Cloud Trace Service

User Guide

Issue   01
Date   2024-12-27

Huawei Cloud Computing Technologies Co., Ltd.

Contents

1 Service Overview

1.1 What Is Cloud Trace Service

The log audit module is a core component necessary for information security audit and an important part for the information systems of enterprises and public institutions to provide security risk management and control.

Cloud Trace Service (CTS) is a log audit service for security. It allows you to collect, store, and query resource operation records. You can use these records to perform security analysis, track resource changes, audit compliance, and locate faults.

Figure 1-1 CTS service diagram
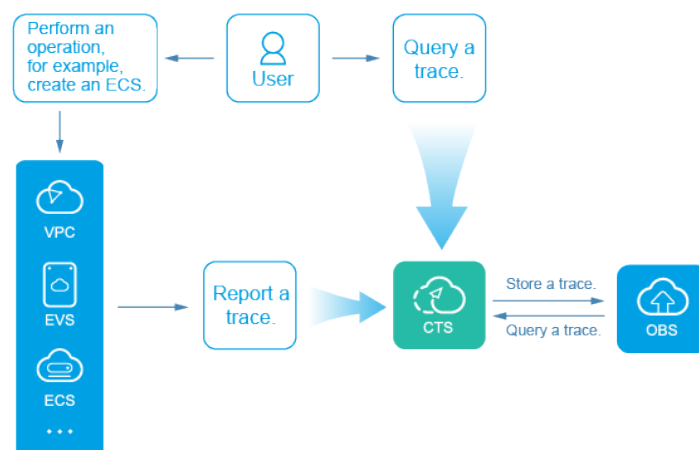
CTS provides the following functions:

- Trace recording: CTS records operations performed on the management console or by calling APIs, as well as operations triggered by each interconnected service.

- Trace query: Operation records of the last seven days can be queried on the management console from multiple dimensions, such as the trace type, trace source, resource type, filter, operator and trace status.

- Trace transfer: Traces can be transferred to Object Storage Service (OBS) buckets or Log Tank Service (LTS) log streams periodically. During transfer, traces are compressed into trace files by service.

- Key event notification: CTS works with Simple Message Notification (SMN) to send notifications to your mobile phones and email addresses to notify you of certain key operations.

1.2 Basic Concepts

Trackers

When you enable CTS for the first time, a management tracker named **system** is created automatically.

Th management tracker identifies and associates with all cloud services your tenant account is using, and records all operations of your tenant account.

Currently, only one tracker can be created for each tenant.

Traces

Traces are operation logs of cloud service resources and are captured and stored by CTS. You can view traces to get to know details of operations performed on specific resources.

Traces: management traces reported by cloud services.

Trace List

The trace list displays traces generated in the last seven days. These traces record operations (in the last hour by default) on cloud service resources, including creation, modification, and deletion, but do not record query operations.

- Management traces: record details about creating, configuring, and deleting cloud service resources in your tenant account.

Trace Files

A trace file is a collection of traces. CTS generates trace files based on services and transfer cycle and send these files to your specified OBS bucket in real time. In most cases, all traces of a service generated in a transfer cycle are compressed into one trace file. However, if there are a large number of traces, CTS will adjust the number of traces contained in each trace file.

Traces files are in JSON format. **Figure 1-2** shows an example of a trace file.

Figure 1-2 Trace file example

```
[{
    "time": 1491482532828,
    "user": {
        "id": "59f40829165447fb9470b56f41dff599",
        "name": "          ",
        "domain": {
            "name": "          ",
            "id": "0f27bc42d1eb46a69482a72cbfc33ed2"
        }
    },
    "request": {
        "bucket_name": "obs-570f",
        "file_prefix_name": "-RsU",
        "status": "disabled"
    },
    "response": {
        "bucket_name": "obs-570f",
        "file_prefix_name": "-RsU",
        "status": "disabled",
        "tracker_name": "system"
    },
    "service_type": "CTS",
    "resource_type": "tracker",
    "resource_name": "system",
    "source_ip": "          ",
    "trace_name": "updateTracker",
    "trace_type": "ConsoleAction",
    "api_version": "1.0",
    "record_time": 1491482532857,
    "trace_id": "7519ef09-1ac6-11e7-8cc0-3d812829baf6",
    "trace_status": "normal"
},
{
    "time": 1491482535203,
    "user": {
        "id": "59f40829165447fb9470b56f41dff599",
        "name": "          ",
        "domain": {
            "name": "          ",
            "id": "0f27bc42d1eb46a69482a72cbfc33ed2"
        }
    },
    "request": {
        "bucket_name": "obs-570f",
        "file_prefix_name": "-RsU",
        "status": "enabled"
    },
    "response": {
        "bucket_name": "obs-570f",
        "file_prefix_name": "-RsU",
        "status": "enabled",
        "tracker_name": "system"
    },
    "service_type": "CTS",
    "resource_type": "tracker",
    "resource_name": "system",
    "source_ip": "          ",
    "trace_name": "updateTracker",
    "trace_type": "ConsoleAction",
    "api_version": "1.0",
    "record_time": 1491482535224,
    "trace_id": "76831bfb-1ac6-11e7-98ff-a1036f244dcd",
    "trace_status": "normal"
}]
```

Regions

A region refers to a geographic area where the server for installing CTS is located. AZs in the same geographic area can communicate with each other through an internal network.

Data centers (DCs) of the cloud platform are scattered across different regions of the world, for example, Europe and Asia. Enabling CTS in different regions makes applications more user-friendly and meets the laws and regulations of different regions.

Projects

A project corresponds to a cloud platform region. Default projects are defined to isolate resources (including computing, storage, and network resources) across regions. You can create sub-projects in a default region project to isolate resources more precisely.

