Cloud Trace Service

Service Overview

Issue 01

Date 2024-03-19

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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

Notice

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

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

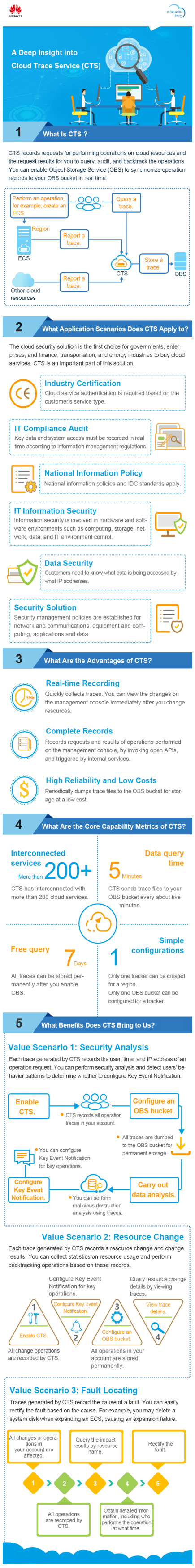
Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 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.

Perform an operation, for example, create an ECS.

Query a trace.

Region

ECS

Report a trace.

CTS

Store a trace.

OBS

Other cloud resources

Report a trace.

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?

Interconnected services
More than 200+
CTS has interconnected with more than 200 cloud services.

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

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

Simple configurations
1
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 traces are dumped to the OBS bucket for permanent storage.

Carry out data analysis.
- You can perform malicious destruction analysis using traces.

Configure Key Event Notification.
- You can configure Key Event Notification for key operations.

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.

1 Enable CTS.
All change operations are recorded by CTS.

2 Configure Key Event Notification.
Configure Key Event Notification for key operations.

3 Configure an OBS bucket.
All operations in your account are stored permanently.

4 View trace details.
Query resource change details by viewing traces.

Value Scenario 3: Fault Locating

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

1 All changes or operations in your account are affected.

2 All operations are recorded by CTS.

3 Query the impact results by resource name.

4 Obtain detailed information, including who performs the operation at what time.

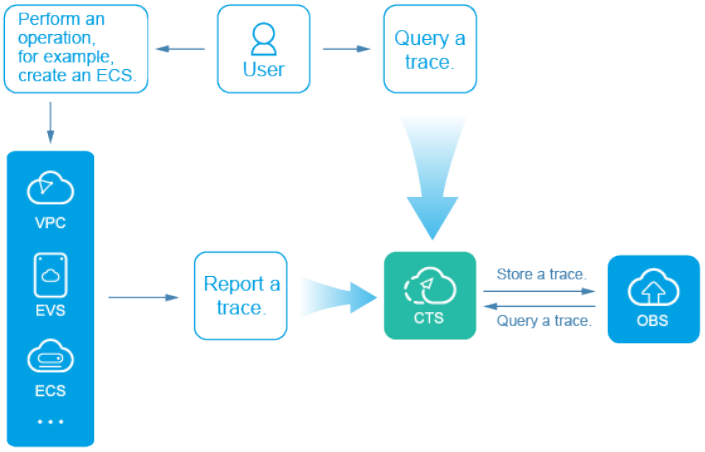
5 Rectify the fault.

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.

Cloud Trace Service (CTS) is a log audit service for Huawei 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 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 can be transferred to Object Storage Service (OBS) buckets or Log Tank Service (LTS) log streams periodically. During transfer, 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.
- Key event notification: CTS works with Simple Message Notification (SMN) to send notifications to your mobile phones and email addresses to notify you of certain key operations.

3 Basic Concepts

Trackers

When you enable CTS for the first time, a management tracker named **system** is created automatically. You can also manually create multiple data trackers on the **Tracker List** page.

Th management tracker identifies and associates with all cloud services your tenant account is using, and records all operations of your tenant account. Data trackers record details of the tenant's operations on data in OBS buckets.

