Log Tank Service

User Guide

Issue	01
Date	2024-04-29

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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.

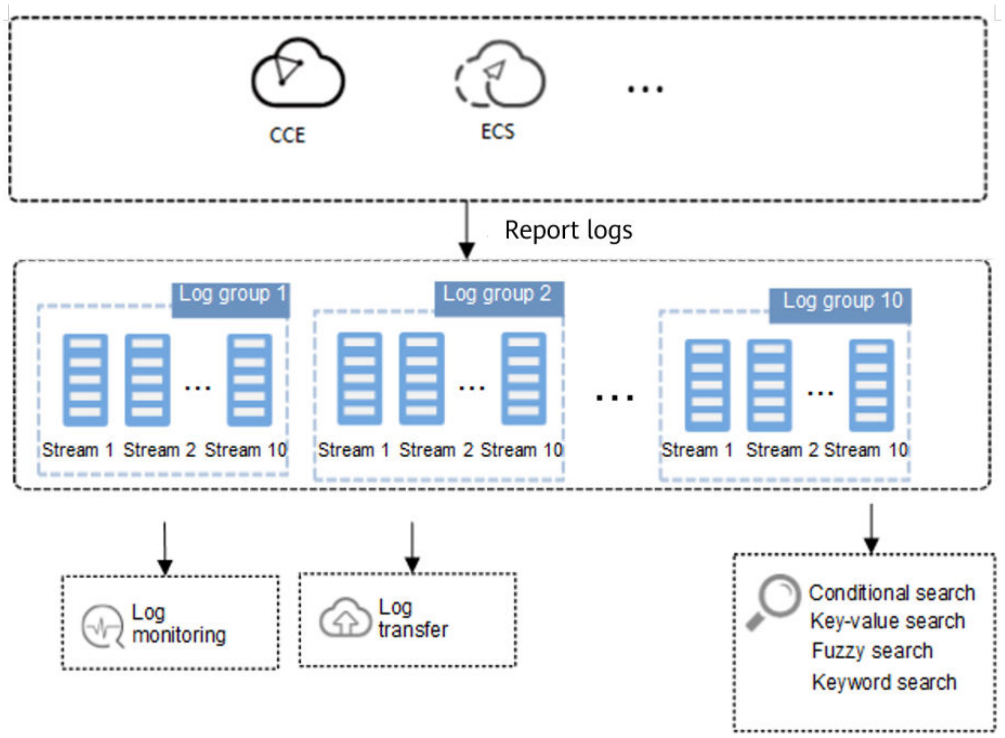
Contents

1 Service Overview

1.1 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.

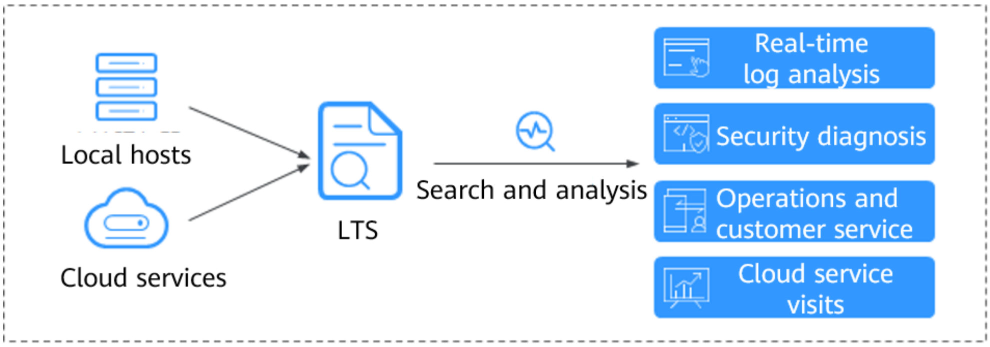
Figure 1-1 How LTS works



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 Features

Real-time Log Collection

LTS collects real-time logs and displays them on the LTS console in an intuitive and orderly manner. You can query logs or transfer logs for long-term storage.

Collected logs can be structured for analysis. To be specific, LTS extracts logs that are in a fixed format or share a similar pattern based on the extraction rules you set. Then you can use SQL syntax to query the structured logs.

Log Query and Real-Time Analysis

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.

Log Transfer

You can customize the retention period of logs reported from ECS and cloud services to LTS. Logs older than the retention period will be automatically deleted. For long-term storage, you can transfer logs to Object Storage Service (OBS). Log transfer is to replicate logs to the target cloud service. It means that, after log transfer, the original logs will still be retained in LTS until the configured retention period ends.

1.3 Application Scenarios

Log Collection and Analysis

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

Service Performance Optimization

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

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

Quickly Locating Network Faults

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

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

1.4 Usage Restrictions

1.4.1 Basic Resources

This section describes restrictions on LTS basic resources.

Table 1-1 Basic resource restrictions

Item	Description	Remarks
Log groups	Up to 100 log groups can be created in an account.	N/A
Log streams	Up to 100 log streams can be created in a log group. **NOTE** The log stream name must be unique.	N/A
Log retention	By default, logs are retained for seven days. The retention duration ranges from one to seven days.	N/A
Host groups	Up to 200 host groups can be created in an account.	N/A
Quick searches	Up to 10 quick searches can be created in a log stream.	N/A
LogItem (Single-line log event)	Using APIs: A single-line log event should be at most 1 MB during ingestion.	N/A
	Using APIs: A single-line log event can contain up to 100 labels.	N/A
	Using ICAgent: A single-line log event should be at most 500 KB during ingestion.	N/A

1.4.2 Log Read/Write

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

Table 1-2 Log read/write restrictions

Category	Item	Description	Remarks
A complete LTS	Number of new logs per day	The number of new logs per day in a complete LTS is limited by the number of vCPUs and log scale-out packages for AOM you purchased. ● Every 100 vCPUs include 50 GB new logs per day. ● Multiple log scale-out packages A maximum of 80 TB new logs per day are supported.	For example: If you purchase 1000 vCPUs and two log scale-out packages with 100 GB per day, restrictions are as follows: ● New logs per day: 500 GB/day (comes with the 1000 vCPUs) + 100 GB/day x 2 log scale-out packages = 700 GB/day ● Steady log rate: 700 GB/day x 1024/24 hours/3600 seconds = 8.3 MB/s ● Peak log rate: 8.3 x 2 = 16.6 MB/s When the usage exceeds the licensed limit, LTS generates an alarm and may limit the traffic rate. If you need higher specifications, purchase a log scale-out package and upgrade.
	Steady log rate	Steady log rate = Number of new logs per day/24 hours/3600 seconds The maximum steady rate is 1000 MB/s.	
	Peak log rate	Peak log rate = 2 x steady log rate The maximum peak rate is 2000 MB/s.	

Category	Item	Description	Remarks
	Log writes	The number of writes is less than 1000 or the number of new logs per day/1 TB x 1000 (whichever is larger) in a complete LTS. The maximum log writes are 10,000 times per second.	N/A
	Log query	Up to 10 MB of logs are returned in a single API query in a complete LTS.	N/A
	Log reads	Logs can be read up to 600 times per minute in a complete LTS.	N/A
Log group	Number of new logs per day	The total number of new logs in all log groups cannot exceed the limit set in a complete LTS.	N/A
	Steady log rate	The total number of new logs in all log groups cannot exceed the limit set in a complete LTS.	N/A
	Peak log rate	The total number of new logs in all log groups cannot exceed the limit set in a complete LTS.	N/A
	Log reads	Logs are read up to 500 times per minute in a log group. N/A	N/A
	Log writes	The total number of new logs in all log groups cannot exceed the limit set in a complete LTS.	N/A
	Log query	Up to 10 MB of logs are returned in a single API query for a log group.	N/A
	Log reads	The total number of new logs in all log groups cannot exceed the limit set in a complete LTS.	N/A
Log stream	Number of new logs per day	The total number of new logs in all log streams cannot exceed the limit set in a complete LTS.	N/A
	Steady log rate	The total number of new logs in all log streams cannot exceed the limit set in a complete LTS.	N/A

Category	Item	Description	Remarks
	Peak log rate	The total number of new logs in all log streams cannot exceed the limit set in a complete LTS.	N/A
	Log writes	The total number of new logs in all log streams cannot exceed the limit set in a complete LTS.	N/A
	Log query	Up to 10 MB of logs are returned in a single API query for a log stream.	N/A
	Log reads	The total number of new logs in all log streams cannot exceed the limit set in a complete LTS.	N/A
	Log time	Logs in a period of 48 hours can be collected. Logs generated 48 hours before or after the current time cannot be collected. For example: ● If the current time is 11:00 on January 7, 2022, logs generated before 11:00 on January 5 cannot be collected. ● If the current time is 11:00 on January 7, 2022, logs generated after 11:00 on January 9 cannot be collected.	N/A

1.4.3 ICAgent

This section describes the restrictions on the log collector ICAgent.

