used to sign the digest file. Example:

SHA256withRSA

## Supplementary Information

- Starting Digest File

A starting digest file is generated after you start verifying trace file integrity. In a starting digest file, the following fields related to the previous digest file will be left empty:

- previous\_digest\_bucket
- previous\_digest\_object
- previous\_digest\_hash\_value
- previous\_digest\_hash\_algorithm
- previous\_digest\_signature

- "Empty" Digest File

CTS will still send a digest file even if no operations have occurred in your account within the one-hour time period recorded by the digest file. The last

field **log\_files:[]** of the digest file will be left empty. It helps you to confirm that no trace files have been sent within the one-hour time period recorded by the digest file.

- Digest File Chain

A digest file contains the digital signature and Hash value of the previous digest file (if any) so that a chain is formed. You can verify digest files successively within a specified time, starting with the latest one.

- Digest File Bucket

A digest file is sent to the OBS bucket that stores trace files recorded in the file.

- Digest File Storage Folder

A digest file is stored in a folder different from that for trace files, making it easy for you to execute fine-grained security policies.

## 10.3 Verifying Trace File Integrity

### Scenario

CTS uses public signature algorithms and hash functions in accordance with industry standards, so you can create tools on your own to verify integrity of CTS trace files. Trace files should contain fields **time**, **service\_type**, **resource\_type**, **trace\_name**, **trace\_rating**, and **trace\_type** for integrity verification. Other fields can be added by services from which traces are collected.

After you enable integrity verification of trace files in CTS, digest files will be sent to your OBS buckets, and you can implement your own verification solution. For details about digest files, see [Digest Files](#).

### Prerequisites

You should understand how digest files are signed.

RSA digital signatures are used in CTS. For each digest file, CTS will:

1. Create a message for digital signing, a character string composed of specified digest file fields, and obtain an RSA private key.
2. Produce a hash value of the digest message. Use the RSA algorithm to generate a digital signature with the hash value and private key, and encode the digital signature to hexadecimal format.
3. Put the digital signature into the meta-signature attribute of the digest file object.

The message for digital signing contains the following digest file fields:

- The ending timestamp of the UTC time range covered by the digest file, for example, 2017-03-28T02-09-17Z.
- The path where the current digest file is stored in the OBS bucket.
- The hash value (hexadecimal encoded) of the current digest file (compressed).
- The hexadecimal digital signature of the previous digest file.

## Procedure

Verify a digest file first and then its referenced trace files.

1. Obtain a digest file.
  - a. Download **OBS Java SDK** from the Huawei Cloud website and call an OBS client interface to obtain the latest digest file within the required time period from OBS buckets.
  - b. Check whether the location where the digest file is stored in the OBS bucket matches with the location recorded in the file.
  - c. Obtain the digital signature from the meta-signature attribute of the digest file object.

2. Obtain the RSA public key for verifying the digital signature.

The RSA public key of CTS is as follows:

```
MIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsjQDkl8COPRhOCvm7Zl8sYZ20ojt+ay/  
gwRSk9q0gkY3pP0RrAhSsEzgYdYjaMCqixkmbpt4AH9AROU4drnoCAZSMqRxcgv0bGC9kVd4q95l4zibsw  
AsksjuNQo/XoJBl+rRAqCa+1uetgVU4k4Yx8RryYxYx/tlmvMe/O4mGAlaTf+rsqt3VXR1Qlj5IYR/nx41BEgC/  
Kb1elYAFDaaab8W55INRprj7qdu6oAo4Ug47WqbecvEtG3JRpj5+oqLyW41Fvse3osC0h5DQdxTt4x00/rVZ  
+gH7Kua00y7gC8YOxFVpYbfn/oW61PUDeHG/N9hUjOrlgDDJpD2YbClQIDAQAB
```

3. Recreate the message for digital signing.

Compute the message for digital signing.