1.3 How CTS Functions

CTS connects to other cloud services on the cloud platform, records operations on cloud resources and the results, and stores these records in the form of trace files to OBS buckets in real time.

You can use CTS to create trackers to record trace files. If trace transfer has been configured, trace files will be stored in the OBS bucket that you have specified.

You can perform the following operations on a trace file:

- Trace file creation and storage
  - When you add, delete, or modify resources on services interconnected with CTS, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), and Image Management Service (IMS), the target services will record the operations and their results automatically and deliver them in the form of trace files to CTS for archiving.
  - Operation records of the last seven days are displayed on the CTS console. If trace transfer has been enabled, operation records are periodically delivered to the OBS bucket that you have specified for long-term storage.
- Trace file query
  - You can query operation records in the last seven days on the **Trace List** page by time and other filters.
  - To query operation records earlier than seven days, you can download the trace files stored in OBS buckets if trace transfer has been configured.
  - You can enable, disable, configure, or delete a tracker on the **Tracker List** page.

For example, if you create an image using IMS, the service will report the creation operation to CTS. Then, CTS will deliver the trace to an OBS bucket for storage if trace transfer has been configured. You can view trace files in the trace list. **Figure 1-3** shows the working principle of CTS.

Figure 1-3 How CTS functions
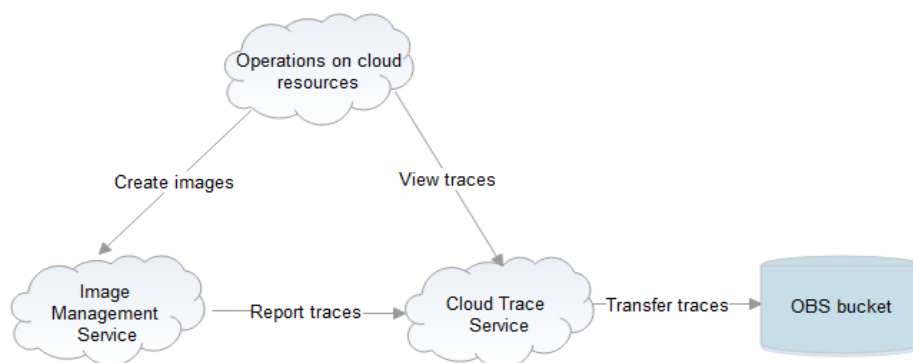
1.4 Application Scenarios

CTS can be used in the following four scenarios:

1.5 Billing

You can use the basic functions of CTS for free, including enabling a tracker, tracking traces, as well as storing and querying traces of the last seven days. In addition, CTS works with other services to provide you with value-added functions such as trace file transfer. These functions may generate fees in other cloud services, but the fees are usually low. Use the value-added functions as needed.

Value-added functions:

- Trace transfer: You can configure a tracker to transfer trace files to OBS buckets. Trace files transferred by the management tracker are permanently stored.

- Trace analysis: This function is provided by CTS and is free to use. However, it depends on log storage of Log Tank Service (LTS), which may generate fees.

- Key event notification: CTS provides the key event notification function to send notifications to your mobile phones and email addresses when specific operations are performed. You need to subscribe to topics on the Simple Message Notification (SMN) console for this function to take effect.

1.6 Permissions Management

You can use Identity and Access Management (IAM) to manage CTS permissions and control access to your resources. IAM provides identity authentication, permissions management, and access control.

With IAM, you can use your account to create IAM users for your employees, and assign permissions to the users to control their access to specific resource types. For example, you can create IAM users for software developers and assign specific permissions to allow them to use CTS resources but prevent them from deleting resources or performing any high-risk operations.

If your account does not require IAM users for permissions management, you may skip this section.

IAM can be used free of charge. You pay only for the resources in your account. For details, see *IAM Service Overview*.

CTS Permissions

By default, new IAM users do not have any permissions assigned. To assign permissions to these new users, add them to one or more groups, and attach permissions policies or roles to these groups.

CTS is a project-level service deployed and accessed in specific physical regions. When assigning CTS permissions to a user group, specify region-specific projects where the permissions will take effect. If you select **All projects**, the permissions will be granted for all region-specific projects. When accessing CTS, the users need to switch to a region where they have been authorized to use this service.

You can grant users permissions by using roles and policies.

- Roles: A type of coarse-grained authorization mechanism that provides only a limited number of service-level roles. When using roles to grant permissions, you also need to assign dependency roles. Roles are not an ideal choice for fine-grained authorization and secure access control.

- Policies: A type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions. This mechanism allows for more flexible policy-based authorization for more secure access control. For example, you can grant ECS users only the permissions for managing a certain type of ECSs. Most policies define permissions based on APIs.

For the API actions supported by CTS, see **Table 1-1**.

Table 1-1 System-defined roles and policies supported by CTS

Role/ Policy Name	Description	Type	Dependency
CTS FullAccess	Full permissions for CTS.	System-defined policy	None
CTS ReadOnlyAccess	Read-only permissions for CTS.	System-defined policy	None
CTS Administrator	Administrator permissions for CTS. Users granted these permissions can perform all operations on CTS. Users with this permission can perform read-only operations on all services except IAM.	System-defined role	This role must be used together with the **Tenant Guest** and **OBS Administrator** roles in the same project.

Table 1-2 lists the common operations supported by each system-defined policy or role of CTS. Select the policies or roles as required.

