Cloud Trace Service

FAQs

Issue	01
Date	2025-11-14

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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 Product Consulting....................1

1.1 To Whom Is CTS Recommended?....................1

1.2 What Do I Do If I Cannot Enable CTS as an IAM User?....................1

1.3 Does the cts_admin_trust Agency Include OBS Authorization?....................2

1.4 Does CTS Support Integrity Verification of Trace Files?....................2

1.5 Can I Disable CTS?....................2

1.6 How Will CTS Be Affected If My Account Balance Is Insufficient?....................2

1.7 Why Are Two deleteMetadata Traces Generated When I Buy an ECS in Pay-per-Use or Yearly/Monthly?....................3

2 Traces....................4

2.1 What Do I Do If I Cannot Query Traces?....................4

2.2 Can I Receive Duplicate Traces?....................5

2.3 What Is the Information on a Trace List?....................5

2.4 How Do I Find Out the Login IP Address of an IAM User?....................5

2.5 Does CTS Record ECS Creation Failures?....................6

2.6 How Do I Find Out Who Created a Specific ECS?....................7

2.7 Why Is an Operation Recorded Twice in the Trace List?....................7

2.8 Why Are There Some Null Fields on the View Trace Page?....................8

2.9 Why Are user and source_ip Null for Some Traces with trace_type as SystemAction?....................8

3 Trackers....................9

3.1 What Do I Do If I Cannot Create a Tracker on the CTS Console?....................9

3.2 What Will Happen If I Have Enabled Trace Transfer But Have Not Configured an Appropriate Policy for an OBS Bucket?....................9

4 Trace Transfer....................10

4.1 How Do I Make the Log Retention Period 180 Days?....................10

4.2 What If I Fail to Transfer Data to an OBS Bucket Authorized with a Key of Another Tenant?....................12

4.3 How Can I Store Trace Files for a Long Time?....................13

4.4 Must I Use an OBS Bucket as an IAM User When Configuring Transfer on CTS as an IAM User?....................13

5 Key Event Notifications....................14

5.1 How Do I Enable Alarm Notifications for EVS?....................14

5.2 What Services Are Supported by Key Event Notifications?....................14

1 Product Consulting

1.1 To Whom Is CTS Recommended?

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.

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

Issue Description

If you fail to enable CTS as an Identity and Access Management (IAM) user, perform the following steps.

Procedure

Step 1 Check whether the IAM user has the required 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 required permission but cannot enable CTS, check whether CTS is enabled in the central region. If not, enable CTS in the central region using the Huawei Cloud account.

----End

1.3 Does the cts_admin_trust Agency Include OBS Authorization?

Issue Description

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**

1.4 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.

1.5 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:

- Delete or disable all trackers. Traces will still be reported after deletion.
- Delete the CTS agency in IAM. Traces will still be reported after deletion.

1.6 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 seven days. This is because records older than seven days will be transferred to OBS buckets in the form of trace files in real time, and storing these trace files in the OBS buckets incurs traffic charges.

When your account is in arrears, the only action you can perform on the CTS console is to delete trackers.

1.7 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.

2 Traces

2.1 What Do I Do If I Cannot Query Traces?

Issue Description

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, enable CTS and create a tracker named **system** in the central region EU-Dublin 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

2.2 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.

2.3 What Is the Information on a 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.

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

Issue Description

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

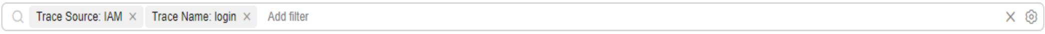
You have enabled CTS.

Procedure

Step 1 Log in to the CTS console.