The message is in the following format:

```
signature_string = digest_end_time  
+ digest_object  
+ Hex(hash(digest-file-content))  
+ previous_digest_signature
```

The following is an example message for digital signing.

```
2017-03-28T02-09-17ZCloudTraces/ap-southeast-1/2017/3/28/Digest/EVS/mylog_CloudTrace-  
Digest_ap-  
southeast-1_2017-03-28T02-09-17Z.json.gze280d203da44015e0eda3faa7a2ec9612221cc0dc8b0fe320d  
b4febe60142350641ad19da18cb6d3f5e7faad792c3efe98836c6d6547f5e5c7a48f7088000a057af26cc3b  
b913cae1637bfa9e4231b7d1fd6d98eaba735e509e7c5ea3c6757f732b4468f7418ef18e3312ac696dd78  
6ec5792eac94aee27cd7be76bf23b641c5e9a686cca6414745787254100c2bee31e584a15c2229270f9dee  
81f9043574
```

4. Verify a digest file.

Pass the computed message obtained in [3](#), digital signature of the digest file, and public key to the RSA signature verification algorithm. If **true** is returned, the digital signature of the digest file matches with the computed message and the digest file is valid.

5. Verify trace files.

You can verify trace files referenced by the digest file after confirming that the digest file is valid.

The digest file records the hash value of each trace file. After a trace file is uploaded to OBS, its hash value will be stored in ETag metadata. If the trace file is modified after CTS sent it to an OBS bucket, the file's hash value will change, and the digital signatures of the digest file will not match.

Do as follows to verify a trace file:

- a. Obtain **bucket** and **object** information about a trace file from the digest file.
- b. Call the OBS client interface to obtain the ETag metadata value in the trace file object header.

- c. Obtain the hash value of the trace file from the **log\_hash\_value** field in the digest file.
  - d. Compare the ETag metadata value with the hash value obtained in the previous step. If they match, the trace file is valid.
6. Verify the previous digest files and trace files.

In each digest file, the following fields provide the location and signature of the previous digest file:

- previous\_digest\_bucket
- previous\_digest\_object
- previous\_digest\_signature

Repeat steps 4 and 5 to verify the signature of each previous digest file and all trace files that the file references.

For these previous digest files, you do not need to obtain the digital signature from the meta-signature attribute of the digest file object. The **previous\_digest\_signature** field in each digest file provides the digital signature of the previous digest file. You can keep verifying the previous digest files and their referenced trace files until you reach the starting digest file or the digest file chain is disconnected.

The following code segment is an example for verifying CTS digest and trace files. The code segment uses the following JAR packages, and you are recommended to use these packages:

- esdk-obs-java-2.1.16.jar
- commons-logging-1.2.jar
- httpasyncclient-4.1.2.jar
- httpclient-4.5.3.jar
- httpcore-4.4.4.jar
- httpcore-nio-4.4.4.jar
- java-xmlbuilder-1.1.jar
- jna-4.1.0.jar
- log4j-api-2.8.2.jar
- log4j-core-2.8.2.jar
- commons-codec-1.9.jar
- json-20160810.jar
- commons-io-2.5.jar