Table 1-2 Common operations supported by system-defined policies or roles

Operation	CTS FullAccess	CTS ReadOnlyAccess	CTS Administrator
Querying traces	√	√	√
Querying quotas	√	√	√
Creating a tracker	√	×	√

Operation	CTS FullAccess	CTS ReadOnlyAccess	CTS Administrator
Modifying a tracker	√	×	√
Disabling a tracker	√	×	√
Enabling a tracker	√	×	√
Querying a tracker	√	√	√
Deleting a tracker	√	×	√
Creating a key event notification	√	×	√
Modifying a key event notification	√	×	√
Disabling a key event notification	√	×	√
Enabling a key event notification	√	×	√
Querying a key event notification	√	√	√
Deleting a key event notification	√	×	√

Custom Permissions Policies

You can create custom permissions policies to supplement the system-defined policies.

● For details, see "Creating a Custom Policy" in the *IAM User Guide*.

2 Getting Started

2.1 Overview

Scenarios

You need to enable CTS before using it. A management tracker named **system** is automatically created when CTS is enabled. All traces recorded by CTS are associated with the tracker.

Trace files must be stored in Object Storage Service (OBS) buckets or Log Tank Service (LTS) log streams. 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.

Associated Services

- OBS: used to store trace files.

    ☐ **NOTE**

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

- LTS: stores logs.

- SMN: Sends email or SMS message notifications to users when key operations are performed.

Procedure

1. Log in to the management console.

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

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

4. Click **Enable CTS**.

5. In the displayed dialog box, click **Enable**. A tracker is automatically created.

   You can view the tracker information on the **Tracker List** page.

   The tracker records operations on cloud resources performed by the tenant who creates the tracker. For details about the cloud services supported by CTS, see **Supported Services and Operations**.

2.2 Querying Real-Time Traces

Scenarios

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

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

- **Viewing Real-Time Traces in the Trace List**

Viewing Real-Time Traces in the Trace List

1. Log in to the management console.

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

3. Choose **Trace List** in the navigation pane on the left.

4. Set filters to search for your desired traces. The following filters are available:

   - **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**: Select a filter from the drop-down list.

     - If you select **Resource ID** for **Search By**, specify a resource ID.

     - If you select **Trace name** for **Search By**, specify a trace name.

     - If you select **Resource name** for **Search By**, specify a resource name.

   - **Operator**: Select a user.

   - **Trace Status**: Select **All trace statuses**, **Normal**, **Warning**, or **Incident**.

   - Time range: You can query traces generated during any time range in the last seven days.

   - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5000 records.

5. Click **Query**.

6. On the **Trace List** page, you can also export and refresh the trace list.

   - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5000 records.

   - Click ↻ to view the latest information about traces.

7. Click ⌄ on the left of a trace to expand its details.

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

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

2.3 Querying Archived Traces

Scenarios

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

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

Prerequisites

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

Querying Traces Transferred to OBS

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

1. Log in to the management console.

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

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

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

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

   – The trace file storage path is as follows:

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

     An example is **User-defined name > CloudTraces > region > 2016 > 5 > 19 > system > ECS**.

   – The trace file naming format is as follows:

     *Trace file prefix*_**CloudTrace**_*Region/Region-project_Time when the trace file was uploaded to OBS: Year-Month-Day***T***Hour-Minute-Second***Z**_*Random characters*.**json.gz**

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

   📖 **NOTE**

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

     Downloading the file will incur request fees and traffic fees.

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

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

Querying Traces Transferred to LTS

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

Step 1 Log in to the management console.

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

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

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

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

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

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

📖 **NOTE**

> Each time you can download up to 5,000 log events. If the number of selected log events exceeds 5000, you cannot download them directly from LTS. Transfer them to OBS and then download them from OBS.

----End

2.4 Configuring Key Event Notifications

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

Scenarios

You can use this function for:

- Real-time detection of high-risk operations (such as VM restart and security configuration changes), cost-sensitive operations (such as creating and deleting expensive resources), and service-sensitive operations (such as network configuration changes).

- Detection of operations such as login of users with admin-level permissions or operations performed by users who do not have the required permissions.

- Connection with your own audit system: You can synchronize all audit logs to your audit system in real time to analyze the API calling success rate, unauthorized operations, security, and costs.

Usage Description

- SMN sends key event notifications to subscribers. Before setting notifications, you need to know how to create topics and add subscriptions on the SMN console.

- You can create up to 100 key event notifications on CTS:

  - Specify key operations, users, and topics to customize notifications.

  - Complete key event notifications can be sent to notification topics.

- If CTS and Cloud Eye use the same message topic, they can receive messages from the same terminal but with different content.

- You can configure one key event notification for operations initiated by a maximum of 50 users in 10 user groups. For each key event notification, you can add users from different user groups, but cannot select multiple user groups at once.

Creating a Key Event Notification

1. Log in to the management console.

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

3. In the navigation pane on the left, choose **Key Event Notifications**.

   The **Key Event Notifications** page is displayed.

4. Click **Create Key Event Notification**. On the displayed page, specify required parameters.

5. Enter a key event notification name.

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

6. Configure key operations.

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

   – **Operation Type**: Select **All** or **Custom**.

     ▪ **All**: This option is suitable if you have connected CTS to your own audit system. When **All** is chosen, you cannot deselect operations because all operations on all cloud services that have connected with CTS will trigger notifications. You are advised to use an SMN topic for which HTTPS is selected.

     ▪ **Custom**: This option is suitable for enterprises that require detection of high-risk, cost-sensitive, service-sensitive, and unauthorized operations. You can connect CTS to your own audit system for log analysis.

       Customize the operations that will trigger notifications. Up to 1000 operations of 100 services can be added for each notification. For details, see **Supported Services and Operations**.

   – **Advanced Filter**: You can set an advanced filter to specify the operations that will trigger notifications. Operations can be filtered by fields **api_version**, **code**, **trace_rating**, **trace_type**, **resource_id**, and **resource_name**. Up to six filter conditions can be set. When you configure multiple conditions, specify whether an operation is considered a match when all conditions are met (AND) or any of the conditions are met (OR).

