

# Cloud Trace Service

## FAQs

**Issue** 01  
**Date** 2023-11-15



**Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2023. All rights reserved.**

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of 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

---

<b>1 Must I Use an IAM User (Sub Account) to Configure Transfer on CTS and Perform Operations on an OBS Bucket?.....</b>	<b>1</b>
<b>2 How Will CTS Be Affected If My Account Is in Arrears?.....</b>	<b>2</b>
<b>3 What Are the Recommended Users of CTS?.....</b>	<b>3</b>
<b>4 What Will Happen If I Have Enabled Trace Transfer But Have Not Configured an Appropriate Policy for an OBS Bucket?.....</b>	<b>4</b>
<b>5 Does CTS Support Integrity Verification of Trace Files?.....</b>	<b>5</b>
<b>6 Why Are There Some Null Fields on the View Trace Page?.....</b>	<b>6</b>
<b>7 Why Is an Operation Recorded Twice in the Trace List?.....</b>	<b>7</b>
<b>8 What Services Are Supported by Key Event Notifications?.....</b>	<b>8</b>
<b>9 How Can I Store Trace Files for a Long Time?.....</b>	<b>9</b>
<b>10 Why Are user and source_ip Null for Some Traces with trace_type as SystemAction?.....</b>	<b>10</b>
<b>11 How Can I Find Out Who Created a Specific ECS?.....</b>	<b>11</b>
<b>12 How Can I Find Out the Login IP Address of an IAM User?.....</b>	<b>12</b>
<b>13 Why Are Two deleteMetadata Traces Generated When I Buy an ECS in Pay-per-Use or Yearly/Monthly?.....</b>	<b>13</b>
<b>14 What Can I Do If I Cannot Query Traces?.....</b>	<b>14</b>
<b>15 Can I Disable CTS?.....</b>	<b>15</b>
<b>16 How Do I Configure the Storage Duration of CTS Audit Logs to 180 Days?.....</b>	<b>16</b>
<b>17 What Should I Do If I Cannot Enable CTS as an IAM User?.....</b>	<b>21</b>
<b>18 How Do I Enable Alarm Notifications for EVS?.....</b>	<b>22</b>

# **1 Must I Use an IAM User (Sub Account) to Configure Transfer on CTS and Perform Operations on an OBS Bucket?**

---

No. You only need to ensure that you have the permissions for OBS buckets.

# 2 How Will CTS Be Affected If My Account Is in Arrears?

---

If your account is in arrears, CTS can still receive operation records from supported services, but the records can only be retained for 7 days. In most cases, records can be merged into trace files and transferred to OBS buckets for long term storage. Trace file storage in OBS buckets generates fees and this function cannot work when your account is in arrears.

In addition, the only action you can perform on trackers is to delete them.

# 3 What Are the Recommended Users of CTS?

---

It is highly recommended that cloud users should enable CTS.

- CTS is core to information security audit. It is an essential part of security risk control for information systems in enterprises and public sectors, and is also necessary for compliance with many industry standards and audit specifications.
- CTS helps accelerate troubleshooting and reduces workforce costs when exceptions occur on cloud resources. With CTS, you can track all operations involved when a fault happens, which helps narrow the possibilities.

# 4 What Will Happen If I Have Enabled Trace Transfer But Have Not Configured an Appropriate Policy for an OBS Bucket?

---

CTS delivers trace files based on the OBS bucket policy. If the policy is configured incorrectly, trace files cannot be delivered.

If an OBS bucket has been deleted or encounters an exception, an error message will be displayed on the management console. In this case, [create an OBS bucket](#) or [reconfigure access control of the OBS bucket](#).

# 5 Does CTS Support Integrity Verification of Trace Files?

---

Yes. The following fields must be included in trace files: **time**, **service\_type**, **resource\_type**, **trace\_name**, **trace\_rating**, and **trace\_type**. Other fields can be added by the services from which traces are collected.



# 6 Why Are There Some Null Fields on the View Trace Page?

---

Fields **source\_ip**, **code**, **request**, **response**, and **message** can be null. These fields are not mandatory for CTS.

