Log Tank Service

User Guide

Issue 01

Date 2024-02-28

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.

Contents

1 Log Management

1.1 LTS Console

The LTS console provides resource statistics, your favorite log streams/favorite log streams (local cache), alarm statistics, latest alarms, FAQs, and recently viewed log streams.

Resource Statistics

This area shows the read/write traffic, index traffic, log volume, and raw log traffic of the account on the previous day, as well as the day-on-day changes.

Figure 1-1 Resource statistics

For details, see **Resource Statistics**.

Log Applications

LTS can collect standard logs from multiple cloud services. LTS provides out-of-the-box log dashboard templates, such as ELB log center, VPC flow log center, CFW log center, and APIG log center, allowing you to analyze logs once after log ingestion.

NOTE

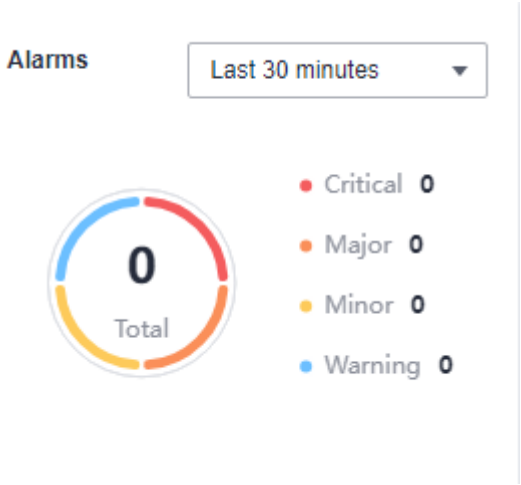
This function is available only in regions AF-Johannesburg, AP-Singapore, CN-Hong Kong, CN East-Shanghai1, LA-Mexico City1, LA-Mexico City2, LA-Santiago, and LA-Sao Paulo1.

Alarm Statistics

This area contains the total number of alarms in LTS and the number of alarms at each severity level. You can view alarm statistics of the last 30 minutes, last 1

hour, last 6 hours, last 1 day, or last 1 week. The alarm severity levels are **Critical**, **Major**, **Minor**, and **Warning**.

Figure 1-2 Alarm Statistics

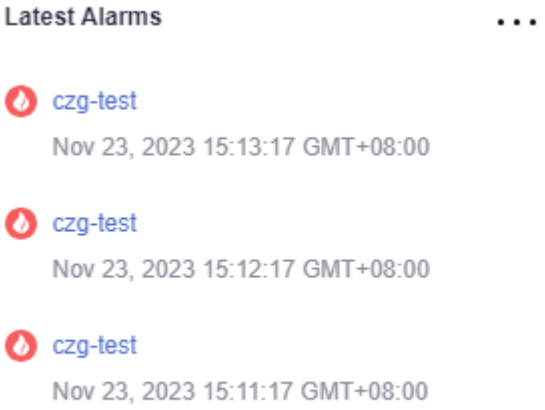


Latest Alarms

This area displays a maximum of three latest alarm rules in the last 30 minutes.

To view more alarms or add alarm rules, click ••• .

Figure 1-3 Latest Alarms



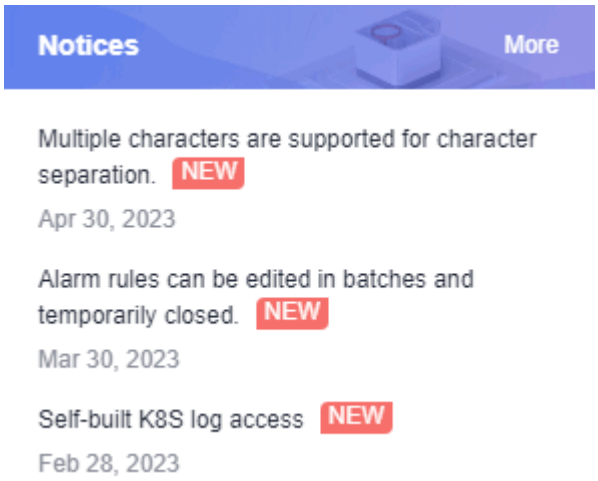
Notices

This area provides descriptions of new functions and displays the news of LTS.

To view more function descriptions, click **More**.

NOTE

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



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. **My Favorites (Local Cache)** is displayed for all accounts.

  NOTE

  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.

You can customize a list of your favorite log streams for quickly locating frequently used log streams.

For example, to add a log stream of the log group **lts-test** to favorites, perform the following steps:

Step 1 Log in to the LTS console.

Step 2 In the **Log Groups** list, click next to the log group name **lts-test**.

Step 3 Click on the right of the log stream. On the displayed **Edit** tab page, select a mode and click **OK**.

NOTE

You can remove a favorite in either of the following ways:

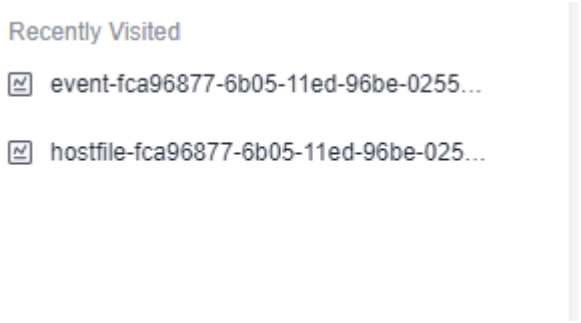
- In the log stream list, click in the row containing a log stream.
- In the **My Favorites** area, hover the cursor over a log stream and click .

----End

Recently Visited

This area displays the log streams that are recently visited.

Figure 1-4 Recently Visited



NOTE

A maximum of three log streams can be displayed in **Recently Visited**.

FAQ

This area displays frequently asked questions.

1.2 Resource Statistics

Log resource statistics are classified into read/write traffic, index traffic, log volume, and raw log traffic. The statistics are for reference only. You can also visualize log resource statistics in charts.

- **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.
- **Indexing**: Raw logs are full-text indexed by default for log search. Index creation will generate fees.
- **Log**: 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

Resource Statistics

Resource statistics display log resource data. By default, log resource data of one week (from now) is displayed. You can select a time range as required.

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

NOTE

- **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.

- The read and write traffic and index traffic data in the selected time range is displayed.
- Day-on-day changes in the selected time range are displayed. You can view the trend.
- The traffic trend chart based on the selected time range is displayed. Each point in the trend chart indicates the data statistics in a certain period. The unit is KB, MB, or GB. The statistics are collected based on site requirements.

Resource Statistics Details

Resource statistics details display the top 100 log groups or log streams by read/write traffic, index traffic, and latest log volume. By default, the log groups or log streams are sorted by the latest log volume (GB). You can also sort the statistics by read/write or index traffic.

- 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 target log groups and log streams.

  NOTE

  The downloaded resource statistics of the target log groups and log streams files are in **.CSV** format.

- You can select a time range to collect statistics on resource details.

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

  NOTE

  - **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.

- The daily log volume (GB), daily index traffic (GB), and daily read/write traffic (GB) are displayed based on the selected time range.

  There are two display modes:

  – Table

  – Bar chart

1.3 Log Groups

A log group is a group of log streams. Up to 100 log groups can be created for a single account.

Prerequisites

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

Creating a Log Group

1. Log in to the LTS console. On the **Log Management** page, click **Create Log Group**.
2. In the dialog box displayed, enter a log group name.

   NOTE

   - Collected logs are sent to the log group. 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.
   - The log name can contain 1 to 64 characters, including only letters, digits, hyphens (-), underscores (_), and periods (.). It cannot start with a period or underscore or end with a period.
3. Set **Log Retention Duration**. You can set it to 1 to 30 days.
4. Enter remarks. The value contains 0 to 1024 characters.
5. Click **OK**.

   – In the log group list, you can view information such as the log group name, tags, and log streams.

   – Click the log group name, the details page of one of its log streams is displayed.

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

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. Deleted log groups cannot be recovered. Exercise caution when performing the deletion.

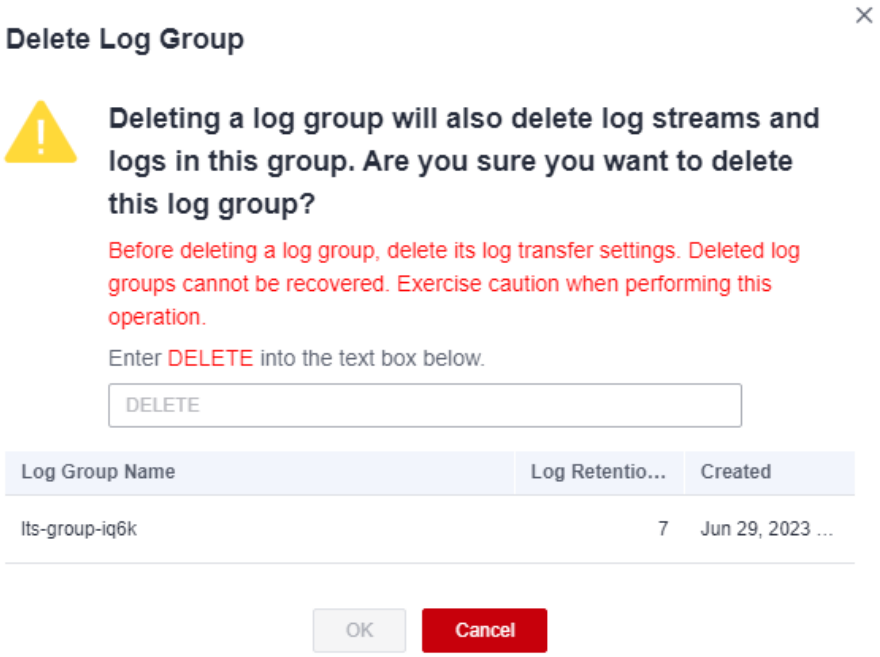
NOTE

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

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

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

Figure 1-5 Deleting a log group



Searching Log Groups/Streams

In the log group list, click the search box and set the following filter criteria:

- Log group/stream
- Log group name/ID
- Log stream name/ID
- Log group tag
- Remarks

1.4 Log Streams

A log stream is the basic unit for reading and writing logs. Sorting logs into different log streams makes it easier to find specific logs when you need them.

Up to 100 log streams can be created in a log group. The upper limit cannot be increased. If you cannot create a log stream because the upper limit is reached, you are advised to delete log streams that are no longer needed and try again, or create log streams in a new log group.

Prerequisites

You have created a log group.

Creating a Log Stream

1. On the LTS console, click on the left of a log group name.
2. Click **Create Log Stream** in the upper left corner of the displayed page, and enter a log stream name. After a log stream is created, its name cannot be changed. A log stream name:
   - Can contain only letters, digits, underscores (_), hyphens (-), and periods (.). The prefix cannot start with a period or underscore, or end with a period.
   - Can contain 1 to 64 characters.

   NOTE

   Collected logs are sent to the created log stream. If there are a large number of logs, you can create multiple log streams and name them for quick log search.
3. Select an enterprise project. You can click **View Enterprise Projects** to view all enterprise projects.
4. Set the tag value in the *Key* = *Value* format, for example, a=b. For details, see **Tag Management**.
5. Enter remarks. The value contains 0 to 1024 characters.
6. Click **OK**. In the log stream list, you can view information such as the log stream name and operations.

Deleting a Log Stream

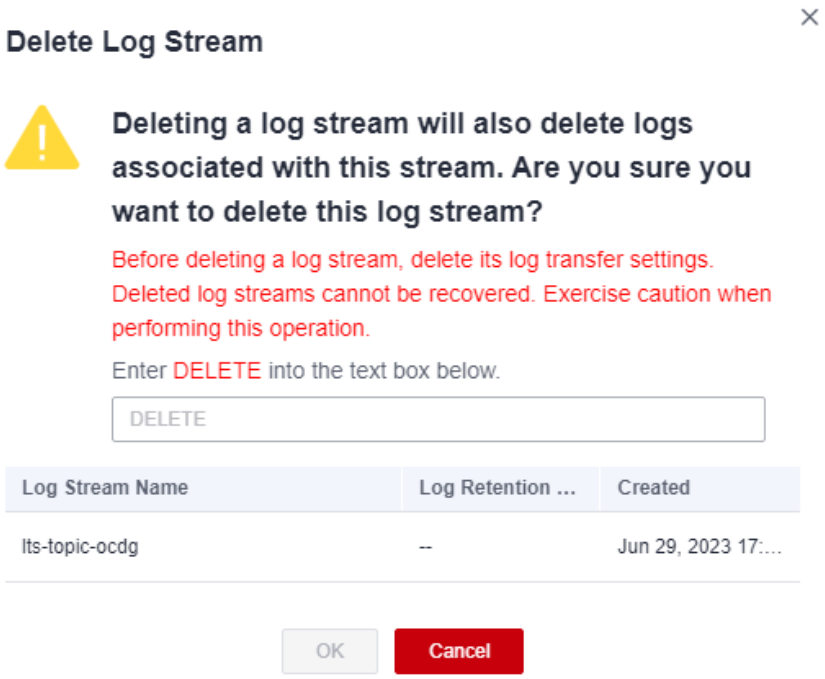
You can delete a log stream that is no longer needed. Deleting a log stream will also delete the log data in the log stream. Deleted log streams cannot be recovered. Exercise caution when performing the deletion.

NOTE

- 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.

1. In the log stream list, locate the target log stream and click in the **Operation** column.
2. Enter **DELETE** and click **OK**.

Figure 1-6 Deleting a log stream



Other Operations

- Adding a log stream to favorites

  Click ☆ in the **Operation** column of a log stream to add the log stream to favorites. The log stream is then displayed in **My Favorites**/**My Favorites (Local Cache)** on **the console home page**.

- **Details**

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

1.5 Tag Management

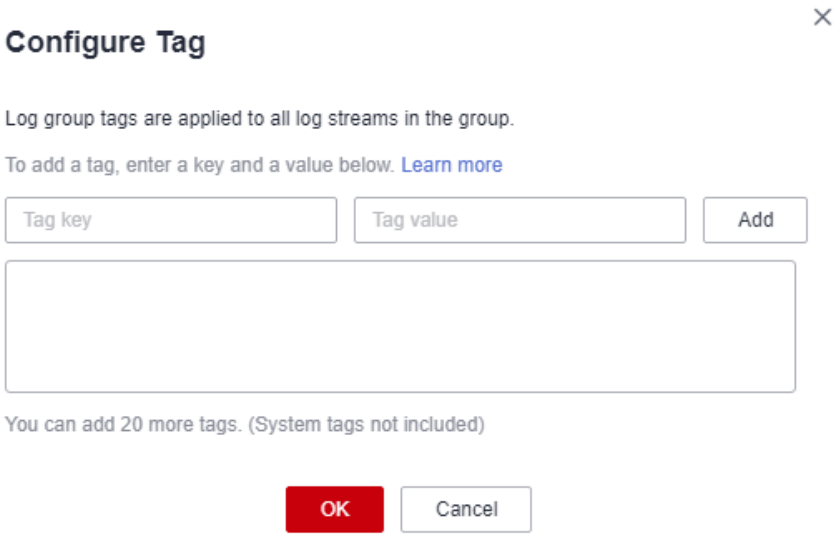
You can tag log groups, log streams, host groups, and log ingestion configurations.

Tagging a Log Group

You can add, delete, modify, and view tags on the log group list page. Tags of a log group are synchronized to all log streams in the log group.

1. Log in to the LTS console, and choose **Log Management** in the navigation pane on the left.
2. Move the cursor to the **Tag** column of the target log group and click ✎.
3. In the **Configure Tag** dialog box displayed, enter a tag key and value, and click **Add**. The entered key and value are then displayed in the *Key* = *Value* format in the text box.

