Cloud Trace Service

Getting Started

Issue	01
Date	2025-11-13

HUAWEI

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..... 1
2 Transferring CTS Traces to OBS and Viewing Them.....7
3 Transferring CTS Traces to LTS and Viewing Them.....14

1 Viewing CTS Traces in the Trace List

Scenarios

Cloud Trace Service (CTS) records operations performed on cloud service resources. A record contains information such as the user who performed the operation, IP address, operation content, and returned response message. These records facilitate security auditing, issue tracking, and resource locating. They also help you plan and use resources, and identify high-risk or non-compliant operations.

What Is a Trace?

A trace is an operation log for a cloud service resource, tracked and stored by CTS. Traces record operations such as adding, modifying, or deleting cloud service resources. You can view them to identify who performed operations and when for detailed tracking.

What Is a Management Tracker and Data Tracker?

A management tracker identifies and associates with all your cloud services, recording all user operations. It records management traces, which are operations performed by users on cloud service resources, such as their creation, modification, and deletion.

A data tracker records details of user operations on data in OBS buckets. It records data traces reported by OBS, detailing user operations on data in OBS buckets, including uploads and downloads.

Constraints

- Before the organization function is enabled, you can query the traces of a single account on the CTS console. After the organization function is enabled, you can only view multi-account traces 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. They are automatically deleted upon expiration and cannot be manually deleted. To store them for longer than seven days, configure transfer to Object Storage Service (OBS) or Log Tank Service (LTS) so that you can view them in OBS buckets or LTS log groups.

- After creating, modifying, or deleting a cloud service resource, you can query management traces on the CTS console 1 minute later and query data traces 5 minutes later.
- Data traces are not displayed in the trace list of the new version. To view them, you need to go to the old version.

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

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

Step 2 In the navigation pane, choose **Trace List**.

Step 3 In the time range drop-down list above the trace list, select a desired query time range: **Last 1 hour**, **Last 1 day**, or **Last 1 week**. You can also select **Custom** to specify a custom time range within the last seven days.

Step 4 The search box above the trace list supports advanced queries. Combine one or more filters to refine your search.

Table 1-1 Trace filtering parameters

Parameter	Description
Trace Name	Name of a trace. The entered value is case-sensitive and requires an exact match. Fuzzy matching is not supported. For details about the operations that can be audited for each cloud service, see **Supported Services and Operations**. Example: **updateAlarm**
Trace Source	Cloud service name abbreviation. The entered value is case-sensitive and requires an exact match. Fuzzy matching is not supported. Example: **IAM**
Resource Name	Name of a cloud resource involved in a trace. The entered value is case-sensitive and requires an exact match. Fuzzy matching is not supported. 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. Example: **ecs-name**
Resource ID	ID of a cloud resource involved in a trace. The entered value is case-sensitive and requires an exact match. Fuzzy matching is not supported. Leave this field empty if the resource has no resource ID or if resource creation failed. Example: *{VM ID}*

Parameter	Description
Trace ID	Value of the **trace_id** parameter for a trace reported to CTS. The entered value requires an exact match. Fuzzy matching is not supported. Example: **01d18a1b-56ee-11f0-ac81-******1e229**
Resource Type	Type of a resource involved in a trace. The entered value is case-sensitive and requires an exact match. Fuzzy matching is not supported. For details about the resource types of each cloud service, see **Supported Services and Operations**. Example: **user**
Operator	User who triggers a trace. Select one or more operators from the drop-down list. If the value of **trace_type** in a trace is **SystemAction**, the operation is triggered by the service and the trace's operator may be empty.
Trace Status	Select one of the following options from the drop-down list: • **normal**: The operation succeeded. • **warning**: The operation failed. • **incident**: The operation caused a fault that is more serious than a normal failure, for example, causing other faults.
Enterprise Project ID	ID of the enterprise project to which a resource belongs. To check enterprise project IDs, go to the Enterprise Project Management Service (EPS) console and choose **Project Management** in the navigation pane. Example: **b305ea24-c930-4922-b4b9-******1eb2**
Access Key	Temporary or permanent access key ID. To check access key IDs, hover over your username in the upper right corner of the console and select **My Credentials** from the pop-up list. On the displayed page, choose **Access Keys** in the navigation pane. Example: **HSTAB47V9V*******TLN9**

Step 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.

Step 6 (Optional) On the **Trace List** page of the new edition, click **Old Edition** in the upper right corner to switch to the **Trace List** page of the old edition.