7. Configure users.

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

   – If you select **All users**, SMN will notify subscribers of key operations initiated by all users.

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

8. Configure an SMN topic.

   – When **Yes** is selected for **Send Notification**:

     ▪ **SMN Topic**: You can select an existing topic or click **SMN** to create one on the SMN console.

   – If you do not want to send notifications, no further action is required.

9. Click **OK**.

Managing Key Event Notifications

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

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner and choose **Management & Deployment** > **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 2-1**.

Table 2-1 Related operations

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

----End

3 Querying Traces

3.1 Querying Real-Time Traces

Scenarios

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

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

- **Viewing Real-Time Traces in the Trace List**

Viewing Real-Time Traces in the Trace List

1. Log in to the management console.

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

3. Choose **Trace List** in the navigation pane on the left.

4. Set filters to search for your desired traces. The following filters are available:

    – **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**: Select a filter from the drop-down list.

        ▪ If you select **Resource ID** for **Search By**, specify a resource ID.

        ▪ If you select **Trace name** for **Search By**, specify a trace name.

        ▪ If you select **Resource name** for **Search By**, specify a resource name.

    – **Operator**: Select a user.

    – **Trace Status**: Select **All trace statuses**, **Normal**, **Warning**, or **Incident**.

    – Time range: You can query traces generated during any time range in the last seven days.

    – Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5000 records.

5. Click **Query**.

6. On the **Trace List** page, you can also export and refresh the trace list.
   - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5000 records.
   - Click ↻ to view the latest information about traces.

7. Click ⌄ on the left of a trace to expand its details.

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

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

3.2 Querying Archived Traces

Scenarios

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

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

Prerequisites

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

Querying Traces Transferred to OBS

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

1. Log in to the management console.

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

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

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

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

   – The trace file storage path is as follows:

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

     An example is **User-defined name > CloudTraces > region > 2016 > 5 > 19 > system > ECS**.

   – The trace file naming format is as follows:

     *Trace file prefix*_**CloudTrace**_*Region/Region-project_Time when the trace file was uploaded to OBS: Year-Month-Day***T***Hour-Minute-Second***Z**_*Random characters*.**json.gz**

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

   📖 **NOTE**

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

   Downloading the file will incur request fees and traffic fees.

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

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

Querying Traces Transferred to LTS

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

Step 1 Log in to the management console.

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

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

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

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

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

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

📖 **NOTE**

Each time you can download up to 5,000 log events. If the number of selected log events exceeds 5000, you cannot download them directly from LTS. Transfer them to OBS and then download them from OBS.

----End

4 Management Trackers

The management tracker records management traces, which are operations on all cloud resources, such as creation, login, and deletion.

This section describes how to use the management tracker.

4.1 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. Th management tracker identifies and associates with all cloud services your tenant account is using, and records all operations of your tenant account.

📖 **NOTE**

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

4.2 Configuring a Tracker

Scenario

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

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

📖 **NOTE**

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

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

This section describes how to configure the management tracker.

Prerequisites

You have enabled CTS.

Procedure

Step 1 Log in to the management console.

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

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

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

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

Step 6 On the **Configure Transfer** page, modify the transfer configurations of the tracker. For details, see **Table 4-1**.

Table 4-1 Transfer parameters

Parameter	Description
Transfer to OBS	Select an existing OBS bucket or create one on this page and set **File Prefix** if **Transfer to OBS** is enabled. When **Transfer to OBS** is disabled, no operation is required.
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	**Existing**: Select an existing OBS bucket.

Parameter	Description
Select Bucket	If you select **New** for **OBS Bucket**, 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	For the management tracker, the retention period configured on the OBS console is used by default and cannot be changed.
File Prefix	A prefix is used to mark a transferred trace file. Your specified prefix will be automatically added to the beginning of the name of a transferred file, helping you quickly filter files. Enter 0 to 64 characters. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed.
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 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 8 (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.

Table 4-2 Tag parameters

Para mete r	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 _.:=+-@, but cannot start or end with a space or start with _sys_.	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 _.:=+-@, but cannot start or end with a space.	Value_0001

----End

4.3 Disabling or Enabling a Tracker

Scenario

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

This section describes how to enable or disable a tracker.

Prerequisites

You have enabled CTS.

Procedure

Step 1 Log in to the management console.

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

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

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

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

Step 6 Click **OK**.

----End

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

4.4 Deleting a Tracker

Scenario

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

Prerequisites

You have enabled CTS.

Procedure

Step 1 Log in to the management console.

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

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

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

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

Step 6 Click **OK**.

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

----End

5 Application Examples

5.1 Security Auditing

Scenario

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

Prerequisites

You have enabled CTS and trackers are running properly.

Procedure (for Old Console)

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

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

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

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

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

5. Set the time range to **Last 1 week**, set filters in sequence, and click **Query**.

   📖 **NOTE**

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

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

📖 NOTE

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

7. Download traces older than seven days or all traces by following the instructions in **Querying Archived Traces**.

8. In the trace files, search traces using keywords **createVolume** or **deleteVolume**.

9. Check the traces obtained from steps **5** and **8** to see whether there are any unauthorized operations or operations that do not conform to security rules.

5.2 Fault Locating

Scenario

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

Prerequisites

You have enabled CTS and trackers are running properly.

Procedure (for Old Console)

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

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

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

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

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

5. Set filters in sequence and click **Query**.

   📖 NOTE

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

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

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

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

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

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

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

5. Select **Management** for **Trace Type**, **ECS** for **Trace Source**, **ecs** for **Resource Type**, and **Warning** for **Trace Status**. In the returned traces, locate the trace named **createServer**.