Table 1-3 ICAgent file collection restrictions

Item	Description	Remarks
File encoding	UTF 8 is supported. Other encoding formats may cause garbled characters. You can configure whether to collect log files containing binary content. Binary characters may be displayed as garbled characters.	N/A
Host type	Only logs of Linux hosts can be collected.	N/A

Item	Description	Remarks
Log file size	Unlimited	N/A
Log file rotation	ICAgent supports configuration of fixed log file names or fuzzy match of log file names. You need to rotate log files manually.	N/A
Log collection path	**Linux** ● Collection paths support recursion. You can use double asterisks (**) to collect logs from up to five directory levels. Example: **/var/logs/**/a.log** ● Collection paths support fuzzy match. You can use an asterisk (*) to represent one or more characters of a directory or file name. Example: **/var/logs/*/a.log** or **/var/logs/service/a*.log** ● 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 text file, that file is directly collected. ● Each collection path must be unique. That is, the same path of the same host cannot be configured for different log groups and log streams.	N/A
Symbolic link	Symbolic links are not supported.	N/A
Single log size	Configure whether log splitting is supported. A log cannot exceed 500 KB. If a log exceeds 500 KB, the extra part will be truncated and discarded. If log splitting is enabled, a log exceeding 500 KB will be split into multiple logs for collection. For example, a 600 KB log will be split into a 500 KB log and a 100 KB log. Only Linux hosts and single-line logs are supported.	N/A
Regular expression	Perl regular expressions are supported.	N/A

Item	Description	Remarks
File collection configuration	A file can be reported to only one log group and stream. If a file is configured for multiple log streams, only one configuration takes effect.	N/A
File opening	Files are opened when being read, and closed after being read.	N/A
First log collection	All logs are collected.	N/A

Table 1-4 ICAgent performance specifications

Item	Description	Remarks
Log collection rate	Raw logs of a single node are collected at a rate up to 50 MB/s.	Service quality cannot be ensured if this limit is exceeded.
Monitored directories	Up to five levels of directories are supported, with up to 1000 files.	N/A
Monitored files	Container scenarios ● The ICAgent can collect a maximum of 20 log files from a volume mounting directory. ● The ICAgent can collect a maximum of 1000 standard container output log files. These files must be in JSON format. VM scenarios ● A maximum of 1000 files are supported.	N/A

Item	Description	Remarks
Default resource restrictions	CPU: Max. two CPU cores Memory: Max. min{4 GB, Physical memory/2}. A restart is triggered if this memory limit is exceeded. "min{4 GB, Physical memory/2}" means that the smaller value between half of the physical memory and 4 GB is used.	N/A
Resource limit reached	A forcible restart is triggered. Logs may be lost or duplicate if rotated during the restart.	N/A
Agent installation, upgrade, or uninstallation	Unlimited	N/A

Table 1-5 Other restrictions on ICAgent

Item	Description	Remarks
Configuration update	Configuration updates take effect in 1 to 3 minutes.	N/A
Dynamic configuration loading	Console configurations can be dynamically delivered. The update of one configuration does not affect other configurations.	N/A
Configurations	Unlimited	N/A
Tenant isolation	Tenants are isolated from each other by default.	N/A
Log collection delay	Normally, the delay from writing logs to the disk to collecting the logs is less than 2s (congestion not considered).	N/A

Item	Description	Remarks
Log upload	File changes are read and uploaded immediately once detected. One or more logs can be uploaded a time.	N/A
Network error handling	Network exceptions trigger retries at an interval of 5s.	N/A
Resource quota used up	If the resources allocated to the ICAgent are insufficient due to massive amounts of logs, the ICAgent continues and retries upon a failure. Logs will be stacked if resources are still insufficient.	N/A
Max. retry timeout	Retry attempts are periodically made.	N/A
Status check	The collector status is monitored through heartbeat detection.	N/A
Checkpoint timeout	Checkpoints are automatically deleted if no updates are made within 12 hours.	N/A
Checkpoint saving	Checkpoints are updated if logs are reported successfully.	N/A
Checkpoint saving path	The default save path: */var/share/oss/manager/ICProbeAgent/internal/TRACE*	N/A

Item	Description	Remarks
Log loss Duplicate logs	ICAgent uses multiple mechanisms to ensure log collection reliability and prevent data loss. However, logs may be lost in the following scenarios: ● Log files are rotated at a high speed, for example, once per second. ● Logs cannot be forwarded due to improper system security settings or syslog itself. ● The container running time, for example, shorter than 30s, is extremely short. ● A single node generates logs at a high speed, exceeding the allowed transmit bandwidth or log collection speed. It is recommended that the log generation speed of a single node is lower than 50 MB/s. When the ICAgent is restarted, identical data may be collected around the restart time.	N/A

1.4.4 Search and Analysis

This section describes the restrictions on LTS query and analysis.

Search

Table 1-6 Log search restrictions

Item	Description	Remarks
Delay from log collection to search	Logs can be searched on the console within 2 minutes after being generated (congestion not considered).	N/A
Keywords	Keywords are conditions excluding Boolean logic operators during query. Up to 30 keywords are supported for a query.	N/A
Concurrent queries	Up to 600 concurrent queries per minute are supported in an account.	N/A
Returned records	Up to 250 records are returned by default for a query on the console.	N/A
	Up to 5000 records are returned by default for an API query.	N/A
Field size	The maximum size of a field value is 2 KB. The excess part will not be used for quick analysis but can be queried by keyword.	N/A
Search result sorting	By default, search results are displayed by time (accurate to the second) in descending order.	N/A
Fuzzy search	● Each word in a query statement must be fewer than 255 characters. ● Words cannot start with an asterisk (*) or a question mark (?). ● Long and double data does not support fuzzy search using asterisks (*) or question marks (?).	N/A

Item	Description	Remarks
Time range	No longer than 30 days	N/A

1.4.5 Log Transfer

This section describes the restrictions on log transfer.

Table 1-7

Category	Item	Description	Remarks
Log transfer to OBS	Transfer tasks for a log stream	A log stream can have only one task for transferring logs to OBS.	N/A
	Log transfer interval	2 minutes, 5 minutes, 30 minutes, 1 hour, 3 hours, 6 hours, 12 hours	N/A
	Data size of each log transfer task	0 MB to 2 GB	N/A
	Transfer rate threshold	Transfer rate is less than the growth rate of new logs per day or the OBS rate limit you purchased, whichever is reached first. Transfer may fail if the threshhold is exceeded.	N/A
	Log transfer delay	10 minutes For example, if the transfer interval is 30 minutes and the transfer starts at 8:30, transfer files will be generated at 8:40 at the latest.	N/A
	Target bucket	Standard buckets are supported. Parallel file systems are not supported.	N/A

1.4.6 Operating Systems

LTS supports multiple operating systems (OSs). When purchasing a host, select an OS supported by LTS. Otherwise, LTS cannot collect logs from the host.

Table 1-8 Supported OSs and versions (Linux)

Operating Systems	Version					
SUSE	SUSE Enterprise 11 SP4 64bit	SUSE Enterprise 12 SP1 64bit	SUSE Enterprise 12 SP2 64bit	SUSE Enterprise 12 SP3 64bit		
openSUSE	13.2 64bit	42.2 64bit	15.0 64-bit (Currently, syslog logs cannot be collected.)			
EulerOS	2.2 64bit	2.3 64bit				
CentOS	6.3 64bit	6.5 64bit	6.8 64bit	6.9 64bit	6.10 64bit	
	7.1 64bit	7.2 64bit	7.3 64bit	7.4 64bit	7.5 64bit	7.6 64bit
	7.7 64bit	7.8 64bit	7.9 64bit	8.0 64bit	8.1 64bit	8.2 64bit
Ubuntu	14.04 server 64bit	16.04 server 64bit	18.04 server 64bit			
Fedora	24 64bit	25 64bit	29 64bit			
Debian	7.5.0 32bit	7.5.0 64bit	8.2.0 64bit	8.8.0 64bit	9.0.0 64bit	
Kylin	Kylin V10 SP1 64bit					

NOTE

- For Linux Arm hosts, LTS supports all the OSs and versions listed in the preceding table except the CentOS of 7.3 and earlier versions.

1.5 Permissions Management

Description

If you need to assign different permissions to employees in your enterprise to access your LTS resources, Identity and Access Management (IAM) is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you secure access to your LTS resources.

With IAM, you can use your account to create IAM users for your employees, and assign permissions to the users to control their access to LTS resources. For example, some software developers in your enterprise need to use LTS resources but should not delete them or perform other high-risk operations. In this case, you can create IAM users for the software developers and grant them only the permissions required.

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

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

LTS Permissions

By default, new IAM users do not have permissions assigned. You need to add users to one or more groups, and attach permissions policies or roles to these groups. Users inherit permissions from the groups to which they are added and can perform specified operations on cloud services based on the permissions.

LTS is a project-level service deployed and accessed in specific physical regions. To assign LTS permissions to a user group, specify the scope as region-specific projects and select projects for the permissions to take effect. If **All projects** is selected, the permissions will take effect for the user group in all region-specific projects. When accessing LTS, the users need to switch to a region where they have been authorized to use LTS.

Policies: A type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions. This mechanism allows for more flexible policy-based authorization, meeting requirements for secure access control. For example, you can grant Elastic Cloud Server (ECS) users only the permissions for managing a certain type of ECSs. Most policies define permissions based on APIs.