Figure 1-7 Tag management



NOTE

- To add multiple tags, repeat this step.
- To delete a tag, click next to the tag in the text 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**.

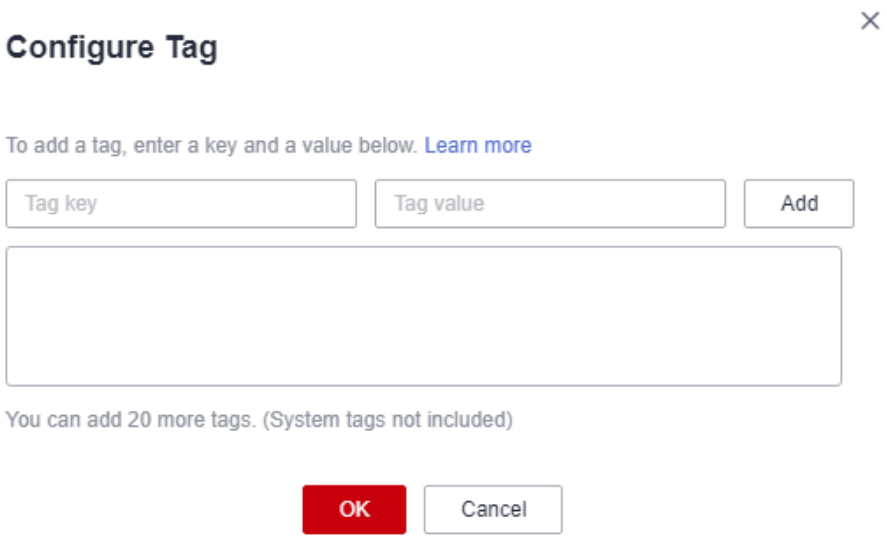
   On the **Log Management** page, you can view the added tags in the **Tags** column of the log group.

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. Log in to the LTS console, and choose **Log Management** in the navigation pane on the left.
2. Click before the name of the target log group.
3. Move the cursor to the **Tag** column of the target log stream and click .
4. In the **Configure Tag** dialog box displayed, enter a tag key and value, and click **Add**. The entered key and value are then displayed in the *Key* = *Value* format in the text box.

Figure 1-8 Tag management



NOTE

- To add multiple tags, repeat this step.
- To delete a tag, click next to the tag in the text 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.

5. 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 on the host group list page. When you manage the tags of a single host group, the changes will not be synchronized to other groups.

1. Log in to the LTS console, and choose **Host Management** in the navigation pane on the left.
2. On the **Host Groups** tab, click in the **Operation** column of a host group.
3. In the **Configure Tag** dialog box displayed, enter a tag key and value, and click **Add**. The entered key and value are then displayed in the *Key* = *Value* format in the text box.

NOTE

- To add multiple tags, repeat this step.
- To delete a tag, click next to the tag in the text 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**.

   On the **Host Management** page, 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 on the log ingestion page. When you manage the tags of a single log ingestion configuration, the changes will not be synchronized to other configurations.

1. Log in to the LTS console, and choose **Log Ingestion** in the navigation pane on the left.
2. Click in the **Operation** column of a log ingestion configuration.
3. In the **Configure Tag** dialog box displayed, enter a tag key and value, and click **Add**. The entered key and value are then displayed in the *Key* = *Value* format in the text box.

   NOTE

   - To add multiple tags, repeat this step.
   - To delete a tag, click next to the tag in the text 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**.

   On the **Log Ingestion** page, you can view the added tags in the **Tags** column of the log ingestion configuration.

2 Log Ingestion

2.1 Collecting Logs from Cloud Services

2.1.1 Collecting Logs from AOM

LTS can collect logs from Application Operations Management (AOM). For details, see **Accessing LTS**.

NOTE

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

2.1.2 Collecting Logs from API Gateway

LTS can collect logs from APIG.

NOTE

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

Prerequisites

You have purchased and used an API gateway.

Procedure

Perform the following operations to configure APIG log ingestion:

Step 1 Log in to the LTS console.

Step 2 In the left navigation pane, choose **Log Ingestion**. On the displayed page, click **APIG (API Gateway)**.

Step 3 Select a log stream.

1. 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.

2. 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.
3. Click **Next: Configure APIG**.

Step 4 Configure APIG.

Click **Configure APIG**.

1. On the APIG console, choose **Monitoring & Analysis** > **Log Analysis**.
2. Click **Configure Log Collection**.
3. Enable log collection, and select a log group and stream.

Step 5 Click **Next: Configure Log Stream**.

Table 2-1 Log stream parameters

Parameter	Description
Auto Structure and Index	If  is enabled, the log stream is automatically structured and indexed. The structuring is based on the APIG template, and the indexing enables quick analysis for all parsed APIG fields.

Step 6 Click **Submit**.

----End

2.1.3 Collecting Logs from BMS

LTS can collect logs from BMS. For details, see **Collecting Logs from ECS**.

NOTE

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

2.1.4 Collecting Logs from CBH

LTS can collect logs from CBH. For details, see **Configuring LTS**.

2.1.5 Collecting Logs from CCE

LTS can collect logs from Cloud Container Engine (CCE).

Prerequisites

- ICAgent has been installed in the CCE cluster and a host group with custom identifiers has been created for related nodes. If ICAgent has not been installed, upgrade it on the **Host Management** page. For details, see **Upgrading ICAgent**.
- You have **disabled** **Output to AOM**.

Restrictions

- Currently, ServiceStage hosting is not supported.
- CCE cluster nodes whose container engine is Docker are supported. For details, see **Node Overview**
- 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.
- Restrictions 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.

Procedure

Perform the following operations to configure CCE log ingestion:

Step 1 Log in to the LTS console.

Step 2 In the left navigation pane, choose **Log Ingestion**. On the displayed page, click **CCE (Cloud Container Engine)**.

Step 3 Select a log stream.

Choose between **Custom log stream** and **Fixed log stream** to suite your requirements.

Custom log stream

1. Select a cluster from the **CCE Cluster** drop-down list.
2. 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.
3. 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.
4. Click **Next: Check Dependencies**.

Fixed log stream

Logs will be collected to a fixed log stream. The default log streams of CCE clusters: **stdout-***{ClusterID}* for standard output/errors, **hostfile-***{ClusterID}* for node files, 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, 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.

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

2. 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**.

   NOTE

   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.

3. Click **Next: Check Dependencies**.

Step 4 Check dependencies.

The system automatically checks whether the following items meet the requirements:

1. ICAgent has been installed (version 5.12.130 or later).
2. There is a host group with the same name and custom identifier **k8s-log-***ClusterID*.
3. There is a log group named **k8s-log-***ClusterID*.
4. There is a recommended log stream. 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**.

NOTE

- **Auto Correct**: Check the previous settings with one click.
- **Check Again**: Recheck dependencies.
- If **Custom log stream** is selected, the check item **There is a log group named k8s-log-*ClusterID*** is optional. Use the switch to enable or disable the check item.

Step 5 (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 **Creating a Host Group (Custom Identifier)**.

   NOTE

   - The host group to which the cluster belongs is selected by default. You can also select host groups as required.
   - You can also deselect the host group. In this case, the collection configuration does not take effect. You are advised to select a host group during the first ingestion. You can skip this step and configure host groups after the ingestion configuration is complete. There are two options to do this:
     - On the LTS console, choose **Host Management** > **Host Groups** and associate host groups with ingestion configurations.
     - On the LTS console, choose **Log Ingestion** in the navigation pane on the left and click an ingestion configuration. On the displayed page, add one or more host groups for association.

2. Click **Next: Configure Collection**.

Step 6 Configure the collection.

Specify collection rules. For details, see **Configuring the Collection**.

Step 7 (Optional) Configure log structuring.

For details, see **Cloud Structuring Parsing**.

NOTE

If the selected log stream has been structured, exercise caution when deleting it.

Step 8 (Optional) Configure indexes.

For details, see **Index Settings**.

NOTE

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

Step 9 Click **Submit**.

----End

Configuring the Collection

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

1. **Basic Information**: Enter a name containing 1 to 64 characters. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed. The name cannot start with a period or underscore, or end with a period.
2. **Data Source**: Select a data source type and configure it.
   - **Container standard output**: Collects stderr and stdout logs of a specified container in the cluster.

     NOTE

     - The standard output of the matched container is collected to the specified log stream. Standard output to AOM stops.
     - The container standard output must be unique to a host.
   - **Container file**: Collects file logs of a specified container in the cluster.
   - **Node file**: Collects files of a specified node in the cluster.

     NOTE

     You cannot add the same host path to more than one log stream.

Table 2-2 Collection configuration parameters

Parameter	Description
Container standard output	Collects container standard output to AOM, and collects stderr and stdout logs of a specified container in the cluster. Collecting container standard output to AOM: ICAgent is installed on hosts in the cluster by default, and logs is collected to AOM. The function of collecting container standard output to AOM is enabled. Disable this function to collect stdout streams to LTS. Either **Container Standard Output (stdout)** or **Container Standard Error (stderr)** must be enabled.
Container file	• **Collection Paths**: LTS collects logs from the specified paths. **NOTE** • 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. • You cannot add the same host path to more than one log stream. • **Set Collection Filters**: Blacklisted directories or files will not be collected. If you specify a directory, all files in the directory are filtered out.
Node file	• **Collection Paths**: LTS collects logs from the specified paths. **NOTE** You cannot add the same host path to more than one log stream. • **Set Collection Filters**: Blacklisted directories or files will not be collected. If you specify a directory, all files in the directory are filtered out.

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

Table 2-3 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. **NOTE** 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. **NOTE** LTS will collect logs of the pods with names matching this expression. To collect logs of all pods, leave this field empty.

Parameter	Description
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. **NOTE** LTS will collect logs of the containers with names matching this expression. To collect logs of all containers, leave this field empty.
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. **NOTE** LTS will match all containers with a container label containing either a **Label Key** with an empty corresponding **Label Value**, or a **Label Key** with its corresponding **Label Value**.
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. **NOTE** LTS will exclude all containers with a container label containing either a **Label Key** with an empty corresponding **Label Value**, or a **Label Key** with its corresponding **Label Value**.
Container Label	After the **Container Label** is set, LTS adds related fields to logs. **NOTE** 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. **NOTE** LTS will match all containers with environment variables containing either an **Environment Variable Key** with an empty corresponding **Environment Variable Value**, or an **Environment Variable Key** with its corresponding **Environment Variable Value**. The relationship between multiple whitelists is based on an OR operation, meaning that a container environment variable can be matched as long as it meets any of key-value pairs.

Parameter	Description
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. **NOTE** LTS will exclude all containers with environment variables containing either an **Environment Variable Key** with an empty corresponding **Environment Variable Value**, or an **Environment Variable Key** with its corresponding **Environment Variable Value**. The relationship between multiple blacklists is based on an OR operation, meaning that a container environment variable can be excluded as long as it meets any of key-value pairs.
Environment Variable Label	After the environment variable label is set, the log service adds related fields to the log. **NOTE** 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. Perform other configurations.

Table 2-4 Other configurations

Parameter	Description
Split Logs	LTS supports log splitting, which is disabled by default. If this option is enabled, a single-line log larger than 500 KB will be split into multiple lines for collection. For example, a line of 600 KB log will be split into two lines for collection, the first line 500 KB and the second line 100 KB. If this option is disabled, a log larger than 500 KB will be truncated.
Collect Binary Files	LTS supports binary file collection, which is disabled by default. 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.

5. Configure the log format and log time.

Table 2-5 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. **NOTE** • 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**. **NOTE** 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
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**.

NOTE

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**.

2.1.6 Collecting Logs from CFW

LTS can collect logs from CFW. For details, see **Log Settings**.

NOTE

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

2.1.7 Collecting Logs from CTS

LTS can collect logs from CTS.

NOTE

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

Procedure

Perform the following operations to configure CTS log ingestion:

Step 1 Log in to the LTS console.

Step 2 In the navigation pane on the left, choose **Log Ingestion** and and click **CTS (Cloud Trace Service)**.

Step 3 Select a log stream.

1. 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.
2. 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.
3. Click **Next: Configure CTS**.

Step 4 Configure CTS.

Click **Configure CTS**.

1. On the CTS console, choose **Tracker List** in the navigation pane on the left.
2. Click **Create Tracker** and configure parameters.
3. Click **Create**.

Step 5 Click **Next: Configure Log Stream**.

Table 2-6 Log stream parameters

Parameter	Description
Auto Structure and Index	If  is enabled, the log stream is automatically structured and indexed. The structuring is based on the CTS template, and the indexing enables quick analysis for all parsed CTS fields.

Step 6 Click **Submit**.

----End

2.1.8 Collecting Logs from DWS

LTS can collect logs from GaussDB(DWS). For details, see **Cluster Log Management**.

NOTE

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

2.1.9 Collecting Logs from ECS

ICAgent collects logs from hosts based on your specified collection rules, and packages and sends the collected log data to LTS on a log stream basis. You can view logs on the LTS console in real time.

Prerequisites

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

Procedure

Perform the following operations to configure ECS log ingestion:

Step 1 Log in to the LTS console.

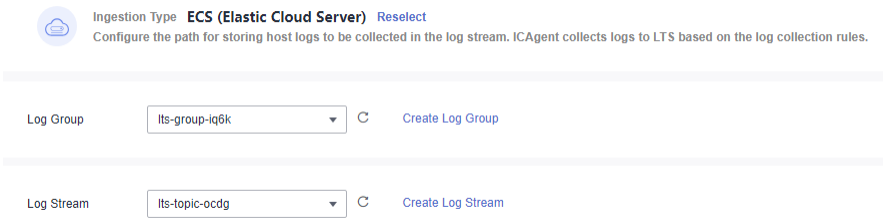
Step 2 In the left navigation pane, choose **Log Ingestion**. On the displayed page, click **ECS (Elastic Cloud Server)**.

Step 3 Select a log group.

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**.

Figure 2-1 Selecting a log stream



Step 4 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 **Creating a Host Group (IP Address)**.

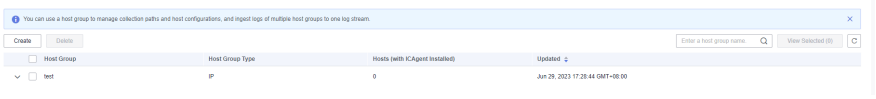
   NOTE

   You can also deselect the host group. In this case, the collection configuration does not take effect. You are advised to select a host group during the first ingestion. You can skip this step and configure host groups after the ingestion configuration is complete. There are two options to do this:

   - On the LTS console, choose **Host Management** > **Host Groups** and associate host groups with ingestion configurations.
   - On the LTS console, choose **Log Ingestion** in the navigation pane on the left and click an ingestion configuration. On the displayed page, add one or more host groups for association.

2. Click **Next: Configure Collection**.

Figure 2-2 Selecting a host group



Step 5 Configure the collection.

Specify collection rules. For details, see **Configurations**.

Step 6 (Optional) Configure log structuring.

For details, see **Cloud Structuring Parsing**.

NOTE

If the selected log stream has been structured, exercise caution when deleting it.

Step 7 (Optional) Configure indexes.

For details, see **Index Settings**.

