

Log Tank Service

User Guide

Issue 01
Date 2023-08-30



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

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

1 Service Overview	1
1.1 What Is LTS?	1
1.2 Basic Concepts	2
1.3 Features	2
1.4 Usage Restrictions	3
1.5 Related Services	5
2 Getting Started	6
2.1 Overview	6
2.2 Step 1: Creating Log Groups and Log Streams	7
2.3 Step 2: Installing ICAgent	8
2.4 Step 3: Ingesting Logs to Log Streams	10
2.5 Step 4: Viewing Logs in Real Time	11
3 Log Management	13
3.1 LTS Console	13
3.2 Resource Statistics	16
3.3 Managing Log Groups	18
3.4 Managing Log Streams	20
4 Log Ingestion	23
4.1 Collecting Logs from Cloud Services	23
4.1.1 Collecting Logs from CCE	23
4.1.2 Collecting Logs from ECS	30
5 Host Management	36
5.1 Managing Host Groups	36
5.2 Managing Hosts	40
5.2.1 Installing ICAgent	40
5.2.2 Upgrading ICAgent	43
5.2.3 Uninstalling ICAgent	44
5.2.4 ICAgent Statuses	46
6 Log Search and View	48
6.1 Log Search	48
6.2 Cloud Structuring Parsing	54

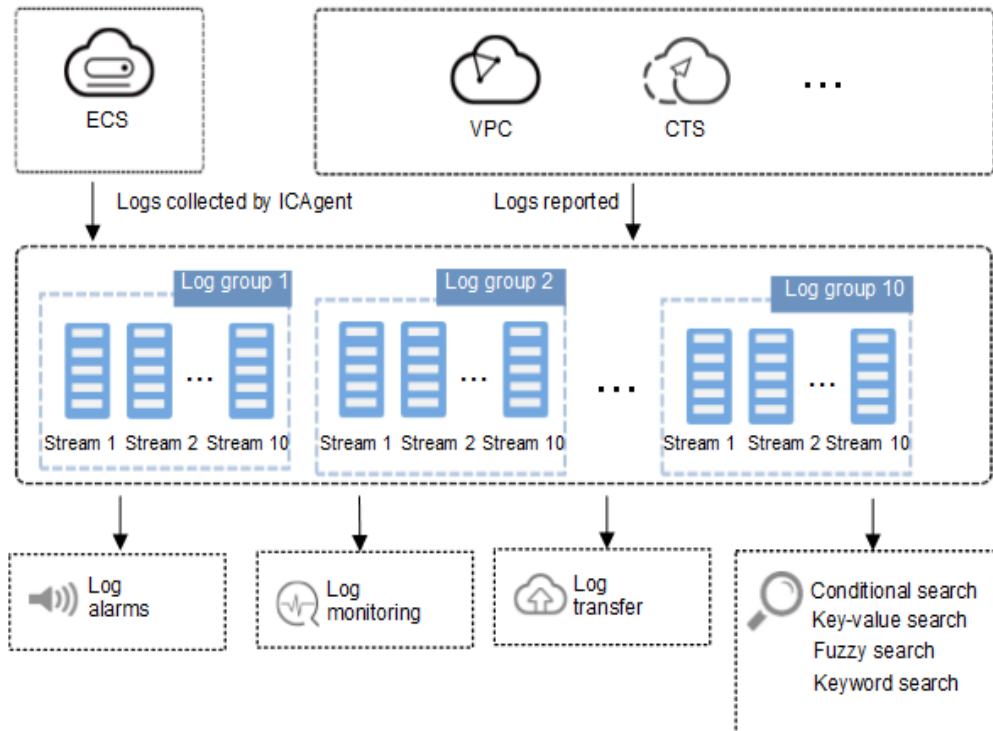
6.2.1 Log Structuring.....	54
6.2.2 Structuring Modes.....	55
6.2.3 Structuring Templates.....	60
6.2.4 Log Structuring Fields.....	61
6.3 Viewing Real-Time Logs.....	64
6.4 Quick Search.....	65
6.5 Quick Analysis.....	66
7 Log Alarms.....	68
7.1 Alarm Rules.....	68
7.1.1 Configuring Keyword Alarms.....	68
7.2 Viewing Alarms.....	72
8 Log Transfer.....	74
8.1 Overview.....	74
8.2 Transferring Logs to OBS.....	74
9 Configuration Center.....	79
9.1 Log Collection.....	79
10 FAQs.....	80
10.1 Log Collection.....	80
10.1.1 What Can I Do If the CPU Usage Is High When ICAgent Is Running?.....	80
10.1.2 What Kind of Logs and Files Can LTS Collect?.....	80
10.1.3 Will LTS Stop Collecting Logs If I Disable "Continue to Collect Logs When the Free Quota Is Exceeded" in AOM?.....	80
10.1.4 How Do I Disable the Function of Collecting CCE Standard Output Logs to AOM?.....	81
10.2 Log Search and Check.....	81
10.2.1 How Often Is the Data Loaded in the Real-Time Log View?.....	81
10.2.2 What Can I Do If I Cannot View Raw Logs on the LTS Console?.....	81
10.2.3 Can I Manually Delete Logs?.....	82
10.3 Log Transfer.....	82
10.3.1 Does LTS Delete Logs That Have Been Transferred to OBS Buckets?.....	82
10.3.2 What Are the Common Causes of Abnormal Log Transfer?.....	82
10.3.3 How Do I Transfer CTS Logs to an OBS Bucket?.....	82
10.4 Others.....	83
10.4.1 How Do I Obtain an AK/SK Pair?.....	83

1 Service Overview

1.1 What Is LTS?

Log Tank Service (LTS) collects log data from hosts and cloud services. By processing a massive number of logs efficiently, securely, and in real time, LTS provides useful insights for you to optimize the availability and performance of cloud services and applications. It also helps you efficiently perform real-time decision-making, device O&M management, and service trend analysis.

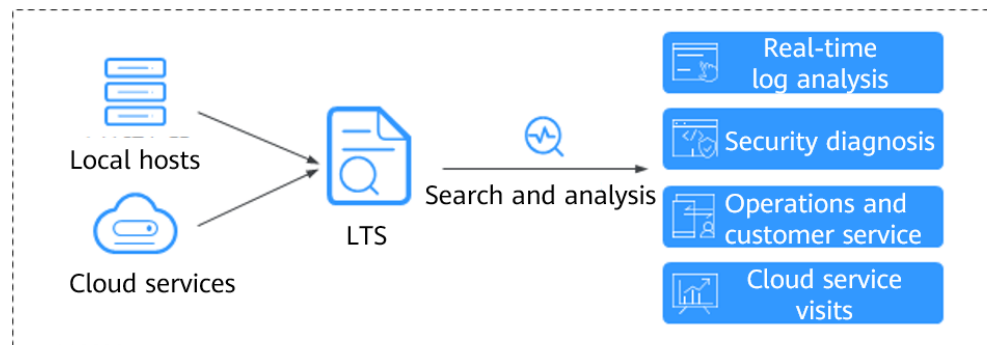
Figure 1-1 How LTS works



Log Collection and Analysis

LTS collects logs from hosts and cloud services, and displays them on the LTS console in an intuitive and orderly manner. You can transfer logs for long-term storage. Collected logs can be quickly queried by keyword or fuzzy match. You can analyze real-time logs for security diagnosis and analysis, or obtain operations statistics, such as cloud service visits and clicks.

Figure 1-2 Log collection and analysis



1.2 Basic Concepts

Log Groups

A log group is the basic unit for LTS to manage logs. You can query and transfer logs in log groups. Up to 100 log groups can be created in your account.

