

Cloud Trace Service

User Guide

Issue	01
Date	2025-11-14



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

- 1 Overview..... 1**
- 2 Traces..... 3**
 - 2.1 Querying Traces in CTS..... 3
 - 2.2 Querying Transferred Traces..... 7
- 3 Management Trackers..... 10**
 - 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
- 4 Data Trackers..... 17**
 - 4.1 Creating a Tracker..... 17
 - 4.2 Configuring a Tracker..... 20
 - 4.3 Disabling or Enabling a Tracker..... 23
 - 4.4 Deleting a Tracker..... 24
- 5 Organization Trackers..... 26**
 - 5.1 Overview..... 26
 - 5.2 Setting CTS as a Trusted Service..... 27
 - 5.3 Configuring an Organization Tracker..... 27
- 6 Using Advanced Query..... 31**
 - 6.1 Enabling Advanced Query and Configuring Field Indexing..... 31
 - 6.2 Querying Access Key Traces..... 34
 - 6.3 Querying Huawei Cloud Account Traces..... 34
- 7 Creating a Key Event Notification..... 36**
- 8 Configuring Query Trace Reporting for Cloud Services..... 41**
- 9 Application Examples..... 44**
 - 9.1 Security Auditing..... 44
 - 9.2 Fault Locating..... 46
 - 9.3 Resource Tracking..... 48
- 10 Trace References..... 50**
 - 10.1 Trace Structure..... 50

10.2 Example Traces..... 55

10.3 Relationship Between IAM Identities and Operators..... 58

11 Cross-Tenant Transfer Authorization.....64

12 Verifying Trace File Integrity..... 69

12.1 Enabling Verification of Trace File Integrity..... 69

12.2 Digest Files..... 69

12.3 Verifying Trace File Integrity..... 73

13 Auditing.....79

14 Permissions Management..... 80

15 Quota Management..... 82

16 Supported Services and Operations..... 83

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 Object Storage Service (OBS) buckets.

You can only query operation records of the last seven days on the CTS console. To query operation records older than seven days, store trace files in an OBS bucket or Log Tank Service (LTS) log stream. Ensure that you have enabled OBS and LTS and have full permissions for the OBS bucket and LTS log stream you are going to use. By default, only the owner of OBS buckets can access the buckets and all objects contained in the buckets, but the owner can grant access permissions to other services and users by configuring access policies.

Prerequisites

- To configure the trace transfer function, you must enable OBS and LTS.
- To enable the key event notification function, you must enable Simple Message Notification (SMN).

Associated Services

- OBS: used to store trace files.
- 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 the console using a Huawei Cloud account, go to [Step 3](#). If you log in to the console as an Identity and Access Management (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.

 NOTE

The management tracker logs user operations like creation, login, and deletion on all cloud service resources. For details about cloud services supported by CTS, see [Supported Services and Operations](#).

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 and check operation records of the last seven days.

----End

2 Traces

2.1 Querying Traces in CTS

Scenarios

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

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

Constraints

- You can only query operation records of the last seven days on the CTS console. They are automatically deleted upon expiration and cannot be manually deleted. To store them for longer than seven days, configure transfer to Object Storage Service (OBS) or Log Tank Service (LTS) so that you can view them in OBS buckets or LTS log groups.
- After creating, modifying, or deleting a cloud service resource, you can query management traces on the CTS console 1 minute later and query data traces 5 minutes later.
- Data traces are not displayed in the trace list of the new version. To view them, you need to go to the old version.

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

Step 1 Log in to the [CTS console](#).

Step 2 In the navigation pane, choose **Trace List**.

Step 3 In the time range drop-down list above the trace list, select a desired query time range: **Last 1 hour**, **Last 1 day**, or **Last 1 week**. You can also select **Custom** to specify a custom time range within the last seven days.

Step 4 The search box above the trace list supports advanced queries. Combine one or more filters to refine your search.

Table 2-1 Trace filtering parameters

Parameter	Description
Trace Name	Name of a trace. The entered value is case-sensitive and requires an exact match. Fuzzy matching is not supported. For details about the operations that can be audited for each cloud service, see Supported Services and Operations. Example: updateAlarm
Trace Source	Cloud service name abbreviation. The entered value is case-sensitive and requires an exact match. Fuzzy matching is not supported. Example: IAM
Resource Name	Name of a cloud resource involved in a trace. The entered value is case-sensitive and requires an exact match. Fuzzy matching is not supported. 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. Example: ecs-name
Resource ID	ID of a cloud resource involved in a trace. The entered value is case-sensitive and requires an exact match. Fuzzy matching is not supported. Leave this field empty if the resource has no resource ID or if resource creation failed. Example: {VM ID}
Trace ID	Value of the trace_id parameter for a trace reported to CTS. The entered value requires an exact match. Fuzzy matching is not supported. Example: 01d18a1b-56ee-11f0-ac81-*****1e229
Resource Type	Type of a resource involved in a trace. The entered value is case-sensitive and requires an exact match. Fuzzy matching is not supported. For details about the resource types of each cloud service, see Supported Services and Operations. Example: user
Operator	User who triggers a trace. Select one or more operators from the drop-down list. If the value of trace_type in a trace is SystemAction, the operation is triggered by the service and the trace's operator may be empty.

Parameter	Description
Trace Status	Select one of the following options from the drop-down list: ● normal: The operation succeeded. ● warning: The operation failed. ● incident: The operation caused a fault that is more serious than a normal failure, for example, causing other faults.

- Step 5** On the **Trace List** page, you can also export and refresh the trace list, and customize columns to display.
- 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 5,000 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.

- Step 6** (Optional) On the **Trace List** page of the new edition, click **Old Edition** in the upper right corner to switch to the **Trace List** page of the old edition.

----End

Viewing Traces in the Trace List of the Old Edition

- Step 1** Log in to the [CTS console](#).
- Step 2** In the navigation pane, choose **Trace List**.
- Step 3** Each time you log in to the CTS console, the new edition is displayed by default. Click **Old Edition** in the upper right corner to switch to the trace list of the old edition.
- Step 4** In the upper right corner of the page, set a desired query time range: **Last 1 hour**, **Last 1 day**, or **Last 1 week**. You can also click **Customize** to specify a custom time range within the last seven days.
- Step 5** Set filters to search for your desired traces.

Table 2-2 Trace filtering parameters

Parameter	Description
Trace Type	Select Management or Data . ● Management traces record operations performed by users on cloud service resources, including creation, modification, and deletion. ● Data traces are reported by OBS and record operations performed on data in OBS buckets, including uploads and downloads.

Parameter	Description
Trace Source	Select the name of the cloud service that triggers a trace from the drop-down list.
Resource type	Select the type of the resource involved in a trace from the drop-down list. For details about the resource types of each cloud service, see Supported Services and Operations .
Search By	Select one of the following options: ● Resource ID: ID of the cloud resource involved in a trace. Leave this field empty if the resource has no resource ID or if resource creation failed. ● Trace name: name of a trace. For details about the operations that can be audited for each cloud service, see Supported Services and Operations. ● Resource name: name of the cloud resource involved in a trace. 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.
Operator	User who triggers a trace. Select one or more operators from the drop-down list. If the value of trace_type in a trace is SystemAction , the operation is triggered by the service and the trace's operator may be empty.
Trace Status	Select one of the following options: ● Normal: The operation succeeded. ● Warning: The operation failed. ● Incident: The operation caused a fault that is more serious than a normal failure, for example, causing other faults.

Step 6 Click **Query**.

Step 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 5,000 records.
- Click  to view the latest information about traces.

Step 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	View Trace

request

trace_id

code

trace_name

resource_type

trace_rating

api_version

message

source_ip

domain_id

trace_type

ApiCall

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

View Trace	×
<pre>{ "request": "", "trace_id": " ", "code": "200", "trace_name": "createDockerConfig", "resource_type": "dockerlogincmd", "trace_rating": "normal", "api_version": "", "message": "createDockerConfig, Method: POST Url=/v2/manage/utils/secret, Reason:", "source_ip": " ", "domain_id": " ", "trace_type": "ApiCall", "service_type": "SWR", "event_type": "system", "project_id": " ", "response": "", "resource_id": "", "tracker_name": "system", "time": "Nov 16, 2023 10:54:04 GMT+08:00", "resource_name": "dockerlogincmd", "user": { "domain": { "name": " ", "id": " " } } }</pre>	

Step 10 (Optional) On the **Trace List** page of the old edition, click **New Edition** in the upper right corner to switch to the **Trace List** page of the new edition.

----End

2.2 Querying Transferred Traces

Scenarios

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

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

Constraints

For global services, you must configure trackers on the CTS console in the central region (EU-Dublin). This configuration enables the function of transferring traces to OBS or LTS. This function will not take effect if you perform the configuration on the CTS console in any other regions.

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

Prerequisites

You have configured a tracker in CTS and enabled **Transfer to OBS** or **Transfer to LTS**. For details about how to configure transfer, see [Configuring a Tracker](#).

