Cloud Trace Service

FAQs

Issue 01

Date 2022-02-17

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks 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 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.

Contents

1 Quick Q&A

Q: If I configure trace transfer on Cloud Trace Service (CTS) as an Identity and Access Management (IAM) user, do I have to use the IAM user to perform operations on Object Storage Service (OBS) buckets as well?

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

2 How Will CTS Be Affected If My Account Is in Arrears?

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.

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 manpower costs when exceptions occur on cloud resources. With CTS, you can track all operations involved when a fault happens, which helps narrow the possibilities.

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 the access control of the OBS bucket**.

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.

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.

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.

8 Why Is the user Field Displayed as user_name/op_service in Some Traces When I Filter Traces by User?

The **op_service** account is used to elevate permissions. If a user submits a request that involves operations requiring high permissions or invocation of other services, the user's permissions may be insufficient. In this case, the user's permissions will be elevated temporarily as long as security requirements are met. When the request is complete, the user's permissions will be returned to their previous level, but the elevation action will be recorded in the request trace. As a result, both the username and **op_service** will be displayed in the **user** field of the trace.

9 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, login, and native OpenStack API calls.

10 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**.

11 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 How Can I Find Out Who Created a Specific ECS?

Solution

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

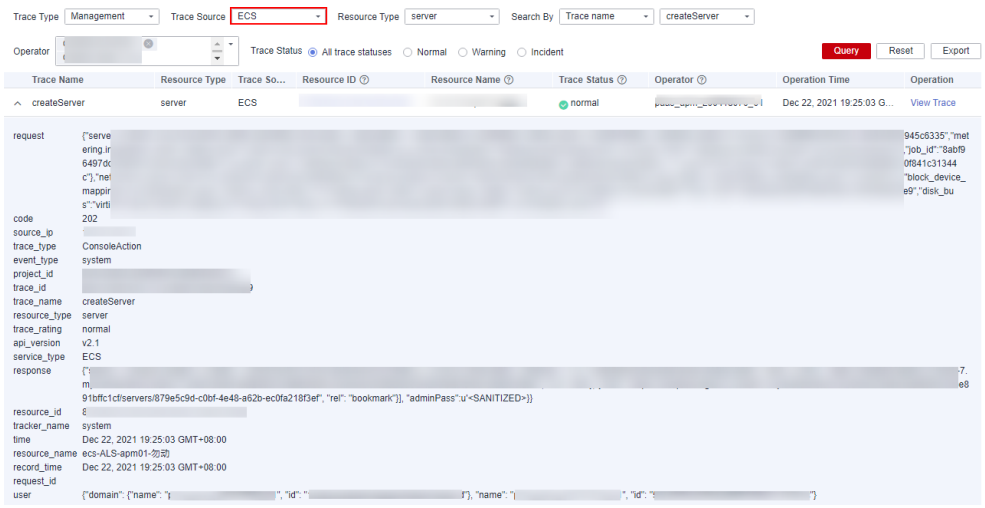
Prerequisites

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

Procedure

Log in to the CTS console, choose **Trace List**, and select **ECS** for **Trace Source**. In the displayed traces, look for the **createServer** trace with the obtained resource ID, and expand the trace 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.



13 How Can I Find Out the Login IP Address of an IAM User?

Solution

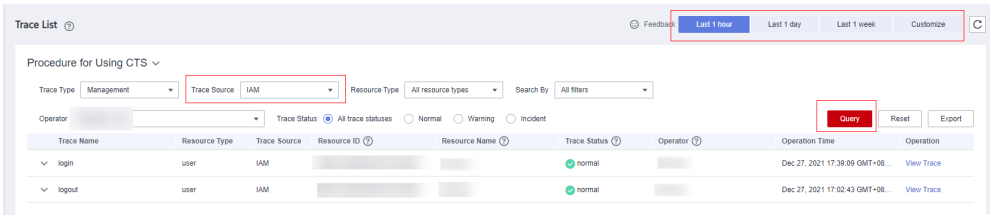
If you want to check if there are security risks in your account by examining the login IP addresses and login time of IAM users, you can view traces recorded by CTS.

Prerequisites

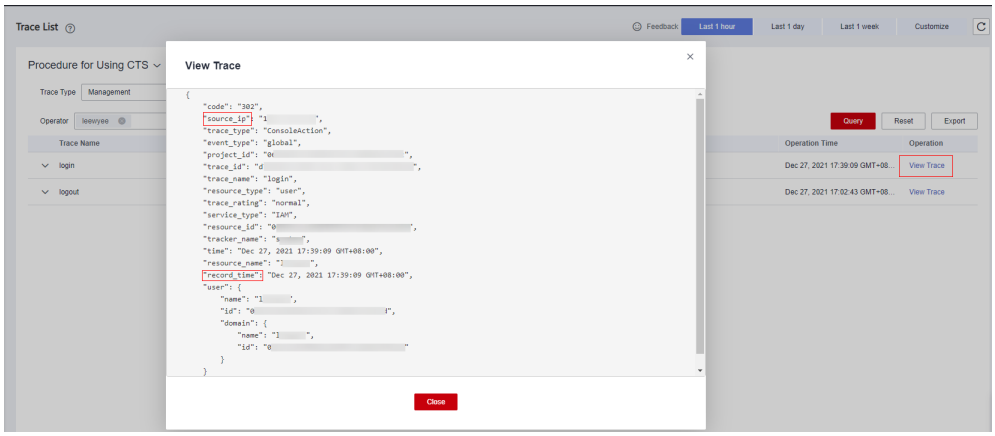
You have enabled CTS.