A management tracker and 100 data trackers can be created for a 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 (in the last hour by default) on cloud service resources, including creation, modification, and deletion, but do not record query operations. There are two types of traces:

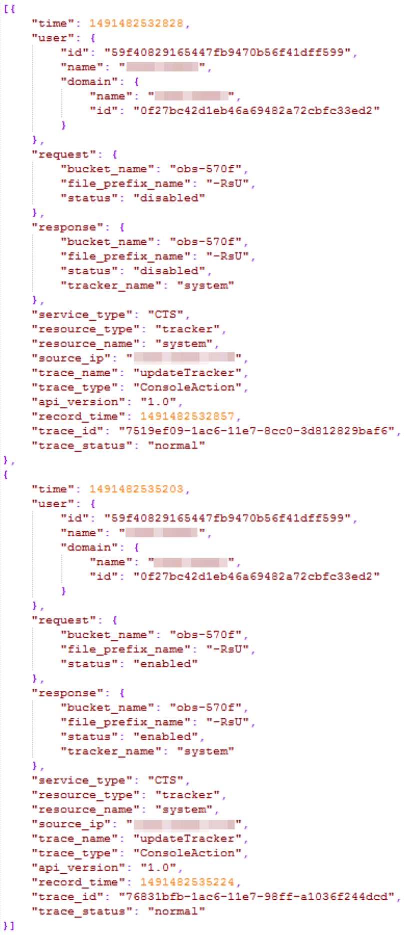
- Management traces: record details about creating, configuring, and deleting cloud service resources in your tenant account.
- Data traces: record operations on data in OBS buckets, such as data upload and download.

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.

Traces files are in JSON format. **Figure 3-1** 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) of the public cloud 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.

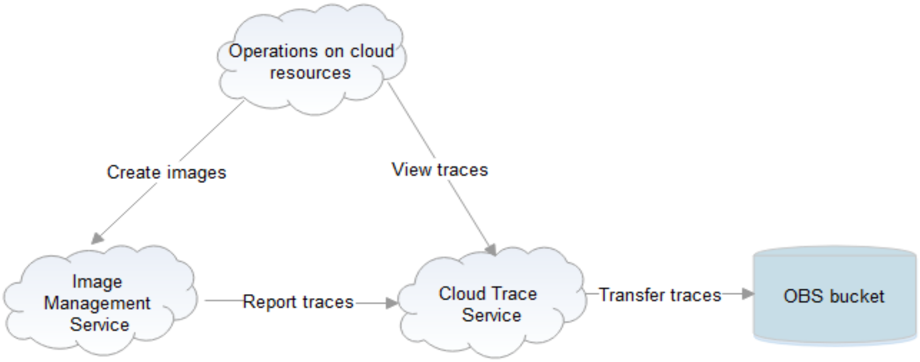
You can use CTS to create trackers to record trace files. If trace transfer has been configured, trace files will be stored in the OBS bucket that you have specified.

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 in the last seven days on the **Trace List** page by time and other filters.
  - 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 compliance. The service records operations of almost all services and resources, 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 workforce 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 Security

6.1 Shared Responsibilities

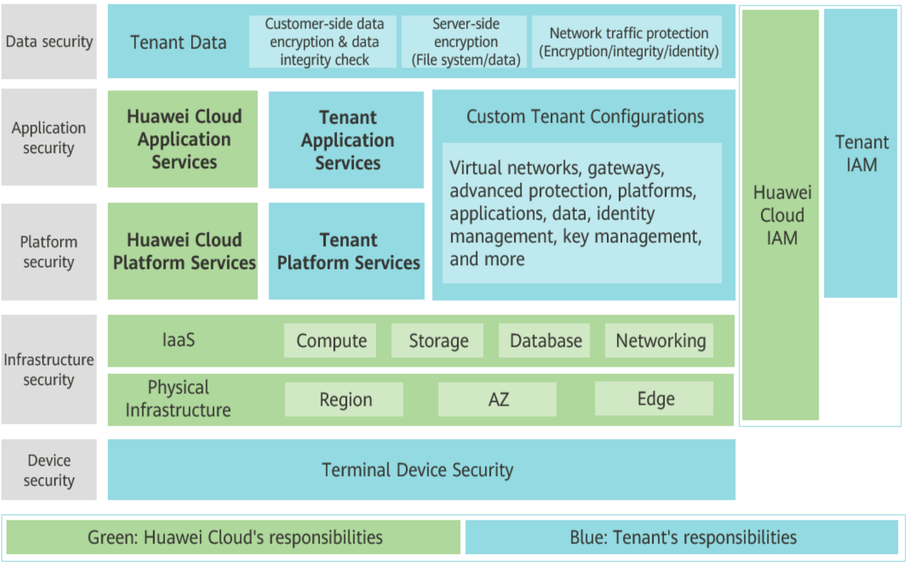
Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system for different regions and industries based on Huawei's unique software and hardware advantages, laws, regulations, industry standards, and security ecosystem.