The system permissions supported by LTS are listed in **Table 1-9**.

Table 1-9 LTS system permissions

Name	Description	Type	Dependency
LTS FullAccess	Full permissions for LTS. Users with these permissions can perform operations on LTS.	System-defined policy	OBS Administrator and AOM FullAccess
LTS ReadOnlyAccess	Read-only permissions for LTS. Users with these permissions can only view LTS data.	System-defined policy	OBS Administrator and AOM FullAccess
LTS Administrator	Administrator permissions for LTS.	System-defined policy	This role is dependent on the **Tenant Guest** and **Tenant Administrator** roles.

Name	Description	Type	Dependency
LTS Admin	Administrator permissions for LTS.	System-defined role	This role is dependent on the **Tenant Guest** and **Tenant Administrator** roles.

Table 1-10 lists the common operations supported by each system-defined policy and role of LTS. Choose the appropriate policies and roles according to this table.

Table 1-10 Common operations supported by each LTS system policy or role

Operation	LTS FullAccess	LTS ReadOnlyAccess	LTS Administrator
Querying a log group	√	√	√
Creating a log group	√	×	√
Modifying a log group	√	×	√
Deleting a log group	√	×	√
Querying a log stream	√	√	√
Creating a log stream	√	×	√
Modifying a log stream	√	×	√
Deleting a log stream	√	×	√
Configuring log collection from hosts	√	×	√
Querying the configuration of log structuring	√	√	√
Configuring log structuring	√	×	√
Enabling quick analysis	√	×	√

Operation	LTS FullAccess	LTS ReadOnlyAccess	LTS Administrator
Disabling quick analysis	√	×	√
Querying a filter	√	√	√
Disabling a filter	√	×	√
Enabling a filter	√	×	√
Deleting a filter	√	×	√
Viewing a log transfer task	√	√	√
Creating a log transfer task	√	×	√
Modifying a log transfer task	√	×	√
Deleting a log transfer task	√	×	√
Enabling a log transfer task	√	×	√
Disabling a log transfer task	√	×	√
Installing ICAgent	√	×	√
Upgrading ICAgent	√	×	√
Uninstalling ICAgent	√	×	√

To use a custom fine-grained policy, log in to IAM as the administrator and select fine-grained permissions of LTS as required.

Table 1-11 describes fine-grained permission dependencies of LTS.

Table 1-11 Fine-grained permission dependencies of LTS

Permission	Description	Dependency
lts:agents:list	List agents	None
lts:buckets:get	Get bucket	None
lts:groups:put	Put log group	None

Permission	Description	Dependency
lts:transfers:create	Create transfer	obs:bucket:PutBucketAcl obs:bucket:GetBucketAcl obs:bucket:GetEncryptionConfiguration obs:bucket:HeadBucket dis:streams:list dis:streamPolicies:list
lts:groups:get	Get log group	None
lts:transfers:put	Put transfer	obs:bucket:PutBucketAcl obs:bucket:GetBucketAcl obs:bucket:GetEncryptionConfiguration obs:bucket:HeadBucket dis:streams:list dis:streamPolicies:list
lts:resourceTags:delete	Delete resource tag	None
lts:ecsOsLogPaths:list	List ecs os logs paths	None
lts:structConfig:create	Create struct config	None
lts:agentsConf:get	Get agent conf	None
lts:logIndex:list	Get log index	None
lts:transfers:delete	Delete transfer	None
lts:regex:create	Create struct regex	None
lts:subscriptions:delete	Delete subscription	None
lts:overviewLogsLast:list	List overview last logs	None
lts:logIndex:get	Get log index	None
lts:sqlalarmrules:create	Create alarm options	None
lts:agentsConf:create	Create agent conf	None
lts:sqlalarmrules:get	Get alarm options	None
lts:datasources:batchdelete	Batch delete datasource	None
lts:structConfig:put	Update struct config	None
lts:groups:list	List log groups	None
lts:sqlalarmrules:delete	Delete alarm options	None

Permission	Description	Dependency
lts:transfers:action	Enabled transfer	None
lts:datasources:post	Post datasource	None
lts:topics:create	Create log topic	None
lts:resourceTags:get	Query resource tags	None
lts:filters:put	Update log filter	None
lts:logs:list	List logs	None
lts:subscriptions:create	Create subscription	None
lts:filtersAction:put	Put log filter action	None
lts:overviewLogsTopTopic:get	List overview top logs	None
lts:datasources:put	Put datasource	None
lts:structConfig:delete	Delete struct config	None
lts:logIndex:delete	Deleting a specified log index	None
lts:filters:get	Get log filter	None
lts:topics:delete	Delete log topics	None
lts:agentSupportedOsLogPaths:list	List agent supported os logs paths	None
lts:topics:put	Put log topic	None
lts:agentHeartbeat:post	Post agent heartbeat	None
lts:logsByName:upload	Upload logs by name	None
lts:buckets:list	List buckets	None
lts:logIndex:post	Create log index	None
lts:logContext:list	List logs context	None
lts:groups:delete	Delete log group	None
lts:filters:delete	Delete log filter	None
lts:resourceTags:put	Update resource tags	None
lts:structConfig:get	Get struct config	None
lts:overviewLogTotal:get	Get overview logs total	None
lts:subscriptions:put	Put subscription	None
lts:subscriptions:list	List subscription	None

Permission	Description	Dependency
lts:datasources:delete	Delete datasource	None
lts:transfersStatus:get	List transfer status	None
lts:logIndex:put	Put log index	None
lts:sqlalarmrules:put	Modify alarm options	None
lts:logs:upload	Upload logs	None
lts:agentDetails:list	List agent diagnostic log	None
lts:agentsConf:put	Put agent conf	None
lts:logstreams:list	Check logstream resources	None
lts:subscriptions:get	Get subscription	None
lts:disStreams:list	Query DIS pipe	None
lts:groupTopics:put	Create log group and log topic	None
lts:resourceInstance:list	Query resource instance	None
lts:transfers:list	List transfers	None
lts:topics:get	Get log topic	None
lts:agentsConf:delete	Delete agent conf	None
lts:agentEcs:list	List agent ecs	None
lts:indiceLogs:list	Search indiceLogs	None
lts:topics:list	List log topic	None

1.6 Glossary

This section describes common terms used in LTS to help you better understand and use LTS.

Table 1-12 Terms

Abbreviation	Full Spelling	Definition
LTS	Log Tank Service	LTS collects, analyzes, and stores logs. You can use LTS for efficient device O&M, service trend analysis, security audits, and monitoring.

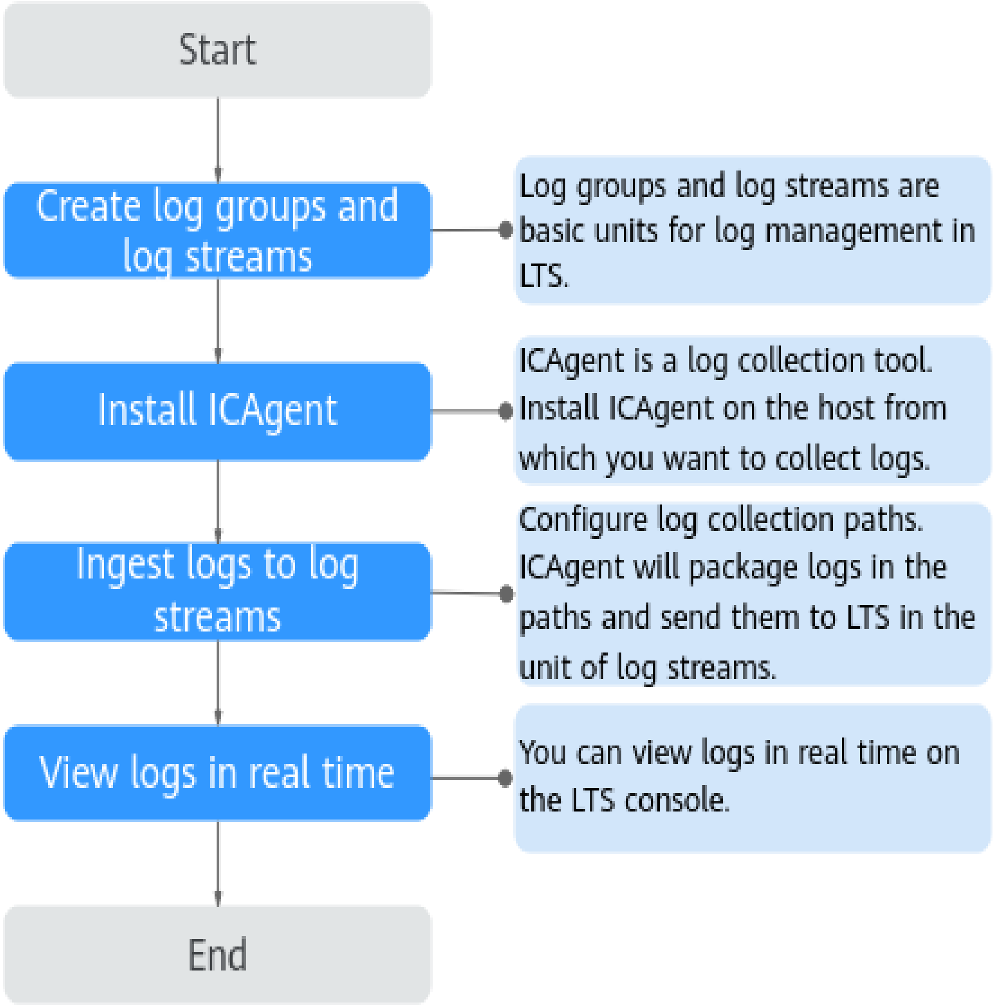
Abbreviation	Full Spelling	Definition
-	Log group	A log group is a group of log streams and is the basic unit for log management in LTS. You need to create a log group before collecting, querying, and transferring logs.
-	Log stream	A log stream is the basic unit for log reads and writes. If there are 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.
-	ICAgent	ICAgent is the log collection tool of LTS. If you want to use LTS to collect logs from a host, you need to install ICAgent on the host. Batch agent installation is supported if you want to collect logs from multiple hosts. After agent installation, you can check the ICAgent status on the LTS console in real time.