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

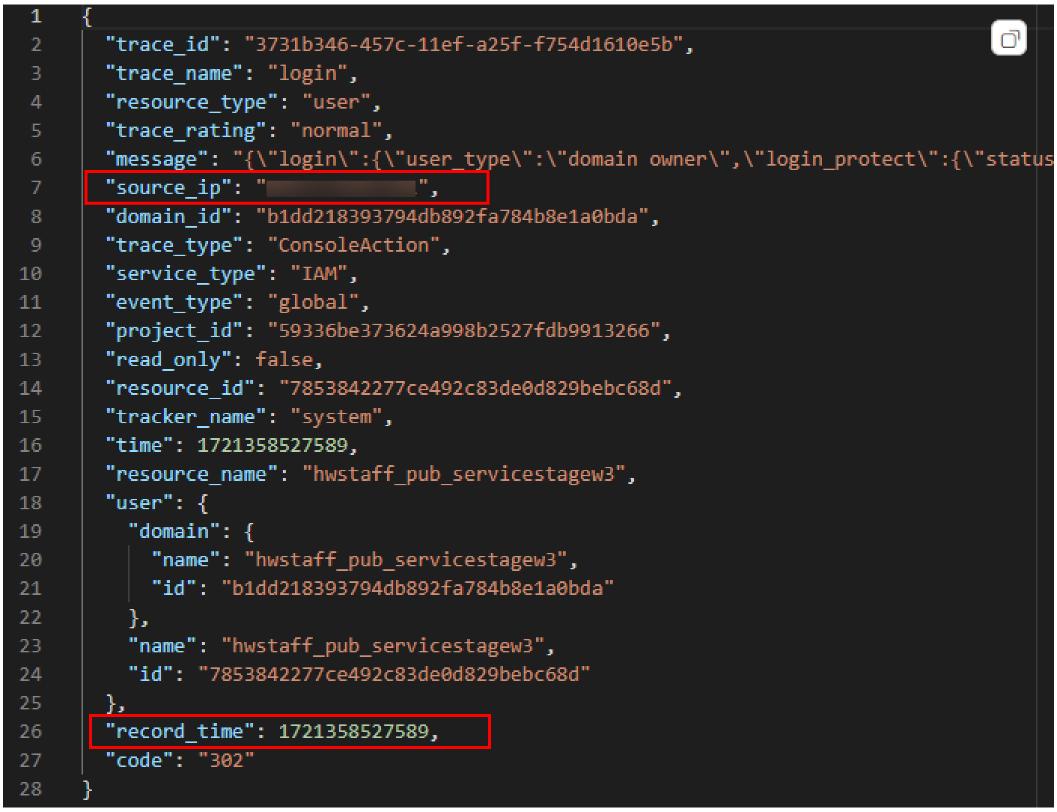
Select **Trace Source** and **IAM**. Select **Trace Name**, enter **login**, and press **Enter**.



Trace Source: IAM ×

Trace Name: login ×

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.



```
{
  "trace_id": "3731b346-457c-11ef-a25f-f754d1610e5b",
  "trace_name": "login",
  "resource_type": "user",
  "trace_rating": "normal",
  "message": "{\"login\":{\"user_type\":\"domain owner\",\"login_protect\":{\"status
  "source_ip": "[redacted]",
  "domain_id": "b1dd218393794db892fa784b8e1a0bda",
  "trace_type": "ConsoleAction",
  "service_type": "IAM",
  "event_type": "global",
  "project_id": "59336be373624a998b2527fdb9913266",
  "read_only": false,
  "resource_id": "7853842277ce492c83de0d829bebc68d",
  "tracker_name": "system",
  "time": 1721358527589,
  "resource_name": "hwstaff_pub_servicestagew3",
  "user": {
    "domain": {
      "name": "hwstaff_pub_servicestagew3",
      "id": "b1dd218393794db892fa784b8e1a0bda"
    },
    "name": "hwstaff_pub_servicestagew3",
    "id": "7853842277ce492c83de0d829bebc68d"
  },
  "record_time": 1721358527589,
  "code": "302"
}
```

----End

2.5 Does CTS Record ECS Creation Failures?

Yes. When you create an Elastic Cloud Server (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.