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

5.3 Resource Tracking

Scenario

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

Prerequisites

You have enabled CTS and trackers are running properly.

Procedure (for Old Console)

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

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

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

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

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

5. Set filters in sequence and click **Query**.

   📖 **NOTE**

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

6. Choose **Tracker List** in the navigation pane on the left.

7. Download traces older than seven days or all traces by following the instructions in **Querying Archived Traces**.

8. Check all the traces obtained in **5** and **7**.

6 Trace References

6.1 Trace Structure

A trace consists of multiple key fields shown in **Table 6-1**.

📖 **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 6-1 Key trace fields

Field	Mandatory	Type	Description
time	Yes	Date	Time when a trace occurred When the field is displayed on the console, its value is the local standard time (in GMT time), for example, **Dec 8, 2016 11:24:04 GMT+08:00**. However, this field is transmitted and stored as a timestamp in APIs. In this case, the value is the number of milliseconds since 00:00:00 on January 1, 1970 (GMT).
user	Yes	Structure	Cloud account used to perform an operation The value is also displayed in the **Operator** column on the **Trace List** page. This field is transmitted and stored as a string in APIs.

Field	Mandatory	Type	Description
request	No	Structure	Requested operation This field is transmitted and stored as a string in APIs.
response	No	Structure	Response to a request This field is transmitted and stored as a string in APIs.
service_type	Yes	String	Operation source
resource_type	Yes	String	Resource type
resource_name	No	String	Resource name
resource_id	No	String	Unique resource ID
source_ip	Yes	String	IP address of the user that performed an operation The value of this field is empty if the operation was triggered by system.
trace_name	Yes	String	Operation 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.

Field	Mandatory	Type	Description
trace_type	Yes	String	Operation type There are three types of operations: • **ConsoleAction**: operations performed on the management console • **SystemAction**: operations triggered by system • **ApiCall**: operations triggered by calling API Gateway • **ObsSDK**: operations on OBS buckets, which were triggered by calling OBS SDKs • **Others**: operations on OBS buckets except those triggered by calling OBS SDKs
api_version	No	String	Version of the cloud service API which was called to perform an operation
message	No	Structure	Remarks
record_time	Yes	Number	Time when the operation was recorded, in the form of a timestamp
trace_id	Yes	String	Unique operation ID
code	No	Number	HTTP return code, such as 200 or 400
request_id	No	String	ID of a recorded request
location_info	No	String	Information required for fault locating after a request error
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

Field	Mandatory	Type	Description
user_agent	No	String	Type of the operations on OBS buckets except those triggered by calling OBS SDKs
content_length	No	Number	Message body length of a request to perform operations on OBS buckets
total_time	No	Number	Response time of a request to perform operations on OBS buckets

6.2 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

```
{
  "time": "2016/12/08 11:07:28 GMT+08:00",
  "user": {
    "name": "aaa/op_service",
    "id": "f2fe9fac63414a35a7d03108d5f1ea73",
    "domain": {
      "name": "aaa",
      "id": "1f9b9ba51f6b4061bd5c1736b28469f8"
    }
  },
  "request": {
    "server": {
      "name": "as-config-15f1_XWO68TFC",
      "imageRef": "b2b2c7dc-bbb0-4d6b-81dd-f0904023d54f",
      "flavorRef": "m1.tiny",
      "personality": [],
      "vpcid": "e4c374b9-3675-482c-9b81-4acd59745c2b",
      "nics": [
        {
          "subnet_id": "fff89132-88d4-4e5b-9e27-d9001167d24f",
          "nictype": null,
          "ip_address": null,
          "binding:profile": null,
          "extra_dhcp_opts": null
        }
      ],
      "adminPass": "********",
      "count": 1,
      "metadata": {
        "op_svc_userid": "26e96eda18034ae9a44130bacb967b96"
      },
      "availability_zone": "az1.dc1",
      "root_volume": {
        "volumetype": "SATA",
        "extendparam": {
          "resourceSpecCode": "SATA"
        },
```

```
         "size": 40
      },
      "data_volumes": [],
      "security_groups": [
         {
            "id": "dd597fd7-d119-4994-a22c-891fcfc54be1"
         }
      ],
      "key_name": "KeyPair-3e51"
   }
},
"response": {
   "status": "SUCCESS",
   "entities": {
      "server_id": "42d39b4a-19b7-4ee2-b01b-a9f1353b4c54"
   },
   "job_id": "4010b39d58b855980158b8574b270018",
   "job_type": "createSingleServer",
   "begin_time": "2016-12-01T03:04:38.437Z",
   "end_time": "2016-12-01T03:07:26.871Z",
   "error_code": null,
   "fail_reason": null
},
"service_type": "ECS",
"resource_type": "ecs",
"resource_name": "as-config-15f1_XWO68TFC",
"resource_id": "42d39b4a-19b7-4ee2-b01b-a9f1353b4c54",
"source_ip": "",
"trace_name": "createSingleServer",
"trace_rating": "normal",
"trace_type": "SystemAction",
"api_version": "1.0",
"record_time": "2016/12/08 11:07:28 GMT+08:00",
"trace_id": "4abc3a67-b773-11e6-8412-8f0ed3cc97c6"
}
```

You can pay special attention to the following fields:

- **time** indicates the time when the trace occurred. In this example, the time is 11:07:28 on December 8.

- **user** indicates the user who performed the operation. In this example, the user is **aaa** (**name** field) under the enterprise account **aaa** (**domain** field).

