Cloud Trace Service

Getting Started

Issue 01

Date 2024-11-22

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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 Viewing CTS Traces in the Trace List

Scenarios

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

NOTE

These operation records are retained for seven days on the CTS console and are automatically deleted upon expiration. Manual deletion is not supported.

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

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

Constraints

- Traces of a single account can be viewed on the CTS console. Multi-account traces can be viewed only on the **Trace List** page of each account, or in the OBS bucket or the **CTS/system** log stream configured for the management tracker with the organization function enabled.
- You can only query operation records of the last seven days on the CTS console. To store operation records for longer than seven days, you must configure transfer to OBS or Log Tank Service (LTS) so that you can view them in OBS buckets or LTS log groups.
- After performing operations on the cloud, you can query management traces on the CTS console one minute later and query data traces five minutes later.

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

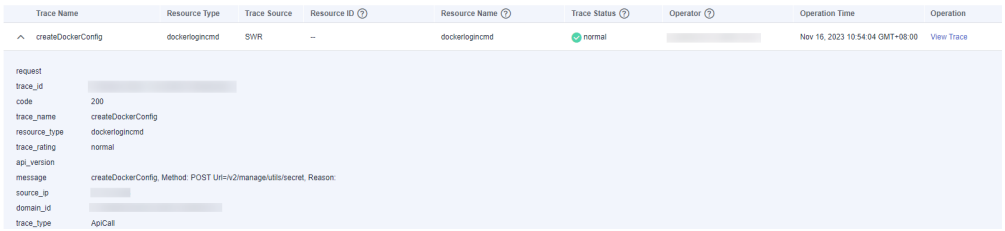
1. Log in to the management console.
2. Click  in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.

4. On the **Trace List** page, use advanced search to query traces. 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.
   - Time range: Select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range within the last seven days.
5. On the **Trace List** page, you can also export and refresh the trace list, and customize columns to display.
   - Enter any keyword in the search box and press **Enter** to filter desired traces.
   - Click **Export** to export all traces in the query result as an .xlsx file. The file can contain up to 5,000 records.
   - Click  to view the latest information about traces.
   - Click  to customize the information to be displayed in the trace list. If **Auto wrapping** is enabled (), excess text will move down to the next line; otherwise, the text will be truncated. By default, this function is disabled.
6. For details about key fields in the trace structure, see **Trace Structure** and **Example Traces**.
7. (Optional) On the **Trace List** page of the new edition, click **Go to Old Edition** in the upper right corner to switch to the **Trace List** page of the old edition.

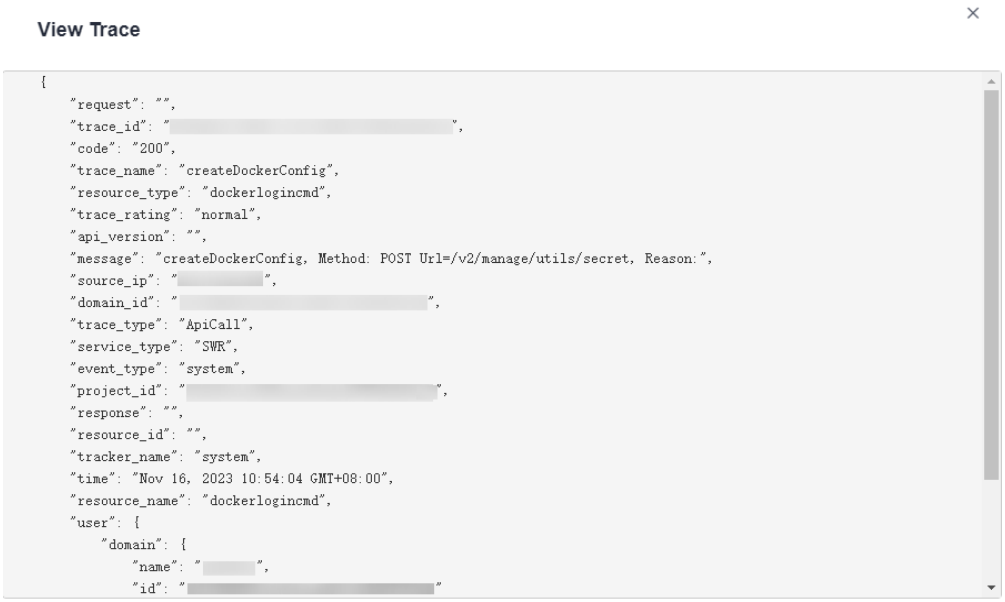
Viewing Real-Time Traces in the Trace List of the Old Edition