Log Streams

Up to 100 streams can be created in a log group.

You can separate logs into different log streams based on log types, and name log streams in an easily identifiable way. This helps you quickly find your desired logs.

1.3 Features

Real-time Log Collection

You can view real-time logs to keep track of the status of the services connected to LTS. You can also pre-view logs.

Log Query and Real-Time Analysis

You can set search criteria to filter reported logs for fault diagnosis and system tracking. This enables easier device O&M and service trend analysis.

Log Transfer

Reported logs are retained in LTS for 7 days by default. Retained logs are deleted once the period is over. For long-term storage, you can transfer logs to Object Storage Service (OBS) buckets.

1.4 Usage Restrictions

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

Table 1-1 Log read/write restrictions

Scope	Item	Description	Remarks
Account	Log write traffic	Logs can be written at up to 5 MB/s in an account.	To increase the upper limit, contact technical support engineers.
	Log writes	Logs can be written up to 1000 times per second in an account.	To increase the upper limit, contact technical support engineers.
	Log query	Up to 1 MB of logs can be returned in a single API query for an account.	To increase the upper limit, contact technical support engineers.
	Log reads	Logs can be read up to 100 times per minute in an account.	To increase the upper limit, contact technical support engineers.
Log group	Log write traffic	Logs can be written at up to 5 MB/s in a log group.	Not mandatory. Service quality cannot be ensured if this limit is exceeded.

Scope	Item	Description	Remarks
	Log writes	Logs can be written up to 100 times per second in a log group.	Not mandatory. Service quality cannot be ensured if this limit is exceeded.
	Log query traffic	Up to 10 MB of logs can be returned in a single API query for a log group.	N/A
	Log reads	Logs can be read up to 50 times per minute in a log group.	Not mandatory. Service quality cannot be ensured if this limit is exceeded.
Log stream	Log write traffic	Logs can be written at up to 5 MB/s in a log stream.	Not mandatory. Service quality cannot be ensured if this limit is exceeded.
	Log writes	Logs can be written up to 50 times per second in a log stream.	Not mandatory. Service quality cannot be ensured if this limit is exceeded.
	Log query traffic	Up to 10 MB of logs can be returned in a single API query for a log stream.	N/A
	Log reads	Logs can be read up to 10 times per minute in a log stream.	Not mandatory. Service quality cannot be ensured if this limit is exceeded.
	Log time	Logs in a period of 24 hours can be collected. Logs generated 24 hours before or after the current time cannot be collected.	N/A

1.5 Related Services

The relationships between LTS and other services are described in [Table 1](#).

Table 1-2 Relationships with other services

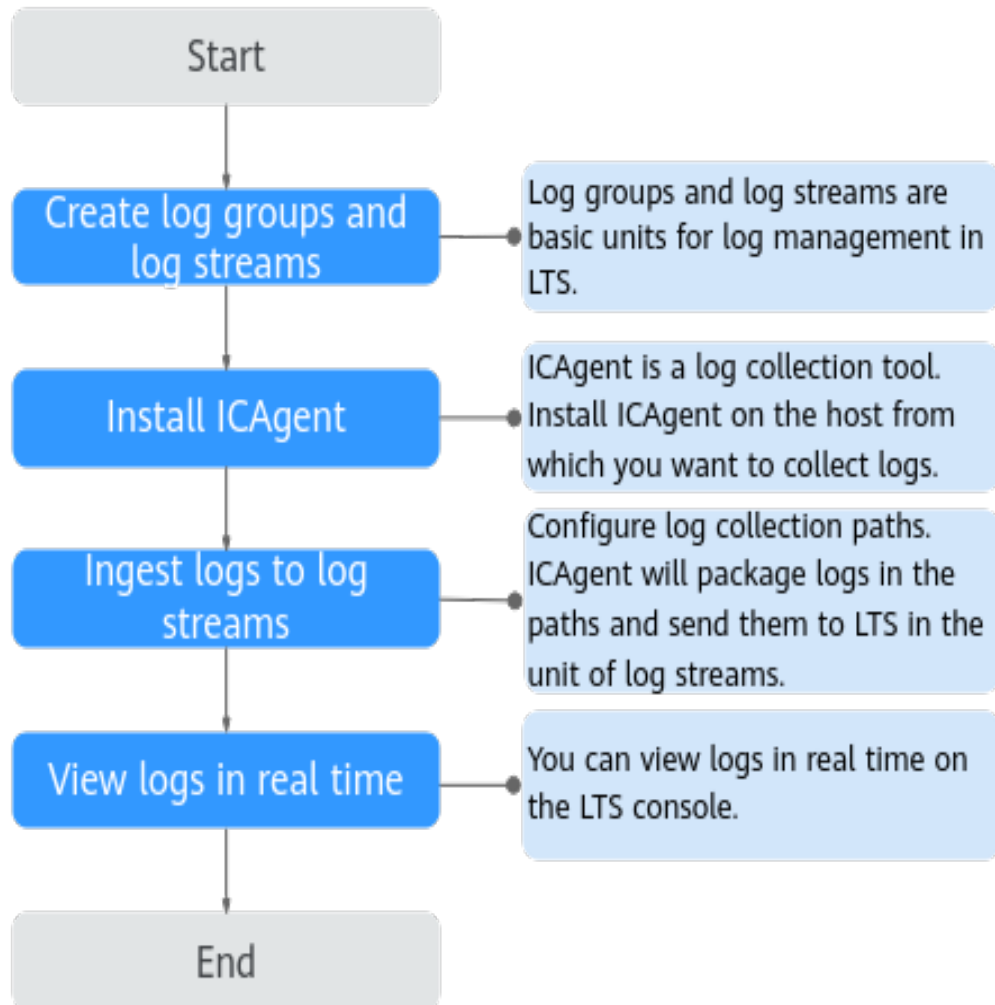
Interaction	Related Service
With Cloud Trace Service (CTS), you can record operations associated with LTS for future query, audit, and backtracking.	CTS
You can transfer logs to Object Storage Service (OBS) buckets for long-term storage, preventing log loss.	OBS
Application Operations Management (AOM)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

2 Getting Started

2.1 Overview

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

Figure 2-1 Flowchart



2.2 Step 1: Creating Log Groups and Log Streams

Log groups and log streams are basic units for log management in LTS. Before using LTS, create a log group and a log stream.

Prerequisites

You have obtained the username and 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.

Create Log Group

Log Group Name ?

Log Retention Duration ?

Remark

NOTE


Collected logs are sent to the log streams of the corresponding log groups. If there are a large number of logs, name log groups and log streams in an easily identifiable way so that you can quickly find the logs you desire.

A log group name:

- Can contain only letters, numbers, underscores (`_`), hyphens (`-`), and periods (`.`). The name cannot start with a period or underscore, or end with a period.
- Can contain 1 to 64 characters.

3. Set **Log Retention Duration** to 1 to 30 days. If this parameter is not specified, logs are retained for 7 days by default.
4. Enter remarks as required.
5. Click **OK**.

Creating a Log Stream

1. Click  on the left of a log group name.
2. Click **Create Log Stream**.
3. In the dialog box displayed, enter a log stream name.

Create Log Stream ?

Log Group Name k8s-log-7c4d1015-d1f2-11ed-bf8c-0255ac101f87

Log Stream Name ?

