

Cloud Trace Service

FAQs

Issue 01
Date 2024-11-20



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: <https://www.huaweicloud.com/intl/en-us/>

Contents

1 Must I Use an IAM User (Sub Account) to Configure Transfer on CTS and Perform Operations on an OBS Bucket?.....	1
2 What Information Is on the Trace List?.....	2
3 How Will CTS Be Affected If My Account Balance Is Insufficient?.....	3
4 What Are the Recommended Users of CTS?.....	4
5 What Will Happen If I Have Enabled Trace Transfer But Have Not Configured an Appropriate Policy for an OBS Bucket?.....	5
6 Does CTS Support Integrity Verification of Trace Files?.....	6
7 Why Are There Some Null Fields on the View Trace Page?.....	7
8 Why Is an Operation Recorded Twice in the Trace List?.....	8
9 What Services Are Supported by Key Event Notifications?.....	9
10 How Can I Store Trace Files for a Long Time?.....	10
11 Why Are user and source_ip Null for Some Traces with trace_type as SystemAction?.....	11
12 How Do I Find Out Who Created a Specific ECS?.....	12
13 How Do I Find Out the Login IP Address of an IAM User?.....	14
14 Why Are Two deleteMetadata Traces Generated When I Buy an ECS in Pay-per-Use or Yearly/Monthly?.....	16
15 What If I Cannot Query Traces?.....	17
16 Can I Disable CTS?.....	19
17 How Do I Make the Log Retention Period 180 Days?.....	20
18 What Can I Do If a Tracker Cannot Be Created on the CTS Console?.....	23
19 What Should I Do If I Cannot Enable CTS as an IAM User?.....	24
20 How Do I Enable Alarm Notifications for EVS?.....	25
21 Can I Receive Duplicate Traces?.....	26

22 What Should I Do If I Fail to Transfer Data to an OBS Bucket Authorized by a Key of Another Tenant?.....	27
23 Does the cts_admin_trust Agency Include OBS Authorization?.....	30
24 Does CTS Record ECS Creation Failures?.....	31

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.

2 What Information Is on the Trace List?

The trace list displays two types of traces: management traces and data traces. Management traces record details about creating, configuring, and deleting cloud service resources in your tenant account. Data traces record operations on data, such as data upload and download. The trace list does not record queries.

3 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.

4 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.

5 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](#).

6 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.

7 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.

8 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.

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 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.

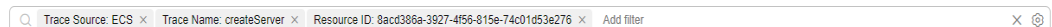
Procedure

Step 1 Log in to the CTS console.

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

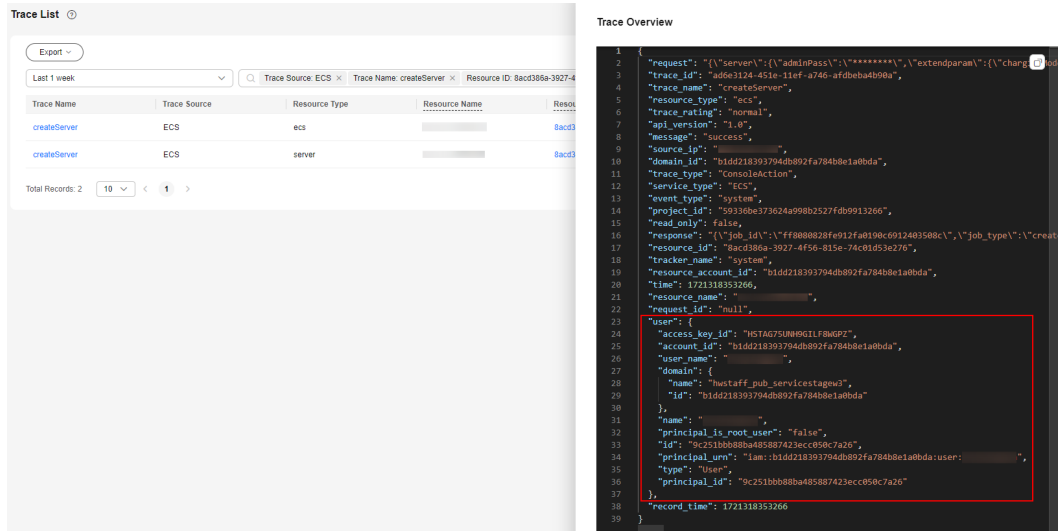
Step 3 Set the time range to 06:00 to 12:00 of a certain day and set the following filters:

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**.