Example code segment:

```
import java.io.BufferedInputStream;
import java.io.BufferedReader;
import java.io.ByteArrayInputStream;
import java.io.InputStream;
import java.io.InputStreamReader;
import java.security.KeyFactory;
import java.security.MessageDigest;
import java.security.PublicKey;
import java.security.Signature;
import java.security.spec.X509EncodedKeySpec;
import java.util.Arrays;
import java.util.zip.GZIPInputStream;

import org.apache.commons.codec.binary.Base64;
```

```
import org.apache.commons.codec.binary.Hex;
import org.apache.commons.io.IOUtils;
import org.json.JSONObject;

import com.obs.services.ObsClient;
import com.obs.services.ObsConfiguration;
import com.obs.services.model.ObjectMetadata;
import com.obs.services.model.S3Object;

public class DigestFileValidator {
    public static void main(String[] args) {
        // Name of the bucket where a digest file is located.
        String digestBucket = "bucketname";
        // Path where a digest file is stored. Example: CloudTraces/eu-de/2017/11/15/Digest/ECS/
tGPYa_CloudTrace-Digest_eu-de_2017-11-15T10-12-10Z.json.gz.
        String digestObject = "digestObject";

        // Directly writing AK/SK in code is risky. For security, encrypt your AK/SK and store them in the
        configuration file or environment variables.
        // In this example, the AK/SK are stored in environment variables for identity authentication.
        Before running this example, set environment variables HUAWEICLOUD_SDK_AK and
HUAWEICLOUD_SDK_SK.
        String ak = System.getenv("HUAWEICLOUD_SDK_AK");
        String sk = System.getenv("HUAWEICLOUD_SDK_SK");

        ObsConfiguration obsConfig = new ObsConfiguration();
        obsConfig.setEndPoint("obs.ap-southeast-1.myhuaweicloud.com");

        ObsClient client = new ObsClient(ak, sk, obsConfig);

        try {
            // Obtain a digest file object.
            S3Object object = client.getObject(digestBucket, digestObject);

            InputStream is = new BufferedInputStream(object.getObjectContent());
            byte[] digestFileBytes = IOUtils.toByteArray(is);

            // Obtain the hash value of a digest file.
            MessageDigest messageDigest = MessageDigest.getInstance("MD5");
            messageDigest.update(digestFileBytes);
            byte[] digestFileHashBytes = messageDigest.digest();

            StringBuilder outStr = new StringBuilder();
            GZIPInputStream gis = new GZIPInputStream(new ByteArrayInputStream(digestFileBytes));
            BufferedReader bufferedReader = new BufferedReader(new InputStreamReader(gis, "UTF-8"));
            String line;
            while ((line = bufferedReader.readLine()) != null) {
                outStr.append(line);
            }
            bufferedReader.close();
            String digestInfo = outStr.toString();

            // Obtain the meta-signature value from the digest file header in an OBS bucket, which is the
            digital signature of the digest file.
            ObjectMetadata objectMetadata = client.getObjectMetadata(digestBucket, digestObject);
            String digestSignature = objectMetadata.getMetadata().get("meta-signature").toString();
            JSONObject digestFile = new JSONObject(digestInfo);
            // Check whether the digest file has been moved in the OBS bucket.
            if (!digestFile.getString("digest_bucket").equals(digestBucket) || !
digestFile.getString("digest_object")
                .equals(digestObject)) {
                System.err.println("Digest file has been moved from its original location.");
            } else {
                // Obtain the message for digital signing.
                String signatureString = digestFile.getString("digest_end_time") +
digestFile.getString("digest_object")
                    + Hex.encodeHexString(digestFileHashBytes) +
digestFile.getString("previous_digest_signature");
```

```
String publicKeyString
=
"MIIBlJANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsjQDkl8COPRhoCvm7ZI8sYZ20ojl+ay/
gwRSk9q0gkY3pP0RrAhSsEzgYdYjaMCqixkmbpt4AH9AROUJ4drnoCAZSMqRxcgv0bGC9kVd4q95L4zibsw
AsksjuNQo/XoJl+rRAqCa+1uetgVU4k4Yx8RryYxYx/tlmvMe/O4mGAlaTf+rsqt3VXR1Qlj5lYR/nx41BEgC/
Kb1elYAfDaaab8WSS5INRprj7qdu6oAo4Ug47WqbecvEtG3JRpj5+oqLyW41Fvse3osC0h5DQdxTt4x00/rVZ
+gH7Kua00y7gC8YOxVfPfbfn/oW61PUDeHG/N9hUjOrigDDJpD2YbCIQIDAQAB";

// Public key used for decryption.
byte[] publicKeyBytes = Base64.decodeBase64(publicKeyString);
// Form the X509EncodedKeySpec object.
X509EncodedKeySpec x509EncodedKeySpec = new X509EncodedKeySpec(publicKeyBytes);

// Specify an encryption algorithm.
KeyFactory keyFactory = KeyFactory.getInstance("RSA");
// Obtain the public key object.
PublicKey publicKey = keyFactory.generatePublic(x509EncodedKeySpec);

Signature signatureInstance = Signature.getInstance("SHA256withRSA");
signatureInstance.initVerify(publicKey);
signatureInstance.update(signatureString.getBytes("UTF-8"));

byte[] signatureHashExpect = Hex.decodeHex(digestSignature.toCharArray());

// Verify whether the signature is valid.
if (signatureInstance.verify(signatureHashExpect)) {
    System.out.println("Digest file signature is valid, validating log files...");

    for (int i = 0; i < digestFile.getJSONArray("log_files").length(); i++) {
        JSONObject logFileJson = digestFile.getJSONArray("log_files").getJSONObject(i);
        String logBucket = logFileJson.getString("bucket");
        String logObject = logFileJson.getString("object");

        // Obtain the ETag value from the trace file header in the OBS bucket, which is the
        // recorded hash value of the trace file.
        ObjectMetadata objectLogMetadata = client.getObjectMetadata(logBucket,
logObject);
        String logHashValue = objectLogMetadata.getMetadata().get("ETag").toString();
        logHashValue = logHashValue.replace("\\", "");
        byte[] logFileHash = Hex.decodeHex(logHashValue.toCharArray());

        // Obtain the hash value of each trace file from the digest file.
        byte[] expectedHash = logFileJson.getString("log_hash_value").getBytes();
        boolean hashMatch = Arrays.equals(expectedHash, logFileHash);
        if (!hashMatch) {
            System.err.println("Validate log file hash failed.");
        } else {
            System.out.println("Log file hash is valid.");
        }
    }
} else {
    System.err.println("Validate digest signature failed.");
}

System.out.println("Digest file validation completed.");

// Obtain values of fields previous_digest_bucket, previous_digest_object, and
previous_digest_signature of the previous digest file. After obtaining the digest file, verify its hash
value and digital signature.
String previousDigestBucket = digestFile.getString("previous_digest_bucket");
String previousDigestObject = digestFile.getString("previous_digest_object");

// Obtain the digital signature from the meta-signature attribute of the digest file object
header.
ObjectMetadata objectPreviousMetadata = client.getObjectMetadata(previousDigestBucket,
previousDigestObject);
String signaturePrevious = objectPreviousMetadata.getMetadata().get("meta-
signature").toString();
String signaturePreviousExpect = digestFile.getString("previous_digest_signature");
```

```
        if (signaturePrevious.equals(signaturePreviousExpect)) {
            System.out.println(
                "Previous digest file signature is valid, " + "validating previous digest file hash
value...");

            String digestPreviousHashValue =
objectPreviousMetadata.getMetadata().get("ETag").toString();
            // The ETag metadata value is the trace file hash value enclosed with quotation marks.
            You need to remove the quotation marks.
            String digestPreviousHashValueExpect = "\"" +
digestFile.getString("previous_digest_hash_value")
                + "\"";
            if (digestPreviousHashValue.equals(digestPreviousHashValueExpect)) {
                System.out.println("Previous digest file hash value is valid.");
            } else {
                System.err.println("Validate previous digest file hash value failed.");
            }
        }
    }
} catch (Exception e) {
    System.out.println("Validate digest file failed.");
}
}
```