- **source\_ip**: If the value of **trace\_type** is **SystemAction**, the operation was triggered by the system. In this case, **source\_ip** is null.
- **request**, **response**, and **code**: These three fields indicate the request content, request result, and HTTP return code of an operation. In some cases, these fields are null or have no service meaning. Therefore, they are left blank based on actual situations.
- **message**: This is a reserved field. Information of other cloud services will be added to this field when necessary. It is normal that the field is null.

# 7 Why Is an Operation Recorded Twice in the Trace List?

---

For an asynchronously invoked trace, such as **deleteDesktop** trace of Workspace, two records with the same trace name, resource type, and resource name will be generated. The two records may seem to be the same. However, they are generated at different times and document different details.

- The first record documents the request initiated by a user.
- The second record documents the response to the request and the operation result, and is usually several minutes later than the first record.

The two records together give a full view of the operation.

# 8 What Services Are Supported by Key Event Notifications?

---

CTS sends notifications of all key operations on services including ECS, EVS, VPC, DEW, native OpenStack, and IAM. These operations include creation, deletion, login, and native OpenStack API calls.

# 9 How Can I Store Trace Files for a Long Time?

---

CTS only retains traces for seven days. To store traces for a long time, configure your tracker to transfer traces to OBS buckets. For details, see section "Configuring a Tracker" in the *Cloud Trace Service User Guide*.

# 10 Why Are user and source\_ip Null for Some Traces with trace\_type as SystemAction?

---

The **trace\_type** field indicates the request source. This field can be **ConsoleAction**, **ApiCall**, and **SystemAction**.

**SystemAction** indicates operations that are not triggered by users, such as alarms, elastic scaling, regular backup, or secondary invocations by systems to complete a user's request. In this case, **user** and **source\_ip** are both null.

# 11 How Can I Find Out Who Created a Specific ECS?

---

## Solution

To identify the user who created a specific ECS, you can view traces recorded by CTS.

## Prerequisites

- You have enabled CTS.
- You have obtained the resource ID of the ECS.

## Procedure

Log in to the CTS console, choose **Trace List**, and select **ECS** for **Trace Source**. In the displayed traces, look for the **createServer** trace with the obtained resource ID, and expand the trace details.

The **user** field shows details of the IAM user who created the ECS. The format is `{"name": "Account name", "id": "Account ID", "domain":{"name": "IAM user name", "id": "IAM user ID"}}`. If the ECS was created by an account, the IAM user name and the account name are the same.

# 12 How Can I Find Out the Login IP Address of an IAM User?

---

## Background

If you want to check if there are security risks in your account by examining the login IP addresses and login time of IAM users, you can view traces recorded by CTS.

## Prerequisites

You have enabled CTS.

## Procedure

- Step 1** Log in to the CTS console, select **IAM** for **Trace Source**, select a time range, and click **Query**.
- Step 2** Click **View Trace** in the **Operation** column of a trace to view its details. **source\_ip** indicates the login IP address, and **record\_time** indicates the login time.

----End

# 13 Why Are Two deleteMetadata Traces Generated When I Buy an ECS in Pay-per-Use or Yearly/Monthly?

---

During ECS creation, metadata is used to store temporary information. When the creation is finished, the information is automatically deleted. Thus, two traces named **deleteMetadata** are generated.



# 14 What Can I Do If I Cannot Query Traces?

---

## Background

Traces cannot be queried on the CTS console.

## Procedure

- Step 1** Check whether you have configured a proper query time range.
- Step 2** Check whether you have configured filters correctly.
- Step 3** For services that do not differentiate regions, such as IAM, you need to enable CTS and create a tracker named **system** in the central region (CN North-Beijing4) so that traces can be reported in other regions. To enable IAM to send SMS messages and emails, you also need to configure notification rules in the central region.
- Step 4** If you still cannot query traces after the preceding steps, submit a service ticket for technical support.

----End

# 15 Can I Disable CTS?

---

If you do need to disable CTS, you can do it in the following two ways:

- Delete or disable existing trackers. (The **system** tracker created by CTS can only be disabled and cannot be deleted.) No traces will be generated.
- Delete the CTS agency from the IAM agency list. CTS will become unavailable.