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

13 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

14 Why Are Two deleteMetadata Traces Generated When I Buy an ECS in Pay-per-Use or Yearly/Monthly?

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.

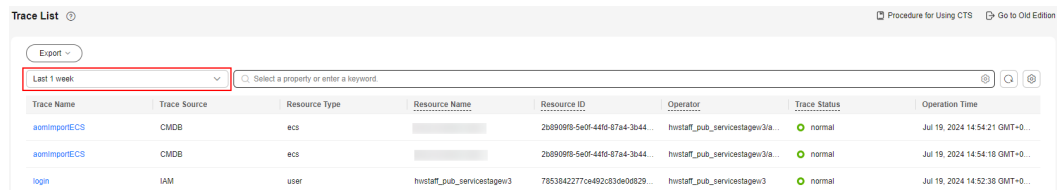
15 What If I Cannot Query Traces?

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.
- **Enterprise Project ID:** Enter an enterprise project ID.

- **Access Key:** Enter a temporary or permanent access key ID.

Step 3 For services that do not differentiate regions, such as IAM, you need to enable CTS and create a tracker named **system** in the central region CN-Hong Kong so that traces can be reported in other regions. To enable IAM to send SMS messages and emails, you also need to configure notification rules in the central region.

Step 4 If you still cannot query traces after the preceding steps, submit a service ticket for technical support.

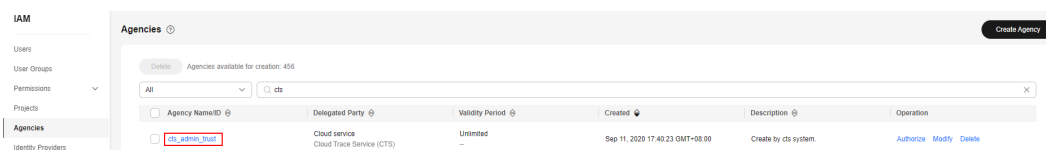
----End

16 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.



17 How Do I Make the Log Retention Period 180 Days?

Background

Audit logs may need to be stored for 180 days for query and backtracking purposes. You can perform the following steps to configure the log retention period.

Procedure

After being enabled, CTS automatically creates a management tracker named **system** and records all operations of your tenant account in the tracker. Configure the tracker for CTS to transfer logs to Log Tank Service (LTS). After the configuration is complete, LTS creates a log group and a log stream automatically and stores CTS audit logs in the log stream for 30 days by default. To store them for 180 days, change the log retention duration setting of the log stream to 180 days on LTS.



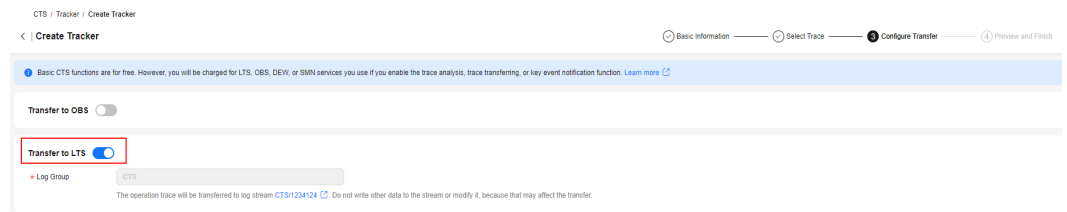
1. Log in to the management console.
 - If you log in to the console using a Huawei Cloud account, directly go to the CTS console.
 - If you log in to the console as an IAM user, contact the administrator (Huawei Cloud account or a user in the user group **admin**) to grant the following permissions to the IAM user. For details, see [Assigning Permissions to an IAM User](#).
 - CTS FullAccess
2. Click  in the upper left corner to select the desired region and project.
3. Click  in the upper left corner and choose **Management & Governance > Cloud Trace Service**.
4. Click **Configure** in the **Operation** column of the **system** tracker to configure the tracker to transfer audit logs to LTS.
5. Enable **Transfer to LTS**. The system automatically creates a log group **CTS** and a log stream **system-trace** on LTS.