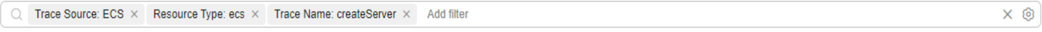
For details about the key ECS operations that can be recorded by CTS, see **Key Operations Supported by CTS**. When you add, delete, or modify an ECS, the ECS service automatically records your operations and results and then sends traces in the specified format to CTS for archiving. CTS stores traces 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.



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

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

Issue Description

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.

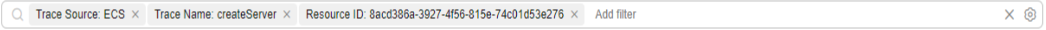
Procedure

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**.



Trace Source: ECS ×
Trace Name: createServer ×
Resource ID: 8acd386a-3927-4f56-815e-74c01d53e276 ×

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

2.7 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.

2.8 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.

2.9 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.

3 Trackers

3.1 What Do I Do If I Cannot Create a Tracker on the CTS Console?

Issue Description

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 EU-Dublin 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 technical support.

----End

3.2 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**.

4 Trace Transfer

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

Issue Description

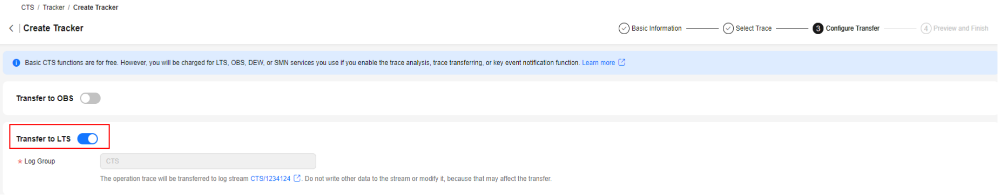
Audit logs may need to be stored for 180 days for query and backtracking. You can perform the following steps to configure the log retention period.

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 and stores CTS audit logs in the log stream for seven days by default. To store them for 180 days, change the log retention duration 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.
     - 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 4-1 Transfer to LTS



CTS / Tracker / Create Tracker

Create Tracker

Basic Information — Select Trace — 3 Configure Transfer — 4 Preview and Finish

Basic CTS functions are for free. However, you will be charged for LTS, OBS, DEW, or SMN services you use if you enable the trace analysis, trace transferring, or key event notification function. Learn more

Transfer to OBS

Transfer to LTS

* Log Group: CTS

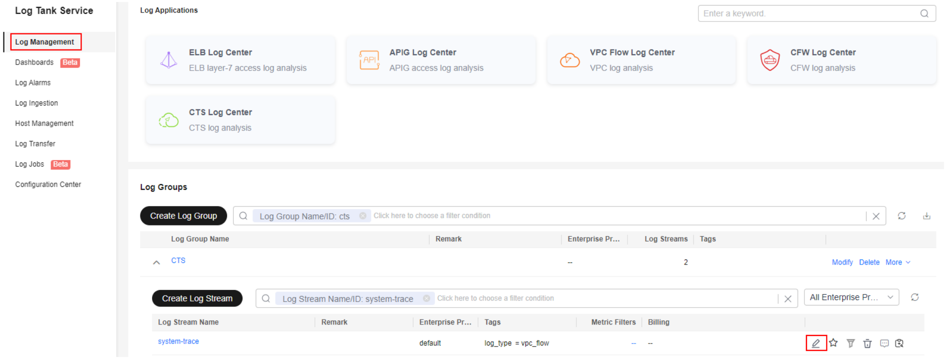
The operation trace will be transferred to log stream CTS/1234124. Do not write other data to the stream or modify it, because that may affect the transfer.

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 modify 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.