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


Start
Create log groups and log streams
Log groups and log streams are basic units for log management in LTS.
Install ICAgent
ICAgent is a log collection tool. Install ICAgent on the host from which you want to collect logs.
Ingest logs to log streams
Configure log collection paths. ICAgent will package logs in the paths and send them to LTS in the unit of log streams.
View logs in real time
You can view logs in real time on the LTS console.
End

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

Creating a Log Group

1. Log in to the LTS console. On the **Log Management** page, click **Create Log Group**.

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

NOTE

Collected logs are sent to the log 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 7 days. If this parameter is not specified, logs are retained for 7 days by default.
4. 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.
4. 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.

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.

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

The Access Key ID/Secret Access Key (AK/SK) can be obtained on the **My Credentials** page. The procedure is as follows:

1. Hover the mouse pointer over the username in the upper right corner of the page and select **My Credentials**.
2. On the **My Credentials** page, choose **Access Keys**.
3. Click **Create Access Key** and enter a description.

   NOTE

   Up to 2 access keys can be created for each user. An access key can be downloaded only right after it is created. If the **Create Access Key** button is grayed out, delete an access key first before creating one.
4. Click **OK**, download the AK/SK, and keep it secure.

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 **Elastic Cloud Server (ECS)** 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: Select Host Group**.

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: Configure Collection**.

Step 5 Configure the collection.

1. Configure the collection parameters. For details, see section "Configuring Collection".
2. Click **Submit**.

Step 6 (Optional) Configure structured logs.

Step 7 (Optional) Configure indexes.

Step 8 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), FAQs, and recently viewed log streams.

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**.

For details, see **Resource Statistics**.

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.

NOTE

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

FAQ

This area displays frequently asked questions.

To view more FAQs, click **More**.

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

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.

- 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. 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.
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** to 1 to 7 days. If this parameter is not specified, logs are retained for 7 days by default.
4. Click **OK**.
   - In the log group list, you can view details of log groups, including log group name, log retention duration (days), creation type, creation time, and number of log streams.
   - Click the log group name, the details page of one of its log streams is displayed.
   - When multiple log groups are created concurrently, there may be a limit exceeding error.

Deleting a Log Group

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

NOTE

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

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

Searching Log Groups/Streams

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

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

3.4 Managing Log Streams

A log stream is the basic unit for reading and writing logs. You can separate different types of logs (such as operation logs and access logs) into different log streams for easier management. 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.

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

   NOTE

   Collected logs are sent to the created log stream. If there are a large number of logs, you can create multiple log streams and name them for quick log search. After a log stream is created, its name cannot be changed.
3. Click **OK**. In the log stream list, you can view information such as the log stream name and operations.

Deleting a Log Stream

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

NOTE

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

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

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**.

- Configuring a metric filter

  Click ▽ in the **Operation** column of a log stream. On the displayed page, configure the metric filter.

  NOTE

  LTS extracts your specified keyword from logs so that you can monitor it and set alarms on AOM (Application Operations Management).

- **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.

3.5 Tag Management

You can tag log groups, log streams, host groups, and log ingestion configurations. There are system and custom tags. System tags (such as log cleaning tags) cannot be modified. Up to 20 custom tags can be added to each resource.

Log Groups

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

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

   NOTE

   - To add multiple tags, repeat this step.
   - To delete a tag, click ⊗ next to the tag in the text box.
   - A tag key can contain up to 128 characters, and a tag value can contain up to 255 characters.
   - A tag key must be unique.

4. Click **OK**.

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

Tagging a Log Stream

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

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

   NOTE

   - To add multiple tags, repeat this step.
   - To delete a tag, click ⊗ next to the tag in the text box.
   - A tag key can contain up to 128 characters, and a tag value can contain up to 255 characters.
   - A tag key must be unique.
5. Click **OK**.

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

Tagging a Host Group

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

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

   NOTE

   - To add multiple tags, repeat this step.
   - To delete a tag, click ⊗ next to the tag in the text box.
   - A tag key can contain up to 128 characters, and a tag value can contain up to 255 characters.
   - A tag key must be unique.

4. Click **OK**.

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

Tagging a Log Ingestion Configuration

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

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

   NOTE

   - To add multiple tags, repeat this step.
   - To delete a tag, click ⊗ next to the tag in the text box.
   - A tag key can contain up to 128 characters, and a tag value can contain up to 255 characters.
   - A tag key must be unique.
4. Click **OK**.

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

4 Log Ingestion

4.1 Collecting Logs from Cloud Services

4.1.1 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:

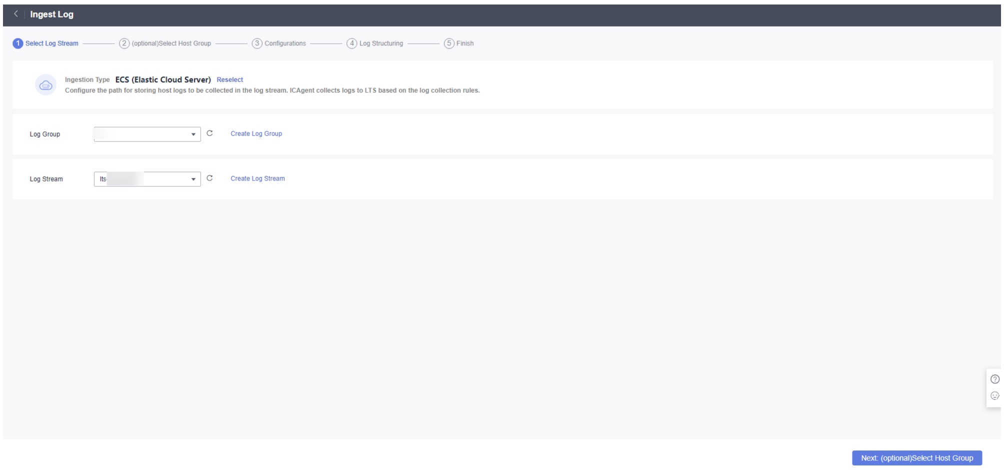
Step 1 Log in to the LTS console.

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

Figure 4-1 Selecting a log group



Ingest Log

1 Select Log Stream — 2 (optional)Select Host Group — 3 Configurations — 4 Log Structuring — 5 Finish

Ingestion Type **ECS (Elastic Cloud Server)** Reselect

Configure the path for storing host logs to be collected in the log stream. ICAgent collects logs to LTS based on the log collection rules.

Log Group: Create Log Group

Log Stream: lts Create Log Stream

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 section "Log Structuring".

NOTE

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

Step 7 (Optional) Configure indexes.

For details, see section "Index Settings".

Step 8 The operation is complete.

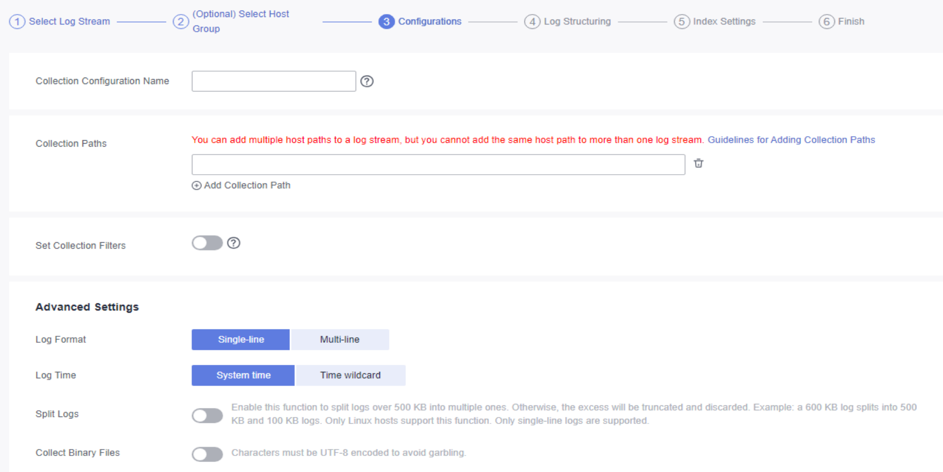
Click **Back to Ingestion Configurations** to **check the ingestion details**. You can also click **View Log Stream** to view the log stream to which logs are ingested.

