Cloud Trace Service

User Guide

Issue	01
Date	2020-09-29

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Contents

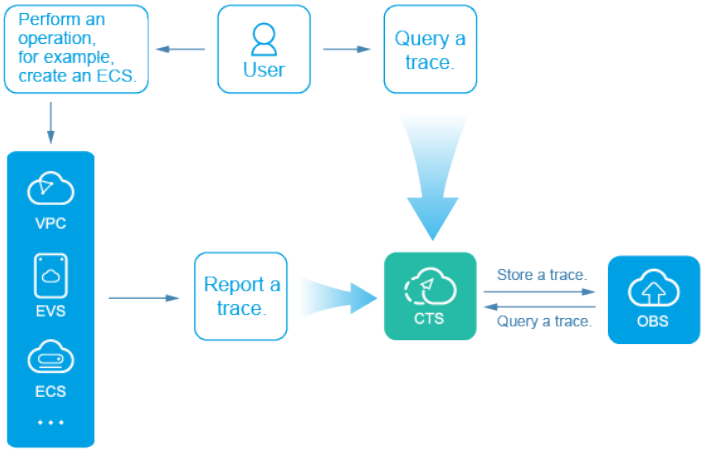
1 Overview

1.1 What Is Cloud Trace Service?

The log audit module is a core component necessary for information security audit and an important information system providing security risk management and control for enterprises and public institutions. As the information system is migrating to the cloud, information and data security management departments around the world have released multiple standards, such as ISO IEC27000, GB/T 20945-2013, COSO, COBIT, ITIL, and NISTSP800.

Cloud Trace Service (CTS) is a log audit service that is available for cloud security. It allows you to collect, store, and query resource operation records. You can use these records to perform security analysis, track resource changes, audit compliance, and locate faults.

Figure 1-1 CTS service diagram



CTS provides the following functions:

- Trace recording: CTS records operations performed on the management console or by calling APIs, as well as operations triggered by each interconnected service.
- Trace query: Operation records of the last seven days can be queried on the management console from multiple dimensions, such as the trace source, trace name, operation type, resource name, resource ID, and time.
- Trace dumping: Traces are delivered to Object Storage Service (OBS) buckets on a regular basis for long-term storage. In this process, traces are compressed into trace files by service.

1.2 Basic Concepts

Trackers

Before using CTS, you need to enable the CTS service. A tracker is automatically created when you enable CTS. This tracker automatically identifies and associates with all cloud services enabled by the current tenant, and records all operations by the tenant.

Currently, only one tracker can be created for each user.

Traces

Traces are operation logs of cloud service resources and are captured and stored by CTS. You can view the traces to get to know details of operations performed on specific resources.

There are two types of traces:

- Real-time traces

  Operation records generated during the last seven days

- Archived traces

  Historical operation records that have been stored in an OBS bucket

Trace Lists

The trace list displays details about the operations that you have performed, such as creating, modifying, or deleting cloud service resources. It contains all of the traces that were generated during the last seven days.

Trace Files

A trace file is a collection of traces. CTS automatically generates multiple trace files by service and dump interval and then synchronizes these files to the OBS bucket that you have specified.

Generally, all traces of a service generated during a dump interval are compressed into one trace file. However, if there are a large number of traces, the system will adjust the number of traces contained in each trace file as needed.

Traces files are in JSON format. **Figure 1-2** shows an example of a trace file.

Figure 1-2 Trace file example


```
[{
    "time": 1491482532828,
    "user": {
        "id": "59f40829165447fb9470b56f41dff599",
        "name": "[redacted]",
        "domain": {
            "name": "[redacted]",
            "id": "0f27bc42d1eb46a69482a72cbfc33ed2"
        }
    },
    "request": {
        "bucket_name": "obs-570f",
        "file_prefix_name": "-RsU",
        "status": "disabled"
    },
    "response": {
        "bucket_name": "obs-570f",
        "file_prefix_name": "-RsU",
        "status": "disabled",
        "tracker_name": "system"
    },
    "service_type": "CTS",
    "resource_type": "tracker",
    "resource_name": "system",
    "source_ip": "[redacted]",
    "trace_name": "updateTracker",
    "trace_type": "ConsoleAction",
    "api_version": "1.0",
    "record_time": 1491482532857,
    "trace_id": "7519ef09-1ac6-11e7-8cc0-3d812829baf6",
    "trace_status": "normal"
},
{
    "time": 1491482535203,
    "user": {
        "id": "59f40829165447fb9470b56f41dff599",
        "name": "[redacted]",
        "domain": {
            "name": "[redacted]",
            "id": "0f27bc42d1eb46a69482a72cbfc33ed2"
        }
    },
    "request": {
        "bucket_name": "obs-570f",
        "file_prefix_name": "-RsU",
        "status": "enabled"
    },
    "response": {
        "bucket_name": "obs-570f",
        "file_prefix_name": "-RsU",
        "status": "enabled",
        "tracker_name": "system"
    },
    "service_type": "CTS",
    "resource_type": "tracker",
    "resource_name": "system",
    "source_ip": "[redacted]",
    "trace_name": "updateTracker",
    "trace_type": "ConsoleAction",
    "api_version": "1.0",
    "record_time": 1491482535224,
    "trace_id": "76831bfb-1ac6-11e7-98ff-a1036f244dcd",
    "trace_status": "normal"
}]
```


For details about how to obtain trace files, see **Querying Archived Traces**. For details about key fields in the structure of a trace, see **Trace Structure**.

1.3 How CTS Functions

CTS interconnects directly with other cloud services and records operations performed on cloud resources and operation results in real time. It delivers records in the form of trace files to OBS buckets.

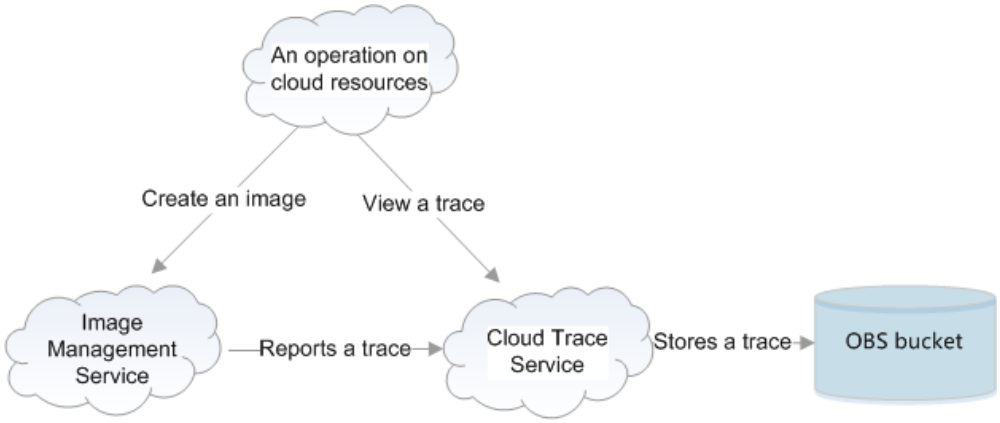
Before enabling CTS, you need to enable OBS. After CTS is enabled, the associated tracker can track the trace files generated and store them in OBS buckets.

You can perform two types of operations on a trace file:

- Trace file creation and storage
  - When you perform adding, deleting, or modifying operations on services interconnected with CTS, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), and Image Management Service (IMS), the target services will record the operations and their results automatically and deliver them in the form of traces to CTS for archiving.
  - CTS stores and displays the last seven days of operation records on its console and periodically synchronizes the records to the OBS bucket that you have specified for long-term storage.
- Trace file query
  - You can query operation records of the last seven days on the **Trace List** page by filter or time.
  - To query operation records earlier than seven days, you can download the trace files stored in OBS buckets.
  - You can enable, disable or delete a tracker on the **Tracker** page.

  For example, if you create an image using the IMS service, the service will report the creation operation to CTS. Then, CTS will deliver the trace to an OBS bucket for storage. You can view trace files in the trace list. **Figure 1-3** shows the working principle of CTS.

Figure 1-3 How CTS functions



1.4 Application Scenarios

CTS is mainly used in the following scenarios:

- **Compliance audit**

  CTS allows you to query all operation records of security control. This is essential for enterprises and organizations, especially financial and payment enterprises, to obtain the certification, such as PCI DSS, GB/T 24589.1, and COSO.