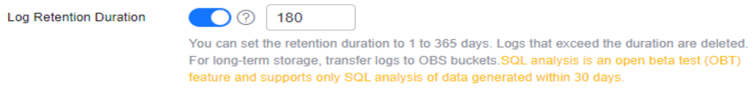
   Figure 4-2 Modifying the log stream

Log Group Name	Remark	Enterprise Pr...	Log Streams	Tags	
CTS		--	2		Modify Delete More

Log Stream Name	Remark	Enterprise Pr...	Tags	Metric Filters	Billing
system-trace		default	log_type = vpc_flow	--	--

   Figure 4-3 Changing the retention period

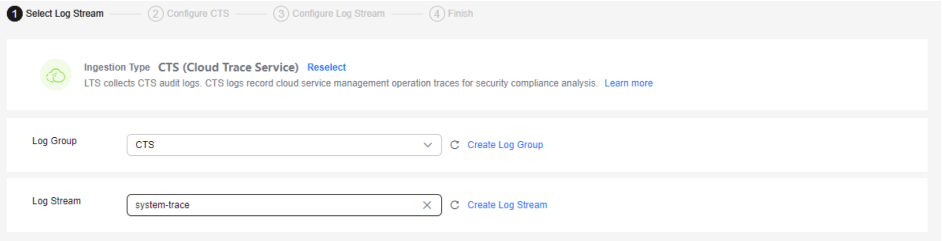
   

   Log Retention Duration 180

   You can set the retention duration to 1 to 365 days. Logs that exceed the duration are deleted. For long-term storage, transfer logs to OBS buckets.SQL analysis is an open beta test (OBT) feature and supports only SQL analysis of data generated within 30 days.

   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 4-4 Selecting a log stream

   1 Select Log Stream — 2 Configure CTS — 3 Configure Log Stream — 4 Finish

   Ingestion Type CTS (Cloud Trace Service) Reselect

   LTS collects CTS audit logs. CTS logs record cloud service management operation traces for security compliance analysis. Learn more

   Log Group: CTS — Create Log Group

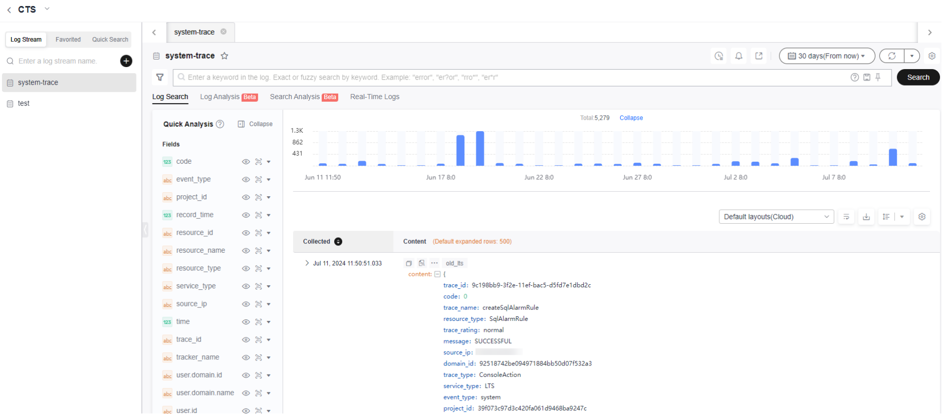
   Log Stream: system-trace — Create Log Stream

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 4-5 Log stream details



```
Jul 11, 2024 11:50:51.033    old_lts
content: {
    trace_id: 9c198bb9-3f2e-11ef-bac5-d5fd7e1dbd2c
    code: 0
    trace_name: createSqlAlarmRule
    resource_type: SqlAlarmRule
    trace_rating: normal
    message: SUCCESSFUL
    source_ip: [redacted]
    domain_id: 92518742be094971884bb50d07f532a3
    trace_type: ConsoleAction
    service_type: LTS
    event_type: system
    project_id: 39f073c97d3c420fa061d9468ba9247c
```

4.2 What If I Fail to Transfer Data to an OBS Bucket Authorized with a Key of Another Tenant?

Issue Description

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 as user B.