Remark

4. Enter remarks as required.
5. Click **OK**.

2.3 Step 2: Installing ICAgent

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

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

Prerequisites

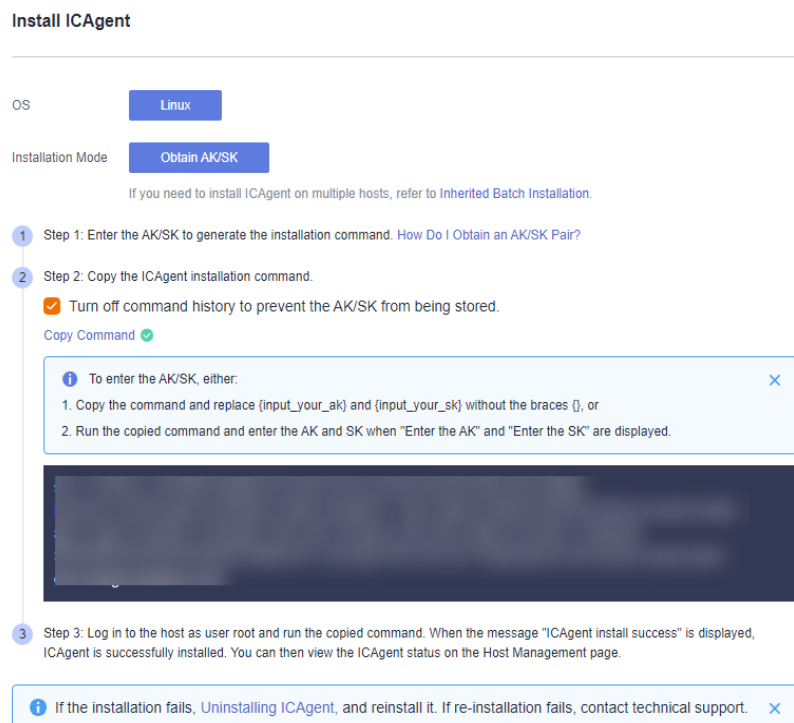
Before installing ICAgent, ensure that the time and time zone of your local browser are consistent with those of the host.

Installing ICAgent

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

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

Figure 2-2 Installing ICAgent



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

Step 4 Set **Installation Mode** to **Obtain AK/SK**.

NOTE

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

Step 5 Click **Copy Command** to copy the ICAgent installation command.

Step 6 Log in as user **root** to the host (for example, by using a remote login tool such as PuTTY). Run the copied command and enter the obtained AK/SK pair 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 on the **Hosts** tab of the **Host Management** page on the LTS console.

----End

2.4 Step 3: Ingesting Logs to Log Streams

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

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

Prerequisites

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

Procedure

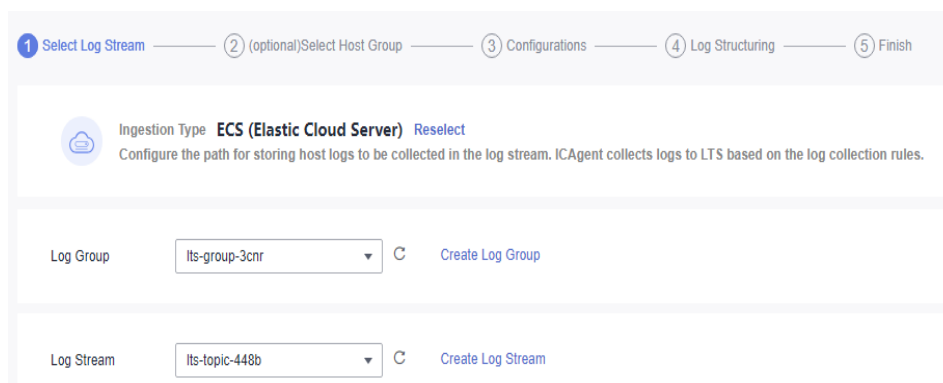
Step 1 Log in to the LTS console and choose **Log Ingestion** in the navigation pane.

Step 2 Click **ECS (Elastic Cloud Server)** to configure log ingestion.

Step 3 Select a log stream.

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

Figure 2-3 Selecting a log stream



Step 4 Select a host group.

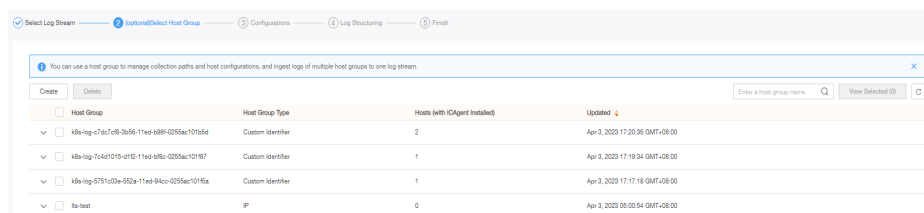
1. In the host group list, select one or more host groups to collect logs. If there are no desired host groups, click **Create** in the upper left corner of the list. On the displayed **Create Host Group** page, create a host group. For details, see [Creating a Host Group \(IP Address\)](#).

NOTE

You can choose not to select a host group in this step, but associate a host group with the ingestion configuration after you finish the procedure here. There are two options to do this:

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

2. Click **Next: Configurations**.

Figure 2-4 Selecting a host group

Step 5 Configure the collection.

1. Configure the collection parameters. For details, see [Configuring Collection](#).
2. Click **Submit**.

Step 6 (Optional) Configure structured logs.

Step 7 The operation is complete.

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

----End

2.5 Step 4: Viewing Logs in Real Time

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

Prerequisites

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

Viewing Logs in Real Time

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

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

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

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

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

 **NOTE**

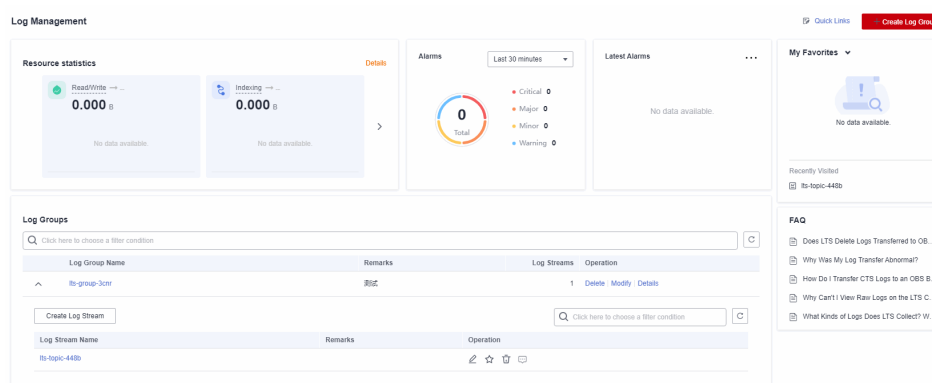
Stay on the **Real-Time Logs** tab to keep updating them in real time. If you leave the **Real-Time Logs** tab, logs will stop being loaded in real time.

3 Log Management

3.1 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.

Figure 3-1 LTS console

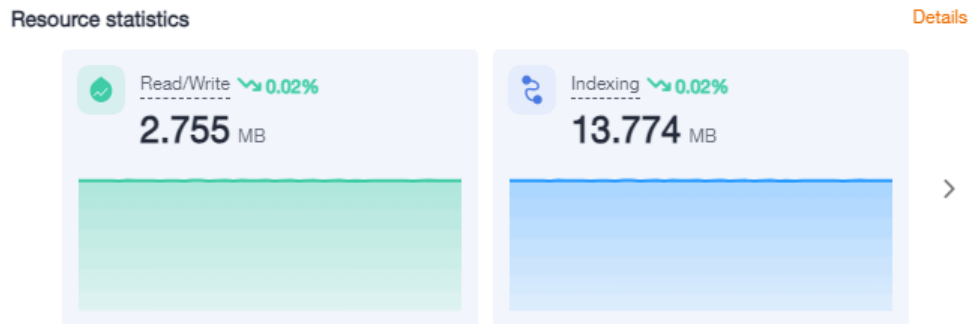


Resource Statistics

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

To view resource details, click **Details**.