- **Resource tracking**

  With CTS, you can search for traces by resource and track operations and changes of any cloud resource throughout its lifecycle, as well as the source and result of each operation or change, to better use resources.

- **Fault locating**

  When a cloud resource becomes faulty, you can use traces generated by CTS to quickly find out the suspicious operation causing the fault and its result, greatly reducing the time and labor costs on fault locating and rectifying.

- **Security analysis**

  Enterprises and public institutions can specify the scope of risky operations or key operations based on their requirements, and periodically view the operator, time and IP address of each operation request to which attention must be paid for security analysis.

1.5 Supported Services

Once you enable CTS, the system automatically identifies cloud services enabled on the current cloud platform, captures key operations on the services, and reports traces of these operations to CTS.

Traces of global-level cloud services are only recorded at the central region of the current site. Multi-project scenarios are not supported.

The key operations of global-level services supported by CTS are as follows:

- **Global-level Key Operations on DNS**
- **Key Operations on IAM**
- **Key Operations on TMS**

Traces of region-level cloud services are recorded in the target region or project to which the operated resources belong.

For key operations of region-level services supported by CTS, see **Supported Services and Operation Lists**.

1.6 How to Access CTS

You can access CTS using a web-based service management console. If you have registered on the public cloud platform, log in to the management console, and choose **Management & Deployment** > **Cloud Trace Service**.

2 Getting Started

2.1 Enabling CTS

Scenarios

You need to enable CTS before using it. A tracker will be automatically created after CTS is enabled. All traces recorded by CTS are associated with the tracker.

Trace files need to be stored in OBS buckets. Therefore, before enabling CTS, you need to enable OBS and have full permissions on the OBS bucket to be used. By default, only the service owner who has enabled OBS can access OBS buckets and all objects contained, and the owner can grant permissions to other services and users by configuring an access policy.

This section describes how to enable CTS.

Prerequisites

You have enabled OBS.

2.2 Querying Real-Time Traces

Scenarios

After CTS is enabled, the tracker starts recording operations on cloud resources. The CTS management console stores the last seven days of operation records.

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

Procedure

1. Log in to the management console.
2. Click in the upper left corner to select the desired region and project.
3. Click **Service List** and choose **Management & Deployment** > **Cloud Trace Service**.
4. In the left navigation pane, choose **Trace List**.
5. Click **Filter** and specify filters as needed. You can query traces by combining the following filters:
   - **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**.

     Select a filter from the drop-down list.

     When you select **Resource ID** for **Search By**, you also need to select or enter a resource ID.
   - **Operator**: Select a specific operator.
   - **Trace Status**: Select one of **All trace statuses**, **normal**, **warning**, and **incident**.
   - **Time Range**: In the upper right corner of the page, you can query traces in the last 1 hour, last 1 day, last 1 week, or within a customized period.
6. Click on the left of the required trace to expand its details.
7. Click **View Trace** in the Operation column. On the displayed **View Trace** dialog box, the trace structure details are displayed.

Figure 2-1 Viewing traces

View Trace


```
{
    "trace_id": "df201462-8373-11e9-a4db-c3ac3c023b88",
    "code": "302",
    "trace_name": "logout",
    "resource_type": "user",
    "trace_rating": "normal",
    "source_ip": "-",
    "service_type": "IAM",
    "trace_type": "SystemAction",
    "event_type": "system",
    "resource_id": "f3f18b9215014f0d9ded3045af020811",
    "tracker_name": "system",
    "time": "May 31, 2019 15:15:29 GMT+08:00",
    "resource_name": "[redacted]",
    "record_time": "May 31, 2019 15:15:29 GMT+08:00",
    "user": {
        "name": "[redacted]",
        "id": "f3f18b9215014f0d9ded3045af020811",
        "domain": {
            "name": "[redacted]",
            "id": "2306579dc99f4c8690b14b68e734fcd9"
        }
    }
}
```


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

2.3 Querying Archived Traces

Scenarios

CTS periodically compresses the recorded traces into trace files and delivers them to OBS buckets. Trace files are collections of traces that CTS automatically generates by service and dump interval. CTS adjusts the number of traces contained in a trace file as the service load changes.

This section describes how to obtain historical operation records from trace files downloaded from the OBS bucket.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner to select the desired region and project.
3. Click **Service List** and choose **Management & Deployment** > **Cloud Trace Service**.
4. Click **Tracker** in the left pane.
5. Click the specified bucket in the **OBS Bucket** column.
6. Select the target trace. Choose *OBS bucket name* > **CloudTraces** > *Region* > *Year* > *Month* > *Day* > *Tracker name* > *Service type directory*. Click **Download** in the **Operation** column to download the trace file to the default path. To download the trace file to a customized path, click **More** > **Download As**.
   - The trace file storage path is as follows:

     OBS bucket name > **CloudTraces** > *Region* > *Year* > *Month* > *Day* > *Tracker name* > *Service type directory*

     An example is *User Define>CloudTraces>region>2016>5>19>system>ECS*.
   - The trace file naming format is as follows:

     *Operation trace file prefix*_CloudTrace_*Region_/Region-projectTime when the log was uploaded to OBS: year-month-day*T*hour-minute-second*Z*_Character randomly generated*.json.gz

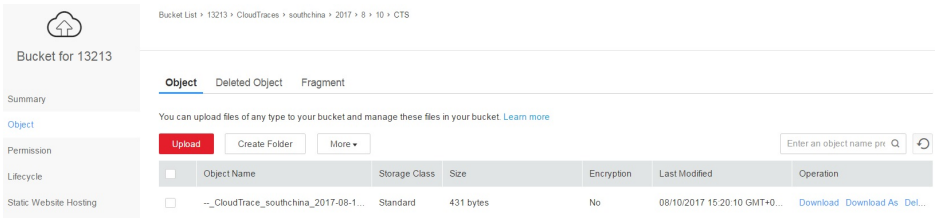
     An example is ***File Prefix*_CloudTrace_region_2016-05-30T16-20-56Z_21d36ced8c8af71e.json.gz**.

   NOTE

   The OBS bucket name and trace file prefix are user-defined, and other parameters are automatically generated.

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

Figure 2-2 Viewing trace file content



7. Extract a JSON file with the same name as the downloaded trace file and open the JSON file using a text file editor to view trace logs.

3 Managing Trackers

3.1 Modifying a Tracker

Scenarios

This section describes how to modify the OBS bucket or file prefix of a created tracker on the CTS console. When you modify the bucket in the tracker, CTS automatically adds a policy to a new OBS bucket so that trace files can be delivered to the new bucket for storage. Modifying the file prefix of the tracker has no impact on the OBS bucket policy. After the modification is complete, the system will immediately start recording operations under the new rule.

This section describes how to modify the tracker configuration.

Prerequisites

You have created a tracker in CTS.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner to select the desired region and project.
3. Click **Service List** and choose **Management & Deployment** > **Cloud Trace Service**.
4. Click **Tracker** in the left pane.
5. Click **Modify** in the **Operation** column.

   You can specify an existing OBS bucket for storing trace files, or rename **File Prefix**.
6. Click **OK**.

After the tracker configuration is modified, you can view its new configuration on the **Tracker** page.

NOTE

Traces recorded by CTS are periodically delivered to the OBS bucket for storage. If you change the OBS bucket for a tracker, traces generated during the current period (generally several minutes) will be delivered to the new OBS bucket. For example, if the current period is from 12:00 to 12:05 and you change the OBS bucket for the tracker at 12:02, traces received from 12:00 to 12:02 will be delivered to the new OBS bucket at 12:05 for storage.

3.2 Disabling or Enabling a Tracker

Scenarios

This section describes how to disable an existing tracker on the CTS console. After the tracker is disabled, the system will stop recording operations, but you can still view operation records that have been recorded.

This section describes how to disable a tracker.

Prerequisites

You have created a tracker in CTS.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner to select the desired region and project.
3. Click **Service List** and choose **Management & Deployment** > **Cloud Trace Service**.
4. Click **Tracker** in the left pane.
5. In the tracker list, click **Disable** in the **Operation** column.
6. Click **Yes**.

   After the tracker is disabled, its status changes from **Disable** to **Enable**. To enable the tracker again, click **Enable** and then click **Yes**. The system will start recording operations again.

3.3 Deleting a Tracker

Scenarios

This section describes how to delete an existing tracker on the CTS console. Deleting a tracker has no impact on the traces that have been received. When you enable CTS again, you still can view those traces.

This section describes how to delete the tracker.