Figure 17-1 Transfer to LTS




6. Go to the LTS console, change the storage duration of LTS log streams to 180 days, and configure the structuring rule to CTS.
 - a. Click  in the upper left corner and choose **Management & Governance > Log Tank Service** to access the LTS console.
 - b. On the **Log Management** page, click the modifying button in the **Operation** column of the **system-trace** log stream created in 5. On the displayed page, enable **Log Retention Duration** and change the duration to 180 days.

Figure 17-2 Modifying the log stream

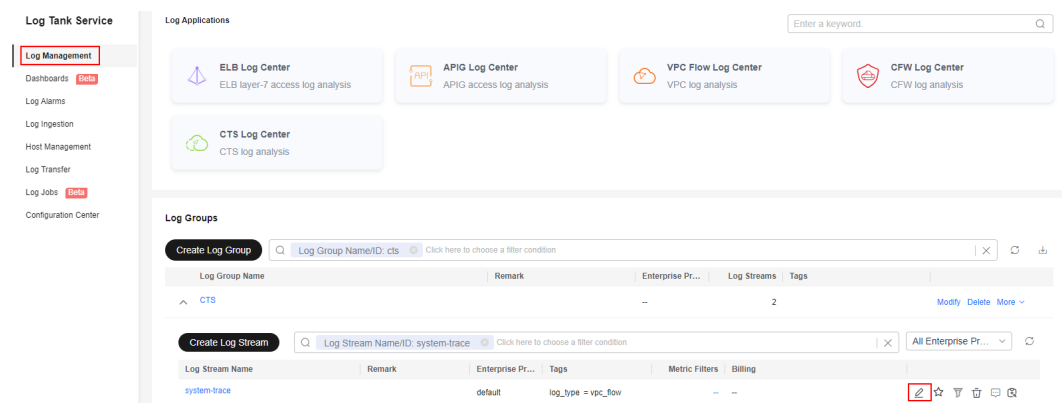
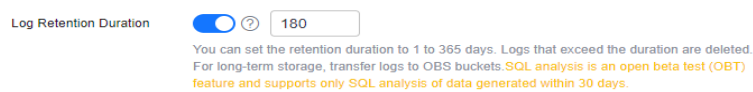
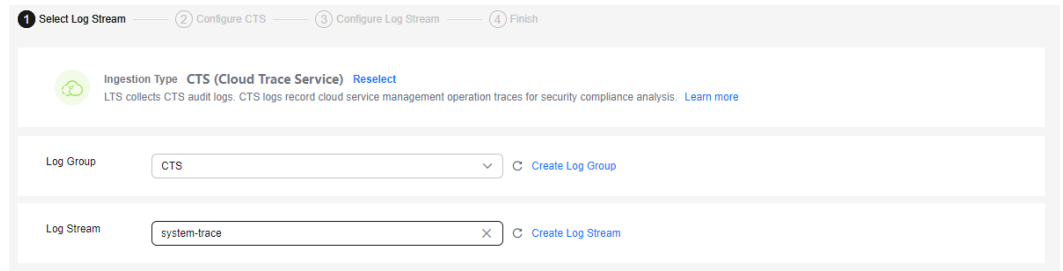