Figure 3-2 Resource statistics



For details, see [Resource Statistics](#).

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 3-3 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 **...**.

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:

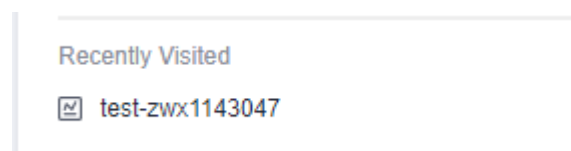
- In the log stream list, click  in the row containing a log stream.
- In the **My Favorites** area, hover the cursor over a log stream and click .

----End

Recently Visited

This area displays the log streams that are recently visited.

Figure 3-4 Recently Visited



 **NOTE**

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

FAQ

This area displays frequently asked questions.

Figure 3-5 FAQ

FAQ

- Does LTS Delete Logs Transferred to OB...
- Why Was My Log Transfer Abnormal?
- How Do I Transfer CTS Logs to an OBS B...
- Why Can't I View Raw Logs on the LTS C...
- What Kinds of Logs Does LTS Collect? W...

3.2 Resource Statistics

Log resource statistics are classified into read/write traffic, index traffic, raw log traffic, and log volume. 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.
- **Log Volume:** Space used for storing compressed logs, indexes, and copies is billed. The space is roughly the size of the raw logs.
- **Raw log traffic:** size of raw logs

Statistics

Figure 3-6 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 to the second. 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 exact current time to the minute. 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 time: queries log data that is generated in a specified time range.
- The read and write traffic, index traffic, log volume, and raw log traffic in the selected time range are displayed.
- Day-on-day changes in the selected time range are displayed. You can view the trend.
- The traffic (or log volume) 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 to the second. 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 exact current time to the minute. 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 time: 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

3.3 Managing Log Groups

A log group is a group of log streams that share the same log retention settings. Up to 100 log groups can be created for a single account.

Prerequisites

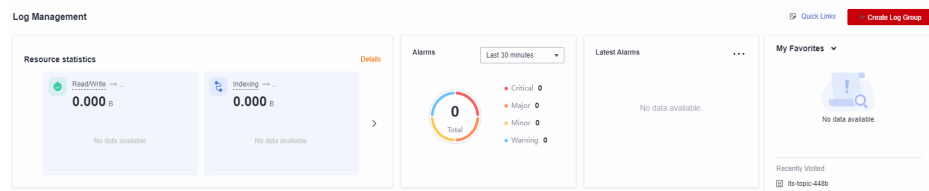
You have obtained an account and its password for logging in to the console.

Creating a Log Group

Log groups can be created in two ways. They are automatically created when other services interconnect with LTS, or you can create one manually by following the steps described here.

1. Log in to the LTS console, choose **Log Management** in the navigation pane on the left, and click **Create Log Group** in the upper right corner.

Figure 3-7 Creating a log group

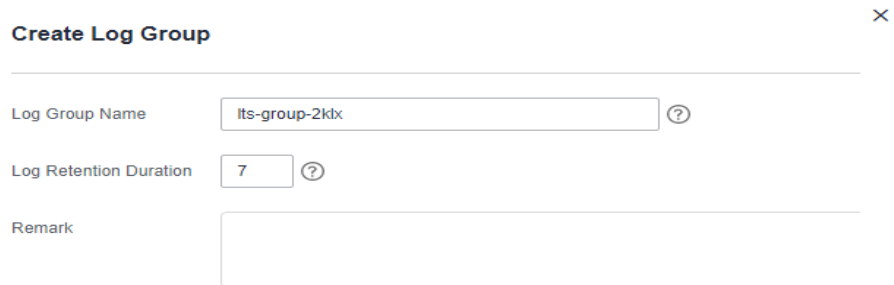


2. In the dialog box displayed, enter a log group name.

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. After a log group is created, its name cannot be changed.
 - 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. If this parameter is not specified, logs are retained for 7 days by default.

Figure 3-8 Creating a log group



Create Log Group ×

Log Group Name ?

Log Retention Duration ?

Remark

4. Enter remarks. The value contains 0 to 1024 characters.
5. Click **OK**.
 - 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.
 - Click **Details** in the **Operation** column of a log group to view details about the log group.

Modifying a Log Group

You can modify the log retention duration or remarks of a log group by performing the following steps:

1. In the log group list, locate the target log group and click **Modify** in the **Operation** column.
2. Modify the log storage duration on the displayed page.

Figure 3-9 Modifying a log group



Modify Log Group ×

Log Group Name/ID k8s-log-1675f7f0-00eb-11ee-90ac-0255ac100084
7e21af81-5d82-48a5-a2db-1a6881c70e9f

Log Retention Duration ?

Remark

3. Click **OK**.

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.

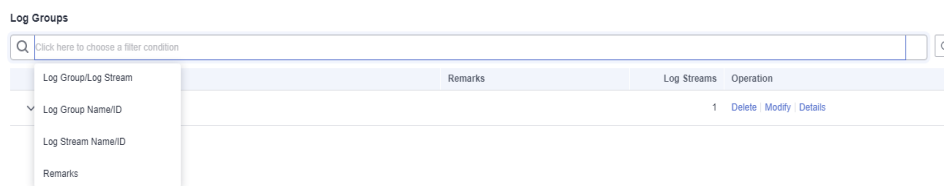
1. In the log group list on the **Log Management** page, locate the target log group and click **Delete** in the **Operation** column.
2. Enter **DELETE** and click **OK**.

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
- Remarks

Figure 3-10 Searching log groups/streams



Other Operations

To view the details of a log group, go to the log group list and click **Details** in the **Operation** column of the desired log group, including the log group name, ID, and creation time.

3.4 Managing 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.

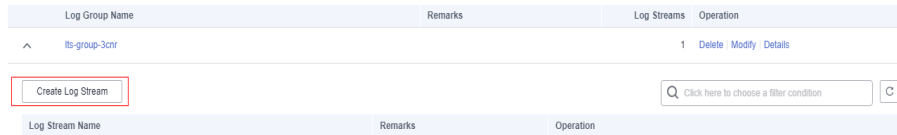
Prerequisites

You have created a log group.

Creating a Log Stream

Log streams can be created in two ways. They are automatically created when other services are connected to LTS, or you can create one manually by following the steps described here.

Figure 3-11 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.

Figure 3-12 Creating a log stream

Create Log Stream 

Log Group Name `k8s-log-c7dc7cf8-3b56-11ed-b98f-0255ac101b5d`

Log Stream Name 

Remark


NOTE

Collected logs are sent to the created log stream. If there are too many logs to collect, you are advised to separate logs into different log streams based on log types, and name log streams in an easily identifiable way.

3. Enter remarks. The value contains 0 to 1024 characters.
4. Click **OK**. In the log stream list, you can view information such as the log stream name and operations.

Modifying a Log Stream

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


1. In the log stream list, locate the target log stream and click  in the **Operation** column.
2. Modify log stream remarks.
3. Click **OK**.

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**.

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, log retention duration (days), creation type, and creation time.

4 Log Ingestion

4.1 Collecting Logs from Cloud Services

4.1.1 Collecting Logs from CCE

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

Prerequisites

- ICAgent has been **installed** and **added** to the host group.
- You have **disabled Output to AOM**.