Prerequisites

You have created a tracker in CTS.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner to select the desired region and project.
3. Click **Service List** and choose **Management & Deployment** > **Cloud Trace Service**.
4. Click **Tracker** in the left pane.
5. In the tracker list, click **Delete** in the **Operation** column.
6. Click **Yes**.

4 Application Examples

4.1 Security Auditing

Scenarios

This section describes how to query records matching a specified characteristic and to perform security analysis on records of operations to check whether the operations are performed by authorized users.

Prerequisites

You have enabled CTS and the tracker is normal. For details about how to enable CTS, see **Enabling CTS**.

Procedure

The following steps take the creation and deletion of EVS disks in the last two weeks as an example:

1. Log in to the management console using the administrator account.
2. Click  in the upper left corner to select the desired region and project.
3. Click **Service List** and choose **Management & Deployment** > **Cloud Trace Service**.
4. Choose **Trace List** in the navigation pane on the left.
5. On the trace list page, click **Filter**. In the displayed box, specify **Trace Source**, **Resource Type**, and **Search By**, and click **Query** to query the specified traces.

   For example, you can select **EVS** for **Trace Source**, **evs** for **Resource Type**, and **Trace name** for **Search By**, select **createVolume** or **deleteVolume** in the right text box, and click **Query** to query all creation or deletion operations performed on EVS in the last seven days.

6. Choose **Tracker** from the left pane to switch to the **Tracker** page and obtain the OBS bucket name.
7. Download traces generated in the last seven days or all traces. For details, see **Querying Archived Traces**.
8. In the trace files, search traces using keywords **createVolume** or **deleteVolume**.
9. Obtain information about the user who performs the operation from the results in **5** and **8**. Check whether the user performs any unauthorized operation or any operation that does not conform to the security operation rules.

4.2 Fault Locating

Scenarios

If a resource or an action encounters an exception, you can query records of the resource or action in a specified time period and view its request and response to facilitate fault locating.

Prerequisites

You have enabled CTS and the tracker is normal. For details about how to enable CTS, see **Enabling CTS**.

Procedure

The following steps use an ECS as an example to describe how to locate an ECS fault.

1. Log in to the management console using the administrator account.
2. Click  in the upper left corner to select the desired region and project.
3. Click **Service List** and choose **Management & Deployment** > **Cloud Trace Service**.
4. Choose **Trace List** in the navigation pane on the left.
5. On the trace list page, click **Filter**. In the displayed box, specify **Trace Source**, **Resource Type**, and **Search By**, and click **Query**.

   NOTE

   For example, you can select **ECS** for **Trace Source**, **ecs** for **Resource Type**, and **Resource ID**for **Search By**, enter *ID of the faulty VM* in the right text box, and set the time range to 06:00 to 12:00 at a certain date.
6. Check the query result. Pay attention to the request type and response of each trace, and traces whose status is **warning** or **incident** and traces whose response shows a failure.

The following steps take the locating of an ECS creation fault as an example.

1. Log in to the management console using the administrator account.
2. Click  in the upper left corner to select the desired region and project.

3. Click **Service List** and choose **Management & Deployment** > **Cloud Trace Service**.
4. Choose **Trace List** in the navigation pane on the left.
5. Specify filters based on the failed ECS creation task. For example, you can select **ECS** for **Trace Source**, **ecs** for **Resource Type**, and **warning** for the trace status to query the trace named **createSingleServer**.
6. Locate the fault based on the error code or error message in the trace.

4.3 Resource Tracking

Scenarios

This section describes how to view operation records of any cloud resource throughout its lifecycle and how to check details of a specific operation.

Prerequisites

You have enabled CTS and the tracker is normal. For details about how to enable CTS, see **Enabling CTS**.

Procedure

The following steps use an ECS as an example to describe how to view all operation records.

1. Log in to the management console using the administrator account.
2. Click  in the upper left corner to select the desired region and project.
3. Click **Service List** and choose **Management & Deployment** > **Cloud Trace Service**.
4. Choose **Trace List** in the navigation pane on the left.
5. On the trace list page, click **Filter**. In the displayed box, specify **Trace Source**, **Resource Type**, and **Search By**, and click **Query** to query the specified traces.

   NOTE

   For example, you can select **ECS** for **Trace Source**, **ecs** for **Resource Type**, and **Resource ID** for **Search By**, enter *ID of the faulty ECS* in the right text box, and click **Query** to query traces of the last seven days.
6. Choose **Tracker** from the left pane to switch to the **Tracker** page and obtain the OBS bucket name.
7. Download traces generated in the last seven days or all traces. For details, see **Querying Archived Traces**.
8. Check all operation and change records of the ECS in the results obtained in **5** and **7**.

5 Trace References

5.1 Trace Structure

The structure of a trace consists of multiple key fields. For details, see **Table 5-1**.

NOTE

- Formats of some fields displayed on the management console are optimized for easy understanding.
- This section describes the key fields of a trace displayed on the management console.

Table 5-1 Key fields of traces

Field	Mandatory	Type	Description
time	Yes	Date	Time when a trace occurred. The value is the local standard time (GMT+local time zone), for example, 12/08/2016 11:24:04 GMT+08:00. This field is transmitted and stored in the form of a timestamp. It is the total number of milliseconds from 00:00:00 on January 1, 1970 (UTC), or 08:00:00 on January 1, 1970 (CST) to the current time.

Field	Mandatory	Type	Description
user	Yes	Structure	Cloud account used to perform an operation This field is displayed in the **Operator** column on the **Trace List** page. This field is transmitted and stored in the API in the form of a string.
request	No	Structure	Content requested by an operation This field is transmitted and stored in the API in the form of a string.
response	No	Structure	Response to the request by an operation This field is transmitted and stored in the API in the form of a string.
service_type	Yes	String	Operation source
resource_type	Yes	String	Resource type
resource_name	No	String	Resource name
resource_id	No	String	Unique resource ID
source_ip	Yes	String	IP address of the user that performs an operation The value of this parameter is empty if the operation is triggered by the system.
trace_name	Yes	String	Operation name
trace_status	Yes	String	Trace level The value can be **All trace statuses**, **normal**, **warning**, or **incident**.

Field	Mandatory	Type	Description
trace_type	Yes	String	Operation type There are types of operations: • ConsoleAction: operations performed on the management console • SystemAction: operations triggered by the system • ApiCall: operations triggered by invoking ApiGateway.
api_version	No	String	API version of the cloud service on which an operation is performed
message	No	Structure	Supplementary information
record_time	Yes	Number	Record time (time stamp) of an operation
trace_id	Yes	String	Unique operation ID
code	No	Number	Trace HTTP return code, for example, 200 or 400
request_id	No	String	Records the ID of the request.
location_info	No	String	Additional information required for fault locating after a request recording error occurs
endpoint	No	String	Endpoint of the page that displays details of cloud resources involved in this operation
resource_url	No	String	Access link (excluding the endpoint) of the page that displays details of cloud resources involved in this operation

5.2 Example Traces

This section provides two example traces and describes their key fields to help you understand the trace information. You can understand traces of other services in the similar way.

For details about the fields in a trace, see **Trace Structure**.

Create an ECS


```
{
   "time": "12/01/2016 11:07:28 GMT+08:00",
   "user": {
      "name": "aaa/op_service",
      "id": "f2fe9fac63414a35a7d03108d5f1ea73",
      "domain": {
         "name": "aaa",
         "id": "1f9b9ba51f6b4061bd5c1736b28469f8"
      }
   },
   "request": {
      "server": {
         "name": "as-config-15f1_XWO68TFC",
         "imageRef": "b2b2c7dc-bbb0-4d6b-81dd-f0904023d54f",
         "flavorRef": "m1.tiny",
         "personality": [],
         "vpcid": "e4c374b9-3675-482c-9b81-4acd59745c2b",
         "nics": [
            {
               "subnet_id": "fff89132-88d4-4e5b-9e27-d9001167d24f",
               "nictype": null,
               "ip_address": null,
               "binding:profile": null,
               "extra_dhcp_opts": null
            }
         ],
         "adminPass": "********",
         "count": 1,
         "metadata": {
            "op_svc_userid": "26e96eda18034ae9a44130bacb967b96"
         },
         "availability_zone": "az1.dc1",
         "root_volume": {
            "volumetype": "SATA",
            "extendparam": {
               "resourceSpecCode": "SATA"
            },
            "size": 40
         },
         "data_volumes": [],
         "security_groups": [
            {
               "id": "dd597fd7-d119-4994-a22c-891fcfc54be1"
            }
         ],
         "key_name": "KeyPair-3e51"
      }
   },
   "response": {
      "status": "SUCCESS",
      "entities": {
         "server_id": "42d39b4a-19b7-4ee2-b01b-a9f1353b4c54"
      },
      "job_id": "4010b39d58b855980158b8574b270018",
      "job_type": "createSingleServer",
      "begin_time": "2016-12-01T03:04:38.437Z",
      "end_time": "2016-12-01T03:07:26.871Z",
      "error_code": null,
      "fail_reason": null
   },
   "service_type": "ECS",
   "resource_type": "ecs",
   "resource_name": "as-config-15f1_XWO68TFC",
   "resource_id": "42d39b4a-19b7-4ee2-b01b-a9f1353b4c54",
   "source_ip": "",
   "trace_name": "createSingleServer",
   "trace_status": "normal",
   "trace_type": "SystemAction",
```



```
    "api_version": "1.0",
    "record_time": "12/01/2016 11:07:28 GMT+08:00",
    "trace_id": "4abc3a67-b773-11e6-8412-8f0ed3cc97c6"
}
```