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

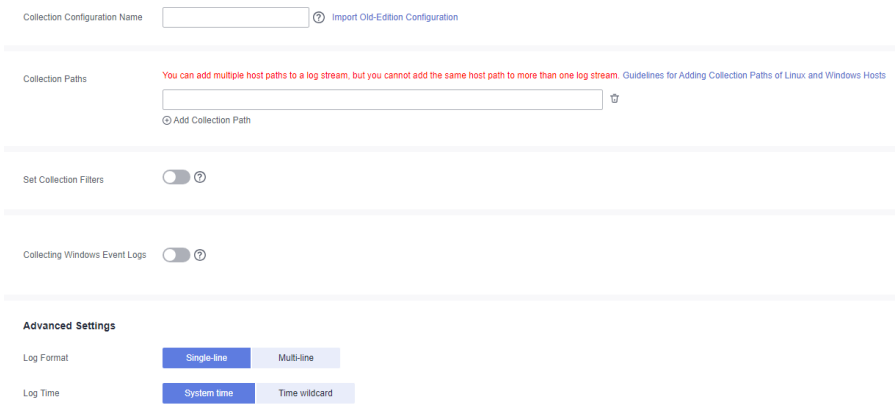
Step 8 Click **Submit**. After the ingestion is successful, click **Back to Ingestion Configurations** to **check the ingestion details**. You can also click **View Log Stream** to view the log stream to which logs are ingested.

----End

Configurations

When you configure host log ingestion, the collection configuration details are as follows.

Figure 2-3 Configuring the collection



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

   > **NOTE**
   >
   > **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. If you need the host log path in the old configuration, import the old configuration or create one.

2. **Collection Paths**: Add one or more host paths. LTS will collect logs from these paths.
   - Logs can be collected recursively. A double asterisk (**) can represent up to 5 directory levels in a path.

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

     ```
     /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
     ```


NOTE

- **/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.

NOTE

If a log collection path is similar to **C:\windows\system32** but logs cannot be collected, enable the 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 directory (such as **/var/logs/**), only **.log**, **.trace**, and **.out** files in the directory are collected.

If the collection path is set to a file name, the corresponding file is collected. Only text files can be collected. To query the file format, run **file -i** *File name*.

NOTE

- Ensure that sensitive information is not collected.
- It only collects logs of ECS (host) instances.
- A collection path can be configured only once. It means that a path of a host cannot be added for different log streams. Otherwise, log collection may be abnormal.
- If a collection path of a host has been configured in AOM, do not configure the path in LTS. If a path is configured in both AOM and LTS, only the path that is configured later takes effect.
- If log files were last modified more than 12 hours earlier than the time when the path is added, the files are not collected.

3. **Collection Blacklist**: Blacklisted directories or files will not be collected. 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.

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

NOTE

- 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.

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

Table 2-7 Parameters for collecting windows event logs

Parameter	Description
Log Type	Log types include **System**, **Application**, **Security**, and **Startup**.
First Collection Time Offset	Example: Set this parameter to **7** to collect logs generated within the 7 days before the collection start time. This offset takes effect only for the first collection to ensure that the logs are not repeatedly collected. Max: 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.

5. Configure the log format and log time.

Table 2-8 Log collection configurations

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. **NOTE** • 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.

Parameter	Description
	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**. **NOTE** 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.
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**.

NOTE

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**.

Checking Ingestion Configurations

On the LTS console, choose **Log Ingestion** in the navigation pane. Alternatively, access the **Log Ingestion** page by clicking **Back to Ingestion Configurations** when you finish configuring log ingestion.

- All ingestion configurations are displayed on the **Log Ingestion** page. Click an ingestion configuration to view its details.
- Click the name of the log group or log stream on the row that contains an ingestion configuration to check the log group or log stream details.
- The **Operation** column in the ingestion configuration list provides buttons for you to modify, delete, and manage tags.

2.1.10 Collecting Logs from ELB

LTS can collect logs from ELB.

NOTE

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

Prerequisites

You have created and used a load balancer.

Restrictions

ELB access logs only record requests sent to layer 7 dedicated and shared load balancers. Layer 4 shared load balancing is not logged.

Procedure

Perform the following operations to configure ELB log ingestion:

Step 1 Log in to the LTS console.

Step 2 In the left navigation pane, choose **Log Ingestion**. On the displayed page, click **ELB (Elastic Load Balance)**.

Step 3 Select a log stream.

1. 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.
2. 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.
3. Click **Next: Configure ELB**.

Step 4 Configure ELB.

Click **Configure ELB**.

1. On the network console, choose **Elastic Load Balance**.
2. On the **Elastic Load Balance** page, click the name/ID of the target load balancer to go to the details page.
3. Click the **Access Logs** tab and click **Configure Access Logging**.
4. Enable log collection, and select a log group and stream.

Step 5 Configure a log stream.

Table 2-9 Log stream parameters

Parameter	Description
Auto Structure and Index	If this option is enabled, the log stream is automatically structured and indexed. The structuring is based on the ELB template, and the indexing enables quick analysis for all parsed ELB fields.

Step 6 The operation is complete.

----End

2.1.11 Collecting Logs from ER

LTS can collect logs from Enterprise Router (ER). For details, see **Creating a Flow Log**.

NOTE

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

Structuring Template Details

- ER log example

Table 2-10 Structuring template example

Template Name	Example Log
ER Enterprise Router	1 0ebc7f641d80f4d32f9dc0056bdaae5b 740cc7e2-c686-496e-9fae-2dfc33e9d443 2756dc58-49be-413d-852f-accc5657a6c3 192.168.3.227 172.16.0.206 0 0 1 279 27342 1670338595 1670339195 egress

- Structuring fields and description

Table 2-11 Structuring fields

Field	Example	Description	Type
version	1	ER flow log version.	long
project_id	0ebc7f641d80f4d32f9dc0056bdaae5b	Project ID.	string
instance_id	740cc7e2-c686-496e-9fae-2dfc33e9d443	Enterprise router ID.	string

Field	Example	Description	Type
resource_id	2756dc58-49be-413d-852f-accc5657a6c3	ID of the attachment that the traffic is generated for.	string
srcaddr	192.168.3.227	Source IP address.	string
dstaddr	172.16.0.206	Destination IP address.	string
srcport	0	Source port.	long
dstport	0	Destination port.	long
protocol	1	Internet Assigned Numbers Authority (IANA) protocol number of the traffic. For more information, see **Assigned Internet Protocol Numbers**.	long
packets	279	Number of data packets during the flow log capture.	long
bytes	27342	Size of the data packet during the flow log capture.	long
start	1670338595	The time when the capture started, in Unix seconds.	long
end	1670339195	The time when the capture ended, in Unix seconds.	long
direct	egress	Traffic direction: • **ingress**: traffic going in to the attachment. • **egress**: traffic going out of the attachment.	string

2.1.12 Collecting Logs from FunctionGraph

LTS can collect logs from FunctionGraph. For details, see **Managing Function Logs**.

NOTE

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

2.1.13 Collecting Logs from SMN

LTS can collect logs from Simple Message Notification (SMN). For details, see **Logs**.

NOTE

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

Structuring Template Details

- Log example

Table 2-12 Structuring template example

Template Name	Example Log
SMN	{"message_id":"1ae49922602a42fc83acb9689a2eb5f4","project_id":"5a9f32e4f1ec4bbe9695ff9da51c2925","topic_urn":"urn:smn:cn-north-1:5a9f32e4f1ec4bbe9695ff9da51c2925:demo","subscriber_urn":"urn:smn:cn-north-1:5a9f32e4f1ec4bbe9695ff9da51c2925:demo:b55c3c6fa7cd471b9f24818d530a8740","protocol_name":"https","endpoint":"https://127.0.0.1:443/https","status":"DELIVERED","http_code":200,"create_time":"2022-11-01T00:00:00Z","send_time":"2022-11-01T00:00:10Z"}

- Structuring fields and description

Table 2-13 Structuring fields

Field	Example	Description	Type
message_id	1ae49922602a42fc83acb9689a2eb5f4	Message ID.	string
project_id	5a9f32e4f1ec4bbe9695ff9da51c2925	Project ID.	string
topic_urn	urn:smn:cn-north-1:5a9f32e4f1ec4bbe9695ff9da51c2925:demo	Resource identifier of a topic, which is unique.	string
subscriber_urn	urn:smn:cn-north-1:5a9f32e4f1ec4bbe9695ff9da51c2925:demo:b55c3c6fa7cd471b9f24818d530a8740	Resource identifier of a subscription, which is unique.	string

Field	Example	Description	Type
protocol_name	https	Subscription protocol. (Different protocols indicate different types of endpoints to receive messages.) The following protocols are supported: **email**: The endpoints are email addresses. **sms**: The endpoints are phone numbers. **functiongraph**: FunctionGraph (function) transmission protocol. The endpoint is a function. **functionstage**: FunctionStage (workflow) transmission protocol. The endpoint is a function workflow. **http** and **https**: The endpoints are URLs.	string
endpoint	https://127.0.0.1:443/https	Message receiving endpoint.	string
status	DELIVERED	Message status. The options are as follows: **DELIVERED**: The message has been delivered. **FAIL_DELIVERED**: The message fails to be sent. **REJECTS**: The message has been rejected. The flow control mechanism is triggered.	string
http_code	200	HTTP return code. Only HTTP/HTTPS messages are supported.	long

Field	Example	Description	Type
create_time	2022-11-01T00:00:00Z	Time when a message is created. The UTC time is in *YYYY-MM-DDTHH:MM:SSZ* format.	string
send_time	2022-11-01T00:00:10Z	Time when a message is sent. The UTC time is in *YYYY-MM-DDTHH:MM:SSZ* format.	string

2.1.14 Collecting Logs from SecMaster

LTS can collect logs from SecMaster. For details, see **Creating a Data Delivery**.

NOTE

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

2.1.15 Collecting Logs from VPC

LTS can collect logs from VPC.

NOTE

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

Procedure

Perform the following operations to configure VPC log ingestion:

Step 1 Log in to the LTS console.

Step 2 In the navigation pane on the left, choose **Log Ingestion** and and click **VPC (Virtual Private Cloud)**.

Step 3 Select a log stream.

1. 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.
2. 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.
3. Click **Next: Configure VPC**.

Step 4 Configure VPC.

Click **Configure VPC**.

1. On the VPC console, choose **VPC Flow Logs**.

2. On the **VPC Flow Logs** page, click **Create VPC Flow Log** and configure parameters.
3. Click **OK**.

Step 5 Click **Next: Configure Log Stream**.

Table 2-14 Log stream parameters

Parameter	Description
Auto Structure and Index	If  is enabled, the log stream is automatically structured and indexed. The structuring is based on the VPC template, and the indexing enables quick analysis for all parsed VPC fields.

Step 6 Click **Submit**.

----End

2.1.16 Collecting Logs from WAF

LTS can collect logs from Web Application Firewall (WAF). For details, see

NOTE

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

2.2 Collecting Logs Using APIs

2.2.1 Collecting Logs Using APIs

You can report logs to LTS with APIs in REST provided by LTS. There are two APIs: reporting logs and reporting high-precision logs.

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

Table 2-15 Scenarios

Name	Log Time	Example	Description

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.

NOTE

You can log in to the LTS console. In the navigation pane, choose **Host Management**, and click **Install ICAgent** to get the access IP address.

2.2.2 Reporting Logs

Function

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

To obtain the access IP address, log in to the LTS console, choose **Host Management** in the navigation pane, and click **Install ICAgent** in the upper right corner. The access IP address is contained in the ICAgent installation command. 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 2-16 URI parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain the project ID, see . No default value. Value length: 32 characters
log_group_id	Yes	String	Log group ID. For details about how to obtain the project ID, see . No default value. Value length: 36 characters
log_stream_id	Yes	String	Log stream ID. For details about how to obtain the project ID, see . No default value. Value length: 36 characters The write rate at most should not exceed 100 MB/s for a single log stream. Otherwise, logs may be lost.

Request Parameters

Table 2-17 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Indicates the user token obtained from IAM. No default value. Minimum length: 1000 characters Maximum length: 2000 characters
Content-Type	Yes	String	Set this parameter to **application/json;charset=UTF-8**. Default value: None Minimum length: 30 characters Maximum length: 30 characters

Table 2-18 Request body parameters

Parameter	Mandatory	Type	Description
log_time_ns	Yes	Long	Indicates the log collection time (UTC time in nanoseconds). **NOTE** The interval between the log collection time and current time must be less than the log retention duration. Otherwise, reported logs will be cleared. For example, if the log retention duration is seven days, the log collection time must be within the last seven days.
contents	Yes	Array of String	Indicates the log content.
labels	Yes	Object	Custom labels.
tenant_project_id	No	String	Tenant ID.

Response Parameters

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

Table 2-19 Response body parameters

Parameter	Type	Description
errorCode	String	Indicates the status code. Example value: ● SVCSTG.ALS.200.200
errorMessage	String	Indicates the response description. Example value: ● Report success.
result	String	Response result.

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

Table 2-20 Response body parameters

Parameter	Type	Description
errorCode	String	Indicates the error code. Example value: ● SVCSTG.ALS.200.201 ● SVCSTG.ALS.200.210
errorMessage	String	Indicates the error description. Example value: ● Request conditions must be json format. ● projectid xxx log's quota has full!!
result	String	Response result.

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

Table 2-21 Response body parameters

Parameter	Type	Description
errorCode	String	Indicates the error code. Example value: ● SVCSTG.ALS.403.105
errorMessage	String	Indicates the error description. Example value: ● Project id is invalid.
result	String	Response result.

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

Table 2-22 Response body parameters

Parameter	Type	Description
errorCode	String	Indicates the error code. Example value: • LTS.200500
errorMessage	String	Indicates the error description. Example value: • Internal error
result	String	Response result.

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

Table 2-23 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 Apri 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",
  "errorMessage": "Report success.",
  "result": null
}
```

Example response with status code **401**:

The authentication information is incorrect or invalid.

```
{
  "errorCode" : "SVCSTG.ALS.403.105",
  "errorMessage" : "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.

2.2.3 Reporting High-Precision Logs

Function

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

To obtain the access IP address, log in to the LTS console, choose **Host Management** in the navigation pane, and click **Install ICAgent** in the upper right corner. The access IP address is contained in the ICAgent installation command. 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.

NOTE

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 2-24 URI parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain the project ID, see . No default value. Value length: 32 characters
log_group_id	Yes	String	Log group ID. For details about how to obtain the project ID, see . No default value. Value length: 36 characters
log_stream_id	Yes	String	Log stream ID. For details about how to obtain the project ID, see . No default value. Value length: 36 characters The write rate at most should not exceed 100 MB/s for a single log stream. Otherwise, logs may be lost.

Request Parameters

Table 2-25 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Indicates the user token obtained from IAM. No default value. Minimum length: 1000 characters Maximum length: 2000 characters
Content-Type	Yes	String	Set this parameter to **application/json;charset=UTF-8**. Default value: None Minimum length: 30 characters Maximum length: 30 characters

Parameter	Mandatory	Type	Description
Content-Encoding	No	String	Log compression format. Enumerated values: • **GZIP** • **SNAPPY** • **gzip** • **snappy**

Table 2-26 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	Tenant ID.

Table 2-27 LogContents

Parameter	Mandatory	Type	Description
log_time_ns	Yes	Long	Indicates the log collection time (UTC time in nanoseconds). **NOTE** The interval between the log collection time and current time must be less than the log retention duration. Otherwise, reported logs will be cleared. For example, if the log retention duration is seven days, the log collection time must be within the last seven days.
log	Yes	String	Indicates the log content.

Response Parameters

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

Table 2-28 Response body parameters

Parameter	Type	Description
errorCode	String	Indicates the status code. Example value: ● SVCSTG.ALS.200.200
errorMessage	String	Indicates the response description. Example value: ● Report success.
result	String	Response result.

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

Table 2-29 Response body parameters

Parameter	Type	Description
errorCode	String	Indicates the error code. Example value: ● SVCSTG.ALS.200.201 ● SVCSTG.ALS.200.210
errorMessage	String	Indicates the error description. Example value: ● Request conditions must be json format. ● projectid xxx log's quota has full!!
result	String	Response result.

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

Table 2-30 Response body parameters

Parameter	Type	Description
errorCode	String	Indicates the error code. Example value: ● SVCSTG.ALS.403.105
errorMessage	String	Indicates the error description. Example value: ● Project id is invalid.
result	String	Response result.