1. Log in to the management console.
2. Click  in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.

3. Choose **Trace List** in the navigation pane on the left.
4. Each time you log in to the CTS console, the new edition is displayed by default. Click **Go to Old Edition** in the upper right corner to switch to the trace list of the old edition.
5. 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: Select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range within the last seven days.
   - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5,000 records.
6. Click **Query**.
7. On the **Trace List** page, you can also export and refresh the trace list.
   - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5,000 records.
   - Click to view the latest information about traces.
8. Click on the left of a trace to expand its details.



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



10. For details about key fields in the trace structure, see **Trace Structure** and **Example Traces** in the *CTS User Guide*.
11. (Optional) On the **Trace List** page of the old edition, click **New Edition** in the upper right corner to switch to the **Trace List** page of the new edition.

2 Transferring CTS Traces to OBS and Viewing Them

CTS records details about operations performed by tenants, such as creating, modifying, and deleting cloud service resources, and retains these records as traces for seven days. To store traces for more than seven days, configure trace transfer to OBS. This allows CTS to periodically transfer trace files to OBS buckets for long-term storage.

This section describes how to configure the transfer and how to view historical traces in OBS buckets.

1. **Preparations**

   Before configuring OBS transfer, ensure that you have registered with Huawei Cloud, completed real-name authentication, topped up your account, and granted the necessary permissions to users.

2. **Configuring Trace Transfer to OBS**

   On the management tracker configuration page, enable **Transfer to OBS** so that trace files will be periodically transferred to an OBS bucket.

3. **Viewing Historical Traces in an OBS Bucket**

   You can download trace files from OBS buckets to view historical operation records.

Constraints

For global services, you must configure trackers on the CTS console in the central region (CN-Hong Kong). This configuration enables the function of transferring traces to OBS. The preceding function will not take effect if you perform the configuration on the CTS console in any region outside the central region.

For details about Huawei Cloud global services, see **Constraints**.

Preparations

1. **Register with Huawei Cloud and complete real-name authentication**.

   If you already have one, skip this step. If you do not have one, do as follows:

   a. Log in to the **Huawei Cloud official website**, and click **Register** in the upper right corner.

b. Complete the registration as prompted. For details, see **Registering with Huawei Cloud**.

Your personal information page is displayed after the registration completes.

c. Complete individual or enterprise real-name authentication by referring to **Real-Name Authentication**.

2. **Top up your account**.

Transferring traces to OBS will incur fees. Ensure that your account balance is sufficient.

- For details about OBS pricing, see **Object Storage Service Pricing Details**.
- For details about how to top up an account, see **Topping Up an Account**.

3. **Grant permissions for users**.

If you log in to the console using a Huawei Cloud account, skip this step.

If you log in to the console as an Identity and Access Management (IAM) user, first contact your CTS administrator (account owner or a user in the **admin** user group) to obtain the **CTS FullAccess** permissions. For details, see **Assigning Permissions to an IAM User**.

Configuring Trace Transfer to OBS

Step 1 Log in to the **CTS console**.

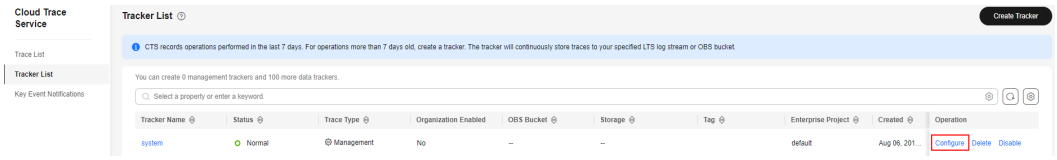
Step 2 Select a region closest to your application to reduce latency and accelerate access.