Key fields in the preceding information are as follows:

- **time**: indicates the time when the trace occurred. In this example, the time is 11:07:28 on December 1.
- **user**: indicates the user who performs the operation. In this example, the user is aaa (**name** field) under the enterprise account aaa (**domain** field).
- **request**: indicates the request to create an ECS. It contains some basic information about the ECS, such as name (**as-config-15f1_XWO68TFC**) and resource ID (**e4c374b9-3675-482c-9b81-4acd59745c2b**).
- **response**: indicates the response to the ECS creation request. It contains **status** (**Success** in this example), **error_code** (**null** in this example), and **fail_reason** (**null** in this example).

Create an EVS Disk


```
{
    "time": "12/01/2016 11:24:04 GMT+08:00",
    "user": {
        "name": "aaa",
        "id": "26e96eda18034ae9a44130bacb967b96",
        "domain": {
            "name": "aaa",
            "id": "1f9b9ba51f6b4061bd5c1736b28469f8"
                }
            },
    "request": "",
    "response": "",
    "service_type": "EVS",
    "resource_type": "evs",
    "resource_name": "volume-39bc",
    "resource_id": "229142c0-2c2e-4f01-a1b4-2dfdf1c678c7",
    "source_ip": "10.146.230.124",
    "trace_name": "deleteVolume",
    "trace_status": "normal",
    "trace_type": "ConsoleAction",
    "api_version": "1.0",
    "record_time": ""12/01/2016 11:24:04 GMT+08:00",
    "trace_id": "c529254f-bcf5-11e6-a89a-7fc778a6c92c"
}
```


Key fields in the preceding information are as follows:

- **time**: indicates the time when the trace occurred. In this example, the time is 11:24:04 on December 1.
- **user**: indicates the user who performs the operation. In this example, the user is aaa (**name** field) under the enterprise account aaa (**domain** field).
- **request**: optional. It is null in this example.
- **response**: optional. It is null in this example.
- **trace_status**: indicates the level of the trace. It can replace the **response** field in indicating the operation result. In this example, the value is **normal**, indicating that the operation is successful.

6 Supported Services and Operation Lists

6.1 Computing

6.1.1 Key Operations on ECS

Elastic Cloud Server (ECS) provides scalable, on-demand cloud servers for secure, flexible, and efficient application environments. An ECS is a computing server that consists of CPUs, memory, images, and EVS disks, and integrates virtual private cloud (VPC), virtual firewall, and multi-data-copy functions to ensure reliable, uninterrupted services.

With CTS, you can record operations associated with ECS for future query, audit, and backtrack operations.

Table 6-1 ECS operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Creating an ECS	ecs	createServer
Deleting an ECS	ecs	deleteServer

Operation	Resource Type	Trace Name
Starting an ECS	ecs	startServer
Restarting an ECS	ecs	rebootServer
Stopping an ECS	ecs	stopServer
Adding a NIC to an ECS	ecs	addNic
Removing a NIC to an ECS	ecs	deleteNic
Attaching a disk to an ECS	ecs	attachVolume
Attaching a disk to an ECS (on the EVS console)	ecs	attachVolume2
Detaching a disk from an ECS	ecs	detachVolume
Reinstalling the OS	ecs	reinstallOs
Changing the OS	ecs	changeOs
Modifying ECS specifications	ecs	resizeServer
Adding the automatic recovery tag to a VM	ecs	addAutoRecovery
Deleting the automatic recovery tag from a VM	ecs	deleteAutoRecovery
Creating a security group	ecs	createSecurityGroup

6.1.2 Key Operations on IMS

Image Management Service (IMS) provides easy and convenient image management. You can use a public or private image to create an ECS. You can also create a private image using an existing ECS or an external image file.

With CTS, you can record operations associated with IMS for later query, audit, and backtrack operations.

Table 6-2 IMS operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Creating an image	ims	createImage
Modifying an image	ims	updateImage
Deleting images in batches	ims	deleteImage
Copying an image	ims	copyImage

Operation	Resource Type	Trace Name
Exporting an image	ims	exportImage
Adding a member	ims	addMember
Modifying members in batches	ims	updateMember
Deleting members in batches	ims	deleteMember

6.1.3 Key Operations on BMS

Bare Metal Servers (BMSs) provide dedicated physical servers in single-tenant environments. They provide excellent computing performance and data security for core databases, key application systems, and high performance computing. They also offer the high scalability of a cloud-based service. You can buy BMSs directly or in a DeC as you need.

With CTS, you can record operations associated with BMS for future query, audit, and backtrack operations.

Table 6-3 BMS operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Creating a BMS	bms	createBareMetalServers
Deleting a BMS	bms	deleteBareMetalServers
Starting a BMS	bms	startBareMetalServers
Stopping a BMS	bms	stopBareMetalServers
Restarting a BMS	bms	rebootBareMetalServers
Attaching a data disk to a BMS	bms	attachDataVolume
Detaching a data disk from a BMS	bms	detachDataVolume

6.1.4 Key Operations on CCE

Cloud Container Engine (CCE) is a high-performance, high-reliability service through which enterprises can manage containerized applications. CCE supports native Kubernetes applications and tools, allowing you to easily set up a container runtime environment on the cloud.

With CTS, you can record operations associated with CCE for later query, audit, and backtrack operations.

Table 6-4 CCE operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Uploading a certificate	aksk	uploadAKSK
Creating a cluster	cluster_cce	createCluster
Upgrading a cluster	cluster_cce	upgradeCluster
Updating a cluster	cluster_cce	updateCluster
Deleting a cluster	cluster_cce	deleteCluster
Creating a node	node	createNode
Deleting a node	node	deleteNode
Creating a template	component	createComponent
Updating a template	component	updateComponent
Deleting a template	component	deleteComponent
Creating an application	app	createApp
Updating an application	app	updateApp
Rolling back an application	app	rollBackApp
Deleting an application	app	deleteApp
Creating an application using a blueprint	app	createAppByBlueprint
Creating a blueprint	blueprint	createBlueprint
Deleting a blueprint	blueprint	deleteBlueprint
Updating a blueprint	blueprint	updateBlueprint
Renaming a blueprint	blueprint	renameBlueprint
Validating a blueprint	blueprint	validateBlueprint
Deleting junk images	image	garbageCollectImage
Deleting a specified image	image	deleteImage
Deleting a tag image	image	deleteTagImage

Operation	Resource Type	Trace Name
Updating the description of an image	image	updateImageDesc
Creating a policy	policy	createPolicy
Updating a policy	policy	updatePolicy
Deleting a policy	policy	deletePolicy
Enabling a policy	policy	enablePolicy
Disabling a policy	policy	disablePolicy
Creating a periodic or scheduled scaling policy	scaling_policy_cce	createScalingPolicy
Deleting a periodic or scheduled scaling policy	scaling_policy_cce	deleteScalingPolicy
Creating a cluster	clusters	createCluster
Updating a cluster	clusters	updateCluster
Deleting a cluster	clusters	deleteCluster
Creating a node	clusters-nodes	createNode
Adding a static node	clusters-nodes	addStaticNode
Updating a node	clusters-nodes	updateNode
Deleting a host	clusters-nodes	deleteOneHost
Deleting all hosts	clusters-nodes	deleteAllHosts
Suspending user resources	N/A	suspendUserResource
Creating a ConfigMap	configmaps	createConfigmaps
Creating a DaemonSet	daemonsets	createDaemonsets
Creating a deployment	deployments	createDeployments
Creating an event	events	createEvents
Creating an ingress	ingress	createIngresses
Creating a job	jobs	createJobs
Creating a namespace	namespaces	createNamespaces
Creating a node	nodes	createNodes

