Cloud Trace Service

Service Overview

Issue	01
Date	2022-09-30

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

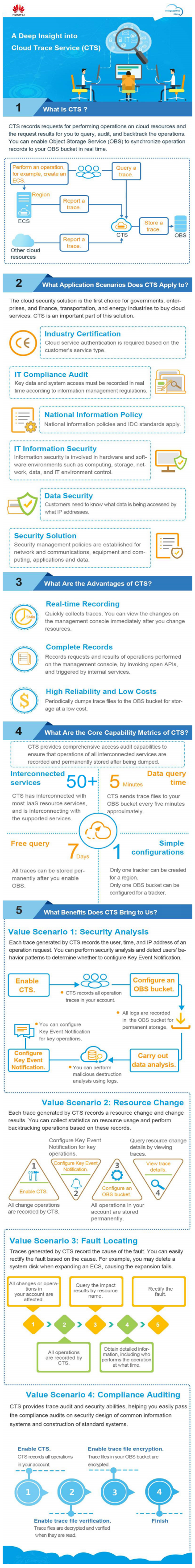
Notice

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 Infographics



A Deep Insight into Cloud Trace Service (CTS)

1 What Is CTS ?

CTS records requests for performing operations on cloud resources and the request results for you to query, audit, and backtrack the operations. You can enable Object Storage Service (OBS) to synchronize operation records to your OBS bucket in real time.

2 What Application Scenarios Does CTS Apply to?

The cloud security solution is the first choice for governments, enterprises, and finance, transportation, and energy industries to buy cloud services. CTS is an important part of this solution.

Industry Certification
Cloud service authentication is required based on the customer's service type.

IT Compliance Audit
Key data and system access must be recorded in real time according to information management regulations.

National Information Policy
National information policies and IDC standards apply.

IT Information Security
Information security is involved in hardware and software environments such as computing, storage, network, data, and IT environment control.

Data Security
Customers need to know what data is being accessed by what IP addresses.

Security Solution
Security management policies are established for network and communications, equipment and computing, applications and data.

3 What Are the Advantages of CTS?

Real-time Recording
Quickly collects traces. You can view the changes on the management console immediately after you change resources.

Complete Records
Records requests and results of operations performed on the management console, by invoking open APIs, and triggered by internal services.

High Reliability and Low Costs
Periodically dumps trace files to the OBS bucket for storage at a low cost.

4 What Are the Core Capability Metrics of CTS?

CTS provides comprehensive access audit capabilities to ensure that operations of all interconnected services are recorded and permanently stored after being dumped.

Interconnected services 50+
CTS has interconnected with most IaaS resource services, and is interconnecting with the supported services.

5 Minutes **Data query time**
CTS sends trace files to your OBS bucket every five minutes approximately.

Free query 7 Days
All traces can be stored permanently after you enable OBS.

1 **Simple configurations**
Only one tracker can be created for a region.
Only one OBS bucket can be configured for a tracker.

5 What Benefits Does CTS Bring to Us?

Value Scenario 1: Security Analysis

Each trace generated by CTS records the user, time, and IP address of an operation request. You can perform security analysis and detect users' behavior patterns to determine whether to configure Key Event Notification.

Enable CTS.
CTS records all operation traces in your account.
Configure an OBS bucket.
All logs are recorded in the OBS bucket for permanent storage.
You can configure Key Event Notification for key operations.
Configure Key Event Notification.
You can perform malicious destruction analysis using logs.
Carry out data analysis.

Value Scenario 2: Resource Change

Each trace generated by CTS records a resource change and change results. You can collect statistics on resource usage and perform backtracking operations based on these records.

Configure Key Event Notification for key operations.
Query resource change details by viewing traces.
1
Enable CTS.
Configure Key Event Notification.
2
3
Configure an OBS bucket.
View trace details.
4
All change operations are recorded by CTS.
All operations in your account are stored permanently.

Value Scenario 3: Fault Locating

Traces generated by CTS record the cause of the fault. You can easily rectify the fault based on the cause. For example, you may delete a system disk when expanding an ECS, causing the expansion fails.

All changes or operations in your account are affected.
Query the impact results by resource name.
Rectify the fault.
1
2
3
4
5
All operations are recorded by CTS.
Obtain detailed information, including who performs the operation at what time.

Value Scenario 4: Compliance Auditing

CTS provides trace audit and security abilities, helping you easily pass the compliance audits on security design of common information systems and construction of standard systems.

