

# Log Tank Service

## FAQs

Issue	01
Date	2024-03-07



**Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. 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.

# Contents

**1 Overview..... 1**

**2 Log Management..... 3**

2.1 What Are the Recommended Scenarios for Using LTS?..... 3

2.2 How Do I Select LTS Compared with Self-Built ELK?.....6

**3 ICAgent Installation..... 13**

3.1 What Can I Do If ICAgent Installation Fails?..... 13

3.2 What Can I Do If the ICAgent Upgrade Fails?..... 13

3.3 What Can I Do If New Logs Cannot Be Queried on the Raw Log Page?..... 13

3.4 What Can I Do If ICAgent Reports Metric Breakpoints or No Metric?..... 15

3.5 What Can I Do If ICAgent Restarts Repeatedly After Being Installed?..... 17

3.6 What Do I Do If ICAgent Is Offline After Being Installed?..... 18

3.7 What Do I Do If I Do Not See a Host with ICAgent Installed?..... 18

**4 Log Collection..... 20**

4.1 What Can I Do If the CPU Usage Is High When ICAgent Is Running?..... 20

4.2 What Kind of Logs and Files Can LTS Collect?..... 20

4.3 Will LTS Stop Collecting Logs If I Disable "Continue to Collect Logs When the Free Quota Is Exceeded" in AOM?..... 20

4.4 What Do I Do If No Logs Are Collected After I Configure Host Log Ingestion?..... 21

4.5 How Can I Use the New Edition of Log Ingestion?..... 21

4.6 How Do I Disable Collecting CCE Standard Output Logs to AOM?..... 24

4.7 What Log Rotation Scheme Should I Use for ICAgent to Collect Logs?..... 24

**5 Log Search and Check..... 26**

5.1 How Often Is the Data Loaded in the Real-Time Log View?..... 26

5.2 What Do I Do If I Cannot View Raw Logs on the LTS Console?..... 26

5.3 Can I Manually Delete Logs?..... 27

5.4 How Do I Solve Log Search Issues?..... 27

**6 Log Transfer..... 29**

6.1 Does LTS Delete Logs That Have Been Transferred to OBS Buckets?..... 29

6.2 What Are the Common Causes of Abnormal Log Transfer?..... 29

6.3 How Do I Transfer CTS Logs to an OBS Bucket?..... 29

6.4 How Do I Make the Log Retention Duration 180 Days?..... 30

6.5 What Do I Do If I Cannot View Historical Data in an OBS Bucket After Transferring Data to OBS?.....	34
<b>7 Billing.....</b>	<b>35</b>
7.1 What Is the Free Quota of 500 MB For?.....	35
7.2 What Is the LTS Pricing and How Does LTS Charge for Log Indexing?.....	35
7.3 How Will I Be Billed If I Use the Log Transfer Function?.....	36
7.4 How Do I Stop Log Collection When My Free Quota Is Used Up?.....	36
7.5 Why Are Fees Generated When the Log Function Is Disabled for a CCE User?.....	36
<b>8 Others.....</b>	<b>38</b>
8.1 Quick Q&A.....	38
8.2 How Do I Obtain an AK/SK Pair?.....	38
8.3 How Do I Install ICAgent by Creating an Agency?.....	39
8.4 How Do I Migrate Logs from a Third-Party Cloud to Huawei Cloud?.....	40
8.5 Can Logs Stored in LTS Be Used for Security Compliance Audit?.....	40
8.6 How Long Does It Take to Generate Logs After Configuring Log Ingestion?.....	40

# 1 Overview

---

This document provides answers to frequently asked questions related to Log Tank Service (LTS).

## Log Management

- [What Are the Recommended Scenarios for Using LTS?](#)
- [How Do I Select LTS Compared with Self-Built ELK?](#)

## Installing ICAgent

- [What Can I Do If ICAgent Installation Fails?](#)
- [What Can I Do If the ICAgent Upgrade Fails?](#)
- [What Can I Do If New Logs Cannot Be Queried on the Raw Log Page?](#)
- [What Can I Do If ICAgent Reports Metric Breakpoints or No Metric?](#)
- [What Can I Do If ICAgent Restarts Repeatedly After Being Installed?](#)
- [What Do I Do If ICAgent Is Offline After Being Installed?](#)
- [What Do I Do If I Do Not See a Host with ICAgent Installed?](#)

## Log Collection

- [What Can I Do If the CPU Usage Is High When ICAgent Is Running?](#)
- [What Kind of Logs and Files Can LTS Collect?](#)
- [Will LTS Stop Collecting Logs If I Disable "Continue to Collect Logs When the Free Quota Is Exceeded" in AOM?](#)
- [What Do I Do If No Logs Are Collected After I Configure Host Log Ingestion?](#)
- [How Can I Use the New Edition of Log Ingestion?](#)
- [How Do I Disable the Function of Collecting CCE Standard Output Logs to AOM?](#)
- [What Log Rotation Scheme Should I Use for ICAgent to Collect Logs?](#)

## Log Search and Check

- [How Often Is the Data Loaded in the Real-Time Log View?](#)

- [What Do I Do If I Cannot View Raw Logs on the LTS Console?](#)
- [Can I Manually Delete Logs?](#)
- [How Do I Solve Log Search Issues?](#)

## Log Transfer

- [Does LTS Delete Logs That Have Been Transferred to OBS Buckets?](#)
- [What Are the Common Causes of Abnormal Log Transfer?](#)
- [How Do I Transfer CTS Logs to an OBS Bucket?](#)
- [How to Configure the Storage Duration of CTS Audit Logs for 180 Days?](#)
- [What Do I Do If I Cannot View Historical Data in an OBS Bucket After Transferring Data to OBS?](#)

## Billing

- [What Is the Free Quota of 500 MB For?](#)
- [What Is the LTS Pricing and How Does LTS Charge for Log Indexing?](#)
- [How Will I Be Billed If I Use the Log Transfer Function?](#)
- [How Do I Stop Log Collection When My Free Quota Is Used Up?](#)
- [Why Are Fees Generated When the Log Function Is Disabled for a CCE User?](#)

## Others

- [Quick Q&A](#)
- [How Do I Obtain an AK/SK Pair?](#)
- [How Do I Migrate Logs from a Third-Party Cloud to Huawei Cloud?](#)
- [Can Logs Stored in LTS Be Used for Security Compliance Audit?](#)
- [How Long Does It Take to Generate Logs After Configuring Log Ingestion?](#)

# 2 Log Management

---

## 2.1 What Are the Recommended Scenarios for Using LTS?

### Cloud Host Application Logs

Scenario description: The following suggestions are applicable when a user application system is deployed on cloud hosts and LTS is used to centrally collect and search for logs. Generally, a user application system consists of multiple components (microservices). Each component is deployed on at least two cloud hosts.

Suggestions:

- Log collection: The log collector ICAgent is recommended. Install ICAgent on the cloud hosts and configure the log collection path by referring to [Collecting Logs from ECS](#). ICAgent is completely decoupled from application systems and does not require code modification. You are not advised to use SDKs or APIs to collect logs because this mode is complex and the application system stability may be affected due to improper code compilation.
- Log group planning: Place the logs of an application system in a log group. The name of the log group can be the same as that of the application system.
- Log stream planning:
  - If your logs are irregular, you can collect logs of similar components, for example, Java, PHP, and Python components, to the same log stream. This approach reduces the number of log streams, making management easier. If your number of components is small (for example, less than 20), you can collect logs of each component to different log streams.
  - For logs support structuring parsing, such as the Nginx gateway logs, it is recommended that logs of the same format be collected into the same log stream. A unified log format within a log stream enables you to use SQL analysis to analyze visualized charts.
- Permission isolation: LTS log streams support enterprise project isolation. By setting enterprise projects for log streams, you can set different log stream access permissions for different IAM users.

## Containerized Application Logs

Scenario description: The following suggestions are applicable when a user application system is deployed on Kubernetes clusters and LTS is used to centrally collect and search for logs. A user application system consists of multiple workloads, each with at least two instances.

Suggestions:

- Log collection:
  - ICAgent is recommended. You can configure the log collection path by referring to [Collecting Logs from CCE](#). ICAgent is completely decoupled from application systems and does not require code modification. You are not advised to use SDKs or APIs to collect logs because this mode is complex and the application system stability may be affected due to improper code compilation.
  - Containerized application logs can be collected as container standard output, container files, node files, and Kubernetes events. Container files are recommended. In contrast to container standard output, container files can be mounted to hosts persistently and the output content can be controlled by users. In contrast to node files, container files collect metadata such as namespaces, workloads, and pods, facilitating log search.
- Log group planning: Place all logs of a CCE cluster in a log group. The log group alias (modifiable) can be the same as the CCE cluster name, and the original log group name (non-modifiable) is recommended to be `k8s-log-{cluster ID}`.
- Log stream planning:
  - If your logs are irregular, you can collect logs of similar components, for example, Java, PHP, and Python components, to the same log stream. This approach reduces the number of log streams, making management easier. If your number of components is small (for example, less than 20), you can collect logs of each component to different log streams.
  - For logs support structuring parsing, such as the Nginx gateway logs, it is recommended that logs of the same format be collected into the same log stream. A unified log format within a log stream enables you to use SQL analysis to analyze visualized charts.
- Permission isolation: LTS log streams support enterprise project isolation. By setting enterprise projects for log streams, you can set different log stream access permissions for different IAM users.

## Cloud Service Log Analysis

- Ingesting cloud service logs to LTS: LTS can [collect logs from cloud services](#). You need to enable the log function on the corresponding cloud service console to collect logs to a specified log group or log stream.
- Optimal status: Many cloud service logs support structuring parsing. You can configure structuring parsing rules for them on the log structuring page. For details, see [Log Structuring](#). After structuring parsing, you can use SQL statements to analyze the logs in a visualized manner.



## Application Monitoring Alarms

Scenario description: The following suggestions are applicable when logs are used to monitor application systems in real time and detect system faults in advance.

Suggestions:

- Alarm statistics mode: LTS supports **keyword alarms** and **SQL alarms**. For irregular logs such as run logs of Java programs, keyword alarms are applicable. For regular logs such as Nginx gateway logs, SQL alarms are applicable. You can use SQL statements to analyze structuring logs and obtain the required metrics to configure alarms.
- Alarm rule configuration: Generally, alarms need to be triggered as soon as possible. The recommended alarm rule statistics period is 1 minute. You can use the default message templates provided by LTS to send alarms. If you have personalized requirements, you can modify the default templates and save them as **message templates** for sending alarms.
- Configuring log alarms for key cloud services, such as ELB and APIG: ELB is often used as the entry of application systems. To detect system faults in a timely manner, enable ELB logs, collect them to LTS, and configure ELB 5XX status code alarms. In addition, you can use the out-of-the-box ELB dashboard to observe the overall success rate of an application system.