- **request** indicates the request to create an ECS server. It contains basic information about the ECS server, such as its name (**as-config-15f1_XWO68TFC**) and VPC ID (**e4c374b9-3675-482c-9b81-4acd59745c2b**).

- **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

```
{
   "time": "2016/12/08 11:24:04 GMT+08:00",
   "user": {
      "name": "aaa",
      "id": "26e96eda18034ae9a44130bacb967b96",
      "domain": {
         "name": "aaa",
         "id": "1f9b9ba51f6b4061bd5c1736b28469f8"
      }
   },
   "request": "",
   "response": "",
   "service_type": "EVS",
```

```
    "resource_type": "evs",
    "resource_name": "volume-39bc",
    "resource_id": "229142c0-2c2e-4f01-a1b4-2dfdf1c678c7",
    "source_ip": "10.146.230.124",
    "trace_name": "deleteVolume",
    "trace_rating": "normal",
    "trace_type": "ConsoleAction",
    "api_version": "1.0",
    "record_time": "2016/12/08 11:24:04 GMT+08:00",
    "trace_id": "c529254f-bcf5-11e6-a89a-7fc778a6c92c"
}
```

You can pay special attention to the following fields:

- **time** indicates the time when the trace occurred. In this example, the time is 11:24:04 on December 8.

- **user** indicates the user who performed the operation. In this example, the user is **aaa** (**name** field) under the enterprise account **aaa** (**domain** field).

- **request**: optional. It is null in this example.

- **response**: optional. It is null in this example.

- **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**.

7 Cross-Tenant Transfer Authorization

Scenario

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

Procedure

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 Policy**.

6. In the upper right corner of the page, select **JSON** and click **Edit**, and grant permissions to tenant A in the following format.

   ```
   {
       "Statement": [{
           "Sid": "xxxx",
           "Effect": "Allow",
           "Principal": {
               "ID": [
                   "domain/{{domainId}}:agency/*"
               ]
           },
           "Action": [
               "PutObject",
               "PutObjectAcl"
           ],
           "Resource": [
               "{{bucketName}}/*"
           ]
   ```

```
        },
        {
            "Sid": "xxxxx1",
            "Effect": "Allow",
            "Principal": {
            // After the OBS bucket permission of tenant B is granted to all sub-users of tenant A, the
sub-users of tenant A can configure cross-tenant transfer.
                "ID": [
                    "domain/{{domainId}}:user/*"
                ]
            // For a federated user, after the OBS bucket permission of tenant B is granted to a specified
identity provider of tenant A, the login federated user can configure cross-tenant transfer. If no
federated users are involved, delete this line.
                "Federated": "domain/{{domainId}}:identity-provider/{{provider-name}}"
            },
            "Action": [
                "HeadBucket"
            ],
            "Resource": [
                "{{bucketName}}"
            ]
        }
    ]
}
```

Table 7-1 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 three actions: "PutObject", "PutObjectAcl", 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 format: ● "domain/*account ID: agency*/*" (indicating all agencies of tenant A) ● "domain/*account ID: user*/*" (indicating all sub-users of tenant A)
Resource	Specifies a group of resources on which the statement takes effect. The wildcard (*) is supported, indicating all resources. **bucketName/*** and **bucketName** are required when cross-account transfer is configured.

7. Click **Save**.

8. If bucket encryption is configured for the OBS bucket of tenant B and the encryption key type is custom, 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, which may cause tenant B to fail to download transferred files.

9. Tenant A logs in to the management console.

10. Click ⊙ in the upper left corner to select the desired region and project.

11. Click ≡ in the upper left corner and choose > **Cloud Trace Service**. The CTS console is displayed.

12. Choose **Tracker List** in the left navigation pane.

13. Locate a data tracker and click **Configure** in the **Operation** column.

14. Select **Yes** for **Transfer to OBS**. If **OBS Bucket Account** is set to **Other users**, you need to enter the name of the bucket used for transfer.

15. Click **OK** to complete the tracker configuration.

8 Verifying Trace File Integrity

8.1 Enabling Verification of Trace File Integrity

Scenario

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

Procedure

1. Log in to the management console.

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

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

4. Choose **Tracker List** in the left navigation pane.

   📖 **NOTE**

   Click **Enable CTS** if you have not enabled CTS.

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

   📖 **NOTE**

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

8.2 Digest Files

8.2.1 Overview

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

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

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

8.2.2 Digest File Name Format

*Trace file prefix_***CloudTrace-Digest_***Region/Region-Project_Time when the digest file was sent to OBS: Year-Month-Day***T** *Hour-Minute-Second* **Z.json.gz**

An example is *Trace file prefix_***CloudTrace-Digest_***Region/Region-Project_***2016-05-30T16-20-56Z.json.gz**.

8.2.3 Digest File Structure

Table 8-1 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.
previous_digest_hash_value	No	String	Specifies the hexadecimal encoded hash value of the previous digest file.

Field	Mandatory	Type	Description
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.

8.2.4 Example Digest File

```
{
 "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-0/2017/3/28/Digest/EVS/mylog_CloudTrace-Digest_eu-west-0/
_2017-03-28T02-09-17Z.json.gz",
 "digest_signature_algorithm": "SHA256withRSA",
 "digest_end": false,
 "previous_digest_bucket": "bucket",
 "previous_digest_object": "CloudTraces/eu-west-0//2017/3/28/Digest/EVS/mylog_CloudTrace-Digest_eu-
west-0/_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-0//2017/3/28/ECS/mylog_CloudTrace_eu-west-0/
_2017-03-28T02-09-17Z_0faa86bc40071242.json.gz",
 "log_hash_value": "633a8256ae7996e21430c3a0e9897828",
 "log_hash_algorithm": "MD5"
}]
}
```

8.2.5 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

8.2.6 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.