In this example, select **CN North-Beijing4**.

Step 3 In the navigation pane, choose **Tracker List**.

Step 4 Click **Configure** in the **Operation** column of the system tracker.

Figure 2-1 Configuring the system tracker



Step 5 On the **Basic Information** page, set parameters as follows and click **Next**.

Figure 2-2 Setting basic information

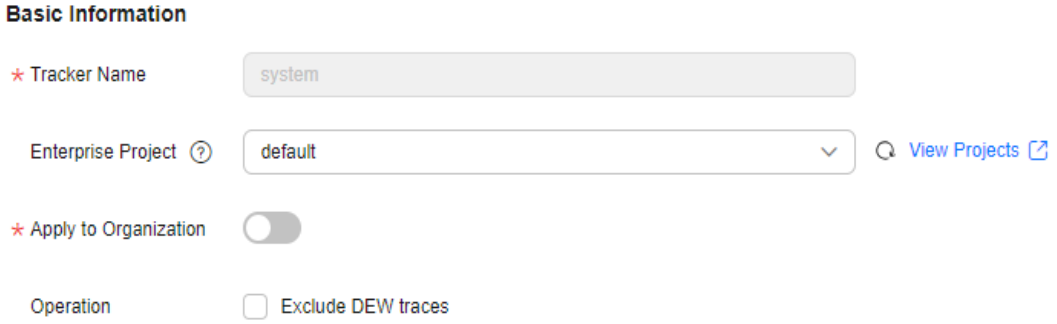


Table 2-1 Setting basic information

Parameter	Description	Example in This Case
Tracker Name	The name of a management tracker is **system** by default and cannot be changed.	system
Enterprise Project	Enterprise projects allow you to manage cloud resources and users by project. For details about how to enable them, see **Creating an Enterprise Project**. • If you have not enabled the enterprise project management service, skip this parameter. • If you have enabled the service, select **default** in this case.	default
Apply to Organization	CTS supports the multi-account management capability of Organizations. After you enable **Apply to Organization**, the following functions are available. For details, see **Organization Trackers**. 1. Use an organization administrator account to set CTS as a trusted service on the Organizations console and specify a delegated administrator account. 2. You can use the delegated administrator account to configure an organization tracker in CTS. Then the delegated administrator account can implement cloud audit capabilities, such as security audit.	Disable
Operation	If you select **Exclude KMS traces**, the tracker will not transfer the data about operations on Data Encryption Workshop (DEW). For details about DEW audit operations, see **Operations supported by CTS**.	Deselect

Step 6 On the **Configure Transfer** page, set parameters as follows and click **Next** > **Configure**. After the tracker is configured, the system starts recording operations based on the new rule.