## Service Operation Analysis

Scenario description: The following suggestions are applicable when you print service logs, such as the transaction amount, customer, and product information, in an application system and then output visualized charts and dashboards using the SQL analysis function of LTS.

Suggestions:

- Log collection mode: You are advised to use ICAgent to collect logs and print them in separate log files. Do not mix the logs with the run logs of applications. You are not advised to use SDKs or APIs to report logs.
- Log structuring parsing: You are advised to use spaces to separate service logs or use the JSON format to quickly configure log structuring parsing rules.
- Log visualization:
  - You can **create a custom dashboard** and use SQL-like syntax to analyze service logs that have been structured. You can add **multiple charts** or filters to a custom dashboard to achieve a BI-like display effect. Using LTS for service analysis can eliminate the procurement costs of data warehouses and BI systems and make it easier to get started.
- Log processing: In certain cases, service logs to be analyzed are mixed with run logs, sensitive data in service logs needs to be deleted, or logs lack multi-dimensional data. To address this, you can use the DSL processing function (dialing test started from September 30, 2023) to normalize, enrich, transfer, anonymize, and filter logs.

## DJCP (MLPS) Compliance

Scenario description: According to the Cybersecurity Law of PRC, listed companies and financial enterprises need to store key system logs for at least 180 days. LTS can centrally collect and store such logs.

Suggestions:

- Log collection:
  - For cloud host and container logs, you are advised to use ICAgent to collect them by following the log ingestion wizard for ECS or CCE.
  - For logs of cloud services such as ELB and Virtual Private Cloud (VPC), enable the function of collecting logs to LTS on the cloud service page.
- Log storage:
  - By default, LTS stores logs for up to 365 days. You can change the storage duration. To store logs for a longer period (up to three years), submit a service ticket.
  - Lower storage costs:  
[Transferring logs to OBS](#) has the advantage of low cost and the disadvantage that the contents of historical logs cannot be searched.

## 2.2 How Do I Select LTS Compared with Self-Built ELK?

This document helps you better understand the main functions and advantages of Huawei Cloud LTS by comparing LTS with self-built ELK.

### Background

Many people use ELK Stack (Elasticsearch/Logstash/Kibana) to build an open-source ELK solution for log search. You can find plenty of content and use cases in the community to guide you.

LTS provides a fully managed log analysis platform that covers three scenarios: application O&M, graded protection compliance, and service operation. It enables customers to collect, store, query, process, analyze, and report logs with ease.

### Function

LTS outperforms ELK in terms of function and feature completeness and log search and analysis performance. For details, see the following table.

Feature	Subfeature	LTS	ELK	Description
Log Collection	Cloud service log collection	☆☆☆☆ ☆	None	ELK: You cannot ingest logs from cloud services.  LTS: Logs of the cloud service tenant plane are collected to LTS.

Feature	Subfeature	LTS	ELK	Description
	VM and container log collection	☆☆☆☆ ☆	☆☆☆☆	ELK: Open-source collectors such as Logstash or Filebeat are used to collect logs.  LTS: ICAgent is used to collect logs. A wizard page is provided, which is easy to use.
	Multi-language SDK Log Collection	☆☆☆	None	ELK: No  LTS: Provides a Java SDK to directly report logs to LTS.
	Host group management (dynamic scaling of hosts)	☆☆☆☆ ☆	None	ELK: No  LTS: Allows you to manage hosts and host groups. You can customize host groups and scale them in or out dynamically.
	Log structuring parsing	☆☆☆☆	☆☆☆☆ ☆	ELK: Implements structuring parsing of customized logs based on the collector.  LTS: Enables structuring parsing logs. You can use regular expressions, JSON, separators, or customized templates to parse logs.
Log Search	Keyword search, fuzz match, and quick analysis	☆☆☆☆ ☆	☆☆☆☆ ☆	ELK and LTS: Provide similar keyword search functions.
	Viewing real-time logs	☆☆☆☆ ☆	None	ELK does not provide the page for viewing real-time logs.  LTS provides page for viewing real-time logs.

Feature	Subfeature	LTS	ELK	Description
	Search of tens of billions of logs in seconds	☆☆☆☆ ☆	☆☆	ELK: Limited by the number of machine resources, it takes a long time to search for massive logs.  LTS: With a large number of elastic computing resources of the public cloud, search results can be returned within 3 seconds for tens of billions of logs.
	Iterative search of hundreds of billions of logs	☆☆☆☆ ☆	None	ELK: Unable to search hundreds of billions of logs directly. And the response times out.  LTS: Provides iterative search. Users can directly search for hundreds of billions of logs.
	Log management scale	100 PB level	100 TB level	ELK: It is often time consuming to keep an eye on machine expansion.  LTS: Pay-per-use. LTS automatically manages 100 PB level logs regardless of underlying resource consumption.
Log Search	SQL analysis logs	☆☆☆☆ ☆	☆☆	ELK does not support nested SQL statements in syntax due to poor performance.  LTS supports nested SQL statements with high performance.
Log Search	SQL functions	☆☆☆☆ ☆	☆☆	ELK only supports basic SQL statistics functions.  Besides basic SQL functions, LTS offers a rich set of extended functions, such as IP, statistics, chain and parallel comparison, and URL functions, that broaden the range of use cases.

Feature	Subfeature	LTS	ELK	Description
Log Search	Charts	☆☆☆☆	☆☆☆	LTS: provides multiple visualized charts, such as tables, line charts, pie charts, and bar charts.
Log Search	Dashboards	☆☆☆☆ ☆	☆☆	ELK: There is no ready-to-use dashboard for cloud service logs.  LTS: Provides ready-to-use dashboards for common cloud service logs, such as ELB, APIG, DDS, DCS, and CFW.
Log alarms	Keyword and SQL alarms	☆☆☆☆ ☆	☆	ELK: Log alarm is not available.  LTS: Quasi-real-time log keyword and SQL alarms are available.
	Alarm notification channels (such as email, SMS, and HTTPS)	☆☆☆☆ ☆	☆	ELK: Alarms cannot be sent to users through DingTalk, WeChat, or SMS messages.  LTS: Interconnects with the Simple Message Notification (SMN) service of Huawei Cloud to notify customers through email, SMS, WeChat, DingTalk, Flying Book, and HTTP.
Log transfer	Transfer to OBS	☆☆☆☆ ☆	None	ELK: Logs cannot be directly transferred to OBS.  LTS: Logs can be transferred to OBS through simple page configuration.
Log Transfer	Transfer to Kafka	☆☆☆☆ ☆	☆☆	ELK: You need to deploy a program to forward logs to Kafka.  LTS: Logs can be transferred to Kafka through simple page configuration.

Feature	Subfeature	LTS	ELK	Description
Log Transfer	Transfer to the data warehouse	☆☆☆☆ ☆	None	ELK: Logs cannot be directly transferred to the data warehouse.  LTS: Logs can be transferred to the data warehouse through simple page configuration.
Log jobs	Scheduled SQL jobs	☆☆☆☆ ☆	None	ELK does not support scheduled SQL jobs.  LTS: You can configure scheduled SQL jobs to process original logs and collect statistics on a small number of logs.
	Function jobs	☆☆☆☆ ☆	None	ELK: Log jobs are not available.  LTS: Supports function triggers. You can write custom scripts in the function service to handle logs flexibly.

## Cost comparison

### Scenario 1:

Suppose you generate 100 GB of raw logs per day (the average log rate is 1.16 MB/s), keep them for 30 days on average, and store them as one primary and one standby. The total size of original logs generated in 30 days is 3000 GB.

Based on the official recommendation of Elasticsearch, the total storage space for raw logs, backup data, and index data is about 2.2 times the size of raw logs in the one primary and one standby mode. Plus, the ES cluster has uneven write and the disk is not fully utilized. So, to store 3000 GB of raw logs, you need disks with at least  $3000 \text{ GB} \times 2.2 \text{ (storage expansion)} \times 2 \text{ (50\% disk redundancy)} = 13200 \text{ GB}$ .

ES needs at least three ECSs (16 vCPUs, 64 GB memory, and 5 TB) as a typical configuration. Two Kafka replicas can store logs of the past 12 hours.

Category	Subcategory	Monthly Cost	Expense Proportion
Setting up ES	3 ECSs (C6 16 vCPUs   64 GB)	$3 \times 1999 = 5997$	47.6%
	Elastic Volume Service (EVS) (high I/O 15 TB)	$0.35 \times 15 \times 1024 = 5376$	42.7%

Category	Subcategory	Monthly Cost	Expense Proportion
Setting up Kafka	3 ECSs (2 vCPUs   4 GB)	$3 \times 208 = 624$	4.9%
	EVS (ultra-high I/O 3 x 200 GB)	600	4.7%
-	-	<b>Self-built ELK: 12,597 in total</b>	-

The monthly cost of LTS calculated using [Price Calculator](#) is around **CNY2102**, which is **16.7%** of the cost of self-built ELK. This is because self-built ELK has a high initial resource cost in scenarios with few logs, while LTS charges you only for what you use, giving it a big edge.

#### Scenario 2:

Suppose you generate 1 TB of raw logs per day (the average log rate is 11.6 MB/s), keep them for 7 days on average, and store them as one primary and one standby. The total size of original logs generated in 7 days is 7 TB. Based on the official recommendation of Elasticsearch, the total storage space for raw logs, backup data, and index data is about 2.2 times the size of raw logs in the one primary and one standby mode. Plus, the ES cluster has uneven write and the disk is not fully utilized. So, to store 7 TB of raw logs, you need disks with at least  $7 \text{ TB} \times 2.2 \text{ (storage expansion)} \times 2 \text{ (50\% disk redundancy)} = 31 \text{ TB}$ .

ES needs at least three ECSs (16 vCPUs, 64 GB memory, and 10 TB) as a typical configuration. Two Kafka replicas can store logs of the past 12 hours.

Category	Subcategory	Monthly Cost	Expense Proportion
Setting up ES	3 ECSs (C6 16 vCPUs   64 GB)	$3 \times 1999 = 5997$	31.7%
	EVS (high I/O 31 TB)	$0.35 \times 31 \times 1024 = 11,110$	58.7%
Setting up Kafka	3 ECSs (2 vCPUs   4 GB)	$3 \times 208 = 624$	3.3%
	EVS (ultra-high I/O 3 x 400 GB)	1200	6.3%
-	-	<b>Self-built ELK: 18,931 in total</b>	-

The monthly cost of LTS calculated using [Price Calculator](#) is around **CNY13,408**, which is **71%** of the cost of self-built ELK. This is because LTS storage is pay-per-

use, while self-built ELK needs a lot of extra disks to keep the clusters running smoothly.