Operation	Resource Type	Trace Name
Creating a PersistentVolume-Claim	persistentvolume-claims	createPersistentvolumeclaims
Creating a pod	pods	createPods
Creating a replica set	replicasets	createReplicasets
Creating a resource quota	resourcequotas	createResourcequotas
Creating a key	secrets	createSecrets
Creating a service	services	createServices
Creating a StatefulSet	statefulsets	createStatefulsets
Creating a volume	volumes	createVolumes
Deleting a ConfigMap	configmaps	deleteConfigmaps
Deleting a DaemonSet	daemonsets	deleteDaemonsets
Deleting a deployment	deployments	deleteDeployments
Deleting an event	events	deleteEvents
Deleting an ingress	ingresses	deleteIngresses
Deleting a job	jobs	deleteJobs
Deleting a namespace	namespaces	deleteNamespaces
Deleting a node	nodes	deleteNodes
Deleting a pod	pods	deletePods
Deleting a replica set	replicasets	deleteReplicasets
Deleting a resource quota	resourcequotas	deleteResourcequotas
Deleting a secret	secrets	deleteSecrets
Deleting a service	services	deleteServices
Deleting a StatefulSet	statefulsets	deleteStatefulsets
Deleting a volume	volumes	deleteVolumes
Replacing a specified ConfigMap	configmaps	updateConfigmaps
Replacing a specified DaemonSet	daemonsets	updateDaemonsets
Replacing a specified deployment	deployments	updateDeployments

Operation	Resource Type	Trace Name
Replacing a specified event	events	updateEvents
Replacing a specified ingress	ingresses	updateIngresses
Replacing a specified job	jobs	updateJobs
Replacing a specified namespace	namespaces	updateNamespaces
Replacing a specified node	nodes	updateNodes
Replacing a specified PersistentVolume-Claim	persistentvolume-claims	updatePersistentvolumeclaims
Replacing a specified pod	pods	updatePods
Replacing a specified replica set	replicasets	updateReplicasets
Replacing a specified resource quota	resourcequotas	updateResourcequotas
Replacing a specified secret	secrets	updateSecrets
Replacing a specified service	services	updateServices
Replacing a specified StatefulSet	statefulsets	updateStatefulsets
Replacing the specified status	status	updateStatus
Uploading a chart	uploadchart	uploadChart
Updating a chart	charts	updateChart
Deleting a chart	charts	deleteChart
Creating a template application	releases	createRelease
Updating a template application	releases	updateRelease
Deleting a template application	releases	deleteRelease

6.2 Storage

6.2.1 Key Operations on CSBS

Cloud Server Backup Service (CSBS) can back up an entire ECS. It can use the consistent backup data of multiple Elastic Volume Service (EVS) disks to restore the service data of an ECS. CSBS ensures data security and service continuity.

With CTS, you can record operations associated with CSBS for future query, audit, and backtrack operations.

Table 6-5 CSBS operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Creating a backup policy	backupPolicy	createBackupPolicy
Updating a backup policy	backupPolicy	updateBackupPolicy
Deleting a backup policy	backupPolicy	deleteBackupPolicy
Binding resources	backupPolicy	bindResources
Executing a backup	checkpointItem	createCheckpoint
Restoring a backup	checkpointItem	restoreCheckpointItem
Deleting a backup	checkpointItem	deleteCheckpointItem
Backing up an ECS	cloudServer	backupCloudServer
Deleting a task	operationLog	deleteOperationLog

6.2.2 Key Operations on EVS

Elastic Volume Service (EVS) is a scalable virtual block storage service that is based on the distributed architecture. EVS disks can be operated online. Using them is similar to using common server hard disks. Compared with common server hard disks, EVS disks have higher data reliability and I/O throughput capabilities. They are also easier to use. EVS disks apply to file systems, databases, or system software or other applications that require block storage devices.

With CTS, you can record operations associated with EVS for later query, audit, and backtrack operations.

Table 6-6 EVS operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Creating an EVS disk	evs	createVolume
Updating an EVS disk	evs	updateVolume
Expanding an EVS disk	evs	extendVolume
Deleting an EVS disk	evs	deleteVolume

6.2.3 Key Operations on VBS

Volume Backup Service (VBS) provides snapshot-based data protection for EVS disks on ECSs in public cloud environments. VBS supports both full and incremental backups. By default, the system performs a full backup initially, and then performs incremental backups. You can use those data backups generated in either backup mode to restore EVS disks to the state they were in when the backup was created.

With CTS, you can record operations associated with VBS for later query, audit, and backtrack operations.

Table 6-7 VBS operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Creating a backup	vbs	bksCreateBackup
Deleting a backup	vbs	bksDeleteBackup
Restoring a backup	vbs	bksRestoreBackup
Binding a backup policy	autobackup	addPolicyResource
Unbinding a backup policy	autobackup	deletePolicyResource
Executing a backup policy	autobackup	actionPolicy
Creating a backup policy	autobackup	createPolicy
Deleting a backup policy	autobackup	deletePolicy
Modifying a backup policy	autobackup	modifyPolicy

Operation	Resource Type	Trace Name
Creating backups scheduled by a backup policy	autobackup	scheduleCreateBackup
Automatically deleting redundant backups scheduled by a backup policy	autobackup	scheduleDeleteBackup
Batch adding or modifying tags of a backup policy	autobackup	batchAddPolicyTag
Batch deleting tags of a backup policy	autobackup	batchDeletePolicyTag
Adding or modifying a backup policy tag	autobackup	addPolicyTag
Deleting a backup policy tag	autobackup	deletePolicyTag

6.2.4 Key Operations on SDRS

Storage Disaster Recovery Service (SDRS) provides disaster recovery (DR) services for many public cloud services, such as Elastic Cloud Server (ECS), Dedicated Distributed Storage Service (DSS), and Elastic Volume Service (EVS). SDRS uses multiple technologies, such as storage replication, data redundancy, and cache acceleration, to provide high data reliability and service continuity for users.

With CTS, you can record operations associated with SDRS for future query, audit, and backtrack operations.

Table 6-8 SDRS operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Creating a protection group	protectionGroup	createProtectionGroup-NoCG
Deleting a protection group	protectionGroup	deleteProtectionGroup-NoCG
Updating a protection group	protectionGroup	updateProtectionGroup

Operation	Resource Type	Trace Name
Enabling protection for a protection group (when the protection group is in the **Available** state)	protectionGroup	startProtectionGroup-NoCG
Enabling protection for a protection group (when the protection group is in the **failed-over** or **failed-over-back** state)	protectionGroup	reprotectProtection-GroupNoCG
Disabling protection for a protection group	protectionGroup	stopProtectionGroup-NoCG
Executing a failover or failback	protectionGroup	failoverProtectionGroup-NoCG
Executing a planned failover or planned failback	protectionGroup	reverseProtectionGroup-NoCG
Action performed when a job of the protection group failed to submit	protectionGroup	protectionGroupAction
Creating a protected instance	protectedInstance	createProtectedInstance-NoCG
Deleting a protected instance	protectedInstance	deleteProtectedInstance-NoCG
Updating a protected instance	protectedInstance	updateProtectedInstance
Attaching a replication pair to a protected instance	protectedInstance	attachReplicationPair
Detaching a replication pair from a protected instance	protectedInstance	detachReplicationPair
Adding a NIC to a protected instance	protectedInstance	addNicNew
Deleting a NIC from a protected instance	protectedInstance	deleteNicNew
Modifying the specifications of a protected instance	protectedInstance	resizeProtectedInstance-New
Creating a replication pair	replicationPair	createReplicationPair-NoCG

Operation	Resource Type	Trace Name
Deleting a replication pair	replicationPair	deleteReplicationPair-NoCG
Updating a replication pair	replicationPair	updateReplicationPair
Expanding the capacity of a replication pair	replicationPair	expandReplicationPair-New
Creating a DR drill	disasterRecoveryDrill	createDisasterRecovery-Drill
Deleting a DR drill	disasterRecoveryDrill	deleteDrDrill
Updating a DR drill	disasterRecoveryDrill	updateDrDrill

6.3 Network

6.3.1 Key Operations on VPC

Virtual Private Cloud (VPC) enables you to provision logically isolated, configurable, and manageable virtual networks for ECSs, improving the security of resources in enterprise clouds and simplifying network deployment.

