Log Tank Service

User Guide

Issue 01

Date 2025-03-27

HUAWEI

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.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 Service Overview

1.1

Log Tank Service (LTS) is a high-performance, cost-effective log platform with diverse functions and high reliability.

It offers full-stack log collection, alarm reporting, and log transfer. It is designed for application O&M, security and compliance, and operations analysis.

1.2 Basic Concepts

Log Groups

A log group is a collection of log streams. It is similar to a folder and is used to classify and manage log streams. You can create log streams in a log group.

Log Streams

A log stream is the basic unit for log reads and writes.

You can sort logs of different types, such as operation logs and access logs, into different log streams. ICAgent will package and send the collected logs to LTS on a log stream basis. It makes it easier to find specific logs when you need them.

The use of log streams greatly reduces the number of log reads and writes and improves efficiency.

ICAgent

ICAgent is the log collection tool of LTS. If you want to use LTS to collect logs from a host, you need to install ICAgent on the host. Batch ICAgent installation is supported if you want to collect logs from multiple hosts. After ICAgent installation, you can check the ICAgent status on the LTS console in real time.

1.3 Features

Before using LTS, learn its main features in **Table 1-1**.

Table 1-1 Features

Feature	Description
Real-time log collection	Collects real-time logs and displays them on the LTS console in an intuitive and orderly manner. You can query logs or transfer logs for long-term storage. Collected logs can be structured or unstructured. Log structuring processes logs in log streams by extracting the logs in a fixed format or with a similar pattern based on the extraction rules you set.
High-volume storage and search	Supports quick log query by keyword or fuzzy match.
Log transfer	You can customize the retention period for the host and cloud service logs reported to LTS. Logs older than the retention period will be automatically deleted. For long-term storage, you can transfer logs to Object Storage Service (OBS). Log transfer is to replicate logs to the target cloud service. It means that, after log transfer, the original logs will still be retained in LTS until the configured retention period ends.

1.4 Application Scenarios

Log Collection and Analysis

When logs are scattered across hosts and cloud services and are periodically cleared, it is inconvenient to obtain the information you want. That's when LTS can come into play. LTS collects logs for unified management, and displays them on the LTS console in an intuitive and orderly manner. You can transfer logs for long-term storage. Collected logs can be quickly queried by keyword or fuzzy match. You can analyze real-time logs for security diagnosis and analysis, or obtain operations statistics, such as cloud service visits and clicks.

Service Performance Optimization

The performance of website services (such as databases and networks) and quality of other services are important metrics for measuring customer satisfaction. With the network congestion logs provided by LTS, you can pinpoint the performance bottlenecks of your website. This helps you improve your website cache and network transmission policies, as well as optimize service performance. For example:

- Analyzing historical website data to build a service network benchmark
- Detecting service performance bottlenecks in time and properly expanding the capacity or degrading the traffic
- Analyzing network traffic and optimizing network security policies

Quickly Locating Network Faults

Network quality is the cornerstone of service stability. Logs are reported to LTS to ensure that you can view and locate faults in time. Then you can quickly locate network faults and perform network forensics. For example:

- Quickly locating the root cause of an issue in Elastic Cloud Server (ECS), for example, excessive bandwidth usage.
- Determining whether services are attacked, unauthorized links are stolen, and malicious requests are sent through analyzing access logs, and locating and rectifying faults in time

1.5 Usage Restrictions

This section describes the restrictions on LTS log read/write.

Table 1-2 Log read/write restrictions

Scope	Item	Description	Remarks
Account	Log write traffic	Logs can be written at up to 5 MB/s in an account.	To increase the upper limit, contact technical support engineers.
	Log writes	Logs can be written up to 1,000 times per second in an account.	To increase the upper limit, contact technical support engineers.
	Log query traffic	Up to 1 MB of logs can be returned in a single API query for an account.	To increase the upper limit, contact technical support engineers.
	Log reads	Logs can be read up to 100 times per minute in an account.	To increase the upper limit, contact technical support engineers.

Scope	Item	Description	Remarks
Log group	Log write traffic	Logs can be written at up to 5 MB/s in a log group.	Not mandatory. Service quality cannot be ensured if this limit is exceeded.
	Log writes	Logs can be written up to 100 times per second in a log group.	Not mandatory. Service quality cannot be ensured if this limit is exceeded.
	Log query traffic	Up to 10 MB of logs are returned in a single API query for a log group.	N/A
	Log reads	Logs can be read up to 50 times per minute in a log group.	Not mandatory. Service quality cannot be ensured if this limit is exceeded.
Log stream	Log write traffic	Logs can be written at up to 5 MB/s in a log stream.	Not mandatory. Service quality cannot be ensured if this limit is exceeded.
	Log writes	Logs can be written up to 50 times per second in a log stream.	Not mandatory. Service quality cannot be ensured if this limit is exceeded.
	Log query traffic	Up to 10 MB of logs are returned in a single API query for a log stream.	N/A

Scope	Item	Description	Remarks
	Log reads	Logs can be read up to 10 times per minute in a log stream.	Not mandatory. Service quality cannot be ensured if this limit is exceeded.
	Log time	Logs in a period of 24 hours can be collected. Logs generated 24 hours before or after the current time cannot be collected.	N/A

1.6 Permissions

Description

If you need to grant your enterprise personnel permission to access your LTS resources, use Identity and Access Management (IAM). IAM provides identity authentication, fine-grained permissions management, and access control. IAM helps you secure access to your LTS resources.

With IAM, you can create IAM users and grant them permission to access only specific resources. For example, if you want some software developers in your enterprise to be able to use LTS resources but do not want them to be able to delete resources or perform any other high-risk operations, you can create IAM users and grant permission to use LTS resources but not permission to delete them.

If your account does not require individual IAM users for permissions management, you can skip this section.

IAM is a free service. You only pay for the resources in your account. For more information about IAM, see section "Service Overview" in *Identity and Access Management User Guide*.

LTS Permissions

New users do not have any permissions assigned by default. You need to first add them to one or more groups and then attach policies or roles to these groups. The users then inherit permissions from the groups and can perform specified operations on LTS based on the permissions they have been assigned.

LTS is a project-level service deployed for specific regions. When you set **Scope** to **Region-specific projects** and select the specified projects in the specified regions, the users only have permissions for LTS in the selected projects. If you select **All projects**, the users have permissions for LTS in all region-specific projects. When accessing LTS, the users need to switch to the authorized region.

You can grant permissions by using roles and policies.

- Roles: A coarse-grained authorization strategy that defines permissions by job responsibility. Only a limited number of service-level roles are available for authorization. Cloud services often depend on each other. When you grant permissions using roles, you also need to attach any existing role dependencies. Roles are not ideal for fine-grained authorization and least privilege access.
- Policies: A fine-grained authorization strategy that defines permissions required to perform operations on specific cloud resources under certain conditions. This type of authorization is more flexible and is ideal for least privilege access.

The system permissions supported by LTS are listed in **Table 1-3**.

Table 1-3 System-defined permissions for LTS

Role/ Policy Name	Description	Type	Dependencies
LTS FullAccess	Full permissions for LTS. Users with these permissions can perform operations on LTS.	System-defined policy	CCE Administrator, OBS Administrator, and AOM FullAccess
LTS ReadOnly Access	Read-only permissions for LTS. Users with these permissions can only view LTS data.	System-defined policy	CCE Administrator, OBS Administrator, and AOM FullAccess
LTS Administrator	Administrator permissions for LTS.	System-defined role	**Tenant Guest** and **Tenant Administrator**

Table 1-4 lists the common operations supported by system-defined permissions for LTS.

Table 1-4 Common operations supported by system-defined permissions

Operation	LTS FullAccess	LTS ReadOnlyAccess	LTS Administrator
Querying a log group	√	√	√
Creating a log group	√	×	√

Operation	LTS FullAccess	LTS ReadOnlyAccess	LTS Administrator
Modifying a log group	√	×	√
Deleting a log group	√	×	√
Querying a log stream	√	√	√
Creating a log stream	√	×	√
Modifying a log stream	√	×	√
Deleting a log stream	√	×	√
Configuring log collection from hosts	√	×	√
Viewing a log transfer task	√	√	√
Creating a log transfer task	√	×	√
Modifying a log transfer task	√	×	√
Deleting a log transfer task	√	×	√
Enabling a log transfer task	√	×	√
Disabling a log transfer task	√	×	√
Installing ICAgent	√	×	√
Upgrading ICAgent	√	×	√
Uninstalling ICAgent	√	×	√

1.7 Collector Privacy Statement

O&M data will be displayed on the LTS console. It is recommended that you do not upload your personal or sensitive data to LTS. Encrypt such data if you need to upload it.

ICAgent Deployment

When you install ICAgent on an ECS, your AK/SK pair is required in the installation command. Before the installation, disable history collection in the ECS to protect your AK/SK pair. After the installation, ICAgent will encrypt your AK/SK pair and store it.

1.8 Related Services

The relationships between LTS and other services are described in **Table 1**.

Table 1-5 Relationships with other services

Interaction	Related Service
With Cloud Trace Service (CTS), you can record operations associated with LTS for future query, audit, and backtracking.	CTS
You can transfer logs to Object Storage Service (OBS) buckets for long-term storage, preventing log loss.	OBS
Application Operations Management (AOM) can collect site access statistics, monitor logs sent from LTS, and generate alarms.	AOM
Identity and Access Management (IAM) allows you to grant LTS permissions to IAM users under your account.	IAM

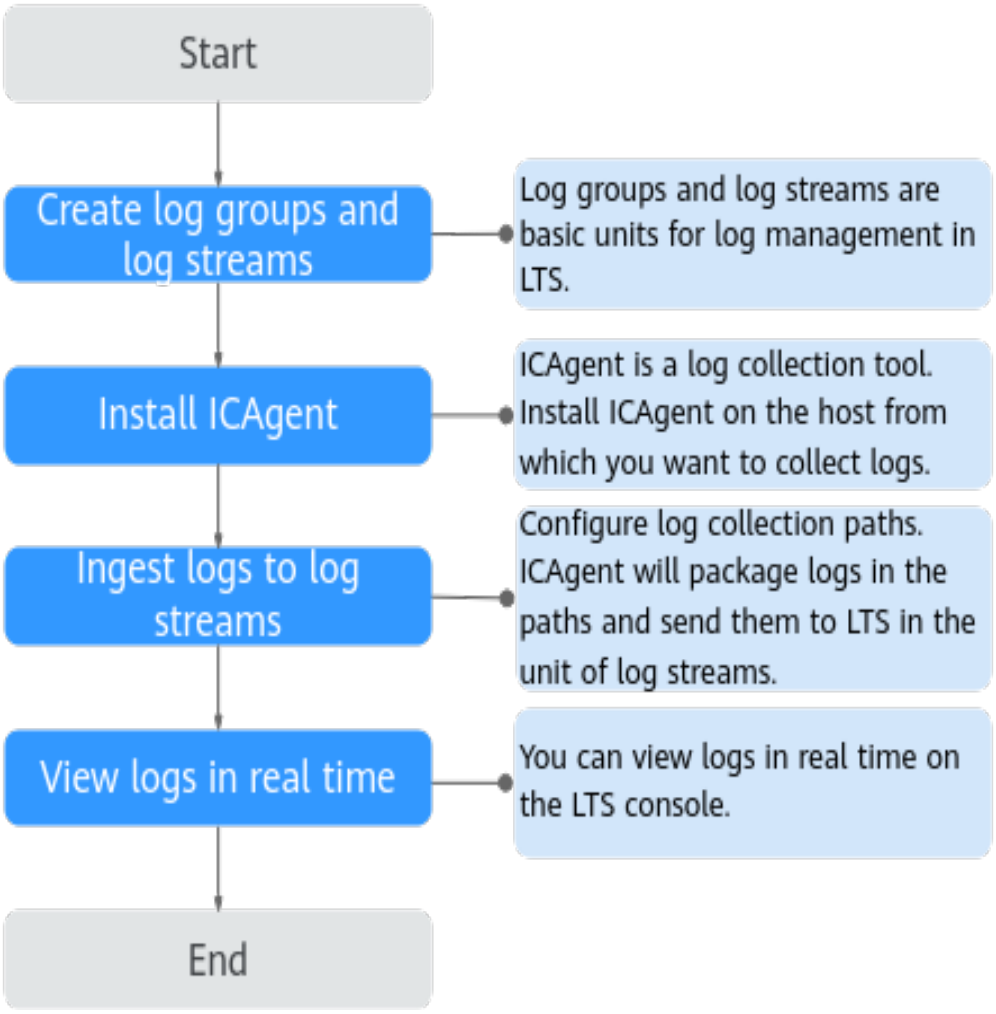
2 Getting Started

2.1 Overview

To help you quickly get started with Log Tank Service (LTS), the following sections will show you how to install ICAgent on a Linux host and ingest logs from the host to LTS.

For details, see **Figure 2-1**.

Figure 2-1 Flowchart



2.2 Creating Log Groups and Log Streams

Prerequisites

You have obtained an account and its password for logging in to the console.

Creating a Log Group

1. Log in to the management console and choose **Management & Deployment** > **Log Tank Service**.
2. On the **Log Management** page, click **Create Log Group**.
3. In the dialog box displayed, set log group parameters by referring to **Table 2-1**.

Table 2-1 Log group parameters

Parameter	Description
Log Group Name	• Enter 1 to 64 characters, including only letters, digits, hyphens (-), underscores (_), and periods (.). Do not start with a period or underscore or end with a period. • Collected logs are sent to log streams of the corresponding log groups. If there are too many logs to collect, separate logs into different log groups based on log types, and name log groups in an easily identifiable way.
Enterprise Project Name	Select an enterprise project. You can click **View Enterprise Projects** to view all enterprise projects. Enterprise projects allow you to manage cloud resources and users by project.
Log Retention (Days)	Specify the log retention period for the log group, that is, how many days the logs will be stored in LTS after being reported to LTS. By default, logs are retained for 30 days. You can set the retention period to one to 30 days.
Tag	Tag the log group as required. Click **Add Tags**, enter a tag key and value, and enable **Apply to Log Stream**. • To add more tags, repeat this step. A maximum of 20 tags can be added. • To delete a tag, click **Delete** in the **Operation** column of the tag. • A tag key can contain up to 128 characters, and a tag value can contain up to 255 characters. • A tag key must be unique. • If a tag is used by a transfer task, you need to modify the task configuration after deleting the tag.
Remark	Enter remarks. The value contains up to 1,024 characters.

4. Click **OK**. The created log group will be displayed in the log group list.

Creating a Log Stream

1. Click on the left of a log group name and click **Create Log Stream**.
2. In the dialog box displayed, set log stream parameters by referring to **Table 2-2**.

Table 2-2 Log stream parameters

Parameter	Description
Log Group Name	The name of the target log group is displayed by default.
Log Stream Name	Enter 1 to 64 characters, including only letters, digits, hyphens (-), underscores (_), and periods (.). Do not start with a period or underscore or end with a period.
Enterprise Project Name	Select the required enterprise project. The default value is **default**. You can click **View Enterprise Projects** to view all enterprise projects.
Log Retention (Days)	Specify the log retention period for the log stream, that is, how many days the logs will be stored in LTS after being reported to LTS. By default, logs are retained for 30 days. You can set the retention period to one to 30 days. • If you enable **Log Retention (Days)** for the log stream, logs are retained for the period set for the log stream. • If you disable **Log Retention (Days)** for the log stream, logs are retained for the period set for the log group. • The logs that exceed the retention period will be automatically deleted. You can transfer logs to OBS buckets for long-term storage.
Tag	You can tag log streams as required. Click **Add Tags** and enter a tag key and tag value. • To add more tags, repeat this step. A maximum of 20 tags can be added. • To delete a tag, click **Delete** in the **Operation** column of the tag. • A tag key can contain up to 128 characters, and a tag value can contain up to 255 characters. • A tag key must be unique. • If a tag is used by a transfer task, you need to modify the task configuration after deleting the tag.
Remark	Enter remarks. The value contains up to 1,024 characters.

3. Click **OK**. The created log stream will be displayed under the target log group.

2.3 Installing ICAgent

ICAgent is the log collection tool of LTS. Install ICAgent on a host from which you want to collect logs.

If ICAgent has been installed on the host when you use other cloud services, skip the installation.

Prerequisites

Before installing ICAgent, ensure that the time and time zone of your local browser are consistent with those of the host.

Installing ICAgent

Step 1 Log in to the management console and choose **Management & Deployment** > **Log Tank Service**.

Step 2 Choose **Host Management** > **Hosts** in the navigation pane.

Step 3 Click **Install ICAgent** in the upper right corner.

Step 4 Set **Host** to **Intra-Region Hosts**.

Step 5 Set **OS** to **Linux**.

Step 6 Set **Installation Mode** to **Obtain AK/SK**.

NOTE

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.

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

Step 7 Click **Copy Command** to copy the ICAgent installation command.

Step 8 Log in as user **root** to the host (for example, by using a remote login tool such as PuTTY). Run the copied command and enter the obtained AK/SK to install ICAgent.

When message **ICAgent install success** is displayed, ICAgent has been installed in the **/opt/oss/servicemgr/** directory of the host. You can then choose **Host Management** > **Hosts** in the navigation pane of the LTS console to check the ICAgent status.

----End

2.4 Ingesting Logs

The following shows how you can ingest host logs to LTS.

When ICAgent is installed, configure the paths of host logs that you want to collect in log streams. ICAgent will pack logs and send them to LTS in the unit of log streams.

Prerequisites

- You have created log groups and log streams.
- You have installed ICAgent.

Procedure

Step 1 Log in to the management console and choose **Management & Deployment** > **Log Tank Service**.

Step 2 In the navigation pane, choose **Log Ingestion** > **Ingestion Center**.

Step 3 Click **ECS (Elastic Cloud Server)** to configure log ingestion.

Step 4 Select a log stream.

1. Select a log group from the drop-down list of **Log Group**. If there are no desired log groups, click **Create Log Group** to create one.
2. Select a log stream from the drop-down list of **Log Stream**. If there are no desired log streams, click **Create Log Stream** to create one.
3. Click **Next: (Optional) Select Host Group**.

Step 5 Select one or more host groups.

1. In the host group list, select one or more host groups to collect logs. If there are no desired host groups, click **Create** in the upper left corner of the list. On the displayed **Create Host Group** page, create a host group. For details, see **Creating a Host Group (IP Address)**.

   NOTE

   You can skip this step and configure host groups as follows after the ingestion configuration is complete. However, you are advised to configure host groups during the first ingestion to ensure that the collection configuration takes effect.

   - Choose **Host Management** > **Host Groups** in the navigation pane and complete the association.
   - Choose **Log Ingestion** > **Ingestion Management** in the navigation pane, click an ingestion configuration, and make the association on the details page.

2. Click **Next: Configurations**.

Step 6 Configure the collection.

For details, see "Configure the Collection" in section "Ingesting ECS Text Logs to LTS" in the *User Guide*.

Step 7 (Optional) Configure structured logs.

Step 8 (Optional) Configure indexes.

Step 9 Click **Submit** Click **Back to Ingestion Configurations** to check the ingestion details. You can also click **View Log Stream** to view the log stream to which logs are ingested.

----End

2.5 Viewing Logs in Real Time

After the log ingestion is configured, you can view the reported logs on the LTS console in real time.

Prerequisites

- You have created log groups and log streams.
- You have installed ICAgent.
- You have ingested logs.

Viewing Logs in Real Time

1. Log in to the management console and choose **Management & Deployment** > **Log Tank Service**.
2. In the log group list, click the name of the target log group.
3. Or in the log stream list, click the name of the target log stream.
4. On the log stream details page, click **Real-Time Logs** to view logs in real time.

   Logs are reported to LTS once every 5 seconds. You may wait for at most 5 seconds before the logs are displayed.

   You can control log display by clicking **Clear** or **Pause** in the upper right corner.

   - **Clear**: Displayed logs will be cleared from the real-time view.
   - **Pause**: Loading of new logs to the real-time view will be paused.

     After you click **Pause**, the button changes to **Continue**. You can click **Continue** to resume the log loading to the real-time view.

     NOTE

     Stay on the **Real-Time Logs** tab to keep updating them in real time. If you leave the **Real-Time Logs** tab, logs will stop being loaded in real time.

3 Granting LTS Permissions to IAM Users

You can use Identity and Access Management (IAM) for fine-grained permissions control for your LTS. With IAM, you can:

- Create IAM users for personnel based on your enterprise's organizational structure. Each IAM user has their own identity credentials for accessing LTS resources.
- Grant users only the permissions required to perform a given task based on their job responsibilities.
- Entrust or a cloud service to perform efficient O&M on your LTS resources.

If your does not require individual IAM users, you can skip this section.

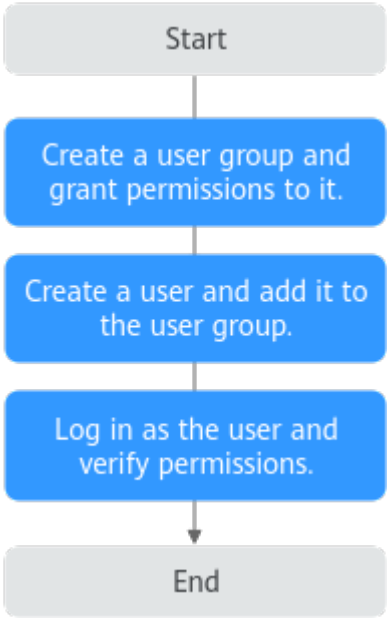
Figure 3-1 shows the process flow of role/policy-based authorization.

Prerequisites

Before granting permissions to user groups, learn about system-defined permissions in **Permissions Management** for LTS.

Process Flow

Figure 3-1 Process of granting LTS permissions



1. Log in to the IAM console. Create a user group on the IAM console and assign the **LTS FullAccess** permissions to the group. For details, see section "Creating a User Group and Assigning Permissions" in the *IAM User Guide*.
2. Create a user on the IAM console and add the user to the user group created in 1. For details, see section "Creating a User and Adding the User to a User Group" in the *IAM User Guide*.
3. Log in to the LTS console as the created user, switch to the authorized region, and verify your permissions by performing operations on the console. For details, see section "Logging In as a User" in the *IAM User Guide*.

4 Log Management

4.1 Overview

LTS manages logs by log group and stream for easy classification. Before using LTS, create a log group and then multiple log streams in the group. By collecting and storing log data in different log streams, you can search, analyze, and transfer log data and set alarm rules by log stream.

To better understand and use LTS, perform the following steps:

1. Create a log group. For details, see **Managing Log Groups**.
2. Create a log stream. For details, see **Managing Log Streams**.
3. On the **Log Management** page, view resource statistics, and the **My Favorites**, **My Favorites(Local Cache)**, and **Recently Visited** lists. For details, see **Viewing Log Management**.

4.2 Managing Log Groups

A log group is the basic unit for LTS to manage logs. It classifies and consists of log streams, but does not store any log data. Up to 100 log groups can be created for each account.

A log group usually corresponds to a project or business in a company. You are advised to sort log streams of various applications or services within a project or business to the same log group. In this way, project staff only need to monitor log streams in the log group corresponding to their project, without being distracted by log streams of other projects.

LTS allows you to add tags to log groups to help O&M personnel manage services.

Prerequisites

You have obtained an account and its password for logging in to the LTS console.

Creating a Log Group

Step 1 Log in to the management console and choose **Management & Deployment** > **Log Tank Service**. The **Log Management** page is displayed by default.

Step 2 On the **Log Management** page, click **Create Log Group**.

Step 3 On the displayed page, set log group parameters by referring to **Table 4-1**.

Table 4-1 Log group parameters

Parameter	Description
Log Group Name	• Enter 1 to 64 characters, including only letters, digits, hyphens (-), underscores (_), and periods (.). Do not start with a period or underscore or end with a period. • Collected logs are sent to log streams of the corresponding log groups. If there are too many logs to collect, separate logs into different log groups based on log types, and name log groups in an easily identifiable way.
Enterprise Project Name	Select an enterprise project. You can click **View Enterprise Projects** to view all enterprise projects. Enterprise projects allow you to manage cloud resources and users by project.
Log Retention (Days)	Specify the log retention period for the log group, that is, how many days the logs will be stored in LTS after being reported to LTS. By default, logs are retained for 30 days. You can set the retention period to one to 30 days.
Tag	Tag the log group as required. Click **Add Tags**, enter a tag key and value, and enable **Apply to Log Stream**. • To add more tags, repeat this step. A maximum of 20 tags can be added. • To delete a tag, click **Delete** in the **Operation** column of the tag. • A tag key can contain up to 128 characters, and a tag value can contain up to 255 characters. • A tag key must be unique. • If a tag is used by a transfer task, you need to modify the task configuration after deleting the tag.
Remark	Enter remarks. The value contains up to 1,024 characters.

Step 4 Click **OK**. The created log group will be displayed in the log group list.

- In the log group list, you can view information such as the log group name, tags, and log streams.
- Click the log group name to access the log stream details page.

- When multiple log groups are created concurrently, there may be a limit exceeding error.

----End

Modifying a Log Group

You can modify log group settings, such as the group name, log retention duration, or tags as follows:

Step 1 In the log group list on the **Log Management** page, locate the target log group and click **Modify** in the **Operation** column.

Step 2 On the page displayed, modify the group name, log retention period, and tags.

Step 3 Click **OK**.

Step 4 After the modification is successful, move the cursor over the log group name. The new and original log group names are displayed.

----End

Deleting a Log Group

You can delete a log group that is no longer needed. Deleting a log group will also delete the log streams and log data in the log group. **This may lead to exceptions in related tasks. In addition, deleted log groups cannot be restored. Exercise caution when performing this operation.**

If you want to delete a log group that is associated with a log transfer task, delete the task first.

Step 1 In the log group list on the **Log Management** page, locate the target log group and click **Delete** in the **Operation** column.

Step 2 Enter **DELETE** and click **OK**.

----End

Other Operations

- To check the details of a log group, including the log group name, ID, and creation time, go to the log group list and click **Details** in the **Operation** column of the desired log group.
- To download all displayed information about a log group to the local PC, click  next to the search box.

4.3 Managing Log Streams

LTS manages logs by log stream. Collected logs of different types are classified and stored in different log streams for easier log management. If there are a large number of logs, you can create multiple log streams and name them for quick log search. For example, you can sort operation logs and access logs into different log

streams, making it easier to find specific logs when you need them. You can add tags to log streams to help O&M personnel manage services.

A maximum of 100 log streams can be created in a log group. If you cannot create a log stream, delete unnecessary log streams and try again, or create log streams in another log group.

Prerequisites

You have created a log group.

Creating a Log Stream

Step 1 Log in to the management console and choose **Management & Deployment** > **Log Tank Service**.

Step 2 On the **Log Management** page, click on the left of the target log group.

Step 3 Click **Create Log Stream**. On the displayed page, set log stream parameters by referring to **Table 4-2**.

Table 4-2 Log stream parameters

Parameter	Description
Log Group Name	The name of the target log group is displayed by default.
Log Stream Name	Enter 1 to 64 characters, including only letters, digits, hyphens (-), underscores (_), and periods (.). Do not start with a period or underscore or end with a period.
Enterprise Project Name	Select the required enterprise project. The default value is **default**. You can click **View Enterprise Projects** to view all enterprise projects.
Log Retention (Days)	Specify the log retention period for the log stream, that is, how many days the logs will be stored in LTS after being reported to LTS. By default, logs are retained for 30 days. You can set the retention period to one to 30 days. • If you enable **Log Retention (Days)** for the log stream, logs are retained for the period set for the log stream. • If you disable **Log Retention (Days)** for the log stream, logs are retained for the period set for the log group. • The logs that exceed the retention period will be automatically deleted. You can transfer logs to OBS buckets for long-term storage.

Parameter	Description
Tag	You can tag log streams as required. Click **Add Tags** and enter a tag key and tag value. • To add more tags, repeat this step. A maximum of 20 tags can be added. • To delete a tag, click **Delete** in the **Operation** column of the tag. • A tag key can contain up to 128 characters, and a tag value can contain up to 255 characters. • A tag key must be unique. • If a tag is used by a transfer task, you need to modify the task configuration after deleting the tag.
Remark	Enter remarks. The value contains up to 1,024 characters.

Step 4 Click **OK**. In the log stream list, you can view information such as the log stream name and operations.

----End

Modifying a Log Stream

By default, a log stream inherits the log retention setting from the log group it belongs to.

Step 1 In the log stream list, locate the target log stream and click **Modify** in the **Operation** column.

Step 2 On the page displayed, modify the stream name, log retention period, and tags.

Step 3 Click **OK**.

Step 4 After the modification is successful, move the cursor over the log stream name. The new and original log stream names are displayed.

----End

Deleting a Log Stream

You can delete a log stream that is no longer needed. Deleting a log stream will also delete the log data in the log stream. **This may lead to exceptions in related tasks. In addition, deleted log streams cannot be restored. Exercise caution when performing this operation.**

- Before deleting a log stream, check whether any log collection task is configured for it. If there is a log collection task, deleting the log stream may affect log reporting.
- If you want to delete a log stream that is associated with a log transfer task, delete the task first.

Step 1 In the log stream list, locate the target log stream and click **Delete** in the **Operation** column.

Step 2 Enter **DELETE** and click **OK**.

----End

Other Operations

- Adding a log stream to favorites

  Click **More** > **Edit** in the **Operation** column of a log stream. On the displayed dialog box, enable **My Favorites** and/or **My Favorites(Local Cache)**. The stream is then displayed in the **My Favorites**/**My Favorites(Local Cache)** list.

- Viewing details

  Click **More** > **Details** in the **Operation** column of a log stream to view its details, including its name, ID, and creation time.

4.4 Viewing Log Management

The log management page displays resource statistics, your favorite log streams/ favorite log streams (local cache), alarm statistics, latest alarms, and recently viewed log streams.

Resource Statistics

The **Statistics** area shows resource statistics and details by category in charts. The statistics are for reference only.

Step 1 Log in to the management console and choose **Management & Deployment** > **Log Tank Service**. The **Log Management** page is displayed by default.

Step 2 Under **Overview** on the **Log Management** page, click **Details** to access the resource statistics details page.

Step 3 Select a time range as required. By default, resource statistics display log resource data of one week (from now).

There are three types of time range: relative time from now, relative time from last, and specified time.

- **From now**: queries log data generated in a time range that ends with the current time, such as the previous 1, 5, or 15 minutes. For example, if the current time is 19:20:31 and **1 hour** is selected as the relative time from now, the charts on the dashboard display the log data that is generated from 18:20:31 to 19:20:31.
- **From last**: queries log data generated in a time range that ends with the current time, such as the previous 1 or 15 minutes. For example, if the current time is 19:20:31 and **1 hour** is selected as the relative time from last, the charts on the dashboard display the log data that is generated from 18:00:00 to 19:00:00.
- **Specified**: queries log data that is generated in a specified time range.

Step 4 View the resource statistics.

- **Read/Write**: LTS charges for the amount of compressed log data read from and written to LTS. Generally, the log compression ratio is 5:1.