Restrictions

- Currently, ServiceStage hosting is not supported.
- CCE cluster nodes whose container engine is Docker are supported.
- CCE cluster nodes whose container engine is Container 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 navigation pane on the left, choose **Log Ingestion** and 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. By default, four types of log streams can be collected from CCE clusters: standard output/error (**stdout-*{ClusterID}***), node file (**hostfile-*{ClusterID}***), and container file (**containerfile-*{ClusterID}***). 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**.

Four log streams can be created in a CCE cluster, including standard output/error (**stdout-*{ClusterID}***), node file (**hostfile-*{ClusterID}***), and container file (**containerfile-*{ClusterID}***). 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:** a one-click option to finish the previous settings.
- **Check Again:** Recheck dependencies.

 NOTE

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.

Step 5 (Optional) Select a host group.

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

 NOTE

- The host group to which the cluster belongs is selected by default. You can select another created host group 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 Log Structuring.

 NOTE

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

Step 8 The operation is complete.

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**

The collection path must be unique to a host.

Table 4-1 Configuration parameters

Parameter	Description
Container standard output	<p>Collects container standard output to AOM, and collects stderr and stdout logs of a specified container in the cluster.</p> <p>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 stdout or stderr must be enabled.</p>
Container file	<ul style="list-style-type: none"> • Collection Paths: LTS collects logs from the specified paths. <p>NOTE</p> <ul style="list-style-type: none"> • 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. • The collection path must be unique to a host. <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Collection Paths: LTS collects logs from the specified paths. <p>NOTE</p> <p>The collection path must be unique to a host.</p> <ul style="list-style-type: none"> • 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 path**.

Table 4-2 Kubernetes matching rules

Parameter	Description
Namespace Name Regular Expression	<p>Specifies the container whose logs are to be collected based on the namespace name. Regular expression matching is supported.</p> <p>NOTE LTS will collect logs of the namespaces with names matching this expression. To collect logs of all namespaces, leave this field empty.</p>
Pod Name Regular Expression	<p>Specifies the container whose logs are to be collected based on the pod name. Regular expression matching is supported.</p> <p>NOTE LTS will collect logs of the pods with names matching this expression. To collect logs of all pods, leave this field empty.</p>
Container Name Regular Expression	<p>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.</p> <p>NOTE LTS will collect logs of the containers with names matching this expression. To collect logs of all containers, leave this field empty.</p>
Container Label Whitelist	<p>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.</p> <p>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.</p>
Container Label Blacklist	<p>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.</p> <p>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.</p>
Container Label	<p>After the Container Label is set, LTS adds related fields to logs.</p> <p>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=lhs", "{app_alias: lhs}" will be added to the log.</p>

Parameter	Description
Environment Variable Whitelist	<p>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.</p> <p>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.</p>
Environment Variable Blacklist	<p>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.</p> <p>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.</p>
Environment Variable Label	<p>After the environment variable label is set, the log service adds related fields to the log.</p> <p>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=lhs", "{app_alias: lhs}" will be added to the log.</p>

4. **Advanced Settings:** Configure the log format and log time.

Table 4-3 Log collection settings

Parameter	Description
Log Format	<ul style="list-style-type: none"> • Single-line: Each log line is displayed as a single log event. • Multi-line: Multiple lines of exception log events can be displayed as a single log event. This is helpful when you check logs to locate problems.

Parameter	Description
Log Time	<p>System time: log collection time by default. It is displayed at the beginning of each log event.</p> <p>NOTE</p> <ul style="list-style-type: none"> 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. <hr/> <p>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.</p> <ul style="list-style-type: none"> 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. <p>NOTE If a log event does not contain year information, ICAgent regards it as printed in the current year.</p> <p>Example:</p> <pre> 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) </pre>
Log Segmentation	<p>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.</p>
Regular Expression	<p>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.</p>

 **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**.

4.1.2 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

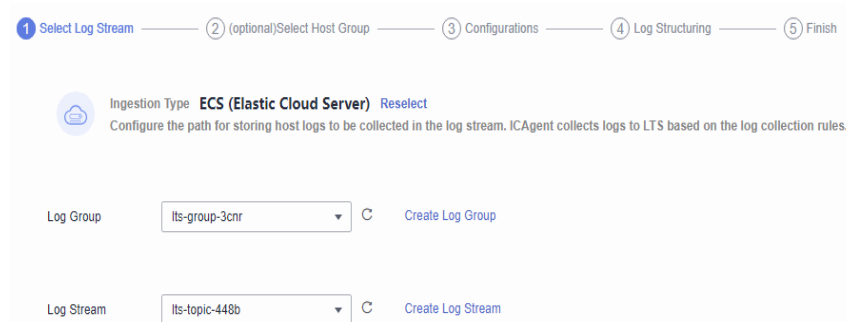
ICAgent has been **installed** and **added** to the host group.

Procedure

Perform the following operations to configure ECS log ingestion:

- Step 1** Log in to the LTS console.
- Step 2** In the navigation pane on the left, choose **Log Ingestion** and 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.

Figure 4-1 Selecting a log stream



- 3. Click **Next: (Optional) Select Host Group**.

- 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**.

Step 5 Configure collection.

Specify collection rules. For details, see [Configurations](#).

Step 6 (Optional) Configure log structuring.

For details, see Log Structuring.

 **NOTE**

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

Step 7 The operation is complete.

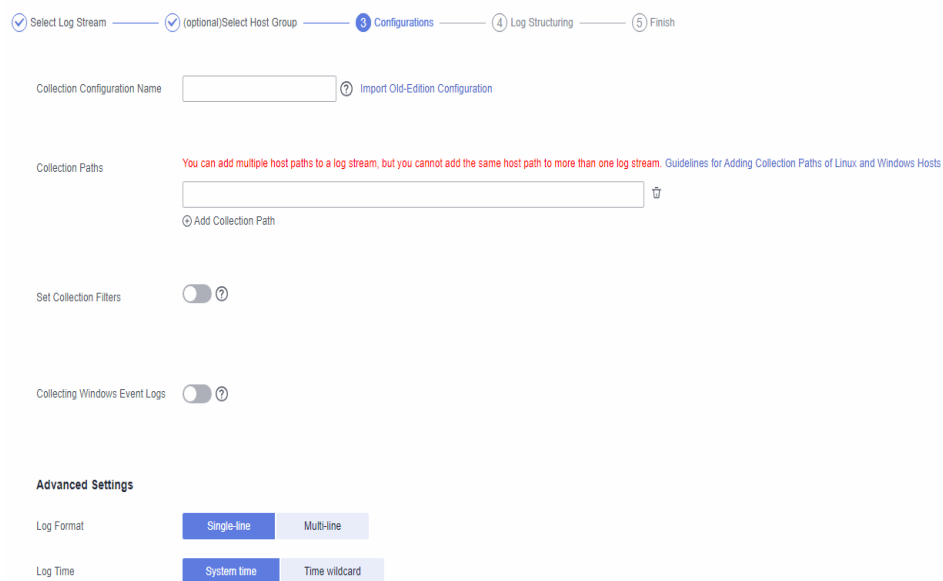
Click **Back to Ingestion Configurations** to [check the ingestion details](#). You can also click **View Log Stream** to view the log stream to which logs are ingested.