# 11 Auditing

Cloud Trace Service (CTS) provides records of operations performed on cloud service resources.

With CTS, you can record operations associated with CTS itself for later query, audit, and backtracking.

**Table 11-1** CTS operations that can be recorded by itself

Operation	Resource Type	Trace Name
Creating a tracker	tracker	createTracker
Modifying a tracker	tracker	updateTracker
Disabling a tracker	tracker	updateTracker
Enabling a tracker	tracker	updateTracker
Deleting a tracker	tracker	deleteTracker
Creating a key event notification	notification	createNotification
Deleting a key event notification	notification	deleteNotification
Modifying a key event notification	notification	updateNotification
Changing the status of a key event notification	notification	updateNotificationStatus
Disabling a key event notification	notification	updateNotification
Enabling a key event notification	notification	updateNotification
Exporting traces	trace	getTrace

# 12 Permissions Management

---

This chapter describes how to use IAM for fine-grained permissions control for your CTS resources. With IAM, you can:

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing CTS resources.
- Manage permissions on a principle of least permissions (PoLP) basis.
- Entrust other Huawei Cloud accounts or cloud services to perform efficient O&M on your CTS resources.

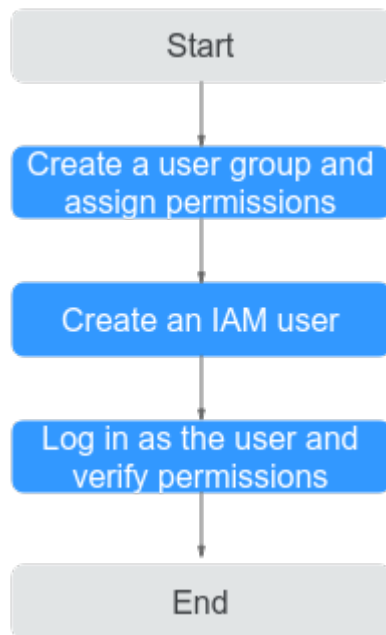
If your Huawei Cloud account does not need IAM users, you can skip this section.