Step 2 Click ☰ in the upper left corner and choose **Management & Governance** > **Identity and Access Management**.

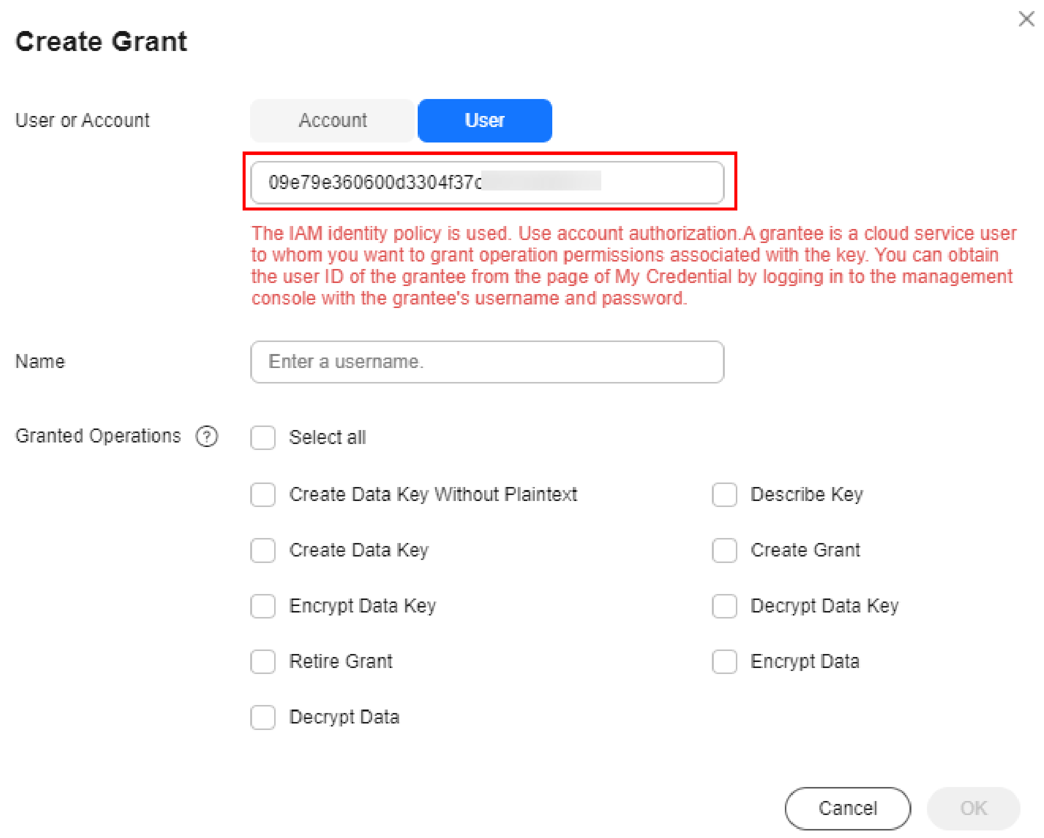
Step 3 In the navigation pane, choose **Agencies**. On the displayed page, enter **cts_admin_trust** in the search box to obtain the agency ID.

Step 4 Log in to the management console as 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

User or Account: Account | User

09e79e360600d3304f37c[redacted]

The IAM identity policy is used. Use account authorization.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: Enter a username.

Granted Operations ?

- □ Select all
- □ Create Data Key Without Plaintext
- □ Create Data Key
- □ Encrypt Data Key
- □ Retire Grant
- □ Decrypt Data
- □ Describe Key
- □ Create Grant
- □ Decrypt Data Key
- □ Encrypt Data

Step 8 Log in to the management console as 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

4.3 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**.

4.4 Must I Use an OBS Bucket as an IAM User When Configuring Transfer on CTS as an IAM User?

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

5 Key Event Notifications

5.1 How Do I Enable Alarm Notifications for EVS?

Issue Description

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

5.2 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, modification, login, and native OpenStack API calls.