- **Index Traffic - Standard**: Raw logs are full-text indexed (delimited) by default for log search.
- **Standard Storage Volume**: Space used for storing compressed logs, indexes, and copies is billed. The space is roughly the size of the raw logs.
- **Raw Log Traffic**: size of raw logs.

Step 5 View the resource statistics of **Log Groups (Top 100)** and **Log Streams (Top 100)**. You can select a time range and view the daily standard storage volume (GB), daily index traffic - standard (GB), and daily read/write traffic (GB) of this period in tables or bar charts.

- For a new log group or log stream, resource statistics will be collected in at least one hour.
- Click the name of one of the top 100 log groups to query its log stream resource statistics.
- Click  to download the resource statistics of the log groups and streams. The downloaded files are in **.CSV** format.

----End

Alarm Statistics and Latest Alarms

In the lower part of **Overview**, you can view alarm statistics and latest alarms.

- The **Alarms** area displays the total number of LTS alarms and the number of alarms of each severity (**Critical**, **Major**, **Minor**, and **Warning**). You can view alarm statistics of the last 30 minutes, last 1 hour, last 6 hours, last 1 day, or last 1 week.
- The **Latest Alarms** area displays a maximum of three latest alarm rules in the last 30 minutes. To view more alarms or add alarm rules, click ••• .

Log Groups

Log groups and log streams are listed in **Log Groups**. For more information, see **Managing Log Groups** and **Managing Log Streams**.

My Favorites/My Favorites (Local Cache)

This area displays the log streams you have added to favorites, including **My Favorites** and **My Favorites(Local Cache)**.

- **My Favorites**: Save log streams to the database. This function is disabled by default. If your account has the write permission, **My Favorites** and **My Favorites(Local Cache)** are displayed.
- **My Favorites(Local Cache)**: Save log streams to the local cache of the browser. This function is disabled by default. This parameter is displayed for both writable and read-only users.

  If your account has the write permission, at least one of **My Favorites** and **My Favorites(Local Cache)** is enabled. Otherwise, log streams cannot be added to favorites.

Adding frequently used log streams to your favorites helps you quickly locate them.

The following example shows how to add a log stream of log group **lts-test** to favorites:

Step 1 In the **Log Groups** list, click on the left of log group **lts-test**.

Step 2 Click **More** > **Edit** in the **Operation** column of the target log stream. On the displayed dialog box, enable **My Favorites** and/or **My Favorites(Local Cache)** and click **OK**.

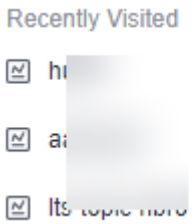
Step 3 After the log stream is added to favorites, it is displayed in **My Favorites**/**My Favorites(Local Cache)** on the right.

----End

Recently Visited

This area displays a maximum of three log streams that are recently visited.

Figure 4-1 Recently visited



4.5 Managing Tags

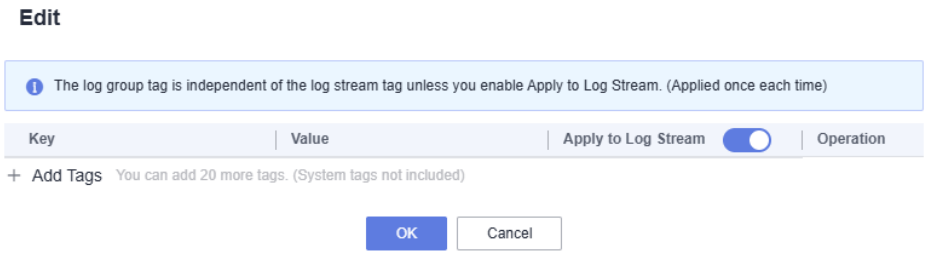
You can tag log groups, log streams, host groups, and log ingestion configurations.

Tagging a Log Group

Users can add, delete, modify, and query tags on the log group page.

1. Log in to the management console and choose **Management & Deployment** > **Log Tank Service**.
2. On the **Log Management** page, move the cursor to the **Tags** column of the target log group and click .
3. On the **Edit** page that is displayed, click **Add Tags** and enter a tag key and value. If you enable **Apply to Log Stream**, the tag will be synchronized to all log streams in the log group.

Figure 4-2 Adding a tag



NOTE

- To add multiple tags, repeat this step.
- To delete a tag, click **Delete** in the **Operation** column of the tag.
- A tag key can contain up to 128 characters, and a tag value can contain up to 255 characters.
- A tag key must be unique.
- If a tag is used by a transfer task, you need to modify the task configuration after deleting the tag.

4. Click **OK**.

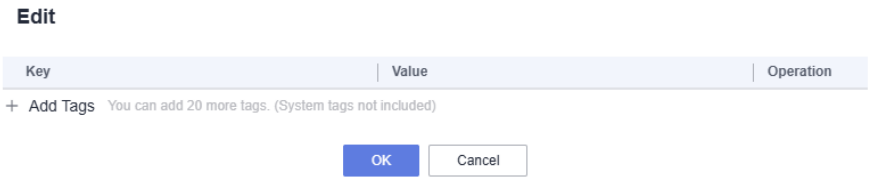
   On the **Log Management** page, you can view the added tags in the **Tags** column of the log group.

Tagging a Log Stream

You can add, delete, modify, and view tags on the log stream list page. When you manage the tags of a single log stream, the changes will not be synchronized to other streams.

1. Click in front of the name of the target log group.
2. Move the cursor to the **Tags** column of the target log stream and click .
3. On the **Edit** page that is displayed, click **Add Tags** and enter a tag key and value.

Figure 4-3 Editing a tag



NOTE

- To add multiple tags, repeat this step.
- To delete a tag, click **Delete** in the **Operation** column of the tag.
- A tag key can contain up to 128 characters, and a tag value can contain up to 255 characters.
- A tag key must be unique.
- If a tag is used by a transfer task, you need to modify the task configuration after deleting the tag.

4. Click **OK**.

   In the log stream list, you can view the system tags and added custom tags in the **Tags** column of the log stream.

Tagging a Host Group

You can add, delete, modify, and view tags of host groups. When you manage the tags of a single host group, the changes will not be synchronized to other groups.

1. Choose **Host Management** > **Host Groups** in the navigation pane.
2. Locate the target host group and click **Configure Tag** in the **Operation** column.
3. On the **Edit** page that is displayed, click **Add Tags** and enter a tag key and value.

   NOTE

   - To add multiple tags, repeat this step.
   - To delete a tag, click **Delete** in the **Operation** column of the tag.
   - A tag key can contain up to 128 characters, and a tag value can contain up to 255 characters.
   - A tag key must be unique.

4. Click **OK**. You can view the added tags in the **Tags** column of the host group.

Tagging a Log Ingestion Configuration

You can add, delete, modify, and view tags of log ingestion configurations. When you manage the tags of a single log ingestion configuration, the changes will not be synchronized to other configurations.

1. In the navigation pane, choose **Log Ingestion** > **Ingestion Management**.
2. Locate the target log ingestion configuration and click **Configure Tag** in the **Operation** column.
3. On the **Edit** page that is displayed, click **Add Tags** and enter a tag key and value.

   NOTE

   - To add multiple tags, repeat this step.
   - To delete a tag, click **Delete** next to the tag on the tag management dialog box.
   - A tag key can contain up to 128 characters, and a tag value can contain up to 255 characters.
   - A tag key must be unique.

4. Click **OK**. You can view the added tags in the **Tags** column of the log ingestion configuration.

5 Log Ingestion

5.1 Overview

Log ingestion is crucial for LTS, as it collects various log data generated during the execution of applications or services, including system statuses, errors, and user operation records. LTS stores the data in a specific location for subsequent analysis and application, which is critical to system O&M, troubleshooting, and service analysis.

LTS enables real-time log ingestion via various methods. Logs can be collected using ICAgent, ingested from cloud services, or reported to LTS via custom software or APIs. Subsequently, you can perform operations on these logs using the LTS console, such as searching and analyzing logs, visualizing log statistics in charts or dashboards, and setting alarm reporting and log transfer.

Before configuring log ingestion, ensure that ICAgent collection is enabled by referring to **Setting LTS Log Collection Quota**.

- This function is enabled by default. If you do not need to collect logs, disable this function to reduce resource usage.
- After this function is disabled, ICAgent will stop collecting logs, and the log collection function on the AOM console will also be disabled.

5.2 Ingesting Cloud Service Logs to LTS

5.2.1 Ingesting CCE Application Logs to LTS

CCE provides highly scalable, high-performance, enterprise-class Kubernetes clusters. With CCE, you can easily deploy, manage, and scale containerized applications.

After ingesting CCE logs to LTS, you can centrally manage and analyze them on the LTS console. This helps you promptly detect container issues and improve container performance and reliability.

Perform the following steps to complete the ingestion configuration:

1. **Step 1: Select a Log Stream**
2. **Step 2: Check Dependencies**
3. **Step 3: (Optional) Select a Host Group**
4. **Step 4: Configure the Collection**
5. **Step: Configure Log Structuring**
6. **Step 5: Configure Indexing**
7. **Step 6: Complete the Ingestion Configuration**

To collect logs from multiple scenarios, **set multiple ingestion configurations in a batch**.

Prerequisites

- ICAgent has been installed in the CCE cluster and a host group with custom identifiers has been created for related nodes. The system will automatically check these configurations and make necessary corrections when CCE logs are ingested to LTS.

  On the **Hosts** page, click **CCE Clusters**, select the target cluster in the search box, and click **Upgrade ICAgent**. For details, see **Upgrading ICAgent**.
- You have disabled **Output to AOM**.

Constraints

- Currently, ServiceStage hosting is not supported.
- CCE cluster nodes whose container engine is Docker are supported. .
- CCE cluster nodes whose container engine is containerd are supported. You must be using ICAgent 5.12.130 or later.
- To collect container log directories mounted to host directories to LTS, you must configure the node file path.
- Constraints on the Docker storage driver: Currently, container file log collection supports only the overlay2 storage driver. devicemapper cannot be used as the storage driver. Run the following command to check the storage driver type:
  ```
  docker info | grep "Storage Driver"
  ```
- If you select **Fixed log stream** for log ingestion, ensure that you have created a CCE cluster.

Step 1: Select a Log Stream

1. Log in to the management console and choose **Management & Deployment** > **Log Tank Service**.
2. Choose **Log Ingestion** > **Ingestion Center** in the navigation pane and click **CCE (Cloud Container Engine)**.

   You can also choose **Log Ingestion** > **Ingestion Management** in the navigation pane and click **Ingest Log**. On the displayed page, choose **CCE (Cloud Container Engine)**.
3. Choose a collection mode between **Fixed log stream** and **Custom log stream**.
   - If you set **Collect** to **Fixed log stream**, perform the following steps:

Logs will be collected to a fixed log stream. The default log streams for a CCE cluster are **stdout-***{ClusterID}* for standard output/errors, **hostfile-***{ClusterID}* for node files, **event-***{ClusterID}* for Kubernetes events, and **containerfile-***{ClusterID}* for container files. Log streams are automatically named with a cluster ID. For example, if the cluster ID is **Cluster01**, the standard output/error log stream is **stdout-Cluster01**.

Log streams that can be created for a CCE cluster are **stdout-***{ClusterID}* for standard output/errors, **hostfile-***{ClusterID}* for node files, **event-***{ClusterID}* for Kubernetes events, and **containerfile-***{ClusterID}* for container files. If one of them has been created in a log group, the log stream will no longer be created in the same log group or other log groups.

i. Select a cluster from the **CCE Cluster** drop-down list.

ii. The default log group is **k8s-log-***ClusterID*. For example, if the cluster ID is **c7f3f4a5-bcb8-11ed-a4ec-0255ac100b07**, the default log group will be **k8s-log-c7f3f4a5-bcb8-11ed-a4ec-0255ac100b07**. If there is no such group, the system displays the following message: This log group does not exist and will be automatically created to start collecting logs.

iii. Click **Next: Check Dependencies**.

– If you set **Collect** to **Custom log stream**, perform the following steps:

i. Select a cluster from the **CCE Cluster** drop-down list.

ii. Select a log group from the **Log Group** drop-down list. If there are no desired log groups, click **Create Log Group** to create one.

iii. Select a log stream from the **Log Stream** drop-down list. If there are no desired log streams, click **Create Log Stream** to create one.

iv. Click **Next: Check Dependencies**.

Step 2: Check Dependencies

The system automatically checks the following items:

1. ICAgent has been installed (version 5.12.130 or later).
2. There is a host group with the custom identifier **k8s-log-***ClusterID*.
3. There is a log group named **k8s-log-***ClusterID*. If **Fixed log stream** is selected, this item is checked.
4. The recommended log stream exists. If **Fixed log stream** is selected, this item is checked.

You need to meet all the requirements before moving on. If not, click **Auto Correct**.

- **Auto Correct**: Check the previous settings with one click.
- **Check Again**: Recheck dependencies.

Step 3: (Optional) Select a Host Group

1. In the host group list, select one or more host groups from which you want to collect logs.

- The host group to which the cluster belongs is selected by default. You can also select host groups as required.
- You can also skip this step, but the collection configuration will not take effect. You are advised to select a host group during the first ingestion configuration. If you skip this step, follow either of the following ways to configure host groups after the ingestion configuration is complete:
  - Choose **Host Management** > **Host Groups** in the navigation pane and associate host groups with ingestion configurations.
  - Choose **Log Ingestion** > **Ingestion Management** in the navigation pane. In the ingestion configuration list, click **Modify** in the **Operation** column. On the page displayed, select required host groups.

2. Click **Next: Configurations**.

Step 4: Configure the Collection

When CCE is used to ingest logs, the configuration details are as follows:

1. **Collection Configuration Name**: Enter 1 to 64 characters. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed. Do not start with a period or underscore, or end with a period.
2. **Data Source**: Select a data source type and configure it. For details, see **Table 5-1**.

Table 5-1 Data source parameters

Parameter	Description
Container standard output	Collects stderr and stdout logs of a specified container in the cluster. The standard output of the matched container is collected to the specified log stream. Standard output to AOM stops. • **Output to AOM**: ICAgent has been installed on hosts in the cluster and collects container standard output to AOM only. This function is enabled by default. To collect container standard output to LTS, disable this function. • Either **Container Standard Output (stdout)** or **Container Standard Error (stderr)** must be enabled. • If you enable **Container Standard Error (stderr)**, select your collection destination path: **Collect standard output and standard error to different files (stdout.log and stderr.log)** or **Collect standard output and standard error to the same file (stdout.log)**. • **Allow Repeated File Collection** (not available to Windows) After you enable this function, one host log file can be collected to multiple log streams. After you disable this function, each collection path must be unique. That is, the same log file in the same host cannot be collected to different log streams.

Parameter	Description
Container file	Collects file logs of a specified container in the cluster. • **Add Collection Path**: Add one or more host paths. LTS will collect logs from these paths. For more examples, see **Collection Paths**. If a container mount path has been configured for the CCE cluster workload, the paths added for this field are invalid. The collection paths take effect only after the mount path is deleted. • **Add Custom Wrapping Rule**: ICAgent determines whether a file is wrapped based on the file name rule. If your wrapping rule does not comply with the built-in rules, you can add a custom wrap rule to prevent log loss during repeated collection and wrapping. The built-in rules are *{basename}{connector}{wrapping identifier}.{suffix}* and *{basename}.{suffix}{connector}{wrapping identifier}*. Connectors can be hyphens (-), periods (.), or underscores (_), wrapping identifiers can contain only non-letter characters, and the suffix can contain only letters. A custom wrapping rule consists of *{basename}* and the feature regular expression of the wrapped file. Example: If your log file name is **test.out.log** and the names after wrapping are **test.2024-01-01.0.out.log** and **test.2024-01-01.1.out.log**, configure the collection path to **/opt/*.log**, and add a custom wrapping rule: *{basename}***\.\d{4}-\d{2}-\d{2}\.\d{1}.out.log**. • **Allow Repeated File Collection** (not available to Windows) After you enable this function, one host log file can be collected to multiple log streams. After you disable this function, each collection path must be unique. That is, the same log file in the same host cannot be collected to different log streams. • **Set Collection Filters**: Blacklisted directories or files will not be collected. If you specify a directory, all files in the directory are filtered out.

Parameter	Description
Node file	Collects files of a specified node in a cluster. • **Add Collection Path**: Add one or more host paths. LTS will collect logs from these paths. For more examples, see **Collection Paths**. • **Add Custom Wrapping Rule**: ICAgent determines whether a file is wrapped based on the file name rule. If your wrapping rule does not comply with the built-in rules, you can add a custom wrap rule to prevent log loss during repeated collection and wrapping. The built-in rules are *{basename}{connector}{wrapping identifier}.{suffix}* and *{basename}.{suffix}{connector}{wrapping identifier}*. Connectors can be hyphens (-), periods (.), or underscores (_), wrapping identifiers can contain only non-letter characters, and the suffix can contain only letters. A custom wrapping rule consists of *{basename}* and the feature regular expression of the wrapped file. Example: If your log file name is **test.out.log** and the names after wrapping are **test.2024-01-01.0.out.log** and **test.2024-01-01.1.out.log**, configure the collection path to **/opt/*.log**, and add a custom wrapping rule: *{basename}***\.\d{4}-\d{2}-\d{2}\.\d{1}.out.log**. • **Allow Repeated File Collection** (not available to Windows) After you enable this function, one host log file can be collected to multiple log streams. After you disable this function, each collection path must be unique. That is, the same log file in the same host cannot be collected to different log streams. • **Set Collection Filters**: Blacklisted directories or files will not be collected. If you specify a directory, all files in the directory are filtered out.
Kubernetes event	Collects event logs of the Kubernetes cluster. Kubernetes events of a Kubernetes cluster can be collected to only one log stream.

3. (Optional) **Kubernetes Matching Rules**: Set these parameters only when the data source type is set to **Container standard output** or **Container file**.

   After entering a regular expression, click **Verify** to verify it.

Table 5-2 Kubernetes matching rules

Parameter	Description
Namespace Name Regular Expression	Specifies the container whose logs are to be collected based on the namespace name. Regular expression matching is supported. LTS will collect logs of the namespaces with names matching this expression. To collect logs of all namespaces, leave this field empty.
Pod Name Regular Expression	Specifies the container whose logs are to be collected based on the pod name. Regular expression matching is supported. LTS will collect logs of the pods with names matching this expression. To collect logs of all pods, leave this field empty.
Container Name Regular Expression	Specifies the container whose logs are to be collected based on the container name (the Kubernetes container name is defined in **spec.containers**). Regular expression matching is supported. LTS will collect logs of the containers with names matching this expression. To collect logs of all containers, leave this field empty.
Label Whitelist	Specifies the containers whose logs are to be collected. If you want to set a Kubernetes label whitelist, **Label Key** is mandatory and **Label Value** is optional. When adding multiple whitelists, you can select the **And** or **Or** relationship. This means a container will be matched when it satisfies all or any of the whitelists. If **Label Value** is empty, LTS will match all containers whose Kubernetes label contains a specified **Label Key**. If **Label Value** is not empty, only containers whose Kubernetes label contains a specified **Label Key** that is equal to its **Label Value** are matched. **Label Key** requires full matching while **Label Value** supports regular matching.

Parameter	Description
Label Blacklist	Specifies the containers whose logs are not to be collected. If you want to set a Kubernetes label blacklist, **Label Key** is mandatory and **Label Value** is optional. When adding multiple blacklists, you can select the **And** or **Or** relationship. This means a container will be excluded when it satisfies all or any of the blacklists. If **Label Value** is empty, LTS will exclude all containers whose Kubernetes label contains a specified **Label Key**. If **Label Value** is not empty, only containers whose Kubernetes label contains a specified **Label Key** that is equal to its **Label Value** will be excluded. **Label Key** requires full matching while **Label Value** supports regular matching.
Kubernetes Label	After the **Kubernetes Label** is set, LTS adds related fields to logs. LTS adds the specified fields to the log when each **Label Key** has a corresponding **Label Value**. For example, if you enter **app** as the key and **app_alias** as the value, when the container label contains **app=lts**, **{app_alias: lts}** will be added to the log.
Container Label Whitelist	Specifies the containers whose logs are to be collected. If you want to set a container label whitelist, **Label Key** is mandatory and **Label Value** is optional. When adding multiple whitelists, you can select the **And** or **Or** relationship. This means a container will be matched when it satisfies all or any of the whitelists. If **Label Value** is empty, LTS will match all containers whose container label contains a specified **Label Key**. If **Label Value** is not empty, only containers whose container label contains a specified **Label Key** that is equal to its **Label Value** are matched. **Label Key** requires full matching while **Label Value** supports regular matching.
Container Label Blacklist	Specifies the containers whose logs are not to be collected. If you want to set a container label blacklist, **Label Key** is mandatory and **Label Value** is optional. When adding multiple blacklists, you can select the **And** or **Or** relationship. This means a container will be excluded when it satisfies all or any of the blacklists. If **Label Value** is empty, LTS will exclude all containers whose container label contains a specified **Label Key**. If **Label Value** is not empty, only containers whose container label contains a specified **Label Key** that is equal to its **Label Value** will be excluded. **Label Key** requires full matching while **Label Value** supports regular matching.

Parameter	Description
Container Label	After the **Container Label** is set, LTS adds related fields to logs. LTS adds the specified fields to the log when each **Label Key** has a corresponding **Label Value**. For example, if you enter **app** as the key and **app_alias** as the value, when the container label contains **app=lts**, **{app_alias: lts}** will be added to the log.
Environment Variable Whitelist	Specifies the containers whose logs are to be collected. If you want to set an environment variable whitelist, **Label Key** is mandatory and **Label Value** is optional. When adding multiple whitelists, you can select the **And** or **Or** relationship. This means a container will be matched when it satisfies all or any of the whitelists. If **Environment Variable Value** is empty, LTS will match all containers whose environment variable contains a specified **Environment Variable Key**. If **Environment Variable Value** is not empty, only containers whose environment variable contains a specified **Environment Variable Key** that is equal to its **Environment Variable Value** are matched. **Label Key** requires full matching while **Label Value** supports regular matching.
Environment Variable Blacklist	Specifies the containers whose logs are not to be collected. If you want to set an environment variable blacklist, **Label Key** is mandatory and **Label Value** is optional. When adding multiple blacklists, you can select the **And** or **Or** relationship. This means a container will be excluded when it satisfies all or any of the blacklists. If **Environment Variable Value** is empty, LTS will exclude all containers whose environment variable contains a specified **Environment Variable Key**. If **Environment Variable Value** is not empty, only containers whose environment variable contains a specified **Environment Variable Key** that is equal to its **Environment Variable Value** will be excluded. **Label Key** requires full matching while **Label Value** supports regular matching.
Environment Variable Label	After the environment variable label is set, the log service adds related fields to the log. LTS adds the specified fields to the log when each **Environment Variable Key** has a corresponding **Environment Variable Value**. For example, if you enter **app** as the key and **app_alias** as the value, when the Kubernetes environment variable contains **app=lts**, **{app_alias: lts}** will be added to the log.

4. Set other configurations.

Table 5-3 Other configurations

Parameter	Description
Split Logs	• If log splitting is enabled, logs exceeding the specified size will be split into multiple logs for collection. Specify the size in the range from 500 KB to 1,024 KB. For example, if you set the size to 500 KB, a 600 KB log will be split into a 500 KB log and a 100 KB log. This restriction is applicable to single-line logs only, not multi-line logs. • If log splitting is disabled, when a log exceeds 500 KB, the extra part will be truncated and discarded.
Collect Binary Files	LTS can collect binary files. Run the **file -i** *File_name* command to view the file type. **charset=binary** indicates that a log file is a binary file. If this option is enabled, binary log files will be collected, but only UTF-8 strings are supported. Other strings will be garbled on the LTS console. If this option is disabled, binary log files will not be collected.
Custom Metadata	• If this option is disabled, ICAgent will report logs to LTS based on the default system fields. You do not need to and cannot configure the fields. • If this option is enabled, ICAgent will report logs based on your selected built-in fields and fields created with custom key-value pairs. **Built-in Fields**: Select built-in fields as required. **Custom Key-Value Pairs**: Click **Add** and set a key and value.

5. Configure the log format and time by referring to **Table 5-4**.

Table 5-4 Log collection settings

Parameter	Description
Log Format	• **Single-line**: Each log line is displayed as a single log event. • **Multi-line**: Multiple lines of exception log events can be displayed as a single log event. This is helpful when you check logs to locate problems.

Parameter	Description
Log Time	**System time**: log collection time by default. It is displayed at the beginning of each log event. • Log collection time is the time when logs are collected and sent by ICAgent to LTS. • Log printing time is the time when logs are printed. ICAgent collects and sends logs to LTS with an interval of 1 second. • Restriction on log collection time: Logs are collected within 24 hours before and after the system time.
	Time wildcard: You can set a time wildcard so that ICAgent will look for the log printing time as the beginning of a log event. • If the time format in a log event is **2019-01-01 23:59:59.011**, the time wildcard should be set to **YYYY-MM-DD hh:mm:ss.SSS**. • If the time format in a log event is **19-1-1 23:59:59.011**, the time wildcard should be set to **YY-M-D hh:mm:ss.SSS**. If a log event does not contain year information, ICAgent regards it as printed in the current year. Example: YY - year (19) YYYY - year (2019) M - month (1) MM - month (01) D - day (1) DD - day (01) hh - hours (23) mm - minutes (59) ss - seconds (59) SSS - millisecond (999) hpm - hours (03PM) h:mmpm - hours:minutes (03:04PM) h:mm:sspm - hours:minutes:seconds (03:04:05PM) hh:mm:ss ZZZZ (16:05:06 +0100) hh:mm:ss ZZZ (16:05:06 CET) hh:mm:ss ZZ (16:05:06 +01:00)
Log Segmentation	This parameter needs to be specified if the **Log Format** is set to **Multi-line**. **By generation time** indicates that a time wildcard is used to detect log boundaries, whereas **By regular expression** indicates that a regular expression is used.

Parameter	Description
By regular expression	You can set a regular expression to look for a specific pattern to indicate the beginning of a log event. This parameter needs to be specified when you select **Multi-line** for **Log Format** and **By regular expression** for **Log Segmentation**. The time wildcard and regular expression will look for the specified pattern right from the beginning of each log line. If no match is found, the system time, which may be different from the time in the log event, is used. In general cases, you are advised to select **Single-line** for **Log Format** and **System time** for **Log Time**.

Step: Configure Log Structuring

1. Configure log structuring. For details, see **Setting Cloud Structuring Parsing**.
2. Click **Next: Index Settings**.

Step 5: Configure Indexing

1. Configure indexing. For details, see **Setting Indexes**.
2. Click **Submit**.

Step 6: Complete the Ingestion Configuration

The created ingestion configuration will be displayed.

- Click its name to view its details.
- Click **Modify** in the **Operation** column to modify the ingestion configuration.
- Click **Configure Tag** in the **Operation** column to add a tag.
- Click **More** > **Copy** in the **Operation** column to copy the ingestion configuration.
- Click **More** > **Delete** in the **Operation** column to delete the ingestion configuration.

  Deleting an ingestion configuration may lead to log collection failures, potentially resulting in service exceptions related to user logs. In addition, the deleted ingestion configuration cannot be restored. Exercise caution when performing this operation.

Setting Multiple Ingestion Configurations in a Batch

You can set multiple ingestion configurations for multiple scenarios in a batch, avoiding repetitive setups.

Step 1 On the **Ingestion Management** page, click **Batch Ingest** to go to the details page. For details, see **Table 5-5**.

Table 5-5 Adding configurations in batches

Type	Parameter	Description
Basic Settings	Ingestion Type	Select **CCE (Cloud Container Engine)**.
	Configurations to Add	Enter the number of ingestion configurations in the text box and click **Add**. A maximum of 100 ingestion configurations can be added, including the one already exists under **Ingestion Settings** by default. Therefore, you can add up to 99 more.
Ingestion Settings	Configuration List	1. The ingestion configurations are displayed on the left. You can add up to 99 more configurations. 2. The ingestion configuration items are displayed on the right. Set them by referring to **Step 4: Configure the Collection**. 3. After an ingestion configuration is complete, you can click **Apply to Other Configurations** to copy its settings to other configurations.

Step 2 Click **Check Parameters**. After the check is successful, click **Submit**.

The added ingestion configurations will be displayed on the **Ingestion Management** page after the batch creation is successful.

Step 3 (Optional) Perform the following operations on ingestion configurations:

- Select multiple existing ingestion configurations and click **Edit**. On the displayed page, select an ingestion type to modify the corresponding ingestion configurations.
- Select multiple existing ingestion configurations and click **Enable** or **Disable**. Logs will not be collected for disabled ingestion configurations.
- Select multiple existing ingestion configurations and click **Delete**.

----End

5.2.2 Ingesting ECS Text Logs to LTS

Elastic Cloud Server (ECS) provides scalable, on-demand cloud servers to build secure, flexible, and efficient environment for your applications.

After you configure ECS log ingestion, ICAgent collects logs from ECSs (hosts) based on your specified rules, and sends the logs to LTS by log stream. You can view and analyze these logs on the LTS console for improving host running stability and information security.

Perform the following steps to complete the ingestion configuration:

1. **Step 1: Select a Log Stream**
2. **Step 2: (Optional) Select a Host Group**

3. **Step 3: Configure the Collection**
4. **Step: Configure Log Structuring**
5. **Step 4: Configure Indexing**
6. **Step 5: Complete the Ingestion Configuration**

To collect logs from multiple scenarios, **set multiple ingestion configurations in a batch**.

Prerequisites

ICAgent has been **installed** and **added** to the host group.

Step 1: Select a Log Stream

1. Log in to the management console and choose **Management & Deployment** > **Log Tank Service**.
2. Choose **Log Ingestion** > **Ingestion Center** in the navigation pane and click **ECS (Elastic Cloud Server)**.

   You can also choose **Log Ingestion** > **Ingestion Management** in the navigation pane and click **Ingest Log**. On the displayed page, choose **ECS (Elastic Cloud Server)**.
3. Select a log group from the **Log Group** drop-down list. If there is no desired log group, click **Create Log Group**. For details, see **Managing Log Groups**.
4. Select a log stream from the **Log Stream** drop-down list. If there is no desired log stream, click **Create Log Stream**. For details, see **Managing Log Streams**.
5. Click **Next: (Optional) Select Host Group**.

Step 2: (Optional) Select a Host Group

1. Select one or more host groups from which you want to collect logs. If there are no desired host groups, click **Create** above the host group list to create one. For details, see **Managing Host Groups**.

   You can also skip this step, but the collection configuration will not take effect. You are advised to select a host group during the first ingestion configuration. If you skip this step, follow either of the following ways to configure host groups after the ingestion configuration is complete:

   - Choose **Host Management** > **Host Groups** in the navigation pane and associate host groups with ingestion configurations.
   - Choose **Log Ingestion** > **Ingestion Management** in the navigation pane. In the ingestion configuration list, click **Modify** in the **Operation** column. On the page displayed, select required host groups.
2. Click **Next: Configurations**.

