

**Cloud Trace Service**

# **Best Practices**

**Date**      **2022-09-30**

---

# Contents

---

<b>1 Auditing and Analyzing Logins and Logouts with FunctionGraph.....</b>	<b>1</b>
1.1 Introduction.....	1
1.2 Preparation.....	2
1.3 Building a Program.....	3
1.4 Adding an Event Source.....	5
1.5 Processing Operation Records.....	5

# 1 Auditing and Analyzing Logins and Logouts with FunctionGraph

## 1.1 Introduction

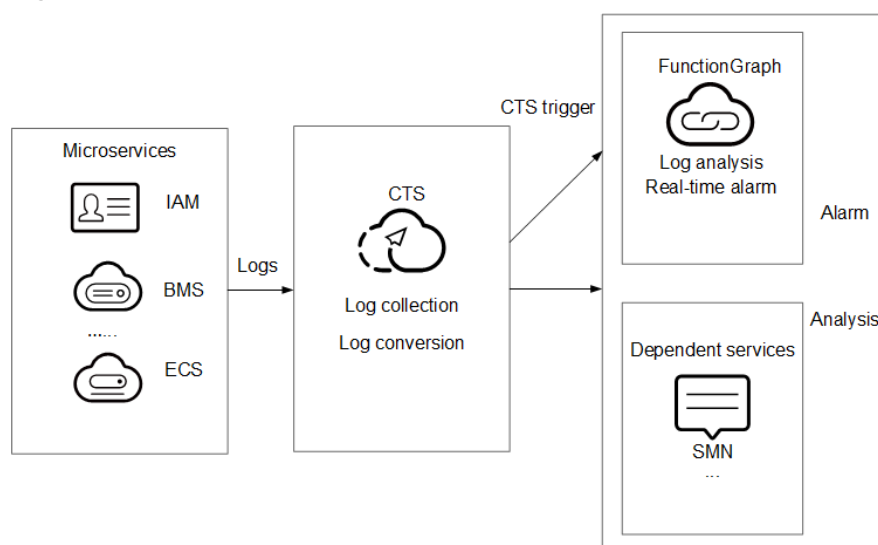
### Description

Cloud Trace Service (CTS) collects real-time records of operations on cloud resources.

You can create a CTS trigger to obtain records of subscribed cloud resource operations, analyze and process the operation records, and report alarms.

You can use Simple Message Notification (SMN) to push alarm messages to service personnel by SMS message or email. [Figure 1-1](#) shows the procedure.

**Figure 1-1** Flowchart





## Values

- Operation records collected by CTS can be quickly analyzed and operations from specified IP addresses can be filtered out.
- CTS processes and analyzes data in response to log events in a serverless architecture, which features automatic scaling, no O&M, and pay-per-use billing.
- CTS sends alarm notifications through SMN.

## 1.2 Preparation

### Enabling CTS

Configure a tracker, and the system immediately starts recording operations based on the new rule.

1. Log in to the console.
2. Click  in the upper left corner of the console and select a region and a project.
3. Click  in the upper left corner and choose **Management & Governance > Cloud Trace Service**.
4. On the displayed page, choose **Tracker List** in the navigation pane on the left.
5. Locate a data tracker and click **Configure** in the **Operation** column.
  - **Operation:** Select the data operations that need to be recorded.
  - **Transfer to OBS**
    - If you select **Yes**, select an existing OBS bucket or create one directly on the **Configure Tracker** page and set **File Prefix**.
    - If you select **No**, no configuration is required.
  - **Create OBS Bucket:** If this function is enabled, an OBS bucket will be created automatically with the name you enter. If this function is disabled, select an existing OBS bucket.
  - **OBS Bucket:** You can create an OBS bucket or select an existing OBS bucket.
  - **Retention Period:** Select the duration for storing traces in the OBS bucket.
  - **File Prefix:** The prefix is used to mark a transferred trace file. Your specified prefix will be automatically added to the beginning of the name of a transferred file, helping you quickly filter files.
  - **Verify Trace File:** When this function is enabled, integrity verification will be performed to check whether trace files in OBS buckets have been tampered with. For details about how to verify the file integrity, see section "Verifying the Integrity of a CTS Trace File" in the *CTS User Guide*.
6. Click **OK** to complete the tracker configuration.

 NOTE

For details about how to configure a tracker, see section "Configuring a Tracker" in the *CTS User Guide*.

## Creating an Agency

1. Log in to the Identity and Access Management (IAM) console. In the navigation pane on the left, choose **Agencies**.
2. On the **Agencies** page, click **Create Agency**.
3. Set the agency information.
  - For **Agency Name**, enter **serverless\_trust**.
  - For **Agency Type**, select **Cloud service**.
  - For **Cloud service**, select **FunctionGraph**.
  - For **Validity Period**, select **Unlimited**.
  - Click **Assign Permissions**. On the **Assign Permissions** page, select **Tenant Administrator**.

 NOTE

Users with the **Tenant Administrator** permission can perform any operations on all cloud resources of the enterprise.