----End

Viewing Traces in the Trace List of the Old Edition

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

Step 2 In the navigation pane, choose **Trace List**.

Step 3 Each time you log in to the CTS console, the new edition is displayed by default. Click **Old Edition** in the upper right corner to switch to the trace list of the old edition.

Step 4 In the upper right corner of the page, set a desired query time range: **Last 1 hour**, **Last 1 day**, or **Last 1 week**. You can also click **Customize** to specify a custom time range within the last seven days.

Step 5 Set filters to search for your desired traces.

Table 1-2 Trace filtering parameters

Parameter	Description
Trace Type	Select **Management** or **Data**. • Management traces record operations performed by users on cloud service resources, including creation, modification, and deletion. • Data traces are reported by OBS and record operations performed on data in OBS buckets, including uploads and downloads.
Trace Source	Select the name of the cloud service that triggers a trace from the drop-down list.
Resource type	Select the type of the resource involved in a trace from the drop-down list. For details about the resource types of each cloud service, see **Supported Services and Operations**.
Operator	User who triggers a trace. Select one or more operators from the drop-down list. If the value of **trace_type** in a trace is **SystemAction**, the operation is triggered by the service and the trace's operator may be empty.

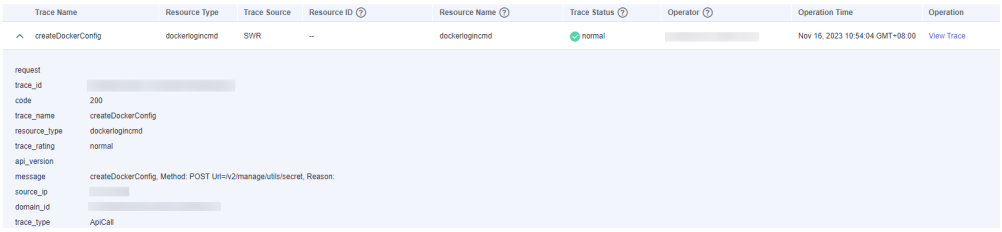
Parameter	Description
Trace Status	Select one of the following options: • **Normal**: The operation succeeded. • **Warning**: The operation failed. • **Incident**: The operation caused a fault that is more serious than a normal failure, for example, causing other faults.

Step 6 Click **Query**.

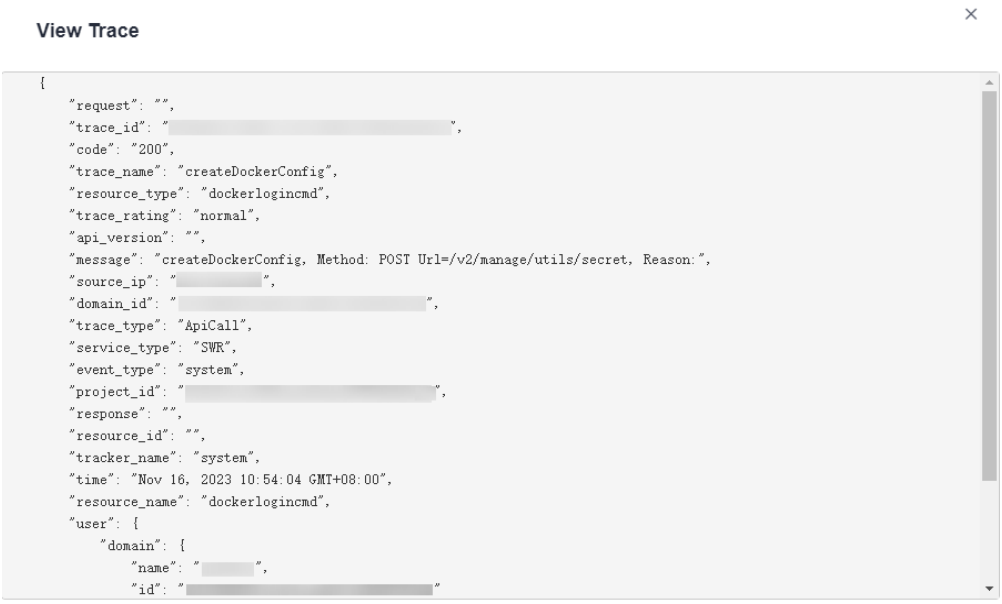
Step 7 On the **Trace List** page, you can also export and refresh the trace list.

- 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.

Step 8 Click on the left of a trace to expand its details.



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



Step 10 (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.