Figure 2-3 Configuring transfer parameters

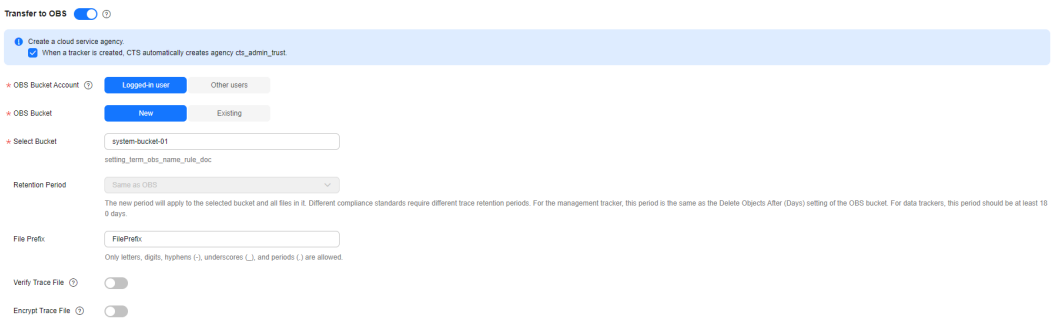


Table 2-2 Setting basic information

Parameter	Description	Example in This Case
Transfer to OBS	CTS records details about operations performed by tenants, such as creating, modifying, and deleting cloud service resources, and retains these records as traces for seven days. To store traces for more than seven days, configure trace transfer to OBS. This allows CTS to periodically transfer trace files to OBS buckets for long-term storage. After **Transfer to OBS** is enabled, trace files will be periodically transferred to OBS buckets.	Enable
Create a cloud service agency.	After enabling **Transfer to OBS**, you must select **Create a cloud service agency**. CTS will automatically create a cloud service agency named **cts_admin_trust** to authorize you to use OBS.	Select
OBS Bucket Account	You can transfer traces to OBS buckets of the logged-in user or 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 OBS bucket owner has granted you the transfer permission. Otherwise, the transfer will fail. For details about how to grant the transfer permission, see **Cross-Tenant Transfer Authorization**.	**Logged-in user**
OBS Bucket	You can create an OBS bucket or select an existing OBS bucket. If you select a region different from the region of the logged-in user, you can only select an existing OBS bucket. • **New**: An OBS bucket will be created automatically with the name you enter. • **Existing**: Select an existing OBS bucket.	**New**
Select Bucket	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.	system-bucket-01
Retention Period	Different compliance standards require different trace retention periods. When you configure a management tracker, **Same as OBS** is selected for **Retention Period** by default and cannot be modified.	**Same as OBS**

Parameter	Description	Example in This Case
File Prefix	A file prefix is used to mark transferred trace files. The prefix you set will be automatically added to the beginning of the file names, facilitating file filtering. Enter 0 to 64 characters. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed. A trace file name is in the following format: *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** Example: *File prefix*_**CloudTrace_region-project_2016-05-30T16-20-56Z_21d36ced8c8af71e.json.gz**	FilePrefix
Verify Trace File	To enable this function, toggle on **Verify Trace File**. Then CTS will generate a digest file for hash values of all trace files recorded in the past hour and synchronize the digest file to the Object Storage Service (OBS) bucket configured for the current tracker. You can implement your own verification solution with these files. For details about integrity verification, see **Verifying Trace File Integrity**. For more information about digest files, see **Digest Files**.	Disable
Encrypt Trace File	CTS supports trace file encryption. Trace files transferred to OBS buckets can be encrypted using keys provided by DEW. If you selected **Logged-in user** for **OBS Bucket Account** and enabled **Encrypt Trace File**, CTS obtains the key IDs of the logged-in user from DEW and displays them in the drop-down list for you to select.	Disable

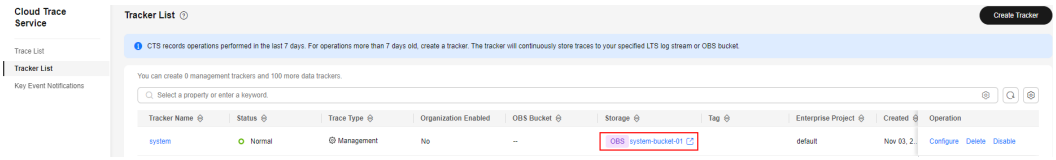
----End

Viewing Historical Traces in an OBS Bucket

After you configure the system tracker to transfer traces to an OBS bucket, the system will record operations based on the new rule and transfer historical trace files to the bucket for you to download and view.

Step 1 On the **Tracker List** page, the OBS bucket **system-bucket-01** that you set when configuring the transfer is displayed in the **Storage** column of the system tracker. Click the bucket name to go to the bucket's management page on the OBS console.

Figure 2-4 Clicking the OBS bucket name



Step 2 In the navigation pane, click **Objects**.