Figure 6-1 illustrates the responsibilities shared by Huawei Cloud and users.

- **Huawei Cloud**: Ensure the security of cloud services and provide secure clouds. Huawei Cloud's security responsibilities include ensuring the security of our IaaS, PaaS, and SaaS services, as well as the physical environments of the Huawei Cloud data centers where our IaaS, PaaS, and SaaS services operate. Huawei Cloud is responsible for not only the security functions and performance of our infrastructure, cloud services, and technologies, but also for the overall cloud O&M security and, in the broader sense, the security and compliance of our infrastructure and services.
- **Tenant**: Use the cloud securely. Tenants of Huawei Cloud are responsible for the secure and effective management of the tenant-customized configurations of cloud services including IaaS, PaaS, and SaaS. This includes but is not limited to virtual networks, the OS of virtual machine hosts and guests, virtual firewalls, API Gateway, advanced security services, all types of cloud services, tenant data, identity accounts, and key management.

Huawei Cloud Security White Paper elaborates on the ideas and measures for building Huawei Cloud security, including cloud security strategies, the shared responsibility model, compliance and privacy, security organizations and personnel, infrastructure security, tenant service and security, engineering security, O&M security, and ecosystem security.

Figure 6-1 Huawei Cloud shared security responsibility model


Data security
Tenant Data
Customer-side data encryption & data integrity check
Server-side encryption (File system/data)
Network traffic protection (Encryption/integrity/identity)
Application security
Huawei Cloud Application Services
Tenant Application Services
Custom Tenant Configurations
Virtual networks, gateways, advanced protection, platforms, applications, data, identity management, key management, and more
Platform security
Huawei Cloud Platform Services
Tenant Platform Services
Infrastructure security
IaaS
Compute
Storage
Database
Networking
Physical Infrastructure
Region
AZ
Edge
Device security
Terminal Device Security
Huawei Cloud IAM
Tenant IAM
Green: Huawei Cloud's responsibilities
Blue: Tenant's responsibilities

6.2 Identity Authentication and Access Control

Identity Authentication

No matter whether you access CTS through the console or APIs, you are required to provide the identity credential and verify the identity validity. In addition, login and login authentication policies are provided to harden identity authentication security. CTS uses Identity and Access Management (IAM) for three identity authentication modes: **passwords**, **access keys**, and **temporary access keys**. **Login protection** and **login authentication policies** are provided.

Access Control

To assign different CTS access permissions to employees in your enterprise, IAM is a good choice for refined permissions management. IAM provides identity authentication, permissions management, and access control, helping you secure access to your Huawei Cloud resources. For details, see **Permissions Management**.

6.3 Data Protection

CTS takes many measures to keep data secure and reliable.

Table 6-1 CTS data protection measures

Measure	Description	Reference
Transmission encryption (HTTPS)	CTS supports HTTPS for enhanced data transmission security.	**Making an API Request**

Measure	Description	Reference
Data redundancy	Audit logs are stored in multiple copies for data reliability.	--
Transferring data to Object Storage Service (OBS)	CTS can transfer logs to OBS, so you can store logs for a longer period of time at a lower cost. You can use encrypted OBS buckets to protect data.	**Creating a Tracker**
Verifying trace file integrity	During a security audit, operation records cannot serve as effective and authentic evidence if trace files have been deleted or tampered with. You can enable integrity verification in CTS to ensure the authenticity of trace files.	**Enabling Verification of Trace File Integrity**