### Scenario 3:

Suppose you generate 5 TB of raw logs per day (the average log rate is 58 MB/s), keep them for 30 days on average, and store them as one primary and one standby. The total size of original logs generated in 30 days is 150 TB.

Based on the official recommendation of Elasticsearch, the total storage space for raw logs, backup data, and index data is about 2.2 times the size of raw logs in the one primary and one standby mode. Plus, the ES cluster has uneven write and the disk is not fully utilized. So, to store 150 TB of raw logs, you need disks with at least  $150 \text{ TB} \times 2.2$  (storage expansion)  $\times 2$  (50% disk redundancy) = 660 TB.

ES needs at least 66 ECSs (16 vCPUs, 64 GB memory, and 10 TB) as a typical configuration. Two Kafka replicas can store logs of the past 12 hours.

Category	Subcategory	Monthly Cost	Expense Proportion
Setting up ES	66 ECSs (C6 16 vCPUs   64 GB)	$66 \times 1999 = 131,934$	35.3%
	EVS (high I/O 660 TB)	$0.35 \times 660 \times 1024 = 236,544$	63.2%
Setting up Kafka	3 ECSs (2 vCPUs   4 GB)	$3 \times 208 = 624$	0.2%
	EVS (ultra-high I/O 3 x 1700 GB)	5100	1.4%
-	-	<b>Self-built ELK: 374,202 in total</b>	-

The monthly cost of LTS calculated using [Price Calculator](#) is around **CNY107,655**, which is **28.8%** of the cost of self-built ELK. This is because LTS storage is pay-per-use, while self-built ELK needs a lot of extra disks to keep the clusters running smoothly.

## Summary

LTS beats ELK in functions, performance, and costs. You are advised to use fully managed LTS instead of self-built ELK.



# 3 ICAgent Installation

---

## 3.1 What Can I Do If ICAgent Installation Fails?

### In a Windows Environment:

**Symptom:** The ICAgent installation fails and the "SERVICE STOP" message is displayed. No ICAgent task exists in Task Manager and the ICAgent service is not displayed in the Service List. When the **sc query icagent** command is executed, a message is displayed, indicating that no ICAgent was found.

**Cause:** The ICAgent registration is blocked by antivirus software, such as 360 Total Security.

**Solution:** Disable any running antivirus software before installing ICAgent.

#### NOTE

If you want to collect logs from a Windows host, specify the files to be collected when configuring the log collection path. Supported file types include **.log**, **.trace**, and **.out**. ICAgent does not collect binary files.

## 3.2 What Can I Do If the ICAgent Upgrade Fails?

If you failed to upgrade ICAgent on the LTS console, log in to the VM and run the ICAgent installation command. ICAgent can be overwrite-installed, eliminating the need to uninstall it before reinstallation.

## 3.3 What Can I Do If New Logs Cannot Be Queried on the Raw Log Page?

### Background

New logs cannot be queried on the raw log page.

## Impact

Users cannot query service logs.

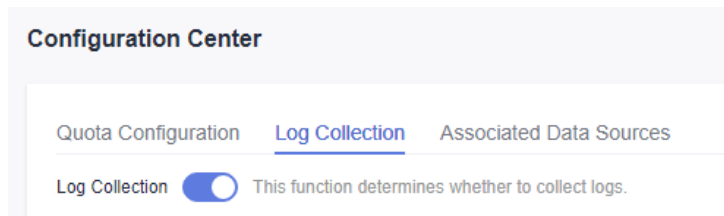
## Possible Causes

1. The log collection function is disabled.
2. A log fails to be sent.
3. An abnormal collection configuration by LTS overwrites the correct collection configuration.

## Fault Locating

**Step 1** Check whether the log collection function is enabled.

1. Log in to the LTS console and choose **Configuration Center** in the navigation pane on the left.
2. On the **Log Collection** tab page, check whether the log collection function is enabled. If not, enable it.



**Step 2** Check the configuration of the log collection function delivered last time.

1. Log in to the ECS host where ICAgent is installed.
2. Run the **cd /var/ICAgent** command to go to the ICAgent log directory.
3. Run the following command to view the log collection configuration.  
**zgrep switchList \*.zip** //Query the compressed package of transferred logs.  
**cat oss.icAgent.trace | grep switchList** //Query the current log file.

```
[root@lts-k8s-65463 ICAgent]#  
[root@lts-k8s-65463 ICAgent]#  
[root@lts-k8s-65463 ICAgent]# cat oss.icAgent.trace | grep switchList  
2023/05/22 19:35:49.629 [w] switchList: [{"switchName": "switch.log", "switchValue": false}, {"switchName": "switch.metric", "switchValue": true}]  
[root@lts-k8s-65463 ICAgent]#  
[root@lts-k8s-65463 ICAgent]#  
[root@lts-k8s-65463 ICAgent]#
```

Search for the latest log time configuration from the filtering result and check whether the value of **switch.log** is **true** (indicating that log collection is enabled).

**Step 3** Check whether the value of **switch.log** in the log collection switch file is **true** (indicating that log collection is enabled).

1. Log in to the host where ICAgent is installed.
2. Query the log collection file path.  
**cat /var/share/oss/manager/ICProbeAgent/internal/TRACE\_CONFIG/swithes\_context.json**

```
[root@lts-k8s-65463 ICAgent]#  
[root@lts-k8s-65463 ICAgent]#  
[root@lts-k8s-65463 ICAgent]# cat /var/share/oss/manager/ICProbeAgent/internal/TRACE_CONFIG/swithes_context.json  
{"switchName": "switch.log", "switchValue": "true"}  
[root@lts-k8s-65463 ICAgent]#  
[root@lts-k8s-65463 ICAgent]#  
[root@lts-k8s-65463 ICAgent]#
```

The value of **switch.log** in the log collection **switch file** is **true**.

**Step 4** Check whether the log fails to be sent.

1. Log in to the ECS host where ICAgent is installed.
2. Run the **cd /var/ICAgent** command to go to the ICAgent log directory.
3. Query the log that failed to be sent.

```
cat oss.icAgent.trace | grep httpsend | grep 'dataType:TRACE' | grep failed
zgrep 'dataType:TRACE' *.zip | grep httpsend | grep failed
```

```
[root@ciAgent-66081 iCAgent#]
[root@ciAgent-66081 iCAgent#] cat oss.tCAgent.trace | grep httpsend | grep 'dataType:TRACE' | grep failed
[root@ciAgent-66081 iCAgent#]
[root@ciAgent-66081 iCAgent#] zgrep 'dataType:TRACE' +zfp | grep httpsend | grep failed
oss.tCAgent.trace.20230517115507539.zfp.2023/05/18 11:21:04.75 [W] sender.go:705 httpsend failed_dataType:TRACE plugin:docker, len:1107
oss.tCAgent.trace.20230517115507539.zfp.2023/05/18 11:21:04.77 [W] sender.go:659 httpsend failed_dataType:TRACE plugin:docker, len:74757
oss.tCAgent.trace.20230518160803829.zfp.2023/05/18 15:49:27.79 [W] sender.go:705 httpsend failed_dataType:TRACE plugin:docker, len:326140
oss.tCAgent.trace.20230518160803829.zfp.2023/05/18 16:01:59.99 [W] sender.go:659 httpsend failed_dataType:TRACE plugin:docker, len:693483
oss.tCAgent.trace.20230518160803829.zfp.2023/05/18 16:02:00.00 [W] sender.go:705 httpsend failed_dataType:TRACE plugin:docker, len:683416
oss.tCAgent.trace.20230518160803829.zfp.2023/05/18 16:02:00.00 [W] sender.go:659 httpsend failed_dataType:TRACE plugin:docker, len:683416
oss.tCAgent.trace.20230518160803829.zfp.2023/05/18 16:03:35.09 [W] sender.go:659 httpsend failed_dataType:TRACE plugin:docker, len:683416
oss.tCAgent.trace.20230518175177705.zfp.2023/05/18 16:16:35.45 [W] sender.go:705 httpsend failed_dataType:TRACE plugin:docker, len:683451
oss.tCAgent.trace.20230518175177705.zfp.2023/05/18 16:16:35.46 [W] sender.go:659 httpsend failed_dataType:TRACE plugin:docker, len:683451
oss.tCAgent.trace.20230518175177705.zfp.2023/05/18 16:17:21.94 [W] sender.go:705 httpsend failed_dataType:TRACE plugin:docker, len:683384
oss.tCAgent.trace.20230518175177705.zfp.2023/05/18 16:17:22.02 [W] sender.go:705 httpsend failed_dataType:TRACE plugin:docker, len:683451
oss.tCAgent.trace.20230518175177705.zfp.2023/05/18 16:17:28.06 [W] sender.go:705 httpsend failed_dataType:TRACE plugin:docker, len:683451
oss.tCAgent.trace.20230518175177705.zfp.2023/05/18 16:17:47.64 [W] sender.go:705 httpsend failed_dataType:TRACE plugin:docker, len:683451
oss.tCAgent.trace.20230518175177705.zfp.2023/05/18 16:18:46.86 [W] sender.go:705 httpsend failed_dataType:TRACE plugin:docker, len:683384
```

If **failed** is displayed, contact LTS technical support.

### Step 5 Confirm the configuration by LTS.

1. Log in to the ECS host where ICAgent is installed.
2. Run the **cd /var/ICAgent** command to go to the ICAgent log directory.
3. Filter log files to query log collection configuration by LTS.

```
cat oss.icAgent.trace | grep 'als event' | grep -v grep | tail -n 1
```

[illegible]

(The preceding figure is for reference only.) Search for the log group, log stream, and collection path set by the user based on the filtering result to ensure that the collection configuration has been delivered.

4. If the log file cannot be found, query the compressed log package.

```
zgrep 'als event' *.zip | grep -v grep | tail -n 1
```

[illegible]

5. Log in to the LTS console and check whether the collection configuration is correctly delivered.

---End

### 3.4 What Can I Do If ICAgent Reports Metric Breakpoints or No Metric?

## Background

ICAgent reports metric breakpoints or no metric.

## Impact on the System

Users cannot view monitoring information.