----End

Configurations

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

Figure 4-2 Configuring the collection



Collection Configuration Name

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

Set Collection Filters

Advanced Settings

Log Format: Single-line

Log Time: System time

Split Logs: Enable this function to split logs over 500 KB into multiple ones. Otherwise, the excess will be truncated and discarded. Example: a 600 KB log splits into 500 KB and 100 KB logs. Only Linux hosts support this function. Only single-line logs are supported.

Collect Binary Files: Characters must be UTF-8 encoded to avoid garbling.

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. Configure the log format and log time.

Table 4-1 Log collection configurations

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

Parameter	Description
Regular Expression	You can set a regular expression to look for a specific pattern to indicate the beginning of a log event. This parameter needs to be specified when you select **Multi-line** for **Log Format** and **By regular expression** for **Log Segmentation**.
Split Logs	LTS supports log splitting, which is disabled by default. If this option is enabled, a single-line log larger than 500 KB will be split into multiple lines for collection. For example, a line of 600 KB log will be split into two lines for collection, the first line 500 KB and the second line 100 KB. If this option is disabled, a log larger than 500 KB will be truncated.
Collect Binary Files	LTS supports binary file collection, which is disabled by default. Run the **file -i** *File_name* command to view the file type. **charset=binary** indicates that a log file is a binary file. If this option is enabled, binary log files will be collected, but only UTF-8 strings are supported. Other strings will be garbled on the LTS console. If this option is disabled, binary log files will not be collected.

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.

- Tag management: Click ▤ in the **Operation** column of the row that contains the desired ingestion configuration to add a tag.

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

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

Deleting Host Groups

Deleting a single host group

1. On the **Host Management** page, the **Host Groups** tab is displayed by default.
2. On the **Host Groups** tab, click the deletion icon in the **Operation** column of the row containing the target host group.
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. If you use LTS to collect logs from a host, you need to install ICAgent on it. This section describes how to install the ICAgent on a host.

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.

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

Step 4 Select an installation mode:

- Obtain the AK/SK pair. 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 on the **Host Management** > **Hosts** page of the LTS console.
- If the installation fails, uninstall ICAgent and reinstall it. If the reinstallation fails, contact technical support.

----End

Inherited Installation (Linux)

Let's assume that you need to install ICAgent on multiple hosts, and one of the hosts already has ICAgent installed. The ICAgent installation package, **ICProbeAgent.tar.gz**, is in the **/opt/ICAgent/** directory. You can follow the directions below to install ICAgent on other hosts one by one.

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

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

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

   NOTE

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

- 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 manually during execution. If one of the hosts uses a different password, type the password behind its IP address.

Procedure

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

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

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

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

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

2. You can then view the ICAgent status on the **Host Management** > **Hosts** page of the LTS console.

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**.
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.
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.
Restricted	The LTS license is restricted. Check the license and update it in a timely manner.

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 **Search**.

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	You can click ⟳ | ▾ to refresh logs in two modes: manual refresh and automatic refresh. ● Manual refresh: Select **Refresh Now** from the drop-down list. ● Automatic refresh: Select an interval from the drop-down list to automatically refresh logs. The interval can be 15 seconds, 30 seconds, 1 minute, or 5 minutes.
Copying logs	Click ⧉ to copy the log content.
Viewing context of a log	Click 🗎 to view the log context.
Simplifying field details	Click ··· to view the simplified field details.
Unfold/Fold	Click ⤶ to display all the log content. Click ☰ to fold the log content. **NOTE** **Unfold** is enabled by default.
Downloading logs	Click ⤓ . On the displayed **Download Logs** page, click **Direct Download** or **Transfer and Download**. **Direct Download**: Download log files to the local PC. Up to 5000 logs can be downloaded at a time. Select **.csv** or **.txt** from the drop-down list and click **Download** to export logs to the local PC. **NOTE** ● If you select **Export .csv**, logs are exported as a table. ● If you select **Export .txt**, logs are exported as a **.txt** file.
Collapse all/ Expand all	Click ☰ to set the number of lines displayed in the log content. Click ☰ | ▾ to close it. **NOTE** By default, logs are not collapsed, and two rows of logs are shown after collapsing. You can display up to six rows.
Layout	Move the cursor over ⚙ and choose **Layout** from the drop-down list. On the displayed **Layout** page, specify whether to simplify field display and show fields. ● **Simple View**: If this is enabled, the fields are displayed in a simplified manner. ● **Show/Hide**: When the visibility of a field is disabled, the field is not displayed in the log content.

Operation	Description
JSON	Move the cursor over ⚙, click **JSON**, and set JSON formatting. **NOTE** Formatting is enabled by default. The default number of expanded levels is 2. ● Formatting enabled: Set the default number of expanded levels. Maximum value: **10**. ● Formatting disabled: JSON logs will not be formatted for display.
Invisible fields (⊘)	This list displays the invisible fields configured in the layout settings. ● The ⊘ button is unavailable for log streams without layout settings configured. ● If the log content is **CONFIG_FILE** and layout settings are not configured, the default invisible fields include **appName**, **clusterId**, **clusterName**, **containerName**, **hostIPv6**, **NameSpace**, **podName**, and **serviceID**.

6.2 Built-in Reserved Fields

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

NOTE

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

Log Example

In the following log example, the value of the **content** field is the original log text, and other fields are common built-in reserved fields.

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

Built-in Reserved Fields Description

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

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

Built-in Reserved Fields	Number Format	Index and Statistics Settings	Description
clusterId	String	Index setting: After this function is enabled, a field index is created for clusterId by default. The index data type is string, and the delimiters are empty. Enter clusterId: xxx during the query.	Cluster ID, used in the Kubernetes scenario. Such as "clusterId":"c7f3f4a5-xxxx-11ed-a4ec-0255ac100b07" in the example.
nameSpace	String	Index setting: After this function is enabled, a field index is created for nameSpace by default. The index data type is string, and the delimiters are empty. Enter nameSpace: xxx during the query.	Namespace used in the Kubernetes scenario. Such as "nameSpace":"monitoring" in the example.
appName	String	Index setting: After this function is enabled, a field index is created for appName by default. The index data type is string, and the delimiters are empty. Enter appName: xxx during the query.	Component name, used as the name of the workload in the Kubernetes scenario. Such as "appName":"alertmanager-alertmanager" in the example.
serviceID	String	Index setting: After this function is enabled, a field index is created for serviceID by default. The index data type is string, and the delimiters are empty. Enter serviceID: xxx during the query.	Workload ID in the Kubernetes scenario. Such as "serviceID":"cf5b453xxxad61d4c483b50da3fad5ad" in the example.

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

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

Built-in Reserved Fields	Number Format	Index and Statistics Settings	Description
content	String	Index setting: After **Index Whole Text** is enabled, the delimiter defined by the full-text index is used to segment the value of the content field. The content field cannot be configured in the field index.	Original log content Such as "content":"level=error ts=2023-04-19T09:21:21.333895559Z" in the example.
logContent	String	The logContent field cannot be configured in the field index.	Not involved
logContentSize	Integer	The logContentSize field cannot be configured in the field index.	Not involved
logIndexSize	Integer	The logIndexSize field cannot be configured in the field index.	Not involved
groupName	String	The groupName field cannot be configured in the field index.	Not involved
logStream	String	The logStream field cannot be configured in the field index.	Not involved

6.3 Index Settings

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

Log Example

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

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

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

The following figure shows a typical index setting of a log example.

Index Types

The following table lists the index types supported by LTS.

Table 6-2 Index types

Index Type	Description
Index Whole Text	LTS splits all field values of an entire log into multiple words when this function is enabled. **NOTE** ● The custom label field uploaded by the user is not included in the full-text index. If you want to search for the custom label field, add the corresponding index field. ● Reserved fields are not included in full-text indexes. You need to use the Key:Value index to search for fields. For details, see **Built-in Reserved Fields**.
Index Fields	Query logs by specified field names and values (Key:Value). **NOTE** ● By default, LTS creates index fields for some built-in reserved fields. For details, see **Built-in Reserved Fields**. ● If an index field is configured for a field, the delimiter of the field value is subject to the index field configuration. ● The quick analysis column in structuring settings has been removed. To use this function, configure index fields and enable quick analysis for the required fields. Here are two examples: ● In the log example, the level and status index fields are configured. The level field is of the **string** type, the field value is error, and a delimiter is configured. The status field is of the **long** type, and no delimiter needs to be configured. You can use level:error to search for all logs whose level value is error. ● In the log example, LTS creates indexes for built-in reserved fields such as hostName, hostIP, and pathFile by default.

Precautions

- Either whole text indexing or index fields must be configured.
- Index settings (such as adding, editing, and deleting fields and modifying items) take effect only for new log data but not for historical log data. Currently, indexes cannot be recreated for historical logs.