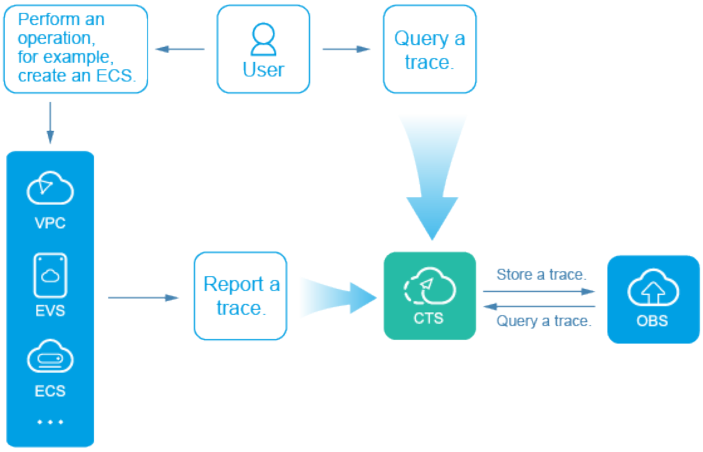
Enable CTS.
CTS records all operations in your account.
Enable trace file encryption.
Trace files in your OBS bucket are encrypted.
1
2
3
4
Enable trace file verification.
Trace files are decrypted and verified when they are read.
Finish

2 What Is Cloud Trace Service?

The log audit module is a core component necessary for information security audit and an important part for the information systems of enterprises and public institutions to provide security risk management and control. As information systems are migrated to the cloud, information and data security management departments around the world, including the Standardization Administration of the People's Republic of China/Technical Committee (SAC/TC), 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 for 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 2-1 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 type, trace source, resource type, filter, operator and trace status.
- Trace transfer: Traces are transferred 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.
- Trace file encryption: Trace files are encrypted using keys provided by Data Encryption Workshop (DEW) during transfer.

3 Basic Concepts

Trackers

A tracker named **system** is automatically created when you enable CTS. This tracker identifies and associates with all cloud services your tenant account is using, and records all operations of your tenant account.

Traces

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

There are two types of traces:

- Management traces

  Traces reported by cloud services.
- Data traces

  Traces of read and write operations reported by OBS.

Trace List

The trace list displays traces generated in the last seven days. These traces record operations on cloud service resources, including creation, modification, and deletion, but query operations are not recorded. There are two types of traces:

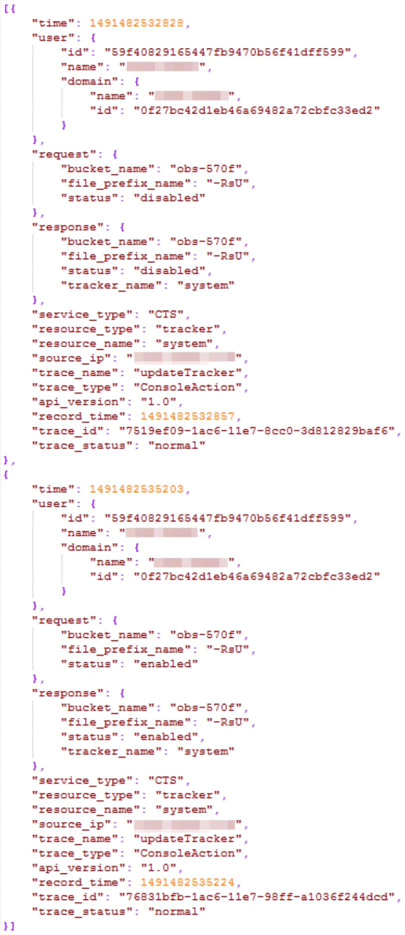
- Management traces: record details about creating, configuring, and deleting cloud service resources in your tenant account.
- Data traces: record operations on data, such as data upload and download.

Trace Files

A trace file is a collection of traces. CTS generates trace files based on services and transfer cycle and send these files to your specified OBS bucket in real time. In most cases, all traces of a service generated in a transfer cycle are compressed into one trace file. However, if there are a large number of traces, CTS will adjust the number of traces contained in each trace file.