----End

Configurations

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


Figure 4-2 Configuring the collection



✓ Select Log Stream — (optional) Select Host Group — **3 Configurations** — 4 Log Structuring — 5 Finish

Collection Configuration Name [? Import Old-Edition Configuration](#)

Collection Paths You can add multiple host paths to a log stream, but you cannot add the same host path to more than one log stream. [Guidelines for Adding Collection Paths of Linux and Windows Hosts](#)



[+ Add Collection Path](#)

Set Collection Filters [?](#)

Collecting Windows Event Logs [?](#)

Advanced Settings

Log Format Single-line Multi-line

Log Time System time Time wildcard

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.

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.

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

Table 4-4 Parameters for collecting windows event logs

Parameter	Description
Log Type	Log types include system, program, security, and startup.
Offset from First Collection Time	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 Severity	The event severity can be information, warning, error, critical, or verbose. Filter and collect by Windows event level. Only Windows Vista or later is supported.

5. Configure the log format and log time.

Table 4-5 Log collection configurations

Parameter	Description
Log Format	<ul style="list-style-type: none"> • 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	<p>System time: log collection time by default. It is displayed at the beginning of each log event.</p> <p>NOTE</p> <ul style="list-style-type: none"> • 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. <p>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.</p> <ul style="list-style-type: none"> • 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. <p>NOTE If a log event does not contain year information, ICAgent regards it as printed in the current year.</p> <p>Example:</p> <pre> 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) </pre>
Log Segmentation	<p>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.</p>



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**.

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.
- To modify an ingestion configuration, click  in the **Operation** column for the target configuration and modify the configuration by referring to [Procedure](#).
- To delete an ingestion configuration, click  in the **Operation** column for the target configuration.


5 Host Management

5.1 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).
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**.
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 5-1 Operations on host groups

Operation	Procedure
Changing a host group name	<ol style="list-style-type: none"> On the Host Management page, the Host Groups tab is displayed by default. On the Host Groups tab, click  in the Operation column of the row containing the target host group. On the displayed dialog box, change the host group name and customized identifier. Click OK.
Adding hosts to a host group	<p>Method 1:</p> <ol style="list-style-type: none"> On the Host Management page, click the Host Groups tab, and click  in the row containing the target host group. Click Add Host. 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. <ul style="list-style-type: none"> 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. Click OK. <p>Method 2:</p> <ol style="list-style-type: none"> On the Host Management page, click the Hosts tab. In the host list, select the target hosts and click Add to Host Group. In the displayed slide-out panel, select the target host group. Click OK.
Removing a host from a host group	<ol style="list-style-type: none"> On the Host Management page, click the Host Groups tab, and click  in the row containing the target host group. In the host list, click Remove in the Operation column of the row containing the host to be removed. In the displayed dialog box, click OK. <p>NOTE This operation is not supported for hosts in the custom identifier host group.</p>

Operation	Procedure
Uninstalling ICAgent from a host	<ol style="list-style-type: none"> 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. <p>NOTE</p> <ul style="list-style-type: none"> • This operation is not supported for hosts in the custom identifier host group. • If the host has also been added to other host groups, it will be removed from those groups as well.
Removing hosts from a host group	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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.
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**.

5.2 Managing Hosts

5.2.1 Installing ICAgent

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.

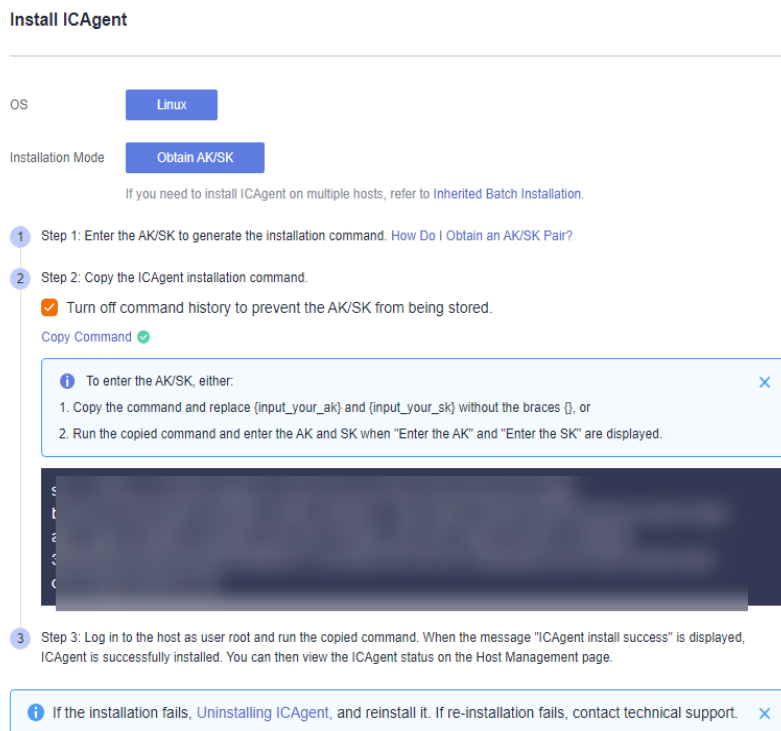
Table 5-2 Installation methods

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 5-1 Installing ICAgent



Step 3 Set OS to Linux.

Step 4 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.

Step 5 Click **Copy Command** to copy the ICAgent installation command.

Step 6 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/remotelInstall/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/remotelInstall/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**.

5.2.2 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 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

- You need to create a CCE cluster before you can collect container standards and send them to AOM.
 - To disable the function of exporting container standards to AOM, you need to have ICAgent 5.12.133 or later.
 - 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.

5.2.3 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.

5.2.4 ICAgent Statuses

The following table lists the ICAgent statuses.

Table 5-3 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.

Status	Description
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.

6 Log Search and View

6.1 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. In the upper right corner, 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 time: 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 in the search box. The drop-down list contains the following items:
 - Structured fields or index fields: Built-in fields are not displayed in the drop-down list. However, when you enter a built-in field, the drop-down list is automatically associated and matched with the field.
 - **NOT, AND, OR, :, and :* keywords can be displayed. Keywords other than NOT are displayed in the drop-down list only after you enter the keyword in the search box.**

 NOTE

- When entering a keyword, you can press **Tab** to automatically add the first keyword displayed in the drop-down list.
 - Keywords are case-insensitive.
- Historical records: A maximum of 20 historical records can be retained, but only the latest three records are displayed in the drop-down list.
 - Quick search: quick search fields that have been created.
 - Search syntax: common search syntax.

Enter a keyword, or select a field and keyword from the drop-down list, and click **Query**.

Logs that contain the keyword are displayed.

 NOTE

- Built-in fields include **appName**, **category**, **clusterId**, **clusterName**, **collectTime**, **containerName**, **hostIP**, **hostIPv6**, **hostId**, **hostName**, **nameSpace**, **pathFile**, **podName** and **serviceID**. By default, the fields are displayed in simplified mode, and **hostIP**, **hostName**, and **pathFile** are displayed at the beginning.
 - The structured 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 6-1 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.

Operation	Description
Refreshing logs	<p>You can click  to refresh logs in two modes: manual refresh and automatic refresh.</p> <ul style="list-style-type: none"> 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	<p>Click  to copy the log content.</p>
Viewing context of a log	<p>Click  to view the log context.</p>
Simplifying field details	<p>Click  to view the simplified field details.</p>
Unfold/Fold	<p>Click  to display all the log content. Click  to fold the log content.</p> <p>NOTE Unfold is enabled by default.</p>
Downloading logs	<p>Click . On the displayed Download Logs page, click Direct Download.</p> <p>Direct Download: Download log files to the local PC. Up to 5000 logs can be downloaded at a time.</p> <p>Select .csv or .txt from the drop-down list and click Download to export logs to the local PC.</p> <p>NOTE</p> <ul style="list-style-type: none"> 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	<p>Click  to set the number of lines displayed in the log content. Click  to close it.</p> <p>NOTE By default, logs are not collapsed, and two rows of logs are shown after collapsing. You can display up to six rows.</p>
Layout	<p>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.</p> <ul style="list-style-type: none"> 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.