- After the index function is disabled, the storage space of historical indexes is automatically cleared after the data storage period of the current log stream expires.
- By default, LTS creates index fields for some built-in reserved fields. For details, see **Built-in Reserved Fields**.
- Different index settings will generate different query and analysis results. Configure the index settings as required. Full-text indexes and index fields do not affect each other.

Configuring Whole Text Indexing

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

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

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

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

NOTE

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

Step 5 Set parameters as described in **Table 6-3**.

Table 6-3 Whole text indexing parameters

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

Parameter	Description
Include Chinese	Indicates whether to distinguish between Chinese and English during query. ● After the function is enabled, if the log contains Chinese characters, the Chinese content is split based on unigram segmentation and the English content is split based on delimiters. **NOTE** Unigram segmentation is to split a Chinese string into Chinese characters. The advantage of unigram segmentation is efficient word segmentation of massive logs, and other Chinese segmentation methods have great impact on the write speed. ● After this function is disabled, all content is split based on delimiters. For example, assume that the log content is: **error,400,I Know TodayIsMonday**. ● After this function is disabled, the English content is split based on delimiters. The log is split into **error**, **400**, **I**, **Know**, and **TodayIsMonday**. You can search for the log by **error** or **TodayIsMonday**. ● After this function is enabled, the background analyzer of LTS splits the log into **error**, **400**, **I**, **Know**, **Today**, **Is**, and **Monday**. You can search for the log by **error** or **Today**.
Delimiters	Splits the log content into multiple words based on the specified delimiter. Default delimiters include ,'";=()[]{}@&<>/:\n\t\r and spaces. If the default settings cannot meet your requirements, you can customize delimiters. All ASCII codes can be defined as delimiters. If the delimiter is set to null, the field value is regarded as a whole. You can search for the corresponding log only through the complete character string or fuzzy search. For example, assume that the log content is: **error,400,I Know TodayIsMonday**. ● If no delimiter is set, the entire log is regarded as a string **error,400,I Know TodayIsMonday**. You can search for the log only by the complete string **error,400,I Know TodayIsMonday** or by fuzzy search **error,400,I K***. ● If the delimiter is set to a comma (,), the raw log is split into: **error**, **400**, and **I Know TodayIsMonday**. You can find the log by fuzzy search or exact words, for example, **error**, **400**, **Kn***, and **TodayIs***. ● If the delimiter is set to a comma (,) and space, the raw log is split into: **error**, **400**, **I**, **Know**, **TodayIsMonday**. You can find the log by fuzzy search or exact words, for example, **Know**, and **TodayIs***.

Step 6 Click **OK**.

----End

Configuring Index Fields

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

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

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

Step 3 Click ⚙ in the upper right corner to go to the **Index Settings** page. Click **Add Field** and enter the field name.

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

NOTE

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

Table 6-4 Index field parameters

Parameter	Description
Field Name	Log field name, including **level** in the example log. The field name can contain only letters, digits, and underscores (_), and must start with a letter or underscore (_). The field name cannot contain double underscores (__). **NOTE** ● Double underscores (__) are used in built-in reserved fields that are not displayed to users in LTS. Double underscores (__) cannot be used in custom log field names. Otherwise, field index names cannot be configured. ● By default, LTS creates index fields for some built-in reserved fields. For details, see **Built-in Reserved Fields**.
Type	● Data type of the log field value. The options are string, long, and float. ● Fields of long and float types do not support **Case-Sensitivity**, **Include Chinese** and **Delimiters**.
Quick Analysis	By default, this option is enabled, indicating that this field will be sampled and collected. For details, see **Quick Analysis**. **NOTE** ● The principle of quick analysis is to collect statistics on 100,000 logs that match the search criteria, not all logs. ● The maximum length of a field for quick analysis is 2000 bytes. ● The quick analysis field area displays the first 100 records.

Parameter	Description
Operation	**Delete**: Delete the field.

Step 5 Click **OK**.

----End

Auto Index Field Configuration

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

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

6.4 Cloud Structuring Parsing

6.4.1 Log Structuring

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

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

Precautions

- You have created a log stream.
- Log structuring is recommended when most logs in a log stream share a similar pattern.

Creating a Structuring Rule

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

To structure logs:

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

Step 2 Select a log group and a log stream.

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

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

NOTE

- If a structured field exceeds 20 KB, only the first 20 KB is retained.
- The following system fields cannot be extracted during log structuring: **groupName**, **logStream**, **lineNum**, **content**, **logContent**, **logContentSize**, **collectTime**, **category**, **clusterId**, **clusterName**, **containerName**, **hostIP**, **hostId**, **hostName**, **nameSpace**, **pathFile**, and **podName**.

Step 4 Click **Save**.

----End

Modifying a Structuring Rule

To modify a structuring rule, perform the following steps:

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

NOTE

You can modify the structuring rules, including the structuring mode, log extraction field, and tag field.

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

6.4.2 Structuring Modes

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

Regular Expressions

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

Step 1 Select a typical log event as the sample.

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

NOTE

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

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

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 structured 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 structured 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 structured 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**.

6.4.3 Structuring Templates

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

System Templates

System templates: VPC, Tomcat, Nginx

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.

6.4.4 Log Structuring Fields

Setting Log Structuring Fields

You can edit extracted fields after log structuring.

Table 6-5 Rules for configuring structured fields

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

6.5 Search Syntax and Functions

6.5.1 Search Syntax

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

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

Search Mode

The search statement is used to specify the filter criteria for log search and return the logs that meet the filter criteria.

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

Table 6-6 Search mode description

Search Mode	Description	Example
Full-Text Search	LTS splits an entire log into multiple keywords when full-text index is set. **NOTE** ● **content** is a built-in field corresponding to the original log text. The search statement **GET** is equivalent to **content:GET**. By default, the original log content is matched. ● By default, multiple keywords are connected through **AND**. The search statement **GET POST** is equivalent to **GET** and **POST**.	● GET POST ● GET and POST ● content:GET and content:POST The preceding search statements have the same function, indicating that logs containing both GET and POST are searched.
Field Search	Search for specified field names and values (key:value) after field indexing is configured. You can perform multiple types of basic search and combined search based on the data type set in the field index. **NOTE** ● The value cannot be empty. ● When field search is used together with the not operator, logs that do not contain this field are matched.	● request_time>60 and request_method:po* indicate that the system searches for logs in which the value of request_time is greater than 60 and the value of request_method starts with po. ● not request_method:GET indicates that logs that do not contain the request_method field and whose request_method value is not GET are searched.
Exact Search	Use exact words for search. LTS searches with word segmentation, which does not define the sequence of keywords. **NOTE** If the search statement is abc def, all logs that contain both abc and def are matched. Logs abc def or def abc are matched. To ensure the sequence of keywords, use **#"abc def"**.	● GET POST: searches for logs that contain both GET and POST. ● request_method:GET indicates that logs in which the value of request_method contains GET are searched. ● #"/var/log" indicates that logs containing the phrase /var/log are searched.

Search Mode	Description	Example
Fuzzy Search	Specify a word in the search statement and add a fuzzy search keyword, that is, an asterisk (*) or a question mark (?), to the middle or end of the word. LTS searches for the word that meets the search criteria and returns all logs that contain the word. **NOTE** ● The asterisk (*) indicates that multiple characters are matched, and the question mark (?) indicates that one character is matched. ● Words cannot start with an asterisk (*) or a question mark (?). ● Long and float data does not support fuzzy search using asterisks (*) or question marks (?).	● GE* indicates that the system searches for words starting with GE in all logs and returns logs containing these words. ● request_method:GE* indicates that the system searches for request_method values starting with GE in all logs and returns logs containing these words.
Search Scope	The long and float data supports range search. ● Method 1: Use operators such as = (equal to) > (greater than) < (less than) operators to search for logs. ● Method 2: Use the in operator to search for logs. The open/closed interval can be modified. **NOTE** The string fields do not support range query.	● request_time>=60 indicates that the system searches for logs whose request_time value is greater than or equal to 60. ● request_time in (60 120] indicates that the system searches for logs whose request_time value is greater than 60 and less than or equal to 120.
Phrase Search	Phrase search is used to fully match target phrases in logs to ensure the sequence in which keywords appear. **NOTE** Fuzzy search is not supported for phrase search.	**#"abc def"** indicates that the system searches all logs for the logs that contain the target phrase abc def.

- Delimiters

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

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

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

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

- Keyword sequence

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

  For example, **request_method:GET POST** is used to query logs that contain both GET and POST, and the sequence of GET and POST is not ensured.

- Invalid keyword

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

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

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

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

Operator

The search statement supports the following operators:

NOTE

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

Table 6-7 Description

Operator	Description
and	AND operator. If there is no syntax keyword between multiple keywords, the AND relationship is used by default. For example, **GET 200** is equivalent to **GET and 200**. **NOTE** When and is used as an operator, use a space before and after it. For example, **1 and 2** indicates that logs containing both **1** and **2** are searched, and **1and2** indicates that logs containing **1and2** are searched.
AND	AND operator, equivalent to and.