Querying Traces Transferred to OBS

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

1. Log in to the management console.
2. Click  in the upper left corner and choose **Management & Governance > Cloud Trace Service**. The CTS console is displayed.
3. Choose **Tracker List** in the navigation pane.
4. Click a bucket in the **OBS Bucket** column.
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/Cloud service
Example: **User Define/CloudTraces/Region/2016/5/19/system/ECS**
 - The trace file naming format is as follows:
Trace file prefix_CloudTrace_Region_Year-Month-DayTHour-Minute-SecondZ_Random characters.json.gz (Year-Month-DayTHour-Minute-Second indicates the time when the trace file was uploaded to OBS.)
Example:
FilePrefix_CloudTrace_region_2024-12-13T01-29-19Z_47b9d51830deff47.json.gz

NOTE

- The OBS bucket name and trace file prefix are set by you and other parameters are automatically generated.
- File download will incur request fees and traffic fees.
- If you disable **Sort by Cloud Service** when configuring a tracker to transfer traces to OBS, the cloud service will not be displayed in the transfer path. Example: **User Define/CloudTraces/Region/2016/5/19/system**

For details about key fields in a trace, see [Trace Structure](#) and [Example Traces](#).

6. Decompress the downloaded package to obtain a JSON file with the same name as the package, as shown in [Figure 2-1](#). Open the JSON file using a text file editor to view traces.

Figure 2-1 JSON file

```
{
  "code": 200,
  "event_type": "system",
  "project_id": "4008a952b3f44b5a919c9a48d90811f3",
  "record_time": 1723533697290,
  "resource_name": "-",
  "resource_type": "bucket",
  "service_type": "OBS",
  "source_ip": "172.30.33.69",
  "time": 1723533697290,
  "trace_id": "eb0472a4-5944-11ef-acee-294fee19871b",
  "trace_name": "listAllMyBucket",
  "trace_rating": "normal",
  "trace_type": "Others",
  "tracker_name": "system",
  "user": "{\"name\":\"\", \"id\":\"5f2cd06722f24250976264e6e7753a08\", \"domain\":\"\", \"name\":\"\", \"id\":\"25fe78d91e0448f6a37f35427c6a420b\"}"
}
```

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.

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 a trace, see [Trace Structure](#) and [Example Traces](#).

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

----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.

Constraints

- CTS records operations performed in the last seven days. To store traces for a longer period, configure a tracker to transfer them to OBS or LTS. The tracker will then continuously transfer traces to your specified OBS bucket or LTS log stream for storage.
- CTS 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

Scenarios

On the CTS console, you can add configurations such as OBS or LTS transfer for the created management tracker.

You can select whether to send recorded traces to an OBS bucket for long-term storage. You can also transfer management traces recorded by other accounts to a same OBS bucket for centralized management.

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

1. For global services, you must configure trackers on the CTS console in the central region (EU-Dublin). This configuration enables the function of transferring traces to OBS or LTS. This function will not take effect if you perform the configuration on the CTS console in any other regions.
For details about Huawei Cloud global services, see [Notes and Constraints](#).
2. There are three storage classes of OBS buckets: Standard, Infrequent Access, and Archive. CTS frequently accesses OBS buckets storing transferred traces. Therefore, when you create an OBS bucket on the CTS console, it defaults to a single-AZ private bucket with Standard storage. If you need other configurations, create the bucket on OBS Console in advance.
3. When configuring the transfer to OBS, you need to select an OBS bucket. If you delete the OBS bucket, CTS cannot transfer traces to OBS, and you cannot query traces of the last seven days.
4. After you configure the transfer in CTS, the retention period of the transferred trace is subject to the configuration on the OBS/LTS console.
 - First, create an OBS bucket and select a storage class on OBS Console. The storage period varies with the selected storage class. When configuring the tracker for transfer traces to OBS, select the created OBS bucket. By default, the retention period of transferred traces is the same as that configured on OBS.
 - The retention period of trace logs transferred to LTS is subject to the log retention period configured in LTS.

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.

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

Parameter	Description
Tracker Name	The default value is system and cannot be changed.
Enterprise Project	Select an enterprise project. NOTE Enterprise projects allow you to manage cloud resources and users by project. For details about how to enable the enterprise project function, see Creating an Enterprise Project .
Excluding DEW traces	Deselected by default. If this option is selected, the createDataKey and decryptDatakey operations on DEW will not be transferred to OBS/LTS. NOTE For details about DEW audit operations, see Operations supported by CTS .

Step 7 On the transfer configuration page, configure the transfer parameters of the tracker. You can only 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 select New to create one, and set File Prefix . When Transfer to OBS 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 Account	CTS allows you to transfer traces to OBS buckets of other users for unified management. • If you select Logged-in user, you do not need to grant the transfer permission. • If you select Other users, 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 Cross-Tenant Transfer Authorization.
OBS Bucket	New: An OBS bucket will be created automatically with the name you enter. NOTE The OBS bucket created on this page is a single-AZ private bucket with Standard storage. If you need other configurations, create the bucket on OBS Console in advance and choose Existing to select it. Existing: Select an existing OBS bucket in the current region.

Parameter	Description
Select Bucket	If you select New for OBS Bucket, enter a name for the new OBS bucket. The bucket name cannot be empty. Enter 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. If you select Existing for OBS Bucket, select an existing OBS bucket.
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	The usage of object storage space can be reduced. • Do not compress: Transfer files in the *.json format. • gzip: Transfer files in *.json.gz format.
Sort by Cloud Service	• 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: /CloutTrace/cn-north-7/2022/11/8/doctest/Cloud service/_XXX.json.gz • When this function is disabled, the cloud service name will not be added to the transfer file path. Example: /CloutTrace/cn-north-7/2022/11/8/doctest/_XXX.json.gz
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 Verifying Trace File Integrity .
Encrypt Trace File	When OBS Bucket Account is set to Logged-in user, you can configure an encryption key for the traces. When Encrypt Trace File is enabled, CTS obtains the key IDs of the current login user from DEW. You can select a key from the drop-down list. NOTE Use DEW keys to fully or partially encrypt objects in an OBS bucket. For details, see Encrypting Data in OBS.

Table 3-2 Parameters for configuring the transfer to LTS

Parameter	Description
Transfer to LTS	When Transfer to LTS is enabled, traces are transferred to the log stream.
Log Group	When Transfer to LTS is enabled, the default log group name CTS is set. When Transfer to LTS 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.

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	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). A tag key: • Can contain 1 to 128 characters. • Can contain letters, digits, spaces, and special characters <code>_.:=+@</code>, but cannot start or end with a space or start with <code>_sys_</code>.	Key_0001

Parameter	Description	Example
Tag value	A tag value can be repetitive or left blank. A tag value: • Can contain 0 to 255 characters. • Can contain letters, digits, spaces, and special characters _./=+-@	Value_0001

----End

3.3 Disabling or Enabling a Tracker

Scenarios

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.

Constraints

After a tracker is disabled, traces can still be reported to CTS. You can view traces of the last seven days in the trace list. However, new traces recorded after you disable the tracker cannot be viewed and transferred to OBS or LTS, and key event notifications will not be sent.

Prerequisites

You have enabled CTS.

Disabling or Enabling the 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 **Disable** in the **Operation** column in the row of the management tracker.

Step 6 Click **OK**. After the tracker is disabled, the **Disable** button changes to **Enable**.

Step 7 To enable the management tracker again, click **Enable** and then click **OK**. The tracker will start recording operations again.

----End

3.4 Deleting a Tracker

Scenarios

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.

Constraints

After a tracker is deleted, traces can still be reported to CTS. You can view traces of the last seven days in the trace list. However, new traces recorded after you disable the tracker cannot be viewed and transferred to OBS or LTS, and key event notifications will not be sent.

Enable CTS again to restore the management tracker.

Prerequisites

You have enabled CTS.

Deleting 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 **Delete** in the **Operation** column of the management tracker.

Step 6 Click **OK**.

----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, that is, logs of tenant operations (such as upload and download) on data in OBS buckets.

This section describes how to use a data tracker.

4.1 Creating a Tracker

Scenarios

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.

Constraints

- If you want to trace operations on OBS buckets, ensure that you create a data tracker in a project instead of a sub-project. Otherwise, tracing fails because there are no sub-projects in OBS.
- CTS records operations performed in the last seven days. To store traces for a longer time, configure your tracker. The tracker will continuously store traces to your specified LTS log stream or OBS bucket.

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 navigation pane. In the upper right corner of the displayed page, click **Create Tracker**.
4. Set basic information. Enter a tracker name and select an enterprise project. Click **Next**.

A data tracker name contains only letters, digits, hyphens (-), and underscores (_), and must start with a letter or digit. It cannot be empty and contains up to 32 characters. Do not use **system** or **system-trace** as a data tracker name.

5. On the **Select Trace** page, set the parameters and click **Next**.

Table 4-1 Parameters for selecting trace objects

Parameter	Description
Data Trace Source	Container for storing data traces. OBS is selected by default.
OBS Bucket	Select an OBS bucket from the drop-down list. After the tracker is created, the OBS bucket name cannot be changed.
Operation	Data operations are classified into read and write operations. Read operations refer to obtaining or downloading object data from OBS buckets. Write operations refer to uploading or writing object data to OBS buckets. • If you select Read, CTS will record only read operations. • If you select Write, CTS will record only write operations. For details about which OBS operations and read/write traces can be recorded by CTS, see "Table 2 OBS data operations logged by CTS" in Using CTS to Audit OBS .