----End

Helpful Links

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

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, you should 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**

   Download trace files from the OBS bucket to view historical operation records.

Constraints

- **Global services can transfer traces to OBS only if you configure a tracker on the CTS console in the central region (EU-Dublin). If you configure a tracker on the CTS console in other regions, this function does not take effect. For details about Huawei Cloud global services, see Constraints.**
- If you have not configured transfer, the CTS console retains operation logs for seven days. After this period, the logs are automatically deleted and cannot be viewed, even if you configure transfer later.

Preparations

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

   If you already have a Huawei Cloud account, skip this step. If you do not have one, do as follows:

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

b. Complete the registration as prompted. For details, see **Signing Up for a HUAWEI ID and Enabling Huawei Cloud Services**.

   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**.

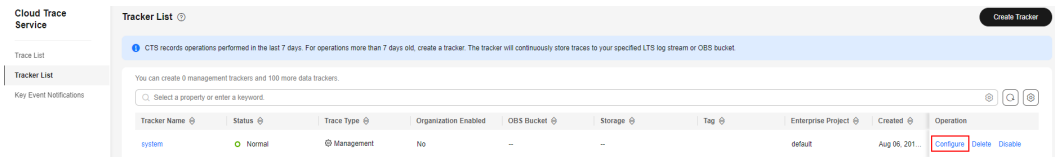
Step 2 Select a region closest to your application to reduce latency and accelerate access.

In this practice, select **EU-Dublin**.

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

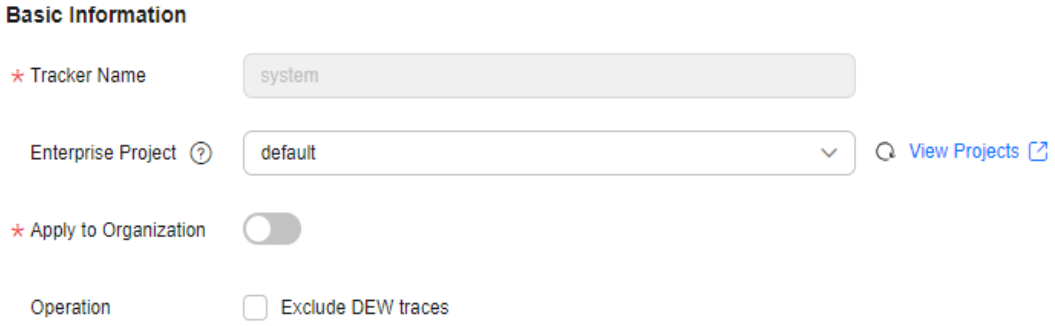


Table 2-1 Setting basic information

Parameter	Description	Example in This Practice
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 practice.	default
Apply to Organization	CTS supports the multi-account management capability of Organizations. After you enable **Apply to Organization**, the following functions are available. 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 DEW 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 **Exclude DEW traces**

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

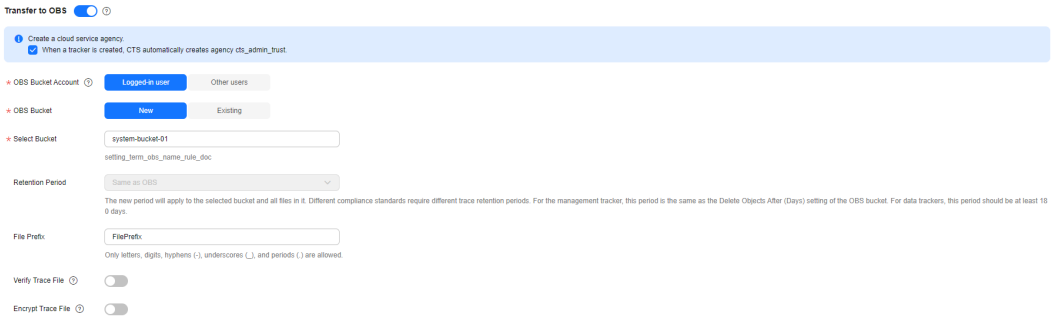


Table 2-2 Setting basic information

Parameter	Description	Example in This Practice
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, audit logs 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 **Create a cloud service agency.**
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**.	Select **Logged-in user**