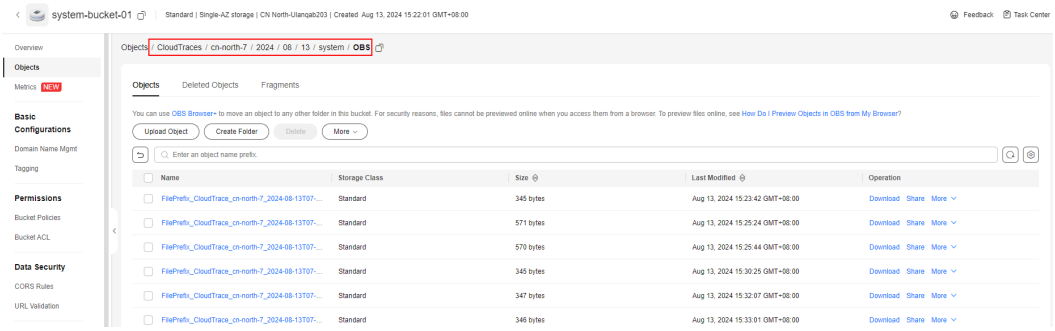
Step 3 On the **Objects** tab page, open the folders in sequence based on the trace file storage path.

In this case, click **CloudTraces** > **cn-north-4** > **2024** > *Month* > *Day* > **system** > **OBS**. *Month* and *Day* indicate the date when you create the OBS bucket **system-bucket-01**.

NOTE

Format of the trace file path: *OBS bucket name* > *CloudTraces* > *Region* > *Year* > *Month* > *Day* > *Tracker name* > *Service directory*

Figure 2-5 Trace file storage path



Step 4 In this case, find the file with the earliest last modification time and click **Download** on the right to download it to the default download path of the browser. To save it to a custom path, click **More** > **Download As** on the right.

NOTE

- Trace file name format: *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**

  Example: *File prefix*_**CloudTrace_cn-north-4_2024-08-13T07-23-42Z_eaac2d5c641fe022.json.gz**
- The OBS bucket name and trace file prefix are set by you and other parameters are automatically generated.
- File download will incur request fees and traffic fees.

Step 5 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 historical traces.

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

Figure 2-6 JSON file

----End

3 Transferring CTS Traces to LTS and Viewing Them

CTS records details of tenant operations, such as creating, modifying, and deleting cloud service resources, and stores these records as traces in the trace list for seven days. To store traces for more than seven days, configure trace transfer to LTS. This allows CTS to periodically transfer trace files to LTS log streams for long-term storage.

This section describes how to configure the transfer and how to view historical traces in OBS buckets.

1. **Preparations**

   Before configuring LTS transfer, ensure that you have registered with Huawei Cloud, completed real-name authentication, topped up your account, and granted the necessary permissions to users.

2. **Configuring Trace Transfer to LTS**

   On the management tracker configuration page, enable **Transfer to LTS** so that trace files will be periodically transferred to an LTS log stream.

3. **Viewing Historical Traces in an LTS Log Stream**

   You can view historical operation records in LTS log streams.

Constraints

For global services, you must configure trackers on the CTS console in the central region (CN-Hong Kong). This configuration enables the function of transferring traces to LTS. The preceding function will not take effect if you perform the configuration on the CTS console in any region outside the central region.

For details about Huawei Cloud global services, see **Constraints**.

Preparations

1. **Register with Huawei Cloud and complete real-name authentication**.

   If you already have one, skip this step. If you do not have one, do as follows:

   a. Log in to the **Huawei Cloud official website**, and click **Register** in the upper right corner.

b. Complete the registration as prompted. For details, see **Registering with Huawei Cloud**.

   Your personal information page is displayed after the registration completes.

c. Complete individual or enterprise real-name authentication by referring to **Real-Name Authentication**.

2. **Top up your account**.

   Transferring logs to LTS will incur fees. Ensure that your account balance is sufficient.

   - For details about LTS pricing, see **Log Tank Service Pricing Details**.
   - For details about how to top up an account, see **Topping Up an Account**.

3. **Grant permissions for users**.

   If you log in to the console using a Huawei Cloud account, skip this step.