6. On the transfer configuration page, set related parameters and click **Next**. You can only 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 Transfer to OBS is enabled, select an existing OBS bucket or select New to create one and set File Prefix . When Transfer to OBS 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	New: An OBS bucket will be created automatically with the name you enter. NOTE The OBS bucket created on this page is a single-AZ private bucket with Standard storage. If you need other configurations, create the bucket on OBS Console in advance and choose Existing to select it. Existing: Select an existing OBS bucket in the current region.
Select Bucket	When you select New, 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. If you select Existing for OBS Bucket, 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. 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.
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 usage of object storage space can be reduced. Do not compress: Transfer files in the *.json format. gzip: Transfer files in *.json.gz format.
Sort by Cloud Service	- 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: /CloutTrace/cn-north-7/2022/11/8/doctest/Cloud service/_XXX.json.gz - When this function is disabled, the cloud service name will not be added to the transfer file path. Example: /CloutTrace/cn-north-7/2022/11/8/doctest/_XXX.json.gz
Transfer Path	Log transfer path is automatically set by the system.

Parameter	Description
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 Verifying Trace File Integrity .

Table 4-3 Parameters for configuring the transfer to LTS

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

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

4.2 Configuring a Tracker

Scenarios

On the CTS console, you can add configurations such as OBS or LTS transfer for the created data trackers.

You can select whether to send recorded traces to an OBS bucket for long-term storage. You can also transfer management traces recorded by other accounts to a same OBS bucket for centralized management.

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

This section describes how to configure a data tracker.

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.

Step 6 On the **Select Trace** page, set the parameters and click **Next**.

Table 4-4 Parameters for selecting traces

Parameter	Description
Data Trace Source	Container for storing data traces. OBS is selected by default.
OBS Bucket	The OBS bucket you set when creating the data tracker is select by default. This option cannot be changed.
Operation	Data operations are classified into read and write operations. Read operations refer to obtaining or downloading object data from OBS buckets. Write operations refer to uploading or writing object data to OBS buckets. • If you select Read, CTS will record only read operations. • If you select Write, CTS will record only write operations. For details about which OBS operations and read/write traces can be recorded by CTS, see "Table 2 OBS data operations logged by CTS" in Using CTS to Audit OBS.

Step 7 On the transfer configuration page, modify the transfer parameters of the tracker. You can only 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 4-5](#) and [Table 4-6](#).

Table 4-5 Parameters for configuring the transfer to OBS

Parameter	Description
Transfer to OBS	If Transfer to OBS is enabled, select an existing OBS bucket or select New to create one and set File Prefix. When Transfer to OBS is disabled, no operation is required.
OBS Bucket	New: An OBS bucket will be created automatically with the name you enter. NOTE The OBS bucket created on this page is a single-AZ private bucket with Standard storage. If you need other configurations, create the bucket on OBS Console in advance and choose Existing to select it. Existing: Select an existing OBS bucket in the current region.

Parameter	Description
Select Bucket	When you select New, 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. If you select Existing for OBS Bucket, 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. 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.
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.
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 Verifying Trace File Integrity.

Table 4-6 Parameters for configuring the transfer to LTS

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

Step 8 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 9 (Optional) On the **Tracker List** page, click  in the **Tag** column to add tags to the tracker.

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 4-7 Tag parameters

Parameter	Description	Example
Tag key	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). A tag key: • Can contain 1 to 128 characters. • Can contain letters, digits, spaces, and special characters <code>_:/=+-@</code>, but cannot start or end with a space or start with <code>_sys_</code>.	Key_0001
Tag value	A tag value can be repetitive or left blank. A tag value: • Can contain 0 to 255 characters. • Can contain letters, digits, spaces, and special characters <code>_:/=+-@</code>	Value_0001

----End

4.3 Disabling or Enabling a Tracker

Scenarios

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.

Constraints

After a tracker is disabled, traces can still be reported to CTS. You can view traces of the last seven days in the trace list. However, new traces recorded after you disable the tracker cannot be viewed and transferred to OBS or LTS, and key event notifications will not be sent.

Prerequisites

You have created a data tracker on the CTS console.

Disabling or Enabling 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 **Disable** in the **Operation** column in the row of the target data tracker.
6. Click **OK**. After the tracker is disabled, the **Disable** button changes to **Enable**.
7. To enable the tracker, click **Enable** and then click **OK**. The tracker will start recording operations again.

4.4 Deleting a Tracker

Scenarios

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 console.

Constraints

After a tracker is deleted, traces can still be reported to CTS. You can view traces of the last seven days in the trace list. However, new traces recorded after you disable the tracker cannot be viewed and transferred to OBS or LTS, and key event notifications will not be sent.

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.
6. Click **OK**.

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.

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.

Prerequisites

1. You are using an organization administrator account.
2. You have created an account for which the delegated administrator permissions need to be set.

Setting CTS as a Trusted Service

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.

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

----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.

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

Step 6 On the transfer configuration 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 select New to create one, and set File Prefix . When Transfer to OBS is disabled, no operation is required.
OBS Bucket	Existing: Select an existing OBS bucket in the current region.
Select Bucket	If you select New for OBS Bucket , enter a name for the new OBS bucket. The bucket name cannot be empty. Enter 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. If you select Existing for OBS Bucket , select an existing OBS bucket.
Retention Period	For the management tracker, the retention period configured on the OBS console is used by default and cannot be changed.

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 usage of object storage space can be reduced. • Do not compress: Transfer files in the *.json format. • gzip: Transfer files in *.json.gz format.
Sort by Cloud Service	• When this function is enabled, the cloud service name is added to the transfer file path, and multiple small files are generated in OBS. • When this function is disabled, the cloud service name will not be added to the transfer file path.
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 Verifying Trace File Integrity .
Encrypt Trace File	When OBS Bucket Account is set to Logged-in user , you can configure an encryption key for the traces. When Encrypt Trace File is enabled, CTS obtains the key IDs of the current login user from DEW. You can select a key from the drop-down list.

Table 5-2 Parameters for configuring the transfer to LTS

Parameter	Description
Transfer to LTS	When Transfer to LTS is enabled, traces are transferred to the log stream.
Log Group	When Transfer to LTS is enabled, the default log group name CTS is set. When Transfer to LTS 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.

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.

----End

6 Using Advanced Query

6.1 Enabling Advanced Query and Configuring Field Indexing

Scenarios

CTS records details of user operations, such as creating, modifying, and deleting cloud service resources, and stores these records as traces in the CTS trace list for seven days. To store traces for more than seven days, you can enable advanced query. This function allows CTS to periodically transfer traces to LTS log streams for long-term audit log storage.

In addition, advanced query offers enhanced trace search capabilities. It supports additional search criteria, LTS query syntax, and professional log interpretation, helping you easily locate and analyze system issues.

Constraints

- Enabling advanced query will transfer audit logs to LTS, which will incur fees. Ensure that your account balance is sufficient. For details about LTS pricing, see [Log Tank Service Pricing Details](#).
- After advanced query is enabled, the system automatically creates a log group and a log stream in LTS. The log group name defaults to **CTS** and cannot be changed. The log stream name defaults to **system-trace**. By default, logs in this log stream are retained for seven days. You can change the log retention period on the LTS console. For details, see [Managing Log Streams](#).
- After the index settings of this log stream are modified in LTS, the modification takes effect only for newly written log data, not for historical log data.

Prerequisites

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

Enabling Advanced Query for Traces

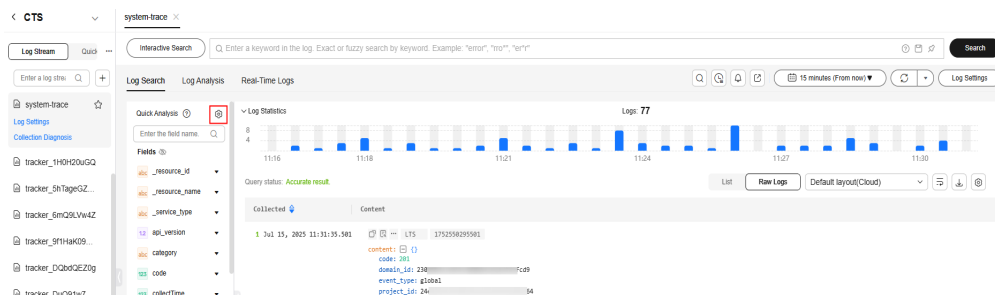
- Step 1** Log in to the [CTS console](#).
- Step 2** In the navigation pane, choose **Advanced Query**.
- Step 3** If you have configured **Transfer to LTS** for the management tracker, skip this step.
Click **Enable** and then **OK**. LTS automatically creates a log group and a log stream. You can view and search the audit logs transferred to LTS on the **Advanced Query** page of the CTS console.
- Step 4** (Optional) To perform more operations on logs, such as creating alarm rule notifications, click **Log Tank Service** in the upper part of the page to go to the LTS console.
- End