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

Table 2-31 Response body parameters

Parameter	Type	Description
errorCode	String	Indicates the error code. Example value: • LTS.200500
errorMessage	String	Indicates the error description. Example value: • Internal error
result	String	Response result.

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

Table 2-32 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 Apri 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",
```



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

Example response with status code **401**:

The authentication information is incorrect or invalid.

```
{
  "errorCode" : "SVCSTG.ALS.403.105",
  "errorMessage" : "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.

2.3 Other Ingestion Modes

2.3.1 Self-Built Kubernetes

LTS can inject self-built Kubernetes application logs.

NOTE

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

Prerequisites

- Ensure that the Helm v3 installation command has been executed in the Kubernetes cluster.
- Ensure that kubectl has been configured for the Kubernetes cluster.

Procedure

Set the log access mode to **Self-Built K8s - Application Logs**. If your Kubernetes cluster is in the cloud, perform the following steps to complete the access configuration.

Step 1 Log in to the LTS console.

Step 2 Choose **Log Ingestion** in the left navigation pane. On the page displayed, click **Self-Built Software** > **Self-Built K8s - Application Logs**.

Step 3 Select a log stream.

Choose between **Fixed log stream** and **Custom log stream** to suite your requirements. You are recommended to use **Fixed log stream**.

Fixed log stream

Logs will be collected to a fixed log stream. The default log streams of CCE clusters: **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.

1. Select **Fixed log stream** for **Collect**.
2. Enter the cluster name and ID.
3. Select a log group.

   NOTE

   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.**
4. Click **Next: Check Dependencies**.

Custom log stream

1. Select **Custom log stream**.
2. Enter the cluster name and ID.
3. 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.
4. 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.
5. Click **Next: Check Dependencies**.

Step 4 Check dependencies.

1. The system automatically checks whether the following are met:
   - There is a host group with the custom identifier **k8s-log-***ClusterID*.
   - There is a log group named **k8s-log-***ClusterID*. The log retention period and description of a log group can be modified.
   - The recommended log stream exists. The log retention period and description of a log stream can be modified. 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**.

NOTE

- **Auto Correct**: a one-click option to finish the previous settings.
- **Check Again**: Recheck dependencies.
- If **Custom log stream** is selected, the check item **There is a log group named k8s-log-*ClusterID*** is optional. Use the switch to turn on or off the check item.

2. Click **Next: Install ICAgent**.

Step 5 Install the log collection component.

In the Kubernetes cluster, perform the following steps on any host:

1. Obtain the ICAgent installation package.
   - Obtain the ICAgent installation package (based on your actual information).
     ```
     wget https://icagent-{regionId}.{obsDomainName}/ICAgent_linux/icagentK8s-5.5.1.2.tar.gz
     ```
   - Decompress the ICAgent installation package.
     ```
     tar -xzvf icagentK8s-5.5.1.2.tar.gz
     ```
   - Go to the directory
     ```
     cd icagentK8s
     ```
   - Generate installation commands

     Select the region of ingested logs.

     Select the project ID of the ingesting account.

     For **Kubernetes Cluster**, select **Intra-Cloud**.
2. Install ICAgent.
   a. Copy the ICAgent installation command.

      To prevent your AK/SK from being disclosed, disable historical record collection.

      The generated installation command is as follows (replace *x.x.x.x* with the actual IP address displayed on the page):

      ```
      set +o history; bash icagent_log_install.sh 2a473356cca5487f8373be891bffc1cf test-xx123456 region0_id {input_your_ak} {input_your_sk} x.x.x.x podlb
      ```

      To enter the AK/SK, either:

      1. Copy the command and replace *{input_your_ak}* and *{input_your_sk}* without the braces {}, or

      2. Run the copied command and enter the AK and SK when "Enter the AK" and "Enter the SK" are displayed.

   b. Use a remote login tool (such as PuTTY) to log in to the target host as the **root** user and run the copied command.

      If the message "ICAgent install success" is displayed, the installation is successful. Then choose **Host Management** in the navigation pane to check the ICAgent status.
3. Click **ICAgent Already Installed**.

Step 6 (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 **Creating a Host Group (Custom Identifier)**.

NOTE

- The host group to which the cluster belongs is selected by default. You can also select host groups as required.
- You can skip this step and configure host groups after the ingestion configuration is complete. There are two options to do this:
  - On the LTS console, choose **Host Management** > **Host Groups** and associate host groups with ingestion configurations.
  - On the LTS console, choose **Log Ingestion** in the navigation pane on the left and click an ingestion configuration. On the displayed page, add one or more host groups for association.

2. Click **Next: Configurations**.

Step 7 Configure the collection.

1. Specify collection rules. For details, see **Configurations**.
2. Click **Next: Log Structuring**.

Step 8 (Optional) Configure log structuring.

1. Click **Skip** or perform structuring configurations. For details, see **Cloud Structuring Parsing**.

   NOTE

   If the selected log stream has been structured, exercise caution when deleting it.

2. Click **Next: Index Settings**.

Step 9 (Optional) Configure indexes.

1. Click **Skip and Submit** or configure the index. For details, see **Index Settings**.
2. Click **Submit**

Step 10 The operation is complete.

----End

Configurations

When you configure log ingestion for self-built Kubernetes clusters, the collection configuration details are as follows.

1. **Basic Settings**: Enter a name containing 1 to 64 characters. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed. The name cannot start with a period or underscore, or end with a period.
2. **Data Source**: Select a data source type and configure it.
   - **Container standard output**: Collects stderr and stdout logs of a specified container in the cluster.

     NOTE

     - The standard output of the matched container is collected to the specified log stream. Standard output to AOM stops.
     - The container standard output must be unique to a host.

   - **Container file**: Collects file logs of a specified container in the cluster.

- **Node file**: Collects files of a specified node in the cluster.

  NOTE

  You cannot add the same host path to more than one log stream.

- **Kubernetes event**: Collects event logs in the Kubernetes cluster.

  NOTE

  Kubernetes events of a Kubernetes cluster can be ingested to only one log stream.

Table 2-33 Collection configuration parameters

Type	Description
Container standard output	Collects stderr and stdout logs of a specified container in the cluster. Either **Container Standard Output (stdout)** or **Container Standard Error (stderr)** must be enabled.
Container file	• **Collection Paths**: LTS collects logs from the specified paths. **NOTE** • 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. • You cannot add the same host path to more than one log stream. • **Set Collection Filters**: Blacklisted directories or files will not be collected. If you specify a directory, all files in the directory are filtered out.
Node file	• **Collection Paths**: LTS collects logs from the specified paths. **NOTE** You cannot add the same host path to more than one log stream. • **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	You do not need to configure this parameter. Only ICAgent 5.12.130 or later is supported.

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

   NOTE

   After entering a regular expression matching rule, click the button of verification to verify the regular expression.

Table 2-34 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. **NOTE** 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. **NOTE** 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. **NOTE** LTS will collect logs of the containers with names matching this expression. To collect logs of all containers, leave this field empty.
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. **NOTE** LTS will match all containers with a container label containing a specified **Label Key** with an empty corresponding **Label Value**. If **Label Value** is not empty, only containers with a container label containing a specified **Label Key** that is equal to its **Label Value** are matched with LTS. **Label Key** requires full matching while **Label Value** supports regular matching. The relationship between multiple whitelists is based on an OR operation, meaning that a container label can be matched as long as it meets any of the whitelists.
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. **NOTE** LTS will exclude all containers with a container label containing a specified **Label Key** with an empty corresponding **Label Value**. If **Label Value** is not empty, only containers with a container label containing 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. The relationship between multiple blacklists is based on an OR operation, meaning that a container label can be excluded as long as it meets any of the blacklists.

Parameter	Description
Container Label	After the **Container Label** is set, LTS adds related fields to logs. **NOTE** 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. **NOTE** LTS will match all containers with environment variables containing either an **Environment Variable Key** with an empty corresponding **Environment Variable Value**, or an **Environment Variable Key** with its corresponding **Environment Variable Value**. **Label Key** requires full matching while **Label Value** supports regular matching. The relationship between multiple whitelists is based on an OR operation, meaning that a container environment variable can be matched as long as it meets any of key-value pairs.
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. **NOTE** LTS will exclude all containers with environment variables containing either an **Environment Variable Key** with an empty corresponding **Environment Variable Value**, or an **Environment Variable Key** with its corresponding **Environment Variable Value**. **Label Key** requires full matching while **Label Value** supports regular matching. The relationship between multiple blacklists is based on an OR operation, meaning that a container environment variable can be excluded as long as it meets any of key-value pairs.
Environment Variable Label	After the environment variable label is set, the log service adds related fields to the log. **NOTE** 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. Perform other configurations.

Table 2-35 Other configurations

Parameter	Description
Split Logs	LTS supports log splitting, which is disabled by default. If this option is enabled, a single-line log larger than 500 KB will be split into multiple lines for collection. For example, a line of 600 KB log will be split into two lines for collection, the first line 500 KB and the second line 100 KB. If this option is disabled, a log larger than 500 KB will be truncated.
Collect Binary Files	LTS supports binary file collection, which is disabled by default. 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.

5. Configure the log format and log time.

Table 2-36 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. **NOTE** • 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.

Parameter	Description
	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**. **NOTE** 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.
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**.

NOTE

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**.

3 Host Management

3.1 Managing Host Groups

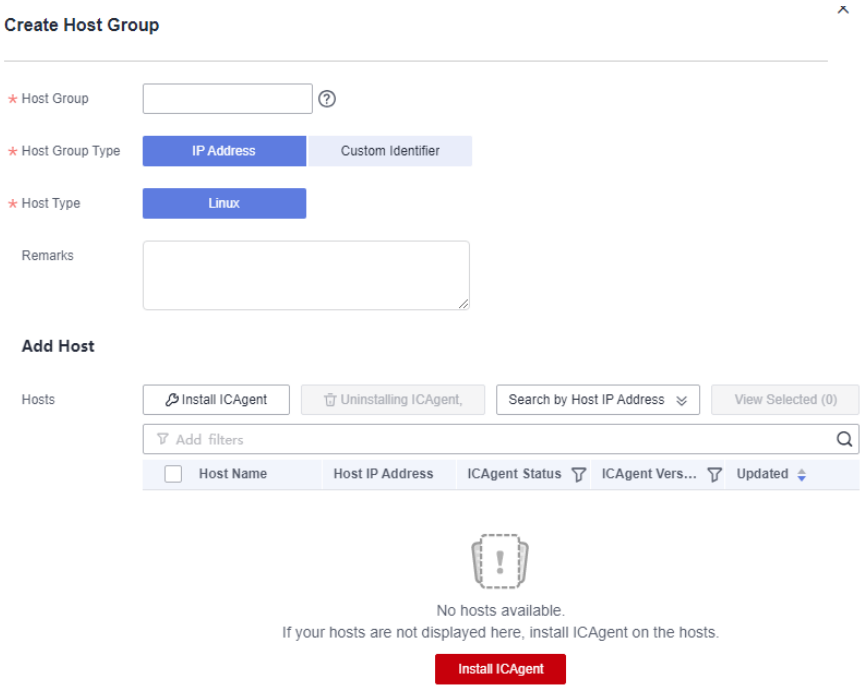
Host groups allow you to configure host log ingestion efficiently. You can sort multiple hosts to a host group and associate the host group with log ingestion configurations. The ingestion configurations will be applied to all the hosts in the host group, saving you the trouble of configuring the hosts individually.

- 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.

Creating a Host Group (IP Address)

1. Log in to the LTS console, and choose **Host Management** in the navigation pane on the left. On the displayed page, click **Create Host Group** in the upper right corner.
2. In the displayed slide-out panel, enter a host group name and select a host OS (Linux).

Figure 3-1 Creating an IP address host group



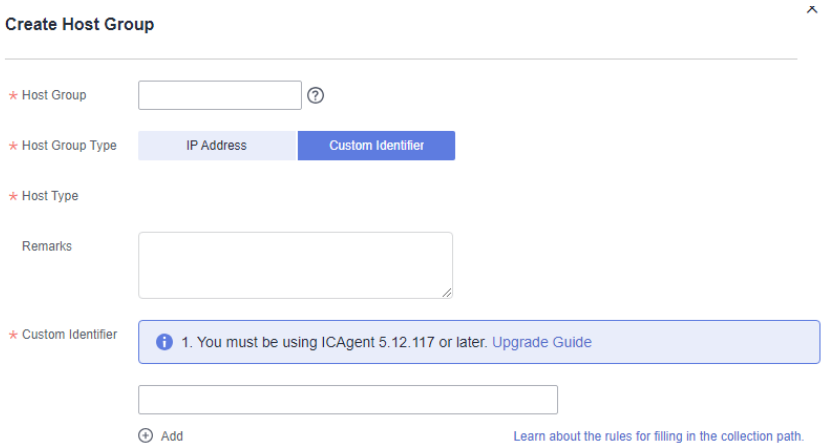
3. In the host list, select one or more hosts to add to the group and click **OK**.
   - You can filter hosts by host name or host IP address. You can also click 

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**.

Creating a Host Group (Custom Identifier)

1. On the **Host Management** page, click **Create Host Group** in the upper right corner.
2. On the displayed **Create Host Group** page, enter a host group name in the **Host Group** field and set **Host Group OS** to **Custom Identifier**.

Figure 3-2 Creating a custom identifier host group



NOTE

- A host group with a custom ID supports only Linux hosts.
- You can click **Learn about the rules for filling in the collection path** to learn how to configure paths.

3. Click Add to add a custom identifier.

   NOTE

   Up to 10 custom identifiers can be added.

4. Click **OK**.
5. Run the following commands to create the **custom_tag** file:
   a. Run the **cd /opt/cloud** command. In the **cloud** directory, run the **mkdir lts** command to create the **lts** directory.
   b. Run the **chmod 750 lts** command to modify the permission on the **lts** directory.
   c. Run the **touch custom_tag** command in the **lts** directory to create the **custom_tag** file.
   d. Run the **chmod 640 custom_tag;vi custom_tag** command to modify the **custom_tag** permission and open the file.
   e. Press **i** to enter the insert mode, enter a custom identifier, press **Esc**, enter **:wq!**, save the modification and exit.

NOTE

After 5, you can use either of the following methods to add hosts to a custom host group:

Method 1 (recommended):

Linux

In the **custom_tag** file of the **/opt/cloud/lts** directory on the host, view the host identifier and add it to the custom host group identifiers to add the host to the host group. For example, in the **custom_tag** file of the **/opt/cloud/lts** directory on the host, the identifier of the host is **test1**, and the custom identifier of the host group is **test1**. That is, the host is added to the host group.

Method 2:

Linux

- To add a host to a host group, add the custom host group identifier to the **custom_tag** file in the **/opt/cloud/lts** directory on the host. For example, if the custom identifier of the host group is **test**, enter **test** in the **custom_tag** file to add the host to the host group.
- If multiple custom identifiers are added, enter any custom identifier in the **custom_tag** file of the **/opt/cloud/lts** directory on the host to add the host to the host group.

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.

Table 3-1 Operations on host groups

Operation	Procedure
Changing a host group name	1. On the **Host Management** page, the **Host Groups** tab is displayed by default. 2. On the **Host Groups** tab page, click the modify button in the **Operation** column of the row containing 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**.

Operation	Procedure
Adding hosts to a host group	**Method 1:** 1. On the **Host Management** page, click the **Host Groups** tab, and click ⌄ in the row containing the target host group. 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. On the **Host Management** page, click the **Hosts** tab. 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. On the **Host Management** page, click the **Host Groups** tab, and 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**. **NOTE** This operation is not supported for hosts in the custom identifier host group.
Uninstalling ICAgent from a host	1. On the **Host Management** page, click the **Host Groups** tab, and 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. **NOTE** • 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.