Figure 17-3 Changing the retention period



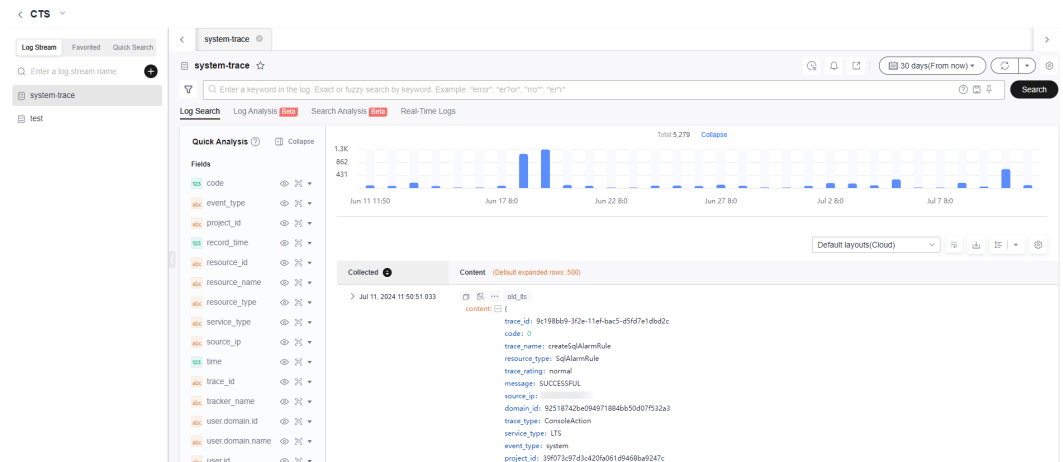
- c. Choose **Log Ingestion** and click **CTS (Cloud Trace Service)**. On the displayed page, select CTS for **Log Group** and **system-trace** for **Log Stream**.

Figure 17-4 Selecting a log stream



- d. Click **Next: Configure Log Stream** to configure the CTS log structuring.
- e. Click **Submit** to complete the log ingestion configuration.
- f. Click **Log Streams**. The log stream details page is displayed.

Figure 17-5 Log stream details



18 What Can I Do If a Tracker Cannot Be Created on the CTS Console?

Background

When you create a tracker on the CTS console, the system reports an error.

Procedure

- Step 1** Press F12 to view the error information. If it is caused by a request failure, your browser may have an interception plug-in installed. Disable the plug-in so that requests can be created.
- Step 2** If you have the permission but cannot create a tracker, log in to the central region CN-Hong Kong to check whether CTS is enabled. If not, enable CTS in the central region by using the master account and then create a tracker.
- Step 3** If you still cannot create trackers after the preceding steps, submit a service ticket for Huawei technical support.

----End

19 What Should I Do If I Cannot Enable CTS as an IAM User?

Background

If you fail to enable CTS as an IAM user, perform the following steps.

Procedure

Step 1 Check whether the IAM user has the permission.

If yes, go to [Step 2](#).

If no, contact the CTS administrator (Huawei Cloud account or a user in user group **admin**) to grant the CTS FullAccess permission to the IAM user. For details, see [Assigning Permissions to an IAM User](#).

Step 2 If the IAM user has the permission but cannot enable CTS, check whether CTS has been enabled in the central region. If not, enable CTS in the central region using the Huawei Cloud account.

----End

20 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.

Operation
SMN notifications will be sent when specified operations are performed.

Operation Type: All Custom

Operation List: EVS evs createVolume × deleteVolume × extendVolume × updateVolume × Add

You can add 100 services or 1000 operations. [Learn more](#)

Service Type	Resource Type	Operation Name	Operation
EVS	evs	createVolume,deleteVolume,extendVolu...	Delete

----End

21 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.