Step 3: Configure the Collection

After selecting host groups, configure the collection as follows:

- Ensure that sensitive information is not collected.
- If a collection path of a host has been configured in AOM, do not configure the path in LTS.

- If log files were last modified more than 12 hours earlier than the time when the path is added, the files are not collected.

1. **Collection Configuration Name**: Enter 1 to 64 characters. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed. Do not start with a period or underscore, or end with a period.

   If you want to reuse existing collection configurations, click **Import Configuration** next to the text box. On the **Import Configuration** page, select a configuration and click **OK**.

   Import Old-Edition Configuration: Import the host ingestion configuration of the old version to the log ingestion of the new version.

   – If LTS is newly installed and **Import Old-Edition Configuration** is not displayed, you can directly create a configuration without importing the old one.

   – If LTS is upgraded, **Import Old-Edition Configuration** is displayed. Import the old configuration or create one as required.

2. **Collection Paths**: Add one or more host paths. LTS will collect logs from these paths. The rules for setting collection paths are as follows:

   – Logs can be collected recursively. A double asterisk (**) can represent up to 5 directory levels in a path.

     For example, **/var/logs/**/a.log** will match the following logs:

     ```
     /var/logs/a.log
     /var/logs/1/a.log
     /var/logs/1/2/a.log
     /var/logs/1/2/3/a.log
     /var/logs/1/2/3/4/a.log
     /var/logs/1/2/3/4/5/a.log
     ```

     - **/1/2/3/4/5/** indicates the 5 levels of directories under the **/var/logs** directory. All the **a.log** files found in all these levels of directories will be collected.
     - Only one double asterisk (**) can be contained in a collection path. For example, **/var/logs/**/a.log** is acceptable but **/opt/test/**/log/**** is not.
     - A collection path cannot begin with a double asterisk (**), such as **/**/test**, to avoid collecting system files.

   – You can use an asterisk (*) as a wildcard for fuzzy match. The wildcard (*) can represent one or more characters of a directory or file name.

     If a log collection path is similar to **C:\windows\system32** but logs cannot be collected, enable Web Application Firewall (WAF) and configure the path again.

     - Example 1: **/var/logs/*/a.log** will match all **a.log** files found in all directories under the **/var/logs/** directory:

       /var/logs/1/a.log

       /var/logs/2/a.log

     - Example 2: **/var/logs/service-*/a.log** will match files as follows:

       /var/logs/service-1/a.log

       /var/logs/service-2/a.log

- Example 3: **/var/logs/service/a*.log** will match files as follows:
  /var/logs/service/a1.log
  /var/logs/service/a2.log

– If the collection path is set to a file name, the corresponding file is collected. Only text files can be collected.

– **Add Custom Wrapping Rule**: ICAgent determines whether a file is wrapped based on the file name rule. If your wrapping rule does not comply with the built-in rules, you can add a custom wrap rule to prevent log loss during repeated collection and wrapping.

The built-in rules are *{basename}{connector}{wrapping identifier}.{suffix}* and *{basename}.{suffix}{connector}{wrapping identifier}*. Connectors can be hyphens (-), periods (.), or underscores (_), wrapping identifiers can contain only non-letter characters, and the suffix can contain only letters.

A custom wrapping rule consists of *{basename}* and the feature regular expression of the wrapped file. Example: If your log file name is **test.out.log** and the names after wrapping are **test.2024-01-01.0.out.log** and **test.2024-01-01.1.out.log**, configure the collection path to **/opt/*.log**, and add a custom wrapping rule: *{basename}***\.\d{4}-\d{2}-\d{2}\.\d{1}.out.log**.

3. **Allow Repeated File Collection** (not available to Windows)

   After you enable this function, one host log file can be collected to multiple log streams.

   After you disable this function, each collection path must be unique. That is, the same log file in the same host cannot be collected to different log streams.

4. **Set Collection Filters**: Blacklisted directories or files will not be collected.

   Blacklist filters can be exact matches or wildcard pattern matches. For details, see **Collection Paths**.

   – If you blacklist a file or directory that has been set as a collection path in the previous step, the blacklist settings will be used and the file or files in the directory will be filtered out.

   – If a log has been added to the blacklist, it cannot be collected even if you create a log ingestion task. You can collect it again only after you delete the collection path from the blacklist.

   – If you specify a directory, all files in the directory are filtered out, but log files in the folders in the directory cannot be filtered out.

5. **Collect Windows Event Logs**: To collect logs from Windows hosts, enable this option and set the following parameters.

Table 5-6 Parameters for collecting windows event logs

Parameter	Description
Log Type	Log types include **System**, **Application**, **Security**, and **Startup**.

Parameter	Description
First Collection Time Offset	If you set this parameter to **7**, logs generated within the seven days before the collection start time are collected. This offset takes effect only for the first collection to ensure that the logs are not repeatedly collected. The maximum value is 7 days.
Event Level	You can filter and collect Windows events based on their severity (**information**, **warning**, **error**, **critical**, and **verbose**). This function is available only to Windows Vista or later.

6. Set other configurations.

Table 5-7 Other configurations

Parameter	Description
Split Logs	• If log splitting is enabled, logs exceeding the specified size will be split into multiple logs for collection. Specify the size in the range from 500 KB to 1,024 KB. For example, if you set the size to 500 KB, a 600 KB log will be split into a 500 KB log and a 100 KB log. This restriction is applicable to single-line logs only, not multi-line logs. • If log splitting is disabled, when a log exceeds 500 KB, the extra part will be truncated and discarded.
Collect Binary Files	LTS can collect binary files. Run the **file -i** *File_name* command to view the file type. **charset=binary** indicates that a log file is a binary file. If this option is enabled, binary log files will be collected, but only UTF-8 strings are supported. Other strings will be garbled on the LTS console. If this option is disabled, binary log files will not be collected.
Custom Metadata	• If this option is disabled, ICAgent will report logs to LTS based on the default system fields. You do not need to and cannot configure the fields. • If this option is enabled, ICAgent will report logs based on your selected built-in fields and fields created with custom key-value pairs. **Built-in Fields**: Select built-in fields as required. **Custom Key-Value Pairs**: Click **Add** and set a key and value.

7. Configure the log format and time by referring to **Table 5-8**.

Table 5-8 Log collection settings

Parameter	Description
Log Format	• **Single-line**: Each log line is displayed as a single log event. • **Multi-line**: Multiple lines of exception log events can be displayed as a single log event. This is helpful when you check logs to locate problems.
Log Time	**System time**: log collection time by default. It is displayed at the beginning of each log event. • Log collection time is the time when logs are collected and sent by ICAgent to LTS. • Log printing time is the time when logs are printed. ICAgent collects and sends logs to LTS with an interval of 1 second. • Restriction on log collection time: Logs are collected within 24 hours before and after the system time.
	Time wildcard: You can set a time wildcard so that ICAgent will look for the log printing time as the beginning of a log event. • If the time format in a log event is **2019-01-01 23:59:59.011**, the time wildcard should be set to **YYYY-MM-DD hh:mm:ss.SSS**. • If the time format in a log event is **19-1-1 23:59:59.011**, the time wildcard should be set to **YY-M-D hh:mm:ss.SSS**. If a log event does not contain year information, ICAgent regards it as printed in the current year. Example: YY - year (19) YYYY - year (2019) M - month (1) MM - month (01) D - day (1) DD - day (01) hh - hours (23) mm - minutes (59) ss - seconds (59) SSS - millisecond (999) hpm - hours (03PM) h:mmpm - hours:minutes (03:04PM) h:mm:sspm - hours:minutes:seconds (03:04:05PM) hh:mm:ss ZZZZ (16:05:06 +0100) hh:mm:ss ZZZ (16:05:06 CET) hh:mm:ss ZZ (16:05:06 +01:00)
Log Segmentation	This parameter needs to be specified if the **Log Format** is set to **Multi-line**. **By generation time** indicates that a time wildcard is used to detect log boundaries, whereas **By regular expression** indicates that a regular expression is used.

Parameter	Description
By regular expression	You can set a regular expression to look for a specific pattern to indicate the beginning of a log event. This parameter needs to be specified when you select **Multi-line** for **Log Format** and **By regular expression** for **Log Segmentation**. The time wildcard and regular expression will look for the specified pattern right from the beginning of each log line. If no match is found, the system time, which may be different from the time in the log event, is used. In general cases, you are advised to select **Single-line** for **Log Format** and **System time** for **Log Time**.

Step: Configure Log Structuring

1. Configure log structuring. For details, see **Setting Cloud Structuring Parsing**.

   If structuring has been configured for the selected log stream, exercise caution when deleting it.
2. Click **Next: Index Settings**.

Step 4: Configure Indexing

1. Configure indexing. For details, see **Setting Indexes**.
2. Click **Submit**.

Step 5: Complete the Ingestion Configuration

The created ingestion configuration will be displayed.

- Click its name to view its details.
- Click **Modify** in the **Operation** column to modify the ingestion configuration.
- Click **Configure Tag** in the **Operation** column to add a tag.
- Click **More** > **Copy** in the **Operation** column to copy the ingestion configuration.
- Click **More** > **Delete** in the **Operation** column to delete the ingestion configuration.

  Deleting an ingestion configuration may lead to log collection failures, potentially resulting in service exceptions related to user logs. In addition, the deleted ingestion configuration cannot be restored. Exercise caution when performing this operation.

Setting Multiple Ingestion Configurations in a Batch

You can set multiple ingestion configurations for multiple scenarios in a batch, avoiding repetitive setups.

Step 1 On the **Ingestion Management** page, click **Batch Ingest** to go to the details page. For details, see **Table 5-9**.

Table 5-9 Adding configurations in batches

Type	Parameter	Description
Basic Settings	Ingestion Type	Select **ECS (Elastic Cloud Server)**.
	Configurations to Add	Enter the number of ingestion configurations in the text box and click **Add**. A maximum of 100 ingestion configurations can be added, including the one already exists under **Ingestion Settings** by default. Therefore, you can add up to 99 more.
Ingestion Settings	Configuration List	1. The ingestion configurations are displayed on the left. You can add up to 99 more configurations. 2. The ingestion configuration items are displayed on the right. Set them by referring to **Step 3: Configure the Collection**. 3. After an ingestion configuration is complete, you can click **Apply to Other Configurations** to copy its settings to other configurations.

Step 2 Click **Check Parameters**. After the check is successful, click **Submit**.

The added ingestion configurations will be displayed on the **Ingestion Management** page after the batch creation is successful.

Step 3 (Optional) Perform the following operations on ingestion configurations:

- Select multiple existing ingestion configurations and click **Edit**. On the displayed page, select an ingestion type to modify the corresponding ingestion configurations.
- Select multiple existing ingestion configurations and click **Enable** or **Disable**. Logs will not be collected for disabled ingestion configurations.
- Select multiple existing ingestion configurations and click **Delete**.

----End

5.3 Using APIs to Ingest Logs to LTS

5.3.1 Collecting Logs Using APIs

You can report logs to LTS with REST APIs. LTS supports APIs for reporting logs and high-precision logs.

The application scenarios and access IP addresses of the APIs are as follows:

Table 5-10 Scenarios

Name	Log Time	Example	Scenario

Reporting Logs	When invoking the API to upload a batch of logs, you can specify an initial time with log_time_ns field.
	Time of each log can be calculated with log_time_ns+sequence count.
		{
		"log_time_ns": "1586850540000000000",
		"contents": [
		"log1",
		"log2"
		],
		"labels": {
		"user_tag": "string"
		}
		}
		When reported to LTS:
		The time of log1 is **1586850540000000000**.
		The time of log2 is **1586850540000000001**.
			The logs are generated in sequence at similar time.

Reporting High-Precision Logs	When you invoke the API to upload a batch of logs, the log_time_ns field must be used to specify the log time for each log.	{
		"contents":[
		{
		"log_time_ns":"1586850540000000000",
		"log":"log3"
		},
		{
		"log_time_ns":"1586850540000000008",
		"log":"log4"
		}
		],
		"labels":{
		"user_tag":"string"
		}
		}
		When reported to LTS:
		The time of log3 is **1586850540000000000**.
		The time of log4 is **1586850540000000008**.
			The uploaded logs are generated out of order at different times. Each log needs to have its own timestamp.

5.3.2 API for Reporting Logs

Function

This API is used to report tenant logs from a host to LTS.

The access IP address is contained in the ICAgent installation command displayed on the LTS console. The port number is 8102. You can check the **Example Request** to see how to add the access IP address and port number in a request.

URI

POST /v2/{project_id}/lts/groups/{log_group_id}/streams/{log_stream_id}/tenant/contents

Table 5-11 URI parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see . Value length: 32 characters
log_group_id	Yes	String	Log group ID. For details about how to obtain it, see . Value length: 36 characters
log_stream_id	Yes	String	Log stream ID. For details about how to obtain it, see . Value length: 36 characters A write rate exceeding 100 MB/s per log stream may cause log losses.

Request Parameters

Table 5-12 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Indicates the user token obtained from IAM. Minimum length: 1,000 characters Maximum length: 2,000 characters
Content-Type	Yes	String	Set this parameter to **application/json;charset=UTF-8**. Minimum length: 30 characters Maximum length: 30 characters

Table 5-13 Request body parameters

Parameter	Mandatory	Type	Description
log_time_ns	Yes	Long	Time when log data is reported (UTC time in nanoseconds). Logs reported to LTS through APIs are retained for two days (from the log reporting time to the current time). Logs reported more than two days ago will be deleted.
contents	Yes	Array of String	Indicates the log content.
labels	Yes	Object	Custom labels.
tenant_project_id	No	String	Project ID. For details about how to obtain it, see .

Response Parameters

When the status code is **200**, the response parameters are as follows:

Table 5-14 Response body parameters

Parameter	Type	Description
errorCode	String	Indicates the error code.
error_msg	String	Indicates the response description.
result	String	Response result.

When the status code is **400**, the response parameters are as follows:

Table 5-15 Response body parameters

Parameter	Type	Description
errorCode	String	Indicates the error code.
error_msg	String	Indicates the error description.
result	String	Response result.

When the status code is **401**, the response parameters are as follows:

Table 5-16 Response body parameters

Parameter	Type	Description
errorCode	String	Indicates the error code.
error_msg	String	Indicates the error description.
result	String	Response result.

When the status code is **500**, the response parameters are as follows:

Table 5-17 Response body parameters

Parameter	Type	Description
errorCode	String	Indicates the error code.
error_msg	String	Indicates the error description.
result	String	Response result.

When the status code is **503**, the response parameter is as follows:

Table 5-18 Response body parameter

Parameter	Type	Description
result	String	The requested service is unavailable.

Example Request

```
POST https://{access_IP_address:8102}/v2/{project_id}/lts/groups/{log_group_id}/streams/{log_stream_id}/tenant/contents

{
    "log_time_ns": 1586850540000000000,
    "contents": [
        "Fri Feb  1 07:48:04 UTC 2019 0\n",
        "Sat April 18 16:04:04 UTC 2019"
    ],
    "labels": {
        "user_tag": "string"
    }
}
```

Example Response

Example response with status code **200**:

Logs are reported.

```
{
  "errorCode": "SVCSTG.ALS.200.200",
```



```
  "error_msg": "Report success.",
  "result": null
}
```

Example response with status code **401**:

The authentication information is incorrect or invalid.

```
{
  "errorCode" : "SVCSTG.ALS.403.105",
  "error_msg" : "Project id is invalid.",
  "result": null
}
```

Status Code

Status Code	Description
200	The request has succeeded.
400	The request is invalid. Modify the request based on the description in **error_msg** before a retry.
401	The authentication information is incorrect or invalid.
500	An internal error occurred.
503	The requested service is unavailable.

5.3.3 API for Reporting High-Precision Logs

Function

This API is used to report tenant logs from a host to LTS.

The access IP address is contained in the ICAgent installation command displayed on the LTS console. The port number is 8102. You can check the **Example Request** to see how to add the access IP address and port number in a request.

Each log event will carry a nanosecond-level timestamp when it is reported. When you view logs on the LTS console, the log events are sorted by timestamp.

URI

POST /v2/{project_id}/lts/groups/{log_group_id}/streams/{log_stream_id}/tenant/contents/high-accuracy

Table 5-19 URI parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see . Value length: 32 characters
log_group_id	Yes	String	Log group ID. For details about how to obtain it, see . Value length: 36 characters
log_stream_id	Yes	String	Log stream ID. For details about how to obtain it, see . Value length: 36 characters A write rate exceeding 100 MB/s per log stream may cause log losses.

Request Parameters

Table 5-20 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Indicates the user token obtained from IAM. Minimum length: 1,000 characters Maximum length: 2,000 characters
Content-Type	Yes	String	Set this parameter to **application/json;charset=UTF-8**. Minimum length: 30 characters Maximum length: 30 characters
Content-Encoding	No	String	Log compression format. Example value: • **GZIP** • **SNAPPY** • **gzip** • **snappy**

Table 5-21 Request body parameters

Parameter	Mandatory	Type	Description
contents	Yes	Array of **LogContents**	Indicates a list of log events that carry reporting timestamps.
labels	Yes	Object	Custom labels.
tenant_project_id	No	String	Project ID. For details about how to obtain it, see .

Table 5-22 LogContents

Parameter	Mandatory	Type	Description
log_time_ns	Yes	Long	Time when log data is reported (UTC time in nanoseconds). Logs reported to LTS through APIs are retained for two days (from the log reporting time to the current time). Logs reported more than two days ago will be deleted.
log	Yes	String	Indicates the log content.

Response Parameters

When the status code is **200**, the response parameters are as follows:

Table 5-23 Response body parameters

Parameter	Type	Description
errorCode	String	Indicates the error code.
error_msg	String	Indicates the response description.
result	String	Response result.

When the status code is **400**, the response parameters are as follows:

Table 5-24 Response body parameters

Parameter	Type	Description
errorCode	String	Indicates the error code.
error_msg	String	Indicates the error description.
result	String	Response result.

When the status code is **401**, the response parameters are as follows:

Table 5-25 Response body parameters

Parameter	Type	Description
errorCode	String	Indicates the error code.
error_msg	String	Indicates the error description.
result	String	Response result.

When the status code is **500**, the response parameters are as follows:

Table 5-26 Response body parameters

Parameter	Type	Description
errorCode	String	Indicates the error code.
error_msg	String	Indicates the error description.
result	String	Response result.

When the status code is **503**, the response parameter is as follows:

Table 5-27 Response body parameter

Parameter	Type	Description
result	String	The requested service is unavailable.

Example Request

```
POST https://{access_IP_address:8102}/v2/{project_id}/lts/groups/{log_group_id}/streams/{log_stream_id}/tenant/contents/high-accuracy

{
   "contents": [
      {
```



```
            "log_time_ns": 1586850540000000000,
            "log": "Fri Feb  15 15:48:04 UTC 2019"
        },
        {
            "log_time_ns": 1586850540000000001,
            "log": "Sat April 18 16:04:04 UTC 2019"
        }
    ],
    "labels": {
        "user_tag": "string"
    }
}
```

Example Response

Example response with status code **200**:

Logs are reported.

```
{
  "errorCode": "SVCSTG.ALS.200.200",
  "error_msg": "Report success.",
  "result": null
}
```

Example response with status code **401**:

The authentication information is incorrect or invalid.

```
{
  "errorCode" : "SVCSTG.ALS.403.105",
  "error_msg" : "Project id is invalid.",
  "result": null
}
```

Status Code

Status Code	Description
200	The request has succeeded.
400	The request is invalid. Modify the request based on the description in **error_msg** before a retry.
401	The authentication information is incorrect or invalid.
500	An internal error occurred.
503	The requested service is unavailable.

5.4 Other Ingestion Modes

5.4.1 Ingesting Logs to LTS Across IAM Accounts

If you choose **Cross-Account Ingestion - Log Stream Mapping** as the log ingestion type, you can create an agency to map the log stream of the delegator account to that of the delegated account. The delegated account is the current account used to log in to LTS.

Prerequisites

An agency relationship has been created.

Constraints

Before data synchronization is complete, data in the target and source log streams may be different. Check back later in one hour.

Setting Cross-Account Ingestion

If you choose cross-account ingestion as the log ingestion type, perform the following operations to configure the ingestion:

Step 1 Log in to the management console and choose **Management & Deployment** > **Log Tank Service**.

Step 2 Choose **Log Ingestion** > **Ingestion Center** in the navigation pane and click **Cross-Account Ingestion - Log Stream Mapping**.

You can also choose **Log Ingestion** > **Ingestion Management** in the navigation pane and click **Ingest Log**. On the displayed page, click **Cross-Account Ingestion - Log Stream Mapping**.

Step 3 Select an agency.

Set parameters by referring to **Table 5-28** and click **Next: Log Stream Mapping**.

Table 5-28 Agency parameters

Parameter	Description
Agency Name	Enter the name of the agency created by the delegator. A delegator account can create an agency to delegate resource management permissions to another account.
Delegator Account Name	Enter the delegator account name to verify the delegation.

Step 4 Map log streams.

On the **Log Stream Mapping** page, there are two ways to configure ingestion rules: automatic and manual configuration.

- **Automatic configuration**
  a. Click **Auto Configure**.
  b. On the displayed page, set the required parameters and click **OK**.

Table 5-29 Parameters of automatic ingestion rule configuration

Parameter	Description
Rule Name Prefix	Enter the rule name prefix. In automatic configuration, this prefix is used to generate multiple ingestion rules. Can contain only letters, digits, underscores (_), hyphens (-), and periods (.). The prefix cannot start with a period or underscore, or end with a period. If you do not specify a prefix, the default rule name prefix **rule** will be used.
Select the log groups or log streams that you want to ingest from the delegator account.	Up to 20 log groups or log streams can be selected.

By default, the names of the target log groups and target log streams of the delegated account are the same as those of the source log groups and source log streams of the delegator account. You can also manually change the names of the target log groups and target log streams.

c. Click **Preview**.

i. There are two types of preview results:

- **A new target log stream will be created**: A target log group or log stream will be created in the delegated account.
- **An existing target log stream will be ingested**: The target log group or log stream already exists in the delegated account.

ii. Preview error messages are as follows:

- Source log stream *xxx* has been configured as the target log stream.
- Target log stream *xxx* has been configured as the source log stream.
- Target log stream *xxx* already exists in another log group.
- Target log stream *xxx* exists in different target log groups.
- Duplicate rule names.
- The source log stream *xxx* is already mapped.
- The number of log groups has reached the upper limit. Select an existing log group.

If any of the preceding error messages is displayed, delete the corresponding ingestion rule of the log stream.

d. After the preview is complete, click **Submit**.

- **Manual configuration**

a. On the **Log Stream Mapping** page, click **Add Rule**. Set the rule by referring to **Table 5-30**.

Table 5-30 Parameters

Parameter		Description
Rule Name		The default value is **rule**_*xxx*. You can also specify a name as needed. Can contain only letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot start with a period or underscore, or end with a period.
Delegator Account	Source Log Group	Log group of the delegator account. Select an existing log group.
	Source Log Stream	Log stream of the delegator account. Select an existing log stream.
Delegated Account	Target Log Group	Log group of the delegator account. You can select an existing log group or enter a name to create one.
	Target Log Stream	Log stream of the delegated account. You can select an existing log stream or enter a name to create one.

b. Click **Preview**.

i. There are two types of preview results:

- **A new target log stream will be created**: A target log group or log stream will be created in the delegated account.
- **An existing target log stream will be ingested**: The target log group or log stream already exists in the delegated account.

ii. Preview error messages are as follows:

- Source log stream *xxx* has been configured as the target log stream.
- Target log stream *xxx* has been configured as the source log stream.
- Target log stream *xxx* already exists in another log group.
- Target log stream *xxx* exists in different target log groups.
- Duplicate rule names.
- The source log stream *xxx* is already mapped.
- The number of log groups has reached the upper limit. Select an existing log group.

If any of the preceding error messages is displayed, delete the corresponding ingestion rule of the log stream.

c. After the preview is complete, click **Submit** and wait until the log ingestion task is created.

Step 5 Complete the ingestion configuration.

After the configuration is complete, data will be synchronized within one hour. Please check back later.

- If multiple log streams are ingested, you can click **Back to Ingestion Configurations** to view the log ingestion list.
- If a single log stream is ingested, click **Back to Ingestion Configurations** to view the log ingestion list. Click **View Log Stream** to view details about the ingested log stream.

----End

6 Host Management

6.1 Managing Host Groups

Host groups allow you to configure host log ingestion efficiently. You can add multiple hosts to a host group and associate the host group with log ingestion configurations. The ingestion configurations will then be applied to all the hosts in the host group.

- When there is a new host, simply add it to a host group and the host will automatically inherit the log ingestion configurations associated with the host group.
- You can also use host groups to modify the log collection paths for multiple hosts at one go.

You can create host groups of the IP address and custom identifier types.

- **Creating a Host Group (IP Address)**: Select hosts of the IP address type and add them to the host group.
- **Creating a Host Group (Custom Identifier)**: You need to create identifiers for each host group and host. Hosts with an identifier will automatically be included in the corresponding host group sharing that identifier.

  Host groups with custom identifiers are suitable for the following scenarios:

  - In custom network environments like VPCs, potential IP address conflicts among hosts may impede ICAgent management in LTS. Using custom identifiers can resolve this issue.
  - Multiple servers using the same custom identifier enable auto scaling of host groups. Simply assign a custom identifier for a new host; LTS will then automatically identify the host and add it to corresponding host group with the same identifier.

Creating a Host Group (IP Address)

Step 1 Log in to the management console and choose **Management & Deployment** > **Log Tank Service**.

Step 2 Choose **Host Management** > **Host Groups** in the navigation pane.

Step 3 Click **Create Host Group** in the upper right corner.

Step 4 In the displayed slide-out panel, enter a host group name, select **IP** for **Host Group Type**, and select a host OS (**Linux** or **Windows**).

Step 5 In the host list, select one or more hosts to add to the group and click **OK**.

- You can filter hosts by host name or host IP address. You can also click **Search by Host IP Address** and enter multiple host IP addresses in the displayed search box to search for matches.
- If your desired hosts are not in the list, click **Install ICAgent**. On the displayed page, install ICAgent on the hosts as prompted. For details, see **Installing ICAgent**.

----End

Creating a Host Group (Custom Identifier)

To create a host group of the custom identifier type, you need to plan the hosts to be identified in advance and ensure that ICAgent has been installed on the hosts.

Step 1 Click **Create Host Group** in the upper right corner.

Step 2 In the displayed slide-out panel, enter a host group name, select **Custom identifier** for **Host Group Type**, and select a host OS (**Linux** or **Windows**).

Step 3 Enter a custom identifier. You can also click 

to enter more.

Up to 10 custom identifiers can be added.

Step 4 Click **OK**. After the host group is created, go to **5** to add hosts to it.

Step 5 Perform the following operations to create the **custom_tag** file to save host tags:

1. Log in to the host and run the **cd /opt/cloud** command. If the system indicates that the **/opt/cloud** directory does not exist, run the **mkdir /opt/cloud/** command to create it. If the **/opt/cloud** directory already exists, navigate to it and run the **mkdir lts** command to create the **lts** directory in it.
2. Run the **chmod 750 lts** command to modify the permission on the **lts** directory.
3. Run the **touch custom_tag** command in the **lts** directory to create the **custom_tag** file.
4. Run the **chmod 640 custom_tag;vi custom_tag** command to modify the **custom_tag** permission and open the file.
5. Press **i** to enter the insert mode, enter a custom identifier, press **Esc**, enter **:wq!**, save the modification and exit.
6. Use either of the following methods to add a host to the custom identifier host group:

Table 6-1 Methods

Type	Method 1 (Recommended)	Method 2
Linux host	View the host's identifier in the **custom_tag** file of the **/opt/cloud/lts** directory on the host. Then, add the identifier to the host group to include the host within it. For example, if the **custom_tag** file in the **/opt/cloud/lts** directory shows the host's identifier as **test1**, simply add **test1** to the group's custom identifiers.	– Add the host group's custom identifier to the **custom_tag** file in the **/opt/cloud/lts** directory on the host to include the host within the host group. For example, if the group's custom identifier is **test**, enter **test** into the **custom_tag** file. – If the group has multiple custom identifiers, simply enter any one of them into the **custom_tag** file of the **/opt/cloud/lts** directory on the host.
Windows host	View the host's identifier in the **custom_tag** file of the **C:\opt\cloud\lts** directory on the host. Then, add the identifier to the host group to include the host within it. For example, if the **custom_tag** file in the **C:\opt\cloud\lts** directory shows the host's identifier as **test1**, simply add **test1** to the group's custom identifiers.	– Add the host group's custom identifier to the **custom_tag** file in the **C:\opt\cloud\lts** directory on the host to include the host within the host group. For example, if the group's custom identifier is **test**, enter **test** into the **custom_tag** file. – If the group has multiple custom identifiers, simply enter any one of them into the **custom_tag** file of the **C:\opt\cloud\lts** directory on the host.

----End

Modifying a Host Group

You can change the name of a host group, add hosts to or remove hosts from a host group, or associate a host group with log ingestion configurations. For details, see **Table 6-2**.

Table 6-2 Operations on host groups

Operation	Procedure
Changing a host group name	1. Go to the **Host Groups** page. 2. In the host group list, click the modification button in the **Operation** column of the target host group. 3. On the displayed dialog box, modify the information such as the host group name and custom identifier. 4. Click **OK**.
Adding hosts to a host group	**Method 1:** 1. In the host group list, click ⌄ in the row containing the target host group whose type is **IP**. 2. Click **Add Host**. 3. In the displayed slide-out panel, all hosts that are not in the host group and run the selected OS type are displayed. Select the hosts to be added to the host group. • You can filter hosts by host name or host IP address. You can also click Search by Host IP Address ⌄⌄ and enter multiple host IP addresses in the displayed search box to search for matches. • If your desired hosts are not in the list, click **Install ICAgent**. On the displayed page, install ICAgent on the hosts as prompted. For details, see **Installing ICAgent**. 4. Click **OK**. **Method 2:** 1. Choose **Host Management** > **Hosts** in the navigation pane. 2. In the host list, select the target hosts and click **Add to Host Group**. 3. In the displayed slide-out panel, select the target host group. 4. Click **OK**.
Removing a host from a host group	1. In the host group list, click ⌄ in the row containing the target host group. 2. In the host list, click **Remove** in the **Operation** column of the row containing the host to be removed. 3. In the displayed dialog box, click **OK**. This operation is not supported for hosts in the custom identifier host group.

Operation	Procedure
Uninstalling ICAgent from a host	1. In the host group list, click ⌄ in the row containing the target host group. 2. In the host list, click **Uninstall ICAgent** in the **Operation** column of the row containing the target host. 3. In the displayed dialog box, click **OK** to uninstall ICAgent from the host and remove the host from the host group. • This operation is not supported for hosts in the custom identifier host group. • If the host has also been added to other host groups, it will be removed from those groups as well.
Removing hosts from a host group	1. In the host group list, click ⌄ in the row containing the target host group. 2. In the host list, select the target hosts and click the **Remove** button above the list. 3. Click **OK**.
Associating a host group with an ingestion configuration	1. In the host group list, click ⌄ in the row containing the target host group. 2. The **Hosts** tab page is displayed by default. Click the **Associated Ingestion Configurations** tab. 3. Click **Associate**. 4. In the displayed slide-out panel, select the target ingestion configuration. 5. Click **OK**. The associated ingestion configuration is displayed in the list.
Disassociating a host group from an ingestion configuration	1. On the **Associated Ingestion Configurations** tab page, locate the target ingestion configuration, and then click **Disassociate** in the **Operation** column. 2. Click **OK**.
Disassociating a host group from multiple ingestion configurations	1. Click the **Associated Ingestion Configurations** tab, select the target ingestion configurations, and then click **Disassociate** above the list. 2. Click **OK**.
Copying a host group ID	Hover your cursor over a host group name to copy the host group ID.