Configuring Cloud Structuring Parsing and Field Indexing

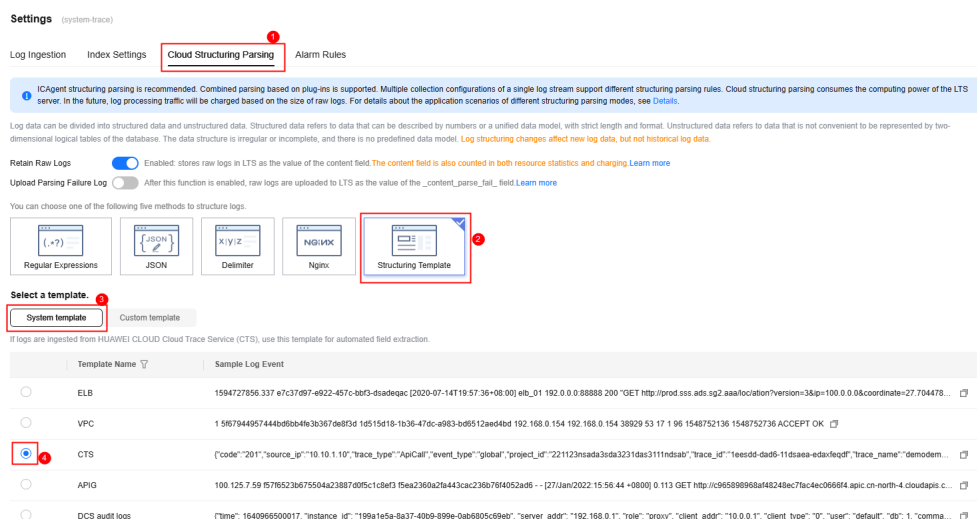
You need to configure structuring parsing before configuring field indexing.

Configuring cloud structuring parsing

- Step 1** On the **Advanced Query** page, click **Log Tank Service** in the upper part of the page to go to the LTS console.
- Step 2** On the **system-trace** log stream page, click  to access the log stream setting page.



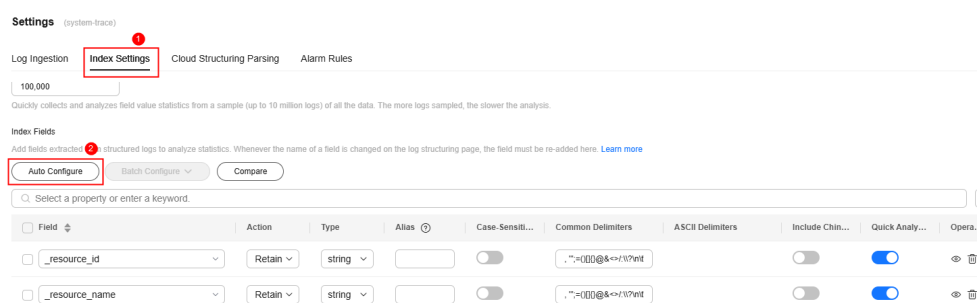
- Step 3** Click the **Cloud Structuring Parsing** tab.
- Step 4** Select **Structuring Template > System Template > CTS**, and click **Save**.



----End

Configuring field indexing

- Step 1** On the displayed log stream setting page, click the **Index Settings** tab.
- Step 2** Click **Auto Configure** under **Index Fields**. The system will automatically extract fields from log structuring and adds them for log data statistics and analysis. To manually add a field index, click **Add Field**. For details, see [Configuring Log Indexing](#).



- Step 3** Click **OK**. After the index settings are modified, the modification takes effect only for newly written log data, not for historical log data.

You can quickly query traces based on specific fields on the **Advanced Query** page of the CTS console.

----End

Helpful Links

- You can use the advanced query function to quickly query traces related to your access key and Huawei Cloud account. For details, see [Querying Access Key Traces](#) and [Querying Huawei Cloud Account Traces](#).
- For details about LTS's log search and analysis functions, see [Log Search and Analysis Overview](#).
- You can use SQL syntax on the **Advanced Query** page to query or analyze audit logs transferred to LTS. For details about the SQL syntax, see [Using SQL Analysis Syntax](#).

6.2 Querying Access Key Traces

An access key consists of an Access Key ID (AK) and a Secret Access Key (SK). It is used to identify and verify a user. Leaking your access key could put your resources at risk. CTS helps you monitor access key traces and respond promptly to access key usage exceptions.

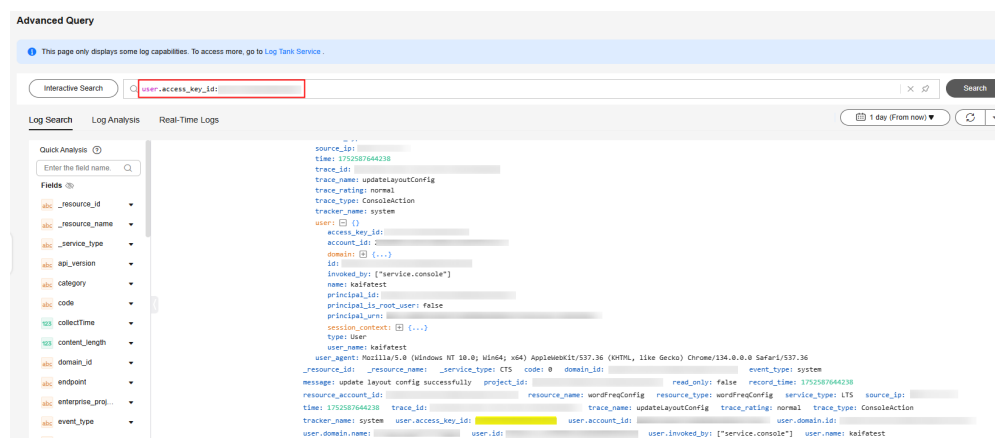
This section guides you through using the advanced query function to efficiently query traces related to your access key.

Prerequisites

You have performed the operations in [Enabling Advanced Query and Configuring Field Indexing](#).

Querying Access Key Traces

- Step 1** Log in to the [CTS console](#).
- Step 2** In the navigation pane, choose **Advanced Query**.
- Step 3** On the **Advanced Query** page, click **15 minutes (From now)** in the upper right corner to set a query time range.
- Step 4** Enter `user.access_key_id:{access_key_id}` in the search box and click **Search** to query traces related to your access key. Replace `{access_key_id}` with your access key ID.



----End

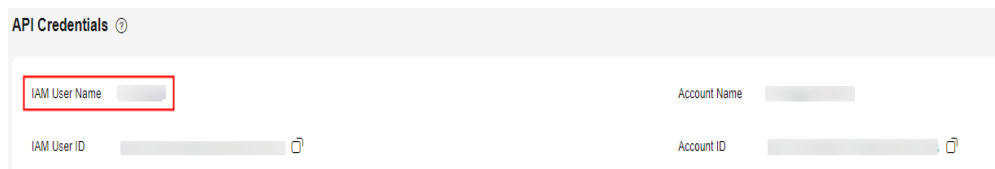
6.3 Querying Huawei Cloud Account Traces

A Huawei Cloud account owns your Huawei Cloud resources and makes payments for the use of these resources. Leaking your Huawei Cloud account could put your resources at risk. You can use CTS to monitor your Huawei Cloud account and set alarms to keep your Huawei Cloud account resources secure.

This section guides you through using the advanced query function to efficiently query traces related to your Huawei Cloud account.

Prerequisites

- You have performed the operations in [Enabling Advanced Query and Configuring Field Indexing](#).
- You have obtained your username. To obtain your username, hover over the username in the upper right corner of the console, select **My Credentials** from the drop-down menu, and locate the name on the right of **IAM Username**.



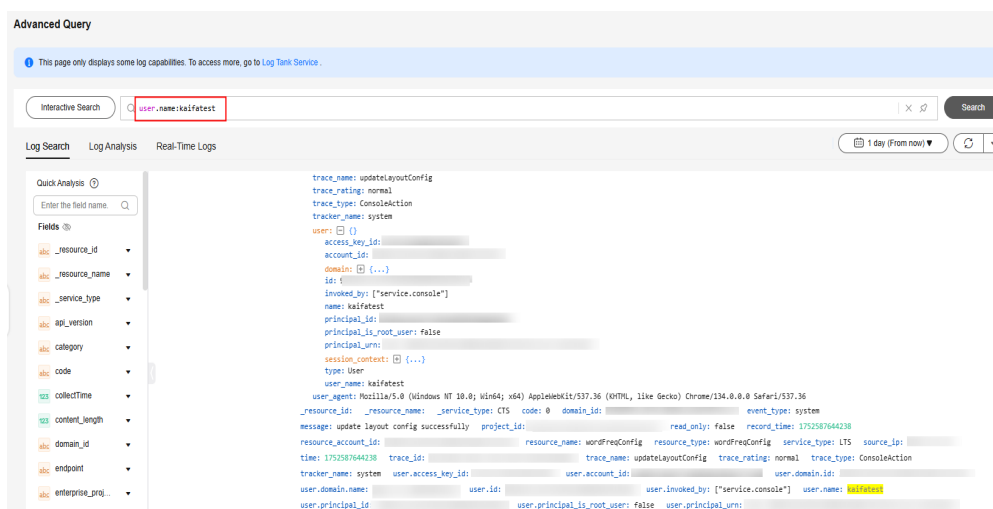
Querying Huawei Cloud Account Traces

Step 1 Log in to the [CTS console](#).