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

Figure 3-1 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"
}]
```

Verifying Trace File Integrity

The authenticity of operation records during a security incident investigation is often affected by trace files being deleted or tampered with. The records therefore cannot be used as an effective basis for investigation. Therefore, CTS provides trace file integrity verification to help you ensure the authenticity of trace files.

The verification function for trace file integrity adopts industry standard algorithms and generates a Hash value for each trace file. This Hash value changes when the trace file is modified or deleted. Therefore, by tracking the Hash value, you can confirm whether the trace file is modified. In addition, the RSA algorithm is used to sign on the digest file to ensure that the file is not modified. In this way, any operations of modifying or deleting trace files are recorded by CTS.

After the verification function for trace file integrity is enabled, CTS generates a digest file for Hash values of all trace files recorded in the past hour and synchronizes the digest file to an OBS bucket configured for the current tracker.

CTS signs on each digest file using public and private keys. You can verify the digest file using the public key after the file is stored to the OBS bucket.

Regions

A region refers to a geographic area where the server for installing CTS is located. AZs in the same geographic area can communicate with each other through an internal network.

Data centers (DCs) are scattered across different regions of the world, for example, Europe and Asia. Enabling CTS in different regions makes applications more user-friendly and meets the laws and regulations of different regions.

Projects

A project corresponds to a Huawei Cloud region. Default projects are defined to isolate resources (including computing, storage, and network resources) across regions. You can create sub-projects in a default region project to isolate resources more precisely.

4 How CTS Functions

CTS connects to other cloud services of Huawei Cloud, records operations on cloud resources and the results, and stores these records in the form of trace files to OBS buckets in real time.

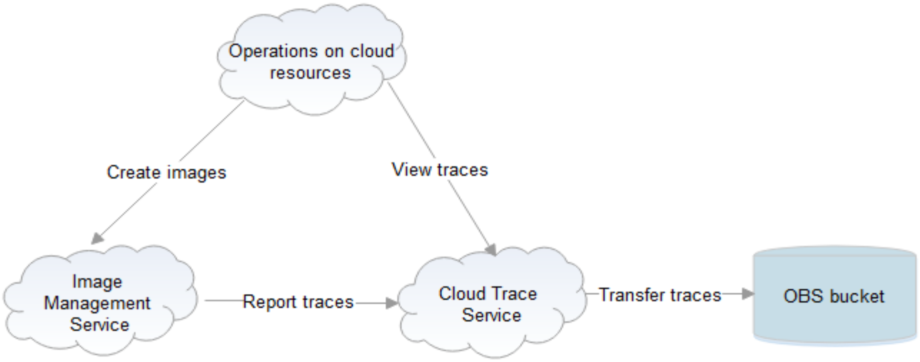
After CTS is enabled, the associated tracker can track the trace files generated. If trace transfer has been configured, trace files will be stored in the OBS bucket that you have specified.

You can perform the following operations on a trace file:

- Trace file creation and storage
  - When you add, delete, or modify resources 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 trace files to CTS for archiving.
  - Operation records of the last seven days are displayed on the CTS console. If trace transfer has been enabled, operation records are periodically delivered 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 if trace transfer has been configured.
  - You can enable, disable, configure, or delete a tracker on the **Tracker List** page.

  For example, if you create an image using IMS, the service will report the creation operation to CTS. Then, CTS will deliver the trace to an OBS bucket for storage if trace transfer has been configured. You can view trace files in the trace list. **Figure 4-1** shows the working principle of CTS.

Figure 4-1 How CTS functions



5 Application Scenarios

CTS can be used in the following four scenarios.

Compliance Auditing

CTS helps you obtain certifications for auditing in industry standards, such as PCI DSS and ISO 27001, for your service systems.

If you want to migrate your services to the cloud, you will need to ensure the compliance of your own service systems, and the cloud vendor you choose will need to ensure the compliance of your service systems and resources.

CTS plays an important role in Huawei Cloud's own compliance. The service records operations of almost all services and resources in Huawei Cloud, and carries out security measures such as encryption, disaster recovery, and anti-tampering to ensure the integrity of traces during their transmission and storage. In addition, you can use CTS to design and implement solutions that help you obtain compliance certifications for your service systems.

Key Event Notifications

CTS works with FunctionGraph to send notifications to natural persons or service APIs when any key operation is performed. The following are real application examples:

- You can configure HTTP or HTTPS notifications targeted at your independent systems and synchronize traces received by CTS to your own audit systems for auditing.
- You can select a certain type of log as a trigger (such as file upload) in FunctionGraph to trigger the preset workflow (for example, convert the file format), simplifying service deployment and O&M and avoiding problems and risks.

Data Mining

CTS mines data in traces to facilitate service health analysis, risk analysis, resource tracking, and cost analysis. You can also obtain the data from CTS and explore the data value yourself.