6.4 Auditing and Logs

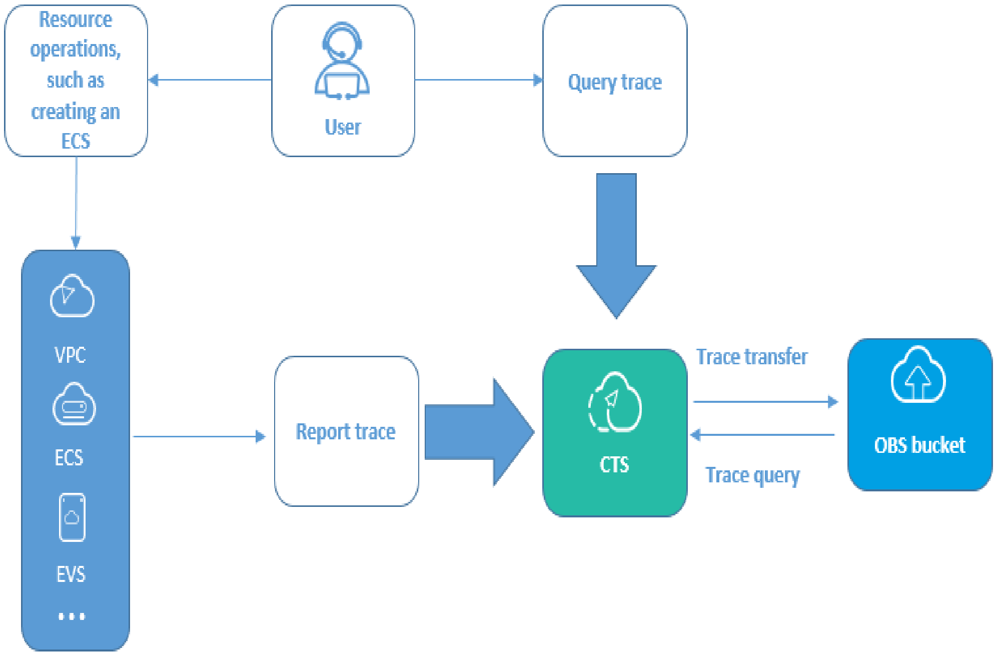
CTS is a log audit service for Huawei Cloud security. It allows you to collect, store, and query cloud resource operation records. You can use these records to perform security analysis, audit compliance, trace resource changes, and locate faults.

After you create and configure a tracker on the CTS console, CTS records management traces of CTS for auditing.

For details about getting started with CTS and basic operations, see **Enabling CTS**.

For details about CTS management traces that can be tracked by CTS, see section **Auditing** in the *User Guide*.

Figure 6-2 CTS



6.5 Resilience

CTS provides a three-level reliability architecture and uses intra-AZ instance disaster recovery (DR), dual-AZ DR, and multiple log data copies to ensure service durability and reliability.

Table 6-2 CTS reliability architecture

Reliability Solution	Description
Intra-AZ instance DR	In a single AZ, CTS implements instance DR in multi-instance mode and quickly rectifies faults to continuously provide services.
Multi-AZ DR	CTS supports cross-AZ DR. An AZ fault does not interrupt continuous services.
Data DR	Multiple copies of log data are used to implement data DR.

6.6 Security Risks Monitoring

CTS monitors security risks through key event notifications for data security and reliability.

Table 6-3 Risks monitoring

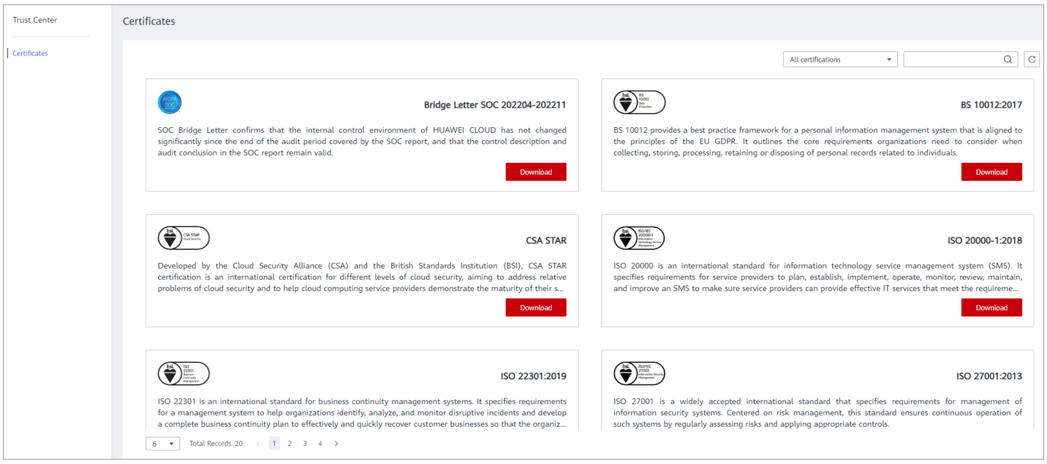
Security Risks Monitoring	Description	Reference
Key event notifications	You can create key event notifications on CTS so that Simple Message Notification (SMN) sends you notifications of key events. This function is triggered by CTS, and notifications are sent by SMN.	**Key Event Notifications**