   If you log in to the console as an Identity and Access Management (IAM) user, first contact your CTS administrator (account owner or a user in the **admin** user group) to obtain the **CTS FullAccess** permissions. For details, see **Assigning Permissions to an IAM User**.

4. **Configure CTS log ingestion on the LTS console**.

   If you transfer CTS logs to LTS for the first time, perform the following steps to configure CTS log ingestion:

   a. Log in to the **LTS console**.

   b. Choose **Log Ingestion** in the navigation pane. On the displayed page, click **CTS (Cloud Trace Service)**.

   c. On the displayed page, retain the default values for **Log Group** and **Log Stream**, and click **Next: Configure CTS** > **Next: Configure Log Stream** > **Submit**.

Configuring Trace Transfer to LTS

Step 1 Log in to the **CTS console**.

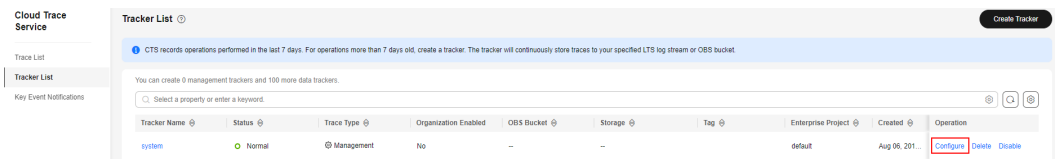
Step 2 Select a region closest to your application to reduce latency and accelerate access.

In this example, select **CN North-Beijing4**.

Step 3 In the navigation pane, choose **Tracker List**.

Step 4 Click **Configure** in the **Operation** column of the system tracker.

Figure 3-1 Configuring the system tracker



Step 5 On the **Basic Information** page, set parameters as follows and click **Next**.

Figure 3-2 Setting basic information

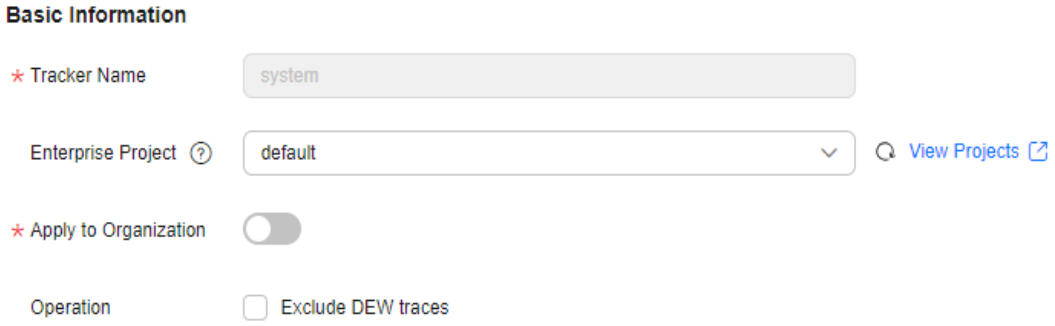


Table 3-1 Setting basic information

Parameter	Description	Example in This Case
Tracker Name	The name of a management tracker is **system** by default and cannot be changed.	system
Enterprise Project	Enterprise projects allow you to manage cloud resources and users by project. For details about how to enable them, see **Creating an Enterprise Project**. • If you have not enabled the enterprise project management service, skip this parameter. • If you have enabled the service, select **default** in this case.	default
Apply to Organization	CTS supports the multi-account management capability of Organizations. After you enable **Apply to Organization**, the following functions are available. For details, see **Organization Trackers**. 1. Use an organization administrator account to set CTS as a trusted service on the Organizations console and specify a delegated administrator account. 2. You can use the delegated administrator account to configure an organization tracker in CTS. Then the delegated administrator account can implement cloud audit capabilities, such as security audit.	Disable
Operation	If you select **Exclude KMS traces**, the tracker will not transfer the data about operations on Data Encryption Workshop (DEW). For details about DEW audit operations, see **Operations supported by CTS**.	Deselect

Step 6 On the **Configure Transfer** page, set parameters as follows and click **Next** > **Configure**. After the tracker is configured, the system starts recording operations based on the new rule.