4. Click **OK**.

## 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 can be sent by emails, SMS messages, and HTTP/HTTPS.
- In this example, when 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 subscribers.

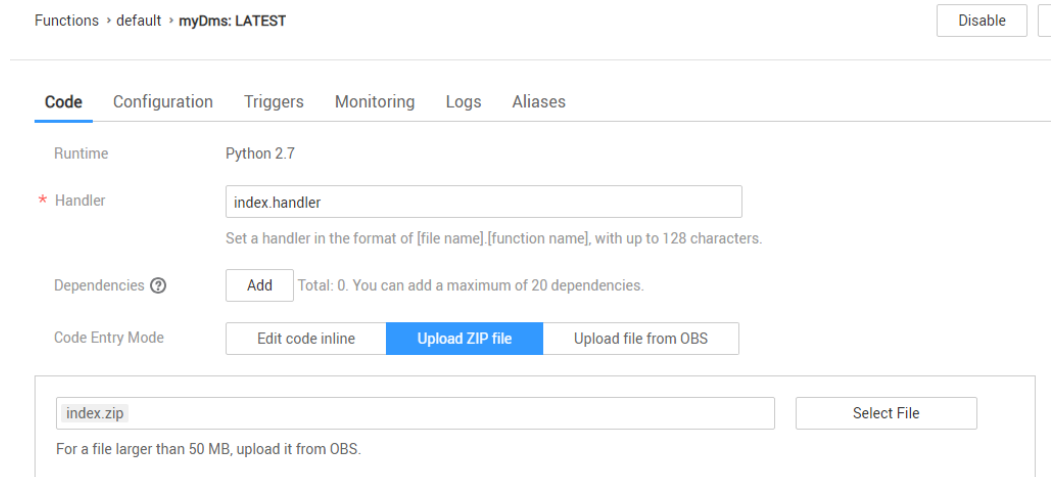
## 1.3 Building a Program

This section describes how to download and use the program package ([index.zip](#)) for log alarms.

### Creating a Function

Create a function for extracting logs and upload the [sample code](#) package, as shown in [Figure 1-2](#). For details, see section "Function Management" in the *FunctionGraph User Guide*.

**Figure 1-2** Creating a 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.

## Setting Environment Variables

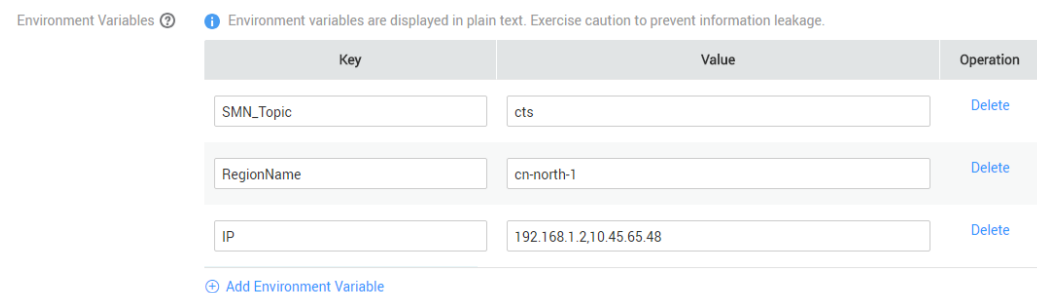
On the **Configuration** tab page of the function, set the environment variables and SMN topic name, as shown in [Table 1-1](#).

**Table 1-1** Environment variable description

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

Set the environment variables ([Figure 1-3](#)) by following the procedure in section "Environment Variables" in the *FunctionGraph User Guide*.

**Figure 1-3** Setting environment variables



## 1.4 Adding an Event Source

Create a CTS trigger, as shown in [Figure 1-4](#). For details, see section "Using a CTS Trigger" in the *FunctionGraph User Guide*.

**Figure 1-4** Creating a CTS trigger

Create Trigger

Trigger Type: CTS  
You can create a maximum of 10 CTS triggers under a project. You have created 2 CTS triggers.

\* Notification Name: cts\_test  
Enter a maximum of 64 characters. Only letters, digits, and underscores (\_) are allowed.

\* Custom Operations: You can add a maximum of 10 services and 100 operations. [Learn more](#).

Service Type	Resource Type	Operation Name	Operation
IAM	user	login	Delete
		logout	

[Add Custom Operation](#)

OK Cancel

CTS records the logins and logouts of users on IAM.

## 1.5 Processing Operation Records

When a user performs login or logout using an account, the subscription service log will be triggered and a function will be directly invoked. The system then checks whether the IP address of the current login or logout account is in the whitelist based on function code. If the IP address is not in the whitelist, SMN will send notifications, as shown in [Figure 1-5](#).

**Figure 1-5** Alarm notification sent by email

```
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 1-6](#).

**Figure 1-6** Function metrics

Functions > ctsMsg: LATEST

Code Configuration Triggers **Monitoring** Logs Aliases

Metrics (last 24 hours)