6.7 Certificates

Compliance Certificates

Huawei Cloud services and platforms have obtained various security and compliance certifications from authoritative organizations, such as International Organization for Standardization (ISO). You can **download** them from the console.

Figure 6-3 Downloading compliance certificates



Bridge Letter SOC 202204-202211

SOC Bridge Letter confirms that the internal control environment of HUAWEI CLOUD has not changed significantly since the end of the audit period covered by the SOC report, and that the control description and audit conclusion in the SOC report remain valid.

BS 10012:2017

BS 10012 provides a best practice framework for a personal information management system that is aligned to the principles of the EU GDPR. It outlines the core requirements organizations need to consider when collecting, storing, processing, retaining or disposing of personal records related to individuals.

CSA STAR

Developed by the Cloud Security Alliance (CSA) and the British Standards Institution (BSI), CSA STAR certification is an international certification for different levels of cloud security, aiming to address relative problems of cloud security and to help cloud computing service providers demonstrate the maturity of their s...

ISO 20000-1:2018

ISO 20000 is an international standard for information technology service management system (SMS). It specifies requirements for service providers to plan, establish, implement, operate, monitor, review, maintain, and improve an SMS to make sure service providers can provide effective IT services that meet the requireme...

ISO 22301:2019

ISO 22301 is an international standard for business continuity management systems. It specifies requirements for a management system to help organizations identify, analyze, and monitor disruptive incidents and develop a complete business continuity plan to effectively and quickly recover customer businesses so that the organiz...

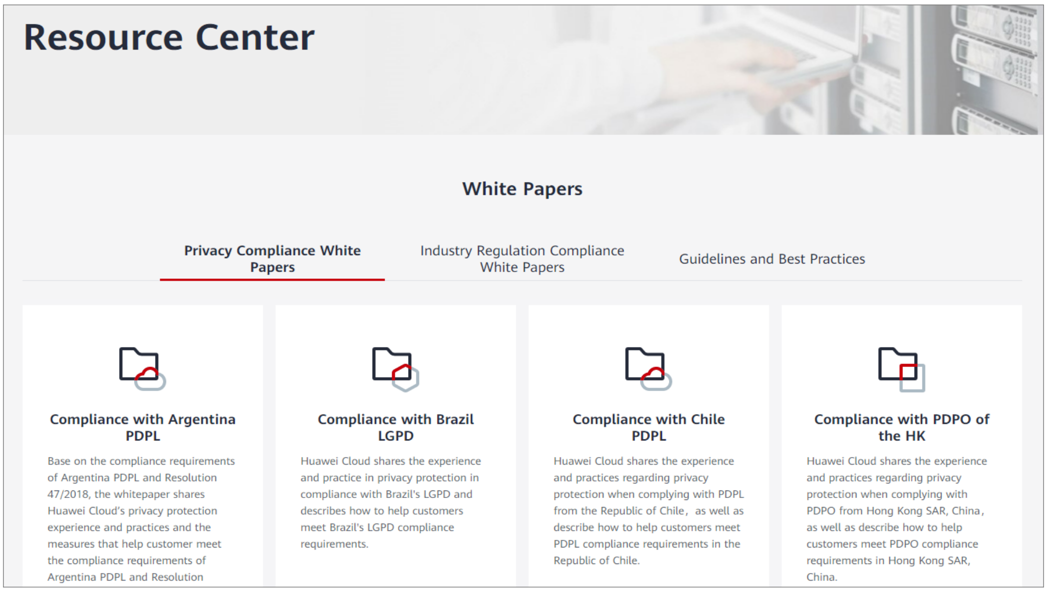
ISO 27001:2013

ISO 27001 is a widely accepted international standard that specifies requirements for management of information security systems. Centered on risk management, this standard ensures continuous operation of such systems by regularly assessing risks and applying appropriate controls.