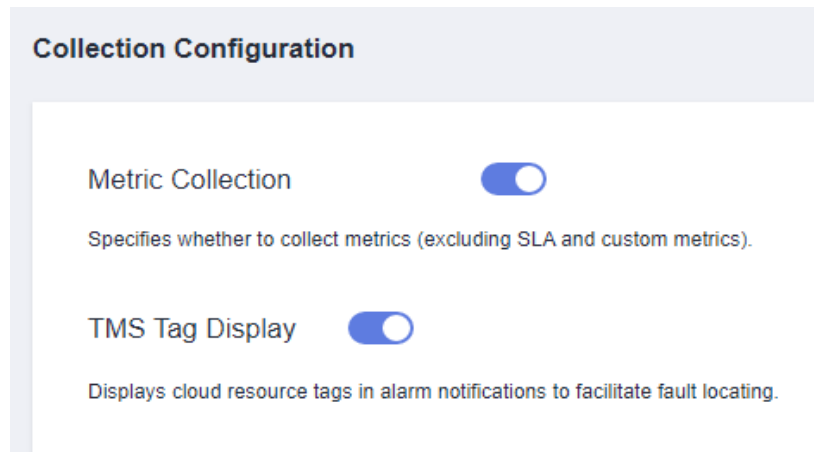
## Possible Causes

1. The metric collection function is disabled.
2. Metrics fail to be sent.

## Fault Locating

**Step 1** Check whether the metric collection is disabled.

1. Log in to the AOM console. In the navigation pane, choose **Configuration Management > Metric Configuration**.
2. Check whether the metric collection is enabled. If not, enable it.



**Step 2** Search for the metric collection switch configuration in the background.

1. Log in to the ECS host where ICAgent is installed.
2. Run the **cd /var/ICAgent** command to go to the ICAgent log directory.
3. Search for the metric collection switch configuration.  
`cat oss.icAgent.trace | grep 'switchL'`

```
[root@icagent-66081 ~]# cat oss.icAgent.trace | grep 'switchL'
2023/05/22 19:15:54.436 [W] switches.go:80 debug, switchLst: [[SwitchName:switch.log SwitchValue:true] [SwitchName:switch.metric SwitchValue:true]]
2023/05/22 19:16:24.437 [W] switches.go:80 debug, switchLst: [[SwitchName:switch.log SwitchValue:true] [SwitchName:switch.metric SwitchValue:true]]
```

4. If it cannot be found, filter the log package.  
`zgrep switchL *.zip`

```
[root@icagent-66081 ~]# zgrep switchL *.zip
oss.icAgent.trace.2023051915547705.zip:2023/05/19 19:16:25.805 [W] switches.go:80 debug, switchLst: [[SwitchName:switch.log SwitchValue:true] [SwitchName:switch.metric SwitchValue:true]]
oss.icAgent.trace.2023051915547705.zip:2023/05/19 19:16:49.804 [W] switches.go:80 debug, switchLst: [[SwitchName:switch.log SwitchValue:true] [SwitchName:switch.metric SwitchValue:true]]
```

**Step 3** Check whether metrics fail to be sent.

1. Log in to the ECS host where ICAgent is installed.
2. Run the **cd /var/ICAgent** command to go to the ICAgent log directory.
3. Query the log for the metric that failed to be sent.  
`cat oss.icAgent.trace | grep httpsend | grep MONITOR | grep failed`

```
[root@icagent-66081 ~]# cat oss.icAgent.trace | grep httpsend | grep MONITOR | grep failed
2023/05/22 18:15:18.330 [W] sender.go:520 httpsend failed, dataType:MONITOR_INVENTORY, plugin:discovery, len:1316
2023/05/22 18:15:18.330 [W] sender.go:692 httpsend failed, dataType:MONITOR_INVENTORY, plugin:discovery, len:1316
2023/05/22 18:15:53.332 [W] sender.go:692 httpsend failed, dataType:MONITOR_INVENTORY, plugin:discovery, len:1316
2023/05/22 18:16:28.335 [W] sender.go:692 httpsend failed, dataType:MONITOR_INVENTORY, plugin:discovery, len:1316
2023/05/22 18:17:03.337 [W] sender.go:687 httpsend failed 3 times, discard dataType:MONITOR_INVENTORY, plugin:discovery, len:1316
2023/05/22 18:20:30.316 [W] sender.go:520 httpsend failed, dataType:MONITOR_INVENTORY, plugin:discovery, len:1316
2023/05/22 18:20:38.316 [W] sender.go:692 httpsend failed, dataType:MONITOR_INVENTORY, plugin:discovery, len:1316
2023/05/22 18:21:13.317 [W] sender.go:692 httpsend failed, dataType:MONITOR_INVENTORY, plugin:discovery, len:1316
2023/05/22 18:21:48.319 [W] sender.go:692 httpsend failed, dataType:MONITOR_INVENTORY, plugin:discovery, len:1316
2023/05/22 18:22:23.320 [W] sender.go:687 httpsend failed 3 times, discard dataType:MONITOR_INVENTORY, plugin:discovery, len:1316
```

4. If the log file cannot be found, query the log package.  
`zgrep httpsend *.zip | grep MONITOR | grep failed`

```
[root@icagent-66081 ICAgent]#  
oss.icagent.trace-2023051620439734.zip:2023/05/16 22:26:47.318 [w] sender.go:566 httpsend failed,dataType=MONITOR_INVENTORY_plugin:discovery,len:1316  
oss.icagent.trace-2023051620439734.zip:2023/05/16 22:26:47.318 [w] sender.go:738 httpsend failed,dataType=MONITOR_INVENTORY_plugin:discovery,len:1316  
oss.icagent.trace-2023051620439734.zip:2023/05/16 22:27:25.319 [w] sender.go:738 httpsend failed,dataType=MONITOR_INVENTORY_plugin:discovery,len:1316  
oss.icagent.trace-2023051620439734.zip:2023/05/16 22:27:57.321 [w] sender.go:738 httpsend failed,dataType=MONITOR_INVENTORY_plugin:discovery,len:1316  
oss.icagent.trace-2023051620439734.zip:2023/05/16 22:28:30.323 [w] sender.go:733 httpsend failed 3 times,discard dataType=MONITOR_INVENTORY_plugin:discovery,len:1316  
oss.icagent.trace-2023051620439734.zip:2023/05/16 22:29:02.324 [w] sender.go:566 httpsend failed,dataType=MONITOR_INVENTORY_plugin:discovery,len:1292  
oss.icagent.trace-2023051620439734.zip:2023/05/16 22:29:02.324 [w] sender.go:738 httpsend failed,dataType=MONITOR_INVENTORY_plugin:discovery,len:1292  
oss.icagent.trace-2023051620439734.zip:2023/05/16 22:29:37.325 [w] sender.go:738 httpsend failed,dataType=MONITOR_INVENTORY_plugin:discovery,len:1292  
oss.icagent.trace-2023051620439734.zip:2023/05/16 22:30:12.326 [w] sender.go:738 httpsend failed,dataType=MONITOR_INVENTORY_plugin:discovery,len:1292  
oss.icagent.trace-2023051620439734.zip:2023/05/16 22:30:47.328 [w] sender.go:713 httpsend failed 3 times,discard dataType=MONITOR_INVENTORY_plugin:discovery,len:1292
```

----End

## 3.5 What Can I Do If ICAgent Restarts Repeatedly After Being Installed?

### Background

ICAgent restarts repeatedly after being installed.

### Impact on the System

ICAgent metrics/logs cannot be collected.

### Possible Causes

1. The resource usage exceeds the maximum allowed limit.
2. ICAgent is abnormal.

### Fault Locating

**Step 1** Log in to the ECS host where ICAgent is installed.

**Step 2** Run the `cd /var/ICAgent` command to go to the ICAgent log directory.

**Step 3** Filter log files and check whether the resource usage exceeds the upper limit.

```
cat oss.icAgent.trace | grep 'icagent exit'
```

```
[root@icagent-66081 ICAgent]#  
[root@icagent-66081 ICAgent]#  
[root@icagent-66081 ICAgent]# cat oss.icAgent.trace | grep 'icagent exit'  
[root@icagent-66081 ICAgent]#  
[root@icagent-66081 ICAgent]#
```

**Step 4** Filter compressed log packages and check whether the resource usage exceeds the upper limit.

```
zgrep 'icagent exit' *.zip
```

```
[root@icagent-66081 ICAgent]#  
[root@icagent-66081 ICAgent]#  
[root@icagent-66081 ICAgent]# zgrep 'icagent exit' *.zip  
[root@icagent-66081 ICAgent]#  
[root@icagent-66081 ICAgent]#
```

**Step 5** Filter log files and check whether ICAgent is abnormal.

```
cat oss.script.trace | grep runtime
```

```
[root@icagent-66081 ICAgent]#  
[root@icagent-66081 ICAgent]#  
[root@icagent-66081 ICAgent]# cat oss.script.trace | grep runtime  
[root@icagent-66081 ICAgent]#  
[root@icagent-66081 ICAgent]#
```

**Step 6** Filter compressed log packages and check whether ICAgent is abnormal.

```
zgrep runtime oss.script.*.zip
```

```
[root@icagent-66081 ICAgent]#  
[root@icagent-66081 ICAgent]# zgrep runtime oss.script*.zip  
gzip: oss.script*.zip.gz: No such file or directory  
[root@icagent-66081 ICAgent]#  
[root@icagent-66081 ICAgent]#
```

----End

## 3.6 What Do I Do If ICAgent Is Offline After Being Installed?

If ICAgent is offline, the possible cause is that ICAgent is abnormal because Access Key ID/Secret Access Key (AK/SK) pair is incorrect. Obtain the correct AK/SK and install them again. For details, see [How Do I Obtain an AK/SK Pair?](#)

## 3.7 What Do I Do If I Do Not See a Host with ICAgent Installed?

If a host with ICAgent installed is not displayed on the **Hosts** tab page on the LTS console, perform the following steps:

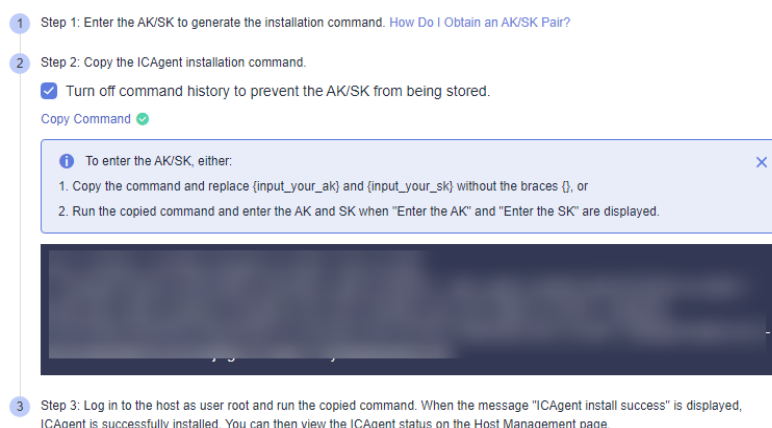
### Prerequisites

You have logged in to the LTS console.