Operation	Procedure
Exporting host information	1. On the **Hosts** page, switch to the **Intra-Region Hosts**, **CCE Cluster**, or **Extra-Region Hosts** tab and select the desired hosts. 2. Click **Export** to export the information of the selected hosts to the local PC.

Deleting Host Groups

Step 1 Choose **Host Management** > **Host Groups** in the navigation pane.

Step 2 Delete a host group:

1. Click the deletion icon in the **Operation** column of the row containing the target host group.
2. In the displayed dialog box, click **OK**.

Step 3 Delete host groups in batches:

1. Select host groups to be deleted and click **Delete** above the list.
2. In the displayed dialog box, click **OK**.

----End

6.2 Managing Hosts

6.2.1 Installing ICAgent

To use LTS to collect logs (such as host metrics, container metrics, node logs, container logs, and standard output logs) from intra-region hosts, you need to install ICAgent on the hosts. ICAgent is a log collection tool for LTS. It runs on hosts where logs need to be collected.

Prerequisites

Before installing ICAgent, ensure that the time and time zone of your local browser are consistent with those of the host. If they are inconsistent, errors may occur during log reporting.

Installation Methods

There are two methods to install ICAgent.

Table 6-3 Installation methods

Method	Scenario
Initial installation	You can use this method to install ICAgent on a host that has no ICAgent installed. Run the **ps -aux | grep icagent** command on the host to check whether there is an ICAgent process. If no, the ICAgent has not been installed.
Inherited installation (supported only for Linux hosts)	When ICAgent has already been installed on one host but needs to be installed on multiple hosts, you can use this method.

Initial Installation (Linux)

Step 1 Log in to the management console and choose **Management & Deployment** > **Log Tank Service**.

Step 2 Choose **Host Management** > **Hosts** in the navigation pane.

Step 3 Click **Install ICAgent** in the upper right corner.

Before installing ICAgent, ensure that the time and time zone of your local browser are consistent with those of the host.

Table 6-4 Installing ICAgent

Parameter	Description	Example
Host	**Intra-region hosts** is selected by default. Check whether the host whose logs need to be collected is in or out of the region.	-
OS	**Linux** is selected by default.	-

Parameter	Description	Example
Installation Mode	• If you select **Obtain AK/SK**, you need to obtain the AK/SK in advance. An AK is used together with an SK to sign requests cryptographically, ensuring that the requests are secret, complete, and correct. For details, see **How Do I Obtain an AK/SK Pair?** 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. • If you select **Create an agency**, you do not need to obtain and enter the AK/SK. ICAgent automatically obtains the AK/SK during agency creation. For details, see **How Do I Install ICAgent by Creating an Agency?**	-

Step 4 On the **Install ICAgent** page, click **Copy Command** to copy the ICAgent installation command.

Step 5 Log in as user **root** to the host which is deployed in the region same as that you are logged in to (by using a remote login tool such as PuTTY) and run the copied command. If you have chosen **Obtain AK/SK** as the installation mode, enter the AK/SK as prompted.

- When message **ICAgent install success** is displayed, ICAgent has been installed in the **/opt/oss/servicemgr/** directory of the host.
- If the installation fails, uninstall ICAgent and then install it again.

Step 6 Choose **Host Management** > **Hosts** in the navigation pane of the LTS console and check whether the ICAgent status is **Running**.

----End

Initial Installation (Windows)

Step 1 Click **Install ICAgent** in the upper right corner.

Step 2 Set **Host** to **Intra-region hosts**.

Step 3 Set **OS** to **Windows**.

Step 4 You can download it to the local PC by clicking the name of the package or visiting the download URL.

Step 5 Save the ICAgent installation package to a directory on the target host, for example, **C:\ICAgent**, and decompress the package.

Step 6 Obtain an AK/SK. For details, see **How Do I Obtain an AK/SK Pair?**

Step 7 On the **Install ICAgent** page, click **Copy Command** to copy the ICAgent installation command to the local PC and replace the AK/SK in the command with the obtained one.

Step 8 Open the Command Prompt, go to the directory where the ICAgent installation package is decompressed, and run the copied command.

If the message **Service icagent installed successfully** is displayed, the installation is successful.

- If you have installed a third-party antivirus software, add ICAgent as a trusted program. Otherwise, ICAgent installation may fail.
- To uninstall ICAgent, go to the **\ICProbeAgent\bin\manual\win** directory where the ICAgent installation package was decompressed, and double-click the script named **uninstall.bat**. When the message **icagent removed successfully** is displayed, the uninstallation is successful.

  Uninstalling ICAgent does not delete the files in the corresponding directories. You need to delete them manually if necessary.
- To check the ICAgent status, go to the directory where the ICAgent installation package was decompressed, open the Command Prompt, and run the **sc query icagent** command. If **RUNNING** is returned, ICAgent is running. If the message **The specified service does not exist as an installed service** is displayed, ICAgent has been uninstalled.
- If you reinstall ICAgent after uninstallation and find that the ICAgent status remains pending, end the **icagent.exe** process in **Task Manager** and try installation again.

Step 9 Choose **Host Management** > **Hosts** in the navigation pane of the LTS console and check whether the ICAgent status is **Running**.

----End

Inherited Installation (Linux)

Assume that you need to install ICAgent on multiple hosts, and one of the hosts already has ICAgent installed. The ICAgent installation package, **ICProbeAgent.tar.gz**, is in the **/opt/ICAgent/** directory. To install ICAgent on other hosts one by one:

Step 1 Run the following command on the host where ICAgent has been installed, where *x.x.x.x* is the IP address of the host you want to install ICAgent on.

```
bash /opt/oss/servicemgr/ICAgent/bin/remoteInstall/remote_install.sh -ip x.x.x.x
```

Step 2 Enter the password for user **root** of the host when prompted.

- If the Expect tool is installed on the host that has ICAgent installed, the ICAgent installation should be able to complete without prompting you for a password. Otherwise, enter the password as prompted.
- Ensure that user **root** can run SSH or SCP commands on the host where ICAgent has been installed to remotely communicate with the remote host to install ICAgent.
- When message **ICAgent install success** is displayed, ICAgent has been installed in the **/opt/oss/servicemgr/** directory of the host. You can then choose **Host Management** > **Hosts** in the navigation pane of the LTS console to check the ICAgent status.
- If **ICAgent install success** is not displayed, the installation fails. Uninstall ICAgent and install it again.

----End

Batch Inherited Installation (Linux)

Assume that you need to install ICAgent on multiple hosts, and one of the hosts already has ICAgent installed. The ICAgent installation package, **ICProbeAgent.tar.gz**, is in the **/opt/ICAgent/** directory. In this case, you can follow the directions below to install ICAgent on other hosts in batches.

- The hosts must all belong to the same VPC and be on the same subnet.
- **Python 3.*** is required for batch installation. If you are prompted that Python cannot be found during ICAgent installation, install Python of a proper version on the host and try again.

Prerequisites

The IP addresses and **root**'s passwords of all hosts to install ICAgent have been collected, sorted in the **iplist.cfg** file, and uploaded to the **/opt/ICAgent/** directory on the host that has ICAgent installed. An IP address and the password of a host's user **root** in the **iplist.cfg** file must be separated by a space. Examples:

192.168.0.109 *Password* (Replace the IP address and password with the actual ones)

192.168.0.39 *Password* (Replace the IP address and password with the actual ones)

- The **iplist.cfg** file contains sensitive information. You are advised to clear it after using it.
- If all hosts share a password, list only IP addresses in the **iplist.cfg** file and enter the password manually during execution. If one of the hosts uses a different password, type the password behind its IP address.

Procedure

Step 1 Run the following command on the host that has ICAgent installed:

```
bash /opt/oss/servicemgr/ICAgent/bin/remoteInstall/remote_install.sh -batchModeConfig /opt/ICAgent/iplist.cfg
```

Enter the default password for user **root** of the hosts to install ICAgent. If the passwords of all hosts have been configured in the **iplist.cfg** file, press **Enter** to skip this step.

```
batch install begin
Please input default passwd:
send cmd to 192.168.0.109
send cmd to 192.168.0.39
2 tasks running, please wait...
2 tasks running, please wait...
2 tasks running, please wait...
End of install agent: 192.168.0.39
End of install agent: 192.168.0.109
All hosts install icagent finish.
```

Wait for a while. When message **All hosts install icagent finish.** is displayed, ICAgent has been installed on all the hosts listed in the configuration file.

Step 2 Choose **Host Management** > **Hosts** in the navigation pane of the LTS console to check the **ICAgent status**.

----End

6.2.2 Installing ICAgent (Extra-Region Hosts)

ICAgent is a log collection tool for LTS. To use LTS to collect logs from extra-region hosts, you need to install ICAgent on the hosts. This section describes how to install ICAgent on an extra-region host.

Prerequisites

Before installing ICAgent, ensure that the time and time zone of your local browser are consistent with those of the host. If they are inconsistent, errors may occur during log reporting.

Installation Methods

There are two methods to install ICAgent.

Table 6-5 Installation methods

Method	Scenario
Initial installation	You can use this method to install ICAgent on a host that has no ICAgent installed.
Inherited installation (supported only for Linux hosts)	When ICAgent has already been installed on one host but needs to be installed on multiple hosts, you can use this method.

Initial Installation (Linux)

Before installing ICAgent on a host not in this region, apply for an ECS as a jump server on the ECS console. For details, see **Using Multiple Jump Servers**.

NOTE

You are advised to use **CentOS 6.5 64bit** or later images. The minimum specifications for the ECS are 1 vCPU and 1 GB of memory, while the recommended specifications are 2 vCPUs and 4 GB of memory.

Step 1 Log in to the management console and choose **Management & Deployment** > **Log Tank Service**.

Step 2 Choose **Host Management** > **Hosts** in the navigation pane.

Step 3 Click **Install ICAgent** in the upper right corner.

Step 4 Set **Host** to **Extra-region hosts**.

Step 5 Set **OS** to **Linux**.

Step 6 Set **Network Connectivity** to **Private line**. When the network is connected via a private line, hosts in other IDCs are disconnected from LTS backend by default and a network connectivity solution is required. You are advised to select **VPCEP**.

NOTE

Private line: Extra-region hosts connect to LTS in the current region through a jump server or VPC Endpoint (VPCEP), offering greater security and stability. In this scenario, extra-region hosts cannot communicate with LTS in the current region by default, and ICAgent installed on these hosts cannot directly access the network segment used by LTS in the current region to report logs. Therefore, you need to configure a network connection solution to use a jump server or VPCEP to connect to the LTS backend and forward data to LTS.

- Jump server: functions as a data forwarder and forwards the data collected by ICAgent from extra-region hosts to LTS. This solution is suitable for tests or scenarios with low log traffic. VPCEP is recommended for scenarios with high log traffic.
- VPCEP: provides private channels to connect your VPC to LTS in the current region, enabling resources in the VPC to access VPC endpoint services without the need for EIPs. This solution reduces the risks of data transmission on public networks and improves the transmission security and efficiency.

Step 7 If you set **LTS Backend Connection** to **VPCEP**, enter the VPCEP domain name and go to **Step 9**.

With the assistance of network engineers, configure DNS domain name resolution rules on other clouds to resolve VPCEP domain names to specified IP addresses.

Then, copy the ping command displayed on this page and run it on the target host whose logs are to be collected. A successful ping test indicates that the network configuration is correct.

Step 8 Enable forwarding ports on the jump server. This step is mandatory when **LTS Backend Connection** is set to **Jump server**.

1. Apply for an ECS in the current region as a jump server.
2. Add security group rules for the jump server and enable the corresponding inbound ports to ensure data connectivity between the extra-region hosts and the jump server.
   a. On the ECS console, click the ECS name to access the details page, and click the **Security Groups** tab. The security group list is displayed.
   b. Click a security group name to access the details page.
   c. On the security group details page, click the **Inbound Rules** tab and then click **Add Rule**. On the page displayed, add a security group rule based on **Table 6-6**.

Table 6-6 Security group rule

Direction	Protocol	Port	Description
Inbound	TCP	8149, 8102, 8923, 30200, 30201, and 80	Ports used by ICAgent to send data to the jump server, ensuring data connectivity between VMs in other regions and the jump server.

3. Enter the private IP address of the jump server and generate an SSH tunneling command.

   NOTE

   The private IP address of the jump server refers to the internal IP address of the VPC where the jump server is located.

4. Click **Copy Command**.
5. Log in to the jump server as user **root** and run the SSH tunneling command:
   ssh -f -N -L {*Jump server IP address*}:8149:{*ELB IP address*}:8149 -L {*Jump server IP address*}:8102:{*ELB IP address*}:8102 -L {*Jump server IP address*}:8923:{*ELB IP address*}:8923 -L {*Jump server IP address*}:30200:{*ELB IP address*}:30200 -L {*Jump server IP address*}:30201:{*ELB IP address*}:30201 -L {*Jump server IP address*}:80:icagent-{*Region*}.{*OBS domain name*}:80 {*Jump server IP address*}

   Enter the password of user **root** as prompted.
6. Run the **netstat -lnp | grep ssh** command to check whether the corresponding TCP ports are being listened to. If the command output similar to **Figure 6-1** is returned, the ports are open.

   Figure 6-1 Open TCP ports

   ```
   [root@ecs-3716 nginx]# netstat -lnp | grep ssh
   tcp        0      0 192.168.0.201:80        0.0.0.0:*               LISTEN      1245
   tcp        0      0 192.168.0.201:8149      0.0.0.0:*               LISTEN      1245
   tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      4590
   tcp        0      0 192.168.0.201:30200     0.0.0.0:*               LISTEN      1245
   tcp        0      0 192.168.0.201:30201     0.0.0.0:*               LISTEN      1245
   tcp        0      0 192.168.0.201:8923      0.0.0.0:*               LISTEN      1245
   tcp        0      0 192.168.0.201:8102      0.0.0.0:*               LISTEN      1245
   tcp6       0      0 :::22                   :::*                    LISTEN      4590
   [root@ecs-3716 nginx]#
   ```

   NOTE

   If the jump server powers off and restarts, run the preceding command again.
7. Obtain an AK/SK and specify **DC** and **Connection IP**.

   NOTE

   - **DC**: Specify a name for the data center of the host so it is easier to find the host.
   - **Connection IP**: For EIP connection, use the EIP of the jump server. For VPC peering connection, use the internal IP address of the VPC where the jump server locates.

Step 9 Copy the ICAgent installation command.

Step 10 Log in as user **root** to the host which is deployed in the region same as that you are logged in to (by using a remote login tool such as PuTTY) and run the copied command.

NOTE

- When message **ICAgent install success** is displayed, ICAgent has been installed in the **/opt/oss/servicemgr/** directory of the host. You can then choose **Host Management** > **Hosts** in the navigation pane of the LTS console to check the ICAgent status.
- If the installation fails, uninstall ICAgent and reinstall it. If the reinstallation fails, contact technical support.

----End

Initial Installation (Windows)

Before installing ICAgent on a host not in this region, apply for a Linux ECS as a jump server on the ECS console. For details, see **Using Multiple Jump Servers**.

NOTE

You are advised to use **CentOS 6.5 64bit** or later images. The minimum specifications for the ECS are 1 vCPU and 1 GB of memory, while the recommended specifications are 2 vCPUs and 4 GB of memory.

Step 1 Click **Install ICAgent** in the upper right corner.

Step 2 Set **Host** to **Extra-region hosts**.

Step 3 Set **OS** to **Windows**.

Step 4 Set **Network Connectivity** to **Private line**. When the network is connected via a private line, hosts in other IDCs are disconnected from LTS backend by default and a network connectivity solution is required. You are advised to select **VPCEP**.

NOTE

Private line: Extra-region hosts connect to LTS in the current region through a jump server or VPC Endpoint (VPCEP), offering greater security and stability. In this scenario, extra-region hosts cannot communicate with LTS in the current region by default, and ICAgent installed on these hosts cannot directly access the network segment used by LTS in the current region to report logs. Therefore, you need to configure a network connection solution to use a jump server or VPCEP to connect to the LTS backend and forward data to LTS.

- Jump server: functions as a data forwarder and forwards the data collected by ICAgent from extra-region hosts to LTS. This solution is suitable for tests or scenarios with low log traffic. VPCEP is recommended for scenarios with high log traffic.
- VPCEP: provides private channels to connect your VPC to LTS in the current region, enabling resources in the VPC to access VPC endpoint services without the need for EIPs. This solution reduces the risks of data transmission on public networks and improves the transmission security and efficiency.

Step 5 If you set **LTS Backend Connection** to **VPCEP**, enter the VPCEP domain name and go to **Step 7**.

With the assistance of network engineers, configure DNS domain name resolution rules on other clouds to resolve VPCEP domain names to specified IP addresses.

Then, copy the ping command displayed on this page and run it on the target host whose logs are to be collected. A successful ping test indicates that the network configuration is correct.

Step 6 Enable forwarding ports on the jump server. This step is mandatory when **LTS Backend Connection** is set to **Jump server**.

1. Apply for a Linux ECS in the current region as a jump server.
2. Modify the security group rule used by the jump server.
   a. On the ECS details page, click the **Security Groups** tab.
   b. Click a security group name to access the details page.
   c. On the security group details page, click the **Inbound Rules** tab and then click **Add Rule**. On the page displayed, add a security group rule based on **Table 6-7**.

Table 6-7 Security group rule

Direction	Protocol	Port	Description
Inbound	TCP	8149, 8102, 8923, 30200, 30201, and 80	ICAgent will send data to the jump server through the listed ports.

3. Enter the private IP address of the jump server and generate an SSH tunneling command.

   NOTE

   The private IP address of the jump server refers to the internal IP address of the VPC where the jump server is located.

4. Click **Copy Command**.
5. Log in to the jump server as user **root** and run the SSH tunneling command:

   ssh -f -N -L {*Jump server IP address*}:8149:{*ELB IP address*}:8149 -L {*Jump server IP address*}:8102:{*ELB IP address*}:8102 -L {*Jump server IP address*}:8923:{*ELB IP address*}:8923 -L {*Jump server IP address*}:30200:{*ELB IP address*}:30200 -L {*Jump server IP address*}:30201:{*ELB IP address*}:30201 -L {*Jump server IP address*}:80:icagent-{*Region*}.{*OBS domain name*}:80 {*Jump server IP address*}

   Enter the password of user **root** as prompted.
6. Run the **netstat -lnp | grep ssh** command to check whether the corresponding TCP ports are being listened to. If the command output similar to **Figure 6-2** is returned, the ports are open.

   Figure 6-2 Open TCP ports

   ```
   [root@ecs-3716 nginx]# netstat -lnp | grep ssh
   tcp        0      0 192.168.0.201:80        0.0.0.0:*               LISTEN      1245
   tcp        0      0 192.168.0.201:8149      0.0.0.0:*               LISTEN      1245
   tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      4590
   tcp        0      0 192.168.0.201:30200     0.0.0.0:*               LISTEN      1245
   tcp        0      0 192.168.0.201:30201     0.0.0.0:*               LISTEN      1245
   tcp        0      0 192.168.0.201:8923      0.0.0.0:*               LISTEN      1245
   tcp        0      0 192.168.0.201:8102      0.0.0.0:*               LISTEN      1245
   tcp6       0      0 :::22                   :::*                    LISTEN      4590
   [root@ecs-3716 nginx]#
   ```

   NOTE

   If the jump server powers off and restarts, run the preceding command again.

Step 7 Download the ICAgent installation package to the local PC as prompted.

Step 8 Save the ICAgent installation package to a directory on the Windows host, for example, **C:\ICAgent**, and decompress the package.

Step 9 Obtain an AK/SK.

Step 10 Generate and copy the installation command.

1. Enter the connection IP in the text box and replace the AK/SK to generate the installation command.

NOTE

Connection IP: For EIP connection, use the EIP of the jump server. For VPC peering connection, use the internal IP address of the VPC where the jump server locates.

2. Click **Copy Command** to copy the ICAgent installation command.

Step 11 Open the Command Prompt, go to the directory where the ICAgent installation package is decompressed, and run the copied command.

NOTE

- If the message **Service icagent installed successfully** is displayed, the installation is successful. You can then choose **Host Management** > **Hosts** in the navigation pane of the LTS console to check the ICAgent status.
- If the installation fails, uninstall ICAgent and reinstall it. If the reinstallation fails, contact technical support.

----End

Using Multiple Jump Servers

NOTE

You can use multiple jump servers to prevent the risk of single point of failures and improve access reliability.

Step 1 Create a Linux ECS that as a jump server.

NOTE

Configure the CPU and memory based on the service requirements. The recommended specifications are 2 vCPUs and 4 GB of memory, or above.

Step 2 Log in to the jump server as use **root** and use the internal IP address of the jump server to create an SSH tunnel.

1. On the ECS console, locate the jump server and obtain its private IP address.
2. On the LTS console, choose **Host Management** in the navigation pane, and click **Install ICAgent** in the upper right corner. In the dialog box displayed, select **Linux** for **OS**, select **Extra-region hosts** for **Host**, and enter the private IP address to generate the SSH tunneling command. Log in to the jump server and run the command to create an SSH tunnel.

Step 3 If there are multiple jump servers, repeat **2** and add them to the same VPC. When creating an ECS, select the same VPC for **Network**.

Step 4 Create a load balancer. When creating the load balancer, you should:

1. Select the same VPC as that of the jump servers.
2. Create an EIP for connecting to the jump servers.
3. Apply for the bandwidth based on the service requirements.

Step 5 Add listeners for TCP ports 30200, 30201, 8149, 8923, and 8102.

Step 6 Add all jump servers to the backend server group.

----End

Inherited Installation (Linux)

Assume that you need to install ICAgent on multiple hosts, and one of the hosts already has ICAgent installed. The ICAgent installation package, **ICProbeAgent.tar.gz**, is in the **/opt/ICAgent/** directory. To install ICAgent on other hosts one by one:

1. Run the following command on the host where ICAgent has been installed, where *x.x.x.x* is the IP address of the host you want to install ICAgent on.

   bash /opt/oss/servicemgr/ICAgent/bin/remoteInstall/remote_install.sh -ip x.x.x.x

2. Enter the password for user **root** of the host when prompted.

   NOTE

   - If the Expect tool is installed on the host that has ICAgent installed, the ICAgent installation should be able to complete without prompting you for a password. Otherwise, enter the password as prompted.
   - Ensure that user **root** can run SSH or SCP commands on the host where ICAgent has been installed to remotely communicate with the remote host to install ICAgent.
   - When message **ICAgent install success** is displayed, ICAgent has been installed in the **/opt/oss/servicemgr/** directory of the host. You can then choose **Host Management** > **Hosts** in the navigation pane of the LTS console to check the ICAgent status.
   - If the installation fails, uninstall ICAgent and reinstall it. If the reinstallation fails, contact technical support.

Batch Inherited Installation (Linux)

Assume that you need to install ICAgent on multiple hosts, and one of the hosts already has ICAgent installed. The ICAgent installation package, **ICProbeAgent.tar.gz**, is in the **/opt/ICAgent/** directory. In this case, you can follow the directions below to install ICAgent on other hosts in batches.

NOTICE

- The hosts must all belong to the same VPC and be on the same subnet.

Prerequisites

The IP addresses and passwords of all hosts to install ICAgent have been collected, sorted in the **iplist.cfg** file, and uploaded to the **/opt/ICAgent/** directory on the host that has ICAgent installed. Each IP address and password in the **iplist.cfg** file must be separated by a space. Examples:

192.168.0.109 *Password* (Replace the IP address and password with the actual ones)

192.168.0.39 *Password* (Replace the IP address and password with the actual ones)

NOTE

- The **iplist.cfg** file contains sensitive information. You are advised to clear it after using it.
- If all hosts share a password, list only IP addresses in the **iplist.cfg** file and enter the password manually during execution. If one of the hosts uses a different password, type the password behind its IP address.

Procedure

1. Run the following command on the host that has ICAgent installed:

   bash /opt/oss/servicemgr/ICAgent/bin/remoteInstall/remote_install.sh -batchModeConfig /opt/ICAgent/iplist.cfg

   Enter the default password for user **root** of the hosts to install ICAgent. If the passwords of all hosts have been configured in the **iplist.cfg** file, press **Enter** to skip this step.

   ```
   batch install begin
   Please input default passwd:
   send cmd to 192.168.0.109
   send cmd to 192.168.0.39
   2 tasks running, please wait...
   2 tasks running, please wait...
   2 tasks running, please wait...
   End of install agent: 192.168.0.39
   End of install agent: 192.168.0.109
   All hosts install icagent finish.
   ```

   If the message **All hosts install icagent finish.** is displayed, ICAgent has been installed on all the hosts listed in the configuration file.

2. Choose **Host Management** > **Hosts** in the navigation pane of the LTS console to check the **ICAgent status**.

6.2.3 Managing ICAgent

After ICAgent is installed, you can **upgrade** and **uninstall** it, and **view its status**.

Upgrading ICAgent

To deliver a better collection experience, LTS regularly upgrades ICAgent. When LTS prompts you that a new ICAgent version is available, you can follow the directions here to obtain the latest version.

Linux hosts support ICAgent upgrade on the LTS console.

Step 1 Log in to the management console and choose **Management & Deployment** > **Log Tank Service**.

Step 2 Choose **Host Management** > **Hosts** in the navigation pane.

Step 3 Select **Intra-Region Hosts** or **Extra-Region Hosts**. When the system prompts you that a new ICAgent version is available, select one or more check boxes of hosts where ICAgent is to be upgraded, and click **Upgrade ICAgent**.

Step 4 Click the **CCE Cluster** tab. Search for and select the cluster whose ICAgent is to be upgraded, and click **Upgrade ICAgent**.

- If you create a CCE cluster for the first time, ICAgent will be installed on hosts in the cluster by default, and logs will be reported to AOM. **Output to AOM** is enabled by default. To report logs to LTS, disable **Output to AOM** before

upgrading ICAgent. You are advised to choose **Log Ingestion** > **Cloud Service** > **Cloud Container Engine (CCE)** to collect container data and output it to LTS instead of AOM.

- CCE cluster ID (ClusterID): Each cluster has a fixed ID.
- When ICAgent is upgraded, LTS creates log groups and host groups for your CCE cluster. The name of the log group and host group is **k8s-log-***{ClusterID}*. You can create an ingestion configuration (**Cloud Services** > **Cloud Container Engine (CCE)**) to add logs of the current CCE cluster to the log group.
- If the hosts of a cluster have no ICAgent installed or outdated ICAgent installed, click **Upgrade ICAgent** to install or upgrade ICAgent on all hosts in the cluster.

Step 5 In the displayed dialog box, click **OK**.

The upgrade begins. This process takes about a minute. When the ICAgent status changes from **Upgrading** to **Running**, the ICAgent upgrade has completed.

If the ICAgent is abnormal after the upgrade or if the upgrade fails, log in to the host and run the installation command. ICAgent can be re-installed on top of itself.

----End

Uninstalling ICAgent

If ICAgent is uninstalled from a host, log collection will be affected. Exercise caution when performing this operation.

Uninstalling ICAgent does not delete the installation files. You need to delete them manually if necessary.

You can uninstall ICAgent using either of the following methods:

- Uninstalling ICAgent on the console: applies to the scenario where ICAgent has been successfully installed.
  a. Choose **Host Management** > **Hosts** in the navigation pane.
  b. Select one or more hosts where ICAgent is to be uninstalled and click **Uninstall ICAgent**.
  c. In the displayed dialog box, click **OK**.

     The uninstallation begins. This process takes about a minute.

     After the uninstallation is complete, the ICAgent status of the host will be displayed as **Uninstalled** in the host list.

     To reinstall ICAgent, wait for 5 minutes after it is uninstalled. Otherwise, the ICAgent may be automatically uninstalled again.
- Logging in to the host to uninstall ICAgent: applies to the scenario where ICAgent fails to be installed.
  a. Log in to a host where ICAgent is to be uninstalled as user **root**.
  b. Run the following command:
     ```
     bash /opt/oss/servicemgr/ICAgent/bin/manual/uninstall.sh
     ```
     If the message **ICAgent uninstall success** is displayed, the uninstallation has completed.

- Remotely uninstalling ICAgent: applies to the scenario where the ICAgent has been successfully installed and needs to be remotely uninstalled.

  You can uninstall ICAgent on one host remotely from another host.

  a. Run the following command on the host where ICAgent has been installed. *x.x.x.x* indicates the IP address of the host you want to uninstall ICAgent from.

  ```
  bash /opt/oss/servicemgr/ICAgent/bin/remoteUninstall/remote_uninstall.sh -ip x.x.x.x
  ```

  b. Enter the password for user **root** of the host when prompted.

  - If the Expect tool is installed on the host that has ICAgent installed, the ICAgent uninstallation should be able to complete without prompting you for a password. Otherwise, enter the password as prompted.
  - Ensure that user **root** can run SSH or SCP commands on the host where ICAgent has been installed to communicate with the remote host.
  - If the message **ICAgent uninstall success** is displayed, the uninstallation has completed.

- Batch uninstalling ICAgent: applies to the scenario where the ICAgent has been installed and needs to be uninstalled in batches.

  If ICAgent has been installed on a host and the ICAgent installation package **ICProbeAgent.tar.gz** is in the **/opt/ICAgent/** directory of the host, you can use this method to uninstall ICAgent from multiple hosts at once.

  The hosts must all belong to the same VPC and be on the same subnet.

  Prerequisites

  The IP addresses and passwords of all hosts to uninstall ICAgent have been collected, sorted in the **iplist.cfg** file, and uploaded to the **/opt/ICAgent/** directory on the host that has ICAgent installed. Each IP address and password in the **iplist.cfg** file must be separated by a space. Examples:

  192.168.0.109 *Password* (Replace the IP address and password with the actual ones)

  192.168.0.39 *Password* (Replace the IP address and password with the actual ones)

  – The **iplist.cfg** file contains sensitive information. You are advised to clear it after using it.