Resource Center

Huawei Cloud also provides the following resources to help users meet compliance requirements. For details, see **Resource Center**.

Figure 6-4 Resource center



Resource Center

White Papers

Privacy Compliance White Papers | Industry Regulation Compliance White Papers | Guidelines and Best Practices

Compliance with Argentina PDPL

Base on the compliance requirements of Argentina PDPL and Resolution 47/2018, the whitepaper shares Huawei Cloud's privacy protection experience and practices and the measures that help customer meet the compliance requirements of Argentina PDPL and Resolution

Compliance with Brazil LGPD

Huawei Cloud shares the experience and practice in privacy protection in compliance with Brazil's LGPD and describes how to help customers meet Brazil's LGPD compliance requirements.

Compliance with Chile PDPL

Huawei Cloud shares the experience and practices regarding privacy protection when complying with PDPL from the Republic of Chile, as well as describe how to help customers meet PDPL compliance requirements in the Republic of Chile.

Compliance with PDPO of the HK

Huawei Cloud shares the experience and practices regarding privacy protection when complying with PDPO from Hong Kong SAR, China, as well as describe how to help customers meet PDPO compliance requirements in Hong Kong SAR, China.

6.8 Organizations Trusted Services

What Is a Trusted Service?

The Organizations service helps you govern multiple accounts within your organization. It enables you to consolidate multiple Huawei Cloud accounts into an organization that you create and centrally manage these accounts. You can use Service Control Policies (SCPs) to control the maximum available permissions for all accounts in your organization. This helps you better meet the service security and compliance requirements of your business.

A trusted service is a Huawei Cloud service that is entrusted by Organizations to provide organizational capabilities. You can use the management account in Organizations to enable trusted services. Each trusted service has access to the information about the organization units (OUs) and member accounts in your organization and also can manage the entire organization.

CTS supports multi-account management of Organizations.

1. Use an organization administrator account to set CTS as a trusted service on the Organizations console and specify a delegated administrator account.
2. You can use the delegated administrator account to configure an organization tracker in CTS. Then the delegated administrator account can implement cloud audit capabilities, such as security audit. Audit logs of all members in the organization in the current region will be transferred to the OBS bucket or LTS log stream configured for the tracker.

Helpful Links

What Is Organizations?

What Is a Trusted Service?

Application Scenarios of Organizations

Functions of Organizations

7 Billing

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

Value-added functions:

- Trace transfer: You can configure a tracker to transfer trace files to OBS buckets. Trace files transferred by the management tracker are permanently stored, and trace files transferred by a data tracker are stored for a specified period.
- 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.
- Key event notification: CTS provides the key event notification function to send notifications to your mobile phones and email addresses when specific operations are performed. You need to subscribe to topics on the Simple Message Notification (SMN) console for this function to take effect.

8 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.

With IAM, you can use your Huawei Cloud account to create IAM users for your employees, and assign permissions to the users 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 account does not require IAM users for permissions management, you may skip this section.

IAM can be used free of charge. You pay only for the resources in your account. For details, see **IAM Service Overview**.

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.

- 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. Roles are not an ideal choice for fine-grained authorization and secure access control.
- 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 8-1**.

Table 8-1 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. Users with this permission can perform read-only operations on all services except IAM.	System-defined role	This role must be used together with the **Tenant Guest** and **OBS Administrator** roles in the same project.

Table 8-2 lists the common operations supported by each system-defined policy or role of CTS. Select the policies or roles as required.