Step 2 In the navigation pane, choose **Advanced Query**.

Step 3 On the **Advanced Query** page, click **15 minutes (From now)** in the upper right corner to set a query time range.

Step 4 Enter **user.name:{username}** in the search box and click **Search** to query traces related to your Huawei Cloud account. Replace **{username}** with your username.



----End

7

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.

Constraints

- For global services, you must configure key event notifications on the CTS console in the central region (EU-Dublin). This configuration enables the function of sending key event notifications. This function will not take effect if you perform the configuration on the CTS console in any other regions. For details about Huawei Cloud global services, see [Notes and 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.
 - You can specify notification topics for complete key event notifications.
- If CTS and Cloud Eye share a message topic, the subscribers receive notifications from both services, with varying 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.
- After you disable or delete a key event notification, CTS will not send related notifications to subscribers.

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.
Select 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 7-1 Advanced filtering parameters

Parameter	Description
api_version	Version of the API called in a trace. Enumerated values: • v1 • v3
code	HTTP status code returned by an API.
trace_rating	Trace status. Enumerated values: • normal • warning • incident
trace_type	Trace type, including API calls, actions taken on the console, and system-triggered actions. Enumerated values: • ApiCall • ConsoleAction • SystemAction
resource_id	ID of a cloud service resource on which operations are performed. Example: 5a0215bed7a14de38193a*****facef
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 creating 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 7-2](#).

Table 7-2 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 Enable or Disable in the Operation column. CTS can trigger key event notifications only after SMN is configured.
Modifying a key event notification	Click Modify in the Operation column.
Deleting a key event notification	Click Delete in the Operation 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.

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

----End

8

Configuring Query Trace Reporting for Cloud Services

Scenarios

After you enable CTS, you can check traces reported by cloud services on the CTS console. A trace is an operation log for a cloud service resource, tracked and stored by CTS. Traces record operations such as adding, modifying, deleting, or querying cloud service resources.

By default, CTS does not record query operations because these are very frequent (such as querying a list of ECSs, metrics, or logs multiple times a day) and can generate a large volume of audit logs, making it difficult to find relevant information.

If you want to check these query operations of specific cloud services, you can configure corresponding reporting rules in CTS's **Configuration Center**.

What Are Query Traces?

A query trace is a log of a query operation on a cloud service resource. On the CTS console, you can determine if a trace is a query trace by checking the **read_only** parameter in its details:

- If the value of **read_only** is **true**, the trace is a query trace.
- If the value of **read_only** is **false**, the trace is not a query trace.

Trace List ⓘ

Export ▾

Last 1 hour ▾

🔍 Select a property or enter a keyword.

Trace Name	Trace Source	Resource Type	Resource Name	Resource ID
createDataKey	KMS	cmk	cms/default	47e6d12f-ce80-4a4...
createDataKey	KMS	cmk	cms/default	47e6d12f-ce80-4a4...
createTokenByAssume...	IAM	token	--	--
createTokenByAssume...	IAM	token	--	--
listEnterpriseProject	EPS	enterpriseList	--	--
createTokenByAssume...	IAM	token	--	--
createTokenByAssume...	IAM	token	--	--

Trace Overview

Basic Information

Trace ID

7e13d3f4-6089-11b0-a568-c53d9cd22e7b

Trace Source

EPS

Trace Time

Jul 14, 2025 16:06:49 GMT+08:00

Resource Type

enterpriseList

Operator

Resource Name

--

Return Code

200

Source IP Address

10.63.237.105

Learn about trace structure

```
1 {
2   "code": "200",
3   "domain_id": "238fcd9",
4   "event_type": "global",
5   "operation_id": "listEnterpriseProject",
6   "project_id": "24edf764",
7   "read_only": true,
8   "resource_account_id": "238fcd9",
9   "resource_type": "enterpriseList",
```

What Do Cloud Services in the Configuration Center Mean?

On the **Configuration Center** page, cloud services refer to the specific services interconnected with CTS, as identified by their **service_type** values.

Trace List

Export

Last 1 hour

Select a property or enter a keyword.

Trace Name	Trace Source	Resource Type	Resource Name	Resource ID
createDatakey	KMS	cmk	cms/default	47e6d12f-ce80-4a4...
listUsers	IAM	users	--	--
createDatakey	KMS	cmk	cms/default	47e6d12f-ce80-4a4...
createDatakey	KMS	cmk	cms/default	47e6d12f-ce80-4a4...
listUsers	IAM	users	--	--
createDatakey	KMS	cmk	cms/default	47e6d12f-ce80-4a4...
createDatakey	KMS	cmk	cms/default	47e6d12f-ce80-4a4...

Trace Overview

Basic Information

Trace ID

d9d30aa5-608d-11b0-a0be-af4ec5d5eb60

Trace Source

KMS

Trace Time

Jul 14, 2025 16:37:59 GMT+08:00

Resource Type

cmk

Operator

Resource Name

cms/default

Return Code

200

Source IP Address

10.172.136.242

1

2

3

4

5

6

7

8

9

10

11

12

{

"code": "200",

"domain_id": "2380",

"event_type": "system",

"operation_id": "createDatakey",

"project_id": "24ed",

"read_only": false,

"resource_account_id": "23e",

"resource_type": "cmk",

"service_type": "KMS",

"source_ip": "",

"trace_id": "d9d30aa5-608d-11b0-a0be-af4ec5d5eb60",

}

Constraints

For global services, you must configure query trace reporting rules on the CTS console in the central region (EU-Dublin). This function will not take effect if you configure the rules on the CTS console in any other regions. For all global services of Huawei Cloud, see [Notes and Constraints](#).

Prerequisites

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

Enabling Query Trace Reporting for Certain Cloud Services

- Step 1 [Log in to the CTS console](#).
- Step 2 In the navigation pane, choose **Configuration Center**.
- Step 3 Select **For certain cloud services** for **Read-Only Trace Reporting**.
- Step 4 Toggle on  on the right of a specific cloud service. Query traces of that service will be reported to CTS.
- Step 5 (Optional) To enable query trace reporting for multiple cloud services, select multiple cloud services in the list and click **Enable**.

Figure 8-1 Enabling reporting for multiple cloud services

Configuration Center

Read-Only Trace Reporting

For certain cloud services

For all cloud services

Enable

Disable

Select a property or enter a keyword.

Cloud Service

Read-Only Trace Reporting

☒ NAT	☐
☒ TerraformExplorer	☐
☒ VPC	☐
☐ CodeArtsTestPlan	☐

----End

Enabling Query Trace Reporting for All Cloud Services

Step 1 [Log in to the CTS console.](#)

Step 2 In the navigation pane, choose **Configuration Center**.

Step 3 Select **For all cloud services** for **Read-Only Trace Reporting**.

Step 4 Click **OK**. Query traces of all cloud services will be reported to CTS.

----End

9 Application Examples

9.1 Security Auditing

Scenarios

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

This section describes how to use CTS to audit EVS creation and deletion operations performed in the last two weeks.

Constraints

To store operation records for longer than seven days, you must configure transfer to OBS or LTS for trackers so that you can view them in OBS buckets or LTS log groups.

Prerequisites

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

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

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.

Last 1 week								
Trace Source: EVS × Resource Type: evs × Trace Name: createVolume × Add filter								
Trace Name	Trace Source	Resource Type	Resource Name	Resource ID	Operator	Trace Status	Operation Time	
createVolume	EVS	evs	Its-...	682e8bf-278c-4a29-9cb2-9...	hwstaff_...	normal	Dec 18, 2024 11:05:01 GM...	
createVolume	EVS	evs	Its-...	5594d9d2-7493-41ce-abee-...	hwstaff_...	normal	Dec 18, 2024 11:05:01 GM...	
createVolume	EVS	evs	Its-...	eb04f4d9-9524-4bac-813f-55...	hwstaff_...	normal	Dec 18, 2024 11:04:59 GM...	
createVolume	EVS	evs	Its-...	97544dc0-c320-45a7-818b-...	hwstaff_...	normal	Dec 18, 2024 11:04:55 GM...	
createVolume	EVS	evs	ecs-...	ff40929-25a5-4a2c-81db-2c...	hwstaff_...	normal	Dec 13, 2024 16:35:46 GM...	

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

Last 1 week								
Trace Source: EVS × Resource Type: evs × Trace Name: deleteVolume × Add filter								
Trace Name	Trace Source	Resource Type	Resource Name	Resource ID	Operator	Trace Status	Operation Time	
deleteVolume	EVS	evs	Its-...	682e8bf-278c-4a29-9cb2-9...	hwstaff_...	normal	Dec 18, 2024 14:26:34 GM...	
deleteVolume	EVS	evs	Its-...	97544dc0-c320-45a7-818b-...	hwstaff_...	normal	Dec 18, 2024 14:26:34 GM...	
deleteVolume	EVS	evs	Its-...	eb04f4d9-9524-4bac-813f-55...	hwstaff_...	normal	Dec 18, 2024 14:26:33 GM...	
deleteVolume	EVS	evs	Its-...	5594d9d2-7493-41ce-abee-...	hwstaff_...	normal	Dec 18, 2024 14:26:33 GM...	

