Cloud Trace Service

Best Practices

Issue	01
Date	2025-01-06

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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 Auditing and Analyzing Logins and Logouts with FunctionGraph

1.1 Introduction

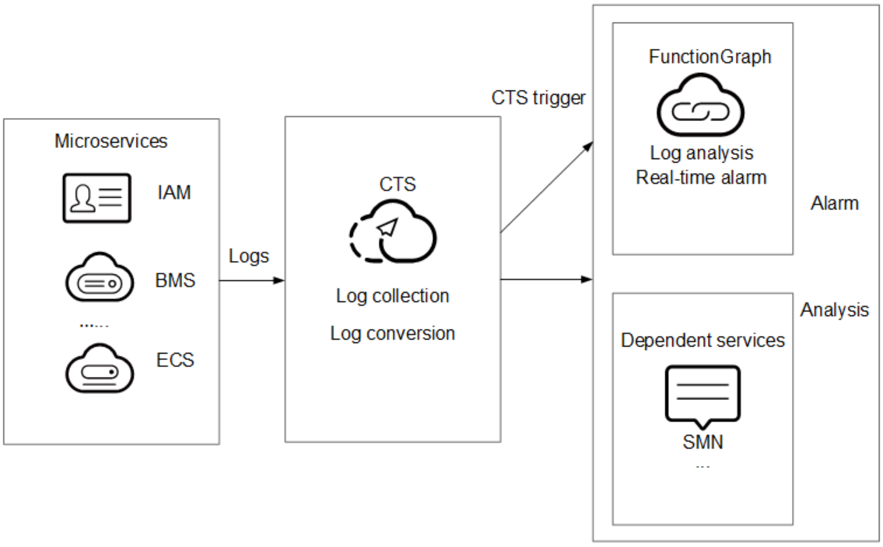
Scenarios

Collect real-time records of operations on cloud resources.

Create a Cloud Trace Service (CTS) trigger to obtain records of subscribed cloud resource operations; analyze and process the operation records, and report alarms.

Use SMN to push alarm messages to service personnel by SMS message or email. The processing workflow is shown in **Figure 1-1**.

Figure 1-1 Processing workflow



Values

- Quickly analyzes operation records collected by CTS and filters out operations from specified IP addresses.

- Processes and analyzes data in response to log events in a serverless architecture, which features automatic scaling, no operation and maintenance, and pay-per-use billing.
- Sends alarm notifications through SMN.

1.2 Preparation

Enabling CTS for the First Time

Step 1 Log in to the management console.

Step 2 If you log in to Huawei Cloud as an administrator, go to **Step 3**. If you log in to Huawei Cloud as an IAM user, first contact your CTS administrator (account owner or a user in the **admin** user group) to obtain the **CTS FullAccess** permissions.

For details, see **Assigning Permissions to an IAM User**.

Step 3 Click ☰ in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.

Step 4 Choose **Tracker List** in the navigation pane on the left and click **Enable CTS** in the upper right corner. A management tracker named **system** will be automatically created.

NOTE

The management tracker records management traces, which are operations on all cloud resources, such as creation, login, and deletion. For details about the cloud services supported by CTS, see **Supported Services and Operations**.

----End

Creating an Agency

Step 1 Log in to the **IAM console**, and choose **Agencies** in the navigation pane.

Step 2 On the **Agencies** page, click **Create Agency**.

Step 3 Set the agency information.

- For **Agency Name**: Enter an agency name, for example, **serverless_trust**.
- For **Agency Type**, select **Cloud service**.
- For **Cloud Service**, select **FunctionGraph**.
- For **Validity Period**, select **Unlimited**.
- For **Description**, enter a description.

Step 4 Click **Next**. On the **Select Policy/Role** page, select **CTS Administrator** and **SMN Administrator**.

NOTE

- **SMN Administrator**: Users with this permission can perform any operation on SMN resources.
- **CTS Administrator** depends on **Tenant Guest**. When you select the former, the latter will also be selected.

Step 5 Click **Next**, select an authorization scope that meets your service requirements, and click **OK**.

----End

Pushing Alarm Messages

- Create a topic named **cts_test** on the SMN console. For details, see **Creating a Topic**.
- Add subscriptions to the **cts_test** topic to push alarm messages. For details, see **Adding a Subscription**.

NOTE

Alarm messages of a subscribed topic can be pushed through emails, SMS messages, and HTTP/HTTPS.

In this example, when operation log events trigger the specified function, the function filters operations that are performed by users not in the IP address whitelist, and pushes alarm messages to the subscription endpoints.

1.3 Building a Program

Download index.zip to create an alarm log analysis function from scratch.

Creating a Function

Create a function by uploading the **sample code package** to extract logs. Select the Python 2.7 runtime and the agency **serverless_trust** created in **Creating an Agency**. For details about how to create a function, see **Creating an Event Function**.