With CTS, you can record operations associated with VPC for future query, audit, and backtrack operations.

Table 6-9 VPC operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Modifying the bandwidth	bandwidth	modifyBandwidth
Creating an EIP	eip	createEip
Releasing an EIP	eip	deleteEip
Binding an EIP	eip	bindEip
Unbinding an EIP	eip	unbindEip
Assigning a private IP address	privateIps	createPrivateIp
Releasing a private IP address	privateIps	deletePrivateIp
Creating a security group	security_group	createSecurityGroup

Operation	Resource Type	Trace Name
Modifying a security group	security_group	modifySecurityGroup
Creating a subnet	subnet	createSubnet
Deleting a subnet	subnet	deleteSubnet
Modifying a subnet	subnet	modifySubnet
Creating a VPC	vpc	createVpc
Deleting a VPC	vpc	deleteVpc
Modifying a VPC	vpc	modifyVpc
Creating a VPN	vpn	createVpn
Deleting a VPN	vpn	deleteVpn
Modifying a VPN	vpn	modifyVpn
Creating a NAT gateway	natgateway	createNatGateway
Updating a NAT gateway	natgateway	updateNatGateway
Deleting a NAT gateway	natgateway	deleteNatGateway
Creating an SNAT rule	snatrule	createSnatRule
Deleting an SNAT rule	snatrule	deleteSnatRule
Creating a DNAT rule	dnatrule	createDnatRule
Deleting a DNAT rule	dnatrule	deleteDnatRule

6.3.2 Key Operations on Direct Connect

Direct Connect (DC) allows you to establish a private, dedicated network connection from your data center, office, or collocation environment to the public cloud platform. It reduces your network latency and provides a more consistent network experience than Internet-based connections.

With CTS, you can record operations associated with Direct Connect for later query, audit, and backtrack operations.

Table 6-10 DC operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Modifying a direct connection	dcaasConnection	modifyConnection

6.3.3 Key Operations on ELB

Elastic Load Balancing (ELB) is a service that automatically distributes access traffic to multiple ECSs to balance their service load. ELB enables you to achieve higher levels of fault tolerance in your applications and expand application service capabilities.

With a web-based console, you can create load balancers, configure the ports required for listening, and add backend ECSs for load balancers. ELB helps eliminate single points of failure (SPOFs), improving availability of the whole system.

With CTS, you can record operations associated with ELB for later query, audit, and backtrack operations.

Table 6-11 ELB operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Adding a backend ECS group	pool	createPool
Modifying a backend ECS group	pool	updatePool
Deleting a backend ECS group	pool	deletePool
Configuring a forwarding policy	l7policy	createL7policy
Modifying a forwarding policy	l7policy	updateL7policy
Deleting a forwarding policy	l7policy	deleteL7policy
Configuring a forwarding rule	l7rule	createL7rule
Modifying a forwarding rule	l7rule	updateL7rule
Deleting a forwarding rule	l7rule	deleteL7rule
Creating a health check	healthmonitor	createHealthmonitor
Deleting a health check	healthmonitor	updateHealthmonitor
Modifying a health check	healthmonitor	deleteHealthmonitor
Creating a certificate	certificate	createCertificate

Operation	Resource Type	Trace Name
Modifying a certificate	certificate	updateCertificate
Deleting a certificate	certificate	deleteCertificate
Creating a listener	listener	createListener
Modifying a listener	listener	updateListener
Deleting a listener	listener	deleteListener
Creating a load balancer	loadbalancer	createLoadbalancer
Modifying a load balancer	loadbalancer	updateLoadbalancer
Deleting a load balancer	loadbalancer	deleteLoadbalancer
Adding a backend ECS	member	createMember
Removing a backend ECS	member	deleteMember
Configuring access logs	accesslog	createAccesslog

6.3.4 Region-level Key Operations on DNS

Domain Name Service (DNS) provides highly available and scalable authoritative DNS services and domain name management services. It translates domain names or application resources into IP addresses required for network connection. By doing so, visitors' access requests are directed to the desired resources.

With CTS, you can record operations associated with DNS for later query, audit, and backtrack operations.

Table 6-12 Region-level DNS operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Creating a record set in a private zone	privateRecordSet	createPrivateRecordSet
Deleting a record set in a private zone	privateRecordSet	deletePrivateRecordSet
Modifying a record set in a private zone	privateRecordSet	updatePrivateRecordSet
Creating a private zone	privateZone	createPrivateZone
Modifying a private zone	privateZone	updatePrivateZone

Operation	Resource Type	Trace Name
Deleting a private zone	privateZone	deletePrivateZone
Associating a VPC	privateZone	associateRouter
Disassociating a VPC	privateZone	disassociateRouter
Configuring a PTR Record	ptrRecord	setPTRRecord
Deleting a PTR record	ptrRecord	resetPTRRecord

6.3.5 Global-level Key Operations on DNS

Domain Name Service (DNS) provides highly available and scalable authoritative DNS services and domain name management services. It translates domain names or application resources into IP addresses required for network connection. By doing so, visitors' access requests are directed to the desired resources.

With CTS, you can record operations associated with DNS for later query, audit, and backtrack operations.

Table 6-13 Global-level DNS operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Creating a record set in a public zone	publicRecordSet	createPublicRecordSet
Deleting a record set in a public zone	publicRecordSet	deletePublicRecordSet
Modifying a record set in a public zone	publicRecordSet	updatePublicRecordSet
Creating a public zone	publicZone	createPublicZone
Modifying a public zone	publicZone	updatePublicZone
Deleting a public zone	publicZone	deletePublicZone
Adding tags to a public zone	publicZoneTag	createPublicZoneTag
Deleting tags of a public zone	publicZoneTag	deletePublicZoneTag
Adding tags to a record set in a public zone	publicRecordSet-Tag	createPublicRecordSetTag
Deleting tags of a record set in a public zone	publicRecordSet-Tag	deletePublicRecordSetTag

Operation	Resource Type	Trace Name
Adding tags to a private zone	privateZoneTag	createPrivateZoneTag
Deleting tags of a private zone	privateZoneTag	deletePrivateZoneTag
Adding tags to a record set in a private zone	privateRecordSet-Tag	createPrivateRecordSetTag
Deleting tags of a record set in a private zone	privateRecordSet-Tag	deletePrivateRecordSetTag
Adding tags to a PTR record	ptrRecordTag	createPTRRecordSetTag
Deleting tags of a PTR record	ptrRecordTag	deletePTRRecordTag

6.4 Management & Deployment

6.4.1 Key Operations on CTS

Cloud Trace Service (CTS) provides records of operations on cloud service resources. With CTS, you can query, audit, and backtrack these operations.

With CTS, you can record operations associated with CTS itself for later query, audit, and backtrack operations.

Table 6-14 CTS operations that can be recorded by itself

Operation	Resource Type	Trace Name
Creating a tracker	tracker	createTracker
Modifying a tracker	tracker	updateTracker
Disabling a tracker	tracker	updateTracker
Enabling a tracker	tracker	updateTracker
Deleting a tracker	tracker	deleteTracker

6.4.2 Key Operations on Cloud Eye

Cloud Eye is an open monitoring platform. It provides monitoring, alarm reporting, and alarm notification for your resources in near-real time.

With CTS, you can record operations associated with Cloud Eye for future query, audit, and backtracking operations.

Table 6-15 Cloud Eye operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Adding an alarm rule	alarm_rule	createAlarmRule
Deleting an alarm rule	alarm_rule	deleteAlarmRule
Disabling an alarm rule	alarm_rule	disableAlarmRule
Enabling an alarm rule	alarm_rule	enableAlarmRule
Modifying an alarm rule	alarm_rule	updateAlarmRule
Updating the alarm status to alarm	alarm_rule	alarmStatusChangeToAlarm
Updating the alarm status to insufficient data	alarm_rule	alarmStatusChangeToInsuffi-cientData
Updating the alarm status to normal	alarm_rule	alarmStatusChangeToOk
Creating a custom alarm template	alarm_template	createAlarmTemplate
Deleting a custom alarm template	alarm_template	deleteAlarmTemplate
Modifying a custom alarm template	alarm_template	updateAlarmTemplate
Creating a monitoring panel	dashboard	createDashboard
Deleting a monitoring panel	dashboard	deleteDashboard
Modifying a monitoring panel	dashboard	updateDashboard
Adding monitoring data	metric	addMetricData
Exporting monitoring data	metric	downloadMetricsReport

6.4.3 Key Operations on IAM

Identity and Access Management (IAM) enables you to centrally manage authentication information, including your authenticated email, phone number, and password. When you invoke an API to apply for an ECS, manage cloud resources, or log in to the public cloud platform in multi-tenant mode, you can query the required project ID, AK/SK, and username in real time.