Parameter	Description	Example in This Practice
OBS Bucket	You can create an OBS bucket or select an existing one. • **New**: An OBS bucket will be created automatically with the name you enter. **NOTE** A single-AZ private bucket with Standard storage will be created. If you need other configurations, create the bucket on OBS Console in advance and choose **Existing** to select it. • **Existing**: Select an existing OBS bucket in the current region.	Select **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.	Select **Same as OBS**
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*_*Year-Month-Day*T*Hour-Minute-Second*Z_*Random characters*.**json.gz** (*Year-Month-Day*T*Hour-Minute-Second* indicates the time when the trace file was uploaded to OBS.) Example: **FilePrefix_CloudTrace**_*region*_**2024-12-13T01-29-19Z_47b9d51830deff47.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

Parameter	Description	Example in This Practice
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

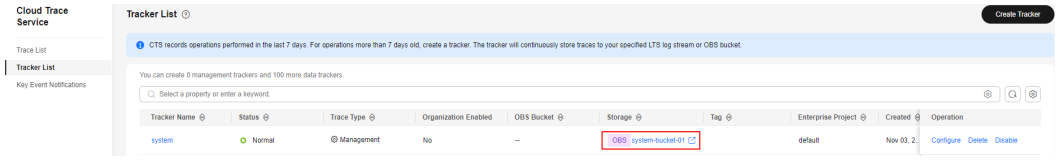
----End

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 trace files to the bucket. Then, you can download the trace files from the bucket to 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 of the management page, click **Objects**.

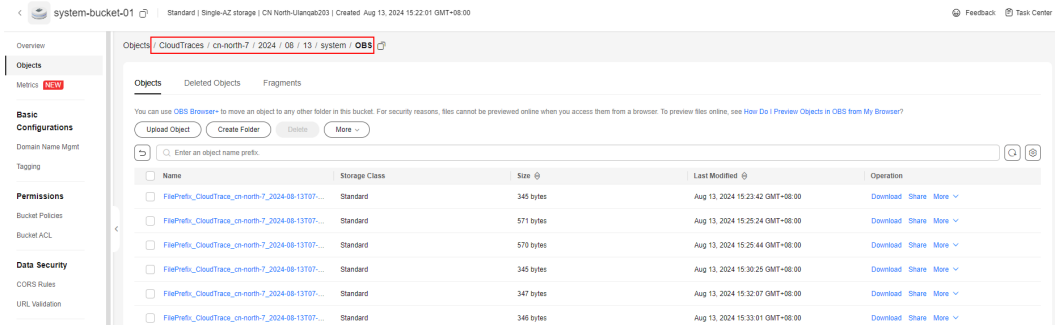
Step 3 On the **Objects** tab page, open the folders in sequence based on the trace file storage path.

In this practice, click **CloudTraces** > **eu-west-101** > **2024** > *Month* > *Day* > **system** > **OBS**. *Month* and *Day* indicate the date when you created the OBS bucket **system-bucket-01**.

NOTE

Trace file path format: *OBS bucket name*/**CloudTraces**/*Region*/*Year*/*Month*/*Day*/*Tracker name*/*Cloud service*

Figure 2-5 Trace file storage path



Step 4 In this practice, find the file with the earliest last modification time and click **Download** on the right to download it to the default download path of your 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*_*Year-Month-Day***T***Hour-Minute-Second***Z**_*Random characters*.**json.gz** (*Year-Month-Day***T***Hour-Minute-Second* indicates the time when the trace file was uploaded to OBS.)
- 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 view historical traces in LTS log streams.

1. **Preparations**

   Before configuring LTS transfer, you should 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.

Preparations

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

   If you already have a Huawei Cloud account, skip this step. If you do not have one, do as follows:

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

   b. Complete the registration as prompted. For details, see **Signing Up for a HUAWEI ID and Enabling Huawei Cloud Services**.

      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 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** > **Ingestion Center** in the navigation pane and 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**.

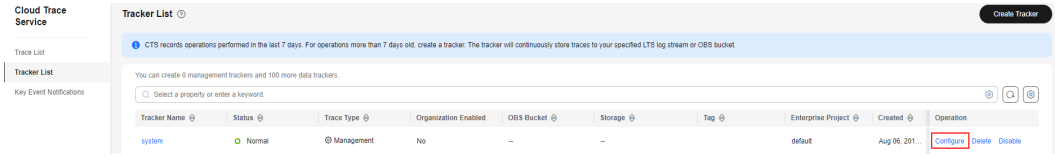
Step 2 Select a region closest to your application to reduce latency and accelerate access.

In this practice, select **EU-Dublin**.