### Procedure

**Step 1** When configuring ECS log ingestion, if the ECS is not displayed on the **Hosts** tab page after you install ICAgent on it:

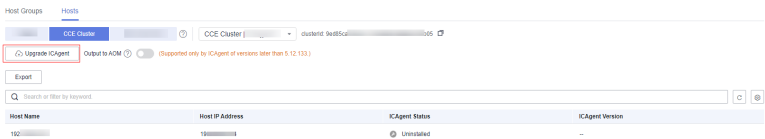
1. On the **Install ICAgent** page, ensure that the installation command is correctly copied. Do not use the installation command across regions.



2. Ensure that the obtained AK/SK pair is correct and has not been deleted.
3. Run the **netstat -nap | grep icagent** command to check whether the host network is proper.

**Step 2** When configuring CCE log ingestion, if the CCE cluster is not displayed on the **Hosts** tab page after you install ICAgent on it:

Ensure that ICAgent has been installed in the CCE cluster and a host group with custom identifiers has been created for related nodes. If ICAgent has not been installed, upgrade it on the **Host Management** page. For details, see [Upgrading ICAgent](#).



- Step 3** ICAgent fails to be installed in a Windows environment:
1. Ensure that you install ICAgent as an administrator.
  2. Ensure that the obtained AK/SK pair is correct and has not been deleted.
- End

# 4 Log Collection

---

## 4.1 What Can I Do If the CPU Usage Is High When ICAgent Is Running?

If the CPU usage is high when ICAgent is running, check whether there are a large number of logs in the log collection path. Clear logs regularly to reduce system resource occupation during log collection.

## 4.2 What Kind of Logs and Files Can LTS Collect?

### Logs That Can Be Collected by LTS:

- Host logs. ICAgent should be installed on the target hosts for log collection.
- Cloud service logs. To collect logs from cloud services, such as Elastic Load Balance (ELB) or Virtual Private Cloud (VPC), enable log reporting to LTS in the cloud services.
- Logs reported by APIs.

### Files That Can Be Collected by LTS:

If the collection path is set to a directory, for example, `/var/logs/`, only `.log`, `.trace`, and `.out` files in the directory are collected. If the collection path is set to the name of a file (only text files are supported), the specified file is collected. Note that LTS only collects logs generated in the last 7 days.

## 4.3 Will LTS Stop Collecting Logs If I Disable "Continue to Collect Logs When the Free Quota Is Exceeded" in AOM?

Yes. If you set the log collection to be stopped when the free quota is used up in AOM, the setting is also applied to LTS.



## 4.4 What Do I Do If No Logs Are Collected After I Configure Host Log Ingestion?

1. Wait for a while if you just completed configuring the ingestion. It takes a moment before log reporting begins.
2. Check whether the host collection path has been added to more than one log stream. If it has, modify the configurations so a host path is configured in only one log stream.
3. Check whether the host collection path has been configured in AOM. If a collection path has been configured in AOM, do not configure it in LTS.
4. Check whether any ingestion settings are improper by referring to [Collecting Logs from ECS](#).
5. If the issue persists after you have tried the methods above, [submit a service ticket](#).

## 4.5 How Can I Use the New Edition of Log Ingestion?

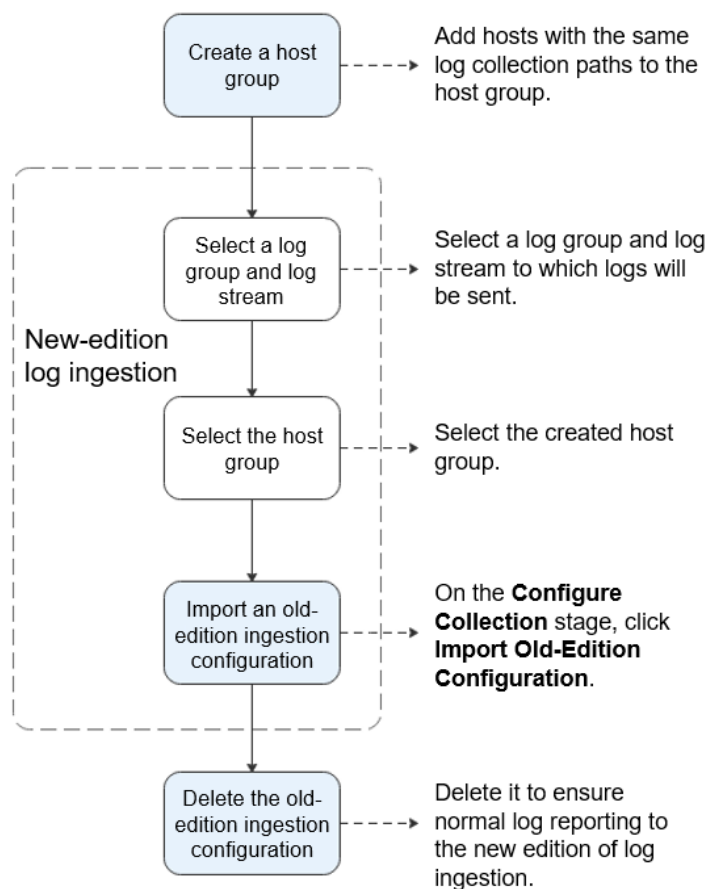
If you want to ingest logs from hosts to log streams, you would have to go to each log stream and configure ingestion one by one for each host with the old edition of log ingestion. This could be time-consuming when you have a large number of log streams and hosts and maintenance could be very burdensome. That is why LTS introduces the concept of host groups. Log ingestion configurations are now associated with host groups instead of hosts. When you add hosts to a host group, the hosts will automatically inherit the ingestion configurations associated with the host group. Configuring log ingestion becomes quick and efficient.

### NOTE

When using the new edition of log ingestion, you need to first create host groups, sort hosts into different host groups based on your requirements, and associate ingestion configurations with host groups.

## Procedure

The following describes the procedure of using the new edition of log ingestion.

**Figure 4-1** Procedure of using the new edition of log ingestion**Step 1** Create a host group.

1. Log in to the LTS console and choose **Host Management** in the navigation pane.
2. Click **Create Host Group** in the upper right corner.
3. In the displayed slide-out panel, enter a host group name and select a host OS (Linux or Windows).
4. In the host list, select one or more hosts to add to the group and click **OK**.

**Step 2** Select a log group and log stream.

1. On the LTS console, choose **Log Ingestion** in the navigation pane.
2. Click **Elastic Cloud Server (ECS)** to configure log ingestion.
3. On the **Select Log Stream** stage, select a log group and log stream to which logs will be sent, and click **Next: Select Host Group**.

**Step 3** Select the host group.

Select the created host group and click **Next: Configure Collection**.

**Step 4** Import an old-edition ingestion configuration.

On the **Configure Collection** stage, enter a collection configuration name, and click **Import Old-Edition Configuration** next to the text box. In the displayed

slide-out panel, select an old-edition configuration to import and click **OK**. After the import is complete, click **Submit**.

**Step 5** Delete the old-edition ingestion configuration.

Go to the details page of the corresponding log stream, choose **Log Ingestion > Host**, and delete the old-edition ingestion configuration imported in [Step 4](#).

**NOTE**

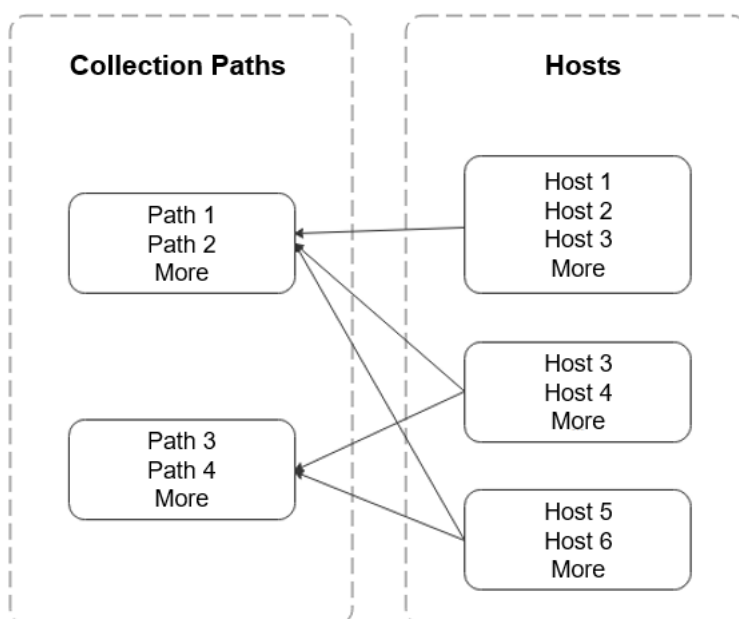
- A collection path can be configured only once. It means that you cannot add the same host path to more than one log stream. Otherwise, log ingestion may be abnormal.
- You must delete the old-edition ingestion configuration after import to ensure that logs can be reported to the new edition of log ingestion.

----End

## Grouping Hosts

A host group can associate with one or more ingestion configurations and all the configurations will be applied to each host in the host group. When you sort hosts to host groups, consider the host configurations, such as which paths of the hosts you want to collect logs from. A host can be added to multiple host groups.

**Figure 4-2** Grouping hosts



## 4.6 How Do I Disable Collecting CCE Standard Output Logs to AOM?

### Symptom

As the products evolve, the default collection of CCE standard output logs to AOM is no longer recommended, but for compatibility with old user habits, the default configuration is not modified. If the default configuration does not meet your requirements, disable it on the LTS console. You are advised to collect CCE standard output logs to LTS for unified log management.

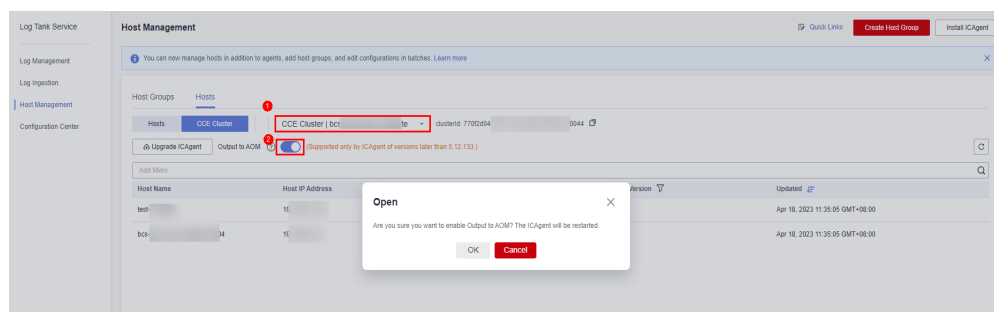
#### NOTE

Only when the collection of CCE standard output to AOM is disabled, the CCE standard output configured in LTS will take effect.