A trace contains up to 21 fields, recording when an operation was performed by a specific user on a specific resource and the IP address from which the operation was performed.

By configuring HTTP or HTTPS notifications, you can synchronize traces to your own system for analysis. In addition, CTS is connected to Cloud Eye and Log Tank Service (LTS) to help you monitor high-risk operations, detect unauthorized operations, and analyze resource usage.

Fault Locating and Analysis

You can configure filters to pinpoint the faulty operation and its details when a fault occurs, reducing the time and manpower required for detecting, locating, and fixing faults.

CTS provides the following search dimensions: trace type, trace source, resource type, filter, operator and trace status. Each trace contains the request and response of an operation. Querying traces is one of the most efficient methods for locating a fault.

If a problem occurs on the cloud, you can configure filters to search for all suspicious operations in a specified time period. You can then synchronize the relevant traces to O&M and customer service personnel who will handle the problem.

6 Billing

You can use basic functions of CTS for free, including enabling a tracker, tracking traces, as well as storing and querying traces of the last seven days. In addition, CTS works with other services to provide you with value-added functions such as trace file transfer and encryption. These functions may generate fees in other cloud services.

Value-added functions:

- Trace transfer: You can permanently store trace files in Object Storage Service (OBS) buckets.
- Trace file encryption: After enabling trace transfer, you can use Data Encryption Workshop (DEW) to encrypt trace files stored in OBS buckets.
- Trace analysis: This function is provided by CTS and is free to use. However, it depends on log storage of Log Tank Service (LTS), which may generate fees.

7 Permissions Management

You can use Identity and Access Management (IAM) to manage CTS permissions and control access to your resources. IAM provides identity authentication, permissions management, and access control.

You can create IAM users for your employees, and assign permissions to these users on a principle of least privilege (PoLP) basis to control their access to specific resource types. For example, you can create IAM users for software developers and assign specific permissions to allow them to use CTS resources but prevent them from deleting resources or performing any high-risk operations.

If your Huawei Cloud accountaccount does not require individual IAM users for permissions management, skip this section.

IAM can be used free of charge. You pay only for the resources in your account.

CTS Permissions

By default, new IAM users do not have any permissions assigned. To assign permissions to these new users, add them to one or more groups, and attach permissions policies or roles to these groups.

CTS is a project-level service deployed and accessed in specific physical regions. When assigning CTS permissions to a user group, specify region-specific projects where the permissions will take effect. If you select **All projects**, the permissions will be granted for all region-specific projects. When accessing CTS, the users need to switch to a region where they have been authorized to use this service.

You can grant users permissions by using roles and policies. Currently, only authorization by roles is supported in CTS.

- Roles: A type of coarse-grained authorization mechanism that provides only a limited number of service-level roles. When using roles to grant permissions, you also need to assign dependency roles.
- Policies: A type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions. This mechanism allows for more flexible policy-based authorization for more secure access control. For example, you can grant ECS users only the permissions for managing a certain type of ECSs. Most policies define permissions based on APIs.

For the API actions supported by CTS, see **Table 7-1**.

Table 7-1 System-defined roles and policies supported by CTS

Role/ Policy Name	Description	Type	Dependency
CTS FullAccess	Full permissions for CTS.	System-defined policy	None
CTS ReadOnlyAccess	Read-only permissions for CTS.	System-defined policy	None
CTS Administrator	Administrator permissions for CTS. Users granted these permissions can perform all operations on CTS.	System-defined role	The **Tenant Guest** and **OBS Administrator** roles need to be assigned in the same project.

Precautions

- To enable CTS, you must have the **Security Administrator** permissions and full permissions for CTS (**CTS FullAccess** is recommended). For details about how to enable CTS, see section "Enabling CTS" in the *Cloud Trace Service Getting Started*. For details about how to assign permissions, see **Assigning Permissions to an IAM User**.
- To use CTS after CTS is enabled, you only need to have related CTS permissions. The **Security Administrator** permissions are not required.

8 Constraints

There are fixed quotas on the number of trackers and key event notifications in CTS.

Table 8-1 CTS constraints

Item	Quota	Changeable
Management tracker	1	No
Data tracker	100	No
Key event notification	100	No