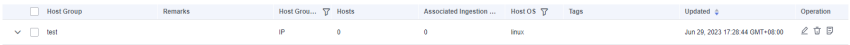
Operation	Procedure
Removing hosts from a host group	1. On the **Host Management** page, click the **Host Groups** tab, and click ⌄ in the row containing the target host group. 2. In the host list, select the target hosts and click the **Remove** button above the list. 3. Click **OK**.
Associating a host group with an ingestion configuration	1. On the **Host Management** page, click the **Host Groups** tab, and click ⌄ in the row containing the target host group. 2. Click the **Associated Ingestion Configuration** 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 Configuration** tab, click **Disassociate** in the **Operation** column of the row containing the target ingestion configuration. 2. Click **OK**.
Disassociating a host group from multiple ingestion configurations	1. On the **Associated Ingestion Configuration** tab, select the target ingestion configurations and click the **Disassociate** button above the list. 2. Click **OK**.

Deleting Host Groups

Deleting a single host group

1. On the **Host Management** page, the **Host Groups** tab is displayed by default.
2. On the **Host Groups** tab, click the deletion icon in the **Operation** column of the row containing the target host group.

   Figure 3-3 Deleting a host group

3. In the displayed dialog box, click **OK**.

Deleting host groups in batches

1. On the **Host Groups** tab, select multiple host groups to be deleted and click **Delete** above the list.
2. In the displayed dialog box, click **OK**.

3.2 Managing Hosts

3.2.1 Installing ICAgent (Cloud Hosts)

ICAgent is a log collection tool for LTS. To use LTS to collect logs from hosts, you need to install ICAgent on the hosts.

Prerequisites

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

Installation Methods

There are two methods to install ICAgent.

Table 3-2 Installation methods

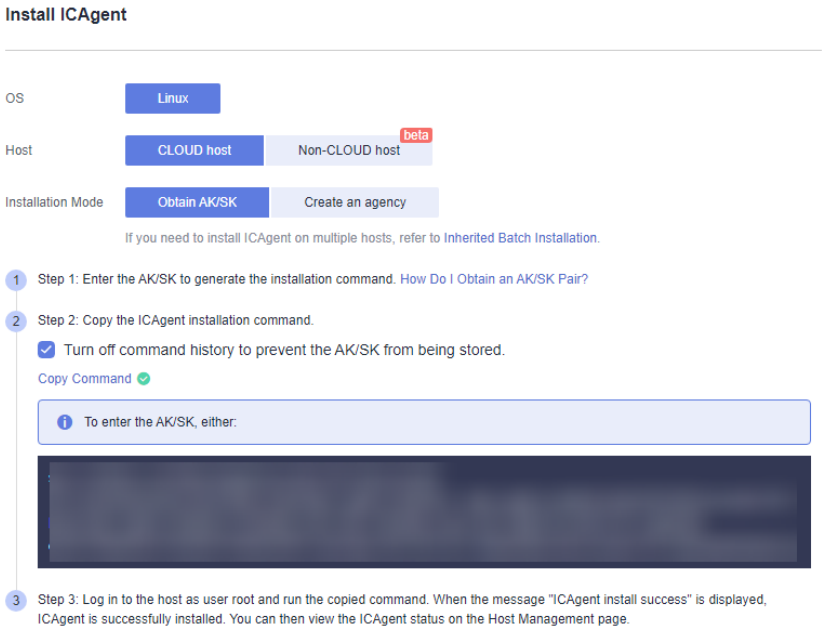
Method	Scenario
Initial installation	You can use this method to install ICAgent on a host that has no ICAgent installed.
Inherited installation (supported only for Linux hosts)	When ICAgent has already been installed on one host but needs to be installed on multiple hosts, you can use this method.

Initial Installation (Linux)

Step 1 Log in to the LTS console and choose **Host Management** in the navigation pane on the left.

Step 2 Click **Install ICAgent** in the upper right corner.

Figure 3-4 Installing ICAgent



Step 3 Set **OS** to **Linux**.

Step 4 Set **Host** to **CLOUD host**.

Step 5 Select an installation mode:

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

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

  NOTICE

  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.

- **Create an agency**. For details, see **How Do I Install ICAgent by Creating an Agency?**.

Step 6 Click **Copy Command** to copy the ICAgent installation command.

Step 7 Log in as user **root** to the host which is deployed in the region same as that you are logged in to (for example, 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 pair as prompted.

NOTE

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

----End

Inherited Installation (Linux)

Let's 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. You can follow the directions below 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 the message **ICAgent install success** is displayed, ICAgent has been installed in the **/opt/oss/servicemgr/** directory of the host. You can then view the ICAgent status by choosing **Host Management** in the navigation pane of the LTS console and then clicking **Hosts**.
   - If the installation fails, uninstall ICAgent and reinstall it. If the reinstallation fails, contact technical support.

Batch Inherited Installation (Linux)

Let's 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. You can follow the directions below to install ICAgent on other hosts in batches.

NOTICE

- The hosts must all belong to the same Virtual Private Cloud (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 and try again.

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, as shown in the following example:

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. You can then view the **ICAgent status** by choosing **Host Management** in the navigation pane of the LTS console and then clicking **Hosts**.

3.2.2 Installing ICAgent (Non-Huawei Cloud Hosts) (Non-Cloud 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.

Prerequisites

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

Restrictions

- Linux: ICAgent can only be installed on hosts running the Linux OSs listed in **OS Usage Restrictions**.
- Windows: ICAgent can only be installed on hosts running the following 64-bit Windows OSs:

  ```
  Windows Server 2016 R2 Datacenter
  Windows Server 2016 R2 Standard
  Windows Server 2016 Datacenter English
  Windows Server 2016 R2 Standard English
  ```



```
Windows Server 2012 R2 Datacenter
Windows Server 2012 R2 Standard
Windows Server 2012 Datacenter English
Windows Server 2012 R2 Standard English

Windows Server 2008 R2 Enterprise
Windows Server 2008 R2 Standard
Windows Server 2008 Enterprise English
Windows Server 2008 R2 Standard English
```

ICAgent installed on Windows hosts cannot be upgraded or uninstalled on the **Host Management** page. To use a newer ICAgent version, uninstall the original one and then install the newer version.

Installation Methods

There are two methods to install ICAgent.

Table 3-3 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

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

Step 1 Apply for an ECS in the current region as a jump server. Modify the security group rules used by the jump server.

1. On the ECS details page, click the **Security Groups** tab.
2. Click a security group name and click **Modify Security Group Rule** in the upper right corner.
3. 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 3-4**.

Table 3-4 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.

NOTE

Open the inbound ports 8149, 8102, 8923, 30200, 30201, and 80 to ensure that data can be transmitted from the host not in this region to the jump server.

Step 2 Log in to the LTS console and choose **Host Management** in the navigation pane on the left.

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

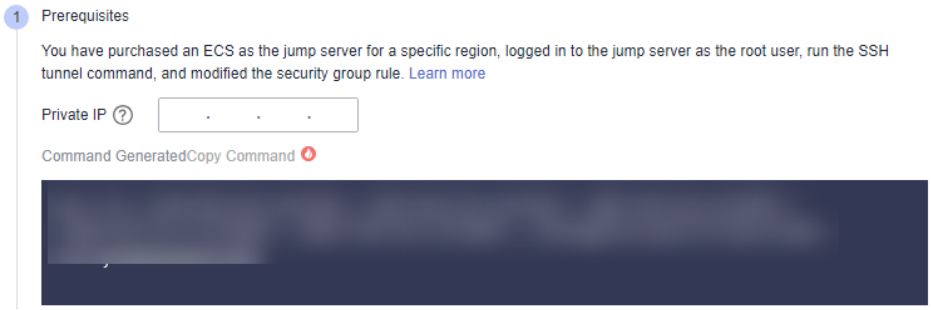
Step 4 Set **OS** to **Linux**.

Step 5 Set **Host** to **Non-CLOUD host**.

Step 6 Open the forwarding ports on the jump server.

1. Enter the private IP address of the jump server and generate an SSH tunneling command, as shown in the following figure.

   Figure 3-5 Entering the private IP address of the jump server

   NOTE

   The private IP address of the jump server refers to the internal IP address of the Virtual Private Cloud (VPC) where the jump server is located.

2. Click **Copy Command**.
3. 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.{*Region*}.myhuaweicloud.com:80 {*Jump server IP address*}

   Enter the password of user **root** as prompted.

4. 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 3-6** is returned, the ports are open.