### Solution

- Step 1** Log in to the LTS console and choose **Host Management** in the navigation pane on the left.
- Step 2** Choose **Hosts** and click **CCE Cluster**.
- Step 3** In the CCE cluster, select the CCE cluster, and disable **Output to AOM**.

**Figure 4-3** Disabling output to AOM



- Step 4** Click **OK**. After ICAgent is restarted, CCE standard output to AOM is disabled.

----End

## 4.7 What Log Rotation Scheme Should I Use for ICAgent to Collect Logs?

Log rotation, also known as log splitting, is used to control the size of a log file. As software system runs for a long time without interrupting services, a large amount of information will be recorded in different logs. As time goes by, the limited disk space will be insufficient to accommodate the increasing log volume. In this case, the size of log files needs to be controlled.

Log rotation can be implemented by time or by log size.

- **By time:** Logs are rotated based on time. When the time when a log is generated reaches the specified time threshold, the log will be rotated. For example, the `/var/log/messages` logs are split based on the rule of rotating once every seven days.
- **By log size:** Logs are rotated based on the log size. When the log size reaches the specified value, the log will be rotated. This mode is applicable to application logs.

When using log rotation, you are advised to:

- **Methods:**

ICAgent does not rotate your logs. You are advised to use mature software packages to customize log rotation rules in applications, such as Java logback, log4j2, Python logging, and Linux logrotate. If the size of a typical configuration log file exceeds 100 MB, 50 MB, or 20 MB, the log file is rotated once and 10 to 20 historical log files are saved.

- **Suggestions on naming rotated log files:**

Assume that your log file path is `/your/log/path/**/*log`. You are advised to name the rotated file as `/your/log/path/**/*log.xxx`. `xxx` refers to the date according to user habits, for example, 20240103. It cannot contain letters.

Custom rotation rule: If your naming rules of rotated log files do not comply with the preceding suggestion, rotated log files may be collected repeatedly. You can customize rotation rules to avoid this problem. You can add a custom rotation rule for each log collection path for matching the names of the rotated files. A file whose name matches the rule is identified as a rotated log file and will not be collected repeatedly. For example, if your log file is `/your/log/path/**/app1.log` and the rotated file is `/your/log/path/**/app1.20240103.biz.log`, you can set the rotation rule to `{basename}\.[0-9-\.] +\.[0-9]+\.\biz\log`.

- **Compress rotated log files is not recommended.**

If your log printing rate is high, the log file will be rotated quickly. In this case, a few logs may not be collected at the end of the rotated file. ICAgent uses the Linux inode to identify the uniqueness of the collected file. If the rotated log file is a compressed file, the inode changes. As both the log file name and inode are changed, ICAgent may not be able to collect the logs that are not collected at the end of the rotation file.

For example, assume that the rotated file is compressed and the file name is `/your/log/path/**/*log.xxx.zip`. If both the file name and inode change, ICAgent may not be able to collect the logs that are not collected at the end of the rotation file.

# 5 Log Search and Check

---

## 5.1 How Often Is the Data Loaded in the Real-Time Log View?

Log data is usually loaded every 5 seconds. However, if no data is generated in a 5-second interval, no new data will be displayed. Log data will be updated in the next 5 seconds if there is new data coming in that interval.

## 5.2 What Do I Do If I Cannot View Raw Logs on the LTS Console?

### Symptom

No log events are displayed on the **Raw Logs** tab in a log stream on the LTS console.

### Possible Causes

- ICAgent has not been installed.
- The collection path is incorrectly configured.
- The **Log Collection** function on the LTS console is disabled.
- You set the log collection to be stopped when the free quota is used up on the LTS console.
- Log collection was stopped because your account is in arrears.
- The rate of writing logs into log streams or length of single-line logs exceeds what is supported.
- The browser has slowed down because of the amount of log data.

### Solution

- Install the ICAgent. For details, see [Installing ICAgent](#).
- If the collection path is set to a directory, for example, `/var/logs/`, only **.log**, **.trace**, and **.out** files in the directory are collected. If the collection

path is set to name of a file, ensure that the file is a text file. For details about log collection paths, see [Collecting Logs from Hosts](#).

- Log in to the LTS console, choose **Configuration Center > Log Collection**, and enable the **Log Collection** function.
- Log usage, including log read/write, log indexing, and log retention, is billed in LTS. If you have disabled **Continue to Collect Logs When the Free Quota Is Exceeded** on the LTS console, log collection will be stopped when the free quota is used up. Log read/write and indexing will no longer be available. No fees will be incurred for log read/write and indexing. To resume log collection, enable **Continue to Collect Logs When the Free Quota Is Exceeded** on the LTS console. For details, see [Configuration Center](#).
- Top up your account if your account is in arrears. For details, see [Making Repayments \(Prepaid Direct Customers\)](#).
- Use Google Chrome or Firefox to query logs.
- If the issue persists after you have tried the methods above, [submit a service ticket](#).

## 5.3 Can I Manually Delete Logs?

No. Manual deletion is not supported. However, logs will be automatically deleted when the retention period ends.

## 5.4 How Do I Solve Log Search Issues?

This topic describes how to troubleshoot common issues that occur when the search syntax is used to query logs.

### Common Issues and Troubleshooting Methods

1. During log query, a message is displayed indicating that the query result is inaccurate.
  - Possible cause: There are too many logs in the query time range, and not all logs are displayed.
  - Solution: Click the query button multiple times until you obtain all logs, or shorten the query time range and query again.
2. Too many log results are matched in a query.
  - Possible cause: Only phrase search **#"value"** can ensure the sequence of keywords. For example, if the query statement is **abc def**, logs that contain either **abc** or **def** and logs that contain the phrase **abc def** will be matched.
  - Solution: Use the phrase **#"abc def"** to accurately match logs containing the phrase **abc def**. For details, see [Phrase Search](#).
3. Expected logs cannot be queried with specific search statements, and no error message is displayed.
  - Possible cause 1: Search delimiters are not supported.
  - Possible cause 2: The **\*** or **?** in a search statement will be regarded as a common character and is not used as a wildcard.

- Solution: Use the correct query statement.

## Error Messages and Solutions

1. An error message is displayed during log query, indicating that no field index is configured for the XXX field and the field cannot be queried.  
Solution: Create an index for the XXX field in the index configuration and run the query statement again. For details, see [Index Settings](#).
2. An error message is displayed during log query, indicating that the full-text index is not enabled and the content field and full-text query are not supported.  
Solution: Enable whole text indexing in the index configuration and run the query statement again. For details, see [Index Settings](#).
3. An error message is displayed during log query, indicating that the asterisk (\*) or question mark (?) cannot be used at the beginning of a word.  
Solution: Modify the query statement or use a correct delimiter to avoid such queries.
4. An error message is displayed during log query, indicating that long and float fields do not support fuzzy query using asterisks (\*) or question marks (?).  
Solution: Modify the query statement and use the operator (>=<) or IN syntax for range query.
5. An error message is displayed during log query, indicating that string fields do not support range query using the operator (>=<) or IN syntax.  
Solution
  - Modify the query statement and use the asterisk (\*) or question mark (?) to perform fuzzy query.
  - Change the value of this field to a number. For details, see [Structuring Modes](#).
6. An error message is displayed during log query, indicating that the search syntax is incorrect and the query statement need to be modified.
  - Possible cause: The syntax of the operator is incorrect.  
Solution: Each operator has its syntax rule. Modify the search statement. For details, see Search Syntax. For example, the syntax rule for the operator = requires that the value on the right must be digits.
  - Possible cause: The search statement contains syntax keywords.  
Solution: If the log to search contains syntax keywords, the search statement must be enclosed in double quotation marks to convert the keywords into common characters. For details, see [Search Syntax](#). For example, if **and** is a syntax keyword, change the query statement **field:and** to **field:"and"**.



# 6 Log Transfer

---

## 6.1 Does LTS Delete Logs That Have Been Transferred to OBS Buckets?

No. During log transfer, logs are "replicated" to OBS buckets. To view transferred log files, click the name of the corresponding OBS bucket on the **Log Transfer** page of the LTS console, and you will be directed to the OBS console to check the files.

## 6.2 What Are the Common Causes of Abnormal Log Transfer?

- The OBS bucket used for log transfer has been deleted. Specify another bucket.
- Access control on the OBS bucket is incorrectly configured. Go to the OBS console to correct the settings.
- The Kafka cluster has been deleted. Reconfigure the Kafka transfer.
- The Kafka topic has been deleted. Create a Kafka topic or specify a Kafka topic.

## 6.3 How Do I Transfer CTS Logs to an OBS Bucket?

When Cloud Trace Service (CTS) is connected to LTS, a log group and log stream are automatically created for CTS on the LTS console. To transfer CTS logs to OBS, do as follows:

1. Log in to the CTS console and choose **Tracker List** in the navigation pane on the left.
2. Click **Configure** in the row of the tracker **system**.
3. In the **Basic Information** step, click **Next**.
4. In the **Configure Transfer** step, configure parameters related to transfer logs to OBS, enable **Transfer to LTS**, and click **Next**.

5. Confirm the configurations and click **Configure**.
6. Access the LTS console, choose **Log Transfer** in the navigation pane on the left, and click **Configure Log Transfer** in the upper right corner.  
Set **Log Group Name** to **CTS** and **Log Stream Name** to **system-trace**. Specify other parameters and click **OK** to transfer CTS logs to the selected OBS bucket.
7. View the transferred CTS logs in the specified OBS bucket on the OBS console.