## Prerequisites

Learn about the permissions (see [Permissions Management](#)) supported by CTS and choose policies or roles according to your requirements. For the permissions of other services, see [System-defined Permissions](#).

## Process Flow

**Figure 12-1** Process of granting CTS permissions



1. **Create a user group and assign permissions.**  
Create a user group on the IAM console, and attach the **CTS Administrator** policy to the group.
2. **Create an IAM user.**  
Create a user on the IAM console and add the user to the user group created in **1**.
3. **Log in** and verify permissions.  
Log in to the console as the user you created, and verify that the user has the assigned permissions.

# 13 Quota Management


---

## What Are Quotas?

A quota is a limit on the quantity or capacity of a certain type of service resources that you can use, for example, the maximum number of key event notifications that you can create.

If the existing resource quota cannot meet your requirements, you can apply for a higher quota.

## How Do I View My Quotas?

1. Log in to the management console.
2. Click  on the upper left corner and choose a region and project.
3. In the upper right corner of the page, choose **Resources > My Quotas**.  
The **Service Quota** page is displayed.
4. Check the total quotas and used quotas of resources.

# 14 Supported Services and Operations

**Table 14-1** Supported services and operations

Category	Cloud Service	Operations
Compute	Elastic Cloud Server (ECS)	<b>ECS operations that can be recorded by CTS</b>
	Image Management Service (IMS)	<b>IMS operations that can be recorded by CTS</b>
	Auto Scaling (AS)	<b>AS operations that can be recorded by CTS</b>
	FunctionGraph	<b>FunctionGraph operations that can be recorded by CTS</b>
	Cloud Phone (CPH)	<b>CPH operations that can be recorded by CTS</b>
Storage	Cloud Server Backup Service (CSBS)	<b>CSBS operations that can be recorded by CTS</b>
	Object Storage Service (OBS)	<b>OBS operations that can be recorded by CTS</b>
	Elastic Volume Service (EVS)	<b>EVS operations that can be recorded by CTS</b>
	Volume Backup Service (VBS)	<b>VBS operations that can be recorded by CTS</b>
	Scalable File Service Turbo (SFS Turbo)	<b>SFS Turbo operations that can be recorded by CTS</b>
	Cloud Backup and Recovery (CBR)	<b>CBR operations that can be recorded by CTS</b>
Network	Direct Connect (DC)	<b>DC operations that can be recorded by CTS</b>

Category	Cloud Service	Operations
	Virtual Private Cloud (VPC)	VPC operations that can be recorded by CTS
	Elastic Load Balance (ELB)	ELB operations that can be recorded by CTS
	NAT Gateway	NAT Gateway operations that can be recorded by CTS
	Virtual Private Network (VPN)	VPN operations that can be recorded by CTS
	VPC Endpoint (VPCEP)	VPCEP operations that can be recorded by CTS
	Global Accelerator (GA)	GA operations that can be recorded by CTS
	Cloud Connect (CC)	CC operations that can be recorded by CTS
	Enterprise Router (ER)	Enterprise router operations that can be recorded by CTS
Container	Cloud Container Engine (CCE)	CCE operations that can be recorded by CTS
	Software Repository for Container (SWR)	SWR operations that can be recorded by CTS
Migration	Object Storage Migration Service (OMS)	OMS operations that can be recorded by CTS
	Cloud Data Migration (CDM)	CDM operations that can be recorded by CTS
	Server Migration Service (SMS)	SMS operations that can be recorded by CTS
Management & Governance	Cloud Eye Service (CES)	CES operations that can be recorded by CTS
	Cloud Trace Service (CTS)	CTS operations that can be recorded by itself
	Identity and Access Management (IAM)	IAM operations that can be recorded by CTS
	Tag Management Service (TMS)	TMS operations that can be recorded by CTS
	Resource Access Manager (RAM)	RMS operations that can be recorded by CTS