# 16 How Do I Configure the Storage Duration of CTS Audit Logs to 180 Days?



## Background

Audit logs may need to be stored for 180 days for query and backtracking purposes. You can perform the following steps to configure the storage duration of audit logs and query and analyze audit logs:


## Procedure

- **Configuring a transfer**

After being enabled, CTS automatically creates a management tracker named **system** and records all operations of your tenant account in the tracker. Configure the tracker for CTS to transfer logs to Log Tank Service (LTS). After the configuration is complete, LTS creates a log group and a log stream automatically and stores CTS audit logs in the log stream for 30 days by default. To store them for 180 days, change the log retention duration setting of the log stream to 180 days on LTS.

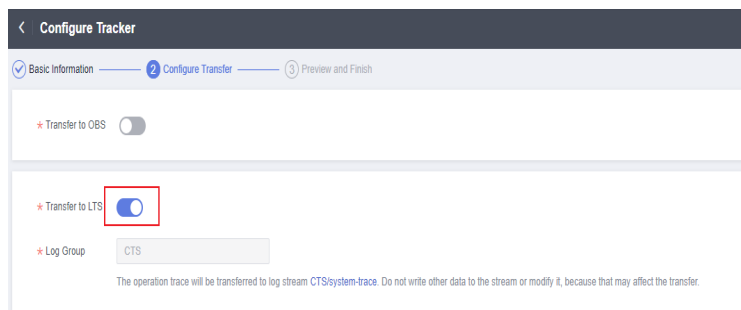
- Log in to the management console.
  - If you log in to the console using a Huawei Cloud account, go to [3](#).
  - If you log in to the console as an IAM user, contact the administrator (Huawei Cloud account or a user in the user group **admin**) to grant the following permissions to the IAM user. For details, see .
    - CTS FullAccess
- Click  in the upper left corner to select the desired region and project.
- Click  in the upper left corner and choose **Management & Governance > Cloud Trace Service**.
- Click **Configure** in the **Operation** column of the **system** tracker to configure the tracker to transfer audit logs to LTS.


**Figure 16-1** Configuring a tracker

Tracker Name	Status	Trace Type	Organization Enabled	OBS Bucket	Storage	Created	Operation
system	 Normal	Management	No	-	LTS CTSsystem-ops	Aug 23, 2023 10:21:35 GMT+	Configure   Delete   Disable

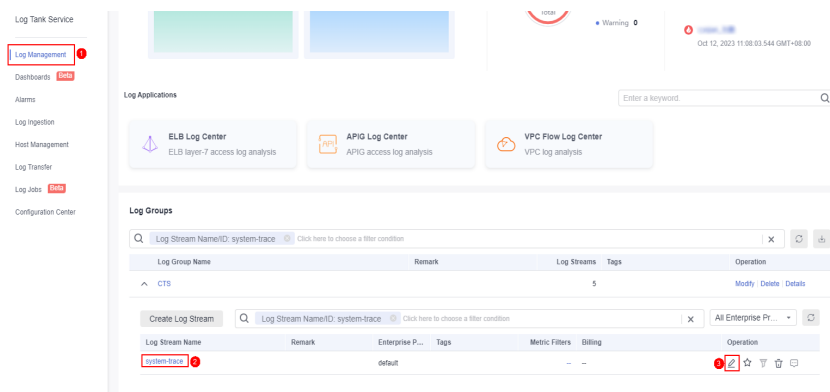
- e. Enable **Transfer to LTS**. The system automatically creates a log group **CTS** and a log stream **system-trace** on LTS.