Operator	Description
&&	AND operator. **NOTE** When && is used as an operator, spaces are not necessary. For example, **1 && 2** is equivalent to **1&&2**, indicating that logs containing both **1** and **2** are searched.
or	OR operator, example: **request_method:GET or status:200** **NOTE** When or is used as an operator, use a space before and after it.
OR	OR operator, equivalent to or.
||	OR operator. When || is used as an operator, spaces are not necessary.
not	NOT operator. Example: **request_method:GET not status:200, not status:200** **NOTE** ● When not is used as an operator, use a space before and after it. ● When field search is used together with the not operator, logs that do not contain this field are matched.
( )	Specify fields that should be matched with higher priority. Example: **(request_method:GET or request_method:POST) and status:200**
:	Search for a specified field (key:value). For example, **request_method:GET**. **NOTE** Use double quotation marks ("") to enclose a field name or value that contains reserved characters, such as spaces and colons (:). Example: **"request method":GET, message:"This is a log"**
""	Enclose a syntax keyword to convert it into common characters. For example, "and" means searching for logs that contain this word. The word and here is not an operator.
\	Escape double quotation marks (""). The escaped quotation marks indicate the symbol itself. For example, to search for **instance_id:nginx"01"**, use **instance_id:nginx\"01\"**.
*	An asterisk can match zero, single, or multiple characters. Example: **request_method:P*T** **NOTE** Put it in the middle or at the end of a keyword.
?	A question mark matches a single character. For example, **request_method:P?T** can match PUT but cannot match POST. **NOTE** Put it in the middle or at the end of a keyword.
>	Searches logs in which the value of a field is greater than a specified value. Example: **request_time>100**

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

Search Statement Examples

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

Table 6-8 Search statement examples

Search Requirement	Search Statement
Logs of POST requests whose status code is 200	request_method:POST and status=200
Logs of successful GET or POST requests (status codes 200 to 299)	(request_method:POST or request_method:GET) and status in [200 299]

Search Requirement	Search Statement
Logs of failed GET or POST requests	(request_method:POST or request_method:GET) not status in [200 299]
Logs of non-GET requests	not request_method:GET
Logs of successful GET request and request time is less than 60 seconds	request_method:GET and status in [200 299] not request_time>=60
Logs whose request time is 60 seconds.	● request_time:60 ● request_time=60
Logs of requests whose time is greater than or equal to 60 seconds and less than 200 seconds	● request_time>=60 and request_time<200 ● request_time in [60 200)
Logs that contain and	content:"and" **NOTE** Double quotation marks are used to enclose and. and is a common string and does not represent an operator.
Logs that do not contain the user field.	not user:*
Logs in which the value of the week field is not Monday	not week: Monday
Logs whose sec-ch-ua-mobile field is ?0	sec-ch-ua-mobile:#"?0" **NOTE** If search is required when log content contains asterisks (*) or question marks (?), use phrases search.

The following describes examples of advanced searches.

Table 6-9 Fuzzy Search

Search Requirement	Search Statement
Logs that contain words starting with GE	GE*
Logs that contain words starting with GE and with only one character after GE.	GE?
Logs in which the value of request_method contains a word starting with G.	request_method:G*

Search Requirement	Search Statement
Logs in which the value of request_method starts with P, ends with T, and contains a single character in the middle.	request_method:P?T
Logs in which the value of request_method starts with P, ends with T, and contains zero, single, or multiple characters in the middle.	request_method:P*T

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

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

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

Table 6-10 Delimiter-based search

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

6.5.2 Phrase Search

Phrase search is used to precisely match the target phrase. For example, the search statement **abc def** matches all logs that contain both **abc** and **def** regardless of the sequence. For details about the differences between phrase search and keyword search, see **Table 6-11**.

- Phrase search: It is implemented based on the keyword search syntax. Phrase search can distinguish the sequence of keywords and is used to accurately match target phrases, making the search result more accurate. Phrase search is applicable to English phrases and Chinese phrases, but cannot be used together with fuzzy search.

- Keyword search: Keyword search is implemented based on word segmentation. Delimiters are used to split the search content into multiple keywords for log matching. Keyword search does not distinguish the sequence of keywords. Therefore, as long as a keyword can be matched in a log based on the AND or NOT logic, the log can be found.

Table 6-11 Differences between two search modes

Search Mode	Phrase Search	Keyword Search
Differences	Distinguishes the sequence of keywords and is used to accurately match target phrases, making the search result more accurate.	Does not distinguish the sequence of keywords. The keyword is matched based on the search logic.
Examples	Assume that your log stream contains the following two raw logs: ● Raw log 1: **this service is lts** ● Raw log 2: **lts is service**	
	If you search for the phrase **#"is lts"**, one log is matched.	If you search for the keyword **is lts**, two logs are matched.
	If you search for the phrase **#"lts is"**, one log is matched.	If you search for the keyword **lts is**, two logs are matched.

Search Syntax

Table 6-12 Search Mode

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

Restrictions

- Fuzzy search cannot be used together with phrase search.

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

- Phrase search does not support search by delimiter.

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

- Phrase search is recommended for search in Chinese.

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

Example

Table 6-13 Search description

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

6.5.3 Viewing Real-Time Logs

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

Prerequisites

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

Procedure

1. On the LTS console, click **Log Management**.
2. In the log group list, click ⌄ on the left of a log group name.

3. In the log stream list, click 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.

6.5.4 Quick Analysis

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

Prerequisites

Quick analysis is 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 You can create a quick analysis task in either of the following ways:

1. Click ⚙ to go to the setting details page. Under **Index Fields**, enable **Quick Analysis** when adding a field.
2. On the **Log Structuring** tab page, enable **Auto Configuration and Analysis**. It is enabled by default. This enables structured fields for configuring indexes and quick analysis.

Step 4 Click **Set Quick Analysis**. On the displayed **Index Settings** page, add fields for quick analysis.

Step 5 Click **OK**. The quick analysis task is created.

NOTE

- The maximum length of a field for quick analysis is 2000 bytes.
- The quick analysis field area displays the first 100 records.

----End

6.5.5 Quick Search

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

Procedure

1. On the LTS console, choose **Log Management** in the navigation pane on the left.
2. In the log group list, click ⌄ on the left of a log group name.
3. In the log stream list, click the name of the target log stream.
4. On the log stream details page, 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 6-14 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**.
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.

7 Log Alarms

7.1 Metric Filters

7.1.1 Creating a Metric Filter

This section describes how you can create a metric filter. The metric will be monitored in AOM. If you set an alarm for the metric, you will be alerted when the number of occurrences of the metric reaches the configured threshold. Up to 5 metric filters can be created in each log stream.

1. Log in to the console.
2. Choose **Service List** ☰ > **Management & Deployment** > **Log Tank Service**.

   Choose **Log Management**.
3. In the log group list, click the name of the log group where the target log is located.

   The log stream list is displayed.
4. Click **Metric Filter**.
5. Configure metric filter parameters by referring to **Table 7-1** and click **OK**.

Table 7-1 Metric filter parameters

Parameter	Description
Filter Name	Filter names are used to distinguish different filters in a log stream. A name cannot start with a period (.) or underscore (_) or end with a period. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed.

Parameter	Description
Filtering Keyword	A filter counts the number of occurrences for the specified keyword in the log stream. Only filtering with a single keyword, such as **Error** and **Warning**, is supported. If you enter multiple keywords, such as **Fail to root**, they are considered as a whole. Filtering is case-sensitive and looks for exact matches. Numbers and special characters must be enclosed by double quotation marks.
Example Log	Example logs are used to test whether the filtering can match logs based on the configured keyword. When you click **To Paste**, you will be directed to the **Raw Logs** tab. You can search for logs containing the keyword and paste them to the test box to check whether the filtering works. You can also modify the keyword.
Metric Name	A metric name maps to a filtering keyword and resembles a key in a key-value pair. LTS carries out metric statistics and releases the results to AOM so you can monitor the frequency of the keyword, set thresholds, and receive alarms when the frequency exceeds the threshold. A metric name can contain 1 to 64 characters and must start with a letter. Only letters, digits, and underscores (_) are allowed. Metric names in a same log stream must be unique. Otherwise, data may be inaccurate.

7.1.2 Disabling a Metric Filter

Scenario

If a filter is no longer needed or becomes invalid because the format or content of logs have changed, you can disable the filter.

Prerequisites

- You have obtained an account and its password for logging in to the console.
- You have created a log group.
- You have created a log stream.
- Logs have been collected.
- You have created a metric filter.

Procedure

1. Log in to the console.
2. Choose ☰ > **Management & Deployment** > **Log Tank Service**.

   Choose **Log Management**.

3. In the log group list, click the name of the log group where the target filter is located.

   The log stream list is displayed.

4. In the log stream list, locate the target log stream.
5. Click the number or hyphen in the **Metric Filter Numbers** column.
6. Locate the row where the target filter is located and click **Disable**.

   NOTE

   After the filter is disabled, the metric corresponding to the filter will stop being monitored by AOM.

7.1.3 Deleting a Metric Filter

Scenario

You can create up to 5 metric filters in each log stream. If you want to create a filter but fail to do so because the upper limit has been reached, delete an unnecessary filter and try again.