9 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 9-1 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

10 Permissions Management

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

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

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

Prerequisites

Learn about the permissions (see **Permissions Management**) supported by CTS and choose policies or roles according to your requirements.

Process Flow

Figure 10-1 Process of granting CTS permissions
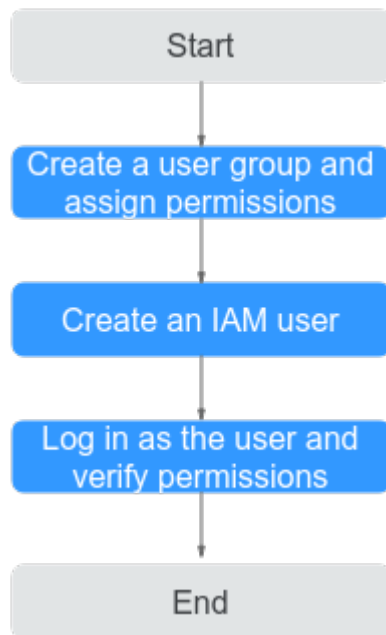
1. Create a user group and assign permissions.

   Create a user group on the IAM console, and attach the **CTS Administrator** policy to the group.

2. Create an IAM user.

   Create a user on the IAM console and add the user to the user group created in **1**.

3. Log in and verify permissions.

   Log in to the console as the user you created, and verify that the user has the assigned permissions.

11 Supported Services and Operations

Table 11-1 Supported services and operations

Category	Cloud Service	Operations
Compute	Elastic Cloud Server (ECS)	ECS User Guide > operations that can be recorded by CTS
	Image Management Service (IMS)	IMS User Guide > operations that can be recorded by CTS
	Auto Scaling (AS)	AS User Guide > operations that can be recorded by CTS
	FunctionGraph	FunctionGraph User Guide > operations that can be recorded by CTS
Storage	Cloud Server Backup Service (CSBS)	CSBS User Guide > operations that can be recorded by CTS
	Volume Backup Service (VBS)	VBS User Guide > operations that can be recorded by CTS
	Cloud Backup and Recovery (CBR)	CBR User Guide > operations that can be recorded by CTS
Network	Elastic Load Balance (ELB)	ELB User Guide > operations that can be recorded by CTS
	Domain Name Service (DNS)	DNS User Guide > operations that can be recorded by CTS
Container	Cloud Container Engine (CCE)	CCE User Guide > operations that can be recorded by CTS
Migration	Server Migration Service (SMS)	SMS User Guide > operations that can be recorded by CTS
Management & Governance	Cloud Trace Service (CTS)	CTS User Guide > operations that can be recorded by itself

Category	Cloud Service	Operations
	Identity and Access Management (IAM)	IAM User Guide > operations that can be recorded by CTS
	Tag Management Service (TMS)	TMS User Guide > operations that can be recorded by CTS
	Simple Message Notification (SMN)	SMN User Guide > operations that can be recorded by CTS
Applications and Middleware	Distributed Message Service (DMS)	DMS User Guide > operations that can be recorded by CTS
	Distributed Message Service (DMS) for Kafka	DMS for Kafka User Guide > operations that can be recorded by CTS
	Distributed Message Service (DMS) for RocketMQ	DMS for RocketMQ User Guide > operations that can be recorded by CTS
	Distributed Cache Service (DCS)	DCS User Guide > operations that can be recorded by CTS
	API Gateway (APIG)	APIG User Guide > operations that can be recorded by CTS
Database	Distributed Database Middleware (DDM)	DDM User Guide > operations that can be recorded by CTS
	Data Admin Service (DAS)	DAS User Guide > operations that can be recorded by CTS
Security	Data Encryption Workshop (DEW)	DEW User Guide > operations that can be recorded by CTS
	Web Application Firewall (WAF)	WAF User Guide > operations that can be recorded by CTS
AI	ModelArts	ModelArts User Guide > operations that can be recorded by CTS
Big Data	MapReduce Service (MRS)	MRS User Guide > operations that can be recorded by CTS
	GaussDB(DWS)	GaussDB(DWS) User Guide > operations that can be recorded by CTS
	Cloud Search Service (CSS)	CSS User Guide > operations that can be recorded by CTS
Content Delivery & Edge Computing	Intelligent EdgeFabric (IEF)	IEF User Guide > operations that can be recorded by CTS

12 FAQs

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

No. You only need to ensure that you have the permissions to perform operations on OBS buckets.

12.2 How Will CTS Be Affected If My Account Balance Is Insufficient?

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

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

12.3 What Are the Recommended Users of CTS?

It is highly recommended that cloud users should enable CTS.

- CTS is core to information security audit. It is an essential part of security risk control for information systems in enterprises and public sectors, and is also necessary for compliance with many industry standards and audit specifications.

- CTS helps accelerate troubleshooting and reduces workforce costs when exceptions occur on cloud resources. With CTS, you can track all operations involved when a fault happens, which helps narrow the possibilities.

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

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

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

12.5 Does CTS Support Integrity Verification of Trace Files?

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

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

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

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

12.7 Why Is an Operation Recorded Twice in the Trace List?

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

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

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

12.8 What Services Are Supported by Key Event Notifications?

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

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

CTS only retains traces for seven days. To store traces for a long time, configure your tracker to transfer traces to OBS buckets. For details, see **Configuring a Tracker**.

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

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

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

12.11 How Do I Find Out Who Created a Specific ECS?

Background

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

Prerequisites

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

Procedure

Step 1 Log in to the CTS console.

Step 2 Choose **Trace List** in the navigation pane.