## 6.4 How Do I Make the Log Retention Duration 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.



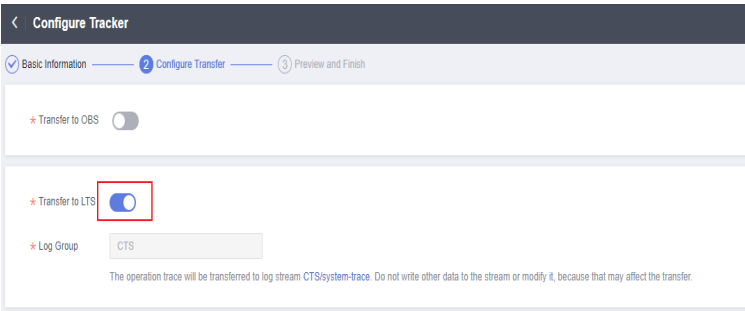
- a. Log in to the management console.
  - If you log in to the console using a Huawei Cloud account, go to [3](#).
  - If you log in to the console as an IAM user, contact the administrator (Huawei Cloud account or a user in the user group **admin**) to grant the following permissions to the IAM user.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

Figure 6-1 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 6-2 Modifying the log stream

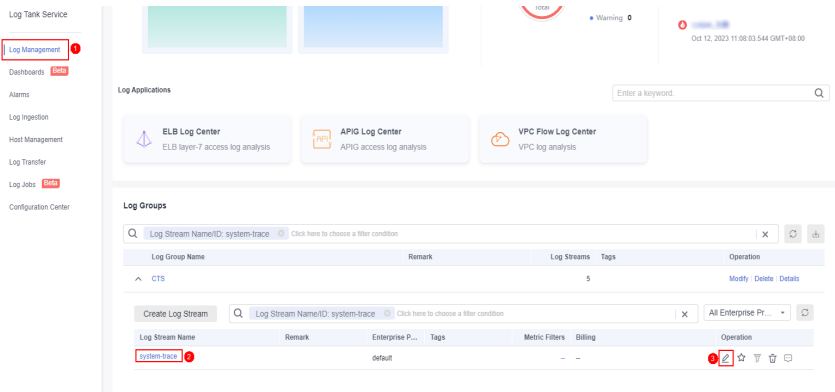
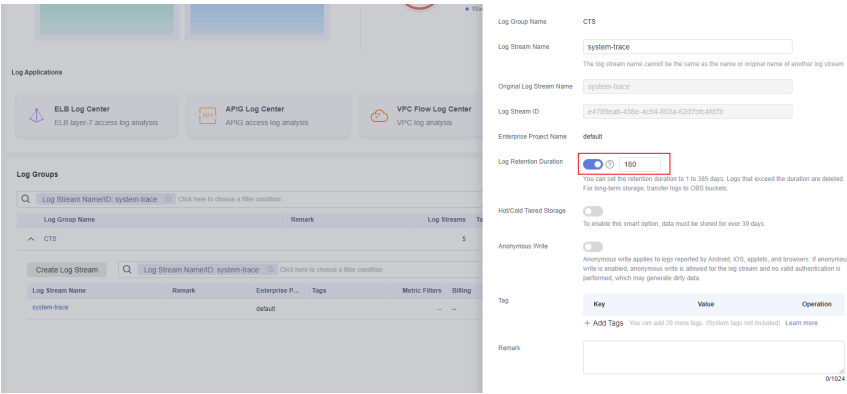
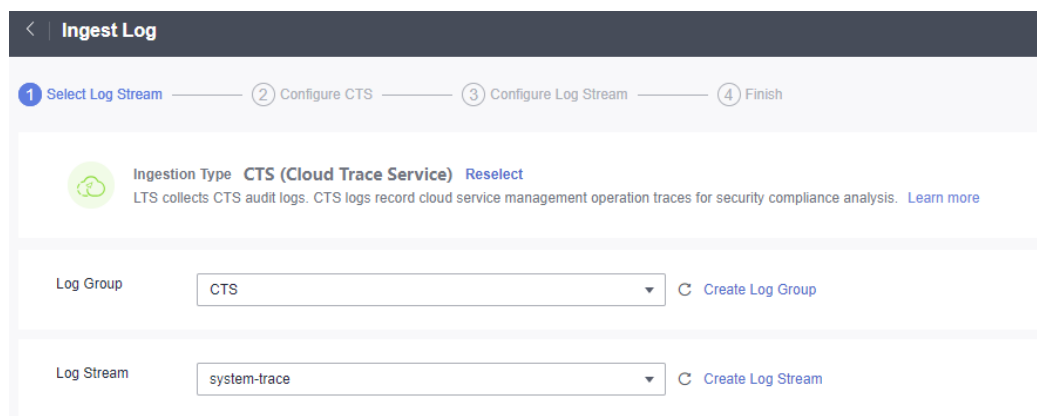


Figure 6-3 Changing the retention period



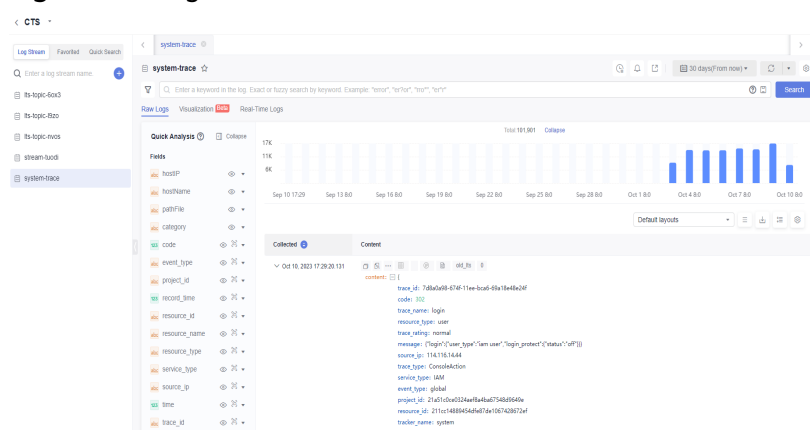
- iii. Choose **Log Ingestion** and click **CTS (Cloud Trace Service)**. On the displayed page, select CTS for **Log Group** and **system-trace** for **Log Stream**.

Figure 6-4 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 6-5 Log stream details

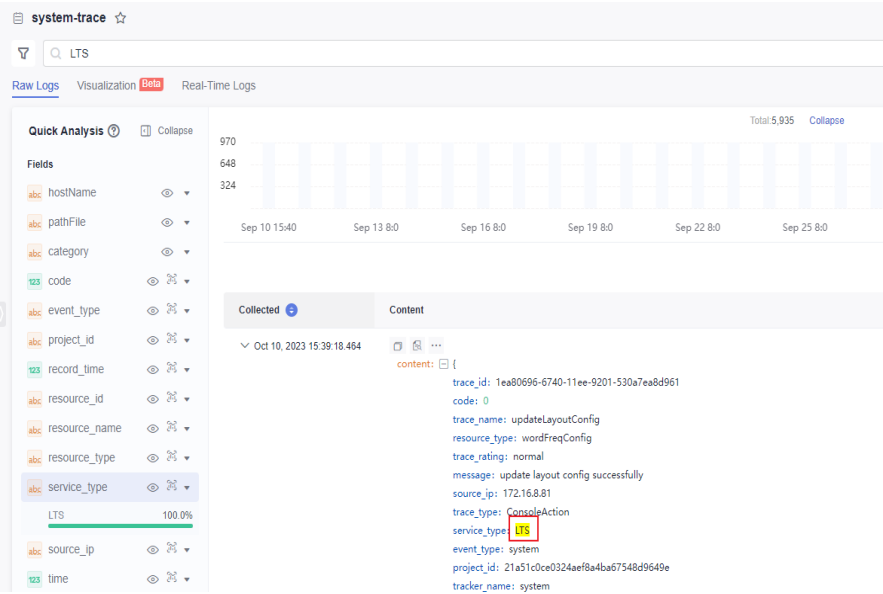


- **Log search and analysis**

After you configure audit log transferring to LTS, you can search for and analyze audit logs on LTS.

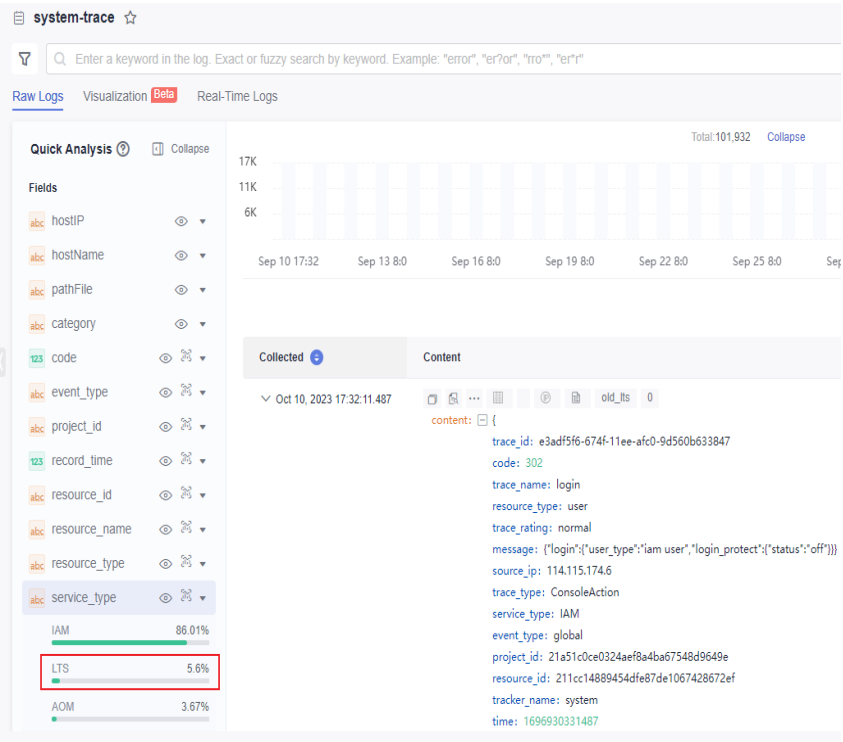
- Method 1: Enter **LTS** in the search box to search for logs.

Figure 6-6 Searching for logs

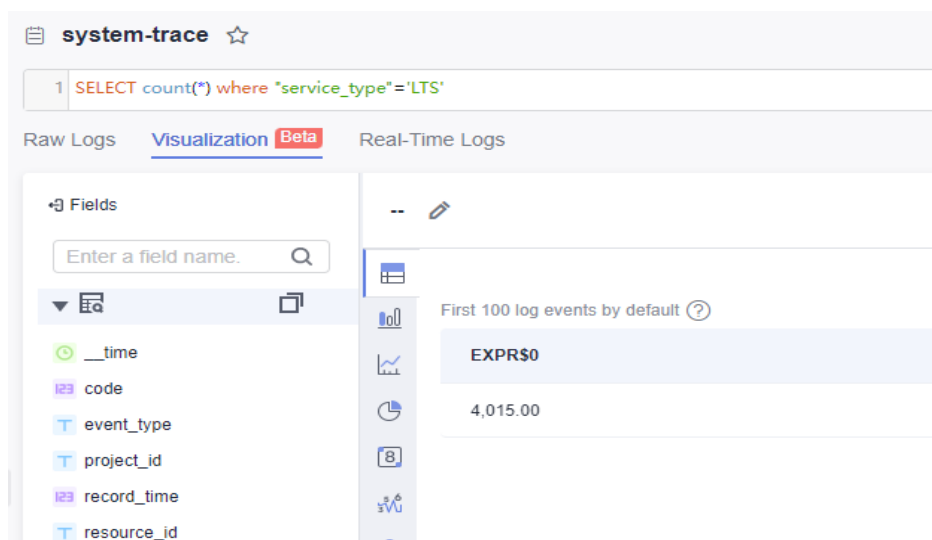


- Method 2: In the **Quick Analysis** area, locate **service\_type** and click **LTS** to quickly search for logs.