Prerequisites

- You have obtained an account and its password for logging in to the console.
- You have created a log group.
- You have created a log stream.
- Logs have been collected.
- You have created a metric filter.

Procedure

1. Log in to the console.
2. Choose ☰ > **Management & Deployment** > **Log Tank Service**.

   Choose **Log Management**.

3. In the log group list, click the name of the log group where the target filter is located.

   The log stream list is displayed.

4. In the log stream list, locate the target log stream.
5. Click the number or hyphen in the **Metric Filter Numbers** column.
6. Click **Delete** in the row where the target filter is located.

   NOTE

   After the filter is deleted, the metric corresponding to the filter will stop being monitored by AOM. The previously configured alarm rules may trigger an alarm due to insufficient data.

8 Log Transfer

8.1 Overview

Logs reported from hosts and cloud services are retained in LTS for seven days and cannot be changed. Retained logs are deleted once the retention period is over. For long-term retention, you can transfer logs to Object Storage Service (OBS) or custom Kafka.

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

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	● Select an OBS bucket. – If no OBS buckets are available, click **View OBS Bucket** to access the OBS console and create an OBS bucket. ● Currently, LTS supports only **Standard** OBS buckets.	N/A

Parameter	Description	Example Value
Custom Log Transfer Path	● Enabled: Logs will be transferred to a custom path to separate transferred log files of different log streams. The format is **/LogTanks/***Region name/ Custom path*. The default custom path is **lts/%Y/%m/%d**, where **%Y** indicates the year, **%m** indicates the month, and **%d** indicates the day. A custom path must meet the following requirements: – Must start with **/LogTanks/***Region name*. – Can contain only letters, digits, and the following special characters: & $@;:,=+?-._/ %. The character % can only be followed only by Y (year), m (month), d (day), H (hour), and M (minute). Any number of characters can be added before and after %Y, %m, %d, %H, and %M, and the sequence of these variables can be changed. – Can contain 1–128 characters. Example: 1. If you enter **LTS-test/%Y/%m/ %done/%H/%m**, the path is **LogTanks**/*Region name*/**LTS-test**/*Y*/ *m*/*d***one**/*H*/*m*/*Log file name*. 2. If you enter **LTS-test/%d/%H/%m/%Y**, the path is **LogTanks**/*Region name*/**LTS-test**/*d*/ *H*/*m*/*Y*/*Log file name*. ● Disabled: Logs will be transferred to the default path. The default path is **LogTanks/***Region name/ 2019/01/01/Log group/Log stream/Log file name*.	LTS-test/%Y/%m/ %done/%H/%m
Log Prefix	The file name prefix of the log files transferred to an OBS bucket The prefix must meet the following requirements: ● Can contain 0 to 64 characters. ● Can contain only letters, digits, hyphens (-), underscores (_), and periods (.). Example: If you enter **LTS-log**, the log file name will be **LTS-log**_*Log file name*.	LTS-log

Parameter	Description	Example Value

Format	The storage format of logs. The value can be **Raw Log Format** or **JSON**.
	● Examples of the raw log format: (Logs displayed on the LTS console are in the raw format.)
	`Sep 30 07:30:01 ecs-bd70 CRON[3459]: (root) CMD (/opt/oss/servicemgr/ICAgent/bin/manual/mstart.sh > /dev/null 2>&1)`
	● The following is an example of the JSON format:
	`{"host_name":"ecs-bd70","ip":"192.168.0.54","line_no":249,"message":"Sep 30 14:40:01 ecs-bd70 CRON[4363]: (root) CMD (/opt/oss/servicemgr/ICAgent/bin/manual/mstart.sh > /dev/null 2>&1)\n","path":"/var/log/syslog","time":1569825602303}`
		Json

Log Transfer Interval	The interval for automatically transferring logs to OBS buckets. The value can be 2, 5, or 30 minutes, or 1, 3, 6, or 12 hours.	3 hours
Time Zone	When logs are transferred to OBS buckets, the time in the transfer directory and file name will use the specified UTC time zone.	(UTC) Coordinated Universal Time
Filter by Tag Fields	During transfer, logs will be filtered by tag fields collected by ICAgent. ● Disabled: Logs will not be filtered by tag fields. ● Enabled: Default tag fields include those for hosts (**hostIP**, **hostId**, **hostName**, **pathFile**, and **collectTime**) and for Kubernetes (**clusterName**, **clusterId**, **nameSpace**, **podName**, **containerName**, and **appName**). Optional public tag fields are **regionName**, **logStreamName**, **logGroupName**, and **projectId**. **NOTE** When **Filter by Tag Fields** is enabled, **Format** must be **JSON**. ● **Filter by Tag Fields**: When this parameter is enabled, logs will be filtered by tags.	Enabled

4. Click **OK**. When the log transfer status changes to **Normal**, the transfer task has been created.
5. Click the OBS bucket name in the **Transfer Destination** column to switch to the OBS console and view the transferred log files.

Transferred logs can be downloaded from OBS to your local computer for viewing.

NOTE

Logs stored in OBS are in raw or JSON format.

Modifying a Log Transfer Task

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

Viewing Transfer Details

1. Locate the target log transfer task and click **Details** in the row of the desired task to view the task details.
2. On the displayed **Transfer Details** page, you can view the log transfer details.

Deleting a Log Transfer Task

If logs do not need to be transferred, you can delete the transfer task.

NOTE

- After a transfer task is deleted, log transfer will be stopped. Exercise caution when performing the deletion.
- After a transfer task is deleted, the logs that have been transferred remain in OBS.
- When you create a transfer task, OBS will grant read and write permissions to LTS for the selected bucket. If one OBS bucket is used by multiple transfer tasks, perform the following operations to delete the transfer task:
  - If only one transfer task is created using this OBS bucket, delete the bucket access permission granted to specific users on the **Access Control** > **Bucket ACLs** tab page on the OBS console when you delete the transfer task.
  - If multiple transfer tasks are created using this OBS bucket, do not delete the bucket access permission. Otherwise, data transfer will fail.

1. Locate the row of the target transfer task and choose **Delete** in the **Operation** column.
2. Click **OK**.

Viewing Transfer Status

The status of a transfer task can be **Normal**, **Abnormal**, or **Disabled**.

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

NOTE

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

----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.

10.2 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 (7 days by default) ends.

10.2.4 Log Search Issues

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

Common Issues and Troubleshooting Methods

1. During log query, a message is displayed indicating that the query result is inaccurate.
   - Possible cause: There are too many logs in the query time range, and not all logs are displayed.
   - Solution: Click the query button multiple times until you obtain all logs, or shorten the query time range and query again.
2. Too many log results are matched in a query.
   - Possible cause: Only phrase search **#"value"** can ensure the sequence of keywords. For example, if the query statement is **abc def**, logs that

contain either **abc** or **def** and logs that contain the phrase **abc def** will be matched.

- Solution: Use the phrase **#"abc def"** to accurately match logs containing the phrase **abc def**. For details, see section "Phrase Search".

3. Expected logs cannot be queried with specific search statements, and no error message is displayed.
   - Possible cause 1: Search delimiters are not supported.
   - Possible cause 2: The ***** or **?** in a search statement will be regarded as a common character and is not used as a wildcard.
   - Solution: Use the correct query statement.

Error Messages and Solutions

1. An error message is displayed during log query, indicating that no field index is configured for the XXX field and the field cannot be queried.

   Solution: Create an index for the XXX field in the index configuration and run the query statement again. For details, see section "Index Settings".

2. An error message is displayed during log query, indicating that the full-text index is not enabled and the content field and full-text query are not supported.

   Solution: Enable the full-text index in the index configuration and run the query statement again. For details, see section "Index Settings".

3. An error message is displayed during log query, indicating that the asterisk (*) or question mark (?) cannot be used at the beginning of a word.

   Solution: Modify the query statement or use a correct delimiter to avoid such queries.

4. An error message is displayed during log query, indicating that long and float fields do not support fuzzy query using asterisks (*) or question marks (?).

   Solution: Modify the query statement and use the operator (>=<) or IN syntax for range query.

5. An error message is displayed during log query, indicating that string fields do not support range query using the operator (>=<) or IN syntax.

   Solution

   - Modify the query statement and use the asterisk (*) or question mark (?) to perform fuzzy query.
   - Change the value of this field to a number.

6. An error message is displayed during log query, indicating that the search syntax is incorrect and the query statement need to be modified.
   - Possible cause: The syntax of the operator is incorrect.

     Solution: Each operator has its syntax rule. Modify the search statement. For details, see Search Syntax. For example, the syntax rule for the operator = requires that the value on the right must be digits.

   - Possible cause: The search statement contains syntax keywords.

     Solution: If the log to search contains syntax keywords, the search statement must be enclosed in double quotation marks to convert the keywords into common characters. For details, see section "Search

Syntax". For example, if **and** is a syntax keyword, change the query statement **field:and** to **field:"and"**.

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. 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.
4. 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: unique access key ID associated with an SK. It is used together with the SK to sign requests.

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

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

NOTE

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

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

Procedure

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

   NOTE

   Keep the AK/SK pair secure.

A Change History

Released On	Description
2024-04-14	This issue is the first official release.