 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](#).

- Step 6 To query operation records of the last seven days, go to the OBS bucket or LTS log group. For details, see [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

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

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

- Log in to the management console as a CTS administrator.
- Click  in the upper left corner to select the desired region and project.
- Click  in the upper left corner and choose **Management & Governance > Cloud Trace Service**. The CTS console is displayed.
- Choose **Trace List** in the left navigation pane.
- 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.

- To query operation records of the last seven days, go to the OBS bucket or LTS log group. For details, see [Querying Transferred Traces](#).

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

9.2 Fault Locating

Scenarios

If a resource or action encounters a fault, you can quickly locate and analyze it. Just query the traces for that resource at the time of the fault and check the related actions and responses.

This section provides examples demonstrating how to use CTS to locate an ECS fault or an ECS creation failure.

Prerequisites

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

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

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 navigation pane.

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

Select **Trace Source: ECS** and **Resource Type: ecs**, then select **Resource ID** and enter *{ID of the faulty VM}*. You can also directly enter *{ID of the faulty VM}*.

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**. The CTS console is displayed.
- Step 4** Choose **Trace List** in the navigation pane.
- Step 5** Set filters as follows:
Select **Trace Source: ECS**, **Resource Type: ecs**, and **Trace Status: warning**.
- Step 6** In the filtering result, locate the trace named **createServer**. Based on its error code or message, identify and analyze the fault.
- End

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

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 navigation pane.
- Step 5** In the time range setting area in the upper right corner, set the time to 06:00 to 12:00 on the certain day.
- Step 6** Set filters above the trace list. Set **Trace Type** to **Management**, **Trace Source** to **ECS**, **Resource Type** to **ecs**, and **Filter By** to **Resource ID**. Enter *{ID of the faulty VM}* in the **Resource ID** text box.
- Step 7** Click **Query**.
- Step 8** 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**. The CTS console is displayed.

- Step 4 Choose **Trace List** in the navigation pane.
- Step 5 Set filters as follows: Set **Management** for **Trace Type**, **ECS** for **Trace Source**, **ecs** for **Resource Type**, and **Warning** for **Trace Status**.
- Step 6 Click **Query**.
- Step 7 In the filtering result, locate the trace named **createServer**. Based on its error code or message, identify and analyze the fault.
- End

9.3 Resource Tracking

Scenarios

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

This section describes how to use CTS to view all operation records of an ECS.

Constraints

To store operation records for longer than seven days, you must configure transfer to OBS or LTS for trackers so that you can view them in OBS buckets or LTS log groups.

Prerequisites

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

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

- 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 *{VM ID}* for **Resource ID**. You can also directly enter *{VM ID}* to view the filtering result.

Last 1 hour	Trace Source: ECS	Resource Type: ecs	Resource ID: 1001ecb0-9b08-4035-bac4-90a4	Add filter				
Trace Name	Trace Source	Resource Type	Resource Name	Resource ID	Operator	Tampered or not	Trace Status	Operation Time
startServer	ECS	ecs	ecs	1001ecb0-9b08-4035-bac4-90a4		No	normal	Dec 19, 2024 15:42:3...
stopServer	ECS	ecs	ecs	1001ecb0-9b08-4035-bac4-90a4		No	normal	Dec 19, 2024 15:42:0...
createServer	ECS	ecs	ecs	1001ecb0-9b08-4035-bac4-90a4		No	normal	Dec 19, 2024 15:40:5...

 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.

Step 6 To query operation records of the last seven days, go to the OBS bucket or LTS log group. For details, see [Querying Transferred Traces](#).

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

----End

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

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 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 displayed page, obtain the OBS bucket or LTS log group information.
7. Query 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](#).

10 Trace References

10.1 Trace Structure

A trace consists of multiple key fields shown in [Table 10-1](#).

 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 10-1 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, 1660927593570 . 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	UserInfo object	Information of the user who performed the operation that triggered the trace.
request	No	String	Request of an operation on resources.
response	No	String	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.
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. - When trace_type is set to system, the default value system is used. - When trace_type is set to data, the value is the name of the corresponding data tracker.
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 normal , warning , or incident . • normal: The operation succeeded. • warning: The operation failed. • incident: The operation caused a serious consequence, for example, a node failure or service interruption.
trace_type	Yes	String	Trace source. For management traces, the value can be ApiCall , ConsoleAction , or SystemAction . For data traces, the value can be ObsSDK or ObsAPI .
api_version	No	String	Version of the API called in a trace.
message	No	String	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 10-2 UserInfo

Field	Mandatory	Type	Description
type	No	String	Identity type of the operator.
principal_id	No	String	Identity ID of the operator. - For an IAM user, the format is <i><user-id></i>. - For an IAM assumed-agency session identity, the format is <i><agency-id>.<agency-session-name></i>. - For an IAM federated identity, the format is <i><idp_id>.<user-session-name></i>.
principal_urn	No	String	URN of the operator. - For an IAM user, the format is <i>iam::<account-id>:user:<user-name></i>. - For an IAM agency session identity, the format is <i>sts::<account-id>:assumed-agency:<agency-name>/<agency-session-name></i>. - For an IAM federated identity, the format is <i>sts::<account-id>:external-user:<idp_id>/<user-session-name></i>.

Field	Mandatory	Type	Description
account_id	No	String	Account ID. To obtain it, hover over the username in the upper right corner of the console, select My Credentials from the drop-down menu, and locate the ID on the right of Account ID .
access_key_id	No	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 My Credentials from the drop-down menu, and locate the ID on the right of IAM User ID .
name	Yes	String	Username. To obtain it, hover over the username in the upper right corner of the console, select My Credentials from the drop-down menu, and locate the name on the right of IAM Username .
domain	Yes	BaseUser object	Domain information of the user who performed the operation generating the trace.
user_name	No	String	Username. The meaning of user_name is the same as that of name .
principal_is_root_user	No	String	Whether the operator is user root . - If the value is true, the operator is user root. - If the value is false, the operator is an IAM user of an assumed-agency session identity, a federated identity, or a non-root user.
invoked_by	No	Array of strings	Name of the service that sends the request. The value is ["service.console"] for console operations.
session_context	No	SessionContext object	Temporary security credential attribute.
OriginUser	No	String	Information about the original user who initiates the assumed session.

Table 10-3 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 My Credentials from the drop-down menu, and locate the ID on the right of Account ID .
name	Yes	String	Account name. To obtain it, hover over the username in the upper right corner of the console, select My Credentials from the drop-down menu, and locate the name on the right of Account Name .

Table 10-4 SessionContext

Field	Mandatory	Type	Description
attributes	No	Attributes object	Temporary security credential attribute.

Table 10-5 Attributes

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

10.2 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                              \"ipproductid\": \"\",\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          }\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    \"resource_id\": \"7285ea5d-f15c-4d9c-9e4e-37d37023f2f4\",\n    \"request_id\": \"null\"\n  }\n}"
```

Note 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\""}
}
```

Note 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](#).

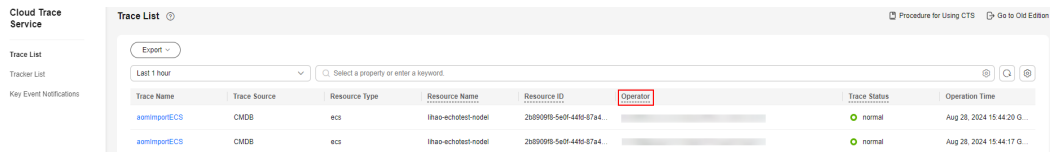
10.3 Relationship Between IAM Identities and Operators

Huawei Cloud IAM provides the following types of identities: IAM users, IAM agencies, cloud service agencies, IAM Identity Center users, and federated users.

The operator information reported to CTS audit logs varies depending on the operators identity. The following describes the format specifications of the username (**user.name** field) and identity ID (**principal_id** field) of different operators:

Operat or Identit y	Identity Type (type)	Operator Name Format (user.name)	Identity ID Format (principal_id)
IAM user	User	<user-name>	<user-id>
IAM agency	AssumedAg ency	<domain-name>/ <agency-name>	<agency-id>:<agency-session- name>
Cloud service agency	AssumedAg ency	<domain-name>/ <agency-name>	<agency-id>:<agency-session- name>
IAM Identity Center	AssumedAg ency	<domain-name>/ <agency-name>	<agency-id>:<agency-session- name>
Federat ed user	ExternalUse r	<idp_id>/<user- session-name>	<idp_id>:<user-session-name>

The **Operator** column of the trace list displays usernames of operators.



This section provides examples of operator information in the trace list when different user identities are used to perform operations on resources.

IAM User

If the operator is an IAM user, the **user** field in the audit log is as follows:

```
{
  "access_key_id": "HSTAZ***YE2GA",
  "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"
}
```

The **user** field records the information about the operator, which is **IAMUserA** (value of the **name** field) in this example. Note the following fields.