  – If all hosts share a password, list only IP addresses in the **iplist.cfg** file and enter the password manually during execution. If one of the hosts uses a different password, type the password behind its IP address.

  a. Run the following command on the host that has ICAgent installed:

  ```
  bash /opt/oss/servicemgr/ICAgent/bin/remoteUninstall/remote_uninstall.sh -batchModeConfig /opt/ICAgent/iplist.cfg
  ```

  Enter the default password for user **root** of the hosts to uninstall ICAgent. If the passwords of all hosts have been configured in the **iplist.cfg** file, press **Enter** to skip this step.

  ```
  batch uninstall begin
  Please input default passwd:
  send cmd to 192.168.0.109
  send cmd to 192.168.0.39
  2 tasks running, please wait...
  ```



```
End of uninstall agent: 192.168.0.109
End of uninstall agent: 192.168.0.39
All hosts uninstall icagent finish.
```

If message **All hosts uninstall icagent finish.** is displayed, the batch uninstallation has completed.

b. Choose **Host Management** > **Hosts** in the navigation pane of the LTS console to check the ICAgent status.

Checking the ICAgent Status

Choose **Host Management** > **Hosts** in the navigation pane to check the ICAgent status of the target host. The following table lists the ICAgent statuses.

Table 6-8 ICAgent statuses

Status	Description
Running	ICAgent is running properly.
Uninstalled	ICAgent is not installed.
Installing	ICAgent is being installed. This process takes about one minute.
Installation failed	ICAgent installation failed.
Upgrading	ICAgent is being upgraded. This process takes about one minute.
Upgrade failed	ICAgent upgrade failed.
Offline	ICAgent is abnormal because the AK/SK is incorrect. Obtain the correct AK/SK and install ICAgent again.
Faulty	ICAgent is faulty. Contact technical support.
Uninstalling	ICAgent is being uninstalled. This process takes about one minute.
Authentication error	Authentication fails because parameters were incorrectly configured during ICAgent installation.

7 Log Search and View

7.1 Overview

Log search and analysis are indispensable to O&M. After configuring log ingestion, you can search and analyze the collected log data on LTS. Its efficient and professional log collection, search, and analysis help you monitor and manage your systems and applications.

Log Structuring

Before searching and analyzing reported logs, you need to configure structuring and indexing for them. Structured data has a unified length and format, which can significantly improve search and analysis efficiency and accuracy.

Log data can be structured or unstructured.

- Structured data refers to the data described using digits or unified data models. It has a fixed length and format, which facilitate storage and analysis.
- Unstructured data has no pre-defined data models and cannot be fit into two-dimensional tables of databases. It is difficult to directly analyze unstructured data.

Log structuring extracts logs with fixed formats or high similarity from log streams and filters out irrelevant logs. .

Log structuring parsing is a process of converting log data from unstructured or semi-structured to structured for better storage, query, and analysis, improving log data readability, searchability, and query efficiency.

Log Search

After structuring the logs, use LTS **search syntax** to set search criteria with higher efficiency. For details, see **Accessing the Log Search Page**.

7.2 Setting Cloud Structuring Parsing

7.2.1 Setting Cloud Structuring Parsing

LTS provides five log structuring modes: regular expressions, JSON, delimiters, Nginx, and structuring templates. You can make your choice flexibly.

- **Regular Expressions**: This mode applies to scenarios where each line in the log text is a raw log event and each log event can be extracted into multiple key-value pairs based on regular expressions. To use this mode to extract fields, you need to enter a log sample and customize a regular expression. Then, LTS extracts the corresponding key-value pairs based on the capture group in the regular expression.
- **JSON**: This mode applies to scenarios where each line in the log text is a raw log event and each log event can be extracted into multiple key-value pairs based on the JSON parsing rule.
- **Delimiter**: This mode applies to scenarios where each line in the log text is a raw log event and each log event can be extracted into multiple key-value pairs based on specified delimiters (such as colons, spaces, or characters).
- **Nginx**: This mode applies to scenarios where each line in the log text is a raw log event, each log event complies with the Nginx format, and the access log format can be defined by the **log_format** command.
- **Structuring Template**: This mode applies to scenarios where the log structure is complex or key-value extraction needs to be customized. You can use a built-in system template or a custom template to extract fields.

After log data is structured, you can use SQL statements to query and analyze it in the same way as you query and analyze data in two-dimensional database tables.

Constraints

- If indexing has not been configured, delimiters for structured fields default to being empty. The maximum size of a field is 20 KB, with any excess data being truncated.
- If indexing has been configured, the default delimiters of structured fields are those listed in **Configuring Log Content Delimiters**. In this case, the maximum size of a field is 500 KB.

Precautions

- Log structuring is performed on a per-log-stream basis.
- Log structuring is recommended when most logs in a log stream share a similar pattern.
- After the structuring configuration is modified, the modification takes effect only for newly written log data, not for historical log data.

Cloud Structuring Parsing

Step 1 Log in to the management console and choose **Management & Deployment** > **Log Tank Service**. The **Log Management** page is displayed by default.

Step 2 Expand the target log group and click the name of the target stream.

Step 3 On the log stream details page, click  in the upper right corner. On the page displayed, click the **Cloud Structuring Parsing** tab to configure log structuring.

- The following system fields cannot be extracted during log structuring: **groupName**, **logStream**, **lineNum**, **content**, **logContent**, **logContentSize**, **collectTime**, **category**, **clusterId**, **clusterName**, **containerName**, **hostIP**, **hostId**, **hostName**, **nameSpace**, **pathFile**, and **podName**.
- **Regular Expressions**: Extract fields using regular expressions.
- **JSON**: Extract key-value pairs from JSON log events.
- **Delimiter**: Extract fields using delimiters (such as commas or spaces).
- **Nginx**: Customize the format of access logs by using the **log_format** command.
- **Structuring Template**: Extract fields using a custom or system template.

Step 4 Modify or delete the configured structuring configuration.

- On the **Cloud Structuring Parsing** tab page, click  to modify the structuring configuration.
- On the **Cloud Structuring Parsing** tab page, click  to delete the structuring configuration.

  Deleted structuring configurations cannot be restored. Exercise caution when performing this operation.

----End

Regular Expressions

If you choose regular expressions, fields are extracted based on your defined regular expressions.

Step 1 Select a typical log event as the sample.

- Click **Select from Existing Logs**, select a log event, and click **OK**. You can select different time ranges to filter logs.

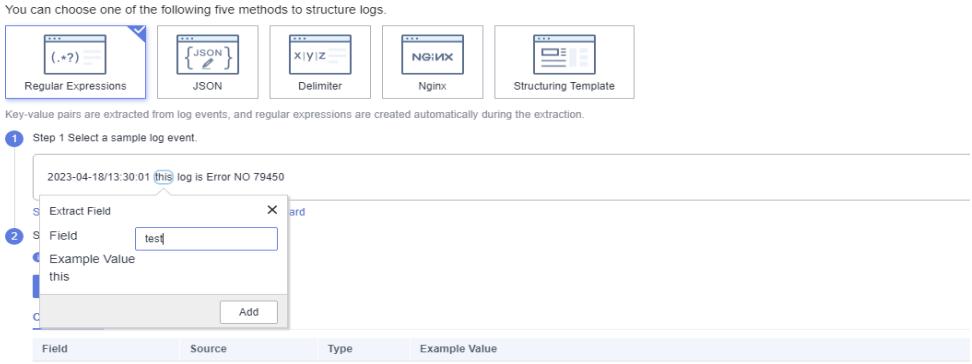
  There are three types of time range: relative time from now, relative time from last, and specified time. Select a time range as required.

  - **From now**: queries log data generated in a time range that ends with the current time, such as the previous 1, 5, or 15 minutes. For example, if the current time is 19:20:31 and **1 hour** is selected as the relative time from now, the charts on the dashboard display the log data that is generated from 18:20:31 to 19:20:31.
  - **From last**: queries log data generated in a time range that ends with the current time, such as the previous 1 or 15 minutes. For example, if the current time is 19:20:31 and **1 hour** is selected as the relative time from last, the charts on the dashboard display the log data that is generated from 18:00:00 to 19:00:00.
  - **Specified**: queries log data that is generated in a specified time range.
- Click **Paste from Clipboard** to paste the copied log content to the sample log box.

Step 2 Extract fields. Extracted fields are shown with their example values. You can extract fields in two ways:

- **Auto generate**: Select the log content you want to extract as a field in the sample log event. In the dialog box displayed, set the field name. The name must start with a letter and contain only letters and digits. Then click **Add**.

  Figure 7-1 Selecting a field

- **Manually enter**: Enter a regular expression in the text box and click **Extract Field**. A regular expression may contain multiple capturing groups, which group strings with parentheses. There are three types of capturing groups:
  - (*exp*): Capturing groups are numbered by counting their opening parentheses from left to right. The numbering starts with 1.
  - (?<*name*>*exp*): named capturing group. It captures text that matches *exp* into the group *name*. The group name must start with a letter and contain only letters and digits. A group is recalled by group name or number.
  - (?:*exp*): non-capturing group. It captures text that matches *exp*, but it is not named or numbered and cannot be recalled.
  - When you select **manually enter**, the regular expression can contain up to 5000 characters. You do not have to name capturing groups when writing the regular expression. When you click **Extract Field**, those unnamed groups will be named as **field1**, **field2**, **field3**, and so on.

Step 3 Specify a field as the log time. For details, see **Setting Custom Log Time**.

Step 4 Click **Save**. The type of extracted fields cannot be changed after the structuring is complete.

----End

JSON

If you choose **JSON**, JSON logs are split into key-value pairs.

Step 1 Select a typical log event as the sample. Click **Select from Existing Logs**, select a log event, or enter a log event in the text box, and click **OK**. You can select different time ranges to filter logs.

Step 2 Extract fields. Extract fields from the log event. Extracted fields are shown with their example values.

Enter the following sample raw log in the text box and click **Intelligent Extraction**.

```
{"a1": "a1", "b1": "b1", "c1": "c1", "d1": "d1"}
```

After fields are extracted, check and edit the fields and save them as a template if needed. For details about rules for configuring extracted fields, see **Setting Structured Fields**.

- The **float** data type has 16 digit precision. If a value contains more than 16 valid digits, the extracted content is incorrect, which affects quick analysis. In this case, you are advised to change the field type to **string**.
- If the data type of the extracted fields is set to **long** and the log content contains more than 16 valid digits, only the first 16 valid digits are displayed, and the subsequent digits are changed to 0.
- If the data type of the extracted fields is set to **long** and the log content contains more than 21 valid digits, the fields are identified as the **float** type. You are advised to change the field type to **string**.

Step 3 Specify a field as the log time. For details, see **Setting Custom Log Time**.

Step 4 Click **Save**. The type of extracted fields cannot be changed after the structuring is complete.

----End

Delimiter

Logs can be parsed by delimiters, such as commas (,), spaces, or other special characters.

Step 1 Select a typical log event as the sample. Click **Select from Existing Logs**, select a log event, or enter a log event in the text box, and click **OK**. You can select different time ranges to filter logs.

There are three types of time range: relative time from now, relative time from last, and specified time. Select a time range as required.

- **From now**: queries log data generated in a time range that ends with the current time, such as the previous 1, 5, or 15 minutes. For example, if the current time is 19:20:31 and **1 hour** is selected as the relative time from now, the charts on the dashboard display the log data that is generated from 18:20:31 to 19:20:31.
- **From last**: queries log data generated in a time range that ends with the current time, such as the previous 1 or 15 minutes. For example, if the current time is 19:20:31 and **1 hour** is selected as the relative time from last, the charts on the dashboard display the log data that is generated from 18:00:00 to 19:00:00.
- **Specified**: queries log data that is generated in a specified time range.

Step 2 Select or customize a delimiter.

- For invisible characters, enter hexadecimal characters starting with 0x. The length ranges from 0 to 4 characters. There are 32 invisible characters in total.
- For custom characters, enter 1 to 10 characters, each as an independent delimiter.

- For a custom string, enter 1 to 30 characters as one whole delimiter.

Step 3 Extract fields. Extract fields from the log event. Extracted fields are shown with their example values.

Enter the following sample raw log in the text box and click **Intelligent Extraction**.

```
1 5f67944957444bd6bb4fe3b367de8f3d 1d515d18-1b36-47dc-a983-bd6512aed4bd 192.168.0.154
192.168.3.25 38929 53 17 1 96 1548752136 1548752736 ACCEPT OK
```

After fields are extracted, check and edit the fields and save them as a template if needed. For details about rules for configuring extracted fields, see **Setting Structured Fields**.

The **float** data type has seven digit precision.

If a value contains more than seven valid digits, the extracted content is incorrect, which affects quick analysis. In this case, you are advised to change the field type to **string**.

Step 4 Specify a field as the log time. For details, see **Setting Custom Log Time**.

Step 5 Click **Save**. The type of extracted fields cannot be changed after the structuring is complete.

----End

Nginx

You can customize the format of access logs by the **log_format** command.

Step 1 Select a typical log event as the sample. Click **Select from Existing Logs**, select a log event, or enter a log event in the text box, and click **OK**. You can select different time ranges to filter logs.

There are three types of time range: relative time from now, relative time from last, and specified time. Select a time range as required.

- **From now**: queries log data generated in a time range that ends with the current time, such as the previous 1, 5, or 15 minutes. For example, if the current time is 19:20:31 and **1 hour** is selected as the relative time from now, the charts on the dashboard display the log data that is generated from 18:20:31 to 19:20:31.
- **From last**: queries log data generated in a time range that ends with the current time, such as the previous 1 or 15 minutes. For example, if the current time is 19:20:31 and **1 hour** is selected as the relative time from last, the charts on the dashboard display the log data that is generated from 18:00:00 to 19:00:00.
- **Specified**: queries log data that is generated in a specified time range.

Step 2 Define the Nginx log format. You can click **Apply Default Nginx Log Format** to apply the default format.

In standard Nginx configuration files, the portion starting with **log_format** indicates the log configuration.

Log format

- Default Nginx log format:

```
log_format  main   '$remote_addr - $remote_user [$time_local] "$request" '
                   '$status $body_bytes_sent "$http_referer" '
                   '"$http_user_agent" "$http_x_forwarded_for"';
```

- You can also customize a format. The format must meet the following requirements:
  - Cannot be blank.
  - Must start with **log_format** and contain apostrophes (') and field names.
  - Can contain up to 5000 characters.
  - Must match the sample log event.
  - Any character except letters, digits, underscores (_), and hyphens (-) can be used to separate fields.
  - Must end with an apostrophe (') or an apostrophe plus a semicolon (';).

Step 3 Extract fields. Extract fields from the log event. Extracted fields are shown with their example values.

Enter the following sample raw logs in the text box.

```
39.149.31.187 - - [12/Mar/2020:12:24:02 +0800] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36" "-"
```

Configure the following Nginx log format in **Step 2**:

```
log_format  main   '$remote_addr - $remote_user [$time_local] "$request" '
                   '$status $body_bytes_sent "$http_referer" '
                   '"$http_user_agent" "$http_x_forwarded_for"';
```

Click **Intelligent Extraction** under **Step 3**.

After fields are extracted, check and edit the fields and save them as a template if needed. For details about rules for configuring extracted fields, see **Setting Structured Fields**.

- The **float** data type has seven digit precision.
- If a value contains more than seven valid digits, the extracted content is incorrect, which affects quick analysis. In this case, you are advised to change the field type to **string**.

Step 4 Specify a field as the log time. For details, see **Setting Custom Log Time**.

Step 5 Click **Save**. The type of extracted fields cannot be changed after the structuring is complete.

----End

Structuring Template

A structuring template extracts fields from either a customized template or a built-in template.

For details, see **Setting a Structuring Template**.

7.2.2 Setting a Structuring Template

LTS supports two types of structuring templates: system and custom templates.

System Templates

You can choose from multiple system templates, but cannot modify the field types in them or delete the fields. For details, see **Table 7-1**.

Step 1 On the **Cloud Structuring Parsing** tab page, select **Structuring Template**.

Step 2 Click **System template** and select a template. A sample log event is displayed for each template.

Step 3 View the log parsing results in the **Template Details** table.

- If you select a system template for structuring, it uses the custom log time.
- Fields of the string type do not support range query using the >, =, or < operators or the "in" syntax. Use asterisks (*) or question marks (?) for fuzzy query. You need to reconfigure the structuring and change the value of this field to a number.

Table 7-1 System template fields

Template Name	Field Name	Field Type Can Be Changed	Field Can Be Deleted
ELB	Defined by ELB.	No	No
VPC	Defined by VPC.	No	No
CTS	Keys in JSON log events.	No	No
APIG	Defined by APIG.	No	No
DCS audit logs	Defined by DCS.	No	No
TOMCAT	Defined by Tomcat.	No	No
NGINX	Defined by Nginx.	No	No
GAUSSV5 audit logs	Defined by GAUSSV5.	No	No
DDS audit logs	Defined by DDS.	No	No
DDS error logs	Defined by DDS.	No	No
DDS slow query logs	Defined by DDS.	No	No
CFW access control logs	Defined by CFW.	No	No
CFW attack logs	Defined by CFW.	No	No
CFW traffic logs	Defined by CFW.	No	No

Template Name	Field Name	Field Type Can Be Changed	Field Can Be Deleted
MySQL error logs	Defined by MySQL.	No	No
MySQL slow query logs	Defined by MySQL.	No	No
POSTGRESQL slow query logs	Defined by PostgreSQL.	No	No
POSTGRESQL error logs	Defined by PostgreSQL.	No	No
SQLServer error logs	Defined by SQL Server.	No	No
GeminiDB Redis slow query logs	Defined by GeminiDB Redis.	No	No
CDN	Defined by CDN.	No	No
SMN	Defined by SMN.	No	No
GAUSSDB_MYSQL error logs	Defined by GaussDB(for MySQL).	No	No
GaussDB_MySQL slow query logs	Defined by GaussDB(for MySQL).	No	No
ER Enterprise Router	Defined by Enterprise Router.	No	No
MySQL audit logs	Defined by MySQL.	No	No
GeminiDB Cassandra slow query logs	Defined by GeminiDB Cassandra.	No	No
GeminiDB Mongo slow query logs	Defined by GeminiDB Mongo.	No	No
GeminiDB Mongo error logs	Defined by GeminiDB Mongo.	No	No
WAF access logs	Defined by WAF.	No	No

Template Name	Field Name	Field Type Can Be Changed	Field Can Be Deleted
WAF attack logs	Defined by WAF.	No	No
DMS rebalancing logs	Defined by DMS.	No	No
CCE audit logs	Defined by CCE.	No	No
CCE event logs	Defined by CCE.	No	No
CCE NGINX-INGRESS logs	Defined by CCE.	No	No -
GeminiDB Redis audit logs	Defined by GeminiDB Redis.	No	No
Influx slow query logs	Defined by Influx.	No	No
Microgateway	Defined by Microgateway.	No	No
GeminiDB Mongo audit logs	Defined by GeminiDB Mongo.	No	No

Step 4 Click **Save**.

----End

Custom Templates

Click **Custom template** and select a template. Custom templates can be obtained in the following ways:

- When you extract fields using methods of regular expression, JSON, delimiter, or Nginx, click **Save as Template** in the lower left corner. In the displayed dialog box, enter a template name and click **OK**. The template will be displayed in the custom template list.
- Create a custom template under the **Structuring Template** option.
  a. Click **Custom template** and **Create Template**.
  b. On the displayed page, select **Regular Expressions**, **JSON**, **Delimiter**, or **Nginx**.
  c. After configuration, enter a template name and click **Save**. The template will be displayed in the custom template list.

7.2.3 Setting Structured and Tag Fields

Setting Structured Fields

You can set extracted fields after cloud structuring. For details, see **Table 7-2**.

Table 7-2 Rules for configuring structured fields

Structuring Method	Field Name	Field Type Can Be Changed	Field Can Be Deleted
Regular expressions (auto generate)	User-defined. The name must start with a letter and contain only letters and digits.	Yes	Yes
Regular expressions (manually enter)	• User-defined. • Default names such as **field1**, **field2**, and **field3** will be used.	Yes	Yes
JSON	Names are set automatically, but you can set aliases for fields.	Yes	Yes
Delimiter	Default names such as **field1**, **field2**, **field3** are used. You can modify these names.	Yes	Yes
Nginx	Names are set based on Nginx configuration, but you can set aliases for fields.	Yes	Yes
Custom templates	User-defined.	Yes	Yes

When you use regular expressions (manually entered), JSON, delimiters, Nginx, or custom templates to structure logs, field names:

Can contain 1 to 64 characters. Use only letters, digits, hyphens (-), underscores (_), and periods (.). Do not use underscores before another underscore or a period. Do not start or end with a period.

Setting Tag Fields

When configuring log structuring, you can set the tag fields for the log information.

Step 1 In **Step 2 Extract fields**, click the **Tag Fields** tab and **Add Field**.

Step 2 In the **Field** column, enter a name for the tag field, for example, **hostIP**.

If you configure tag fields for a structuring rule that was created before the function of tag fields was brought online, no example values will be shown with the tag fields.

Step 3 To add more fields, click **Add Field**.

Step 4 Click **Save**.

- Tag fields can be the following system fields: **category**, **clusterId**, **clusterName**, **containerName**, **hostIP**, **hostId**, **hostName**, **nameSpace**, **pathFile**, and **podName**.
- Tag fields cannot be the following system fields: **groupName**, **logStream**, **lineNum**, **content**, **logContent**, **logContentSize**, and **collectTime**.
- You can configure both field extraction and tag fields during log structuring.

----End

7.2.4 Setting Custom Log Time

When configuring log ingestion, you can enable **Custom Log Time** to set a time field in the logs as the ingestion configuration time.

Enabling Custom Log Time

Step 1 Log in to the management console and choose **Management & Deployment** > **Log Tank Service**. The **Log Management** page is displayed by default.

Step 2 Expand the target log group and click the name of the target stream.

Step 3 On the log stream details page, click  in the upper right corner. On the page displayed, click the **Cloud Structuring Parsing** tab. For details, see **Setting Cloud Structuring Parsing**.

Step 4 After cloud structuring parsing is configured, enable **Custom Log Time** and specify the following parameters.

A time deviation may occur around the time displayed on the log search page when you enable or disable **Custom Log Time**. Do not frequently enable or disable it.

Table 7-3 Parameter configuration

Parameter	Description	Example
Key	Name of an extracted field. You can select an extracted field from the drop-down list. The field is of the **string** or **long** type.	test
Value	For an extracted field, after you select a key, its value is automatically filled in. **NOTE** The value of the field must be within 24 hours earlier or later than the current time.	2022-07-19 12:12:00

Parameter	Description	Example
Format	For details, see **Common Log Time Formats**.	yyyy-MM-dd HH:mm:ss
Operation	Click **Verify**. If the message **The time format is successfully matched with the time field value.** is displayed, the verification is successful.	-

----End

Common Log Time Formats

Table 7-4 lists common log time formats.

By default, log timestamps in LTS are accurate to seconds. You do not need to configure information such as milliseconds and microseconds.

Table 7-4 Time formats

Format	Description	Example
EEE	Abbreviation for Week.	Fri
EEEE	Full name for Week.	Friday
MMM	Abbreviation for Month.	Jan
MMMM	Full name for Month.	January
dd	Number of the day in a month, ranging from 01 to 31 (decimal).	07, 31
HH	Hour, in 24-hour format.	22
hh	Hour, in 12-hour format.	11
MM	Number of the month, ranging from 01 to 12 (decimal).	08
mm	Number of the minute, ranging from 00 to 59 (decimal).	59
a	AM or PM	AM, PM
hh:mm:ss a	Time in the 12-hour format.	11:59:59 AM
HH:mm	Hour and minute format.	23:59
ss	Number of the second, ranging from 00 to 59 (decimal).	59
yy	Year without century, ranging from 00 to 99 (decimal).	04, 98

Format	Description	Example
yyyy	Year (decimal).	2004, 1998
d	Number of the day in a month, ranging from 1 to 31 (decimal).	7, 31
DDD	Number of the day in a year, ranging from 001 to 366 (decimal).	365
u	Number of the day in a week, ranging from 1 to 7 (decimal). The value 1 indicates Monday.	2
w	Number of the week in a year. Sunday is the start of a week. The value ranges from 00 to 53.	23
W	Number of the week in a month, ranging from 0 to 5.	2
U	Number of the day in a week, ranging from 0 to 6 (decimal). The value 0 indicates Sunday.	5
EEE MMM dd HH:mm:ss yyyy	Standard date and time.	Tue Nov 20 14:12:58 2020
EEE MMM dd yyyy	Standard date without time.	Tue Nov 20 2020
HH:mm:ss	Standard time without date.	11:59:59
%s	UNIX Timestamp.	147618725

Examples

Table 7-5 lists common time standards, examples, and expressions.

Table 7-5 Examples

Example	Time Expression	Time Standard
2022-07-14T19:57:36+08:00	yyyy-MM-dd'T'HH:mm:ssXXX	Custom
1548752136	%s	Custom
27/Jan/2022:15:56:44	dd/MMM/yyyy:HH:mm:ss	Custom
2022-08-15 17:53:23+08	yyyy-MM-dd HH:mm:ssX	Custom
2022-08-05T08:24:15.536+0000	yyyy-MM-dd'T'HH:mm:ss.SSSZ	Custom

Example	Time Expression	Time Standard
2022-08-20T10:04:03.204000Z	yyyy-MM-dd'T'HH:mm:ss.SSSZ	Custom
2022-08-22T06:52:08Z	yyyy-MM-dd'T'HH:mm:ssZ	Custom
2022-07-24T10:06:41.000	yyyy-MM-dd'T'HH:mm:ss.SSS	Custom
Monday, 02-Jan-06 15:04:05 MST	EEEE, dd-MMM-yy HH:mm:ss Z	RFC850
Mon, 02 Jan 2006 15:04:05 MST	EEE, dd MMM yyyy HH:mm:ss Z	RFC1123
02 Jan 06 15:04 MST	dd MMM yy HH:mm Z	RFC822
02 Jan 06 15:04 -0700	dd MMM yy HH:mm Z	RFC822Z
2023-01-02T15:04:05Z07:00	yyyy-MM-dd'T'HH:mm:ssZ	RFC3339
2022-12-11 15:05:07	yyyy-MM-dd HH:mm:ss	Custom

7.3 Setting Indexes

An index is a storage structure used to query and analyze logs. Different index settings will generate different query and analysis results. Configure the index settings as required.

Index Types

LTS supports full-text and field indexes. For details, see **Table 7-6**.

Table 7-6 Index types

Index Type	Description
Index Whole Text	LTS splits all field values of an entire log into multiple words when this function is enabled. • The custom label field uploaded by the user is not included in the full-text index. If you want to search for the custom label field, add the corresponding index field. • System reserved fields are not included in full-text indexes. You need to use index fields (Key:Value) to search for them. For details, see **System Reserved Fields**.

Index Type	Description
Index Fields	Query logs by specified field names and values (Key:Value). • LTS creates index fields for certain system reserved fields by default. For details, see **System Reserved Fields**. • If an index field is configured for a field, the delimiter of the field value is subject to the index field configuration. • The quick analysis column in structuring settings has been removed. To use quick analysis, configure index fields and enable quick analysis for the required fields. • In the example log, the **level** and **status** index fields are configured. For the **level** field, it is of the **string** type, its value is **error**, and delimiters are configured. For the **status** field, it is of the **long** type, and no delimiter needs to be configured. You can use **level:error** to search for all logs whose **level** value is **error**. • In the example log, LTS creates indexes for system reserved fields such as **hostName**, **hostIP**, and **pathFile** by default.

The following is a typical example log. The value of the **content** field is the original log content. Use commas (,) to parse the original log content into three fields: **level**, **status**, and **message**.

In the example log, **hostName**, **hostIP**, and **pathFile** are common system reserved fields. For details about the system fields, see **System Reserved Fields**.

```
{
"hostName":"epstest-xx518",
"hostIP":"192.168.0.31",
"pathFile":"stdout.log",
"content":"error,400,I Know XX",
"level":"error",
"status":400,
"message":"I Know XX"
}
```

Precautions

- Either whole text indexing or index fields must be configured.
- After the index function is disabled, the storage space of historical indexes is automatically cleared after the data storage period of the current log stream expires.
- LTS creates index fields for certain system reserved fields by default. For details, see **System Reserved Fields**.
- Different index settings will generate different query and analysis results. Configure the index settings as required. Full-text indexes and index fields do not affect each other.
- After the index configuration is modified, the modification takes effect only for newly written log data.

Configuring Full-Text Indexing

Step 1 Log in to the management console and choose **Management & Deployment** > **Log Tank Service**. The **Log Management** page is displayed by default.

Step 2 Expand the target log group and click the name of the target stream.

Step 3 Click  next to **Quick Analysis** to go to the **Index Settings** tab page.

Step 4 Set index parameters by referring to **Table 7-7**. **Index Whole Text** is enabled by default.

Table 7-7 Custom full-text indexing parameters

Parameter	Description
Index Whole Text	If **Index Whole Text** is enabled, a full-text index is created.
Case-Sensitive	Indicates whether letters are case-sensitive during query. • If this function is enabled, the query result is case-sensitive. For example, if the example log contains **Know**, you can query the log only with **Know**. • If this function is disabled, the query result is case-insensitive. For example, if the example log contains **Know**, you can also query the log with **KNOW** or **know**.

Parameter	Description
Include Chinese	Indicates whether to distinguish between Chinese and English during query. ● After the function is enabled, if the log contains Chinese characters, the Chinese content is split based on unigram segmentation and the English content is split based on delimiters. – Unigram segmentation is to split a Chinese string into Chinese characters. – The advantage of unigram segmentation is efficient word segmentation of massive logs, and other Chinese segmentation methods have great impact on the write speed. – If **Include Chinese** is enabled, unigram segmentation is used for Chinese characters (each Chinese character is segmented separately). To obtain more accurate search results, use phrases with the syntax #"*phrase to be searched for*". ● After this function is disabled, all content is split based on delimiters. For example, assume that the log content is: **error,400,I Know TodayIsMonday**. ● After this function is disabled, the English content is split based on delimiters. The log is split into **error**, **400**, **I**, **Know**, and **TodayIsMonday**. You can search for the log by **error** or **TodayIsMonday**. ● After this function is enabled, the background analyzer of LTS splits the log into **error**, **400**, **I**, **Know**, **Today**, **Is**, and **Monday**. You can search for the log by **error** or **Today**.

Parameter	Description
Delimiters	Splits the log content into multiple words based on the specified delimiters. If the default settings cannot meet your requirements, you can customize delimiters. If you leave **Delimiters** blank, the field value is regarded as a whole. You can search for logs only through a complete string or by fuzzy match. Click **Preview** the see the effect. For example, assume that the log content is: **error,400,I Know TodayIsMonday**. • If no delimiter is set, the entire log is regarded as a string **error,400,I Know TodayIsMonday**. You can search for the log only by the complete string **error,400,I Know TodayIsMonday** or by fuzzy match **error,400,I K***. • If the delimiter is set to a comma (,), the raw log is split into: **error**, **400**, and **I Know TodayIsMonday**. You can search for the log by fuzzy or exact match, for example, **error**, **400**, **I Kn***, and **TodayIs***. • If the delimiters are set to a comma (,) and space, the raw log is split into: **error**, **400**, **I**, **Know**, **TodayIsMonday**. You can search for the log by fuzzy or exact match, for example, **Know**, and **TodayIs***.
ASCII Delimiters	Click **Add ASCII Delimiter** and enter the ASCII value by referring to **ASCII Table**.

Step 5 Click **OK**.