**Figure 16-2** Transfer to LTS

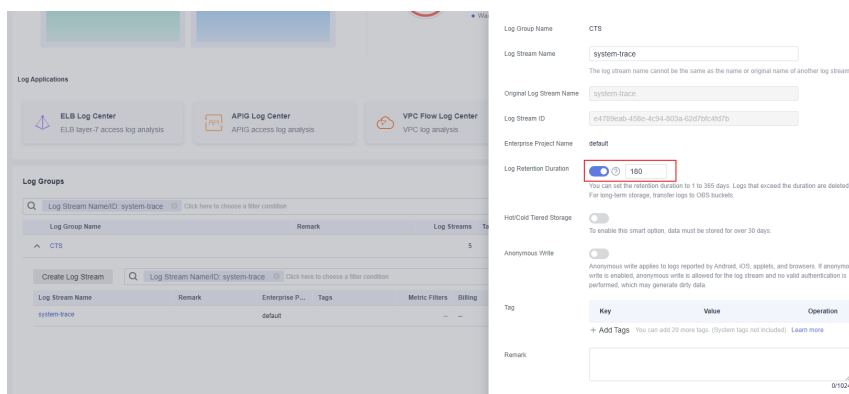


- f. Go to the LTS console, change the storage duration of LTS log streams to 180 days, and configure the structuring rule to CTS.
  - i. Click  in the upper left corner and choose **Management & Governance > Log Tank Service** to access the LTS console.
  - ii. On the **Log Management** page, click the modifying button in the **Operation** column of the **system-trace** log stream created in e. On the displayed page, enable **Log Retention Duration** and change the duration to 180 days.

**Figure 16-3** Modifying the log stream

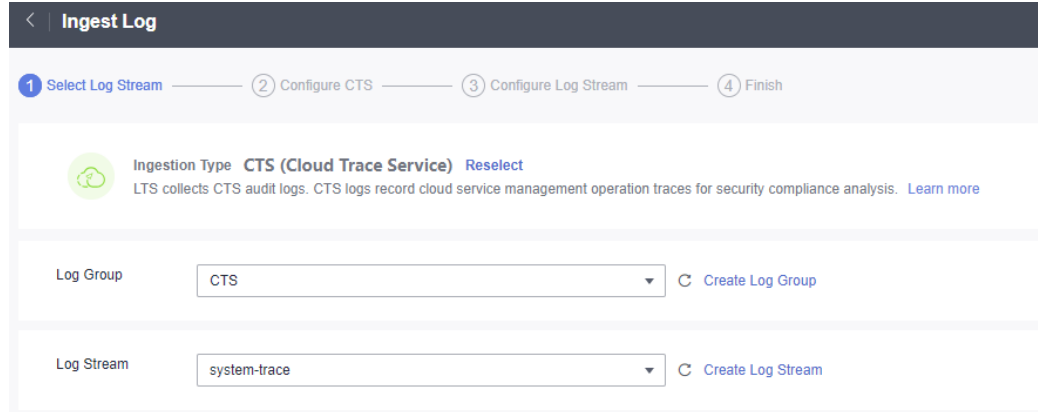


**Figure 16-4** Changing the retention period



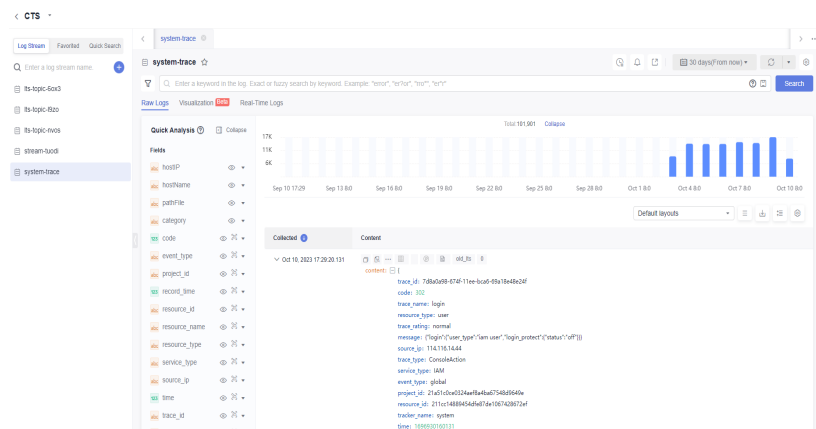
- iii. Choose **Log Ingestion** and click **CTS (Cloud Trace Service)**. On the displayed page, select CTS for **Log Group** and **system-trace** for **Log Stream**.