Figure 3-6 Open TCP ports

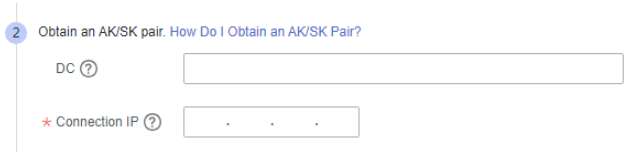
```
[root@ecs-3716 nginx]# netstat -lnp | grep ssh
tcp        0      0 192.168.0.201:80        0.0.0.0:*               LISTEN      1245
tcp        0      0 192.168.0.201:8149      0.0.0.0:*               LISTEN      1245
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN     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

- Enter **http://***IP address of the jump server ECS* in the address box of the browser. If the access is successful, the security group rule has taken effect.
- If the jump server is powered off and restarted, run the preceding commands again.

Step 7 **Obtain the AK/SK pair** and specify the DC and the jump server connection IP address.

Figure 3-7 Obtaining the AK/SK pair

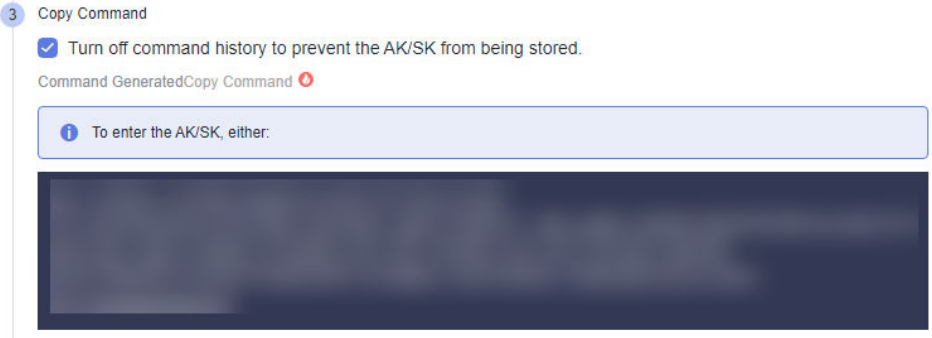


NOTE

- **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 peer connection, use the internal IP address of the VPC where the jump server locates.

Step 8 Copy the ICAgent installation command.

Figure 3-8 Copying the ICAgent installation command



Step 9 Log in as user **root** to the host which is deployed in the region same as that you are logged in to (for example, by using a remote login tool such as PuTTY) and run the copied command.

NOTE

- When the message **ICAgent install success** is displayed, ICAgent has been installed in the **/opt/oss/servicemgr/** directory of the host. You can then view the ICAgent status by choosing **Host Management** in the navigation pane of the LTS console and then clicking **Hosts**.
- 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.

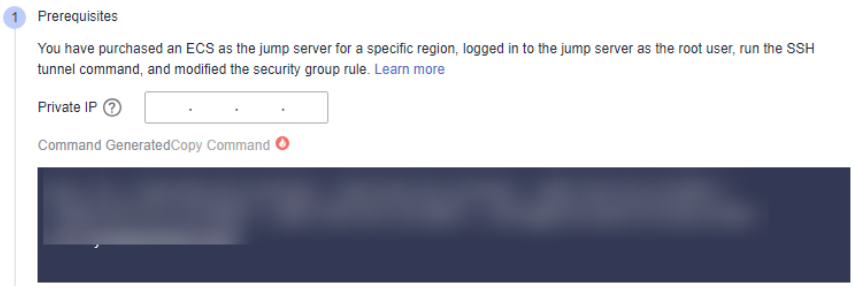
1. On the ECS console, locate the jump server and obtain its private IP address.

   Figure 3-9 Obtaining the private IP address

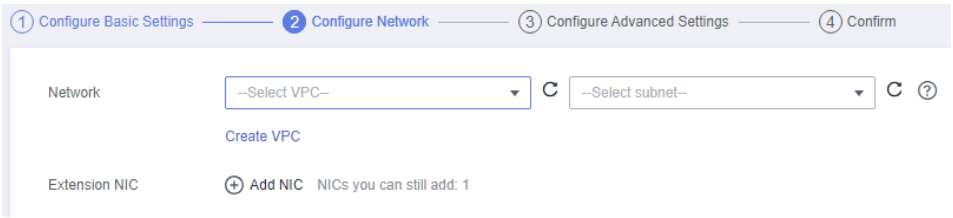
2. On the LTS console, choose **Host Management** in the navigation pane, and click **Install ICAgent** in the upper right corner. In the dialog box displayed, select **Linux** for **OS**, select **Non-CLOUD host** for **Host**, and enter the private IP address to generate the SSH tunneling command.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

   Figure 3-10 Creating 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**.

Figure 3-11 Creating an ECS



Step 4 Create a load balancer. For details, see **Creating a Dedicated 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. For details, see **Adding a TCP Listener**.

Step 6 Add all jump servers to the backend server group. For details, see **Adding Backend Servers**.

----End

Inherited Installation (Linux)

Let's 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. You can follow the directions below 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 the message **ICAgent install success** is displayed, ICAgent has been installed in the **/opt/oss/servicemgr/** directory of the host. You can then view the ICAgent status by choosing **Host Management** in the navigation pane of the LTS console and then clicking **Hosts**.
   - If the installation fails, uninstall ICAgent and reinstall it. If the reinstallation fails, contact technical support.

Batch Inherited Installation (Linux)

Let's 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. You can follow the directions below to install ICAgent on other hosts in batches.

NOTICE

- The hosts must all belong to the same Virtual Private Cloud (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 and try again.

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, as shown in the following example:

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. You can then view the **ICAgent status** by choosing **Host Management** in the navigation pane of the LTS console and then clicking **Hosts**.

3.2.3 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.

NOTE

Linux hosts support ICAgent upgrade on the **Host Management** page of the LTS console.

Procedure

1. Log in to the LTS console and choose **Host Management** in the navigation pane on the left.
2. On the **Host Management** page, click the **Hosts** tab.
3. Select **Hosts**, select one or more check boxes of hosts where ICAgent is to be upgraded, and click **Upgrade ICAgent**.

   Select **CCE Cluster**. In the drop-down list on the right, select the cluster whose ICAgent is to be upgraded, and click **Upgrade ICAgent**.

   NOTE

   - If you create a CCE cluster for the first time, ICAgents 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 ICAgents. 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 ICAgent is not installed on hosts in a cluster or the ICAgent version is too early, click **Upgrade ICAgent** to install the ICAgent on all hosts in the cluster.
4. 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.

   NOTE

   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.

3.2.4 Uninstalling ICAgent

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

NOTE

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

There are a number of ways to uninstall ICAgent:

- **Uninstalling ICAgent on the Console**: This can be used to uninstall ICAgent that has been successfully installed.
- **Uninstalling ICAgent on a Host**: This can be used to remove ICAgent that fails to be installed for reinstallation.
- **Remotely Uninstalling ICAgent**: This can be used to remotely uninstall ICAgent that has been successfully installed.
- **Batch Uninstalling ICAgent**: This can be used to uninstall ICAgent that has been successfully installed from a batch of hosts.

Uninstalling ICAgent on the Console

1. Log in to the LTS console and choose **Host Management** in the navigation pane on the left.
2. Click the **Hosts** tab.
3. Select one or more hosts where ICAgent is to be uninstalled and click **Uninstall ICAgent**.
4. In the displayed dialog box, click **OK**.

   The uninstallation begins. This process takes about a minute.

   Once uninstalled, the host will be removed from the host list.

   NOTE

   To reinstall ICAgent, wait for 5 minutes after the uninstallation completes, or the reinstalled ICAgent may be unintentionally uninstalled again.

Uninstalling ICAgent on a Host

1. Log in to a host where ICAgent is to be uninstalled as user **root**.
2. 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

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

1. Run the following command on the host where ICAgent has been installed, *x.x.x.x* is 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*
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 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 to uninstall ICAgent.
   - If the message **ICAgent uninstall success** is displayed, the uninstallation has completed.

Batch Uninstalling ICAgent

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.

NOTICE

The hosts must all belong to the same Virtual Private Cloud (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, as shown in the following example:

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

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

2. Choose **Host Management** > **Hosts** on the LTS console to view the ICAgent status.

3.2.5 ICAgent Statuses

The following table lists the ICAgent statuses.

Table 3-5 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 Access Key ID/Secret Access Key (AK/SK) pair is incorrect. Obtain the correct AK/SK pair 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.

4 Log Search and Analysis

4.1 Log Search

Follow the directions below to search logs by keyword and time range:

1. On the LTS console, choose **Log Management** in the navigation pane on the left.
2. In the log group list, click on the left of a log group name.
3. In the log stream list, click a log stream name.
4. Above the search box, select a 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.

   NOTE

   - 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.
5. On the log stream details page, you can search for logs using the following methods:
   a. 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**.

      Logs that contain the keyword are displayed on the **Raw Logs** tab page.

      NOTE

      - The structuring fields are displayed in **key:value** format.

   b. On the **Raw Logs** page, click a field in blue in the log content. You can select **Copy**, **Add To Search**, and **Exclude from Search** from the displayed drop-down list.

c. Click a field for which quick analysis has been created to add it to the search box.

NOTE

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.

d. 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 **Query**.

Common Log Search Operations

Log search operations include sharing logs and refreshing logs.

Table 4-1 Common operations

Operation	Description
Creating quick search criteria	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.
Simplifying field details	Click to view the simplified field details.
Unfold/Fold	Click to display all the log content. Click to fold the log content. **NOTE** **Unfold** is enabled by default.

Operation	Description
Downloading logs	Click . On the displayed **Download Logs** page, click **Direct 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.
Collapse all/ Expand all	Click to set the number of lines displayed in the log content. Click to close it. **NOTE** By default, logs are not collapsed, and two rows of logs are shown after collapsing. You can display up to six rows.
Layout	Move the cursor over and choose **Layout** from the drop-down list. On the displayed **Layout** page, specify whether to simplify field display and show fields. • **Simple View**: If this is enabled, the fields are displayed in a simplified manner. • **Show/Hide**: When the visibility of a field is disabled, the field is not displayed in the log content.
JSON	Move the cursor over , click **JSON**, and set JSON formatting. **NOTE** 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.
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**.

Syntax and Examples of Searching

Search syntax:

Table 4-2 Search syntax

Filter	Description
Exact search by keyword	LTS searches for logs containing the exact keyword (case-sensitive) that you specify. A keyword is the word between two adjacent delimiters.
Exact search by phrase	LTS searches for logs containing the exact phrase (case-sensitive) that you specify.
&&	Intersection of search results
||	Union of search results
AND	Intersection of search results
and	Intersection of search results
OR	Union of search results
or	Union of search results
NOT	Logs that contain the keyword after **NOT** are excluded.
not	Logs that contain the keyword after **not** are excluded.
?	Fuzzy search. The question mark (?) can be put in the middle or at the end of a keyword to replace a character.
>	Search for structured long or float fields with values greater than a specified number. For example, **num > 10**.
<	Search for structured long or float fields with values less than a specified number. For example, **num < 10**.
=	Search for structured long or float fields with values equal to a specified number. For example, **num = 10**.
>=	Search for structured long or float fields with values greater than or equal to a specified number. For example, **num >= 10**.
<=	Search for structured long or float fields with values less than or equal to a specified number. For example, **num <= 10**.
:	Search for a specified field (key:value). For example, **request_method:GET**. Use double quotation marks ("") to enclose a field name or value that contains reserved characters, such as spaces and colons (:). For example, **"file info":apsara**.

Filter	Description
""	Enclose a syntax keyword to convert it into common characters. For example, **"and"**. This "and" means searching for logs that contain this word. It is not an operator. All words enclosed in double quotation marks ("") are considered as a whole.
\	Escape double quotation marks (""). The escaped quotation marks indicate the symbol itself. For example, to search for **instance_id:nginx"01"**, use **instance_id:nginx\"01\"**.
*	An asterisk (*) can be placed only after the keyword and can match zero, one, or multiple characters. For example, **host:abcd*c**. **NOTE** LTS will find 100 words that meet the search criteria in all logs and return these logs.
in	Query 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. Example: **request_time in [100 200]** and **request_time in (100 200]** **NOTE** Enter **in** in lowercase and use only long or float fields.
()	Specify fields that should be matched with higher priority. Use **and**, **or**, and **not** to connect fields. Example: **(request_method:GET or request_method:POST) and status:200**
key:#"abc def"	Search for specified field names and values (key:value) after field indexing is configured.
#"abc def"	Full text search. LTS splits an entire log into multiple words based on the delimiter you set. Search for logs using specified keywords (field name and value) and rules.

NOTE

Operators (such as **&&**, **||**, **AND**, **OR**, **NOT**, *****, **?**, **:**, **"**, **>**, **<**, **=**, **>=**, and **<=**) contained in raw logs cannot be used to search for logs.

Search rules:

- Fuzzy search is supported.

  For example, if you enter **error***, all logs containing **error** will be displayed and those start with **error** will be highlighted.
- You can use a combination of multiple search criteria in the key and value format: *key1:value1* **AND** *key2:value2* or *key1:value1* **OR** *key2:value2*. After

entering or selecting *key1:value1*, you need to add **AND** or **OR** before entering or selecting *key2:value2* in the search box.

- Click a keyword and select one of the three operations from the displayed drop-down list: **Copy**, **Add To Search**, and **Exclude from Search**.

  Copy: Copy the field.

  Add To Search: Add **AND** *field: value* to the search statement.

  Exclude from Search: Add **NOT** *field: value* to the query statement.

Searching sample

- Search for logs containing **start**: Enter **start**.
- Search for logs containing **start to refresh**: Enter **start to refresh**.
- Search for the logs containing both keywords **start** and **unexpected**: Enter **start && unexpected**.
- Search for the logs containing both keywords **start** and **unexpected**: Enter **start AND unexpected**.
- Search for the logs containing keyword **start** or **unexpected**: Enter **start || unexpected**.
- Search for the logs containing keyword **start** or **unexpected**: Enter **start OR unexpected**.
- Log data that does not contain *query1*: **NOT content:** *query1*.
- **error***: logs that contain **error**.
- **er?or**: logs that start with **er**, is followed by any single character, and end with **or**.
- If your keyword contains a colon (:), use the **content:** *Keyword* format. Example: **content: "120.46.138.115:80"** or **content: 120.46.138.115:80**.
- *query1* **AND** *query2* **AND NOT content:** *query3*: logs that contain both *query1* and *query2* but not *query3*.

NOTE

- When you enter a keyword to query logs, the keyword is case-sensitive. Log contents you queried are case-sensitive but the highlighted log contents are case-sensitive.
- The asterisk (*) and question mark (?) do not match special characters such as hyphens (-) and spaces.
- For fuzzy match, the question mark (?) or asterisk (*) can only go in the middle or at the end of a keyword. For example, you can enter **ER?OR** or **ER*R**.
- When you search logs by keyword, if a single log contains more than 255 characters, exact search may fail.

4.2 Built-in 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 built-in reserved fields of LTS.

NOTE

- When using APIs to write log data or add ICAgent configurations, do not set field names to built-in reserved fields. Otherwise, problems such as duplicate field names and inaccurate query may occur.
- The name of a custom log field cannot contain double underscores (_). Otherwise, the index cannot be configured.

NOTE

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

Log Example

The following is a CCE log. The value of the content field is the original log text, and other fields are common built-in reserved fields.

```
{
"hostName":"epstest-xx518",
"hostIP":"192.168.0.31",
"clusterId":"c7f3f4a5-xxxx-11ed-a4ec-0255ac100b07",
"pathFile":"stdout.log",
"content":"level=error ts=2023-04-19T09:21:21.333895559Z",
"podIp":"10.0.0.145",
"containerName":"config-reloader",
"clusterName":"epstest",
"nameSpace":"monitoring",
"hostIPv6":"",
"collectTime":"1681896081334",
"appName":"alertmanager-alertmanager",
"hostId":"318c02fe-xxxx-4c91-b5bb-6923513b6c34",
"lineNum":"1681896081333991900",
"podName":"alertmanager-alertmanager-54d7xxxx-wnfsh",
"__time__":"1681896081334",
"serviceID":"cf5b453xxxad61d4c483b50da3fad5ad",
"category":"LTS"
}
```

Built-in Reserved Field Description

Table 4-3 Built-in reserved field description

Field	Data Format	Index and Statistics Settings	Description
collectTime	Integer, Unix timestamp (ms)	Index setting: After this function 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. In the example, "collectTime":"1681896081334" is 2023-04-19 17:21:21 when converted into standard time.

Field	Data Format	Index and Statistics Settings	Description
__time__	Integer, Unix timestamp (ms)	Index setting: After this function 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. In the example, "__time__":"1681896081334" is 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.
lineNum	Integer	Index setting: After this function 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. Such as "lineNum":"1681896081333991900" in the example.
category	String	Index setting: After this function 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. For 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.

Field	Data Format	Index and Statistics Settings	Description
clusterName	String	Index setting: After this function 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. Such as "clusterName":"epstest" in the example.
clusterId	String	Index setting: After this function 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. Such as "clusterId":"c7f3f4a5-xxxx-11ed-a4ec-0255ac100b07" in the example.
nameSpace	String	Index setting: After this function 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. Such as "nameSpace":"monitoring" in the example.
appName	String	Index setting: After this function 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, used as the name of the workload in the Kubernetes scenario. Such as "appName":"alertmanager-alertmanager" in the example.

Field	Data Format	Index and Statistics Settings	Description
serviceID	String	Index setting: After this function 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. Such as "serviceID":"cf5b453xxxad61d4c483b50da3fad5ad" in the example.
podName	String	Index setting: After this function 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. Such as "podName":"alertmanager-alertmanager-0" in the example.
podIp	String	Index setting: After this function 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 in the Kubernetes scenario. Such as "podIp":"10.0.0.145" in the example.
containerName	String	Index setting: After this function 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. Such as "containerName":"config-reloader" in the example.

Field	Data Format	Index and Statistics Settings	Description
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.
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.

Field	Data Format	Index and Statistics Settings	Description
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.
content	String	Index setting: After **Index Whole Text** is enabled, the delimiter defined by the full-text index is used to segment the value of the content field. The content field cannot be configured in the field index.	Original log content Such as "content":"level=error ts=2023-04-19T09:21:21.333895559Z" in the example.
__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.
__client_time__	Integer, Unix timestamp (ms)	Index setting: After this function is enabled, a field index is created for **__client_time__** by default. The index data type is long.	Time when the client reports a device log.

Field	Data Format	Index and Statistics Settings	Description
_content_parse_fail_	String	Index setting: After this function 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.
__save_time__	Integer, Unix timestamp (ms)	The **__save_time__** field cannot be configured in the field index.	Time field of the log stream engine. Log data in the period specified by this field is obtained.
__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
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

4.3 Index Settings

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.

NOTE

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

Log Example

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

In the example log, **hostName**, **hostIP**, and **pathFile** are common built-in reserved fields. For details about the built-in fields, see **Built-in 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"
}
```

Index Types

The following table lists the index types supported by LTS.

Table 4-4 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. **NOTE** • 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. • Reserved fields are not included in full-text indexes. You need to use the Key:Value index to search for fields. For details, see **Built-in Reserved Fields**.

Index Type	Description
Index Fields	Query logs by specified field names and values (Key:Value). **NOTE** • By default, LTS creates index fields for some built-in reserved fields. For details, see **Built-in 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 this function, configure index fields and enable quick analysis for the required fields. Here are two examples: • In the log example, the level and status index fields are configured. The level field is of the **string** type, the field value is error, and a delimiter is configured. The status field 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 log example, LTS creates indexes for built-in reserved fields such as hostName, hostIP, and pathFile by default.

Precautions

- Either whole text indexing or index fields must be configured.
- Index settings (such as adding, editing, and deleting fields and modifying items) take effect only for new log data but not for historical log data. Currently, indexes cannot be recreated for historical logs.
- 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.
- By default, LTS creates index fields for some built-in reserved fields. For details, see **Built-in 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 Whole Text Indexing

Step 1 Log in to the LTS console and choose **Log Management**.

Step 2 In the log group list, click on the left of a log group, and click a log stream to go to the details page.

Step 3 Click in the upper right corner to go to the **Index Settings** page.

Step 4 **Index Whole Text** is enabled by default.

NOTE

- For automatic configuration, the intersection of the raw logs and built-in fields in the last 15 minutes is obtained by default. LTS automatically combines the intersection of the raw logs and built-in fields, current structured fields, and tag fields to form the table data below the field index.
- If no raw log is generated within 15 minutes, obtain the hostIP, hostName, pathFile, structured field, and tag field to form the table data below the field index.
- When **Log Structuring** is configured for ECS ingestion, the category, hostName, hostId, hostIP, hostIPv6 and pathFile fields are automatically added on the **Index Settings** page. A field will not be added if the same one already exists.
- When **Log 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 Settings** page. A Field will not be added if the same one already exists.

Step 5 Set parameters as described in **Table 4-5**.

Table 4-5 Whole 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. **NOTE** 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. ● 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**.
Delimiters	Splits the log content into multiple words based on the specified delimiter. Default delimiters include ,'";=()[]{}@&<>/:\n\t\r and spaces. If the default settings cannot meet your requirements, you can customize delimiters. All ASCII codes can be defined as delimiters. If the delimiter is set to null, the field value is regarded as a whole. You can search for the corresponding log only through the complete character string or fuzzy search. 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 search **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 find the log by fuzzy search or exact words, for example, **error**, **400**, **Kn***, and **TodayIs***. ● If the delimiter is set to a comma (,) and space, the raw log is split into: **error**, **400**, **I**, **Know**, **TodayIsMonday**. You can find the log by fuzzy search or exact words, for example, **Know**, and **TodayIs***.

Parameter	Description
ASCII Delimiters	Click **Add ASCII Delimiter** and enter the ASCII value by referring to **ASCII Table**.

Step 6 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.

NOTE

Custom and special delimiters of field indexes are available only to whitelisted users. To use them, .

Step 1 Click **Add Field** under **Index Fields** and set field information by referring to **Table 4-6**.

Step 2 Alternatively, select fields and click **Batch configuration**. On the displayed page, configure parameters.

Step 3 Configure the index field by referring to **Table 4-6**.

NOTE

- The preceding indexing parameters take effect only for the current field.
- Index fields that do not exist in log content are invalid.

Table 4-6 Index field parameters

Parameter	Description
Field Name	Log field name, including **level** in the example log. The field name can contain only letters, digits, and underscores (_), and must start with a letter or underscore (_). The field name cannot contain double underscores (__). **NOTE** • Double underscores (__) are used in built-in reserved fields that are not displayed to users in LTS. Double underscores (__) cannot be used in custom log field names. Otherwise, field index names cannot be configured. • By default, LTS creates index fields for some built-in reserved fields. For details, see **Built-in Reserved Fields**.
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**.