----End

Configuring Index Fields

When creating a field index, you can add a maximum of 500 fields. A maximum of 100 subfields can be added for JSON fields.

Step 1 Specify the number of samples for quick analysis. The value ranges from 100,000 (default) to 10 million. Quick analysis provides a fast overview by sampling field value statistics rather than analyzing all log data. The more logs sampled, the slower the analysis.

Step 2 Click **Add Field** under **Index Fields** to configure field indexing. For details, see **Table 7-8**.

- The indexing parameters take effect only for the current field.
- Index fields that do not exist in log content are invalid.
- For details about the system fields, see **System Reserved Fields**.
- Automatically configuring field indexes: Click **Auto Configure**. LTS generates field indexes based on the first log event in the preview or common system reserved fields (such as **hostIP**, **hostName**, and **pathFile**). You can add or delete fields as required.

- Configuring field indexes in batches: Select fields and click **Batch Configure**.
- For automatic configuration, LTS obtains the intersection of the raw logs and system fields in the last 15 minutes by default, and combines the intersection with current structured fields and tag fields to form the table data below **Index Fields**.
- If no raw log is generated in the last 15 minutes, LTS obtains **hostIP**, **hostName**, **pathFile**, structured fields, and tag fields to form the table data.
- When structuring is configured for ECS ingestion, the **category**, **hostName**, **hostId**, **hostIP**, **hostIPv6** and **pathFile** fields are automatically added to **Index Fields** on the **Index Settings** page. A field will not be added if the same one already exists.
- When structuring is configured for CCE ingestion, the **category**, **clusterId**, **clusterName**, **nameSpace**, **podName**, **containerName**, **appName**, **hostName**, **hostId**, **hostIP**, **hostIPv6** and **pathFile** fields are automatically added to **Index Fields** on the **Index Settings** page. A field will not be added if the same one already exists.

Table 7-8 Custom index field parameters

Parameter	Description
Field	Log field name, such as **level** in the example log. • A field name can contain only letters, digits, hyphens (-), underscores (_), and periods (.). Do not use an underscore before another underscore or a period. Do not start or end with a period. • Double underscores (__) are used in built-in reserved fields that are not displayed to users in LTS. Avoid using them in custom log field names, as this will prevent the configuration of field index names. • LTS creates index fields for certain system reserved fields by default. For details, see **System Reserved Fields**. • For system fields, **system** is displayed next to their names.
Action	Displays the field status, such as **New**, **Retain**, **Modify**, and **Delete**. After the index field is changed, click **Compare** to view the differences between the original and modified configurations. • New fields cannot be modified. • When you modify the settings of **Type**, **Case-Sensitive**, **Common Delimiters**, **ASCII Delimiters**, **Include Chinese**, or **Quick Analysis**, the system compares the modified settings with the original settings and changes the action to modified. • After you click **OK**, the fields whose action is deleted are not saved.

Parameter	Description
Type	• Data type of the log field value. The options are **string**, **long**, and **float**. • Fields of long and float types do not support **Case-Sensitivity**, **Include Chinese**, and **Delimiters**.
Case-Sensitive	Indicates whether letters are case-sensitive during query. • If this function is enabled, the query result is case-sensitive. For example, if the **message** field in the example log contains **Know**, you can query the log only with **message:Know**. • If this function is disabled, the query result is case-insensitive. For example, if the **message** field in the example log contains **Know**, you can also query the log with **message:KNOW** or **message:know**.
Common Delimiters	Splits the log content into multiple words based on the specified delimiters. If the default settings cannot meet your requirements, you can customize delimiters. If you leave **Delimiters** blank, the field value is regarded as a whole. You can search for logs only through a complete string or by fuzzy match. For example, the content of the **message** field in the example log is **I Know TodayIsMonday**. • If no delimiter is set, the entire log is regarded as a string **I Know TodayIsMonday**. You can search for the log only by the complete string **message:I Know TodayIsMonday** or by fuzzy search **message:I Know TodayIs***. • If the delimiter is set to a space, the raw log is split into: **I**, **Know**, and **TodayIsMonday**. You can find the log by fuzzy search or exact words, for example, **message:Know**, or **message: TodayIsMonday**.
ASCII Delimiters	Click **Add ASCII Delimiter** and enter the ASCII value by referring to **ASCII Table**.

Parameter	Description
Include Chinese	Indicates whether to distinguish between Chinese and English during query. • After the function is enabled, if the log contains Chinese characters, the Chinese content is split based on unigram segmentation and the English content is split based on delimiters. – Unigram segmentation is to split a Chinese string into Chinese characters. – The advantage of unigram segmentation is efficient word segmentation of massive logs, and other Chinese segmentation methods have great impact on the write speed. – If **Include Chinese** is enabled, unigram segmentation is used for Chinese characters (each Chinese character is segmented separately). To obtain more accurate search results, use phrases with the syntax #"*phrase to be searched for*". • After this function is disabled, all content is split based on delimiters. For example, the content of the **message** field in the example log is **I Know TodayIsMonday**. • After this function is disabled, the English content is split based on delimiters. The log is split into **I**, **Know**, and **TodayIsMonday**. You can search for the log by **message:Know** or **message:TodayIsMonday**. • After this function is enabled, the background analyzer of LTS splits the log into **I**, **Know**, **Today**, **Is**, and **Monday**. You can search for the log by **message:Know** or **message:Today**.
Quick Analysis	By default, this option is enabled, indicating that this field will be sampled and collected. For details, see **Creating an LTS Quick Analysis Task**. • The principle of quick analysis is to collect statistics on 100,000 logs that match the search criteria, not all logs. • The maximum length of a field for quick analysis is 2,000 bytes. • The quick analysis field area displays the first 100 records.
Operation	Click  to delete the target field.

Step 3 Click **OK**.

----End

System Reserved Fields

During log collection, LTS adds information such as the collection time, log type, and host IP address to logs in the form of Key-Value pairs. These fields are system reserved fields.

- When using APIs to write log data or add ICAgent configurations, avoid using the same field names as reserved field names to prevent issues such as duplicate field names and incorrect queries.
- A custom log field must not contain double underscores (__) in its name. If it does, indexing cannot be configured for the field.

Table 7-9 System reserved field description

Field	Data Format	Index and Statistics Settings	Description
collectTime	Integer, Unix timestamp (ms)	Index setting: After indexing is enabled, a field index is created for **collectTime** by default. The index data type is long. Enter **collectTime :** *xxx* during the query.	Indicates the time when logs are collected by ICAgent. Example: **"collectTime":"1681896081334"** indicates 2023-04-19 17:21:21 when converted into standard time.
__time__	Integer, Unix timestamp (ms)	Index setting: After indexing is enabled, a field index is created for **time** by default. The index data type is long. This field cannot be queried.	Log time refers to the time when a log is displayed on the console. Example: **"__time__":"1681896081334"** indicates 2023-04-19 17:21:21 when converted into standard time. By default, the collection time is used as the log time. You can also customize the log time.

Field	Data Format	Index and Statistics Settings	Description
lineNum	Integer	Index setting: After indexing is enabled, a field index is created for **lineNum** by default. The index data type is long.	Line number (offset), which is used to sort logs. Non-high-precision logs are generated based on the value of **collectTime**. The default value is **collectTime * 1000000 + 1**. For high-precision logs, the value is the nanosecond value reported by users. Example: **"lineNum":"1681896081333991900"**
category	String	Index setting: After indexing is enabled, a field index is created for **category** by default. The index data type is string, and the delimiters are empty. Enter **category:** *xxx* during the query.	Log type, indicating the source of the log. Example: The field value of logs collected by ICAgent is **LTS**, and that of logs reported by a cloud service such as DCS is **DCS**.
clusterName	String	Index setting: After indexing is enabled, a field index is created for **clusterName** by default. The index data type is string, and the delimiters are empty. Enter **clusterName:** *xxx* during the query.	Cluster name, used in the Kubernetes scenario. Example: **"clusterName":"eps test"**

Field	Data Format	Index and Statistics Settings	Description
clusterId	String	Index setting: After indexing is enabled, a field index is created for **clusterId** by default. The index data type is string, and the delimiters are empty. Enter **clusterId:** *xxx* during the query.	Cluster ID, used in the Kubernetes scenario. Example: **"clusterId":"c7f3f4a5-xxxx-11ed-a4ec-0255ac100b07"**
nameSpace	String	Index setting: After indexing is enabled, a field index is created for **nameSpace** by default. The index data type is string, and the delimiters are empty. Enter **nameSpace:** *xxx* during the query.	Namespace used in the Kubernetes scenario. Example: **"nameSpace":"monitoring"**
appName	String	Index setting: After indexing is enabled, a field index is created for **appName** by default. The index data type is string, and the delimiters are empty. Enter **appName:** *xxx* during the query.	Component name, that is, the workload name in the Kubernetes scenario. Example: **"appName":"alertmanager-alertmanager"**
serviceID	String	Index setting: After indexing is enabled, a field index is created for **serviceID** by default. The index data type is string, and the delimiters are empty. Enter **serviceID:** *xxx* during the query.	Workload ID in the Kubernetes scenario. Example: **"serviceID":"cf5b453xxxad61d4c483b50da3fad5ad"**

Field	Data Format	Index and Statistics Settings	Description
podName	String	Index setting: After indexing is enabled, a field index is created for **podName** by default. The index data type is string, and the delimiters are empty. Enter **podName:** *xxx* during the query.	Pod name in the Kubernetes scenario. Example: **"podName":"alertmanager-alertmanager-0"**
podIp	String	Index setting: After indexing is enabled, a field index is created for **podIp** by default. The index data type is string, and the delimiters are empty. Enter **podIp:** *xxx* during the query.	Pod IP address in the Kubernetes scenario. Example: **"podIp":"10.0.0.145"**
containerName	String	Index setting: After indexing is enabled, a field index is created for **containerName** by default. The index data type is string, and the delimiters are empty. Enter **containerName:** *xxx* during the query.	Container name used in the Kubernetes scenario. Example: **"containerName":"config-reloader"**
hostName	String	Index setting: After this function is enabled, a field index is created for **hostName** by default. The index data type is string, and the delimiters are empty. Enter hostName: xxx during the query.	Indicates the host name where ICAgent resides. Such as "hostName":"epstest-xx518" in the example.

Field	Data Format	Index and Statistics Settings	Description
hostId	String	Index setting: After this function is enabled, a field index is created for **hostId** by default. The index data type is string, and the delimiters are empty. Enter hostId: xxx during the query.	Indicates the host ID where ICAgent resides. The ID is generated by ICAgent. Such as "hostId":"318c02fe-xxxx-4c91-b5bb-6923513b6c34" in the example.
hostIP	String	Index setting: After this function is enabled, a field index is created for **hostIP** by default. The index data type is string, and the delimiters are empty. Enter hostIP: xxx during the query.	Host IP address where the log collector resides (applicable to IPv4 scenario) Such as "hostIP":"192.168.0.31" in the example.
hostIPv6	String	Index setting: After this function is enabled, a field index is created for **hostIPv6** by default. The index data type is string, and the delimiters are empty. Enter hostIPv6: xxx during the query.	Host IP address where the log collector resides (applicable to IPv6 scenario) Such as "hostIPv6":"" in the example.
pathFile	String	Index setting: After this function is enabled, a field index is created for **pathFile** by default. The index data type is string, and the delimiters are empty. Enter pathFile: xxx during the query.	File path is the path of the collected log file. Such as "pathFile":"stdout.log" in the example.

Field	Data Format	Index and Statistics Settings	Description
content	String	Index setting: After **Index Whole Text** is enabled, the delimiters defined in **Index Whole Text** are used to delimit the value of the **content** field. The **content** field cannot be configured in the field index.	Original log content. Example: **"content":"level=error ts=2023-04-19T09:21:21.333895559Z"**
__receive_time__	Integer, Unix timestamp (ms)	Index setting: After this function is enabled, a field index is created for **__receive_time__** by default. The index data type is long.	Time when a log is reported to the server, which is same as the time when the LTS collector receives the log.
_content_parse_fail_	String	Index setting: After indexing is enabled, a field index is created for **_content_parse_fail_** by default. The index data type is string, and the default delimiter is used. Enter **_content_parse_fail_: xxx** during the query.	Content of the log that fails to be parsed.
__time	Integer, Unix timestamp (ms)	The **__time field** cannot be configured in the field index.	N/A
logContent	String	The **logContent** field cannot be configured in the field index.	N/A
logContentSize	Integer	The **logContentSize** field cannot be configured in the field index.	N/A
logIndexSize	Integer	The **logIndexSize** field cannot be configured in the field index.	N/A

Field	Data Format	Index and Statistics Settings	Description
groupName	String	The **groupName** field cannot be configured in the field index.	N/A
logStream	String	The **logStream** field cannot be configured in the field index.	N/A

ASCII Table

Table 7-10 ASCII table

ASCII Value	Character	ASCII Value	Character	ASCII Value	Character	ASCII Value	Character
0	NUL (Null)	32	Space	64	@	96	`
1	SOH (Start of heading)	33	!	65	A	97	a
2	STX (Start of text)	34	"	66	B	98	b
3	ETX (End of text)	35	#	67	C	99	c
4	EOT (End of transmission)	36	$	68	D	100	d
5	ENQ (Enquiry)	37	%	69	E	101	e
6	ACK (Acknowledge)	38	&	70	F	102	f
7	BEL (Bell)	39	'	71	G	103	g
8	BS (Backspace)	40	(	72	H	104	h
9	HT (Horizontal tab)	41	)	73	I	105	i
10	LF (Line feed)	42	*	74	J	106	j

ASCII Value	Character	ASCII Value	Character	ASCII Value	Character	ASCII Value	Character
11	VT (Vertical tab)	43	+	75	K	107	k
12	FF (Form feed)	44	,	76	L	108	l
13	CR (Carriage return)	45	-	77	M	109	m
14	SO (Shift out)	46	.	78	N	110	n
15	SI (Shift in)	47	/	79	O	111	o
16	DLE (Data link escape)	48	0	80	P	112	p
17	DC1 (Device control 1)	49	1	81	Q	113	q
18	DC2 (Device control 2)	50	2	82	R	114	r
19	DC3 (Device control 3)	51	3	83	S	115	s
20	DC4 (Device control 4)	52	4	84	T	116	t
21	NAK (Negative acknowledge)	53	5	85	U	117	u
22	SYN (Synchronous idle)	54	6	86	V	118	v
23	ETB (End of transmission block)	55	7	87	W	119	w
24	CAN (Cancel)	56	8	88	X	120	x
25	EM (End of medium)	57	9	89	Y	121	y
26	SUB (Substitute)	58	:	90	Z	122	z
27	ESC (Escape)	59	;	91	[	123	{
28	FS (File separator)	60	<	92	\	124	|

ASCII Value	Character	ASCII Value	Character	ASCII Value	Character	ASCII Value	Character
29	GS (Group separator)	61	=	93	]	125	}
30	RS (Record separator)	62	>	94	^	126	~
31	US (Unit separator)	63	?	95	_	127	DEL (Delete)

7.4 Searching Logs

7.4.1 Accessing the Log Search Page

After configuring log structuring parsing and indexing, you can enter statements to search for log records that contain specific keywords. You can also search for log data by time range to locate events and issues that occur in a specified period.

Search statements are used to define the filter criteria for log query and obtain the logs that meet the criteria. A search statement may be a keyword, a value, a value range, a space, an asterisk (*), or the like. If it is a space or asterisk (*), no filtering criteria is specified. For more information, see **Using LTS Search Syntax**.

Searching Logs

Step 1 Log in to the management console and choose **Management & Deployment** > **Log Tank Service**. The **Log Management** page is displayed by default.

Step 2 Click the target log group or stream. The log stream details page is displayed.

Step 3 Select a time range from the drop-down list to view log data accordingly.

There are three types of time range: relative time from now, relative time from last, and specified time. Select a time range as required.

- **From now**: queries log data generated in a time range that ends with the current time, such as the previous 1, 5, or 15 minutes. For example, if the current time is 19:20:31 and **1 hour** is selected as the relative time from now, the charts on the dashboard display the log data that is generated from 18:20:31 to 19:20:31.
- **From last**: queries log data generated in a time range that ends with the current time, such as the previous 1 or 15 minutes. For example, if the current time is 19:20:31 and **1 hour** is selected as the relative time from last, the charts on the dashboard display the log data that is generated from 18:00:00 to 19:00:00.
- **Specified**: queries log data that is generated in a specified time range.

Step 4 Enter search criteria in the search box based on **Using LTS Search Syntax** to view, search for, and filter log data.

1. In the search area, click the search box, enter a keyword or select a field or keyword from the drop-down list, and click **Search**.
   - The structured fields are displayed in **key:value** format.
2. In the search area, press the up and down arrows on the keyboard to select a keyword or search syntax from the drop-down list, press **Tab** or **Enter** to select a keyword or syntax, and click **Search**.
3. Click a field for which quick analysis has been enabled to add it to the search box. For details about how to enable quick analysis, see **Creating an LTS Quick Analysis Task**.

   If the field you click already exists in the search box, it will be replaced by this newly added one. If the field is added for the first time, fields in the search box are searched using the AND operator.

Step 5 On the **Log Search** tab page, perform the following operations. For more operations, see **Common Log Search Operations**.

1. Under **Log Statistics**, view the bar chart showing the log quantity in different time segments. The scale of the log quantity is displayed on the left.
2. In the log content area, hover the cursor over a field and click the log content in blue. You can search for logs by copying, adding to query, and excluding from query.
3. In the log content area, you can select a list or raw log to display its log content.

Step 6 Set the layout of log data, including whether to display fields or display fields in a simple view.

1. Select **Edit layouts** from the drop-down list to access the layout setting page. The list also contains options such as the default layout, pure layout, and default container log layout, for you to set whether to display fields.
   - **Cloud**: This mode is applicable to users who have the write permission. Layout information is stored on the cloud.
   - **Local Cache**: This mode is applicable to users who have only the read permission. Layout information is cached in the local browser.
2. Click  to add a custom layout and set the layout name and visibility of layout fields.
3. After the setting is complete, click **OK**. The new custom layout is displayed in the drop-down list.

----End

Common Log Search Operations

In the log content display area, you can share and download logs, and view context. For details, see **Table 7-11**.

Table 7-11 Common operations

Operation	Description
Interactive search	Click **Interactive Mode** in front of the search box. In the displayed **Interactive Search** dialog box, select fields for index configuration, set the filtering mode, and add associations and groups. After the setting is complete, you can preview the search syntax.
Creating quick search	Click  to create a quick search.
Sharing logs	Click  to copy the link of the current log search page to share the logs that you have searched.
Refreshing logs	You can click  to refresh logs in two modes: manual refresh and automatic refresh. • Manual refresh: Select **Refresh Now** from the drop-down list. • Automatic refresh: Select an interval from the drop-down list to automatically refresh logs. The interval can be 15 seconds, 30 seconds, 1 minute, or 5 minutes.
Copying logs	Click  to copy the log content.
Viewing context of a log	Click  to view the log context. You can select **Simple View** to view the log context. You can also download the context.
More operations	Click to access the log details page of the time segment and view more log information. • On the **Extended Fields** tab page, view field names and values. You can also click buttons in the **Operation** column to add a field to or exclude a field from a query, set whether a field exists or does not exist, or set whether a field is hidden. • On the **JSON Format** tab page, view the JSON format of logs. • On the **Context Logs** tab page, you can set the number of lines to be queried and filtered fields. You can also download logs and enable the summary mode.
Unfold/Fold	Click  to display all the log content. This unfold button is enabled by default. Click  to fold the log content.

Operation	Description
Downloading logs	Click  . On the displayed **Download Logs** page, click **Direct Download** or **Transfer and Download**. **Direct Download**: Download log files to the local PC. Up to 5,000 logs can be downloaded at a time. Select **.csv** or **.txt** from the drop-down list and click **Download** to export logs to the local PC. **NOTE** • If you select **Export .csv**, logs are exported as a table. • If you select **Export .txt**, logs are exported as a **.txt** file. **Transfer and Download**: Download log files through OBS transfer tasks. Up to 20 million logs can be downloaded at a time. Click **Transfer** to access the **Configure Log Transfer** page. For details, see **Transferring Logs to OBS**.
Hiding/ Expanding all	Click  to set the number of lines displayed in the log content. Click  to hide the log content.
JSON	Move the cursor over  , click **JSON**, and set JSON formatting. Formatting is enabled by default. The default number of expanded levels is 2. • Formatting enabled: Set the default number of expanded levels. Maximum value: **10**. • Formatting disabled: JSON logs will not be formatted for display.
Collapse configuration	Move the cursor over  , click **Log Collapse**, and set the maximum characters to display in a log. If the number of characters in a log exceeds the maximum, the extra characters will be hidden. Click **Expand** to view all. Logs are collapsed by default, with a default character limit of 400.
Log time display	Move the cursor over  and click **Log Time Display**. On the page that is displayed, set whether to display milliseconds and whether to display the time zone. Milliseconds are displayed by default.

Operation	Description
Virtual Scrolling	Move the cursor over  and click **Virtual Scrolling**. On the page that is displayed, set whether to enable virtual scrolling and enter the buffer size. • Virtual scrolling eliminates or minimizes frame and page freezing for better user experience. • Data is re-rendered during the process. This may affect smoothness. • The buffer size determines the amount of data that can be loaded simultaneously. The larger the buffer, the more data loaded simultaneously, but the worse the scrolling performance.
Invisible fields ()	This list displays the invisible fields configured in the layout settings. • The  button is unavailable for log streams without layout settings configured. • If the log content is **CONFIG_FILE** and layout settings are not configured, the default invisible fields include **appName**, **clusterId**, **clusterName**, **containerName**, **hostIPv6**, **NameSpace**, **podName**, and **serviceID**.

7.4.2 Using LTS Search Syntax

LTS provides a range of search syntax to set search criteria and filtering rules for filtering records that meet the search criteria. Then, you can apply analysis statements on the filtering results for advanced analysis and processing.

To quickly understand and use the search syntax, you are advised to learn **Search Modes**, **Phrase Search**, **Operators**, and **Search Statement Examples**.

- Before using the search syntax, set the delimiters in **Index Settings**. If there is no special requirement, use the default delimiters: **,'";=()[]{}@&<>/:\\?\n\t\r and spaces**.
- Search syntax does not support searches by delimiter. For example, in the search statement **var/log**, **/** is a delimiter. The search statement is equivalent to **var log** and searches for all logs that contain both **var** and **log**. Similarly, search statements such as **"var:log"** and **var;log** are used to search for all logs that contain both **var** and **log**.

Search Modes

Search statements are used to define the filter criteria for log search and obtain the logs that meet the criteria.

Depending on the index configuration mode, it can be classified into full-text search and field search; according to the search accuracy, it can be classified into exact search and fuzzy search. Other types of search modes include range search and phrase search.

Table 7-12 Search modes

Search Mode	Description	Example
By full text	LTS splits an entire log into multiple keywords when full-text index is set. • **content** is a built-in field corresponding to the original log text. The search statement **GET** is equivalent to **content:GET**. By default, the original log content is matched. • By default, multiple keywords are connected through **AND**. The search statement **GET POST** is equivalent to **GET** and **POST**.	• GET POST • GET and POST • content:GET and content:POST The preceding search statements have the same function, indicating that logs containing both GET and POST are searched.
By field	Search for specified field names and values (key:value) after field indexing is configured. You can perform multiple types of basic search and combined search based on the data type set in the field index. • The **value** parameter cannot be empty. You can use the **key:""** statement to search for logs with empty field values. • When field search is used together with the **not** operator, logs that do not contain this field are matched.	• **request_time>60 and request_method:po*** indicates that the system searches for logs in which the value of **request_time** is greater than 60 and the value of **request_method** starts with **po**. • **request_method:""** indicates that logs in which the value of **request_method** is empty are searched. • **not request_method:GET** indicates that logs that do not contain the **request_method** field and whose **request_method** value is not **GET** are searched.

Search Mode	Description	Example
By exact match	Use exact words for search. LTS searches with word segmentation, which does not define the sequence of keywords. If the search statement is **abc def**, all logs that contain both **abc** and **def** are matched, for example, logs **abc def** and **def abc**. To ensure the sequence of keywords, use **#"abc def"**.	• **GET POST** indicates that logs containing both **GET** and **POST** are searched. • **request_method:GET** indicates that logs in which the value of **request_method** contains **GET** are searched. • **#"/var/log"** indicates that logs containing phrase **/var/log** are searched.
By fuzzy match	Specify a keyword in the search statement and add a wildcard, that is, an asterisk (*) or a question mark (?), to the middle or end of the keyword. LTS searches all logs for 100 words that meet the search criteria and returns logs that contain the words. The more precise the specified word is, the more accurate the search results are. • The asterisk (*) indicates that multiple characters are matched, and the question mark (?) indicates that one character is matched. • When an asterisk (*) and a question mark (?) are used as delimiters, fuzzy search is not supported since the question mark is a default delimiter. To perform a fuzzy search, remove the question mark from delimiters. • Words cannot start with an asterisk (*) or a question mark (?). • Long and float data does not support fuzzy search using asterisks (*) or question marks (?). • If the fuzzy condition prefix is short and more than 100 words meet the criteria, the search results will be inaccurate.	• **GE*** indicates that the system searches for words starting with **GE** in all logs and returns logs containing these words. • **request_method:GE*** indicates that the system searches for **request_method** values starting with **GE** in all logs and returns logs containing these words.

Search Mode	Description	Example
By scope	The long and float data supports range search. The string fields do not support range query. • Method 1: Use operators such as = (equal to) > (greater than) < (less than) operators to search for logs. • Method 2: Use the in operator to search for logs. The open/closed interval can be modified.	• request_time>=60 indicates that the system searches for logs whose request_time value is greater than or equal to 60. • request_time in (60 120] indicates that the system searches for logs whose request_time value is greater than 60 and less than or equal to 120.
By phrase	Phrase search is used to match exact target phrases in logs. Phrases ensure the sequences of keywords. Fuzzy search is not supported for phrase search.	**#"abc def"** indicates that the system searches all logs for the logs that contain the target phrase abc def.

- Delimiters

  LTS splits the log content into multiple words based on delimiters. Default delimiters include **,'";=()[]{}@&<>/:\\?\n\t\r and spaces**.

  For example, the default delimiters divide the log **2023-01-01 09:30:00** into four parts: **2023-01-01**, **09**, **30**, and **00**.

  In this case, the search statement **2023** cannot match the log. You can search for the log using **2023-01*** or **2023-01-01**.

  If the delimiter is set to null, the field value is regarded as a whole. You can search for the corresponding log only through complete log content or fuzzy search.

- Keyword sequence

  Only the phrase search **#"abc def"** can ensure the sequence of keywords. In other search modes, multiple keywords are connected by AND.

  For example, **request_method:GET POST** is used to query logs that contain both **GET** and **POST**, and the sequence of **GET** and **POST** is not ensured. To ensure their sequence, **Phrase Search** is recommended.

- Chinese search

  Fuzzy search is not required for Chinese search. Phrase search is recommended to match more accurate results.

  In LTS, English content is split into words of different lengths. Therefore, you can use fuzzy search to match logs with English words with the same prefix.

Unigram segmentation is used to a Chinese string into Chinese characters. Each Chinese character is independent, and the length of each part is 1 character.

For example, the search statement **Monday** indicates that logs containing M, o, n, d, a, and y are searched. The search statement **#"Monday"** indicates that logs containing the target phrase **Monday** are searched.

- Invalid keyword

  The syntax keywords of log search statements include: && || AND OR and or NOT not in : > < = ( ) [ ]

  When **and AND or OR NOT not in** are used as syntax keywords, separate them with a space.

  If the log contains syntax keywords and needs to be searched, the search statement must be enclosed in double quotation marks. Otherwise, syntax errors may occur or incorrect results may be found.

  For example, if the search statement **content:and** contains the syntax keyword **and**, change it to **content:"and"**.

Phrase Search

Phrase search precisely matches target phrases. For example, the search statement **#"abc def"** searches all logs containing both **abc** and **def** in that specific sequence, with **abc** preceding **def**. For details about the differences between phrase search and keyword search, see **Table 7-13**.

- Phrase search: It is implemented based on the keyword search syntax. Phrase search can distinguish the sequence of keywords and is used to accurately match target phrases, making the search result more accurate. Phrase search is applicable to English phrases and Chinese phrases, but cannot be used together with fuzzy search.
- Keyword search: Keyword search is implemented based on word segmentation. Delimiters are used to split the search content into multiple keywords for log matching. Keyword search does not distinguish the sequence of keywords. Therefore, as long as a keyword can be matched in a log based on the AND or NOT logic, the log can be found.

Table 7-13 Differences between two search modes

Search Mode	Description	Example
By phrase	Distinguishes the sequence of keywords and is used to accurately match target phrases, making the search result more accurate.	Assume that your log stream contains the following two raw logs: • Raw log 1: **this service is lts** • Raw log 2: **lts is service** If you search for **#"is lts"** or **#"lts is"**, each query matches one log.

Search Mode	Description	Example
By keyword	Does not distinguish the sequence of keywords. The keyword is matched based on the search logic.	Assume that your log stream contains the following two raw logs: • Raw log 1: **this service is lts** • Raw log 2: **lts is service** If you search for **is lts** or **lts is**, each query matches two logs.

The constraints are as follows:

- Fuzzy search cannot be used together with phrase search.

  The asterisk (*) and question mark (?) in phrase search are regarded as common characters. Therefore, phrase search does not support fuzzy search and can be used to search for the asterisk (*) and question mark (?) in logs.
- Phrase search does not support search by delimiter.

  For example, in the search statement **#"var/log"**, **/** is a delimiter. The search statement is equivalent to **#"var log"**, and is used to search for logs containing the target phrase **var log**. Similarly, search statements such as **#"var:log"** and **#"var;log"** are used to search for logs that contain the target phrase **var log**.
- Phrase search is recommended for search in Chinese.

  By default, unary word segmentation is used for Chinese characters. Each Chinese character is segmented separately. During the search, logs that contain each Chinese character in the search statement are matched, which is similar to fuzzy search. When more accurate results are required, phrase search is recommended.

Operators

For details about operators supported by the search statements, see **Table 7-14**.