Figure 3-3 Configuring transfer parameters

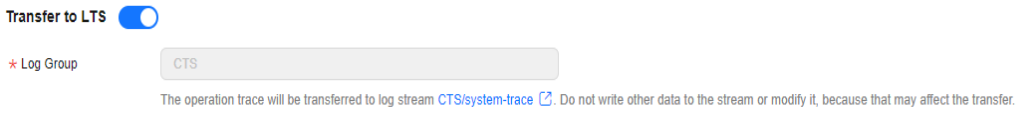


Table 3-2 Setting basic information

Parameter	Description	Example in This Case
Transfer to LTS	CTS records details of tenant operations, such as creating, modifying, and deleting cloud service resources, and stores these records as traces in the trace list for seven days. To store traces for more than seven days, configure trace transfer to LTS. This allows CTS to periodically transfer trace files to LTS log streams for long-term storage. To enable this function, toggle on **Transfer to LTS**.	Enable
Log Group	The default log group name is **CTS** and cannot be changed. Traces will be transferred to the **CTS/system-trace** log stream.	CTS

----End

Viewing Historical Traces in an LTS Log Stream

After you configure the system tracker to transfer traces to an LTS log stream, the system will record operations based on the new rule and transfer historical trace files to the stream for you to view.

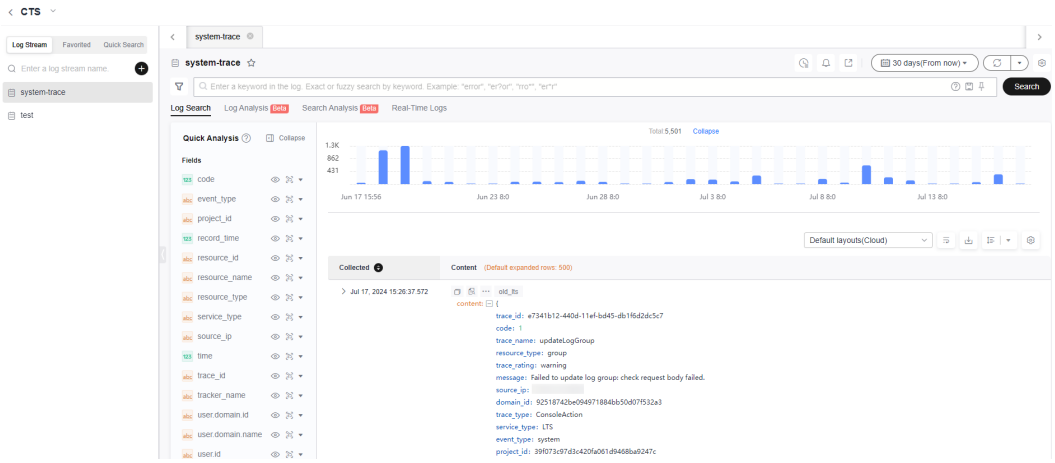
Step 1 On the **Tracker List** page, the log stream **CTS/system-trace** that you set when configuring the transfer is displayed in the **Storage** column of the system tracker. Click the stream name to go to the stream details page on the LTS console.

Figure 3-4 Clicking the log stream name

Step 2 On the page displayed, view historical logs.

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

Figure 3-5 system-trace log stream page



Step 3 Click to download the log file to your local PC.

NOTE

Each time you can download up to 5,000 log events. If you select over 5,000 log events, you need to transfer them to OBS and then download them from OBS.

----End

4 Common Practices

After completing basic operations such as viewing traces and configuring trackers, you can implement common practices based on this section.

Table 4-1 Common practices

Practice	Description
Auditing and Analyzing Logins and Logouts with FunctionGraph	This practice describes how to use CTS to collect real-time records of operations on cloud resources. Obtain operation records of subscribed cloud resources with a CTS trigger, analyze and process the records using a custom function, and report alarms. Then, use SMN to push alarm messages to service personnel by SMS or email.