Figure 6-7 Searching for logs



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

**Figure 6-8** Querying logs using a SQL statement

## 6.5 What Do I Do If I Cannot View Historical Data in an OBS Bucket After Transferring Data to OBS?

If historical data cannot be viewed in the OBS bucket after data is transferred to OBS, it is because LTS only transfers the latest logs to an OBS bucket, and not the historical logs.

# 7 Billing

---

## 7.1 What Is the Free Quota of 500 MB For?

LTS provides a free quota of 500 MB per month for each category of operations:

- **Log read, write, and indexing:** If the traffic for log read, write, and indexing exceeds the free quota, additional traffic will be billed on a pay-per-use basis.
- **Log retention:** If the used storage space exceeds the free quota, additional storage space will also be billed on a pay-per-use basis.

If you want to suspend log collection when the free quota is used up, see [How Do I Stop Log Collection When My Free Quota Is Used Up?](#).

## 7.2 What Is the LTS Pricing and How Does LTS Charge for Log Indexing?

LTS provides a free quota of 500 MB for log read/write, log indexing, and log retention each month. When the free quota is used up, subsequent log usage will be billed. For details, see [Product Pricing Details](#).

1. Log read/write: LTS charges for the amount of compressed log data read from and written to LTS. Usually, the log compression ratio is 5: 1.  
For example, if the raw logs are 10 GB in size and are compressed down to 2 GB, 2 GB is billed.
2. Log indexing: Raw logs are full-text indexed by default for log search. Index creation will generate fees.  
For example, if the raw logs are 10 GB in size, the amount of data used for indexing is 10 GB and the indexing fee is \$0.8 USD.
3. Log retention: Space used for retaining compressed logs, indexes, and copies is billed. The space is roughly the size of the raw logs.  
For example: If the size of raw logs is 10 GB, the daily retention fee will be at most  $\$0.000125 \text{ USD/GB/hour} \times 24 \text{ hours} \times 10 \text{ GB} = \$0.03 \text{ USD}$ . Decimal numerals will be rounded off and accurate to two decimal places. If the fee is less than \$0.01 USD (after rounding off), \$0.01 USD will be displayed.

## 7.3 How Will I Be Billed If I Use the Log Transfer Function?

The **Log Transfer** of LTS is in the **open beta test (OBT)** period and is **free of charge**. After the OBT ends, you will be billed based on your traffic usage. However, if you transfer logs to OBS or DIS, you will be billed by OBS or DIS. For details, see [Product Pricing Details](#).

## 7.4 How Do I Stop Log Collection When My Free Quota Is Used Up?

LTS can collect logs from hosts and cloud services.

- **Host logs:** Host logs are collected by ICAgent. If the monthly free quota of 500 MB is used up, you will be charged for the excess log usage on a pay-per-use basis. To stop log collection when the free quota is used up, log in to the LTS console, choose **Configuration Center** in the navigation pane on the left, and disable **Continue to Collect Logs When the Free Quota Is Exceeded**. For details, see [Configuration Center](#). When log collection stops, no fees will be generated for log read/write and indexing. However, log retention will still be charged, so you are advised to change the log retention period to the minimum 1 day to accelerate the aging of collected logs. When the retention period ends, no fees will be generated for log retention.  
  
If you set the log collection to be stopped when the free quota runs out in AOM, the setting is also applied to LTS. To view the used quota, log in to the AOM console and choose **Configuration Management > Quota Configuration**.
- **Cloud service logs:** To stop collecting logs from cloud services, disable log reporting in the corresponding cloud services. For example, on the Elastic Load Balance (ELB) console, disable logging when configuring ELB access logging. For details, see [Access Logging](#). For details about how to disable log reporting for Virtual Private Cloud (VPC), see [Enabling or Disabling VPC Flow Log](#).

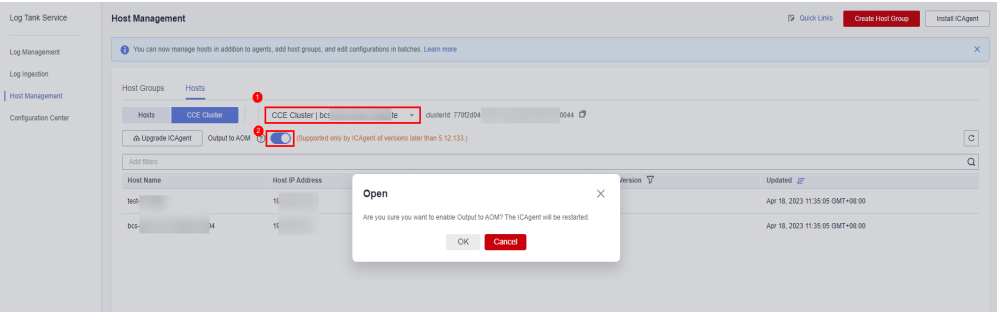
## 7.5 Why Are Fees Generated When the Log Function Is Disabled for a CCE User?

When you [buy a CCE Cluster](#), **Output to AOM** is selected by default to collect O&M data such as logs (standard output logs), metrics, and Kubernetes events. To disable the log function, perform the following steps:

- Step 1** Log in to the LTS console and choose **Host Management** in the navigation pane on the left.
- Step 2** Choose **Hosts** and click **CCE Cluster**.
- Step 3** In the CCE cluster, select the CCE cluster, and disable **Output to AOM**.



Figure 7-1 Disabling output to AOM



**Step 4** Click **OK**. After ICAgent is restarted, CCE standard output to AOM is disabled.

-----End

# 8 Others

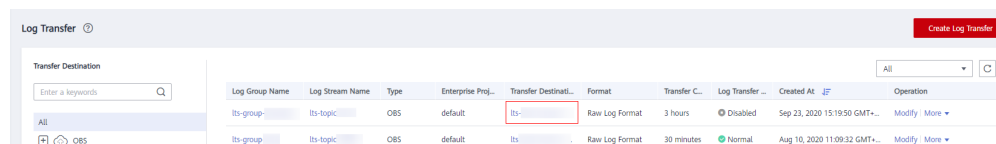
## 8.1 Quick Q&A

**Q:** Can I manually delete logs when there are too many log files?

**A:** No. Manual deletion is not supported. However, logs will be automatically deleted when the retention period ends.

**Q:** Does LTS delete logs that have been transferred to OBS buckets? How do I view transferred logs?

**A:** No. The logs will not be deleted. During log transfer, logs are "replicated" to OBS buckets. To view transferred log files, click the name of the corresponding OBS bucket on the **Log Transfer** page of the LTS console, and you will be directed to the OBS console to check the files.



**Q:** Will LTS stop collecting logs if I disable log collection in AOM?

**A:** Yes. The enablement/disablement status of log collection is synchronized between LTS and AOM. Likewise, if you set the log collection to be stopped when the free quota is used up in AOM, the setting is also applied to LTS.

## 8.2 How Do I Obtain an AK/SK Pair?

An access key ID and secret access key (AK/SK) constitute an access key.

- AK: access key ID, which is a unique identifier used in conjunction with a secret access key to sign requests cryptographically.
- SK: secret access key used in conjunction with an AK to sign requests cryptographically. It identifies a request sender and prevents the request from being modified.

Obtain and use the AK/SK of a public account.

## 8.3 How Do I Install ICAgent by Creating an Agency?

When installing ICAgent, you can create an IAM agency, and ICAgent will automatically obtain an AK/SK pair and generate the ICAgent installation command.

### Procedure

1. Log in to the console and choose > **Management & Deployment > Identity and Access Management**.
2. Choose **Agencies** in the navigation pane on the left.
3. Click **Create Agency** in the upper right corner and set parameters as follows:

**Table 8-1** Agency parameters

Parameter	Description
Agency Name	Set the agency name. For example, <b>lts_ecm_trust</b> .
Agency Type	Select <b>Cloud service</b> .
Cloud Service	Select <b>Elastic Cloud Server (ECS) and Bare Metal Server (BMS)</b> .
Validity Period	Select <b>Unlimited</b> .
Description	(Optional) Provide details about the agency.

4. Click **Next**.
5. Set **Scope** to **Region-specific projects** and select one or more projects. Under **Permissions**, search for **LTS Admin** and **APM Administrator** and select them.
6. Click **OK**. The authorization takes effect 15 to 30 minutes later.

### Making an Agency Effective

1. Choose **Service List > Computing > Elastic Cloud Server**.
2. Click the ECS where ICAgent is installed. The ECS details page is displayed.
3. Select the created agency and confirm the configuration to make the agency effective.
4. (Optional) If you want to set an agency when you are purchasing an ECS, do as follows: Click **Buy ECS** on the ECS console. In the **Configure Advanced Settings** step, set **Advanced Options** to **Configure now** and select an agency from the **Agency** drop-down list. Set the other parameters and click **Next**.

## 8.4 How Do I Migrate Logs from a Third-Party Cloud to Huawei Cloud?

If you use the log service of a third-party cloud vendor, a large amount of log data is on the vendor's object storage. You can perform the following operations to migrate the logs to Huawei Cloud:

- Hot logs (for search and analysis): typically stored for 7 to 14 days for application O&M. These logs do not need to be migrated to Huawei Cloud. Directly enable LTS on Huawei Cloud. After your services run on Huawei Cloud for 14 days, the logs stored by the third-party cloud vendor will be aged. For details, see [Accessing LTS](#).
- Archived logs (for compliance audit): generally stored on in object storage service for more than 180 days for security compliance audit. Use an object storage migration tool to migrate files from the third-party object storage service to Huawei Cloud OBS. For details, see [Migrating Data from Third-Party Cloud Service Vendors to OBS](#).

## 8.5 Can Logs Stored in LTS Be Used for Security Compliance Audit?

Logs stored in LTS can be used for security compliance audit. LTS protects logs reported to it from being modified and tampered with. You can store logs in LTS for a long time and query them at any time for security compliance audit.

## 8.6 How Long Does It Take to Generate Logs After Configuring Log Ingestion?

After configuring log ingestion on the **Log Ingestion** page of the LTS console, click the target log group on the **Log Management** page to access the details page, choose the corresponding log stream, and click the **Real-Time Logs** tab. If real-time logs are displayed, log ingestion is successful. Wait for 1 to 5 minutes. You can then view the reported raw logs on the **Raw Logs** page.