- Except the in operator, other operators are case-insensitive.
- The priorities of operators in descending order are as follows:
  a. Colon (:)
  b. Double quotation marks ("")
  c. Parentheses: ()
  d. and, not
  e. or

Table 7-14 Operators

Operator	Description	Example
and	If there is no syntax keyword between multiple keywords, the **and** relationship is used by default. When **and** is used as an operator, use a space before and after it. For example, **1 and 2** indicates that logs containing both **1** and **2** are searched, and **1and2** indicates that logs containing **1and2** are searched.	**GET 200** is equivalent to **GET and 200**.
AND	**AND** operator, equivalent to **and**.	GET AND 200
&&	**AND** operator. When **&&** is used as an operator, spaces are not necessary. For example, **1 && 2** is equivalent to **1&&2**, indicating that logs containing both **1** and **2** are searched.	1&&2
or	**or** operator. When **or** is used as an operator, use a space before and after it.	request_method:GET or status:200
OR	**OR** operator, equivalent to **or**.	request_method:GET OR status:200
||	**OR** operator. When **||** is used as an operator, spaces are not necessary.	request_method:GET || status:200
not	**not** operator. • When **not** is used as an operator, use a space before and after it. • When field search is used together with the not operator, logs that do not contain this field are matched.	request_method:GET not status:200, not status:200
( )	Specifies fields that should be matched with higher priority.	(request_method:GET or request_method:POST) and status:200

Operator	Description	Example
:	Searches for a specified field (key:value). Use double quotation marks ("") to enclose a field name (key) or value that contains reserved characters, such as spaces and colons (:). Examples: • **"request method":GET** • **message:"This is a log"** • **time:"09:00:00"** • **ipv6:"2024:AC8:2ac::d09"**	request_method:GET
""	Encloses a syntax keyword to convert it into common characters. For example, **"and"** means searching for logs that contain this word. The word **and** here is not an operator.	request_method:"GET"
\	Escapes double quotation marks (""). The escaped quotation marks indicate the symbol itself.	To search for **instance_id:nginx"01"**, use **instance_id:nginx\"01\"**.
*	An asterisk is a wildcard that matches zero, single, or multiple characters. Put ***** in the middle or at the end of a keyword.	request_method:P*T
?	A question mark matches a single character. Put **?** in the middle or at the end of a keyword.	**request_method:P?T** can match **PUT** but cannot match **POST**.
>	Searches logs in which the value of a field is greater than a specified value.	request_time>100
>=	Searches logs in which the value of a field is greater than or equal to a specified value.	request_time>=100
<	Searches logs in which the value of a field is less than a specified value.	request_time<100
<=	Searches logs in which the value of a field is less than or equal to a specified value.	request_time<=100

Operator	Description	Example
=	Searches logs in which the value of a field is equal to a specified value, applying only to float or long fields. For fields of this type, the equal sign (=) and colon (:) have the same function.	**request_time=100** is equivalent to **request_time:100**.
in	Searches for logs whose field values are in a specified range. Brackets indicate a closed interval, and parentheses indicate an open interval. Numbers are separated with spaces. Enter **in** in lowercase. When it is used as an operator, use a space before and after it.	• request_time in [100 200] • request_time in (100 200]
#""	Searches for logs that contain the target phrase, ensuring the sequence of keywords. The asterisk (*) and question mark (?) in phrase search are regarded as common characters. Therefore, phrase search does not support fuzzy search and can be used to search for the asterisk (*) and question mark (?) in logs.	request_method:#"GET POST"

Search Statement Examples

For the same search statement, different search results are displayed for different log content and index configurations. This section describes search statement examples based on the following log sample and indexes.

Figure 7-2 Log sample

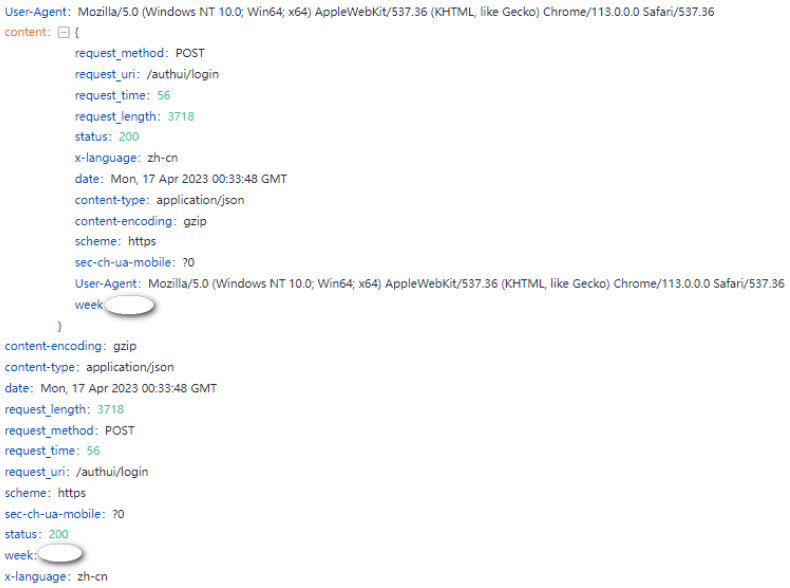


Table 7-15 Search statement examples

Search Requirement	Search Statement
Logs of POST requests whose status code is 200	request_method:POST and status=200
Logs of successful GET or POST requests (status codes 200 to 299)	(request_method:POST or request_method:GET) and status in [200 299]
Logs of failed GET or POST requests	(request_method:POST or request_method:GET) not status in [200 299]
Logs of non-GET requests	not request_method:GET
Logs of successful GET request and request time is less than 60 seconds	request_method:GET and status in [200 299] not request_time>=60
Logs whose request time is 60 seconds.	• request_time:60 • request_time=60
Logs of requests whose time is greater than or equal to 60 seconds and less than 200 seconds	• request_time>=60 and request_time<200 • request_time in [60 200)
Logs that contain and	content:"and" Double quotation marks are used to enclose **and**. In this case, **and** is a common string, not an operator.

Search Requirement	Search Statement
Logs that do not contain the user field.	not user:*
Logs in which the value of **user** is empty are searched.	user:""
Logs in which the value of the week field is not Monday	not week: Monday
Logs in which the value of **sec-ch-ua-mobile** is **?0** are searched.	sec-ch-ua-mobile:#"?0" If search is required when log content contains asterisks (*) or question marks (?), use phrases search.

For more complex search examples, see **Table 7-16**.

Table 7-16 Fuzzy search

Search Requirement	Search Statement
Logs that contain words starting with GE	GE*
Logs that contain words starting with GE and with only one character after GE.	GE?
Logs in which the value of request_method contains a word starting with G.	request_method:G*
Logs in which the value of request_method starts with P, ends with T, and contains a single character in the middle.	request_method:P?T
Logs in which the value of request_method starts with P, ends with T, and contains zero, single, or multiple characters in the middle.	request_method:P*T

Search based on delimiters. For example, the value of the **User-Agent** field is **Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36**.

- If this parameter is left blank, the value of this field is considered as a whole. In this case, when you use **User-Agent:Chrome** to search for logs, no log can be found.
- When the delimiter is set to **, '";=()[]{}?@&<>/:\n\t\r**, the value of this field is split into **Mozilla**, **5.0**, **Windows**, **NT**, **10.0**, **Win64**, **x64**, **AppleWebKit**, **537.36**, **KHTML**, **like**, **Gecko**, **Chrome**, **113.0.0.0**, **Safari**, and **537.36**.

Then you can use search statements such as **User-Agent:Chrome** for search.

Table 7-17 Delimiter-based search

Search Requirement	Search Statement
Logs in which the value of User-Agent contains Chrome	User-Agent:Chrome
Logs in which the value of User-Agent contains the word starting with Win	User-Agent:Win*
Logs in which the value of User-Agent contains Chrome and Linux	User-Agent:"Chrome Linux"
Logs in which the value of User-Agent contains Firefox or Chrome	User-Agent:Chrome OR User-Agent:Linux
Logs in which the value of User-Agent contains Chrome but not Linux	User-Agent:Chrome NOT User-Agent:Linux

7.4.3 Creating an LTS Quick Analysis Task

Logs contain information such as system performance and business status. For example, the frequency of keyword **ERROR** indicates the system health, and the frequency of keyword **BUY** indicates the business activity. You can use the quick analysis function to query specified log keywords. LTS collects statistics on the keywords and generates metric data, so that you can learn about the system performance and business in real time.

- Supports analysis on first 100,000 logs.

  The purpose of quick analysis is to quickly return the distribution and change trend of field values. It does not analyze all data, but only samples.
- Logs can be filtered by query time and criteria for analysis.

  Quick analysis is to analyze the logs queried by query statements. When the number of queried logs is 0, no result is displayed for quick analysis.
- Quick analysis can be used to generate query statements.

  You can click an analysis result to automatically generate a query statement, query logs, and generate a new quick analysis.
- The maximum length of a field for quick analysis is 2 KB.
- The distribution statistics in quick analysis field area displays the first 100 records.
- If quick analysis is not enabled within the analysis time range, a field does not exist, or a field value is null, the analysis result of the field is **null**.
  - When you click **null** to add a string field to the search box, *Field* **: "null"OR NOT** *Field* **: *** will be displayed.
  - When you click **null** to add a float or long field to the search box, **NOT** *Field* **: *** will be displayed.
  - If quick analysis is not enabled, the column-store data used for analysis is not stored, and the analysis result is **null**. In this case, log search is meaningless and no log may be matched.

Prerequisites

Quick analysis is conducted on fields extracted from structured logs. **Setting Cloud Structuring Parsing** raw logs before you create a quick analysis task.

Creating a Quick Analysis Task

Quick analysis is performed on a per-log-stream basis. You can create a quick analysis task as follows:

Step 1 Log in to the management console and choose **Management & Deployment** > **Log Tank Service**. The **Log Management** page is displayed by default.

Step 2 Click the target log group or stream to access the log stream details page.

Step 3 On the **Log Search** tab page, click  next to **Quick Analysis** to go to the **Index Settings** tab page. Under **Index Fields**, enable quick analysis when adding a field.

Step 4 Click **OK**. The quick analysis task is created.

-  indicates a field of the **string** type.
-  indicates a field of the **float** type.
-  indicates a field of the **long** type.
- The maximum length of a field for quick analysis is 2,000 bytes.
- The quick analysis field area displays the first 100 records.

----End

7.4.4 Saving Conditions for Quick Search

If you need to repeatedly use a keyword to search for logs, you can set and save the keyword as a quick query statement for faster log querying and analysis.

Saving Conditions for Quick Search

Step 1 Log in to the management console and choose **Management & Deployment** > **Log Tank Service**. The **Log Management** page is displayed by default.

Step 2 Click the target log group or stream to access the log stream details page.

Step 3 Click  on the **Log Search** tab page. Enter a name and statement for quick search. By default, quick search and quick search (local cache) are enabled.

- A quick search name is used to distinguish multiple quick search statements. The name can be customized and must meet the following requirements:
  - Can contain only letters, digits, hyphens (-), underscores (_), and periods (.).
  - Cannot start with a period (.) or underscore (_) or end with a period (.).
  - Can contain 1 to 64 characters.
- A quick search statement is used to repeatedly search for logs, for example, **error***.

Step 4 Click **OK**. On the **Quick Search** tab page in the left navigation pane, you can view the statements that are successfully saved.

Click the name of a quick search statement to view log details.

----End

Viewing Context of a Log

You can check the logs generated before and after a log for quick fault locating.

Step 1 On the **Log Search** tab page of the log details page, click  to view the context.

Details of several logs generated before and after the log are displayed.

Step 2 On the displayed page, check the log context. For details, see **Table 7-18**.

Table 7-18 Introduction to log context viewing

Feature	Description
Search Rows	Select the number of lines of logs to be queried as required.
Highlighting	Enter a string to be highlighted and press **Enter**.
Filter	Enter a string to be filtered and press **Enter**. When both **Highlighting** and **Filter** are configured, the filtered string can also be highlighted.
Fields	The default field for viewing log context is **content**. Click **Fields** to view the context of other fields.
Prev	View half the number of **Search Rows** leading to the current position. For example, if **Search Rows** is set to 100 and you click **Prev**, 50 rows prior to the current position are displayed. In this case, the current line number is **-50**. If you click **Prev** again, the line number will become **-100**, **-150**, **-200**, and so on.
Current	Current log position. When **Prev** or **Update** is set, you can click **Current** to return to the position where the context starts (when the line number is 0).
Update	View half the number of **Search Rows** following the current position. For example, if **Search Rows** is set to 100 and you click **Update**, 50 rows following the current position are displayed. In this case, the current line number is 50. If you click **Update** again, the line number will become **100**, **150**, **200**, and so on.
Summary Mode	• If this mode is enabled, only the line number and content are displayed. • If this mode is disabled, log details are displayed.
Download	Only content in the **content** field can be downloaded to the local PC.

----End

7.5 Viewing Real-Time Logs

Logs are reported to LTS about every minute, allowing you to view them on the **Real-Time Logs** page within 1 minute after configuring log ingestion. This enables rapid search and analysis.

Prerequisites

- You have created log groups and log streams.
- You have performed operations provided in **Installing ICAgent**.
- You have configured log collection rules.

Viewing Real-Time Logs

Stay on the **Real-Time Logs** tab page to keep updating them in real time. If you leave the **Real-Time Logs** tab page, logs will stop being loaded. The next time you access the tab page, the logs that were shown before you left the tab page will not be displayed.

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.

Step 1 Log in to the management console and choose **Management & Deployment** > **Log Tank Service**. The **Log Management** page is displayed by default.

Step 2 Click the target log group or stream to access the log stream details page.

Step 3 Click the **Real-Time Logs** tab to view the real-time logs.

Filter host and Kubernetes logs by source.

- If **Source** is set to **Host**, set the host IP address and file path.
- If **Source** is set to **K8s**, set the instance name, container name, and file path.

Logs are reported to LTS once every minute. You may wait for at most 1 minute before the logs are displayed.

In addition, you can customize log display by clicking **Clear** or **Pause** in the upper right corner.

- **Filter**: Obtain data from the index configuration, structuring configuration, and latest logs.
- **Clear**: Displayed logs will be cleared from the real-time view.
- **Pause**: Loading of new logs to the real-time view will be paused.

  After you click **Pause**, the button changes to **Continue**. You can click **Continue** to resume the log loading to the real-time view.

----End

8 Log Alarms

8.1 Configuring Log Alarm Rules

You can set alarm rules based on **key words** for logs in log streams to monitor service status in real time. Currently, up to 200 keyword alarm rules can be created for each account.

Prerequisites

A log group and stream have been created. For details, see **Managing Log Groups** and **Managing Log Streams**.

Creating a Keyword Alarm Rule

LTS allows you to collect statistics on log keywords in log streams and set alarm rules to monitor them. By checking the number of keyword occurrences in a specified period, you can have a real-time view of the service running.

Step 1 Log in to the management console and choose **Management & Deployment** > **Log Tank Service**.

Step 2 Choose **Log Alarms** in the navigation pane.

Step 3 Click the **Alarm Rules** tab.

Step 4 Click **Create**. The **Create Alarm Rule** right panel is displayed.

Step 5 Configure alarm rule parameters.

Table 8-1 Keyword alarm rule parameters

Category	Parameter	Description
Basic Info	Rule Name	Name of the alarm rule. Do not start or end with a hyphen (-) or underscore (_). Only letters, digits, hyphens, and underscores are allowed. After an alarm rule is created, the rule name can be modified. After the modification, move the cursor over the rule name to view both new and original rule names. The original rule name cannot be changed.
	Description	Description of the rule.
Statistical Analysis	Statistics	**By keyword**: applicable when keywords are used to search for and configure log alarms.
	Query Condition	**Log Group Name**: Select a log group.
		Log Stream Name: Select a log stream. If a log group contains more than one log stream, you can select multiple log streams when creating a keyword alarm rule.
		Query Time Range: Specify the query period of the statement. It is one period earlier than the current time. For example, if **Query Time Range** is set to one hour and the current time is 9:00, the period of the query statement is 8:00–9:00. • The value ranges from 1 to 60 in the unit of minutes. • The value ranges from 1 to 24 in the unit of hours.
		Keywords: Enter log keywords that can be queried on the **Log Search** tab page. LTS monitors logs in the log stream based on these keywords. Exact and fuzzy matches are supported. Keywords are case-sensitive and can contain up to 1,024 characters. For details about how to set keyword search, see **Using LTS Search Syntax**.

Category	Parameter	Description
	Check Rule	Configure a condition that will trigger the alarm. **Matching Log Events**: When the number of log events that contain the configured keywords reaches the specified value, an alarm is triggered. Four comparison operators are supported: greater than (**>**), greater than or equal to (**>=**), less than (**<**), and less than or equal to (**<=**). ● Click **+** to add a conditional expression with an OR relationship. A maximum of 20 conditional expressions can be added. ● Click  to delete a conditional expression. The number of queries refers to the number of occurrences of the **Query Frequency** set in **Advanced Settings**. The number of times the condition is met refers to the number of times that the keyword appears. The number of queries must be greater than or equal to the number of times the condition must be met. ● The alarm severity can be **critical** (default), **major**, **minor**, or **info**. ● Number of queries: 1–10

Category	Parameter	Description
Advanced Settings	Query Frequency	The options for this parameter are: • **Hourly**: The query is performed at the top of each hour. • **Daily**: The query is run at a specific time every day. • **Weekly**: The query is run at a specific time on a specific day every week. • **Custom interval**: You can specify the interval from 1 minute to 60 minutes or from 1 hour to 24 hours. For example, if the current time is 9:00 and the **Custom interval** is set to 5 minutes, the first query is at 9:00, the second query is at 9:05, the third query is at 9:10, and so on. When the query time range is set to a value larger than 1 hour, the query frequency must be set to every 5 minutes or a lower frequency. • **CRON**: CRON expressions support schedules down to the minute and use 24-hour format. Examples: – **0/10 * * * ***: The query starts from 00:00 and is performed every 10 minutes. That is, queries start at 00:00, 00:10, 00:20, 00:30, 00:40, 00:50, 01:00, and so on. For example, if the current time is 16:37, the next query is at 16:50. – **0 0/5 * * ***: The query starts from 00:00 and is performed every 5 hours at 00:00, 05:00, 10:00, 15:00, 20:00, and so on. For example, if the current time is 16:37, the next query is at 20:00. – **0 14 * * ***: The query is performed at 14:00 every day. – **0 0 10 * ***: The query is performed at 00:00 on the 10th day of every month.
Advanced Settings	Restores	Configure a policy for sending an alarm clearance notification. If alarm clearance notification is enabled and the trigger condition has not been met for the specified number of statistical periods, an alarm clearance notification is sent. Number of last queries: 1–10

Category	Parameter	Description
Advanced Settings	Notify When	• **Alarm triggered**: Specify whether to send a notification when an alarm is triggered. If this option is enabled, a notification will be sent when the trigger condition is met. • **Alarm cleared**: Specify whether to send a notification when an alarm is cleared. If this option is enabled, a notification will be sent when the recovery policy is met.
Advanced Settings	Frequency	You can select **Once**, **Every 5 minutes**, **Every 10 minutes**, **Every 15 minutes**, **Every 30 minutes**, **Every hour**, **Every 3 hours**, or **Every 6 hours** to send alarms. **Once** indicates that a notification is sent once an alarm is generated. **Every 10 minutes** indicates that the minimum interval between two notifications is 10 minutes, preventing alarm storms.
Advanced Settings	Alarm Action Rules	Select a desired rule from the drop-down list. If no rule is available, click **Create Alarm Action Rule** on the right.
Advanced Settings	Language	Select the language used to send alarms.

Step 6 Click **OK**.

After an alarm rule is created, its status is **Enabled** by default. After the alarm rule is disabled, the alarm status is **Disabled**. After the alarm rule is disabled temporarily, the alarm status is **Temporarily closed to May 30, 2023 16:21:24.000 GMT+08:00**. (The time is for reference only.)

When the alarm rule is enabled, an alarm will be triggered if the alarm rule is met. When it is disabled, an alarm will not be triggered even if the alarm rule is met.

----End

Follow-up Operations on Alarm Rules

After creating an alarm rule, you can modify, enable, disable, copy, or delete it. Exercise caution when performing these operations.

- You can perform the following operations on a single alarm rule.

  Modifying an alarm rule: Click **Modify** in the **Operation** column of the target alarm rule. On the displayed page, modify the rule name, query condition, and check rule, and click **OK**.

  Enabling an alarm rule: Click **More** > **Enable** in the **Operation** column of the target alarm rule and ensure the status changes to **Enabled**.

Disabling an alarm rule: Click **More** > **Disable** in the **Operation** column of the target alarm rule and ensure the status changes to **Disabled**.

Temporarily disabling an alarm rule: Click **More** > **Disable Temporarily** in the **Operation** column of the target alarm rule.

Copying an alarm rule: Click **More** > **Copy** in the **Operation** column of the target alarm rule.

Deleting an alarm rule: Click **Delete** in the **Operation** column of the target alarm rule. In the displayed dialog box, click **OK**. Deleted alarm rules cannot be recovered. Exercise caution when performing this operation.

- After selecting multiple alarm rules, you can perform the following operations on them: **Enable**, **Disable**, **Disable Temporarily**, **Re-Enable**, **Enable Clearance**, **Disable Clearance**, **Delete**, and **Export**.
- You can move the cursor to the rule name to view both the new and original names after modification. The original rule name cannot be changed.

8.2 Configuring Log Alarm Notifications

8.2.1 Creating a Message Template on the LTS Console

A message template defines the format of alarm notification messages sent to subscribers. LTS provides built-in message templates. Subscribers can select templates based on protocols. If the template of a specified protocol does not exist, the built-in template of that protocol is used to send messages to subscribers. When using a message template to send alarm notification messages, the system automatically replaces the template variables with the content in the alarm rule.

Creating a Message Template

Step 1 Log in to the management console and choose **Management & Deployment** > **Log Tank Service**.

Step 2 Choose **Log Alarms** in the navigation pane and click the **Alarm Action Rules** tab.

By default, LTS provides the following built-in message templates. If no message content is configured in your selected template, LTS uses a built-in template instead.

- **keywords_template** (English): keyword alarm template

Step 3 Click **Create** on the **Message Templates** tab page. On the displayed page, set the required parameters.

- The email content supports HTML tags and message preview.
- You can create up to 100 message templates for AOM and LTS. If there are already 100 templates, delete unnecessary templates before creating a new one.

Table 8-2 Message template parameters

Parameter	Description	Verification Rule	Example
Template Name	Message template name.	Include digits, letters, underscores (_), and hyphens (-). Do not start or end with an underscore or hyphen. (Max. 100 characters)	LTS-test
Description	Description of the template.	Include digits, letters, and underscores (_). Do not start or end with an underscore. (Max. 1,024 characters)	-
Message Header	Default message header to be added in messages.	• English	• "Dear user,"
Notification method	Notification method.	• Email • SMS • HTTP/HTTPS	-
Topic	Message topic.	Customize the topic name or use variables. (Max. 512 characters) Only email templates need a topic name.	test

Parameter	Description	Verification Rule	Example
Body	Message content.	**Add Variable** • Original rule name: *${event_name}* • Alarm severity: *${event_severity}* • Occurrence time: *${starts_at}* • Occurrence region: *${region_name}* • Account: *${domain_name}* • Alarm source: *$event.metadata.resource_provider* • Resource type: *$event.metadata.resource_type* • Resource ID: *${resources}* • Alarm status: *$event.annotations.alarm_status* • Expression: *$event.annotations.condition_expression* • Current value: *$event.annotations.current_value* • Statistical period: *$event.annotations.frequency* • Rule name: *$event.annotations.alarm_rule_alias* • Frequency: *$event.annotations.notification_frequency* • Original log group name: *$event.annotations.results[0].log_group_name* • Original log stream name: *$event.annotations.results[0].log_stream_name* • Variables supported by keyword alarms:	${event_name} ${event_severity} ${starts_at} ${region_name}

Parameter	Description	Verification Rule	Example
		1. Query time: *$event.annotations.results[0].time* 2. Query logs: (The maximum log size is 2 KB. If a log exceeds 2 KB, the extra part will be truncated and discarded.) *$event.annotations.results[0].raw_results* 3. Query URL: *$event.annotations.results[0].url* 4. Log group/stream name: *$event.annotations.results[0].resource_id* Only the original name of the log group or log stream created for the first time can be added. The modified log group or log stream name cannot be added. 5. Enterprise project ID of the log stream: *$event.annotations.results[0].eps_id* 6. Query custom field: *$event.annotations.results[0].fields.xxx* *xxx* indicates the structured fields and system fields (such as **hostIP** and **hostName**) of the raw logs. The maximum size of a log field is 1 KB. If a field exceeds 1 KB, the extra part will be truncated and discarded. **Copy from Existing** • keywords_template • Custom templates (created with variables)	

Step 4 When the configuration is complete, click **OK**.

----End

Modifying a Message Template

Step 1 In the message template list, click **Modify** in the row that contains the target template, and modify the template according to **Table 8-2**. The template name cannot be modified. Built-in message templates cannot be modified.

Step 2 Click **OK**.

----End

Copying a Message Template

Step 1 In the message template list, click **Copy** in the row that contains the target template. Set a new template name.

Step 2 Click **OK**.

----End

Deleting a Message Template

Step 1 In the message template list, click **Delete** in the **Operation** column of the target template. Built-in message templates cannot be deleted.

Step 2 Click **OK**.

----End

Deleting Message Templates in a Batch

Step 1 In the message template list, select the templates to be deleted and click **Delete**.

Step 2 Click **OK**.

----End

Exporting Message Templates

Step 1 In the message template list, select the templates to be exported and click **Export**.

Step 2 Click **Export all data to an XLSX file** or **Export selected data to an XLSX file**. After the data is exported, you can view it on the local PC.

----End

8.2.2 Creating an Alarm Action Rule

LTS allows you to customize alarm action rules. You can create an alarm action rule to associate an SMN topic with a message template. You can also customize notification content when creating a message template.

Prerequisites

- A topic has been created.
- A topic policy has been configured.
- A subscriber has been added to the topic. A subscriber is the recipient of the notification, for example, an email or SMS message receiver.

Precaution

You can create a maximum of 1,000 alarm action rules. If this number has been reached, delete unnecessary rules.

Creating an Alarm Action Rule

Step 1 Log in to the management console and choose **Management & Deployment** > **Log Tank Service**.

Step 2 Choose **Log Alarms** in the navigation pane.

Step 3 Click the **Alarm Action Rules** tab.

Step 4 Click **Create**. Set parameters such as the action rule name and action rule configuration.

Table 8-3 Parameters for configuring an alarm action rule

Parameter	Description
Action Rule	Enter 1 to 64 characters. Only digits, letters, underscores (_), and hyphens (-) are allowed. Do not start or end with an underscore or hyphen.
Enterprise Project	Select an enterprise project. This parameter is displayed only when the enterprise project function is enabled for the current account.
Description	Enter a description for the rule. Up to 1,024 characters are allowed.
Topic	SMN topic. Select your desired topic from the drop-down list. If there is no topic you want to select, create one on the SMN console.
Message Template	Notification message template. Select your desired template from the drop-down list. If no message template is available, click **Create** to create one.

Step 5 Click **OK**.

----End

More Operations

After an alarm action rule is created, you can perform operations described in Table 8-4.

Table 8-4 Related operations

Operation	Description
Modifying an alarm action rule	Click **Modify** in the **Operation** column.
Exporting an alarm action rule	Select one or more alarm action rules and click **Export**. If no alarm action rule is selected, clicking **Export** will export all alarm action rules.
Deleting an alarm action rule	• To delete a single rule, click **Delete** in the **Operation** column in the row that contains the rule, and then click **Yes** on the displayed page. • To delete one or more rules, select them, click **Delete** above the rule list, and then click **Yes** on the displayed page. Before deleting an alarm action rule, you need to delete the alarm rule bound to the action rule.
Searching for an alarm action rule	Enter a rule name in the search box in the upper right corner and click .

8.3 Viewing Alarms in LTS

LTS allows you to configure keyword alarm rules to periodically query log data. When an alarm rule is met, an alarm will be reported. You can view the alarms on the LTS console.

Prerequisites

You have created an alarm rule.

Procedure

Step 1 Log in to the management console and choose **Management & Deployment** > **Log Tank Service**.

Step 2 Choose **Log Alarms** in the navigation pane.

Step 3 Click the **Alarms** tab. The alarms generated in 30 minutes from now and their trend charts are displayed by default.

Step 4 Set criteria to search for your target alarms.

- In the search box above the alarm list, select a log group, log stream, alarm severity, and rule name.

- Set a time range. By default, 30 minutes is specified (relative time from now).

  There are three types of time range: relative time from now, relative time from last, and specified time. Select a time range as required.

  - From now: queries log data generated in a time range that ends with the current time, such as the previous 1, 5, or 15 minutes. For example, if the current time is 19:20:31 and 1 hour is selected as the relative time from now, the charts on the dashboard display the log data that is generated from 18:20:31 to 19:20:31.
  - From last: queries log data generated in a time range that ends with the current time, such as the previous 1 or 15 minutes. For example, if the current time is 19:20:31 and **1 hour** is selected as the relative time from last, the charts on the dashboard display the log data that is generated from 18:00:00 to 19:00:00.
  - **Specified**: queries log data that is generated in a specified time range.

Step 5 Click  after you set the search criteria. The details and trend of the alarms that match the criteria will be displayed.

Step 6 You can point to the **Details** column of an alarm on the **Active Alarms** tab to view the complete alarm details. Alternatively, click the name in the **Alarm Name** column of an alarm. Details about the alarm are displayed in the right panel that pops up.

After the reported fault is rectified, you can click the deletion button in the row that contains the corresponding alarm on the **Active Alarms** tab to clear the alarm. The cleared alarm will then be displayed on the **Historical Alarms** tab.

If you have configured search criteria to filter alarms, you need to manually refresh the alarm list. To enable automatic refresh, click  in the upper right corner and select **Refresh Every 30s**, **Refresh Every 1m**, or **Refresh Every 5m** from the drop-down list box. You can still manually refresh the alarm list when automatic refresh is enabled by selecting **Refresh Now** from the drop-down list box.

----End

9 Log Transfer

9.1 Overview

After being reported from hosts and cloud services to LTS, logs will be retained in LTS for the retention period you specify. Once this period ends, LTS will delete them. You can specify the retention period when creating a log group or stream. For details, see **Managing Log Groups** and **Managing Log Streams**. Retained logs are deleted once the period is over. For long-term storage or persistent logging, you can transfer logs to other cloud services.

Log transfer refers to when logs are replicated to other cloud services. LTS deletes retained logs once the retention period is over, but the logs that have been transferred to other services are not affected.

9.2 Transferring Logs to OBS

You can transfer logs to OBS and download log files from the OBS console. You can choose scheduled or one-time transfers.

- **Creating a Log Transfer Task**
- **Creating a One-off Log Transfer Task**

Prerequisites

- Logs have been ingested to LTS. For details, see **Log Ingestion**.
- You have created an OBS bucket.

Creating a Log Transfer Task

- To use this function, you must have the **OBS Administrator** permissions apart from the LTS permissions.
- LTS transfers only logs generated after the transfer task is configured, not historical logs.

Step 1 Log in to the management console and choose **Management & Deployment** > **Log Tank Service**.

Step 2 Choose **Log Transfer** in the navigation pane.

Step 3 Click **Configure Log Transfer** in the upper right corner.

Step 4 On the displayed page, configure the log transfer parameters.