With CTS, you can record operations associated with IAM for future query, audit, and backtrack operations.

NOTE

IAM is a global-level service and IAM traces are only displayed in the central region of the current site.

Table 6-16 IAM operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Creating a token	token	createTokenByPwd
Creating a token	token	createTokenByHwAccessKey
Creating a token	token	createTokenByToken
Creating a token	token	createTokenByAssumeRole
Creating a token	token	createTokenByHwRenewToken
User login	user	login
User logout	user	logout
Changing a user password	user	changePassword
Creating a user	user	createUser
Modifying user information	user	updateUser
Deleting a user	user	deleteUser
Changing a user password	user	updateUserPwd
Creating an AK/SK	user	addCredential
Deleting an AK/SK	user	deleteCredential
Changing an email address	user	modifyUserEmail
Changing a mobile phone number	user	modifyUserMobile
Changing a password	user	modifyUserPassword
Enabling two-factor authentication for login	user	modifySMVerify
Uploading a user picture	user	modifyUserPicture
Setting a user password	user	setPasswordByAdmin
Creating a user group	userGroup	createGroup
Modifying a user group	userGroup	updateGroup
Deleting a user group	userGroup	deleteGroup

Operation	Resource Type	Trace Name
Adding a user to a user group	userGroup	addUserToGroup
Deleting a user from a user group	userGroup	removeUserFromGroup
Creating a project	project	createProject
Changing a project	project	updateProject
Deleting a project	project	deleteProject
Updating the project status	project	updateProjectStatus
Canceling a project deletion task	project	cancelProjectDeletion
Creating an agency	agency	createAgency
Modifying an agency	agency	updateAgency
Deleting an agency	agency	deleteAgency
Switching the role	agency	switchRole
Registering an identity provider	identityProvider	createIdentityProvider
Modifying an identity provider	identityProvider	updateIdentityProvider
Deleting an identity provider	identityProvider	deleteIdentityProvider
Updating IDP metadata	identityProvider	updateMetaConfigure
Updating preset IDP metadata	identityProvider	updateSystemMetaConfigure
Creating a mapping	mapping	createMapping
Updating a mapping	mapping	updateMapping
Deleting a mapping	mapping	deleteMapping
Creating a protocol	protocol	createProtocol
Changing a protocol	protocol	updateProtocol
Deleting a protocol	protocol	deleteProtocol
Granting permissions to an agency based on tenant information	roleAgencyDomain	assignRoleToAgencyOnDomain

Operation	Resource Type	Trace Name
Revoking permissions from an agency based on tenant information	roleAgencyDomain	unassignRoleToAgencyOnDomain
Granting permissions to an agency based on project Information	roleAgencyProject	assignRoleToAgencyOnProject
Deleting permissions from an agency based on project information	roleAgencyProject	unassignRoleToAgencyOnProject
Granting permissions to a user group of a tenant	roleGroupDomain	assignRoleToGroupOnDomain
Deleting permissions of a specified user group of a tenant	roleGroupDomain	unassignRoleToGroupOnDomain
Assigning permissions to a user group corresponding to a project	roleGroupProject	assignRoleToGroupOnProject
Revoking permissions from a user group corresponding to a project	roleGroupProject	unassignRoleToGroupOnProject
Modifying a security policy	domain	updateSecurityPolicies
Updating a password policy	domain	updatePasswordPolicies
Modifying an ACL policy	domain	updateACLPolicies
Updating a security warning policy	domain	updateWarningPolicies
Creating a domain	domain	createDomain

6.4.4 Key Operations on RTS

Resource Template Service (RTS) provides templates for combining cloud resources and allows users to automatically create cloud resources they need using templates.

With CTS, you can record operations associated with RTS for later query, audit, and backtrack operations.

Table 6-17 RTS operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Creating a configuration	software_configs	createSoftwareConfigs
Deleting a configuration	software_configs	deleteSoftwareConfigs
Creating a deployment	software_deployments	createSoftwareDeployments
Deleting a deployment	software_deployments	deleteSoftwareDeployments
Updating a deployment	software_deployments	updateSoftwareDeploy-ments
Stack management actions, such as canceling stack update or checking stack resources	stacks	createStacksActions
Sending a signal to resources in a stack	stacks	createStacksResourcesSignal
Creating a stack	stacks	createStacks
Deleting a stack	stacks	deleteStacks
Updating a stack	stacks	updateStacks
Previewing a stack	stacks	createStacksPreview
Identifying a resource as unhealthy	stacks	patchStacksResource
Validating a template	validate	createValidate

6.4.5 Key Operations on TMS

Tag Management Service (TMS) is a visualized service for fast, unified tag management that enables you to control your resource permissions and billing more efficiently. It allows you to tag and categorize cloud services across regions, and it can be accessed through the TMS console or using APIs.

With CTS, you can record operations associated with TMS for future query, audit, and backtrack operations.

NOTE

TMS is a global-level service and TMS traces are only displayed in the central region of the current site.

Table 6-18 TMS operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Adding a predefined tag	application	addTag
Deleting a predefined tag	application	deleteTag
Modifying a predefined tag	application	modifyTag
Creating a resource tag	application	addResourceTag
Deleting a resource tag	application	deleteResourceTag

6.5 Database

6.5.1 Key Operations on RDS

Relational Database Service (RDS) is a cloud-based web service that is reliable, scalable, easy to manage, and immediately ready for use.

With CTS, you can record operations associated with RDS for future query, audit, and backtrack operations.

Table 6-19 RDS operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Creating a DB instance, restoring data to a new DB instance, creating a read replica (using the console, Open API, or Trove API)	instance	createInstance
Restarting and scaling up a DB instance, changing the DB instance class, and restoring data to the old DB instance (using the console, Open API, or Trove API)	instance	instanceAction
Resetting the password (using the console)	instance	resetPassword
Setting the DB version parameters (using Open API)	instance	setDBParameters

Operation	Resource Type	Trace Name
Resetting the DN version parameters (using Open API)	instance	resetDBParameters
Setting **Backup Policy** to **On**, **Off,** or **Modify** (using the console or Open API)	instance	setBackupPolicy
Modifying the DB port number (using the console)	instance	changeInstancePort
Binding or unbinding an elastic IP address (using the console)	instance	setOrResetPublicIP
Modifying a security group (using the console)	instance	modifySecurityGroup
Creating a tag (using the console or Open API)	instance	createTag
Deleting a tag (using the console or Open API)	instance	deleteTag
Modifying a tag (using the console or Open API)	instance	modifyTag
Deleting a DB instance from a cluster (using the console, Open API, or Trove API)	instance	deleteInstance
Creating a snapshot (using the console or Open API)	backup	createManualSnapshot
Copying a snapshot (using the console)	backup	copySnapshot
Deleting a snapshot (using the console or Open API)	backup	deleteManualSnapshot
Creating a parameter group (using the console or Trove API)	config	createParameterGroup
Modifying a parameter group (using the console or Trove API)	config	updateParameterGroup

Operation	Resource Type	Trace Name
Deleting a parameter group (using the console or Trove API)	config	deleteParameterGroup
Copying a parameter group (using the console)	config	copyParameterGroup
Resetting a parameter group (using the console)	config	resetParameterGroup
Comparing parameter groups (using the console)	config	compareParameterGroup
Applying a parameter group (using the console)	config	applyParameterGroup

6.6 Security

6.6.1 Key Operations on Anti-DDoS

Anti-DDoS is a network security service that defends IP addresses against distributed denial of service (DDoS) attacks.

Anti-DDoS monitors traffic directed to specified IP addresses in real time and detects access traffic at network egresses to discover DDoS attacks as soon as possible. It then cleans abnormal traffic according to user-configured defense policies so that services run as normal. It also generates reports to present users with a clear evaluation of network security.