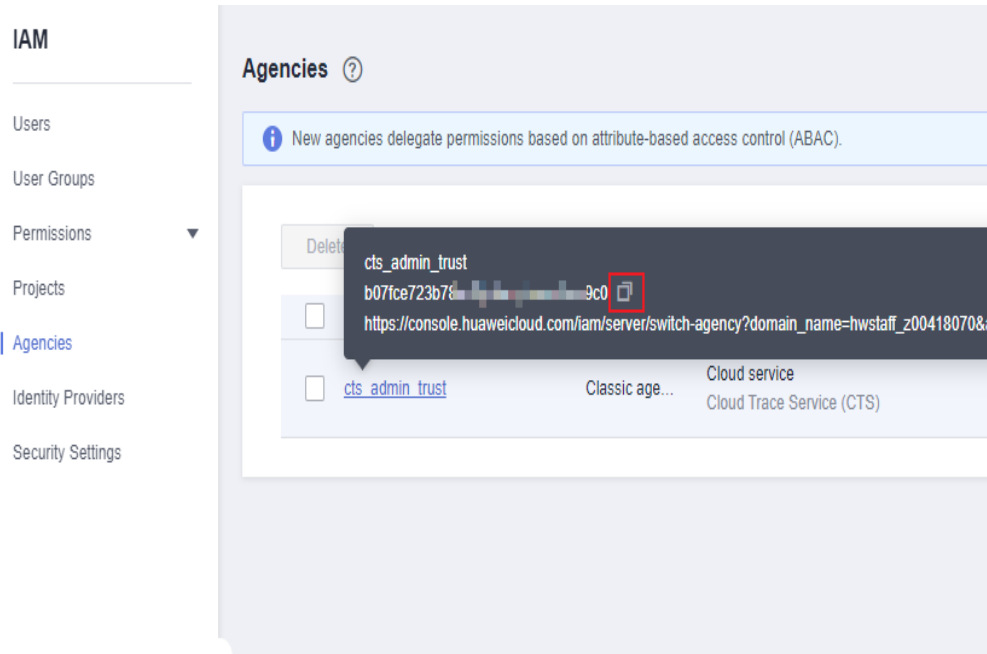
22 What Should I Do If I Fail to Transfer Data to an OBS Bucket Authorized by a Key of Another Tenant?

Background


Tenant A uses the key authorization mechanism of Data Encryption Workshop (DEW) to share a DEW key with user B of another tenant by user ID. User B has created an OBS bucket encrypted using the DEW key of tenant A. However, user B fails to configure the CTS system tracker to transfer data to this bucket.

Procedure

- Step 1** Log in to the management console of user B.
- Step 2** Click  in the upper left corner and choose **Management & Governance > Identity and Access Management**.
- Step 3** In the left navigation pane, choose **Agencies**. On the displayed page, enter `cts_admin_trust` in the search box to obtain the agency ID.



Step 4 Log in to the management console of tenant A.

Step 5 Click  in the upper left corner and choose **Security & Compliance > Data Encryption Workshop**.

Step 6 On the **Key Management Service** page, click the name of the target key.

Step 7 Click the **Grants** tab and click **Create Grant**. In the user ID text box, enter the agency ID of **cts_admin_trust** obtained in Step 3.

Create Grant



Key ID

★ User or Account User Account

A grantee is a cloud service user to whom you want to grant operation permissions associated with the key. You can obtain the user ID of the grantee from the page of My Credential by logging in to the management console with the grantee's username and password.

Name

Granted Operations Select all

<input type="checkbox"/> Create Data Key Without Plaintext	<input type="checkbox"/> Describe Key
<input type="checkbox"/> Create Data Key	<input type="checkbox"/> Create Grant
<input type="checkbox"/> Encrypt Data Key	<input type="checkbox"/> Decrypt Data Key
<input type="checkbox"/> Retire Grant	<input type="checkbox"/> Encrypt Data
<input type="checkbox"/> Decrypt Data	

Step 8 Log in to the management console of user B.

Step 9 Click in the upper left corner and choose **Management & Governance > Cloud Trace Service**.

Step 10 Go to the tracker transfer configuration page and select the OBS bucket encrypted with the DEW shared key.

----End

23 Does the `cts_admin_trust` Agency Include OBS Authorization?

Background

When I log in to IAM to view the authorization records of `cts_admin_trust`, I only see KMS and SMN authorizations. OBS authorization is not displayed.

Solution

OBS authorization is not displayed but actually included in the `cts_admin_trust` agency. You can use it.

The `cts_admin_trust` agency of IAM contains the following permissions:

- OBS Administrator
- KMS Administrator
- SMN Administrator

24 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 [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.



NOTE

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

----End