Log Tank Service

FAQs

Issue 01

Date 2024-03-07

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

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 the ICAgent Upgrade Fails?
- 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?

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?

Log Transfer

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

- **What Are the Common Causes of Abnormal Log Transfer?**
- **What Do I Do If I Cannot View Historical Data in an OBS Bucket After Transferring Data to OBS?**

Others

- **How Do I Obtain an AK/SK Pair?**
- **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.
- 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**.
  - 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**.

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 allows you to **configure keyword alarm rules**. Keyword alarms are applicable to irregular logs, such as run logs of Java programs.
- 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 5*XX* status code alarms.

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 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.

NOTE

This function is available only in regions AF-Johannesburg, AP-Singapore, CN-Hong Kong, CN East-Shanghai1, LA-Mexico City1, LA-Mexico City2, LA-Santiago, and LA-Sao Paulo1.

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.
	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.

Feature	Subfeature	LTS	ELK	Description
	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.
	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.

Feature	Subfeature	LTS	ELK	Description
	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 alarms	Keyword 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.

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 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.

3.2 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?**.

3.3 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.

----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, **create 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.

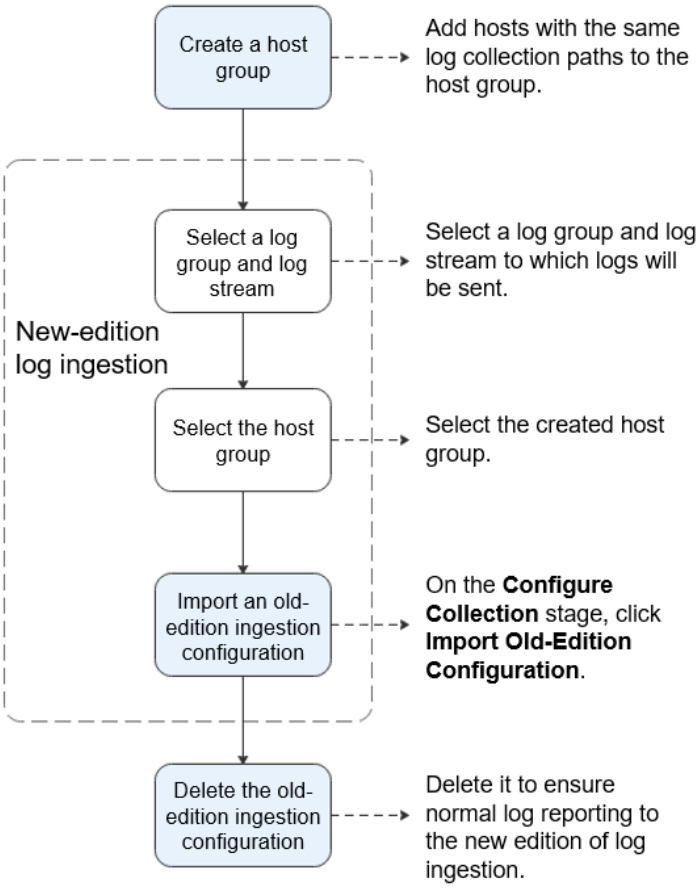
NOTE

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

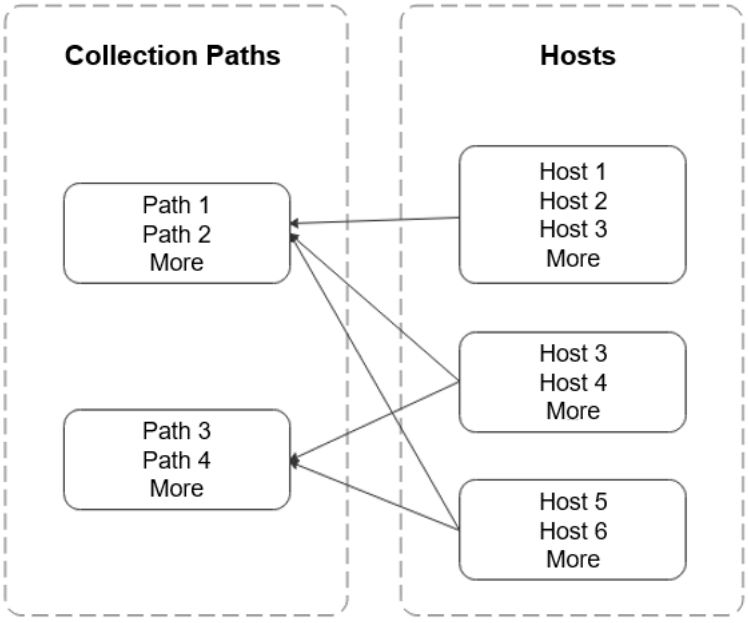
- A collection path can be configured only once. It means that you cannot add the same host path to more than one log stream. Otherwise, log ingestion may be abnormal.
- You must delete the old-edition ingestion configuration after import to ensure that logs can be reported to the new edition of log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

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

----End

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.
- 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.

- Log in to the LTS console, choose **Configuration Center** > **Log Collection**, and enable the **Log Collection** function.
- Top up your account if your account is in arrears. For details, see **Making Repayments (Postpaid 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**.
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.

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.

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.

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 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.

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 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 Others

7.1 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.

NOTE

Each user can create up to two AK/SK pairs. Once they are generated, they are permanently valid.

Ensure that the public account and AK/SK will not be deleted or disabled. If the AK/SK is deleted, the ICAgent cannot report data to LTS.

Procedure

1. Log in to the console, hover the mouse pointer over the username in the upper right corner, and select **My Credentials** from the drop-down list.
2. Choose **Access Keys**.
3. Click **Create Access Key** above the list and enter a description.
4. Click **OK** and download the AK/SK immediately.

   NOTE

   Keep the AK/SK pair secure.

7.2 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 7-1 Agency parameters

Parameter	Description
Agency Name	Set the agency name. For example, **lts_ecm_trust**.
Agency Type	Select **Cloud service**.
Cloud Service	Select **Elastic Cloud Server (ECS) and Bare Metal Server (BMS)**.
Validity Period	Select **Unlimited**.
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**.

7.3 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.