This function analyzes received operation records, filters logins or logouts from unauthorized IP addresses using a whitelist, and sends alarms under a specified SMN topic. This function can be used to build an account security monitoring service.

Setting Environment Variables

On the **Configuration** tab page of the function details page, set the environment variables listed in **Table 1-1**.

Table 1-1 Environment variables

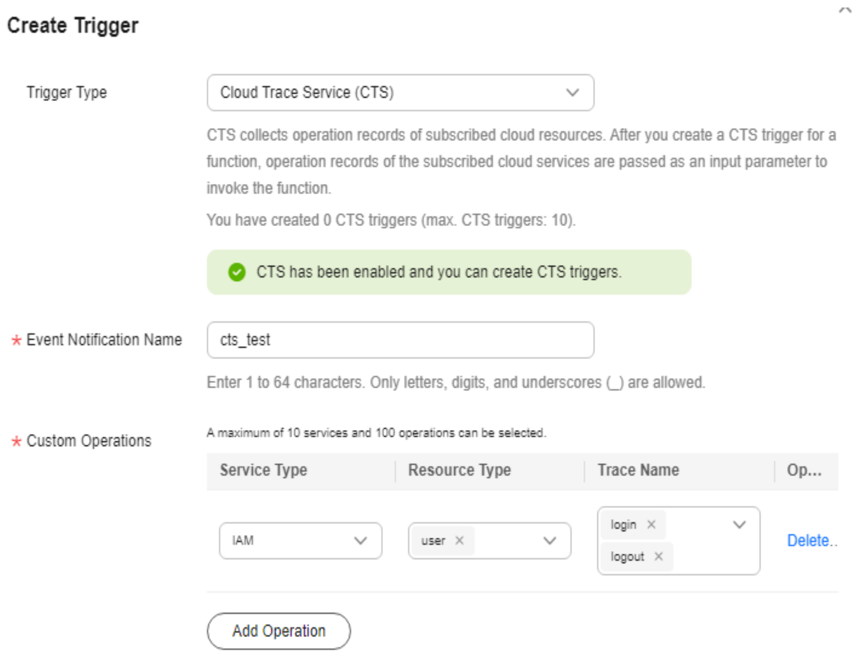
Environment Variable	Description
SMN_Topic	SMN topic.
RegionName	Region name.
IP	IP address whitelist.

Set the environment variables by following the procedure in **Environment Variables**.

1.4 Adding an Event Source

Create a CTS trigger, as shown in **Figure 1-2**.

Figure 1-2 Creating a CTS trigger



Create Trigger

Trigger Type: Cloud Trace Service (CTS)

CTS collects operation records of subscribed cloud resources. After you create a CTS trigger for a function, operation records of the subscribed cloud services are passed as an input parameter to invoke the function.

You have created 0 CTS triggers (max. CTS triggers: 10).

CTS has been enabled and you can create CTS triggers.

* Event Notification Name: cts_test

Enter 1 to 64 characters. Only letters, digits, and underscores (_) are allowed.

* Custom Operations

A maximum of 10 services and 100 operations can be selected.

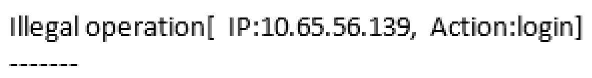
Service Type	Resource Type	Trace Name	Op...
IAM	user	login logout	Delete..

CTS records the logins and logouts of users on IAM.

1.5 Processing Operation Records

The function runs in response to account logins and logouts to filter those not from the IP address whitelist, and sends a message or email through SMN, as shown in **Figure 1-3**.

Figure 1-3 Email notification

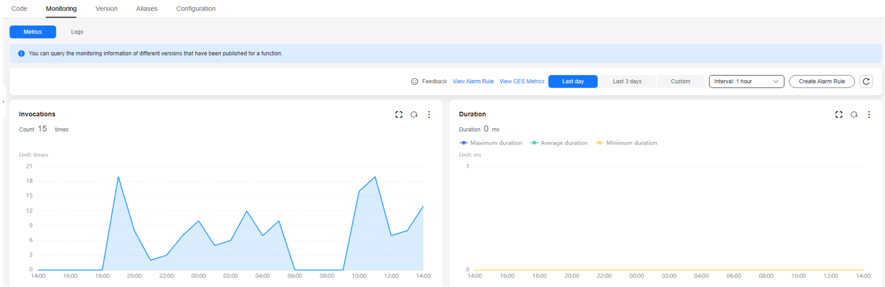


```
Illegal operation[ IP:10.65.56.139, Action:login]
-------
```

The email contains the unauthorized IP address and user operation (login or logout).

On the **Monitoring** tab page of the function, check the number of invocations, as shown in **Figure 1-4**.

Figure 1-4 Function metrics



You can query the monitoring information of different versions that have been published for a function.

Interval: 1 hour

Invocations

Count 15 times

Duration

Duration 0 ms