Parameter	Description
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 delimiter. Default delimiters include ,'";=()[]{}@&<>/:\n\t\r and spaces. If the default settings cannot meet your requirements, you can customize delimiters. All ASCII codes can be defined as delimiters. If the delimiter is set to null, the field value is regarded as a whole. You can search for the corresponding log only through the complete character string or fuzzy search. 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. **NOTE** 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. • 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 **Quick Analysis**. **NOTE** • 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 2000 bytes. • The quick analysis field area displays the first 100 records.
Operation	Click  to delete the target field.

Step 4 Click **OK**.

----End

Auto Index Field Configuration

When creating an index field, you can click **Auto Config**. The log service automatically adds some index fields. You can add or delete fields as required.

- The log service automatically generates an index field based on the first content in the preview data during collection.
- The log service selects several common built-in reserved fields (such as **hostIP**, **hostName**, and **pathFile**) and adds them to the index field.

ASCII Table

Table 4-7 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
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

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

4.4 Cloud Structuring Parsing

4.4.1 Log Structuring

Log data can be structured or unstructured. Structured data is quantitative data or can be defined by unified data models. It has a fixed length and format. Unstructured data has no pre-defined data models and cannot be fit into two-dimensional tables of databases.

During log structuring, logs with fixed or similar formats are extracted from a log stream based on your defined structuring method and irrelevant logs are filtered out.

Precautions

- You have created a log stream.
- 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.

Creating a Structuring Rule

Add structuring rules to a log stream and LTS will extract logs based on the rules.

To structure logs:

Step 1 Log in to the LTS console and choose **Log Management** in the navigation pane on the left.

Step 2 Select a log group and a log stream.

Step 3 On the log stream details page, click  in the upper right corner. On the page displayed, select **Log Structuring** to structure logs.

- **Regular Expressions**
- **JSON**
- **Delimiter**
- **Nginx**
- **Structuring Template**

NOTE

- If a structured field exceeds 20 KB, only the first 20 KB is retained.
- 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**.

Step 4 Click **Save**.

----End

Modifying a Structuring Rule

To modify a structuring rule, perform the following steps:

Step 1 On the **Log Structuring** page, click to modify a structuring rule.

NOTE

- You can modify the structuring rules, including the structuring mode, log extraction field, and tag field.
- System templates cannot be modified.

Step 2 Click **Save**.

----End

Deleting a Structuring Rule

If a log structuring rule is no longer used, perform the following steps to delete it:

Step 1 On the **Log Structuring** page, click to delete a structuring rule.

Step 2 In the displayed dialog box, click **OK**.

NOTE

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

----End

4.4.2 Structuring Modes

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

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 log events**, select a log event, and click **OK**. You can select different time ranges to filter logs.
- Click **Paste from Clipboard** to copy the cut log content to the sample log box.

NOTE

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 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.
- **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.

NOTE

- 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 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 log events**, 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.

NOTE

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

Click **Intelligent Extraction**. Take the following log event as an example.

Enter the log event in the text box.

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

NOTE

- The **float** data type has 16 digit precision. If a value contains more than 16 valid digits, the extracted content is incorrect, which affects visualization and 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**.

Check and edit the fields if needed. For details about rules for configuring extracted fields, see **Setting Log Structuring Fields**.

Step 3 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 log events**, 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.

NOTE

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.

NOTE

- 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 custom character 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.

Click **Intelligent Extraction**. Take the following log event as an example.

Enter the log event in the text box.

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

NOTE

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

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

Check and edit the fields if needed. For details about rules for configuring extracted fields, see **Setting Log Structuring Fields**.

Step 4 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 log events**, 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.

NOTE

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,

NOTE

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.

Click **Intelligent Extraction**. Take the following log event as an example.

Enter the log event 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"';
```

NOTE

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

Check and edit the fields if needed. For details about rules for configuring extracted fields, see **Setting Log Structuring Fields**.

Step 4 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 **Structuring Templates**.

4.4.3 Structuring Templates

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

System Templates

Step 1 Click **System template** and select a template. A sample log event is displayed for each template.

Step 2 When you select a template, the log parsing result is displayed in the **Template Details** area. Click **Save**.

NOTE

During log structuring, if a system template is used, the time in the system template is the customized log time.

----End

Custom Templates

Click **Custom template** and select a template. There are two ways to obtain a custom template:

- 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 the template name and click **OK**. The template will be displayed in the custom template list.
- Create a custom template under the **Structuring Template** option.

  Select **Custom template** and click **Create Template**. Enter a template name, select **Regular Expressions**, **JSON**, **Delimiter**, or **Nginx**, configure the template, and click **Save**. The template will be displayed in the custom template list.

4.4.4 Log Structuring Fields

Restrictions

The maximum size of a structured field value is 16 KB. The excess part will be truncated.

Setting Log Structuring Fields

You can edit extracted fields after log structuring.

Table 4-8 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 for unnamed fields. You can modify these names.	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
ELB structuring template	Defined by ELB.	No	No
VPC structuring template	Defined by VPC.	No	No
CTS structuring template	Keys in JSON log events.	No	No
APIG structuring template	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

Structuring Method	Field Name	Field Type Can Be Changed	Field Can Be Deleted
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
MySQL error logs	Defined by MySQL.	No	No
MySQL slow query logs	Defined by MySQL.	No	No
PostgreSQL error logs	Defined by PostgreSQL.	No	No
SQL Server error logs	Defined by SQL Server.	No	No
GaussDB(for Redis) slow query logs	Defined by GaussDB(for Redis).	No	No
CDN	Defined by CDN.	No	No
SMN	Defined by SMN.	No	No
GaussDB_MySQL error logs	Defined by GaussDB_MySQL.	No	No
GaussDB_MySQL slow query logs	Defined by GaussDB_MySQL.	No	No
Enterprise Router	Defined by ER.	No	No
MySQL audit logs	Defined by MySQL.	No	No
GaussDB(for Cassandra) slow query logs	Defined by GaussDB(for Cassandra).	No	No
GaussDB(for Mongo) slow query logs	Defined by GaussDB(for Mongo).	No	No

Structuring Method	Field Name	Field Type Can Be Changed	Field Can Be Deleted
GaussDB(for Mongo) error logs	Defined by GaussDB(for Mongo).	No	No
Custom templates	User-defined.	Yes	Yes

NOTE

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

- 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.

Setting Tag Fields

When you structure logs, you can configure tag fields, so you can use these fields to run SQL queries on the **Visualization** page.

Step 1 During field extraction, click the **Tag Fields** tab.

Step 2 Click **Add Field**.

Step 3 In the **Field** column, enter the name of the tag field, for example, **hostIP**.

NOTE

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 4 To add more fields, click **Add Field**.

Step 5 Click **Save** to save the settings.

NOTE

- 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

4.5 Search Syntax and Functions

4.5.1 Search Syntax

LTS provides a set of search syntax for setting search criteria, helping you search for logs more effectively.

NOTE

- Before using the search syntax, set the delimiters in **Index Settings**. If there is no special requirement, use the default delimiters **, '";=()[]{}@&<>/:\n\t\r**.
- The search syntax does not support search by delimiter.

  Search statements do not support delimiters. 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 all logs that contain both **var** and **log**. Similarly, the search statements such as **"var:log"** and **var;log** are used to search for all logs that contain both **var** and **log**.

NOTE

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

Search Mode

The search statement is used to specify the filter criteria for log search and return the logs that meet the filter 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 4-9 Search mode description

Search Mode	Description	Example
Full-Text Search	LTS splits an entire log into multiple keywords when full-text index is set. **NOTE** • **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.

Search Mode	Description	Example
Field Search	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. **NOTE** • 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*** indicate 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.
Exact Search	Use exact words for search. LTS searches with word segmentation, which does not define the sequence of keywords. **NOTE** If the search statement is abc def, all logs that contain both abc and def are matched. Logs abc def or def abc are matched. To ensure the sequence of keywords, use **#"abc def"**.	• GET POST: searches for logs that contain both GET and POST. • request_method:GET indicates that logs in which the value of request_method contains GET are searched. • #"/var/log" indicates that logs containing the phrase /var/log are searched.

Search Mode	Description	Example
Fuzzy Search	Specify a word in the search statement and add a fuzzy search keyword, that is, an asterisk (*) or a question mark (?), to the middle or end of the word. LTS searches for the word that meets the search criteria and returns all logs that contain the word. **NOTE** • The asterisk (*) indicates that multiple characters are matched, and the question mark (?) indicates that one character is matched. • Words cannot start with an asterisk (*) or a question mark (?). • Long and float data does not support fuzzy search using asterisks (*) or question marks (?).	• 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 Scope	The long and float data supports range search. • 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. **NOTE** The string fields do not support range query.	• 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.
Phrase Search	Phrase search is used to fully match target phrases in logs to ensure the sequence in which keywords appear. **NOTE** 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 delimiter divides 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. **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 solit 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"**.

Operator

The search statement supports the following operators:

NOTE

- Except the in operator, other operators are case-insensitive.
- The priorities of operators in descending order are as follows:
  1. Colon (:)
  2. Double quotation marks ("")
  3. Parentheses: ()
  4. and, not
  5. or

Table 4-10 Description

Operator	Description
and	AND operator. If there is no syntax keyword between multiple keywords, the AND relationship is used by default. For example, **GET 200** is equivalent to **GET and 200**. **NOTE** 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.
AND	AND operator, equivalent to and.
&&	AND operator. **NOTE** 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.
or	OR operator, example: **request_method:GET or status:200** **NOTE** When or is used as an operator, use a space before and after it.
OR	OR operator, equivalent to or.
||	OR operator. When || is used as an operator, spaces are not necessary.
not	NOT operator. Example: **request_method:GET not status:200, not status:200** **NOTE** • 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.
( )	Specify fields that should be matched with higher priority. Example: **(request_method:GET or request_method:POST) and status:200**
:	Search for a specified field (key:value). For example, **request_method:GET**. **NOTE** Use double quotation marks ("") to enclose a field name or value that contains reserved characters, such as spaces and colons (:). Example: **"request method":GET, message:"This is a log"**
""	Enclose 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.
\	Escape double quotation marks (""). The escaped quotation marks indicate the symbol itself. For example, to search for **instance_id:nginx"01"**, use **instance_id:nginx\"01\"**.

Operator	Description
*	An asterisk can match zero, single, or multiple characters. Example: **request_method:P*T** **NOTE** Put it in the middle or at the end of a keyword.
?	A question mark matches a single character. For example, **request_method:P?T** can match PUT but cannot match POST. **NOTE** Put it in the middle or at the end of a keyword.
>	Searches logs in which the value of a field is greater than a specified value. Example: **request_time>100**
>=	Searches logs in which the value of a field is greater than or equal to a specified value. Example: **request_time>=100**
<	Searches logs in which the value of a field is less than a specified value. Example: **request_time<100**
<=	Searches logs in which the value of a field is less than or equal to a specified value. Example: **request_time<=100**
=	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. For example, **request_time=100** is equivalent to **request_time:100**.
in	Search 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. Example: **request_time in [100 200]** and **request_time in (100 200]** **NOTE** Enter **in** in lowercase. When it is used as an operator, use a space before and after it.
#""	Searches for logs that contain the target phrase, ensuring the sequence of keywords. **NOTE** 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.

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 examples and indexes:

Table 4-11 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" **NOTE** Double quotation marks are used to enclose and. and is a common string and does not represent 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 whose sec-ch-ua-mobile field is ?0	sec-ch-ua-mobile:#"?0" **NOTE** If search is required when log content contains asterisks (*) or question marks (?), use phrases search.

The following describes examples of advanced searches.

Table 4-12 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 4-13 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

4.5.2 Phrase Search

Phrase search is used to precisely match the target phrase. For example, the search statement **abc def** matches all logs that contain both **abc** and **def** regardless of the sequence. For details about the differences between phrase search and keyword search, see **Table 4-14**.

- 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 4-14 Differences between two search modes

Search Mode	Phrase Search	Keyword Search
Differences	Distinguishes the sequence of keywords and is used to accurately match target phrases, making the search result more accurate.	Does not distinguish the sequence of keywords. The keyword is matched based on the search logic.

Search Mode	Phrase Search	Keyword Search
Examples	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 the phrase **#"is lts"**, one log is matched.	If you search for the keyword **is lts**, two logs are matched.
	If you search for the phrase **#"lts is"**, one log is matched.	If you search for the keyword **lts is**, two logs are matched.

NOTE

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

Search Syntax

Table 4-15 Search Mode

Search Mode	Description
Full-text search	• #"abc def" • content:#"abc def" **NOTE** **content** is a built-in field corresponding to the original log text. **#"abc def"** is equivalent to **content:#"abc def"** and matches the original log content by default.
Field Search	key:#"abc def" **NOTE** • The value cannot be empty. • When field search is used together with the not operator, logs that do not contain this field are matched.

Restrictions

- 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.

Example

Table 4-16 Search description

Search Requirement	Search Statement
Logs in which the value of User-Agent contains the phrase Mon, 17 Apr 2023.	User-Agent:#"Mon, 17 Apr 2023"
Logs in which the value of User-Agent contains the phrase Mozilla/5.0.	User-Agent:#"Mozilla/5.0"
Logs in which the value of week contains the phrase Monday.	week:#"Monday"

4.5.3 Viewing Real-Time Logs

You can view reported logs on the LTS console in real time.

Prerequisites

- You have created log groups and log streams.
- You have installed **ICAgent**.
- You have configured log collection rules.

Procedure

1. On the LTS console, click **Log Management**.
2. In the log group list, click on the left of a log group name.
3. In the log stream list, click the name of the target log stream.
4. Click the **Real-Time Logs** tab to view the real-time logs.

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.

- **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 page, logs will stop being loaded in real time. The next time you access the tab, the logs that were shown before you left the tab will not be displayed.

4.5.4 Quick Analysis

Monitoring keywords in logs helps you keep track of system performance and services. For example, the number of **ERROR** keywords indicates the system health, and the number of **BUY** keywords indicates the sales volume. LTS provides quick analysis for you to obtain statistics on your specified keywords.

Prerequisites

Quick analysis is conducted on fields extracted from structured logs. **Structure** raw logs before you create a quick analysis task.

Creating a Quick Analysis Task

You can enable **Quick Analysis** for the fields on the **Log Structuring** page. You can also perform the following steps to create a quick analysis task:

Step 1 Log in to the LTS console. In the navigation pane on the left, choose **Log Management**.

Step 2 A quick analysis is performed on a log stream. Select the target log group and log stream on the **Log Management** page.

Step 3 On the **Raw Logs** tab page, click **Set Quick Analysis**or . On the displayed page, add fields for quick analysis.

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

NOTE

- abc indicates a field of the **string** type.
- 1.2 indicates a field of the **float** type.
- 123 indicates a field of the **long** type.
- The maximum length of a field for quick analysis is 2000 bytes.
- The quick analysis field area displays the first 100 records.

----End

4.5.5 Quick Search

To search for logs using a keyword repeatedly, perform the following operations to configure quick search.

Procedure

1. On the LTS console, choose **Log Management** in the navigation pane on the left.
2. In the log group list, click ⌄ on the left of a log group name.
3. In the log stream list, click the name of the target log stream.
4. Click the **Raw Logs** tab, click , and specify **Name** and **Keyword**.
   - 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***.
5. Click **OK**.

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

Viewing Context of a Log

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

1. On the **Raw Logs** tab of the log details page, click to view the context.

   The context of the log is displayed.
2. On the displayed **View Context** page, check the log context.

Table 4-17 Introduction to log context viewing

Feature	Description
Search Rows	Select the number of rows to search. The options are 100, 200, 500, 1,000, and 2,000.
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.

5 Log Alarms

5.1 Alarm Rules

5.1.1 Configuring Keyword Alarms

LTS allows you to collect statistics on log keywords 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. Currently, up to 200 keyword alarms can be created for each account.

Prerequisites

You have created log groups and log streams.

Creating an Alarm Rule

Step 1 Log in to the LTS console, and choose **Alarms** in the navigation pane on the left.

Step 2 Click the **Alarm Rules** tab.

Step 3 Click **Create**. The **Create Alarm Rule** right panel is displayed.

Step 4 Configure an alarm rule.

Table 5-1 Alarm rule parameters

Parameter	Description	Check Rule	Example
Rule Name	Name of the alarm rule.	A name can contain 1 to 64 characters, including only letters, digits, hyphens (-), underscores (_), and periods (.). It cannot start with a period or underscore or end with a period.	LTS-Alarm
Description	Rule description.	It cannot exceed 64 characters.	-
Statistics	Select **By keyword**.	-	By keyword
Log Group Name	Select a log group.	-	-
Enterprise Project Name	Select an enterprise project. This parameter is displayed only when the enterprise project function is enabled for the current account.	-	-
Log Stream Name	Select a log stream.	-	-
Keywords	Enter keywords that you want LTS to monitor in logs.	Exact and fuzzy matches are supported. A keyword is case-sensitive and contains up to 1024 characters.	hostIP:192

Parameter	Description	Check Rule	Example
Query Time Range	Time range for the keyword query, which 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 keyword query 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.	-	1 hour

Parameter	Description	Check Rule	Example
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. **NOTE** 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.	-	Daily 01:00

Parameter	Description	Check Rule	Example
	– **0 0 10 * ***: The query is performed at 00:00 on the 10th day of every month.		
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 (**<=**).	Number of log events: 1–2,147,483,647	> 10
Triggers	Configure a condition that will trigger the alarm. Specify the number of statistical periods and the number of times the condition must be met to trigger the alarm. The number of queries must be greater than or equal to the number of times the condition must be met.	Number of queries: 1–10	4, 2
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: 3–10	3
Notify	Specify whether to send a notification when the alarm is cleared. By default, this option is disabled. If this option is enabled, a notification will be sent when the policy is met.	-	Enabled
Alarm Severity	Possible values are **critical** (default), **major**, **minor**, and **info**.	-	Critical
Send Notifications	Possible values are **No** (default) and **Yes**.	-	No

Parameter	Description	Check Rule	Example
SMN Topic	If you select **Yes** for **Send Notifications**, select a Simple Message Notification (SMN) topic, time zone, language, and message template. You can select multiple topics.	This parameter is required when **Send Notifications** is set to **Yes**.	-

Step 5 Click **OK**. The keyword alarm rule is created.

You can also choose **Log Management** in the navigation pane, and select a log stream. On the **Raw Logs** tab page displayed, click in the upper right corner, and click **Alarms Rules** to create an alarm rule.

----End

Modifying an Alarm Rule

Step 1 Click **Modify** in the **Operation** column of the row that contains the target alarm rule, and modify the parameters by referring to **Table 5-1**. **Rule Name** and **Statistics** cannot be modified.

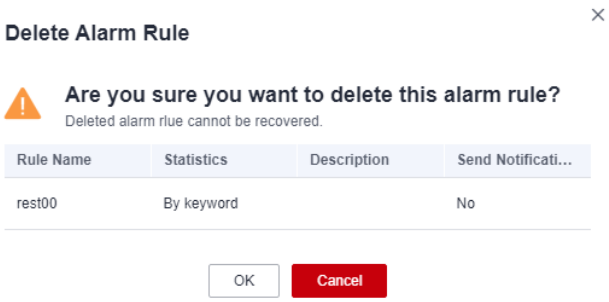
Step 2 Click **OK**.

----End

Deleting an Alarm Rule

Step 1 Click **Delete** in the **Operation** column of the row that contains the target alarm rule.

Figure 5-1 Deleting an Alarm Rule



Step 2 Click **OK**.

----End

5.2 Alarm Notifications

5.2.1 Message Templates

A message template defines the format of alarm notification messages sent to subscribers. LTS provides built-in keywords_template and sql_template. Subscribers can select templates based on protocols. If the template of a specified protocol does not exist, the built-in template is used to send messages to subscribers of that protocol. 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 On the LTS console, choose **Alarms** > **Message Templates**.

NOTE

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**: keyword alarm template
- **sql_template**: SQL alarm template

Step 2 Click **Create**. On the displayed page, set the required parameters.

Table 5-2 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. 1024 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** • Alarm severity: *${event_severity}* • Occurrence time: *${starts_at}* • Occurrence region: *${region_name}* • Alarm source: *$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: *$event.annotations.current_value* • Statistical period: *${frequency}* • Rule name: *${event_name}* • Variables supported by keyword alarms: 1. Query time: *$event.annotations.results[0].time* 2. Query log: *$event.annotations.results[0].raw_results* 3. Query URL: *$event.annotations.results[0].url* 4. Log group/stream name: *$event.annotations.results[0].resource_id*	${event_name} ${event_severity} ${starts_at} ${region_name}

Parameter	Description	Verification Rule	Example
		NOTE 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. Query custom field: *$event.annotations.results[0].fields.xxx* **NOTE** *xxx* indicates a structured or built-in field (such as **hostIP** and **hostName**) in raw logs. • Variables supported by SQL alarms: 1. Log group/stream names of chart 0: *$event.annotations.results[0].resource_id* **NOTE** 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. 2. Query statement of chart 0: *$event.annotations.results[0].sql* 3. Query time of chart 0: *$event.annotations.results[0].time* 4. Query URL of chart 0: *$event.annotations.results[0].url* 5. Query log of chart 0: *$event.annotations.results[0].raw_results* **Copy from Existing** • keywords_template • sql_template • Custom templates (created with variables)	

- Create a message template.
- Copy from an existing template.

NOTE

- The email content supports HTML tags and message preview.
- Templates such as WeCom and DingTalk support markdown syntax 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.

Step 3 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 5-2**. The template name cannot be modified.

NOTE

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, and set a new template name.

Step 2 Click **OK**.

----End

Deleting a Message Template

Deleting a Single Message Template

Step 1 In the message template list, click **Delete** in the **Operation** column of the target template.

NOTE

Built-in message templates cannot be deleted.

Step 2 Click **OK**.

----End

Deleting Multiple Message Templates

Step 1 In the message template list, select the templates to be deleted and click **Delete** above the list.

Step 2 Click **OK**.

----End

5.3 Viewing Alarms

You can configure keyword alarm rules to query and monitor log data. When alarm rules are met, alarms will be triggered. You can view the alarms on the LTS console.

Prerequisites

You have created an alarm rule.

Procedure

Step 1 Log in to the LTS console, and choose **Alarms** in the navigation pane.

Step 2 Click the **Alarms** tab. The alarms generated in 30 minutes from now and their trend charts are displayed by default.

Step 3 Set criteria to search for your target alarms.

- In the search box in the upper part of the page, select a log group, log stream, and alarm severity.
- 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.

  NOTE

  - 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 Click  after you set the search criteria. The details and trend of the alarms that match the criteria will be displayed.

Step 5 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

6 Log Transfer

6.1 Overview

Logs reported from hosts and cloud services are retained in LTS. You can set the retention period. Retained logs are deleted once the retention period is over. For long-term retention, you can transfer logs to other cloud services.

NOTE

Log transfer refers to when logs are replicated to other cloud services. Retained logs are deleted once the retention period is over, but the logs that have been transferred to other services are not affected.

- You can transfer logs to OBS based on your service scenario.
  - **Transferring Logs to OBS**

    Object Storage Service (OBS) provides massive, secure, and cost-effective data storage for you to store data of any type and size.

6.2 Transferring Logs to OBS

You can transfer logs to OBS and download log files from the OBS console.

NOTE

To transfer logs, you must have the **OBS Administrator** permissions apart from the LTS permissions.

Prerequisites

- Logs have been ingested to LTS.
- You have created an OBS bucket.

Creating a Log Transfer Task

Step 1 Log in to the LTS console and choose **Log Transfer** in the navigation pane on the left.

Step 2 Click **Configure Log Transfer** in the upper right corner.

Step 3 On the displayed page, configure the log transfer parameters.

Table 6-1 Transfer parameters

Parameter	Description	Example Value
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
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. **NOTE** Log streams that have been configured with OBS transfer settings cannot be configured again.	-

Parameter	Description	Example Value
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. **NOTE** If you select an unauthorized OBS bucket, LTS will take 15 minutes to authorize the ACL for the bucket. If your configuration fails, try again 15 minutes later. To prevent log transfer failures, exercise caution when modifying bucket policies.	-
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/%done/%H/%m**, the path is **LogTanks**/*Region name*/**LTS-test**/*Y*/*m*/*d***one**/*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/%done/%H/%m

Parameter	Description	Example Value
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

Format	The storage format of logs. The value can be **Raw Log Format** or **JSON**.
	• Examples 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)`
	• The following is an 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

Parameter	Description	Example Value
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**. **NOTE** When **Filter by Tag Fields** is enabled, **Format** must be **JSON**. • **Filter by Tag Fields**: When this parameter is enabled, logs will be filtered by tags.	Enabled

Step 4 Click **OK**. When the log transfer status changes to **Normal**, the transfer task has been created.

Step 5 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.

NOTE

Logs stored in OBS are in raw or JSON format.

----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 **Details** in the row of the desired task to view the task 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.

NOTE

- 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. If one OBS bucket is used by multiple transfer tasks, perform the following operations to delete the transfer task:
  - If only one transfer task is created using this OBS bucket, delete the bucket access permission granted to specific users on the **Access Control** > **Bucket ACLs** tab page on the OBS console when you delete the transfer task.
  - If multiple transfer tasks are created using 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 **Disabled**.

- **Normal**: The log transfer task works properly.
- **Abnormal**: An error occurred in the log transfer task. The possible causes are as follows:
  - The OBS bucket has been deleted. Specify another OBS bucket.
  - Access control on the OBS bucket is configured incorrectly. Access the OBS console to correct the settings.
- **Disabled**: The log transfer task is stopped.

7 Configuration Center

7.1 Quota Configuration

Enabling or Disabling Log Collection Beyond Free Quota

NOTE

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

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.

Step 1 Log in to the LTS console and choose **Configuration Center** in the navigation pane on the left.

Step 2 Disable **Continue to Collect Logs When the Free Quota Is Exceeded**.

When the free quota is used up, log collection will be suspended.

NOTE

- If this function is enabled, logs will continue to be collected after the free quota 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.

----End

7.2 Delimiter Configuration

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.

NOTE

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

Precautions

Your custom delimiters are applicable only to the log events generated after the delimiters are configured.

Procedure

Step 1 Log in to the LTS console, choose **Configuration Center** in the navigation pane on the left, and click the **Delimiters** tab.

Step 2 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 delimiters in the text box.
- **ASCII Delimiters**: Click **Edit**. On the displayed page, click **Add ASCII Delimiter** and enter ASCII values by referring to **ASCII Table**.

Step 3 Preview the parsing result.

Enter log content in the text box and click **Preview**.

Step 4 Check whether the parsing result is correct. If it is correct, click **Save**.

NOTE

You can click **Reset** to restore the default delimiters, which include:

```
, '";=()[]{}@&<>/:\n\t\r
```

----End

ASCII Table

Table 7-1 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
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

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

7.3 Log Collection

To reduce the memory, database, and disk space usage, you can set log collection as required. The log collection switch is used to determine whether to collect log data.

Step 1 Log in to the LTS console, choose **Configuration Center** in the navigation pane on the left, and click the **Log Collection** tab.

Step 2 Enable or disable **Log Collection**.

NOTE

This function is enabled by default. If you do not need to collect logs, disable this function to reduce resource usage.

After the log collection function is disabled, ICAgents will stop collecting logs, and this function on the AOM console will also be disabled.

----End

8 Appendixes

8.1 How Do I Obtain an AK/SK Pair?

An access key comprises an access key ID (AK) and secret access key (SK), and is used as a long-term identity credential to **sign your requests for Huawei Cloud APIs**. AK is used together with SK to sign requests cryptographically, ensuring that the requests are secret, complete, and correct.

Important Notes

1. You can create a maximum of two access keys with identical permissions and unlimited validity. **Each access key can be downloaded only once when created.** Keep your access keys secure and change them periodically for security purposes. To change an access key, delete it and create a new one.
2. Federated users can only create temporary access credentials (temporary AK/SKs and security tokens). For details, see **Temporary Access Key (for Federated Users)**.
3. If you are an IAM user, point to the username in the upper right corner of the management console, choose **Security Settings**, click the **Critical Operations** tab, and check the enabling status of the **Access Key Management** feature.
   - Disabled: All IAM users under the account can manage (create, enable, disable, and delete) their own access keys.
   - Enabled: Only the administrator can manage users' access keys.
4. If you cannot manage your access keys, request the **administrator** to perform either of the following operations:
   - Manage your access keys (see **Managing Access Keys for an IAM User**).
   - Grant the permissions you require (see **Assigning Permissions to an IAM User**) or enable access key management (see **Access Key Management**).
5. If you are an administrator, you can view the AK of an IAM user on the user details page. The SK is kept by the user.

Creating an Access Key

Step 1 Hover the mouse pointer over the username in the upper right corner and choose **My Credentials** from the drop-down list.

Step 2 Choose **Access Keys** in the navigation pane on the left.

Step 3 Click **Create Access Key** and enter a description.

NOTE

- You can create up to two access keys. The quota cannot be increased. If you already have two access keys and want to create a new one, delete one first.
- To change an access key, **delete it** and create a new one.

Step 4 Click **OK**, download the AK/SK, and keep it secure.

You can obtain the AK from the access key list and SK from the downloaded CSV file.

NOTE

- Keep the CSV file properly. You can only download the file right after the access key is created. However, if you cannot find the file to obtain the key information, you can create a key.
- Open the CSV file in the lower left corner, or choose **Downloads** in the upper right corner of the browser and open the CSV file.
- Keep your access keys secure and change them periodically for security purposes. To change an access key, delete it and create a new one.

----End

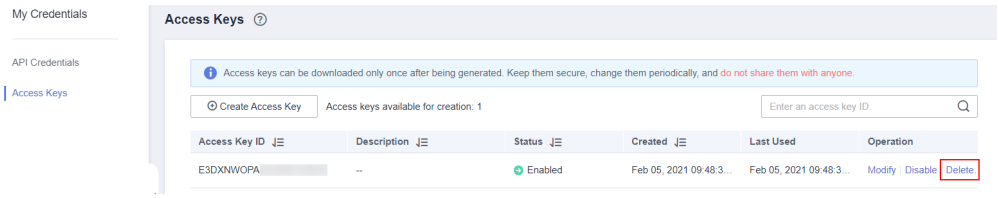
Deleting an Access Key

If your access keys are forgotten or leaked, delete them on the **My Credentials** page or contact the administrator to delete them in IAM.

NOTE

Deleted access keys cannot be restored. Make sure that the deleted access keys have not been used for more than one week.

Step 1 On the **Access Keys** page, locate the access key to be deleted and click **Delete** in the **Operation** column.



Step 2 In the displayed dialog box, click **Yes**.

----End

8.2 How Do I Install ICAgent by Creating an Agency?

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

Procedure

1. Log in to the console.
2. Hover the mouse pointer over the username in the upper right corner of the page and select **Identity and Access Management**.
3. Choose **Agencies** in the navigation pane on the left.
4. Click **Create Agency** in the upper right corner and set parameters as follows:

   Table 8-1 Agency parameters

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

5. Click **Next**. On the page displayed, no authorization is required.
6. Click **Next**. Close the dialog box to return to the **Agencies** page. The created agency is displayed.

Making an Agency Effective

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