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

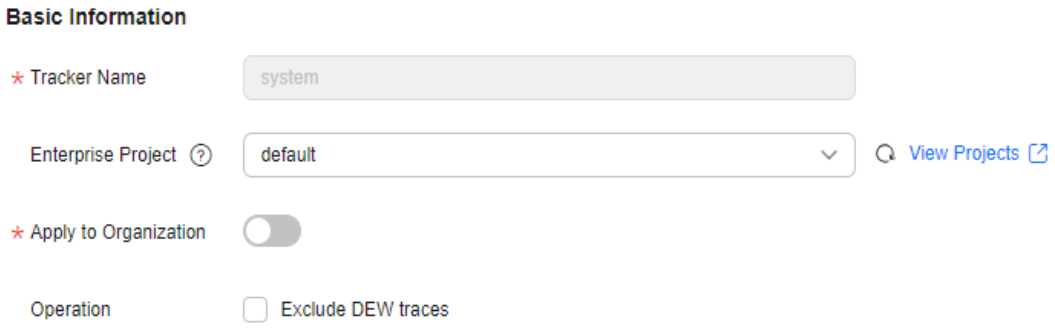


Table 3-1 Setting basic information

Parameter	Description	Example in This Practice
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 practice.	default
Apply to Organization	CTS supports the multi-account management capability of Organizations. After you enable **Apply to Organization**, the following functions are available. 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 DEW 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 **Exclude DEW traces**

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

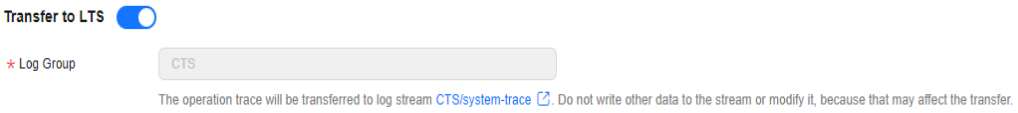


Table 3-2 Setting basic information

Parameter	Description	Example in This Practice
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. After **Transfer to LTS** is enabled, audit logs will be periodically transferred to LTS log streams.	Enable
Log Group	The log group name defaults to **CTS** and cannot be changed. Traces will be transferred to log stream **CTS/system-trace**.	CTS

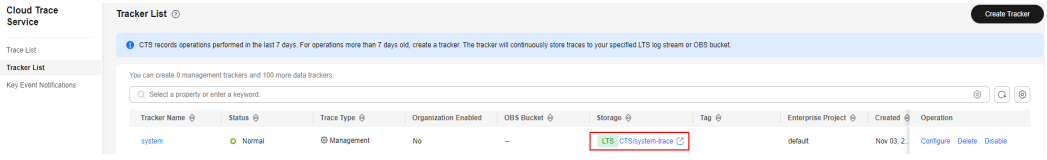
----End

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 trace files to the log stream. Then, you can view the trace files in the log stream.

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.

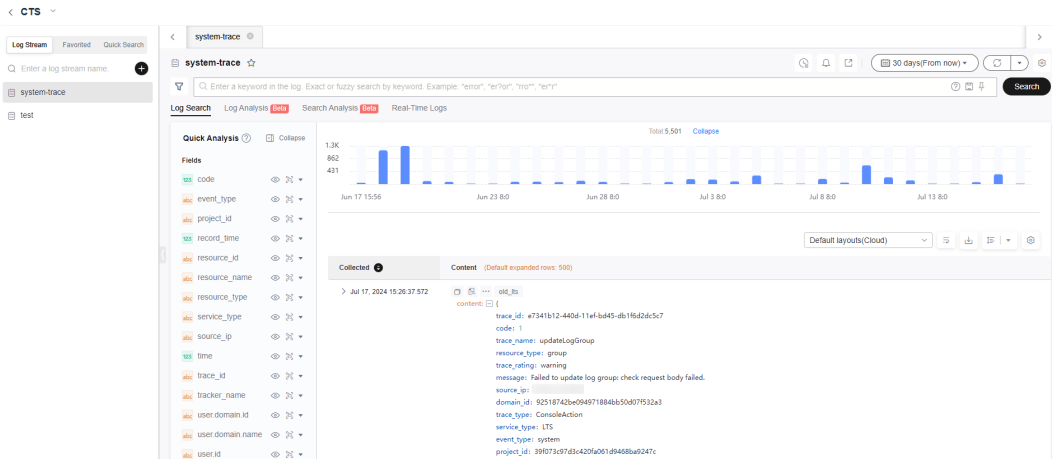
Figure 3-4 Clicking the log stream name



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.

----End