Category	Cloud Service	Operations
	Log Tank Service (LTS)	LTS operations that can be recorded by CTS
	Config	Config operations that can be recorded by CTS
	Application Operations Management (AOM)	AOM operations that can be recorded by CTS
	Application Performance Management (APM)	APM operations that can be recorded by CTS
	Simple Message Notification (SMN)	SMN operations that can be recorded by CTS
	Resource Formation Service (RFS)	RFS operations that can be recorded by CTS
Applications and Middleware	Cloud Service Engine (CSE)	CSE operations that can be recorded by CTS
	Distributed Message Service (DMS) for Kafka	DMS for Kafka operations that can be recorded by CTS
	DMS for RabbitMQ	DMS for RabbitMQ operations that can be recorded by CTS
	DMS for RocketMQ	DMS for RocketMQ operations that can be recorded by CTS
	Distributed Cache Service (DCS)	DCS operations that can be recorded by CTS
	API Gateway (APIG)	API Gateway operations that can be recorded by CTS
Database	Relational Database Service (RDS)	RDS for MySQL operations that can be recorded by CTS
		RDS for PostgreSQL operations that can be recorded by CTS
		RDS for SQL Server operations that can be recorded by CTS
	Document Database Service (DDS)	DDS operations that can be recorded by CTS
	Data Replication Service (DRS)	DRS operations that can be recorded by CTS
	GaussDB	GaussDB operations that can be recorded by CTS

Category	Cloud Service	Operations
	GeminiDB	GeminiDB Redis operations that can be recorded by CTS
		GeminiDB Influx operations that can be recorded by CTS
		GeminiDB Cassandra operations that can be recorded by CTS
		GeminiDB Mongo operations that can be recorded by CTS
	TaurusDB	TaurusDB operations that can be recorded by CTS
	Data Admin Service (DAS)	DAS operations that can be recorded by CTS
Development and O&M	Distributed Database Middleware (DDM)	DDM operations that can be recorded by CTS
	Database and Application Migration UGO (UGO)	UGO operations that can be recorded by CTS
	ServiceStage	ServiceStage operations that can be recorded by CTS
Security	CodeArts PerfTest	PerfTest operations that can be recorded by CTS
	Cloud Application Engine (CAE)	CAE operations that can be recorded by CTS
	Data Encryption Workshop (DEW)	DEW operations that can be recorded by CTS
	Cloud Firewall (CFW)	CFW operations that can be recorded by CTS
	Anti-DDoS Service (AAD)	AAD operations that can be recorded by CTS
	Web Application Firewall (WAF)	WAF operations that can be recorded by CTS
	Database Security Service (DBSS)	DBSS operations that can be recorded by CTS
Host Security Service (HSS)	HSS operations that can be recorded by CTS	
	Data Security Center (DSC)	DSC operations that can be recorded by CTS



Category	Cloud Service	Operations
	Cloud Bastion Host (CBH)	<b>CBH operations that can be recorded by CTS</b>
	SecMaster	<b>SecMaster operations that can be recorded by CTS</b>
Enterprise Application	ROMA Connect	<b>ROMA Connect operations that can be recorded by CTS</b>
	Domain Name Service (DNS)	<b>DNS operations that can be recorded by CTS</b>
Blockchain	Blockchain Service (BCS)	<b>BCS operations that can be recorded by CTS</b>
AI	Face Recognition Service (FRS)	<b>FRS operations that can be recorded by CTS</b>
	ModelArts	<b>ModelArts operations that can be recorded by CTS</b>
	Optical Character Recognition (OCR)	<b>OCR operations that can be recorded by CTS</b>
Big Data	MapReduce Service (MRS)	<b>MRS operations that can be recorded by CTS</b>
	Data Lake Insight (DLI)	<b>DLI operations that can be recorded by CTS</b>
	GaussDB(DWS)	<b>GaussDB(DWS) operations that can be recorded by CTS</b>
	Cloud Search Service (CSS)	<b>CSS operations that can be recorded by CTS</b>
	DataArts Studio	<b>DataArts Studio operations that can be recorded by CTS</b>
Content Delivery & Edge Computing	Content Delivery Network (CDN)	<b>CDN operations that can be recorded by CTS</b>
	Intelligent EdgeFabric (IEF)	<b>IEF operations that can be recorded by CTS</b>
User Service	Enterprise Project Management (EPS)	<b>EPS operations that can be recorded by CTS</b>
Internet of Things (IoT)	Global SIM Link (GSL)	<b>GSL operations that can be recorded by CTS</b>