Table 8-2 Common operations supported by system-defined policies or roles

Operation	CTS FullAccess	CTS ReadOnlyAccess	CTS Administrator
Querying traces	√	√	√
Querying quotas	√	√	√
Creating a tracker	√	×	√
Modifying a tracker	√	×	√
Disabling a tracker	√	×	√
Enabling a tracker	√	×	√
Querying a tracker	√	√	√

Operation	CTS FullAccess	CTS ReadOnlyAccess	CTS Administrator
Deleting a tracker	√	×	√
Creating a key event notification	√	×	√
Modifying a key event notification	√	×	√
Disabling a key event notification	√	×	√
Enabling a key event notification	√	×	√
Querying a key event notification	√	√	√
Deleting a key event notification	√	×	√

Fine-grained Permissions

To use a custom fine-grained policy, log in to IAM as the administrator and select fine-grained permissions of CTS as required. For details about fine-grained permissions of CTS, see **Table 8-3**.

Table 8-3 CTS fine-grained permissions

Permission	Description	Dependency	Application Scenario
cts:quota:get	Querying the tracker quota of a tenant	-	Querying the tracker quota of a tenant
cts:trace:list	Querying real-time traces	-	Querying records of operations on resources in the last seven days
cts:trace:listResource		-	
cts:trace:listTraceUser		-	

Permission	Description	Dependency	Application Scenario
cts:notification:create	Creating a key event notification	smn:topic:listTopic iam:agencies:listAgencies iam:agencies:createAgency iam:permissions:grantRoleToAgencyOnProject iam:permissions:listRolesForAgencyOnProject iam:projects:listProjects iam:groups:listGroups iam:users:listUsers iam:users:listUsersForGroup	Creating a key event notification
cts:notification:update	Modifying a key event notification		Modifying a key event notification
cts:notification:delete	Deleting a key event notification	-	Deleting a key event notification
cts:notification:list	Querying all key event notifications	-	Querying all key event notifications
cts:tracker:delete	Deleting a tracker	-	Deleting a created tracker

Permission	Description	Dependency	Application Scenario
cts:tracker:update	Updating a tracker	iam:agencies:listAgencies iam:agencies:createAgency iam:permissions:grantRoleToAgencyOnProject iam:permissions:listRolesForAgencyOnProject iam:projects:listProjects iam:groups:listGroups iam:users:listUsersForGroup lts:topics:list lts:topics:create lts:topics:get lts:logstreams:list lts:groups:get lts:groups:list lts:groups:create obs:bucket:CreateBucket obs:bucket:HeadBucket obs:bucket:GetLifecycleConfiguration obs:bucket:PutLifecycleConfiguration obs:bucket:GetBucketAcl obs:bucket:PutBucketAcl obs:bucket:ListAllMyBuckets kms:cmk:list kms:cmk:get eps:enterpriseProjects:list organizations:trustedServices:list organizations:organizations:get organizations:deletgatedAdministrators:list organizations:accounts:list organizations:deletgatedServices:list	Modifying configurations of a created tracker
cts:tracker:create	Creating a tracker		Creating a tracker to associate all operations recorded by the system

Permission	Description	Dependency	Application Scenario
cts:tracker:list	Querying all trackers	obs:bucket:GetBucketAcl obs:bucket:ListAllMyBuckets	Viewing details of trackers
cts:tag:create	Adding resource tags in batches	-	Adding resource tags in batches
cts:tag:delete	Deleting resource tags in batches	-	Deleting resource tags in batches

Custom Permissions Policies

You can create custom permissions policies to supplement the system-defined policies.

- For the actions that can be configured in custom permissions policies, see **Permissions Policies and Supported Actions**.
- For details, see **Creating a Custom Policy**.

Helpful Links

- **IAM Service Overview**
- **IAM Basic Concepts**
- **Creating a User Group and User and Granting CTS Permissions**

9 Constraints

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

Table 9-1 CTS constraints

Item	Maximum Value
Maximum number of trackers that can be created by a Huawei Cloud account	Management tracker: 1 Data trackers: 100
Maximum number of key event notifications that can be configured by a Huawei Cloud account	100
Maximum number of OBS buckets that can be configured for a tracker	1
Time from when an operation is performed to when the operation data can be queried on the console	Management traces: 1 minute Data traces: 5 minutes
Time from when a member quits or is removed from an organization to when the organization tracker is withdrawn.	5 minutes
Time period in which traces can be queried on the console **NOTE** By default, CTS only records traces generated in the last seven days for each Huawei Cloud account. To store races generated seven days ago, you need to transfer them.	7 days