With CTS, you can record operations associated with Anti-DDoS for future query, audit, and backtrack operations.

Table 6-20 Anti-DDoS operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Enabling Anti-DDoS	anti-ddos	openAntiddos
Disabling Anti-DDoS	anti-ddos	deleteAntiddos
Updating Anti-DDoS	anti-ddos	updateAntiddos

6.7 Enterprise Application

6.7.1 Key Operations on Workspace

Workspace is a cloud computing–based desktop service that is superior to traditional desktop services. Workspace supports access by various devices, including PCs running Windows or Mac, iPad, iPhone, and Android smart devices. It enables you to access, store, and obtain files and applications anywhere and at any time, that is, mobile working and entertainment. Workspace provides configuration similar to a traditional desktop, including vCPU, GPU, memory, disks, and Windows. You can use it in the same way you use a PC.

With CTS, you can record operations associated with Workspace for later query, audit, and backtrack operations.

Table 6-21 Workspace operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Updating the status of a cloud service	workspace	updateDesktopMetadata
Subscribing to Workspace	workspace	orderVm
Restarting a VM	workspace	rebootDesktop
Stopping a VM	workspace	shutdownDesktop
Starting a VM	workspace	startDesktop
Deleting a VM	workspace	deleteDesktop
Updating the status of a desktop	workspace	updateDesktopStatus
Deleting user information	workspace	deleteUser
Exporting user information	workspace	exportUserInfo
Unlocking a user	workspace	unlockUser
Resetting the password	workspace	resetUserPassword
Downloading a user template	workspace	downloadUserModel
Deleting an on-demand task	workspace	deleteJob
Applying for modifying the password (the domain user)	workspace	updateDomainUserPassword

Operation	Resource Type	Trace Name
Synchronizing the resource tenants (Identity and Access Management)	workspace	synIamResourceTenant
Updating the policy group	workspace	updatePolicy
Enabling Workspace	workspace	openService
Changing the domain password	workspace	updateAdPwd
Disabling Workspace	workspace	tenantClose
Retrying failed Workspace enabling and disabling tasks	workspace	tenantRetryServiceTask
Restoring the infrastructure VM	workspace	restoreManagerVmBackup
Modifying the desktop attributes	workspace	modifyDesktopAttributes
Updating the domain name	workspace	updateRecordSet

6.8 Enterprise Intelligence

6.8.1 Key Operations on MRS

MapReduce Service (MRS) is a data processing and analysis service that is based on a cloud computing platform. It is stable, reliable, scalable, and easy to manage.

With CTS, you can record operations associated with MRS for later query, audit, and backtrack operations.

Table 6-22 MRS operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Creating a cluster	cluster	createCluster
Deleting a cluster	cluster	deleteCluster
Expanding a cluster	cluster	scaleOutCluster
Shrinking a cluster	cluster	scaleInCluster

6.9 Key Operations on DeC

Dedicated Cloud (DeC) provides isolated virtual resource pools on the public cloud. You have exclusive use of all physical devices, computing and network resources, and reliable distributed storage inside a DeC.

With CTS, you can record operations associated with DeC for future query, audit, and backtrack operations.

Table 6-23 DeC operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Enabling DeC	dec	openDEC

7 Quota Adjustment

What Is the Quota?

Quotas are enforced for service resources on the platform to prevent unforeseen spikes in resource usage. Quotas can limit the number or amount of resources available to users. For example, the CTS quota limits the number of key event notifications that you can create.

If the existing resource quota cannot meet your service requirements, you can apply for a higher quota.

How do I View My Quota?

1. Log in to the management console.
2. Click  (the **My Quota** icon) in the upper right corner of the page.
   The **Service Quota** page is displayed.
3. On this page, you can view the total quota and used quota of resources.

8 FAQs

8.1 Can I Create Multiple Trackers?

Currently, only one tracker can be created for each user.

8.2 Which Type of Information Is Displayed on the Trace List?

The trace list records two types of traces: management traces and data traces. Management traces refer to the details about creating, configuring, and deleting

cloud service resources in cloud accounts. Data traces refer to operation logs of data, such as data uploading and downloading. The trace list does not record information about query operations.

8.3 Can Information Be Deleted from the Trace List?

This operation is not allowed. According to the regulations of SAC/TC and international information and data security management departments, logs used for auditing must be objective, comprehensive, and accurate. For this reason, the deletion and modification functions are not provided.

8.4 What Users May Require CTS?

All cloud users need to enable CTS.

- From the perspective of policies and industry standards, CTS is essential to information security audit. It is also important to information system security risk control of enterprises and public institutions, and necessary for many industry standards and audit specifications.
- From the perspective of application, CTS helps reduce fault locating time and manpower costs when cloud resources encounter an exception. With CTS, you can locate all operations involved by the fault to narrow the troubleshooting scope.

8.5 How Long Can Trace Files Be Retained?

By default, CTS stores the last seven days of trace files on the management console and can deliver traces to OBS buckets for a longer duration.

8.6 What Will Happen If I Have Enabled CTS But Have Not Configured a Correct Policy for the OBS Bucket?

In this case, CTS will deliver trace files based on the existing OBS bucket policy. If the policy is incorrectly configured, CTS may not deliver trace files to the OBS bucket.

If an OBS bucket has been deleted or encounters an exception, an error message will be displayed on the management console. In this case, you can choose to create an OBS bucket or reconfigure the access permissions of the OBS bucket. For detailed operations, see section "Bucket Management" in the *Object Storage Service User Guide*.

8.7 Does CTS Support Integrity Verification of Trace Files?

Yes. The following fields must be included: **time**, **service_type**, **resource_type**, **trace_name**, **trace_status**, and **trace_type**. Other fields are defined by different services.

8.8 Will Performance of Other Cloud Service Resources Be Affected If I Enable CTS?

No. Enabling CTS does not affect the performance of other cloud resources.

8.9 Why Are Fields of Some Traces Displayed Null 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 is triggered by the system. It is normal that the **source_ip** field is empty.
- **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 empty or have no service meaning. Therefore, they are left blank based on actual situations.
- **message**: This is a reserved field. Additional information of other cloud services will be added in this field when necessary. It is normal that it is left blank.

8.10 Why Are the of Some Traces in the Trace List Hyperlinks?

For ECS, EVS, VBS, IMS, AS, Cloud Eye, and VPC, you can click of some traces to go to the resource details page. The resource ID of such a trace is a hyperlink. More traces will be supported in future.

8.11 Why Do Some Operation Records Occur Twice in the Trace List?

For an asynchronously invoked trace, two records with the same trace name, resource type, and resource name will be generated. In the trace list, two records are displayed for the same trace, for example, the **deleteDesktop** trace of Workspace. The two records are associated, but have different content because they are not invoked at the same time. Details are as follows:

- The first record contains the request of a user to perform an operation.
- The second record contains the response to the user request and operation result, and is usually several minutes later than the first record.

The two records together indicate the operation result.

8.12 Why Are user_name and op_service Displayed When I Filter Traces by User?

If you submit a request that involves operations requiring high permissions or invocation of other services, you may not have the required permissions. In this case, your permissions will be elevated temporarily on condition that security requirements are met. Your permissions will be resumed after the request is processed, but the permissions elevation will be recorded in CTS logs and the operation user is recorded as **user_name** or **op_service**.

8.13 Which Type of OBS Buckets Is Suitable for CTS to Store Traces?

OBS provides three storage classes of buckets for storage, respectively standard access, infrequent access, or archive. You must select a standard OBS bucket because CTS needs to frequently access the OBS bucket that stores traces.

8.14 Why Are user and source_ip Empty for Some Traces with trace_type as systemAction?

The **trace_type** field indicates the request resource. This field can be **ConsoleAction**, **ApiCall**, and **SystemAction**.

SystemAction indicates that the operations are not triggered by users, such as automatic alarms, elastic scaling, scheduled backup tasks, and secondary invocations generated within the system to respond to the user's request. In this case, no user or device that triggers an operation exists. Therefore, **user** and **source_ip** are both empty.

8.15 What Are the Meanings of the Three Trace Statuses?

The trace status is defined based on **trace_status** information recorded in a trace. Different fields have different meanings as follows:

- **normal**: indicates that this operation succeeded.
- **warning**: indicates that this operation failed.
- **incident**: indicates that this operation causes a more serious consequence than a failure, for example, causing a node failure or service interruption.

A Change History

Release On	What's New
2018-07-30	This issue is the first official release.