Procedure

Step 1 Log in to the CTS console, select **IAM** for **Trace Source**, select a time range, and click **Query**.



Step 2 Click **View Trace** in the **Operation** column of a trace to view its details. **source_ip** indicates the login IP address, and **record_time** indicates the login time.



----End

14 What Should I Do If I Deleted the cts_admin_trust Agency by Mistake?

Background

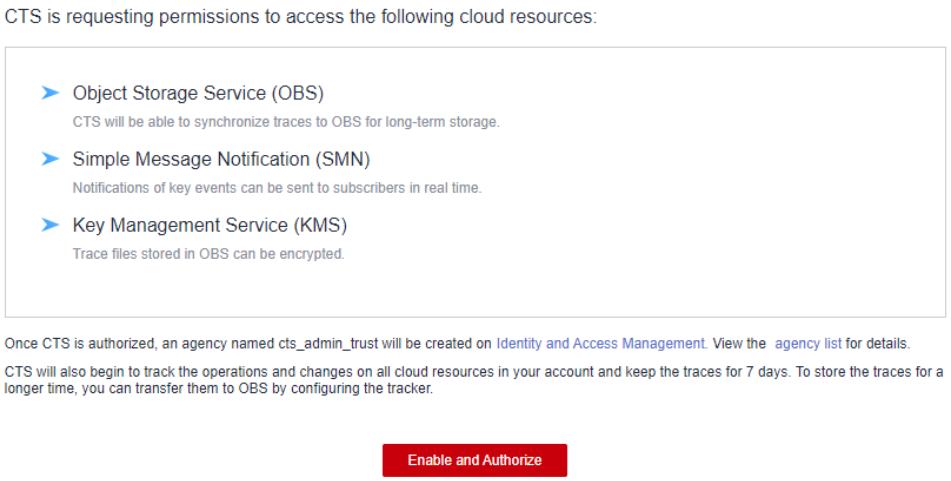
If the **cts_admin_trust** agency is deleted, traces cannot be transferred to Object Storage Service (OBS).

Solution

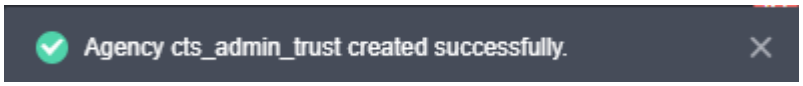
Log in to the CTS console and create the agency. Trace transfer to OBS will resume within 24 hours.

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 authorization page is displayed.



Step 3 Click **Enable and Authorize**. You will be directed to the CTS console. A message is displayed in the upper right corner, indicating that the **cts-admin_trust** agency is created.



----End

15 Why Are Two deleteMetadata Traces Generated When I Buy a Pay-per-Use or Yearly/Monthly 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. The trace type of **deleteMetadata** has now been changed to **SystemAction**.

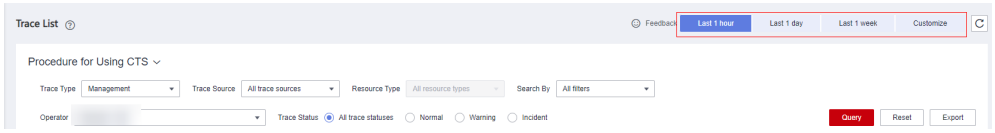
16 What Can I Do If I Cannot Query Traces?

Background

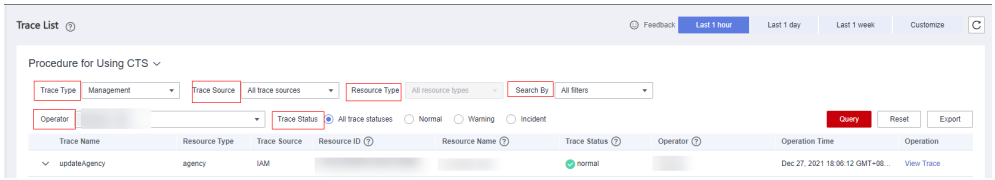
Traces cannot be queried on the CTS console.

Solution

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



Step 2 Check whether you have configured filters correctly.



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

----End

17 Can I Disable CTS?

CTS itself is free. You can use the basic services for free, including enabling trackers, tracking operations, retaining and searching for traces within 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:

- Delete or disable existing trackers. (The **system** tracker created by CTS can only be disabled and cannot be deleted.) No traces will be generated.
- Delete the CTS agency from the IAM agency list. CTS will become unavailable.