Field	Description
user_name	Username of the operator. To obtain it, hover over the username in the upper right corner of the console, select My Credentials from the drop-down menu, and locate the name on the right of IAM Username . In this example, it is IAMUserA .
name	
id	User ID of the operator. To obtain it, hover over the username in the upper right corner of the console, select My Credentials from the drop-down menu, and locate the name on the right of IAM User ID . In this example, it is f36972ced***d619f1214 .
principal_id	Identity ID of the operator. The format is <i>user-id</i> . In this example, the value is f36972ced***d619f1214 .
principal_urn	URN of the operator. The format is <i>iam::<account-id>:user:<user-name></i> . In this example, the value is iam::7e0d78c85***d0b9b7cba:user:IAMUserA .
domain.name	Account name of the operator. To obtain it, hover over the username in the upper right corner of the console, select My Credentials from the drop-down menu, and locate the name on the right of Account Name . In this example, it is IAMUserB .
domain.id	Account ID of the operator. To obtain it, hover over the username in the upper right corner of the console, select My Credentials from the drop-down menu, and locate the name on the right of Account ID . In this example, it is 7e0d78c85***d0b9b7cba .
account_id	

IAM Agency

If the operator is an IAM agency, the **user** field in the audit log is as follows:

```
{
  "access_key_id": "HSTAB***6DEEB",
  "invoked_by": [
    "service.console"
  ],
  "account_id": "302893da***5a7453e5733",
  "domain": {
    "name": "hc_beta_***",
    "id": "302893da***5a7453e5733"
  },
}
```

```
{
  "name": "hc_beta_***/agencyname",
  "session_context": {
    "attributes": {
      "created_at": "1724744585642",
      "mfa_authenticated": "false"
    },
    "assumed_by": {
      "principal_id": "3cd5b27548***a58b5801d9d"
    }
  },
  "principal_urn": "sts::302893da***5a7453e5733:assumed-agency:agencyname/null",
  "type": "AssumedAgency",
  "principal_id": "40c79f4571***8bc54784b61:null"
}
```

The **user** field records the information about the operator, which is **hc_beta_***/agencyname** (value of the **name** field) in this example. Note the following fields.

Field	Description
name	Username of the operator. The format is <i><domain-name>/<agency-name></i> .
principal_id	Identity ID of the operator. The format is <i><agency-id>.<agency-session-name></i> . In this example, the value is 40c79f4571***8bc54784b61:null .
principal_urn	URN of the operator. For an IAM agency, the format is <i>sts::<account-id>:assumed-agency:<agency-name>/<agency-session-name></i> . In this example, the value is sts::302893da***5a7453e5733:assumed-agency:agencyname/null .
session_context.assumed_by.principal_id	ID of the delegated account in IAM. For details, see Switching Roles (by a Delegated Party) .

Cloud Service Agency

If the operator is a cloud service agency, the **user** field in the audit log is as follows:

```
{
  "access_key_id": "HSTAR***LG6FC",
  "account_id": "302893da***53e5733",
  "domain": {
    "name": "hc_beta_***",
    "id": ""302893da***53e5733""
  },
  "name": "hc_beta_***/ServiceLinkedAgencyForCloudTraceService",
  "session_context": {
    "attributes": {
      "created_at": "1724744380046",
      "mfa_authenticated": "false"
    },
    "assumed_by": {
      "service_principal": "service.CTS"
    }
  }
}
```

```
{
  "principal_urn": "sts::302893da***53e5733:assumed-agency:ServiceLinkedAgencyForCloudTraceService/302893da***53e5733",
  "type": "AssumedAgency",
  "principal_id": "4bc820d3***b786c83:302893da***53e5733"
}
```

The **user** field records the information about the operator, which is **hc_beta_***/ServiceLinkedAgencyForCloudTraceService** (value of the **name** field) in this example. Note the following fields.

Field	Description
name	Username of the operator. The format is <i><domain-name>/<agency-name></i> . In this example, it is hc_beta_***/ServiceLinkedAgencyForCloudTraceService .
principal_id	Identity ID of the operator. The format is <i><agency-id>:<agency-session-name></i> . In this example, the value is 4bc820d3***b786c83:302893da***53e5733 .
principal_urn	URN of the operator. The format is <i>sts::<account-id>:assumed-agency:<agency-name>/<agency-session-name></i> . In this example, the value is sts::302893da***53e5733:assumed-agency:ServiceLinkedAgencyForCloudTraceService/302893da***53e5733 .
session_context.assumed_by.service_principal	Name of the delegated cloud service. The format is <i>service.<service-name></i> .

IAM Identity Center User

If the operator is a user created in IAM Identity Center, the **user** field in the audit log is as follows:

```
{
  "access_key_id": "HSTA9***CKG7E",
  "invoked_by": [
    "service.console"
  ],
  "account_id": "302893da***53e5733",
  "domain": {
    "name": "hc_beta_***",
    "id": "302893da***53e5733"
  },
  "name": "hc_beta_***/SysReservedV3_evs-FullAccess-***",
  "session_context": {
    "attributes": {
      "created_at": "1724744395079",
      "mfa_authenticated": "false"
    },
    "assumed_by": {
      "service_principal": "service.IdentityCenter"
    }
  }
}
```

```
    },
    "principal_urn": "sts::302893da***53e5733:assumed-agency:SysReservedV3_evs-FullAccess-***/
IdentityCenterUsername",
    "type": "AssumedAgency",
    "principal_id": "dbc60d8***ef5fd807:***"
  }
}
```

The **user** field records the information about the operator, which is **hc_beta_***/SysReservedV3_evs-FullAccess-***** (value of the **name** field) in this example. Note the following fields.

Field	Description
name	Username of the operator. For a service-linked agency, the format is <i><domain-name>/<agency-name></i> . In this example, the value is hc_beta_***/SysReservedV3_evs-FullAccess-*** .
principal_id	Identity ID of the operator. The format is <i><agency-id>:<agency-session-name></i> . In this example, the value is dbc60d8***ef5fd807:*** .
principal_urn	URN of the operator. The format is <i>sts::<account-id>:assumed-agency:<agency-name>/<agency-session-name></i> . In this example, the value is sts::302893da***53e5733:assumed-agency:SysReservedV3_evs-FullAccess-***/IdentityCenterUsername .
session_context.assumed_by.service_principal	Name of the entrusted cloud service. The value is fixed at service.IdentityCenter .

Federated User

If the operator is a federated user, the **user** field in the audit log is as follows:

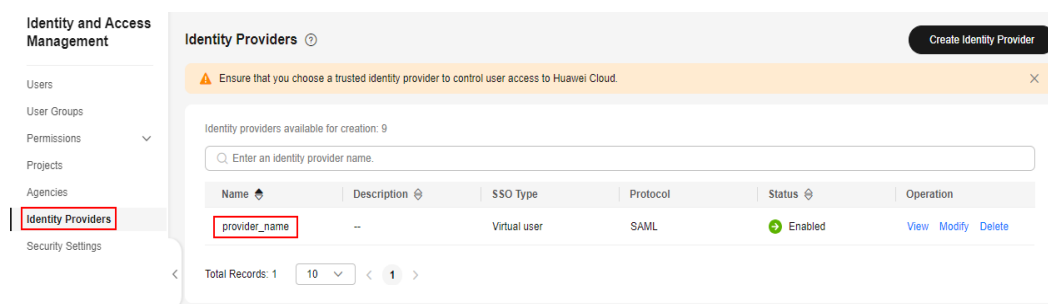
```
{
  "access_key_id": "HSTAX***3IBZB",
  "account_id": "797c8fc3c***2dc6bf70bd",
  "domain": {
    "name": "****",
    "id": "797c8fc3c***2dc6bf70bd"
  },
  "name": "provider_name/UserA",
  "session_context": {
    "federation_data": {
      "identity_provider": "provider_name",
      "protocol": "SAML",
      "group_ids": [
        "fedf7a460***46451be85"
      ]
    }
  },
  "principal_urn": "sts::797c8fc3c***2dc6bf70bd:external-user:provider_name/UserA",
  "type": "ExternalUser",
  "principal_id": "provider_name:UserA"
}
```

The **user** field records the information about the operator, which is **provider_name/UserA** (value of the **name** field) in this example. Note the following fields.

Field	Description
name	Username of the operator. The format is <code><idp_id>/<user-session-name></code> . In this example, the value is provider_name/UserA .
principal_id	Identity ID of the operator. The format is <code><idp_id>.<user-session-name></code> . In this example, the value is provider_name:UserA .
principal_urn	URN of the operator. The format is <code>sts::<account-id>:external-user:<idp_id>/<user-session-name></code> . In this example, the value is sts::797c8fc3c***2dc6bf70bd:external-user:provider_name/UserA .

NOTE

idp_id indicates the name of the IAM identity provider. To obtain its value, log in to the IAM console and view the identity provider name on the **Identity Providers** page.



11

Cross-Tenant Transfer Authorization

Scenarios

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 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 11-1 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: PutObject and HeadBucket .
Effect	Whether the permission in a statement is allowed or denied. The value is Allow or Deny .
Principal	Tenant A is authorized to use the bucket policy. You can obtain the domain ID on the My Credential page. Principal formats: • domain/Tenant A's account ID:agency/cts_admin_trust: indicates that permissions are granted to the cts_admin_trust agency of tenant A, allowing CTS to transfer logs to OBS buckets using the agency. • domain/Account ID:user/*: indicates that permissions are granted to all users of tenant A. • domain/Account ID:identity-provider/provider-name: indicates that permissions are granted to the specified identity provider of tenant A.
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.