**Figure 16-5** Selecting a log stream



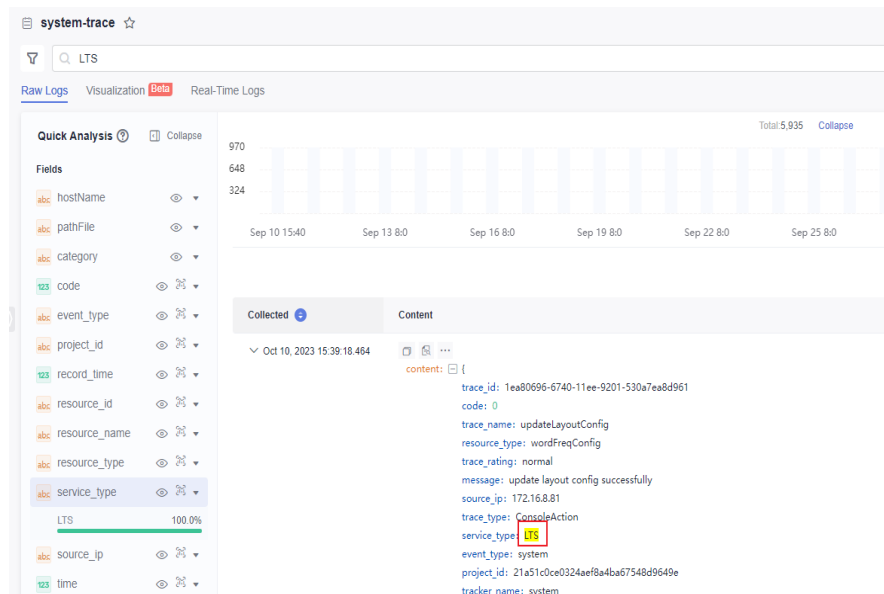
- iv. Click **Next: Configure Log Stream** to configure the CTS log structuring.
- v. Click **Submit** to complete the log ingestion configuration.
- vi. Click **Log Streams**. The log stream details page is displayed.

**Figure 16-6** Log stream details



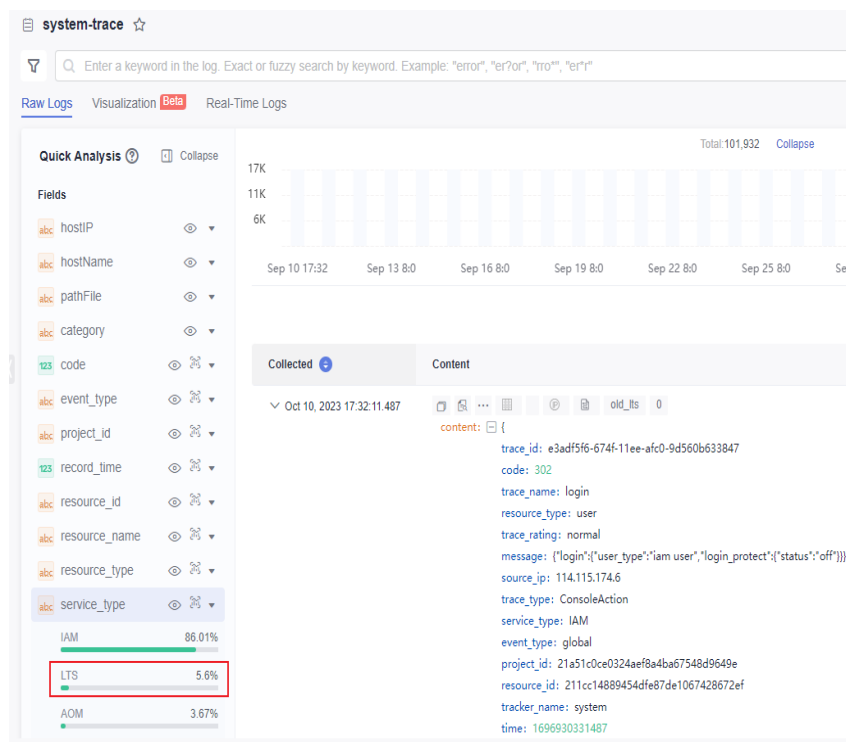
- **Log search and analysis**  
After you configure audit log transferring to LTS, you can search for and analyze audit logs on LTS.
  - Method 1: Enter **LTS** in the search box to search for logs.