Operation	Description
JSON	<p>Move the cursor over , click JSON, and set JSON formatting.</p> <p>NOTE Formatting is enabled by default. The default number of expanded levels is 2.</p> <ul style="list-style-type: none"> • Formatting enabled: Set the default number of expanded levels. Maximum value: 10. • Formatting disabled: JSON logs will not be formatted for display.
Invisible fields ()	<p>This list displays the invisible fields configured in the layout settings.</p> <ul style="list-style-type: none"> • 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 6-2 Search syntax

Filter	Description
Exact search by keyword	<p>LTS searches for logs containing the exact keyword (case-sensitive) that you specify. A keyword is the word between two adjacent delimiters.</p> <p>You can add an asterisk (*) after a keyword, for example, error*, if you are not familiar with delimiters.</p>
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.

Filter	Description
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 .
""	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.

Filter	Description
()	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-insensitive.
- 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.

6.2 Cloud Structuring Parsing

6.2.1 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.

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](#)

You can then use SQL statements to query structured logs in the same way as you query data in two-dimensional database tables.

 **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.

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

6.2.2 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 time: 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 time:** 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"}
```

The following fields will be extracted:

Figure 6-1 Extraction results

You can choose one of the following five methods to structure logs.



Parse the log body in JSON format and split it into key-value pairs.

Step 1 Select a sample log event.

Select from existing log events

Step 2 Extract fields.

Intelligent Extraction

Content Fields Tag Fields

Field	Source	Type	Example Value	Alias	Quick Analysis	Operation
a1	Content Fields	string	a1	-	<input checked="" type="checkbox"/>	
b1	Content Fields	string	b1	-	<input checked="" type="checkbox"/>	
c1	Content Fields	string	c1	-	<input checked="" type="checkbox"/>	
d1	Content Fields	string	d1	-	<input checked="" type="checkbox"/>	

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 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 time: 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
```

The following fields will be extracted:

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 time: 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";
```

The following fields will be extracted:

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](#).

6.2.3 Structuring Templates

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

System Templates

System templates: ELB, VPC, CTS, APIG, DCS (audit logs), Tomcat, Nginx, GAUSSV5 audit logs, DDS (audit, error, and slow logs), CFW (access control, attack, and traffic logs), MySQL (error and slow logs), PostgreSQL (error and slow logs), SQL Server error logs, GAUSSDB_REDIS slow logs, CDN, SMN, GaussDB_MySQL (error and slow logs), ER, MySQL audit logs, GaussDB(forCassandra) slow logs, GaussDB(forMongo) (slow and error logs)

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.

6.2.4 Log Structuring Fields

Setting Log Structuring Fields

You can edit extracted fields after log structuring.

Table 6-3 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)	<ul style="list-style-type: none"> • 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

Structuring Method	Field Name	Field Type Can Be Changed	Field Can Be Deleted
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
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

Structuring Method	Field Name	Field Type Can Be Changed	Field Can Be Deleted
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
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


6.3 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 a log stream name. The log stream details page is displayed.
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.

6.4 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 6-4 Introduction to log context viewing

Feature	Description
Search Rows	Number of rows to search. The options are 100, 200, and 500.
Highlighting	Enter a string to be highlighted and press Enter .

Feature	Description
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.

6.5 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 performed 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:


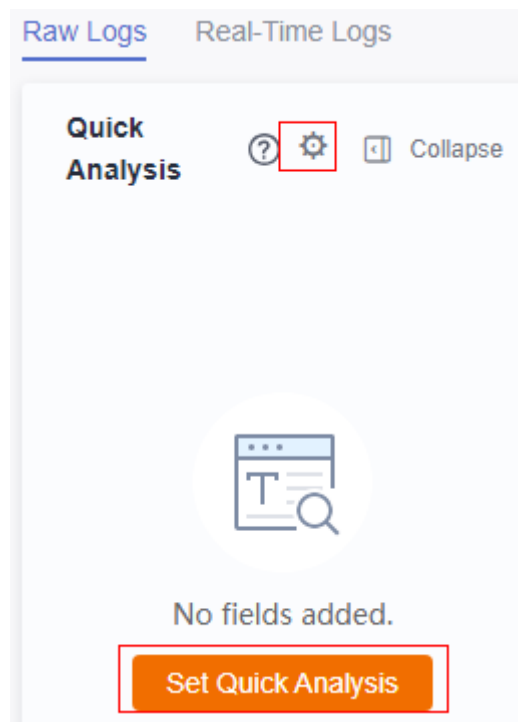




- Step 1** Log in to the LTS console. In the navigation pane on the left, choose **Log Management**.
- Step 2** A quick analysis is performed on a log stream. Select the target log group and log stream on the **Log Management** page.
- Step 3** On the **Raw Logs** tab page, click **Set Quick Analysis** or . On the displayed page, add fields for quick analysis.

Figure 6-2 Creating a quick analysis task



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

NOTE

-  indicates a field of the **string** type.
-  indicates a field of the **float** type.
-  indicates a field of the **long** type.
- The maximum length of a field for quick analysis is 2000 bytes.
- The quick analysis field area displays the first 100 records.
- Click  in the upper right corner of the **Quick Analysis** area to modify or delete an existing field. If you delete a field or modify the name of a field on the **Log Structuring** page, the field will be updated in the quick analysis.

----End

7 Log Alarms

7.1 Alarm Rules

7.1.1 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 7-1 Alarm rule parameters

Parameter	Description	Verification Rule	Example Value
Rule Name	Name of the alarm rule.	The 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.	Enter up to 64 characters.	-
Statistics	Select By keyword .	-	By keyword
Log Group Name	Select a log group.	-	-
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
Query Time Range	Time range for the keyword query, which is one period earlier than the current time. For example, if the 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. <ul style="list-style-type: none"> 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 h

Parameter	Description	Verification Rule	Example Value
Query Frequency	<p>The options for this parameter are:</p> <ul style="list-style-type: none"> ● 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. <p>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.</p> <ul style="list-style-type: none"> ● CRON: CRON expressions support schedules down to the minute and use 24-hour format. Examples: <ul style="list-style-type: none"> - 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 run at 14:00 every day. 	-	Daily 01:00

Parameter	Description	Verification Rule	Example Value
	<ul style="list-style-type: none"> 0 0 10 * *: The query is run at 00:00 on the 10th day of every month. 		
Matching Log Events	<p>When the number of log events that contain the configured keywords reaches the specified value, an alarm is triggered.</p> <p>Four comparison operators are supported: greater than (>), greater than or equal to (>=), less than (<), and less than or equal to (<=).</p>	The minimum value is 1 and the maximum value is 2147483647.	>10
Triggers	<p>Configure a condition that will trigger the alarm.</p> <p>Specify the number of statistical periods and the number of times the condition must be met to trigger the alarm. The number of statistical periods must be greater than or equal to the number of times the condition must be met.</p>	Statistical periods: 1-10	4, 2
Alarm Severity	Possible values are critical (default), major , minor , and info .	-	critical
Send Notifications	Possible values are No (default) and Yes .	-	No
SMN Topic	<p>If you select Yes for Send Notifications, select a Simple Message Notification (SMN) topic. You can select multiple topics.</p> <p>If there are no topics that you desire, click Create Topic.</p> <p>If you want to change the time zone or language, click Modify and set the preferences in the account center.</p>	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 page displayed, click the **Raw Logs** tab and click  in the upper right corner. On the **Settings** page displayed, click the **Alarms Rules** tab and **Create** to create an alarm rule.

 NOTE

After an alarm rule is created, **Status** is enabled by default. When **Status** is enabled, an alarm will be triggered if the alarm rule is met. When **Status** is disabled, an alarm will not be triggered even if the alarm rule is met.

----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 7-1](#). **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, and click **OK**.

----End

7.2 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 alarm rules. For details, see [Configuring Keyword Alarms](#).

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 time: 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  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

8 Log Transfer

8.1 Overview

Logs reported from hosts and cloud services are retained in LTS for seven days by default. You can set the retention period to 1 to 30 days. Retained logs are deleted once the retention period is over. For long-term retention, you can transfer logs to Object Storage Service (OBS).

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.

8.2 Transferring Logs to OBS

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

NOTE

- Currently, this function is available only to whitelisted users. To use this function, you need to submit a service ticket. For details, see .
- 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

1. Log in to the LTS console and choose **Log Transfer** in the navigation pane on the left.
2. Click **Configure Log Transfer** in the upper right corner.
3. On the displayed page, configure the log transfer parameters.

 **NOTE**

After a transfer task is created, you can modify parameters except the log group name, transfer destination, and log stream name.

Table 8-1 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
Log Stream Name	Select a log stream.	N/A
OBS Bucket	<ul style="list-style-type: none"> • Select an OBS bucket. <ul style="list-style-type: none"> – If no OBS buckets are available, click View OBS Bucket to access the OBS console and create an OBS bucket. – If encryption has been enabled for the selected OBS bucket, select a key name and select I agree to grant permissions on Key Management Service (KMS) to LTS so LTS can create and use keys to encrypt and decrypt transferred logs. • Currently, LTS supports only Standard OBS buckets. 	N/A
Key Name	Select a key name for an OBS bucket for which encryption has been enabled. If no keys are available, click Create Key and Authorize to go to the Data Encryption Workshop (DEW) console and create a key.	N/A

Parameter	Description	Example Value
Custom Log Transfer Path	<ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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: <ol style="list-style-type: none"> If you enter LTS-test/%Y/%m/%done/%H/%m, the path is LogTanks/Region name/LTS-test/Y/m/done/H/m/Log file name. 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
Log Prefix	<p>The file name prefix of the log files transferred to an OBS bucket</p> <p>The prefix must meet the following requirements:</p> <ul style="list-style-type: none"> Can contain 0 to 64 characters. Can contain only letters, digits, hyphens (-), underscores (_), and periods (.). <p>Example: If you enter LTS-log, the log file name will be LTS-log_Log file name.</p>	LTS-log

Parameter	Description	Example Value
Format	<p>The storage format of logs. The value can be Raw Log Format or JSON.</p> <ul style="list-style-type: none"> Examples of the raw log format: (Logs displayed on the LTS console are in the raw format.) <pre>Sep 30 07:30:01 ecs-bd70 CRON[3459]: (root) CMD (/opt/oss/servicemgr/ICAgent/bin/manual/mstart.sh > /dev/null 2>&1)</pre> The following is an example of the JSON format: <pre>{"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}</pre> 	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

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

Modifying a Log Transfer Task

- Locate the row that contains the target transfer task and click **Modify** in the **Operation** column.
- Click **OK**.

Viewing Transfer Details

- Locate the target log transfer task and click **Details** in the row of the desired task to view the task details.
- 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.
 - The key for the encrypted OBS bucket has been deleted or the authorization has been canceled. Ensure that the key is valid.
- **Disabled:** The log transfer task is stopped.

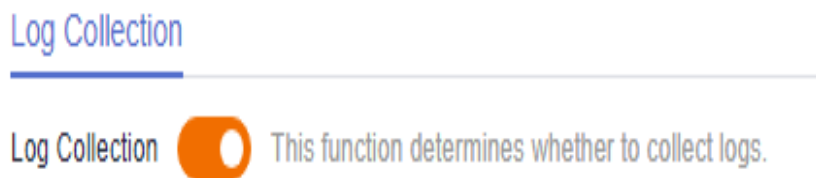
9 Configuration Center

9.1 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**.

Figure 9-1 Enabling or disabling 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

10 FAQs

10.1 Log Collection

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

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

10.1.2 What Kind of Logs and Files Can LTS Collect?

Logs That Can Be Collected by LTS:

- Host logs. ICAgent should be installed on the target hosts for log collection.
- Cloud service logs. To collect logs from cloud services enable log reporting to LTS in the cloud services.

Files That Can Be Collected by LTS:

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

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

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

10.1.4 How Do I Disable the Function of Collecting CCE Standard Output Logs to AOM?

Symptom

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

NOTE

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

Solution

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

Step 2 Choose **Hosts** and click **CCE Cluster**.

Step 3 In the CCE cluster, select the CCE cluster, and disable **Output to AOM**.

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

----End

10.2 Log Search and Check

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

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

10.2.2 What Can I Do If I Cannot View Raw Logs on the LTS Console?

Symptom

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

Possible Causes

- ICAgent has not been installed.
- The collection path is incorrectly configured.

- The **Log Collection** function on the LTS console is disabled.
- Log collection was stopped because your account is in arrears.
- The rate of writing logs into log streams or length of single-line logs exceeds what is supported.
- The browser has slowed down because of the amount of log data.

Solution

- Install the ICAgent. For details, see [Installing ICAgent](#).
- If the collection path is set to a directory, for example, `/var/logs/`, only **.log**, **.trace**, and **.out** files in the directory are collected. If the collection path is set to name of a file, ensure that the file is a text file.
- Log in to the LTS console, choose **Configuration Center > Log Collection**, and enable the **Log Collection** function.
- Use Google Chrome or Firefox to query logs.

10.2.3 Can I Manually Delete Logs?

No. Manual deletion is not supported. Logs are automatically deleted when their retention period ends.

10.3 Log Transfer

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

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

10.3.2 What Are the Common Causes of Abnormal Log Transfer?

- The OBS bucket used for log transfer has been deleted. Specify another bucket.
- Access control on the OBS bucket is incorrectly configured. Go to the OBS console to correct the settings.

10.3.3 How Do I Transfer CTS Logs to an OBS Bucket?

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

1. Log in to the CTS console and choose **Tracker List** in the navigation pane on the left.

2. Click **Configure** in the row of the tracker **system**.
3. Select an OBS bucket under **Transfer to OBS**.

Configure Tracker

Transfer to OBS

The CTS console stores traces generated in the last 7 days. To store the traces for a longer duration, transfer them to OBS.

* Transfer Trace to OBS Yes No

* OBS Bucket Account Logged-in user Other users [?](#)

* OBS Bucket [View Bucket](#)

OBS will grant read and write permissions to CTS and LTS for the selected bucket. When modifying the bucket policy, ensure that CTS has read and write permissions for the bucket to prevent log transfer failures.

File Prefix [?](#)

This prefix is added to trace files to help you distinguish them from other files in the OBS bucket.

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

10.4 Others

10.4.1 How Do I Obtain an AK/SK Pair?

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

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

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

Procedure

1. Log in to the console, hover the mouse pointer over the username in the upper right corner, and select **My Credentials** from the drop-down list.
2. On the **My Credentials** page, choose **Temporary Access Key**.
3. On the page displayed, click **Create** in the **Operation** column to generate an access key.

 **NOTE**

Keep the AK/SK pair secure.