Step 3 Set the time range to 06:00 to 12:00 of a certain day and set the following filters:

In the search box, select **Trace Source** and **ECS**. Select **Trace Name**, enter **createServer**, and press **Enter**. Then, select **Resource ID**, enter *{Resource ID of the ECS}*, and press **Enter**.

| Q Trace Source: ECS × Trace Name: createServer × Resource ID: 8acd386a-3927-4f56-815e-74c01d53e276 × Add filter | X ⚙ |
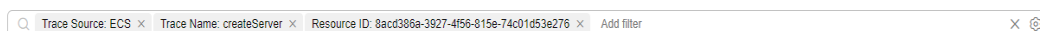
Step 4 In the filter result, click the target trace to view its details.

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

----End

12.12 How Do I Find Out the Login IP Address of an IAM User?

Background

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

Prerequisites

You have enabled CTS.

Procedure

Step 1 Log in to the CTS console.

Step 2 Select a time range and set the following filters in the search box:

Select **Trace Source** and **IAM**. Select **Trace Name**, enter **login**, and press **Enter**.

Step 3 In the filter result, click the target trace to view its details. **source_ip** indicates the login IP address, and **record_time** indicates the login time.

```
 1  {
 2      "trace_id": "3731b346-457c-11ef-a25f-f754d1610e5b",
 3      "trace_name": "login",
 4      "resource_type": "user",
 5      "trace_rating": "normal",
 6      "message": "{\"login\":{\"user_type\":\"domain owner\",\"login_protect\":{\"status
 7      "source_ip": "          ",
 8      "domain_id": "b1dd218393794db892fa784b8e1a0bda",
 9      "trace_type": "ConsoleAction",
10      "service_type": "IAM",
11      "event_type": "global",
12      "project_id": "59336be373624a998b2527fdb9913266",
13      "read_only": false,
14      "resource_id": "7853842277ce492c83de0d829bebc68d",
15      "tracker_name": "system",
16      "time": 1721358527589,
17      "resource_name": "hwstaff_pub_servicestagew3",
18      "user": {
19          "domain": {
20              "name": "hwstaff_pub_servicestagew3",
21              "id": "b1dd218393794db892fa784b8e1a0bda"
22          },
23          "name": "hwstaff_pub_servicestagew3",
24          "id": "7853842277ce492c83de0d829bebc68d"
25      },
26      "record_time": 1721358527589,
27      "code": "302"
28  }
```

----End

12.13 Why Are Two deleteMetadata Traces Generated When I Buy an ECS?

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

12.14 What If I Cannot Query Traces?

Background

Traces cannot be queried on the CTS console.

Procedure

Step 1 Check whether you have configured a proper query time range.

Step 2 Check whether you have configured filters correctly. You can combine one or more filters.

- **Trace Name**: Enter a trace name.
- **Trace ID**: Enter a trace ID.

- **Resource Name**: Enter a resource name. If the cloud resource involved in the trace does not have a resource name or the corresponding API operation does not involve the resource name parameter, leave this field empty.

- **Resource ID**: Enter a resource ID. Leave this field empty if the resource has no resource ID or if resource creation failed.

- **Trace Source**: Select a cloud service name from the drop-down list.

- **Resource Type**: Select a resource type from the drop-down list.

- **Operator**: Select one or more operators from the drop-down list.

- **Trace Status**: Select **normal**, **warning**, or **incident**.

  - **normal**: The operation succeeded.

  - **warning**: The operation failed.

  - **incident**: The operation caused a fault that is more serious than the operation failure, for example, causing other faults.

Step 3 If you still cannot query traces after the preceding steps, submit a service ticket for technical support.

----End

12.15 Can I Disable CTS?

You can use the basic functions of CTS for free, including enabling a tracker, tracking traces, as well as storing and querying traces of the last seven days. Only value-added services, such as trace transfer, are charged. If you only use the basic services, you do not need to disable CTS since no fees are generated.

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

- You can delete or disable a tracker. After a tracker is deleted or disabled, traces can still be reported.

- Delete the CTS agency from the IAM agency list. CTS will become unavailable.

12.16 How Do I Enable Alarm Notifications for EVS?

Background

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

Procedure

Step 1 Log in to the CTS console.

Step 2 In the navigation pane, choose **Key Event Notifications**. On the page displayed, click **Create Key Event Notification**.

Step 3 In the **Operation** area, select **Custom** for **Operation Type**, and select **EVS**, **evs**, and the four key operations from the **Operation List** drop-down lists to enable alarm notifications for EVS operations.

----End

12.17 Can I Receive Duplicate Traces?

Yes. CTS sends subscribed traces to your specified OBS bucket at least once. In some cases, CTS may send the same trace multiple times. As a result, you may receive duplicate traces.

12.18 Does CTS Record ECS Creation Failures?

Yes. When you create an ECS, the operation and its result will be reported to CTS.

How It Works

With CTS, you can record ECS operations for later query, auditing, and backtracking.

For details about the key ECS operations that can be recorded by CTS, see section "Key Operations Supported by CTS". When you add, delete, or modify an ECS, the ECS service automatically records your operations and results and then sends traces in the specified format to CTS for archiving. CTS stores traces of the last seven days and displays them on the **Trace List** page.

Procedure

Step 1 Log in to the CTS console.

Step 2 On the **Trace List** page, set the time range to **Last 1 week**.

Step 3 In the search box, select **Trace Source** and **ECS**, select **Resource Type** and **ecs**, and then select **Trace Name** and enter **createServer**. Press **Enter** to view the filtering result.

| Q Trace Source: ECS ×   Resource Type: ecs ×   Trace Name: createServer ×   Add filter | × ⚙ |

📖 **NOTE**

To obtain traces of the last seven days, use **createServer** as the keyword to query transferred traces in OBS buckets.

----End