**Figure 16-7** Searching for logs



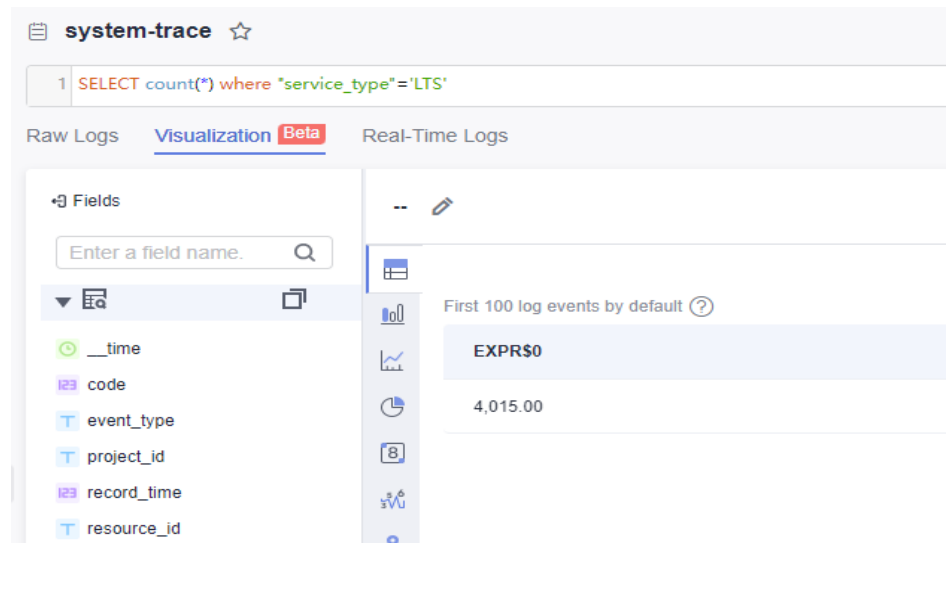
- Method 2: In the **Quick Analysis** area, locate **service\_type** and click **LTS** to quickly search for logs.

**Figure 16-8** Searching for logs



- Method 3: Enter a SQL statement in **Visualization** to filter audit logs and calculate the total number of audit logs.

**Figure 16-9** Querying logs using a SQL statement



# 17 What Should I Do If I Cannot Enable CTS as an IAM User?

---

## Background

If you fail to enable CTS as an IAM user, perform the following steps.

## Procedure

**Step 1** Check whether the IAM user has the permission.

If yes, go to [Step 2](#).

If no, contact the CTS administrator (Huawei Cloud account or a user in user group **admin**) to grant the CTS FullAccess permission to the IAM user. For details, see [Assigning Permissions to an IAM User](#).

**Step 2** If the IAM user has the permission but cannot enable CTS, check whether CTS has been enabled in the central region. If not, enable CTS in the central region using the Huawei Cloud account.

----End



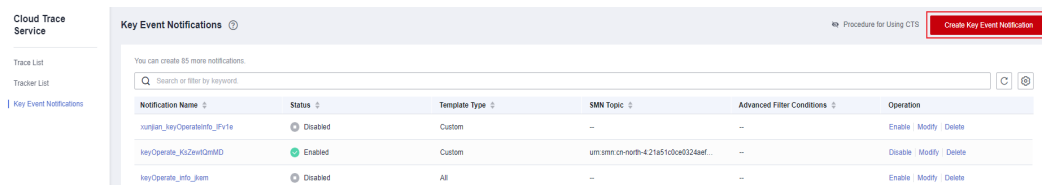
# 18 How Do I Enable Alarm Notifications for EVS?

## Background

You can perform the following steps to enable alarm notifications for Elastic Volume Service (EVS) operations.

## Procedure

- Step 1** Log in to the CTS console, click **Key Event Notifications** on the left, and click **Create Key Event Notification** in the upper right corner.



- Step 2** In the **Operation** area, select **Custom** for **Operation Type**, and select **EVS, evs**, and the four key operations from the **Operation List** drop-down lists to enable alarm notifications for EVS operations.

**Key Event Notifications** < Back to Key Event Notification List

**Basic Information**

Notification Name:

---

**Operation**

SMN notifications will be sent when specified operations are performed.

Operation Type: All Custom

Operation List:     Add

You can add 100 services or 1000 operations. [Learn more](#)

Service Type	Resource Type	Operation
<input checked="" type="checkbox"/>		createVolume
<input checked="" type="checkbox"/>		updateVolume
<input checked="" type="checkbox"/>		extendVolume
<input checked="" type="checkbox"/>		deleteVolume

----End