Cloud Trace Service

Service Overview

Issue 01
Date 2020-04-28
Contents

1 What Is Cloud Trace Service?................................................................. 1
2 Basic Concepts.................................................................................. 3
3 How CTS Functions........................................................................ 6
4 Application Scenarios.................................................................... 8
5 Service Pricing................................................................................ 10
6 Permissions Management............................................................... 11
7 What's New....................................................................................... 13
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 information systems migrate 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 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 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 type, trace source, resource type, search by, 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.
Basic Concepts

Trackers

Before using CTS, you must 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.

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 reported by OBS. (OBS is deployed in an independent region and isolated from other services. Traces reported by OBS are called data traces.)

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 generated in the last seven days.

Trace Files

A trace file is a collection of traces. CTS automatically generates multiple trace files by service and transfer period and then synchronizes these files to OBS buckets you specified.

Generally, all traces of a service generated during a transfer period 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.

Trace files are in JSON format. Figure 1 shows an example of a trace file.
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 the function of verifying trace file integrity, which is designed 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.
Cloud Trace Service (CTS) interconnects directly with other cloud services of HUAWEI CLOUD and records operations performed on cloud resources and operation results in real time. It delivers records in the form of trace files to Object Storage Service (OBS) buckets.

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

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 trace files to CTS for archiving.
  - Operation records of the last seven days are displayed on the CTS console. If OBS 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 the OBS service has been enabled.
  - You can enable, disable, configure, 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 if OBS has been enabled. You can view trace files in the trace list. **Figure 1** shows the working principle of CTS.
Figure 3-1 How CTS functions

- An operation on cloud resources
- Create an image
- View a trace
- Reports a trace
- Stores a trace

Cloud Trace Service
Service Overview

Issue 01 (2020-04-28)  Copyright © Huawei Technologies Co., Ltd. 7
CTS is mainly used in the following scenarios:

**Compliance Audit**

CTS helps your service systems easily pass classified protection compliance, PCI DSS, ISO 27001, and other industry-standard audit certifications.

To migrate services to the cloud, auditing compliance certification is divided into two parts: compliance certification of carriers' service systems and resources and compliance certification of your service systems.

CTS provides core assurance for the compliance of carriers' service systems and resources. It can record operations of almost all services and resources, protecting audit logs during transmission, storage, encryption, disaster recovery, and tamper protection. CTS also helps your service systems pass compliance certification.

**Key Event Notification**

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 enables you mine value data in traces to provide support for service health analysis, risk analysis, resource tracking, and cost analysis. In addition, you can obtain audit data from CTS and explore values of the data yourself.

A trace contains 19 fields, including the time, operator, operation device IP address, operated resource, operation details, and other information. Each trace is worth mining.
By configuring HTTP or HTTPS notifications, you can synchronize traces to your own system for analysis. In addition, CTS is currently being interconnected with Cloud Eye Service (CES) and Log Tank Service (LTS) to provide functions such as high-risk operation display, unauthorized operation analysis, resource usage distribution, as well as data support for service health analysis and cost analysis.

**Fault Location and Analysis**

You can configure query 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, search by, 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 when you migrate your services to the cloud, you can configure filters to search for all suspicious operations in a specified time period. You can then synchronize the associated audit logs to O&M and customer service personnel who will handle the problem.
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 can also work with other cloud services to provide you with value-added services, such as trace transferring and trace encryption. These value-added services may incur additional fees that are included in the fees of the associated service. Generally, the fees of value-added services are low. Therefore, you are advised to use the services together as required.

The following are some value-added services:

- Trace transfer: You can enable OBS to permanently store traces in OBS buckets.
- Trace file encryption and storage: After enabling the trace transferring function, you use DEW to encrypt trace files stored in OBS buckets.

For details about value-added service fees, see Product Pricing Details.
If you need to assign different permissions to employees in your enterprise to access your CTS resources, Identity and Access Management (IAM) is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, securing access to your HUAWEI CLOUD resources.

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, software developers in your enterprise may need to use CTS resources but must not delete them or perform any high-risk operations. To ensure this, you can create IAM users for the software developers and grant them only the permissions required for using CTS resources.

If your HUAWEI CLOUD account does not require individual 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.

**CTS Permissions**

By default, new IAM users do not have any permissions assigned. You must add them to user groups and assign permissions policies or roles to these groups. Users then inherit permissions from the groups. This process is called authorization. Users can perform specified operations on cloud services based on their assigned permissions.

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

Policies are 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, meeting requirements for secure access control. For example, you can grant Elastic Cloud Server (ECS) users only the permissions for managing a certain type of ECS. Most fine-grained policies divide permissions by API.
Table 6-1 lists all the system permissions supported by CTS.

**Table 6-1 CTS system permissions**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Policy Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTS Administrator</td>
<td>Administrator permissions of CTS</td>
<td>System-defined role</td>
</tr>
</tbody>
</table>
## 7 What's New

### Table 7-1 What's new

<table>
<thead>
<tr>
<th>Released On</th>
<th>Description</th>
</tr>
</thead>
</table>
| 2019-08-15  | - Cloud Trace Service (CTS) console is separated from the Log Tank Service (LTS) console. LTS console is an independent console now.  
- Both management traces and data traces can be displayed in the trace list.  
- Traces can be displayed by region and global. |