Table 9-1 Transfer parameters

Parameter	Description	Example
Log Source Account	• **Current**: Logs of the current account will be transferred. • **Other**: Logs of the delegator account will be transferred. Ensure that the delegator has created an agency for log transfer delegation. For details, see **Creating an Agency**.	Current
Transfer Mode	If you select the current account as the log source account, select **Scheduled**. **Scheduled**: Logs are periodically transferred to OBS for long-term storage.	Scheduled
Agency Name	This parameter is required when **Log Source Account** is set to **Other**. Enter the name of the agency created by the delegator.	-
Delegator Account Name	This parameter is required when **Log Source Account** is set to **Other**. Enter the account name of the delegator.	-
Enable Transfer	Enabled by default.	Enabled
Transfer Destination	Select a cloud service for log transfer.	OBS
Log Group Name	Select a log group.	N/A

Parameter	Description	Example
Enterprise Project Name	Select an enterprise project. • This parameter is displayed only when the enterprise project function is enabled for the current account. • If the enterprise project function is enabled for the current account: – All enterprise projects under the current account are displayed in the drop-down list when **Log Source Account** is set to **Current**. – **default** is displayed when **Log Source Account** is set to **Other** and the enterprise project function is not enabled for the delegator account. – All enterprise projects under the delegator account are displayed when **Log Source Account** is set to **Other** and the enterprise project function is enabled for the delegator account.	-
Log Stream Name	Select a log stream. Log streams that have been configured with OBS transfer settings cannot be configured again.	-
OBS Bucket	• Select an OBS bucket. – If no OBS buckets are available, click **View OBS Bucket** to access the OBS console and create an OBS bucket. • Currently, LTS supports only **Standard** OBS buckets.	-

Parameter	Description	Example
Custom Log Transfer Path	• Enabled: Logs will be transferred to a custom path to separate transferred log files of different log streams. The format is **/LogTanks/***Region name*/*Custom path*. The default custom path is **lts/%Y/%m/%d**, where **%Y** indicates the year, **%m** indicates the month, and **%d** indicates the day. A custom path must meet the following requirements: – Must start with **/LogTanks/***Region name*. – Can contain only letters, digits, and the following special characters: &$@;:,= +?-._/ %. The character % can only be followed only by Y (year), m (month), d (day), H (hour), and M (minute). Any number of characters can be added before and after %Y, %m, %d, %H, and %M, and the sequence of these variables can be changed. – Can contain 1–128 characters. Example: 1. If you enter **LTS-test/%Y/%m/%d/%H/%M**, the path is **LogTanks/***Region name*/**LTS-test/***Y*/*m*/*d*/*H*/*M*/*Log file name*. 2. If you enter **LTS-test/%d/%H/%m/%Y**, the path is **LogTanks/***Region name*/**LTS-test/***d*/*H*/*m*/*Y*/*Log file name*. • Disabled: Logs will be transferred to the default path. The default path is **LogTanks/***Region name/2019/01/01/Log group/Log stream/Log file name*.	LTS-test/%Y/%m/%d/%H/%M
Log Prefix	The file name prefix of the log files transferred to an OBS bucket The prefix must meet the following requirements: • Can contain 0 to 64 characters. • Can contain only letters, digits, hyphens (-), underscores (_), and periods (.). Example: If you enter **LTS-log**, the log file name will be **LTS-log**_*Log file name*.	LTS-log

Parameter	Description	Example

Format	The storage format of logs. The value can be **Raw log format** or **JSON**.
	• Example of the raw log format: (Logs displayed on the LTS console are in the raw format.)
	`Sep 30 07:30:01 ecs-bd70 CRON[3459]: (root) CMD (/opt/oss/servicemgr/ICAgent/bin/manual/mstart.sh > /dev/null 2>&1)`
	• Example of the JSON format:
	`{"host_name":"ecs-bd70","ip":"192.168.0.54","line_no":249,"message":"Sep 30 14:40:01 ecs-bd70 CRON[4363]: (root) CMD (/opt/oss/servicemgr/ICAgent/bin/manual/mstart.sh > /dev/null 2>&1)\n","path":"/var/log/syslog","time":1569825602303}`
		JSON

Log Transfer Interval	The interval for automatically transferring logs to OBS buckets. The value can be 2, 5, or 30 minutes, or 1, 3, 6, or 12 hours.	3 hours
Time Zone	When logs are transferred to OBS buckets, the time in the transfer directory and file name will use the specified UTC time zone.	(UTC) Coordinated Universal Time
Filter by Tag Fields	During transfer, logs will be filtered by tag fields collected by ICAgent. • Disabled: Logs will not be filtered by tag fields. • Enabled: Default tag fields include those for hosts (**hostIP**, **hostId**, **hostName**, **pathFile**, and **collectTime**) and for Kubernetes (**clusterName**, **clusterId**, **nameSpace**, **podName**, **containerName**, and **appName**). Optional public tag fields are **regionName**, **logStreamName**, **logGroupName**, and **projectId**. When **Filter by Tag Fields** is enabled, **Format** must be **JSON**. • **Transfer Tag**: After this function is enabled, log stream tags are also transferred.	Enabled
Compressed Format	Non-compression and gzip/zip/snappy compression are supported.	gzip

Step 5 Click **OK**. When the log transfer status changes to **Normal**, the transfer task has been created.

Step 6 Click the OBS bucket name in the **Transfer Destination** column to switch to the OBS console and view the transferred log files.

Transferred logs can be downloaded from OBS to your local computer for viewing. Logs stored in OBS are in raw or JSON format.

----End

Creating a One-off Log Transfer Task

Step 1 Click **Configure Log Transfer** in the upper right corner.

Step 2 On the displayed page, configure the log transfer parameters.

Table 9-2 Transfer parameters

Parameter	Description	Example
Transfer Mode	**One-time**: Logs are transferred to OBS for long-term storage in a one-time way.	One-time
Transfer Destination	Select a cloud service for log transfer.	OBS
Log Group Name	Select a log group.	N/A
Enterprise Project Name	Select an enterprise project. • This parameter is displayed only when the enterprise project function is enabled for the current account. • If the enterprise project function is enabled for the current account: – All enterprise projects under the current account are displayed in the drop-down list when **Log Source Account** is set to **Current**. – **default** is displayed when **Log Source Account** is set to **Other** and the enterprise project function is not enabled for the delegator account. – All enterprise projects under the delegator account are displayed when **Log Source Account** is set to **Other** and the enterprise project function is enabled for the delegator account.	-
Log Stream Name	Select a log stream. Log streams that have been configured with OBS transfer settings cannot be configured again.	-
Filter By	**Keyword** is selected by default. Enter the keyword to be filtered in the text box.	-

Parameter	Description	Example
Log Time Range	There are three types of time range: relative time from now, relative time from last, and specified time. Select a time range as required. • **From now**: queries log data generated in a time range that ends with the current time, such as the previous 1, 5, or 15 minutes. For example, if the current time is 19:20:31 and **1 hour** is selected as the relative time from now, the charts on the dashboard display the log data that is generated from 18:20:31 to 19:20:31. • **From last**: queries log data generated in a time range that ends with the current time, such as the previous 1 or 15 minutes. For example, if the current time is 19:20:31 and **1 hour** is selected as the relative time from last, the charts on the dashboard display the log data that is generated from 18:00:00 to 19:00:00. • **Specified**: queries log data that is generated in a specified time range.	-
Total Log Events	Total number of log events.	-
Log Files	Max log events for each transfer: 20 million. Max transfer files: 200.	-
OBS Bucket	• Select an OBS bucket. If no OBS buckets are available, click **View OBS Bucket** to access the OBS console and create an OBS bucket. • Currently, LTS supports only **Standard** OBS buckets. • Data cannot be transferred to an OBS bucket whose storage class is **Archive** or for which cross-region replication has been configured.	-
Bucket Directory	Directory of the OBS bucket. Do not start or end with a slash (/).	-
Transfer File Name	Custom transfer file name. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed.	-

Parameter	Description	Example

Format	Storage format of logs. The value can be **Raw log format**, **JSON**, or **CSV**.
	• Example of the raw log format:
	(Logs displayed on the LTS console are in the raw format.)
	`Sep 30 07:30:01 ecs-bd70 CRON[3459]: (root) CMD (/opt/oss/servicemgr/ICAgent/bin/manual/mstart.sh > /dev/null 2>&1)`
	• Example of the JSON format:
	`{"host_name":"ecs-bd70","ip":"192.168.0.54","line_no":249,"message":"Sep 30 14:40:01 ecs-bd70 CRON[4363]: (root) CMD (/opt/oss/servicemgr/ICAgent/bin/manual/mstart.sh > /dev/null 2>&1)\n","path":"/var/log/syslog","time":1569825602303}`
	• **CSV**: Log content is displayed in a table.
		JSON

Public Tag Fields	Optional public tag fields are **regionName**, **logStreamName**, **logGroupName**, and **projectId**.	-
Transfer Tag	After this function is enabled, log stream tags are also transferred.	-

Step 3 Click **OK**. When the log transfer status changes to **Normal**, the transfer task has been created.

Step 4 Click the OBS bucket name in the **Transfer Destination** column to switch to the OBS console and view the transferred log files.

Step 5 Download the transferred logs from OBS for viewing.

----End

Modifying a Log Transfer Task

1. Locate the row that contains the target transfer task and click **Modify** in the **Operation** column.
2. Click **OK**.

Viewing Transfer Details

1. Locate the target log transfer task and click **More** > **Details** in the row of the desired task to view its details.
2. On the displayed **Transfer Details** page, you can view the log transfer details.

Deleting a Log Transfer Task

If logs do not need to be transferred, you can delete the transfer task.

- After a transfer task is deleted, log transfer will be stopped. Exercise caution when performing the deletion.

- After a transfer task is deleted, the logs that have been transferred remain in OBS.
- When you create a transfer task, OBS will grant read and write permissions to LTS for the selected bucket. To delete a transfer task that uses an OBS bucket, perform the following operations:
  - If only one transfer task uses this OBS bucket, delete the bucket access permission granted to specific users on the **Permissions** > **Bucket ACL** tab page on the OBS console when you delete the transfer task.
  - If multiple transfer tasks use this OBS bucket, do not delete the bucket access permission. Otherwise, data transfer will fail.

1. Locate the row of the target transfer task and choose **Delete** in the **Operation** column.
2. Click **OK**.

Viewing Transfer Status

The status of a transfer task can be **Normal**, **Abnormal**, or **Closed**.

- **Normal**: The log transfer task works properly.
- **Abnormal**: An error occurred in the log transfer task. The possible cause is that the access control on the OBS bucket is configured incorrectly. Access the OBS console to correct the settings.
- **Closed**: The log transfer task is stopped.

10 Configuration Center

10.1 Setting LTS Log Collection Quota

Enabling or Disabling Log Collection Beyond Free Quota

When the monthly free quota (500 MB) is used up, you will be billed for any excess usage on a pay-per-use basis. To avoid extra expenses, you can configure log collection to stop when the quota runs out.

- The function is enabled by default. If it is enabled, logs will continue to be collected after the free quota (500 MB) is used up. You will be billed for the excess usage on a pay-per-use basis.
- Log usage, including log read/write, log indexing, and log retention, are billed in LTS. If log collection is disabled when the free quota is used up, no fee is generated for log read/write and indexing because these operations will not be performed. However, log data that beyond the free quota is still retained in LTS and fees are generated for the log retention. When the logs age out after the specified retention period, no fees will be generated.
- If you enable or disable **Continue to Collect Logs When the Free Quota is Exceeded** in AOM, this function will be synchronously enabled or disabled in LTS.

Step 1 Log in to the management console and choose **Management & Deployment** > **Log Tank Service**.

Step 2 In the navigation pane, choose **Configuration Center**. The **Quota Configuration** tab page is displayed by default.

Step 3 Disable **Continue to Collect Logs When the Free Quota Is Exceeded**.

When the free quota (500 MB) is used up, log collection will be suspended. You can view the current resource usage in **Overview** area on the **Log Management** page. For details, see **Viewing Log Management**.

----End

10.2 Configuring Log Content Delimiters

You can configure delimiters to split log content into words, so you can search for logs by these words. LTS has preconfigured the following delimiters:

```
, '";=()[]{}@&<>/:\\?\n\t\r
```

If the default delimiters cannot meet your needs, you can set custom delimiters.

Precautions

- Your custom delimiters are applicable only to the log events generated after the delimiters are configured.
- The delimiter configured on the **Delimiters** tab page takes effect for all log streams in the current region. For details about how to configure delimiters for a single log stream, see **Setting Indexes**.

Procedure

Step 1 Log in to the management console and choose **Management & Deployment** > **Log Tank Service**.

Step 2 Choose **Configuration Center** in the navigation pane and click the **Delimiters** tab.

Step 3 Configure delimiters.

You can configure delimiters in either of the following ways. If you use both ways, the delimiters configured in the two ways will all take effect.

- **Common Delimiters**: Click **Edit** and enter custom delimiters in the text box.
- **ASCII Delimiters**: Click **Edit** > **Add ASCII Delimiter**, and enter ASCII values by referring to **ASCII Table**.

Step 4 Preview the parsing result.

Enter log content in the text box and click **Preview**.

Step 5 Check whether the parsing result is correct. If it is correct, click **Save**.

You can click **Reset** to restore the default delimiters.

----End

ASCII Table

Table 10-1 ASCII table

ASCII Value	Character	ASCII Value	Character	ASCII Value	Character	ASCII Value	Character
0	NUL (Null)	32	Space	64	@	96	`

ASCII Value	Character	ASCII Value	Character	ASCII Value	Character	ASCII Value	Character
1	SOH (Start of heading)	33	!	65	A	97	a
2	STX (Start of text)	34	"	66	B	98	b
3	ETX (End of text)	35	#	67	C	99	c
4	EOT (End of transmission)	36	$	68	D	100	d
5	ENQ (Enquiry)	37	%	69	E	101	e
6	ACK (Acknowledge)	38	&	70	F	102	f
7	BEL (Bell)	39	'	71	G	103	g
8	BS (Backspace)	40	(	72	H	104	h
9	HT (Horizontal tab)	41	)	73	I	105	i
10	LF (Line feed)	42	*	74	J	106	j
11	VT (Vertical tab)	43	+	75	K	107	k
12	FF (Form feed)	44	,	76	L	108	l
13	CR (Carriage return)	45	-	77	M	109	m
14	SO (Shift out)	46	.	78	N	110	n
15	SI (Shift in)	47	/	79	O	111	o
16	DLE (Data link escape)	48	0	80	P	112	p
17	DC1 (Device control 1)	49	1	81	Q	113	q
18	DC2 (Device control 2)	50	2	82	R	114	r

ASCII Value	Character	ASCII Value	Character	ASCII Value	Character	ASCII Value	Character
19	DC3 (Device control 3)	51	**3**	83	**S**	115	**s**
20	DC4 (Device control 4)	52	**4**	84	**T**	116	**t**
21	NAK (Negative acknowledge)	53	**5**	85	**U**	117	**u**
22	SYN (Synchronous idle)	54	**6**	86	**V**	118	**v**
23	ETB (End of transmission block)	55	**7**	87	**W**	119	**w**
24	CAN (Cancel)	56	**8**	88	**X**	120	**x**
25	EM (End of medium)	57	**9**	89	**Y**	121	**y**
26	SUB (Substitute)	58	**:**	90	**Z**	122	**z**
27	ESC (Escape)	59	**;**	91	**[**	123	**{**
28	FS (File separator)	60	**<**	92	\	124	**|**
29	GS (Group separator)	61	**=**	93	**]**	125	**}**
30	RS (Record separator)	62	**>**	94	**^**	126	**~**
31	US (Unit separator)	63	**?**	95	_	127	DEL (Delete)

10.3 Setting ICAgent Collection

On the **ICAgent Collection** tab page, you can disable or enable ICAgent collection (that is, specify whether ICAgent collects log data), syslog log collection to AOM, and container standard output to AOM.

Setting Collection

Step 1 Log in to the management console and choose **Management & Deployment** > **Log Tank Service**.

Step 2 Choose **Configuration Center** in the navigation pane and click the **ICAgent Collection** tab.

Step 3 Toggle the **ICAgent Collection** switch to control whether ICAgent collects logs.

- **ICAgent Collection** is toggled on by default. If you do not need to collect logs, toggle it off to reduce resource usage.
- After it is toggled off, ICAgent will stop collecting logs, and the log collection function on the AOM console will also be disabled.

Step 4 Toggle the **Collect Syslog Logs to AOM** switch to set whether ICAgent collects Syslogs to AOM 1.0. If it is toggled off, ICAgent does not collect Syslog logs to AOM 1.0. This function is only available with ICAgent 5.12.182 and later.

Step 5 **Output to AOM**: Select a CCE cluster and toggle on or off the **Apply to Cluster** switch for it. If it is toggled off, ICAgent does not collect the cluster stdout logs to AOM. This function is only available with ICAgent 5.12.133 and later. You are advised to collect container standard output to LTS instead of AOM. For details, see **Ingesting CCE Application Logs to LTS**.

----End

11 Querying Real-Time LTS Traces

Overview

CTS can record operations (traces) related to LTS for query, audit, and backtracking.

After you enable CTS, the system starts to record LTS operations. CTS stores operation records from the last seven days.

Enabling CTS

To enable CTS, see **Enabling CTS**.

After CTS is enabled, if you want to view LTS traces, see **Querying Real-Time Traces**.

LTS Operations That Can Be Recorded by CTS

Table 11-1 LTS operations that can be logged by CTS

Operation	Resource Type	Trace Name
Creating a log group	group	createLogGroup
Modifying a log group	group	updateLogGroup
Deleting a log group	group	deleteLogGroup
Creating a log stream	topic	createLogStream
Modifying a log stream	topic	updateLogStream
Deleting a log stream	topic	deleteLogStream
Deleting a log bucket	logPailSetting	deleteLogPail
Creating an OBS log transfer task	als	addLogPailToOBS
Modifying an OBS log transfer task	als	updateLogPailToOBS

Operation	Resource Type	Trace Name
Deleting an OBS log transfer task	als	deleteLogPailToOBS
Batch enabling and disabling log transfer tasks	als	batchActionLogPail-ToOBS
Enabling log transfer	transfer	createLogTransfer
Modifying log transfer	transfer	updateLogTransfer
Deleting log transfer	transfer	deleteLogTransfer
Creating quick search criteria	searchCriteria	createLogSearchCriteria
Modifying quick search criteria	searchCriteria	updateLogSearchCriteria
Deleting quick search criteria	searchCriteria	deleteLogSearchCriteria
Adding a collection path	LogAgent	createLogAgent
Modifying a collection path	LogAgent	updateLogAgent
Deleting a collection path	LogAgent	deleteLogAgent
Creating a structuring template	structLogConfig	createLogStreamStruct-Config
Modifying a structuring template	structLogConfig	updateLogStreamStruct-Config
Deleting a structuring template	structLogConfig	deleteLogStreamStruct-Config
Creating a quick analysis task	wordFreqConfig	updateWordFreqConfig
Saving the path configuration	path	addLogPath
Adding a statistical rule	rule	addRuleStatistics
Modifying a statistical rule	rule	updateRuleStatistics
Deleting a statistical rule	rule	deleteRuleStatistics
Creating a structuring rule	structurization	addStructurization
Deleting a structuring rule	structurization	deleteStructurization

Operation	Resource Type	Trace Name
Adding a Kafka instance	dmsKafka	registerKafkaInfo
Modifying a Kafka instance	dmsKafka	updateKafkaInfo
Deleting a Kafka instance	dmsKafka	deleteKafkaInfo
Creating a DIS transfer task	transfer	createDisTransfer
Modifying a DIS transfer task	transfer	updateDisTransfer
Deleting a DIS transfer task	transfer	deleteDisTransfer
Creating a Kafka transfer task	kafkaTransfer	createKafkaTransfer
Modifying a Kafka transfer task	kafkaTransfer	updateKafkaTransfer
Deleting a Kafka transfer task	kafkaTransfer	deleteKafkaTransfer
Creating a chart	logChart	createLogChart
Modifying a chart	logChart	updateLogChart
Deleting a chart	logChart	deleteLogChart
Creating a dashboard	logDashboard	createLogDashboard
Modifying a dashboard	logDashboard	updateLogDashboard
Deleting a dashboard	logDashboard	deleteLogDashboard
Enabling continuation of log collection when the free quota is exceeded	LogCollectionSwitchOperation	LogCollectionSwitchOperation
Disabling continuation of log collection when the free quota is exceeded	LogCollectionSwitchOperation	LogCollectionSwitchOperation
Creating an ELB log bucket	elbPailType	createElbPail
Modifying an ELB log bucket	elbPailType	updateElbPail
Deleting an ELB log bucket	elbPailType	deleteElbPail
Adding a log path collection rule	logPathCollectionType	createLogPathCollection

Operation	Resource Type	Trace Name
Modifying a log path collection rule	logPathCollectionType	updateLogPathCollection
Deleting a log path collection rule	logPathCollectionType	deleteLogPathCollection
Clearing Redis cache	cleanTenantResource-Type	deleteCleanTenantRe-source

12 FAQs

12.1 Host Management

12.1.1 What Do I Do If ICAgent Installation Fails in Windows and the Message "SERVICE STOP" Is Displayed?

Background

The ICAgent installation fails and the message **SERVICE STOP** is displayed.

The following issues may occur after the installation fails:

- No ICAgent task exists in the task manager.
- No ICAgent service exists in the system service list.
- When **sc query icagent** is executed in the command line tool (CLI), a message is displayed, indicating that no ICAgent was found.

Possible Causes

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

Solution

1. Check whether any antivirus software is running. If yes, go to the next step.
2. Stop the antivirus software and install ICAgent again.

12.1.2 What Do I Do If ICAgent Upgrade Fails on the LTS Console?

ICAgent is installed in overwrite mode. If an upgrade fails, directly run the installation command again and re-upgrade ICAgent.

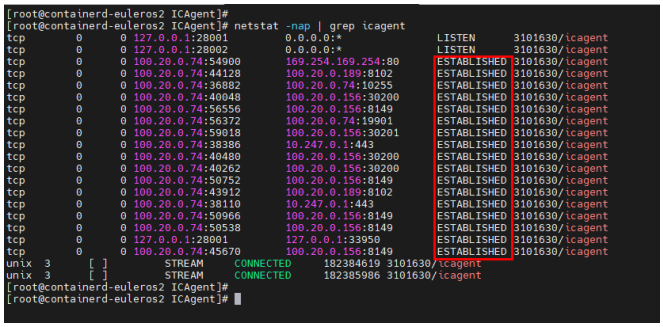
12.1.3 What Do I Do If ICAgent Is Displayed as Offline on the LTS Console After Installation?

In this case, perform the following steps:

Step 1 Check whether the ICAgent network connection is normal.

1. Log in to the host where ICAgent is installed.
2. Run the **netstat -nap | grep icagent** command to check whether the network connection status of the ICAgent process is **ESTABLISHED**. If yes, the network connection is normal.

   Check whether the connection status of ports 30200 and 30201 on the server is **ESTABLISHED**. If not, check whether these ports are allowed in the security group.



Step 2 Check whether the ICAgent authentication is successful.

1. Run the **cd /var/ICAgent** command to go to the ICAgent log directory.
2. Run the **zgrep 'msworkflow' * | grep 'retCode\['** command to query the ICAgent authentication log.
   - If **200** is returned, the authentication is successful. If ICAgent is still offline, contact technical support.
   - If the return code is not 200, check whether the AK/SK pair entered during ICAgent installation is correct. If not, go to the next step.

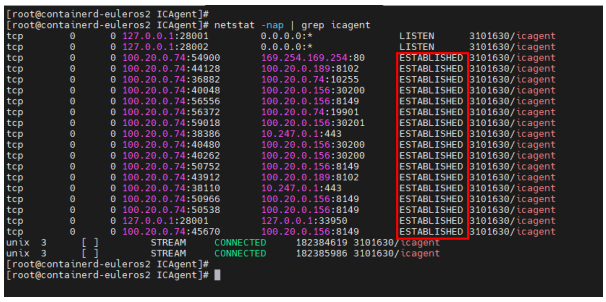
Step 3 Obtain the correct AK/SK pair and install ICAgent again.

----End

12.1.4 What Do I Do If I Do Not See a Host with ICAgent Installed on the LTS Console?

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

- If you are configuring ECS log ingestion and do not see the host with ICAgent installed on the **Hosts** tab page:
  a. On the **Install ICAgent** page, ensure that the installation command is correctly copied. Do not use the installation command across regions.
  b. Ensure that the obtained AK/SK pair is correct and has not been deleted.
  c. Run the **netstat -nap | grep icagent** command to check whether the network connection status of the host is **ESTABLISHED**. If yes, the network connection is normal.



- If you are configuring CCE log ingestion and do not see the host with ICAgent installed on the **Hosts** tab page:

  a. Ensure that ICAgent has been installed in the CCE cluster.

  b. If ICAgent is not installed, click **CCE Cluster** on the **Hosts** tab page and click **Upgrade ICAgent**.

12.1.5 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 pair of a public account.

- 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 pair will not be deleted or disabled. If the AK/SK pair is deleted, 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 pair immediately. Keep the AK/SK pair secure.

12.1.6 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.

Creating an Agency

1. Log in to the management console and choose **Identity and Access Management** in the service list.

2. Choose **Agencies** in the navigation pane.
3. Click **Create Agency** in the upper right corner and set parameters as follows:

Table 12-1 Agency parameters

Parameter	Description
Agency Name	Set the agency name. For example, **lts_ecm_trust**.
Agency Type	Select **Cloud service**.
Cloud Service	Select **ECS**.
Validity Period	Select **Unlimited**.
Description	(Optional) Provide details about the agency.

4. Click **Next**.
5. Search for **LTS Administrator** and **APM Administrator** in the permission search box and select them.
6. Click **Next**, set the authorization scope to **Region-specific projects**, and select projects.
7. 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.

12.2 Log Ingestion

12.2.1 What Do I Do If the CPU Usage Is High When ICAgent Is Collecting Logs?

If the CPU usage is high when ICAgent is collecting logs (causing issues like slow running or program breakdown), 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.

12.2.2 What Kinds of Logs and Files Does 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, enable log reporting to LTS on their consoles.

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 a file name (only text files are supported), the specified file is collected. Note that LTS only collects logs generated in the last 7 days (depending on the local time zone of the host).

12.2.3 Will LTS Stop Collecting Logs After the Free Quota Is Used Up If I Disable "Continue to Collect Logs When the Free Quota Is Exceeded" in AOM?

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.

12.2.4 How Do I Disable the Function of Collecting CCE Standard Output Logs to AOM on the LTS Console?

Symptom

As the products evolve, collecting CCE standard output logs to AOM is no longer recommended. You can disable this function on the LTS console as needed. You are advised to collect CCE standard output logs to LTS for unified log management.

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

Solution

Step 1 Log in to the management console and choose **Management & Deployment** > **Log Tank Service**.

Step 2 Choose **Host Management** > **Hosts** in the navigation pane.

Step 3 On the **CCE Clusters** tab page, select the target CCE cluster and disable **Output to AOM**.

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

----End

12.2.5 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 LTS console.

12.3 Log Search and Analysis

12.3.1 How Often Is the Data Loaded in the Real-Time Log View in LTS?

Generally, the real-time logs are loaded to the LTS console 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.

12.3.2 What Do I Do If I Cannot View Reported Logs in LTS?

Symptom

Logs reported to LTS are not displayed on the LTS console.

Possible Causes

- ICAgent has not been installed.
- The collection path is incorrectly configured.
- **ICAgent Collection** in **Configuration Center** on the LTS console is disabled.
- 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

- If ICAgent has not been installed, install it. For details, see **Installing ICAgent**.
- If the collection path is incorrectly configured, modify it. 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 a text file name, that file is directly collected.
- If **ICAgent Collection** is disabled, log in to the LTS console, choose **Configuration Center** > **ICAgent Collection**, and enable **ICAgent Collection**.
- If the rate of writing logs into log streams or length of single-line logs exceeds the limit, or the browser has slowed down because of the amount of log data, use Google Chrome or Firefox to query logs.

12.3.3 Can I Manually Delete Logs on the LTS Console?

No. Manual deletion is not supported. LTS automatically deletes logs when the retention duration ends.

12.3.4 What Do I Do If I Could Not Search for Logs on LTS?

When you search for logs on the LTS console, if a message is displayed indicating that the query result is inaccurate, too many log results are matched, or field *XXX* without indexing configured cannot be queried, perform the following operations:

Message Displayed During Query: Inaccurate Query Results

- Possible causes: 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.

Too Many Logs Results from Log Query

- Possible cause: Only searches with phrase **#"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 phrase **#"abc def"** to accurately match logs containing phrase **abc def**.

Expected Logs Not Obtained with Specific Search Statements and No Error Message Displayed

- Possible causes: Search delimiters are not supported, or ***** and **?** in a search statement are regarded as common characters and are not used as wildcards.
- Solution: Use the correct query statement.

Message Displayed During Query: Field *XXX* Is Not Configured with Indexing and Cannot Be Queried

- Possible cause: No field indexing is configured.
- Solution: Create an index for field *XXX* on the **Index Settings** tab page and run the query statement again.

Message Displayed During Query: Full-Text Index Not Enabled and content Field and Full-Text Query Unsupported

- Possible cause: Full-text indexing is disabled.
- Solution: Enable **Index Whole Text** on the **Index Settings** tab page and run the query statement again.

Message Displayed During Query: Do Not Start with an Asterisk (*) or a Question Mark (?)

- Possible cause: An asterisk (*) or question mark (?) is placed before the query statement.
- Solution: Modify the query statement or use a correct delimiter.

Message Displayed During Query: long and float Fields Do Not Support Fuzzy Query Using Asterisks (*) or Question Marks (?)

- Possible cause: An asterisk (*) or question mark (?) is used to query fields of the long and float types.
- Solution: Modify the query statement and use operators (>=<) or IN syntax for range query.

Message Displayed During Query: string Fields Do Not Support Range Query Using the Operator (>=<) or IN Syntax

- Possible cause: Operators (>=<) or the IN syntax is used to query fields of the string type.
- Solutions:
  a. Modify the query statement and use the asterisk (*) or question mark (?) to perform fuzzy query.
  b. Change the value of this field to a number.

Message Displayed During Query: The Search Syntax Is Incorrect and the Query Statement Needs to Be Modified

- Possible cause: The syntax of the operator is incorrect.

  Solution: Each operator has its syntax rule. Modify the search statement based on the rule. For example, 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"**.

12.4 Log Transfer

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

The log transfer function only forwards existing logs and does not delete them. LTS deletes retained logs once the retention period is over, but the logs that have been transferred to other services are not affected.

During log transfer, logs are "replicated" from LTS to OBS. 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.

12.4.2 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.
2. Click **Configure** in the row of the tracker **system**.
3. On the **Basic Information** page, click **Next**.
4. In the **Configure Transfer** step, configure parameters of log transfer 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.

12.4.3 What Are the Common Causes of LTS Log Transfer Abnormalities?

If a log transfer task is in the abnormal state on the **Log Transfer** page of the LTS console:

Possible cause: The OBS bucket policy is incorrect.

Solution: Go to the OBS console to correct the settings.

12.4.4 What Do I Do If I Cannot View Historical Data in an OBS Bucket After Transferring Data from LTS to OBS?

This occurs because LTS only transfers logs generated after you configure the transfer task to OBS buckets. Logs that already exist before the configuration will not be transferred.