- Click **Save**.
- If the OBS bucket of tenant B is encrypted using a custom key, you need to authorize tenant A in Data Encryption Workshop (DEW).

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.

- Tenant A logs in to the management console.
- Click  in the upper left corner to select the desired region and project.
- Click  in the upper left corner and choose **Management & Governance > Cloud Trace Service**. The CTS console is displayed.
- Choose **Tracker List** in the navigation pane.
- Locate a data tracker and click **Configure** in the **Operation** column.
- 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.

12 Verifying Trace File Integrity

12.1 Enabling Verification of Trace File Integrity

Scenarios

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. CTS supports integrity verification of trace files for trackers configured with OBS transfer.

Enabling Verification of Trace File Integrity

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.

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 transfer configuration step.

12.2 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/Cloud service

Example: **User Define/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_Year-Month-DayT Hour-Minute-SecondZ.json.gz (*Year-Month-DayT Hour-Minute-Second* indicates the time when the digest file was sent to OBS.)

Example: *File prefix_CloudTrace-Digest_Region_2016-05-30T16-20-56Z.json.gz*

Digest File Structure

Table 12-1 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.
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.

Field	Mandatory	Type	Description
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 12-1](#).

```
{
  "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/eu-west-101/2017/3/28/Digest/EVS/mylog_CloudTrace-Digest_eu-west-101/_2017-03-28T02-09-17Z.json.gz",
  "digest_signature_algorithm": "SHA256withRSA",
  "digest_end": false,
  "previous_digest_bucket": "bucket",
  "previous_digest_object": "CloudTraces/eu-west-101/2017/3/28/Digest/EVS/mylog_CloudTrace-Digest_eu-west-101/_2017-03-28T01-09-17Z.json.gz",
  "previous_digest_hash_value": "5e08875de01b894eda5d1399d7b049fe",
  "previous_digest_hash_algorithm": "MD5",
  "previous_digest_signature":
    "7af7cbef4f3c78eab5048030d402810841400cf70eb22f93d4fedd13b13a8208a5dc04ce2f8bd0a4918f933ca3fc"
```

```
b17595ae59386a2dc3e3046fa97688a9815a2d036fa10193534c0ebbecff67221e22ac9cf8b781cbae3a81eaccfc  
0a2bd1a99081b1e4fe99b19caa771876ba7cce16d002feb4578cd89bc6f1faaca639ab48f3cb56007bcc5e248968  
f4a17a95b8cdbc7d8bbd7c63630da878cd4d471fc75c60bac5f730d94fefe8fdd2f2fa8accd62dbe100eab7773e79  
15e91be4474291b9dacea63a8267390bcb4855b5825554ebb07d4a29ce077c364213c575c461d1e9fafa0c29fde  
1c6de1d5630e015200821b2f3ae91e53cd8591433dd7c0b4c8bc",  
"previous_digest_end": false,  
"log_files": [{  
  "bucket": "bucket",  
  "object": "CloudTraces/eu-west-101/2017/3/28/ECS/mylog_CloudTrace_eu-west-101/  
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  
07bcc5e248968f4a17a95b8cdbc7d8bbd7c63630da878cd4d471fc75c60bac5f730d94fefe8fdd2f2fa8accd  
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.

12.3 Verifying Trace File Integrity

Scenarios

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.

Verifying Trace File Integrity

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

1. Obtain a digest file.
 - a. Obtain the latest digest file within the time range to be verified from the OBS bucket.

- 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:

```
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsjQDkl8COPRhOCvm7ZI8sYZ20oJl+ay/  
gwRSk9q0gkY3pP0RrAhSsEzgYdYjaMCqixkmbpt4AH9AROU4drnoCAZSMqRxcgvObGC9kVd4q95l4zibsw  
AsksjuNQo/XoJbL+rRAqCa+1uetgVU4k4Yx8RryYxYx/tlmvMe/O4mGAlaTf+rsqt3VXR1Qlj5lYR/nx41BEgC/  
Kb1eLYAfDaaab8WS5INRprj7qdu6oAo4Ug47WqbecvEtG3JRpj5+oqLyW41Fvse3osC0h5DQdxTt4x00/rVZ  
+gH7Kua00y7gC8YOxFVpYbfn/oW61PUDeHG/N9hUjOrlgDDJpD2YbCIQIDAQAB
```

- -
 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/eu-west-101/2017/3/28/Digest/EVS/mylog_CloudTrace-Digest_eu-  
west-101/  
_2017-03-28T02-09-17Z.json.gze280d203da44015e0eda3faa7a2ec9612221cc0dc8b0fe320db4febe6014  
2350641ad19da18cb6d3f5e7faad792c3efe98836c6d6547f5e5c7a48f7088000a057af26cc3bb913cae163  
7bfa9e4231b7d1fd6d98eaba735e509e7c5ea3c6757f732b4468f7418ef18e3312ac696dd786ec5792eacf  
94aee27cd7be76bf23b641c5e9a686cca6414745787254100c2bee31e584a15c2229270f9dee81f9043574
```

- -
 -
 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.BufferedReader;
import java.io.BufferedInputStream;
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.eu-west-101.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
        =
        "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsjQDkl8COPRhOCvm7ZI8sYZ20ojl+ay/
        gwRSk9q0gkY3pP0RrAhSsEzgYdYjaMCqixkmbpt4AH9AROU4drnoCAZSMqRxcgv0bGC9kVd4q95l4zibsw
        AsksjuNQo/XoJbL+rRAqCa+1uetgVU4k4Yx8RryYxYx/tlmvMe/O4mGAlaTf+rsqt3VXR1QIj5IYR/nx41BEgC/
        Kb1eYAfDaaab8WS5INRprj7qdu6oAo4Ug47WqbecvEtG3JRpj5+oqLyW41Fvse3osC0h5DQdxTt4x00/rVZ
        +gH7Kua00y7gC8YOxFPyYbfn/oW61PUDeHG/N9hUjOrlgDDJpD2YbCIQIDAQAB";

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

```
// Specify a cryptographic 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 signatruePrevious = objectPreviousMetadata.getMetadata().get("meta-
signature").toString();
String signatruePreviousExpect = digestFile.getString("previous_digest_signature");
if (signatruePrevious.equals(signatruePreviousExpect)) {
    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.");
}
}
```

13 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 13-1 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

14 Permissions Management

You can use Identity and Access Management (IAM) for fine-grained permissions control for your CTS. With IAM, you can:

- Create IAM users for personnel based on your enterprise's organizational structure. Each IAM user has their own identity credentials for accessing CTS resources.
- Grant only the permissions required for users to perform a specific task.
- Entrust other Huawei Cloud accounts or cloud services to perform efficient O&M on your CTS resources.

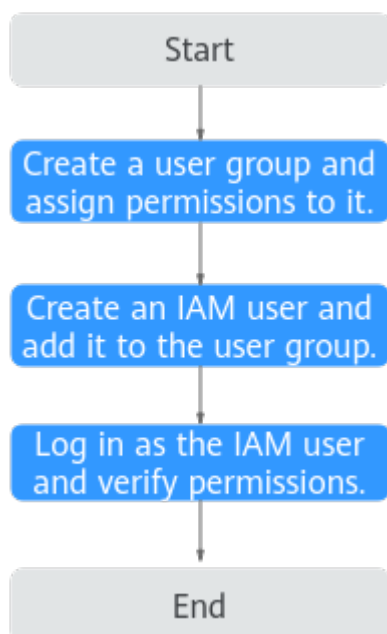
If your Huawei Cloud account does not require individual IAM users, you can skip this section.

Prerequisites

Before granting permissions to user groups, learn about system-defined permissions in [System-defined roles and policies supported by CTS](#)).

Process Flow

Figure 14-1 Process of granting CTS permissions



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

15 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.

16 Supported Services and Operations

Table 16-1 Supported services and operations

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

Category	Cloud Service	Operations
	Virtual Private Network (VPN)	VPN operations that can be recorded by CTS
	Global Accelerator	Global Accelerator operations that can be recorded by CTS
	Enterprise Router	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 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
	Application Operations Management (AOM)	AOM 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	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

Category	Cloud Service	Operations
	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
	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
	TaurusDB	TaurusDB operations that can be recorded by CTS
	Data Admin Service (DAS)	DAS operations that can be recorded by CTS
	Distributed Database Middleware (DDM)	DDM operations that can be recorded by CTS
Security	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

Category	Cloud Service	Operations
	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
	Cloud Bastion Host (CBH)	CBH operations that can be recorded by CTS
	SecMaster	SecMaster operations that can be recorded by CTS
Enterprise Application	ROMA Connect	ROMA Connect operations that can be recorded by CTS
	Domain Name Service (DNS)	DNS operations that can be recorded by CTS
Big Data	MapReduce Service (MRS)	MRS operations that can be recorded by CTS
	Data Lake Insight (DLI)	DLI operations that can be recorded by CTS
	GaussDB(DWS)	GaussDB(DWS) operations that can be recorded by CTS
	Cloud Search Service (CSS)	CSS operations that can be recorded by CTS
	DataArts Studio	DataArts Studio operations that can be recorded by CTS